微软活动目录升级迁移解决方案

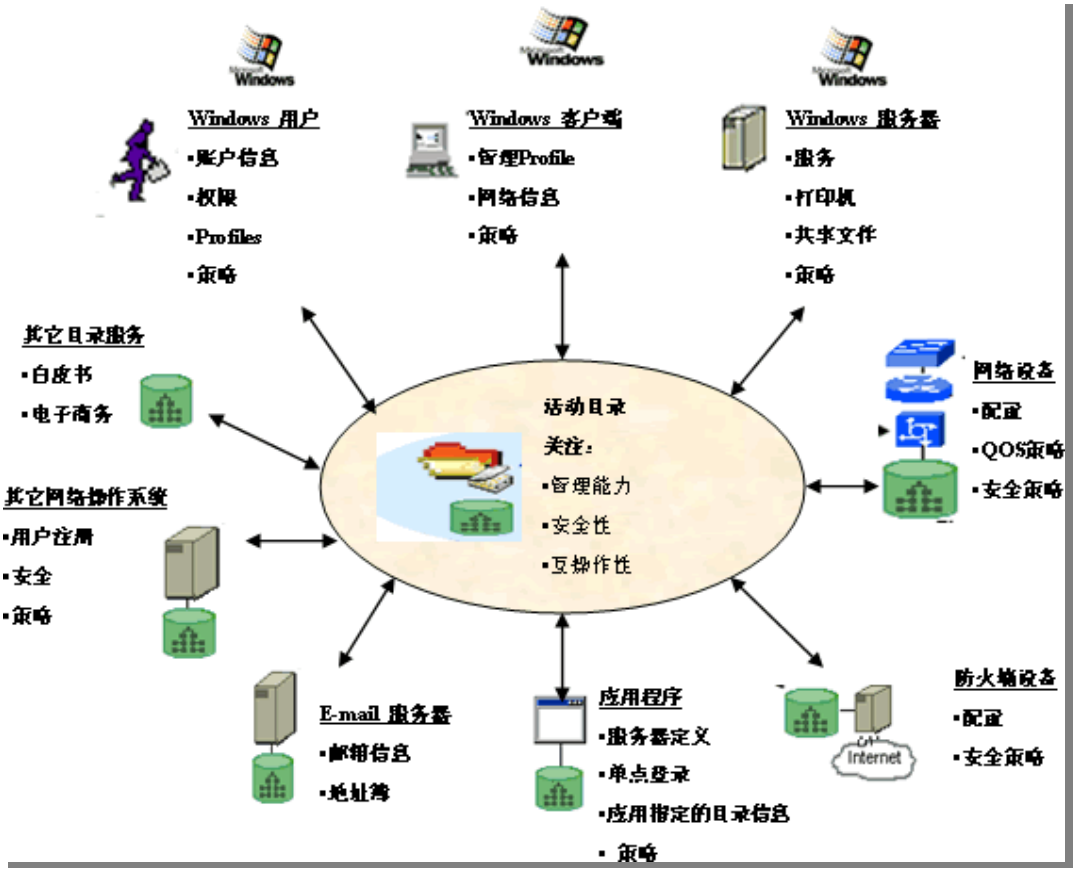
1 企业面临的问题

随着企业不断的发展，信息化建设可能也会遇到以下的瓶颈：

- 活动目录服务器过于老化，多年更换。
- 活动目录平台版本过低，无法扩充人员信息。
- 只是搭建活动目录平台，没彻底发挥活动目录的管理功能。
- 活动目录存在单点故障的问题，没有搭建活动目录冗余功能。
- 有基于活动目录的建设及设计的想法，但又不知道从何入手。

2 解决方案的特点

活动目录是包含了 Windows Server 的目录服务。它扩展了以前基于 Windows 的目录服务的功能，并增加了一些全新的功能。活动目录是安全的、分布式、可分区和可复制的。它的设计保证能在任何规模的安装中正常工作，从只有几百个对象，一台服务器的小系统到拥有数百万对象，上千台服务器的庞大系统它都支持。活动目录增加了许多新功能，这些功能使浏览并管理大量信息变得更容易，为管理员和终端用户都节约了时间。



1. 活动目录模型

活动目录的设计包括逻辑架构设计、物理设计和相关基础组件设计。在逻辑架构设计中，将涵盖森林、域、组织单元和对象等要素的设计。在物理设计阶段，将涵盖站点、域控制器、站点连接等要素的设计。

对于 Windows Server 2008 的活动目录，存在四种设计模型：

- 一个森林一个域
- 一个森林一个树多个域
- 一个森林多个树多个域
- 多个森林多个域

针对域模型的设计，我们主要考虑以下因素：

- 帐户及配置数据的集中
- 高效、简单和灵活分配的管理
- 设计不产生不必要的复杂性
- 对外部和分支机构加入可以扩展
- 简单的域名，便于雇员和合作伙伴使用
- 根据管理政策需要，可以实施管理委派，减轻管理员的工作
- 降低总体维护成本

因此，我们推荐客户使用：单域模型结构。

域模型为单域结构这种结构的优点在于：

- 集中管理整个集团总部的安全策略。
- 可通过委派方式实现管理权（如用户帐号、邮箱添加等）的适当下放。
- 数据信息的集中提升了系统运行性能。
- 完全利用组织单元反映集团的管理结构。
- 当集团机构重组时可以非常灵活的进行调整，比如加入新的域。
- 当资源和用户需要在组织机构内迁移时可以非常灵活的调整。
- 相对其它几种方案，可以使用较少的域控制器。
- 简单的名字空间设计 － 只需要一个DNS名字后缀.。
- 用户在查找AD内的信息时相对简单。
- 单一的组策略更容易实施。

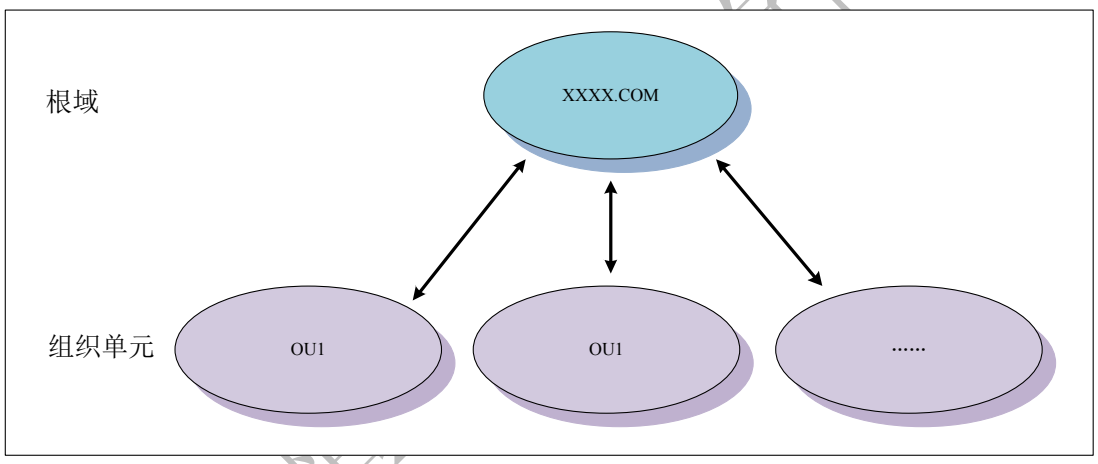
采用单域模型，简化了网络的管理，便于移动用户的使用，不存在域间复制，从管理的角度可以降低维护成本，并能够提供管理委派功能，从用户数据角度，也进行了集中，便于查询分析、备份和恢复。

域模型为单域结构这种结构的缺点在于：

- ◆ 如果各地分支机构系统管理相对独立，提供不了广阔的操作空间。
- ◆ 对总部的系统管理工作要求及工作量相对提高。

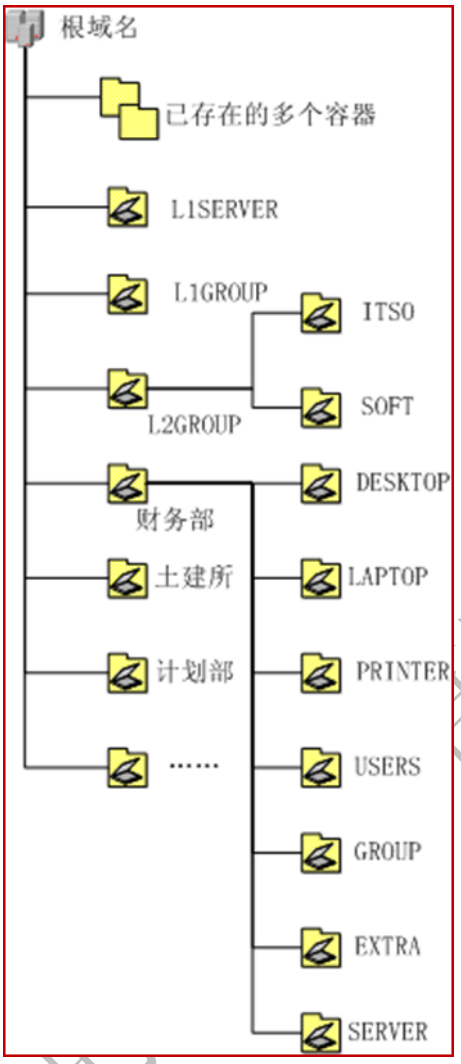
我们建议建立一个新的基于 Windows Server 2008 的森林，并根据管理要求建立两台主域控制器和多个 OU：

XXXX.com： 是整个森林的根域，其中将包含所有基础服务对应的资源，多个 OU 包含所有管理职能部门、所有下属公司，并且，根据物理网段划分，在活动目录中创建对应的“子网”对象及“站点”对象，以保证活动目录可以根据网络带宽优化相关操作。



2. 基于 OU 结构的权限委派

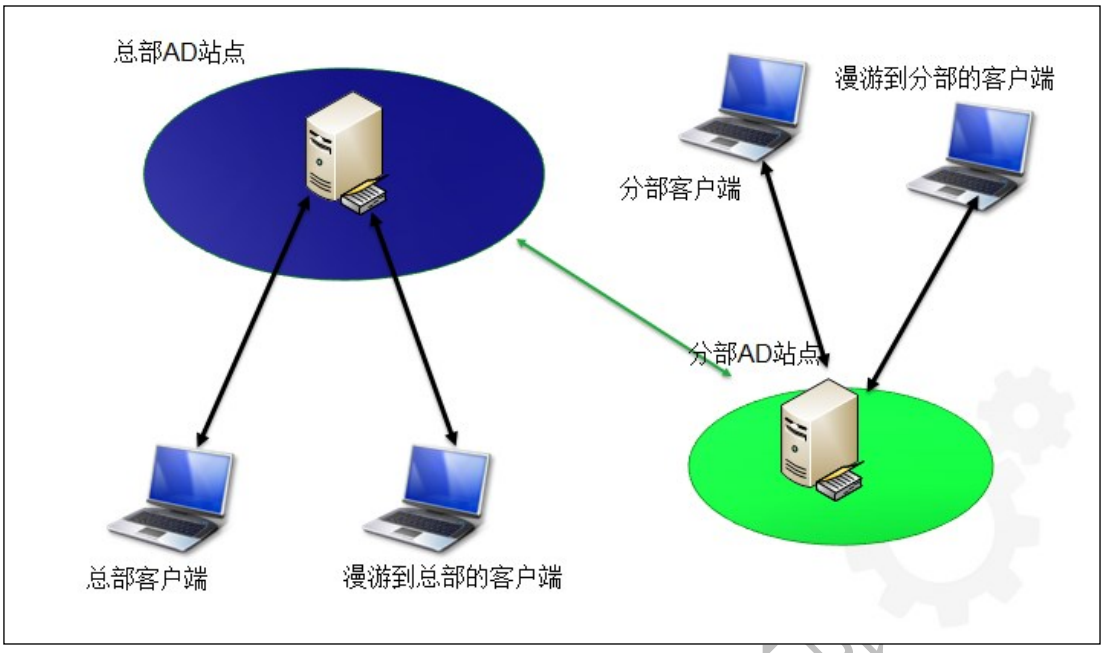
对于一个大型的机构或企业而言，管理 IT 资源的人员不可能局限于一两个人。在有多个管理员同时存在的情况下，如何分配管理权限是一个重要的问题。Windows Server 2008 提供了一种叫做管理控制委派（Delegation of Administrative Control）的机制来解决这一问题。管理委派是 Active Directory 的一项重要功能，它提供了成功管理 Active Directory 环境的手段。



3. AD 物理站点设计

活动目录分为两种结构：逻辑结构和物理结构。活动目录的逻辑结构指的就是域（domain），而物理结构指的就是站点（site）。

- 优化 Active Directory 复制的流量。
- 能够使用户通过稳定、高速的线路连接到域控制器。



4. 组策略管理

对于大部分计算机用户来说，管理计算机基本上是借助某些第三方工具，甚至是自己手工修改注册表来实现。其实 Windows 组策略已经把这些功能集于一体，通过组策略及相关工具完全可以实现我们所需要的功能。

1) Windows Server 2008 组策略非常强大，他主要对域成员服务器起到管理的作用。我们可以简要摘录通过组策略可以实现的功能：

2) 安全性：密码策略规划，登陆权限限制，帐号锁定规则设置。

3) 软件限制：在特定情况可以限制客户端允许及禁止安装软件。

4) 网络限制：通过IP安全策略对网络行为限制。还可以通过DNS客户端、网络连接、SNMP、后台智能传输等策略进行网络行为设定。

5) 用户权限限制：主要是给用户一些权限让他可以允许或禁止某些操作的权限，例如：用户可以更改自己IP地址。

3 解决方案实施的说明

将活动目录和 DNS 服务器从旧硬件迁移到新硬件的最佳实践。迁移现有安装的哪些元素完全取决于服务器管理员。除服务器角色以外，这些元素通常还包括其配置、数据、系统身份和操作系统设置。本文档不假定服务器角色之间可能存在的依存关系。相反，为了达到

目的，在不更改拓扑、站点设置、站点链接设置或子网设置的情况下，将一台计算机上的 活动目录和 DNS 服务器迁移到网络中的另一台计算机上。

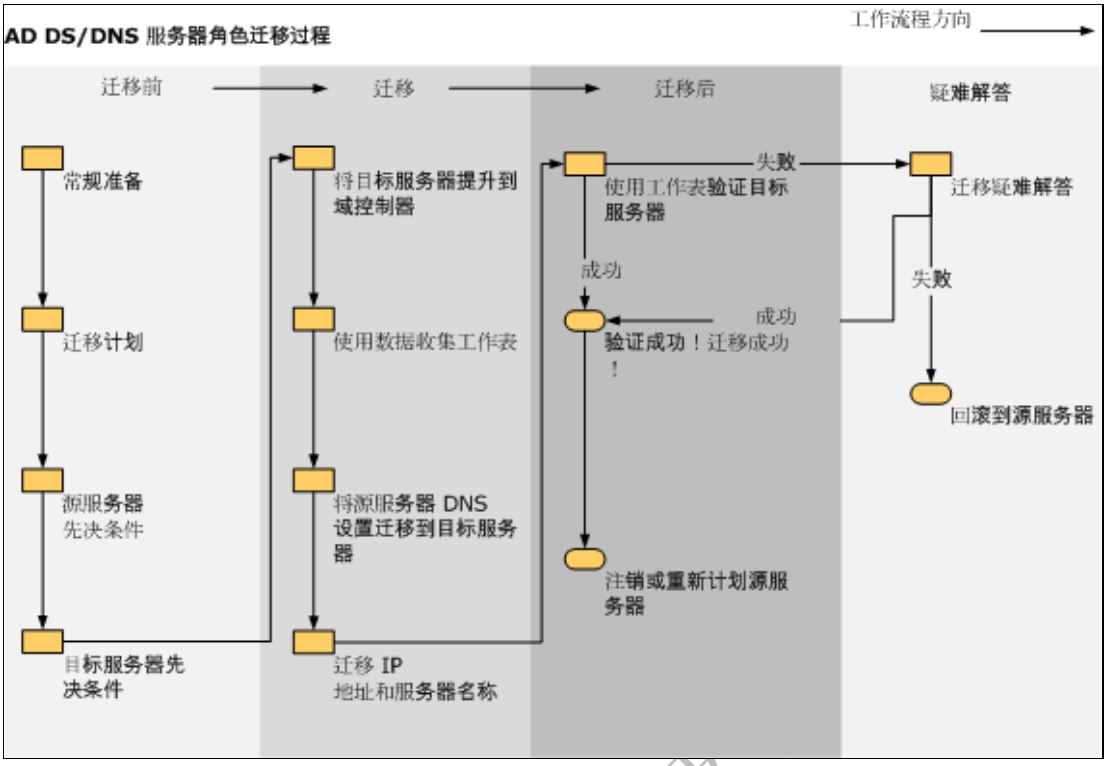
1. 操作主机转移解决方案

如果活动目录在同一森林同一域下升级到 Windows Server 2008，我们采用操作主机转移解决方案，执行迁移时，需要完成以下步骤：

- 计划迁移
- 准备源服务器

  在迁移开始之前，从源服务器收集 Active Directory 或 DNS 设置。
- 将基于 x64 的新 Windows Server 2008 R2 服务器添加到网络中并将其设置为域控制器。
- 迁移强制设置
- 验证迁移是否成功
- 执行迁移后任务（可能包括源服务器的降级）
- 按照 AD DS 和 DNS 服务器迁移：独立 DNS 迁移中的单独说明执行操作，仅迁移 DNS 服务器角色。

下图显示了迁移过程。



在迁移过程的这一时刻，源服务器作为域控制器，而目标服务器作为成员服务器。

下列步骤对迁移过程进行了概述：

- 使目标成员服务器成为域控制器
- 记录源服务器上的 DNS 设置
- 将源服务器 DNS 设置导入到目标服务器
- 通过运行聚合验证脚本验证源服务器与目标服务器之间是否发生了设置复制。
- 可以将操作主机（也称为灵活单主机操作或 FSMO）角色或站点间拓扑生成器 (ISTG) 角色从源服务器手动迁移至目标服务器。
- 将源 IP 地址从源服务器迁移至目标服务器
- 将源服务器名称迁移至目标服务器

2. 跨林的迁移解决方案

如果活动目录不在同一森林的情况，无法使用操作主机的迁移。在这种情况下，我们可以采用跨林的迁移解决方案。

Active Directory 迁移工具 (ADMT) 提供了一个方便、可靠和快捷的方法，从 Windows 迁移到 Windows Server 2008 Active Directory 服务。您还可以使用 ADMT 重构 Windows

Server 2008 Active Directory 域。在开始迁移操作前，此工具可帮助系统管理员诊断任何可能的问题。随后，基于任务的向导就会允许您迁移用户、组和计算机，设置正确的文件权限以及迁移 Microsoft Exchange Server 邮箱。在迁移前后，您可以使用此工具的报表功能，评估迁移所带来的影响。在很多情况下，如果出现问题，您可以使用回滚功能，自动恢复原来的结构。此工具还提供对并行域的支持，所以您可以在部署 Windows Server 2008 操作系统的同时，保持现有的 Microsoft Windows 操作系统。

4 用户的收益

企业的活动目录升级到 Windows Server 2008 活动目录后带来如下收益：

- **强大的硬体与扩充功能** Windows Server 2008 R2 的设计目的是为了提供与 Windows Server 2008 同等级或更优异的硬体基础。此外，R2 也是第一套只能够移转到 64 位元架构的 Windows Server 作业系统。
- **消除冗余管理任务** 提供对 Windows 用户账号、客户、服务器和应用程序以及现存目录同步能力进行单一点管理。
- **降低桌面系统的行程** 针对用户在公司中所担当的角色自动向其分发软件，以减少或消除系统管理员为软件安装和配置而安排的多次行程。
- **更好的实现 IT 资源的最大化** 安全地将管理功能分派到组织机构的所有层次上。
- **降低总体拥有成本（TCO）** 通过使网络资源容易被定位、配置和使用来简化对文件和打印服务的管理和使用。

【完】