IBM SPSS Analytic Server
Versión 3.0.1

Guía de instalación y de configuración

Nota
Antes de utilizar esta información y el producto al que da soporte, lea la información del apartado "Avisos" en la página 51.

Información sobre el producto

Esta edición se aplica a la versión 3, release 0, 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 1

Capítulo 2. Instalación y configuración de Ambari 3
Requisitos previos específicos de Ambari 3
Instalación en Ambari 3
Instalación fuera de línea 4
Instalación de Analytic Server en un entorno MySQL gestionado externamente 5
Configuración 6
Seguridad 6
Habilitación del soporte para Essentials for R . . 11
Habilitación de orígenes de bases de datos relacionales 12
Habilitación de orígenes de datos de HCatalog 13
Cambio de puertos utilizados por Analytic Server 14
Analytic Server de alta disponibilidad 14
Optimización de opciones de la JVM para datos pequeños 14
Actualización de las dependencias del cliente . . 15
Configuración de Apache Knox. 15
Actualización y migración 19
desinstalar. 22
Desinstalación de Essentials for R 22

Capítulo 3. Instalación y configuración de Cloudera 23
Visión general de Cloudera 23
Requisitos previos específicos de Cloudera 23
Configuración de MySQL para Analytic Server 23
Instalación en Cloudera 24
Configuración de Cloudera 26
Seguridad 26
Habilitación del soporte para Essentials for R . . 30
Habilitación de orígenes de bases de datos relacionales 31
Habilitación de orígenes de datos de HCatalog 32
Cambio de puertos utilizados por Analytic Server 33
Analytic Server de alta disponibilidad 33
Optimización de opciones de la JVM para datos pequeños 33
Migración 33
Desinstalación de Analytic Server en Cloudera . . 34

Capítulo 4. Instalación y configuración de MapR 35
Visión general de MapR 35
Instalación de Analytic Server en MapR 35
Configuración de MapR 38
Habilitación del retrotracción de base de datos . 38
Habilitación de Apache Hive 38
Habilitación de Apache HBase 40
Habilitación de Apache Spark 40
Habilitación de distintivos de característica . . . 41
Habilitación de R 41
Habilitación de LZO 41
Configuración de un clúster de IBM SPSS Analytic Server para MapR 42
Desinstalación de MapR 42
Migración de IBM SPSS Analytic Server en MapR 42
Resolución de problemas de MapR 44

Capítulo 5. Configuración de IBM SPSS Modeler para su uso con IBM SPSS Analytic Server 45

Capítulo 6. Resolución de problemas 47

Avisos 51
Marcas registradas 53

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**.

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

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.

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 Si desea 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.

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, se deberá asegurar de que HDFS, YARN, MapReduce2, Hive y Zookeeper se han añadido como servicios Ambari.

SSH sin contraseña

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

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. A continuación figuran unos pasos más detallados.

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 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 http://ibm-open-platform.ibm.com.

   [Solo GPFS (Spectrum Scale)] Descargue el archivo http://ibm-open-platform.ibm.com/repos/IBM-SPSS-AnalyticServer/3.0.1.0/x86_64/IBM-SPSS-AnalyticServer-3.0.1.0.repo (x86) o https://ibm-open-platform.ibm.com/repos/IBM-SPSS-AnalyticServer/3.0.1.0/ppc64le/IBM-SPSS-AnalyticServer-3.0.1.0.repo (ppc64le) y colóquelo en la carpeta `/etc/yum.repos.d` (RHEL, CentOS) o `/etc/zypp/repos.d` (SLES) en todos los nodos en los que añada el Metastore de Analytic Server como un servicio.

   Instalación fuera de línea

   Elija fuera de línea si el host del servidor Ambari no tiene acceso a Internet. Para obtener información detallada, consulte “Instalación fuera de línea” en la página 4.
3. Reinicie el servidor Ambari.

   ```
   ambari-server restart
   ```
4. Inicie 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.

   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://{HOST_DB2}:{PUERTO}/{Nombre_BD}:currentSchema={Nombre_esquema};`, donde
   - {HOST_DB2} 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**.

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

5. 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 6. Para obtener información sobre la migración de una configuración existente a una nueva instalación, consulte el tema: "Actualización y migración" en la página 19.
6. 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 sesión como administrador de Analytic Server. De forma predeterminada este ID de usuario es admin y la contraseña es admin.

Instalación fuera de línea

La instalación fuera de línea descarga los archivos RPM necesarios y debe ejecutarse en una máquina que pueda acceder a https://ibm-open-platform.ibm.com/repos/IBM-SPSS-AnalyticServer/3.0.1.0/. El archivo binario ejecutable se encuentra en los directorios de distribución de Ambari `<AS_INSTALLABLE_HOME>` disponibles. Copie todo el contenido del directorio de `<AS_INSTALLABLE_HOME>` adecuado en el host del servidor Ambari.

1. Instale la herramienta que le permitirá crear un repositorio Yum local.

   ```
   yum install createrepo
   ```

2. Cree un nuevo directorio que actuará como repositorio para los archivos de RPM de Analytic Server. Consulte el ejemplo siguiente.

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

3. Copie los archivos de RPM necesarios de Analytic Server en este directorio. Los archivos de RPM que necesita dependen de la distribución, la versión y la arquitectura, tal como se muestra a continuación.

   BigInsights 4.2 (x86_64)

   ```
   IBM-SPSS-AnalyticServer-ambari-2.1-BI-4.2-3.0.1.0-1.x86_64.rpm

   IBM-SPSS-AnalyticServer-3.0.1.0-1.x86_64.rpm
   ```

   BigInsights 4.2 (PPC64LE)

   ```
   IBM-SPSS-AnalyticServer-ambari-2.1-BI-4.2-3.0.1.0-1.ppc64le.rpm

   IBM-SPSS-AnalyticServer-3.0.1.0-1.ppc64le.rpm
   ```

   HDP 2.4 (x86_64)

   ```
   IBM-SPSS-AnalyticServer-3.0.1.0-1.x86_64.rpm

   IBM-SPSS-AnalyticServer-ambari-2.1-HDP-2.4-3.0.1.0-1.x86_64.rpm
   ```

4. Cree la definición del repositorio local. Por ejemplo, cree un archivo denominado `IBM-SPSS-AnalyticServer-3.0.1.0.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
   ```

5. Cree el repositorio Yum local. Consulte el ejemplo siguiente.

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

6. 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 persistidas en el mandato de instalación ejecutable binario y emite el mandato de plataforma adecuado (parda instalar las rpm).
7. 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_acceso al repositorio local}/</URL_base>
           <repoid>IBM-SPSS-AnalyticServer</repoid>
           <reponame>IBM-SPSS-AnalyticServer-3.0.1.0</reponame>
      </repo>
   </os>
   ```

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 `/opt/AS_Installable/IBM-SPSS-AnalyticServer` en el nodo/host donde está instalada la instancia MySQL que se utilizará como `AS_MetaStore`. Por ejemplo, `/opt/AS_InstallTools`.
   - 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` and `-t` para pasar `dbuserid` y `dbuserid_password`. El script utiliza `dbuserid` y `dbuserid_password` para realizar operaciones MySQL.
4. Reinicie el servidor Ambari.
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 está desplegado Analytic Server; por ejemplo, `>/opt/IBM/SPSS/AnalyticServer/{version}`.
- {RAÍZ_SERVIDOR_AS} hace referencia a la ubicación de los archivos de configuración, registro y servidor; por ejemplo, `/opt/IBM/SPSS/AnalyticServer/{version}/ae_wlpserver/usr/servers/aeserver`.
- {INICIO_AS} hace referencia a la ubicación de HDFS que utiliza Analytic Server como carpeta raíz.

Seguridad

El parámetro **`security.config`** define el registro de usuarios y grupos que se pueden añadir como principales al sistema de Analytic Server.

De forma predeterminada, se define un registro básico con un único usuario, `admin`, con la contraseña `admin`. Para cambiar el registro edite **`security.config`** o configure Kerberos. Puede encontrar el parámetro **`security.config`** en la sección **Advanced analytics.cfg** de la pestaña Configs del servicio Analytic Server.

Nota: Si edita el parámetro **`security.config`** para modificar el registro, luego tiene que añadir nuevos usuarios como principales al sistema de Analytic Server. Consulte la *IBM SPSS Analytic ServerGuía del administrador* para obtener detalles sobre la gestión del inquilino.

Realización de cambios en el registro básico

El registro básico permite definir una base de datos de usuarios y grupos en el parámetro **`security.config`**.

El registro básico predeterminado es parecido al siguiente.

```
<basicRegistry id="basic" realm="ibm">
   <user name="admin" password="admin"/>
</basicRegistry>
```

A continuación se proporciona un ejemplo de registro básico modificado.

```
<basicRegistry id="basic" realm="ibm">
  <user name="usuario1" password="{xor}Dz4sLG5tbGs="/>
  <user name="usuario2" password="Pass"/>
  <user name="usuario3" password="Pass"/>
  <user name="usuario4" password="Pass"/>
  <user name="admin" password="{xor}KzosKw=="/>
  <group name="Desarrollo">
    <member name="usuario1"/>
    <member name="usuario2"/>
  </group>
  <group name="QA">
    <member name="usuario3"/>
    <member name="usuario4"/>
  </group>
  <group name="ADMIN">
    <member name="usuario1"/>
    <member name="admin"/>
  </group>
</basicRegistry>
```

Las contraseñas pueden codificarse para ocultar sus valores con la herramienta securityUtility, ubicada en `{RAÍZ_AS}/ae_wlpserver/bin`.

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

Nota: Consulte http://www-01.ibm.com/support/knowledgecenter/SSD28V_8.5.5/com.ibm.websphere.wlp.core.doc/ae/rwlp_command_securityutil.html si desea detalles de la herramienta securityUtility.

Nota: El registro básico es útil en un entorno de recinto de seguridad (sandbox), pero no se recomienda en un entorno de producción.

Configurar un registro 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>



<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 usuario 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".

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

1. Inicie 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 sesión en la consola de Ambari y actualice el valor de configuración de Analytic Server **ssl.keystore.config** 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 de Analytic Server **security.config** 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.

   Nota: Si la instalación de Analytic Server utiliza un registro básico, debe incluir las cuentas de usuario de Kerberos, utilizando "-" como la contraseña. A continuación se proporciona un ejemplo.

```
<basicRegistry id="basic" realm="ibm">
  <user name="admin" password="-"/>
  <user name="user1" password="-"/>
  <user name="user2" password="-"/>
  <group name="group1">
     <member name="admin"/>
     <member name="usuario1"/>
     <member name="usuario2"/>
  </group>
  <group name="grupo2">
     <member name="admin"/>
     <member name="usuario1"/>
  </group>
</basicRegistry>
```

2. 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 mediante el mandato kinit para iniciar 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.

3. 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.
4. [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 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 Amabri 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 Amabri.

Ahora los usuarios pueden iniciar una sesión en Analytic Server utilizando el SSO de Kerberos.

Inhabilitación de Kerberos

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

   ```
   default.security.provider
   hdfs.keytab
   hdfs.user
   java.security.krb5.conf
   jdbc.db.connect.method.kerberos
   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/3.0/ae_wlpserver/bin/securityUtility encode <contraseña>`

   Si desea generar un certificado firmado automáticamente, puede utilizar securityUtility; por ejemplo: `/opt/ibm/spss/analyticserver/3.0/ae_wlpserver/bin/securityUtility createSSLCertificate --server=myserver --password=mypassword --validity=365 --subject=CN=mycompany,O=myOrg,C=myCountry`.

   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.

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. Descargue el archivo autoextraíble (BIN) para el RPM de IBM SPSS Modeler Essentials for R. 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.
2. 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 http://ibm-open-platform.ibm.com.

[Solo GPFS (Spectrum Scale)] Descargue el archivo http://ibm-open-platform.ibm.com/repos/IBM-SPSS-ModelerEssentialsR/3.0.1.0/x86_64/IBM-SPSS-AnalyticServer-3.0.1.0.repo (x86) o http://ibm-open-platform.ibm.com/repos/IBM-SPSS-ModelerEssentialsR/3.0.1.0/x86_64/IBM-SPSS-AnalyticServer-3.0.1.0.repo (ppc64le) y colóquelo en la carpeta `/etc/yum.repos.d` (RHEL, CentOS) o `/etc/zypp/repos.d` (SLES) en todos los nodos en los que añada el Metastore de Analytic Server como un servicio.

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 de RPM necesarios y se deberá ejecutar en una máquina que pueda acceder a http://ibm-open-platform.ibm.com. Los archivos de RPM se pueden copiar en el host del servidor Ambari.

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

   BigInsights 4.2 (x86_64)
   `IBM-SPSS-ModelerEssentialsR-ambari-2.1-BI-4.2-8.4.0.0-1.x86_64.rpm`

   BigInsights 4.2 (PPC64LE)
   `IBM-SPSS-ModelerEssentialsR-ambari-2.1-BI-4.2-8.4.0.0-1.ppc64le.rpm`

   HDP 2.4 (x86_64)
   `IBM-SPSS-ModelerEssentialsR-ambari-2.1-HDP-2.4-8.4.0.0-1.x86_64.rpm`

b. Instale el RPM. Por ejemplo, el mandato siguiente instala Essentials for R en BigInsights 4.1.

```
rpm -i IBM-SPSS-ModelerEssentialsR-ambari-2.1-BI-4.2-8.4.0.0-1.x86_64.rpm
```

3. Reinicie el servidor Ambari.

```
ambari-server restart
```

4. Inicie 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.

5. Renueve el servicio Analytic Server.
6. Ejecute el script `update_clientdeps` utilizando las instrucciones que figuran en "Actualización de las dependencias del cliente" en la página 15.
7. 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 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 1. 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
DashDB	Bluemix Service	db2jcc.jar	IBM
DB2 para Linux, UNIX y Windows	10.5, 10.1, 9.7	db2jcc.jar	IBM
DB2 z/OS	11, 10	db2jcc.jar, db2_license_cisuz.jar	IBM
Greenplum	5, 4.2.x	postgresql.jar	Greenplum
Hive	1.1, 1.2	hive-jdbc-*.jar	Apache
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
Sybase IQ	16.x, 15.4, 15.2	jconnect70.jar	Sybase
Teradata	14, 14.1, 15	tdgssconfig.jar, terajdbc4.jar	Teradata

Nota: 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 todos los nodos Analytic Server.
3. Reiniciar el servicio Hive Metastore.
4. Renovar el servicio Analytic Metastore.
5. Reiniciar todas las instancias del servicio Analytic Server.

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.

Apache Spark

Si desea utilizar Spark (versión 1.5 o posterior) con el origen de datos de entrada HCatalog, debe añadir manualmente la propiedad `spark.version` al archivo `analytics.cfg` personalizado.

1. Abra la consola de Amabri y añada la propiedad siguiente en la sección Analytic Server **Custom analytics.cfg**.
   - **Key**: `spark.version`
   - **Value**: Especifique el número de versión de Spark (por ejemplo, `1.5`).
2. Guarde la configuración y reinicie todos los servicios Analytic Server desde la consola Amabri.

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**.

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/2.4/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.

Importante: Analytic Server no se puede instalar en el mismo nodo de clúster que el servidor Knox.

Requisitos previos

- Analytic Server no se puede instalar en el mismo nodo de clúster que el servidor Knox.
- Los nodos de Analytic Server se deben conectar con el servidor Knox server 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_0.7-3.0.0.0.jar`: El archivo se debe copiar desde la ubicación de Analytic Server:

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

  al 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:.

  `<Analytic_Server_Installation_Path>/ae_wlpserver/usr/servers/aeserver/configuration/knox`

  al nodo del servidor Knox:

  `/KnoxServicePath/data/services`

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

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 el siguiente `<service>` en la configuración de Knox:

   ```
   <service>
       <role>ANALYTICSERVER</role>
       <url>http://{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. En el servidor Knox, cree el subdirectorio <knox_server>/data/service/analyticserver/3.0, a continuación cargue los archivos service.xml y rewrite.xml en el nuevo directorio. Los dos archivos en Analytic Server en <analytic_server>/configuration/knox/analyticserver/3.0.1 (por ejemplo,/opt/ibm/spss/analyticserver/3.0/ae_wlpserver/usr/servers/aeserver/configuration/knox/analyticserver/3.0/*.xml)
2. En <knox_server>/bin, ejecute el script ./knoxcli.sh redeploy --cluster default
3. Cargue el archivo com.ibm.spss.knoxservice_0.7.0-*.jar en <knox_server>/ext. El archivo se encuentra en Analytic Server en <analytic_server>/apps/AE_BOOT.war/WEB-INF/lib/com.ibm.spss.knox_0.7-3.0.1.0.jar (por ejemplo,/opt/ibm/spss/analyticserver/3.0/ae_wlpserver/usr/servers/aeserver/apps/AE_BOOT.war/WEB-INF/lib/com.ibm.spss.knox_0.7-3.0.1.0.jar).
4. En la interafz de usuario Ambari, añada el elemento siguiente en **Knox** > **Configs** > **Advanced topology**:

   ```
   <service>
      <role>ANALYTICSERVER</role>
      <url>http://{AS-Host}:{AS-port}/analyticserver</url>
   </service>
   ```
5. En la interaz de usuario Ambari, añada o actualice los usuarios en **Knox** > **Configs** > **Advanced users-ldif** (por ejemplo admin, qauser1, qauser2).
6. Reinicie LDAP desde **Knox** > **Service Actions** > **Start Demo LDAP**.
7. Reinicie el servicio Knox.

Instalación de Apache Knox on Hortonworks Data Platform (HDP)

Los pasos siguientes describen el proceso de instalación de Apache Knox en un clúster. HDP

1. Verifique si un usuario de Knox existe en el clúster HDP. Si un usuario Knox no existe, debe crear uno.
2. Descargue y extraiga Apache Knox en una carpeta bajo /home/knox.
3. En HDP, cambie al usuario Knox y vaya a la carpeta knox. El usuario Knox debe tener permission(RWX) en todas las subcarpetas knox.
4. Configure Apache Knox para Analytic Server. Para obtener más información, consulte la sección **Configuración de Apache Knox**.
   a. Cree una jerarquía de carpetas analyticserver/3.0.1 en {knox}/data/services.
   b. Copie los archivos rewrite.xml y service.xml de la ubicación de Analytic Server:.

      /opt/ibm/spss/analyticserver/3.0.1/ae_wlpserver/usr/servers/aeserver/configuration/knox/analyticserver/3.0.1

      al nodo del servidor Knox:

      {knox}/data/services/analyticserver/3.0.1
   c. Copie el archivo *.jar de Knox en el host de Analytic Server:

      /opt/ibm/spss/analyticserver/3.0.1/ae_wlpserver/usr/servers/aeserver/apps/AE_BOOT.war/WEB-INF/lib/com.ibm.spss.knox_0.7-*.jar

en el directorio ext de Knox:

{knox}/ext

d. Actualice el archivo default.xml en {knox}/conf/topologies para que coincida con el ejemplo siguiente:

Nota: Debe crear el archivo si no existe.

```
<topology>
   <gateway>
      <provider>
         <role>authentication</role>
         <name>ShiroProvider</name>
         <enabled>true</enabled>
         <param>
            <name>sessionTimeout</name>
            <value>30</value>
         </param>
         <param>
            <name>main.ldapRealm</name>
            <value>org.apache.hadoop.gateway.shirorealm.KnoxLdapRealm</value>
         </param>
         <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://localhost:33389</value>
         </param>
         <param>
            <name>main.ldapRealm.contextFactory.authenticationMechanism</name>
            <value>simple</value>
         </param>
         <param>
            <name>urls./**</name>
            <value>authcBasic</value>
         </param>
      </provider>
      <provider>
         <role>identity-assertion</role>
         <name>Default</name>
         <enabled>true</enabled>
      </provider>
      <provider>
         <role>authorization</role>
         <name>AclsAuthz</name>
         <enabled>true</enabled>
      </provider>

   </gateway>

   <!--otro servicio-->
   <service>
      <role>ANALYTICSERVER</role>
      <!--replace the {AS-host}nas {AS-port} with real value-->
      <url>http://{AS-host}:{AS-port}/analyticserver</url>
   </service>

</topology>
```

5. Run {knox}/bin/knoxcli.sh.
6. Run {knox}/bin/ldap.sh start.

Nota: El script utiliza el puerto 33389. Asegúrese de que el puerto no está en uso actualmente.

7. Run {knox}/bin/gateway.sh start.

Nota: El script utiliza el puerto 8443. Asegúrese de que el puerto no está en uso actualmente.

8. Compruebe la instalación.
   a. Ejecute el mandato curl en Analytic Server en el URL de Knox:

```
curl -ikvu {username}:{password} https://{knox-host}:8443/gateway/default/analyticserver/admin
```

Resolución de problemas

Problema: Analytic Server no funciona en Knox tras la instalación.

Solución: Detenga Knox, elimine todos los archivos en `{knox}/data/deployments/*` y, a continuación, reinicie Knox.

Problema: No se puede iniciar la sesión en Analytic Server a través de Knox.

Solución: Verifique los usuarios en `{knox}/conf/users.ldif`. Actualice los usuarios existentes de o añada nuevos usuarios a Analytic Server. Los principales de usuario y las credenciales de Knox deben coincidir con los usuarios de Analytic Server.

Estructura de URL del Analytic Server habilitado para Apache Knox

El URL de interfaz de usuario de Analytic Server habilitado por Knox es `https://{knox-host}:{knox-port}/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`.

Actualización y migración

Analytic Server le permite actualizar o migrar valores y datos de configuración desde la instalación de Analytic Server hasta nueva instalación.

Actualización desde la versión 3.0 a 3.0.1

Si tiene una instalación existente de Analytic Server 3.0, puede actualizarla a la versión 3.0.1.

1. En la consola de Ambari, detenga el servicio Analytic Server.
2. En función del tipo de instalación, siga estos pasos.

   Actualización en línea

   a. Asegúrese de que el host del servidor Ambari y todos los nodos del clúster pueden acceder a http://ibm-open-platform.ibm.com.

   b. Descargue el archivo `IBM-SPSS-AnalyticServer-3.0.1.0.repo` from http://ibm-open-platform.ibm.com/repos/IBM-SPSS-AnalyticServer/3.0.1.0/x86_64/IBM-SPSS-AnalyticServer-3.0.1.0.repo (x86) o http://ibm-open-platform.ibm.com/repos/IBM-SPSS-AnalyticServer/3.0.1.0/ppc64le/IBM-SPSS-AnalyticServer-3.0.1.0.repo (ppc64le) en cada host de Analytic Server y múevalo a la carpeta `/etc/yum.repos.d` (RHEL or CentOS) o `/etc/zypp/repos.d` (SLES).

   Actualización fuera de línea

   a. La actualización fuera de línea descarga los archivos RPM y debe ejecutarse en una máquina que pueda acceder a http://ibm-open-platform.ibm.com/repos/IBM-SPSS-AnalyticServer/3.0.1.0/.

   b. Cree un nuevo directorio que actuará como repositorio para los archivos de RPM de Analytic Server. Consulte el ejemplo siguiente:

   ```
   mkdir /home/root/repos/IBM-SPSS-AnalyticServer/3.0.1.0/x86_64
   ```

   c. Copie los archivos de RPM necesarios de Analytic Server en este directorio. Los archivos de RPM que necesita dependen de la distribución, la versión y la arquitectura. Para BigInsights 4.1, los archivos necesarios se muestran a continuación.

Tabla 2. BigInsights 4.2 RPMs

BigInsights 4.2 (x86_64)	BigInsights 4.2 (PPC64LE)	HDP 2.4 (x86_64)
IBM-SPSS-AnalyticServer-ambari-2.1-BI-4.2-3.0.1.0-1.x86_64.rpm	IBM-SPSS-AnalyticServer-ambari-2.1-BI-4.2-3.0.1.0-1.ppc64le.rpm	IBM-SPSS-AnalyticServer-ambari-2.1-HDP-2.4-3.0.1.0-1.x86_64.rpm
IBM-SPSS-AnalyticServer-3.0.1.0-1.x86_64.rpm	IBM-SPSS-AnalyticServer-3.0.1.0-1.ppc64le.rpm	IBM-SPSS-AnalyticServer-3.0.1.0-1.x86_64.rpm

d. Cree la definición del repositorio local. Por ejemplo, cree un archivo llamado `analyticserver.repo` in `/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-3.0.1.0
baseurl=file:///{vía_acceso al repositorio local}
enabled=1
gpgcheck=0
protect=1
```

e. Cree el repositorio Yum local. Consulte el ejemplo siguiente:

```
createrepo /home/root/repos/IBM-SPSS-AnalyticServer/3.0.1.0/x86_64
```

3. Limpie los metadatos de Ambari de la memoria caché local. Por ejemplo, para limpiar la memoria caché en RHEL o en CentOS, ejecute el mandato siguiente:

```
sudo yum clean all
```

Nota: El mandato `yum` no funciona cuando hay dos repositorios de Analytic Server listados. Como resultado, los archivos `*.repo` originales relacionados con Analytic Server deben denominarse o eliminarse. En SLES, el mandato cambia del modo siguiente:

```
sudo zypper refresh
```

4. En cada host de Analytic Server, actualice los RPM. Por ejemplo, para actualizar en RHEL o en CentOS, ejecute los mandatos siguientes:

```
chown -R as_user:hadoop /opt/ibm/spss/analyticserver/3.0
sudo yum upgrade IBM-SPSS-AnalyticServer
```

En SLES, el mandato cambia de la manera siguiente:

```
sudo zypper up IBM-SPSS-AnalyticServer
```

5. Renueve la pila.

BigInsights

a. En la consola de Ambari, inicie y detenga a continuación el servicio Analytic Server.

b. Ejecute la acción personalizada **Renovar**.

Hortonworks

Navegue hasta uno de sus nodos de Analytic Server y ejecute el mandato siguiente:

```
sudo -u as_user /opt/ibm/spss/analyticserver/3.0/bin/refresh.sh
```

6. Instalación sólo fuera de línea. 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-3.0.1.0</reponame>
   </repo>
</os>
```

7. Borre el estado de Zookeeper. Ejecute el mandato siguiente en el directorio bin de Zookeper (por ejemplo, `/usr/iop/current/zookeeper-server/bin`):

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

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

Migración de una nueva versión de Analytic Server

Si tiene una instalación existente de Analytic Server 2.0 o 2.1 y ha adquirido 3.0, puede migrar los valores de configuración de 2.0/2.1 a la instalación de 3.0/3.0.1.

Restricciones:

- Si tiene instalada una versión anterior a 2.0, en primer lugar, debe migrar la versión anterior a 2.0/2.1 y, a continuación de la versión 2.0/2.1 a 3.0/3.0.1.
- Las instalaciones de 2.0/2.1 y 3.0/3.0.1 no pueden coexistir en el mismo clúster de Hadoop. Si configura la instalación de 3.0/3.0.1 para que utilice el mismo clúster de Hadoop que la instalación de 2.0/2.1, la instalación de 2.0/2.1 dejará de funcionar.

Pasos de migración, 2.0/2.1 a 3.0/3.0.1

1. Instale la nueva instalación de Analytic Server de acuerdo a las instrucciones de "Instalación en Ambari" en la página 3.
2. Copie la raíz analítica de la instalación antigua a su nueva instalación.
   a. Si desconoce la de la raíz analítica, ejecute `hadoop -fs ls`. La vía de acceso de la raíz analítica adoptará la forma `/user/aeuser/analytic-root`, donde aeuser es el ID de usuario que posee la raíz analítica.
   b. Cambie la propiedad de la raíz analítica de aeuser a as_user
      ```
      hadoop dfs -chown -R {as_user:{grupo}} {vía de acceso a analytic-root 2.0/2.1}
      ```
      Nota: Si tiene previsto utilizar la instalación existente de Analytic Server tras la migración, haga una copia del directorio analytic-root en HDFS y, después, cambie la propiedad en la copia del directorio.
   c. 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`, si existe.
   d. Ejecute el script de copia siguiente.
      ```
      hadoop distcp hftp://{host de 2.0/2.1 namenode}:50070/{path to 2.0/2.1 analytic-root}
      hdfs://{host of 3.0/3.0.1 namenode}/user/as_user/analytic-root
      ```
3. En la consola de Ambari, detenga el servicio Analytic Server.
4. Asegúrese de que el servicio Analytic Metastore se está ejecutando.
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.
6. 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/3.0/ASConfiguration_2.1.0.0.xxx.zip
   ```
7. Borre el estado de Zookeeper. En el directorio bin de Zookeper (por ejemplo, `/usr/hdp/current/zookeeper-client` en Hortonworks o `/usr/iop/current/zookeeper-server` en BigInsights), ejecute el mandato siguiente.
   ```
   ./zkCli.sh rmr /AnalyticServer
   ```
8. En la consola de Ambari, 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.

desinstalar

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 BigInsights 4.2, el directorio `ESSENTIALR` se encuentra en `/var/lib/ambari-server/resources/stacks/BigInsights/4.2/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

Repositorio de metadatos

Si tiene previsto utilizar MySQL como el repositorio de metadatos de Analytic Server, siga las instrucciones que figuran en "Configuración de MySQL para Analytic Server".

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 24.
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`.

6. Abra Cloudera Manager y vaya a la pestaña Configuration del servicio Analytic Server.
   a. En la propiedad **Analytic Server metastore driver class (jndi.aedb.driver)**, seleccione `com.mysql.jdbc.Driver`.
   b. Debe especificar valores coincidentes para el nombre de base de datos, el nombre de usuario de base de datos y la contraseña de base de datos de Analytic Server que anotó anteriormente, en el panel donde se especifiquen las entradas de configuración de Analytic Server. Deben actualizarse las propiedades **Analytic Server metastore repository URL (jndi.aedb.url)**, **Analytic Server metastore username (jndi.aedb.username)**y **Analytic Server metastore password (jndi.aedb.password)** para que coincidan con los valores que se hayan proporcionado al mandato `add_mysql_user.sh`.

Instalación en Cloudera

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

Instalación en línea

1. Descargue y 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.
2. Reinicie Cloudera Manager después de que se haya completado la instalación.
3. Abra la interfaz de Cloudera Manager (por ejemplo, `http://${HOST_CM}:7180/cmf/login` con las credenciales de inicio de sesión predeterminadas `admin/admin`), renueve el valor de **Remote Parcel Repository URLs** y verifique que los URL sean correctos. Por ejemplo:

   ```
   http://ibm-open-platform.ibm.com/repos/IBM-SPSS-AnalyticServer/3.0.1.0/cloudera/parcels/latest/

   o bien

   http://ibm-open-platform.ibm.com/repos/IBM-SPSS-AnalyticServer/3.0.1.0/cloudera/
   ```

   Nota: Los valores **Parcel Update Frequency** y **Remote Parcel Repository URLs** pueden actualizarse para que se ajusten sus necesidades específicas.
4. 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**.
5. Seleccione **Download** > **Distribute** > **Activate**. El estado del paquete **AnalyticServer** se actualiza a **Distributed, Activated**.
6. Configure MySQL para Analytic Server.
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:
   - Nombre de usuario de metastore de Analytic Server
   - Contraseña de metastore de Analytic Server

   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.

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-3.0.1.0-el6.parcel
- AnalyticServer-3.0.1.0-el6.parcel.sha
- manifest.json

  o bien
- AnalyticServer-3.0.1.0-el7.parcel
- AnalyticServer-3.0.1.0-el7.parcel.sha

SuSE Linux requiere los archivos siguientes:

- AnalyticServer-3.0.1.0-sles11.parcel
- AnalyticServer-3.0.1.0-sles11.parcel.sha
- manifest.json

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).

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

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

Actualización de Analytic Server en Cloudera

Si tiene una instalación existente de Analytic Server 3.0, puede actualizarla a la versión 3.0.1.

1. En Cloudera Manager, detenga y a continuación suprima el servicio de Analytic Server.
2. En Cloudera Manager, desactive la versión anterior de Analytic Server.
3. Consulte las secciones "En línea" o "Fuera de línea" en “Actualización y migración” en la página 19 para obtener instrucciones sobre cómo instalar Analytic Server 3.0.1.

   4. Después de que se haya instalado el servicio Analytic Server y lo haya añadido en Cloudera Manager, ejecute **Renovar binarios de Analytic Server**. Analytic Server 3.0.1 está ahora listo para su uso.

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 parámetro **`security_cfg`** define el registro de usuarios y grupos que se pueden añadir como principales al sistema de Analytic Server.

De forma predeterminada, se define un registro básico con un único usuario, `admin`, con la contraseña `admin`. Para cambiar el registro edite **`security_cfg`** o configure Kerberos como el proveedor de seguridad. Puede encontrar el parámetro **`security_cfg`** en la sección **Analytic Server Advanced Configuration Snippet** de la pestaña Configuration del servicio Analytic Server.

Nota: Si edita el parámetro **`security_cfg`** para modificar el registro, luego tiene que añadir nuevos usuarios como principales al sistema de Analytic Server. Consulte la *IBM SPSS Analytic ServerGuía del administrador* para obtener detalles sobre la gestión del inquilino.

Realización de cambios en el registro básico

El registro básico permite definir una base de datos de usuarios y grupos en el parámetro **`security_cfg`**.

El registro básico predeterminado es parecido al siguiente.

```
<basicRegistry id="basic" realm="ibm">
   <user name="admin" password="admin"/>
</basicRegistry>
```

A continuación se proporciona un ejemplo de registro básico modificado.

```
<basicRegistry id="basic" realm="ibm">
  <user name="usuario1" password="{xor}Dz4sLG5tbGs="/>
  <user name="usuario2" password="Pass"/>
  <user name="usuario3" password="Pass"/>
  <user name="usuario4" password="Pass"/>
  <user name="admin" password="{xor}KzosKw=="/>
  <group name="Desarrollo">
    <member name="usuario1"/>
    <member name="usuario2"/>
  </group>
  <group name="QA">
    <member name="usuario3"/>
    <member name="usuario4"/>
  </group>
  <group name="ADMIN">
    <member name="usuario1"/>
    <member name="admin"/>
  </group>
</basicRegistry>
```

Las contraseñas pueden codificarse para ocultar sus valores con la herramienta securityUtility, ubicada en `{RAÍZ_AS}/ae_wlpserver/bin`.

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

Nota: Consulte http://www-01.ibm.com/support/knowledgecenter/SSD28V_8.5.5/com.ibm.websphere.wlp.core.doc/ae/rwlp_command_securityutil.html si desea detalles de la herramienta securityUtility.

Nota: El registro básico es útil en un entorno de recinto de seguridad (sandbox), pero no se recomienda en un entorno de producción.

Configurar un registro LDAP

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

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>
```

Puede obtener ejemplos adicionales de configuraciones consultando la carpeta de plantillas {RAÍZ_AS}/ae_wlpserver/templates/config.

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

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

1. Inicie 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 sesión en Cloudera Manager y actualice el valor de configuración de Analytic Server **ssl_cfg** 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 de Analytic Server **security_cfg** 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.

1. Cree cuentas en el repositorio de usuarios de Kerberos para todos los usuarios a los que tiene previsto otorgar acceso a Analytic Server.

   Nota: Si la instalación de Analytic Server utiliza un registro básico, debe incluir las cuentas de usuario de Kerberos, utilizando "-" como la contraseña. A continuación se proporciona un ejemplo.

```
<basicRegistry id="basic" realm="ibm">
  <user name="admin" password="-"/>
  <user name="user1" password="-"/>
  <user name="user2" password="-"/>
  <group name="group1">
     <member name="admin"/>
     <member name="usuario1"/>
     <member name="usuario2"/>
  </group>
  <group name="grupo2">
     <member name="admin"/>
     <member name="usuario1"/>
  </group>
</basicRegistry>
```

2. 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 mediante el mandato kinit para iniciar 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.
3. 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.
4. [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 Configuración del servicio HDFS en Cloudera Manager.

      Nota: Los parámetros 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 parámetro **hadoop.proxyuser.hive.groups** para que tenga el valor `*` o un grupo que contiene todos los usuarios con permiso para iniciar 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 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 una sesión en Analytic Server utilizando el SSO de Kerberos.

Inhabilitación de Kerberos

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

   ```
   default.security.provider
   hdfs.keytab
   hdfs.user
   java.security.krb5.conf
   jdbc.db.connect.method.kerberos
   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.
4. Pulse **Guardar cambios** y reinicie el servicio Analytic Server.

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. 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.
2. 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++
3. 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 de R predeterminada que se instala es la 3.1.0. 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.

4. 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).
5. 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.
6. 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 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 3. 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
DashDB	Bluemix Service	`db2jcc.jar`	IBM
DB2 para Linux, UNIX y Windows	10.5, 10.1, 9.7	`db2jcc.jar`	IBM

Tabla 3. Bases de datos soportadas (continuación)

Base de datos	Versiones soportadas	Archivos JAR del controlador JDBC	Distribuidor
DB2 z/OS	11, 10	`db2jcc.jar`, `db2_license_cisuz.jar`	IBM
Greenplum	5, 4.2.x	postgresql.jar	Greenplum
Hive	1.1, 1.2	`hive-jdbc-*.jar`	Apache
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
Sybase IQ	16.x, 15.4, 15.2	`jconnect70.jar`	Sybase
Teradata	14, 14.1, 15	`tdgssconfig.jar`, `terajdbc4.jar`	Teradata

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 todos los nodos Analytic Server.
3. Reiniciar el servicio Hive Metastore.
4. Reiniciar todas las instancias del servicio Analytic Server.

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.

Apache Spark

Si desea utilizar Spark (versión 1.5 o posterior) con un origen de datos de entrada HCatalog, debe añadir manualmente la propiedad `spark.version=1.5.0`.

1. Abra Cloudera Manager y añada o actualice las propiedades siguientes en el área **Advanced Configuration Snippet (Safety Valve) for analyticserver-conf/config.properties** de Analytic Server.
   ```
   spark.version=1.5.0
   ```
2. Guarde la configuración y reinicie todos los servicios Analytic Server desde 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.

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
```

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 2.0/2.1 y ha adquirido una versión más reciente, puede migrar los valores de configuración de 2.0/2.1 a la nueva instalación.

Restricción: Si tiene una versión anterior a 2.0 instalada, en primer lugar, debe migrar la versión anterior a 2.0/2.1 y, después, de la versión 2.0/2.1 a la versión más reciente.

Restricción: Las instalaciones de la versión 2.0/2.1 y la nueva 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 2.0/2.1, la instalación de 2.0/2.1 dejará de funcionar.

Pasos de migración, 2.1 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 24.
2. Copie la raíz analítica de la instalación antigua a su nueva instalación.

a. Si desconoce la de la raíz analítica, ejecute `hadoop -fs ls`. La vía de acceso de la raíz analítica adoptará la forma `/user/aeuser/analytic-root`, donde aeuser es el ID de usuario que posee la raíz analítica.

b. Cambie la propiedad de la raíz analítica de aeuser a as_user

```
hadoop dfs -chown -R {as_user:{group}} {path to 2.1 analytic-root}
```

Nota: Si tiene previsto utilizar la instalación existente de Analytic Server tras la migración, haga una copia del directorio analytic-root en HDFS y, después, cambie la propiedad en la copia del directorio.

c. 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`, si existe.

d. Ejecute el script de copia siguiente.

```
hadoop distcp hftp://{host of 2.1 namenode}:50070/{path to 2.1 analytic-root}
hdfs://{host of 3.0 namenode}/user/as_user/analytic-root
```

3. En Cloudera Manager, detenga el servicio Analytic Server.
4. 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.
5. 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/3.0/ASConfiguration_2.1.0.0.xxx.zip
```

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. 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 Analytic Server.
2. Debe **Desactivar** y **Eliminar de los hosts** 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.

Capítulo 4. Instalación y configuración de MapR

Visión general de MapR

MapR es una distribución completa de Apache Hadoop que empaqueta más de una docena de proyectos del ecosistema de Hadoop para proporcionar un amplio conjunto de posibilidades de datos grandes.

No se puede acceder al sistema de archivos de MapR desde fuera del clúster de servidores. Como consecuencia, IBM SPSS Analytic Server debe desplegarse en los nodos de clúster de MapR. En este escenario de despliegue, debe ejecutar Analytic Server un usuario que tenga autorización para poder acceder al sistema de archivos de MapR y enviar trabajos a Yarn para desplegarlos en Analytic Server (como <as_user>).

Instalación de Analytic Server en MapR

En los pasos siguientes se detalla el proceso de instalar IBM SPSS Analytic Server manualmente en un clúster de MapR.

1. Ejecute el instalador de Analytic Server (spss_as-3.0.1.0-mapr5.1-lx86-64_en.bin) con un usuario root, o un usuario que pertenezca al grupo sudo. Siga las instrucciones de instalación para aceptar la licencia y seleccione instalar Analytic Server en línea o fuera de línea.
   a. Seleccione la opción en línea cuando el servidor en el que se aloja Analytic Server tenga una conexión a Internet a http://ibm-open-platform.ibm.com. El instalador instala Analytic Server automáticamente.
   b. Seleccione la opción fuera de línea cuando el servidor en el que se aloja Analytic Server no tenga una conexión a Internet a http://ibm-open-platform.ibm.com. Ejecute el instalador en otro servidor que tenga acceso al URL, y elija instalar Analytic Server fuera de línea. El instalador descarga el paquete RPM automáticamente.
2. Busque y ejecute el RPM de Analytic Server:

   ```
   rpm -ivh IBM-SPSS-AnalyticServer-3.0.1.0-1.x86_64.rpm
   ```

   Tanto para las modalidades de instalación en línea y fuera de línea, Analytic Server se instala en /opt/ibm/spss/analyticserver/3.0 (como <vía_acceso_instalación_as>).
3. Cambie todos los archivos de la vía de acceso de instalación del usuario que ejecute Analytic Server:

   ```
   chown -R <as_user> <vía_acceso_instalación_as>
   ```

   Cambie el usuario por <as_user>; todos los pasos posteriores utilizarán <as_user>.
4. Configure la propiedad HTTP. Cree un archivo denominado http_endpoint.xml en la vía de acceso <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver y añada al archivo las líneas siguientes:

   ```
   <server>
       <httpEndpoint host="*" id="defaultHttpEndpoint" httpPort="<puerto_http>" httpsPort="<puerto_https>" onError="FAIL"/>
   </server>
   ```

   <puerto_http> y <puerto_https> son los puertos que Analytic Server utiliza a través de los protocolos HTTP y HTTPS. Sustitúyalos por los puertos disponibles.
5. Añada usuarios y grupos. Cree un archivo denominado security_cfg.xml en la vía de acceso <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver y añada al archivo las líneas siguientes:

   ```
   <server>
       <basicRegistry id="basic" realm="ibm">
           <user name="admin" password="test"/>
       </basicRegistry>
   </server>
   ```

En el estado predeterminado, el archivo XML contiene sólo el usuario administrador. Debe añadir otros usuarios y grupos en el valor <basicRegistry> manualmente, o cambiar el valor por ldapRegistry.

6. Configure la base de datos de metadatos. Analytic Server da soporte a las bases de datos DB2 y MySQL.
   a. Configure los usuarios de la base de datos. Cuando utilice la base de datos MySQL, ejecute el script SQL siguiente en el shell MySQL:

      ```
      DROP DATABASE IF EXISTS <nombre_BD>;
      CREATE DATABASE <nombre_BD> DEFAULT CHARACTER SET utf8 DEFAULT COLLATE utf8_bin;
      CREATE USER '<nombre_usuario_BD>'@'%' IDENTIFIED BY '<contraseña_BD>';
      CREATE USER '<nombre_usuario_BD>'@'localhost' IDENTIFIED BY '<contraseña_BD>';
      GRANT ALL PRIVILEGES ON *.* TO '<nombre_usuario_BD>'@'%';
      GRANT ALL PRIVILEGES ON *.* TO '<nombre_usuario_BD>'@'localhost';
      ```

   b. Cifre la contraseña. Las contraseñas de los usuarios de base de datos deben cifrarse para que se puedan pasar a Analytic Server. Ejecute el mandato siguiente:

      ```
      java -Duser.language=en -cp <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/apps/AE_BOOT.war/WEB-INF/lib/*
      com.spss.ae.encryption.provider.EncryptKeystorePassword <contraseña_BD>
      ```

      Nota: Cuando el mandato se ejecuta directamente en un shell de Linux, es posible que el carácter * deba escaparse como *.

      La salida del mandato es la siguiente: La contraseña cifrada es '<contraseña cifrada>'. Tome nota de la contraseña de base de datos cifrada.

   c. Suprima el archivo <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/configuration/config.properties, si existe, y cree un archivo nuevo con el mismo nombre. Cambie las propiedades siguientes cuando utilice la base de datos DB2:

      ```
      jndi.aedb=jdbc/aeds
      jndi.aedb.url=jdbc:db2://<nombre_BD>:<puerto_BD>/<nombre_BD>:currentSchema=<nombre_esquema_BD>;
      jndi.aedb.driver=com.ibm.db2.jcc.DB2Driver
      jndi.aedb.username=<nombre_usuario_BD>
      jndi.aedb.password=<contraseña_DB_cifrada>
      ```

      Si el esquema <nombre_esquema_BD> no existe, el usuario <nombre_usuario_BD> deberá tener permiso implícito para poder crear el esquema. Cambie las propiedades siguientes cuando utilice la base de datos MySQL:

      ```
      jndi.aedb=jdbc/aeds
      jndi.aedb.url=jdbc:mysql://<host_BD>:<puerto_BD>/<nombre_BD>?createDatabaseIfNotExist=true
      jndi.aedb.driver=com.mysql.jdbc.Driver
      jndi.aedb.username=<nombre_usuario_BD>
      jndi.aedb.password=<contraseña_DB_cifrada>
      ```

   d. El controlador JDBC de MySQL debe estar instalado cuando utilice la base de datos MySQL. Ejecute el mandato siguiente:

      ```
      yum install mysql-connector-java
      ```

   e. Ejecute el mandato siguiente al crear las tablas necesarias:

      ```
      cd <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/sql/<tipo_BD>
      java -Xmx128m -Xms128m -cp <vía_instalación_as>/ae_wlpserver/usr/servers/aeserver/apps/AE_BOOT.war/WEB-INF/lib/*:/usr/share/java/*
      com.spss.ae.dbscript.ScriptRunner ../../configuration/config.properties schema.sql true
      ```

      <tipo_BD> es db2 o mysql, dependiendo de qué base de datos se utilice.

      Nota: Cuando se utiliza MySQL con el motor de MYISAM, el segundo mandato informa de los mensajes de error siguientes, que pueden ignorarse:

      ```
      Se ha producido un error al ejecutar: set global innodb_large_prefix=ON
      java.sql.SQLException: Variable de sistema desconocida 'innodb_large_prefix'
      Se ha producido un error al ejecutar: set global innodb_file_format=BARRACUDA
      java.sql.SQLException: Variable de sistema desconocida 'innodb_file_format'
      Se ha producido un error al ejecutar: set global innodb_file_format_max=BARRACUDA
      java.sql.SQLException: Variable de sistema desconocida 'innodb_file_format_max'
      Se ha producido un error al ejecutar: set global innodb_file_per_table=TRUE
      java.sql.SQLException: La variable 'innodb_file_per_table' es una variable de sólo lectura
      ```

7. Ejecute el mandato siguiente para desempaquetar la biblioteca cf.

   ```
   cd <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/configuration
   unzip cf.zip
   ```

8. Configure la vía de acceso de clases de los módulos de inicio de sesión de JAAS creando un archivo denominado private_library.xml en la vía de acceso <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver y especifique en el archivo la información siguiente:

```
<server>
 <library id="maprLib">
  <fileset dir="${wlp.install.dir}/usr/servers/aeserver/apps/AE_BOOT.war/WEB-INF/lib" includes="*.jar"/>
  <fileset dir="/usr/share/java" includes="*.jar"/>
  <folder dir="/opt/mapr/hadoop/hadoop-2.7.0/etc/hadoop"/>
  <fileset dir="/opt/mapr/hadoop/hadoop-2.7.0/share/hadoop/common" includes="*.jar"/>
  <fileset dir="/opt/mapr/hadoop/hadoop-2.7.0/share/hadoop/common/lib" includes="*.jar"/>
  <fileset dir="/opt/mapr/hadoop/hadoop-2.7.0/share/hadoop/hdfs" includes="*.jar"/>
  <fileset dir="/opt/mapr/hadoop/hadoop-2.7.0/share/hadoop/hdfs/lib" includes="*.jar"/>
  <fileset dir="/opt/mapr/hadoop/hadoop-2.7.0/share/hadoop/yarn" includes="*.jar"/>
  <fileset dir="/opt/mapr/hadoop/hadoop-2.7.0/share/hadoop/yarn/lib" includes="*.jar"/>
  <fileset dir="/opt/mapr/hadoop/hadoop-2.7.0/share/hadoop/mapreduce" includes="*.jar"/>
  <fileset dir="/opt/mapr/hadoop/hadoop-2.7.0/share/hadoop/mapreduce/lib" includes="*.jar"/>
 </library>
 <jaasLoginModule id="maprLoginModule1" className="org.apache.hadoop.security.login.GenericOSLoginModule"
  controlFlag="REQUIRED" libraryRef="maprLib"></jaasLoginModule>
 <jaasLoginModule id="maprLoginModule2" className="org.apache.hadoop.security.login.HadoopLoginModule"
  controlFlag="REQUIRED" libraryRef="maprLib"></jaasLoginModule>
 <jaasLoginContextEntry id="hadoop_simple" name="hadoop_simple" loginModuleRef="maprLoginModule1,maprLoginModule2" />
 <application context-root="/analyticserver" id="AS_BOOT" location="AE_BOOT.war" name="AS_BOOT" type="war">
   <classloader commonLibraryRef="maprLib"></classloader>
 </application>
 <application id="help" location="help.war" name="help" type="war" context-root="/analyticserver/help"/>
</server>
```

Nota: El ejemplo anterior sirve para configurar el módulo `hadoop_simple login`. La configuración debe cambiarse cuando MapR utilice otros módulos de inicio de sesión.

9. Verifique si el archivo `ASModules.xml` existe en la vía de acceso `<vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/configuration/`. Si el archivo no existe, cambie el nombre del archivo `ASModules.xml.template` (en la misma vía de acceso) por `ASModules.xml`.
10. Configure la información del clúster añadiendo las propiedades siguientes al archivo `<vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/configuration/config.properties`.

    ```
    ae.cluster.zookeeper.connect.string=
    ae.cluster.member.name=
    ae.cluster.collective.name=mapr_5.1
    ```

    La propiedad `ae.cluster.zookeeper.connect.string` es la lista de nodos de Zookeeper separados por comas. La propiedad puede compartir el clúster de Zookeeper que MapR utiliza. `ae.cluster.member.name` es el nombre de host del nodo que aloja Analytic Server.
11. Abra el archivo `<vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/server.env` y añada al archivo las líneas siguientes:

    ```
    JAVA_HOME=<dir_inicial_Java>

    PATH=<vía_instalación_as>/ae_wlpserver/usr/servers/aeserver/configuration/linux/lib_64:<dir_inicial_Java>/jre/lib/amd64:/usr/sbin:
    /usr/bin:/sbin:/bin

    IBM_SPSS_AS_NATIVE_PATH=<vía_instalación_as>/ae_wlpserver/usr/servers/aeserver/configuration/linux/lib_64

    LD_LIBRARY_PATH=<vía_instalación_as>/ae_wlpserver/usr/servers/aeserver/configuration/linux/lib_64:<dir_inicial_Java>/jre/lib/amd64:
    /opt/mapr/hadoop/hadoop-2.7.0/lib/native
    ```

    Sustituya `<vía de acceso a página de inicio>` y `<dir_inicial_Java>` por la vía de acceso de instalación real, y la vía de acceso de inicio de Java.
12. Edite la raíz analítica abriendo el archivo `<vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/configuration/config.properties` y añadiendo la línea siguiente:

    ```
    distrib.fs.root=<raíz_analítica>
    ```

    `<raíz_analítica>` es una vía de acceso del sistema de archivos de MapR que aloja los archivos remotos esenciales de Analytic Server. La vía de acceso recomendada es `/user/<as_user>/raíz_analítica`.
13. Establezca el usuario administrador abriendo el archivo `<vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/configuration/config.properties` y añadiendo la línea siguiente:

    ```
    admin.username=admin
    ```

    El valor debe ser un nombre de usuario administrador de Analytic Server, y debe ser uno de los usuarios que haya configurado en el archivo `security_cfg.xml`.
14. Cargue las dependencias de Analytic Server en el sistema de archivos de MapR añadiendo la línea siguiente en la línea 69 del archivo `<vía_acceso_instalación_as>/bin/hdfsUpdate.sh`:

```
JAVA_CLASS_PATH=`hadoop classpath`:$JAVA_CLASS_PATH
```

Ejecute los mandatos siguientes para crear la <raíz_analítica>:

```
cd <vía_acceso_instalación_as>/bin
./hdfsUpdate.sh
```

<as_user> debe tener permiso de escritura en el directorio padre <raíz_analítica>.

15. Inicie y detenga Analytic Server.
    a. Ejecute el mandato siguiente para iniciar Analytic Server:

    ```
    cd <vía_acceso_instalación_as>/ae_wlpserver/bin
    ./server start aeserver
    ```

    b. Ejecute el mandato siguiente para detener Analytic Server:

    ```
    cd <vía_acceso_instalación_as>/ae_wlpserver/bin
    ./server stop aeserver
    ```

Configuración de MapR

Después de la instalación, si lo desea puede configurar y administrar las características MapR de Analytic Server.

Habilitación del retrotracción de base de datos

El retrotracción de base de datos es la práctica de leer datos de una base de datos y procesar directamente en los datos.

IBM SPSS Analytic Server da soporte al retrotracción para las bases de datos siguientes:

- DashDB
- DB2
- DB2 para Z
- Hive
- MySQL
- Netezza
- Oracle
- PostgreSQL
- Redshift
- SQL Server
- Sybase IQ
- Terradata

Utilice los pasos siguientes para habilitar el retrotracción de base de datos.

1. Copie los archivos JAR de controlador JDBC adecuados en <vía_acceso_instalación_as>/jdbc.
2. Abra el archivo <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/private_library.xml, localice la biblioteca de códigos que tenga el ID maprLib, y añada la línea siguiente en el código:

   ```
   <fileset dir="<vía_acceso_instalación_as>/jdbc" includes="*.jar"/>
   ```

3. Ejecute los mandatos siguientes:

   ```
   cd <vía_acceso_instalación_as>/jdbc
   hadoop fs -put *.jar <raíz_analítica_as>/cluster1/classpath
   ```

4. Reinicie Analytic Server.

Habilitación de Apache Hive

Apache Hive es una infraestructura de almacén de datos que se crea encima de Hadoop para proporcionar resumen, consulta y análisis de datos.

Nota: Hive debe configurarse para que utilice MySQL como un metastore. El archivo `hive-site.xml` que existe en el nodo en que se aloja IBM SPSS Analytic Server debe ser el mismo que el archivo del nodo en el que se ejecuta el metastore de Hive.

Para habilitar el soporte de Apache Hive después de una instalación satisfactoria de MapR:

1. Cargue las dependencias de Hive y hcatalog en el sistema de archivos de MapR, ejecutando los mandatos siguientes:

   ```
   cd /opt/mapr/hive/hive-1.2/lib
   hadoop fs -put *.jar <raíz_analítica_as>/cluster1/classpath
   cd /opt/mapr/hive/hive-1.2/hcatalog/share/hcatalog
   hadoop fs -put *.jar <raíz_analítica_as>/cluster1/classpath
   ```

   `<raíz_analítica_as>` es la vía de acceso raíz analítica que se define en "Instalación de Analytic Server en MapR" en la página 35.

2. Abra el archivo `<vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/private_library.xml`, localice la biblioteca de códigos que tenga el ID `maprLib`, y añada las líneas siguientes en el código:

   ```
   <fileset dir="/opt/mapr/hive/hive-1.2/lib" includes="*.jar"/>
   <fileset dir="/opt/mapr/hive/hive-1.2/hcatalog/share/hcatalog" includes="*.jar"/>
   ```

3. Ejecute los mandatos siguientes para crear los enlaces del archivo de configuración hcatalog y de Hive:

   ```
   mkdir <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/configuration/hive-conf
   ln -s /opt/mapr/hive/hive-1.2/conf/* <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/configuration/hive-conf
   ```

4. Añada la línea siguiente al archivo `private_library.xml` cuando haya archivos jar adicionales en el directorio auxlib de Hive:

   ```
   <fileset dir="/opt/mapr/hive/hive-1.2/auxlib" includes="*.jar"/>
   ```

   Ejecute los mandatos siguientes después de añadir la línea anterior:

   ```
   cd /opt/mapr/hive/hive-1.2/auxlib
   hadoop fs -put *.jar <raíz_analítica_as>/cluster1/classpath
   ```

5. Reinicie Analytic Server.

Ejecución de Hive en modalidad HTTP

De forma predeterminada, Hive se ejecuta en modalidad binaria (modalidad TCP). Para ejecutar Hive en modalidad HTTP, debe actualizar las propiedades de configuración Hive siguientes (en particular la propiedad `hive.server2.transport.mode`).

Nota: Para obtener más información respecto a cada propiedad, consulte Propiedades de configuración de Hive.

Tabla 4. Propiedades de Hive para modalidad HTTP

Nombre de propiedad	Valor predeterminado	Descripción
hive.server2.transport.mode	binary	Modalidad de transporte del servidor. El valor puede ser `binary` o `http`. Establezca en `http` para habilitar la modalidad de transporte HTTP.
hive.server2.thrift.http.port	10001	El número de puerto cuando está en modalidad HTTP.
hive.server2.thrift.http.path	cliservice	Componente de vía de acceso del punto final URL cuando está en modalidad HTTP.
hive.server2.thrift.http.min.worker.threads	5	Número mínimo de hebras, en la agrupación de servidores, cuando se encuentra en modalidad HTTP.
hive.server2.thrift.http.max.worker.threads	500	Número máximo de hebras de trabajo, en la agrupación de servidores, cuando están en modalidad HTTP.

Nota: Hive debe reiniciarse después de que se actualicen las propiedades.

Habilitación de Apache HBase

Apache HBase es una base de datos distribuida no relacional, de código abierto, que está escrita en Java. Se ha desarrollado como parte del proyecto Apache Hadoop de Apache Software Foundation, y se ejecuta sobre HDFS (sistema de archivos de archivos distribuido de Hadoop).

Para habilitar el soporte de Apache HBase después de una instalación satisfactoria de MapR:

1. Cargue las dependencias de HBase en el sistema de archivos de MapR y ejecute los mandatos siguientes:

   ```
   cd /opt/mapr/hbase/hbase-0.98.12/lib
   hadoop fs -put *.jar <raíz_analítica_as>/cluster1/classpath
   ```

   <raíz_analítica_as> es la vía de acceso raíz analítica que se define en "Instalación de Analytic Server en MapR" en la página 35.
2. Abra el archivo <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/private_library.xml, localice la biblioteca de códigos que tenga el ID maprLib, y añada la línea siguiente en el código:

   ```
   <fileset dir="/opt/mapr/hbase/hbase-0.98.12/lib" includes="*.jar"/>
   ```
3. Ejecute los mandatos siguientes para crear los enlaces del archivo de configuración hcatalog y de HBase:

   ```
   mkdir <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/configuration/hbase-conf
   ln -s /opt/mapr/hbase/hbase-0.98.12/conf/* <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/configuration/hbase-conf
   ```
4. Reinicie IBM SPSS Analytic Server.

Habilitación de Apache Spark

Apache Spark es un estándar abierto para el proceso de datos en memoria flexible, para el análisis avanzado, de proceso por lotes, en tiempo real.

Para habilitar el soporte de Apache Spark después de una instalación satisfactoria de MapR:

1. Copie el archivo spark-assembly-1.4.1-hadoop2.5.1-mapr-1501.jar de /opt/mapr/spark/spark-1.4.1/lib a <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/modules/spark/.
2. Cargue las dependencias de Spark en el sistema de archivos de MapR y ejecute los mandatos siguientes:

   ```
   cd <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/modules/spark/
   hadoop fs -put *.jar <raíz_analítica_as>/cluster1/classpath
   ```

   <raíz_analítica_as> es la vía de acceso raíz analítica que se define en "Instalación de Analytic Server en MapR" en la página 35.
3. Abra el archivo <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/private_library.xml, localice la biblioteca de códigos que tenga el ID maprLib, y añada la línea siguiente en el código:

   ```
   <fileset dir="/opt/mapr/spark/spark-1.4.1/lib" includes="spark-assembly-*.jar"/>
   ```
4. Ejecute los mandatos siguientes para crear los enlaces del archivo de configuración de Spark:

   ```
   mkdir <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/configuration/spark-conf
   ln -s /opt/mapr/spark/spark-1.4.1/conf/* <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/configuration/spark-conf
   ```
5. Añada la línea siguiente en el archivo <vía_acceso_instalación_as/ae_wlpserver/usr/servers/aeserver/server.env:

   ```
   SPARK_HOME=/opt/mapr/spark/spark-1.4.1
   ```
6. Añada la línea siguiente en el archivo <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/configuration/config.properties:

   ```
   spark.executor.extraLibraryPath=/opt/mapr/hadoop/hadoop-2.7.0/lib/native
   ```
7. Reinicie IBM SPSS Analytic Server.
8. Para habilitar la característica PySpark, añada la línea siguiente en el archivo yarn-env.sh y, a continuación, reinicie ResourceManagers y NodeManagers:

```
export SPARK_HOME=/opt/mapr/spark/spark-1.4.1
```

Habilitación de distintivos de característica

Los distintivos de características proporcionan la posibilidad de habilitar e inhabilitar características específicas de la aplicación.

Para habilitar el soporte de distintivo de característica después de una instalación satisfactoria de MapR:

1. Añada la línea siguiente en el archivo <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/configuration/config.properties:

   ```
   load.feature.flags.on.msg=true
   ```

2. Reinicie IBM SPSS Analytic Server.

Habilitación de R

R es un lenguado y un entorno para realizar cálculos y crear gráficos estadísticos.

Para habilitar el soporte de R después de una instalación satisfactoria de MapR:

Nota: El paquete siguiente debe estar ya instalado para poder ejecutar el instalador en todos los nodos del clúster en que se alojan NodeManager y IBM SPSS Analytic Server:

```
gcc-gfortran
libgfortran
gcc-c++
```

1. Ejecute el instalador spss_er-8.3.0.0-mapr5.1-lx86_64_en.bin en todos los nodos del clúster en los que se alojan NodeManager y Analytic Server. El usuario que ejecuta el instalador debe tener permiso de escritura en la vías de instalación de R y de Analytic Server.
2. Siga las instrucciones de instalación, aceptando el acuerdo de licencia y especificando la información pertinente. Si se ha instalado Analytic Server en el servidor de instalación, seleccione Sí cuando se le solicite, y especifique <vía_acceso_instalación_as>. Si no se ha instalado Analytic Server en el servidor de instalación, elija No cuando se le solicite.
3. Al instalar Analytic Server, Essentials for R se instala automáticamente en la vía de instalación de Analytic Server.
   - Si no se ha instalado Analytic Server, Essentials for R se instalará en la vía de acceso <via_acceso_instalador>/IBM_SPSS_ModelerEssentialsR/linux.
   - Si Analytic Server se instala más adelante, utilice el mandato siguiente para copiar Essentials for R en la vía de acceso de configuración de Analytic Server donde se haya instalado Analytic Server.

     ```
     cp -r <vía_instalación_as>/IBM_SPSS_ModelerEssentialsR/linux <via_acceso_instalador>/ae_wlpserver/usr/servers/aeserver/configuration
     ```

4. Suprima el archivo cf.zip en la vía de acceso <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/configuration y genere un nuevo archivo, con los mandatos siguientes:

   ```
   cd <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/configuration
   zip -r cf.zip linux
   ```

5. Ejecute los mandatos siguientes:

   ```
   cd <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/configuration
   hadoop fs -rm <raíz_analítica_as>/cluster1/configuration/cf.zip
   hadoop fs -put cf.zip <raíz_analítica_as>/cluster1/configuration/
   ```

6. Reinicie Analytic Server.

Habilitación de LZO

LZO es una biblioteca de compresión de datos sin pérdidas que favorece la velocidad con respecto a la proporción de compresión. MapR debe configurarse manualmente para que proporcione soporte de LZO.

En el sitio siguiente se proporcionan instrucciones de instalación y configuración de LZO: https://github.com/twitter/hadoop-lzo.

En los pasos siguientes se detalla el proceso de importar una biblioteca de LZO en MapR.

1. Copie el archivo hadoop-lzo-<versión>.jar a la vía de acceso de clases de Hadoop. La vía de acceso recomendada es /opt/mapr/hadoop/hadoop-2.7.0/share/hadoop/mapreduce/lib.
2. Copie los archivos libgplcompression.so y liblzo2.so.2 nativos a /opt/mapr/hadoop/hadoop-2.7.0/lib/native, y añada las propiedades siguientes en el archivo core-site.xml:

```
<property>
   <name>io.compression.codecs</name>
   <value>org.apache.hadoop.io.compress.GzipCodec,org.apache.hadoop.io.compress.DefaultCodec,com.hadoop.compression.lzo.
    LzoCodec,com.hadoop.compression.lzo.LzopCodec,org.apache.hadoop.io.compress.BZip2Codec</value>
</property>
<property>
    <name>io.compression.codec.lzo.class</name>
    <value>com.hadoop.compression.lzo.LzoCodec</value>
</property>
```

3. Abra el archivo <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/server.env y añada <vía_acceso_nativa_lzo> al parámetro LD_LIBRARY_PATH. <vía_acceso_nativa_lzo> es la carpeta que contiene la biblioteca nativa de Hadoop-LZO.

```
LD_LIBRARY_PATH=<vía_instalación_as>/ae_wlpserver/usr/servers/aeserver/configuration/linux/lib_64:<dir_inicial_Java>/jre/lib/amd64:
/opt/mapr/hadoop/hadoop-2.7.0/lib/native:<vía_acceso_nativa_lzo>
```

4. Reinicie IBM SPSS Analytic Server.

Configuración de un clúster de IBM SPSS Analytic Server para MapR

Utilice los pasos siguientes para configurar un entorno de clúster de IBM SPSS Analytic Server para el soporte de MapR.

1. Añada la línea siguiente en el archivo <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/configuration/config.properties.

```
enable.resume=true
```

2. Copie la vía de acceso de instalación a los demás nodos del clúster, y cambie la propiedad ae.cluster.member.name del archivo config.properties por el nombre de host correcto.
3. Inicie todos los nodos del clúster.

Desinstalación de MapR

En los pasos siguientes se explica el proceso de desinstalación de MapR:

1. Detenga IBM SPSS Analytic Server.
2. Suprima la base de datos de metadatos.
   a. Ejecute los mandatos siguientes:

```
cd <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/sql/<tipo_BD>
java -Xmx128m -Xms128m -cp <vía_instalación_as>/ae_wlpserver/usr/servers/aeserver/apps/AE_BOOT.war/WEB-INF/lib/*:/usr/share/java/*
com.spss.ae.dbscript.ScriptRunner ../../configuration/config.properties drop.sql true
```

   b. Ejecute la sentencia SQL siguiente para descartar la base de datos:

```
drop database <nombre_BD>
```

3. Desinstale el paquete RPM:

```
rpm -e IBM-SPSS-AnalyticServer-3.0.1.0-1.x86_64
```

4. Suprima la vía de acceso de instalación:

```
rm -r <vía_acceso_instalación_as>
```

5. Suprima la raíz analítica:

```
hadoop fs -rm -r <raíz_analítica>
```

6. Suprima los datos de Zookeeper:

```
/opt/mapr/zookeeper/zookeeper-3.4.5/bin/zkCli.sh -server <host_Zookeeper>:<puerto_Zookeeper>
rmr /AnalyticServer
```

Migración de IBM SPSS Analytic Server en MapR

IBM SPSS Analytic Server puede migrar en MapR.

Utilice los pasos siguientes para migrar IBM SPSS Analytic Server 2.0 o 2.1 a la versión 3.0.1 en MapR.

1. Instale Analytic Server 3.0.1 en un clúster de MapR siguiendo las instrucciones de instalación que figuran en "Instalación de Analytic Server en MapR" en la página 35.
2. Copie la raíz analítica.

   Nota: Este paso se puede pasar por alto si no se modifica la raíz analítica.

   - Ejecute el mandato siguiente en uno de los nodos de datos si la raíz analítica tanto para la versión 2.0/2.1 como para la 3.0.1 de Analytic Server se encuentra en el mismo clúster de MapR:

     ```
     hadoop fs -cp <raíz_analítica_antigua>/analytic-workspace/* <raíz_analítica_nueva>/analytic-workspace
     ```

   - Los servicios de WEBHDFS o NFS instalados dictan cuándo la raíz analítica para Analytic Server, versiones 2.0/2.1 y 3.0.1, están en clústeres de MapR diferentes. WEBHDFS o NFS son necesarios para poder copiar los datos de la raíz analítica porque no se puede acceder al sistema de archivos de MapR directamente fuera del clúster.

     a. Ejecute el mandato siguiente en uno de los nuevos nodos de clúster de Analytic Server 2.1 cuando el clúster de Analytic Server 2.0/2.1 antiguo incluya el servicio WEBHDFS:

        ```
        hadoop distcp webhdfs://<servidor_hdfs_web>:<puerto_hdfs_web>/<raíz_analítica_antigua>/analytic-workspace/*
        maprfs://<raíz_analítica_nueva>/analytic-workspace
        ```

     b. Ejecute el mandato siguiente en uno de los antiguos nodos de clúster de Analytic Server 2.0/2.1 cuando el clúster de Analytic Server 3.0.1 nuevo incluya el servicio WEBHDFS:

        ```
        hadoop distcp maprfs://<raíz_analítica_antigua>/analytic-workspace/*
        webhdfs://<servidor_hdfs_web>:<puerto_hdfs_web>/<raíz_analítica_nueva>/analytic-workspace
        ```

     c. Ejecute el mandato siguiente en uno de los antiguos nodos de clúster de Analytic Server 2.0/2.1 cuando el clúster antiguo incluya NFS, y también se monte NFS en uno de los nodos de clúster de Analytic Server 3.0.1 nuevos:

        ```
        hadoop distcp file:///<vía_montaje>/<raíz_analítica_antigua>/analytic-workspace/* maprfs://<raíz_analítica_nueva>/analytic-workspace
        ```

     d. Ejecute el mandato siguiente en uno de los nuevos nodos de clúster de Analytic Server 3.0.1 cuando el clúster nuevo incluya NFS, y también se monte NFS en uno de los nodos de clúster de Analytic Server 2.0/2.1 antiguos:

        ```
        hadoop discp maprfs://<raíz_analítica_antigua>/analytic-workspace/* file:///<vía_montaje>/<raíz_analítica_nueva>/analytic-workspace
        ```

   Revise el sitio Data Migration de MapR para obtener información sobre la migración de datos entre clústeres de MapR diferentes.
3. Ejecute los mandatos siguientes para cambiar el propietario y los permisos de la raíz analítica nueva:

   ```
   hadoop fs -chown -R <as_user> <raíz_analítica>
   hadoop fs -chmod -R 755 <>
   ```

4. Detenga Analytic Server 3.0.1, pero asegúrese de que la base de datos de metadatos siga ejecutándose.
5. Recopile los valores de configuración de la instalación antigua de clúster de Analytic Server 2.0/2.1.
   a. Copie el archivo `configcollector.zip` de la nueva instalación del clúster de Analytic Server 3.0.1 a `<vía_acceso_instalación_as_antigua>/tools` en la antigua instalación del clúster de Analytic Server 2.0/2.1.
   b. Extraiga el contenido de `configcollector.zip` en la antigua instalación del clúster de Analytic Server 2.0/2.1. Se crea un nuevo subdirectorio `configcollector` la antigua instalación del clúster de Analytic Server 2.0/2.1.
   c. Ejecute la herramienta de recopilador de configuración en la antigua instalación del clúster de Analytic Server 2.0/2.1, ejecutando el script `configcollector` en `<vía_acceso_instalación_as_antigua>/tools/configcollector`. Copie el archivo comprimido resultante (ZIP) en la nueva instalación del clúster de Analytic Server 3.0.1.
6. Ejecute la herramienta de migración en el nuevo clúster de Analytic Server 3.0.1 ejecutando el script `migrationtool` y pasando la vía de acceso del archivo comprimido, que creó el recopilador de configuración, como argumento. Por ejemplo:

   ```
   migrationtool.sh /opt/ibm/spss/analyticserver/3.0/ASConfiguration_2.1.0.0.xxx.zip
   ```

7. Inicie Analytic Server 3.0.1.

Resolución de problemas de MapR

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

Problemas con el script hdfsUpdate.sh

El script `hdfsUpdate.sh` debe ejecutarse sólo una vez, porque elimina todos los archivos de la raíz analítica antes de cargar nuevos archivos. Cuando ejecute el script más de una vez, deberá volver a cargar las dependencias del retrotracción de base de datos, Hive, HBase y Spark. Ejecute los mandatos siguientes para volver a cargar las dependencias necesarias:

```
cd <vía_acceso_instalación_as>/jdbc

hadoop fs -put *.jar <raíz_analítica_as>/cluster1/classpath

cd /opt/mapr/hive/hive-1.2/lib
hadoop fs -put *.jar <raíz_analítica_as>/cluster1/classpath
cd /opt/mapr/hive/hive-1.2/hcatalog/share/hcatalog
hadoop fs -put *.jar <raíz_analítica_as>/cluster1/classpath

cd /opt/mapr/hbase/hbase-0.98.12/lib
hadoop fs -put *.jar <raíz_analítica_as>/cluster1/classpath

cd <vía_acceso_instalación_as>/ae_wlpserver/usr/servers/aeserver/modules/spark/

hadoop fs -put *.jar <raíz_analítica_as>/cluster1/classpath
```

Capítulo 5. 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 del servidor que aloja 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 6. 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/iop/4.1.0.0/knox/data/deployments`.

Problemas con distribuciones Hadoop específicas

La acción Renovar para el servicio Analytic Server está inhabilitada en Hortonworks 2.4

Para renovar manualmente las bibliotecas de Analytic Server en Hortonworks 2.4 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/3.0.1/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.

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 relacionados con las corrientes de IBM SPSS Modeler que se ejecutan en un proceso de Spark

Las corrientes de SPSS Modeler no logran completarse cuando están obligadas a ejecutarse en un proceso Spark. Las corrientes 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 corriente, la interfaz de usuario del gestor de recursos indica que se ejecuta la nueva aplicación, pero la corriente nunca se completa y permanece en un estado `Running`. No hay ningún mensaje que indica por qué la corriente no se logra completar en los registros de Analytic Server, YARN logs, or Spark logs.

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 4GB permite que las corrientas de SPSS Modeler anteriormente fallidas se completen en menos de 2 minutos (en un entorno de un único clúster de nodo).

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 15.

java.net.SocketTimeoutException: se ha agotado el tiempo de espera de lectura

Cambie la variable de entorno de tiempo de espera de Liberty ND como se indica a continuación:

```
export LIBERTYND_READ_TIMEOUT=<milisegundos>
```

Donde <milisegundos> es el número de segundos para utilizar el tiempo de espera de lectura de JMX.

java.io.IOException: CWWKX7202E: El valor de tiempo de espera de 60 (segundos) para el mandato ./server start ha caducado

Añada lo siguiente al archivo server.xml de Controller Server

```
<!-- Aumente el tiempo de espera de inicio y parada de servidor para adaptar el hardware lento -->
<serverCommands startServerTimeout="120" stopServerTimeout="120"/>
```

java.lang.OutOfMemoryError: espacio de almacenamiento dinámico de Java

Añada las líneas siguientes a `jvm.options` en cada miembro del clúster de alta disponibilidad.

```
-Xms512M
-Xmx2048M
```

"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: cadena 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 dos situaciones comunes en las que los trabajos de Analytic Server no se reanudan.

1. 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 no se reanuda el trabajo, compruebe para asegurarse de que hay por lo menos 4 miembros de clúster en el clúster de alta disponibilidad.
2. Cuando desactiva temporalmente un miembro de clúster, todos los trabajos de Analytic Server en ese servidor se reanudan normalmente en otro miembro de clúster. Para asegurarse de que se reanudan los trabajos, establezca `-Dcom.spss.ae.remoteclient.failover.threshold=100` y utilice la modalidad remota.

El servidor Analytic Server se cuelga de vez en cuando se apaga el servidor.

Interrumpa el servidor manualmente.

Avisos

Esta información se ha desarrollado para productos y servicios que se comercializan en los EE.UU. Este material puede estar disponible en otros idiomas en IBM. 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 FACILITA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍAS DE NINGÚN TIPO, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO INFRACCIÓN, COMERCIALIZACIÓN O ADECUACIÓN A UN FIN CONCRETO. Algunas jurisdicciones no permiten la renuncia a las garantías explícitas o implícitas en ciertas transacciones, por tanto, es posible que esta declaración no resulte aplicable a 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 en esta información a sitios web que no son de IBM se proporcionan solo por comodidad y de ningún modo suponen un aval de dichos sitios web. Los materiales de estos sitios web no forma parte del material correspondiente a este producto IBM y el uso de estos sitios web es a cuenta y riesgo del usuario.

IBM puede utilizar o distribuir la información que se le proporcione del modo que estime apropiado 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 este) y (ii)el uso mutuo de información que se haya 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 reales de rendimiento pueden variar en función de configuraciones y condiciones de funcionamiento específicas.

La información respecto a productos que no son de IBM se obtuvo de los proveedores de estos productos, sus anuncios publicados u otras fuentes disponibles de forma pública. IBM no ha probado esos productos y no puede confirmar la exactitud del rendimiento, la compatibilidad ni ninguna otra afirmación relacionada con productos no IBM. Las consultas sobre las prestaciones de productos que no sean de IBM se deben dirigir a los proveedores de esos productos.

Las declaraciones sobre el futuro rumbo o intención de IBM están sujetas a cambio o retirada sin previo aviso y representan únicamente metas y objetivos.

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 los nombres de personas o empresas 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 los nombres de personas o empresas 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:

© el nombre de su empresa) (año). Partes de este código se derivan de IBM Corp. Sample Programs.

© Copyright IBM Corp. _especifique el año o años_. Reservados todos los derechos.

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