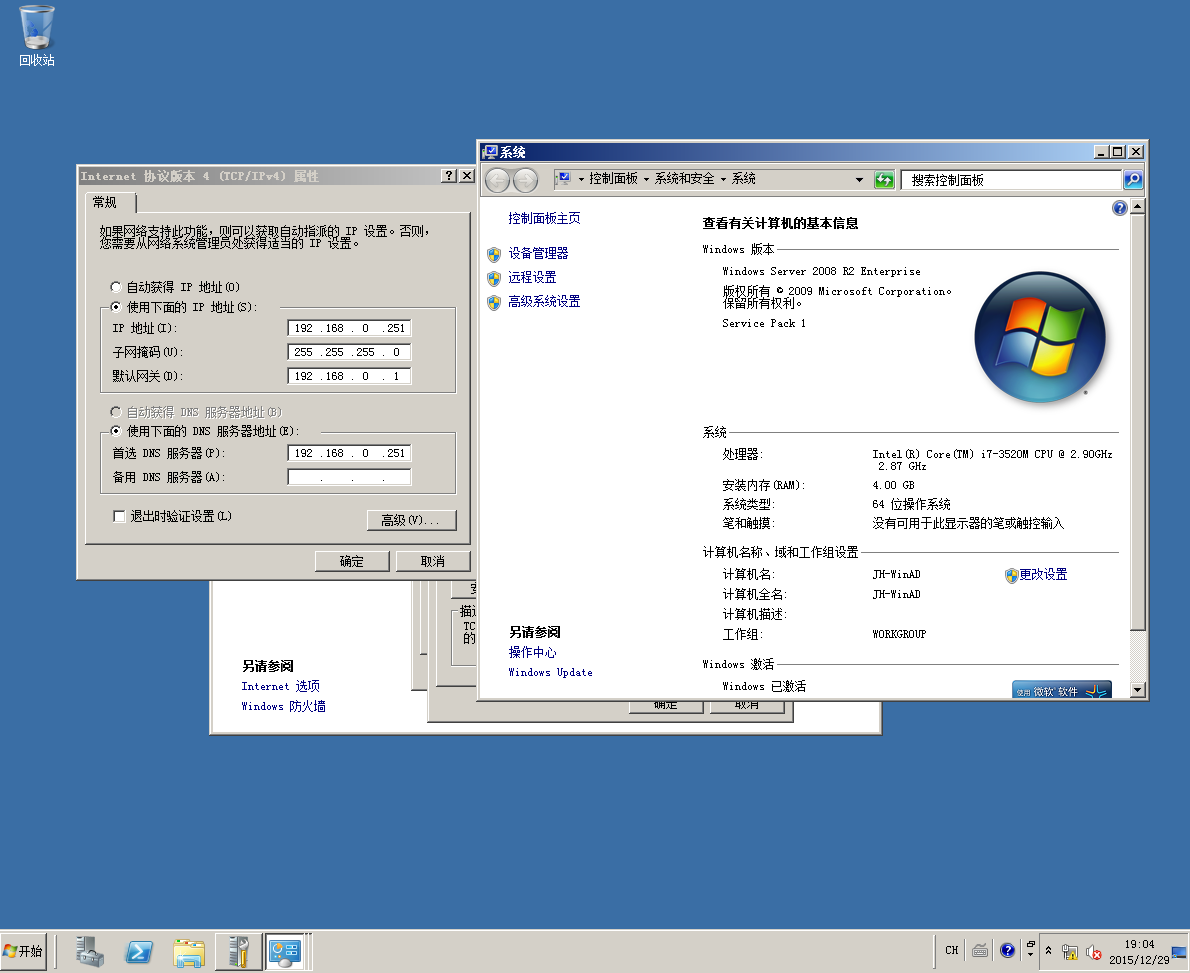
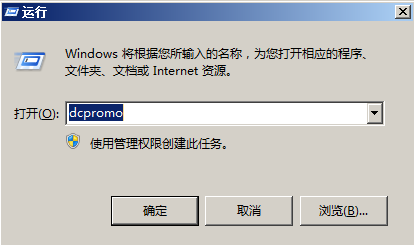
Windows Server 2008 安装AD和配置证书

1. 安装AD服务

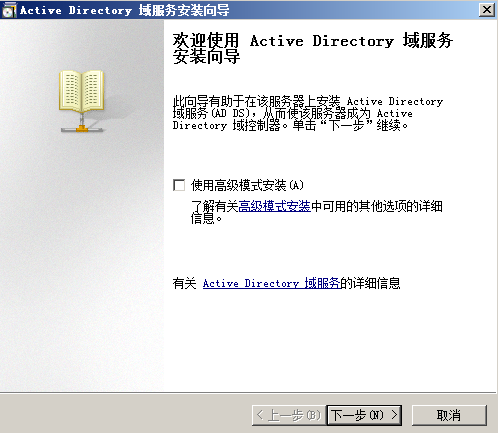
如下图，是全新的windows 2008 R2，已配置系统的ip和hostname。



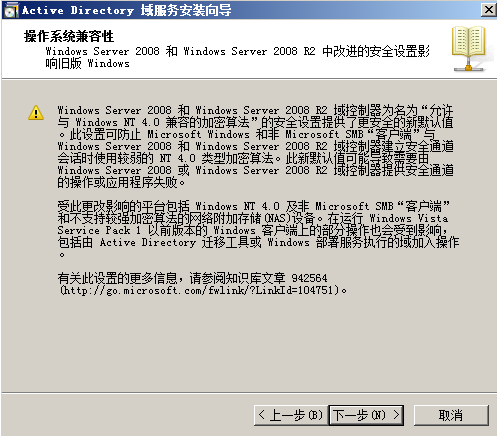
win+R打开命令行，输入：dcpromo /forceremoval



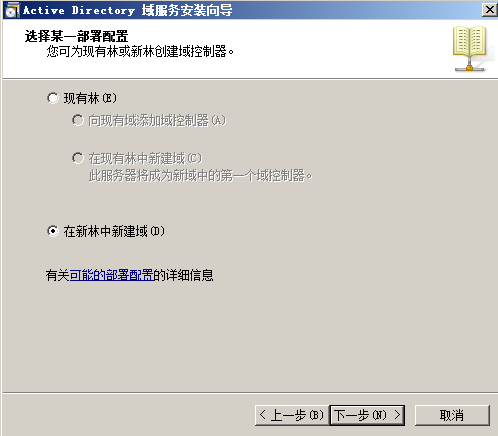
直接按图选择下一步，



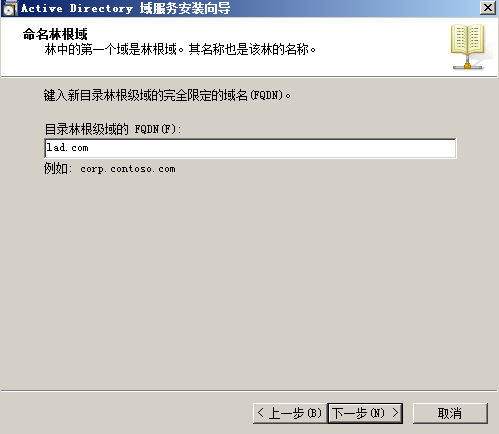
选择下一步，



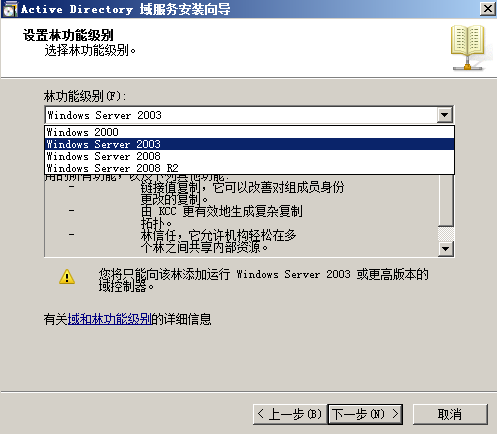
这里我们选择在新林中新建域（因为是全新安装），选择下一步



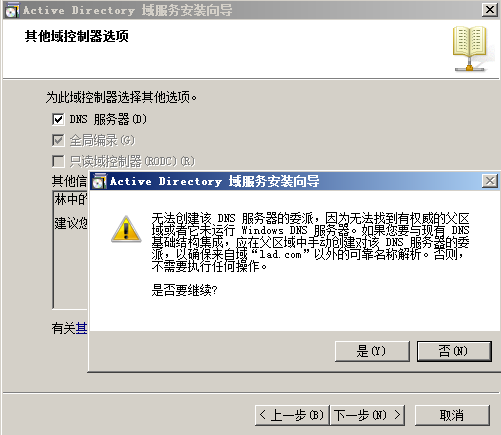
输入域名，这里输入的是jhtest.com，选择下一步



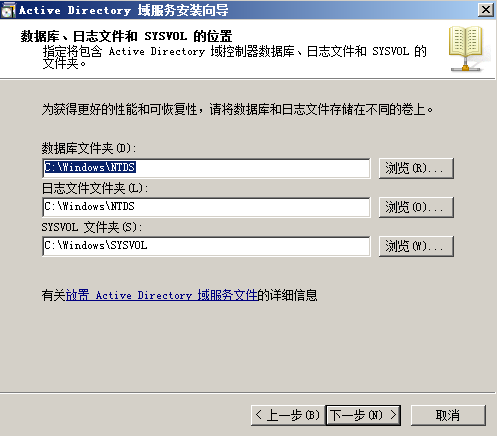
选择林功能级别，考虑向下兼容性的话，选择Windows Server 2003，我这里选择的是Windows Server 2003，下一步。



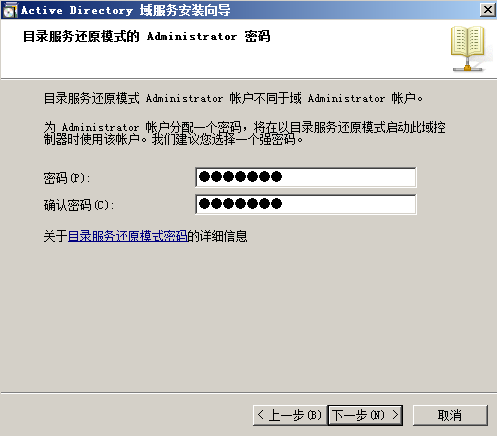
下一步，选择“是”，下一步，



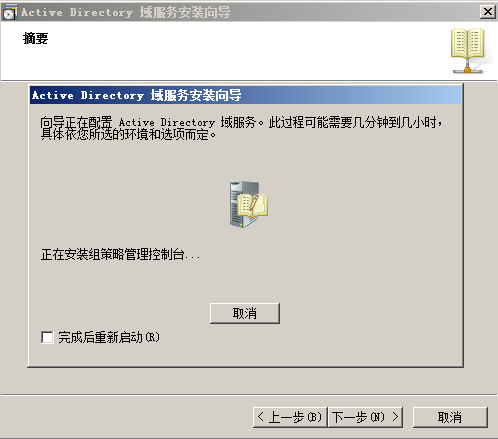
保持默认，选择下一步，



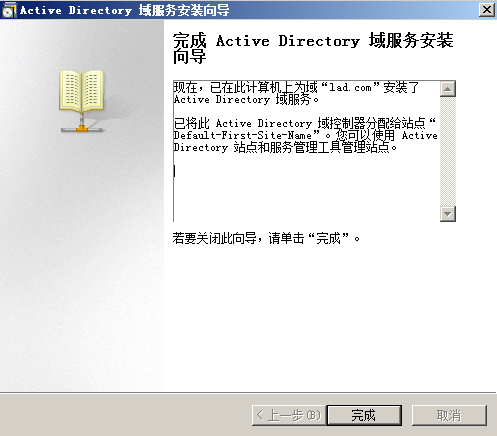
输入密码，这里输入了Jhadm1n



下一步



点击完成，重启。



1. 安装AD证书服务

添加AD证书，



点击确认，全部默认安装，然后选择安装

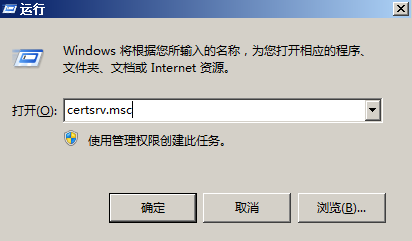


点击关闭

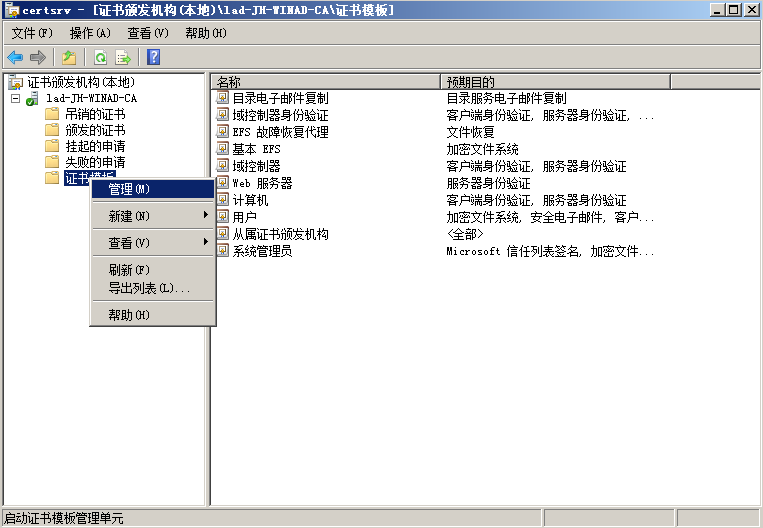


1. 生成证书

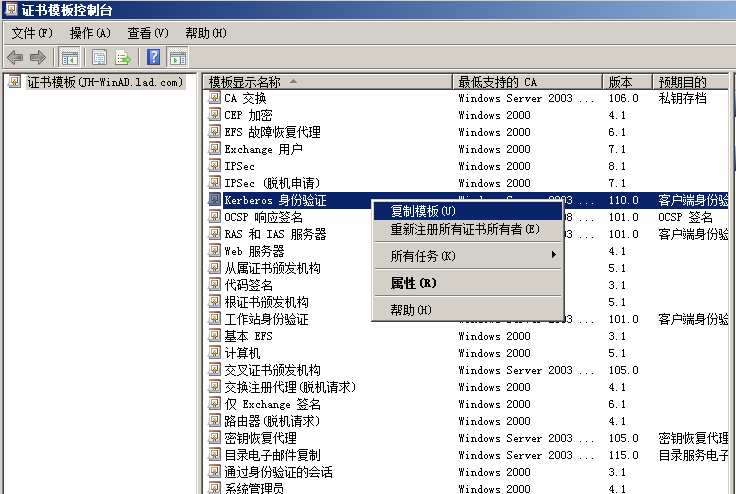
win+R 打开命令行，输入certsrv.msc



右键点击证书模板，选择管理



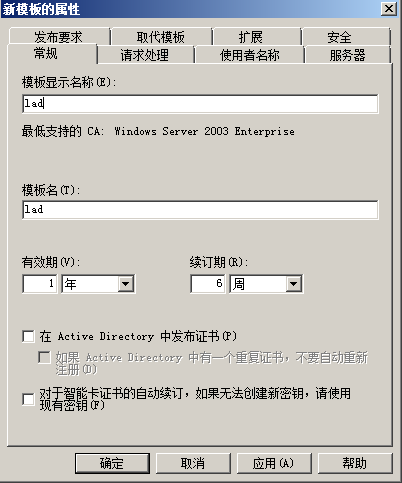
选中 Kerberos 身份验证，点击右键，选择复制模板



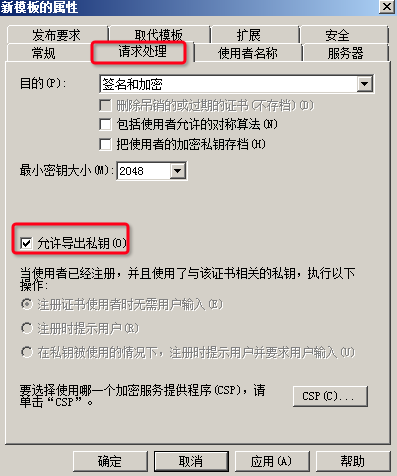
选择默认



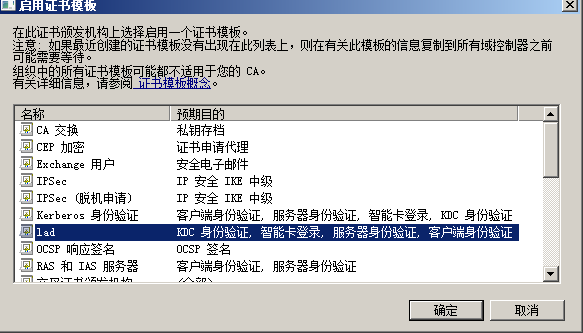
输入模板名，我这里输入了lad



请求处理，选中允许导出私钥



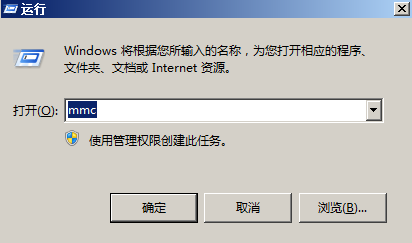
回到certsrv窗口，选择证书模板，右键选择新建->要颁发的证书模板



选择前面复制的证书模板，点击确定。

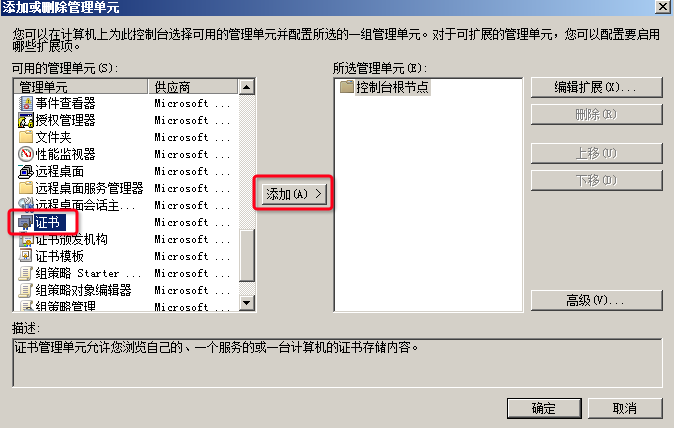
1. 导出证书

win+R 打开命令行，输入mmc

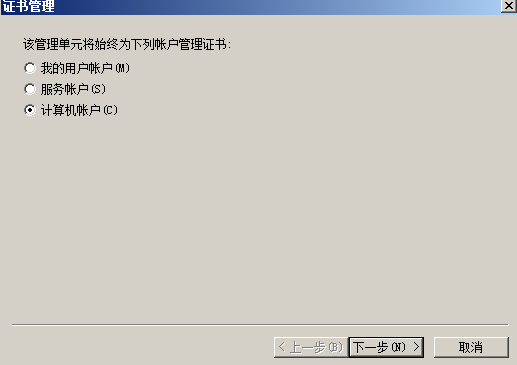


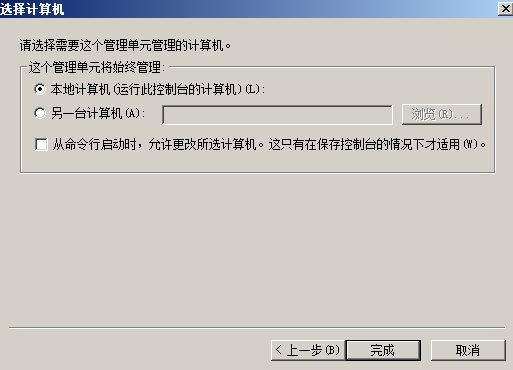
点击文件->添加/删除管理单元

选择证书，点击添加



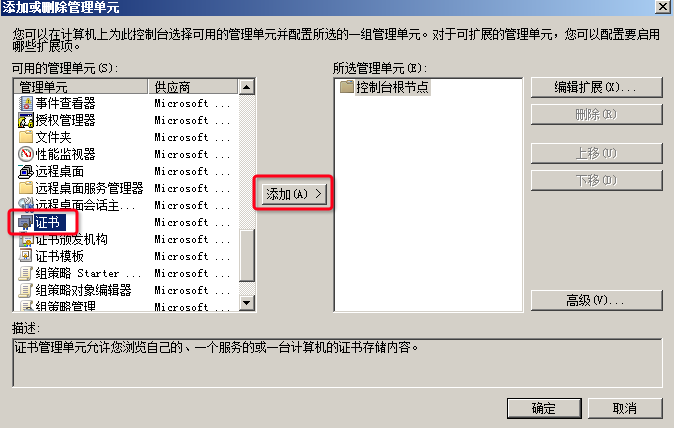
选择计算机账号，下一步



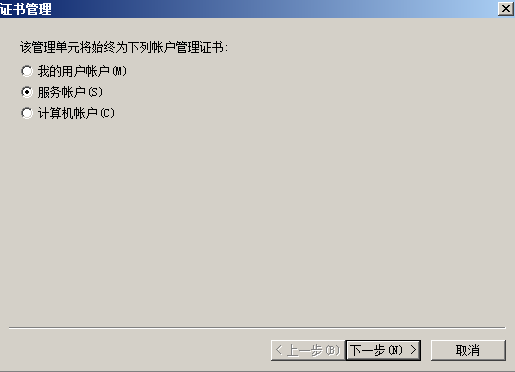


默认，点击完成。

再次选择证书，点击添加



选择 服务账户



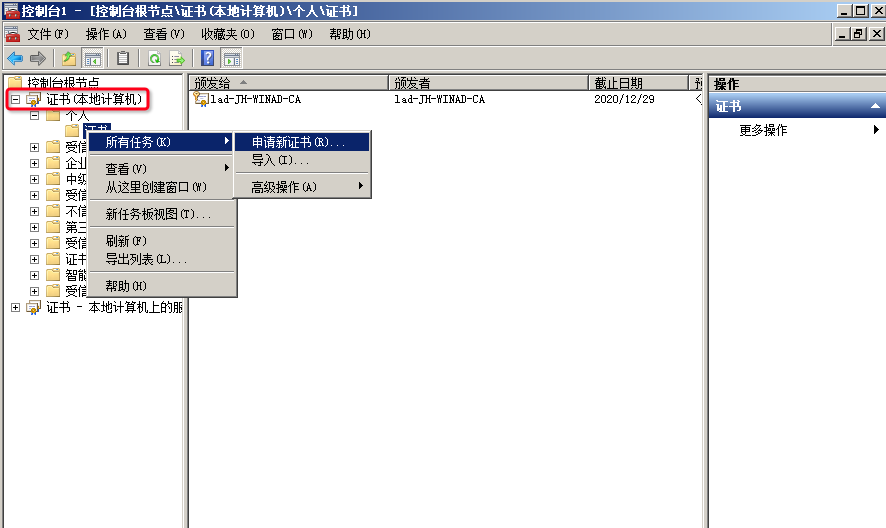
默认下一步

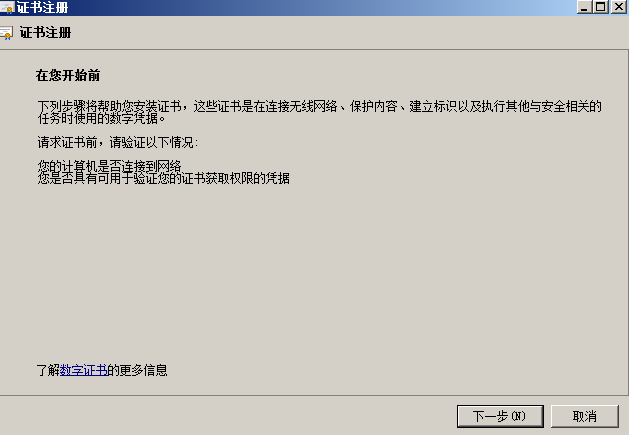


选择Active Directory Domain Services，点击完成，

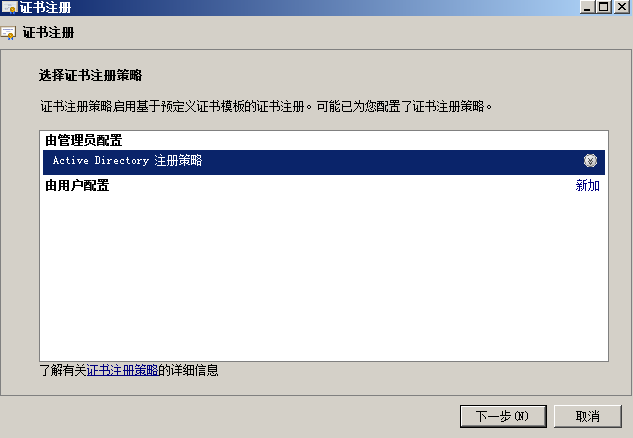
点击确定。

首先，选择证书（本地计算机）展开个人，右击证书，选择所有任务->申请新证书





默认下一步

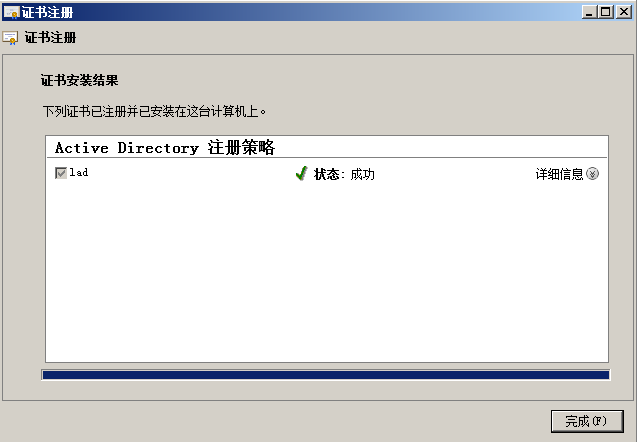


默认下一步

选中前面的lad证书模板，下一步

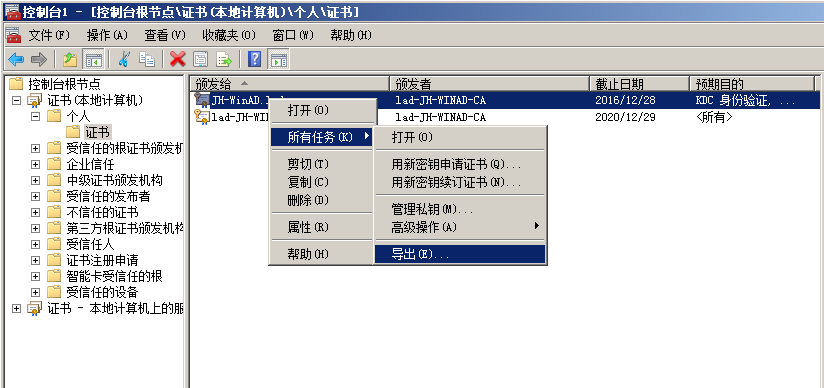


点击注册

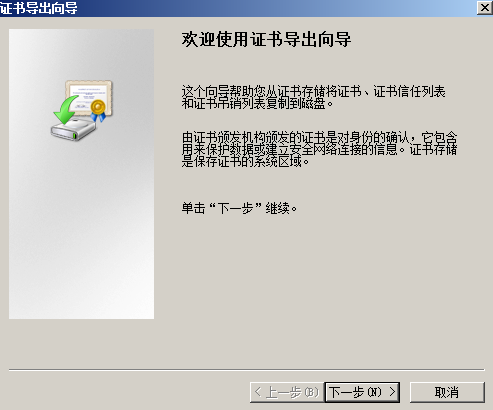


点击完成

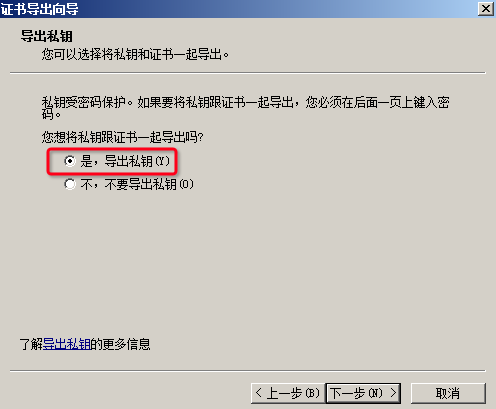
选择新建的证书，右键，选择所有任务->导出



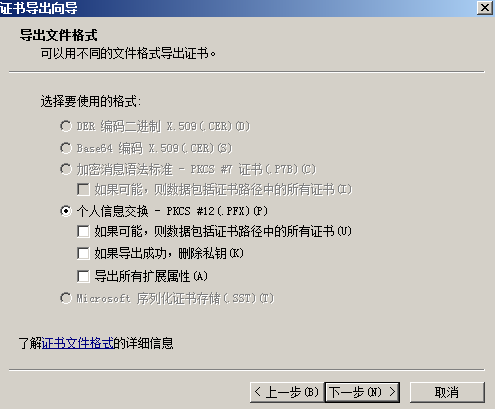
默认下一步



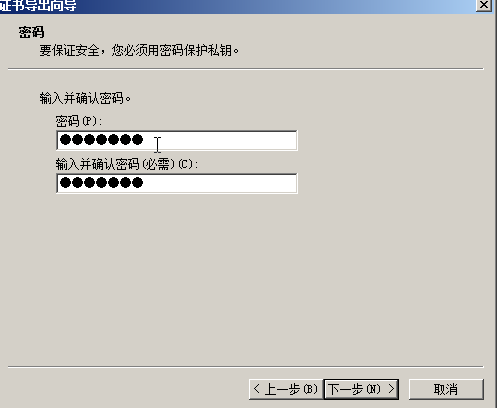
选择是，导出私钥，下一步



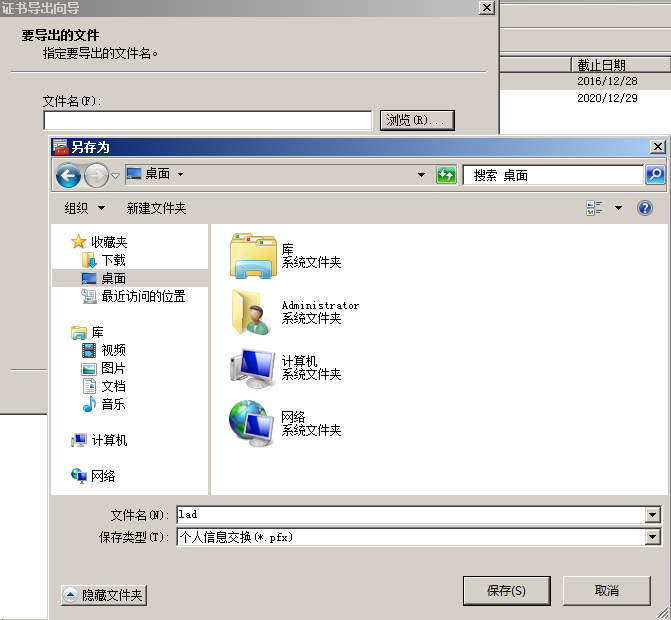
默认下一步

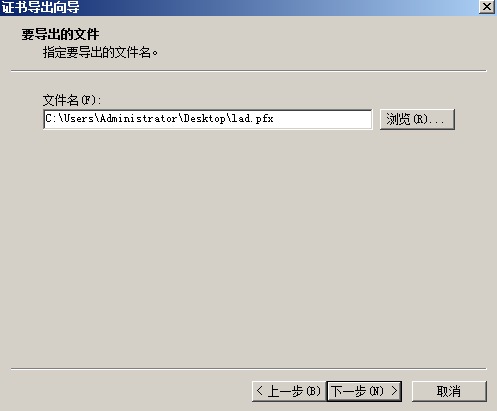


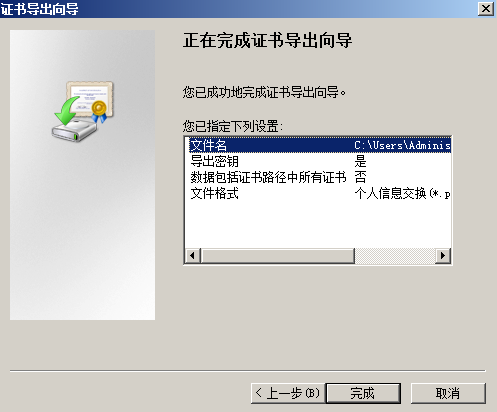
输入密码，这里我输入了Jhadm1n，这个密码后面要用，需记住。



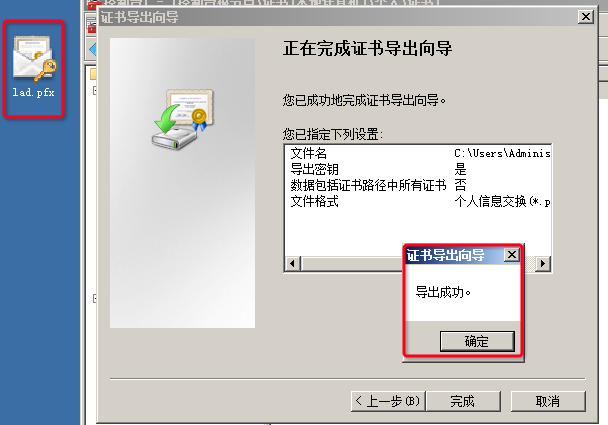
选择保存的路径，我保存在桌面，名称为lad



下一步

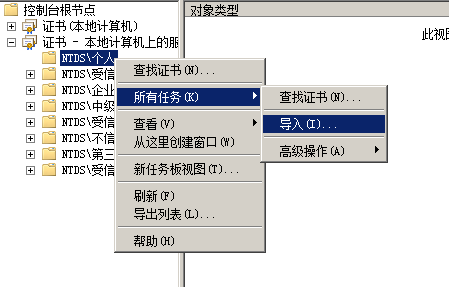


点击完成。



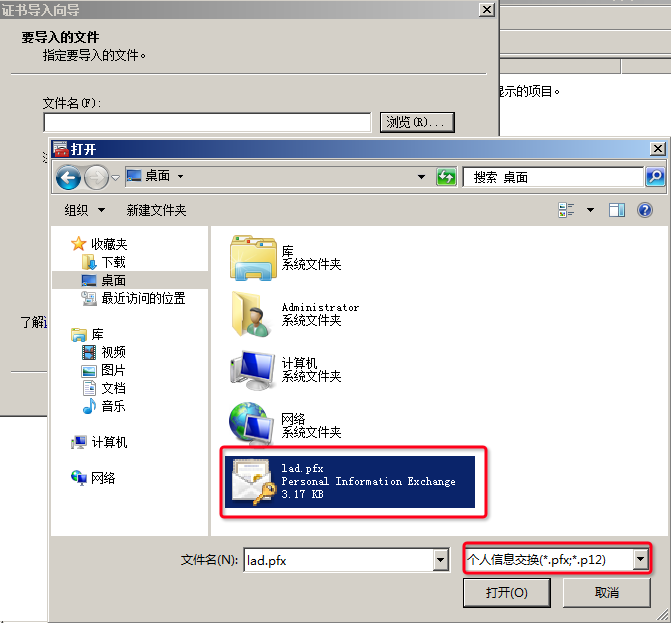
展开证书-本地计算机上的服务

右击NTDS\个人，选择所有任务->导入

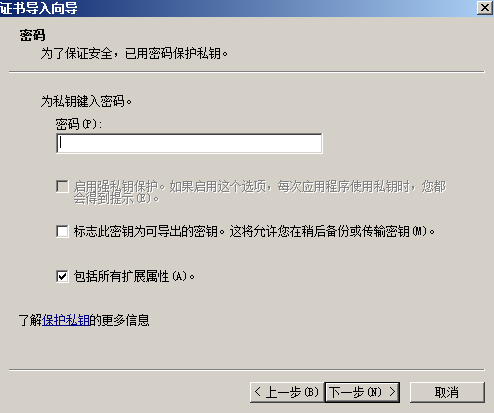


默认下一步

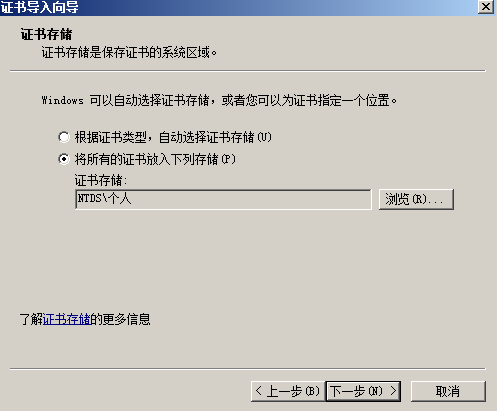
选择刚才保存的pfx文件，我保存在桌面



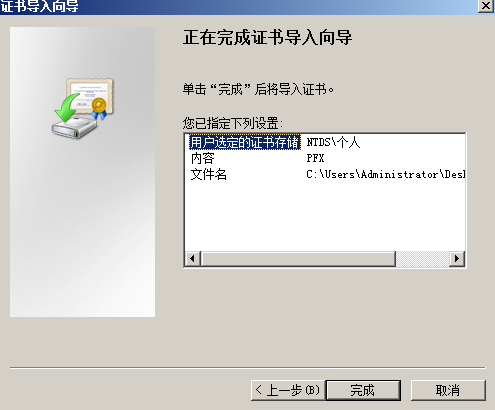
输入密码，密码为刚才导入时的密码，我的是Jhadm1n



默认下一步

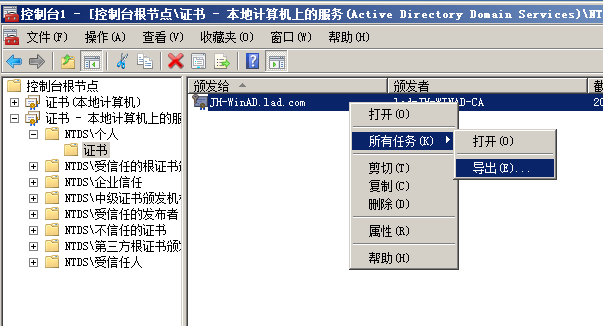


点击完成

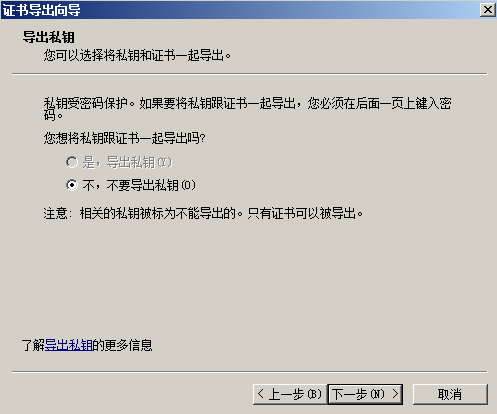


选择“NTDS\个人”下面的证书，

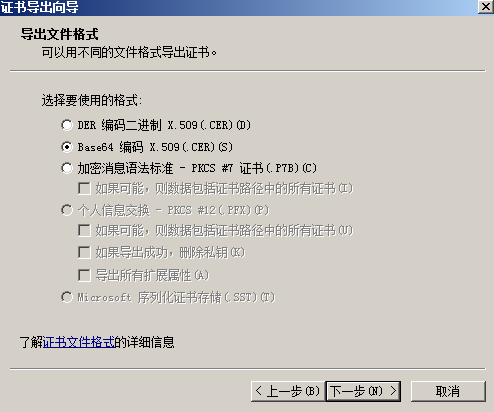
在右边选择刚才导入的证书，选择所有任务->导出



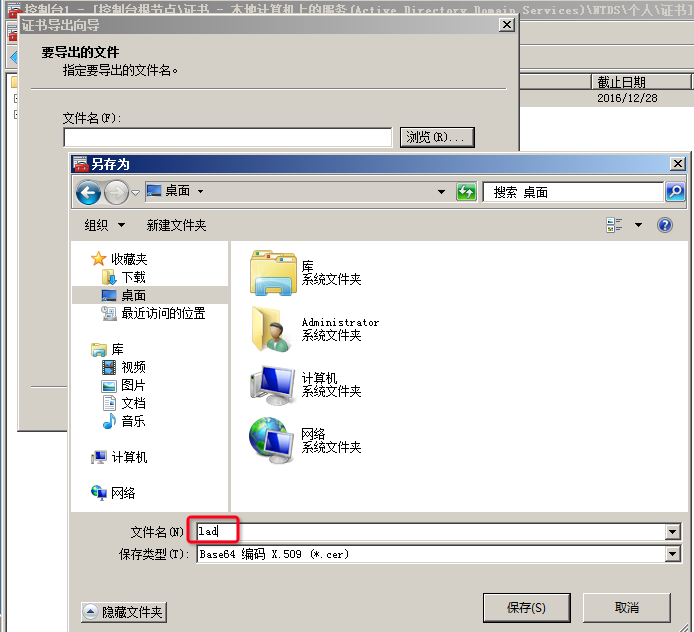
默认下一步

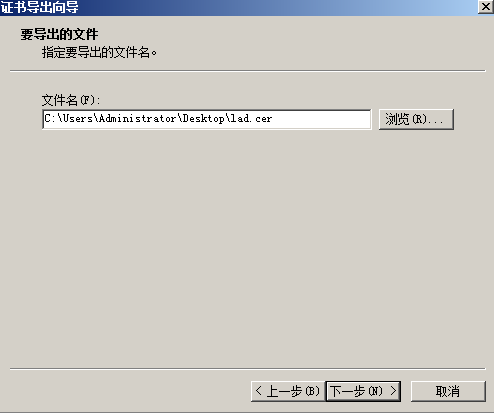


选择Base64 编码 X.509



输入导出的文件明，我输入的lad





默认下一步，点击完成





lad.cer 文件就是我们需要的证书文件。

1. appform 导入证书

将前面的lad.cer文件拷贝到appform机器上

比如，在/tmp/lad.cer

然后进入到appform安装目录下的jre中

cd ${APPFORM\_TOP} /jre/lib/security

keytool -importcert -keystore cacerts -file /tmp/lad.cer -alias lad

keytool 的默认密码是changeit