1

第 1 章　Active Directory 域服务（AD DS）

在Windows Server的网络环境中，Active Directory域服务（Active Directory Domain Services，AD DS）提供了各种强大的功能来组织、管理与控制网络资源。

- 1.1 Active Directory域服务概述
- 1.2 域功能级别与林功能级别
- 1.3 Active Directory轻型目录服务

1.1 Active Directory域服务概述

什么是**directory**呢？日常生活中的电话簿内记录着亲朋好友的姓名与电话等数据，这是**telephone directory**（电话目录）；计算机中的文件系统（file system）内记录着文件的文件名、大小与日期等数据，这是**file directory**（文件目录）。

如果有系统能对这些directory内的数据加以整理，那么用户就能够很容易地快速查找到所需数据，而directory service（目录服务）所提供的服务就是让用户容易且快速地在Directory内查找所需数据。

Active Directory域内的directory database（目录数据库）被用来存储用户账户、计算机账户、打印机与共享文件夹等对象，而提供目录服务的组件就是**Active Directory域服务（AD DS）**，它负责目录数据库的存储、添加、删除、修改与查询等工作。

1.1.1 Active Directory域服务的适用范围

Active Directory域服务的适用范围（scope）非常广泛，可以用在单台计算机、小型局域网络（LAN）或多个广域网（WAN）的组合。它涵盖了该范围中的所有对象，例如文件、打印机、应用程序、服务器、域控制器与用户账户等。

1.1.2 命名空间

命名空间（namespace）是一个界定好的区域（bounded area），在此区域内，我们可以利用某个名称来找到与此名称有关的信息。例如一本电话簿就是一个**命名空间**，在这本电话簿内（界定好的区域内），我们可以利用姓名来找到此人的电话、地址与生日等数据。又例如Windows操作系统的NTFS文件系统也是一个**命名空间**，在此文件系统内，我们可以利用文件名来找到此文件的大小、修改日期与文件内容等数据。

Active Directory域服务（AD DS）也是一个**命名空间**，利用它，我们可以通过对象名称来找到与此对象有关的所有信息。

在TCP/IP网络环境内利用域名系统（Domain Name System，DNS）来解析主机名与IP地址的对应关系，例如通过DNS来得知主机的IP地址。AD DS也与DNS紧密地集成在一起，它的域名**空间**也是采用DNS架构，因此域名采用DNS格式来命名，例如可以将AD DS的域名命名为sayms.local。

1.1.3 对象与属性

AD DS内的资源是以**对象**（object）的形式存在，例如用户、计算机等都是对象，而对象通过**属性**（attribute）来描述其特征，也就是说对象本身是一些**属性**的集合。例如，如果要为

用户**王乔治**创建账户，则需添加一个对象类型（object class）为**用户**（user）的对象（也就是用户账户），然后在此对象内输入**王乔治**的姓、名、登录账户与地址等信息，其中的用户账户就是对象，而姓、名与登录账户等就是该对象的属性（见表1-1-1）。另外，图1-1-1中的**王乔治**就是对象类型为**用户**的对象。

表1-1-1 创建对象和属性

对象（object）	属性（attributes）
用户（user）	姓 名 登录账户 地址 ……

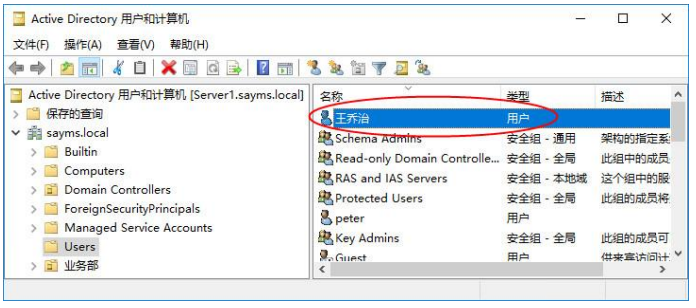

图 1-1-1

1.1.4　容器与组织单位

容器（container）与对象相似，也有自己的名称，也是一些属性的集合，不过容器内可以包含其他对象（例如**用户**、**计算机**等），也可以包含其他容器。而组织单位（organization units，OU）是一个比较特殊的容器，其内除了可以包含其他对象与组织单位之外，还有**组策略**（group policy）的功能。

如图1-1-2所示就是一个名称为**业务部**的组织单位，其内包含多个对象，其中有两个**计算机**对象、两个**用户**对象与两个本身也是组织单位的对象。AD DS以层级结构（hierarchical）将对象、容器与组织单位等组合在一起，并将它们存储到AD DS数据库内。

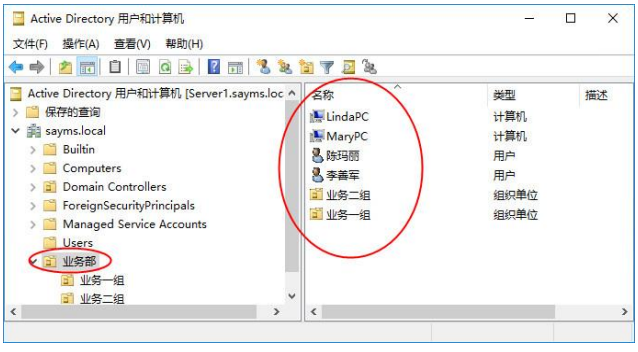

图 1-1-2

1.1.5 域树

我们可以搭建包含多个域的网络，而且网络以域树（domain tree）的形式存在，例如图1-1-3就是一棵域树，其中最上层的域名为sayms.local，它是此域树的根域（root domain）；根域之下还有两个子域（sales.sayms.local与mkt.sayms.local），之下总共还有3个子域。

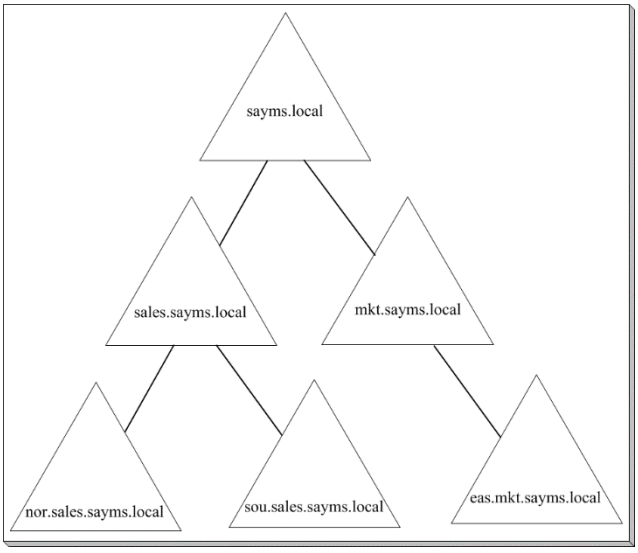

图 1-1-3

图中域树符合DNS域名空间的命名原则，而且具有连续性，也就是子域的域名中包含其父域的域名，例如域sales.sayms.local的后缀中包含其前一层（父域）的域名sayms.local，而nor.sales.sayms.local的后缀中包含其前一层的域名sales.sayms.local。

域树内的所有域共享一个 AD DS，也就是在此域树之下只有一个AD DS，不过其中的数据分散存储在各域内，每一个域内只存储隶属于该域的数据，例如该域内的用户账户（存储在域控制器内）。

1.1.6 信任

两个域之间必须拥有信任关系（trust relationship），才可以访问对方域内的资源。而任何一个新的AD DS域被加入域树后，这个域会自动信任其上一层的父域，同时父域也会自动信任此新的子域，而且这些信任关系具备双向传递性（two-way transitive）。由于此信任工作是通过Kerberos security protocol来完成的，因此也被称为Kerberos trust。

Q 域A的用户登录到其所隶属的域后，这个用户可否访问域B内的资源呢？

A 只要域B信任域A就没有问题。

我们以图1-1-4来解释双向传递性，图中域A信任域B（箭头由A指向B）、域B又信任域C，

因此域A自动信任域C；另外域C信任域B（箭头由C指向B）、域B又信任域A，因此域C自动信任域A。结果是域A和域C之间自动有着双向的信任关系。

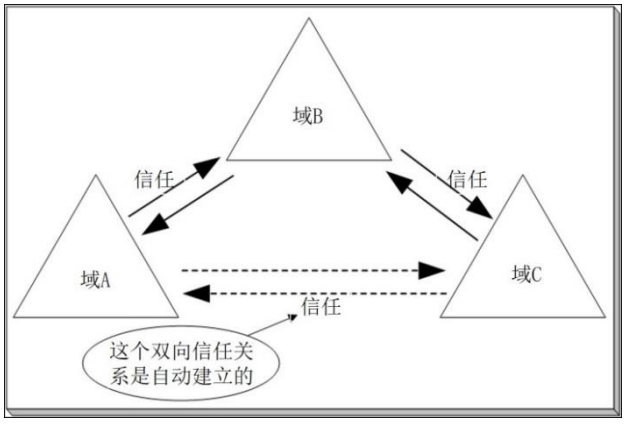

图 1-1-4

因此，当任何一个新域加入域树后，它会自动双向信任这个域树内所有的域，所以只要拥有适当权限，这个新域内的用户便可以访问其他域内的资源；同理，其他域内的用户也可以访问这个新域内的资源。

1.1.7　林

林（forest）由一棵或多棵域树组成，每一棵域树都有自己唯一的命名空间，如图1-1-5所示，其中一棵域树内的每一个域名都是以sayms.local结尾，而另一棵域树内的每一个域名则都是以say365.local结尾。

第一棵域树的根域，就是整个林的根域（forest root domain），同时其域名就是林的名称。例如图1-1-5中的sayms.local是第一棵域树的根域，它就是整个林的根域，而林名称就是sayms.local。

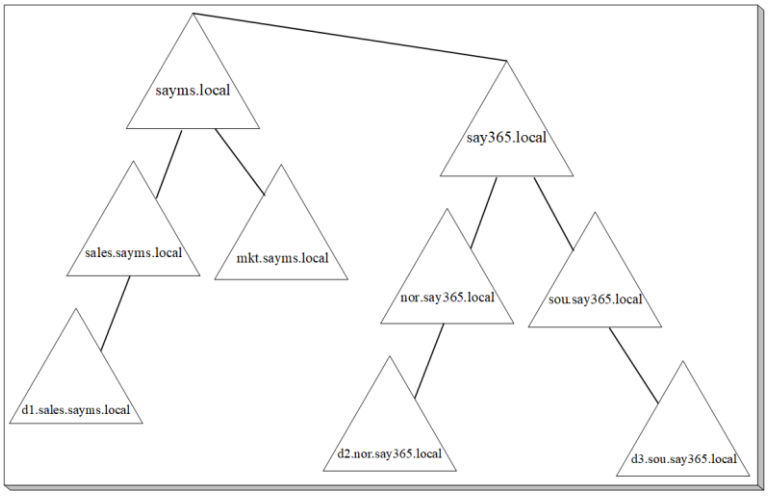

图 1-1-5

当创建林时，每一棵域树的根域与林根域之间会自动建立起双向可传递的信任关系。因此，在每一棵域树中的每一个域内，只要用户拥有相应的权限，就可以访问其他任何一棵域树内的资源，也可以登录到其他任何一棵域树内的成员计算机上。

1.1.8 架构

AD DS对象的类型与属性数据定义在**架构**（schema）内，例如它定义了**用户**对象类型内包含的属性（姓、名、电话等）、每一个属性的数据类型等信息。

隶属于Schema Admins组的用户可以修改**架构**内的数据，应用程序也可以自行在**架构**内添加所需的对象类型或属性。在一个林内的所有域树共享相同的**架构**。

1.1.9 域控制器

AD DS的目录数据存储在域控制器内。一个域内可以有多台域控制器（domain controller），每一台域控制器的地位（几乎）是平等的，它们各自存储着一份相同的AD DS数据库。当在任何一台域控制器内添加一个用户账户后，此账户默认被创建在此域控制器的AD DS数据库中，之后会自动被复制（replicate）到其他域控制器的AD DS数据库（见图1-1-6），以便让所有域控制器内的AD DS数据库都能够同步（synchronize）。

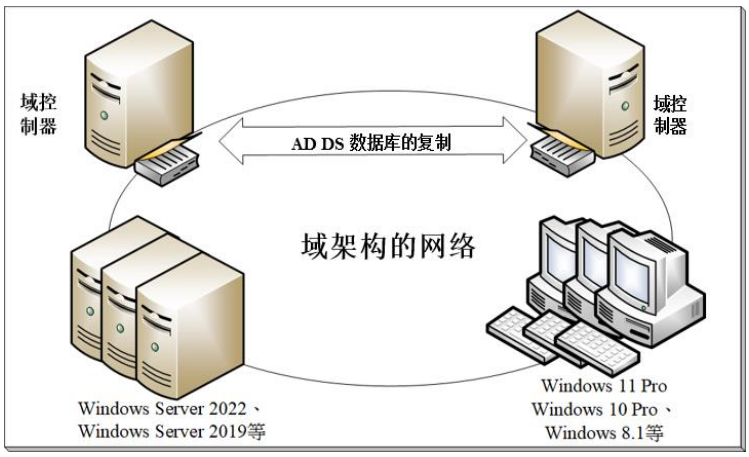

图 1-1-6

当用户在某台域成员计算机登录时，会由其中一台域控制器根据其AD DS数据库内的账户数据，来审核用户所输入的账户与密码是否正确。如果是正确的，那么用户就可以成功登录；反之，会被拒绝登录。

多台域控制器还可以改善用户的登录效率，因为多台域控制器可以分担审核用户登录身份（账户名称与密码）的负担。另外它也可以提供容错功能，即使其中一台域控制器有故障，其他域控制器仍然能够继续提供服务。

域控制器是由服务器级别的计算机来扮演的，例如Windows Server 2022、Windows Server 2019、Windows Server 2016等。

1.1.10　只读域控制器

只读域控制器（Read-Only Domain Controller，RODC）的AD DS数据库只可以被读取，不可以被修改，也就是说用户或应用程序无法直接修改RODC的AD DS数据库。RODC的AD DS数据库内容只能够从其他**可读写域控制器**复制过来。RODC主要是设计给远程分公司来使用，因为一般来说远程分公司的网络规模比较小、用户人数比较少，此网络的安全措施或许不如总公司完备，同时也可能比较缺乏IT技术人员，采用RODC可避免因其AD DS数据库被破坏而影响到整个AD DS环境的运行。

1. RODC的AD DS数据库内容

RODC的AD DS数据库内会存储AD DS域内的所有对象与属性，但是用户账户的密码除外。远程分公司内的应用程序要读取AD DS数据库内的对象时，可以通过RODC来快速获取。不过因为RODC并不存储用户的密码，所以在验证用户名与密码时，仍然需要将它们发送到总公司的可读写域控制器来验证。

由于RODC的AD DS数据库是只读的，因此当远程分公司的应用程序要更改AD DS数据库的对象（或用户要更改密码）时，这些更改要求都会被提交到总公司的可读写域控制器来处理，总公司的可读写域控制器再通过AD DS数据库的复制程序将这些更新数据复制到RODC。

2. 单向复制（unidirectional replication）

当总公司的可读写域控制器的AD DS数据库发生变化时，变化数据会被复制到RODC。然而因用户或应用程序无法直接更改RODC的AD DS数据库，故企业分支机构不会把更新数据复制到总公司的可读写域控制器，因而可以降低网络的负担。

除此之外，可读写域控制器通过DFS分布式文件系统将SYSVOL文件夹（用来存储组策略的相关设置）复制给RODC，采用的也是单向复制。

3. 认证缓存（credential caching）

RODC在验证用户的密码时，仍然需要将它们发送到总公司的可读写域控制器来验证，如果希望加快验证速度，可以选择将用户的密码存储到RODC的认证缓存区，不过需要通过**密码复制策略**（password replication policy）来选择可以被RODC缓存的账户。建议不要缓存太多账户，因为分公司的安全措施可能比较差，如果RODC被入侵，存储在缓存区内的认证信息就可能会外泄。

4. 系统管理员角色隔离（administrator role separation）

可以通过**系统管理员角色隔离**来将任何一位域用户委派为RODC的本地系统管理员，他可以登录RODC这台域控制器执行管理工作，例如更新驱动程序等，但他无法执行其他域的管理工作，也无法登录其他域控制器。此功能可以将RODC的一般管理工作委派给用户，但却不会危害到域安全。

5. 只读域名系统（read-only domain name system）

可以在RODC上搭建DNS服务器，RODC会复制DNS服务器的所有应用程序目录分区。客户端可以向这台RODC角色的DNS服务器提出DNS查询要求。

不过RODC的DNS服务器不支持客户端直接动态更新，因此客户端的更新记录请求会被该DNS服务器提交到其他DNS服务器，让客户端转向其他DNS服务器更新，而RODC的DNS服务器也会自动从这台DNS服务器复制这次更新记录。

1.1.11 可重启的AD DS

如果要进行AD DS数据库维护工作（例如数据库脱机重整），那么可以选择进入**目录服务还原模式**（directory service restore mode，或译为**目录服务修复模式**）来完成此工作。不过需要先重新启动计算机，再进入**目录服务还原模式。**如果这台域控制器同时提供其他网络服务，例如它同时也是DHCP服务器，则重新启动计算机期间将造成DHCP服务暂时中断。

Windows Server 2022系统提供了**可重启的AD DS**（Restartable AD DS）功能，也就是说如果要执行AD DS数据库维护工作，则只需将AD DS服务停止即可，不需要通过重新启动计算机来进入**目录服务还原模式**，如此不但可以让AD DS数据库的维护工作变得更容易、更快速，而且其他服务也不会被中断。完成维护工作后再重新启动AD DS服务即可。

在AD DS服务停止的情况下，只要还有其他域控制器在线，则仍然可以在这台AD DS服务已经停止的域控制器上利用域用户账户来登录。如果没有其他域控制器在线，则在这台AD DS服务已停止的域控制器上，默认只能够使用**目录服务还原模式**的系统管理员账户来进入**目录服务还原模式**。

1.1.12 Active Directory回收站

系统管理员如果不小心删除了AD DS对象，则将造成不少困扰，例如如果误删组织单位，则其内所有对象都会不见，此时虽然系统管理员可以进入**目录服务还原模式**来恢复被误删的对象，但比较耗费时间，而且在进入**目录服务还原模式**这段时间内，域控制器会暂时停止对客户端提供服务。**Active Directory回收站**让系统管理员不需要进入**目录服务还原模式**就可以快速恢复被删除的对象。

1.1.13 AD DS的复制模式

域控制器之间在复制AD DS数据库时，分为以下两种复制模式：

- **多主机复制模式**（multi-master replication model）：AD DS数据库内的大部分数据是使用此模式进行复制。在此模式下，可以直接更新任何一台域控制器内的AD DS对象，之后这个更新过的对象会被自动复制到其他域控制器。例如当在任何一台域控制器的AD DS数据库内添加一个用户账户后，此账户会被自动复制到域内的其他域控制器。

- **单主机复制模式**（single-master replication model）：AD DS数据库内少量数据是使用**单主机复制模式**进行复制。在此模式下，当提出**更改**对象数据的**请求**时，会由其中一台域控制器（被称为**操作主机**）负责接收与处理此要求，也就是说该对象首先在**操作主机**上进行更新，再由**操作主机**将它复制给其他域控制器。例如，当添加或删除一个域时，此更改信息会先被写入扮演**域命名操作主机**角色的域控制器内，再由它复制给其他域控制器（见第10章）。

1.1.14　域中的其他成员计算机

如果想要完全管理网络内的计算机，可以将它们加入域。用户在域成员计算机上才能利用AD DS数据库内的域用户账户来登录，在未加入域的计算机上只能够利用本地用户账户登录。域中的成员计算机包括：

- 成员服务器（member server），例如：
  - Windows Server 2022 Datacenter/Standard
  - Windows Server 2019 Datacenter/Standard
  - Windows Server 2016 Datacenter/Standard
  - ……

上述服务器级别的计算机加入域后被称为**成员服务器**，但其内并没有AD DS数据库，它们也不负责审核AD DS域用户名称与密码，而是提交给域控制器来审核。未加入域的服务器被称为**独立服务器**（或**工作组服务器**）。但不论是独立服务器还是成员服务器，都有**本地安全账户数据库**（SAM），系统可以利用它来审核本地用户（非AD DS域用户）的身份。

- 其他常用的Windows计算机，例如：
  - Windows 11 Enterprise/Pro/Education
  - Windows 10 Enterprise/Pro/Education
  - Windows 8.1Enterprise/Pro
  - Windows 8 Enterprise/Pro
  - ……

当上述客户端计算机加入域以后，用户就可以在这些计算机上利用AD DS内的用户账户来登录，否则只能够利用本地用户账户来登录。

可以将Windows Server 2022、Windows Server 2019等独立服务器或成员服务器升级为域控制器，也可以将域控制器降级为独立服务器或成员服务器。

较低的版本，例如Windows 11 Home、Windows 10 Home等计算机无法加入域，因此只能够利用本地用户账户来登录。

1.1.15 DNS服务器

域控制器需将自己注册到DNS服务器内，以便让其他计算机通过DNS服务器来找到自己，因此域环境需要具备可支持AD DS的DNS服务器。此服务器最好支持**动态更新**（dynamic update）功能，以便当域控制器的角色有变化或域成员计算机的IP地址等数据有变化时，可以自动更新DNS服务器内的记录。

1.1.16 轻量级目录访问协议

轻量级目录访问协议（Lightweight Directory Access Protocol，LDAP）是一种用来查询与更新AD DS数据库的目录服务通信协议。AD DS是利用**LDAP命名路径**（LDAP naming path）来表示对象在AD DS数据库内的位置，以便用它来访问AD DS数据库内的对象。**LDAP命名路径**包含：

- **标识名称**（Distinguished Name，DN）：它是对象在AD DS内的完整路径，例如在图1-1-7中，用户账户名称为**林小洋**，其DN为：

  CN=林小洋,OU=业务一组,OU=业务部,DC=sayms,DC=local

  其中DC（domain component，域名组件）为DNS域名中的组件，例如sayms.local中的sayms与local；OU为组织单位；CN（common name）为通用名称，一般为用户名或计算机名。除了DC与OU之外，其他都是利用CN来表示，例如用户与计算机对象都属于CN。上述DN表示法中的**sayms.local**为域名，**业务部**、**业务一组**都是组织单位。此DN表示账户**林小洋**是存储在**sayms.local\业务部\业务一组**路径内。

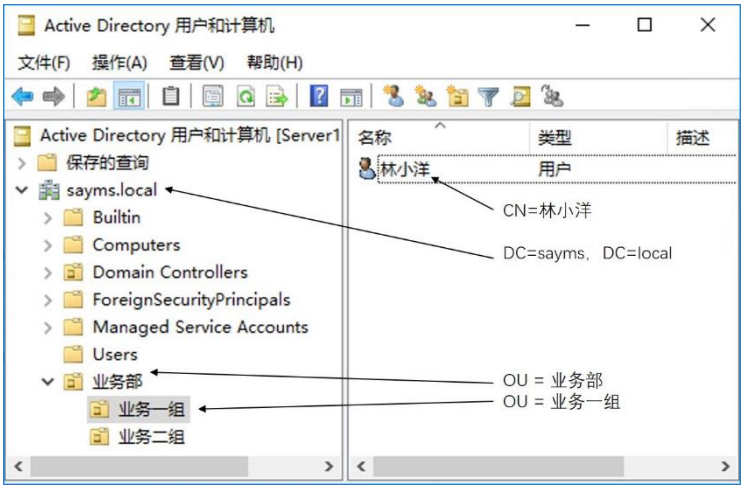

图 1-1-7

- 相对标识名称（Relative Distinguished Name，RDN）：RDN用来代表DN完整路径中的部分路径，例如前述路径中，CN=林小洋与OU=业务一组等都是RDN。

除了DN与RDN这两个对象名称外，还有以下名称：

- **全局唯一标识**（Global Unique Identifier，GUID）：系统会自动为每一个对象指定一个唯一的、128位数值的GUID。虽然可以更改对象名称，但其GUID永远不会改变。
- **用户主体名称**（User Principal Name，UPN）：每一个用户还可以有一个比DN更短、更容易记忆的UPN，例如图1-1-7中的林小洋隶属域sayms.local，则其UPN可为bob@sayms.local。用户登录时所输入的账户名称最好使用UPN，因为无论此用户的账户被移动到哪一个域，其UPN都不会改变，所以用户可以一直使用同一个名称来登录。
- **服务器主体名称**（Service Principal Name，SPN）：SPN是一个内含多重设置值的名称，它根据DNS主机名来创建。SPN用来代表某台计算机所支持的服务，它让其他计算机可以通过SPN来与这台计算机的服务通信。

1.1.17　全局编录

虽然在域树内的所有域共享一个AD DS数据库，但其数据分散在各个域内，而每一个域只存储该域本身的数据。为了让用户、应用程序能够快速找到位于其他域内的资源，在AD DS内便设计了**全局编录**（global catalog）。一个林内的所有域树共享相同的**全局编录**。

全局编录的数据存储在域控制器内，这台域控制器可被称为**全局编录服务器**。虽然它存储着林内所有域的AD DS数据库内的所有对象，但是它只存储对象的部分属性，这些属性都是平常会被用来搜寻的属性，例如用户的电话号码、登录账户名称等。**全局编录**让用户即使不知道对象位于哪一个域内，也仍然可以快速地找到所需对象。

用户登录时，**全局编录服务器**还负责提供该用户所隶属的**通用组**（后述）信息；用户利用UPN登录时，**全局编录服务器**也负责提供用户隶属于哪一个域的信息。

1.1.18　站点

站点（site）由一个或多个IP子网组成，这些子网之间通过**高速且可靠的链路**连接起来，也就是这些子网之间的连接速度要快且稳定，符合需求，否则就应该将它们分别规划为不同的站点。

一般来说，一个LAN（局域网）之内的各个子网之间的链路都符合速度快且高可靠度的要求，因此可以将一个LAN规划为一个站点；而WAN（广域网）内的各个LAN之间的连接速度一般都比较慢，因此WAN之中的各个LAN应分别规划为不同的站点，如图1-1-8所示。

域是逻辑的（logical）分组，而站点是物理的（physical）分组。在AD DS内每一个站点可能内含多个域；而一个域内的计算机们也可能分别散布在不同的站点内。

如果一个域的域控制器分布在不同站点内，而站点之间是低速链路，则由于不同站点的域控制器之间会互相复制AD DS数据库，因此为了避免复制时占用站点之间链路的带宽，影响站点之间其他数据的传输效率，需谨慎规划执行复制的时段，也就是尽量在离峰时期才执行复制工作，同时复制频率不要太高。

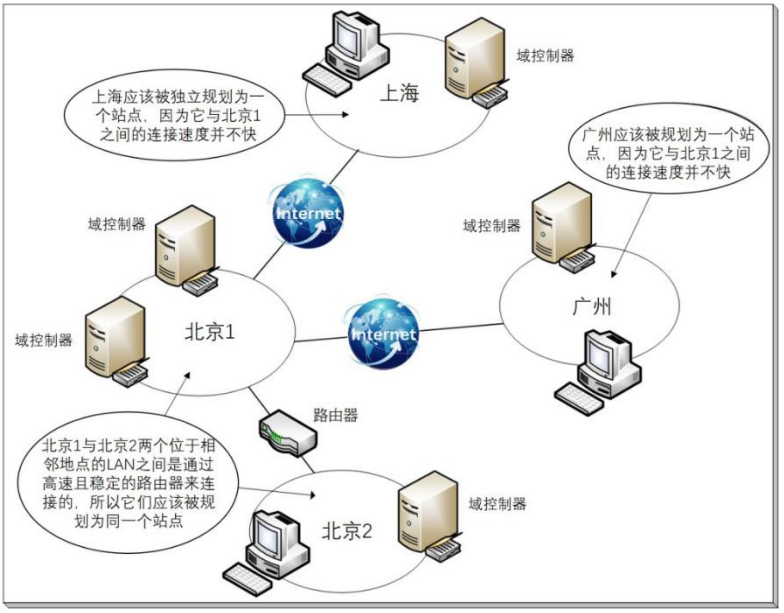

图 1-1-8

同一个站点内的域控制器之间通过快速链路连接在一起，因此在复制AD DS数据时，可以快速复制。AD DS会设置让同一个站点内、隶属于同一个域的域控制器之间自动执行复制工作，且默认的复制频率也比不同站点之间的复制频率高。

不同站点之间在复制时所传送的数据会被压缩，以减少站点之间链路带宽的负担；但是同一个站点内的域控制器之间在复制时并不会压缩数据。

1.1.19 目录分区

AD DS数据库被逻辑地分为以下多个目录分区（directory partition）：

- **架构目录分区（schema directory partition）**：它存储着整个林中所有对象与属性的定义数据，也存储着创建新对象与属性的规则。整个林内所有域共享一份相同的**架构目录分区**，它会被复制到林中所有域的所有域控制器中。
- **配置目录分区（configuration directory partition）**：其内存储着整个AD DS的结构，例如有哪些域、有哪些站点、有哪些域控制器等资料。整个林共享一份相同的**配置目录分区**，它会被复制到林中所有域的所有域控制器中。
- **域目录分区（domain directory partition）**：每一个域各有一个**域目录分区**，其内存储着与该域有关的对象，例如用户、组与计算机等对象。每一个域各自拥有一份**域目录分区**，它只会被复制到该域内的所有域控制器中，并不会被复制到其他域的域控制器中。
- **应用程序目录分区（application directory partition）**：一般来说，它是由应用程序创建的，其内存储着与该应用程序有关的数据。例如由Windows Server 2022扮演的DNS服务器，如果所创建的DNS区域为**Active Directory集成区域**，则它便会在AD

DS数据库内创建**应用程序目录分区**，以便存储该区域的数据。**应用程序目录分区**会被复制到林中的特定域控制器中，而不是所有的域控制器。

1.2　域功能级别与林功能级别

AD DS将域与林划分为不同的功能级别，每个级别各有不同的特色与限制。

1.2.1　域功能级别

Active Directory域服务的**域功能级别**（domain functionality level）设置只会影响到该域本身，不会影响到其他域。**域功能级别**分为以下几种模式：

- **Windows Server 2008**：域控制器需Windows Server 2008或新版。
- **Windows Server 2008 R2**：域控制器需Windows Server 2008 R2或新版。
- **Windows Server 2012**：域控制器需Windows Server 2012或新版。
- **Windows Server 2012 R2**：域控制器需Windows Server 2012 R2或新版。
- **Windows Server 2016**：域控制器需Windows Server 2016或新版。

其中的Windows Server 2016级别拥有AD DS的所有功能。可以提升域功能级别，例如将Windows Server 2012 R2提升到Windows Server 2016。

Windows Server 2022、Windows Server 2019并未添加新的域功能级别与林功能级别，目前最高级别仍然是**Windows Server 2016**。

1.2.2　林功能级别

Active Directory域服务的**林功能级别**（forest functionality level）设置，会影响到该林内的所有域。**林功能级别**分为以下几种模式：

- **Windows Server 2008**：域控制器需Windows Server 2008或新版。
- **Windows Server 2008 R2**：域控制器需Windows Server 2008 R2或新版。
- **Windows Server 2012**：域控制器需Windows Server 2012或新版。
- **Windows Server 2012 R2**：域控制器需Windows Server 2012 R2或新版。
- **Windows Server 2016**：域控制器需Windows Server 2016或新版。

其中的Windows Server 2016级别拥有AD DS的所有功能。可以提升林功能级别，例如将Windows Server 2012 R2提升到Windows Server 2016。

表1-2-1中列出每一个林功能级别所支持的域功能级别。

表1-2-1 林功能级别所支持的域功能级别

林功能级别	支持的域功能级别
Windows Server 2008	Windows Server 2008、Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016
Windows Server 2008 R2	Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016
Windows Server 2012	Windows Server 2012、Windows Server 2012 R2、Windows Server 2016
Windows Server 2012 R2	Windows Server 2012 R2、Windows Server 2016
Windows Server 2016	Windows Server 2016

1.3 Active Directory轻型目录服务

我们从前面的介绍已经知道AD DS数据库是一个符合LDAP规范的目录服务数据库，它除了可以用来存储AD DS域内的对象（例如用户账户、计算机账户等）之外，也提供**应用程序目录分区**，以便让支持目录访问的应用程序（directory-enabled application）可以将该程序的相关数据存储到AD DS数据库内。

然而前面所介绍的环境，必须创建AD DS域与域控制器才能够使用AD DS目录服务与数据库。为了让没有域的环境也能够拥有跟AD DS一样的目录服务，因此便提供了一个称为**Active Directory轻型目录服务**（Active Directory Lightweight Directory Services，**AD LDS**）的服务。

AD LDS支持在计算机内创建多个目录服务的环境，每一个环境被称为一个**AD LDS实例**（instance），每一个**AD LDS实例**分别拥有独立的目录设置与架构（schema），也分别拥有专属的目录数据库，以供支持目录访问的应用程序来使用。

在Windows Server 2022内安装AD LDS角色的方法如下：【单击左下角的**开始**图标⊞➲**服务器管理器**➲单击**仪表板**处的**添加角色及功能**➲一直单击“**下一步**”按钮➲如图1-3-1所示选择 **Active Directory轻型目录服务**➲……】。之后就可以通过以下方法来创建**AD LDS实例**：【单击左下角的**开始**图标⊞➲**Windows管理工具**➲**Active Directory轻型目录服务安装向导**】。也可以通过【单击左下角的**开始**图标⊞➲**Windows管理工具**➲**ADSI编辑器**】来管理**AD LDS实例**内的目录设置、架构、对象等。

图 1-3-1

2

第 2 章　创建 AD DS 域

创建AD DS域环境后，就可以通过AD DS的强大功能更加容易、高效地管理网络。

- 2.1 创建AD DS域前的准备工作
- 2.2 创建AD DS域
- 2.3 确认AD DS域是否正常
- 2.4 提升域与林功能级别
- 2.5 新建额外域控制器与RODC
- 2.6 RODC阶段式安装
- 2.7 将Windows计算机加入或脱离域
- 2.8 在域成员计算机内安装AD DS管理工具
- 2.9 删除域控制器与域

2.1 创建AD DS域前的准备工作

要创建AD DS域，可以先安装一台服务器，然后将它升级（promote）为域控制器。在创建AD DS域前，需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域名采用的是DNS的架构与命名方法，因此先为AD DS域取一个符合DNS格式的域名，例如sayms.local（本书皆以虚拟的**最高层域名**.local为例来说明）。

2.1.2 准备好一台支持AD DS的DNS服务器

在AD DS域中，域控制器会将它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服务器来找到自己，因此需要一台DNS服务器，且它需支持SRV记录（Service Location Resource Record，服务位置资源记录），最好也支持**动态更新**与**增量区域传输**（Incremental Zone Transfer，IXFR）等功能：

- **SRV记录**：域控制器需将它所扮演的角色注册到DNS服务器的SRV记录内，因此DNS服务器需支持SRV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**：如果未支持此功能，则域控制器将无法自动将自己注册到DNS服务器的SRV记录内，此时需由管理员手动将数据输入DNS服务器，如此会增加管理负担。Windows Server与BIND的DNS服务器都支持此功能。
- **增量区域传输**：它让DNS服务器与其他DNS服务器在执行**区域转送**（zone transfer）时，只会复制最新变化记录，而不会复制区域内的所有记录。它可以提升复制效率，减少网络负担。Windows Server 与BIND的 DNS服务器都支持此功能。

可以采用以下两种方法之一来搭建DNS服务器：

- 在将服务器升级为域控制器时，顺便让系统自动在这台服务器上安装 DNS服务器。它还会自动创建一个支持AD DS域的DNS区域，例如AD DS域名为sayms.local，则它自动创建的区域名称为sayms.local，并会自动启用动态更新。
  需先在这台即将成为域控制器与DNS服务器的计算机上清除其**首选DNS服务器**的IP地址，或改为输入自己的IP地址（见图2-1-1），无论选择哪一种设置方法，升级时系统都可以自动安装DNS服务器角色。

- 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服务器内创建用来支持AD DS域的区域。例如AD DS域名为sayms.local，则自行创建一个名称为sayms.local的DNS区域，然后启用动态更新功能。如图2-1-2所示为选择**非安全**动态更新，如果它是**Active Directory集成区域**，则还可以选择**只有安全的**动态更新。别忘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。

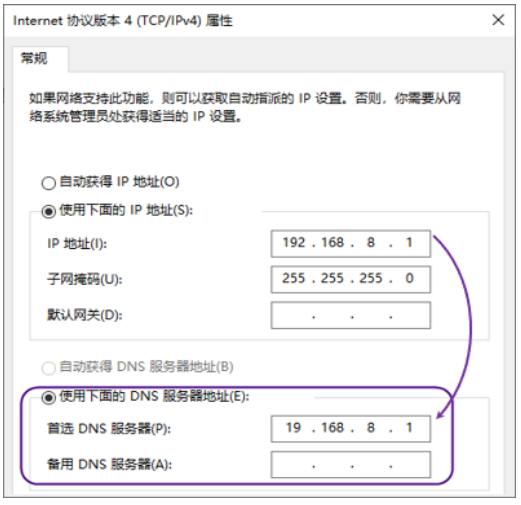

图 2-1-1

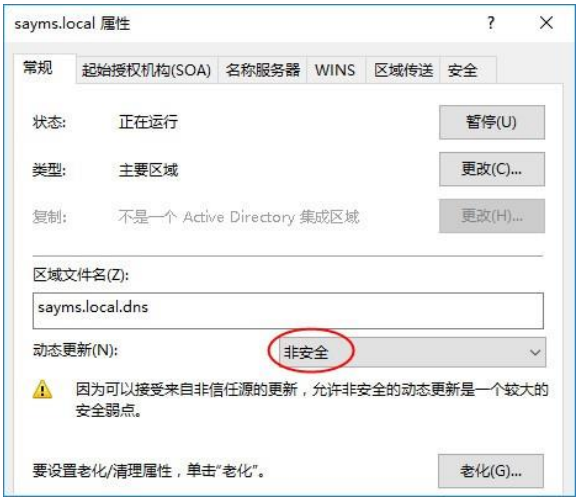

图 2-1-2

可通过【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【打开**服务器管理器**➲单击右上角的**工具菜单**➲**DNS**➲选中**正向查找区域**并右击➲**新建区域**】的方法来创建区域。

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数据库的变化信息。
- **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，其中的SYSVOL文件夹需位于NTFS磁盘内。建议将AD DS数据库与日志文件分别存储到不同硬盘内，一方面是因为两块硬盘独立运行，可以提升工作效率；另一方面是因为分开存储，可以避免两份数据同时出问题，以提升AD DS数据库的恢复能力。

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，而系统默认将它们都存储到Windows Server 2022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，但计算机内目前并没有其他NTFS磁盘，那么可以采用以下方法来创建NTFS磁盘：

- **如果磁盘内还有未划分的可用空间**：此时可以通过【打开**服务器管理器**➲单击右上角的**工具**菜单➲**计算机管理**➲**存储**➲**磁盘管理**➲右击未配置的可用空间】的方法来创建一个新的NTFS磁盘。
- **利用CONVERT命令来转换现有磁盘**：例如要将D:磁盘（FAT或FAT32）转换成NTFS磁盘，可执行CONVERT D: /FS:NTFS命令。

2.2 创建AD DS域

下面使用图2-2-1来说明如何创建第1个林中的第1个域（根域）：我们先安装一台Windows Server 2022服务器，然后将它升级为域控制器并创建域。我们也将搭建此域的第2台域控制器（Windows Server 2022）、第3台域控制器（Windows Server 2022）、一台成员服务器（Windows Server 2022）与一台加入域的Windows 11计算机。

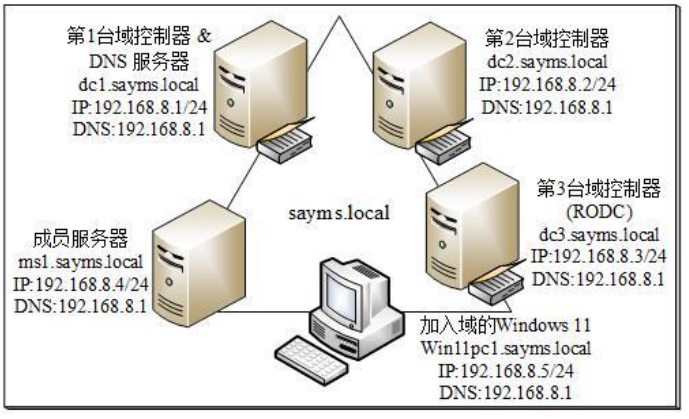

图 2-2-1

建议利用Hyper-V、VMware Workstation或VirtualBox等提供虚拟环境的软件来创建图中的网络环境。如果图中的虚拟机是从现有的虚拟机复制来的，那么记得需先执行C:\windows\System32\Sysprep内的Sysprep.exe文件，并勾选**通用**。

如果要升级现有域，则林中的域控制器都必须是Windows Server 2008（含）以上的版本，且需先分别执行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 2022光盘或系统镜像文件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，因为它是第一台域控制器，因此这个升级动作会同时完成以下工作：

- 创建第一个新林。
- 创建此新林中的第一棵域树。
- 创建此新域树中的第一个域。
- 创建此新域中的第一台域控制器。

换句话说，在创建图2-2-1中第一台域控制器dc1.sayms.local时，它就会同时创建此域控制器所隶属的域sayms.local，创建域sayms.local所隶属的域树，而域sayms.local也是此域树的根域。由于是第一棵域树，因此它同时会创建新林，林名称就是第一棵域树的根域的域名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法来将图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　先在图2-2-1中左上角的服务器dc1.sayms.local上安装Windows Server 2022，并将其计算机名称设置为DC1，而IPv4地址等配置信息依照图中所示进行设置（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**，然后单击 添加功能 按钮。

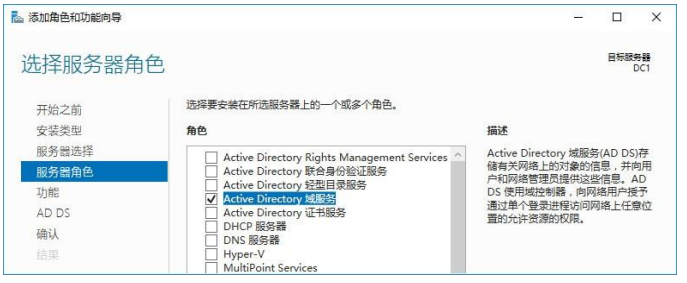

图 2-2-2

STEP 4　持续单击 下一步 按钮，一直到**确认安装选项**界面，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

如果已经关闭如图2-2-3所示的界面，则单击**服务器管理器**上方的旗帜符号（见图2-2-4），在弹出的对话框中单击**将此服务器提升为域控制器**。

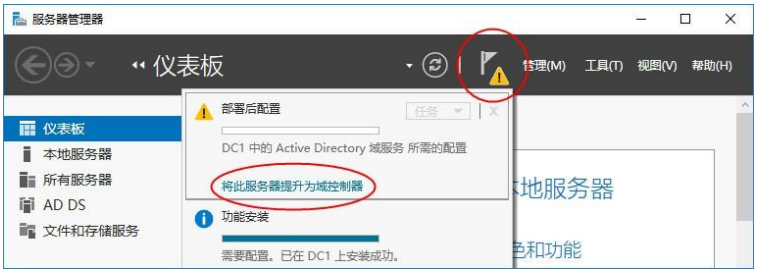

图2-2-4

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），然后单击下一步按钮（因为篇幅原因未截取整个页面，故图2-2-5中看不到这个按钮，该按钮其实在这个页面的下方，后文采用类似的方式来说明）。

图 2-2-5

STEP 7 完成图2-2-6中的设置后单击下一步按钮：

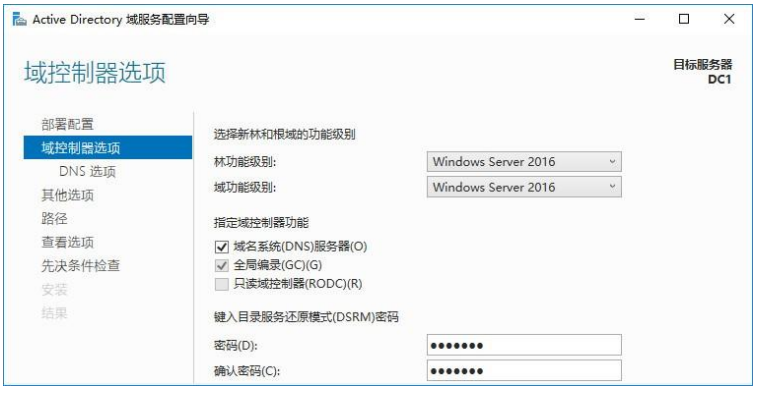

图 2-2-6

- 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默认的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，就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**的管理员密码：**目录服务还原模式**（目录服务修复模式）是安全模式，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输入此处所设置的密码（详见第11章）。

密码默认需至少7个字符，且不可包含用户账户名称（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 出现如图2-2-7所示的警示界面时，因为目前不会产生影响，故不必理会它，直接单击下一步按钮。

图 2-2-7

STEP 9 在**其他选项**界面中，安装程序会自动为此域设置一个NetBIOS域名。如果此名称已被占用，则会自动指定建议名称。完成后单击下一步按钮。（默认为DNS域名第1个句点左侧的文字，例如DNS名称为sayms.local，则NetBIOS名称为SAYMS，它让不支持DNS名称的旧系统可以通过NetBIOS名称来与此域通信。NetBIOS名称不区分字母大小写）。

STEP 10 在图2-2-8所示的界面中可直接单击下一步按钮。

图 2-2-8

- **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数据库的变化记录，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）。

STEP 11 在**查看选项**界面中，确认选项无误后单击下一步按钮。

STEP 12 在图2-2-9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。

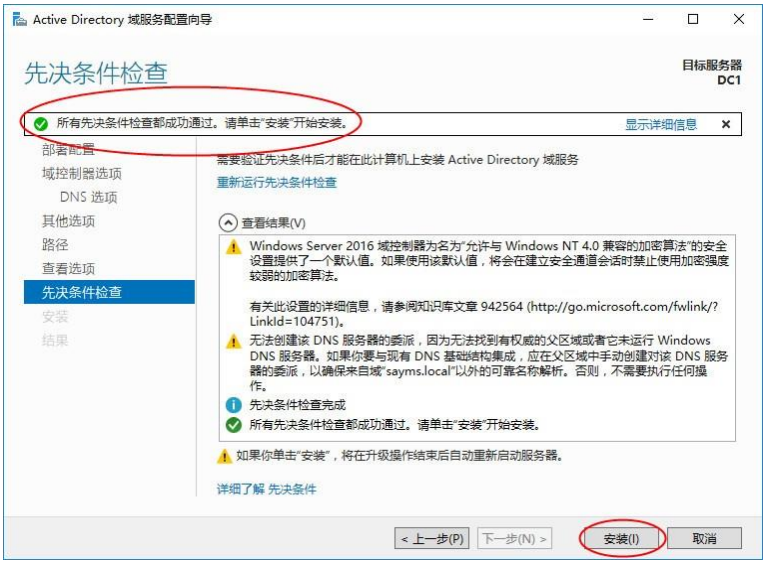

图 2-2-9

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转移到AD DS数据库。另外，由于它本身也是DNS服务器，因此会如图2-2-10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。

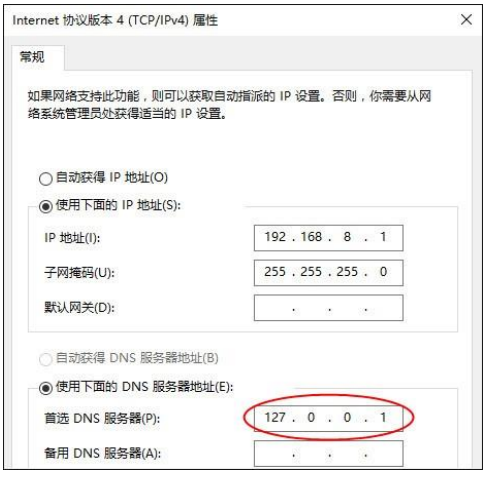

图 2-2-10

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

2.3　确认AD DS域是否正常

AD DS域创建完成后，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地创建完成。

2.3.1　检查DNS服务器内的记录是否完整

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，以便让其他计算机通过DNS服务器来找到自己。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：【到兼具DNS服务器角色的dc1.sayms.local上打开**服务器管理器**➲单击右上角的**工具**菜单➲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已成功将其主机名与IP地址注册到DNS服务器内。

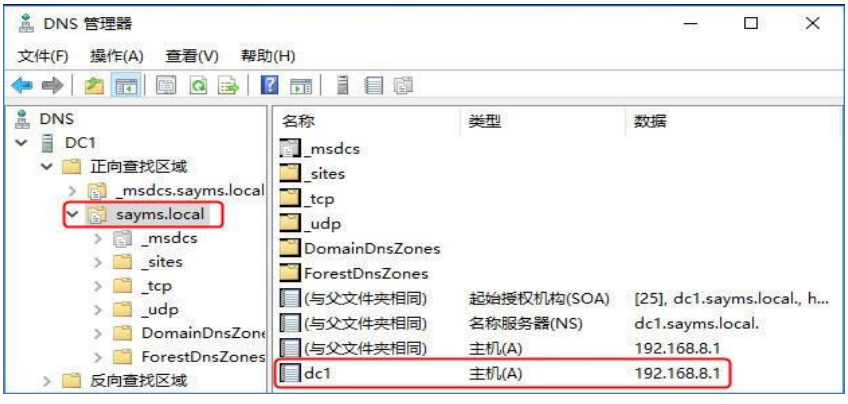

图 2-3-1

2. 利用DNS控制台检查SRV记录

如果域控制器已经成功将其所扮演的角色注册到DNS服务器，则还会有如图2-3-2所示的_tcp、_udp 等文件夹。图中_tcp文件夹中的数据类型为**服务位置（SRV）**的_ldap记录，表示dc1.sayms.local已经成功注册为域控制器。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扮演的。

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

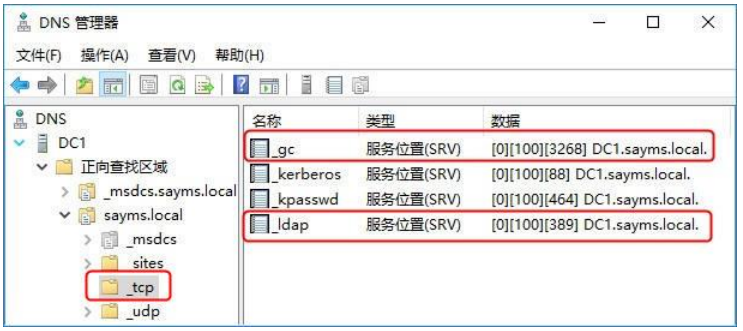

图 2-3-2

DNS区域内有了这些数据（或信息）后，其他欲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。域内的其他成员计算机（成员服务器、Windows 11等客户端计算机）默认也会将其主机名称与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_msdcs文件夹。如果DNS服务器是在安装AD DS时同时安装的，则还会创建一个名为_msdcs.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数据注册到_msdcs.sayms.local内，而不是_msdcs内。如图2-3-3所示为_msdcs.sayms.local区域内的部分记录。

图 2-3-3

在完成第一个域的创建之后，系统就会自动创建一个名为Default-First-Site-Name的站点，而我们所创建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，在此站点内扮演**全局编录服务器**（gc）、**Kerberos服务器**、**LDAP服务器**这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

也可以利用**nslookup**命令来检查DNS服务器内的SRV记录。

STEP 1　单击左下角的**开始**图标⊞➲Windows PowerShell。

STEP 2　执行nslookup命令。

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，从图中可以看出域控制器dc1.sayms.local已经成功地将其扮演的LDAP服务器角色的信息注册到DNS服务器内。

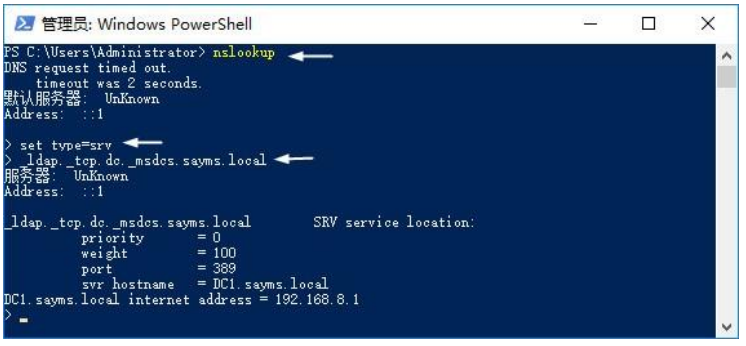

图 2-3-5

界面中之所以会出现“DNS request timed out.”与“默认服务器：UnKnown”消息（可以不必理会这些消息），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，则可以将网络连接处的TCP/IPv6禁用或修改TCP/IPv6设置为“自动取得DNS服务器地址”，或在DNS服务器创建适当的IPv4/IPv6反向对应区域与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。还可以利用**ls -t SRV sayms.local**命令来查看所有的SRV记录，不过需先在DNS服务器上将sayms.local区域的**允许区域转送**权限开放给查询计算机，否则在此计算机上查询会失败，且会显示**Query refused**的警告消息。执行**exit**命令可以结束**nslookup**。

DNS服务器的**区域转送**设置方法：【选中sayms.local区域并右击➲**属性**➲**区域转送**】。

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，则可在解决问题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，那么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，那么到此域控制器上通过【打开**服务器管理器**➲单击右上角的**工具**菜单➲**服务**➲如图2-3-6所示选中**Netlogon**服务并右击➲重新启动】的方法来注册。

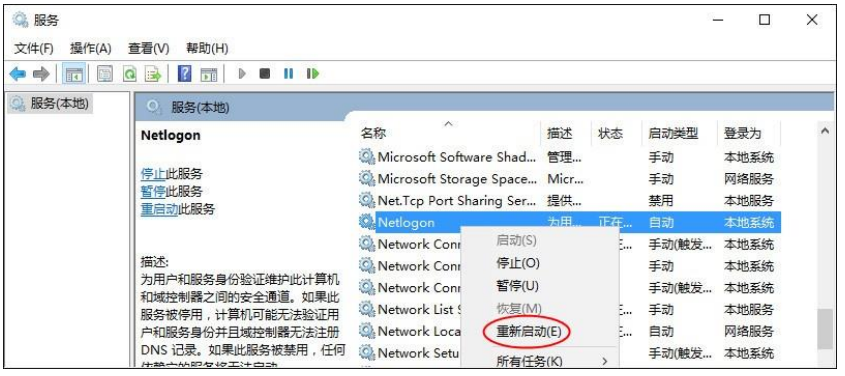

图 2-3-6

域控制器默认会自动每隔24小时向DNS服务器注册1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在%***systemroot***%**ntds**文件夹内，因此可以通过【按⊞+R组合键➲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完成，如图2-3-7中的ntds.dit就是AD DS数据库文件，而edb、edb00001等文件是日志文件（其扩展名为.log，默认会被隐藏）。

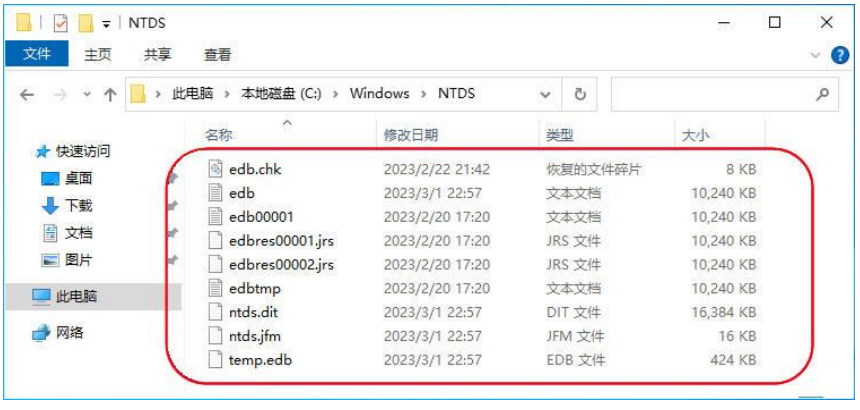

图 2-3-7

另外SYSVOL默认被创建在%***systemroot***%**SYSVOL**文件夹内，因此可以通过【按⊞+ R组合键➲输入%***systemroot***%**SYSVOL**➲单击确定按钮】的方法来检查，如图2-3-8所示。

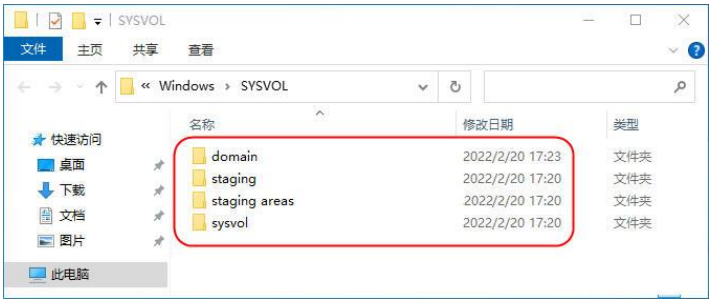

图 2-3-8

图中SYSVOL文件夹之下会有4个子文件夹，其中的sysvol与其内的scripts都应该被设为共享文件夹。可以通过【打开**服务器管理器**➲单击右上角的**工具**菜单➲**计算机管理➲系统工具➲共享文件夹➲共享**（见图2-3-9）】的方法或如图2-3-10所示利用**net share**命令，来检查它们是否已被设置为共享文件夹。

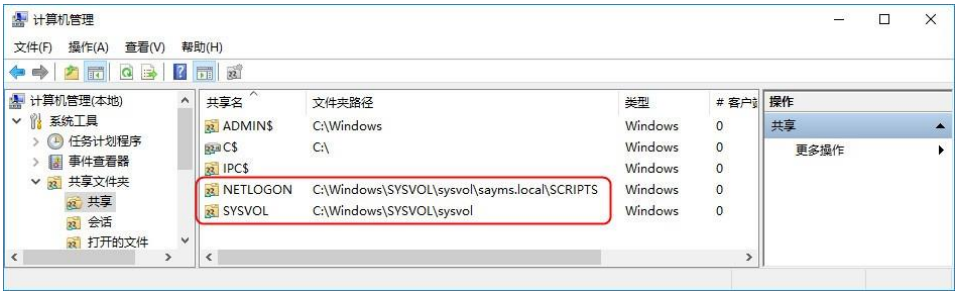

图 2-3-9

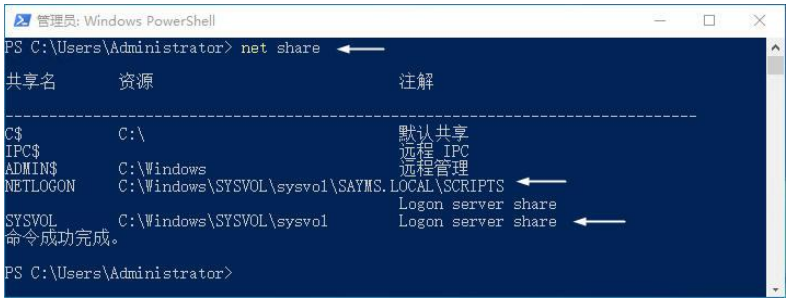

图 2-3-10

2.3.4　新增加的管理工具

AD DS安装完成后，通过【打开**服务器管理器**➲单击右上角的**工具**菜单】就可以看到增加的一些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；或是通过【单击左下角的**开始**图标⊞➲**Windows管理工具**】来查看，如图2-3-11所示。

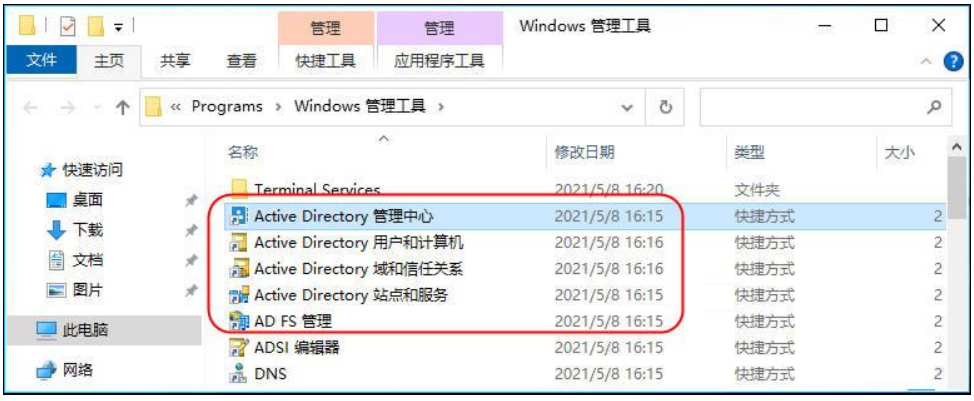

图 2-3-11

2.3.5 查看事件日志文件

可以通过【打开**服务器管理器**➲单击右上角的**工具**菜单➲**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节已经讲解过域与林功能级别，此处将介绍如何提升现有的级别：【打开**服务器管理器**➲单击右上角的**工具**菜单】，然后【执行**Active Directory管理中心**➲单击域名**sayms（本地）**➲单击图2-4-1右侧的**提升林功能级别...**或**提升域功能级别...**】。Windows Server 2022并未增加新的域功能级别与林功能级别，最高级别仍然是Windows Server 2016。

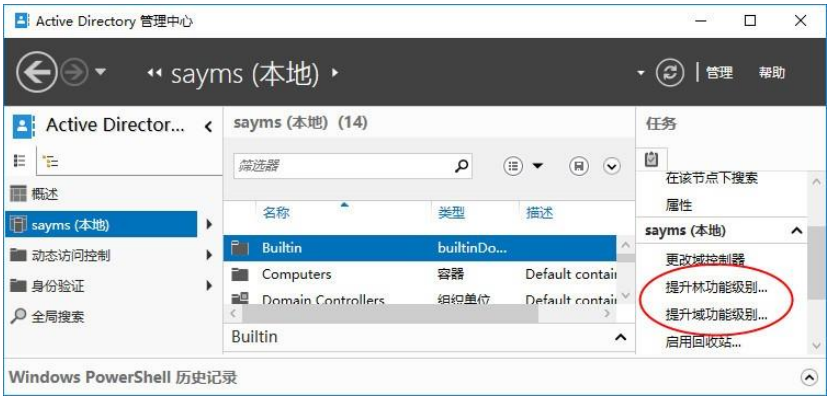

图 2-4-1

也可以通过【单击左下角的**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【单击左下角的**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**】的方法来提升现有的级别。

提升域功能级别可参考表2-4-1。提升林功能级别可参考表2-4-2。升级后，这些升级信息会被自动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。

表2-4-1 提升域功能级别

目前的域功能级别	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 提升林功能级别

目前的林功能级别	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

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，便可以拥有以下优势：

- **改善用户登录的效率**：多台域控制器来同时对客户端提供服务，可以分担审核用户登录身份（账户与密码）的负担，让用户登录的效率更高。
- **容错功能**：当域控制器发生故障时，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。系统提供了两种复制方法：

- **通过网络直接复制**：如果AD DS数据库十分庞大，那么此方法会增加网络负担，影响网络效率，尤其是当这台新域控制器位于远程网络时。
- **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），其内包含着AD DS数据库，接着将**安装媒体**复制到U盘、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介质内读取**安装媒体**内的AD DS数据库，这种方法可降低对网络所造成的影响。

如果在**安装媒体**制作完成之后，现有域控制器的AD DS数据库内有最新的变化数据，那么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中右上角的dc2.sayms.local升级为一般的（可读写域控制器）**额外域控制器**，将右下角的dc3.sayms.local升级为**只读域控制器**（RODC）。

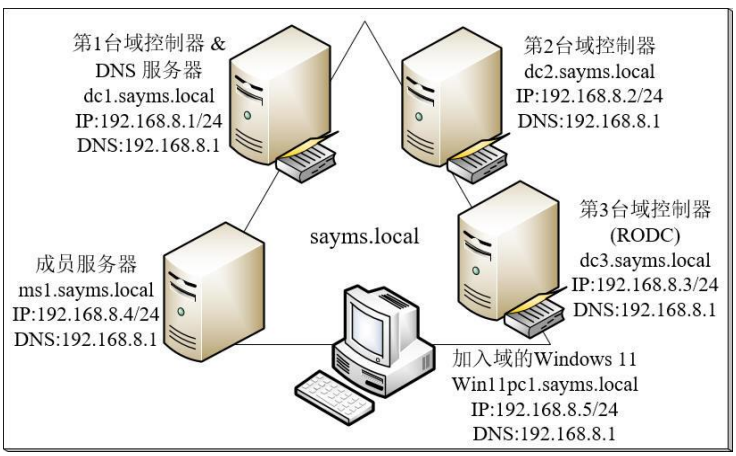

图 2-5-1

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 2022，将计算机名称分别设置为DC2与DC3，IPv4地址等配置信息依照图中所示进行设置（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，它们会分别被自动改为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一直到**选择服务器角色**界面，勾选**Active Directory域服务**，然后单击添加功能按钮。

STEP 4　持续单击下一步按钮一直到**确认安装所选择内容**界面，单击安装按钮。

STEP 5　图2-5-2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 2-5-2

STEP 6　在图2-5-3所示的界面中选择**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。

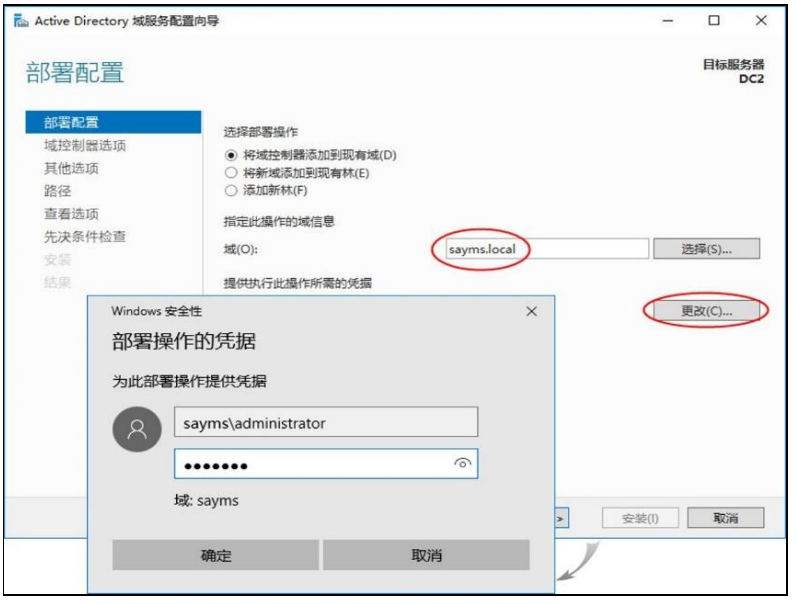

图 2-5-3

只有Enterprise Admins或Domain Admins内的用户有权限创建其他域控制器。如果现在所登录的账户不是隶属于这两个群组（例如我们现在所登录的账户为本地Administrator），则需如图2-5-3所示指定有权限的用户账户。

STEP 7 完成图2-5-4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，则勾选此选项。
- 设置**目录服务还原模式**的管理员密码（需符合复杂性需求）。

图2-5-4

STEP 8 如果在图2-5-4所示的界面中未勾选**只读域控制器（RODC）**，则直接跳到STEP 9。如果是安装RODC，则会出现如图2-5-5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：

图2-5-5

- **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群组，他们在这台RODC上将拥有本地管理员权限，且如果采用阶段式安装RODC（后述），则他们也有权限将此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群组内的用户有权限管理此RODC与执行附加工作。
- **允许将密码复制到RODC的账户**：默认仅允许群组Allowed RODC Password Replication Group内的用户的密码可被复制到RODC（此群组默认并无任何成员）。可通过单击添加按钮来添加用户或群组。

- **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。部分内建的组账户（例如Administrators、Server Operators等）默认已被列于此清单内。可通过单击添加按钮来添加用户或群组。

在安装域中的第1台RODC时，系统会自动创建与RODC有关的组账户，这些账户会被自动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群组信息，则会显示警告消息，此时应等这些群组信息完成复制后，再继续安装这台RODC。

STEP 9　如果不是安装RODC，会出现如图2-5-6所示的界面，直接单击下一步按钮。

图 2-5-6

STEP 10　在图2-5-7所示的界面中单击下一步按钮，它会直接从其他任何一台域控制器复制AD DS数据库。

图 2-5-7

STEP 11　出现**路径**界面时直接单击下一步按钮（此界面的说明可参考图2-2-8）。

STEP 12　在**查看选项**界面中，确认选项无误后单击下一步按钮。

STEP 13　出现**先决条件检查**界面时，如果顺利通过检查，就直接单击安装按钮，否则根据界面提示先排除问题。

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（参考前面第2.3.1节**检查DNS服务器内的记录是否完整**）。

这两台域控制器的AD DS数据库属性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**，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，要求安装向导从**安装媒体**来读取AD DS数据库，这种方法可以降低对网络所造成的影响。

1. 制作“安装媒体”

到现有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**使用，则需到现有的一台**可读写域控制器**上执行**ntdsutil**命令。
- 如果此安装媒体是要给**RODC**（只读域控制器）使用，则可以到现有的一台**可读写域控制器**或**RODC**上执行**ntdsutil**命令。

STEP 1 到域控制器上利用域管理员的身份进行登录。

STEP 2 单击左下角的**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2-5-8）：

```
ntdsutil
```

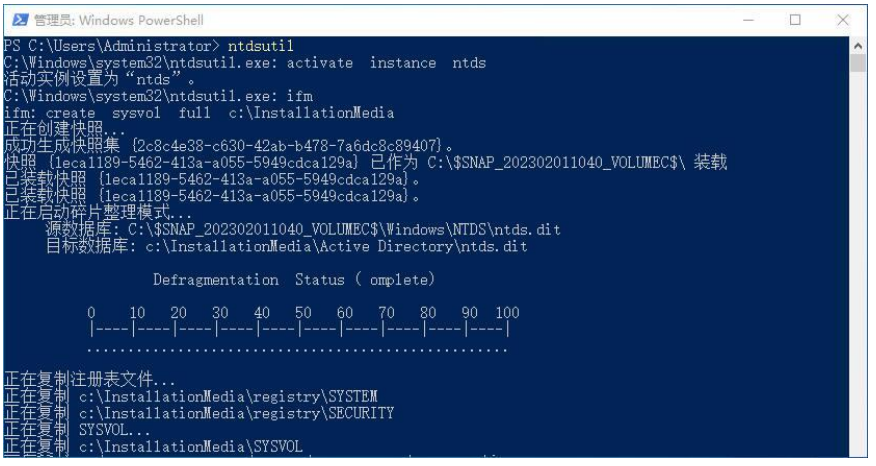

图 2-5-8

STEP 4 在**ntdsutil**：提示字符下，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**：提示字符下，执行以下命令：

```
ifm
```

STEP 6　在**ifm**：提示字符下，执行以下命令：

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

此命令假设是将**安装媒体**的内容存储到C:\InstallationMedia文件夹内。

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，则将**full**改为**rodc**。

STEP 7　连续执行两次**quit**命令来结束**ntdsutil**。图2-5-8为部分操作界面。

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

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，或是将它们放到可以访问的共享文件夹内。

由于利用**安装媒体**来安装额外域控制器的方法与上一节大致上相同，因此以下仅列出不同之处。以下假设**安装媒体**是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2-5-9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 2-5-9

安装过程中会从**安装媒体**所在的文件夹C:\InstallationMedia来读取、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数据库内有新的变化数据，那么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RODC系统管理工作的委派设置或密码复制策略，那么打开**Active Directory管理中心**后，如图2-5-10所示【选择组织单位**Domain Controllers**界面中间扮演RODC角色的域控制器➲单击右侧的**属性**➲通过选择图2-5-11中的**管理者**小节与**扩展**小节中的**密码复制策略**选项卡来设置】。

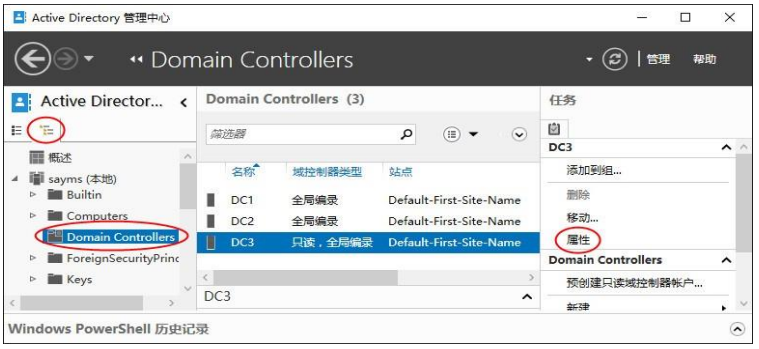

图 2-5-10

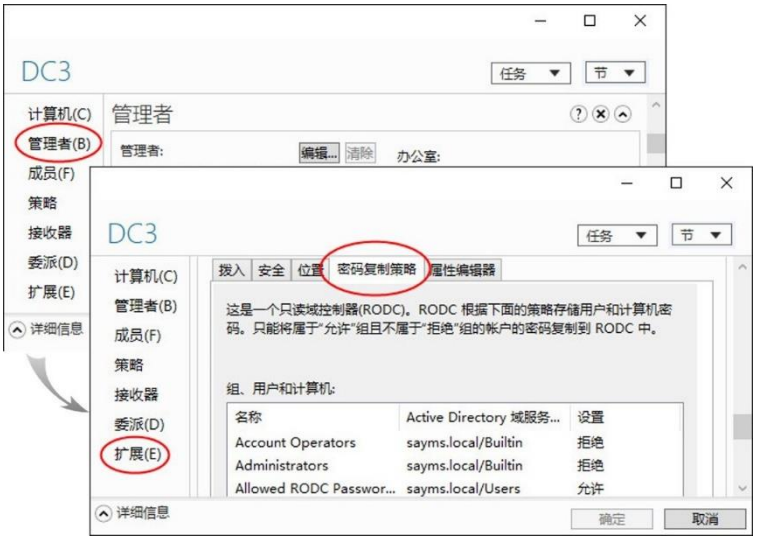

图 2-5-11

也可以执行**Active Directory用户和计算机**，然后【单击组织单位**Domain Controllers**➲选中右侧扮演RODC角色的域控制器并右击➲**属性**➲通过**密码复制策略**与**管理者**选项卡来设置】。

2.6 RODC阶段式安装

可以采用两阶段式来安装RODC（只读域控制器），这两个阶段分别由不同的用户来完成，这种安装方法通常用来安装远程分公司所需的RODC。

- 第1阶段：创建RODC账户。
  此阶段通常是在总公司内执行，且只有域管理员（Domain Admins群组的成员）才有权限来执行这一阶段的工作。在此阶段内，管理员需在AD DS数据库内替RODC创建计算机账户、设置选项，并将第2阶段的安装工作委派给指定的用户或群组。

- 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，被委派者有权限在此阶段来完成安装RODC的工作。被委派者并不需要具备域管理员权限。默认只有Domain Admins或Enterprise Admins群组内的用户有权限执行这个阶段的安装工作。在此阶段内，被委派者需要在远程分公司内，将即将成为RODC的服务器**附加**（attach）到第1个阶段中所创建的计算机账户，如此便可完成RODC的安装工作。

2.6.1 创建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，本节以它被安装到同一个站点内为例来进行说明，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法将图2-6-1中右下角的dc4.sayms.local升级为**只读域控制器**（RODC）。

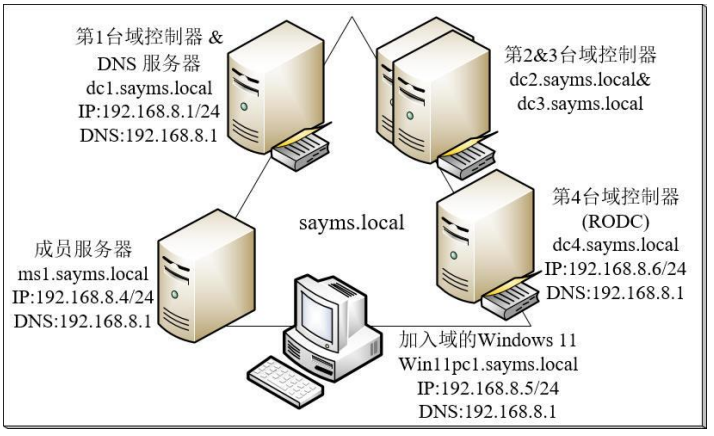

图2-6-1

STEP 1　到现有的一台域控制器上利用域管理员身份登录。

STEP 2　打开**服务器管理器**➲单击右上角的**工具**菜单➲**Active Directory管理中心**➲如图2-6-2所示单击组织单位Domain Controllers右侧的**预创建只读域控制器账户**（也可以使用**Active Directory用户和计算机**）。

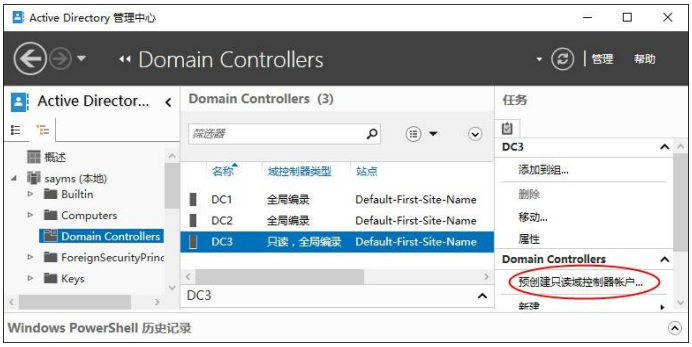

图2-6-2

STEP 3 如图2-6-3所示勾选**使用高级模式安装**后单击下一步按钮。

STEP 4 当前登录的用户为域Administrator，他有权限安装域控制器，因此在图2-6-4中选择默认的**我的当前登录凭证**后单击下一步按钮。

图 2-6-3

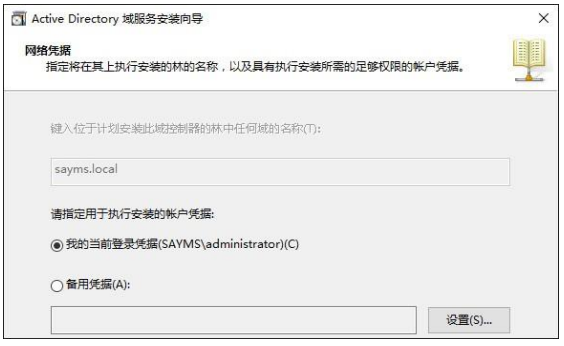

图 2-6-4

如果当前登录的用户没有权限安装域控制器，则选择图中的**备用凭证**，然后通过单击设置按钮来输入有权限的用户名称与密码。

STEP 5 在图2-6-5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。

STEP 6 出现**选择一个站点**界面时，选择新域控制器所在的AD DS站点，默认是当前仅有的站点Default-First-Site-Name。直接单击下一步按钮。

STEP 7 在图2-6-6所示的界面中直接单击下一步按钮。由图可知它会在此服务器上安装DNS服务器，同时会将此服务器设置为**全局编录**，并自动勾选**只读域控制器（RODC）**。

图 2-6-5

图 2-6-6

STEP 8 通过图2-6-7所示的界面来设置**密码复制策略**：图中默认仅允许群组Allowed RODC Password Replication Group内的用户的密码可以被复制到RODC（此群组内默认并无任何成员），且一些重要账户（例如Administrators、Server Operators等群组内的用

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。完成后单击下一步按钮。

图 2-6-7

STEP 9　在图2-6-8所示的界面中将安装RODC的工作委派给指定的用户或群组，图中将它委派给域（SAYMS）用户george。RODC安装完成后，该用户在此台RODC内会自动被赋予本地管理员的权限。单击下一步按钮。

图 2-6-8

STEP 10　接下来依次单击下一步按钮，直到单击完成按钮，图2-6-9为完成后的界面。

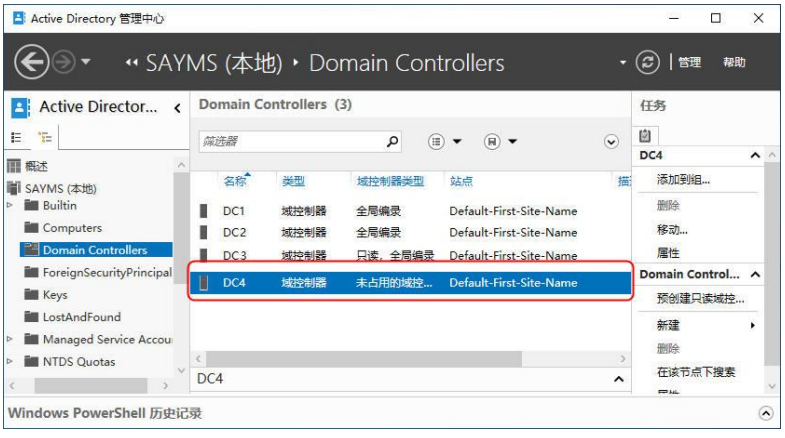

图 2-6-9

2.6.2 将服务器附加到RODC账户

STEP 1 在图2-6-1右侧的服务器dc4.sayms.local上安装Windows Server 2022，并将其计算机名称设置为DC4，IPv4地址等配置信息依照图中所示进行设置（此处采用TCP/IPv4）。注意，将其计算机名称设置为DC4即可，等升级为域控制器后，它会自动被改为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一直到**选择服务器角色**界面，勾选**Active Directory域服务**，然后单击添加功能按钮。

STEP 4 持续单击下一步按钮一直到**确认安装选项**界面，单击安装按钮。

STEP 5 图2-6-10为完成安装后的界面，单击**将此服务器提升为域控制器**。

图 2-6-10

STEP 6 在图2-6-11所示的界面中选择**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，然后单击确定按钮、下一步按钮。

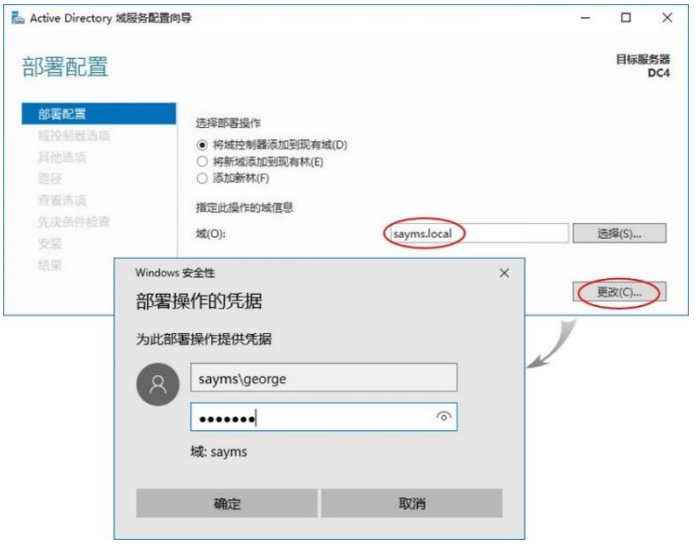

图 2-6-11

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

STEP 7　接下来会出现如图2-6-12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**的管理员密码后（需符合复杂性需求）单击下一步按钮。

图 2-6-12

STEP 8　在接下来的**其他选项**、**路径**与**查看选项**界面中都可直接单击下一步按钮。

STEP 9　出现**先决条件检查**界面时，如果顺利通过检查，就直接单击安装按钮，否则根据界面提示先排除问题。

STEP 10　安装完成后会自动重新启动。请重新登录。

STEP 11　图2-6-13为完成后的界面。

图 2-6-13

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数据库与其他的域资源，例如用户可以在

这些计算机上利用域用户账户来登录域、访问域中其他计算机内的资源。下面列出部分可以被加入域的计算机（以安装的操作系统为准入标准）：

- Windows Server 2022 Datacenter/Standard
- Windows Server 2019 Datacenter/Standard
- Windows Server 2016 Datacenter/Standard
- Windows 11 Enterprise/Pro/Education
- Windows 10 Enterprise/Pro/Education
- Windows 8.1 Enterprise/Pro
- Windows 8 Enterprise/Pro
- ……

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 2022 Datacenter；同时也要将下方的Windows 11计算机加入域，假设它是Windows 11 Professional。下面利用服务器ms1（Windows Server 2022）来说明。

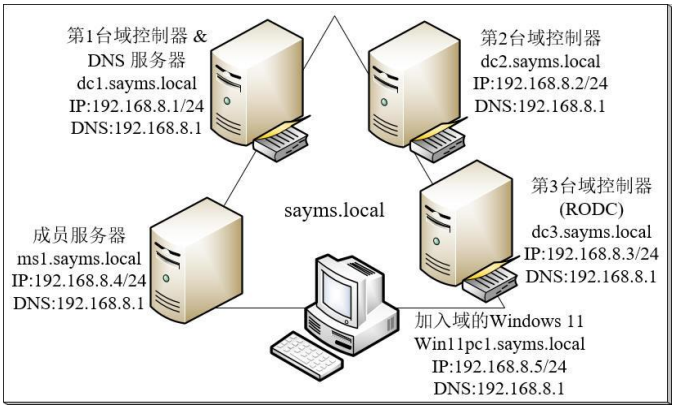

图 2-7-1

加入域后的计算机（非域控制器），其计算机账户默认会自动被创建在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，则可以事先在该容器或组织单位内创建此计算机账户：如果是使用**Active Directory管理中心**，【单击该容器或组织单位➲单击右侧**任务**窗格的**新建➲计算机**】；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**】。完成后，再将计算机加入域。也可以事后将计算机账户搬移到其他容器或组织单位。

STEP 1 先将该台计算机的计算机名称设置为ms1，IPv4地址等配置信息依照图2-7-1中所示进行设置。注意计算机名称设置为ms1即可，等加入域后，其计算机名称会自动被改为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**工作组**处的WORKGROUP。

图 2-7-2

如果是Windows 11计算机：【右击左下角的**开始**图标➲系统➲单击**域或工作组**➲单击更改按钮】。

如果是Windows 10计算机：【右击左下角的**开始**图标➲**系统**➲单击**重新命名此计算机（高级）**➲单击更改按钮】。

如果是Windows 8.1计算机：【按Windows键切换到**开始**菜单➲单击菜单左下方图标➲右击**这台电脑**➲单击**属性**➲单击右侧的**更改设置**】。

如果是Windows 8计算机：【按Windows键切换到**开始**菜单➲在空白处右击➲单击**所有应用程序**➲选中**计算机**并右击➲单击下方的**属性**➲……】。

STEP 3　在图2-7-3所示的界面中单击更改按钮。

STEP 4　在图2-7-4所示的界面中选择**域**➲输入域名sayms.local➲单击确定按钮➲输入域内任何一位用户账户（隶属于Domain Users群组）与密码，图中是administrator➲单击确定按钮。

图 2-7-3

图 2-7-4

如果出现错误警告，则检查TCP/IPv4的设置是否有误，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**欢迎加入sayms.local域**界面表示已经成功加入域，也就是此计算机的计算机账户已经被创建在AD DS数据库内（默认会被创建在Computers容器内）。单击确定按钮。

如果出现错误警告，则检查所输入的账户与密码是否正确。不需要域管理员账户也可以，不过如果是非域管理员，则只可以在AD DS数据库内最多加入10台计算机（创建最多10个计算机账户）。

STEP 6 出现提醒需要重新启动计算机的界面时单击确定按钮。

STEP 7 从图2-7-5中可以看出，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。

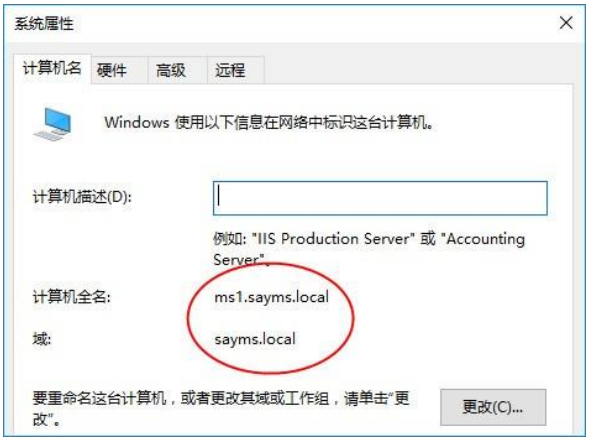

图 2-7-5

STEP 8 依照界面指示重新启动计算机。

STEP 9 请自行将图2-7-1中的Windows 11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，利用本地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，如果要利用本地用户账户登录，请先在账户前输入计算机名称，如图2-7-6所示的ms1\administrator，其中ms1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。

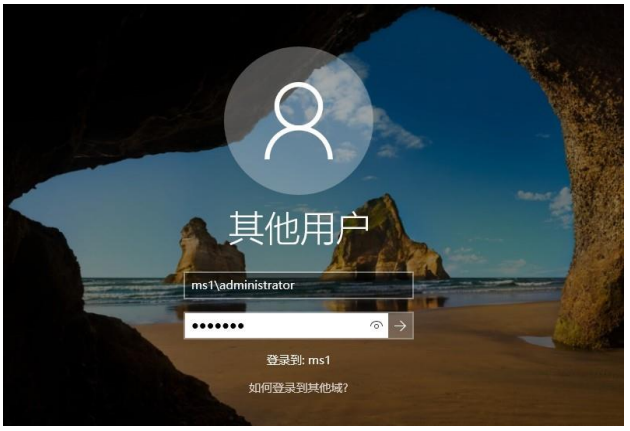

图 2-7-6

此时系统会利用本地安全性数据库来检查用户账户与密码是否正确，如果正确，就可以成功登录，也可访问此计算机内的资源（如果有权限），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。

2. 利用域用户账户登录

如果要改用域用户账户来登录，请先在账户前输入域名，如图2-7-7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（域名也可以是DNS域名，例如sayms.local\Administrator）。

图 2-7-7

用户账户名称与密码会发送给域控制器，并利用AD DS数据库来检查是否正确，如果正确，就可以登录成功，且可以直接连接域内任何一台计算机与访问其内的资源（如果有被赋予权限），不需要再另外手动输入用户名称与密码。

2.7.3 脱机加入域

客户端计算机具备脱机加入域的功能（offline domain join），也就是它们在未与域控制器连接的情况下，仍然可以加入域。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的必要信息。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win11pc2。为了实际演练脱机加入域功能，先确认win11pc2处于脱机状态。脱机将win11pc2加入域的步骤如下：

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djoin.exe程序（见图2-7-8），它会创建一个文本文件，此文件内包含脱机计算机win11pc2所需的所有信息：

```
Djoin /provision /domain sayms.local /machine win11pc2 /savefile
c:\win11pc2.txt
```

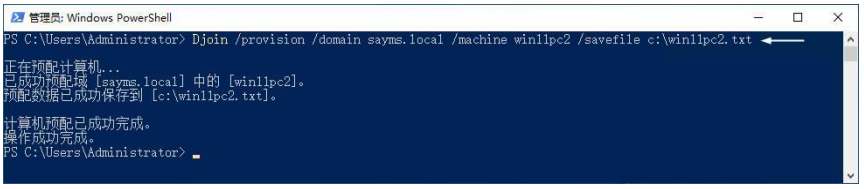

图 2-7-8

其中sayms.local为域名，win11pc2为脱机计算机的计算机名称，win11pc2.txt为所创建的文本文件（图中的文件win11pc2.txt会被创建在C:\）。此命令默认会将计算机账户win11pc2创建到**Computers**容器内（见图2-7-9）。

图 2-7-9

STEP 2 到即将加入域的脱机计算机win11pc2上利用djoin.exe来导入上述文件内的信息。在Windows 11计算机上需以管理员身份来执行此程序，因此【选中桌面下方的**开始**图标并右击➲Windows 终端（管理员）】，然后执行以下命令（参见图2-7-10，图中假设我们已经将文件win11pc2.txt复制到计算机win11pc2的C:\）：

```
Djoin --% /requestODJ /loadfile C:\win11pc2.txt /windowspath %SystemRoot%
/localos
```

STEP 3 当win11pc2连上网络且可以与域控制器通信时，重新启动win11pc2，它便完成了加入域的操作。

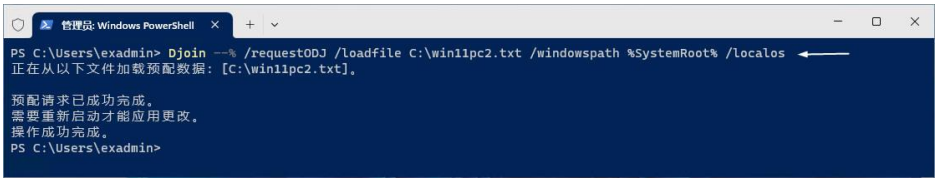

图 2-7-10

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的成员或本地管理员才有权限将此计算机脱离域。

脱离域的方法为（以Windows Server 2022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➲选中图2-7-11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2-7-12所示的提示界面，一旦脱离域后，在这台计算机上只能够利用本地用户账户来登录，无法再使用域用户账户，因此在确认记得本地管理员的密码后再单击确定按钮，否则单击取消按钮。

图 2-7-11

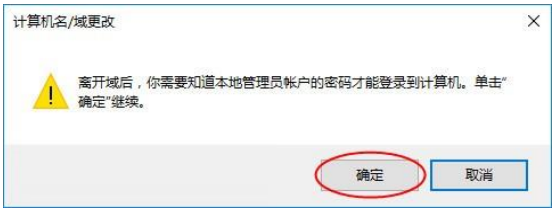

图 2-7-12

这些计算机脱离域后，其原本在AD DS的Computers容器内的计算机账户会被禁用（计算机账户图标上会多一个向下的箭头）。

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 2022、Windows Server 2019、Windows Server 2016等成员

服务器与Windows 11、Windows 10、Windows 8.1等客户端计算机内默认没有管理AD DS的工具，例如**Active Directory用户和计算机**、**Active Directory管理中心**等，但可以另外安装。

1. Windows Server 2022、Windows Server 2019等成员服务器

Windows Server 2022、Windows Server 2019、Windows Server 2016成员服务器可以通过**添加角色和功能**的方法来拥有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一直到出现如图2-8-1所示的**选择功能**界面时，勾选**远程服务器管理工具**之下的**AD DS及AD LDS工具**】，安装完成后可以通过【单击左下角的**开始**图标⊞➲Windows 管理工具】来使用这些工具。

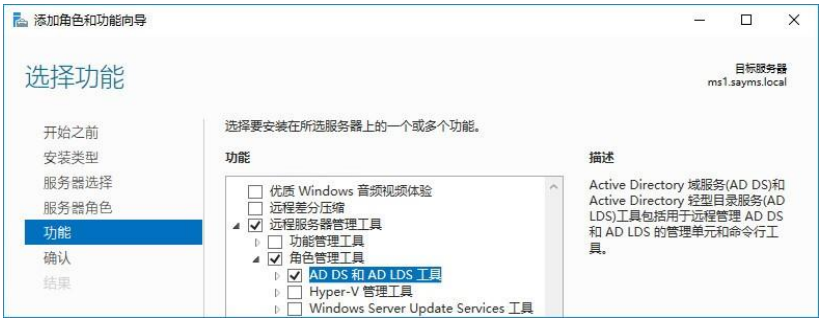

图 2-8-1

2. Windows 11

通过【单击左下角的**开始**图标➲单击**设置**➲单击**应用**处的**可选功能**➲单击**添加选用功能**处的**查看功能**➲如图2-8-2所示勾选所需的工具】（这台计算机需要连网），完成安装后，可以通过【单击下方的**开始**图标➲单击右上方的**所有应用程序**➲Windows工具】来使用这些工具。

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**Windows 10的远程服务器管理工具**，安装完成后可通过【单击左下角的**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（Windows 8）计算机需要到微软网站下载与安装**Windows 8.1 的远程服务器管理工具**（**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➲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。

2.9 删除域控制器与域

可以通过降级的方法来删除域控制器，也就是将AD DS从域控制器中删除。在降级前要注意以下事项：

- 如果域内还存在其他域控制器，则它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，故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群组的成员才有权限删除域控制器。

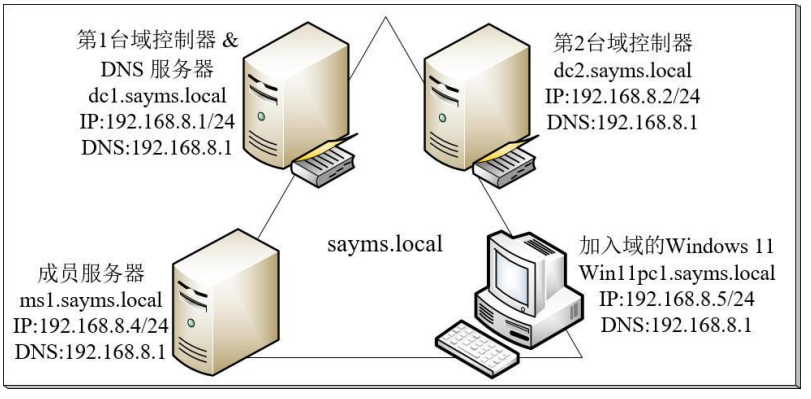

图 2-9-1

- 如果这台域控制器是此域内的最后一台域控制器，则它会被降级为独立服务器，且域也会被删除。例如假设图2-9-1中已被dc2.sayms.local降级，此时如果再降级dc1.sayms.local，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。

建议先将此域的其他成员计算机（例如win11pc1.sayms.local、ms1.sayms.local等）脱离域后，再删除域。

Enterprise Admins群组的成员才有权限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，请先删除子域。

- 如果此域控制器是**全局编录服务**器，则检查其所属站点内是否还有其他**全局编录服务**器，如果没有，就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【打开**服务器管理器**➲单击**工具菜单**➲**Active Directory站点和服务**➲**Sites**➲**Default-First-Site-Name**➲**Servers**➲选择服务器➲右击**NTDS Settings**➲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，则林会一并被删除。Enterprise Admins群组的成员才有权限删除这台域控制器与林。

删除域控制器的步骤如下：

STEP 1 打开**服务器管理器**➲选择图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一直到出现如图2-9-3所示的界面时，取消勾选**Active Directory域服务**，然后单击删除功能按钮。

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 如果当前的用户有权限删除此域控制器，则在图2-9-5所示的界面中单击下一步按钮，否则单击更改按钮来输入有权限的账户与密码。

图 2-9-5

如果因故无法删除此域控制器（例如在删除域控制器时，需能够连接到其他域控制器，但却无法连接），此时可勾选图中**强制删除此域控制器**。

如果是最后一台域控制器，则勾选图2-9-6中**域中的最后一个域控制器**。

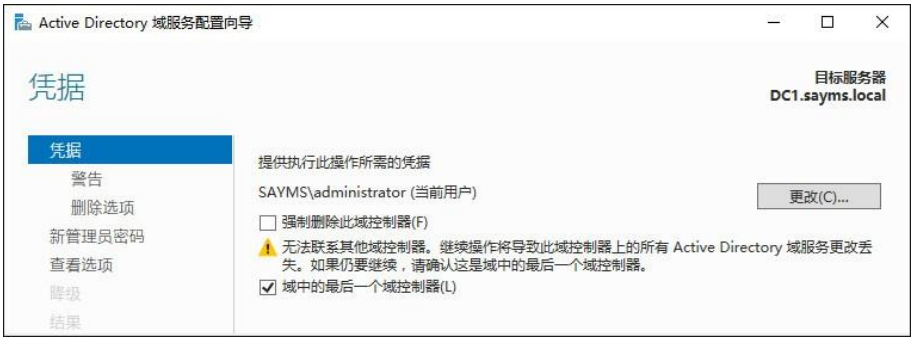

图 2-9-6

STEP 5 在图2-9-7所示的界面中勾选**继续删除**后单击下一步按钮。

图 2-9-7

STEP 6 如果出现类似图2-9-8所示的界面，则可以选择是否要删除DNS区域与删除应用程序分区，然后单击下一步按钮。

STEP 7 在图2-9-9所示的界面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，然后单击下一步按钮。

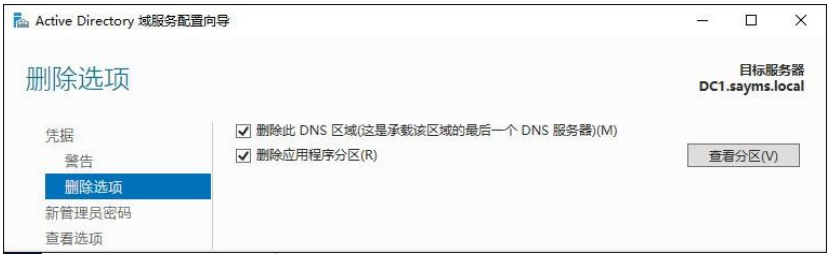

图 2-9-8

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，请重新登录。

虽然这台服务器已经不再是域控制器了，但其**Active Directory域服务**组件仍然存在，并没有被删除，因此如果现在要再将它升级为域控制器，可以参考前面的说明。

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

STEP 11 出现**开始之前**界面时单击下一步按钮。

STEP 12 确认在**服务器选择**界面中的服务器无误后，单击下一步按钮。

STEP 13 在图2-9-10所示的界面中取消勾选**Active Directory域服务**，单击删除功能按钮。

图 2-9-10

STEP 14 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），然后单击下一步按钮。

STEP 15 出现**删除功能**界面时，单击下一步按钮。

STEP 16 在**确认删除选项**界面中单击删除按钮。

STEP 17 完成后，重新启动计算机。