**UDH安全配置手册**

**（V1.0.1）**

目录

[1. Kerberos简介 1](#_Toc419991577)

[2. UDH启用安全系统 1](#_Toc419991578)

[2.1. 安装Kerberos前准备 1](#_Toc419991579)

[2.2. 安装Kerberos 2](#_Toc419991580)

[2.3. 配置安全 2](#_Toc419991581)

[2.3.1. 启用安全 3](#_Toc419991582)

[2.3.2. 创建Principals和Keytabs 3](#_Toc419991583)

[2.3.3. 应用安全 4](#_Toc419991584)

[2.4. 服务检测 4](#_Toc419991585)

[2.4.1. 运行服务检测 5](#_Toc419991586)

[2.4.2. HTTP Spnego 检测 5](#_Toc419991587)

[3. UDH禁用安全系统 5](#_Toc419991588)

# Kerberos简介

“Kerberos 是一种在**不可信网络**上对**可信任主机**之间的认证协议”，即在开放、不安全的网络上，主机之间的通信可能被拦截，Kerberos协议用于在这样的网络上提供可靠的认证服务。但如果使用的计算机很容易受到攻击，Kerberos则无法提供任何保证：认证服务器、应用服务器（imap, pop, smtp, telnet, ftp, ssh , AFS, lpr, ...）、客户端必须保持密码的周期性更新，以保证请求服务的用户和服务提供者之间的正确认证。

例如，如果某人获取了一台机器的特许访问权限，可以复制包含密钥的文件，则Kerberos的认证策略就失去用途了。侵入者可以复制密钥文件到另一台机器上，设置相同的DNS和IP，认证服务器会认为它就是真正的客户端。

# UDH启用安全系统

## 安装Kerberos前准备

在UDH环境下安装Kerberos需要**注意**：

* **NameNode与DataNode分开安装**
* **SNameNode与DataNode分开安装**
* **NameNode与SNameNode分开安装**
* **ResouceManager与NodeManager分开安装**

**即上述各条中的组件不能同时安装在一个节点上（NameNode可与ResouceManager安装于同一节点），否则容易造成启用安全后，服务无法启动。**

安装配置好UDH后，若需要启用安全系统，需要经历以下三个步骤：安装kerberos，配置UDH安全，运行服务检测。

## 安装Kerberos

UDH提供Kerberos的自动安装脚本：kerberos\_install.sh。该脚本在执行的服务器上安装KDC，即krb5-server。

在脚本路径下执行：

#bash ./kerberos\_install.sh

将出现以下提示信息：

>>Please use uppercase enter default\_realm eg:YONYOU.COM: **YONYOU.COM**

>>Please enter kadmin's passwd:

>>Please confirm the script execute on udh manager-server? [Y/N]:

安装过程中按提示输入即可。

这里，**脚本支持KDC两种安装方式**：

1. UDH Manager机器上部署

即在安装UDH的集群内的一台机器上执行kerberos\_install.sh脚本，并在**Please confirm the script execute on udh manager-server? [Y/N]:**步骤选择**Y，说明将在安装UDH的集群中部署kerberos，部署范围涉及整个集群。**

1. UDH集群外独立机器上部署

即在安装UDH的集群外的一台机器上执行kerberos\_install.sh脚本，并在**Please confirm the script execute on udh manager-server? [Y/N]:**步骤选择**N，说明将在UDH集群外机器上安装KDC，在UDH集群内的机器上安装client, 部署范围涉及执行脚本的服务器中/etc/hosts下的所有域内机器（@yonyou.com）。**

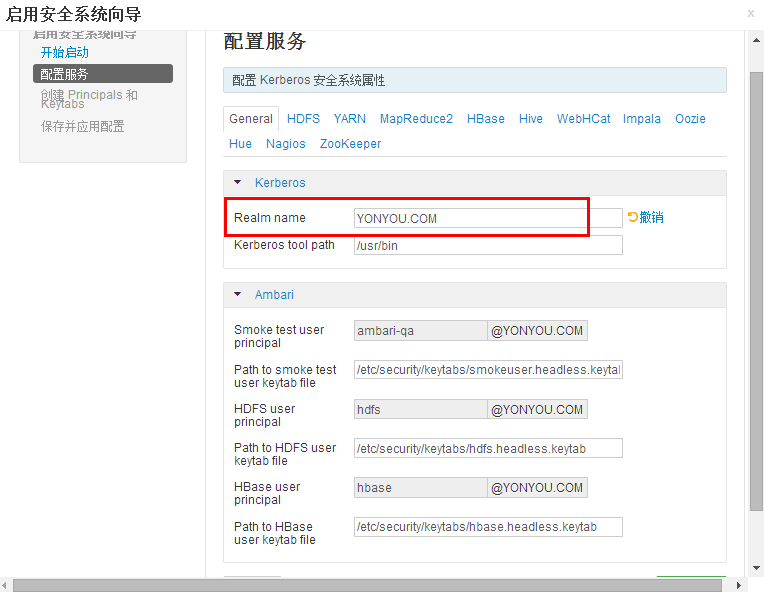
## 配置安全

安装配置好Kerberos后，在管理菜单里选择“安全”，点击“启用安全系统”。

### 启用安全

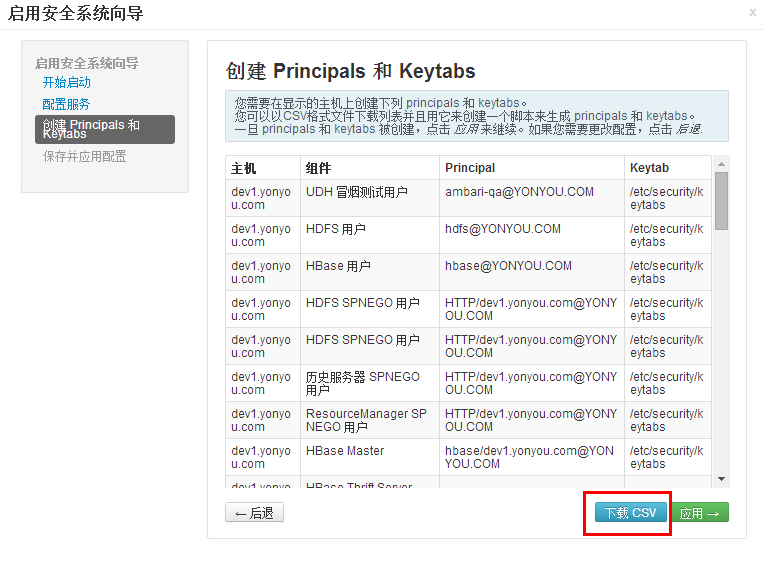
1. 指定Kerberos的Realm域：本例中设置为YONYOU.COM；

2、（可选）修改各服务的Principal名称及Keytab文件的存储位置，建议保持原值；



### 创建Principals和Keytabs

导出用于生成Principal及Keytab的CSV文件，上传到KDC所在的服务器。因为KDC要生成Keytab文件，并分发到各客户端，也就是Hadoop集群里的每一台机器上，所以要保证KDC可以无密码访问这些客户端。在UDH中，我们的策略是将KDC部署在集群的主节点（master）上面，这样就可以方便的生成Principal并将相应的Keytab文件分发送到各从节点。同时，启用了安全认证的集群里每个服务都需要进行安全配置，所以我们统一生成配置文件，并在下面的步骤里重启整个集群。



在CSV上传到KDC（UDH主节点）之后，执行以下命令，系统将生成所有的Principal及Keytab文件，并分发到相应的Kerberos客户端上。其中，各客户端上Keytab文件存放的路径与步骤1中配置服务页面中的Keytab文件路径一致。

***/var/lib/ambari-server/resources/scripts/kerberos-setup.sh /root/tools/host-principal-keytab-list.csv /root/.ssh/***

其中参数’ *host-principal-keytab-list.csv*’是我们导出的CSV文件，参数’ */root/.ssh/*’是SSH目录，系统要读取该目录下的密钥。

注意，必须先**下载CSV**，生成Principal及Keytab文件之后，才可以点击**应用**按钮，否则系统将无法启动！

### 应用安全

点击页面的‘应用’按钮，系统将停止所有服务，并在应用所有服务的安全配置后，重新启动所有服务，集群进入安全系统运行模式。这个过程可能用时较长，通常要十几分钟或更长时间，请耐心等待，不要在部署过程中点击确定（或者是同意）按钮。

## 服务检测

启用安全后，在各服务的“配置”界面中，非log4j.properties的“自定义配置文件”下，都显示了该服务安全相关的配置项，可进行查看。

### 运行服务检测

各服务界面右上角处有“服务操作”按钮，点击下拉菜单中的“运行服务检测”可执行该服务的安全验证脚本，运行成功意味着该服务在安全模式下可正常运行。

### HTTP Spnego 检测

基本上需要网页访问的服务都需要进行HTTP Spnego验证

1、各节点执行kinit(使用具体的主机名和域名替代{{hostname@REALM}}):

kinit –k –t /etc/security/keytabs/spnego.service.keytab HTTP/{{hostname@REALM}}

2、安装VNC

yum install tigervnc

yum install tigervnc-server

vncserver :18

1. 下载VNC Viewer并安装。打开 VNC Viewer，安装Firefox，输入：

yum install firefox

1. 在VNC Viewer中打开Firefox，进行如下配置：

* 在地址栏输入‘about:config’，回车；
* 在过滤器内输入过滤条件‘network.negotiate-auth.trusted-uris’；
* 双击条目，在输入框内输入要访问的主机列表，主机之间以逗号分隔‘hostname1.yonyou.com, hostname2.yonyou.com, hostname3.yonyou.com, hostname 4.yonyou.com’

1. 打开HDFS页面，例如：http:// hostname1.yonyou.com:50070

如果提示需要进行HTTP认证，在dev1上执行如下命令：

kinit -k -t /etc/security/keytabs/spnego.service.keytab [HTTP/ hostname1.yonyou.com@YONYOU.COM](mailto:HTTP/%20hostname1.yonyou.com@YONYOU.COM)

**注意：测试过程中需要针对不同的服务设置用户:**

如HDFS需要：

kinit -k -t /etc/security/keytabs/hdfs.headless.keytab [hdfs/hostname1.yonyou.com@YONYOU.COM](mailto:hdfs/hostname1.yonyou.com@YONYOU.COM)或

kinit -k -t /etc/security/keytabs/hdfs.headless.keytab [hdfs@YONYOU.COM](mailto:hdfs@YONYOU.COM)

# UDH禁用安全系统

UDH禁用安全系统比启用操作更为简单，只需在管理菜单里选择“安全”，点击“禁用安全系统”即可。