

第2章 建立AD DS域

建立AD DS（Active Directory Domain Services）域后，就可以通过AD DS的强大功能提高网络管理效率，减轻网络管理人员的工作负担。

- ✎ 建立AD DS域前的准备工作
- ✎ 建立AD DS域
- ✎ 确认AD DS域是否正常
- ✎ 提升域与林功能级别
- ✎ 添加额外域控制器与RODC
- ✎ RODC阶段式安装
- ✎ 将Windows计算机加入或脱离域
- ✎ 在域成员计算机内安装AD DS管理工具
- ✎ 删除域控制器与域

2.1 建立AD DS域前的准备工作

建立AD DS域的方法，可以先安装一台服务器，然后将其升级（promote）为域控制器。在建立AD DS域前，请先确认以下的准备工作是否已经完成：

- ✎ 选择适当的DNS域名
- ✎ 准备好一台用来支持AD DS的DNS服务器
- ✎ 选择AD DS数据库的存储位置

2.1.1 选择适当的DNS域名

AD DS域名是采用DNS的架构与命名方式，因此请先为AD DS域取一个符合DNS格式的域名，例如sayms.local（以下均以虚拟的**顶级域名.local**为例来说明）。虽然域名可以在域建立完成后更改，不过步骤烦琐，因此请事先谨慎命名。

2.1.2 准备好一台支持AD DS的DNS服务器

在AD DS域中，域控制器会将自己所扮演的角色注册到DNS服务器内，以便让其他计算机通过DNS服务器来找到这台域控制器，因此需要一台DNS服务器，并且它需要支持SRV记录，同时最好支持**动态更新**、Incremental Zone Transfer与Fast Zone Transfer等功能：

- ✎ **SVR记录（Service Location Resource Record, SRV RR）**：域控制器需将其所扮演的角色注册到DNS服务器的SRV记录内，因此DNS服务器必须支持此类型的记录。Windows Server 的DNS服务器与BIND DNS服务器都支持此功能。
- ✎ **动态更新**：虽然不一定需要具备动态更新功能，但是强烈建议具备此功能，否则域控制器无法自动将自己注册到DNS服务器的SRV记录内，此时便需由系统管理员手动将数据输入到DNS服务器，如此势必增加管理负担。Windows Server 与BIND的DNS服务器都支持此功能。
- ✎ **Incremental Zone Transfer（IXFR）**：它让此DNS服务器与其他DNS服务器之间在执行**区域传送（zone transfer）**时，只会复制最新变动记录，而不是复制区域内的所有记录。它可提高复制效率，减少网络负担。Windows Server 与BIND的DNS服务器都支持此功能。
- ✎ **Fast Zone Transfer**：它让DNS服务器可以利用**快速区域传送**将区域内的记录复制给其他DNS服务器。**快速区域传送**可对数据压缩，每一条传送消息内可包含多条记录。Windows Server与BIND的DNS服务器都支持此功能。
Windows Server 的DNS服务器默认已启用**快速区域传送**，但有些厂商的DNS服务器

并不支持此功能，因此如果要通过区域传送将记录复制给不支持快速区域传送功能的DNS服务器的话，需禁用此功能（以Windows Server 2016为例）：【单击左下角开始图标田Windows 管理工具DNS选中DNS服务器并右击属性如图2-1-1所示勾选高级选项卡下的启用BIND辅助区域】。

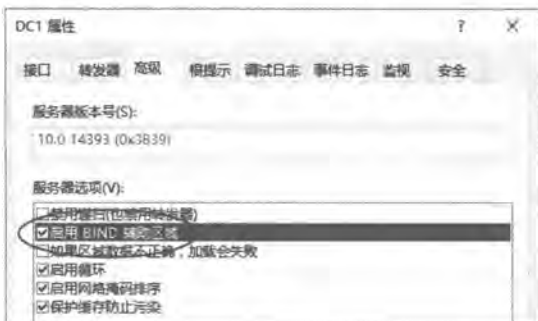


图 2-1-1

可以采用以下两种方式之一来搭建DNS服务器：

- 在将服务器升级为域控制器时，同时让系统自动在这台服务器上安装 DNS 服务器角色。系统还会自动在此DNS服务器内建立一个支持AD DS域的区域，例如AD DS域名为sayms.local，则其所自动建立的区域名称为sayms.local，并自动启用安全动态更新。

请先在这台即将成为域控制器与DNS服务器计算机上，清除其首选DNS服务器的IP地址或改为输入自己的IP地址（如图2-1-2所示），无论选择哪一种设置方式，升级时系统可以自动安装DNS服务器角色。

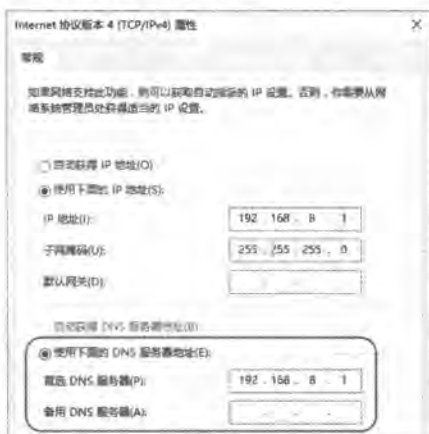


图 2-1-2

- 使用现有DNS服务器或另外安装一台DNS服务器，然后在这台DNS服务器内建立用来支持AD DS域的区域，例如AD DS域名为sayms.local，则请自行建立一个名称为sayms.local的DNS区域，然后启用动态更新功能，如图2-1-3所示为选择非安全动态更新，如果它是Active Directory集成区域的话，则还可以选择安全动态更新。别忘了

了先在即将升级为域控制器的计算机上，将其**首选DNS服务器**的IP地址指定到这台DNS服务器。



图 2-1-3

附注

请通过【打开**服务器管理器**→单击仪表板处的**添加角色和功能**→……→勾选**DNS服务器**→……】的方法来安装DNS服务器，然后通过【单击左下角开始图标→**Windows 管理工具**→**DNS**→选中**正向查找区域**并右击→**新建区域**】的方法来建立区域。

2.1.3 选择AD DS数据库的存储位置

域控制器需要利用磁盘空间来存储以下三个与AD DS有关的数据：






- **AD DS数据库**：用来存储AD DS对象
- **日志文件**：用来存储AD DS数据库的变动日志
- **SYSVOL文件夹**：用来存储域共享文件（例如与组策略有关的文件）

它们都必须被存储到本地磁盘内，并且SYSVOL文件夹需要位于NTFS磁盘分区内。建议将AD DS数据库与日志文件分别存储到不同的硬盘内，一方面是因为两块硬盘独立工作，可以提高工作效率，另一方面是因为分开存储，可以避免两份数据同时出现问题，以提高恢复AD DS数据库的能力。

应该将AD DS数据库与日志文件都存储到NTFS磁盘分区内，以便通过NTFS权限来增加这些文件的安全性，而系统默认是将它们都存储到Windows Server 2016的安装磁盘分区内（它是NTFS磁盘分区）。

如果要将AD DS数据库、日志文件或SYSVOL文件夹存储到另外一个NTFS磁盘分区，但

计算机内目前并没有其他NTFS磁盘分区的话，可采用以下方法来建立NTFS磁盘分区：

- ❏ 如果磁盘内还有未划分的可用空间：此时可以利用【单击左下角开始图标  Windows 管理工具  计算机管理  存储  磁盘管理  选中未配置的可用空间并右击】的方法来建立一个新的NTFS磁盘分区。
- ❏ 利用CONVERT命令来转换现有磁盘分区：例如要将D:磁盘分区（FAT或FAT32）转换成NTFS磁盘的话，可执行CONVERT D: /FS:NTFS命令。如果该磁盘分区当前有文件正处于使用中的话，则系统无法立刻执行转换的工作，此时可以选择让系统在下次重新启动时再自动转换。

注意

AD DS数据库与日志文件的存储位置可以事后利用ntdsutil命令来更改（见第11章）。但如果要更改SYSVOL的存储位置的话，建议采用以下方法：删除域控制器的AD DS，然后在重新安装AD DS时指定新的存储位置。

2.2 建立AD DS域

以下利用图2-2-1来说明如何建立第1个林中的第1个域（根域）：我们将先安装一台Windows Server 2016服务器，然后将其升级为域控制器并建立域。我们也将搭建此域的第2台域控制器（Windows Server 2016）、第3台域控制器（Windows Server 2016）、一台成员服务器（Windows Server 2016）与一台加入AD DS域的Windows 10计算机。

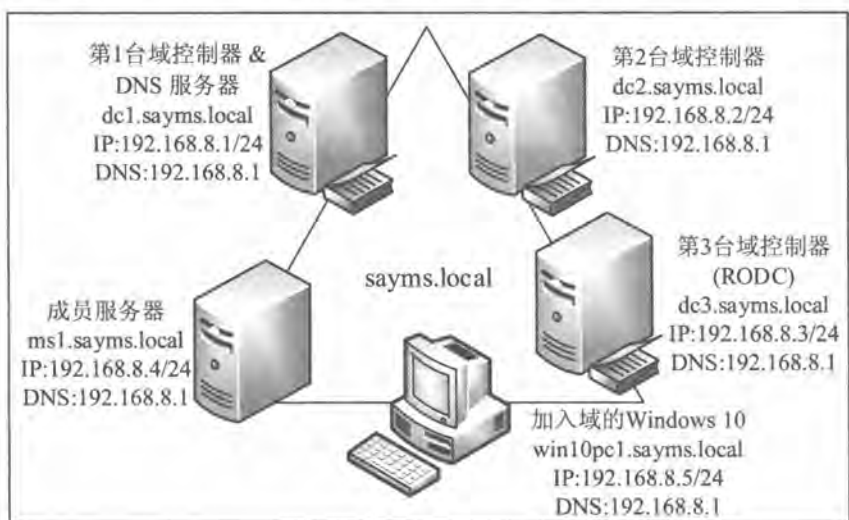


图 2-2-1

建议利用Windows Server 2016 Hyper-V等提供虚拟环境的软件来搭建图中的网络环境。

如果是复制现有虚拟机的话，记得要执行Sysprep.exe并勾选通用。

附注

如果要对现有域升级的话，则林中的域控制器都必须是Windows Server 2008（含）以上的版本，而且需要先分别执行Adprep /forestprep与Adprep /domainprep命令来为林与域执行准备工作，此脚本文件位于Windows Server 2016安装包support\adprep文件夹中。其他升级步骤与操作系统升级的步骤类似。

我们要将图2-2-1左上角的服务器升级为域控制器（安装Active Directory域服务），因为它是第一台域控制器，因此这个升级操作会同时完成以下工作：

- 建立第一个新林；
- 建立此新林中的第一个域树；
- 建立此新域树中的第一个域；
- 建立此新域中的第一台域控制器。

换句话说，在建立图2-2-1中第一台域控制器dc1.sayms.local时，它就会同时建立此域控制器所隶属的域sayms.local、建立域sayms.local所隶属的域树，而域sayms.local也是此域树的根域。由于是第一个域树，因此它同时会建立一个新林，林名称就是第一个域树根域的域名sayms.local。域sayms.local就是整个林的林根域。

我们将通过添加服务器角色的方式，来将图2-2-1中左上角的服务器dc1.sayms.local升级为网络中的第一台域控制器。

STEP 1 请先在图2-2-1中左上角的服务器dc1.sayms.local上安装Windows Server 2016、将其计算机名称设置为dc1、IPv4地址等依照图所示来设置（图中采用TCP/IPv4）。注意将计算机名称设置为dc1即可，等升级为域控制器后，它会自动被改为dc1.sayms.local。

STEP 2 打开服务器管理器、单击仪表板处的添加角色和功能。

STEP 3 持续单击下一步按钮一直到图2-2-2中勾选Active Directory域服务、单击添加功能按钮。



图 2-2-2

STEP 4 持续单击 **下一步** 按钮，直到**确认安装所选内容**界面中单击**安装**按钮。

STEP 5 图2-2-3为完成安装后的界面，请单击**将此服务器提升为域控制器**。



图 2-2-3

附注

如果在图2-2-3中直接单击**关闭**按钮，则之后要将其升级为域控制器的话，请如图2-2-4所示单击**服务器管理器**上方旗帜符号、单击**将此服务器提升为域控制器**。

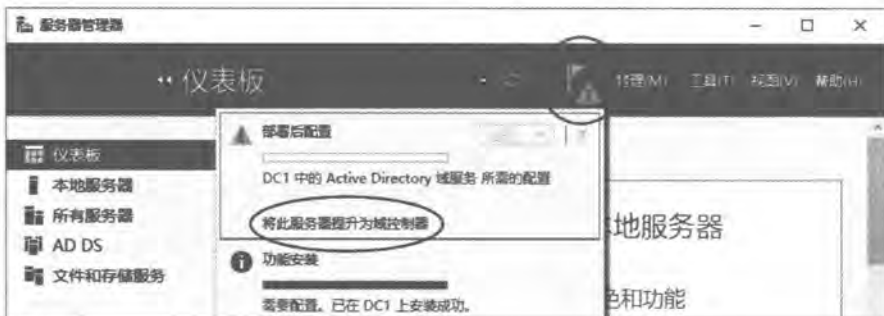


图 2-2-4

STEP 6 如图2-2-5所示选择**添加新林**、设置**林根域名称**（假设是sayms.local）、单击**下一步**按钮。

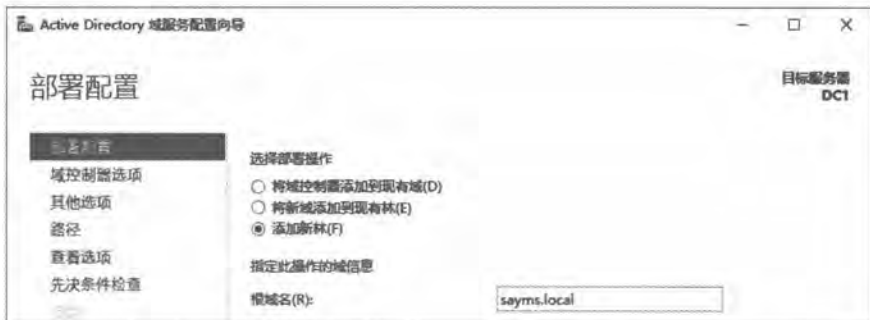


图 2-2-5

STEP 7 完成图2-2-6中的设置后单击 **下一步** 按钮：

- 选择林功能级别、域功能级别。此处我们所选择的林功能级别为Windows Server 2016，此时域功能级别只能选择Windows Server 2016。如果选择其他林功能级别的话，还可以选择其他域功能级别。
- 默认会直接在此服务器上安装DNS服务器。
- 第一台域控制器需要扮演**全局编录服务器**角色。
- 第一台域控制器不能是**只读域控制器（RODC）**。
- 设置**目录服务还原模式**的系统管理员密码：目录服务还原模式（目录服务修复模式）是一个安全模式，进入此模式可以修复AD DS数据库，不过进入目录服务还原模式前需要输入此处所设置的密码（详见第11章）。



图 2-2-6

注意

密码默认需至少7个字符，不能包含用户账户名称（指用户SamAccountName）或全名，还有至少要包含A - Z、a - z、0 - 9、非字母数字（例如!、\$、#、%）等4组字符中的3组，例如123abcABC为有效密码，而1234567为无效密码。

STEP 8 出现图2-2-7的警告界面时，因为目前不会有影响，因此不必理会它，直接单击 **下一步** 按钮。DNS服务器的相关说明可参考《Windows Server 2016网络管理与架站》这本书。



图 2-2-7

STEP 9 在图2-2-8中会自动为此域设置一个NetBIOS域名，也可以更改此名称。如果该NetBIOS域名已被占用的话，安装程序会自动指定一个建议名称。完成后单击 **下一步** 按钮。



图 2-2-8

附注

不支持 DNS 域名的旧版 Windows 系统（例如 Windows 98、Windows NT），可以通过 NetBIOS 域名来与此域通信。默认的 NetBIOS 名称为 DNS 域名第一个句点左侧的文字，例如 DNS 域名为 sayms.local，则 NetBIOS 域名为 SAYMS。

STEP 10 在图2-2-9中可直接单击 **下一步** 按钮：

- ✎ **数据库文件夹**：用来存储 AD DS 数据库。
- ✎ **日志文件文件夹**：用来存储 AD DS 数据库的更新日志，此日志文件可用来修复 AD DS 数据库。
- ✎ **SYSVOL 文件夹**：用来存储域共享文件（例如组策略相关的文件）。



图 2-2-9

如果计算机内有多块硬盘，建议将数据库与日志文件文件夹，分别设置到不同硬盘内，因为两块硬盘分别工作可以提高工作效率，而且分开存储可以避免两份数据同时出现问题，以提高修复 AD DS 数据库的能力。

STEP 11 在查看选项界面中单击 **下一步** 按钮。

STEP 12 在图2-2-10的界面中，若顺利通过检查的话，就直接单击 **安装** 按钮，否则请根据界面提示先排除问题。安装完成后会自动重新启动。



图 2-2-10

完成域控制器的安装后，原本这台计算机的本地用户账户会被异动到AD DS数据库。另外由于它本身也是DNS服务器，因此会如图2-2-11所示自动将**首选DNS服务器**的IP地址改为代表自己的127.0.0.1。

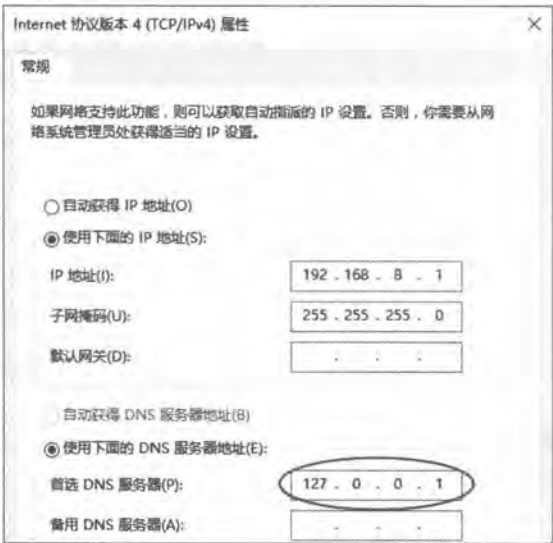


图 2-2-11

附注

此计算机升级为域控制器后，它会自动在**Windows防火墙**中例外开放AD DS相关的端口，以便让其他计算机可以与此域控制器通信。

2.3 确认AD DS域是否正常

AD DS域建立完成后，我们来检查DNS服务器内的SRV与主机记录、域控制器内的SYSVOL文件夹、AD DS数据库文件等是否都已经正常的建立完成。

2.3.1 检查DNS服务器内的记录是否完备

域控制器会将其主机名、IP地址与所扮演角色等数据注册到DNS服务器，以便让其他计算机能够通过DNS服务器找到此域控制器，因此我们先检查DNS服务器内是否有这些记录。请利用域管理员（sayms\Administrator）登录。

1. 检查主机记录

首先检查域控制器是否已将其主机名与IP地址注册到DNS服务器内：【到兼具DNS服务器角色的dc1.sayms.local上单击左下角开始图标→Windows 管理工具→DNS】，如图2-3-1所示会有一个sayms.local区域，图中主机（A）记录表示域控制器dc1.sayms.local已经正确地将其主机名与IP地址注册到DNS服务器内。

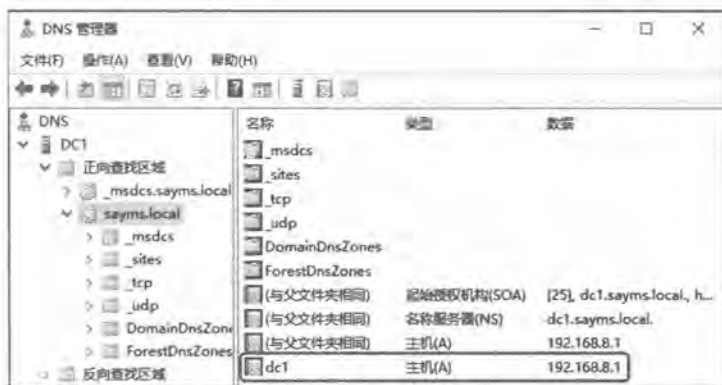


图 2-3-1

2. 利用 DNS 控制台检查 SRV 记录

如果域控制器已经正确将其所扮演角色注册到DNS服务器的话，则还会有如图2-3-2所示的_tcp、_udp等文件夹。图中_tcp文件夹右侧数据类型为服务位置（SRV）的_lldap记录，表示dc1.sayms.local已经成功地注册为域控制器。由图中的_gc记录还可以看出全局编录服务器的角色也是由dc1.sayms.local所扮演。



图 2-3-2

附注

LDAP服务器是用来提供AD DS数据库访问的服务器，而域控制器就是扮演LDAP服务器的角色。

DNS区域内有了这些数据后，其他要加入域的计算机，就可以通过此区域来得知域控制器为dc1.sayms.local。其他的域成员计算机（成员服务器、Windows 10等客户端计算机）默认也会将其主机与IP地址数据注册到此区域内。

域控制器不但会将自己所扮演的角色注册到_tcp、_sites等相关的文件夹内，还会另外注册到_msdc文件。如果DNS服务器是在安装AD DS时同时安装的，则它除了会自动建立一个用来支持AD DS的区域（sayms.local）外，还会建立一个名称为_msdc.sayms.local的区域，它是专供Windows Server域控制器来注册的，此时域控制器会将其信息注册到_msdc.sayms.local区域内，而不是_msdc文件夹。如图2-3-3所示为注册在_msdc.sayms.local区域内的部分记录。



图 2-3-3

在完成第一个域的建立之后，系统就会自动建立一个名称为Default-First-Site-Name的站点（site），而我们所建立的域控制器默认也是位于此站点内，因此在DNS服务器内也会有这些记录，例如图2-3-4中位于此站点内扮演全局编录服务器（gc）、Kerberos服务器、LDAP

服务器等三个角色的域控制器都是dc1.sayms.local。

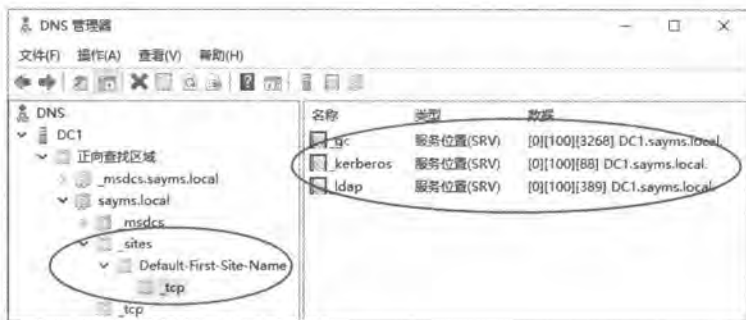


图 2-3-4

3. 利用 NSLOOKUP 命令检查 SRV 记录

可以利用NSLOOKUP命令来检查DNS服务器内的SRV记录。

- STEP 1** 单击左下角开始图标田 Windows PowerShell。
- STEP 2** 执行nslookup。
- STEP 3** 输入set type=srv后按Enter键，表示要显示SRV记录。
- STEP 4** 如图2-3-5所示输入_ldap._tcp.dc._msdcs.sayms.local后按Enter键，由图中可看出域控制器dc1.sayms.local已经成功地将其扮演LDAP服务器角色的信息注册到DNS服务器内。

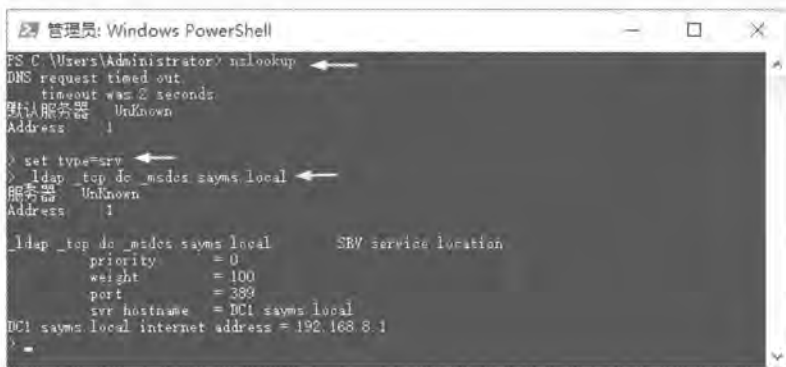


图 2-3-5

附注

界面中之所以会出现“DNS request timed out...”与“默认服务器: UnKnown”（可以不理会这些消息），是因为nslookup会根据TCP/IP处的DNS服务器IP地址设置，来查询DNS服务器的主机名，但却查询不到。如果不想出现此消息，可将网络连接处的TCP/IPv6禁用，或修改TCP/IPv6设置为“自动获取DNS服务器地址”，或在DNS服务器建立适当的IPv4/IPv6反向查找区域与PTR记录。



STEP 5 还可以利用更多类似的命令来查看其他SRV记录，例如利用 `_gc._tcp.sayms.local` 命令来查看扮演全局编录服务器的域控制器。可以利用 `ls -t SRV sayms.local` 命令来查看所有的SRV记录，不过需要事先在DNS服务器上为sayms.local区域的允许区域传送权限开放给查询计算机，否则查询会失败，并且会显示Query refused的警告消息。

2.3.2 排除注册失败的问题

如果因为域成员本身的设置有误或网络问题，造成它们无法将数据注册到DNS服务器的话，可在问题解决后，重新启动这些计算机或利用以下方法来手动注册：





- ✎ 如果是某域成员计算机的主机名与IP地址没有正确注册到DNS服务器的话，此时可到此计算机上执行 `ipconfig /registerdns` 来手动注册。完成后，到DNS服务器检查是否已有正确记录，例如域成员主机名为 `dc1.sayms.local`，IP地址为 `192.168.8.1`，则请检查区域 `sayms.local` 内是否有 `dc1` 的主机（A）记录、其IP地址是否为 `192.168.8.1`。
- ✎ 如果发现域控制器并没有将其所扮演的角色注册到DNS服务器内，也就是并没有类似前面图2-3-2中的 `tcp` 等文件夹与相关记录时，请到这台域控制器上利用【单击左下角开始图标  Windows 管理工具  服务  如图2-3-6所示选中 `Netlogon` 服务并右击  **重新启动**】的方式来注册。








图 2-3-6

附注

域控制器默认会自动每隔24小时向DNS服务器注册一次。

2.3.3 检查AD DS数据库文件与SYSVOL文件夹

AD DS数据库文件与日志文件默认是存储在 `%systemroot%\ntds` 文件夹内，可以利用【按  +  键  输入 `%systemroot%\ntds`  单击 **确定** 按钮  来检查文件夹与文件是否已经被正确地创

建,如图2-3-7中的ntds.dit就是AD DS数据库文件,而edb.log、edb00001.log等扩展名为.log的文件是日志文件(扩展名默认会被隐藏)。

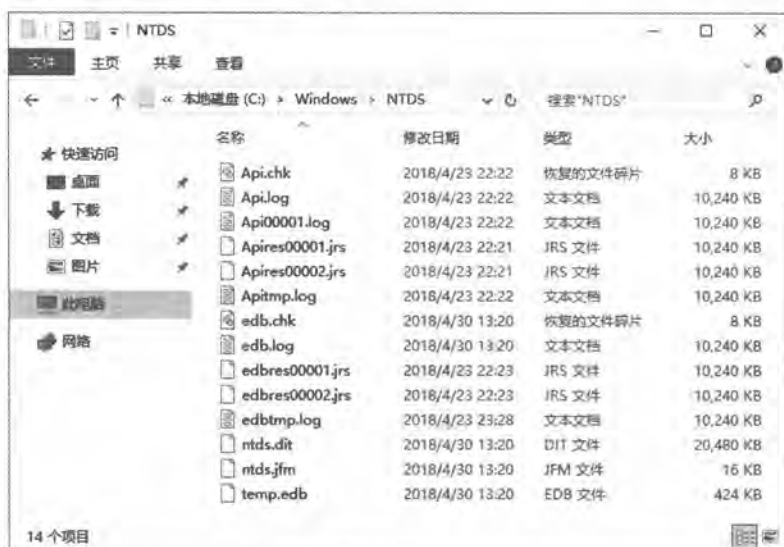


图 2-3-7

另外SYSVOL默认是被建立在%systemroot%\SYSVOL文件夹内,因此可以利用【按 $\text{Win}+\text{R}$ 键 \rightarrow 输入%systemroot%\SYSVOL \rightarrow 单击确定按钮】的方式来检查,如图2-3-8所示。

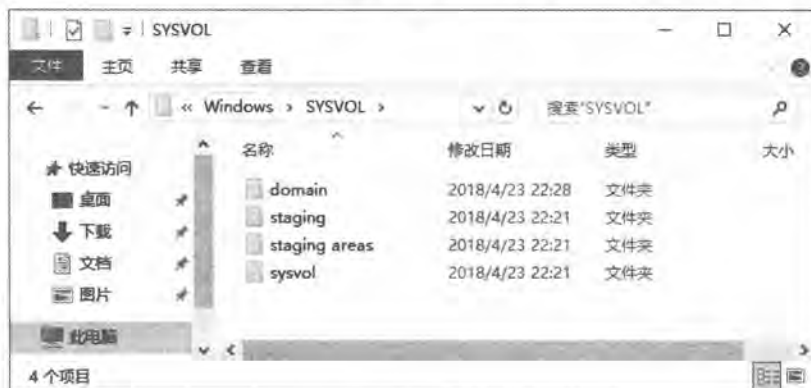


图 2-3-8

图中SYSVOL文件夹之下会有4个子文件夹,sysvol与其中的scripts都被设置为共享文件夹。可以如图2-3-9所示利用计算机管理或如图2-3-10所示利用netshare命令,来检查它们是否已被设置为共享文件夹。



图 2-3-9



图 2-3-10

2.3.4 新增的管理工具

AD DS安装完成后，通过【单击左下角开始图标→Windows管理工具】可看到新增了一些AD DS的管理工具，例如Active Directory用户和计算机、Active Directory管理中心、Active Directory站点和服务等（如图2-3-11所示）。



图 2-3-11

2.3.5 查看事件日志文件

可以利用【单击左下角开始图标田Windows管理工具事件查看器】来查看事件日志文件，以便检查任何与AD DS有关的问题，例如在图2-3-12中可以利用系统、Directory Service、DNS Server等日志文件来检查。



图 2-3-12

2.4 提升域与林功能级别

我们在1.2节内已经解说过域与林功能级别，此处将介绍如何将现有的级别提高。可以通过【单击左下角开始图标田Windows管理工具Active Directory管理中心单击域名sayms（本地）单击图2-4-1右方的提升林功能级别…或提升域功能级别…】的方法来提升级别。



图 2-4-1

也可以通过【单击左下角开始图标→Windows 管理工具→Active Directory域和信任关系→选中Active Directory域和信任关系并右击→提升林功能级别】或【单击左下角开始图标→Windows 管理工具→Active Directory用户和计算机→选中域名sayms.local并右击→提升域功能级别】的方法。可参考表2-4-1来提升域功能级别。可参考表2-4-2来提升林功能级别。

表2-4-1

当前的域功能级别	可提升的级别
Windows Server 2008	Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016
Windows Server 2008 R2	Windows Server 2012、Windows Server 2012 R2、Windows Server 2016
Windows Server 2012	Windows Server 2012 R2、Windows Server 2016
Windows Server 2012 R2	Windows Server 2016

表2-4-2

当前的林功能级别	可提升的级别
Windows Server 2008	Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016
Windows Server 2008 R2	Windows Server 2012、Windows Server 2012 R2、Windows Server 2016
Windows Server 2012	Windows Server 2012 R2、Windows Server 2016
Windows Server 2012 R2	Windows Server 2016

这些提升信息会自动被复制到所有的域控制器，不过可能需要花费15秒或更久的时间。

2.5 新建额外域控制器与RODC

一个域内如果有多台域控制器的话，便可以拥有以下优势。

- ✎ **改善用户登录的效率：**同时有多台域控制器来对客户端提供服务的话，可以分担审核用户登录身份（账户名与密码）的负担，让用户登录的效率更高。
- ✎ **容错功能：**如果有域控制器发生故障的话，此时仍然可以由其他正常的域控制器来继续提供服务，因此对用户的服务并不会停止。

在安装额外域控制器（additional domain controller）时，需要将AD DS数据库由现有的域控制器复制到这台新的域控制器，然而如果数据库非常庞大的话，这个复制操作势必会增加网络负担，尤其是这台新域控制器是位于远程网络内。系统提供了两种复制AD DS数据库的方式：

- ✎ **通过网络直接复制：**如果AD DS数据库庞大的话，此方法会增加网络负担、影响网络效率。

通过安装媒体：需要事先到一台域控制器内制作安装媒体（installation media），其中包含着AD DS数据库，接着将安装媒体复制到U盘、CD、DVD等介质或共享文件夹内。然后在安装额外域控制器时，要求安装向导到这个媒体内读取安装媒体内的AD DS数据库，这种方式可以大幅降低对网络所造成的影响。

若在安装媒体制作完成之后，现有域控制器的AD DS数据库内如果有最新的更改数据的话，这些少量数据会在完成额外域控制器的安装后，再通过网络自动复制过来。

2.5.1 安装额外域控制器

以下同时说明如何将图2-5-1中右上角dc2.sayms.local升级为额外域控制器（可读写的域控制器）、将右下角dc3.sayms.local升级为只读域控制器（RODC）。

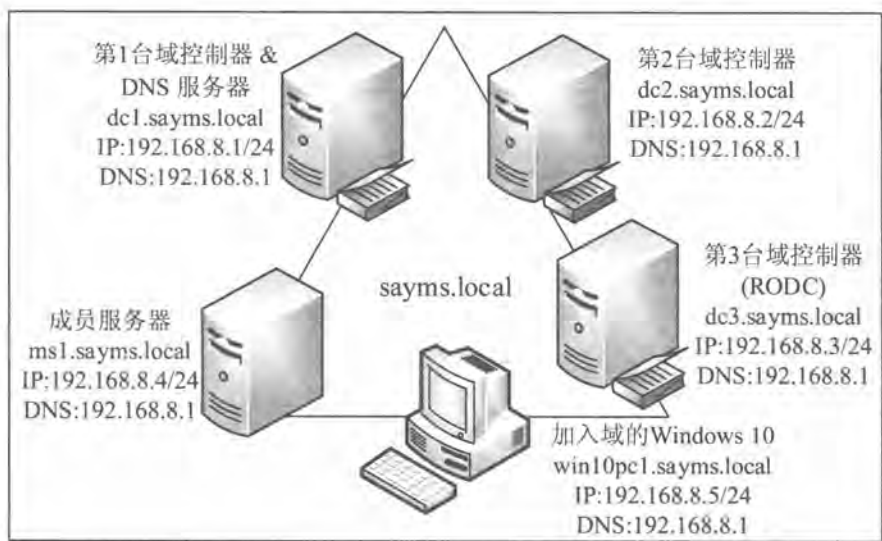


图 2-5-1

STEP 1 先在图2-5-1中的服务器dc2.sayms.local与dc3.sayms.local上安装Windows Server 2016、将计算机名称分别设置为dc2与dc3、IPv4地址等依照图所示来设置（图中采用TCP/IPv4）。注意将计算机名称分别设置为dc2与dc3即可，等升级为域控制器后，它们会分别自动被改为dc2.sayms.local与dc3.sayms.local。

STEP 2 打开服务器管理器、单击仪表板处的添加角色和功能。

STEP 3 持续单击下一步按钮，在图2-5-2中勾选Active Directory域服务、单击添加功能按钮。



图 2-5-2

STEP 4 持续单击 **下一步** 按钮，在**确认安装所选内容**界面中单击 **安装** 按钮。

STEP 5 图2-5-3为完成安装后的界面，请单击**将此服务器提升为域控制器**。



图 2-5-3

附注

如果在图2-5-3中直接单击**关闭**按钮，则之后要将其升级为域控制器的话，请如图2-5-4所示单击**服务器管理器**上方旗帜符号、单击**将此服务器提升为域控制器**。

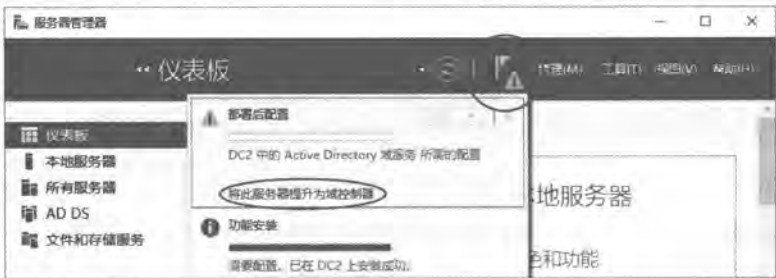


图 2-5-4

STEP 6 在图2-5-5中选择**将域控制器添加到现有域**、输入域名sayms.local、单击**更改**按钮后输入有权限添加域控制器的账户（sayms\ Administrator）与密码。完成后单击**下一步**按钮：



图 2-5-5

注意

只有Enterprise Admins或Domain Admins内的用户有权限建立其他域控制器。如果现在所登录的账户不是隶属于这两个组（例如我们现在所登录的账户为本地Administrator），则需要如前景图所示另外指定有权限的用户账户。

STEP 7 完成图2-5-6中的设置后单击 **下一步** 按钮：

- ✎ 选择是否在此服务器上安装DNS服务器（默认会）。
- ✎ 选择是否将其设置为全局编录服务器（默认会）。
- ✎ 选择是否将其设置为只读域控制器（默认不会），如果是安装dc3.sayms.local的话，请勾选此复选框。
- ✎ 设置目录服务还原模式的管理员密码（需要符合复杂性要求）。



图 2-5-6



STEP 8 如果在图2-5-6中未勾选只读域控制器（RODC），请直接跳到下一个步骤。如果是安装RODC的话，则会出现如图2-5-7所示的界面，在完成图中的设置后单击 **下一步** 按钮，然后跳到**STEP 10**：

- **委派的管理员账户**：可通过**选择**按钮来选择被委派的用户或组，他们在这台RODC将拥有本地系统管理员的权限，并且如果采用阶段式安装RODC的话（后述），则他们也可将此RODC服务器附加到（attach to）AD DS数据库内的计算机账户。默认仅Domain Admins或Enterprise Admins组内的用户有权限管理此RODC与执行附加操作。
- **允许将密码复制到RODC的账户**：默认仅允许组Allowed RODC Password Replication Group内的用户的密码可以被复制到RODC（这个组默认并无任何成员）。可通过单击**添加**按钮来添加用户或组账户。
- **拒绝将密码复制到RODC的账户**：此处的用户账户，其密码会被拒绝复制到RODC。此处的设置优先于允许将密码复制到RODC的账户的设置。部分内置的组账户（例如Administrators、Server Operators等）默认已被列于此列表内。可以通过单击**添加**按钮来添加用户或组账户。



图 2-5-7

附注

在安装域中的第一台RODC时，系统会自动建立与RODC有关的组账户，这些账户会自动被复制给其他域控制器，不过可能需要花费一点时间，尤其是复制给位于不同站点的域控制器。之后在其他站点安装RODC时，若安装向导无法从这些域控制器得到这些组信息的话，它会显示警告信息，此时等这些组信息完成复制后，再继续安装这台RODC。

STEP 9 如果不是安装RODC的话，会出现如图2-5-8所示的界面，请直接单击 **下一步** 按钮。



图 2-5-8

STEP 10 在图2-5-9中单击 **下一步** 按钮，它会直接从其他任何一台域控制器复制AD DS数据库。



图 2-5-9

STEP 11 在图2-5-10中可直接单击 **下一步** 按钮。

- **数据库文件夹**：用来存储AD DS数据库。
- **日志文件文件夹**：用来存储AD DS数据库的更改日志，此日志文件可被用来修复AD DS数据库。
- **SYSVOL文件夹**：用来存储域共享文件（例如组策略相关的文件）。



图 2-5-10

STEP 12 在**查看选项**界面中单击 **下一步** 按钮。

STEP 13 在图2-5-11界面中，如果顺利通过检查的话，就直接单击 **安装** 按钮，否则请根据界面提示先排除问题。



图 2-5-11

STEP 14 安装完成后会自动重新启动，请重新登录。

STEP 15 检查DNS服务器内是否有域控制器dc2.sayms.local与dc3.sayms.local的相关记录（参考前面2.3.1节检查DNS服务器内的记录是否完备）。

这两台域控制器的AD DS数据库内容是从其他域控制器复制过来的，而原本这两台计算机内的本地用户账户会被删除。

2.5.2 利用安装媒体来安装额外域控制器


我们将先到一台域控制器上制作**安装媒体**（installation media），也就是将AD DS数据库存储到**安装媒体**内，并将**安装媒体**复制到U盘、CD、DVD等媒体或共享文件夹内。然后在安装额外域控制器时，要求安装向导从**安装媒体**来读取AD DS数据库，这种方式可以大幅降低对网络所造成的负担。

1. 制作安装媒体

请到现在的一台域控制器上执行ntdsutil命令来制作**安装媒体**：

- ❏ 如果此安装媒体是要给**可读写域控制器**来使用的话，则需要到现在的一台**可读写域控制器**上执行ntdsutil命令。
- ❏ 如果安装媒体是要给**RODC**（只读域控制器）来使用的话，则可以到现在的一台**可读写域控制器**或**RODC**上执行ntdsutil命令。

STEP 1 请到域控制器上利用域管理员的身份登录。

STEP 2 单击左下角开始图标 Windows PowerShell。

STEP 3 输入以下命令后按Enter键（操作界面可参考图2-5-12）：

```
ntdsutil
```

STEP 4 在ntdsutil：提示符下，执行以下命令：

```
activate instance ntds
```

它会将此域控制器的AD DS数据库设置为使用中。

STEP 5 在ntdsutil：提示符下，执行以下命令

```
ifm
```

STEP 6 在ifm：提示符下，执行以下命令：

```
create sysvol full c:\InstallationMedia
```

这条命令假设是要将**安装媒体**的内容存储到C:\InstallationMedia文件夹。

附注

其中的**sysvol**表示要制作包含ntds.dit与SYSVOL的**安装媒体**；**full**表示要制作供可读写域控制器使用的**安装媒体**，如果是要制作供RODC使用的安装媒体的话，请将**full**改为**rodc**。

STEP 7 连续执行两次quit命令来结束ntdsutil。图2-5-12为部分的操作界面。

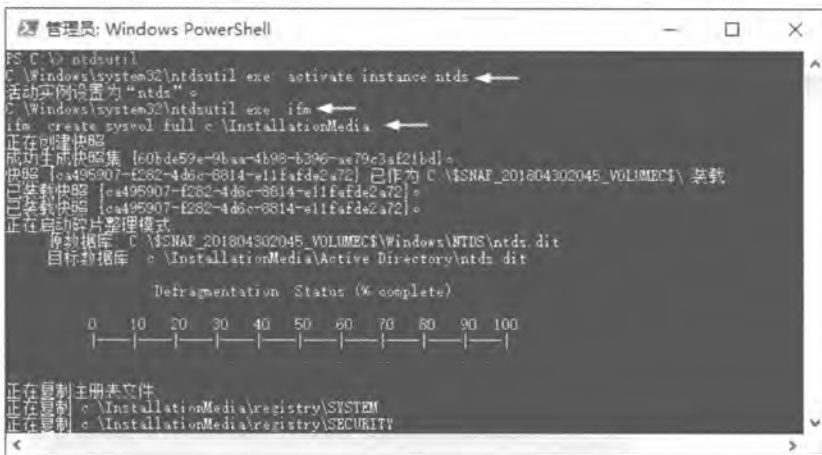


图 2-5-12

STEP 8 将整个C:\InstallationMedia文件夹内的所有数据复制到U盘、CD、DVD等媒体或共享文件夹内。

2. 安装额外域控制器

将包含**安装媒体**的U盘、CD或DVD拿到即将扮演额外域控制器角色的计算机上，或是将

其放到可以访问到的共享文件夹内。

由于利用**安装媒体**来安装额外域控制器的方法与前一节大致上相同，因此以下仅列出不同之处。以下假设**安装媒体**被复制到即将升级为额外域控制器的服务器的C:\InstallationMedia文件夹内：在图2-5-13中选择**指定从介质安装（IFM）选项**，并在**路径**处指定存储**安装媒体**的文件夹C:\InstallationMedia。



图 2-5-13

安装过程中会从**安装媒体**所在的文件夹C:\InstallationMedia复制AD DS数据库。如果在**安装媒体**制作完成之后，现有域控制器的AD DS数据库产生新的更新数据的话，这些少量数据会在完成额外域控制器安装后，再通过网络自动复制过来。

2.5.3 更改RODC的委派与密码复制策略设置

如果要更改密码复制策略设置或RODC管理工作的委派设置的话，请在打开**Active Directory 用户和计算机**后：【如图2-5-14所示单击容器**Domain Controllers**右侧扮演RODC角色的域控制器，单击上方的**属性**图标，通过图2-5-15中的**密码复制策略与管理者**选项卡进行设置】。



图 2-5-14

也可以通过**Active Directory管理中心**来更改上述设置：打开**Active Directory管理中心**后，如图2-5-16所示【选择容器**Domain Controllers**界面中间扮演RODC角色的域控制器，单击右侧的**属性**，通过图2-5-17中的**管理者**小节与**扩展**小节中的**密码复制策略**选项卡进行设置】。

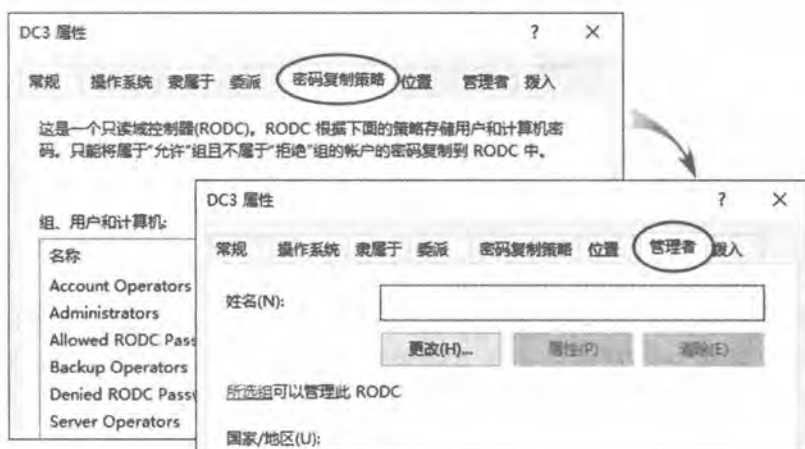


图 2-5-15

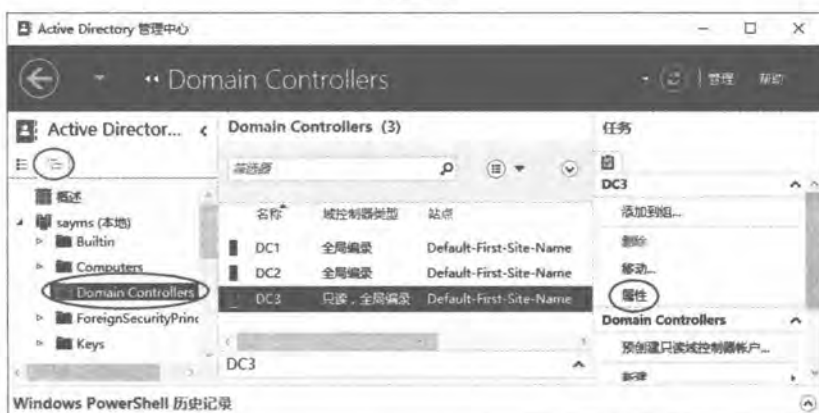


图 2-5-16

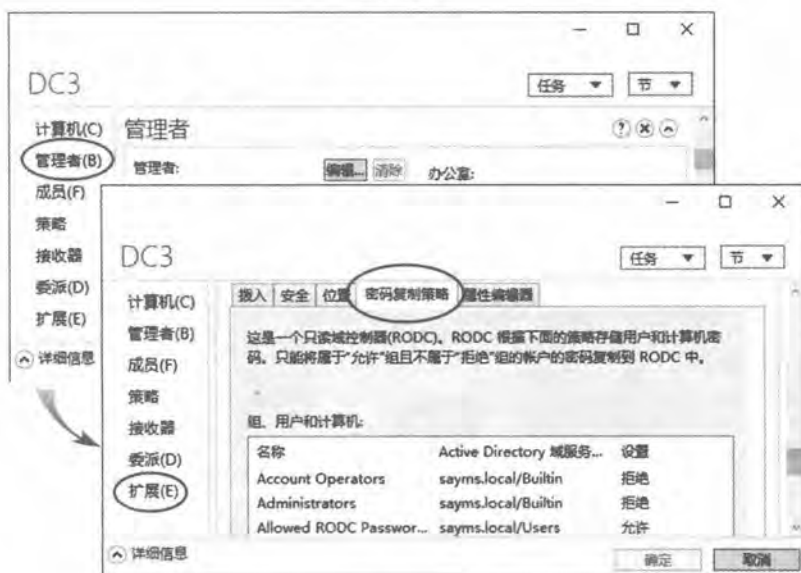


图 2-5-17

2.6 RODC阶段式安装

可以采用两个阶段的方式来安装RODC（只读域控制器），这两个阶段是分别由不同的用户来完成，这种安装方式通常是用来安装远程分公司所需的RODC。

第1阶段：建立RODC账户

此阶段通常是在总公司内执行，并且只有域管理员（Domain Admins组的成员）才有权限来执行这一阶段的工作。在此阶段内，域管理员需要在AD DS数据库内为RODC建立计算机账户、设置选项、将第2阶段的安装工作委派给指定的用户或组。

第2阶段：将服务器附加到RODC账户

此阶段通常是在远程分公司内执行，被委派的用户有权限在此阶段来完成安装RODC的工作。被委派的用户并不需要具备域管理员权限。如果没有委派其他用户或组的话，则默认只有Domain Admins或Enterprise Admins组内的用户有权限执行这个阶段的安装工作。

在此阶段内，被委派的用户需要在远程分公司将即将成为RODC的服务器附加（attach）到第1个阶段中所建立的计算机账户，便可完成RODC的安装工作。

2.6.1 建立RODC账户

一般来说，阶段式安装主要是用来在远程分公司（另外一个AD DS站点内）安装RODC，不过为了方便起见，本节以它是被安装到同一个站点内为例来说明，也就是默认的站点Default-First-Site-Name。以下步骤说明如何采用阶段式安装方式，来将图2-6-1中右下角的dc4.sayms.local升级为只读域控制器（RODC）。

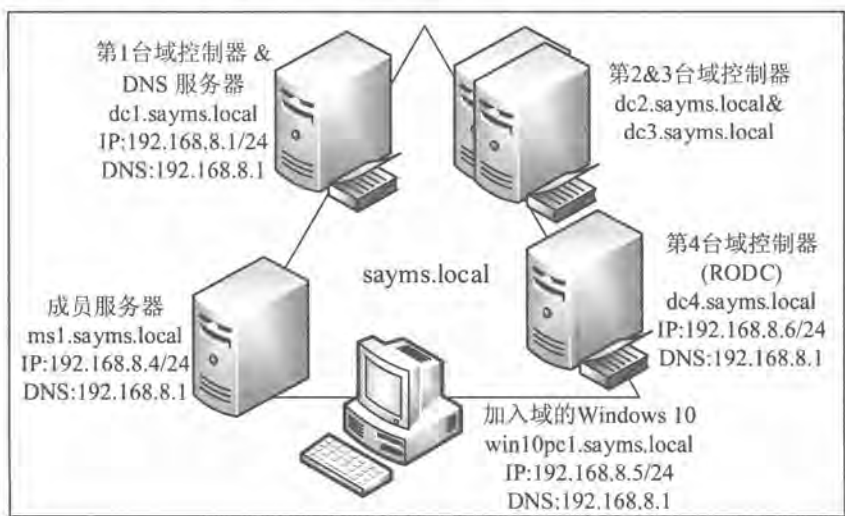


图 2-6-1

STEP 1 请到现在有一台域控制器上利用域系统管理员身份登录。





STEP 2 单击左下角开始图标  Windows 管理工具  Active Directory 用户和计算机  如图2-6-2所示选中容器 Domain Controllers 并右击  预创建只读域控制器账户 (如果使用 Active Directory 管理中心的话, 参考图2-6-3)。



图 2-6-2



图 2-6-3


STEP 3 如图2-6-4所示勾选使用高级模式安装后单击  下一步按钮。



图 2-6-4


STEP 4 当前登录的用户为域 Administrator, 他有权安装域控制器, 故请在图2-6-5中选中我的当前登录凭据后单击  下一步按钮。



图 2-6-5

注意

若当前登录的用户没有权限安装域控制器的话，请选中图中的**备用凭据**，然后通过单击**设置**按钮来输入有权限的用户名与密码。

STEP 5 在图2-6-6中输入即将扮演RODC角色的服务器的计算机名称，例如dc4，完成后单击**下一步**按钮。



图 2-6-6

STEP 6 在图2-6-7中选择新域控制器所在的AD DS站点，目前只有一个默认的站点Default-First-Site-Name。请直接单击**下一步**按钮。



图 2-6-7

STEP 7 在图2-6-8中直接单击 **下一步** 按钮。由图中可知它会在此服务器上安装DNS服务器，同时会将其设置为全局编录服务器，并自动勾选只读域控制器（RODC）。

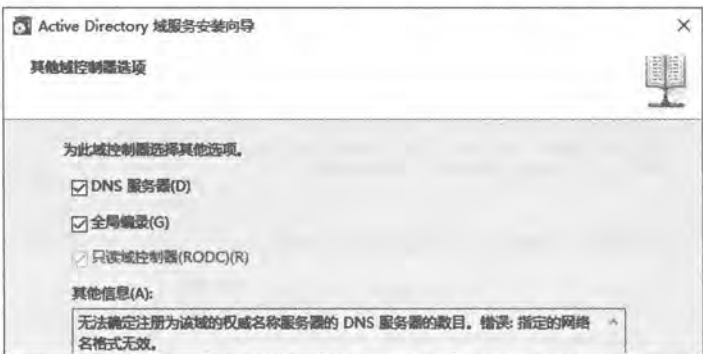


图 2-6-8

STEP 8 通过图2-6-9来设置指定密码复制策略：图中默认仅允许组Allowed RODC Password Replication Group内的用户的密码可以被复制到RODC（此组内默认并无任何成员），并且一些重要账户（例如Administrators、Server Operators等组内的用户）的密码已明确地被拒绝复制到RODC。可以通过单击 **添加** 按钮来添加用户或组账户，单击 **下一步** 按钮。

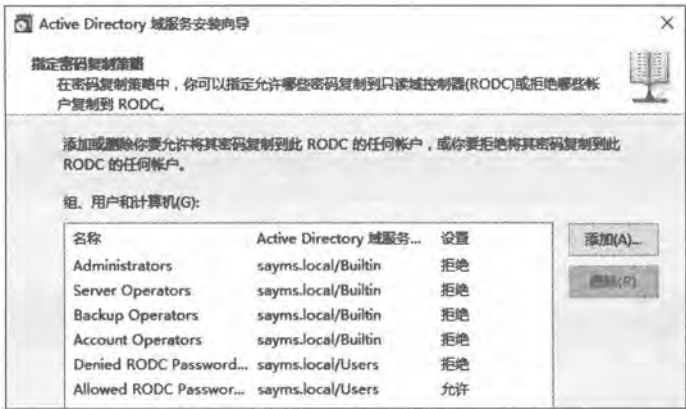


图 2-6-9

附注

在安装域中的第1台RODC时，系统会自动建立与RODC有关的组账户，这些账户会自动被复制给其他域控制器，不过可能需要花费一点时间，尤其是复制给位于不同站点的域控制器。之后在其他站点安装RODC时，如果安装向导无法从这些域控制器得到这些组信息的话，它会显示警告信息，此时请这些组信息完成复制后，再继续安装这台RODC。

STEP 9 在图2-6-10中将安装RODC的工作委派给指定的用户或组，图中将其委派给域（SAYMS）用户george。RODC安装完成后，该用户在这台RODC内会自动被赋予本地系统管理员的权限，单击 **下一步** 按钮。



图 2-6-10

STEP 10 接下来依次单击 **下一步** 按钮、**完成** 按钮，图2-6-11为完成后的界面。



图 2-6-11

2.6.2 将服务器附加到RODC账户

STEP 1 请在图2-6-1中右边的服务器dc4.sayms.local上安装Windows Server 2016、将其计算机名称设置为dc4、IPv4地址等依照图所示进行设置（此处采用TCP/IPv4）。请将其计算

机名称设置为dc4即可，等升级为域控制器后，会自动被改为dc4.sayms.local。

STEP 2 打开服务器管理器、单击仪表板处的添加角色和功能。

STEP 3 持续单击 **下一步** 按钮，在图2-6-12中勾选 **Active Directory域服务**，单击 **添加功能** 按钮。



图 2-6-12

STEP 4 持续单击 **下一步** 按钮，在 **确认安装选项** 界面中单击 **安装** 按钮。

STEP 5 图2-6-13为完成安装后的界面，请单击 **将此服务器提升为域控制器**。



图 2-6-13

附注

如果在图2-6-13中直接单击关闭按钮，则之后要将其升级为域控制器的话，请单击 **服务器管理器** 上方旗帜符号并单击 **将此服务器提升为域控制器**。

STEP 6 在图2-6-14中选择 **将域控制器添加到现有域**，输入域名 sayms.local，单击 **更改** 按钮后输入被委派的用户名称（sayms\george）与密码后单击 **确定** 按钮、**下一步** 按钮：

注意

可输入被委派的用户账户、Enterprise Admins或Domain Admins组内的用户账户。



图 2-6-14

STEP 7 接下来会出现如图2-6-15所示的界面，由于其计算机账户已经事先在AD DS内创建完成，因此会多显示图上方的两个选项。在选择默认的选项与设置目录服务还原模式的密码后（需符合复杂性要求）单击 **下一步** 按钮。



图 2-6-15

STEP 8 在图2-6-16中单击 **下一步** 按钮，它会直接从其他任何一台域控制器复制AD DS数据库。



图 2-6-16

- STEP 9
- 接下来的路径与查看选项界面中都可直接单击下一步按钮。

STEP 10

在如图2-6-17所示的界面中，如果顺利通过检查，就直接单击安装按钮，否则请根据界面提示先排除问题。



图 2-6-17

- STEP 11
- 安装完成后会自动重新启动。请重新登录。

STEP 12

图2-6-18为完成后，通过Active Directory用户和计算机控制台所看到的界面，其中DC4图形上原本的向下箭头已消失。

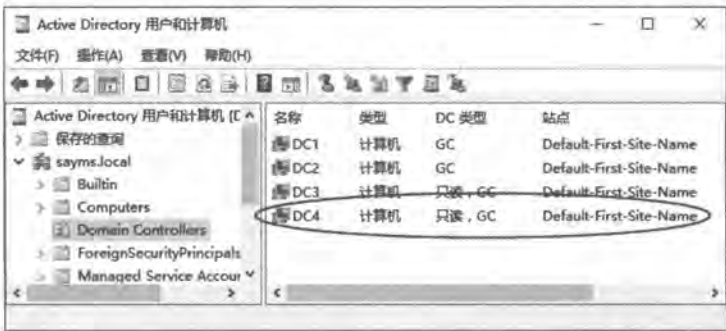


图 2-6-18

2.7 将Windows计算机加入或脱离域

Windows计算机加入域后，便可以访问AD DS数据库与其他域资源，例如用户可以在这些计算机上利用域用户账户来登录域，并利用此账户来访问其他域成员计算机内的资源。以下是可以被加入域的计算机：

- Windows Server 2016 Datacenter/Standard
- Windows Server 2012 (R2) Datacenter/Standard
- Windows Server 2008 (R2) Datacenter/Enterprise/Standard
- Windows 10 Enterprise/Pro/Education
- Windows 8.1 (8) Enterprise/Pro
- Windows 7 Ultimate/ Enterprise/Professional
- Windows Vista Ultimate/Enterprise/Business

2.7.1 将Windows计算机加入域

我们要将图2-7-1左下角的服务器ms1加入域，假设它是Windows Server 2016 Datacenter；同时也要将下方的Windows 10计算机加入域，假设它是Windows 10 Pro。以下利用服务器ms1（Windows Server 2016）来说明。

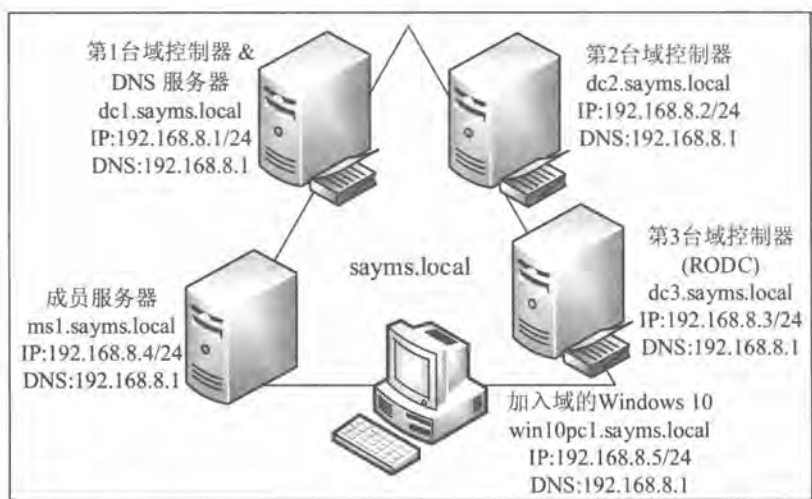


图 2-7-1

附注

加入域的客户端计算机，其计算机账户默认会自动被建立在Computers容器内，如果想将此计算机账户放置到其他容器或组织单位的话，可以事先在该容器或组织单位内建立此计算机账户。如果是使用**Active Directory用户和计算机**：【选中该容器或组织单位并右击**新建计算机**】，如果是使用**Active Directory管理中心**：【单击该容器或组织单位后**单击右侧任务窗格的新建计算机**】。

STEP 1 请先将该台计算机的计算机名称设置为ms1、IPv4地址等设置为图2-7-1中所示。注意计算机名称设置为ms1即可，等加入域后，其计算机名称自动会被改为ms1.sayms.local。

STEP 2 打开服务器管理器⇨单击左侧本地服务器⇨如图2-7-2所示单击中间工作组处的WORKGROUP。



图 2-7-2

如果是Windows 10计算机的话：【单击下方的文件资源管理器图标⇨选中此电脑并右击⇨属性⇨单击右侧的更改设置⇨……】。

如果是Windows 8.1计算机的话：【切换到开始菜单（可按Windows键⇨）⇨单击菜单左下方⇨符号⇨选中图2-7-3的这台电脑并右击⇨单击下方属性⇨……】。



图 2-7-3

如果是Windows 8计算机的话：【按⇨键切换到开始菜单⇨选中空白处并右击⇨单击所有应用⇨选中计算机右击⇨单击下方属性⇨……】。

如果是Windows Server 2008（R2）、Windows 7与Windows Vista的话：【开始⇨选中计算机并右击⇨属性⇨单击右下角的更改设置】。

附注

因为Windows Vista（含）之后的系统默认已经启用用户账户控制，因此如果不是本地系统管理员的话，则此时系统会先要求输入本地系统管理员的密码。

STEP 3 单击图2-7-4中的**更改**按钮。



图 2-7-4

STEP 4 选择图2-7-5中的**域**，输入域名 sayms.local，单击**确定**按钮，输入域内任何一个用户账户与密码（此账户需要隶属于Domain Users组，图中使用Administrator），单击**确定**按钮（一般域用户账户只有10次将计算机加入域的机会，但是域系统管理员没有次数限制）。



图 2-7-5

注意

如果出现错误警告的话，请检查TCP/IPv4设置是否有误，尤其是**首选DNS服务器**的IPv4地址是否正确，以本范例来说应该是192.168.8.1。

STEP 5 出现如图2-7-6所示的界面表示已经成功地加入域（其计算机账户会被建立在AD DS数据库内），请单击**确定**按钮。



图 2-7-6

注意

若出现错误界面的话，请检查所输入的用户名称与密码是否正确。

STEP 6 出现需要重启计算机的界面时单击**确定**按钮。

STEP 7 回到图2-7-7可看出，加入域后，其完整计算机名称的后缀就会附上域名，如图中的ms1.sayms.local，单击**关闭**按钮。

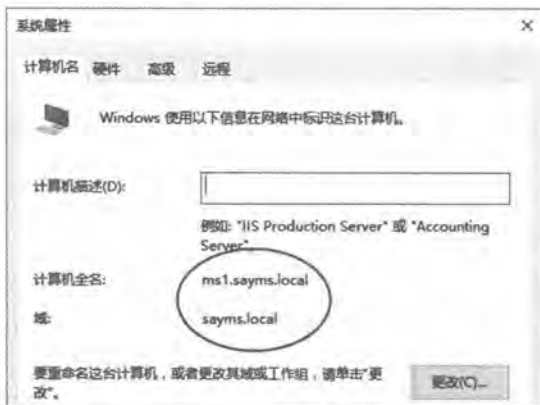


图 2-7-7

STEP 8 依照界面提示重新启动计算机。

STEP 9 请重复以上步骤将图2-7-1中的Windows 10计算机加入域。

2.7.2 利用已加入域的计算机登录

可以在已经加入域的计算机上，利用本机或域用户账户来登录。

1. 利用本地用户账户登录

出现登录界面时，如果要用本地用户账户登录的话，请在账户前输入计算机名称，如图



2-7-8所示msl\administrator，其中msl为计算机名称、administrator为用户账户名称，接着输入其密码就可以登录。

此时系统会利用本地安全数据库来检查账户与密码是否正确，如果正确，就能成功登录，也可以访问此计算机内的资源(如果有权限的话)，不过无法访问域内其他计算机的资源，除非在连接其他计算机时另外输入有权限的用户名称与密码。



图 2-7-8

2. 利用域用户账户登录

如果要使用域用户账户登录的话，请在账户前输入域名，如图2-7-9所示的sayms\administrator，表示要利用域sayms内的账户administrator来登录，接着输入其密码就可以登录（账户名称前面的域名也可以是DNS域名，例如sayms.local\Administrator）。



图 2-7-9

用户账户名称与密码会发送给域控制器，并利用AD DS数据库来检查账户与密码是否正确，如果正确，就可以成功登录，并且可以直接连接域内任何一台计算机与访问其中的资源(如果被赋予权限的话)，不需要再另外手动输入用户名与密码。

2.7.3 脱机加入域

旧版本Windows客户端计算机要加入域的话，该计算机需要连接网络，而且必须能够直接与域控制器通信，从Windows 7开始的客户端计算机具备脱机加入域的功能（offline domain join），也就是让它们在并未与域控制器连接的情况下，就可以被加入域。我们需要通过djoin.exe程序来执行脱机加入域的程序。

先到一台已经加入域的计算机上，利用djoin.exe来创建一个文本文件，此文件内包含即将加入域的计算机所需的所有信息。接着到即将加入域的脱机计算机上，利用djoin.exe来将上述文件内的信息导入到此计算机内。

以下假设域名为sayms.local、一台已经加入域的成员服务器为ms1、即将脱机加入域的计算机为win10pc2。为了实际练习脱机加入域功能，请确认win10pc2是处于脱机状态。脱机将win10pc2加入域的步骤如下所示。

STEP 1 到成员服务器ms1上利用域管理员身份登录，然后执行以下的djoin.exe程序（参考图2-7-10），它会创建一个文本文件，此文件内包含脱机计算机win10pc2所需的所有信息：

```
Djoin /provision /domain sayms.local /machine win10pc2 /savefile win10pc2.txt
```

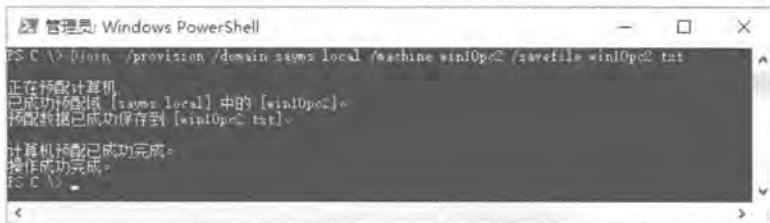


图 2-7-10

STEP 2 其中sayms.local为域名、win10pc2为脱机计算机的计算机名称、win10pc2.txt为所创建的文本文件（图中的文件win10pc2.txt会被创建在C:\）。此命令默认会将计算机账户win10pc2创建到Computers容器内（如图2-7-11所示）。



图 2-7-11

STEP 3 在即将加入域的脱机计算机win10pc2上利用djoin.exe来将上述文件内的信息导入到win10pc2。Windows 10计算机必须以系统管理员身份来执行此程序，因此请使用【单击左下角开始图标➤Windows系统➤选中命令提示符并右击➤更多➤以管理员身份运行】（Windows 10 1703版可使用【选中左下角开始图标➤右击➤Windows PowerShell（管理员）】），然后执行以下命令（参见图2-7-12，图中假设我们已经将文件win10pc2.txt复制到计算机win10pc2的C:\）：

```
Djoin /requestODJ /loadfile C:\win10pc2.txt /windowspath %SystemRoot%\localos
```



图 2-7-12

STEP 4 当win10pc2连上网络并且可以与域控制器通信时，请重新启动win10pc2，它便完成了加入域的操作。

2.7.4 脱离域

脱离域的方法与加入域的方法大同小异，不过必须是Enterprise Admins、Domain Admins的成员或本地系统管理员才有权限将此计算机脱离域。还有因为从Windows 7开始的计算机默认已经启用用户账户控制，因此如果没有权限更改此设置的话，系统会先要求输入有权限的账户名称与密码。

脱离域的方法为（以Windows Server 2016为例）：【打开服务器管理器➤单击左侧本地服务器➤单击右侧域处的sayms.local➤单击更改按钮➤选择图2-7-13中的工作组➤输入适当的工作组名称（例如WORKGROUP）➤出现欢迎加入工作组界面时单击确定按钮➤重新启动计算机】。

接下来会出现如图2-7-14所示的提示界面：一旦脱离域后，在这台计算机上只能利用本地用户账户来登录，无法再使用域用户账户，因此确认已掌握本



图 2-7-13

地系统管理员的密码后再单击 **确定** 按钮，否则单击 **取消** 按钮。

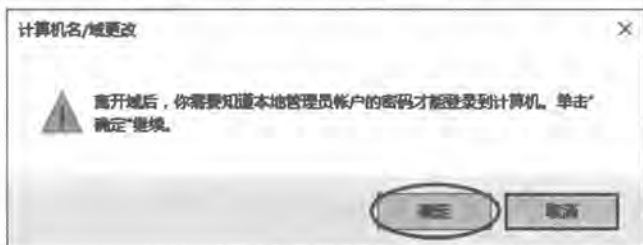


图 2-7-14

2.8 在域成员计算机内安装AD DS管理工具

非域控制器的Windows Server 2016、Windows Server 2012(R2)、Windows Server 2008(R2)等成员服务器与Windows 10、Windows 8.1(8)、Windows 7等客户端计算机内默认并没有管理AD DS的工具，例如**Active Directory用户和计算机**、**Active Directory管理中心**等，不过只要另外安装这些工具后，就可以在这些计算机上利用安装的工具来管理AD DS。

1. Windows Server 2016、Windows Server 2012(R2)成员服务器

Windows Server 2016、Windows Server 2012(R2)成员服务器可以通过添加角色和功能的方式来拥有AD DS管理工具：**【打开服务器管理器⇨单击仪表板处的添加角色和功能⇨持续单击下一步按钮并在图2-8-1的选择功能界面时勾选远程服务器管理工具之下的AD DS和AD LDS工具】**，安装完成后可以到开始菜单的**Windows 管理工具（系统管理工具）**来执行这些工具。



图 2-8-1

2. Windows Server 2008 R2、Windows Server 2008 成员服务器

Windows Server 2008 R2、Windows Server 2008成员服务器可以通过添加功能的方式来拥

有AD DS管理工具：**【打开服务器管理器**➡单击功能右侧的**添加功能**➡勾选图2-8-2中**远程服务器管理工具**之下的**AD DS和AD LDS工具**】，安装完成后可以到**系统管理工具**中执行这些工具。

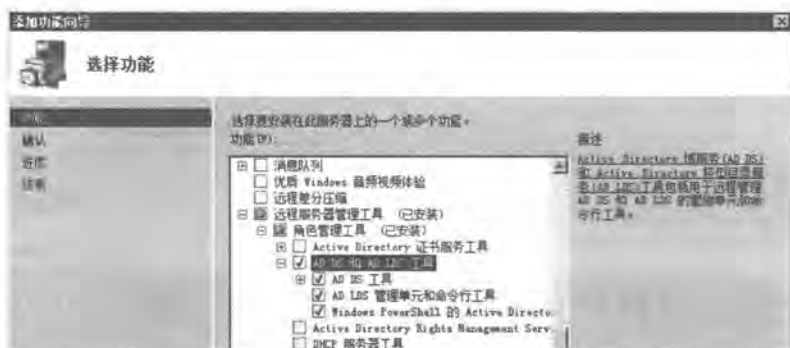


图 2-8-2

3. Windows 10、Windows 8.1、Windows 8

Windows 10计算机需要到微软网站下载与安装Remote Server Administration Tools for Windows 10(Windows 10的远程服务器管理工具)，安装完成后可通过**【单击左下角开始图标**➡**Windows管理工具**】来选用**Active Directory管理中心**与**Active Directory用户和计算机**等工具。

Windows 8.1计算机需要到微软网站下载与安装Remote Server Administration Tools for Windows 8.1 (Windows 8.1 的远程服务器管理工具)，安装完成后可通过**【按Windows键**⊞**切换到开始菜单**➡单击菜单左下方⊞图标➡**管理工具**】来选用**Active Directory管理中心**与**Active Directory用户和计算机**等工具。

Windows 8计算机需要到微软网站下载与安装Remote Server Administration Tools for Windows 8 (Windows 8的远程服务器管理工具)，安装完成后可通过**【按Windows键**⊞**切换到开始菜单**➡**管理工具**】来选用这些工具。

4. Windows 7

Windows 7计算机需要到微软网站下载与安装Remote Server Administration Tools for Windows 7 with SP1 (Windows 7 SP1的远程服务器管理工具)，安装完成之后选用**【开始**➡**控制面板**➡单击最下方的**程序**➡单击最上方的**打开或关闭Windows功能**➡勾选图2-8-3中**远程服务器管理工具**之下的**Active Directory管理中心**】。完成之后，就可以在**【开始**➡**系统管理工具**】中来选用**Active Directory管理中心**与**Active Directory用户和计算机**等工具。



图 2-8-3

2.9 删除域控制器与域

可以通过降级的方式来删除域控制器，也就是将AD DS从域控制器中删除。在降级前请先注意以下事项：

- 如果域内还有其他域控制器存在，会被降级为该域的成员服务器，例如将图2-9-1中的 dc2.sayms.local降级时，由于还有另外一台域控制器dc1.sayms.local存在，因此dc2.sayms.local会被降级为域sayms.local的成员服务器。必须是Domain Admins或Enterprise Admins组的成员才有权限删除域控制器。

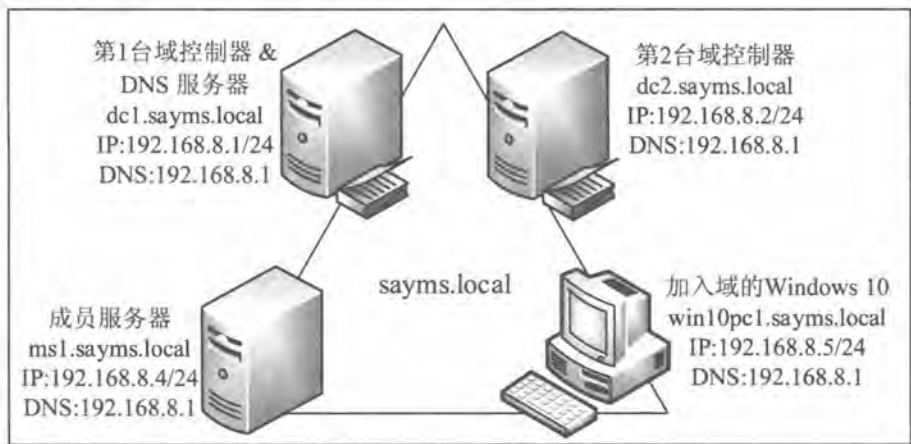


图 2-9-1

- 如果这台域控制器是此域内的最后一台域控制器，例如假设图2-9-1中的dc2.sayms.local已被降级，此时再将dc1.sayms.local降级的话，则域内将不会再有其



他域控制器存在，因此域会被删除，而dc1.sayms.local也会被降级为独立服务器。
必须是Enterprise Admins组的成员，才有权删除域内的最后一台域控制器（也就是删除域）。如果此域之下还有子域的话，请先删除该子域。

附注

建议先将成员服务器dc2.sayms.local脱离域，因为域删除后，在这台dc2.sayms.local计算机上利用域账户就无法登录了。

- ❏ 如果此域控制器是全局编录服务器的话，请检查其所属站点（site）内是否还有其他全局编录服务器，如果没有的话，请先分配另外一台域控制器来扮演全局编录服务器。否则将影响用户登录，分配的方法为：【单击左下角开始图标→Windows 管理工具→Active Directory 站点和服务→Sites→Default-First-Site-Name→Servers→选择服务器→选中NTDS Settings并右击→属性→勾选全局编录】。
- ❏ 如果所删除的域控制器是林内最后一台域控制器的话，则林会一并被删除。Enterprise Admins组的成员才有权删除这台域控制器与林。

移除域控制器的步骤如下所示：

STEP 1 单击左下角开始图标→服务器管理器→单击图2-9-2中管理菜单下的删除角色和功能。



图 2-9-2

STEP 2 持续单击下一步按钮，在出现如图2-9-3所示的界面时，取消勾选Active Directory域服务，单击删除功能按钮。

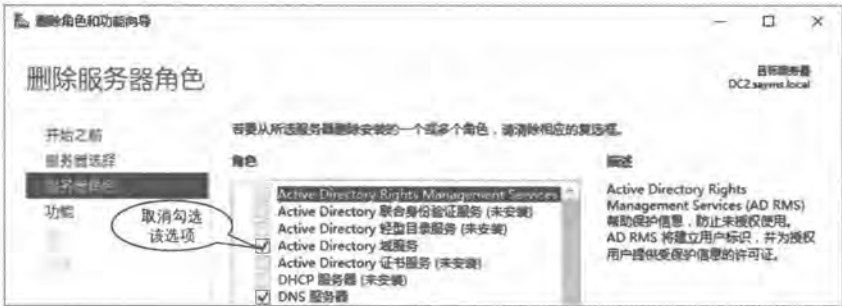


图 2-9-3

STEP 3 出现如图2-9-4所示的界面时，单击**将此域控制器降级**。



图 2-9-4

STEP 4 如果当前用户有权限删除此域控制器的话，请在图2-9-5中直接单击**下一步**按钮，否则单击**更改**按钮来输入另一个账户与密码。

附注

如果因故无法删除此域控制器的话（例如在移除域控制器时，需要连接到其他域控制器，但却无法连接），此时可勾选图中的**强制删除此域控制器**。



图 2-9-5

如果是最后1台域控制器，请勾选图2-9-6中域中的最后一个域控制器。



图 2-9-6

STEP 5 在图2-9-7中勾选继续删除后单击下一步按钮。



图 2-9-7

STEP 6 如果出现如图2-9-8所示界面的话, 可选择是否要删除DNS区域与应用程序分区, 后单击下一步按钮。

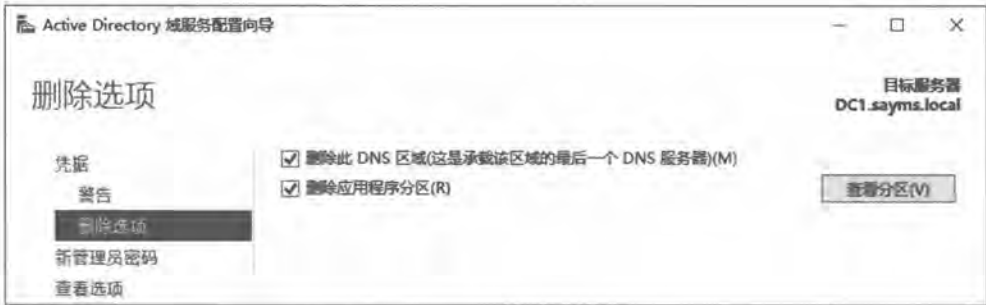


图 2-9-8

附注 RODC: 会有保留域控制器元数据选项供选择, 此时可直接单击下一步按钮即可。

STEP 7 在图2-9-9中为这台即将被降级为独立或成员服务器的计算机, 设置其本地 Administrator 的新密码 (需要符合密码复杂性要求) 后单击下一步按钮。

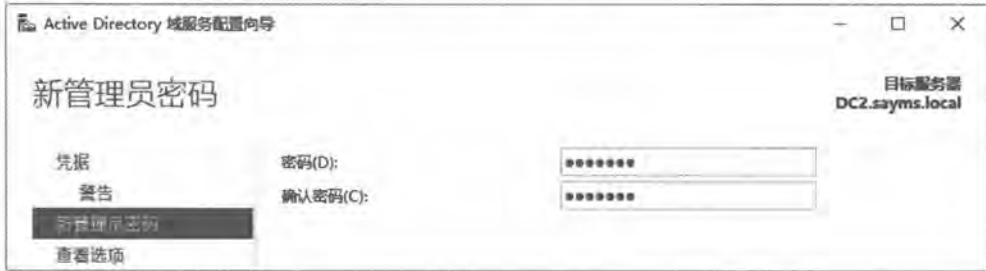


图 2-9-9

STEP 8 在查看选项界面中单击降级按钮。

STEP 9 完成后会自动重新启动计算机，再重新登录。

附注

虽然这台服务器已经不再是域控制器了，不过此时其**Active Directory域服务**组件仍然存在，并没有被删除，因此如果现在要再重新将其升级为域控制器的话，可以参考前面的说明。

STEP 10 在**服务器管理器**中选择**管理**菜单下的**删除角色和功能**。

STEP 11 持续单击**下一步**按钮，直到出现如图2-9-10所示的界面时，取消勾选**Active Directory域服务**，单击**删除功能**按钮。



图 2-9-10

STEP 12 回到**删除服务器角色**界面时，确认**Active Directory域服务**已经被取消勾选（也可以一并取消勾选**DNS服务器**）后单击**下一步**按钮。

STEP 13 出现**删除功能**界面时，单击**下一步**按钮。

STEP 14 在**确认删除选项**界面中单击**删除**按钮。

STEP 15 完成后，重新启动计算机。