# 1、生成keytab文件

**1、在AD域中，创建1个域账号，密码设置为永不过期**

**2、使用上面创建的域账号，创建SPN（服务主体名称）**

**SPN：**Kerberos身份验证使用SPN将服务实例与服务登录帐户相关联

使用administrator账户登录AD域控服务器，在命令行运行以下命令：

setspn -S [HTTP/cas.test.com@apitest.domain.com](mailto:HTTP/cas.test.com@apitest.domain.com) loginName

参数说明：

cas.test.com：CAS服务器域名

apitest. domain.com：AD域服务器的域名

loginName：域登录账号

**3、生成keytab文件**

使用administrator账户登录AD域服务器，在命令行运行以下命令：

ktpass /out cas.keytab /princ HTTP/cas.test.com@APITEST.DOMAIN.COM /pass \* /mapuser loginName@APITEST. DOMAIN.COM /ptype KRB5\_NT\_PRINCIPAL /crypto RC4-HMAC-NT

参数说明：

cas.keytab：生产的keytab文件

cas.test.com：CAS服务器域名

APITEST.DOMAIN.COM：AD域服务器的域名（大写）

loginName：域登录账号

# 2、搭建Kerberos

Kerberos和CAS需要安装在同一台服务器上，且该服务器必须有域名

1、解压缩安装包：krb5-1.17.tar.gz（Linux版）

2、进入到安装包src目录下，编译安装

./configure

make && make install

3、修改Kerberos配置文件 /etc/krb5.conf

[logging]

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

kdc = FILE:/var/log/krb5kdc.log

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

[libdefaults]

ticket\_lifetime = 24000

default\_realm = APITEST.PACTERA.COM

default\_keytab\_name = /root/cas.keytab

dns\_lookup\_realm = true

dns\_lookup\_kdc = true

default\_tkt\_enctypes = rc4-hmac

default\_tgs\_enctypes = rc4-hmac

[realms]

APITEST.PACTERA.COM = {

kdc = apitest.pactera.com:88

}

[domain\_realm]

.apitest.pactera.com = APITEST.PACTERA.COM

apitest.pactera.com = APITEST.PACTERA.COM

3、查看是否安装成功

klist



# 3、搭建CAS

1、添加依赖

<dependency>

<groupId>org.apereo.cas</groupId>

<artifactId>cas-server-support-spnego-webflow</artifactId>

<version>${cas.version}</version>

</dependency>

<dependency>

<groupId>org.apereo.cas</groupId>

<artifactId>cas-server-support-ldap</artifactId>

<version>${cas.version}</version>

</dependency>

2、添加配置

#如果在域环境中，使用域账户登录，免登

cas.authn.spnego.kerberosConf=/etc/krb5.conf

cas.authn.spnego.jcifsServicePrincipal=HTTP/cas.test.com@APITEST.PACTERA.COM

cas.authn.spnego.loginConf=classpath:login.conf

cas.authn.spnego.kerberosKdc=10.12.30.160

cas.authn.spnego.jcifsDomain=cas.test.com

cas.authn.spnego.kerberosDebug=true

cas.authn.spnego.kerberosRealm=APITEST.PACTERA.COM

cas.authn.spnego.ntlm=false

cas.authn.spnego.jcifsServicePassword=abcd-123 #生成keytab文件域账号的密码

#不是域用户，需要输入域账号密码登录

cas.authn.ldap[0].type=AUTHENTICATED

cas.authn.ldap[0].ldapUrl=ldap://172.16.253.237:389

cas.authn.ldap[0].useSsl=false

cas.authn.ldap[0].connectTimeout=5000

cas.authn.ldap[0].baseDn=DC=apitest,DC=pactera,DC=com

cas.authn.ldap[0].userFilter=(|(sAMAccountName={user})(mail={user})(mobile={user}))

cas.authn.ldap[0].subtreeSearch=true

cas.authn.ldap[0].bindDn=shiyonghui

cas.authn.ldap[0].bindCredential=abcd-123

3、添加配置文件login.conf（指定keytab文件位置）

jcifs.spnego.initiate {

com.sun.security.auth.module.Krb5LoginModule required storeKey=true useKeyTab=true keyTab="/root/cas.keytab";

};

jcifs.spnego.accept {

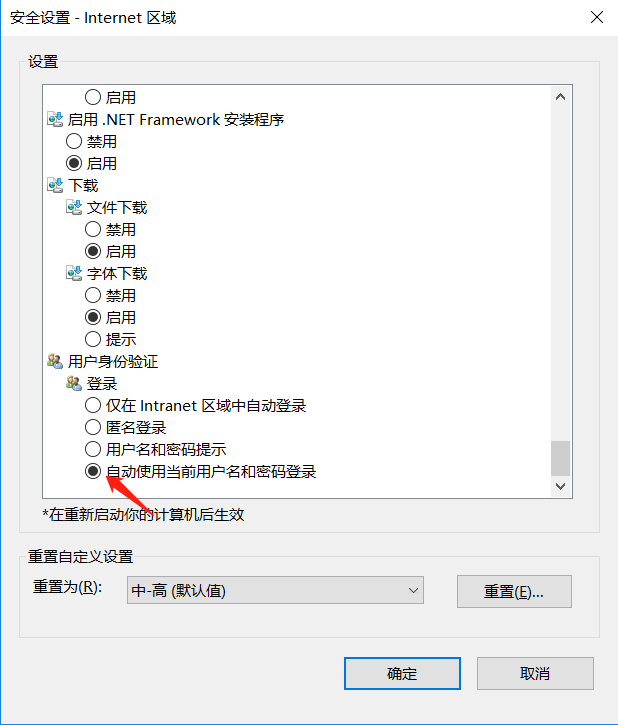
com.sun.security.auth.module.Krb5LoginModule required storeKey=true useKeyTab=true keyTab="/root/cas.keytab";

};

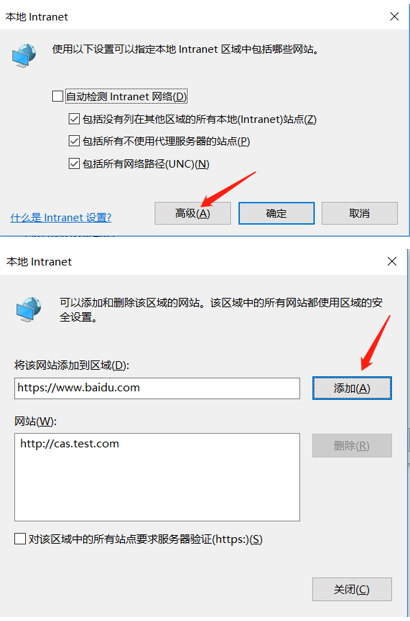
# 4、浏览器配置

免密登录，需要浏览器开启windows身份验证。

1. **IE开启windows身份验证**
2. 工具 - Internet选项 – 安全 – 自定义级别 – 自动使用当前用户名和密码登录



2）本地Intranet – 站点 – 高级 – 添加（CAS登录地址）



1. **谷歌浏览器开启windows身份验证**

IE开启后，谷歌浏览器不需要配置