IBM Security Directory Server
Versión 6.3.1.5

Guía de instalación y configuración

SC11-7875-02

IBM Security Directory Server
Versión 6.3.1.5

Guía de instalación y configuración

SC11-7875-02

Nota

Antes de utilizar esta información y el producto al que da soporte, lea la información general del apartado “Avisos” en la página 271.

Nota de edición

Nota: Esta edición se aplica a la versión 6.3.1.5 de *IBM Security Directory Server* **(número de producto 5724-J39) y a todos los releases y modificaciones posteriores hasta que se indique lo contrario en nuevas ediciones.**

Contenido

Acerca de esta publicación

IBM® Security Directory Server, anteriormente conocido como IBM Tivoli Directory Server, es una implementación de IBM de Lightweight Directory Access Protocol para los siguientes sistemas operativos:

- Microsoft Windows
- AIX
- Linux (System x, System z, System p, y System i)
- Solaris
- Hewlett-Packard UNIX (HP-UX) (Itanium)

La *Guía de instalación y configuración de IBM Security Directory Server,* contiene información para la instalación, configuración y desinstalación de IBM Security Directory Server. También incluye información sobre cómo actualizar desde una versión anterior.

Acceso a publicaciones y terminología

En esta sección se proporciona:

- Una lista de publicaciones de la "Biblioteca de IBM Security Directory Server".
- Enlaces a "Publicaciones en línea" en la página x.
- Un enlace a la "Sitio web de terminología de IBM" en la página xi.

Biblioteca de IBM Security Directory Server

Los siguientes documentos están disponibles en la biblioteca de IBM Security Directory Server:

- *IBM Security Directory Server, Versión 6.3.1.5 Visión general del producto*, GC43-1261-01

  Proporciona información sobre el producto IBM Security Directory Server, nuevas características en el release actual, e información de requisitos del sistema.
- *IBM Security Directory Server, Versión 6.3.1.5 Guía de inicio rápido*, GC43-1262-02

  Proporciona ayuda de iniciación con IBM Security Directory Server. Incluye una breve descripción del producto y diagrama de arquitectura, y un puntero al sitio web de documentación del producto y a las instrucciones de instalación.
- *IBM Security Directory Server, Versión 6.3.1.5 Guía de instalación y configuración*, SC11-7875-02

  Contiene información completa para instalar, configurar y desinstalar IBM Security Directory Server. Incluye información sobre la actualización desde una versión anterior de IBM Security Directory Server.
- *IBM Security Directory Server, Versión 6.3.1.5 Guía de administración*, SC27-2749-02

  Contiene instrucciones para las tareas de administración mediante la Herramienta de administración web y la línea de mandatos.
- *IBM Security Directory Server, Versión 6.3.1.5 Guía de creación de informes*, SC27-6531-00

Describe las herramientas y el software para crear informes para IBM Security Directory Server.

- *IBM Security Directory Server, Versión 6.3.1.5 Consulta de mandatos*, SC27-2753-02

  Describe la sintaxis y el uso de los programas de utilidad de la línea de mandatos incluidos en IBM Security Directory Server.

- *IBM Security Directory Server, Versión 6.3.1.5 Consulta de plugins de servidor*, SC27-2750-02

  Contiene información acerca de cómo crear conectores del servidor.

- *IBM Security Directory Server, Versión 6.3.1.5 Consulta de programación*, SC27-2754-02

  Contiene información acerca de cómo crear aplicaciones cliente de LDAP (Lightweight Directory Access Protocol) en C y en Java™.

- *IBM Security Directory Server, Versión 6.3.1.5 Guía de ajuste de rendimiento y planificación de capacidad*, SC27-2748-02

  Contiene información detallada acerca de cómo ajustar el servidor de directorios para obtener un mejor rendimiento. Describe los requisitos de disco y otros requisitos de hardware para directorios de distintos tamaños y con distintas velocidades de lectura y escritura. Describe casos de ejemplo de trabajo conocidos para cada uno de estos niveles de directorio y el disco y memoria utilizados; también sugiere reglas generales.

- *IBM Security Directory Server, Versión 6.3.1.5 Guía de resolución de problemas*, GC27-2752-02

  Contiene información sobre posibles problemas y acciones correctoras que se pueden llevar a cabo antes de ponerse en contacto con el servicio de soporte de software de IBM.

- *IBM Security Directory Server, Versión 6.3.1.5 Consulta de mensajes de error*, GC27-2751-02

  Contiene una lista de todos los avisos y mensajes de error asociados a IBM Security Directory Server.

Publicaciones en línea

IBM coloca publicaciones de productos cuando se lanza el producto y cuando se actualizan las publicaciones en las siguientes ubicaciones:

Sitio web de documentación de IBM Security Directory Server
El sitio http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/welcome.htm muestra la página de bienvenida de la documentación para este producto.

Central de documentación y página de bienvenida de IBM Security Systems
Central de documentación de IBM Security Systems proporciona una lista alfabética de toda la documentación del producto IBM Security Systems. También puede encontrar enlaces a la documentación del producto para versiones específicas de cada producto.

Bienvenida a la documentación de IBM Security Systems proporciona una introducción, enlaces, e información general sobre documentación de IBM Security Systems.

IBM Publications Center
El sitio http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss ofrece funciones de búsqueda personalizadas para ayudarle a encontrar todas las publicaciones de IBM que necesita.

Sitio web de terminología de IBM

El sitio web de terminología de IBM consolida terminología para las bibliotecas de productos en una ubicación. Puede acceder al sitio web de Terminología en http://www.ibm.com/software/globalization/terminology.

Accesibilidad

Las características de accesibilidad proporcionan ayuda a los usuarios con discapacidades físicas, tales como movilidad restringida o visión limitada, para que puedan utilizar los productos de software satisfactoriamente. Con este producto, puede utilizar tecnologías de ayuda para escuchar y navegar por la interfaz. También puede utilizar el teclado en lugar del ratón para utilizar todas las características de la interfaz gráfica de usuario.

Para obtener más información, consulte el Apéndice de accesibilidad en la *Visión general del productoIBM Security Directory Server*.

Formación técnica

Para obtener la información de la formación técnica, consulte el siguiente sitio web de IBM Education en http://www.ibm.com/software/tivoli/education.

Información de soporte

IBM Support ayuda a la rutina y a los problemas relacionados con código, a la instalación de corta duración o a las preguntas de utilización. Puede acceder directamente al sitio de IBM Software Support en http://www.ibm.com/software/support/probsub.html.

IBM Security Directory Server Troubleshooting Guide proporciona detalles sobre:

- Qué información desea recopilar antes de ponerse en contacto con IBM Support.
- Los diversos métodos para ponerse en contacto con IBM Support.
- Cómo utilizar IBM Support Assistant.
- Instrucciones y recursos de determinación de problemas para aislar y solucionar el propio problema.

Nota: El separador **Comunidad y soporte** del centro de información del producto puede proporcionar recursos de soporte adicionales.

Sentencia de buenas prácticas de seguridad

La seguridad del sistema de TI implica la protección de sistemas y de la información mediante la prevención, la detección y la respuesta al acceso indebido desde dentro y fuera de la empresa. El acceso indebido puede dar lugar a que la información se altere, se destruya, se desvíe, o se utilice indebidamente o que pueda dar lugar a daños o a una utilización indebida de los sistemas, incluso en caso de ataques en terceros. Ningún producto o sistema de TI se debe considerar como totalmente seguro y ningún producto, servicio o medida de seguridad puede ser completamente efectivo a la hora de prevenir el acceso o el uso indebido. Los sistemas, productos y servicios de IBM están diseñados para formar parte de un enfoque de seguridad global, que implicará necesariamente procedimientos operativos adicionales, y que puede que necesite otros sistemas, productos o servicios para que sea más efectivo. IBM NO GARANTIZA QUE NINGÚN

SISTEMA, PRODUCTO O SERVICIO SEA INMUNE, O QUE CONVIERTA A SU EMPRESA EN INMUNE, DE LA CONDUCTA MALICIOSA O INDEBIDA DE CUALQUIER OTRA PARTE.

Capítulo 1. Planificación para la instalación

Debe decidir el hardware, el software, los roles de usuario, la seguridad y otros requisitos para el entorno de servidor de directorios antes de la instalación de IBM Security Directory Server.

Hoja de ruta de planificación

Utilice la lista de comprobación de esta sección para instalar un servidor.

Si realiza la actualización desde un release anterior, no utilice esta lista de comprobación, sino que consulte el Capítulo 14, "Actualizar una instancia de una versión anterior", en la página 91 para obtener instrucciones.

Para instalar el servidor:

1. Lea una breve visión general para entender los componentes de IBM Security Directory Server que instalará:
2. Asegúrese de tener el software y hardware mínimo requerido. Para obtener más información sobre los requisitos, consulte "Requisitos de espacio en disco" en la página 3.
3. Instale IBM Security Directory Server mediante IBM Installation Manager.
4. En sistemas Windows, si se reinicia el sistema, inicie la sesión como el mismo usuario con el que había iniciado la sesión durante la instalación.
5. Utilice la Herramienta de administración de instancias para gestionar las instancias de servidor de directorios.
6. Opcionalmente, verifique la instalación y configuración cargando el archivo LDIF de ejemplo en la base de datos. Para obtener más información, consulte el Apéndice B, "Carga de una base de datos de ejemplo e inicio del servidor", en la página 257.
7. Inicie la instancia de servidor de directorios y, si ha instalado la Herramienta de administración de instancias, iníciela.
8. Consulte la sección Administración de la documentación de IBM Security Directory Server para obtener información acerca de cómo configurar y utilizar el servidor y la Herramienta de administración web.

Si ha instalado un servidor de directorios completo y desea planificar la organización de la base de datos, consulte el "Planificación de la configuración" en la página 127 para obtener información.

Capítulo 2. Visión general de la instalación

Debe preparar el sistema y elegir la modalidad de instalación apropiada de IBM Security Directory Server aplicable para el entorno.

El instalador basado en IBM Installation Manager se proporciona para Windows, Linux64 y AIX. Hay instaladores de derivador disponibles para IBM Security Directory Server en sistemas UNIX, excepto Linux 64 y AIX. Con el instalador basado en Installation Manager, se da soporte a la instalación de la GUI y en modalidad silenciosa para IBM Security Directory Server V6.3.1.

Requisitos de espacio en disco

Para la instalación satisfactoria de IBM Security Directory Server y del software necesario, el sistema debe contener el espacio de disco necesario. Los requisitos de espacio de disco varían en función del sistema operativo y de las características de IBM Security Directory Server y del software necesario que seleccione para su instalación.

Requisitos de espacio de disco en Windows

Nota: Si selecciona la característica de Servidor proxy o de Servidor de directorios completo para su instalación, añada los tamaños para el SDK de cliente, IBM Java Development Kit y el cliente Java una vez.

Tabla 1. Los requisitos de espacio de disco para las características de IBM Security Directory Server y el software necesario en Windows

Característica instalable	**Espacio de disco para la instalación (en MB)**
Client Software Development Kit	25 MB
IBM Java Development Kit	200 MB
Java Client	124 MB
La Herramienta de administración web desplegada (incluye WebSphere Application Server incorporado y la Herramienta de administración web que se despliega en WebSphere Application Server incorporado)	440 MB
El despliegue de la Herramienta de administración web en WebSphere Application Server incorporado o en WebSphere Application Server	260 MB
Servidor base	23 MB
Servidor proxy (añada los tamaños para el SDK de cliente, el cliente Java y el servidor base)	40 MB
Servidor de directorios completo (añada los tamaños para el SDK de cliente, el cliente Java y el servidor base)	8 MB
IBM DB2	763 MB
IBM Global Security Kit	11 MB

Requisitos de espacio de disco en AIX

Nota: Si selecciona la característica de Servidor proxy o de Servidor de directorios completo para su instalación, añada los tamaños para el SDK de cliente, IBM Java Development Kit y el cliente Java una vez.

Tabla 2. Los requisitos de espacio de disco para las características de IBM Security Directory Server y el software necesario en AIX

Característica instalable	**Espacio de disco para la instalación (en MB)**
Client Software Development Kit	8 MB
IBM Java Development Kit	200 MB
Java Client	91 MB
La Herramienta de administración web desplegada (incluye WebSphere Application Server incorporado y la Herramienta de administración web que se despliega en WebSphere Application Server incorporado)	443 MB
El despliegue de la Herramienta de administración web en WebSphere Application Server incorporado o en WebSphere Application Server	500 MB
Herramienta de administración de Web SSL	51 MB
Servidor base	39 MB
Servidor proxy (añada los tamaños para el SDK de cliente, el cliente Java y el servidor base)	4 MB
Servidor de directorios completo (añada los tamaños para el SDK de cliente, el cliente Java y el servidor base)	12 MB
IBM DB2	1250 MB
IBM Global Security Kit	16 MB

Requisitos de espacio de disco en Linux

Nota: Si selecciona la característica de Servidor proxy o de Servidor de directorios completo para su instalación, añada los tamaños para el SDK de cliente, IBM Java Development Kit y el cliente Java una vez.

Tabla 3. Los requisitos de espacio de disco para las características de IBM Security Directory Server y el software necesario en Linux

Característica instalable	**Espacio de disco para la instalación (en MB)**
Client Software Development Kit	9 MB
IBM Java Development Kit	200 MB
Java Client	166 MB
La Herramienta de administración web desplegada (incluye WebSphere Application Server incorporado y la Herramienta de administración web que se despliega en WebSphere Application Server incorporado)	443 MB

Tabla 3. Los requisitos de espacio de disco para las características de IBM Security Directory Server y el software necesario en Linux (continuación)

Característica instalable	**Espacio de disco para la instalación (en MB)**
El despliegue de la Herramienta de administración web en WebSphere Application Server incorporado o en WebSphere Application Server	375 MB
Servidor base	32 MB
Servidor proxy (añada los tamaños para el SDK de cliente, el cliente Java y el servidor base)	40 MB
Servidor de directorios completo (añada los tamaños para el SDK de cliente, el cliente Java y el servidor base)	8 MB
IBM DB2 (System x Linux)	460 MB
IBM DB2 (System zLinux)	670 MB
IBM DB2 (System i y System p Linux)	520 MB
IBM DB2 (AMD64/EM64T Linux)	1300 MB
IBM Global Security Kit	40 MB

Nota: (Aplicable para el instalador basado en Installation Manager). En el directorio de recursos compartidos, se requieren 200 MB de espacio de disco duro. En el directorio de instalación de IBM Security Directory Server, se requieren 200 MB adicionales de espacio de disco duro.

Requisito de espacio para el directorio temp predeterminado del sistema: Si se selecciona la instalación de DB2, se requieren 2048 MB + 500 MB de espacio libre en el directorio temp. Sin DB2, se requieren 500 MB de espacio libre en el directorio temp.

Requisitos de espacio de disco en Solaris

Nota: Si selecciona la característica de Servidor y Servidor proxy para su instalación, añada los tamaños de C Client, IBM Java Development Kit y Java Client una vez.

Tabla 4. Los requisitos de espacio de disco para las características de IBM Security Directory Server y el software necesario en Solaris

Característica instalable	**Espacio de disco para la instalación (en MB)**	**Comentarios**
C Client	11 MB	
IBM Java Development Kit		
Java Client	145 MB	
64 bits	47 MB	Añada los tamaños de C Client y del cliente Java
Proxy Server	40 MB	Añada los tamaños de C Client y del cliente Java

Tabla 4. Los requisitos de espacio de disco para las características de IBM Security Directory Server y el software necesario en Solaris (continuación)

Característica instalable	Espacio de disco para la instalación (en MB)	Comentarios
Herramienta de administración web	470 MB	Incluye WebSphere Application Server, incorporado y la Herramienta de administración web que se despliega en WebSphere Application Server incorporado
IBM DB2	1155 MB	
IBM Global Security Kit	34 MB	

Requisitos de espacio de disco en HP-UX

Tabla 5. Los requisitos de espacio de disco para las características de IBM Security Directory Server y el software necesario en HP-UX

Característica instalable	Espacio de disco para la instalación (en MB)
C Client	26 MB
IBM Java Development Kit	
Java Client	172 MB
IBM Global Security Kit	41 MB

Preparación del soporte de instalación

El paquete del producto IBM Security Directory Server incluye IBM Security Directory Server, el software necesario, y el programa de instalación. Puede obtener el soporte de instalación de los DVD de instalación o desde el sitio web de Passport Advantage.

El producto IBM Security Directory Server está disponible en tres tipos de archivos: `.zip`, `.tar`, e `.iso`. Un archivo `.iso` contiene varios archivos que se corresponden con varios archivos `.zip` o `.tar`.

Tabla 6. El producto IBM Security Directory Server está disponible en el siguiente formato en diversos sistemas operativos

AIX, Linux, Solaris, y Windows	AIX, Linux, Solaris, y HP-UX	Windows
Imagen ISO (archivo `.iso`)	Archivos de archivado de cinta (archivos `.tar`)	Archivos de archivado (archivos `.zip`)

Para utilizar DVD como soporte de instalación, debe completar una de las siguientes tareas:

- Cree una imagen de DVD desde la imagen del producto IBM Security Directory Server para el sistema operativo.
- Almacene la imagen del producto IBM Security Directory Server en el disco duro del sistema y móntela si es necesario.

Al descargar los archivos de archivado del producto, debe cumplir los requisitos siguientes:

1. Descargue todos los archivos de archivado necesarios en el mismo directorio. Evite la descarga de los archivos de archivado a una ubicación de directorios que contenga espacios en el nombre de la vía de acceso.
2. Descomprima todos los archivos de archivado del mismo directorio que no contengan espacios en la vía de acceso de directorios. La vía de acceso de directorio del instalable no debe contener espacios.

Para descargar el producto IBM Security Directory Server desde Passport Advantage, consulte "Descarga del software desde Passport Advantage".

Tras preparar el soporte de instalación, debe cumplir los requisitos de software de requisito previo para el sistema operativo. Consulte el apartado "Requisitos previos de instalación" en la página 15.

Descarga del software desde Passport Advantage

Para la instalación de IBM Security Directory Server, debe descargar el software desde IBM Passport Advantage.

Antes de empezar

Debe registrarse y obtener un número de cuenta de cliente y una contraseña para acceder a IBM Passport Advantage.

Procedimiento

1. Vaya al sitio web de IBM Passport Advantage en http://www.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm.
2. Pulse **Inicio de sesión del cliente**.
3. En el campo **ID de IBM**, especifique el ID de IBM.
4. En el campo **Contraseña**, especifique la contraseña.
5. Pulse **Iniciar sesión**.
6. Siga las instrucciones para descargar el software de IBM Security Directory Server.

Estructura de directorios de los archivos descargados

Debe comprobar la estructura de directorios tras haber descargado los archivos de instalación para IBM Security Directory Server.

Estructura de directorios de los paquetes de Windows

Los nombres de archivos de los paquetes de Security Tivoli Directory Server 6.3.1 para Windows son:

Imagen de DVD: sds631-win.iso
Archivos .zip:
– sds631-win-base.zip (Security Directory Server 6.3.1 Cliente y Servidor)
– sds631-win-db2.zip (DB2 V9.7)
– sds631-win-ewas.zip (WebSphere Application Server 7.0.0.29 incorporado)
– sds631-win-gskit.zip (GSKit 8.0)
– sds631-win-jdk.zip (IBM Java Development Kit)
– sds631-win-IM.zip (IBM Installation Manager)

Después de crear el DVD o de descomprimir los archivos .zip, la estructura de directorios es la siguiente:

\sdsV6.3.1 (Directorio de nivel superior de los archivos descomprimidos)
– ibm_gskit\ (GSKit)
– license\ (licencias para Security Directory Server y otros productos proporcionados)
– quickstart\ (Guías de inicio rápido en inglés y en otros idiomas)
– entitlement\ (Archivos de titularidad para el servidor proxy)
– entitlement.txt
– tools\ (Herramientas que incluyen migbkup)
– migbkup.bat
– ibm_db2_32bit\ (DB2)
– ibm_db2_64bit\ (DB2)
– ibm_ewas_32bit\ (WebSphere Application Server incorporado)
– ibm_ewas_64bit\ (WebSphere Application Server incorporado)
– ibm_im_32bit\ (IBM Installation Manager)
– ibm_im_64bit\ (IBM Installation Manager)
– ibm_jdk\ (IBM Java Development Kit)
– ibm_sds\ (archivos del instalador)
– atoc
– files
– native
– Offerings
– plugins
– ShareableEntities
– build.properties
– repository.config
– repository.xml
– launchpad\
– SilentInstallScripts\ (archivos de respuestas utilizados en la instalación silenciosa)
– autorun.inf
– imLauncherWindows.bat
– launchpad.exe
– launchpad.ini
– launchpad64.exe
– launchpad64.ini
– sds_install.xml
– write_sds_path.bat

Paquete Windows solo de cliente

Archivo .zip:
– sds631-win-client.zip (Security Directory Server 6.3.1 Cliente)

Después de descomprimir el archivo .zip, la estructura de directorios es la siguiente:

\sdsV6.3.1 (Directorio de nivel superior de los archivos descomprimidos)
– ibm_gskit\ (GSKit 8)
– jdk\ (IBM Java Development Kit)
– ibm_im_32bit (IBM Installation Manager)
– ibm_im_64bit (IBM Installation Manager)
– ibm_sds\ (archivos del instalador)
– launchpad\
– SilentInstallScripts\

– autorun.inf
– license\ (licencias para Security Directory Server y otros productos proporcionados)
– quickstart\ (Guías de inicio rápido en inglés y en otros idiomas)
– ibm_im_32bit\ (IBM Installation Manager)
– ibm_im_64bit\ (IBM Installation Manager)
– imLauncherWindows.bat
– launchpad.exe
– launchpad.ini
– launchpad64.exe
– launchpad64.ini
– sds_install.xml
– write_sds_path.bat

Estructura de directorios de los paquetes de AIX

Los nombres de archivos de los paquetes de Security Tivoli Directory Server 6.3.1 para AIX son:

Imagen de DVD: sds631-aix-ppc64.iso
Archivos .tar:
– tds63-aix-ppc64-base.tar (Security Directory Server 6.3.1 Cliente y Servidor)
– sds631-aix-ppc64-db2.tar (DB2 V9.7)
– sds631-aix-ppc64-ewas.tar (WebSphere Application Server 7.0.0.29 incorporado)
– sds631-aix-ppc64-gskit.tar (GSKit 8.0)
– sds631-aix-ppc64-jdk.tar (IBM Java Development Kit)
– sds631-aix-ppc64-IM.tar (IBM Installation Manager)

Después de crear el DVD o de descomprimir los archivos .tar, la estructura de directorios es la siguiente:

/sdsV6.3.1 (Directorio de nivel superior de los archivos descomprimidos)
– license/ (licencias para Security Directory Server y otros productos proporcionados)
–quickstart/ (Guías de inicio rápido en inglés y en otros idiomas)
– ibm_im (IBM Installation Manager)
– ibm_db2/ (DB2)
– ibm_ewas/ (WebSphere Application Server incorporado)
– ibm_gskit/ (GSKit 8)
– ibm_jdk/ (IBM Java Development Kit)
– ibm_sds/ (archivos del instalador)
– atoc/
– files/
– native/
– Offerings/
– plugins/
– ShareableEntities
– build.properties
– repository.config
– repository.xml

– tools/ (Herramientas que incluyen migbkup)
– launchpad/
– SilentInstallScripts/
– launchpad.sh
– sds_install.xml

– write_sds_path.sh
– entitlement/ (Archivos de titularidad para el servidor proxy)
– native / (paquetes nativos)

Paquete AIX solo de cliente

Archivo .zip:
– sds631-aix-ppc64-client.tar (Security Directory Server 6.3.1 Cliente)

Después de descomprimir el archivo .zip, la estructura de directorios es la siguiente:

\sdsV6.3.1 (Directorio de nivel superior de los archivos descomprimidos)
– ibm_gskit\ (GSKit 8)
– ibm_jdk\ (IBM Java Development Kit)
– ibm_im\ (IBM Installation Manager)
– ibm_sds\ (archivos del instalador)
– launchpad\
– SilentInstallScripts\
– autorun.inf
– license\ (licencias para Security Directory Server y otros productos proporcionados)
– quickstart\ (Guías de inicio rápido en inglés y en otros idiomas)
– ibm_im\ (IBM Installation Manager)
– imLauncherWindows.bat
– launchpad.exe
– launchpad.ini
– sds_install.xml
– write_sds_path.bat

Estructura de directorios de los paquetes del servidor Linux x86_64

Los nombres de archivos de los paquetes de Security Tivoli Directory Server 6.3.1 para el servidor de Linux x86_64 son:

Imagen de DVD: sds631-linux-x86-64.iso
Archivos .tar:
– sds631-linux-x86-64-base.tar (IBM Security Directory Server 6.3.1 Cliente y Servidor)
– sds631-linux-x86-64-IM.tar (IBM Installation Manager)
– sds631-linux-x86-64-gskit.tar (GSKit 8)
– sds631-linux-x86-64-db2.tar (DB2 vV9.7)
– sds631-linux-x86-64-ewas.tar (WebSphere Application Server 7.0.0.29 incorporado)
– sds631-linux-x86-64-jdk.tar (IBM Java Development Kit)

Después de crear el DVD o de descomprimir los archivos .tar, la estructura de directorios es la siguiente:

/sdsV6.3.1 (Directorio de nivel superior de los archivos descomprimidos)
– license/ (licencias para Security Directory Server y otros productos proporcionados)
–quickstart/ (Guías de inicio rápido en inglés y en otros idiomas)
– ibm_im (IBM Installation Manager)
– ibm_db2/ (DB2)
– ibm_ewas/ (WebSphere Application Server incorporado)
– ibm_gskit/ (GSKit 8)

– ibm_jdk/ (IBM Java Development Kit)
– ibm_sds/ (archivos del instalador)
– atoc/
– files/
– native/
– Offerings/
– plugins/
– ShareableEntities
– build.properties
– repository.config
– repository.xml

– tools/ (Herramientas que incluyen migbkup)
– launchpad/
– SilentInstallScripts/
– launchpad.sh
– sds_install.xml
– write_sds_path.sh
– entitlement/ (Archivos de titularidad para el servidor proxy)
– native / (paquete nativo)

Paquete solo de cliente de Linux x86_64

Archivo .zip:
– sds631-linux-x86-64-client.tar (Security Directory Server 6.3.1 Cliente)

Después de descomprimir el archivo .zip, la estructura de directorios es la siguiente:

\sdsV6.3.1 (Directorio de nivel superior de los archivos descomprimidos)
– ibm_jdk\ (IBM Java Development Kit)
– ibm_im (IBM Installation Manager)
– ibm_sds\ (archivos del instalador)
– launchpad\
– SilentInstallScripts\
– autorun.inf
– license\ (licencias para Security Directory Server y otros productos proporcionados)
– quickstart\ (Guías de inicio rápido en inglés y en otros idiomas)
– ibm_im\ (IBM Installation Manager)
– imLauncherWindows.bat
– launchpad.exe
– launchpad.ini
– sds_install.xml
– write_sds_path.bat

Estructura de directorios de los paquetes del servidor Linux x86

Los nombres de archivos de los paquetes de Security Tivoli Directory Server 6.3.1 para el servidor Linux x86 son:

Imagen de DVD: sds631-linux-x86.iso
Archivos .tar:
– sds631-linux-x86-base.tar (IBM Security Directory Server 6.3.1 Cliente y Servidor)
– sds631-linux-x86-gskit.tar (GSKit 8)
– sds631-linux-x86-db2.tar (DB2 v9.7)

– sds631-linux-x86-ewas.tar (WebSphere Application Server 7.0.0.29 incorporado)
– sds631-linux-x86-jdk.tar (IBM Java Development Kit)

Después de crear el DVD o de descomprimir los archivos .tar, la estructura de directorios es la siguiente:

/sdsV6.3.1 (Directorio de nivel superior de los archivos descomprimidos)
– appsrv/ (WebSphere Application Server incorporado)
– db2 (DB2)
– gskit/ (GSKit 8)
– jdk/ (IBM Java Development Kit)
– ids_detectGskitVersion
– idsinstall_i
– idsNativeInstall.sh
– images/ (imágenes nativas)
– license/ (licencias para Security Directory Server y otros productos)
– responseFile.txt (archivos de respuestas)

Paquete solo de cliente de Linux x86

Archivo .zip:
– sds631-linux-x86-client.tar (Security Directory Server 6.3.1 Cliente)

Después de descomprimir el archivo .zip, la estructura de directorios es la siguiente:

\sdsV6.3.1 (Directorio de nivel superior de los archivos descomprimidos)
– gskit/ (GSKit 8)
– image/
– license/ (licencias para Security Directory Server y otros productos)
– jdk (IBM Java Development Kit)

Estructura de directorios de los paquetes del servidor Linux ppc

Los nombres de archivos de los paquetes de Security Tivoli Directory Server 6.3.1 para el servidor Linux ppc son:

Imagen de DVD: sds631-linux-ppc64.iso
Archivos .tar:
– sds631-linux-ppc64-base.tar (IBM Security Directory Server 6.3.1 Cliente y Servidor)
– sds631-linux-ppc64-gskit.tar (GSKit 8)
– sds631-linux-ppc64-db2.tar (DB2 V9.7)
– sds631-linux-ppc64-ewas.tar (WebSphere Application Server 7.0.0.29 incorporado)
– sds631-linux-ppc64-jdk.tar (IBM Java Development Kit)

Después de crear el DVD o de descomprimir los archivos .tar, la estructura de directorios es la siguiente:

/sdsV6.3.1 (Directorio de nivel superior de los archivos descomprimidos)
– appsrv/ (WebSphere Application Server incorporado)
– db2 (DB2)
– gskit/ (GSKit 8)
– jdk/ (IBM Java Development Kit)
– ids_detectGskitVersion
– idsinstall_i
– idsNativeInstall.sh

– images/ (imágenes nativas)
– license/ (licencias para Security Directory Server y otros productos)
– responseFile.txt (archivos de respuestas)

Paquete solo de cliente de Linux ppc

Archivo .zip:
– sds631-linux-ppc64-client.tar (Security Directory Server 6.3.1 Cliente)

Después de descomprimir el archivo .zip, la estructura de directorios es la siguiente:

\sdsV6.3.1 (Directorio de nivel superior de los archivos descomprimidos)
– gskit/ (GSKit 8)
– image/
– license/ (licencias para Security Directory Server y otros productos)
– jdk (IBM Java Development Kit)

Estructura de directorios de los paquetes del servidor Linux s390

Los nombres de archivos de los paquetes de Security Tivoli Directory Server 6.3.1 para el servidor Linux s390 son:

Imagen de DVD: sds631-linux-s390x.iso
Archivos .tar:
– sds631-linux-s390x-base.tar (IBM Security Directory Server 6.3.1 Cliente y Servidor)
– sds631-linux-s390x-gskit.tar (GSKit 8)
– sds631-linux-s390x-db2.tar (DB2 V9.7)
– sds631-linux-s390x-ewas.tar (WebSphere Application Server 7.0.0.29 incorporado)
– sds631-linux-s390x-jdk.tar (IBM Java Development Kit)

Después de crear el DVD o de descomprimir los archivos .tar, la estructura de directorios es la siguiente:

/sdsV6.3.1 (Directorio de nivel superior de los archivos descomprimidos)
– appsrv/ (WebSphere Application Server incorporado)
– db2 (DB2)
– gskit/ (GSKit 8)
– jdk/ (IBM Java Development Kit)
– ids_detectGskitVersion
– idsinstall_i
– idsNativeInstall.sh
– images/ (imágenes nativas)
– license/ (licencias para Security Directory Server y otros productos)
– responseFile.txt (archivos de respuestas)

Paquete solo de cliente de Linux s390

Archivo .zip:
– sds631-linux-s390x-client.tar (Security Directory Server 6.3.1 Cliente)

Después de descomprimir el archivo .zip, la estructura de directorios es la siguiente:

\sdsV6.3.1 (Directorio de nivel superior de los archivos descomprimidos)
– gskit/ (GSKit 8)
– image/
– license/ (licencias para Security Directory Server y otros productos)
– jdk (IBM Java Development Kit)

Estructura de directorios de los paquetes del servidor Solaris x86_64

Los nombres de archivos de los paquetes de Security Tivoli Directory Server 6.3.1 para el servidor de Solaris x86_64 son:

Imagen de DVD: sds631-solaris-x86-64.iso
Archivos .tar:
– sds631-solaris-x86-64-base.tar (IBM Security Directory Server 6.3.1 Cliente y Servidor)
– sds631-solaris-x86-64-gskit.tar (GSKit 8)
– sds631-solaris-x86-64-db2.tar(DB2 v9.7)
– sds631-solaris-x86-64-ewas.tar (WebSphere Application Server 7.0.0.29 incorporado)
– sds631-solaris-x86-64-jdk.tar (IBM Java Development Kit)

Después de crear el DVD o de descomprimir los archivos .tar, la estructura de directorios es la siguiente:

/sdsV6.3.1 (Directorio de nivel superior de los archivos descomprimidos)
– appsrv/ (WebSphere Application Server incorporado)
– db2 (DB2)
– gskit/ (GSKit 8)
– jdk/ (IBM Java Development Kit)
– ids_detectGskitVersion
– idsinstall_i
– idsNativeInstall.sh
– images/ (imágenes nativas)
– license/ (licencias para Security Directory Server y otros productos)
– responseFile.txt (archivos de respuestas)

Paquete solo de cliente de Solaris x86_64

Archivo .zip:
– sds631-solaris-x86-64-client.tar (Security Directory Server 6.3.1 Cliente)

Después de descomprimir el archivo .zip, la estructura de directorios es la siguiente:

\sdsV6.3.1 (Directorio de nivel superior de los archivos descomprimidos)
– gskit/ (GSKit 8)
– image/
– license/ (licencias para Security Directory Server y otros productos)
– jdk (IBM Java Development Kit)

Estructura de directorios de los paquetes del servidor Solaris sparc

Los nombres de archivos de los paquetes de Security Tivoli Directory Server 6.3.1 para el servidor de Solaris sparc son:

Imagen de DVD:
Archivos .tar:
– sds631-solaris-sparc.iso
– sds631-solaris-sparc-base.tar (IBM Security Directory Server 6.3.1 Cliente y Servidor)
– sds631-solaris-sparc-gskit.tar (GSKit 8)
– sds631-solaris-sparc-db2.tar (DB2 v9.7)
– sds631-solaris-sparc-ewas.tar (WebSphere Application Server 7.0.0.29 incorporado)
– sds631-solaris-sparc-jdk.tar (IBM Java Development Kit)

Después de crear el DVD o de descomprimir los archivos .tar, la estructura de directorios es la siguiente:

/sdsV6.3.1 (Directorio de nivel superior de los archivos descomprimidos)
– appsrv/ (WebSphere Application Server incorporado)
– db2 (DB2)
– gskit/ (GSKit 8)
– jdk/ (IBM Java Development Kit)
– ids_detectGskitVersion
– idsinstall_i
– idsNativeInstall.sh
– images/ (imágenes nativas)
– license/ (licencias para Security Directory Server y otros productos)
– responseFile.txt (archivos de respuestas)

Paquete solo de cliente de Solaris Sparc

Archivo .zip:
– sds631-solaris-sparc-client.tar (Security Directory Server 6.3.1 Cliente)

Después de descomprimir el archivo .zip, la estructura de directorios es la siguiente:

\sdsV6.3.1 (Directorio de nivel superior de los archivos descomprimidos)
– gskit/ (GSKit 8)
– image/
– license/ (licencias para Security Directory Server y otros productos)
– jdk (IBM Java Development Kit)

Requisitos previos de instalación

La instalación de IBM Security Directory Server y del software necesario puede requerir la instalación de requisitos previos para el sistema operativo. El software de requisito previo debe estar instalado antes de la instalación de IBM Security Directory Server y del software necesario.

Paquetes de requisito previo que son necesarios en diversos sistemas operativos

Debe actualizar el sistema con los paquetes de requisito previo necesarios para la instalación de IBM Security Directory Server y de sus productos necesarios.

El shell Korn es necesario en los sistemas operativos AIX, Linux, Solaris, y HP-UX (Itanium). En SuSE Linux Enterprise Server, `PDKSH` es necesario.

Los siguientes paquetes de requisito previo son necesarios para la instalación de IBM Security Directory Server en los siguientes sistemas operativos:

AIX Para la instalación de los paquetes de rpm en AIX, descargue el gestor de paquetes de `rpm` para sistemas AIX desde el sitio web ftp://public.dhe.ibm.com/aix/freeSoftware/aixtoolbox/INSTALLP/ppc/rpm.rte.

Tabla 7. Los paquetes de requisito previo que son necesarios en un sistema operativo AIX

Paquetes	Motivo	Dirección de descarga
Navegador web Mozilla Firefox para AIX	Para abrir el Launchpad en AIX, debe existir una versión soportada del navegador.	Para obtener más información sobre los navegadores web para AIX, consulte el sitio web http://www.ibm.com/systems/power/software/aix/browsers/.
`gtk+ RPM (gtk2-2.10.6-4.aix5.2.ppc.rpm)`	Eclipse ha modificado el requisito de sistema de ventanas de `motif` a `gtk` en los sistemas operativos UNIX. Para AIX, esta modificación del sistema de ventanas de Eclipse requiere que se instalen las bibliotecas de `gtk` para dar soporte a la GUI. Para IBM Installation Manager, la GUI es la modalidad de asistente de la operación.	Para obtener más información sobre la instalación de las bibliotecas de `gtk`, consulte la nota técnica Required gtk libraries for Installation Manager on AIX en el sitio web http://www.ibm.com/support/docview.wss?uid=swg21631478.
GNU `tar`	Para descomprimir archivos de archivado que se proporcionan con IBM Security Directory Server en sistemas AIX, es necesario el programa de archivado de archivos GNU. Debe establecer la vía de acceso del programa GNU `tar` antes del programa `tar` que se proporciona con el sistema operativo. El programa GNU `tar` está instalado en el directorio `/opt/freeware/bin`, y el programa `tar` que se proporciona con el sistema operativo en el directorio `/usr/bin`. Para establecer la vía de acceso `/opt/freeware/bin`, ejecute el mandato siguiente: `export PATH=/opt/freeware/bin:$PATH`.	Para descargar el archivo archivador `tar` de GNU (`tar`), consulte el sitio web de http://www.ibm.com/systems/power/software/aix/linux/toolbox/alpha.html .
Conjunto de archivos `X11.adt.lib`	El conjunto de archivos `X11.adt.lib` es un requisito previo para instalar los paquetes `idsldap.cltjava631` e `idsldap.webadmin631` en sistemas AIX.	

Tabla 7. Los paquetes de requisito previo que son necesarios en un sistema operativo AIX (continuación)

Paquetes	Motivo	Dirección de descarga
`xlC.rte 8.0.0.6` y `xlC.aix50.rte 8.0.0.6` o niveles posteriores	IBM C++ Runtime Environment Components for AIX requiere los niveles de tiempo de ejecución `xlC.rte 8.0.0.6` y `xlC.aix50.rte 8.0.0.6` o posteriores.	
`bos.loc.iso.en_US 5.3.0.0`	IBM Security Directory Server, versión 6.3.1 requiere el mínimo nivel de conjunto de archivos de entorno local del sistema de nivel base en `bos.loc.iso.en_US 5.3.0.0`.	

Requisitos previos para el cliente LDAP en PowerPC LE

Si desea ejecutar el cliente de IBM Security Directory Server en PowerPC LE (Little Endian), debe instalar IBM Advance Toolchain Versión 7.1 en el sistema PowerPC LE.

Debe instalar IBM Advance Toolchain Versión 7.1 tanto si piensa ejecutar el cliente LDAP como si piensa escribir sus propios cliente enlazando a las bibliotecas proporcionadas.

Para descargar e instalar IBM Advanced Toolchain Versión 7.1 para su sistema operativo, consulte la documentación de IBM Advance Toolchain.

El usuario y grupo `idsldap`

Si selecciona la característica Server o Proxy Server para su instalación, el programa de instalación puede crear el usuario y grupo `idsldap`.

El programa de instalación crea el usuario y grupo `idsldap` si no existen.

Nota: En AIX, Linux, y Solaris, la instalación con los programas de utilidad del sistema operativo crea el usuario `idsldap` si no existe. Sin embargo, si existe el directorio `/home/idsldap` en Linux y AIX o el directorio `/export/home/idsldap` en Solaris, puede que no sea posible crear el usuario `idsldap`. Por lo tanto, debe asegurarse de que el directorio de inicio para `idsldap` no existe si no existe el usuario `idsldap`.

Si el entorno requiere que controle el usuario y el grupo `idsldap`, puede crearlos antes de la instalación. El usuario y el grupo `idsldap` deben cumplir los siguientes requisitos:

- El usuario `idsldap` debe ser miembro del grupo `idsldap`.
- En AIX, Linux, y Solaris, el usuario root debe ser miembro del grupo `idsldap`. En Windows, el Administrador debe ser miembro del grupo `idsldap`.
- El usuario `idsldap` debe tener un directorio de inicio.
- En AIX, Linux, y Solaris, el shell predeterminado para el usuario `idsldap` debe ser el shell Korn.
- El usuario `idsldap` puede tener una contraseña, pero no es obligatorio.

- El usuario idsldap puede ser el propietario de la instancia de servidor de director.

Debe cumplir todos los requisitos antes de la instalación de IBM Security Directory Server. Si existe el usuario idsldap pero no cumple los requisitos, es posible que falle la instalación de la característica de Proxy Server.

Nota: Para obtener más información sobre los requisitos del ID de usuario para una instancia, instancia de directorio, propietario de base de datos, consulte "Usuarios y grupos que están asociados con una instancia de servidor de directorios" en la página 123.

Puede utilizar Herramienta de administración de instancias para crear usuarios y grupos al crear una instancia de servidor de directorios. También puede utilizar los programas de utilidad del sistema operativo para crear el usuario y el grupo idsldap y configurarlos correctamente.

Ejemplos

Ejecute los siguientes programas de utilidad del sistema operativo para crear el grupo idsldap, el usuario idsldap, la contraseña, y para añadir root como miembro del grupo idsldap.

En sistemas AIX:

Para crear el grupo idsldap, ejecute el siguiente mandato:

```
mkgroup idsldap
```

Para crear el ID de usuario idsldap como miembro del grupo idsldap y para establecer el shell Korn como el shell predeterminado, ejecute el mandato siguiente:

```
mkuser pgrp=idsldap home=/home/idsldap shell=/bin/ksh idsldap
```

Para establecer la contraseña para el usuario idsldap, ejecute el mandato siguiente:

```
passwd idsldap
```

Para añadir el ID de usuario root como miembro del grupo idsldap, ejecute el siguiente mandato:

```
/usr/bin/chgrpmem -m + root idsldap
```

En sistemas Linux:

Para crear el grupo idsldap, ejecute el siguiente mandato:

```
groupadd idsldap
```

Para crear el ID de usuario idsldap como miembro del grupo idsldap y para establecer el shell Korn como el shell predeterminado, ejecute el mandato siguiente:

```
useradd -g idsldap -d /home/idsldap -m -s /bin/ksh idsldap
```

Para establecer la contraseña para el usuario idsldap, ejecute el mandato siguiente:

```
passwd idsldap
```

Para añadir el ID de usuario root como miembro del grupo idsldap, ejecute el siguiente mandato:

```
usermod -G idsldap,gruposroot root
```

Puede recuperar los valores de *rootgroups* para el sistema con el mandato `groups root`.

En los sistemas Solaris:

Para crear el grupo `idsldap`, ejecute el siguiente mandato:

```
groupadd idsldap
```

Para crear el ID de usuario `idsldap` como miembro del grupo `idsldap` y para establecer el shell Korn como el shell predeterminado, ejecute el mandato siguiente:

```
useradd -g idsldap -d /export/home/idsldap -m -s /bin/ksh idsldap
```

Para establecer la contraseña para el usuario `idsldap`, ejecute el mandato siguiente:

```
passwd idsldap
```

Para añadir el ID de usuario root como miembro del grupo `idsldap`, ejecute el siguiente mandato:

```
usermod -G idsldap,root idsldap
```

Para modificar el ID de usuario root para que root sea miembro del grupo `idsldap`, utilice una herramienta adecuada.

Para obtener más información sobre el mandato para añadir el usuario y el grupo, consulte la documentación para el sistema operativo.

Métodos de instalación

Para la instalación de IBM Security Directory Server y su software necesario, debe elegir el método de instalación adecuado que se ajuste mejor a su entorno.

Puede utilizar los métodos siguientes para la instalación de IBM Security Directory Server y su software necesario:

- Instalación con IBM Installation Manager
- Instalación con los programas de utilidad de línea de mandatos del sistema operativo

PRECAUCIÓN:

- **No debe utilizar modalidades de instalación distintas en el mismo sistema. Debe ejecutar la instalación de IBM Security Directory Server con IBM Installation Manager o programas de utilidad de líneas de mandato del sistema operativo, pero no ambos. Si mezcla las dos modalidades de instalación, es posible que la instalación no incluya todos los paquetes correctos para una característica.**
- **Debe evitar la instalación manual de DB2 y de WebSphere Application Server incorporado en su vía de acceso de instalación predeterminada que utilice IBM Installation Manager. Tal instalación manual puede provocar errores de instalación, modificación, o desinstalación al ejecutar estas operaciones con IBM Installation Manager. Para obtener más información sobre la vía de acceso de instalación predeterminada, consulte “Ubicaciones de la instalación predeterminada” en la página 27.**

Capítulo 3. Instalación con IBM Installation Manager

IBM Installation Manager es una herramienta que puede utilizar para la instalación y el mantenimiento de IBM Security Directory Server y del software necesario.

Visión general de IBM Installation Manager

IBM Installation Manager es un asistente de instalación que le guiará a través de los pasos para instalar, modificar, actualizar, retrotraer o desinstalar productos de IBM. Puede utilizar repositorios de software remotos o locales para su instalación.

IBM Installation Manager también le ayuda a gestionar las aplicaciones o los paquetes de IBM que instala en el sistema de las siguientes formas:

- Mantiene un registro de lo que ha instalado
- Determina y muestra los paquetes que están disponibles para su instalación
- Comprueba los requisitos previos y las interdependencias

IBM Installation Manager incluye seis asistentes que facilitan el mantenimiento de paquetes:

- El asistente **Instalar** le guiará a través del proceso de instalación. Puede instalar uno o varios paquetes a la vez. Puede aceptar los valores predeterminados o puede modificar los valores para crear una instalación personalizada cuando sea posible. Antes de instalar, obtendrá un resumen completo de las selecciones de todo el asistente.
- El asistente **Actualizar** busca actualizaciones disponibles para los paquetes instalados en el sistema. Los detalles del contenido de la actualización se proporcionan en el asistente. Puede elegir si desea aplicar una actualización.
- El asistente **Modificar** le ayuda a modificar determinados elementos de un paquete que ya está instalado. Durante la primera instalación del paquete, seleccione las características que desea instalar. Posteriormente, si necesita otras características, puede utilizar el asistente modificar paquetes para añadirlos al paquete. También puede eliminar las características.
- El asistente **Gestionar licencias** le ayuda a configurar las licencias para los paquetes. Utilice este asistente para cambiar la licencia de prueba por una licencia completa, para configurar los servidores por licencias flotantes, y para seleccionar qué tipo de licencia utilizar para cada paquete.
- El asistente **Retrotraer** le ayuda a revertir a una versión anterior de un paquete.
- El asistente **Desinstalar** elimina un paquete del sistema. Puede desinstalar más de un paquete a la vez.

Sistemas operativos soportados

Puede utilizar IBM Installation Manager para la instalación de IBM Security Directory Server en AIX (ppc64), Linux (arquitectura de AMD64/EM64T), y Microsoft Windows.

Las siguientes secciones muestran las versiones de los sistemas operativos soportados para la instalación de IBM Security Directory Server con IBM Installation Manager.

Si desea instalar IBM Security Directory Server en un sistema operativo que no se muestra en las siguientes secciones:

1. Compruebe si la versión del sistema operativo está soportada para IBM Security Directory Server. Para obtener una lista de todos los sistemas operativos soportados, consulte *Visión general del productoIBM Security Directory Server*.
2. Si está soportado, puede utilizar los programas de utilidad de línea de mandatos del sistema operativo para la instalación de IBM Security Directory Server.

AIX (ppc64)

- AIX Versión 6.1
- AIX Versión 7.1

Linux (AMD64/EM64T)

- Red Hat Enterprise Linux 5, Advanced Platform
- Red Hat Enterprise Linux 6
- SUSE Linux Enterprise Server 10
- SUSE Linux Enterprise Server 11

Microsoft Windows (x64)

- Microsoft Windows Server 2008 R2, Enterprise Edition
- Microsoft Windows Server 2008 R2, Standard Edition
- Microsoft Windows Server 2008, Enterprise Edition
- Microsoft Windows Server 2008, Standard Edition
- Microsoft Windows Server 2012, Standard Edition

Tipos de paquetes de instalación de IBM Security Directory Server

Para elegir el paquete de instalación correcto de IBM Security Directory Server, debe conocer los tipos disponibles de paquetes de instalación.

Los siguientes tipos de paquetes de instalación de IBM Security Directory Server están disponibles para su instalación con IBM Installation Manager:

Tabla 8. Tipo de paquete de instalación de IBM Security Directory Server y las características disponibles para la instalación

Todas las características	Características del instalador de productos completo	Características del instalador sólo del cliente
IBM DB2	Sí	No
IBM Global Security Kit	Sí	Sí
C Client	Sí	Sí
IBM Java Development Kit	Sí	Sí
Java Client	Sí	Sí
64 bits	Sí	No
Proxy Server	Sí	No
Herramienta de administración web	Sí	No

Nota: Si opta por instalar la Herramienta de administración web, IBM Installation Manager proporciona una opción para instalar WebSphere Application Server incorporado.

Directrices de instalación

Debe tener en cuenta algunas restricciones antes de comenzar la instalación de IBM Security Directory Server con IBM Installation Manager.

Método de instalación

Al instalar IBM Security Directory Server, puede elegir instalar con IBM Installation Manager o con los programas de utilidad de línea de mandatos del sistema operativo. Para cualquier instalación futura o desinstalación de los paquetes, características y fixpacks de IBM Security Directory Server, debe utilizar el mismo método de instalación de un sistema. Por ejemplo, si instala IBM Security Directory Server con IBM Installation Manager, no debe utilizar los programas de utilidad de línea de mandatos para instalar características o para desinstalar el producto. Si lo hace, la configuración de IBM Security Directory Server puede resultar dañada o podría quedar inutilizable.

Versión de IBM Installation Manager

IBM Installation Manager Versión 1.7.0 y posterior están soportados para la instalación de IBM Security Directory Server. Aparece un mensaje de error en la página Instalar paquetes de IBM Installation Manager y no se podrá seguir con la instalación en los siguientes casos de ejemplo:

- Intente iniciar la instalación de IBM Security Directory Server con una versión anterior de IBM Installation Manager.
- Se ha detectado una versión anterior de IBM Installation Manager al iniciar la instalación de IBM Security Directory Server desde el programa Launchpad.

Varias instalaciones

No puede instalar varias copias de la misma versión de IBM Security Directory Server en el mismo sistema. Al seleccionar el paquete de instalación para la misma versión de nuevo, IBM Installation Manager generará un mensaje de aviso y no podrá continuar con la instalación. Sin embargo, pueden coexistir distintas versiones de IBM Security Directory Server en el mismo sistema.

Ubicación de instalación en sistemas AIX y Linux:

IBM Security Directory Server sólo se puede instalar en la ubicación predefinida en los sistemas AIX y Linux. La vía de acceso está especificada de forma predeterminada en el campo **Directorio de instalación** en IBM Installation Manager. Aunque este campo es editable en IBM Installation Manager, si cambia la vía de acceso que se especifica de forma predeterminada, no podrá pulsar **Siguiente** para continuar con la instalación. Debe volver a la vía de acceso de instalación predeterminada para IBM Security Directory Server.

Esta restricción no se aplica a los sistemas operativos Microsoft Windows. IBM Security Directory Server puede instalarse en cualquier ubicación personalizada de los sistemas operativos Microsoft Windows. Aunque seleccione una ubicación de instalación personalizada para IBM Security Directory Server, el directorio `idsinstinfo` y el archivo `idsinstances.ldif` que contiene siempre se crearán en la partición especificada por

%SystemDrive%. Si IBM Security Directory Server está instalado en la unidad E: y el sistema operativo está en la unidad C:, puede observar los cambios siguientes:

- Se creará el directorio idsinstinfo en la unidad C: (C:\idsinstinfo), en lugar de en el directorio E:\Program Files\IBM\ldap.

Para obtener más información sobre las ubicaciones de instalación predeterminadas, consulte "Ubicaciones de la instalación predeterminada" en la página 27.

Componentes de IBM Security Directory Server

Al instalar IBM Security Directory Server con IBM Installation Manager, puede seleccionar los componentes que desee instalar. IBM Installation Manager muestra las dependencias de cada componente que seleccione.

Los siguientes componentes de IBM Security Directory Server están disponibles para su instalación:

IBM DB2

Puede instalar IBM DB2 como una función. Si se ha instalado una versión soportada de IBM DB2, no necesita instalar DB2 proporcionado con el paquete de IBM Security Directory Server. Para obtener información sobre las versiones soportadas de DB2 para distintos sistemas operativos, consulte *Vision general del producto de IBM Security Directory Server*.

El servidor de directorios completo requiere IBM DB2 porque los datos de directorio se almacenan en una base de datos de DB2. IBM DB2 no es necesario para Proxy Server.

IBM Global Security Kit

Puede instalar IBM Global Security Kit (GSKit) como una característica junto con otras características de IBM Security Directory Server. GSKit es una característica opcional que sólo es necesaria si desea utilizar el protocolo de comunicación Secure Sockets Layer (SSL) o Transport Layer Security (TLS). GSKit debe estar instalado en los sistemas del servidor y del cliente para establecer y utilizar conexiones seguras.

C Client

Puede instalar C Client como una característica por sí misma o junto con otras características de IBM Security Directory Server. La característica C Client no tiene ninguna dependencia en otras características. Sin embargo, las características de Server y Proxy Server dependen del C Client. Al instalar la característica Server o Proxy Server, la característica C Client se seleccionará automáticamente para su instalación.

C Client es SDK (Software Development Kit) del cliente que proporciona las herramientas necesarias para desarrollar aplicaciones LDAP de lenguaje C. El paquete de C Client contiene los siguientes archivos y aplicaciones:

- Bibliotecas de cliente que proporcionan un conjunto de interfaces de programación de aplicaciones de lenguaje C (API)
- Archivos de cabecera C para crear y compilar aplicaciones LDAP
- Programas de utilidad del cliente y del servidor C
- Programas de ejemplo en formato de origen

IBM Java Development Kit

Puede instalar IBM Java Development Kit como una característica por sí misma o junto con otras características de IBM Security Directory Server.

Cuando se selecciona instalar IBM Java Development Kit, IBM Installation Manager extrae el archivo comprimido al subdirectorio `java` de la ubicación de instalación de IBM Security Directory Server. IBM Java Development Kit proporciona IBM Java SDK y Java 1.6 SR 14. IBM Java Development Kit es obligatorio para compilar programas de ejemplo de Java, y para ejecutar programas de Java, como por ejemplo Herramienta de administración de instancias (**idsxinst**) y Herramienta de configuración (**idsxcfg**).

Java Client

Puede instalar Java Client como una característica por sí misma o junto con otras características de IBM Security Directory Server. La característica de Java Client no tiene ninguna dependencia con respecto a otras características. Sin embargo, las características de Server y Proxy Server dependen de Java Client. Al instalar la característica Server o Proxy Server, la característica Java Client se selecciona automáticamente para su instalación.

Java Client incluye el kit de herramientas de JNDI de IBM Security Directory Server y los programas de utilidad de Java Client.

64 bits

Puede instalar Server como una característica junto con otras características de IBM Security Directory Server. La característica Server tiene dependencia en las características C Client y Java Client. Al seleccionar la característica Server para su instalación, se seleccionarán las características C Client y Java Client para su instalación.

Server es necesario para crear un servidor de un servidor de directorios completo o un servidor LDAP. Debe configurar un servidor de directorios completo con una instancia de base de datos. Procesa las solicitudes de clientes que requieren acceder a entradas almacenadas en la base de datos. DB2 es obligatorio para un servidor de directorios completo.

Proxy Server

Puede instalar Proxy Server como una característica junto con otras características de IBM Security Directory Server. La característica de Proxy Server tiene dependencia en las características C Client y Java Client. Al seleccionar la característica Proxy Server para su instalación, se seleccionarán las características C Client y Java Client para su instalación.

Proxy Server es un servidor LDAP que actúa como componente frontal para el directorio. Autentica las solicitudes de clientes para todo el directorio y direcciona solicitudes a los servidores de directorios completos. Proxy Server también se puede utilizar en el componente frontal de un clúster de servidor o un directorio distribuido para proporcionar migración tras error y equilibrio de carga.

Herramienta de administración web

Puede instalar la Herramienta de administración web como una característica por sí misma o junto con otras características de IBM Security Directory Server. Herramienta de administración web es una característica opcional necesaria si desea gestionar el servidor de directorios de forma remota. Para utilizar la Herramienta de administración web, debe desplegarla en una versión soportada de WebSphere Application Server incorporado o WebSphere Application Server.

Al instalar la Herramienta de administración web, los archivos de Directory Services Markup Language (DSML) también se copiarán al

sistema. Para obtener más información sobre DSML, consulte el apartado Apéndice A, “Directory Services Markup Language”, en la página 255.

Puede utilizar la Herramienta de administración web como una consola para gestionar servidores de directorios, que pueden ser de los tipos siguientes:

- IBM Security Directory Server, versión 6.3.1
- IBM Security Directory Server, versión 6.3
- IBM Security Directory Server, versión 6.2
- IBM Security Directory Server, versión 6.1
- IBM Security Directory Server, versión 6.0
- i5/OS V5 R4
- z/OS V1 R6 Integrated Security Services
- z/OS V1 R8 Integrated Security Services
- z/OS V1 R8 IBM Tivoli Directory Server
- z/OS V1 R9 IBM Tivoli Directory Server
- z/OS V1 R10 IBM Tivoli Directory Server

Importante: En z/OS, la gestión de los datos de directorio está soportada y no la administración del servidor.

WebSphere Application Server incorporado
Puede instalar WebSphere Application Server incorporado si selecciona instalar la Herramienta de administración web. WebSphere Application Server incorporado sólo es necesario si desea desplegar y ejecutar la Herramienta de administración web. Si se ha instalado una versión soportada de WebSphere Application Server en el sistema, puede elegir no instalar WebSphere Application Server incorporado. Puede desplegar la Herramienta de administración web en un WebSphere Application Server existente o WebSphere Application Server incorporado instalado en el sistema.

Personalización de instalación de IBM Security Directory Server

Puede personalizar la instalación de IBM Security Directory Server para que se ajuste al uso del producto.

Puede categorizar la instalación de IBM Security Directory Server para la siguiente finalidad:

- Producto completo
- Servidor de directorios completo
- Servidor proxy
- 32 bits
- Gestión de servidor remoto con la Herramienta de administración web

Tabla 9. Características de IBM Security Directory Server para la instalación basada en el uso del producto

Todas las características	Servidor de directorios completo	Servidor proxy	32 bits	Gestión de servidor remoto con la Herramienta de administración web
IBM DB2	Sí	No	No	No
IBM Global Security Kit	Sí	Sí	Sí	No
C Client	Sí	Sí	Sí	No
IBM Java Development Kit	Sí	Sí	Sí	No
Java Client	Sí	Sí	Sí	No
64 bits	Sí	No	No	No
Proxy Server	No	Sí	No	No
Herramienta de administración web	Opcional	Opcional	No	Sí

Nota: Si opta por instalar la Herramienta de administración web, IBM Installation Manager proporciona una opción para instalar WebSphere Application Server incorporado.

Puede elegir opcionalmente WebSphere Application Server incorporado y la Herramienta de administración web para la instalación con Servidor de directorios completo y servidor proxy.

Ubicaciones de la instalación predeterminada

Si ejecuta IBM Installation Manager para la instalación, IBM Security Directory Server y el software necesario se instalará en la ubicación predefinida de la instalación.

Tabla 10. La ubicación de instalación predeterminada de IBM Security Directory Server, IBM DB2, WebSphere Application Server incorporado, e IBM Java Development Kit.

Sistema operativo	IBM Security Directory Server	IBM DB2	WebSphere Application Server incorporado	IBM Java Development Kit
Linux	`/opt/ibm/ldap/V6.3.1`	`/opt/ibm/sdsV6.3.1db2`	`/opt/ibm/ldap/V6.3.1/appsrv`	`/opt/ibm/ldap/V6.3.1/java`
AIX	`/opt/IBM/ldap/V6.3.1`	`/opt/IBM/sdsV6.3.1db2`	`/opt/IBM/ldap/V6.3.1/appsrv`	`/opt/IBM/ldap/V6.3.1/java`
Microsoft Windows	`C:\Program Files\IBM\ldap\V6.3.1`	`C:\Program Files\IBM\sdsV6.3.1db2`	`C:\Program Files\IBM\ldap\V6.3.1\appsrv`	`C:\Program Files\IBM\ldap\V6.3.1\java`

IBM Security Directory Server sólo se puede instalar en la ubicación predefinida en los sistemas AIX y Linux. La vía de acceso está especificada de forma

predeterminada en el campo **Directorio de instalación** en IBM Installation Manager. Aunque este campo es editable en IBM Installation Manager, si cambia la vía de acceso que se especifica de forma predeterminada, no podrá pulsar **Siguiente** para continuar con la instalación. Debe volver a la vía de acceso de instalación predeterminada para IBM Security Directory Server.

Esta restricción no se aplica a los sistemas operativos Microsoft Windows. IBM Security Directory Server puede instalarse en cualquier ubicación personalizada de los sistemas operativos Microsoft Windows. Aunque seleccione una ubicación de instalación personalizada para IBM Security Directory Server, el directorio `idsinstinfo` y el archivo `idsinstances.ldif` que contiene siempre se crearán en la partición especificada por `%SystemDrive%`. Si IBM Security Directory Server está instalado en la unidad `E:` y el sistema operativo está en la unidad `C:`, puede observar los cambios siguientes:

- Se creará el directorio `idsinstinfo` en la unidad `C:` (`C:\idsinstinfo`), en lugar de en el directorio `E:\Program Files\IBM\ldap`.

Repositorios de instalación

El repositorio de instalación es la ubicación donde están disponibles los paquetes de IBM Security Directory Server para la instalación.

Puede instalar IBM Security Directory Server desde una de las siguientes ubicaciones:

- Disco de configuración del producto
- Unidad compartida remota o un directorio local que contenga una imagen electrónica del paquete de instalación

Puede utilizar el repositorio para iniciar una instalación de las siguientes formas:

- Utilice el Launchpad para iniciar una instalación desde:
  - Un disco de configuración del producto
  - Una imagen electrónica del paquete de instalación en una unidad compartida remota o un directorio local

  Al utilizar el Launchpad, el proceso de instalación ya se ha configurado con la ubicación del repositorio que contiene el paquete de instalación.
- Inicie IBM Installation Manager directamente y especifique las preferencias del repositorio manualmente. Por ejemplo:
  - El URL para el repositorio en un servidor web
  - La vía de acceso a una unidad compartida remota que contiene el paquete del producto

Inicio de la instalación

Puede iniciar la instalación de IBM Security Directory Server utilizando el Launchpad o utilizando el conjunto de IBM Installation Manager con las preferencias del repositorio.

Inicio de la instalación con el launchpad

El launchpad proporciona una ubicación única para iniciar el proceso de instalación.

Acerca de esta tarea

Puede utilizar el launchpad para iniciar una instalación en los siguientes casos de ejemplo:

- Instalación desde un disco de configuración del producto.
- Instalación desde un directorio local o una unidad compartida remota que contiene una imagen electrónica del paquete de producto.

Al utilizar el launchpad para iniciar la instalación, se instalará automáticamente IBM Installation Manager si no hay una versión soportada en el sistema.

Procedimiento

1. Vaya al directorio raíz del paquete de instalación.
   - Si está utilizando el disco de configuración del producto IBM Security Directory Server, inserte el disco en la unidad de disco.
   - Si está instalando a partir de una imagen electrónica del paquete de instalación del producto, vaya al directorio donde se encuentra la imagen.
2. Inicie el launchpad.

   Nota: Para los sistemas operativos Windows, pulse con el botón derecho del ratón el archivo `.exe` para el launchpad, y seleccione **`Ejecutar como administrador`**.

Sistema operativo	Mandato a ejecutar:
Windows de 32 bits	`launchpad.exe`
Windows de 64 bits	`launchpad64.exe`
AIX y Linux	`./launchpad.sh`

   Se iniciará el launchpad de IBM Security Directory Server y se mostrará la página de Bienvenida.
3. En la página de **Bienvenida**, seleccione el idioma desde la lista **Seleccionar un idioma**, y pulse **Aceptar**.
4. En el área de navegación izquierdo, pulse **IBM Security Directory Server Installation**.
5. En la página **Instalación**, pulse el enlace **Iniciar el instalador de IBM Security Directory Server**. Se iniciará IBM Installation Manager.
6. Asegúrese de que se seleccionan los siguientes paquetes para su instalación:
   - IBM Installation Manager (Sólo aparece listado si una versión soportada aún no está instalada en el sistema).
   - IBM Security Directory Server
7. Continúe con los pasos para instalar IBM Security Directory Server. Consulte el apartado “Instalación con IBM Installation Manager” en la página 31.
8. Tras finalizar la instalación, pulse **Salir**.

Resultados

Al utilizar el launchpad para iniciar la instalación de IBM Security Directory Server, el launchpad creará un archivo temporal, `sds631.temp`, que contiene el nombre de la vía de acceso de soporte. El archivo `sds631.temp` se crea en la siguiente ubicación del sistema operativo:

AIX y Linux
`/tmp`

Microsoft Windows
El directorio temporal predeterminado del conjunto del sistema en la variable *TEMP*.

No puede instalar varias copias de la misma versión de IBM Security Directory Server en el mismo sistema. Al seleccionar el paquete de instalación para la misma versión de nuevo, IBM Installation Manager generará un mensaje de aviso y no podrá continuar con la instalación. Sin embargo, pueden coexistir distintas versiones de IBM Security Directory Server en el mismo sistema.

Qué hacer a continuación

Continúe con los pasos para instalar IBM Security Directory Server. Consulte el apartado "Instalación con IBM Installation Manager" en la página 31.

Inicio de la instalación estableciendo las preferencias de repositorio

Si está instalada en el sistema la versión soportada de IBM Installation Manager, puede iniciarla directamente y especificar las preferencias del repositorio.

Antes de empezar

IBM Installation Manager Versión 1.7.0 y posterior están soportados para la instalación de IBM Security Directory Server. Aparece un mensaje de error en la página Instalar paquetes de IBM Installation Manager y no se podrá seguir con la instalación en los siguientes casos de ejemplo:

- Intente iniciar la instalación de IBM Security Directory Server con una versión anterior de IBM Installation Manager.
- Se ha detectado una versión anterior de IBM Installation Manager al iniciar la instalación de IBM Security Directory Server desde el programa Launchpad.

Si el sistema contiene IBM Installation Manager anterior a la versión 1.7.0, debe actualizar a la versión 1.7.0 o posterior. Puede elegir una de las formas siguientes para instalar la versión necesaria de IBM Installation Manager.

- Inicie la instalación de IBM Installation Manager con el Launchpad. Para obtener más información, consulte el "Inicio de la instalación con el launchpad" en la página 28.
- Descargue IBM Installation Manager, versión 1.7.0 o posterior para su sistema operativo. Para obtener más información acerca de la instalación en modalidad silenciosa de IBM Installation Manager, consulte la documentación de IBM Installation Manager en http://www-01.ibm.com/support/knowledgecenter/SSDV2W/welcome.

Acerca de esta tarea

Puede iniciar la instalación configurando las preferencias del repositorio en los siguientes casos de ejemplo de instalación:

- Instalación desde un directorio local o una unidad compartida remota que contiene el paquete del producto descargado desde IBM Passport Advantage.
- Instalación desde un URL para el repositorio en un servidor web.

Procedimiento

1. Inicie IBM Installation Manager.

   Windows
   Desde el menú **Inicio**, pulse **Todos los programas** > **IBM Installation Manager** > **IBM Installation Manager**.

   AIX y Linux
   Especifique el mandato siguiente en el indicador de mandatos. Modifique la siguiente vía de acceso predeterminada si IBM Installation Manager se ha instalado en una ubicación distinta.

   ```
   /opt/IBM/InstallationManager/eclipse/IBMIM
   ```

2. En la página Inicio de IBM Installation Manager, pulse **Archivo** > **Preferencias**.
3. En la página Repositorios, pulse **Añadir repositorio**.
4. En la página Añadir repositorio, especifique el URL de la ubicación de repositorio o vaya al mismo y establezca una vía de acceso de archivo.
5. Pulse **Aceptar**. Si ha proporcionado un HTTPS o una ubicación de repositorio restringida, se le solicitará que especifique un ID de usuario y una contraseña. Se listará la ubicación de repositorio nueva o modificada.
6. Para verificar el acceso de repositorio, pulse **Probar conexiones**.
7. Pulse **Aceptar** para salir de la página Repositorios.

Resultados

No puede instalar varias copias de la misma versión de IBM Security Directory Server en el mismo sistema. Al seleccionar el paquete de instalación para la misma versión de nuevo, IBM Installation Manager generará un mensaje de aviso y no podrá continuar con la instalación. Sin embargo, pueden coexistir distintas versiones de IBM Security Directory Server en el mismo sistema.

Qué hacer a continuación

Continúe con los pasos para instalar IBM Security Directory Server. Consulte el apartado “Instalación con IBM Installation Manager”.

Instalación con IBM Installation Manager

Complete los pasos para instalar IBM Security Directory Server con IBM Installation Manager.

Antes de empezar

Inicie la instalación.

Procedimiento

1. En la página de Inicio de IBM Installation Manager, pulse **Instalar**.
2. En la página Instalar paquetes, seleccione el paquete de IBM Security Directory Server para la instalación.
3. Pulse **Siguiente**. IBM Installation Manager comprueba los paquetes de requisito previo en el sistema.
4. Si el sistema no cumple la comprobación de requisitos previos, la página **Resultados de validación** mostrará los requisitos previos.
   a. Para verificar si se han cumplido los requisitos previos tras instalar los paquetes de requisitos previos, pulse **Volver a comprobar el estado**. Para

obtener más información sobre los requisitos previos, consulte "Paquetes de requisito previo que son necesarios en diversos sistemas operativos" en la página 15.

b. Si se han cumplido todos los requisitos previos, pulse **Siguiente**.

5. Pulse **Acepto los términos del acuerdo de licencia**, y pulse **Siguiente**. Se mostrará la ubicación del directorio de recursos compartidos.
6. Opcional: Utilice la vía de acceso predeterminada o especifique una vía de acceso en el campo **Directorio de recursos compartidos**. El directorio de recursos compartidos es el directorio donde se almacenan los artefactos de instalación para que los pueda utilizar uno o varios grupos de paquetes de productos. Puede especificar el directorio de recursos compartidos sólo la primera vez que instale un paquete.
7. Pulse **Siguiente**. Se mostrarán el nombre de grupo de paquetes y la ubicación de instalación predeterminada. La opción **Crear un nuevo grupo de paquetes** está seleccionada de forma predeterminada y únicamente esta opción está soportada para la instalación de IBM Security Directory Server. Un grupo de paquetes representa un directorio en el que los paquetes comparten recursos con otros paquetes del mismo grupo. Un grupo de paquetes tiene asignado un nombre automáticamente.

   Restricción:

   IBM Security Directory Server sólo se puede instalar en la ubicación predefinida en los sistemas AIX y Linux. La vía de acceso está especificada de forma predeterminada en el campo **Directorio de instalación** en IBM Installation Manager. Aunque este campo es editable en IBM Installation Manager, si cambia la vía de acceso que se especifica de forma predeterminada, no podrá pulsar **Siguiente** para continuar con la instalación. Debe volver a la vía de acceso de instalación predeterminada para IBM Security Directory Server.

   Para obtener una lista de las ubicaciones de instalación predeterminadas en varios sistemas operativos, consulte "Ubicaciones de la instalación predeterminada" en la página 27.

   Esta restricción no se aplica a los sistemas operativos Microsoft Windows. IBM Security Directory Server puede instalarse en cualquier ubicación personalizada de los sistemas operativos Microsoft Windows. Aunque seleccione una ubicación de instalación personalizada para IBM Security Directory Server, el directorio `idsinstinfo` y el archivo `idsinstances.ldif` que contiene siempre se crearán en la partición especificada por `%SystemDrive%`. Si IBM Security Directory Server está instalado en la unidad `E:` y el sistema operativo está en la unidad `C:`, puede observar los cambios siguientes:

   - Se creará el directorio `idsinstinfo` en la unidad `C:` (`C:\idsinstinfo`), en lugar de en el directorio `E:\Program Files\IBM\ldap`.

8. Pulse **Siguiente**.
9. En la página **Instalar paquetes**, seleccione las características que necesite. Para ver los dependientes de una característica seleccionada o las dependencias de la característica en otras características, marque el recuadro de selección **Mostrar dependencias**.

Tabla 11. Características de IBM Security Directory Server disponibles para su instalación en un paquete de producto completo o de sólo cliente

Todas las características	Dependencias de instalación	Características del paquete del producto completo	Características del paquete de sólo cliente
IBM DB2	Ninguno	Sí	No
IBM Global Security Kit	Ninguno	Sí	Sí
C Client	Ninguno	Sí	Sí
IBM Java Development Kit	Ninguno	Sí	Sí
Java Client	Ninguno	Sí	Sí
64 bits	C Client Java Client	Sí	No
Proxy Server	C Client Java Client	Sí	No
Herramienta de administración web	Ninguno	Sí	No

10. Pulse **Siguiente**.
11. Si selecciona la característica de IBM DB2 para su instalación, pulse **IBM DB2** y, a continuación, realice una de las acciones siguientes:
    - Para instalar IBM DB2, realice las acciones siguientes:
      a. Pulse **Instalar DB2**.
      b. En el campo **Vía de acceso instalable de DB2**, especifique el nombre de la vía de acceso del instalable de DB2. Puede pulsar **Examinar** y especificar la vía de acceso.
      c. En Windows, especifique el ID de usuario del sistema que desee en los grupos `DB2ADMNS` o `DB2USERS` del campo **Nombre de usuario**. Puede utilizar este ID de usuario para ejecutar aplicaciones y herramientas de DB2 locales en el sistema. Si el ID de usuario no existe, el programa de instalación creará la cuenta de usuario.
      d. En Windows, especifique la contraseña para el ID de usuario en la **Contraseña** archivada. Si la contraseña no cumple con la política de contraseñas establecida en el sistema, es posible que falle la instalación.
      e. En Windows, especifique la contraseña para el ID de usuario en **Confirmar contraseña** archivado.
      f. Pulse **Siguiente**.
    - Si el sistema contiene una versión soportada de IBM DB2 instalada en él, realice una de las acciones siguientes:
      a. Para continuar con una versión de IBM DB2 existente, pulse **Continuar con DB2 existente**.

         Importante: Si elige continuar con DB2 existente durante la instalación, IBM Installation Manager actualizará su registro con la entrada de características de DB2.
      b. En la lista, seleccione una versión soportada de DB2 que desee utilizar con IBM Security Directory Server.
      c. Pulse **Siguiente**.

12. Si selecciona la característica de IBM Global Security Kit para la instalación, pulse **IBM Global Security Kit** y, a continuación, realice una de las acciones siguientes:
    - Si el sistema no contiene GSKit, versión 8.0 o posterior instalado en él, realice las acciones siguientes:
        a. Pulse **Instalar GSKit**.
        b. En el campo **Vía de acceso instalable de GSKit**, especifique el nombre de la vía de acceso del instalable de GSKit. Puede pulsar **Examinar** y especificar la vía de acceso.

           Nota: La vía de acceso que especifique debe contener el instalable de GSKit de 64 bits y de 32 bits.
        c. Pulse **Siguiente**.
    - Si el sistema contiene GSKit, versión 8.0 o posterior instalado en él, realice una de las acciones siguientes:
        a. Para continuar con una versión existente de GSKit, pulse **Continuar con el GSKit existente**.

           Importante: Si elige continuar con el GSKit existente durante la instalación, IBM Installation Manager actualizará su registro con la entrada de características de GSKit.
        b. Pulse **Siguiente**.
13. Si selecciona la característica de IBM Java Development Kit para la instalación, pulse **IBM Java Development Kit**, y complete los pasos siguientes:
    a. En el campo **IBM Java Development Kit**, especifique el nombre de archivo con el nombre de la vía de acceso del archivo comprimido JDK. Puede pulsar **Examinar** y especificar la vía de acceso.
    b. Pulse **Siguiente**.
14. Si selecciona la característica Herramienta de administración web para la instalación, pulse la **Herramienta de administración web**, y realice los pasos siguientes:
    a. Para instalar WebSphere Application Server incorporado, realice las acciones siguientes:
        1) Seleccione **Instalar WebSphere Application Server incorporado**.
        2) En el campo **Vía de acceso instalable de WebSphere Application Server incorporado**, especifique el nombre de la vía de acceso del instalable de WebSphere Application Server incorporado. Puede pulsar **Examinar** y especificar la vía de acceso.
    b. Para desplegar la Herramienta de administración web, realice una de las acciones siguientes:
        - Para desplegar el WebSphere Application Server incorporado que se encuentra en la vía de acceso de instalación predeterminada, pulse **Desplegar en el WebSphere Application Server incorporado predeterminado**.

          Nota: Si existe una versión anterior de la Herramienta de administración web, el programa de instalación la migrará a la versión actual si se cumplen las condiciones siguientes:
            1) Están instaladas la versión anterior de la Herramienta de administración web y WebSphere Application Server incorporado en la vía de acceso de instalación predeterminada.

2) Está desplegada la versión anterior de la Herramienta de administración web en WebSphere Application Server incorporado que se encuentra en la vía de acceso de instalación predeterminada.
3) Herramienta de administración web que se proporciona con IBM Security Directory Server, versión 6.1, 6.2, o 6.3 están soportados para la migración.

- Para desplegar en el WebSphere Application Server o en el WebSphere Application Server incorporado que se encuentra en una vía de acceso de instalación personalizada, pulse **Desplegar en un WebSphere Application Server existente**.
  1) En el campo **Vía de acceso de instalación de WebSphere Application Server o WebSphere Application Server incorporado**, especifique la vía de acceso de instalación de un servidor de aplicaciones web existente.
- Para desplegar la Herramienta de administración web más adelante en un servidor de aplicaciones web soportado, pulse **Desplegar manualmente más tarde**.

15. Pulse **Siguiente**. Se mostrará la información de resumen de preinstalación, que incluye la ubicación de instalación, la lista de paquetes, y la información del repositorio.
16. Verifique la información de resumen, y pulse **Instalar**. Se iniciará la instalación y se mostrará una barra de progreso. Tras la instalación, se mostrará la página de resumen posterior a la instalación.
17. Pulse el enlace **Ver archivo de registro** para verificar que ha instalación ha sido satisfactoria. Para obtener más información, consulte el Capítulo 5, "Archivos de registro de IBM Installation Manager", en la página 45.
18. Para iniciar uno de los programas siguientes, realice una de las siguientes acciones:
    - Para iniciar Herramienta de administración de instancias, pulse **Herramienta de administración de instancias (idsxinst)**.
    - Si no desea iniciar ningún programa, pulse **Ninguno**.
19. Pulse **Finalizar**.
20. Pulse **Archivo** > **Salir**.

Resultados

Si la instalación se ha realizado correctamente, se instalará IBM Security Directory Server en la ubicación de instalación. Para obtener más información sobre la ubicación de instalación predeterminada, consulte "Ubicaciones de la instalación predeterminada" en la página 27. Si la instalación no se realiza correctamente para ninguna de las características seleccionadas, se retrotraerá la instalación de los paquetes de IBM Security Directory Server.

Qué hacer a continuación

Tras la instalación de IBM Security Directory Server, debe realizar las siguientes acciones:

- Para utilizar IBM Security Directory Server como un servidor de directorios completo, cree una instancia de servidor de directorios. Para obtener más información, consulte el "Creación de la instancia de servidor de directorios predeterminada" en la página 137.

- Para utilizar IBM Security Directory Server como un servidor proxy, cree una instancia de servidor proxy. Para obtener más información, consulte el “Creación de una instancia de servidor proxy con valores personalizados” en la página 147.

Instalación en modalidad silenciosa

Puede utilizar la instalación en modalidad silenciosa para instalar IBM Security Directory Server en varios sistemas sin ninguna intervención manual.

Para la instalación en modalidad silenciosa, debe completar las actividades siguientes:

1. Instale IBM Installation Manager, si no está presente.
2. Utilice el archivo de respuestas predeterminado o grabe un archivo de respuestas personalizado.
3. Instale los paquetes.

Archivo de respuestas para la instalación silenciosa

En la instalación de modalidad silenciosa, la interfaz de usuario no está disponible. El archivo de respuestas sirve como entrada para la instalación. Un archivo de respuestas es un archivo XML que contiene los datos necesarios para completar la instalación silenciosa.

Grabación de un archivo de respuestas personalizado

Puede grabar un archivo de respuestas para las siguientes tareas:

- Instalación de paquetes
- Modificación de paquetes
- Desinstalación de paquetes

Para grabar un archivo de respuestas, debe grabar las preferencias y las acciones de instalación con IBM Installation Manager en la modalidad de interfaz de usuario. Cuando grabe por primera vez un archivo de respuestas para la instalación silenciosa, puede elegir no instalar los paquetes con el parámetro **-skipInstall** *agentDataLocation*.

La ubicación *agentDataLocation* almacena los datos para instalar el producto. Para grabar un archivo de respuestas para la modificación silenciosa o la desinstalación del producto, debe utilizar la misma ubicación *agentDataLocation* con el parámetro **-skipInstall** .

Para varios casos de ejemplo de instalación, debe grabar distintos archivos de respuestas con una ubicación *agentDataLocation* distinta para cada caso de ejemplo.

Para obtener más información acerca de cómo registrar un archivo de respuestas para la instalación silenciosa, consulte la documentación de IBM Installation Manager en http://www-01.ibm.com/support/knowledgecenter/SSDV2W/welcome.

Verificación de la instalación silenciosa

Una vez que se haya completado la instalación, debe verificar la instalación silenciosa. Puede verificar la instalación de una de las formas siguientes:

- Comprobación de los códigos de retorno
- Comprobación del archivo de registro
- Comprobación de los paquetes

Instalación silenciosa con un archivo de respuestas

Utilice la instalación silenciosa de IBM Security Directory Server para instalar los paquetes necesarios sin ninguna intervención manual.

Antes de empezar

IBM Installation Manager, versión 1.7.0 o posterior es necesario para la instalación silenciosa de los paquetes de IBM Security Directory Server.

Acerca de esta tarea

Puede utilizar el archivo de respuestas predeterminado o registrar un archivo de respuestas personalizado y utilizarlo como el archivo de entrada para la instalación silenciosa.

Procedimiento

1. Inicie sesión en el sistema como administrador.
2. Acceda al mandato **IBMIM** en la ubicación de instalación de IBM Installation Manager.

Sistema operativo	Ubicación predeterminada del mandato IBMIM:
Microsoft Windows	`C:\Program Files\IBM\InstallationManager\eclipse`
AIX y Linux	`/opt/IBM/InstallationManager/eclipse`

3. Opcional: Ejecute el mandato **IBMIM** para registrar un archivo de respuestas para la instalación.

   Consejo: Puede utilizar el archivo de respuestas de ejemplo para la instalación. Consulte la ubicación predeterminada del archivo de respuestas de ejemplo, "Instalación en modalidad silenciosa" en la página 36.

   a. Para registrar los pasos de instalación sin instalar el producto, ejecute los mandatos siguientes en varios sistemas operativos:

      Microsoft Windows

      ```
      IBMIM.exe -record nombre_vía_acceso\responseFile.xml
      -skipInstall UbicaciónDatosagente
      ```

      AIX y Linux

      ```
      ./IBMIM -record nombre_vía_acceso/responseFile.xml
      -skipInstall UbicaciónDatosagente
      ```

      El mandato abrirá IBM Installation Manager.

   b. Configure el repositorio de IBM Security Directory Server. Para obtener más información, consulte 2 en la página 31

   c. Complete el registro de instalación de IBM Security Directory Server. Para obtener más información, consulte "Instalación con IBM Installation Manager" en la página 31

4. Ejecute el mandato **imcl** para iniciar la instalación silenciosa con el archivo de respuestas como entrada. El mandato **imcl** debe estar presente en *<dir_instalación_IBM_Installation_Manager>*/eclipse/tools.

Sistema operativo	Mandato a ejecutar:
Microsoft Windows	`imcl.exe input` *`nombre_vía_acceso`*`\` *`responseFile.xml`* `-acceptLicense -showProgess`
AIX y Linux	`./imcl input` *`nombre_vía_acceso`*`/` *`responseFile.xml`* `-acceptLicense -showProgess`

Nota: Existen muchos otros parámetros que se pueden utilizar junto con el mandato **imcl**. Para obtener información detallada, consulte la ayuda del mandato **imcl**.

5. Verifique el resumen de instalación y los archivos de registro.

Sistema operativo	Vía de acceso de registro predeterminado:
Microsoft Windows	`C:\ProgramData\IBM\InstallationManager\logs`
AIX y Linux	`/var/ibm/InstallationManager/logs/`

6. Verifique si los paquetes de IBM Security Directory Server se encuentran en el nivel necesario.

Sistema operativo	Verificación de paquetes:
Microsoft Windows	Consulte el apartado "Verificación de las características de IBM Security Directory Server con IBM Installation Manager" en la página 85.
AIX y Linux	Consulte el apartado "Verificación de las características de IBM Security Directory Server con IBM Installation Manager" en la página 85.

Resultados

Si la instalación es satisfactoria, IBM Security Directory Server se instalará en la ubicación de instalación de IBM Security Directory Server. Para obtener más información sobre la ubicación de instalación predeterminada, consulte "Ubicaciones de la instalación predeterminada" en la página 27. Si la instalación no se realiza correctamente para ninguna de las características seleccionadas, se retrotraerá la instalación de los paquetes de IBM Security Directory Server.

Qué hacer a continuación

Nota: Si selecciona Herramienta de administración de instancias para abrir al registrar el archivo de respuestas para su instalación, Herramienta de administración de instancias no se abrirá tras la instalación silenciosa de IBM Security Directory Server.

Si ha seleccionado la característica de Server o Proxy Server para su instalación, abra Herramienta de administración de instancias para crear una instancia de servidor de directorios o una instancia de servidor proxy. Consulte el apartado "Inicio de Herramienta de administración de instancias" en la página 134.

Capítulo 4. Modificación con IBM Installation Manager

Puede instalar características de IBM Security Directory Server que no ha instalado anteriormente, desinstalar características que ya ha instalado, o ambos, con IBM Installation Manager.

No puede eliminar una característica si es un requisito previo para otras características instaladas. Puede eliminar una dependencia sólo si están seleccionadas todas las características dependientes para la eliminación o están eliminadas.

Importante: Si elige continuar con una versión existente de un DB2 o GSKit durante la instalación, IBM Installation Manager actualiza su registro con la entrada de características. Si elimina una característica que se ha instalado con la opción **Continuar con el existente**, Installation Manager realiza las siguientes acciones:

- Elimina la entrada de característica desde el registro de IBM Installation Manager.
- No desinstala la característica del sistema.

Modificación de características con IBM Installation Manager

Complete los pasos para modificar las características de IBM Security Directory Server con IBM Installation Manager.

Antes de empezar

Debe detener todos los procesos del cliente y del servidor de IBM Security Directory Server.

- Servidor de directorios
- Servidor de administración
- Rastreos de LDAP
- Aplicaciones LDAP personalizadas

Si alguno de los procesos está en uso, no se podrán eliminar los programas ni las bibliotecas.

Procedimiento

1. Inicie IBM Installation Manager.
   - AIX y Linux:
     a. Abra una ventana de línea de mandatos y vaya al directorio que contiene IBM Installation Manager. El siguiente directorio es la ubicación de instalación predeterminada de IBM Installation Manager:
        `opt/IBM/InstallationManager/eclipse`
     b. Ejecute el siguiente mandato:
        `./IBMIM`
   - Microsoft Windows:
     a. Pulse **Inicio** > **Todos los programas** > **IBM Installation Manager** > **IBM Installation Manager**.

2. Pulse **Modificar**.
3. Seleccione **IBM Security Directory Server**, y, a continuación, pulse **Siguiente**.
4. En la página **Modificar paquetes**, debe realizar las acciones siguientes:
   a. Seleccione las características que desee instalar.
   b. Borre las características que desee desinstalar.

Tabla 12. Características de IBM Security Directory Server disponibles para las modificaciones en paquetes de producto completo y de sólo cliente

Todas las características	Dependencias de instalación	Características del paquete del producto completo	Características del paquete de sólo cliente
IBM DB2	Ninguno	Sí	No
IBM Global Security Kit	Ninguno	Sí	Sí
C Client	Ninguno	Sí	Sí
IBM Java Development Kit	Ninguno	Sí	Sí
Java Client	Ninguno	Sí	Sí
64 bits	C Client Java Client	Sí	No
Proxy Server	C Client Java Client	Sí	No
Herramienta de administración web	Ninguno	Sí	No

Importante: Si elige continuar con una versión existente de un DB2 o GSKit durante la instalación, IBM Installation Manager actualiza su registro con la entrada de características. Si elimina una característica que se ha instalado con la opción **Continuar con el existente**, Installation Manager realiza las siguientes acciones:

- Elimina la entrada de característica desde el registro de IBM Installation Manager.
- No desinstala la característica del sistema.

Si existen las instancias de DB2 que ha creado con la copia de DB2 instalada con IBM Installation Manager, no podrá eliminar IBM DB2. En tal situación, deberá eliminar manualmente las instancias de DB2 e intentarlo de nuevo. Es recomendable realizar la copia de seguridad de la base de datos antes de eliminar las instancias de DB2.

   c. Pulse **Siguiente**.
5. Si selecciona la característica de IBM DB2 para su instalación, pulse **IBM DB2** y, a continuación, realice una de las acciones siguientes:
   - Para instalar IBM DB2, realice las acciones siguientes:
     a. Pulse **Instalar DB2**.
     b. En el campo **Vía de acceso instalable de DB2**, especifique el nombre de la vía de acceso del instalable de DB2. Puede pulsar **Examinar** y especificar la vía de acceso.
     c. En Windows, especifique el ID de usuario del sistema que desee en los grupos `DB2ADMNS` o `DB2USERS` del campo **Nombre de usuario**. Puede utilizar este ID de usuario para ejecutar aplicaciones y herramientas de

DB2 locales en el sistema. Si el ID de usuario no existe, el programa de instalación creará la cuenta de usuario.

d. En Windows, especifique la contraseña para el ID de usuario en la **Contraseña** archivada. Si la contraseña no cumple con la política de contraseñas establecida en el sistema, es posible que falle la instalación.

e. En Windows, especifique la contraseña para el ID de usuario en **Confirmar contraseña** archivado.

f. Pulse **Siguiente**.

- Si el sistema contiene una versión soportada de IBM DB2 instalada en él, siga estos pasos:

  a. Para continuar con una versión de IBM DB2 existente, pulse **Continuar con DB2 existente**.

     Importante: Si elige continuar con DB2 existente durante la instalación, IBM Installation Manager actualizará su registro con la entrada de características de DB2.

  b. En la lista, seleccione una versión soportada de DB2 que desee utilizar con IBM Security Directory Server.

  c. Pulse **Siguiente**.

6. Si selecciona la característica de IBM Global Security Kit para la instalación, pulse **IBM Global Security Kit** y, a continuación, realice una de las acciones siguientes:

   - Si el sistema no contiene GSKit, versión 8.0 o posterior instalado en él, siga estos pasos:

     a. Pulse **Instalar GSKit**.

     b. En el campo **Vía de acceso instalable de GSKit**, especifique el nombre de la vía de acceso del instalable de GSKit. Puede pulsar **Examinar** y especificar la vía de acceso.

        Nota: La vía de acceso que especifique debe contener el instalable de GSKit de 64 bits y de 32 bits.

     c. Pulse **Siguiente**.

   - Si el sistema contiene GSKit, versión 8.0 o posterior instalado en él, siga estos pasos:

     a. Para continuar con una versión existente de GSKit, pulse **Continuar con el GSKit existente**.

        Importante: Si elige continuar con el GSKit existente durante la instalación, IBM Installation Manager actualizará su registro con la entrada de características de GSKit.

     b. Pulse **Siguiente**.

7. Si selecciona la característica de IBM Java Development Kit para la instalación, pulse **IBM Java Development Kit**, y complete los pasos siguientes:

   a. En el campo **IBM Java Development Kit**, especifique el nombre de archivo con el nombre de la vía de acceso del archivo comprimido JDK. Puede pulsar **Examinar** y especificar la vía de acceso.

   b. Pulse **Siguiente**.

8. Si ha seleccionado la característica Herramienta de administración web para la instalación, pulse la **Herramienta de administración web** y siga estos pasos:

   a. Para instalar WebSphere Application Server incorporado, realice las acciones siguientes:

1) Seleccione **Instalar WebSphere Application Server incorporado**.
2) En el campo **Vía de acceso instalable de WebSphere Application Server incorporado**, especifique el nombre de la vía de acceso del instalable de WebSphere Application Server incorporado. Puede pulsar **Examinar** y especificar la vía de acceso.

b. Para desplegar la Herramienta de administración web, realice una de las acciones siguientes:
   - Para desplegar el WebSphere Application Server incorporado que se encuentra en la vía de acceso de instalación predeterminada, pulse **Desplegar en el WebSphere Application Server incorporado predeterminado**.

     Nota: Si existe una versión anterior de la Herramienta de administración web, el programa de instalación la migrará a la versión actual si se cumplen las condiciones siguientes:
     1) Están instaladas la versión anterior de la Herramienta de administración web y WebSphere Application Server incorporado en la vía de acceso de instalación predeterminada.
     2) Está desplegada la versión anterior de la Herramienta de administración web en WebSphere Application Server incorporado que se encuentra en la vía de acceso de instalación predeterminada.
     3) Herramienta de administración web que se proporciona con IBM Security Directory Server, versión 6.1, 6.2, o 6.3 están soportados para la migración.
   - Para desplegar en el WebSphere Application Server o en el WebSphere Application Server incorporado que se encuentra en una vía de acceso de instalación personalizada, pulse **Desplegar en un WebSphere Application Server existente**.
     1) En el campo **Vía de acceso de instalación de WebSphere Application Server o WebSphere Application Server incorporado**, especifique la vía de acceso de instalación de un servidor de aplicaciones web existente.
   - Para desplegar la Herramienta de administración web más adelante en un servidor de aplicaciones web soportado, pulse **Desplegar manualmente más tarde**.

9. Pulse **Siguiente**.

   Importante: Si elige continuar con una versión existente de un DB2 o GSKit durante la instalación, IBM Installation Manager actualiza su registro con la entrada de características. Si elimina una característica que se ha instalado con la opción **Continuar con el existente**, Installation Manager realiza las siguientes acciones:
   - Elimina la entrada de característica desde el registro de IBM Installation Manager.
   - No desinstala la característica del sistema.

10. Verifique la información de resumen y pulse **Modificar**.
11. Opcional: Si se produce un error durante la modificación, pulse **Ver archivo de registro** para leer los detalles. Para obtener más información, consulte el Capítulo 5, “Archivos de registro de IBM Installation Manager”, en la página 45.
12. Pulse **Finalizar**.
13. Pulse **Archivo** > **Salir**.

Resultados

Si la modificación es satisfactoria, podrá observar el siguiente cambio:

- Las características de IBM Security Directory Server que ha seleccionado añadir se instalarán en la ubicación de instalación. Para obtener más información sobre la ubicación de instalación predeterminada, consulte "Ubicaciones de la instalación predeterminada" en la página 27.
- Las características de IBM Security Directory Server que ha seleccionado eliminar se desinstalarán.

Capítulo 5. Archivos de registro de IBM Installation Manager

Puede verificar la instalación, la modificación, o la desinstalación de IBM Security Directory Server y de sus componentes comprobando el archivo de registro que crea IBM Installation Manager.

Si se produce un error durante la instalación, modificación, o desinstalación de IBM Security Directory Server y de sus componentes, debe comprobar los archivos de registro. IBM Installation Manager crea los archivos de registro en la ubicación predeterminada.

Tabla 13. La ubicación predeterminada de los archivos de registro de IBM Installation Manager en varios sistemas operativos

Sistema operativo	**Ubicación de registro predeterminada de IBM Installation Manager**
AIX y Linux	`/var/ibm/InstallationManager/logs`
Microsoft Windows	`C:\ProgramData\IBM\InstallationManager\logs`

Las ubicaciones predeterminadas son aplicables a todas las versiones soportadas de AIX, Linux, y Microsoft Windows.

Capítulo 6. Consulta de paquetes de IBM Security Directory Server

Verifique los paquetes de IBM Security Directory Server consultando los paquetes de IBM Security Directory Server en plataformas soportadas.

Acerca de esta tarea

Después de instalar los paquetes de IBM Security Directory Server, debe asegurarse de que los paquetes se encuentren en el nivel requerido. Esta tarea le ayuda a consultar el número de versión de los paquetes de IBM Security Directory Server instalados.

Procedimiento

Inicie sesión en el sistema en el que ha instalado los paquetes de IBM Security Directory Server y ejecute los mandatos con privilegios root.

- En sistemas AIX: Ejecute el mandato **lslpp**. Por ejemplo:
  ```
  lslpp -l 'idsldap*'
  ```
- En sistemas Linux: Ejecute el mandato **rpm**. Por ejemplo:
  ```
  rpm -qa | grep idsldap
  ```
- En los sistemas Solaris:
  1. Para listar los paquetes instalados, ejecute el mandato **pkginfo**. Por ejemplo:
     ```
     pkginfo | grep IDSl
     ```
  2. Para consultar la versión de un paquete concreto de IBM Security Directory Server, ejecute el mandato **pkgparam**. Por ejemplo:
     ```
     pkgparam IDSlbc63 VERSION
     ```
- En sistemas HP-UX (Itanium): Ejecute el mandato **swlist**. Por ejemplo:
  ```
  swlist | grep idsldap
  ```

Capítulo 7. Instalación y configuración nativa mediante scripts

Puede instalar y configurar IBM Security Directory Server utilizando scripts.

Hoja de ruta de instalación

Utilice la hoja de ruta para instalar IBM Security Directory Server en sistemas Linux x86, Linux i/pSeries, Linux s390, Solaris y HP-UX.

1. Asegúrese de que su sistema cumple con los requisitos mínimos de hardware y software. Para obtener más información, consulte el tema *Requisitos del sistema* en la sección Visión general del producto de la documentación de IBM Security Directory Server.
2. Instale el software de requisito previo, por ejemplo, DB2. Si todavía no se ha instalado, asegúrese de que la vía de acceso a DB2 instalable está accesible y de que tiene los permisos necesarios.
3. Si tiene previsto utilizar cualquiera de las características siguientes, debe instalar el software de requisito previo opcional. Si todavía no se ha instalado, asegúrese de que la vía de acceso al software de requisito previo opcional está accesible y de que tiene los permisos necesarios.
   - Para utilizar la herramienta de administración web, se requiere una versión de WebSphere Application Server incorporado o de WebSphere Application Server. Asimismo, se requiere una versión del navegador soportada.
   - Para el cifrado de SSL (Secure Socket Layer) o TLS (Transport Layer Security), se requiere una versión soportada de IBM Global Security Kit (GSKit).
4. En sistemas Linux x86, Linux i/pSeries, Linux s390, Solaris y HP-UX utilice el programa de instalación **idsNativeInstall** para instalar los paquetes de IBM Security Directory Server y otro software necesario.
5. Después de instalar IBM Security Directory Server, utilice el mandato **idsdefinst** para crear y configurar una instancia del servidor de directorios.
6. Inicie la instancia de servidor de directorios.
7. Cargue el archivo LDIF de ejemplo en la base de datos. Consulte la sección Administración de la documentación de IBM Security Directory Server para obtener información acerca de cómo utilizar la instancia del servidor de directorios.

Nota: El script de instalación nativo, **idsNativeInstall**, no se proporciona para los sistemas operativos Windows, AIX y Linux x86_64 (64 bits). Utilice IBM Installation Manager o los programas de utilidad de línea de mandatos del sistema operativo para instalar manualmente en estos sistemas operativos.

Instalación de los paquetes de IBM Security Directory Server en las plataformas Linux, Solaris y HP-UX

Utilice los pasos que se proporcionan para instalar o actualizar paquetes de IBM Security Directory Server en sistemas Linux x86, Linux i/pSeries, Linux s390, Solaris y HP-UX.

Antes de empezar

Antes de comenzar la instalación de los paquetes de IBM Security Directory Server, debe realizar los pasos siguientes:

1. Inicie sesión en el sistema con privilegios root.
2. Extraiga el archivo de archivado de IBM Security Directory Server Versión 6.3.1 en un directorio, por ejemplo, `/sdsV6.3.1`, con espacio de disco adecuado.
3. Detenga todos los procesos de cliente y servidor de IBM Security Directory Server, incluidos el servidor de directorios, el servidor de administración y las aplicaciones LDAP personalizadas. Los programas y bibliotecas no se pueden sustituir mientras se estén utilizando. Si está establecido el rastreo, ejecute `ldtrc off` para detener el proceso de rastreo. Consulte la sección "Tareas básicas de administración del servidor" y la sección "Servidor de administración de directorios" en la sección *Administración* de la documentación de IBM Security Directory Server para obtener las instrucciones acerca de cómo detener las instancias del servidor de directorios y de los servidores de administración.

Acerca de esta tarea

Utilice el mandato **idsNativeInstall** para instalar o actualizar paquetes de IBM Security Directory Server en sistemas Linux x86, Linux i/pSeries, Linux s390, Solaris y HP-UX. También puede utilizar el mandato **idsNativeInstall** para instalar opcionalmente DB2, GSKit y WebSphere Application Server incorporado, si todavía no están instalados en su sistema.

Nota:

- El script de instalación nativo, **idsNativeInstall**, no se proporciona para los sistemas operativos Windows, AIX y Linux x86_64 (64 bits). Utilice IBM Installation Manager o los programas de utilidad de línea de mandatos del sistema operativo para instalar manualmente en estos sistemas operativos.
- En los sistemas HP-UX, los paquetes solo de cliente de IBM Security Directory Server están disponibles para su instalación o actualización.

Procedimiento

1. Vaya al directorio con el programa de instalación de **idsNativeInstall** y el archivo `responseFile.txt`. Los archivos `idsNativeInstall` y `responseFile.txt` deben estar presentes en el mismo directorio.
2. Actualice el archivo `responseFile.txt` para las entradas siguientes. De forma predeterminada, los valores de las variables de instalación de características se establecen en `false` y sus variables de vía de acceso correspondientes no se establecen.
   - Para instalar DB2, establezca la variable *db2FeatureInstall* en `true` y actualice la variable *db2InstallimagePath* con la vía de acceso absoluta de DB2 instalable. Por ejemplo:

     ```
     db2FeatureInstall=true
     db2InstallimagePath=/sdsV6.3.1/db2
     ```

     Importante: Para el servidor de directorios completos, DB2 debe estar instalada en el sistema. Si establece las variables de DB2, *db2FeatureInstall* y *db2InstallimagePath*, entonces DB2 se instala en `/opt/ibm/sdsV6.3.1db2` en Linux o `/opt/IBM/sdsV6.3.1db2` en Solaris. Si ya está instalada una versión de DB2 en la ubicación especificada, la instalación sobrescribe los archivos existentes.

- Para instalar GSKit, establezca la variable *gskitFeatureInstall* en `true` y actualice la variable *gskitInstallimagePath* con la vía de acceso absoluta del GSKit instalable. Por ejemplo:

  ```
  gskitFeatureInstall=true
  gskitInstallimagePath=/sdsV6.3.1/gskit
  ```

  Importante: Para configurar una instancia de servidor de directorios que se comunique a través de SSL o TLS, se debe instalar en el sistema una versión necesaria de GSKit.
- Para instalar IBM Java Development Kit, establezca la variable *JDKFeatureInstall* en `true` y actualice la variable *JDKInstallimagePath* con la vía de acceso absoluta de IBM Java Development Kit instalable. Por ejemplo:

  ```
  JDKFeatureInstall=true
  JDKInstallimagePath=/sdsV6.3.1/java/ibm-java-16sr14-linux-i386.tar
  ```

  IBM Java Development Kit se instala en `/opt/ibm/ldap/V6.3.1/java` en sistemas Linux y Solaris.
- Para instalar la versión de WebSphere Application Server incorporada, establezca la variable *eWasFeatureInstall* en `true` y actualice la variable *eWasInstallimagePath* con la vía de acceso absoluta de la versión incorporada de WebSphere Application Server instalable. Por ejemplo:

  ```
  eWasFeatureInstall=true
  eWasInstallimagePath=/sdsV6.3.1/appsrv
  ```

  La versión incluida de WebSphere Application Server se instala en `/opt/ibm/ldap/V6.3/appsrv` en sistemas Linux y Solaris.
- Para instalar IBM Security Directory Server Versión 6.3.1 GA (General Availability), actualice la variable *tdsInstallimagePath* con la vía de acceso absoluta de IBM Security Directory Server Versión 6.3.1 GA instalable. Por ejemplo:

  ```
  tdsInstallimagePath=/sdsV6.3.1
  ```

  Si especifica `/sdsV6.3.1` como su ubicación instalable de IBM Security Directory Server Versión 6.3.1, asegúrese de que los archivos siguientes estén presentes en el directorio `/sdsV6.3.1`.

  ```
  idsinstall
  idsinstall_i
  ids_detectGskitVersion
  ```

  Los paquetes de IBM Security Directory Server Versión 6.3.1 deben estar presentes en el directorio `/sdsV6.3.1/tdsfiles`.

3. Ejecute el mandato **`idsNativeInstall`** en el indicador de mandatos.

Resultados

Una vez ejecutado el mandato **`idsNativeInstall`**, se instalan los paquetes de IBM Security Directory Server 6.3.1. El mandato **`idsNativeInstall`** también instala DB2, GSKit, IBM Java Development Kit o WebSphere Application Server incorporado basándose en los valores del archivo de respuestas.

Nota: Si IBM Security Directory Server Versión 6.3.1 no está instalado en el sistema, entonces se instalan todos los componentes de IBM Security Directory Server Versión 6.3.1. IBM Security Directory Server Versión 6.3.1 se instala en `/opt/ibm/ldap/V6.3.1/` en sistemas Linux, Solaris y HP-UX.

Qué hacer a continuación

Después de instalar IBM Security Directory Server, debe comprobar si se han instalado los paquetes de IBM Security Directory Server. Para obtener más información acerca de cómo comprobar los registros, consulte "Verificación de los registros de instalación".

Verificación de los registros de instalación

Determine el archivo de registro que debe comprobar para verificar el estado de instalación en sistemas Linux x86, Linux i/pSeries, Linux s390, Solaris y HP-UX.

Una vez finalizada la instalación, el mandato **idsNativeInstall** muestra los mensajes adecuados que indican si la instalación se ha realizado correctamente o no. Para verificar si se han instalado los paquetes de IBM Security Directory Server, compruebe en el archivo de registro los registros de instalación.

El archivo de registro es `/var/idsldap/V6.3/idsNativeInstall_`*`indicación_fecha_y_hora`*`.log`.

Después de verificar el registro de instalación, asegúrese de que todos los paquetes se hayan instalado correctamente y estén en el nivel necesario. Para obtener más información acerca de cómo consultar el número de versión de los paquetes instalados, consulte Capítulo 6, "Consulta de paquetes de IBM Security Directory Server", en la página 47.

Capítulo 8. Instalación de IBM DB2

Para crear una instancia de IBM Security Directory Server con una base de datos de DB2 configurada con el mismo, el sistema debe contener una versión soportada de IBM DB2 instalado.

El soporte de instalación de IBM Security Directory Server proporciona una versión soportada de IBM DB2. Si está utilizando los programas de utilidad del sistema operativo para la instalación de IBM Security Directory Server, debe completar la instalación de IBM DB2. Al ejecutar la instalación de IBM Security Directory Server, se actualizarán los archivos de propiedades con los detalles de la versión soportada de IBM DB2. Si el sistema contiene una versión soportada de IBM DB2 instalada en el mismo, puede utilizar DB2 y configurarlo con la instancia de servidor de directorios. Para obtener más información sobre la actualización del archivo `ldapdb.properties`, consulte Apéndice C, "Actualización del archivo `ldapdb.properties` manualmente", en la página 259.

Para instalar IBM DB2, acceda al soporte de instalación de IBM Security Directory Server y vaya al directorio que contiene el instalable de IBM DB2.

Debe cumplir los requisitos previos de DB2 antes de ejecutar la instalación de IBM DB2. Para verificar si el sistema cumple la comprobación de requisitos previos de DB2, ejecute el mandato **db2prereqcheck**. Si falta algún paquete en el sistema, debe actualizar el sistema para los paquetes necesarios.

En AIX, Linux, y Solaris, puede utilizar el mandato **db2_install** para la instalación de IBM DB2. En Windows, utilice el mandato **setup.exe** para la instalación de IBM DB2.

En System x Linux en la arquitectura de 32 bits de Intel, debe elegir Workspace Server Edition especificando WSE. Para otros sistemas operativos soportados, elija Enterprise Server Edition especificando ESE.

Tras la instalación de IBM DB2, compruebe el archivo `/tmp/db2_install_log.`*XXXXX* para verificar que la instalación ha sido satisfactoria. *XXXXX* es un número aleatorio asociado con la instalación.

Para obtener más información acerca de los requisitos previos de DB2 y de la instalación de IBM DB2, consulte la documentación del producto IBM DB2 en http://www-01.ibm.com/support/knowledgecenter/SSEPGG/welcome.

Parámetros de kernel en sistemas Solaris

En sistemas Solaris, es posible que sea necesario actualizar los parámetros de kernel en el archivo `/etc/system` antes de la instalación de IBM DB2. Puede utilizar el mandato **db2osconf** para determinar los valores de parámetros correctos de kernel para el sistema. Puede utilizar el mandato **projmod** para configurar los valores de parámetros de kernel de Solaris antes de la instalación de DB2 en Solaris.

En un sistema Solaris con zonas configuradas, el mandato **db2osconf** sólo se podrá ejecutar desde la zona global en Solaris.

Para obtener más información acerca del mandato **db2osconf**, busque db2osconf en la documentación del producto IBM DB2 en http://www-01.ibm.com/support/knowledgecenter/SSEPGG/welcome.

Capítulo 9. IBM Java Development Kit for IBM Security Directory Server

Para compilar programas de ejemplo de Java, y para ejecutar programas de Java, como por ejemplo Herramienta de administración de instancias y Herramienta de configuración, debe descomprimir IBM Java Development Kit en la ubicación de instalación de IBM Security Directory Server.

El soporte de instalación de IBM Security Directory Server proporciona una versión soportada de IBM Java Development Kit, IBM Java 1.6 SR 14. Si está utilizando los programas de utilidad del sistema operativo para la instalación de IBM Security Directory Server, debe completar la instalación de IBM Java Development Kit.

Para instalar IBM Java Development Kit, acceda al soporte de instalación de IBM Security Directory Server y vaya al directorio que contiene el archivo comprimido de IBM Java Development Kit.

Debe descomprimir el archivo de archivado de IBM Java Development Kit en la ubicación de instalación de IBM Security Directory Server. El archivo de archivado de IBM Java Development Kit está descomprimido en el directorio `java`. Para obtener más información sobre la ubicación de instalación de IBM Security Directory Server, consulte "Ubicaciones de la instalación predeterminada" en la página 27.

En AIX, puede utilizar el `tar` de GNU para descomprimir el archivo de archivado de IBM Java Development Kit en la ubicación de instalación de IBM Security Directory Server. De lo contrario, es posible que necesite mover el directorio `java`, que ha descomprimido, a la ubicación de instalación de IBM Security Directory Server. Para obtener más información sobre los paquetes de requisito previo, consulte "Paquetes de requisito previo que son necesarios en diversos sistemas operativos" en la página 15.

Tabla 14. Paquetes de IBM Java Development Kit que están disponibles en diversos sistemas operativos

Sistema operativo	Nombre del paquete
AIX	`ibm-java-16sr14-aix-ppc-64.tar`
System x Linux (Intel de 32 bits)	`ibm-java-16sr14-linux-i386.tar`
System i y System p Linux	`ibm-java-16sr14-linux-ppc-64.tar`
System z Linux	`ibm-java-16sr14-linux-s390-64.tar`
Linux en AMD64/EM64T	`ibm-java-16sr14-linux-64.tar`
HP-UX (Itanium)	`ibm-java-16sr14-hp-itanium-64.tar`
Solaris en AMD64/EM64T	`ibm-java-16sr14-solaris-amd-64.tar`
Solaris SPARC	`ibm-java-16sr14-solaris-sparc-64.tar`
Windows de 32 bits	`ibm-java-16sr14-win-i386.zip`
Windows en AMD64/EM64T	`ibm-java-16sr14-win-x86_64.zip`

Ejemplos

Ejemplo 1:

Para descomprimir el archivo de archivado de IBM Java Development Kit en la ubicación de instalación de IBM Security Directory Server en un sistema Linux, ejecute el mandato siguiente:

```
tar -xf ibm-java-16sr14-linux-64.tar -C /opt/ibm/ldap/V6.3.1/
```

Capítulo 10. Instalación de IBM Global Security Kit

Para utilizar Secure Sockets Layer (SSL) y Transaction Layer Security (TLS) con IBM Security Directory Server, el sistema debe contener una versión soportada de IBM Global Security Kit (GSKit).

Si los sistemas operativos no dan soporte a la instalación con IBM Installation Manager, puede utilizar los programas de utilidad del sistema operativo para la instalación de IBM Global Security Kit. Debe instalar GSKit en los sistemas del servidor y del cliente para establecer y utilizar conexiones seguras.

El paquete de cifrado de GSKit es necesario para el soporte de cifrado de bajo nivel. El paquete GSKit SSL es necesario para operaciones de reconocimiento de comunicaciones seguras. El paquete de cifrado de GSKit es un requisito previo para el paquete GSKit SSL.

El soporte de instalación de IBM Security Directory Server proporciona los siguientes paquetes GSKit para distintos sistemas operativos:

Nota: Para arquitecturas Solaris x64 y SPARC, los nombres de paquetes GSKit son los mismos.

AIX

Nombres de paquetes de GSKit (64 bits)

```
GSKit8.gskcrypt64.ppc.rte

GSKit8.gskssl64.ppc.rte
```

Nombres de paquetes de GSKit (32 bits)

```
GSKit8.gskcrypt32.ppc.rte

GSKit8.gskssl32.ppc.rte
```

System x Linux

Nombres de paquetes de GSKit (32 bits)

```
gskcrypt32-8.0.14.26.linux.x86.rpm

gskssl32-8.0.14.26.linux.x86.rpm
```

System z Linux

Nombres de paquetes de GSKit (64 bits)

```
gskcrypt64-8.0.14.26.linux.s390x.rpm

gskssl64-8.0.14.26.linux.s390x.rpm
```

Nombres de paquetes de GSKit (32 bits)

```
gskcrypt31-8.0.14.26.linux.s390.rpm

gskssl31-8.0.14.26.linux.s390.rpm
```

System i y System p Linux

Nombres de paquetes de GSKit (64 bits)

```
gskcrypt64-8.0.14.26.linux.ppc.rpm

gskssl64-8.0.14.26.linux.ppc.rpm
```

Nombres de paquetes de GSKit (32 bits)

```
gskcrypt32-8.0.14.26.linux.ppc.rpm
```

gskssl32-8.0.14.26.linux.ppc.rpm

Linux IA64 (Itanium) y AMD64/EM64T Linux

Nombres de paquetes de GSKit (64 bits)

gskcrypt64-8.0.14.26.linux.x86_64.rpm

gskssl64-8.0.14.26.linux.x86_64.rpm

Nombres de paquetes de GSKit (32 bits)

gskcrypt32-8.0.14.26.linux.x86.rpm

gskssl32-8.0.14.26.linux.x86.rpm

Solaris

Nombres de paquetes de GSKit (64 bits)

gsk8cry64.pkg

gsk8ssl64.pkg

Nombres de paquetes de GSKit (32 bits)

gsk8cry32.pkg

gsk8ssl32.pkg

HP-UX (Itanium)

Nombres de paquetes de GSKit (64 bits)

gskcrypt64

gskssl64

Nombres de paquetes de GSKit (32 bits)

gskcrypt32

gskssl32

Microsoft Windows

Nombres de paquetes de GSKit (64 bits)

gsk8crypt64.exe

gsk8ssl64.exe

Nombres de paquetes de GSKit (32 bits)

gsk8crypt32.exe

gsk8ssl32.exe

Instalación de IBM Global Security Kit con `installp`

Puede utilizar el mandato **installp** para completar la instalación de IBM Global Security Kit en un sistema AIX.

Antes de empezar

Acceda al soporte de instalación de IBM Security Directory Server para hacer que se pueda instalar IBM Global Security Kit. Consulte el apartado "Preparación del soporte de instalación" en la página 6.

Acerca de esta tarea

El programa de instalación de **installp** instala IBM Global Security Kit (GSKit) en un sistema AIX.

Procedimiento

1. Inicie sesión como usuario root.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al directorio `gskit` donde se almacena el instalable de IBM Global Security Kit.
4. Ejecute el mandato **installp** para instalar los paquetes de IBM Global Security Kit.
   a. Para instalar los paquetes de 64 bits de GSKit, ejecute los mandatos siguientes:
      ```
      installp -acgXd . GSKit8.gskcrypt64.ppc.rte
      installp -acgXd . GSKit8.gskssl64.ppc.rte
      ```
   b. Para instalar los paquetes de 32 bits de GSKit, ejecute los mandatos siguientes:
      ```
      installp -acgXd . GSKit8.gskcrypt32.ppc.rte
      installp -acgXd . GSKit8.gskssl32.ppc.rte
      ```
5. Ejecute el mandato siguiente para verificar si se ha realizado correctamente la instalación de IBM Global Security Kit:
   ```
   lslpp -aL GSKit8*
   ```

Resultados

El programa de instalación instala IBM Global Security Kit en las siguientes ubicaciones en un sistema AIX:

GSKit de 64 bits
`/usr/opt/ibm/gsk8_64/`

GSKit de 32 bits
`/usr/opt/ibm/gsk8/`

Instalación de IBM Global Security Kit con los programas de utilidad de Linux

Utilice el mandato **rpm** para completar la instalación de IBM Global Security Kit en un sistema Linux.

Antes de empezar

Acceda al soporte de instalación de IBM Security Directory Server para hacer que se pueda instalar IBM Global Security Kit. Consulte el apartado “Preparación del soporte de instalación” en la página 6.

Acerca de esta tarea

El mandato **rpm** instala IBM Global Security Kit (GSKit) en un sistema Linux. En el ejemplo, se mostrará la instalación de IBM Global Security Kit en AMD64 Opteron/EM64T Linux. Para System z, System i o System p, o System x Linux, debe sustituirla por los nombres de paquetes adecuados.

Procedimiento

1. Inicie sesión como usuario root.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al directorio `gskit` donde se almacena el instalable de IBM Global Security Kit.

4. Ejecute el mandato **rpm** para instalar los paquetes de IBM Global Security Kit.
   a. Para instalar los paquetes de 64 bits de GSKit, ejecute los mandatos siguientes:
      ```
      rpm -ivh gskcrypt64-8.0.14.26.linux.x86_64.rpm
      rpm -ivh gskssl64-8.0.14.26.linux.x86_64.rpm
      ```
   b. Para instalar los paquetes de 32 bits de GSKit, ejecute los mandatos siguientes:
      ```
      rpm -ivh gskcrypt32-8.0.14.26.linux.x86.rpm
      rpm -ivh gskssl32-8.0.14.26.linux.x86.rpm
      ```
5. Ejecute el mandato siguiente para verificar si se ha realizado correctamente la instalación de IBM Global Security Kit:
   ```
   rpm -qa | grep -i gsk
   ```

Resultados

El programa de instalación instala IBM Global Security Kit en las siguientes ubicaciones en un sistema Linux:

GSKit de 64 bits
`/usr/local/ibm/gsk8_64/`

GSKit de 32 bits
`/usr/local/ibm/gsk8/`

Instalación de IBM Global Security Kit con programas de utilidad de Solaris

Utilice el mandato **pkgadd** para completar la instalación de IBM Global Security Kit en un sistema Solaris.

Antes de empezar

Acceda al soporte de instalación de IBM Security Directory Server. Consulte el apartado “Preparación del soporte de instalación” en la página 6.

Acerca de esta tarea

El mandato **pkgadd** instala IBM Global Security Kit (GSKit) en un sistema Solaris. Los nombres de paquetes y los nombres de archivos son los mismos para los sistemas operativos Solaris SPARC y Solaris X64.

Procedimiento

1. Inicie sesión como usuario root.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al directorio `gskit` donde se almacena el instalable de IBM Global Security Kit.
4. Ejecute el mandato **pkgadd** para instalar los paquetes de IBM Global Security Kit.
   a. Para instalar los paquetes de 64 bits de GSKit, ejecute los mandatos siguientes:
      ```
      pkgadd -d gsk8cry64.pkg
      pkgadd -d gsk8ssl64.pkg
      ```
   b. Para instalar los paquetes de 32 bits de GSKit, ejecute los mandatos siguientes:

```
pkgadd -d gsk8cry32.pkg
pkgadd -d gsk8ssl32.pkg
```

5. Ejecute el mandato siguiente para verificar si se ha realizado correctamente la instalación de IBM Global Security Kit:

   ```
   pkginfo | grep -i gsk
   pkgparam nombre_paquete VERSION
   ```

   Sustituya el valor `nombre_paquete` por el nombre de paquete de GSKit para verificar la versión.

Instalación de IBM Global Security Kit con programas de utilidad de HP-UX

Utilice el mandato **swinstall** para completar la instalación de IBM Global Security Kit en un sistema HP-UX.

Antes de empezar

Acceda al soporte de instalación de IBM Security Directory Server para hacer que se pueda instalar IBM Global Security Kit. Consulte el apartado “Preparación del soporte de instalación” en la página 6.

Procedimiento

1. Inicie sesión como usuario root.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al directorio `gskit` donde se almacena el instalable de IBM Global Security Kit.
4. Ejecute el mandato **swinstall** para instalar los paquetes de IBM Global Security Kit.
   a. Para instalar los paquetes de 64 bits de GSKit, ejecute los mandatos siguientes:

      ```
      swinstall -s vía_acceso_a_instalable_gskit/gskcrypt64 gskcrypt64
      swinstall -s vía_acceso_a_instalable_gskit/gskssl64 gskssl64
      ```

      Debe proporcionar el nombre de vía de acceso absoluta del instalable de GSKit con el parámetro **-s**.
   b. Para instalar los paquetes de 32 bits de GSKit, ejecute los mandatos siguientes:

      ```
      swinstall -s vía_acceso_a_instalable_gskit/gskcrypt32 gskcrypt32
      swinstall -s vía_acceso_a_instalable_gskit/gskssl32 gskssl32
      ```
5. Ejecute el mandato siguiente para verificar si se ha realizado correctamente la instalación de IBM Global Security Kit:

   ```
   swlist | grep -i gsk
   ```

Instalación de IBM Global Security Kit en Windows

Ejecute el programa de instalación de IBM Global Security Kit para completar la instalación de IBM Global Security Kit en un sistema Windows.

Antes de empezar

Acceda al soporte de instalación de IBM Security Directory Server para hacer que se pueda instalar IBM Global Security Kit. Consulte el apartado "Preparación del soporte de instalación" en la página 6.

Acerca de esta tarea

En el ejemplo, se muestra la instalación del cifrado GSKit de 64 bits y de GSKit SSL de 64 bits. Para la instalación de GSKit de 32 bits, utilice los paquetes adecuados. En el sistema operativo Windows de 64 bits, puede instalar los paquetes GSKit de 64 bits y de 32 bits.

Procedimiento

1. Inicie sesión como miembro del grupo de administradores.
2. Cambie el directorio de trabajo actual al directorio `gskit` donde se almacena el instalable de IBM Global Security Kit.
3. Para instalar los paquetes de GSKit de 64 bits, ejecute el programa de instalación de GSKit.
   a. Ejecute el paquete de instalación de cifrado de GSKit8, `gsk8crypt64.exe`.
   b. En la ventana de instalación de cifrado de GSKit8, siga estos pasos:
      1) Especifique la vía de acceso de instalación para el cifrado de GSKit8.
      2) Pulse **Siguiente**.
      3) Pulse **Instalar**.
      4) Pulse **Finalizar**.
   c. Ejecute el paquete de instalación de GSKit8 SSL, `gsk8ssl64.exe`.
   d. En la ventana de instalación de GSKit8 SSL, siga estos pasos:
      1) Especifique la vía de acceso de instalación para GSKit8 SSL.
      2) Pulse **Siguiente**.
      3) Pulse **Instalar**.
      4) Pulse **Finalizar**.
4. Para ejecutar mandatos de GSKit desde la línea de mandatos, configure la variable *PATH* con los directorios `bin` y `lib64` en el sistema Windows x86_64.

   Nota: En Windows de 32 bits, configure la variable *PATH* con los directorios `bin` y `lib`.
   Si la ubicación de instalación de GSKit es `C:\Program Files\IBM\gsk8`, configure la variable *PATH* con los valores siguientes:

   ```
   set PATH="C:\Program Files\IBM\gsk8\bin";%PATH%
   set PATH="C:\Program Files\IBM\gsk8\lib64";%PATH%
   ```

Instalación de IBM Global Security Kit de forma silenciosa en Windows

Ejecute el programa de instalación de IBM Global Security Kit desde el indicador de mandatos para completar la instalación de IBM Global Security Kit de forma silenciosa en un sistema Windows.

Antes de empezar

Acceda al soporte de instalación de IBM Security Directory Server para hacer que se pueda instalar IBM Global Security Kit. Consulte el apartado "Preparación del soporte de instalación" en la página 6.

Acerca de esta tarea

En el ejemplo, se muestra la instalación del cifrado GSKit de 64 bits y de GSKit SSL de 64 bits. Para la instalación de GSKit de 32 bits, utilice los paquetes adecuados. En el sistema operativo Windows de 64 bits, puede instalar los paquetes GSKit de 64 bits y de 32 bits.

Procedimiento

1. Inicie sesión como miembro del grupo de administradores.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al directorio `gskit` donde se almacena el instalable de IBM Global Security Kit.
4. Para instalar los paquetes de GSKit de 64 bits de forma silenciosa, ejecute los mandatos siguientes:

   ```
   gsk8crypt64.exe /s /v"/quiet"
   gsk8ssl64.exe /s /v"/quiet"
   ```

5. Para ejecutar mandatos de GSKit desde la línea de mandatos, configure la variable *PATH* con los directorios `bin` y `lib64` en el sistema Windows x86_64.

   Nota: En Windows de 32 bits, configure la variable *PATH* con los directorios `bin` y `lib`.
   Si la ubicación de instalación de GSKit es `C:\Program Files\IBM\gsk8`, configure la variable *PATH* con los valores siguientes:

   ```
   set PATH="C:\Program Files\IBM\gsk8\bin";%PATH%
   set PATH="C:\Program Files\IBM\gsk8\lib64";%PATH%
   ```

Capítulo 11. Instalación de paquetes de idiomas

Para generar los mensajes de servidor de directorios en idiomas distintos del inglés, debe instalar paquetes de idiomas para los idiomas que desee utilizar.

IBM Installation Manager puede instalar todos los paquetes de idiomas que están disponibles para el sistema operativo si selecciona una característica de instalación desde el instalador completo. Los paquetes de idiomas están instalados en el subdirectorio `nls` de la ubicación de instalación de IBM Security Directory Server.

Nota: No es necesario instalar paquetes de idiomas para el cliente. Puede instalar paquetes de idiomas para el cliente si desea generar mensajes en un idioma distinto al inglés para los mandatos **idslink** e **idsrmlink**. Para obtener más información sobre los mandatos **idslink** e **idsrmlink**, consulte la *Consulta de mandatos*.

Puede instalar paquetes de idiomas con IBM Installation Manager o con programas de utilidad del sistema operativo en sistemas AIX y Linux. La instalación del paquete de idiomas con IBM Installation Manager se proporciona con el instalador del producto completo de IBM Security Directory Server.

Recuerde: La instalación del paquete de idiomas con IBM Installation Manager sólo está soportada en AIX, Linux en la arquitectura AMD64/EM64T, y en sistemas Microsoft Windows. En sistemas operativos que soportan la instalación de IBM Security Directory Server con IBM Installation Manager, no debe instalar manualmente los paquetes de idiomas con los programas de utilidad del sistema operativo. Si no está soportado para su instalación del sistema operativo de paquetes de idiomas con IBM Installation Manager, utilice los programas de utilidad operativos para la instalación de los paquetes de idiomas.

Tabla 15. Lista de idiomas soportados en los sistemas operativos AIX, Linux, Solaris, y Windows

Idiomas	AIX	Linux	Solaris	Microsoft Windows
Checoslovaco	✓			
Francés	✓	✓	✓	✓
Alemán	✓	✓	✓	✓
Húngaro	✓			
Italiano	✓	✓	✓	✓
Japonés	✓	✓	✓	✓
Coreano	✓	✓	✓	✓
Polaco	✓			
Portugués (Brasil)	✓	✓	✓	✓
Ruso	✓			
Eslovaco	✓			
Español	✓	✓	✓	✓
Chino simplificado	✓	✓	✓	✓
Chino tradicional	✓	✓	✓	✓

Paquetes de paquete de idiomas para la instalación

Debe identificar los nombres de paquetes asociados con cada idioma para un sistema operativo soportado antes de instalar un paquete de idioma.

Idioma y nombres de paquetes de idiomas

Recuerde: Los paquetes de idiomas para Linux están soportados para las siguientes arquitecturas:

- System x Linux
- System z Linux
- AMD64 Opteron / Intel EM64T Linux
- System i y System p Linux

Recuerde: Los paquetes de idiomas para Solaris están soportados para las siguientes arquitecturas:

- Solaris SPARC
- Solaris X64

Tabla 16. La lista de idiomas soportados con los nombres de paquetes de idiomas en los sistemas operativos AIX, Linux, y Solaris

Idiomas	AIX	Linux	Solaris
Checoslovaco	idsldap.msg631.cs_CZ		
Francés	idsldap.msg631.fr_FR	idsldap-msg631-fr-6.3.1-0.noarch.rpm	idsldap.msg631.fr.pkg
Alemán	idsldap.msg631.de_DE	idsldap-msg631-de-6.3.1-0.noarch.rpm	idsldap.msg631.de.pkg
Húngaro	idsldap.msg631.hu_HU		
Italiano	idsldap.msg631.it_IT	idsldap-msg631-it-6.3.1-0.noarch.rpm	idsldap.msg631.it.pkg
Japonés	idsldap.msg631.ja_JP	idsldap-msg631-ja-6.3.1-0.noarch.rpm	idsldap.msg631.ja.pkg
Coreano	idsldap.msg631.ko_KO	idsldap-msg631-ko-6.3.1-0.noarch.rpm	idsldap.msg631.ko.pkg
Polaco	idsldap.msg631.pl_PL		
Portugués (Brasil)	idsldap.msg631.pt_BR	idsldap-msg631-pt_BR-6.3.1-0.noarch.rpm	idsldap.msg631.pt_BR.pkg
Ruso	idsldap.msg631.ru_RU		
Eslovaco	idsldap.msg631.sk_SK		
Español	idsldap.msg631.es_ES	idsldap-msg631-es-6.3.1-0.noarch.rpm	idsldap.msg631.es.pkg
Chino simplificado	idsldap.msg631.zh_CN	idsldap-msg631-zh_CN-6.3.1-0.noarch.rpm	idsldap.msg631.zh_CN.pkg
Chino tradicional	idsldap.msg631.zh_TW	idsldap-msg631-zh_TW-6.3.1-0.noarch.rpm	idsldap.msg631.zh_TW.pkg

Instalación de paquetes de idiomas con los programas de utilidad del sistema operativo

Utilice los programas de utilidad del sistema operativo para la instalación del paquete de idiomas si el sistema operativo no da soporte a la instalación con IBM Installation Manager.

Antes de empezar

Debe preparar el soporte de instalación de IBM Security Directory Server. Consulte el apartado "Preparación del soporte de instalación" en la página 6.

Acerca de esta tarea

Para generar los mensajes de servidor de directorios en idiomas distintos del inglés, debe instalar paquetes de idiomas para los idiomas que desee utilizar.

Procedimiento

1. Inicie sesión como usuario root.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al directorio donde se almacena el instalable de IBM Security Directory Server.
4. Vaya al subdirectorio `tdsLangpack`.
5. Para instalar el paquete de idiomas para un idioma, ejecute los mandatos de instalación del paquete. En el ejemplo siguiente, se mostrará la instalación del paquete de idiomas del idioma francés. Puede instalar cualquier paquete de idiomas sustituyéndolo por el nombre del paquete adecuado para el sistema operativo.

Sistema operativo	**Mandato a ejecutar:**
AIX	`installp -acgXd . idsldap.msg631.fr_FR`
Linux	`rpm -ivh idsldap-msg631-fr-6.3.1-0.noarch.rpm`
Solaris	`pkgadd -d idsldap.msg631.fr.pkg`

6. Verifique si la instalación del paquete de idiomas ha sido satisfactoria. Para obtener más información, consulte el "Verificación de los paquetes de IBM Security Directory Server" en la página 87.

Resultados

El programa de instalación instala los paquetes de idiomas en los directorios siguientes:

Tabla 17. La ubicación de instalación predeterminada de los paquetes de idiomas de IBM Security Directory Server

Sistema operativo	**Ubicación de instalación del paquete de idiomas**
Linux	`/opt/ibm/ldap/V6.3.1/nls/msg`
AIX y Solaris	`/opt/IBM/ldap/V6.3.1/nls/msg`

Capítulo 12. Instalación con los programas de utilidad de línea de mandatos del sistema operativo

Puede ejecutar la instalación de IBM Security Directory Server con los programas de utilidad de línea de mandatos del sistema operativo si el sistema no proporciona soporte de X11.

PRECAUCIÓN:

- **No debe utilizar modalidades de instalación distintas en el mismo sistema. Debe ejecutar la instalación de IBM Security Directory Server con IBM Installation Manager o programas de utilidad de líneas de mandato del sistema operativo, pero no ambos. Si mezcla las dos modalidades de instalación, es posible que la instalación no incluya todos los paquetes correctos para una característica.**
- **Debe evitar la instalación manual de DB2 y de WebSphere Application Server incorporado en su vía de acceso de instalación predeterminada que utilice IBM Installation Manager. Tal instalación manual puede provocar errores de instalación, modificación, o desinstalación al ejecutar estas operaciones con IBM Installation Manager. Para obtener más información sobre la vía de acceso de instalación predeterminada, consulte "Ubicaciones de la instalación predeterminada" en la página 27.**

Debe obtener el origen de instalación de IBM Security Directory Server antes de instalar el producto. El producto de IBM Security Directory Server está disponible en archivos de archivado o como una imagen instalable. Puede crear DVD de instalación desde la imagen instalable.

Debe preparar el soporte de instalación. Para obtener más información, consulte el "Preparación del soporte de instalación" en la página 6.

Importante: Para utilizar IBM Security Directory Server como un servidor de directorios completo, instale una versión soportada de IBM DB2 en el sistema si no está instalado. Debe configurar el archivo `ldapdb.properties` con el nombre de la vía de acceso y la versión de IBM DB2.

Instalación con los programas de utilidad de AIX

Puede utilizar los programas de utilidad de línea de mandatos de AIX para instalar IBM Security Directory Server en un sistema AIX.

Puede utilizar uno de los siguientes programas de utilidad para la instalación de IBM Security Directory Server:

SMIT El método de instalación preferido es utilizar el programa de utilidad. Para obtener más información, consulte el "Instalación con SMIT" en la página 72.

installp
Para obtener más información, consulte el "Instalación con **installp**" en la página 73.

Paquetes para la instalación en un sistema AIX

Para utilizar IBM Security Directory Server como un servidor de directorios completo, un servidor proxy, o un cliente en un sistema AIX, debe instalar los paquetes adecuados.

Paquetes y conjuntos de archivos

IBM Security Directory Server proporciona los paquetes para un sistema AIX. Cada paquete contiene uno o varios conjuntos de archivos.

Tabla 18. Paquetes y conjuntos de archivos contenidos en los paquetes

Paquetes	Conjuntos de archivos asociados con el paquete
idsldap.license631	idsldap.license631.rte - Licencia
idsldap.cltbase631	• idsldap.cltbase631.rte - Tiempo de ejecución del cliente base • idsldap.cltbase631.adt - SDK del cliente base
idsldap.clt32bit631	• idsldap.clt32bit631.rte - C Client de 32 bits (sin SSL ni TLS)
idsldap.clt64bit631	• idsldap.clt64bit631.rte - C Client de 64 bits (sin SSL ni TLS)
idsldap.clt_max_crypto32bit631	• idsldap.clt_max_crypto32bit631.rte - C Client de 32 bits (con SSL y TLS)
idsldap.clt_max_crypto64bit631	• idsldap.clt_max_crypto64bit631.rte - C Client de 64 bits (con SSL y TLS)
idsldap.cltjava631	• idsldap.cltjava631.rte - Java Client
idsldap.srvbase64bit631	• idsldap.srvbase64bit631.rte - Base Server
idsldap.srv_max_cryptobase64bit631	• idsldap.srv_max_cryptobase64bit631.rte - Base Server (SSL)
idsldap.srvproxy64bit631	• idsldap.srvproxy64bit631.rte - Proxy Server (64 bits)
idsldap.srv64bit631	• idsldap.srv64bit631.rte - Directory Server (64 bits)
idsldap.webadmin631	• idsldap.webadmin631.rte - Herramienta de administración web (sin SSL ni TLS)
idsldap.webadmin_max_crypto631	• idsldap.webadmin_max_crypto631.rte - Herramienta de administración web (con SSL y TLS)
idsldap.msg631.en_US	No disponible
idsldap.ent631	• idsldap.ent631.rte - IBM Directory Server Entitlement (proporcionado únicamente en Passport Advantage)

Secuencia de instalación

Puede instalar todas las características al mismo tiempo. Si las instala por separado, debe instalarlas en un orden específico.

Importante:

- Si desea utilizar SSL (Secure Socket Layer) o TLS (Transport Layer Security), debe instalar una versión soportada de IBM Global Security Kit.
- Para el soporte de Kerberos en sistemas AIX, se requiere una versión soportada de Network Authentication Service.

Nota: Si el sistema no da soporte a X11, puede saltarse la instalación del componente de JDK que se proporciona en el IBM JDK. Si el componente de JDK no está instalado, es posible que no pueda utilizar Herramienta de administración de instancias o Herramienta de configuración.

Tabla 19. La secuencia de instalación para la característica del cliente

cliente de 32 bits (sin SSL ni TLS)	cliente de 32 bits (con SSL y TLS)	cliente de 64 bits (sin SSL ni TLS)	cliente de 64 bits (con SSL y TLS)
1. idsldap.cltbase631 2. idsldap.clt32bit631 3. idsldap.cltjava631	1. idsldap.cltbase631 2. idsldap.clt32bit631 3. idsldap.clt_max_crypto32bit631 4. idsldap.cltjava631	1. idsldap.cltbase631 2. idsldap.clt64bit631 3. idsldap.cltjava631	1. idsldap.cltbase631 2. idsldap.clt64bit631 3. idsldap.clt_max_crypto32bit631 4. idsldap.cltjava631

Nota: Al utilizar el archivo archivado Cliente-Servidor con titularidad o una imagen ISO con titularidad para la instalación de IBM Security Directory Server, debe aceptar en primer lugar los términos de licencia e instalar el paquete `idsldap.license631`.

Tabla 20. La secuencia de instalación para la característica del servidor de directorios completa

Servidor de directorios completo de 64 bits (sin SSL ni TLS)	Servidor de directorios completo de 64 bits (con SSL y TLS)
1. idsldap.license631 2. idsldap.cltbase631 3. idsldap.clt64bit631 4. idsldap.cltjava631 5. idsldap.srvbase64bit631 6. idsldap.srv64bit631 7. idsldap.msg631.en_US 8. idsldap.ent631	1. idsldap.license631 2. idsldap.cltbase631 3. idsldap.clt64bit631 4. idsldap.clt_max_crypto64bit631 5. idsldap.cltjava631 6. idsldap.srvbase64bit631 7. idsldap.srv_max_cryptobase64bit631 8. idsldap.srv64bit631 9. idsldap.msg631.en_US 10. idsldap.ent631

Tabla 21. La secuencia de instalación para la característica del servidor proxy

Servidor proxy de 64 bits (sin SSL ni TLS)	Servidor proxy de 64 bits (con SSL y TLS)
1. idsldap.license631 2. idsldap.cltbase631 3. idsldap.clt64bit631 4. idsldap.cltjava631 5. idsldap.srvbase64bit631 6. idsldap.srvproxy64bit631 7. idsldap.msg631.en_US 8. idsldap.ent631	1. idsldap.license631 2. idsldap.cltbase631 3. idsldap.clt64bit631 4. idsldap.clt_max_crypto64bit631 5. idsldap.cltjava631 6. idsldap.srvbase64bit631 7. idsldap.srv_max_cryptobase64bit631 8. idsldap.srvproxy64bit631 9. idsldap.msg631.en_US 10. idsldap.ent631

Nota: Para utilizar la Herramienta de administración web, debe desplegarla en un servidor de aplicaciones web. Para obtener más información sobre la instalación de WebSphere Application Server incorporado, consulte “Instalación de WebSphere Application Server incorporado manualmente” en la página 111.

Tabla 22. Paquete de instalación de la Herramienta de administración web

Herramienta de administración web (sin SSL ni TLS)	Herramienta de administración web (con SSL y TLS)
1. idsldap.license631 2. idsldap.webadmin631	1. idsldap.license631 2. idsldap.webadmin_max_crypto631

Al instalar la Herramienta de administración web, los archivos de Directory Services Markup Language (DSML) también se copiarán al sistema. Para obtener más información sobre DSML, consulte el apartado Apéndice A, "Directory Services Markup Language", en la página 255.

Instalación con SMIT

Utilice el mandato **smit** para completar la instalación de IBM Security Directory Server en un sistema AIX.

Antes de empezar

Debe preparar el soporte de instalación de IBM Security Directory Server. Consulte el apartado "Preparación del soporte de instalación" en la página 6.

Acerca de esta tarea

El programa de instalación de **smit** instala IBM Security Directory Server en un sistema AIX. Si se ha instalado una versión soportada de IBM DB2 en el sistema, el proceso de instalación actualizará el archivo `ldapdb.properties` con el nombre de la vía de acceso y versión de DB2.

Procedimiento

1. Inicie sesión como usuario root.
2. Acceda al indicador de mandatos.
3. Ejecute el mandato **idsLicense**.
   ```
   ./idsLicense
   ```
4. Si acepta los términos del acuerdo de licencia de software, especifique 1. Están disponibles las siguientes opciones:
   - 1: Para aceptar el acuerdo de licencia.
   - 2: Para rechazar el acuerdo de licencia y salir de la instalación.
   - 3: Para imprimir el acuerdo de licencia.
   - 4: Para leer términos que no sean de IBM en el acuerdo de licencia.
   - 99: Para volver a la pantalla anterior.

   Al aceptar los términos del acuerdo de licencia, se creará un archivo `LAPID` y una carpeta `license` en la ubicación de instalación de IBM Security Directory Server. La carpeta de licencia contiene los archivos de licencia de IBM Security Directory Server en todos los idiomas soportados.

   Importante: No modifique ni suprima el archivo `LAPID` ni los archivos de licencia en la carpeta de licencia.
5. Ejecute el mandato **smit install**. Se abrirá la ventana **Instalación y mantenimiento de software**.
6. Pulse **Instalar y actualizar software** > **Instalar y actualizar desde todo el software disponible**.

7. Seleccione el soporte de instalación.
   - Si realiza la instalación desde el DVD, realice las acciones siguientes:
     a. Pulse **Lista** para acceder al dispositivo que contiene las imágenes de IBM Security Directory Server.
   - Si está instalando desde el archivo de archivado descomprimido, especifique **.** en el campo **Dispositivo/Directorio de ENTRADA para software**.
8. Pulse **Ir**.
9. Mueva el cursor a **Software a instalar**, y realice las acciones siguientes:
   a. Para instalar el conjunto de archivos de `idsldap`, escriba `idsldap`.
   b. Pulse **Lista** para listar todos los conjuntos de archivos, y seleccione los conjuntos de archivos que desee instalar.
   c. Pulse **Aceptar**.
10. Para comenzar la instalación, pulse **Aceptar**.
11. Compruebe el resumen de instalación al final de la salida para verificar la instalación satisfactoria de los conjuntos de archivos.
12. Una vez que se haya completado la instalación, pulse **Terminado**.
13. Para salir del programa **SMIT**, pulse la tecla `F12`.
14. Verifique si la instalación de IBM Security Directory Server se ha realizado correctamente. Para obtener más información, consulte el "Verificación de los paquetes de IBM Security Directory Server" en la página 87.

Resultados

El programa de instalación instala IBM Security Directory Server en el directorio `/opt/IBM/ldap/V6.3.1` del sistema AIX. Si se ha instalado una versión soportada de IBM DB2 en el sistema, el proceso de instalación actualizará el archivo `ldapdb.properties` con el nombre de la vía de acceso y versión de DB2.

Qué hacer a continuación

Tras la instalación de IBM Security Directory Server, debe realizar la acción siguiente:

- Para utilizar IBM Security Directory Server como un servidor de directorios completo, cree una instancia de servidor de directorios. Consulte el apartado "Creación de la instancia de servidor de directorios predeterminada" en la página 137.
- Para utilizar IBM Security Directory Server como un servidor proxy, cree una instancia de servidor proxy. Consulte el apartado "Creación de una instancia de servidor proxy con valores personalizados" en la página 147.

Instalación con `installp`

Utilice el mandato **`installp`** para completar la instalación de IBM Security Directory Server en un sistema AIX.

Antes de empezar

Debe preparar el soporte de instalación de IBM Security Directory Server. Consulte el apartado "Preparación del soporte de instalación" en la página 6.

Acerca de esta tarea

El programa de instalación de **installp** instalará IBM Security Directory Server en un sistema AIX. Si se ha instalado una versión soportada de IBM DB2 en el sistema, el proceso de instalación actualizará el archivo `ldapdb.properties` con el nombre de la vía de acceso y versión de DB2.

Procedimiento

1. Inicie sesión como usuario root.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al directorio donde está almacenado el instalable de IBM Security Directory Server.
4. Ejecute el mandato **idsLicense**.
   ```
   ./idsLicense
   ```
5. Si acepta los términos del acuerdo de licencia de software, especifique 1. Están disponibles las siguientes opciones:
   - 1: Para aceptar el acuerdo de licencia.
   - 2: Para rechazar el acuerdo de licencia y salir de la instalación.
   - 3: Para imprimir el acuerdo de licencia.
   - 4: Para leer términos que no sean de IBM en el acuerdo de licencia.
   - 99: Para volver a la pantalla anterior.

   Al aceptar los términos del acuerdo de licencia, se creará un archivo `LAPID` y una carpeta `license` en la ubicación de instalación de IBM Security Directory Server. La carpeta de licencia contiene los archivos de licencia de IBM Security Directory Server en todos los idiomas soportados.

   Importante: No modifique ni suprima el archivo `LAPID` ni los archivos de licencia en la carpeta de licencia.
6. Determine qué paquetes de IBM Security Directory Server desea instalar.
   ```
   installp -ld . | grep idsldap
   ```

   Se mostrará una lista de todos los paquetes instalables de IBM Security Directory Server.
7. Ejecute el mandato siguiente para instalar los paquetes:
   ```
   installp -acgXd . nombres_paquetes
   ```

   Para instalar todos los paquetes de IBM Security Directory Server desde la vía de acceso actual, ejecute el mandato siguiente:
   ```
   installp -acgXd . idsldap
   ```
8. Una vez finalizada la instalación, el sistema generará un resumen de la instalación.
9. Verifique si la instalación de IBM Security Directory Server se ha realizado correctamente. Para obtener más información, consulte el "Verificación de los paquetes de IBM Security Directory Server" en la página 87.

Resultados

El programa de instalación instala IBM Security Directory Server en el directorio `/opt/IBM/ldap/V6.3.1` del sistema AIX. Si se ha instalado una versión soportada de IBM DB2 en el sistema, el proceso de instalación actualizará el archivo `ldapdb.properties` con el nombre de la vía de acceso y versión de DB2.

Qué hacer a continuación

Tras la instalación de IBM Security Directory Server, debe realizar las siguientes acciones:

- Para utilizar IBM Security Directory Server como un servidor de directorios completo, cree una instancia de servidor de directorios. Para obtener más información, consulte el "Creación de la instancia de servidor de directorios predeterminada" en la página 137.
- Para utilizar IBM Security Directory Server como un servidor proxy, cree una instancia de servidor proxy. Para obtener más información, consulte el "Creación de una instancia de servidor proxy con valores personalizados" en la página 147.

Instalación con programas de utilidad de Linux

Puede utilizar los programas de utilidad de línea de mandatos de Linux para instalar IBM Security Directory Server en un sistema Linux.

IBM Security Directory Server proporciona paquetes independientes para sistemas con distintos sistemas operativos y arquitecturas. Debe seleccionar los paquetes adecuados para la instalación en el sistema. Para obtener más información sobre los nombres de paquetes, consulte "Paquetes para la instalación en un sistema Linux".

Paquetes para la instalación en un sistema Linux

Para utilizar IBM Security Directory Server como un servidor de directorios completo, un servidor proxy, o un cliente en un sistema Linux, debe instalar paquetes adecuados.

Paquetes proporcionados para distintos sistemas Linux

Tabla 23. Paquetes que se proporcionan con IBM Security Directory Server para distintos sistemas Linux

Paquetes de IBM Security Directory Server	AMD64 Opteron/EM64T Linux	System i o System p	System x	System z
IBM Directory Server - Licencia	idsldap-license631-6.3.1-0.x86_64.rpm	idsldap-license631-6.3.1-0.ppc.rpm	idsldap-license631-6.3.1-0.i386.rpm	idsldap-license631-6.3.1-0.s390.rpm
IBM Directory Server - Cliente base	idsldap-cltbase631-6.3.1-0.x86_64.rpm	idsldap-cltbase631-6.3.1-0.ppc.rpm	idsldap-cltbase631-6.3.1-0.i386.rpm	idsldap-cltbase631-6.3.1-0.s390.rpm
IBM Directory Server - Cliente de 32 bits	idsldap-clt32bit631-6.3.1-0.x86_64.rpm	idsldap-clt32bit631-6.3.1-0.ppc.rpm	idsldap-clt32bit631-6.3.1-0.i386.rpm	idsldap-clt32bit631-6.3.1-0.s390.rpm
IBM Directory Server - Cliente de 64 bits	idsldap-clt64bit631-6.3.1-0.x86_64.rpm	idsldap-clt64bit631-6.3.1-0.ppc64.rpm	No disponible	idsldap-clt64bit631-6.3.1-0.s390x.rpm
IBM Directory Server - Cliente Java	idsldap-cltjava631-6.3.1-0.x86_64.rpm	idsldap-cltjava631-6.3.1-0.ppc.rpm	idsldap-cltjava631-6.3.1-0.i386.rpm	idsldap-cltjava631-6.3.1-0.s390.rpm
IBM Directory Server - Servidor base	idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm	idsldap-srvbase64bit631-6.3.1-0.ppc64.rpm	idsldap-srvbase32bit631-6.3.1-0.i386.rpm	idsldap-srvbase64bit631-6.3.1-0.s390x.rpm
IBM Directory Server - Proxy Server	idsldap-srvproxy64bit631-6.3.1-0.x86_64.rpm	idsldap-srvproxy64bit631-6.3.1-0.ppc64.rpm	idsldap-srvproxy32bit631-6.3.1-0.i386.rpm	idsldap-srvproxy64bit631-6.3.1-0.s390x.rpm
IBM Directory Server - Server de 32 bits	No disponible	No disponible	idsldap-srv32bit631-6.3.1-0.i386.rpm	No disponible
IBM Directory Server - Server de 64 bits	idsldap-srv64bit631-6.3.1-0.x86_64.rpm	idsldap-srv64bit631-6.3.1-0.ppc64.rpm	No disponible	idsldap-srv64bit631-6.3.1-0.s390x.rpm

Tabla 23. Paquetes que se proporcionan con IBM Security Directory Server para distintos sistemas Linux (continuación)

Paquetes de IBM Security Directory Server	AMD64 Opteron/EM64T Linux	System i o System p	System x	System z
IBM Directory Server - Herramienta de administración web	idsldap-webadmin631-6.3.1-0.x86_64.rpm	idsldap-webadmin631-6.3.1-0.ppc.rpm	idsldap-webadmin631-6.3.1-0.i386.rpm	idsldap-webadmin631-6.3.1-0.s390.rpm
IBM Directory Server - Mensajes en inglés de Estados Unidos	idsldap-msg631-en-6.3.1-0.x86_64.rpm	idsldap-msg631-en-6.3.1-0.ppc.rpm	idsldap-msg631-en-6.3.1-0.i386.rpm	idsldap-msg631-en-6.3.1-0.s390.rpm
IBM Directory Server Entitlement (proporcionado únicamente en Passport Advantage)	idsldap-ent631-6.3.1-0.x86_64.rpm	idsldap-ent631-6.3.1-0.ppc.rpm	idsldap-ent631-6.3.1-0.i386.rpm	idsldap-ent631-6.3.1-0.s390.rpm

Dependencia del paquete

Para la instalación de determinados paquetes, debe instalar las dependencias en primer lugar.

Nota: Al utilizar el Cliente-Servidor con el archivo archivado de titularidad o una imagen ISO con titularidad para la instalación de IBM Security Directory Server, debe aceptar en primer lugar los términos de licencia e instalar el paquete idsldap-license631-6.3.1-0.*arch*.rpm.

En la tabla, se muestra la dependencia del paquete en AMD64 Opteron/EM64T Linux. Para System z, System i o System p, o System x Linux, sustitúyalos con los nombres de paquetes adecuados.

Tabla 24. Paquete y sus paquetes dependientes

Nombre del paquete	Depende de
idsldap-clt32bit631-6.3.1-0.x86_64.rpm	idsldap-cltbase631-6.3.1-0.x86_64.rpm
idsldap-clt64bit631-6.3.1-0.x86_64.rpm	idsldap-cltbase631-6.3.1-0.x86_64.rpm
idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm	1. idsldap-license631-6.3.1-0.x86_64.rpm 2. idsldap-cltbase631-6.3.1-0.x86_64.rpm 3. idsldap-clt64bit631-6.3.1-0.x86_64.rpm
idsldap-srv64bit631-6.3.1-0.x86_64.rpm	1. idsldap-license631-6.3.1-0.x86_64.rpm 2. idsldap-cltbase631-6.3.1-0.x86_64.rpm 3. idsldap-clt64bit631-6.3.1-0.x86_64.rpm 4. idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm
idsldap-srvproxy64bit631-6.3.1-0.x86_64.rpm	1. idsldap-license631-6.3.1-0.x86_64.rpm 2. idsldap-cltbase631-6.3.1-0.x86_64.rpm 3. idsldap-clt64bit631-6.3.1-0.x86_64.rpm 4. idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm

Secuencia de instalación

Puede instalar todas las características al mismo tiempo. Si las instala por separado, debe instalarlas en un orden específico.

Importante: Si desea utilizar SSL (Secure Socket Layer) o TLS (Transport Layer Security), debe instalar una versión soportada de IBM Global Security Kit.

En el ejemplo de secuencia de instalación, se utilizará AMD64 Opteron/EM64T Linux. Para System z, System i o System p, o System x Linux, sustitúyalos con los nombres de paquetes adecuados.

Tabla 25. La secuencia de instalación para la característica del cliente

Cliente de 32 bits	Cliente de 64 bits
1. idsldap-cltbase631-6.3.1-0.x86_64.rpm	1. idsldap-cltbase631-6.3.1-0.x86_64.rpm
2. idsldap-clt32bit631-6.3.1-0.x86_64.rpm	2. idsldap-clt64bit631-6.3.1-0.x86_64.rpm
3. idsldap-cltjava631-6.3.1-0.x86_64.rpm	3. idsldap-cltjava631-6.3.1-0.x86_64.rpm

Tabla 26. La secuencia de instalación para el servidor de directorios completo y la característica del servidor proxy

Servidor de directorios completo de 64 bits	Servidor proxy de 64 bits
1. idsldap-license631-6.3.1-0.x86_64.rpm	1. idsldap-license631-6.3.1-0.x86_64.rpm
2. idsldap-cltbase631-6.3.1-0.x86_64.rpm	2. idsldap-cltbase631-6.3.1-0.x86_64.rpm
3. idsldap-clt64bit631-6.3.1-0.x86_64.rpm	3. idsldap-clt64bit631-6.3.1-0.x86_64.rpm
4. idsldap-cltjava631-6.3.1-0.x86_64.rpm	4. idsldap-cltjava631-6.3.1-0.x86_64.rpm
5. idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm	5. idsldap-srvbase64bit631-6.3.1-0.x86_64.rpm
6. idsldap-srv64bit631-6.3.1-0.x86_64.rpm	6. idsldap-srvproxy64bit631-6.3.1-0.x86_64.rpm
7. idsldap-msg631-en-6.3.1-0.x86_64.rpm	7. idsldap-msg631-en-6.3.1-0.x86_64.rpm
8. idsldap-ent631-6.3.1-0.x86_64.rpm	8. idsldap-ent631-6.3.1-0.x86_64.rpm

Nota: Para utilizar la Herramienta de administración web, debe desplegarla en un servidor de aplicaciones web. Para obtener más información sobre la instalación de WebSphere Application Server incorporado, consulte “Instalación de WebSphere Application Server incorporado manualmente” en la página 111.

Tabla 27. Paquete de instalación de la Herramienta de administración web

Herramienta de administración web
1. idsldap-license631-6.3.1-0.x86_64.rpm
2. idsldap-webadmin631-6.3.1-0.x86_64.rpm

Al instalar la Herramienta de administración web, los archivos de Directory Services Markup Language (DSML) también se copiarán al sistema. Para obtener más información sobre DSML, consulte el apartado Apéndice A, “Directory Services Markup Language”, en la página 255.

Instalación con programas de utilidad de Linux

Utilice el mandato **rpm** para completar la instalación de IBM Security Directory Server en un sistema Linux.

Antes de empezar

Debe preparar el soporte de instalación de IBM Security Directory Server. Consulte el apartado “Preparación del soporte de instalación” en la página 6.

Acerca de esta tarea

El programa de instalación de **rpm** instala IBM Security Directory Server en un sistema Linux. Si se ha instalado una versión soportada de IBM DB2 en el sistema, el proceso de instalación actualizará el archivo `ldapdb.properties` con el nombre de la vía de acceso y versión de DB2.

Procedimiento

1. Inicie sesión como usuario root.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al directorio donde se almacena el instalable de IBM Security Directory Server.
4. Ejecute el mandato **idsLicense**.

   ```
   ./idsLicense
   ```
5. Si acepta los términos del acuerdo de licencia de software, especifique 1. Están disponibles las siguientes opciones:
   - 1: Para aceptar el acuerdo de licencia.
   - 2: Para rechazar el acuerdo de licencia y salir de la instalación.
   - 3: Para imprimir el acuerdo de licencia.
   - 4: Para leer términos que no sean de IBM en el acuerdo de licencia.
   - 99: Para volver a la pantalla anterior.

   Al aceptar los términos del acuerdo de licencia, se creará un archivo `LAPID` y una carpeta `license` en la ubicación de instalación de IBM Security Directory Server. La carpeta de licencia contiene los archivos de licencia de IBM Security Directory Server en todos los idiomas soportados.

   Importante: No modifique ni suprima el archivo `LAPID` ni los archivos de licencia en la carpeta de licencia.
6. Ejecute el mandato siguiente para instalar el paquete:

   ```
   rpm -ivh nombre_paquete
   ```

   Para instalar todos los paquetes de IBM Security Directory Server, ejecute el mandato siguiente:

   ```
   rpm -ivh idsldap*
   ```
7. Verifique si la instalación de IBM Security Directory Server se ha realizado correctamente. Para obtener más información, consulte el "Verificación de los paquetes de IBM Security Directory Server" en la página 87.

Resultados

El programa de instalación instala IBM Security Directory Server en el directorio `/opt/ibm/ldap/V6.3.1` en el sistema Linux. Si se ha instalado una versión soportada de IBM DB2 en el sistema, el proceso de instalación actualizará el archivo `ldapdb.properties` con el nombre de la vía de acceso y versión de DB2.

Qué hacer a continuación

Tras la instalación de IBM Security Directory Server, debe realizar la acción siguiente:

- Para utilizar IBM Security Directory Server como un servidor de directorios completo, cree una instancia de servidor de directorios. Para obtener más información, consulte el “Creación de la instancia de servidor de directorios predeterminada” en la página 137.
- Para utilizar IBM Security Directory Server como un servidor proxy, cree una instancia de servidor proxy. Para obtener más información, consulte el “Creación de una instancia de servidor proxy con valores personalizados” en la página 147.

Instalación con los programas de utilidad de Solaris

Puede utilizar los programas de utilidad de línea de mandatos de Solaris para instalar IBM Security Directory Server en un sistema Solaris.

IBM Security Directory Server proporciona el mismo conjunto de paquetes para sistemas con distinta arquitectura. Hay paquetes disponibles para los sistemas operativos Sun SPARC Solaris y AMD64 Opteron/EM64T Solaris. Los nombres de paquete y de archivo son los mismos para ambos sistemas operativos. Para obtener más información sobre los nombres de paquetes, consulte “Paquetes para la instalación en un sistema Solaris”.

Al instalar los paquetes de IBM Security Directory Server, no debe utilizar el sistema predeterminado de ALL. Si utiliza elegir los paquetes ALL, el sistema no secuenciará los paquetes correctamente y la instalación fallará.

Paquetes para la instalación en un sistema Solaris

Para utilizar IBM Security Directory Server como un servidor de directorios completo, un servidor proxy, o un cliente en un sistema Solaris, debe instalar los paquetes adecuados.

Paquetes proporcionados para sistemas Solaris

Importante: Los nombres de paquete y de archivo son los mismos para los sistemas operativos Solaris SPARC y AMD64 Opteron/EM64T Solaris.

Tabla 28. Paquetes proporcionados con IBM Security Directory Server para distintos sistemas Solaris

Paquetes de IBM Security Directory Server	Nombres de paquetes	Nombre de archivo
IBM Directory Server - Licencia	IDSllicense631	idsldap-license631.pkg
IBM Directory Server - Cliente base	IDSlbc631	idsldap.cltbase631.pkg
IBM Directory Server - Cliente de 32 bits	IDSl32c631	idsldap.clt32bit631.pkg
IBM Directory Server - Cliente de 64 bits	IDSl64c631	idsldap.clt64bit631.pkg
IBM Directory Server - Cliente Java	IDSljc631	idsldap.cltjava631.pkg
IBM Directory Server - Servidor base	IDSlbs631	idsldap.srvbase64bit631.pkg
IBM Directory Server - Proxy Server	IDSl64p631	idsldap.srvproxy64bit631.pkg
IBM Directory Server - Server de 64 bits	IDSl64s631	idsldap.srv64bit631.pkg
IBM Directory Server - Herramienta de administración web	IDSlweb631	idsldap.webadmin631.pkg
IBM Directory Server - Mensajes en inglés de Estados Unidos	IDSlen631	idsldap.msg631.en.pkg
IBM Directory Server Entitlement (proporcionado únicamente en Passport Advantage)	IDSlent631	idsldap.ent631.pkg

Dependencia del paquete

Para la instalación de determinados paquetes, debe instalar las dependencias en primer lugar.

Tabla 29. Paquete y sus paquetes dependientes

Nombre del paquete	Depende de
idsldap.clt32bit631.pkg	idsldap.cltbase631.pkg
idsldap.clt64bit631.pkg	idsldap.cltbase631.pkg
idsldap.srvbase64bit631.pkg	1. idsldap-license631.pkg 2. idsldap.cltbase631.pkg 3. idsldap.clt64bit631.pkg
idsldap.srv64bit631.pkg	1. idsldap-license631.pkg 2. idsldap.cltbase631.pkg 3. idsldap.clt64bit631.pkg 4. idsldap.srvbase64bit631.pkg
idsldap.srvproxy64bit631.pkg	1. idsldap-license631.pkg 2. idsldap.cltbase631.pkg 3. idsldap.clt64bit631.pkg 4. idsldap.srvbase64bit631.pkg

Secuencia de instalación

Al instalar los paquetes en un sistema Solaris, debe instalarlos en un orden específico.

Importante: Si desea utilizar SSL (Secure Socket Layer) o TLS (Transport Layer Security), debe instalar una versión soportada de IBM Global Security Kit.

Tabla 30. La secuencia de instalación para la característica del cliente

Cliente de 32 bits	Cliente de 64 bits
1. idsldap.cltbase631.pkg 2. idsldap.clt32bit631.pkg 3. idsldap.cltjava631.pkg	1. idsldap.cltbase631.pkg 2. idsldap.clt64bit631.pkg 3. idsldap.cltjava631.pkg

Nota: Al utilizar el Cliente-Servidor con el archivo de archivado de titularidad o una imagen ISO con titularidad para la instalación de IBM Security Directory Server, debe aceptar en primer lugar los términos de licencia e instalar el paquete idsldap-license631.pkg.

Tabla 31. La secuencia de instalación para el servidor de directorios completo y la característica del servidor proxy

Servidor de directorios completo de 64 bits	Servidor proxy de 64 bits
1. idsldap-license631.pkg	1. idsldap-license631.pkg
2. idsldap.cltbase631.pkg	2. idsldap.cltbase631.pkg
3. idsldap.clt64bit631.pkg	3. idsldap.clt64bit631.pkg
4. idsldap.cltjava631.pkg	4. idsldap.cltjava631.pkg
5. idsldap.srvbase64bit631.pkg	5. idsldap.srvbase64bit631.pkg
6. idsldap.srv64bit631.pkg	6. idsldap.srvproxy64bit631.pkg
7. idsldap.msg631.en.pkg	7. idsldap.msg631.en.pkg
8. idsldap.ent631.pkg	8. idsldap.ent631.pkg

Nota: Para utilizar la Herramienta de administración web, debe desplegarla en un servidor de aplicaciones web. Para obtener más información sobre la instalación de WebSphere Application Server incorporado, consulte "Instalación de WebSphere Application Server incorporado manualmente" en la página 111.

Tabla 32. Paquete de instalación de la Herramienta de administración web

Herramienta de administración web
1. idsldap-license631.pkg
2. idsldap.webadmin631.pkg

Al instalar la Herramienta de administración web, los archivos de Directory Services Markup Language (DSML) también se copiarán al sistema. Para obtener más información sobre DSML, consulte el apartado Apéndice A, "Directory Services Markup Language", en la página 255.

Instalación con los programas de utilidad de Solaris

Utilice el mandato **pkgadd** para completar la instalación de IBM Security Directory Server en un sistema Solaris.

Antes de empezar

Acceda al soporte de instalación de IBM Security Directory Server. Consulte el apartado "Preparación del soporte de instalación" en la página 6.

Acerca de esta tarea

El programa de instalación **pkgadd** instala IBM Security Directory Server en un sistema Solaris. Si se ha instalado una versión soportada de IBM DB2 en el sistema, el proceso de instalación actualizará el archivo `ldapdb.properties` con el nombre de la vía de acceso y versión de DB2.

Procedimiento

1. Inicie sesión como usuario root.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al directorio donde está almacenado el instalable de IBM Security Directory Server.
4. Ejecute el mandato **idsLicense**.

   ```
   ./idsLicense
   ```

5. Si acepta los términos del acuerdo de licencia de software, especifique 1. Están disponibles las siguientes opciones:
   - 1: Para aceptar el acuerdo de licencia.
   - 2: Para rechazar el acuerdo de licencia y salir de la instalación.
   - 3: Para imprimir el acuerdo de licencia.
   - 4: Para leer términos que no sean de IBM en el acuerdo de licencia.
   - 99: Para volver a la pantalla anterior.

   Al aceptar los términos del acuerdo de licencia, se creará un archivo `LAPID` y una carpeta `license` en la ubicación de instalación de IBM Security Directory Server. La carpeta de licencia contiene los archivos de licencia de IBM Security Directory Server en todos los idiomas soportados.

   Importante: No modifique ni suprima el archivo `LAPID` ni los archivos de licencia en la carpeta de licencia.
6. Ejecute el mandato siguiente para instalar un paquete:

   Nota: Debe instalar los paquetes de IBM Security Directory Server en un sistema Solaris en un orden específico. Para obtener más información, consulte el "Paquetes para la instalación en un sistema Solaris" en la página 79.

   ```
   pkgadd -d nombre_paquete
   ```
7. Verifique si la instalación de IBM Security Directory Server se ha realizado correctamente. Para obtener más información, consulte el "Verificación de los paquetes de IBM Security Directory Server" en la página 87.

Resultados

El programa de instalación instala IBM Security Directory Server en el directorio `/opt/IBM/ldap/V6.3.1` en el sistema Solaris. Si se ha instalado una versión soportada de IBM DB2 en el sistema, el proceso de instalación actualizará el archivo `ldapdb.properties` con el nombre de la vía de acceso y versión de DB2.

Qué hacer a continuación

Tras la instalación de IBM Security Directory Server, debe realizar la acción siguiente:

- Para utilizar IBM Security Directory Server como un servidor de directorios completo, cree una instancia de servidor de directorios. Para obtener más información, consulte el "Creación de la instancia de servidor de directorios predeterminada" en la página 137.
- Para utilizar IBM Security Directory Server como un servidor proxy, cree una instancia de servidor proxy. Para obtener más información, consulte el "Creación de una instancia de servidor proxy con valores personalizados" en la página 147.

Instalación con los programas de utilidad de HP-UX

Puede utilizar los programas de utilidad de línea de mandatos de HP-UX para instalar IBM Security Directory Server en un sistema HP-UX.

IBM Security Directory Server proporciona paquetes sólo para clientes para HP-UX en sistemas Itanium (servidores basados en el procesador Intel IA64). Para obtener más información, consulte el "Paquetes para la instalación en un sistema HP-UX Itanium" en la página 83.

Paquetes para la instalación en un sistema HP-UX Itanium

Para utilizar IBM Security Directory Server como cliente en un sistema HP-UX, debe instalar los paquetes adecuados.

Paquetes proporcionados para sistemas HP-UX

IBM Security Directory Server proporciona paquetes sólo para clientes para HP-UX en sistemas Itanium (servidores basados en el procesador Intel IA64).

Tabla 33. Paquetes que se proporcionan con IBM Security Directory Server para sistemas HP-UX

Paquetes de IBM Security Directory Server	Nombres de paquetes
IBM Directory Server - Cliente base	idsldap.cltbase631.depot
IBM Directory Server - Cliente de 32 bits	idsldap.clt32bit631.depot
IBM Directory Server - Cliente de 64 bits	idsldap.clt64bit631.depot
IBM Directory Server - Cliente Java	idsldap.cltjava631.depot
IBM Directory Server - Licencia	idsldap.license631.depot

Dependencia del paquete

Para la instalación de determinados paquetes, debe instalar las dependencias en primer lugar.

Tabla 34. Paquete y sus paquetes dependientes

Nombre del paquete	Depende de
idsldap.clt32bit631.depot	idsldap.cltbase631.depot
idsldap.clt64bit631.depot	idsldap.cltbase631.depot

Secuencia de instalación

Al instalar los paquetes en un sistema HP-UX, debe instalarlos en un orden específico.

Importante: Si desea utilizar SSL (Secure Socket Layer) o TLS (Transport Layer Security), debe instalar una versión soportada de IBM Global Security Kit.

Tabla 35. La secuencia de instalación para la característica del cliente

Cliente de 32 bits	Cliente de 64 bits
1. idsldap.cltbase631.depot 2. idsldap.clt32bit631.depot 3. idsldap.cltjava631.depot	1. idsldap.cltbase631.depot 2. idsldap.clt64bit631.depot 3. idsldap.cltjava631.depot

Instalación con los programas de utilidad de HP-UX

Puede utilizar el mandato **swinstall** para completar la instalación de IBM Security Directory Server en un sistema HP-UX.

Antes de empezar

Debe preparar el soporte de instalación de IBM Security Directory Server. Consulte el apartado “Preparación del soporte de instalación” en la página 6.

Acerca de esta tarea

El programa de instalación **pkgadd** instala IBM Security Directory Server en un sistema Solaris. Si se ha instalado una versión soportada de IBM DB2 en el sistema, el proceso de instalación actualizará el archivo `ldapdb.properties` con el nombre de la vía de acceso y versión de DB2.

Procedimiento

1. Inicie sesión como usuario root.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al directorio donde se almacena el instalable de IBM Security Directory Server.
4. Ejecute el mandato siguiente para instalar los paquetes:

```
swinstall -s vía_acceso_instalable_sds/idsldap.cltbase631.depot \*
swinstall -s vía_acceso_instalable_sds/idsldap.clt32bit631.depot \*
swinstall -s vía_acceso_instalable_sds/idsldap.clt64bit631.depot \*
swinstall -s vía_acceso_instalable_sds/idsldap.cltjava631.depot \*
```

5. Verifique si la instalación de IBM Security Directory Server se ha realizado correctamente. Para obtener más información, consulte el "Verificación de los paquetes de IBM Security Directory Server" en la página 87.

Resultados

El programa de instalación instala IBM Security Directory Server en el directorio `/opt/IBM/ldap/V6.3.1` en el sistema HP-UX.

Capítulo 13. Verificación de las características de IBM Security Directory Server

Tras la instalación, modificación o desinstalación de IBM Security Directory Server, debe verificar si las características de IBM Security Directory Server están correctamente instaladas, modificadas o desinstaladas.

Puede utilizar IBM Installation Manager o los programas de utilidad del sistema operativo para verificar si la instalación, la modificación, o la desinstalación es satisfactoria.

Verificación de las características de IBM Security Directory Server con IBM Installation Manager

Utilice IBM Installation Manager para verificar las características de IBM Security Directory Server y los productos necesarios que ha instalado con IBM Installation Manager.

Procedimiento

1. Inicie IBM Installation Manager.

   Windows
   Desde el menú **Inicio**, pulse **Todos los programas** > **IBM Installation Manager** > **IBM Installation Manager**.

   AIX y Linux
   Especifique el mandato siguiente en el indicador de mandatos. Modifique la siguiente vía de acceso predeterminada si IBM Installation Manager se ha instalado en una ubicación distinta.

   ```
   /opt/IBM/InstallationManager/eclipse/IBMIM
   ```

2. En la página **IBM Installation Manager**, pulse **Archivo** > **Ver paquetes instalados**.
3. Desde la lista **Paquetes y arreglos instalados** de la página **Paquete instalado**, expanda **IBM Security Directory Server**.
4. Desde la lista **Paquetes y arreglos instalados**, pulse la versión de IBM Security Directory Server para la que desea ver las características.
5. En el área **Detalles**, verifique la instalación de características y de productos necesarios.
6. Para cerrar la página **Paquete instalado**, pulse **Cerrar**.
7. Para cerrar **IBM Installation Manager**, pulse **Archivo** > **Salir**.

Verificación de las características de IBM Security Directory Server en Windows

Puede verificar si la instalación, la modificación o la desinstalación de IBM Security Directory Server ha sido satisfactoria comprobando el registro de Microsoft Windows.

Acerca de esta tarea

Microsoft Windows mantiene entradas de registro para realizar un seguimiento del software que se encuentra en un sistema Windows. Tras una instalación, modificación o desinstalación satisfactoria de las características de IBM Security Directory Server, se modificarán las entradas de registro para registrar la actualización más reciente del sistema. Un ejemplo de las entradas de registro se mostrará tras una instalación satisfactoria de las características de IBM Security Directory Server. Al modificar o desinstalar las características de IBM Security Directory Server, se modificarán las entradas de registro que realizan un seguimiento de las características para mostrar el estado más reciente. Las entradas de registro se muestran para Microsoft Windows en la arquitectura de AMD64/EM64T.

Procedimiento

1. Inicie la sesión en el sistema Windows con los privilegios del administrador.
2. Acceda al indicador de mandatos, y ejecute el mandato siguiente:
   ```
   regedit
   ```
3. En la ventana **Editor del registro**, pulse **Mi PC** > **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Wow6432NODE** > **IBM** > **IDSLDAP** > **6.3.1**

   Nota: Para verificar la instalación de IBM Security Directory Server en sistemas Microsoft Windows que se encuentran en la arquitectura de Intel x86 (IA32), expanda **Mi PC** > **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **IBM** > **IDSLDAP** > **6.3.1**.
   `Mi PC\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1` muestra las versiones principales de las características de IBM Security Directory Server que están instaladas en el sistema.

   ```
   BaseServerMajorVersion      6.3.1
   BitMode   64            ClientMajorVersion          6.3.1
   JavaClientMajorVersion      6.3.1
   LDAPHome                    ubicación_instalación
   ProxyServerMajorVersion     6.3.1
   ServerMajorVersion          6.3.1
   WebadminMajorVersion        6.3.1
   WebSphereAppSrvMajorVersion 7.0
   ```

   Las versiones secundarias de las características de IBM Security Directory Server que están instaladas en el sistema y se muestran en `Mi PC\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1`. Por ejemplo:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\BaseServer\
             BaseServerMinorVersion 1.0

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\Client\
             ClientMinorVersion 1.0

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\JavaClient\
             JavaClientMinorVersion 1.0

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\ProxyServer\
             ProxyServerMinorVersion 1.0

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\Server\
             ServerMinorVersion 1.0

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\Webadmin\
             WebadminMinorVersion 1.0
   ```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432NODE\IBM\IDSLDAP\6.3.1\WebSphereAppSrv\
          WebSphereAppSrvMinorVersion 0.25
```

4. Para cerrar la ventana **Editor del registro**, pulse **Archivo** > **Salir**.

Verificación de los paquetes de IBM Security Directory Server

Puede verificar si la instalación de IBM Security Directory Server se ha realizado correctamente comprobando el sistema para los paquetes de IBM Security Directory Server.

Acerca de esta tarea

Tras la instalación de IBM Security Directory Server, debe asegurarse de que los paquetes se encuentren en el nivel requerido. Puede consultar el número de versión de los paquetes de IBM Security Directory Server.

Procedimiento

1. Inicie sesión como usuario root.
2. Acceda a un indicador de mandatos, y ejecute el mandato siguiente:

Sistema operativo	Mandato para consultar los paquetes:
AIX	`lslpp -l 'idsldap*'`
Linux	`rpm -qa | grep -i idsldap`
Solaris	`pkginfo | grep IDSl` `pkgparam nombre_paquete VERSION`
HP-UX	`swlist | grep -i idsldap`

Resultados

El mandato lista los paquetes de IBM Security Directory Server que están instalados en el sistema.

Verificación de la versión de la Herramienta de administración web

Para verificar si se ha instalado o actualizado correctamente la Herramienta de administración web, debe verificar la versión de la Herramienta de administración web.

Procedimiento

1. Inicie sesión con los privilegios de administrador.
2. Vaya al directorio *ubicación_instalación_ds*/idstools. La *ubicación_instalación_ds* es la ubicación de instalación de IBM Security Directory Server. Las ubicaciones siguientes son las predeterminadas para varios sistemas operativos:

Tabla 36. La ubicación de instalación predeterminada de IBM Security Directory Server en varios sistemas operativos

Sistemas operativos	Ubicaciones de instalación predeterminadas:
Microsoft Windows	`c:\Program Files\IBM\ldap\V6.3.1`
AIX y Solaris	`/opt/IBM/ldap/V6.3.1`

Tabla 36. La ubicación de instalación predeterminada de IBM Security Directory Server en varios sistemas operativos (continuación)

Sistemas operativos	Ubicaciones de instalación predeterminadas:
Linux	`/opt/ibm/ldap/V6.3.1`

3. Ejecute el siguiente mandato:

Sistemas operativos	Mandato a ejecutar:
Microsoft Windows	`deploy_IDSWebApp.bat -v`
AIX, Linux, y Solaris	`deploy_IDSWebApp -v`

El mandato muestra la siguiente información:

- Los valores de versión y de fecha del mandato **deploy_IDSWebApp**.
- Los valores de versión y de fecha del archivo `IDSWebApp.war` instalado.
- Los valores de versión y de fecha del archivo `IDSWebApp.war` instalado en este momento.

Qué hacer a continuación

Debe comprobar los valores siguientes:

1. Si los valores de versión y de fecha del archivo instalado `IDSWebApp.war` son distintos de los valores de versión y de fecha del archivo `IDSWebApp.war` instalado en este momento.
2. Si los valores son distintos, instale la Herramienta de administración web más reciente en Web Application Server.

Verificación de la instalación de IBM Global Security Kit en Windows

Verifique el estado de la instalación de IBM Global Security Kit (GSKit) para confirmar si la instalación se ha realizado satisfactoriamente en Windows.

Procedimiento

1. Acceda al archivo `gskitinst.log`.

Sistema operativo	Vía de acceso predeterminada:
Windows	`C:\Program Files\IBM\ldap\V6.3.1\var`

2. Verifique si se ha creado el directorio siguiente: `C:\Program Files\IBM\gsk8`
3. Verifique si el archivo `gskitinst.log` contiene el valor `EXIT 0`. Si la instalación de IBM Global Security Kit ha sido satisfactoria, se establecerá 0; de lo contrario, se establecerá un valor distinto a cero.
4. Opcional: Si la instalación de IBM Global Security Kit no ha sido satisfactoria, los detalles de errores se almacenarán en el archivo `C:\Program Files\IBM\ldap\V6.3.1\var\gskitinsterr.log`.

Verificación de la instalación de IBM Global Security Kit en AIX, Linux, Solaris, y HP-UX

Verifique la instalación de IBM Global Security Kit (GSKit) para confirmar si la instalación ha sido satisfactoria.

Acerca de esta tarea

Tras la instalación de IBM Global Security Kit, debe asegurarse de que los paquetes se encuentren en el nivel requerido. Puede consultar el número de versión de IBM Global Security Kit.

Procedimiento

1. Inicie sesión como usuario root.
2. Acceda a un indicador de mandatos, y ejecute el mandato siguiente:

Sistema operativo	**Mandato a ejecutar:**
AIX	`lslpp -al | grep -i gsk`
Linux	`rpm -qa | grep -i gsk`
Solaris	`pkginfo | grep gsk` `pkgparam nombre_paquete VERSION`
HP-UX	`swlist | grep -i gsk`

Capítulo 14. Actualizar una instancia de una versión anterior

Para convertir una instancia existente en una instancia funcional de una versión más reciente y para continuar con los archivos de configuración existentes, debe actualizar una instancia.

El proceso de actualización mantiene los cambios en las definiciones de esquemas, los cambios en los archivos de configuración y los datos de una instancia de servidor de directorios.

La actualización de una instancia de una versión anterior requiere que finalice el siguiente proceso:

1. Completar la instalación de IBM Security Directory Server.
2. Actualizar una instancia existente de una versión anterior.

El servidor y el cliente de IBM Security Directory Server, versión 6.3.1 pueden coexistir con servidores y clientes de versiones 6.0, 6.1, 6.2, y 6.3.

Puede actualizar directamente las instancias de servidor de directorios de las siguientes versiones a IBM Security Directory Server, versión 6.3.1:

- IBM Security Directory Server, versión 6.3
- IBM Security Directory Server, versión 6.2
- IBM Security Directory Server, versión 6.1

Importante: La actualización directa de IBM Security Directory Server, de las instancias de versión 6.0 a IBM Security Directory Server, versión 6.3.1 no está soportada. Puede actualizar instancias 6.0 a 6.1, 6.2 o 6.3 y, a continuación, a 6.3.1.

Puede actualizar una instancia de una versión anterior de las siguientes formas:

- Actualización de una instancia existente en un sistema local con IBM Security Directory Server Herramienta de administración de instancias (**idsxinst**) o el mandato **idsimigr**. No debe eliminar la instancia de servidor de directorios que desea actualizar. Para obtener una instancia completa de servidor de directorios, no desconfigure la base de datos. La actualización no estará soportada si se elimina la instancia de servidor de directorios o si se desconfigura la base de datos.
- Actualización de una instancia en un sistema remoto con los mandatos **migbkup** e **idsimigr**. Para obtener más información, consulte el "Actualización de una instancia remota de una versión anterior con el mandato **idsimigr**" en la página 96.

Atención: Debe realizar una copia de seguridad de los esquemas, de los archivos de configuración, y de la base de datos de una instancia para recuperarse de anomalías de actualización.

Actualización de bases de datos de DB2

Al actualizar una instancia, también se actualizará su base de datos de DB2 asociada si la versión de DB2 es inferior que la versión soportada por IBM Security Directory Server, versión 6.3.1. El mandato **idsdbmigr** se ejecutará internamente para actualizar la base de datos de DB2.

Importante: La actualización directa de una instancia de servidor de directorios configurada con DB2, versión 9.1 a una instancia con DB2, versión 10.1.0.2 o inferior no está soportada. Puede actualizar una instancia configurada con DB2, versión 9.1 a una instancia con DB2, versión 10.1.0.2 o posterior de una de las formas siguientes:

- Actualice la instancia con DB2, versión 9.1 a una instancia con DB2, versión 9.5 y, a continuación, a una instancia con DB2, versión 10.1.0.2 o posterior.
- Actualice la instancia con DB2, versión 9.1 a una instancia con DB2, versión 9.7 y, a continuación, a una instancia con DB2, versión 10.1.0.2 o posterior.

Actualización de la instalación del cliente

Si ha instalado características únicamente del cliente con el instalador del cliente de IBM Security Directory Server, no necesita actualizar. Los clientes de la versión 6.0, 6.1, 6.2, y 6.3 pueden coexistir con el servidor y el cliente de 6.3.1.

Configuración del entorno para actualizar una instancia

Debe configurar el entorno del servidor de directorios para actualizar una instancia existente.

Antes de empezar

Debe completar las tareas siguientes para configurar el entorno:

- Acceda al soporte de instalación de IBM Security Directory Server.
- Complete la instalación de IBM Security Directory Server, versión 6.3.1. Consulte el apartado "Inicio de la instalación" en la página 28.
- Inicie sesión como usuario root en el sistema operativo AIX, Linux, o Solaris, y como un miembro del grupo de administradores en el sistema operativo Windows.

Procedimiento

1. Asegúrese de que el sistema operativo en el que está presente la instancia para la actualización está soportado por IBM Security Directory Server, versión 6.3.1.
2. Asegúrese de que la instancia de una versión anterior que desee actualizar se inicia satisfactoriamente. Si desea actualizar una instancia de servidor de directorios, debe configurar la base de datos, si aún no está configurada.

   Atención: No está soportada la actualización de un servidor proxy o de un servidor de directorios, si el servidor no se inicia satisfactoriamente.
3. Realice una copia de seguridad fuera de línea de la instancia que desee actualizar. Para una instancia de servidor de directorios, realice una copia de seguridad de las bases de datos y de los valores de DB2. Para obtener más información, consulte el mandato **idsdbback** en la *Consulta de mandatos*.
4. Para realizar una copia de seguridad de los archivos de esquemas y de configuración, ejecute el mandato **migbkup**:

Sistema operativo	Mandato a ejecutar:
Microsoft Windows	**migbkup.bat** drive_name\idsslapd-instance_name directorio_copia_seguridad
AIX, Linux, y Solaris	**migbkup** user_home_dir/idsslapd-instance_name directorio_copia_seguridad

El mandato **migbkup** se encuentra en el subdirectorio tools del soporte de

instalación de IBM Security Directory Server. Si ha completado la instalación de IBM Security Directory Server, el mandato **migbkup** se encontrará en la carpeta `sbin` de la ubicación de instalación de IBM Security Directory Server. El directorio siguiente es la ubicación de instalación predeterminada en distintos sistemas operativos:

Microsoft Windows
`C:\Program Files\IBM\ldap\V6.3.1`

AIX y Solaris
`/opt/IBM/ldap/V6.3.1`

Linux `/opt/ibm/ldap/V6.3.1`

El mandato **migbkup** realiza una copia de seguridad de los archivos siguientes:

- `ibmslapd.conf`
- `V3.config.at`
- `V3.config.oc`
- `V3.ibm.at`
- `V3.ibm.oc`
- `V3.system.at`
- `V3.system.oc`
- `V3.user.at`
- `V3.user.oc`
- `V3.modifiedschema`
- `V3.ldapsyntaxes`
- `V3.matchingrules`
- `ibmslapdcfg.ksf`
- `ibmslapddir.ksf`
- `perftune_stat.log`
- `perftune_input.conf`
- `ibmdiradmService.cmd` (para Windows)
- `ibmslapdService.cmd` (para Windows)

El mandato **migbkup** creará los archivos siguientes:

- `db2info` contiene la información de nombre de vía de acceso y de versión de la DB2 que utiliza la instancia de servidor de directorios. El mandato **idsimigr** o Herramienta de administración de instancias utiliza este archivo para actualizar las instancias y las bases de datos de DB2 al actualizar una instancia de servidor de directorios. Para una instancia de servidor proxy, este archivo no está disponible.
- `platforminfo` contiene la información sobre el sistema operativo y el tipo de proceso.

5. Si ha modificado manualmente el archivo `V3.modifiedschema` de una instancia para su actualización, el archivo no debe contener ningún OID (duplicate object identifiers) para clases de objetos o atributos. Si el archivo contiene OID duplicados, no se conservarán durante la actualización. Si el archivo de esquemas contiene OID duplicados, el OID del `V3.modifiedschema` se conservará. Si los archivos de esquemas no contienen los atributos o las clases de objetos, es posible que no se inicie el servidor de administración ni el proceso `idsslapd`. En tales situaciones, debe añadir manualmente los atributos que faltan o las clases de objetos a los archivos de esquemas antes de iniciar los servidores.

6. Si ha configurado la instancia con archivos de esquemas personalizados, copie los archivos manualmente al directorio de copia de seguridad. Al realizar una copia de seguridad de los esquemas y de los archivos de configuración, el mandato **migbkup** realiza una copia de seguridad de los archivos de esquemas personalizados. Sin embargo, es posible que estos archivos de esquemas no se utilicen al actualizar la instancia.

Qué hacer a continuación

Tras configurar el entorno, ejecute el mandato **idsimigr** o Herramienta de administración de instancias para actualizar una instancia desde una versión anterior. Para actualizar una instancia, utilice uno de los métodos siguientes:

- "Actualización de una instancia de una versión anterior con el mandato **idsimigr**"
- "Actualización de una instancia de una versión anterior con Herramienta de administración de instancias" en la página 152

Actualización de una instancia de una versión anterior con el mandato idsimigr

Utilice el mandato **idsimigr** para actualizar una instancia de servidor de directorios o una instancia de servidor proxy de una versión anterior a la versión actual.

Antes de empezar

Debe completar las tareas siguientes para actualizar una instancia con el mandato **idsimigr**:

- Complete la instalación de IBM Security Directory Server.Consulte el apartado "Inicio de la instalación" en la página 28.
- Configure el entorno antes de actualizar una instancia. Consulte el apartado "Configuración del entorno para actualizar una instancia" en la página 92.
- Inicie sesión como usuario root en el sistema operativo AIX, Linux, o Solaris, y como un miembro del grupo de administradores en el sistema operativo Windows.

También puede actualizar una instancia existente en un sistema con Herramienta de administración de instancias. Para obtener más información, consulte el "Actualización de una instancia de una versión anterior con Herramienta de administración de instancias" en la página 152.

Acerca de esta tarea

Tras actualizar una instancia de una versión anterior, la instancia se convierte en una instancia totalmente funcional de la versión actual de IBM Security Directory Server.

Procedimiento

1. Acceda al indicador de mandatos.
2. Cambie el directorio de trabajo actual a `sbin`. La ubicación predeterminada es la predeterminada en varios sistemas operativos:

   Microsoft Windows

   ```
   C:\Program Files\IBM\ldap\V6.3.1\sbin
   ```

AIX y Solaris
/opt/IBM/ldap/V6.3.1/sbin

Linux /opt/ibm/ldap/V6.3.1/sbin

3. Detenga el proceso de ibmslapd y el servidor de administración de la instancia que tiene previsto actualizar.

```
ibmslapd -I nombre_instancia -k
ibmdiradm -I nombre_instancia -k
```

4. No desinstale la versión del producto de IBM Security Directory Server asociada con la instancia que tiene previsto actualizar.
5. Ejecute el mandato **idsimigr** para actualizar la instancia desde una versión anterior a la versión actual de IBM Security Directory Server.

```
idsimigr -I nombre_instancia
```

6. Inicie el proceso de ibmslapd y el servidor de administración de la instancia.

```
ibmslapd -I nombre_instancia -n
ibmdiradm -I nombre_instancia
```

7. Realice una copia de seguridad fuera de línea de la instancia. Consulte el apartado “Copia de seguridad de servidor de directorios” en la página 195.

Actualizar una instancia de una versión anterior a un sistema distinto

Puede actualizar una instancia existente de una versión anterior que esté en un sistema a una versión posterior en un sistema distinto.

Es posible que desee actualizar una instancia existente de forma remota por uno de los siguientes motivos:

- El sistema operativo de un sistema en el que existe una instancia de una versión anterior puede no ser un sistema operativo soportado por IBM Security Directory Server, versión 6.3.1. Es posible que no desee actualizar o cambiar el sistema operativo en el sistema.
- Desea instalar IBM Security Directory Server, versión 6.3.1 en un sistema con un sistema operativo que es distinto del sistema operativo en el que existe una versión anterior. Sin embargo, desea crear una instancia con la información como la instancia existente de una versión anterior. Por ejemplo, tiene una instancia existente de una versión anterior en un sistema AMD64/EM64T Linux, pero desea el servidor 6.3.1 en un sistema AIX. En tal caso, los dos sistemas operativos deben ser del mismo tipo de bytes. Si el primer sistema es de byte menos significativo, el segundo sistema debe ser también de byte menos significativo. El tipo de bytes tiene que ver con el orden de bits utilizado para representar los datos en la memoria. Si los sistemas operativos no tienen el mismo tipo de bytes, no estará soportada la actualización de una instancia.

El procedimiento para la actualización remota es similar al procedimiento para la actualización en el mismo sistema. La excepción es que debe copiar los archivos de copia de seguridad del sistema a un sistema donde instale IBM Security Directory Server, versión 6.3.1.

Nota: Si actualiza una instancia remota desde un sistema que participa en la réplica, realice las acciones siguientes:

- Habilite la réplica con el sistema de origen como proveedor.
- Habilite la réplica con el sistema de destino como consumidor.

La réplica garantiza que las actualizaciones se ponen en cola y que se pueden replicar cuando el sistema de destino se pone en línea de nuevo. Debe habilitar la réplica antes de realizar la copia de seguridad de una instancia en el sistema de origen.

Sistemas operativos soportados para actualizar una instancia remota

Para actualizar una instancia remota en un sistema operativo de destino adecuado, debe identificar los sistemas operativos que son el origen y el destino para una instancia.

Tabla 37. Sistemas operativos soportados de origen y de destino para la actualización remota de instancias

	Sistema operativo: sistema de destino (IBM Security Directory Server, versión 6.3.1)								
Sistema operativo: sistema de origen (IBM Security Directory Server, 6.3 o anterior) ↓	**Intel Windows de 32 bits**	**AMD64/ EM64T Windows**	**System x Linux (de 32 bits)**	**AMD64/ EM64T Linux**	**System i y System p Linux**	**System z Linux**	**AIX**	**Solaris SPARC**	**Solaris X64**
Intel Windows de 32 bits	✓	✓	✓	✓					✓
AMD/ EM64T Windows	✓	✓	✓	✓					✓
System x Linux (de 32 bits)	✓	✓	✓	✓					✓
AMD/ EM64T Linux	✓	✓	✓	✓					✓
System i y System p Linux					✓	✓	✓	✓	
System z Linux					✓	✓	✓	✓	
AIX					✓	✓	✓	✓	
Solaris SPARC					✓	✓	✓	✓	
Solaris X64	✓	✓	✓	✓					✓

Actualización de una instancia remota de una versión anterior con el mandato `idsimigr`

Utilice el mandato **idsimigr** con el parámetro **-u** para actualizar una instancia de servidor de directorios remota o una instancia de servidor proxy de una versión anterior a la versión 6.3.1.

Antes de empezar

Debe realizar las siguientes tareas para actualizar una instancia con el mandato **idsimigr** con el parámetro **-u**:

- Configure el entorno antes de actualizar una instancia. Consulte "Configuración del entorno para actualizar una instancia" en la página 92.
- Inicie sesión como usuario root en el sistema operativo AIX, Linux, o Solaris, y como un miembro del grupo de administradores en el sistema operativo Windows.

También puede actualizar una instancia remota con archivos de copia de seguridad utilizando Herramienta de administración de instancias. Para obtener más información, consulte el "Actualización de una instancia remota de una versión anterior con Herramienta de administración de instancias" en la página 153.

Acerca de esta tarea

Tras completar el proceso de actualización, el mandato **idsimigr** creará una instancia de 6.3.1 en el sistema con la información desde la instancia remota.

Procedimiento

1. Realice una copia de seguridad de la base de datos de una instancia de servidor de directorios que se encuentra en un sistema remoto con el mandato **idsdb2ldif**.

   Importante: Si está actualizando una instancia de servidor proxy, no realice una copia de seguridad de la base de datos. El servidor proxy no contiene ninguna base de datos asociada con él.

   ```
   idsdb2ldif -I nombre_instancia -o inst_out.ldif
   ```

   Para obtener más información sobre el mandato **idsdb2ldif**, consulte la *Consulta de mandatos*.
2. Complete la instalación de IBM Security Directory Server en un sistema en el que desee actualizar la instancia remota. Consulte "Inicio de la instalación" en la página 28.
3. Para realizar una copia de seguridad de los esquemas y de los archivos de configuración de la instancia remota, ejecute el mandato **migbkup** de la versión a la que desea actualizar:

Sistema operativo	Mandato a ejecutar:
Microsoft Windows	**migbkup.bat** drive_name\idsslapd-instance_name directorio_copia_seguridad
AIX, Linux, y Solaris	**migbkup** user_home_dir/idsslapd-instance_name directorio_copia_seguridad

   El mandato **migbkup** se encuentra en el subdirectorio tools del soporte de instalación de IBM Security Directory Server.
4. Copie el directorio de copia de seguridad, directorio_copia_seguridad, que ha creado con **migbkup**, desde el sistema remoto al sistema con IBM Security Directory Server.
5. Opcional: Copie el archivo de copia de seguridad de la base de datos, inst_out.ldif, desde el sistema remoto al sistema con IBM Security Directory Server.

6. Ejecute el mandato **idsimigr** con el parámetro **-u** para crear una instancia con los datos de copia de seguridad de la instancia remota.

   ```
   idsimigr -u directorio_copia_seguridad
   ```

7. Configure una base de datos, un sufijo y un nombre distinguido de administrador y una contraseña para la instancia de servidor de directorios.

   Importante: Si está actualizando una instancia de servidor proxy, no ejecute el mandato **idscfgdb** para configurar una base de datos.

   ```
   idscfgdb -I nombre_instancia –a id_admin_bd –w pwd_admin_bd –t nombre_bd –l ubicación_bd
   idscfgsuf -I nombre_instancia –s sufijo
   idsdnpw -I nombre_instancia –u DN_admin –p PWD_admin
   ```

8. Opcional: Ejecute el mandato **idsldif2db** para importar el archivo de copia de seguridad de la base de datos, `inst_out.ldif`, a la instancia de servidor de directorios actualizada.
9. Inicie el proceso de `ibmslapd` y el servidor de administración de la instancia.

   ```
   ibmslapd -I nombre_instancia -n
   ibmdiradm -I nombre_instancia
   ```

10. Realice una copia de seguridad de la instancia. Para obtener más información, consulte el “Copia de seguridad de servidor de directorios” en la página 195.

Enlaces a programas de utilidad del cliente y del servidor

Puede utilizar el mandato **idslink** para establecer los enlaces para las bibliotecas y los programas de utilidad de línea de mandatos del servidor de directorios.

Después de la instalación de IBM Security Directory Server, puede establecer enlaces para programas de utilidad de cliente y servidor. Estos enlaces no se establecen automáticamente durante la instalación.

Si ha configurado enlaces a programas de utilidad de una versión anterior de IBM Security Directory Server, los enlaces permanecen a no ser que los modifique. Para eliminar los enlaces que se definan mediante el mandato `idslink`, utilice el mandato **idsrmlink**.

Puede utilizar el mandato **idslink** para establecer los enlaces en los programas de utilidad de línea de mandatos, como por ejemplo **idsldapmodify** e **idsldapadd**, y bibliotecas, como por ejemplo `libibmldap.so`. Estos enlaces apuntan a la ubicación donde se almacenan las bibliotecas y los programas de utilidad de IBM Security Directory Server.

Para obtener más información sobre los mandatos **idslink** e **idsrmlink**, consulte la *Consulta de mandatos*.

Capítulo 15. Migración de datos y soluciones de una instancia de una versión anterior

Puede migrar datos de directorio, soluciones, o ambos, que haya configurado con una instancia de una versión anterior para utilizarlos con una instancia de 6.3.1.

Migración de datos de DB2 de IBM DB2 Enterprise Server Edition (ESE) a IBM DB2 Workspace Server Edition (WSE)

En System x Linux (arquitectura de Intel de 32 bits), IBM DB2 ESE, versión 9.7 o posterior no está soportado. En System x Linux, IBM Security Directory Server utiliza IBM DB2 WSE, versión 9.7, Fixpack 6 o posterior para crear y configurar la base de datos.

Al actualizar una instancia de 6.1 o 6.2 con datos a 6.3.1, es posible que requiera ejecutar la actualización remota de una instancia. Puede actualizar una instancia de 6.3 con DB2 WSE, versión 9.7 o posterior a una instancia de 6.3.1 con DB2 WSE, versión 9.7 o posterior. En System x Linux, la actualización directa de una instancia de 6.1 o 6.2 con DB2 ESE, versión 9.1 o posterior a una instancia de 6.3.1 con DB2 WSE, versión 9.7 o posterior puede fallar. Para obtener más información sobre cómo migrar la base de datos DB2 ESE a DB2 WSE, consulte "Migración de una instancia con una base de datos DB2 ESE a una instancia con una base de datos DB2 WSE" en la página 100.

Migración de soluciones de servidor de directorios que se basan en IBM Security Directory Integrator

Para utilizar soluciones configuradas con una versión anterior de instancia con una instancia de 6.3.1, debe migrar estas soluciones.

Están soportadas las siguientes soluciones:

- Herramienta de gestión del registro
- Simple Network Management Protocol (SNMP)
- Sincronización de Active Directory

Para obtener más información acerca de las soluciones del servidor de directorios, consulte los temas de *Administración* en la documentación del producto IBM Security Directory Server.

Para que la solución funcione, el sistema debe contener IBM Security Directory Integrator, versión 7.1. Para obtener más información acerca de la instalación y administración de IBM Security Directory Integrator, con la sección *Instalación y administración* de la documentación del producto en http://www-01.ibm.com/support/knowledgecenter/SSCQGF/welcome.

Si la vía de acceso de instalación de IBM Security Directory Integrator es distinta de la vía de acceso de instalación predeterminada, establezca la variable *IDS_LDAP_TDI_HOME* con la ubicación de instalación de IBM Security Directory Integrator. Las siguientes vías de acceso de instalación son las predeterminadas para IBM Security Directory Integrator, versión 7.1, en diversos sistemas operativos:

AIX, Linux, y Solaris

```
/opt/IBM/TDI/V7.1
```

Windows

```
C:\Program Files\IBM\TDI\V7.1
```

Migración de una instancia con una base de datos DB2 ESE a una instancia con una base de datos DB2 WSE

Para actualizar una instancia de 6.1 o 6.2 con DB2 ESE a una instancia de 6.3.1 con DB2 WSE, migre datos desde la base de datos DB2 ESE a la base de datos DB2 WSE.

Antes de empezar

Debe completar las tareas siguientes antes de migrar datos de una instancia de una versión anterior a una instancia de 6.3.1:

- Complete la instalación de IBM Security Directory Server, versión 6.3.1 con IBM DB2 WSE. Consulte el apartado "Inicio de la instalación" en la página 28.
- Configure el entorno antes de actualizar una instancia. Consulte el apartado "Configuración del entorno para actualizar una instancia" en la página 92.
- Inicie sesión como usuario root en el sistema operativo AIX, Linux, o Solaris, y como un miembro del grupo de administradores en el sistema operativo Windows.

Procedimiento

1. Detenga la instancia de servidor de directorios desde la que desea migrar los datos de directorio.
2. Ejecute el mandato **migbkup** que se proporciona con IBM Security Directory Server, versión 6.3.1 para realizar una copia de seguridad de la instancia. Consulte el apartado "Configuración del entorno para actualizar una instancia" en la página 92. Para obtener más información sobre el mandato **migbkup**, consulte *Consulta de mandatos*.
3. Realice una copia de seguridad de la base de datos de la instancia de servidor de directorios desde la que desea migrar datos. Para realizar una copia de seguridad de la base de datos de una instancia, `dsrdbm01`, siga estos pasos:
   a. Cambie el contexto de usuario al propietario de la instancia de DB2.
      ```
      su - dsrdbm01
      ```
   b. Ejecute el `db2profile` para el usuario.
      ```
      sqllib/db2profile
      ```
   c. Realice una copia de seguridad de la base de datos de DB2 para la instancia.
      ```
      db2 backup database dsrdbm01 to directorio_copia_seguridad_base_datos
      ```
      El propietario de la base de datos debe tener permisos de lectura, grabación y ejecución en el directorio de copia de seguridad de la base de datos, `directorio_copia_seguridad_base_datos`.
   d. Realice una copia de seguridad de la base de datos de registro de cambios si está configurada para la instancia de servidor de directorios.
      ```
      db2 backup db ldapclog to directorio_copia_seguridad_registro_cambios
      ```
      El propietario de la base de datos debe tener permisos de lectura, grabación y ejecución en el directorio de copia de seguridad del registro de cambios, `directorio_copia_seguridad_registro_cambios`.
   e. Ejecute el mandato `exit` para salir del contexto de usuarios.

4. Suprima la instancia de servidor de directorios con la base de datos. Para obtener más información sobre la supresión de una instancia con la base de datos, consulte "Supresión de una instancia con el programa de utilidad de línea de mandatos" en la página 169.
5. Cambie el directorio de trabajo actual al subdirectorio `sbin` de la ubicación de instalación de IBM Security Directory Server, versión 6.3.1.
6. Para utilizar el directorio de copia de seguridad de instancias para la actualización remota de una instancia, ejecute el mandato **idsimigr** en el formato siguiente:

   ```
   idsimigr -I dsrdbm01 -u ubicación_copia_seguridad_instancia
    -l directorio_inicio_instancia -n
   ```

7. Para configurar la instancia, ejecute el mandato **idscfgdb** en el formato siguiente:

   ```
   idscfgdb -I dsrdbm01 -a propietario_base_datos -w contraseña
    -t dsrdbm01 -l directorio_inicio_instancia -n
   ```

8. Si se ha configurado la base de datos de registro de cambios para la instancia, configure la base de datos de registro de cambios para la instancia:

   ```
   idscfgchglg -I dsrdbm01 -n
   ```

9. Restaure la base de datos a partir de la imagen de copia de seguridad. Para restaurar la base de datos de una instancia, `dsrdbm01`, siga estos pasos:
   a. Cambie el contexto de usuario al propietario de la instancia de DB2.

      ```
      su - dsrdbm01
      ```

   b. Restaure la base de datos de DB2 para la instancia.

      ```
      db2 restore database dsrdbm01 from dir_copia_seguridad_bd replace existing
      ```

   c. Restaure la base de datos del registro de cambios si está configurada para la instancia de servidor de directorios.

      ```
      db2 restore db ldapclog from  directorio_copia_seguridad_registro_cambios
      ```

   d. Ejecute el mandato `exit` para salir del contexto de usuarios.
10. Para catalogar la base de datos restaurada, ejecute los mandatos siguientes:

    ```
    su - dsrdbm01
    db2 uncatalog database dsrdbm01
    db2 catalog database dsrdbm01 as dsrdbm01 authentication server
    exit
    ```

11. Para catalogar la base de datos de registro de cambios restaurada, ejecute los mandatos siguientes:

    ```
    su - dsrdbm01
    db2 uncatalog database ldapclog
    db2 catalog database ldapclog as ldapclog authentication server
    exit
    ```

12. Inicie el servidor de directorios y el servidor de administración.

    ```
    ibmslapd -I dsrdbm01 -n -t
    ibmdiradm -I dsrdbm01
    ```

Migración de la solución de gestión de registro

Puede migrar la solución de gestión de registro que se ha configurado con una instancia de una versión anterior en una instancia de 6.3.1.

Antes de empezar

Debe completar las tareas siguientes para migrar la solución de gestión de registro de una instancia de una versión anterior a una instancia 6.3.1:

- Complete la instalación de IBM Security Directory Server, versión 6.3.1. Consulte el apartado "Inicio de la instalación" en la página 28.
- Complete la instalación de IBM Security Directory Integrator, versión 7.1, si no está instalado en el sistema.
- Inicie sesión como usuario root en el sistema operativo AIX, Linux, o Solaris, y como un miembro del grupo de administradores en el sistema operativo Windows.

Procedimiento

1. Realice una copia de seguridad del archivo `solution.properties` que se encuentra en el directorio *inicio_instancia_DS*`/idsslapd-`*nombre_instancia*`/etc/logmgmt` para la instancia de servidor de directorios existente.
2. Actualice la versión anterior de la instancia a la instancia 6.3.1. Consulte el apartado Capítulo 14, "Actualizar una instancia de una versión anterior", en la página 91.
3. Elimine todos los archivos y subdirectorios del directorio *inicio_instancia_DS*`/idsslapd-`*nombre_instancia*`/etc/logmgmt` para la instancia actualizada.
4. Si IBM Security Directory Integrator es anterior a la versión 7.1, complete la instalación de IBM Security Directory Integrator, versión 7.1.
5. Cambie el contexto de usuario como propietario de la instancia de servidor de directorios.

   ```
   su - propietario_instancia
   ```
6. Copie los archivos siguientes:
   a. Copie los archivos y directorios de *ubicación_instalación_Directory_Integrator_v7.1*`/etc` a *inicio_instancia_DS*`/idsslapd-`*nombre_instancia*`/etc/logmgmt`.
   b. Copie los archivos y directorios de *ubicación_instalación_Directory_Integrator_v7.1*`/serverapi` a *inicio_instancia_DS*`/idsslapd-`*nombre_instancia*`/etc/logmgmt`.
   c. Copie *ubicación_instalación_Directory_Integrator_v7.1*`/idisrv.sth` a *inicio_instancia_DS*`/idsslapd-`*nombre_instancia*`/etc/logmgmt`.
   d. Copie *ubicación_instalación_Directory_Integrator_v7.1*`/testserver.jks` a *inicio_instancia_DS*`/idsslapd-`*nombre_instancia*`/etc/logmgmt`.
7. Cree un directorio con el nombre `logs` en *inicio_instancia_DS*`/idsslapd-`*nombre_instancia*`/etc/logmgmt`.
8. Añada la entrada `systemqueue.on=false` al final del archivo *inicio_instancia_DS*`/idsslapd-`*nombre_instancia*`/etc/logmgmt/solutions.properties`.
9. Si la vía de acceso de instalación de IBM Security Directory Integrator, versión 7.1 es distinta de la vía de acceso predeterminada, configure la variable *IDS_LDAP_TDI_HOME* con la ubicación de instalación.
10. Ejecute la solución de gestión de registro.

Migración de la solución SNMP

Puede migrar la solución Simple Network Management Protocol (SNMP) configurada con una instancia de una versión anterior a una instancia de 6.3.1.

Antes de empezar

Debe completar las tareas siguientes para migrar la solución SNMP de una instancia de una versión anterior a una instancia 6.3.1:

- Complete la instalación de IBM Security Directory Server, versión 6.3.1. Consulte el apartado "Inicio de la instalación" en la página 28.
- Complete la instalación de IBM Security Directory Integrator, versión 7.1, si no está instalado en el sistema.
- Inicie sesión como usuario root en el sistema operativo AIX, Linux, o Solaris, y como un miembro del grupo de administradores en el sistema operativo Windows.

Procedimiento

1. Realice una copia de seguridad del directorio `snmp` que se encuentra en la ubicación de instalación de IBM Security Directory Server asociada con la instancia existente de la versión anterior.
2. Actualice la versión anterior de la instancia a la instancia 6.3.1. Consulte el apartado Capítulo 14, "Actualizar una instancia de una versión anterior", en la página 91.
3. Sustituya el archivo `/idstools/snmp/idssnmp.conf` que se encuentra en la vía de acceso de instalación de IBM Security Directory Server, versión 6.3.1, por el archivo `/idstools/snmp/idssnmp.conf` que se encuentra en la vía de acceso de instalación de la versión anterior de IBM Security Directory Server.
4. Sustituya el archivo `/idstools/snmp/idssnmp.properties` que se encuentra en la vía de acceso de instalación de IBM Security Directory Server, versión 6.3.1, por el archivo `/idstools/snmp/idssnmp.properties` que se encuentra en la vía de acceso de instalación de la versión anterior de IBM Security Directory Server.
5. Sustituya el archivo `/idstools/snmp/IBM-DIRECTORYSERVER-MIB` que se encuentra en la vía de acceso de instalación de IBM Security Directory Server, versión 6.3.1, por el archivo `/idstools/snmp/IBM-DIRECTORYSERVER-MIB` que se encuentra en la vía de acceso de instalación de la versión anterior de IBM Security Directory Server.
6. Sustituya el archivo `/idstools/snmp/INET-ADDRESS-MIB` que se encuentra en la vía de acceso de instalación de IBM Security Directory Server, versión 6.3.1, por el archivo `/idstools/snmp/INET-ADDRESS-MIB` que se encuentra en la vía de acceso de instalación de la versión anterior de IBM Security Directory Server.
7. Si la vía de acceso de instalación de IBM Security Directory Integrator, versión 7.1 es distinta de la vía de acceso predeterminada, configure la variable *IDS_LDAP_TDI_HOME* con la ubicación de instalación.
8. Ejecute la solución SNMP.

Migración de la solución de sincronización de Active Directory

Puede migrar la solución de sincronización de Active Directory configurada con una instancia de una versión anterior a una instancia de 6.3.1.

Antes de empezar

Debe completar las tareas siguientes para migrar la solución de sincronización de Active Directory desde una instancia de una versión anterior a una instancia de 6.3.1:

- Complete la instalación de IBM Security Directory Server, versión 6.3.1. Consulte el apartado "Inicio de la instalación" en la página 28.

- Complete la instalación de IBM Security Directory Integrator, versión 7.1, si no está instalado en el sistema.
- Inicie sesión como usuario root en el sistema operativo AIX, Linux, o Solaris, y como un miembro del grupo de administradores en el sistema operativo Windows.

Desde IBM Security Directory Server, versión 6.3.1, la solución de sincronización Active Directory está en desuso. En su lugar, utilice la solución LDAPSync.

Procedimiento

1. Actualice la versión anterior de la instancia a la instancia 6.3.1. Consulte el apartado Capítulo 14, "Actualizar una instancia de una versión anterior", en la página 91.
2. Cree una instancia de servidor de directorios. Consulte el apartado "Creación de instancias con Herramienta de administración de instancias" en la página 136.
3. Configure la instancia de servidor de directorios para la sincronización de Active Directory. Consulte el apartado "Sincronización de Active Directory" en la página 222.
4. Restaure los cambios en el archivo *inicio_instancia_DS*/idsslapd-*nombre_instancia*/etc/tdisoldir/solution.properties antes de actualizar la instancia.

   Nota: Si sustituye el archivo solution.properties recientemente creado por el archivo anterior, es posible que falle la sincronización de Active Directory. El formato del archivo solution.properties que se crea al ejecutar el mandato **idsadscfg** es distinto del archivo anterior.
5. Ejecute la solución de sincronización de Active Directory. Para obtener más información sobre el mandato **idsadsrun**, consulte *Consulta de mandatos*.

Migrar una versión anterior de la configuración de la Herramienta de administración web

Migre una versión anterior de la configuración de la Herramienta de administración web para continuar utilizando los mismos valores con una versión posterior de la Herramienta de administración web.

Para migrar una configuración existente de la Herramienta de administración web de una versión anterior con el mandato **idswmigr**, se deben cumplir las siguientes condiciones:

1. La versión anterior de la Herramienta de administración web se ha instalado en el sistema.
2. La versión anterior de WebSphere Application Server incorporado se ha instalado en el sistema.
3. La versión anterior de la Herramienta de administración web se ha desplegado en la versión anterior de WebSphere Application Server incorporado.
4. Instale la Herramienta de administración web que se proporciona con IBM Security Directory Server, versión 6.3.1.
5. Instale WebSphere Application Server incorporado que se proporciona con IBM Security Directory Server, versión 6.3.1.
6. No despliegue la Herramienta de administración web que se proporciona con 6.3.1 en WebSphere Application Server incorporado.

La Herramienta de administración web de las siguientes versiones de IBM Security Directory Server que está desplegada en la siguiente versión de WebSphere Application Server incorporado está soportada para la migración:

- IBM Security Directory Server, versión 6.1 y WebSphere Application Server incorporado, versión 6.1.0.7 o posterior
- IBM Security Directory Server, versión 6.2 y WebSphere Application Server incorporado, versión 6.1.0.13 o posterior (en UNIX) o WebSphere Application Server incorporado, versión 6.1.0.17 (en Windows) o posterior
- IBM Security Directory Server, versión 6.3 y WebSphere Application Server incorporado, versión 7.0.0.7 o posterior

Al utilizar el mandato **idswmigr** para migrar los valores de configuración de una versión anterior de la Herramienta de administración web, el mandato realiza las siguientes operaciones:

1. Guarda los archivos de configuración para la versión anterior de la Herramienta de administración web.
2. Desinstala la versión anterior de la Herramienta de administración web de la versión anterior de WebSphere Application Server incorporado.
3. Realiza una copia de seguridad de la configuración de la versión anterior de WebSphere Application Server incorporado en una ubicación temporal que se especifique.
4. Restaura la configuración de la versión anterior de WebSphere Application Server incorporado en una ubicación.
5. Instala la Herramienta de administración web en la versión actual de WebSphere Application Server incorporado que se proporciona con IBM Security Directory Server, versión 6.3.1.
6. Migra los archivos de configuración anteriores de la Herramienta de administración web y restaura estos archivos en la versión posterior de WebSphere Application Server incorporado.

Nota: La migración de la Herramienta de administración web será posible utilizando IBM Installation Manager solo si la versión de WebSphere Application Server incorporado que se ha de migrar es más pequeña que la versión principal de WebSphere Application Server incorporado (recién instalada).

idswmigr

Utilice el mandato **idswmigr** para migrar una configuración existente de la Herramienta de administración web de una versión anterior a una versión posterior de la Herramienta de administración web.

Descripción

Para migrar una configuración existente de la Herramienta de administración web de una versión anterior con el mandato **idswmigr**, se deben cumplir las siguientes condiciones:

1. La versión anterior de la Herramienta de administración web se ha instalado en el sistema.
2. La versión anterior de WebSphere Application Server incorporado se ha instalado en el sistema.
3. La versión anterior de la Herramienta de administración web se ha desplegado en la versión anterior de WebSphere Application Server incorporado.
4. Instale la versión posterior de la Herramienta de administración web.

5. Instale la versión posterior de WebSphere Application Server incorporado.
6. No despliegue la Herramienta de administración web que sea de una versión posterior en el WebSphere Application Server incorporado.

Sinopsis

```
idswmigr -l vía_acceso_temp [-s vía_acceso_origen -t vía_acceso_destino
         -r nombre_perfil -a nombre_apl -v -o vía_acceso_puertos]
```

Opciones

El mandato **idswmigr** toma los parámetros siguientes:

-a *nombre_apl*
Especificado en el nombre de la aplicación. Si no se especifica, el valor predeterminado es `IDSWebApp.war`.

-l *vía_acceso_temp*
Especifica una ubicación para almacenar los archivos temporales.

-o *vía_acceso_puertos*
Especifica la vía de acceso completa del archivo de definición de puertos. Si no se especifica, se utilizará la vía de acceso predeterminada siguiente:

Windows
`C:\Program Files\IBM\ldap\V6.3.1\idstools\TDSWEBPortDef.props`

AIX y Solaris
`/opt/IBM/ldap/V6.3.1/idstools/TDSWEBPortDef.props`

Linux `/opt/ibm/ldap/V6.3.1/idstools/TDSWEBPortDef.props`

-r *nombre_perfil*
Especifica el nombre del perfil asociado con la aplicación. Si no se especifica, el valor predeterminado será `TDSWebAdminProfile`.

-s *vía_acceso_origen*
Especifica la ubicación de origen para la versión anterior de WebSphere Application Server incorporado.

-t *vía_acceso_destino*
Especifica la ubicación de instalación de una versión posterior de WebSphere Application Server incorporado.

-v
Muestra la información de la versión.

Ejemplos

Ejemplo 1

Para migrar una configuración existente de la Herramienta de administración web de la versión 6.2 a la versión 6.3.1, ejecute el mandato siguiente:

```
idswmigr -l /tmp/web_migr -s /opt/ibm/ldap/V6.2/appsrv \
-t /opt/ibm/ldap/V6.3.1/appsrv -r TDSWebAdminProfile \
-a IDSWebApp.war
```

Migración manual de la herramienta de administración web

Puede migrar manualmente la herramienta de administración web.

Antes de empezar

Para migrar manualmente la herramienta de administración, en primer lugar, debe estar instalada la herramienta de migración web. Siga los pasos para migrar la herramienta de administración web manualmente. En el ejemplo que se muestra, la herramienta de administración web en IBM Security Directory Server V6.3 se migra a IBM Security Directory Server V6.3.1.

En AIX, los mandatos de migración son similares a los mandatos de Linux, excepto la vía de acceso `/opt/ibm/ldap` que debería sustituirse por `/opt/IBM/ldap`.

Procedimiento

1. En Windows, añada el servicio de WebSphere Application Server mediante el mandato siguiente:

   ```
   "C:\Program Files\IBM\ldap\V6.3.1\appsrv\bin\WASService.exe" -add
   TDSWebAdmin-V6.3.1 -serverName server1 -profilePath
   "C:\Program Files\IBM\ldap\V6.3.1\appsrv\profiles\TDSWebAdminProfile"
   -startType automatic
   ```

2. Realice una copia de seguridad de la herramienta de administración web archivos desde el release anterior.
   - En Windows, busque estos archivos bajo el directorio:

     ```
     C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\
      installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\
      WEB-INF\classes\
     ```

     o

     ```
     C:\Program Files\IBM\LDAP\V6.3\appsrv\installedApps\DefaultNode
     \IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes
     ```

   - En Linux, busque estos archivos bajo el directorio siguiente:

     ```
     /opt/ibm/ldap/V6.3/appsrv/profiles/TDSWebAdminProfile/installedApps
     /DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes
     ```

     o

     ```
     /opt/ibm/ldap/V6.3/appsrv/installedApps/DefaultNode
     /IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes
     ```

   Copie sólo los siguientes cinco archivos de los directorios:

   ```
   security\console_passwd
   IDSConfig\IDSSessionConfig\IDSSessionMgmt.xml
   IDSConfig\IDSServersConfig\IDSServersInfo.xml
   IDSConfig\IDSAppReg\IDSAppReg.xml
   IDSConfig\IDSSearchSettings\IDSSearchMgmt.xml
   ```

   Por ejemplo:

   ```
     copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\
   installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\
   security\console_passwd" c:\BackUp
     copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\
   installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\
   IDSConfig\IDSSessionConfig\IDSSessionMgmt.xml" c:\BackUp
     copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\
   installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\
   IDSConfig\IDSServersConfig\IDSServersInfo.xml" c:\BackUp
     copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\
   installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\
   IDSConfig\IDSAppReg\IDSAppReg.xml" c:\BackUp
   ```

```
  copy "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\
installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\classes\
IDSConfig\IDSSearchSettings\IDSSearchMgmt.xml" c:\BackUp
```

3. Desinstale el archivo war del release anterior.
   - En Windows, el mandato se encuentra bajo el directorio siguiente:

     ```
     C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\bin\wsadmin.bat
     ```

     o

     ```
     C:\Program Files\IBM\LDAP\V6.3\appsrv\bin\wsadmin.bat
     ```

   - En Linux, el mandato se encuentra bajo el directorio siguiente:

     ```
     /opt/ibm/ldap/V6.3/appsrv/profiles/TDSWebAdminProfile/bin/wsadmin.sh
     ```

     o

     ```
     /opt/ibm/ldap/V6.3/appsrv/bin/wsadmin.sh
     ```

   ```
   wsadmin.bat -conntype NONE -c "$AdminApp uninstall IDSWebApp.war"
   ```

   Por ejemplo:

   ```
   "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\bin\wsadmin.bat"
    -conntype NONE -c "$AdminApp uninstall IDSWebApp.war"
   ```

4. Si se está ejecutando el servidor WebSphere Application Server anterior incorporado, detenga el servidor de aplicaciones.
   - En Windows, el mandato se encuentra bajo el directorio siguiente:

     ```
     C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\bin\
     stopServer.bat
     ```

     o

     ```
     C:\Program Files\IBM\LDAP\V6.3\appsrv\bin\stopServer.bat
     ```

   - En Linux, el mandato se encuentra bajo el directorio siguiente:

     ```
     /opt/ibm/ldap/V6.3/appsrv/profiles/TDSWebAdminProfile/bin/stopServer.sh
     ```

     o

     ```
     /opt/ibm/ldap/V6.3/appsrv/bin/stopServer.sh
     ```

   Por ejemplo:

   ```
   "C:\Program Files\IBM\LDAP\V6.3\appsrv\profiles\TDSWebAdminProfile\bin\
   stopServer.bat" server1
   ```

5. Compruebe si existe el perfil en el nuevo WebSphere Application Server incorporado. Si no existe el perfil, cree un perfil nuevo.
   - En Windows, ejecute el mandato siguiente para crear un nuevo perfil:

     ```
     "C:\Program Files\IBM\LDAP\V6.3.1\appsrv\bin\manageprofiles.bat" -create
      -profileName TDSWebAdminProfile -profilePath "C:\Program Files\IBM\
      LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile" -templatePath
      "C:\Program Files\IBM\LDAP\V6.3.1\appsrv\ profileTemplates\default"
      -nodeName DefaultNode -hostName localhost -cellName
      DefaultNode -isDefault -portsFile "C:\Program Files\IBM\LDAP\V6.3.1\idstools
      \TDSWEBPortDef.props"
     ```

   - En Linux, ejecute el mandato siguiente para crear un nuevo perfil:

     ```
     /opt/ibm/ldap/V6.3.1/appsrv/bin/manageprofiles.sh -create -profileName
      TDSWebAdminProfile -profilePath "/opt/ibm/ldap/V6.3.1/appsrv/profiles/
      TDSWebAdminProfile" -templatePath "/opt/ibm/ldap/V6.3.1/appsrv/
      profileTemplates/default" -nodeName DefaultNode -hostName localhost
      -cellName DefaultNode -isDefault -portsFile "/opt/ibm/ldap/V6.3.1/idstools
      /TDSWEBPortDef.props"
     ```

6. Copie el nuevo archivo war en el nuevo directorio de WebSphere Application Server.

- En Windows, ejecute el mandato siguiente:

```
copy "C:\Program Files\IBM\LDAP\V6.3.1\idstools\IDSWebApp.war"
 "C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\
 installableApps"
```

- En Linux, ejecute el siguiente mandato:

```
cp "/opt/ibm/ldap/V6.3.1/idstools/IDSWebApp.war"
 "/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installableApps"
```

7. Instale el nuevo archivo WAR en el nuevo producto WebSphere Application Server.
   - En Windows, ejecute el mandato siguiente:

```
"C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\bin
 \wsadmin.bat" -conntype NONE -c "$AdminApp install {C:\Program Files\
 IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\installableApps\
 IDSWebApp.war} {-configroot \"C:\Program Files\IBM\LDAP\V6.3.1\
 appsrv\config\" -node DefaultNode -usedefaultbindings -nodeployejb
 -appname IDSWebApp.war -contextroot \"IDSWebApp\"}"
```

   - En Linux, ejecute el siguiente mandato:

```
"/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin/wsadmin.sh"
 -conntype NONE -c "\$AdminApp install {/opt/ibm/ldap/V6.3.1/appsrv/
 profiles/TDSWebAdminProfile/installableApps/IDSWebApp.war}
 {-configroot \"/opt/ibm/ldap/V6.3.1/appsrv/config\"
 -node DefaultNode -usedefaultbindings -nodeployejb -appname IDSWebApp.war
 -contextroot \"IDSWebApp\"}"
```

8. Restaure los archivos de configuración de la herramienta de administración web que ha guardado previamente.
   - En Windows, sustituya los archivos siguientes por los archivos de copia de seguridad:

```
C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\
 installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\
 classes\security\console_passwd
 C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\
 installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\
 classes\IDSConfig\IDSSessionConfig\IDSSessionMgmt.xml
 C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\
 installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\
 classes\IDSConfig\IDSServersConfig\IDSServersInfo.xml
 C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\
 installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\
 classes\IDSConfig\IDSAppReg\IDSAppReg.xml
 C:\Program Files\IBM\LDAP\V6.3.1\appsrv\profiles\TDSWebAdminProfile\
 installedApps\DefaultNode\IDSWebApp.war.ear\IDSWebApp.war\WEB-INF\
 classes\IDSConfig\IDSSearchSettings\IDSSearchMgmt.xml
```

   - En Linux, sustituya los archivos siguientes por los archivos de copia de seguridad:

```
/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installedApps/
 DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/security/
 console_passwd
 /opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installedApps/
 DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/IDSConfig/
 IDSSessionConfig/IDSSessionMgmt.xml
 /opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installedApps/
 DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/IDSConfig/
 IDSServersConfig/IDSServersInfo.xml
 /opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installedApps/
 DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/IDSConfig/
 IDSAppReg/IDSAppReg.xml
 /opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/installedApps/
 DefaultNode/IDSWebApp.war.ear/IDSWebApp.war/WEB-INF/classes/IDSConfig/
 IDSSearchSettings/IDSSearchMgmt.xml
```

9. En Windows, inicie el servicio que se ha añadido.

```
"C:\Program Files\IBM\ldap\V6.3.1\appsrv\bin\WASService.exe"
 -start TDSWebAdmin-V6.3.1
```

10. En Linux, inicie el servidor.

```
/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin/startServer.sh server1
```

Capítulo 16. Despliegue manual de la Herramienta de administración web

Para gestionar y administrar las instancias de servidor de directorios con la Herramienta de administración web, debe desplegar la Herramienta de administración web en un servidor de aplicaciones web soportadas.

Para desplegar la Herramienta de administración web, el sistema debe contener una versión soportada del servidor de aplicaciones web. El soporte de instalación de IBM Security Directory Server proporciona WebSphere Application Server incorporado, versión 7.0.0.25. Puede utilizar IBM Installation Manager para completar la instalación de la Herramienta de administración web, y desplegarlo en WebSphere Application Server incorporado.

Si el sistema operativo no soporta la instalación de IBM Security Directory Server con IBM Installation Manager, complete la instalación de WebSphere Application Server incorporado manualmente. Tras la instalación de WebSphere Application Server incorporado, debe desplegar la Herramienta de administración web en WebSphere Application Server incorporado.

Si el sistema contiene una versión soportada de WebSphere Application Server, puede desplegar la Herramienta de administración web en ella.

WebSphere Application Server es el entorno de ejecución de IBM para las aplicaciones basadas en Java. Para obtener más información, consulte la documentación del producto WebSphere Application Server en http://www-01.ibm.com/support/knowledgecenter/SSEQTP/welcome.

Instalación de WebSphere Application Server incorporado manualmente

Para desplegar la Herramienta de administración web, debe completar la instalación de WebSphere Application Server incorporado en el sistema.

Antes de empezar

Para la instalación de WebSphere Application Server incorporado, siga estos pasos:

1. Acceda al soporte de instalación de IBM Security Directory Server que contiene el WebSphere Application Server incorporado instalable. Consulte el apartado “Preparación del soporte de instalación” en la página 6.

Acerca de esta tarea

Para desplegar la Herramienta de administración web con el mandato `deploy_IDSWebApp` sin utilizar ningún parámetro, debe proporcionar los valores siguientes:

1. Especifique el directorio `appsrv` en la vía de acceso de instalación de IBM Security Directory Server como la ubicación de instalación para WebSphere Application Server incorporado. Para obtener más información sobre la vía de acceso de instalación predeterminada de IBM Security Directory Server, consulte “Ubicaciones de la instalación predeterminada” en la página 27.

Puede proporcionar cualquier otra ubicación de instalación para WebSphere Application Server incorporado. En tal caso, debe especificar los parámetros y valores **-w**, **-p**, **-r**, y **-o** con el mandato `deploy_IDSWebApp` para el despliegue de la Herramienta de administración web.

Procedimiento

1. Inicie sesión con privilegios de administrador.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al directorio que contiene el WebSphere Application Server incorporado instalable.
4. Para instalar WebSphere Application Server incorporado en la vía de acceso de instalación predeterminada de IBM Security Directory Server, ejecute el mandato siguiente:

Sistemas operativos	**Mandato a ejecutar:**
Microsoft Windows	`install.bat -installRoot c:\Program Files\IBM\ldap\V6.3.1\appsrv`
AIX y Solaris	`install.sh -installRoot /opt/IBM/ldap/V6.3.1\appsrv`
Linux	`install.sh -installRoot /opt/ibm/ldap/V6.3.1\appsrv`

Qué hacer a continuación

Si la Herramienta de administración web no está instalado en el sistema, complete la instalación de la Herramienta de administración web. Consulte el apartado Capítulo 12, “Instalación con los programas de utilidad de línea de mandatos del sistema operativo”, en la página 69.

Si la Herramienta de administración web se ha instalado en el sistema, complete el despliegue de la Herramienta de administración web. Consulte el apartado “Despliegue de la Herramienta de administración web en WebSphere Application Server incorporado” en la página 113.

Puertos predeterminados para la Herramienta de administración web

Para evitar conflictos de puertos entre la Herramienta de administración web y otras aplicaciones, debe conocer los puertos predeterminados que utiliza la Herramienta de administración web.

WebSphere Application Server incorporado utiliza los siguientes valores predeterminados de puertos para la Herramienta de administración web:

- Transporte HTTP (puerto 1): 12100
- Transporte HTTPS (puerto 2): 12101
- Puerto de la consola de administrador (para administrar WebSphere Application Server): 12104
- Puerto de la consola de administrador segura (para administrar WebSphere Application Server): 12105

WebSphere Application Server incorporado utiliza los siguientes valores de puerto predeterminados para otras aplicaciones:

- Puerto de Bootstrap/rmi: 12102

- Puerto del conector SOAP: 12103

El resto de los números de puerto que puede utilizar el WebSphere Application Server incluido: 9405, 9406, 9407, 9375, 9105, 7276, 7286, 5558, 5577, 5075, 5076.

Si existe un conflicto de puertos con otra aplicación que puede estar utilizando uno o varios puertos predeterminados, realice una de las acciones siguientes que sea adecuada para el entorno:

- Cambie los puertos predeterminados a puertos inactivos, e inicie la aplicación con el puerto inactivo.
- Si la aplicación que está utilizando los puertos predeterminados no es un servidor o un servicio importante, modifique su número de puerto y libere el puerto predeterminado.

Para cambiar los números de puerto predeterminados que WebSphere Application Server incorporado inicializa para la aplicación, debe establecer el número de puerto adecuado en el archivo `portdef.props`. El archivo `portdef.props` se encuentra en el directorio `\appsrv\profiles\TDSWebAdminProfile\properties\` de la ubicación de la instalación de IBM Security Directory Server. Para obtener más información sobre la ubicación de instalación predeterminada de IBM Security Directory Server, consulte "Ubicaciones de la instalación predeterminada" en la página 27.

Puerto 1 de transporte HTTP
Para modificar el puerto para Puerto 1 de transporte HTTP, cambie la entrada con el número de puerto 12100 al número de puerto que no está en uso.

Puerto 2 de transporte HTTPS
Para modificar el puerto para Puerto 2 de transporte HTTPS, cambie la entrada con el número de puerto 12101 al número de puerto que no está en uso.

Puerto de Bootstrap/rmi
Para modificar el puerto para el puerto de Bootstrap/rmi, cambie la entrada con el número de puerto 12102 al número de puerto que no está en uso.

Puerto del conector SOAP
Para modificar el puerto para el Puerto del conector SOAP, cambie la entrada con el número de puerto 12103 al número de puerto que no está en uso.

Puerto de la consola de administrador
Para modificar el puerto para el Puerto de la consola de administrador, cambie la entrada con el número de puerto 12104 al número de puerto que no está en uso.

Puerto de la consola de administración segura
Para modificar el puerto para el puerto de la Consola de administración segura, cambie la entrada con el número de puerto 12105 al número de puerto que no está en uso.

Despliegue de la Herramienta de administración web en WebSphere Application Server incorporado

Para utilizar la Herramienta de administración web, debe desplegarla en un servidor de aplicaciones web.

Antes de empezar

Debe realizar las acciones siguientes antes de desplegar la Herramienta de administración web:

1. Complete la instalación del paquete de la Herramienta de administración web para el sistema operativo.
2. Complete la instalación de una versión soportada del servidor de aplicaciones web.
3. Si tiene previsto migrar una configuración existente de la Herramienta de administración web de una versión anterior, no debe desplegar una versión posterior de la Herramienta de administración web.

Acerca de esta tarea

Al desplegar la Herramienta de administración web, el mandato realiza las acciones siguientes:

1. Elimina una versión anterior de la Herramienta de administración web, si la hay.
2. Despliega la Herramienta de administración web en un servidor de aplicaciones web.
3. Inicia el servidor de aplicaciones web.

Procedimiento

1. Inicie sesión con los privilegios de administrador.
2. Vaya al directorio *ubicación_instalación_DS*/idstools. La *ubicación_instalación_DS* es la ubicación de instalación de IBM Security Directory Server. Las ubicaciones siguientes son las predeterminadas para varios sistemas operativos:

Sistemas operativos	**Ubicaciones de instalación predeterminadas:**
Microsoft Windows	c:\Program Files\IBM\ldap\V6.3.1
AIX y Solaris	/opt/IBM/ldap/V6.3.1
Linux	/opt/ibm/ldap/V6.3.1

3. Ejecute el siguiente mandato:

   Nota: Si ha instalado WebSphere Application Server incorporado en la ubicación de instalación predeterminada de IBM Security Directory Server, no proporcione ningún parámetro en el mandato deploy_IDSWebApp. Para obtener más información sobre el mandato deploy_IDSWebApp, consulte el uso del mandato, deploy_IDSWebApp -h.

Sistemas operativos	**Mandato a ejecutar:**
Microsoft Windows	deploy_IDSWebApp.bat -w *vía_acceso_a_archivo_war* -p *vía_acceso_instalación_was* -r *perfil* -o archivo_puertos
AIX, Linux, y Solaris	deploy_IDSWebApp -w *vía_acceso_a_archivo_war* -p *vía_acceso_instalación_was* -r *perfil* -o archivo_puertos

Resultados

El mandato despliega la Herramienta de administración web en el servidor de aplicaciones web especificado por *vía_acceso_instalación_was*.

Qué hacer a continuación

Para acceder a la Herramienta de administración web, abra una ventana del navegador y especifique `http://nombre_host:12100/IDSWebApp`. La variable *nombre_host* indica el nombre de host o la dirección IP del sistema donde ha instalado la Herramienta de administración web.

Despliegue de la Herramienta de administración web en WebSphere Application Server

Si desea gestionar aplicaciones en el sistema con WebSphere Application Server, puede desplegar la Herramienta de administración web en WebSphere Application Server.

Antes de empezar

Para desplegar la Herramienta de administración web en WebSphere Application Server, debe cumplir los requisitos siguientes:

1. Complete la instalación del paquete de la Herramienta de administración web para el sistema operativo. Consulte el apartado "Instalación con IBM Installation Manager" en la página 31.
2. El sistema debe contener una versión soportada de WebSphere Application Server.

Acerca de esta tarea

El soporte de instalación de IBM Security Directory Server proporciona la Herramienta de administración web y WebSphere Application Server incorporado. Si el sistema contiene WebSphere Application Server, puede desplegar la Herramienta de administración web en WebSphere Application Server. Para desplegar la Herramienta de administración web, debe desplegar el archivo `IDSWebApp.war` que se encuentra en el directorio `idstools` de la ubicación de instalación de IBM Security Directory Server.

Procedimiento

1. Utilice el URL `http://servidor_WAS_nombre_host:9060/ibm/console` para iniciar sesión en la consola de administración de WebSphere. Sustituya la variable *servidor_WAS_nombre_host* por el nombre de host o la dirección IP del sistema en el que está instalado WebSphere Application Server. Si se ha especificado un puerto personalizado para acceder a la consola de administración de WebSphere, sustituya el puerto predeterminado, `9060`, por el número de puerto.
2. Especifique el ID de usuario y la contraseña del usuario. El usuario debe contener el permiso necesario para ejecutar operaciones en WebSphere Application Server.
3. En el panel de navegación izquierdo, pulse **Aplicación** > **Nueva aplicación**.
4. En la página **Nueva aplicación**, pulse **Nueva aplicación empresarial**.

5. En la página **Vía de acceso a la nueva aplicación**, seleccione una de las siguientes opciones que se basan en desde donde se ha accedido a la consola de administración de WebSphere:
   - Si ha accedido a la consola de administración de WebSphere desde un sistema local, seleccione **Sistema de archivos local**, y especifique la vía de acceso del archivo `IDSWebApp.war` en el campo **Vía de acceso completa**. También puede pulsar **Examinar** para especificar la vía de acceso.
   - Si ha accedido a la consola de administración de WebSphere desde un sistema remoto, seleccione **Sistema de archivos remoto**, y especifique la vía de acceso del archivo `IDSWebApp.war` en el campo **Vía de acceso completa**. También puede pulsar **Examinar** para especificar la vía de acceso.
6. En la página **Cómo desea instalar la aplicación**, seleccione la opción **Vía de acceso rápida** y pulse **Siguiente**.
7. En la página **Seleccionar opciones de instalación**, se seleccionarán las opciones predeterminadas.
8. Pulse **Siguiente**.
9. En la página **Correlacionar módulos al servidor**, puede correlacionar módulos a los servidores especificados en el campo **Clústeres y servidores**.
   a. Marque el recuadro de selección para el módulo necesario, y pulse **Aplicar**.
   b. Tras completar la correlación, pulse **Siguiente**.
10. En la página **Correlacionar hosts virtuales para módulos web**, puede correlacionar la aplicación web en servidores virtuales específicos. Si hay más hosts virtuales, el servidor requiere información sobre el entorno de WebSphere para seleccionar el módulo derecho. En este ejemplo, la opción `host_predeterminado` está disponible para su selección.
11. Pulse **Siguiente**.
12. En la página **Correlacionar raíces de contexto para los módulos web**, especifique la raíz de contexto como `/IDSWebApp` en el campo.
13. Aparecerá un resumen con la selección.
14. Pulse **Finalizar**. Se iniciará la instalación de la aplicación. Aparecerá un resumen de la instalación.
15. Para guardar los cambios en la configuración maestra, pulse **Guardar**.
16. En el panel de navegación de la izquierda, pulse **Aplicaciones** > **Tipos de aplicaciones** > **Aplicaciones empresariales de WebSphere**.
17. En la página **Aplicaciones empresariales**, marque el recuadro de selección junto a `IDSWebApp_war`, y pulse **Inicio**.
18. Inicie la Herramienta de administración web.
19. Para acceder a la Herramienta de administración web, abra un navegador y especifique la siguiente dirección:
    - Para el acceso no seguro (HTTP), especifique `http://WAS_server_hostname:9080/IDSWebApp`.
    - Para el acceso seguro (HTTPS), especifique `https://WAS_server_hostname:9443/IDSWebApp`

    El puerto, 9080, es el puerto HTTP predeterminado para WebSphere Application Server, y el puerto, 9443, es el puerto HTTPS predeterminado. Si estos puertos no son los puertos configurados para WebSphere Application Server, proporcione el número de puerto adecuado. Si la seguridad Global o Administrativa está configurada para WebSphere Application Server, debe cumplir los requisitos siguientes:

a. Despliegue la Herramienta de administración web en WebSphere Application Server como un nuevo perfil.
b. Configure SSL para la Herramienta de administración web.
c. Si no se puede desplegar la Herramienta de administración web en un perfil, añada el certificado de servidor de directorios al almacén de confianza del perfil. Para la autenticación de servidor-cliente, añada el certificado del perfil de WebSphere Application Server al almacén de confianza del servidor de directorios.

Inicio de WebSphere Application Server incorporado para utilizar la Herramienta de administración web

Inicie el servidor de aplicaciones web asociado con la Herramienta de administración web para añadir, gestionar y administrar instancias de servidor de directorios.

Antes de empezar

Debe realizar las siguientes tareas para iniciar el servidor de aplicaciones web asociado con la Herramienta de administración web:

1. Completar la instalación de la Herramienta de administración web.
2. Desplegar la Herramienta de administración web en un servidor de aplicaciones web soportado.

Nota: Si utiliza IBM Installation Manager para la instalación y el despliegue de la Herramienta de administración web en WebSphere Application Server incorporado, el servidor de aplicaciones se iniciará tras completar el despliegue de la Herramienta de administración web.

Procedimiento

1. Para iniciar el servidor de aplicaciones asociado con la Herramienta de administración web, ejecute el mandato siguiente en diversos sistemas operativos:

   Windows

   Si no se ha iniciado el servidor de aplicaciones, ejecute el mandato siguiente:

   ```
   vía_acceso_instalación\idstools\bin\startWebadminApp.bat
   ```

   La vía de acceso de instalación predeterminada es `C:\Program Files\IBM\ldap\V6.3.1`.

   AIX y Solaris

   ```
   /opt/IBM/ldap/V6.3.1/idstools/bin/startWebadminApp
   ```

   Linux

   ```
   /opt/ibm/ldap/V6.3.1/idstools/bin/startWebadminApp
   ```

2. Abra un navegador web.
3. Especifique el siguiente URL en la barra de direcciones del navegador web:

   Nota: Si ha instalado y desplegado la Herramienta de administración web en un sistema remoto, sustituya el nombre de host o la dirección IP del sistema en lugar de `localhost`.

   ```
   http://localhost:12100/IDSWebApp
   ```

Qué hacer a continuación

Para gestionar y administrar las instancias de servidor de directorios, añada servidores en la consola de la Herramienta de administración web. Consulte el apartado "Acceso a la Herramienta de administración web".

Acceso a la Herramienta de administración web

Para gestionar las instancias del servidor de directorios de forma remota, abra la Herramienta de administración web y configure la instancia de servidor de directorios para la gestión remota.

Antes de empezar

Debe completar las tareas siguientes para acceder a la Herramienta de administración web:

1. Completar la instalación de la Herramienta de administración web.
2. Desplegar la Herramienta de administración web en un servidor de aplicaciones web soportado.
3. Iniciar el servidor de aplicaciones web que está asociado con la Herramienta de administración web.

Procedimiento

1. Para acceder a la Herramienta de administración web, utilice una de las siguientes opciones:
   - Abra un navegador web y escriba la siguiente URL:
     - Para el acceso no seguro, especifique `http://nombrehost:12100/IDSWebApp`.
     - Para el acceso seguro, especifique `https://nombrehost:12101/IDSWebApp`.
   - Abra el archivo siguiente en un navegador web:

     Windows

     Para el acceso no seguro, abra *vía_acceso_instalación_ds*`\idstools\bin\idswebadmin.html`. También puede pulsar **Inicio** > **Todos los programas** > **IBM Security Directory Server 6.3.1** > **Herramienta de administración web**.

     Para el acceso seguro, abra *vía_acceso_instalación_ds*`\idstools\bin\idswebadminssl.html`. También puede pulsar **Inicio** > **Todos los programas** > **IBM Security Directory Server 6.3.1** > **Herramienta de administración web (seguro)**.

     AIX, Linux, y Solaris

     Para el acceso no seguro, abra *vía_acceso_instalación_ds*`/idstools/bin/idswebadmin.html`.

     Para el acceso seguro, especifique *vía_acceso_instalación_ds*`/idstools/bin/idswebadminssl.html`.

     La variable *vía_acceso_instalación_ds* representa la ubicación de instalación de IBM Security Directory Server. Para obtener más información sobre la ubicación predeterminada, consulte "Ubicaciones de la instalación predeterminada" en la página 27.
2. Inicie sesión en la consola de la Herramienta de administración web como el administrador de la consola.
   a. En el campo **ID de usuario**, especifique `superadmin`.

b. En el campo **Contraseña**, especifique **secret**.

   Nota: Debe cambiar la contraseña del administrador de la consola después de iniciar la sesión por primera vez.

c. Pulse **Iniciar sesión**.

3. Para añadir un servidor de directorios a la consola, siga estos pasos:
   a. En la página **Introducción**, pulse **Gestionar servidores de la consola**.
   b. En la página **Gestionar servidores de la consola**, pulse **Añadir**.
   c. En el campo **Nombre de servidor**, especifique un nombre exclusivo para identificar el servidor. Si no proporciona un valor, la aplicación asignará un valor `nombrehost:puerto` o un valor `dirección_IP:puerto`.
   d. En el campo **Nombrehost**, el nombre de host o la dirección IP del servidor de directorios.
   e. En el campo **Puerto**, especifique el número de puerto del servidor.
   f. Para especificar si la consola debe comunicarse con el servidor de forma segura, seleccione **Habilitar cifrado SSL**.
   g. Para habilitar el control del puerto de Administración, seleccione **Servidor de administración soportado**.
   h. En el campo **Puerto de administración**, especifique el número de puerto del servidor de administración.
   i. Para aplicar los cambios, pulse **Aceptar**.
4. Para cerrar sesión de la consola de la Herramienta de administración web, pulse **Cerrar sesión**.

Detención del servidor de aplicaciones web

Antes de la desinstalación de la Herramienta de administración web, debe cerrar sesión de la Herramienta de administración web y detener el servidor de aplicaciones web asociado a ella.

Antes de empezar

Debe completar las siguientes tareas para detener el servidor de aplicaciones web asociado con la Herramienta de administración web:

1. Desplegar la Herramienta de administración web en un servidor de aplicaciones web soportado.
2. Iniciar el servidor de aplicaciones web que está asociado con la Herramienta de administración web.

Procedimiento

1. Inicie sesión de root en sistemas UNIX, y como un miembro de un grupo de administradores en Windows.
2. Acceda al indicador de mandatos.
3. Vaya al subdirectorio `bin` en el perfil Herramienta de administración web. La ubicación siguiente es la vía de acceso de instalación predeterminada de WebSphere Application Server incorporado donde se ha desplegado la Herramienta de administración web. Si ha especificado una vía de acceso de instalación personalizada para WebSphere Application Server incorporado, debe realizar los cambios adecuados.

Sistema operativo	Vía de acceso
Windows	`C:\Program Files\IBM\ldap\V6.3.1\appsrv\profiles\TDSWebAdminProfile\bin`
AIX y Solaris	`/opt/IBM/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin`
Linux	`/opt/ibm/ldap/V6.3.1/appsrv/profiles/TDSWebAdminProfile/bin`

4. Para detener el servidor de aplicaciones web asociado con la Herramienta de administración web, ejecute el mandato siguiente:

Sistema operativo	Mandato a ejecutar:
Windows	`stopServer.bat servidor1`
AIX, Linux, y Solaris	`./stopServer servidor1`

Nota: En Windows, también puede detener el servicio asociado con el servidor de aplicaciones web desde la ventana **Servicios**.

HTTPS con WebSphere Application Server incorporado

Para garantizar el acceso web a la aplicación, puede configurar e iniciar la aplicación en la modalidad HTTPS.

Tras desplegar la Herramienta de administración web en WebSphere Application Server incorporado, podrá iniciar la aplicación. Puede conectarse a la Herramienta de administración web de forma segura proporcionando la dirección web HTTPS y el puerto seguro.

Para utilizar HTTPS, proporcione la siguiente dirección web para acceder a la Herramienta de administración web:

`https://`*`hostname`*`:12101/IDSWebApp`

Para utilizar una conexión no HTTPS, proporcione la siguiente dirección web para acceder a la Herramienta de administración web:

`http://`*`hostname`*`:12100/IDSWebApp`

También puede cambiar los archivos JKS predeterminados con certificados que se proporcionan con el servidor de aplicaciones web para la comunicación segura SSL/TLS. Puede crear nuevos archivos de bases de datos de claves y de almacén de confianza para utilizar con la aplicación desplegada en WebSphere Application Server incorporado. Los archivos predeterminados de bases de datos de claves y de almacén de confianza están separados y se encuentran en el directorio *WAS_HOME*`/profiles/TDSWebAdminProfile/etc/`. La variable *WAS_HOME* es la ubicación de instalación de WebSphere Application Server incorporado. El archivo de base de datos clave predeterminado es `DummyServerKeyFile.jks`, y el archivo de base de datos de almacén de confianza predeterminado es `DummyServerTrustFile.jks`.

Si ha creado los archivos JKS, puede cambiar los archivos de base de datos clave y de almacén de confianza. Para configurar los archivos JKS, contraseñas y formatos

de archivos, añada o modifique las siguientes entradas (resaltadas en **negrita**) en el archivo *WAS_HOME*/profiles/TDSWebAdminProfile/config/cells/DefaultNode/security.xml:

```
<keyStores xmi:id="KeyStore_DefaultNode_10"
 name="DummyServerKeyFile"
 password="{xor}CDo9Hgw="
 provider="IBMJCE"
 location="${WAS_HOME}/profiles/TDSWebAdminProfile/etc/DummyServerKeyFile.jks"
 type="JKS"
 fileBased="true"
 hostList=""
 managementScope="ManagementScope_DefaultNode_1"/>
<keyStores xmi:id="KeyStore_DefaultNode_11"
 name="DummyServerTrustFile"
 password="{xor}CDo9Hgw="
 provider="IBMJCE"
 location="${WAS_HOME}/profiles/TDSWebAdminProfile/etc/DummyServerTrustFile.jks"
 type="JKS"
 fileBased="true"
 hostList=""
 managementScope="ManagementScope_DefaultNode_1"/>
```

Desinstalación de la Herramienta de administración web de WebSphere Application Server incorporado

Para sustituir una Herramienta de administración web existente (archivo IDSWebApp.war) por una versión posterior, debe desinstalar la Herramienta de administración web existente.

Procedimiento

1. Inicie el servidor de aplicaciones web asociado con la Herramienta de administración web, si se encuentra en un estado detenido. Consulte el apartado "Inicio de WebSphere Application Server incorporado para utilizar la Herramienta de administración web" en la página 117.
2. Vaya al directorio *ubicación_instalación_DS*/idstools. La *ubicación_instalación_DS* es la ubicación de instalación de IBM Security Directory Server. Las ubicaciones siguientes son las predeterminadas para varios sistemas operativos:

Sistemas operativos	**Ubicaciones de instalación predeterminadas:**
Microsoft Windows	c:\Program Files\IBM\ldap\V6.3.1
AIX y Solaris	/opt/IBM/ldap/V6.3.1
Linux	/opt/ibm/ldap/V6.3.1

3. Ejecute el siguiente mandato:

   Nota: Si ha instalado WebSphere Application Server incorporado en una ubicación personalizada, también debe proporcionar los parámetros **-a**, **-w**, **-p**, y **-r** al mandato deploy_IDSWebApp. Para obtener más información sobre el mandato deploy_IDSWebApp, consulte el uso del mandato, deploy_IDSWebApp -h.

Sistemas operativos	**Mandato a ejecutar:**
Microsoft Windows	deploy_IDSWebApp.bat -u
AIX, Linux, y Solaris	deploy_IDSWebApp -u

Capítulo 17. Planificación para una configuración de instancias

Debe decidir los valores de configuración para el sistema antes de crear y configurar el entorno de LDAP.

Para crear una instancia de servidor de directorios o una instancia de servidor proxy, debe crear en primer lugar un ID de usuario de sistema que sea el propietario de la instancia. Para almacenar datos de directorios en una instancia de servidor de directorios, debe decidir la página de códigos que desea utilizar.

La instalación de IBM Security Directory Server y de productos de software necesario y la creación de una instancia de servidor de directorios requiere que cree el usuario y el grupo en el sistema. La instalación de productos de software necesario de IBM Security Directory Server, como por ejemplo IBM DB2, requiere la creación del ID de usuario de sistema para el administrador de DB2.

Usuarios y grupos que están asociados con una instancia de servidor de directorios

Para crear una instancia de servidor de directorios o una instancia de servidor proxy, debe crear usuarios y grupos con los permisos necesarios.

Si desea crear una instancia en el sistema, debe asociar la instancia con un ID de usuario de sistema. Este ID de usuario es el propietario de la instancia de servidor de directorios. Si no existe un ID de usuario de sistema para una instancia, debe crear un ID de usuario en el sistema. Para crear un ID de usuario para el propietario de la instancia de servidor de directorios, el propietario de la instancia de base de datos, y el propietario de base de datos, debe seguir las reglas de denominación. Para obtener más información sobre las reglas de denominación, consulte “Reglas de denominación” en la página 124.

Para obtener un servidor de directorios completo, también debe asociar ID de usuario de sistema como propietarios de la base de datos y de la instancia de base de datos. Puede utilizar el mismo ID de usuario para los tres roles. Si utiliza el mismo ID de usuario, la instancia de servidor de directorios, la instancia de base de datos y el propietario de la base de datos contendrán el mismo nombre de propietario.

Si utiliza Herramienta de administración de instancias para crear una instancia de servidor de directorios, puede crear el ID de usuario del propietario de instancias de servidor de directorios con la herramienta. También puede utilizar el mandato **idsadduser** para crear el ID de usuario del propietario de instancias de servidor de directorios. El mandato creará un ID de usuario que cumpla todos los requisitos.

El ID de usuario que asocie con el propietario de instancias de servidor de directorios, el propietario de instancias de base de datos, y el propietario de bases de datos contiene los roles siguientes:

Propietario de la instancia de servidor de directorios
Debe existir un ID de usuario de sistema en el sistema que sirve como propietario de la instancia de servidor de directorios. El ID de usuario para el propietario de la instancia de servidor de directorios también es el

nombre de la instancia de servidor de directorios. A este usuario se le ha asignado la autoridad para gestionar la instancia de servidor de directorios.

En Windows, un miembro del grupo Administradores también tendrá la autoridad de gestionar la instancia de servidor de directorios. En AIX, Linux, y Solaris, el grupo primario del propietario de instancias de servidor de directorios también contiene la autoridad para gestionar la instancia de servidor de directorios.

Nota: En AIX, Linux, y Solaris, los nombres del propietario de instancias distinguen entre mayúsculas y minúsculas. También debe especificar el nombre de la instancia de servidor de directorios y el propietario exactamente como se ha especificado el ID de usuario. El ejemplo siguiente muestra dos nombres de propietarios distintos, `JoeSmith` y `joesmith`.

Propietario de la instancia de base de datos
El ID de usuario que sirve como propietario de instancias de base de datos es propietario de la instancia de base de datos configurada para una instancia de servidor de directorios. El nombre de la instancia de base de datos y el nombre del propietario de la instancia de base de datos son el mismo. Este usuario gestiona la instancia de base de datos. Además, el propietario de la instancia de servidor de directorios puede gestionar la instancia de base de datos. De forma predeterminada, este ID de usuario es el mismo que el ID de usuario que es propiedad de la instancia de servidor de directorios.

Propietario de la base de datos
Este ID de usuario es propietario de la base de datos utilizada por la instancia de servidor de directorios para almacenar los datos de directorio. La base de datos está almacenada en la instancia de base de datos propiedad del propietario de la instancia de base de datos. La instancia de servidor de directorios utiliza el ID de usuario del propietario de la base de datos y la contraseña para conectarse a la base de datos.

Reglas de denominación

El ID de usuario y el grupo primario para una instancia de servidor de directorios debe cumplir las directrices de la regla de denominación.

El requisito de reglas de denominación se aplicará a los siguientes ID de usuario:

- El nombre de la instancia de servidor de directorios (el ID de usuario que posee la instancia de servidor de directorios).
- El nombre de la instancia de base de datos (el ID de usuario que posee la instancia de base de datos). Este ID de usuario es normalmente el mismo que el nombre de la instancia de servidor de directorios.
- En AIX, Linux, y Solaris, los grupos primarios del ID de usuario del propietario de la instancia de servidor de directorios y el ID de usuario del propietario de la instancia de base de datos.

Nota: Al crear el ID de usuario y el grupo, debe asignar los permisos adecuados. Consulte el apartado “Requisitos de creación de usuarios y grupos” en la página 125.

Los ID de grupo y de usuario deben cumplir los requisitos siguientes:

- No puede tener más de 8 caracteres.
- No pueden tener ninguno de los nombres siguientes:

  - USERS
  - ADMINS
  - GUESTS
  - PUBLIC
  - LOCAL
  - idsldap
- No pueden comenzar con ninguno de los siguientes prefijos:
  - IBM
  - SQL
  - SYS
- No puede contener caracteres acentuados
- Puede contener los caracteres siguientes:
  - De la A a la Z
  - De la a a la z
  - Del 0 al 9
  - _ (Carácter de subrayado)
- Deben empezar por uno de los siguientes caracteres:
  - De la A a la Z
  - De la a a la z

Requisitos de creación de usuarios y grupos

Al crear usuarios y grupos para la instancia, debe asignar usuarios y grupos con permisos adecuados y añadirlos como miembro de los grupos adecuados.

Una vez que cree los usuarios y grupos necesarios para la instancia, debe asignar permisos adecuados y añadir los usuarios en los grupos correctos. Debe cumplir los requisitos siguientes para los ID de usuario y grupo:

Windows

- Añada el propietario de la instancia de servidor de directorios y el propietario de la instancia de base de datos como miembros del grupo Administradores.
- Establezca un entorno local válido para el propietario de la instancia de base de datos en un idioma en el que desee que genere idiomas el servidor. Si es necesario, inicie sesión como el usuario y cambie el entorno local con el valor adecuado.

AIX, Linux, y Solaris

- Añada el ID raíz como miembro del grupo primario del propietario de la instancia de servidor de directorios y del propietario de la instancia de base de datos.
- Añada el ID raíz como miembro del grupo `idsldap`.
- Añada el propietario de la instancia de servidor de directorios y el propietario de la instancia de base de datos como miembros del grupo `idsldap`.
- Cree directorios de inicio para el propietario de la instancia de servidor de directorios y el propietario de la instancia de base de datos.
- Asigne permisos adecuados para el directorio de inicio del propietario de la instancia de servidor de directorios.

  - La propiedad de usuario para la instancia en el propietario de la instancia de servidor de directorios.
  - La propiedad del grupo para la instancia es el grupo primario del propietario de la instancia de servidor de directorios.
  - Debe asignar permisos de lectura, grabación y ejecución al directorio de inicio para el propietario de la instancia de servidor de directorios y su grupo primario.
- Asigne el acceso de lectura, grabación y ejecución en la ubicación donde se crea la base de datos para el propietario de la instancia de servidor de directorios y su grupo primario.
- El propietario de la instancia de servidor de directorios y el propietario de la instancia de base de datos para una instancia de servidor de directorios pueden ser usuarios distintos. En tal caso, el propietario de la instancia de servidor de directorios debe ser un miembro del grupo primario del propietario de la instancia de base de datos.
- Si el propietario de la instancia de servidor de directorios, el propietario de la instancia de DB2, y el propietario de la base de datos son distintos, deben ser miembros del mismo grupo.
- Establezca el script de shell Korn (`/usr/bin/ksh`) como el shell de inicio de sesión del propietario de la instancia de servidor de directorios, el propietario de la instancia de base de datos, y el propietario de la base de datos.

Debe establecer la contraseña del propietario de la instancia de servidor de directorios, el propietario de la instancia de base de datos, y el propietario de la base de datos correctamente y deben estar listos para utilizarse. La contraseña no debe haber caducado ni debe estar a la espera de una primera validación de ningún tipo. Puede verificar si la contraseña está establecida de forma correcta accediendo a telnet en el sistema e inicie sesión con el ID de usuario y la contraseña.

Al configurar la base de datos no es necesario, aunque sí habitual, especificar el directorio de inicio del propietario de la instancia de base de datos como ubicación de la base de datos. Si especifica alguna otra ubicación, el directorio de inicio del propietario de la instancia de base de datos debe contener 3 - 4 MB de espacio disponible. DB2 crea enlaces y añade archivos en el directorio de inicio del propietario de la instancia de base de datos aunque la propia base de datos esté en otra ubicación. Si el sistema no contiene el espacio necesario en el directorio de inicio del propietario de la instancia de base de datos, puede añadir espacio o cambiar el directorio de inicio.

Ejemplos

Para crear un propietario de la instancia que cumpla los requisitos para un propietario de la instancia de servidor de directorios, puede ejecutar el mandato **idsadduser**. El mandato **idsadduser** se encuentra en el subdirectorio `sbin` de la ubicación de instalación de IBM Security Directory Server.

Ejemplo 1:

Para crear una cuenta de usuario en AIX, Linux, o Solaris, con los valores siguientes, ejecute el mandato **idsadduser**:

- Nombre de usuario: `JoeSmith`
- Grupo primario: `empleados`
- Directorio de inicio: `/home/joe` (En Solaris, utilice `/export/home/joe`)

- Contraseña: joespw

```
idsadduser –u JoeSmith –g employees –l /home/joe –w joespw
```

Ejemplo 2:

Para crear una cuenta de usuario como miembro del grupo de Administradores de Windows con los valores siguientes, ejecute el mandato **idsadduser**:

- Nombre de usuario: JoeSmith
- Contraseña: joespw

```
idsadduser –u JoeSmith –w joespw
```

Planificación de la configuración

Para el entorno de servidor de directorios, debe decidir el tipo de datos que tiene previsto almacenar, la estructura de datos, y la seguridad de datos a establecer.

Debe tomar las decisiones siguientes antes de configurar y rellenar la base de datos:

El tipo de datos que desea almacenar en el servidor de directorios

Debe decidir los esquemas que desea utilizar para el servidor de directorios y el tipo de datos que desea almacenar en el servidor de directorios. Se incluye un conjunto estándar de definiciones de atributo-tipo y de clase de objeto en el servidor de directorios. Para personalizar los datos, es posible que desee añadir las definiciones de tipo de atributo personalizado y de clase de objeto antes de añadir entradas al servidor de directorios.

Puede realizar la adición o la modificación en los esquemas una vez que el directorio se rellene con datos. En algunas situaciones, es posible que los cambios de los esquemas le pidan que descargue y que vuelva a cargar los datos.

La página de códigos que desea utilizar

Decida si desea crear la base de datos utilizando la página de códigos local o utilizando el juego de caracteres universal (UTF-8). Si selecciona una página de códigos local, permite a las aplicaciones y a los usuarios de IBM Security Directory Server recuperar resultados de búsqueda tal como se espera para la secuencia de cotejo del idioma. Sin embargo, si utiliza una página de códigos local, los datos de dicha página de códigos específica se almacenará en el directorio. Si utiliza UTF-8, puede almacenar cualquier dato de caracteres UTF-8 en el directorio. Para obtener más información sobre UTF-8, consulte el “Soporte de UTF-8” en la página 128.

Nota: Si desea utilizar códigos de idioma, debe utilizar UTF-8 como la página de códigos de la base de datos.

Defina una estructura de jerarquía para almacenar los datos del directorio

IBM Security Directory Server almacena datos de directorio en una estructura de árbol jerárquica. Los nombres de las entradas del directorio se basan en la posición relativa de las entradas de la estructura de árbol. Es importante definir una organización lógica en el directorio que sea apropiado para el entorno de LDAP. Una organización lógica facilita que los clientes determinen la rama del árbol que tienen que buscar para localizar la información necesaria.

Defina los requisitos de seguridad de los datos

Para impedir el acceso a los datos del directorio a través de un puerto no

seguro, puede configurar el servidor de directorios para una comunicación segura. Para obtener más información acerca de cómo proteger sus datos, consulte la sección Administración en la documentación de IBM Security Directory Server.

Defina los permisos de acceso necesarios para los datos de directorio
Para obtener más información sobre cómo utilizar los permisos de acceso, consulte las listas de control de acceso en la sección Administración de la documentación de IBM Security Directory Server.

Acceda si necesita un servidor proxy
Si hay muchos datos de directorio y el entorno es de grabación intensiva, considere la posibilidad de utilizar un servidor proxy. Los grandes entornos de directorio que requieren mucha lectura pueden conseguir una escala adecuada configurando la réplica. Consulte la lista de funciones admitidas en un servidor proxy en la sección Administración de la documentación de IBM Security Directory Server, antes de decidir si utiliza un servidor proxy.

Soporte de UTF-8

Puede configurar un servidor de directorios para almacenar cualquier carácter de idioma nacional que se pueda representar en UTF-8.

IBM Security Directory Server da soporte a una amplia variedad de caracteres de idioma nacional mediante el juego de caracteres UTF-8 (UCS Transformation Format). En el protocolo LDAP Versión 3, todos los datos de caracteres con los que se comunica un cliente y un servidor de LDAP están en UTF-8.

El servidor determina los tipos de caracteres que se pueden almacenar y que se pueden buscar en función de la página de códigos que se utiliza para configurar una base de datos. Puede especificar el juego de caracteres de la base de datos como UTF-8 o utilizar el juego de caracteres local del sistema en el que existe el servidor. El juego de caracteres local se basa en el entorno local, idioma y entorno de la página del código del sistema.

Si especifica UTF-8, puede almacenar cualquier dato de caracteres UTF-8 en el directorio. Los clientes de LDAP de un sistema que dan soporte a cualquier idioma soportado por UTF-8 pueden acceder y buscar el directorio correctamente. Si los clientes de LDAP se encuentran en un sistema con un conjunto de caracteres local, es posible que el cliente no muestre correctamente los resultados que se han recuperado del servidor en un juego de caracteres concreto.

Si utiliza una base de datos de UTF-8, el rendimiento de la base de datos mejorará debido a que no es necesaria una conversión de datos al almacenar o recuperar datos de la base de datos.

Nota: Si desea utilizar códigos de idioma, la base de datos debe ser UTF-8.

Uso de UTF-8 en un servidor de directorios

Para decidir qué página de códigos utilizar, debe comprender la forma en que un servidor de directorios utiliza la página de códigos para almacenar y acceder a los datos de directorios.

Una base de datos de UTF-8 tiene una secuencia de cotejo fija y dicha secuencia es el orden binario de los caracteres UTF-8. No es posible realizar un cotejo sensible al idioma con una base de datos UTF-8.

Para que las aplicaciones o los usuarios de LDAP obtengan los resultados siguientes, UTF-8 puede que no sea el juego de caracteres adecuado para la base de datos:

- Una búsqueda con un filtro de solicitud, como por ejemplo `"name >= SMITH"`, y si espera el orden similar en el entorno local.
- Una búsqueda con el control para clasificar los resultados, y si espera el orden similar en el entorno local.

En tales situaciones, el sistema del servidor LDAP y todos los sistemas clientes deben ejecutarse con el mismo juego de caracteres y entorno local.

Por ejemplo, una base de datos de servidor LDAP que esté configurada con el entorno local Español devuelve resultados de búsqueda en función del orden del carácter, como esperan los clientes del idioma español. Dicha configuración limita a la comunidad de usuarios del directorio a un único juego de caracteres en dicho entorno local y secuencia de cotejo.

Creación de un archivo LDIF con valores UTF-8 utilizando programas de utilidad de servidor

Puede utilizar una extensión `charset` para crear un formato LDIF con valores UTF-8.

La creación manual de un archivo LDIF que contenga valores UTF-8 es difícil. En la cabecera del archivo LDIF, puede especificar la extensión que da soporte a un nombre de juego de caracteres IANA (Internet Assigned Numbers Authority) junto con el número de versión. Para obtener más información sobre los juegos de caracteres IANA soportados, consulte “Juegos de caracteres IANA soportados” en la página 130.

Ejemplos

Ejemplo 1:

Para que los programas de utilidad de servidor se conviertan automáticamente desde el juego de caracteres especificado a UTF-8, puede utilizar la etiqueta `charset`.

```
versión: 1
juego de caracteres: ISO-8859-1

dn: cn=Juan Griego, ou=University of New Mexico, o=sample
cn: Juan Griego
sn: Griego
description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvd
title: Associate Dean
title: [title in Spanish]
jpegPhoto:< file:///usr/local/photos/jgriego.jpg
```

En el ejemplo siguiente, todos los nombres de atributos con valores separados por dos puntos únicos se convierten desde el juego de caracteres `ISO-8859-1` a UTF-8. Todos los nombres de atributos con valores separados por dos puntos dobles, como por ejemplo `description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvd`, deben ser `base 64-encoded` y deben estar en cadenas de caracteres binarias o UTF-8. Si los valores se leen

desde un archivo, como por ejemplo el atributo `jpegPhoto`, que se especifican mediante la dirección web, también deben estar en binaria o UTF-8. Para tales valores de atributos, no se realizará ninguna conversión del `charset` especificado a UTF-8.

Ejemplo 2:

En el ejemplo siguiente, se espera que el contenido de un archivo LDIF sin la etiqueta `charset` esté en UTF-8:

```
# Archivo LDIF de IBM Directorysample
#
# El sufijo "o=sample" debe estar definido antes de intentar cargar
# estos datos.

 versión: 1

 dn: o=sample
 objectclass: top
 objectclass: organization
 o: sample

 dn: ou=Austin, o=sample
 ou: Austin
 objectclass: organizationalUnit
 seealso: cn=Mary Smith, ou=Austin, o=sample
```

En IBM Security Directory Server, el archivo LDIF con el siguiente contenido se puede utilizar sin la información de cabecera `version: 1`:

```
# Archivo LDIF de IBM Directorysample
#
# El sufijo "o=sample" debe estar definido antes de intentar cargar
# estos datos.

 dn: o=sample
 objectclass: top
 objectclass: organization
 o: sample

 dn: ou=Austin, o=sample
 ou: Austin
 objectclass: organizationalUnit
 seealso: cn=Linda Carlesberg, ou=Austin, o=sample
```

Juegos de caracteres IANA soportados

Puede utilizar los nombres de juegos de caracteres IANA (Internet Assigned Number Authority) en un archivo LDIF o con la interfaz C Client para identificar el juego de caracteres de los datos de directorios.

IBM Security Directory Server da soporte a los nombres del juego de caracteres IANA (Internet Assigned Number Authority) por sistemas operativos.

Para obtener más información sobre los juegos de caracteres registrados para IANA, consulte el sitio web Juegos de caracteres en www.iana.org/assignments/character-sets.

Tabla 38. juegos de caracteres definidos con IANA

Carácter	Local					Página de códigos de DB2	
Nombre del juego	**HP-UX**	**Linux, Linux_390,**	**Windows**	**AIX**	**Solaris**	**UNIX**	**Windows**
ISO-8859-1	X	X	X	X	X	819	1252

Tabla 38. juegos de caracteres definidos con IANA (continuación)

Carácter	Local					Página de códigos de DB2	
Nombre del juego	HP-UX	Linux, Linux_390,	Windows	AIX	Solaris	UNIX	Windows
ISO-8859-2	X	X	X	X	X	912	1250
ISO-8859-5	X	X	X	X	X	915	1251
ISO-8859-6	X	X	X	X	X	1089	1256
ISO-8859-7	X	X	X	X	X	813	1253
ISO-8859-8	X	X	X	X	X	916	1255
ISO-8859-9	X	X	X	X	X	920	1254
ISO-8859–15	X	n/d	X	X	X		
IBM437	n/d	n/d	X	n/d	n/d	437	437
IBM850	n/d	n/d	X	X	n/d	850	850
IBM852	n/d	n/d	X	n/d	n/d	852	852
IBM857	n/d	n/d	X	n/d	n/d	857	857
IBM862	n/d	n/d	X	n/d	n/d	862	862
IBM864	n/d	n/d	X	n/d	n/d	864	864
IBM866	n/d	n/d	X	n/d	n/d	866	866
IBM869	n/d	n/d	X	n/d	n/d	869	869
IBM1250	n/d	n/d	X	n/d	n/d		
IBM1251	n/d	n/d	X	n/d	n/d		
IBM1253	n/d	n/d	X	n/d	n/d		
IBM1254	n/d	n/d	X	n/d	n/d		
IBM1255	n/d	n/d	X	n/d	n/d		
IBM1256	n/d	n/d	X	n/d	n/d		
TIS-620	n/d	n/d	X	X	n/d	874	874
EUC-JP	X	X	n/d	X	X	954	n/d
EUC-KR	n/d	n/d	n/d	X	X	970	n/d
EUC-CN	n/d	n/d	n/d	X	X	1383	n/d
EUC-TW	X	n/d	n/d	X	X	964	n/d
Shift-JIS	n/d	X	X	X	X	932	943
KSC	n/d	n/d	X	n/d	n/d	n/d	949
GBK	n/d	n/d	X	X	n/d	1386	1386
Big5	X	n/d	X	X	X	950	950
GB18030	n/d	X	X	X	X		
HP15CN	X (sin GB18030)						

Nota:

- El estándar del juego de caracteres chino, GB18030, está soportado por los parches adecuados disponibles desde www.oracle.com y www.microsoft.com
- En los sistemas operativos Windows, debe establecer la variable de entorno *zhCNGB18030* en TRUE.

Caracteres ASCII del 33 al 126

Utilice la tabla de caracteres ASCII para determinar los caracteres que se deben utilizar para el inicio de cifrado y el algoritmo de cifrado de la instancia de servidor de directorios.

Puede utilizar los caracteres ASCII del 33 al 126 en la cadena de inicio de cifrado y en el algoritmo de cifrado.

Tabla 39. Caracteres ASCII del 33 al 126

Código ASCII	Carácter	Código ASCII	Carácter	Código ASCII	Carácter
33	! signo de exclamación	34	" comillas dobles	35	# signo de almohadilla
36	$ signo de dólar	37	% signo de porcentaje	38	& ampersand
39	' apóstrofo	40	(paréntesis izquierdo	41	) paréntesis derecho
42	* asterisco	43	+ signo más	44	, coma
45	- guión	46	. punto	47	/ barra inclinada
48	0	49	1	50	2
51	3	52	4	53	5
54	6	55	7	56	8
57	9	58	: dos puntos	59	; punto y coma
60	< signo menor que	61	= signo igual	62	> signo mayor que
63	? interrogación	64	@ arroba	65	A a mayúscula
66	B b mayúscula	67	C c mayúscula	68	D de mayúscula
69	E e mayúscula	70	F f mayúscula	71	G g mayúscula
72	H h mayúscula	73	I i mayúscula	74	J j mayúscula
75	K k mayúscula	76	L l mayúscula	77	M m mayúscula
78	N n mayúscula	79	O o mayúscula	80	P p mayúscula
81	Q q mayúscula	82	R r mayúscula	83	S s mayúscula
84	T t mayúscula	85	U u mayúscula	86	V v mayúscula
87	W w mayúscula	88	X x mayúscula	89	Y y mayúscula
90	Z z mayúscula	91	[corchete izquierdo	92	\ barra inclinada invertida
93	] corchete derecho	94	^ acento circunflejo	95	_ subrayado
96	` acento grave	97	a a minúscula	98	b b minúscula
99	c c minúscula	100	d d minúscula	101	e e minúscula
102	f f minúscula	103	g g minúscula	104	h h minúscula
105	i i minúscula	106	j j minúscula	107	k k minúscula
108	l l minúscula	109	m m minúscula	110	n n minúscula
111	o o minúscula	112	p p minúscula	113	q q minúscula
114	r r minúscula	115	s s minúscula	116	t t minúscula
117	u u minúscula	118	v v minúscula	119	w w minúscula
120	x x minúscula	121	y y minúscula	122	z z minúscula
123	{ llave izquierda	124	| barra vertical	125	} llave derecha
126	~ tilde				

Capítulo 18. Creación y administración de instancias

Para utilizar un servidor de directorios en una infraestructura de identidades, debe crear una instancia de servidor de directorios según sus necesidades.

Tras completar la instalación de IBM Security Directory Server, debe crear una instancia de servidor de directorios y, a continuación, definir el nombre distinguido y la contraseña del administrador para la instancia. Puede crear un servidor de directorios completo o un servidor proxy. Para crear una instancia de servidor de directorios o una instancia de servidor proxy, debe crear un ID de usuario de sistema en el sistema. El ID de usuario de sistema es el propietario de la instancia de servidor de directorios o de la instancia de servidor proxy.

Para obtener un servidor de directorios completo, debe crear una base de datos de DB2 y configurar la base de datos con la instancia de servidor de directorios. Para crear una base de datos de DB2, debe instalar una versión soportada de DB2 en el sistema. Debe comprobar si el archivo `ldapdb.properties` está actualizado con la versión y la vía de acceso de instalación de DB2. Para obtener más información, consulte el Apéndice C, "Actualización del archivo `ldapdb.properties` manualmente", en la página 259.

Nota: Al utilizar IBM Security Directory Server Herramienta de administración de instancias (**idsxinst**) para crear una instancia de servidor de directorios completa, también se crea un archivo `ldapdb.properties` en el directorio de inicio de la instancia. En Windows, el archivo `ldapdb.properties` se encuentra en el directorio *inicio_instancia*\idsslapd-*nombre_instancia*\etc. En AIX, Linux, o Solaris, el archivo se encuentra en el directorio *inicio_instancia*/idsslapd-*nombre_instancia*/etc.

Para una instancia de servidor proxy, no cree ni configure una base de datos de DB2 con la instancia de servidor proxy.

Herramienta de administración de instancias es una interfaz gráfica de usuario (GUI) que puede utilizar para crear y gestionar las instancias de servidor de directorios. Para utilizar Herramienta de administración de instancias, es necesario IBM Java Development Kit. Al utilizar Herramienta de administración de instancias, la herramienta proporciona un asistente para ayudarle a completar la tarea.

Puede utilizar Herramienta de administración de instancias para crear, ver, copiar, modificar información sobre, y suprimir instancias. También puede utilizar la herramienta para crear o editar los usuarios que tienen instancias de servidor de directorios y para actualizar instancias de versiones anteriores de IBM Security Directory Server. Puede utilizar Herramienta de administración de instancias para iniciar o detener el servidor o el servidor de administración para las instancias. Además, puede abrir Herramienta de configuración de Herramienta de administración de instancias.

También puede utilizar los programas de utilidad de línea de mandatos para crear y gestionar instancias de servidor de directorios.

Inicio de Herramienta de administración de instancias

Inicie Herramienta de administración de instancias para crear y administrar una instancia de servidor de directorios o una instancia de servidor proxy.

Antes de empezar

Para utilizar Herramienta de administración de instancias, debe instalar IBM Security Directory Server con el Server, Proxy Server, o ambas características. Para ejecutar Herramienta de administración de instancias, inicie sesión con las siguientes credenciales:

AIX, Linux, y Solaris
Inicie sesión como usuario root.

Windows
Inicie sesión como miembro del grupo de administradores.

Debe existir IBM Java Development Kit en la vía de acceso de instalación de IBM Security Directory Server. Para la vía de acceso de instalación predeterminada de IBM Security Directory Server, consulte "Ubicaciones de la instalación predeterminada" en la página 27.

Procedimiento

Para iniciar Herramienta de administración de instancias, utilice una de las siguientes opciones:

Opciones para abrir Herramienta de administración de instancias	**Mandato a ejecutar:**
Instalación de la característica IBM Security Directory Server Server	En la página **Resumen**, pulse **Herramienta de administración de instancias (idsxinst)**. Para obtener más información, consulte "Instalación con IBM Installation Manager" en la página 31.

Opciones para abrir Herramienta de administración de instancias	Mandato a ejecutar:
El mandato `idsxinst`	**Windows** 1. Cambie el directorio actual al directorio `sbin` en la ubicación de instalación de IBM Security Directory Server. 2. Ejecute el mandato **`idsxinst`**. **Nota:** También puede pulsar **Inicio** > **Todos los programas** > **IBM Security Directory Server 6.3.1** > **Herramienta de administración de instancias**. **AIX, Linux, y Solaris** 1. Cambie el directorio actual al directorio `sbin` en la ubicación de instalación de IBM Security Directory Server. 2. Ejecute el mandato **`idsxinst`**. Para obtener más información sobre la vía de acceso de instalación de IBM Security Directory Server, consulte "Ubicaciones de la instalación predeterminada" en la página 27.

Inicio de Herramienta de administración de instancias para actualizar una instancia

Ejecute Herramienta de administración de instancias con parámetros para abrir Herramienta de administración de instancias para actualizar una instancia remota que contenga datos de copia de seguridad.

Antes de empezar

Para actualizar una instancia remota, debe cumplir los requisitos siguientes:

- El sistema debe contener los datos de copia de seguridad de la instancia creados con el mandato **`migbkup`**. Debe utilizar el mandato **`migbkup`** de una versión a la que desee actualizar la instancia remota.
- Inicie la sesión como usuario root en sistemas AIX, Linux, y Solaris. En Windows, inicie sesión como miembro de un grupo de administradores.

Procedimiento

1. Acceda al indicador de mandatos.
2. Cambie el directorio de trabajo actual al directorio `sbin` de la ubicación de instalación de IBM Security Directory Server. Para obtener más información sobre la vía de acceso de instalación predeterminada, consulte "Ubicaciones de la instalación predeterminada" en la página 27.
3. Ejecute el mandato **`idsxinst`** en el formato siguiente:

   ```
   idsxinst -migrate directorio_copia_seguridad
   ```

Sustituya la variable *directorio_copia_seguridad* por la ubicación en la que ha almacenado los datos de copia de seguridad de la instancia creada con el mandato **migbkup**.

Creación de la instancia de servidor de directorios

Para utilizar una instancia de servidor de directorios en un entorno de LDAP, cree una instancia sincronizada criptográficamente con la instancia existente para obtener un rendimiento óptimo

Si crea una instancia de servidor de directorios como una copia de una instancia de servidor de directorios existente, las dos instancias de servidor de directorios se sincronizarán criptográficamente. No es necesario sincronizarlas.

Si crea una instancia que no es una copia de una instancia existente, sincronice criptográficamente la instancia con la instancia existente. Debe sincronizar criptográficamente las instancias del servidor para obtener el mejor rendimiento en el entorno siguiente:

- Réplica
- Directorio distribuido
- Importe y exporte los datos LDIF entre las instancias del servidor

Debe sincronizar las instancias del servidor antes de realizar ningunas de las operaciones siguientes:

- Inicie la nueva instancia de servidor.
- Ejecute el mandato **idsbulkload** en la instancia de servidor.
- Ejecute el mandato **idsldif2db** en la instancia de servidor.

Para obtener más información acerca de cómo sincronizar los servidores de directorios, consulte la sección *Administración* en la documentación de IBM Security Directory Server.

Tras crear una instancia de servidor de directorios y configurarla con una base de datos de DB2, realice una copia de seguridad de la instancia de servidor de directorios. Debe realizar una copia de seguridad de la configuración, los esquemas, la base de datos de DB2, y los archivos de ocultación claves del directorio. Puede utilizar el mandato **idsdbback** para crear la copia de seguridad de la instancia de servidor de directorios. Puede utilizar el mandato **idsdbrestore** para restaurar los archivos de ocultación clave si es necesario. Para obtener más información sobre los mandatos de copia de seguridad y de restauración, consulte *Consulta de mandatos*.

Creación de instancias con Herramienta de administración de instancias

Debe evaluar los requisitos del entorno y crear una instancia de servidor de directorios en una fase adecuada para el entorno.

Puede utilizar Herramienta de administración de instancias para crear una instancia de varias formas:

- Crear una instancia predeterminada con un nombre predeterminado y otros valores. Consulte el apartado "Creación de la instancia de servidor de directorios predeterminada" en la página 137.

- Cree una instancia con valores personalizados. Consulte el apartado "Creación de una instancia de servidor de directorios con valores personalizados" en la página 139.
- Actualice una instancia de una versión anterior de IBM Security Directory Server. Consulte "Actualización de una instancia de una versión anterior con el mandato **idsimigr**" en la página 94 o "Actualización de una instancia de una versión anterior con Herramienta de administración de instancias" en la página 152.
- Cree una instancia que sea una copia de una instancia existente del sistema o de otro sistema. Consulte el apartado "Creación de una copia de una instancia existente con Herramienta de administración de instancias" en la página 158.

Creación de la instancia de servidor de directorios predeterminada

Utilice la opción de creación de instancia predeterminada para crear una instancia de servidor de directorios con el nombre de instancia predefinido y los valores predeterminados.

Antes de empezar

Para crear una instancia predeterminada, debe realizar estas tareas:

1. Instale IBM Security Directory Server con la característica de Servidor. Consulte el apartado "Instalación con IBM Installation Manager" en la página 31.
2. Instale IBM DB2. Consulte el apartado "Instalación con IBM Installation Manager" en la página 31.
3. Verifique si el archivo `ldapdb.properties` contiene la vía de acceso de instalación de DB2 y la información de la versión. Consulte el apartado Apéndice C, "Actualización del archivo `ldapdb.properties` manualmente", en la página 259.

Acerca de esta tarea

Si el sistema contiene una instancia de servidor de directorios existente con el nombre de instancia predeterminado, no podrá crear la instancia de servidor de directorios predeterminada.

La instancia de servidor de directorios predeterminada contiene los valores siguientes, que no se pueden cambiar:

Tabla 40. Los valores para una instancia de servidor de directorios predeterminada

Valores	Microsoft Windows	AIX y Linux	Solaris
Nombre	`dsrdbm01`	`dsrdbm01`	`dsrdbm01`
Ubicación de la instancia	`c:\idsslapd-dsrdbm01`	`/home/dsrdbm01`	`/export/home/dsrdbm01`
Nombre de grupo	`Administradores`	`grrdbm01`	`grrdbm01`
Nombre distinguido del administrador	`cn=root`	`cn=root`	`cn=root`
Nombre de base de datos	`dsrdbm01`	`dsrdbm01`	`dsrdbm01`

El espacio de tablas de DB2 para la instancia de servidor de directorios predeterminada es DMS (Database Managed Storage).

Para la instancia de servidor de directorios predeterminada, Herramienta de administración de instancias creará el sufijo `o=sample`. Puede añadir más sufijos más tarde con Herramienta de configuración o con el mandato **idscfgsuf**. Para obtener más información, consulte el "Configuración de sufijos" en la página 210.

Procedimiento

1. Inicie la Herramienta de administración de instancias. Consulte el apartado "Inicio de Herramienta de administración de instancias" en la página 134.
2. Pulse **Crear una instancia**.
3. En la ventana **Crear nueva instancia del servidor de directorios**, siga estos pasos:
   a. Pulse **Crear instancia predeterminada**.
   b. Pulse **Siguiente**.
   c. En el campo **Contraseña de usuario**, especifique una contraseña para la cuenta de usuario que es propietaria de la instancia de servidor de directorios.
   d. En el campo **Confirmar contraseña**, especifique la contraseña de nuevo para la cuenta de usuario que es propietaria de la instancia de servidor de directorios.
   e. En el campo **Inicio de cifrado**, especifique un inicio de cifrado para la instancia de servidor de directorios.

      Recuerde: Debe recordar el inicio de cifrado de una instancia de servidor de directorios, ya que puede ser necesario para otras tareas de configuración.
      El inicio de cifrado sólo debe contener caracteres imprimibles `ISO-8859-1 ASCII` con valores en el rango de 33 a 126. El inicio de cifrado debe contener un mínimo de 12 y un máximo de 1016 caracteres. Para obtener información sobre los caracteres a utilizar, consulte "Caracteres ASCII del 33 al 126" en la página 132. El servidor de directorios utiliza el inicio de cifrado para generar un conjunto de valores claves secretos de AES (Advanced Encryption Standard). Los archivos de ocultación claves de una instancia de servidor de directorios almacenan los valores claves, y se utilizan para cifrar y descifrar la contraseña y los atributos.
   f. En el campo **Confirmar inicio de cifrado**, especifique el inicio de cifrado para la instancia de servidor de directorios.
   g. En la **Contraseña del nombre distinguido del administrador** archivada, especifique una contraseña para el administrador de la instancia de servidor de directorios.
   h. En **Confirmar contraseña** archivado, especifique la contraseña para el administrador de instancias de servidor de directorios.
   i. Pulse **Siguiente**.
   j. Verifique la información sobre la instancia de servidor de directorios predeterminada. y
   k. Para comenzar a crear la instancia de servidor de directorios predeterminada, pulse **Finalizar**. Se mostrará la ventana Resultados con la información de registro.
4. Verifique que la información de registro se muestra en la ventana **Resultados**.
5. Para cerrar la ventana **Resultados**, pulse **Cerrar**.
6. Para cerrar Herramienta de administración de instancias, pulse **Cerrar**.

Resultados

Herramienta de administración de instancias creará la instancia de servidor de directorios predeterminada, `dsrdbm01`, en el sistema.

Qué hacer a continuación

Deberá iniciar el proceso y el servidor de administración de `ibmslapd` que está asociado con la instancia de servidor de directorios. Consulte el apartado "Iniciar o detener un servidor de directorios y un servidor de administración" en la página 161.

Creación de una instancia de servidor de directorios con valores personalizados

Utilice Servidor de administración de instancias para crear una instancia de servidor de directorios con valores personalizados según sus requisitos.

Antes de empezar

Para crear una instancia de servidor de directorios, debe completar las tareas siguientes:

1. Instale IBM Security Directory Server con la característica de Servidor. Consulte el apartado "Instalación con IBM Installation Manager" en la página 31.
2. Para crear un servidor de directorios completo con el programa de fondo RDBM, instale IBM DB2. Consulte el apartado "Instalación con IBM Installation Manager" en la página 31.
3. Verifique si el archivo `ldapdb.properties` contiene la vía de acceso de instalación de DB2 y la información de la versión. Consulte el apartado Apéndice C, "Actualización del archivo `ldapdb.properties` manualmente", en la página 259.

Procedimiento

1. Inicie la Herramienta de administración de instancias. Consulte el apartado "Inicio de Herramienta de administración de instancias" en la página 134.
2. Pulse **Crear una instancia**.
3. En el panel **Crear o migrar** de la ventana **Crear nueva instancia de servidor de directorios**, pulse **Crear una nueva instancia de servidor de directorios**.
4. Pulse **Siguiente**.
5. En el panel **Detalles de instancia** de la ventana **Crear nueva instancia de servidor de directorios**, especifique los valores siguientes:
   a. En la lista **Nombre de usuario**, seleccione el nombre del usuario propietario de la instancia de servidor de directorios. La instancia de servidor de directorios se asigna al mismo nombre que el nombre del usuario.
   b. Si desea asociar una nueva cuenta de usuario con la instancia, pulse **Crear usuario**. En la ventana **Crear usuario nuevo para la instancia de servidor de directorios**, siga estos pasos:
      1) En el campo **Nombre de usuario**, especifique el nombre de usuario.
      2) En el campo **Contraseña**, especifique una contraseña para la cuenta de usuario.
      3) En el campo **Confirmar contraseña**, especifique la contraseña para la cuenta de usuario.

4) En el campo **Directorio de inicio**, especifique el directorio de inicio a configurar para la cuenta de usuario. Puede pulsar **Examinar** y especificar el directorio de inicio.
5) En el campo **Grupo primario**, especifique el nombre de grupo primario del usuario.
6) Para crear la cuenta de usuario, pulse **Crear**.

c. Para modificar una cuenta de usuario existente, seleccione el nombre de usuario desde la lista **Nombre de usuario** y pulse **Editar usuario**. En la ventana **Editar el usuario para la instancia de servidor de directorios**, siga estos pasos:
1) El campo **Nombre de usuario** se rellenará con el nombre de usuario.
2) En el campo **Contraseña**, especifique una contraseña para la cuenta de usuario.
3) En el campo **Confirmar contraseña**, especifique la contraseña para la cuenta de usuario.
4) En el campo **Directorio de inicio**, especifique el directorio de inicio a configurar para la cuenta de usuario. Puede pulsar **Examinar** y especificar el directorio de inicio.
5) En el campo **Grupo primario**, especifique el nombre de grupo primario del usuario.
6) Para editar la cuenta de usuario, pulse **Editar**.

6. En el campo **Ubicación de la instancia**, especifique la ubicación de la instancia de servidor de directorios. Puede pulsar **Examinar** y especificar el directorio de inicio de la instancia. La ubicación debe contener al menos 30 MB de espacio libre en disco. En sistemas Windows, la ubicación es una unidad de disco, como por ejemplo `C:`. Los archivos de instancias de directorio se almacenan en el directorio `\idsslapd-`*`nombre_instancia`* en la unidad de disco que especifique. La variable *nombre_instancia* es el nombre de la instancia de servidor de directorios. En sistemas AIX, Linux, y Solaris, el directorio de inicio del propietario de la instancia de servidor de directorios es la ubicación de instancias predeterminada, pero puede especificar una vía de acceso distinta.
7. En el campo **Cadena de inicio de cifrado**, especifique el inicio de cifrado para la instancia de servidor de directorios.

   Recuerde: Debe recordar el inicio de cifrado de una instancia de servidor de directorios, ya que puede ser necesario para otras tareas de configuración. El inicio de cifrado sólo debe contener caracteres imprimibles `ISO-8859-1 ASCII` con valores en el rango de 33 a 126. El inicio de cifrado debe contener un mínimo de 12 y un máximo de 1016 caracteres. Para obtener información sobre los caracteres a utilizar, consulte “Caracteres ASCII del 33 al 126” en la página 132. El servidor de directorios utiliza el inicio de cifrado para generar un conjunto de valores claves secretos de AES (Advanced Encryption Standard). Los archivos de ocultación claves de una instancia de servidor de directorios almacenan los valores claves, y se utilizan para cifrar y descifrar la contraseña y los atributos.
8. En el campo **Confirmar inicio de cifrado**, especifique el inicio de cifrado para la instancia de servidor de directorios.
9. Si desea proporcionar un valor de algoritmo de cifrado, pulse **Utilizar valor de algoritmo de cifrado**.
   a. En el campo **Cadena de algoritmo de cifrado**, especifique un valor de algoritmo de cifrado para la instancia de servidor de directorios. El

algoritmo de cifrado debe contener únicamente caracteres imprimibles ISO-8859-1 ASCII con valores en el rango de 33 a 126. El algoritmo de cifrado debe contener 12 caracteres. Para obtener información sobre los caracteres a utilizar, consulte "Caracteres ASCII del 33 al 126" en la página 132. Para sincronizar criptográficamente un servidor de directorios con otra instancia de servidor de directorios, debe utilizar el mismo inicio de cifrado y los mismos valores de algoritmo.

b. En el campo **Confirmar algoritmo de cifrado**, especifique el valor de algoritmo de cifrado para la instancia de servidor de directorios.

10. Opcional: En el campo **Descripción de instancias**, una descripción de la instancia de servidor de directorios. La descripción ayuda a identificar la instancia.
11. Pulse **Siguiente**.
12. En el campo **Nombre de la instancia de DB2** del panel **Detalles de la instancia de DB2**, especifique el nombre de la instancia de DB2 para la instancia de servidor de directorios.

    Nota: La instancia de DB2 para la instancia de servidor de directorios no la deben configurar ni utilizar otros programas ni productos.

    De forma predeterminada, el nombre de la instancia de DB2 es el mismo que el nombre de instancia de servidor de directorios. Sin embargo, puede especificar un nombre distinto para la instancia de DB2. Si especifica un nombre distinto, debe existir un ID de usuario de sistema con el mismo nombre en el sistema. Este nombre de cuenta de usuario no debe estar asociado con otra instancia de servidor de directorios.
13. Pulse **Siguiente**.
14. En el panel **Valores TCP/IP para hosts múltiples**, seleccione una de las siguientes opciones:
    - Si desea que la instancia de servidor de directorios escuche en todas las direcciones IP, seleccione **Escuchar en todas las direcciones IP configuradas**.
    - Si desea que la instancia escuche en un conjunto determinado de direcciones IP configuradas en el sistema, siga estos pasos:
      a. Borre **Escuchar en todas las direcciones IP configuradas**.
      b. Desde la lista **Seleccionar las direcciones IP específicas en las que escuchar**, seleccione la dirección o direcciones IP en la que desea que escuche la instancia.
15. Pulse **Siguiente**.
16. En el panel **Valores de puerto TCP/IP**, especifique los valores siguientes:

    Nota: Debe asignar números de puerto exclusivos a los puertos de servidor de directorios y no debe entrar en conflicto con los puertos existentes que están en uso en el sistema. En los sistemas AIX, Linux, y Solaris, los números de puerto en el rango de 1 a 1000 sólo los puede utilizar root.

    a. En el campo **Puerto del servidor**, especifique el número de puerto que desea que utilice el servidor como puerto no seguro. El número debe estar en el rango de 1 a 65535.
    b. En el campo **Puerto seguro del servidor**, especifique el número de puerto que desea que utilice el servidor como puerto seguro. El número debe estar en el rango de 1 a 65535.

c. En el campo **Puerto del servidor de administración**, especifique el número de puerto que desea que utilice el servidor de administración como puerto no seguro. El número debe estar en el rango de 1 a 65535.

d. En el campo **Puerto seguro del servidor de administración**, especifique el número de puerto que desea que utilice el servidor de administración como puerto seguro. El número debe estar en el rango de 1 a 65535.

e. Pulse **Siguiente**.

17. En el panel **Pasos opcionales**, realice estos pasos:

a. Para configurar el nombre distinguido y la contraseña del administrador para la instancia de servidor de directorios, seleccione **Configurar nombre distinguido y contraseña del administrador**. Debe configurar el nombre distinguido y la contraseña del administrador para un servidor proxy y un servidor de directorios completo.

b. Para configurar la base de datos para la instancia de servidor de directorios, seleccione **Configurar base de datos**.

c. Pulse **Siguiente**.

18. En el panel **Configurar nombre distinguido y contraseña del administrador**, siga estos pasos:

a. En el campo **Nombre distinguido del administrador**, especifique un nombre distinguido válido o acepte el nombre distinguido predeterminado, `cn=root`. El valor de nombre distinguido del administrador no distingue entre mayúsculas ni minúsculas. El usuario de nombre distinguido del administrador tiene acceso completo a todos los datos en la instancia del servidor de directorios.

b. En el campo **Contraseña del administrador**, especifique la contraseña para el nombre distinguido del administrador. Las contraseñas son sensibles a las mayúsculas y minúsculas. Los caracteres pertenecientes al juego de caracteres de doble byte (DBCS) de la contraseña no son válidos.

c. En el campo **Confirmar contraseña**, especifique la contraseña para el nombre distinguido del administrador. Debe recordar la contraseña para referencia futura.

d. Pulse **Siguiente**.

19. En el panel **Configurar base de datos**, lleve a cabo las tareas siguientes para configurar la base de datos para la instancia de servidor de directorios: Herramienta de administración de instancias añade la información de la base de datos en el archivo de configuración, `ibmslapd.conf`, para la instancia de servidor de directorios. Si la base de datos no existe, Herramienta de administración de instancias creará la base de datos.

a. En el campo **Nombre de usuario de base de datos**, especifique un ID de administrador de DB2 válido. Debe existir el ID de administrador de DB2 en el sistema y debe contener el permiso de acceso necesario antes de configurar la base de datos.

Nota: El ID de administrador de DB2 debe establecer el entorno local adecuado para el idioma en el que desea que se muestren los mensajes del servidor antes del inicio del servidor.

b. En el campo **Contraseña**, especifique la contraseña para el administrador de DB2. La contraseña distingue entre mayúsculas y minúsculas.

Nota: Si cambia la contraseña del sistema para el administrador de DB2, no podrá actualizarla con Herramienta de administración de instancias. Debe utilizar Herramienta de configuración o el mandato **idscfgdb** con el

parámetro **-w**. Para obtener más información, consulte el "Gestión de la contraseña del administrador de bases de datos de DB2" en la página 187.

c. En el campo **Nombre de base de datos**, especifique un nombre de base de datos de DB2. El nombre debe estar en el rango de 1 a 8 caracteres de longitud.

d. Opcional: Si desea establecer cualquiera de los siguientes valores de configuración de DB2, seleccione **Mostrar opciones avanzadas de espacio de tabla**.

Nota: DB2 puede utilizar el tipo de almacenamiento de datos de SMS (System Managed Storage) o DMS (Database Managed Storage) cuando crea espacios de tablas. El valor predeterminado para IBM Security Directory Server es DMS (Database Managed Storage). Las versiones de IBM Security Directory Server anteriores a 6.2 utilizan SMS para todas las bases de datos. Si borra **Mostrar opciones avanzadas del espacio de tablas**, se crearán espacios de tablas de `USERSPACE1` y `LDAPSPACE` utilizando DMS con los tamaños y las ubicaciones predeterminados. En AIX, Linux, y Solaris, la vía de acceso y el nombre de archivo predeterminados para el espacio de tablas de `USERSPACE1` es *`ubicación_base_datos`*`/`*`nombre_instancia`*`/NODE0000/SQL00001/USPACE`. En Windows, la vía de acceso y el nombre de archivo predeterminados para el espacio de tablas de `USERSPACE1` es *`ubicación_base_datos`*`\`*`nombre_instancia`*`\NODE0000\SQL00001\USPACE`. En AIX, Linux, y Solaris, la vía de acceso y el nombre de archivo predeterminados para el espacio de tablas de `LDAPSPACE` es *`ubicación_base_datos`*`/ldap32kcont_`*`nombre_instancia`*`/ldapspace`. En Windows, la vía de acceso y el nombre de archivo predeterminados para el espacio de tablas de `LDAPSPACE` es *`ubicación_base_datos`*`\ldap32kcont_`*`nombre_instancia`*`\ldapspace`.

- Desea que la base de datos utilice el almacenamiento de datos de SMS (System Managed Storage) para los espacios de tablas de DB2. Cuando se utiliza SMS, el gestor del sistema de archivos del sistema operativo asigna y gestiona el espacio de tablas donde se almacenan las tablas de DB2.
- Desea que la base de datos utilice el almacenamiento de datos de DMS (Database Managed Storage) para los espacios de tablas de DB2. Además, desea configurar la base de datos para los espacios de tablas, el tamaño y la ubicación de `USERSPACE1` y `LDAPSPACE`. Cuando se utiliza DMS, los espacios de tablas los gestiona el gestor de bases de datos. El administrador de bases de datos decide qué dispositivos y archivos va a utilizar y DB2 gestiona el espacio en dichos dispositivos y archivos.

e. Pulse **Siguiente**.

20. En el panel **Opciones de base de datos**, siga estos pasos:

a. En el campo **Ubicación de instalación de base de datos**, especifique la vía de acceso de ubicación de la base de datos. Puede pulsar **Examinar** para especificar un directorio. En Windows, debe proporcionar una ubicación de unidad de disco, `C:`. En AIX, Linux, y Solaris, la ubicación debe ser un nombre de directorio, como por ejemplo `/home/ldapdb`.

Nota: El espacio de disco mínimo necesario para una base de datos de DMS es 1 GB. Para una base de datos de SMS, es necesario un mínimo de 150 MB de espacio de disco. Estos requisitos son para una base de datos vacía. Si almacena datos en la base de datos, necesitará más espacio de disco.

b. Para configurar el servidor de directorios con la base de datos para la copia de seguridad en línea, siga estos pasos:
   1) Seleccione **Configurar para la copia de seguridad en línea**.
   2) En el campo **Ubicación de copia de seguridad de base de datos**, especifique la ubicación donde desea almacenar la imagen de copia de seguridad. Puede pulsar **Examinar** para especificar la ubicación.

   Nota: No salga de Herramienta de administración de instancias cuando se esté ejecutando la operación de copia de seguridad.
   Al configurar la base de datos para la copia de seguridad en línea una vez que haya finalizado la configuración de la base de datos, se ejecutará una copia de seguridad inicial y fuera de línea de la base de datos. Una vez que haya finalizado la operación de copia de seguridad fuera de línea, se reiniciará el servidor de administración. También puede configurar la copia de seguridad en línea para una instancia de servidor de directorios con el mandato **idscfgdb**. Sin embargo, no puede desconfigurar la copia de seguridad en línea con el mandato **idscfgdb** ni el parámetro **-c**. Si configura la copia de seguridad en línea para una instancia con Herramienta de administración de instancias o Herramienta de configuración, puede desconfigurarla con Herramienta de configuración o con el mandato **idscfgdb**.

c. En el área **Opción de juego de caracteres**, elija una de las siguientes opciones para crear un tipo de base de datos:

   Nota: Cree una base de datos universal de DB2 si tiene previsto almacenar datos en varios idiomas en el servidor de directorios. Una Base de datos universal de DB2 también es más eficaz porque requiere menor conversión de datos. Si desea utilizar códigos de idioma, la base de datos debe ser UTF-8. Para obtener más información sobre UTF-8, consulte el "Soporte de UTF-8" en la página 128.
   - Para crear una base de datos de UTF-8 (UCS Transformation Format) en la que los clientes de LDAP pueden almacenar datos de caracteres UTF-8, pulse **Crear una base de datos universal de DB2**.
   - Para crear una base de datos en la página de códigos local, pulse **Crear una base de datos de DB2 de página de códigos local**.

d. Pulse **Siguiente**.

21. Si ha seleccionado **Mostrar opciones avanzadas del espacio de tablas** en el panel **Configurar base de datos**, debe seguir los valores siguientes en el panel **Configurar espacios de tablas de base de datos**:
    a. En la lista **Seleccionar tipo de espacio de tabla de base de datos**, seleccione un tipo de base de datos. El tipo de espacio de tablas de la base de datos de DMS es el predeterminado. Si selecciona el tipo de espacio de tablas de base de datos de SMS, se inhabilitarán el resto de los campos. El soporte del espacio de tablas de DMS sólo se utilizará para los espacios de tablas de `USERSPACE1` y `LDAPSPACE`. El resto de los espacios de tablas, como por ejemplo espacios de tabla de catálogo y temporales, son del tipo SMS.
    a. En el área **Detalles del espacio de tablas de USERSPACE1**, especifique los detalles siguientes:
       1) En la lista **Contenedor del espacio de tablas**, seleccione el tipo de contenedor. Si desea la ubicación del espacio de tablas de `USERSPACE1` en el sistema de archivos, seleccione **Archivo**. Si la ubicación del contenedor del espacio de tablas de la base de datos se encuentra en un sistema de archivos, se creará un espacio de tablas `cooked` de DMS.

Puede especificar el tamaño inicial para el espacio de tablas y un tamaño de unidad extensible, y el espacio de tablas se expandirá automáticamente cuando sea necesario. Si desea crear el espacio de tablas de USERSPACE1 en un dispositivo sin formato, seleccione **Dispositivo sin formato**. Un dispositivo sin formato es un dispositivo donde no hay instalado ningún sistema de archivos, como por ejemplo un disco duro que no contiene un sistema de archivos. Si la ubicación del contenedor del espacio de tablas de la base de datos se encuentra en un dispositivo sin formato, se creará un espacio de tablas raw de DMS. En este caso, el tamaño del contenedor del espacio de tablas de la base de datos es fijo y no se puede ampliar. Si selecciona **Dispositivo sin formato**, especifique el tamaño junto con la ubicación del contenedor en lugar de aceptar los valores predeterminados.

2) Si ha seleccionado **Archivo** en la lista **Contenedor del espacio de tablas**, especifique los detalles siguientes:
   a) En el campo **Vía de acceso de directorio**, especifique la vía de acceso del directorio en la que desea crear el espacio de tablas de USERSPACE1. Puede pulsar **Examinar** para seleccionar el directorio.
   b) En el campo **Nombre de archivo**, especifique el nombre de archivo del espacio de tablas que desee crear, o acepte el nombre de archivo predeterminado, USPACE.
   c) En el campo **Tamaño inicial**, especifique el tamaño inicial para el espacio de tablas de USERSPACE1 en páginas o acepte el valor predeterminado. Para el contenedor del espacio de tablas del tipo **Archivo**, el contenedor del espacio de tablas de USERSPACE1 es del tipo autoincremental. Puede proporcionar el tamaño inicial en el campo **Tamaño inicial**, y un tamaño de unidad extensible en el campo **Tamaño extensible**. El valor predeterminado para el tamaño inicial es 16.000 páginas, y el tamaño de unidad extensible predeterminado es 8.000 páginas. El tamaño de página para el contenedor del espacio de tablas de USERSPACE1 es de 4 KB por página.
3) Si ha seleccionado **Dispositivo sin formato** en la lista **Contenedor del espacio de tablas**, especifique los detalles siguientes:
   a) En el campo **Vía de acceso del dispositivo**, especifique la ubicación del dispositivo sin formato. En Windows, la vía de acceso debe comenzar por \\.\. Un ejemplo que muestra la vía de acceso con el nombre del dispositivo, \\.*nombre_dispositivo*. En AIX, Linux, y Solaris, la vía de acceso del dispositivo debe ser una vía de acceso válida.
   b) En el campo **Tamaño inicial**, especifique el tamaño inicial para el espacio de tablas de USERSPACE1 o acepte el valor predeterminado. Para el contenedor del espacio de tablas de tipo **Dispositivo sin formato**, el tamaño del contenedor del espacio de tablas de USERSPACE1 es fijo. El tamaño predeterminado es de 16.000 páginas. Para obtener mejores resultados, especifique el tamaño que desee.

b. En el área **Detalles del espacio de tablas de LDAPSPACE**, especifique los detalles siguientes:
   1) En la lista **Contenedor del espacio de tablas**, seleccione el tipo de contenedor. Si desea la ubicación del espacio de tablas de LDAPSPACE en un sistema de archivos, seleccione **Archivo**. Si desea crear el espacio de tablas de LDAPSPACE en un dispositivo sin formato, seleccione **Dispositivo sin formato**. Un dispositivo sin formato es un dispositivo

donde no hay instalado ningún sistema de archivos, como por ejemplo un disco duro que no contiene un sistema de archivos.

2) Si ha seleccionado **Archivo** en la lista **Contenedor del espacio de tablas**, especifique los detalles siguientes:
   a) En el campo **Vía de acceso de directorio**, especifique la vía de acceso del directorio donde desee crear el espacio de tablas de LDAPSPACE. Puede pulsar **Examinar** para seleccionar el directorio.
   b) En el campo **Nombre de archivo**, especifique el nombre del archivo del espacio de tablas que desee crear, o acepte el nombre de archivo predeterminado, ldapspace.
   c) En el campo **Tamaño inicial**, especifique el tamaño inicial para el espacio de tablas de LDAPSPACE en páginas o acepte el valor predeterminado. Para el contenedor del espacio de tablas del tipo **Archivo**, el contenedor del espacio de tablas de LDAPSPACE es de tipo autoincremental. Puede proporcionar el tamaño inicial en el campo **Tamaño inicial**, y un tamaño de unidad extensible en el campo **Tamaño extensible**. El valor predeterminado para el tamaño inicial es 16.000 páginas, y el tamaño de unidad extensible predeterminado es 8.000 páginas. El tamaño de página para el contenedor del espacio de tablas de LDAPSPACE es de 32 KB por página.
3) Si ha seleccionado **Dispositivo sin formato** en la lista **Contenedor del espacio de tablas**, especifique los detalles siguientes:
   a) En el campo **Vía de acceso del dispositivo**, especifique la ubicación del dispositivo sin formato. En Windows, la vía de acceso debe comenzar por \\.\. Un ejemplo que muestra la vía de acceso con el nombre del dispositivo, \\.*nombre_dispositivo*. En AIX, Linux, y Solaris, la vía de acceso del dispositivo debe ser una vía de acceso válida.
   b) En el campo **Tamaño inicial**, especifique el tamaño inicial para el espacio de tablas de LDAPSPACE o acepte el valor predeterminado. Para el contenedor del espacio de tablas del tipo **Dispositivo sin formato**, el tamaño del contenedor del espacio de tablas de LDAPSPACE es fijo. El tamaño predeterminado es de 16.000 páginas. Para obtener mejores resultados, especifique el tamaño que desee.

c. Si ha seleccionado **Archivo** en uno o ambos de los campos **Contenedor del espacio de tablas**, especifique el número de páginas por el que se deben ampliar los contenedores de espacios de tablas en el campo **Tamaño expansible**.
d. Pulse **Siguiente**.

22. En el panel **Verificar valores**, verifique el resumen que se genera.
23. Para empezar la creación de la instancia de servidor de directorios, pulse **Finalizar**.
24. En la ventana **Resultados**, verifique los mensajes de registros que se generan para las operaciones de creación de instancias.
25. Para cerrar la ventana **Resultados**, pulse **Cerrar**.
26. Para cerrar Herramienta de administración de instancias, pulse **Cerrar**.

Resultados

Herramienta de administración de instancias creará una instancia de servidor de directorios en el sistema.

Qué hacer a continuación

Deberá iniciar el proceso y el servidor de administración de `ibmslapd` que está asociado con la instancia de servidor de directorios. Consulte el apartado "Iniciar o detener un servidor de directorios y un servidor de administración" en la página 161.

Creación de una instancia de servidor proxy con valores personalizados

Utilice Servidor de administración de instancias para crear una instancia de servidor proxy con valores personalizados según sus requisitos.

Antes de empezar

Para crear una instancia de servidor proxy, debe completar las tareas siguientes:

1. Instale IBM Security Directory Server con la característica de Proxy Server. Consulte el apartado "Instalación con IBM Installation Manager" en la página 31.

Procedimiento

1. Inicie la Herramienta de administración de instancias. Consulte el apartado "Inicio de Herramienta de administración de instancias" en la página 134.
2. Pulse **Crear una instancia**.
3. En el panel **Crear o migrar** de la ventana **Crear nueva instancia del servidor de directorios**, complete los pasos siguientes para crear una instancia de servidor proxy:
   a. Pulse **Crear una nueva instancia de servidor de directorios**.
   b. Pulse **Configurar como proxy**.
4. Pulse **Siguiente**.
5. En el panel **Detalles de instancia** de la ventana **Crear nueva instancia de servidor de directorios**, especifique los valores siguientes:
   a. Desde la lista **Nombre de usuario**, seleccione el nombre de usuario que es propietario de la instancia. La instancia tiene asignado el mismo nombre que el nombre de usuario.
   b. Si desea asociar una nueva cuenta de usuario con la instancia, pulse **Crear usuario**. En la ventana **Crear usuario nuevo para la instancia de servidor de directorios**, siga estos pasos:
      1) En el campo **Nombre de usuario**, especifique el nombre de usuario.
      2) En el campo **Contraseña**, especifique una contraseña para la cuenta de usuario.
      3) En el campo **Confirmar contraseña**, especifique la contraseña para la cuenta de usuario.
      4) En el campo **Directorio de inicio**, especifique el directorio de inicio a configurar para la cuenta de usuario. Puede pulsar **Examinar** y especificar el directorio de inicio.
      5) En el campo **Grupo primario**, especifique el nombre de grupo primario del usuario.
      6) Para crear la cuenta de usuario, pulse **Crear**.

c. Para modificar una cuenta de usuario existente, seleccione el nombre de usuario desde la lista **Nombre de usuario** y pulse **Editar usuario**. En la ventana **Editar el usuario para la instancia de servidor de directorios**, siga estos pasos:
   1) El campo **Nombre de usuario** se rellenará con el nombre de usuario.
   2) En el campo **Contraseña**, especifique una contraseña para la cuenta de usuario.
   3) En el campo **Confirmar contraseña**, especifique la contraseña para la cuenta de usuario.
   4) En el campo **Directorio de inicio**, especifique el directorio de inicio a configurar para la cuenta de usuario. Puede pulsar **Examinar** y especificar el directorio de inicio.
   5) En el campo **Grupo primario**, especifique el nombre de grupo primario del usuario.
   6) Para editar la cuenta de usuario, pulse **Editar**.
   7) En la ventana de confirmación **Editar el usuario para la instancia de servidor de directorios**, pulse **Sí**.

6. En el campo **Ubicación de la instancia**, especifique la ubicación de la instancia del servidor proxy. Puede pulsar **Examinar** y especificar el directorio de inicio de la instancia. La ubicación debe contener al menos 30 MB de espacio libre en disco. En sistemas Windows, la ubicación es una unidad de disco, como por ejemplo `C:`. Los archivos de instancias de directorio se almacenan en el directorio `\idsslapd-`*`nombre_instancia`* en la unidad de disco que especifique. La variable *nombre_instancia* es el nombre de la instancia de servidor proxy. En sistemas AIX, Linux, y Solaris, el directorio de inicio del propietario de instancias de servidor proxy es la ubicación de instancias predeterminada, pero puede especificar una vía de acceso distinta.
7. En el campo **Cadena de inicio de cifrado**, especifique el inicio de cifrado para la instancia.

   Recuerde: Debe recordar el inicio de cifrado de la instancia, ya que puede ser necesario para otras tareas de configuración.
   El inicio de cifrado sólo debe contener caracteres imprimibles `ISO-8859-1 ASCII` con valores en el rango de 33 a 126. El inicio de cifrado debe contener un mínimo de 12 y un máximo de 1016 caracteres. Para obtener información sobre los caracteres a utilizar, consulte “Caracteres ASCII del 33 al 126” en la página 132. El servidor de directorios utiliza el inicio de cifrado para generar un conjunto de valores claves secretos de AES (Advanced Encryption Standard). Los archivos de ocultación claves de una instancia de servidor de directorios almacenan los valores claves, y se utilizan para cifrar y descifrar la contraseña y los atributos.
8. En el campo **Confirmar inicio de cifrado**, especifique el inicio de cifrado para la instancia.
9. Si desea proporcionar un valor de algoritmo de cifrado, pulse **Utilizar valor de algoritmo de cifrado**.
   a. En el campo **Cadena de algoritmo de cifrado**, especifique un valor de algoritmo de cifrado para la instancia. El algoritmo de cifrado debe contener únicamente caracteres imprimibles `ISO-8859-1 ASCII` con valores en el rango de 33 a 126. El algoritmo de cifrado debe contener 12 caracteres. Para obtener información sobre los caracteres a utilizar, consulte “Caracteres ASCII del 33 al 126” en la página 132.
   b. En el campo **Confirmar algoritmo de cifrado**, especifique el valor de algoritmo de cifrado para la instancia.

10. Opcional: En el campo **Descripción de instancias**, una descripción de la instancia. La descripción ayuda a identificar la instancia.
11. Pulse **Siguiente**.
12. En el panel **Valores TCP/IP para hosts múltiples**, seleccione una de las siguientes opciones:
    - Si desea que la instancia escuche en todas las direcciones IP, seleccione **Escuchar en todas las direcciones IP configuradas**.
    - Si desea que la instancia escuche en un conjunto determinado de direcciones IP configuradas en el sistema, siga estos pasos:
      a. Borre **Escuchar en todas las direcciones IP configuradas**.
      b. Desde la lista **Seleccionar las direcciones IP específicas en las que escuchar**, seleccione la dirección o direcciones IP en la que desea que escuche la instancia.
13. Pulse **Siguiente**.
14. En el panel **Valores de puerto TCP/IP**, especifique los valores siguientes:

    Nota: Debe asignar números de puerto exclusivos a los puertos de servidor de directorios y no debe entrar en conflicto con los puertos existentes que están en uso en el sistema. En los sistemas AIX, Linux, y Solaris, los números de puerto en el rango de 1 a 1000 sólo los puede utilizar root.
    a. En el campo **Puerto del servidor**, especifique el número de puerto que desea que utilice el servidor como puerto no seguro. El número debe estar en el rango de 1 a 65535.
    b. En el campo **Puerto seguro del servidor**, especifique el número de puerto que desea que utilice el servidor como puerto seguro. El número debe estar en el rango de 1 a 65535.
    c. En el campo **Puerto del servidor de administración**, especifique el número de puerto que desea que utilice el servidor de administración como puerto no seguro. El número debe estar en el rango de 1 a 65535.
    d. En el campo **Puerto seguro del servidor de administración**, especifique el número de puerto que desea que utilice el servidor de administración como puerto seguro. El número debe estar en el rango de 1 a 65535.
    e. Pulse **Siguiente**.
15. En el panel **Pasos opcionales**, realice estos pasos:
    a. Para configurar el nombre distinguido y la contraseña del administrador para la instancia, seleccione **Configurar nombre distinguido y contraseña del administrador**. Debe configurar el nombre distinguido y la contraseña del administrador para una instancia de servidor proxy.
    b. Pulse **Siguiente**.
16. En el panel **Configurar nombre distinguido y contraseña del administrador**, siga estos pasos:
    a. En el campo **Nombre distinguido del administrador**, especifique un nombre distinguido válido o acepte el nombre distinguido predeterminado, `cn=root`. El valor de nombre distinguido del administrador no distingue entre mayúsculas ni minúsculas. El usuario de nombre distinguido del administrador tiene acceso completo a todos los datos de la instancia.
    b. En el campo **Contraseña del administrador**, especifique la contraseña para el nombre distinguido del administrador. Las contraseñas son sensibles a las mayúsculas y minúsculas. Los caracteres pertenecientes al juego de caracteres de doble byte (DBCS) de la contraseña no son válidos.

c. En el campo **Confirmar contraseña**, especifique la contraseña para el nombre distinguido del administrador. Debe recordar la contraseña para referencia futura.
d. Pulse **Siguiente**.

17. En el panel **Verificar valores**, verifique el resumen que se genera.
18. Para comenzar la creación de la instancia de servidor proxy, pulse **Finalizar**.
19. En la ventana **Resultados**, verifique los mensajes de registros que se generan para las operaciones de creación de instancias.
20. Para cerrar la ventana **Resultados**, pulse **Cerrar**.
21. Para cerrar Herramienta de administración de instancias, pulse **Cerrar**.

Resultados

Herramienta de administración de instancias crea una instancia de servidor proxy en el sistema.

Qué hacer a continuación

Debe iniciar el servidor de administración y el proceso `ibmslapd` en la modalidad de sólo configuración y configurar servidores de fondo. Consulte la sección *Administración* en la documentación de IBM Security Directory Server.

Creación de una instancia con el programa de utilidad de línea de mandatos

Utilice el programa de utilidad de línea de mandatos, **idsicrt**, para crear una instancia.

Antes de empezar

Para crear una instancia con el programa de utilidad de línea de mandatos, debe cumplir las condiciones siguientes:

1. Instale IBM Security Directory Server con el Server, Proxy Server, o ambas características. Consulte el apartado "Instalación con IBM Installation Manager" en la página 31.
2. Debe existir un ID de usuario de sistema que sea propietario de la instancia. Para obtener más información sobre la creación de un ID de usuario de sistema, consulte "Usuarios y grupos que están asociados con una instancia de servidor de directorios" en la página 123.

Acerca de esta tarea

Al ejecutar el mandato **idsicrt**, el mandato creará una instancia y una instancia de la base de datos de DB2 para la instancia de servidor de directorios completa.

Procedimiento

1. Inicie sesión como el usuario root en AIX, Linux, o Solaris, y como un miembro administrador en Windows.
2. Cambie el directorio de trabajo actual al subdirectorio `sbin` en la ubicación de instalación de IBM Security Directory Server.
3. Para crear una instancia, ejecute el mandato siguiente: Sustituya la variable *nombre_instancia* por el nombre de un ID de usuario de sistema válido.

Tarea a completar	Mandato a ejecutar:
Cree una instancia de servidor de directorios	`idsicrt -I nombre_instancia -e mysecretkey! -l inicio_instancia`
Cree una instancia de servidor proxy	`idsicrt -I nombre_instancia -e mysecretkey! -l inicio_instancia -x`

Para obtener más información sobre el mandato **idsicrt**, consulte *Consulta de mandatos*.

Ejemplos

Ejemplo 1:

Para crear una instancia de servidor de directorios con los valores siguientes en AIX, Linux, o Solaris, ejecute el mandato siguiente:

- Nombre de instancia: `myinst`
- Puerto no seguro: `389`
- Puerto seguro: `636`
- Inicio de cifrado: `mysecretkey!`
- Algoritmo de cifrado: `mysecretsalt`
- Inicio de instancia: `/home/myinst` en AIX y Linux, y `/export/home/myinst` en Solaris

```
idsicrt -I myinst -p 389 -s 636 -e mysecretkey!\
-g mysecretsalt -l /home/myinst
```

Para crear una instancia de servidor de directorios con los valores siguientes en Windows, ejecute el mandato siguiente:

- Nombre de instancia: `myinst`
- Puerto no seguro: `389`
- Puerto seguro: `636`
- Inicio de cifrado: `mysecretkey!`
- Algoritmo de cifrado: `mysecretsalt`
- Inicio de instancia: `C:`

```
idsicrt -I myinst -p 389 -s 636 -e mysecretkey!
-g mysecretsalt -l C:
```

Ejemplo 2:

Para crear una instancia de servidor proxy con los valores siguientes en AIX, Linux, o Solaris, ejecute el mandato siguiente:

- Nombre de instancia: `myproxy`
- Puerto no seguro: `389`
- Puerto seguro: `636`
- Inicio de cifrado: `mysecretkey!`
- Algoritmo de cifrado: `mysecretsalt`
- Inicio de instancia: `/home/myproxy` en AIX y Linux, y `/export/home/myproxy` en Solaris

```
idsicrt -I myproxy -p 389 -s 636 -e mysecretkey!\
-g mysecretsalt -l /home/myproxy -x
```

Para crear una instancia de servidor proxy con los valores siguientes en Windows, ejecute el mandato siguiente:

- Nombre de instancia: `myproxy`
- Puerto no seguro: `389`

- Puerto seguro: `636`
- Inicio de cifrado: `mysecretkey!`
- Algoritmo de cifrado: `mysecretsalt`
- Inicio de instancia: `C:`

```
idsicrt -I myproxy -p 389 -s 636 -e mysecretkey!
-g mysecretsalt -l C: -x
```

Qué hacer a continuación

Complete la configuración siguiente para crear una instancia funcional:

1. Configure una instancia de base de datos de DB2 para una instancia de servidor de directorios completa.
2. Configure el nombre distinguido y la contraseña del administrador para la instancia.
3. Configure los sufijos para la instancia.

Actualización de una instancia de una versión anterior con Herramienta de administración de instancias

Utilice Herramienta de administración de instancias para actualizar una instancia de servidor de directorios o una instancia de servidor proxy de una versión anterior a la versión 6.3.1.

Antes de empezar

Debe completar las tareas siguientes para actualizar una instancia con Herramienta de administración de instancias:

- Complete la instalación de IBM Security Directory Server, versión 6.3.1. Consulte "Inicio de la instalación" en la página 28.
- Configure el entorno antes de actualizar una instancia. Consulte "Configuración del entorno para actualizar una instancia" en la página 92.
- Inicie sesión como usuario root en el sistema operativo AIX, Linux, o Solaris, y como un miembro del grupo de administradores en el sistema operativo Windows.

Acerca de esta tarea

Tras actualizar una instancia de una versión anterior, la instancia se convierte en una instancia totalmente funcional de IBM Security Directory Server, versión 6.3.1.

Procedimiento

1. Acceda al indicador de mandatos.
2. Cambie el directorio de trabajo actual a `sbin`. La siguiente ubicación es la predeterminada en varios sistemas operativos:

   Microsoft Windows
   `C:\Program Files\IBM\ldap\V6.3.1\sbin`

   AIX y Solaris
   `/opt/IBM/ldap/V6.3.1/sbin`

   Linux `/opt/ibm/ldap/V6.3.1/sbin`
3. Para iniciar Herramienta de administración de instancias, ejecute el mandato siguiente:

Nota: En el sistema Windows, puede iniciar desde el menú **Inicio**. Pulse **Inicio** > **Todos los programas** > **IBM Security Directory Server 6.3.1** > **Herramienta de administración de instancias**.

```
idsxinst
```

4. Seleccione una versión anterior de una instancia que desea actualizar.
5. Pulse **Migrar**.
6. En la ventana **Migrar instancia de servidor de directorios**, pulse **Migrar**.
7. Cuando se muestra Herramienta de administración de instancias una vez que se complete la operación de actualización, pulse **Aceptar**.
8. Verifique la información de resumen.
9. Para cerrar la ventana **Migrar instancia de servidor de directorios**, pulse **Cerrar**.
10. Realice una copia de seguridad fuera de línea de la instancia. Para obtener más información, consulte el "Copia de seguridad de servidor de directorios" en la página 195.
11. Para cerrar Herramienta de administración de instancias, pulse **Cerrar**.

Resultados

Herramienta de administración de instancias actualiza una versión anterior de la instancia de servidor de directorios a 6.3.1.

Qué hacer a continuación

Deberá iniciar el proceso y el servidor de administración de `ibmslapd` que está asociado con la instancia de servidor de directorios. Consulte el apartado "Iniciar o detener un servidor de directorios y un servidor de administración" en la página 161.

Actualización de una instancia remota de una versión anterior con Herramienta de administración de instancias

Utilice Herramienta de administración de instancias para actualizar una instancia de servidor de directorios remota o una instancia de servidor proxy de una versión anterior a la versión 6.3.1.

Antes de empezar

Debe completar las tareas siguientes para actualizar una instancia con Herramienta de administración de instancias:

- Configure el entorno antes de actualizar una instancia. Consulte "Configuración del entorno para actualizar una instancia" en la página 92.
- Inicie sesión como usuario root en el sistema operativo AIX, Linux, o Solaris, y como un miembro del grupo de administradores en el sistema operativo Windows.

Acerca de esta tarea

Tras completar el proceso de actualización, Herramienta de administración de instancias creará una instancia de 6.3.1 en el sistema con la información de instancia remota.

Procedimiento

1. Realice una copia de seguridad de la base de datos de una instancia de servidor de directorios que se encuentra en un sistema remoto con el mandato **idsdb2ldif**.

   Importante: Si está actualizando una instancia de servidor proxy, no realice una copia de seguridad de la base de datos. El servidor proxy no contiene ninguna base de datos asociada con él.

   ```
   idsdb2ldif -I nombre_instancia -o inst_out.ldif
   ```

   Para obtener más información sobre el mandato **idsdb2ldif**, consulte la *Consulta de mandatos*.
2. Complete la instalación de IBM Security Directory Server, versión 6.3.1, en un sistema en el que desea actualizar la instancia remota. Consulte "Inicio de la instalación" en la página 28.
3. Para realizar una copia de seguridad de los esquemas y de los archivos de configuración de la instancia remota, ejecute el mandato **migbkup** de la versión 6.3.1 a la que desea actualizar:

Sistema operativo	Mandato a ejecutar:
Microsoft Windows	**migbkup.bat** drive_name\idsslapd-instance_name directorio_copia_seguridad
AIX, Linux, y Solaris	**migbkup** user_home_dir/idsslapd-instance_name directorio_copia_seguridad

   El mandato **migbkup** se encuentra en el subdirectorio `tools` del soporte de instalación de IBM Security Directory Server.
4. Copie el directorio de copia de seguridad, `directorio_copia_seguridad`, que ha creado con **migbkup**, desde el sistema remoto al sistema con IBM Security Directory Server, versión 6.3.1.
5. Opcional: Copie el archivo de copia de seguridad de la base de datos, `inst_out.ldif`, desde el sistema remoto al sistema con IBM Security Directory Server, versión 6.3.1.
6. Inicie la Herramienta de administración de instancias. Consulte el apartado "Inicio de Herramienta de administración de instancias" en la página 134.
7. Pulse **Crear una instancia**.
8. En el panel **Crear o migrar**, lleve a cabo las tareas siguientes:
   a. Pulse **Migrar desde una versión anterior del servidor de directorios**.
   b. En el campo **Especificar la vía de acceso de los archivos de los que se ha realizado copia de seguridad**, especifique la vía de acceso donde ha copiado la copia de seguridad de la configuración de la instancia remota y de los archivos de esquemas. Puede pulsar **Examinar** y especificar la ubicación de copia de seguridad.
   c. Pulse **Siguiente**.
9. En el panel **Detalles de instancia** de la ventana **Crear nueva instancia del servidor de directorios**, especifique los siguientes valores:

   Nota: Si está actualizando una instancia, no puede editar una información de usuario existente.

   a. Desde la lista **Nombre de usuario**, seleccione el nombre de usuario que debe poseer la instancia de servidor de directorios. La instancia de servidor de directorios se asigna al mismo nombre que el nombre del usuario.

b. Si desea asociar una nueva cuenta de usuario con la instancia, pulse **Crear usuario**. En la ventana **Crear usuario nuevo para la instancia de servidor de directorios**, siga estos pasos:
   1) En el campo **Nombre de usuario**, especifique el nombre de usuario.
   2) En el campo **Contraseña**, especifique una contraseña para la cuenta de usuario.
   3) En el campo **Confirmar contraseña**, especifique la contraseña para la cuenta de usuario.
   4) En el campo **Directorio de inicio**, especifique el directorio de inicio a configurar para la cuenta de usuario. Puede pulsar **Examinar** y especificar el directorio de inicio.
   5) En el campo **Grupo primario**, especifique el nombre de grupo primario del usuario.
   6) Para crear la cuenta de usuario, pulse **Crear**.

10. En el campo **Ubicación de la instancia**, especifique la ubicación de la instancia de servidor de directorios. Puede pulsar **Examinar** y especificar el directorio de inicio de la instancia. La ubicación debe contener al menos 30 MB de espacio libre en disco. En sistemas Windows, la ubicación es una unidad de disco, como por ejemplo `C:`. Los archivos de instancias de directorio se almacenan en el directorio `\idsslapd-`*`nombre_instancia`* en la unidad de disco que especifique. La variable *nombre_instancia* es el nombre de la instancia de servidor de directorios. En los sistemas AIX, Linux, y Solaris, el directorio de inicio del propietario de la instancia de servidor de directorios es la instancia predeterminada, pero puede especificar una vía de acceso distinta.
11. Opcional: En el campo **Descripción de instancias**, una descripción de la instancia de servidor de directorios. La descripción ayuda a identificar la instancia.
12. Pulse **Siguiente**.
13. Si está actualizando una instancia de servidor de directorios remota con los detalles de base de datos de DB2, pulse **Siguiente** en el panel **Detalles de la instancia de DB2**. Si los archivos de copia de seguridad son de una instancia de servidor proxy remota, es posible que no se visualice el panel **Detalles de la instancia de DB2**.
14. En el panel **Valores TCP/IP para hosts múltiples**, seleccione una de las siguientes opciones:
    - Si desea que la instancia de servidor de directorios escuche en todas las direcciones IP, seleccione **Escuchar en todas las direcciones IP configuradas**.
    - Si desea que la instancia de servidor de directorios escuche en un conjunto concreto de direcciones IP que estén configuradas en el sistema, borre **Escuchar en todas las direcciones IP configuradas**. Seleccione la dirección o direcciones IP de la lista en la que desee que escuche la instancia de servidor de directorios.
15. Pulse **Siguiente**.
16. En el panel **Valores de puerto TCP/IP**, especifique los valores siguientes:

    Nota: Debe asignar números de puerto exclusivos a los puertos de servidor de directorios y no debe entrar en conflicto con los puertos existentes que están en uso en el sistema. En los sistemas AIX, Linux, y Solaris, los números de puerto en el rango de 1 a 1000 sólo los puede utilizar root.

a. En el campo **Puerto del servidor**, especifique el número de puerto que desea que utilice el servidor como puerto no seguro. El número debe estar en el rango de 1 a 65535.
b. En el campo **Puerto seguro del servidor**, especifique el número de puerto que desea que utilice el servidor como puerto seguro. El número debe estar en el rango de 1 a 65535.
c. En el campo **Puerto del servidor de administración**, especifique el número de puerto que desea que utilice el servidor de administración como puerto no seguro. El número debe estar en el rango de 1 a 65535.
d. En el campo **Puerto seguro del servidor de administración**, especifique el número de puerto que desea que utilice el servidor de administración como puerto seguro. El número debe estar en el rango de 1 a 65535.
e. Pulse **Siguiente**.

17. En el panel **Verificar valores**, verifique el resumen que se genera.
18. Para iniciar la creación de la instancia de servidor de directorios con la configuración y los archivos de esquemas de los que se han realizado copia de seguridad, pulse **Finalizar**.
19. En la ventana **Resultados**, verifique los mensajes de registros que se generan para las operaciones de creación de instancias.
20. Para cerrar la ventana **Resultados**, pulse **Cerrar**.
21. Para cerrar Herramienta de administración de instancias, pulse **Cerrar**.

Resultados

Herramienta de administración de instancias creará una instancia de servidor de directorios en el sistema.

Qué hacer a continuación

Deberá iniciar el proceso y el servidor de administración de `ibmslapd` que está asociado con la instancia de servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración" en la página 162.

Realice una copia de seguridad de la instancia. Para obtener información sobre cómo realizar una copia de seguridad de una instancia de servidor de directorios, consulte "Copia de seguridad de servidor de directorios" en la página 195.

Creación de instancias desde una instancia existente

Puede utilizar Herramienta de administración de instancias para crear una instancia de servidor de directorios desde una instancia existente que se encuentre en un sistema local o un sistema remoto. El servidor de directorios de origen sirve como plantilla para la instancia de servidor de directorios de destino.

IBM Security Directory Server Herramienta de administración de instancias da soporte a la copia de una instancia de servidor de directorios de origen sólo si la herramienta y la instancia son de la misma versión. El servidor de directorios de destino se creará en el sistema en el que se ejecute Herramienta de administración de instancias. Si el servidor de directorios de origen se encuentra en un sistema distinto, los sistemas operativos de los dos sistemas pueden ser distintos. Por ejemplo, puede crear una instancia de servidor de directorios en un sistema Windows que sea una copia de una instancia en un sistema Linux.

Al utilizar la herramienta para copiar una instancia de origen, la herramienta puede realizar las siguientes operaciones que se basan en la entrada:

- Puede crear un servidor de directorios de destino con los mismos valores de configuración y archivos de esquemas de la instancia de servidor de directorios de origen. También sincroniza archivos de ocultación claves del directorio en el servidor de destino desde el servidor de origen.
- Si la instancia de servidor de directorios de origen es un servidor de directorios completo, la instancia de servidor de directorios de destino que se cree será también un servidor de directorios completo. Puede elegir copiar los datos desde la instancia de servidor de directorios existente. Si el servidor de directorios de origen está configurado para la copia de seguridad en línea, puede crear un servidor de directorios de destino funcional con entradas en su base de datos.
- Si la instancia de servidor de directorios de origen es un servidor proxy, la instancia de servidor de directorios de destino que se cree será también un servidor proxy.
- Si el servidor de directorios de origen es un entorno de réplica, puede configurar la instancia de destino como un servidor de réplica o como un servidor de iguales en el servidor de origen.
- Si el servidor de directorios de origen se encuentra en un entorno distribuido, puede configurar la instancia de servidor de directorios de destino como un servidor proxy.
- Si la instancia de servidor de directorios de origen está configurada para la comunicación segura, Herramienta de administración de instancias copiará los archivos de base de datos clave en el servidor de directorios de destino.

Debe asegurarse de que el servidor de directorios de origen cumple las condiciones siguientes antes de crear un servidor de directorios desde el servidor de directorios de origen:

- El servidor de directorios de origen debe ser de IBM Security Directory Server, versión 6.3.1. El servidor de directorios de origen no puede ser una instancia de versión anterior.
- El servidor de directorios de origen debe estar en ejecución en la modalidad normal. La copia de una instancia que está en ejecución en la modalidad de configuración no está soportada.
- El servidor de directorios de origen debe estar accesible desde el sistema en el que está ejecutando Herramienta de administración de instancias.
- Para crear el servidor de directorios de destino como una réplica o igual, debe existir un contexto de réplica en la instancia de servidor de directorios de origen. No puede utilizar Herramienta de administración de instancias para configurar la primera réplica o igual en una topología de réplica. La instancia de servidor de directorios de origen debe contener al menos un contexto de réplica, un grupo de réplica, y una subentrada de réplica definida. Si desea configurar la instancia como una réplica, la instancia de origen debe contener la topología de réplica inicial, incluido un acuerdo con al menos otro servidor. Si desea configurar la instancia como un igual, el servidor de origen debe estar definido como maestro para una o varias de las subentradas de la configuración de réplica.
- Si desea crear la instancia como un igual o una réplica, se creará una nueva subentrada de réplica en el DN `ibm-replicaGroup=default,`*`replicationContext`*. Si el DN no está presente, la instancia no se podrá copiar.

Si desea copiar datos desde la instancia de servidor de directorios de origen a la instancia de servidor de directorios de destino, debe cumplir los siguientes requisitos:

- La versión de DB2 puede ser distinta para ambas instancias de servidor de directorios. Se puede restaurar una copia de seguridad de base de datos en un sistema operativo en cualquier sistema que tenga el mismo tipo de sistema operativo. Por ejemplo, puede restaurar una base de datos creada en DB2 UDB versión 9 en sistemas Windows en un sistema con DB2, versión 10. En sistemas AIX, Linux, y Solaris, puede restaurar copias de seguridad que se han creado en DB2 UDB, versión 9 a DB2, versión 10 si el orden de los bytes (byte más significativo o byte menos significativo) de la copia de seguridad y de los sistemas operativos de restauración son los mismos.
- Debe configurar la instancia de servidor de directorios de origen para la copia de seguridad en línea. Puede configurar la copia de seguridad en línea durante la configuración de la base de datos inicial. Puede utilizar Herramienta de administración de instancias o Herramienta de configuración para configurar la copia de seguridad en línea.
- Debe realizar una copia de seguridad fuera de línea inicial de la instancia de servidor de directorios de origen antes de utilizar Herramienta de administración de instancias para copiar la instancia de servidor de directorios. La vía de acceso que especifique para la copia de seguridad debe contener únicamente una imagen de copia de seguridad.
- La vía de acceso con la imagen de copia de seguridad debe estar accesible para la instancia de servidor de directorios de origen y la instancia de servidor de directorios de destino.

Creación de una copia de una instancia existente con Herramienta de administración de instancias

Utilice Herramienta de administración de instancias para crear una copia de una instancia existente.

Antes de empezar

Para crear una copia de una instancia existente, debe cumplir los requisitos siguientes:

- Iniciar el proceso y el servidor de administración de `ibmslapd` de la instancia en modalidad normal.
- Asegurarse de que se puede acceder al servidor de directorios de origen desde Herramienta de administración de instancias.

Procedimiento

1. Inicie la Herramienta de administración de instancias. Consulte el apartado "Inicio de Herramienta de administración de instancias" en la página 134.
2. Elija una de las siguientes opciones para crear una copia de una instancia existente:
   - Para crear una copia de una instancia existente que se encuentre en el sistema local, pulse **Copiar instancia local**.
   - Para crear una copia de una instancia existente que se encuentra en un sistema remoto, pulse **Copiar instancia remota**.
3. En el panel **Copiar instancia de servidor de directorios**, proporcione los valores siguientes:

a. En el campo **Host**, especifique la dirección IP o el nombre de host si el servidor del directorio de origen se encuentra en un sistema remoto. Si el servidor del directorio de origen se encuentra en un sistema local, el campo se rellenará con `localhost` y no se podrá editar.

b. En el campo **Puerto**, especifique el número de puerto del servidor de directorios si el número de puerto del campo no es válido. Si desea utilizar la conexión segura, debe especificar el número de puerto seguro de la instancia de servidor de directorios de origen.

c. En el campo **Nombre distinguido del administrador**, especifique el nombre distinguido del administrador del servidor de directorios de origen si la instancia se encuentra en un sistema remoto. Si el servidor de directorios de origen se encuentra en un sistema local, el campo se rellenará con el valor nombre distinguido del administrador y no se podrá editar.

d. En el campo **Contraseña**, especifique la contraseña del nombre distinguido del administrador.

e. En el campo **Inicio de cifrado**, especifique el inicio de cifrado para la instancia de servidor de directorios de origen.

f. Si el servidor de directorios de origen está configurado para las comunicaciones seguras y desea configurar el servidor de directorios de destino con él, pulse **Utilizar conexión SSL**.

   1) En el campo **Archivo de claves**, especifique el nombre de archivo con la vía de acceso del archivo de base de datos de claves. Puede pulsar **Examinar** y especificar la ubicación.

   2) En el campo **Nombre de claves**, especifique el nombre de clave privada a utilizar desde el archivo de claves del servidor de directorios de origen.

   3) En el campo **Contraseña clave**, especifique la contraseña de base de datos clave del archivo de claves.

g. Pulse **Siguiente**.

4. En el panel **Configuración de instancias - paso 1**, siga estos pasos:

   a. Verifique los pasos **URL de origen** y **Tipo de instancia de origen** para obtener información sobre el servidor de directorios de origen. El **Tipo de instancias de origen** puede ser un servidor de directorios completo o una instancia de servidor proxy.

   b. Para configurar el servidor de directorios de destino como un igual o una réplica en una topología de réplica existente, seleccione **Configurar como servidor Igual o Réplica** y seleccione una de las siguientes opciones:

      - Para configurar el servidor de directorios de destino como una réplica, pulse **Réplica**.
      - Para configurar el servidor de directorios de destino como un igual, pulse **Igual**.

   c. En el campo **Nombre de usuario**, especifique el ID de usuario de sistema que debe ser propiedad de la instancia de servidor de directorios de destino. El nombre no puede tener más de 8 caracteres. El mismo nombre también se establece para el nombre de instancias del servidor de directorios, el ID de administrador de DB2, el nombre de la instancia de base de datos, y el nombre de la base de datos. El ID de usuario debe existir en el sistema y no debe estar asociado con ninguna otra instancia de servidor de directorios del sistema. Consulte el “Usuarios y grupos que están asociados con una instancia de servidor de directorios” en la página 123 para obtener información detallada sobre el ID de usuario.

d. En el campo **Contraseña**, especifique la contraseña para el ID de usuario.
e. En el campo **Ubicación de la instancia**, especifique la ubicación de la instancia de servidor de directorios. Puede pulsar **Examinar** y especificar el directorio de inicio de la instancia. La ubicación debe contener al menos 30 MB de espacio libre en disco. En sistemas Windows, la ubicación es una unidad de disco, como por ejemplo `C:`. Los archivos de instancias de directorio se almacenan en el directorio `\idsslapd-`*`nombre_instancia`* en la unidad de disco que especifique. La variable *nombre_instancia* es el nombre de la instancia de servidor de directorios. En los sistemas AIX, Linux, y Solaris, el directorio de inicio del propietario de la instancia de servidor de directorios es la instancia predeterminada, pero puede especificar una vía de acceso distinta.
f. Pulse **Siguiente**.

5. En el panel **Configuración de instancias - paso 2**, siga estos pasos:
   a. En el campo **Nombre distinguido del administrador**, especifique un nombre distinguido válido para la instancia de servidor de directorios de destino. El valor de nombre distinguido del administrador no distingue entre mayúsculas ni minúsculas. El usuario de nombre distinguido del administrador tiene acceso completo a todos los datos en la instancia del servidor de directorios.
   b. En el campo **Contraseña**, especifique la contraseña para el nombre distinguido del administrador. Las contraseñas son sensibles a las mayúsculas y minúsculas. Los caracteres pertenecientes al juego de caracteres de doble byte (DBCS) de la contraseña no son válidos.
   c. En el campo **Confirmar contraseña**, especifique la contraseña para el nombre distinguido del administrador. Debe recordar la contraseña para referencia futura.
   d. Para copiar datos de la base de datos del servidor de origen al servidor de destino, seleccione **Copiar datos de la instancia de origen a la nueva instancia** y siga estos pasos:

      Nota: Si ha seleccionado crear el servidor de directorios de destino como un igual o una réplica, se marcará este recuadro de selección y no podrá borrarlo.

      1) En el campo **Vía de acceso para las imágenes de copia de seguridad**, especifique el nombre de la vía de acceso de la imagen de copia de seguridad del servidor de origen. Puede pulsar **Examinar** para especificar la ubicación.Si la instancia de origen se encuentra en un sistema remoto, la vía de acceso de copia de seguridad debe ser compartida y debe estar accesible desde los sistemas de origen y de destino. Un ejemplo de vía de acceso compartida es un sistema de archivos NFS de lectura/grabación.
   e. Pulse **Siguiente**.
6. En el panel **Verificar valores**, verifique el resumen que se genera.
7. Para iniciar la creación de la copia de los servidores de directorios de origen, pulse **Finalizar**.
8. En la ventana **Resultados**, verifique los mensajes de registros que se generan para las operaciones de creación de instancias.
9. Para cerrar la ventana **Resultados**, pulse **Cerrar**.
10. Para cerrar Herramienta de administración de instancias, pulse **Cerrar**.

Resultados

Herramienta de administración de instancias creará una copia de la instancia de servidor de directorios de origen en el sistema.

Qué hacer a continuación

Deberá iniciar el proceso y el servidor de administración de `ibmslapd` que está asociado con la instancia de servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración" en la página 162.

Realice una copia de seguridad de la instancia. Para obtener información sobre cómo realizar una copia de seguridad de una instancia de servidor de directorios, consulte "Copia de seguridad de servidor de directorios" en la página 195.

Creación de una copia de una instancia existente con el programa de utilidad de línea de mandatos

Utilice el programa de utilidad de línea de mandatos, **idsideploy**, para crear una copia de una instancia.

Antes de empezar

Para crear una copia de una instancia existente, debe cumplir los requisitos siguientes:

- Inicie el proceso y el servidor de administración de `ibmslapd` de la instancia de origen en modalidad normal. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos" en la página 163.
- Asegúrese de que se pueda acceder al servidor de directorios de origen desde el sistema en el que desea crear la copia de la instancia.

Procedimiento

1. Inicie sesión como el usuario root en AIX, Linux, o Solaris, y como un miembro administrador en Windows.
2. Cambie el directorio de trabajo actual al subdirectorio `sbin` en la ubicación de instalación de IBM Security Directory Server.
3. Para crear una copia de la instancia sin los datos desde una instancia de servidor de directorios existente, ejecute el mandato siguiente:

   ```
   idsideploy -sU ldap://host:puerto -sD DNadmin_origen -sw PWDadmin_origen
   -e iniciocifrado -I nombre_instancia -a instPWD -D DNadmin
   -w PWDadmin -l ubicación_inst
   ```

   Para obtener más información sobre el mandato **idsideploy**, consulte *Consulta de mandatos*.

Iniciar o detener un servidor de directorios y un servidor de administración

Para utilizar una instancia de servidor de directorios, debe iniciar el proceso `ibmslapd` y el servidor de administración asociado con la instancia.

Si modifica la configuración de un servidor de directorios, es posible que necesite detener e iniciar el servidor y el servidor de administración para aplicar los

cambios. Puede detener el servidor de directorios y el servidor de administración sólo si se ejecuta en la modalidad normal o de configuración.

Puede utilizar Servidor de administración de instancias o programas de utilidad de servidor, como por ejemplo **ibmslapd** e **ibmdiradm**, para iniciar y detener los servidores. El proceso `ibmslapd` está asociado con el servidor de directorios. Puede iniciar la instancia de servidor de directorios sólo en modalidad normal con Herramienta de administración de instancias. Para iniciar un servidor de directorios en modalidad de sólo configuración, utilice las opciones de la línea de mandatos.

Un servidor de directorios puede estar en uno de los estados siguientes:

- Iniciado
- Detenido
- Iniciado (sólo para la configuración)

Un servidor de administración puede estar en uno de los siguientes estados:

- Iniciado
- Detenido

Inicio o detención de un servidor de directorios y un servidor de administración

Utilice Herramienta de administración de instancias para iniciar o detener el servidor de directorios, el servidor de administración, o ambos, asociados con una instancia.

Antes de empezar

Para iniciar o detener un servidor de directorios y un servidor de administración de una instancia, debe cumplir las siguientes condiciones:

1. Debe existir una instancia con la misma versión de Herramienta de administración de instancias.
2. Si no existe una instancia, créela. Consulte "Creación de la instancia de servidor de directorios predeterminada" en la página 137 o "Creación de una instancia de servidor de directorios con valores personalizados" en la página 139.

Procedimiento

1. Inicie la Herramienta de administración de instancias. Consulte el apartado "Inicio de Herramienta de administración de instancias" en la página 134.
2. Desde la lista **Lista de instancias de servidor de directorios instaladas en el sistema**, seleccione una instancia con la misma versión de Herramienta de administración de instancias.
3. Para iniciar o detener el servidor de directorios, el servidor de administración, o ambos, pulse **Iniciar/Detener**.
4. En la ventana **Gestionar estado del servidor**, realice las acciones siguientes:
   - Para iniciar el servidor de directorios, el servidor de administración, o ambos, de una instancia, complete los pasos siguientes:
     - Para iniciar el servidor de directorios, pulse **Iniciar servidor**.
     - Para iniciar el servidor de administración, pulse **Iniciar servidor de administración**.
     - Pulse **Aceptar**.

- Para detener el servidor de directorios, el servidor de administración, o ambos, complete los pasos siguientes:
  - Para detener el servidor de directorios, pulse **Detener servidor**.
  - Para detener el servidor de administración, pulse **Detener servidor de administración**.
  - Pulse **Aceptar**.

5. Para cerrar la ventana **Gestionar estado del servidor**, pulse **Cerrar**.
6. Para cerrar Herramienta de administración de instancias, pulse **Cerrar**.

Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos

Utilice los programas de utilidad de línea de mandatos para iniciar o detener el servidor de directorios, el servidor de administración, o ambos, asociados con una instancia.

Antes de empezar

Para iniciar o detener un servidor de directorios y un servidor de administración de una instancia, debe cumplir las siguientes condiciones:

- Debe existir una instancia con la misma versión de los programas de utilidad de línea de mandatos. Si no existe una instancia, créela. Consulte "Creación de la instancia de servidor de directorios predeterminada" en la página 137 o "Creación de una instancia de servidor de directorios con valores personalizados" en la página 139.

Procedimiento

1. Inicie sesión en el sistema con el permiso necesario. Consulte el apartado Capítulo 20, "Configuración de instancia", en la página 173.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al subdirectorio `sbin` en la ubicación de instalación de IBM Security Directory Server.
4. Para iniciar el servidor y el servidor de administración de una instancia, *nombre_instancia*, ejecute los mandatos siguientes: Sustituya el valor `nombre_instancia` por el nombre de la instancia.

   ```
   ibmslapd -I nombre_instancia
   ibmdiradm -I nombre_instancia
   ```

5. Para detener el servidor y el servidor de administración de una instancia, ejecute los mandatos siguientes: Sustituya el valor `nombre_instancia` por el nombre de la instancia.

   ```
   ibmslapd -I nombre_instancia -k
   ibmdiradm -I nombre_instancia -k
   ```

Gestión de la configuración de instancias del servidor de directorios

Puede utilizar Herramienta de configuración para verificar el estado, gestionar y modificar la configuración de una instancia de un servidor de directorios o de una instancia de servidor proxy.

Puede utilizar Herramienta de configuración para gestionar y modificar la configuración de una instancia de servidor de directorios o de una instancia de servidor proxy que sea de la misma versión. No puede utilizar Herramienta de

configuración que se proporciona con una versión de IBM Security Directory Server para gestionar una instancia de servidor de directorios o una instancia de servidor proxy de una versión anterior o posterior.

Puede abrir Herramienta de configuración para obtener una instancia con una de las siguientes opciones:

- Utilice Herramienta de administración de instancias.
- Ejecute el mandato **idsxcfg** con el nombre de instancia del valor del parámetro.

Para obtener más información sobre Herramienta de configuración, consulte Capítulo 20, "Configuración de instancia", en la página 173.

Apertura de Herramienta de configuración desde Herramienta de administración de instancias

Abra IBM Security Directory Server Herramienta de configuración para gestionar o modificar la configuración de una instancia de servidor de directorios o una instancia de servidor proxy.

Antes de empezar

Para gestionar una instancia con Herramienta de configuración, debe cumplir las siguientes condiciones:

- Debe existir una instancia con la misma versión de Herramienta de configuración. Si no existe una instancia, créela. Consulte "Creación de la instancia de servidor de directorios predeterminada" en la página 137 o "Creación de una instancia de servidor de directorios con valores personalizados" en la página 139.

Procedimiento

1. Inicie la Herramienta de administración de instancias. Consulte el apartado "Inicio de Herramienta de administración de instancias" en la página 134.
2. Desde la lista **Lista de instancias de servidor de directorios instaladas en el sistema**, seleccione una instancia con la misma versión de Herramienta de administración de instancias.
3. Para gestionar la instancia con Herramienta de configuración, pulse **Gestionar**. Se abrirá la ventana IBM Security Directory Server Herramienta de configuración para la instancia.
4. Para cerrar Herramienta de configuración, pulse **Archivo** > **Salir**.
5. En la ventana de confirmación Herramienta de configuración, pulse **Sí**.

Modificar los valores TCP/IP de una instancia

Puede utilizar Herramienta de administración de instancias o los programas de utilidad de línea de mandatos para modificar los valores TCP/IP de una instancia de servidor de directorios o una instancia de servidor proxy.

Para modificar los valores TCP/IP de una instancia, la versión de la instancia y Herramienta de administración de instancias deben ser la misma.

Modificación de los valores TCP/IP de una instancia con Herramienta de administración de instancias

Utilice Herramienta de administración de instancias para modificar los valores TCP/IP para una instancia existente.

Antes de empezar

Para modificar los valores TCP/IP de una instancia con Herramienta de administración de instancias, debe cumplir las siguientes condiciones:

1. Debe existir una instancia con la misma versión de Herramienta de administración de instancias.
2. Detenga el servidor de directorios y el servidor de administración de la instancia. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración" en la página 162.

Procedimiento

1. Inicie la Herramienta de administración de instancias. Consulte el apartado "Inicio de Herramienta de administración de instancias" en la página 134.
2. Desde la lista **Lista de instancias de servidor de directorios instaladas en el sistema**, seleccione una instancia con la misma versión de Herramienta de administración de instancias.
3. Para modificar los valores TCP/IP de la instancia, pulse **Editar valores TCP/IP**. Se abrirá la ventana **Editar valores TCP/IP** para la instancia.
4. En la ventana **Editar valores TCP/IP**, seleccione una de las siguientes opciones:
   - Si desea que la instancia escuche en todas las direcciones IP configuradas del sistema, seleccione **Escuchar en todas las direcciones IP configuradas**.
   - Si desea que la instancia escuche en un conjunto determinado de direcciones IP configuradas en el sistema, siga estos pasos:
     a. Borre **Escuchar en todas las direcciones IP configuradas**.
     b. Desde la lista **Seleccionar las direcciones IP específicas en las que escuchar**, seleccione la dirección o direcciones IP en la que desea que escuche la instancia.
5. Pulse **Siguiente**.
6. En el panel **Detalles de puerto**, especifique los valores siguientes:

   Nota: Debe asignar números de puerto exclusivos a los puertos de servidor de directorios y no debe entrar en conflicto con los puertos existentes que están en uso en el sistema. En los sistemas AIX, Linux, y Solaris, los números de puerto en el rango de 1 a 1000 sólo los puede utilizar root.

   a. En el campo **Puerto del servidor**, especifique el número de puerto que desea que utilice el servidor como puerto no seguro. El número debe estar en el rango de 1 a 65535.
   b. En el campo **Puerto seguro del servidor**, especifique el número de puerto que desea que utilice el servidor como puerto seguro. El número debe estar en el rango de 1 a 65535.
   c. En el campo **Puerto del servidor de administración**, especifique el número de puerto que desea que utilice el servidor de administración como puerto no seguro. El número debe estar en el rango de 1 a 65535.
   d. En el campo **Puerto seguro del servidor de administración**, especifique el número de puerto que desea que utilice el servidor de administración como puerto seguro. El número debe estar en el rango de 1 a 65535.

e. Pulse **Finalizar**.

7. En la ventana **Editar resultados TCP/IP**, verifique los mensajes de registro que se generan para la operación de edición de los valores TCP/IP.
8. Para cerrar la ventana **Editar resultados TCP/IP**, pulse **Cerrar**.
9. Para cerrar Herramienta de administración de instancias, pulse **Cerrar**.

Modificación de los valores TCP/IP de una instancia con programas de utilidad de línea de mandatos

Utilice los mandatos **idssethost** e **idssetport** para modificar TCP/IP y los valores de puerto para una instancia existente.

Antes de empezar

Para modificar los valores TCP/IP de una instancia con programas de utilidad de línea de mandatos, debe cumplir las condiciones siguientes:

1. Debe existir una instancia con la misma versión de los programas de utilidad de línea de mandatos.
2. Detenga el servidor de directorios y el servidor de administración de la instancia. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos" en la página 163.

Procedimiento

1. Inicie sesión como el usuario root en AIX, Linux, o Solaris, y como un miembro administrador en Windows.
2. Cambie el directorio de trabajo actual al subdirectorio `sbin` en la ubicación de instalación de IBM Security Directory Server.
3. Para actualizar las direcciones IP del servidor de directorios, *nombre_instancia*, elija una de las siguientes opciones: Sustituya la variable *nombre_instancia* por el nombre de la instancia.

Dirección IP para vincular	Mandato a ejecutar:
Una dirección IP específica, xx.xx.xx.xx, en el sistema	`idssethost -I nombre_instancia -i xx.xx.xx.xx`
Todas las direcciones IP configuradas en el sistema	`idssethost -I nombre_instancia -i all`

4. Para actualizar los números de puerto del servidor de directorios, *nombre_instancia*, ejecute el mandato siguiente: Sustituya la variable *nombre_instancia* por el nombre de la instancia.

   Nota: Debe asignar números de puerto exclusivos a los puertos de servidor de directorios y no debe entrar en conflicto con los puertos existentes que están en uso en el sistema. En los sistemas AIX, Linux, y Solaris, los números de puerto en el rango de 1 a 1000 sólo los puede utilizar root.

Puertos a configurar	Mandato a ejecutar:
Puerto del servidor	`idssetport -I nombre_instancia -p no_puerto`
Puerto seguro del servidor	`idssetport -I nombre_instancia -s puerto_seguro`

Puertos a configurar	Mandato a ejecutar:
Puerto del servidor de administración	`idssetport -I nombre_instancia -a puerto_adm`
Puerto seguro del servidor de administración	`idssetport -I nombre_instancia -c puerto_seguro_adm`

Para obtener más información sobre los mandatos **idssethost** e **idssetport**, consulte *Consulta de mandatos*.

5. Inicie el servidor de directorios y el servidor de administración. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos" en la página 163.

Ver información sobre una instancia

Puede utilizar Herramienta de administración de instancias o el programa de utilidad de línea de mandatos para ver detalles de la instancia, como por ejemplo el directorio de inicio de la instancia, las direcciones IP y los puertos.

Puede ver información sobre todas las instancias existentes en el sistema. El estado de la instancia puede estar en el estado detenido o iniciado.

El mandato **idsilist** también proporciona información similar para una instancia o todas las instancias disponibles en el sistema. Para obtener más información sobre el mandato **idsilist**, consulte *Consulta de mandatos*.

Visualización de información sobre una instancia con Herramienta de administración de instancias

Utilice Herramienta de administración de instancias para ver detalles de una instancia existente.

Procedimiento

1. Inicie la Herramienta de administración de instancias. Consulte el apartado "Inicio de Herramienta de administración de instancias" en la página 134.
2. Desde la lista **Lista de instancias de servidor de directorios instaladas en el sistema**, seleccione una instancia para la que desee ver detalles.
3. Pulse **Ver**. Se mostrará la ventana **Ver detalles de instancia** con detalles generales y de TCP/IP para la instancia seleccionada.
4. Para cerrar la ventana **Ver detalles de instancia**, pulse **Cerrar**.
5. Para cerrar Herramienta de administración de instancias, pulse **Cerrar**.

Visualización de información sobre una instancia con el programa de utilidad de línea de mandatos

Utilice el mandato **idsilist** para ver información sobre una instancia existente.

Procedimiento

1. Inicie sesión como el usuario root en AIX, Linux, o Solaris, y como un miembro administrador en Windows.
2. Cambie el directorio de trabajo actual al subdirectorio `sbin` en la ubicación de instalación de IBM Security Directory Server.

3. Para ver información sobre las instancias en un sistema, ejecute el mandato **idsilist** adecuado:

Tarea a completar	Mandato a ejecutar:
Listar todas las instancias	`idsilist`
Listar todas las instancias con información y descripción completa	`idsilist -a`
Listar todas las instancias con información completa básica	`idsilist -r`
Listar una instancia específica	`idsilist -I nombre_instancia`
Listar una instancia específica con información y descripción completa	`idsilist -I nombre_instancia -a`
Listar una instancia específica con información completa básica	`idsilist -I nombre_instancia -r`

Para obtener más información sobre el mandato **idsilist**, consulte *Consulta de mandatos*.

Supresión de instancias de servidor de directorios

Puede utilizar Herramienta de administración de instancias o el programa de utilidad de línea de mandatos para suprimir una instancia de servidor de directorios o una instancia de servidor proxy.

Es posible que necesite suprimir una instancia de un sistema, si ha migrado una instancia a otro sistema o ya no necesita la instancia.

Si está suprimiendo un servidor de directorios con una base de datos de DB2, es aconsejable realizar una copia de seguridad antes de suprimir la instancia. Si está suprimiendo una instancia de servidor proxy, es recomendable realizar una copia de seguridad de la instancia.

Nota: Para una instancia de servidor proxy, la supresión de la instancia es la única opción válida.

Con Herramienta de administración de instancias, puede seleccionar las opciones siguientes:

- Suprimir una instancia de servidor de directorios y conservar la instancia de base de datos
- Suprimir una instancia de servidor de directorios y eliminar la instancia de base de datos de DB2 asociada

Con el mandato **idsidrop**, puede seleccionar las siguientes opciones:

- Suprimir una instancia de servidor de directorios y conservar la instancia de base de datos
- Suprimir una instancia de servidor de directorios y eliminar la instancia de base de datos de DB2 asociada
- Desconfigurar la instancia de servidor de directorios desde la instancia de base de datos de DB2, y no suprimir la instancia de servidor de directorios

Para obtener más información sobre el mandato **idsidrop**, consulte *Consulta de mandatos*.

Supresión de una instancia con Herramienta de administración de instancias

Utilice Herramienta de administración de instancias para suprimir una instancia de servidor de directorios o una instancia de servidor proxy.

Antes de empezar

Para modificar los valores TCP/IP de una instancia con Herramienta de administración de instancias, debe cumplir las siguientes condiciones:

1. Debe existir una instancia con la misma versión de Herramienta de administración de instancias.
2. Detenga el servidor de directorios y el servidor de administración de la instancia. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración" en la página 162.

Procedimiento

1. Inicie la Herramienta de administración de instancias. Consulte el apartado "Inicio de Herramienta de administración de instancias" en la página 134.
2. Desde la lista **Lista de instancias de servidor de directorios instaladas en el sistema**, seleccione una instancia con la misma versión de Herramienta de administración de instancias.
3. Para iniciar la operación de supresión, pulse **Suprimir**.
4. En la ventana **Suprimir instancia de servidor de directorios**, siga estos pasos:
   a. Elija uno de los siguientes métodos de supresión:
      - Para eliminar la instancia de servidor de directorios sin eliminar la instancia de la base de datos de DB2 asociada, pulse **Suprimir únicamente la instancia de servidor de directorios**.

        Nota: Para una instancia de servidor proxy, **Suprimir únicamente la instancia de servidor de directorios** es la única opción válida disponible.
      - Para eliminar la instancia de servidor de directorios con la instancia de la base de datos de DB2 asociada, pulse **Suprimir la instancia de servidor de directorios y destruir la instancia de base de datos asociada**.

   b. Pulse **Suprimir**.
   c. En la ventana **Aviso**, pulse **Sí** para confirmar la supresión de la instancia.
   d. En la ventana **Información**, pulse **Aceptar**.
   e. Para cerrar la ventana **Suprimir la instancia de servidor de directorios**, pulse **Cerrar**.
   f. Para cerrar Herramienta de administración de instancias, pulse **Cerrar**.

Supresión de una instancia con el programa de utilidad de línea de mandatos

Utilice el mandato **idsidrop** para suprimir una instancia existente.

Antes de empezar

Para suprimir una instancia con el programa de utilidad de línea de mandatos, debe cumplir las condiciones siguientes:

1. Debe existir una instancia con la misma versión del programa de utilidad de línea de mandatos.

2. Detenga el servidor de directorios y el servidor de administración de la instancia. Consulte el apartado “Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos” en la página 163.

Procedimiento

1. Inicie sesión como el usuario root en AIX, Linux, o Solaris, y como un miembro administrador en Windows.
2. Cambie el directorio de trabajo actual al subdirectorio `sbin` en la ubicación de instalación de IBM Security Directory Server.
3. Para suprimir una instancia, *nombre_instancia*, elija una de las siguientes opciones: Sustituya la variable *nombre_instancia* por el nombre de la instancia.

Tarea a completar	Mandato a ejecutar:
Para suprimir una instancia de servidor de directorios y para conservar la instancia de base de datos asociada	`idsidrop -I nombre_instancia`
Para suprimir una instancia de servidor de directorios y para suprimir la instancia de base de datos asociada	`idsidrop -I nombre_instancia -r`
Para desconfigurar la instancia de base de datos asociada sin suprimir la instancia de servidor de directorios	`idsidrop -I nombre_instancia -R`

Para obtener más información sobre el mandato **idsidrop**, consulte *Consulta de mandatos*.

Capítulo 19. Verificación de la estructura de directorios

Debe comprobar la estructura de directorios tras instalar IBM Security Directory Server.

sistemas Windows de 32 bits y de 64 bits

Tras instalar IBM Security Directory Server en el sistema operativo Windows, puede ver los directorios y los archivos siguientes en la ubicación de instalación, por ejemplo: `C:\Program Files\IBM\LDAP\V6.3.1` (puede cambiar la ubicación de instalación)

appsrv
etc java
lib
messages
bin
examples
javalib
lib64
nls
var
codeset
idstools
jre
license
properties
config
include
ldapcfg.ico
logs sbin

sistemas Linux de 64 bits

Tras instalar IBM Security Directory Server en el sistema operativo Linux, puede ver los directorios y archivos siguientes en la ubicación de instalación, por ejemplo: `/opt/ibm/ldap/V6.3.1` (no puede cambiar la ubicación de instalación)

bin
codeset
config
etc examples
idstools
include
javalib
LAPID
lib
lib64
nls
properties
sbin
tmp web

Capítulo 20. Configuración de instancia

Puede utilizar Herramienta de configuración o programas de utilidad de línea de mandatos para configurar una instancia de servidor de directorios o una instancia de servidor proxy según sus necesidades.

IBM Security Directory Server Herramienta de configuración (**idsxcfg**) es una interfaz gráfica de usuario (GUI) que puede utilizar para configurar una instancia. Para utilizar Herramienta de configuración, es necesario IBM Java Development Kit.

Para iniciar Herramienta de configuración, debe iniciar sesión con las siguientes credenciales:

AIX, Linux, o Solaris

- Usuario root
- Propietario de la instancia de servidor de directorios
- ID de usuario que esté en el grupo primario del propietario de la instancia de servidor de directorios

Windows

- ID de usuario que esté en el grupo de administradores predeterminados

También puede utilizar Herramienta de configuración para cambiar la configuración del servidor de directorios existente.

Puede utilizar Herramienta de configuración para las siguientes tareas en una instancia de servidor de directorios completa:

- Iniciar o detener el servidor
- Gestionar la contraseña y el nombre distinguido del administrador primario
- Configurar y desconfigurar la base de datos de DB2 para una instancia de servidor de directorios
- Optimizar la base de datos asociada con una instancia
- Mantener la base de datos de DB2 con la organización del índice de DB2 o con la compresión de fila de DB2
- Hacer copia de seguridad y restaurar la base de datos
- Ajustar el rendimiento de instancias de servidor de directorios
- Habilitar e inhabilitar el registro de cambios
- Añadir o eliminar sufijos
- Añadir o eliminar archivos de esquemas
- Importar o exportar datos de LDIF
- Configurar la sincronización de Active Directory

Puede utilizar Herramienta de configuración para las siguientes tareas en una instancia de servidor proxy:

- Iniciar o detener el servidor
- Gestionar la contraseña y el nombre distinguido del administrador primario
- Añadir o eliminar sufijos
- Añadir o eliminar archivos de esquemas

- Hacer copia de seguridad y restaurar la instancia

Inicio de Herramienta de configuración

Inicie IBM Security Directory Server Herramienta de configuración para una instancia para configurar la instancia según los requisitos del entorno del directorio.

Antes de empezar

Para gestionar una instancia con Herramienta de configuración, debe cumplir las siguientes condiciones:

- Debe existir una instancia con la misma versión de Herramienta de configuración. Si no existe una instancia, créela. Consulte "Creación de una instancia de servidor de directorios con valores personalizados" en la página 139 o "Creación de una instancia de servidor proxy con valores personalizados" en la página 147.
- Debe existir IBM Java Development Kit en la vía de acceso de instalación de IBM Security Directory Server. Para la vía de acceso de instalación predeterminada de IBM Security Directory Server, consulte "Ubicaciones de la instalación predeterminada" en la página 27.

Procedimiento

1. Inicie sesión en el sistema con los permisos necesarios. Consulte el apartado Capítulo 20, "Configuración de instancia", en la página 173.
2. Abra el indicador de mandatos.
3. Cambie el directorio actual al subdirectorio `sbin` en la ubicación de instalación de IBM Security Directory Server.
4. Ejecute el mandato **idsxcfg** en el formato siguiente: Sustituya la variable *nombre_instancia* por el nombre de la instancia.

   ```
   idsxcfg -I nombre_instancia
   ```

   Se abrirá la ventana IBM Security Directory Server Herramienta de configuración para la instancia especificada.
5. Para cerrar la ventana Herramienta de configuración, pulse **Archivo** > **Salir**.
6. En la ventana de confirmación Herramienta de configuración, pulse **Sí**.

Iniciar o detener un servidor de directorios y un servidor de administración con Herramienta de configuración

Puede utilizar Herramienta de configuración para iniciar el proceso `ibmslapd` y el servidor de administración asociado con una instancia.

Si modifica la configuración de un servidor de directorios, es posible que necesite detener e iniciar el servidor y el servidor de administración para aplicar los cambios. Puede detener el servidor de directorios y el servidor de administración sólo si se ejecuta en la modalidad normal o de configuración.

Puede utilizar Herramienta de configuración o programas de utilidad del servidor, como por ejemplo **ibmslapd** e **ibmdiradm**, para iniciar y detener el servidor y el servidor de administración. El proceso `ibmslapd` está asociado con el servidor de directorios. Puede iniciar la instancia de servidor de directorios sólo en modalidad

normal con Herramienta de configuración. Para iniciar un servidor de directorios en modalidad de sólo configuración, utilice las opciones de la línea de mandatos.

Un servidor de directorios puede estar en uno de los estados siguientes:

- Iniciado
- Detenido
- Iniciado (sólo para la configuración)

Un servidor de administración puede estar en uno de los siguientes estados:

- Iniciado
- Detenido

Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración

Utilice Herramienta de configuración para iniciar o detener el servidor de directorios, el servidor de administración, o ambos, que están asociados con una instancia.

Procedimiento

1. Inicie Herramienta de configuración para una instancia. Consulte el apartado "Inicio de Herramienta de configuración" en la página 174.
2. Desde la lista de tareas del panel de navegación de la izquierda, pulse **Gestionar estado del servidor**.
3. En la página **Estado actual**, verifique el estado actual del servidor y del servidor de administración.
4. En la página **Estado actual**, realice las siguientes acciones:
   - Para iniciar el servidor de directorios, el servidor de administración, o ambos, de una instancia, complete los pasos siguientes:
     - Para iniciar el servidor de directorios, pulse **Iniciar servidor**.
     - Para iniciar el servidor de administración, pulse **Iniciar servidor de administración**.
     - En la ventana **Información**, pulse **Aceptar**.
   - Para detener el servidor de directorios, el servidor de administración, o ambos, complete los pasos siguientes:
     - Para detener el servidor de directorios, pulse **Detener servidor**.
     - Para detener el servidor de administración, pulse **Detener servidor de administración**.
     - En la ventana **Información**, pulse **Aceptar**.
5. Para cerrar la página **Estado actual**, pulse **Cerrar**.
6. Para cerrar la ventana Herramienta de configuración, pulse **Archivo** > **Salir**.
7. En la ventana de confirmación Herramienta de configuración, pulse **Sí**.

Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos

Utilice los programas de utilidad de línea de mandatos para iniciar o detener el servidor de directorios, el servidor de administración, o ambos, asociados con una instancia.

Antes de empezar

Para iniciar o detener un servidor de directorios y un servidor de administración de una instancia, debe cumplir las siguientes condiciones:

- Debe existir una instancia con la misma versión de los programas de utilidad de línea de mandatos. Si no existe una instancia, créela. Consulte "Creación de la instancia de servidor de directorios predeterminada" en la página 137 o "Creación de una instancia de servidor de directorios con valores personalizados" en la página 139.

Procedimiento

1. Inicie sesión en el sistema con el permiso necesario. Consulte el apartado Capítulo 20, "Configuración de instancia", en la página 173.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al subdirectorio `sbin` en la ubicación de instalación de IBM Security Directory Server.
4. Para iniciar el servidor y el servidor de administración de una instancia, *nombre_instancia*, ejecute los mandatos siguientes: Sustituya el valor `nombre_instancia` por el nombre de la instancia.

   ```
   ibmslapd -I nombre_instancia
   ibmdiradm -I nombre_instancia
   ```

5. Para detener el servidor y el servidor de administración de una instancia, ejecute los mandatos siguientes: Sustituya el valor `nombre_instancia` por el nombre de la instancia.

   ```
   ibmslapd -I nombre_instancia -k
   ibmdiradm -I nombre_instancia -k
   ```

Gestión del nombre distinguido del administrador primario para una instancia

Para acceder a la configuración y a todos los datos de directorios de una instancia, debe crear y configurar un nombre distinguido (DN) del administrador primario para una instancia.

El nombre distinguido del administrador es el nombre distinguido utilizado por el administrador primario de una instancia. Sólo puede crear un administrador primario para una instancia.

El nombre distinguido predeterminado es `cn=root`. El valor de nombre distinguido no distingue entre mayúsculas ni minúsculas.

Un nombre distinguido contiene pares `attribute:value`, que están separados por comas. Aparece un ejemplo de un valor de DN.

```
cn=Ben Gray,ou=dept_audit,o=sample
```

Puede utilizar Herramienta de configuración o el programa de utilidad de línea de mandatos, **idsdnpw**, para establecer o cambiar el nombre distinguido del administrador primario. Para establecer o cambiar el nombre distinguido del administrador primario, debe detener el proceso `ibmslapd` asociado con la instancia.

Gestión del nombre distinguido del administrador primario con Herramienta de configuración

Utilice Herramienta de configuración para configurar el nombre distinguido del administrador primario para una instancia.

Antes de empezar

Para configurar el nombre distinguido del administrador primario para una instancia, debe completar los requisitos siguientes:

- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Procedimiento

1. Inicie Herramienta de configuración para una instancia. Consulte el apartado "Inicio de Herramienta de configuración" en la página 174.
2. Desde la lista de tareas del panel de navegación izquierdo, pulse **Gestionar el nombre distinguido del administrador**.
3. En el campo **Nombre distinguido del administrador**, especifique el nombre distinguido para el administrador primario o acepte el nombre distinguido predeterminado, `cn=root`.
4. Pulse **Aceptar**.
5. Para confirmar la acción, pulse **Aceptar**.
6. Para cerrar la ventana Herramienta de configuración, pulse **Archivo** > **Salir**.
7. Para confirmar la acción, pulse **Sí**.

Qué hacer a continuación

Inicie el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Gestión del nombre distinguido del administrador primario con el programa de utilidad de línea de mandatos

Utilice el programa de utilidad de línea de mandatos, **idsdnpw**, para gestionar el nombre distinguido del administrador primario para una instancia.

Antes de empezar

Para configurar el nombre distinguido del administrador primario para una instancia, debe completar los requisitos siguientes:

- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos" en la página 163.

Acerca de esta tarea

Si no especifica el valor de nombre distinguido del administrador, el valor predeterminado, `cn=root`, se establecerá en el archivo `ibmslapd.conf` para la instancia de servidor de directorios. Debe especificar la contraseña del administrador primario para una instancia.

Si no especifica la contraseña, el mandato **idsdnpw** le indicará la contraseña. La contraseña no se mostrará en el indicador de mandatos cuando la escriba.

Procedimiento

1. Inicie la sesión como propietario de la instancia de servidor de directorios.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al subdirectorio `sbin` en la ubicación de instalación de IBM Security Directory Server.
4. Para establecer el nombre distinguido del administrador para una instancia, ejecute el mandato siguiente: Sustituya los valores `nombre_instancia`, `DNadmin`, y `PWDadmin` según sus requisitos.

   ```
   idsdnpw -I nombre_instancia -u DNadmin -p PWDadmin
   ```

   Para obtener más información sobre el mandato **idsdnpw**, consulte *Consulta de mandatos*.

Qué hacer a continuación

Inicie el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos" en la página 163.

Gestión de la contraseña del administrador primario para una instancia

Para autenticarse en una instancia y acceder a la configuración y a todos los datos del directorio, debe crear y configurar una contraseña del administrador primario para una instancia.

La contraseña del administrador distingue entre mayúsculas y minúsculas. No debe utilizar los caracteres pertenecientes al juego de caracteres de doble byte (DBCS) en la contraseña, ya que no están soportados. Debe guardar la contraseña del administrador para referencia futura.

Puede utilizar Herramienta de configuración o el programa de utilidad de línea de mandatos, **idsdnpw**, para configurar la contraseña del administrador primario. Para configurar la contraseña del administrador, debe detener el proceso `ibmslapd` asociado con la instancia.

Si habilita la política de contraseñas de administración, la contraseña del administrador primario debe cumplir los requisitos de la política de contraseñas de administración. Para obtener más información acerca de la política de contraseñas, consulte la sección *Administración* en la documentación de IBM Security Directory Server.

Gestión de la contraseña del administrador primario con Herramienta de configuración

Utilice Herramienta de configuración para configurar la contraseña para el administrador primario de una instancia.

Antes de empezar

Para configurar la contraseña para el nombre distinguido del administrador primario de una instancia, debe completar los requisitos siguientes:

- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Procedimiento

1. Inicie Herramienta de configuración para una instancia. Consulte el apartado "Inicio de Herramienta de configuración" en la página 174.
2. Desde la lista de tareas del panel de navegación izquierdo, pulse **Gestionar contraseña del administrador**.
3. En el campo **Contraseña del administrador**, especifique la contraseña para el administrador primario.
4. En el campo **Confirmar contraseña**, especifique la contraseña para el administrador primario.
5. Pulse **Aceptar**.
6. Para confirmar la acción, pulse **Aceptar**.
7. Para cerrar la página **Gestionar la contraseña del administrador**, pulse **Aceptar**.
8. Para cerrar la ventana Herramienta de configuración, pulse **Archivo** > **Salir**.
9. Para confirmar la acción, pulse **Sí**.

Qué hacer a continuación

Inicie el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Gestión de la contraseña del administrador primario con el programa de utilidad de línea de mandatos

Utilice el programa de utilidad de línea de mandatos, **idsdnpw**, para gestionar la contraseña del administrador primario para una instancia.

Antes de empezar

Para configurar la contraseña del administrador primario para una instancia, debe completar los requisitos siguientes:

- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos" en la página 163.

Procedimiento

1. Inicie la sesión como propietario de la instancia de servidor de directorios.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al subdirectorio `sbin` en la ubicación de instalación de IBM Security Directory Server.
4. Para configurar la contraseña del administrador para una instancia, ejecute el mandato siguiente: Sustituya los valores `nombre_instancia`, `DNadmin`, y `PWDadmin` según sus requisitos.

```
idsdnpw -I nombre_instancia -u DNadmin -p PWDadmin
```

Para obtener más información sobre el mandato **idsdnpw**, consulte *Consulta de mandatos*.

Qué hacer a continuación

Inicie el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos" en la página 163.

Configuración de base de datos para una instancia de servidor de directorios

Para utilizar una instancia como un servidor de directorios y almacenar datos de directorio, debe configurar una base de datos de DB2 para la instancia.

Puede utilizar Herramienta de administración de instancias, Herramienta de configuración, o el mandato **idscfgdb**, para crear y configurar una base de datos de DB2. Debe detener el servidor de directorios antes de configurar o desconfigurar la base de datos. Para obtener más información sobre el mandato **idscfgdb**, consulte *Consulta de mandatos*.

Si decide crear la instancia predeterminada con Herramienta de administración de instancias, la instancia de base de datos de DB2 también se creará y configurará para la instancia. Para una instancia de servidor proxy, no necesita configurar una base de datos de DB2.

Al configurar una base de datos de DB2 para una instancia, se actualizará el archivo de configuración de la instancia con la información de base de datos de DB2. La herramienta también crea los valores de bucle de retorno local y de base de datos.

Se crean los valores de la base de datos y el bucle de retorno local, si éstos no existen. Puede especificar si desea crear la base de datos como una base de datos de página de código local o como una base de datos de UTF-8. La página de código predeterminado que se utiliza para la creación de la base de datos de DB2 es UTF-8.

Configuración de una base de datos para una instancia con Herramienta de configuración

Utilice Herramienta de configuración para configurar una base de datos de DB2 para una instancia de servidor de directorios.

Antes de empezar

Para configurar una base de datos de DB2 para una instancia de servidor de directorios, debe finalizar las tareas siguientes:

- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.
- Debe existir un ID de usuario de sistema como propietario de la instancia de base de datos de DB2. Para obtener más información sobre los requisitos del ID

de usuario de sistema, consulte “Usuarios y grupos que están asociados con una instancia de servidor de directorios” en la página 123.

Procedimiento

1. Inicie Herramienta de configuración para una instancia. Consulte el apartado “Inicio de Herramienta de configuración” en la página 174.
2. Desde la lista de tareas del panel de navegación de la izquierda, pulse **Tareas de base de datos** > **Configurar base de datos**.
3. En la página **Configurar base de datos**, seleccione una de las siguientes opciones:
   - Para configurar una base de datos para una instancia, siga estos pasos:
     a. En el campo **Nombre de usuario de base de datos**, especifique el ID de usuario de sistema que debe ser propietario de la base de datos. La instancia de servidor de directorios utiliza este ID de usuario de sistema para conectarse a la base de datos.
     b. En el campo **Contraseña**, especifique la contraseña para el administrador de bases de datos.
     c. En el campo **Nombre de la base de datos**, especifique el nombre de la base de datos.
     d. Si desea establecer cualquiera de los siguientes valores de configuración de DB2, seleccione **Mostrar opciones avanzadas de espacio de tabla**.
        – Desea que la base de datos utilice el almacenamiento de datos de SMS (System Managed Storage) para los espacios de tablas de DB2. Cuando se utiliza SMS, el gestor del sistema de archivos del sistema operativo asigna y gestiona el espacio de tablas donde se almacenan las tablas de DB2.
        – Desea que la base de datos utilice el almacenamiento de datos de DMS (Database Managed Storage) para los espacios de tablas de DB2. Además, desea configurar la base de datos para los espacios de tablas, el tamaño y la ubicación de `USERSPACE1` y `LDAPSPACE`. Cuando se utiliza DMS, los espacios de tablas los gestiona el gestor de bases de datos. El administrador de bases de datos decide qué dispositivos y archivos va a utilizar y DB2 gestiona el espacio en dichos dispositivos y archivos.

        Si no selecciona **Mostrar opciones avanzadas de espacio de tabla**, se creará una base de datos de DB2 con los espacios de tablas de `USERSPACE1` y `LDAPSPACE` utilizando DMS con tamaños y ubicaciones predeterminados. Si configura una instancia con una base de datos existente, se inhabilitará **Mostrar opciones avanzadas de espacio de tablas** al especificar el nombre de una base de datos existente en el campo **Nombre de base de datos**.
     e. Pulse **Siguiente**.
   - Para configurar la contraseña del administrador de bases de datos de nuevo, siga estos pasos:
     a. Pulse **Restablecer contraseña**.
     b. En el campo **Contraseña**, especifique la contraseña para el administrador de bases de datos.
     c. En el campo **Confirmar contraseña**, especifique la contraseña para el administrador de bases de datos.
     d. Pulse **Siguiente**.
4. Si crea y configura una base de datos de DB2, siga estos pasos:

a. En el campo **Ubicación de instalación de base de datos**, especifique la vía de acceso de ubicación de la base de datos. Puede pulsar **Examinar** para especificar un directorio. En Windows, debe proporcionar una ubicación de unidad de disco, como por ejemplo `C:`. En AIX, Linux, y Solaris, la ubicación debe ser un nombre de directorio, como por ejemplo `/home/ldapdb`.

   Nota: El espacio de disco mínimo necesario para una base de datos de DMS es 1 GB. Para una base de datos de SMS, es necesario un mínimo de 150 MB de espacio de disco. Estos requisitos son para una base de datos vacía. Si almacena datos en la base de datos, necesitará más espacio de disco.

b. Para configurar el servidor de directorios con la base de datos para la copia de seguridad en línea, siga estos pasos:
   1) Seleccione **Configurar para la copia de seguridad en línea**.
   2) En el campo **Ubicación de copia de seguridad de base de datos**, especifique la ubicación donde desea almacenar la imagen de copia de seguridad. Puede pulsar **Examinar** para especificar la ubicación.

   Nota: No salga de la Herramienta de configuración ni cancele la operación cuando se esté ejecutando la operación de copia de seguridad.
   Al configurar la base de datos para la copia de seguridad en línea una vez que haya finalizado la configuración de la base de datos, se ejecutará una copia de seguridad inicial y fuera de línea de la base de datos. Una vez que haya finalizado la operación de copia de seguridad fuera de línea, se reiniciará el servidor de administración. También puede configurar la copia de seguridad en línea para una instancia de servidor de directorios con el mandato **idscfgdb**. Sin embargo, no puede desconfigurar la copia de seguridad en línea con el mandato **idscfgdb** ni el parámetro **-c**. Si configura la copia de seguridad en línea para una instancia con Herramienta de administración de instancias o Herramienta de configuración, puede desconfigurarla con Herramienta de configuración o con el mandato **idscfgdb**.

c. En el área **Opción de juego de caracteres**, elija una de las siguientes opciones para crear un tipo de base de datos:

   Nota: Cree una base de datos universal de DB2 si tiene previsto almacenar datos en varios idiomas en el servidor de directorios. Una Base de datos universal de DB2 también es más eficaz porque requiere menor conversión de datos. Si desea utilizar códigos de idioma, la base de datos debe ser UTF-8. Para obtener más información sobre UTF-8, consulte el "Soporte de UTF-8" en la página 128.
   - Para crear una base de datos de UTF-8 (UCS Transformation Format) en la que los clientes de LDAP pueden almacenar datos de caracteres UTF-8, pulse **Crear una base de datos universal de DB2**.
   - Para crear una base de datos en la página de códigos local, pulse **Crear una base de datos de DB2 de página de códigos local**.

d. Pulse **Siguiente**.

5. Si ha seleccionado **Mostrar opciones avanzadas del espacio de tablas**, debe seguir estos pasos:
   a. En la lista **Seleccionar tipo de espacio de tabla de base de datos**, seleccione un tipo de base de datos. El tipo de espacio de tablas de la base de datos de DMS es el predeterminado. Si selecciona el tipo de espacio de tablas de base de datos de SMS, se inhabilitarán el resto de los campos. El

soporte del espacio de tablas de DMS sólo se utilizará para los espacios de tablas de USERSPACE1 y LDAPSPACE. El resto de los espacios de tablas, como por ejemplo espacios de tabla de catálogo y temporales, son del tipo SMS.

a. En el área **Detalles del espacio de tablas de USERSPACE1**, especifique los detalles siguientes:
   1) En la lista **Contenedor del espacio de tablas**, seleccione el tipo de contenedor. Si desea la ubicación del espacio de tablas de USERSPACE1 en el sistema de archivos, seleccione **Archivo**. Si la ubicación del contenedor del espacio de tablas de la base de datos se encuentra en un sistema de archivos, se creará un espacio de tablas cooked de DMS. Puede especificar el tamaño inicial para el espacio de tablas y un tamaño de unidad extensible, y el espacio de tablas se expandirá automáticamente cuando sea necesario. Si desea crear el espacio de tablas de USERSPACE1 en un dispositivo sin formato, seleccione **Dispositivo sin formato**. Un dispositivo sin formato es un dispositivo donde no hay instalado ningún sistema de archivos, como por ejemplo un disco duro que no contiene un sistema de archivos. Si la ubicación del contenedor del espacio de tablas de la base de datos se encuentra en un dispositivo sin formato, se creará un espacio de tablas raw de DMS. En este caso, el tamaño del contenedor del espacio de tablas de la base de datos es fijo y no se puede ampliar. Si selecciona **Dispositivo sin formato**, especifique el tamaño junto con la ubicación del contenedor en lugar de aceptar los valores predeterminados.
   2) Si ha seleccionado **Archivo** en la lista **Contenedor del espacio de tablas**, especifique los detalles siguientes:
      a) En el campo **Vía de acceso de directorio**, especifique la vía de acceso del directorio en la que desea crear el espacio de tablas de USERSPACE1. Puede pulsar **Examinar** para seleccionar el directorio.
      b) En el campo **Nombre de archivo**, especifique el nombre de archivo del espacio de tablas que desee crear, o acepte el nombre de archivo predeterminado, USPACE.
      c) En el campo **Tamaño inicial**, especifique el tamaño inicial para el espacio de tablas de USERSPACE1 en páginas o acepte el valor predeterminado. Para el contenedor del espacio de tablas del tipo **Archivo**, el contenedor del espacio de tablas de USERSPACE1 es del tipo autoincremental. Puede proporcionar el tamaño inicial en el campo **Tamaño inicial**, y un tamaño de unidad extensible en el campo **Tamaño extensible**. El valor predeterminado para el tamaño inicial es 16.000 páginas, y el tamaño de unidad extensible predeterminado es 8.000 páginas. El tamaño de página para el contenedor del espacio de tablas de USERSPACE1 es de 4 KB por página.
   3) Si ha seleccionado **Dispositivo sin formato** en la lista **Contenedor del espacio de tablas**, especifique los detalles siguientes:
      a) En el campo **Vía de acceso del dispositivo**, especifique la ubicación del dispositivo sin formato. En Windows, la vía de acceso debe comenzar por \\.\. Un ejemplo que muestra la vía de acceso con el nombre del dispositivo, \\.*nombre_dispositivo*. En AIX, Linux, y Solaris, la vía de acceso del dispositivo debe ser una vía de acceso válida.
      b) En el campo **Tamaño inicial**, especifique el tamaño inicial para el espacio de tablas de USERSPACE1 o acepte el valor predeterminado. Para el contenedor del espacio de tablas de tipo **Dispositivo sin formato**, el tamaño del contenedor del espacio de tablas de

USERSPACE1 es fijo. El tamaño predeterminado es de 16.000 páginas. Para obtener mejores resultados, especifique el tamaño que desee.

b. En el área **Detalles del espacio de tablas de LDAPSPACE**, especifique los detalles siguientes:

   1) En la lista **Contenedor del espacio de tablas**, seleccione el tipo de contenedor. Si desea la ubicación del espacio de tablas de LDAPSPACE en un sistema de archivos, seleccione **Archivo**. Si desea crear el espacio de tablas de LDAPSPACE en un dispositivo sin formato, seleccione **Dispositivo sin formato**. Un dispositivo sin formato es un dispositivo donde no hay instalado ningún sistema de archivos, como por ejemplo un disco duro que no contiene un sistema de archivos.

   2) Si ha seleccionado **Archivo** en la lista **Contenedor del espacio de tablas**, especifique los detalles siguientes:

      a) En el campo **Vía de acceso de directorio**, especifique la vía de acceso del directorio donde desee crear el espacio de tablas de LDAPSPACE. Puede pulsar **Examinar** para seleccionar el directorio.

      b) En el campo **Nombre de archivo**, especifique el nombre del archivo del espacio de tablas que desee crear, o acepte el nombre de archivo predeterminado, ldapspace.

      c) En el campo **Tamaño inicial**, especifique el tamaño inicial para el espacio de tablas de LDAPSPACE en páginas o acepte el valor predeterminado. Para el contenedor del espacio de tablas del tipo **Archivo**, el contenedor del espacio de tablas de LDAPSPACE es de tipo autoincremental. Puede proporcionar el tamaño inicial en el campo **Tamaño inicial**, y un tamaño de unidad extensible en el campo **Tamaño extensible**. El valor predeterminado para el tamaño inicial es 16.000 páginas, y el tamaño de unidad extensible predeterminado es 8.000 páginas. El tamaño de página para el contenedor del espacio de tablas de LDAPSPACE es de 32 KB por página.

   3) Si ha seleccionado **Dispositivo sin formato** en la lista **Contenedor del espacio de tablas**, especifique los detalles siguientes:

      a) En el campo **Vía de acceso del dispositivo**, especifique la ubicación del dispositivo sin formato. En Windows, la vía de acceso debe comenzar por \\.\. Un ejemplo que muestra la vía de acceso con el nombre del dispositivo, \\.*nombre_dispositivo*. En AIX, Linux, y Solaris, la vía de acceso del dispositivo debe ser una vía de acceso válida.

      b) En el campo **Tamaño inicial**, especifique el tamaño inicial para el espacio de tablas de LDAPSPACE o acepte el valor predeterminado. Para el contenedor del espacio de tablas del tipo **Dispositivo sin formato**, el tamaño del contenedor del espacio de tablas de LDAPSPACE es fijo. El tamaño predeterminado es de 16.000 páginas. Para obtener mejores resultados, especifique el tamaño que desee.

c. Si ha seleccionado **Archivo** en uno o ambos de los campos **Contenedor del espacio de tablas**, especifique el número de páginas por el que se deben ampliar los contenedores de espacios de tablas en el campo **Tamaño expansible**.

6. Pulse **Finalizar**.
7. Para aceptar la finalización de la tarea, pulse **Aceptar**.
8. Verifique los registros que se generan para la operación de configuración de la base de datos.

9. Para cerrar la página **Configurar base de datos**, pulse **Cerrar**.
10. Para cerrar la ventana Herramienta de configuración, pulse **Archivo** > **Salir**.
11. Para confirmar la acción, pulse **Sí**.

Qué hacer a continuación

Tras configurar una base de datos, debe finalizar las siguientes configuraciones para una instancia:

- Configurar el nombre distinguido y la contraseña del administrador primario. Consulte "Gestión del nombre distinguido del administrador primario con Herramienta de configuración" en la página 177 y "Gestión de la contraseña del administrador primario con Herramienta de configuración" en la página 178.
- Configurar los sufijos necesarios. Consulte el apartado "Configuración de sufijos" en la página 210.

Configuración de una base de datos para una instancia con el programa de utilidad de la línea de mandatos

Utilice el programa de utilidad de línea de mandatos, **idscfgdb**, para configurar una base de datos de DB2 para una instancia de servidor de directorios.

Antes de empezar

Para configurar una base de datos de DB2 para una instancia de servidor de directorios, debe finalizar las tareas siguientes:

- No establezca la variable de entorno *DB2COMM* al configurar una base de datos.
- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos" en la página 163.
- Debe existir un ID de usuario de sistema como propietario de la instancia de base de datos de DB2. Para obtener más información sobre los requisitos del ID de usuario de sistema, consulte "Usuarios y grupos que están asociados con una instancia de servidor de directorios" en la página 123.

Acerca de esta tarea

Puede ejecutar el mandato **idscfgdb** para completar las operaciones siguientes:

- Crea y configura la base de datos para una instancia de servidor de directorios. Crea los valores de bucle de retorno local, si no existen.
- Añade información sobre la base de datos al archivo `ibmslapd.conf` de la instancia de servidor de directorios

Puede especificar si desea crear la base de datos como una base de datos de página de códigos local o como una base de datos de UTF-8, que es la predeterminada.

Procedimiento

1. Inicie la sesión como propietario de la instancia de servidor de directorios.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al subdirectorio `sbin` en la ubicación de instalación de IBM Security Directory Server.
4. Para configurar una base de datos de DB2 en una instancia de servidor de directorios con los valores siguientes, ejecute el mandato siguiente:

- Nombre de instancia: `ldapdb`
- Nombre de base de datos: `ldapdb`
- ID de administrador de bases de datos de DB2: `ldapdb`
- Contraseña del administrador de bases de datos de DB2: `ldapdb123`
- Ubicación de la base de datos: `/home/ldapdb`

```
idscfgdb -I ldapdb -a ldapdb -w ldapdb123 -t ldapdb
-l /home/ldapdb
```

En Windows, especifique el nombre de unidad de disco para la ubicación de la base de datos. En Solaris, especifique una ubicación de base de datos adecuada. Para obtener más información sobre el mandato **idscfgdb**, consulte *Consulta de mandatos*. El mandato configura una base de datos con espacios de tablas de DMS con tamaños predeterminados.

Ejemplos

Ejemplo 1:

Para configurar una base de datos con un espacio de tablas DMS en un sistema de archivos y con un tamaño específico para el espacio de tablas, ejecute el mandato **idscfgdb** con los valores siguientes:

- Nombre de instancia: `ldapdb`
- Nombre de base de datos: `ldapdb`
- ID de administrador de bases de datos de DB2: `dbadmin`
- Contraseña del administrador de bases de datos de DB2: `ldapdb123`
- Ubicación de base de datos: `c:\dblocation`
- Ubicación del espacio de tablas `USERSPACE1`: `c:\dblocation\ldapinst\tablespaceloc\USPACE`
- Tamaño del contenedor de los espacios de tablas `USERSPACE1`: 10000 páginas
- Tamaño de extensión: 16 páginas

```
idscfgdb -I ldapdb -a dbadmin -t ldapdb
-w ldapdb123 -n -l c:\dblocation
-u c:\dblocation\ldapinst\tablespaceloc\USPACE -U 10000 -z 16
```

Ejemplo 2:

Para configurar la misma base de datos con espacios de tablas de SMS, ejecute el mandato **idscfgdb** con los valores siguientes:

- Nombre de instancia: `ldapdb`
- Nombre de base de datos: `ldapdb`
- ID de administrador de bases de datos de DB2: `dbadmin`
- Contraseña del administrador de bases de datos de DB2: `ldapdb123`
- Ubicación de base de datos: `c:\dblocation`

```
idscfgdb -I ldapdb -a dbadmin -t ldapdb
-w ldapdb123 -n -l c:\dblocation
-m SMS
```

Qué hacer a continuación

Tras configurar una base de datos, debe finalizar las siguientes configuraciones para una instancia:

- Configurar el nombre distinguido y la contraseña del administrador primario. Consulte "Gestión del nombre distinguido del administrador primario con el

programa de utilidad de línea de mandatos" en la página 177 y "Gestión de la contraseña del administrador primario con el programa de utilidad de línea de mandatos" en la página 179.

- Configurar los sufijos necesarios. Consulte el apartado "Configuración de sufijos" en la página 210.

Gestión de la contraseña del administrador de bases de datos de DB2

Si cambia la contraseña del sistema para el propietario de instancias de DB2, debe actualizar el archivo de configuración de instancias de servidor de directorios con la contraseña.

Al cambiar la contraseña del sistema para el propietario de la instancia de DB2 de una base de datos configurada con una instancia, la contraseña no se actualizará en el archivo de configuración de instancias. Si la contraseña del administrador de bases de datos del archivo de configuración de una instancia no coincide con la contraseña del sistema del propietario de la instancia de DB2 asociada con la base de datos, es posible que la instancia no se inicie en la modalidad normal. Debe actualizar el archivo de configuración de instancias con la contraseña más reciente del propietario de instancias de DB2.

Puede utilizar Herramienta de configuración, el mandato **idscfgdb**, o el mandato **idsldapmodify** para actualizar la contraseña del administrador de bases de datos de DB2.

Al utilizar Herramienta de configuración o el mandato **idscfgdb** para cambiar la contraseña del administrador de bases de datos, debe detener el servidor de directorios antes de cambiar la contraseña. Para cambiar la contraseña del administrador de bases de datos con el mandato **idsldapmodify**, debe iniciar el servidor de directorios en modalidad de configuración. Ejecute el mandato **idsldapmodify** con el administrador de servidor de directorios primario o como un miembro del grupo de administradores local con el rol `dirdata`.

Para obtener más información sobre los mandatos **idscfgdb** e **idsldapmodify**, consulte *Consulta de mandatos*.

Modificación de la contraseña del administrador de bases de datos de DB2 con Herramienta de configuración

Utilice Herramienta de configuración para actualizar la contraseña del administrador de bases de datos de DB2 en el archivo de configuración de instancias de servidor de directorios.

Antes de empezar

Para actualizar la contraseña del administrador de bases de datos de DB2 en el archivo de configuración de instancias, debe completar las tareas siguientes:

- Debe existir una instancia de servidor de directorios que esté configurada con una base de datos de DB2. Consulte el apartado "Configuración de una base de datos para una instancia con Herramienta de configuración" en la página 180.
- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Acerca de esta tarea

Herramienta de configuración actualiza la contraseña del administrador de bases de datos de DB2 en el archivo de configuración de instancias de servidor de directorios. Si está configurado el registro de cambio para la instancia, la herramienta también actualizará la contraseña para el propietario de la base de datos de registro de cambios en el archivo de configuración.

Procedimiento

1. Inicie Herramienta de configuración para una instancia. Consulte el apartado "Inicio de Herramienta de configuración" en la página 174.
2. Desde la lista de tareas del panel de navegación de la izquierda, pulse **Tareas de base de datos** > **Configurar base de datos**.
3. En la página **Configurar base de datos**, siga estos pasos:
   a. Seleccione **Restablecer contraseña**.
   b. En el campo **Contraseña**, especifique la contraseña para el administrador de bases de datos.
   c. En el campo **Confirmar contraseña**, especifique la contraseña para el administrador de bases de datos.
   d. Pulse **Siguiente**.
4. Pulse **Finalizar**.
5. Para aceptar la finalización de la tarea, pulse **Aceptar**.
6. Verifique los registros que se generan para la operación de configuración de la contraseña de la base de datos.
7. Para cerrar la página **Configurar base de datos**, pulse **Cerrar**.
8. Para cerrar la ventana Herramienta de configuración, pulse **Archivo** > **Salir**.
9. Para confirmar la acción, pulse **Sí**.

Qué hacer a continuación

Inicie el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Modificación de la contraseña del administrador de bases de datos de DB2 con el programa de utilidad de línea de mandatos

Utilice el programa de utilidad de línea de mandatos **idscfgdb** o **idsldapmodify** para actualizar la contraseña del administrador de bases de datos de DB2 en el archivo de configuración de instancias de servidor de directorios.

Antes de empezar

Para actualizar la contraseña del administrador de bases de datos de DB2 en el archivo de configuración de instancias, debe completar las tareas siguientes:

- Debe existir una instancia de servidor de directorios que esté configurada con una base de datos de DB2. Consulte el apartado "Configuración de una base de datos para una instancia con el programa de utilidad de la línea de mandatos" en la página 185.

Acerca de esta tarea

Puede ejecutar el mandato **idscfgdb** para actualizar el archivo de configuración de una instancia con la contraseña del administrador de bases de datos de DB2. Debe detener el servidor de directorios para ejecutar el mandato **idscfgdb**.

Puede utilizar el mandato **idsldapmodify** para cambiar la contraseña cuando esté en ejecución la instancia de servidor de directorios. Ejecute el mandato **idsldapmodify** con el administrador de servidor de directorios primario o como un miembro del grupo de administradores local con el rol `dirdata`.

Para obtener más información sobre los mandatos **idscfgdb** e **idsldapmodify**, consulte *Consulta de mandatos*.

Procedimiento

1. Inicie la sesión como propietario de la instancia de servidor de directorios.
2. Acceda al indicador de mandatos.
3. Para cambiar la contraseña del administrador de bases de datos de DB2, elija uno de los métodos siguientes:
   - Para cambiar la contraseña del administrador de bases de datos de DB2 con el mandato **idscfgdb**, siga estos pasos:
     a. Cambie el directorio de trabajo actual al subdirectorio `sbin` en la ubicación de instalación de IBM Security Directory Server.
     b. Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos" en la página 163.
     c. Ejecute el mandato **idscfgdb** en el formato siguiente:
        ```
        idscfgdb -I nombre_instancia -w PWDadmindb2
        ```
     d. Inicie el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos" en la página 163.
   - Para cambiar la contraseña del administrador de bases de datos de DB2 con el mandato **idsldapmodify**, siga estos pasos:
     a. Cambie el directorio de trabajo actual al subdirectorio `bin` en la ubicación de instalación de IBM Security Directory Server.
     b. Ejecute el mandato **idsldapmodify** en el formato siguiente:
        ```
        idscfgdb -h dirección_IP -p puerto -D DNadmin -w PWDadmin -i file1.ldif
        ```

        `file1.ldif` contiene las siguientes entradas:
        ```
        dn: cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas,
         cn=Configuration
        changetpye: modify
        replace: ibm-slapdDbUserPW
        ibm-slapdDbUserPW: PWDadmindb2
        ```
     c. Reinicie el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos" en la página 163.

Desconfiguración de la base de datos de una instancia de servidor de directorios

Para utilizar una instancia de servidor de directorios existente con otra base de datos de DB2, debe desconfigurar la base de datos de DB2 existente de una instancia.

Para una instancia de servidor de directorios, sólo puede desconfigurar una base de datos si ha configurado la base de datos de DB2 para la instancia.

Con Herramienta de configuración o el mandato **idsucfgdb**, puede elegir ejecutar las siguientes operaciones:

- Eliminar la información de la base de datos de DB2 del archivo de configuración de una instancia de servidor de directorios. En esta operación, el programa de utilidad desconfigura la base de datos de DB2 de una instancia y no suprime la base de datos de DB2.
- Eliminar la información de la base de datos de DB2 del archivo de configuración de una instancia de servidor de directorios y suprimir la base de datos de DB2. En esta operación, se suprimirá la base de datos de DB2 y se perderán todos los datos.

Tras desconfigurar la base de datos de DB2 de una instancia de servidor de directorios, la base de datos quedará inaccesible para la instancia.

Para una instancia de servidor proxy, no está soportada la operación de desconfiguración de la base de datos.

Para obtener más información sobre el mandato **idsucfgdb**, consulte *Consulta de mandatos*.

Desconfiguración de la base de datos de DB2 desde una instancia con Herramienta de configuración

Utilice Herramienta de configuración para desconfigurar la base de datos de DB2 desde una instancia de servidor de directorios.

Antes de empezar

Para desconfigurar la base de datos de DB2 desde una instancia, la instancia debe cumplir los requisitos siguientes:

- Debe existir una instancia de servidor de directorios que esté configurada con una base de datos de DB2. Consulte el apartado "Configuración de una base de datos para una instancia con Herramienta de configuración" en la página 180.
- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Procedimiento

1. Inicie Herramienta de configuración para una instancia. Consulte el apartado "Inicio de Herramienta de configuración" en la página 174.
2. Desde la lista de tareas del panel de navegación izquierdo, pulse **Tareas de base de datos** > **Desconfigurar base de datos**.
3. En la página **Desconfigurar base de datos**, siga estos pasos:
   a. En el área Opciones, seleccione una de las opciones siguientes:

- Para desconfigurar la base de datos de DB2 desde una instancia sin suprimir la base de datos de DB2, pulse **Desconfigurar la base de datos**.
- Para desconfigurar la base de datos de DB2 desde una instancia y para suprimir la base de datos de DB2, pulse **Desconfigurar y destruir la base de datos**.

b. Para eliminar la copia de seguridad de la base de datos para la instancia si la base de datos está configurada para la copia de seguridad en línea, seleccione **Eliminar la copia de seguridad de la base de datos**.

c. Para iniciar la desconfiguración, pulse **Desconfigurar**.

d. En la ventana de confirmación, pulse **Sí**.

4. Para aceptar la finalización de la tarea, pulse **Aceptar**.
5. Verifique los registros que se generan para la operación de desconfiguración de la base de datos.
6. Para cerrar la página **Desconfigurar la base de datos**, pulse **Cancelar**.
7. Para cerrar la ventana Herramienta de configuración, pulse **Archivo** > **Salir**.
8. Para confirmar la acción, pulse **Sí**.

Desconfiguración de la base de datos de DB2 desde una instancia con el programa de utilidad de línea de mandatos

Utilice el programa de utilidad de línea de mandatos, **idsucfgdb**, para desconfigurar la base de datos de DB2 desde una instancia de servidor de directorios.

Antes de empezar

Para desconfigurar la base de datos de DB2 desde una instancia, la instancia debe cumplir los requisitos siguientes:

- Debe existir una instancia de servidor de directorios que esté configurada con una base de datos de DB2. Consulte el apartado "Configuración de una base de datos para una instancia con el programa de utilidad de la línea de mandatos" en la página 185.
- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos" en la página 163.

Procedimiento

1. Inicie la sesión como propietario de la instancia de servidor de directorios.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al subdirectorio `sbin` en la ubicación de instalación de IBM Security Directory Server.
4. Para desconfigurar la base de datos de DB2 desde una instancia, elija una de las siguientes opciones:
   - Para desconfigurar la base de datos desde una instancia de servidor de directorios, ejecute el mandato **idsucfgdb** en el formato siguiente:

     ```
     idsucfgdb -I nombre_instancia
     ```

   - Para desconfigurar y suprimir la base de datos desde una instancia de servidor de directorios, ejecute el mandato **idsucfgdb** en el formato siguiente:

     ```
     idsucfgdb -I nombre_instancia -r
     ```

Optimización de la base de datos

Para mejorar el rendimiento de búsqueda de la base de datos de DB2, puede optimizar la base de datos y actualizar las estadísticas de DB2 para las tablas de la base de datos.

Puede utilizar Herramienta de configuración o el mandato **idsrunstats** para optimizar la base de datos de DB2. Debe ejecutar la operación de optimización de DB2 periódicamente o una vez que se actualice la base de datos, como por ejemplo tras las operaciones de importación de datos.

Al ejecutar la optimización de bases de datos, la herramienta recopilará estadísticas en todos los índices definidos en tablas y las actualizará. El optimizador de consultas de DB2 utiliza estas estadísticas para determinar la vía de acceso óptima para acceder a los datos.

No podrá ejecutar la optimización de DB2 si la instancia es un servidor proxy, o la instancia no está configurada con una base de datos de DB2.

Para obtener más información sobre el mandato **idsrunstats**, consulte *Consulta de mandatos*.

Optimización de bases de datos con Herramienta de configuración

Utilice Herramienta de configuración para optimizar la base de datos de DB2 asociada con una instancia.

Antes de empezar

Para optimizar la base de datos de DB2 para una instancia, ésta debe cumplir los requisitos siguientes:

- Debe existir una instancia de servidor de directorios que esté configurada con una base de datos de DB2. Consulte el apartado "Configuración de una base de datos para una instancia con Herramienta de configuración" en la página 180.

Procedimiento

1. Inicie Herramienta de configuración para una instancia. Consulte el apartado "Inicio de Herramienta de configuración" en la página 174.
2. Desde la lista de tareas del panel de navegación izquierdo, pulse **Tareas de base de datos** > **Optimizar base de datos**.
3. En la página **Optimizar base de datos**, siga estos pasos:
   a. Para iniciar la operación de optimización de bases de datos, pulse **Optimizar**.
   b. Para aceptar la finalización de la tarea, pulse **Aceptar**.
   c. Verifique los registros que se generan para la operación de optimización de bases de datos.
   d. Para borrar los registros, pulse **Borrar resultados**.
4. Para cerrar la página **Optimizar base de datos**, pulse **Cerrar**.
5. Para cerrar la ventana Herramienta de configuración, pulse **Archivo** > **Salir**.
6. Para confirmar la acción, pulse **Sí**.

Optimización de bases de datos con el programa de utilidad de línea de mandatos

Utilice el programa de utilidad de línea de mandatos, **idsrunstats**, para optimizar la base de datos de DB2 asociada con una instancia.

Antes de empezar

Para optimizar la base de datos de DB2 de una instancia, la instancia debe cumplir los requisitos siguientes:

- Debe existir una instancia de servidor de directorios que esté configurada con una base de datos de DB2. Consulte el apartado "Configuración de una base de datos para una instancia con el programa de utilidad de la línea de mandatos" en la página 185.

Procedimiento

1. Inicie la sesión como propietario de la instancia de servidor de directorios.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al subdirectorio `sbin` en la ubicación de instalación de IBM Security Directory Server.
4. Para optimizar la base de datos de DB2, ejecute el mandato **idsrunstats** en el formato siguiente:

   ```
   idsrunstats -I nombre_instancia
   ```

   Para obtener más información sobre el mandato **idsrunstats**, consulte *Consulta de mandatos*.

Mantenimiento de la base de datos

Para mejorar las operaciones de búsqueda o de actualización en una instancia, puede ejecutar la reorganización de índices de DB2 o la compresión de filas de DB2.

Puede utilizar Herramienta de configuración o el mandato **idsdbmaint** para ejecutar la reorganización de índices de DB2 o la compresión de filas de DB2.

Cuando se actualizan las tablas de DB2 de una base de datos con muchas inserciones y supresiones, las operaciones de búsqueda y actualización en la base de datos se ralentizan. Si reorganiza el índice de DB2, el rendimiento de las operaciones de búsqueda y actualización mejorará.

Al ejecutar la compresión de filas de DB2, la herramienta busca patrones repetidos y los sustituye por cadenas de símbolos más cortas. La herramienta analizará y, a continuación, ejecutará la compresión de filas sólo si la compresión da como resultado una mejora de más del 30 por ciento.

También puede utilizar el mandato **idsdbmaint** para convertir un espacio de tablas SMS en un espacio de tablas DMS o un espacio de tablas DMS en un espacio de tablas SMS. La conversión del espacio de tablas no está soportada por Herramienta de configuración. Para obtener más información sobre el mandato **idsdbmaint**, consulte *Consulta de mandatos*.

Ejecución del mantenimiento de bases de datos con Herramienta de configuración

Utilice Herramienta de configuración para mantener la base de datos de DB2 asociada con una instancia.

Antes de empezar

Para mantener la base de datos de DB2 para una instancia, ésta debe cumplir los requisitos siguientes:

- Debe existir una instancia de servidor de directorios que esté configurada con una base de datos de DB2. Consulte el apartado "Configuración de una base de datos para una instancia con Herramienta de configuración" en la página 180.
- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Procedimiento

1. Inicie Herramienta de configuración para una instancia. Consulte el apartado "Inicio de Herramienta de configuración" en la página 174.
2. Desde la lista de tareas del panel de navegación izquierdo, pulse **Tareas de base de datos** > **Mantenimiento**.
3. En la página **Mantenimiento**, siga estos pasos:
   a. Seleccione la operación de mantenimiento de bases de datos de DB2 que desee ejecutar:
      - Para ejecutar la reorganización del índice de DB2, pulse **Realizar la reorganización del índice**.
      - Para ejecutar la compresión de filas de DB2, pulse **Inspeccionar las tablas y realizar la compresión de filas**.
   b. Pulse **Aceptar**.
   c. En la ventana de finalización de tarea, pulse **Aceptar**.
   d. Verifique los registros generados para la operación de mantenimiento de bases de datos.
   e. Para borrar los registros, pulse **Borrar resultados**.
4. Para cerrar la página **Mantenimiento**, pulse **Cerrar**.
5. Para cerrar la ventana Herramienta de configuración, pulse **Archivo** > **Salir**.
6. Para confirmar la acción, pulse **Sí**.

Qué hacer a continuación

Inicie el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Ejecución del mantenimiento de la base de datos con el programa de utilidad de línea de mandatos

Utilice el programa de utilidad de línea de mandatos, **idsdbmaint**, para ejecutar la operación de mantenimiento en la base de datos de DB2 asociada con una instancia.

Antes de empezar

Para ejecutar la operación de mantenimiento de bases de datos de DB2, la instancia debe cumplir los requisitos siguientes:

- Debe existir una instancia de servidor de directorios que esté configurada con una base de datos de DB2. Consulte el apartado "Configuración de una base de datos para una instancia con el programa de utilidad de la línea de mandatos" en la página 185.
- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos" en la página 163.

Procedimiento

1. Inicie la sesión como propietario de la instancia de servidor de directorios.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al subdirectorio `sbin` en la ubicación de instalación de IBM Security Directory Server.
4. Para ejecutar la reorganización del índice de DB2, ejecute el mandato **idsdbmaint** en el formato siguiente:

   ```
   idsdbmaint -I nombre_instancia -i
   ```

   Para obtener más información sobre el mandato **idsdbmaint**, consulte *Consulta de mandatos*.
5. Para ejecutar la compresión de filas de DB2, ejecute el mandato **idsdbmaint** en el formato siguiente:

   ```
   idsdbmaint -I nombre_instancia -r
   ```

Qué hacer a continuación

Inicie el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos" en la página 163.

Copia de seguridad de servidor de directorios

Para recuperarse de la anomalía de una instancia de servidor de directorios, debe realizar una copia de seguridad de la instancia de servidor de directorios con frecuencia.

Puede utilizar Herramienta de configuración o el mandato **idsdbback** para realizar una copia de seguridad de una instancia. No puede utilizar el mandato **idsdbback** para realizar una copia de seguridad de una instancia de servidor proxy porque no hay ninguna base de datos asociada con un servidor proxy.

Puede configurar una base de datos que está asociada a una instancia para la copia de seguridad en línea utilizando el mandato **idscfgdb**. Sin embargo, no puede desconfigurar la copia de seguridad en línea utilizando el mandato **idscfgdb** con el parámetro **-c**. Si configura la copia de seguridad en línea para una instancia utilizando Herramienta de administración de instancias o Herramienta de configuración, puede desconfigurarla con Herramienta de configuración o con el mandato **idscfgdb**. Para obtener resultados más fidedignos, utilice Herramienta de administración de instancias o Herramienta de configuración para configurar la copia de seguridad en línea para una instancia con la base de datos.

También puede utilizar el mandato **idsdb2ldif** para exportar las entradas de un servidor de directorios a un archivo LDIF. Puede utilizar el mandato **migbkup** para realizar una copia de seguridad de los esquemas y de los archivos de configuración para una instancia de servidor de directorios y una instancia de servidor de proxy. Para obtener más información sobre el mandato **idsdbback**, **idsdb2ldif**, o **migbkup**, consulte *Consulta de mandatos*. Para obtener más información acerca del mandato adecuado que se ha de utilizar en su entorno, consulte la sección *Ajuste de rendimiento y Planificación de capacidad* en la documentación de IBM Security Directory Server.

Con Herramienta de configuración, puede realizar las acciones siguientes:

- Realizar una copia de seguridad de los valores de configuración para una instancia de servidor de directorios o una instancia de servidor de proxy.
- Realizar una copia de seguridad de la instancia de servidor de directorios con su base de datos.
- Realizar una copia de seguridad de la instancia de servidor de directorios y la base de datos de registro de modificación si está configurada para una instancia.

Para obtener más información acerca de las operaciones de copia de seguridad y restauración, consulte la sección *Administración* en la documentación de IBM Security Directory Server.

Copia de seguridad de la base de datos de una instancia de servidor de directorios con Herramienta de configuración

Utilice Herramienta de configuración para realizar una copia de seguridad de una instancia de servidor de directorios con su base de datos para recuperarse de los errores.

Antes de empezar

Para realizar una copia de seguridad de una instancia de servidor de directorios con su base de datos, la instancia debe cumplir los requisitos siguientes:

- Debe existir una instancia de servidor de directorios que esté configurada con una base de datos de DB2. Consulte el apartado "Configuración de una base de datos para una instancia con Herramienta de configuración" en la página 180.

Procedimiento

1. Inicie Herramienta de configuración para una instancia. Consulte el apartado "Inicio de Herramienta de configuración" en la página 174.
2. Desde la lista de tareas del panel de navegación izquierdo, pulse **Copia de seguridad/Restaurar** > **Base de datos de copia de seguridad**.
3. En la página **Base de datos de copia de seguridad**, siga estos pasos:
   a. En el campo **Directorio de copia de seguridad**, especifique la vía de acceso del directorio en la que desea realizar una copia de seguridad de todas las fechas de directorio y de los archivos de configuración. También puede pulsar **Examinar** para especificar la vía de acceso del directorio.
   b. Para la copia de seguridad en línea, elija una de las siguientes opciones:
      - Para configurar el servidor de directorios y su base de datos para la copia de seguridad en línea si no se ha configurado aún para la copia de seguridad en línea, seleccione **Actualizar la configuración de la base de datos para dar soporte a la copia de seguridad en línea**.

- Para ejecutar la copia de seguridad en línea para la instancia de servidor de directorios si se ha configurado la copia de seguridad en línea en el servidor, seleccione **Realizar la copia de seguridad en línea**.

c. Para hacer una copia de seguridad de la base de datos del registro de cambios para la instancia si se ha configurado el registro de cambios, seleccione **Incluir los datos del registro de cambios en la copia de seguridad**.

d. Para excluir los archivos de base de datos de la copia de seguridad, seleccione **No realizar una copia de seguridad de los archivos de base de datos**. Si selecciona **No realizar una copia de seguridad de los archivos de base de datos**, no se realizará una copia de seguridad de la base de datos ni de los archivos de base de datos de registro de cambio para la instancia de servidor de directorios. La herramienta realiza una copia de seguridad de los archivos de la instancia de servidor de directorios, como por ejemplo los archivos de ocultación claves, los esquemas, y los archivos de configuración.

e. Para decidir si desea continuar con la copia de seguridad si existe el directorio de copia de seguridad o lo contrario, elija una de las opciones siguientes:

- Para crear el directorio de copia de seguridad si no existe, pulse **Crear directorio de copia de seguridad según sea necesario**.
- Si el directorio de copia de seguridad no existe, y no desea crearlo, pulse **Detener si el directorio de copia de seguridad no se encuentra**. Si no existe un directorio de copia de seguridad y selecciona esta opción, no se realizará una copia de seguridad de la base de datos.

Nota: No salga de Herramienta de configuración cuando se esté ejecutando la operación de copia de seguridad.

f. Para iniciar la operación de copia de seguridad, pulse **Copia de seguridad**.

g. Si la operación de copia de seguridad requiere que detenga el servidor de directorios, pulse **Sí**.

h. Para confirmar la finalización de la tarea, pulse **Aceptar**.

i. Verifique los registros que se generan para la operación de copia de seguridad.

j. Para borrar los registros, pulse **Borrar resultados**.

k. Para cerrar la página **Base de datos de copia de seguridad**, pulse **Cerrar**.

4. Para cerrar la ventana Herramienta de configuración, pulse **Archivo** > **Salir**.
5. Para confirmar la acción, pulse **Sí**.

Copia de seguridad de una instancia de servidor proxy con Herramienta de configuración

Utilice Herramienta de configuración para realizar una copia de seguridad de una instancia de servidor proxy para recuperarse de los errores.

Antes de empezar

Para realizar una copia de seguridad de una instancia de servidor proxy, debe existir una instancia de servidor proxy. Consulte el apartado "Creación de una instancia de servidor proxy con valores personalizados" en la página 147.

Procedimiento

1. Inicie Herramienta de configuración para una instancia. Consulte el apartado "Inicio de Herramienta de configuración" en la página 174.

2. Desde la lista de tareas del panel de navegación izquierdo, pulse **Copia de seguridad/Restaurar** > **Instancia de copia de seguridad**.
3. En la página **Instancia de copia de seguridad**, siga estos pasos:
   a. En el campo **Directorio de copia de seguridad**, especifique la vía de acceso del directorio en el que desea realizar la copia de seguridad de los esquemas y de los archivos de configuración. También puede pulsar **Examinar** para especificar la vía de acceso del directorio.
   b. Para una instancia de servidor proxy, se seleccionará el recuadro de selección **No realizar una copia de seguridad de los archivos de base de datos**.
   c. Para decidir si desea continuar con la copia de seguridad si existe el directorio de copia de seguridad o lo contrario, elija una de las opciones siguientes:
      - Para crear el directorio de copia de seguridad si no existe, pulse **Crear directorio de copia de seguridad según sea necesario**.
      - Si el directorio de copia de seguridad no existe, y no desea crearlo, pulse **Detener si el directorio de copia de seguridad no se encuentra**. Si no existe un directorio de copia de seguridad y selecciona esta opción, no se realizará la copia de seguridad de la instancia de proxy.

      Nota: No salga de Herramienta de configuración cuando se esté ejecutando la operación de copia de seguridad.
   d. Para iniciar la operación de copia de seguridad, pulse **Copia de seguridad**.
   e. Si la operación requiere que detenga la instancia, pulse **Sí**.
   f. Para confirmar la finalización de la tarea, pulse **Aceptar**.
   g. Verifique los registros que se generan para la operación de copia de seguridad.
   h. Para borrar los registros, pulse **Borrar resultados**.
   i. Para cerrar la página **Instancia de copia de seguridad**, pulse **Cerrar**.
4. Para cerrar la ventana Herramienta de configuración, pulse **Archivo** > **Salir**.
5. Para confirmar la acción, pulse **Sí**.

Restaurar un servidor de directorios

Si falla la instancia de servidor de directorios, puede restaurar la instancia en la imagen de copia de seguridad más reciente.

Puede utilizar Herramienta de configuración o el mandato **idsdbestore** para restaurar datos de directorios y, opcionalmente, valores de configuración de los que se ha realizado anteriormente copia de seguridad. Debe detener el servidor de directorios antes de poder restaurar la base de datos, los valores de configuración, o ambos.

Para un servidor proxy, puede restaurar los valores de configuración. Para un servidor proxy, debe ejecutar el mandato **idsdbrestore** con el parámetro **-x**.

Para una instancia con una base de datos de DB2, puede restaurar la base de datos en una base de datos y una instancia de base de datos con el mismo nombre que se ha utilizado para la copia de seguridad de la base de datos. Para un servidor de directorios con una base de datos de DB2, sólo podrá restaurarlo si una base de datos está configurada para la instancia de servidor de directorios. El mandato **idsdbestore** restaurará la base de datos de copia de seguridad en la base de datos

configurada actualmente. El mandato fallará si la instancia de base de datos y la base de datos de las que se ha realizado una copia de seguridad no coinciden con la instancia de base de datos y la base de datos configuradas. Para restaurar la base de datos, la ubicación de la base de datos de la que se ha realizado copia de seguridad y de la base de datos que está restaurando el mandato debe ser la misma.

Para obtener más información sobre el mandato **idsdbrestore**, consulte *Consulta de mandatos*.

Restauración de bases de datos de un servidor de directorios con Herramienta de configuración

Utilice Herramienta de configuración para restaurar una instancia de servidor de directorios y su base de datos de una imagen de la que se ha realizado copia de seguridad.

Antes de empezar

Para restaurar una instancia de servidor de directorios y su base de datos, la instancia debe cumplir los requisitos siguientes:

- Debe existir una instancia de servidor de directorios que esté configurada con una base de datos de DB2. Consulte el apartado "Configuración de una base de datos para una instancia con Herramienta de configuración" en la página 180.
- Debe existir una imagen de copia de seguridad de la instancia de servidor de directorios. Consulte el apartado "Copia de seguridad de la base de datos de una instancia de servidor de directorios con Herramienta de configuración" en la página 196.
- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Procedimiento

1. Inicie Herramienta de configuración para una instancia. Consulte el apartado "Inicio de Herramienta de configuración" en la página 174.
2. Desde la lista de tareas del panel de navegación de la izquierda, pulse **Copia de seguridad/Restaurar** > **Restaurar base de datos**.
3. En la página **Restaurar base de datos**, siga estos pasos:
   a. En el campo **Restaurar directorio**, especifique la vía de acceso del directorio que contiene la imagen de copia de seguridad de la instancia. También puede pulsar **Examinar** para especificar la vía de acceso del directorio.
   b. Si sólo desea restaurar los datos de directorio y no los valores de configuración de la imagen de la que se ha realizado copia de seguridad, seleccione **Conservar valores de configuración actuales**. Si desea restaurar los valores de base de datos y de configuración, debe borrar **Conservar valores de configuración actuales**.
   c. Si el registro de cambios está configurado para la instancia y desea restaurar los datos del registro de cambios, seleccione **Incluir los datos del registro de cambios en la restauración**.
   d. Para iniciar la operación de restauración, pulse **Restaurar**.
   e. Si la operación requiere detener el servidor de directorios, pulse **Sí**.
   f. Para confirmar la finalización de la tarea, pulse **Aceptar**.
   g. Verifique los registros generados para la operación de restauración.

h. Para borrar los registros, pulse **Borrar resultados**.
i. Para cerrar la página **Restaurar base de datos**, pulse **Cerrar**.

4. Para cerrar la ventana Herramienta de configuración, pulse **Archivo** > **Salir**.
5. Para confirmar la acción, pulse **Sí**.

Restauración de una instancia de servidor proxy con Herramienta de configuración

Utilice Herramienta de configuración para restaurar una instancia de servidor proxy para recuperarse de los errores.

Antes de empezar

Para restaurar una instancia de servidor proxy, la instancia de servidor proxy debe cumplir los requisitos siguientes:

- Debe existir la instancia de servidor proxy. Consulte el apartado "Creación de una instancia de servidor proxy con valores personalizados" en la página 147.
- Debe existir una imagen de copia de seguridad de la instancia de servidor proxy. Consulte el apartado "Copia de seguridad de una instancia de servidor proxy con Herramienta de configuración" en la página 197.
- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Procedimiento

1. Inicie Herramienta de configuración para una instancia. Consulte el apartado "Inicio de Herramienta de configuración" en la página 174.
2. Desde la lista de tareas del panel de navegación izquierdo, pulse **Copia de seguridad/Restaurar** > **Restaurar instancia**.
3. En la página **Restaurar instancia**, siga estos pasos:
   a. En el campo **Restaurar directorio**, especifique la vía de acceso del directorio que contiene la imagen de copia de seguridad de la instancia. También puede pulsar **Examinar** para especificar la vía de acceso del directorio.
   b. Si desea restaurar los valores de configuración a partir de la imagen de la que se ha realizado una copia de seguridad, seleccione **Conservar valores de configuración actuales**.
   c. Para iniciar la operación de restauración, pulse **Restaurar**.
   d. Si la operación requiere detener el servidor de directorios, pulse **Sí**.
   e. Para confirmar la finalización de la tarea, pulse **Aceptar**.
   f. Verifique los registros generados para la operación de restauración.
   g. Para borrar los registros, pulse **Borrar resultados**.
   h. Para cerrar la página **Restaurar instancia**, pulse **Cerrar**.
4. Para cerrar la ventana Herramienta de configuración, pulse **Archivo** > **Salir**.
5. Para confirmar la acción, pulse **Sí**.

Ajuste de un servidor de directorios para el rendimiento

Debe ajustar una instancia de servidor de directorios para mejorar el rendimiento de búsqueda y de actualización.

Puede ejecutar Herramienta de configuración o el mandato **idsperftune** para ajustar una instancia de servidor de directorios. La herramienta genera los valores de ajuste de rendimiento para las memorias caché de servidor de directorios y las agrupaciones de almacenamiento intermedio de DB2. La herramienta genera los valores de ajuste que se basan en los valores que se proporcionan sobre la instancia de servidor de directorios. La herramienta también puede actualizar los valores de ajuste para una instancia. La herramienta realiza una copia de seguridad del archivo `ibmslapd.conf` y lo guarda en el archivo `logs/ibmslapd.conf.save` en el directorio de inicio para una instancia de servidor de directorios.

La herramienta guarda la información que proporciona en el archivo `logs/perftune_input.conf` en el directorio de inicio para una instancia de servidor de directorios.

Herramienta de configuración o el mandato **idsperftune** utiliza los valores que proporciona para calcular los siguientes valores de ajuste para la instancia:

- Tamaño de memoria caché de las entradas
- Tamaño de memoria caché de los filtros
- Tamaño de memoria caché de los miembros de grupo
- Límite de derivación de memoria caché de los miembros de grupo
- Tamaño de la agrupación de almacenamiento intermedio `DB2 LDAPDB`
- Tamaño de la agrupación de almacenamiento intermedio `DB2 IBMDEFAULTDB`

Si se está ejecutando la instancia de servidor de directorios, la herramienta supervisa el rendimiento de la instancia y proporciona la información de comprobación del estado de la base de datos. La información de comprobación de estado de la base de datos incluye los siguientes parámetros de DB2:

- `DB2 NUM_IOSERVERS`
- `DB2 NUM_IOCLEANERS`
- `CATALOGCACHE_SZ`
- `PCKCACHESZ`
- `LOGFILSIZ`
- `LOCKLIST`

Si ejecuta el ajuste avanzado en una instancia, la herramienta recopila y analiza datos sobre la instancia de servidor de directorios. Debe ejecutar la instancia durante algún tiempo para recopilar datos de ajuste de DB2 durante el análisis de comprobación de estado de la base de datos. La herramienta genera los valores de ajuste para los siguientes parámetros de DB2 y los guarda en el archivo `logs/perftune_stat.log` para la instancia.

- `SORTHEAP`
- `MAXFILOP`
- `DBHEAP`
- `CHNGPGS_THRESH`
- `NUM_IOSERVERS`
- `NUM_IOCLEANERS`

Las sugerencias del estado de salud para los parámetros de DB2 puede ser uno de los valores siguientes:

- `Aceptar`
- `Increase`

- `Decrease`
- `Not Collected`

El estado de salud de los parámetros de DB2 que no están analizados tiene asignado el valor `Not Collected`. Puede utilizar los valores sugeridos para decidir los parámetros de DB2 que puede ajustar para obtener un mejor rendimiento.

Para obtener un mejor rendimiento, debe ejecutar la herramienta en una instancia en el momento en el que cargue los datos iniciales de directorios. Tras el ajuste inicial, ejecute la herramienta periódicamente, sobre todo tras agregar muchas entradas o modificar el contenido de las entradas.Para obtener más información acerca de cómo ajustar una instancia del servidor de directorios, consulte la sección *Ajuste de rendimiento y Planificación de capacidad* en la documentación de IBM Security Directory Server.

No puede utilizar Herramienta de configuración ni el mandato **idsperftune** para ajustar una instancia de servidor proxy o una instancia que no esté configurada con una base de datos.

Configuración de un servidor de directorios para el ajuste de rendimiento con Herramienta de configuración

Utilice Herramienta de configuración para ajustar un servidor de directorios para mejorar el rendimiento de las operaciones de búsqueda y de actualización.

Antes de empezar

Para ajustar una instancia de servidor de directorios, la instancia debe cumplir los requisitos siguientes:

- Debe existir una instancia de servidor de directorios que esté configurada con una base de datos de DB2. Consulte el apartado "Configuración de una base de datos para una instancia con Herramienta de configuración" en la página 180.

Procedimiento

1. Inicie Herramienta de configuración para una instancia. Consulte el apartado "Inicio de Herramienta de configuración" en la página 174.
2. Desde la lista de tareas del panel de navegación izquierdo, pulse **Tareas de base de datos** > **Ajuste de rendimiento**.
3. En la página **Ajuste de rendimiento**, siga estos pasos:
   a. En el campo **Porcentaje de memoria del sistema disponible que se va a asignar en esta instancia de directorio**, especifique el porcentaje de memoria del sistema que desea tener asignado a la instancia. La memoria del sistema disponible se divide entre varias instancias de servidor de directorios, o entre instancias y otros servidores que tiene previsto ejecutar en el sistema. La herramienta utiliza el valor que proporciona para calcular los tamaños de la entrada y de las memorias caché del filtro.
   b. En el campo **Número de grupos planificados**, especifique el número de grupos que se espera añadir a la instancia. La herramienta utiliza el valor que especifica para calcular los tamaños para las memorias caché del servidor de directorios.
   c. En el campo **Número máximo de miembros en un grupo al que se hará referencia con frecuencia**, especifique el número promedio de miembros para los grupos a los que se hace referencia con frecuencia.

d. En el área **Número de entradas y tamaño promedio de entrada**, elija una de las opciones siguientes:
   - Si desea calcular el número de entradas del directorio y el tamaño promedio de una entrada, siga estos pasos:
     1) En el campo **Número planificado de entradas**, especifique el número total de entradas planificadas para la instancia. La herramienta intenta determinar el número de entradas de la instancia de servidor de directorios. Si no puede, utiliza el valor predeterminado de 10.000 entradas. La herramienta utiliza este valor para calcular los tamaños para las memorias caché del servidor de directorios.
     2) En el campo **Tamaño promedio de una entrada**, especifique el tamaño promedio en bytes de una entrada que se encuentra en la instancia. La herramienta intenta calcular el tamaño de una entrada en la instancia de servidor de directorios. Si no puede, utiliza el valor predeterminado de 2650 bytes. La herramienta utiliza este valor para calcular los tamaños para las memorias caché del servidor de directorios.
   - Si desea que la herramienta determine el número total de entradas y el tamaño promedio de la entrada, pulse **Cargar desde la base de datos de instancia de servidor**. La herramienta rellena los campos **Número planificado de entradas** y **Tamaño promedio de una entrada**.

e. En el área **Frecuencia de actualización**, elija una de las siguientes opciones:
   - Si tiene previstas actualizaciones frecuentes a la instancia, pulse **Actualizaciones frecuentes**. (Como directriz, pueden considerarse actualizaciones frecuentes un promedio de más de una actualización para cada 500 búsquedas).
   - Si tiene previstas actualizaciones menos frecuentes o si las actualizaciones se agrupan y se realizan a horas concretas del día, pulse **Actualizaciones de proceso por lotes**.

   La herramienta utiliza esta información para establecer el tamaño de la memoria caché de filtro. La memoria caché de filtro es útil únicamente cuando hay actualizaciones poco frecuentes de la instancia y las mismas búsquedas se ejecutan varias veces. Si están previstas actualizaciones frecuentes, la memoria caché de filtro se establecerá en 0. Si están previstas actualizaciones poco frecuentes o de proceso por lotes, la memoria caché de filtro se establecerá en 1024 entradas de memoria caché de filtro.

f. Si desea que la herramienta proporcione valores de análisis de rendimiento, seleccione **Habilitar la recopilación de datos del sistema adicionales para un ajuste ampliado**.
   - Al seleccionar el recuadro de verificación, se habilitarán los conmutadores del supervisor de DB2 `BUFFERPOOL` y `SORTHEAP`. El rendimiento de la instancia de servidor de directorios puede degradarse cuando la herramienta habilita a los conmutadores del supervisor de DB2 para recopilar los datos.
   - Para obtener datos exactos para ofrecer el ajuste óptimo de la instancia de servidor de directorios, marque el recuadro de selección cuando la actividad del directorio sea normal para el entorno. Si ejecuta la comprobación del estado de la base de datos cuando el servidor no está ocupado, el proceso normal no proporciona los valores de rendimiento óptimos.

g. Pulse **Siguiente**. Se abrirá la página **Ajuste de rendimiento: verificación**.

4. En la página **Ajuste de rendimiento: verificación**, siga estos pasos:
   a. En la lista **Estado de salud de la base de datos**, verifique los valores de ajuste de rendimiento que genera la herramienta. Si no hay actividades de base de datos para la instancia, es posible que no se rellene la lista **Estado de salud de la base de datos**. La lista se rellenará si la herramienta recopila información sobre al menos un parámetro relacionado con DB2. Los valores de ajuste también se registran en el archivo `perftune_stat.log`.
   b. Para modificar los valores de parámetros de la base de datos, pulse **Ajustar parámetros de la base de datos**. Se abrirá la ventana **Parámetros de la base de datos**.
   c. En la ventana **Parámetros de la base de datos**, especifique los valores para los siguientes parámetros de la base de datos:
      1) En el campo **Almacenamiento dinámico de base de datos**, especifique el número máximo de memoria en páginas que establecer para el almacenamiento dinámico de base de datos. El almacenamiento dinámico de la base de datos contiene información de bloqueo de control para tablas, índices, espacios de tablas y agrupaciones de almacenamiento intermedio. También contiene memoria para el almacenamiento intermedio de registro y la memoria temporal que utilizan los programas de utilidad.
      2) En el campo **Tamaño de la memoria caché de paquetes**, especifique el tamaño en páginas para almacenar en caché las secciones para las sentencias estáticas y dinámicas de SQL y XQuery en una base de datos.
      3) En el campo **Tamaño de almacenamiento intermedio de registro**, especifique el tamaño en páginas para el almacenamiento intermedio que se debe asignar para los registros de anotaciones. Debe especificar la cantidad de almacenamiento intermedio de base de datos a utilizar como almacenamiento intermedio para los registros de anotaciones.
      4) En el campo **Número máximo de archivos de base de datos abiertos por aplicación**, especifique el número máximo de descriptores de archivos que se pueden abrir para cada agente de base de datos.
      5) En el campo **Umbral de páginas modificado**, especifique el porcentaje de páginas modificadas.
      6) En el campo **Tamaño de almacenamiento dinámico de clasificación**, especifique el tamaño máximo para el almacenamiento dinámico de clasificación en las páginas. El almacenamiento dinámico de clasificación se puede utilizar como páginas de memoria privada para las clasificaciones privadas o como páginas de memoria compartidas para clasificaciones compartidas.
      7) En el campo **Tamaño de archivo de registro**, especifique el tamaño en kB para los archivos de registro. Este parámetro define el tamaño de cada archivo de registro primario y secundario.
      8) En el campo **Vía de acceso de registro de base de datos**, especifique la ubicación donde desea almacenar los archivos de registro. Puede pulsar **Examinar** para especificar la ubicación.
      9) Para guardar los valores configurados y para actualizar los parámetros de base de datos con los valores, pulse **Aceptar**. Si no especifica valores para los parámetros, se establecerán los valores predeterminados.
5. Para confirmar si desea actualizar los valores del directorio y de la base de datos con los valores de ajuste, elija una de las opciones siguientes:

- Para actualizar los valores de ajuste para la instancia de servidor de directorios, pulse **Sí, utilizar los valores recomendados para actualizar los valores de configuración del directorio y de la base de datos**.
- Si no desea utilizar los valores ajuste, pulse **No, mantener los valores actuales. No se actualizarán los valores de configuración**.

6. Para aplicar los cambios, pulse **Finalizar**.
7. Para confirmar la finalización de la tarea, pulse **Aceptar**.
8. Verifique los registros que se generan al actualizar los valores de ajuste.
9. Para borrar los registros, pulse **Borrar resultados**.
10. Para cerrar la página **Ajuste de rendimiento**, pulse **Cerrar**.
11. Para cerrar la ventana Herramienta de configuración, pulse **Archivo** > **Salir**.
12. Para confirmar la acción, pulse **Sí**.

Configuración de un servidor de directorios para el ajuste de rendimiento con el programa de utilidad de línea de mandatos

Utilice el programa de utilidad de línea de mandatos, **idsperftune**, para ajustar un servidor de directorios para mejorar el rendimiento de las operaciones de búsqueda y de actualización.

Antes de empezar

Para ajustar una instancia de servidor de directorios, la instancia debe cumplir los requisitos siguientes:

- Debe existir una instancia de servidor de directorios que esté configurada con una base de datos de DB2. Consulte el apartado "Configuración de una base de datos para una instancia con el programa de utilidad de la línea de mandatos" en la página 185.

Procedimiento

1. Inicie la sesión como propietario de la instancia de servidor de directorios.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al subdirectorio `sbin` en la ubicación de instalación de IBM Security Directory Server.
4. Para ajustar un servidor de directorios y su base de datos, ejecute el mandato **idsperftune**.
   - Para ejecutar el ajuste básico del servidor de directorios, ejecute el mandato **idsperftune** en el formato siguiente:

     ```
     idsperftune -I nombre_instancia -i archivo_propiedades -B -u
     ```

     Al especificar el parámetro **-u**, los valores de memoria caché LDAP y de agrupación de almacenamiento intermedio de DB2 se actualizarán en el servidor y en la base de datos. Si no especifica el parámetro **-u**, sólo se registrarán los valores de ajuste en el archivo `perftune_stat.log`.
   - Para obtener el número de entradas y el promedio de tamaño de entrada de una instancia y su base de datos, ejecute el mandato **idsperftune** en el formato siguiente:

     ```
     idsperftune -I nombre_instancia -s
     ```
   - Para ejecutar el ajuste avanzado del servidor de directorios, ejecute el mandato **idsperftune** en el formato siguiente:

     ```
     idsperftune -I nombre_instancia -i archivo_propiedades -A -m
     ```

Al especificar el parámetro **-m**, se activarán los conmutadores del supervisor para BUFFERPOOL y SORT. Para obtener datos exactos para ofrecer el ajuste óptimo de la instancia, ejecute el mandato cuando la actividad de directorio sea normal para el entorno.

Para obtener más información sobre el mandato **idsperftune**, consulte *Consulta de mandatos*.

Gestión del registro de modificación para una instancia de servidor de directorios

Puede configurar la base de datos de registro de modificación para registrar las modificaciones en los esquemas o en las entradas del directorio de una instancia.

Las grabaciones del registro de modificación actualizarán las operaciones, como por ejemplo add, delete, modify, y modrdn, en una instancia de servidor de directorios. Puede utilizar los programas de utilidad del cliente para recuperar los datos de registro de modificación que se graban cuando se realizan los cambios en una base de datos de servidor de directorios.

Puede utilizar Herramienta de configuración o los programas de utilidad de línea de mandatos para habilitar o inhabilitar la base de datos de registro de modificación. Debe detener el servidor de directorios antes de configurar o desconfigurar la base de datos de registro de modificación.

Para configurar el registro de modificación para un servidor de directorios, utilice el mandato **idscfgchglg**. Para desconfigurar el registro de modificaciones para un servidor de directorios, utilice el mandato **idsucfgchglg**. No puede configurar una base de datos de registro de modificación para una instancia de servidor proxy.

Para configurar el registro de modificación para una instancia de servidor de directorios, debe cumplir los criterios siguientes:

1. Debe existir una instancia de DB2 con el mismo nombre que la instancia de servidor de directorios.
2. Debe configurar una base de datos para la instancia de servidor de directorios.
3. En AIX, Linux, y Solaris, se debe registrar el servicio de bucle de retorno local en el archivo /etc/services.

Al configurar una base de datos de registro de modificación, se creará en la misma instancia de base de datos que la base de datos de instancia de servidor de directorios. Para la base de datos de registro de modificación, son necesarios 30 MB adicionales de espacio de disco duro. Al configurar el registro de modificación, se añadirá la entrada de registro de modificación al archivo de configuración de la instancia de servidor de directorios.

Configuración del registro de cambios con Herramienta de configuración

Utilice Herramienta de configuración para configurar la base de datos del registro de cambios para una instancia de servidor de directorios.

Antes de empezar

Para configurar el registro de cambios para una instancia, la instancia debe cumplir los siguientes requisitos:

- Debe existir una instancia de servidor de directorios que esté configurada con una base de datos de DB2. Consulte el apartado "Configuración de una base de datos para una instancia con Herramienta de configuración" en la página 180.
- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Procedimiento

1. Inicie Herramienta de configuración para una instancia. Consulte el apartado "Inicio de Herramienta de configuración" en la página 174.
2. Desde la lista de tareas del panel de navegación izquierdo, pulse **Gestionar el registro de cambios**.
3. En la página **Gestionar el registro de cambios**, siga estos pasos:
   a. Para configurar el registro de cambios, seleccione **Habilitar la base de datos del registro de cambios**.
   b. En el área **Número máximo de entradas de registro**, especifique el número máximo de entradas que desea registrar en la base de datos del registro de cambios.
      - Para registrar el número de entradas ilimitadas en el registro de cambios, pulse **Ilimitado**.
      - Para registrar un número específico de entradas, pulse **Entradas** y especifique el número de entradas. El número de entradas predeterminado es 1.000.000.
   c. En el área **Duración máxima**, especifique el número máximo de duraciones para las que desea almacenar entradas en la base de datos de registros de cambios.
      - Para almacenar las entradas en el registro de cambios de forma indefinida, pulse **Ilimitado**.
      - Para almacenar entradas por una duración específica, pulse **Duración** y especifique el número de días y horas.
   d. Para aplicar los cambios, pulse **Actualizar**.
   e. Para confirmar la finalización de la tarea, pulse **Aceptar**.
   f. Verifique los registros generados para la configuración de la base de datos de registros de cambios.
   g. Para borrar los registros, pulse **Borrar resultados**.
   h. Para cerrar la página **Gestionar registro de cambios**, pulse **Cerrar**.
4. Para cerrar la ventana Herramienta de configuración, pulse **Archivo** > **Salir**.
5. Para confirmar la acción, pulse **Sí**.

Qué hacer a continuación

Inicie el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Configuración del registro de cambios con el programa de utilidad de línea de mandatos

Utilice el programa de utilidad de línea de mandatos, **idscfgchglg**, para configurar la base de datos del registro de cambios para una instancia de servidor de directorios.

Antes de empezar

Para configurar el registro de cambios para una instancia, la instancia debe cumplir los siguientes requisitos:

- Debe existir una instancia de servidor de directorios que esté configurada con una base de datos de DB2. Consulte el apartado "Configuración de una base de datos para una instancia con el programa de utilidad de la línea de mandatos" en la página 185.
- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos" en la página 163.

Procedimiento

1. Inicie la sesión como propietario de la instancia de servidor de directorios.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al subdirectorio `sbin` en la ubicación de instalación de IBM Security Directory Server.
4. Para configurar el registro de cambios para la instancia de servidor de directorios, ejecute el mandato **idscfgchglg**.
   - Para configurar el registro de cambios para una instancia sin límite de duración o tamaño, ejecute el mandato **idscfgchglg**:

     ```
     idscfgchglg -I nombre_instancia -m 0
     ```

   - Para configurar el registro de cambios para una instancia con un límite de tamaño de 1.000.000 y una duración de 25 horas, ejecute el mandato **idscfgchglg**:

     ```
     idscfgchglg -I nombre_instancia -m 1000000 -y 1 -h 1
     ```

   Para obtener más información sobre el mandato **idscfgchglg**, consulte *Consulta de mandatos*.

Qué hacer a continuación

Inicie el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos" en la página 163.

Desconfiguración del registro de cambios con Herramienta de configuración

Utilice Herramienta de configuración para desconfigurar la base de datos del registro de cambios desde una instancia de servidor de directorios.

Antes de empezar

Para desconfigurar el registro de cambios de una instancia, la instancia debe cumplir los requisitos siguientes:

- Debe estar configurado el registro de cambios para una instancia. Consulte el apartado "Configuración del registro de cambios con Herramienta de configuración" en la página 206.
- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Procedimiento

1. Inicie Herramienta de configuración para una instancia. Consulte el apartado "Inicio de Herramienta de configuración" en la página 174.
2. Desde la lista de tareas del panel de navegación izquierdo, pulse **Gestionar el registro de cambios**.
3. En la página **Gestionar el registro de cambios**, siga estos pasos:
   a. Para desconfigurar el registro de cambios, borre **Habilitar la base de datos del registro de cambios**.
   b. Para aplicar los cambios, pulse **Actualizar**.
   c. En la ventana **Gestionar el registro de cambios**, pulse **Sí** para confirmar la acción.
   d. Verifique los registros que se generan al desconfigurar la base de datos de registro de cambios.
   e. Para borrar los registros, pulse **Borrar resultados**.
   f. Para cerrar la página **Gestionar registro de cambios**, pulse **Cerrar**.
4. Para cerrar la ventana Herramienta de configuración, pulse **Archivo** > **Salir**.
5. Para confirmar la acción, pulse **Sí**.

Qué hacer a continuación

Inicie el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Desconfiguración del registro de cambios con el programa de utilidad de línea de mandatos

Utilice el programa de utilidad de línea de mandatos, **idsucfgchglg**, para desconfigurar la base de datos de registro de cambios desde una instancia de servidor de directorios.

Antes de empezar

Para desconfigurar el registro de cambios de una instancia, la instancia debe cumplir los requisitos siguientes:

- Debe estar configurado el registro de cambios para una instancia. Consulte el apartado "Configuración del registro de cambios con el programa de utilidad de línea de mandatos" en la página 207.
- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos" en la página 163.

Procedimiento

1. Inicie la sesión como propietario de la instancia de servidor de directorios.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al subdirectorio `sbin` en la ubicación de instalación de IBM Security Directory Server.
4. Para desconfigurar el registro de cambios para una instancia de servidor de directorios, ejecute el mandato **idsucfgchglg** en el formato siguiente:

   ```
   idsucfgchglg -I nombre_instancia
   ```

Para obtener más información sobre el mandato **idsucfgchglg**, consulte *Consulta de mandatos*.

Qué hacer a continuación

Inicie el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos" en la página 163.

Configuración de sufijos

Para crear una jerarquía de directorios, debe configurar el sufijo necesario para la instancia de servidor de directorios.

Un sufijo es conocido como un contexto de denominación. Es un nombre distinguido (DN) que identifica la entrada superior de una jerarquía de directorios. LDAP utiliza el esquema de denominación relativo. Por lo tanto, un DN también es el sufijo para todas las entradas de una jerarquía de directorios. En un servidor de directorios, puede añadir varios sufijos, cada uno de los cuales identifica una jerarquía de directorios. Al añadir un sufijo, la entrada se agrega en el archivo de configuración de una instancia de servidor de directorios. En el ejemplo siguiente se muestra una entrada de sufijo, `o=sample`.

Puede utilizar Herramienta de configuración para agregar o eliminar sufijos. También puede utilizar el mandato **idscfgsuf** para añadir sufijos y el mandato **idsucfgsuf** para eliminar sufijos. Debe detener el servidor de directorios antes de añadir o eliminar un sufijo. Para obtener más información sobre el mandato **idscfgsuf** o **idsucfgsuf**, consulte *Consulta de mandatos*.

No puede eliminar los sufijos definidos por el sistema de una instancia de servidor de directorios. Estos sufijos no están disponibles en una instancia de servidor de proxy. Los siguientes sufijos están definidos por el sistema:

- `cn=localhost`
- `cn=configuration`
- `cn=ibmpolicies`
- `cn=Deleted Objects`

Al añadir entradas en un servidor de directorios, debe tener en cuenta los puntos siguientes:

- Debe añadir una entrada de sufijo en un servidor de directorios para un DN de sufijo.
- Un DN de entrada que añada a un servidor de directorios debe contener un sufijo que coincida con el valor de DN de sufijo. El ejemplo siguiente muestra una entrada con un DN de sufijo, `ou=Marketing,o=sample`.
- No puede añadir una entrada en una instancia de servidor proxy o un servidor de directorios que no esté configurado con una base de datos de DB2.

Si una consulta contiene un sufijo que no coincide con ningún sufijo configurado para la base de datos local, ésta se remitirá al servidor de LDAP identificado por la remisión predeterminada. Si no se ha especificado ninguna remisión predeterminada de LDAP, se generará el siguiente mensaje: `El objeto no existe`.

Adición de un sufijo con Herramienta de configuración

Utilice Herramienta de configuración para añadir un sufijo para una instancia.

Antes de empezar

Para añadir un sufijo para una instancia, debe realizar estos pasos:

- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Acerca de esta tarea

Al añadir un sufijo a una instancia, se añadirá la entrada de sufijo al archivo de configuración de una instancia.

Procedimiento

1. Inicie Herramienta de configuración para una instancia. Consulte el apartado "Inicio de Herramienta de configuración" en la página 174.
2. Desde la lista de tareas del panel de navegación de la izquierda, pulse **Gestionar sufijos**.
3. En la página **Gestionar sufijos**, siga estos pasos:
   a. En el campo DN de sufijo, especifique el sufijo que desea añadir a la instancia.
   b. Pulse **Añadir**.
   c. Para aplicar el cambio, pulse **Aceptar**.
4. Para cerrar la ventana Herramienta de configuración, pulse **Archivo** > **Salir**.
5. Para confirmar la acción, pulse **Sí**.

Qué hacer a continuación

Inicie el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Adición de un sufijo con el programa de utilidad de línea de mandatos

Utilice el programa de utilidad de línea de mandatos, **idscfgsuf**, para añadir un sufijo para una instancia.

Antes de empezar

Para añadir un sufijo para una instancia, debe realizar estos pasos:

- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos" en la página 163.

Acerca de esta tarea

Al añadir un sufijo a una instancia, se añadirá la entrada de sufijo al archivo de configuración de una instancia.

Procedimiento

1. Inicie la sesión como propietario de la instancia de servidor de directorios.
2. Acceda al indicador de mandatos.

3. Cambie el directorio de trabajo actual al subdirectorio `sbin` en la ubicación de instalación de IBM Security Directory Server.
4. Para añadir el sufijo `o=sample` a una instancia, ejecute el mandato **idscfgsuf** en el formato siguiente:

   ```
   idscfgsuf -I nombre_instancia -s "o=sample"
   ```

   Para obtener más información sobre el mandato **idscfgsuf**, consulte *Consulta de mandatos*.

Qué hacer a continuación

Inicie el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos" en la página 163.

Eliminación de un sufijo con Herramienta de configuración

Utilice Herramienta de configuración para eliminar un sufijo de una instancia de servidor de directorios.

Antes de empezar

Para eliminar un sufijo de una instancia de servidor de directorios, debe seguir los pasos siguientes:

- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Acerca de esta tarea

Al eliminar un sufijo en una instancia, se eliminará la entrada del sufijo del archivo de configuración de una instancia.

Procedimiento

1. Inicie Herramienta de configuración para una instancia. Consulte el apartado "Inicio de Herramienta de configuración" en la página 174.
2. Desde la lista de tareas del panel de navegación de la izquierda, pulse **Gestionar sufijos**.
3. En la página **Gestionar sufijos**, siga estos pasos:
   a. Desde la lista **Nombres distinguidos del sufijo actual**, seleccione el sufijo que desee eliminar. Para obtener un servidor de directorios completo, no puede eliminar los siguientes sufijos definidos por el sistema:
      - `cn=localhost`
      - `cn=configuration`
      - `cn=ibmpolicies`
      - `cn=Deleted Objects`

   b. Pulse **Eliminar**.
   c. En la ventana de confirmación **Gestionar sufijos**, pulse **Aceptar**
   d. Para aplicar el cambio, pulse **Aceptar**.
4. Para cerrar la ventana Herramienta de configuración, pulse **Archivo** > **Salir**.
5. Para confirmar la acción, pulse **Sí**.

Qué hacer a continuación

Inicie el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Eliminación de un sufijo con el programa de utilidad de línea de mandatos

Utilice el programa de utilidad de línea de mandatos, **idsucfgsuf**, para eliminar un sufijo de una instancia.

Antes de empezar

Para eliminar un sufijo de una instancia, debe seguir los pasos siguientes:

- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Acerca de esta tarea

Al eliminar un sufijo en una instancia, se eliminará la entrada del sufijo del archivo de configuración de una instancia. Para obtener un servidor de directorios completo, no puede eliminar los siguientes sufijos definidos por el sistema:

- `cn=localhost`
- `cn=configuration`
- `cn=ibmpolicies`
- `cn=Deleted Objects`

Procedimiento

1. Inicie la sesión como propietario de la instancia de servidor de directorios.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al subdirectorio `sbin` en la ubicación de instalación de IBM Security Directory Server.
4. Para eliminar el sufijo `o=sample` de una instancia, ejecute el mandato **idsucfgsuf**:

   ```
   idsucfgsuf -I nombre_instancia -s "o=sample"
   ```

   Para obtener más información sobre el mandato **idsucfgsuf**, consulte *Consulta de mandatos*.

Qué hacer a continuación

Inicie el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos" en la página 163.

Gestión de esquemas

Si desea que una instancia dé soporte a los atributos y a las clases de objetos personalizados, debe añadir un archivo de esquemas que defina los atributos y clases de objetos personalizados.

Puede utilizar Herramienta de configuración o los programas de utilidad de línea de mandatos, como por ejemplo **idscfgsch** o **idsucfgsch**, para gestionar los archivos de esquemas. El archivo de esquemas ya debe existir en el sistema. Para obtener más información sobre el mandato **idscfgsch** o el mandato **idsucfgsch**, consulte *Consulta de mandatos*.

Debe detener el servidor de directorios antes de añadir o eliminar los archivos de esquemas.

Al añadir o eliminar archivos de esquemas, se actualizará el archivo de configuración de la instancia. Puede ejecutar las siguientes operaciones de gestión de esquemas:

- Añadir un archivo de esquemas a la lista de archivos de esquemas que está cargada en el inicio del servidor.
- Eliminar un archivo de esquemas de la lista de archivos de esquemas que se actualiza en el inicio del servidor.
- Cambiar el tipo de comprobación de validación que se realiza para los archivos de esquemas.

No podrá eliminar los siguientes archivos de esquemas definidos por el sistema:

- `V3.config.at`
- `V3.config.oc`
- `V3.ibm.at`
- `V3.ibm.oc`
- `V3.system.at`
- `V3.system.oc`
- `V3.user.at`
- `V3.user.oc`
- `V3.ldapsyntaxes`
- `V3.matchingrules`
- `V3.modifiedschema`

También puede utilizar Herramienta de configuración para especificar la regla de validación de esquemas para comprobar si las entradas cumplen las reglas de esquemas. La regla de validación de esquemas predeterminada es `Versión 3 (Indulgente)`. Las siguientes reglas de validación de esquemas están soportadas por un servidor de directorios:

Versión 3 (Estricta)
El servidor ejecuta la comprobación de validación estricta de LDAP versión 3 en las entradas. Con este tipo de validación, todas las clases de objetos padre deben estar presentes al añadir entradas.

Versión 3 (Indulgente)
El servidor ejecuta la comprobación de validación indulgente de LDAP versión 3 en las entradas. Con este tipo de validación, todas las clases de objetos padre no requieren estar presentes al añadir entradas. LDAP versión 3 indulgente es la regla de validación de esquemas predeterminado.

Versión 2
El servidor ejecuta la comprobación de LDAP versión 2 en las entradas.

Ninguno
El servidor no ejecuta la comprobación de validación.

Gestión de un archivo de esquemas con Herramienta de configuración

Utilice Herramienta de configuración para gestionar los archivos de esquemas para una instancia.

Antes de empezar

Para gestionar los archivos de esquemas para una instancia, debe completar los pasos siguientes:

- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Acerca de esta tarea

Al añadir o eliminar un archivo de esquemas, se actualizará el archivo de configuración de una instancia con la entrada de los esquemas.

Procedimiento

1. Inicie Herramienta de configuración para una instancia. Consulte el apartado "Inicio de Herramienta de configuración" en la página 174.
2. Desde la lista de tareas del panel de navegación izquierdo, pulse **Gestionar archivos de esquemas**.
3. En la página **Gestionar archivos de esquemas**, seleccione la operación que desee ejecutar.
   - Para añadir un archivo de esquemas en el archivo de configuración de una instancia, siga estos pasos:
     a. En el campo **Vía de acceso y nombre del archivo**, especifique el nombre del archivo de esquemas con la vía de acceso. Puede pulsar **Examinar** y especificar el nombre del archivo de esquemas y la ubicación.
     b. Pulse **Añadir**.
   - Para eliminar un archivo de esquemas en el archivo de configuración de una instancia, siga estos pasos:
     a. En la lista **Archivos de esquemas actuales**, seleccione el nombre de archivo de esquemas que desea eliminar.
     b. Pulse **Eliminar**.
     c. En la ventana de confirmación **Gestionar archivos de esquemas**, pulse **Aceptar**.
4. Para aplicar el cambio, pulse **Aceptar**.
5. Para cerrar la ventana Herramienta de configuración, pulse **Archivo** > **Salir**.
6. Para confirmar la acción, pulse **Sí**.

Qué hacer a continuación

Inicie el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Gestión de un archivo de esquemas con el programa de utilidad de línea de mandatos

Utilice los programas de utilidad de línea de mandatos para gestionar los archivos de esquemas para una instancia de servidor de directorios.

Antes de empezar

Para gestionar los archivos de esquemas para una instancia, debe completar los pasos siguientes:

- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos" en la página 163.

Acerca de esta tarea

Al añadir o eliminar un archivo de esquemas, se actualizará el archivo de configuración de una instancia con la entrada de los esquemas.

Procedimiento

1. Inicie la sesión como propietario de la instancia de servidor de directorios.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al subdirectorio `sbin` en la ubicación de instalación de IBM Security Directory Server.
4. Para gestionar un archivo de esquemas para una instancia, elija la operación que desee ejecutar.
   - Para añadir un archivo de esquemas para una instancia, ejecute el mandato **idscfgsch** en el formato siguiente:

     ```
     idscfgsch -I nombre_instancia -s schema_file.oc
     ```

   - Para eliminar un archivo de esquemas de una instancia, ejecute el mandato **idsucfgsch** en el formato siguiente:

     ```
     idsucfgsch -I nombre_instancia -s schema_file.oc
     ```

   Para obtener más información sobre el mandato **idscfgsch** o **idsucfgsch**, consulte *Consulta de mandatos*.

Qué hacer a continuación

Inicie el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos" en la página 163.

Configuración de la comprobación de validación de esquemas con Herramienta de configuración

Utilice Herramienta de configuración para configurar la comprobación de validación de esquemas para una instancia.

Antes de empezar

Para configurar una regla de validación de esquemas para una instancia, debe seguir estos pasos:

- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Acerca de esta tarea

Al configurar la comprobación de validación de esquemas, se actualizará el archivo de configuración de una instancia con el valor.

Procedimiento

1. Inicie Herramienta de configuración para una instancia. Consulte el apartado "Inicio de Herramienta de configuración" en la página 174.
2. Desde la lista de tareas del panel de navegación izquierdo, pulse **Gestionar archivos de esquemas**.
3. En el área **Reglas de validación de esquemas** de la página **Gestionar archivos de esquemas**, elija una de las siguientes reglas de validación de esquemas a configurar:
   - Para configurar la comprobación de validación de LDAP versión 3 estricta, pulse **Versión 3 (Estricta)**.
   - Para configurar la comprobación de validación de LDAP versión 3 indulgente, pulse **Versión 3 (Indulgente)**.
   - Para configurar la comprobación de LDAP versión 2, pulse **Versión 2**.
   - Para configurar la comprobación de LDAP versión 2, pulse **Ninguno**.
4. Para aplicar el cambio, pulse **Aceptar**.
5. Para cerrar la ventana Herramienta de configuración, pulse **Archivo** > **Salir**.
6. Para confirmar la acción, pulse **Sí**.

Qué hacer a continuación

Inicie el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Gestión de datos LDIF

Para utilizar datos de directorios, debe añadir datos a una instancia de servidor de directorios desde una instancia existente o desde un archivo LDIF (LDAP Data Interchange Format).

Puede utilizar Herramienta de configuración para importar datos desde un archivo LDIF o para exportar datos de una base de datos a un archivo LDIF. LDIF se utiliza para representar entradas LDAP en formato de texto. Al importar datos, puede añadir entradas a una base de datos de directorios vacía o a una base de datos que contenga entradas. También puede utilizar Herramienta de configuración para validar los datos del archivo LDIF sin añadir los datos al directorio.

Puede añadir datos a una instancia configurada con una base de datos de DB2. No debe añadir datos de directorios a una instancia de servidor proxy, ya que no está soportado.

Si no desea importar datos LDIF desde otra instancia de servidor, debe sincronizar criptográficamente las instancias de servidor. Debe sincronizar la criptografía bidireccional entre instancias de servidor de directorios para reducir el tiempo

necesario para cifrar y descifrar los datos durante las comunicaciones del servidor. Al importar datos LDIF que no están sincronizados criptográficamente, las entradas cifradas de AES del archivo no se importarán. Para obtener más información sobre la sincronización de la criptografía bidireccional, consulte *Consulta de mandatos*.

Si las instancias de servidor no están sincronizadas criptográficamente, proporcione el inicio de cifrado y el algoritmo de cifrado del servidor de destino al exportar un archivo LDIF desde un servidor de origen. Los datos cifrados de AES se descifrarán utilizando las claves AES del servidor de origen y, a continuación, se cifrarán con los valores de inicio y algoritmo de cifrado del servidor de destino. Estos datos cifrados se almacenan en el archivo LDIF.

Para importar datos, debe cumplir los siguientes requisitos antes de iniciar el proceso:

- La importación o exportación de datos LDIF no está soportada para una instancia de servidor proxy o una instancia no configurada con una base de datos de DB2.
- Añada los sufijos necesarios en el servidor de destino en el que desea importar los datos. Consulte el apartado "Configuración de sufijos" en la página 210.
- Debe detener el servidor de destino en el que desea importar datos.

Una vez que cargue grandes cantidades de datos, como por ejemplo rellenar la base de datos con **idsbulkload**, debe optimizar la base de datos. Esta operación puede mejorar el rendimiento de la base de datos.

También puede utilizar los siguientes programas de utilidad de línea de mandatos para importar, exportar, o validar datos LDIF:

- Para importar datos desde un archivo LDIF, utilice el programa de utilidad **idsldif2db** o **idsbulkload**.
- Para exportar datos a un archivo LDIF, utilice el programa de utilidad **idsdb2ldif**.
- Para validar los datos en el archivo LDIF, utilice el programa de utilidad **idsbulkload**

Para obtener más información sobre los programas de utilidad de línea de mandatos, consulte *Consulta de mandatos*.

Ejemplos

Para recuperar el valor del algoritmo de cifrado de un servidor, ejecute el mandato **idsldapsearch** del formato siguiente:

```
idsldapsearch -h nombre_host -p puerto -D DNadmin -w PWDadmin \
 -b "cn=crypto,cn=localhost" objectclass=* ibm-slapdCryptoSalt

ibm-slapdCryptoSalt=:SxaQ+.qdKor
```

La cadena después del signo igual (=) del atributo `ibm-slapdCryptoSalt` es el algoritmo de cifrado. En el ejemplo, `:SxaQ+.qdKor` es el algoritmo de cifrado.

Importación de datos LDIF con Herramienta de configuración

Utilice Herramienta de configuración para importar datos a una instancia de servidor de directorios desde un archivo LDIF.

Antes de empezar

Para importar datos de un archivo LDIF a una instancia, la instancia debe cumplir los siguientes requisitos:

- Debe existir una instancia de servidor de directorios que esté configurada con una base de datos de DB2. Consulte el apartado "Configuración de una base de datos para una instancia con Herramienta de configuración" en la página 180.
- Se deben configurar las entradas de sufijo necesarias. Consulte el apartado "Adición de un sufijo con Herramienta de configuración" en la página 210.
- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Procedimiento

1. Inicie Herramienta de configuración para una instancia. Consulte el apartado "Inicio de Herramienta de configuración" en la página 174.
2. Desde la lista de tareas del panel de navegación izquierdo, pulse **Tareas LDIF** > **Importar datos LDIF**.
3. En la página **Importar datos LDIF**, siga estos pasos:
   a. En el campo **Vía de acceso y nombre de archivo LDIF**, especifique la vía de acceso y nombre de archivo del archivo LDIF desde el que desea importar datos. También puede pulsar **Examinar** y especificar el nombre de archivo LDIF con la vía de acceso.
   b. Si desea eliminar los espacios finales de los datos, seleccione **Eliminar espacios finales en Importación estándar o carga en bloque**.
   c. En función del número de entradas que desee importar, seleccione una opción adecuada:
      - Para importar los datos utilizando el programa de utilidad **idsldif2db**, pulse **Importación estándar**. Utilice esta opción si el archivo LDIF contiene un número menor de entradas.
      - Para importar los datos utilizando el programa de utilidad **idsbulkload**, pulse **Carga en bloque**. Para los archivos LDIF con un gran número de entradas, el programa de utilidad **idsbulkload** es más rápido que el programa de utilidad **idsldif2db** para importar datos.
   d. Si ha seleccionado la opción **Carga en bloque** para importar datos, especifique los tipos de validación que desea ejecutar de los datos LDIF:
      1) Para verificar si los datos LDIF se ajustan a los esquemas, seleccione **Habilitar comprobación de los esquemas**.
      2) Para verificar si los datos LDIF contienen ACL adecuados, seleccione **Habilitar comprobación de ACL**.
   e. Para iniciar la operación de importación, pulse **Importar**.
   f. Para confirmar la finalización de la tarea, pulse **Aceptar**.
   g. Verifique los registros generados para la operación de importación del archivo LDIF.
   h. Para borrar los registros, pulse **Borrar resultados**.
   i. Para cerrar la página **Importar datos LDIF**, pulse **Cerrar**.
4. Para cerrar la ventana Herramienta de configuración, pulse **Archivo** > **Salir**.
5. Para confirmar la acción, pulse **Sí**.

Qué hacer a continuación

Inicie el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175. Una vez que cargue grandes cantidades de datos, como por ejemplo rellenar la base de datos con **idsbulkload**, debe optimizar la base de datos. Para obtener más información sobre la optimización de la base de datos, consulte "Optimización de bases de datos con Herramienta de configuración" en la página 192.

Validación de datos de LDIF con Herramienta de configuración

Utilice Herramienta de configuración para validar un archivo LDIF en los esquemas del servidor de directorios sin añadir los datos a la base de datos.

Antes de empezar

Para validar datos en un archivo LDIF con los esquemas del servidor de directorios, la instancia debe cumplir los requisitos siguientes:

- Debe existir una instancia de servidor de directorios que esté configurada con una base de datos de DB2. Consulte el apartado "Configuración de una base de datos para una instancia con Herramienta de configuración" en la página 180.
- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Procedimiento

1. Inicie Herramienta de configuración para una instancia. Consulte el apartado "Inicio de Herramienta de configuración" en la página 174.
2. Desde la lista de tareas del panel de navegación izquierdo, pulse **Tareas LDIF** > **Importar datos LDIF**.
3. En la página **Importar datos LDIF**, siga estos pasos:
   a. En el campo **Vía de acceso y nombre de archivo LDIF**, especifique la vía de acceso y nombre de archivo del archivo LDIF desde el que desea importar datos. También puede pulsar **Examinar** y especificar el nombre de archivo LDIF con la vía de acceso.
   b. Pulse **Sólo validación de datos**.
   c. Para iniciar la operación de validación de datos, pulse **Importar**.
   d. Para confirmar la finalización de la tarea, pulse **Aceptar**.
   e. Verifique los registros que se generan para la operación de validación de datos.
   f. Para borrar los registros, pulse **Borrar resultados**.
   g. Para cerrar la página **Importar datos LDIF**, pulse **Cerrar**.
4. Para cerrar la ventana Herramienta de configuración, pulse **Archivo** > **Salir**.
5. Para confirmar la acción, pulse **Sí**.

Qué hacer a continuación

Inicie el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Exportación de datos LDIF con Herramienta de configuración

Utilice Herramienta de configuración para exportar datos de directorio desde una instancia a un archivo LDIF.

Antes de empezar

Para exportar datos de una instancia a un archivo LDIF, la instancia debe cumplir los siguientes requisitos:

- Debe existir una instancia de servidor de directorios que esté configurada con una base de datos de DB2. Consulte el apartado "Configuración de una base de datos para una instancia con Herramienta de configuración" en la página 180.
- La instancia debe contener entradas de directorio.

Procedimiento

1. Inicie Herramienta de configuración para una instancia. Consulte el apartado "Inicio de Herramienta de configuración" en la página 174.
2. Desde la lista de tareas del panel de navegación izquierdo, pulse **Tareas LDIF** > **Exportar datos LDIF**.
3. En la página **Exportar datos LDIF**, siga estos pasos:
   a. En el campo **Vía de acceso y nombre de archivo LDIF**, especifique la vía de acceso y el nombre de archivo del archivo LDIF al que desee exportar datos. También puede pulsar **Examinar** y especificar el nombre de archivo LDIF con la vía de acceso.
   b. Si existe el archivo y desea sobrescribir el archivo con datos, seleccione **Sobrescribir si existe el archivo**.
   c. Si desea exportar los atributos de la operación, como por ejemplo `creatorsName`, `createTimestamp`, `modifiersName`, y `modifyTimestamp`, seleccione **Exportar atributos operativos**. Los atributos operativos los crea y modifica el servidor cuando se crea o modifica una entrada de directorio. Los atributos contienen información sobre el usuario que ha creado o modificado la entrada y la hora en que se ha creado o modificado la entrada. Estas entradas se almacenan como un control codificado de base 64 en el archivo LDIF.
   d. Para importar datos en un servidor de destino habilitado para AES (Advanced Encryption Standard) y si el servidor no está sincronizado criptográficamente con el servidor de origen, seleccione **Exportar datos para el servidor de destino habilitado para AES**.
   e. Para exportar entradas que se han suprimido pero que aún se almacenan en el subárbol de marcador de exclusión, seleccione **Exportar entradas suprimidas**. Para obtener más información acerca del subárbol tombstone, consulte la sección Administración en la documentación de IBM Security Directory Server.
   f. Si ha seleccionado **Exportar datos para el servidor de destino habilitado para AES**, especifique los valores siguientes:
      - En el campo **Inicio de cifrado**, especifique el inicio de cifrado del servidor de destino.
      - En el **Inicio de cifrado** archivado, especifique el algoritmo de cifrado del servidor de destino. Para obtener más información sobre cómo recuperar el algoritmo de cifrado, consulte "Gestión de datos LDIF" en la página 217.
   g. Para especificar un filtro para entradas exportadas en un archivo LDIF, especifique el nombre distinguido de un filtro de réplica válido en el campo

Nombre distinguido de entrada de filtro. El filtro exporta entradas de base de datos específicas que cumplen los criterios para el archivo LDIF. Para obtener más información acerca de los filtros de réplica, consulte la sección Administración en la documentación de IBM Security Directory Server.

h. Si desea añadir comentarios al archivo LDIF, especifique comentarios en el campo **Comentarios**.

i. Si desea exportar entradas en un subárbol específico, especifique el nombre distinguido del subárbol en el campo **Nombre distinguido del subárbol**. El nombre distinguido del subárbol identifica la entrada superior del subárbol para que se grabe en el archivo LDIF. El subárbol y todas las entradas del mismo de la jerarquía del directorio se graban en el archivo. Si no especifica un nombre distinguido de subárbol, todas las entradas de directorio que se almacenen en la base de datos se grabarán en el archivo de salida. Las entradas se identifican en función de los sufijos que se especifican en el archivo de configuración de la instancia de servidor de directorios.

j. Para iniciar la operación de exportación, pulse **Exportar**.

k. Para confirmar la finalización de la tarea, pulse **Aceptar**.

l. Verifique los registros que se generan para la operación de exportación de datos LDIF.

m. Para borrar los registros, pulse **Borrar resultados**.

n. Para cerrar la página **Exportar datos LDIF**, pulse **Cerrar**.

4. Para cerrar la ventana Herramienta de configuración, pulse **Archivo** > **Salir**.
5. Para confirmar la acción, pulse **Sí**.

Sincronización de Active Directory

Puede sincronizar las entradas del contenedor de usuarios y de grupos que se encuentran en Microsoft Active Directory con una instancia de IBM Security Directory Server. La sincronización de datos es un modo de Active Directory en una instancia de servidor de directorios.

Nota: Desde IBM Security Directory Server, versión 6.3.1, la solución de sincronización Active Directory está en desuso. En su lugar, utilice la solución LDAPSync.

Puede utilizar Herramienta de configuración o los programas de utilidad de la línea de mandatos, como por ejemplo **idsadscfg** e **idsadsrun**, para configurar y ejecutar la sincronización de Active Directory.

Nota: La sincronización de usuarios y grupos de Active Directory en una instancia de IBM Security Directory Server a través de IBM Security Directory Proxy Server no está soportada.

La sincronización de Active Directory utiliza IBM Security Directory Integrator para sincronizar los contenedores de usuarios y grupos. Debe instalar IBM Security Directory Integrator antes de utilizar la sincronización de Active Directory.

IBM Security Directory Integrator es necesario para las siguientes acciones:

- Ejecutar la configuración
- Iniciar, detener, reiniciar, y supervisar las operaciones

Debe tener en cuenta los puntos siguientes al configurar la sincronización de Active Directory:

- La aplicación de sincronización de Active Directory y IBM Security Directory Integrator deben estar en el mismo sistema que la instancia de servidor de directorios.
- La sincronización de Active Directory sincroniza sólo el contenedor de usuarios y de grupos. La herramienta no sincroniza otros objetos o contenedores en una instancia de servidor de directorios.
- La solución también comprueba las pertenencias a grupos de la entrada de usuario y la entrada de usuario se añadirá a cualquier grupo de la instancia que esté sincronizado con Active Directory. Cuando una entrada de usuario existente se traslada de contenedor de usuario, la entrada de usuario se suprime de la instancia. La entrada de usuario también se suprime de todos los grupos de la instancia.
- La sincronización de Active Directory no sincroniza unidades organizativas anidadas (`ou`).
- Varios atributos de Active Directory no se pueden correlacionar con un solo atributo en una instancia de servidor de directorios.
- El atributo `userpassword` de Active Directory no se puede correlacionar con una instancia de servidor de directorios. La contraseña de usuario no está sincronizada por esta solución.
- La sincronización de Active Directory puede sincronizar usuarios y grupos de uno o varios contenedores de usuarios de Active Directory a una unidad organizativa única (`ou`) de un servidor de directorios. Sin embargo, la herramienta no sincroniza varios contenedores de usuarios y grupos de Active Directory en varias unidades organizativas (`ou`) de un servidor de directorios.
- Puede especificar varios contenedores de usuarios para que se sincronicen con una unidad organizativa única (`ou`) en un servidor de directorios con el punto y coma (`;`) como separador. El uso de otros caracteres como separadores no está soportado. Si utiliza el punto y coma (`;`) como separador, especifique el argumento entre comillas (`"`). El ejemplo siguiente muestra el punto y coma (`;`) como separador:
  `"ou=SWUGroups,dc=adsync,dc=com;ou=STGGroups,dc=adsync,dc=com"`.
- El atributo `SAMAccountName` de Active Directory se utiliza para componer el atributo `$dn` en IBM Security Directory Server. El atributo `SAMAccountName` es exclusivo en un dominio, no hay conflictos al sincronizar varios contenedores de usuarios de Active Directory en una unidad organizativa única de un servidor de directorios.
- La solución da soporte a una conexión segura con Active Directory, pero no da soporte a una conexión segura en una instancia de servidor de directorios.
- Si cambia el nombre distinguido del administrador, la contraseña, o ambos, para una instancia de servidor de directorios tras configurar la sincronización de Active Directory, debe volver a configurar la sincronización de Active Directory.
- Si se cambian los contenedores de usuarios o de grupos de Active Directory cuando se ejecuta la sincronización de Active Directory, debe volver a configurar la sincronización de Active Directory con los nombres modificados. De lo contrario, es posible que no se ejecute el programa de sincronización de Active Directory.
- Si modifica los usuarios y los grupos de IBM Security Directory Server desde cualquier otra herramienta que no sea la sincronización de Active Directory, es posible que la sincronización de Active Directory no funcione correctamente.

Configuración y ejecución de la sincronización de Active Directory

Para sincronizar los contenedores de usuario y grupo de Active Directory en una instancia de IBM Security Directory Server, configure y ejecute la sincronización de Active Directory.

Antes de empezar

Para configurar e iniciar la sincronización de Active Directory, debe instalar el software siguiente:

- IBM Security Directory Server
- IBM Security Directory Integrator

Procedimiento

1. Si ha instalado IBM Security Directory Integrator en una vía de acceso personalizada, establezca la variable de entorno *IDS_LDAP_TDI_HOME* con la vía de acceso de instalación.

   Nota: En sistemas Windows, establezca la variable de entorno con una vía de acceso de instalación que no contenga espacios ni comillas. Utilice el nombre abreviado al especificar la vía de acceso.
   La siguiente vía de acceso es la vía de acceso de instalación predeterminada de IBM Security Directory Integrator:

   AIX y Solaris
   `/opt/IBM/TDI/V7.1`

   Linux `/opt/ibm/TDI/V7.1`

   Windows
   `C:\Program Files\IBM\TDI\V7.1`
2. Opcional: Cargue los archivos `users.ldif` y `groups.ldif` de ejemplo en Active Directory.
3. Ejecute el mandato **idsadscfg** para configurar la sincronización de Active Directory. También puede ejecutar Herramienta de configuración para configurar la sincronización de Active Directory. El mandato crea los archivos `adsync_private.prop` y `adsync_public.prop`.
4. Modifique el archivo `adsync_public.prop` para personalizar los atributos opcionales y los parámetros SSL. Para obtener más información acerca de cómo proteger las comunicaciones, consulte la sección *Administración* en la documentación de IBM Security Directory Server.
5. Ejecute el mandato **idsadsrun** para iniciar la sincronización de Active Directory. El mandato le indicará si desea sincronizar completamente, seguido de la sincronización a tiempo real, o iniciar la sincronización a tiempo real. La herramienta de sincronización de Active Directory identifica los cambios en las entradas de Active Directory y los sincroniza con las entradas de IBM Security Directory Server.
6. Opcional: Ejecute IBM Security Directory Integrator Administration and Monitoring Console para administrar y supervisar la sincronización.

Configuración de la sincronización de Active Directory con Herramienta de configuración

Utilice Herramienta de configuración para configurar la sincronización de Active Directory con una instancia de servidor de directorios.

Antes de empezar

Para configurar la sincronización de Active Directory, debe cumplir los requisitos siguientes:

- Instale IBM Security Directory Integrator.
- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con Herramienta de configuración" en la página 175.

Procedimiento

1. Inicie Herramienta de configuración para una instancia. Consulte el apartado "Inicio de Herramienta de configuración" en la página 174.
2. Desde la lista de tareas en el panel de navegación izquierdo, pulse **Sincronización de Active Directory**.
3. En la página **Sincronización de Active Directory: Detalles de instancia**, proporcione los detalles de configuración para la instancia de IBM Security Directory Server. La información que proporcione se guardará en los archivos `adsync_private.properties` y `adsync_public.properties`. Los archivos se almacenan en el subdirectorio `etc/tdisoldir` del directorio de inicio de la instancia.
4. En el campo **Sufijo de directorio**, especifique el sufijo del servidor de directorios que desea utilizar para la sincronización de Active Directory. El campo **LDAP URL** se rellena con el URL para la instancia de servidor de directorios. Este campo no puede editarse.
5. En el campo **DN de entrada del contenedor de grupos**, especifique el DN de un contenedor existente en el que desea copiar grupos desde Active Directory. Los grupos y las pertenencias de los usuarios a grupos están sincronizados entre Active Directory e IBM Security Directory Server. Al añadir o eliminar un usuario de un grupo en Active Directory, la entrada se añade o se elimina del grupo correspondiente en la instancia de IBM Security Directory Server.
6. En el campo **DN de entrada del contenedor de usuarios**, especifique el DN de un contenedor existente en el que desea copiar usuarios desde Active Directory.
7. Si desea utilizar una conexión SSL con Active Directory, seleccione **Utilizar conexión SSL con Active Directory**. La conexión SSL para IBM Security Directory Server no está soportada. Para obtener más información acerca de los pasos para configurar una conexión SSL con Active Directory, consulte la sección *Administración* de la documentación de IBM Security Directory Server.
8. Pulse **Siguiente**. Se abrirá la página **Sincronización de Active Directory: Detalles de Active Directory**.
9. En el campo **Dirección de host**, especifique el nombre de host o la dirección IP del controlador de dominios de Active Directory.
10. En el campo **Puerto de host**, especifique el puerto que utiliza Active Directory.
11. En el campo **Nombre de inicio de sesión**, especifique el nombre de inicio de sesión que IBM Security Directory Integrator debe utilizar para enlazarse con Active Directory. El ID de inicio de sesión debe contener el permiso necesario para leer las entradas de Active Directory que se propagarán a la instancia de servidor de directorios.
12. En el campo Contraseña de inicio de sesión, especifique la contraseña que IBM Security Directory Integrator debe utilizar para enlazarse con Active Directory.

13. En el campo **Base de búsqueda**, especifique el subárbol de Active Directory en el que desea propagar los cambios en la instancia. Los cambios en las entradas de usuarios del subárbol se propagan a la instancia de servidor de directorios. Para propagar todos los usuarios de los grupos de Active Directory a la instancia, configure la base de búsqueda en la parte superior de la jerarquía de Active Directory.
14. En el campo **DN de entrada del contenedor de grupos**, especifique el DN del contenedor de Active Directory desde el que desea sincronizar los grupos en la instancia.
15. En el campo **DN de entrada del contenedor de usuarios**, especifique el DN del contenedor de Active Directory desde el que desea sincronizar las entradas de usuarios en la instancia.
16. Pulse **Finalizar**. Se abrirá la ventana **Sincronización de Active Directory: Resultados**.
17. Verifique los mensajes de registro que se generan para la configuración de sincronización de Active Directory.
18. Para borrar los registros, pulse **Borrar resultados**.
19. Para cerrar la página **Sincronización de Active Directory**, pulse **Cerrar**.
20. Para cerrar la ventana Herramienta de configuración, pulse **Archivo** > **Salir**.
21. Para confirmar la acción, pulse **Sí**.

Configuración de la sincronización de Active Directory con el programa de utilidad de línea de mandatos

Utilice el programa de utilidad de línea de mandatos, **idsadscfg**, para configurar la sincronización de Active Directory con una instancia de servidor de directorios.

Antes de empezar

Para configurar la sincronización de Active Directory, debe cumplir los requisitos siguientes:

- Instale IBM Security Directory Integrator.
- Detenga el servidor de directorios. Consulte el apartado "Inicio o detención de un servidor de directorios y un servidor de administración con los programas de utilidad de línea de mandatos" en la página 163.

Procedimiento

1. Inicie sesión como root en AIX, Linux, o Solaris, y como miembro de grupo de administradores en Windows.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al subdirectorio `sbin` en la ubicación de instalación de IBM Security Directory Server.
4. Para configurar la sincronización de Active Directory con una instancia, ejecute el mandato **idsadscfg** en el formato siguiente:

   ```
   idsadscfg -I nombre_instancia -adH ldap://LDAP_server1:389 -adb dc=adsynctest,dc=com
   -adD cn=administrator,cn=users,dc=adsynctest,dc=com -adw secret -adg ou=testgroup1,
   dc=adsynctest,dc=com -adu ou=testuser1,dc=adsynctest,dc=com -idss o=sample -idsg
   ou=Testgroup1,ou=groups,o=sample -idsu ou=Testuser1,ou=users,o=sample
   ```

   Para obtener más información sobre el mandato **idsadscfg**, consulte *Consulta de mandatos*.

Qué hacer a continuación

Ejecute el mandato **idsadsrun** para iniciar la sincronización de Active Directory. Para obtener más información sobre el mandato **idsadsrun**, consulte *Consulta de mandatos*.

Capítulo 21. Inicio automático de las instancias de servidor de directorios al iniciar el sistema operativo

Puede configurar las instancias de servidor de directorios para que se inicien automáticamente cuando se reinicie un sistema una vez que se cierre para su mantenimiento o actualización.

Al crear una instancia de servidor de directorios, el servidor de administración se inicia si la creación de la instancia ha sido satisfactoria. Para iniciar un servidor de directorios con la base de datos de DB2, debe iniciar el proceso de `ibmslapd` o `idsslapd` para la instancia.

Al reiniciar un sistema, debe iniciar el servidor de administración y el proceso de `ibmslapd` asociado con la instancia. Sin embargo, puede configurar los servicios y procesos que están asociados con una instancia para que se inicien automáticamente en el sistema operativo.

Para iniciar la instancia de servidor de directorios en AIX, Linux, o Solaris al iniciar el sistema operativo, debe actualizar el archivo `/etc/inittab` con la información del servidor. El archivo `inittab` especifica los procesos que se deben iniciar al iniciar el sistema y durante el funcionamiento normal. Debe añadir una entrada para el servidor de directorios en el archivo `inittab` en el formato siguiente:

```
id:runlevels:action:process
```

Los atributos del archivo `inittab` requieren los siguientes valores:

id Este atributo especifica un ID exclusivo de 1 a 4 dígitos en el archivo.

runlevels
El atributo `runlevels` indica la modalidad `runlevel` del sistema operativo en el que se inicia automáticamente el proceso. Hace referencia a la modalidad de operación de un sistema operativo AIX, Linux, o Solaris. La configuración del atributo `runlevels` difiere entre sistemas operativos. Consulte el manual del sistema operativo para ver detalles específicos de configuración de `runlevel`.

action La `action` especifica el tipo de acción.

process
El atributo `process` especifica el proceso a iniciar.

Configuración del inicio automático para una instancia de servidor de directorios en Windows

Utilice la ventana **Servicios** para configurar el inicio automático de una instancia de servidor de directorios en Windows.

Antes de empezar

Para configurar una instancia de servidor de directorios para que se inicie automáticamente una vez que inicie el sistema operativo, el sistema debe cumplir los requisitos siguientes:

- El sistema debe contener una instancia de servidor de directorios que se pueda ejecutar en modalidad normal.

Acerca de esta tarea

En Windows, puede iniciar un servidor de directorios, el proceso `idsslapd`, desde la ventana **Servicios** o con el mandato **`idsslapd`**. Para una instancia de servidor de directorios con la base de datos de DB2, debe configurar el servicio asociado con el servidor de directorios para que dependa del servicio de instancias de DB2. Para una instancia de servidor de directorios con base de datos de DB2, se debe iniciar DB2 antes de iniciar el proceso `idsslapd`. Si no establece la dependencia y configura el campo **Tipo de inicio** en `Automático` para el servicio que está asociado con el servidor, se pueden producir errores al reiniciar el sistema. Para una instancia de servidor proxy, no necesita configurar la dependencia en el servicio asociado con la instancia de DB2.

Para una instancia de servidor proxy, utilice 1, 2, 4, 5, y los pasos de 6.

Procedimiento

1. Inicie sesión como miembro de grupo administrador.
2. Para abrir la ventana **Servicios**, siga estos pasos:
   a. Pulse **Inicio** > **Ejecutar**.
   b. En el campo **Abrir**, especifique `services.msc`.
   c. Pulse **Aceptar**.
3. Busque el nombre del servicio de DB2 asociado con la instancia de servidor de directorios que desea iniciar automáticamente. El nombre del servicio empieza por `DB2 - SDSV631DB2 -`. Si el nombre de la instancia de DB2 es `DSRDBM01`, la entrada será `DB2 - SDSV631DB2 - DSRDBM01`. Efectúe una doble pulsación en el servicio y registre el valor que se proporciona después de `DB2 - SDSV631DB2 -` en el campo **Nombre de visualización**. En el ejemplo, el valor será `DSRDBM01`.
4. Busque el servicio para la instancia de servidor de directorios que desee iniciar automáticamente. El nombre del servicio empieza por `IBM Security Directory Server Instance 6.3.1`. Si el nombre de la instancia es `dsrdbm01`, la entrada será `IBM Security Directory Server Instance 6.3.1 - dsrdbm01`. Efectúe una doble pulsación en el servicio y registre el valor que viene después de `IBM Security Directory Server Instance 6.3.1 -` en el campo **Nombre de visualización**. En el ejemplo, para la instancia, `dsrdbm01`, el valor será `idsslapd-dsrdbm01`.
5. En la ventana de Propiedades `IBM Security Directory Server Instance 6.3.1 - dsrdbm01`, desde la lista **Tipo de inicio**, seleccione `Automático`.
6. Pulse **Aceptar**.
7. Para cerrar la ventana **Servicios**, pulse **Archivo** > **Salir**.
8. Para abrir el registro de Windows, siga estos pasos:
   a. Pulse **Inicio** > **Ejecutar**.
   b. En el campo **Abrir**, especifique `regedit`.
   c. Pulse **Aceptar**.
9. En el panel de navegación izquierdo, vaya a **Mi PC** > **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Servicios**.
10. Busque el servicio asociado con la instancia de servidor de directorios. En el ejemplo, es `idsslapd-dsrdbm01`.
11. Pulse el servicio asociado con la instancia.

12. En el panel derecho de la ventana, efectúe una doble pulsación en el atributo `DependOnService`.
13. En la ventana **Editar cadenas múltiples**, añada el nombre de servicio de DB2 asociado con la instancia de **LanmanServer**. En el ejemplo, será `DSRDBM01`.
14. Pulse **Aceptar**. Crea una dependencia en el servicio de DB2.
15. Para cerrar el registro de Windows, pulse **Archivo** > **Salir**.

Resultados

Al reiniciar el sistema, la instancia de servidor de directorios se iniciará automáticamente.

Configuración del inicio automático para una instancia de servidor de directorios en UNIX

Actualice el archivo `/etc/inittab` con entradas del servidor de directorios para configurar el inicio automático de una instancia de servidor de directorios en AIX, Linux, o Solaris.

Antes de empezar

Para configurar una instancia de servidor de directorios para que se inicie automáticamente una vez que inicie el sistema operativo, el sistema debe cumplir los requisitos siguientes:

- El sistema debe contener una instancia de servidor de directorios que se pueda ejecutar en modalidad normal.

Procedimiento

1. Inicie sesión como usuario root.
2. Para configurar una instancia de servidor de directorios o una instancia de servidor proxy para el inicio automático, añada las siguientes entradas en el archivo `/etc/inittab`:
   a. Para añadir el proceso `idsslapd` y el servidor de administración que está asociado con una instancia de servidor de directorios, añada las entradas siguientes:

      AIX
      ```
      srv1:2:once:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I nombre_instancia > /dev/null 2>&1 #Autostart IBM Directory Server Instance

      adm1:2:once:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I nombre_instancia > /dev/null 2>&1 #Autostart IBM Directory Administration Server
      ```

      Linux
      ```
      srv1:2345:once:/opt/ibm/ldap/V6.3.1/sbin/ibmslapd -I nombre_instancia > /dev/null 2>&1 #Autostart IBM Directory Server Instance

      adm1:2345:once:/opt/ibm/ldap/V6.3.1/sbin/ibmdiradm -I nombre_instancia > /dev/null 2>&1 #Autostart IBM Directory Administration Server
      ```

      Solaris
      ```
      srv1:234:once:/opt/IBM/ldap/V6.3.1/sbin/ibmslapd -I nombre_instancia > /dev/null 2>&1 #Autostart IBM Directory Server Instance
      ```

```
adm1:234:once:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I
nombre_instancia > /dev/null 2>&1 #Autostart IBM Directory
Administration Server
```

Sustituya la variable *nombre_instancia* por el nombre de la instancia.

b. Para añadir el proceso `idsslapd` y el servidor de administración que está asociado con una instancia de servidor proxy, debe iniciar en primer lugar las instancias de servidor de directorios. Debe iniciar todos los servidores de directorios con la base de datos de DB2 antes de iniciar el servidor proxy. Si el sistema contiene servidores de directorios completos y un servidor proxy, añada un retardo entre el servidor de directorios completo y el arranque del servidor proxy. En el ejemplo siguiente, el retardo se ha introducido añadiendo una entrada del formato siguiente, `id:2345:wait`, el archivo `/etc/inittab`.

AIX

```
srv1:2345:once:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I
nombre_instancia1 > /dev/null 2>&1 #Autostart IBM Directory
Server Instance

adm1:2345:once:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I
nombre_instancia1 > /dev/null 2>&1 #Autostart IBM Directory
Administration Server

srv2:2345:once:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I
nombre_instancia2 > /dev/null 2>&1 #Autostart IBM Directory
Server Instance

adm2:2345:once:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I
nombre_instancia2 > /dev/null 2>&1 #Autostart IBM Directory
Administration Server

srv3:2345:wait:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I
instancia_proxy1 -k > /dev/null 2>&1 #Autostart IBM Directory
Proxy Server Instance

adm3:2345:wait:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I
instancia_proxy1 -k > /dev/null 2>&1 #Autostart IBM Directory
Administration Server

srv4:2345:wait:/opt/IBM/ldap/V6.3.1/sbin/idsslapd -I
instancia_proxy1 > /dev/null 2>&1 #Autostart IBM Directory
Proxy Server Instance

adm4:2345:wait:/opt/IBM/ldap/V6.3.1/sbin/ibmdiradm -I
instancia_proxy1 > /dev/null 2>&1 #Autostart IBM Directory
Administration Server
```

Sustituya las variables *nombre_instancia1* y *nombre_instancia2* por los nombres de instancias de servidor de directorios. Sustituya la variable *instancia_proxy1* por el nombre de instancia de servidor proxy.

Resultados

Una vez que se hayan añadido las entradas al archivo `/etc/inittab`, se podrá iniciar automáticamente la instancia de servidor de directorios (completo o proxy) tras el reinicio del sistema.

Capítulo 22. Estrategia del fixpack

Obtenga información acerca de los fixpacks y parches para IBM Security Directory Server.

En AIX, Linux, Solaris y HP-UX, los parches o fixpacks están disponibles para una instalación nativa basada en scripts.

En Windows, hay disponibles parches y fixpacks basados en IBM Installation Manager.

Los parches o fixpacks basados en IBM Installation Manager se pueden instalar en la interfaz gráfica de usuario y en la modalidad de instalación silenciosa.

La versión del parche o fixpack instalado se puede identificar con IBM Installation Manager de cualquiera de las siguientes maneras:

- Seleccione **Archivo** > **Ver paquetes instalados**
- Utilice el mandato **imcl** desde el directorio de herramientas del directorio de instalación de IBM Installation Manager.

En sistemas UNIX, compruebe las versiones de los paquetes nativos para determinar la versión del parche o fixpack instalado.

Nota: Una vez aplicado el fixpack basado en el método nativo en la versión base, IBM Installation Manager no debe realizar ninguna tarea de modificación o desinstalación. Después de aplicar el fixpack nativo, utilice únicamente el método nativo para las operaciones adicionales.

Instalación de fixpacks con IBM Installation Manager

IBM Installation Manager sirve para aplicar fixpacks o para instalar mejoras en la secuencia de servicios en sistemas operativos Microsoft Windows.

Antes de empezar

- Consulte la información sobre la estrategia de fixpacks.
- Asegúrese de que IBM Installation Manager, versión 1.7.0 o superior está instalado en su sistema. Consulte la documentación de IBM Installation Manager.
- Antes de iniciar la instalación de fixpacks, debe detener todos los servicios o procesos en ejecución de IBM Security Directory Server. Puede hacer esto manualmente o pulsando **Detener todos los procesos que bloquean** en Installation Manager.

Acerca de esta tarea

El fixpack únicamente actualiza aquellas características que ya estaban instaladas. Debe actualizar el producto antes de utilizar el asistente **Modificar** para instalar características que todavía no están instaladas en su sistema.

El fixpack no actualiza IBM DB2, IBM GSKit, IBM Embedded WebSphere Application Server ni IBM Java Development Kit. Utilice el asistente **Modificar** para actualizar dicho software.

Procedimiento

1. Descargue los fixpacks desde http://www-01.ibm.com/support/docview.wss?uid=swg21496581#v631.
2. Establezca las preferencias del repositorio en IBM Installation Manager.
   a. Para iniciar IBM Installation Manager, desde el menú **Inicio**, pulse **Todos los programas** > **IBM Installation Manager** > **IBM Installation Manager**.
   b. En la página Inicio de IBM Installation Manager, pulse **Archivo** > **Preferencias**.
   c. En la página Repositorios, pulse **Añadir repositorio**.
   d. En la página Añadir repositorio, especifique una de las siguientes ubicaciones de repositorio:
      - Vía de acceso de archivos a un directorio local o una unidad compartida remota que contenga el paquete de producto que se descarga desde el sitio web de soporte de IBM.
      - URL para el repositorio en un servidor web.
   e. Pulse **Aceptar**. Si ha proporcionado un HTTPS o una ubicación de repositorio restringida, se le solicitará que especifique un ID de usuario y una contraseña. Se listará la ubicación de repositorio nueva o modificada.
   f. Para verificar el acceso de repositorio, pulse **Probar conexiones**.
   g. Pulse **Aceptar** para salir de la página Repositorios.
3. Inicie la instalación.
   - Si IBM Security Directory Server Versión 6.3.1 no está instalado en el sistema, siga los siguientes pasos:
     a. En la página de Inicio de IBM Installation Manager, pulse **Instalar**. El asistente **Instalar** le guiará a través del proceso de instalación.
     b. Complete el procedimiento de instalación que se describe en "Instalación con IBM Installation Manager" en la página 31.
   - Si IBM Security Directory Server Versión 6.3.1 está instalado en el sistema, siga los siguientes pasos para aplicar el fixpack:
     a. En la página de Inicio de IBM Installation Manager, pulse **Actualizar**. El asistente **Actualizar** busca actualizaciones disponibles para los paquetes instalados en el sistema.
     b. Seleccione **IBM Security Directory Server**. El directorio de instalación es el directorio en el que se instaló la versión 6.3.1 y no es posible cambiarlo. Pulse **Siguiente**.
     c. Seleccione el producto a actualizar, **IBM Security Directory Server** y, a continuación, seleccione la actualización a aplicar, **Versión 6.3.1.5**. Pulse **Siguiente**.
     d. Acepte la licencia para el fixpack y, a continuación, pulse **Siguiente**.
     e. De forma predeterminada, se seleccionan las características a actualizar. Únicamente se visualizarán para ser actualizadas las características que se instalaron de forma previa en el sistema. Pulse **Siguiente**.

        Nota: Si intenta desmarcar cualquiera de las selecciones, se marca para desinstalar la característica.

        Restricción: A pesar de que se lista IBM DB2 en esta página como una característica y que se selecciona para ser actualizada de forma predeterminada, esta característica no se actualiza. El software requisito previo no se actualiza al seleccionar el asistente **Actualizar** en IBM

Installation Manager. No desmarque la selección de IBM DB2 porque la característica de servidor también se desmarca.

f. En la página de resumen, revise la información y, a continuación, pulse **Siguiente** para iniciar la instalación.

4. Verifique la instalación. Para obtener información sobre la verificación con IBM Installation Manager y la verificación del sistema operativo que le corresponda, consulte la sección Capítulo 13, “Verificación de las características de IBM Security Directory Server”, en la página 85.

Qué hacer a continuación

Para desinstalar el fixpack, utilice el asistente de **Retrotraer**, que revierte a la versión anterior del paquete.

Instalación en modalidad silenciosa para fixpacks

Puede utilizar IBM Installation Manager para instalar fixpacks en la modalidad silenciosa.

Nota: En un archivo de respuestas para las actualizaciones, no se puede proporcionar una característica que no esté ya instalada. Si lo hace, el proceso de actualización de fixpacks fallará.

Generación de un nuevo archivo de respuestas para la instalación de fixpacks

Si el archivo de respuestas que se utilizó durante la instalación del producto no está disponible, grabe un nuevo archivo de respuestas.

1. Inicie IBM Installation Manager en una modalidad de instalación simulada. Por ejemplo:

   ```
   C:\Program Files\IBM\Installation Manager\eclipse\IBMIM.exe
        -record c:\SDS_6310\install_resp.xml -skipInstall agentDataLocation
   ```

   donde

   La ubicación *agentDataLocation* almacena los datos para instalar el producto.
2. Establezca las preferencias del repositorio en la versión 6.3.1.0.
3. Complete el proceso de instalación simulado.
4. Cierre IBM Installation Manager. Se creará un archivo de respuesta para el proceso de instalación sin instalar el producto.
5. Complete los pasos de la siguiente sección.

Instalación con el archivo de respuestas que se utilizó durante la instalación del producto

1. Edite el archivo de respuestas `install_resp.xml`, y realice los siguientes cambios:
   a. Actualice la vía de acceso al repositorio con la vía de acceso al repositorio de la versión 6.3.1.5.

      ```
      <repository location='C:\SDS_6315\ibm_sds'/>
      ```

   b. Actualice la versión en offering a 6.3.1.5.

      ```
      <offering id='com.ibm.security.directoryserver.v631' version='6.3.1.5' profile=.......
      ```
2. Inicie la instalación en modalidad silenciosa para aplicar el fixpack. Por ejemplo:

   ```
   C:\Program Files\IBM\Installation Manager\eclipse\tools\imcl.exe
         input c:\SDS_6310\install_resp.xml -acceptLicense -showProgress
   ```

En este mandato, también se puede utilizar la opción `-stopBlockingProcesses` si es necesario, para bloquear todos los procesos de forma silenciosa antes de instalar el fixpack.

Instalación de fixpacks con scripts nativos

Ejecute el script proporcionado desde la línea de mandatos para aplicar los fixpacks o para instalar mejoras en la secuencia de servicios en sistemas AIX, Linux y Solaris.

Antes de empezar

Consulte la información sobre la estrategia de fixpacks.

Procedimiento

1. Descargue los fixpacks desde http://www-01.ibm.com/support/docview.wss?uid=swg21496581#v631.
2. Extraiga el archivador de arreglos en un directorio con suficiente espacio libre. Encontrará detalles sobre el contenido del fixpack, incluido el directorio y los nombres de archivo que se proporcionan en el archivo *README* que se incluye con el fixpack.
3. Detenga todos los procesos de cliente o servidor asociados con IBM Security Directory Server. El conjunto de procesos de daemon incluye el servidor de directorio, el servidor de administración, el servidor proxy (si se utiliza) y las aplicaciones LDAP que tenga personalizadas. Los programas y bibliotecas no se pueden sustituir mientras se estén utilizando. Si el rastreo está habilitado, ejecute **ldtrc off** para desactivarlo. Para obtener información sobre cómo detener los procesos de administración y las instancias de servidor de directorio, consulte los temas bajo Tareas de administración de servidor básicas en la documentación de IBM Security Directory Server.
4. En la línea de mandatos, cámbiese a la carpeta en la que extrajo el archivador de arreglos.
5. Ejecute el mandato siguiente como `root`:

   ```
   idsinstall -u -f
   ```

   El programa de instalación actualiza los componentes que ya están instalados en su sistema.
6. Verifique la instalación.
   a. El programa de instalación visualiza un mensaje que indica si la instalación ha sido satisfactoria. Compruebe el registro de instalación en `/tmp/idsinstall_`*`indicación_fecha_y_hora`*.
   b. Si la instalación no ha sido satisfactoria o si recibe un mensaje que indica que no se han instalado todos los paquetes, corrija los errores que aparezcan en el registro, por ejemplo, falta de espacio en el disco. A continuación, ejecute de nuevo el programa de instalación para asegurarse de que todos los paquetes se han instalado de forma satisfactoria.
   c. Compruebe el número de versión de los paquetes para verificar que están todos en el nivel adecuado. Consulte Capítulo 6, “Consulta de paquetes de IBM Security Directory Server”, en la página 47 para obtener más instrucciones.

Capítulo 23. Desinstalación de IBM Security Directory Server: Una visión general

Consulte la visión general para desinstalar el producto IBM Security Directory Server y considere algunos aspectos importantes a considerar antes de realizar la desinstalación.

Antes de empezar

Para desinstalar IBM Security Directory Server, debe iniciar sesión con privilegios root en sistemas AIX, Linux, Solaris o HP-UX y como miembro del grupo de administradores en sistemas Windows.

Acerca de esta tarea

Cuando se desinstala IBM Security Directory Server, no se eliminan las instancias y sus archivos de configuración.

Procedimiento

1. Detenga todos los procesos de cliente o servidor de IBM Security Directory Server, incluidos el servidor de directorios, el daemon de administración y las aplicaciones LDAP personalizadas. Los programas y bibliotecas no se pueden sustituir mientras se estén utilizando. Si está establecido el rastreo, ejecute el mandato **ldtrc off** para desactivar el proceso de rastreo.
2. En función del sistema operativo y la modalidad de instalación de IBM Security Directory Server, utilice la misma modalidad para desinstalar IBM Security Directory Server. Los métodos disponibles para desinstalar los paquetes de IBM Security Directory Server son:
   a. Programa de desinstalación de la GUI.
   b. Programas de utilidad del sistema operativo. Los nombres de paquetes en los sistemas Linux son ligeramente diferentes para las actualizaciones que para la versión GA. Por ejemplo, el nombre de paquete del cliente base para la versión GA en xSeries Linux es `idsldap-cltbase63-6.3.0-0.i386.rpm`. Puede utilizar el mandato **rpm -qa** para listar todos los paquetes.
3. Después de desinstalar IBM Security Directory Server, consulte si todos los paquetes de IBM Security Directory Server se han eliminado correctamente. Para obtener más información, consulte el Capítulo 6, “Consulta de paquetes de IBM Security Directory Server”, en la página 47.

Información relacionada:

http://www-01.ibm.com/support/knowledgecenter/SSVJJU/welcome
Para obtener más información, consulte el tema *Desinstalación de IBM Security Directory Server* en la sección *Instalación y configuración* de la documentación del producto IBM Security Directory Server.

Capítulo 24. Desinstalación de IBM Security Directory Server y de software necesario

Es posible que desee eliminar IBM Security Directory Server y su software necesario si tiene previsto utilizar el sistema para un objetivo distinto o tiene previsto retirar el sistema.

Puede utilizar IBM Installation Manager o los programas de utilidad del sistema operativo para la desinstalación de IBM Security Directory Server. Debe utilizar la misma modalidad para la desinstalación que ha utilizado para la instalación. Debe utilizar IBM Installation Manager tanto para la instalación como para la desinstalación, o los programas de utilidad del sistema operativo tanto para la instalación como para la desinstalación. No debe utilizar una mezcla de ambas modalidades para la instalación y desinstalación.

Si desea eliminar IBM Security Directory Server de su sistema, tenga en cuenta las siguientes condiciones antes de la desinstalación:

1. Debe detener todos los procesos del cliente y del servidor de IBM Security Directory Server.
   - Servidor de directorios
   - Servidor de administración
   - Rastreos de LDAP
   - Herramienta de administración web y el servidor de aplicaciones asociado con ella
   - Aplicaciones LDAP personalizadas
2. Si tiene previsto ejecutar la instalación de IBM Security Directory Server de nuevo en el sistema, no necesita suprimir la instancia de servidor de directorios ni desconfigurar la base de datos de DB2 de la instancia. Si elimina IBM Security Directory Server del sistema, las instancias del servidor de directorios se quedarán intactas, a menos que las elimine o las desconfigure manualmente.
3. El usuario y el grupo `idsldap` que se han creado durante la instalación de IBM Security Directory Server se quedarán en el sistema tras la desinstalación. Debe tener en cuenta las condiciones adicionales antes de la desinstalación del formulario de AIX, Linux, o Solaris de IBM Security Directory Server.
   - Si no desea que se defina el usuario o el grupo de `idsldap`, utilice los programas de utilidad del sistema operativo para eliminarlos. El usuario y el grupo de `idsldap` son necesarios para el servidor proxy y el servidor de directorios completo y deben existir en el sistema si contiene IBM Security Directory Server instalado.
   - Si elimina el usuario `idsldap` y no elimina el directorio de inicio del usuario, se pueden producir problemas al crearse el usuario `idsldap` durante la instalación de IBM Security Directory Server. Por lo tanto, asegúrese de eliminar el directorio de inicio del usuario `idsldap` si elimina el usuario `idsldap`. Si utiliza el mandato **`userdel`** para eliminar el usuario `idsldap`, asegúrese de utilizar el parámetro **`-r`** para eliminar el directorio de inicio, `userdel -r idsldap`.
4. En Windows, el servidor de administración y los servicios del servidor de directorios se eliminarán durante la desinstalación de IBM Security Directory Server. Los servicios no se sustituirán durante la instalación de IBM Security Directory Server. Puede utilizar el mandato **`idsslapd`** para añadir el servicio del

servidor, y el mandato **idsdiradm** para añadir el servicio del servidor de administración. Para obtener más información sobre los mandatos **idsslapd** e **idsdiradm**, consulte *Consulta de mandatos de IBM Security Directory Server*.

Desinstalación con IBM Installation Manager

Si ha utilizado IBM Installation Manager para la instalación de IBM Security Directory Server, utilice IBM Installation Manager para la desinstalación de IBM Security Directory Server y de sus componentes.

Al utilizar IBM Installation Manager para la desinstalación de IBM Security Directory Server, el programa elimina IBM Security Directory Server y todo el software necesario que se haya instalado. No puede eliminar de forma selectiva características de IBM Security Directory Server durante la desinstalación con IBM Installation Manager.

Si ha instalado IBM DB2 que se proporciona con IBM Security Directory Server, debe eliminar todas las instancias de DB2 que se hubieran creado con la copia de DB2 para la desinstalación correcta de IBM DB2. Si permanece en el sistema una instancia de DB2 que se hubiera creado con la copia de DB2, no se eliminará DB2 durante la desinstalación de IBM Security Directory Server. IBM Installation Manager registra mensajes de error en su archivo de registro.

Debe utilizar IBM Installation Manager o programas de utilidad del sistema operativo para la instalación, modificación o desinstalación de IBM Security Directory Server y de sus componentes. No debe utilizar IBM Installation Manager ni los programas de utilidad del sistema operativo para la instalación, modificación, o desinstalación de IBM Security Directory Server ni de sus componentes.

Desinstalación con IBM Installation Manager

Utilice IBM Installation Manager para la desinstalación de IBM Security Directory Server, si ha utilizado IBM Installation Manager para la instalación de IBM Security Directory Server.

Antes de empezar

Debe detener todos los procesos del cliente y del servidor de IBM Security Directory Server.

- Servidor de directorios
- Servidor de administración
- Rastreos de LDAP
- Aplicaciones LDAP personalizadas

Si alguno de los procesos está en uso, no se podrán eliminar los programas ni las bibliotecas.

Procedimiento

1. Inicie IBM Installation Manager.
   - AIX y Linux:
     a. Abra una ventana de línea de mandatos y vaya al directorio que contiene IBM Installation Manager. El siguiente directorio es la ubicación de instalación predeterminada de IBM Installation Manager:

opt/IBM/InstallationManager/eclipse

b. Ejecute el siguiente mandato:

./IBMIM

- Microsoft Windows:
  a. Pulse **Inicio** > **Todos los programas** > **IBM Installation Manager** > **IBM Installation Manager**.

2. Pulse **Desinstalar**.
3. Seleccione **IBM Security Directory Server** con la versión adecuada y, a continuación, pulse **Siguiente**.
4. En la ventana **Desinstalar paquetes**, revise los paquetes que se seleccionan para su desinstalación.

   Importante: Si elige continuar con una versión existente de un DB2 o GSKit durante la instalación, IBM Installation Manager actualiza su registro con la entrada de características. Si elimina una característica que se ha instalado con la opción **Continuar con el existente**, Installation Manager realiza las siguientes acciones:

   - Elimina la entrada de característica desde el registro de IBM Installation Manager.
   - No desinstala la característica del sistema.

   Si existen instancias de DB2 que se han creado con la copia de DB2 instalada con IBM Installation Manager, no podrá desinstalar IBM Security Directory Server. En tal situación, deberá eliminar manualmente las instancias de DB2 e intentarlo de nuevo. Es recomendable realizar la copia de seguridad de la base de datos antes de eliminar las instancias de DB2.
5. Pulse **Desinstalar**. Cuando finalice la desinstalación, IBM Installation Manager indicará si la desinstalación ha resultado satisfactoria o anómala.
6. Opcional: Si se produce un error durante la desinstalación, pulse **Ver archivo de registro** para leer los detalles. Para obtener más información, consulte el Capítulo 5, “Archivos de registro de IBM Installation Manager”, en la página 45.
7. Pulse **Finalizar**.
8. Pulse **Archivo** > **Salir**.

Resultados

IBM Installation Manager desinstala IBM Security Directory Server y sus componentes.

Desinstalación silenciosa con un archivo de respuestas

Complete los pasos para desinstalar los componentes de IBM Security Directory Server de forma silenciosa con un archivo de respuestas.

Antes de empezar

IBM Installation Manager, versión 1.7.0 o posterior es necesario para la instalación silenciosa de los paquetes de IBM Security Directory Server.

Acerca de esta tarea

Puede utilizar el archivo de respuestas predeterminado o registrar un archivo de respuestas personalizado y utilizarlo como el archivo de entrada para la desinstalación silenciosa.

Procedimiento

1. Inicie sesión en el sistema como administrador.
2. Acceda al mandato **IBMIM** en la ubicación de instalación de IBM Installation Manager.

Sistema operativo	Ubicación predeterminada del mandato **IBMIM**:
Microsoft Windows	`C:\Program Files\IBM\InstallationManager\eclipse`
AIX y Linux	`/opt/IBM/InstallationManager/eclipse`

3. Opcional: Ejecute el mandato **IBMIM** para registrar un archivo de respuestas para la desinstalación silenciosa.
   a. Ejecute los mandatos siguientes en distintos sistemas operativos:

      Microsoft Windows

      ```
      IBMIM.exe -record nombre_vía_acceso\uninstall_responseFile.xml
      -skipInstall UbicaciónDatosagente
      ```

      AIX y Linux

      ```
      ./IBMIM -record nombre_vía_acceso/uninstall_responseFile.xml
      -skipInstall UbicaciónDatosagente
      ```

      El mandato abrirá IBM Installation Manager.

   b. Complete el registro de desinstalación de IBM Security Directory Server. Para obtener más información, consulte 2 en la página 241
4. Ejecute el mandato **IBMIM** para iniciar la desinstalación silenciosa con el archivo de respuestas como entrada.

Sistema operativo	Mandato a ejecutar:
Microsoft Windows	`IBMIM.exe -silent -input nombre_vía_acceso\uninstsll_responseFile.xml -noSplash`
AIX y Linux	`./IBMIM -silent -input nombre_vía_acceso/uninstall_responseFile.xml -noSplash`

5. Verifique el resumen de desinstalación y los archivos de registro.

Sistema operativo	Vía de acceso de registro predeterminado:
Microsoft Windows	`C:\ProgramData\IBM\InstallationManager\logs`
AIX y Linux	`/var/ibm/InstallationManager/logs/`

6. Verifique si los paquetes de IBM Security Directory Server están desinstalados.

Sistema operativo	Verificación de paquetes:
Microsoft Windows	Consulte el apartado "Verificación de las características de IBM Security Directory Server en Windows" en la página 85.
AIX y Linux	Consulte el apartado "Verificación de los paquetes de IBM Security Directory Server" en la página 87.

Resultados

IBM Installation Manager desinstala los componentes de IBM Security Directory Server de forma silenciosa.

Desinstalación silenciosa con el mandato `imcl uninstall`

Complete los pasos para desinstalar los componentes de IBM Security Directory Server de forma silenciosa con el mandato **`imcl uninstall`**.

Antes de empezar

IBM Installation Manager, versión 1.7.0 o posterior es necesario para la instalación silenciosa de los paquetes de IBM Security Directory Server.

Acerca de esta tarea

Puede utilizar el mandato **`imcl uninstall`** para desinstalar IBM Security Directory Server en modalidad silenciosa.

Procedimiento

1. Inicie sesión en el sistema como administrador.
2.
3. Ejecute el mandato **`imcl listInstalledPackages`** desde el directorio *<dir_instalación_IBM_Installation_Manager>*`/eclipse/tools`.

Sistema operativo	Mandato a ejecutar
Microsoft Windows	`imcl.exe listInstalledPackages`
AIX y Linux	`./imcl listInstalledPackages`

   Este mandato lista todos los paquetes que instala IBM Installation Manager.
4. Ejecute **`imcl uninstall com.ibm.security.directoryserver.v631_6.3.1.0`**. Utilice la entrada Security Directory Server, que será la salida del mandato **`imcl listInstalledPackages`** mencionado anteriormente.

Sistema operativo	Mandato a ejecutar:
Microsoft Windows	`imcl.exe uninstall com.ibm.security.directoryserver.v631_6.3.1.0`
AIX y Linux	`./imcl uninstall com.ibm.security.directoryserver.v631_6.3.1.0`

Resultados

IBM Installation Manager desinstala los componentes de IBM Security Directory Server de forma silenciosa.

Desinstalación de IBM Security Directory Server con los programas de utilidad del sistema operativo

Si ha utilizado programas de utilidad del sistema operativo para la instalación de IBM Security Directory Server, utilice los programas de utilidad del sistema operativo para la desinstalación de IBM Security Directory Server.

Puede utilizar los programas de utilidad del sistema operativo para la desinstalación de IBM Security Directory Server en sistemas con sistemas operativos AIX, Linux, Solaris, y HP-UX. En Windows, debe utilizar IBM Installation Manager para la instalación y desinstalación de IBM Security Directory Server. Consulte el apartado "Desinstalación con IBM Installation Manager" en la página 240.

Al utilizar los programas de utilidad del sistema operativo para la desinstalación de IBM Security Directory Server, el programa elimina IBM Security Directory Server. Puede eliminar de forma selectiva las características de IBM Security Directory Server durante la desinstalación con los programas de utilidad del sistema operativo.

Debe detener todos los procesos del cliente y del servidor de IBM Security Directory Server antes de la desinstalación de IBM Security Directory Server.

- Servidor de directorios
- Servidor de administración
- Rastreos de LDAP
- Herramienta de administración web y el servidor de aplicaciones asociado con ella
- Aplicaciones LDAP personalizadas

Si ha creado y configurado una instancia de servidor de directorios con una base de datos de DB2, no se eliminarán al utilizar programas de utilidad del sistema operativo para la desinstalación de IBM Security Directory Server.

Desinstalación con programas de utilidad de AIX

Puede utilizar los programas de utilidad de línea de mandatos de AIX para la desinstalación de IBM Security Directory Server de un sistema AIX.

Puede utilizar uno de los siguientes programas de utilidad para la desinstalación de IBM Security Directory Server:

SMIT El método de desinstalación preferido es utilizar el programa de utilidad. Para obtener más información, consulte el "Desinstalación con SMIT".

installp
Para obtener más información, consulte el "Desinstalación con **installp**" en la página 245.

Desinstalación con SMIT

Utilice el mandato **smit** para completar la desinstalación de IBM Security Directory Server desde un sistema AIX.

Antes de empezar

Debe detener todos los procesos del cliente y del servidor de IBM Security Directory Server.

- Servidor de directorios
- Servidor de administración
- Rastreos de LDAP
- Herramienta de administración web y el servidor de aplicaciones asociado con ella
- Aplicaciones LDAP personalizadas

Procedimiento

1. Inicie sesión como usuario root.
2. Acceda al indicador de mandatos.
3. Ejecute el mandato **smit**. Se abrirá la ventana **Instalación y mantenimiento de software**.
4. Seleccione **Instalación y mantenimiento de software** > **Mantenimiento y programas de utilidad de software**.
5. Seleccione **Eliminar software instalado**.
6. En el campo **Nombre de software**, pulse **F4** para mostrar la lista de software instalado. Puede proporcionar el valor `idsldap` en el campo para listar todos los paquetes de IBM Security Directory Server.
7. Seleccione los paquetes que desee eliminar y pulse Intro.

Resultados

El programa de utilidad de SMIT elimina IBM Security Directory Server del sistema AIX. Si ha seleccionado eliminar todos los paquetes de IBM Security Directory Server, el programa de utilidad también eliminará el directorio de instalación de IBM Security Directory Server, `/opt/IBM/ldap/V6.3.1`, del sistema AIX.

Qué hacer a continuación

Verifique si ha sido satisfactoria la desinstalación de IBM Security Directory Server. Para obtener más información, consulte el "Verificación de los paquetes de IBM Security Directory Server" en la página 87.

Desinstalación con `installp`

Utilice el mandato **installp** para completar la desinstalación de IBM Security Directory Server desde un sistema AIX.

Antes de empezar

Debe detener todos los procesos del cliente y del servidor de IBM Security Directory Server.

- Servidor de directorios
- Servidor de administración
- Rastreos de LDAP
- Herramienta de administración web y el servidor de aplicaciones asociado con ella
- Aplicaciones LDAP personalizadas

Procedimiento

1. Inicie sesión como usuario root.
2. Acceda al indicador de mandatos.

3. Ejecute el mandato siguiente para determinar los paquetes de IBM Security Directory Server que desea eliminar:

   ```
   lslpp -l 'idsldap*'
   ```

4. Para eliminar un paquete de IBM Security Directory Server, ejecute el mandato siguiente:

   ```
   installp -u nombre_paquete
   ```

   Para eliminar IBM Security Directory Server por completo, elimine todos los paquetes de IBM Security Directory Server. Para la desinstalación de IBM Security Directory Server, debe proporcionar paquetes en el orden contrario de instalación. Para obtener más información sobre la secuencia, consulte "Paquetes para la instalación en un sistema AIX" en la página 70. Para eliminar el paquete `idsldap.ent631`, ejecute el siguiente mandato:

   ```
   installp -u idsldap.ent631
   ```

Qué hacer a continuación

Verifique si ha sido satisfactoria la desinstalación de IBM Security Directory Server. Para obtener más información, consulte el "Verificación de los paquetes de IBM Security Directory Server" en la página 87.

Desinstalación con programas de utilidad de Linux

Puede utilizar los programas de utilidad de línea de mandatos de Linux para la desinstalación de IBM Security Directory Server a partir de un sistema Linux.

Los nombres de paquetes de IBM Security Directory Server son distintos para los sistemas con distinta arquitectura y sistemas operativos. Debe verificar los paquetes instalados de IBM Security Directory Server antes de la desinstalación.

Desinstalación con programas de utilidad de Linux

Utilice el mandato **rpm** para completar la desinstalación de IBM Security Directory Server desde un sistema Linux.

Antes de empezar

Debe detener todos los procesos del cliente y del servidor de IBM Security Directory Server.

- Servidor de directorios
- Servidor de administración
- Rastreos de LDAP
- Herramienta de administración web y el servidor de aplicaciones asociado con ella
- Aplicaciones LDAP personalizadas

Acerca de esta tarea

El ejemplo siguiente muestra la desinstalación de paquetes de IBM Security Directory Server desde un sistema AMD64 Opteron/EM64T de Linux. Para System z, System i o System p, o System x de Linux, debe sustituirlo por los nombres de paquetes adecuados.

Procedimiento

1. Inicie sesión como usuario root.
2. Acceda al indicador de mandatos.
3. Ejecute el mandato siguiente para determinar los paquetes de IBM Security Directory Server que desea eliminar:

   ```
   rpm -qa | grep -i idsldap
   ```

4. Para eliminar un paquete de IBM Security Directory Server, ejecute el mandato siguiente:

   ```
   rpm -ev nombre_paquete
   ```

   Para eliminar IBM Security Directory Server por completo, elimine todos los paquetes de IBM Security Directory Server. Para desinstalar IBM Security Directory Server, debe proporcionar paquetes en orden inverso a la secuencia de instalación. Para obtener más información sobre la secuencia, consulte "Paquetes para la instalación en un sistema Linux" en la página 75. Para eliminar el paquete de `idsldap-srv64bit631-6.3.1-0.x86_64.rpm`, ejecute el mandato siguiente:

   ```
   rpm -ev idsldap-srv64bit631-6.3.1-0.x86_64.rpm
   ```

Qué hacer a continuación

Verifique si ha sido satisfactoria la desinstalación de IBM Security Directory Server. Para obtener más información, consulte el "Verificación de los paquetes de IBM Security Directory Server" en la página 87.

Desinstalación con programas de utilidad de Solaris

Puede utilizar los programas de utilidad de línea de mandatos de Solaris para la desinstalación de IBM Security Directory Server de un sistema Solaris.

Los nombres de paquetes de IBM Security Directory Server son los mismos para los sistemas Solaris SPARC y Solaris X64.

Desinstalación con los programas de utilidad de Solaris

Utilice el mandato **pkgrm** para completar la desinstalación de IBM Security Directory Server desde un sistema Solaris.

Antes de empezar

Debe detener todos los procesos del cliente y del servidor de IBM Security Directory Server.

- Servidor de directorios
- Servidor de administración
- Rastreos de LDAP
- Herramienta de administración web y el servidor de aplicaciones asociado con ella
- Aplicaciones LDAP personalizadas

Procedimiento

1. Inicie sesión como usuario root.
2. Acceda al indicador de mandatos.
3. Ejecute el mandato siguiente para determinar los paquetes de IBM Security Directory Server que desea eliminar:

```
pkginfo | grep -i IDSl
```

4. Para eliminar un paquete de IBM Security Directory Server, ejecute el mandato siguiente:

   ```
   pkgrm nombre_paquete
   ```

   Para eliminar IBM Security Directory Server por completo, elimine todos los paquetes de IBM Security Directory Server. Para desinstalar IBM Security Directory Server, debe proporcionar paquetes en orden inverso a la secuencia de instalación. Para obtener más información sobre la secuencia, consulte "Paquetes para la instalación en un sistema Solaris" en la página 79. Para eliminar el paquete `IDSlent631`, ejecute el siguiente mandato:

   ```
   pkgrm IDSlent631
   ```

Qué hacer a continuación

Verifique si ha sido satisfactoria la desinstalación de IBM Security Directory Server. Para obtener más información, consulte el "Verificación de los paquetes de IBM Security Directory Server" en la página 87.

Desinstalación con los programas de utilidad de HP-UX

Puede utilizar los programas de utilidad de línea de mandatos de HP-UX para la desinstalación de IBM Security Directory Server desde un sistema de HP-UX.

En sistemas HP-UX (Itanium), sólo están soportados los paquetes de cliente de IBM Security Directory Server.

Desinstalación con programas de utilidad de HP-UX

Utilice el mandato **swremove** para completar la desinstalación de IBM Security Directory Server desde un sistema HP-UX.

Antes de empezar

Debe detener todos los procesos del cliente de IBM Security Directory Server.

- Rastreos de LDAP
- Aplicaciones LDAP personalizadas

Procedimiento

1. Inicie sesión como usuario root.
2. Acceda al indicador de mandatos.
3. Ejecute el mandato siguiente para determinar los paquetes de IBM Security Directory Server que desea eliminar:

   ```
   swlist | grep -i idsldap
   ```

4. Para eliminar un paquete de IBM Security Directory Server, ejecute el mandato siguiente:

   ```
   swremove nombre_paquete
   ```

   Para eliminar IBM Security Directory Server por completo, elimine todos los paquetes de IBM Security Directory Server. Para desinstalar IBM Security Directory Server, debe proporcionar paquetes en orden inverso a la secuencia de instalación. Para obtener más información sobre la secuencia, consulte "Paquetes para la instalación en un sistema HP-UX Itanium" en la página 83. Para eliminar el paquete de `idsldap.cltjava631.depot`, ejecute el mandato siguiente:

```
swremove idsldap.cltjava631.depot
```

Qué hacer a continuación

Verifique si ha sido satisfactoria la desinstalación de IBM Security Directory Server. Para obtener más información, consulte el "Verificación de los paquetes de IBM Security Directory Server" en la página 87.

Desinstalación de IBM DB2 con mandatos de DB2

Si ha instalado la copia de IBM DB2 que se proporciona con IBM Security Directory Server manualmente, utilice los mandatos de DB2 para eliminar IBM DB2 del sistema.

Si ha instalado la copia de IBM DB2 con IBM Installation Manager durante la instalación de IBM Security Directory Server, IBM DB2 está instalado en una ubicación predefinida. Para obtener más información sobre la ubicación predeterminada, consulte "Ubicaciones de la instalación predeterminada" en la página 27. Si ha instalado la copia de IBM DB2 con IBM Installation Manager, debe utilizar IBM Installation Manager para la desinstalación de IBM DB2.

Si el sistema contiene instancias de DB2 para la copia de IBM DB2, debe eliminar manualmente las instancias de DB2 antes de la desinstalación de IBM DB2. Es recomendable realizar una copia de seguridad de las bases de datos y de los datos de DB2 antes de la desinstalación.

Si ha instalado manualmente IBM DB2 en una ubicación personalizada con los mandatos de DB2, utilice los mandatos de DB2 para la desinstalación de IBM DB2. En AIX, Linux, y Solaris, ejecute el mandato **db2_deinstall** en el directorio *ubicación_instalación_DB2*/install/ para la desinstalación de IBM DB2. En Windows, ejecute el mandato **db2unins** en el directorio *ubicación_instalación_DB2*\bin para la desinstalación de IBM DB2. Para obtener más información acerca de la desinstalación de IBM DB2, consulte la documentación del producto IBM DB2 en http://www-01.ibm.com/support/knowledgecenter/SSEPGG/welcome.

Desinstalación de IBM Global Security Kit con programas de utilidad del sistema operativo

Si ha utilizado programas de utilidad del sistema operativo para la instalación de IBM Global Security Kit (GSKit), utilice los programas de utilidad del sistema operativo para la desinstalación de GSKit.

Puede utilizar los programas de utilidad del sistema operativo para la desinstalación de GSKit de sistemas con sistemas operativos AIX, Linux, Solaris, y HP-UX.

En Windows, puede ejecutar la desinstalación de GSKit manualmente sólo si ha seleccionado utilizar una versión instalada de GSKit con IBM Installation Manager durante la instalación. Si IBM Security Directory Server está instalado en el sistema, no debe eliminar GSKit si está en uso. Si desea utilizar la versión más reciente de GSKit, debe utilizar IBM Installation Manager para modificar la característica de GSKit para eliminarla de su registro. A continuación, puede ejecutar la desinstalación de GSKit.

Desinstalación de IBM Global Security Kit con SMIT

Utilice el mandato **smit** para completar la desinstalación de IBM Global Security Kit (GSKit) desde un sistema AIX.

Procedimiento

1. Inicie sesión como usuario root.
2. Acceda al indicador de mandatos.
3. Ejecute el mandato **smit**. Se abrirá la ventana **Instalación y mantenimiento de software**.
4. Seleccione **Instalación y mantenimiento de software** > **Mantenimiento y programas de utilidad de software**.
5. Seleccione **Eliminar software instalado**.
6. En el campo **Nombre de software**, pulse **F4** para mostrar la lista de software instalado. Puede proporcionar el valor GSKit en el campo para listar todos los paquetes de GSKit.
7. Establezca el valor para **ELIMINAR software dependiente** en SÍ para eliminar productos de software y actualizaciones que dependen del producto que esté eliminando.
8. Seleccione los paquetes que desee eliminar y pulse Intro.
9. Verifique si la desinstalación de GSKit ha sido satisfactoria.

   ```
   lslpp -l 'GSK*'
   ```

Desinstalación de IBM Global Security Kit con installp

Utilice el mandato **installp** para completar la desinstalación de IBM Global Security Kit (GSKit) desde un sistema AIX.

Procedimiento

1. Inicie sesión como usuario root.
2. Acceda al indicador de mandatos.
3. Ejecute el mandato siguiente para determinar los paquetes de GSKit que desea eliminar:

   ```
   lslpp -l 'GSK*'
   ```

4. Para eliminar un paquete de GSKit, ejecute el mandato siguiente:

   ```
   installp -u nombre_paquete
   ```

   Para eliminar GSKit por completo, elimine todos los paquetes de GSKit de la misma versión. Para la desinstalación de GSKit, debe eliminar en primer lugar el paquete de GSKit SSL y, a continuación, el paquete de cifrado de GSKit. Para eliminar los paquetes GSKit8.gskssl64.ppc.rte y GSKit8.gskcrypt64.ppc.rte, ejecute el mandato siguiente:

   ```
   installp -u GSKit8.gskssl64.ppc.rte
   installp -u GSKit8.gskcrypt64.ppc.rte
   ```

5. Verifique si la desinstalación de GSKit ha sido satisfactoria.

   ```
   lslpp -l 'GSK*'
   ```

Desinstalación de IBM Global Security Kit con los programas de utilidad de Linux

Utilice el mandato **rpm** para completar la desinstalación de IBM Global Security Kit (GSKit) desde un sistema Linux.

Acerca de esta tarea

El ejemplo siguiente muestra la desinstalación de los paquetes de GSKit desde un sistema AMD64 Opteron/EM64T de Linux. Para System z, System i o System p, o System x de Linux, debe sustituirlo por los nombres de paquetes adecuados.

Procedimiento

1. Inicie sesión como usuario root.
2. Acceda al indicador de mandatos.
3. Ejecute el mandato siguiente para determinar los paquetes de GSKit que desea eliminar:

   ```
   rpm -qa | grep -i gsk
   ```

4. Para eliminar un paquete de GSKit, ejecute el mandato siguiente:

   ```
   rpm -ev nombre_paquete
   ```

   Para eliminar GSKit por completo, elimine todos los paquetes de GSKit de la misma versión. Para la desinstalación de GSKit, debe eliminar en primer lugar el paquete de GSKit SSL y, a continuación, el paquete de cifrado de GSKit. Para eliminar los paquetes `gskssl64-8.0-14.26.x86_64` y `gskcrypt64-8.0-14.26.x86_64`, ejecute el mandato siguiente:

   ```
   rpm -ev gskssl64-8.0-14.26.x86_64
   rpm -ev gskcrypt64-8.0-14.26.x86_64
   ```

5. Verifique si la desinstalación de GSKit ha sido satisfactoria.

   ```
   rpm -qa | grep -i gsk
   ```

Desinstalación de IBM Global Security Kit con programas de utilidad de Solaris

Utilice el mandato **pkgrm** para completar la desinstalación de IBM Global Security Kit (GSKit) desde un sistema Solaris.

Procedimiento

1. Inicie sesión como usuario root.
2. Acceda al indicador de mandatos.
3. Ejecute el mandato siguiente para determinar los paquetes de GSKit que desea eliminar:

   ```
   pkginfo | grep -i gsk
   ```

4. Para eliminar un paquete de GSKit, ejecute el mandato siguiente:

   ```
   pkgrm nombre_paquete
   ```

   Para eliminar GSKit por completo, elimine todos los paquetes de GSKit de la misma versión. Para la desinstalación de GSKit, debe eliminar en primer lugar el paquete de GSKit SSL y, a continuación, el paquete de cifrado de GSKit. Para eliminar los paquetes `gsk8ssl64` y `gsk8cry64`, ejecute el mandato siguiente:

   ```
   pkgrm gsk8ssl64
   pkgrm gsk8cry64
   ```

5. Verifique si la desinstalación de GSKit ha sido satisfactoria.

   ```
   pkginfo | grep -i gsk
   ```

Desinstalación de IBM Global Security Kit con los programas de utilidad de HP-UX

Utilice el mandato **swremove** para completar la desinstalación de IBM Global Security Kit (GSKit) desde un sistema HP-UX.

Procedimiento

1. Inicie sesión como usuario root.
2. Acceda al indicador de mandatos.
3. Ejecute el mandato siguiente para determinar los paquetes de GSKit que desea eliminar:

   ```
   swlist | grep -i gsk
   ```

4. Para eliminar un paquete de GSKit, ejecute el mandato siguiente:

   ```
   swremove nombre_paquete
   ```

   Para eliminar GSKit por completo, elimine todos los paquetes de GSKit de la misma versión. Para la desinstalación de GSKit, debe eliminar en primer lugar el paquete de GSKit SSL y, a continuación, el paquete de cifrado de GSKit. Para eliminar los paquetes `gskssl64` y `gskcrypt64`, ejecute el mandato siguiente:

   ```
   swremove gskssl64
   swremove gskcrypt64
   ```

5. Verifique si la desinstalación de GSKit ha sido satisfactoria.

   ```
   swlist | grep -i gsk
   ```

Desinstalación de IBM Global Security Kit en Windows

Utilice los mandatos IBM Global Security Kit (GSKit) para completar la desinstalación de GSKit de un sistema Windows.

Acerca de esta tarea

En el ejemplo, se mostrará la desinstalación silenciosa de los paquetes de GSKit SSL de 64 bits y de GSKit de cifrado de 64 bits de un sistema Windows en una arquitectura AMD64/EM64T. Para un sistema operativo Windows en una arquitectura IA32/x86, los nombres de paquetes de GSKit son distintos. Para obtener información sobre los nombres de paquetes de GSKit, consulte Capítulo 10, “Instalación de IBM Global Security Kit”, en la página 57.

Nota: También puede utilizar **Inicio** > **Panel de control** > **Agregar o quitar programas** para eliminar los paquetes de GSKit.

Procedimiento

1. Inicie sesión como miembro del grupo de administradores.
2. Acceda al indicador de mandatos.
3. Cambie el directorio de trabajo actual al directorio `gskit` donde se almacena el instalable de IBM Global Security Kit.
4. Para eliminar los paquetes de GSKit de 64 bits de forma silenciosa, ejecute los mandatos siguientes: Para eliminar GSKit por completo, elimine todos los paquetes de GSKit de la misma versión. Para la desinstalación de GSKit, debe eliminar en primer lugar el paquete de GSKit SSL y, a continuación, el paquete de cifrado de GSKit.

   ```
   gsk8ssl64.exe /s /x /v"/quiet"
   gsk8crypt64.exe /s /x /v"/quiet"
   ```

Desinstalación de paquetes de idiomas

Para completar la desinstalación de IBM Security Directory Server, debe desinstalar los paquetes de idiomas instalados en el sistema.

Si ha instalado IBM Security Directory Server y los paquetes de idiomas en el sistema con IBM Installation Manager, debe utilizar IBM Installation Manager para la desinstalación de los paquetes de idiomas.

Si ha utilizado los programas de utilidad del sistema operativo para la instalación de los paquetes de idiomas, utilice los programas de utilidad del sistema operativo para la desinstalación de los paquetes de idioma.

Todos los paquetes de idiomas se desinstalarán del sistema, si no selecciona la característica Proxy Server o Server para la instalación.

Desinstalación de paquetes de idiomas con programas de utilidad del sistema operativo

Utilice los programas de utilidad del sistema operativo para completar la desinstalación de un paquete de idiomas si ha instalado el paquete de idiomas con los programas de utilidad del sistema operativo.

Antes de empezar

Debe detener todos los procesos del cliente y del servidor de IBM Security Directory Server para desinstalar los paquetes de idiomas de IBM Security Directory Server.

- Servidor de directorios
- Servidor de administración
- Rastreos de LDAP
- Aplicaciones LDAP personalizadas

Procedimiento

1. Inicie sesión como usuario root.
2. Acceda al indicador de mandatos.
3. Determine los paquetes de idiomas en el sistema que desee eliminar:

Sistema operativo	**Mandato a ejecutar:**
AIX	`lslpp -l 'idsldap.msg631*'`
Linux	`rpm -qa | grep -i idsldap-msg631`
Solaris	`pkginfo | grep IDSl`

4. Para desinstalar el paquete de idiomas para un idioma, ejecute los mandatos de desinstalación del paquete. En el ejemplo siguiente, se mostrará la desinstalación del paquete de idiomas para el idioma francés. Puede desinstalar cualquier paquete de idiomas sustituyéndolo por los nombres de paquetes adecuados para el sistema operativo.

Sistema operativo	**Mandato a ejecutar:**
AIX	`installp -u idsldap.msg631.fr_FR`
Linux	`rpm -ev idsldap-msg631-fr-6.3.1-0.noarch.rpm`

Sistema operativo	Mandato a ejecutar:
Solaris	`pkgrm IDSlfr631`

5. Verifique si la instalación del paquete de idiomas ha sido satisfactoria. Para obtener más información, consulte el “Verificación de los paquetes de IBM Security Directory Server” en la página 87.

Apéndice A. Directory Services Markup Language

Puede utilizar Directory Services Markup Language para representar la información de estructura de directorios, las consultas y las actualizaciones de directorios, y los resultados de las operaciones del directorio en formato XML.

Cuando haya finalizado la instalación de la Herramienta de administración web de IBM Security Directory Server, se almacenará un archivo de archivado de archivos de Directory Services Markup Language (DSML), `DSML.zip`, en el sistema. El `DSML.zip` se almacena en el subdirectorio `idstools` de la ubicación de instalación de IBM Security Directory Server. Para obtener más información sobre la ubicación de instalación predeterminada de IBM Security Directory Server, consulte "Ubicaciones de la instalación predeterminada" en la página 27.

El archivo `DSML.zip` contiene documentación e instalables de DSML que le guían con la instalación, la configuración y el uso de DSML. El archivo `DSML.zip` contiene los archivos siguientes:

`DSMLReadme.txt`
: El archivo `DSMLReadme.txt` lista los archivos del paquete y las instrucciones para la instalación y configuración de DSML.

`dsml.pdf`
: El archivo `dsml.pdf` se encuentra en formato PDF y describe cómo utilizar DSML.

`dsml.htm`
: El archivo `dsml.htm` se encuentra en formato HTML y describe cómo utilizar DSML.

Apéndice B. Carga de una base de datos de ejemplo e inicio del servidor

Cargue la base de datos de ejemplo e inicie el servidor de directorios para añadir, actualizar y buscar entradas.

Antes de empezar

Cree una instancia de servidor de directorios. Consulte el apartado "Creación de la instancia de servidor de directorios" en la página 136.

Acerca de esta tarea

Puede utilizar la Herramienta de configuración para cargar los datos LDIF en un servidor de directorios e iniciar el servidor.

Procedimiento

1. Para iniciar la Herramienta de configuración, ejecute el mandato siguiente:
   ```
   idsxcfg -I nombre_instancia
   ```
2. En el área de navegación de la izquierda, pulse **Tareas LDIF** > **Importar datos LDIF**.
3. En el campo **Vía de acceso y nombre del archivo LDIF**, especifique el nombre del archivo LDIF con la vía de acceso. También puede pulsar Examinar y especificar el nombre de archivo LDIF. El siguiente nombre de vía de acceso predeterminada y archivo de datos LDIF en diferentes sistemas operativos:

   Windows
   vía_acceso_instalación\examples\sample.ldif

   AIX y Solaris
   /opt/IBM/ldap/V6.3.1/examples/sample.ldif

   Linus /opt/ibm/ldap/V6.3.1/examples/sample.ldif
4. Pulse **Importación estándar**.
5. Pulse **Importar**.
6. Para iniciar la instancia de servidor de directorios, realice las acciones siguientes:
   a. En el área de navegación de la izquierda, pulse **Gestionar estado del servidor**.
   b. Pulse **Iniciar servidor**.

Apéndice C. Actualización del archivo ldapdb.properties manualmente

Si instala IBM Security Directory Server en un sistema que no contiene una versión soportada de IBM DB2, el archivo ldapdb.properties no se rellenará durante la instalación. En tal caso, debe instalar una versión soportada de IBM DB2 y, a continuación, actualizar el archivo ldapdb.properties manualmente.

Antes de empezar

Debe asegurarse de que esté instalado el paquete del servidor de directorios completo.

Procedimiento

1. Instale una versión soportada de IBM DB2, si no está instalado.
2. Ejecute el mandato **db2ls** para listar las versiones de DB2 que están instaladas en el sistema y sus vías de acceso de instalación.
3. Actualice el archivo ldapdb.properties con la versión soportada de DB2 y la vía de acceso de instalación. La ubicación predeterminada del archivo ldapdb.properties con valores de ejemplo para varios sistemas operativos:

   Microsoft Windows

   ```
   C:\Program Files\IBM\ldap\V6.3.1\etc\ldapdb.properties

   currentDB2InstallPath=C:\Program Files\IBM\SQLLIB
   currentDB2Version=9.7.0.6
   ```

   AIX y Solaris

   ```
   /opt/IBM/ldap/V6.3.1/etc/ldapdb.properties

   currentDB2InstallPath=/opt/IBM/db2/V9.7
   currentDB2Version=9.7.0.6
   ```

   Linux `/opt/ibm/ldap/V6.3.1/etc/ldapdb.properties`

   ```
   currentDB2InstallPath=/opt/ibm/db2/V9.7
   currentDB2Version=9.7.0.6
   ```

4. Guarde el archivo ldapdb.properties.

Apéndice D. Características de accesibilidad para Security Directory Server

Las características de accesibilidad ayudan a los usuarios con discapacidades físicas, como movilidad restringida o visión limitada, a utilizar los productos de tecnología de información correctamente.

Las funciones de accesibilidad más importantes de este producto permiten a los usuarios realizar las acciones siguientes:

- Utilice las tecnologías de asistencia, por ejemplo, el software de lectura de pantalla para oír lo que se visualiza en la pantalla. Consulte la documentación del producto de la tecnología de asistencia para obtener detalles sobre la utilización de estas tecnologías con este producto.
- Realizar funciones específicas o equivalentes utilizando únicamente el teclado.
- Ampliar lo que aparece en la pantalla.

Además, se ha modificado la documentación del producto con el objeto de incluir las funciones siguientes para ayudar a la accesibilidad:

- Toda la documentación está disponible en formatos HTML para facilitar al máximo la aplicación del software de lectura de pantalla para los usuarios.
- Todas las imágenes de la documentación se proporcionan con texto alternativo de forma que los usuarios con problemas de visión puedan comprender el contenido de las imágenes.

Accesibilidad

La lista siguiente incluye las características de accesibilidad más importantes de IBM Security Directory Server.

- Sólo da soporte al funcionamiento del teclado
- Da soporte a las interfaces utilizadas normalmente por los lectores de pantalla
- Las teclas se pueden distinguir por el tacto y no se activan con sólo tocarlas

La documentación de IBM Security Directory Server está habilitada para accesibilidad. Las características de accesibilidad de la documentación se describen en la documentación en línea.

Navegación por teclado

El producto utiliza teclas de atajo y aceleración estándar, que se describen en el sistema operativo. Consulte la documentación proporcionada por el sistema operativo para obtener más información.

Este producto utiliza teclas de navegación estándar de Microsoft Windows.

Ampliación de lo que se visualiza en la pantalla

Puede aumentar el tamaño de la información de las ventanas del producto con los recursos que facilitan los sistemas operativos en el que se ejecuta el producto. Por ejemplo, en un entorno Microsoft Windows, puede bajar la resolución de la pantalla para agrandar el tamaño de la fuente del texto de la pantalla. Consulte la

documentación proporcionada por el sistema operativo para obtener más información.

IBM y la accesibilidad

Consulte la página web IBM Human Ability and Accessibility Center para obtener más información acerca del compromiso de IBM con la accesibilidad:
`http://www.ibm.com/able`

Índice

E

F

G

H

I

L

M

N

P

R

S

T

U

V

W

Avisos

Esta información se ha desarrollado para productos y servicios ofrecidos en EE.UU. Puede que IBM no ofrezca los productos, servicios o características descritos en este documento en otros países. Consulte al representante local de IBM para obtener información sobre los productos y servicios disponibles actualmente en su área. Las referencias a programas, productos o servicios de IBM no pretenden establecer ni implicar que sólo puedan utilizarse los productos, programas o servicios de IBM. En su lugar se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de IBM. Sin embargo, la evaluación y verificación del funcionamiento de cualquier producto, programa o servicio que no sea de IBM son responsabilidad del usuario.

IBM puede tener patentes o solicitudes de patentes pendientes que cubran algunos temas descritos en este documento. La entrega de este documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 EE.UU.

Para consultas sobre licencias relacionadas con la información del conjunto de caracteres de doble byte (DBCS), póngase en contacto con el IBM Intellectual Property Department de su país o envíe sus consultas, por escrito, a:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokio 103-8510, Japón

El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país donde estas disposiciones sean incompatibles con la legislación local:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN NINGÚN TIPO DE GARANTÍA, NI EXPLÍCITA NI IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO INCUMPLIMIENTO, COMERCIALIZACIÓN O DE IDONEIDAD PARA UN PROPÓSITO DETERMINADO.

Algunos países no permiten la renuncia a garantías explícitas o implícitas en determinadas transacciones y, por lo tanto, esta declaración puede que no se aplique a su caso.

Esta información puede incluir imprecisiones técnicas o errores tipográficos. Periódicamente se efectúan cambios en la información aquí contenida; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede realizar en cualquier momento mejoras o cambios en los productos o programas descritos en esta publicación sin previo aviso.

Las referencias contenidas en esta información a sitios web que no sean de IBM sólo se proporcionan por comodidad y en ningún modo constituyen una aprobación de dichos sitios web. Los materiales de dichos sitios web no forman parte de los materiales para este producto de IBM y el uso de dichos sitios web corre a cuenta y riesgo del usuario.

IBM puede utilizar o distribuir la información que se le proporciona en la forma que considere adecuada, sin incurrir por ello en ninguna obligación para con el cliente.

Los titulares de licencias de este programa que deseen información sobre el mismo con el fin de permitir: (i) el intercambio de información entre programas creados independientemente y otros programas (incluido éste) y (ii) la utilización mutua de la información intercambiada, deben ponerse en contacto con:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 EE.UU.

Dicha información puede estar disponible, sujeta a los términos y condiciones apropiados, incluyendo en algunos casos el pago de una tarifa.

El programa bajo licencia descrito en esta información y todo el material bajo licencia disponible para el mismo los proporciona IBM bajo los términos de las Condiciones Generales de IBM, el Acuerdo Internacional de Programas Bajo Licencia de IBM o cualquier acuerdo equivalente entre IBM y el cliente.

Los datos sobre rendimiento que contiene este documento se determinaron en un entorno controlado. Por lo tanto, los resultados obtenidos en otros entornos pueden variar significativamente. Determinadas mediciones pueden haberse efectuado en sistemas que estén desarrollándose, por lo que no puede garantizarse que dichas mediciones sean iguales en los sistemas de los que se dispone habitualmente. Además, algunas de las mediciones pueden haberse estimado mediante extrapolaciones. Los resultados reales podrían ser distintos. Los usuarios de este documento deberían comprobar cuáles son los datos que se aplican a su entorno específico.

La información relacionada con productos que no son de IBM se ha obtenido de los proveedores de dichos productos, sus anuncios publicados o de otras fuentes disponibles públicamente. IBM no ha probado estos productos y no puede confirmar la precisión de su rendimiento, compatibilidad o cualquier otra reclamación relacionada con los productos que no son de su propiedad. Las preguntas relacionadas con las capacidades de productos que no sean de IBM deben dirigirse a los proveedores de dichos productos.

Todas las declaraciones relativas a las futuras direcciones o intenciones de IBM están sujetas a cambios o anulación sin previo aviso y representan únicamente metas y objetivos.

Todos los precios de IBM que se muestran son precios sugeridos por IBM para minoristas, están actualizados y se pueden modificar sin previo aviso. Los precios de los distribuidores pueden variar.

Esta información se proporciona únicamente con fines de planificación. La información aquí contenida está sujeta a cambios antes de que los productos descritos estén disponibles.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales habituales. Para ilustrarlos de la mejor manera posible, los ejemplos incluyen nombres de personas, empresas y productos. Todos ellos son ficticios y cualquier parecido con los nombres y direcciones utilizados por una empresa real son mera coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en el idioma de origen, que ilustran técnicas de programación en diversas plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo de cualquier forma sin pagar a IBM, para los fines de programas de aplicaciones de desarrollo, uso, marketing o distribución conformes a la interfaz de programación de aplicaciones para la plataforma operativa para la que se escriben los programas de ejemplo. Estos ejemplos no se han probado completamente en todas las condiciones. IBM, por lo tanto, no puede garantizar o implicar la fiabilidad, capacidad de servicio ni la función de estos programas. Puede copiar, modificar y distribuir estos programas de ejemplo de cualquier forma sin pagar a IBM para los fines de los programas de aplicaciones de desarrollo, uso, marketing o distribución conformes a las interfaces de programación de la aplicación de IBM.

Cada copia o parte de estos programas de ejemplo o cualquier trabajo derivado deben incluir un aviso de copyright como el siguiente:

© (el nombre de la empresa) (año). Algunas partes de este código se derivan de programas de ejemplo de IBM Corp. © Copyright IBM Corp. _especifique el año o años_. Reservados todos los derechos.

Si está visualizando esta información en formato de copia software, es posible que las fotografías y las ilustraciones a color no se visualicen.

Marcas registradas

IBM, el logotipo de IBM e ibm.com son marcas registradas o marcas comerciales registradas de International Business Machines Corp., registradas en muchas jurisdicciones de todo el mundo. Los nombres de otros productos y servicios pueden ser marcas registradas de IBM u otras empresas. Hay una lista actual disponible de las marcas registradas de IBM en la web de "Copyright and trademark information" en www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript y todas las marcas registradas basadas en Adobe son marcas comerciales registradas o marcas registradas de Adobe Systems Incorporated en Estados Unidos o en otros países.

IT Infrastructure Library es una marca registrada de Central Computer and Telecommunications Agency, que ahora forma parte de la Office of Government Commerce (Oficina de comercio gubernamental).

Intel, el logotipo de Intel, Intel Inside, el logotipo de Intel Inside, Intel Centrino, el logotipo de Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium, y Pentium son marcas registradas o marcas comerciales registradas de Intel Corporation o de sus filiales en Estados Unidos y en otros países.

Linux es una marca comercial de Linus Torvalds en los Estados Unidos o en otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en los Estados Unidos o en otros países.

ITIL es una marca registrada y una marca comunitaria registrada de la Office of Government Commerce y está registrada en la Oficina de patentes y marcas de los Estados Unidos.

UNIX es una marca registrada de The Open Group en Estados Unidos y en otros países.

Java y todos los logotipos y las marcas registradas que se basan en Java son marcas registradas o marcas comerciales registradas de Oracle y/sus afiliados.

Cell Broadband Engine es una marca registrada de Sony Computer Entertainment, Inc. en Estados Unidos, o en otros países, y se utiliza bajo licencia.

Linear Tape-Open, LTO, el logotipo de LTO, Ultrium, y el logotipo de Ultrium son marcas registradas de HP, IBM Corp. y Quantum en Estados Unidos y en otros países.

Impreso en España

SC11-7875-02