

## 07Exchange Server白手起家系列之七：软件安装和服务器管理的规范化

配置和变更管理。

- ◆ 配置管理和变更管理不是万能的，但没有这些是万万不能的！
- ◆ 企业IT系统不是一两个专家的杰作，而是严格流程下的产物
  - 同样Level的工程师 + 同样的流程 = 一致的SLA
- ◆ 流程的细化和量化, 量化所有细节
- ◆ 参考：从管理和运营的角度看IT
  - <http://www.microsoft.com/china/technet/webcasts/class/mof.mspx>

软件安装和服务器管理的规范化

- ◆ 服务器应该有固定的角色，杜绝一机多用
- ◆ 每种角色的服务器应该有固定的软件、工具和附属文档的安装列表，杜绝安装无用的非业务软件
- ◆ 服务器重要属性的记录和及时更新
- ◆ 厂商联系信息和维修记录
- ◆ 服务器的补丁管理，禁用自动更新

配置管理

### *Mission Statement*

*The identification, recording, and reporting of IT components, including their versions, constituent components and relationships. Items that should be under the control of Configuration Management include hardware, software and associated documentation.*

从静态的角度讨论IT基础架构对组织IT服务运营的支持。

配置管理的目标

- ◆ 计量所有IT资产(软硬件、服务、流程、文档)
- ◆ 为其他服务流程提供准确的信息
- ◆ 作为事故管理、变更管理和发布管理的基础
- ◆ 验证基础架构记录的准确性并纠正发现的错误

配置管理的主要活动

#### ◆ 配置管理规划

- purpose, scope, objectives, policies and procedures, and the organizational and technical context

#### ◆ 配置识别

- of all the Configuration Items (CIs), their attributes and relationships, and assigning IDs and entering information

#### ◆ 配置项控制

- of updates to the CMDB using Change Management

#### ◆ 配置状况报告

- tracking changes in status. History vs. Actual (baseline)

#### ◆ 配置验证和审核

- Manual or electronic audit of CMDB

### 变更管理

#### *Objective:*

*Ensure that standardised methods and procedures are used for efficient and prompt handling of all Changes, in order to minimize the impact of Change-related Incidents upon service quality, and consequently to improve the day-to-day operations of the organization.*

从动态的角度讨论IT基础架构对组织IT服务运营的支持。

为了在最短的中断时间内完成基础架构或者服务的任一方面的变更而对其进行控制的过程。

### 规范化的exchange的安装流程

- ◆ 操作系统安装、更改默认设置和性能优化
- ◆ Exchange安装，服务设置
- ◆ 默认参数、重要文件夹位置的修改
- ◆ 应用系统策略、邮箱数据库策略等

RIB卡，是跟服务器独立的设备，有独立的IP，类似于带外管理，HP的ilo。  
将新服务器的信息更新到CMDB表中。

## 步骤一 信息收集和汇总



- ◆ Server Name
- ◆ Site Name
- ◆ Date
- ◆ Exchange Admin name
- ◆ IP address
- ◆ Subnet
- ◆ Gateway
- ◆ RIB Card IP address
- ◆ Number of Users

Microsoft TechNet

规划服务器的磁盘设置，服务器硬件的RAID设置。

为了优化磁盘读写，要对存放数据的E/F盘做特殊的格式化，4K扇区对齐。

## 步骤二 磁盘配置

- ◆ 数据库和日志使用的阵列
- ◆ Diskpar的作用
  - <http://blogs.itecn.net/blogs/yuyong/default.aspx>
- ◆ 使用Z盘做安装文件、补丁和工具的保存，可以采用DFS同步，确保每个服务器都是一样的

Small site supporting up to 1,000 users	
Label	Device
C: SYSTEM	RAID 1 Internal
D: CDROM	
E: SG1 LOGS	RAID 1 on PCI RAID Controller/Disk Shelf
F: SG1 IS	RAID 5 on PCI RAID Controller/Disk Shelf
Z: SYSAPPS	RAID 1 Internal

Large site supporting up to 2,000 users The following should be used for a typical server with two Storage Groups	
Label	Device
C: SYSTEM	RAID 1 Internal
D: CDROM	
E: SG1 LOGS	RAID 1 on PCI RAID Controller/Disk Shelf
F: SG1 IS	RAID 5 on PCI RAID Controller/Disk Shelf
G: SG2 LOGS	RAID 1 on DUAL Channel RAID or SAN
H: SG2 IS	RAID 5 on DUAL Channel RAID or SAN
Z: SYSAPPS	RAID 1 Internal

先决条件准备工作。



## 步骤三 安装前的验证

- ◆ 安装并启动下面的服务
  - Network News Transport Protocol (NNTP)
  - Simple Mail Transport Protocol (SMTP)
  - World Wide Web Publishing Service
  - Telnet
  - ASP.NET is installed
  - RPC over HTTP
- ◆ 确认 Front-Page Extensions 没有被安装
- ◆ Windows 的语言包 (Language Pack)

虽然是exchange 2003的流程，但是对现在exchange2010,2013的安装还是有启发意义。  
outlook不能装，因为outlook有个MAPI32.DLL的文件，会跟exchange有冲突。  
不需要装杀毒软件。

## 步骤四 Exchange安装

- ◆ 企业版或者标准版？
- ◆ 补丁的安装  
Windows->Windows SP->Post Hotfix->Exchange->Exchange SP->Post Hotfix
- ◆ 为服务器选择正确的路由组和管理组
- ◆ OWA改密码
  - HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeWEB\OWA
  - Set 'DisablePassword' key to '0'
- ◆ 安装ExBPA, ExDRA等工具
- ◆ 不要安装Outlook和其他Office软件
- ◆ Exmerge等工具
  - <http://www.microsoft.com/technet/prodtechnol/exchange/downloads/2003/tools.mspx>
- ◆ 文档：
  - <http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/default.mspx>

针对后端服务器，可以停止的服务。

## 步骤五 停止不必要的服务

- ◆ 如果只是后端邮箱服务器，请停用以下的服务
  - Automatic Update Service
  - Distributed Link Tracking Client
  - File Replication
  - Indexing Service
  - Internet Connection Sharing
  - Microsoft Exchange IMAP4
  - Microsoft Exchange POP3
  - NetMeeting Remote Desktop Sharing
  - Network News Transport Protocol (NNTP) - EXCEPT on PF Servers
  - Print Spooler
- ◆ 建议把Exchange IS服务设置为手动启动
  - 当磁盘阵列出现问题时，设置自动启动会增加数据库损坏的风险

非系统盘。分开存放。规划名称路径。

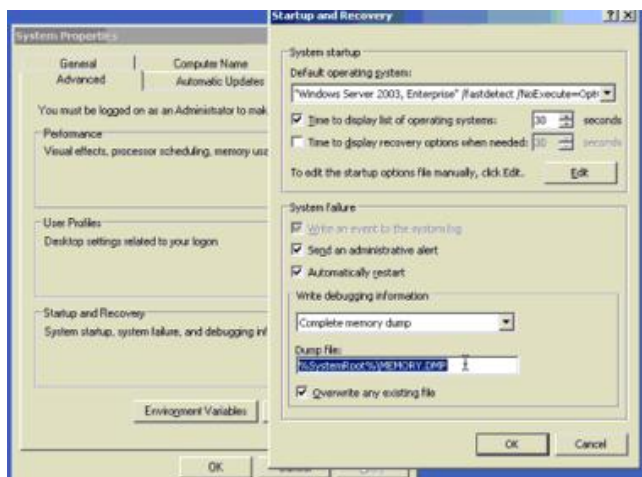
在每一台服务器上规划离线地址簿和忙闲信息的副本（公共文件夹）。

## 步骤六 创建存储组和数据库

- ◆ 选择正确的磁盘和卷来保存
  - 每个保存Exchange数据库的文件夹都应该有同样的名字
- ◆ 合理的命名规则
- ◆ 本地化离线地址簿、忙闲信息
- ◆ 应用服务器、邮箱策略
- ◆ 设置和移动系统日志文件的位置
  - EventLog的记录范围
  - IIS Log
  - Message Tracking Log

C盘保留一个200-300M的页面文件，否则Windows蓝屏的时候，无法生成dump。其他盘可以设置一个比较大的页面文件。

下图是设置生成一个完整的DUMP文件。



3G参数，可以让exchange数据库有更多的虚拟内存空间去工作（information store）

## 步骤七 服务器全局配置

- ◆ 页面文件
- ◆ 崩溃转储文件
- ◆ 针对内存进行优化
  - /3GB
  - 在基于 Windows Server 2003 的系统中安装 Exchange Server 2003 时使用 /3GB 参数
  - <http://support.microsoft.com/kb/823440/zh-cn>
  - 如何优化 Exchange Server 2003 中的内存使用
  - <http://support.microsoft.com/kb/815372/zh-cn>

exchange防病毒排除

## 步骤八 辅助软件的安装

- ◆ 备份软件
- ◆ OS防病毒
  - 设置病毒库的自动更新
  - 排除所有Exchange的文件夹
- ◆ Exchange防病毒
  - 设置病毒库的自动更新
  - 隔离文件夹的位置和定期清除或归档
- ◆ 监控

## 第九步 收尾工作

- ◆ 运行ExBPA



第一批用户：pilot领航员。

小范围试用，IT部门首当其冲。一般选择总用户的5%到15%。

## 用户迁移的注意事项和最佳实践

- ◆ **Pilot用户的概念**
  - IT部门首当其冲, **eat your dog-food**
  - 及时的从**Pilot**用户获取反馈
- ◆ 软件客户端的部署和批量配置安装
- ◆ 建立详细的用户列表和迁移计划
- ◆ 预先通知用户并作出完整的沟通计划
- ◆ **Helpdesk**的技术支持能力要及时跟进

迁移要做非常多的准备和指导工作。

## 用户迁移的注意事项和最佳实践

- ◆ **从外部邮件系统(ISP)迁移**
  - 一次性完成
  - 培训和前期测试工作较多
  - 邮件收发的监控
- ◆ **从内部异构邮件系统迁移**
  - 与异构系统的共存
  - 权限、策略是否被满足

不仅仅适应于exchange的项目，道理都是想通的。

- ◆ **成功的条件**
  - 系统前期的部署和测试
  - 用户培训和沟通计划
  - **IT**支持部门对用户针对新系统问题的及时解答

风险控制，回退机制。

## 生产服务器的压力监控

- ◆ 收集和分析如下的反馈
  - 性能指标
  - 服务状态
  - 客户主观的反馈信息
- ◆ 制定相应的回退计划
  - **Pilot**用户测试失败
  - 性能没有达到预期
  - 制定回退计划，将**Pilot**用户迁移回旧的系统

基于ITIL的发布管理。

## 理论总结

- ◆ ITIL的发布管理(release management)
- ◆ **Release Management takes a holistic view of a Change to an IT service and should ensure that all aspects of a Release, both technical and non-technical, are considered together.**

发布管理包含的一系列活动。

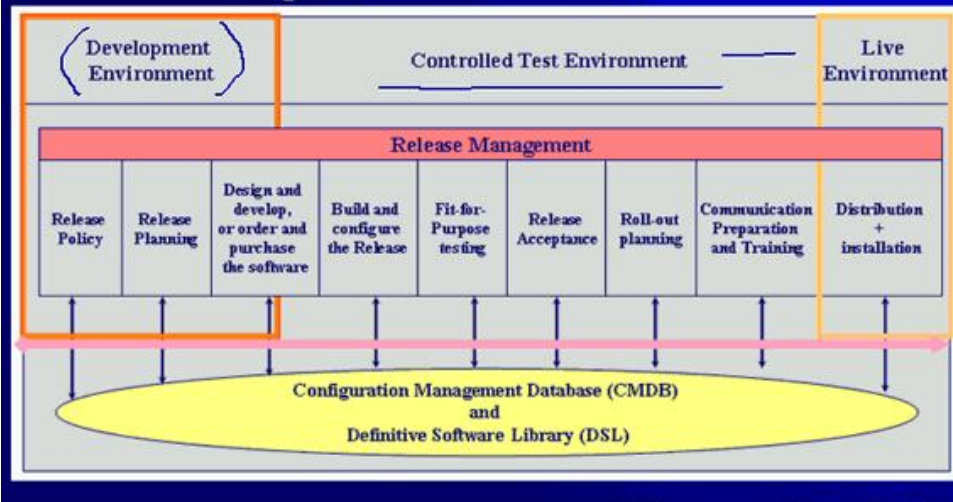
## Activities

- ◆ Release policy and planning
- ◆ Designing, building and configuring a release
- ◆ Release Acceptance
- ◆ Rollout planning
- ◆ Communication, preparation and training
- ◆ Distribution and installation
- ◆ Storage of controlled software in both centralized and distributed systems



# Release Management

## Release Management Environments



exchange 5.5自带ds目录服务，而exchange 2000以后的是吧这一块功能由AD来处理了。

## Exchange 5.5的架构特征

- ◆ Exchange自带目录服务
- ◆ NT PDC只提供了一个账号，所有邮箱属性都保存在Exchange自己的目录中
- ◆ 一个账号可以对用多个邮箱

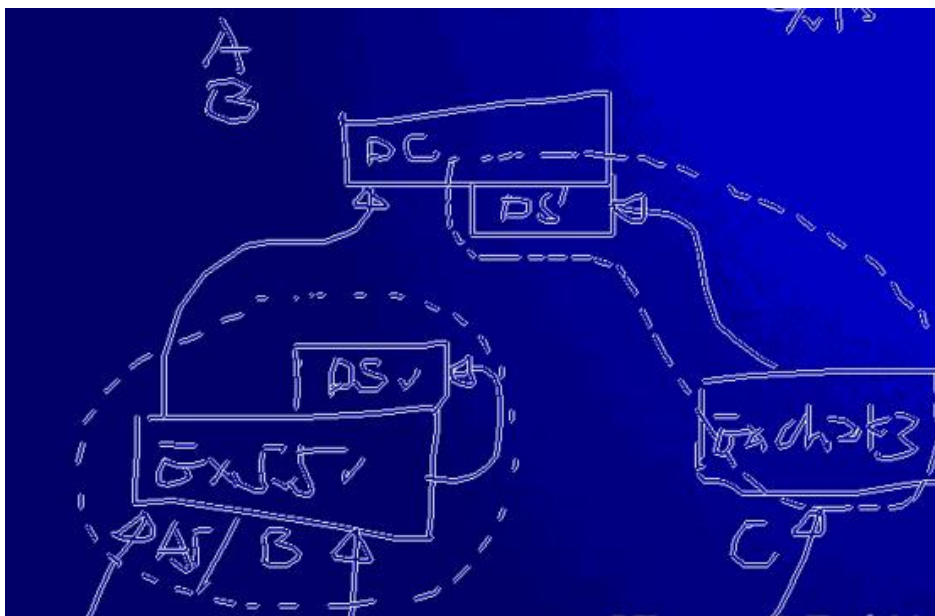
需要先升级AD。

## Active Directory Connector

- ◆ 必须有ADC，Exchange 5.5才可能顺利迁移到Exchange 2003
- ◆ 必须使用Active Directory的DNS
- ◆ ADC负责Exchange 5.5 DS与Windows 2003 的Active Directory之间进行目录复制
  - 必须安装在Windows 2003
  - 以Update Sequence Number (USN)为复制的基准
  - 使用LDAP协议 (Exchange 5.5必须升级到 SP3以上)
  - 可以选择以下的对象进行复制Mailbox, DL, Custom Recipient, Public Folder

下图两个DS系统是各自存在的。所以会存在共存的问题。

要解决exchange 5.5DS和AD之间同步的问题。

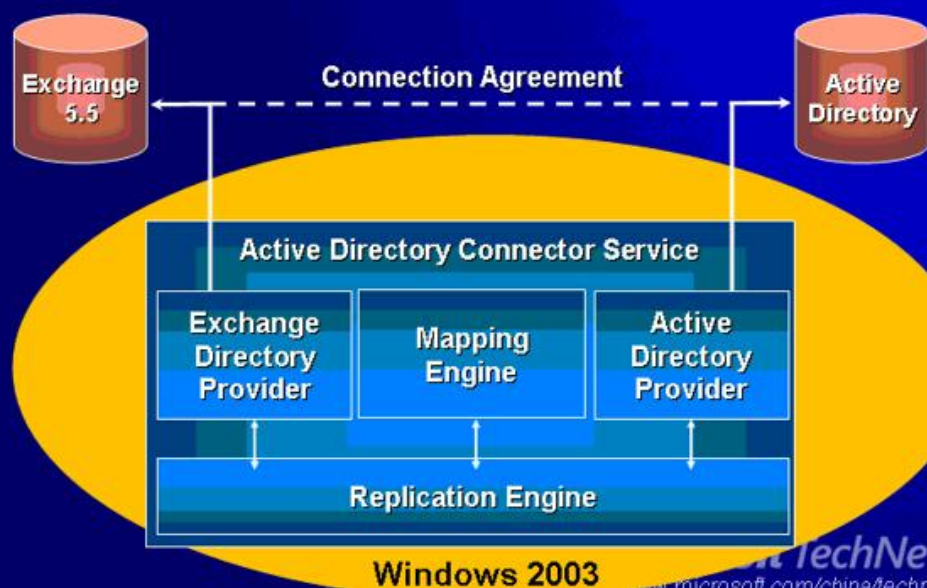


## 安装和配置 ADC

- ◆ From Exchange to Active Directory
  - 在Ex55端进行管理
- ◆ From Active Directory to Exchange
  - 在AD端进行管理
- ◆ Two-Way
  - One two-way Recipient CA for each 5.5 site
  - Two one-way CA's do **NOT** equal one two-way CA

# ADC 结构

#13



## 安装Exchange 2003 Server join to Exchange 5.5 ORG (一)

- ◆ **Setup /forestprep** 可以选择是新建组织，还是加入到Ex55的组织
- ◆ 如果加入到Ex55 site
  - 输入site中的一台机器的名字
  - 输入 site service account信息
- ◆ Ex2k继承了Ex55的组织名字
- ◆ Site 和管理组是一一对应的关系
- ◆ 以后加入到这个AG的Ex2k也相应地加入到这个Ex55 Site



## 安装Exchange 2003 Server join to Exchange 5.5 ORG (二)

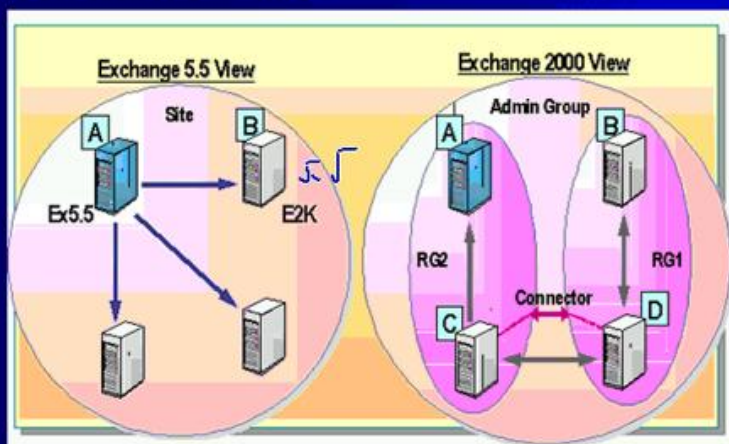
- ◆ 设定整个ORG的Connection Agreement
  - 要开始升级的site：双向
  - 其他的site：单向
- ◆ 安装Windows 2003 SP1以上的版本
- ◆ 安装SMTP 和NNTP Service
- ◆ 安装完成后，以Exchange 5.5的site-addressing的SMTP为预设的Recipient Policy
- ◆ 成为缺省的RUS server
- ◆ 成为Routing Group Master

SRS把exchange 2000伪装为exchange 5.5

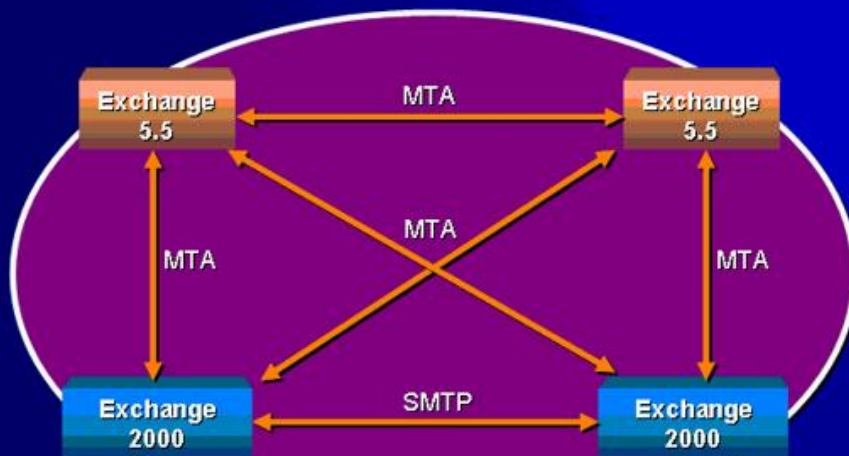
## Messaging Coexistence: Routing

- Ex55 site 变成了Ex2k中的AG和RG
- Ex55 不能识别AG中的RG

SRS



## Intrasite Message Transport

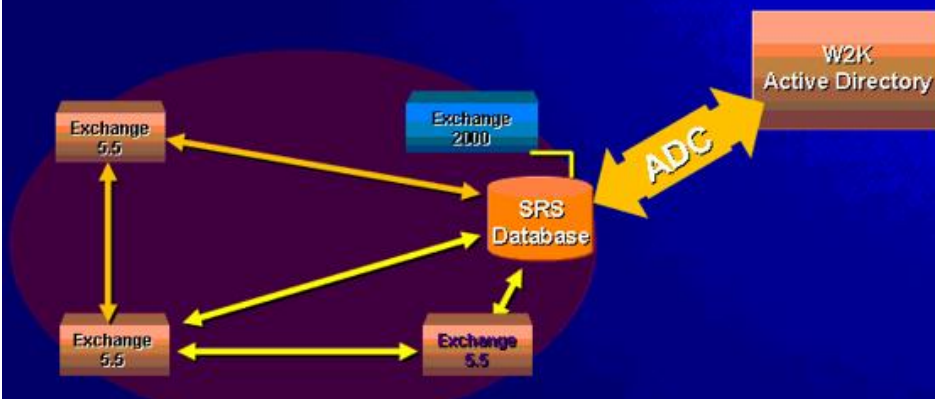


## Directory Co-Existence With Exchange 5.5

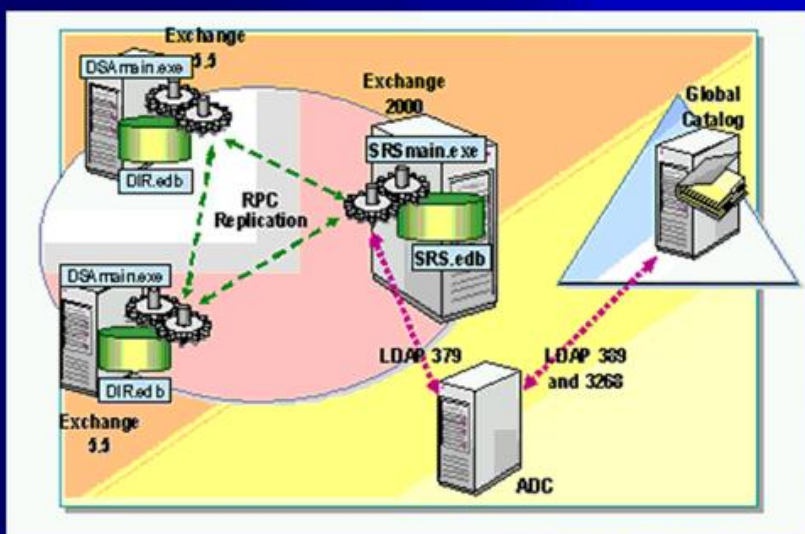
### ◆ Directory Connectivity

- SRS参与了Ex55站点之间的目录复制
- ADC在Ex55目录服务（或SRS）和Active Directory之间进行复制
- Site Replication Service 是在Exchange 2k和Exchange 5.5 共存的环境才有的

## Site之间目录复制



# Configuration Coexistence:



DIR.EDB就是exchange 5.5自带的目录数据库。可以和SRS.EDB进行连接，然后在和活动目录进行复制。

## 升级到Address List

- ◆ Address List的功能，相当于Exchange 5.5的Address Book View
- ◆ 升级Exchange 5.5到Exchange 2003后，并不会升级Address Book View到Address List
- ◆ Exchange 2003 会自动建立 GAL 和其他预设的Address lists
- ◆ 使用LDAP filters建立virtual views
- ◆ Messaging Connectivity
  - Exchange 5.5 ↔ Exchange 5.5 uses MTA
  - Exchange 5.5 ↔ Exchange 2003 uses MTA
  - Exchange 2003 ↔ Exchange 2003 uses SMTP

=====

**09Exchange Server白手起家系列之九：大规模的用户帐号管理、组管理中采用的常见策略**

及时更新跟用户相关的属性信息。



# 大规模的用户管理的原则

- ◆ 及时地进行更新，反映实际的用户情况
- ◆ 信息的更新和权限的调整尽可能在客户端完成
- ◆ 用户帐号禁用、删除的流程
- ◆ 用户组能够反映实际的组织结构，并能够满足信息传播的要求

明确森林、域、子域的功能。

按照地域或者办公城市设置OU。

以每个OU为单位进行管理员权限设置。

把管理员账号和服务账号从用户的普通OU分开。

基层管理员（helpdesk）只需要有改密码和解锁用户的功能。

微软建议的子域的数量并不是越多越好，一般不超过2层。

## 账号申请流程的控制

- ◆ 审批流程和工作流控制的网站程序
- ◆ 重要用户属性的输入，并自动加入到AD中
  - 职称、上层经理等信息由公司同意控制
  - 联系方式、办公地址等可自行开发程序由用户来更改
- ◆ 信息更改的流程和及时的同步到AD中

在变更AD账号信息的时候，IT处于被动的角色的，需要人事的批准才可以更改的，工程师是不能擅自更改的，信息是由公司来控制，由人事登陆到特定的网站，来更改相关的信息。

需要一套程序，来自动把需要修改的属性信息同步到AD中。**信息的完善是后续做管理和查询的基础。**

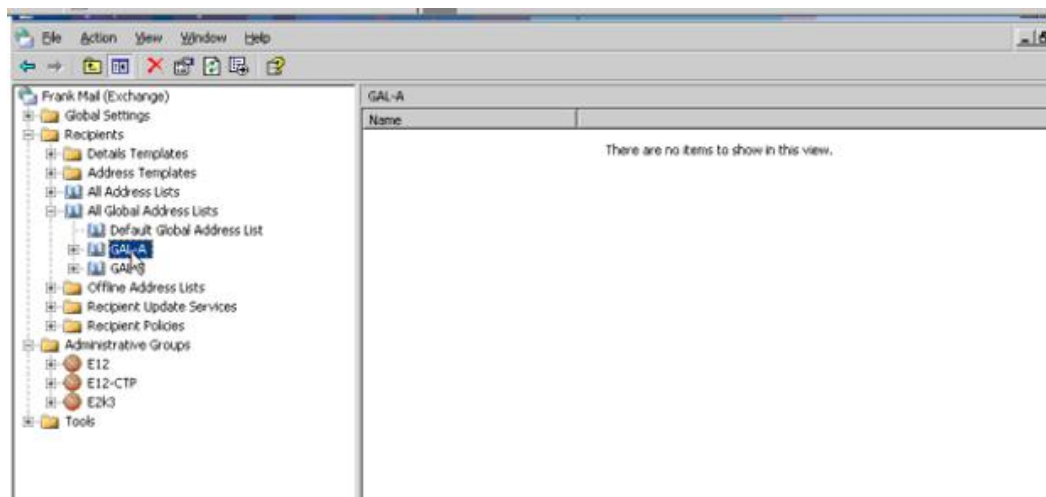
## 案例：员工离职的账号处理

- ◆ 帐号：禁用还是删除？
  - 禁用，过了一定时间后再删除
  - 或者重设密码使他人无法登陆
- ◆ 邮箱：保留还是删除？
  - 如果有后续业务往来邮件，可保留邮箱并开放权限给他人
  - 一般只开放只读权限，禁止发送和更改内容
  - 如果有重要邮件需要移交，可直接把邮箱转移到继任者名下，或者Exmerge导出

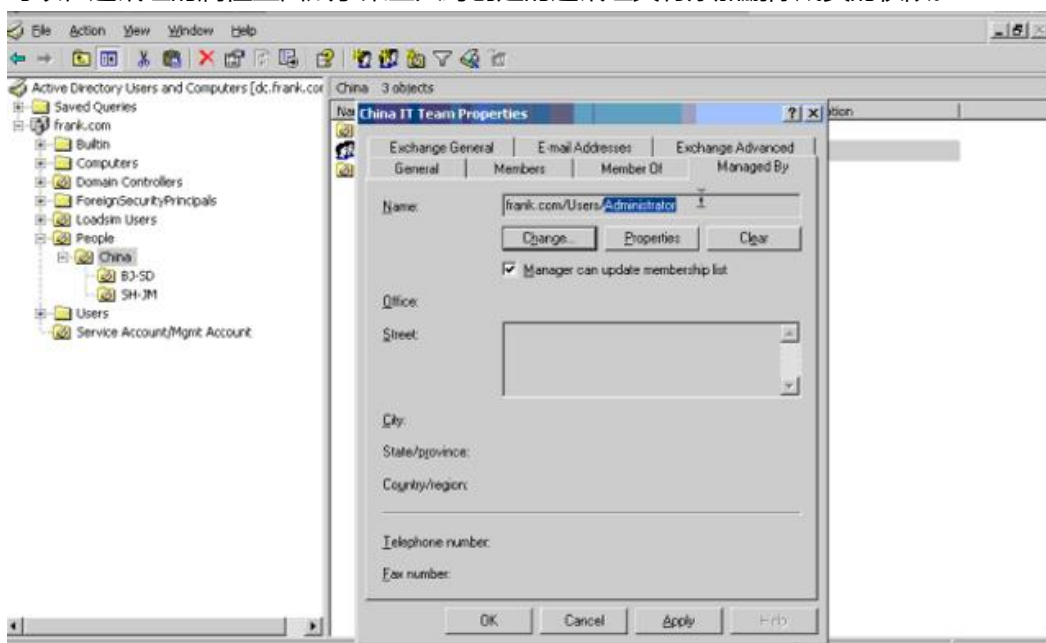
避免服务账号和非用户账号显示在地址簿之中。

display name的自定义设置。

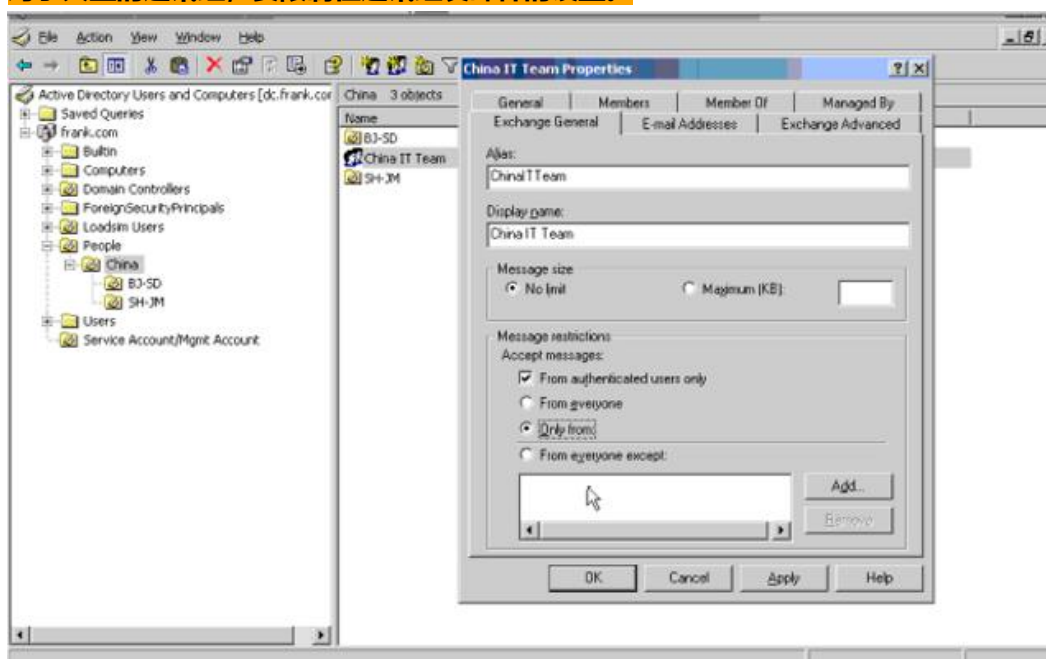
exchange server 2003自定义GAL，查询条件属于A或者B公司，然后控制GAL的访问权限，可以实现不同的人看到不同的地址簿，如图。



安全组是具有SID的，可以赋予权限的，而distribution组呢，只能包含用户，没办法设置权限。  
可以在通讯组的属性里面赋予某些人对创建的通讯组具有添加删除成员的权限。



**对于大型的通讯组，要限制往通讯组发邮件的设置。**

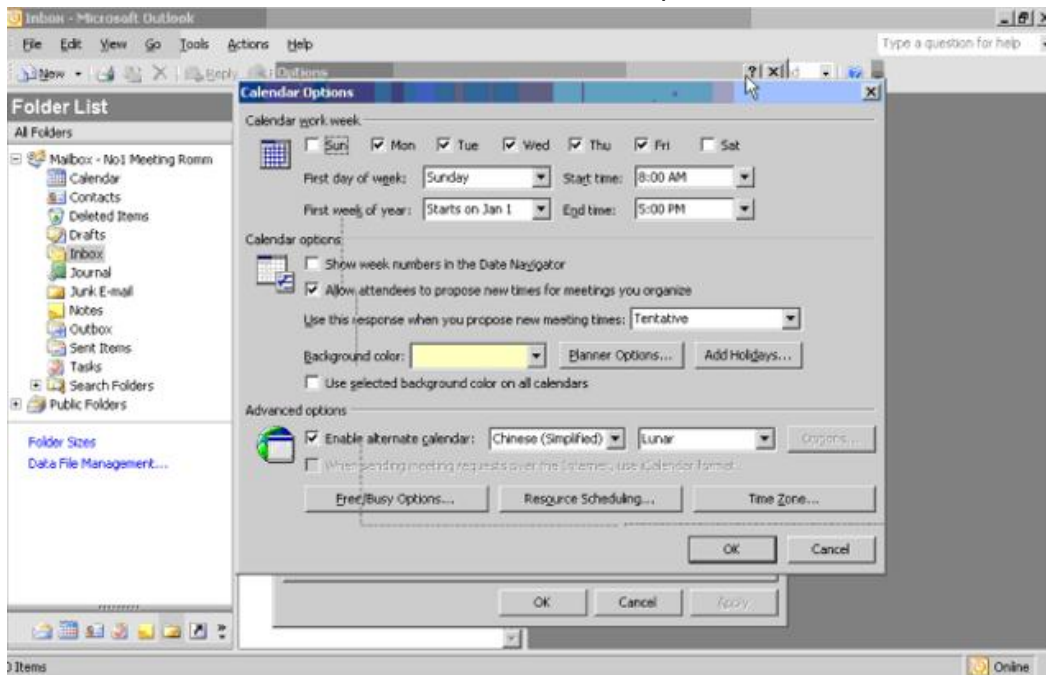


邮件组能够反映组织结构，能够便于传播和广播信息。对重要的组进行发送权限的控制。  
autogroup自动创建组工具。

资源账号：用户共享会议室和其他资源，可以在outlook中进行订阅。

**管理员可以使用outlook客户端登陆到会议室邮箱里面，做进一步的自定义的设置。**

设置会议室邮箱自动接受或者拒绝请求。在calendar options里面选择resource scheduling



在resource scheduling里面还可以设置权限set permission，配置哪些人可以查看会议室的忙闲等信息。

