

*IBM SPSS Statistics Server Guía del
administrador*



Nota

Antes de utilizar esta información y el producto al que se refiere, lea la información en [“Avisos” en la página 61](#).

Información del producto

Esta edición se aplica a la versión 30, release 0, modificación 0 de IBM® SPSS Statistics Server y a todas las versiones y modificaciones posteriores hasta que se indique lo contrario en nuevas ediciones.

© Copyright International Business Machines Corporation .

Contenido

Capítulo 1. Visión general.....	1
Productos y sistemas operativos.....	1
Arquitectura.....	1
Componentes de software.....	3
Utilización de la modalidad distribuida.....	4
Administración de software de servidor.....	4
Uso de este documento.....	5
Capítulo 2. Instalado.....	7
Instalación del software de servidor.....	7
Instalación de la aplicación cliente.....	7
Capítulo 3. Acceso a datos.....	9
Vista de los datos.....	9
Tecnología de acceso a datos.....	9
Connect ODBC.....	9
acceso a datos.....	10
Datos de referencia.....	10
Control de acceso a datos.....	11
Orígenes de datos.....	11
Configuración del entorno UNIX para acceso a datos.....	11
Capítulo 4. Configuración, supervisión del uso y mantenimiento.....	15
Gestión de cuentas y archivos de usuario final.....	15
Cuentas.....	15
Acceso a datos.....	15
Archivos.....	15
Perfiles.....	16
Grupos y perfiles de usuario del servidor de IBM SPSS Statistics.....	16
Configuración de orígenes de datos ODBC.....	16
Orígenes de datos ODBC y IBM SPSS Data Access Pack.....	16
Utilización de un motor de clasificación de terceros.....	17
Administración de servidor de IBM SPSS Statistics.....	17
Configuración de Xtensiones.....	17
Configuración de la interfaz de línea de comandos de unidad de producción para enviar trabajos.....	18
Configuración de varias instancias.....	19
Control del inicio del servicio.....	20
Parámetros de línea de mandatos de script de inicio.....	21
Otros mantenimientos.....	21
Inicio y detención del software de servidor.....	22
Para iniciar el servicio o el daemon.....	22
Para detener el servicio o el daemon.....	22
Configuración para mejorar el rendimiento.....	22
Capítulo 5. Usuarios finales de soporte.....	23
Autenticación.....	23
Configuración de la autenticación a nivel de sistema operativo.....	23
Configuración de PAM.....	23
Configuración de la autenticación interna.....	24
Configuración de la autenticación unix2.....	25

Configuración del inicio de sesión único (SSO).....	26
Permisos.....	31
Permisos de nivel de administrador.....	31
Autorización de grupo.....	31
Perfiles.....	32
Versiones de cliente y servidor.....	32
Conexión de usuarios a través de un cortafuegos.....	32
Configuración de conexiones a través de un cortafuegos.....	33
Conexión de usuarios con PPTP.....	35
Uso de SSL para transferencias de datos seguras.....	35
Cómo funciona SSL.....	35
Cómo habilitar SSL con GSKit.....	36
Habilitar SSL mediante OpenSSL.....	40
Establecimiento de un entorno local.....	43
Conexión con el software de servidor.....	44
Acceso a datos y archivos.....	45
Guardar datos y archivos.....	45
Capítulo 6. Análisis y mejora del rendimiento.....	47
Obtención de información de rendimiento.....	47
Mejora del uso de disco.....	48
Mejora del uso de CPU.....	49
Mejora del uso de memoria.....	49
Mejora del uso de red.....	49
Utilización eficiente de IBM SPSS Statistics.....	50
Apéndice A. Resolución de problemas.....	51
Software de servidor.....	51
Software de cliente.....	51
Apéndice B. IBM SPSS Statistics Batch Facility.....	53
Información que necesita saber.....	53
Apéndice C. Tareas del sistema operativo Windows.....	55
Propiedades del archivo.....	55
Propiedades del sistema.....	55
Gestor de usuarios.....	56
Panel de control de servicios.....	56
Gestor de tareas.....	56
Administrador de ODBC.....	56
Para configurar un DSN del sistema.....	57
Para configurar un DSN de usuario.....	57
Apéndice D. Tareas del sistema operativo UNIX.....	59
Chmod.....	59
env.....	59
Scripts.....	59
ps y kill.....	59
odbc.ini.....	60
Avisos.....	61
Marcas comerciales.....	62
Índice.....	65

Capítulo 1. Visión general

La tecnología de servidor de IBM SPSS Statistics es una **arquitectura distribuida**, junto con las optimizaciones de gestión de datos clave, da soporte al análisis escalable. La tecnología se basa en cliente/servidor. Distribuye las solicitudes de cliente para operaciones de uso intensivo de recursos a un potente software de servidor. Cuando el cliente y el servidor trabajan juntos de este modo, se hace referencia a él como **modo de análisis distribuido**. El análisis distribuido permite a los usuarios finales realizar análisis que sus equipos de escritorio no pueden soportar.

Para obtener la máxima flexibilidad, las aplicaciones cliente que utilizan la tecnología de servidor también se pueden configurar para que se ejecuten únicamente en el sistema de escritorio del usuario final; esto se conoce como **modo de análisis local**. Los usuarios finales pueden cambiar fácilmente de modo.

Productos y sistemas operativos

La tecnología de servidor da soporte a la aplicación cliente de IBM SPSS Statistics y el software de servidor se ejecuta en varios sistemas operativos (consulte las instrucciones de instalación para obtener detalles específicos). Puede instalar varias versiones de software de servidor en el sitio, en el mismo sistema de servidor o en distintos sistemas de servidor.

Arquitectura

El software de servidor tiene una arquitectura distribuida de dos niveles. Distribuye las operaciones de software entre los sistemas cliente y servidor. Las operaciones de memoria intensiva, tales como acceder a una base de datos grande o analizar un archivo de datos grande, se realizan en la computadora del servidor sin descargar los datos a la computadora del cliente.

Capa de cliente

La aplicación **cliente** . Se instala y se ejecuta en el ordenador del usuario final. La aplicación cliente proporciona la interfaz gráfica de usuario para el acceso y análisis de datos. Presenta los resultados de los análisis del usuario final.

Nivel de servidor

El software de **servidor** . Se instala y se ejecuta en un sistema servidor en red. El software de servidor proporciona la infraestructura necesaria para manejar varios clientes, los algoritmos utilizados en el análisis estadístico y el acceso a datos.

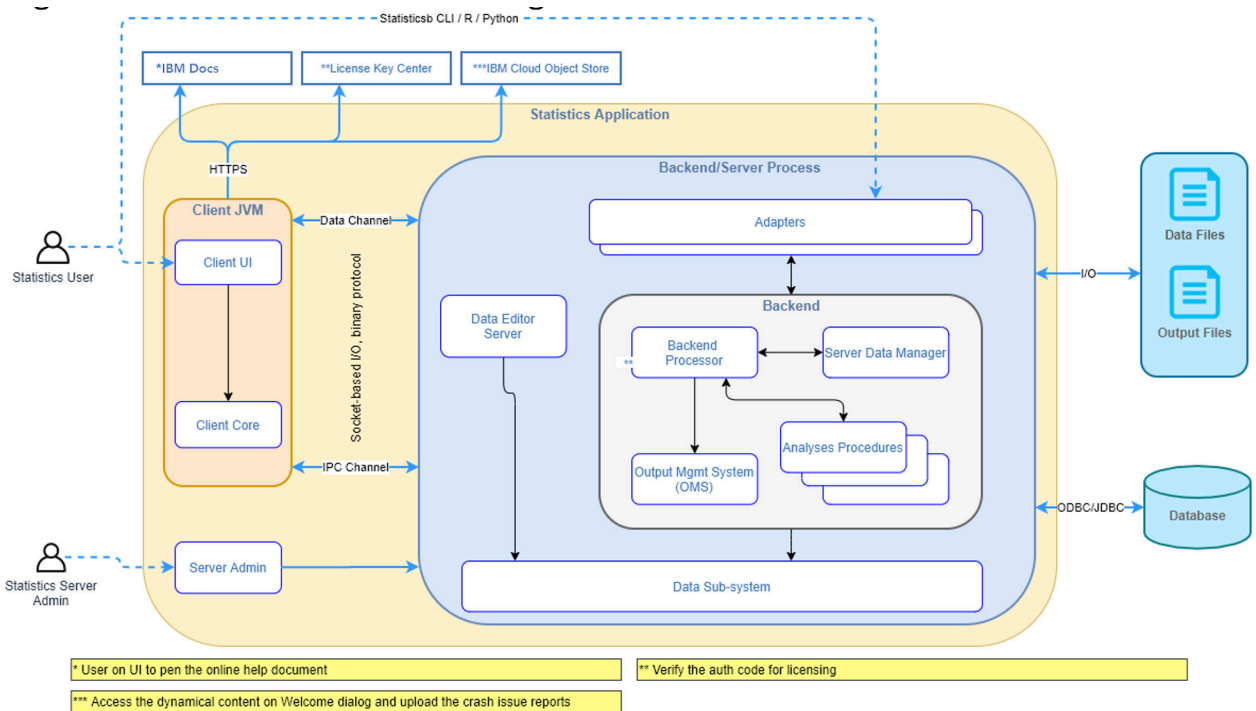
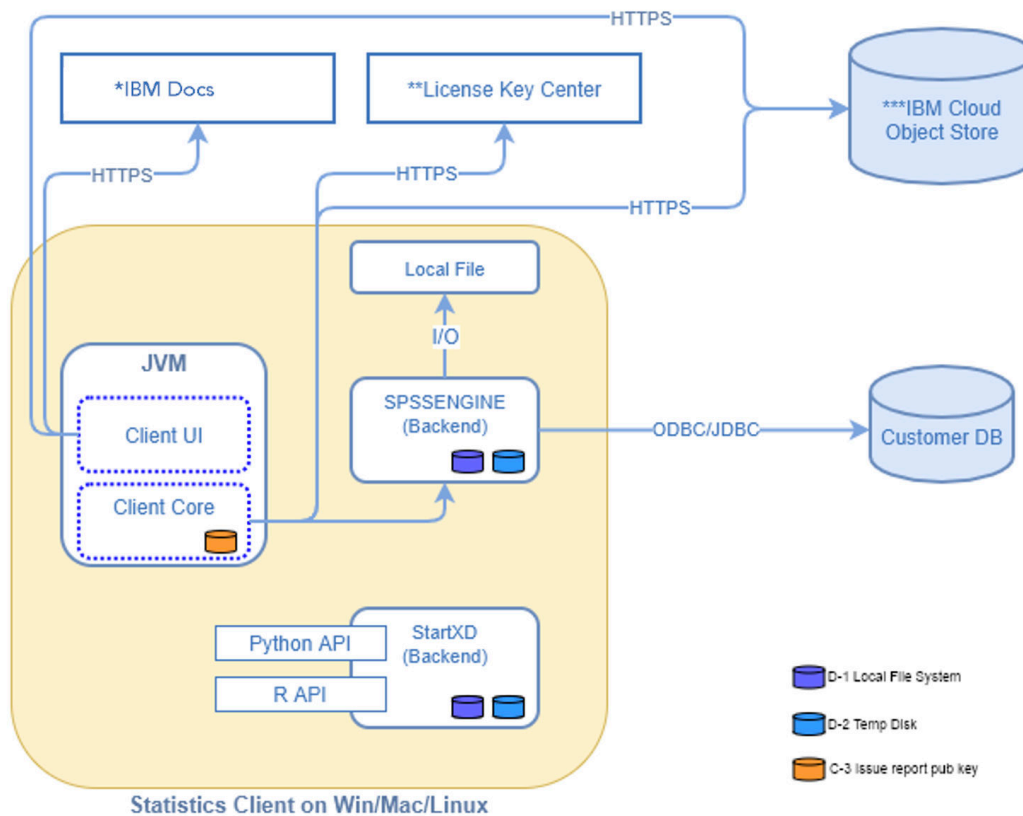


Figura 1. Modo de análisis distribuido

Para los análisis que no requieren un acceso intensivo a los datos o un proceso numérico, el software de cliente se puede utilizar como una aplicación de escritorio autónoma estándar. Cuando se está en modo de análisis local, el acceso a todos los datos y el procesamiento estadístico se manejan en el ordenador del usuario final.



* User on UI to pen the online help document

** Verify the auth code for licensing

*** Access the dynamical content on Welcome dialog and upload the crash issue reports

Figura 2. Modo de análisis local

Componentes de software

Como se muestra en la figura "Modo de análisis distribuido", los componentes de la tecnología de servidor son los siguientes. (Consulte Figura 1 en la página 2.)

Software cliente. La aplicación cliente es una instalación completa del producto IBM Corp. del usuario final (por ejemplo, IBM SPSS Statistics). Cuando se utiliza para el análisis distribuido, sólo se utilizan la interfaz gráfica de usuario y las prestaciones de edición. Cuando se utiliza para el análisis local, también se utilizan sus capacidades de acceso a datos y procesamiento estadístico.

Software de servidor. El software de servidor está formado por subcomponentes: una infraestructura que gestiona la comunicación cliente/servidor, procesos de cliente que gestionan las solicitudes de cliente y módulos que acceden a los datos y realizan análisis.

- **Infraestructura.** La infraestructura del software de servidor es un servicio (en Windows) o daemon (en UNIX). Maneja toda la comunicación entre la aplicación cliente y los módulos. La infraestructura se ejecuta continuamente en el sistema servidor, a la espera de conexiones de cliente. Cuando un cliente se conecta, la infraestructura inicia un proceso que maneja las solicitudes para ese cliente.
- **Proceso de cliente.** Un proceso de cliente es efectivamente una sesión para el cliente. Hay un proceso para cada cliente. Un proceso se inicia cuando el cliente se conecta y termina cuando el cliente se desconecta. El proceso gestiona las solicitudes de datos y análisis de sus clientes. Carga los módulos necesarios para acceder a los datos y analizarlos. Descarga módulos cuando ya no son necesarios.
- **Módulos.** Un módulo es una biblioteca ejecutable, DLL o compartida que accede a los datos y ejecuta procedimientos analíticos. El software de servidor analítico tiene varios módulos. Los módulos se cargan a petición. Los módulos pueden cargar otros módulos.

Utilización de la modalidad distribuida

Los pasos siguientes se producen cuando un usuario final ejecuta un producto en modo de análisis distribuido:

1. **Inicie la aplicación cliente.** El usuario final lanza el software de cliente en su ordenador de sobremesa. La aplicación cliente presenta una interfaz de usuario completa.
2. **Conectar con el servidor.** El usuario final se conecta al software de servidor iniciando sesión desde la aplicación cliente. El servicio o daemon de la infraestructura de servidor siempre está en ejecución, a la espera de solicitudes de conexión. Cuando se efectúa una conexión, el software del servidor inicia un proceso para manejar el usuario final.
3. **Acceder a los datos.** El usuario final accede a los datos como de costumbre desde la aplicación cliente, excepto que su vista de controladores de base de datos, archivos de datos, directorios y unidades representa el sistema servidor remoto, no el sistema de escritorio. El proceso de servidor carga los módulos de acceso a datos adecuados y recupera los datos. Se envía un pequeño segmento de los datos a la aplicación cliente para que el usuario final pueda hacer referencia a él al seleccionar un análisis. La mayoría de los datos permanecen en el servidor. También puede configurar el software de servidor para evitar que se envíen datos a la aplicación cliente. Puede utilizar la aplicación de administración (IBM SPSS Statistics Administration Console, que se instala como parte de IBM SPSS Deployment Manager) para evitar que los datos se envíen a todos los clientes. Consulte el tema Usuarios en la publicación *Deployment Manager User's Guide* (que se incluye en la ayuda de IBM SPSS Servicios de Colaboración e Implantación) para obtener más información. También puede configurar el acceso para cada usuario o grupo. Consulte el tema IBM SPSS Statistics Server User Profiles and Groups, en la publicación *Deployment Manager User's Guide*, para obtener más información.
4. **Analizar los datos.** Utilizando la interfaz de usuario de la aplicación cliente, el usuario final selecciona los datos y solicita el tipo de análisis que desea. La solicitud se envía al proceso del servidor, que carga los paquetes de análisis de datos adecuados y procesa el análisis. Todas las tareas relacionadas con los datos, como leer datos, transformar datos, calcular nuevas variables y calcular estadísticas, se realizan en el sistema servidor.
5. **Revise los resultados.** El software de servidor envía la salida de la solicitud del cliente de nuevo a la aplicación cliente. Sólo se envían los resultados, los datos permanecen en el servidor. A continuación, el usuario final puede utilizar la aplicación cliente para refinar y editar los resultados.

Administración de software de servidor

Esta guía está pensada principalmente para los administradores del sistema que son responsables de integrar la tecnología de servidor en un entorno de red en el que las aplicaciones cliente se ejecutan en modo de análisis distribuido. Las tareas administrativas incluyen:

Instalación. El software de servidor está diseñado para ejecutarse continuamente y responder a los inicios de sesión y solicitudes de los equipos de escritorio del usuario final. Seleccione un equipo servidor apropiado para el software servidor-uno que tenga poco tiempo de inactividad, esté configurado para el acceso de usuario final y esté conectado en red a los equipos de escritorio apropiados. Cuanto más memoria y potencia de proceso tiene el sistema servidor, más rápido se manejan las solicitudes de cliente. La aplicación cliente debe estar instalada en los equipos de escritorio del usuario final. La instalación del cliente se puede realizar desde una ubicación de red. [Capítulo 2, “Instalado”, en la página 7](#) proporciona una visión general de cómo instalar el software de servidor y la aplicación cliente. Se incluyen instrucciones de instalación detalladas en el producto DVD.

Acceso a datos. Si necesita proporcionar a los usuarios finales acceso a los datos de un servidor remoto mientras trabajan en modalidad distribuida, el software del servidor debe poder acceder a dichos datos. Los productos de IBM Corp. pueden acceder a los datos desde diversos tipos de archivos de datos, incluidas las bases de datos. Para facilitar el trabajo, los productos de IBM Corp. se distribuyen con DataDirect Connect ODBC para acceder a los datos de una base de datos. [Capítulo 3, “Acceso a datos”, en la página 9](#) introduce el acceso a datos para productos IBM Corp. . Se incluye documentación adicional en el producto DVD.

Configuración y mantenimiento. Puesto que el software del servidor está pensado para un funcionamiento continuo, un administrador del sistema debe supervisarlos a intervalos regulares. Hay varias opciones de configuración que le dan control sobre cómo funciona el software del servidor. Capítulo 4, “Configuración, supervisión del uso y mantenimiento”, en la página 15 analiza la configuración y supervisión del software del servidor.

Soporte a usuarios finales. Los usuarios finales requieren información sobre nombres de servidor, cuentas de usuario y dónde encontrar datos. También es posible que necesite asistirlos en la resolución de problemas. Capítulo 5, “Usuarios finales de soporte”, en la página 23 analiza el tipo de soporte que requieren los usuarios finales.

Rendimiento. Capítulo 6, “Análisis y mejora del rendimiento”, en la página 47 proporciona estrategias para mejorar el rendimiento del software de servidor.

Resolución de problemas. “Software de servidor” en la página 51 proporciona sugerencias para la resolución de problemas.

IBM SPSS Statistics Batch Facility (solo IBM SPSS Statistics Server). El producto IBM SPSS Statistics Server incluye IBM SPSS Statistics Batch Facility, que está pensado para la producción automatizada de informes estadísticos. Si está ejecutando IBM SPSS Statistics Server en su sitio, lea Apéndice B, “IBM SPSS Statistics Batch Facility”, en la página 53, que describe el recurso por lotes de IBM SPSS Statistics y las tareas que puede necesitar realizar para soportarlo.

Uso de este documento

Esta guía está pensada principalmente para los administradores del sistema que son responsables de instalar y mantener el software del servidor en un entorno de red en el que las aplicaciones cliente se ejecutan en modo de análisis distribuido.

Capítulo 2. Instalado

Los productos que utilizan la tecnología de servidor se empaquetan en varios soportes: un DVD para el software de servidor y un DVD para la aplicación cliente.

Para desplegar la tecnología de servidor, debe:

- Instale el software de servidor en un sistema servidor en red.
- Instale o supervise la instalación de la aplicación cliente para que sea accesible desde los equipos de escritorio del usuario final.

Este capítulo proporciona una visión general del proceso de instalación. Las instrucciones de instalación detalladas están disponibles en el producto DVD en el directorio */Documentation/<language>/InstallationDocuments*.

Consulte “Productos y sistemas operativos” en la página 1 para obtener una lista completa de los productos de servidor y sus aplicaciones cliente asociadas.

Instalación del software de servidor

Instale el software de servidor en un sistema servidor en red. El sistema servidor debe estar ejecutando la versión adecuada del sistema operativo. Si es posible, utilice un sistema servidor configurado para, y dedicado a, procesamiento numérico rápido y acceso a datos. La potencia de procesamiento y la memoria adicionales mejoran el rendimiento del software del servidor. Los requisitos detallados de hardware y software, incluidos los requisitos del sistema operativo, aparecen en las instrucciones de instalación.

La instalación de la tecnología de servidor instala software que gestiona el acceso a los datos y realiza los cálculos necesarios para el análisis estadístico. También instala un servicio (en Windows) o daemon (en UNIX) que escucha las solicitudes de inicio de sesión de usuario final entrantes y lanza un proceso para manejar cada usuario final.

Para instalar el software de servidor, siga las instrucciones del directorio */Documentation/<language>/InstallationDocuments* en el servidor DVD.

Instalación de la aplicación cliente

La instalación de la aplicación cliente instala el software que maneja la interfaz de usuario y la presentación de los resultados. Debe instalar o supervisar la instalación de la aplicación cliente en el ordenador de sobremesa de cada usuario final. El ordenador de sobremesa debe estar ejecutando Windows y debe cumplir los requisitos mínimos de hardware y sistema operativo. Los requisitos detallados aparecen en las instrucciones de instalación, que se encuentran en el directorio */Documentation/<language>/InstallationDocuments* en el cliente DVD.

Antes de leer cualquier otro documento de instalación, consulte *Getting Started with Installation and Licensing.pdf*.

Capítulo 3. Acceso a datos

Si desea que los usuarios finales puedan acceder a los datos de los servidores remotos, incluidos los datos de las bases de datos, debe planificar, instalar y configurar el acceso a los datos. Para ello, es necesario comprender cómo decide la aplicación dónde buscar los datos. También debe decidir si desea utilizar la tecnología de acceso a datos que ofrece DataDirect Connect ODBC. También puede utilizar orígenes de datos OLE DB.

Vista de los datos

Antes de empezar a planificar el acceso a los datos para los usuarios finales, es importante comprender cómo decide la aplicación qué datos están disponibles para el usuario final. La vista de los datos que se presentan a los usuarios finales depende de cómo están ejecutando el programa, de forma local o en modalidad distribuida.

Análisis en modo local. En la modalidad de análisis local, en la que todos los accesos y procesos de datos se producen en el ordenador local del usuario final, la vista de los archivos de datos, los orígenes de datos ODBC, los directorios y las unidades es desde la perspectiva del ordenador local, es decir, cuando el usuario final intenta abrir un archivo de datos, ve los archivos de datos, los directorios y las unidades de red en su ordenador local.

Análisis en modo distribuido. En la modalidad de análisis distribuido, en la que el acceso y el proceso de datos se producen en un servidor remoto, la vista de archivos de datos, orígenes de datos ODBC, directorios y unidades es desde la perspectiva del sistema servidor, es decir, cuando el usuario final intenta abrir un archivo de datos, ve los archivos de datos, directorios y unidades montadas en el sistema servidor.

El trabajo consiste en configurar el acceso a los datos en modo de análisis local o en modo de análisis distribuido, según lo requiera el usuario final.

Tecnología de acceso a datos

A continuación se proporciona una breve descripción de Connect ODBC. Para obtener más información sobre cómo funciona la tecnología de acceso a datos con los productos IBM Corp. y para obtener enlaces a documentación detallada para bases de datos específicas, consulte *IBM SPSS Data Access Pack Instrucciones de instalación* en el directorio `/Documentation/<language>/InstallationDocuments` en el producto DVD.

Connect ODBC

Connect ODBC es un conjunto completo de controladores individuales específicos de la base de datos que utilizan ODBC para ofrecer conectividad a todos los principales almacenes de datos, desde bases de datos relacionales a datos de archivos sin formato.

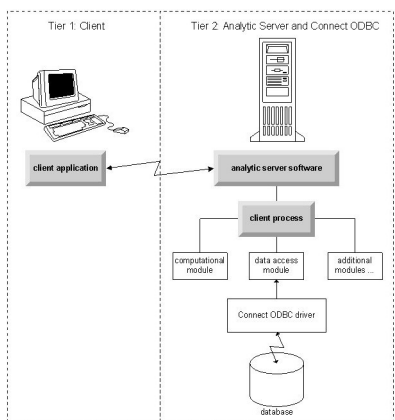


Figura 3. Connect ODBC en análisis en modo distribuido

acceso a datos

Al configurar el acceso a los datos, tenga en cuenta lo siguiente:

Tecnología de acceso a datos. Decida si desea utilizar una de las tecnologías de acceso a datos distribuidas con el producto IBM Corp. . Consulte el tema “Tecnología de acceso a datos” en la página 9 para obtener más información. En las *IBM SPSS Data Access Pack Instrucciones de instalación* (en / Documentation/<language>/InstallationDocuments en el producto DVD) aparece una descripción más detallada de cómo elegir una tecnología.

Modo de análisis. El modo de análisis del usuario final determina a qué datos puede acceder. Consulte el tema “Vista de los datos” en la página 9 para obtener más información.

Rendimiento del sistema de archivos (sólo Windows). Si la mayoría de los datos están en un formato propietario de IBM Corp. (por ejemplo, archivos .sav) en lugar de en una base de datos, le recomendamos que almacene los datos en una unidad NTFS de Windows en red para obtener el mejor rendimiento.

Formato de archivo. El software maneja la apertura y lectura de archivos en formato UNIX automáticamente-usted y sus usuarios finales no necesitan tomar ninguna acción para decirle al software que un archivo está en formato UNIX.

Datos de referencia

Algún software de cliente permite al usuario final guardar referencias a datos y otros archivos. Estas referencias deben escribirse desde la perspectiva del ordenador que accederá a los datos. Por ejemplo, si el usuario final se ejecuta en modalidad de análisis local, una referencia a `C:\mydata\mydata.sav` hace que el software intente acceder al archivo en la unidad `C` local del sistema de escritorio. Si el usuario final se está ejecutando en modo de análisis distribuido, la misma referencia a `C:\mydata\mydata.sav` hace que el software intente acceder al archivo en la unidad `C` local de sistema servidor, lo que podría provocar un error.

Windows. Si está administrando un sistema Windows, puede decidir almacenar datos en el mismo sistema que el software del servidor. Si lo hace, recomendamos que los usuarios hagan referencia a la ubicación de los datos desde la perspectiva del sistema servidor (por ejemplo, `C:\ServerData\mydata.sav`). El rendimiento es más rápido porque la red no se utiliza para localizar el archivo. Si los datos están en otro sistema en red, se recomienda que los usuarios utilicen referencias de archivo UNC (por ejemplo, `\\mydataserver\ServerData\mydata.sav`). Tenga en cuenta que los nombres UNC solo se pueden utilizar cuando las ubicaciones referenciadas contienen el nombre de un recurso compartido en la red. Se recomienda a los usuarios finales que cambian con frecuencia del modo de análisis distribuido al local que utilicen referencias de archivo UNC porque funcionan independientemente del modo.

UNIX. Si está administrando una versión UNIX del software de servidor, puede decidir poner archivos en un servidor UNIX. Los usuarios finales pueden hacer referencia a archivos en un servidor UNIX-indicarles que utilicen la especificación de archivo completa y las barras inclinadas (por ejemplo, `/FILE = '/public/`

data/ourdata.txt.) Evite utilizar el carácter de barra inclinada invertida en el directorio UNIX y en los nombres de archivo utilizados con el software de servidor.

Control de acceso a datos

Puede controlar el acceso a los datos utilizando el sistema operativo para establecer permisos por ID de usuario y grupos. El usuario final se conecta al software de servidor iniciando sesión desde la aplicación cliente. El software de servidor utiliza el sistema operativo para imponer los permisos para ese usuario.

Nota: Es posible que se pueda aplicar una seguridad de datos adicional con el software de base de datos: los módulos de acceso a datos del software del servidor solicitan ID y contraseñas cuando la base de datos los requiere.

Windows. La forma en que se establecen los permisos de acceso en Windows depende de dónde se almacenan los datos.

- Si los archivos residen en un sistema en red que no sea el sistema que ejecuta el software de servidor, asigne permisos a los recursos compartidos.
- Si los archivos residen en el sistema servidor y en una unidad NTFS, utilice los valores de seguridad. No puede controlar el acceso a archivos para los datos en el sistema servidor en una unidad FAT.

Consulte “Propiedades del archivo” en la [página 55](#) para obtener información sobre cómo establecer permisos de compartición y seguridad en Windows.

UNIX. Cuando el usuario final se conecta al software de servidor iniciando sesión desde la aplicación cliente, el software de servidor pasa el ID de inicio de sesión y la contraseña del usuario al sistema operativo y lanza un proceso para el usuario. El proceso iniciado tiene los derechos de acceso al archivo de la cuenta de inicio de sesión del usuario final.

Orígenes de datos

ODBC

El software de servidor de IBM SPSS Statistics utiliza ODBC para acceder a la mayoría de los datos que no están en un formato propietario, incluidos los datos almacenados en bases de datos. ODBC requiere un origen de datos ODBC. Un origen de datos ODBC es la combinación de:

- Un nombre descriptivo
- Un controlador específico
- Una referencia a una base de datos u otro tipo de archivo de datos

Para acceder a la mayoría de los datos, debe configurar, o ayudar a los usuarios finales a configurar, los orígenes de datos ODBC que necesitan.

La ubicación del origen de datos configurado es crítica. Debe estar configurado en el sistema que está accediendo y procesando los datos; por lo tanto, configure el origen de datos ODBC en el *sistema servidor* para el análisis distribuido y en el *sistema de escritorio* para el análisis local. Por ejemplo, compare la ubicación de los controladores ODBC en las figuras que se muestran en “Connect ODBC” en la [página 9](#).

Si está empezando a utilizar la tecnología de acceso a datos (introducida en “Tecnología de acceso a datos” en la [página 9](#)), debe realizar algunas tareas adicionales antes de configurar un origen de datos. Consulte las *IBM SPSS Data Access Pack Instrucciones de instalación* (en /Documentation/<language>/InstallationDocuments en el producto DVD). La configuración del origen de datos se describe de nuevo en [Capítulo 4](#), “Configuración, supervisión del uso y mantenimiento”, en la [página 15](#) de esta guía.

Configuración del entorno UNIX para acceso a datos

Para que la tecnología de acceso a datos funcione en sistemas UNIX, se debe configurar el script de inicio del software del servidor.

Abrir el script de inicio

1. Vaya al subdirectorio `/bin` en el directorio de instalación del software de servidor. Por ejemplo, en la solicitud de UNIX, escriba:

```
cd /usr/local/serverproduct/bin
```

donde `/usr/local/serverproduct/bin` es el subdirectorio `/bin` del directorio en el que está instalado el software del servidor.

2. Abra `statsenv.sh` con un editor de texto.

Especifique el script DataDirect

1. Busque el primer comentario que contiene el texto:

```
SCRIPT_ENTORNO_ENTORNO
```

2. Busque la línea que define la ubicación de `odbc.sh`.
3. Edite la línea para que contenga la vía de acceso correcta a la instalación del cliente de Connect ODBC y elimine el carácter de comentario si tiene uno. Por ejemplo, cambie:

```
# MERANT_ENVIRONMENT_SCRIPT=/usr/slodbc50/5_01_00/odbc.sh
```

a:

```
MERANT_ENVIRONMENT_SCRIPT=/usr/myDataAccess/slodbc50/5_01_00/odbc.sh
```

Añadir variable de entorno odbc.ini

1. Añada las líneas siguientes después de las líneas anteriores para crear una variable de entorno, `ODBCINI`, que permita a IBM SPSS Statistics Server encontrar el archivo `odbc.ini` :

```
ODBCINI=ODBCDIR/odbc.ini  
export ODBCINI
```

donde `ODBCDIR` se sustituye por la vía de acceso al directorio de instalación de Connect ODBC .

Añadir vías de acceso a bibliotecas de base de datos

1. Añada las líneas adecuadas para la base de datos, normalmente el *directorio de inicio de la base de datos* y, si *no* utiliza los controladores Data Direct Wire Protocol, una *vía de acceso a las bibliotecas de base de datos*. Por ejemplo, si utiliza Oracle en Linux, añada las líneas siguientes:

```
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/bigdisk/oracle/product/8.1.6/lib  
export LD_LIBRARY_PATH  
ORACLE_HOME=/bigdisk/oracle/product/8.1.6  
export ORACLE_HOME
```

donde `/bigdisk/oracle/product/8.1.6` se sustituye por la vía de acceso al directorio de instalación de Oracle y `LD_LIBRARY_PATH` es la variable de vía de acceso de biblioteca para el sistema operativo.

Tenga en cuenta que los controladores Data Direct Wire Protocol no requieren la instalación de bibliotecas de cliente de base de datos. Sin embargo, otros controladores Data Direct requieren estas bibliotecas.

Guardar el script de inicio

1. Guarde `statsenv.sh`.

Edite odbc.ini

1. Edite `odbc.ini`, el archivo de configuración ODBC , para que se pueda acceder a los orígenes de datos de ODBC desde IBM SPSS Statistics Server. Consulte el apéndice "El entorno UNIX" en la publicación *DataDirect Connect ODBC Reference* de DataDirect(disponible si ha instalado la documentación

adicional de DataDirect al instalar Connect ODBC) y los capítulos para controladores específicos en *odbchelp.pdf* en el subdirectorio *doc* del directorio de instalación de Connect ODBC .

El cambio entrará en vigor la próxima vez que inicie el software del servidor.

Nota: Si tiene previsto utilizar ODBC con IBM SPSS Statistics Batch Facility, debe modificar el script de inicio de IBM SPSS Statistics Batch Facility de la misma forma.

Capítulo 4. Configuración, supervisión del uso y mantenimiento

Después de instalar el software de servidor, configure su entorno de la siguiente forma:

- Gestión de cuentas y archivos de usuario final
- Configuración de orígenes de datos ODBC
- Utilización de la aplicación de administración (IBM SPSS Statistics Administration Console) para configurar y supervisar el software de servidor
- Control del inicio del servicio

Estas tareas se describen en las secciones siguientes.

Gestión de cuentas y archivos de usuario final

Esta sección proporciona una visión general de lo que necesita hacer para dar soporte a los usuarios finales en su sitio. Para obtener más información, consulte el tema [Capítulo 5, “Usuarios finales de soporte”](#), en la página 23.

Cuentas

Los usuarios finales necesitan cuentas para poder iniciar sesión en el software del servidor y acceder a los datos. Estas cuentas deben estar autenticadas y deben ser capaces de leer, escribir y/o ejecutar en carpetas específicas en la máquina del servidor. Para obtener más información sobre los permisos de archivo, consulte el tema [“Permisos”](#) en la página 31. Para obtener más información sobre la autenticación, consulte el tema [“Autenticación”](#) en la página 23.

El software de base de datos impone los permisos de base de datos. Utilice las herramientas de administración de base de datos habituales para gestionar estas cuentas. Si la base de datos está restringida, los módulos de acceso a datos del software del servidor solicitan al usuario que inicie sesión y devuelva dicha información a la base de datos para su verificación antes de acceder a los datos.

Acceso a datos

De forma predeterminada, cada usuario final puede ver todos los datos al abrir un archivo mientras está conectado al software del servidor. La visualización de todos los datos puede afectar negativamente al rendimiento y aumentar el tráfico de red. Puede optar por impedir que los sistemas cliente de usuario final muestren los datos cambiando el valor global con la aplicación de administración (IBM SPSS Statistics Administration Console, que se instala como parte de IBM SPSS Deployment Manager). Consulte el tema [Usuarios](#) en la publicación *Deployment Manager User's Guide* (que se incluye en la ayuda de IBM SPSS Servicios de Colaboración e Implantación) para obtener más información. También puede modificar los valores de perfil de usuario y grupos para especificar el acceso a datos para usuarios o grupos individuales. Consulte el tema [IBM SPSS Statistics Server User Profiles and Groups](#), en la publicación *Deployment Manager User's Guide*, para obtener más información.

Archivos

La mayoría de los archivos que los usuarios finales necesitan guardar deben guardarse en la computadora de escritorio; sin embargo, es posible que desee permitir que los usuarios guarden archivos de datos en una computadora en red. Cuando el usuario final inicia sesión en el software del servidor analítico por primera vez, el directorio predeterminado para abrir y guardar archivos es el directorio de instalación del software del servidor. Es evidente que no se trata de una ubicación en la que desee que los usuarios escriban archivos, así que configure un directorio con permiso de escritura y distribuya dicha ubicación

a los usuarios finales. Una vez que accedan a esa ubicación desde la interfaz de usuario, la aplicación cliente la almacenará y se convertirá en la ubicación predeterminada para los archivos guardados.

Perfiles

El software de servidor también le permite crear perfiles para los usuarios. Un perfil puede especificar el directorio temporal, el valor umask de UNIX, la prioridad de proceso de CPU, el valor de acceso a datos de cliente y el número máximo de hebras para cada usuario o grupo de usuarios.

Grupos y perfiles de usuario del servidor de IBM SPSS Statistics

El software de servidor proporciona la capacidad de crear perfiles de usuarios individuales y grupos de usuarios. El perfil especifica el directorio de los archivos temporales, el valor umask de UNIX, la prioridad de proceso de la CPU, el acceso a datos de cliente y el número máximo de hebras para el usuario o grupo de usuarios. Estos ajustes anulan los ajustes globales por defecto asociados. .

Archivo de perfiles

Los valores de grupo y perfil de usuario se almacenan en el archivo de perfil *UserSettings.xml*. Por defecto, este archivo se encuentra en el subdirectorio `config` del directorio de instalación del servidor IBM SPSS Statistics. Antes de realizar cambios en los perfiles y grupos de usuarios, se recomienda mover el archivo predeterminado y especificar la nueva ubicación en la aplicación de administración (IBM SPSS Statistics Administration Console).

Cómo aplica el servidor los valores

El servidor sigue estos pasos para determinar el directorio de archivos temporales, el valor de umask, la prioridad de la CPU, el acceso a datos de cliente y el número máximo de hebras de un usuario determinado.

1. Buscar un perfil de usuario para el nombre de usuario y el dominio del usuario que se conecta al servidor. Seleccione la primera coincidencia encontrada. En UNIX, el servidor ignora el dominio, y el nombre de usuario es sensible a mayúsculas y minúsculas. En Windows, el dominio y las mayúsculas y minúsculas del nombre de usuario no tienen importancia. Además, si un usuario ha iniciado sesión en el servidor sin especificar un dominio, el servidor buscará una coincidencia de nombre de usuario con un dominio en blanco. Si no puede encontrar uno, utilizará solo una coincidencia con el nombre de usuario.
2. Si el perfil de usuario define los valores, aplique estos valores al proceso del servidor.
3. Si el perfil de usuario no define los valores o no los define todos, aplique los valores del grupo del usuario al proceso del servidor.
4. Si algunas configuraciones aún no están definidas o no había ningún perfil de usuario coincidente, aplica la máscara de umask por defecto, el directorio de archivos temporales, la configuración de acceso a datos del cliente y el número máximo de hilos definidos por la aplicación de administración (IBM SPSS Statistics Administration Console). No se utiliza el procesamiento de prioridad de CPU predeterminado. .

Configuración de orígenes de datos ODBC

Si los usuarios finales acceden a datos de bases de datos mientras trabajan en modo de análisis distribuido, debe configurar orígenes de datos ODBC en el sistema en el que está instalado el software de servidor.

Orígenes de datos ODBC y IBM SPSS Data Access Pack

Si está utilizando la tecnología de acceso a datos de IBM Corp. , lea [Capítulo 3, “Acceso a datos”](#), en [la página 9](#) en este documento. Lea las *Instrucciones de instalación* correspondientes para obtener una visión general de la configuración del acceso a bases de datos y enlaces a documentación detallada

sobre el acceso a datos para bases de datos específicas (el documento se encuentra en */Documentation/<language>/InstallationDocuments* en el producto DVD).

Windows. Configure orígenes de datos ODBC utilizando el administrador de ODBC . Consulte el tema “Administrador de ODBC” en la página 56 para obtener más información.

UNIX. Edite el script de entorno de inicio para el software de servidor tal como se describe en “Configuración del entorno UNIX para acceso a datos” en la página 11 y configure los orígenes de datos de ODBC utilizando el archivo *odbc.ini* . Consulte el tema “odbc.ini” en la página 60 para obtener más información.

Utilización de un motor de clasificación de terceros

De forma predeterminada, el software de servidor intenta utilizar un motor externo de terceros para la ordenación. Para utilizar el motor de ordenación correcto, realice los pasos siguientes:

1. Si el motor de ordenación de terceros no está instalado en el sistema servidor, instálelo. IBM Corp. no proporciona los motores. Debe adquirir y obtener una licencia de un motor de un proveedor de terceros.
2. Asegúrese de que la biblioteca del motor de clasificación está en la variable de vía de acceso de biblioteca o ejecución del sistema. En Windows, es la variable de entorno PATH; en UNIX, es LD_LIBRARY_PATH o LIBPATH, en función del proveedor de UNIX. Este paso es necesario para permitir que el software del servidor cargue la biblioteca de clasificación de terceros.
3. Utilizando la aplicación de administración (IBM SPSS Statistics Administration Console, que se instala como parte de IBM SPSS Deployment Manager), establezca la opción Ordenar en el motor de terceros adecuado. Consulte el tema Usuarios en la publicación *Deployment Manager User's Guide* (que se incluye en la ayuda de IBM SPSS Servicios de Colaboración e Implantación) para obtener más información.

Cualquier procedimiento que requiera clasificación (por ejemplo, SORT) utilizará posteriormente el motor de clasificación de terceros. La emisión del mandato de sintaxis SET SORT=INTERNAL fuerza al software del servidor a utilizar el algoritmo interno para la ordenación. Un usuario final también puede especificar explícitamente la ordenación de terceros emitiendo el mandato SET SORT=EXTERNAL . Sin embargo, esto no es necesario porque la ordenación de terceros es el valor predeterminado.

Comprobación de la opción de ordenación actual

Para comprobar qué opción de ordenación se está utilizando, puede emitir el mandato de sintaxis SET MESSAGES ON y ejecutar un trabajo SORT . También puede utilizar el mandato de sintaxis SHOW SORT .

Administración de servidor de IBM SPSS Statistics

La IBM SPSS Statistics Administration Console proporciona una interfaz de usuario para supervisar y configurar las instalaciones del servidor de IBM SPSS Statistics. El IBM SPSS Statistics Administration Console se instala como parte de IBM SPSS Deployment Manager. La documentación completa de IBM SPSS Statistics Administration Console se incluye en la sección *Consolas de administración* de la *Guía del usuario del gestor de despliegue* (incluida en la ayuda para IBM SPSS Servicios de Colaboración e Implantación).

Configuración de Xtensiones

Un administrador de IBM SPSS Statistics Server debe seguir los pasos para que los procedimientos Xtension (krr, lenr, lrr y lrr) estén disponibles para ejecutarse en **statsb** y SPSS Statistics Server. Los procedimientos Xtension incluyen:

- Regresión Kernel Ridge (KRR)
- Regresión de red elástica lineal (LENR)
- Regresión de lazo lineal (LLR)

- Regresión de cresta lineal (LRR)

Instalación de Xtensiones en SPSS Statistics Server

1. En el cliente IBM SPSS Statistics , instale las tensiones (en modalidad local) desde el Hub de extensión.
2. Asegúrese de que la biblioteca **sklearn** está instalada en el servidor de IBM SPSS Statistics .

UNIX[®]

Ejecute el mandato siguiente como el usuario que ha instalado SPSS Statistics Server.

```
./statisticspython3 -m pip install sklearn
```

Nota: statisticspython3 se encuentra en el directorio bin de la instalación de SPSS Statistics Server.

Windows[®]

Ejecute el mandato siguiente.

```
statisticspython3.bat -m pip install sklearn
```

Nota: statisticspython3.bat Se encuentra en el directorio de instalación de SPSS Statistics Server.

3. Copie el directorio xtensions y su contenido del cliente SPSS Statistics (%APPDATA%\IBM\SPSS Statistics\one\xtensions\ en Windows, \$HOME/Library/Application Support/IBM/SPSS Statistics/one/xtensions en macOS) en el directorio de instalación de SPSS Statistics Server.

El servidor de SPSS Statistics ahora está preparado para ejecutar los procedimientos Xtension que están instalados en el directorio xtensions .

Configuración de la interfaz de línea de comandos de unidad de producción para enviar trabajos

A partir de IBM SPSS Statistics versión 26, puede utilizar la interfaz de línea de comandos Unidad de producción para enviar trabajos al servidor de SPSS Statistics. Cuando la interfaz de línea de comandos Unidad de producción se utiliza junto con el Programador de tareas de Microsoft Windows/macOS Automator para planificar trabajos, puede sustituir de forma efectiva IBM SPSS Servicios de Colaboración e Implantación para procesar trabajos de SPSS Statistics.

El mandato SPSS Statistics **INSERT HIDDEN** puede ejecutar trabajos que generan salida. Cuando se utiliza el comando, los usuarios no pueden acceder o ver la sintaxis de SPSS Statistics de origen.

Nota: El comando **INSERT HIDDEN** requiere un servidor de SPSS Statistics. El mandato no funcionará en una máquina cliente de SPSS Statistics.

Característica INSERT HIDDEN

Los administradores pueden habilitar la característica **INSERT HIDDEN** utilizando la consola de administración del servidor de SPSS Statistics o editando el archivo <install_path>/config/statisticsd.conf (**INSERT HIDDEN = Enabled**). El campo **INSERTAR CARACTERÍSTICA OCULTA** se encuentra en la pestaña Configuración del servidor SPSS Statistics de la consola de administración de SPSS Statistics Server (en la sección **Usuarios**).

1. Seleccione **Habilitado** como valor de **Característica INSERT HIDDEN**. Tenga en cuenta que un asterisco(*) aparece en la pestaña Configuración de servidor de SPSS Statistics.
2. Guarde el cambio. Pulse el icono **Guardar** en la barra de herramientas, Control-S, o seleccione **Archivo > Guardar**.
3. Reinicie el servidor SPSS Statistics.

- Después de que el servidor se reinicie en servidores Windows, aparece un diálogo solicitando al administrador que introduzca la contraseña de la **característica INSERT HIDDEN**. En servidores Linux, el administrador debe iniciar manualmente el servidor de SPSS Statistics. Cuando se reinicia el servidor, éste solicita la contraseña al administrador.

La contraseña se almacena en el registro del sistema (parecido a una contraseña SSL) y todos los archivos de sintaxis ocultos se cifran a través de la misma contraseña.

De forma opcional, el administrador puede denegar el acceso de usuario a los archivos **INSERT HIDDEN** a través de los controles de acceso del sistema de archivos.

El proceso de daemon de servidor de SPSS Statistics requiere acceso de lectura a los archivos **INSERT HIDDEN**. Se puede utilizar un comando OMS para envolver la sintaxis para asegurar que los resultados no se envían al Visor de resultados.

```
OMS /SELECT ALL /DESTINATION VIEWER=NO.  
* commands executed here will not output to the viewer.  
DESC ALL.  
FREQ ALL.  
OMSEND.
```

La sintaxis de **INSERT HIDDEN** es parecida a la sintaxis **INSERT FILE**. Por ejemplo:

```
INSERT HIDDEN  
SOURCE='source specification'  
[SYNTAX = {INTERACTIVE*}]  
  {BATCH }  
[ERROR = {CONTINUE*}]  
  {STOP }  
[ENCODING = 'encoding specification']
```

El autor del archivo **INSERT HIDDEN** proporciona las vías de acceso del archivo oculto para los usuarios del cliente de SPSS Statistics. Durante el tiempo de ejecución, los usuarios del cliente ejecutan la sintaxis **INSERT HIDDEN SOURCE="<file_path>"**.

Consulte la publicación *IBM SPSS Statistics Command Syntax Guide* para obtener información más detallada.

El proceso de cliente en el servidor de SPSS Statistics envía la vía de acceso de **SOURCE** al proceso de daemon del servidor. El proceso del daemon descifra el archivo y, a continuación, lo devuelve al proceso de cliente para su ejecución.

El proceso de cliente inhabilita registros y diarios, ejecuta el archivo descifrado y, a continuación, vuelve a habilitar registros y diarios. El resultado que es que el visor de resultados de SPSS Statistics no contiene ningún registro de sintaxis de origen (contiene resultados). El diario tampoco contiene sintaxis de origen.

Configuración de varias instancias

Puede crear varias instancias del software de servidor, cada una con su propio número de puerto. A menudo se utiliza de forma conjunta con la autorización de grupo para asignar un grupo de usuarios a una instancia específica. Sin embargo, se pueden utilizar varias instancias independientemente de la autorización de grupo. Para obtener más información sobre la autorización de grupo, consulte [“Autorización de grupo” en la página 31](#).

Creación de una instancia nueva

Para crear una instancia de grupo del software de servidor, debe ejecutar un script.

En Windows, ejecute el script siguiente desde el directorio de instalación del servidor.

```
create_group_service <group_name> <port_number>
```

En UNIX y Linux, ejecute el script siguiente del subdirectorio bin del directorio de instalación.

```
create_group_configuration -group <group_name> -port <port_number>
```

<group_name> es un nombre exclusivo para la instancia y <port_number> es el número de puerto disponible que utilizará la instancia.

Después de ejecutar el script, habrá una carpeta de configuración que sea específica para la instancia. Busque `config_<groupname>` en la dirección de instalación del servidor. La carpeta contiene varios archivos de configuración como, por ejemplo, `statisticsd.conf` y `UserSettings.xml`. Cuando desee actualizar la configuración de una instancia específica, asegúrese de actualizar el archivo de configuración en la ubicación correcta.

Inicio de la instancia del servidor

En Windows, la instancia es un servicio aparte llamado *IBM SPSS Statistics NN.m*, donde *NN* es el número de versión principal y *m* es el número de versión menor. Puede iniciar y detener este servicio como cualquier otro servicio de Windows.

En Linux y UNIX, tiene que especificar el nombre de grupo al ejecutar el script de inicio:

```
./start_statistics_server -d -g <group_name>
```

donde <group_name> es el nombre del grupo de instancias.

Eliminación de una instancia de servidor

1. En Windows, elimine la entrada de servicio:
 - a. Abra un indicador de comandos como Administrador.
 - b. Ejecute el mandato siguiente:

```
sc delete "IBM SPSS Statistics NN.m Server <group_name>"
```

donde *NN* es el número de versión principal, *m* es el número de versión menor y < nombre_grupo> es el grupo de instancias.

2. Suprima el subdirectorío `config_<groupname>` en el directorío de instalación del servidor.

Control del inicio del servicio

El software de servidor tiene un componente de infraestructura que maneja todas las comunicaciones entre la aplicación cliente y los módulos. En Windows, el componente de infraestructura es un servicio. En UNIX, el componente de infraestructura es una aplicación, normalmente se ejecuta como daemon.

Windows

De forma predeterminada, el servicio está configurado para el inicio automático, lo que significa que se reiniciará automáticamente cuando se reinicie el sistema. Cuando se inicia de esta forma, el servicio se ejecuta de forma desatendida y el sistema del servidor puede desconectarse sin que ello afecte al servicio. Puede utilizar el Panel de control de servicios de Windows para cambiar los parámetros de inicio del servicio. Consulte el tema “Panel de control de servicios” en la página 56 para obtener más información. Si está ejecutando varias instancias, el Panel de servicios incluirá una entrada para cada instancia de servidor.

Nota: Si el sistema servidor no da soporte a la dirección IP localhost (127.0.0.1:::1), debe crear una variable de entorno del sistema denominada `STATS_LH_OVERRIDE` y establecer su valor en YES antes de iniciar el servidor. Para obtener información sobre cómo iniciar y detener el servidor, consulte “Inicio y detención del software de servidor” en la página 22.

UNIX

Se incluye un script de inicio, `start_statistics_server`, en el subdirectorío `/bin` del directorío de instalación. El script llama a `statsenv.sh` para configurar el entorno para el software de servidor y, a continuación, inicia la aplicación. Debe iniciar el software de servidor con este script. El script de inicio debe ejecutarse desde el subdirectorío `/bin`. Para ejecutarlo, debe haber iniciado sesión como **root** si utiliza la autenticación unix predeterminada o el módulo de autenticación conectable (PAM). De lo contrario, debe haber iniciado la sesión como el usuario propietario del daemon de software de

servidor. Para obtener más información sobre la autenticación, consulte el tema [“Autenticación”](#) en la [página 23](#). El mandato:

```
./start_statistics_server -d
```

iniciará el software del servidor como un proceso de daemon, que es la forma recomendada para ejecutar el software del servidor.

Si está ejecutando varias instancias del software de servidor, este mandato iniciará la instancia predeterminada. Para iniciar otra instancia, especifique el grupo de instancias con el conmutador `-g` :

```
./start_statistics_server -d -g <groupname>
```

donde `<groupname>` es el nombre del grupo de instancias.

Nota: Si el equipo servidor no permite utilizar la dirección IP de localhost (127.0.0.1:::1), deben establecer la variable de entorno `STATS_LH_OVERRIDE` en YES para poder iniciar el servidor. `STATS_LH_OVERRIDE` se establece desde `statsenv.sh`, que está incluido en el subdirectorio `/bin` del directorio de instalación. Para obtener información sobre cómo iniciar y detener el servidor, consulte [“Inicio y detención del software de servidor”](#) en la [página 22](#).

Parámetros de línea de mandatos de script de inicio

El script `start_statistics_server` acepta los siguientes parámetros de línea de mandatos (en cualquier orden):

- **Daemon.** Ejecute el software de servidor como un proceso de daemon especificando opcionalmente `-d`. Si omite `-d`, el servidor se iniciará como un proceso en primer plano. Por ejemplo, para iniciar el software de servidor como daemon, utilice el mandato:

```
./start_statistics_server -d
```

- **Grupo.** Si está ejecutando varias instancias del software de servidor, especifique el grupo que está asociado con la instancia:

```
start_statistics_server -g <groupname>
```

donde

`<groupname>` es el nombre de grupo adecuado.

- **Puerto.** Opcionalmente, se puede especificar un número de puerto en la línea de mandatos del script de inicio. Por ejemplo, para especificar un número de puerto, utilice el mandato:

```
start_statistics_server -p nnnn
```

donde

`nnnn` es el número de puerto deseado.

Especifique un número de puerto sólo si necesita resolver un conflicto de número de puerto. El valor predeterminado funcionará a menos que otra aplicación del sistema esté utilizando el mismo número. Este valor de línea de mandatos altera temporalmente el valor establecido en la aplicación de administración.

Otros mantenimientos

Eliminar archivos innecesarios. Compruebe periódicamente la ubicación del archivo temporal y la ubicación del archivo de registro para los archivos innecesarios y elimínelos. Las ubicaciones se definen con la aplicación de administración.

Comprobar procesos en ejecución. Si no reinicia regularmente el sistema servidor, compruebe periódicamente los procesos que se ejecutan en el sistema y finalice los procesos que no estén en uso. Los nombres de proceso se listan en [“Inicio y detención del software de servidor”](#) en la [página 22](#).

Inicio y detención del software de servidor

La aplicación de administración reiniciará automáticamente el software de servidor para que se puedan confirmar los cambios de configuración; sin embargo, a veces es posible que tenga que iniciar o detener el software de servidor desde el sistema operativo. Siga los pasos siguientes para su sistema operativo, utilizando el nombre de proceso del producto de servidor. En Windows, el nombre de servicio predeterminado es *IBM SPSS Statistics NN.m*, donde *NN* es el número de versión principal y *m* es el número de versión menor. Si está ejecutando varias instancias, el nombre de servicio es *IBM SPSS Statistics NN.m < nombre_grupo >*, donde *NN* es el número de versión principal, *m* es el número de versión menor y *< nombre_grupo >* es el grupo de la instancia. En UNIX y Linux, el nombre del daemon es *statisticsd*.

Nota de planificación: La detención del servicio o daemon desconecta a los usuarios finales y termina sus procesos, por lo que debe intentar planificar las tareas de configuración y mantenimiento para un momento en el que espera que pocos usuarios accedan al sistema (por ejemplo, a primera hora de la mañana o a última hora de la noche).

Para iniciar el servicio o el daemon

Windows. Utilice el Panel de control de servicios de Windows para iniciar el servicio. Consulte el tema [“Panel de control de servicios”](#) en la página 56 para obtener más información.

UNIX. Inicie el servidor con el script de inicio, *start_statistics_server*, que se incluye en el subdirectorio */bin* del directorio de instalación. El script de inicio debe ejecutarse desde el subdirectorio */bin*. Para ejecutarlo, debe haber iniciado sesión como **root** si utiliza la autenticación unix predeterminada o el módulo de autenticación conectable (PAM). De lo contrario, debe haber iniciado la sesión como el usuario propietario del daemon de software de servidor. Para obtener más información sobre la autenticación, consulte el tema [“Autenticación”](#) en la página 23.

Para detener el servicio o el daemon

Windows. Utilice el Panel de control de servicios de Windows para detener el servicio. Consulte el tema [“Panel de control de servicios”](#) en la página 56 para obtener más información.

UNIX. Interrumpa el proceso del servidor. (Consulte [“ps y kill”](#) en la página 59 para ver un ejemplo.) El daemon crea automáticamente un archivo (*statisticsd.pid*) que contiene el ID de proceso para el daemon. Puede utilizar este archivo junto con el mandato kill ejecutando lo siguiente desde el subdirectorio *config* del directorio de instalación o *config_<group_name>* para otra instancia del software de servidor:

```
kill -9 `cat statisticsd.pid`
```

Plataforma independiente. Utilice la aplicación de administración (IBM SPSS Statistics Administration Console, que se instala como parte de IBM SPSS Deployment Manager). Consulte el tema Control de IBM SPSS Statistics Server en la publicación *Deployment Manager User's Guide* (incluida en la ayuda de IBM SPSS Servicios de Colaboración e Implantación) para obtener más información.

Configuración para mejorar el rendimiento

Consulte Capítulo 6, “Análisis y mejora del rendimiento”, en la [página 47](#) para obtener información sobre cómo modificar la configuración del software de servidor para mejorar el rendimiento.

Capítulo 5. Usuarios finales de soporte

El soporte a los usuarios finales implica asegurarse de que tienen la información que necesitan para ejecutar su producto IBM Corp. en modo de análisis distribuido. Para utilizar el software de servidor, los usuarios finales deben saber:

- Cómo conectarse al software del servidor.
- Cómo acceder a datos y archivos.
- Dónde guardar datos y archivos.

Autenticación

Tiene varias opciones para autenticar usuarios. Algunas opciones requieren que el servidor se ejecute con privilegios root.

Método	Disponibilidad de SO	¿El servidor debe ejecutarse como sistema/raíz?
Autenticación a nivel de SO estándar (cuenta de Windows o UNIX)	<ul style="list-style-type: none">• Windows• UNIX	Sí
Módulo de autenticación conectable (PAM)	<ul style="list-style-type: none">• UNIX	Sí
Autenticación interna	<ul style="list-style-type: none">• Windows• UNIX	Nee
unix2	<ul style="list-style-type: none">• UNIX	Nee
Inicio de sesión único	<ul style="list-style-type: none">• Windows• UNIX	Nee

Configuración de la autenticación a nivel de sistema operativo

La autenticación a nivel de SO es el método de autenticación predeterminado. Utilice las herramientas de administración del sistema habituales para crear y gestionar cuentas de usuario final de nivel de SO estándar (consulte “Gestor de usuarios” en la página 56 para obtener información sobre cómo acceder al gestor de usuarios de Windows).

Si intenta otro método de autenticación y desea volver a la autenticación a nivel de sistema operativo, debe actualizar el elemento *userauth* en el archivo *statisticsd.conf* y cambiar el parámetro *value* a *unix* o *win32*.

Configuración de PAM

El software de servidor en UNIX puede utilizar Pluggable Authentication Module (PAM) para autenticar usuarios. Primero debe configurar el software de servidor para utilizar PAM. A continuación, configure PAM siguiendo las instrucciones específicas de su proveedor de UNIX. Siga los pasos para Linux. Estos pueden variar, en función de la versión y el proveedor.

Nota: Si el software del servidor se está ejecutando, debe reiniciarlo después de completar todos los pasos.

Configurar el software de servidor para utilizar PAM

1. Inicie sesión en la máquina UNIX como *root*.
2. En el subdirectorio *config* del directorio de instalación de software del servidor, abra el archivo de configuración (por ejemplo, *statisticsd.conf*) en un editor de texto.
3. Busque el elemento *userauth* y cambie el parámetro *value* de *unix* a *pam*.
4. Guarde el archivo.

Configurar PAM en Linux

1. Cambie al directorio de configuración de PAM (por ejemplo, */etc/pam.d*).
2. Utilice un editor de texto para crear un archivo denominado *statisticsd*.
3. Añada la información de configuración de PAM que desee utilizar. Por ejemplo:

```
auth      include      system-auth
account  required    pam_nologin.so
account  include     system-auth
password include     system-auth
session  optional    pam_keyinit.so force revoke
session  include     system-auth
session  required    pam_loginuid.so
```

Nota: Estas líneas pueden variar en función de su configuración concreta. Consulte la documentación de Linux para obtener más información.

4. Guarde el archivo.

Configuración de la autenticación interna

La autenticación interna permite que el software del servidor se ejecute sin privilegios *root*. Sin embargo, limita las conexiones de cliente al mismo acceso de disco. Cada usuario que se conecta al software del servidor tiene la misma seguridad de acceso a disco. Por lo tanto, un usuario puede suprimir el archivo de otro usuario. Si esto es un problema, se recomienda que utilice el método de autenticación *unix2* en su lugar. Este método no restringe las conexiones de cliente porque utiliza el archivo *passwd* de UNIX para la autenticación. Consulte el tema [“Configuración de la autenticación unix2”](#) en la página 25 para obtener más información.



Aviso: No utilice la autenticación interna al ejecutar el daemon/servicio como *root*/*SYSTEM*. Hacerlo es lo mismo que dar acceso *root*/*SYSTEM* a su servidor a cualquier usuario que se conecte.

Configuración de la autenticación interna en UNIX

1. Cree un grupo para los usuarios que se conectarán al software de servidor. Se recomienda denominar a este grupo **statistics**.
2. Un miembro de este grupo debe instalar el software de servidor. Este usuario será el propietario del daemon de software de servidor.
3. Otro miembro de este grupo (distinto del propietario del daemon y normalmente del usuario que mantiene los usuarios de software del servidor) crea un archivo *statisticsusers* en el directorio *config* del directorio de instalación de software del servidor. Este archivo debe tener acceso de lectura/escritura para el usuario que lo ha creado. Debe tener acceso de lectura para el grupo de usuarios. Ningún otro usuario debería poder acceder a él. Si no crea este archivo manualmente, se crea automáticamente la primera vez que ejecuta la herramienta de línea de mandatos *statisticsuser* (consulte el paso siguiente). La herramienta de línea de mandatos establece los permisos adecuados.
4. En el directorio *config*, utilice la herramienta de línea de mandatos *statisticsuser* para añadir usuarios. Como usuario que ha creado el archivo *statisticsusers*, escriba *statisticsuser <username>* para crear un usuario normal (por ejemplo, *statisticsuser jdoe*). Utilice la opción *-a* para crear un usuario administrador (por ejemplo, *statisticsuser -a jdoe*). La herramienta de línea de mandatos *statisticsuser* le solicita una contraseña. Un usuario final especifica el nombre de usuario y la contraseña para conectarse al software de servidor. Asegúrese de distribuir el

nombre de usuario y las contraseñas de forma adecuada. Para suprimir un usuario, utilice la opción `-d` (por ejemplo, `statisticsuser -d jdoe`).

5. Con la sesión iniciada como propietario del daemon de software de servidor, abra el archivo de configuración (por ejemplo, `statisticsd.conf`) en un editor de texto.
6. Busque el elemento `userauth` y cambie el parámetro `value` de `unix` a `internal`.
7. Inicie la sesión como propietario del daemon de software de servidor, inicie el servidor.

Configuración de la autenticación interna en Windows

1. Edite la entrada IBM SPSS Statistics Server para ejecutarla como un usuario específico:
 - a. Abra el Panel de servicios de Windows y efectúe una doble pulsación en la entrada para *IBM SPSS Statistics NN.m*, donde *NN* es el número de versión principal y *m* es el número de versión menor.
 - b. Pulse el separador **Iniciar sesión**.
 - c. En **Iniciar sesión como**, seleccione **Esta cuenta**.
 - d. Especifique el dominio `\nombre_usuario` y la contraseña del usuario que será propietario del proceso de servidor. Este usuario necesitará el privilegio *Iniciar sesión como servicio*.
2. El mismo usuario debe crear un archivo `statisticsusers` en el directorio `config` del directorio de instalación de software del servidor. Este archivo debe tener acceso de lectura/escritura para el usuario que lo ha creado. Ningún otro usuario debe tener acceso de escritura. Si no crea este archivo manualmente, se crea automáticamente la primera vez que ejecuta la herramienta de línea de mandatos `statisticsuser` (consulte el paso siguiente).
3. En el directorio `config`, utilice la herramienta de línea de mandatos `statisticsuser` para añadir usuarios. Como usuario que ha creado el archivo `statisticsusers`, escriba `statisticsuser <username>` para crear un usuario normal (por ejemplo, `statisticsuser jdoe`). Utilice la opción `-a` para crear un usuario administrador (por ejemplo, `statisticsuser -a jdoe`). La herramienta de línea de mandatos `statisticsuser` le solicita una contraseña. Un usuario final especifica el nombre de usuario y la contraseña para conectarse al software de servidor. Asegúrese de distribuir el nombre de usuario y las contraseñas de forma adecuada. Para suprimir un usuario, utilice la opción `-d` (por ejemplo, `statisticsuser -d jdoe`).
4. Si ha iniciado sesión como propietario del daemon de software de servidor, abra el archivo de configuración (por ejemplo, `statisticsd.conf`) en un editor de texto.
5. Busque el elemento `userauth` y cambie el parámetro `value` de `win32` a `internal`.
6. Vaya al Panel de servicios de Windows e inicie el servicio.

Configuración de la autenticación unix2

La autenticación `unix2` permite que el software del servidor se ejecute sin privilegios `root` y se autentique en el archivo `passwd` de UNIX con cuentas de usuario estándar. Un archivo ejecutable (`suauth`) instalado con el software de servidor realiza la autenticación. Para que funcione correctamente, debe establecer los permisos necesarios.

Para configurar la autenticación `unix2`, realice los pasos siguientes:

1. Utilizando `setuid` y `setgid` o control de acceso basado en roles (RBAC), cambie los permisos del ejecutable `suauth` para que el usuario que ejecutará el daemon de software de servidor tenga los permisos de `root` necesarios. Este usuario debe poder autenticar el usuario en el archivo `passwd` y cambiar el ID de usuario y el ID de grupo del proceso de servidor generado para cada usuario final. A continuación se muestran los detalles sobre el establecimiento de permisos. Tenga en cuenta que utiliza RBAC o bien `setuid/setgid` o . No utilice ambos métodos.
2. Abra el archivo de configuración (por ejemplo, `statisticsd.conf`) en un editor de texto.
3. Busque el elemento `userauth` y cambie el parámetro `value` de `unix` a `unix2`.
4. Inicie la sesión como propietario del daemon de software de servidor, inicie el servidor.

Establecimiento de permisos con `setuid` y `setgid`

1. Cree un grupo para el usuario que ejecutará el software de servidor. Se recomienda denominar a este grupo **statistics**. También se recomienda limitar la pertenencia a grupos sólo al usuario que ejecutará el daemon de software de servidor.
2. Un miembro de este grupo debe instalar el software de servidor. Este usuario será el propietario del daemon de software de servidor.
3. Inicie una sesión de terminal como *root*.
4. Vaya al directorio *bin* en el directorio de instalación de software del servidor.
5. Cambie el propietario del archivo *suauth* para que sea *root*.

```
chown root suauth
```

6. Añada los bits `setuid` y `setgid` a *suauth*. Estos bits permiten al usuario del grupo de instalador ejecutar el archivo y ejecutarlo temporalmente como *root*. Los privilegios raíz son necesarios por las razones indicadas anteriormente en este tema.

```
chmod 6550 suauth
```

7. Salga como *root* e inicie sesión como propietario del daemon de software de servidor.

Establecimiento de permisos con control de acceso basado en roles

También debe poder utilizar el control de acceso basado en roles (RBAC) para establecer los permisos necesarios. Consulte la documentación de RBAC del proveedor para obtener información. Tendrá que hacer lo siguiente:

1. Cree una autorización para el ejecutable *suauth*.
2. Cree un rol para esta autorización.
3. Asigne el propietario del daemon de software de servidor al rol.
4. Configure la autorización para permitir los permisos siguientes:
 - Lea el archivo *passwd*.
 - Cambie el ID de usuario.
 - Cambiar ID de grupo.

Configuración del inicio de sesión único (SSO)

Puede utilizar el inicio de sesión único para conectarse a un servidor que se ejecuta en cualquier plataforma soportada. Primero debe configurar el servidor de IBM SPSS Statistics, el cliente de IBM SPSS Statistics y las máquinas IBM SPSS Servicios de Colaboración e Implantación. La autenticación interna permite que el software del servidor se ejecute sin privilegios *root*.

Si utiliza el inicio de sesión único para conectarse tanto a IBM SPSS Statistics Server como a IBM SPSS Servicios de Colaboración e Implantación, debe conectarse a IBM SPSS Servicios de Colaboración e Implantación antes de conectarse a IBM SPSS Statistics Server.

Para interactuar con instalaciones de Active Directory más modernas y seguras, debe instalar el paquete de cifrado de alta seguridad para Java porque los algoritmos de cifrado necesarios no están soportados de forma predeterminada. Debe instalar el paquete tanto para el cliente, como para el servidor. Se muestra un mensaje de error como `Illegal key size` en el cliente cuando falla una conexión de servidor porque el paquete no está instalado. Consulte [“Instalación del cifrado de potencia ilimitada” en la página 40](#).

Nota: Antes de configurar el servidor de SPSS Statistics, el cliente de SPSS Statistics y las máquinas IBM SPSS Servicios de Colaboración e Implantación para el inicio de sesión único, debe asegurarse de que las máquinas tienen acceso al servidor del controlador de dominio.

Para obtener información sobre cómo configurar IBM SPSS Servicios de Colaboración e Implantación para el inicio de sesión único, consulte [Visión general de servicios de inicio de sesión único de IBM SPSS Servicios de Colaboración e Implantación](#).

Configuración del servidor para el inicio de sesión único

Configurar el servidor en Windows

1. Asegúrese de que la máquina del servidor Windows es miembro del dominio de Active Directory (AD).
2. En la ubicación de instalación de IBM SPSS Statistics Server, localice la carpeta denominada `config`.
3. En la carpeta `config`, cree una subcarpeta denominada `sso`.
4. En la carpeta `sso`, cree un archivo `krb5.conf`. Las instrucciones sobre cómo crear el archivo `krb5.conf` se pueden encontrar en http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/krb5_conf.html. A continuación se proporciona un ejemplo de un archivo `krb5.conf`:

```
[libdefaults]
    default_realm = STATISTICSSSO.COM
    dns_lookup_kdc = true
    dns_lookup_realm = true

[realms]
    STATISTICSSSO.COM = {
        kdc = statisticssso.com:88
        admin_server = statisticssso.com:749
        default_domain = STATISTICSSSO.COM
    }

[domain_realm]
    .statisticssso.com = STATISTICSSSO.COM
```

Configurar el servidor en UNIX

Para configurar el inicio de sesión único para máquinas de servidor UNIX, puede añadir la máquina UNIX al dominio de Windows AD y, a continuación, seguir las instrucciones para configurar el inicio de sesión único en Windows. De forma alternativa, puede realizar los pasos siguientes:

1. Cree una cuenta de usuario de dominio para la máquina UNIX.
2. Cambie el nombre de host. Si utiliza RedHat Linux, abra el archivo `/etc/sysconfig/network` y modifique `HOSTNAME` con el formato `<name>.<realm>`. Esto permite a AD encontrar las credenciales del servidor.
3. Para habilitar el servidor DNS para encontrar la máquina UNIX, realice uno de los pasos siguientes:
 - Abra el archivo `%windows%/system32/drivers/etc/hosts` y añada la correlación IP/host, por ejemplo:

```
192.168.1.102 test.statisticssso.com test
```

O

- Añada una nueva entrada de zona de búsqueda inversa. Esto añadirá una correlación de IP/host en el servidor DNS.

Si la entrada DNS para la máquina UNIX no es correcta, puede añadir manualmente la entrada de búsqueda inversa en el servidor DNS.

Configuración del cliente para el inicio de sesión único

Los pasos son comunes a todos los clientes excepto los pasos que se indican específicamente para Windows.

1. Asegúrese de que la máquina Windows local que ejecuta IBM SPSS Statistics es miembro del dominio de Active Directory (AD).

2. Añada el usuario de dominio como administrador en la máquina local.
3. Habilite Windows para acceder a la clave de sesión TGT:
 - a. En el menú **Inicio**, pulse **Ejecutar**.
 - b. Entre `regedit` y pulse **Aceptar** para abrir el **Editor de registro**.
 - c. Vaya a la siguiente ubicación de registro:


```
My
Computer\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\
Parameters
```
 - d. Pulse con el botón derecho del ratón en la carpeta y seleccione **Nuevo > DWORD**. El nombre del nuevo valor debe ser `allowtgtsessionkey`.
 - e. Defina el valor de `allowtgtsessionkey` en un valor hexadecimal de 1, es decir, `0x0000001`.
 - f. Cierre el **Editor del registro**.
 - g. Ejecute `kinit.exe`, que se puede encontrar en `<IBM SPSS Statistics installation location>\jre\bin`.
4. En la carpeta `config` de la ubicación de instalación de IBM SPSS Statistics, cree una carpeta denominada `sso`.
5. Copie el archivo `krb5.conf` del servidor en la carpeta `sso`.
6. Reinicie la máquina cliente y la máquina servidor.

Registro del nombre de principio de servicio (SPN)

Cada instancia de servidor debe registrar un *nombre principal de servicio (SPN)* exclusivo para acreditar su propia identidad, y el cliente debe especificar el mismo SPN cuando se conecta al servidor.

Un SPN para una instancia del software de servidor tiene el formato:

```
statisticsserver/<host>:<port>
```

Por ejemplo:

```
statisticsserver/jdoemachine.ibm.com:3023
```

Tenga en cuenta que el nombre de host debe estar calificado con su dominio DNS (`ibm.com` en este ejemplo) y el dominio debe correlacionarse con el dominio Kerberos.

La combinación formada por el nombre de host y el número de puerto hace que el SPN sea exclusivo (pues cada instancia situada en un host determinado debe estar a la escucha en un puerto diferente). Y tanto el cliente y como el servidor ya tienen el nombre de host y el número de puerto y por tanto pueden construir el SPN adecuado para la instancia. El paso de configuración adicional necesario es registrar el SPN en la base de datos de Kerberos.

Registrar el SPN en Windows

Si está utilizando Active Directory como implementación de Kerberos, utilice el comando `setspn` para registrar el SPN. Para ejecutar este comando, se deben cumplir las condiciones siguientes:

- Debe haber iniciado una sesión en un controlador de dominio
- Debe ejecutar el comando con privilegios elevados (ejecutar como administrador)
- Debe ser miembro del grupo Administradores de dominios (o tener el permiso apropiado otorgado por un administrador de dominios)

Para obtener más información, consulte los artículos siguientes:

- [Consulta de línea de mandatos Setspn](#)
- [Delegación de autorizaciones para modificar los SPN](#)

Para la instancia predeterminada, escuchando en el puerto estándar (3023 para la versión 23, por ejemplo) y ejecutándose bajo la cuenta del sistema local, debe registrar el SPN en el nombre del sistema del servidor. Por ejemplo:

```
setspn -s statisticsserver/jdoemachine.spss.com:3023 jdoemachine
```

Para cada instancia de servidor posterior, escuchando en un puerto personalizado (por ejemplo, 3099) y ejecutándose bajo una cuenta de usuario arbitraria (por ejemplo, johndoe) con la opción `userauth` establecida en `internal` (es decir, utilizando la autenticación interna), debe registrar el SPN en el nombre de cuenta de usuario de servicio:

```
setspn -s statisticsserver/jdoemachine.spss.com:3099 jdoe
```

Observe que en este caso (cuando la cuenta de servicio no es el sistema local), no es suficiente registrar el SPN para permitir que un cliente se conecte. La sección siguiente describe pasos de configuración adicionales.

Para ver los SPN que están registrados en la cuenta `jdoe`:

```
setspn -l jdoe
```

Registrar el SPN en UNIX

Si utiliza Active Directory como implementación de Kerberos , utilice el mandato `setspn` tal como se describe en la sección anterior de Windows. Esto presupone que ya ha creado el sistema o la cuenta de usuario en el directorio. O puede experimentar con `ktpass`, si lo desea (consulte [Referencia de línea de mandatos de Ktpass](#)).

Si está utilizando alguna otra implementación de Kerberos , utilice la herramienta de administración de Kerberos favorita para añadir el principal de servicio a la base de datos Kerberos . Para convertir el SPN en un identificador individual de Kerberos, debe añadir el nombre del dominio Kerberos. Por ejemplo:

```
statisticsserver/jdoemachine.ibm.com:3023@ibm.com
```

Añadir este mismo principal y contraseña al archivo `keytab` del servidor. El archivo `keytab` debe contener una entrada para cada instancia que se ejecuta en el host.

Configuración de SSO cuando se ejecuta como no root/sistema

Cuando el servicio/daemon de servidor se ejecuta como un usuario arbitrario (no root en UNIX y no System en Windows), necesita registrar la cuenta de servicio/daemon. Necesita el SPN que ha creado anteriormente.

1. Cree el directorio `<STATISTICSSERVER>\config\sso`.
2. Copie el archivo `krb5.conf` del directorio SSO del cliente en el directorio SSO del servidor que ha creado en el paso 1.
3. Utilice el comando siguiente para crear el archivo `krb5.keytab` en el directorio del servidor SSO:

```
<STATISTICSSERVER>\jre\bin\ktab -a <spn>@<realm> -k krb5.keytab
```

Por ejemplo:

```
"..\jre\bin\ktab.exe" -a statisticsserver/  
jdoemachine.ibm.com:3023@ibm.com  
-k krb5.keytab
```

Se le solicitará una contraseña. La contraseña que especifique deberá ser la contraseña de la cuenta de servicio. Por lo tanto, si la cuenta de servicio es `jdoe`, por ejemplo, debe especificar la contraseña para el usuario `jdoe`.

La propia cuenta de servicio no se menciona en el archivo keytab, sino antes de que haya registrado el SPN en la cuenta utilizando `setspn`. Esto significa que la contraseña del principal de servicio y la contraseña de la cuenta de servicio son la misma y única contraseña.

Para cada nueva instancia de servidor que cree, debe registrar el SPN para dicha instancia (utilizando `setspn`) y crear un archivo de tabla de claves. El archivo de tabla de claves debe copiarse en el subdirectorio `config_<group_name>/sso` del directorio de instalación del servidor. La instancia predeterminada no necesita un archivo de tabla de claves.

Para verificar que una instancia esté incluida en el archivo keytab:

```
ktab.exe -l -e -k krb5.keytab
```

Es posible que vea varias entradas para cada principal con diferentes tipos de cifrado, pero esto es normal.

Configuración de la pertenencia a grupos

Si está utilizando la autorización de grupo, puede configurar IBM SPSS Servicios de Colaboración e Implantación para consultar un proveedor LDAP para determinar el grupo al que pertenece un usuario autenticado. Para obtener más información sobre la autorización de grupo, consulte el tema [“Autorización de grupo”](#) en la página 31.

A continuación, para que la búsqueda de grupos funcione correctamente, primero debe configurar el repositorio para añadir un proveedor LDAP o Active Directory y, a continuación, habilitar SSO utilizando dicho proveedor:

1. Inicie el cliente IBM SPSS Deployment Manager y seleccione **Archivo > Nuevo > Conexión de servidor administrado...** para crear una conexión de servidor administrado para el repositorio (si aún no tiene una).
2. Inicie una sesión en la conexión de servidor administrado y expanda la carpeta **Configuración**.
3. Pulse con el botón derecho del ratón **Proveedores de seguridad**, seleccione **Nuevo > Definición del proveedor de seguridad...**, y especifique los valores adecuados. Pulse **Ayuda** en el diálogo para obtener más información.
4. Expanda la carpeta **Proveedores de inicio de sesión único**, pulse con el botón derecho en **Proveedor de inicio de sesión único Kerberos** y seleccione **Abrir**.
5. Pulse **Habilitar**, seleccione el proveedor de seguridad y luego pulse **Guardar**. No es necesario que proporcione más datos aquí a menos que desee utilizar el inicio de sesión único (simplemente habilitar el proveedor es suficiente para permitir la búsqueda de grupos).

Importante: para que la búsqueda de grupos funcione correctamente, el proveedor Kerberos que configure aquí debe ser el mismo que el proveedor que configuró para IBM SPSS Statistics Server. En particular, deben trabajar en el mismo dominio Kerberos. Por lo tanto, si un usuario inicia la sesión en el servidor utilizando SSO y lo identifica como `jdoe@ibm.com` (donde `ibm.com` es el reino), esperará que el proveedor de seguridad de IBM SPSS Servicios de Colaboración e Implantación reconozca ese nombre de principal de usuario y devuelva la pertenencia al grupo correspondiente desde el directorio LDAP.

Configuración de SSO para orígenes de datos

Puede conectarse a bases de datos desde IBM SPSS Statistics utilizando un inicio de sesión único. Si desea crear una conexión de base de datos utilizando el inicio de sesión único, primero debe utilizar el software de gestión de ODBC para configurar correctamente un origen de datos y un elemento de inicio de sesión único. A continuación, cuando se conecta a una base de datos en IBM SPSS Statistics, IBM SPSS Statistics utilizará ese mismo elemento de inicio de sesión único y al usuario no se le solicitará que inicie la sesión en el origen de datos.

Sin embargo, si el origen de datos no se ha configurado correctamente para el inicio de sesión único, IBM SPSS Statistics solicitará al usuario que inicie la sesión en el origen de datos. El usuario todavía podrá acceder al origen de datos después de proporcionar credenciales válidas.

Para obtener información completa sobre la configuración de orígenes de datos ODBC en el sistema con el inicio de sesión único habilitado, consulte la documentación del proveedor de base de datos. A continuación se muestra un ejemplo de los pasos generales que se requieren:

1. Configure la base de datos para que dé soporte al inicio de sesión único de Kerberos.
2. En la máquina servidor, cree un origen de datos ODBC y pruébelo. La conexión DSN no debería requerir un ID de usuario ni una contraseña.
3. Conéctese al servidor utilizando el inicio de sesión único y empiece a utilizar el origen de datos ODBC creado y validado en el paso 2.

Permisos

Si no está utilizando la autenticación interna o la autorización de grupo con inicio de sesión único, el software de servidor inicia un proceso para el usuario final, pasando el ID de usuario y la contraseña al sistema operativo. El proceso iniciado tiene los derechos de acceso al archivo de la cuenta del usuario final. Un usuario que se conecta al software de servidor debe iniciar sesión con una cuenta que tenga los permisos siguientes:

- Permisos de lectura y ejecución en el directorio de instalación del servidor y sus subdirectorios
- Permisos de lectura, ejecución y escritura en la ubicación del directorio para archivos temporales

Para la autenticación interna y el inicio de sesión único, el usuario cliente que se conecta tiene los permisos asignados al usuario que ha iniciado el servicio/daemon.

Puede utilizar la aplicación de administración (IBM SPSS Statistics Administration Console, que se instala como parte de IBM SPSS Deployment Manager) para cambiar la ubicación predeterminada de los archivos temporales. Consulte el tema Ubicaciones de archivos en la publicación *Deployment Manager User's Guide* (que se incluye en la ayuda de IBM SPSS Servicios de Colaboración e Implantación) para obtener más información. También puede cambiar la ubicación para usuarios o grupos individuales. Consulte el tema IBM SPSS Statistics Server User Profiles and Groups, en la publicación *Deployment Manager User's Guide*, para obtener más información.

Permisos de nivel de administrador

De forma predeterminada, el grupo de administradores para el software de servidor es el grupo de administradores para la máquina en la que se ejecuta el software de servidor. Puede cambiar el grupo de administradores para el software de servidor especificándolo en el cuadro de texto Grupo de administradores de la aplicación de administración (IBM SPSS Statistics Administration Console, que se instala como parte de IBM SPSS Deployment Manager). Consulte el tema Usuarios en la publicación *Deployment Manager User's Guide* (que se incluye en la ayuda de IBM SPSS Servicios de Colaboración e Implantación) para obtener más información. Si utiliza la autenticación interna en UNIX, puede crear administradores directamente. Consulte el tema [“Configuración de la autenticación interna”](#) en la página 24 para obtener más información.

Autorización de grupo

Puede configurar el software de servidor para que admita la autorización de grupo. Se ejecuta una instancia independiente del servicio/daemon para cada grupo autorizado de usuarios.

Configuración de autorización de grupo

1. Cree una instancia de servidor para cada grupo. Para obtener más información sobre la creación de instancias de servidor, consulte [“Configuración de varias instancias”](#) en la página 19.
2. Cree los grupos en IBM SPSS Servicios de Colaboración e Implantación y asigne usuarios a los grupos.
3. Abra la aplicación de administración y actualice el valor de **URL de servicio de autorización de grupo** a la URL de IBM SPSS Servicios de Colaboración e Implantación. Asegúrese de incluir el número de puerto (por ejemplo, `http://myserver.mydomain.com:9080`).

Control del acceso de DSN por grupo

La autenticación de varios factores (MFA) requiere que se puedan restringir los usuarios en el conjunto de nombres de orígenes de datos (DSN) de ODBC para el que tienen permiso de acceso, en función de su pertenencia a grupos.

1. Abra la aplicación de administración y establezca **Restringir acceso a base de datos** en Yes.
2. En el campo **Orígenes de base de datos permitidos**, especifique una lista de DSN separados por punto y coma (;) que están permitidos para el acceso (por ejemplo, Fraud - Analytic; Fraud - Operational).

Cuando está habilitada esta restricción, los resultados son los siguientes:

- Cuando un usuario busca orígenes de datos en el asistente de base de datos, en lugar de aparecer todos los DSN definidos en el sistema del servidor, solo verá el subconjunto de DSN definido por la aplicación de administración. Observe que la vía de acceso pueden contener algunos DSN que no están definidos en el servidor. Estos DSN no se tienen en cuenta y no se muestran al usuario.
- Si un usuario modifica la sintaxis de GET DATA /TYPE=ODBC que especifica un DSN que no ha especificado la aplicación de administración, la sintaxis no se ejecutará y al usuario se le presentará un error similar a **Acceso denegado al origen de datos: < X>**.

Perfiles

El software de servidor proporciona la capacidad de crear perfiles de usuarios individuales y grupos de usuarios. Estos perfiles de usuario y grupos le permiten definir valores para usuarios específicos.

Versiones de cliente y servidor

A partir de la versión 20.0.1, el software de cliente no tiene que estar en el mismo nivel de release que el software de servidor al que se está conectando. Por ejemplo, el cliente 20.0.1 puede conectarse al software de servidor 21 y el cliente 21 puede conectarse a un servidor 20.0.1. Tenga en cuenta que también puede ejecutar varias versiones del software de servidor en un sistema servidor.

La combinación de niveles de release sólo está permitida para simplificar las actualizaciones. Los niveles de release se pueden escalonar durante el periodo de actualización, y no es necesario actualizar los clientes simultáneamente. Sin embargo, no se recomienda mantener esta configuración durante más tiempo. Si el servidor es más moderno que el cliente, el servidor puede generar resultados que no pueda leer el cliente. Si el cliente es más moderno que el servidor, es posible que el servidor no reconozca la sintaxis enviada por el cliente. Por lo tanto, debe actualizar el software de cliente o servidor tan pronto como sea posible, en función de qué uno esté rezagado respecto al otro.

Cuando distribuya información de conexión a los usuarios finales, tenga en cuenta qué versión del software de cliente están ejecutando y asegúrese de que tienen la información de conexión para una versión de servidor coincidente.

Conexión de usuarios a través de un cortafuegos

Si utiliza un **cortafuegos** para mantener la seguridad de la red frente a intrusos, puede configurar el cortafuegos y el software de servidor para que los usuarios finales fuera del cortafuegos puedan conectar el cliente al software de servidor. El cortafuegos puede utilizar **NAT** (Network Address Translation), pero no es necesario.

El escenario típico para conectar usuarios finales a través de un cortafuegos que utiliza NAT es el siguiente:

1. El usuario final conecta la aplicación cliente al software de servidor utilizando la **IP enmascarada** (la dirección IP que NAT presenta al mundo exterior) y el número de puerto del servidor. Por ejemplo, el usuario final se conecta con la IP 10.10.10.2 y el número de puerto 3016.
2. El cortafuegos permite la conexión porque se ha configurado para aceptar conexiones de la IP enmascarada.

3. El cortafuegos redirige la IP enmascarada a la IP interna real del servidor. Permite la conexión porque el puerto (por ejemplo, 3016) está habilitado en el cortafuegos.
4. El servidor genera un proceso para la conexión de cliente del usuario final y le asigna un número de puerto de la lista en la variable de entorno del sistema STATISTICS_CLIENT_PORTS. Por ejemplo, el proceso se comunica a través del puerto 3287.
5. El cortafuegos permite la comunicación a través de ese puerto (por ejemplo, 3287) porque está habilitado en el cortafuegos.

Configuración de conexiones a través de un cortafuegos

Introducción

IBM SPSS Statistics Server vuelve a utilizar el mismo número de puerto para las conexiones de cliente. Esto significa que sólo es necesario abrir dos puertos a través del cortafuegos: el daemon SPSS Statistics o el puerto de escucha (el valor predeterminado es 3028, aunque se puede modificar si es necesario) y el puerto de respuesta a través del cual los clientes de SPSS Statistics hablan con sus procesos hijo de SPSS Statistics Server.

Nota: La reutilización de puerto está vinculada a la prestación de reconexión de cliente. De forma predeterminada, la reconexión de cliente está habilitada durante 100 segundos. Cuando la reconexión de cliente está habilitada, SPSS Statistics Server tiene una proporción de 1: 1 entre clientes conectados y puertos de respuesta abiertos. Para habilitar la reutilización de puertos, primero debe inhabilitar la reconexión de cliente. Esto se realiza editando el valor **reconnect-timeout** en <Statistics Install Path>/config/statisticsd.conf. Por ejemplo:

```
<reconnect-timeout desc="The timeout in minutes that the server uses to drop disconnected clients (default: 100)." value="0"/>
```

En un entorno con muchas conexiones de cliente-servidor posibles, es posible que desee configurar más de un puerto de respuesta de cliente. Cuando un cliente de SPSS Statistics está en proceso de conexión con el servidor de SPSS Statistics, el puerto de cliente está básicamente bloqueado y sólo lo puede utilizar un cliente hasta que haya finalizado el proceso de conexión. El tiempo para conectarse está en el rango de 1 a 3 segundos (este tiempo puede variar en función de la carga del sistema). Cuando un segundo o tercer cliente de SPSS Statistics intenta conectarse durante este tiempo, los clientes se bloquean hasta que el puerto de cliente pasa a estar disponible. La apertura de varios puertos de cliente reduce el tiempo de espera al conectarse en un entorno en el que muchos usuarios inician simultáneamente sesiones de SPSS Statistics.

Ejemplo

Supongamos que se listan cinco puertos de cliente en la variable de entorno del sistema **STATISTICS_CLIENT_PORTS** (puertos 40001-40005) y que hay cuatro posibles clientes. Un usuario inicia una conexión con el servidor de SPSS Statistics y el primer contacto se realiza a través del puerto de escucha (3028). El servidor genera un proceso hijo y continúa la comunicación a través del primer puerto de cliente disponible (4001). Si el puerto 40001 no está bloqueado (porque la comunicación con otro cliente se acaba de iniciar), el puerto se volverá a utilizar. Si el puerto 40001 está bloqueado, la comunicación pasa al siguiente puerto (4002), suponiendo que no esté bloqueado, y así sucesivamente.

Después de que los cuatro clientes estén conectados, lo más probable es que todos utilicen el mismo número de puerto (40001). Existe una pequeña posibilidad de que uno o más clientes utilicen el puerto 40002, una menor posibilidad de que un cliente utilice el puerto 40003, y una probabilidad aún menor de que uno o más clientes utilicen el puerto 40004. No hay ninguna posibilidad de que un cliente utilice el puerto 40005 porque sólo hay cuatro clientes y el algoritmo se inicia en el primer número de puerto disponible que se lista en la variable de entorno del sistema STATISTICS_CLIENT_PORTS.

Existen dos métodos recomendados para configurar conexiones de SPSS Statistics Server a través de un cortafuegos.

Configurar el cortafuegos para permitir procesos

Utilizando el software de cortafuegos, asegúrese de que los siguientes procesos pueden aceptar conexiones de red.

statisticsproc.exe

El proceso `statisticsproc.exe` abre, cierra y vuelve a utilizar los puertos de respuesta (o los puertos definidos en `STATISTICS_CLIENT_PORTS`).

statisticsrsvr.exe (Microsoft Windows) o statisticsd (UNIX o Linux)

El proceso es el principal servicio de Windows, o daemon UNIX/Linux, y gestiona el puerto de escucha.

Proporcionar acceso a los procesos permite de forma efectiva cualquier puerto que el proceso vaya a utilizar.

Nota: Se aplican las condiciones siguientes cuando el valor de tiempo de espera de reconexión es mayor que 0 y se permite que `statisticsproc.exe` acepte conexiones de red:

- `STATISTICS_CLIENT_PORTS` es irrelevante, excepto para los diagnósticos. Se puede utilizar cualquier puerto.
- No hay ningún límite en el número de conexiones a menos que los puertos estén definidos en **STATISTICS_CLIENT_PORTS**. El número de puertos **STATISTICS_CLIENT_PORTS** definidos limita de forma efectiva los puertos que utilizará el servidor de SPSS Statistics.

Configurar el cortafuegos abriendo manualmente los puertos

Para configurar manualmente el software del servidor y el cortafuegos, siga estos pasos:

1. Instale el software de servidor como de costumbre. Debe conocer la dirección IP del sistema en el que está instalado el servidor y el número de puerto que el software del servidor utiliza para las comunicaciones. Por ejemplo, instale el servidor en 202.123.456.78 en el puerto de escucha 3028.
2. Configure la variable de entorno del sistema `STATISTICS_CLIENT_PORTS` especificando al menos un número de puerto. La variable de entorno lista los puertos que se utilizan para continuar las conexiones de cliente con el servidor (puertos **RESPONSE**). Si es necesario, puede especificar una lista delimitada por comas y un rango de puertos (por ejemplo, 4001, 4002, 4003-4005).

Importante:

- Cuando se establece el tiempo de espera de reconexión automática en un valor mayor que 0, `STATISTICS_CLIENT_PORTS` define el número máximo de conexiones de cliente y servidor simultáneas permitidas.
- No liste el puerto **LISTEN** (3028) en la variable de entorno `STATISTICS_CLIENT_PORTS`.

Microsoft® Windows™

Utilice las propiedades del sistema Windows para crear y configurar la variable de entorno. Consulte [“Propiedades del sistema”](#) en la [página 55](#) para obtener instrucciones.

UNIX

Edite el script de entorno del software de servidor, `statsenv.sh`, que se incluye en el subdirectorio `/bin` del directorio de instalación. Defina el puerto que pueden utilizar los procesos de cliente que inicia el servidor. Por ejemplo, añada las líneas siguientes:

```
STATISTICS_CLIENT_PORTS=4001  
  
export STATISTICS_CLIENT_PORTS
```

3. Cuando utilice NAT (Network Address Translation), cree y correlacione IP. Utilizando el software de cortafuegos, cree una IP enmascarada para uso externo y correlaciónelo con la IP interna del servidor. Por ejemplo, cree una IP de enmascaramiento 10.10.10.2 y correlaciónela con 202.123.456.78.
4. Utilizando el software de cortafuegos, habilite los números de puerto en el cortafuegos:
 - El número de puerto **LISTEN** del servidor. Por ejemplo, habilite el puerto 3028.

- Los números de puerto que ha especificado en la variable de entorno `STATISTICS_CLIENT_PORTS`. Por ejemplo, habilite el puerto 4001.
5. Distribuya la información de conexión a los usuarios que se conectan al software del servidor desde fuera del cortafuegos.
- Si se utiliza, la IP enmascarada del sistema en el que está instalado el software del servidor (no distribuya la IP interna del servidor). Por ejemplo, distribuya `10.10.10.2` como IP del servidor.
 - Distribuya el número de puerto del software del servidor como de costumbre. Por ejemplo, distribuya 3028 como el número de puerto **LISTEN** del servidor.

Conexión de usuarios con PPTP

Los usuarios finales pueden conectar un sistema cliente remoto al software de servidor analítico con **Protocolo de túnel punto a punto (PPTP)**. PPTP es un protocolo de red que da soporte a redes privadas virtuales (VPN) multiprotocolo. Permite a los usuarios finales remotos acceder a su red de forma segura a través de Internet.

Para utilizar conexiones PPTP:

1. **Configure un servidor de acceso remoto para PPTP.** Asegúrese de crear suficientes direcciones IP para los clientes porque el software de servidor da soporte a varias conexiones de cliente. Cada conexión de cliente requiere su propia dirección IP.
2. **Configure el sistema de escritorio del cliente.** Utilice el panel de control Red de Windows para añadir una conexión de red privada utilizando PPTP. Especifique una dirección IP que el servidor de acceso remoto reconocerá como una conexión PPTP.
3. **Habilitar la conexión PPTP en el sistema de escritorio del cliente.** Cuando los usuarios finales desean conectarse al software de servidor desde una ubicación remota, habilitan la conexión PPTP y, a continuación, utilizan el software de cliente para conectarse al servidor como de costumbre.

Uso de SSL para transferencias de datos seguras

SSL (Secure Sockets Layer) es un protocolo para cifrar datos transferidos entre dos ordenadores. SSL garantiza que la comunicación entre los ordenadores es segura. SSL puede cifrar la autenticación de un nombre de usuario/contraseña y el contenido de un intercambio entre un servidor y un cliente.

Nota: Versión 30.0.0 en adelante, SSL está en desuso y los usuarios deben utilizar GSKit.

Cómo funciona SSL

SSL se basa en las claves públicas y privadas del servidor, junto con un certificado de clave pública que enlaza la identidad del servidor con su clave pública.

1. Cuando un cliente se conecta a un servidor, el cliente autentica el servidor con el certificado de clave pública.
2. El cliente genera a continuación un número aleatorio, cifra el número con la clave pública del servidor, y envía el mensaje cifrado de vuelta al servidor.
3. El servidor descifra el número aleatorio con su clave privada.
4. A partir del número aleatorio, tanto el servidor como el cliente crean las claves de sesión utilizadas para cifrar y descifrar la información posterior.

El certificado de clave pública está firmado normalmente por una entidad emisora de certificados. Las entidades emisoras de certificados, como VeriSign y Thawte, son organizaciones que emiten, autentican y gestionan las credenciales de seguridad contenidas en los certificados de clave pública. Esencialmente, la entidad emisora de certificados confirma la identidad del servidor. La entidad emisora de certificados normalmente cobra una tarifa por un certificado, pero también pueden generarse certificados autofirmados.

Cómo habilitar SSL con GSKit

Cómo asegurar las comunicaciones cliente-servidor y servidor-servidor con GSKit

Los pasos principales en las comunicaciones cliente-servidor y servidor-servidor seguras con SSL son:

1. Obtener e instalar el certificado SSL y las claves.
2. Habilitar y configurar un archivo de configuración especificado ubicado en el directorio de instalación del servidor IBM SPSS Statistics.

Nota: El servidor IBM SPSS Statistics admite el protocolo TLSv1.2. GSKit no admite actualmente ninguna otra versión.

3. Si se utilizan certificados de cifrado con una potencia mayor que 2048 bits, instale el cifrado de potencia ilimitada en los sistemas del cliente.
4. Indicar a los usuarios que habiliten SSL cuando se conecten con el servidor.

Nota: En algunas ocasiones un servidor actúa como cliente. Un ejemplo es IBM SPSS Statistics Server conectándose al IBM SPSS Repositorio de Servicios de Colaboración y Despliegue. En este caso, IBM SPSS Statistics Server es el *cliente*.

Obtención e instalación de certificados y claves SSL

Los primeros pasos que debe seguir para configurar el soporte de SSL son:

1. Obtenga un archivo de certificado y de clave SSL. Hay varias maneras de hacerlo:
 - Adquirirlos a través de una entidad emisora de certificados pública (como Verisign, Thawte o Entrust). La entidad emisora de certificados pública (CA) firma el certificado para verificar el servidor que lo utiliza.
 - Obtenga los archivos de claves y certificados de una entidad emisora de certificados de terceros. Si se utiliza este método, el certificado raíz *.pfx de la entidad emisora de certificados de terceros debe importarse en el archivo de almacén de claves del servidor (se explica a continuación).
 - Genera los archivos de clave y de certificado mediante una entidad emisora de certificados autofirmados interna. Los pasos para hacerlo son los siguientes:
 - a. Prepare una base de datos de claves. Consulte el tema [“Crear una base de datos de claves SSL”](#) en la [página 38](#) para obtener más información.
 - b. Cree un certificado autofirmado. Consulte el tema [“Creación de un certificado SSL autofirmado”](#) en la [página 38](#) para obtener más información.
2. Para la entidad emisora de certificados (CA) o los certificados autofirmados, copie los archivos .kdb y .sth del paso 1 en un directorio al que el IBM SPSS Statistics Server tenga acceso y especifique la vía de acceso a dicho directorio en el archivo statisticsd.conf. El archivo statisticsd.conf se encuentra en <Statistics Server installation directory>/config/; para certificados de terceros, copie los archivos .pfx y .sth del paso 1.
3. Establezca los parámetros siguientes en el archivo statisticsd.conf:

Para una entidad emisora de certificados (CA) o un certificado autofirmado:

 - <gsk desc="0=GSKSSL Disabled; 1=GSKSSL Enabled" value="<value>"/>, donde <value> es 0 o 1 que indica si se debe habilitar GSKit.
 - <gsk-keystore desc="GSKSSL Key store database filename." value="<filename>.kdb"/>, donde <filename> es el nombre del archivo de base de datos de claves.
 - <gsk-keystore-stash desc="GSKSSL Key store stash filename." value="<filename>.sth"/>, donde <filename> es el nombre del archivo de ocultación de contraseñas de la base de datos de claves.
 - <gsk-cert-label desc="GSKSSL certificate label." value=""/>, donde <label> es la etiqueta del certificado.

Para certificados de terceros:

- `<gsk desc="0=GSKSSL Disabled; 1=GSKSSL Enabled" value="<value>"/>`, donde `<value>` es 0 o 1 que indica si se debe habilitar GSKit.
- `<gsk-keystore = "<*.pfx_file_location>"`, donde `<*.pfx_file_location>` es la ubicación y el nombre del archivo de certificado raíz `*.pfx`.
- `<gsk-keystore-stash desc="GSKSSL Key store stash filename." value="<filename>.sth"/>`, donde `<filename>` es el nombre del archivo de ocultación de contraseñas de la base de datos de claves.
- `<gsk-cert-label desc="GSKSSL certificate label." value=""/>`, donde `<label>` es la etiqueta del certificado.

4. Para certificados de terceros:

- a. Extraiga el archivo `root.pem` del archivo `*.pfx`, utilizando el siguiente mandato GSK como ejemplo:

```
gsk8capiCmd_64.exe -cert -extract -db C:\SSL\<certificate_name>.pfx -stashed -label  
<cert-certificate_issuing_server.com> -target C:\SSL\root.pem
```

- b. Copie `root.pem` en la carpeta `C:\ProgramData\IBM\SPSS\certificates (Windows)` o `Library/Application Support/IBM/SPSS/certificates (macOS)` en el cliente.
- c. En el cliente, establezca la conexión utilizando el nombre de dominio completo (por ejemplo, `cert-certificate_issuing_server.com`) " en el campo **Nombre de servidor** y habilite la opción **SSL**.

5. Para certificados autofirmados, instale el certificado en sistemas cliente. Para los certificados públicos de CA o de terceros adquiridos, este paso no es necesario. Asegúrese de que los permisos de acceso no permitan un examen casual del directorio que contiene el certificado. Consulte el tema [“Instalación de un certificado SSL autofirmado”](#) en la página 38 para obtener más información.

Configurar el entorno para ejecutar GSKit

GSKCapiCmd es una herramienta de línea de mandatos no basada en Java y no es necesario instalar Java™ en el sistema para utilizar esta herramienta; se encuentra en la carpeta `<Statistics Server installation directory>/bin`. El proceso de configurar el entorno para ejecutar IBM Global Security Kit (GSKit) varía dependiendo de la plataforma que se utilice.

Para configurar para Linux/Unix, añada el directorio de bibliotecas compartidas `<Statistics Server installation directory>/lib` al entorno:

```
$export <Shared library path environment variable>=<Statistics_server_install_path>/lib:<Shared  
library  
path environment variable>  
$export PATH=$PATH:<Statistics_server_install_path>/bin
```

El nombre de la variable para la vía de acceso de bibliotecas compartidas depende de la plataforma que utilice:

- Linux utiliza el nombre de variable: `LD_LIBRARY_PATH`

Por ejemplo, para definir el entorno en Linux, utilice:

```
$export LD_LIBRARY_PATH=/opt/IBM/SPSS/StatisticsServer/25/lib:$LD_LIBRARY_PATH  
$export PATH=$PATH:/opt/IBM/SPSS/StatisticsServer/25/bin
```

Acceso de cuenta a archivos

Asegúrese de que otorga los permisos correctos para las cuentas que accederán a los archivos SSL:

1. Para todas las cuentas utilizadas por IBM SPSS Statistics para la conexión, otorgue acceso de lectura a los archivos SSL.

Nota: Esto también se aplica al usuario de *Iniciar sesión como* que se ha definido en el servicio IBM SPSS Statistics Server. En UNIX o Linux, se aplica al usuario con el que inicia el servidor.

2. Para Windows, no basta con que las cuentas estén en el grupo Administradores y que el permiso se proporcione al grupo Administradores cuando el control de acceso de usuario (UAC) está habilitado. Además, debe realizar una de las acciones siguientes:

- Proporcionar el permiso de cuentas por separado.
- Crear un grupo nuevo, añadir las cuentas en el grupo nuevo y proporcionar al grupo el permiso para acceder a los archivos SSL.
- Inhabilitar UAC.

Crear una base de datos de claves SSL

Utilice la herramienta GSKCapiCmd para crear la base de datos de claves. Antes de utilizar la herramienta, debe configurar el entorno; consulte el tema [“Configurar el entorno para ejecutar GSKit”](#) en la página 37 si desea más información

Para crear la base de datos de claves, ejecute GSKit y escriba el comando siguiente:

```
gsk<ver>capicmd[_64] -keydb -create -populate -db <filename>.kdb -pw <password> -stash
```

donde <ver> es el número de versión de GSKit, <filename> es el nombre que desea utilizar para el archivo de base de datos de claves y <password> es la contraseña de la base de datos de claves.

La opción `-stash` crea un archivo de ocultación en la misma vía de acceso que la base de datos de claves, con una extensión de archivo de `.sth`. GSKit utiliza el archivo de ocultación para obtener la contraseña de la base de datos de claves y así no tener que entrarla cada vez en la línea de comandos.

Nota: Debe utilizar una protección de sistema de archivos sólida en el archivo `.sth`.

Creación de un certificado SSL autofirmado

Para generar un certificado autofirmado y almacenarlo en la base de datos de claves, utilice el siguiente comando:

```
gsk<ver>capicmd[_64] -cert -create -db <filename>.kdb -stashed -dn  
"CN=myserver,OU=mynetwork,O=mycompany,  
C=mycountry" -label <label> -expire <Number of days certificate is valid>
```

donde <ver> es el número de versión de GSKit, <filename> es el nombre del archivo de base de datos de claves, <Number of days certificate is valid> es el número físico de días que el certificado es válido y <label> es una etiqueta descriptiva para ayudarlo a identificar el archivo (por ejemplo, puede utilizar una etiqueta como: `myselfsigned`).

Instalación de un certificado SSL autofirmado

En las máquinas de cliente que se conectan al servidor utilizando SSL, debe distribuir la parte pública del certificado a los clientes, de modo que se pueda almacenar en sus bases de datos de claves. Para ello, realice los pasos siguientes:

Nota: Omita este paso si está utilizando un certificado firmado por una entidad emisora de certificados. Si está utilizando un certificado autofirmado, necesita copiar la entidad emisora de certificados de confianza en los sistemas del cliente. Tenga en cuenta que un equipo servidor también puede actuar como un cliente. Un ejemplo es IBM SPSS Statistics Server que se conecta al IBM SPSS Repositorio de Servicios de Colaboración y Despliegue. En este caso, IBM SPSS Statistics Server es el cliente y, por lo tanto, debe copiar el certificado para el servidor IBM SPSS Repositorio de Servicios de Colaboración y Despliegue en IBM SPSS Statistics Server.

1. Extraiga la parte pública de un archivo utilizando el comando siguiente:

```
gsk<ver>capicmd[_64] -cert -extract -db <filename>.kdb -stashed -label <label> -target  
root.pem
```

2. Distribuya `root . pem` a los clientes. Si tiene varias entidades emisoras de certificados de confianza, cópielas en un solo archivo `root . pem`. Las entidades emisoras de certificados de confianza son archivos de texto, así que puede copiar y pegar el certificado o certificados. Copie `root . pem` en la ubicación siguiente en los sistemas del cliente. Si ya ha copiado un archivo `root . pem` en el cliente para otro producto de IBM, añada la información de la entidad emisora de certificados raíz de confianza de su entidad emisora al archivo `root . pem` existente. De forma predeterminada, todos los productos de IBM buscan en esta ubicación para ver archivos de certificado autofirmado de confianza. Si desea utilizar otra ubicación, cree una variable de entorno `SSL_CERT_DIR` y establezca el valor de la variable en la ubicación.

- Windows 7 y superior: `C:\ProgramData\IBM\SPSS\certificates`
- Mac: `/Library/Application Support/IBM/SPSS/certificates`
- UNIX y Linux: `/opt/IBM/SPSS/certificates`

Configuración del certificado de cliente

Cuando se configura SPSS Statistics Server para utilizar una conexión SSL y está utilizando un certificado firmado automáticamente, debe copiar y configurar la entidad certificadora de confianza para todas las estaciones de trabajo de cliente.

Un ejemplo sería cuando IBM SPSS Servicios de Colaboración e Implantación envía un trabajo a SPSS Statistics Server (que está habilitado para SSL). En este caso, IBM SPSS Servicios de Colaboración e Implantación es el cliente. La entidad certificadora de confianza (`root . pem` en el SPSS Statistics Server) se debe copiar y configurar en todas las máquinas IBM SPSS Servicios de Colaboración e Implantación.

Configuración de archivos de certificado para IBM SPSS Servicios de Colaboración e Implantación

El soporte de IBM SPSS Servicios de Colaboración e Implantación se puede desplegar en un servidor de aplicaciones web (por ejemplo, IBM WebSphere y RedHat JBoss EAP).

El primer paso para configurar los archivos de certificado para el soporte de IBM SPSS Servicios de Colaboración e Implantación es recuperar el archivo SPSS Statistics Server `root . pem` del administrador.

El proceso de configuración del certificado SSL depende de qué servidor de aplicaciones web se emplee.

IBM WebSphere y RedHat JBoss EAP

Las instrucciones siguientes se aplican tanto para IBM WebSphere como para RedHat JBoss EAP.

RedHat JBoss EAP note: Cuando el SPSS Statistics Server utiliza IBM GSKit SSL, debe utilizar IBM JDK al configurar IBM SPSS Servicios de Colaboración e Implantación en JBoss EAP.

1. Distribuya el archivo `root . pem` a la máquina de IBM SPSS Servicios de Colaboración e Implantación Server. Si tiene varias entidades emisoras de certificados de confianza, cópielas en un único archivo `root . pem` (las entidades emisoras de certificados de confianza son archivos de texto, por lo que puede copiar y pegar los certificados) Copie `root . pem` en la siguiente ubicación del servidor de IBM SPSS Servicios de Colaboración e Implantación .

Si ya ha copiado un archivo `root . pem` en el cliente para otro producto IBM, añada la información de la entidad emisora de certificados raíz de confianza de su entidad emisora en el archivo `root . pem` existente. Cree una variable de entorno `SSL_CERT_DIR` y establezca el valor de la variable en la ubicación del servidor que desee que contenga el archivo `root . pem`.

2. Verifique que el usuario del servidor IBM SPSS Servicios de Colaboración e Implantación añade la variable de entorno `SSL_CERT_DIR`.

Nota: El servidor IBM SPSS Servicios de Colaboración e Implantación se debe reiniciar después de añadir la variable de entorno.

Instalación del cifrado de potencia ilimitada

Java Runtime Environment, que se incluye como parte del producto, tiene activado el cifrado de potencia para exportación de EE.UU. Para mejorar la seguridad de los datos, se recomienda actualizar a cifrado de potencia ilimitada.

1. Extraiga los archivos de políticas de jurisdicción sin limitaciones que están empaquetados en el archivo comprimido. El archivo comprimido contiene un archivo `US_export_policy.jar` y un archivo `local_policy.jar`.
2. Sustituya las copias existentes de los archivos `US_export_policy.jar` y `local_policy.jar` con los dos archivos que ha descargado y extraído.

Indicar a los usuarios que habiliten SSL

Cuando los usuarios se conectan al servidor mediante un producto cliente, tienen que habilitar SSL en el cuadro de diálogo para conectarse con el servidor. Asegúrese de indicar a sus usuarios que seleccionen la casilla de verificación apropiada.

Habilitar SSL mediante OpenSSL

Proteger comunicaciones de cliente/servidor y servidor-servidor con OpenSSL

Nota: A partir de la versión 30.0.0, Open SSL 1.1 está obsoleto.

Los pasos principales en las comunicaciones cliente-servidor y servidor-servidor seguras con SSL son:

1. Instalar OpenSSL en el ordenador servidor.
2. Obtener e instalar el certificado SSL y las claves.
3. Activar y configurar SSL en la aplicación de administración de servidores (IBM SPSS Deployment Manager).

Nota: IBM SPSS Statistics El servidor da soporte al protocolo TLSv1. Se ha comprobado que SSLv3 tiene una vulnerabilidad de seguridad y no se debe utilizar.

4. Si se utilizan certificados de cifrado con una potencia mayor que 2048 bits, instale el cifrado de potencia ilimitada en los sistemas cliente de .
5. Si utiliza un certificado autofirmado, copie el certificado en el sistema del cliente.
6. Indicar a los usuarios que habiliten SSL cuando se conecten con el servidor.

Nota: En algunas ocasiones un servidor actúa como cliente. Un ejemplo es IBM SPSS Statistics Server conectándose al IBM SPSS Repositorio de Servicios de Colaboración y Despliegue. En este caso, IBM SPSS Statistics Server es el *cliente*.

Instalar OpenSSL

Si OpenSSL no está aún disponible en el servidor, deberá instalarlo.

1. Descargue OpenSSL desde <http://www.openssl.org/>. Asegúrese de utilizar la versión de OpenSSL apropiada para la versión del servidor:

Producto servidor	Versión de OpenSSL compatible
IBM SPSS Statistics 29	1.1.1f o posterior
IBM SPSS Statistics 28	1.1.1f o posterior

<i>Tabla 2. Versiones de OpenSSL (continuación)</i>	
Producto servidor	Versión de OpenSSL compatible
IBM SPSS Statistics 27.0.1	1.1.1f o posterior Nota: El soporte para el protocolo SSLv3 no seguro ha quedado en desuso.
IBM SPSS Statistics 26-27	1.0.2 o posterior
IBM SPSS Statistics 24-25	1.0.1f o posterior
IBM SPSS Statistics 20-23	1.0.0
IBM SPSS Statistics 17-19 (no Linux® en System z®)	0.9.8 y sus subversiones (0.9.8a, 0.9.8b, etc.)
IBM SPSS Statistics 19 (Linux® en System z®)	1.0.0

2. Siga las instrucciones para instalar y configurar el software. Se recomienda que cree OpenSSL usted mismo con las siguientes directrices:

Windows. OpenSSL debe crearse con bibliotecas DLL (que son multiproceso de forma predeterminada).

UNIX. OpenSSL debe admitir subprocesos múltiples (que no es siempre el valor predeterminado) y bibliotecas compartidas.

3. Asegúrese de que los módulos OpenSSL están incluidos en la ruta del sistema.

Nota: Si hay más de una versión de los módulos OpenSSL en el sistema servidor, copie los módulos de OpenSSL para el servidor de IBM SPSS Statistics en el directorio en el que está instalado el servidor de IBM SPSS Statistics.

Obtención e instalación de certificados y claves SSL

1. Obtenga un archivo de certificado y de clave SSL. Existen dos formas de hacerlo:
 - Adquiéralos a través de una entidad emisora de certificados públicos (como Comodo, Symantec o GoDaddy). La entidad emisora de certificados públicos firma el certificado para verificar el servidor que lo utiliza. Este es el método recomendado.
 - Genere los archivos de clave y de certificado mediante una entidad emisora de certificados autofirmados interna. OpenSSL proporciona una herramienta de gestión de certificados para este fin, o puede buscar instrucciones en Internet acerca de la creación de un certificado autofirmado de SSL.
2. Copie el certificado y el archivo o archivos de claves a un directorio o directorios locales en el servidor. Las claves públicas y privadas pueden almacenarse en directorios separados. También se pueden almacenar en un único archivo. Asegúrese de que la clave privada no esté en una ubicación que se pueda encontrar durante el examen casual del sistema de archivos.
3. Copie la entidad emisora de certificados de confianza denominada *root.pem* en la ubicación siguiente en el sistema del servidor. Si desea utilizar otra ubicación, cree una variable de entorno `SSL_CERT_DIR` y establezca el valor de la variable en la ubicación.

Windows 7 y superior: `C:\ProgramData\IBM\SPSS\certificates`

Mac: `/Library/Application Support/IBM/SPSS/certificates`

UNIX y Linux: `/opt/IBM/SPSS/certificates`

Habilite y configure SSL en el IBM SPSS Deployment Manager

1. Inicie la aplicación de administración de servidor (IBM SPSS Statistics Administration Console, instalada como parte de IBM SPSS Deployment Manager) y conecte con el servidor.
2. En la página de configuración, asigne **Secure Sockets Layer** a Sí.
3. En el **archivo de clave pública SSL**, especifique la vía de acceso completa al archivo de clave pública.
4. En el **archivo de clave privada SSL**, especifique la vía de acceso completa al archivo de clave privada.
Nota: Si las claves pública y privada están almacenadas en un archivo, especifique el mismo archivo en el **archivo de clave pública SSL** y en el **archivo de clave privada SSL**.
5. En los menús seleccione:
Archivo > Guardar
6. Reinicie el servicio o centinela servidor. Cuando reinicie, se le solicitará la contraseña SSL. En Windows, puede seleccionar **Recordar contraseña** para almacenar la contraseña de forma segura. Esta opción elimina la necesidad de introducir la contraseña cada vez que se inicia el servidor.

Instalación del cifrado de potencia ilimitada

Java Runtime Environment, que se incluye como parte del producto, tiene activado el cifrado de potencia para exportación de EE.UU. Para mejorar la seguridad de los datos, se recomienda actualizar a cifrado de potencia ilimitada.

1. Extraiga los archivos de políticas de jurisdicción sin limitaciones que están empaquetados en el archivo comprimido. El archivo comprimido contiene un archivo `US_export_policy.jar` y un archivo `local_policy.jar`.
2. Sustituya las copias existentes de los archivos `US_export_policy.jar` y `local_policy.jar` con los dos archivos que ha descargado y extraído.

Copia del archivo de certificado a ordenadores cliente

Nota: Omita este paso si está utilizando un certificado que está firmado por una entidad emisora de certificados.

Si está utilizando un certificado autofirmado, tendrá que copiar la entidad emisora de certificados de confianza a los ordenadores *cliente*. Tenga en cuenta que un ordenador servidor también puede actuar como un cliente. Un ejemplo es IBM SPSS Statistics Server conectándose al IBM SPSS Repositorio de Servicios de Colaboración y Despliegue. En este caso, IBM SPSS Statistics Server es el *cliente*, y por lo tanto tiene que copiar el certificado para el servidor del IBM SPSS Repositorio de Servicios de Colaboración y Despliegue a IBM SPSS Statistics Server.

1. Cree una entidad emisora de certificados de confianza denominada `root.pem`. Por ejemplo, si está creando la entidad emisora de certificados de confianza con OpenSSL, utilice el conmutador `-out` para especificar el archivo de salida como `root.pem`. Si tiene varias entidades emisoras de certificados de confianza, cópielas en un único archivo `root.pem`. Las entidades emisoras de certificados de confianza son archivos de texto, de modo que puede copiar y pegar el certificado o los certificados.
2. Copie `root.pem` en la ubicación siguiente en los sistemas del cliente. Si ya ha copiado un archivo `root.pem` al cliente para otro producto IBM Corp., anexe la información de la entidad emisora de certificados de raíz de confianza de la entidad al archivo `root.pem` existente. De forma predeterminada, todos los productos cliente IBM Corp. buscan en esta ubicación archivos de certificados autofirmados de confianza. Si desea utilizar otra ubicación, cree una variable de entorno `SSL_CERT_DIR` y establezca el valor de la variable en la ubicación.

Windows 7 y superior: `C:\ProgramData\IBM\SPSS\certificates`

Mac: `/Library/Application Support/IBM/SPSS/certificates`

UNIX y Linux: `/opt/IBM/SPSS/certificates`

Indicar a los usuarios que habiliten SSL

Cuando los usuarios se conectan al servidor mediante un producto cliente, tienen que habilitar SSL en el cuadro de diálogo para conectarse con el servidor. Asegúrese de indicar a sus usuarios que seleccionen la casilla de verificación apropiada.

Establecimiento de un entorno local

El software de servidor y el cliente que se conecta a él deben ejecutarse en el mismo juego de caracteres, codificación y entorno local. El software de servidor obtiene su entorno local del cliente. De forma predeterminada, es el entorno local del *sistema* del cliente. Sin embargo, el cliente puede alterar temporalmente el valor predeterminado para procesar archivos de datos en otros entornos locales. Al alterar temporalmente el valor predeterminado, el usuario indica al software del servidor que se ejecute en un entorno local especificado sin cambiar el entorno local del sistema del cliente.

Sintaxis

El usuario altera temporalmente el valor predeterminado utilizando el mandato de sintaxis SET LOCALE :

```
SET LOCALE="localeid"
```

localeid es una serie que identifica el entorno local en el que se ejecutará el software del servidor. SET LOCALE escribe una entrada de registro en la máquina cliente. Esta entrada persiste para que la próxima vez que se inicie IBM SPSS Statistics en la máquina cliente, IBM SPSS Statistics se ejecute en ese entorno local.

El convenio de denominación para el ID de entorno local puede diferir entre plataformas y proveedores. Por lo tanto, hay un archivo XML instalado con el servidor que correlaciona los entornos locales del cliente con los entornos locales del servidor. Este archivo, *loclmap.xml*, se encuentra en el directorio de instalación del servidor en Windows y en el subdirectorio */bin* en UNIX.

loclmap.xml

El elemento raíz en *loclmap.xml* es el siguiente. El elemento raíz también identifica la ubicación del esquema.

```
<locale-map xmlns="http://xml.spss.com/spss/mls"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.spss.com/spss/mls
http://xml.spss.com/spss/mls/locale-map-1.0.xsd">
```

El elemento raíz contiene elementos `<client-locale>` con un atributo `name` que identifica el entorno local del cliente. Los elementos `<client-locale>` contienen uno o más elementos `<server-locale>`. Cada elemento `<server-locale>` tiene un atributo `name` que identifica un entorno local del servidor que corresponde al entorno local del cliente. El software del servidor convierte el ID de entorno local del cliente en uno que se puede utilizar en la máquina del servidor. Comprueba cada entorno local del servidor en orden, hasta que encuentra uno que sea válido en la máquina del servidor.

Ninguno de los entornos locales de servidor predeterminados en *loclmap.xml* son entornos locales de Windows. Los entornos locales del sistema Windows generalmente no son necesarios porque el software del servidor primero intenta utilizar el mismo entorno local que el entorno local del sistema del cliente. Un servidor Windows debe tener el entorno local que coincida con el entorno local del cliente. Sin embargo, puede añadir entornos locales de servidor Windows a *loclmap.xml* si necesita sustituir un entorno local de Windows diferente pero similar.

Puede modificar *loclmap.xml* según sea necesario. Sólo tenga en cuenta que los elementos XML deben validarse con respecto al esquema.

Ejemplo

A continuación se muestra un ejemplo del contenido de *loclmap.xml*:

```
<client-locale name="French">
  <server-locale name="fr_FR.cp1252"></server-locale>
  <server-locale name="fr_FR.IBM-1252@euro"></server-locale>
  <server-locale name="fr_FR.IBM-1252"></server-locale>
  <server-locale name="fr_FR.8859-15"></server-locale>
  <server-locale name="fr_FR.IS08859-15"></server-locale>
  <server-locale name="fr_FR.iso885915@euro"></server-locale>
  <server-locale name="fr_FR@euro"></server-locale>
  <server-locale name="fr_FR"></server-locale>
  <server-locale name="fr"></server-locale>
  <server-locale name="fr_FR.iso88591"></server-locale>
  <server-locale name="fr_FR.IS08859-1"></server-locale>
  <server-locale name="fr_FR.windows-1252"></server-locale>
  <server-locale name="fr_FR.utf8"></server-locale>
  <server-locale name="fr_FR.UTF-8"></server-locale>
  <server-locale name="French_France.1252"></server-locale>
</client-locale>
```

En este caso, si el usuario emite SET LOCALE="French", el software del servidor comprueba primero fr_FR.cp1252. Considere el caso de un servidor AIX. El entorno local de fr_FR.cp1252 no funciona en AIX, por lo que el software del servidor continúa comprobando hasta que alcanza fr_FR.windows-1252, lo que funciona en AIX.

Utilización de un entorno local de servidor

Si el usuario emite SET LOCALE utilizando un ID de entorno local de servidor no reconocido en la máquina cliente, la máquina cliente utiliza *loclmap.xml* para buscar el ID de entorno local de cliente asociado a un ID de entorno local de servidor. Escribe este ID de entorno local en el registro. Por ejemplo, si el usuario emite SET LOCALE="fr_FR.windows-1252", French se escribe en el registro. Para ver qué entrada de *loclmap.xml* se aplica al cliente, puede ejecutar el mandato SHOW LOCALE en modalidad local.

Posibles problemas

Tenga en cuenta que el uso del mandato SET LOCALE puede causar problemas funcionales en algunos casos:

- Es posible que los nombres de variable actuales no estén legales en la nueva página de códigos.
- Las coincidencias de nombres que no distinguen entre mayúsculas y minúsculas pueden fallar. El error se puede producir porque las series se convierten a caracteres en mayúsculas en coincidencias de nombres que no distinguen entre mayúsculas y minúsculas (por ejemplo, al comparar nombres de variables). Si el entorno local es incorrecto, esta conversión cambiaría el carácter (por ejemplo, en la página de códigos de Europa central, 1250).
- Algunos bytes podrían interpretarse incorrectamente como bytes iniciales, y podría producirse un problema debido a un byte de seguimiento inesperado.
- SET LOCALE no cambia el entorno local del sistema del cliente. Por lo tanto, si el entorno local de IBM SPSS Statistics asociado con SET LOCALE es diferente del entorno local del sistema del cliente, habrá problemas de visualización en varios lugares. En esta situación, un usuario tampoco puede utilizar un editor de métodos de entrada (IME) para especificar caracteres nacionales.
- El entorno local de IBM SPSS Statistics, el valor OLANG y la codificación utilizada para los datos deben ser compatibles. De lo contrario, es posible que la salida sea inutilizable e ilegible.

Conexión con el software de servidor

El usuario final se conecta al software de servidor iniciando sesión desde la aplicación cliente. Para iniciar una sesión, un usuario final necesita la siguiente información:

- **Nombre de sistema o dirección IP.** Cuando los usuarios finalizan la conexión con el software de servidor, inician la sesión desde la aplicación cliente. Para ello, deben especificar correctamente el nombre del sistema que ejecuta el software de servidor. El sistema servidor se puede identificar mediante un nombre alfanumérico (por ejemplo, myserver) o una dirección IP asignada al sistema

servidor (por ejemplo, 202 . 123 . 456 . 78), lo que prefiera. Si configura los equipos de escritorio de servidor y cliente para utilizar SSL (Secure Sockets Layer), el usuario final debe utilizar un nombre de dominio completo (por ejemplo, myserver . mycompany . com).

- **Número de puerto.** Los usuarios finales deben especificar correctamente el puerto en el que el software del servidor está a la escucha de conexiones. El número de puerto es el valor predeterminado para el servidor, o lo que haya especificado al configurar el software del servidor.
- **Nombre de dominio (sólo Windows).** Es posible que los usuarios finales también necesiten especificar un nombre de dominio. Un nombre de dominio sólo es necesario cuando el sistema servidor está en un dominio distinto al de los sistemas de escritorio de usuario final.
- **ID de usuario y contraseña.** Los usuarios finales deben iniciar sesión en el sistema servidor. Para ello, los usuarios necesitan una cuenta válida, con los permisos adecuados, para el sistema en el que se ejecuta el software de servidor.
- **Capa de sockets seguros (SSL).** Si utiliza SSL para cifrar las comunicaciones que se producen cuando los usuarios finales se conectan al software del servidor, indique a los usuarios que habiliten SSL cuando configuran la conexión del servidor. Los clientes no necesitan saber qué protocolo SSL está utilizando el servidor. El software del cliente intentará ambos y usará el que funciona.

Acceso a datos y archivos

Cuando los usuarios finales se conectan al software de servidor analítico, su vista de orígenes de datos y archivos es desde la perspectiva del equipo servidor, no de sus equipos de escritorio.

- **Orígenes de datos ODBC.** Si los usuarios finales necesitan acceder a los orígenes de datos ODBC definidos en el sistema servidor, distribuya los nombres, las descripciones y la información de inicio de sesión para dichos orígenes de datos. Consulte [Capítulo 3, “Acceso a datos”, en la página 9](#) para obtener información sobre el acceso a la base de datos desde el software del servidor.
- **Acceso a archivos.** Distribuya los nombres y las ubicaciones de los archivos en el sistema servidor al que desea que accedan los usuarios finales. Consulte el tema [“Datos de referencia” en la página 10](#) para obtener más información.

Guardar datos y archivos

Cuando los usuarios finales guardan archivos mientras están conectados al software del servidor, la ubicación predeterminada para la operación de salvar es el directorio desde el que se ha abierto el archivo. En muchos casos, este es el ordenador local de escritorio; sin embargo, para los archivos de datos, a menudo será una ubicación protegida contra escritura en el ordenador del servidor. Indique a los usuarios dónde guardar los archivos de datos. Normalmente, la ubicación es el directorio de inicio del usuario en algún lugar de la red.

Nota de UNIX: indique a los usuarios finales que utilicen la especificación de archivo completa y las barras inclinadas al guardar archivos (por ejemplo, /public/myhome/myserverdata/data.sav). Evite utilizar el carácter de barra inclinada invertida en el directorio UNIX y los nombres de archivo utilizados con el software de servidor.

Capítulo 6. Análisis y mejora del rendimiento

Si necesita mejorar el rendimiento del software del servidor, consulte este capítulo para ver diversas estrategias, desde cambios de configuración hasta actualizaciones de hardware. Antes de realizar estos cambios, obtenga información de rendimiento para saber qué áreas son problemáticas.

También proporcionamos un documento técnico que incluye información adicional sobre cómo mejorar el rendimiento. Vaya a <http://www.ibm.com/developerworks/spssdevcentral> y busque el enlace a "Libros y artículos".

Obtención de información de rendimiento

Para comprobar el rendimiento, compare el uso en las áreas siguientes cuando el servidor no se está utilizando cuando se está utilizando mucho.

- Uso de disco
- Uso de CPU
- Uso de memoria
- Uso de red

Registro

La aplicación de administración (IBM SPSS Statistics Administration Console, que se instala como parte de IBM SPSS Deployment Manager) le permite configurar el software de servidor para registrar información de rendimiento. Utilizando el nodo **Intervalo de registro de rendimiento**, puede especificar la frecuencia con la que el software del servidor graba información de rendimiento en el registro. Consulte el tema Registro en la publicación *Deployment Manager User's Guide* (incluida en la ayuda de IBM SPSS Servicios de Colaboración e Implantación) para obtener más información. También puede obtener información de rendimiento directamente del sistema operativo.

Obtención de información de rendimiento en Windows

En Windows, puede obtener información de rendimiento utilizando el Supervisor de rendimiento.

Área	Objeto de supervisor de rendimiento de Windows	Contador útil
Uso de disco	PhysicalDisk	% de tiempo desocupado
Uso de CPU	Procesador	% de tiempo de procesador
Uso de memoria	Memoria	Bytes confirmados
Uso de red	Interfaz de red	Total de bytes/seg para cada instancia de interfaz física (no la interfaz de bucle de retorno de MS TSP)

Obtención de información de rendimiento en UNIX

En UNIX, hay varios mandatos para obtener información de rendimiento, en función del proveedor.

Tabla 4. Información de rendimiento de UNIX

Área	Proveedor	Mandato	Nota
Uso de disco	Linux	iostat -x	Compruebe la columna %util .
Uso de disco	AIX	iostat -d	Compruebe la columna % tm_actl .
Uso de CPU	Linux	principal	Utilice el mandato interactivo P para ordenar por uso de CPU.
Uso de CPU	AIX	ps aux	Utilice el conducto para el mandato sort para ordenar por la columna %CPU .
Uso de CPU	Todos	tiempo de funcionamiento	Compruebe el promedio de carga.
Uso de memoria	Linux	principal	Utilice el mandato interactivo M para ordenar por uso de CPU.
Uso de memoria	AIX	ps aux	Interconectar con el mandato sort para ordenar por la columna RSS .
Uso de red	Todos	netsat	Utilice los conmutadores -i y -s para obtener información.

Paso siguiente

Después de recopilar esta información, debe ser capaz de identificar el área o áreas que son problemáticas. Las secciones siguientes describen posibles soluciones y recomendaciones para cada área.

Mejora del uso de disco

Tenga en cuenta lo siguiente para mejorar el uso del disco.

por un solo espacio. Deje suficiente espacio de disco. Normalmente, cada usuario necesita un espacio de disco temporal igual al doble del tamaño del archivo de datos (SAV) en uso (el espacio necesario oscila entre 1 y 2.5 veces). Un usuario que ordena un archivo puede necesitar espacio temporal más de tres veces el tamaño del archivo. Por ejemplo, si seis usuarios simultáneos están accediendo a un archivo y dos están ordenando a la vez, es posible que necesiten hasta 17 veces el tamaño del archivo. En la práctica, no estarán en el pico de uso simultáneamente, por lo que 12 veces el tamaño del archivo sería suficiente.

Hardware. Utilice discos SCSI para obtener el rendimiento más rápido. No utilice IDE.

Configuración del sistema. Mantenga los archivos temporales en un huso separado. También puede definir varias ubicaciones de archivos temporales utilizando la aplicación de administración. Asegúrese de que cada ubicación esté en un huso separado. Si utiliza RAID, utilice RAID0 para el huso del archivo temporal. La velocidad de los archivos reutilizables obtenida de RAID0 es preferible a la redundancia obtenida de RAID1. Si la CPU no es un problema y el sistema servidor ejecuta Windows, también puede comprimir el directorio de datos o los archivos de datos en el disco. No asigne más memoria virtual.

Configuración de IBM SPSS Statistics . Si la memoria no es un problema, pero el uso de disco sí lo es, aumente el espacio de trabajo en IBM SPSS Statistics para obtener un rendimiento más rápido. Intente establecerlo dividiendo la cantidad de RAM en el sistema servidor por el número esperado de usuarios simultáneos. Por ejemplo, si el sistema servidor tiene 1 GB de RAM, establezca el espacio de trabajo en 0.25 GB de RAM.

Directorio de archivos temporales. Modifique los valores de perfil de usuario o grupos para que los directorios de archivos temporales para cada usuario se encuentren en unidades físicas diferentes.

Compresión de caché. Si los usuarios trabajan de forma coherente con archivos de datos grandes (especialmente si el tamaño de los archivos es mayor que la mitad de la RAM del servidor), intente habilitar la compresión de memoria caché en la aplicación de administración.

Mejora del uso de CPU

Tenga en cuenta lo siguiente para mejorar el uso de CPU:

Número. Añada más procesadores. Si desea acercarse a la velocidad que experimentaría un usuario al ejecutar IBM SPSS Statistics localmente, intente tener un procesador por cada dos usuarios simultáneos. Utilice también procesadores que sean tan rápidos o más rápidos que el procesador del ordenador de sobremesa. Por ejemplo, si espera un promedio de cuatro usuarios simultáneos, configure el sistema servidor con dos procesadores rápidos.

Hardware. Utilice procesadores rápidos. Añadir unos pocos procesadores realmente rápidos es mejor que añadir muchos lentos. Si el uso de CPU sigue siendo un problema con los procesadores rápidos, considere la posibilidad de añadir más sistemas de servidor al sistema.

Acceso y ubicaciones de archivo SAV. Si muchos usuarios simultáneos utilizan con frecuencia determinados archivos, considere la posibilidad de mover los archivos entre varios servidores para equilibrar la carga de usuario. Por ejemplo, si *TestScores.sav* y *GPA.sav* se utilizan mucho, póngales en servidores separados. Controlar el acceso a los archivos con los permisos del sistema operativo (por grupo o por usuario) en lugar de controlar el acceso a través de cuentas de servidor.

Prioridad de CPU. Si determinados usuarios necesitan una prioridad de CPU más alta que otros usuarios (por ejemplo, los usuarios que ejecutan trabajos rápidos frente a los que ejecutan trabajos largos), modifique los valores del perfil de usuario o del grupo.

Compresión de caché. La compresión de memoria caché tiene una sobrecarga de CPU para la compresión y descompresión de archivos reutilizables. Si los usuarios no están trabajando con archivos de datos grandes, es posible que desee desactivarlo.

Mejora del uso de memoria

Tenga en cuenta lo siguiente para mejorar el uso de memoria:

Cantidad. Añada tanta RAM como sea posible. Intente tener 128 MB de RAM para cada usuario simultáneo. Por lo tanto, si hay cuatro usuarios simultáneos, configure el servidor con 512 MB de RAM.

Configuración de IBM SPSS Statistics . Disminuya el espacio de trabajo en IBM SPSS Statistics.

Mejora del uso de red

Tenga en cuenta lo siguiente para mejorar el uso de la red:

Configuración del sistema. Planifique las operaciones que requieren un uso intensivo de la red para las horas en las que el software del servidor no está en uso (por ejemplo, ejecutar copias de seguridad del sistema durante la noche). Si identifica un problema con el tráfico de red en un sistema en el que se está ejecutando el servidor, IBM Corp. trabajará con usted para diagnosticar el problema más adelante.

Utilización eficiente de IBM SPSS Statistics

Además de centrarse en áreas problemáticas específicas, también puede mejorar el rendimiento adhiriéndose a las directrices siguientes para utilizar IBM SPSS Statistics de forma eficiente.

Gestión de datos. Si tiene archivos de datos grandes que requieren una actualización regular y los comparten los usuarios, considere la posibilidad de realizar las actualizaciones una vez y, a continuación, liberar los archivos a los usuarios para su análisis. Por ejemplo, si añade regularmente datos mensuales a un archivo, lo ordena y realiza transformaciones, designe una persona para ejecutar el trabajo en el archivo. Los demás usuarios pueden obtener los datos que necesitan sin tener que repetir la fusión, la ordenación y las transformaciones.

Interactivo frente a lote. Si tiene operaciones regulares que requieren mucho tiempo que realiza con IBM SPSS Statistics, considere ejecutarlas desde el recurso por lotes de IBM SPSS Statistics en lugar de desde un cliente conectado al servidor. Utilice el cliente para crear los informes y ejecútelos desde IBM SPSS Statistics Batch Facility después de que los informes estén listos.

Apéndice A. Resolución de problemas

Software de servidor

Error de inicio de sesión local (solo Windows). Los usuarios pueden encontrarse con una situación en la que el inicio de sesión falla porque no tienen el privilegio de inicio de sesión local en el servidor. Para resolver este problema, debe realizar cambios en el `spssprod.inf` archivo. Para obtener más información sobre este problema conocido y la solución provisional relacionada, consulte [Solución alternativa para el requisito del servidor de que los usuarios tengan el privilegio "permitir iniciar sesión localmente"](#).

Conflicto de número de puerto. Si hay un conflicto de número de puerto, es posible que el software del servidor no se pueda iniciar. Corrija el problema utilizando la aplicación de administración (IBM SPSS Statistics Administration Console, que se instala como parte de IBM SPSS Deployment Manager) para cambiar el número de puerto. Consulte el tema Conexiones en la publicación *Deployment Manager User's Guide* (incluida en la ayuda de IBM SPSS Servicios de Colaboración e Implantación) para obtener más información.

Comportamiento errático. El software del servidor puede comportarse de forma errática si su archivo de configuración (por ejemplo, `statisticsd.conf`) está dañado o falta. Para corregir el problema, restaure el archivo de configuración desde la copia de seguridad. Cópielo en la ubicación especificada en la aplicación de administración o en la variable de entorno del archivo de configuración y reinicie el software del servidor. Para obtener más información sobre el reinicio, consulte ["Inicio y detención del software de servidor"](#) en la página 22 en.

La aplicación de administración no funciona (sólo UNIX). Si utiliza la aplicación de administración para controlar o configurar el software del servidor y no funciona (por ejemplo, no puede detener el servidor), puede deberse a que no ha iniciado el software del servidor con el script de inicio proporcionado por IBM Corp.. Corrija el problema iniciando el software del servidor con el script de inicio `start_statistics_server`. Consulte el tema ["Para detener el servicio o el daemon"](#) en la página 22 para obtener más información. Si recibe un mensaje de error cuando intenta controlar o configurar el software del servidor, puede deberse a que se ha conectado con una cuenta que no tiene permisos de administrador.

No se puede cambiar la ubicación de los archivos temporales (sólo UNIX). Si utiliza la aplicación de administración para cambiar la ubicación de los archivos temporales y el cambio no es efectivo, puede deberse a que la nueva ubicación no tiene suficientes permisos de archivo para los usuarios finales. Elija una ubicación que tenga un acceso de **lectura, escritura y ejecución** para todos los usuarios que se conectan al software de servidor.

El servidor no se inicia (sólo UNIX). Si el software del servidor no se inicia, puede deberse a que no tiene los parches necesarios del sistema operativo. Para corregir el problema, descargue e instale el parche adecuado. Los parches necesarios se listan en las instrucciones de instalación de UNIX para el producto de servidor.

Software de cliente

El usuario final no puede conectarse al servidor. Es posible que el usuario no tenga los permisos adecuados o que el cortafuegos esté bloqueando el software del servidor. Para obtener información sobre los permisos de usuario, consulte ["Permisos"](#) en la página 31. Para obtener información sobre cómo configurar el cortafuegos, consulte ["Configuración de conexiones a través de un cortafuegos"](#) en la página 33.

El inicio de sesión del usuario final falla con el mensaje "no se ha encontrado el sistema de servidor remoto especificado". Es posible que el servicio o daemon no se esté ejecutando. Confirme esto comprobando el estado del software del servidor. Para corregir el problema, reinicie el servicio o daemon. Consulte el tema ["Inicio y detención del software de servidor"](#) en la página 22 para obtener más información.

El inicio de sesión del usuario final falla con el mensaje "error al conectarse al paquete". El usuario final ha especificado el nombre o la dirección IP de un sistema servidor que no está en la red. Para corregir el problema, solicite al usuario final que especifique un nombre de servidor válido.

El origen de datos de DataDirect ODBC falla con el mensaje "sin licencia". La tecnología de acceso a datos DataDirect se distribuye con productos IBM Corp. . Solo funciona con productos IBM Corp. más recientes; no funciona con versiones anteriores ni con aplicaciones que no sean de IBM Corp. . Si los usuarios finales intentan utilizar orígenes de datos DataDirect con un producto anterior o sin licencia, obtendrán un mensaje que contiene el texto **No tiene licencia para utilizar el controlador DataDirect ODBC**. Para corregir el problema con el producto IBM Corp. , actualice los usuarios a una versión actual. Para corregir el problema con los productos sin licencia, actualice la licencia con DataDirect o solicite a los usuarios finales que no intenten utilizar los orígenes de datos que ha definido para los productos IBM Corp. con aplicaciones sin licencia.

El usuario final no puede encontrar un archivo de datos o un origen de datos ODBC . Cuando los usuarios finales se ejecutan en modo de análisis distribuido, solo tendrán acceso a los archivos de datos y a los orígenes de datos ODBC en el sistema que ejecuta el software de servidor. Cuando los usuarios finales se ejecutan en modo de análisis local, solo tendrán acceso a los archivos de datos y a los orígenes de datos ODBC en sus sistemas de escritorio. Para corregir el problema, solicite al usuario final que ejecute la aplicación cliente en la modalidad adecuada.

El usuario final no puede ejecutar un procedimiento estadístico (sólo IBM SPSS Statistics Server). Cuando los usuarios finales están conectados al software de servidor, solo tienen acceso a las opciones de IBM SPSS Statistics que se instalaron durante la instalación de IBM SPSS Statistics Server. Para corregir el problema, pida al usuario final que ejecute el procedimiento mientras está en modalidad de análisis local o instale el procedimiento solicitado en el sistema servidor.

Apéndice B. IBM SPSS Statistics Batch Facility

Nota: IBM SPSS Statistics Batch Facility es un programa de utilidad de proceso por lotes que se incluye con **IBM SPSS Statistics Server**.

Normalmente, el cliente para IBM SPSS Statistics Server es IBM SPSS Statistics que se ejecuta en un sistema de escritorio. Sin embargo, IBM SPSS Statistics Batch Facility es una forma alternativa de utilizar la potencia de IBM SPSS Statistics Server y se ejecuta en el sistema servidor. IBM SPSS Statistics Batch Facility está pensado para la **producción automatizada** de informes estadísticos. La producción automatizada proporciona la capacidad de ejecutar análisis sin intervención del usuario. La producción automatizada es ventajosa si los usuarios de su sitio requieren regularmente un conjunto de análisis que requieren mucho tiempo, como por ejemplo informes semanales.

IBM SPSS Statistics Batch Facility toma como entrada una solicitud de informe contenida en un archivo de **sintaxis de mandatos**. A continuación, IBM SPSS Statistics Batch Facility genera automáticamente los informes estadísticos especificados por la sintaxis.

Información que necesita saber

. IBM SPSS Statistics Batch Facility está disponible actualmente con todos los servidores IBM SPSS Statistics, UNIX y Windows.

Instalación. IBM SPSS Statistics Batch Facility se instala automáticamente en el directorio de instalación de IBM SPSS Statistics Server en Windows y el subdirectorio */bin* del directorio de instalación en UNIX.

Invocación. IBM SPSS Statistics Batch Facility se ejecuta desde la línea de mandatos utilizando el archivo ejecutable *statisticsb*. Se ejecuta independientemente de IBM SPSS Statistics Server-IBM SPSS Statistics Server no tiene que iniciarse para que se ejecute. También se puede ejecutar simultáneamente con IBM SPSS Statistics Server.

Modalidades de operación. Los mandatos se envían a IBM SPSS Statistics Batch Facility en **batch** o **interactive mode**. En modalidad de proceso por lotes, el analista o profesional de TI envía un archivo de sintaxis de mandatos a IBM SPSS Statistics Batch Facility para su ejecución: los mandatos del archivo se leen y actúan como un lote, y la salida se dirige a un archivo. IBM SPSS Statistics Batch Facility se ejecuta de forma desatendida y termina después de ejecutar el último mandato. Esta es la forma habitual de utilizar IBM SPSS Statistics Batch Facility. En modalidad interactiva, el analista escribe mandatos de uno en uno en un indicador de mandatos. Los mandatos se ejecutan inmediatamente y la salida se visualiza en la ventana. El recurso por lotes de IBM SPSS Statistics espera el siguiente mandato.

Documentación. La guía del usuario, escrita para los analistas y profesionales de TI en un sitio que utilizará IBM SPSS Statistics Batch Facility, está en el IBM SPSS Statistics Servidor DVD en */Documentation/<language>/Manuals*. La guía de referencia de sintaxis de mandatos que los analistas necesitarán para crear archivos de sintaxis de mandatos para IBM SPSS Statistics Batch Facility está en el IBM SPSS Statistics Servidor DVD en */Documentation/<language>/Manuals*. IBM SPSS Statistics Batch Facility for UNIX también se distribuye con una página manual, *statisticsb.1*, que se encuentra en el subdirectorio */bin* del directorio de instalación de IBM SPSS Statistics Server. Si está administrando un sistema UNIX, cópielo en la ubicación donde mantiene las páginas de manual.

Documentación adicional. La guía del usuario de IBM SPSS Statistics Batch Facility contiene información suficiente para un analista con experiencia en el lenguaje de sintaxis de mandatos IBM SPSS Statistics para crear archivos de sintaxis de mandatos para IBM SPSS Statistics Batch Facility. Si los analistas del sitio son nuevos en IBM SPSS Statistics, es posible que necesiten documentación adicional. Si lo hacen, diríjrelos a nuestro sitio web en <http://www.ibm.com/software/analytics/spss/>, o pídale que se pongan en contacto con su representante de ventas.

Apéndice C. Tareas del sistema operativo Windows

Puede realizar la mayoría de las tareas administrativas con la aplicación de administración ; sin embargo, es posible que sea necesario realizar algunas tareas con el sistema operativo Windows. Utilice las siguientes características del sistema operativo para administrar el software del servidor que se ejecuta en Windows:

- **Propiedades de archivo.** Se utiliza para establecer el acceso del usuario final al directorio de instalación del software del servidor, la ubicación del archivo temporal y los archivos de datos.
- **Propiedades del sistema.** Se utiliza para crear variables de entorno.
- **Gestor de usuarios.** Se utiliza para crear cuentas de usuario final.
- **Panel de control de servicios.** Se utiliza para iniciar, detener y configurar el servicio.
- **Administrador de ODBC .** Se utiliza para configurar orígenes de datos.

Propiedades del archivo

Utilice Propiedades de archivo para establecer permisos en archivos. Para los archivos de datos, la forma de hacerlo depende de dónde se almacenen los datos. Cuando almacena datos en el mismo sistema que el software de servidor, controla el acceso al directorio de datos estableciendo permisos en un directorio en una unidad NTFS.

En el sistema servidor, inicie la sesión como administrador:

1. Utilice el Explorador de Windows para ir al directorio de datos.
2. Pulse el directorio, pulse con el botón derecho del ratón y pulse **Compartir** en el menú contextual.
3. Pulse la pestaña **Seguridad** y configure los permisos.

Nota: La pestaña Seguridad sólo está disponible en las unidades NTFS. Si no está seguro de qué tipo de sistema de archivos utiliza el hardware, siga estos pasos:

4. Utilice el Explorador de Windows para navegar a la unidad.
5. Pulse la unidad, pulse con el botón derecho del ratón y pulse **Propiedades** en el menú contextual.
6. Pulse la pestaña **General** y examine el valor del sistema de archivos.

Cuando almacena datos en un sistema de la red, puede controlar el acceso al directorio de datos creando un recurso compartido y estableciendo los permisos de forma adecuada.

En el sistema en red, ha iniciado la sesión como administrador:

7. Utilice el Explorador de Windows para ir al directorio de datos.
8. Pulse el directorio, pulse con el botón derecho del ratón y pulse **Compartir** en el menú contextual.
9. Pulse la pestaña **Compartir** en el recuadro de diálogo, pulse **Compartido como**, especifique un nombre de compartición y establezca el acceso adecuado.

Propiedades del sistema

Utilice las propiedades del sistema para crear variables de entorno.

En el sistema servidor, inicie la sesión como administrador:

1. En el escritorio de Windows, haga clic con el botón derecho en el icono del equipo. Por ejemplo, pulse con el botón derecho del ratón en **Mi PC**.
2. Seleccione **Propiedades** en el menú.
3. Pulse la pestaña **Avanzado** y, a continuación, pulse **Variables de entorno**.
4. Haga clic en **Nuevo**.

5. Escriba el nombre de la nueva variable.
6. Escriba el valor de la nueva variable.

Gestor de usuarios

Utilice el Gestor de usuarios para crear cuentas de usuario final.

En el sistema servidor, inicie la sesión como administrador:

1. En el menú Inicio de Windows, seleccione:
Programas > Herramientas administrativas
 - Seleccione **Administración de equipos** y, a continuación, **Usuarios y grupos locales**.
2. Cree las cuentas de usuario.

Panel de control de servicios

Utilice el Panel de control de servicios de Windows para:

- Detenga e inicie el servicio.
- Cambie los parámetros de inicio del servicio.
- Compruebe el estado del servidor.

Para acceder y utilizar el Panel de control de servicios:

1. En el menú Inicio de Windows, seleccione:
Valores > Panel de control
2. Seleccione **Herramientas administrativas** y, a continuación, **Servicios**.
3. Seleccione el servicio. Ahora puede comprobar su estado, iniciarlo o detenerlo y editar los parámetros de inicio.

Nota: Puede iniciar, detener y comprobar el estado del software del servidor con la aplicación de administración.

Gestor de tareas

Utilice el Gestor de tareas para ver cuántos procesos relacionados con el servidor se están ejecutando.

1. Abra el Administrador de tareas de Windows pulsando Ctrl-Alt-Delete y eligiendo **Administrador de tareas**.
2. Pulse la pestaña **Procesos**.
3. Pulse **Nombre de imagen** para ordenar los procesos alfabéticamente.
4. Busque el nombre de archivo del proceso de servidor (*statisticssrvr.exe*).
5. Busque el nombre de archivo del proceso de cliente (*statisticsproc.exe*). Hay un proceso para cada usuario final conectado actualmente al software del servidor.

Nota: Puede supervisar procesos de servidor y cliente con la aplicación de administración.

Administrador de ODBC

Utilice el administrador de ODBC para configurar los orígenes de datos del sistema y del usuario para utilizarlos con el software del servidor.

La forma en que se crea el origen de datos ODBC afecta a quién puede verlo y utilizarlo. Utilice los DSN de *system* cuando desee permitir el acceso general al origen de datos. Utilice los DSN de *usuario* cuando desee restringir el acceso a información confidencial o cuando desee adaptar el DSN a un usuario específico.

Para configurar un DSN del sistema

Los DSN del sistema pueden ser utilizados por cualquiera que haya iniciado sesión en el sistema en el que están definidos. Los DSN del sistema son más fáciles de configurar y administrar porque lo hace una sola vez para todos los usuarios.

En el sistema en el que desea que resida el origen de datos, inicie la sesión como administrador:

1. En el menú Inicio de Windows, seleccione:

Valores > Panel de control

2. Seleccione **Herramientas administrativas** y, a continuación, **Orígenes de datos**.

3. Pulse en el separador **DSN del sistema**.

4. Pulse **Añadir**.

5. Seleccione un controlador de la lista. Si está configurando un origen de datos que utiliza la tecnología de acceso a datos de IBM Corp. , los nombres de controlador Connect ODBC se etiquetan con el texto IBM Corp. OEM.

6. Pulse **Finalizar**.

7. Especifique la información adecuada en el recuadro de diálogo **Configuración de controlador** .

8. Pulse **Aceptar**.

Para configurar un DSN de usuario

Los DSN de usuario sólo pueden ser utilizados por la cuenta del usuario que los ha creado. Configure los DSN de usuario cuando desee restringir el acceso a información confidencial o cuando desee adaptar el DSN a un usuario específico.

Inicie la sesión como usuario y siga los pasos para un DSN del sistema, con esta excepción:

- Pulse la pestaña **DSN de usuario** en lugar de la pestaña **DSN del sistema** .

Apéndice D. Tareas del sistema operativo UNIX

Puede realizar la mayoría de las tareas administrativas con la aplicación de administración ; sin embargo, es posible que sea necesario realizar algunas tareas con el sistema operativo UNIX. Utilice las siguientes características del sistema operativo para administrar el software del servidor que se ejecuta en UNIX:

- **chmod**. Se utiliza para establecer el acceso de usuario final a los archivos de datos.
- **env**. Se utiliza para comprobar los valores de las variables de entorno.
- **scripts**. Se utiliza para iniciar el software de servidor y configurar su entorno.
- **ps y kill**. Se utiliza para comprobar y detener procesos de servidor.
- **odbc.ini**. Se utiliza para configurar orígenes de datos ODBC .

Chmod

Utilice el mandato chmod (o chown) para cambiar o asignar la modalidad de permisos para directorios y archivos de datos. Por ejemplo, para establecer el directorio */usr/data* en sólo lectura para todo el mundo:

1. Inicie sesión como superusuario o como propietario del directorio.
2. En el indicador de comandos de UNIX, escriba:

```
chmod a-w /usr/data
```

env

Utilice el mandato env para comprobar los valores actuales de las variables de entorno. Por ejemplo, para utilizar env para comprobar los valores actuales de las variables de entorno para el software de servidor:

1. Inicie sesión como la cuenta que ha iniciado el daemon, normalmente *root*.
2. En el indicador de comandos de UNIX, escriba:

```
env
```

3. Compruebe los valores de las variables de interés.

Scripts

Para cambiar el valor de las variables de entorno, edite el script de variable de entorno al que llama el script que inicia el software de servidor. Para editar el script de variable de entorno:

1. Utilice un editor de texto para abrir el script *statsenv.sh* , que se incluye en el subdirectorio */bin* del directorio de instalación de IBM SPSS Statistics Server. Por ejemplo, abra */usr/local/myserverproduct/bin/statsenv.sh*.
2. Si es necesario, elimine el comentario de la línea que define la variable y, a continuación, especifique el nuevo valor para la variable.
3. Guarde el archivo.

El script *start_statistics_server* llama a *statsenv.sh* . Las variables de entorno establecidas y exportadas en *statsenv.sh* sólo afectan a los procesos iniciados con el script *start_statistics_server* .

ps y kill

Utilice el comando ps para obtener información sobre los procesos que está ejecutando el servidor y el informe del estado del proceso. Por ejemplo:

1. En el indicador de comandos de UNIX, escriba:

```
ps -efl.
```

2. Busque el nombre de archivo del proceso de daemon (por ejemplo, *statisticsd*). Este proceso tiene el **UID** del usuario que ha iniciado el proceso de daemon de software de servidor (normalmente *root*).
3. Busque el nombre de archivo del proceso de cliente, *statisticsproc.exe*. Hay un proceso para cada usuario final conectado actualmente al software del servidor. La columna *UID* muestra el ID de inicio de sesión del usuario final propietario del proceso de cliente.

Utilice el mandato `kill` para terminar un proceso. Por ejemplo:

4. Inicie la sesión como el usuario que ha iniciado el daemon.

5. En el indicador de comandos de UNIX, escriba:

```
kill -9 PID
```

donde *pid* es el ID de proceso del proceso.

El daemon de software de servidor también crea automáticamente un archivo que contiene su ID de proceso. En lugar de buscar manualmente el PID con el mandato `ps`, puede utilizar este archivo junto con el mandato `kill` directamente para terminar el proceso de daemon directamente:

```
kill -9 `cat statisticsd.pid`
```

Nota: Si desea utilizar la aplicación de administración para supervisar y terminar procesos, debe iniciar el software de servidor con el script de inicio proporcionado por IBM Corp.. Para obtener más información, consulte el tema "[Control del inicio del servicio](#)" en la página 20.

odbc.ini

Es posible que tenga que configurar orígenes de datos ODBC en el sistema servidor si:

- Está utilizando el paquete de acceso a datos de IBM Corp.

y

- El software del servidor necesita acceder a las bases de datos

No existe ningún administrador de ODBC en UNIX. Para configurar un origen de datos ODBC en UNIX, edite un archivo de texto de información del sistema, *odbc.ini*. *Odbc.ini* se instala al instalar el paquete de acceso a datos para UNIX. Las instrucciones de instalación aparecen en *IBM Corp. Data Access Pack Installation Instructions for Unix.pdf* (el documento se encuentra en el directorio */Documentation/<language>/InstallationDocuments* en el producto DVD). Asegúrese de instalar la documentación adicional para tener acceso a los documentos listados a continuación.

Connect ODBC. Para obtener información sobre cómo editar el archivo *odbc.ini* y establecer variables de entorno importantes, consulte la sección "Configuración de controladores y orígenes de datos" en el capítulo "Instalación en UNIX" de *Instrucciones de instalación de Connect ODBC* para obtener instrucciones detalladas.

La documentación del producto de DataDirect correspondiente a Connect ODBC se incluye, de forma predeterminada, como parte de la instalación de IBM SPSS Data Access Pack. El instalador crea la entrada IBM SPSS OEM Connect y ConnectXE para ODBC junto con las entradas de los demás programas del menú Inicio. Puede acceder a la documentación del producto de DataDirect a través de este elemento de menú.

Puede encontrar la documentación de producto de DataDirect para Connect ODBC en el directorio en el que ha extraído los archivos.

Nota: También se puede acceder a la documentación desde la página principal de DataDirect en <http://www.datadirect.com>.

Avisos

Esta información se ha desarrollado para productos y servicios que se ofrecen en EE.UU. Este material de IBM podría estar disponible en otros idiomas. Sin embargo, puede que se le exija poseer una copia del producto o de una versión del producto en ese idioma para poder acceder a él.

Es posible que IBM no ofrezca los productos, servicios o características descritos en este documento en otros países. Póngase en contacto con el representante local de IBM, que le informará sobre los productos y servicios disponibles actualmente en su área. Cualquier referencia a un producto, programa o servicio de IBM no pretende afirmar ni implicar que solo se puede utilizar dicho producto, programa o servicio de IBM. En su lugar, se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos intelectuales de IBM. Sin embargo, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patentes pendientes que cubran el tema principal descrito en este documento. El suministro 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, MD-NC119Armonk, NY 10504-1785Estados Unidos

Para consultas sobre licencias relacionadas con información de doble byte (DBCS), póngase en contacto con el departamento de propiedad intelectual de IBM de su país o envíe sus consultas, por escrito, a:

Licencia de Propiedad intelectual

Legal and Intellectual Property Law

IBM Japan Ltd.

19-21, Nihonbashi-Hakozakicho, Chuo-kuTokio 103-8510, Japón

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍAS DE NINGUNA CLASE, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN, COMERCIALIZACIÓN O ADECUACIÓN A UN FIN DETERMINADO. Algunas jurisdicciones no permiten la renuncia de garantías expresas o implícitas en determinadas transacciones, por lo que esta declaración podría no ser aplicable a su caso.

Esta publicación puede contener inexactitudes 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 en esta información a sitios web que no son de IBM se proporcionan solo por comodidad y de ningún modo suponen un aval de dichos sitios. La información de esos sitios web no forma parte de la información de este producto de IBM y la utilización de esos sitios web se realiza bajo la responsabilidad del usuario.

IBM puede utilizar o distribuir cualquier información que proporcione de la forma que crea adecuada sin incurrir por ello en ninguna obligación con el cliente.

Los licenciarios de este programa que deseen tener información sobre él con el fin de permitir: (i) el intercambio de información entre programas creados independientemente y otros programas (incluido el presente programa) y (ii) el uso recíproco de la información que se ha intercambiado, deben ponerse en contacto con:

IBM Director of Licensing

IBM Corporation

North Castle Drive, MD-NC119Armonk, NY 10504-1785Estados Unidos

Dicha información puede estar disponible, sujeta a los términos y condiciones correspondientes, incluidos en algunos casos, el pago de una tarifa.

El programa bajo licencia que se describe en este documento y todo el material bajo licencia disponible lo proporciona IBM bajo los términos de las Condiciones generales de IBM, Acuerdo internacional de programas bajo licencia de IBM o cualquier otro acuerdo equivalente entre ambas partes.

Los ejemplos de cliente y datos de rendimiento citados se presentan solo con fines ilustrativos. Los resultados de rendimiento reales pueden variar en función de las configuraciones específicas y de las condiciones de funcionamiento.

La información relativa a los productos que no son de IBM se ha obtenido de los proveedores de dichos productos, de sus anuncios publicados o de otras fuentes disponibles públicamente. IBM no ha probado estos productos y no puede confirmar la precisión del rendimiento, la compatibilidad ni ninguna otra declaración relacionada con productos no IBM. Las preguntas sobre las prestaciones de productos que no son de IBM deben dirigirse a los proveedores de dichos productos.

Las declaraciones relativas a la dirección o intenciones futuras de IBM pueden cambiar o ser retiradas sin previo aviso, y solo representan propósitos y objetivos.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales diarias. Para ilustrarlos de la forma más completa posible, los ejemplos incluyen nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con los nombres de personas o empresas reales es pura coincidencia.

LICENCIA DE DERECHOS DE AUTOR:

Esta información contiene programas de aplicación de ejemplo en lenguaje fuente, que se utilizan para ilustrar las técnicas de programación y distintas plataformas operativas. Puede copiar, modificar y distribuir estos programas de muestra de cualquier modo sin pagar a IBM con el fin de desarrollar, utilizar, comercializar o distribuir programas de aplicación que se ajusten a la interfaz de programación de aplicaciones para la plataforma operativa para la que se ha escrito el código de muestra. Estos ejemplos no se han probado exhaustivamente en todas las condiciones. Por lo tanto, IBM no puede garantizar ni dar por supuesta la fiabilidad, la capacidad de servicio ni la funcionalidad de estos programas. Los programas de muestra se proporcionan "TAL CUAL" sin garantía de ningún tipo. IBM no se hará responsable de los daños derivados del uso de los programas de muestra.

Cada copia o cualquier parte de estos programas de muestra o cualquier trabajo derivado debe incluir un aviso de copyright, de esta manera:

© Copyright IBM Corp. 2021. Las partes de este código se derivan de IBM Corp. Programas de ejemplo.

© Copyright IBM Corp. 1989 - 2021. Reservados todos los derechos.

Marcas comerciales

IBM, el logotipo de IBM e ibm.com son marcas registradas o marcas comerciales registradas de International Business Machines Corp., registradas en muchas jurisdicciones en todo el mundo. Otros nombres de productos y servicios pueden ser marcas registradas de IBM o de otras empresas. Hay disponible una lista actualizada de las marcas registradas de IBM en la web, en "Copyright and trademark information", en www.ibm.com/legal/copytrade.shtml.

Adobe, el logotipo de Adobe, PostScript y el logotipo de PostScript son marcas registradas de Adobe Systems Incorporated en los Estados Unidos o en otros países.

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 de Intel Corporation o de sus subsidiarias en los Estados Unidos y en otros países.

Linux es una marca registrada de Linus Torvalds en los Estados Unidos y/o en otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en Estados Unidos o en otros países.

UNIX es una marca registrada de The Open Group en Estados Unidos y otros países.

Java y todas las marcas registradas y logotipos basados en Java son marcas comerciales o marcas registradas de Oracle y/o sus filiales.

Índice

A

Acceso a datos de
 configuración de orígenes de datos ODBC para [16](#)
 Connect ODBC [9](#)
 control [10](#)
 en UNIX [11](#)
 Factores a tener en cuenta [10](#)
 hacer referencia a datos del software de cliente [10](#)
 Orígenes de datos ODBC para [10](#)
acceso a un archivo de datos
 Información de interés para los usuarios finales [45](#)
acceso de DSN [31](#)
Administración de [17](#)
administradores del sistema
 Información de interés para los usuarios finales [23](#)
 visión general de las tareas administrativas [4](#)
aplicación cliente
 instalación de [7](#)
 resolución de problemas [51](#)
aplicación de administración [17](#)
archivo de configuración
 resolución de problemas [51](#)
archivo de perfil [16](#)
arquitectura distribuida [1](#)
autenticación
 inicio de sesión único [26](#)
 interno [24](#)
 OS [23](#)
 PAM [23](#)
 unix2 [25](#)
autorización de grupo [19](#), [31](#)

C

Capa de sockets seguros (SSL) [35](#)
certificados
 configurar [39](#)
cifrado
 SSL [35](#)
clasificación de terceros [17](#)
configuración del software de servidor [15](#)
configurar
 certificados [39](#)
 xtensiones [17](#)
Connect ODBC
 arquitectura [9](#)
 establecer el entorno UNIX para [11](#)
 visión general de [9](#)
Consola de administración de IBM SPSS Statistics [17](#)
Control de acceso basado en roles [25](#)
cortafuegos [32](#)
cuentas [15](#)

E

ejecución sin privilegios de root [24–26](#)

entorno local [43](#)
Entorno UNIX y acceso a datos [11](#)
espacio de trabajo [48](#), [49](#)
Espacio de trabajo IBM SPSS Statistics [48](#), [49](#)
espacio en disco [48](#)
estadísticas [53](#)

G

grupos
 visión general [16](#)
grupos de usuarios
 visión general [16](#)

I

IBM SPSS Servicios de Colaboración e Implantación
 sustitución [18](#)
ID de usuario y contraseña
 Información de interés para los usuarios finales [44](#)
IDE [48](#)
información de rendimiento [47](#)
inicio de sesión único
 Configuración del cliente [27](#)
 Configuración del servidor [27](#)
 nombre de principio de servicio [28](#), [29](#)
 orígenes de datos [30](#)
 pertenencia a grupos [30](#)
INSERT HIDDEN
 Unidad de producción [18](#)
instalación
 aplicación cliente [7](#)
 software de servidor [7](#)

M

mejora del rendimiento [47](#)
modalidad de análisis local
 definida [1](#)
 vista de datos [9](#)
Modo de análisis distribuido
 definida [1](#)
 pasos a utilizar [1](#)
 vista de datos [9](#)
Módulo de autenticación conectable [23](#)

N

NAT [32](#)
nombre de dominio
 Información de interés para los usuarios finales [44](#)
Nombre de la computadora
 Información de interés para los usuarios finales [44](#)
nombre de principio de servicio [28](#), [29](#)
nombres de proceso por producto [22](#)
número de puerto

número de puerto (*continuación*)
Información de interés para los usuarios finales [44](#)
resolución de problemas [51](#)

O

ordenación [17](#)
orígenes de datos
 inicio de sesión único [30](#)
Orígenes de datos ODBC
 configurar [16](#)
 Información de interés para los usuarios finales [45](#)
 resolución de problemas [51](#)
 y software de servidor [11](#)
orígenes de datos ODBC , UNIX
 definido en odbc.ini [60](#)
orígenes de datos ODBC , Windows
 DSN de usuario [56](#)
 DSN del sistema [56](#)

P

PAM [23](#)
perfiles
 visión general [16](#)
perfiles de usuario
 visión general [16](#)
permisos [31](#)
permisos a nivel de administrador [31](#)
PPTP [35](#)
Privilegios de root [24–26](#)
procesadores [49](#)
producción automatizada con IBM SPSS Statistics Server [53](#)
productos y sistemas operativos [1](#)
protocolo de túnel punto a punto [35](#)

R

RAID [48](#)
RAM [49](#)
RBAC [25](#)
Recurso por lotes IBM SPSS Statistics
 introducción a [53](#)
 lo que necesita saber [53](#)
Referencias de archivo de datos UNC [45](#)
rendimiento
 mejora [47](#)
resolución de problemas
 aplicación cliente [51](#)
 archivo de configuración [51](#)
 inicio de sesión cliente [51](#)
 número de puerto [51](#)
 Orígenes de datos ODBC [51](#)
 software de servidor [51](#)

S

SCSI [48](#)
seguridad
 SSL [35](#)
servidor_estadísticas_inicio [20](#)
software de servidor
 administradores [31](#)

software de servidor (*continuación*)
 arquitectura [1](#)
 componentes [1](#)
 Configuración de [15](#)
 configuración de orígenes de datos ODBC [16](#)
 control del inicio [20](#)
 definida [1](#)
 gestión de cuentas y archivos de usuario final [15](#)
 inicio y detención [22](#)
 instalación de [7](#)
 mantenimiento rutinario de [21](#)
 nombres de proceso por producto [22](#)
 productos [1](#)
 resolución de problemas [51](#)
 utilización del script de inicio de UNIX [20](#)
 varias instancias [19](#)

SSL
 comunicaciones seguras [36, 40](#)
 visión general [35](#)
SSO [26](#)
SyncSort [17](#)

T

tareas del sistema operativo, UNIX
 utilización de odbc.ini para configurar orígenes de datos [60](#)
 utilización de scripts para establecer variables de entorno [59](#)
 utilización del mandato ps para comprobar los procesos del servidor [59](#)
 utilizar el mandato chmod para establecer permisos de archivo [59](#)
 utilizar el mandato env para comprobar las variables de entorno [59](#)
 utilizar el mandato kill para detener los procesos del servidor [59](#)
tareas del sistema operativo, Windows
 crear variables de entorno [55](#)
 establecer propiedades de archivo [55](#)
 utilización del Gestor de tareas [56](#)
 utilización del gestor de usuarios [56](#)
 utilización del panel de control Servicios [56](#)
 utilizando el administrador de ODBC [56](#)
tecnología acceso datos [9](#)

U

Unidad de producción
 INSERT HIDDEN [18](#)
UNIX
 Comprobación de las variables de entorno [59](#)
 comprobación de procesos de servidor [59](#)
 creación y configuración de orígenes de datos ODBC [60](#)
 detención de procesos de servidor [59](#)
 establecer permisos de archivo [59](#)
 establecimiento de las variables de entorno [59](#)
Uso de CPU
 mejora [49](#)
uso de memoria
 mejora [49](#)
Uso de red
 mejora [49](#)

usuarios finales

- acceso a un archivo de datos [45](#)
- ID de usuario y contraseña [44](#)
- lista de lo que necesitan saber [23](#)
- nombre de dominio [44](#)
- Nombre de la computadora [44](#)
- número de puerto [44](#)
- Orígenes de datos ODBC [45](#)
- soporte [23](#)

utilización de disco

- mejora [48](#)

V

- ver datos [15](#)
- versiones [32](#)
- vista de datos [15](#)

W

Windows

- cambiar parámetros de inicio de servicio [56](#)
- comprobación de procesos de servidor [56](#)
- comprobación del estado del servicio [56](#)
- creación y configuración de orígenes de datos ODBC [56](#)
- crear cuentas de usuario final [56](#)
- crear variables de entorno [55](#)
- establecer permisos de archivo [55](#)
- iniciar y detener servicios [56](#)

X

xtensiones

- configurar [17](#)

