LDAP服务器和证书服务器属于相同域时iMC和LDAP进行SSL通信的典型配置

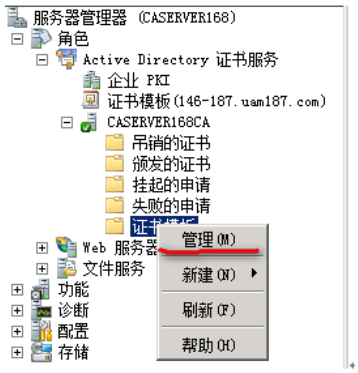
LDAP 罗孝晨 2016-06-01 发表

LDAP服务器和证书服务器属于相同域时iMC和LDAP进行SSL通信的典型配置

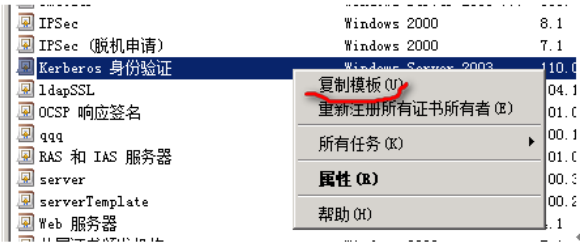
本次配置需要两台机器，都安装windows server 2008 R2 Datacenter，IP分别为10.153.146.168（计算机名：CASERVER168.uam187.com）和10.153.146.187（计算机名：146-187.uam187.com）。其中10.153.146.168安装Active Directory 证书服务作为证书服务器，10.153.146.187安装Active Directory域服务和Active Directory轻型目录服务作为ldap服务器，10.153.146.187同时也作为域控制器，其域为um187.com，并将10.153.146.168也加入这个域中。安装的服务如下图所示：
146.168安装的服务有：

146.187安装的服务有：

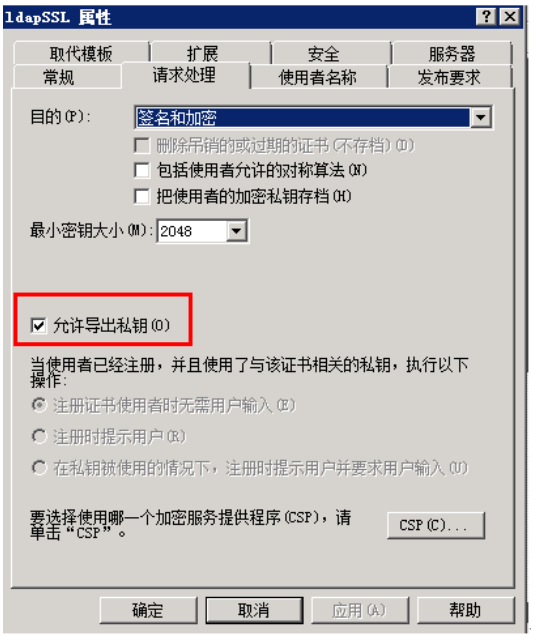
1）在证书服务器上，“证书模板”上点击“管理”：



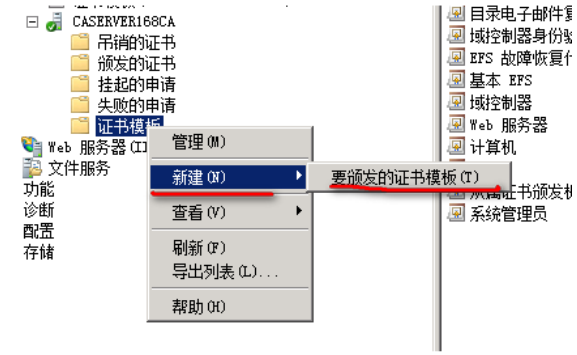
2）复制一个“Kerberos身份验证”模板命名为ldapSSL



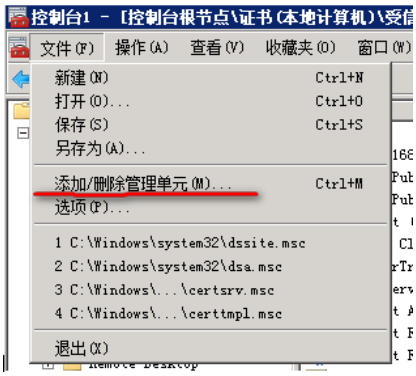
3)勾选“允许导出私钥”：



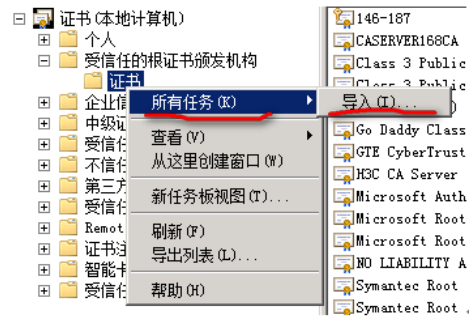
4）将这个模板（ldapSSL）加入到要颁发的证书模板中：



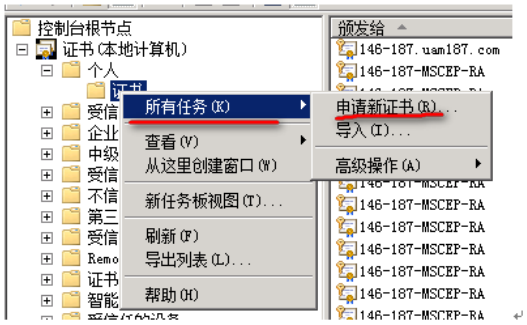
5）LDAP服务器上，在运行里输入mmc，在文件里选择下面这个菜单，并在下拉列表里选择证书，依次选择“计算机帐号”、“本地计算机”并完成：



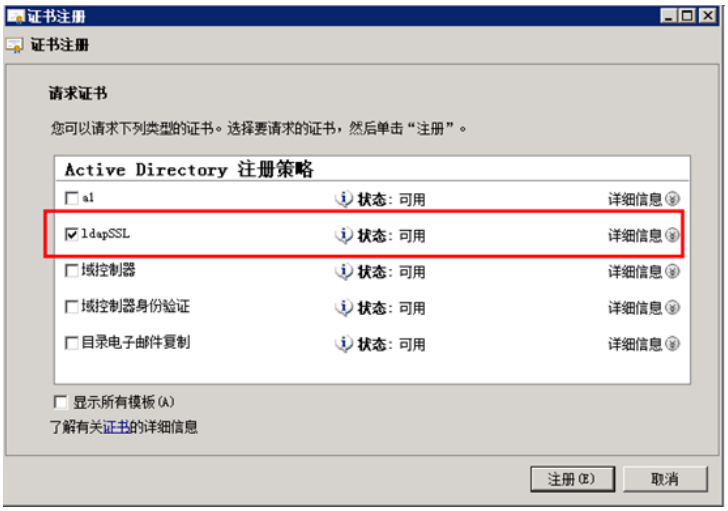
6）将证书服务器上的根证书导入LDAP服务器：



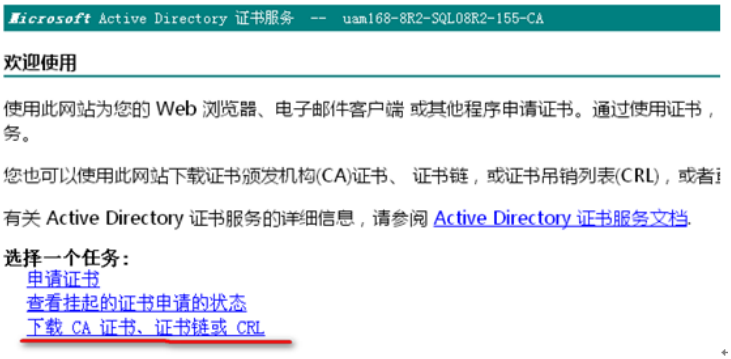
7）申请一个“个人证书”：



8）选择ldapSSL这个模板并完成注册：



9）在iMC服务器上添加一个LDAP服务器，勾选“启用SSL连接”，将证书服务器上的根证书上传上去，点击测试可以连接成功：



1、证书模板复制时要选择“Kerberos身份验证”模板，kerberos是由MIT开发的提供网络认证服务的系统。它可用来为网络上的各种server提供认证服务,使得口令不再是以明文方式在网络上传输，并且联接之间通讯是加密的。它和PKI认证的原理不一样，PKI使用公钥体制(不对称密码体制)，kerberos基于私钥体制(对称密码体制)。Kerberos称为可信的第三方验证协议

2、配置ldapSSL模板时要勾选“允许导出私钥”

3、证书服务器上的根证书要导入LDAP服务器