1

第 1 章　Active Directory 域服务（AD DS）

在Windows Server 2016的网络环境中，Active Directory域服务（Active Directory Domain Services，AD DS）提供了用来组织、管理与控制网络资源的各种强大功能。

- Active Directory域服务概述
- 域功能级别与林功能级别
- 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和电话等数据，它就是**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，它就是**file directory**（文件目录）。

如果这些directory内的数据能够系统地加以整理的话，用户就能够很容易与快速地找到所需要的数据，而directory service（目录服务）所提供的服务，就是要让用户很容易与快速地在directory内查找所需要的数据。在现实生活中，查号台也是一种目录服务；在Internet上，Google网站所提供的搜索功能也是一种目录服务。

Active Directory域内的directorydatabase（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**（Active Directory Domain Services，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（Scope）

AD DS的适用范围非常广泛，它可以用在一台计算机、一个小型局域网（LAN）或多个广域网（WAN）结合的环境中。它包含此范围中的所有对象，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 名称空间（Namespace）

名称空间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**名称空间**，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、地址与生日等信息。又如Windows操作系统的NTFS文件系统也是一个**名称空间**，在这个文件系统内，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信息。

Active Directory域服务（AD DS）也是一个**名称空间**。利用AD DS，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Domain Name System （DNS）来解析主机名与IP地址的映射关系，例如利用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，因此域名是采用DNS格式来命名的，例如可以将AD DS的域名命名为

sayms.local。

1.1.3 对象（Object）与属性（Attribute）

AD DS内的资源是以对象的形式存在，例如用户、计算机等都是对象，而对象是通过**属性**来描述其特征的，也就是对象本身是一些**属性**的集合。例如如果要为用户**王乔治**建立一个账户，则需要新建一个对象类型（object class）为**用户**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、登录名与地址等，这其中的用户账户就是对象，而姓、名与登录名等就是该对象的属性（参见表1-1-1）。另外，图1-1-1中的**王乔治**就是对象类型为**用户**（user）的对象。

表1-1-1

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

图 1-1-1

1.1.4 容器（Container）与组织单位（Organization Units，OU）

容器与对象相似，它也有自己的名称，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。而组织单位是一个比较特殊的容器，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。图1-1-2所示就是一个名称为**业务部**的组织单位，其中包含着多个对象，其中两个为**用户**对象、两个为**计算机**对象与两个本身也是组织单位的对象。

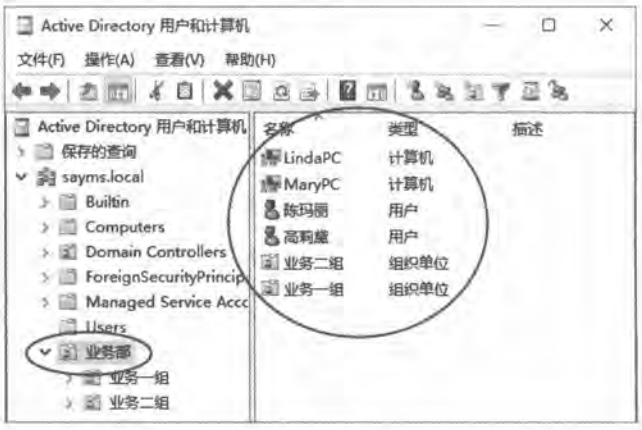

图 1-1-2

AD DS是以层级式架构（hierarchical）将对象、容器与组织单位等组合在一起，并将其存储到AD DS数据库内。

1.1.5 域树（Domain Tree）

我们可以搭建包含多个域的网络，而且是以域树（domain tree）的形式存在，如图1-1-3就是一个域树，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。

图中域树符合DNS域名空间的命名原则，而且具有连续性的，也就是子域的域名包含其父域的域名，例如域sales.sayms.local的后缀内包含其上层（父域）的域名sayms.local；而nor.sales.sayms.local的后缀内包含其上层的域名sales.sayms.local。

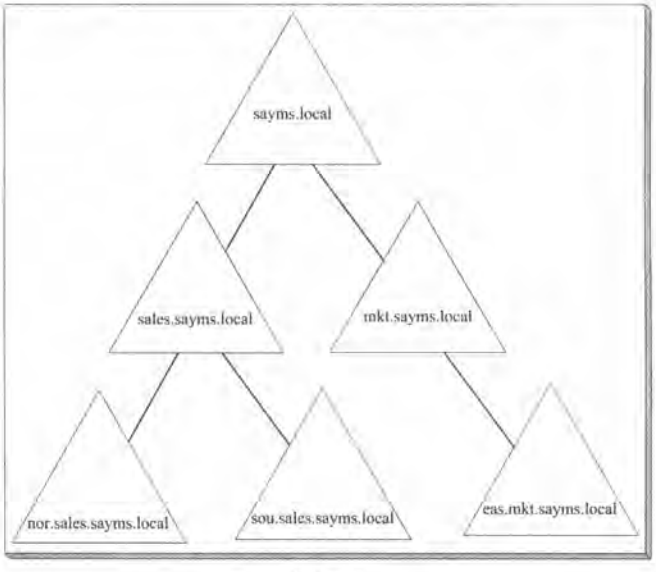

图 1-1-3

在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，不过其中的数据是分散存储在各个域中的，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（Trust）

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域被加入到域树后，这个域会自动信任其上层的父域，同时父域也会自动信任此新子域，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，这个用户是否能够访问域B内的资源呢?

A 只要域B有信任域A就可以。

我们以图1-1-4来解释双向可传递性，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会自动信任域 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会自动信任域 A。结果是域A和域C之间也就自动地建立起双向的信任关系。

当任何一个新域加入到域树后，它会自动双向信任这个域树内所有的域，因此只要拥有适当权限，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。

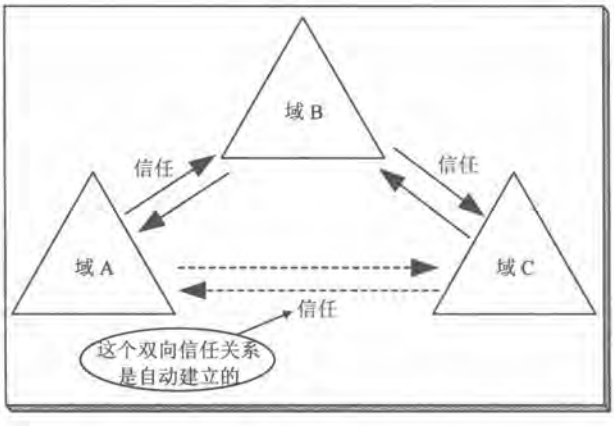

图 1-1-4

1.1.7 林（Forest）

林是由一个或多个域树所组成的，每一个域树都有自己唯一的名称空间，如图1-1-5所

示，其中一个域树内的每一个域名都以sayms.local结尾，而另一个则都以say365.local结尾。

第一个域树的根域，就是整个林的根域（forest root domain），同时其域名就是林的林名称。如图1-1-5中的sayms.local是第一个域树的根域，它就是整个林的根域，而林名称就是sayms.local。

在建立林时，每一个域树的根域与林根域之间双向的、可传递的信任关系都会被自动建立起来，因此每一个域树中的每一个域内的用户，只要拥有权限，就可以访问其他任何一个域树内的资源，也可以到其他任何一个域树内的成员计算机登录。

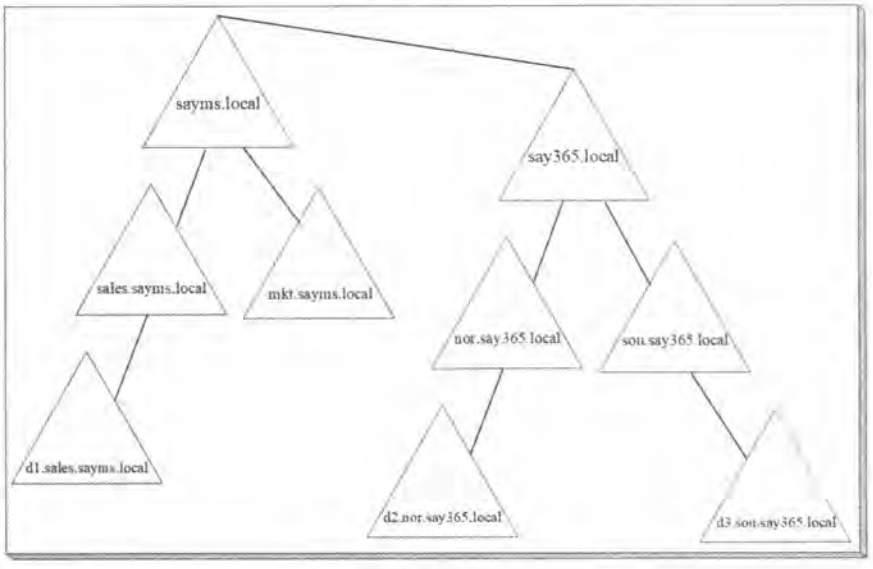

图 1-1-5

1.1.8 架构（Schema）

AD DS对象类型与属性数据是定义在**架构**内的，例如它定义了**用户**对象类型内包含哪一些属性（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**内添加其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（Domain Controller）

Active Directory域服务（AD DS）的目录数据是存储在域控制器内的。一个域内可以有多台域控制器，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了一个用户账户后，此账户默认是被建立在此域控制器的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）。

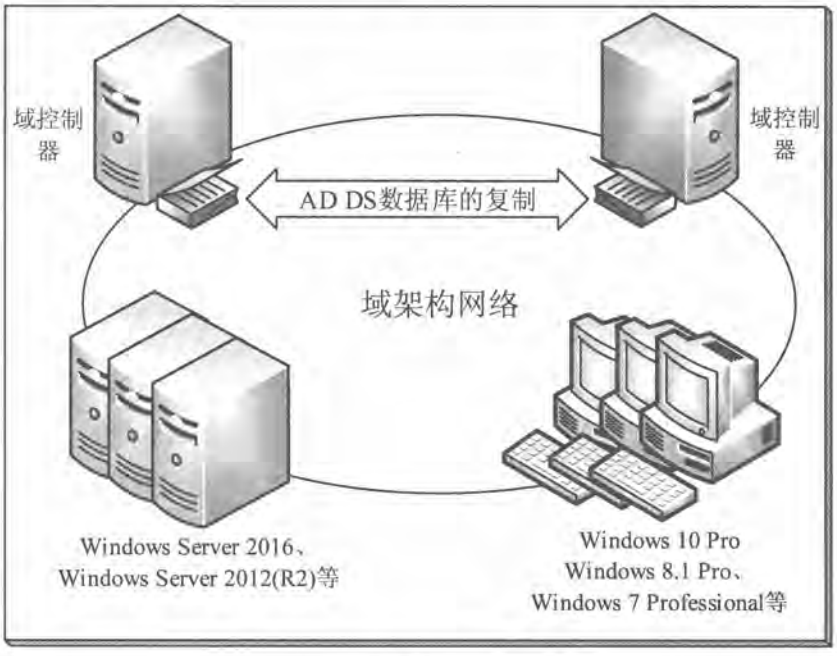

图 1-1-6

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。如果正确，用户就可以成功登录；反之，会被拒绝登录。

多台域控制器可以提供容错功能，也就是即使有一台域控制器出现故障了，仍然能够由其他域控制器来提供服务。另外它也可以提升用户登录效率，因为多台域控制器可以分担审核登录用户身份（用户名与密码）的负担。

域控制器是由服务器级别的计算机来扮演的，例如Windows Server 2016、Windows Server 2012（R2）、Windows Server 2008（R2）等。

1.1.10 只读域控制器（RODC）

只读域控制器（Read-Only Domain Controller，RODC）的AD DS数据库只能被读取、不能被修改，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网络来使用，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并不如总公司完备，同时也可能缺乏IT技术人员，因此采用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

除了用户账户的密码之外，RODC的AD DS数据库内会存储AD DS域内的所有对象与属性。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，因此它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进行验证。

由于RODC的AD DS数据库是只读的，因此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的话，这些变更请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改动数据复制到RODC。

2. 单向复制（Unidirectional Replication）

总公司的可读写域控制器的AD DS数据库发生变化时，这些变化数据会被复制到RODC。然而因为用户或应用程序无法直接更改RODC的AD DS数据库，因此总公司的可读写域控制器不会从RODC同步数据，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（用于存储与组策略有关的设置）复制给RODC时，也是采用单向复制。

3. 认证缓存（Credential Caching）

RODC在验证用户的密码时，仍然需将它们提交到总公司的可读写域控制器来验证，如果希望提高验证效率的话，可以选择将用户的密码存储到RODC的认证缓存区。这需要通过**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被入侵的话，则存储在缓存区内的认证信息可能会外泄。

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，他可以在RODC这台域控制器登录、执行管理工作，例如更新驱动程序等，但他却无法登录其他域控制器，也无法执行其他域管理工作。此功能允许将RODC的一般管理工作委派给特定的用户，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。客户端可向这一台扮演RODC角色的DNS服务器提出DNS查询请求。

不过RODC的DNS服务器不支持客户端直接进行动态更新，因此客户端的更新记录请求，会被此DNS服务器提交到其他DNS服务器，让客户端转向该DNS服务器进行更新，而RODC的DNS服务器也会自动从这台DNS服务器复制这条更新记录。

1.1.11 可重启的AD DS（Restartable AD DS）

在旧版的Windows域控制器内，如果要进行AD DS数据库维护工作的话（例如数据库脱机整理），就需重新启动计算机、进入**目录服务还原模式**（或译为**目录服务修复模式**，Directory Service Restore Mode）来执行维护工作。如果这台域控制器也同时提供其他网络服务的话，例如它同时也是DHCP服务器，则重新启动计算机期间将造成这些服务暂时中断。

除了进入**目录服务还原模式**之外，Windows Server 2016等域控制器还提供**可重新启动的AD DS**功能，也就是说如果要执行AD DS数据库维护工作的话，只需要将AD DS服务停止即可，不需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数据库的维护工作更容易、更快完成，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，默认只能够利用**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

在旧版Windows系统中，系统管理员如果不小心将AD DS对象删除，如果要恢复被删除的对象会有很多先决条件，且操作复杂。例如误删组织单位的话，则其中所有对象都会被删除，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，不过这种操作很耗费时间，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。Windows Server 2016具备**Active Directory回收站**功能，它让系统管理员不需要进入**目录服务还原模式**，就可以恢复被删除的对象。

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利用此模式进行复制的。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数据库内新建一个用户账户后，此账户会自动被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数据库内少部分数据是采用**单主机复制模式**来复制的。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**）负责接收与处理此请求，也就是说该对象是先被更新在**操作主机**，再由**操作主机**将它复制给其他域控制器。例如添加或删除一个域时，这个更改信息会先被写入到扮演**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

如果要完全管理网络内的计算机，请将它们加入域。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含：

- 成员服务器（member server），例如：
  - Windows Server 2016 Datacenter/Standard/Essentials
  - Windows Server 2012（R2） Datacenter/Standard
  - Windows Server 2008（R2） Datacenter/Enterprise/Standard

  上述服务器级别的计算机加入域后被称为**成员服务器**，但成员服务器内并没有AD DS数据库，它们也不负责审核AD DS域用户名与密码，而是将其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 10 Enterprise/Pro/Education
  - Windows 8.1（8） Enterprise/Pro
  - Windows 7 Ultimate/Enterprise/Professional
  - Windows Vista Ultimate/Enterprise/Business

  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。

注意

其他入门级的客户端计算机（例如Windows 10 Home）无法加入域。

可以将Windows Server 2016、Windows Server 2012（R2）、Windows Server 2008（R2）

等独立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或成员服务器。

1.1.15 DNS服务器

域控制器需要将自己注册到DNS服务器内，以便让其他计算机通过DNS服务器来找到这台域控制器，因此域环境需要有可支持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发生变化或域成员计算机的IP地址等数据发生变化时，可以自动更新DNS服务器内的记录。

1.1.16 轻型目录访问协议（LDAP）

LDAP（Lightweight Directory Access Protocol）是一种用来查询与更新AD DS的目录服务通信协议。AD DS利用**LDAP名称路径**（LDAP naming path）来表示对象在AD DS内的位置，以便用它来访问AD DS对象。**LDAP名称路径**包含：

- **Distinguished Name（DN）**：它是对象在AD DS内的完整路径，例如图1-1-7中的用户账户名称为**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）表示DNS域名中的组件，例如sayms.local中的sayms与local；OU为组织单位；CN为common name。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是属于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。
- **Relative Distinguished Name（RDN）**：RDN是用来代表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。

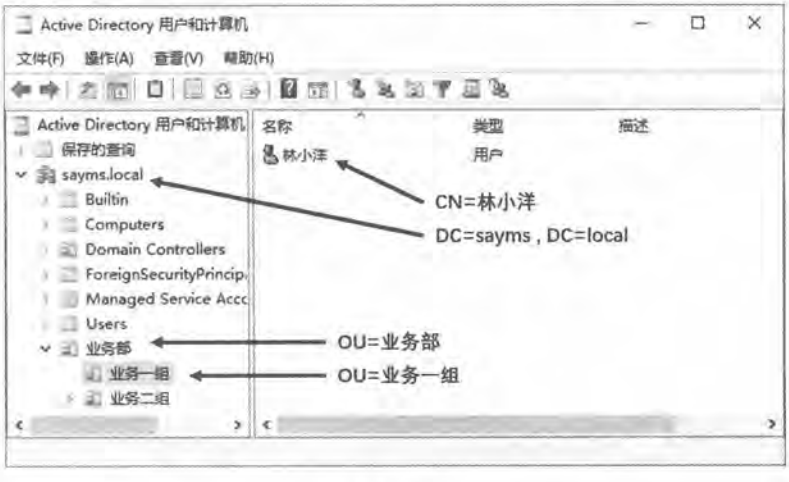

图 1-1-7

除了DN与RDN这两个对象名称外，另外还有以下名称：

- **Global Unique Identifier（GUID）**：系统会自动为每一个对象分配一个唯一的、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。
- **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，如图1-1-7中的**林小洋**是隶属域sayms.local，则其UPN可为bob@sayms.local。用户登录时所输入账户名称最好使用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，因此用户可以一直用同一个名称来登录。
- **Service Principal Name（SPN）**：SPN是一个包含多重设置值的名称，它是根据DNS主机名建立的。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（Global Catalog）

虽然在域树内的所有域共享一个AD DS数据库，但其数据却是分散在各个域内的，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，因此在AD DS内设计了**全局编录**。一个林内的所有域树共享相同的**全局编录**。

全局编录的数据是存储在域控制器内的，这台域控制器可被称为**全局编录服务器**，它存储着林内所有域的AD DS数据库内的每一个对象，不过只存储对象的部分属性，这些属性都是常用的、用于查找对象的属性，例如用户的电话号码、登录名等。**全局编录**让用户即使不知道对象是位于哪一个域内，仍然可以快速地找到对象。

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**信息；用户利用UPN登录时，它也负责提供该用户是隶属于哪一个域的信息。

1.1.18 站点（Site）

站点是由一或多个IP子网所组成，这些子网之间通过**高速且可靠的链路**连接在一起，也就是这些子网之间的连接速度要够快且稳定，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）内的各个子网之间的链路都符合速度并且高可靠的要求，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不快，因此WAN之中的各个LAN应分别规划为不同的站点，参见图1-1-8。

域是逻辑的（logical）分组，而站点则是物理的（physical）分组。在AD DS内一个站点可能包含多个域；而一个域内的各个计算机也可能分属于不同的站点。

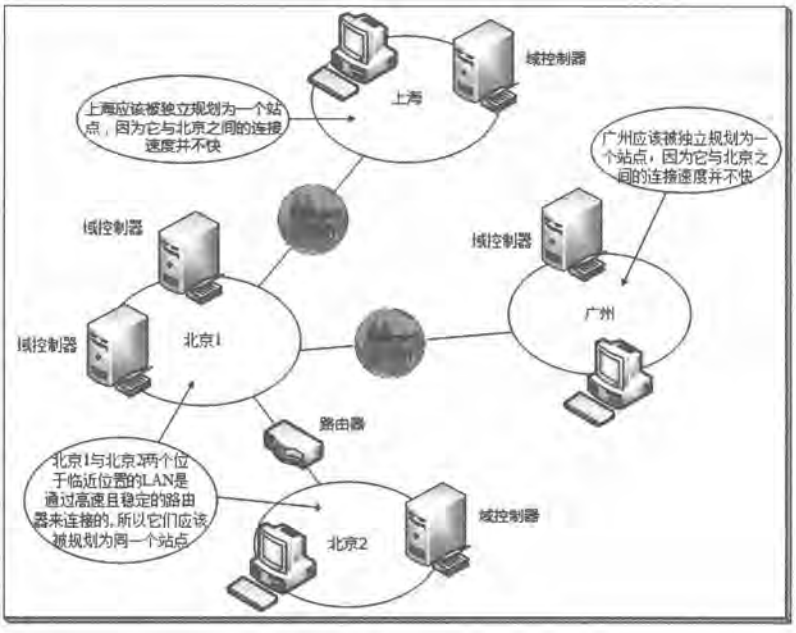

图 1-1-8

如果一个域的域控制器分布在不同的站点中，而站点之间是慢速连接的话，由于不同站点的域控制器之间会互相复制AD DS数据库，因此要谨慎规划执行复制的时段，也就是尽量在离峰时段执行复制工作，同时复制的频率不要太高，以避免复制时占用站台之间的连接带宽，影响站点之间其他数据的传输效率。

同一个站点内的域控制器之间是通过快速链路连接在一起的，因此在复制AD DS数据时，可以实现快速复制。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操作，并且默认的复制频率也要高于不同站点之间的域控制器。

不同站点之间在复制时所传送的数据会被压缩，以减少站点之间连接带宽的负担；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（Directory Partition）

AD DS数据库被逻辑的分为以下多个目录分区：

- **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，也存储着如何建立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。
- **配置目录分区（Configuration Directory Partition）**：其中存储着整个AD DS的结构，例如有哪些域、有哪些站点、有哪些域控制器等信息。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。
- **域目录分区（Domain Directory Partition）**：每一个域各有一个**域目录分区**，其中

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，但并不会被复制到其他域的域控制器。

- **应用程序目录分区（Application Directory Partition）**：一般来说，**应用程序目录分区**是由应用程序所建立的，其中存储着与该应用程序有关的数据。例如由Windows Server 2016扮演的DNS 服务器，如果所建立的DNS区域为**Active Directory集成区域**的话，则它会在AD DS数据库内建立**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，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功能与限制。

1.2.1 域功能级别（Domain Functionality Level）

Active Directory域服务（AD DS）的**域功能级别**设置只会影响到该域而已，不会影响到其他域。**域功能级别**分为以下几种模式：

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

其中最新的**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**。

1.2.2 林功能级别（Forest Functionality Level）

Active Directory域服务（AD DS）的**林功能级别**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**：域控制器为Windows Server 2008或新版。
- **Windows Server 2008 R2**：域控制器为Windows Server 2008 R2或新版。
- **Windows Server 2012**：域控制器为Windows Server 2012或新版。
- **Windows Server 2012 R2**：域控制器为Windows Server 2012 R2或新版。
- **Windows Server 2016**：域控制器为Windows Server 2016。

其中最新的**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**WindowsServer 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	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（比如用户账户、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中，必须建立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，也能够拥有与AD DS一样的目录服务，以便让支持目录访问的应用程序可以有一个目录数据库来存储数据，因此提供了一个称为**Active Directory轻型目录服务**（Active Directory Lightweight Directory Services，**AD LDS**）的服务。

AD LDS可以允许在计算机内建立多个目录服务的环境，每一个环境被称为是一个**AD LDS实例**（instance），每一个**AD LDS实例**分别拥有独立的目录配置与架构（schema），也分别拥有专用的目录数据库，以供支持目录访问的应用程序来使用。

如果要在Windows Server 2016内安装AD LDS角色：【单击左下角**开始**图标➲服务器管理器➲单击**仪表板**处的**添加角色和功能**➲……➲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建立**AD LDS实例**：【单击左下角**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**开始**图标➲**Windows管理工具**➲**ADSI编辑器**】来管理**AD LDS实例**内的目录配置、架构、对象等。


添加角色和功能向导
选择服务器角色
目标服务器
Server1
开始之前
安装类型
服务器选择
服务器角色
功能
AD LDS
确认
选择要安装在所选服务器上的一个或多个角色。
角色
Active Directory Rights Management Services
Active Directory 联合身份验证服务
Active Directory 轻型目录服务
Active Directory 域服务
Active Directory 证书服务
DHCP 服务器
DNS 服务器
Hyper-V
描述
Active Directory 轻型目录服务(AD LDS)为应用程序特定的数据以及启用目录的应用程序(不需要 Active Directory 域服务基础结构)提供存储。一个服务器上可以存在多个 AD LDS 实例，其中每个实例都可以有自己的架构。

图 1-3-1