UDH Keberos安全认证机制简介

目录

[UDH Keberos安全认证机制简介 1](#_Toc418010271)

[1、 Hadoop 的安全认证机制 1](#_Toc418010272)

[2、 Kerberos安全认证协议 1](#_Toc418010273)

[3、 搭建Keberos 2](#_Toc418010274)

[4、 Keberos 用户操作 4](#_Toc418010275)

在UDH上使用Keberos认证，它会根据所安装的服务生成对应主机和服务的principal、keytab等信息的csv文件，并且在启动后通过脚本自动生成keytab存放到对应主机目录上（/etc/security/keytabs）。

所以，只需在安装完KDC 环境执行UDH中kerberos-setup.sh脚本，UDH就能够完成大部分的初始化工作。

#### Hadoop 的安全认证机制

简单来说,没有做kerberos认证的Hadoop，只要有client端就能够连接上。而且，通过一个有root的权限的内网机器，通过创建对应的linux用户，就能够得到Hadoop集群上对应的权限。

而实行Kerberos后，任意机器的任意用户都必须现在Kerberos的KDC中有记录，才允许和集群中其它的模块进行通信。

#### Kerberos安全认证协议

Kerberos是一种网络认证协议，其设计目标是通过密钥系统为客户机 / 服务器应用程序提供强大的认证服务。

简单介绍：

使用Kerberos时，一个客户端需要经过三个步骤来获取服务:

认证：客户端向认证服务器发送一条报文，并获取一个含时间戳的Ticket-Granting Ticket（TGT）。

授权：客户端使用TGT向Ticket-Granting Server（TGS）请求一个服务Ticket。

服务请求：客户端向服务器出示服务Ticket，以证实自己的合法性。该服务器提供客户端所需服务，在Hadoop应用中，服务器可以是namenode或jobtracker。

为此，Kerberos需要The Key Distribution Centers（KDC）来进行认证。KDC只有一个Master，可以带多个slaves机器。slaves机器仅进行普通验证。Mater上做的修改需要自动同步到slaves。

另外，KDC需要一个admin，来进行日常的管理操作。这个admin可以通过远程或者本地方式登录。

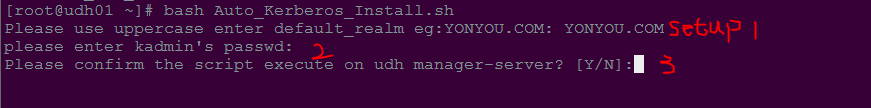
#### 搭建Keberos

**a. UDH集群内环境安装**

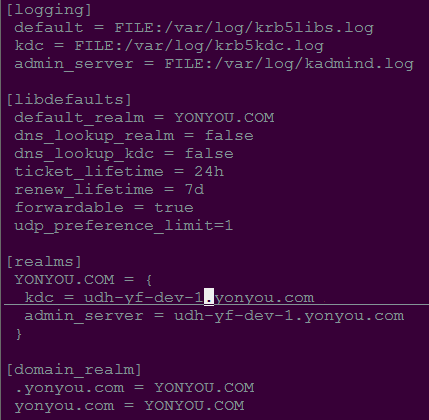
    环境：udh-yf-dev-1~udh-yf-dev-4， 选择udh-yf-dev-1，udh-yf-dev-2，udh-yf-dev-3组成分布式的KDC，udh-yf-dev-1作为Master机器，

安装：通过执行Auto\_Kerberos\_Install.sh 脚本自动安装，

* setup1.根据提示填写KDC的realm 域 如：YONYOU.COM
* setup2.设置kadmin的密码，注意这里的密码也是kdc数据库的密码
* setup3.确认是否执行在UDH server所在机器上



配置说明： Kerberos的配置文件只有两个，分别为/etc/krb5.conf、/var/kerberos/krb5kdc/kdc.conf，Keberos脚本根据集群环境相应主机生成默认配置文件，/etc/krb5.conf :包含Kerberos的配置信息。例如，KDC的位置，Kerberos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。



    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 = YONYOU.COM 默认的realm，必须跟要配置的realm的名称一致。

        udp\_preference\_limit = 1 禁止使用udp可以防止一个Hadoop中的错误

        [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

/var/kerberos/krb5kdc/kdc.conf:包括KDC的配置信息



说明：

YONYOU.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。

max\_renewable\_life = 7d 涉及到是否能进行ticket的renwe必须配置。

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。推荐不使用。

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]**

支持通配符等。最简单的写法是

**\*/admin@YONYOU.COM      \***

代表名称匹配\*/admin@YONYOU.COM 都认为是admin，权限是 \*。代表全部权限。

admin\_keytab:KDC进行校验的keytab。后文会提及如何创建。

supported\_enctypes:支持的校验方式。注意把aes256-cts去掉。

注意：执行完Kerboers安装脚本，已经初始化KDC数据库、同步配置到所有slave kdcs 并启动。

**b.UDH集群外环境安装**

     新增一个节点作为KDC server，只需在执行Auto\_Kerberos\_Install.sh脚本setup3填写N就可以了，脚本安装后的环境一样，这里不在重复介绍。

#### Keberos 用户操作

**a. 查看当前的认证用户：klist**

**b. 认证用户：kinit -k -t  /xxx/xxx/kerberos.keytab hdfs/udh-yf-dev-1.yonyou.com**

**c. 删除当前的认证的缓存：kdestroy**

启动、停止、重启命令

 /etc/init.d/krb5kdc start|stop|restart

 /etc/init.d/kadmin  start|stop|restart