IBM SPSS Analytic Server
버전 3.2.1

설치 및 구성 안내서

참고

이 정보와 이 정보가 지원하는 제품을 사용하기 전에, 87 페이지의 『주의사항』에 있는 정보를 확인하십시오.

제품 정보

이 개정판은 새 개정판에 별도로 명시하지 않는 한, IBM SPSS Analytic Server의 버전 3, 릴리스 2, 수정사항 1 및 모든 후속 릴리스와 수정에 적용됩니다.

목차

제 1 장 필수조건

Analytic Server를 설치하기 전에 다음 정보를 검토하십시오.

시스템 요구사항

최신 시스템 요구사항 정보는 IBM 기술 지원 사이트(http://publib.boulder.ibm.com/infocenter/prodguid/v1r0/clarity/softwareReqsForProduct.html)에서 제공하는 자세한 시스템 요구사항 보고서를 참조하십시오. 이 페이지에서 다음을 수행하십시오.

1. SPSS Analytic Server를 제품 이름으로 입력하고 **검색**을 클릭하십시오.
2. 원하는 버전과 보고서의 범위를 선택한 다음 **제출**을 클릭하십시오.

WebSocket 트래픽

클라이언트와 Analytic Server 간의 WebSocket 트래픽이 방화벽, VPN 또는 기타 포트 차단 방법으로 차단되지 않는지 확인해야 합니다. WebSocket 포트는 일반 Analytic Server 포트와 동일합니다.

SuSE Linux(SLES) 12

SuSE Linux 12에서 Analytic Server를 설치하기 전에 다음 태스크를 수행하십시오.

1. 다음 URL에서 공개 키를 호스트에 다운로드하십시오.

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

2. 호스트에서 다음 명령을 실행하여 공개 키를 가져오십시오.

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

Power 시스템

IBM XLC 및 XLF 컴파일러가 클러스터의 모든 호스트에서 설치되어 PATH에 포함됩니다.

이러한 컴파일러의 라이센스 가져오기에 대한 자세한 정보는 다음 웹 사이트에서 찾을 수 있습니다.

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

Hortonworks Data Platform(HDP)

Analytic Server을 설치하기 전에 하나 이상의 HDP 클라이언트가 클러스터 환경에 배포되었는지 확인해야 합니다. Ambari Manager를 호스트하는 노드에 `/usr/hdp` 디렉토리가 필요하기 때문에 Analytic Server 엔진은 HDP 클라이언트가 없는 경우 실패합니다.

Hive/HCatalog

NoSQL 데이터 소스를 사용할 계획이라면 Hive 및 HCatalog를 원격 액세스용으로 구성하십시오. 또한 `hive-site.xml`에 활성 Thrift Hive Metastore 서버를 가리키는 `thrift://<host_name>:<port>` 양식으로 *hive.metastore.uris* 특성이 포함되어 있는지 확인하십시오. 세부사항은 Hadoop 배포 문서를 참조하십시오.

참고: Analytic Server Metastore는 Hive Metastore와 동일한 시스템에 설치할 수 없습니다.

Hive 2.1을 사용하려면 Ambari 콘솔에서 **대화형 쿼리** 설정을 사용으로 설정하여 Hive 2.1을 사용하도록 설정한 다음, Analytic Server 설치 중에 `2.x`를 `hive.version` 특성으로 입력해야 합니다.

1. Ambari 콘솔을 열고 다음 특성을 **Analytic Server 고급 analytics.cfg** 섹션에 추가하십시오.
   - 키: `hive.version`
   - 값: 적절한 Hive 버전(예: 2.x)을 입력하십시오.
2. 구성을 저장하십시오.

참고: Hive 2.1은 Spark 2.x가 설치된 HDP 2.5 및 2.6에서 지원됩니다.

메타데이터 리포지토리

기본적으로 Analytic Server는 MySQL 데이터베이스를 설치하고 사용합니다. 또는 Analytic Server에서 기존 Db2 설치를 사용하도록 구성할 수 있습니다. 선택하는 데이터베이스의 유형에 상관없이 인코딩이 UTF-8이어야 합니다.

MySQL

MySQL의 기본 문자 세트가 버전 및 운영 체제에 따라 다릅니다. 다음 단계를 사용하여 MySQL의 설치가 UTF-8로 설정되었는지 여부를 판별하십시오.

1. MySQL의 버전을 판별하십시오.

   ```
   mysql -V
   ```

2. MySQL 명령행 인터페이스에서 다음 쿼리를 실행하여 MySQL의 기본 문자 세트를 판별하십시오.

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

   문자 세트가 이미 UTF-8로 설정된 경우 추가로 변경할 필요가 없습니다.

3. MySQL 명령행 인터페이스에서 다음 쿼리를 실행하여 MySQL의 기본 데이터 정렬을 판별하십시오.

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

   데이터 정렬이 이미 UTF-8로 설정된 경우 추가로 변경할 필요가 없습니다.

4. 기본 문자 세트 또는 데이터 정렬이 UTF-8로 설정되지 않은 경우 MySQL 문서에서 /etc/my.cnf 편집 방법에 대한 세부사항을 참조하고 MySQL 디먼을 다시 시작하여 문자 세트를 UTF-8로 변경하십시오.

Db2 Db2 구성에 대한 자세한 정보는 Knowledge Center http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.kc.doc/welcome.html의 내용을 참조하십시오.

고가용성 클러스터

로드 밸런서

고가용성 클러스터에는 세션 선호도(스티키(sticky) 세션이라고도 함)를 지원하는 로드 밸런서가 있어야 합니다. Analytic Server는 쿠키 "request-token"이 있는 세션을 식별합니다. 이를 통해 애플리케이션 제어 세션 선호도에 사용할 사용자 로그인 기간에 대한 세션을 식별합니다. 자세한 세션 선호도 지원 방법을 보려면 특정 로드 밸런서의 문서를 확인하십시오.

Analytic Server 작업 실패

클러스터 멤버가 실패하여 Analytic Server 작업이 실패하는 경우에는 일반적으로 다른 클러스터 멤버에서 작업이 자동으로 다시 시작됩니다. 작업이 다시 실행되지 않으면 고가용성 클러스터에 네 개 이상의 클러스터 멤버가 있는지 확인하십시오.

제 2 장 Ambari 설치 및 구성

Ambari 관련 필수조건

일반 필수조건 이외에도 다음 정보를 검토하십시오.

서비스

Analytic Server는 Ambari 서비스로 설치됩니다. Analytic Server를 설치하기 전에 다음 클라이언트가 Ambari 서비스로 설치되었는지 확인해야 합니다.

- HDFS/HDFS_CLIENT
- MAPREDUCE2/MAPREDUCE2_CLIENT
- HIVE/HIVE_CLIENT
- SPARK/SPARK_CLIENT(Spark 1.x가 사용되는 경우)
- SPARK2/SPARK2_CLIENT(Spark 2.x가 사용되는 경우)
- HBASE/HBASE_CLIENT(HBASE가 사용되는 경우)
- YARN
- Zookeeper

비밀번호 없는 SSH

Analytic Metastore 호스트 및 클러스터의 모든 호스트 간에 루트 사용자의 비밀번호 없는 SSH를 설정하십시오.

설치 사전 검사 및 사후 검사 도구 - Ambari

사전 검사 도구 개요

Analytic Server 설치 사전 검사 도구는 Analytic Server 설치 전에 잠재적인 환경 문제를 식별함으로써 설치 문제 및 런타임 오류를 감소시키는 데 도움을 줍니다.

사전 검사 도구는 다음을 확인합니다.

- 로컬 시스템의 OS 및 Ambari 버전
- 로컬 시스템의 OS ulimit 설정
- 로컬 시스템에서 사용 가능한 디스크 공간
- Hadoop 버전
- Ambari 서비스 가용성(HDFS, HCatalog, Spark, Hive, MapReduce, Yarn, Zookeeper 등)
- Analytic Server에 한정된 Ambari 설정

참고: 사전 검사 도구는 자체 추출 Analytic Server 2진 파일을 실행한 후 사용될 수 있습니다.

사후 검사 도구 개요

Analytic Server 설치 사후 검사 도구는 Analytic Server 설치 후에 처리에 필요한 REST API 요청을 제출하여 구성 문제를 식별합니다.

- HDFS의 데이터
- Hive/HCatalog의 데이터
- 압축 데이터(deflate, bz2, snappy 포함)
- PySpark를 사용하는 데이터
- 네이티브 SPSS 구성요소를 사용하는 데이터(alm, 트리, 신경망, 스코어링, tascoring 포함)
- MapReduce를 사용하는 데이터
- 인메모리 MapReduce를 사용하는 데이터

도구 위치 및 필수조건

Analytic Server 서비스를 설치하기 전에 Analytic Server 서비스의 일부가 될 모든 노드에서 사전 검사 도구를 실행하여 Linux 환경이 Analytic Server를 설치할 준비가 되었는지 확인하십시오.

사전 검사 도구가 설치의 일부로 자동 호출됩니다. 도구는 각 호스트에서 설치를 실행하기 전에 Analytic Metastore 및 각 Analytic Server 노드를 검사합니다. 또한 Ambari 서버 노드에서 사전 검사 도구를 수동으로 호출할 수 있으며, 이 도구로 서비스가 설치되기 전에 시스템을 유효성 검증합니다.

자체 추출 Analytic Server 2진 파일을 실행한 후 사전 검사 도구는 다음 디렉토리에 위치합니다.

- **HDP**

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

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

Analytic Server 설치 후에는 사후 검사 도구가 다음 디렉토리에 위치합니다.

- **HDP**

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

이러한 도구는 루트로 실행되어야 하며 Python 2.6.X 이상이 필요합니다.

사전 검사 도구가 실패를 보고하는 경우, Analytic Server 설치를 계속 수행하기 전에 해당 실패를 처리해야 합니다.

`chktool` 디렉토리는 Analytic Server 자체 추출 2진이 실행된 후에 사용 가능합니다(8 페이지의 『Ambari에 설치』 절의 2단계). 12 페이지의 『오프라인 설치』를 실행하기로 선택하면 메타데이터 RPM이 설치된 후에 `chktool` 디렉토리가 사용 가능합니다.

사전 검사 도구 실행

자동

Analytic Server가 Ambari 콘솔을 통해 서비스로 설치되면 Analytic Server 설치의 일부로 사전 검사 도구를 자동 호출할 수 있습니다. Ambari 서버 사용자 이름 및 비밀번호를 수동으로 입력해야 합니다.

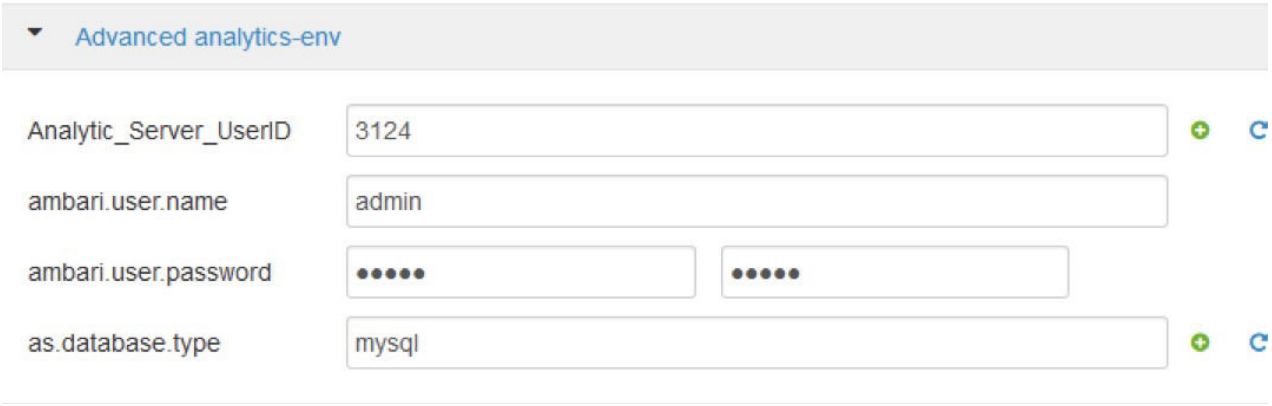

그림 *1.* 고급 *analytics-env* 설정

수동

Ambari 서버 노드에서 사전 검사 도구를 수동으로 호출할 수 있습니다.

다음 사전 검사 예는 SSL을 사용하는 myambarihost.ibm.com:8080에서 실행 중인 Ambari 클러스터 MyCluster를 검사하고 로그인 신임 정보 admin:admin을 사용합니다.

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

참고:

- as_host 값은 IP 주소 또는 완전한 도메인 이름을 사용하여 제공되어야 합니다.
- 비밀번호 인수가 생략되면 비밀번호에 대한 도구가 프롬프트됩니다.
- precheck.py 명령에는 --h 인수를 사용하여 표시되는 사용법 도움말(python ./precheck.py --help)이 포함됩니다.
- --cluster 인수는 선택적입니다. (현재 클러스터는 --cluster가 사용되지 않을 때 식별됩니다.)

사전 검사 도구가 검사를 실행할 때 각 검사의 상태가 명령 창에 표시됩니다. 실패가 발생하면 로그 파일에서 세부사항을 볼 수 있습니다. 정확한 로그 파일 위치는 명령 창에 표시됩니다. 로그 파일은 추가 지원이 필요할 때 IBM 기술 지원에 제공될 수 있습니다.

사후 검사 도구 실행

사후 검사 도구는 Analytic Server가 적절히 실행 중인지, 단순 작업을 처리할 수 있는지 확인합니다. 다음 사후 검사 예는 SSL을 사용하는 myanalyticserverhost.ibm.com:9443에서 실행 중인 Analytic Server를 검사하고 로그인 신임 정보 admin:ibmspss를 사용합니다.

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

Knox가 Analytic Server와 함께 사용되는 경우, 명령은 다음과 같습니다.

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

단일 검사를 수행하려면 다음 명령을 사용하십시오.

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

참고:

- 비밀번호 인수가 생략되면 비밀번호에 대한 도구가 프롬프트됩니다.
- postcheck.py 명령에는 --h 인수를 사용하여 표시되는 사용법 도움말(python ./postcheck.py --help)이 포함됩니다.

사후 검사 도구가 검사를 실행할 때 각 검사의 상태가 명령 창에 표시됩니다. 실패가 발생하면 로그 파일에서 세부사항을 볼 수 있습니다. 정확한 로그 파일 위치는 명령 창에 표시됩니다. 로그 파일은 추가 지원이 필요할 때 IBM 기술 지원에 제공될 수 있습니다.

Ambari에 설치

기본 프로세스는 Ambari 클러스터 내의 호스트에 Analytic Server 파일을 설치한 다음 Analytic Server를 Ambari 서비스로 추가하는 것입니다.

『온라인 설치』

Ambari 서버 호스트 및 클러스터의 모든 노드가 https://ibm-open-platform.ibm.com에 액세스할 수 있는 경우 온라인 설치를 선택하십시오.

12 페이지의 『오프라인 설치』

Ambari 서버 호스트에게 인터넷 액세스 권한이 없는 경우 오프라인을 선택하십시오.

온라인 설치

Ambari 서버 호스트 및 클러스터의 모든 노드가 https://ibm-open-platform.ibm.com에 액세스할 수 있는 경우 온라인 설치를 선택하십시오.

1. IBM Passport Advantage® 웹 사이트로 이동한 다음 사용 중인 스택, 스택 버전 및 하드웨어 아키텍처에 해당하는 자체 추출 2진 파일을 Ambari 관리자 노드로 다운로드하십시오. 사용 가능한 Ambari 2진은 다음과 같습니다.

표 *1. Analytic Server* 자체 추출 *2*진 파일

설명	2진 파일 이름
IBM® SPSS® Analytic Server 3.2.1 for Hortonworks Data Platform 2.5, 2.6, 3.0 및 3.1 Linux x86-64 영어	`spss_as-3.2.1.0-hdp2.5-3.1-lx86.bin`
IBM SPSS Analytic Server 3.2.1 for Hortonworks Data Platform 2.6, 3.0 및 3.1 Linux on System p LE 영어	`spss_as-3.2.1.0-hdp2.6-3.1-lppc64.bin`

2. 자체 추출 2진 파일을 실행하고, 다음 지시사항에 따라 라이센스를 확인하고 라이센스에 동의한 다음, 온라인 또는 오프라인 설치를 선택하고 Analytic Server가 사용하는 데이터베이스 유형에 맞게 설치 프로세스를 선택하십시오. 다음 데이터베이스 유형 옵션이 제공됩니다.
   - 새 MySQL 인스턴스
   - 기존 MySQL 또는 DB2 인스턴스
3. `/var/lib/ambari-server/resources/stacks/<stack-name>/<stack-version>/services/ANALYTICSERVER/package/scripts` 디렉토리에서, `update_clientdeps.sh` 스크립트를 적합한 인수와 함께 실행하십시오(예를 들어 `--help` 인수 사용).
4. Ambari 서버를 다시 시작하십시오.

   ```
   ambari-server restart
   ```
5. Ambari 서버에 로그온하고 Ambari UI를 통해 Analytic Server를 서비스로 설치하십시오.

메타데이터 리포지토리

Analytic Server는 기본적으로 MySQL을 사용하여 데이터 소스, 프로젝트, 테넌트에 대한 정보를 추적합니다. 설치 중 Analytic Server와 MySQL 간 JDBC 연결에 사용된 사용자 이름(**metadata.repository.user.name**)과 비밀번호(**metadata.repository.password**)를 제공해야 합니다. 그러면 설치 프로그램이 MySQL 데이터베이스에 사용자를 작성하지만, 해당 사용자는 MySQL 데이터베이스에만 사용되므로 기존 Linux 또는 Hadoop 사용자일 필요가 없습니다.

메타데이터 리포지토리를 Db2로 변경하려면 다음 단계를 수행하십시오.

참고: 설치가 완료된 후에는 메타데이터 리포지토리를 변경할 수 없습니다.

a. Db2가 다른 시스템에 설치되어 있는지 확인하십시오. 자세한 정보는 1 페이지의 제 1 장 『필수조건』 주제의 메타데이터 리포지토리 절을 참조하십시오.

b. Ambari 서비스 탭에서 Analytic Server 서비스의 구성 탭으로 이동하십시오.

c. **고급 analytics-env** 섹션을 여십시오.

d. **as.database.type**의 값을 `mysql`에서 `db2`로 변경하십시오.

e. **고급 analytics-meta** 섹션을 여십시오.

f. **metadata.repository.driver** 값을 `com.mysql.jdbc.Driver`에서 `com.ibm.db2.jcc.DB2Driver`로 변경하십시오.

g. **metadata.repository.url** 값을 `jdbc:db2://{Db2_HOST}:{PORT}/{DBName}:currentSchema={SchemaName};`으로 변경하십시오. 여기서,

- {Db2_HOST}는 Db2가 설치된 서버의 호스트 이름입니다.
- {PORT}는 Db2가 청취하는 포트입니다.
- {SchemaName}은 사용 가능하지만 사용되지 않는 스키마입니다.

입력할 값을 모르는 경우 Db2 관리자와 함께 작업하십시오.

h. **metadata.repository.user.name** 및 **metadata.repository.password**에 유효한 Db2 신임 정보를 제공하십시오.

i. **저장**을 클릭하십시오.

LDAP 구성

Analytic Server는 LDAP 서버를 사용하여 사용자 및 그룹을 저장하고 인증합니다. Analytic Server 설치 중에 필수 LDAP 구성 정보를 제공하십시오.

표 *2. LDAP* 구성 설정

LDAP 설정	설명
as.ldap.type	LDAP 유형. 값은 ads, ad 또는 openladp일 수 있습니다. • ads - Apache Directory Server(기본 설정) • ad - Microsoft Active Directory • openladp - OpenLDAP
as.ldap.host	LDAP 호스트
as.ldap.port	LDAP 포트 번호
as.ldap.binddn	LDAP 바인드 DN
as.ldap.bindpassword	LDAP 바인드 DN 비밀번호
as.ldap.basedn	LDAP 기본 DN
as.ldap.filter	LDAP 사용자 및 그룹 필터 규칙
as.ldap.ssl.enabled	Analytic Server와 LDAP 간에 통신하는 데 SSL을 사용하는지 여부를 지정합니다. 값은 true 또는 false일 수 있습니다.
as.ldap.ssl.reference	LDAP SSL 참조 ID
as.ldap.ssl.content	LDAP SSL 구성

- 기본적으로 as.ldap.type은 ads로 설정되고 기타 관련 설정에는 기본 설정이 포함됩니다. 예외는 as.ldap.bindpassword 설정에 비밀번호를 제공해야 한다는 것입니다. Analytic Server는 구성 설정을 사용하여 ADS(Apache Directory Server)를 설치하고 서버 초기화를 실행합니다. 기본 ADS 프로파일에는 admin의 사용자와 admin의 비밀번호가 포함됩니다. Analytic Server 콘솔을 통해 관리를 수행하거나 <Analytic Root>/bin 폴더에 있는 importUser.sh 스크립트를 통해 XML 파일에서 사용자 및 그룹 정보를 가져올 수 있습니다.
- 외부 LDAP 서버(예: Microsoft Active Directory 또는 OpenLDAP)를 사용할 계획인 경우 실제 LDAP 값에 따라 구성 설정을 정의해야 합니다. 자세한 정보는 Liberty에서 LDAP 사용자 레지스트리 구성을 참조하십시오.

- Analytic Server가 설치된 후 LDAP 구성을 변경할 수 있습니다(예: Apache Directory Server에서 OpenLDAP로 변경). 그러나 처음에 Microsoft Active Directory 또는 OpenLDAP로 시작하고 나중에 Apache Directory Server로 전환하는 경우 Analytic Server는 설치 중에 Apache Directory Server를 설치하지 않습니다. 초기 Analytic Server 설치 중에 Apache Directory Server가 선택된 경우 Apache Directory Server만 설치됩니다.

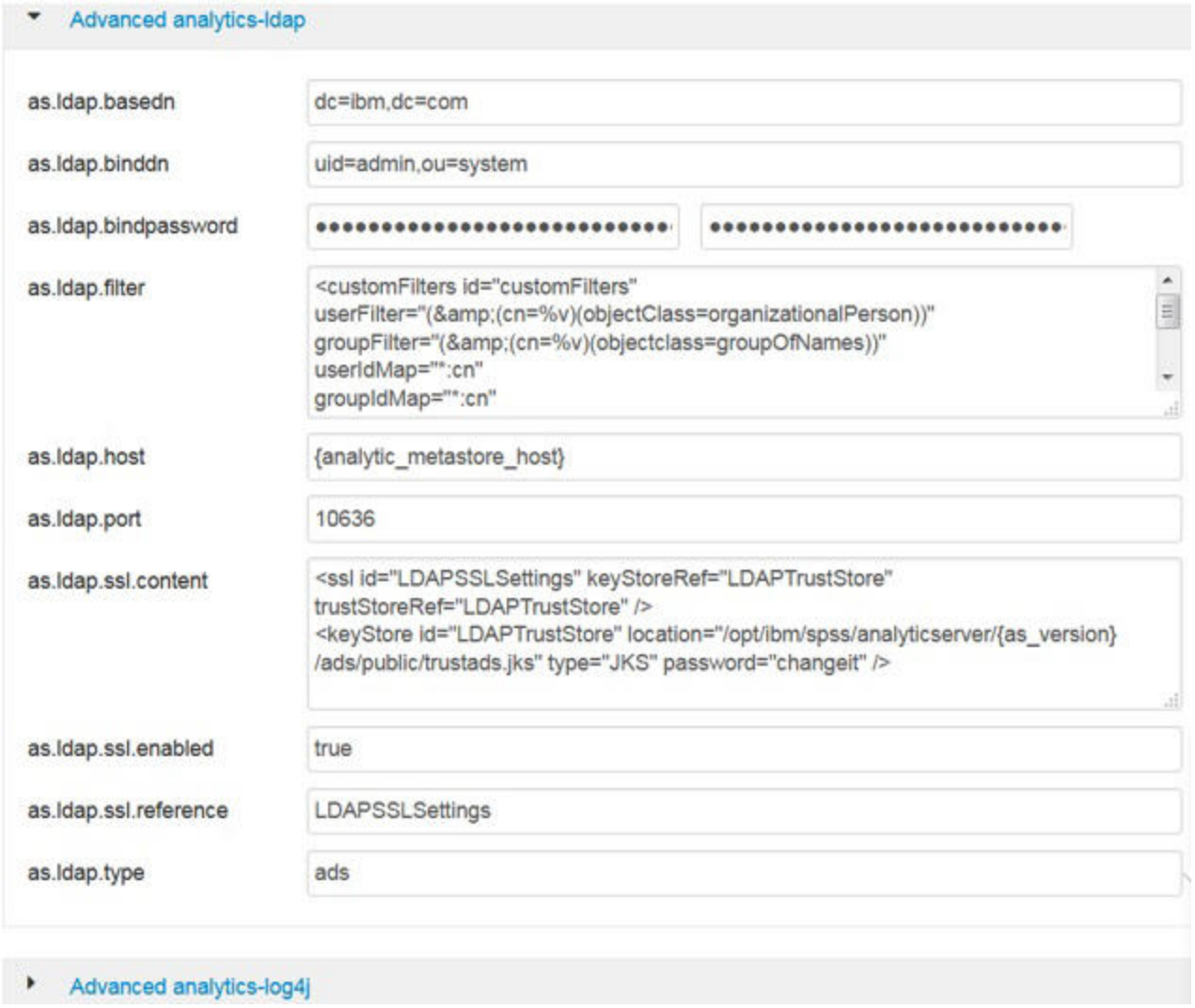

그림 2. *LDAP* 구성 설정의 예

설치 후 변경되지 않아야 하는 구성 설정

설치 후 다음 설정을 변경하지 마십시오. 그렇지 않으면 Analytic Server가 작업에 실패합니다.

- Analytic_Server_User
- Analytic_Server_UserID

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

6. 이제 Analytic Server의 인스턴스가 작동합니다. 추가 구성은 선택사항입니다. Analytic Server 구성 및 관리에 대한 자세한 정보는 19 페이지의 『구성』 주제를 참조하십시오. 기존 구성을 새 설치로 마이그레이션하는 방법에 대한 자세한 정보는 41 페이지의 『Ambari에서 IBM SPSS Analytic Server 마이그레이션』 주제를 참조하십시오.
7. 웹 브라우저를 열고 주소 `http://<host>:<port>/analyticserver/admin/ibm`을 입력하십시오. 여기서 <host>는 Analytic Server 호스트의 주소이고 <port>는 Analytic Server가 청취하는 포트입니다. 기본적으로 9080입니다. 이 URL은 Analytic Server 콘솔의 로그인 대화 상자를 엽니다. Analytic Server 관리자로 로그인하십시오. 기본적으로 이 사용자 ID는 admin이고 비밀번호도 admin입니다.

오프라인 설치

IBM SPSS Analytic Server 오프라인 설치는 자동으로 또는 수동으로 수행될 수 있습니다.

『HDP에서 자동 설치』

자동 설치 프로세스는 Ambari REST API를 활용하며, 설치에 선호되는

방법입니다.

14 페이지의 『HDP(RHEL, SLES)에서 수동 설치』

Hortonworks Data Platform에서 Analytic Server를 수동으로 설치하는 경우

17 페이지의 『HDP(Ubuntu)에서 수동 설치』

Ubuntu Linux에서 Analytic Server를 수동으로 설치하는 경우

HDP에서 자동 설치

자동 설치 프로세스는 Ambari REST API를 활용하며, 설치에 선호되는 방법입니다.

중요사항:

- 오프라인 자동 설치 프로시저는 임베드된 ADS(Apache Directory Server)를 설치합니다. 써드파티 LDAP 서버를 사용하려는 경우 IBM SPSS Analytic Server 설치가 완료된 후 LDAP 설정을 구성할 수 있습니다.
- 오프라인 자동 설치 프로시저는 단일 Analytic Server 서비스 인스턴스만 설치할 수 있습니다. 초기 설치가 완료된 후 더 많은 인스턴스를 추가할 수 있습니다.
- 오프라인 자동 설치 프로시저는 Kerberos 사용 클러스터에서의 Analytic Server 설치를 지원하지 않습니다.

이 제한사항은 수동 HDP 또는 Ubuntu 설치에 적용되지 않습니다.

1. IBM Passport Advantage® 웹 사이트로 이동한 다음 자체 추출 2진 파일을 https://ibm-open-platform.ibm.com에 액세스할 수 있는 컴퓨터로 다운로드하십시오.

표 *3. Analytic Server* 자체 추출 *2*진 파일

설명	2진 파일 이름
IBM SPSS Analytic Server 3.2.1 for Hortonworks Data Platform 2.5, 2.6, 3.0 및 3.1 Linux x86-64 영어	spss_as-3.2.1.0-hdp2.5-3.1-lx86.bin
IBM SPSS Analytic Server 3.2.1 for Hortonworks Data Platform 2.6, 3.0 및 3.1 Linux on System p LE 영어	spss_as-3.2.1.0-hdp2.6-3.1-lppc64.bin

2. 1단계에서 다운로드한 실행 가능한 2진 파일을 실행하고 오프라인 설치를 지정하십시오. 오프라인 설치는 나중에 설치 프로세스에 필요한 RPM 또는 DEB 파일을 다운로드하며 https://ibm-open-platform.ibm.com에 액세스할 수 있는 컴퓨터에서 실행되어야 합니다. 다운로드한 파일은 현재 실행 가능한 2진 디렉토리 ./IBM-SPSS-AnalyticServer에 있습니다.
3. 실행 가능한 2진 디렉토리 ./IBM-SPSS-AnalyticServer의 전체 컨텐츠를 인터넷 액세스가 가능한 시스템에서 Ambari 관리자 노드(방화벽 뒤에 있음)로 복사하십시오.
4. Ambari 관리자 노드에서 다음 명령을 사용하여 Ambari 서버가 실행 중인지 확인하십시오.

   ```
   ambari-server status
   ```

5. Ambari 관리자 노드 및 Analytic Server를 배치할 기타 모든 노드에서 로컬 yum 리포지토리를 작성하는 도구를 설치하십시오.

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

   또는

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

6. Ambari 관리자 노드에서 실행 가능한 2진 파일 ./IBM-SPSS-AnalyticServer/packages/spss_as-ambari-offlineinstall.bin을 실행하십시오. 설치 중에 실행 가능한 2진이 필요한 Analytic Server RPM/DEB 파일이 패키지 디렉토리에 있는지 확인합니다. 필요한 RPM 파일은 배포판, 버전 및 아키텍처에 따라 다릅니다.

   HDP 2.5, 2.6, 3.0 및 3.1(x86_64)

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

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

   HDP 2.6, 3.0 및 3.1(PPC64LE)

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

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

   HDP 2.5, 2.6, 3.0 및 3.1(Ubuntu)

   IBM-SPSS-AnalyticServer-ambari-2.x_3.2.1.0_amd64.deb

   IBM-SPSS-AnalyticServer_1_amd64.deb

설치 중에 Analytic Server 버전, JDBC 드라이버, Spark 버전, Hive 버전 등을 입력하라는 메시지가 표시됩니다.

HDP(RHEL, SLES)에서 수동 설치

HDP(RHEL, SLES)에서 수동 오프라인 설치에 대한 일반적인 워크플로우는 다음과 같습니다.

1. IBM Passport Advantage® 웹 사이트로 이동한 다음 자체 추출 2진 파일을 https://ibm-open-platform.ibm.com에 액세스할 수 있는 컴퓨터로 다운로드하십시오.

표 *4. Analytic Server* 자체 추출 2진 파일

설명	2진 파일 이름
IBM SPSS Analytic Server 3.2.1 for Hortonworks Data Platform 2.5, 2.6, 3.0 및 3.1 Linux x86-64 영어	spss_as-3.2.1.0-hdp2.5-3.1-lx86.bin
IBM SPSS Analytic Server 3.2.1 for Hortonworks Data Platform 2.6, 3.0 및 3.1 Linux on System p LE 영어	spss_as-3.2.1.0-hdp2.6-3.1-lppc64.bin

2. 1단계에서 다운로드한 실행 가능한 2진 파일을 실행하고 오프라인 설치를 지정하십시오. 오프라인 설치는 나중에 설치 프로세스에 필요한 RPM 파일을 다운로드하며 https://ibm-open-platform.ibm.com에 액세스할 수 있는 컴퓨터에서 실행되어야 합니다. 다운로드한 파일은 현재 실행 가능한 2진 디렉토리 ./IBM-SPSS-AnalyticServer에 있습니다.
3. 실행 가능한 2진 디렉토리 ./IBM-SPSS-AnalyticServer의 전체 컨텐츠를 인터넷 액세스가 가능한 시스템에서 Ambari 관리자 노드의 <AS_INSTALLABLE_HOME> 디렉토리(Ambari 관리자 노드는 방화벽 뒤에 있음)로 복사하십시오.
4. Ambari 관리자 노드에서 다음 명령을 사용하여 Ambari 서버가 실행 중인지 확인하십시오.

   ```
   ambari-server status
   ```

5. 로컬 yum 리포지토리를 작성하는 도구를 설치하십시오.

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

   또는

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

6. Analytic Server RPM 파일의 리포지토리 역할을 하는 디렉토리를 작성하십시오. 다음 예를 참조하십시오.

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

7. 필수 Analytic Server RPM 파일을 새 디렉토리로 복사하십시오. 필요한 RPM 파일은 배포판, 버전 및 아키텍처에 따라 다릅니다.

   HDP 2.5, 2.6, 3.0 및 3.1(x86_64)

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

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

   HDP 2.6, 3.0 및 3.1(PPC64LE)

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

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

8. 로컬 리포지토리 정의를 작성하십시오. 예를 들어 다음 컨텐츠를 포함하는 IBM-SPSS-AnalyticServer-3.2.1.0.repo라는 파일을 /etc/yum.repos.d/(RHEL, CentOS의 경우) 또는 /etc/zypp/repos.d/(SLES의 경우)에 작성하십시오.

```
[IBM-SPSS-AnalyticServer]
name=IBM-SPSS-AnalyticServer
baseurl=file:///{path to local repository}
enabled=1
gpgcheck=0
protect=1
```

9. 로컬 yum 리포지토리를 작성하십시오.

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

10. 루트 사용자 명령 창에서 <AS_INSTALLABLE_HOME>/IBM-SPSS-AnalyticServer 디렉토리로 cd를 수행하고 run ./offLineInstall.sh를 수행하십시오. 스크립트가 이전에 실행된 2진 실행 파일 설치 명령에 대한 지속적인 반응을 읽고 rpm을 설치하는 데 적절한 플랫폼 명령을 실행합니다.

    참고: 외부에서 관리되는 MySQL 환경을 사용하는 경우에만 11단계가 적용됩니다.

11. AS_MetaStore로 사용될 MySQL 인스턴스가 설치되는 노드/호스트에서 add_mysql_user.sh 스크립트를 실행하십시오.

    a. add_mysql_user.sh 스크립트를 <AS_INSTALLABLE_HOME>/IBM-SPSS-AnalyticServer에서 MySQL 인스턴스(AS_MetaStore로 사용됨)가 설치된 노드/호스트로 복사하십시오.

       - MySQL 노드/호스트에서 add_mysql_user.sh 스크립트를 실행하십시오. 예를 들어, ./add_mysql_user.sh -u as_user -p spss -d aedb입니다.

       참고:

       - 사용자 이름 및 비밀번호가 Ambari 구성 화면의 AS_Metastore에 입력한 데이터베이스 사용자 이름 및 비밀번호와 일치해야 합니다.
       - 필요한 경우, 명령을 실행하도록 add_mysql_user.sh 스크립트를 수동으로 업데이트할 수 있습니다.
       - 보안 (루트 사용자 액세스) MySQL 데이터베이스에 대해 add_mysql_user.sh 스크립트를 실행하는 경우, -r 및 -t 매개변수를 사용하여 dbuserid 및 dbuserid_password를 전달하십시오. 스크립트가 dbuserid 및 dbuserid_password를 사용하여 MySQL 작업을 확인합니다.

    참고: AS_Configuration 화면의 metadata.repository.url 설정(**고급 analytics-meta**)이 MySQL 데이터베이스 호스트를 지정하도록 수정되어야 합니다. 예를 들어, JDBC 설정 mysql:///{analytic_metastore_host}/aedb?createDatabaseIfNotExist=true를 mysql:///{MySQL_DB}/aedb?createDatabaseIfNotExist=true로 변경하십시오.

12. 일반적으로 /var/lib/ambari-server/resources/stacks/$stackName/$stackVersion/repos/에 있는 Ambari 리포지토리 파일 repoinfo.xml을 업데이트하고 다음 행을 추가하여 로컬 yum 리포지토리를 사용하십시오.

```
<os type="host_os">
   <repo>
        <baseurl>file:///{path to local repository}/</baseurl>
        <repoid>IBM-SPSS-AnalyticServer</repoid>
        <reponame>IBM-SPSS-AnalyticServer-3.2.1.0</reponame>
   </repo>
</os>
```

예 {path to local repository}는 다음과 유사합니다.

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

13. 각각의 Ambari 비서버 클러스터 노드에 대해 다음 단계를 반복하십시오.
    a. 적절한 <AS_INSTALLABLE_HOME> 디렉토리의 전체 컨텐츠를 인터넷 액세스가 가능한 시스템에서 Ambari 비서버 클러스터 노드로 복사하십시오.
    b. 로컬 yum 리포지토리를 작성하는 도구를 설치하십시오.

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

       또는

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

    c. Analytic Server RPM 파일의 리포지토리 역할을 하는 디렉토리를 작성하십시오. 다음 예를 참조하십시오.

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

    d. 필수 Analytic Server RPM 파일을 새 디렉토리로 복사하십시오. 필요한 RPM 파일은 배포판, 버전 및 아키텍처에 따라 다릅니다.

       HDP 2.5, 2.6, 3.0 및 3.1(x86_64)

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

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

       HDP 2.6, 3.0 및 3.1(PPC64LE)

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

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

    e. 로컬 리포지토리 정의를 작성하십시오. 예를 들어 다음 컨텐츠를 포함하는 IBM-SPSS-AnalyticServer-3.2.1.0.repo라는 파일을 /etc/yum.repos.d/(RHEL, CentOS의 경우) 또는 /etc/zypp/repos.d/(SLES의 경우)에 작성하십시오.

       ```
       [IBM-SPSS-AnalyticServer]
       name=IBM-SPSS-AnalyticServer
       baseurl=file:///{path to local repository}
       enabled=1
       gpgcheck=0
       protect=1
       ```

    f. 로컬 yum 리포지토리를 작성하십시오.

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

14. 8 페이지의 『온라인 설치』 절의 3단계를 계속 수행하십시오.

HDP(Ubuntu)에서 수동 설치

HDP(Ubuntu)에서 수동 오프라인 설치에 대한 일반적인 워크플로우는 다음과 같습니다.

1. IBM Passport Advantage® 웹 사이트로 이동한 다음 적절한 Ubuntu 자체 추출 2진 파일을 https://ibm-open-platform.ibm.com에 액세스할 수 있는 컴퓨터로 다운로드하십시오.

표 *5. Analytic Server* 자체 추출 *2*진 파일

설명	2진 파일 이름
IBM SPSS Analytic Server 3.2.1 for Hortonworks Data Platform 2.5, 2.6, 3.0 및 3.1 Linux x86-64 영어	spss_as-3.2.1.0-hdp2.5-3.1-lx86.bin

2. 1단계에서 다운로드한 실행 가능한 2진 파일을 실행하고 오프라인 설치를 지정하십시오. 오프라인 설치는 나중에 설치 프로세스에 필요한 DEB 파일을 다운로드하며 https://ibm-open-platform.ibm.com에 액세스할 수 있는 컴퓨터에서 실행되어야 합니다. 다운로드한 파일은 현재 실행 가능한 2진 디렉토리 ./IBM-SPSS-AnalyticServer에 있습니다.
3. 실행 가능한 2진 디렉토리 ./IBM-SPSS-AnalyticServer의 전체 컨텐츠를 인터넷 액세스가 가능한 시스템에서 Ambari 관리자 노드의 <AS_INSTALLABLE_HOME> 디렉토리(Ambari 관리자 노드는 방화벽 뒤에 있음)로 복사하십시오.
4. Ambari 관리자 노드에서 다음 명령을 사용하여 Ambari 서버가 실행 중인지 확인하십시오.

   ```
   ambari-server status
   ```

5. Analytic Server DEB 파일의 리포지토리 역할을 하는 <local_repo> 디렉토리를 작성하십시오. 예를 들어, 다음과 같습니다.

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

6. 필수 Analytic Server DEB 파일을 <local_repo>로 복사하십시오.
   - IBM-SPSS-AnalyticServer-ambari-2.x_3.2.1.0_amd64.deb
   - IBM-SPSS-AnalyticServer_1_amd64.deb
7. 로컬 리포지토리를 작성하십시오.
   a. 다음과 같이 로컬 리포지토리를 작성하는 도구를 설치하십시오.

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

   b. 다음과 같이 소스 패키지 파일을 생성하십시오.

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

   c. 로컬 리포지토리의 구성요소(기본) 및 아키텍처(예: binary-i386, binary-amd64)를 작성하십시오.

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

   d. 다음과 같이 소스 패키지를 복사하십시오.

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

8. 로컬 리포지토리 정의를 작성하십시오. 예를 들어 다음 컨텐츠를 포함하는 IBM-SPSS-AnalyticServer-3.2.1.0.list라는 파일을 /etc/apt/sources.list.d에 작성하십시오.

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

9. 다음 명령을 실행하여 리포지토리 목록을 업데이트하십시오.

   ```
   apt-get update
   ```

10. 다음 명령을 실행하여 IBM SPSS Analytic Server 3.2.1를 설치하십시오.

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

    참고: 로컬 리포지토리가 올바르게 설정되었는지 확인하려는 경우 <local_repo> 디렉토리에서 이전의 명령을 실행하지 마십시오. 설치 시 패키지를 찾을 수 없는 경우 로컬 리포지토리가 올바르게 설치되지 않았음을 의미합니다(이 경우 이전의 모든 단계를 확인해야 함).

11. 각각의 Ambari 비서버 클러스터 노드에 대해 다음 단계를 반복하십시오.
    a. Analytic Server DEB 파일의 리포지토리 역할을 하는 <local_repo> 디렉토리를 작성하십시오. 예를 들어, 다음과 같습니다.

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

    b. <local_repo> 디렉토리의 전체 컨텐츠를 Ambari 관리자 노드 시스템에서 Ambari 비서버 클러스터 노드의 <local_repo> 디렉토리로 복사하십시오. 디렉토리에는 다음 파일이 포함되어야 합니다.
       - <local_repo>/IBM-SPSS-AnalyticServer-ambari-2.x_3.2.1.0_amd64.deb
       - <local_repo>/IBM-SPSS-AnalyticServer_1_amd64.deb
       - <local_repo>/Packages.gz
       - <local_repo>/dists/IBM-SPSS-AnalyticServer/main/binary-amd64/Packages
       - <local_repo>/dists/IBM-SPSS-AnalyticServer/main/binary-i386/Packages

    c. 로컬 리포지토리 정의를 작성하십시오. 예를 들어 다음 컨텐츠를 포함하는 IBM-SPSS-AnalyticServer-3.2.1.0.list라는 파일을 /etc/apt/sources.list.d에 작성하십시오.

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

12. 8 페이지의 『온라인 설치』 절의 3단계를 계속 수행하십시오.

외부적으로 관리되는 MySQL 환경에 대해 Analytic Server 설치

외부적으로 관리되는 MySQL 환경에 대해 설치하는 경우에 Analytic Server 설치 프로세스는 일반 설치와 다릅니다.

다음 단계에서는 외부적으로 관리되는 MySQL 환경에 대해 Analytic Server를 설치하는 프로세스에 대해 설명합니다.

1. IBM Passport Advantage® 웹 사이트로 이동한 다음 사용 중인 스택, 스택 버전 및 하드웨어 아키텍처에 해당하는 자체 추출 2진 파일을 Ambari 클러스터 내의 호스트로 다운로드하십시오.
2. 자체 추출 2진 파일을 실행하고, 다음 지시사항에 따라 라이센스를 확인하고(선택사항) 라이센스에 동의하십시오.

a. 온라인 옵션을 선택하십시오.

b. 프롬프트되면 **외부 MySQL 데이터베이스** 옵션을 선택하십시오.

3. add_mysql_user.sh 스크립트를 <AS_INSTALLABLE_HOME>/IBM-SPSS-AnalyticServer에서 MySQL 인스턴스(AS_MetaStore로 사용됨)가 설치된 노드/호스트로 복사하십시오.
   - MySQL 노드/호스트에서 add_mysql_user.sh 스크립트를 실행하십시오. 예를 들어, ./add_mysql_user.sh -u as_user -p spss -d aedb입니다.

   참고:
   - 사용자 이름 및 비밀번호가 Ambari 구성 화면의 AS_Metastore에 입력한 데이터베이스 사용자 이름 및 비밀번호와 일치해야 합니다.
   - 필요한 경우, 명령을 실행하도록 add_mysql_user.sh 스크립트를 수동으로 업데이트할 수 있습니다.
   - 보안 (루트 사용자 액세스) MySQL 데이터베이스에 대해 add_mysql_user.sh 스크립트를 실행하는 경우, -r 및 -t 매개변수를 사용하여 dbuserid 및 dbuserid_password를 전달하십시오. 스크립트가 dbuserid 및 dbuserid_password를 사용하여 MySQL 작업을 확인합니다.
4. Ambari 서버를 다시 시작하십시오.

   ```
   ambari-server restart
   ```
5. Ambari 콘솔에서 일반적인 방법으로 AnalyticServer 서비스를 추가하십시오. (3단계에서 입력한 것과 동일한 데이터베이스 사용자 이름 및 비밀번호를 입력하십시오.)

   참고: AS_Configuration 화면의 metadata.repository.url 설정(**고급 analytics-meta**)이 MySQL 데이터베이스 호스트를 지정하도록 수정되어야 합니다. 예를 들어, JDBC 설정 mysql://{analytic_metastore_host}/aedb?createDatabaseIfNotExist=true를 mysql://{MySQL_DB}/aedb?createDatabaseIfNotExist=true로 변경하십시오.

구성

설치 후 Ambari UI를 통해 Analytic Server를 선택적으로 구성하고 관리할 수 있습니다.

참고: Analytic Server 파일 경로에는 다음 규칙을 사용합니다.

- {AS_ROOT}는 Analytic Server가 배포된 위치를 나타냅니다(예: /opt/IBM/SPSS/AnalyticServer/3.2.
- {AS_SERVER_ROOT}는 구성, 로그 및 서버 파일의 위치를 나타냅니다 (예: /opt/IBM/SPSS/AnalyticServer/3.2/ae_wlpserver/usr/servers/aeserver).
- {AS_HOME}은 Analytic Server에서 루트 폴더로 사용되는 HDFS의 위치를 나타냅니다.

보안

LDAP 레지스트리 구성

LDAP 레지스트리를 사용하면 외부 LDAP 서버(예: Active Directory 또는 OpenLDAP)로 사용자를 인증할 수 있습니다.

중요사항: LDAP 사용자가 Ambari에서 Analytic Server 관리자로 지정되어야 합니다.

다음은 OpenLDAP용 ldapRegistry의 예제입니다.

```
<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>
```

다음 예는 Active Directory를 사용하는 Analytic Server 인증을 제공합니다.

```
<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>
```

참고: LDAP 뷰어 타사 도구를 사용하여 LDAP 구성을 확인하는 것이 도움이 되는 경우가 종종 있습니다.

다음 예는 Active Directory를 사용하는 WebSphere Liberty 프로파일 인증을 제공합니다.

```
<ldapRegistry id="ldap" realm="SampleLdapADRealm"
    host="ldapserver.mycity.mycompany.com" port="389" ignoreCase="true"
    baseDN="cn=users,dc=adtest,dc=mycity,dc=mycompany,dc=com"
    bindDN="cn=testuser,cn=users,dc=adtest,dc=mycity,dc=mycompany,dc=com"
    bindPassword="testuserpwd"
    ldapType="Microsoft Active Directory"
```

```
    sslEnabled="true"
    sslRef="LDAPSSLSettings">
    <actived Filters
       userFilter="(&amp;(sAMAccountName=%v)(objectcategory=user))"
       groupFilter="(&amp;(cn=%v)(objectcategory=group))"
       userIdMap="user:sAMAccountName"
       groupIdMap="*:cn"
       groupMemberIdMap="memberOf:member" >
    </actived Filters>
</ldapRegistry>

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

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

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

참고:

- Analytic Server에서 LDAP에 대한 지원은 WebSphere Liberty에 의해 제어됩니다. 자세한 정보는 Liberty에서 LDAP 사용자 레지스트리 구성을 참조하십시오.
- LDAP이 SSL로 보안되는 경우, 다음 "Analytic Server에서 LDAP으로의 SSL(Secure Socket Layer) 연결 구성"의 지시사항을 따르십시오.

Analytic Server에서 LDAP으로의 SSL(Secure Socket Layer) 연결 구성

Analytic Server 설치 중에 Apache Directory Server(ads) LDAP 옵션을 선택하고 기본 구성을 사용하는 경우 SSL을 구성하고 사용으로 설정하여 Apache Directory Server가 설치되었습니다(Analytic Server가 SSL을 사용하여 Apache Directory Server와 통신함).

Analytic Server 설치 중에 기타 LDAP 옵션 중 하나가 선택된 경우(예: 외부 LDAP 서버를 사용한 경우) 다음 단계를 사용하여 SSL을 구성하십시오.

1. 각 Analytic Server 시스템에 Analytic Server 사용자로 로그인하고 SSL 인증서를 위한 공통 디렉토리를 작성하십시오.

   참고: 기본적으로 as_user는 Analytic Server 사용자입니다. Ambari 콘솔의 관리자 탭에서 **서비스 계정**을 참조하십시오.

2. 키 저장소 및 신뢰 저장소 파일을 모든 Analytic Server 시스템의 공통 디렉토리에 복사하십시오. 또한 신뢰 저장소에 LDAP 클라이언트 CA 인증서를 추가하십시오. 다음은 샘플 지시사항입니다.

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

   참고: JAVA_HOME은 Analytic Server 시작에 사용되는 동일한 JRE입니다.

3. {AS_ROOT}/ae_wlpserver/bin에 있는 securityUtility 도구를 사용하여 비밀번호를 명확하지 않은 값으로 인코딩할 수 있습니다. 예제는 다음과 같습니다.

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

4. Ambari 콘솔에 로그인하고 올바른 SSL 구성 설정을 사용하여 Analytic Server 구성 설정 **ssl.keystore.config**를 업데이트하십시오. 예제는 다음과 같습니다.

```
<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="/>
```

   참고: 키 및 신뢰 저장소 파일의 절대 경로를 사용하십시오.

5. 올바른 LDAP 구성 설정을 사용하여 Analytic Server 구성 설정 **security.config**를 업데이트하십시오. 예를 들어 **ldapRegistry** 요소에서, **sslEnabled** 속성을 true로, **sslRef** 속성을 defaultSSLConfig로 설정하십시오.

Kerberos 구성

Analytic Server는 Ambari를 사용하여 Kerberos를 지원합니다.

참고: IBM SPSS Analytic Server는 Apache Knox와 함께 사용될 때 Kerberos 싱글 사인온(SSO)을 지원하지 않습니다.

1. Analytic Server에 대한 액세스 권한을 제공할 모든 사용자를 위해 Kerberos 사용자 리포지토리의 계정을 작성하십시오.
2. LDAP 서버에서 동일한 계정(이전 단계의)을 작성하십시오.
3. 모든 Analytic Server 노드 및 Hadoop 노드 각각에서 이전 단계에서 작성한 각 사용자의 OS 사용자 계정을 작성하십시오.
   - 모든 시스템에서 이러한 사용자의 UID가 일치하는지 확인하십시오. 이 kinit 명령 사용을 테스트하여 각 계정에 로그인할 수 있습니다.
   - UID가 "작업 제출용 최소 사용자 ID" Yarn 설정을 준수하는지 확인하십시오. 이는 container-executor.cfg에서 **min.user.id** 매개변수입니다. 예를 들어, **min.user.id**가 1000이면 작성된 각 사용자 계정의 UID가 1000 이상이어야 합니다.
4. Analytic Server의 모든 프린시펄에 대해 HDFS에 사용자 홈 폴더를 작성하십시오. 예를 들어, testuser1을 Analytic Server 시스템에 추가하는 경우 HDFS에 /user/testuser1과 같은 홈 폴더를 작성하고 testuser1에 이 폴더에 대한 읽기 및 쓰기 권한이 있는지 확인하십시오.
5. [선택사항] HCatalog 데이터 소스를 사용하려 하고 Analytic Server가 Hive metastore와 다른 시스템에 설치되어 있는 경우 HDFS에서 Hive 클라이언트로 위장해야 합니다.
   a. Ambari 콘솔에 있는 HDFS 서비스의 구성 탭으로 이동하십시오.
   b. * 값 또는 Analytic Server에 로그인할 수 있는 모든 사용자가 포함된 그룹을 포함하도록 **hadoop.proxyuser.hive.groups** 매개변수를 편집하십시오.

c. * 값 또는 Analytic Server의 모든 인스턴스 및 Hive metastore가 서비스로 설치된 호스트 목록을 포함하도록 **hadoop.proxyuser.hive.groups** 매개변수를 편집하십시오.

d. HDFS 서비스를 다시 시작하십시오.

이러한 단계가 수행되고 Analytic Server가 설치되면 Analytic Server가 자동으로 Kerberos를 구성합니다.

Kerberos를 통한 싱글 사인온(SSO)용 HAProxy 구성

1. HAProxy 문서 안내서에 따라서 HAProxy 구성하고 시작하십시오. http://www.haproxy.org/#docs
2. HAProxy 호스트의 Kerberos 원칙(HTTP/<proxyHostname>@<realm>) 및 키탭 파일을 작성하십시오. 여기서 <proxyHostname>은 HAProxy 호스트의 전체 이름이고 <realm>은 Kerberos 영역입니다.
3. 키탭 파일을 각 Analytic Server 호스트에 /etc/security/keytabs/spnego_proxy.service.keytab으로 복사하십시오.
4. 각 Analytic Server 호스트에서 이 파일에 대한 권한을 업데이트하십시오. 예제는 다음과 같습니다.

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

5. Amabri 콘솔을 열고 Analytic Server '사용자 정의 analytics.cfg' 섹션에서 다음 특성을 업데이트하십시오.

```
web.authentication.kerberos.keytab=/etc/security/keytabs/spnego_proxy.service.keytab
web.authentication.kerberos.principal=HTTP/<proxy machine full name>@<realm>
```

6. 구성을 저장하고 모든 Analytic Server 서비스를 Amabri 콘솔에서 다시 시작하십시오.

이제 사용자가 IBM SPSS Analytic Server 로그인 화면에서 **싱글 사인온 로그인** 옵션을 사용하여 Analytic Server에 로그인할 수 있습니다.

Kerberos 위장 사용

위장을 사용하면 스레드를 소유한 프로세스의 보안 컨텍스트와 다른 보안 컨텍스트에서 스레드를 실행할 수 있습니다. 예를 들어, 위장은 Hadoop 작업에 대해 표준 Analytic Server 사용자(as_user) 이외의 사용자로 실행할 수 있는 방법을 제공합니다. Kerberos 위장을 사용하려면 다음과 같이 수행하십시오.

1. Kerberos 사용 클러스터에서 실행되는 경우, 위장 구성 속성을 HDFS 또는 Hive 서비스 구성에 추가하십시오. HDFS의 경우, 다음 특성이 HDFS core-site.xml 파일에 추가되어야 합니다.

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

여기서, <analytic_server_service_principal_name>은 Analytic Server 구성의 Analytic_Server_User 필드에서 지정되는 기본 as_user 값입니다.

데이터가 Hive/HCatalog를 통해 HDFS에서 액세스되는 경우, 다음 특성도 HDFS core-site.xml 파일에 추가되어야 합니다.

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

2. Analytic Server가 as_user 외의 사용자 이름을 사용하도록 구성된 경우, 기타 사용자 이름(예: hadoop.proxyuser.xxxxx.hosts, 여기서, xxxxx는 Analytic Server 구성에서 지정된 구성된 사용자 이름)을 반영하도록 특성 이름을 수정해야 합니다.
3. Analytic Server 노드의 명령 쉘에서 다음 명령을 실행하십시오.

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

다중 영역 사용

다중 영역을 정의하는 경우 **as.kdc.realms** 설정이 필요합니다. **as.kdc.realms** 값은 Amabri 콘솔의 Analytic Server '고급 analytics.cfg' 섹션에 있습니다.

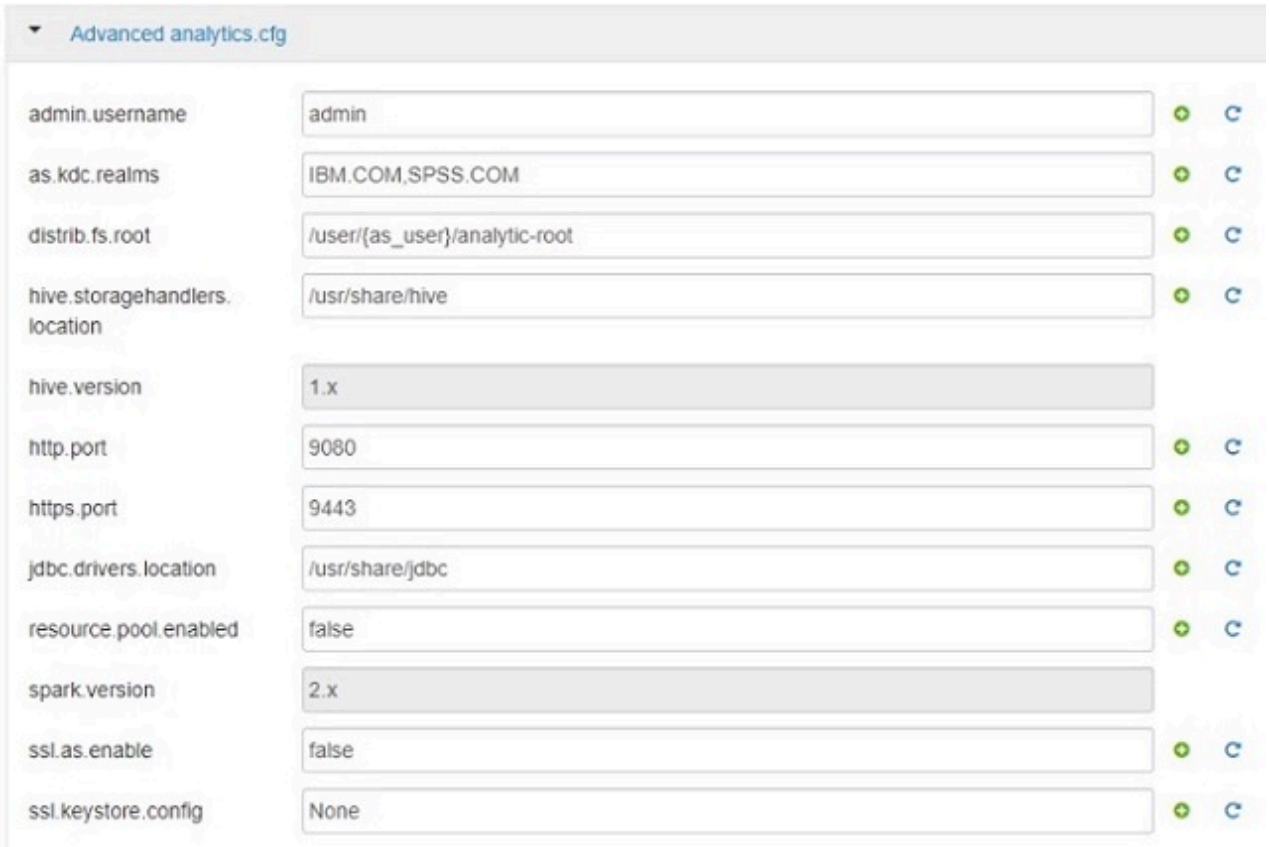

그림 *3.* 고급 *analytics.cfg* 설정

다중 영역 이름은 쉼표로 구분된 경우에 지원됩니다. 지정된 Kerberos 영역 이름은 사용자 이름과 일치하며 사용자 이름과 연관됩니다. 예를 들어 사용자 이름 UserOne@us.ibm.com 및 UserTwo@eu.ibm.com은 us.ibm.com,eu.ibm.com 영역과 일치합니다.

둘 이상의 영역이 **Kerberos 영역 이름**으로 지정된 경우 Kerberos 교차 영역 신뢰를 구성해야 합니다. Analytic Server 콘솔 로그인 프롬프트에 입력한 사용자 이름이 영역 이름 접미부 없이 입력됩니다. 따라서 다중 영역이 지정된 경우 **영역** 드롭 다운 목록이 사용자에게 표시되며 사용자는 이 목록에서 영역을 선택할 수 있습니다.

참고: 영역이 한 개만 지정된 경우 Analytic Server에 로그인할 때 **영역** 드롭 다운 목록이 사용자에게 표시되지 않습니다.

Kerberos 사용 안함

1. Ambari 콘솔에서 Kerberos를 사용 안함으로 설정하십시오.
2. Analytic Server 서비스를 중지하십시오.
3. 사용자 정의 `analytics.cfg`에서 다음 매개변수를 제거하십시오.

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

4. **저장**을 클릭하고 Analytic Server 서비스를 다시 시작하십시오.

Analytic Server 콘솔에 대한 SSL(Secure Socket Layer) 연결 사용

기본적으로 Analytic Server는 자체 서명된 인증서를 생성하여 SSL(Secure Socket Layer)을 사용합니다. 이렇게 하면 자체 서명된 인증서를 채택하여 보안 포트를 통해 Analytic Server 콘솔에 액세스할 수 있습니다. HTTPS 액세스의 보안을 강화하려면 써드파티 벤더 인증서를 설치해야 합니다.

써드파티 벤더 인증서를 설치하려면 다음 단계를 수행하십시오.

1. 써드파티 벤더 키 저장소 및 신뢰 저장소 인증서를 모든 Analytic Server 노드의 동일한 디렉토리에 복사하십시오(예: `/home/as_user/security`).

   참고: Analytic Server 사용자에게 이 디렉토리에 대한 읽기 액세스 권한이 있어야 합니다.
2. Ambari 서비스 탭에서 Analytic Server 서비스의 구성 탭으로 이동하십시오.
3. **`ssl.keystore.config`** 매개변수를 편집하십시오.

```
<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>"/>
```

다음과 같이 바꾸십시오.

- <KEYSTORE-LOCATION>을 키 저장소의 절대 위치로(예: /home/as_user/security/mykey.jks)
- <TRUSTSTORE-LOCATION>을 신뢰 저장소의 절대 위치로(예: /home/as_user/security/mytrust.jks)
- <TYPE>을 인증서 유형으로(예: JKS, PKCS12 등)
- <PASSWORD>를 Base64 암호화 형식의 암호화된 비밀번호로. 인코딩의 경우 securityUtility를 사용할 수 있습니다(예: /opt/ibm/spss/analyticserver/3.2/ae_wlpserver/bin/securityUtility encode <password>).

자체 서명된 인증서를 생성하려는 경우 securityUtility를 사용할 수 있습니다(예: /opt/ibm/spss/analyticserver/3.2/ae_wlpserver/bin/securityUtility createSSLCertificate --server=myserver --password=mypassword --validity=365 --subject=CN=mycompany,O=myOrg,C=myCountry). .

참고: CN 값에 대해 적절한 호스트 도메인 이름을 제공해야 합니다.

securityUtility 및 기타 SSL 설정에 대한 자세한 정보는 WebSphere Liberty Profile 문서를 참조하십시오.

4. **저장**을 클릭하고 Analytic Server 서비스를 다시 시작하십시오.

SSL을 통해 Apache Hive와 통신

SSL 연결을 통해 Apache Hive와 통신하려면 hive.properties 파일을 업데이트해야 합니다. 또는 Apache Hive 환경이 고가용성에 대해 사용으로 설정된 경우 기본 Analytic Server 데이터 소스 페이지에 있는 고가용성 매개변수를 선택할 수 있습니다.

hive.properties 파일 업데이트

1. hive.properties 파일을 여십시오. 이 파일은 /opt/ibm/spss/AnalyticServer-3.2.1.0/ae_wlpserver/usr/servers/aeserver/configuration/database에 있습니다.
2. 다음 행을 찾으십시오.

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

3. 다음과 같이 **굵게** 표시된 정보를 추가하여 행을 업데이트하십시오.

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

4. hive.properties 파일을 저장하십시오.

Essentials for R에 대한 지원 사용

Analytic Server에서는 R 모델 스코어링 및 R 스크립트 실행을 지원합니다.

Analytic Server 설치 완료 후에 R의 지원을 구성하려면 다음을 수행하십시오.

1. Essentials for R에 대한 서버 환경을 프로비저닝하십시오.

RedHat Linux x86_64

다음 명령을 실행하십시오.

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

Ubuntu Linux

다음 명령을 실행하십시오.

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

SUSE Linux

SUSE에 Essentials for R을 설치하려면 구성된 ZYPPER 리포지토리에서는 일반적으로 사용 불가능하며 SUSE SDK 매체에서만 사용 가능한 호환 가능한 FORTRAN이 필요합니다. 결과적으로 FORTRAN을 설치할 수 없어서 SUSE 서버에서 Essentials for R에 대해 Ambari 설치 실행이 실패합니다. 다음 단계를 사용하여 SUSE에서 프로비저닝하십시오.

a. GCC C++을 설치하십시오.

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

b. GCC FORTRAN을 설치하십시오. 필수 RPM 파일이 SUSE SDK 매체에서 복사되어 다음 순서로 설치되어야 합니다.

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

c. 다음 명령을 실행하여 Essentials for R 라이브러리를 설치하십시오.

```
R_PREFIX=/opt/ibm/spss/R
cd $R_PREFIX
rm -fr $R_PREFIX/r_libs
mkdir -p $R_PREFIX/r_libs
cd $R_PREFIX/r_libs
wget https://zlib.net/fossils/zlib-1.2.11.tar.gz --no-check-certificate
tar zxvf zlib-1.2.11.tar.gz
cd zlib-1.2.11/
./configure
make && make install
cd $R_PREFIX/r_libs
wget http://www.bzip.org/1.0.6/bzip2-1.0.6.tar.gz
tar xzvf bzip2-1.0.6.tar.gz
cd bzip2-1.0.6
sed "s|^CC=gcc|CC=gcc -fPIC|" -i ./Makefile
make -f Makefile-libbz2_so
make clean
make
make install
cd $R_PREFIX/r_libs
wget https://tukaani.org/xz/xz-5.2.3.tar.gz
tar xzvf xz-5.2.3.tar.gz
cd xz-5.2.3
./configure
make -j3
make install
cd $R_PREFIX/r_libs
wget http://ftp.pcre.org/pub/pcre/pcre-8.38.tar.gz
tar xzvf pcre-8.38.tar.gz
cd pcre-8.38
./configure --enable-utf8
make
make install
```

```
cd $R_PREFIX/r_libs
wget https://www.openssl.org/source/openssl-1.0.2l.tar.gz --no-check-certificate
tar zxvf openssl-1.0.2l.tar.gz
cd openssl-1.0.2l/
./config shared
make
make install
echo '/usr/local/ssl/lib' >> /etc/ld.so.conf
ldconfig
cd $R_PREFIX/r_libs
wget --no-check-certificate https://curl.haxx.se/download/curl-7.50.1.tar.gz
tar xzvf curl-7.50.1.tar.gz
cd curl-7.50.1
./configure --with-ssl
make -j3
make install
cd $R_PREFIX/r_libs
wget ftp://rpmfind.net/linux/opensuse/distribution/12.3/repo/oss/suse/x86_64/libgomp1-4.7.2_20130108-2.1.6.x86_64.rpm --no-check-certificate
rpm -ivh libgomp1-4.7.2_20130108-2.1.6.x86_64.rpm
```

2. IBM SPSS Modeler Essentials for R RPM 또는 DEB의 자체 추출 아카이브(BIN)를 다운로드하십시오. Essentials for R을 다운로드할 수 있습니다(https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=swg-tspssp). 스택, 스택 버전 및 하드웨어 아키텍처에 대한 파일을 선택하십시오.
3. 자체 추출 2진 파일을 실행하고, 다음 지시사항에 따라 라이센스를 확인하고(선택사항) 라이센스에 동의한 다음, 온라인 또는 오프라인 설치를 선택하십시오.

   온라인 설치

   Ambari 서버 호스트 및 클러스터의 모든 노드가 https://ibm-open-platform.ibm.com에 액세스할 수 있는 경우 온라인 설치를 선택하십시오.

   오프라인 설치

   Ambari 서버 호스트에게 인터넷 액세스 권한이 없는 경우 오프라인을 선택하십시오. 오프라인 설치는 필요한 RPM 파일을 다운로드하며 https://ibm-open-platform.ibm.com에 액세스할 수 있는 시스템에서 실행해야 합니다. 그런 다음 RPM 파일을 Ambari 서버 호스트에 복사할 수 있습니다.

   a. Ambari 서버 호스트에서 임의의 위치로 필요한 Essentials for R RPM 또는 DEB 파일을 복사하십시오. 필요한 RPM/DEB 파일은 아래에 표시된 배포판, 버전 및 아키텍처에 따라 다릅니다.

      HDP 2.5 및 2.6(x86_64)

      IBM-SPSS-ModelerEssentialsR-ambari-2.1-HDP-2.6-9.0.0.0-1.x86_64.rpm

      HDP 2.6(PPC64LE)

      IBM-SPSS-ModelerEssentialsR-ambari-2.1-HDP-2.6-9.0.0.0-1.ppc64le.rpm

      HDP 2.5 및 2.6(Ubuntu)

      IBM-SPSS-ModelerEssentialsR-ambari-3.2.1.0_3.2.1.0_amd64.deb

   b. RPM 또는 DEB를 설치하십시오. 다음 예에서는 명령이 HDP 2.6(x86_64)에 Essentials for R을 설치합니다.

      ```
      rpm -i IBM-SPSS-ModelerEssentialsR-ambari-2.1-HDP-2.6-9.0.0.0-1.x86_64.rpm
      ```

      다음 예에서는 명령이 HDP 2.5(Ubuntu)에 Essentials for R을 설치합니다.

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

4. Ambari 서버를 다시 시작하십시오.

   ```
   ambari-server restart
   ```

5. Ambari 서버에 로그온하고 Ambari 콘솔을 통해 SPSS Essentials for R을 서비스로 설치하십시오. SPSS Essentials for R이 Analytic Server 및 Analytic Metastore가 설치된 모든 호스트에 설치되어야 합니다.

   참고: Ambari는 R 설치 이전에 gcc-c++, gcc-gfortran(RHEL) 및 gcc-fortran(SUSE)을 설치합니다. 이러한 패키지는 R의 Ambari 서비스 정의에서 종속 항목으로 선언됩니다. R을 설치 및 실행할 서버가 gcc-c++ 및 gcc-[g]fortran RPM을 다운로드하도록 구성되어 있는지 확인하거나 GCC 및 FORTRAN 컴파일러가 설치되어 있는지 확인하십시오. Essentials for R 설치에 실패한 경우 Essentials for R을 설치하기 전에 이러한 패키지를 수동으로 설치하십시오.

6. Analytic Server 서비스를 새로 고치십시오.
7. 34 페이지의 『클라이언트 종속 항목 업데이트』의 지시사항에 따라 `update_clientdeps` 스크립트를 실행하십시오.
8. 또한 SPSS Modeler 서버를 호스트하는 시스템에서 Essentials for R을 설치해야 합니다. 세부사항은 SPSS Modeler 문서를 참조하십시오.

관계형 데이터베이스 소스 사용

사용자가 각 Analytic Server 호스트에서 공유 디렉토리에 JDBC 드라이버를 제공하면 Analytic Server가 관계형 데이터베이스 소스를 사용할 수 있습니다. 기본적으로 이 디렉토리는 `/usr/share/jdbc` 입니다.

공유 디렉토리를 변경하려면 다음 단계를 수행하십시오.

1. Ambari 서비스 탭에서 Analytic Server 서비스의 구성 탭으로 이동하십시오.
2. **고급 analytics.cfg** 섹션을 여십시오.
3. **jdbc.drivers.location**에 JDBC 드라이버의 공유 디렉토리 경로를 지정하십시오.
4. **저장**을 클릭하십시오.
5. Analytic Server 서비스를 중지하십시오.
6. **새로 고치기**를 클릭하십시오.
7. Analytic Server 서비스를 시작하십시오.

표 *6.* 지원되는 데이터베이스

데이터베이스	지원되는 버전	JDBC 드라이버 jar	벤더
Amazon Redshift	8.0.2 이상	`RedshiftJDBC41-1.1.6.1006.jar` 이상	Amazon
BigSQL	4.1.0.0 이상	db2jcc.jar	IBM
DashDB	Bluemix Service	`db2jcc.jar`	IBM
Linux, UNIX 및 Windows용 Db2	11.1, 10.5, 10.1, 9.7	`db2jcc.jar`	IBM

표 6. 지원되는 데이터베이스 (계속)

데이터베이스	지원되는 버전	JDBC 드라이버 jar	벤더
Db2 z/OS	11, 10	db2jcc.jar, db2_license_cisuz.jar	IBM
Greenplum	5	postgresql.jar	Greenplum
Hive	1.2, 2.1	hive-jdbc-*.jar	Apache
MySQL	5.6, 5.7	mysql-connector-java-commercial-5.1.25-bin.jar	MySQL
Netezza	7, 6.x	nzjdbc.jar	IBM
Oracle	12c, 11g R2(11.2)	ojdbc6.jar, orai18n.jar	Oracle
SQL Server	2014, 2012, 2008 R2	sqljdbc4.jar	Microsoft
Teradata	15, 15.1	tdgssconfig.jar, terajdbc4.jar	Teradata

참고

- Analytic Server를 설치하기 전에 Redshift 데이터 소스를 작성한 경우 Redshift 데이터 소스를 사용하려면 다음 단계를 수행해야 합니다.
  1. Analytic Server 콘솔에서 Redshift 데이터 소스를 여십시오.
  2. Redshift 데이터베이스 데이터 소스를 선택하십시오.
  3. Redshift 서버 주소를 입력하십시오.
  4. 데이터베이스 이름과 사용자 이름을 입력하십시오. 비밀번호는 자동으로 채워져야 합니다.
  5. 데이터베이스 테이블을 선택하십시오.
- BigSQL은 Apache Hadoop 환경에 대한 IBM SQL 인터페이스입니다. BigSQL은 관계형 데이터베이스가 아니지만 Analytic Server가 JDBC를 통해 이에 액세스하도록 지원합니다. JDBC jar 파일은 Db2용으로 사용되는 것과 동일합니다.

  Analytic Server와 함께 BigSQL을 사용하는 일반적인 방법은 HCatalog 데이터 소스를 통해 BigSQL Hadoop/HBase 테이블에 액세스하는 것입니다.

HCatalog 데이터 소스 사용

Analytic Server는 Hive/HCatalog를 통해 많은 데이터 소스에 대한 지원을 제공합니다. 일부 소스에는 수동 구성 단계가 필요합니다.

1. 데이터 소스를 사용하는 데 필요한 JAR 파일을 수집하십시오. 추가 단계 없이 Apache HBase 및 Apache Accumulo에 대한 지원을 사용할 수 있습니다. 기타 NoSQL 데이터 소스의 경우 데이터베이스 벤더에 문의하여 저장 공간 핸들러 및 관련 jar를 확보하십시오. 지원되는 HCatalog 데이터 소스에 대한 정보는 IBM SPSS Analytic Server 3.2.1 사용자 안내서의 "HCatalog 데이터 소스 사용" 절을 참조하십시오.
2. 이 JAR 파일을 각 Analytic Server 노드의 {HIVE_HOME}/auxlib 디렉토리 및 /usr/share/hive 디렉토리에 추가하십시오.

3. Hive Metastore 서비스를 다시 시작하십시오.
4. Analytic Metastore 서비스를 새로 고치십시오.
5. Analytic Server 서비스의 인스턴스를 각각 다시 시작하십시오.

참고:

- Analytic Server Metastore는 Hive Metastore와 동일한 시스템에 설치할 수 없습니다.
- Analytic Server HCatalog 데이터 소스를 통해 HBase 데이터에 액세스하는 경우 액세스하는 사용자는 HBase 테이블에 대한 읽기 권한이 있어야 합니다.
  - Kerberos 이외의 환경에서 Analytic Server는 `as_user`를 사용하여 HBase에 액세스합니다(`as_user`는 HBase에 대한 읽기 권한이 있어야 함).
  - Kerberos 환경에서 `as_user` 및 로그인 사용자는 모두 HBase 테이블에 대한 읽기 권한이 있어야 합니다.

NoSQL 데이터베이스

Analytic Server는 벤더에서 사용할 수 있는 Hive 저장 공간 핸들러의 모든 NoSQL 데이터베이스를 지원합니다.

추가 단계 없이 Apache HBase 및 Apache Accumulo에 대한 지원을 사용할 수 있습니다.

기타 NoSQL 데이터베이스의 경우 데이터베이스 벤더에 문의하여 저장 공간 핸들러 및 관련 jar를 확보하십시오.

파일 기반 Hive 테이블

Analytic Server는 사용 가능한 기본 제공 또는 사용자 정의 Hive SerDe(직렬 변환기-병렬 변환기)의 파일 기반 Hive 테이블을 지원합니다.

XML 파일 처리를 위한 Hive XML SerDe는 http://search.maven.org/#search%7Cga%7C1%7Chivexmlserde의 Maven 중앙 리포지토리에 있습니다.

MapReduce v2 작업

Analytic Server **사용자 정의 analytics.cfg** 섹션에서 **preferred.mapreduce** 설정을 사용하여 MapReduce 작업이 처리되는 방식을 제어하십시오.

표 7. 사용자 정의 *analytics.cfg* 특성

특성	설명
`preferred.mapreduce`	MapReduce 작업이 실행되는 방식을 제어합니다. 유효한 값은 다음과 같습니다. • `spark` • `m3r` • `hadoop` 예: `preferred.mapreduce=spark`

Apache Spark

Spark(버전 1.5 이상)를 사용하려면 Analytic Server 설치 중에 `spark.version` 특성을 수동으로 추가해야 합니다.

1. Amabri 콘솔을 열고 다음 특성을 Analytic Server **고급 analytics.cfg** 섹션에 추가하십시오.
   - **키**: `spark.version`
   - **값**: 적절한 Spark 버전 번호(예를 들어, `1.x`, `2.x` 또는 `None`)를 입력하십시오.
2. 구성을 저장하십시오.

참고: HCatalog가 사용자 정의 `analytics.cfg` 설정을 통해 Spark를 사용하지 않도록 자동 설정할 수 있습니다.

1. Amabri 콘솔을 열고 다음 특성을 Analytic Server **사용자 정의 analytics.cfg** 섹션에 추가하십시오.
   - **키**: `spark.hive.compatible`
   - **값**: `false`

Analytic Server가 사용하는 포트 변경

Analytic Server는 기본적으로 HTTP의 경우 9080 포트를, HTTPS의 경우 9443 포트를 사용합니다. 포트 설정을 변경하려면 다음 단계를 수행하십시오.

1. Ambari 서비스 탭에서 Analytic Server 서비스의 구성 탭으로 이동하십시오.
2. **고급 analytics.cfg** 섹션을 여십시오.
3. **http.port** 및 **https.port**에 각각 원하는 HTTP 및 HTTPS 포트를 지정하십시오.
4. **저장**을 클릭하십시오.
5. Analytic Server 서비스를 다시 시작하십시오.

고가용성 Analytic Server

클러스터의 여러 노드에 서비스로 추가하여 Analytic Server의 가용성을 높일 수 있습니다.

1. Ambari 콘솔의 호스트 탭으로 이동하십시오.
2. 아직 Analytic Server를 실행하지 않는 호스트를 서비스로 선택하십시오.
3. 요약 탭에서 **추가**를 클릭하고 Analytic Server를 선택하십시오.
4. **추가 확인**을 클릭하십시오.

다중 클러스터 지원

다중 클러스터 기능은 IBM SPSS Analytic Server의 고가용성 기능에 대한 향상된 기능이며 다중 테넌트 환경에서 더 효율적으로 격리할 수 있습니다. 기본적으로 Ambari 또는 Cloudera Manager에서 Analytic Server 서비스를 설치하면 단일 분석 서버 클러스터가 정의됩니다.

클러스터 스펙은 Analytic Server 클러스터 멤버십을 정의합니다. 클러스터 스펙 수정은 XML 컨텐츠로(Ambari Analytic Server 구성의 analytics-cluster 필드에서 또는 Cloudera Manager의 configuration/analytics-cluster.xml 파일을 수동으로 편집하여) 수행됩니다. 다중 Analytic Server 클러스터를 구성하는 경우, 자체 로드 밸런서를 사용하여 각 Analytic Server 클러스터에 요청을 피드해야 합니다.

다중 클러스터 기능을 사용하면 한 테넌트에 대한 작업이 다른 테넌트의 클러스터에서 수행되는 작업에 부정적인 영향을 미치지 못하도록 할 수 있습니다. 고가용성 작업의 경우, 작업이 시작된 Analytic Server 클러스터의 범위 내에서만 작업 장애 복구가 발생할 수 있습니다. 다음 예는 다중 클러스터 XML 스펙을 제공합니다.

참고: Analytic Server는 서비스로 클러스터 내의 다중 노드에 추가함으로써 고가용성으로 만들 수 있습니다.

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

이전 예에서는 두 개의 로드 밸런서가 필요합니다. 한 개의 로드 밸런서가 cluster1 멤버(one.cluster 및 two.cluster)에 요청을 전송하고 다른 로드 밸런서가 cluster2 멤버(three.cluster 및 four.cluster)에 요청을 전송합니다.

다음 예는 단일 클러스터 XML 스펙(기본 구성)을 제공합니다.

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

이전 예에서는 구성된 클러스터 멤버가 두 개 이상인 경우를 처리하기 위해 단일 로드 밸런서가 필요합니다.

참고

- 싱글톤 클러스터만 **memberName** 요소에서의 와일드카드 사용을 지원합니다. 예를 들어, 클러스터 카디널리티 = "1"인 경우입니다. 카디널리티 요소에 대해 유효한 값은 1 및 1+입니다.
- **memberName**은 Analytic Server 역할이 지정된 호스트 이름과 동일한 방법으로 지정되어야 합니다.
- 모든 클러스터의 모든 서버는 클러스터 구성 변경이 적용된 후에 다시 시작되어야 합니다.

- Cloudera Manager에서는 모든 Analytic Server 노드에서 analytics-cluster.xml 파일을 수정 및 유지보수해야 합니다. 모든 노드가 동일한 컨텐츠를 포함하도록 유지보수되어야 합니다.

작은 데이터를 위한 JVM 옵션 최적화

작은(M3R) 작업을 실행할 때 시스템을 최적화하기 위해 JVM 특성을 편집할 수 있습니다.

Ambari 콘솔의 Analytic Server 서비스에서 구성 탭의 고급 analytics-jvm-options 절을 참조하십시오. 다음 매개변수를 수정하여 Hadoop이 아니라 Analytic Server를 호스트하는 서버에서 실행되는 작업에 대한 힙 크기를 설정하십시오. 이는 작은(M3R) 작업을 실행하는 경우에 중요하며 시스템을 최적화하기 위해 해당 값을 사용하여 시험해야 합니다.

```
-Xms512M
-Xmx2048M
```

클라이언트 종속 항목 업데이트

이 절에서는 update_clientdeps 스크립트를 사용하여 Analytic Server 서비스의 종속 항목을 업데이트하는 방법에 대해 설명합니다.

1. Ambari 서버 호스트에 루트로 로그인하십시오.
2. 디렉토리를 /var/lib/ambari-server/resources/stacks/<stack-name>/<stack-version>/services/ANALYTICSERVER/package/scripts로 변경하십시오. 다음 예제를 참조하십시오.

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

3. 다음 인수로 update_clientdeps 스크립트를 실행하십시오.

   -u <ambari-user>
   Ambari 계정 사용자 이름

   -p <ambari-password>
   Ambari 계정 사용자의 비밀번호입니다.

   -h <ambari-host>
   Ambari 서버의 호스트 이름입니다.

   -x <ambari-port>
   Ambari가 청취하는 포트입니다.

   다음 예를 참조하십시오.

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

4. 다음 명령으로 Ambari 서버를 다시 시작하십시오.

   ```
   ambari-server restart
   ```

Apache Knox 구성

Apache Knox 게이트웨이는 Apache Hadoop 서비스에 대한 단일 보안 액세스 지점을 제공하는 시스템입니다. 이 시스템은 클러스터 데이터에 액세스하고 작업을 실행하는 사용자 및 액세스를 제어하

고 클러스터를 관리하는 운영자 둘 다에 대한 Hadoop 보안을 단순화합니다. 게이트웨이는 하나 이상의 Hadoop 클러스터를 제공하는 서버 또는 서버 클러스터로 실행됩니다.

참고: IBM SPSS Analytic Server는 Kerberos 싱글 사인온(SSO)과 함께 사용될 때 Apache Knox를 지원하지 않습니다.

Apache Knox 게이트웨이는 효율적으로 Hadoop 클러스터 토폴로지 세부사항을 숨기고 엔터프라이즈 LDAP 및 Kerberos와 통합됩니다. 다음 절에서는 필수 Apache Knox 및 Analytic Server 구성 태스크에 대한 정보를 제공합니다.

필수조건

- 알려진 Apache Knox 문제는 HTTP 쿠키 및 헤더에 포함된 보안 정보를 전파하지 않습니다(자세한 정보는 https://issues.apache.org/jira/browse/KNOX-895 참조). 이 문제는 Knox 0.14.0(이상)에서 해결되었습니다. Knox를 사용하여 Analytic Server에서 작업하기 전에 Knox 0.14.0(이상)을 포함하는 업데이트된 Hortonworks 배포판을 확보해야 합니다. 자세한 정보는 Hortonworks 제공자에게 문의하십시오.
- Analytic Server 노드는 비밀번호가 없는 SSH 연결을 사용하여 Knox 서버와 연결되어야 합니다. 비밀번호가 없는 SSH 연결은 Analytic Server에서 Knox로 이동합니다(**Analytic Server** > **Knox**).
- Analytic Server는 Knox 서비스가 설치된 후에 설치되어야 합니다.

일부 경우에는 예상치 못한 문제로 인해 구성 파일이 자동으로 복사되지 않습니다. 이러한 경우에는 다음 구성 파일을 수동으로 복사해야 합니다.

- `com.ibm.spss.knox_0.6-3.2.1.0.jar`: 이 파일을 다음 Analytic Server 위치에서

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

  다음 Knox 서버 노드로 복사해야 합니다.

  `/KnoxServicePath/ext`

  예: `/usr/iop/4.1.0.0/knox/ext`
- `rewrite.xml` 및 `service.xml` 파일을 다음 Analytic Server 위치에서

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

  다음 Knox 서버 노드로 복사해야 합니다.

  `/KnoxServicePath/data/services`

  예: `/usr/iop/4.1.0.0/knox/data/services`

참고: rewrite.xml 및 service.xml 파일은 두 세트가 있습니다(한 세트는 http://rest 트래픽용, 다른 하나의 세트는 ws://websocket 트래픽용). rewrite.xml 및 service.xml(analyticserver 및 analyticserver_ws용)을 모두 Knox 서버 노드에 복사하십시오.

Ambari 구성

Ambari 사용자 인터페이스에 Analytic Server 서비스를 다음과 같이 구성해야 합니다.

1. Ambari 사용자 인터페이스에서 **Knox** > **구성** > **고급 토폴로지**를 탐색하십시오. 현재 Knox 구성 설정이 **컨텐츠** 창에 표시됩니다.
2. Knox 구성에서 다음 두 개의 서비스를 **고급 토폴로지** 섹션에 추가하십시오.

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

   적절한 Analytic Server 서버 이름 및 포트 번호로 {analyticserver-host} 및 {analyticserver-port}를 바꿔야 합니다.

   - {analyticserver-host} URL은 Ambari 사용자 인터페이스(**SPSS Analytic Server** > **요약** > **Analytic Server**)에 있습니다.
   - {analyticserver-port} 번호는 Ambari 사용자 인터페이스(**SPSS Analytic Server** > **구성** > **고급 analytics.cfg** > **http.port**)에 있습니다.

   참고: Analytic Server가 여러 노드에 배포되고 로드 밸런서가 사용되는 경우 {analyticserver-host} 및 {analyticserver-port}는 로드 밸런서 URL 및 포트 번호와 일치해야 합니다.
3. Knox 서비스를 다시 시작하십시오.

LDAP이 사용되는 경우 Knox의 기본값은 제공된 "데모" LDAP입니다. 엔터프라이즈 LDAP 서버(예: Microsoft LDAP 또는 OpenLDAP)로 변경할 수 있습니다.

Analytic Server 구성

Analytic Server에 LDAP을 사용하려면 Analytic Server가 Apache Knox에서 사용하는 것과 동일한 LDAP 서버를 사용하도록 구성되어야 합니다. 적절한 Knox LDAP 서버 설정을 반영하도록 다음 Ambari 설정에 대한 <값> 항목을 업데이트해야 합니다.

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

값은 Ambari 사용자 인터페이스의 **Knox** > **구성** > **고급 토폴로지**에서 사용 가능합니다. 예를 들어, 다음과 같습니다.

```
<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://{{knox_host_name}}:33389</value>
</param>
```

Knox LDAP 설정을 업데이트한 후에 Knox 서비스를 다시 시작하십시오.

중요사항: Analytic Server 관리자 비밀번호는 Knox 관리자 비밀번호와 동일해야 합니다.

Apache Knox 구성

1. Knox gateway.jks 파일을 새로 고치십시오.
   a. Knox 서버에서 Knox 서비스를 중지하십시오.
   b. /var/lib/knox/data-2.6.2.0-205/security/keystores에서 gateway.jks를 삭제하십시오.
   c. Knox 서비스를 다시 시작하십시오.
2. Knox 서버에서 서브디렉토리 <knox_server>/data/service/analyticserver/3.2.1.0을 작성한 다음 service.xml 및 rewrite.xml 파일을 새 디렉토리로 업로드하십시오. 이 두 파일은 Analytic Server의 <analytic_server>/configuration/knox/analyticserver/에 있습니다(예: /opt/ibm/spss/analyticserver/3.2/ae_wlpserver/usr/servers/aeserver/configuration/knox/analyticserver/*.xml).
3. <knox_server>/bin에서 ./knoxcli.sh redeploy --cluster default 스크립트를 실행하십시오.
4. com.ibm.spss.knoxservice_0.6-*.jar 파일을 <knox_server>/ext로 업로드하십시오. 이 파일은 Analytic Server의 <analytic_server>/apps/AE_BOOT.war/WEB-INF/lib/com.ibm.spss.knox_0.6-3.2.1.0.jar에 있습니다(예: /opt/ibm/spss/analyticserver/3.2/ae_wlpserver/usr/servers/aeserver/apps/AE_BOOT.war/WEB-INF/lib/com.ibm.spss.knox_0.6-3.2.1.0.jar).
5. Ambari 사용자 인터페이스에서 다음 요소를 **Knox** > **구성** > **고급 토폴로지**에 추가하십시오.

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

   참고: 기본적으로 WebSocket 기능은 사용 안함으로 설정되어 있습니다. /conf/gateway-site.xml 파일에서 gateway.websocket.feature.enabled 특성을 true로 변경하여 사용으로 설정할 수 있습니다.
6. Ambari 사용자 인터페이스에서 **Knox** > **구성** > **고급 사용자 LDIF**에 사용자를 추가하거나 업데이트하십시오. 예를 들어, admin, qauser1, qauser2입니다.
7. **Knox** > **서비스 조치** > **데모 LDAP 시작**에서 LDAP을 다시 시작하십시오.
8. Knox 서비스를 다시 시작하십시오.

Hortonworks Data Platform(HDP)에 Apache Knox 설치

다음 단계는 HDP 클러스터에 Apache Knox를 설치하는 프로세스를 설명합니다.

1. Knox 사용자가 HDP 클러스터에 있는지 확인하십시오. Knox 사용자가 없으면 작성해야 합니다.
2. Apache Knox를 /home/knox 아래의 폴더에 다운로드하고 추출하십시오.
3. HDP에서 Knox 사용자로 전환하고 knox 폴더로 이동하십시오. Knox 사용자가 모든 knox 서브폴더에 대해 permission(RWX)을 갖고 있어야 합니다.
4. Analytic Server에 대해 Apache Knox를 구성하십시오. 자세한 정보는 **Apache Knox 구성** 절을 참조하십시오.
   a. {knox}/data/services 아래에 analyticserver/3.2.1.0 폴더 계층 구조를 작성하십시오.
   b. rewrite.xml 및 service.xml 파일을 다음 Analytic Server 위치에서

      /opt/ibm/spss/analyticserver/3.2/ae_wlpserver/usr/servers/aeserver/configuration/knox/analyticserver/

      다음 Knox 서버 노드로 복사해야 합니다.

      {knox}/data/services/analyticserver/3.2.1.0
   c. Knox *.jar 파일을 다음 Analytic Server 호스트에서

      /opt/ibm/spss/analyticserver/3.2/ae_wlpserver/usr/servers/aeserver/apps/AE_BOOT.war/WEB-INF/lib/com.ibm.spss.knox_0.6-*.jar

      다음 Knox ext 디렉토리로 복사하십시오.

      {knox}/ext
   d. 다음 예와 일치하도록 {knox}/conf/topologies의 default.xml 파일을 업데이트하십시오.

      참고: 파일이 없으면 작성해야 합니다.

```
<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>

   <!--other service-->
   <service>
      <role>ANALYTICSERVER</role>
      <!--replace the {analyticserver-host} and {analyticserver-port} with real value-->
      <url>http://{analyticserver-host}:{analyticserver-port}/analyticserver</url>
      <role>ANALYTICSERVER_WS</role>
      <url>ws://{analyticserver-host}:{analyticserver-port}/analyticserver</url>
   </service>

</topology>
```

참고: 기본적으로 WebSocket 기능은 사용 안함으로 설정되어 있습니다. /conf/gateway-site.xml 파일에서 gateway.websocket.feature.enabled 특성을 true로 변경하여 사용으로 설정할 수 있습니다.

5. {knox}/bin/knoxcli.sh를 실행하십시오.
6. {knox}/bin/ldap.sh start를 실행하십시오.

   참고: 스크립트가 포트 33389를 사용합니다. 포트가 현재 사용 중이 아닌지 확인하십시오.

7. {knox}/bin/gateway.sh start를 실행하십시오.

   참고: 스크립트가 포트 8443을 사용합니다. 포트가 현재 사용 중이 아닌지 확인하십시오.

8. 설치를 확인하십시오.
   a. Knox URL에서 Analytic Server에 대해 curl 명령을 실행하십시오.

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

문제 해결

문제: Analytic Server가 설치 후에 Knox에서 작동하지 않습니다.

해결 방법: Knox를 중지하고 {knox}/data/deployments/* 아래의 파일을 모두 제거한 다음 Knox를 다시 시작하십시오.

문제: Knox를 통해 Analytic Server에 로그인할 수 없습니다.

해결 방법: {knox}/conf/users.ldif에서 사용자를 확인하십시오. 기존 사용자를 업데이트하거나 새 Analytic Server 사용자를 추가하십시오. Knox 사용자 프린시펄 및 신임 정보가 Analytic Server 사용자와 일치해야 합니다.

Apache Knox를 사용하는 Analytic Server의 URL 구조

Knox를 사용하는 Analytic Server 사용자 인터페이스 URL은 https://{knox-host}:{knox-port}/gateway/default/analyticserver/admin입니다.

- HTTPS 프로토콜 - 웹 브라우저에서 진행하려면 인증서를 수락해야 합니다.
- knox-host는 Knox 호스트입니다.
- knox-port는 Knox 포트 번호입니다.
- URI는 gateway/default/analyticserver입니다.

각 IBM SPSS Analytic Server 테넌트에 대한 별도의 YARN 큐 구성 - HDP

Yarn 큐 구성은 Spark 동적 자원 할당 기술을 사용하여 수행됩니다.

Hortonworks Data Platform 2.x

1. Ambari 사용자 인터페이스에서 **SPSS Analytic Server 서비스** > **구성** > **고급 analytics.cfg** 탭으로 이동하십시오.
2. **resource.pool.enabled** 값을 true로 변경하십시오.
3. **사용자 정의 analytics.cfg** 탭에서 다음 특성을 추가하십시오.

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

표 *8.* 사용자 정의 *analytics.cfg* 특성

특성	설명
config.folder.path	디렉토리에는 Spark 풀 특성 정보를 포함한 fairscheduler.xml 파일이 포함되어 있습니다. 파일은 필수이며 수동으로 구성되어야 합니다. 자세한 정보는 **fairscheduler.xml example** 절을 참조하십시오.
resource.pool.mapping	**Spark:** 테넌트를 fairscheduler.xml 파일에 정의된 풀에 맵핑합니다. 테넌트 쌍은 쉼표로 구분되어야 합니다(예: tenant1:test,tenant2:production). 풀을 지정하기 전에 풀이 fairscheduler.xml 파일에 구성되어 있는지 확인하십시오. **MapReduce:** 테넌트를 YARN 큐 관리자에 정의된 큐에 맵핑합니다. 테넌트 쌍은 쉼표로 구분되어야 합니다(예: tenant1:test,tenant2:production). 큐를 지정하기 전에 시스템이 큐로 구성되어 있고 큐에 작업을 제출하기 위해 액세스가 허용되는지 확인해야 합니다. **참고:** Spark 및 MapReduce 작업을 함께 실행하려면 테넌트 맵 값의 이름이 fairscheduler.xml 파일 및 YARN 큐 관리자에서 동일해야 합니다.

표 8. 사용자 정의 *analytics.cfg* 특성 (계속)

특성	설명
resource.pool.default	**Spark:** 기본 자원 풀을 정의합니다. 값은 default 또는 fairscheduler.xml 파일에 정의된 풀 이름일 수 있습니다. 테넌트가 구성되지 않은 경우(또는 올바르지 않게 구성된 경우) default 설정을 사용하십시오. **MapReduce:** 작업이 제출되는 기본 큐를 정의합니다.
spark.scheduler.mode=FAIR	**Spark:** 페어(Fair) 스케줄러를 사용으로 설정합니다. 이 특성은 변경하면 안됩니다.
spark.yarn.queue	**Spark:** 애플리케이션이 제출되는 YARN 큐의 이름입니다. YARN 큐 관리자에서 사용자 정의된 YARN 큐 이름을 지정할 수 있습니다.

4. 구성을 저장하고 Analytic Server 서비스를 다시 시작하십시오.

fairscheduler.xml 예제

fairscheduler.xml 파일에는 Spark 풀 특성 정보가 포함되어 있습니다. 파일은 필수이며 수동으로 구성되어야 합니다.

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

참조

자세한 정보는 다음 사이트를 참조하십시오.

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

Ambari에서 IBM SPSS Analytic Server 마이그레이션

Analytic Server는 데이터 및 구성 설정을 기존 Analytic Server 설치에서 새 설치로 마이그레이션할 수 있습니다. 마이그레이션은 동일한 클러스터 환경 또는 새 클러스터 환경에서 발생할 수 있습니다.

Analytic Server 3.1.2에서 동일한 서버 클러스터의 3.2.1로 마이그레이션

Analytic Server 3.1.2가 이미 설치되어 있는 경우 3.1.2 구성 설정을 동일한 서버 클러스터의 3.2.1 설치로 마이그레이션할 수 있습니다.

1. 이전 Analytic Server 버전(Analytic Server 3.1.2)에서 구성 설정을 수집하십시오.

a. {AS_ROOT}\tools\unzip configcollector.zip 아카이브를 펼치십시오(configcollector라는 새 폴더가 생성됨).

b. configcollector 폴더에서 configcollector.sh 스크립트를 실행하십시오. 생성되는 압축(ZIP) 파일 ASConfiguration_3.1.2.0.xxx.zip을 다른 폴더 위치(백업)로 복사하십시오.

2. 분석 루트를 이전 Analytic Server 3.1.2 버전 설치에서 새 위치로 백업하십시오.

   a. 분석 루트의 위치를 모르는 경우 **hadoop fs -ls**를 실행하십시오. 분석 루트에 대한 경로는 /user/as_user/analytic-root/analytic-workspace와 유사합니다. 여기서, as_user는 분석 루트를 소유한 사용자 ID입니다.

   b. **hadoop fs -copyToLocal** 및 **hadoop fs -copyFromLocal** 명령을 사용하여 이전 Analytic Server 버전 analytic-workspace 폴더를 새 위치(예: /user/as_user/analytic-root/AS31Location)로 복사하십시오.

3. 임베드된 Apache Directory Server를 사용하는 경우 써드파티 LDAP 클라이언트 도구로 현재 사용자/그룹 구성을 백업하십시오. Analytic Server 3.2.1가 설치된 후 백업 사용자/그룹 구성을 Apache Directory Server로 가져오십시오.

   참고: 외부 LADP 서버를 사용하는 경우 이 단계를 건너뛸 수 있습니다.

4. Ambari 콘솔을 열고 **Analytic Server 서비스**를 중지하십시오.

5. 이전 Analytic Server 버전(Analytic Server 3.1.2)을 설치 제거한 후 Analytic Server 3.2.1을 설치하십시오. 설치 지시사항은 5 페이지의 제 2 장 『Ambari 설치 및 구성』의 내용을 참조하십시오.

6. Ambari 콘솔을 열고 **Analytic Server 서비스**를 중지하십시오. (Ambari에서 **Analytic Metastore 서비스**가 실행 중인지 확인하십시오.)

7. 2단계에서 백업된 Analytic Server 3.1.2 분석 루트를 새 Analytic Server 버전 위치로 복사하십시오.

   a. 새로 설치된 Analytic Server 버전에서 analytic-workspace를 제거하십시오.

   b. 백업된 Analytic Server 3.1.2 분석 작업공간 폴더(/user/as_user/analytic-root/AS31Location)를 새 버전 위치(예: /user/as_user/analytic-root/analytic-workspace)로 복사하십시오. 분석 작업공간 소유자가 as_user로 정의되어 있는지 확인해야 합니다.

8. Zookeeper 상태를 지우십시오. Zookeeper bin 디렉토리(예: Hortonworks의 /usr/hdp/current/zookeeper-client)에서 다음 명령을 실행하십시오.

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

9. 1단계의 백업 아카이브 ASConfiguration_3.1.2.0.xxx.zip을 새 Analytic Server 버전 위치 (예: /opt/ibm/spss/analyticserver/3.2/)로 복사하십시오.

10. **migrationtool.sh** 스크립트를 실행하고 ASConfiguration_3.1.2.0.xxx.zip 아카이브 파일(구성 콜렉터를 통해 작성됨)의 경로를 인수로 전달하여 마이그레이션 도구를 실행하십시오. 예를 들어, 다음과 같습니다.

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

11. 모든 Analytic Server 클러스터 노드에서 ae_wlpserver/usr/servers/aeserver/configuration/config.properties 파일을 업데이트하십시오.
    - as_user에 대한 항목을 파일에 추가하십시오. 예를 들어, 다음과 같습니다.

      ```
      hdfs.user=as_user/host@REALM
      ```

      host는 config.properties 파일이 상주하는 Analytic Server 노드 호스트 이름과 일치해야 합니다.

      각 노드에 다른 hdfs.user 값이 있으며 각 호스트 값은 상주하는 Analytic Server 호스트와 일치해야 합니다.
12. Analytic Server 노드의 명령 쉘에서 다음 명령을 실행하십시오.

    ```
    hadoop fs -chmod -R 755 /user/as_user/analytic-root/analytic-workspace
    ```
13. Ambari 콘솔에서 **Analytic Server 서비스**를 시작하십시오.

Analytic Server 3.1.2에서 새 서버 클러스터의 3.2.1로 마이그레이션

Analytic Server 3.1.2가 이미 설치되어 있는 경우 3.1.2 구성 설정을 새 서버 클러스터의 3.2.1 설치로 마이그레이션할 수 있습니다.

1. 8 페이지의 『Ambari에 설치』의 지시사항에 따라 새 Analytic Server 버전을 설치하십시오.
2. 분석 작업공간을 이전 설치에서 새 설치로 복사하십시오.
   a. 분석 작업공간의 위치를 모르는 경우 hadoop fs -ls를 실행하십시오. 분석 작업공간에 대한 경로는 /user/as_user/analytic-root/analytic-workspace와 유사합니다. 여기서, as_user는 분석 작업공간을 소유한 사용자 ID입니다.
   b. 새 서버에서 analytic-workspace를 제거하십시오.
   c. hadoop fs -copyToLocal 및 hadoop fs -copyFromLocal을 사용하여 이전 서버의 분석 작업공간을 새 서버의 /user/as_user/analytic-root/analytic-workspace 폴더로 복사하십시오. (소유자가 as_user로 설정되어 있는지 확인하십시오.)
3. 임베드된 Apache Directory Server를 사용하는 경우 써드파티 LDAP 클라이언트 도구로 현재 사용자/그룹 구성을 백업하십시오. Analytic Server 3.2.1가 설치된 후 백업 사용자/그룹 구성을 Apache Directory Server로 가져오십시오.

   참고: 외부 LADP 서버를 사용하는 경우 이 단계를 건너뛸 수 있습니다.
4. 새 서버에서 Ambari 콘솔을 열고 Analytic Server 서비스를 중지하십시오. (Ambari의 경우, Analytic Metastore 서비스가 실행 중인지 확인하십시오.)
5. 이전 설치에서 구성 설정을 수집하십시오.
   a. 새 설치의 configcollector.zip 아카이브를 이전 설치의 {AS_ROOT}\tools에 복사하십시오.
   b. configcollector.zip의 사본을 추출하십시오. 이렇게 하면 이전 설치에 configcollector 서브디렉토리가 새로 작성됩니다.

c. {AS_ROOT}\tools\configcollector에서 **configcollector** 스크립트를 실행하여 이전 설치에서 구성 콜렉터 도구를 실행하십시오. 결과 압축(ZIP) 파일을 새 설치를 호스트하는 서버에 복사하십시오.

중요사항: 제공된 **configcollector** 스크립트는 최신 Analytic Server 버전과 호환되지 않을 수 있습니다. **configcollector** 스크립트에 문제점이 발생하면 IBM 기술 지원 담당자에게 문의하십시오.

6. Zookeeper 상태를 지우십시오. Zookeeper bin 디렉토리(예: Hortonworks의 /usr/hdp/current/zookeeper-client)에서 다음 명령을 실행하십시오.

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

7. **migrationtool** 스크립트를 실행하고 구성 콜렉터를 통해 작성된 압축 파일의 경로를 인수로 전달하여 마이그레이션 도구를 실행하십시오. 예제는 다음과 같습니다.

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

8. 모든 Analytic Server 노드에서 ae_wlpserver/usr/servers/aeserver/configuration/config.properties 파일을 업데이트하십시오. as_user에 대한 항목을 파일에 추가하십시오. 예를 들어, 다음과 같습니다.

```
hdfs.user=as_user/host@REALM
```

host는 config.properties 파일이 상주하는 Analytic Server 노드 호스트 이름과 일치해야 합니다. 각 노드에 다른 hdfs.user 값이 있으며 각 host 값은 상주하는 Analytic Server 호스트와 일치해야 합니다.

9. Analytic Server 노드의 명령 쉘에서 다음 명령을 실행하십시오.

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

10. Ambari 콘솔에서 Analytic Server 서비스를 시작하십시오.

참고: 기존 Analytic Server 설치와 함께 사용하도록 R을 구성한 경우, 새 Analytic Server 설치를 사용하여 이를 구성하는 단계를 따르십시오.

설치 제거

중요사항: Essentials for R이 설치되면 먼저 remove_R.sh 스크립트를 실행해야 합니다. Analytic Server를 설치 제거하기 전에 Essentials for R을 설치 제거하지 못하면 나중에 Essentials for R을 설치 제거할 수 없습니다. remove_R.sh 스크립트는 Analytic Server 설치 제거 시 제거됩니다. Essentials for R 설치 제거에 대한 정보는 45 페이지의 『Essentials for R 설치 제거』의 내용을 참조하십시오.

1. Analytic Metastore 호스트에서 다음 매개변수로 remove_as.sh 스크립트를 {AS_ROOT}/bin 디렉토리에서 실행하십시오.

u 필수입니다. Ambari 서버 관리자의 사용자 ID입니다.

p 필수입니다. Ambari 서버 관리자의 비밀번호입니다.

h 필수입니다. Ambari 서버 호스트 이름입니다.

x 필수입니다. Ambari 서버 포트입니다.

l 선택사항입니다. 보안 모드를 사용합니다.

예제는 다음과 같습니다.

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

Ambari 호스트 one.cluster가 포함된 클러스터에서 Analytic Server를 제거합니다.

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

보안 모드에서 Ambari 호스트 one.cluster가 포함된 클러스터에서 Analytic Server를 제거합니다.

참고: 이 작업으로 HDFS에서 Analytic Server 폴더가 제거됩니다.

참고: 이 작업으로 Analytic Server와 연관된 Db2 스키마가 제거되지는 않습니다. 스키마 수동 제거에 대한 정보는 Db2 문서를 참조하십시오.

Essentials for R 설치 제거

1. Essentials for R 호스트에서 다음 매개변수를 사용하여 remove_R.sh 스크립트를 {AS_ROOT}/bin 디렉토리에서 실행하십시오.

   u 필수입니다. Ambari 서버 관리자의 사용자 ID입니다.

   p 필수입니다. Ambari 서버 관리자의 비밀번호입니다.

   h 필수입니다. Ambari 서버 호스트 이름입니다.

   x 필수입니다. Ambari 서버 포트입니다.

   l 선택사항입니다. 보안 모드를 사용합니다.

   예제는 다음과 같습니다.

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

   Ambari 호스트 one.cluster가 포함된 클러스터에서 Essentials for R을 제거합니다.

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

   보안 모드로 Ambari 호스트 one.cluster가 포함된 클러스터에서 Essentials for R을 제거합니다.
2. Ambari 서버 서비스 디렉토리에서 R 서비스 디렉토리를 제거하십시오. 예를 들어, HDP 2.6에서 ESSENTIALR 디렉토리는 /var/lib/ambari-server/resources/stacks/HDP/2.6/services에 있습니다.
3. Ambari 콘솔에서 Essentials for R 서비스가 더 이상 존재하지 않는지 확인하십시오.

제 3 장 Cloudera 설치 및 구성

Cloudera 개요

Cloudera는 개방형 소스 Apache Hadoop 배포입니다. Apache Hadoop(CDH)을 포함한 Cloudera Distribution은 해당 기술의 엔터프라이즈급 배포를 목표로 합니다.

Analytic Server는 CDH 플랫폼에서 실행할 수 있습니다. CDH에는 대형 데이터 세트(주로 MapReduce 및 HDFS)의 신뢰할 수 있는 확장 가능한 분산 데이터 처리를 제공하는 Hadoop의 기본 핵심 요소와 하드웨어 및 기타 소프트웨어와의 통합, 고가용성 및 보안을 제공하는 기타 엔터프라이즈 지향 구성요소가 포함됩니다.

Cloudera 관련 필수조건

일반 필수조건 이외에도 다음 정보를 검토하십시오.

서비스

각 Analytic Server 호스트에 다음 인스턴스가 설치되어 있는지 확인하십시오.

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

다음 인스턴스는 해당 기능이 사용되는 경우에만 필수입니다.

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

메타데이터 리포지토리

Analytic Server 메타데이터 리포지토리로 DB2 및 MySQL을 사용할 수 있습니다. MySQL을 Analytic Server 메타데이터 리포지토리로 사용하려는 경우 49 페이지의 『Analytic Server에 대해 MySQL 구성』의 지시사항을 따르십시오.

Kerberos 사용 Cloudera 환경

Kerberos 사용 Cloudera 환경에서 Analytic Server를 설치할 계획인 경우 Kerberos가 Analytic Server와 호환 가능한 방식으로 올바르게 구성되었는지 확인해야 합니다.

다음 절의 내용은 Kerberos가 이미 설치된 Cloudera 환경에 적용됩니다. 다음 절은 Cloudera에 Analytic Server를 설치하기 전에 수행되어야 합니다. 절의 내용 중에 Kerberos 관련 용어(예: **`kinit`**, **`kadmin`**)가 포함되어 있으므로 사용자가 기본 Kerberos 인증 지식을 갖고 있다고 가정합니다.

참고: Analytic Server는 인증에 사용할 Kerberos 관련 값에 대해 HDFS 구성을 검사합니다.

Kerberos 인증

Analytic Server를 설치하기 전에 Kerberos 인증이 각 Cloudera 클러스터 노드에 구성되어 있는지 확인하십시오. 자세한 정보는 Cloudera 제품 문서에 있는 Cloudera 관리자에 인증 구성을 참조하십시오.

참고: 각 Cloudera 클러스터 노드에 Kerberos 인증을 구성한 후 Analytic Server를 설치하기 전에 **cloudera-scm-server** 및 **cloudera-scm-agent** 서비스를 다시 시작해야 합니다. 모든 클러스터 노드에서 **cloudera-scm-agent** 서비스를 다시 시작해야 합니다.

Kerberos에서 필수 계정 작성

1. Analytic Server에 대한 액세스 권한을 제공할 모든 사용자를 위해 Kerberos 사용자 리포지토리의 계정을 작성하십시오.
2. LDAP 서버에서 동일한 계정(이전 단계의)을 작성하십시오.
3. 모든 Analytic Server 노드 및 Hadoop 노드 각각에서 이전 단계에서 작성한 각 사용자의 OS 사용자 계정을 작성하십시오.
   - 모든 시스템에서 이러한 사용자의 UID가 일치하는지 확인하십시오. 이 `kinit` 명령 사용을 테스트하여 각 계정에 로그인할 수 있습니다.
   - UID가 **작업 제출용 최소 사용자 ID** Yarn 설정을 준수하는지 확인하십시오. 이는 `container-executor.cfg`에서 **min.user.id** 설정입니다. 예를 들어, **min.user.id**가 1000이면 작성된 각 사용자 계정의 UID가 1000 이상이어야 합니다.
4. Analytic Server 관리자에 대해 HDFS에 사용자 홈 폴더를 작성하십시오. 폴더 권한은 `777`로 설정되고, 소유자는 `admin`으로 정의되고, 사용자 그룹은 `hdfs`로 설정되어야 합니다. 굵게 표시된 다음 예제를 참조하십시오.

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

Found 9 items

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

5. HCatalog 데이터 소스를 사용하려고 계획하고 Analytic Server가 Hive Metastore와 다른 시스템에 설치되면 HDFS에서 Hive 클라이언트를 위장해야 합니다.
   a. Cloudera Manager에서 HDFS 서비스의 구성 탭으로 이동하십시오.

참고: 다음 설정은 이미 설정된 경우 **구성** 탭에 표시되지 않을 수 있습니다. 이 경우 검색을 실행하여 찾으십시오.

b. * 값 또는 Analytic Server에 로그인할 수 있는 모든 사용자가 포함된 그룹을 포함하도록 **hadoop.proxyuser.hive.groups** 설정을 편집하십시오.

c. * 값 또는 Analytic Server의 모든 인스턴스 및 Hive metastore가 서비스로 설치된 호스트 목록을 포함하도록 **hadoop.proxyuser.hive.groups** 설정을 편집하십시오.

d. HDFS 서비스를 다시 시작하십시오.

이러한 단계가 수행되고 Analytic Server가 설치되면 Analytic Server가 자동으로 Kerberos를 구성합니다.

Kerberos 위장 사용

위장을 사용하면 스레드를 소유한 프로세스의 보안 컨텍스트와 다른 보안 컨텍스트에서 스레드를 실행할 수 있습니다. 예를 들어, 위장은 Hadoop 작업에 대해 표준 Analytic Server 사용자(as_user) 이외의 사용자로 실행할 수 있는 방법을 제공합니다. Kerberos 위장을 사용하려면 다음과 같이 수행하십시오.

1. Cloudera Manager를 열고 **core-site.xml에 대한 클러스터 범위 고급 구성 스니펫(안전 밸브)** 영역에서 다음 특성을 추가하거나 업데이트하십시오. **HDFS(서버 범위)** > **구성** 탭에 있습니다.
   - **이름:** hadoop.proxyuser.as_user.hosts
   - **값:** *
   - **이름:** hadoop.proxyuser.as_user.groups
   - **값:** *

   참고: core-site.xml 설정은 Hadoop 구성에 적용됩니다(Analytic Server 아님).
2. Analytic Server 노드의 명령 쉘에서 다음 명령을 실행하십시오.

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

Analytic Server에 대해 MySQL 구성

Cloudera Manager에서 IBM SPSS Analytic Server를 구성하려면 MySQL 서버 데이터베이스를 설치하고 구성해야 합니다.

1. MySQL 데이터베이스가 저장된 노드의 명령 창에서 다음 명령을 실행하십시오.

   ```
   yum install mysql-server
   ```

   참고: SuSE Linux의 경우 zypper install mysql을 사용하십시오.
2. 각 Cloudera 클러스터 노드의 명령 창에서 다음 명령을 실행하십시오.

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

   참고: SuSE Linux의 경우 sudo zypper install mysql-connector-java를 사용하십시오.

3. Analytic Server가 MySQL 데이터베이스에 액세스할 때 사용하는 Analytic Server 데이터베이스 이름, 데이터베이스 사용자 이름 및 데이터베이스 비밀번호를 확인하고 메모해 두십시오.
4. 52 페이지의 『Cloudera에 설치』의 지시사항에 따라 Analytic Server를 설치하십시오.
5. /opt/cloudera/parcels/AnalyticServer/bin/add_mysql_user.sh 스크립트를 Cloudera에서 관리하는 서버 중 하나에서 MySQL 데이터베이스가 설치된 노드로 복사하십시오. 특정 구성에 적합한 매개변수와 함께 스크립트를 실행하십시오. 예를 들어, 다음과 같습니다.

   ```
   ./add_mysql_user.sh -u <database_user_name> -p <database_password> -d
   <database_name>
   ```

   참고: a -r <dbRootPassword) 매개변수는 데이터베이스가 보안 모드로 실행되는 경우(루트 사용자 비밀번호가 설정됨) 필수입니다.

   -r <dbUserPassword> 및 -t <dbUserName> 매개변수는 데이터베이스가 root 이외의 사용자 이름을 사용하여 보안 모드로 실행 중인 경우 필수입니다.

설치 사전 검사 및 사후 검사 도구 - Cloudera

도구 위치 및 필수조건

Analytic Server 서비스를 설치하기 전에 Analytic Server 서비스의 일부가 될 모든 노드에서 사전 검사 도구를 실행하여 Linux 환경이 Analytic Server를 설치할 준비가 되었는지 확인하십시오.

사전 검사 도구가 설치의 일부로 자동 호출됩니다. 도구는 각 호스트에서 설치를 실행하기 전에 각 Analytic Server 노드를 검사합니다. 또한 각 노드에서 사전 검사 도구를 수동으로 호출할 수 있으며, 이 도구로 서비스가 설치되기 전에 시스템을 유효성 검증할 수 있습니다.

자체 추출 Analytic Server 2진 파일을 실행한 후 사전 검사 도구는 다음 디렉토리에 위치합니다.

- **Cloudera**

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

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

참고: Cloudera Manager의 Parcels 페이지에서 실행 가능한 2진 파일을 실행한 후 Analytic Server를 배포(**다운로드** > **배포**)하고 활성화할 때까지 tools 디렉토리에서 사전 검사 도구를 사용할 수 없습니다.

Analytic Server 설치 후에는 사후 검사 도구가 다음 디렉토리에 위치합니다.

- **Cloudera**

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

이러한 도구는 루트로 실행되어야 하며 Python 2.6.X 이상이 필요합니다.

사전 검사 도구가 실패를 보고하는 경우, Analytic Server 설치를 계속 수행하기 전에 해당 실패를 처리해야 합니다.

사전 검사 도구 실행

자동

Analytic Server가 Cloudera Manager 콘솔을 통해 서비스로 설치되면 Analytic Server 설치의 일부로 사전 검사 도구를 자동 호출할 수 있습니다. Cloudera Manager 관리자의 사용자 이름 및 비밀번호를 수동으로 입력해야 합니다.

그림 *4. Cloudera Manager* 관리자 설정

수동

각 클러스터 노드에서 사전 검사 도구를 수동으로 호출할 수 있습니다.

다음 사전 검사 예에서는 myclouderahost.ibm.com:7180에서 실행 중인 Cloudera 클러스터 MyCluster를 검사하고 로그인 신임 정보 admin:admin을 사용합니다.

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

참고:

- as_host 값은 IP 주소 또는 완전한 도메인 이름을 사용하여 제공되어야 합니다.
- 비밀번호 인수가 생략되면 비밀번호에 대한 도구가 프롬프트됩니다.
- precheck.py 명령에는 --h 인수를 사용하여 표시되는 사용법 도움말(python ./precheck.py --help)이 포함됩니다.

- --cluster 인수는 선택적입니다. (현재 클러스터는 --cluster가 사용되지 않을 때 식별됩니다.)

사전 검사 도구가 검사를 실행할 때 각 검사의 상태가 명령 창에 표시됩니다. 실패가 발생하면 로그 파일에서 세부사항을 볼 수 있습니다. 정확한 로그 파일 위치는 명령 창에 표시됩니다. 로그 파일은 추가 지원이 필요할 때 IBM 기술 지원에 제공될 수 있습니다.

사후 검사 도구 실행

사후 검사 도구는 Analytic Server가 적절히 실행 중인지, 단순 작업을 처리할 수 있는지 확인합니다. 다음 사후 검사 예는 SSL을 사용하는 myanalyticserverhost.ibm.com:9443에서 실행 중인 Analytic Server를 검사하고 로그인 신임 정보 admin:ibmspss를 사용합니다.

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

Knox가 Analytic Server와 함께 사용되는 경우, 명령은 다음과 같습니다.

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

단일 검사를 수행하려면 다음 명령을 사용하십시오.

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

참고:

- 비밀번호 인수가 생략되면 비밀번호에 대한 도구가 프롬프트됩니다.
- postcheck.py 명령에는 --h 인수를 사용하여 표시되는 사용법 도움말(python ./postcheck.py --help)이 포함됩니다.

사후 검사 도구가 검사를 실행할 때 각 검사의 상태가 명령 창에 표시됩니다. 실패가 발생하면 로그 파일에서 세부사항을 볼 수 있습니다. 정확한 로그 파일 위치는 명령 창에 표시됩니다. 로그 파일은 추가 지원이 필요할 때 IBM 기술 지원에 제공될 수 있습니다.

Cloudera에 설치

다음 단계에서는 Cloudera Manager에 IBM SPSS Analytic Server를 수동으로 설치하는 프로세스에 대해 설명합니다.

Analytic Server 3.2.1

온라인 설치

1. IBM Passport Advantage® 웹 사이트로 이동한 다음 사용 중인 스택, 스택 버전 및 하드웨어 아키텍처에 해당하는 자체 추출 2진 파일을 Cloudera 클러스터 내의 호스트로 다운로드하십시오. 사용 가능한 Cloudera 2진은 다음과 같습니다.

표 *9. Analytic Server* 자체 추출 *2*진 파일

설명	2진 파일 이름
IBM SPSS Analytic Server 3.2.1 for Cloudera 5.11, 5.12, 5.13, 5.14, 5.15, 6.0 및 6.1 Ubuntu 영어	`spss_as-3.2.1.0-cdh5.11-6.1-ubun.bin`
IBM SPSS Analytic Server 3.2.1 for Cloudera 5.11, 5.12, 5.13, 5.14, 5.15, 6.0 및 6.1 Linux x86-64 영어	`spss_as-3.2.1.0-cdh5.11-6.1-lx86.bin`

2. Cloudera Manager 마스터 클러스터 노드에서 Cloudera 자체 추출 `*.bin` 설치 프로그램을 실행하십시오. 설치 프롬프트에 따라 라이센스 계약에 동의하고 기본 CSD 설치 디렉토리를 유지하십시오.

   참고: CSD 디렉토리를 기본 위치에서 변경한 경우 다른 CSD 디렉토리를 지정해야 합니다.

3. 설치가 완료되면 다음 명령을 사용하여 Cloudera Manager를 다시 시작하십시오.

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

4. Cloudera Manager 인터페이스(예: 기본 로그인 신임 정보 `admin/admin`을 사용할 경우 `http://${CM_HOST}:7180/cmf/login`)를 열고 **원격 Parcel 리포지토리 URL**(**호스트** > **Parcel** > **구성 클릭**에 있음)을 새로 고친 다음 URL이 올바른지 확인하십시오. 예를 들어, 다음과 같습니다.

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

   참고: 사용자의 특정 요구사항에 적합하도록 **Parcel 업데이트 빈도** 및 **원격 Parcel 리포지토리 URL**을 업데이트할 수 있습니다.

5. Cloudera Manager가 Parcel 파일을 새로 고치면(**새 Parcel 확인**을 클릭하여 Parcel 파일을 수동으로 새로 고칠 수 있음) **AnalyticServer** Parcel 상태가 **원격에서 사용 가능**으로 설정됩니다.
6. **다운로드** > **배포** > **활성화**를 선택하십시오. **AnalyticServer** Parcel 상태가 **배포됨, 활성화됨**으로 업데이트됩니다.
7. Cloudera Manager에서 Analytic Server를 서비스로 추가하고 Analytic Server 배치 위치를 결정하십시오. 서비스 추가 마법사에 다음 정보를 제공해야 합니다.

   참고: 서비스 추가 마법사가 서비스 작성 프로세스의 각 단계 중 전체 진행률을 표시하며, 서비스가 클러스터에 성공적으로 설치 및 구성되면 최종 확인 메시지를 제공합니다.

   - Analytic Server Metastore 호스트 이름
   - Analytic Server Metastore 데이터베이스 이름
   - Analytic Server Metastore 사용자 이름
   - Analytic Server Metastore 비밀번호

   Analytic Server 메타데이터 리포지토리로의 MySQL

   - Analytic Server Metastore 드라이버 클래스: `com.mysql.jdbc.Driver`
   - Analytic Server Metastore 리포지토리 URL: `jdbc:mysql://${MySQL_DB}/{DBName}?createDatabaseIfNotExist=true`

     `{MySQL_DB}`는 MySQL이 설치된 서버의 호스트 이름입니다.

Analytic Server 메타데이터 리포지토리로의 DB2

- Analytic Server Metastore 드라이버 클래스: com.ibm.db2.jcc.DB2Driver
- Analytic Server Metastore 리포지토리 URL: jdbc:db2://{Db2_HOST}:{PORT}/{DBName}:currentSchema={SchemaName};

  {Db2_HOST}는 DB2가 설치된 서버의 호스트 이름입니다.

  {PORT}는 DB2가 청취하는 포트입니다.

  {SchemaName}은 사용 가능하지만 사용되지 않는 스키마입니다.

  입력할 값을 모르는 경우 DB2 관리자와 함께 작업하십시오.

LDAP 구성

Analytic Server는 LDAP 서버를 사용하여 사용자 및 그룹을 저장하고 인증합니다. Analytic Server 설치 중에 필수 LDAP 구성 정보를 제공하십시오.

표 *10. LDAP* 구성 설정

LDAP 설정	설명
as.ldap.type	LDAP 유형. 값은 ads, ad 또는 openladp일 수 있습니다. • ads - Apache Directory Server(기본 설정) • ad - Microsoft Active Directory • openladp - OpenLDAP
as.ldap.host	LDAP 호스트
as.ldap.port	LDAP 포트 번호
as.ldap.binddn	LDAP 바인드 DN
as.ldap.bindpassword	LDAP 바인드 DN 비밀번호
as.ldap.basedn	LDAP 기본 DN
as.ldap.filter	LDAP 사용자 및 그룹 필터 규칙 **참고:** 이 값에 새로 막대(|) 문자가 포함된 경우 문자는 백슬래시 문자(예: \\\|)로 이스케이프 처리되어야 합니다.
as.ldap.ssl.enabled	Analytic Server와 LDAP 간에 통신하는 데 SSL을 사용하는지 여부를 지정합니다. 값은 true 또는 false일 수 있습니다.
as.ldap.ssl.reference	LDAP SSL 참조 ID
as.ldap.ssl.content	LDAP SSL 구성

- 기본적으로 as.ldap.type은 ads로 설정되고 기타 관련 설정에는 기본 설정이 포함됩니다. 예외는 as.ldap.bindpassword 설정에 비밀번호를 제공해야 한다는 것입니다. Analytic Server는 구성 설정을 사용하여 ADS(Apache Directory Server)를 설치하고 서버 초기화를 실행합니다. 기본 ADS 프로파일에는 admin의 사용자와 admin의 비밀번호가 포함됩니다. Analytic Server 콘솔을 통해 관리를 수행하거나 <Analytic Root>/bin 폴더에 있는 importUser.sh 스크립트를 통해 XML 파일에서 사용자 및 그룹 정보를 가져올 수 있습니다.

- 외부 LDAP 서버(예: Microsoft Active Directory 또는 OpenLDAP)를 사용할 계획인 경우 실제 LDAP 값에 따라 구성 설정을 정의해야 합니다. 자세한 정보는 Liberty에서 LDAP 사용자 레지스트리 구성을 참조하십시오.
- Analytic Server가 설치된 후 LDAP 구성을 변경할 수 있습니다(예: Apache Directory Server에서 OpenLDAP로 변경). 그러나 처음에 Microsoft Active Directory 또는 OpenLDAP로 시작하고 나중에 Apache Directory Server로 전환하는 경우 Analytic Server는 설치 중에 Apache Directory Server를 설치하지 않습니다. 초기 Analytic Server 설치 중에 Apache Directory Server가 선택된 경우 Apache Directory Server만 설치됩니다.

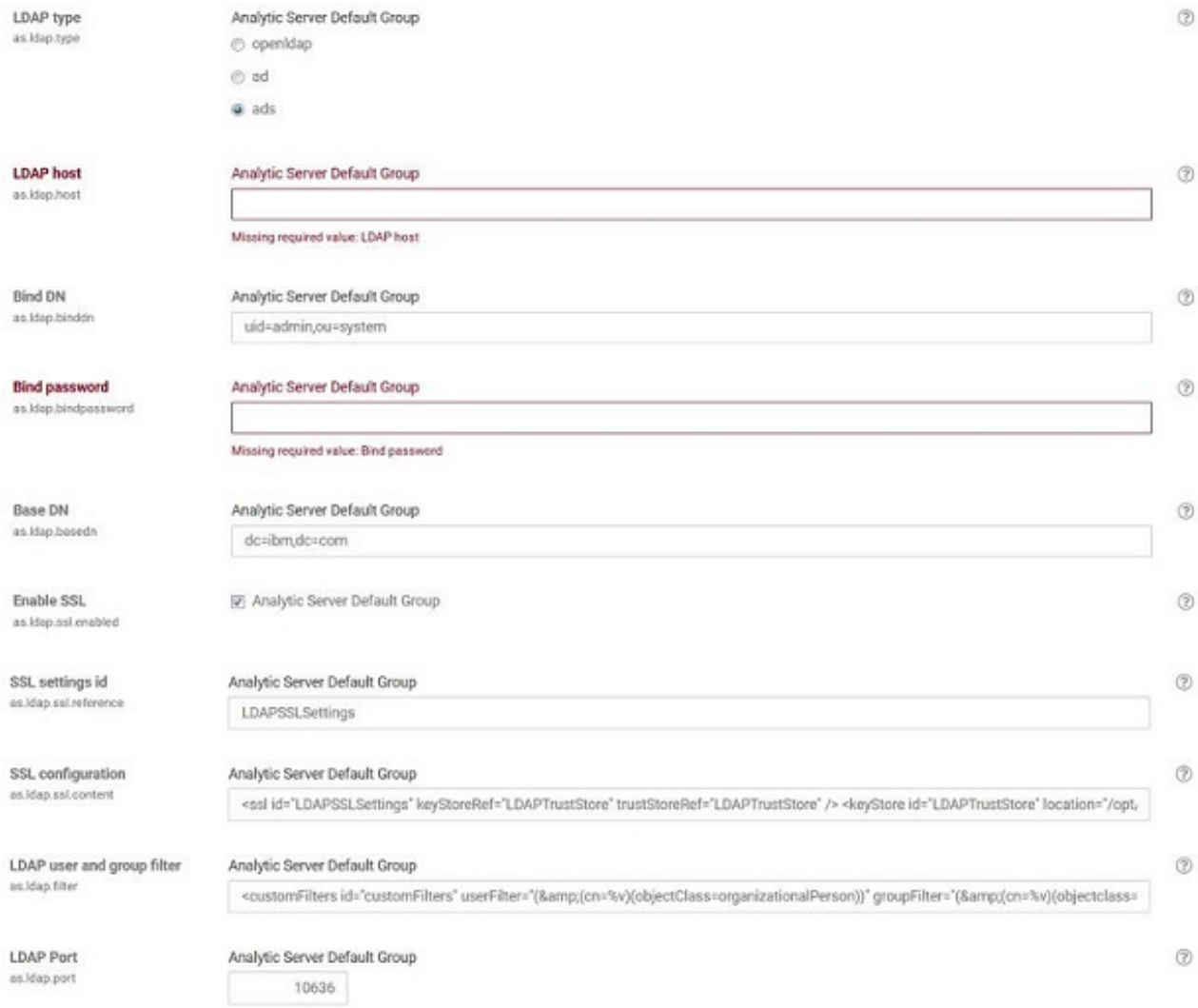

그림 *5. LDAP* 구성 설정의 예

8. Kerberos 사용 Cloudera 환경에서 Analytic Server를 설치하는 경우 서비스 추가 마법사에서 다음 설정도 구성해야 합니다.

   참고: Analytic Server는 인증에 사용할 Kerberos 관련 값에 대해 HDFS 구성을 검사합니다.

- Analytic Server 콘솔에 로그인할 때 Kerberos 인증을 사용으로 설정할 경우 **Analytic Server 보안** 설정으로 Kerberos를 선택하십시오. **Kerberos**가 **Analytic Server 보안** 설정으로 선택된 경우 Analytic Server 콘솔은 Kerberos 로그인 모드를 기본으로 설정합니다.
- Kerberos 사용 데이터베이스에 연결할 경우 **Analytic Server 데이터베이스 데이터 소스 연결 방법** 설정으로 Kerberos를 선택하십시오. **Kerberos**가 **Analytic Server 데이터베이스 데이터 소스 연결 방법** 설정으로 선택된 경우 Analytic Server 콘솔은 데이터베이스에 연결할 때 Kerberos 모드를 사용합니다.
- **Kerberos 영역 이름** 및 **KDC 호스트** 설정은 필수입니다. **Kerberos 영역 이름**(**as.kdc.realms**) 및 **KDC 호스트**(**kdcserver**) 값은 Kerberos KDC(Key Distribution Center) 서버의 krb5.conf 파일에 있습니다.

  다중 영역 이름은 쉼표로 구분된 경우에 지원됩니다. 지정된 Kerberos 영역 이름은 사용자 이름과 일치하며 사용자 이름과 연관됩니다. 예를 들어 사용자 이름 UserOne@us.ibm.com 및 UserTwo@eu.ibm.com은 us.ibm.com,eu.ibm.com 영역과 일치합니다.

  둘 이상의 영역이 **Kerberos 영역 이름**으로 지정된 경우 Kerberos 교차 영역 신뢰를 구성해야 합니다. Analytic Server 콘솔 로그인 프롬프트에 입력한 사용자 이름이 영역 이름 접미부 없이 입력됩니다. 따라서 다중 영역이 지정된 경우 **영역** 드롭 다운 목록이 사용자에게 표시되며 사용자는 이 목록에서 영역을 선택할 수 있습니다.

  참고: 영역이 한 개만 지정된 경우 Analytic Server에 로그인할 때 **영역** 드롭 다운 목록이 사용자에게 표시되지 않습니다.

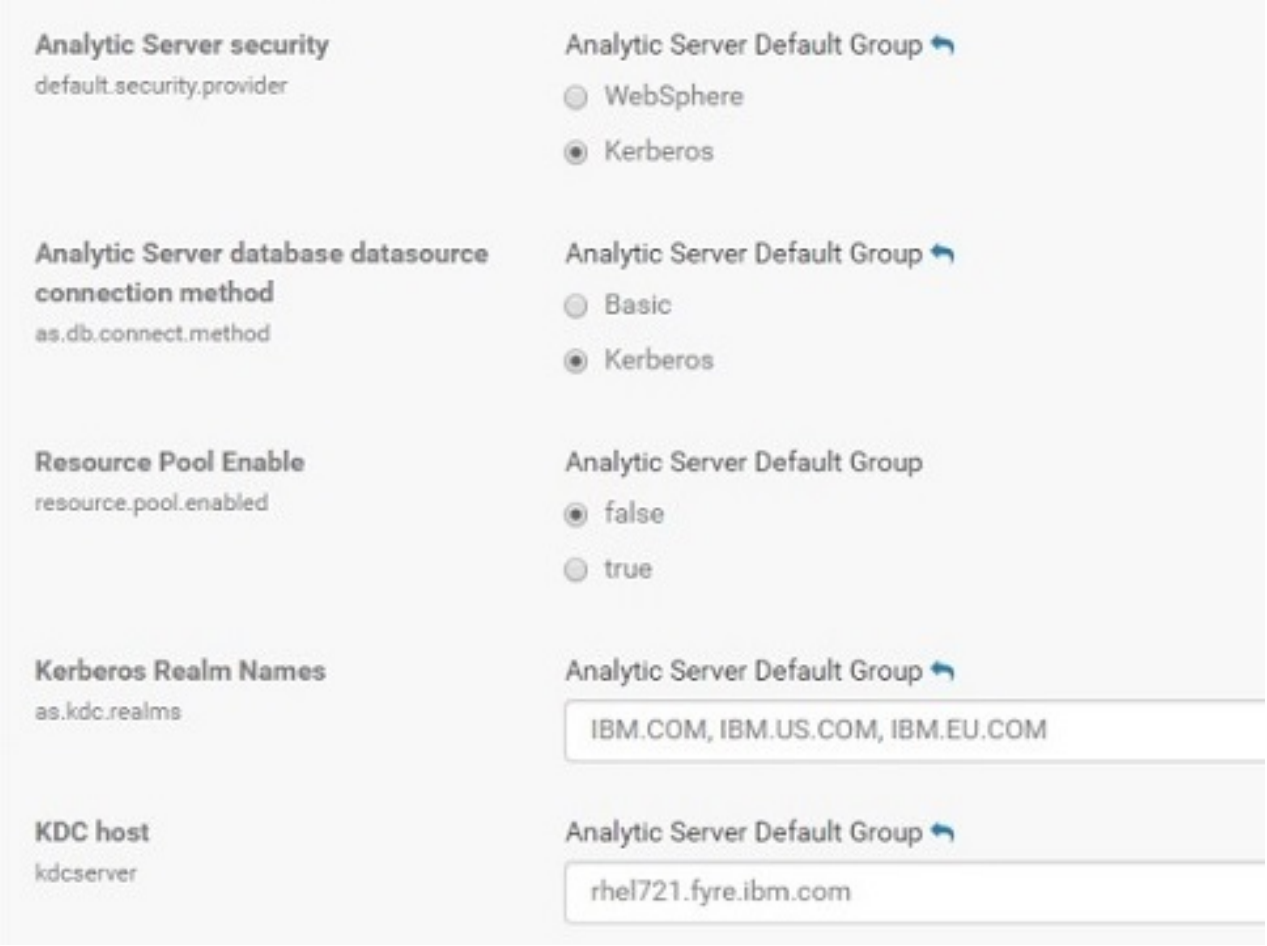

그림 *6. Kerberos* 설정 예

참고:

- **Analytic Server 보안** 및 **Analytic Server 데이터베이스 데이터 소스 연결 방법** 설정은 IBM SPSS Modeler 클라이언트 및 Analytic Server 콘솔 인증에 적용됩니다.
- **Analytic Server 데이터베이스 데이터 소스 연결 방법**이 `Kerberos`로 설정되는 경우 대상 데이터베이스도 Kerberos 사용인지 확인해야 합니다.
- **Analytic Server 보안** 및 **Analytic Server 데이터베이스 데이터 소스 연결 방법** 설정은 Hadoop 클러스터의 Kerberos 인증을 구성하지 않습니다. 자세한 정보는 "Kerberos 위장 사용" 절을 참조하십시오.
- 로그인 시 Kerberos 인증을 사용으로 설정할 경우 유효한 Kerberos 클라이언트로 IBM SPSS Modeler 클라이언트를 배포해야 합니다. 이는 Kerberos KDC(Key Distribution Center) 서버에서 **`addprinc`** 명령을 사용하여 수행됩니다. 자세한 정보는 IBM SPSS Modeler 문서를 참조하십시오.

Kerberos 사용 Cloudera 환경에서 Analytic Server를 설치하는 경우 Kerberos에 필요한 계정을 작성하고 Kerberos 위장도 사용으로 설정해야 합니다. 추가 정보는 60 페이지의 『Kerberos 구성』의 내용을 참조하십시오.

참고: Analytic Server가 성공적으로 설치되면 Cloudera Manager에서 Analytic Server 서비스 페이지의 조치 목록에서 **Analytic Server Metastore 작성**을 클릭하지 마십시오. Metastore를 작성하면 기존 메타데이터 리포지토리를 덮어씁니다.

오프라인 설치

오프라인 설치 단계는 온라인 단계와 동일합니다. 단, 사용자의 특정 운영 체제에 적합한 Parcel 파일과 메타데이터를 수동으로 다운로드해야 합니다.

RedHat Linux의 경우 다음 파일이 필요합니다.

- AnalyticServer-3.2.1.0-el7.parcel
- AnalyticServer-3.2.1.0-el7.parcel.sha
- manifest.json

SuSE Linux의 경우 다음 파일이 필요합니다.

- AnalyticServer-3.2.1.0-sles11.parcel
- AnalyticServer-3.2.1.0-sles11.parcel.sha
- manifest.json

  또는

- AnalyticServer-3.2.1.0-sles12.parcel
- AnalyticServer-3.2.1.0-sles12.parcel.sha

Ubuntu Linux 14.04의 경우 다음 파일이 필요합니다.

- AnalyticServer-3.2.1.0-trusty.parcel
- AnalyticServer-3.2.1.0-trusty.parcel.sha

Ubuntu Linux 16.04의 경우 다음 파일이 필요합니다.

- AnalyticServer-3.2.1.0-xenial.parcel
- AnalyticServer-3.2.1.0-xenial.parcel.sha

1. Cloudera Manager 마스터 클러스터 노드에서 Cloudera 자체 추출 `*.bin` 설치 프로그램을 다운로드하여 실행하십시오. 설치 프롬프트에 따라 라이센스 계약에 동의하고 기본 `CSD` 설치 디렉토리를 유지하십시오.

   참고: `CSD` 디렉토리가 기본 위치와 다른 경우 다른 CSD 디렉토리를 지정해야 합니다.
2. 필수 Parcel 및 메타데이터 파일을 Cloudera Manager 마스터 클러스터 노드의 로컬 Cloudera `repo` 경로로 복사하십시오. 기본 경로는 `/opt/cloudera/parcel-repo`입니다. 경로는 Cloudera Manager 사용자 인터페이스에서 구성할 수 있습니다.
3. 다음 명령을 사용하여 Cloudera Manager를 다시 시작하십시오.

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

Cloudera Manager가 Parcel을 새로 고치면 **AnalyticServer** Parcel이 **다운로드됨**으로 표시됩니다. **새 Parcel 확인**을 클릭하면 강제로 새로 고칠 수 있습니다.

4. **배포** > **활성화**를 클릭하십시오.

   AnalyticServer Parcel이 배포됨 및 활성화됨으로 표시됩니다.

5. Cloudera Manager에서 서비스로 Analytic Server를 추가하십시오. 자세한 정보는 "온라인 설치" 절의 7단계 및 8단계를 참조하십시오.

Cloudera 구성

설치 후 Cloudera Manager를 통해 Analytic Server를 선택적으로 구성하고 관리할 수 있습니다.

참고: Analytic Server 파일 경로에는 다음 규칙을 사용합니다.

- {AS_ROOT}는 Analytic Server가 배포된 위치를 나타냅니다(예: `/opt/cloudera/parcels/AnalyticServer`).
- {AS_SERVER_ROOT}는 구성, 로그 및 서버 파일의 위치를 나타냅니다(예: `/opt/cloudera/parcels/AnalyticServer/ae_wlpserver/usr/servers/aeserver`).
- {AS_HOME}은 Analytic Server에서 루트 폴더로 사용되는 HDFS의 위치를 나타냅니다(예: `/user/as_user/analytic-root`).

보안

IBM SPSS Modeler `options.cfg` 파일의 기본 **`tenant_id`** 값은 **`ibm`**입니다. Analytic Server 콘솔에서 테넌트를 볼 수 있습니다. 테넌트 관리에 대한 세부사항은 *IBM SPSS Analytic Server* 관리자 안내서를 참조하십시오.

LDAP 레지스트리 구성

Analytic Server 설치 중에 LDAP이 구성됩니다. Analytic Server 설치 후에 다른 LDAP 서버 방법으로 변경할 수 있습니다.

참고: Analytic Server에서 LDAP에 대한 지원은 WebSphere Liberty에 의해 제어됩니다. 자세한 정보는 Liberty에서 LDAP 사용자 레지스트리 구성을 참조하십시오.

Analytic Server에서 LDAP으로의 SSL(Secure Socket Layer) 연결 구성

1. 각 Analytic Server 시스템에 Analytic Server 사용자로 로그인하고 SSL 인증서를 위한 공통 디렉토리를 작성하십시오.

   참고: Cloudera에서 Analytic Server 사용자는 항상 as_user이며, 이는 변경할 수 없습니다.

2. 키 저장소 및 신뢰 저장소 파일을 모든 Analytic Server 시스템의 공통 디렉토리에 복사하십시오. 또한 신뢰 저장소에 LDAP 클라이언트 CA 인증서를 추가하십시오. 다음은 샘플 지시사항입니다.

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

참고: JAVA_HOME은 Analytic Server 시작에 사용되는 동일한 JRE입니다.

3. {AS_ROOT}/ae_wlpserver/bin에 있는 securityUtility 도구를 사용하여 비밀번호를 명확하지 않은 값으로 인코딩할 수 있습니다. 예제는 다음과 같습니다.

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

4. Cloudera Manager에 로그인한 다음 Analytic Server 구성 설정 **ssl_cfg**를 올바른 SSL 구성 설정으로 업데이트하십시오. 예제는 다음과 같습니다.

```
<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="/>
```

참고: 키 및 신뢰 저장소 파일의 절대 경로를 사용하십시오.

5. Analytic Server 구성 설정 **security_cfg**를 올바른 LDAP 구성 설정으로 업데이트하십시오. 예를 들어 **ldapRegistry** 요소에서, **sslEnabled** 속성을 true로, **sslRef** 속성을 defaultSSLConfig로 설정하십시오.

Kerberos 구성

Analytic Server는 Cloudera에서 Kerberos를 지원합니다. 다음 스크립트는 Kerberos가 Analytic Server와 호환 가능한 방식으로 올바르게 구성되었는지 확인하기 위한 구성 설정을 제공합니다.

참고: Analytic Server는 인증에 사용할 Kerberos 관련 값에 대해 HDFS 구성을 검사합니다.

Analytic Server 및 Kerberos 설정

Kerberos 사용 Cloudera 환경에서 Analytic Server를 설치하는 경우 다음 설정을 유지하십시오.

- Analytic Server 콘솔에 로그인할 때 Kerberos 인증을 사용으로 설정할 경우 **Analytic Server 보안** 설정으로 Kerberos를 선택하십시오. **Kerberos**가 **Analytic Server 보안** 설정으로 선택된 경우 Analytic Server 콘솔은 Kerberos 로그인 모드를 기본으로 설정합니다.
- Kerberos 사용 데이터베이스에 연결할 경우 **Analytic Server 데이터베이스 데이터 소스 연결 방법** 설정으로 Kerberos를 선택하십시오. **Kerberos**가 **Analytic Server 데이터베이스 데이터 소스 연결 방법** 설정으로 선택된 경우 Analytic Server 콘솔은 데이터베이스에 연결할 때 Kerberos 모드를 사용합니다.
- **Kerberos 영역 이름** 및 **KDC 호스트** 설정은 필수입니다. **Kerberos 영역 이름**(**as.kdc.realms**) 및 **KDC 호스트**(**kdcserver**) 값은 Kerberos KDC(Key Distribution Center) 서버의 krb5.conf 파일에 있습니다.

다중 영역 이름은 쉼표로 구분된 경우에 지원됩니다. 지정된 Kerberos 영역 이름은 사용자 이름과 일치하며 사용자 이름과 연관됩니다. 예를 들어 사용자 이름 `UserOne@us.ibm.com` 및 `UserTwo@eu.ibm.com`은 `us.ibm.com,eu.ibm.com` 영역과 일치합니다.

둘 이상의 영역이 **Kerberos 영역 이름**으로 지정된 경우 Kerberos 교차 영역 신뢰를 구성해야 합니다. Analytic Server 콘솔 로그인 프롬프트에 입력한 사용자 이름이 영역 이름 접미부 없이 입력됩니다. 따라서 다중 영역이 지정된 경우 **영역** 드롭 다운 목록이 사용자에게 표시되며 사용자는 이 목록에서 영역을 선택할 수 있습니다.

참고: 영역이 한 개만 지정된 경우 Analytic Server에 로그인할 때 **영역** 드롭 다운 목록이 사용자에게 표시되지 않습니다.

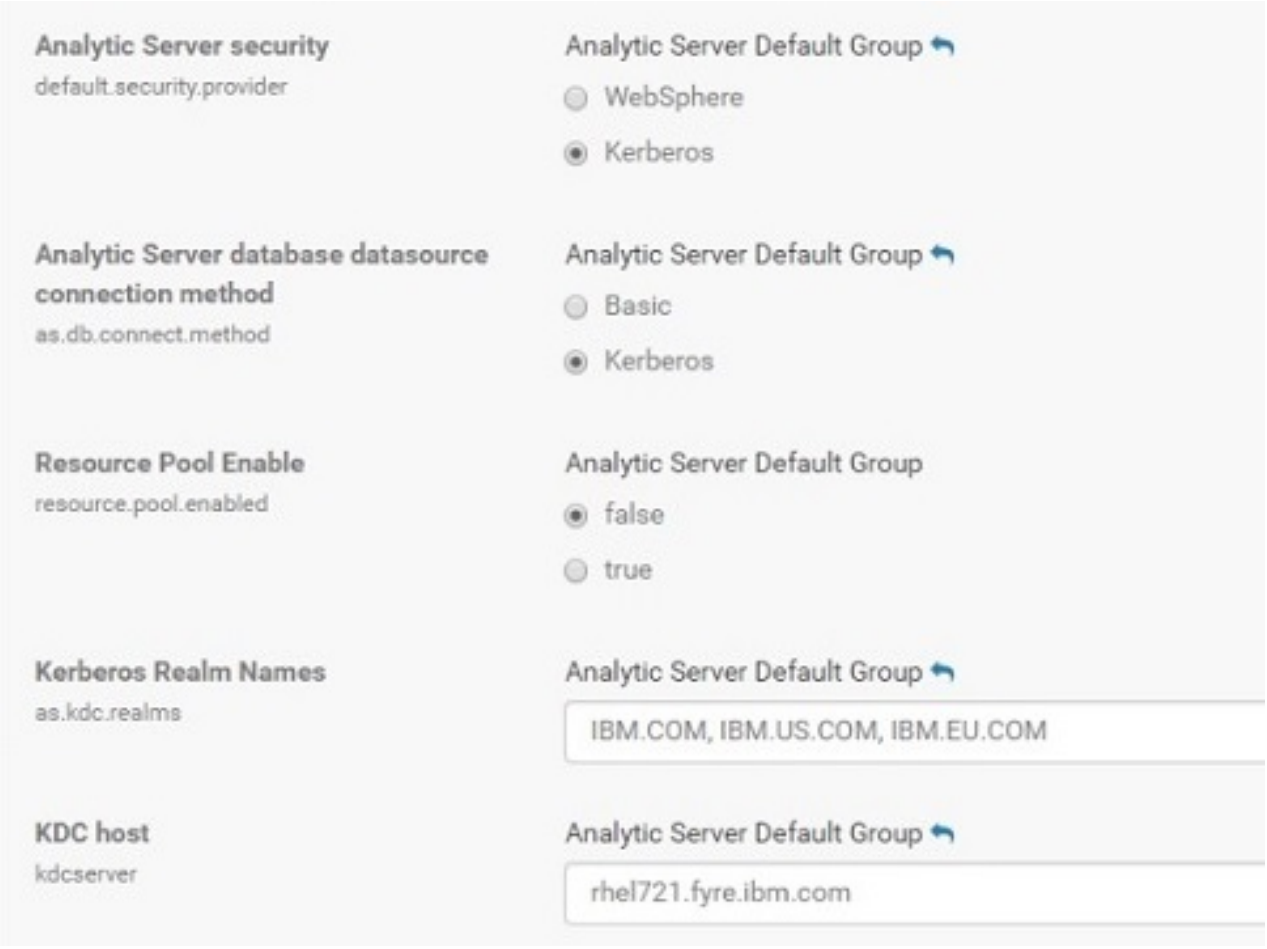

그림 *7. Kerberos* 설정 예

참고:

- **Analytic Server 보안** 및 **Analytic Server 데이터베이스 데이터 소스 연결 방법** 설정은 IBM SPSS Modeler 클라이언트 및 Analytic Server 콘솔 인증에 적용됩니다.
- **Analytic Server 데이터베이스 데이터 소스 연결 방법**이 `Kerberos`로 설정되는 경우 대상 데이터베이스도 Kerberos 사용인지 확인해야 합니다.

– **Analytic Server 보안** 및 **Analytic Server 데이터베이스 데이터 소스 연결 방법** 설정은 Hadoop 클러스터의 Kerberos 인증을 구성하지 않습니다. 자세한 정보는 "Kerberos 위장 사용" 절을 참조하십시오.

– 로그인 시 Kerberos 인증을 사용으로 설정할 경우 유효한 Kerberos 클라이언트로 IBM SPSS Modeler 클라이언트를 배포해야 합니다. 이는 Kerberos KDC(Key Distribution Center) 서버에서 **addprinc** 명령을 사용하여 수행됩니다. 자세한 정보는 IBM SPSS Modeler 문서를 참조하십시오.

Kerberos에서 필수 계정 작성

1. Analytic Server에 대한 액세스 권한을 제공할 모든 사용자를 위해 Kerberos 사용자 리포지토리의 계정을 작성하십시오.
2. LDAP 서버에서 동일한 계정(이전 단계의)을 작성하십시오.
3. 모든 Analytic Server 노드 및 Hadoop 노드 각각에서 이전 단계에서 작성한 각 사용자의 OS 사용자 계정을 작성하십시오.
   - 모든 시스템에서 이러한 사용자의 UID가 일치하는지 확인하십시오. 이 `kinit` 명령 사용을 테스트하여 각 계정에 로그인할 수 있습니다.
   - UID가 **작업 제출용 최소 사용자 ID** Yarn 설정을 준수하는지 확인하십시오. 이는 `container-executor.cfg`에서 **min.user.id** 설정입니다. 예를 들어, **min.user.id**가 1000이면 작성된 각 사용자 계정의 UID가 1000 이상이어야 합니다.
4. Analytic Server 관리자에 대해 HDFS에 사용자 홈 폴더를 작성하십시오. 폴더 권한은 `777`로 설정되고, 소유자는 `admin`으로 정의되고, 사용자 그룹은 `hdfs`로 설정되어야 합니다. 굵게 표시된 다음 예제를 참조하십시오.

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

Found 9 items

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

5. HCatalog 데이터 소스를 사용하려고 계획하고 Analytic Server가 Hive Metastore와 다른 시스템에 설치되면 HDFS에서 Hive 클라이언트를 위장해야 합니다.
   a. Cloudera Manager에서 HDFS 서비스의 구성 탭으로 이동하십시오.

      참고: 다음 설정은 이미 설정된 경우 **구성** 탭에 표시되지 않을 수 있습니다. 이 경우 검색을 실행하여 찾으십시오.

b. * 값 또는 Analytic Server에 로그인할 수 있는 모든 사용자가 포함된 그룹을 포함하도록 **hadoop.proxyuser.hive.groups** 설정을 편집하십시오.

c. * 값 또는 Analytic Server의 모든 인스턴스 및 Hive metastore가 서비스로 설치된 호스트 목록을 포함하도록 **hadoop.proxyuser.hive.groups** 설정을 편집하십시오.

d. HDFS 서비스를 다시 시작하십시오.

이러한 단계가 수행되고 Analytic Server가 설치되면 Analytic Server가 자동으로 Kerberos를 구성합니다.

Kerberos 위장 사용

위장을 사용하면 스레드를 소유한 프로세스의 보안 컨텍스트와 다른 보안 컨텍스트에서 스레드를 실행할 수 있습니다. 예를 들어, 위장은 Hadoop 작업에 대해 표준 Analytic Server 사용자(as_user) 이외의 사용자로 실행할 수 있는 방법을 제공합니다. Kerberos 위장을 사용하려면 다음과 같이 수행하십시오.

1. Cloudera Manager를 열고 **core-site.xml에 대한 클러스터 범위 고급 구성 스니펫(안전 밸브)** 영역에서 다음 특성을 추가하거나 업데이트하십시오. **HDFS(서버 범위)** > **구성** 탭에 있습니다.
   - **이름:** hadoop.proxyuser.as_user.hosts
   - **값:** *
   - **이름:** hadoop.proxyuser.as_user.groups
   - **값:** *

   참고: core-site.xml 설정은 Hadoop 구성에 적용됩니다(Analytic Server 아님).
2. Analytic Server 노드의 명령 쉘에서 다음 명령을 실행하십시오.

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

Kerberos를 통한 싱글 사인온(SSO)용 HAProxy 구성

1. HAProxy 문서 안내서에 따라서 HAProxy 구성하고 시작하십시오. http://www.haproxy.org/#docs
2. HAProxy 호스트의 Kerberos 원칙(HTTP/<proxyHostname>@<realm>) 및 키탭 파일을 작성하십시오. 여기서 <proxyHostname>은 HAProxy 호스트의 전체 이름이고 <realm>은 Kerberos 영역입니다.
3. 키탭 파일을 각 Analytic Server 호스트에 /etc/security/keytabs/spnego_proxy.service.keytab으로 복사하십시오.
4. 각 Analytic Server 호스트에서 이 파일에 대한 권한을 업데이트하십시오. 예제는 다음과 같습니다.

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

5. Cloudera Manager를 열고 Analytic Server의 **analyticserver-conf/config.properties에 대한 Analytic Server 고급 구성 스니펫(안전 밸브)** 영역에서 다음 특성을 추가하거나 업데이트하십시오.

```
web.authentication.kerberos.keytab=/etc/security/keytabs/spnego_proxy.service.keytab
web.authentication.kerberos.principal=HTTP/<proxy machine full name>@<realm>
```

6. 구성을 저장하고 모든 Analytic Server 서비스를 Cloudera Manager에서 다시 시작하십시오.
7. 사용자의 브라우저가 Kerberos를 사용하도록 구성하십시오.

이제 사용자가 IBM SPSS Analytic Server 로그인 화면에서 **싱글 사인온 로그인** 옵션을 사용하여 Analytic Server에 로그인할 수 있습니다.

Kerberos 사용 안함

1. Cloudera Manager 콘솔에서 Kerberos를 사용 안함으로 설정하십시오.
2. Analytic Server 서비스를 중지하십시오.
3. **analyticserver-conf/config.properties에 대한 Analytic Server 고급 구성 스니펫(안전 밸브)** 영역에서 다음 설정을 제거하십시오.

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

4. **변경사항 저장**을 클릭하고 Analytic Server 서비스를 다시 시작하십시오.

Analytic Server 콘솔에 대한 SSL(Secure Socket Layer) 연결 사용

기본적으로 Analytic Server는 자체 서명된 인증서를 생성하여 SSL(Secure Socket Layer)을 사용합니다. 이렇게 하면 자체 서명된 인증서를 채택하여 보안 포트를 통해 Analytic Server 콘솔에 액세스할 수 있습니다. HTTPS 액세스의 보안을 강화하려면 써드파티 벤더 인증서를 설치해야 합니다.

써드파티 벤더 인증서를 설치하려면 다음 단계를 수행하십시오.

1. 써드파티 벤더 키 저장소 및 신뢰 저장소 인증서를 모든 Analytic Server 노드의 동일한 디렉토리에 복사하십시오(예: `/home/as_user/security`).

   참고: Analytic Server 사용자에게 이 디렉토리에 대한 읽기 액세스 권한이 있어야 합니다.
2. Cloudera Manager에서 Analytic Server 서비스의 구성 탭으로 이동하십시오.
3. **`ssl_cfg`** 매개변수를 편집하십시오.

```
<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>"/>
```

다음과 같이 바꾸십시오.

- <KEYSTORE-LOCATION>을 키 저장소의 절대 위치로(예: /home/as_user/security/mykey.jks)
- <TRUSTSTORE-LOCATION>을 신뢰 저장소의 절대 위치로(예: /home/as_user/security/mytrust.jks)
- <TYPE>을 인증서 유형으로(예: JKS, PKCS12 등)
- <PASSWORD>를 Base64 암호화 형식의 암호화된 비밀번호로. 인코딩의 경우 securityUtility를 사용할 수 있습니다(예: {AS_ROOT}/ae_wlpserver/bin/securityUtility encode <password>).

자체 서명된 인증서를 생성하려는 경우 securityUtility를 사용할 수 있습니다(예: {AS_ROOT}/ae_wlpserver/bin/securityUtility createSSLCertificate --server=myserver --password=mypassword --validity=365 --subject=CN=mycompany,O=myOrg,C=myCountry). securityUtility 및 기타 SSL 설정에 대한 자세한 정보는 WebSphere Liberty Profile 문서를 참조하십시오.

참고: CN 값에 대해 적절한 호스트 도메인 이름을 제공해야 합니다.

4. **변경사항 저장**을 클릭하고 Analytic Server 서비스를 다시 시작하십시오.

SSL을 통해 Apache Hive와 통신

SSL 연결을 통해 Apache Hive와 통신하려면 hive.properties 파일을 업데이트해야 합니다. 또는 Apache Hive 환경이 고가용성에 대해 사용으로 설정된 경우 기본 Analytic Server 데이터 소스 페이지에 있는 고가용성 매개변수를 선택할 수 있습니다.

hive.properties 파일 업데이트

1. hive.properties 파일을 여십시오. 이 파일은 /opt/cloudera/parcels/AnalyticServer-3.2.1.0/ae_wlpserver/usr/servers/aeserver/configuration/database에 있습니다.
2. 다음 행을 찾으십시오.

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

3. 다음과 같이 **굵게** 표시된 정보를 추가하여 행을 업데이트하십시오.

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

4. hive.properties 파일을 저장하십시오.

Essentials for R에 대한 지원 사용

Analytic Server에서는 R 모델 스코어링 및 R 스크립트 실행을 지원합니다.

Cloudera Manager에서 Analytic Server를 설치한 후 Essentials for R을 설치하려면 다음을 수행하십시오.

1. Essentials for R에 대한 서버 환경을 프로비저닝하십시오. 자세한 정보는 26 페이지의 『Essentials for R에 대한 지원 사용』에서 1단계를 참조하십시오.
2. IBM SPSS Modeler Essentials for R RPM의 자체 추출 아카이브(BIN)를 다운로드하십시오. Essentials for R은 다운로드할 수 있습니다(https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=swg-tspssp). 스택, 스택 버전 및 하드웨어 아키텍처에 대한 파일을 선택하십시오.
3. Cloudera Manager 서버 호스트에서 자체 추출 아카이브를 루트 또는 sudo 사용자로 실행하십시오. 구성된 리포지토리에서 다음 패키지를 설치하거나 사용할 수 있어야 합니다.
   - Red Hat Linux: gcc-gfortran, zip, gcc-c++
   - SUSE Linux: gcc-fortran, zip, gcc-c++
   - Ubuntu Linux: gcc-fortran, zip, gcc-c++
4. 자체 추출 설치 프로그램이 다음 태스크를 수행합니다.
   a. 필요한 라이센스를 표시하고 이러한 라이센스에 동의하는지 묻는 프롬프트를 설치 프로그램에 표시합니다.
   b. R 소스 위치를 입력할지 아니면 기본 위치를 계속 사용할지 묻는 프롬프트를 설치 프로그램에 표시합니다. 설치되는 기본 R 버전은 3.3.2입니다. 다른 버전을 설치하려면 다음을 수행하십시오.
      - 온라인 설치: 필요한 R 버전 아카이브의 URL을 제공하십시오. 예를 들어 R 2.15.3의 경우 https://cran.r-project.org/src/base/R-2/R-2.15.3.tar.gz입니다.
      - 오프라인 설치: 필요한 R 버전 아카이브를 다운로드한 다음 Cloudera Manager 서버 호스트로 복사하십시오. 아카이브의 이름을 변경하지 마십시오. 기본 아카이브 이름은 `R-x.x.x.tar.gz`입니다. 복사한 R 아카이브의 URL을 제공하십시오(예: `file://<R_archive_directory>/R-x.x.x.tar.gz`). `R-2.15.3.tar.gz` 아카이브를 다운로드하여 `/root`로 복사한 경우 URL은 `file:///root/R-2.15.3.tar.gz`입니다.

      참고: 다른 R 버전은 https://cran.r-project.org/src/base/에 있습니다.
   c. R에 필요한 패키지를 설치합니다.
   d. R 및 Essentials for R 플러그인을 다운로드하고 설치합니다.
   e. Parcel 및 `parcel.sha` 파일을 작성하고 `/opt/cloudera/parcel-repo`로 복사하십시오. 위치가 변경된 경우 올바른 위치를 변경하십시오.
5. 설치가 완료되면 Cloudera Manager에서 **Essentials for R** Parcel을 배포하고 활성화하십시오. Parcel 목록을 새로 고치려면 **새 Parcel 확인**을 클릭하십시오.
6. Analytic Server 서비스가 이미 설치된 경우 다음을 수행하십시오.
   a. 서비스를 중지하십시오.
   b. Analytic Server 2진을 새로 고치십시오.

c. 서비스를 시작하여 Essentials for R 설치를 완료하십시오.

7. Analytic Server 서비스가 설치되지 않은 경우 설치를 계속 진행하십시오.

참고: 모든 Analytic Server 호스트에 적합한 아카이브(`zip` 및 `unzip`) 패키지가 설치되어 있어야 합니다.

관계형 데이터베이스 소스 사용

사용자가 각 Analytic Server 호스트에서 공유 디렉토리에 JDBC 드라이버를 제공하면 Analytic Server가 관계형 데이터베이스 소스를 사용할 수 있습니다. 기본적으로 이 디렉토리는 `/usr/share/jdbc` 입니다.

공유 디렉토리를 변경하려면 다음 단계를 수행하십시오.

1. Cloudera Manager에서 Analytic Server 서비스의 구성 탭으로 이동하십시오.
2. **`jdbc.drivers.location`**에 JDBC 드라이버의 공유 디렉토리 경로를 지정하십시오.
3. **변경사항 저장**을 클릭하십시오.
4. **조치** 드롭 다운에서 **중지**를 선택하여 Analytic Server 서비스를 중지하십시오.
5. **조치** 드롭 다운에서 **Analytic Server 2진 새로 고치기**를 선택하십시오.
6. **조치** 드롭 다운에서 **시작**을 선택하여 Analytic Server 서비스를 시작하십시오.

표 *11.* 지원되는 데이터베이스

데이터베이스	지원되는 버전	JDBC 드라이버 jar	벤더
Amazon Redshift	8.0.2 이상	`RedshiftJDBC41-1.1.6.1006.jar` 이상	Amazon
Apache Impala	2.5.5 이상이 설치된 JDBC 4	`ImpalaJDBC4.jar`, `commons-codec-*.jar`, `commons-logging-*.jar`, `httpclient-*.jar`, `httpcore-*.jar`, `log4j-*.jar`, `libthrift-*.jar`, `libfb303-*.jar`, `slf4j-api-*.jar`, `ql.jar`, `zookeeper-*.jar`, `TCLIServiceClient.jar`	Apache
DashDB	Bluemix Service	`db2jcc.jar`	IBM
Linux, UNIX 및 Windows용 Db2	11.1, 10.5, 10.1, 9.7	`db2jcc.jar`	IBM
Db2 z/OS	11, 10	`db2jcc.jar`, `db2_license_cisuz.jar`	IBM
Greenplum	5.x	postgresql.jar	Greenplum
Hive	1.1	`hive-jdbc-*.jar`	Apache
MySQL	5.6, 5.7	mysql-connector-java-commercial-5.1.25-bin.jar	MySQL
Netezza	7, 6.x	`nzjdbc.jar`	IBM

표 *11.* 지원되는 데이터베이스 *(*계속*)*

데이터베이스	지원되는 버전	JDBC 드라이버 jar	벤더
Oracle	12c, 11g R2(11.2)	ojdbc6.jar, orai18n.jar	Oracle
SQL Server	2014, 2012, 2008 R2	sqljdbc4.jar	Microsoft
Teradata	15, 15.1	tdgssconfig.jar, terajdbc4.jar	Teradata

참고

- Analytic Server를 설치하기 전에 Redshift 데이터 소스를 작성한 경우 Redshift 데이터 소스를 사용하려면 다음 단계를 수행해야 합니다.
  1. Analytic Server 콘솔에서 Redshift 데이터 소스를 여십시오.
  2. Redshift 데이터베이스 데이터 소스를 선택하십시오.
  3. Redshift 서버 주소를 입력하십시오.
  4. 데이터베이스 이름과 사용자 이름을 입력하십시오. 비밀번호는 자동으로 채워져야 합니다.
  5. 데이터베이스 테이블을 선택하십시오.

HCatalog 데이터 소스 사용

Analytic Server는 Hive/HCatalog를 통해 많은 데이터 소스에 대한 지원을 제공합니다. 일부 소스에는 수동 구성 단계가 필요합니다.

1. 데이터 소스를 사용하는 데 필요한 JAR 파일을 수집하십시오. 세부사항은 다음 절을 참조하십시오.
2. 이 JAR 파일을 각 Analytic Server 노드의 {HIVE_HOME}/auxlib 디렉토리 및 /usr/share/hive 디렉토리에 추가하십시오.
3. Hive Metastore 서비스를 다시 시작하십시오.
4. Analytic Server 서비스의 인스턴스를 각각 다시 시작하십시오.

참고:

Analytic Server HCatalog 데이터 소스를 통해 HBase 데이터에 액세스하는 경우 액세스하는 사용자는 HBase 테이블에 대한 읽기 권한이 있어야 합니다.

- Kerberos 이외의 환경에서 Analytic Server는 as_user를 사용하여 HBase에 액세스합니다(as_user는 HBase에 대한 읽기 권한이 있어야 함).
- Kerberos 환경에서 as_user 및 로그인 사용자는 모두 HBase 테이블에 대한 읽기 권한이 있어야 합니다.

NoSQL 데이터베이스

Analytic Server는 벤더에서 사용할 수 있는 Hive 저장 공간 핸들러의 모든 NoSQL 데이터베이스를 지원합니다.

추가 단계 없이 Apache HBase 및 Apache Accumulo에 대한 지원을 사용할 수 있습니다.

기타 NoSQL 데이터베이스의 경우 데이터베이스 벤더에 문의하여 저장 공간 핸들러 및 관련 jar를 확보하십시오.

파일 기반 Hive 테이블

Analytic Server는 사용 가능한 기본 제공 또는 사용자 정의 Hive SerDe(직렬 변환기-병렬 변환기)의 파일 기반 Hive 테이블을 지원합니다.

XML 파일 처리를 위한 Hive XML SerDe는 http://search.maven.org/#search%7Cga%7C1%7Chivexmlserde의 Maven 중앙 리포지토리에 있습니다.

MapReduce v2 작업

analyticserver-conf/config.properties에 대한 Analytic Server 고급 구성 스니펫(안전 밸브) 영역에서 **preferred.mapreduce** 설정을 사용하여 MapReduce 작업이 처리되는 방식을 제어하십시오.

표 *12. analyticserver-conf/config.properties*에 대한 *Analytic Server* 고급 구성 스니펫*(*안전 밸브*)*

특성	설명
preferred.mapreduce	MapReduce 작업이 실행되는 방식을 제어합니다. 유효한 값은 다음과 같습니다. • spark • m3r • hadoop 예: preferred.mapreduce=spark

Apache Spark

Spark(버전 1.5 이상)를 사용하려면 Analytic Server 설치 중에 spark.version을 선택해야 합니다.

1. Cloudera Manager를 열고 **Analytic Server Spark 버전** 영역에서 적절한 spark.version(예: 없음, 1.x 또는 2.x)을 선택하십시오.

   참고: Spark 1.x를 사용하는 경우 **analyticserver-conf/config.properties에 대한 Analytic Server 고급 구성 스니펫(안전 밸브)** 영역에서 다음 행도 추가해야 합니다.

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

2. 구성을 저장하십시오.

Apache Impala 구성

Apache Impala는 Analytic Server 데이터베이스 데이터 소스 또는 HCatalog 데이터 소스에 대해 Cloudera에서 실행 중일 때 지원됩니다(Impala에서의 SSL 사용 가능 여부에 상관없음).

Apache Impala 데이터의 데이터베이스 데이터 소스 작성

1. 기본 Analytic Server **데이터 소스** 페이지에서, **새로 작성**을 클릭하여 새 데이터 소스를 작성하십시오. 새 데이터 소스 대화 상자가 표시됩니다.
2. **새 데이터 소스** 필드에 적합한 이름을 입력하고 데이터베이스를 **컨텐츠 유형** 값으로 선택한 후 **확인**을 클릭하십시오.
3. **데이터베이스 선택사항** 섹션을 열고 다음 정보를 입력하십시오.

   데이터베이스:

   드롭 다운 메뉴에서 **Impala**를 선택하십시오.

   서버 주소:

   Impala 디먼을 호스트하는 서버의 URL을 입력하십시오. 완전한 도메인 이름은 Kerberos가 Analytic Server에 대해 사용으로 설정된 경우 필수입니다.

   서버 포트:

   Impala 데이터베이스가 청취하는 포트 번호를 입력하십시오.

   데이터베이스 이름:

   연결하려는 데이터베이스의 이름을 입력하십시오.

   사용자 이름:

   권한 있는 사용자 이름을 입력하여 Impala 데이터베이스에 로그인하십시오.

   비밀번호:

   적합한 사용자 이름과 비밀번호를 입력하십시오.

   테이블 이름:

   사용하려는 데이터베이스의 테이블 이름을 입력하십시오. **선택**을 클릭하여 수동으로 파일을 선택하십시오.

   최대 동시 읽기 수:

   데이터 소스에 지정된 테이블에서 읽을 수 있도록 Analytic Server에서 데이터베이스로 전송할 수 있는 병렬 쿼리 수의 한도를 입력하십시오.
4. 필수 정보를 입력한 후 **저장**을 클릭하십시오.

Apache Impala 데이터의 HCatalog 데이터 소스 작성

1. 기본 Analytic Server **데이터 소스** 페이지에서, **새로 작성**을 클릭하여 새 데이터 소스를 작성하십시오. 새 데이터 소스 대화 상자가 표시됩니다.
2. **새 데이터 소스** 필드에 적합한 이름을 입력하고 HCatalog를 **컨텐츠 유형** 값으로 선택한 후 **확인**을 클릭하십시오.
3. **데이터베이스 선택사항** 섹션을 열고 다음 정보를 입력하십시오.

   데이터베이스:

   드롭 다운 메뉴에서 **기본값**을 선택하십시오.

테이블 이름:

사용하려는 데이터베이스의 테이블 이름을 입력하십시오.

HCatalog 스키마

HCatalog 요소 옵션을 선택한 후 적합한 **HCatalog 필드 맵핑** 옵션을 선택하십시오.

4. 필수 정보를 입력한 후 **저장**을 클릭하십시오.

Apache Impala 사용 데이터에 연결

1. Cloudera Manager 콘솔에서 다음 Impala SSL 설정을 정의하십시오.

Impala에 TLS/SSL 사용 설정(client_services_ssl_enabled)

Impala(서비스 범위) 옵션을 선택하십시오.

Impala TLS/SSL 서버 인증서 파일(PEM 형식)(ssl_server_certificate)

자체 서명된 PEM 형식 인증서 위치 및 파일 이름을 입력하십시오(예: `/tmp/<user_name>/ssl/ll4200v21.crt`).

Impala TLS/SSL 서버 개인 키 파일(PEM 형식)(ssl_private_key)

PEM 형식의 개인 키, 위치 및 파일 이름을 입력하십시오(예: `/tmp/<user_name>/ssl/ll4200v21.key`).

2. Analytic Server 호스트에서, `*.crf` 파일(Impala SSL을 사용으로 설정하는 데 사용됨)을 `*.jks` 파일로 가져오십시오. cacerts 파일(예를 들어, `/etc/pki/java/cacerts`) 또는 임의의 기타 `*.jks` 파일일 수 있습니다.
3. Analytic Server 호스트에서, 다음 `jdbcurl` 키 값을 추가하여 Impala 구성 파일(`impala.properties`)을 업데이트하십시오.

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

참고: `*.jks` 파일(cacerts 이외에)이 사용되면 다음도 지정해야 합니다.

SSLTrustStore=<your_pks_file>;**SSLTrustStorePwd**=<password_for_pks_file>;

4. Cloudera Manager 콘솔에서 Analytic Server를 다시 시작하십시오.

Analytic Server가 사용하는 포트 변경

Analytic Server는 기본적으로 HTTP의 경우 9080 포트를, HTTPS의 경우 9443 포트를 사용합니다. 포트 설정을 변경하려면 다음 단계를 수행하십시오.

1. Cloudera Manager에서 Analytic Server 서비스의 구성 탭으로 이동하십시오.
2. **http.port** 및 **https.port** 매개변수에 각각 원하는 HTTP 및 HTTPS 포트를 지정하십시오.

참고: 이러한 매개변수를 표시하려면 필터 섹션에서 **포트 및 주소** 카테고리를 선택해야 할 수 있습니다.

3. **변경사항 저장**을 클릭하십시오.
4. Analytic Server 서비스를 다시 시작하십시오.

고가용성 Analytic Server

클러스터의 여러 노드에 서비스로 추가하여 Analytic Server의 가용성을 높일 수 있습니다.

1. Cloudera Manager에서 Analytic Server 서비스의 인스턴스 탭으로 이동하십시오.
2. **역할 인스턴스 추가**를 클릭하고 Analytic Server를 서비스로 추가할 호스트를 선택하십시오.

다중 클러스터 지원

다중 클러스터 기능은 IBM SPSS Analytic Server의 고가용성 기능에 대한 향상된 기능이며 다중 테넌트 환경에서 더 효율적으로 격리할 수 있습니다. 기본적으로 Ambari 또는 Cloudera Manager에서 Analytic Server 서비스를 설치하면 단일 분석 서버 클러스터가 정의됩니다.

클러스터 스펙은 Analytic Server 클러스터 멤버십을 정의합니다. 클러스터 스펙 수정은 XML 컨텐츠로(Ambari Analytic Server 구성의 `analytics-cluster` 필드에서 또는 Cloudera Manager의 `configuration/analytics-cluster.xml` 파일을 수동으로 편집하여) 수행됩니다. 다중 Analytic Server 클러스터를 구성하는 경우, 자체 로드 밸런서를 사용하여 각 Analytic Server 클러스터에 요청을 피드해야 합니다.

다중 클러스터 기능을 사용하면 한 테넌트에 대한 작업이 다른 테넌트의 클러스터에서 수행되는 작업에 부정적인 영향을 미치지 못하도록 할 수 있습니다. 고가용성 작업의 경우, 작업이 시작된 Analytic Server 클러스터의 범위 내에서만 작업 장애 복구가 발생할 수 있습니다. 다음 예는 다중 클러스터 XML 스펙을 제공합니다.

참고: Analytic Server는 서비스로 클러스터 내의 다중 노드에 추가함으로써 고가용성으로 만들 수 있습니다.

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

이전 예에서는 두 개의 로드 밸런서가 필요합니다. 한 개의 로드 밸런서가 `cluster1` 멤버(`one.cluster` 및 `two.cluster`)에 요청을 전송하고 다른 로드 밸런서가 `cluster2` 멤버(`three.cluster` 및 `four.cluster`)에 요청을 전송합니다.

다음 예는 단일 클러스터 XML 스펙(기본 구성)을 제공합니다.

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

이전 예에서는 구성된 클러스터 멤버가 두 개 이상인 경우를 처리하기 위해 단일 로드 밸런서가 필요합니다.

참고

- 싱글톤 클러스터만 **memberName** 요소에서의 와일드카드 사용을 지원합니다. 예를 들어, 클러스터 카디널리티 = "1"인 경우입니다. 카디널리티 요소에 대해 유효한 값은 1 및 1+입니다.
- **memberName**은 Analytic Server 역할이 지정된 호스트 이름과 동일한 방법으로 지정되어야 합니다.
- 모든 클러스터의 모든 서버는 클러스터 구성 변경이 적용된 후에 다시 시작되어야 합니다.
- Cloudera Manager에서는 모든 Analytic Server 노드에서 analytics-cluster.xml 파일을 수정 및 유지보수해야 합니다. 모든 노드가 동일한 컨텐츠를 포함하도록 유지보수되어야 합니다.

작은 데이터를 위한 JVM 옵션 최적화

작은(M3R) 작업을 실행할 때 시스템을 최적화하기 위해 JVM 특성을 편집할 수 있습니다.

Cloudera Manager에서 Analytic Server 서비스의 구성 탭에 있는 **Jvm 옵션(jvm.options)** 컨트롤을 표시하십시오. 다음 매개변수를 수정하여 Hadoop이 아니라 Analytic Server를 호스트하는 서버에서 실행되는 작업에 대한 힙 크기를 설정하십시오. 이는 작은(M3R) 작업을 실행하는 경우에 중요하며 시스템을 최적화하기 위해 해당 값을 사용하여 시험해야 합니다.

```
-Xms512M
-Xmx2048M
```

각 IBM SPSS Analytic Server 테넌트에 대한 별도의 YARN 큐 구성 - Cloudera

Yarn 큐 구성은 Spark 동적 자원 할당 기술을 사용하여 수행됩니다.

Cloudera 5.x

SPSS Analytic Server 서비스를 기존 클러스터에 추가하는 경우 다음 단계를 수행하십시오.

1. Cloudera Manager에서 **SPSS Analytic Server 서비스** > **구성**으로 이동하십시오.
2. **자원 풀 사용: resource.pool.enabled** 값을 true로 변경하십시오.
3. 다음 특성을 **Analytic Server 고급 구성** > **analyticserver-conf.config.properties**에 추가하십시오.

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

표 *13. analyticserver-conf.config.properties* 설정

특성	설명
config.folder.path	디렉토리에는 Spark 풀 특성 정보를 포함한 fairscheduler.xml 파일이 포함되어 있습니다. 파일은 필수이며 수동으로 구성되어야 합니다. 자세한 정보는 **fairscheduler.xml example** 절을 참조하십시오.

표 *13. analyticserver-conf.config.properties* 설정 *(계속)*

특성	설명
resource.pool.mapping	**Spark:** 테넌트를 fairscheduler.xml 파일에 정의된 풀에 맵핑합니다. 테넌트 쌍은 쉼표로 구분되어야 합니다(예: tenant1:test,tenant2:production). 풀을 지정하기 전에 풀이 fairscheduler.xml 파일에 구성되어 있는지 확인하십시오. **MapReduce:** 테넌트를 동적 자원 풀 구성에 정의된 큐에 맵핑합니다. 테넌트 쌍은 쉼표로 구분되어야 합니다(예: tenant1:test,tenant2:production). 큐를 지정하기 전에 시스템이 큐로 구성되어 있고 큐에 작업을 제출하기 위해 액세스가 허용되는지 확인해야 합니다. **참고:** Spark 및 MapReduce 작업을 함께 실행하려면 테넌트 맵 값의 이름이 fairscheduler.xml 파일 및 동적 자원 풀 구성에서 동일해야 합니다.
resource.pool.default	**Spark:** 기본 자원 풀을 정의합니다. 값은 default 또는 fairscheduler.xml 파일에 정의된 풀 이름일 수 있습니다. 테넌트가 구성되지 않은 경우(또는 올바르지 않게 구성된 경우) default 설정을 사용하십시오. **MapReduce:** 작업이 제출되는 기본 큐를 정의합니다.
spark.scheduler.mode=FAIR	**Spark:** 페어(Fair) 스케줄러를 사용으로 설정합니다. 이 특성은 변경하면 안됩니다.
spark.yarn.queue	**Spark:** 애플리케이션이 제출되는 YARN 큐의 이름입니다. 동적 자원 풀 구성에서 사용자 정의된 YARN 큐 이름을 지정할 수 있습니다.

4. 구성을 저장하고 Analytic Server 서비스를 다시 시작하십시오.

fairscheduler.xml 예제

fairscheduler.xml 파일에는 Spark 풀 특성 정보가 포함되어 있습니다. 파일은 필수이며 수동으로 구성되어야 합니다.

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

참조

자세한 정보는 다음 사이트를 참조하십시오.

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

마이그레이션

Analytic Server에서는 데이터 및 구성 설정을 기존 Analytic Server 설치에서 새 설치로 마이그레이션할 수 있습니다.

Analytic Server의 새 버전으로 업그레이드

Analytic Server 3.1.2가 이미 설치되어 있으며 최신 버전을 구매한 경우에는 3.1.2 구성 설정을 최신 설치로 마이그레이션할 수 있습니다.

제한사항: 3.1.2와 최신 설치는 동일한 Hadoop 클러스터에서 공존할 수 없습니다. 3.1.2 설치와 동일한 Hadoop 클러스터를 사용하도록 최신 설치를 구성할 경우 3.1.2 설치가 더 이상 작동하지 않습니다.

마이그레이션 단계(3.1.2에서 최신 버전으로)

1. 52 페이지의 『Cloudera에 설치』의 지시사항에 따라 Analytic Server의 새 설치를 수행합니다.
2. 분석 작업공간을 이전 설치에서 새 설치로 복사하십시오.
   a. 분석 작업공간의 위치를 모르는 경우 `hadoop -fs ls`를 실행하십시오. 분석 작업공간에 대한 경로는 `/user/as_user/analytic-root/analytic-workspace` 양식으로 되어 있습니다. 여기서, `as_user`는 분석 작업공간을 소유한 사용자 ID입니다.
   b. 새 Analytic Server 설치의 호스트에 `as_user`로 로그인하십시오. 있는 경우 `/user/as_user/analytic-root/analytic-workspace` 디렉토리를 삭제하십시오.
   c. 다음 복사 스크립트를 실행하십시오.

```
hadoop distcp hftp://{host of 3.1.2 namenode}:50070/{path to 3.1.2 analytic-workspace}
hdfs://{host of 3.2.1 namenode}/user/as_user/analytic-root/analytic-workspace
```

3. 임베드된 Apache Directory Server를 사용하는 경우 써드파티 LDAP 클라이언트 도구로 현재 사용자/그룹 구성을 백업하십시오. Analytic Server 3.2.1이 설치된 후 백업 사용자/그룹 구성을 Apache Directory Server로 가져오십시오.

   참고: 외부 LADP 서버를 사용하는 경우 이 단계를 건너뛸 수 있습니다.
4. Cloudera Manager에서 Analytic Server 서비스를 중지하십시오.
5. 이전 설치에서 구성 설정을 수집하십시오.
   a. 새 설치의 `configcollector.zip` 아카이브를 이전 설치의 `{AS_ROOT}\tools`에 복사하십시오.
   b. `configcollector.zip`의 사본을 추출하십시오. 이렇게 하면 이전 설치에 `configcollector` 서브디렉토리가 새로 작성됩니다.
   c. `{AS_ROOT}\tools\configcollector`에서 **`configcollector`** 스크립트를 실행하여 이전 설치에서 구성 콜렉터 도구를 실행하십시오. 결과 압축(ZIP) 파일을 새 설치를 호스트하는 서버에 복사하십시오.

   중요사항: 제공된 **`configcollector`** 스크립트는 최신 Analytic Server 버전과 호환되지 않을 수 있습니다. **`configcollector`** 스크립트에 문제점이 발생하면 IBM 기술 지원 담당자에게 문의하십시오.

6. Zookeeper 상태를 지우십시오. Zookeper bin 디렉토리(예: Cloudera의 경우 /opt/cloudera/parcels/CDH-5.4...../lib/zookeeper/bin)에서 다음 명령을 실행하십시오.

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

7. **migrationtool** 스크립트를 실행하고 구성 콜렉터가 작성하는 압축 파일의 경로를 인수로 전달하여 마이그레이션 도구를 실행하십시오. 예제는 다음과 같습니다.

   ```
   migrationtool.sh /opt/ibm/spss/analyticserver/3.2/ASConfiguration_3.1.2.xxx.zip
   ```

8. Analytic Server 노드의 명령 쉘에서 다음 명령을 실행하십시오.

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

9. Cloudera Manager에서 Analytic Server 서비스를 시작하십시오.

   참고: 기존 Analytic Server 설치와 함께 사용하도록 R을 구성한 경우, 새 Analytic Server 설치를 사용하여 이를 구성하는 단계에 따라야 합니다.

Cloudera에서 Analytic Server 설치 제거

Cloudera에서는 Analytic Server 서비스와 Parcel을 설치 제거하는 데 필요한 대부분의 단계가 자동으로 처리됩니다.

Cloudera 환경에서 Analytic Server를 정리하려면 다음 단계를 수행해야 합니다.

1. Analytic Server 서비스를 중지하고 삭제하십시오.
2. Analytic Server Parcel을 **비활성화**하고 **호스트에서 제거**한 다음 **삭제**하십시오.
3. HDFS에서 Analytic Server 사용자 디렉토리를 삭제하십시오. 기본 위치는 /user/as_user/analytic-root입니다.
4. Analytic Server에서 사용하는 데이터베이스 또는 스키마를 삭제하십시오.
5. Analytic Server 설치 패키지의 나머지 부분을 정리하십시오. 이는 다음을 삭제하여 수행됩니다.
   - csd 폴더
   - parcels, parcel-cache 및 parcel-repo 폴더에 있는 기존 3.1.2 파일

제 4 장 IBM SPSS Analytic Server와 함께 사용하도록 IBM SPSS Modeler 구성

SPSS Modeler를 Analytic Server와 함께 사용하려면 SPSS Modeler 서버 설치를 업데이트해야 합니다.

1. SPSS Modeler 서버를 구성하여 Analytic Server 설치와 연관시키십시오.
   a. 기본 서버 설치 디렉토리의 config 서브디렉토리에서 options.cfg 파일을 편집하고 다음 행을 추가하거나 편집하십시오.

```
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

Analytic Server에 보안 통신이 구성된 경우 Y를 지정하고 그렇지 않으면 N을 지정하십시오.

as_host

Analytic Server를 호스트하는 서버의 IP 주소/호스트 이름입니다.

참고: SSL이 Analytic Server에 대해 사용으로 설정된 경우 적절한 IP 주소/호스트 도메인 이름을 제공해야 합니다.

as_port

Analytic Server가 청취하는 포트(기본값: 8080).

as_context_root

Analytic Server 컨텍스트 루트(기본값: analyticserver).

as_tenant

SPSS Modeler 서버 설치가 멤버인 테넌트(기본 테넌트는 ibm).

as_prompt_for_password

SPSS Modeler 서버가 Analytic Server에서 사용하는 사용자 및 비밀번호 인증 시스템과 동일한 인증 시스템으로 구성된 경우(예: Kerberos 인증을 사용하는 경우) N을 지정하십시오. 그렇지 않으면 Y를 지정하십시오.

SPSS Modeler를 일괄처리 모드로 실행 중이면 -analytic_server_username {ASusername} -analytic_server_password {ASpassword}를 clemb 명령의 인수로 추가합니다.

as_kerberos_auth_mode

SPSS Modeler에서 Kerberos SSO를 사용으로 설정하려면 Y를 지정하십시오.

as_kerberos_krb5_conf

Analytic Server가 사용하는 Kerberos 구성 파일에 대한 경로를 지정하십시오(예: `\etc\krb5.conf`).

as_kerberos_krb5_spn

Analytic Server Kerberos SPN을 지정하십시오
(예: HTTP/ashost.mydomain.com@MYDOMAIN.COM).

b. SPSS Modeler 서버 서비스를 다시 시작하십시오.

SSL/TLS를 사용하는 Analytic Server 설치에 연결하려면 SPSS Modeler 서버와 클라이언트 설치를 구성하는 추가 단계를 수행해야 합니다.

a. `http{s}://{HOST}:{PORT}/{CONTEXT-ROOT}/admin/{TENANT}`로 이동하여 Analytic Server 콘솔에 로그온하십시오.

b. 브라우저에서 인증 파일을 다운로드하여 사용자의 파일 시스템에 저장하십시오.

c. SPSS Modeler 서버와 SPSS Modeler 클라이언트 설치에서 각각 JRE에 인증 파일을 추가하십시오. 업데이트 위치는 SPSS Modeler 설치 경로의 `/jre/lib/security/cacerts` 서브디렉토리에 있습니다.

1) `cacerts` 파일이 읽기 전용 파일이면 안됩니다.

2) Modeler와 함께 제공된 keytool 프로그램을 사용하십시오. 이 프로그램은 SPSS Modeler 설치 경로의 `/jre/bin/keytool` 서브디렉토리에 있습니다.

다음 명령을 수행하십시오.

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

<as-alias>는 `cacerts` 파일의 별명입니다. `cacerts` 파일에 대해 고유한 이름을 임의로 사용할 수 있습니다.

따라서 예제 명령은 다음과 비슷합니다.

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

d. SPSS Modeler 서버와 SPSS Modeler 클라이언트를 다시 시작하십시오.

2. [선택사항] 스트림에서 R 모델을 Analytic Server 데이터 소스와 함께 스코어링하려면 IBM SPSS Modeler - Essentials for R을 설치하십시오. IBM SPSS Modeler - Essentials for R을 다운로드할 수 있습니다(https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=swg-tspssp).

제 5 장 라이센스 부여를 추적하기 위한 SLM 태그 사용

SLM 태그는 자원 이용률 측정용 ISO/IEC 19770-4 표준 드래프트를 기반으로 합니다. SLM 태그는 제품이 라이센스 메트릭(소프트웨어 자산의 사용과 관련된 자원)의 소비를 보고하도록 표준화된 기능을 제공합니다. 제품에서 SLM을 사용 가능하도록 설정한 후에 라이센스 사용을 자체 보고하기 위해 런타임 XML 파일이 생성됩니다.

Analytic Server가 시작될 때 slmtag 파일이 <as_installation_path>/logs/slmtag 폴더에 작성됩니다.

두 개의 라이센스 유형이 있으므로 두 개의 서로 다른 메트릭이 정기적으로 기록됩니다.

- 현재 Analytic Server 버전의 경우, 라이센스 부여가 가상 서버를 기반으로 하는 Hadoop 클러스터 내의 데이터 노드의 총 수를 기반으로 합니다. 노드 수는 다음 slmtag 파일 섹션에 기록됩니다.

```
<Type>VIRTUAL_SERVER</Type>
   <SubType>Number of Data Nodes in Hadoop</SubType>
   <Value>2</Value>
   ...
```

- Analytic Server 버전 3.1 미만의 경우, 라이센스 부여가 RVU를 기반으로 하는 Hadoop 클러스터 내의 HDFS 저장 공간 크기를 기반으로 했습니다. 예를 들어, 저장 공간 크기(테가바이트 단위)는 다음 slmtag 파일 섹션에 기록됩니다.

```
<Type>RESOURCE_VALUE_UNIT</Type>
   <SubType>HDFS storage (Unit: Tega byte)</SubType>
   <Value>0.21</Value>
```

SLM 태그 출력은 스레드에서 시작되고 SlmTagOutput.properties 파일에서 정의된 특성에 의해 영향을 받습니다. 파일은 <as_installation_path>/configuration 폴더에 있습니다.

표 *14. SLM* 태그 특성

특성	설명
license.metric.logger.output.enabled	SLM 로그 파일 생성을 제어합니다. 기본값은 False입니다.
license.metric.logger.output.dir	SLM 태그 파일을 저장하는 디렉토리에 대한 상대 경로입니다. 기본 디렉토리는 <as_installation_path>/ logs입니다.
license.metric.logger.output.SLMLogFrequency	SLM 로그 수집에 필요한 시간 간격(단위: 밀리초)입니다.
icense.metric.logger.file.size	최대 SML 태그 파일 크기이며 바이트 단위입니다.
license.metric.logger.file.number	한 소프트웨어 ID 인스턴스에 대한 SLM 태그 파일의 최대 수입니다.

제 6 장 문제 해결

이 절에서는 공통 설치 및 구성 문제와 수정 방법에 대해 설명합니다.

일반 문제

경고와 함께 설치에 성공했지만, 사용자가 "요청을 완료할 수 없습니다. 이유: 권한 거부됨" 오류로 데이터 소스를 작성할 수 없습니다.

distrib.fs.root 매개변수를 Analytic Server 사용자(기본적으로 as_user)가 액세스할 수 없는 디렉토리로 설정하면 오류가 발생합니다. Analytic Server 사용자가 **distrib.fs.root** 디렉토리를 읽고 쓰며 실행하도록 권한이 부여되었는지 확인하십시오.

Analytic Server 성능이 점점 저하됩니다.

Analytic Server 성능이 기대에 미치지 못하는 경우, Knox 서비스 배포 경로: /<KnoxServicePath>/data/ deployments에서 모든 *.war 파일을 제거하십시오. 예를 들어, /usr/iop/4.1.0.0/knox/data/deployments입니다.

Ambari에서 Analytic Server 또는 Essentials for R 제거

Ambari에서 Analytic Server 또는 Essentials for R을 제거할 때 제거 프로세스가 정지되는 경우가 있습니다. 이 문제가 발생하면 수동으로 Ambari 서버의 프로세스 ID를 중지해야 합니다.

Analytic Server가 OpenJDK를 사용하는 POWER 시스템에 설치되는 경우의 문제

Analytic Server가 OpenJDK를 사용하는 POWER 시스템에서 실행되는 경우, 수동으로 다음 구성 단계를 수행하여 좌표계 API가 예상대로 작동하는지 확인하십시오.

참고: 좌표계 API를 사용하지 않는 경우, 구성 요구사항을 무시할 수 있습니다.

1. Ambari 콘솔에서 **Analytic Server 서비스** > **구성 탭** > **고급 analytics-jvm-options**로 이동하여 다음 행을 컨텐츠 영역에 추가하십시오.

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

2. Ambari 콘솔에서 **사용자 정의 analytics.cfg** 섹션으로 이동하여 다음 세 가지 구성을 추가하십시오.

   spark.executor.extraJavaOptions

   값을 다음과 같이 구성: -XX:CompileCommand=exclude,com/esri/sde/sdk/pe/engine/PeHznTwoPointEquidistant$GCSHorizon.*

   spark.driver.extraJavaOptions

   값을 다음과 같이 구성: -XX:CompileCommand=exclude,com/esri/sde/sdk/pe/engine/PeHznTwoPointEquidistant$GCSHorizon.*

mapred.child.java.opts

값을 다음과 같이 구성: `-XX:CompileCommand=exclude,com/esri/sde/sdk/pe/engine/PeHznTwoPointEquidistant$GCSHorizon.*`

SuSE Linux 12에서 Analytic Server를 설치할 때 오류 발생

SuSE Linux 12에서 Analytic Server를 설치할 때 다음 오류가 발생할 수 있습니다.

```
Signature verification failed [4-Signatures public key is not available]
```

SuSE Linux 12에서 Analytic Server를 설치하기 전에 다음 태스크를 수행하여 문제를 해결할 수 있습니다.

1. 다음 URL에서 공개 키를 호스트에 다운로드하십시오.

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

2. 호스트에서 다음 명령을 실행하여 공개 키를 가져오십시오.

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

특정 Hadoop 배포 문제

Analytic Server 서비스에 대한 새로 고치기 조치가 Hortonworks 2.3-2.6에서 사용 불가능함

Hortonworks 2.3-2.6에서 Analytic Server 라이브러리를 수동으로 새로 고치려면 다음 단계를 사용하십시오.

1. Analytic Metastore를 실행하는 호스트에 Analytic Server 사용자(기본적으로 as_user)로 로그온하십시오.

   참고: Ambari 콘솔에서 이 호스트 이름을 찾을 수 있습니다.

2. {AS_ROOT}/bin 디렉토리에서 **refresh** 스크립트를 실행하십시오. 예를 들어, 다음과 같습니다.

   ```
   cd /opt/ibm/spss/analyticserver/3.2/bin
   ./refresh
   ```

3. Ambari 콘솔에서 Analytic Server 서비스를 다시 시작하십시오.

외부 사이트에서 다운로드한 패키지가 Cloudera Manager에서 해시 검사 실패

해시 확인 오류가 Parcel 목록에 표시됩니다. 다운로드 프로세스가 완료되도록 허용한 다음 cloudera-scm-server 서비스를 통해 Cloudera를 다시 시작하여 문제를 해결할 수 있습니다. 서비스가 다시 시작된 후에는 오류가 발생하지 않습니다.

HDFS supergroup 특성

as_user가 **dfs.permissions.supergroup/dfs.permissions.superusergroup** HDFS 그룹 특성의 멤버가 아닌 경우 Analytic Server는 시작 중에 예외를 로그합니다. 예를 들어, 다음과 같습니다.

```
[11/15/17 7:32:35:510 PST] 000000bf SystemOut
O 2017-11-15 07:32:35,510 | : |  |  |  |  | ERROR | slmtagoutput.SlmOuputAgent | SLM Logger => Error in performing callback function when calculating number
of nodes in kerberos environment: org.apache.hadoop.ipc.RemoteException(org.apache.hadoop.security.AccessControlException): Access denied for user as_user.
Superuser privilege is required
at org.apache.hadoop.hdfs.server.namenode.FSPermissionChecker.checkSuperuserPrivilege(FSPermissionChecker.java:93)
at org.apache.hadoop.hdfs.server.namenode.FSNamesystem.checkSuperuserPrivilege(FSNamesystem.java:6606)
at org.apache.hadoop.hdfs.server.namenode.FSNamesystem.datanodeReport(FSNamesystem.java:5595)
at org.apache.hadoop.hdfs.server.namenode.NameNodeRpcServer.getDatanodeReport(NameNodeRpcServer.java:928)
at org.apache.hadoop.hdfs.server.namenode.AuthorizationProviderProxyClientProtocol.getDatanodeReport(AuthorizationProviderProxyClientProtocol.java:390)
at org.apache.hadoop.hdfs.protocolPB.ClientNamenodeProtocolServerSideTranslatorPB.getDatanodeReport(ClientNamenodeProtocolServerSideTranslatorPB.java:694)
```

```
at org.apache.hadoop.hdfs.protocol.proto.ClientNamenodeProtocolProtos$ClientNamenodeProtocol$2.callBlockingMethod(ClientNamenodeProtocolProtos.java)
at org.apache.hadoop.ipc.ProtobufRpcEngine$Server$ProtoBufRpcInvoker.call(ProtobufRpcEngine.java:617)
at org.apache.hadoop.ipc.RPC$Server.call(RPC.java:1073)
at org.apache.hadoop.ipc.Server$Handler$1.run(Server.java:2141)
at org.apache.hadoop.ipc.Server$Handler$1.run(Server.java:2137)
at java.security.AccessController.doPrivileged(Native Method)
at javax.security.auth.Subject.doAs(Subject.java:415)
at org.apache.hadoop.security.UserGroupInformation.doAs(UserGroupInformation.java:1912)
at org.apache.hadoop.ipc.Server$Handler.run(Server.java:2135)
```

dfs.permissions.supergroup/dfs.permissions.superusergroup hdfs-site 구성 특성에 정의된 OS 그룹에 as_user를 수동으로 추가해야 합니다.

- Cloudera의 경우 기본 특성 값은 **supergroup**이며 이를 실제 존재하는 OS 그룹으로 변경해야 합니다. Cloudera에서 supergroup 설정에 대한 정보는 Cloudera 문서를 참조하십시오.
- Ambari의 경우 기본 특성 값은 **hdfs**입니다. 기본적으로 Ambari 설치 중에 Analytic Server는 as_user를 HDFS 및 Hadoop 그룹에 추가합니다.

Linux에서는 **usermod** 명령을 사용하여 as_user를 HDFS **superusergroup**에 추가하십시오(이미 존재하지 않는 경우).

HDFS 권한에 대한 일반 정보는 HDFS Permissions Guide를 참조하십시오.

메타데이터 리포지토리 문제

add_mysql_user 스크립트를 실행하는 경우 CREATE USER 작업이 실패함

add_mysql_user 스크립트를 실행하기 전에 먼저 추가하려는 사용자를 mysql 데이터베이스에서 수동으로 제거해야 합니다. 사용자는 MySQL 워크벤치 UI 또는 MySQL 명령을 통해 제거할 수 있습니다. 예를 들어, 다음과 같습니다.

```
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'@'%';"
```

위 명령에서 $AEDB_USERNAME_VALUE는 제거할 사용자 이름으로 바꾸고, $METASTORE_HOST는 데이터베이스가 설치된 호스트 이름으로 바꾸십시오.

Apache Spark 문제

Spark 프로세스 내에서 실행되는 스트림 문제

SPSS Modeler 스트림이 Spark 프로세스 내에서 실행하도록 자동 설정된 경우에 완료되지 않습니다. 실패하는 SPSS Modeler 스트림은 Analytic Server 소스 노드(HDFS 파일)를 사용하여 작성되고 Sort 노드에 링크된 다음 다른 Analytic Server 데이터 소스를 내보내도록 설정됩니다. 스트림이 실행된 후에 자원 관리자 사용자 인터페이스가 새 애플리케이션이 실행 중임을 표시하나 스트림이 완료되지 않고 Running 상태로 남아 있습니다. Analytic Server 로그, YARN 로그 또는 Spark 로그에 스트림이 완료되지 않는 이유를 설명하는 메시지가 없습니다.

이 문제는 Analytic Server 구성 내의 사용자 정의 analytics.cfg 파일에 spark.executor.memory 설정을 추가하여 해결할 수 있습니다. (단일 노드 클러스터 환경의 경우) 메모리 값을 4GB로 설정하면 이전에 실패한 SPSS Modeler 스트림이 2분 내에 완료되도록 허용합니다.

Cloudera 5.x 및 Spark 1.x로 Spark 작업 실행 시 실패

Spark 1.x와 함께 Cloudera 5.x를 사용하는 경우 다음 예외가 발생할 수 있습니다.

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

예외는 org.apache.spark.scheduler.SparkListener를 캐스트할 수 없는 java.lang.ClassCastException: com.cloudera.spark.lineage.ClouderaNavigatorListener로 인해 발생합니다.

예외가 발생하지 않으려면 **analyticserver-conf/config.properties에 대한 Analytic Server 고급 구성 스니펫(안전 밸브)** 영역에서 다음 행을 추가해야 합니다.

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

SparkML 케이스 실행 중 다음 오류가 발생했습니다. "Exception during HdfsAuthcom.spss.utilities.i18n.LocException:Execution failed. Reason: com.spss.ae.filesystem.exception.FileSystemException: Unable to initialize the file system access."

이 오류는 Spark에서 계보 로그 디렉토리를 찾을 수 없을 때 발생합니다. 이 문제의 임시 해결책은 spark.lineage.log.dir의 경로를 /ae_wlpserver/usr/servers/aeserver/logs/spark로 재지정하는 것입니다.

고가용성 클러스터

종속성이 변경되어 더 많은 호스트에 Analytic Server를 추가할 수 없음

34 페이지의 『클라이언트 종속 항목 업데이트』의 지시사항에 따라 update_clientdeps 스크립트를 실행하십시오.

"Analytic Cluster Service와 Zookeeper의 접속이 예기치 않게 유실되어, 이 JVM이 클러스터 무결성을 유지보수하는 데 종료되었습니다."

Zookeeper에 작성하려는 데이터의 양이 너무 클 경우에 이 오류가 발생할 수 있습니다. 이 경우 Zookeeper 로그에 다음과 같은 예외가 표시됩니다.

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

또는 Analytic Server 로그에 다음과 같은 메시지가 표시됩니다.

```
Caused by: java.io.UTFDataFormatException: encoded string too long: 2054758 bytes
  at java.io.DataOutputStream.writeUTF(DataOutputStream.java:375)
```

1. Ambari 콘솔에서 Zookeeper 서비스 구성 탭을 탐색하고 다음 행을 env-template에 추가한 다음 Zookeeper 서비스를 다시 시작하십시오.

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

2. Ambari 콘솔에서 Analytic Server 서비스 구성 탭으로 이동하여 고급 analytics-jvm-options에 다음을 추가한 다음 Analytic Cluster 서비스를 다시 시작하십시오.

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

jute.maxbuffer 설정에 대해 지정할 숫자는 예외 메시지에 표시된 숫자보다 커야 합니다.

Zookeeper 트랜잭션 데이터를 관리할 수 없음

Zookeeper 트랜잭션 로그를 자동으로 제거할 수 있도록 설정하려면 zoo.cfg에서 **autopurge.purgeInterval** 매개변수를 1로 설정하십시오.

Analytic 클러스터 서비스와 Zookeeper의 연결이 끊김

zoo.cfg에서 **tickTime**, **initLimit** 및 **syncLimit** 매개변수를 검토하고 수정하십시오. 예를 들어, 다음과 같습니다.

```
# The number of milliseconds of each tick
tickTime=2000
# The number of ticks that the initial
# synchronization phase can take
initLimit=30
# The number of ticks that can pass between
# sending a request and getting an acknowledgement
syncLimit=15
```

세부사항은 https://zookeeper.apache.org/doc/r3.3.3/zookeeperAdmin.html에서 Zookeeper 문서를 참조하십시오.

Analytic Server 작업이 다시 실행되지 않음

Analytic Server 작업이 재개하지 않는 공통 상황이 있습니다.

- 클러스터 멤버가 실패하여 Analytic Server 작업이 실패하는 경우에는 일반적으로 다른 클러스터 멤버에서 작업이 자동으로 다시 시작됩니다. 작업이 다시 실행되지 않으면 고가용성 클러스터에 네 개 이상의 클러스터 멤버가 있는지 확인하십시오.

주의사항

이 정보는 미국에서 제공되는 제품 및 서비스용으로 작성된 것입니다. 이 자료는 IBM에서 다른 언어로 제공할 수도 있습니다. 그러나 자료에 접근하기 위해서는 해당 언어로 된 제품 또는 제품 버전의 사본이 필요할 수 있습니다.

IBM은 다른 국가에서 이 책에 기술된 제품, 서비스 또는 기능을 제공하지 않을 수도 있습니다. 현재 사용할 수 있는 제품 및 서비스에 대한 정보는 한국 IBM 담당자에게 문의하십시오. 이 책에서 IBM 제품, 프로그램 또는 서비스를 언급했다고 해서 해당 IBM 제품, 프로그램 또는 서비스만을 사용할 수 있다는 것을 의미하지는 않습니다. IBM의 지적 재산권을 침해하지 않는 한, 기능상으로 동등한 제품, 프로그램 또는 서비스를 대신 사용할 수도 있습니다. 그러나 비IBM 제품, 프로그램 또는 서비스의 운영에 대한 평가 및 검증은 사용자의 책임입니다.

IBM은 이 책에서 다루고 있는 특정 내용에 대해 특허를 보유하고 있거나 현재 특허 출원 중일 수 있습니다. 이 책을 제공한다고 해서 특허에 대한 라이센스까지 부여하는 것은 아닙니다. 라이센스에 대한 의문사항은 다음으로 문의하십시오.

07326
서울특별시 영등포구
국제금융로 *10, 3IFC*
한국 아이.비.엠 주식회사
대표전화서비스*: 02-3781-7114*

2바이트(DBCS) 정보에 관한 라이센스 문의는 한국 IBM에 문의하거나 다음 주소로 서면 문의하시기 바랍니다.

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

IBM은 타인의 권리 비침해, 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 어떠한 종류의 보증 없이 이 책을 "현상태대로" 제공합니다. 일부 국가에서는 특정 거래에서 명시적 또는 묵시적 보증의 면책사항을 허용하지 않으므로, 이 사항이 적용되지 않을 수도 있습니다.

이 정보에는 기술적으로 부정확한 내용이나 인쇄상의 오류가 있을 수 있습니다. 이 정보는 주기적으로 변경되며, 변경된 사항은 최신판에 통합됩니다. IBM은 이 책에서 설명한 제품 및/또는 프로그램을 사전 통지 없이 언제든지 개선 및/또는 변경할 수 있습니다.

이 정보에서 언급되는 비IBM 웹 사이트는 단지 편의상 제공된 것으로, 어떤 방식으로든 이들 웹 사이트를 옹호하고자 하는 것은 아닙니다. 해당 웹 사이트의 자료는 본 IBM 제품 자료의 일부가 아니므로 해당 웹 사이트 사용으로 인한 위험은 사용자 본인이 감수해야 합니다.

IBM은 귀하의 권리를 침해하지 않는 범위 내에서 적절하다고 생각하는 방식으로 귀하가 제공한 정보를 사용하거나 배포할 수 있습니다.

(i) 독립적으로 작성된 프로그램과 기타 프로그램(본 프로그램 포함) 간의 정보 교환 및 (ii) 교환된 정보의 상호 이용을 목적으로 본 프로그램에 관한 정보를 얻고자 하는 라이센스 사용자는 다음 주소로 문의하십시오.

07326
서울특별시 영등포구
국제금융로 *10, 3IFC*
한국 아이.비.엠 주식회사
대표전화서비스*: 02-3781-7114*

이러한 정보는 해당 조건(예를 들면, 사용료 지불 등)하에서 사용될 수 있습니다.

이 정보에 기술된 라이센스가 부여된 프로그램 및 프로그램에 대해 사용 가능한 모든 라이센스가 부여된 자료는 IBM이 IBM 기본 계약, IBM 프로그램 라이센스 계약(IPLA) 또는 이와 동등한 계약에 따라 제공한 것입니다.

인용된 성능 데이터와 고객 예제는 예시 용도로만 제공됩니다. 실제 성능 결과는 특정 구성과 운영 조건에 따라 다를 수 있습니다.

비IBM 제품에 관한 정보는 해당 제품의 공급업체, 공개 자료 또는 기타 범용 소스로부터 얻은 것입니다. IBM에서는 이러한 제품들을 테스트하지 않았으므로, 비IBM 제품과 관련된 성능의 정확성, 호환성 또는 기타 청구에 대해서는 확신할 수 없습니다. 비IBM 제품의 성능에 대한 의문사항은 해당 제품의 공급업체에 문의하십시오.

IBM이 제시하는 방향 또는 의도에 관한 모든 언급은 특별한 통지 없이 변경될 수 있습니다.

여기에 나오는 모든 IBM의 가격은 IBM이 제시하는 현 소매가이며 통지 없이 변경될 수 있습니다. 실제 판매가는 다를 수 있습니다.

이 정보는 계획 수립 목적으로만 사용됩니다. 이 정보는 기술된 제품이 GA(General Availability)되기 전에 변경될 수 있습니다.

이 정보에는 일상의 비즈니스 운영에서 사용되는 자료 및 보고서에 대한 예제가 들어 있습니다. 이들 예제에는 개념을 가능한 완벽하게 설명하기 위하여 개인, 회사, 상표 및 제품의 이름이 사용될 수 있습니다. 이들 이름은 모두 가공의 것이며 실제 인물 또는 기업의 이름과 유사하더라도 이는 전적으로 우연입니다.

저작권 라이센스:

이 정보에는 일상의 비즈니스 운영에서 사용되는 자료 및 보고서에 대한 예제가 들어 있습니다. 이들 예제에는 개념을 가능한 완벽하게 설명하기 위하여 개인, 회사, 상표 및 제품의 이름이 사용될 수 있습니다. 이들 이름은 모두 가공의 것이며 실제 인물 또는 기업의 이름과 유사하더라도 이는 전적으로 우연입니다.

이러한 샘플 프로그램 또는 파생 제품의 각 사본이나 그 일부에는 반드시 다음과 같은 저작권 표시가 포함되어야 합니다.

상표

IBM, IBM 로고 및 ibm.com은 전세계 여러 국가에 등록된 International Business Machines Corp.의 상표 또는 등록상표입니다. 기타 제품 및 서비스 이름은 IBM 또는 타사의 상표입니다. 현재 IBM 상표 목록은 웹 "저작권 및 상표 정보"(www.ibm.com/legal/copytrade.shtml)에 있습니다.

Adobe, Adobe 로고, PostScript 및 PostScript 로고는 미국 및/또는 기타 국가에서 사용되는 Adobe Systems Incorporated의 등록상표 또는 상표입니다.

IT Infrastructure Library는 현재 Office of Government Commerce의 일부인 Central Computer and Telecommunications Agency의 등록상표입니다.

Intel, Intel 로고, Intel Inside, Intel Inside 로고, Intel Centrino, Intel Centrino 로고, Celeron, Intel Xeon, Intel SpeedStep, Itanium 및 Pentium은 미국 또는 기타 국가에서 사용되는 Intel Corporation 또는 그 계열사의 상표 또는 등록상표입니다.

Linux는 미국 또는 기타 국가에서 사용되는 Linus Torvalds의 등록상표입니다.

Microsoft, Windows, Windows NT 및 Windows 로고는 미국 또는 기타 국가에서 사용되는 Microsoft Corporation의 상표입니다.

ITIL은 미국 특허청(U.S. Patent and Trademark Office)에 등록된 The Minister for the Cabinet Office의 등록상표 및 등록 공동체 상표입니다.

UNIX는 미국 및 기타 국가에서 사용되는 The Open Group의 등록상표입니다.

Cell Broadband Engine은 미국 또는 기타 국가에서 해당 라이센스에 의거하여 사용되는 Sony Computer Entertainment, Inc.의 상표입니다.

Linear Tape-Open, LTO, LTO 로고, Ultrium 및 Ultrium 로고는 미국 및 기타 국가에서 사용되는 HP, IBM Corp. 및 Quantum의 상표입니다.