Kerberos主从配置文档

# Kerberos主从同步机制

在Master上通过以下命令同步数据:

kdb5\_util dump /var/kerberos/krb5kdc/slave\_db

kprop –f /var/kerberos/krb5kdc/slave\_db kerberos2.hadoop.com

Slave1

192.168.88.89

Master

192.168.88.88

kpropd

Krb5kdc

kadmin

# 搭建 Kerberos

## 环境

我们在两个备用NameNode节点上实现Kerberos主从，并在其它需要接入认证的主机上安装Kerberos客户端。

* **操作系统**：CentOS 6.7/RedHart 6.7
* **运行用户**：root

## 安装

我们是基于RedHart 6.7/CentOS 6.7操作系统，相关Kerberos安装包通过yum依赖获取。

### 准备工作

确认三台机器添加主机名解析到 /etc/hosts 文件中。

$ cat /etc/hosts

192.168.88.88 kerberos.hadoop.com master

192.168.88.89 kerberos2.hadoop.com slave1

192.168.88.90 slave2

注意：hostname 请使用小写，要不然在集成 kerberos 时会出现一些错误。

### 安装 kdc server

在 **KDC (**这里是master 和 slave1**)** 上安装包 **krb5**、**krb5-server** 和 **krb5-client**。

yum install krb5-server krb5-libs krb5-auth-dialog -y

yum install krb5-workstation -y

在其他节点（kerberos 所有认证客户端，这里是slave2）安装 krb5-libs、krb5-workstation

yum install krb5-libs -y

yum install krb5-workstation –y

### 修改配置文件

kdc 服务器涉及到三个配置文件：

/etc/krb5.conf

/var/kerberos/krb5kdc/kdc.conf

/var/kerberos/krb5kdc/kadm5.acl

配置 **Kerberos** 的一种方法是编辑配置文件 **/etc/krb5.conf**。默认安装的文件中包含多个示例项。

$ cat /etc/krb5.conf

  [logging]

   default = FILE:/var/log/krb5libs.log

   kdc = FILE:/var/log/krb5kdc.log

   admin\_server = FILE:/var/log/kadmind.log

  [libdefaults]

   default\_realm = HADOOP.COM

   dns\_lookup\_realm = false

   dns\_lookup\_kdc = false

   clockskew = 120

   ticket\_lifetime = 24h

   renew\_lifetime = 7d

   forwardable = true

   renewable = true

   udp\_preference\_limit = 1

   default\_tgs\_enctypes = arcfour-hmac

   default\_tkt\_enctypes = arcfour-hmac

 [realms]

   HADOOP.COM = {

    kdc = kerberos.hadoop.com:88

   kdc = kerberos2.hadoop.com:88

   admin\_server = kerberos.hadoop.com:749

   }

  [domain\_realm]

   .hadoop.com = HADOOP.COM

   www.hadoop.com = HADOOP.COM

  [kdc]

  profile=/var/kerberos/krb5kdc/kdc.conf

**说明：**

* [logging]：表示 server 端的日志的打印位置
* [libdefaults]：每种连接的默认配置，需要注意以下几个关键的小配置
  + default\_realm = HADOOP.COM：设置 Kerberos 应用程序的默认领域。如果您有多个领域，只需向 [realms] 节添加其他的语句。
  + udp\_preference\_limit= 1：禁止使用 udp 可以防止一个Hadoop中的错误
  + clockskew：时钟偏差是不完全符合主机系统时钟的票据时戳的容差，超过此容差将不接受此票据。通常，将时钟扭斜设置为 300 秒（5 分钟）。这意味着从服务器的角度看，票证的时间戳与它的偏差可以是在前后 5 分钟内。
  + ticket\_lifetime： 表明凭证生效的时限，一般为24小时。
  + renew\_lifetime： 表明凭证最长可以被延期的时限，一般为一个礼拜。当凭证过期之后，对安全认证的服务的后续访问则会失败。
* [realms]：列举使用的 realm。
  + kdc：代表要 kdc 的位置。格式是 机器:端口
  + admin\_server：代表 admin 的位置。格式是 机器:端口
  + default\_domain：代表默认的域名
* [appdefaults]：可以设定一些针对特定应用的配置，覆盖默认配置。

修改 /var/kerberos/krb5kdc/kdc.conf ，该文件包含 Kerberos 的配置信息。例如，KDC 的位置，Kerbero 的 admin 的realms 等。需要所有使用的 Kerberos 的机器上的配置文件都同步。这里仅列举需要的基本配置。详细参考：http://web.mit.edu/~kerberos/krb5-devel/doc/admin/conf\_files/krb5\_conf.html

$ cat /var/kerberos/krb5kdc/kdc.conf

[kdcdefaults]

 v4\_mode = nopreauth

 kdc\_ports = 88

 kdc\_tcp\_ports = 88

[realms]

 HADOOP.COM = {

  #master\_key\_type = aes256-cts

  acl\_file = /var/kerberos/krb5kdc/kadm5.acl

  dict\_file = /usr/share/dict/words

  admin\_keytab = /var/kerberos/krb5kdc/kadm5.keytab

  supported\_enctypes =  des3-hmac-sha1:normal arcfour-hmac:normal des-hmac-sha1:normal des-cbc-md5:normal des-cbc-crc:normal des-cbc-crc:v4 des-cbc-crc:afs3

  max\_life = 24h

  max\_renewable\_life = 10d

  default\_principal\_flags = +renewable, +forwardable

 }

**说明：**

* HADOOP.COM： 是设定的 realms。名字随意。Kerberos 可以支持多个 realms，会增加复杂度。大小写敏感，一般为了识别使用全部大写。这个 realms 跟机器的 host 没有大关系。
* master\_key\_type：和 supported\_enctypes 默认使用 aes256-cts。由于，JAVA 使用 aes256-cts 验证方式需要安装额外的 jar 包（后面再做说明）。推荐不使用，并且删除 aes256-cts。
* acl\_file：标注了 admin 的用户权限，需要用户自己创建。文件格式是：Kerberos\_principal permissions [target\_principal] [restrictions]
* supported\_enctypes：支持的校验方式。
* admin\_keytab：KDC 进行校验的 keytab。

**关于AES-256加密**：

对于使用 centos5. 6及以上的系统，默认使用 AES-256 来加密的。这就需要集群中的所有节点上安装 [Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy File](http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html)。

下载的文件是一个 zip 包，解开后，将里面的两个文件放到下面的目录中：$JAVA\_HOME/jre/lib/security

为了能够不直接访问 KDC 控制台而从 Kerberos 数据库添加和删除主体，请对 Kerberos 管理服务器指示允许哪些主体执行哪些操作。通过编辑文件 /var/lib/kerberos/krb5kdc/kadm5.acl 完成此操作。ACL（访问控制列表）允许您精确指定特权。

$ cat /var/kerberos/krb5kdc/kadm5.acl

  \*/admin@HADOOP.COM \*

### 同步配置文件

将 kdc 中的 /etc/krb5.conf 拷贝到客户端slave2

$ scp /etc/krb5.conf slave1:/etc/krb5.conf

$ scp /etc/krb5.conf slave2:/etc/krb5.conf

请确认集群是否关闭了 selinux。

### 创建数据库

在 master 上运行初始化数据库命令。其中 -r 指定对应 realm。

$ kdb5\_util create -r HADOOP.COM -s

出现 Loading random data 的时候另开个终端执行点消耗CPU的命令如 cat /dev/sda > /dev/urandom 可以加快随机数采集。

该命令会在 /var/kerberos/krb5kdc/ 目录下创建 principal 数据库。

如果遇到数据库已经存在的提示，可以把 /var/kerberos/krb5kdc/ 目录下的 principal 的相关文件都删除掉。默认的数据库名字都是 principal。可以使用 -d 指定数据库名字。

### 启动服务

在 master 节点上运行：

$ chkconfig --level 35 krb5kdc on

$ chkconfig --level 35 kadmin on

$ service krb5kdc start

$ service kadmin start

### 创建 kerberos 管理员

关于 kerberos 的管理，可以使用 kadmin.local 或 kadmin，至于使用哪个，取决于账户和访问权限：

* 如果有访问 kdc 服务器的 root 权限，但是没有 kerberos admin 账户，使用 kadmin.local
* 如果没有访问 kdc 服务器的 root 权限，但是用 kerberos admin 账户，使用 kadmin

在 master 上创建远程管理的管理员：

*#手动输入两次密码，这里密码为123456*

$ kadmin.local -q "addprinc root/admin"

*# 也可以不用手动输入密码*

$ echo -e "123456\n123456" | kadmin.local -q "addprinc root/admin"

系统会提示输入密码，密码不能为空，且需妥善保存

### Slave1 KDC配置

1. **Slave上创建数据库**

[root@slave1 ~]# kdb5\_util create -r HADOOP.COM -s

Loading random data

Initializing database '/var/kerberos/krb5kdc/principal' for realm 'HADOOP.COM',

master key name 'K/M@HADOOP.COM'

You will be prompted for the database Master Password.

It is important that you NOT FORGET this password.

Enter KDC database master key:

Re-enter KDC database master key to verify:

密码：123456

[root@slave1 ~]# ll /var/kerberos/krb5kdc/

总用量 24

-rw------- 1 root root 21 11月 28 09:04 kadm5.acl

-rw------- 1 root root 404 11月 28 08:58 kdc.conf

-rw------- 1 root root 8192 11月 28 09:17 principal

-rw------- 1 root root 8192 11月 28 09:17 principal.kadm5

-rw------- 1 root root 0 11月 28 09:17 principal.kadm5.lock

-rw------- 1 root root 0 11月 28 2017 principal.ok

1. **创建host keytab 文件**

在master服务器上

[root@master ~]#  kadmin.local

kadmin.local: addprinc -randkey host/kerberos.hadoop.com

#添加principal

kadmin.local：ktadd host/kerberos.hadoop.com

#生成keytab文件

kadmin.local: addprinc -randkey host/kerberos2.hadoop.com

#添加principal

kadmin.local：ktadd host/kerberos2.hadoop.com

#生成keytab文件

在slave1服务器上

[root@slave1 ~]#  kadmin.local

kadmin: addprinc –randkey host/kerberos2.hadoop.com

#添加principal

kadmin: ktadd host/kerberos2.hadoop.com

#生成keytab文件

1. **将master上的几个文件拷贝到从服务器**

文件: krb5.conf、kdc.conf、kadm5.acl、master key stash file

[root@master ~]# scp /etc/krb5.conf slave1:/etc/

[root@master ~]# cd /var/kerberos/krb5kdc

[root@master ~]# scp kdc.conf kadm5.acl .k5.HADOOP.COM slave1:/var/kerberos/krb5kdc/

1. **在slave服务器上创建kpropd.acl文件**

[root@slave1 ~]# touch /var/kerberos/krb5kdc/kpropd.acl

添加如下内容：

host/kerberos.hadoop.com@HADOOP.COM

host/kerberos2.hadoop.com@HADOOP.COM

1. **在slave1上启动kpropd服务**

[root@slave1 ~]# kpropd -S

至此，slave上的kdc服务还不能启动，因为无kdc的database数据

1. **在master上将相关数据同步到slave1上**

[root@master ~]# kdb5\_util dump /var/kerberos/krb5kdc/slave\_datatrans

[root@master ~]# kprop -f /var/kerberos/krb5kdc/slave\_datatrans kerberos2.hadoop.com

成功后，会出现以下信息：

Database propagation to kerberos2.hadoop.com: SUCCEEDED

以上命令，可以封装成一个bash，定时运行，即定时更新slave上的database。

1. **Slave1上/var/kerberos/krb5kdc/会多出一些文件，如：**

from\_master、principal、pricipal.kadm5、principal.kadmin5.lock、principal.ok

至此，可以启动slave上的kdc服务

1. **测试主从是否生效**

从第三台服务器，使用kinit 获取ticket，正常情况下会从master上获取

关闭master上的kdc服务

再次从第三台服务器上，使用kinit 获取ticket，如果成功，说明生效。

也可以观察kdc的日志，在 /var/log/krb5kdc.log

### 测试 kerberos

查看当前的认证用户：

*# 查看principals*

$ kadmin: list\_principals

*# 添加一个新的principal*

kadmin:  addprinc test

WARNING: no policy specified for user1@JAVACHEN.COM; defaulting to no policy

Enter password for principal "test@HADOOP.COM":

Re-enter password for principal "test@JHADOOP.COM":

Principal "test@HADOOP.COM" created.

*# 删除principal*

kadmin:  delprinc test

Are you sure you want to delete the principal "test@HADOOP.COM"? (yes/no): yes

Principal "test@HADOOP.COM" deleted.

Make sure that you have removed this principal from all ACLs before reusing.

kadmin: exit

也可以直接通过下面的命令来执行：

*# 提示需要输入密码*

$ kadmin -p root/admin -q "list\_principals"

$ kadmin -p root/admin -q "addprinc test"

$ kadmin -p root/admin -q "delprinc test"

*# 不用输入密码*

$ kadmin.local -q "list\_principals"

$ kadmin.local -q "addprinc test"

$ kadmin.local -q "delprinc test"

创建一个测试用户 test，密码设置为 test：

$ echo -e "test\ntest" | kadmin.local -q "addprinc test"

获取 test 用户的 ticket：

*# 通过用户名和密码进行登录*

$ kinit test

Password for test@JAVACHEN.COM:

$ klist -e

Ticket cache: FILE:/tmp/krb5cc\_0

Default principal: test@JAVACHEN.COM

Valid starting     Expires            Service principal

11/07/14 15:29:02  11/08/14 15:29:02  krbtgt/JAVACHEN.COM@JAVACHEN.COM

  renew until 11/17/14 15:29:02, Etype (skey, tkt): AES-128 CTS mode with 96-bit SHA-1 HMAC, AES-128 CTS mode with 96-bit SHA-1 HMAC

Kerberos 4 ticket cache: /tmp/tkt0

klist: You have no tickets cached

销毁该 test 用户的 ticket：

$ kdestroy

$ klist

klist: No credentials cache found (ticket cache FILE:/tmp/krb5cc\_0)

Kerberos 4 ticket cache: /tmp/tkt0

klist: You have no tickets cached

更新 ticket：

$ kinit root/admin

  Password for root/admin@JAVACHEN.COM:

$  klist

  Ticket cache: FILE:/tmp/krb5cc\_0

  Default principal: root/admin@JAVACHEN.COM

  Valid starting     Expires     Service principal

  11/07/14 15:33:57  11/08/14 15:33:57  krbtgt/JAVACHEN.COM@JAVACHEN.COM

  renew until 11/17/14 15:33:57

  Kerberos 4 ticket cache: /tmp/tkt0

  klist: You have no tickets cached

$ kinit -R

$ klist

  Ticket cache: FILE:/tmp/krb5cc\_0

  Default principal: root/admin@JAVACHEN.COM

  Valid starting     Expires            Service principal

  11/07/14 15:34:05  11/08/14 15:34:05  krbtgt/JAVACHEN.COM@JAVACHEN.COM

  renew until 11/17/14 15:33:57

  Kerberos 4 ticket cache: /tmp/tkt0

  klist: You have no tickets cached

抽取密钥并将其储存在本地 keytab 文件 /etc/krb5.keytab 中。这个文件由超级用户拥有，所以您必须是 root 用户才能在 kadmin shell 中执行以下命令：

$ kadmin.local -q "ktadd kadmin/admin"

$ klist -k /etc/krb5.keytab

  Keytab name: FILE:/etc/krb5.keytab

  KVNO Principal

  ---- --------------------------------------------------------------------------

     3 kadmin/admin@HADOOP.COM

     3 kadmin/admin@HADOOP .COM

     3 kadmin/admin@HADOOP .COM

     3 kadmin/admin@HADOOP .COM

     3 kadmin/admin@HADOOP .COM

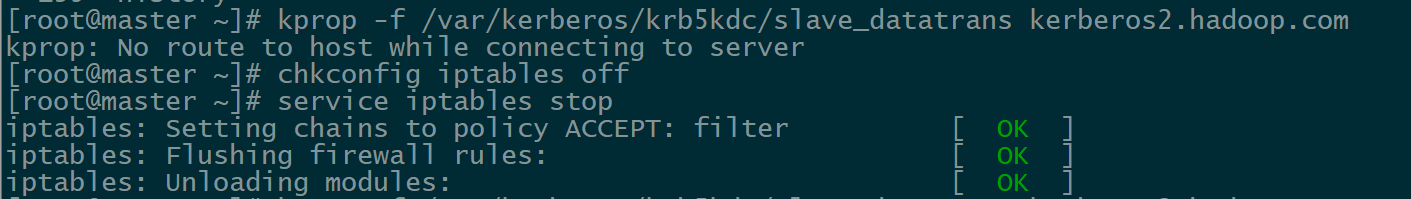
### CDH集群启用kerberos(略)

### 错误

kprop: No route to host while connecting to server

chkconfig iptables off

service iptables stop



http://web.mit.edu/kerberos/krb5-devel/doc/admin/troubleshoot.html#kprop-no-route

其他常见错误：

<http://web.mit.edu/kerberos/krb5-devel/doc/admin/troubleshoot.html>