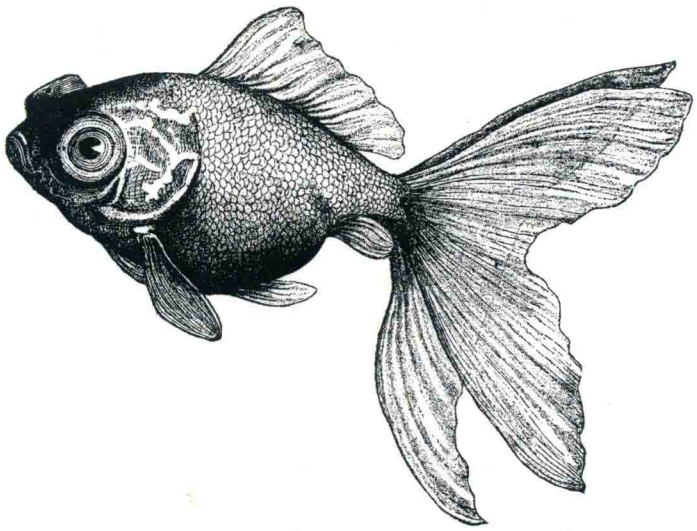
工业和信息化“十三五”
人才培养规划教材



Windows Server 2012 活动目录企业应用 微课版

Windows Server 2012 Active Directory Enterprise Application

杨云 ◎ 著

二维码扫一扫，同步看**微课视频**

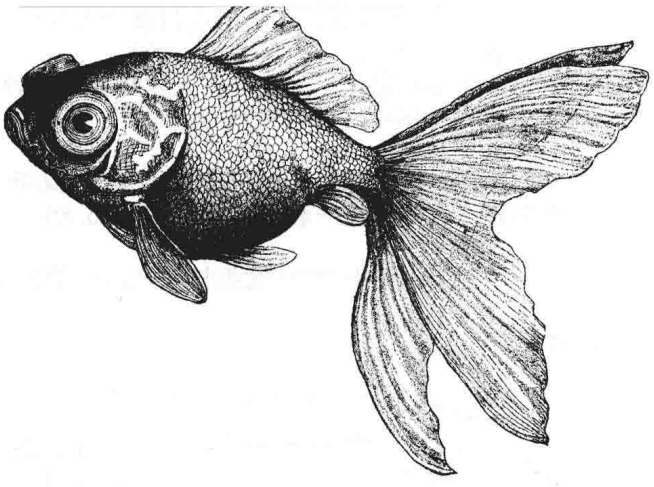
采用基于工作过程导向“**教**、**学**、**做**”一体化编写方式

提供大量**企业真实案例**，所有案例都可以在实验环境中**完整实现**

中国工信出版集团

人民邮电出版社
POSTS & TELECOM PRESS

工业和信息化“十三五”
人才培养规划教材



Windows Server 2012 活动目录企业应用 微课版

Windows Server 2012 Active Directory Enterprise Application

杨云 ◎ 著

人 民 邮 电 出 版 社
北 京

图书在版编目（CIP）数据

Windows Server 2012活动目录企业应用 : 微课版 / 杨云著. -- 北京 : 人民邮电出版社, 2018.8
工业和信息化“十三五”人才培养规划教材
ISBN 978-7-115-48295-2

Ⅰ. ①W… Ⅱ. ①杨… Ⅲ. ①Windows操作系统－网络服务器－高等学校－教材 Ⅳ. ①TP316.86

中国版本图书馆CIP数据核字(2018)第076669号

内 容 提 要

本书以目前被广泛应用的 Windows Server 2012 R2 为例，采用教、学、做相结合的模式，着眼实践应用，以企业真实案例为基础，全面、系统地介绍活动目录在企业中的应用。全书共分 3 部分：构建 AD DS 环境、配置与管理组策略和管理与维护 AD DS。

本书结构合理，知识全面且实例丰富，语言通俗易懂。本书采用“任务驱动、项目导向”的方式，注重知识的实用性和可操作性，强调职业技能训练。本书所有项目的知识点、技能点和项目实训操作都已录制成微课，并以二维码形式嵌入相应位置，读者可通过扫码看微课。

本书适合高等院校、高等职业院校计算机网络相关专业学生，以及 Windows Server 2012 R2 初、中级用户、网络系统管理工程师、网络系统运维工程师和社会培训人员等学习，是网络工程师必备的学习宝典。

◆ 著　　杨　云
责任编辑　马小霞
责任印制　马振武

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
固安县铭成印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：16.5　　2018 年 8 月第 1 版
字数：384 千字　　2018 年 8 月河北第 1 次印刷

定价：49.80 元

读者服务热线：(010)81055256　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字 20170147 号

前 言 FOREWORD

一、编写背景

活动目录服务是微软 Windows 操作系统最重要的服务，而 Windows Server 2012 R2 是其最新的服务版本，经过两年多的市场应用，目前已经成为业界的主流应用版本。

活动目录的配置与管理是网络系统管理工程师、网络系统运维工程师的典型工作任务，是计算机网络技术高技能人才必须具备的核心技能，也是应用型本科和高职计算机网络类专业一门重要的专业核心课程。本书以培养读者活动目录的构建、应用、维护与管理技能为目标，详细介绍构建活动目录域服务（Active Directory Domain Service，AD DS）环境、配置与管理组策略、管理与维护 AD DS 等内容。

本书将用实际的企业应用案例为读者展现强大的活动目录功能，通过每一个工作任务的训练，让读者快速掌握活动目录的操作技能；并通过举一反三，让读者快速地将 Windows Server 2012 R2 活动目录的知识和技能与自身工作联系起来。

二、本书特点

本书具有以下特点。

（1）适于零基础读者，入门门槛低，很容易上手。

（2）基于工作过程导向的“教、学、做”一体化的编写方式，涵盖活动目录企业应用的各个方面。

（3）提供大量企业真实案例，适用性、实践性强。全书列举的所有示例和实例，读者都可以在自己的实验环境中完整实现。

（4）作者录制了大量视频进行讲解，读者可以通过扫二维码看视频，更直观地学习。

三、本书的章节安排

全书共分 3 部分。

第一部分　构建 AD DS 环境（第 1 章 ~ 第 3 章）

第一部分主要内容包括部署与管理 AD DS、建立域树和林、管理域用户和组。

第二部分　配置与管理组策略（第 4 章 ~ 第 6 章）

第二部分主要内容包括使用组策略管理用户工作环境、利用组策略部署软件与限制软件运行、管理组策略。

第三部分　管理与维护 AD DS（第 7 章 ~ 第 10 章）

第三部分主要内容包括配置活动目录的对象和信任、配置 AD DS 站点和复制、管理操作主机、维护活动目录，以及在 AD DS 中发布资源。

四、本书适合的读者

（1）活动目录初、中级用户；

（2）网络系统管理工程师；
（3）网络系统运维工程师；
（4）大中专院校的学生；
（5）社会培训人员。

五、其他

本书由杨云著，参与编写工作的还有张晖、杨翠玲、王世存、杨昊龙、崔希等。由于著者水平有限，书中难免存在错误和不妥之处，恳请广大读者批评指正。欢迎加入 Linux& Windows 教师 QQ 交流群：189934741。

著　者
2018 年 3 月

目录 CONTENTS

第一部分　构建 AD DS 环境

第二部分　配置与管理组策略

第三部分　管理与维护 AD DS

第一部分

构建 AD DS 环境

第1章 部署与管理 AD DS

学习背景

未名公司组建的单位内部的办公网络原来是基于工作组方式的，近期由于公司业务发展，人员激增，基于方便和网络安全管理的需要，考虑将基于工作组的网络升级为基于域的网络，现在需要将一台或多台计算机升级为域控制器，并将其他所有计算机加入域成为成员服务器。同时将原来的本地用户账户和组也升级为域用户和组进行管理。

学习目标

- 掌握规划和安装局域网中的活动目录的方法
- 掌握创建目录林根级域的方法
- 掌握安装额外域控制器的方法
- 掌握创建子域的方法

1.1 理论基础

Active Directory 又称活动目录，是 Windows Server 系统中非常重要的目录服务。Active Directory 用于存储网络上各种对象的有关信息，包括用户账户、组、打印机、共享文件夹等，并把这些信息存储在目录服务数据库中，便于管理员和用户查询及使用。活动目录具有安全、可扩展、可伸缩的特点，与 DNS 集成在一起，可基于策略进行管理。

AD DS 域服务相关知识

1.1.1 认识活动目录及意义

什么是活动目录呢？活动目录就是 Windows 网络中的目录服务（Directory Service），即（Active Directory Domain Service，AD DS）活动目录域服务。目录服务包含两方面内容：目录及与目录相关的服务。

活动目录负责目录数据库的保存、新建、删除、修改与查询等服务，用户能很容易地在目录内寻找所需要的数据。

AD DS 的适用范围非常广泛，它可以用在一台计算机、一个小型局域网络（LAN）或数个广域网（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、域控制器和用户账户等。活动目录具有以下意义。

1. 简化管理

活动目录和域密切相关。域是指网络服务器和其他计算机的一种逻辑分组，凡是在共享域逻辑范围内的用户都使用公共的安全机制和用户账户信息，每个使用者在域中只拥有一个账户，每次登录的是整个域。

活动目录用于将域中的资源分层次地组织在一起，每个域都包含一个或多个域控制器（Directory Controler，DC）。域控制器就是安装活动目录的 Windows Server 2012（R2）的计算机，它存储域目录完整的副本。为了简化管理，域中的所有域控制器都是对等的，可以在任意一台域控制器上做修改，更新的内容将被复制到该域中所有其他域控制器。活动目录为管理网络上的所有资源提供单一入口，进一步简化了管理，管理员可以登录任意一台计算机管理网络。

2. 安全性

安全性通过登录身份验证及目录对象的访问控制集成在活动目录之中。通过单点网络登录，管理员可以管理分散在网络各处的目录数据和组织单位，经过授权的网络用户可以访问网络任意位置的资源，基于策略的管理简化了网络的管理。

活动目录通过对象访问控制列表及用户凭据保护用户账户和组信息。因为活动目录不但可以保存用户凭据，而且可以保存访问控制信息，所以登录到网络上的用户既能够获得身份验证，也可以获得访问系统资源所需的权限。例如，在用户登录到网络时，安全系统会利用存储在活动目录中的信息验证用户的身份，在用户试图访问网络服务时，系统会检查在服务的自由访问控制列表（DCAL）中定义的属性。

活动目录允许管理员创建组账户，管理员可以更加有效地管理系统的安全性，通过控制组权限即可控制组成员的访问操作。

3. 改进的性能与可靠性

Windows Server 2012 能够更加有效地管理活动目录的复制与同步，不管是在域内还是在域间，管理员都可以更好地控制要在域控制器间进行同步的信息类型。活动目录还提供了许多技术，可以智能地选择只复制发生更改的信息，而不是机械地复制整个目录的数据库。

1.1.2 名称空间

名称空间（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、地址与生日等数据。再如 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数据。

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 网络环境下利用 Domain Name System（DNS）来解析主机名与 IP 地址的对应关系，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 long.com。

1.1.3 对象和属性

AD DS 内的资源以对象（Objects）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（Atributes）来描述其特征的，也就是对象本身是一些属性的集合。例如若要为使用者张三建立一个账户，则需新建一个对象类型（object class）为用户的对象（也就是用户账户），然后在此对象内输入张三的姓、名、登录名与地址等，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。

1.1.4 容器

容器（Container）与对象类似，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。

组织单位是一个比较特殊的容器，其内可以包含其他对象与组织单位。组织单位也是应用组策略（group policy）和委派责任的最小单位。

AD DS 以层次式架构（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 可重新启动的 AD DS

在旧版 Windows 域控制器内，若要进行 AD DS 数据库维护工作（例如数据库脱机重整），就需要重新启动计算机、进入目录服务还原模式（Directory Service Restore Mode）来执行维护工作。若这台域控制器也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 2012 （R2）等域控制器还提供可重新启动的 AD DS（Restartable AD DS）功能，也就是说若要执行 AD DS 数据库维护工作，只需要将 AD DS 服务停止即可，不需要重新启动计算机来进入目录服务还原模式。这样不但可以让 AD DS 数据库的维护工作更容易、更快速地完成，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 服务停止的域控制器上利用域用户账户登录。若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。

1.1.6 Active Directory 回收站

在旧版 Windows 系统中，系统管理员若不小心将 AD DS 对象删除，其恢复过程耗时耗力，例如误删组织单位，其内所有对象都会丢失，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。Windows Server 2012（R2）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，就可以快速恢复被删除的对象。

1.1.7 AD DS 的复制模式


AD DS 域服务相关知识

域控制器之间在复制 AD DS 数据库时，分为下面两种复制模式。

- 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操作的。在此模式下，您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，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进行复制的。在此模式下，当您提出修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在操作主机中被更新，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，此变动数据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（详见第 10 章）。

1.1.8 认识活动目录的逻辑结构

活动目录的结构是指网络中所有用户、计算机以及其他网络资源的层次关系，就像一个大型仓库中分出若干个小储藏间，每个小储藏间又分别用来存放东西。通常活动目录的结构可分为逻辑结构和物理结构，分别包含不同的对象。

活动目录的逻辑结构非常灵活，目录中的逻辑单元通常包括架构、域、组织单位、域树、域林、站点和目录分区。

1. 架构

AD DS 对象类型与属性数据是定义在架构（Schema）内的，例如它定义了用户对象类型内包含哪些属性（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。

2. 域

域是在 Windows NT/2000/2003/2008/2012 网络环境中组建客户机/服务器网络的实现方式。所谓域，是由网络管理员定义的一组计算机集合，实际上就是一个网络。在这个网络中，至少有一台称为域控制器的计算机，充当服务器角色。在域控制器中保存着整个网络的用户账号及目录数据库，即活动目录。管理员可以通过修改活动目录的配置来实现对网络的管理和控制，如管理员可以在活动目录中为每个用户创建域用户账号，使他们可登录域并访问域的资源。同时，管理员也可以控制所有网络用户的行为，如控制用户能否登录、在什么时间登录、登录后能执行哪些操作等。而域中的客户计算机要访问域的资源，则必须先加入域，并通过管理员为其创建的域用户账号登录域，才能访问域资源，同时，也必须接受管理员的控制和管理。构建域后，管理员可以对整个网络实施集中控制和管理。

3. 组织单位

组织单位（Organizational Unit，OU）在活动目录（Active Directory，AD）中扮演特殊的角色，它是一个当普通边界不能满足要求时创建的边界。OU 把域中的对象组织成逻辑管理组，而不是安全组或代表地理实体的组。OU 是应用组策略和委派责任的最小单位。

组织单位是包含在活动目录中的容器对象。创建组织单位的目的是对活动目录对象进行分类。比如，由于一个域中的计算机和用户较多，会使活动中的对象非常多。这时，管理员如果想查找某一个用户账号并进行修改是非常困难的。另外，如果管理员只想对某一部门的用户账号进行操作，实现起来不太方便。但如果管理员在活动目录中创建了组织单位，所有操作就会变得非常简单。比如管理员可以按照公司的部门创建不同的组织单位，如财务部组织单位、市场部组织单位、策划部组织单位等，并将不同部门的用户账号建立在相应的组织单位中，更便于管理。除此之外，管理员还可以针对某个组织单位设置组策略，实现对该组织单位内所有对象的管理和控制。

总之，创建组织单位有如下好处。

① 可以分类组织对象，使所有对象结构更清晰。

② 可以对某些对象配置组策略，实现对这些对象的管理和控制。

③ 可以委派管理控制权，如管理员可以给不同部门的网络主管授权，让他们管理本部门的账号。

因此组织单位是可将用户、组、计算机和其他单元放入活动目录的容器，组织单位不能包括来自其他域的对象。组织单位是可以指派组策略设置或委派管理权限的最小作用单位。使用组织单位，用户可在组织单位中代表逻辑层次结构的域中创建容器，这样就可以根据组织模型管理网络资源的配置和使用。可授予用户对域中某个组织单位的管理权限，组织单位的管理员不需要具有域中任何其他组织单位的管理权。

4. 域目录树

当要配置一个包含多个域的网络时，应该将网络配置成域目录树结构，如图 1-1 所示。

图 1-1　域目录树

在图 1-1 所示的域目录树中，最上层的域名为 China.com，是这个域目录树的根域，也称为父域。下面两个域 Jinan.China.com 和 Beijing.China.com 是 China.com 域的子域。3 个域共同构成了这个域目录树。

活动目录的域名仍然采用 DNS 域名的命名规则。如图 1-1 所示的域目录树中，两个子域的域名 Jinan.China.com 和 Beijing.China.com 中仍包含父域的域名 China.com，因此，它们的名称空间是连续的。这也是判断两个域是否属于同一个域目录树的重要条件。

在整个域目录树中，所有域共享同一个活动目录，即整个域目录树中只有一个活动目录。只不过这个活动目录分散地存储在不同的域中（每个域只负责存储和本域有关的数据），整体上形成一个大的分布式的活动目录数据库。在配置一个较大规模的企业网络时，可以配置为域目录树结构，比如将企业总部的网络配置为根域，各分支机构的网络配置为子域，

整体上形成一个域目录树，以实现集中管理。

5. 域目录林

如果网络的规模比前面提到的域目录树还要大，甚至包含了多个域目录树，这时可以将网络配置为域目录林（也称森林）结构。域目录林由一个或多个域目录树组成，如图 1-2 所示。域目录林中的每个域目录树都有唯一的命名空间，它们之间并不是连续的，这一点从图 1-2 中的两个目录树中可以看到。

整个域目录林中也存在一个根域，这个根域是域目录林中最先安装的域。在图 1-2 所示的域目录林中，China.com 是最先安装的，则这个域是域目录林的根域。

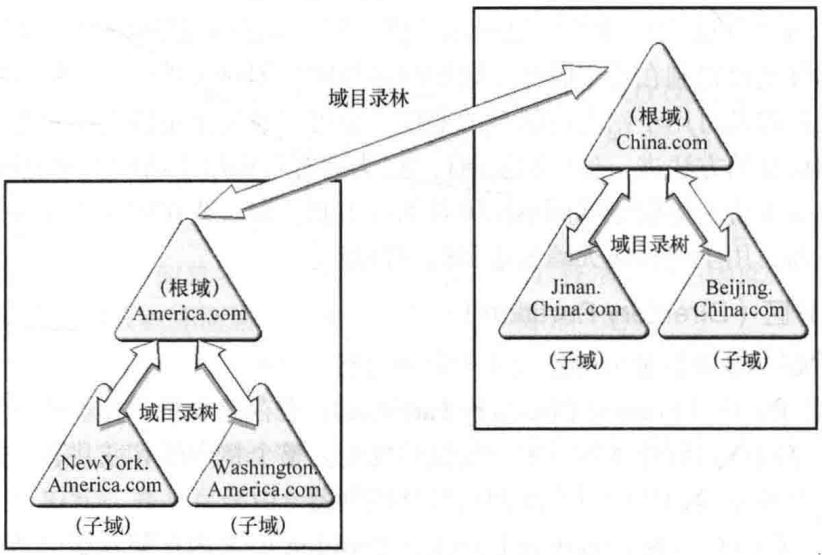


图 1-2 域目录林

注意：在创建域目录林时，组成域目录林的两个域目录树的树根之间会自动创建相互的、可传递的信任关系。由于有了双向的信任关系，域目录林中的每个域中的用户都可以访问其他域的资源，也可以从其他域登录到本域中。

6. 站点

AD DS 域服务相关知识

站点由一个或多个 IP 子网组成，这些子网通过高速网络设备连接在一起。站点往往由企业的物理位置分布情况决定，可以依据站点结构配置活动目录的访问和复制拓扑关系，使得网络更有效地连接，复制策略更合理，用户登录更快速。活动目录中的站点与域是两个完全独立的概念，一个站点中可以有多个域，多个站点也可以位于同一个域中。

活动目录站点和服务可以通过使用站点提高大多数配置目录服务的效率。通过使用活动目录站点和服务来发布站点，并提供有关网络物理结构的信息，从而确定如何复制目录信息和处理服务的请求。计算机站点是根据其在子网或组已连接好子网中的位置指定的，子网用来为网络分组，类似于生活中使用邮政编码划分地址。划分子网可方便发送有关网络与目录连接的物理信息，而且同一子网中计算机的连接情况通常优于不同网络。

使用站点的意义主要有如下 3 点。

① 提高了验证过程的效率。当客户使用域账户登录时，登录机制首先搜索与客户处于同一站点内的域控制器，使用客户站点内的域控制器可以使网络传输本地化，从而加快了身份验证的速度，提高了验证过程的效率。

② 平衡了复制频率。活动目录信息可在站点内部或站点之间进行信息复制，但由于网络的原因，活动目录在站点内部复制信息的频率高于站点间的复制频率，这样做可以平衡对最新目录的信息需求和可用网络带宽带来的限制，可以通过站点链接来定制活动目录如何复制信息以指定站点的连接方法，活动目录使用有关站点如何连接的信息生成连接对象，以便提供有效的复制和容错。

③ 可提供有关站点链接信息。活动目录可使用站点链接信息费用、链接使用次数、链接何时可用以及链接使用频度等信息确定应使用哪个站点来复制信息以及何时使用该站点。定制复制计划使复制在特定时间（诸如网络传输空闲时）进行，会使复制更为有效。通常所有域控制器都可用于站点间信息的变换，也可以通过指定桥头堡服务器优先发送和接收站间复制信息的方法进一步控制复制行为。当拥有希望用于站间复制的特定服务器时，我们宁愿建立一个桥头堡服务器而不使用其他可用服务器。或在配置代理服务器时建立一个桥头堡服务器，用于通过防火墙发送和接收信息。

7. 目录分区（Directory Partition）

AD DS 数据库被逻辑地分为下面 4 个目录分区。

① 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。

② 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、哪些站点、哪些域控制器等数据。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。

③ 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，但并不会被复制到其他域的域控制器。

④ 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，其内存储着与该应用程序有关的数据，例如由 Windows Server 2012 R2 扮演的 DNS 服务器，若所建立的 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特定的域控制器中，而不是所有的域控制器。

1.1.9 认识活动目录的物理结构

活动目录的物理结构与逻辑结构是彼此独立的两个概念。逻辑结构侧重于网络资源的管理，而物理结构则侧重于网络的配置和优化。物理结构的 3 个重要概念是域控制器、只读域控制器（RODC）和全局编录服务器。

1. 域控制器

域控制器是指安装了活动目录的 Windows Server 2012 的服务器，它保存了活动目录信

息的副本。域控制器管理目录信息的变化，并把这些变化复制到同一个域中的其他域控制器上，使各域控制器上的目录信息同步。域控制器负责用户的登录过程以及其他与域有关的操作，如身份鉴定、目录信息查找等。一个域可以有多个域控制器，规模较小的域可以只有 2 个域控制器，一个实际应用，另一个用于容错性检查；规模较大的域则使用多个域控制器。

域控制器没有主次之分，采用多主机复制方案，每一个域控制器都有一个可写入的目录副本，这为目录信息容错带来了无尽的好处。尽管在某个时刻，不同的域控制器中的目录信息可能有所不同，但一旦活动目录中的所有域控制器执行同步操作之后，最新的变化信息就会一致。

2. 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的域控制器复制过来。RODC 主要是为远程分公司网络设计、使用的。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，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 环境的问题。

（1）RODC 的 AD DS 数据库内容

除了账户的密码之外，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 并不存储用户账户的密码，因此它在验证用户名称与密码时，仍然需将它们送到总公司的可写域控制器来验证。

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如果要修改 AD DS 数据库的对象或用户要修改密码，这些变更请求都会被转发到总公司的可写域控制器来处理，总公司的可写域控制器再通过 AD DS 数据库的复制程序将这些变动数据复制到 RODC。

（2）单向复制（Unidirectional Replication）

总公司的可写域控制器的 AD DS 数据库有变动时，此变动数据会被复制到 RODC。然而因为用户或应用程序无法直接修改 RODC 的 AD DS 数据库，故总公司的可写域控制器不会向 RODC 索取变动数据，因而可以降低网络的负担。

除此之外，可写域控制器通过 DFS 分布式文件系统将 SYSVOL 文件夹（用来存储与组策略有关的设置）复制给 RODC 时，也采用单向复制。

（3）认证缓存（Credential Caching）

RODC 在验证用户的密码时，仍然需要将它们送到总公司的可写域控制器来验证，若希望提高验证速度，可以选择将用户的密码存储到 RODC 的认证缓存区。您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，若 RODC 被入侵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）

您可以通过系统管理员角色隔离功能来将任何一位域用户指定为 RODC 的本机系统管