



CDH 5.x 快速安装和配置 Kerberos 操作说明 (SuSE 11 sp3 版本)



目录

1	概述	3
2	安装 MIT Kerberos	3
2.1	安装 krb5-server krb5-client openldap2-client.....	3
2.2	修改/etc/krb5.conf.....	3
2.2	下载 UnlimitedJCEPolicyJDK7.zip 并替换 JDK 目录 jar 文件.....	4
2.2	创建 Kerberos 数据库	5
2.2	修改/var/lib/kerberos/krb5kdc/kdc.conf	5
2.2	修改/var/lib/kerberos/krb5kdc/kadm5.acl.....	6
2.3	启动 kdc 和 admin 服务	6
2.3	执行 kadmin 命令	6
3	使用 Cloudera Manager Kerberos 配置向导	8
3.1	进入 Cloudera Manager	8
3.1	启用 Kerberos	9
4	常见问题及解决方法	13
4.1	kadmin no matching key in entry having a permitted enctype.....	13
4.2	login failure for hue/hacdh01@CLOUDERA from keytab cmon.keytab, connection refused.....	14
4.3	login failure for hue/hacdh01@CLOUDERA from keytab cmon.keytab, krbexception checksum failed	14
	14
	参考	15

1 概述

在一个小型 CDH 集群上（节点个数~5），在某些测试场景下，需要验证 Kerberos 安全认证。本文将描述如何在 CDH 5.4.2，操作系统为 SuSE 11 sp3 上快速安装和配置 Kerberos。

2 安装 MIT Kerberos

2.1 安装 krb5-server krb5-client openldap2-client

在集群中选中一个节点作为 Krb5 服务器，例如 CM 节点，安装 krb5-server krb5-client openldap2-client。执行如下命令

```
zypper install krb5-server krb5-client openldap2-client
```

在其他节点上安装 krb5-client openldap2-client。执行如下命令

```
zypper install krb5-client openldap2-client
```

注意，安装 krb5 后，kdc.conf 文件位于 /var/lib/kerberos/krb5kdc 目录下，而 CentOS 6 下 kdc.conf 文件的目录为 /var/kerberos/krb5kdc。

2.2 修改/etc/krb5.conf

在 Krb5 服务器上（本次操作为 CM 节点）的命令行中逐条执行如下命令

```
# set the Realm
sed -i.orig 's/EXAMPLE.COM/CLOUDERA/g' /etc/krb5.conf
# set the hostname for the kerberos server
sed -i.m1 's/kerberos.example.com/hacdh01/g' /etc/krb5.conf
# change domain name to cloudera
sed -i.m2 's/example.com/cloudera/g' /etc/krb5.conf
```

注意：表格中红色字体为本次测试的主机名，请替换填写正确的主机名。

编辑/etc/krb5.conf 文件，添加如下红色字体内容

```
[libdefaults]
default_realm = CLOUDERA
dns_lookup_kdc = false
dns_lookup_realm = false
ticket_lifetime = 86400
renew_lifetime = 604800
forwardable = true
default_tgs_enctypes = aes256-cts-hmac-sha1-96
default_tkt_enctypes = aes256-cts-hmac-sha1-96
permitted_enctypes = aes256-cts-hmac-sha1-96
udp_preference_limit = 1

[realms]
CLOUDERA = {
kdc = hacdh01
admin_server = hacdh01
}
```

注意：表格中 kdc 和 admin_server 需要正确填写对应的主机名，本例为 hacdh01

2.2 下载 UnlimitedJCEPolicyJDK7.zip 并替换 JDK 目录 jar 文件

```
mkdirjce
cd jce
unzip ../UnlimitedJCEPolicyJDK7.zip
# save the original jar files
cp /usr/java/jdk1.7.0_67-cloudera/jre/lib/security/local_policy.jar local_policy.jar.orig
cp /usr/java/jdk1.7.0_67-cloudera/jre/lib/security/US_export_policy.jar
US_export_policy.jar.orig

# copy the new jars into place
cp /root/jce/UnlimitedJCEPolicy/local_policy.jar /usr/java/jdk1.7.0_67-
cloudera/jre/lib/security/local_policy.jar
cp /root/jce/UnlimitedJCEPolicy/US_export_policy.jar /usr/java/jdk1.7.0_67-
```

```
cloudera/jre/lib/security/US_export_policy.jar
```

2.2 创建 Kerberos 数据库

创建 kerberos 数据库，建议输入密码 cloudera

```
kdb5_util create -s
```

2.2 修改/var/lib/kerberos/krb5kdc/kdc.conf

在 Krb5 服务器上（本次操作为 CM 节点）的命令行中逐条执行如下命令

```
# update the kdc.conf file
sed -i.orig 's/EXAMPLE.COM/CLOUDERA/g' /var/lib/kerberos/krb5kdc/kdc.conf
# this will add a line to the file with ticket life
sed -i.m1 '/dict_file/a max_life = 1d' /var/lib/kerberos/krb5kdc/kdc.conf
# add a max renewable life
sed -i.m2 '/dict_file/a max_renewable_life = 7d' /var/lib/kerberos/krb5kdc/kdc.conf
# indent the two new lines in the file
sed -i.m3 's/^max_/ max_/ ' /var/lib/kerberos/krb5kdc/kdc.conf

# update the kdc.conf file to allow renewable
sed -i.m3 '/supported_enctypes/a default_principal_flags = +renewable, +forwardable'
/var/lib/kerberos/krb5kdc/kdc.conf
# fix the indenting
sed -i.m4 's/^default_principal_flags/ default_principal_flags/'
/var/lib/kerberos/krb5kdc/kdc.conf
```

注意：需要向/var/lib/kerberos/krb5kdc/kdc.conf 文件中手工添加 supported_enctypes，如下红色字体所示。在 CentOS 6 上 kdc.conf 该行默认存在，而 SuSE 11 上没有

```
supported_enctypes = aes256-cts:normal aes128-cts:normal des3-hmac-sha1:normal arcfour-
hmac:normal des-hmac-sha1:normal des-cbc-md5:normal des-cbc-crc:normal
default_principal_flags = +renewable, +forwardable
```

2.2 修改/var/lib/kerberos/krb5kdc/kadm5.acl

```
# theacl file needs to be updated so the */admin
# is enabled with admin privileges
sed -i 's/EXAMPLE.COM/CLOUDERA/' /var/lib/kerberos/krb5kdc/kadm5.acl
```

2.3 启动 kdc 和 admin 服务

启动 kdc server 和 admin server 服务，在 kdc 服务器的命令行中输入如下命令

```
service krb5kdc start
chkconfig krb5kdc on
service kadmind start
chkconfig kadmind on
```

2.3 执行 kadmin 命令

在 kadmin 服务器的命令行中输入如下命令

```
kadmin.local<<eoj
modprinc -maxrenewlife 1week krbtgt/CLOUDERA@CLOUDERA
eoj
# now just add a few user principals
#kadmin: addprinc -pw <Password>
# cloudera-scm/admin@YOUR-LOCAL-REALM.COM

# add the admin user that CM will use to provision
# kerberos in the cluster
kadmin.local<<eoj
addprinc -pw clouderacloudera-scm/admin@CLOUDERA
modprinc -maxrenewlife 1week cloudera-scm/admin@CLOUDERA
eoj
```

```
# add the hdfs principal so you have a superuser for hdfs
```

```
kadmin.local<<eoj
```

```
addprinc -pw clouderahdfs@CLLOUDERA
```

```
eoj
```

```
# add a cloudera principal for the standard user
```

```
# in the Cloudera Quickstart VM
```

```
kadmin.local<<eoj
```

```
addprinc -pw clouderacloudera@CLLOUDERA
```

```
eoj
```

```
# test the server by authenticating as the CM admin user
```

```
# enter the password cloudera when you are prompted
```

```
kinitcloudera-scm/admin@CLLOUDERA
```

```
# once you have a valid ticket you can see the
```

```
# characteristics of the ticket with klist -e
```

```
# you will see the encryption type which you will
```

```
# need for a screen in the wizard, for example
```

```
# Etype (skey, tkt): aes256-cts-hmac-sha1-96
```

```
klist -e
```

3 使用 Cloudera Manager Kerberos 配置向导

3.1 进入 Cloudera Manager



3.1 启用 Kerberos

cloudera manager

主页 群集 主机 诊断 审核 图表 备份 管理

搜索 (Hotkey: /)

支持

admin

Kerberos

状态 凭据

状态

要启用用于这些群集的 Kerberos，请单击下面的启用 **Kerberos** 按钮。

群集

状态

Cluster 1

禁用 Kerberos

启用 Kerberos

安全性检查器

勾选如下四项，点击【继续】



启用 Kerberos 用于 Cluster 1

欢迎

此向导将指导您完成配置 Cloudera Manager 和 CDH 以使用 Kerberos 进行身份验证的步骤。集群中的所有服务以及 Cloudera Management Service 将作为向导的一部分重启。请阅读有关启用 Kerberos 的文档，然后继续使用向导。

使用向导前，请确保已执行以下步骤：

设置正在运行的 KDC。Cloudera Manager 支持 MIT KDC 和 Active Directory。

☒ 是的，我已设置正在运行的 KDC。

KDC 应配置为拥有非零票证生存期和可更新的生存期。如果票证不可更新，则 CDH 不能正常工作。

☒ 是的，我已检查 KDC 允许可更新的票证。

如果想使用 Active Directory，OpenLdap 客户端库应安装在 Cloudera Manager Server 主机中。另外，Kerberos 客户端库应安装在所有主机中。

☒ 是的，我已安装客户端库。

Cloudera Manager 需要有权限在 KDC 中创建其他帐户的帐户。

☒ 是的，我已为 Cloudera Manager 创建适当的帐户。

◀ 返回

1 2 3 4 5 6 7 8 9

▶ 继续

填写 KDC Server 主机以及 Kerberos 加密类型 aes256-cts-hmac-sha1-96，点击【继续】

启用 Kerberos 用于 Cluster 1

KDC 信息

指定有关 KDC 的信息。Cloudera Manager 使用下面的属性生成在群集中运行的 CDH 守护程序的主体。

KDC 类型

- ☒ MIT KDC
☐ Active Directory



KDC Server 主机

kdc

hacdh01



Kerberos 安全领域

default_realm

CLOUDERA



Kerberos 加密类型

aes256-cts-hmac-sha1-96



Kerberos Principal 最大可更新生命期

5 天

[返回](#)

1 2 3 4 5 6 7 8 9

[继续](#)

点击【继续】

启用 Kerberos 用于 Cluster 1

KRB5 配置

指定为群集生成 krb5.conf 所需的属性。可以使用“安全阀”字段指定高级 KDC 设置的配置；例如，使用跨领域身份验证。

通过 Cloudera Manager 管理
krb5.conf

Kerberos 票证生存期
ticket_lifetime

1 天

Kerberos 可更新生存期
renew_lifetime

7 天

DNS 查找 KDC
dns_lookup_kdc

☐

可转发票证
forwardable

☒

krb5.conf 的 [libdefaults] 小节的高级
配置代码段（安全阀）

krb5.conf 的默认领域的高级配置代码段
（安全阀）

返回

1 2 3 4 5 6 7 8 9

继续

启用 Kerberos 用于 Cluster 1

KDC Account Manager 凭据

输入有权限创建其他用户的帐户的凭据。Cloudera Manager 将以加密形式存储该凭据并在需要生成新主体时使用它。

用户名 @
密码

[返回](#)

1 2 3 4 5 6 7 8 9

[继续](#)

点击【继续】，直至配置完成。

4 常见问题及解决方法

4.1 kadmin no matching key in entry having a permitted enctype

krb5.conf 和 kdc.conf 不一致，在 SuSE 11 环境里，需要向 kdc.conf 文件中手工添加
master_key_type = aes256-cts

```
[realms]  
CLOUDERA = {  
master_key_type = aes256-cts  
acl_file = /var/kerberos/krb5kdc/kadm5.acl
```

```
dict_file = /usr/share/dict/words
max_renewable_life = 7d
max_life = 1d
admin_keytab = /var/kerberos/krb5kdc/kadm5.keytab
supported_enctypes = aes256-cts:normal aes128-cts:normal des3-hmac-sha1:normal arcfour-
hmac:normal des-hmac-sha1:normal des-cbc-md5:normal des-cbc-crc:normal
default_principal_flags = +renewable, +forwardable
}
```

4.2 login failure for hue/hacdh01@CLUDERA from keytabcmon.keytab, connection refused

向 kdc.conf 文件的 kdcdefaults 部分添加 kdc_tcp_ports

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

4.3 login failure for hue/hacdh01@CLUDERA from keytabcmon.keytab, krbexception checksum failed

1. 停止集群服务
2. 重新生成所有 keytabs
3. 启动集群服务

参考

<http://blog.cloudera.com/blog/2015/03/how-to-quickly-configure-kerberos-for-your-apache-hadoop-cluster/>