6

第 6 章　限制软件的运行

我们可以通过**软件限制策略**（Software Restriction Policy，SRP）所提供的多种规则，来限制或允许用户可以运行的程序。

- 软件限制策略概述
- 启用软件限制策略

6.1 软件限制策略概述

我们在4-5节中介绍过如何利用文件名来限制用户可以或不可以运行特定的应用程序，然而如果用户有权更改文件名的话，就可以突破此限制，此时我们仍然可以通过本章的**软件限制策略**来管理。此策略的安全级别分为以下3种：

- **不受限**：所有登录的用户都可以运行指定的程序（只要用户拥有适当的访问权限，例如NTFS权限）。
- **不允许**：不论用户对程序文件的访问权限如何，都不允许运行。
- **基本用户**：允许以普通用户的权限（users组的权限）来运行程序。

系统默认的安全级别是所有程序都**不受限**，也就是只要用户对要运行的程序文件拥有适当访问权限的话，他就可以运行此程序。不过可以通过**哈希规则**、**证书规则**、**路径规则**与**网络区域规则**等4 种规则来建立例外的安全级别，以便拒绝用户运行所指定的程序。

6.1.1 哈希规则

哈希（hash）是根据程序的文件内容所算出来的一连串字节，不同程序有着不同的哈希值，所以系统可用它来识别程序。在为某个程序建立**哈希规则**，并利用它限制用户不允许运行此程序时，系统就会为该程序建立一个哈希值。而当用户要执行此程序时，其Windows系统就会比较自行算出来的哈希值是否与软件限制策略中的哈希值相同，如果相同，表示它就是被限制的程序，因此会被拒绝运行。

即使此程序的文件名被改变或被移动到其他位置，也不会改变其哈希值，因此仍然会受到哈希规则的约束。

附注

如果用户计算机端的程序文件内容被修改的话（例如感染计算机病毒），此时因为用户的计算机所算出的哈希值与哈希规则中的哈希值不同，因此不会认为它是受限制的程序，故不会拒绝此程序的运行。

6.1.2 证书规则

软件发行公司可以利用证书（certificate）来签署其所开发的程序，而软件限制策略可以通过此正式来识别程序，也就是说可以建立**证书规则**来识别利用此证书所签署的程序，以便允许或拒绝用户执行此程序。

6.1.3　路径规则

可以通过**路径规则**来允许或拒绝用户运行位于某个文件夹内的程序。由于是根据路径来识别程序，因此如果程序被移动到其他文件夹的话，此程序将不会再受到路径规则的约束。

除了文件夹路径外，也可以通过**注册表**路径来限制，例如开放用户可以执行在注册表中所指定的文件夹内的程序。

6.1.4　网络区域规则

可以利用**网络区域规则**来允许或拒绝用户执行位于某个区域内的程序，这些区域包含**本地计算机**、**Internet**、**本地 Intranet**、**受信任的站点**与**受限制的站点**。

除了本地计算机与Internet之外，可以设置其他三个区域内所包含的计算机或网站：【按⊞+R键➲输入control后按Enter键➲**网络和Internet**➲**Internet选项**➲单击图6-1-1中的**安全**选项卡➲选择要设置的区域后单击网站按钮】。

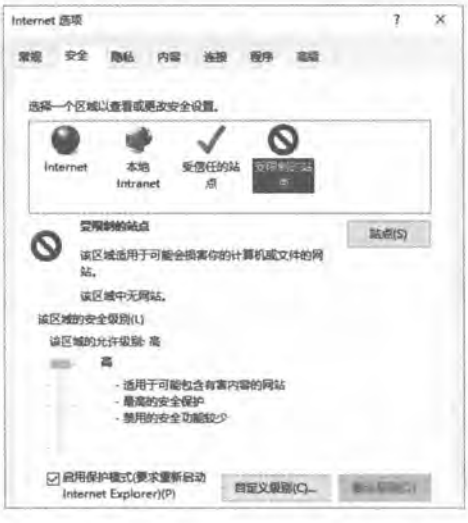

图 6-1-1

附注

网络区域规则适用于扩展名为.msi的Windows Installer Package。

6.1.5　规则的优先级

可能会针对同一个程序设置不同的软件限制规则，而这些规则的优先级由高到低为：哈希规则、证书规则、路径规则、网络区域规则。

例如针对某个程序设置了哈希规则，并且设置其安全级别为**不受限**，然而同时针对此程

序所在的文件夹设置了路径规则，并且设置其安全级别为**不允许**，此时因为哈希规则的优先级高于路径规则，故用户仍然可以运行此程序。

6.2 启用软件限制策略

可以通过本地计算机、站点、域与组织单位等四个不同地方来设置软件限制策略。以下将利用前几章所使用的组织单位**业务部**内的**测试用的GPO**来练习软件限制策略（如果尚未有此组织单位与GPO的话，请先建立）：请到域控制器上【单击左下角**开始**图标⊞➲**Windows管理工具**➲**组策略管理**➲展开到组织单位**业务部**➲选中**测试用的GPO**并右击➲编辑➲在图6-2-1中展开**用户配置**➲**策略**➲**Windows设置**➲**安全设置**➲选中**软件限制策略**并右击➲**创建软件限制策略**】。

图 6-2-1

接着单击图6-2-2中的**安全级别**，从右侧**不受限**前面的对勾符号可知默认安全级别是所有程序都**不受限**，也就是只要用户对要运行的程序文件拥有适当访问权限的话，他就可以运行该程序。

图 6-2-2

6.2.1 建立哈希规则

例如要利用哈希规则来限制用户不能安装号称**网络剪刀手**的Netcut的话，则其步骤如下所示（假设为Netcut 3.0版、其安装文件为Netcut.exe）：

STEP 1 我们将到域控制器上设置，因此请先将Netcut 3.0的安装文件Netcut.exe复制到此计算机上。

STEP 2 如图6-2-3所示【选中**其他规则**并右击➲**新建哈希规则**➲单击浏览按钮】。

图 6-2-3

STEP 3 在图6-2-4中浏览到Netcut 3.0安装文件的存储位置后选择Netcut.exe，单击打开按钮。

图 6-2-4

STEP 4 在图6-2-5中选择**不允许**安全级别后，单击确定按钮。

图 6-2-5

STEP 5　图6-2-6为完成后的界面。

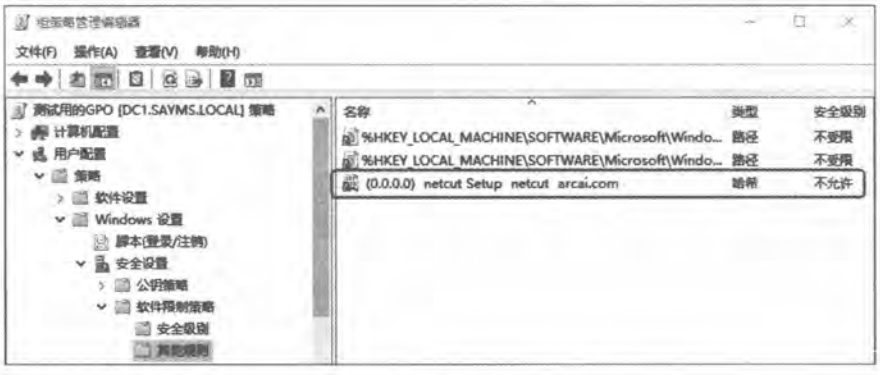

图 6-2-6

位于组织单位**业务部**内的用户应用此策略后，在执行Netcut 3.0的安装文件Netcut.exe时会被拒绝，并且会出现图6-2-7的警告界面。

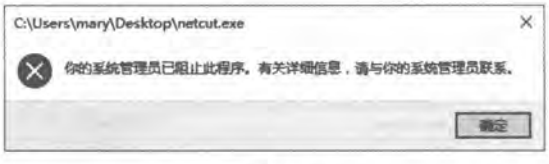

图 6-2-7

注意

1. 不同版本的Netcut，其安装文件的哈希值也都不相同，因此如果要禁止用户安装其他版本Netcut的话，需要再针对它们建立哈希规则。
2. 为了加强阻挡效果，建议也禁止用户执行Netcut可执行文件，例如如果可执行文件为Netcut.exe，则请针对此文件建立哈希规则来禁止用户执行此可执行文件。

6.2.2 建立路径规则

路径规则分为文件夹路径与注册表路径规则两种。路径规则中可以使用环境变量，例如%*Userprofile*%、%*SystemRoot*%、%*Appdata*%、%*Temp*%、%*Programfiles*%等。

1. 建立文件夹路径规则

举例来说，如果要利用文件夹路径规则来限制用户不能执行位于\\dc1\SystemTools共享文件夹内所有程序的话，则其设置步骤如下所示。

STEP 1 如图6-2-8所示【选中**其他规则**并右击➲**新建路径规则**】。

图 6-2-8

STEP 2 如图6-2-9所示来输入或浏览路径、**安全级别**选择**不允许**、单击确定按钮。

图 6-2-9

附注

如果只是要限制用户执行此路径内某个程序的话，请输入此程序的文件名，例如要限制的程序为netcut.exe的话，请输入\\dc1\SystemTools\netcut.exe；如果不论此程序位于何处，均要禁止用户执行的话，则输入程序名称netcut.exe即可。

STEP 3　图6-2-10为完成后的界面。

图 6-2-10

2. 建立注册表路径规则

可以通过**注册表**（registry）路径来开放或禁止用户执行路径内的程序，由图6-2-11中可看出系统已经内置了两个注册表路径。

图 6-2-11

其中第一个注册表路径是要开放用户可以执行位于以下注册表路径内的程序：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot
```

而可以利用注册表编辑器（REGEDIT.EXE）来查看其所对应到的文件夹，如图6-2-12所示为C:\Windows，也就是说用户可以执行位于文件夹C:\Windows内的所有程序。

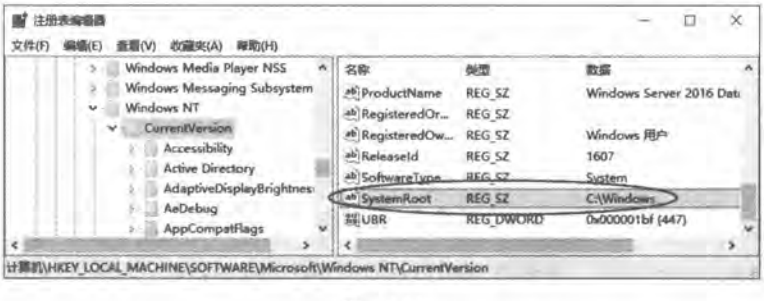

图 6-2-12

如果要编辑或新建注册表路径规则的话，记得在路径前后要附加%符号，例如：

```
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SystemRoot%
```

6.2.3 建立证书规则

由于客户端计算机默认并未启用证书规则，因此这些计算机在执行扩展名为.exe的可执行文件时，并不会处理与证书有关的事宜。以下我们将先启用客户端的证书规则，然后再来建立证书规则。

1. 启用客户端的证书规则

证书规则的启用是通过组策略来设置的，以下假设是要针对组织单位**业务部**内的计算机来启用证书规则，而且是通过**测试用的GPO**来设置。

请到域控制器上【单击左下角**开始**图标⊞➲**Windows 管理工具**➲**组策略管理**➲展开到组织单位**业务部**➲选中**测试用的GPO**并右击➲**编辑**➲在图6-2-13中展开**计算机配置**➲**策略**➲**Windows设置**➲**安全设置**➲**本地策略**➲**安全选项**➲将右侧的**系统设置：将Windows可执行文件中的证书规则用于软件限制策略**设置为**已启用**】。完成后，位于此组织单位**业务部**内的计算机在应用策略后便具备通过证书来限制程序执行的功能。

图 6-2-13

附注

如果要启用本地计算机的证书规则：【执行**GPEDIT.MSC**➲**计算机配置**➲**Windows设置**...（以下与前述域组策略路径相同）】，若此设置与域组策略设置发生冲突时，则以域组策略的设置优先。

也可以通过以下方法来启用客户端的证书规则：【在图6-2-14中展开**计算机配置**➲策略➲**Windows设置**➲**安全设置**➲**软件限制策略**➲双击右侧的**强制**➲点选**强制证书规则**】。

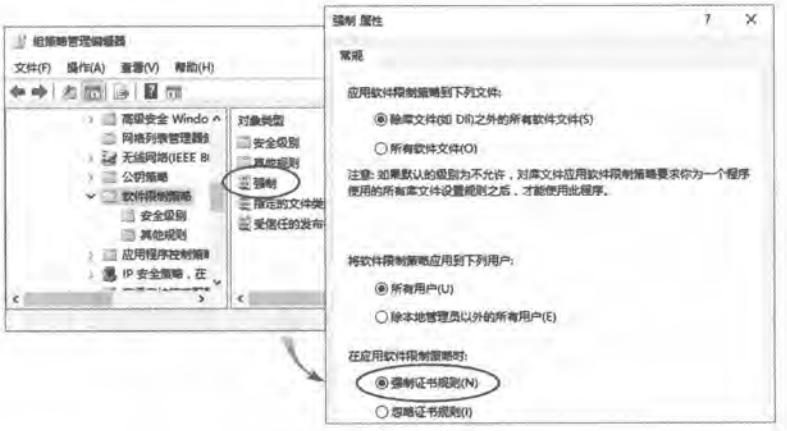

图 6-2-14

2. 建立证书规则

以下假设在组织单位**业务部**内默认的安全级别是**不允许**，也就是此组织单位内的用户无法运行所有程序，但只要程序是经过Sayms公司所申请的**代码签署证书**签署的话，该程序就允许运行，假设此证书的证书文件为SaymsCert.cer。

附注

可以通过自行搭建的CA来练习，其步骤为：搭建CA（例如独立根CA）、利用浏览器来向此CA申请**代码签名证书**（记得勾选**将密钥标记为可导出**）、下载与安装证书、将证书导出保存（通过【按⊞+ R键➲输入control后按Enter键➲**网络和Internet➲Internet选项➲内容➲证书➲**选择证书➲**导出**】的方法）。CA与证书的完整说明可参考《Windows Server 2016 网络管理与架站》。

STEP 1 选中图6-2-15中的**其他规则**并右击➲**新建证书规则**➲单击浏览按钮。

图 6-2-15

STEP 2 在图6-2-16中浏览到证书文件SaymsCert.cer后单击打开按钮。

图 6-2-16

STEP 3 在图6-2-17中选择**不受限**后单击确定按钮。

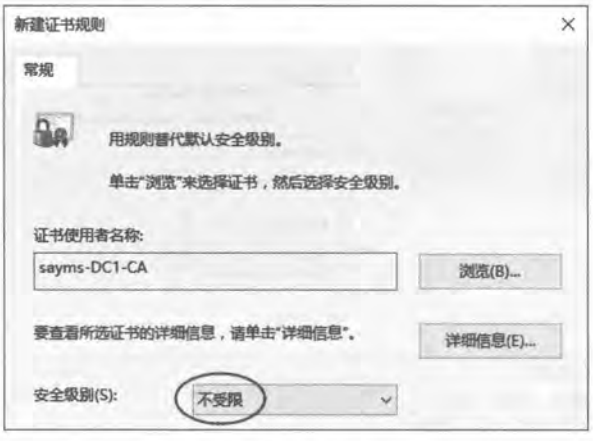

图 6-2-17

STEP 4 图6-2-18为完成后的界面。位于组织单位**业务部**内的用户应用此策略后，在运行所有经过Sayms证书签名的程序时，都会被允许。

图 6-2-18

6.2.4 建立网络区域规则

可利用**网络区域规则**来允许或拒绝用户执行位于某个区域内的程序，这些区域包含**本地计算机、Internet、本地 Intranet、受信任的站点**与**受限制的站点**。

建立网络区域规则的方法与其他规则很类似，也就是如图6-2-19所示【选中**其他规则**并右击➲**新建网络区域规则**➲从**网络区域**下拉列表中选择区域➲选择**安全级别**】，图中表示只要是位于**受限制的站点**内的程序都不允许运行。图6-2-20为完成后的界面。

图 6-2-19

图 6-2-20

6.2.5 不要将软件限制策略应用到本地系统管理员

如果不想将软件限制策略应用到本地系统管理员组（Administrators）的话，可以如图6-2-21所示【双击**软件限制策略**右侧的**强制**➲在**将软件限制策略应用到下列用户**处选择**除本地管理员以外的所有用户**➲单击确定按钮】。


组策略管理编辑器
文件(F) 操作(A) 查看(V) 帮助(H)
测试用的GPO [DC1.SAYMS.LOCAL] 策略
计算机配置
用户配置
策略
软件设置
Windows 设置
脚本(登录/注销)
安全设置
公钥策略
软件限制策略
安全级别
其他规则
对象类型
安全级别
其他规则
强制
强制 属性
常规
应用软件限制策略到下列文件:
除库文件(如 Dll)之外的所有软件文件(S)
所有软件文件(O)
注意: 如果默认的级别为不允许，对库文件应用软件限制策略要求你为一个程序使用的所有库文件设置规则之后，才能使用此程序。
将软件限制策略应用到下列用户:
所有用户(U)
除本地管理员以外的所有用户(E)

图 6-2-21