hadoop中配置Kerberos

有问题请找：沈国栋

安装配置Kerberos KDC（Key distribution center）

1. 安装如下Kerberos包: **krb5-server**, **krb5-workstation**, **krb5-libs**。
   执行如下命令进行安装：
   `# yum install krb5-server krb5-workstation krb5-libs`

2. 修改配置文件**/etc/krb5.conf**。
   将文件中所有配置为**EXAMPLE.COM**的地方改成实际的realm，如BCHKDC。将文件中左右配置为**kerberos.example.com**的地方改成本机的域名（通过hostname查看）。**example.com**改成本机域名对应的后缀。

3. 修改配置文件**/var/kerberos/krb5kdc/kdc.conf**。
   将文件中所有配置为**EXAMPLE.COM**的地方改成实际的realm（与**/etc/krb5.conf**中配置的realm保持一致）。

4. 用**kdb5_util**命令创建Kerberos realm的数据库。
   执行如下命令创建：
   `# /usr/sbin/kdb5_util create -s`
   执行该命令后，会在**/var/kerberos/krb5kdc**目录下生成5个文件：

   - 两个Kerberos数据库文件**principal**和**principal.ok**
   - Kerberos管理数据库文件principal.kadm5
   - 管理数据库的锁文件principal.kadm5.lock
   - 贮藏(stash)文件，这里是.k5.BCHKDC

5. 配置**/var/kerberos/krb5kdc/kadm5.acl**文件。 这个文件是**kadmin**命令用来确定哪些principals拥有Kerberos数据库的访问权限。一般建议配置成一行，如下所示：
   `*/admin@BCHKDC *`

6. 执行如下命令启动Kerberos：
   `# service krb5kdc start`
   `# service kadmin start`

7. 检查KDC是否分发票据(ticket)。

   - 在kadmin中添加一条principal，其中username为对应的用户名： `# /usr/sbin/kadmin.local : addprinc username`
   - 使用对应用户执行**kinit**命令获取一个票据并存在缓存文件中
   - 使用对应用户执行**klist**命令查看缓存中的票据
   - 使用对应用户执行**kdestroy**命令销毁缓存中的票据。

   > 说明： kinit默认使用系统登录的用户名到KDC中获取票据。如果principal和当前用户的用户名不一样，将会报错。kinit可以指定principal，如下principal为指定的值。
   > `kinit principal`

安装配置Kerberos客户端

> 注意：需要确保Kerberos客户端和服务端时间同步，否则会影响客户端到服务端的鉴权。可以使用NTP做时间同步。

1. 安装如下Kerberos包: **krb5-workstation**, **krb5-libs**。
   执行如下命令进行安装：
   `# yum install krb5-workstation krb5-libs`

2. 修改配置文件**/etc/krb5.conf**。
   与KDC节点的**/etc/krb5.conf**文件配置成一样即可。

创建Kerberos principal

- 根据实际节点上安装的组件，为每个节点上的组件创建一个principal。其中hostname为主机名，BCHKDC为Kerberos的realm。

> 例如，要为hadoop1节点的NameNode创建一条principal，首先登陆到kdc节点，依次执行如下命令进行创建：
> `# kadmin.local`
> `kadmin.local: addprinc -randkey nn/hadoop1@BCHKDC`

组件	**principal**	**keytab**（建议）	属组	权限
JournalNode	jn/hostname@BCHKDC	jn.service.keytab	hdfs:hadoop	400
NameNode	nn/hostname@BCHKDC	nn.service.keytab	hdfs:hadoop	400
NM的SPNEGO用户	HTTP/hostname@BCHKDC	spnego.service.keytab	root:hadoop	440
DataNode	dn/hostname@BCHKDC	dn.service.keytab	hdfs:hadoop	400
HDFS用户	hdfs@BCHKDC	hdfs.headless.keytab	hdfs:hadoop	440
HDFS的SPENGO用户	HTTP/hostname@BCHKDC	spnego.service.keytab	root:hadoop	440
ResourceManager	rm/hostname@BCHKDC	rm.service.keytab	yarn:hadoop	400
RM的SPNEGO用户	HTTP/hostname@BCHKDC	spnego.service.keytab	root:hadoop	440
NodeManager	nm/hostname@BCHKDC	nm.service.keytab	mapred:hadoop	400
History Server	jhs/hostname@BCHKDC	jsh.service.keytab	hdfs:hadoop	400
HS的SPNEGO用户	HTTP/hostname@BCHKDC	spnego.service.keytab	root:hadoop	440
ZooKeeper Server	zookeeper/hostname@BCHKDC	zk.service.keytab	zookeeper:hadoop	400

生成**Keytab**并部署

1. 根据上节生成的principal，生成对应keytab文件。

   > 例如，要为hadoop1节点的NameNode的principal生成一个keytab文件，依次执行如下命令进行生成：
   > `# kadmin.local`
   > `kadminv.local: xst -k hadoop1/nn.service.keytab nn/hadoop1@BCHKDC`

2. 将keytab文件放到对应服务器上（如/etc/security/keytabs目录下）

3. 按"创建Kerberos principal"中的表格，修改各keytab的属组和权限。

   > 例如，NameNode组件，将nn.service.keytab放到/etc/security/keytabs，依次执行如下命令修改属组和权限：
   > `chown hdfs:hadoop /etc/security/keytabs/nn.service.keytab` `chmod 400 /etc/security/keytabs/nn.service.keytab`

修改配置文件

1. 修改hadoop全局配置项，使hadoop使用Kerberos进行鉴权。

   > 说明：hadoop的配置文件在$HADOOP_HOME/etc/hadoop目录下，如果是ambari安装的环境，则在/etc/hadoop/conf目录下。
   > 默认keytab文件统一放在/etc/security/keytabs目录下。

配置文件	**name**	**value**
core-site.xml	hadoop.security.authentication	kerberos
	hadoop.security.authorization	true
	hadoop.security.auth_to_local	RULE:[2:$1@$0](rm@.*BCHKDC)s/.*/yarn/ RULE:[2:$1@$0](nm@.*BCHKDC)s/.*/yarn/ RULE:[2:$1@$0](nn@.*BCHKDC)s/.*/hdfs/ RULE:[2:$1@$0](dn@.*BCHKDC)s/.*/hdfs/ RULE:[2:$1@$0](jhs@.*BCHKDC)s/.*/mapred/ RULE:[2:$1@$0](jn/_HOST@.*BCHKDC)s/.*/hdfs/s DEFAULT

2. 根据各组件的安装情况，在各节点上修改该节点所安装的组件的对应配置参数。下表为各组件需要新增的配置参数：

组件	配置文件	**name**	**value**
ResourceManager	yarn-site.xml	yarn.resourcemanager.principal	rm/_HOST@BCHKDC
		yarn.resourcemanager.keytab	/etc/security/keytabs/rm.service.keytab
		yarn.resourcemanager.webapp.spnego-principal	HTTP/_HOST@BCHKDC
		yarn.resourcemanager.webapp.spnego-keytab-file	/etc/security/keytabs/spnego.service.keytab
NodeManager	yarn-site.xml	yarn.nodemanager.principal	nm/_HOST@BCHKDC
		yarn.nodemanager.keytab	/etc/security/keytabs/nm.service.keytab
		yarn.nodemanager.webapp.spnego-principal	HTTP/_HOST@BCHKDC
		yarn.nodemanager.webapp.spnego-keytab-file	/etc/security/keytabs/spnego.service.keytab
History Server	mapred-site.xml	mapreduce.jobhistory.principal	jhs/_HOST@BCHKDC
		mapreduce.jobhistory.keytab	/etc/security/keytabs/jhs.service.keytab
		mapreduce.jobhistory.webapp.spnego-principal	HTTP/_HOST@BCHKDC
		mapreduce.jobhistory.webapp.spnego-keytab-file	/etc/security/keytabs/spnego.service.keytab
JournalNode	hdfs-site.xml	dfs.journalnode.kerberos.principal	jn/_HOST@BCHKDC
		dfs.journalnode.keytab.file	/etc/security/keytabs/jn.service.keytab
NameNode	hdfs-site.xml	dfs.namenode.kerberos.principal	nn/_HOST@BCHKDC
		dfs.namenode.keytab.file	/etc/security/keytabs/nn.service.keytab
		dfs.web.authentication.kerberos.principal	HTTP/_HOST@BCHKDC
		dfs.web.authentication.kerberos.keytab	/etc/security/keytabs/spnego.service.keytab
		dfs.namenode.kerberos.internal.spnego.principal	HTTP/_HOST@BCHKDC
DataNode	hdfs-site.xml	dfs.datanode.kerberos.principal	dn/_HOST@BCHKDC
		dfs.datanode.keytab.file	/etc/security/keytabs/dn.service.keytab

3. 修改zookeeper配置项。

> 说明：zookeeper的配置文件在$ZK_HOME/conf目录下，如果是ambari安装的环境，则在/etc/zookeeper/conf目录下。
> 默认keytab文件统一放在/etc/security/keytabs目录下。

- 修改配置文件：zoo.cfg，增加配置参数：

```
authProvider.1=org.apache.zookeeper.server.auth.SASLAuthenticationProvider
jaasLoginRenew=3600000
kerberos.removeHostFromPrincipal=true
kerberos.removeRealmFromPrincipal=true
```

- 在zookeeper的conf目录下增加配置文件zookeeper_jaas.conf，内容如下（其中，默认使用/etc/security/keytabs作为keytab存放路径，hadoop1为主机名，BCHKDC为Kerberos的realm）：

```
Server {
com.sun.security.auth.module.Krb5LoginModule required
useKeyTab=true
storeKey=true
useTicketCache=false
keyTab="/etc/security/keytabs/zk.service.keytab"
principal="zookeeper/hadoop1@BCHKDC";
};
```

- 在zookeeper的conf目录下增加配置文件zookeeper*client*jaas.conf，内容如下：

```
Client {
com.sun.security.auth.module.Krb5LoginModule required
useKeyTab=false
useTicketCache=true;
};
```

- 修改配置文件：zookeeper-env.sh，增加配置参数(这里配置的路径为zookeeper*jaas.conf*和*zookeeper*client_jaas.conf实际存放路径)：

```
export SERVERJVMFLAGS="$SERVERJVMFLAGS -Djava.security.auth.login.config=/etc/zookeeper/conf/zookeeper_jaas.conf"
export CLIENTJVMFLAGS="$CLIENTJVMFLAGS -Djava.security.auth.login.config=/etc/zookeeper/conf/zookeeperclientjaas.conf"
```

重启**hadoop**服务

NA

功能测试

1. 没有keytab文件，或者没有配置principal和keytab参数的进程将启动失败。

   例如，未生成DataNode的keytab文件放到对应目录下，启动DataNode进程时报错，如下图所示：

```
2014-07-16 17:24:06,481 FATAL datanode.DataNode (DataNode.java:secureMain(1989)) - Exception in secureMain
java.io.IOException: Login failure for dn/ambari1@SGDKDC from keytab /etc/security/keytabs/dn.service.keytab
        at org.apache.hadoop.security.UserGroupInformation.loginUserFromKeytab(UserGroupInformation.java:890)
        at org.apache.hadoop.security.SecurityUtil.login(SecurityUtil.java:242)
        at org.apache.hadoop.security.SecurityUtil.login(SecurityUtil.java:206)
        at org.apache.hadoop.hdfs.server.datanode.DataNode.instantiateDataNode(DataNode.java:1764)
        at org.apache.hadoop.hdfs.server.datanode.DataNode.createDataNode(DataNode.java:1806)
        at org.apache.hadoop.hdfs.server.datanode.DataNode.secureMain(DataNode.java:1982)
        at org.apache.hadoop.hdfs.server.datanode.SecureDataNodeStarter.start(SecureDataNodeStarter.java:78)
        at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
        at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:57)
        at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
        at java.lang.reflect.Method.invoke(Method.java:606)
        at org.apache.commons.daemon.support.DaemonLoader.start(DaemonLoader.java:243)
Caused by: javax.security.auth.login.LoginException: Unable to obtain password from user
```

FAQ

1. 执行kadmin，输入密码后登陆不成功，报如下错误：

```
[root@yum krb5kdc]# kadmin
Authenticating as principal root/admin@BCHKDC with password.
Password for root/admin@BCHKDC:
kadmin: GSS-API (or Kerberos) error while initializing kadmin interface
```

解决方法： 升级OpenSSL:

```
yum install openssl
```

1. 在客户端执行kinit时，报如下错误:

```
[root@ambari1 scripts]# kinit kinit: Cannot contact any KDC for realm 'BCHKDC' while getting initial credentials
```

解决方法： 检查KDC服务器上防火墙是否打开，如果打开着，需要关闭。

```
service iptables status
```

```
service iptables stop
```

> 说明： 关闭时状态显示为：
> iptables: Firewall is not running.

1. 启动服务时报如下错误:

> ipc.Server (Server.javaoRead(801)) - IPC Server listener on 8020: readAndProcess from client 192.168.198.101 threw exception [javax.security.sasl.SaslException: GSS initiate failed [Caused by GSSException: Failure unspecified at GSS-API level (Mechanism level: **Encryption type AES256 CTS mode with HMAC SHA1-96 is not supported/enabled**)]]

解决方法： 安装JCE策略文件。
下载jce包后，根据里面的README.txt文件进行安装。