Informatica®
10.5.2

Guía de seguridad

Informatica Guía de seguridad
10.5.2
Abril 2022

Fecha de publicación: 2022-06-22

Tabla de contenido

Prefacio

Use la *Guía de seguridad de Informatica* para obtener información sobre cómo habilitar la seguridad en un dominio de Informatica. Sepa cómo configurar y administrar varios protocolos de autenticación, como el protocolo ligero de acceso a directorios, Kerberos y el lenguaje de marcado de aserción de seguridad. Aprenda también a administrar usuarios y grupos y a usar permisos, privilegios y funciones para administrar la seguridad de los usuarios.

Recursos de Informatica

Informatica proporciona una variedad de recursos de productos a través de Informatica Network y otros portales en línea. Use los recursos para sacar el mayor provecho de los productos y las soluciones de Informatica y aprender de otros expertos en la materia y usuarios de Informatica.

Informatica Network

Informatica Network es la puerta de entrada a muchos recursos, entre ellos, la base de conocimientos de Informatica y el servicio internacional de atención al cliente de Informatica. Para entrar en Informatica Network, visite https://network.informatica.com.

Como miembro de Informatica Network, tiene las siguientes opciones:

- Buscar recursos de productos en la base de conocimientos
- Vea la información de disponibilidad del producto.
- Crear y revisar casos de soporte
- Buscar su red de grupos de usuarios de Informatica locales y colaborar con sus iguales.

Base de conocimiento de Informatica

Use la base de conocimientos de Informatica para encontrar recursos de productos como artículos prácticos, procedimientos recomendados, tutoriales de video y respuestas a preguntas frecuentes.

Para buscar en la base de conocimiento, visite https://search.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.

Documentación de Informatica

Use el portal de documentación de Informatica para recorrer una extensa biblioteca de documentación para las versiones de productos actuales y recientes. Para recorrer el portal de documentación, visite https://docs.informatica.com.

Si tiene preguntas, comentarios o ideas acerca de la documentación de los productos, póngase en contacto con el equipo de la documentación de Informatica en infa_documentation@informatica.com.

Matrices de disponibilidad de producto 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 y destinos de datos admitidos por la versión de un producto. Puede recorrer las PAM de Informatica en https://network.informatica.com/community/informatica-network/product-availability-matrices.

Informatica Velocity

Informatica Velocity es una colección de consejos y procedimientos recomendados desarrollados por los servicios profesionales de Informatica que se basan en experiencias reales de cientos de proyectos de administración de datos. Informatica Velocity represente el conocimiento colectivo de los consultores de Informatica que trabajan con organizaciones de todo el mundo para planificar, desarrollar, implementar y dar mantenimiento a soluciones de administración de datos exitosas.

Puede encontrar 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.

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. Aproveche cualquiera de los cientos de soluciones de socios y desarrolladores de Informatica que se encuentran en el catálogo para mejorar su productividad y acelerar la implementación de los proyectos. Puede encontrar el 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 de Informatica Network.

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: https://www.informatica.com/services-and-training/customer-success-services/contact-us.html.

Para buscar recursos de asistencia en línea en Informatica Network, visite https://network.informatica.com y seleccione la opción eSupport.

CAPÍTULO 1

Introducción a la seguridad de Informatica

Este capítulo incluye los siguientes temas:

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

Puede emplear la utilidad de administración de claves y certificados Java keytool para crear un certificado SSL o una solicitud de firma de certificado (CSR), así como almacenes de claves y truststores en formato JKS.

La utilidad keytool se encuentra en el siguiente directorio de los nodos de dominio:

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

Si los nodos de dominio se ejecutan en AIX, puede utilizar la utilidad keytool que se proporciona con el JDK de IBM para crear un certificado SSL o una solicitud de firma de certificado (CSR), así como almacenes de claves y truststores.

OpenSSL

Puede utilizar OpenSSL para crear un certificado SSL o una 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 *_infaInternalNamespace*. El dominio de seguridad _infaInternalNamespace contiene la cuenta de usuario Administrador predeterminada que creó durante la instalación. Tras la instalación, no puede añadir usuarios al dominio de seguridad _infaInternalNamespace 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

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.

Cuando el dominio de Informatica reside en las instalaciones y no en una instancia AWS EC2, no puede usar el protocolo de autenticación EMRFS en integración con Amazon EMR.

Puede cifrar el token de credenciales del usuario con la clave de sitio única. Para cifrar el token de credenciales del usuario, configure la variable de entorno `infaEnableAdvancedEncryptionSchemeForCredential` como *true*. En el caso de la autenticación de usuario nativa y LDAP, después de la autenticación de usuario correcta, se utiliza el token de credenciales cifrado en lugar de la contraseña de usuario.

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

Un dominio de Informatica se puede configurar para que los usuarios de un servicio de directorio de LDAP puedan iniciar sesión en aplicaciones cliente de Informatica. Se pueden crear varias configuraciones de

LDAP de un dominio, y cada una de ellas se conecta a un servidor de LDAP distinto. Un dominio 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.

Un dominio de Informatica se puede configurar para que use la autenticación entre dominios Kerberos. Con la autenticación entre dominios Kerberos, los clientes de Informatica que pertenecen a un dominio Kerberos se pueden autenticar en los nodos y servicios de aplicación que pertenecen a otro dominio Kerberos.

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.

Autenticación SAML para aplicaciones web de Informatica

Un dominio de Informatica se puede configurar para permitir a los usuarios utilizar la autenticación del lenguaje de marcado de aserción de seguridad (SAML) para iniciar sesión en las aplicaciones web de la herramienta del administrador, la herramienta del analista, la herramienta de ingesta masiva, Metadata Manager 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) son el proveedor de identidad, que autentica 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

Autenticación de LDAP

Este capítulo incluye los siguientes temas:

Resumen

Un dominio de Informatica se puede configurar para permitir que los usuarios importados de uno o varios servicios de directorio de LDAP inicien sesión en nodos, servicios y clientes de aplicaciones de Informatica, como Informatica Developer e Informatica Analyst.

Un servicio de directorio de LDAP almacena los nombres de usuario y las contraseñas de las cuentas. El uso de la autenticación de LDAP permite consolidar las credenciales de todos los usuarios de Informatica en un único almacén de identidades, lo que simplifica la labor de crear y actualizar las credenciales de cuenta.

La autenticación nativa y la autenticación de LDAP se pueden utilizar a la vez en un dominio de Informatica. El administrador de servicios que se ejecuta en el nodo de puerta de enlace maestra del dominio autentica a los usuarios en función del dominio de seguridad al que pertenezcan los usuarios. Si un usuario pertenece al dominio de seguridad nativo predeterminado, el administrador de servicios autentica al usuario con la información de cuenta en el repositorio de configuración del dominio. Si el usuario pertenece a un dominio de seguridad de LDAP, el administrador de servicios pasa las credenciales del usuario al servidor de LDAP para la autenticación.

Dominios de seguridad de LDAP

Un dominio de seguridad de LDAP contiene usuarios y grupos importados desde un servicio de directorio de LDAP. Es posible definir varios dominios de seguridad de LDAP en un dominio de Informatica. A

continuación, se pueden importar cuentas desde diversos servicios de directorio de LDAP en los dominios de seguridad.

Debe crear un dominio de seguridad de LDAP si configura un dominio de Informatica para utilizar la autenticación Kerberos. 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.

Cuando crea un dominio de seguridad de LDAP, configura bases de búsqueda y filtros que definen el conjunto de cuentas de usuario y grupos de LDAP que deben incluirse en el dominio de seguridad. El administrador de servicios utiliza la configuración del dominio de seguridad para importar o sincronizar los usuarios y grupos en el dominio de seguridad con los usuarios y grupos en el servicio de directorio de LDAP.

El administrador de servicios utiliza los siguientes criterios cuando importa o sincroniza usuarios y grupos dentro de un dominio de seguridad de LDAP:

- El administrador de servicios utiliza las bases de búsqueda y los filtros de usuario para importar cuentas de usuario.
- El administrador de servicios utiliza las bases de búsqueda y los filtros de grupo para importar grupos.
- El administrador de servicios importa los grupos incluidos en el filtro de grupos y las cuentas de usuario incluidas en el filtro de usuarios.

Sincronización de cuentas de usuario

El administrador de servicios actualiza el dominio de seguridad con los usuarios y grupos en un servicio de directorio LDAP de forma programada. Puede configurar el programa de sincronización cuando establezca la autenticación de LDAP.

El administrador de servicios realiza los siguientes pasos durante la sincronización:

- Recupera una lista actualizada de los usuarios y grupos del servicio de directorio de LDAP, basada en la base de búsqueda y los filtros que configuró para el dominio de seguridad.
- Actualiza la lista de usuarios y grupos de LDAP en el dominio de seguridad. Si un usuario de LDAP en el dominio de seguridad se eliminó en el servicio de directorio de LDAP, el administrador de servicios transfiere la propiedad de los objetos del usuario a la cuenta del administrador del dominio.

Servicios de directorio de LDAP

Las cuentas de usuario se pueden importar en un dominio de seguridad de Informatica desde diversos servicios de directorio de LDAP.

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

- IBM Tivoli Directory Server
- Microsoft Active Directory
- Microsoft Azure Active Directory
- Novell eDirectory
- OpenLDAP

- Oracle Directory Server (ODSEE)
- Oracle Unified Directory (OUD)
- Sun Java System Directory Server

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

El administrador de servicios requiere un ID único (UID) para poder identificar usuarios en cada servicio de directorio de LDAP. En la siguiente tabla se muestra el UID predeterminado de cada servicio de directorio de LDAP:

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

Azure Active Directory para la autenticación de LDAP seguro

Los usuarios se pueden importar desde Azure Active Directory (Azure AD) a un dominio de seguridad de LDAP.

Azure Active Directory Domain Services proporciona una dirección IP pública de LDAP seguro que se utiliza para importar cuentas de usuario de Azure Active Directory a un dominio de seguridad de LDAP. Los usuarios que se importan pueden utilizar sus credenciales de LDAP para iniciar sesión en nodos, servicios y aplicaciones de Informatica que se ejecutan en máquinas virtuales en un dominio administrado por Azure Active Directory.

Para ver las versiones compatibles de Active Directory, consulte la tabla de disponibilidad de productos en Informatica Network: https://network.informatica.com/community/informatica-network/product-availability-matrices.

Debe habilitar la autenticación de Protocolo ligero de acceso a directorios seguro (LDAP seguro) en Azure Active Directory Domain Services para autenticar a los usuarios de Informatica.

Puede consultar los siguientes artículos de la biblioteca de procedimientos de Informatica para obtener una visión completa del proceso para usar la autenticación LDAP con Active Directory:

- Enabling SAML Authentication with Active Directory Federation Services in Informatica 10.4.0
- Enabling SAML Authentication with Azure Active Directory for Web Applications

Prepararse para importar cuentas de usuario de Active Directory

Complete los siguientes pasos para importar cuentas de usuario de Azure Active Directory a un dominio de Informatica:

1. Compruebe que se pueda acceder a través del cortafuegos al puerto 636, que es el puerto LDAP seguro de Azure Active Directory.
2. Habilite la autenticación de LDAP seguro en Azure Active Directory Domain Services.

   Utilice el portal de Azure para habilitar LDAP seguro en Azure Active Directory Domain Services. Para obtener información acerca de cómo configurar LDAP seguro en Azure Active Directory Domain Services, consulte el siguiente vínculo:

   https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-admin-guide-configure-secure-ldap
3. Cuando configure el certificado de LDAP seguro en Azure Active Directory Domain Services, asegúrese de que el nombre de Asunto en el certificado sea el nombre de dominio completo (FQDN) de Azure Active Directory.
4. Convierta el formato PFX del certificado de LDAP seguro al formato PEM. Java requiere que el certificado esté en formato PEM.
5. Importe los certificados que utilizan todos los nodos de dominio al archivo de truststore `cacerts` de Java del siguiente directorio en un nodo de puerta de enlace del dominio:

   ```
   <directorio de instalación de Informatica>/java/jre/lib/security/
   ```
6. Copie el archivo `cacerts` que contiene los certificados importados en el mismo directorio de cada nodo de puerta de enlace del dominio.
7. Añada la dirección IP pública de Azure Active Directory y el nombre de dominio completo (FQDN) de Azure Active Directory al archivo /etc/hosts en cada nodo de puerta de enlace en el dominio. Use el siguiente formato:

   ```
   <dirección IP de host de Azure Active Directory> ldaps.<FDQN de Azure Active Directory>
   ```

Crear una configuración de LDAP

Se pueden crear una o varias configuraciones de LDAP para permitir que las cuentas de usuario y los grupos de usuarios importados desde diversos servicios de directorio de LDAP se puedan autenticar en un dominio de Informatica.

La creación y administración de los usuarios y grupos de LDAP se realiza en el servicio de directorio de LDAP. Hay que configurar una conexión con el servidor de directorio de LDAP y usar filtros de búsqueda para especificar los usuarios y grupos que quiere que tengan acceso al dominio de Informatica. Tras ello, las cuentas de usuario se importan en un dominio de seguridad de LDAP. Si el servidor de LDAP utiliza un protocolo SSL, también debe especificar la ubicación del certificado de SSL.

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, hay que 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 en el que se van a importar las cuentas de usuario. También puede utilizar el cuadro de diálogo Configuración de LDAP para configurar un programa de sincronización.

Haga lo siguiente para crear una configuración de LDAP:

1. Configure la conexión con el servidor de LDAP que contiene el servicio de directorio desde el que quiere importar las cuentas de usuario y los grupos de usuarios.
2. Debe crear un dominio de seguridad de LDAP para cada conjunto de cuentas de usuario y grupos que desee importar desde el servidor de directorio de LDAP.
3. Configure una programación diaria para que el administrador de servicios actualice los dominios de seguridad de LDAP con los usuarios y grupos nuevos o modificados en el servicio de directorio de LDAP.

Crear la configuración de LDAP y configurar la conexión de servidor de LDAP

Cree la configuración de LDAP y configure la conexión con el servidor de LDAP que contiene el servicio de directorio desde el que desea importar las cuentas de usuario.

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 que utiliza cada nodo del dominio en el archivo de truststore `cacerts` en un dominio de nodos de puerta de enlace. Después, copie el archivo `cacerts` que contiene los certificados importados en el mismo directorio de cada nodo del dominio. Para obtener más información, consulte "Uso de un certificado SSL autofirmado" en la página 31.

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 la ficha **Configuración de LDAP**.
3. Haga clic en el menú **Acciones** y, luego, seleccione **Crear configuración de LDAP**.
4. En el cuadro de diálogo **Crear configuración de LDAP**, haga clic en la ficha **Conectividad de LDAP**.
5. Configure las propiedades de conexión del servidor de LDAP.

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

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

Propiedad	Descripción
Nombre de configuración de LDAP	Nombre de la configuración de LDAP.
Nombre del servidor	Nombre de host o dirección IP del equipo que hospeda el servicio de directorio de LDAP.

Propiedad	Descripción
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. **Nota:** Si utiliza la autenticación Kerberos, debe seleccionar el servicio 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. Para conectar con Azure Active Directory, especifique el nombre de la entidad de seguridad del usuario (UPN) del usuario principal.
Contraseña	La contraseña del usuario principal. Déjela en blanco para un inicio de sesión anónimo.
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.
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.
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, *member* o *memberof*.
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.

6. Haga clic en **Probar conexión** para verificar que la conexión al servidor de LDAP sea válida.
7. Haga clic en **Aceptar** para guardar la configuración de LDAP.

Configurar el dominio de seguridad

Debe crear un dominio de seguridad de LDAP para cada conjunto de cuentas de usuario y grupos que desee importar desde el servidor de directorio de LDAP. Establezca bases de búsqueda y filtros para definir el conjunto de cuentas de usuario y grupos que se deben incluir en un dominio de seguridad.

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 ni grupos de LDAP si los nombres no siguen las reglas de nombres de usuarios o grupos nativos. Tenga en cuenta que, a diferencia de los nombres de usuarios nativos, los nombres de usuarios de LDAP pueden distinguir mayúsculas de minúsculas.

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 utiliza los filtros para importar grupos y la lista de usuarios que pertenecen a cada grupo.

Si modifica las propiedades de conexión de LDAP para que se conecte a un servidor de LDAP diferente, el administrador de servicios 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 Informatica.

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**.

   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. No se aplica la distinción entre mayúsculas y minúsculas al nombre, el cual debe ser único en el dominio. La cadena 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.

5. 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.

6. 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.

7. Haga clic en **Aceptar** para guardar el dominio de seguridad.

Configurar el programa de sincronización

Puede configurar una programación diaria para que el administrador de servicios actualice los dominios de seguridad de LDAP con los usuarios y grupos nuevos o modificados en el servicio de directorio de LDAP.

Cuando el administrador de servicios sincroniza los dominios de seguridad de LDAP con el servicio de directorio de LDAP, importa todos los usuarios que coinciden con la configuración del filtro de usuarios del servicio de directorio de LDAP en el dominio de seguridad. A continuación, el administrador de servicios importa todos los grupos que coinciden con la configuración del filtro de grupos, y asocia los usuarios a los grupos correspondientes. El administrador de servicios también elimina del dominio de seguridad todos los usuarios o grupos que no encuentre en el servicio de directorio de LDAP.

De forma predeterminada, el administrador de servicios no tiene una hora programada para la sincronización con el servicio de directorio de LDAP. Para garantizar que la lista de usuarios y grupos en los dominios de seguridad de LDAP sea precisa, programe el momento en el que el administrador de servicios sincronizará los dominios de seguridad de LDAP con el servicio de directorio 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.

Para garantizar que la sincronización se realice correctamente, tenga en cuenta las siguientes recomendaciones antes de configurar el programa de sincronización:

Compruebe que el archivo /etc/hosts contenga una entrada para el servidor de LDAP.

Compruebe que el archivo `/etc/hosts` en cada puerta de enlace de nodo en el dominio contenga una entrada con el nombre de host y la dirección IP del servidor de LDAP. Si el administrador de servicios no puede resolver el nombre de host del servidor de LDAP, la sincronización podría generar un error.

Habilite la paginación en LDAP si va a sincronizar más de 100 usuarios o grupos.

Habilite la paginación en el servicio de directorio de LDAP antes de sincronizar más de 100 usuarios o grupos. Si no habilita la paginación en el servicio de directorio de LDAP, la sincronización puede fallar.

Sincronice los dominios de seguridad en los momentos del día donde la mayoría de los usuarios no estén conectados a las aplicaciones de Informatica.

Durante la sincronización, el administrador de servicios bloquea todas las cuentas de usuario que sincroniza. Es posible que los usuarios no puedan iniciar sesión en los clientes de aplicación de Informatica durante la sincronización. Es posible que los usuarios que hayan iniciado sesión en un cliente de aplicación cuando comience la sincronización no puedan realizar ciertas tareas.

Para configurar un programa que sincronice los dominios de seguridad de LDAP con el servicio de directorio 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 **Programar**.
4. Haga clic en el botón **Añadir** (+) para añadir una hora.

   El programa de sincronización utiliza un formato de 24 horas.
5. Para sincronizar inmediatamente los usuarios y grupos de los dominios de seguridad de LDAP 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: Espere hasta que el administrador de servicios se sincronice con el servicio de directorio de LDAP antes de reiniciar el dominio de Informatica para evitar perder los períodos de sincronización que defina en el programa.

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, emplee la utilidad de administración de claves y certificados Java keytool para importar los certificados que utilizan todos los nodos de dominio al archivo de truststore `cacerts` de Java en un nodo de puerta de enlace del dominio. Después, copie el archivo de almacén de claves `cacerts` que contiene los certificados importados en los otros nodos 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\bin
```

Reinicie el nodo después de importar el certificado.

Eliminar una configuración de LDAP

Una configuración de LDAP y los dominios de seguridad asociados correspondientes se pueden eliminar para prohibir de forma permanente que los usuarios accedan al dominio.

Cuando una configuración de LDAP se elimina, antes hay que eliminar los dominios de seguridad asociados a ella. El administrador de servicios elimina de la base de datos de configuración del dominio todas las cuentas de usuario y todos los grupos que haya en cada dominio de seguridad de LDAP.

1. En la Herramienta del administrador, haga clic en la ficha **Seguridad**.
2. Haga clic en la ficha **Configuración de LDAP**.
3. Haga clic en la ficha **Dominios de seguridad** y, después, en el botón **Editar**.
4. Seleccione un dominio de seguridad en el cuadro de diálogo **Editar configuración de LDAP** y, luego, haga clic en **Eliminar**.
5. Seleccione la configuración de LDAP que quiera eliminar en el navegador de configuraciones de LDAP.
6. Haga clic en el menú **Acciones** y, luego, seleccione **Eliminar configuración de LDAP**.
7. Haga clic en **Aceptar** para confirmar que desea eliminar la configuración de LDAP.

CAPÍTULO 4

Autenticación Kerberos

Este capítulo incluye los siguientes temas:

Resumen de Kerberos

Kerberos es un protocolo informático de autenticación de red que permite la comunicación entre clientes, nodos y servicios de Informatica en una red para conectarse entre sí de modo seguro.

La autenticación Kerberos elimina las cuentas nativas de Informatica y hace que no sea necesario pasar las credenciales de usuario a un servidor LDAP. Después de habilitar la autenticación Kerberos en un dominio, los clientes de Informatica usan los vales de Kerberos creados durante el proceso de autenticación de Windows para iniciar sesión en los servicios de Informatica que se ejecutan en el dominio.

Puede habilitar la autenticación Kerberos en un dominio que se ejecuta en una red de Windows. La red debe usar Microsoft Active Directory Domain Services (AD DS) como base de datos de entidad de seguridad de Kerberos.

Para habilitar la autenticación de Kerberos en un dominio de Informatica, lleve a cabo los siguientes pasos:

Prepárese para habilitar la autenticación Kerberos.

Deberá completar varias tareas antes de habilita la autenticación Kerberos. Las tareas que debe completar son las siguientes:

- Cree el archivo de configuración de Kerberos.
- Cree cuentas de usuarios de la entidad de seguridad de Kerberos en Active Directory.
- Genere el nombre de entidad de seguridad de servicio (SPN) y los formatos de tablas de claves.
- Cree los archivos de tabla de claves usados para autenticar los usuarios y servicios de la red.

Habilite la autenticación Kerberos en el dominio de Informatica.

Puede habilitar la autenticación Kerberos en un dominio de Informatica cuando instale los servicios de Informatica. También puede habilitar la autenticación Kerberos después de instalar los servicios. 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.

Habilite la autenticación Kerberos en nodos o hosts cliente de Informatica

Después de habilitar Kerberos en el dominio, copie el archivo de configuración de Kerberos en cada nodo del dominio y en cada host cliente de Informatica. Configure también los exploradores web para que accedan a las aplicaciones web de Informatica.

Permita que los usuarios de Informatica puedan usar la autenticación de Kerberos.

Después de habilitar la autenticación Kerberos, importe los usuarios de Informatica desde Active Directory en un dominio de seguridad de LDAP que contenga las cuentas de usuario de Kerberos. También debe migrar los grupos, las funciones, los privilegios y los permisos de las cuentas de usuario nativas a las cuentas de usuario del dominio de seguridad de LDAP.

Cómo funciona Kerberos en un dominio de Informatica

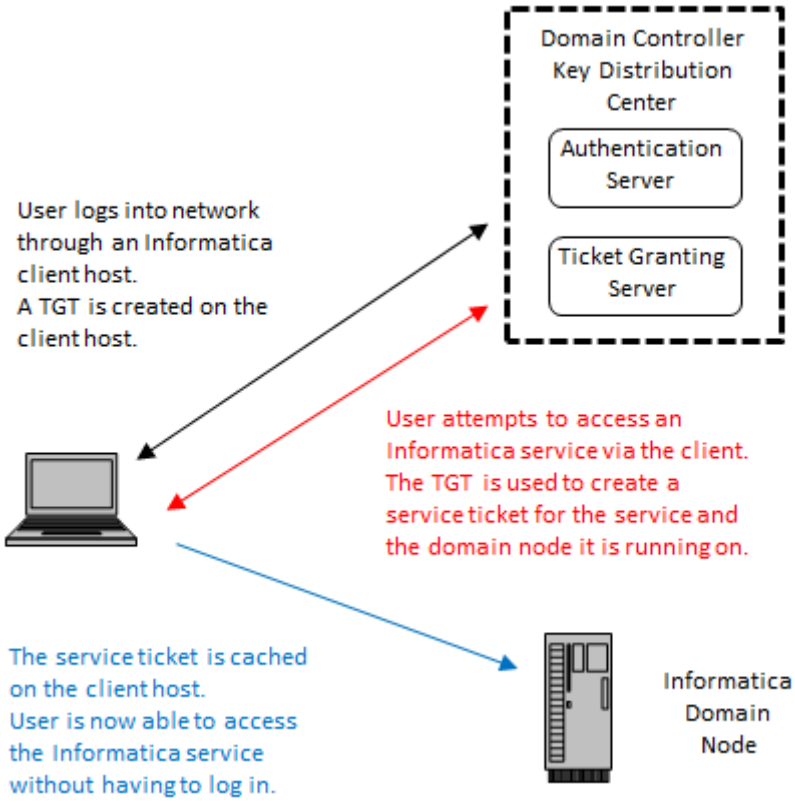
En un dominio configurado para usar la autenticación Kerberos, los clientes de Informatica se autentican con nodos y servicios de aplicación en el dominio, sin necesidad de contraseñas.

En un dominio donde se usa la autenticación Kerberos, los servicios que se ejecutan dentro de ese dominio (procesos de nodo, procesos de aplicación web y servicios de aplicación de Informatica incluidos) son *entidades de seguridad* de Kerberos. La base de datos de entidades de seguridad de Active Directory que el dominio Kerberos utiliza contiene una cuenta de usuario por cada entidad de seguridad.

El protocolo de autenticación Kerberos emplea *tablas de claves* para autenticar clientes de Informatica con servicios que se ejecutan dentro del dominio. La tabla de claves de una entidad de seguridad se almacena en el nodo en el que el servicio se ejecuta. La tabla de claves contiene el *nombre de entidad de seguridad del servicio (SPN)* que distingue al servicio dentro del dominio Kerberos, así como la clave asignada a dicho SPN en Active Directory.

Cuando el KDC da un vale de servicio a un cliente, cifra el vale con la clave asignada al SPN. El servicio solicitado utiliza la clave para descifrar el vale de servicio.

La siguiente imagen muestra el flujo básico de la autenticación Kerberos:



El siguiente gráfico describe el flujo básico de la autenticación Kerberos:

1. Un usuario de cliente de Informatica inicia sesión en un equipo de la red que aloja un cliente de Informatica.
2. La solicitud de inicio de sesión se dirige al *servidor de autenticación*, un componente del *centro de distribución de claves (KDC) de Kerberos*. El KDC es un servicio de red con acceso a la información de la cuenta del usuario que se ejecuta en cada controlador de dominio del dominio de Active Directory.
3. El Servidor de autenticación comprueba que el usuario existe en la base de datos de la entidad de seguridad y después crea un token de Kerberos llamado *ticket-granting-ticket (TGT)* en el equipo del usuario.
4. El usuario intenta acceder a un proceso o servicio del dominio de Informatica mediante un cliente de Informatica.
5. Informatica y las bibliotecas de Kerberos usan el TGT para solicitar un *vale de servicio* y una *clave de sesión* del servicio solicitado al *servidor de concesión de vales*, que también se ejecuta en el KDC.

   Por ejemplo si el usuario accede a un Servicio de repositorio de modelos del cliente de Informatica Developer, el TGT solicita un vale de servicio del nodo en el que se ejecuta el servicio solicitado. El TGT también solicita un vale de servicio del Servicio de repositorio de modelos.
6. Kerberos usa el vale de servicio para autenticar el cliente con el servicio solicitado.
   El vale de servicio se almacena en la memoria caché en el equipo que aloja el cliente de Informatica, permitiendo que el cliente use el vale mientras siga siendo válido. Si el usuario cierra y después reinicia el cliente de Informatica, el cliente vuelve a usar el mismo vale para acceder a los procesos y servicios del dominio de Informatica.

Autenticación entre dominios Kerberos

Un dominio de Informatica se puede configurar para que use la autenticación entre dominios Kerberos. Con la autenticación entre dominios Kerberos, los clientes de Informatica que pertenecen a un dominio Kerberos se pueden autenticar en los nodos y servicios de aplicación que pertenecen a otro dominio Kerberos.

Cuando se configura un dominio para que use la autenticación entre dominios Kerberos, las propiedades de cada dominio Kerberos se añaden al archivo de configuración de Kerberos. También se incluye el nombre de cada dominio cuando se ejecutan comandos infasetup para permitir la autenticación Kerberos en el dominio y en los nodos de dominio.

Los servidores de Active Directory que el dominio usa en la autenticación entre dominios Kerberos deben pertenecer al mismo bosque de Active Directory. Un bosque de Active Directory es un grupo de dominios de Active Directory que tienen en común un catálogo global, un esquema de directorio, una estructura lógica y una configuración de directorio. Hay que conectarse al catálogo global para importar usuarios desde los servidores de Active Directory a los dominios de seguridad de LDAP.

Para usar la autenticación entre dominios Kerberos, debe haber una confianza bidireccional habilitada entre los servidores de Active Directory y el bosque.

Pasar un dominio de autenticación de un solo dominio Kerberos a autenticación entre dominios Kerberos

Un dominio de Informatica que usa un solo dominio Kerberos se puede convertir para autenticar usuarios que usen la autenticación entre dominios Kerberos.

El dominio se debe actualizar a la versión 10.2 HotFix 2 para que se pueda convertir para usar la autenticación entre dominios Kerberos.

También hay que importar las cuentas de usuario y de grupo desde el catálogo global de Active Directory a un dominio de seguridad de LDAP. Cuando se importan cuentas, las cuentas existentes en el dominio de seguridad de LDAP (que hacen uso del atributo de nombre samAccount) se eliminan y reemplazan por otras nuevas que utilizan el atributo de nombre de entidad de seguridad.

Los usuarios inician sesión en los clientes de Informatica mediante el nombre de entidad de seguridad de usuario completo, que presenta el siguiente formato:

```
<nombre de usuario>@<NOMBRE DE DOMINIO KERBEROS>
```

Tras importar las cuentas de usuario y de grupo, asigne a ellas privilegios, funciones y permisos.

1. Actualice el dominio a la versión 10.2 HotFix 2.
2. Añada al archivo de configuración de Kerberos las propiedades de cada dominio Kerberos que sean necesarias.

   Establezca las propiedades de cada dominio en el archivo de configuración `krb5.conf` de cada nodo del dominio. Reinicie el dominio después de actualizar el archivo en todos los nodos del dominio.

   Para obtener más información sobre cómo configurar el archivo de configuración `krb5.conf` para la autenticación entre dominios Kerberos, consulte "Configurar el archivo de configuración de Kerberos" en la página 38.
3. Copie el archivo `krb5.conf` actualizado en el siguiente directorio de todos los equipos que alojen un cliente de Informatica:

   ```
   <directorio de instalación de Informatica>\clients\shared\security
   ```
4. Ejecute los comandos infasetup UpdateGatewayNode e infasetup UpdateWorkerNode en los nodos de dominio.

Especifique los nombres de los dominios Kerberos que el dominio usa para autenticar usuarios como los valores de las opciones -srn y -urn (separados por una coma).

Para obtener más información sobre cómo ejecutar los comandos infasetup, consulte el capítulo de referencia de comandos infasetup de la *referencia de comandos de Informatica 10.2 HotFix 2*.

5. Ejecute el comando UpdateKerberosConfig en un nodo de puerta de enlace del dominio.

   Especifique los nombres de los dominios Kerberos que el dominio usa para autenticar usuarios como los valores de las opciones -srn y -urn (separados por una coma).

6. Ejecute el comando UpdateKerberosAdminUser en un nodo de puerta de enlace del dominio.

   Indique el nombre de entidad de seguridad de usuario completo de la cuenta del usuario administrador del dominio.

7. Importe las cuentas de usuario y de grupo a dominios de seguridad de LDAP.

   Conéctese al catálogo global de Active Directory. Cuando se establece una conexión con el catálogo global, se importan los usuarios desde el servidor de Active Directory que cada dominio Kerberos usa.

   Para obtener más información sobre cómo conectarse al catálogo global e importar cuentas, consulte "Importar cuentas de usuario desde Active Directory a dominios de seguridad de LDAP" en la página 60.

8. Asigne privilegios, funciones y permisos a las cuentas de usuario y de grupo que ha importado a un dominio de seguridad de LDAP.

   Para obtener más información sobre cómo asignar privilegios y funciones, consulte Capítulo 9, "Privilegios y funciones" en la página 147.

   Para obtener más información sobre cómo asignar permisos, consulte Capítulo 10, "Permisos" en la página 192.

Prepararse para habilitar la autenticación Kerberos

Deberá completar varias tareas para preparar la habilitación de la autenticación Kerberos en un dominio de Informatica. Los procedimientos que siga en cada tarea dependen del nivel de entidad de seguridad de servicio en el que habilite Kerberos.

Nota: No puede deshabilitar la autenticación Kerberos en un dominio después de habilitarla. Tampoco puede cambiar el nivel de entidad de seguridad de servicio entre el nivel de nodo y el nivel de proceso.

Determinar el nivel de entidad de seguridad de servicio de Kerberos

Cuando se prepare para habilitar la autenticación Kerberos, determine el nivel de entidad de seguridad de servicio requerido. El nivel de entidad de seguridad de servicio requerido determina los procedimientos que debe seguir para habilitar la autenticación Kerberos en el dominio.

Puede habilitar la autenticación Kerberos en uno de los siguientes niveles:

Nivel de nodo

Si usa el dominio para pruebas de validación o desarrollo, y el dominio no requiere un alto nivel de seguridad, puede habilitar Kerberos en el nivel de nodo. Puede usar un único nombre de entidad de seguridad de servicio y un único archivo de tabla de claves para el nodo y para todos los procesos y servicios que se ejecutan en el nodo. También debe crear un SPN y un archivo de tabla de claves para los procesos HTTP que se ejecutan en el nodo.

Nivel de proceso

Si utiliza el dominio para producción y este requiere un alto nivel de seguridad, puede configurar la entidad de seguridad del servicio a nivel de proceso. Cree un único SPN y un único archivo de tabla de claves para cada nodo y cada proceso del nodo. También debe crear un SPN y un archivo de tabla de claves para los procesos HTTP que se ejecutan en el nodo.

Kerberos habilitado a nivel de proceso proporciona el más alto nivel de seguridad, pero podría ser difícil de administrar en un dominio de Informatica que contenga muchos nodos o que tenga muchos servicios. En este escenario, sería conveniente habilitar Kerberos a nivel de nodo.

Configurar el archivo de configuración de Kerberos

Establezca las propiedades requeridas por Informatica en el archivo de configuración de Kerberos y después copie el archivo en cada nodo del dominio de Informatica.

Kerberos almacena la información de configuración en un archivo llamado *krb5.conf*. Debe establecer las propiedades en el archivo de configuración krb5.conf y, a continuación, copiar el archivo en cada nodo del dominio de Informatica.

Si el dominio usa la autenticación entre dominios Kerberos, indique las propiedades que se necesitan de cada dominio Kerberos.

1. En la sección *libdefaults* del archivo, configure las siguientes propiedades de biblioteca de Kerberos.

   La siguiente tabla describe las propiedades que se deben especificar:

Propiedad	Descripción
default_realm	El nombre del dominio Kerberos al que pertenecen los servicios del dominio de Informatica. El nombre del dominio debe escribirse en mayúsculas. Si el dominio usa un único dominio Kerberos en la autenticación, el nombre de dominio del servicio y el nombre de dominio del usuario deben ser el mismo.
forwardable	Permite que un servicio delegue credenciales de usuario del cliente a otro servicio. El dominio de Informatica requiere que los servicios de aplicación autentiquen las credenciales de usuario del cliente con otros servicios. Establecida en true.
default_tkt_enctypes	Los tipos de cifrado de la clave de sesión incluidos en los vales de concesión de vales (TGT). Establezca esta propiedad solo si las claves de la sesión deben usar tipos de cifrado específicos. Asegúrese de que el Centro de distribución de claves (KDC) de Kerberos admite el tipo de cifrado especificado. No establezca esta propiedad para permitir que el protocolo de Kerberos seleccione el tipo de cifrado que se debe usar. Si los hosts del nodo o los hosts del cliente de Informatica usan cifrado de 256 bits, instale los archivos de directiva de fortaleza ilimitada de Java Cryptography Extension (JCE) en todos los hosts del nodo y en los hosts del cliente de Informatica para evitar problemas con la autenticación.
rdns	Determina si se usa la búsqueda de nombres inversa además de la búsqueda de nombres directa para dar formato canónico a los nombres de hosts que se usarán en los nombres de entidad de seguridad del servicio. Establecida en false.
renew_lifetime	La vigencia renovable predeterminada de las solicitudes de vales iniciales.

Propiedad	Descripción
ticket_lifetime	La vigencia predeterminada de las solicitudes de vales iniciales.
udp_preference_limit	Determina el protocolo que utiliza Kerberos cuando envía un mensaje al KDC. Establézcalo en 1 para usar el protocolo TCP si el dominio tiene errores de autenticación Kerberos intermitentes.
dns_lookup_kdc	Indica si el cliente Kerberos utiliza registros SRV de DNS para localizar los KDC u otros servidores para un dominio, si no aparecen en la información del dominio. DNS utiliza registros SRV para identificar equipos que alojan servicios específicos del host. Obligatoria cuando el dominio está habilitado para Kerberos. Requiere que defina la propiedad de dominio admin_server. Establecida en true.
dns_lookup_realm	Indica si el cliente Kerberos utiliza registros TXT de DNS para determinar el dominio Kerberos de un host. DNS utiliza registros de texto o TXT para asociar texto arbitrario con un host u otro nombre, como información legible sobre un servidor, una red, un centro de datos u otra información de contabilidad. Obligatoria cuando el dominio está habilitado para Kerberos. Establecida en true.

2. Defina cada dominio Kerberos en la sección *realms* del archivo.

   En el siguiente ejemplo se muestra la entrada de un dominio Kerberos llamado COMPANY.COM:

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

3. Indique las siguientes propiedades de dominio dentro de los corchetes de cada dominio Kerberos en la sección *realms* del archivo.

   La siguiente tabla describe las propiedades que se deben especificar:

Propiedad	Descripción
admin_server	El nombre o la dirección IP del host del servidor de administración de Kerberos. Puede incluir un número de puerto opcional separado del nombre de host por el signo de dos puntos. El valor predeterminado es 749. Obligatoria si configura dns_lookup_kdc en la sección *libdefaults*.
kdc	El nombre o la dirección IP de un host que ejecuta el Centro de distribución de claves (KDC) del dominio Kerberos. Puede incluir un número de puerto opcional separado del nombre de host por el signo de dos puntos. El valor predeterminado es 88.

   En el siguiente ejemplo se muestran las entradas de cada dominio Kerberos en una configuración entre dominios Kerberos:

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

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

4. En la sección *domain_realms*, asigne el nombre del dominio o el nombre de host a un nombre de dominio Kerberos. El nombre de dominio tiene un punto (.) como prefijo.

   En el siguiente ejemplo se muestran los parámetros del domain_realm de Hadoop si el dominio de Informatica no utiliza la autenticación Kerberos:

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

   En el siguiente ejemplo se muestran los parámetros del domain_realm de Hadoop si el dominio de Informatica utiliza la autenticación Kerberos:

   ```
   [domain_realm]
   .infa_ad_realm.com = INFA-AD-REALM
     infa_ad_realm.com = INFA-AD-REALM
   .hadoop_realm.com = HADOOP-REALM
     hadoop_realm.com = HADOOP-REALM
   ```

5. Copie el archivo `krb5.conf` en las siguientes ubicaciones del equipo que aloja el servicio de integración de datos:

   - `<Directorio de instalación de Informatica>/services/shared/security/`
   - `<Directorio de instalación de Informatica>/java/jre/lib/security/`

En el siguiente ejemplo se muestra el contenido de un archivo de configuración de Kerberos con las propiedades necesarias en una configuración de un solo dominio Kerberos:

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

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

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

En el siguiente ejemplo se muestra el contenido de un archivo de configuración de Kerberos con las propiedades necesarias en una configuración entre dominios Kerberos:

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

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

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

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

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

Crear cuentas de entidad de seguridad de Kerberos en Active Directory

Cree cuentas de usuario de LDAP para las entidades de seguridad de Kerberos en Active Directory. Una entidad de seguridad de Kerberos es un proceso, un servicio o un usuario en el dominio Kerberos.

Si establece la propiedad default_tkt_enctypes en el archivo de configuración krb5.conf con los tipos de cifrado AES de 128 bits o 256 bits, configure cada cuenta para que use el tipo de cifrado correspondiente en Active Directory.

Las cuentas que cree dependen de si habilita Kerberos en el nivel de nodo o en el nivel de proceso.

Nota: Los nombres de cuenta pueden tener una longitud máxima de 20 caracteres.

Cuentas requeridas a nivel de nodo

Cree las cuentas de usuario de LDAP requeridas para habilitar la autenticación Kerberos a nivel de nodo en Active Directory.

Cree las siguientes cuentas de entidad de seguridad de Kerberos en Active Directory si habilita Kerberos a nivel de nodo:

Procesos del nodo

Cree una cuenta por cada nodo que se ejecute en el dominio.

Proceso HTTP

Cree una cuenta para las aplicaciones web de Informatica que se ejecuten en un nodo del dominio. Las aplicaciones web que se ejecutan en un nodo podrían incluir la Herramienta del administrador, Informatica Analyst y Catalog Administrator. Cree una cuenta única que compartan todas las aplicaciones web que se ejecuten en el nodo.

Nombre distintivo (DN) del usuario de enlace

Cree una cuenta de usuario de enlace de LDAP que puede usar para sincronizar el dominio de seguridad de LDAP que contenga las cuentas de usuario de Kerberos con Active Directory.

Cuentas requeridas a nivel de proceso

Cree las cuentas de usuario de LDAP requeridas para habilitar la autenticación Kerberos a nivel de proceso en Active Directory.

Cree las siguientes cuentas de entidad de seguridad de Kerberos en Active Directory si habilita Kerberos a nivel de proceso:

Procesos del nodo

Cree una cuenta por cada nodo que se ejecute en el dominio.

Procesos HTTP

Cree una cuenta para las aplicaciones web de Informatica que se ejecuten en un nodo del dominio. Las aplicaciones web que se ejecutan en un nodo podrían incluir Informatica Analyst y Catalog Administrator. Cree una cuenta única que compartan todas las aplicaciones web que se ejecuten en el nodo.

Servicio de Informatica Administrator

Cree una cuenta de la Herramienta del administrador en cada nodo de puerta de enlace en el dominio.

Servicios de aplicación de Informatica

Cree una cuenta por cada servicio de aplicación de Informatica que se ejecute en cada nodo del dominio.

Nombre distintivo (DN) del usuario de enlace

Cree una cuenta de usuario de LDAP que puede usar para sincronizar el dominio de seguridad de LDAP que contenga las cuentas de usuario de Kerberos con Active Directory.

Generar los formatos de los nombres de la entidad de seguridad de servicio y del archivo de tabla de claves

Utilice la utilidad Informatica Kerberos SPN Format Generator para generar los formatos del nombre de entidad de seguridad de servicio (SPN) y del nombre de archivo de tabla de claves requeridos para usar la autenticación de Kerberos. La utilidad Kerberos SPN Format Generator genera un archivo de texto llamado SPNKeytabFormat.txt que contiene el formato correcto de los SPN y los nombre de archivo de tabla de claves.

Los formatos de SPN y de nombre de archivo de tabla de claves que genere dependen de si habilita Kerberos al nivel de nodo o al nivel de proceso.

Generar los formatos de los nombres de la entidad de seguridad de servicio y del archivo de tabla de claves a nivel de nodo

Genere los formatos de los SPN y los nombres de archivo de tabla de claves requeridos para habilitar la autenticación Kerberos a nivel de nodo.

El dominio de Informatica requiere SPN y archivos de tabla de claves para los siguientes procesos cuando se habilita la autenticación Kerberos a nivel de proceso:

Procesos del nodo

Informatica requiere un SPN y un archivo de tabla de claves para cada nodo del dominio. Kerberos utiliza el mismo nombre de entidad de seguridad de servicio y tabla de claves para autenticar los servicios de aplicación de Informatica que se ejecutan en el nodo.

Procesos HTTP

Informatica requiere un SPN y un archivo de tabla de claves para las aplicaciones web que se ejecutan en cada nodo del dominio. Las aplicaciones web que se ejecutan en un nodo podrían incluir la Herramienta del administrador, Informatica Analyst y Catalog Administrator. Kerberos utiliza el mismo nombre de entidad de seguridad de servicio para autenticar todas las aplicaciones web que se ejecutan en el nodo.

1. En un host del nodo de Informatica en Windows, vaya al directorio que contiene el archivo por lotes SPNFormatGenerator.bat:

   ```
   <directorio de instalación de Informatica>\tools\Kerberos
   ```

   En un host del nodo de Informatica en UNIX, vaya al directorio que contiene el archivo de shell SPNFormatGenerator.sh:

   ```
   <directorio de instalación de Informatica>/tools/Kerberos
   ```

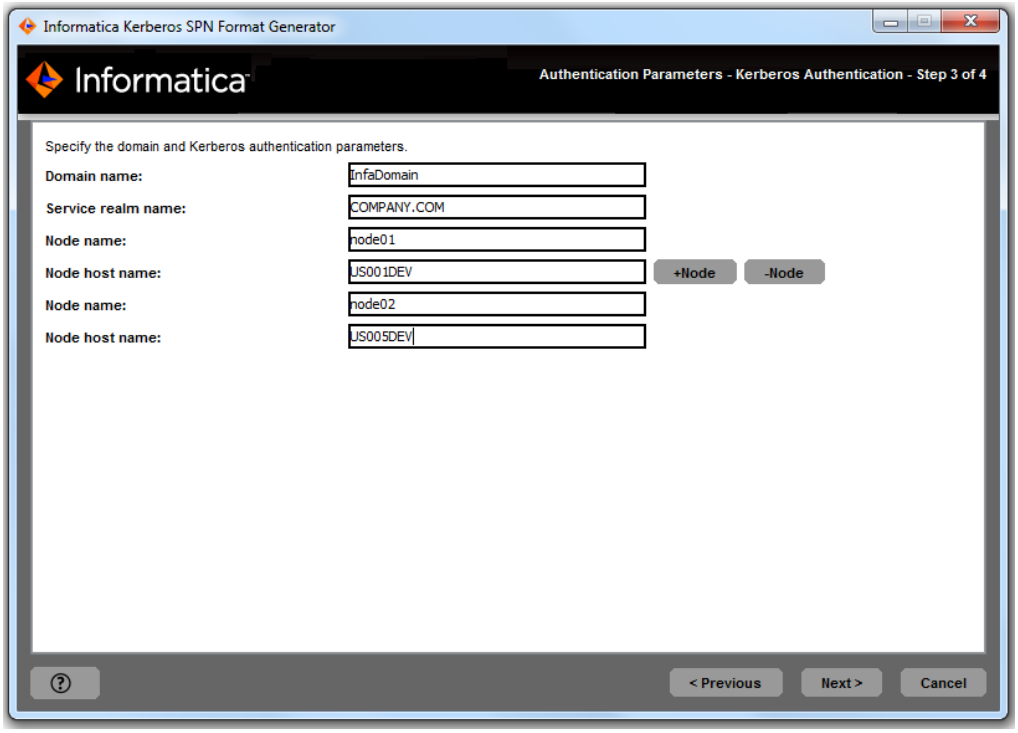
2. Ejecute SPNFormatGenerator.bat o SPNFormatGenerator.sh.
3. Haga clic en **Siguiente**.
4. Seleccione **Nivel de nodo**.
5. Haga clic en **Siguiente**.
6. Especifica las propiedades requeridas para generar los formatos de SPN y de archivo de tabla de claves.

   La siguiente tabla describe las propiedades:

Solicitud	Descripción
Nombre del dominio	Nombre de dominio de Informatica. El nombre no debe superar los 128 caracteres y debe ser ASCII de 7 bits. No puede contener un espacio ni cualquiera de los siguientes caracteres: ` % * + ; " ? , < > \ /
Nombre del dominio de servicio	Nombre del dominio Kerberos. El nombre del dominio debe escribirse en mayúsculas.
Nombre de nodo	El nombre del nodo de Informatica.
Nombre de host del nodo	Nombre completo del host de nodo. El nombre de host del nodo no puede contener el carácter de subrayado (_). **Nota:** No utilice *localhost*. El nombre de host debe identificar el host de forma expresa.

7. Para generar el formato de SPN para otro nodo, haga clic en **+nodo** y especifique el nombre del nodo y el nombre de host.

   En la siguiente imagen se muestran las entradas de varios nodos en el dominio InfaDomain de la utilidad SPN Format Generator:



8. Haga clic en **Siguiente**.

   La utilidad SPN Format Generator muestra la ruta y el nombre de archivo del archivo que contiene la lista de nombres de entidad de seguridad del servicio y los nombres de archivo de tabla de claves.

9. Haga clic en **Terminado** para salir de la utilidad SPN Format Generator.

Generar los formatos de los nombres de la entidad de seguridad de servicio y del archivo de tabla de claves a nivel de proceso

Genere los formatos de los SPN y los nombres de archivo de tabla de claves requeridos para habilitar la autenticación Kerberos a nivel de proceso.

El dominio de Informatica requiere SPN y archivos de tabla de claves para los siguientes procesos y servicios cuando se habilita la autenticación Kerberos a nivel de proceso:

Procesos del nodo

Informatica requiere un SPN y un archivo de tabla de claves para cada nodo del dominio.

Informatica Administrator

Informatica requiere un SPN y un archivo de tabla de claves para la Herramienta del administrador por cada nodo de puerta de enlace del dominio.

Procesos HTTP

Informatica requiere un SPN y un archivo de tabla de claves para las aplicaciones web que se ejecutan en un nodo del dominio. Las aplicaciones web que se ejecutan en un nodo podrían incluir Informatica Analyst y Catalog Administrator.

Procesos de servicio de la aplicación de Informatica

Informatica requiere un SPN y un archivo de tabla de claves para cada servicio de aplicación de Informatica se ejecuta en cada nodo del dominio.

1. En un host del nodo de Informatica en Windows, vaya al directorio que contiene el archivo por lotes SPNFormatGenerator.bat:

   ```
   <directorio de instalación de Informatica>\tools\Kerberos
   ```

   En un host del nodo de Informatica en UNIX, vaya al directorio que contiene el archivo de shell SPNFormatGenerator.sh:

   ```
   <directorio de instalación de Informatica>/tools/Kerberos
   ```

2. Ejecute SPNFormatGenerator.bat o SPNFormatGenerator.sh.
3. Haga clic en **Siguiente**.
4. Seleccione **Nivel de proceso**.
5. Haga clic en **Siguiente**.
6. Especifica las propiedades requeridas para generar los formatos de SPN y de archivo de tabla de claves.

   La siguiente tabla describe las propiedades:

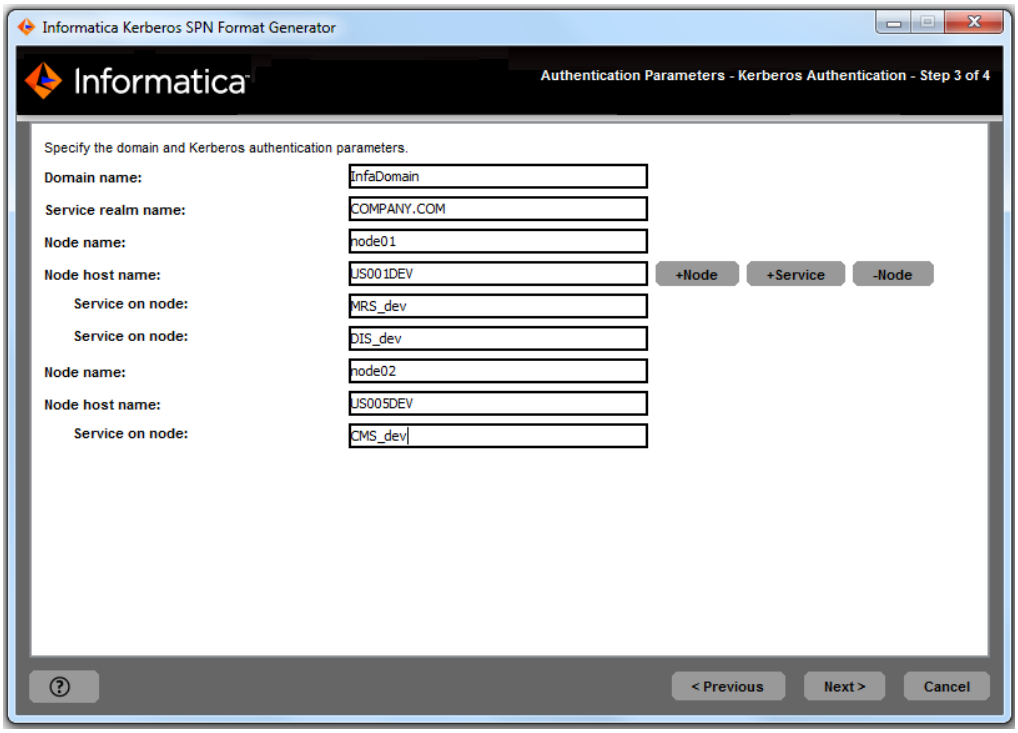
Solicitud	Descripción
Nombre del dominio	Nombre de dominio de Informatica. El nombre no debe superar los 128 caracteres y debe ser ASCII de 7 bits. No puede contener un espacio ni cualquiera de los siguientes caracteres: ` % * + ; " ? , < > \ /
Nombre del dominio de servicio	Nombre del dominio Kerberos. El nombre del dominio debe escribirse en mayúsculas.
Nombre de nodo	El nombre del nodo de Informatica.
Nombre de host del nodo	Nombre completo dirección IP del host del nodo. El nombre de host del nodo no puede contener el carácter de subrayado (_). **Nota:** No utilice *localhost*. El nombre de host debe identificar el host de forma explícita.

7. Para generar el formato de SPN de un servicio de aplicación de Informatica que se ejecuta en un nodo, haga clic en **Servicio** después de especificar los detalles del nodo.

   Especifique el nombre del servicio de aplicación de Informatica tal como se muestra en la Herramienta del administrador. Complete este paso por cada servicio de aplicación de Informatica que se ejecute en cada nodo del dominio.

8. Para generar el formato de SPN para otro nodo, haga clic en **+nodo** y especifique el nombre del nodo y el nombre de host.

   En la siguiente imagen se muestran las entradas de varios nodos y servicios de aplicación que se ejecutan en el dominio InfaDomain de la utilidad SPN Format Generator:



9. Haga clic en **Siguiente**.

   La utilidad SPN Format Generator muestra la ruta y el nombre de archivo del archivo que contiene la lista de nombres de entidad de seguridad del servicio y los nombres de archivo de tabla de claves.

10. Haga clic en **Terminado** para salir de la utilidad SPN Format Generator.

Revisar el archivo de texto de los formatos de nombres de la entidad de seguridad de servicio y del archivo de tabla de claves

Después de generar el archivo SPNKeytabFormat.txt, podrá revisarlo.

Use la información del archivo para generar los archivos de tabla de claves y para asociar cada SPN con la cuenta de usuario de entidad de seguridad correspondiente en Active Directory.

El archivo SPNKeytabFormat.txt contiene la siguiente información:

Nombre de entidad

Identifica el nodo o el servicio asociado al proceso.

Nombre de entidad de seguridad de servicio

Formato del SPN. El SPN distingue entre mayúsculas y minúsculas.

Nota: Si se especifica una cadena que contiene varios nombres de dominio Kerberos o se añade un asterisco antes del sufijo de un dominio (para, así, incluir todos los dominios que contengan ese sufijo), el formato del SPN no incluye el nombre de dominio.

En la tabla siguiente se describen los formatos de SPN:

Tipo de tabla de claves	Formato de SPN
NODE_SPN	isp/<nombre de nodo>/<nombre de dominio>@<NOMBRE DE DOMINIO KERBEROS>
NODE_AC_SPN	_AdminConsole/<nombre de nodo>/<nombre de dominio>@<NOMBRE DE DOMINIO KERBEROS>
NODE_HTTP_SPN	HTTP/<nombre de host del nodo>@<NOMBRE DE DOMINIO KERBEROS> **Nota:** 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	<nombre de servicio de aplicación>/<nombre de nodo>/<nombre de dominio>@<NOMBRE DE DOMINIO KERBEROS>

Nombre de archivo de tabla de claves

Formato del nombre del archivo de tabla de claves que se va a crear para el SPN asociado. El nombre del archivo de tabla de claves distingue entre mayúsculas y minúsculas.

En la siguiente tabla se describen los formatos de nombre de archivo de tabla de claves:

Tipo de tabla de claves	Nombre de archivo de tabla de claves
NODE_SPN	<nombre de nodo>.keytab
NODE_AC_SPN	_AdminConsole.keytab
NODE_HTTP_SPN	webapp_http.keytab
SERVICE_PROCESS_SPN	<nombre de servicio de aplicación>.keytab

Principales de servicio a nivel de nodo

La siguiente imagen muestra el contenido del archivo SPNKeytabFormat.txt generado para las entidades de seguridad de servicio a nivel del nodo:

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

Principales de servicio a nivel de proceso

La siguiente imagen muestra el contenido del archivo SPNKeytabFormat.txt generado para las entidades de seguridad de servicio a nivel del proceso:

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

Generar los archivos de tabla de claves

Genere los archivos de tabla de claves usados para autenticar los usuarios y servicios de Informatica.

Use la utilidad ktpass de Microsoft Windows Server para generar un archivo de tabla de claves para cada cuenta de usuario que haya creado en Active Directory. Deberá generar los archivos de tabla de claves en un servidor miembro o en un controlador de dominio en el dominio de Active Directory. No puede generar archivos de tabla de claves en un sistema operativo de estación de trabajo como Microsoft Windows 7.

Para usar ktpass para que genere un archivo de tabla de claves, ejecute el siguiente comando:

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

En la siguiente tabla se describen las opciones de comando:

Opción	Descripción
-out	El nombre del archivo de tabla de claves de Kerberos que se debe generar como se muestra en la columna `KEY_TAB_NAME` del archivo SPNKeytabFormat.txt.
-princ	El nombre de entidad de seguridad de servicio mostrado en la columna `SPN` del archivo SPNKeytabFormat.txt. Si el dominio utiliza la autenticación entre dominios Kerberos, el nombre de entidad de seguridad del servicio debe ser único en todos los dominios Kerberos.
-mapuser	Cuenta de usuario de Active Directory que se va a asociar al SPN. El nombre de cuenta puede tener una longitud máxima de 20 caracteres.
-pass	La contraseña establecida en Active Directory para la cuenta de usuario de Active Directory, si corresponde.
-crypto	Especifica los tipos de claves generados en el archivo de tabla de claves. Defínalo como all si desea usar todos los tipos criptográficos admitidos.
-ptype	El tipo de entidad de seguridad. Defínalo como KRB5_NT_PRINCIPAL.
-target	Nombre del dominio al que el servidor de Active Directory pertenece. Incluya esta opción si se produce el siguiente error al ejecutar la utilidad: DsCrackNames devolvió 0x2 en el nombre

Los archivos de tabla de claves que genere dependen de si habilita Kerberos en el nivel de nodo o en el nivel de proceso.

Generar los archivos de tabla de claves a nivel de nodo

Cuando se ejecuta ktpass para generar los archivos de tabla de claves a nivel de nodo, se asocia cada cuenta de usuario de entidad de seguridad de Kerberos con el SPN correspondiente en Active Directory.

La siguiente tabla muestra la asociación entre las cuentas de usuario de la entidad de seguridad de Kerberos y los SPN mostrados en el archivo de ejemplo SPNKeytabFormat.txt:

Cuenta de usuario	Tipo de tabla de claves	Nombre de entidad de seguridad de servicio
nodeuser01	NODE_SPN	isp/node01/InfaDomain/COMPANY.COM
httpuser01	NODE_HTTP_SPN	HTTP/US001DEV.company.com@COMPANY.COM
nodeuser02	NODE_SPN	isp/node02/InfaDomain/COMPANY.COM
httpuser02	NODE_HTTP_SPN	HTTP/US005DEV.company.com@COMPANY.COM

También puede crear una tabla de claves para la cuenta de usuario de enlace de LDAP que se use para acceder a Active Directory y realizar búsquedas durante la sincronización de LDAP.

1. Cree un archivo de tabla de claves para la cuenta de usuario de entidad de seguridad de Kerberos que haya creado para cada nodo de Active Directory.

   Copie el nombre del archivo de tabla de claves de la columna `KEY_TAB_NAME` en el archivo SPNKeytabFormat.txt. Copie el nombre de entidad de seguridad del servicio de la columna `SPN` en el archivo SPNKeytabFormat.txt.

   En el siguiente ejemplo se crea un archivo de tabla de claves para una cuenta de usuario de entidad de seguridad de Kerberos llamada nodeuser0:

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

2. Cree un archivo de tabla de claves para cada cuenta de usuario de entidad de seguridad de Kerberos del proceso HTTP que haya creado en Active Directory.

   Si el dominio utiliza la autenticación entre dominios Kerberos, la cuenta de usuario de entidad de seguridad puede estar en cualquier dominio Kerberos que el dominio utilice.

   Copie el nombre del archivo de tabla de claves de la columna `KEY_TAB_NAME` en el archivo SPNKeytabFormat.txt. Copie el nombre de entidad de seguridad del servicio de la columna `SPN` en el archivo SPNKeytabFormat.txt.

   En el siguiente ejemplo se crea un archivo de tabla de claves para una cuenta de usuario de entidad de seguridad de Kerberos llamada httpuser01:

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

3. Cree una tabla de claves para la cuenta de usuario de enlace de LDAP que se usa para acceder a Active Directory y realizar búsquedas durante la sincronización de LDAP.

   Estructure el valor de la opción -princ como <nombre de entidad de seguridad>@<DOMINIO DE KERBEROS>. Incluya en el nombre del archivo de claves el nombre de la configuración de LDAP del servidor de Active Directory. Estructure el nombre del archivo de claves del siguiente modo: <nombre_configuración de LDAP de Active Directory>.keytab.

   En el siguiente ejemplo se crea un archivo de tabla de claves para una cuenta de usuario de entidad de seguridad del servicio llamada ldapuser:

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

Generar los archivos de tabla de claves a nivel de proceso

Cuando se ejecuta ktpass para generar los archivos de tabla de claves a nivel de proceso, se asocia cada cuenta de usuario de entidad de seguridad de Kerberos con el SPN correspondiente en Active Directory.

La siguiente tabla muestra la asociación entre las cuentas de usuario de la entidad de seguridad de Kerberos y los SPN mostrados en el archivo de ejemplo SPNKeytabFormat.txt:

Cuenta de usuario	Tipo de tabla de claves	Nombre de entidad de seguridad de servicio
nodeuser01	NODE_SPN	isp/node01/InfaDomain/COMPANY.COM
admintooluser01	NODE_AC_SPN	_AdminConsole/node01/InfaDomain@COMPANY.COM
httpuser01	NODE_HTTP_SPN	HTTP/US001DEV.company.com@COMPANY.COM
MRSdevuser01	SERVICE_PROCESS_SPN	MRS_dev/node01/InfaDomain@COMPANY.COM
DISdevuser01	SERVICE_PROCESS_SPN	DIS_dev/node01/InfaDomain@COMPANY.COM
nodeuser02	NODE_SPN	isp/node02/InfaDomain/COMPANY.COM
admintooluser02	NODE_AC_SPN	_AdminConsole/node02/InfaDomain@COMPANY.COM
httpuser02	NODE_HTTP_SPN	HTTP/US005DEV.company.com@COMPANY.COM
CATdevuser01	SERVICE_PROCESS_SPN	CAT_dev/node02/InfaDomain@COMPANY.COM

También puede crear una tabla de claves para la cuenta de usuario de enlace de LDAP que se use para acceder a Active Directory y realizar búsquedas durante la sincronización de LDAP.

1. Cree un archivo de tabla de claves para la cuenta de usuario de entidad de seguridad de Kerberos que haya creado para cada nodo de Active Directory.

   Copie el nombre de archivo de la columna `KEY_TAB_NAME` del archivo SPNKeytabFormat.txt. Copie el nombre de entidad de seguridad del servicio de la columna `SPN` en el archivo SPNKeytabFormat.txt.

   En el siguiente ejemplo se crea un archivo de tabla de claves de una cuenta de usuario de entidad de seguridad de Kerberos llamada nodeuser01:

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

2. Cree un archivo de tabla de claves por cada cuenta de usuario de entidad de seguridad de Kerberos del proceso HTTP que haya creado.

   Si el dominio utiliza la autenticación entre dominios Kerberos, la cuenta de usuario de entidad de seguridad puede estar en cualquier dominio Kerberos que el dominio utilice.

   Copie el nombre de archivo de la columna `KEY_TAB_NAME` en el archivo SPNKeytabFormat.txt. Copie el nombre de entidad de seguridad del servicio de la columna `SPN` en el archivo SPNKeytabFormat.txt.

   En el siguiente ejemplo se crea un archivo de tabla de claves para una cuenta de usuario de entidad de seguridad de Kerberos llamada httpuser01:

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

3. Cree un archivo de tabla de claves para cada cuenta de usuario de entidad de seguridad de Kerberos de la Herramienta del administrador que haya creado.

   Copie el nombre de archivo de la columna `KEY_TAB_NAME` en el archivo SPNKeytabFormat.txt. Copie el nombre de entidad de seguridad del servicio de la columna `SPN` en el archivo SPNKeytabFormat.txt.

   En el siguiente ejemplo se crea un archivo de tabla de claves para una cuenta de usuario de entidad de seguridad de Kerberos llamada admintooluser01:

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

4. Cree un archivo de tabla de claves para cada cuenta de usuario de entidad de seguridad de Kerberos del servicio de aplicación de Informatica que haya creado.

   Copie el nombre de archivo de la columna `KEY_TAB_NAME` en el archivo SPNKeytabFormat.txt. Copie el nombre de entidad de seguridad del servicio de la columna `SPN` en el archivo SPNKeytabFormat.txt.

   En el siguiente ejemplo se crea un archivo de tabla de claves para una cuenta de usuario de entidad de seguridad de Kerberos del servicio llamada MRSdevuser01:

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

5. Cree una tabla de claves para la cuenta de usuario de enlace de LDAP que se usa para acceder a Active Directory y realizar búsquedas durante la sincronización de LDAP.

   Estructure el valor de la opción -princ como <nombre de entidad de seguridad>@<DOMINIO DE KERBEROS>. Incluya en el nombre del archivo de claves el nombre de la configuración de LDAP del servidor de Active Directory. Estructure el nombre del archivo de claves del siguiente modo: <nombre_configuración de LDAP de Active Directory>.keytab.

   En el siguiente ejemplo se crea un archivo de tabla de claves para una cuenta de usuario de entidad de seguridad del servicio llamada ldapuser:

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

Comprobar los nombres de entidad de seguridad de servicio y los archivos de tabla de claves

Puede usar las utilidades de Kerberos para comprobar que los SPN y los archivos de tabla de claves sean válidos. También puede usar las utilidades para determinar el estado del centro de distribución de claves (KDC) de Kerberos.

Puede usar las utilidades de Kerberos como *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. 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:

kinit

Puede usar la utilidad *kinit* para solicitar un vale de concesión de vales (TGT) del KDC y comprobar que un archivo de tabla de claves se puede usar para establecer una conexión de Kerberos. Si la tabla de claves y el SPN especificado son válidos, el comando obtiene un vale y después almacena dicho vale en la memoria caché especificada.

La utilidad kinit se encuentra en el siguiente directorio de un nodo de Informatica:

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

Para solicitar un ticket que otorga tickets para un SPN, ejecute el siguiente comando:

```
kinit -c <nombre de memoria caché> -k -t <nombre de archivo de tabla de claves>
<nombre de entidad de seguridad de servicio>
```

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:

```
Memoria caché: \temp\krb Con entidad de seguridad: isp/node01/InfaDomain/COMPANY.COM
Con tabla de claves: node01.keytab Autenticado con Kerberos v5
```

klist

Puede usar la utilidad *klist* para enumerar las entidad de seguridad 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 <nombre de archivo de tabla de claves>
```

El siguiente ejemplo de una salida muestra las entidades de seguridad en un archivo de tabla de claves:

```
Nombre de tabla de claves: FILE:node01.keytab KVNO Timestamp Principal ----
---------------- ------------------------------------------------------- 3
12/31/16 19:00:00 MRS_dev/node01/InfaDomain@COMPANY.COM 3 12/31/16 19:00:00 MRS_dev/
node01/InfaDomain@COMPANY.COM 3 12/31/16 19:00:00 MRS_dev/node01/
InfaDomain@COMPANY.COM 3 12/31/16 19:00:00 MRS_dev/node01/InfaDomain@COMPANY.COM
```

Habilitar la autenticación Kerberos

Puede habilitar la autenticación Kerberos en un dominio de Informatica cuando instale los servicios de Informatica. También puede habilitar la autenticación Kerberos después de instalar los servicios.

Para obtener información sobre cómo habilitar la autenticación Kerberos al instalar Servicios de Informatica, consulte la *Guía de instalación y configuración de Informatica 10.2 HotFix 2*.

Si no habilita la autenticación Kerberos durante la instalación, siga los pasos de esta sección para usar los programas de la línea de comandos de Informatica para habilitar la autenticación Kerberos después de instalar los servicios.

Habilitar la autenticación Kerberos en el dominio

Habilite Kerberos en un nodo de puerta de enlace del dominio.

Ejecute el comando infasetup switchToKerberosMode en un nodo de puerta de enlace del dominio para cambiar la autenticación a la autenticación de red de Kerberos.

1. Cierre el dominio y todos los servicios de Informatica. Cierre los servicios de en el siguiente orden:
   - Servicio de Metadata Manager
   - Servicio de integración de PowerCenter®
   - Servicio de repositorio de PowerCenter®
   - Servicio de administración del contenido
   - Servicio del analista
   - servicio de integración de datos
   - Servicio de repositorio de modelos
2. En la línea de comandos en un nodo de puerta de enlace, cambie al directorio en el que se encuentra el ejecutable de infasetup.

   ```
   <directorio de instalación de Informatica>\isp\bin
   ```
3. Ejecute el siguiente comando:

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

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

Opción	Argumento	Descripción
-administratorName -ad	user_name	El nombre de usuario de la cuenta de administrador del dominio que se crea al configurar la autenticación Kerberos. Especifique el nombre de una cuenta que exista en Active Directory. Después de configurar la autenticación Kerberos, este usuario se incluye en el dominio de seguridad *_infaInternalNamespace* que el comando crea. Si el dominio usa un solo dominio Kerberos para autenticar usuarios, especifique el nombre samAccount de la cuenta que quiera usar como cuenta del administrador. Si el dominio usa la autenticación entre dominios Kerberos, especifique el nombre de entidad de seguridad de usuario completo de la cuenta que quiera usar como cuenta del administrador, incluido el nombre de dominio. Por ejemplo: sysadmin@COMPANY.COM
-ServiceRealmName -srn	Kerberos_realm_name	Nombre del dominio Kerberos que el dominio usa para autenticar usuarios. El nombre del dominio debe escribirse en mayúsculas y distingue mayúsculas de minúsculas. Para configurar la autenticación entre dominios Kerberos, especifique el nombre de todos los dominios Kerberos que el dominio utiliza para autenticar usuarios, separados por coma. Por ejemplo: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Coloque un asterisco como carácter comodín antes del nombre del dominio para englobar todos los dominios que incluyan ese nombre. Por ejemplo: *EAST.COMPANY.COM

Opción	Argumento	Descripción
-UserRealmName -urn	Kerberos_realm_name	Nombre del dominio Kerberos que el dominio usa para autenticar usuarios. El nombre del dominio debe escribirse en mayúsculas y distingue mayúsculas de minúsculas. Para configurar la autenticación entre dominios Kerberos, especifique el nombre de todos los dominios Kerberos que el dominio utiliza para autenticar usuarios, separados por coma. Por ejemplo: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Coloque un asterisco como carácter comodín antes del nombre del dominio para englobar todos los dominios que incluyan ese nombre. Por ejemplo: *EAST.COMPANY.COM
-SPNShareLevel -spnSL	NODE|PROCESS	El nivel principal de servicio del dominio. Establézcalo en NODE para habilitar Kerberos a nivel de nodo. Establézcalo en PROCESS para habilitar Kerberos a nivel de proceso.

En el siguiente ejemplo se cambia la autenticación de dominios a Kerberos, y la cuenta de usuarios sysadmin se establece como la cuenta de administrador en un dominio que usa un solo dominio Kerberos para autenticar usuarios:

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

En el siguiente ejemplo se cambia la autenticación de dominios a Kerberos, y la cuenta de usuarios sysadmin se establece como la cuenta de administrador en un dominio que usa la autenticación entre dominios Kerberos:

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

Actualizar los nodos del dominio

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

Use los siguientes comandos para actualizar la puerta de enlace y los nodos de trabajo:

infasetup UpdateGatewayNode

Utilice el comando UpdateGatewayNode para establecer los parámetros de la 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 la 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 la línea de comandos de un nodo, cambie al directorio en el que se encuentra el ejecutable de infasetup.

   ```
   <directorio de instalación de Informatica>\isp\bin
   ```

2. Para definir los parámetros de autenticación Kerberos en un nodo de puerta de enlace, ejecute el siguiente comando:

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

   Para definir los parámetros de autenticación Kerberos en un nodo de trabajo, ejecute el siguiente comando:

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

   La siguiente tabla describe las opciones y los argumentos requeridos para habilita la autenticación Kerberos en un nodo:

Opción	Argumento	Descripción
-EnableKerberos -krb	true|false	Configura el dominio de Informatica para utilizar la autenticación Kerberos. Se establece en true para habilitar la autenticación Kerberos. El valor predeterminado es false.
-ServiceRealmName -srn	Kerberos_realm_name	Nombre del dominio Kerberos que el dominio usa para autenticar usuarios. El nombre del dominio debe escribirse en mayúsculas y distingue mayúsculas de minúsculas. Para configurar la autenticación entre dominios Kerberos, especifique el nombre de todos los dominios Kerberos que el dominio utiliza para autenticar usuarios, separados por coma. Por ejemplo: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Coloque un asterisco como carácter comodín antes del nombre del dominio para englobar todos los dominios que incluyan ese nombre. Por ejemplo: *EAST.COMPANY.COM
-UserRealmName -urn	Kerberos_realm_name	Nombre del dominio Kerberos que el dominio usa para autenticar usuarios. El nombre del dominio debe escribirse en mayúsculas y distingue mayúsculas de minúsculas. Para configurar la autenticación entre dominios Kerberos, especifique el nombre de todos los dominios Kerberos que el dominio utiliza para autenticar usuarios, separados por coma. Por ejemplo: COMPANY.COM,EAST.COMPANY.COM,WEST.COMPANY.COM Coloque un asterisco como carácter comodín antes del nombre del dominio para englobar todos los dominios que incluyan ese nombre. Por ejemplo: *EAST.COMPANY.COM

En el siguiente ejemplo se actualiza un nodo de trabajo para usar la autenticación Kerberos:

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

En el siguiente ejemplo se actualiza un nodo de trabajo para usar la autenticación entre dominios Kerberos:

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

Habilitar Kerberos en nodos de Informatica

Después de habilitar Kerberos en el dominio, deberá copiar el archivo de configuración de Kerberos en cada nodo del dominio. También deberá configurar los exploradores web para que accedan a las aplicaciones web de Informatica.

Copie los archivos de tabla de claves en el siguiente directorio de cada nodo:

```
<directorio de instalación de Informatica>\isp\config\keys
```

Los archivos de tabla de claves que copie dependen de si habilita la autenticación Kerberos al nivel de nodo o al nivel de proceso.

Archivos de tabla de claves a nivel de nodo

Copie cada archivo de tabla de claves generado a nivel de nodo en el nodo correspondiente.

La siguiente tabla muestra el nodo en el que copiar cada archivo de tabla de claves:

Archivo de tabla de claves	Ubicación en el nodo
<nombre de nodo>.keytab	Copie cada archivo en el nodo correspondiente.
webapp_http.keytab	Copie cada archivo en el nodo de puerta de enlace correspondiente.
ldapuser.keytab	Copie el archivo en cada nodo de puerta de enlace.

Archivos de tabla de claves a nivel de proceso

Copie cada archivo de tabla de claves generado a nivel de proceso en el nodo correspondiente.

La siguiente tabla muestra el nodo en el que copiar cada archivo de tabla de claves:

Archivo de tabla de claves	Ubicación en el nodo
<nombre de nodo>.keytab	Copie cada archivo en el nodo correspondiente.
webapp_http.keytab	Copie cada archivo en el nodo de puerta de enlace correspondiente.
_AdminConsole.keytab	Copie cada archivo en el nodo de puerta de enlace correspondiente.

Archivo de tabla de claves	Ubicación en el nodo
<nombre de servicio de aplicación>.keytab	Copie cada archivo en el nodo correspondiente en el que se ejecuta la aplicación de Informatica.
ldapuser.keytab	Copie el archivo en cada nodo de puerta de enlace.

Configure los exploradores web para acceder a las aplicaciones web de Informatica.

En Microsoft Internet Explorer y en Google Chrome, añada la URL de las aplicaciones web de Informatica, como la Herramienta del analista, a la lista de sitios de confianza.

Si utiliza Chrome 41 o posterior, también debe definir las directivas AuthServerWhitelist y AuthNegotiateDelegateWhitelist.

Copiar los archivos de tabla de claves en los nodos de Informatica

Después de crear los archivos de tabla de claves, copie cada archivo de tabla de claves en el nodo correspondiente.

Copie los archivos de tabla de claves en el siguiente directorio de cada nodo:

```
<directorio de instalación de Informatica>\isp\config\keys
```

Los archivos de tabla de claves que copie dependen de si habilita la autenticación Kerberos al nivel de nodo o al nivel de proceso.

Archivos de tabla de claves a nivel de nodo

Copie cada archivo de tabla de claves generado a nivel de nodo en el nodo correspondiente.

La siguiente tabla muestra el nodo en el que copiar cada archivo de tabla de claves:

Archivo de tabla de claves	Ubicación en el nodo
<nombre de nodo>.keytab	Copie cada archivo en el nodo correspondiente.
webapp_http.keytab	Copie cada archivo en el nodo correspondiente.
ldapuser.keytab	Copie el archivo en cada nodo de puerta de enlace.

Archivos de tabla de claves a nivel de proceso

Copie cada archivo de tabla de claves generado a nivel de proceso en el nodo correspondiente.

La siguiente tabla muestra el nodo en el que copiar cada archivo de tabla de claves:

Archivo de tabla de claves	Ubicación en el nodo
<nombre de nodo>.keytab	Copie cada archivo en el nodo correspondiente.
webapp_http.keytab	Copie cada archivo en el nodo correspondiente.
_AdminConsole.keytab	Copie cada archivo en el nodo correspondiente.

Archivo de tabla de claves	Ubicación en el nodo
<nombre de servicio de aplicación>.keytab	Copie cada archivo en el nodo correspondiente en el que se ejecuta la aplicación de Informatica.
ldapuser.keytab	Copie el archivo en cada nodo.

Habilitar la autenticación Kerberos para los clientes de Informatica

Copie el archivo de configuración de Kerberos en cada equipo que aloje un cliente de Informatica y después establezca una variable de entorno que apunte al archivo de configuración. También deberá configurar el los exploradores del cliente para que accedan 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 en cada host cliente de Informatica.

Copie el archivo `krb5.conf` en cada equipo que aloje un cliente de Informatica, como PowerCenter Client o Informatica Developer (Developer tool). Copie el archivo en el siguiente directorio de cada host:

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

Establezca la variable de entorno KRB5_CONFIG en cada host cliente de Informatica.

Establezca la variable de entorno KRB5_CONFIG en la ruta de acceso y el nombre del archivo de configuración de Kerberos de cada equipo que aloja clientes de Informatica como PowerCenter Client y Developer tool.

Configure los exploradores web para acceder a las aplicaciones web de Informatica.

En Microsoft Internet Explorer y en Google Chrome, añada la URL de las aplicaciones web de Informatica, como la Herramienta del analista, a la lista de sitios de confianza.

Si utiliza Chrome 41 o posterior, también debe definir las directivas `AuthServerWhitelist` y `AuthNegotiateDelegateWhitelist`.

Habilitación de Kerberos para la integración de Hadoop

Para ejecutar asignaciones en un clúster habilitado para Kerberos y ver metadatos desde Developer tool, realice tareas de configuración en la Herramienta del administrador y en cada equipo de Developer tool.

Realice las tareas siguientes:

- Configurar el archivo de configuración de Kerberos
- Crear artefactos de autenticación de usuario
- Configurar las propiedades para la autenticación Kerberos del dominio de Informatica
- Importar archivos de configuración a cada máquina de Developer tool
- Generar un archivo de credenciales de Kerberos para la máquina de Developer tool

Si desea ver cómo realizar estas tareas, lea el capítulo sobre cómo ejecutar asignaciones con autenticación Kerberos en la *Guía de Data Engineering Administrator*.

Habilitar cuentas de usuario para usar la autenticación Kerberos

Después de habilitar la autenticación Kerberos en el dominio, importe las cuentas de usuario de Informatica desde Active Directory en el dominio de seguridad de LDAP que contenga las cuentas de usuario de Kerberos. También deberá migrar los grupos, las funciones, los privilegios y los permisos de dominio de seguridad nativo a las cuentas de usuario correspondientes de Active Directory en el dominios de seguridad de LDAP que contenga las cuentas de usuario de Kerberos.

Importar cuentas de usuario desde Active Directory a dominios de seguridad de LDAP

Importe cuentas de usuario desde Active Directory a dominios de seguridad de LDAP.

Cuando se habilita la autenticación Kerberos en el dominio, Informatica crea un dominio de seguridad de LDAP vacío con el mismo nombre que el dominio Kerberos. Puede importar cuentas de usuario de Active Directory en este dominio de seguridad de LDAP o puede importar las cuentas de usuario en un dominio de seguridad de LDAP diferente.

Utilice la Herramienta del administrador para importar las cuentas de usuario que usan la autenticación Kerberos de Active Directory en un dominio de seguridad de LDAP.

Para configurar la autenticación entre dominios Kerberos, conéctese al catálogo global de Active Directory. Cuando se establece una conexión con el catálogo global, se importan los usuarios desde el servidor de Active Directory que cada dominio Kerberos usa.

1. Inicie el dominio y todos los servicios de Informatica.
2. Inicie sesión en Windows con la cuenta de administrador que especificó cuando habilitó la autenticación Kerberos en el dominio.
3. Inicie sesión en la herramienta Administrator. Seleccione _infaInternalNamespace como el dominio de seguridad.
4. En la Herramienta del administrador, haga clic en la ficha **Seguridad**.
5. Haga clic en el menú **Acciones** y seleccione **Configuración de LDAP**.
6. En el cuadro de diálogo **Configuración de LDAP**, haga clic en la ficha **Conectividad de LDAP**.
7. Configure las propiedades de conexión de Active Directory.

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

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

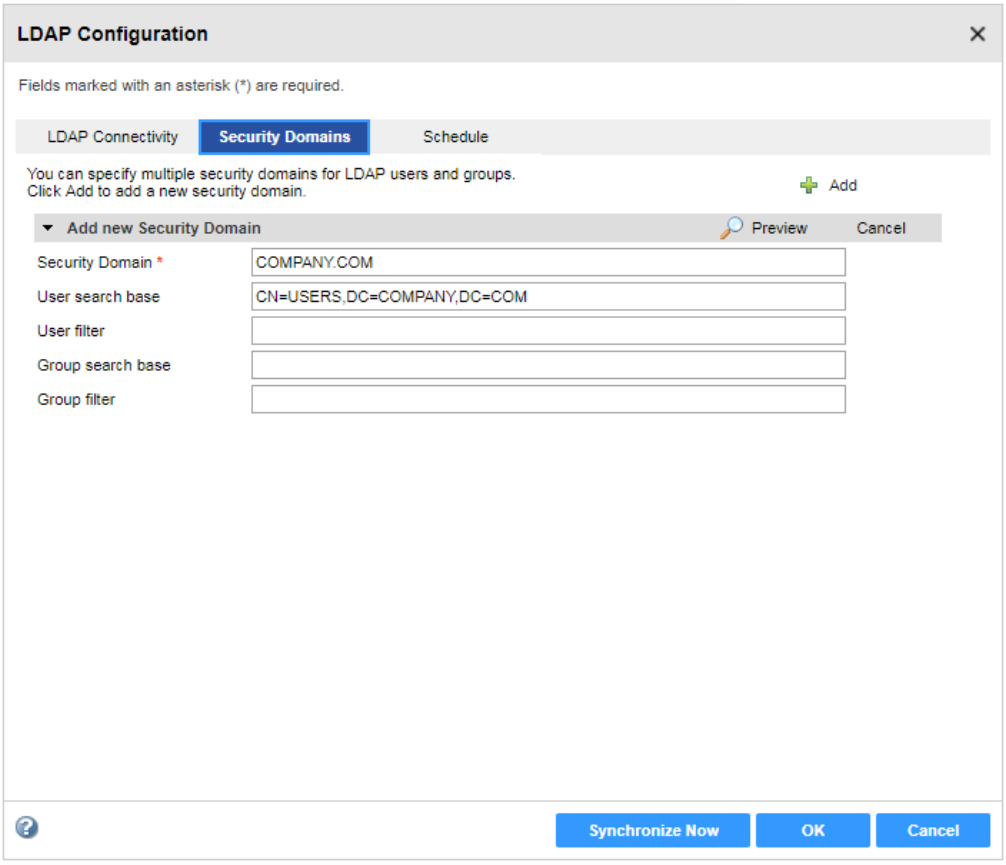
Propiedad	Descripción
Nombre del servidor	Nombre o dirección IP del host del servidor de Active Directory. Para configurar la autenticación entre dominios Kerberos, conéctese al host de catálogo global de Active Directory. Indique el nombre de host completo. Por ejemplo: host.company.local
puerto	El puerto de escucha del servidor de Active Directory. El valor predeterminado es 389. El puerto SSL predeterminado es 636. Para configurar la autenticación entre dominios Kerberos, conéctese al puerto del catálogo global de Active Directory. El valor predeterminado es 3268. El puerto SSL predeterminado es 3269.
Servicio de directorio de LDAP	Seleccione **Servicio Microsoft Active Directory**.
Nombre	Especifique la cuenta de usuario de enlace que creó en Active Directory para sincronizar cuentas en Active Directory con el dominio de seguridad de LDAP. Como el dominio está habilitado para la autenticación Kerberos, no tiene la opción para proporcionar una contraseña para la cuenta. Si el dominio usa la autenticación entre dominios Kerberos, incluya el nombre del dominio al que la base de datos de entidades de seguridad de Active Directory pertenece.
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.
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.
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, *member* o *memberof*.
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.

8. En el cuadro de diálogo **Configuración de LDAP**, haga clic en la ficha **Dominios de seguridad**.
9. Haga clic en **Añadir**.

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 en el que desea importar cuentas de usuario de Active Directory.
Base de búsqueda de usuarios	El nombre distinguido (DN) de la entrada que sirve de punto de inicio para buscar nombres de usuarios en Active Directory. La búsqueda encuentra un objeto en el directorio en función de la ruta de acceso en el nombre distintivo del objeto. Por ejemplo, para buscar el contenedor USERS que contiene las cuentas de usuario de Informatica en el dominio de Windows example.com, especifique CN=USERS,DC=EXAMPLE,DC=COM.
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.
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.

La siguiente imagen muestra la información requerida para importar usuarios de LDAP de Active Directory en el dominios de seguridad de LDAP que se creó al habilitar Kerberos en el dominio:



10. 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.

11. Haga clic en **Aceptar** para guardar el dominio de seguridad de LDAP.

Migrar privilegios y permisos de usuarios nativos a un dominio de seguridad de Kerberos

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

1. Revise la lista de cuentas de usuario nativas y determine las cuentas que desea migrar al dominio de seguridad de LDAP para autenticación Kerberos.

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

   ```
   infacmd isp ListAllUsers
   ```

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

2. Cree el archivo de migración de usuarios.

   El archivo de migración de usuarios es un archivo de texto sin formato que contiene la lista de usuarios nativos y de usuarios de Kerberos correspondientes que deben tener los mismos grupos, funciones, privilegios y permisos.

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

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

   En el siguiente ejemplo se muestra un archivo de migración de usuarios que contiene la lista de los usuarios que se van a migrar al dominio de seguridad COMPANY.COM:

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

3. Ejecute el comando infacmd isp migrateUsers para migrar privilegios y permisos de la cuenta del dominio de seguridad nativo a las cuentas del dominio de seguridad de Kerberos.

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

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

   La siguiente tabla describe las opciones del comando

Opción	Descripción
-DomainName -dn	Nombre de dominio de Informatica.
-UserName -un	Nombre de usuario que se va a conectar al dominio. Especifique el nombre de usuario de la cuenta de administrador que ha especificado en el comando infasetup switchToKerberosMode.
-Password -pd	Contraseña de la cuenta de administrador.
-SecurityDomain -sdn	Dominio de seguridad de LDAP de la cuenta de administrador usada para conectar con el dominio. Especifique _infaInternalNamespace.
-UserMigrationFile -umf	Ruta de acceso y nombre del archivo de migración de usuarios. El comando omite las entradas con nombres de usuario de origen o de destino duplicados.

   En el siguiente ejemplo se migran los grupos, las funciones, los privilegios y los permisos de los usuarios según el archivo de migración de usuarios `um_s.txt`:

   ```
   infacmd isp migrateUsers -dn InfaDomain -un nodeuser01 -pd password -sdn
   _infaInternalNamespace -umf C:\Infa\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 denominado `infacmd_umt_<fecha>_<hora>.txt` en el directorio donde se ejecuta el comando.

Delegación Kerberos

La delegación de Kerberos permite que un servicio de Kerberos se haga pasar por un usuario del cliente Kerberos y obtenga un vale de servicio para otro servicio en nombre del usuario del cliente.

Los servicios de un dominio de Informatica deben conectarse a otros servicios para completar una operación. Puede conectarse a otros servicios mediante autenticación delegada. En la autenticación delegada, cuando un servicio autentica un usuario, usa esas credenciales para conectarse a otro servicio. Por ejemplo, cuando un usuario de pmcmd accede al servicio de integración de Power Center, el servicio actúa como el usuario de pmcmd para autenticarse con el servicio de repositorio de Power Center.

Tipos de delegación de Kerberos

Cuando usa la autenticación delegada, puede elegir uno de los siguientes tipos de delegación:

Delegación completa

La delegación completa es la implementación inicial de la delegación de Kerberos. En este método de delegación, un cliente reenvía su Ticket Granting Ticket (TGT) a un servicio después de la autenticación Kerberos. El servicio utiliza el TGT para obtener tickets de servicio para acceder a cualquier otro servicio de la red. Este tipo de delegación no se considera segura porque un administrador no puede controlar los servicios a los que el servidor puede acceder utilizando la identidad del cliente. La delegación completa también se conoce como "delegación sin restricciones".

Delegación restringida basada en recursos

Con la delegación restringida basada en recursos, los administradores pueden restringir el uso de la identidad del cliente por parte de los servicios. En este método de delegación, el cliente no reenvía TGT al servidor. En este método, los servicios especifican en quién confían y quién puede delegarles la autenticación.

La delegación restringida utiliza extensiones de protocolo Kerberos llamadas Servicio para usuarios (S4U) que permiten que un servicio obtenga un vale de servicio Kerberos en nombre de un usuario.

Nota: No puede utilizar la delegación restringida y la delegación completa en un solo dominio. Puede configurar el dominio para utilizar la delegación completa o la delegación restringida.

Extensión de Servicio para usuarios (S4U)

Las extensiones de Servicio para usuarios (S4U) permiten que un servicio obtenga un vale de servicio Kerberos en nombre de un usuario. A continuación se muestran los dos tipos de extensiones S4U:

- Servicio para usuarios para sí mismo (S4U2Self). Esta extensión permite que un servicio obtenga un ticket de servicio para sí mismo en nombre de un usuario cliente.
- Servicio para usuarios para proxy (S4U2Self). Esta extensión permite que un servicio obtenga un ticket de servicio para otro servicio en nombre de un usuario cliente. Para realizar S4U2proxy, un servicio necesita un ticket de servicio para sí mismo. El usuario cliente puede presentar el ticket de servicio o puede obtenerse a través de la extensión S4U2Self.

Para obtener más información sobre las extensiones S4U, consulte la documentación de Microsoft.

Habilite la delegación restringida basada en recursos con S4U2Self

Asegúrese de que el indicador de reenvío esté establecido en verdadero en la sección libdefaults del archivo krb5.conf.

Puede configurar la delegación restringida basada en recursos solo a través de comandos de PowerShell. Asegúrese de que a PowerShell lo inicie un usuario con los privilegios necesarios para cambiar las propiedades de las cuentas de KDC, preferiblemente un administrador de KDC.

Para habilitar la delegación restringida basada en recursos con S4U2Self, realice los siguientes pasos en cada cuenta de keytab de Informatica en el servidor KDC:

1. Haga clic con el botón derecho en la cuenta de usuario y seleccione **Propiedades** .

   A continuación, aparece el cuadro de diálogo **Propiedades**.
2. Sobre la pestaña **Delegación**, seleccione **No confiar en esta computadora para la delegación**.
3. Haga clic en **Aplicar**.
4. Ejecute el siguiente comando para configurar el atributo `PrincipalsAllowedToDelegateToAccount`:

   ```
   $IntermediateService = Get-ADUser -Identity <samAccountName de cuenta de servidor intermedio> -Properties *
   ```

   ```
   Set-ADUser -Identity <samAccountName de cuenta de servidor de destino> -PrincipalsAllowedToDelegateToAccount $IntermediateService1, $IntermediateService2, $IntermediateService3
   ```

   Nota: Puede utilizar valores separados por comas para agregar varias cuentas en el atributo `PrincipalsAllowedToDelegateToAccount`.
5. Si desea desarmar el atributo `PrincipalsAllowedToDelegateToAccount`, ejecute el siguiente comando:

   ```
   Set-ADUser -Identity <samAccountName de cuenta de servidor de destino> PrincipalsAllowedToDelegateToAccount $null
   ```
6. Para ver las entidad de seguridad existentes en la lista `PrincipalsAllowedToDelegateToAccount`, ejecute los siguientes comandos:

   ```
   $FormatEnumerationLimit=-1
   Get-ADUser -Identidad <nombre de cuenta sam> -properties
   ```

   ```
   PrincipalsAllowedToDelegateToAccount
   ```

   Nota: De forma predeterminada, la salida del comando de powershell muestra cuatro valores en la lista principal de servicio en la salida. Establezca este parámetro en -1 para mostrar la lista completa de entidades de seguridad.

Habilitar la delegación para las cuentas de entidad de seguridad Kerberos en Active Directory

Cree los archivos de tabla de claves utilizando el comando `ktpass`.

Para usar la delegación completa, deberá habilitar la delegación para todas las cuentas que haya creado, excepto para la cuenta de usuario de enlace de LDAP que use para acceder a Active Directory durante la sincronización de LDAP.

Para habilitar la delegación completa, realice los siguientes pasos para cada cuenta de usuario:

1. Haga clic con el botón derecho en la cuenta de usuario y seleccione **Propiedades** .

   A continuación, aparece el cuadro de diálogo **Propiedades**.
2. Sobre la pestaña **Delegación**, seleccione **Confiar en este usuario para la delegación a cualquier servicio (solo Kerberos)**.
3. Haga clic en **Aplicar**.

   La delegación completa está habilitada.

Cambiar de delegación completa a delegación restringida

Si está utilizando la delegación completa y desea utilizar la delegación restringida, realice los siguientes pasos.

1. Cerrar el dominio.
2. "Habilite la delegación restringida basada en recursos con S4U2Self" en la página 65 para los usuarios existentes de Active Directory asociados con la cuenta keytab en el servidor KDC.
3. Iniciar el dominio.

CAPÍTULO 5

Autenticación SAML para aplicaciones web de Informatica

Este capítulo incluye los siguientes temas:

Resumen de la autenticación SAML

Puede configurar la autenticación del lenguaje de marcado de aserción de seguridad (SAML) para las aplicaciones web de Informatica.

El lenguaje de marcado de aserción de seguridad es un formato de datos basado en XML para intercambiar información de autenticación entre un proveedor de servicios y un proveedor de identidades. En un dominio de Informatica, la aplicación web de Informatica es el proveedor de servicios.

Las siguientes aplicaciones web de Informatica se pueden configurar para que usen la autenticación SAML:

- Informatica Administrator
- Informatica Analyst
- Herramienta de ingesta masiva
- Metadata Manager
- Enterprise Data Catalog
- Enterprise Data Preparation
- Data Privacy Management

Nota: La autenticación SAML no se puede utilizar en un dominio de Informatica configurado para utilizar la autenticación Kerberos.

Si un dominio se habilita para que use la autenticación SAML, todas las aplicaciones web que se ejecutan en dicho dominio usarán el proveedor de identidades que se haya configurado en el dominio de forma predeterminada. Sin embargo, las aplicaciones web que se ejecutan en un mismo dominio se pueden configurar para que usen proveedores de identidades distintos. Así, por ejemplo, podríamos configurar

Informatica Administrator para que use AD FS como proveedor de identidades e Informatica Analyst, para que use PingFederate.

Para obtener más información sobre cómo configurar aplicaciones web para que usen proveedores de identidades distintos, consulte "Configurar aplicaciones web para que usen proveedores de identidades distintos" en la página 77.

Directorio predeterminado del almacén de claves y truststore

La implementación de Informatica incluye archivos de almacén de claves y de truststore predeterminados en el directorio `<directorio de instalación de Informatica>\services\shared\security`.

Informatica le recomienda que utilice el almacén de claves y truststore predeterminados solo para casos de uso de configuración y prueba de conceptos. Para proteger un entorno de producción, use las siguientes directrices:

- Configure un almacén de claves y truststore personalizados para la autenticación SAML en una ubicación que no sea el directorio predeterminado:
  `<directorio de instalación de Informatica>\services\shared\security`
- No puede utilizar el almacén de claves y el truststore predeterminados para configurar otros servicios o clientes.
- Cuando habilita la autenticación SAML, importa los archivos de certificado y las claves privadas del almacén de claves o del truststore en el directorio predeterminado:
  `<directorio de instalación de Informatica>\services\shared\security`
- Cuando asigne un alias al almacén de claves o al truststore, no utilice "Informatica LLC", que Informatica usa para la autenticación de claves privadas y la firma de certificados.
- Solo se permite modificar el almacén de claves o truststore SAML predeterminado cuando el directorio predeterminado está configurado como el directorio del almacén de claves o truststore SAML y desea importar claves privadas y entradas de certificado en el almacén de claves o truststore predeterminado.

  No puede utilizar "Informatica LLC" como alias para las nuevas entradas en el almacén de claves o truststore predeterminado. Puede utilizar "Informatica LLC" como alias para las entradas de almacén de claves-truststore personalizadas.

  No se permite ninguna otra operación para los archivos del almacén de claves o truststore predeterminado, incluida la eliminación o sustitución de los archivos, el cambio de la contraseña del almacén de claves o truststore, o la modificación, eliminación o sustitución de la clave privada generada por Informatica y el certificado de firma.

Proveedores de identidades admitidos

Utilice un proveedor de identidades admitido para administrar la autenticación SAML en el dominio para las aplicaciones web.

Informatica admite los siguientes proveedores de identidades. Haga clic en el vínculo del artículo de la biblioteca de procedimientos (H2L) para obtener instrucciones sobre la integración entre cada proveedor de identidades y el dominio.

Proveedor de identidades	Artículo de la biblioteca de procedimientos (H2L)
Microsoft Active Directory Federation Services (AD FS)	SAML Authentication with Active Directory Federation Services in Informatica 10.4.0
PingFederate	SAML Authentication with PingFederate in Informatica 10.4.0
F5 Big-IP	SAML Authentication with F5 Networks BIG-IP in Informatica 10.4.1
NetScaler	SAML Authentication with NetScaler for Web Applications
Oracle Access Manager (OAM)	SAML Authentication with Oracle Access Manager for Web Applications
Okta SSO	SAML Authentication with Okta SSO for Web Applications
Azure Active Directory	SAML Authentication with Azure Active Directory for Web Applications

Para obtener información sobre las versiones compatibles de estos proveedores de identidades, consulte la tabla de disponibilidad de productos en Informatica Network: https://network.informatica.com/community/informatica-network/product-availability-matrices.

Proceso de la autenticación SAML

Las aplicaciones web de Informatica y el proveedor de identidades intercambian información de autenticación para hacer posible la autenticación SAML en un dominio de Informatica.

En los siguientes pasos se describe el flujo de autenticación SAML básico:

1. Un usuario accede a una aplicación web de Informatica.
2. En la página de inicio de sesión de la aplicación, el usuario selecciona el dominio de seguridad que contiene las cuentas de usuario de LDAP utilizadas en la autenticación SAML y, luego, hace clic en el botón para iniciar sesión.

   Si el usuario selecciona un dominio de seguridad nativo, debe especificar un nombre de usuario y una contraseña, e iniciar sesión en la aplicación.
3. Según cuál sea la configuración del proveedor de identidades, puede que se pida al usuario las credenciales necesarias para autenticarse por primera vez.
4. El proveedor de identidades valida esas credenciales y crea una sesión para el usuario.

   El proveedor de identidades valida también la URL de la aplicación web de destino y, luego, redirige al usuario a la aplicación web con un token de SAML que contiene la información de identidad del usuario.
5. La aplicación valida el token de SAML y la información de identidad del usuario, crea una sesión de usuario y finaliza el proceso de inicio de sesión del usuario.

La sesión de usuario existente en el navegador se usará en autenticaciones posteriores. Para acceder a otra aplicación web de Informatica configurada para usar autenticación SAML, el usuario deberá seleccionar el dominio de seguridad de LDAP en la página de inicio de sesión de la aplicación en cuestión. El usuario no necesita proporcionar un nombre de usuario o contraseña.

El usuario permanece conectado a todas las aplicaciones web de Informatica que se están ejecutando en la misma sesión de navegador. Sin embargo, si el usuario cierra la sesión en una aplicación web de Informatica, también la cierra para el resto de aplicaciones web de Informatica que se ejecutan en la misma sesión de navegador.

Habilitar la autenticación SAML en un dominio

Configure el proveedor de identidades, el dominio de Informatica y los nodos en el dominio para que usen la autenticación SAML.

Realice las siguientes tareas para configurar la autenticación SAML en las aplicaciones web de Informatica que se ejecutan en un dominio:

1. Cree una configuración de LDAP para conectarse con el almacén de identidades de LDAP que contiene las cuentas de usuario de aplicaciones web de Informatica. También hay que crear un dominio de seguridad de LDAP e importar en él las cuentas de usuario.
2. Exporte el certificado de firma de aserciones del proveedor de identidades.
3. Importe el certificado de firma de aserciones en un archivo de TrustStore en cada nodo de puerta de enlace del dominio. El certificado se puede importar en el archivo de TrustStore predeterminado de Informatica o en un archivo de TrustStore personalizado.
4. Añada una o varias relaciones de confianza o proveedores de servicios al proveedor de identidades.
5. Añada la URL de cada aplicación web de Informatica al proveedor de identidades.
6. Habilite la autenticación SAML en el dominio.
7. Habilite la autenticación SAML en cada nodo del dominio.

Nota: Para varios de los proveedores de identidades SAML que admite Informatica, puede seguir los pasos de integración detallados en un artículo de la biblioteca de procedimientos (H2L). Consulte "Proveedores de identidades admitidos" en la página 70 para obtener vínculos a los artículos.

Crear una configuración de LDAP del proveedor de identidades o del almacén de LDAP

Utilice la Herramienta del administrador para crear una configuración del proveedor de identidades o del almacén de LDAP que contiene las cuentas de usuario de aplicaciones web que usan autenticación SAML.

Cuando se crea una configuración de LDAP, hay que crear un dominio de seguridad de las cuentas de usuario e importar a este esas cuentas. Después de importar las cuentas al dominio de seguridad, asigne las funciones, los privilegios y los permisos del dominio de Informatica pertinentes en las cuentas dentro del dominio de seguridad.

Para obtener información sobre cómo crear una configuración de LDAP, consulte "Crear una configuración de LDAP" en la página 26.

Exportar el certificado de firma de aserciones

El proveedor de identidades envía aserciones de autenticidad a los proveedores de servicios en forma de certificado de firma de aserción.

Una aserción firmada contiene una firma que crea el proveedor de identidades utilizando un algoritmo elegido por el administrador del proveedor de identidades. A continuación, Informatica verifica la firma con el certificado público correspondiente que el administrador del dominio importó al truststore de SAML.

Informatica recomienda que habilite la aserción firmada.

Exporte el certificado de firma de aserción del proveedor de identidades para habilitar la aserción firmada.

Importar el certificado en el archivo de TrustStore que se utiliza para la autenticación SAML

Importe el certificado de firma de aserciones que el proveedor de identidades utiliza en el archivo de TrustStore que se usa para realizar la autenticación SAML en cada nodo de puerta de enlace del dominio de Informatica.

El certificado se puede importar en el archivo de TrustStore de Informatica predeterminado o en un archivo de TrustStore personalizado.

Configurar el proveedor de identidades

Configure el proveedor de identidades para emitir tokens de SAML a las aplicaciones web de Informatica.

Realice las siguientes tareas para configurar el proveedor de identidades:

- Añada una relación de confianza del dominio en el proveedor de identidades. La definición de relación de confianza permite al proveedor de identidades aceptar las solicitudes de autenticación procedentes de las aplicaciones web de Informatica que se ejecutan en el dominio.
- Edite la regla Enviar atributos de LDAP como notificaciones para asignar atributos de LDAP del almacén de identidades a los tipos correspondientes utilizados en los tokens de SAML emitidos por el proveedor de identidades.

Debe proporcionar el nombre de la relación de confianza para usuario autenticado cuando habilite la autenticación de SAML en un dominio. En función de los requisitos de seguridad, se pueden crear varias relaciones de confianza en el proveedor de identidades para permitir que los dominios utilizados por diferentes organizaciones dentro de la empresa usen la autenticación SAML.

Informatica reconoce "Informatica" como el nombre predeterminado de relación de confianza para usuario autenticado. Si crea una única relación de confianza para usuario autenticado cuyo nombre sea "Informatica", no es necesario que proporcione el nombre de la relación de confianza para usuario autenticado cuando habilite la autenticación de SAML en un dominio.

Nota: En todas las cadenas del proveedor de identidades (URL incluidas) se distinguen mayúsculas de minúsculas.

Añadir URL de aplicaciones web de Informatica al proveedor de identidades

Añada al proveedor de identidades la URL de cada aplicación web de Informatica que usa autenticación SAML.

La URL de una aplicación web de Informatica se proporciona para que el proveedor de identidades pueda aceptar las solicitudes de autenticación que envía la aplicación. Proporcionar la URL también permite al proveedor de identidades enviar el token de SAML a la aplicación tras autenticar al usuario.

Configurar la autenticación SAML en el dominio

La autenticación SAML se puede configurar en un dominio de Informatica existente o bien habilitarse al crear un dominio.

Cuando un dominio se habilita para que use la autenticación SAML, todas las aplicaciones web que se ejecutan en dicho dominio usarán el proveedor de identidades predeterminado que se especificó al habilitar la autenticación SAML en el dominio.

Seleccione una de las siguientes opciones:

Habilitar la autenticación SAML al ejecutar el programa de instalación de Informatica.

Puede habilitar la autenticación SAML y especificar la URL del proveedor de identidad al configurar el dominio como parte del proceso de instalación.

Habilitar la autenticación SAML en un dominio existente.

Utilice el comando infasetup updateDomainSamlConfig para habilitar la autenticación SAML en un dominio de Informatica existente. Puede ejecutar el comando en cualquier nodo de puerta de enlace dentro del dominio.

Habilitar la autenticación SAML al crear un dominio.

Utilice el comando infasetup defineDomain para habilitar la autenticación SAML al crear un dominio.

Consulte la *Referencia de comandos de Informatica* para obtener instrucciones sobre cómo usar los comandos.

Habilitar la autenticación SAML en los nodos

La autenticación SAML se debe configurar en cada nodo de trabajo y puerta de enlace del dominio de Informatica.

Seleccione una de las opciones siguientes para configurar la autenticación SAML en un nodo de puerta de enlace:

Habilitar la autenticación SAML al definir un nodo de puerta de enlace en un equipo.

Use el comando infasetup DefineGatewayNode para habilitar la autenticación SAML en el nodo de puerta de enlace.

Habilitar la autenticación SAML al configurar un nodo de puerta de enlace para que se una a un dominio que use la autenticación SAML.

Use el comando infasetup UpdateGatewayNode para habilitar la autenticación SAML en el nodo de puerta de enlace.

Habilitar la autenticación SAML al convertir un nodo de trabajo en un nodo de puerta de enlace.

Use el comando sip SwitchToGatewayNode para habilitar la autenticación SAML en el nodo.

Seleccione una de las opciones siguientes para configurar la autenticación SAML en un nodo de trabajo:

Habilitar la autenticación SAML al definir un nodo de trabajo en un equipo.

Use el comando infasetup DefineGatewayNode para habilitar la autenticación SAML en el nodo de trabajo.

Habilitar la autenticación SAML al configurar un nodo de trabajo para que se una a un dominio que use la autenticación SAML.

Use el comando infasetup UpdateWorkerNode para habilitar la autenticación SAML en el nodo de trabajo.

Consulte la *Referencia de comandos de Informatica* para obtener instrucciones sobre cómo usar los comandos.

Seguridad de la autenticación mejorada

Puede habilitar la firma de solicitudes, la respuesta firmada o la aserción cifrada para mejorar la seguridad de la autenticación:

Firma de solicitudes

Una solicitud de autenticación firmada contiene una firma para verificar la autenticidad de la propia solicitud. Informatica actúa como proveedor de servicios y envía una solicitud de autenticación al proveedor de identidades. Para mantener la integridad de la solicitud, se puede firmar la solicitud de autenticación.

Informatica firma una solicitud SAML con una clave privada y el proveedor de identidades verifica la firma con el certificado público correspondiente.

Informatica envía solicitudes de autenticación SAML a través de HTTP-Redirect. Las solicitudes utilizan la codificación deflate, que coloca la firma en un parámetro de URL.

Respuesta firmada

El proveedor de identidades responde a las solicitudes de autenticación de un proveedor de servicios. Una respuesta firmada contiene una firma que crea el proveedor de identidades utilizando un algoritmo elegido por el administrador del proveedor de identidades. A continuación, Informatica verifica la firma con el certificado público correspondiente que el administrador del dominio importó en el truststore de SAML.

Aserción firmada y aserción cifrada

El proveedor de identidades envía aserciones de autenticidad a los proveedores de servicios.

Una aserción firmada contiene una firma que crea el proveedor de identidades utilizando un algoritmo elegido por el administrador del proveedor de identidades. A continuación, Informatica verifica la firma con el certificado público correspondiente que el administrador del dominio importó en el truststore de SAML. Informatica recomienda que habilite la aserción firmada.

Informatica Administrator genera una clave asimétrica (clave pública-privada).

El proveedor de identidades puede cifrar la aserción mediante una clave de cifrado de aserción, que es una clave simétrica generada por el proveedor de identidades.

Cuando se habilita la aserción cifrada, el proveedor de identidades también cifra la clave simétrica mediante el certificado público que el administrador de seguridad importó en el proveedor de identidades. La respuesta SAML contendrá la aserción cifrada y una clave simétrica cifrada. Actuando como proveedor de servicios, Informatica descifra la clave simétrica cifrada utilizando la clave privada

correspondiente que Informatica administrator importa en el almacén de claves de SAML. Después de obtener la clave simétrica, Informatica descifra la aserción cifrada.

Siga los pasos de esta sección para habilitar la firma de solicitudes, la aserción cifrada o la respuesta firmada.

Firma de solicitudes

Puede habilitar la firma de solicitud durante el proceso de instalación-actualización o después de la instalación-actualización mediante infasetup.

Durante el proceso de instalación o actualización, marque la opción **Solicitud firmada** en la utilidad del programa de instalación.

Después del proceso de instalación o actualización, configure la firma de solicitud usando infasetup.

También puede configurar la firma de solicitud para las aplicaciones web mediante la interfaz de usuario de la aplicación web o la herramienta del administrador.

infasetup

Para usar infasetup, use las siguientes opciones con el comando `infasetup updateDomainSamlConfig`:

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

Para obtener información sobre los comandos, consulte la *Referencia de comandos de Informatica*.

Herramienta del administrador

Configure la firma de solicitudes en la Herramienta del administrador.

1. En el navegador del dominio, seleccione el nodo del dominio.
2. En las propiedades del nodo, haga clic en el icono **Editar** en la sección **Configuración de SAML**.
3. Seleccione **Habilitar la solicitud de firma**.
4. Rellene las siguientes propiedades:
   - Alias de clave privada de firma
   - Contraseña de clave privada de firma
   - Algoritmo de firma
5. Haga clic en **Aceptar**.
6. Reinicie el dominio.

Respuesta firmada

Habilite la respuesta firmada para permitir que el proveedor de identidades firme las respuestas de solicitud de autenticación del proveedor de servicios.

Puede habilitar la respuesta firmada durante el proceso de instalación-actualización o después de la instalación-actualización mediante infasetup.

Durante el proceso de instalación o actualización, marque la opción **Respuesta firmada** en la utilidad del programa de instalación.

Después del proceso de instalación o actualización, configure la firma de respuesta usando infasetup.

También puede configurar la respuesta firmada para las aplicaciones web mediante la interfaz de usuario de la aplicación web o la herramienta del administrador .

Nota: El proveedor de identidades de Okta SSO no admite la respuesta firmada.

infasetup

Para usar infasetup, use las siguientes opciones con el comando `infasetup updateDomainSamlConfig`:

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

Para obtener información sobre los comandos, consulte la *Referencia de comandos de Informatica*.

Administrator Tool

Configure la firma de respuestas en la Herramienta del administrador.

1. En el navegador del dominio, seleccione el nodo del dominio.
2. En las propiedades del nodo, haga clic en el icono **Editar** en la sección **Configuración de SAML**.
3. Seleccione **Habilitar la firma de respuesta**.
4. Rellene la propiedad Alias del certificado de firma de respuestas.
5. Haga clic en **Aceptar**.
6. Reinicie el dominio.

Aserción cifrada

Habilite la afirmación cifrada para permitir que el proveedor de identidades cifre las aserciones de autenticidad mediante una clave simétrica.

Puede habilitar la firma de aseción o aserción cifrada durante el proceso de instalación-actualización o después de la instalación-actualización mediante infasetup.

Durante el proceso de instalación o actualización, marque la opción **Cifrar aserción** en la utilidad del programa de instalación.

Después del proceso de instalación o actualización, configure la aserción cifrada usando infasetup.

También puede configurar la respuesta firmada para las aplicaciones web mediante la interfaz de usuario de la aplicación web o la herramienta del administrador .

infasetup

Para usar infasetup, use las siguientes opciones con el comando `infasetup updateDomainSamlConfig`:

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

Para obtener información sobre los comandos, consulte la *Referencia de comandos de Informatica*.

Administrator Tool

Configure la aserción cifrada en la Herramienta del administrador.

1. En el navegador del dominio, seleccione el nodo del dominio.
2. En las propiedades del nodo, haga clic en el icono **Editar** en la sección **Configuración de SAML**.
3. Seleccione **Habilitar el cifrado de aserciones**.
4. Rellene las siguientes propiedades:
   - Alias de clave privada de la aserción de cifrado
   - Contraseña de clave privada de la aserción de cifrado
5. Haga clic en **Aceptar**.
6. Reinicie el dominio.

Configurar aplicaciones web para que usen proveedores de identidades distintos

Las aplicaciones web de Informatica que se ejecutan en un mismo dominio se pueden configurar para que usen proveedores de identidades distintos. Así, por ejemplo, podríamos configurar Informatica Administrator para que use AD FS como proveedor de identidades e Informatica Analyst, para que use PingFederate.

Cuando un dominio se habilita para que use la autenticación SAML, todas las aplicaciones web que se ejecutan en dicho dominio usarán el proveedor de identidades predeterminado que se especificó al habilitar la autenticación SAML en el dominio. Por ejemplo, si se configura AD FS como proveedor de identidades, todas las aplicaciones web usarán AD FS, a menos que una aplicación web se configure para usar otro proveedor de identidades.

El proveedor de identidades predeterminado se especifica cuando se usa una de las siguientes opciones para habilitar la autenticación SAML:

- Al crear el dominio e instalar los servicios de Informatica
- Al ejecutar el comando infasetup defineDomain para crear un dominio
- Al ejecutar el comando infasetup updateDomainSamlConfig para habilitar la autenticación SAML en un dominio de existente

Para configurar una aplicación web para que use un proveedor de identidades distinto, se usa la Herramienta del administrador. Para configurar la Herramienta del administrador o la aplicación de supervisión para que usen un proveedor de identidades distinto, hay que modificar la configuración de SAML en el nodo donde la aplicación se ejecuta. Para configurar otras aplicaciones web para que usen un proveedor de identidades distinto, hay que modificar la configuración de SAML dentro del proceso de la aplicación.

Preparación para usar un proveedor de identidades

Realice las siguientes tareas para preparar una aplicación web de Informatica para que use un proveedor de identidades.

1. Cree una configuración de LDAP del almacén del proveedor de identidades que contiene las cuentas de usuario de aplicaciones web de Informatica. También hay que crear un dominio de seguridad de LDAP e importar en él las cuentas de usuario.
2. Exporte el certificado de firma de aserciones del proveedor de identidades.

3. Importe el certificado de firma de aserciones del proveedor de identidades en un archivo de TrustStore en cada nodo de puerta de enlace del dominio. El certificado se puede importar en el archivo de TrustStore predeterminado de Informatica o en un archivo de TrustStore personalizado.

   Si cambia el nombre de alias, importe el certificado correspondiente en el archivo de TrustStore de cada nodo de puerta de enlace y, tras ello, reinicie el nodo.
4. Añada una o varias relaciones de confianza al proveedor de identidades y asigne atributos de LDAP a los tipos correspondientes utilizados en los tokens de seguridad emitidos por el proveedor de identidades.
5. Añada la URL de la aplicación web de Informatica al proveedor de identidades.

Configurar Informatica Administrator para que use un proveedor de identidades

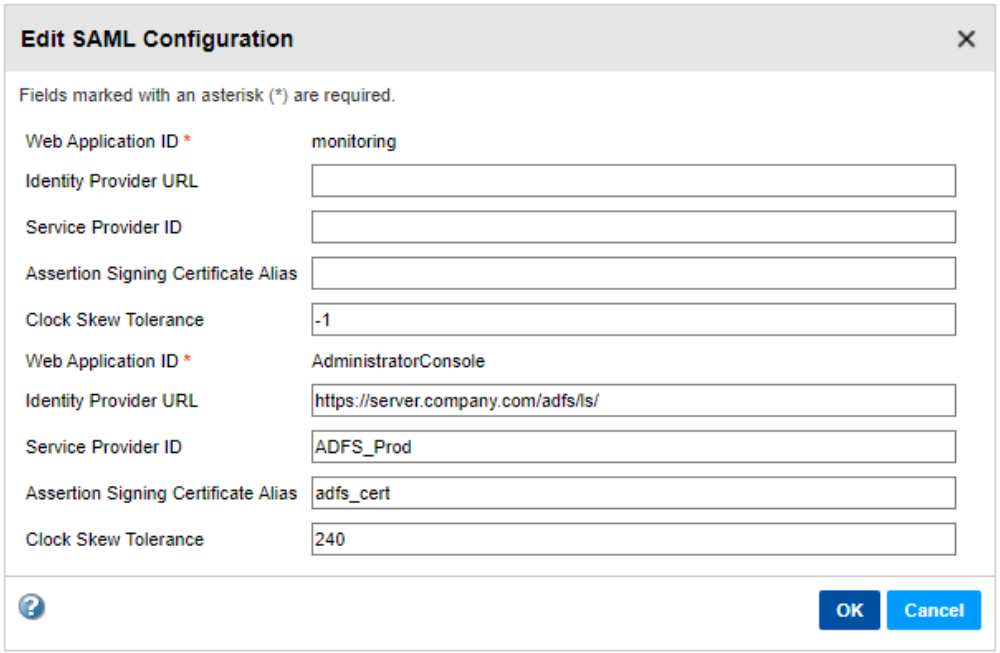
Use la Herramienta del administrador para configurar la Herramienta del administrador o la aplicación de supervisión para que usen un proveedor de identidades de SAML. La Herramienta del administrador o la aplicación de supervisión se configuran para que usen un proveedor de identidades en el nodo donde la aplicación se ejecuta.

1. En la Herramienta del administrador, haga clic en la ficha **Servicios y nodos**.
2. En el navegador de dominios, seleccione el nodo de puerta de enlace donde la Herramienta del administrador o la aplicación de supervisión se ejecutan.
3. Haga clic en el icono de edición junto a Configuración de SAML.
4. Especifique las propiedades necesarias para permitir que la aplicación use un proveedor de identidades.

   En la siguiente tabla se describen las propiedades que se pueden especificar:

Propiedad	Descripción
URL del proveedor de identidades	Opcional. URL del servidor del proveedor de identidades. Debe especificar la cadena de URL completa.
ID de proveedor de servicios	Opcional. Nombre de relación de confianza del usuario autenticado o identificador del proveedor de servicios del dominio, según se define en el proveedor de identidades.
Alias del certificado de firma de la aserción	Opcional. El nombre de alias especificado cuando se importa el certificado de firma de aserciones del proveedor de identidades en el archivo de TrustStore que se utiliza para la autenticación SAML. Si cambia el nombre de alias, importe el certificado correspondiente en el archivo de TrustStore de cada nodo de puerta de enlace y, tras ello, reinicie el nodo.
Tolerancia permitida para el desplazamiento del reloj	Opcional. Diferencia horaria permitida entre el reloj del sistema de host del proveedor de identidades y el reloj del sistema del nodo de puerta de enlace maestra. Opcional. La vida útil de los tokens de SAML emitidos por el proveedor de identidades se establece de acuerdo con el reloj del sistema del host del proveedor de identidades. La vida útil de un token de SAML emitido por el proveedor de identidades es válida si la hora de inicio y la hora de finalización establecidas en el token están dentro del número de segundos especificado del reloj del sistema del nodo de puerta de enlace maestra. Los valores deben estar comprendidos entre 0 y 600 segundos. Establezca esta propiedad en -1 para que use el valor configurado del dominio. El valor predeterminado es 120 segundos.

En la siguiente imagen se muestra la configuración para permitir que la Herramienta del administrador use AD FS como proveedor de identidades. Si no se especifica un valor de una propiedad, el dominio usará el valor establecido en la configuración de SAML predeterminada.



5. Haga clic en **Aceptar**.
6. Reinicie la aplicación.

Configurar una aplicación web de Informatica

Use la Herramienta del administrador para configurar una aplicación web de Informatica para que use un proveedor de identidades de SAML.

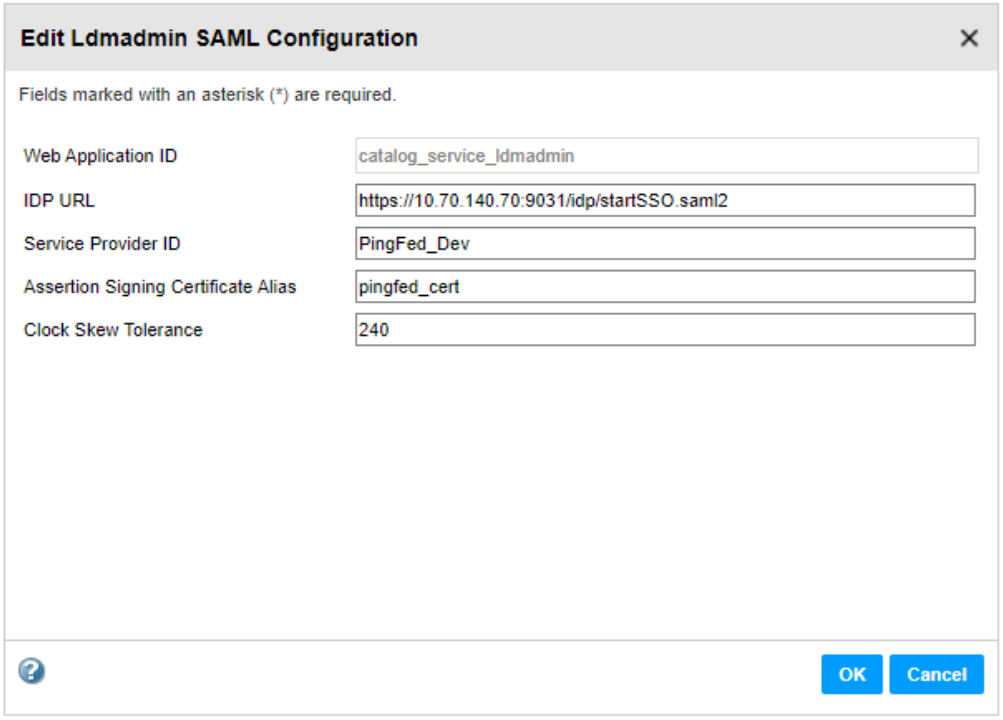
1. En la Herramienta del administrador, haga clic en la ficha **Servicios y nodos**.
2. Seleccione la aplicación o el servicio de la aplicación en el navegador de dominios.
   - Para configurar la aplicación Herramienta del analista para que use un proveedor de identidades, seleccione el servicio del analista y, después, haga clic en la ficha **Procesos**.
   - Para configurar la aplicación Herramienta de ingesta masiva para que use un proveedor de identidades, seleccione el servicio de ingesta masiva y, después, haga clic en la ficha **Procesos**.
   - Para configurar la aplicación Metadata Manager para que use un proveedor de identidades, seleccione el servicio de Metadata Manager y, después, haga clic en la ficha **Propiedades**.
   - Para configurar la aplicación Enterprise Data Catalog para que use un proveedor de identidades, seleccione el servicio de Catalog y, después, haga clic en la ficha **Procesos**.
   - Para configurar la aplicación Enterprise Data Preparation para que use un proveedor de identidades, seleccione el servicio de Enterprise Data Preparation y, después, haga clic en la ficha **Procesos**.
   - Para configurar la aplicación Data Privacy Management para que use un proveedor de identidades, seleccione el Servicio de Data Privacy Management y, después, haga clic en la ficha **Procesos**.
3. Haga clic en el icono de edición junto a **Configuración de SAML**.

4. Especifique las propiedades necesarias para permitir que la aplicación web use un proveedor de identidades.

   En la siguiente tabla se describen las propiedades que se pueden especificar:

Propiedad	Descripción
URL del proveedor de identidades	Opcional. URL del servidor del proveedor de identidades. Debe especificar la cadena de URL completa.
ID de proveedor de servicios	Opcional. Nombre de relación de confianza del usuario autenticado o identificador del proveedor de servicios del dominio, según se define en el proveedor de identidades.
Alias del certificado de firma de la aserción	Opcional. El nombre de alias especificado cuando se importa el certificado de firma de aserciones del proveedor de identidades en el archivo de TrustStore que se utiliza para la autenticación SAML. Si cambia el nombre de alias, importe el certificado correspondiente en el archivo de TrustStore de cada nodo de puerta de enlace y, tras ello, reinicie el nodo.
Tolerancia permitida para el desplazamiento del reloj	Opcional. Diferencia horaria permitida entre el reloj del sistema de host del proveedor de identidades y el reloj del sistema del nodo de puerta de enlace maestra. Opcional. La vida útil de los tokens de SAML emitidos por el proveedor de identidades se establece de acuerdo con el reloj del sistema del host del proveedor de identidades. La vida útil de un token de SAML emitido por el proveedor de identidades es válida si la hora de inicio y la hora de finalización establecidas en el token están dentro del número de segundos especificado del reloj del sistema del nodo de puerta de enlace maestra. Los valores deben estar comprendidos entre 0 y 600 segundos. El valor predeterminado es 120 segundos.

En la siguiente imagen se muestra la configuración para permitir que Enterprise Data Catalog use PingFederate como proveedor de identidades:



5. Haga clic en **Aceptar**.
6. Reinicie la aplicación o el servicio de la aplicación después de haberlos configurado para que usen un proveedor de identidades de SAML.

CAPÍTULO 6

Seguridad del dominio

Este capítulo incluye los siguientes temas:

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 del administrador. 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 aplicaciones web, como el servicio del analista o el servicio del concentrador de operaciones REST, 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.

Directorio predeterminado para el almacén de claves y el truststore

La implementación de Informatica incluye archivos de almacén de claves y de truststore predeterminados en el siguiente directorio predeterminado:

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

Informatica le recomienda que utilice el almacén de claves y truststore predeterminados solo para casos de uso de configuración y prueba de conceptos.

Para proteger un entorno de producción, use las siguientes directrices:

- Cuando configure la comunicación segura, no modifique, reemplace ni elimine archivos en el directorio predeterminado:
  `<directorio de instalación de Informatica>\services\shared\security`
- Configure un almacén de claves y truststore personalizados para la comunicación segura en una ubicación que no sea el directorio predeterminado:
  `<directorio de instalación de Informatica>\services\shared\security`
- No puede utilizar el almacén de claves y el truststore predeterminados para configurar otros servicios o clientes.

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 proteger 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`.

El archivo de almacén de claves debe contener los certificados SSL raíz e intermedio.

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_truststore.pem` y un truststore con formato JKS denominado `infa_truststore.jks`.

Los archivos de truststore deben contener los certificados SSL raíz, intermedio y de usuario final.

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.

Aplicó el encabezado de respuesta HTTP Strict Transport Security (HSTS).

Puede optar por habilitar el encabezado de respuesta HSTS en su dominio para evitar amenazas de seguridad de intermediario (MITM). Si habilita el encabezado de respuesta HSTS, puede detener los redireccionamientos HTTP a HTTPS y asegurarse de que solo se acceda a URL seguras (HTTPS).

Importante: Informatica admite la ejecución de varias aplicaciones y servicios tanto en HTTP como en HTTPS. Si habilita esta opción, no podrá acceder a las aplicaciones o servicios con URL HTTP.

Para habilitar esta opción, configure la variable de entorno `INFA_HSTS_HEADER_ENABLED` en `true` e importe los certificados de `infa_truststore` y el almacén de claves de Informatica Administrator a su navegador.

Directrices para el uso de archivos de truststore predeterminados y personalizados

El programa de instalación coloca los archivos infa_truststore.jks y de almacén de claves predeterminados en el directorio `<directorio de instalación de Informatica>/services/shared/security` de cada nodo. Puede utilizar el truststore predeterminado para la configuración y la prueba de concepto, pero los archivos de truststore y de almacén de claves predeterminados proporcionan una seguridad limitada. Para la producción, Informatica recomienda el uso de archivos de truststore y de almacén de claves personalizados para una comunicación y una autenticación SAML más seguras.

Coloque los archivos de truststore y de almacén de claves personalizados en un directorio personalizado. El nombre del archivo de truststore debe ser `infa_truststore.jks`.

No sobrescriba, elimine ni mueva los archivos predeterminados. los archivos de truststore y de almacén de claves predeterminados. No coloque archivos de truststore y de almacén de claves personalizados en el directorio `<directorio de instalación de Informatica>/services/shared/security`

Cuando cree un alias para nuevos certificados y claves privadas, no utilice el nombre predeterminado "Informatica LLC", que utilizan los archivos de truststore y de almacén de claves predeterminados.

Directrices para la creación de certificados y archivos de truststore y de almacén de claves personalizados

Puede emplear la utilidad de administración de claves y certificados Java keytool para crear un certificado SSL o una solicitud de firma de certificado (CSR), así como almacenes de claves y truststores en formato JKS.

La utilidad keytool se encuentra en el siguiente directorio de los nodos de dominio:

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

Si los nodos de dominio se ejecutan en AIX, puede utilizar la utilidad keytool que se proporciona con el JDK de IBM para crear un certificado SSL o una solicitud de firma de certificado (CSR), así como almacenes de claves y truststores.

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.
3. Ejecute la utilidad keytool para importar el certificado.
4. Reinicie el nodo.

Siguientes pasos

Para obtener más información acerca de cómo crear un almacén de claves y un truststore personalizados e importar certificados en su navegador, consulte el artículo de la Biblioteca de asistencia de Informatica sobre la creación de archivos de truststore y de almacén de claves para comunicaciones seguras en el dominio de Informatica: https://docs.informatica.com/data-integration/shared-content-for-data-integration/h2l/how-to-create-keystore-and-truststore-files-for-secure-communica/abstract.html.

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 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. Directorio que contiene los archivos de truststore. 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. 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 almacén de claves en todos los nodos del dominio.

6. Reinicie el dominio.

Habilitar la comunicación segura para el dominio en la Herramienta del administrador

La comunicación segura para el dominio se puede habilitar mediante la Herramienta del administrador. Al habilitar la comunicación segura en la Herramienta del administrador, también debe ejecutar los comandos infasetup para actualizar los nodos.

Al habilitar la opción Comunicación segura en la Herramienta del administrador, 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 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 del administrador, 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. Directorio que contiene los archivos de truststore. 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. 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 almacén de claves en todos los nodos del dominio.

9. Reinicie el dominio.

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: `<directorio 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:

Puede utilizar 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.

Importante: Si se envía procesamiento a un clúster de cálculo y el servicio de integración de datos se ejecuta en una cuadrícula, importe los certificados una sola vez y, tras ello, cópielos en cada servicio de integración de datos en la cuadrícula. Cada vez que se importa un certificado, el contenido del certificado es idéntico, pero no los valores hexadecimales. Esto hace que las asignaciones simultáneas que se ejecutan en la cuadrícula generen errores de inicialización.

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.

Utiliza el certificado SSL predeterminado de Informatica, pero los archivos de truststore no se encuentran en el directorio predeterminado de Informatica.

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
-DatabaseTlsEnabled -dbtls	database_tls_enabled	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 True.
-DatabaseTruststoreLocation -dbtl	database_truststore_location	Obligatorio. Ruta de acceso y nombre del archivo de truststore que contiene el certificado SSL de la base de datos.
-DatabaseTruststorePassword -dbtp	database_truststore_password	Obligatorio. Contraseña del archivo truststore 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.

   Restaure 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 infasetup RestoreDomain en el paso5
-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 del concentrador de operaciones REST

- 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 *changeit*.
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 del servicio del concentrador de operaciones REST

Cuando utiliza el servicio del concentrador de operaciones REST, puede configurar las propiedades de HTTPS seguro para el concentrador de operaciones REST.

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

Propiedad	Descripción
Puerto HTTP	Número de puerto HTTP único para el proceso del servicio del concentrador de operaciones REST cuando el servicio usa el protocolo HTTP. El valor predeterminado es 6555.
Puerto HTTPS	Número de puerto en el que se ejecuta el servicio del concentrador de operaciones REST cuando se habilita el protocolo de seguridad de la capa de transporte (TLS). Utilice un número de puerto diferente al número de puerto HTTP.
Habilitar Transport Layer Security	Selecciónelo para habilitar una conexión segura entre el servicio del concentrador de operaciones REST y el cliente REST.
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 esta propiedad no se establece, el servicio del concentrador de operaciones REST utiliza la contraseña predeterminada.
Protocolo SSL	Un campo en blanco habilita la versión más alta de TLS disponible. La versión de TLS habilitada depende del valor. 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: - HTTP. Permite ejecutar el concentrador de servicios web solo en HTTP. - HTTPS. Permite ejecutar el concentrador de servicios web solo en HTTPS. - HTTP y HTTPS. Permite ejecutar el concentrador de servicios web en los modos HTTP y HTTPS.
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 *changeit*.

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. **Nota:** 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 **Esquema URL** 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. **Nota:** El servicio de Metadata Manager utiliza cifrado RSA. Por lo tanto, Informatica 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 “Lista predeterminada de conjuntos de cifrado” en la página 100

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.

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.

Lista predeterminada de conjuntos de cifrado

De forma predeterminada, el dominio de Informatica 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

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 la 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 Informatica.

   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 Informatica.

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 listDomainCiphers -l EFFECTIVE
   ```

Orígenes y destinos seguros

Informatica 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: rwx-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 `rwx` 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 `rwx` 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 la opción encryptionKeyLocation para generar una clave de cifrado:

Opción	Argumento	Descripción
-encryptionKeyLocation -kl	encryption_key_location	Directorio que contiene la clave de cifrado actual. El nombre del archivo de cifrado es *sitekey*. Informatica cambia el nombre del archivo *sitekey* actual a *sitekey_old* y genera una clave de cifrado en un archivo nuevo denominado *sitekey* en el mismo directorio.

   Nota: El programa de instalación crea una clave de cifrado durante la instalación y la actualización. No necesita las opciones de palabra clave y nombre de dominio al generar el archivo de cifrado sitekey. Asegúrese de guardar una copia de la clave única del sitio. Si pierde la clave de sitio, no puede volver a generarla. No comparta la clave única del sitio con otras personas.
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	Directorio donde se almacenan el archivo con la clave de cifrado antigua, llamado *siteKey_old*, y el archivo con la clave de cifrado nueva, llamado *siteKey*. 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. Si el dominio tiene varios nodos, cualquiera de los nodos del dominio donde se ejecute el comando migrateEncryptionKey debe poder acceder a este directorio. Cuando migra un dominio multinodo, todos los nodos del dominio deben usar la misma clave de cifrado. Para cambiar la clave de cifrado del dominio, ejecute el comando infasetup migrateEncryptionKey en todos los nodos del dominio. **Nota:** En UNIX, el nombre de archivo *siteKey_old* 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.
-IsDomainMigrated -mig	is_domain_migrated	Indica si el dominio se ha actualizado para utilizar la clave de cifrado más reciente. Cuando ejecute el comando migrateEncryptionKey por primera vez, establezca esta opción en False para indicar que el dominio utiliza la clave de cifrado antigua. Tras la primera vez, cuando ejecute el comando migrateEncryptionKey para actualizar otros nodos del dominio, establezca esta opción en True para indicar que el dominio se ha actualizado para utilizar la clave de cifrado más reciente. O bien, puede ejecutar el comando migrateEncryptionKey sin esta opción. El valor predeterminado es True.

5. 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.

6. Reinicie el dominio.

   Debe actualizar todos los servicios de repositorio en el dominio para actualizar y cifrar los datos confidenciales en los repositorios con la nueva clave de cifrado. También debe migrar la clave del sitio después de actualizar el dominio.

7. 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	`infacmd mrs UpgradeContents`
Servicio de repositorio de PowerCenter	`pmrep Upgrade`

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 HTTPS de Informatica Administrator	Sin puerto predeterminado. Introduzca el número de puerto requerido cuando cree el servicio. Si se establece el valor de este puerto como 0, se deshabilitará una conexión HTTPS a la Herramienta del administrador.
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.

Puerto	Descripción
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 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 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)	8080
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.
Base de datos de almacén de creación de perfiles	Sin puerto predeterminado. Introduzca el número de puerto de la base de datos.

Servicio de acceso a metadatos

La siguiente tabla muestra el puerto predeterminado asociado con el servicio de acceso a metadatos:

Tipo	Puerto predeterminado
Servicio de acceso a metadatos (HTTP)	7080 El servicio de acceso a metadatos utiliza números de puerto consecutivos para conectar varias distribuciones de Hadoop.
Servicio de acceso a metadatos (HTTPS)	Sin puerto predeterminado. Introduzca el número de puerto requerido cuando cree el servicio. El servicio de acceso a metadatos utiliza números de puerto consecutivos para conectar varias distribuciones de Hadoop.

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)	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 DBMOVER.

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 DBMOVER.

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 7

Administración de seguridad en Informatica Administrator

Este capítulo incluye los siguientes temas:

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 de seguridad. Administrar usuarios, grupos, funciones y privilegios.

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.
- **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.

- **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.

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 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 acceso a metadatos
- Servicio de Metadata Manager
- Servicio de concentrador de servicios web

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.

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

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.

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 configuraciones de LDAP y perfiles del sistema operativo. También es posible ver los usuarios que disponen de privilegios para un servicio.

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.
- Sección Perfiles operativos. Seleccione un perfil operativo para ver las propiedades del perfil de sistema operativo y los permisos asignados a los usuarios y grupos que usan el perfil de sistema operativo.
- Sección Configuración de LDAP. Seleccione una configuración para ver los detalles de la conexión del servidor de LDAP, el dominio de seguridad de LDAP que contiene los usuarios y grupos importados desde el servicio de directorio de LDAP y la programación de sincronización de LDAP.

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 incluye un menú Acciones para administrar grupos, usuarios, funciones, perfiles de sistema operativo o configuraciones de LDAP.
- Haga clic con el botón derecho en un objeto. Haga clic con el botón derecho en el navegador para mostrar las opciones disponibles 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 Informatica. La autenticación nativa usa el dominio de seguridad nativo, que contiene los usuarios y los grupos creados y administrados en la Herramienta del administrador. La autenticación de LDAP usa los dominios de seguridad de LDAP que contienen los usuarios y grupos importados del servicio de directorio de LDAP.

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.

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.

- Permisos. Muestra el nivel de acceso que los usuarios del grupo tienen para realizar tareas en objetos de dominio, incluidos nodos, cuadrículas y servicios de aplicación. También muestra el nivel de acceso que los usuarios dentro del grupo tienen para realizar tareas en los objetos de conexión y los perfiles del sistema operativo.

Usuarios

Un usuario con una cuenta en el dominio de Informatica puede iniciar sesión en las siguientes aplicaciones cliente:

- Informatica Administrator
- Cliente de PowerCenter
- Informatica Developer
- Informatica Analyst
- Metadata Manager

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 del administrador. La autenticación de LDAP usa los dominios de seguridad de LDAP que contienen los usuarios y grupos importados del servicio de directorio de LDAP.

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.

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.
- Permisos. Muestra el nivel de acceso que el usuario tiene para realizar tareas en objetos de dominio, incluidos nodos, cuadrículas y servicios de aplicación. También muestra el nivel de acceso que el usuario tiene para realizar tareas en los objetos de conexión y en los perfiles del sistema operativo.

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.

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.

Perfiles del sistema operativo

Un perfil del sistema operativo es un mecanismo de seguridad que el servicio de integración de datos y el servicio de integración de PowerCenter utilizan para ejecutar asignaciones, flujos de trabajo y trabajos de creación de perfiles.

La sección Perfiles del sistema operativo del navegador enumera los perfiles del sistema operativo configurados en el dominio.

Cuando seleccione un perfil del sistema operativo en el navegador, el panel de contenido mostrará las siguientes fichas:

- Propiedades. Muestra propiedades generales del perfil del sistema operativo configurado para el servicio de integración de datos, para el servicio de integración de PowerCenter o para ambos servicios de aplicación.
- Permisos. Muestra los permisos asignados a los usuarios y grupos que utilizan el perfil del sistema operativo. También indica si el perfil del sistema operativo es el perfil predeterminado asignado a un usuario o grupo.

Configuración de LDAP

Puede configurar un dominio de Informatica para permitir que los usuarios y los grupos importados de uno o varios servicios de directorio de LDAP puedan iniciar sesión en los nodos, servicios y clientes de aplicaciones de Informatica.

En la sección Configuración de LDAP del navegador se enumeran las configuraciones de LDAP que el dominio utiliza.

Cuando seleccione una configuración de LDAP, aparecerán las siguientes fichas en la ficha Configuración de LDAP:

- Resumen. Enumera los detalles de conexión del servidor de LDAP que contiene el servicio de directorio desde el que desea importar usuarios y grupos.
- Dominios de seguridad. Enumera los detalles del dominio de seguridad de LDAP que contiene los usuarios y grupos importados desde el servicio de directorio de LDAP.
- Programación. Enumera los detalles de la programación de sincronización, especificando cuándo el Administrador de servicios actualiza el dominio de seguridad con los usuarios y grupos en el servicio de directorio de LDAP.

Administración de cuentas

Para mejorar la seguridad en el dominio de Informatica, puede bloquear las cuentas de usuario y administrador tras un número especificado de intentos de inicio de sesión incorrectos.

La sección Configuración de bloqueo de cuentas de la página Administración de cuentas muestra si el bloqueo de cuentas está habilitado para las cuentas de usuario y las cuentas de administrador. Además, indica el número máximo de intentos de inicio de sesión incorrectos permitido.

La sección Usuarios nativos bloqueados de la página enumera las cuentas de usuario bloqueadas en el dominio de seguridad nativo. Puede desbloquear una cuenta de usuario en el dominio de seguridad nativo.

La sección Usuarios LDAP bloqueados de la página enumera las cuentas de usuario bloqueadas en un dominio de seguridad de LDAP. Puede desbloquear una cuenta de usuario en el dominio de Informatica. Sin embargo, el administrador de LDAP debe desbloquear la cuenta de usuario en el servidor de LDAP. El usuario

no puede iniciar sesión en el dominio de Informatica hasta que el administrador de LDAP desbloquee la cuenta de usuario.

Informes de auditoría

Los informes de auditoría proporcionan información acerca de los usuarios y grupos en el dominio de Informatica, así como de los privilegios, las funciones y los permisos asignados a cada usuario o grupo.

Seleccione el informe de auditoría que desee generar en el menú Seleccionar tipo de informe. Puede generar los siguientes informes de auditoría:

Información personal del usuario

Muestra información de contacto y detalles de estado de las cuentas de usuario en el dominio. 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.

Gestión de contraseñas

Puede cambiar la contraseña mediante la aplicación Cambiar contraseña.

Puede abrir la aplicación Cambiar contraseña desde la Herramienta del administrador 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.

Para una cuenta de usuario nativa, si habilita la complejidad de la contraseña, utilice las siguientes directrices al crear o cambiar una contraseña:

- La longitud de la contraseña debe ser de al menos ocho caracteres.

- Debe ser una combinación de un carácter alfabético, un carácter numérico y un carácter no alfanumérico, como por ejemplo:
  ! \ " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ] ^ _ ` { | } ~

Cuando se utilizan caracteres especiales en una contraseña, el shell a veces los interpreta de forma diferente. Por ejemplo, $ se interpreta como una variable. En este caso, utilice un carácter de escape antes del carácter especial.

Cambio 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.

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.

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.

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

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.

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.
- 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 del sistema operativo. Si ejecuta el servicio de integración en UNIX o Linux, puede configurar el servicio de integración para que utilice perfiles del sistema operativo. Utilice perfiles del 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.

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

Administrador predeterminado

Cuando se instalan servicios de Informatica, 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.

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.

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 Informatica Analyst

Tiene permisos y privilegios totales en Informatica Analyst. El administrador de Informatica Analyst puede iniciar sesión en Informatica 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 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.

Creación de usuarios nativos

En la ficha Seguridad, puede añadir, editar o eliminar usuarios nativos.

1. En la Herramienta del administrador, 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 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. 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.

Propiedad	Descripción
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: < > “
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: < > “

4. 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.

1. En Administrator Tool, haga clic en la ficha Seguridad.
2. En la sección Usuarios del navegador, seleccione una cuenta de usuario nativo y haga clic en Editar.
3. Para cambiar la contraseña, seleccione Cambiar contraseña.

   En la ficha Seguridad, aparecen vacíos los campos Contraseña y Confirmar contraseña.
4. Escriba una nueva contraseña y confirme.
5. Puede modificar el nombre completo, la descripción, el correo electrónico y el teléfono según sea necesario.
6. Haga clic en Aceptar para aplicar los cambios.

Asignar usuarios nativos a grupos nativos

Asigne usuarios nativos a grupos nativos en la ficha Seguridad.

1. En Administrator Tool, haga clic en la ficha Seguridad.
2. En la sección Usuarios del navegador, seleccione una cuenta de usuario nativo y haga clic en **Editar**.
3. Haga clic en la ficha Grupos.
4. 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.

5. 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 la Herramienta del administrador, haga clic en la ficha **Seguridad**.
2. En la sección Grupos del navegador, seleccione un grupo nativo y después 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 después 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 después 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.

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**.

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 tools 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 los servicios de Informatica. 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

Use la ficha Registros de Administrator tool para ver los registros de actividad del usuario. Vea los registros de actividad del usuario para revisar los intentos de inicio de sesión que se han realizado desde aplicaciones cliente de Informatica. A través de los registros también puede determinar cuándo un usuario ha creado, actualizado o eliminado servicios, nodos, usuarios, grupos o funciones.

Consulte la *Guía de Informatica Administrator* si desea más información sobre los registros de actividad del usuario y la ficha Registros de Administrator tool.

También puede usar el comando infacmd isp getUserActivityLog para ver los datos de los registros de actividad del usuario. El comando infacmd isp getUserActivityLog utiliza la siguiente sintaxis:

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

El comando infacmd isp getUserActivityLog requiere que tenga asignada la función de administrador o que pertenezca al grupo Administrador. Para obtener más información sobre el comando isp getUserActivityLog, consulte *Referencia de comando de Informatica*.

Entre los datos del registro de actividad del usuario se incluyen los intentos que ha hecho el usuario de iniciar sesión desde clientes de Informatica, tanto si han sido satisfactorios como si no. Si el cliente establece las propiedades personalizadas en solicitudes de inicio de sesión, en los datos del registro se incluirán las propiedades personalizadas.

Nota: Los registros de actividad del usuario no incluyen los intentos de inicio de sesión que realiza el usuario en un dominio configurado para usar la autenticación de Kerberos.

En los datos de actividad del usuario se incluyen las siguientes propiedades para cada intento de inicio de sesión desde un cliente de Informatica:

- Nombre de la aplicación
- Versión de la aplicación
- Nombre de host o dirección IP del host de aplicación

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 escribir los eventos 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. Consulte *Referencia de comando de Informatica* si desea más información sobre cómo usar el comando isp convertUserActivityLog.

Códigos de actividad del usuario

Los registros de actividad del usuario incluyen códigos que indican si las actividades se han realizado correctamente o no.

Los códigos de actividad válidos incluyen lo siguiente:

- CCM_10437. Indica que una actividad se ha realizado correctamente.
- CCM_10438. Indica que no se ha podido realizar una actividad.
- CCM_10778. Indica que se ha realizado correctamente un intento de inicio de sesión con propiedades personalizadas.
- CCM_10779. Indica que no se ha podido realizar un intento de inicio de sesión con propiedades personalizadas.
- CCM_10786. Indica que se ha realizado correctamente un intento de inicio de sesión sin propiedades personalizadas.
- CCM_10787. Indica que no se ha podido realizar un intento de inicio de sesión sin propiedades personalizadas.

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.
- CCM_10778. Indica que se ha realizado correctamente un intento de inicio de sesión con propiedades personalizadas.
- CCM_10779. Indica que no se ha podido realizar un intento de inicio de sesión con propiedades personalizadas.
- CCM_10786. Indica que se ha realizado correctamente un intento de inicio de sesión sin propiedades personalizadas.
- CCM_10787. Indica que no se ha podido realizar un intento de inicio de sesión sin propiedades personalizadas.

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 Informatica
- 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 Informatica.

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.

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.

Propiedad	Descripción
$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.
$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 del sistema operativo para el servicio de integración de datos

La siguiente tabla describe las propiedades de perfil del sistema operativo para el servicio de integración de datos:

Propiedad	Descripción
Nombre	Nombre de sólo lectura del perfil del sistema operativo. El nombre no puede exceder los 128 caracteres. No puede incluir 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: * ? < > " | , [ ]
$DISTempDir	Directorio de los archivos temporales creados cuando se ejecutan los trabajos. No puede contener los siguientes caracteres especiales: * ? < > " | , [ ] El valor predeterminado es <directorio raíz>/disTemp. **Nota:** Si el servicio de integración de datos está configurado para usar varios perfiles de sistema operativo, especifique un directorio común para todos los perfiles porque un directorio independiente para cada perfil da como resultado un uso excesivo del espacio en disco.
$DISCacheDir	El directorio de los archivos de índice y memoria caché de datos de las transformaciones. No puede contener los siguientes caracteres especiales: * ? < > " | , [ ] El valor predeterminado es <directorio raíz>/cache.
$DISSourceDir	El directorio para archivos sin formato de origen utilizados en una asignación. No puede contener los siguientes caracteres especiales: * ? < > " | , [ ] El valor predeterminado es <directorio raíz>/source.
$DISTargetDir	El directorio para los archivos sin formato de destino utilizados en una asignación. No puede contener los siguientes caracteres especiales: * ? < > " | , [ ] El valor predeterminado es <directorio raíz>/target.
$DISRejectedFilesDir	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: * ? < > " | , [ ] El valor predeterminado es <directorio raíz>/reject.

Propiedad	Descripción
$DISLogDir	Directorio para los registros. No puede contener los siguientes caracteres especiales: * ? < > " | , [ ] El valor predeterminado es <directorio raíz>/disLogs.
Habilitar propiedades de suplantación de Hadoop	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. El usuario de suplantación de Hadoop predeterminado es el usuario que ha iniciado sesión. Para especificar otro usuario de suplantación de Hadoop diferente, seleccione **Utilizar el usuario especificado como usuario de suplantación de Hadoop** e introduzca un nombre de usuario.
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 del 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 del sistema operativo. Si no especifica la variable de entorno LD_LIBRARY_PATH en las propiedades del perfil del sistema operativo, el servicio de integración usa su variable de entorno LD_LIBRARY_PATH. **Nota:** 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.
Directorio de la memoria caché de archivos sin formato	El directorio de la memoria caché de archivos sin formato donde la herramienta del analista almacena los archivos sin formato cargados. Si el servicio del analista se conecta a un servicio de integración de datos que utiliza perfiles del 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.

Propiedades de perfil del sistema operativo para el servicio de acceso a metadatos

La siguiente tabla describe las propiedades de perfil del sistema operativo para el servicio de acceso a metadatos:

Propiedad	Descripción
Nombre	Nombre de sólo lectura del perfil del sistema operativo. El nombre no puede exceder los 128 caracteres. No puede incluir espacios ni los siguientes caracteres especiales: % * + \ / ? ; < >
Nombre del usuario del sistema	Nombre de solo lectura de un usuario del sistema operativo que ya existe en los sistemas en los que se ejecuta el servicio de acceso a metadatos. El servicio de acceso a metadatos permite a Developer tool acceder a la información de conexión de Hadoop para importar y obtener una vista previa de los metadatos usando el acceso al sistema del usuario del sistema operativo.
Habilitar propiedades de suplantación de Hadoop	Indica que el servicio de acceso a metadatos usa el usuario de suplantación de Hadoop para importar y obtener una vista previa de los metadatos. El usuario de suplantación de Hadoop predeterminado es el usuario que ha iniciado sesión. Para especificar otro usuario de suplantación de Hadoop diferente, seleccione **Utilizar el usuario especificado como usuario de suplantación de Hadoop** e introduzca un nombre de usuario.

Crear un perfil del sistema operativo

Cree un perfil del 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 del sistema operativo. El servicio de integración de PowerCenter usa el perfil del sistema operativo para ejecutar flujos de trabajo. El servicio de integración de datos utiliza el perfil del sistema operativo para ejecutar asignaciones, perfiles y flujos de trabajo. El servicio de acceso a metadatos utiliza el perfil del sistema operativo para acceder a la información de la conexión de Hadoop e importar y obtener una vista previa de los metadatos.

1. En la Herramienta del administrador, haga clic en la ficha **Seguridad**.
2. En el menú Acciones de seguridad, haga clic en **Crear perfil del sistema operativo**.

   El cuadro de diálogo **Crear perfil del sistema operativo: paso 1 de 3** aparece.

3. Especifique las siguientes propiedades generales para el perfil del sistema operativo:

Propiedad	Descripción
Nombre	Nombre del perfil del 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. **Nota:** Cuando cree perfiles del 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 del sistema operativo: paso 2 de 3** aparece.
5. Seleccione el servicio que utilizará el perfil del sistema operativo.
   - Servicio de integración de PowerCenter
   - Servicio de integración de datos
   - Servicio de acceso a metadatos
6. Configure las propiedades del perfil del sistema operativo para los servicios seleccionados. Para crear un perfil del sistema operativo para el servicio de acceso a metadatos, también debe seleccionar el servicio de integración de datos junto con el servicio de acceso a metadatos y especificar la variable $DISRootDir para el servicio de integración de datos.
7. Si los servicios acceden a un entorno de Hadoop en tiempo de diseño o de ejecución, configure las propiedades de suplantación de Hadoop de la siguiente manera:
   a. Seleccione **Habilitar propiedades de suplantación de Hadoop**.
   b. 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 del sistema operativo, configure las propiedades del servicio del analista.
10. Haga clic en **Siguiente**.

    El cuadro de diálogo **Asignar grupos y usuarios al perfil del sistema operativo: paso 3 de 3** aparece.
11. En la ficha **Grupos** , asigne grupos al perfil del sistema operativo de la siguiente manera:
    a. Para asignar grupos específicos al perfil del sistema operativo, seleccione uno o varios grupos y haga clic en **Añadir**.
    b. Para asignar todos los grupos disponibles al perfil del sistema operativo, haga clic en **Añadir todos**.
12. Opcionalmente, asigne el perfil del 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 del sistema operativo de la siguiente manera:
    a. Para asignar usuarios específicos al perfil del sistema operativo, seleccione uno o varios usuarios y haga clic en **Añadir**.
    b. Para asignar todos los usuarios disponibles al perfil del sistema operativo, haga clic en **Añadir todos**.
14. Opcionalmente, asigne el perfil del 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 del sistema operativo, el panel de detalles muestra las propiedades del perfil del sistema operativo y los grupos y usuarios a los que se ha asignado el perfil.

Editar un perfil del sistema operativo

Puede editar un perfil del 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 del sistema operativo. Si no desea usar el usuario del sistema operativo especificado en el perfil del sistema operativo, elimine el perfil del sistema operativo.

1. En la Herramienta del administrador, haga clic en la ficha **Seguridad**.
2. Seleccione la vista **Perfiles del sistema operativo**.
3. Seleccione el perfil del 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, el servicio de integración de PowerCenter o el servicio de acceso a metadatos que desee configurar.
6. Edite las propiedades del servicio.
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 Informatica 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 Informatica 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 Informatica.
- 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 **Habilitar el bloqueo de cuentas de administrador** 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 **Habilitar bloqueo de cuenta** 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:

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.
- 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 ingesta masiva. Determina las acciones que los usuarios pueden realizar con la herramienta de ingesta masiva.
- 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.
- Privilegios del servicio de repositorio de PowerCenter. Determinan las acciones del repositorio de PowerCenter que los usuarios pueden realizar mediante el Repository Manager, 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.

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 privilegios 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.

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: Using Groups and Roles to Manage Access Controls.

Privilegios del dominio

Los privilegios del dominio determinan las acciones que pueden realizar los usuarios con la Herramienta del administrador y los programas de la línea de comandos infacmd y pmrep.

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, las conexiones y las configuraciones de clúster.
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 del administrador.
Administración en la nube	Incluye privilegios para añadir y ver organizaciones de Informatica Cloud en la herramienta del administrador.

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. 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: - Asignar privilegios y funciones a usuarios y grupos para el dominio y servicio de aplicaciones. - Editar y quitar los privilegios y funciones asignados a usuarios y grupos.

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: - Configurar la autenticación de LDAP para el dominio. - Crear, editar y eliminar usuarios, grupos y funciones. - Importar usuarios y grupos de LDAP.
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.
- Determinar las configuraciones de clúster.
- 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: - Ver las propiedades y los eventos de registro del dominio. - Definir la configuración de supervisión.
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 del administrador, 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: - 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. - Recibir alertas de servicio de aplicación.

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: - Configurar servicios de aplicación. - Conceder permiso para los servicios de aplicación.
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.
Servicio de Metadata Manager	El usuario puede realizar las siguientes acciones: - Realizar una copia de seguridad del contenido del repositorio de Metadata Manager. - Eliminar contenido del repositorio de Metadata Manager. - Actualizar el contenido del Servicio de Metadata Manager. **Nota:** Para crear o restaurar el contenido del repositorio de Metadata Manager, el usuario debe pertenecer al grupo Administrador predeterminado.
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	El usuario puede realizar las siguientes acciones: - Crear y eliminar contenido del repositorio de modelos. - Crear, eliminar y volver a indizar el índice de búsqueda. - Actualizar el contenido del servicio de repositorio de modelos mediante el menú **Acciones** 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.
Servicio de integración de PowerCenter	El usuario puede ejecutar el servicio de integración de PowerCenter en modo seguro.

Permiso en	Descripción
Servicio de repositorio de PowerCenter	El usuario puede realizar las siguientes acciones: - Hacer copias de seguridad, restaurar y actualizar el repositorio de PowerCenter. - Configurar el linaje de datos para el repositorio de PowerCenter. - Copiar contenido desde otro repositorio de PowerCenter. - Cerrar conexiones de usuario y liberar bloqueos del repositorio de PowerCenter. - Crear y eliminar contenido del repositorio de PowerCenter. - Crear, editar y eliminar extensiones de metadatos reutilizables en el PowerCenter Repository Manager. - Habilitar el control de versiones para el repositorio de PowerCenter. - Administrar un dominio del repositorio de PowerCenter. - Realizar una purga avanzada de las versiones de objetos en el nivel de repositorio en el PowerCenter Repository Manager. - Registrar y cancelar el registro de complementos del repositorio de PowerCenter. - Ejecutar el repositorio de PowerCenter en modo exclusivo. - Enviar notificaciones del repositorio de PowerCenter a los usuarios. - Actualizar las estadísticas del repositorio de PowerCenter. - Actualizar el contenido del servicio de repositorio de PowerCenter.
Servicio de Test Data Manager	El usuario puede realizar las siguientes acciones: - Crear y eliminar el contenido del repositorio de Test Data Manager. - Actualizar el contenido del servicio de Test Data Manager.
Objeto de licencia	El usuario puede realizar las siguientes acciones: - Editar objetos de licencia. - Conceder permiso para los objetos de licencia.
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.

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: - Configurar y cerrar nodos y cuadrículas. - Conceder permiso para nodos y cuadrículas.
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: - Editar carpetas. - Conceder permiso para carpetas.
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 también pueden crear, actualizar y eliminar configuraciones de clúster, así como establecer y borrar propiedades de la configuración en Administrator tool y el programa de la 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.

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 y configuraciones de clúster.
Escribir al conectar	El usuario puede copiar, editar y eliminar conexiones.
Conceder al conectar	El usuario puede conceder y revocar permisos en las conexiones.
Escribir en la configuración del clúster	El usuario puede crear, actualizar y eliminar configuraciones de clúster. El usuario puede establecer y borrar propiedades de la configuración del clúster.

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. **Nota:** En un dominio que utilice la autenticación Kerberos, los usuarios también deben tener la función de administrador en el servicio de repositorio de modelos de supervisión para acceder a la vista Estadísticas de resumen y a las estadísticas de los objetos de dominio.
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: - Anular trabajos. - Emitir de nuevo trabajos de asignación. - Ver registros de trabajos.

Los usuarios no necesitan tener el privilegio Acceder a Informatica 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: - Iniciar sesión en Administrator Tool. - Administrar su propia cuenta cuenta de usuario en Administrator Tool. - Exportar eventos de registro.

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. **Nota:** Al seleccionar este privilegio también se concede el privilegio **Acceder a especificaciones de asignación** 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 **Diseño**. - Espacio de trabajo **Detección**. - Espacio de trabajo **Glosario**. - Espacio de trabajo **Cuadros de mando**. **Nota:** 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 **Espacio de trabajo de diseño**, **Espacio de trabajo de detección**, **Espacio de trabajo del glosario** o **Espacio de trabajo de cuadros de mando** para acceder a los proyectos.
Espacio de trabajo Diseño	-	El usuario puede acceder al espacio de trabajo **Diseño**.
Espacio de trabajo Detección	-	El usuario puede acceder al espacio de trabajo **Detección**.
Espacio de trabajo Glosario	-	El usuario puede acceder al espacio de trabajo **Glosario**.
Espacio de trabajo Cuadros de mando	-	El usuario puede acceder al espacio de trabajo **Cuadros de mando**.

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	- Cree una tabla de referencia en las herramientas Analyst y Developer. - Cree una tabla de referencia con el comando infacmd rtm import. - Importe un objeto de la tabla de referencia en el repositorio de modelos. - Copie una tabla de referencia en las herramientas Analyst y Developer. - Cree una tabla de referencia a partir de datos de perfil. **Nota:** El privilegio Crear también concede el privilegio Editar de forma predeterminada.
Editar los datos y metadatos de la tabla de referencia	Lectura en proyecto	- Edite los valores de los datos en las herramientas Developer y Analyst. - Añada los datos de perfil en una tabla de referencia. - 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.

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.

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	El usuario puede realizar las siguientes acciones: - Realizar copias de seguridad y restaurar una aplicación en un archivo. - Implementar una aplicación en un servicio de integración de datos y resolver conflictos de nombres. - Iniciar una aplicación después de la implementación. - Buscar una aplicación. - Inicie o detenga objetos en una aplicación. - Configurar las propiedades de la aplicación.

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.

Privilegio del Servicio de ingesta masiva

El privilegio del servicio de ingesta masiva determina qué acciones pueden realizar los usuarios mediante la herramienta de ingesta masiva.

En la siguiente tabla se enumeran las acciones que los usuarios pueden realizar con el privilegio para el servicio de ingesta masiva:

Privilegio	Descripción
Acceso de especificación de ingesta masiva	El usuario puede realizar las acciones siguientes: - Examinar todas las especificaciones de ingesta masiva - Editar una especificación de ingesta masiva - Ejecutar una especificación de ingesta masiva - Eliminar una especificación de ingesta masiva

Nota: Un usuario que no tiene asignado el privilegio de acceso a la especificación de ingesta masiva o la función de administrador en el dominio solo puede realizar estas acciones en las especificaciones de ingesta masiva que crea el mismo usuario.

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 Metada Manager.
Cargar	Incluye privilegios para administrar objetos en la página de carga de la interfaz de Metadata Manager.

Grupos de privilegios	Descripción
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: - Ejecutar análisis de linaje de datos en objetos de metadatos, categorías y términos de negocio. - Ejecutar análisis de linaje de datos en PowerCenter Designer. Además, los usuarios deben tener permiso de lectura en la carpeta del repositorio de PowerCenter.
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: - Ver recursos y objetos de metadatos en el catálogo de metadatos. - Realizar búsquedas en el catálogo de metadatos.
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.

Privilegio	Privilegios incluidos	Permiso	Descripción
Eliminar comentarios	- Insertar comentarios - Ver comentarios	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.
Ver glosario	n/d	Lectura	El usuario puede realizar las siguientes acciones: - Ver glosarios empresariales en la vista **Glosario**. - Realizar búsquedas en glosarios de negocio.
Administrar objetos	n/d	Escritura	El usuario puede realizar las siguientes acciones: - Editar objetos de metadatos del catálogo. - Crear, editar y eliminar objetos de metadatos personalizados. Los usuarios deben tener además el privilegio Ver modelo. - Crear, editar y eliminar recursos de metadatos personalizados. Los usuarios deben tener además el privilegio Administrar recurso.

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: - Ver recursos y sus propiedades en el almacén de Metadata Manager. - Exportar configuraciones de recursos. - Descargar el programa de instalación del Agente de Metadata Manager.
Cargar recurso	Ver recursos	Escritura	El usuario puede realizar las siguientes acciones: - Cargar metadatos para un recurso en el almacén de Metadata Manager.* - Crear vínculos entre objetos en recursos conectados para linaje de datos. - Configurar indexación de búsqueda para recursos. - Importar configuraciones de recursos.
Administrar programas	Ver recursos	Escritura	El usuario puede realizar las siguientes acciones: - Crear y editar programas. - Añadir programas a los recursos.

Privilegio	Privilegios incluidos	Permiso	Descripción
Purgar metadatos	Ver recursos	Escritura	El usuario puede quitar metadatos para un recurso desde el almacén de Metadata Manager.
Administrar recursos	- Purgar metadatos - Ver recursos	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. Añada 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: - Asignar usuarios y permisos del grupo en recursos, objetos de metadatos, categorías y términos empresariales. - Editar permisos en recursos, objetos de metadatos, categorías y términos empresariales.

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 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: - Editar proyectos. - Eliminar proyectos si los ha creado el usuario. - Actualizar el contenido del Servicio de repositorio de modelos. Para actualizar el servicio mediante el menú **Acciones** 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.
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 **Administración de dominio de datos**.
Administrar notificaciones	N/A	El usuario puede configurar notificaciones de cuadro de mandos. Este privilegio forma parte del grupo de privilegios **Administración de creación de perfiles**.

Privilegio	Permiso	Descripción
Administrar desarrollo basado en equipos	N/A	El usuario puede administrar los estados de bloqueado o desbloqueado 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: - Nombre de los proyectos para los que los usuarios no tienen permiso de lectura. - Detalles de los mensajes de error y de advertencia.

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: - Conectar con el repositorio de PowerCenter mediante el administrador de repositorios. - Ejecutar comandos *pmrep*.
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: - Comparar carpetas. - Ver los objetos de las carpetas.

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: - Cambiar el estado de las carpetas. - Realizar un purgado avanzado de versiones de objetos en el nivel de carpeta.

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: - Comparar objetos de diseño. - Copiar objetos de diseño como imágenes. - Exportar objetos de diseño. - Generar código para la transformación personalizada y los procedimientos externos. - Recibir mensajes de notificación del repositorio de PowerCenter. - 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. - Buscar objetos de diseño. - Ver los objetos de diseño, las dependencias de los objetos de diseño y el historial de los objetos de diseño.
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: - Copiar objetos de diseño de una carpeta a otra. - 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.
Lectura y escritura en carpeta	El usuario puede realizar las siguientes acciones: - Cambiar comentarios para un objeto de diseño con versión. - Proteger y deshacer desprotección de objetos de diseño desprotegidos por su propia cuenta de usuario. - Desproteger objetos de diseño. - Copiar y pegar objetos de diseño en la misma carpeta. - 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. - Crear, editar y eliminar objetos de diseño. - Generar y limpiar programas SAP ABAP. - Generar asignaciones de integración de contenido de negocio. Los usuarios deben tener además el privilegio Crear, editar y eliminar orígenes y destinos. - Importar objetos de diseño mediante Designer. Los usuarios deben tener además el privilegio Crear, editar y eliminar orígenes y destinos. - 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. - Revertir a una versión anterior de los objetos de diseño. - Validar asignaciones, mapplets y funciones definidas por el usuario.

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	El usuario puede realizar las siguientes acciones: - Cambiar el estado de los objetos de diseño. - Proteger y deshacer desprotección de objetos de diseño desprotegidos por otros usuarios. - Purgar versiones de objetos de diseño. - Recuperar objetos de diseño eliminados.

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	El usuario puede realizar las siguientes acciones: - Comparar objetos de origen y destino. - Exportar objetos de origen y destino. - Obtener una vista previa de datos de origen y destino. - Recibir mensajes de notificación del repositorio de PowerCenter. - 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. - Buscar objetos de origen y destino. - Ver objetos de origen y destino, dependencias de objetos de origen y destino e historial de objetos de origen y destino.
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: - Copiar objetos de origen y destino en otra carpeta. - 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.
Lectura y escritura en carpeta	El usuario puede realizar las siguientes acciones: - Cambiar comentarios para un objeto de origen o de destino con versión. - Proteger y deshacer una desprotección de objetos de origen y destino protegidos por sus correspondientes cuentas de usuario. - Desproteger objetos de origen y destino. - Copiar y pegar objetos de origen y destino en la misma carpeta. - Crear, editar y eliminar objetos de origen y destino. - Importar funciones SAP. - Importar objetos de origen y destino mediante Designer. Los usuarios también deben contar con el privilegio Crear, editar y eliminar objetos de diseño. - 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. - Generar y ejecutar SQL para crear destinos en una base de datos relacional. - Revertir a una versión anterior de un objeto de origen o de destino.

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	El usuario puede realizar las siguientes acciones: - Cambiar el estado de objetos de origen y destino. - Proteger y deshacer la protección de objetos de origen y destino desprotegidos por otros usuarios. - Purgar versiones de objetos de origen y destino. - Recuperar objetos de origen y destino.

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	El usuario puede realizar las siguientes acciones: - Comparar objetos en tiempo de ejecución. - Exportar objetos en tiempo de ejecución. - Recibir mensajes de notificación del repositorio de PowerCenter. - Buscar objetos en tiempo de ejecución. - Usar las variables y los parámetros de asignación en una sesión. - Ver objetos en tiempo de ejecución, las dependencias del objeto y el historial del objeto en tiempo de ejecución.
Lectura y ejecución en carpeta	Detener y anular tareas y flujos de trabajo iniciados por la cuenta de usuario propia. 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.

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: - Copiar tareas, flujos de trabajo o worklets de una carpeta a otra. - 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.
Lectura y escritura en carpeta	El usuario puede realizar las siguientes acciones: - Asignar un servicio de integración de PowerCenter a un flujo de trabajo en las propiedades del flujo de trabajo. - Asignar un nivel de servicio a un flujo de trabajo. - Cambiar comentarios para un objeto en tiempo de ejecución con versión. - Proteger y anular la desprotección de los objetos en tiempo de ejecución desprotegidos por la cuenta de usuario propia. - Desproteger los objetos en tiempo de ejecución. - Copiar y pegar tareas, flujos de trabajo y worklets en la misma carpeta. - 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. - Crear, editar y eliminar objetos de configuración de sesión. - Eliminar y validar tareas, flujos de trabajo y worklets. - 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. - Importar objetos en tiempo de ejecución con el administrador de flujos de trabajo. - Revertir a una versión de objeto anterior.
Lectura y escritura en carpeta Lectura en objeto de conexión	El usuario puede realizar las siguientes acciones: - Eliminar y editar tareas, flujos de trabajo y worklets. - Reemplazar una conexión de base de datos relacional para todas las sesiones que usan la conexión.

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	El usuario puede realizar las siguientes acciones: - Cambiar el estado de los objetos en tiempo de ejecución. - Proteger y anular la desprotección de los objetos en tiempo de ejecución desprotegidos por otros usuarios. - Purgar versiones de objetos en tiempo de ejecución. - Recuperar objetos eliminados en tiempo de ejecución.

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	El usuario puede realizar las siguientes acciones: - Ver propiedades de los objetos en tiempo de ejecución en el supervisor de flujo de trabajo. - Ver los registros de sesión y de flujo de trabajo en el supervisor de flujo de trabajo. - Ver los detalles del objeto en tiempo de ejecución y del rendimiento en el supervisor de flujo de trabajo. 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 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	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. 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	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: - Iniciar, iniciar en frío y reiniciar tareas y flujos de trabajo. - Recuperar tareas y flujos de trabajo iniciados por la cuenta de usuario propia. 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: - Detener y anular tareas y flujos de trabajo iniciados por otros usuarios. - Detener y anular tareas que se recuperaron automáticamente. - Anular la programación de flujos de trabajo. 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	El usuario puede realizar las siguientes acciones: - Recuperar tareas y flujos de trabajo iniciados por otros usuarios. - Recuperar tareas que se recuperaron automáticamente. 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.
Lectura, escritura y ejecución en carpeta Lectura y ejecución en objeto de conexión	El usuario puede realizar las siguientes acciones: - Crear y editar un programador reutilizable desde el menú Flujos de trabajo > Programadores. - Editar un programador no reutilizable desde las propiedades del flujo de trabajo. - 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. 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.

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: - Editar grupos de implementación. - Quitar objetos de un grupo de implementación.
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.	- Servicio de programador - El servicio de integración de datos que ejecuta las tareas que el usuario desea programar
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.	- Servicio de programador - El servicio de integración de datos que ejecuta las tareas que el usuario desea programar
Eliminar programa	El usuario puede eliminar programas.	Servicio de programador
Ver programas	El usuario puede acceder a la vista **Programaciones** 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 llevar a cabo mediante Test Data Manager. Configure privilegios en la ficha **Seguridad** de la Herramienta del administrador.

La siguiente tabla describe cada grupo de privilegios de Test Data Manager.

Grupo de privilegios	Descripción
Administración	Incluye los privilegios para crear y administrar conexiones, frases de contraseña y funciones; para asignar privilegios a usuarios y grupos de usuarios de Informatica Administrator; para administrar repositorios; para añadir licencias, y para configurar atributos de flujo de trabajo y proyecto. **Nota:** 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.
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.

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:

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: - Crear conexiones. - Editar conexiones. - Eliminar conexiones. - Ver conexiones. - Probar conexiones.

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: - Crear dominios de datos. - Editar dominios de datos. - Eliminar dominios de datos. - Ver dominios de datos.

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: - Añadir asignaciones de reglas y directivas. - Eliminar asignaciones de reglas y directivas. - Reemplazar propiedades de reglas. - Ver asignaciones de enmascaramiento de datos.

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:

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: - Crear directivas. - Editar directivas. - Eliminar directivas. - Ver directivas.

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:
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.

Grupo de privilegios Reglas

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:

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: - Ver asignaciones de reglas de generación de datos - Añadir asignaciones de reglas de generación de datos. - Eliminar asignaciones de reglas de generación de datos. - Reemplazar asignaciones de reglas de generación de datos.

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.

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 aquélla 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 ingesta masiva, 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.

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.

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.

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, el servicio de ingesta masiva y el servicio de repositorio de PowerCenter:

Servicio	Tareas
Dominio	- Configurar las propiedades del dominio. - Determinar las configuraciones de clúster. - Crear los perfiles del sistema operativo. - Eliminar los perfiles del sistema operativo. - Conceder permiso sobre el dominio y los perfiles del sistema operativo. - 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.
Servicio de integración de datos	- Actualizar el servicio de integración de datos mediante el menú Acciones.
Servicio de ingesta masiva	- Examinar todas las especificaciones de ingesta masiva. - Editar una especificación de ingesta masiva. - Ejecutar una especificación de ingesta masiva. - Eliminar una especificación de ingesta masiva.
Servicio de repositorio de PowerCenter	- Asignar perfiles del sistema operativo a carpetas del repositorio si el servicio de integración de PowerCenter utiliza perfiles de sistema operativo.* - Cambiar el propietario de las carpetas y de los objetos globales.* - Configurar permisos de carpeta y objeto global.* - Conectarse al servicio de integración de PowerCenter desde el cliente de PowerCenter al ejecutar el servicio de integración de PowerCenter en modo seguro. - Eliminar un servicio de integración de PowerCenter desde el navegador del administrador de flujos de trabajo. - Eliminar carpetas y objetos globales.* - Designar carpetas para compartirlas.* - Editar el nombre y la descripción de las carpetas.* *El propietario del objeto global o de la carpeta del repositorio de PowerCenter también pueden realizar estas tareas.

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

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:

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.

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.

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.

Tipo de objeto de dominio	Descripción del permiso
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 Informatica 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.

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 la Herramienta del administrador, haga clic en la ficha **Seguridad**.
2. Haga clic en la ficha **Grupos** o en la ficha **Usuarios**.
3. Seleccione un usuario o grupo.
4. Haga clic en la ficha **Permisos**.

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.

Para ver si el permiso se ha asignado directamente o es heredado, haga clic en **Ver detalles del permiso**. Si revoca un permiso en un objeto, el usuario o grupo aún podrá heredar el permiso de un grupo u objeto primario.

1. En la Herramienta del administrador, haga clic en la ficha **Seguridad**.
2. Haga clic en la ficha **Grupos** o en la ficha **Usuarios**.
3. Seleccione un usuario o grupo.
4. Haga clic en la ficha **Permisos**.
5. Seleccione un objeto de dominio y después haga clic en **Editar permisos directos**.
6. Para asignar un permiso en el objeto, seleccione **Permitir**.
7. Para revocar permisos en el objeto, seleccione **Revocar**.
8. Haga clic en **Aceptar**.

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.

Asignar permisos en un perfil del sistema operativo

Al asignar permisos en un perfil del sistema operativo, los usuarios de Informatica ejecutan asignaciones, perfiles y flujos de trabajo con dicho perfil. Los usuarios de PowerCenter ejecutan los flujos de trabajo asignados al perfil del sistema operativo.

1. En la Herramienta del administrador, haga clic en la ficha **Seguridad**.
2. Haga clic en la ficha **Perfiles del sistema operativo**.
3. Seleccione el perfil del sistema operativo y después haga clic en la ficha **Permisos**.
4. Haga clic en la ficha **Grupos** o la ficha **Usuarios** y después seleccione **Editar permisos directos**.
5. Seleccione un objeto de dominio y después haga clic en **Editar permisos directos**.
6. Para asignar un permiso en el objeto, seleccione **Permitir**.
7. Para revocar permisos en el objeto, seleccione **Revocar**.
8. Haga clic en **Aceptar**.

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.

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.

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
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.	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.

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. 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.
6. Haga clic en **Cerrar**
7. 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 configuración del clúster

Los permisos controlan el nivel de acceso que un usuario o grupo tiene en la configuración de un clúster.

Los permisos de configuración de un clúster se pueden determinar en Administrator tool y en la interfaz de la línea de comandos de Informatica.

Un usuario o un grupo pueden tener los siguientes permisos para configurar un clúster:

- Lectura. Los miembros del usuario o el grupo pueden ver la configuración del clúster.
- Escritura. Los miembros del usuario o el grupo pueden editar la configuración del clúster. Incluye el permiso de lectura.
- Ejecución. Los miembros del usuario o el grupo pueden ejecutar asignaciones en el entorno de Hadoop.
- Concesión. Los miembros del usuario o el grupo pueden conceder permiso para la configuración del clúster a otros usuarios y grupos. Incluye el permiso de lectura.
- Todos. El usuario hereda todos los permisos admitidos.

De forma predeterminada, todos los usuarios tienen permiso para ver el nombre de la configuración del clúster.

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**
9. 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.

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 u objeto de aplicación.
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**.

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 Informatica (Informatica How-To Library): 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 consulte 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

Utilice los informes de auditoría para ver información sobre los usuarios y los grupos del dominio de Informatica, 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

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 infacmd as	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 cluster

Para poder ejecutar comandos *infacmd cluster*, los usuarios deben tener uno de los conjuntos enumerados de privilegios del dominio y permisos de configuración del clúster.

La siguiente tabla enumera los privilegios y los permisos necesarios para los comandos *infacmd cluster*:

Comando infacmd cluster	Grupo de privilegios	Nombre de privilegio	Permiso de...
clearConfigurationProperties	Administración de dominios	Administrar conexiones	Escribir en la configuración del clúster
createConfiguration	Administración de dominios	Administrar conexiones	Escribir en configuraciones de clúster
deleteConfiguration	Administración de dominios	Administrar conexiones	Escribir en configuraciones de clúster
exportConfiguration con propiedades confidenciales	-	-	Escribir en la configuración del clúster

Comando infacmd cluster	Grupo de privilegios	Nombre de privilegio	Permiso de...
exportConfiguration sin propiedades confidenciales	-	-	Leer en configuraciones de clúster
listAssociatedConnections	-	-	-
listConfigurations	-	-	-
listConfigurationGroupPermissions	-	-	-
listConfigurationProperties	-	-	Leer en configuraciones de clúster
listConfigurationSets	-	-	Leer en configuraciones de clúster
listConfigurationUserPermissions	-	-	-
refreshConfiguration	Administración de dominios	Administrar conexiones	Escribir en configuraciones de clúster
setConfigurationPermissions	-	-	Concesión en configuración del clúster
setConfigurationProperties	Administración de dominios	Administrar conexiones	Escribir en configuraciones de clúster

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 infacmd dis	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

Comando de infacmd dis	Grupo de privilegios	Nombre de privilegio	Permiso de...
DeployApplication	Administración de la aplicación	Administrar aplicaciones	Aplicación
ListApplicationObjects	-	-	-
ListApplications	-	-	-
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

Comando de infacmd dis	Grupo de privilegios	Nombre de privilegio	Permiso de...
UpdateServiceOptions	Administración de dominios	Gestionar servicios	Servicio de integración de datos
UpdateServiceProcessOptions	Administración de dominios	Gestionar servicios	Servicio de integración de datos

Comandos infacmd dp

Los usuarios deben ser usuarios nativos o tener asignada la función de administrador para poder ejecutar los siguientes comandos infacmd dp:

- startSparkJobServer
- stopSparkJobServer

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.

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
AddAlertUser (para otros usuarios)	Administración de seguridad	Gestionar usuarios, grupos y roles	-
AddAlertUser (para su cuenta de usuario)	-	-	-
AddConnectionPermissions	-	-	Conceder al conectar
AddDomainLink*	-	-	-
AddDomainNode	Administración de dominios	Administrar nodos y mallas	Dominio y nodo
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 principal
AddNodeResource	Administración de dominios	Administrar nodos y mallas	Nodo
AddRolePrivilege	Administración de seguridad	Gestionar usuarios, grupos y roles	-
AddServiceLevel*	-	-	-
AddUserToGroup	Administración de seguridad	Gestionar usuarios, grupos y roles	-
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

Comando infacmd isp	Grupo de privilegios	Nombre del privilegio	Permiso en
AssignGroupPermission (en perfiles del sistema operativo)*	-	-	-
AssignISTOMMService	Administración de dominios	Gestionar servicios	Servicio de Metadata Manager
AssignLicense	Administración de dominios	Gestionar servicios	Objeto de licencia y servicio de aplicación
AssignRSToWSHubService	Administración de dominios	Gestionar servicios	Servicio de repositorio de PowerCenter y concentrador de servicios web
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.
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.
AssignedToLicense	Administración de dominios	Gestionar servicios	Objeto de licencia y servicio de aplicación
ConvertLogFile	-	-	Servicio de aplicación o dominio

Comando infacmd isp	Grupo de privilegios	Nombre del privilegio	Permiso en
CreateConnection*	-	-	-
CreateFolder	Administración de dominios	Administrar carpetas del dominio	Dominio o carpeta principal
CreateGrid	Administración de dominios	Administrar nodos y mallas	Dominio o carpeta principal 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 principal donde se ejecuta el servicio de integración de PowerCenter, objeto de licencia y servicio de repositorio de PowerCenter asociado
CreateMMService	Administración de dominios	Gestionar servicios	Dominio, carpeta o nodo principal 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 principal 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	-

Comando infacmd isp	Grupo de privilegios	Nombre del privilegio	Permiso en
CreateWSHubService	Administración de dominios	Gestionar servicios	Dominio, malla, carpeta o nodo principal 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
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 conexiones)	Administración de dominios	Administrar conexiones	Leer al conectar

Comando infacmd isp	Grupo de privilegios	Nombre del privilegio	Permiso en
ExportDomainObjects (para usuarios, grupos y funciones)	Administración de seguridad	Gestionar usuarios, grupos y roles	-
ExportUsersAndGroups	Administración de seguridad	Gestionar usuarios, grupos y roles	-
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 conexiones)	Administración de dominios	Administrar conexiones	Escribir al conectar
ImportDomainObjects (para usuarios, grupos y funciones)	Administración de seguridad	Gestionar usuarios, grupos y roles	-
ImportUsersAndGroups	Administración de seguridad	Gestionar usuarios, grupos y roles	-
ListAlertUsers	-	-	Dominio
ListAllGroups	-	-	-
ListAllRoles	-	-	-
ListAllUsers	-	-	-
ListConnectionOptions	-	-	Leer al conectar
ListConnectionPermissions	-	-	-
ListConnectionPermissions por grupo	-	-	-

Comando infacmd isp	Grupo de privilegios	Nombre del privilegio	Permiso en
ListConnectionPermissions por usuario	-	-	-
ListConnections	-	-	-
ListDomainLinks	-	-	Dominio
ListDomainOptions	-	-	Dominio
ListFolders	-	-	Carpetas
ListGridNodes	-	-	-
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.
ListGroupsForUser	-	-	Dominio
ListLDAPConnectivity	Administración de seguridad	Gestionar usuarios, grupos y roles	-
ListLicenses	-	-	Objetos de licencia
ListNodeOptions	-	-	Nodo
ListNodeResources	-	-	Nodo
ListNodes	-	-	-
ListPlugins	-	-	-
ListRepositoryLDAPConfiguration	-	-	Dominio
ListRolePrivileges	-	-	-
ListSMTPOptions	-	-	Dominio
ListSecurityDomains	Administración de seguridad	Gestionar usuarios, grupos y roles	-
ListServiceLevels	-	-	Dominio
ListServiceNodes	-	-	Servicio de aplicación
ListServicePrivileges	-	-	-
ListServices	-	-	-

Comando infacmd isp	Grupo de privilegios	Nombre del privilegio	Permiso en
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*	-	-	-
RemoveAlertUser (para otros usuarios)	Administración de seguridad	Gestionar usuarios, grupos y roles	-
RemoveAlertUser (para su cuenta de usuario)	-	-	-
RemoveConnection	-	-	Escribir al conectar
RemoveConnectionPermissions	-	-	Conceder al conectar
RemoveDomainLink*	-	-	-
RemoveFolder	Administración de dominios	Administrar carpetas del dominio	Dominio o carpeta principal y carpeta que se va a quitar
RemoveGrid	Administración de dominios	Administrar nodos y mallas	Dominio o carpeta y malla principal
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 principal y objeto de licencia

Comando infacmd isp	Grupo de privilegios	Nombre del privilegio	Permiso en
RemoveNode	Administración de dominios	Administrar nodos y mallas	Dominio o carpeta y nodo principal
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 principal y servicio de aplicación
RemoveServiceLevel*	-	-	-
RemoveUser	Administración de seguridad	Gestionar usuarios, grupos y roles	-
RemoveUserFromGroup	Administración de seguridad	Gestionar usuarios, grupos y roles	-
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 otros usuarios)	Administración de seguridad	Gestionar usuarios, grupos y roles	-
ResetPassword (para su cuenta de usuario)	-	-	-
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

Comando infacmd isp	Grupo de privilegios	Nombre del privilegio	Permiso en
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
UnAssignRoleFromGroup	Administración de seguridad	Conceder privilegios y roles	Dominio, servicio de Metadata Manager, servicio de repositorio de modelos o servicio de repositorio de PowerCenter.
UnAssignRoleFromUser	Administración de seguridad	Conceder privilegios y roles	Dominio, servicio de Metadata Manager, servicio de repositorio de modelos o servicio de repositorio de PowerCenter.
UnassignLicense	Administración de dominios	Gestionar servicios	Objeto de licencia y servicio de aplicación
UnassignRSWSHubService	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

Comando infacmd isp	Grupo de privilegios	Nombre del privilegio	Permiso en
UpdateMMService	Administración de dominios	Gestionar servicios	Servicio de Metadata Manager
UpdateNodeOptions	Administración de dominios	Administrar nodos y mallas	Nodo
UpdateNodeRole	Administración de dominios	Administrar nodos y mallas	Nodo
UpdateOSProfile	Administración de seguridad	Gestionar usuarios, grupos y roles	Perfil del sistema operativo
UpdateRepositoryService	Administración de dominios	Gestionar servicios	Servicio de repositorio de PowerCenter
UpdateSAPBWService	Administración de dominios	Gestionar servicios	Servicio SAP BW
UpdateSMTPOptions*	-	-	-
UpdateServiceLevel*	-	-	-
UpdateServiceProcess	Administración de dominios	Gestionar servicios	Servicio de integración de PowerCenter Cada nodo añadido al servicio de integración de PowerCenter
UpdateWSHubService	Administración de dominios	Gestionar servicios	concentrador de servicios web
generateHadoopConnectionFromHiveConection	-	-	-
listMonitoringOptions	Supervisión	Configuración de supervisión	Dominio
purgeMonitoringData	Supervisión	Configuración de supervisión	Dominio
updateMonitoringOptions	Supervisión	Configuración de supervisión	Dominio
** Para ejecutar estos comandos, los usuarios deben tener asignada la función de administrador en el dominio.*			

Comandos infacmd mas

Para ejecutar los comandos *infacmd mas*, los usuarios deben tener uno de los conjuntos de privilegios del dominio indicados, privilegios del servicio de acceso a metadatos y permisos del objeto de dominio.

La siguiente tabla enumera los privilegios y los permisos necesarios para los comandos *infacmd mas*:

Comando de infacmd dis	Grupo de privilegios	Nombre de privilegio	Permiso de...
CreateService	Administración de dominios	Gestionar servicios	Dominio o nodo donde se ejecuta el servicio de acceso a metadatos
ListServiceOptions	Administración de dominios	Gestionar servicios	Servicio de acceso a metadatos
ListServiceProcessOptions	Administración de dominios	Gestionar servicios	Servicio de acceso a metadatos
UpdateServiceOptions	Administración de dominios	Gestionar servicios	Servicio de acceso a metadatos
UpdateServiceProcessOptions	Administración de dominios	Gestionar servicios	Servicio de acceso a metadatos

Comandos infacmd mi

Los usuarios deben tener asignada la función de administrador en el servicio de ingesta masiva para ejecutar los siguientes comandos infacmd mi:

- clearSamlConfig
- updateSamlConfig

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 infacmd mrs	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...
deleteMappingPersistedOutputs	-	-	Ejecución en la aplicación
getRequestLog	-	-	-
listMappingParams	-	-	-
listMappingPersistedOutputs	-	-	Visualización en una aplicación
listMappings	-	-	-
runMapping	-	-	Ejecución de objetos de conexión usados por la asignación

Comandos infacmd tools

Para ejecutar comandos *infacmd tools*, 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 tools*:

Comando infacmd tools	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	-	-	-
Ejecución	-	-	Lectura en proyecto Ejecución en el objeto de conexión de origen
List	-	-	Lectura en proyecto
Purge	-	-	Lectura y escritura en proyecto

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	-
DisplayEventsLogger	Comandos informativos	displayevents	-

Comando infacmd pwx	Grupo de privilegios	Nombre de privilegio	Permiso de...
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
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
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

Comando infacmd sch	Grupo de privilegios	Nombre del privilegio	Permiso en
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	-	-	-
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

Comando infacmd sql	Grupo de privilegios	Nombre de privilegio	Permiso de...
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	-	-	-
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)

Comando pmcmd	Grupo de privilegios	Nombre de privilegio	Permiso
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
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
- CreateQuery
- DeleteConnection
- DeleteDeploymentGroup
- DeleteFolder
- DeleteLabel
- DeleteQuery
- 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	Administrar 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	Gestionar servicios	Permiso para el servicio de repositorio de PowerCenter
ChangeOwner	-	-	-
CheckIn (para las desprotecciones propias)	Objetos de diseño	Crear, editar y eliminar	Lectura y escritura en carpeta

Comando pmrep	Grupo de privilegios	Nombre de privilegio	Permiso
CheckIn (para las desprotecciones propias)	Orígenes y destinos	Crear, editar y eliminar	Lectura y escritura en carpeta
CheckIn (para las desprotecciones propias)	Objetos en tiempo de ejecución	Crear, editar y eliminar	Lectura y escritura en carpeta
CheckIn (para las desprotecciones de otros)	Objetos de diseño	Administrar versiones	Lectura y escritura en carpeta
CheckIn (para las desprotecciones de otros)	Orígenes y destinos	Administrar versiones	Lectura y escritura en carpeta
CheckIn (para las desprotecciones de otros)	Objetos en tiempo de ejecución	Administrar versiones	Lectura y escritura en carpeta
CleanUp	-	-	-
ClearDeploymentGroup	Objetos globales	Administrar grupos de implementación	Lectura y escritura en grupo de implementación
Connect	-	-	-
Crear	Administración de dominios	Gestionar servicios	Permiso para el servicio de repositorio de PowerCenter
CreateConnection	Objetos globales	Crear conexiones	-
CreateDeploymentGroup	Objetos globales	Administrar grupos de implementación	-
CreateFolder	Carpetas	Crear	-
CreateLabel	Objetos globales	Crear etiquetas	-
CreateQuery	Objetos globales	Crear consultas	-
Eliminar	Administración de dominios	Gestionar servicios	Permiso para el servicio de repositorio de PowerCenter
DeleteConnection	-	-	-
DeleteDeploymentGroup	-	-	-
DeleteFolder	-	-	-
DeleteLabel	-	-	-
DeleteObject	Objetos de diseño	Crear, editar y eliminar	Lectura y escritura en carpeta
DeleteObject	Orígenes y destinos	Crear, editar y eliminar	Lectura y escritura en carpeta
DeleteObject	Objetos en tiempo de ejecución	Crear, editar y eliminar	Lectura y escritura en carpeta
DeleteQuery	-	-	-

Comando pmrep	Grupo de privilegios	Nombre de privilegio	Permiso
DeployDeploymentGroup	Objetos globales	Administrar 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	Gestionar 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	Gestionar servicios	Permiso para el servicio de repositorio de PowerCenter
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	Administrar versiones	Lectura y escritura en carpeta
Notificar	Administración de dominios	Gestionar servicios	Permiso para el servicio de repositorio de PowerCenter
ObjectExport	-	-	Lectura en carpeta
ObjectImport	Objetos de diseño	Crear, editar y eliminar	Lectura y escritura en carpeta
ObjectImport	Orígenes y destinos	Crear, editar y eliminar	Lectura y escritura en carpeta

Comando pmrep	Grupo de privilegios	Nombre de privilegio	Permiso
ObjectImport	Objetos en tiempo de ejecución	Crear, editar y eliminar	Lectura y escritura en carpeta
PurgeVersion	Objetos de diseño	Administrar versiones	Lectura y escritura en carpeta Lectura, escritura y ejecución en consulta si se especifica un nombre de consulta
PurgeVersion	Orígenes y destinos	Administrar versiones	Lectura y escritura en carpeta Lectura, escritura y ejecución en consulta si se especifica un nombre de consulta
PurgeVersion	Objetos en tiempo de ejecución	Administrar 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	Administrar versiones	Lectura y escritura en carpeta
PurgeVersion (para purgar objetos en el nivel del repositorio)	Administración de dominios	Gestionar servicios	Permiso para el servicio de repositorio de PowerCenter
Register	Administración de dominios	Gestionar servicios	Permiso para el servicio de repositorio de PowerCenter
RegisterPlugin	Administración de dominios	Gestionar servicios	Permiso para el servicio de repositorio de PowerCenter
Restore	Administración de dominios	Gestionar servicios	Permiso para el servicio de repositorio de PowerCenter
RollbackDeployment	Objetos globales	Administrar grupos de implementación	Lectura y escritura en carpeta de destino
Run	-	-	-
ShowConnectionInfo	-	-	-
SwitchConnection	Objetos en tiempo de ejecución	Crear, editar y eliminar	Lectura y escritura en carpeta Lectura en objeto de conexión
TruncateLog	Objetos en tiempo de ejecución	Administrar ejecución	Lectura y ejecución en carpeta
UndoCheckout (para las desprotecciones propias)	Objetos de diseño	Crear, editar y eliminar	Lectura y escritura en carpeta
UndoCheckout (para las desprotecciones propias)	Orígenes y destinos	Crear, editar y eliminar	Lectura y escritura en carpeta

Comando pmrep	Grupo de privilegios	Nombre de privilegio	Permiso
UndoCheckout (para las desprotecciones propias)	Objetos en tiempo de ejecución	Crear, editar y eliminar	Lectura y escritura en carpeta
UndoCheckout (para las desprotecciones de otros)	Objetos de diseño	Administrar versiones	Lectura y escritura en carpeta
UndoCheckout (para las desprotecciones de otros)	Orígenes y destinos	Administrar versiones	Lectura y escritura en carpeta
UndoCheckout (para las desprotecciones de otros)	Objetos en tiempo de ejecución	Administrar versiones	Lectura y escritura en carpeta
Unregister	Administración de dominios	Gestionar servicios	Permiso para el servicio de repositorio de PowerCenter
UnregisterPlugin	Administración de dominios	Gestionar servicios	Permiso para el servicio de repositorio de PowerCenter
UpdateConnection	-	-	Lectura y escritura en objeto de conexión
UpdateEmailAddr	Objetos en tiempo de ejecución	Crear, editar y eliminar	Lectura y escritura en carpeta
UpdateSeqGenVals	Objetos de diseño	Crear, editar y eliminar	Lectura y escritura en carpeta
UpdateSrcPrefix	Objetos en tiempo de ejecución	Crear, editar y eliminar	Lectura y escritura en carpeta
UpdateStatistics	Administración de dominios	Gestionar servicios	Permiso para el servicio de repositorio de PowerCenter
UpdateTargPrefix	Objetos en tiempo de ejecución	Crear, editar y eliminar	Lectura y escritura en carpeta
Upgrade	Administración de dominios	Gestionar servicios	Permiso para el servicio de repositorio de PowerCenter
Validate	Objetos de diseño	Crear, editar y eliminar	Lectura y escritura en carpeta
Validate	Objetos en tiempo de ejecución	Crear, editar y eliminar	Lectura y escritura en carpeta
Version	-	-	-

APÉNDICE B

Funciones personalizadas

Este apéndice incluye los siguientes temas:

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	- Compartir accesos directos - Ver linaje - Ver catálogos relacionados - Ver informes - Ver resultados de perfil - Ver catálogo - Ver relaciones - Administrar relaciones - Ver comentarios - Insertar comentarios - Eliminar comentarios - Ver vínculos - Administrar vínculos - Ver glosario - Administrar objetos
Cargar	- Ver recurso - Cargar recurso - Administrar programas - Purgar metadatos - Administrar recursos
Modelo	- Ver modelo - Administrar modelo - Exportar/Importar modelos
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	- Ver linaje - Ver catálogos relacionados - Ver catálogo - Ver relaciones - Ver comentarios - Ver vínculos
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	- Ver linaje - Ver catálogos relacionados - Ver informes - Ver resultados de perfil - Ver catálogo - Ver relaciones - Ver comentarios - Insertar comentarios - Eliminar comentarios - Ver vínculos - Administrar vínculos - Ver glosario
Cargar	- Ver recurso - Cargar recurso
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	El grupo de privilegios Supervisión incluye los siguientes privilegios: - Ver: Ver trabajos de otros usuarios - Ver: Ver estadísticas - Ver: Ver informes - Acceder a la supervisión: Acceso desde la Herramienta del analista - Acceder a la supervisión: Acceso desde Developer tool - Acceder a la supervisión: Acceso desde la herramienta Administrator - Realizar acciones en tareas **Nota:** 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.
Programador	El grupo de privilegios Programador incluye los siguientes privilegios: - Administrar trabajos programados: Crear programa - Administrar trabajos programados: Eliminar programa - Administrar trabajos programados: Editar programa - Administrar los trabajos programados: Ver programas
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	- Acceso a Designer - Acceso al administrador de flujos de trabajo - Acceso al supervisor de flujos de trabajo
Objetos de diseño	- Crear, editar y eliminar - Administrar versiones
Orígenes y destinos	- Crear, editar y eliminar - Administrar versiones
Objetos en tiempo de ejecución	- Crear, editar y eliminar - Ejecutar - Administrar versiones - Supervisar

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	- Ejecutar - Administrar ejecución - Supervisar

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	- Copiar - Crear - Administrar versiones
Objetos globales	- Administrar grupos de implementación - Ejecutar grupos de implementación - Crear etiquetas - Crear consultas

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	- Ver conexiones - Administrar conexiones - Administrar preferencias

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	- Ver directivas - Administrar directivas
Dominios de datos	- Ver dominios de datos - Administrar dominios de datos
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	- Ver proyecto - Ejecutar proyecto - Supervisar proyecto - Auditar proyecto
Administración	- Ver conexiones - Administrar conexiones

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
Dominios de datos	Ver dominios de datos
Proyectos	- Ver proyecto - Detectar proyecto - Ejecutar proyecto - Supervisar proyecto - Auditar proyecto - Importar metadatos
Enmascaramiento de datos	- Ver enmascaramiento de datos - Administrar enmascaramiento de datos
Subconjunto de datos	- Ver subconjuntos de datos - Administrar subconjuntos de datos
Administración	- Ver conexiones - Administrar conexiones

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
Dominios de datos	Ver dominios de datos
Proyectos	- Ver proyecto - Administrar proyecto - Detectar proyecto - Ejecutar proyecto - Supervisar proyecto - Auditar proyecto - Importar metadatos
Enmascaramiento de datos	- Ver enmascaramiento de datos - Administrar enmascaramiento de datos
Subconjunto de datos	- Ver subconjuntos de datos - Administrar subconjuntos de datos
Administración	- Ver conexiones - Administrar conexiones

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
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
Dominios de datos	- Ver dominios de datos - Administrar dominios de datos
Proyectos	- Ver proyecto - Administrar proyecto - Detectar proyecto - Ejecutar proyecto - Supervisar proyecto - Auditar proyecto - Importar metadatos
Enmascaramiento de datos	- Ver enmascaramiento de datos - Administrar enmascaramiento de datos
Subconjunto de datos	- Ver subconjuntos de datos - Administrar subconjuntos de datos
Administración	- Ver conexiones - Administrar conexiones

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	- Ver proyecto - Supervisar proyecto

INDICE

A

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W