

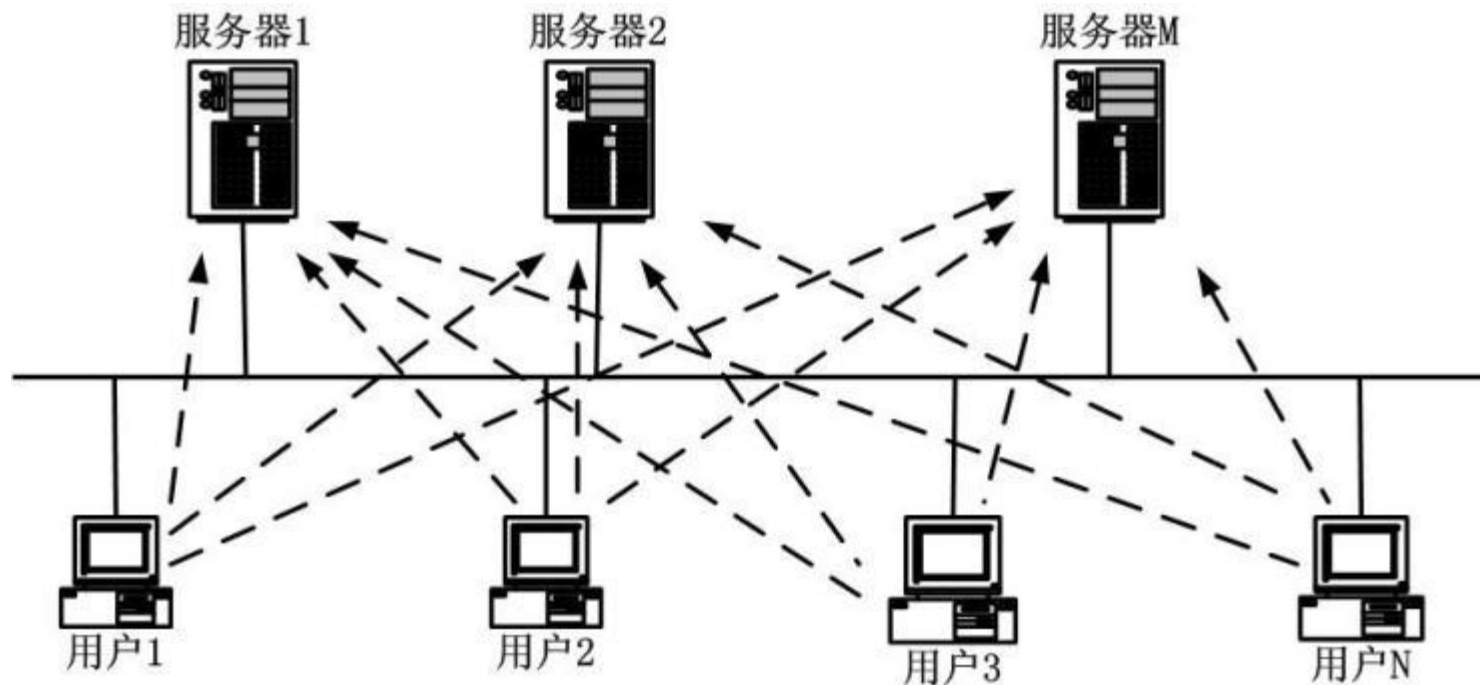
MICROSOFT OFFICIAL COURSE

# MCITP-活动目录(1)

- windows server 2008活动目录
- 创建第一个域

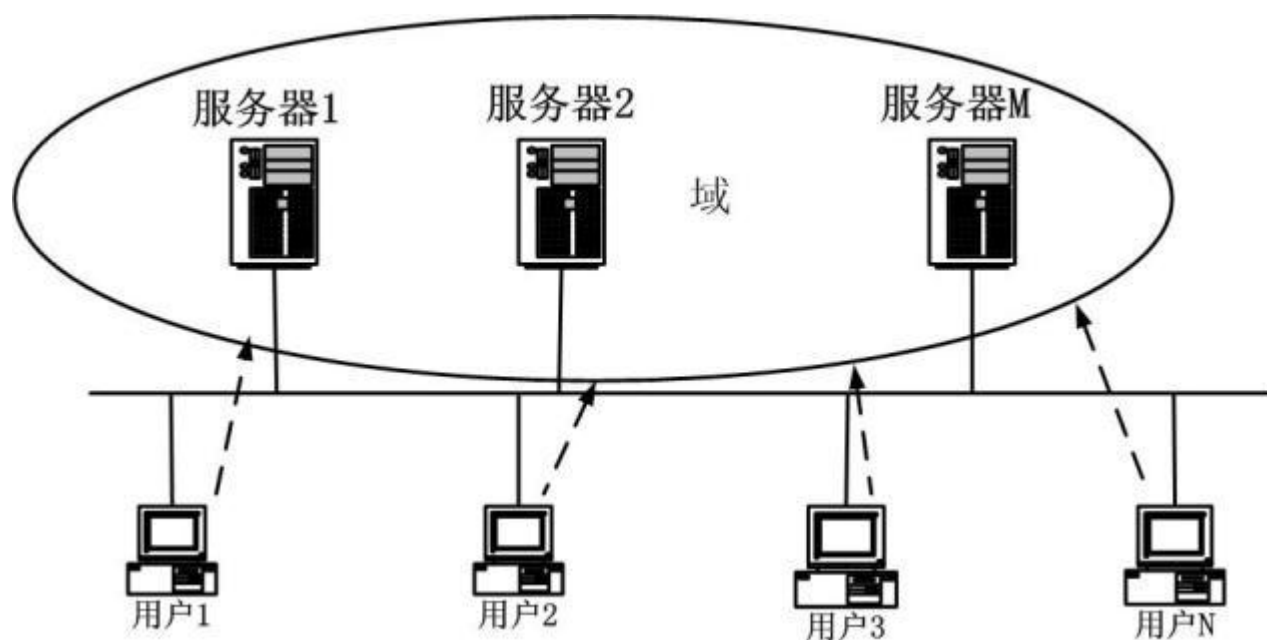
# 为什么需要域

- 如果资源分布在多台服务器上，要在每台服务器分别为每一员工建立一个账户（共  $M*N$ ），用户则需要在每台服务器上（共  $M$  台）登录



# 域的好处-简化管理使之更加清晰

- 服务器和用户的计算机都在同一个域中，用户在域中只要拥有一个账号
- 用户只需要在域中拥有一个域账户，只需要在域中登录一次就可以访问域中的资源了。



## 增强安全性

- 活动目录集成了登录身份验证以及目录对象的访问控制
- 管理员可以管理分散在网络各处的目录数据
- 经过授权的用户才可访问网络各处的资源
- 活动目录通过对象访问控制列表及用户凭据保护其存储的用户账户和组信息

## 具有扩展性和可伸缩性

- 管理员可以在计划中增加新的对象类，定义新的对象类的属性
- 活动目录可包含一个或多个域，又可包含一个或多个域控制器，以便根据网络需要调整目录规模
- 多个域可以组成域树，多个域树又可以组成为域林

# 智能的信息复制能力

- 使用多主机复制，允许用户在任何域控制器上而不是单个主域控制器上更新目录-容错
- 在域控制器上创建或修改目录信息后，发送到域中的所有域控制器上-总是最新
- 活动目录其它优势
  - 与DNS紧密集成
  - 与其它目录服务具有互操作性
  - 信息查询更加灵活

# AD DS结构

- 逻辑结构

- 域
- OU
- 域树
- 域林

- 物理结构

- 站点
- 域控制器



# AD DS对象与组件

- 默认容器
  - Builtin
  - Computers
  - Domain Controllers
  - Users
- 容器的对象



# Active Directory复制与信任关系

- 全局编目(所承担的目录角色)
  - 查找对象
  - 提供用户身份验证
  - 在多域的环境下提供通用组的成员身份信息
  - 查看是否DC=GC
- 复制
- 域与域之间的信任关系

# Windows server2008目录服务的改进

- 功能增强的DCPROMO命令
- 安全有效的只读域控制器(RODC)
- 可重启的目录服务
- ADSI服务界面编辑器
- 精准的密码策略(颗粒化)
- 管理员角色分离
- AD DS审核
- 支持 server core

# 本章操作重点

- 建立第1个域
- 计算机在域内和域外的角色
- 将独立服务器加入域
- 将Windows XP加入域
- 退出域和DC降级
- 林与域功能级别

# 建立域

- 在微软的企业网络架构里,『域』占有举足轻重的地位,可以说Windows Server 2008的重要功能都建立在域上。
- 安装活动目录前的规划
  - 文件系统和网络协议的准备
  - 规划域的结构(DNS必须设计为静态IP)
  - 确定域名

# 建立第1个域

- 具体来说,建立第1个域就是要建立第1部域控制器 ( Domain Controller,以下简称为DC )。
- 而建立DC的第1个动作就是执行Dcpromo.exe
  - - 但是必须具有系统管理员权限才能执行此程序,因此务必先以具有系统管理员权限的用户帐户登入。

# 建立第一部DC

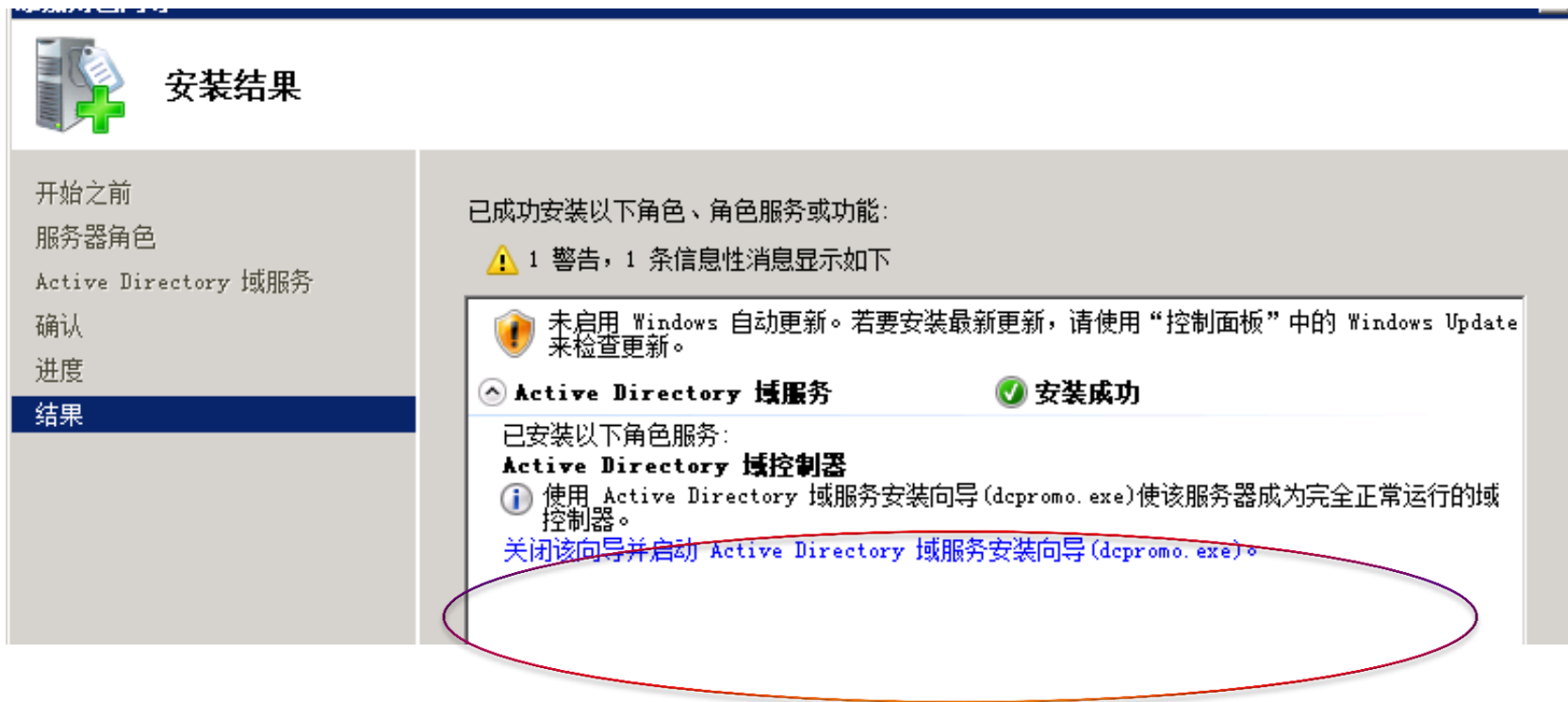
- 以下的示范步骤,系假设目前的网络无任何域,所  
要建立的是整个网络的第一个域 - - 又称为根域  
( Root Domain )。

## 『新增角色』并未建立DC

- 安装Windows Server 2008后,启动时预设会自动开启初始化设定工作视窗,虽然可以在此窗口中点选新增角色,接着选取安装Active Directory域服务,以使该计算机扮演DC角色。
- 然而,这种作法并未真正建立DC,到了最后一个画面还是要求必须执行Dcpromo.exe,如下图。



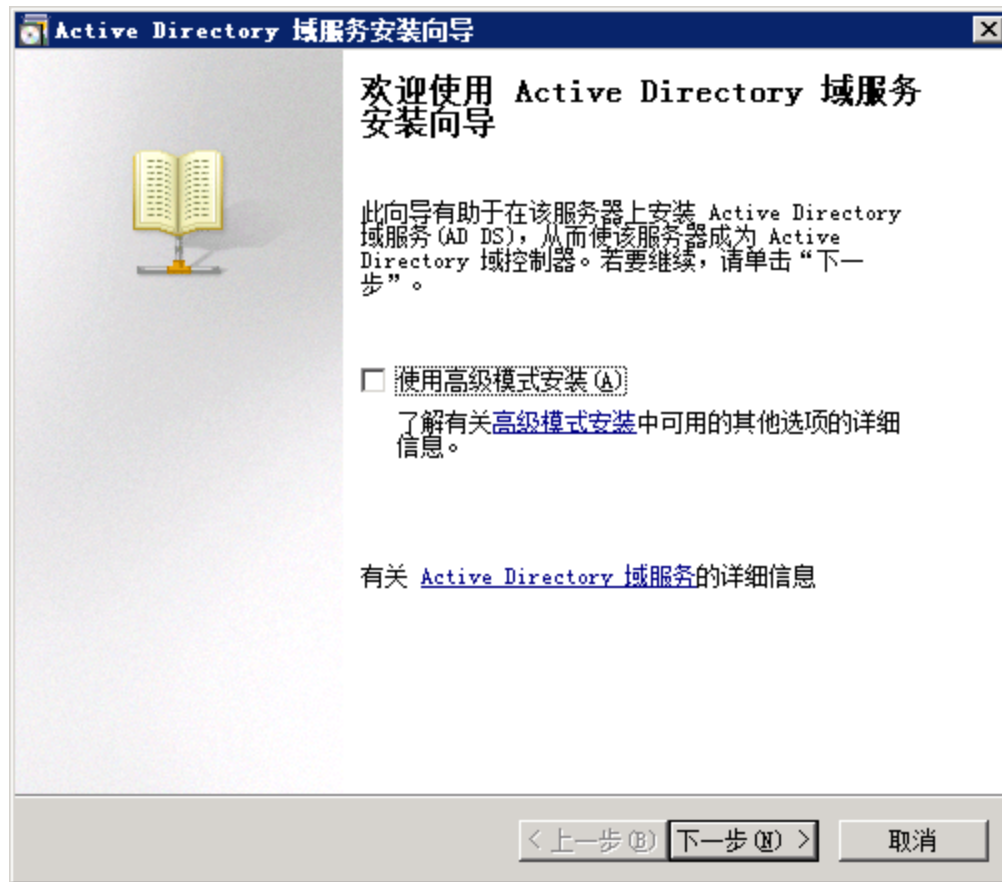
# 『新增角色』并未建立DC



- 所以我们也可无须使用新增角色功能,直接执行 Dcpromo.exe

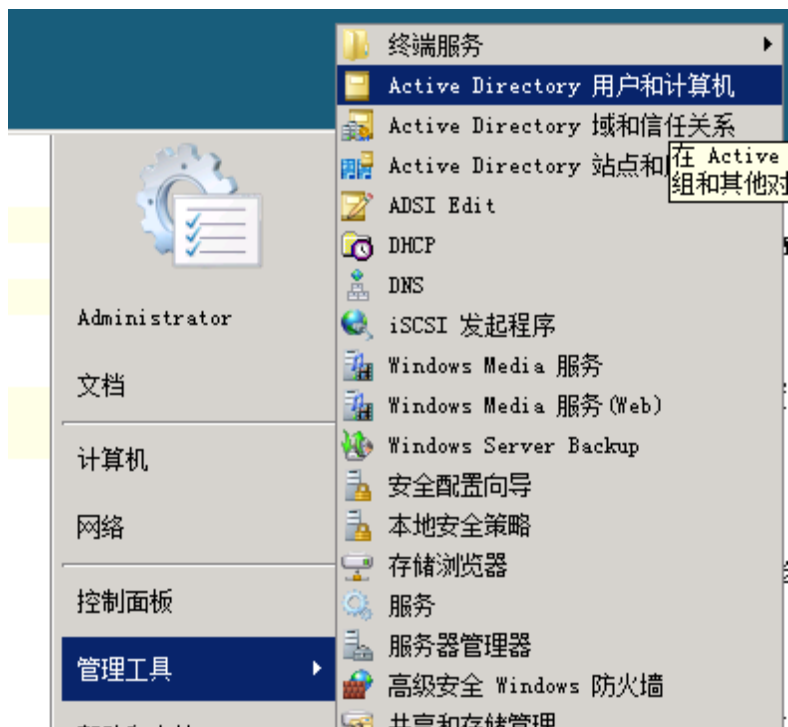
# 执行Dcpromo.exe

- 请按开始钮,输入"dcpromo"、按Enter键：



# 执行Dcpromo.exe

- 之后按完成钮,再按立即重新启动钮。
- 重新启动后若要确认此计算机是否已经是DC,从『开始/系统管理工具』菜单是否出现关于Active Directory的命令即可得知：



# 执行Dcpromo.exe

- 安装角色步骤中所设的密码,适用于当AD数据库毁损时,可在开机启动Windows Server 2008之前按F8键,进入目录服务还原模式,重建AD数据库。
- 由于此重建动作会改变既有的AD资料,为防止滥用,因此必须以密码保护,而且此密码不必和域系统管理员的密码相同。

# 计算机在域内和域外的角色

- 同一部计算机会因为加入域或退出域,而扮演不同的角色。
- 在大多数的技术文件中,对这些角色都有固定的称呼,后面将介绍它们的名称与功能。

# 域中的计算机

- 除了域控制器之外,域中的计算机还可区分成以下两类：
  - 成员服务器 ( Member Server )
  - 工作站 ( Workstation )

# 成员服务器

- 安装Windows Server 2008、Windows Server 2003 / 2003 R2、Windows 2000 Server等系统,加入了域、但不是DC的计算机。
- 或是安装Windows NT Server系统,且加入域的电脑,都算是成员服务器。
- 依据提供不同的服务,成员服务器通常还有不同的称呼,例如：文件服务器、应用程序服务器或数据库服务器等等。



# 成员服务器

- 由于这些服务器都是域的成员,所以审核使用者身份的工作,都交由DC执行,使用者只要通过DC的身份验证,即可依据设定的权限来使用服务器所提供的服务。
- 换言之,成员服务器都信任DC的身份验证。

## 最好停用成员服务器的本机账户

- 虽然加入了域,但是成员服务器上仍保留本机的帐户数据库,因此使用者仍可利用这些本机帐户,登入该服务器。
- 对域的安全管理而言,这些本机账户可能会是漏洞,所以我们建议停用成员服务器的本机帐户,强迫使用者一律以域账户登入。

# 工作站

- 所有安装以下作业系统,而且加入域的计算机都算是工作站：
  - Windows NT Workstation
  - Windows 2000 Professional
  - Windows XP Professional
  - Windows Vista商用入门版、商用进阶版和旗舰版
  - Windows 7

# 工作站

- 使用者可利用这些工作站登陆域,存取域中的资源、执行应用程序等等,但是Windows Server 2008的某些新功能,必须搭配Windows 7的工作站才能发挥效果。
- 而工作站本身仍然保留了本机帐户的数据库,使用者利用本机账户登入工作站时,只能使用本机（该工作站）的资源,但无法存取域上的资源。

# 域外的计算机

- 首先,应该要知道哪些计算机不能加入AD域?
- 执行Linux、Unix等等非Windows系统的电脑,不能加入AD域。
- 此外, Windows 95 / 98 / Me、Windows XP家用版、Windows Vista家用入门版、Windows Vista家用进阶版以及Win7的Home版,也都没有加入域的功能。

# 域外的计算机

- 即使具有加入域功能,也未必要加入域。
- 因此,无论该计算机是不能或不想加入域,统统归类为域外的计算机。
- 从功能面来看,域外的计算机也可概分为两类：
  - 独立服务器 ( Stand-alone Server )
  - 客户端计算机 ( Client )

# 域外的计算机

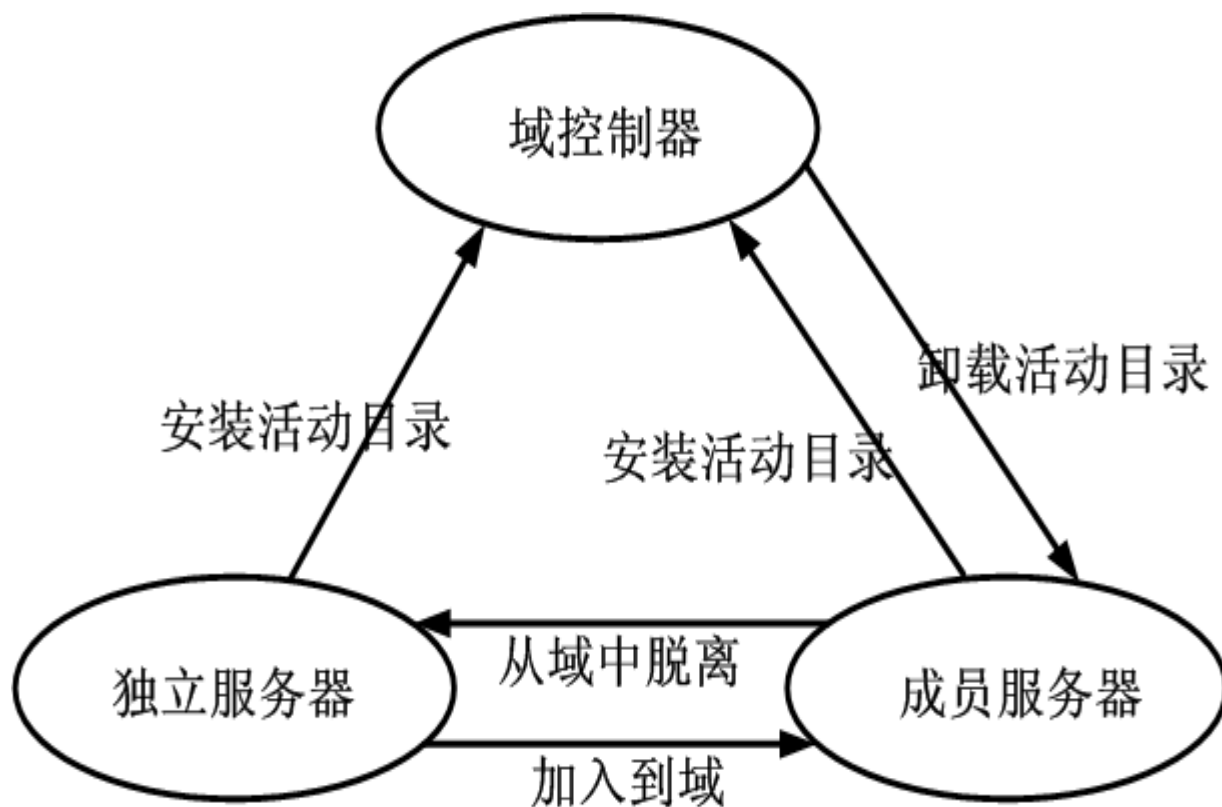
- 虽然在域之外,但使用者只要拥有合法的域帐户,仍可利用这些计算机存取域中的资源。
- 不过每次存取不同计算机上的资源时,皆须输入域的帐户名称与密码,而且由于这些计算机并未受到域的管制,也容易变成信息安全的漏洞。



# 独立服务器

- 简单地说,未加入域的服务器就是『独立服务器』
  - - 无论安装的是Windows或非Windows的服务器操作系统。
- 它一旦加入域后,角色即转换为『成员服务器』。
- 相反地,『成员服务器』如果退出域,则又成为『独立服务器』。如果在『独立服务器』上执行Dcpromo.exe,则可升级为DC。

# 独立服务器



# 客户端计算机

- 无论是执行何种作业系统,只要未加入域,而且不是独立服务器的电脑,都可以归为此类。
- 使用者虽然不能用它们登入域,但仍可利用域帐户,透过这些计算机存取域资源。

# 将独立服务器加入域

- 建立域之后,通常会优先将网络上的独立服务器加入域,以便集中管理。
- 以下示范将Windows Server 2008独立服务器加入域的步骤（此步骤亦适用于Windows 7）。

# 1.修改『首先DNS服务器』的设定

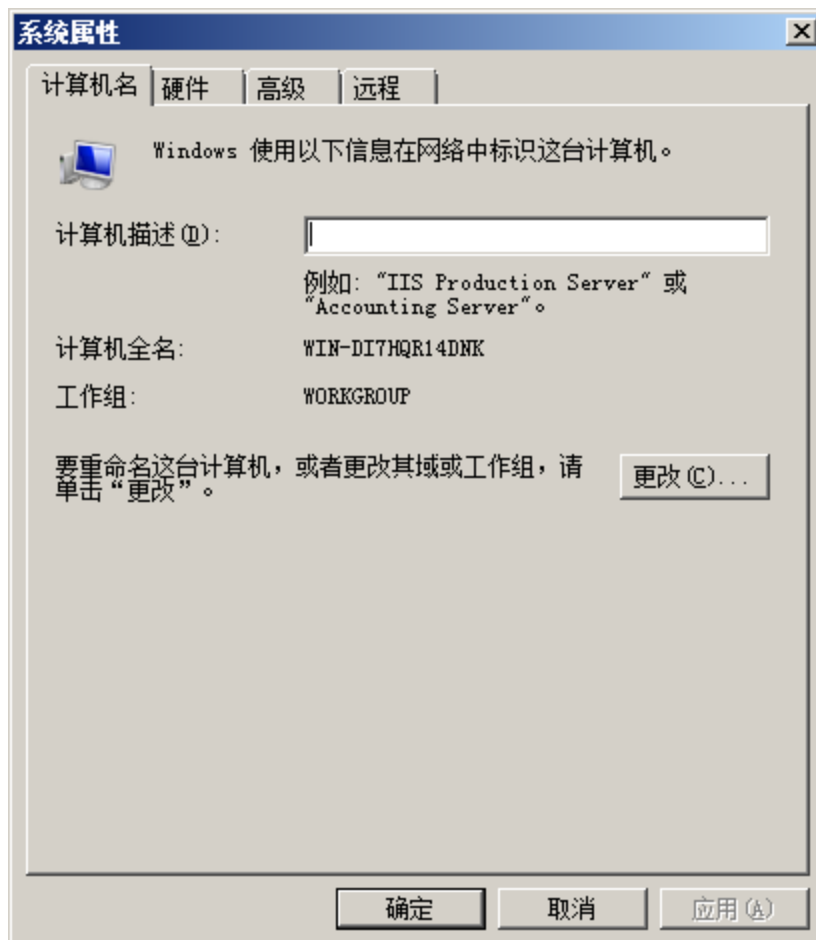
- 加入域的先决条件是要能够连结到该域的DC,而要连到DC就必须先设定正确的DNS服务器地址。
- 先前建立DC的时候,其实已经将该域的DNS服务器和DC安装在一起了。
- 换言之,域里的DC和DNS服务器实为同一部电脑,所以应该将独立服务器上的首先DNS服务器,设为DC的IP地址。

## 修改『首先DNS服务器』的设定

- 首先以该独立服务器的本机系统管理员身分登入本机
- 定义好本机的名称(重启)
- 设置好固定的同一网段的IP地址
- 确定DNS地址

## 2.修改『成员隶属』的设定

- 请按开始钮,在电脑项目上按右键、执行『内容』命令：





# 修改『成员隶属』的设定

- 加入域后的电脑,其名称预设会出现在DC的Active Directory使用者和电脑窗口的Computers容器中：



這是加入網域的電腦

選取 Computers 容器

# demo

- 实验 Windows Server 2008之AD DS 活动目录安装的详细部署步骤

MICROSOFT OFFICIAL COURSE

# MCITP-活动目录(2)

- 退域和删除域
- 创建子域和额外域控制器

# 退出域和DC降级

- 先前已经介绍了客户端加入域的方法,这一节将继续说明退出域和DC降级的方法。
  - 退出域
  - DC降级

# 退出域

- 将成员服务器退出域,也就是让该服务器重新转变为起初的独立服务器,以下示范将Windows Server 2008成员服务器退出域的步骤。
- 请先以域或本机系统管理员的身分登入域或本机,参考前文开启系统属性窗口,按计算机名称变更钮
- 接着选择工作组确定钮,再按关闭钮,最后按立刻重新开机钮重新启动,启动后此计算机便成为工作组的成员,使用者必须用服务器上的本机账户才能登陆,必须让域管理员事先开启。

# DC降级

- 要将DC降级,首先以域系统管理员的用户帐户登入,然后按开始钮,输入"dcpromo"、按Enter键,接着按下下一步钮：



# DC降级注意

- 若域中仍有其它DC存在,则重新启动后的计算机便担任『成员服务器』,仍可用域账户登入域或本机。
- 如果域内唯一的DC遭降级后,使得域不复存在,则它会变成『独立服务器』,不能用域账户登入本机,而必须改用本机账户登入本机。
- 如果该域控制器是全局编录,降级后将不再扮演全局编录角色,因此要先确定网络上是否还有其它全局编录,如果没有需先指派,否则影响所有用户登录。

# 创建子域

- 子域是名称空间树种直接位于另一个域(父域)下面的一个DNS域，新子域的名称将包含父域的全名。
- 必须先成为域成员，并且需以域管理员或域企业管理员用户组成员登录，否则将会被提示无权
- 系统版本需为windows 2000 server版以上
- 正确配置DNS地址



# 添加额外域控制器

- 额外域控制器优势
  - 提高用户登录效率
  - 提供容错功能
  - 不用备份活动目录
- 注意升级后本机账户和密码将被删除，应事先备份。已被加密的数据也将无法读取，应当事先解密并备份。

# demo

- 实验 Windows Server 2008之AD DS 活动目录卸载的详细部署步骤

MICROSOFT OFFICIAL COURSE

# MCITP-活动目录(3)

- 林和域的功能级别
- AD目录服务

## 本章重点

- 目录服务的基本概念
- 目录的架构
- X.500和LDAP
- AD目录服务
- AD对象的名称

# 何谓『应用程序分区』？

- 应用程序分区(Application Directory Partition)是指存在于AD数据库的某一类资料,由应用程序或服务所产生,可以由人工或应用程序指定仅复写到特定的DC,而非所有的DC。
- 由于此一特性,我们会将比较常变动的数据设为此类,以避免稍一变动就使所有DC都忙于复写。

# 何谓『应用程序分区』？

- 例如：若DC兼任DNS服务器,便会存在DNS的应用程序分区,而这份资料只会复写到也是兼任DNS服务器的DC。
- 当DC降级时,通常应删除应用程序分区,才能恢复到升级前的状态。

# 林与域功能级别

- 在升级为DC的过程,曾遇到选择『林功能级别』( Forest Functional Level ) 和『域功能级别』( Domain FunctionalLevel ) 的对话框,当时都暂时采用默认值。
- 究竟不同的功能级别有何差异? 该如何做最适当的选择?

# 功能级别的种类与高低

- Windows Server 2008提供的林功能级别有『Windows 2000』、『Windows Server 2003』和『Windows Server 2008』等3种。
- 域功能级别则有『Windows 2000混合』、『Windows Server 2003』和『Windows Server 2008』等3种。



# 功能级别的种类与高低

- 愈新的操作系统代表愈高的功能级别,因此 Windows Server 2008的等级最高; Windows Server 2003次之; Windows2000 (混合)模式的等级最低。
- 在选择林和域功能级别时,要注意域功能级别不能低于林功能级别。
- 假设林功能级别为『Windows Server 2003』, 则域功能级别就只有『Windows Server 2003』和『Windows Serer 2008』可选。

# 功能级别的种类与高低

- 若林功能级别为『Windows Server 2008』,则域功能级别就一定是『Windows Serer 2008』。
- 林和域功能级别的默认值都是最低等级（ Windows 2000和Windows 2000原生 ）,这是为了有最大的兼容性。
- 若要林和域支持最多的功能,应在符合限制条件下尽量选择最高等级。

# 不同功能级别的影响

- 选择不同的功能级别,对于林或域会造成以下的影响：
  - 哪些DC可以加入林或域：虽然都是DC,但是所执行的操作系统可能是Windows 2000、Windows 2003或Windows 2008,因此在不同的功能级别会限制某些DC不能加入林或域。
  - 林或域支持哪些功能：在不同的功能级别,林或域所支持的功能也有差异。
  - 功能级别愈高,所支持的功能愈多。

# 不同功能级别所导致的功能差异

- 不同林功能级别的主要功能差异如下表：

樹系功能等級	主要功能差異
Windows 2000	支援 AD DS 預設的功能
Windows Server 2003	除了支援 AD DS 預設的功能，還包括以下功能： <ul style="list-style-type: none"><li>■ 樹系信任（Forest Trust）</li><li>■ 網域更名（Domain Rename）</li><li>■ 部署 RODC（請參考第 6 章）</li></ul>
Windows Server 2008	與 Windows Server 2003 相同。後續加入此樹系的網域預設採用 Windows Server 2008 網域功能等級

# 不同功能级别所导致的功能差异

- 不同域功能级别的限制条件与功能差异如下表：

網域功能等級	主要功能差異
Windows 2000 原生	<ul style="list-style-type: none"><li>■ 支援 AD DS 預設的功能</li><li>■ 萬用群組 (Universal Group)</li><li>■ 巢狀群組 (Group Nesting)</li><li>■ 群組類型轉換 (Group Conversion)</li><li>■ SID 歷程紀錄 (SID history)</li></ul>
Windows Server 2003	<p>除了具有 Windows 2000 原生的功能外, 還包括以下功能：</p> <ul style="list-style-type: none"><li>■ 限制委派 (Forest Trust)</li><li>■ DC 更名 (Domain Controller Rename)</li><li>■ 部署 RODC (請參考第 6 章)</li></ul>
Windows Server 2008	<p>除了具有 Windows Server 2003 的功能外, 還包括以下功能：</p> <ul style="list-style-type: none"><li>■ DFS 複寫時會包括系統磁碟區的檔案</li><li>■ 支援協定的進階加密功能, 包括 AES 128 和 AES 256</li><li>■ 對於使用者和通用安全性群組, 有更多的密碼原則可供設定</li></ul>

## 变更林或域功能级别

- 建立第一个林的第一部DC时,因为只有自己一部DC,所以选择林功能级别或域功能级别时都没有任何限制,通常先采用预设值,将来再视需求来变更。
- 以下说明变更林和域功能级别时的注意事项与步骤。

# 变更功能级别时的注意事项

- 当林或域内的DC不只一部时,要变更林或域功能级别时,就必须注意以下事项：
  - 若林功能级别是Windows 2008,则只有执行Windows Server 2008的DC可加入此林。
  - 若林功能级别是Windows 2003,则只有执行Windows Server 2008或Windows Server 2003的DC可加入此林。
  - 若域功能级别是Windows 2008,则只有执行Windows Server 2008的DC可加入此域。

# 变更功能级别时的注意事项

- 若域功能级别是Windows 2003,则只有执行Windows Server 2008或Windows Server 2003的DC可加入此域。
- 此外,还要知道：无论是林功能级别或域功能级别,都只能提升、不能调降！所以一旦提升之后,就不能降为原先的等级。
- 而且必须是Enterprise Admin群组的成员才能变更林功能级别；必须是Domain Admin群组的成员才能变更域功能级别。



## 变更林功能级别

- 请以隶属于Enterprise Admin群组的用户帐户登入,而后执行『开始/系统管理工具/ Active Directory域及信任』命令,点击右键。

## 变更域功能级别

- 请以隶属于Domain Admin群组的使用者账户登入,而后执行『开始/系统管理工具/ Active Directory域及信任』命令,点击右键。

# 目录服务

- 微软在2000年开始推出的目录服务,可以说是新、旧技术的分水岭。
- 从Windows 2000 Server、Windows Server2003、2003 R2,直到Windows Server 2008,许多重要的功能都与目录服务相关。
- 所以我们先来了解目录服务的相关知识,为后面的学习打好基础。

# 目录服务的基本观念

- 何谓目录
- 目录与数据库的差异
- 何谓目录服务
- 计算机网络为何需要目录服务

# 何谓目录

- 其实目录早已存在日常生活中,例如电话簿可用来查询用户的电话号码、姓名与地址,就是一种目录。
- 而计算机的文件系统记录了文件夹与档案的名称、建立日期、修改日期、储存位置等等资讯,因此使用者以文件名或某种文件属性(例如：修改日期),就能从众多的文件夹中找出所要的档案。

# 何谓目录

- 从以上的例子可知,目录是用来记载特定环境中、一群对象的相关信息。
- 在此所谓的对象,泛指环境中的各种独立个体 - 包括人、事、物。

# 目录与数据库的差异

- 许多初次接触目录或目录服务的使用者,经常产生一个问题：「目录与数据库有何差异？」
- 其实,目录与数据库都是用来储存资料,两者的确很相似。
- 不过,深入比较其细节,就会发现通常有以下两点差异：
  - 目录强调查询,数据库重视异动。
  - 目录对于查询动作做过优化,因此查询的速度很快,适合处理变动少、查询多的数据。

# 目录与数据库的差异

- 数据库则是重视异动（ Transaction ），适合处理变动较多的数据。
- 目录以树状架构为主，数据库以关系型数据表为主。
- 绝大多数的目录都采用阶层式树状架构来储存数据；至于资料库,虽然也有少数采用树状架构,但是主流产品是『关系型数据库』,其主要架构为『存在关联性的数据表』。



# 目录与数据库的差异

- 虽然目录与数据库有以上的差异,可是在许多文件或人们平常的交谈中,经常将两者混淆,几乎视为相同。
- 所以,我们也毋须太计较其中的差异,不妨将目录当成是一种查询速度很快的数据库即可。

# 何谓目录服务

- 有了目录之后,理论上就可以用来查询所要的信息。但是当这份目录包含庞大的数据时,用人工查询和维护便显得没有效率。
- 翻阅厚厚的电话簿时很不方便,但是透过查号台,利用计算机来搜寻电话用户数据库,便能快速又准确地知道结果,所以查号台的服务便是一种目录服务。
- 简而言之,即由目录服务,我们能够方便迅速地查询与维护目录,提高工作效率。

# 计算机网络为何需要目录服务

- 在单机时代,档案、打印机、扫描仪和调制解调器等等,都是在一部电脑,使用者能轻易地找到这些资源,因此感受不到目录服务的重要。
- 可是到了网络时代,这些资源可能散布在5部或10部计算机上,使用者如何找得到?即使找到了,是否就有权限使用?
- 倘若读取每一个档案或使用每一部打印机时,都得重复输入账户名称与密码,岂不是很麻烦?

# 计算机网络为何需要目录服务

- 为了解决这些因为网络规模膨胀而出现的问题,我们需要一份目录,上头记载着计算机名称、打印机名称、帐户名称、密码、权限等等,再设计一种好用的目录服务,让大家透过该目录服务就能轻易地使用网络资源。
- 不过在实务应用上,考虑到信息安全,因此软件厂商所设计的目录服务,大都还会结合身分验证 ( Authentication ) 机制。

# 计算机网络为何需要目录服务

- 亦即在使用目录服务之前,必须表明自己的身分,通常是输入账户名称与密码,但也可以用插入IC卡或是扫描指纹等等方式,待系统验证无误后,用户才能查询或修改目录内容。

# 目录的架构

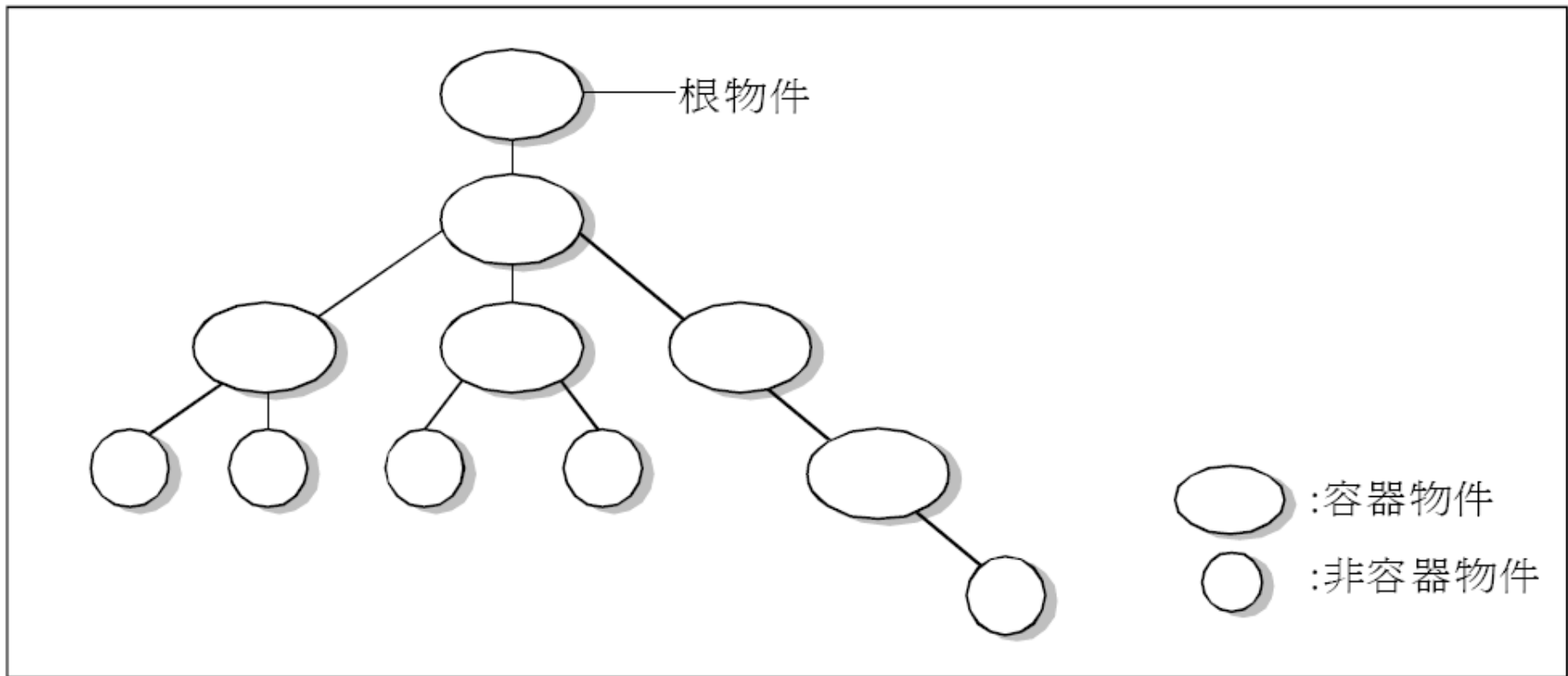
- 目录的架构是指在目录中储存对象的方式,明白这方面的知识,有助于未来的维护和设计工作。
  - 目录树
  - 对象的属性

# 目录树

- 若目录中的对象是以『阶层式树状架构』来组织, 则该架构称为『目录树』(Directory Tree), 包含以下两类的对象：
  - 容器对象(Container Object)：这类对象的下层可再存放其他对象。位于整个目录树顶端的容器对象, 称为『根』对象(Root Object)。
  - 非容器对象(Non-container Object)：这类对象的下层不可再存放其他对象。非容器对象必定是位于目录树的末端, 又称为『叶』对象(Leaf Object)。

# 目录树

- 整体的架构图如下：



目錄樹的階層式架構



# 对象的属性

- 在目录树中,各对象都有所谓的『属性』(Attribute),记载着该对象的特性。对象与属性的关系,类似于数据库中纪录与字段的关系。
- 一笔纪录可以有多个栏位,同理,一个对象可以有多个属性,而且不同性质的对象会有不同的属性。
- 举例来说：使用者（User）对象有『公司名称』『部门名称』和『电话号码』这些属性,但是文件夹对象就没有这些属性,而有『建立日期』和『大小』等属性。

# 对象的属性

- 属性的内容通常称为属性值,不同对象的某些属性值可以相同、某些则必须唯一。
- 例如：A、B两位使用者隶属于相同部门,所以它们的公司名称、部门名称,甚至电话号码都相同,但是『员工编号』就绝对不能相同。

# X.500和LDAP

- 由于计算机网络可能包含了多种不同的作业系统,当我们要用一种目录服务将它们整合在一起时,如果没有统一的标准,就必须为每一个系统设计专属的客户端软体,如此势必增加复杂度与成本。
- 当初在『目录』观念刚萌芽时, ITU-T发表了一系列名为『X.500 Recommendation』文件,探讨目录的观念、模型、存取协议等等技术。

## X.500和LDAP

- 业界便以X.500作为目录的标准,以DAP (Directory Access Protocol)协议作为存取X.500目录的共同方式。
- 但是厂商在实作时,发觉DAP协定过于复杂,而且客户端程序的负荷太大,于是将其改良,推出了LDAP (Lightweight Directory Access Protocol)协定。

## X.500和LDAP

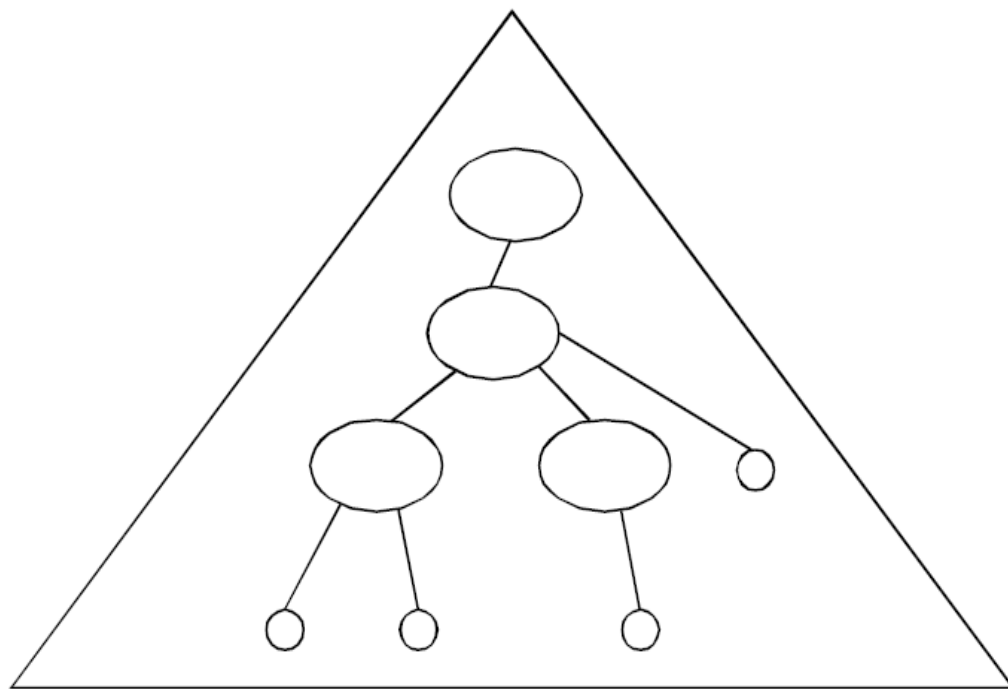
- 顾名思义, LDAP为『轻量级』(Lightweight)的DAP,一方面简化架构、易于设计,另一方面也减轻客户端软件的负荷,因此成为主流。
- Lotus Domino、Sun One Directory Server、Novell Directory Services (NDS)和微软的Active Directory Services等等目录服务产品,都标榜支持LDAP协定。

# AD目录服务

- 微软自Windows 2000 Server开始提供完整的目录服务,命名为AD ( ActiveDirectory ) 目录服务。
- 搭配该服务的目录便称为AD目录 - - 许多文件是以『AD数据库』来称呼AD目录。
- 虽然AD目录与AD目录服务大致上符合X.500及LDAP规范,但是难免加入了微软独家的规格与技术,因此本节将介绍其中比较值得注意的一些特性。

# AD目录的架构

- AD目录仍然是以对象组合成阶层式树状架构,不过却多了『域』( Domain )对象。
- 将一般对象先整合到网
- 域中,再形成所谓的
- 『域树』
- ( Domain Tree ),
- 如右图 :



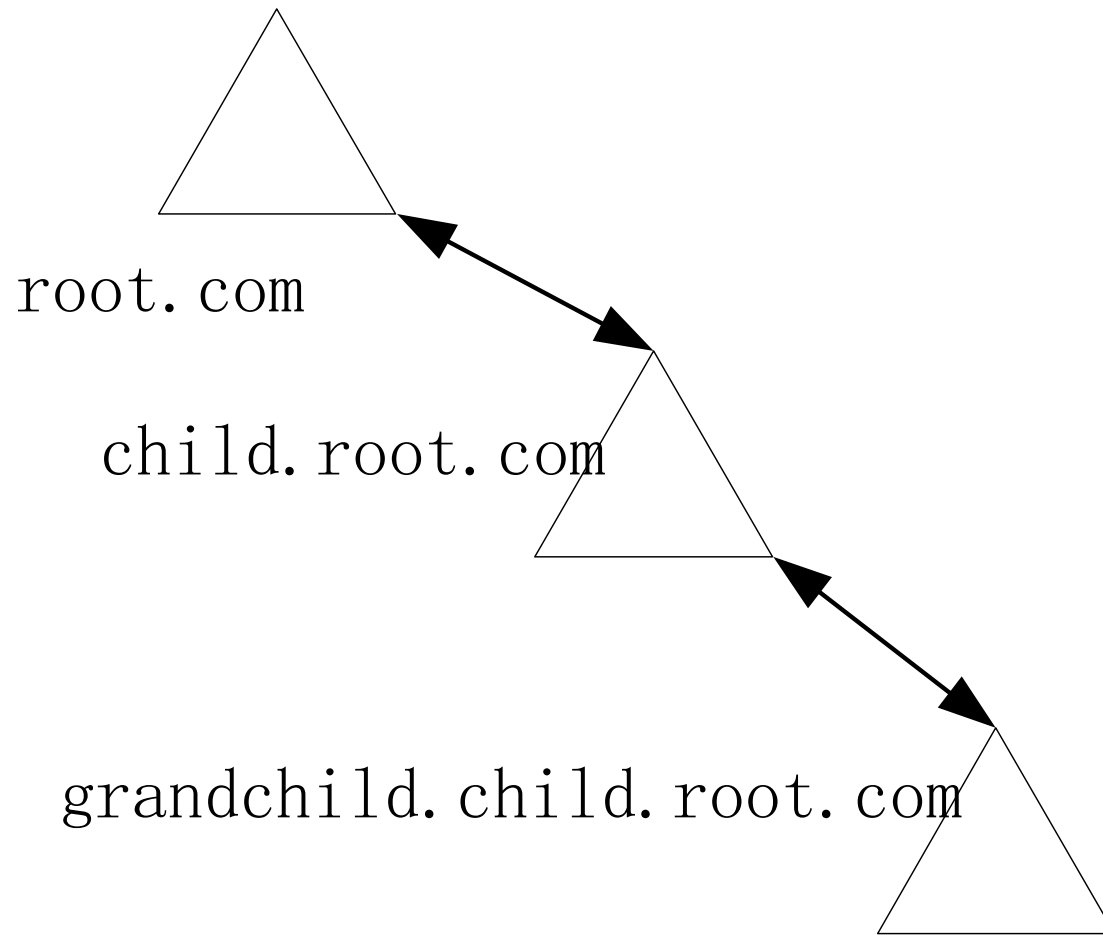
△：網域    ○：容器物件    ○：非容器物件

# AD目录的架构

- 其实域树与先前提过的目录树很像,只不过多了域这个容器对象。各个对象先隶属于域,再由域组合成目录。
- 而且多个域树还可以再结合成『林』 ( Forest ), 如下图。



# AD目录的架构



# AD对象的共同特性

- 在AD目录中的对象称为AD对象。虽然大多数AD对象的特性各不相同,但是却有一些共同点。
- 认识这些共同的特性,可让我们更深入地了解AD对象。

# GUID

- Windows Server 2008会赋予各对象一个独一无二的代码,称为GUID(Globally Unique Identifier,全局唯一识别元)。
- GUID的长度高达128位,以确保不会彼此重复。
- 对象的GUID一旦产生,永远不会改变,因此不论对象的名称或属性如何变更,应用程序仍可透过GUID找到对象。

# ACL

- 从Windows 2000 Server到Windows Server 2008,都存在所谓的安全策略(Security Principal)对象,它包含『用户帐户、计算机帐户与群组』等3种对象。
- 而AD对象都有一份列表(List),记载着安全策略对象对自己有哪些权限,这份清单称为访问控制列表(ACL, Access Control List)。
- 换言之, ACL记载了『哪些安全策略对象,可以对哪些对象做什么动作』——访问控制列表

# ACL

- 例如：『王小华』可以读取『人事部门』文件夹、但不能删除或修改其内容；『美编组』的成员可以使用彩色打印机、但不能修改设定等等。
- 我们不妨将对象的ACL想象成如下的表格：

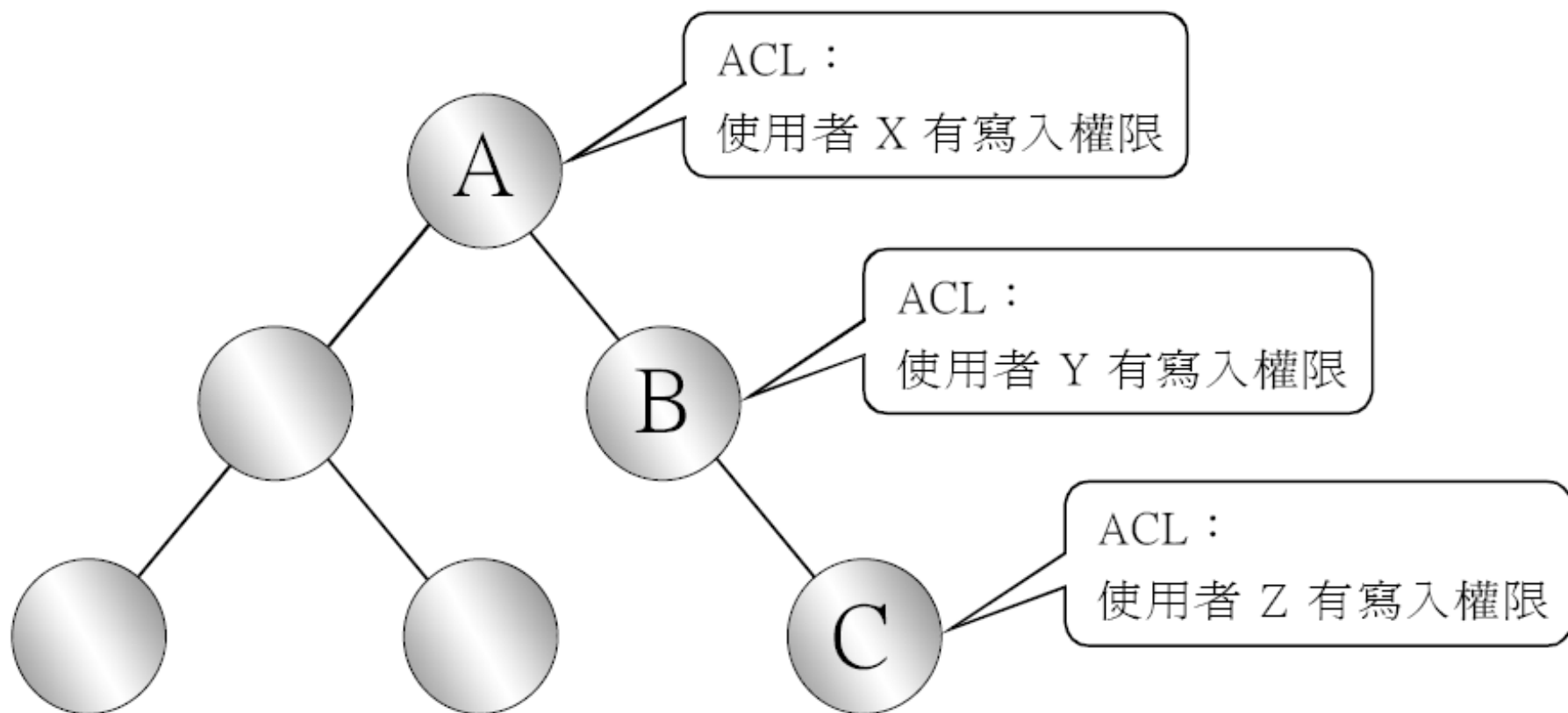
安全性原則物件	權限
系統管理員	完全控制
王小華	寫入與讀取
美編組	讀取

# ACL

- 当然,以上的内容系经过简化,目的是要让读者容易理解。实际的ACL是用一堆代码来记录,远比上表来得复杂。

# ACL的继承关系

- 虽然AD对象各自拥有一份独立的ACL,然而系统管理员可以根据实际需求,决定是否让下层对象继承上层对象的ACL。以下图为例：

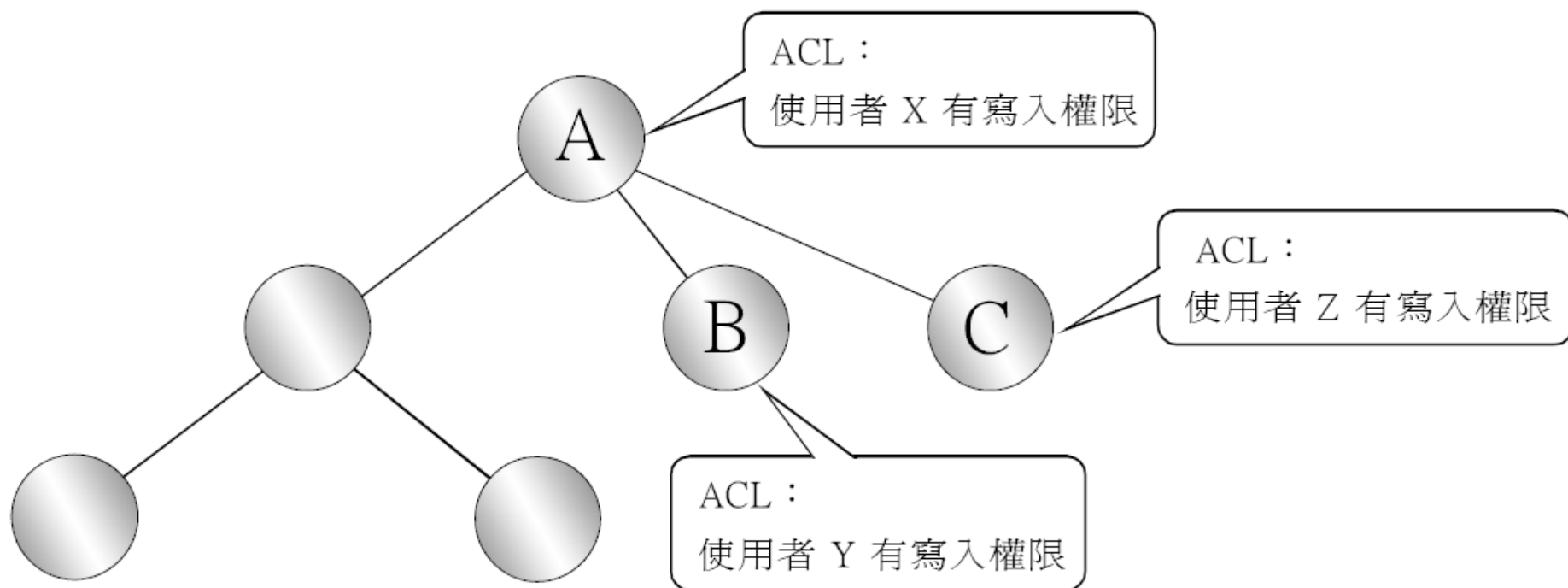


# ACL的继承关系

- 当C对象继承上层对象（A和B对象）的ACL时,连带使得X和Y使用者都对C对象具有写入权限,造成X、Y和Z三位使用者都对C对象有写入权限。
- 若将C对象移动至其它位置时,本身的ACL并未改变,但因所继承的ACL不同会导致不同的结果。
- 以下图为例：



# ACL的继承关系



- 将C对象移至A对象下层后,则只有X、Z使用者对C对象具有写入权限, Y使用者则丧失对C对象的写入权限。

# AD对象的属性

- AD对象的主要功能是记载AD域内各种资源的资讯,这些信息便是对象的属性。
- 每个AD对象通常有多个属性,以使用者 ( User ) 对象为例,预设有两百多个属性,较常用到的属性如下：
  - sn：使用者的姓。
  - givenName：使用者的名字。
  - userPassword：用户的密码。
  - objectGUID：使用者的GUID。

# AD对象的属性

- lastLogon : 使用者最近一次的登入时间。
  - userCertificate : 使用者的数字证书。
  - url : 使用者的个人网址。
  - homePhone : 用户家中的电话号码。
  - thumbnailPhoto : 使用者的数码相片。
- 在实际的应用上,通常不会用到所有的属性,而是依需求来存取部份的属性,因此用户仅能存取应用程序所提供的属性。

# AD对象的属性

- 例如：Windows Server 2008的用户帐户管理界面,并没有出现thumbnailPhoto属性可供设定。
- 倘若有储存使用者相片档的需求,则必须另行撰写程序,提供该属性的设定选项,让操作者能将相片文件储存在用户对象中。

# AD Schema

- 先前提过,不同类的AD对象可能具有不同的属性,例如:打印机对象有『纸张尺寸』属性,但是用户对象就不可能有此属性。
- 到底什么样的对象具有哪些属性,这是由AD schema所决定。
- AD schema如同一份规格文件,将对象分成各种类别(Class),并定义每一种类别的对象该有哪些属性。

# AD Schema

- 透过这些已定义属性的对象类别来建立对象,可确保套用这个类别所产生的对象,皆有相同的属性。
- 例如：定义user类别所包含的属性之后,所有的用户对象都根据user类别来建立,如此所产生的用户对象便会有相同的属性。
- 在其它的目录服务中, schema经常是以文本文件的形式来呈现。

# AD Schema

- 但是在AD中,则将schema包装成AD对象,换言之,虽然AD schema本身是用来定义对象,可是自己也是一种对象,可以说是『用来定义对象』的对象。
- 在AD schema中,相同属性可以存在于不同类别,例如：description属性同时存在于user、group、computer等类别,而且彼此完全独立。

# AD Schema

- 修改user的description属性不会影响group对象的description属性。
- 虽然Windows Server 2008已经提供相当多的类别与属性,但为了提高AD功能的弹性,仍允许系统管理员自行定义新的类别或属性。



# AD对象的名称

- 由于用户或网络程序可能会以不同方式来存取对象,而每一种存取方式对于对象都有自己的命名方式,因此AD对象会有多种名称,以适用于不同的场合。

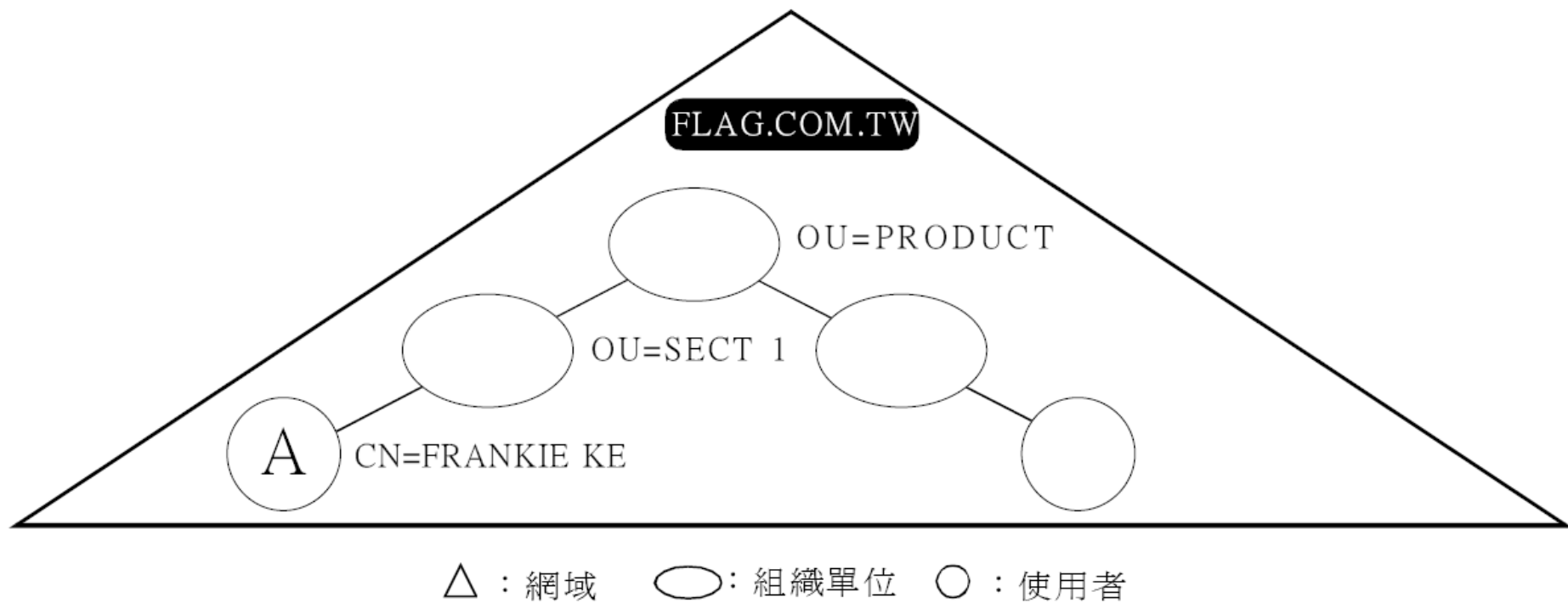
# LDAP名称

- AD是采用LDAP 3协议的目录服务,因此客户端可透过LDAP协定来存取AD中的对象。
- 存取时所指定的对象名称,可区分为以下2类：
  - DN (Distinguished Name)与RDN (Relative Distinguished Name)
  - 标准名称

# DN与RDN

- AD目录中各对象皆具有符合LDAP规格的DN与RDN名称,以便让LDAP客户端程序存取对象。
- 对象本身具有有一个RDN属性,用以记载自己的RDN ; 对象的DN则是由自己的RDN再加上层所有对象的RDN所组成,以下图为例。

# DN与RDN



- 对象A的RDN为： CN=FRANKIE

# DN与RDN

- DN为：

CN=FRANKIE,OU=SECT1,OU=PRODUCT,DC=FLAG,DC=COM,DC=TW

- 其中, CN (Common Name)通常用来代表对象名称,例如用户名称、打印机名称等等；OU (Organizational Unit)代表组织单位名称；DC (Domain Component)代表域名。
- 这里要注意我们首先的是DNS域名称,例如：flag.com.tw,但是LDAP则是用『DC=』加在每个域之前,形成『DC=flag, DC=com, DC=tw』的表示法。

# DN与RDN

- 对象的DN是由系统根据对象的RDN与其位置而自动产生的。移动对象时, DN也会随之变更,以反映移动后的位置。
- 除了程序设计师在开发程序时,会用到冗长难记的DN外,一般情形很少直接使用DN来存取对象。

# 标准名称

- 标准名称是以简化方式表示LDAP的DN,假设对象的DN为：

CN=FRANKIE,OU=SECT1,OU=PRODUCT,DC=FLAG,DC=COM,DC=TW

- 则在AD中此对象的标准名称为：

FLAG.COM.TW/PRODUCT/SECT1/FRANKIE

- 换言之,标准名称省略了DN中的"CN="、"OU="等等保留字,并改用DNS域名来表示DN中的域名。

# 登陆名称

- 使用者在登陆Windows Server 2008主机或域时,可使用以下两种名称：
  - UPN (User Principal Name)
  - SAM (Security Account Manager)账户名称



# UPN


- UPN的格式与首先的Email地址相似。
- 例如：frankie@xdom.com,其中frankie是使用者名称（一般又称为『账户名称』或『账号』），xdom.com是frankie所隶属的DNS域名。
- 开机启动Windows Server 2008后,首先出现请按CTRL + ALT + DELETE来登入的画面,使用者按下Ctrl +Alt +Del键,便可输入UPN来登入域,如下图。

Windows 安全

×

您的凭据不工作

之前用于连接到 192.168.12.139 的凭据无法工作。请输入新凭据。



Administrator



administrator@xdom.com

●●●●●●●●●●

域: xdom.com

☐ 记住我的凭据

☒ 登录没有成功

确定

取消

# UPN

- UPN虽然容易记忆,但是因为是在同一个域内不得重复,所以若存在成千上百个使用者时,如何为自己取一个好记、又不跟别人相同的名称,就成为让人头痛的问题。

# SAM账户名称

- 在Windows NT时代,使用一个名为SAM的档案来储存账户相关资讯,包括：用户名称、密码、允许登入的时段、失效日期等等,因此大家将SAM档所储存的使用者名称叫做『SAM账户名称』。
- 如今SAM账户名称之所以仍然存在,主要是为了与Windows NT相容。

# SAM账户名称

- 因为考虑到仍存在使用Windows NT的电脑,而这些计算机不认得UPN的格式,所以必须以『域名\使用者名称』的格式输入。
- 不过由于SAM账户名称并无阶层式的架构,因此同样容易发生名称重复的问题。

# 小结

- 就管理工作而言,比较常遇到的是UPN与SAM账户名称。其他名称主要提供系统内部或程序设计员使用,一般使用者则较少接触。
- 以下是本节介绍之数种对象名称的归纳表：

物件名稱	說明	範例
LDAP RDN	LDAP 相對識別名稱	CN=FRANKIE KE
LDAP DN	LDAP 識別名稱	CN=FRANKIE KE,OU=SECT1, OU=PRODUCT, DC=FLAG,DC=COM,DC=TW
標準名稱	物件在 AD 中的表示法	FLAG.COM.TW/PRODUCT/SECT1/FRANKIE KE
UPN	登入 AD 網域所用的名稱	<a href="mailto:frankie@flag.com.tw">frankie@flag.com.tw</a>
SAM 帳戶名稱	相容於 Windows NT 網域的登入名稱	frankie

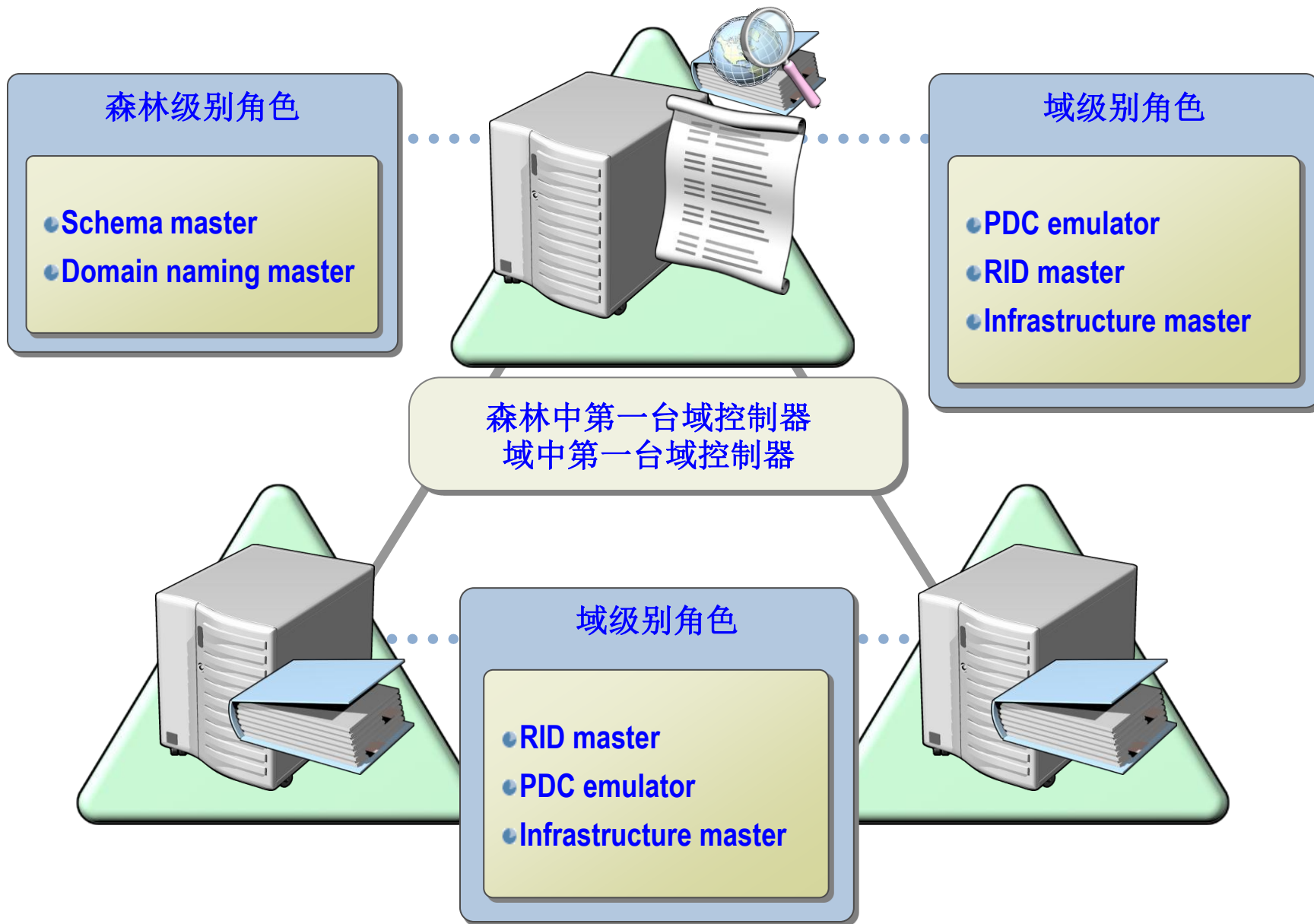
MICROSOFT OFFICIAL COURSE

# MCITP-活动目录(4)

- 操作主机角色
- 活动目录升级概述



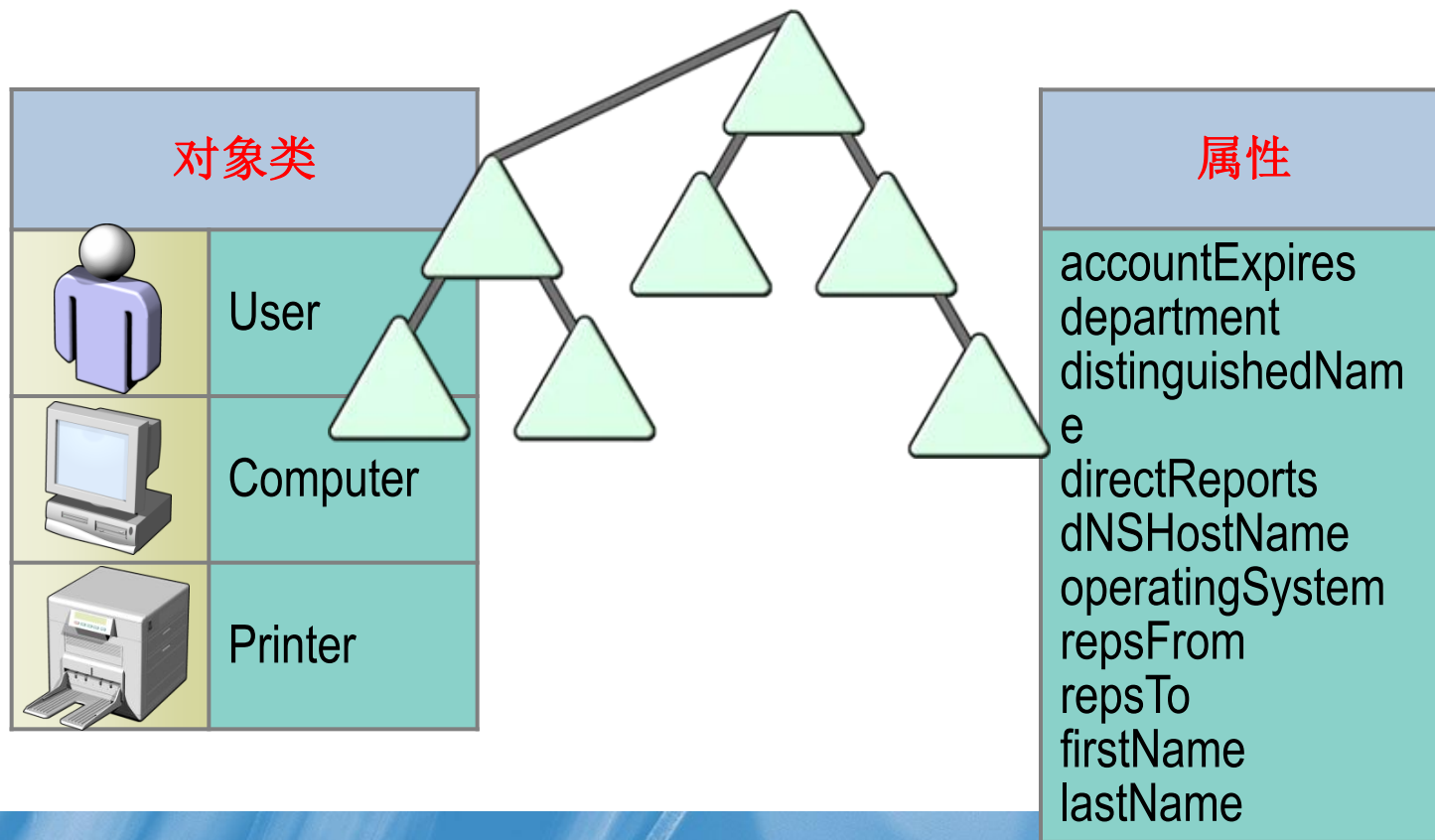
# 操作主机简介





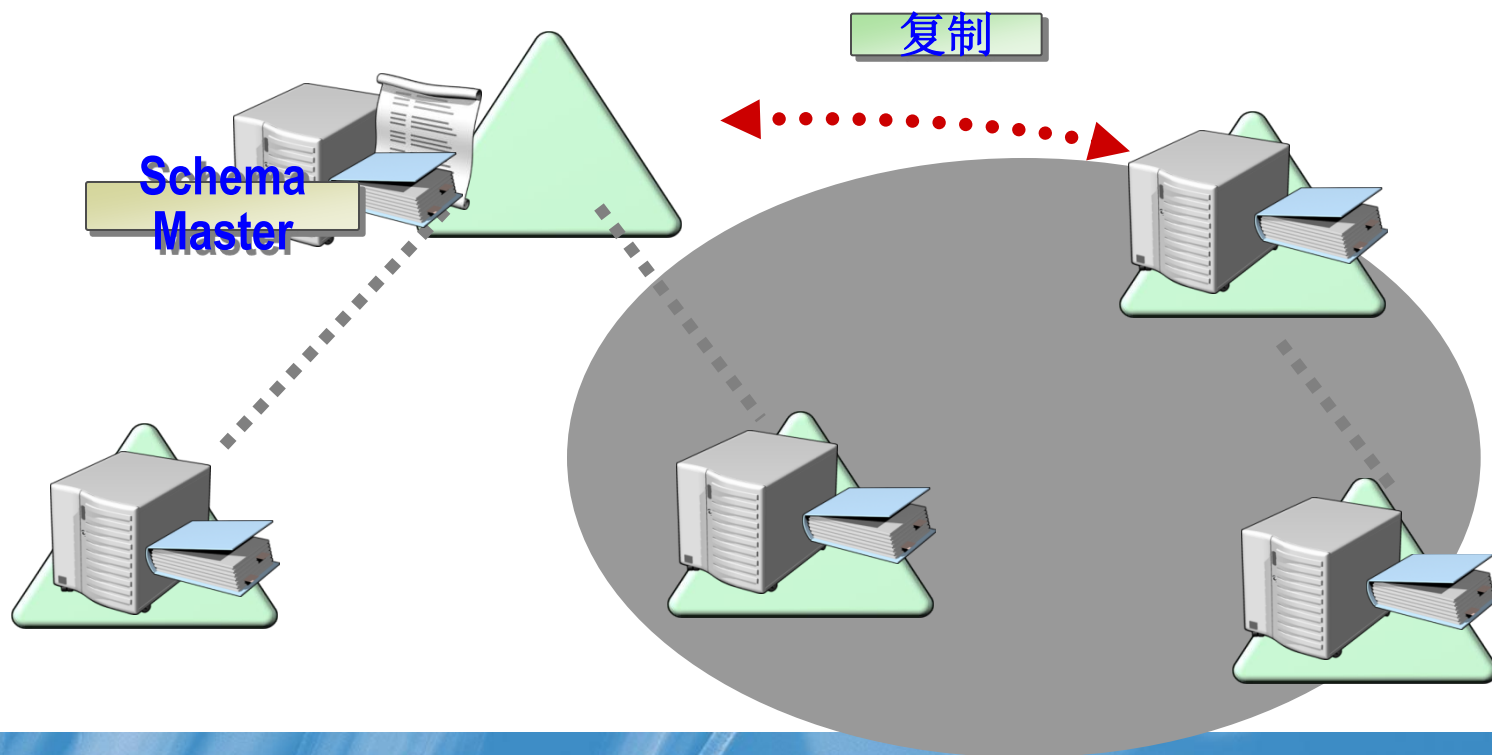
# 什么是活动目录的Schema ?

- Active Directory 架构包含森林中所有对象的定义，架构由对象类和属性组成。
- 架构可以被重新定义或者禁用



# Schema Master架构主机

- 在 Active Directory 中承担架构操作主机角色的域控制器。架构主机执行到目录架构的写操作，并将更新复制到林中所有其他域控制器。不论何时都只能将架构主机角色指派给林内的一个域控制器。



# 查看架构主机

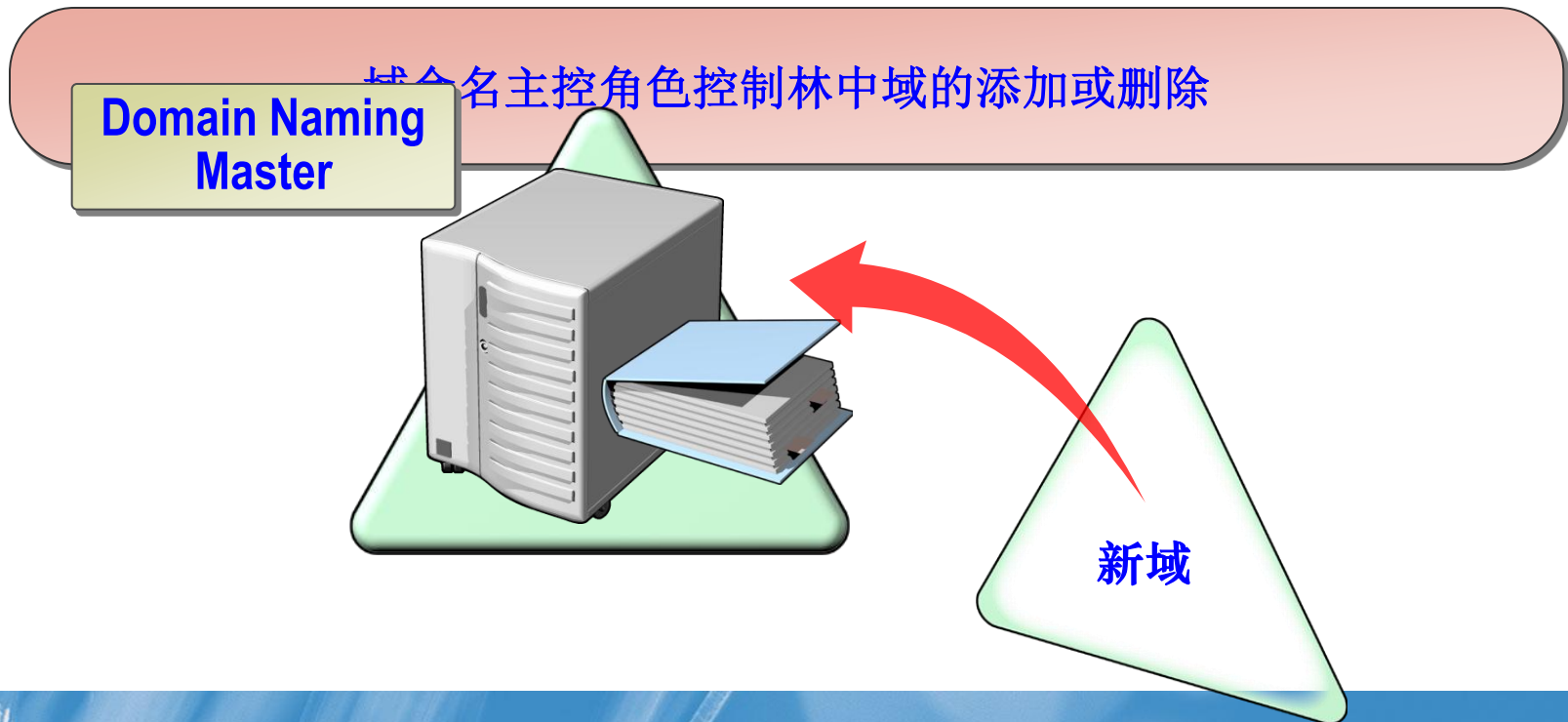
- 方法一：
  - dsquery server -hasfsmo schema
- 方法二:(必须安装support tools)
  - netdom query fsmo
- 方法三:
  - replmon.exe (添加服务器 - 属性 - fsmo roles)
  - 为 “Active Directory Schema” 注册 .dll
  - regsvr32 schmmgmt.dll

# 架构主机故障

- 如果“架构主机”出现故障或离线，可能会影响某些软件的运作。例如某些服务器级的软件在安装时，会在schema添加对象，如果“架构主机”出现故障或离线，将无法安装这些软件。

# Domain Naming Master (域命名主机)

- 在 Active Directory 中担任域命名操作主机角色的域控制器。域命名主机会控制林中域的添加或删除。在任何时候，域命名操作主机角色都只能指派给林中的一台域控制器。



# 查看命名主机

- 方法一：
  - dsquery server -hasfsmo name
- 方法二:(必须安装support tools)
  - netdom query fsmo
- 方法三:
  - replmon.exe (添加服务器 - 属性 - fsmo roles)

# 命名主机故障

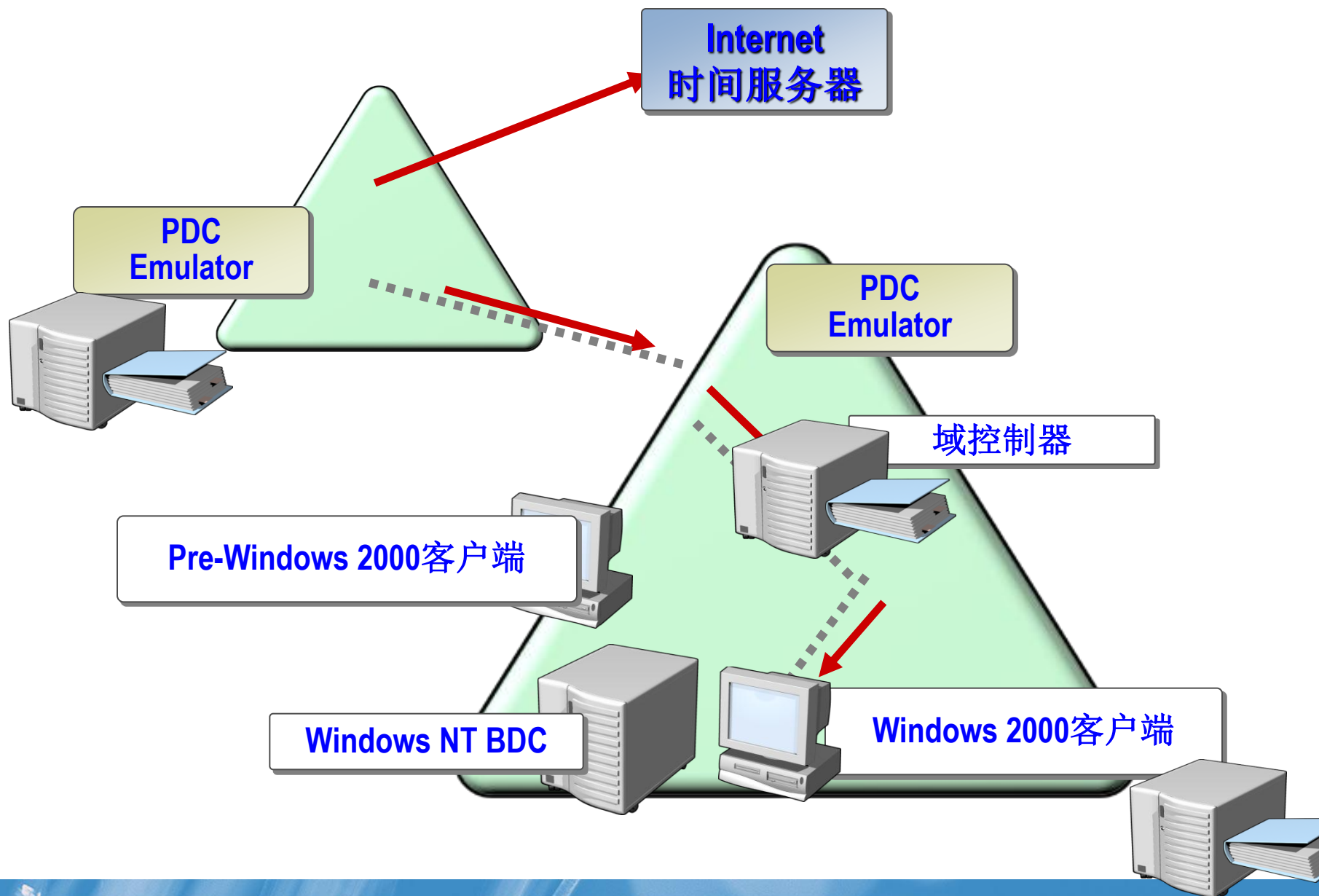
- 如果“域命名主机”出现故障或离线，将无法在林内添加或删除域
- 如果“林功能”级别为“windows 2000”，将“域命名主机”与“全局编录”设为同一台域控制器
- 如果“林功能”级别为“windows server 2003”，“域命名主机”与“全局编录”可以不设在一台域控制器

# PDC 仿真主机

- Active Directory 中担任 PDC 仿真操作主机角色的域控制器。PDC 模拟器为没有安装 Active Directory 客户端软件的网络客户端提供服务，并将目录的更改复制到域内任意 Windows NT 备份域控制器 (BDC) 中。
- PDC 模拟器处理密码验证请求，该请求包括最近已更改但尚未在整个域中复制的密码。在任何时候，每个域中都只能将 PDC 仿真主机角色指派给一个域控制器。



# PDC Emulator ( PDC仿真 )



# 时间服务器

- 查看服务器所使用的时间服务器
  - net time /querysnTP
  - (simple network time protocol)
- 设置服务器所使用的时间服务器
  - net time /setsntp:服务器名
- 手动同步时间
  - W32tm /resync

# PDC仿真器的作用

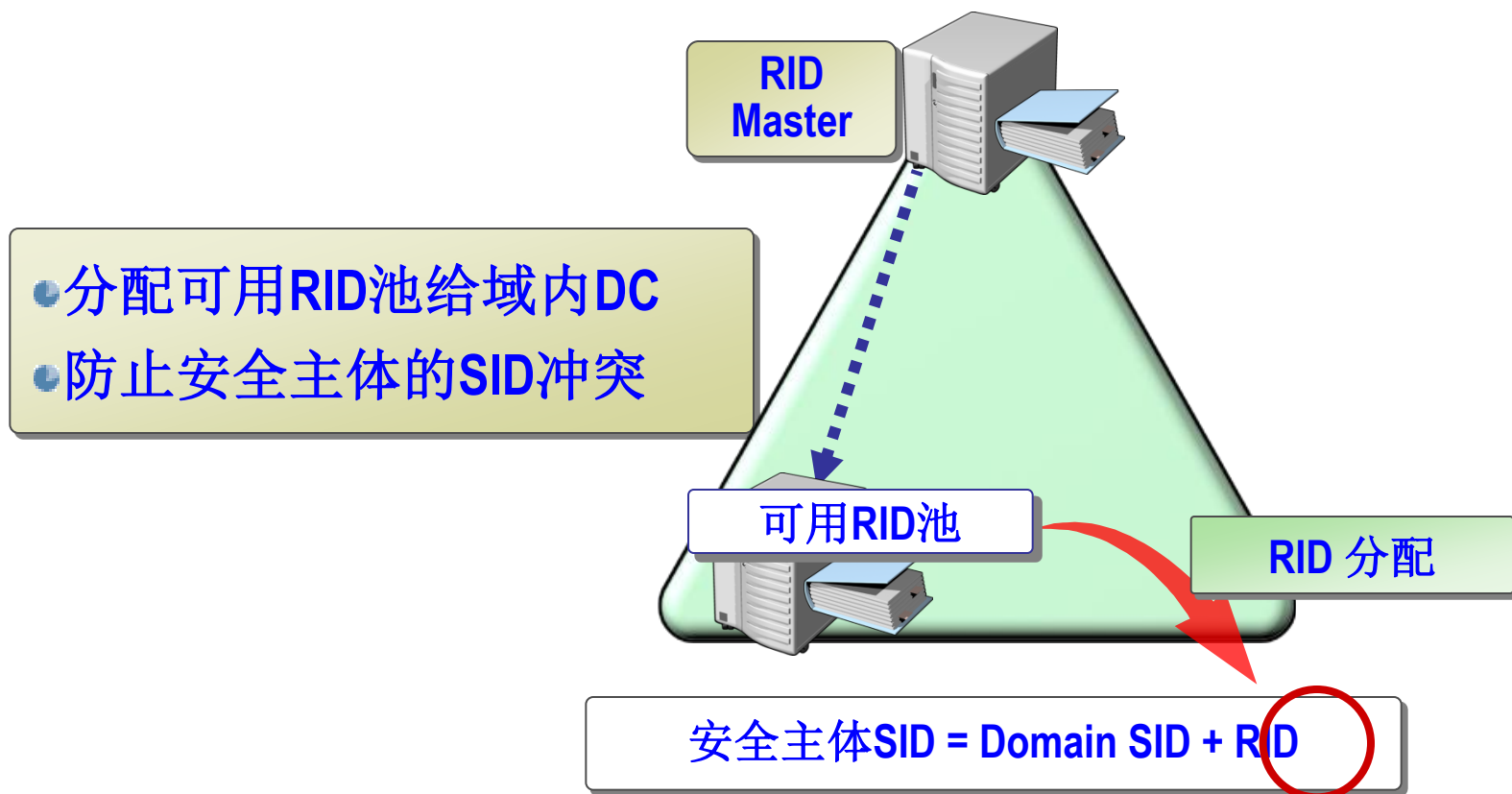
- 统一域内所有客户端和服务器的时间
- 默认的域主浏览器
- 统一更改组策略模版
- 对域内Pre-Windows 2000操作系统的计算机提供支持
- 统一管理域帐号密码更新、验证及锁定

# 查看PDC仿真主机

- 方法一：
  - dsquery server -hasfsmo pdc
- 方法二:(必须安装support tools)
  - netdom query fsmo
- 方法三:
  - replmon.exe (添加服务器 - 属性 - fsmo roles)

# RID Master

- RID 主机将系列相对 ID (RID) 分配给域中每个不同的域控制器。在任何时候，林中的每个域中只能有一个域控制器作为 RID 主机。



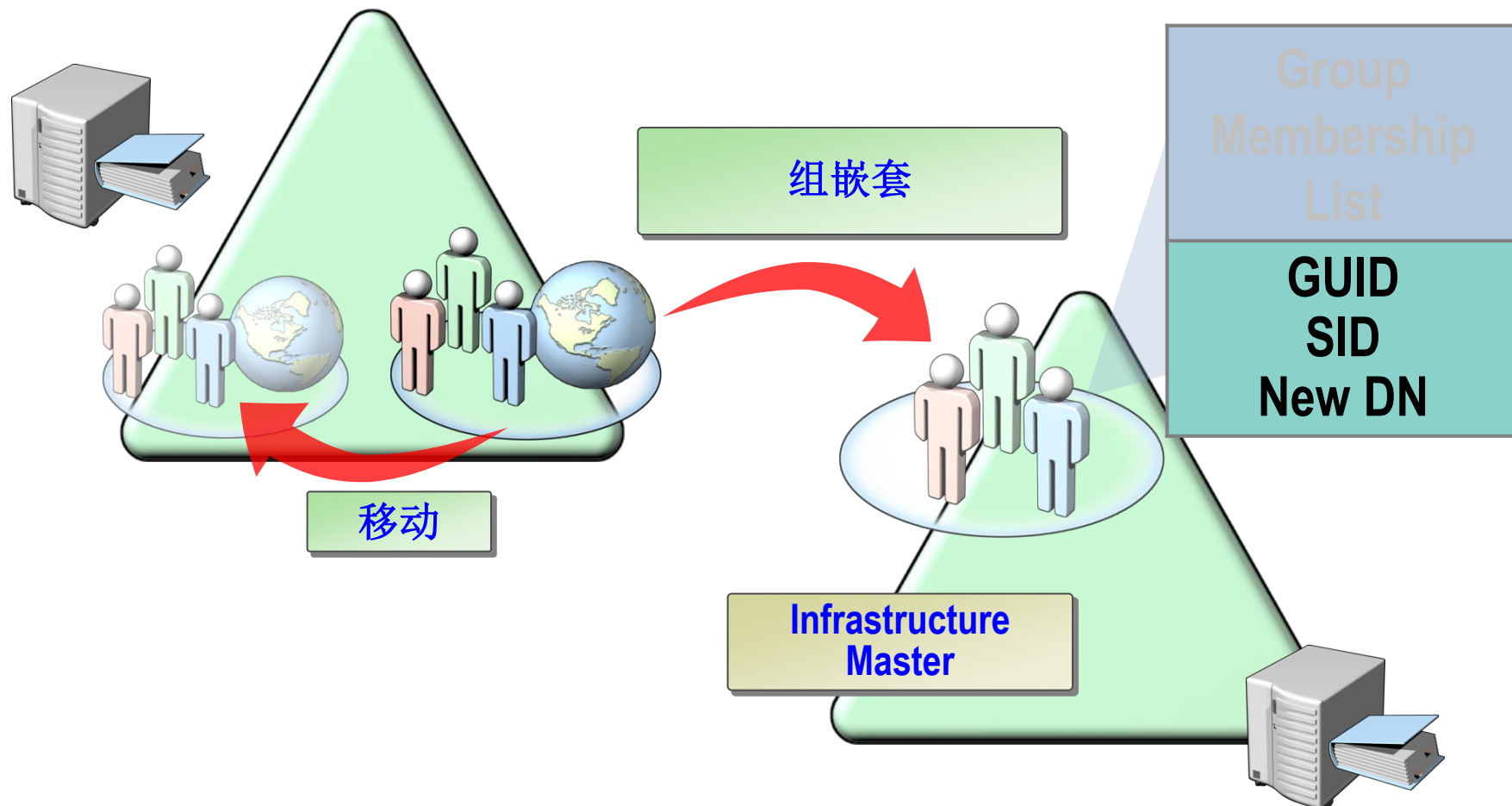
# RID Master

- 移动对象 无论目前所连接的域控制器是哪，当要将某个对象传送到另外一个域时，系统会移动位于“RID主机”内的对象，然后通知其他域控制器该对象已被转移。
- 这种做法可避免位于不同域控制器的同一个对象，被重复传送到不同域的情况发生。

# 查看RID主机

- 方法一：
  - dsquery server -hasfsmo rid
- 方法二:(必须安装support tools)
  - netdom query fsmo
- 方法三:
  - replmon.exe (添加服务器 - 属性 - fsmo roles)

# Infrastructure Master ( 结构主机 )





# 结构主机

- 在任何时候，每个域中只能有一个域控制器作为结构主机。结构主机负责更新从它所在的域中的对象到其他域中对象的引用。结构主机将其数据与全局编录的数据进行比较。全局编录通过复制操作定期接受所有域中对象的更新，从而使全局编录的数据始终保持最新。如果结构主机发现数据过时，则它从全局编录申请更新的数据。结构主机然后将这些更新的数据复制到域中的其他域控制器。

# 查看结构主机

- 方法一：
  - dsquery server -hasfsmo infr
- 方法二:(必须安装support tools)
  - netdom query fsmo
- 方法三:
  - replmon.exe (添加服务器 - 属性 - fsmo roles)

# 实验室demo

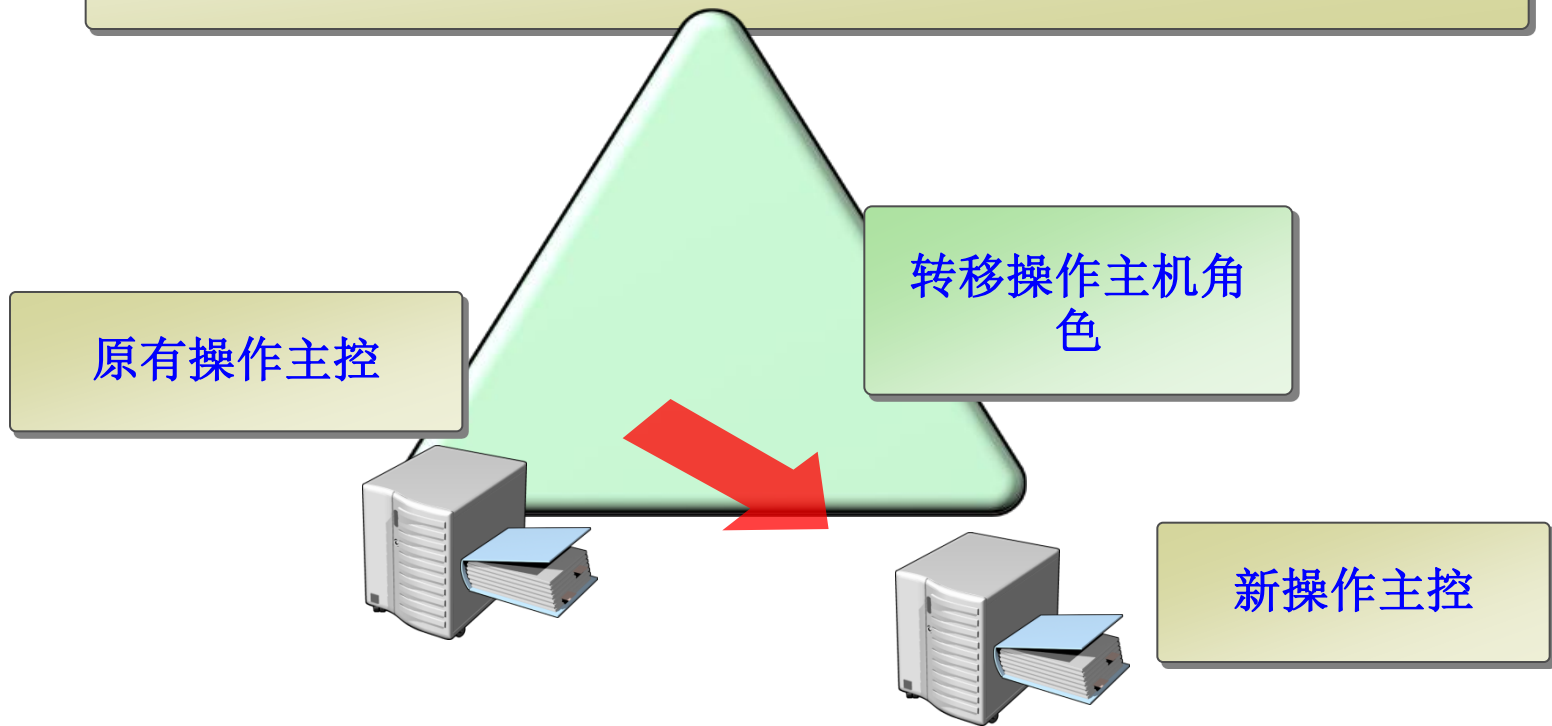
- 查看操作主机

# 操作主机角色管理

- 何时需要转移操作主机角色？
- 决定操作主机角色拥有者：图形化接口工具和 ntdsutil
- 移转方式：transfer(在线移转) 和 seize(强制转移)
- 移转工具：图形化接口工具（AD用户和计算机、AD域和信任关系、AD架构）
- 命令行方式下转移FSMO角色

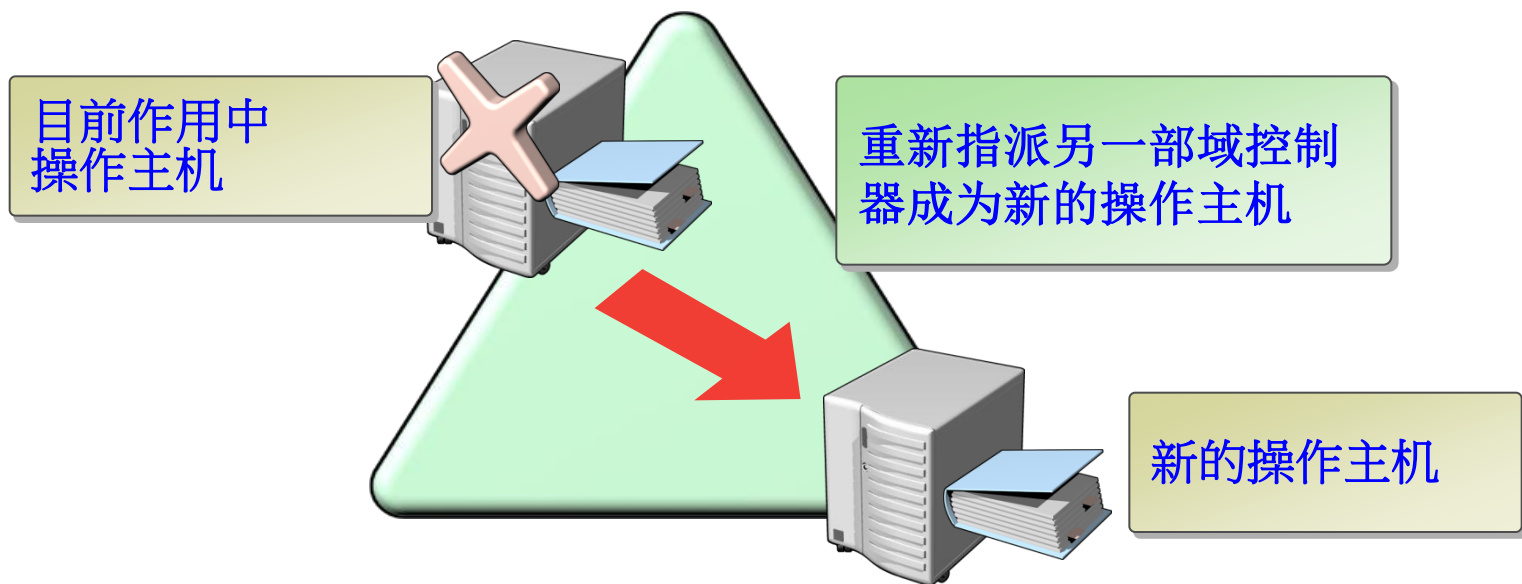
# 转移操作主机角色

转移操作主机角色意味着在原角色所有者配合下，将其从一个域控制器移动到另一个域控制器

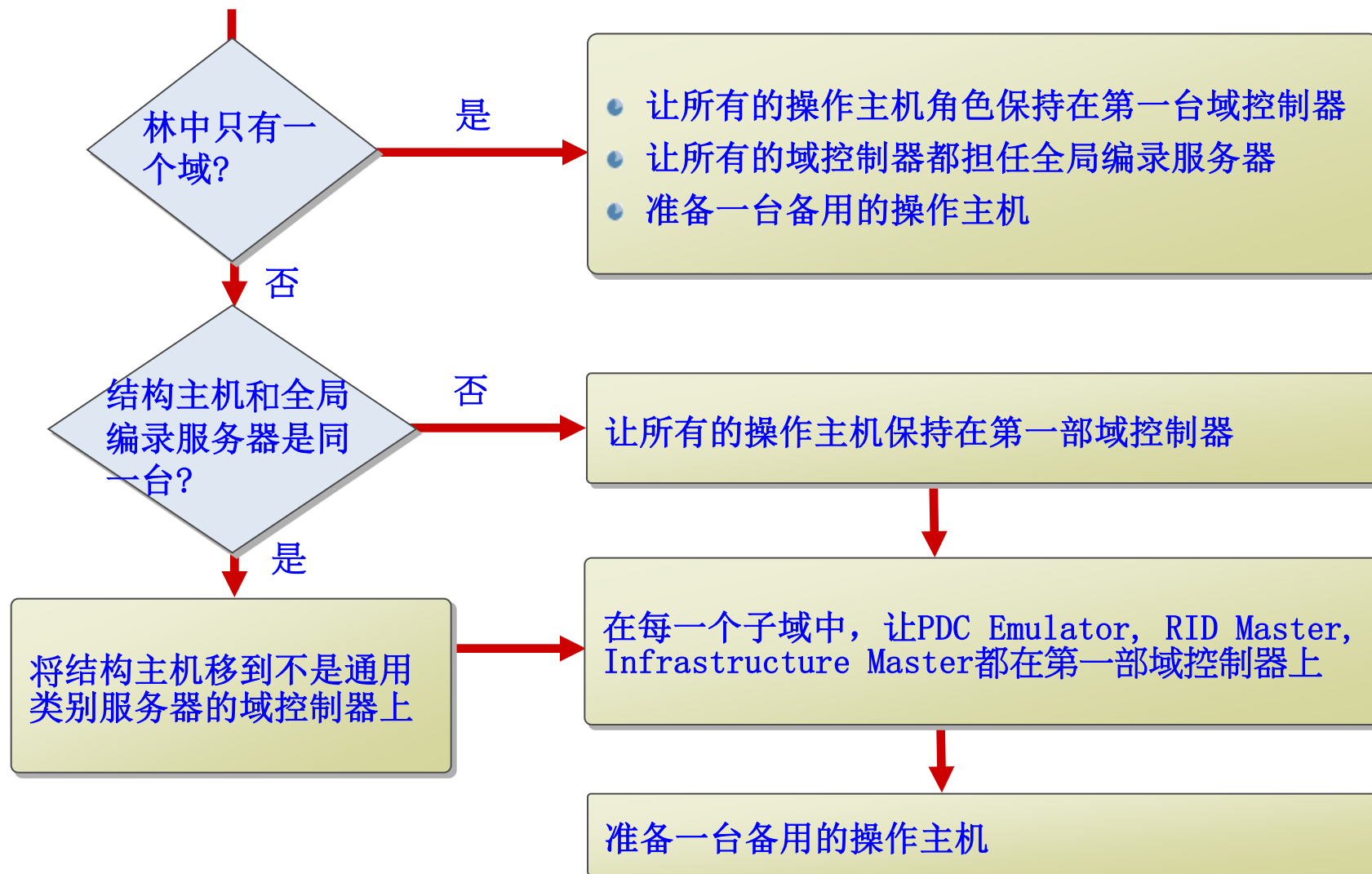


# 什么时候要强制转移操作主机？

- 如果无法进行正常移转操作主机的动作时
- 原操作主机上有变更的数据有可能会遗失



# 操作主机位置的决定准则



# demo

- 实验室 Windows Server 2008之AD DS 活动目录版本升级（迁移）



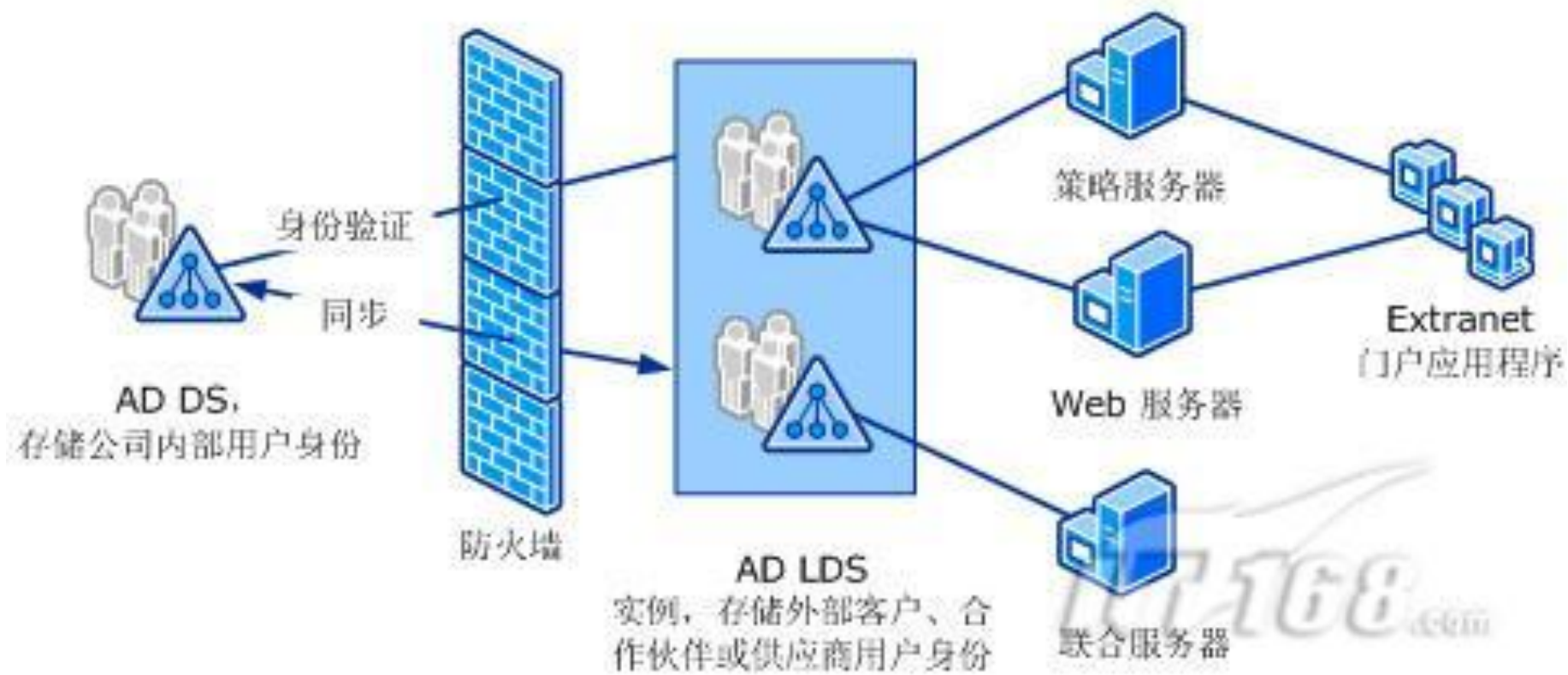
MICROSOFT OFFICIAL COURSE

# MCITP-活动目录(4)

- AD LDS 轻型目录服务(选讲)

# 何为轻型目录服务(AD LDS)

- Windows Server 2008 Active Directory 轻型目录服务(AD LDS)角色是一个功能齐全且易于安装部署的目录服务。它提供了一个用于应用程序的专门数据存储，并可进行单独配置和管理。作为非操作系统服务运行允许多个AD LDS实例在一台服务器上并发运行，并可以独立配置每个实例以便为多个应用程序服务，AD LDS同样不需要在域控制器上（依靠Active Directory 目录服务（AD DS））进行部署。



- 什么是 AD LDS 实例
- AD LDS 的实例是 AD LDS 的单一运行副本。与 AD DS 服务不同，AD LDS 的多个副本可以同事在同一计算机上运行。从多个服务器复制实例时，这样可以提高可用性和实现负载均衡。AD LDS 的每个实例都具有创建实例时分配的单独目录，唯一服务名和唯一服务说明。

- 什么是 AD LDS 复制分区
- AD LDS 的每个实例都可以包含一个或多个应用程序目录分区以保存应用程序数据。AD LDS 目录实例中的所有应用程序目录分区共享一个单一架构，此架构用于定义可以存储在目录中的对象和属性。创建应用程序目录时，可选择新建空应用程序分区，或可从现有 AD LDS 实例中复制一个或多个应用程序目录分区。

## • AD DS 和 AD LDS 的相似点

- 他们都使用LDAP协议并且都支持LDAP客户端连接。
- 使用多主机复制引擎分发复制数据。
- 支持分区，组织(OUs)，组，角色或用户的委派管理。
- 使用可扩展的存储引擎 (ESE)进行数据存储。



- AD DS 和 AD LDS 的不同点
- AD DS和AD LDS各自自身都具有明确和独一无二的用途，他们有几个区别。AD DS 一开始设计为是为企业的运营，管理，审核等提供服务。而AD LDS设计为为其他的应用程序提供健全而简单的工具和基础架构来实现管理，审核等功能的数据 存储的保障。

# AD LDS应用环境

- 1、提供企业目录存储
- 2、提供 Extranet 身份验证存储
- 3、合并标识系统
- 4、为 AD DS 和 AD LDS 提供开发环境
- 5、为分布式应用程序提供配置存储
- 6、迁移旧版已启用目录的应用程序