英特尔® Hadoop 发行版

版本 2.2

安全指南

目录

1 简介

文档目的

本文档用于指导英特尔® Hadoop 发行版用户配置基于 Kerberos 的集群安全通信机制。

1.1 Kerberos 简介

Kerberos 是一种计算机网络认证协议，它允许某实体在非安全网络环境下通信，向另一个实体以一种安全的方式证明自己的身份。麻省理工大学实现此协议，并发布的一套免费软件。它的设计主要针对客户-服务器模型，并提供了一系列交互认证——用户和服务器都能验证对方的身份，可以保护网络实体免受窃听和重复攻击。Kerberos 协议基于对称密码学，并需要一个值得信赖的第三方，协议的扩展可以为认证的某些阶段提供公钥密码学支持。

2 安全配置

2.1 安装 IDH

第一步，在终端窗口输入以下命令进入安装目录并开始安装带有 Kerberos 的 IDH，确保所有安装都处于成功状态。

```
cd intelhadoop
 ./install
```

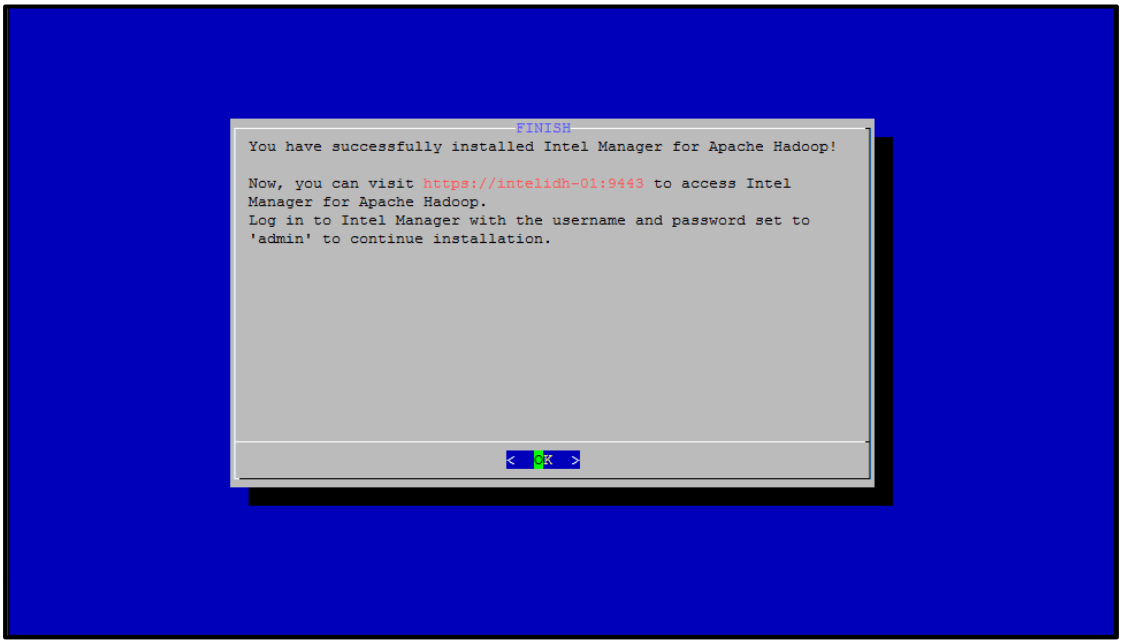

图 2.1 安装 IDH

第二步，配置集群节点认证协议，选择 Kerberos 安全策略。安装与集群节点配置过程可参考《英特尔® Hadoop 发行版 新手指南》。

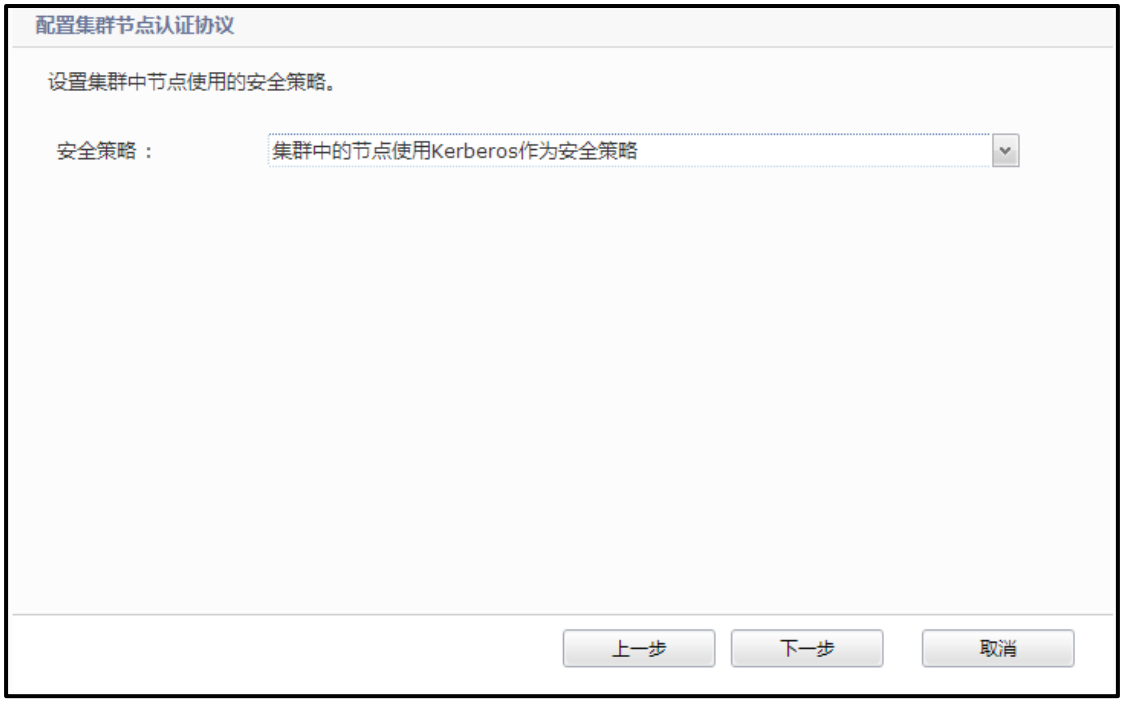

图 2.2 配置集群节点认证协议

第三步，向集群中添加节点，并配置角色。

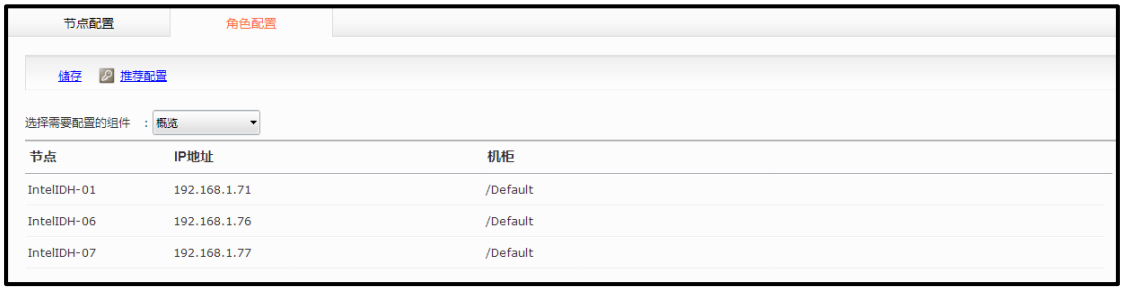

图 2.3 配置节点角色

注意：如果在网络环境中选用 DNS 方式使用主机名互相访问，需要管理员保证每个节点的反向 DNS 正常工作。

2.2 改变 Kerberos 域

第一步，切换至 Kerberos 配置页面，点击左上角的 change realm 按钮，改变 Kerberos 域。

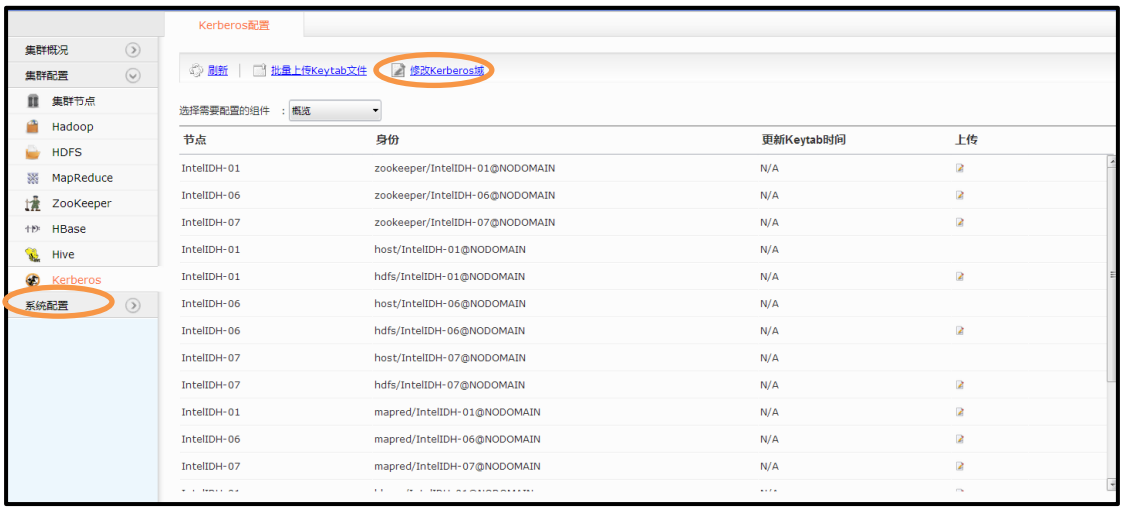

图 2.4 改变 Kerberos 域

第二步，改变 Kerberos 域，如 SH.INTEL.COM，域名需要以大写字母的形式表示，点击确定完成修改。

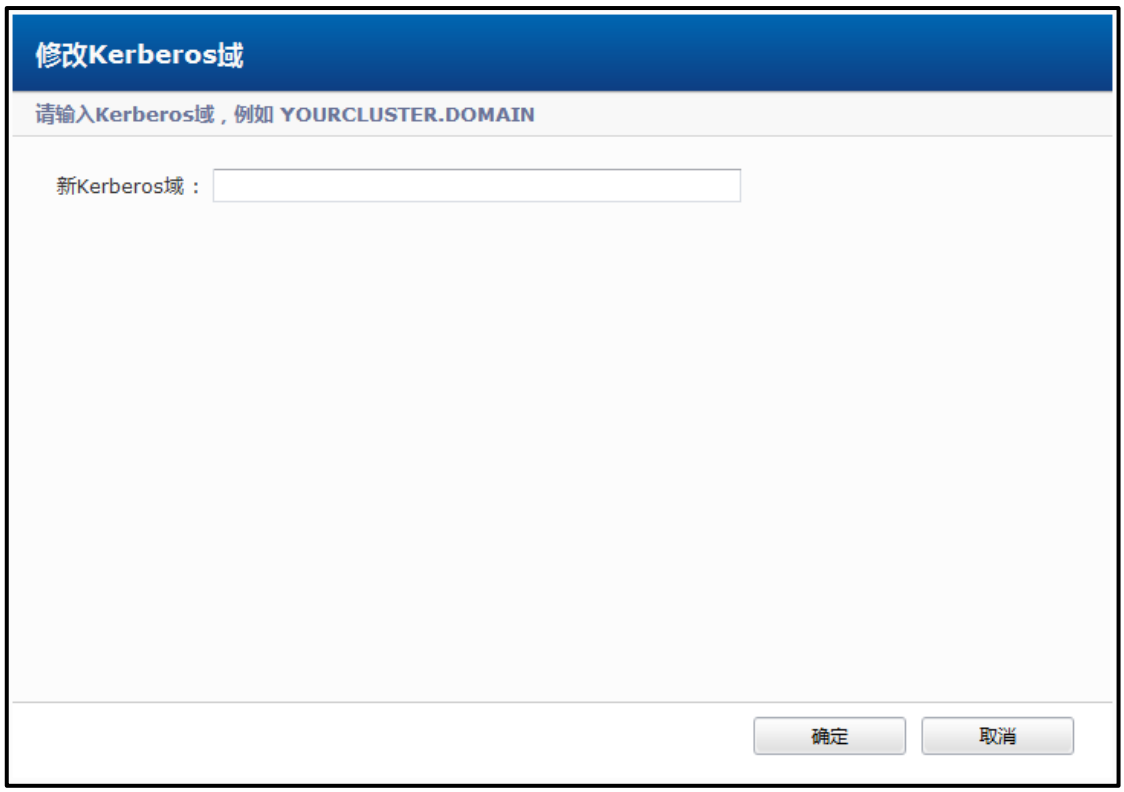

图 2.5 改变 Kerberos 的领域

2.3 安装配置 KDC 服务器

第一步，选择集群中的一个节点成为 KDC 服务器，在终端窗口输入以

下命令来安装 KDC 服务器。

```
yum install krb5-server
```

```
Running Transaction
  Installing : krb5-server-1.9-33.el6.x86_64                                1/1
  Verifying  : krb5-server-1.9-33.el6.x86_64                                1/1

Installed:
  krb5-server.x86_64 0:1.9-33.el6

Complete!
```

图 2.6 安装 KDC 服务器

第二步，修改 KDC 服务器上的配置文件。

修改/etc/krb5.conf 文件，将<kdc_server_hostname>指 KDC 服务器实际的 hostname，<REALM>指之前配置的 Kerberos realms，<domain>为集群所在的域。

default_tkt_enctypes、default_tgs_enctypes 和 permitted_enctypes 表示加密的方式。如果设置 AES-256 的加密方式，必须在所有节点上安装 Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy File。如果您不想使用 AES-256 的加密方式，可在 kdc.conf 和 krb5.conf 参数下移除 aes256-cts:normal 条目。

若需要使用 Secondary NameNode，请务必将 allow_weak_crypto 设置为 true。因为在 FS 检查点时将使用 Kerberized SSL（KSSL）协议来传输 fsimage。配置样例如下：

```
[libdefaults]
        default_realm = <REALM>
        dns_lookup_realm = false
        dns_lookup_kdc = false
        ticket_lifetime = 24h
        renew_lifetime = 7d
        forwardable = true
        default_tkt_enctypes = des-cbc-md5 des-cbc-crc des3-cbc-sha1
        default_tgs_enctypes = des-cbc-md5 des-cbc-crc des3-cbc-sha1
        permitted_enctypes = des-cbc-md5 des-cbc-crc des3-cbc-sha1
        allow_weak_crypto = true

[realms]
        <REALM> = {
                kdc = <kdc_server_hostname>:88
                admin_server = <kdc_server_hostname>:749
                default_domain = <domain>
        }

[domain_realm]
        .<domain> = <REALM>
```

```
        <domain> = <REALM>

[logging]
        kdc = FILE:/var/log/krb5kdc.log
        admin_server = FILE:/var/log/kadmin.log
        default = FILE:/var/log/krb5libs.log
```

修改/var/kerberos/krb5kdc/kdc.conf 文件，将<REALM>部分修改为相应的 Kerberos realms（如 SH.INTEL.COM）。supported_enctypes 参数用于设置加密方式。配置样例如下：

```
[kdcdefaults]
        kdc_ports = 88
        kdc_tcp_ports = 88

[realms]
        <REALM> = {
                admin_keytab = /etc/kadm5.keytab
                database_name = /var/kerberos/krb5kdc//principal
                acl_file = /var/kerberos/krb5kdc//kadm5.acl
                key_stash_file = /var/kerberos/krb5kdc//stash
                admin_keytab = /var/kerberos/krb5kdc/kadm5.keytab
                master_key_type = des3-hmac-sha1
                supported_enctypes = arcfour-hmac:normal des3-hmac-sha1:normal
des-cbc-crc:normal des:normal des:v4 des:norealm des:onlyrealm des:afs3
                default_principal_flags = +preauth
        }
```

修改/var/kerberos/krb5kdc/kadm5.acl 控制访问权限。若要给予 admin 所有权限，配置样例如下：

```
*/admin *
```

第三步，执行如下命令创建对应 Kerberos 领域数据库，并改变数据库及管理员的密码。

```
rm -f /etc/kadm5.keytab
kdb5_util -P <password> -r <realm> create -s
kadmin.local -q 'cpw -pw <admin_password> kadmin/admin'
```

注意：<password>指创建的数据库密码，<realm>指 Kerberos 领域名，<admin_password>指 kadmin/admin 的密码。

```
[root@IntelIDH-06 krb5kdc]# kdb5_util -P apple -r SH.INTEL.COM create -s
Loading random data
Initializing database '/var/kerberos/krb5kdc//principal' for realm 'SH.INTEL.COM
',
master key name 'K/M@SH.INTEL.COM'
[root@IntelIDH-06 krb5kdc]# kadmin.local -q 'cpw -pw apple kadmin/admin'
Authenticating as principal root/admin@SH.INTEL.COM with password.
```

图 2.7 配置 KDC 服务器

第四步，用以下命令启动刚刚配置完成的服务器。

```
service krb5kdc start
service kadmin start
```

```
[root@IntelIDH-06 krb5kdc]# service krb5kdc start
Starting Kerberos 5 KDC:                                   [  OK  ]
[root@IntelIDH-06 krb5kdc]# service kadmin start
Starting Kerberos 5 Admin Server:                          [  OK  ]
```

图 2.8 启动 KDC 服务

2.4 安装 Kerberos 客户端程序

执行以下命令安装 Kerberos 客户端程序，然后复制 KDC 服务器上的 krb5.conf 到集群中每个节点的当前目录下。

```
yum install krb5-workstation
cp krb5.conf /etc/
```

```
Running Transaction
  Installing : krb5-workstation-1.9-33.el6.x86_64                1/1
  Verifying  : krb5-workstation-1.9-33.el6.x86_64                1/1

Installed:
  krb5-workstation.x86_64 0:1.9-33.el6
```

图 2.9 安装 Kerberos 客户端程序

2.5 生成身份条目（principal）和密钥表（keytab）

按以下命令行规则创建在 Kerberos 页面中的身份条目（principal），并生成相应的密钥表（keytab）。

```
kadmin -w <admin_password> -p kadmin/admin -q 'addprinc -randkey <principal_name>'

e.g. 为 intelidh-01 创建 hdfs principal 和 host principal
```

```
kadmin -w <admin_password> -p kadmin/admin -q
   'addprinc -randkey hdfs/ intelidh-01@SH.INTEL.COM'
kadmin -w <admin_password> -p kadmin/admin -q
   'addprinc -randkey host/ intelidh-01@SH.INTEL.COM'
```

```
kadmin -w <admin_password> -p kadmin/admin -q 'xst -k <keytab_name> <principal_name>'

e.g. 生成 hdfs 和 host 的 keytab
kadmin -w <admin_password> -p kadmin/admin -q 'xst -k
   /tmp/hdfs.keytab hdfs/ intelidh-01@SH.INTEL.COM'
kadmin -w <admin_password> -p kadmin/admin -q 'xst -k
   /tmp/hdfs.keytab host/ intelidh-01@SH.INTEL.COM'
```

注意：生成 hdfs 的 keytab 时需生成 host 规则于同一 keytab 中。<keytab_name>代表创建的 keytab 的文件名，<principal_name>代表包含在<keytab_name>的身份条目。

在集群配置高可用性（High-Availability）的情况下，Intel Manager 会在 Kerberos 页面中产生如下几条特殊的身份条目:

```
hdfs/<Virtual host FQDN>@<REALM>
host/<Virtual host FQDN>@<REALM>
mapred/<Virtual host FQDN>@<REALM>
```

其中，前两条是高可用性的 namenode 和 backup namenode 所使用的 principal，需生成到 namenode.keytab 中，并将此 keytab 上传至对应的 principal 中或放入 namenode 和 backup namenode 对应的 keytab 文件夹中用于批量上传。

第三条是 HA 的 jobtracker 和 backup jobtracker 所使用的 principal，需生成到 jobtracker.keytab 中，并将此 keytab 上传至对应的 principal 中或放入 jobtracker 和 backup jobtracker 对应的 keytab 文件夹中用于批量上传。

```
[root@intelcloud-vm-11 ~]# kadmin -w secure -p kadmin/admin -q 'addprinc -randke
y hdfs/intelcloud-vm-11.sh.intel.com@SH.INTEL.COM'
Authenticating as principal kadmin/admin with password.
WARNING: no policy specified for hdfs/intelcloud-vm-11.sh.intel.com@SH.INTEL.COM
; defaulting to no policy
Principal "hdfs/intelcloud-vm-11.sh.intel.com@SH.INTEL.COM" created.
[root@intelcloud-vm-11 ~]# kadmin -w secure -p kadmin/admin -q 'addprinc -randke
y host/intelcloud-vm-11.sh.intel.com@SH.INTEL.COM'
Authenticating as principal kadmin/admin with password.
WARNING: no policy specified for host/intelcloud-vm-11.sh.intel.com@SH.INTEL.COM
; defaulting to no policy
Principal "host/intelcloud-vm-11.sh.intel.com@SH.INTEL.COM" created.
```

图 2.10 添加身份条目

```
[root@intelcloud-vm-11 ~]# kadmin -w secure -p kadmin/admin -q 'xst -k /tmp/hdfs
-intelcloud-vm-11.keytab host/intelcloud-vm-11.sh.intel.com@SH.INTEL.COM'
Authenticating as principal kadmin/admin with password.
Entry for principal host/intelcloud-vm-11.sh.intel.com@SH.INTEL.COM with kvno 2,
 encryption type arcfour-hmac added to keytab WRFILE:/tmp/hdfs-intelcloud-vm-11.
keytab.
Entry for principal host/intelcloud-vm-11.sh.intel.com@SH.INTEL.COM with kvno 2,
 encryption type des3-cbc-sha1 added to keytab WRFILE:/tmp/hdfs-intelcloud-vm-11
.keytab.
Entry for principal host/intelcloud-vm-11.sh.intel.com@SH.INTEL.COM with kvno 2,
 encryption type des-cbc-crc added to keytab WRFILE:/tmp/hdfs-intelcloud-vm-11.k
eytab.
```

图 2.11 生成密钥表

2.6 上传密钥表（keytab）文件

第一步，将身份条目（principal）和密钥表（keytab）全部生成完毕后，用 SCP 等工具将所有 keytab 复制到本地文件夹中。

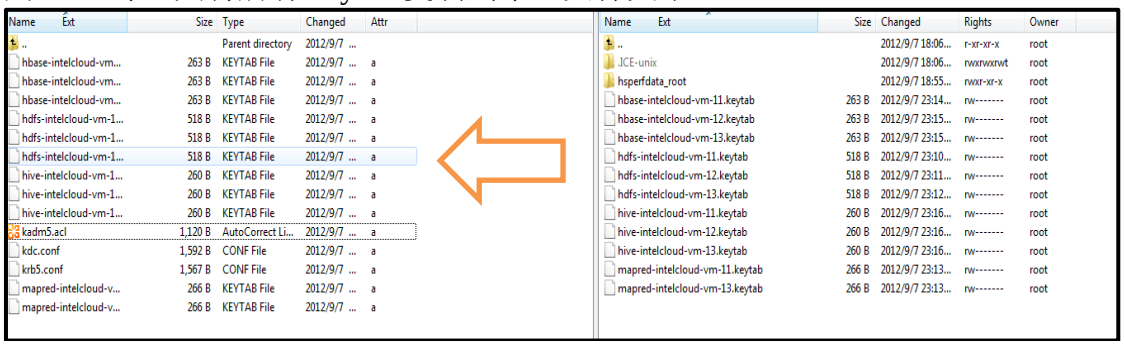

图 2.12 复制 keytab 到本地文件夹

第二步，在 Kerberos 配置页面中上传对应的 keytab 文件，上传成功后可看到 keytab 最后更新的时间。

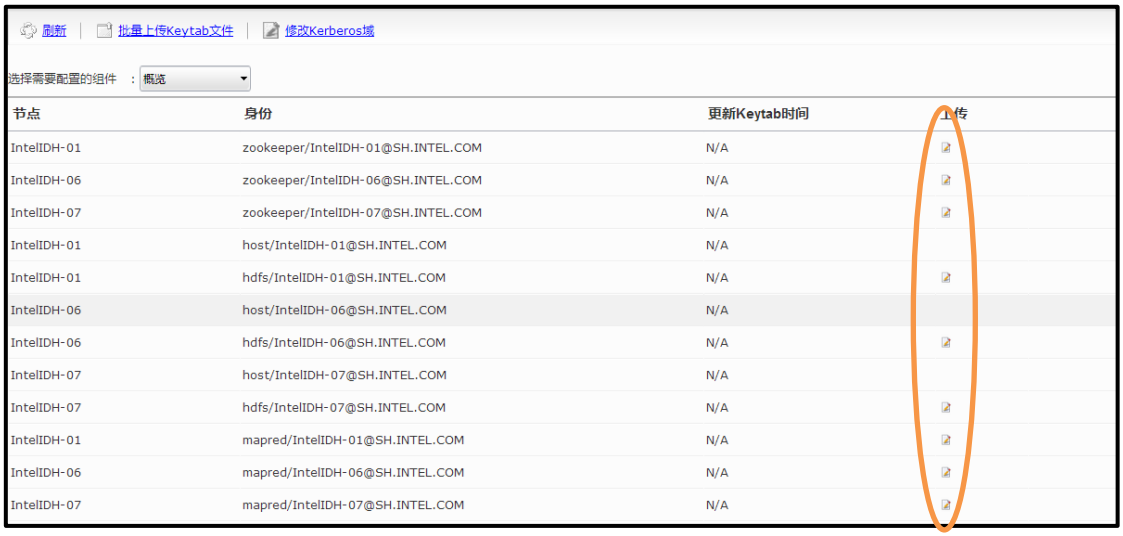

图 2.13 上传 keytab 文件

2.7 批量上传 keytab 文件

在 IDH2.1 或以上的版本中，支持批量上传 keytab 文件的功能。第一步，新建对应节点名称（一般为 Full Qualified Domain Name）的文件夹，如节点名为 intelidh-01，则文件夹为 intelidh-01。

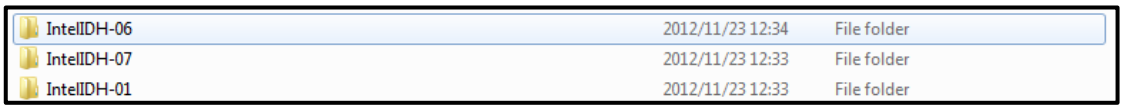

图 2.14 根据结点名称新建文件夹

第二步，将之前生成的 keytab 文件根据规则重新命名为 hdfs.keytab、mapred.keytab、zookeeper.keytab、hbase.keytab 和 hive.keytab 放入对应的文件夹中。

图 2.15 重命名 keytab 文件

第三步，将之前创建的文件夹放入一个新建文件夹中，然后执行下列命令压缩成 tar 包，后缀名为.tar。

```
tar -cf <file_name>.tar <directory_name>
```

第四步，将刚刚生成的 tar 包复制到本地文件夹中，然后在 kerberos 配置页面中选择批量上传 keytab，上传成功后可看到 keytab 最后更新的时间。

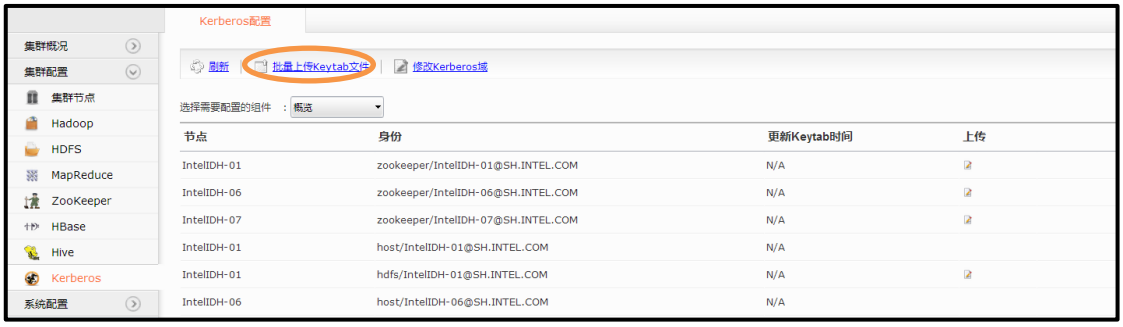

图 2.16 批量上传 keytab 文件

2.8 开启 HBase 权限验证

第一步，切换至 HBase 配置页面，点击全配置标签。

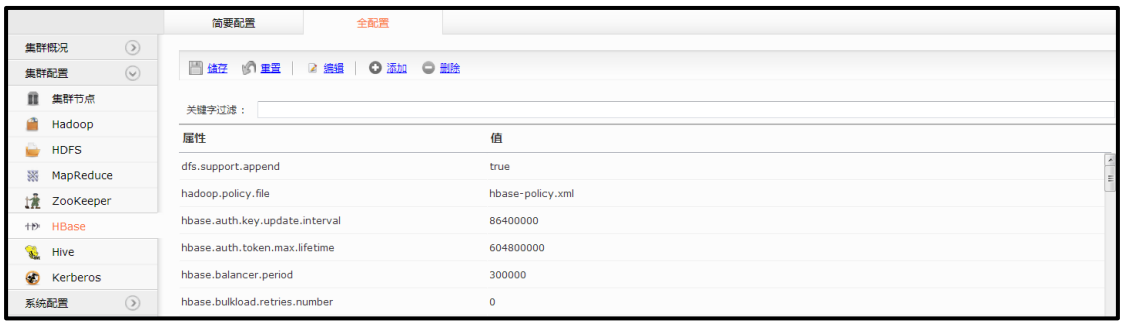

图 2.17 更改 HBase 权限验证

第二步，在列表中找到属性 *hbase.coprocessor.master.classes*，添加值为 *org.apache.hadoop.hbase.security.access.AccessController*；在列表中找到属性 *hbase.coprocessor.region.classes*，添加值为 *org.apache.hadoop.hbase.security.token.TokenProvider,org.apache.hadoop.hbase.security.access.AccessController*，然后点击保存按钮提交修改。

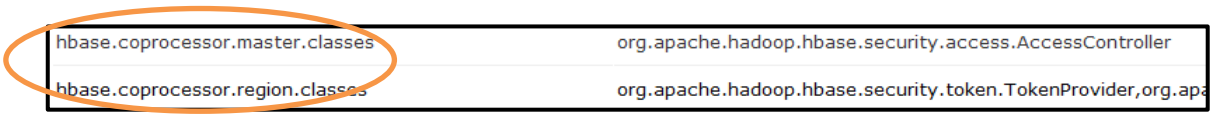

图 2.18 添加 HBase 权限验证属性

第三步，通过 Hbase shell 的方式，为权限验证配置访问控制表

```
grant <user> <permissions>[ <table>[ <column family>[ <column qualifier> ] ] ]
# grants permissions
revoke <user> <permissions> <table> [ <column family> [ <column qualifier> ] ]
# revokes permissions
alter <table> {OWNER => <user>}
# sets the table owner
user_permission <table>
# displays existing permissions
```

在上述命令行中，<>中为变量，[]为可选，permissions 可由 RWCA 这 4 个字母中的多个组成，其中：

- R 代表读取权限，执行 Get, Scan, 及 Exists 调用时需要此权限
- W 代表写入权限，执行 Put, Delete, LockRow, UnlockRow, IncrementColumnValue, CheckAndDelete, CheckAndPut, Flush 以及 Compact 调用时需要此权限

- C 代表创建权限，执行 Create, Alter 以及 Drop 调用时需要此权限
- A 代表管理员权限执行 Enable, Disable, MajorCompact, Grant, Revoke 和 Shutdown 调用时需要此权限

2.9 部署更改

在集群节点页面中，点击配置所有节点按钮部署所有更改。

图 2.19 部署所有更改

2.10 新建 map/reduce 任务用户

第一步，在集群中执行 map/reduce 任务的每台机器上，执行如下命令添加一个用户来执行 map/reduce 任务。

```
useradd <username> -u <uid>
```

注意：uid 需要在 500 以上

第二步，在 KDC 服务器所在的机器上，创建相应的身份条目(principal)。

```
kadmin -w <admin_password> -p kadmin/admin -q 'addprinc <username>'
```

```
[root@xtt-portal ~]# kadmin -w secure -p kadmin/admin -q 'addprinc mrtester'
Authenticating as principal kadmin/admin with password.
WARNING: no policy specified for mrtester@SH.INTEL.COM; defaulting to no policy
Enter password for principal "mrtester@SH.INTEL.COM":
Re-enter password for principal "mrtester@SH.INTEL.COM":
Principal "mrtester@SH.INTEL.COM" created.
```

图 2.20 创建 map/reduce 用户身份条目

第三步，使用刚才添加的用户获取新票据。

```
sudo -u <username> kinit
```

```
[mrtester@xmlqa-clv9 mapred]$ kinit
Password for mrtester@SH.INTEL.COM:
```

图 2.21 获取新票据

第四步，测试 map/reduce 任务是否能成功运行。

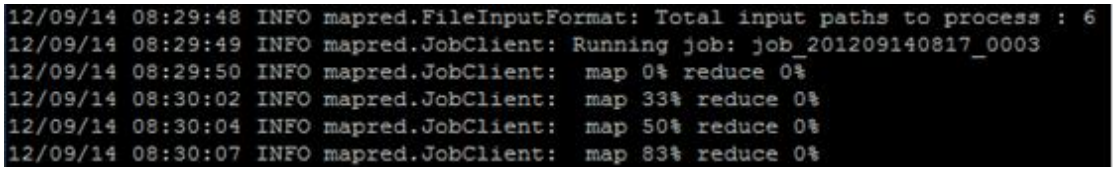

图 2.22 测试 map/reduce 任务

至此，Kerberos 在 IDH 中的配置已经全部完成。

3 附录 - 常见问题

3.1 在应用 Kerberos 安全策略后运行 Hadoop 失败

描述：

用户必须拥有有效的 Kerberos 票据来与 Hadoop 集群交互，如果没有此票据，则任何 Hadoop 命令（如 hadoop fs -ls）将会失败，并且会出现如下错误信息：

```
ERROR: java.lang.RuntimeException: SASL authentication failed. The most likely cause is missing or invalid credentials. Consider 'kinit'.
```

解决方法：

用 klist 命令检查当前票据缓存中是否存在 Kerberos 票据。您可以通过 kinit 命令输入 principal 密码或使用 keytab 文件来获得票据。
用以下命令通过 keytab 文件来获得票据：

```
kinit -k -t <keytab_filename> <principal_name>@<realm>
```

3.2 JAVA 不能读取 Kerberos1.81 或更高版本所创建的票据缓存

描述：

在使用 Kerberos1.81 或更高版本时，当用户尝试与 hadoop 集群交互时，会出现以下错误，尽管用户已经使用 kinit 命令成功获取了 Kerberos 票据：

```
java.io.IOException: javax.security.sasl.SaslException: GSS initiate failed
```

由于 Kerberos 票据缓存格式的改变，Oracle JDK 6 Update 26 之前的版本将不能读取 Kerberos1.81 版本以上的票据缓存

解决方法：

在用 kinit 命令获取票据后，使用 kinit -R 命令将获得的票据更新，票据会重新以一种 JAVA 能够识别的格式写入。