13

第 13 章　自动信任根 CA

在PKI（Public Key Infrastructure，公钥基础结构）的架构下，企业可以通过向CA（Certification Authority，证书颁发机构）所申请到的证书，来确保数据在网络上传送的安全性，然而用户的计算机需要信任发放证书的CA。本章将介绍如何通过AD DS的组策略，来让域内的计算机自动信任指定的**根CA**（root CA）。

- 自动信任CA的设置准则
- 自动信任内部的独立CA
- 自动信任外部的CA

13.1 自动信任CA的设置准则

可以通过AD DS组策略（group policy），来让域内所有计算机都自动信任指定的根CA，也就是自动将这些根CA的证书发送、安装到域内所有计算机。

- 如果是企业根CA（enterprise root CA），则不需要另外设置组策略，因为AD DS会自动通过组策略将企业根CA的证书发送到域内所有计算机，也就是说域内所有计算机都会自动信任企业根CA。
- 如果是安装在成员服务器上的独立根CA（stand-alone root CA），而且是由具备访问AD DS权限的域系统管理员所安装的，则也不需要另外设置组策略，因为AD DS会自动通过组策略将此独立根CA的证书发送到域内所有计算机。
- 如果是安装在独立服务器的独立根CA、是安装在成员服务器上的独立根CA但执行安装工作的用户不具备访问AD DS的权限，则需要另外通过**受信任的根证书颁发机构策略**（trusted root certificate authority policy），来将此独立根CA的证书自动发送到域内所有计算机。
- 如果不是搭建在公司内部的独立根CA，而是外界的独立根CA，则需要另外通过**企业信任策略**（enterprise trust policy），来将此独立根CA的证书自动发送到域内所有计算机。

附注

Windows计算机只要信任了根CA，它们默认就会自动信任根CA之下所有的二级CA（subordinate CA）。

我们将针对后面两种情况，说明如何利用**受信任的根证书颁发机构策略**与**企业信任策略**，来让域内的计算机自动信任我们所指定的独立根CA。

13.2 自动信任内部的独立CA

如果公司内部的独立根CA是利用Windows Server的**Active Directory 证书服务**所搭建的，而且是安装在独立服务器，或是安装在成员服务器但执行安装工作的用户不具备访问AD DS权限的话，则需要通过**受信任的根证书颁发机构策略**来将此独立根CA的证书，自动发送到域内的计算机，也就是让域内的计算机都自动信任此独立根CA。我们将利用以下两大步骤来练习将名称为**Server1Standalone Root CA**的独立根CA的证书，自动发送到域内的所有计算机。

- 下载独立根CA的证书并保存。

将独立根CA的证书导入到受信任的根证书颁发机构策略。

13.2.1 下载独立根CA的证书并保存

STEP 1 请到域控制器或任何一台计算机上运行网页浏览器，并输入以下的URL路径：

```
http://CA 的主机名、计算机名称或 IP 地址/certsrv
```

以下利用IP地址来举例，并假设CA的IP地址为192.168.8.31。

附注

如果是在Windows Server上执行Internet Explorer的话，可暂时先将其**IE增强的安全配置**（IE ESC）禁用，否则系统会阻挡连接CA网站：【打开**服务器管理器**➲单击**本地服务器**➲单击**IE增强的安全配置**➲...】。

STEP 2 在图13-2-1中单击**下载CA证书、证书链或CRL**。

图 13-2-1

STEP 3 在图13-2-2中单击**下载CA证书**或**下载CA证书链**。

图 13-2-2

STEP 4 请通过接下来的界面将下载的CA证书保存到本地：

- 如果前一个步骤中选择**下载CA证书**，则会将其文件名设置为certnew.cer（包含证书）。
- 如果前一个步骤中选择**下载CA证书链**，则会将其文件名设置为certnew.p7b的文件（包含证书与证书路径）。

附注

如果计算机的**根证书存储区域**（root store）内已经有该CA的证书，也就是此计算机已经信任该CA的话，则可以利用另外一种方式来将CA的证书文件：【按⊞+ R键➲输入control后按Enter键➲**网络和Internet➲Internet选项**➲选择**属性**选项卡➲单击证书按钮➲如图13-2-3所示选择**受信任的根证书颁发机构**选项卡➲选择CA的证书➲单击导出按钮】。

图 13-2-3

13.2.2 将CA证书导入到受信任的根证书颁发机构

假设要让域内所有计算机都自动信任前述的独立根CA：**Server1Standalone Root CA**，而且要通过Default Domain Policy GPO来设置。

附注

如果仅是要让某个组织单位内的计算机来信任前述独立根CA的话，请通过该组织单位的GPO来设置。

STEP 1 到域控制器上【单击左下角**开始**图标⊞➲Windows 管理工具➲**组策略管理**➲如图13-2-4所示展开到域sayms.local➲选中**Default Domain Policy** 并右击➲**编辑**】。

图 13-2-4

STEP 2 如图13-2-5所示【展开**计算机配置➲策略➲Windows设置➲安全设置➲公钥策略➲**选中**受信任的根证书颁发机构**并右击**➲导入**】。

图 13-2-5

STEP 3 出现**欢迎使用证书导入向导**界面时单击下一步按钮。

STEP 4 在图13-2-6中选择之前下载的CA证书文件后单击下一步按钮，图中我们选择包含证书与证书路径的.p7b文件。

图 13-2-6

STEP 5 在图13-2-7中单击下一步按钮。

图 13-2-7

STEP 6 出现**正在完成证书导入向导**界面时单击完成按钮。

STEP 7 图13-2-8为完成后的界面。

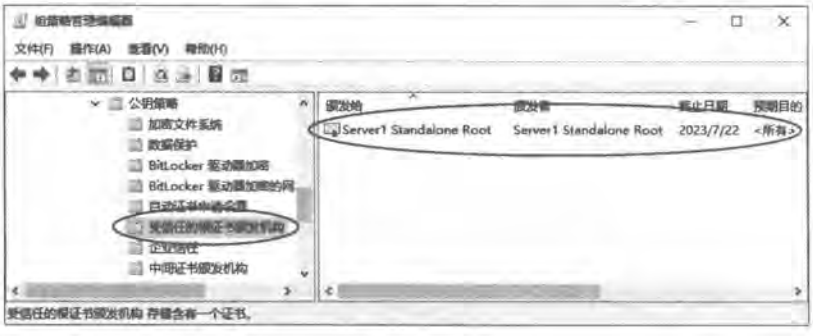

图 13-2-8

完成以上步骤后，域内所有计算机在应用这个策略后，它们就都会自动信任上述的独立根CA。也可以在每一台成员计算机上执行**gpupdate /force**命令来快速应用此策略，然后通过以下方法来检查这些计算机是否已经信任这台名称为**Server1Standalone Root CA**的独立根CA：【按⊞+R键➲输入control后按Enter键➲**网络和Internet**➲**Internet选项**➲单击**属性**选项卡➲单击证书按钮➲如图13-2-9所示单击**受信任的根证书颁发机构**选项卡】，由图中可知此计算机（假设是Windows 10客户端）已经信任此独立根CA。

图 13-2-9

13.3 自动信任外部的CA

可以让域内所有计算机都自动信任位于外部的根CA，其方法是先建立**证书信任列表**（Certificate Trust List，CTL），然后通过**企业信任策略**来将**证书信任列表**内所有根CA的证书发送到域内所有计算机，让域内所有计算机都自动信任这些根CA。

虽然外部的根CA可以发放各种不同用途的证书，例如用来保护电子邮件的证书、服务器验证的证书等，可是有时候只希望信任此根CA所发放的证书只能够用在单一用途上，例如服务器验证，其他用途一概拒绝信任，这些设置也是一并通过**证书信任列表**来完成。

以下将建立一个**证书信任列表**来让域内所有计算机都自动信任名称为External Standalone Root CA的独立根CA，不过只信任其用在**服务器验证**的单一用途上。

首先需要取得此独立根CA的证书，然后因为**证书信任列表**必须经过签名，故还需要申请一个可以用来将**证书信任列表**签名的证书。我们将通过以下三大步骤来练习：

- 下载独立根CA的证书并保存。
- 申请可以将**证书信任列表**签名的证书。
- 建立**证书信任列表**（CTL）。

13.3.1 下载独立根CA的证书并保存

下载名称为External Standalone Root CA的独立根CA的证书并保存，假设其文件名为ExtCertnew.p7b：

- 如果这台独立根CA是利用Windows Server的**Active Directory证书服务**所搭建的，则其操作方法与13.2.1节相同，请前往参考。

如果这台根CA是利用其他软件所搭建的，则请参考该软件的文件来操作。

申请可以将证书信任列表签名的证书

由于**证书信任列表**需要经过签名，因此必须申请一个可以将**证书信任列表**签名的证书。假设要向名称为Sayms Enterprise Root CA的企业根CA申请此证书。

STEP 1 请到域控制器上登录，然后暂时将浏览器的**本地Intranet**的安全级别降为**低**（否则CA网站需拥有SSL证书，并且向CA网站申请证书时需要采用https）：【单击左下角**开始**图标⊞➲**控制面板**➲**网络和Internet**➲**Internet选项**➲如图13-3-1单击**安全**选项卡➲单击**本地Intranet**➲将安全等级别调整为**低**】。

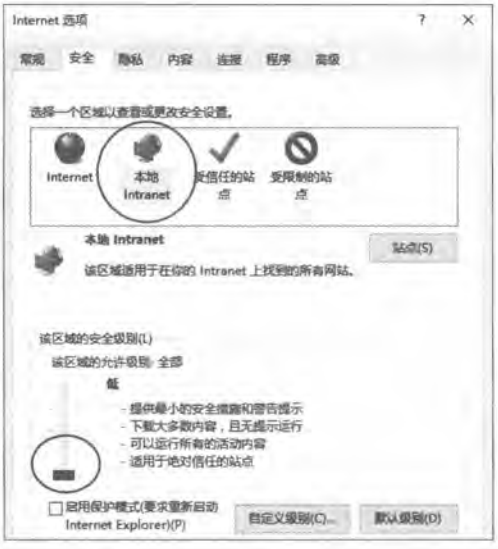

图 13-3-1

STEP 2 假设要向名称为Sayms Enterprise Root CA的企业根CA申请用来将**证书信任列表**签名的证书，因此请将此企业根CA网站加入到**本地Intranet**：【单击前面图13-3-1右侧站点按钮➲单击图13-3-2中的高级按钮➲在前景图中将http://192.168.8.1/加入此区域后单击关闭、单击两次确定按钮】，图中假设192.168.8.1是企业根CA的IP地址。

图 13-3-2

STEP 3 在浏览器内输入网址http://192.168.8.1/certsrv/。

附注

如果出现Windows安全界面的话，请输入**域系统管理员**的用户账户（sayms\administrator）与密码。

STEP 4 在图13-3-3中选择**申请证书、高级证书申请、创建并向此CA提交一个申请。**

图 13-3-3

STEP 5 接下来的两个界面都单击**是（Y）**按钮。

STEP 6 在图13-3-4中的**证书模板**处选择**管理员**后单击**提交**按钮。

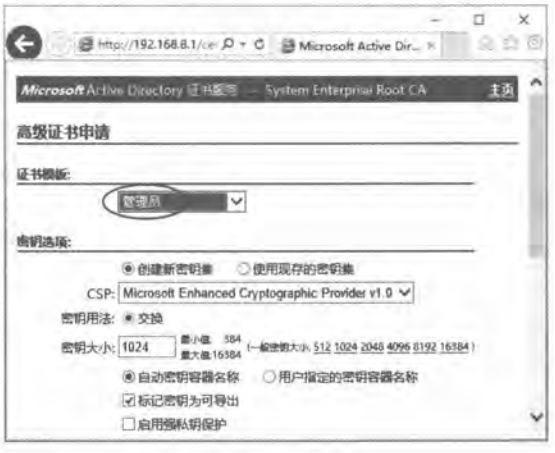

图 13-3-4

STEP 7 接下来的两个界面都单击**是（Y）**按钮。

STEP 8 在图13-3-5中单击**安装此证书。**

图 13-3-5

STEP 9 将**本地Intranet**的安全级别恢复为原级别（默认为**中低**）。

13.3.2 建立证书信任列表（CTL）

以下所要建立的**证书信任列表**（CTL）内包含名称为**External Standalone Root CA**的外部独立根CA的证书，也就是要让域内所有计算机都自动信任此独立根CA，而我们将通过Default Domain Policy GPO来设置。

STEP 1 到域控制器上【单击左下角**开始**图标⊞➲**Windows 管理工具**➲**组策略管理**➲如图13-3-6所示展开到域**sayms.local**➲选中**Default Domain Policy**并右击➲**编辑**】。

图 13-3-6

STEP 2 展开**计算机配置**➲策略➲**Windows设置**➲**安全设置**➲**公钥策略**➲如图13-3-7所示选中**企业信任**并右击➲**新建**➲**证书信任列表**。

图 13-3-7

STEP 3 出现**欢迎使用证书信任列表向导**界面时单击下一步按钮。

STEP 4 在图13-3-8中勾选CTL的用途（**服务器身份验证**）后单击下一步按钮。

图 13-3-8

STEP 5 在图13-3-9中点击**从文件添加**按钮。

图 13-3-9

STEP 6 图13-3-10中选择外部独立根CA（External Standalone Root CA）的证书文件后，单击打开按钮。

图 13-3-10

STEP 7 回到图13-3-11的界面时单击下一步按钮。

图 13-3-11

STEP 8 在图13-3-12中【单击从存储区选择按钮➲选择我们在前面申请用来对CTL签名的证书➲单击确定按钮】。

图 13-3-12

STEP 9 接下来的两个界面都直接单击下一步按钮。

STEP 10 在图13-3-13中为此列表设置好记的名称与描述后单击下一步按钮。

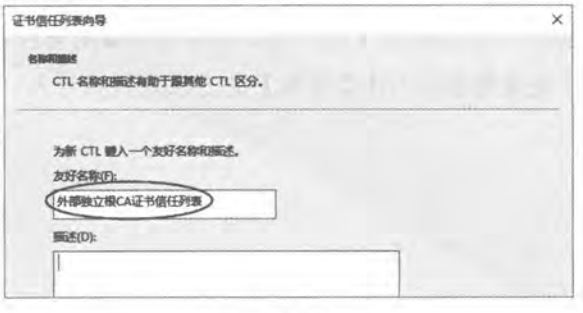

图 13-3-13

STEP 11 出现**正在完成证书信任列表向导**界面时单击完成按钮、单击确定按钮。

STEP 12 图13-3-14为完成后的界面。

图 13-3-14

完成以上步骤后，域内所有计算机在应用这个策略，它们就都会自动信任上述的外部独立根CA。可以到每一台计算机上执行**gpupdate /force**命令来快速应用此策略，然后在这些计算机上通过自定义本地计算机的**证书**管理控制台来检查它们是否已经取得这个证书信任列表。如图13-3-15所示为已经成功取得此列表的界面。

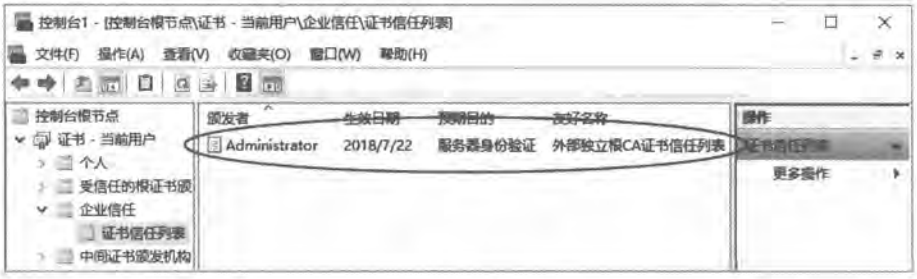

图 13-3-15

附注

通过**证书信任列表**所信任的CA证书，并不会显示在用户计算机的**受信任的根证书颁发机构**存储区。

可以将此CTL导出保存，其方法为【选中此CTL并右击➲**所有任务**➲**导出**】，以后需要使用时可以再通过【选中**企业信任**并右击➲**导入**】的方法来将其导入。