IBM SPSS Analytic Server
Versión 3.2.1

Guía de instalación y configuración

Nota
Antes de utilizar esta información y el producto al que da soporte, lea la información del apartado "Avisos" en la página 73.

Información sobre el producto

Esta edición se aplica a la versión 3, release 2, modificación 1 de IBM SPSS Analytic Server y a todos los releases y modificaciones posteriores hasta que se indique lo contrario en nuevas ediciones.

Contenido

Capítulo 1. Requisitos previos

Antes de instalar Analytic Server, revise la información siguiente.

Requisitos del sistema

Para obtener la información más actualizada sobre los requisitos del sistema, utilice los informes detallados de requisitos del sistema en el sitio de soporte técnico de IBM: http://publib.boulder.ibm.com/infocenter/prodguid/v1r0/clarity/softwareReqsForProduct.html. En esta página:

1. Especifique SPSS Analytic Server como nombre de producto y pulse **Search**.
2. Seleccione la versión deseada y el ámbito del informe y, a continuación, haga clic en **Submit**.

Tráfico de WebSocket

Debe asegurarse de que el tráfico de WebSocket entre los clientes y el Analytic Server no esté bloqueado por cortafuegos, VPN u otros métodos de bloqueo de puertos. El puerto de WebSocket es el mismo que el puerto general de Analytic Server.

SuSE Linux (SLES) 12

Realice las tareas siguientes antes de instalar Analytic Server en SuSE Linux 12:

1. Descargue una clave pública en el host desde el URL siguiente:

   ```
   https://ibm-open-platform.ibm.com/repos/IBM-SPSS-AnalyticServer/3.2.1.0/IBM-SPSS-ANALYTICSERVER-GPG-KEY.public
   ```

2. Importe la clave pública ejecutando el mandato siguiente en el host:

   ```
   rpm --import IBM-SPSS-ANALYTICSERVER-GPG-KEY.public
   ```

Sistemas de alimentación

Asegúrese de que los compiladores IBM XLC y XLF están instalador e incluidos en la PATH en todos los hosts del clúster.

Puede encontrar más información sobre cómo obtener una licencia para estos compiladores en los sitios web siguientes:

- XL C para Linux: http://www-03.ibm.com/software/products/en/xlcpp-linux
- XL Fortran para Linux: http://www-03.ibm.com/software/products/en/xlfortran-linux

Hortonworks Data Platform (HDP)

Antes de instalar Analytic Server, debe asegurarse de que se ha desplegado como mínimo un cliente HDP en el entorno en clúster. Dado que el nodo que aloja Ambari Manager espera el directorio `/usr/hdp`, Analytic Server fallará en ausencia de un cliente HDP.

Hive/HCatalog

Si tiene previsto utilizar los orígenes de datos NoSQL, configure Hive y HCatalog para el acceso remoto. Asegúrese también de que `hive-site.xml` contiene una propiedad *hive.metastore.uris* de la forma `thrift://<nombre_host>:<puerto>` que señala al servidor Thrift Hive Metastore activo. Consulte la documentación de distribución de Hadoop para obtener detalles.

Nota: Analytic Server Metastore no se puede instalar en la misma máquina que Hive Metastore.

Si desea utilizar Hive 2.1, debe habilitar Hive 2.1 habilitando el valor **Consulta interactiva** en la consola de Ambari y, a continuación, entre `2.x` como propiedad `hive.version` durante la instalación de Analytic Server.

1. Abra la consola Ambari y añada la siguiente propiedad en la sección **Analytic Server Advanced analytics.cfg**.
   - Clave: `hive.version`
   - Valor: Entre la versión de Hive adecuada (por ejemplo, 2.x)
2. Guarde la configuración.

Nota: Hive 2.1 está soportado en HDP 2.5 y posteriores con Spark 2.x.

Repositorio de metadatos

De forma predeterminada, Analytic Server instala y utiliza una base de datos MySQL. De forma alternativa, puede configurar Analytic Server para que utilice una instalación existente de Db2. Independientemente del tipo de base de datos que elija, debe tener una codificación de UTF-8.

MySQL

El conjunto de caracteres predeterminado para MySQL depende de la versión y del sistema operativo. Utilice los pasos siguientes para determinar si la instalación de MySQL está establecida en UTF-8.

1. Determine la versión de MySQL.

   ```
   mysql -V
   ```

2. Determine el conjunto de caracteres predeterminado para MySQL ejecutando la consulta siguiente desde la interfaz de línea de mandatos de MySQL.

   ```
   mysql>show variables like 'char%';
   ```

   Si los conjuntos de caracteres ya están establecidos en UTF-8, no es necesario ningún cambio adicional.

3. Determine la ordenación predeterminada para MySQL ejecutando la consulta siguiente desde la interfaz de línea de mandatos de MySQL.

   ```
   mysql>show variables like 'coll%';
   ```

   Si la ordenación ya está establecida en UTF-8, no es necesario ningún cambio adicional.

4. Si el conjunto de caracteres o la ordenación predeterminados no es UTF-8, consulte la documentación de MySQL para ver detalles sobre cómo editar /etc/my.cnf y reinicie el daemon de MySQL para cambiar el conjunto de caracteres a UTF-8.

Db2 Para obtener más información sobre cómo configurar Db2, consulte el Knowledge Center http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.kc.doc/welcome.html.

Clústeres de alta disponibilidad

Equilibrador de carga

El clúster de alta disponibilidad debe tener un equilibrador de carga que dé soporte a la afinidad de sesiones, a veces también conocida como sesiones permanentes. Analytic Server identifica las sesiones con la cookie "request-token". Ésta identifica una sesión durante la duración de un inicio de sesión del usuario para su uso en la afinidad de sesiones controlada por aplicación. Consulte la documentación de su equilibrador de carga para conocer los detalles de soporte a la afinidad de sesiones.

Anomalía de trabajo de Analytic Server

Cuando un trabajo de Analytic Server falla porque falla un miembro de clúster, el trabajo se suele reiniciar automáticamente en otro miembro de clúster. Si el trabajo no se reanuda, compruebe para asegurarse de que haya al menos 4 miembros de clúster en el clúster de alta disponibilidad.

Capítulo 2. Instalación y configuración de Ambari

Requisitos previos específicos de Ambari

Además de los requisitos previos generales, revise la información siguiente.

Servicios

Analytic Server está instalado como un servicio Ambari. Antes de instalar Analytic Server, asegúrese de que los clientes están instalados como servicios de Ambari:

- HDFS/HDFS_CLIENT
- MAPREDUCE2/MAPREDUCE2_CLIENT
- HIVE/HIVE_CLIENT
- SPARK/SPARK_CLIENT (cuando se utiliza Spark 1.x)
- SPARK2/SPARK2_CLIENT (cuando se utiliza Spark 2.x)
- HBASE/HBASE_CLIENT (cuando se utiliza HBASE)
- YARN
- Zookeeper

SSH sin contraseña

Configure SSH sin contraseña para el usuario root entre el host de Analytic Metastore y todos los hosts del clúster.

Herramientas de comprobación previa y posterior a la instalación - Ambari

Visión general de la herramienta de comprobación previa

La herramienta de comprobación previa de Analytic Server le ayuda a reducir las incidencias y errores de ejecución de la instalación identificando los posibles problemas del entorno antes de la instalación de Analytic Server.

La herramienta de comprobación previa verifica:

- Las versiones del sistema operativo y de Ambari en el sistema local
- Los valores ulimit del sistema operativo en el sistema local
- El espacio de disco disponible en el sistema local
- La versión de Hadoop
- La disponibilidad del servicio de Ambari (HDFS, HCatalog, Spark, Hive, MapReduce, Yarn, Zookeeper, etc.)
- Valores Ambari específicos de Analytic Server

Nota: La herramienta de comprobación previa se puede utilizar después de ejecutar el archivo binario de Analytic Server autoextraíble.

Visión general de la herramienta de comprobación posterior

La herramienta de comprobación posterior de Analytic Server identifica los problemas de configuración que aparecen después de la instalación de Analytic Server, enviando solicitudes de API REST para procesar:

- Datos en HDFS
- Datos en Hive/HCatalog

- Datos comprimidos (incluyendo deflate, bz2, snappy)
- Datos con PySpark
- Datos que utilizan componentes SPSS nativos (incluyendo alm, tree, neuralnet, scoring, tascoring)
- Datos con MapReduce
- Datos con MapReduce en memoria

Ubicación y requisitos previos de la herramienta

Antes de instalar el servicio Analytic Server, ejecute la herramienta de comprobación previa en todos los nodos que forman parte del servicio Analytic Server para verificar que su entorno Linux ya está instalado Analytic Server.

La herramienta de comprobación previa se invoca automáticamente como parte de la instalación. La herramienta realiza una comprobación en Analytic Metastore y en todos los nodos de Analytic Server antes de ejecutar la instalación en cada host. También puede invocar manualmente la herramienta de comprobación previa en el nodo del servidor Ambari, que validará la máquina antes de instalar el servicio.

Después de ejecutar el archivo binario de Analytic Server autoextraíble, la herramienta de comprobación previa se encuentra en los directorios siguientes:

- **HDP**

```
/opt/ibm/spss/analyticserver-ambari/3.2/ANALYTICSERVER/package/chktool/precheck.py

[root@servername chktool]# cd /opt/ibm/spss/analyticserver-ambari/3.2/ANALYTICSERVER/package/chktool
[root@servername chktool]# ls
checkers data lib logs postcheck.py precheck.py readme.txt
```

Después de instalar Analytic Server, la herramienta de comprobación posterior se encuentra en el siguiente directorio:

- **HDP**

```
/opt/ibm/spss/analyticserver/3.2/tools/com.spss.ibm.checker.zip
```

Las herramientas deben ejecutarse como root y requieren Python 2.6.X (o superior).

Si la herramienta de comprobación previa informa de alguna anomalía, ésta debe abordarse antes de continuar con la instalación de Analytic Server.

El directorio `chktool` está disponible después de ejecutar el binario autoextraíble de Analytic Server (paso 2 de la sección "Instalación en Ambari" en la página 6). Si elige ejecutar una "Instalación fuera de línea" en la página 10, el directorio `chktool` está disponible después de instalar el RPM de metadatos.

Ejecución de la herramienta de comprobación previa

Automático

La herramienta de comprobación previa puede invocarse automáticamente como parte de la instalación de Analytic Server cuando Analytic Server se ha instalado como servicio mediante la consola de Ambari. Deberá especificar manualmente el nombre de usuario y la contraseña del servidor Ambari.

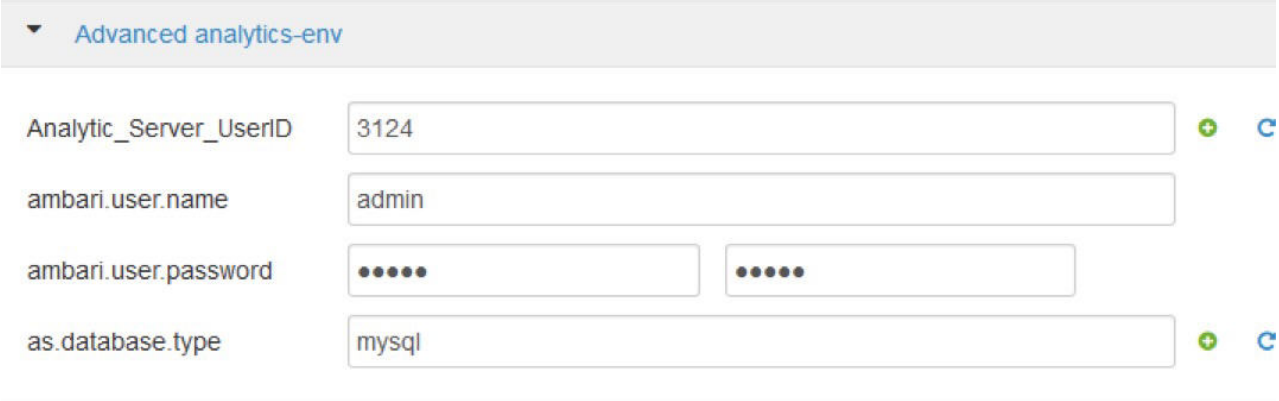

Figura 1. Configuración de Advanced analytics-env

Manual

Puede invocar manualmente la herramienta de comprobación previa en el nodo del servidor de Ambari.

El ejemplo siguiente de comprobación previa verifica el clúster `MyCluster` de Ambari que se ejecuta en `myambarihost.ibm.com:8080`, con SSL habilitado, y utiliza las credenciales de inicio de sesión: `admin:admin`

```
python ./precheck.py --target B --cluster MyCluster --username admin
--password admin --host myambarihost.ibm.com --port 8080 --as_host myashost.ibm.com --ssl
```

Notas:

- El valor `as_host` debe proporcionarse mediante la dirección IP o un nombre de dominio completo.
- La herramienta solicita una contraseña cuando se omite el argumento de contraseña.
- El mandato `precheck.py` incluye ayuda para su utilización, que se muestra con el argumento `--h` (`python ./precheck.py --help`).
- El argumento `--cluster` es opcional (el clúster actual se identifica cuando `--cluster` no se utiliza).

A medida que la herramienta de comprobación previa ejecuta sus comprobaciones, se muestra el estado de cada comprobación en la ventana de mandatos. Cuando se produce un error, encontrará información detallada en el archivo de registro (la ubicación exacta del archivo de registro se proporciona en la ventana de mandatos). El archivo de registro puede proporcionarse al servicio de soporte técnico de IBM cuando se necesita ayuda adicional.

Ejecución de la herramienta de comprobación posterior

La herramienta de comprobación posterior verifica que Analytic Server se está ejecutando correctamente y puede procesar trabajos simples. El ejemplo de comprobación posterior siguiente comprueba una instancia de Analytic Server que se ejecuta en `myanalyticserverhost.ibm.com:9443`, con SSL habilitado, y utiliza las credenciales de inicio de sesión: `admin:ibmspss`

```
python ./postcheck.py --host myanalyticserverhost.ibm.com --port 9443
--username admin --password ibmspss --ssl
```

Cuando se utiliza Knox con Analytic Server, el mandato es el siguiente:

```
python ./postcheck.py --host myknoxserverhost.ibm.com --port 8443
--username admin --password ibmspss --ssl --gateway_url /gateway/default
```

Para realizar una sola comprobación, utilice el mandato siguiente:

```
python ./postcheck.py --host myknoxserverhost.ibm.com --port 8443
--username admin --password ibmspss --ssl --gateway_url /gateway/default --check AS_PYSPARK_BUILDMODEL
```

Notas:

- La herramienta solicita una contraseña cuando se omite el argumento de contraseña.
- El mandato `postcheck.py` incluye ayuda para su utilización, que se muestra con el argumento `--h` (`python ./postcheck.py --help`).

A medida que la herramienta de comprobación posterior ejecuta sus comprobaciones, se muestra el estado de cada comprobación en la ventana de mandatos. Cuando se produce un error, encontrará información detallada en el archivo de registro (la ubicación exacta del archivo de registro se proporciona en la ventana de mandatos). El archivo de registro puede proporcionarse al servicio de soporte técnico de IBM si se necesita ayuda adicional.

Instalación en Ambari

El proceso básico es instalar los archivos de Analytic Server en un host que esté dentro del clúster Ambari y, a continuación, añadir Analytic Server como un servicio Ambari.

"Instalación en línea"
Elija la instalación en línea si el host del servidor Ambari y todos los nodos del clúster pueden acceder a https://ibm-open-platform.ibm.com.

"Instalación fuera de línea" en la página 10
Elija fuera de línea si el host del servidor Ambari no tiene acceso a Internet.

Instalación en línea

Elija la instalación en línea si el host del servidor Ambari y todos los nodos del clúster pueden acceder a https://ibm-open-platform.ibm.com.

1. Vaya al Sitio web de IBM Passport Advantage® y descargue el archivo binario autoextraíble específico de la pila, la versión de pila y la arquitectura de hardware en el nodo de Ambari Manager. Los binarios de Ambari disponibles son:

Tabla 1. Archivos binarios autoextraíbles de Analytic Server

Descripción	Nombre del archivo binario
IBM® SPSS Analytic Server 3.2.1 para Hortonworks Data Platform 2.5, 2.6, 3.0 y 3.1, Linux x86-64, inglés	`spss_as-3.2.1.0-hdp2.5-3.1-lx86.bin`
IBM SPSS Analytic Server 3.2.1 para Hortonworks Data Platform 2.6, 3.0 y 3.1, Linux en System p LE, inglés	`spss_as-3.2.1.0-hdp2.6-3.1-lppc64.bin`

2. Ejecute el archivo binario autoextraíble y siga las instrucciones para ver la licencia, acepte la licencia, elija la instalación en línea y seleccione el proceso de instalación para el tipo de base de datos que utiliza Analytic Server. Se le proporcionan las opciones de tipo de base de datos siguientes:
   - Instancia nueva de MySQL
   - Instancia de MySQL o Db2 preexistente
3. Desde el directorio `/var/lib/ambari-server/resources/stacks/<stack-name>/<stack-version>/services/ANALYTICSERVER/package/scripts`, ejecute el script `update_clientdeps.sh` con los argumentos adecuados (utilice el argumento `--help` para obtener ejemplos).
4. Reinicie el servidor Ambari.

   ```
   ambari-server restart
   ```

5. Inicie la sesión en el servidor Ambari e instale Analytic Server como un servicio mediante la interfaz de usuario de Ambari.

   Repositorio de metadatos

   Analytic Server utiliza MySQL de forma predeterminada para realizar el seguimiento de la información sobre orígenes de datos, proyectos e inquilinos. Durante la instalación, deberá proporcionar un nombre de usuario (**`metadata.repository.user.name`**) y la contraseña **`metadata.repository.password`** utilizados en la conexión JDBC entre Analytic Server y

MySQL. El instalador crea el usuario en la base de datos MySQL, pero dicho usuario es específico de la base de datos MySQL, y no es necesario que sea un usuario existente de Linux o Hadoop.

Nota: Si desea instalar una instancia nueva de MySQL durante la instalación, debe instalar el metastore de Analytic Server en una máquina en la que MySQL no esté instalado.

Para cambiar el repositorio de metadatos a Db2, siga estos pasos.

Nota: No puede cambiar el repositorio de metadatos una vez completada la instalación.

a. Asegúrese de que Db2 está instalado en otra máquina. Para obtener más información, consulte la sección de repositorio de metadatos del tema Capítulo 1, "Requisitos previos", en la página 1.
b. En la pestaña Ambari Services, vaya hasta la pestaña Configs del servicio Analytic Server.
c. Abra la sección **Advanced analytics-env**.
d. Cambie el valor de **as.database.type** de `mysql` por `db2`.
e. Abra la sección **Advanced analytics-meta**.
f. Cambie el valor `com.mysql.jdbc.Driver` de **metadata.repository.driver** por `com.ibm.db2.jcc.DB2Driver`.
g. Cambie el valor de **metadata.repository.url** por `jdbc:db2://{Db2_HOST}:{PORT}/{DBName}:currentSchema={SchemaName};`, donde
   - {Db2_HOST} es el nombre de host del servidor donde está instalado Db2
   - {PUERTO} es el puerto en el que Db2 escucha
   - {Nombre_esquema} es un esquema disponible, no utilizado.

   Si no está seguro de qué valores especificar, consulte al administrador de Db2.
h. Proporcione unas credenciales de Db2 válidas en **metadata.repository.user.name** y **metadata.repository.password**.
i. Pulse **Guardar**.

Configuración de LDAP

Analytic Server utiliza un servidor LDAP para almacenar y autenticar usuarios y grupos. Proporcione la información de configuración de LDAP necesaria durante la instalación de Analytic Server.

Tabla 2. Valores de configuración de LDAP

Valor de LDAP	Descripción
`as.ldap.type`	Tipo de LDAP. El valor puede ser `ads`, `ad` u `openladp`. • `ads` - Apache Directory Server (valor predeterminado) • `ad` - Microsoft Active Directory • `openladp` - OpenLDAP
`as.ldap.host`	Host LDAP
`as.ldap.port`	Número de puerto LDAP
`as.ldap.binddn`	DN de enlace de LDAP
`as.ldap.bindpassword`	Contraseña de DN de enlace de LDAP
`as.ldap.basedn`	DN base LDAP
`as.ldap.filter`	Regla de filtro de usuario y grupo de LDAP
`as.ldap.ssl.enabled`	Especifica si se debe utilizar SSL para comunicarse entre Analytic Server y LDAP. El valor puede ser `true` o `false`.
`as.ldap.ssl.reference`	ID de referencia SSL de LDAP

Tabla 2. Valores de configuración de LDAP (continuación)

Valor de LDAP	Descripción
as.ldap.ssl.content	Configuración SSL de LDAP

- De forma predeterminada, as.ldap.type se establece en ads y los otros valores relacionados contienen valores predeterminados. La excepción es que debe proporcionar una contraseña para el valor as.ldap.bindpassword. Analytic Server utiliza los valores de configuración para instalar un servidor de Apache Directory Server (ADS) y ejecutar la inicialización del servidor. El perfil de ADS predeterminado incluye el usuario admin con una contraseña de admin. Puede llevar a cabo la gestión de usuarios a través de la consola de Analytic Server o importar la información de usuarios y de grupos desde un archivo XML mediante el script importUser.sh que se encuentra en la carpeta <Analytic Root>/bin.
- Si tiene previsto utilizar un servidor LDAP externo, como por ejemplo Microsoft Active Directory u OpenLDAP, debe definir los valores de configuración según los valores de LDAP reales. Para obtener más información, consulte Configuración de registros de usuarios de LDAP en Liberty.
- Puede cambiar la configuración de LDAP después de que se haya instalado Analytic Server (por ejemplo, cambiar de Apache Directory Server a OpenLDAP). Sin embargo, si inicialmente se empieza con Microsoft Active Directory u OpenLDAP, y decide cambiar posteriormente a Apache Directory Server, Analytic Server no instalará un servidor de Apache Directory Server durante la instalación. Apache Directory Server solo se instala cuando se selecciona durante la instalación inicial de Analytic Server.

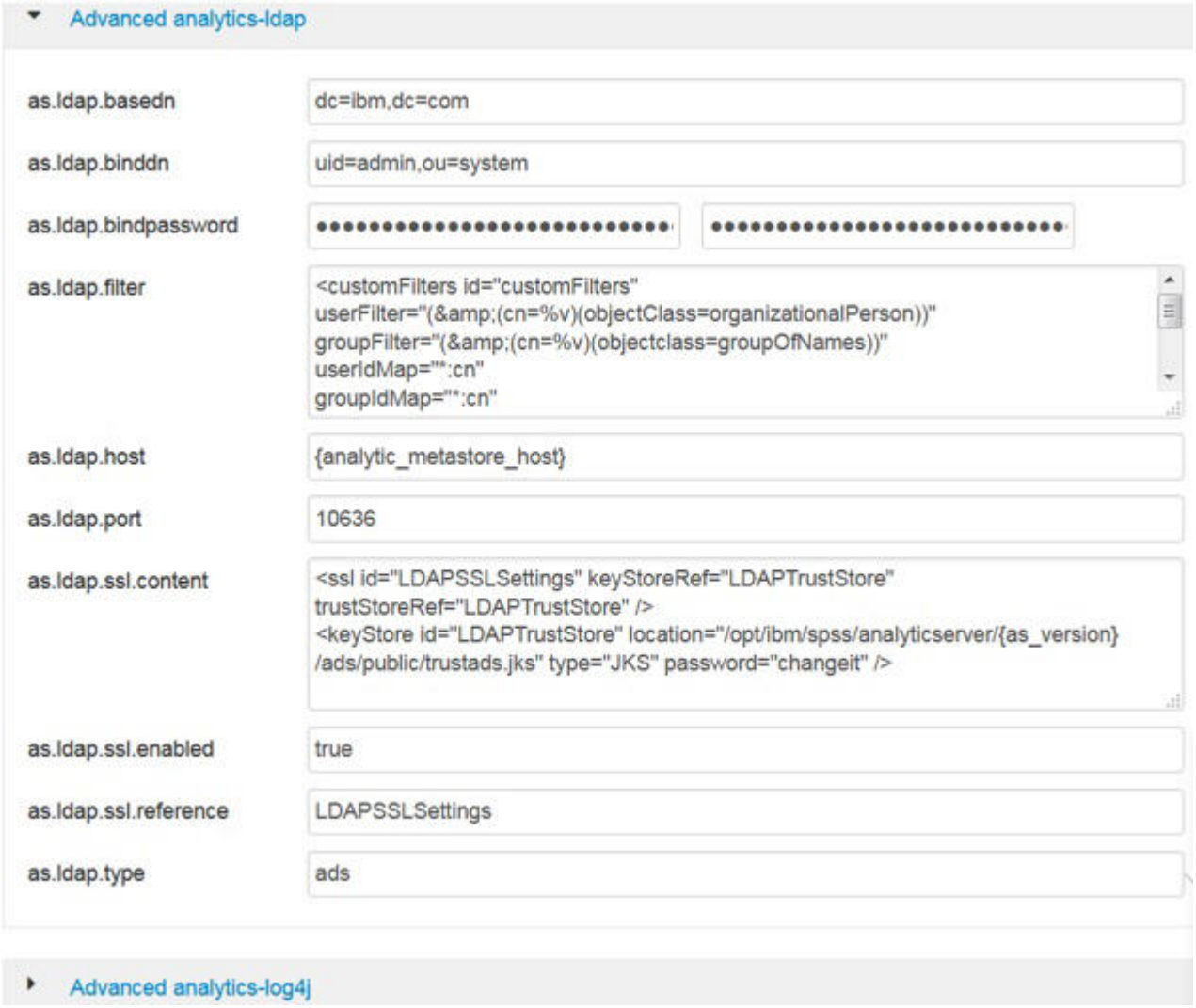

Figura 2. Valores de configuración de LDAP de ejemplo

Los valores de configuración que no se deben modificar tras la instalación.

No cambie los valores siguientes tras la instalación, o Analytic Server no funcionará.

- Analytic_Server_User
- Analytic_Server_UserID
- as.database.type
- metadata.repository.driver
- distrib.fs.root

6. Ahora tiene una instancia en funcionamiento de Analytic Server. Es opcional realizar una configuración adicional. Para obtener más información sobre una cómo configurar y administrar Analytic Server, consulte el tema: “Configuración” en la página 15. Para obtener información sobre la migración de una configuración existente a una nueva instalación, consulte el tema: “Migración de IBM SPSS Analytic Server en Ambari” en la página 33.
7. Abra un navegador web y especifique la dirección `http://<host>:<puerto>/analyticserver/admin/ibm`, donde <host> es la dirección del host de Analytic Server y <puerto> es el puerto en que Analytic Server escucha. De forma predeterminada, este valor es 9080. Este URL abre el diálogo de inicio de sesión de la consola de Analytic Server. Inicie la sesión como administrador de Analytic Server. De forma predeterminada este ID de usuario es admin y la contraseña es admin.

Instalación fuera de línea

Una instalación fuera de línea de IBM SPSS Analytic Server se puede realizar de forma automática o manual.

"Instalación automática en HDP"

El proceso de instalación automática utiliza la API REST de Ambari, y es el método preferido para

la instalación.

"Instalación manual en HDP (RHEL, SLES)" en la página 11
Para la instalación manual de Analytic Server en Hortonworks Data Platform

"Instalación manual en HDP (Ubuntu)" en la página 13
Para la instalación manual de Analytic Server en Ubuntu Linux.

Instalación automática en HDP

El proceso de instalación automática utiliza la API REST de Ambari, y es el método preferido para la instalación.

Importante:

- El procedimiento de instalación automática fuera de línea instala un Apache Directory Server (ADS) incorporado. Si desea utilizar un servidor LDAP de terceros, puede configurar los valores de LDAP después de que se haya completado la instalación de IBM SPSS Analytic Server.
- El procedimiento de instalación automática fuera de línea solo puede instalar una única instancia de servicio de Analytic Server. Puede añadir más instancias después de que se haya completado la instalación inicial.
- El procedimiento de instalación automática fuera de línea no da soporte a la instalación de Analytic Server en un clúster habilitado para Kerberos.
- El procedimiento de instalación automática fuera de línea no da soporte a la instalación de Analytic Server en HDP 3.0 o 3.1.

Estas limitaciones no se aplican a las instalaciones manuales de HDP ni de Ubuntu.

1. Vaya al Sitio web de IBM Passport Advantage® y descargue el archivo binario autoextraíble en un sistema que pueda acceder a https://ibm-open-platform.ibm.com.

Tabla 3. Archivo binario autoextraíble de Analytic Server

Descripción	Nombre del archivo binario
IBM SPSS Analytic Server 3.2.1 para Hortonworks Data Platform 2.5, 2.6, 3.0 y 3.1, Linux x86-64, inglés	`spss_as-3.2.1.0-hdp2.5-3.1-lx86.bin`
IBM SPSS Analytic Server 3.2.1 para Hortonworks Data Platform 2.6, 3.0 y 3.1, Linux en System p LE, inglés	`spss_as-3.2.1.0-hdp2.6-3.1-lppc64.bin`

2. Ejecute el binario ejecutable que ha descargado en el paso 1 y especifique una instalación fuera de línea. Una instalación fuera de línea descarga los archivos RPM o DEB que se necesitan más adelante en el proceso de instalación, y se debe ejecutar en un sistema que pueda acceder a https://ibm-open-platform.ibm.com. Los archivos descargados se encuentran en el directorio binario ejecutable actual `./IBM-SPSS-AnalyticServer`.
3. Copie todo el contenido del directorio ejecutable `./IBM-SPSS-AnalyticServer` desde la máquina con acceso a Internet al nodo de Ambari Manager (situado detrás del cortafuegos).
4. En el nodo de Ambari Manager, utilice el siguiente mandato para verificar si el servidor Ambari está en ejecución:

   ```
   ambari-server status
   ```

5. En el nodo Ambari Manager, y en todos los demás nodos en los que desea desplegar Analytic Server, instale la herramienta que crea un repositorio `yum` local.

`yum install createrepo (RHEL, CentOS)`

o bien

`apt-get install dpkg-dev (Ubuntu)`

6. En el nodo de Ambari Manager, ejecute el archivo binario ejecutable `./IBM-SPSS-AnalyticServer/packages/spss_as-ambari-offlineinstall.bin`. Durante la instalación, el binario ejecutable verifica que los archivos de Analytic Server RPM/DEB necesarios se encuentren en el directorio de paquetes. Los archivos de RPM que necesita dependen de la distribución, la versión y la arquitectura.

   HDP 2.5, 2.6, 3.0 y 3.1 (x86_64)
   IBM-SPSS-AnalyticServer-ambari-2.x-3.2.1.0-1.noarch.rpm

   IBM-SPSS-AnalyticServer-3.2.1.0-1.x86_64.rpm

   HDP 2.6, 3.0 y 3.1 (PPC64LE)
   IBM-SPSS-AnalyticServer-ambari-2.x-3.2.1.0-1.noarch.rpm

   IBM-SPSS-AnalyticServer-3.2.1.0-1.ppc64le.rpm

   HDP 2.5, 2.6, 3.0 y 3.1 (Ubuntu)
   IBM-SPSS-AnalyticServer-ambari-2.x_3.2.1.0_amd64.deb

   IBM-SPSS-AnalyticServer_1_amd64.deb

Durante la instalación, se le solicita entrar la versión de Analytic Server, el controlador JDBC, la versión de Spark, la versión de Hive, etc.

Instalación manual en HDP (RHEL, SLES)

El flujo de trabajo general para una instalación fuera de línea manual en HDP (RHEL, SLES) es el siguiente:

1. Vaya al Sitio web de IBM Passport Advantage® y descargue el archivo binario autoextraíble en un sistema que pueda acceder a https://ibm-open-platform.ibm.com.

Tabla 4. Archivos binarios autoextraíbles de Analytic Server

Descripción	Nombre del archivo binario
IBM SPSS Analytic Server 3.2.1 para Hortonworks Data Platform 2.5, 2.6, 3.0 y 3.1, Linux x86-64, inglés	`spss_as-3.2.1.0-hdp2.5-3.1-lx86.bin`
IBM SPSS Analytic Server 3.2.1 para Hortonworks Data Platform 2.6, 3.0 y 3.1, Linux en System p LE, inglés	`spss_as-3.2.1.0-hdp2.6-3.1-lppc64.bin`

2. Ejecute el binario ejecutable que ha descargado en el paso 1 y especifique una instalación fuera de línea. Una instalación fuera de línea descarga los archivos RPM que se necesitan más adelante en el proceso de instalación, y se debe ejecutar en un sistema que pueda acceder a https://ibm-open-platform.ibm.com. Los archivos descargados se encuentran en el directorio binario ejecutable actual `./IBM-SPSS-AnalyticServer`.
3. Copie todo el contenido del directorio binario ejecutable `./IBM-SPSS-AnalyticServer` desde la máquina con acceso a Internet al directorio `<AS_INSTALLABLE_HOME>` del nodo de Ambari Manager (el nodo de Ambari Manager se encuentra detrás del cortafuegos).
4. En el nodo de Ambari Manager, utilice el siguiente mandato para verificar si el servidor Ambari está en ejecución:

   `ambari-server status`
5. Instale la herramienta que crea un repositorio `yum` local.

   `yum install createrepo (RHEL, CentOS)`

   o bien

   `zypper install createrepo (SLES)`
6. Cree un directorio que sirva como repositorio para los archivos de RPM de Analytic Server. Consulte el ejemplo siguiente.

```
mkdir /home/root/repos/IBM-SPSS-AnalyticServer/x86_64
```

7. Copie los archivos de RPM necesarios de Analytic Server en el nuevo directorio. Los archivos de RPM que necesita dependen de la distribución, la versión y la arquitectura.

   HDP 2.5, 2.6, 3.0 y 3.1 (x86_64)

   IBM-SPSS-AnalyticServer-ambari-2.x-3.2.1.0-1.noarch.rpm

   IBM-SPSS-AnalyticServer-3.2.1.0-1.x86_64.rpm

   HDP 2.6, 3.0 y 3.1 (PPC64LE)

   IBM-SPSS-AnalyticServer-ambari-2.x-3.2.1.0-1.noarch.rpm

   IBM-SPSS-AnalyticServer-3.2.1.0-1.ppc64le.rpm

8. Cree la definición del repositorio local. Por ejemplo, cree un archivo denominado `IBM-SPSS-AnalyticServer-3.2.1.0.repo` en `/etc/yum.repos.d/` (para RHEL, CentOS) o `/etc/zypp/repos.d/` (para SLES) con el contenido siguiente.

```
[IBM-SPSS-AnalyticServer]
name=IBM-SPSS-AnalyticServer
baseurl=file:///{vía_acceso al repositorio local}
enabled=1
gpgcheck=0
protect=1
```

9. Cree el repositorio local `yum`.

```
createrepo /home/root/repos/IBM-SPSS-AnalyticServer/x86_64 (RHEL, CentOS, SLES)
```

10. En una ventana de mandatos de usuario root, realice `cd` en el directorio `<AS_INSTALLABLE_HOME>/IBM-SPSS-AnalyticServer` y `run ./offLineInstall.sh`. El script lee las respuestas persistentes al mandato de instalación ejecutable binario que se ha ejecutado previamente y emite el mandato plataforma adecuado (para instalar el rpm).

    Nota: El paso 11 solo se aplica si se utiliza un entorno MySQL gestionado de forma externa.

11. Ejecute el script `add_mysql_user.sh` en el nodo/host donde está instalada la instancia de MySQL que se utilizará como `AS_MetaStore`.

    a. Copie el script `add_mysql_user.sh` de `<AS_INSTALLABLE_HOME>/IBM-SPSS-AnalyticServer` en el nodo/host donde está instalada la instancia de MySQL que se utilizará como `AS_MetaStore`.

       - Ejecute el script `add_mysql_user.sh` en el nodo/host MySQL. Por ejemplo, `./add_mysql_user.sh -u as_user -p spss -d aedb`

       Notas:

       - El nombre de usuario y la contraseña deben coincidir con el nombre de usuario y la contraseña de la base de datos que se introdujo para `AS_Metastore` en la pantalla de configuración Ambari.
       - El script `add_mysql_user.sh` se puede actualizar manualmente para emitir mandatos (si lo desea).
       - Al ejecutar el script `add_mysql_user.sh` en una base de datos MySQL (acceso de usuario root), utilice los parámetros `-r` y `-t` para pasar `dbuserid` y `dbuserid_password`. El script utiliza `dbuserid` y `dbuserid_password` para realizar operaciones MySQL.

    Nota: El valor `metadata.repository.url` en la pantalla **AS_Configuration** (**Advanced analytics-meta**) se debe modificar para que apunte al host de base de datos de MySQL. Por ejemplo, cambie el valor JDBC `mysql://{analytic_metastore_host}/aedb?createDatabaseIfNotExist=true` en `mysql://{MySQL_DB}/aedb?createDatabaseIfNotExist=true`

12. Actualice el archivo de repositorio de Ambari `repoinfo.xml`, normalmente, se encuentra en `/var/lib/ambari-server/resources/stacks/$stackName/$stackVersion/repos/`, para utilizar el repositorio `yum` local, añadiendo las líneas siguientes.

```
<os type="host_os">
   <repo>
        <baseurl>file:///{vía de acceso al repositorio local}/</baseurl>
```

```
        <repoid>IBM-SPSS-AnalyticServer</repoid>
        <reponame>IBM-SPSS-AnalyticServer-3.2.1.0</reponame>
    </repo>
</os>
```

Este sería un posible ejemplo {vía_acceso al repositorio local}:

```
/home/root/repos/IBM-SPSS-AnalyticServer/x86_64/
```

13. Repita los pasos siguientes para cada nodo de clúster no servidor de Ambari.
    a. Copie todo el contenido del directorio <AS_INSTALLABLE_HOME> adecuado de la máquina con acceso a Internet al nodo de clúster no servidor de Ambari.
    b. Instale la herramienta que crea un repositorio yum local.

       ```
       yum install createrepo (RHEL, CentOS)
       ```

       o bien

       ```
       zypper install createrepo (SLES)
       ```

    c. Cree un directorio que sirva como repositorio para los archivos de RPM de Analytic Server. Consulte el ejemplo siguiente.

       ```
       mkdir /home/root/repos/IBM-SPSS-AnalyticServer/x86_64
       ```

    d. Copie los archivos de RPM necesarios de Analytic Server en el nuevo directorio. Los archivos de RPM que necesita dependen de la distribución, la versión y la arquitectura.

       HDP 2.5, 2.6, 3.0 y 3.1 (x86_64)

       IBM-SPSS-AnalyticServer-ambari-2.x-3.2.1.0-1.noarch.rpm

       IBM-SPSS-AnalyticServer-3.2.1.0-1.x86_64.rpm

       HDP 2.6, 3.0 y 3.1 (PPC64LE)

       IBM-SPSS-AnalyticServer-ambari-2.x-3.2.1.0-1.noarch.rpm

       IBM-SPSS-AnalyticServer-3.2.1.0-1.ppc64le.rpm

    e. Cree la definición del repositorio local. Por ejemplo, cree un archivo denominado IBM-SPSS-AnalyticServer-3.2.1.0.repo en /etc/yum.repos.d/ (para RHEL, CentOS) o /etc/zypp/repos.d/ (para SLES) con el contenido siguiente.

       ```
       [IBM-SPSS-AnalyticServer]
       name=IBM-SPSS-AnalyticServer
       baseurl=file:///{vía_acceso al repositorio local}
       enabled=1
       gpgcheck=0
       protect=1
       ```

    f. Cree el repositorio local yum.

       ```
       createrepo /home/root/repos/IBM-SPSS-AnalyticServer/x86_64 (RHEL, CentOS, SLES)
       ```

14. Continúe con el paso 3 en la sección "Instalación en línea" en la página 6.

Instalación manual en HDP (Ubuntu)

El flujo de trabajo general para una instalación fuera de línea manual en HDP (Ubuntu) es el siguiente:

1. Vaya al Sitio web de IBM Passport Advantage® y descargue el archivo binario autoextraíble de Ubuntu adecuado en un sistema que pueda acceder a https://ibm-open-platform.ibm.com.

Tabla 5. Archivos binarios autoextraíbles de Analytic Server

Descripción	Nombre del archivo binario
IBM SPSS Analytic Server 3.2.1 para Hortonworks Data Platform 2.5, 2.6, 3.0 y 3.1, Linux x86-64, inglés	spss_as-3.2.1.0-hdp2.5-3.1-lx86.bin

2. Ejecute el binario ejecutable que ha descargado en el paso 1 y especifique una instalación fuera de línea. Una instalación fuera de línea descarga los archivos DEB que se necesitan más adelante en el

proceso de instalación y se debe ejecutar en un sistema que pueda acceder a https://ibm-open-platform.ibm.com. Los archivos descargados se encuentran en el directorio binario ejecutable actual `./IBM-SPSS-AnalyticServer`.

3. Copie todo el contenido del directorio binario ejecutable `./IBM-SPSS-AnalyticServer` desde la máquina con acceso a Internet al directorio `<AS_INSTALLABLE_HOME>` del nodo de Ambari Manager (el nodo de Ambari Manager se encuentra detrás del cortafuegos).
4. En el nodo de Ambari Manager, utilice el siguiente mandato para verificar si el servidor Ambari está en ejecución:

   ```
   ambari-server status
   ```

5. Cree un directorio `<local_repo>` que sirva como repositorio para los archivos DEB de Analytic Server. Por ejemplo:

   ```
   mkdir –p /usr/local/mydebs
   ```

6. Copie los archivos DEB de Analytic Server necesarios en el directorio `<local_repo>`.
   - `IBM-SPSS-AnalyticServer-ambari-2.x_3.2.1.0_amd64.deb`
   - `IBM-SPSS-AnalyticServer_1_amd64.deb`
7. Cree el repositorio local.
   a. Instale la herramienta que crea un repositorio local:

      ```
      apt-get install dpkg-dev
      ```

   b. Genere el archivo de paquete de origen:

      ```
      cd <local_repo>
      dpkg-scanpackages . /dev/null | gzip -9c > Packages.gz
      ```

   c. Cree el componente (principal) y la arquitectura (por ejemplo, `binary-i386`, `binary-amd64`) de su repositorio local:

      ```
      mkdir -p <local_repo>/dists/IBM-SPSS-AnalyticServer/main/binary-amd64/
      mkdir -p <local_repo>/dists/IBM-SPSS-AnalyticServer/main/binary-i386/
      ```

   d. Copie el paquete de origen:

      ```
      cp -fr <local_repo>/Packages.gz <local_repo>/dists/IBM-SPSS-AnalyticServer/main/binary-amd64/Packages
      cp -fr <local_repo>/Packages.gz <local_repo>/dists/IBM-SPSS-AnalyticServer/main/binary-i386/Packages
      ```

8. Cree la definición del repositorio local. Por ejemplo, cree un archivo denominado `IBM-SPSS-AnalyticServer-3.2.1.0.list` en `/etc/apt/sources.list.d` con el contenido siguiente.

   ```
   deb file:/usr/local/mydebs ./
   ```

9. Ejecute el mandato siguiente para actualizar la lista de repositorios:

   ```
   apt-get update
   ```

10. Ejecute el mandato siguiente para instalar IBM SPSS Analytic Server 3.2.1:

    ```
    apt-get install ./IBM-SPSS-AnalyticServer-ambari-2.x
    ```

    Nota: Para verificar que el repositorio local se ha configurado correctamente, no ejecute el mandato anterior en el directorio `<local_repo>`. Si la instalación no puede encontrar el paquete, significa que el repositorio local no se ha configurado correctamente (en cuyo caso debe verificar todos los pasos anteriores).
11. Repita los pasos siguientes para cada nodo de clúster no servidor de Ambari.
    a. Cree un directorio `<local_repo>` que sirva como repositorio para los archivos DEB de Analytic Server. Por ejemplo:

       ```
       mkdir –p /usr/local/mydebs
       ```

    b. Copie todo el contenido del directorio `<local_repo>` de la máquina de nodo de Ambari Manager al directorio `<local_repo>` del nodo de clúster de Ambari que no es del servidor. El directorio debe contener los archivos siguientes:
       - `<local_repo>/IBM-SPSS-AnalyticServer-ambari-2.x_3.2.1.0_amd64.deb`
       - `<local_repo>/IBM-SPSS-AnalyticServer_1_amd64.deb`
       - `<local_repo>/Packages.gz`
       - `<local_repo>/dists/IBM-SPSS-AnalyticServer/main/binary-amd64/Packages`
       - `<local_repo>/dists/IBM-SPSS-AnalyticServer/main/binary-i386/Packages`

c. Cree la definición del repositorio local. Por ejemplo, cree un archivo denominado `IBM-SPSS-AnalyticServer-3.2.1.0.list` en `/etc/apt/sources.list.d` con el contenido siguiente.

```
deb file:/usr/local/mydebs ./
```

12. Continúe con el paso 3 en la sección "Instalación en línea" en la página 6.

Instalación de Analytic Server en un entorno MySQL gestionado externamente

El proceso de instalación de Analytic Server difiere de una instalación normal al instalarse en un entorno MySQL gestionado externamente.

Los pasos siguientes explican el proceso de instalar Analytic Server en un entorno MySQL gestionado externamente.

1. Navegue hasta el Sitio web de IBM Passport Advantage® y descargue el archivo binario autoextraíble específico de su pila, versión de pila y arquitectura de hardware en un sistema principal que se encuentre dentro del clúster Ambari.
2. Ejecute el archivo binario autoextraíble y siga las instrucciones para (opcionalmente) ver la licencia, aceptar la licencia.
   a. Elija la opción en línea.
   b. Seleccione la opción **Base de datos MySQL externa** cuando se le solicite.
3. Copie el script `add_mysql_user.sh` de `<AS_INSTALLABLE_HOME>/IBM-SPSS-AnalyticServer` en el nodo/host donde está instalada la instancia de MySQL que se utilizará como `AS_MetaStore`.
   - Ejecute el script `add_mysql_user.sh` en el nodo/host MySQL. Por ejemplo, `./add_mysql_user.sh -u as_user -p spss -d aedb`

   Notas:
   - El nombre de usuario y la contraseña deben coincidir con el nombre de usuario y la contraseña de la base de datos que se introdujo para `AS_Metastore` en la pantalla de configuración Ambari.
   - El script `add_mysql_user.sh` se puede actualizar manualmente para emitir mandatos (si lo desea).
   - Al ejecutar el script `add_mysql_user.sh` en una base de datos MySQL (acceso de usuario root), utilice los parámetros `-r` y `-t` para pasar `dbuserid` y `dbuserid_password`. El script utiliza `dbuserid` y `dbuserid_password` para realizar operaciones MySQL.
4. Reinicie el servidor Ambari.

   ```
   ambari-server restart
   ```
5. En la consola Ambari, añada el servicio `AnalyticServer` como normal (entre el mismo nombre de usuario y contraseña de base de datos que se introdujo en el paso 3).

   Nota: El valor `metadata.repository.url` en la pantalla **AS_Configuration** (**Advanced analytics-meta**) se debe modificar para que apunte al host de base de datos de MySQL. Por ejemplo, cambie el valor JDBC `mysql://{analytic_metastore_host}/aedb?createDatabaseIfNotExist=true` en `mysql://{MySQL_DB}/aedb?createDatabaseIfNotExist=true`

Configuración

Después de la instalación, si lo desea puede configurar y administrar Analytic Server a través de la interfaz de usuario Ambari.

Nota: Para las vías de acceso de archivo de Analytic Server se utilizan las convenciones siguientes.

- {RAÍZ_AS} hace referencia a la ubicación en la que se ha desplegado Analytic Server; por ejemplo, `/opt/IBM/SPSS/AnalyticServer/3.2`.
- {RAÍZ_SERVIDOR_AS} hace referencia a la ubicación de la configuración, al registro y a los archivos de servidor; por ejemplo, `/opt/IBM/SPSS/AnalyticServer/3.2/ae_wlpserver/usr/servers/aeserver`.

- {INICIO_AS} hace referencia a la ubicación de HDFS que utiliza Analytic Server como carpeta raíz.

Seguridad

Configuración de un registro de LDAP

El registro LDAP permite autenticar a los usuarios con un servidor LDAP externo como Active Directory u OpenLDAP.

Importante: Un usuario LDAP debe estar designado como administrador de Analytic Server en Ambari.

A continuación se muestra un ejemplo de ldapRegistry para OpenLDAP.

```
<ldapRegistry
    baseDN="ou=people,dc=aeldap,dc=org"
    ldapType="Custom"
    port="389"
    host="server"
    id="OpenLDAP"
    bindDN="cn=admin,dc=aeldap,dc=org"
    bindPassword="{xor}Dz4sLG5tbGs="
    searchTimeout="300000m"
    recursiveSearch="true">
    <customFilters
        id="customFilters"
        userFilter="(&amp;(uid=%v)(objectClass=inetOrgPerson))"
        groupFilter="(&amp;(cn=%v)(|(objectclass=organizationalUnit)))"
        groupMemberIdMap="posixGroup:memberUid"/>
</ldapRegistry>
```

El ejemplo siguiente proporciona autenticación de Analytic Server con Active Directory:

```
<ldapRegistry id="Microsoft Active Directory" realm="ibm"
  host="host"
  port="389"
  baseDN="cn=users,dc=adtest,dc=mycompany,dc=com"
  bindDN="cn=administrator,cn=users,dc=adtest,dc=mycompany,dc=com"
  bindPassword ="adminpassword"
  ldapType="Custom"
    <customFilters
    userFilter="(&amp;(sAMAccountName=%v)(objectcategory=user))"
    groupFilter="(&amp;(cn=%v)(objectcategory=group))"
    userIdMap="user:sAMAccountName"
    groupIdMap="*:cn"
    groupMemberIdMap="memberOf:member" />
</ldapRegistry>
```

Nota: A menudo es útil para utilizar una herramienta de terceros de visor LDAP para verificar la configuración LDAP.

El ejemplo siguiente proporciona autenticación de perfil de WebSphere Liberty con Active Directory:

```
<ldapRegistry id="ldap" realm="SampleLdapADRealm"
    host="ldapserver.mycity.mycompany.com" port="389" ignoreCase="true"
    baseDN="cn=users,dc=adtest,dc=mycity,dc=mycompany,dc=com"
    bindDN="cn=testuser,cn=users,dc=adtest,dc=mycity,dc=mycompany,dc=com"
    bindPassword="testuserpwd"
    ldapType="Microsoft Active Directory"
    sslEnabled="true"
    sslRef="LDAPSSLSettings">
    <actived Filters
       userFilter="(&amp;(sAMAccountName=%v)(objectcategory=user))"
       groupFilter="(&amp;(cn=%v)(objectcategory=group))"
       userIdMap="user:sAMAccountName"
       groupIdMap="*:cn"
       groupMemberIdMap="memberOf:member" >
```

```
    </actived Filters>
</ldapRegistry>

<ssl id="LDAPSSLSettings" keyStoreRef="LDAPKeyStore" trustStoreRef="LDAPTrustStore" />

<keyStore id="LDAPKeyStore" location="${server.config.dir}/LdapSSLKeyStore.jks"
          type="JKS" password="{xor}CDo9Hgw=" />

<keyStore id="LDAPTrustStore" location="${server.config.dir}/LdapSSLTrustStore.jks"
          type="JKS" password="{xor}CDo9Hgw=" />
```

Notas:

- Soporte para LDAP en Analytic Server está controlado por WebSphere Liberty. Para obtener más información, consulte Configuración de registros de usuarios de LDAP en Liberty.
- Cuando LDAP esté protegido mediante SSL, siga las instrucciones en la conexión "Configuración de una conexión (SSL) de capa de sockets seguros en la sección Analytic Server en LDAP".

Configuración de una conexión SSL (capa de sockets seguros) de Analytic Server a LDAP

Si selecciona la opción de LDAP de Apache Directory Server (`ads`) durante la instalación de Analytic Server, y utiliza la configuración predeterminada, Apache Directory Server se instala con SSL configurado y habilitado (Analytic Server utilizará automáticamente SSL para comunicarse con el Apache Directory Server).

Configure SSL utilizando los pasos siguientes cuando se seleccione una de las otras opciones de LDAP durante la instalación de Analytic Server (por ejemplo, cuando se utiliza un servidor LDAP externo).

1. Inicie la sesión en todas las máquinas de Analytic Server como el usuario de Analytic Server y cree un directorio común para los certificados SSL.

   Nota: de forma predeterminada, as_user es el usuario de Analytic Server; consulte **Service accounts** bajo la pestaña Admin de la consola de Ambari.

2. Copie los archivos de almacén de claves y de almacén de confianza en algún directorio común en todas las máquinas de Analytic Server. Además, añada el certificado de autoridad emisora de certificados LDAP al almacén de confianza. A continuación figuran algunas instrucciones de ejemplo.

   ```
   mkdir /home/as_user/security
   cd /home/as_user/security
   openssl s_client -connect <nombre_host_LDAP>:636 -showcerts > client.cert
   $JAVA_HOME/bin/keytool -import -file ./client.cert -alias ldapCA -keystore mytrust.jks
   password : changeit
   ```

   Nota: JAVA_HOME es el mismo JRE utilizado para el inicio de Analytic Server.

3. Las contraseñas pueden codificarse para ocultar sus valores con la herramienta securityUtility, ubicada en `{RAÍZ_AS}/ae_wlpserver/bin`. A continuación se proporciona un ejemplo.

   ```
   securityUtility encode changeit
            {xor}PDc+MTg6Nis=
   ```

4. Inicie la sesión en la consola de Ambari y actualice el valor de configuración **`ssl.keystore.config`** de Analytic Server con los valores de configuración SSL correctos. A continuación se proporciona un ejemplo.

   ```
   <ssl id="defaultSSLConfig" keyStoreRef="defaultKeyStore" trustStoreRef="defaultTrustStore"
         clientAuthenticationSupported="true"/>
             <keyStore id="defaultKeyStore" location="/home/as_user/security/mykey.jks" type="JKS"
                       password="{xor}Ozo5PiozKxYdEgwPDAweDG1uDz4sLCg7"/>
             <keyStore id="defaultTrustStore" location="/home/as_user/security/mytrust.jks" type="JKS"
                       password="{xor}PDc+MTg6Nis="/>
   ```

   Nota: utilice la vía de acceso absoluta para los archivos de almacén de claves y de almacén de confianza.

5. Actualice el valor de configuración **security.config** de Analytic Server con los valores de configuración LDAP correctos. Por ejemplo, en el elemento **ldapRegistry**, establezca el atributo **sslEnabled** en `true` y el atributo **sslRef** en `defaultSSLConfig`.

Configuración de Kerberos

Analytic Server admite Kerberos con Ambari.

Nota: IBM SPSS Analytic Server no da soporte a Kerberos Single-Sign-On (SSO) cuando se utiliza en conjunción con Apache Knox.

1. Cree cuentas en el repositorio de usuarios de Kerberos para todos los usuarios a los que tiene previsto otorgar acceso a Analytic Server.
2. Cree las mismas cuentas (desde el paso anterior) en el servidor LDAP.
3. Cree una cuenta de usuario de sistema operativo para cada uno de los usuarios creados en el paso anterior en todos los nodos de Analytic Server y en el nodo de Hadoop.
   - Asegúrese de que el ID de usuario de estos usuarios coincide en todas las máquinas. Puede probar esto utilizando el mandato kinit para iniciar la sesión en cada una de las cuentas.
   - Asegúrese de que el UID cumple el valor de Yum "ID de usuario mínimo para enviar trabajo". Éste es el parámetro **min.user.id** en container-executor.cfg. Por ejemplo, si **min.user.id** es 1000, cada cuenta de usuario creada debe tener un UID mayor o igual que 1000.
4. Cree una carpeta de inicio de usuario en HDFS para todos los principales de Analytic Server. Por ejemplo, si añade testuser1 al sistema de Analytic Server, cree una carpeta de inicio como `/user/testuser1` en HDFS y asegúrese de que testuser1 tenga permisos de lectura y escritura para esta carpeta.
5. [Opcional] Si tiene previsto utilizar los orígenes de datos de HCatalog y Analytic Server está instalado en una máquina distinta del metastore de Hive, tiene que suplantar al cliente de Hive en HDFS.
   a. Vaya hasta la pestaña Configs del servicio HDFS en la consola de Ambari.
   b. Edite el parámetro **hadoop.proxyuser.hive.groups** para que tenga el valor `*` o un grupo que contiene todos los usuarios con permiso para iniciar la sesión en Analytic Server.
   c. Edite el parámetro **hadoop.proxyuser.hive.hosts** para que tenga el valor `*` o la lista de hosts en los que están instalados como servicios el metastore de Hive y todas las instancias de Analytic Server.
   d. Reinicie el servicio HDFS.

Después de que se hayan realizado estos pasos y esté instalado Analytic Server, Analytic Server configurará de forma silenciosa y automática Kerberos.

Configuración de HAProxy para el inicio de sesión único (SSO) utilizando Kerberos

1. Configure e inicie HAProxy de acuerdo con la guía de documentación de HAProxy: http://www.haproxy.org/#docs
2. Cree el principio de Kerberos (HTTP/<nombre_host_proxy>@<reino>) y el archivo de tabla de claves para el host de HAProxy, donde <nombre_host_proxy> es el nombre completo del host de HAProxy y <reino> es el dominio Kerberos.
3. Copie el archivo de tabla de claves en cada uno de los hosts de Analytic Server como `/etc/security/keytabs/spnego_proxy.service.keytab`
4. Actualice los permisos en este archivo en cada uno de los hosts de Analytic Server. A continuación se proporciona un ejemplo.

   ```
   chown root:hadoop /etc/security/keytabs/spnego_proxy.service.keytab
   chmod 440 /etc/security/keytabs/spnego_proxy.service.keytab
   ```

5. Abra la consola Ambari y actualice las propiedades siguientes en la sección 'analytics.cfg personalizado' de Analytic Server.

```
web.authentication.kerberos.keytab=/etc/security/keytabs/spnego_proxy.service.keytab
web.authentication.kerberos.principal=HTTP/<nombre completo de
máquina proxy>@<realm>
```

6. Guarde la configuración y reinicie todos los servicios Analytic Server desde la consola Ambari.

Ahora los usuarios pueden iniciar sesión en Analytic Server utilizando la opción **Inicio de sesión con inicio de sesión único** en la pantalla de inicio de sesión de IBM SPSS Analytic Server.

Habilitación de la suplantación de Kerberos

La suplantación permite ejecutar un hilo en un contexto de seguridad que difiere del contexto de seguridad del proceso que es propietario de la hebra. Por ejemplo, la suplantación proporciona un medio para que los trabajos de Hadoop se ejecuten como otros usuarios que no sean los usuarios estándar de Analytic Server (`as_user`). Para habilitar la suplantación de Kerberos:

1. Añada atributos de configuración de suplantación a HDFS (o las configuraciones de servicio Hive) cuando se ejecuta en un clúster habilitado para Kerberos. En el caso de HDFS, deben añadirse las siguientes propiedades al archivo HDFS `core-site.xml`:

   ```
   hadoop.proxyuser.<nombre_principal_servicio_analytic_server> .hosts = *
   hadoop.proxyuser.<nombre_principal_servicio_analytic_server> .groups = *
   ```

   donde `<nombre_principal_servicio_analytic_server>` es el valor `as_user` predeterminado que está especificado en el campo `Usuario_Analytic_Server` de la configuración de Analytic Server.

   Las siguientes propiedades también deben añadirse al archivo HDFS `core-site.xml` en casos en los que el acceso a los datos se realiza desde HDFS vía Hive/HCatalog:

   ```
   hadoop.proxyuser.hive.hosts = *
   hadoop.proxyuser.hive.groups = *
   ```

2. Si Analytic Server está configurado para utilizar un nombre de usuario distinto de `as_user`, debe modificar los nombres de propiedad para reflejar el nombre de otro usuario (por ejemplo, `hadoop.proxyuser.xxxxx.hosts`, donde `xxxxx` es el nombre de usuario configurado que se especifica en la configuración de Analytic Server).
3. Ejecute el mandato siguiente desde un shell de mandatos en el nodo Analytic Server:

   ```
   hadoop fs -chmod -R 755 /user/as_user/analytic-root/analytic-workspace
   ```

habilitar varios dominios

El valor **as.kdc.realms** es obligatorio para definir varios dominios. Los valores de **as.kdc.realms** se encuentran en la sección 'Advanced analytics.cfg' de Analytic Server de la consola Ambari.

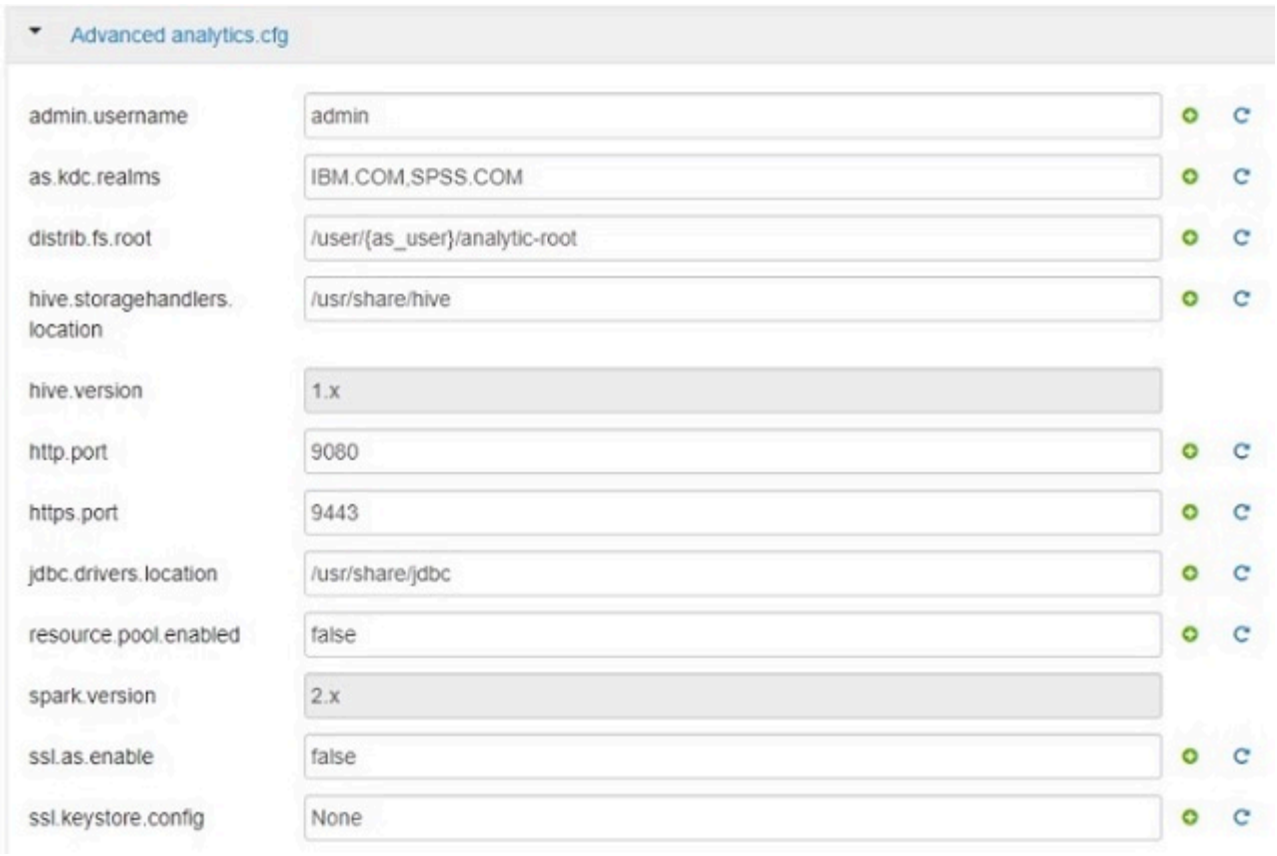

Figura 3. Valores de Advanced analytics.cfg

Se admiten varios nombres de dominios cuando están separados por comas. Los nombres de dominio Kerberos especificados corresponden a nombres de usuario y están asociados a los mismos. Por ejemplo, los nombres de usuario `UserOne@us.ibm.com` y `UserTwo@eu.ibm.com` corresponderían a los dominios `us.ibm.com,eu.ibm.com`.

Se deben configurar confianzas entre dominios de Kerberos cuando se especifica más de un dominio como **Nombre de dominio de Kerberos**. El nombre de usuario que se especifica durante la solicitud de inicio de sesión en la consola de Analytic Server se especifica sin el sufijo de nombre de dominio. Como resultado, cuando se especifican varios dominios, se presenta a los usuarios una lista desplegable de **Dominios** que les permite seleccionar el dominio adecuado.

Nota: Cuando sólo se especifica un dominio, no se presenta a los usuarios ninguna lista despegable **Dominios** al iniciar sesión en Analytic Server.

Inhabilitación de Kerberos

1. Inhabilite Kerberos en la consola de Ambari.
2. Detenga el servicio Analytic Server.
3. Elimine los parámetros siguientes del archivo `analytics.cfg` personalizado.

```
default.security.provider
hdfs.keytab
hdfs.user
java.security.krb5.conf
as.db.connect.method
web.authentication.kerberos.keytab
web.authentication.kerberos.principal
```

4. Pulse **Guardar** y reinicie el servicio Analytic Server.

Habilitación de conexiones SSL (capa de sockets seguros) a la consola de Analytic Server

De forma predeterminada, Analytic Server genera certificados firmados automáticamente para habilitar la capa de sockets seguros (SSL), de modo que puede acceder a la consola de Analytic Server a través del puerto seguro aceptando los certificados firmados automáticamente. Para que el acceso HTTPS sea más seguro, tendrá que instalar certificados de proveedores de terceros.

Para instalar certificados de proveedores de terceros, siga estos pasos.

1. Copie el proveedor de terceros y los certificados de almacén de confianza en el mismo directorio en todos los nodos de Analytic Server; por ejemplo, `/home/as_user/security`.

   Nota: El usuario de Analytic Server debe tener acceso de lectura a este directorio.
2. En la pestaña Ambari Services, vaya hasta la pestaña Configs del servicio Analytic Server.
3. Edite el parámetro **`ssl.keystore.config`**.

   ```
   <ssl id="defaultSSLConfig"
        keyStoreRef="defaultKeyStore"
        trustStoreRef="defaultTrustStore"
        clientAuthenticationSupported="true"/>
   <keyStore id="defaultKeyStore"
             location="<KEYSTORE-LOCATION>"
             type="<TYPE>"
             password="<PASSWORD>"/>
   <keyStore id="defaultTrustStore"
             location="<TRUSTSTORE-LOCATION>"
             type="<TYPE>"
             password="<PASSWORD>"/>
   ```

   Sustituya
   - <KEYSTORE-LOCATION> por la ubicación absoluta del almacén de claves; por ejemplo: `/home/as_user/security/mykey.jks`
   - <TRUSTSTORE-LOCATION> por la ubicación absoluta del almacén de confianza; por ejemplo: `/home/as_user/security/mytrust.jks`
   - <TYPE> por el tipo de certificado; por ejemplo: JKS, PKCS12 etc.
   - <PASSWORD> por la contraseña cifrada en formato de cifrado Base64. Para la codificación puede utilizar securityUtility; por ejemplo: `/opt/ibm/spss/analyticserver/3.2/ae_wlpserver/bin/securityUtility encode <contraseña>`

   Si desea generar un certificado firmado automáticamente, puede utilizar securityUtility; por ejemplo: `/opt/ibm/spss/analyticserver/3.2/ae_wlpserver/bin/securityUtility createSSLCertificate --server=myserver --password=mypassword --validity=365 --subject=CN=mycompany,O=myOrg,C=myCountry`.

   Nota: Debe proporcionar un nombre de dominio de host adecuado para el valor `CN`.

   Para obtener más información sobre securityUtility y otros valores de SSL, consulte la documentación de WebSphere Liberty Profile
4. Pulse **Guardar** y reinicie el servicio Analytic Server.

Comunicarse con Apache Hive sobre SSL

Debe actualizar el archivo `hive.properties` con el fin de comunicarse con Apache Hive a través de una conexión SSL. De forma alternativa, si el entorno de Apache Hive está habilitado para alta disponibilidad, puede seleccionar los parámetros de alta disponibilidad en la página principal de orígenes de datos de Analytic Server.

Actualización del archivo hive.properties

1. Abra el archivo `hive.properties`. El archivo se encuentra en: `/opt/ibm/spss/analyticserver/3.2/ae_wlpserver/usr/servers/aeserver/configuration/database`
2. Localice la línea siguiente:

```
jdbcurl = jdbc:hive2://{db.servername}:{db.serverport}/{db.databasename};user={db.username};password={db.password}
```

3. Actualice la línea añadiendo la información en **negrita** siguiente:

```
jdbcurl = jdbc:hive2://{db.servername}:{db.serverport}/{db.databasename};user={db.username};password={db.password};
ssl=true;sslTrustStore=pathtotheirtruststorefile;trustStorePassword=xxxtheirTrustStorePassword
```

4. Guarde el archivo `hive.properties`.

Habilitación del soporte para Essentials for R

Analytic Server da soporte a la puntuación de modelos R y la ejecución de scripts R.

Para configurar el soporte para R tras una instalación satisfactoria de Analytic Server:

1. Suministre el entorno del servidor para Essentials for R.

RedHat Linux x86_64

Ejecute los mandatos siguientes:

```
yum update
yum install -y zlib zlib-devel
yum install -y bzip2 bzip2-devel
yum install -y xz xz-devel
yum install -y pcre pcre-devel
yum install -y libcurl libcurl-devel
```

Ubuntu Linux

Ejecute los mandatos siguientes:

```
apt-get update
apt-get install -y zlib1g-dev
apt-get install -y libreadline-dev
apt-get install -y libxt-dev
apt-get install -y bzip2
apt-get install -y libbz2-dev
apt-get install -y liblzma-dev
apt-get install -y libpcre3 libpcre3-dev
apt-get install -y libcurl4-openssl-dev
apt-get install -y liblzma-dev
apt-get install -y libpcre3 libpcre3-dev
apt-get install -y libcurl4-openssl-dev
```

SUSE Linux

La instalación de Essentials for R en SUSE requiere un FORTRAN compatible que no suele estar disponible en los repositorios ZYPPER configurados (solo está disponible desde el soporte SDK de SUSE). Como resultado, la ejecución de una instalación de Ambari para Essentials for R en un servidor SUSE fallará puesto que no podrá instalar FORTRAN. Utilice los pasos siguientes para suministrar en SUSE:

a. Instale GCC C++.

```
zypper install gcc-c++
```

b. Instale GCC FORTRAN. Los archivos RPM necesarios pueden copiarse desde el soporte SDK de SUSE y debe instalarse en el orden siguiente.

```
zypper install libquadmath0-4.7.2_20130108-0.19.3.x86_64.rpm
zypper install libgfortran3-4.7.2_20130108-0.19.3.x86_64.rpm
zypper install gcc43-fortran-4.3.4_20091019-0.37.30.x86_64.rpm
zypper install gcc-fortran-4.3-62.200.2.x86_64.rpm
```

c. Ejecute el mandato siguiente para instalar las bibliotecas de Essentials for R.

```
R_PREFIX=/opt/ibm/spss/R
cd $R_PREFIX
rm -fr $R_PREFIX/r_libs
mkdir -p $R_PREFIX/r_libs
cd $R_PREFIX/r_libs
wget https://zlib.net/fossils/zlib-1.2.11.tar.gz --no-check-certificate
tar zxvf zlib-1.2.11.tar.gz
cd zlib-1.2.11/
./configure
make && make install
cd $R_PREFIX/r_libs
wget http://www.bzip.org/1.0.6/bzip2-1.0.6.tar.gz
tar xzvf bzip2-1.0.6.tar.gz
cd bzip2-1.0.6
```

```
sed "s|^CC=gcc|CC=gcc -fPIC|" -i ./Makefile
make -f Makefile-libbz2_so
make clean
make
make install
cd $R_PREFIX/r_libs
wget https://tukaani.org/xz/xz-5.2.3.tar.gz
tar xzvf xz-5.2.3.tar.gz
cd xz-5.2.3
./configure
make -j3
make install
cd $R_PREFIX/r_libs
wget http://ftp.pcre.org/pub/pcre/pcre-8.38.tar.gz
tar xzvf pcre-8.38.tar.gz
cd pcre-8.38
./configure --enable-utf8
make
make install
cd $R_PREFIX/r_libs
wget https://www.openssl.org/source/openssl-1.0.2l.tar.gz --no-check-certificate
tar zxvf openssl-1.0.2l.tar.gz
cd openssl-1.0.2l/
./config shared
make
make install
echo '/usr/local/ssl/lib' >> /etc/ld.so.conf
ldconfig
cd $R_PREFIX/r_libs
wget --no-check-certificate https://curl.haxx.se/download/curl-7.50.1.tar.gz
tar xzvf curl-7.50.1.tar.gz
cd curl-7.50.1
./configure --with-ssl
make -j3
make install
cd $R_PREFIX/r_libs
wget ftp://rpmfind.net/linux/opensuse/distribution/12.3/repo/oss/suse/x86_64/libgomp1-4.7.2_20130108-2.1.6.x86_64.rpm
 --no-check-certificate
rpm -ivh libgomp1-4.7.2_20130108-2.1.6.x86_64.rpm
```

2. Descargue el archivo autoextraíble (BIN) para el RPM de IBM SPSS Modeler Essentials for R RPM o DEB. Essentials for R está disponible para la descarga (https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=swg-tspssp). Elija el archivo específico a su pila, versión de pila y arquitectura de hardware.
3. Ejecute el archivo binario autoextraíble y siga las instrucciones para ver (opcionalmente) la licencia, aceptar la licencia y elegir la instalación en línea o fuera de línea.

   Instalación en línea
   Elija la instalación en línea si el host del servidor Ambari y todos los nodos del clúster pueden acceder a https://ibm-open-platform.ibm.com.

   Instalación fuera de línea
   Elija fuera de línea si el host del servidor Ambari no tiene acceso a Internet. La instalación fuera de línea descargará los archivos RPM necesarios y deberá ejecutarse en una máquina que pueda acceder a https://ibm-open-platform.ibm.com. Los archivos de RPM se pueden copiar en el host del servidor Ambari.

   a. Copie los archivos de RPM o DEB necesarios de Essentials for R en cualquier ubicación en el host del servidor Ambari. Los archivos de RPM/DEB que necesita dependen de la distribución, la versión y la arquitectura, tal como se muestra a continuación.

      HDP 2.5, 2.6, 3.0 y 3.1 (x86_64)
      IBM-SPSS-ModelerEssentialsR-ambari-2.1-HDP-2.6-9.1.0.0-1.x86_64.rpm

      HDP 2.6, 3.0 y 3.1 (PPC64LE)
      IBM-SPSS-ModelerEssentialsR-ambari-2.1-HDP-2.6-9.1.0.0-1.ppc64le.rpm

      HDP 2.5, 2.6, 3.0 y 3.1 (Ubuntu)
      IBM-SPSS-ModelerEssentialsR-ambari-3.2.1.0_3.2.1.0_amd64.deb

   b. Instale el RPM o DEB. En el ejemplo siguiente, el mandato instala Essentials for R en HDP 2.6 (x86_64).

      ```
      rpm -i IBM-SPSS-ModelerEssentialsR-ambari-2.1-HDP-2.6-9.1.0.0-1.x86_64.rpm
      ```

      En el siguiente ejemplo, el mandato instala Essentials for R en HDP 2.5 (Ubuntu).

      ```
      dpkg -i IBM-SPSS-ModelerEssentialsR-ambari-3.2.1.0_3.2.1.0_amd64.deb
      ```

4. Reinicie el servidor Ambari.

```
ambari-server restart
```

5. Inicie la sesión en el servidor Ambari e instale SPSS Essentials for R como servicio a través de la consola de Ambari. SPSS Essentials for R se debe instalar en cada host donde Analytic Server y Analytic Metastore están instalados.

   Nota: Ambari tratará de instalar gcc-c++ y gcc-gfortran (RHEL) y gcc-fortran (SUSE) antes de instalar R. Estos paquetes se declaran como dependencias de definición de servicio Ambari de R. Asegúrese de que los servidores donde se va a instalar y ejecutar R se han configurado para descargar los RPM gcc-c++ y gcc-[g]fortran o que tienen instalados los compiladores GCC y FORTRAN. Si la instalación de Essentials for R falla, instale estos paquetes manualmente antes de instalar Essentials for R.
6. Renueve el servicio Analytic Server.
7. Ejecute el script `update_clientdeps` utilizando las instrucciones que figuran en "Actualización de las dependencias del cliente" en la página 28.
8. También debe instalar Essentials for R en la máquina que aloja SPSS Modeler Server. Consulte la Documentación de SPSS Modeler para ver más detalles.

Habilitación de orígenes de bases de datos relacionales

Analytic Server puede utilizar orígenes de bases de datos relacionales si proporciona los controladores JDBC en un directorio compartido en cada metsstore de Analytic Server y cada host de Analytic Server. De forma predeterminada, el directorio es `/usr/share/jdbc`.

Para cambiar el directorio compartido, siga estos pasos.

1. En la pestaña Ambari Services, vaya hasta la pestaña Configs del servicio Analytic Server.
2. Abra la sección **Advanced analytics.cfg**.
3. Especifique la vía de acceso del directorio compartido de los controladores JDBC en **`jdbc.drivers.location`**.
4. Pulse **Guardar**.
5. Detenga el servicio Analytic Server.
6. Pulse **Renovar**.
7. Inicie el servicio Analytic Server.

Tabla 6. Bases de datos soportadas

Base de datos	Versiones soportadas	Archivos JAR del controlador JDBC	Distribuidor
Amazon Redshift	8.0.2 o posterior.	`RedshiftJDBC41-1.1.6.1006.jar` o posterior	Amazon
BigSQL	4.1.0.0 o posterior.	db2jcc.jar	IBM
DashDB	Bluemix Service	`db2jcc.jar`	IBM
Db2 para Linux, UNIX y Windows	11.1, 10.5, 10.1, 9.7	`db2jcc.jar`	IBM
Db2 z/OS	11, 10	`db2jcc.jar`, `db2_license_cisuz.jar`	IBM
Greenplum	5	postgresql.jar	Greenplum
Hive	1.2, 2.1	`hive-jdbc-*.jar`	Apache
MySQL	5.6, 5.7	mysql-connector-java-commercial-5.1.25-bin.jar	MySQL
Netezza	7, 6.x	`nzjdbc.jar`	IBM
Oracle	12c, 11g R2 (11.2)	`ojdbc6.jar`, `orai18n.jar`	Oracle
SQL Server	2014, 2012, 2008 R2	`sqljdbc4.jar`	Microsoft

Tabla 6. Bases de datos soportadas (continuación)

Base de datos	Versiones soportadas	Archivos JAR del controlador JDBC	Distribuidor
Teradata	15, 15.1	`tdgssconfig.jar`, `terajdbc4.jar`	Teradata

Notas

- Si ha creado un origen de datos Redshift antes de instalar Analytic Server, necesitará efectuar los pasos siguientes para utilizar el origen de datos Redshift.
  1. En la consola de Analytic Server, abra el origen de datos Redshift.
  2. Seleccione el origen de datos de la base de datos `Redshift`.
  3. Especifique la dirección del servidor de Redshift.
  4. Entre el nombre de la base de datos y el nombre de usuario. La contraseña se debe llenar automáticamente.
  5. Seleccione la tabla de base de datos.
- BigSQL es la interfaz SQL de IBM para el entorno Apache Hadoop. BigSQL no es una base de datos relacional, pero el acceso de soporte de Analytic Server a la misma se realiza a través de JDBC (el archivo jar JDBC es igual al que se utiliza para Db2).

  Un uso común para BigSQL con Analytic Server es acceder a tablas Hadoop/HBase de BigSQL a través de un origen de datos HCatalog.

Habilitación de orígenes de datos de HCatalog

Analytic Server proporciona soporte de varios orígenes de datos a través de Hive/HCatalog. Algunos orígenes requieren pasos de configuración manuales.

1. Recopile los archivos JAR necesarios para habilitar el origen de datos. No es necesario ningún paso adicional para habilitar el soporte de Apache HBase y Apache Accumulo. Para otros orígenes de datos NoSQL, póngase en contacto con el proveedor de base de datos y obtenga el manejador de almacenamiento y los jar relacionados. Para obtener información sobre los orígenes de datos de HCatalog soportados, consulte la sección "Utilización de orígenes de datos de HCatalog" de la Guía del usuario de IBM SPSS Analytic Server 3.2.1.
2. Añadir estos archivos JAR al directorio `{INICIO_HIVE}/auxlib` y al directorio `/usr/share/hive` en cada metastore de Analytic Server y cada nodo de Analytic Server.
3. Reiniciar el servicio Hive Metastore.
4. Renovar el servicio Analytic Metastore.
5. Reiniciar todas las instancias del servicio Analytic Server.

Notas:

- Analytic Server Metastore no se puede instalar en la misma máquina que Hive Metastore.
- Al acceder a los datos de HBase a través de un origen de datos HCatalog de Analytic Server, el usuario de acceso debe tener permiso de lectura para las tablas HBase.
  - En entornos que no sean kerberos, Analytic Server accede a HBase utilizando `as_user` (`as_user` debe tener permiso de lectura para HBase).
  - En entornos de kerberos, tanto `as_user` como el usuario de inicio de sesión deben tener permiso de lectura para las tablas HBase.

Bases de datos NoSQL

Analytic Server admite cualquier base de datos NoSQL para la que está disponible un manejador de almacenamiento de Hive del proveedor.

No es necesario ningún paso adicional para habilitar el soporte de Apache HBase y Apache Accumulo.

Para otras bases de datos NoSQL, póngase en contacto con el proveedor de base de datos y obtenga el manejador de almacenamiento y los jar relacionados.

Tablas Hive basadas en archivo

Analytic Server admite las tablas Hive basadas en archivo para las que está disponible un Hive SerDe (serializador-deserializador) incorporado o personalizado.

Hive XML SerDe para procesar los archivos XML se ubica en el repositorio central de Maven en http://search.maven.org/#search%7Cga%7C1%7Chivexmlserde.

Trabajos de MapReduce v2

Utilice el valor **preferred.mapreduce** de la sección **Custom analytic.cfg** de Analytic Server para controlar cómo se manejan los trabajos MapReduce:

Tabla 7. Propiedades de analytics.cfg personalizadas

Propiedad	Descripción
preferred.mapreduce	Controla el método en el que se ejecutan los trabajos MapReduce. Los valores válidos incluyen: • spark • m3r • hadoop Por ejemplo: preferred.mapreduce=spark

Apache Spark

Si desea utilizar Spark (versión 1.5 o posterior), debe añadir manualmente la propiedad spark.version durante Analytic Server.

1. Abra la consola Ambari y añada la siguiente propiedad en la sección **Advanced analytics.cfg** de Analytic Server.
   - **Clave**: spark.version
   - **Valor**: Especifique el número de versión de Spark adecuado (por ejemplo, 1.x, 2.xo Ninguno).
2. Guarde la configuración.

Nota: Puede forzar que HCatalog no utilice nunca Spark a través de un valor analytics.cfg personalizado.

1. Abra la consola Ambari y añada la siguiente propiedad en la sección **Custom analytic.cfg** de Analytic Server.
   - **Clave**: spark.hive.compatible
   - **Valor**: false

Entornos de HDP 3.0 habilitado para Kerberos (o posterior)

Entornos de HDP 3.0 habilitado para Kerberos (o posterior) puede requerir valores de configuración de seguridad adicionales. En HDFS, se utilizan facls de sistema de archivos en el directorio /warehouse/tablespace/managed/hive. Puede identificar el requisito para establecer facls en el metastore de Hive cuando aparezcan las siguientes excepciones en los archivos messages.log o as_trace.log:

```
Caused by: org.apache.hadoop.hive.ql.metadata.HiveException: java.security.AccessControlException:
Permission denied: user=xxxx, access=READ, inode="/warehouse/tablespace/managed/hive/hcat_primitives":hive:hadoop:drwxrwx---
at org.apache.hadoop.hdfs.server.namenode.FSPermissionChecker.check(FSPermissionChecker.java:399)
```

```
at org.apache.hadoop.hdfs.server.namenode.FSPermissionChecker.checkPermission(FSPermissionChecker.java:261)
at org.apache.hadoop.hdfs.server.namenode.FSPermissionChecker.checkPermission(FSPermissionChecker.java:193)
at org.apache.hadoop.hdfs.server.namenode.FSDirectory.checkPermission(FSDirectory.java:1850)
at org.apache.hadoop.hdfs.server.namenode.FSDirectory.checkPermission(FSDirectory.java:1834)
at org.apache.hadoop.hdfs.server.namenode.FSDirectory.checkPathAccess(FSDirectory.java:1784)
at org.apache.hadoop.hdfs.server.namenode.FSNamesystem.checkAccess(FSNamesystem.java:7767)
```

El ejemplo siguiente muestra un mandato **setfacl** que proporciona un amplio acceso (en este ejemplo, a todos los miembros del grupo `hadoop`) al directorio `warehouse` de Hive:

```
hadoop fs -setfacl -R -m group:hadoop:rwx /warehouse/tablespace/managed/hive/
```

De otra manera, deben utilizarse variaciones más restrictivas cuando es necesario un control de acceso más granular.

Los sitios siguientes proporcionan información de referencia adicional.

https://docs.hortonworks.com/HDPDocuments/HDP3/HDP-3.1.0/hdfs-acls/content/acl_examples.html

https://docs.hortonworks.com/HDPDocuments/HDP3/HDP-3.1.0/securing-hive/content/hive_sba_permissions_model.html

Cambio de puertos utilizados por Analytic Server

Analytic Server utiliza el puerto 9080 para HTTP y el puerto 9443 para HTTPS de forma predeterminada. Para cambiar los valores de puerto, siga estos pasos.

1. En la pestaña Ambari Services, vaya hasta la pestaña Configs del servicio Analytic Server.
2. Abra la sección **Advanced analytics.cfg**.
3. Especifique los puertos HTTP y HTTPS deseados en **http.port** y **https.port**, respectivamente.
4. Pulse **Guardar**.
5. Reinicie el servicio Analytic Server.

Analytic Server de alta disponibilidad

Puede hacer que Analytic Server sea de alta disponibilidad añadiéndolo como un servicio a varios nodos del clúster.

1. En la consola de Ambari, vaya hasta la pestaña Hosts.
2. Seleccione un host que no esté ejecutando ya Analytic Server como un servicio.
3. En la pestaña Resumen, pulse **Añadir** y seleccione Analytic Server.
4. Pulse **Confirmar la adición**.

Soporte de varios clústeres

La característica de varios clústeres es una mejora a la prestación de Alta disponibilidad de IBM SPSS Analytic Server y proporciona un aislamiento mejorado en entornos de varios inquilinos. De forma predeterminada, la instalación del servicio de Analytic Server (en Ambari o ClouderaManager) da lugar a la definición de un único clúster de servidor de análisis.

La especificación de clúster define la pertenencia al clúster de Analytic Server. La modificación de la especificación del clúster se realiza con contenido XML (en el campo `analytics-cluster` de la configuración de Analytic Server de Ambari o manualmente editando el archivo `configuration/analytics-cluster.xml`) de Cloudera Manager. Al configurar varios clústeres de Analytic Server , es necesario alimentar solicitudes para cada clúster de Analytic Server con su propio equilibrador de carga.

Mediante la característica de varios clústeres garantiza que el trabajo para un inquilino no puede afectar negativamente al trabajo que se realice en el clúster de otro inquilino. Respecto a trabajos de altamente disponibles, la migración tras error de trabajo solo se produce en el ámbito de clúster de Analytic Server en el que se inició el trabajo. En el ejemplo siguiente se proporciona una especificación XML de varios clústeres.

Nota: Puede hacer que Analytic Server sea de alta disponibilidad añadiéndolo como un servicio a varios nodos del clúster.

```
<analayticServerClusterSpec>
    <cardinality>1+</cardinality>
    <cluster name="cluster1">
        <memberName>one.cluster</memberName>
        <memberName>two.cluster</memberName>
    </cluster>
    <cluster name="cluster2">
        <memberName>three.cluster</memberName>
        <memberName>four.cluster</memberName>
    </cluster>
</analayticServerClusterSpec>
```

En el ejemplo anterior, se precisan dos equilibradores de carga. Un equilibrador de carga envía solicitudes a miembros de `cluster1` (`one.cluster` y `two.cluster`) y el otro envía solicitudes a miembros de `cluster2` (`three.cluster` y `four.cluster`).

En el ejemplo siguiente se proporciona una especificación XML de clúster único (la configuración predeterminada).

```
<analayticServerClusterSpec>
    <cardinality>1</cardinality>
    <cluster name="cluster1">
        <memberName>*</memberName>
    </cluster>
</analayticServerClusterSpec>
```

En el ejemplo anterior, un equilibrador de carga único se precisa para manejar casos en los que existe más de un miembro de clúster configurado.

Notas

- Solo clústeres singleton dan soporte al uso de comodines en el elemento **`memberName`** (por ejemplo, cardinalidad de clúster = "1"). Los valores válidos para el elemento de cardinalidad son 1 y 1+.
- **`memberName`** se debe especificar de la misma manera que el nombre de host al que se ha asignado el rol de Analytic Server.
- Todos los servidores en todos los clústeres deben reiniciarse después de que se apliquen los cambios de configuración del clúster.
- En Cloudera Manager, debe modificar y mantener el archivo `analytics-cluster.xml` en todos los nodos de Analytic Server. Todos los nodos deben mantenerse para garantizar que contengan el mismo contenido.

Optimización de opciones de la JVM para datos pequeños

Puede editar las propiedades de la JVM para poder optimizar su sistema al ejecutar trabajos pequeños (M3R).

En la consola de Ambari, consulte la sección Advanced analytics-jvm-options de la pestaña Configs del servicio Analytic Server. La modificación de los parámetros siguientes establece el tamaño de almacenamiento dinámico para trabajos que se ejecutan en el servidor que aloja Analytic Server; es decir, no Hadoop. Esto es importante si se ejecutan trabajos (M3R) pequeños y es posible que tenga que experimentar con estos valores para optimizar el sistema.

```
-Xms512M
-Xmx2048M
```

Actualización de las dependencias del cliente

En esta sección se describe cómo actualizar las dependencias del servicio Analytic Server utilizando el script `update_clientdeps`.

1. Inicie una sesión el host del servidor Ambari como root.

2. Cambie el directorio `/var/lib/ambari-server/resources/stacks/<nombre_pila>/<versión_pila>/services/ANALYTICSERVER/package/scripts`; consulte el ejemplo siguiente.

   ```
   cd "/var/lib/ambari-server/resources/stacks/HDP/2.6/services/ANALYTICSERVER/package/scripts"
   ```

3. Ejecute el script `update_clientdeps` con los argumentos siguientes.

   -u <ambari-user>
   El nombre de usuario de la cuenta de Ambari

   -p <ambari-password>
   La contraseña para el usuario de la cuenta de Ambari.

   -h <ambari-host>
   El nombre de host del servidor Ambari.

   -x <ambari-port>
   El puerto en el cual escucha Ambari.

   Consulte el ejemplo siguiente.

   ```
   ./update_clientdeps.sh -u admin -p admin -h host.domain -x 8080
   ```

4. Reinicie el servidor Ambari utilizando el mandato siguiente.

   ```
   ambari-server restart
   ```

Configuración de Apache Knox

Apache Knox Gateway es un sistema que proporciona un único punto de acceso seguro a los servicios de Apache Hadoop. El sistema simplifica la seguridad de Hadoop, tanto para los usuarios (que acceden a los datos del clúster y ejecutan trabajos) como para los operadores (que controlan el acceso y gestionan el clúster). Apache Knox Gateway ejecuta un servidor (o clúster de servidores) que sirve a uno o más clústeres de Hadoop.

Nota: IBM SPSS Analytic Server no da soporte a Apache Knox cuando se utiliza conjuntamente con Kerberos Single-Sign-On (SSO).

Apache Knox oculta eficazmente los detalles de topología del clúster de Hadoop y se integra en el LDAP empresarial y Kerberos. Las secciones siguientes proporcionan información sobre las tareas de configuración de Apache Knox y Analytic Server necesarias.

Requisitos previos

- Un problema conocido de Apache Knox no propaga la información de seguridad que está contenida en las cookies y cabeceras HTTP (para obtener más información, consulte https://issues.apache.org/jira/browse/KNOX-895). El problema se resuelve en Knox 0.14.0 (o posterior). Debe obtener una distribución de Hortonworks actualizada, que incluya Knox 0.14.0 (o posterior), antes de Knox con el trabajo con Analytic Server. Póngase en contacto con el proveedor de Hortonworks para obtener más información.
- Los nodos de Analytic Server se deben conectar con el servidor Knox con una conexión SSH sin contraseña. La conexión SSH sin contraseña se mueve de Analytic Server a Knox (**Analytic Server** > **Knox**).
- Analytic Server se debe instalar después de que se haya instalado el servicio de Knox.

En algunos casos, algunos problemas imprevistos pueden dar lugar a que los archivos de configuración no se copien automáticamente. En estos casos, debe copiar manualmente los archivos de configuración siguientes:

- `com.ibm.spss.knox_0.6-3.2.1.0.jar`: El archivo se debe copiar desde la ubicación de Analytic Server:

  `<vía_acceso_instalación_Analytic_Server>/ae_wlpserver/usr/servers/aeserver/apps/AE_BOOT.war/WEB-INF/lib`

  en el nodo del servidor Knox:

/KnoxServicePath/ext

Por ejemplo: /usr/iop/4.1.0.0/knox/ext

- rewrite.xml y service.xml: Los archivos se deben copiar desde la ubicación de Analytic Server:

  <vía_acceso_instalación_Analytic_Server>/ae_wlpserver/usr/servers/aeserver/configuration/knox

  en el nodo del servidor Knox:

  /KnoxServicePath/data/services

  Por ejemplo: /usr/iop/4.1.0.0/knox/data/services

  Nota: Hay dos conjuntos de archivos rewrite.xml y service.xml (un conjunto para el tráfico http://rest y un conjunto para el tráfico ws://websocket). Copie todos los archivos rewrite.xml y service.xml tanto para analyticserver como para analyticserver_ws en el nodo de servidor Knox.

Configuración de Ambari

El servicio Analytic Server debe configurarse en la interfaz de usuario de Ambari:

1. En la interfaz de usuario de Ambari, vaya a **Knox** > **Configs** > **Advanced topology**. Los valores actuales de la configuración de Knox se muestran en la ventana **content**.
2. Añada los dos servicios siguientes a la sección **Topología avanzada** en la configuración de Knox:

```
<service>
    <role>ANALYTICSERVER</role>
    <url>http://{analyticserver-host}:{analyticserver-port}/analyticserver</url>
 </service>
<service>
    <role>ANALYTICSERVER_WS</role>
    <url>ws://{analyticserver-host}:{analyticserver-port}/analyticserver</url>
 </service>
```

   {analyticserver-host} y {analyticserver-port} deben sustituirse por el nombre de servidor y el número de puerto de Analytic Server correspondientes:

   - El URL de {analyticserver-host} puede encontrarse en la interfaz de usuario de Ambari (**SPSS Analytic Server** > **Summary** > **Analytic Server**).
   - El número de {analyticserver-port} puede encontrarse en la interfaz de usuario de Ambari (**SPSS Analytic Server** > **Configs** > **Advanced analytics.cfg** > **http.port**).

   Nota: Cuando Analytic Server se despliega en varios nodos y se utiliza LoadBalancer, {analyticserver-host} y {analyticserver-port} deben corresponderse con el URL y el número de puerto de LoadBalancer.
3. Reinicie el servicio Knox.

Cuando se utiliza LDAP, Knox toma el valor predeterminado de LDAP "Demo". Puede cambiarlo por un servidor LDAP empresarial (como Microsoft LDAP o OpenLDAP).

Configuración de Analytic Server

Para utilizar LDAP para Analytic Server, Analytic Server debe configurarse para que utilice el mismo servidor LDAP que Apache Knox. Deben actualizarse las entradas <value> de los siguientes valores de Ambari para que reflejen los valores del servidor LDAP Knox correspondientes:

- main.ldapRealm.userDnTemplate
- main.ldapRealm.contextFactory.url

Los valores están disponibles en la interfaz de usuario de Ambari en: **Knox** > **Configs** > **Advanced topology**. Por ejemplo:

```
<param>
   <name>main.ldapRealm.userDnTemplate</name>
   <value>uid={0},ou=people,dc=hadoop,dc=apache,dc=org</value>
</param>
```

```
<param>
   <name>main.ldapRealm.contextFactory.url</name>
   <value>ldap://{{nombre_host_knox}}:33389</value>
</param>
```

Reinicie el servicio Knox tras actualizar los valores LDAP de Knox.

Importante: La contraseña de administrador de Analytic Server debe ser la misma que la contraseña de administrador de Knox.

Configuración de Apache Knox

1. Renueve el archivo gateway.jks de Knox:
   a. En el servidor de Knox, detenga el servicio de Knox.
   b. Suprima el archivo gateway.jks de /var/lib/knox/data-2.6.2.0-205/security/keystores.
   c. Reinicie el servicio Knox.
2. En el servidor de Knox, cree el subdirectorio <servidor_knox>/data/service/analyticserver/3.2.1.0 y, a continuación, cargue los archivos service.xml y rewrite.xml en el nuevo directorio. Los dos archivos se encuentran en Analytic Server en <analytic_server>/configuration/knox/analyticserver/ (por ejemplo,/opt/ibm/spss/analyticserver/3.2/ae_wlpserver/usr/servers/aeserver/configuration/knox/analyticserver/*.xml)
3. En <knox_server>/bin, ejecute el script ./knoxcli.sh redeploy --cluster default
4. Cargue el archivo com.ibm.spss.knoxservice_0.6-*.jar en <servidor_knox>/ext. El archivo está en Analytic Server en <analytic_server>/apps/AE_BOOT.war/WEB-INF/lib/com.ibm.spss.knox_0.6-3.2.1.0.jar (por ejemplo,/opt/ibm/spss/analyticserver/3.2/ae_wlpserver/usr/servers/aeserver/apps/AE_BOOT.war/WEB-INF/lib/com.ibm.spss.knox_0.6-3.2.1.0.jar).
5. En la interfaz de usuario Ambari, añada el elemento siguiente en **Knox** > **Configs** > **Advanced topology**:

   ```
   <service>
      <role>ANALYTICSERVER</role>
      <url>http://{analyticserver-host}:{analyticserver-port}/analyticserver</url>
      <role>ANALYTICSERVER_WS</role>
      <url>ws://{analyticserver-host}:{analyticserver-port}/analyticserver</url>
   </service>
   ```

   Nota: De forma predeterminada, la funcionalidad de WebSocket está inhabilitada. Se puede habilitar cambiando la propiedad gateway.websocket.feature.enabled a true en el archivo /conf/gateway-site.xml.
6. En la interfaz de usuario Ambari, añada o actualice los usuarios en **Knox** > **Configs** > **Advanced users-ldif** (por ejemplo admin, qauser1, qauser2).
7. Reinicie LDAP desde **Knox** > **Service Actions** > **Start Demo LDAP**.
8. Reinicie el servicio Knox.

Estructura de URL del Analytic Server habilitado para Apache Knox

El URL de interfaz de usuario de Analytic Server habilitado por Knox es https://{host-knox}:{puerto-knox}/gateway/default/analyticserver/admin

- protocolo https - los usuarios deben aceptar un certificado para continuar en el navegador web.
- host-knox es el host de Knox.
- puerto-knox es el número de puerto de Knox.
- El URI es gateway/default/analyticserver.

Configuración de colas YARN separadas para cada inquilino de IBM SPSS Analytic Server - HDP

La configuración de las colas Yarn se lleva a cabo mediante el uso de los técnicos de Spark Dynamic Resource Allocation.

Hortonworks Data Platform 2.x

1. En la interfaz de usuario de Ambari, vaya a la pestaña **Servicio de SPSS Analytic Server** > **Configs** > **Advanced analytics.cfg**.
2. Cambie el valor **resource.pool.enabled** por `true`.
3. Añada las propiedades siguientes en la pestaña **Custom analytics.cfg**:

```
config.folder.path=/etc/spark2/conf
resource.pool.mapping=tenant1:test,tenant2:production
resource.pool.default=default
spark.scheduler.mode=FAIR
spark.yarn.queue=default
```

Tabla 8. Propiedades de analytics.cfg personalizadas

Propiedad	Descripción
`config.folder.path`	El directorio contiene el archivo `fairscheduler.xml` que contiene la información de propiedades de la agrupación de Spark. El archivo es necesario y se debe crear manualmente. Para obtener más información, consulte la sección **fairscheduler.xml example**.
`resource.pool.mapping`	**Spark:** Correlaciona los inquilinos con las agrupaciones que están definidas en el archivo `fairscheduler.xml`. Los pares de inquilinos deben estar separados por comas (por ejemplo, `tenant1:test,tenant2:production`. Antes de especificar una agrupación, asegúrese de que la agrupación esté configurada en el archivo `fairscheduler.xml`. **MapReduce:** Correlaciona los inquilinos con la cola definida en YARN Queue Manager. Los pares de inquilinos deben estar separados por comas (por ejemplo, tenant1:test,tenant2:production). Antes de especificar una cola, asegúrese de que el sistema esté configurado con la cola, y que el acceso esté permitido para enviar trabajos a la cola. **Nota:** Si desea ejecutar los trabajos Spark y MapReduce juntos, los valores de correlación de inquilinos deben tener el mismo nombre en el archivo `fairscheduler.xml` y en YARN Queue Manager.
`resource.pool.default`	**Spark:** Define la agrupación de recursos predeterminada. El valor puede ser `default` o un nombre de agrupación que esté definido en el archivo `fairscheduler.xml`. Utilice el valor `default` cuando los inquilinos no estén configurados (o estén configurados incorrectamente). **MapReduce:** Define la cola predeterminada a la que se envían los trabajos.
`spark.scheduler.mode=FAIR`	**Spark:** Habilita el planificador limpio. La propiedad no se debe cambiar.
`spark.yarn.queue`	**Spark:** El nombre de la cola YARN a la que se envía la aplicación. Puede especificar un nombre de cola YARN personalizado en el YARN Queue Manager.

4. Guarde la configuración y reinicie el servicio de Analytic Server.

Ejemplo de fairscheduler.xml

El archivo `fairscheduler.xml` contiene la información de propiedades de la agrupación de Spark. El archivo es necesario y se debe crear manualmente.

```
<?xml version="1.0"?>
<allocations>
  <pool name="production">
    <schedulingMode>FAIR</schedulingMode>
    <weight>1</weight>
    <minShare>2</minShare>
```

```
  </pool>
  <pool name="test">
    <schedulingMode>FIFO</schedulingMode>
    <weight>2</weight>
    <minShare>3</minShare>
  </pool>
</allocations>
```

Referencia

Consulte los sitios siguientes para obtener más información:

- https://spark.apache.org/docs/latest/job-scheduling.html#dynamic-resource-allocation
- https://spark.apache.org/docs/latest/running-on-yarn.html

Migración de IBM SPSS Analytic Server en Ambari

Analytic Server puede migrar datos y valores de configuración desde una instalación existente de Analytic Server a una nueva instalación. La migración se puede producir en el mismo entorno de clúster, o en un nuevo entorno de clúster.

Migración de Analytic Server 3.1.2 a 3.2.1 en el mismo clúster de servidores

Si tiene una instalación existente de Analytic Server 3.1.2, puede migrar los valores de configuración de 3.1.2 a su instalación de 3.2.1 en el mismo clúster de servidores.

1. Recopile los valores de configuración de la versión de Analytic Server antigua (Analytic Server 3.1.2).
   a. Expanda el archivador `{AS_ROOT}\tools\unzip configcollector.zip` (creará una carpeta nueva llamada `configcollector`).
   b. Ejecute el script `configcollector.sh` en la carpeta `configcollector`. Copie el archivo comprimido resultante (ZIP) `ASConfiguration_3.1.2.0.xxx.zip` en una ubicación de carpeta distinta (como copia de seguridad).
2. Realice una copia de seguridad de la raíz analítica de la instalación de la versión anterior de Analytic Server 3.1.2 a una nueva ubicación.
   a. Si no está seguro de la ubicación de la raíz analítica, ejecute el mandato **`hadoop fs -ls`**. La vía de acceso a la raíz analítica es similar a `/user/as_user/analytic-root/analytic-workspace`, donde `as_user` es el ID de usuario que es propietario de la raíz analítica.
   b. Utilice los mandatos **`hadoop fs -copyToLocal`** y **`hadoop fs -copyFromLocal`** para copiar la antigua carpeta `analytic-workspace` de la versión Analytic Server en la nueva ubicación (por ejemplo, `/user/as_user/analytic-root/AS31Location`).
3. Si utiliza el Apache Directory Server incorporado, realice una copia de seguridad de la configuración de usuario/grupo actual con una herramienta de cliente LDAP de terceros. Después de que Analytic Server 3.2.1 se instale, importe la configuración de usuario/grupo de copia de seguridad en el servidor de Apache Directory Server.

   Nota: Este paso se puede omitir si utiliza un servidor LDAP externo.
4. Abra la consola la Ambari y detenga el **servicio de Analytic Server**.
5. Desinstale la versión anterior de Analytic Server (Analytic Server 3.1.2) y, a continuación, instale Analytic Server 3.2.1. Para ver las instrucciones de instalación, consulte Capítulo 2, “Instalación y configuración de Ambari”, en la página 3.
6. Abra la consola de Ambari y detenga el **servicio de Analytic Server** (en Ambari, asegúrese de que el **servicio de Analytic Metastore** esté en ejecución).
7. Copie la raíz analítica de Analytic Server 3.1.2 respaldada, desde el paso 2, a la nueva ubicación de la versión de Analytic Server.
   a. Elimine el `analytic-workspace` de la versión recientemente instalada de Analytic Server.

b. Copie la carpeta del espacio de trabajo analítico de Analytic Server 3.1.2 respaldado (/user/as_user/analytic-root/AS31Location) en la nueva ubicación de la versión (por ejemplo, /user/as_user/analytic-root/analytic-workspace). Debe asegurarse de que el propietario del espacio de trabajo analítico esté definido como as_user.

8. Borre el estado de Zookeeper. En el directorio bin de Zookeeper (por ejemplo, /usr/hdp/current/zookeeper-client on Hortonworks), ejecute el mandato siguiente:

```
./zkCli.sh rmr /AnalyticServer
```

9. Copie el archivo de copia de seguridad ASConfiguration_3.1.2.0.xxx.zip desde el paso 1 hasta la nueva ubicación de la versión de Analytic Server (por ejemplo, /opt/ibm/spss/analyticserver/3.2/).
10. Ejecute la herramienta de migración ejecutando el script **migrationtool.sh** y pasando la vía de acceso del archivo de archivado ASConfiguration_3.1.2.0.xxx.zip (que creó el recopilador de la configuración) como un argumento. Por ejemplo:

```
migrationtool.sh /opt/ibm/spss/analyticserver/3.2/ASConfiguration_3.1.2.0.xxx.zip
```

11. Ejecute el mandato siguiente desde un shell de mandatos en el nodo Analytic Server:

```
hadoop fs -chmod -R 755 /user/as_user/analytic-root/analytic-workspace
```

12. En la consola de Ambari, inicie el **servicio de Analytic Server**.

Migración de Analytic Server 3.1.2 a 3.2.1 en un nuevo clúster de servidores

Si tiene una instalación existente de Analytic Server 3.1.2, puede migrar los valores de configuración de 3.1.2 a su instalación de 3.2.1 en un nuevo clúster de servidor.

1. Instale la nueva versión de Analytic Server según las instrucciones en "Instalación en Ambari" en la página 6.
2. Copie el espacio de trabajo analítico de la instalación antigua a la nueva.
   a. Si no está seguro de la ubicación del espacio de trabajo analítico, ejecute hadoop fs -ls. La vía de acceso al espacio de trabajo analítico es similar a /user/as_user/analytic-root/analytic-workspace, donde as_user es el ID de usuario que es el propietario del espacio de trabajo analítico.
   b. Elimine el analytic-workspace en el nuevo servidor.
   c. Utilice hadoop fs -copyToLocal y hadoop fs -copyFromLocal para copiar el espacio de trabajo analítico del servidor antiguo en la carpeta /user/as_user/analytic-root/analytic-workspace de nuevo servidor (asegúrese de que el propietario esté establecido como as_user).
3. Si utiliza el Apache Directory Server incorporado, realice una copia de seguridad de la configuración de usuario/grupo actual con una herramienta de cliente LDAP de terceros. Después de que Analytic Server 3.2.1 se instale, importe la configuración de usuario/grupo de copia de seguridad en el servidor de Apache Directory Server.

   Nota: Este paso se puede omitir si utiliza un servidor LDAP externo.
4. En el nuevo servidor, abra la consola de Ambari y detenga el servicio de Analytic Server (en Ambari, asegúrese de que el servicio de Analytic Metastore está en ejecución).
5. Recopile los valores de configuración de la instalación antigua.
   a. Copie el archivado configcollector.zip de la nueva instalación en {RAÍZ_AS}\tools de la instalación anterior.
   b. Extraiga la copia de configcollector.zip, que crea un nuevo subdirectorio configcollector en la instalación anterior.
   c. Ejecute la herramienta de recopilador de configuración en la instalación existente ejecutando el script **configcollector** en {AS_ROOT}\tools\configcollector. Copie el archivo comprimido resultante (ZIP) en el servidor que aloja su nueva instalación.

   Importante: El script **configcollector** proporcionado no puede ser compatible con la versión de Analytic Server más reciente. Póngase en contacto con el representante de soporte técnico de IBM si encuentra problemas con el scripts **configcollector**.

6. Borre el estado de Zookeeper. En el directorio bin de Zookeeper (por ejemplo, `/usr/hdp/current/zookeeper-client` on Hortonworks), ejecute el mandato siguiente.
   ```
   ./zkCli.sh rmr /AnalyticServer
   ```
7. Ejecute la herramienta de migración ejecutando el script **migrationtool** y pasando la vía de acceso del archivo comprimido que creó el recopilador de la configuración como argumento. A continuación se proporciona un ejemplo.
   ```
   migrationtool.sh /opt/ibm/spss/analyticserver/3.2/ASConfiguration_3.1.2.0.xxx.zip
   ```
8. Ejecute el mandato siguiente desde un shell de mandatos en el nodo Analytic Server:
   ```
   hadoop fs -chmod -R 755 /user/as_user/analytic-root/analytic-workspace
   ```
9. En la consola de Ambari, inicie el servicio Analytic Server.

   Nota: Si ha configurado R para utilizarlo con la instalación de Analytic Server existente, siga los pasos para configurarlo con la nueva instalación de Analytic Server.

Desinstalación

Importante: Cuando tenga instalado Essentials for R, primero debe ejecutar el script `remove_R.sh`. Si no desinstala Essentials for R antes de desinstalar Analytic Server, no podrá desinstalar Essentials for R más adelante. El script `remove_R.sh` se elimina cuando se desinstala Analytic Server. Para obtener información sobre la desinstalación de Essentials for R, consulte "Desinstalación de Essentials for R".

1. En el host de Analytic Metastore, ejecute el script `remove_as.sh` en el directorio `{RAÍZ_AS}/bin` con los parámetros siguientes.

   u Necesario. El ID de usuario del administrador del servidor Ambari.

   p Necesario. La contraseña del administrador del servidor Ambari.

   h Necesario. El nombre de host del servidor Ambari.

   x Necesario. El puerto del servidor Ambari.

   l Opcional. Habilita la modalidad segura.

   A continuación, se muestran ejemplos.
   ```
   remove_as.sh -u admin -p admin -h one.cluster -x 8081
   ```

   Elimina Analytic Server de un clúster con el host de Ambari one.cluster.
   ```
   remove_as.sh -u admin -p admin -h one.cluster -x 8081 -l
   ```

   Elimina Analytic Server de un clúster con el host de Ambari host one.cluster, en la modalidad segura.

Nota: Esta operación elimina la carpeta Analytic Server en HDFS.

Nota: Esta operación no elimina ningún esquema de Db2 asociado a Analytic Server. Consulte la documentación de Db2 para obtener información sobre cómo eliminar esquemas manualmente.

Desinstalación de Essentials for R

1. En el host de Essentials for R, ejecute el script `remove_R.sh` en el directorio `{RAÍZ_AS}/bin` con los parámetros siguientes.

   u Necesario. El ID de usuario del administrador del servidor Ambari.

   p Necesario. La contraseña del administrador del servidor Ambari.

   h Necesario. El nombre de host del servidor Ambari.

   x Necesario. El puerto del servidor Ambari.

l Opcional. Habilita la modalidad segura.

A continuación, se muestran ejemplos.

```
remove_R.sh -u admin -p admin -h one.cluster -x 8081
```

Elimina Essentials for R de un clúster con el host de Ambari one.cluster.

```
remove_R.sh -u admin -p admin -h one.cluster -x 8081 -l
```

Elimina Essentials for R de un clúster con el host de Ambari host one.cluster, en la modalidad segura.

2. Eliminar el directorio de servicios de R del directorio de servicios del servidor Ambari. Por ejemplo, en HDP 2.6, el directorio `ESSENTIALR` se encuentra en `/var/lib/ambari-server/resources/stacks/HDP/2.6/services`.
3. En la consola de Ambari, verifique que el servicio Essentials for R ya no exista.

Capítulo 3. Instalación y configuración de Cloudera

Visión general de Cloudera

Cloudera es distribución de Apache Hadoop de un código abierto. CDH (Cloudera Distribution Including Apache Hadoop) está orientado a despliegues de clase de empresa de dicha tecnología.

Analytic Server puede ejecutarse en la plataforma de CDH. CDH contiene los elementos principales y más importantes de Hadoop que un proceso de datos distribuidos, fiable y escalable, de grandes conjuntos de datos (principalmente MapReduce y HDFS), así como otros componentes orientados a empresa que proporcionan seguridad, alta disponibilidad y la integración con otro tipo de hardware y software.

Requisitos previos específicos de Cloudera

Además de los requisitos previos generales, revise la información siguiente.

Servicios

Asegúrese de que las instancias siguientes estén instaladas en cada host de Analytic Server.

- HDFS: Gateway, DataNode o NameNode
- Hive: Gateway, Hive Metastore Server o HiveServer2
- Yarn: Gateway, ResourceManager o NodeManager

Las instancias siguientes sólo son necesarias cuando se utilizan sus características:

- Accumulo: Gateway
- HBase: Gateway, Master o RegionServer
- Spark: Gateway
- Spark 2: Gateway

Repositorio de metadatos

Puede utilizar Db2 y MySQL como repositorio de metadatos de Analytic Server. Si tiene previsto utilizar MySQL como repositorio de metadatos de Analytic Server, siga las instrucciones que figuran en “Configuración de MySQL para Analytic Server” en la página 39.

Entornos de Cloudera habilitados para Kerberos

Si tiene previsto instalar Analytic Server en un entorno de Cloudera habilitado para Kerberos, debe verificar que Kerberos esté correctamente configurado de una forma compatible con Analytic Server.

Las secciones siguientes se aplican a entornos de Cloudera en los que ya está instalado Kerberos. Se deben seguir las secciones siguientes antes de instalar Analytic Server en Cloudera. Se presupone que tiene conocimientos básicos de autenticación Kerberos, ya que las secciones incluyen terminología específica de Kerberos (por ejemplo, **`kinit`**, **`kadmin`**, etc.).

Nota: Analytic Server inspecciona la configuración de HDFS para que los valores relacionados con Kerberos se utilicen para la autenticación.

Autenticación Kerberos

Verifique que la autenticación Kerberos se haya configurado en cada nodo de clúster de Cloudera antes de instalar Analytic Server. Para obtener más información, consulte Configuración de la autenticación en Cloudera Manager en la documentación del producto Cloudera.

Nota: Después de configurar la autenticación Kerberos en cada nodo de clúster Cloudera, se deben reiniciar los servicios **cloudera-scm-server** y **cloudera-scm-agent** antes de instalar Analytic Server. El servicio **cloudera-scm-agent** debe reiniciarse en todos los nodos de clúster.

Creación de las cuentas necesarias en Kerberos

1. Cree cuentas en el repositorio de usuarios de Kerberos para todos los usuarios a los que tiene previsto otorgar acceso a Analytic Server.
2. Cree las mismas cuentas (desde el paso anterior) en el servidor LDAP.
3. Cree una cuenta de usuario de sistema operativo para cada uno de los usuarios creados en el paso anterior en todos los nodos de Analytic Server y en el nodo de Hadoop.
   - Asegúrese de que el ID de usuario de estos usuarios coincide en todas las máquinas. Puede probar esto utilizando el mandato `kinit` para iniciar la sesión en cada una de las cuentas.
   - Asegúrese de que el UID cumple el valor de Yarn **ID de usuario mínimo para enviar trabajo**. Este es el valor de **min.user.id** en `container-executor.cfg`. Por ejemplo, si **min.user.id** es 1000, cada cuenta de usuario creada debe tener un UID mayor o igual que 1000.
4. Cree una carpeta de inicio de usuario en HDFS para el usuario administrador de Analytic Server. El permiso de carpeta debe establecerse en 777, el propietario debe definirse como `admin`, y el grupo de usuarios debe establecerse como `hdfs`. Consulte el ejemplo siguiente, en negrita:

```
[root@xxxxx configuration]# hadoop fs -ls /user

Found 9 items

drwxrwxrwx   - hdfs     supergroup      0 2017-07-26 03:41 /user/AE
drwxrwxrwx   - admin    hdfs            0 2017-06-08 01:33 /user/admin
drwxr-x--x   - as_user  hdfs            0 2017-06-06 01:00 /user/as_user
drwx------   - hdfs     supergroup      0 2017-07-31 00:17 /user/hdfs
drwxrwxrwx   - mapred   hadoop          0 2017-06-05 00:28 /user/history
drwxrwxr-t   - hive     hive            0 2017-06-05 00:30 /user/hive
drwxrwxr-x   - hue      hue             0 2017-06-05 00:30 /user/hue
drwxrwxr-x   - impala   impala          0 2017-07-19 00:52 /user/impala
drwxr-x--x   - spark    spark           0 2017-06-05 01:34 /user/spark
```

5. Si tiene previsto utilizar los orígenes de datos de HCatalog y Analytic Server está instalado en una máquina distinta del metastore de Hive, tiene que suplantar al cliente de Hive en HDFS.
   a. Vaya hasta la pestaña Configuración del servicio HDFS en Cloudera Manager.

      Nota: Los valores siguientes pueden no aparecer en la pestaña **Configuración** si todavía no se han establecido. En este caso, ejecute una búsqueda para encontrarlos.

   b. Edite el valor **hadoop.proxyuser.hive.groups** para que tenga el valor `*`, o un grupo que contenga todos los usuarios permitidos para iniciar la sesión en Analytic Server.
   c. Edite el valor **hadoop.proxyuser.hive.hosts** para que tenga el valor `*` o la lista de hosts en los que están instalados como servicios el metastore de Hive y todas las instancias de Analytic Server.
   d. Reinicie el servicio HDFS.

Después de que se hayan realizado estos pasos y esté instalado Analytic Server, Analytic Server configurará de forma silenciosa y automática Kerberos.

Habilitación de la suplantación de Kerberos

La suplantación permite ejecutar un hilo en un contexto de seguridad que difiere del contexto de seguridad del proceso que es propietario de la hebra. Por ejemplo, la suplantación proporciona un medio para que los trabajos de Hadoop se ejecuten como otros usuarios que no sean los usuarios estándar de Analytic Server (`as_user`). Para habilitar la suplantación de Kerberos:

1. Abra Cloudera Manager y añada o actualice las propiedades siguientes en el área **Cluster-wide Advanced Configuration Snippet (Safety Valve) for core-site.xml** (situada en la pestaña **HDFS (Service-Wide)** > **Configuration**).
   - **Nombre:** `hadoop.proxyuser.as_user.hosts`
   - **Valor:** `*`

- **Nombre:** `hadoop.proxyuser.as_user.groups`
- **Valor:** `*`

Nota: Los valores de **core-site.xml** se aplican a la configuración de Hadoop (no a Analytic Server).

2. Ejecute el mandato siguiente desde un shell de mandatos en el nodo Analytic Server:
   ```
   hadoop fs -chmod -R 755 /user/as_user/analytic-root/analytic-workspace
   ```

Configuración de MySQL para Analytic Server

La configuración de IBM SPSS Analytic Server en Cloudera Manager requiere la instalación y configuración de una base de datos de servidor MySQL.

1. Ejecute el mandato siguiente desde una ventana de mandatos en el nodo en el que se almacene la base de datos MySQL:
   ```
   yum install mysql-server
   ```

   Nota: Utilice `zypper install mysql` en SuSE Linux.

2. Ejecute el mandato siguiente desde una ventana de mandatos, en cada nodo de clúster de Cloudera:
   ```
   yum install mysql-connector-java
   ```

   Nota: Utilice `sudo zypper install mysql-connector-java` para SuSE Linux.

3. Decida, y tome nota de, el nombre de base de datos, el nombre de usuario de bases de datos y la contraseña de base de datos de Analytic Server que Analytic Server utilice cuando acceda a la base de datos MySQL.
4. Instale Analytic Server de acuerdo a las instrucciones de "Instalación en Cloudera" en la página 41.
5. Copie el script `/opt/cloudera/parcels/AnalyticServer/bin/add_mysql_user.sh` de uno de los servidores gestionados por Cloudera al nodo en el que se haya instalado la base de datos MySQL. Ejecute el script con los parámetros apropiados para su configuración en particular. Por ejemplo:
   ```
   ./add_mysql_user.sh -u <nombre_usuario_base_datos> -p <contraseña_base_datos> -d
   <nombre_base_datos>
   ```

   Notas: El parámetro a `-r <contraseña_root_BD)` es necesario cuando la base de datos se ejecuta en modalidad segura (se ha establecido la contraseña del usuario root).

   Los parámetros `-r <contraseña_usuario_BD>` y `-t <nombre_usuario_BD>` son necesarios cuando la base de datos se esté ejecutando en modalidad segura con un nombre de usuario que no sea `root`.

Herramientas de comprobación previa y posterior a la instalación - Cloudera

Ubicación y requisitos previos de la herramienta

Antes de instalar el servicio Analytic Server, ejecute la herramienta de comprobación previa en todos los nodos que forman parte del servicio Analytic Server para verificar que su entorno Linux ya está instalado Analytic Server.

La herramienta de comprobación previa se invoca automáticamente como parte de la instalación. La herramienta realiza una comprobación de cada nodo de Analytic Server antes de ejecutar la instalación en cada host. También puede invocar manualmente la herramienta de comprobación previa en cada nodo, que puede validar la máquina antes de instalar el servicio.

Después de ejecutar el archivo binario de Analytic Server autoextraíble, la herramienta de comprobación previa se encuentra en los directorios siguientes:

- **Cloudera**

```
/opt/cloudera/parcels/AnalyticServer-3.2.1.0/tools/com.spss.ibm.checker.zip

[root@servername ~]# cd /opt/cloudera/parcels/AnalyticServer-3.2.1.0/tools/
[root@servername tools]# ls
com.spss.ibm.checker.zip configcollector.zip regex-files
```

Nota: La herramienta de comprobación previa no estará disponible en el directorio `tools` hasta que se ejecuta el archivo binario ejecutable y, a continuación, se distribuye (**Descargar** > **Distribuir**) y se activa Analytic Server en la página Paquetes de Cloudera Manager.

Después de instalar Analytic Server, la herramienta de comprobación posterior se encuentra en el siguiente directorio:

- **Cloudera**

  ```
  /opt/cloudera/parcels/AnalyticServer-3.2.1.0/tools/com.spss.ibm.checker.zip
  ```

Las herramientas deben ejecutarse como root y requieren Python 2.6.X (o superior).

Si la herramienta de comprobación previa informa de alguna anomalía, ésta debe abordarse antes de continuar con la instalación de Analytic Server.

Ejecución de la herramienta de comprobación previa

Automático

La herramienta de comprobación previa puede invocarse automáticamente como parte de la instalación de Analytic Server cuando Analytic Server se ha instalado como servicio mediante la consola de Cloudera Manager. Deberá especificar manualmente el nombre de usuario y la contraseña del administrador de Cloudera Manager:

Figura 4. Valores del administrador de Cloudera Manager

Manual

Puede invocar manualmente la herramienta de comprobación previa en cada nodo de clúster.

El ejemplo siguiente de comprobación previa comprueba el clúster de Cloudera `MyCluster` que se ejecuta en `myclouderahost.ibm.com:7180`, y utiliza las credenciales de inicio de sesión `admin:admin`:

```
python ./precheck.py --target C --cluster MyCluster --username admin
--password admin --host myclouderahost.ibm.com --port 7180 --as_host myashost.ibm.com
```

Notas:

- El valor `as_host` debe proporcionarse mediante la dirección IP o un nombre de dominio completo.
- La herramienta solicita una contraseña cuando se omite el argumento de contraseña.
- El mandato `precheck.py` incluye ayuda para su utilización, que se muestra con el argumento `--h` (`python ./precheck.py --help`).
- El argumento `--cluster` es opcional (el clúster actual se identifica cuando `--cluster` no se utiliza).

A medida que la herramienta de comprobación previa ejecuta sus comprobaciones, se muestra el estado de cada comprobación en la ventana de mandatos. Cuando se produce un error, encontrará información detallada en el archivo de registro (la ubicación exacta del archivo de registro se proporciona en la ventana de mandatos). El archivo de registro puede proporcionarse al servicio de soporte técnico de IBM cuando se necesita ayuda adicional.

Ejecución de la herramienta de comprobación posterior

La herramienta de comprobación posterior verifica que Analytic Server se está ejecutando correctamente y puede procesar trabajos simples. El ejemplo de comprobación posterior siguiente comprueba una instancia de Analytic Server que se ejecuta en `myanalyticserverhost.ibm.com:9443`, con SSL habilitado, y utiliza las credenciales de inicio de sesión: `admin:ibmspss`

```
python ./postcheck.py --host myanalyticserverhost.ibm.com --port 9443
--username admin --password ibmspss --ssl
```

Cuando se utiliza Knox con Analytic Server, el mandato es el siguiente:

```
python ./postcheck.py --host myknoxserverhost.ibm.com --port 8443
--username admin --password ibmspss --ssl --gateway_url /gateway/default
```

Para realizar una sola comprobación, utilice el mandato siguiente:

```
python ./postcheck.py --host myknoxserverhost.ibm.com --port 8443
--username admin --password ibmspss --ssl --gateway_url /gateway/default --check AS_PYSPARK_BUILDMODEL
```

Notas:

- La herramienta solicita una contraseña cuando se omite el argumento de contraseña.
- El mandato `postcheck.py` incluye ayuda para su utilización, que se muestra con el argumento `--h` (`python ./postcheck.py --help`).

A medida que la herramienta de comprobación posterior ejecuta sus comprobaciones, se muestra el estado de cada comprobación en la ventana de mandatos. Cuando se produce un error, encontrará información detallada en el archivo de registro (la ubicación exacta del archivo de registro se proporciona en la ventana de mandatos). El archivo de registro puede proporcionarse al servicio de soporte técnico de IBM si se necesita ayuda adicional.

Instalación en Cloudera

En los pasos siguientes se explica el proceso de instalar IBM SPSS Analytic Server manualmente en Cloudera Manager.

Analytic Server 3.2.1

Instalación en línea

1. Navegue hasta el Sitio web de IBM Passport Advantage® y descargue el archivo binario autoextraíble específico de su pila, versión de pila y arquitectura de hardware en un sistema principal que se encuentre dentro del clúster Cloudera. Los binarios de Cloudera disponibles son:

Tabla 9. Archivos binarios autoextraíbles de Analytic Server

Descripción	Nombre del archivo binario
IBM SPSS Analytic Server 3.2.1 para Cloudera 5.11, 5.12, 5.13, 5.14, 5.15, 6.0 y 6.1, Ubuntu, inglés	`spss_as-3.2.1.0-cdh5.11-6.1-ubun.bin`
IBM SPSS Analytic Server 3.2.1 para Cloudera 5.11, 5.12, 5.13, 5.14, 5.15, 6.0 y 6.1, Linux x86-64, inglés	`spss_as-3.2.1.0-cdh5.11-6.1-lx86.bin`

2. Ejecute el instalador autoextraíble de Cloudera `*.bin` en el nodo de clúster maestro de Cloudera Manager. Siga las indicaciones de la instalación, aceptando el acuerdo de licencia y manteniendo el directorio de instalación de CSD predeterminado.

   Nota: Debe especificar un directorio CSD diferente si se ha modificado el de la ubicación predeterminada.
3. Utilice el mandato siguiente para reiniciar Cloudera Manager después de que se haya completado la instalación:

   ```
   service cloudera-scm-server restart
   ```
4. Abra la interfaz de Cloudera Manager (por ejemplo, `http://${CM_HOST}:7180/cmf/login` con las credenciales de inicio de sesión predeterminadas de `admin/admin`), renueve las **Remote Parcel Repository URLs** (ubicadas en **Host** > **Parcels** > **click Configuration**) y verifique que los URL sean correctos. Por ejemplo:

   ```
   https://ibm-open-platform.ibm.com
   ```

   Nota: Los valores **Parcel Update Frequency** y **Remote Parcel Repository URLs** pueden actualizarse para que se ajusten sus necesidades específicas.
5. Después de que Cloudera Manager renueva los paquetes (puede renovarlos manualmente pulsando **Check for New Parcels**), verá que el estado del paquete **AnalyticServer** se ha establecido en **Available Remotely**.
6. Seleccione **Download** > **Distribute** > **Activate**. El estado del paquete **AnalyticServer** se actualiza a **Distributed, Activated**.
7. En Cloudera Manager, añada Analytic Server como un servicio, y decida dónde colocar Analytic Server. Debe proporcionar la información siguiente en Add Service Wizard:

   Nota: El asistente Add Service Wizard muestra el progreso global durante cada fase del proceso de creación de servicios, y proporcionará un mensaje de confirmación final cuando el servicio se haya instalado y configurado correctamente en el clúster.
   - Nombre de host de metastore de Analytic Server
   - Nombre de base de datos de metastore de Analytic Server
   - Nombre de usuario de metastore de Analytic Server
   - Contraseña de metastore de Analytic Server

   MySQL como repositorio de metadatos de Analytic Server
   - Clase de controlador de metastore de Analytic Server: `com.mysql.jdbc.Driver`
   - URL del repositorio de metastore de Analytic Server: `jdbc:mysql://${MySQL_DB}/{DBName}?createDatabaseIfNotExist=true`

     `{MySQL_DB}` es el nombre de host del servidor donde está instalado MySQL

   Db2 como repositorio de metadatos de Analytic Server
   - Clase de controlador de metastore de Analytic Server: `com.ibm.db2.jcc.DB2Driver`

- URL del repositorio de metastore de Analytic Server: `jdbc:db2://{Db2_HOST}:{PORT}/{DBName}:currentSchema={SchemaName};`

  `{Db2_HOST}` es el nombre de host del servidor donde está instalado Db2.

  `{PORT}` es el puerto en el que Db2 escucha.

  `{SchemaName}` es un esquema disponible, no utilizado.

  Trabaje con el administrador de Db2 si no está seguro de los valores que deben especificarse.

Configuración de LDAP

Analytic Server utiliza un servidor LDAP para almacenar y autenticar usuarios y grupos. Proporcione la información de configuración de LDAP necesaria durante la instalación de Analytic Server.

Tabla 10. Valores de configuración de LDAP

Valor de LDAP	Descripción
`as.ldap.type`	Tipo de LDAP. El valor puede ser `ads`, `ad` u `openladp`. • `ads` - Apache Directory Server (valor predeterminado) • `ad` - Microsoft Active Directory • `openladp` - OpenLDAP
`as.ldap.host`	Host LDAP
`as.ldap.port`	Número de puerto LDAP
`as.ldap.binddn`	DN de enlace de LDAP
`as.ldap.bindpassword`	Contraseña de DN de enlace de LDAP
`as.ldap.basedn`	DN base LDAP
`as.ldap.filter`	Regla de filtro de usuario y grupo de LDAP **Nota:** Cuando este valor contenga caracteres de barra vertical `|`, los caracteres deben escaparse con caracteres de barra inclinada invertida (por ejemplo, `\\|`).
`as.ldap.ssl.enabled`	Especifica si se debe utilizar SSL para comunicarse entre Analytic Server y LDAP. El valor puede ser `true` o `false`.
`as.ldap.ssl.reference`	ID de referencia SSL de LDAP
`as.ldap.ssl.content`	Configuración SSL de LDAP

- De forma predeterminada, `as.ldap.type` se establece en `ads` y los otros valores relacionados contienen valores predeterminados. La excepción es que debe proporcionar una contraseña para el valor `as.ldap.bindpassword`. Analytic Server utiliza los valores de configuración para instalar un servidor de Apache Directory Server (ADS) y ejecutar la inicialización del servidor. El perfil de ADS predeterminado incluye el usuario `admin` con una contraseña de `admin`. Puede llevar a cabo la gestión de usuarios a través de la consola de Analytic Server o importar la información de usuarios y de grupos desde un archivo XML mediante el script `importUser.sh` que se encuentra en la carpeta `<Analytic Root>/bin`.
- Si tiene previsto utilizar un servidor LDAP externo, como por ejemplo Microsoft Active Directory u OpenLDAP, debe definir los valores de configuración según los valores de LDAP reales. Para obtener más información, consulte Configuración de registros de usuarios de LDAP en Liberty.
- Puede cambiar la configuración de LDAP después de que se haya instalado Analytic Server (por ejemplo, cambiar de Apache Directory Server a OpenLDAP). Sin embargo, si inicialmente se empieza con Microsoft Active Directory u OpenLDAP, y decide cambiar posteriormente a Apache Directory Server, Analytic Server no instalará un servidor de Apache Directory Server durante la instalación. Apache Directory Server solo se instala cuando se selecciona durante la instalación inicial de Analytic Server.

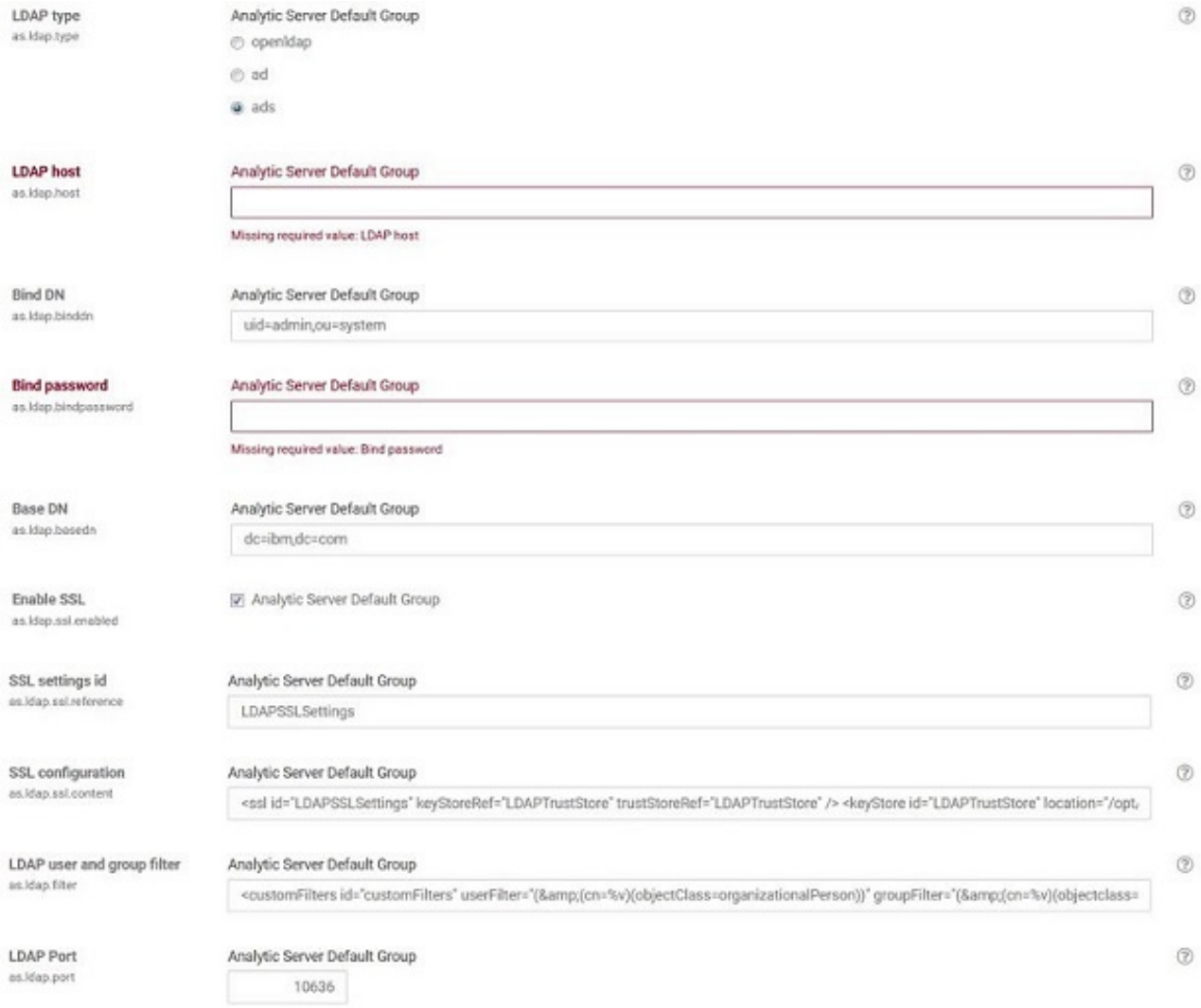

Figura 5. Valores de configuración de LDAP de ejemplo

8. Al instalar Analytic Server en un entorno de Cloudera habilitado para Kerberos, también se deben configurar los valores siguientes en el Asistente para añadir servicio:

   Nota: Analytic Server inspecciona la configuración de HDFS para que los valores relacionados con Kerberos se utilicen para la autenticación.

   - Seleccione `Kerberos` como el valor de **Seguridad de Analytic Server** si desea habilitar la autenticación Kerberos al iniciar sesión en la consola de Analytic Server. Cuando se selecciona **Kerberos** como el valor de **Seguridad de Analytic Server**, la consola de Analytic Server toma de forma predeterminada el modo de inicio de sesión de Kerberos.
   - Seleccione `Kerberos` como el valor de **Método de conexión de origen de datos de base de datos de Analytic Server** cuando desee conectarse a las bases de datos habilitadas para Kerberos. Cuando se selecciona **Kerberos** como valor del **Método de conexión de origen de datos de base de datos de Analytic Server**, la consola de Analytic Server utiliza la modalidad Kerberos al conectarse a una base de datos
   - Los valores de **Nombre de dominio de Kerberos** y **Host de KDC** son obligatorios. Los valores de **Nombre de dominio de Kerberos** (**`as.kdc.realms`**) y **Host de KDC** (**`kdcserver`**) se encuentran en el archivo `krb5.conf` en el servidor del centro de distribución de claves (KDC) de Kerberos.

Se admiten varios nombres de dominios cuando están separados por comas. Los nombres de dominio Kerberos especificados corresponden a nombres de usuario y están asociados a los mismos. Por ejemplo, los nombres de usuario `UserOne@us.ibm.com` y `UserTwo@eu.ibm.com` corresponderían a los dominios `us.ibm.com,eu.ibm.com`.

Se deben configurar confianzas entre dominios de Kerberos cuando se especifica más de un dominio como **Nombre de dominio de Kerberos**. El nombre de usuario que se especifica durante la solicitud de inicio de sesión en la consola de Analytic Server se especifica sin el sufijo de nombre de dominio. Como resultado, cuando se especifican varios dominios, se presenta a los usuarios una lista desplegable de **Dominios** que les permite seleccionar el dominio adecuado.

Nota: Cuando sólo se especifica un dominio, no se presenta a los usuarios ninguna lista despegable **Dominios** al iniciar sesión en Analytic Server.

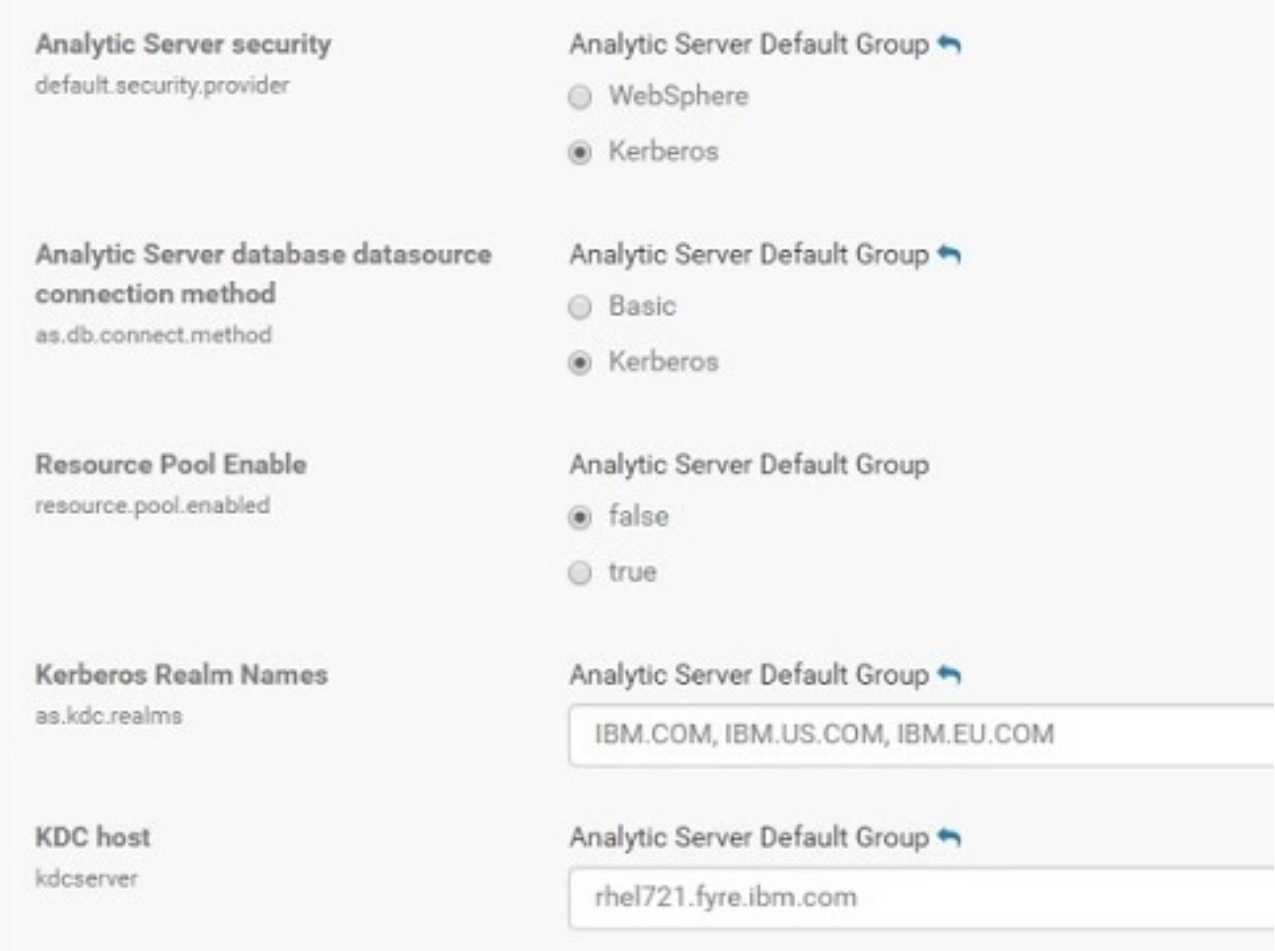

Figura 6. Valores de Kerberos de ejemplo

Notas:

- Los valores **Seguridad de Analytic Server** y **Método de conexión de origen de datos de base de datos de Analytic Server** son aplicables al cliente de IBM SPSS Modeler y a la autenticación de la consola de Analytic Server.
- Cuando el **método de conexión de origen de datos de base de datos de Analytic Server** se establece en `Kerberos`, debe asegurarse de que las bases de datos de destino también estén habilitadas para Kerberos.

- Los valores de **Seguridad de Analytic Server** y **Método de conexión de origen de datos de base de datos de Analytic Server** no configuran la autenticación Kerberos en el clúster de Hadoop. Para obtener más información, consulte la sección "Habilitación de la suplantación de Kerberos".
- Si desea que la autenticación Kerberos esté habilitada en el inicio de sesión, debe desplegar el cliente de IBM SPSS Modeler como un cliente Kerberos válido. Esto se consigue utilizando el mandato **addprinc** en el servidor del centro de distribución de claves (KDC) de Kerberos. Para obtener más información, consulte la documentación de IBM SPSS Modeler.

Al instalar Analytic Server en un entorno de Cloudera habilitado para Kerberos, también debe crear las cuentas necesarias en Kerberos y habilitar la suplantación de Kerberos. Para obtener más información, consulte “Configuración de Kerberos” en la página 48.

Nota: Tras instalar correctamente Analytic Server, no pulse **Create Analytic Server Metastore** en la lista de Acciones en la página de servicios de Analytic Server en Cloudera Manager. La creación de un Metastore sobrescribe el repositorio de metadatos existente.

Instalación fuera de línea

Los pasos de instalación fuera de línea son los mismos que los de la instalación en línea, excepto que debe descargar manualmente los archivos de paquetes y de metadatos que resultan adecuados para su sistema operativo en particular.

RedHat Linux requiere los archivos siguientes:
- AnalyticServer-3.2.1.0-el7.parcel
- AnalyticServer-3.2.1.0-el7.parcel.sha
- manifest.json

SuSE Linux requiere los archivos siguientes:
- AnalyticServer-3.2.1.0-sles11.parcel
- AnalyticServer-3.2.1.0-sles11.parcel.sha
- manifest.json

  o bien
- AnalyticServer-3.2.1.0-sles12.parcel
- AnalyticServer-3.2.1.0-sles12.parcel.sha

Ubuntu Linux 14.04 requiere los archivos siguientes:
- AnalyticServer-3.2.1.0-trusty.parcel
- AnalyticServer-3.2.1.0-trusty.parcel.sha

Ubuntu Linux 16.04 requiere los archivos siguientes:
- AnalyticServer-3.2.1.0-xenial.parcel
- AnalyticServer-3.2.1.0-xenial.parcel.sha

1. Descargue y ejecute el instalador autoextraíble de Cloudera `*.bin` en el nodo de clúster maestro de Cloudera Manager. Siga las solicitudes de instalación aceptando el acuerdo de licencia y manteniendo el directorio de instalación `CSD` predeterminado.

   Nota: Debe especificar un directorio `CSD` diferente si difiere de la ubicación predeterminada.
2. Copie los archivos de metadatos y de paquete necesarios en la vía de acceso `repo` de Cloudera en el nodo de clúster maestro de Cloudera Manager. La vía de acceso predeterminada es `/opt/cloudera/parcel-repo` (la vía de acceso se puede configurar en la interfaz de usuario de Cloudera Manager).
3. Utilice el mandato siguiente para reiniciar Cloudera Manager:

```
service cloudera-scm-server restart
```

El paquete **AnalyticServer** aparecerá como **downloaded** después de que Cloudera Manager renueve el paquete. Puede pulsar **Check for New Parcels** para forzar una renovación.

4. Pulse **Distribute** > **Activate**.

   El paquete **AnalyticServer** se mostrará como distribuido y activado.

5. En Cloudera Manager, añada Analytic Server como servicio. Consulte los pasos 7 y 8 en la sección "Instalación en línea" para obtener más información.

Configuración de Cloudera

Después de la instalación, si lo desea puede configurar y administrar Analytic Server a través de Cloudera Manager.

Nota: Para las vías de acceso de archivo de Analytic Server se utilizan las convenciones siguientes.

- {RAÍZ_AS} hace referencia a la ubicación en la que se ha desplegado Analytic Server; por ejemplo, `/opt/cloudera/parcels/AnalyticServer`.
- {RAÍZ_SERVIDOR_AS} hace referencia a la ubicación de los archivos de configuración, registro y servidor; por ejemplo, `/opt/cloudera/parcels/AnalyticServer/ae_wlpserver/usr/servers/aeserver`.
- {INICIO_AS} hace referencia a la ubicación de HDFS que utiliza Analytic Server como carpeta raíz; por ejemplo, `/user/as_user/analytic-root`.

Seguridad

El valor predeterminado de **`tenant_id`** del archivo `options.cfg` de IBM SPSS Modeler es **`ibm`**. Puede ver inquilinos en la consola de Analytic Server. Consulte la *Guía del administrador de IBM SPSS Analytic Server* para obtener detalles sobre la gestión del inquilino.

Configurar un registro LDAP

LDAP se configura durante la instalación de Analytic Server. Puede cambiar a otro método de servidor LDAP después de la instalación de Analytic Server.

Nota: Soporte para LDAP en Analytic Server está controlado por WebSphere Liberty. Para obtener más información, consulte Configuración de registros de usuarios de LDAP en Liberty.

Configurar una conexión SSL (capa de sockets seguros) de Analytic Server a LDAP

1. Inicie la sesión en todas las máquinas de Analytic Server como el usuario de Analytic Server y cree un directorio común para los certificados SSL.

   Nota: En Cloudera, el usuario de Analytic Server es siempre as_user, y no se puede cambiar.

2. Copie los archivos de almacén de claves y de almacén de confianza en algún directorio común en todas las máquinas de Analytic Server. Además, añada el certificado de autoridad emisora de certificados LDAP al almacén de confianza. A continuación figuran algunas instrucciones de ejemplo.

   ```
   mkdir /home/as_user/security
   cd /home/as_user/security
   openssl s_client -connect <nombre_host_LDAP>:636 -showcerts > client.cert
   $JAVA_HOME/bin/keytool -import -file ./client.cert -alias ldapCA -keystore mytrust.jks
   password : changeit
   ```

   Nota: JAVA_HOME es el mismo JRE utilizado para el inicio de Analytic Server.

3. Las contraseñas pueden codificarse para ocultar sus valores con la herramienta securityUtility, ubicada en `{RAÍZ_AS}/ae_wlpserver/bin`. A continuación se proporciona un ejemplo.

   ```
   securityUtility encode changeit
            {xor}PDc+MTg6Nis=
   ```

4. Inicie la sesión en Cloudera Manager y actualice el valor de configuración **ssl_cfg** de Analytic Server con los valores de configuración SSL correctos. A continuación se proporciona un ejemplo.

```
<ssl id="defaultSSLConfig" keyStoreRef="defaultKeyStore" trustStoreRef="defaultTrustStore"
      clientAuthenticationSupported="true"/>
          <keyStore id="defaultKeyStore" location="/home/as_user/security/mykey.jks" type="JKS"
                    password="{xor}Ozo5PiozKxYdEgwPDAweDG1uDz4sLCg7"/>
          <keyStore id="defaultTrustStore" location="/home/as_user/security/mytrust.jks" type="JKS"
                    password="{xor}PDc+MTg6Nis="/>
```

   Nota: utilice la vía de acceso absoluta para los archivos de almacén de claves y de almacén de confianza.

5. Actualice el valor de configuración **security_cfg** de Analytic Server con los valores de configuración LDAP correctos. Por ejemplo, en el elemento **ldapRegistry**, establezca el atributo **sslEnabled** en `true` y el atributo **sslRef** en `defaultSSLConfig`.

Configuración de Kerberos

Analytic Server admite Kerberos en Cloudera. En las secciones siguientes se proporcionan los valores de configuración para asegurarse de que Kerberos se ha configurado correctamente de una forma compatible con Analytic Server.

Nota: Analytic Server inspecciona la configuración de HDFS para que los valores relacionados con Kerberos se utilicen para la autenticación.

Valores de Analytic Server y Kerberos

Tenga en cuenta los valores siguientes al instalar Analytic Server en un entorno de Cloudera habilitado para Kerberos.

- Seleccione `Kerberos` como el valor de **Seguridad de Analytic Server** si desea habilitar la autenticación Kerberos al iniciar sesión en la consola de Analytic Server. Cuando se selecciona **Kerberos** como el valor de **Seguridad de Analytic Server**, la consola de Analytic Server toma de forma predeterminada el modo de inicio de sesión de Kerberos.
- Seleccione `Kerberos` como el valor de **Método de conexión de origen de datos de base de datos de Analytic Server** cuando desee conectarse a las bases de datos habilitadas para Kerberos. Cuando se selecciona **Kerberos** como valor del **Método de conexión de origen de datos de base de datos de Analytic Server**, la consola de Analytic Server utiliza la modalidad Kerberos al conectarse a una base de datos
- Los valores de **Nombre de dominio de Kerberos** y **Host de KDC** son obligatorios. Los valores de **Nombre de dominio de Kerberos** (**as.kdc.realms**) y **Host de KDC** (**kdcserver**) se encuentran en el archivo `krb5.conf` en el servidor del centro de distribución de claves (KDC) de Kerberos.

  Se admiten varios nombres de dominios cuando están separados por comas. Los nombres de dominio Kerberos especificados corresponden a nombres de usuario y están asociados a los mismos. Por ejemplo, los nombres de usuario `UserOne@us.ibm.com` y `UserTwo@eu.ibm.com` corresponderían a los dominios `us.ibm.com,eu.ibm.com`.

  Se deben configurar confianzas entre dominios de Kerberos cuando se especifica más de un dominio como **Nombre de dominio de Kerberos**. El nombre de usuario que se especifica durante la solicitud de inicio de sesión en la consola de Analytic Server se especifica sin el sufijo de nombre de dominio. Como resultado, cuando se especifican varios dominios, se presenta a los usuarios una lista desplegable de **Dominios** que les permite seleccionar el dominio adecuado.

  Nota: Cuando sólo se especifica un dominio, no se presenta a los usuarios ninguna lista despegable **Dominios** al iniciar sesión en Analytic Server.

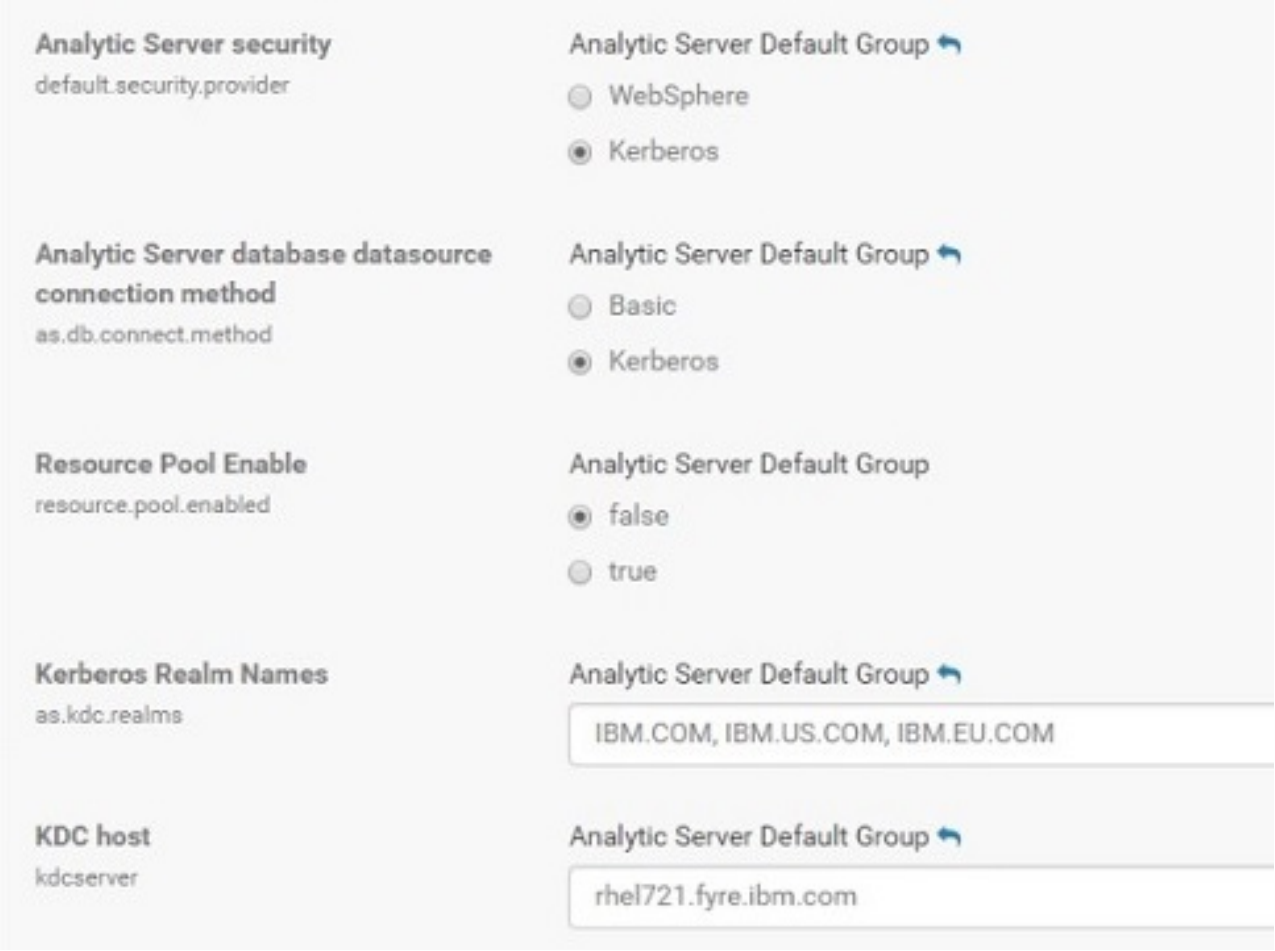

Figura 7. Valores de Kerberos de ejemplo

Notas:

- Los valores **Seguridad de Analytic Server** y **Método de conexión de origen de datos de base de datos de Analytic Server** son aplicables al cliente de IBM SPSS Modeler y a la autenticación de la consola de Analytic Server.
- Cuando el **método de conexión de origen de datos de base de datos de Analytic Server** se establece en `Kerberos`, debe asegurarse de que las bases de datos de destino también estén habilitadas para Kerberos.
- Los valores de **Seguridad de Analytic Server** y **Método de conexión de origen de datos de base de datos de Analytic Server** no configuran la autenticación Kerberos en el clúster de Hadoop. Para obtener más información, consulte la sección "Habilitación de la suplantación de Kerberos".
- Si desea que la autenticación Kerberos esté habilitada en el inicio de sesión, debe desplegar el cliente de IBM SPSS Modeler como un cliente Kerberos válido. Esto se consigue utilizando el mandato **`addprinc`** en el servidor del centro de distribución de claves (KDC) de Kerberos. Para obtener más información, consulte la documentación de IBM SPSS Modeler.

Creación de las cuentas necesarias en Kerberos

1. Cree cuentas en el repositorio de usuarios de Kerberos para todos los usuarios a los que tiene previsto otorgar acceso a Analytic Server.
2. Cree las mismas cuentas (desde el paso anterior) en el servidor LDAP.
3. Cree una cuenta de usuario de sistema operativo para cada uno de los usuarios creados en el paso anterior en todos los nodos de Analytic Server y en el nodo de Hadoop.

- Asegúrese de que el ID de usuario de estos usuarios coincide en todas las máquinas. Puede probar esto utilizando el mandato `kinit` para iniciar la sesión en cada una de las cuentas.
- Asegúrese de que el UID cumple el valor de Yarn **ID de usuario mínimo para enviar trabajo**. Este es el valor de **`min.user.id`** en `container-executor.cfg`. Por ejemplo, si **`min.user.id`** es 1000, cada cuenta de usuario creada debe tener un UID mayor o igual que 1000.

4. Cree una carpeta de inicio de usuario en HDFS para el usuario administrador de Analytic Server. El permiso de carpeta debe establecerse en `777`, el propietario debe definirse como `admin`, y el grupo de usuarios debe establecerse como `hdfs`. Consulte el ejemplo siguiente, en negrita:

```
[root@xxxxx configuration]# hadoop fs -ls /user

Found 9 items

drwxrwxrwx   - hdfs     supergroup      0 2017-07-26 03:41 /user/AE
drwxrwxrwx   - admin    hdfs            0 2017-06-08 01:33 /user/admin
drwxr-x--x   - as_user  hdfs            0 2017-06-06 01:00 /user/as_user
drwx------   - hdfs     supergroup      0 2017-07-31 00:17 /user/hdfs
drwxrwxrwx   - mapred   hadoop          0 2017-06-05 00:28 /user/history
drwxrwxr-t   - hive     hive            0 2017-06-05 00:30 /user/hive
drwxrwxr-x   - hue      hue             0 2017-06-05 00:30 /user/hue
drwxrwxr-x   - impala   impala          0 2017-07-19 00:52 /user/impala
drwxr-x--x   - spark    spark           0 2017-06-05 01:34 /user/spark
```

5. Si tiene previsto utilizar los orígenes de datos de HCatalog y Analytic Server está instalado en una máquina distinta del metastore de Hive, tiene que suplantar al cliente de Hive en HDFS.
   a. Vaya hasta la pestaña Configuración del servicio HDFS en Cloudera Manager.

      Nota: Los valores siguientes pueden no aparecer en la pestaña **Configuración** si todavía no se han establecido. En este caso, ejecute una búsqueda para encontrarlos.
   b. Edite el valor **`hadoop.proxyuser.hive.groups`** para que tenga el valor `*`, o un grupo que contenga todos los usuarios permitidos para iniciar la sesión en Analytic Server.
   c. Edite el valor **`hadoop.proxyuser.hive.hosts`** para que tenga el valor `*` o la lista de hosts en los que están instalados como servicios el metastore de Hive y todas las instancias de Analytic Server.
   d. Reinicie el servicio HDFS.

Después de que se hayan realizado estos pasos y esté instalado Analytic Server, Analytic Server configurará de forma silenciosa y automática Kerberos.

Habilitación de la suplantación de Kerberos

La suplantación permite ejecutar un hilo en un contexto de seguridad que difiere del contexto de seguridad del proceso que es propietario de la hebra. Por ejemplo, la suplantación proporciona un medio para que los trabajos de Hadoop se ejecuten como otros usuarios que no sean los usuarios estándar de Analytic Server (`as_user`). Para habilitar la suplantación de Kerberos:

1. Abra Cloudera Manager y añada o actualice las propiedades siguientes en el área **Cluster-wide Advanced Configuration Snippet (Safety Valve) for core-site.xml** (situada en la pestaña **HDFS (Service-Wide)** > **Configuration**).
   - **Nombre:** `hadoop.proxyuser.as_user.hosts`
   - **Valor:** `*`
   - **Nombre:** `hadoop.proxyuser.as_user.groups`
   - **Valor:** `*`

   Nota: Los valores de **core-site.xml** se aplican a la configuración de Hadoop (no a Analytic Server).
2. Ejecute el mandato siguiente desde un shell de mandatos en el nodo Analytic Server:

```
hadoop fs -chmod -R 755 /user/as_user/analytic-root/analytic-workspace
```

Configuración de HAProxy para el inicio de sesión único (SSO) utilizando Kerberos

1. Configure e inicie HAProxy de acuerdo con la guía de documentación de HAProxy: http://www.haproxy.org/#docs

2. Cree el principio de Kerberos (HTTP/<nombre_host_proxy>@<reino>) y el archivo de tabla de claves para el host de HAProxy, donde <nombre_host_proxy> es el nombre completo del host de HAProxy y <reino> es el dominio Kerberos.
3. Copie el archivo de tabla de claves en cada uno de los hosts de Analytic Server como `/etc/security/keytabs/spnego_proxy.service.keytab`
4. Actualice los permisos en este archivo en cada uno de los hosts de Analytic Server. A continuación se proporciona un ejemplo.

   ```
   chown root:hadoop /etc/security/keytabs/spnego_proxy.service.keytab
   chmod 440 /etc/security/keytabs/spnego_proxy.service.keytab
   ```

5. Abra Cloudera Manager y añada o actualice las propiedades siguientes en el área **Analytic Server Advanced Configuration Snippet (Safety Valve) for analyticserver-conf/config.properties** de Analytic Server.

   ```
   web.authentication.kerberos.keytab=/etc/security/keytabs/spnego_proxy.service.keytab
   web.authentication.kerberos.principal=HTTP/<nombre completo de
   máquina proxy>@<realm>
   ```

6. Guarde la configuración y reinicie todos los servicios Analytic Server desde Cloudera Manager.
7. Dé instrucciones a los usuarios para que configuren su navegador para que utilice Kerberos.

Ahora los usuarios pueden iniciar sesión en Analytic Server utilizando la opción **Inicio de sesión con inicio de sesión único** en la pantalla de inicio de sesión de IBM SPSS Analytic Server.

Inhabilitación de Kerberos

1. Inhabilite Kerberos en la consola de Cloudera Manager.
2. Detenga el servicio Analytic Server.
3. Elimine los valores siguientes del área **Analytic Server Advanced Configuration Snippet (Safety Valve) for analyticserver-conf/config.properties**.

   ```
   default.security.provider
   hdfs.keytab
   hdfs.user
   java.security.krb5.conf
   as.db.connect.method
   web.authentication.kerberos.keytab
   web.authentication.kerberos.principal
   ```

4. Pulse **Guardar cambios** y reinicie el servicio Analytic Server.

Habilitación de conexiones SSL (capa de sockets seguros) a la consola de Analytic Server

De forma predeterminada, Analytic Server genera certificados firmados automáticamente para habilitar la capa de sockets seguros (SSL), de modo que puede acceder a la consola de Analytic Server a través del puerto seguro aceptando los certificados firmados automáticamente. Para que el acceso HTTPS sea más seguro, tendrá que instalar certificados de proveedores de terceros.

Para instalar certificados de proveedores de terceros, siga estos pasos.

1. Copie el proveedor de terceros y los certificados de almacén de confianza en el mismo directorio en todos los nodos de Analytic Server; por ejemplo, `/home/as_user/security`.

   Nota: El usuario de Analytic Server debe tener acceso de lectura a este directorio.
2. En Cloudera Manager, vaya hasta la pestaña Configuración del servicio Analytic Server.
3. Edite el parámetro **`ssl_cfg`**.

   ```
   <ssl id="defaultSSLConfig"
        keyStoreRef="defaultKeyStore"
        trustStoreRef="defaultTrustStore"
        clientAuthenticationSupported="true"/>
   <keyStore id="defaultKeyStore"
   ```

```
          location="<KEYSTORE-LOCATION>"
          type="<TYPE>"
          password="<PASSWORD>"/>
<keyStore id="defaultTrustStore"
          location="<TRUSTSTORE-LOCATION>"
          type="<TYPE>"
          password="<PASSWORD>"/>
```

Sustituya

- <KEYSTORE-LOCATION> por la ubicación absoluta del almacén de claves; por ejemplo: `/home/as_user/security/mykey.jks`
- <TRUSTSTORE-LOCATION> por la ubicación absoluta del almacén de confianza; por ejemplo: `/home/as_user/security/mytrust.jks`
- <TYPE> por el tipo de certificado; por ejemplo: JKS, PKCS12 etc.
- <PASSWORD> por la contraseña cifrada en formato de cifrado Base64. Para la codificación puede utilizar securityUtility; por ejemplo: `{RAÍZ_AS}/ae_wlpserver/bin/securityUtility codificar <contraseña>`

Si desea generar un certificado firmado automáticamente, puede utilizar securityUtility; por ejemplo: `{RAÍZ_AS}/ae_wlpserver/bin/securityUtility createSSLCertificate --server=mmi_servidor --password=mi_contraseña --validity=365 --subject=CN=mycompany,O=myOrg,C=myCountry`. Para obtener más información sobre securityUtility y otros valores de SSL, consulte la documentación del perfil WebSphere Liberty.

Nota: Debe proporcionar un nombre de dominio de host adecuado para el valor `CN`.

4. Pulse **Guardar cambios** y reinicie el servicio Analytic Server.

Comunicarse con Apache Hive sobre SSL

Debe actualizar el archivo `hive.properties` con el fin de comunicarse con Apache Hive a través de una conexión SSL. De forma alternativa, si el entorno de Apache Hive está habilitado para alta disponibilidad, puede seleccionar los parámetros de alta disponibilidad en la página principal de orígenes de datos de Analytic Server.

Actualización del archivo hive.properties

1. Abra el archivo `hive.properties`. El archivo se encuentra en: `/opt/cloudera/parcels/analyticserver/3.2/ae_wlpserver/usr/servers/aeserver/configuration/database`
2. Localice la línea siguiente:

```
jdbcurl = jdbc:hive2://{db.servername}:{db.serverport}/{db.databasename};user={db.username};password={db.password}
```

3. Actualice la línea añadiendo la información en **negrita** siguiente:

```
jdbcurl = jdbc:hive2://{db.servername}:{db.serverport}/{db.databasename};user={db.username};password={db.password};
ssl=true;sslTrustStore=pathtotheirtruststorefile;trustStorePassword=xxxtheirTrustStorePassword
```

4. Guarde el archivo `hive.properties`.

Habilitación del soporte para Essentials for R

Analytic Server da soporte a la puntuación de modelos R y la ejecución de scripts R.

Para instalar Essentials for R después de una instalación satisfactoria de Analytic Server en Cloudera Manager:

1. Suministre el entorno del servidor para Essentials for R. Para obtener más información, consulte el paso 1 en “Habilitación del soporte para Essentials for R” en la página 22.
2. Descargue el archivo autoextraíble (BIN) para el RPM de IBM SPSS Modeler Essentials for R. Essentials for R está disponible para su descarga en (https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=swg-tspssp). Elija el archivo específico a su pila, versión de pila y arquitectura de hardware.

3. Ejecute el archivo autoextraíble como un usuario root, o un usuario que pertenezca al grupo sudo, en el host de servidor de Cloudera Manager. Los paquetes siguientes deben estar instalados, o disponibles desde los repositorios configurados:
   - Red Hat Linux: gcc-gfortran, zip, gcc-c++
   - SUSE Linux: gcc-fortran, zip, gcc-c++
   - Ubuntu Linux: gcc-fortran, zip, gcc-c++
4. El instalador autoextraíble realiza las tareas siguientes:
   a. Muestra las licencias necesarias, y solicita al instalador que las acepte.
   b. Solicita al instalador que especifique la ubicación de origen de R, o que continúe con la ubicación predeterminada. La versión R predeterminada que se instala es 3.3.2. Para instalar una versión diferente:
      - Instalación en línea: proporcione el URL del archivo de la versión necesaria de R. Por ejemplo, https://cran.r-project.org/src/base/R-2/R-2.15.3.tar.gz, para R 2.15.3.
      - Instalación fuera de línea: descargue y, a continuación, copie el archivo de la versión necesaria de R en el host de servidor de Cloudera Manager. No cambie el nombre del archivo (de forma predeterminada, se denomina `R-x.x.x.tar.gz`). Proporcione el URL del archivo de R copiado, de la siguiente manera: `file://<directorio_archivo_R>/R-x.x.x.tar.gz`. Si se ha descargado el archivo `R-2.15.3.tar.gz`, y se ha copiado en `/root`, el URL es `file:///root/R-2.15.3.tar.gz`.

      Nota: Las demás versiones de R pueden encontrarse en https://cran.r-project.org/src/base/.
   c. Instala los paquetes que R necesita.
   d. Descarga e instala R, además del plugin de Essentials for R.
   e. Crea el paquete y el archivo `parcel.sha`, y los copia en `/opt/cloudera/parcel-repo`. Especifique la ubicación correcta, si la ubicación ha cambiado.
5. Tras completarse la instalación, distribuya y active el paquete de **Essentials for R** en Cloudera Manager (pulse **Check for New Parcels** para renovar la lista de paquetes).
6. Si el servicio Analytic Server ya está instalado:
   a. Detenga el servicio.
   b. Renueve los binarios de Analytic Server.
   c. Inicie el servicio para finalizar la instalación de Essentials for R.
7. Si el servicio Analytic Server no está instalado, prosiga con su instalación.

Nota: Todos los hosts de Analytic Server deben tener instalados los paquetes (`zip` y `unzip`) de archivo adecuados.

Habilitación de orígenes de bases de datos relacionales

Analytic Server puede utilizar orígenes de bases de datos relacionales si proporciona los controladores JDBC en un directorio compartido en cada metsstore de Analytic Server y cada host de Analytic Server. De forma predeterminada, el directorio es `/usr/share/jdbc`.

Para cambiar el directorio compartido, siga estos pasos.

1. En Cloudera Manager, vaya hasta la pestaña Configuración del servicio Analytic Server.
2. Especifique la vía de acceso del directorio compartido de los controladores JDBC en **`jdbc.drivers.location`**.
3. Pulse **Guardar cambios**.
4. Seleccione **Detener** en la lista desplegable **Acciones**, para detener el servicio Analytic Server.
5. Seleccione **Renovar binarios de Analytic Server** en la lista desplegable **Acciones**.
6. Seleccione **Iniciar** en la lista desplegable **Acciones**, para iniciar el servicio Analytic Server.

Tabla 11. Bases de datos soportadas

Base de datos	Versiones soportadas	Archivos JAR del controlador JDBC	Distribuidor
Amazon Redshift	8.0.2 o posterior.	`RedshiftJDBC41-1.1.6.1006.jar` o posterior	Amazon
Apache Impala	JDBC 4 con 2.5.5 o posterior	`ImpalaJDBC4.jar`, `commons-codec-*.jar`, `commons-logging-*.jar`, `httpclient-*.jar`, `httpcore-*.jar`, `log4j-*.jar`, `libthrift-*.jar`, `libfb303-*.jar`, `slf4j-api-*.jar`, `ql.jar`, `zookeeper-*.jar`, `TCLIServiceClient.jar`	Apache
DashDB	Bluemix Service	`db2jcc.jar`	IBM
Db2 para Linux, UNIX y Windows	11.1, 10.5, 10.1, 9.7	`db2jcc.jar`	IBM
Db2 z/OS	11, 10	`db2jcc.jar`, `db2_license_cisuz.jar`	IBM
Greenplum	5.x	postgresql.jar	Greenplum
Hive	1.1	`hive-jdbc-*.jar`	Apache
MySQL	5.6, 5.7	mysql-connector-java-commercial-5.1.25-bin.jar	MySQL
Netezza	7, 6.x	`nzjdbc.jar`	IBM
Oracle	12c, 11g R2 (11.2)	`ojdbc6.jar`, `orai18n.jar`	Oracle
SQL Server	2014, 2012, 2008 R2	`sqljdbc4.jar`	Microsoft
Teradata	15, 15.1	`tdgssconfig.jar`, `terajdbc4.jar`	Teradata

Notas

- Si ha creado un origen de datos Redshift antes de instalar Analytic Server, necesitará efectuar los pasos siguientes para utilizar el origen de datos Redshift.
  1. En la consola de Analytic Server, abra el origen de datos Redshift.
  2. Seleccione el origen de datos de la base de datos `Redshift`.
  3. Especifique la dirección del servidor de Redshift.
  4. Entre el nombre de la base de datos y el nombre de usuario. La contraseña se debe llenar automáticamente.
  5. Seleccione la tabla de base de datos.

Habilitación de orígenes de datos de HCatalog

Analytic Server proporciona soporte de varios orígenes de datos a través de Hive/HCatalog. Algunos orígenes requieren pasos de configuración manuales.

1. Recopile los archivos JAR necesarios para habilitar el origen de datos. Consulte las secciones que figuran a continuación para obtener detalles.
2. Añadir estos archivos JAR al directorio `{INICIO_HIVE}/auxlib` y al directorio `/usr/share/hive` en cada metastore de Analytic Server y cada nodo de Analytic Server.
3. Reiniciar el servicio Hive Metastore.

4. Reiniciar todas las instancias del servicio Analytic Server.

Nota:

Al acceder a los datos de HBase a través de un origen de datos HCatalog de Analytic Server, el usuario de acceso debe tener permiso de lectura para las tablas HBase.

- En entornos que no sean kerberos, Analytic Server accede a HBase utilizando `as_user` (`as_user` debe tener permiso de lectura para HBase).
- En entornos de kerberos, tanto `as_user` como el usuario de inicio de sesión deben tener permiso de lectura para las tablas HBase.

Bases de datos NoSQL

Analytic Server admite cualquier base de datos NoSQL para la que está disponible un manejador de almacenamiento de Hive del proveedor.

No es necesario ningún paso adicional para habilitar el soporte de Apache HBase y Apache Accumulo.

Para otras bases de datos NoSQL, póngase en contacto con el proveedor de base de datos y obtenga el manejador de almacenamiento y los jar relacionados.

Tablas Hive basadas en archivo

Analytic Server admite las tablas Hive basadas en archivo para las que está disponible un Hive SerDe (serializador-deserializador) incorporado o personalizado.

Hive XML SerDe para procesar los archivos XML se ubica en el repositorio central de Maven en http://search.maven.org/#search%7Cga%7C1%7Chivexmlserde.

Trabajos de MapReduce v2

Utilice el valor **`preferred.mapreduce`** del área **Analytic Server Advanced Configuration Snippet (Safety Valve) for analyticserver-conf/config.properties** para controlar cómo se manejan los trabajos MapReduce:

Tabla 12. Analytic Server Advanced Configuration Snippet (Safety Valve) for analyticserver-conf/config.properties

Propiedad	Descripción
`preferred.mapreduce`	Controla el método en el que se ejecutan los trabajos MapReduce. Los valores válidos incluyen: • `spark` • `m3r` • `hadoop` Por ejemplo: `preferred.mapreduce=spark`

Apache Spark

Si desea utilizar Spark (versión 1.5 o posterior) debe seleccionar `spark.version` durante la instalación de Analytic Server.

1. Abra Cloudera Manager y seleccione `spark.version` adecuado (por ejemplo, `None`, `1.x` o `2.x`) en el área **Analytic Server Spark Version**.

   Nota: Cuando se utiliza Spark 1.x, también debe añadir la línea siguiente en el área **Analytic Server Advanced Configuration Snippet (Safety Valve) for analyticserver-conf/config.properties**.

   ```
   spark.extraListeners=org.apache.spark.JavaSparkListener
   ```

2. Guarde la configuración.

Configuración de Apache Impala

Ahora se puede utilizar Apache Impala cuando se ejecuta en Cloudera para un origen de datos de base de datos de Analytic Server o un origen de datos de HCatalog (independientemente de si Impala está habilitado para SSL).

Creación de un origen de base de datos para datos de Apache Impala

1. En la página principal **Orígenes de datos** de Analytic Server pulse **Nuevo** para crear un nuevo origen de datos. Se muestra el diálogo Nuevo origen de datos.
2. Especifique un nombre adecuado en el campo **Nuevo origen de datos**, seleccione `Base de datos` como valor para **Tipo de contenido** y después pulse **Aceptar**.
3. Abra la sección **Selecciones de base de datos** y especifique la siguiente información.

   Base de datos:
   Seleccione **Impala** desde el menú desplegable.

   Dirección de servidor:
   Escriba el URL del servidor que aloja el daemon de Impala. Es necesario un nombre de dominio completo cuando Kerberos está habilitado para Analytic Server.

   Puerto del servidor:
   Escriba el número de puerto en el que escucha la base de datos de Impala.

   Nombre de la base de datos:
   Escriba el nombre de la base de datos a la que desea conectarse.

   Nombre del usuario:
   Escriba un nombre de usuario con autorización para iniciar la sesión en la base de datos de Impala.

   Contraseña:
   Escriba la contraseña correspondiente.

   Nombre de la tabla:
   Especifica el nombre de la tabla de base de datos que desee utilizar. Pulse **Seleccionar** para seleccionar manualmente un archivo.

   Número máximo de lecturas simultáneas:
   Especifique el límite en el número de consultas paralelas que se pueden enviar desde Analytic Server a la base de datos para leer desde la tabla especificada en el origen de datos.
4. Pulse **Guardar** después de especificar la información necesaria.

Creación de un origen de datos de HCatalog para datos de Apache Impala

1. En la página principal **Orígenes de datos** de Analytic Server pulse **Nuevo** para crear un nuevo origen de datos. Se muestra el diálogo Nuevo origen de datos.
2. Especifique un nombre adecuado en el campo **Nuevo origen de datos**, seleccione `HCatalog` como valor para **Tipo de contenido** y después pulse **Aceptar**.
3. Abra la sección **Selecciones de base de datos** y especifique la siguiente información.

   Base de datos:
   Seleccione **predeterminado** desde el menú desplegable.

   Nombre de la tabla:
   Especifica el nombre de la tabla de base de datos que desee utilizar.

   Esquema de HCatalog
   Seleccione la opción **Elemento de HCatalog** y seleccione a continuación las opciones **Correlaciones de campos de HCatalog** adecuadas.

4. Pulse **Guardar** después de especificar la información necesaria.

Conexión a datos habilitados para Apache Impala

1. Defina los siguientes valores de Impala SSL en la consola de Cloudera Manager.

   Habilite TLS/SSL para Impala (client_services_ssl_enabled)
   Seleccione la opción **Impala (Service-Wide)**.

   Archivo de certificado del servidor TLS/SSL de Impala (formato PEM) (ssl_server_certificate)
   Especifique la ubicación y el nombre de archivo del certificado firmado automáticamente con formato PEM (por ejemplo: `/tmp/<nombre_usuario>/ssl/ll4200v21.crt`).

   Archivo de clave privada del servidor TLS/SSL de Impala (formato PEM) (ssl_private_key)
   Especifique la clave privada, en formato PEM, la ubicación y el nombre de archivo (por ejemplo: `/tmp/<nombre_usuario>/ssl/ll4200v21.key`).
2. En el host de Analytic Server, importe el archivo `*.crf` (que se utiliza para habilitar SSL en Impala) a un archivo `*.jks`. El archivo puede ser un archivo cacerts (por ejemplo `/etc/pki/java/cacerts`) o cualquier otro archivo `*.jks`.
3. En el host de Analytic Server, actualice el archivo de configuración de Impala (`impala.properties`) añadiendo el siguiente valor para la clave `jdbcurl`:

   ```
   SSL=1;AllowSelfSignedCerts=1;CAIssuedCertNamesMismatch=1;
   ```

   Nota: Cuando se utiliza un archivo `*.jks` (que no sea cacerts), debe especificar lo siguiente:

   ```
   SSLTrustStore=<your_pks_file>;SSLTrustStorePwd=<contraseña_para_archivo_pks>;
   ```
4. Reinicie Analytic Server en la consola de Cloudera Manager.

Cambio de puertos utilizados por Analytic Server

Analytic Server utiliza el puerto 9080 para HTTP y el puerto 9443 para HTTPS de forma predeterminada. Para cambiar los valores de puerto, siga estos pasos.

1. En Cloudera Manager, vaya hasta la pestaña Configuración del servicio Analytic Server.
2. Especifique los puertos HTTP y HTTPS deseados en los parámetros **`http.port`** y **`https.port`**, respectivamente.

   Nota: Es posible que tenga que seleccionar la categoría **Puertos y direcciones** en la sección Filtros para ver estos parámetros.
3. Pulse **Guardar cambios**.
4. Reinicie el servicio Analytic Server.

Analytic Server de alta disponibilidad

Puede hacer que Analytic Server sea de alta disponibilidad añadiéndolo como un servicio a varios nodos del clúster.

1. En Cloudera Manager, vaya hasta la pestaña Instancias del servicio Analytic Server.
2. Pulse **Añadir instancias de rol** y seleccione los hosts en los que se deba añadir Analytic Server como un servicio.

Soporte de varios clústeres

La característica de varios clústeres es una mejora a la prestación de Alta disponibilidad de IBM SPSS Analytic Server y proporciona un aislamiento mejorado en entornos de varios inquilinos. De forma predeterminada, la instalación del servicio de Analytic Server (en Ambari o ClouderaManager) da lugar a la definición de un único clúster de servidor de análisis.

La especificación de clúster define la pertenencia al clúster de Analytic Server. La modificación de la especificación del clúster se realiza con contenido XML (en el campo `analytics-cluster` de la configuración de Analytic Server de Ambari o manualmente editando el archivo `configuration/`

analytics-cluster.xml) de Cloudera Manager. Al configurar varios clústeres de Analytic Server , es necesario alimentar solicitudes para cada clúster de Analytic Server con su propio equilibrador de carga.

Mediante la característica de varios clústeres garantiza que el trabajo para un inquilino no puede afectar negativamente al trabajo que se realice en el clúster de otro inquilino. Respecto a trabajos de altamente disponibles, la migración tras error de trabajo solo se produce en el ámbito de clúster de Analytic Server en el que se inició el trabajo. En el ejemplo siguiente se proporciona una especificación XML de varios clústeres.

Nota: Puede hacer que Analytic Server sea de alta disponibilidad añadiéndolo como un servicio a varios nodos del clúster.

```
<analayticServerClusterSpec>
    <cardinality>1+</cardinality>
    <cluster name="cluster1">
        <memberName>one.cluster</memberName>
        <memberName>two.cluster</memberName>
    </cluster>
    <cluster name="cluster2">
        <memberName>three.cluster</memberName>
        <memberName>four.cluster</memberName>
    </cluster>
</analayticServerClusterSpec>
```

En el ejemplo anterior, se precisan dos equilibradores de carga. Un equilibrador de carga envía solicitudes a miembros de cluster1 (one.cluster y two.cluster) y el otro envía solicitudes a miembros de cluster2 (three.cluster y four.cluster).

En el ejemplo siguiente se proporciona una especificación XML de clúster único (la configuración predeterminada).

```
<analayticServerClusterSpec>
    <cardinality>1</cardinality>
    <cluster name="cluster1">
        <memberName>*</memberName>
    </cluster>
</analayticServerClusterSpec>
```

En el ejemplo anterior, un equilibrador de carga único se precisa para manejar casos en los que existe más de un miembro de clúster configurado.

Notas

- Solo clústeres singleton dan soporte al uso de comodines en el elemento **memberName** (por ejemplo, cardinalidad de clúster = "1"). Los valores válidos para el elemento de cardinalidad son 1 y 1+.
- **memberName** se debe especificar de la misma manera que el nombre de host al que se ha asignado el rol de Analytic Server.
- Todos los servidores en todos los clústeres deben reiniciarse después de que se apliquen los cambios de configuración del clúster.
- En Cloudera Manager, debe modificar y mantener el archivo analytics-cluster.xml en todos los nodos de Analytic Server. Todos los nodos deben mantenerse para garantizar que contengan el mismo contenido.

Optimización de opciones de la JVM para datos pequeños

Puede editar las propiedades de la JVM para poder optimizar su sistema al ejecutar trabajos pequeños (M3R).

En la Cloudera Manager, revise el control **Opciones de la JVM (jvm.options)** en la pestaña Configuración en el servicio Analytic Server. La modificación de los parámetros siguientes establece el tamaño de almacenamiento dinámico para trabajos que se ejecutan en el servidor que aloja Analytic Server; es decir, no Hadoop. Esto es importante si se ejecutan trabajos (M3R) pequeños y es posible que tenga que experimentar con estos valores para optimizar el sistema.

```
-Xms512M
-Xmx2048M
```

Configuración de colas YARN separadas para cada inquilino de IBM SPSS Analytic Server - Cloudera

La configuración de las colas Yarn se lleva a cabo mediante el uso de los técnicos de Spark Dynamic Resource Allocation.

Cloudera 5.x

Siga estos pasos al añadir SPSS Analytic Server Service a un clúster existente.

1. En Cloudera Manager, vaya a **SPSS Analytic Server Service** > **Configuración**.
2. Cambie el valor **Resource Pool Enable: resource.pool.enabled** a `true`.
3. Añada las propiedades siguientes a **Analytic Server Advanced Configuration Snippet (Safety Valve)** > **analyticserver-conf.config.properties**:

```
config.folder.path=/etc/spark2/conf
resource.pool.mapping=tenant1:test,tenant2:production
resource.pool.default=default
spark.scheduler.mode=FAIR
spark.yarn.queue=default
```

Tabla 13. Valores de analyticserver-conf.config.properties

Propiedad	Descripción
`config.folder.path`	El directorio contiene el archivo `fairscheduler.xml` que contiene la información de propiedades de la agrupación de Spark. El archivo es necesario y se debe crear manualmente. Para obtener más información, consulte la sección **fairscheduler.xml example**.
`resource.pool.mapping`	**Spark:** Correlaciona los inquilinos con las agrupaciones que están definidas en el archivo `fairscheduler.xml`. Los pares de inquilinos deben estar separados por comas (por ejemplo, `tenant1:test,tenant2:production`. Antes de especificar una agrupación, asegúrese de que la agrupación esté configurada en el archivo `fairscheduler.xml`. **MapReduce:** Correlaciona los inquilinos con la cola definida en Dynamic Resource Pool Configuration. Los pares de inquilinos deben estar separados por comas (por ejemplo, tenant1:test,tenant2:production). Antes de especificar una cola, asegúrese de que el sistema esté configurado con la cola, y que el acceso esté permitido para enviar trabajos a la cola. **Nota:** Si desea ejecutar los trabajos Spark y MapReduce juntos, los valores de correlación de inquilinos deben tener el mismo nombre en el archivo `fairscheduler.xml` y en Dynamic Resource Pool Configuration.
`resource.pool.default`	**Spark:** Define la agrupación de recursos predeterminada. El valor puede ser `default` o un nombre de agrupación que esté definido en el archivo `fairscheduler.xml`. Utilice el valor `default` cuando los inquilinos no estén configurados (o estén configurados incorrectamente). **MapReduce:** Define la cola predeterminada a la que se envían los trabajos.
`spark.scheduler.mode=FAIR`	**Spark:** Habilita el planificador limpio. La propiedad no se debe cambiar.
`spark.yarn.queue`	**Spark:** El nombre de la cola YARN a la que se envía la aplicación. Puede especificar un nombre de cola YARN personalizado en Dynamic Resource Pool Configuration.

4. Guarde la configuración y reinicie el servicio de Analytic Server.

Ejemplo de fairscheduler.xml

El archivo `fairscheduler.xml` contiene la información de propiedades de la agrupación de Spark. El archivo es necesario y se debe crear manualmente.

```
<?xml version="1.0"?>
<allocations>
  <pool name="production">
    <schedulingMode>FAIR</schedulingMode>
    <weight>1</weight>
    <minShare>2</minShare>
  </pool>
  <pool name="test">
    <schedulingMode>FIFO</schedulingMode>
    <weight>2</weight>
    <minShare>3</minShare>
  </pool>
</allocations>
```

Referencia

Consulte los sitios siguientes para obtener más información:

- https://spark.apache.org/docs/latest/job-scheduling.html#dynamic-resource-allocation
- https://spark.apache.org/docs/latest/running-on-yarn.html

Migración

Analytic Server le permite migrar datos y valores de configuración de una instalación existente de Analytic Server a una nueva instalación.

Actualice a una versión nueva de Analytic Server

Si tiene una instalación existente de Analytic Server 3.1.2 y ha adquirido una versión más reciente, puede migrar los valores de configuración de 3.1.2 a la nueva instalación.

Restricción: Su instalación de la versión 3.1.2 y las nuevas no pueden coexistir en el mismo clúster de Hadoop. Si configura la instalación nueva para que utilice el mismo clúster de Hadoop que la instalación de 3.1.2, la instalación de 3.1.2 dejará de funcionar.

Pasos de migración, de 3.1.2 a una versión más reciente

1. Instale la nueva instalación de Analytic Server de acuerdo a las instrucciones de "Instalación en Cloudera" en la página 41.
2. Copie el espacio de trabajo analítico de la instalación antigua a la nueva.
   a. Si no está seguro de la ubicación del espacio de trabajo analítico, ejecute `hadoop -fs ls`. La vía de acceso al espacio de trabajo analítico tendrá el formato `/user/as_user/analytic-root/analytic-workspace`, donde `as_user` es el ID de usuario que posee el espacio de trabajo analítico.
   b. Inicie una sesión en el host de la nueva de instalación de Analytic Server como `as_user`. Suprima el directorio `/user/as_user/analytic-root/analytic-workspace`, si existe.
   c. Ejecute el script de copia siguiente.

      ```
      hadoop distcp hftp://{host of 3.1.2 namenode}:50070/{path to 3.1.2 analytic-workspace}
      hdfs://{host of 3.2.1 namenode}/user/as_user/analytic-root/analytic-workspace
      ```
3. Si utiliza el Apache Directory Server incorporado, realice una copia de seguridad de la configuración de usuario/grupo actual con una herramienta de cliente LDAP de terceros. Después de instalar Analytic Server 3.2.1, importe la configuración de usuario/grupo de copia de seguridad al Apache Directory Server.

   Nota: Este paso se puede omitir si utiliza un servidor LDAP externo.
4. En Cloudera Manager, detenga el servicio Analytic Server.
5. Recopile los valores de configuración de la instalación antigua.

a. Copie el archivado `configcollector.zip` de la nueva instalación en `{RAÍZ_AS}\tools` de la instalación anterior.
b. Extraiga la copia de `configcollector.zip`. Esto crea un nuevo subdirectorio `configcollector` en la instalación anterior.
c. Ejecute la herramienta de recopilador de configuración en la instalación anterior ejecutando el script **configcollector** en `{RAÍZ_AS}\tools\configcollector`. Copie el archivo comprimido resultante (ZIP) en el servidor que aloja su nueva instalación.

Importante: El script **configcollector** proporcionado no puede ser compatible con la versión de Analytic Server más reciente. Póngase en contacto con el representante de soporte técnico de IBM si encuentra problemas con el scripts **configcollector**.

6. Borre el estado de Zookeeper. En el directorio bin de Zookeper (por ejemplo, `/opt/cloudera/parcels/CDH-5.4...../lib/zookeeper/bin` en Cloudera), ejecute el mandato siguiente.
```
./zkCli.sh rmr /AnalyticServer
```
7. Ejecute la herramienta de migración ejecutando el script **migrationtool** y pasando la vía de acceso del archivo comprimido creado por el recopilador de la configuración como argumento. A continuación se proporciona un ejemplo.
```
migrationtool.sh /opt/ibm/spss/analyticserver/3.2/ASConfiguration_3.1.2.xxx.zip
```
8. Ejecute el mandato siguiente desde un shell de mandatos en el nodo Analytic Server:
```
hadoop fs -chmod -R 755 /user/as_user/analytic-root/analytic-workspace
```
9. En Cloudera Manager, inicie el servicio Analytic Server.

Nota: Si ha configurado R para utilizarlo con la instalación de Analytic Server existente, tendrá que seguir los pasos para configurarlo con la nueva instalación de Analytic Server.

Desinstalación de Analytic Server en Cloudera

Cloudera maneja, automáticamente, la mayoría de los pasos necesarios para desinstalar el servicio y el y paquete de Analytic Server.

Los pasos siguientes son necesarios para poder limpiar Analytic Server del entorno de Cloudera:

1. Detenga y suprima el servicio de Analytic Server.
2. **Desactive**, **Elimine de hosts** y **Suprima** los paquetes de Analytic Server.
3. Suprima el directorio del usuario de Analytic Server en HDFS. La ubicación predeterminada es `/user/as_user/analytic-root`.
4. Suprima la base de datos, o el esquema, que Analytic Server utilice.
5. Limpieza de cualquier resto del paquete de instalación de Analytic Server. Esto se lleva a cabo suprimiendo lo siguiente:
   - Carpeta `csd`
   - Todos los archivos 3.2.1 existentes que se encuentran en las carpetas `parcels`, `parcel-cache` y `parcel-repo`.

Capítulo 4. Configuración de IBM SPSS Modeler para su uso con IBM SPSS Analytic Server

Para habilitar SPSS Modeler a fin de utilizarlo con Analytic Server, debe realizar algunas actualizaciones en la instalación de SPSS Modeler Server.

1. Configure SPSS Modeler Server para asociarlo con una instalación de Analytic Server.
   a. Edite el archivo `options.cfg` en el subdirectorio `config` del directorio de instalación del servidor principal, y añada o edite las líneas siguientes:

```
as_ssl_enabled, {Y|N}
as_host, "{AS_SERVER}"
as_port, PORT
as_context_root, "{CONTEXT-ROOT}"
as_tenant, "{TENANT}"
as_prompt_for_password, {Y|N}
as_kerberos_auth_mode, {Y|N}
as_kerberos_krb5_conf, {CONF-PATH}
as_kerberos_krb5_spn, {AS-SPN}
```

   as_ssl_enabled
   Especifique Y si la comunicación segura está configurada en Analytic Server; de lo contrario, especifique N.

   as_host
   La dirección IP/nombre de host del servidor que aloja Analytic Server.

   Nota: Debe proporcionar una dirección IP/nombre de dominio de host apropiado cuando SSL está habilitado para Analytic Server.

   as_port
   El puerto en el que Analytic Server está a la escucha (el valor predeterminado es 8080).

   as_context_root
   La raíz de contexto de Analytic Server (el valor predeterminado es analyticserver).

   as_tenant
   El inquilino del que la instalación de SPSS Modeler Server forma parte (el inquilino predeterminado es ibm).

   as_prompt_for_password
   Especifique N si SPSS Modeler Server está configurado con el mismo sistema de autenticación de usuarios y contraseñas que el utilizado en Analytic Server; por ejemplo, al utilizar la autenticación Kerberos. De lo contrario, especifique Y.

   Al ejecutar SPSS Modeler en modalidad de proceso por lotes, añada `-analytic_server_username {ASusername} -analytic_server_password {ASpassword}` como argumentos al mandato `clemb`.

   as_kerberos_auth_mode
   Especifique Y para habilitar el inicio de sesión único Kerberos en SPSS Modeler.

   as_kerberos_krb5_conf
   Especifique la vía de acceso del archivo de configuración de Kerberos que Analytic Server debe utilizar; por ejemplo, `\etc\krb5.conf`.

   as_kerberos_krb5_spn
   Especifique el SPN Kerberos de Analytic Server; por ejemplo, HTTP/ ashost.mydomain.com@MYDOMAIN.COM.

   b. Reinicie el servicio de SPSS Modeler Server.

Para poder conectarse a una instalación de Analytic Server que tiene habilitado SSL/TLS, deben realizarse algunas tares adicionales para configurar las instalaciones de SPSS Modeler Server y de cliente.

a. Navegue a `http{s}://{HOST}:{PORT}/{CONTEXT-ROOT}/admin/{TENANT}` e inicie la sesión en la consola de Analytic Server.
b. Descargue el archivo de certificación del navegador y guárdelo en su sistema de archivos.
c. Añada el archivo de certificación en el JRE de las instalaciones de SPSS Modeler Server y de SPSS Modeler Client. La ubicación de actualizaciones puede encontrarse en el subdirectorio `/jre/lib/security/cacerts` de la vía de instalación de SPSS Modeler.
   1) Asegúrese de que el archivo `cacerts` no sea de sólo lectura.
   2) Utilice el programa keytool que se suministra con Modeler - que puede encontrarse en el subdirectorio `/jre/bin/keytool` de la vía de instalación de SPSS Modeler.

      Ejecute el siguiente mandato

      ```
      keytool
      -import -alias <alias-as> -file <archivo-cert> -keystore "<archivo-cacerts>"
      ```

      Tenga en cuenta que <alias-as> es un alias para el archivo `cacerts`. Puede utilizar cualquier nombre que desee, siempre y cuando sea exclusivo para el archivo `cacerts`.

      Un mandato de ejemplo podría ser parecido al siguiente.

      ```
      keytool -import -alias MySSLCertAlias -file C:\Download\as.cer
              -keystore "c:\Archivos de programa\IBM\SPSS\Modeler\{ModelerVersion}\jre\lib
                        \security\cacerts"
      ```

d. Reinicie SPSS Modeler Server y SPSS Modeler Client.

2. [opcional] Instale IBM SPSS Modeler - Essentials for R si tiene previsto puntuar modelos R en secuencias con orígenes de datos de Analytic Server. IBM SPSS Modeler - Essentials for R está disponible para descarga (https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=swg-tspssp).

Capítulo 5. Configuración de la integración de UDF de Hive

Todos los nodos de IBM SPSS Analytic Server con capacidad de integración se integrarán en la UDF de Hive siempre que sea posible. Una vez se haya registrado la UDF de Hive en la base de datos de Hive, Analytic Server puede utilizar las nuevas funciones UDF para realizar la integración.

La integración de UDF de Hive está inhabilitada de forma predeterminada y deben habilitarse manualmente mediante el valor **udfmodule** del archivo ASModules.xml (cambiar el valor **disabled** a **enabled**). Una vez habilitada, debe reiniciar Analytic Server y registrar manualmente la UDF en Hive.

Los ejemplos siguientes ilustran cómo registrar/desregistrar la UDF en Hive en los entornos HDP y Cloudera.

Registrar/desregistrar la UDF en HDP

Registrar la UDF

```
su - hive -c 'hive -f /opt/ibm/spss/analyticserver/3.2/bin/udfRegister.sql'
```

Desregistrar la UDF

```
su - hive -c 'hive -f /opt/ibm/spss/analyticserver/3.2/bin/udfUnregister.sql'
```

Registrar/desregistrar la UDF en Cloudera

Registrar la UDF

```
sudo -u hive kinit -k -t hive.keytab hive/bosperf5-master.fyre.ibm.com@IBM.COM
sudo -u hive hive -f /opt/cloudera/parcels/AnalyticServer/bin/udfRegister.sql
```

Desregistrar la UDF

```
sudo -u hive hive -f /opt/cloudera/parcels/AnalyticServer/bin/udfUnregister.sql
```

Capítulo 6. Utilización de etiquetas SLM para el seguimiento de licencias

Las etiquetas SLM se basan en el proyecto estándar ISO/IEC 19770-4 para la utilización de medición de utilización de recursos. Las etiquetas SLM proporcionan una funcionalidad estandarizada para que un producto informe de su consumo de métricas de licencia (recursos relacionados con el uso de un activo de software). Tras habilitar SLM en un producto, se genera un archivo XML de tiempo de ejecución para autoevaluar el uso de su licencia.

Cuando se inicia Analytic Server, se crean los archivos `slmtag` en la carpeta `<vía_acceso_instalación_as>/logs/slmtag`.

Dado que hay dos tipos de licencias, se registran periódicamente dos métricas diferentes:

- Para la versión de Analytic Server actual, las licencias se basan en el número total de nodos de datos en el clúster Hadoop (basándose en Virtual Server). El número de nodos se registra en la sección del archivo `slmtag` siguiente.

```
<Type>VIRTUAL_SERVER</Type>
   <SubType>Número de nodos de datos en Hadoop</SubType>
   <Value>2</Value>
   ...
```

- Para versiones de Analytic Server anteriores a 3.1, las licencias se basaban en el tamaño de almacenamiento HDFS en el clúster Hadoop (basándose en RVU). Por ejemplo, el tamaño de almacenamiento (en tegabytes) se registra en la sección del archivo `slmtag` siguiente.

```
<Type>RESOURCE_VALUE_UNIT</Type>
   <SubType>almacenamiento HDFS (Unidad: Tegabyte)</SubType>
   <Value>0.21</Valor>
```

La salida de la etiqueta SLM se inicia en una hebra y se ve afectada por las propiedades que están definidas en el archivo `SlmTagOutput.properties`. El archivo se encuentra en la carpeta `<vía_acceso_instalación_as>/configuration`.

Tabla 14. Propiedades de etiquetas SLM

Propiedades	**Descripción**
license.metric.logger.output.enabled	Controla la generación de archivos de registro SLM. El valor predeterminado es `False`.
license.metric.logger.output.dir	Vía de acceso relativa al directorio que almacena los archivos de etiquetas SLM. El directorio predeterminado es `<vía_acceso_instalación_as>/ logs`.
license.metric.logger.output. SLMLogFrequency	El intervalo de tiempo (unit:milliseconds) para recopilar registros SLM.
icense.metric.logger.file.size	El tamaño máximo de archivo de etiqueta SML, en bytes.
license.metric.logger.file.number	El número máximo de archivos de etiquetas SLM para una instancia de identidad de software.

Capítulo 7. Resolución de problemas

En este apartado se describen algunos problemas comunes de instalación y configuración y cómo corregirlos.

Cuestiones generales

La instalación se realiza satisfactoriamente con avisos, pero los usuarios no pueden crear orígenes de datos con el error "No se puede completar la solicitud. Razón: Permiso rechazado"

Si define el parámetro **distrib.fs.root** en un directorio para el que el usuario de Analytic Server (de forma predeterminada, as_user) no tiene acceso se generarán errores. Asegúrese de que el usuario de Analytic Server está autorizado para leer, escribir y ejecutar el directorio **distrib.fs.root**.

El rendimiento de Analytic Server empeora progresivamente.

Cuando el rendimiento de Analytic Server no cumple las expectativas, elimine todos los archivos `*.war` files de la vía de acceso de despliegue del servicio Knox: `/<KnoxServicePath>/data/deployments`. Por ejemplo: `/usr/hdp/3.1.0.0-78/knox/data/deployments`.

Desinstalación de Analytic Server o Essentials for R en Ambari

En algunos casos, el proceso de desinstalación se cuelga cuando se desinstala Analytic Server o Essentials for R en Ambari. Cuando se presente el problema, debe detener manualmente el ID de proceso del servidor Ambari.

Problemas cuando Analytic Server está instalado en POWER System que utiliza OpenJDK

Cuando Analytic Server se ejecuta en un sistema POWER que utiliza OpenJDK, debe realizar manualmente los siguientes pasos de configuración para asegurarse de que la API del sistema de coordenadas funciona como se esperaba

Nota: Puede ignorar el requisito de configuración si no utiliza la API del sistema de coordenadas.

1. En la consola de Ambari, vaya a **Analytic Server service** > **Configs tab** > **Advanced analytics-jvm-options** y añada la línea siguiente al área de contenido:
   ```
   -XX:CompileCommand=exclude,com/esri/sde/sdk/pe/engine/PeHznTwoPointEquidistant$GCSHorizon.*
   ```
2. En la consola de Ambari, vaya a la sección **Custom analytics.cfg** y añada las 3 configuraciones siguientes:

   spark.executor.extraJavaOptions

   Establezca el valor en: `-XX:CompileCommand=exclude,com/esri/sde/sdk/pe/engine/PeHznTwoPointEquidistant$GCSHorizon.*`

   spark.driver.extraJavaOptions

   Establezca el valor en: `-XX:CompileCommand=exclude,com/esri/sde/sdk/pe/engine/PeHznTwoPointEquidistant$GCSHorizon.*`

   mapred.child.java.opts

   Establezca el valor en: `-XX:CompileCommand=exclude,com/esri/sde/sdk/pe/engine/PeHznTwoPointEquidistant$GCSHorizon.*`

Error al instalar Analytic Server en SuSE Linux 12

Puede encontrar el siguiente error al instalar Analytic Server en SuSE Linux 12:

```
Ha fallado la verificación de firmas [la clave pública de 4 firmas no está disponible]
```

El problema se puede resolver realizando las tareas siguientes antes de instalar Analytic Server en SuSE Linux 12:

1. Descargue una clave pública en el host desde el URL siguiente:
   ```
   https://ibm-open-platform.ibm.com/repos/IBM-SPSS-AnalyticServer/3.2.1.0/IBM-SPSS-ANALYTICSERVER-GPG-KEY.public
   ```

2. Importe la clave pública ejecutando el mandato siguiente en el host:

```
rpm --import IBM-SPSS-ANALYTICSERVER-GPG-KEY.public
```

Problemas con distribuciones Hadoop específicas

La acción Renovar para el servicio Analytic Server está inhabilitada en Hortonworks 2.3-2.6

Para renovar manualmente las bibliotecas de Analytic Server en Hortonworks 2.3-2.6 utilice los pasos siguientes.

1. Inicie una sesión en el host que ejecuta Analytic Metastore como usuario de Analytic Server (de forma predeterminada, as_user).

   Nota: Puede encontrar este nombre de host en la consola de Ambari.
2. Ejecute el script **refresh** en el directorio {RAÍZ_AS}/bin; por ejemplo:

   ```
   cd /opt/ibm/spss/analyticserver/3.2/bin
   ./refresh
   ```
3. Reinicie el servicio Analytic Server en la consola de Ambari.

Los paquetes que se descargan de un sitio externo no logran superar la comprobación de hash en Cloudera Manager

Aparece el error de verificación hash en la lista de paquetes. El problema se puede resolver permitiendo que el proceso de descarga finalice y, a continuación, reiniciando Cloudera a través del servicio cloudera-scm-server. El error no se produce después de que se reinicie el servicio.

Propiedades de supergrupo HDFS

Analytic Server registrará una excepción durante el inicio si el as_user no es un miembro de las siguientes propiedades de grupo de HDFS: **dfs.permissions.supergroup/ dfs.permissions.superusergroup**. Por ejemplo:

```
[11/15/17 7:32:35:510 PST] 000000bf SystemOut
O 2017-11-15 07:32:35,510 | : |  |  |  |  | ERROR | slmtagoutput.SlmOuputAgent | SLM Logger => Error in performing callback function when calculating number
of nodes in kerberos environment: org.apache.hadoop.ipc.RemoteException(org.apache.hadoop.security.AccessControlException): Access denied for user as_user.
Superuser privilege is required
at org.apache.hadoop.hdfs.server.namenode.FSPermissionChecker.checkSuperuserPrivilege(FSPermissionChecker.java:93)
at org.apache.hadoop.hdfs.server.namenode.FSNamesystem.checkSuperuserPrivilege(FSNamesystem.java:6606)
at org.apache.hadoop.hdfs.server.namenode.FSNamesystem.datanodeReport(FSNamesystem.java:5595)
at org.apache.hadoop.hdfs.server.namenode.NameNodeRpcServer.getDatanodeReport(NameNodeRpcServer.java:928)
at org.apache.hadoop.hdfs.server.namenode.AuthorizationProviderProxyClientProtocol.getDatanodeReport(AuthorizationProviderProxyClientProtocol.java:390)
at org.apache.hadoop.hdfs.protocolPB.ClientNamenodeProtocolServerSideTranslatorPB.getDatanodeReport(ClientNamenodeProtocolServerSideTranslatorPB.java:694)
at org.apache.hadoop.hdfs.protocol.proto.ClientNamenodeProtocolProtos$ClientNamenodeProtocol$2.callBlockingMethod(ClientNamenodeProtocolProtos.java)
at org.apache.hadoop.ipc.ProtobufRpcEngine$Server$ProtoBufRpcInvoker.call(ProtobufRpcEngine.java:617)
at org.apache.hadoop.ipc.RPC$Server.call(RPC.java:1073)
at org.apache.hadoop.ipc.Server$Handler$1.run(Server.java:2141)
at org.apache.hadoop.ipc.Server$Handler$1.run(Server.java:2137)
at java.security.AccessController.doPrivileged(Native Method)
at javax.security.auth.Subject.doAs(Subject.java:415)
at org.apache.hadoop.security.UserGroupInformation.doAs(UserGroupInformation.java:1912)
at org.apache.hadoop.ipc.Server$Handler.run(Server.java:2135)
```

Debe añadir manualmente as_user al grupo de SO que está definido en las propiedades de configuración hdfs-site: **dfs.permissions.supergroup/dfs.permissions.superusergroup**.

- Para Cloudera, el valor de propiedad predeterminado es **supergroup** y debe cambiarse a un grupo de SO que existe realmente. Para obtener información sobre el valor de supergroup en Cloudera, consulte la documentación de Cloudera.
- Para Ambari, el valor de propiedad predeterminado es **hdfs**. De forma predeterminada, durante una instalación de Ambari,Analytic Server añade as_user a los grupos HDFS y Hadoop.

En Linux, utilice el mandato **usermod** para añadir as_user al HDFS **superusergroup** (si todavía no existe).

Para obtener información general sobre los permisos de HDFS, consulte HDFS Permissions Guide.

Los trabajos MapReduce fallan en HDP 3.0

Puede encontrar el siguiente error con los trabajos MapReduce en HDP 3.0:

```
No se ha podido completar la solicitud. Razón: java.lang.IllegalStateException: El trabajo está en estado DEFINE en lugar
de RUNNING (as_trace.log)
```

El estado de error puede revolverse de la siguiente manera:

1. Añada la configuración siguiente en el archivo `Custom analytics.cfg`:
   ```
   exclude.mapreduce.jars=icu4j-
   ```
2. Reinicie Analytic Server.

Una vez reiniciado Analytic Server, los trabajos MapReduce se ejecutarán de forma normal.

Problemas con el repositorio de metadatos

La operación CREATE USER falla cuando se ejecuta el script add_mysql_user

Antes de ejecutar el script **add_mysql_user**, deberá eliminar manualmente el usuario que esté intentando añadir de la base de datos MySQL. Puede eliminar los usuarios a través de la interfaz de usuario del entorno de trabajo de MySQL, o a través de los mandatos de MySQL. Por ejemplo:

```
mysql -u root -e "DROP USER '$AEDB_USERNAME_VALUE'@'localhost';"
mysql -u root -e "DROP USER '$AEDB_USERNAME_VALUE'@'$METASTORE_HOST';"
mysql -u root -e "DROP USER '$AEDB_USERNAME_VALUE'@'%';"
```

En los mandatos anteriores, sustituya $AEDB_USERNAME_VALUE por el nombre de usuario que desee eliminar, y sustituya $METASTORE_HOST por el nombre del host en el que se haya instalado la base de datos.

Problemas con Apache Spark

Problemas con las secuencias que se ejecutan en un proceso de Spark

Las secuencias de SPSS Modeler no logran completarse cuando están obligadas a ejecutarse en un proceso Spark. Las secuencias de SPSS Modeler que fallan se construyen con un nodo de origen de Analytic Server (archivo HDFS), que está enlazado con un nodo `Sort` y, a continuación, establezca exportar a otro origen de datos de Analytic Server. Después de que se ejecute la secuencia, la interfaz de usuario del gestor de recursos indica que se ejecuta la nueva aplicación, pero la secuencia nunca se completa y permanece en un estado `Running`. No hay ningún mensaje que indica por qué la secuencia no se logra completar en los registros de Analytic Server, de YARN o de Spark.

El problema se puede resolver añadiendo el valor `spark.executor.memory` al archivo personalizado `analytics.cfg` en la configuración de Analytic Server. Establecer el valor de memoria en 4 GB permite que las secuencias de SPSS Modeler anteriormente fallidas se completen en menos de 2 minutos (en un entorno de un único clúster de nodo).

No se han podido ejecutar los trabajos de Spark con Cloudera 5.x ni Spark 1.x

Puede encontrarse con la siguiente excepción al utilizar Cloudera 5.x con Spark 1.x:

```
org.apache.spark.SparkException: Exception when registering SparkListener
```

La excepción está causada porque `java.lang.ClassCastException: com.cloudera.spark.lineage.ClouderaNavigatorListener` no puede emitir `org.apache.spark.scheduler.SparkListener`.

Para evitar la excepción, debe añadir la línea siguiente en el área **Analytic Server Advanced Configuration Snippet (Safety Valve) for analyticserver-conf/config.properties**.

```
spark.extraListeners=org.apache.spark.JavaSparkListener
```

El error "Excepción durante HdfsAuthcom.spss.utilities.i18n.LocException:la ejecución ha fallado. Motivo: com.spss.ae.filesystem.exception.FileSystemException: No se ha podido inicializar el acceso al sistema de archivos." Se he encontrado al ejecutar los casos SparkML.

El error se ha generado cuando Spark no ha podido encontrar el directorio de registro. Un método alternativo para resolver este problema consiste en redirigir `spark.lineage.log.dir` a `/ae_wlpserver/usr/servers/aeserver/logs/spark`.

Clústeres de alta disponibilidad

Analytic Server no se puede añadir a más hosts debido a cambios en dependencias.

Ejecute el script `update_clientdeps` utilizando las instrucciones que figuran en "Actualización de las dependencias del cliente" en la página 28.

"El servicio de clúster de análisis ha perdido inesperadamente contacto con Zookeeper, esta JVM se está terminando para mantener la integridad del clúster."

Un aspecto que puede causar este problema es que la cantidad de datos que se graben en Zookeeper sea demasiado grande. Si, en los registros de Zookeeper hay excepciones como, por ejemplo:

```
java.io.IOException: Unreasonable length = 2054758
```

o en los registros de Analytic Server hay mensajes como, por ejemplo:

```
Causado por: java.io.UTFDataFormatException: serie codificada demasiada larga: 2054758 bytes
  en java.io.DataOutputStream.writeUTF(DataOutputStream.java:375)
```

1. En la consola de Ambari, vaya hasta la pestaña Configs del servicio Zookeeper y añada la línea siguiente a env-template y, después, reinicie el servicio Zookeeper.

   ```
   export JVMFLAGS="-Xmx2048m -Djute.maxbuffer=2097152"
   ```

2. En la consola de Ambari, vaya hasta la pestaña Configs del servicio Analytic Server y añada lo siguiente en Advanced analytics-jvm-options y, a continuación, reinicie el servicio de clúster de análisis.

   ```
   -Djute.maxbuffer=2097152
   ```

El número para especificar para el valor de jute.maxbuffer debe ser mayor que el número indicado en los mensajes de excepción.

Los datos de transacciones de Zookeeper dejan de ser gestionables

Establezca el parámetro **`autopurge.purgeInterval`** de `zoo.cfg` en 1 para habilitar las depuraciones automáticas del registro de transacciones de Zookeeper.

El servicio de clúster de análisis ha perdido contacto con Zookeeper

Revise y modifique los parámetros **`tickTime`**, **`initLimit`** y **`syncLimit`** de `zoo.cfg`. Por ejemplo:

```
# El número de milisegundos de cada marca
tickTime=2000
# El número de marcas que la
# fase de sincronización inicial puede aceptar
initLimit=30
# El número de marcas que pueden pasar entre
# el envío de una solicitud y la obtención de un acuse de recibo
syncLimit=15
```

Consulte la documentación de Zookeeper para obtener detalles: https://zookeeper.apache.org/doc/r3.3.3/zookeeperAdmin.html

Los trabajos de Analytic Server no se reanudan

Hay un situación común en la que los trabajos de Analytic Server no se reanudan.

- Cuando un trabajo de Analytic Server falla porque falla un miembro de clúster, el trabajo se suele reiniciar automáticamente en otro miembro de clúster. Si el trabajo no se reanuda, compruebe para asegurarse de que haya al menos 4 miembros de clúster en el clúster de alta disponibilidad.

Avisos

Esta información se ha desarrollado para productos y servicios que se comercializan en los EE.UU. Este material puede estar disponible en IBM en otros idiomas. Sin embargo, es probable que sea necesario que disponga de una copia del producto o versión del producto en dicho idioma para tener acceso.

Es posible que IBM no ofrezca en otros países los productos, servicios o características que se describen en este documento. Póngase en contacto con el representante local de IBM, que le informará sobre los productos y servicios disponibles actualmente en su área. Las referencias a programas, productos o servicios de IBM no pretenden establecer ni implicar que sólo puedan utilizarse dichos productos, programas o servicios de IBM. En su lugar, se puede utilizar cualquier producto, programa o servicio equivalente que no infrinja ninguno de los derechos de propiedad intelectual de IBM. No obstante, 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 patente pendientes que cubran la materia descrita 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-NC119
Armonk, NY 10504-1785
EE.UU.

Si tiene consultas sobre licencias relacionadas con información DBCS (de doble byte), póngase en contacto con el Departamento de propiedad intelectual de IBM en su país o envíelas, por escrito, a:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokio 103-8510, Japón

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍAS DE NINGÚN TIPO, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUIDAS, AUNQUE SIN LIMITARSE A, LAS GARANTÍAS DE NO CONTRAVENCIÓN, COMERCIALIZACIÓN O ADECUACIÓN A UN PROPÓSITO DETERMINADO. Algunas jurisdicciones no permiten la renuncia a las garantías explícitas o implícitas en determinadas transacciones; por lo tanto, es posible que esta declaración no sea aplicable en su caso.

Es posible que esta información contenga imprecisiones técnicas o errores tipográficos. Periódicamente se realizan cambios en la información que aquí se presenta; estos cambios se incorporarán en las 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 hechas en esta publicación a sitios web que no son de IBM se proporcionan sólo para la comodidad del usuario y no constituyen un aval de esos sitios web. Los materiales de dichos sitios web no forman parte del material de este producto de IBM y el usuario es el único responsable del uso que haga de ellos.

IBM puede utilizar o distribuir la información que se le proporcione del modo que considere adecuado sin incurrir por ello en ninguna obligación con el remitente.

Los titulares de licencias de este programa que deseen obtener información sobre el mismo con el fin de permitir: (i) el intercambio de información entre programas creados independientemente y otros programas (incluido éste) y (ii) el uso mutuo de la información que se ha intercambiado, deben ponerse en contacto con:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
EE.UU.

Dicha información puede estar disponible, sujeta a los términos y condiciones correspondientes, incluyendo, 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 los proporciona IBM bajo los términos de las Condiciones Generales de IBM, Acuerdo Internacional de Programas Bajo Licencia de IBM o cualquier acuerdo equivalente entre las partes.

Los ejemplos de datos de rendimiento y de clientes citados se presentan solamente a efectos ilustrativos. Los resultados de rendimiento reales pueden variar en función de las configuraciones específicas y de las condiciones de funcionamiento.

La información relativa a productos que no son de IBM se ha obtenido de los proveedores de dichos productos, de los anuncios publicados y de otras fuentes de información pública. IBM no ha comprobado estos productos y no puede confirmar la precisión de su rendimiento, compatibilidad ni contemplar ninguna otra reclamación relacionada con los productos que no son de IBM. Las preguntas relacionadas con 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 están sujetas a cambio o retirada sin previo aviso y representan únicamente objetivos y metas.

Todos los precios de IBM que se muestran son precios actuales recomendados por IBM de venta al público y están sujetos a cambios sin notificación previa. Los precios en los distribuidores pueden variar.

Esta información es sólo para fines de planificación. Dicha información está sujeta a cambios antes de que los productos descritos estén disponibles.

Esta información contiene ejemplos de datos e informes utilizados en operaciones empresariales diarias. Para ilustrarlas lo mejor posible, los ejemplos contienen nombres de personas, compañías, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con personas o empresas comerciales reales es pura coincidencia.

LICENCIA DE DERECHOS DE AUTOR:

Esta información contiene ejemplos de datos e informes utilizados en operaciones empresariales diarias. Para ilustrarlas lo mejor posible, los ejemplos contienen nombres de personas, compañías, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con personas o empresas comerciales reales es pura coincidencia.

Cada copia o cada parte de estos programas de ejemplo, o trabajos derivados, debe incluir un aviso de copyright como se indica a continuación:

Marcas registradas

IBM, el logotipo de IBM e ibm.com son marcas registradas o marcas comerciales registradas de International Business Machines Corp., registrada en muchas jurisdicciones en todo el mundo. Otros nombres de productos y servicios podrían ser marcas registradas de IBM u otras compañías. En Internet hay disponible una lista actualizada con las marcas registradas de IBM, en "Copyright and trademark information", en la dirección www.ibm.com/legal/copytrade.shtml.

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

IT Infrastructure Library es una marca registrada de la Agencia central de informática y telecomunicaciones que ahora es parte de la Cámara de Comercio.

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 de Intel Corporation o de sus subsidiarias en EE.UU. y en otros países.

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

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

ITIL es una marca registrada, y una marca de comunidad registrada de The Minister for the Cabinet Office, y está registrada en U.S. Patent and Trademark Office.

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

Cell Broadband Engine es una marca comercial de Sony Computer Entertainment, Inc. en Estados Unidos, otros países o ambos y se utiliza bajo licencia.

Linear Tape-Open, LTO, el logotipo de LTO, Ultrium y el logotipo de Ultrium son marcas comerciales de HP, IBM Corp. y Quantum en Estados Unidos y otros países.

Impreso en España