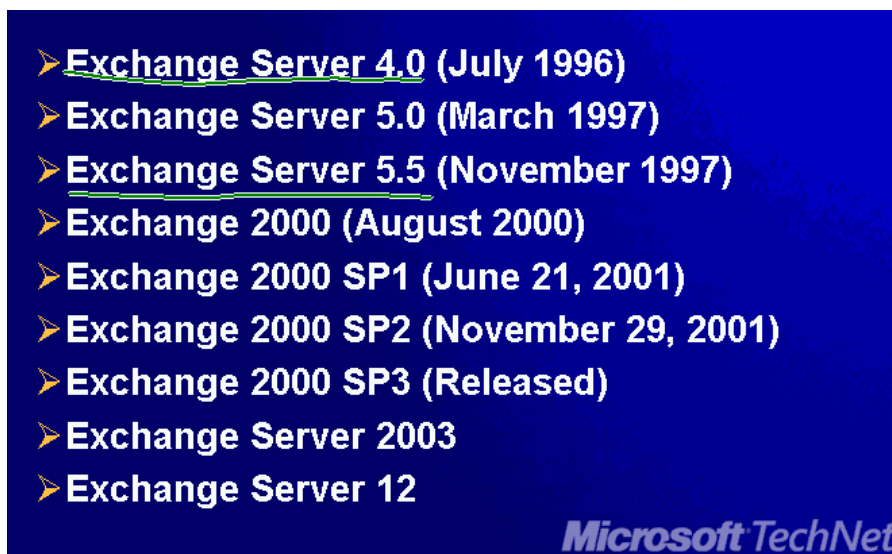


第一节：规划与部署

windows server 2003时代的体系结构



exchange 的发展历史



9. exchange server 5.5引入了目录服务系统

10. exchange server 2000目录服务系统玻璃出来，后来发展为目录服务AD

11. exchange 2003和exchange 5.5的区别在于exchange 5.5自带活动目录服务

12. 2000和2003主要是功能上的区别，结构一样

13. 而早于2000的版本，除了功能，结构也不太一样的

14. 出色的用户管理能力：与活动目录的高度集成、增强的用户账号管理工具。

15. 可开发的消息协作系统：Forms, Front page extensions; CDO; ADO; OLEDB; Events, workflow

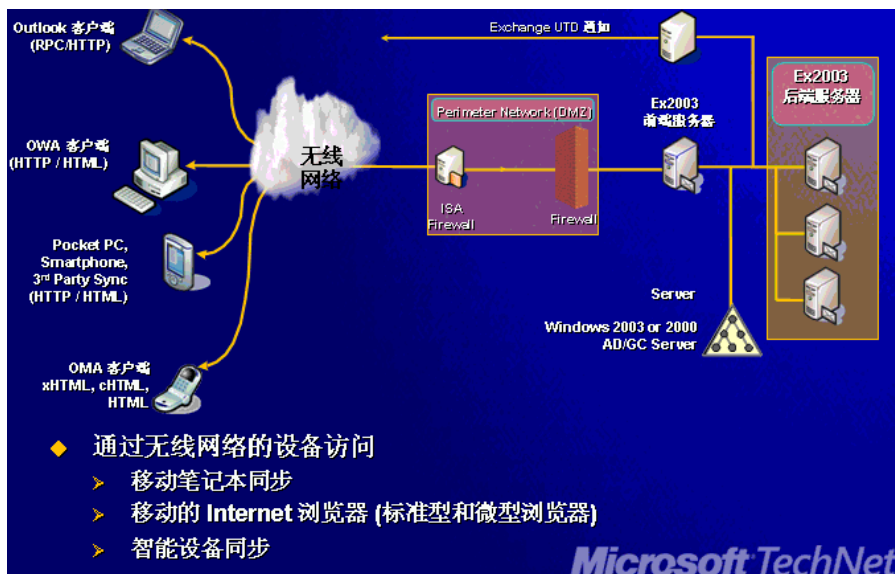
16. 内置了邮件的web接入方式：OWA

丰富的接入方式

4. exchange 2000上面还有实时协作的版本，包含会议服务器的版本，到2003里面就砍掉了，就是专门做异步协作

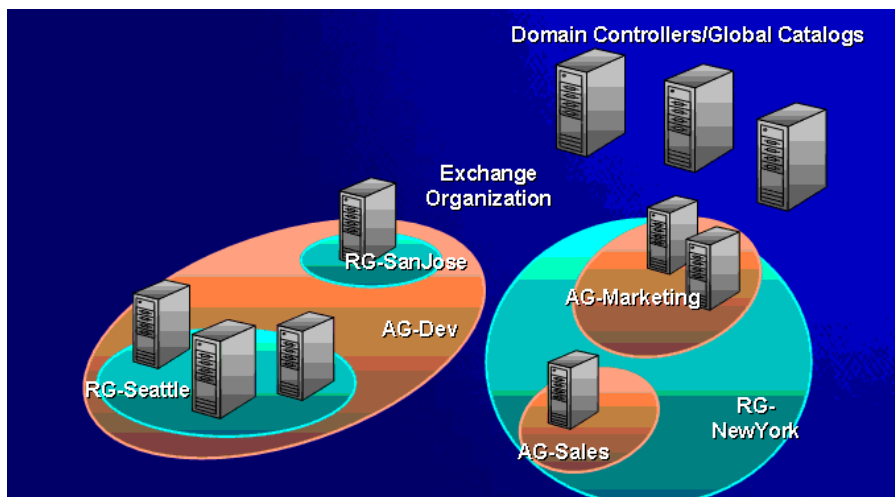
5. 之前对于移动设备的支持需要二次开发或者购买第三方的产品，而现在是内置功能

6. 通过活动目录实现账号管理以及存储exchange的配置信息

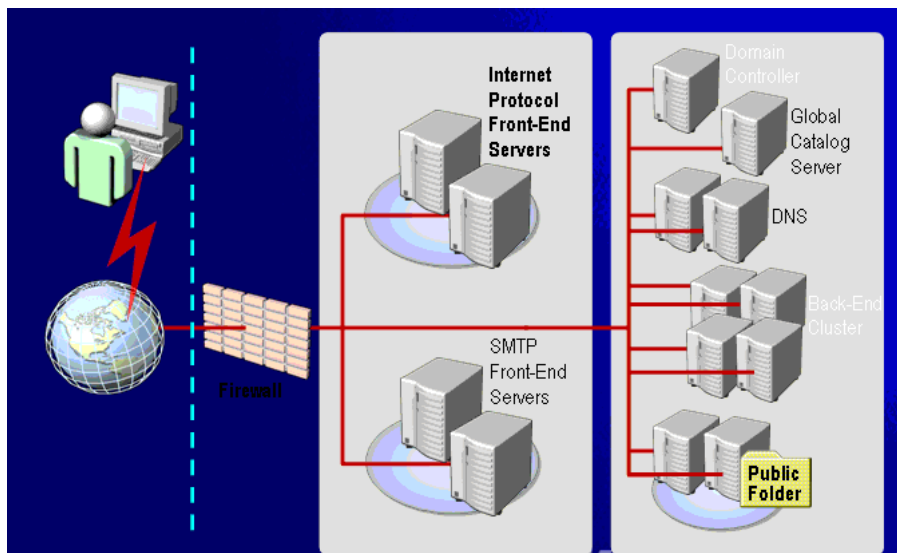


外部架构概述

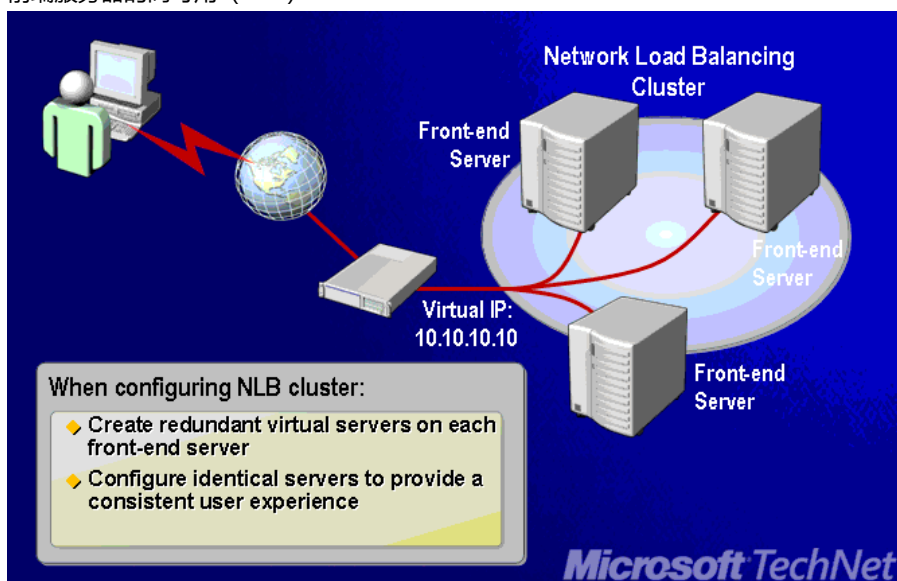
4. organization组织，部署的时候会提示新建exchange组织还是加入现有的组织，实际上是活动目录里面的一个容器，所有exchange的配置信息都在这个容器里面，对应AD的配置分区中的exchange分区，部署的时候会问我们当前有没有exchange组织，也就是AD中有没有现存的exchange容器，**一个活动目录只能有一个exchange组织**
5. administrative group管理组AG，是一系列exchange对象的逻辑性的组合，与网络链路无关，是权限细化的一个基本单元，在组织上右键，可以选择委派控制，为组织指派不同权限的管理员，权限是组织级别的范围的，我们可以再管理组级别去指派权限，管理员的权限仅仅限于管理组节点下面的组件，例如服务器，路由组，共用文件夹等
6. routing group路由组RG，是一系列具有可靠网络连接的exchange服务器的组合，大型企业在不同地区都有不同的服务器，通过一系列的高速可靠的链接连接起来，路由组定义了一组exchange服务器，这一组服务器之间有可靠的连接，在通信的时候不受任何限制，但是如果邮件跨路由组连接，则要受到路由组的限制，比如SMTP connectors



3. site站点（这是exchange 5.5的概念，等同于AG和RG），exchange5.5用站点作为管理整个组织的基础
4. front end server前端服务器，不负责数据库的处理，不管是前端还是后端，一定会运行DSAccess，只负责transport传输，以及客户端的访问，实际上用户直接同前端打交道，前端跟后端打交道，降低了后端服务器的负载，但是并不意味着前端服务器一定不运行information store，如果是SMTP的server，即使是前端服务器，也要运行information store，只是没有用户也邮箱，对于面向Internet的前端，可以没有information store



前端服务器的高可用 (NLB)



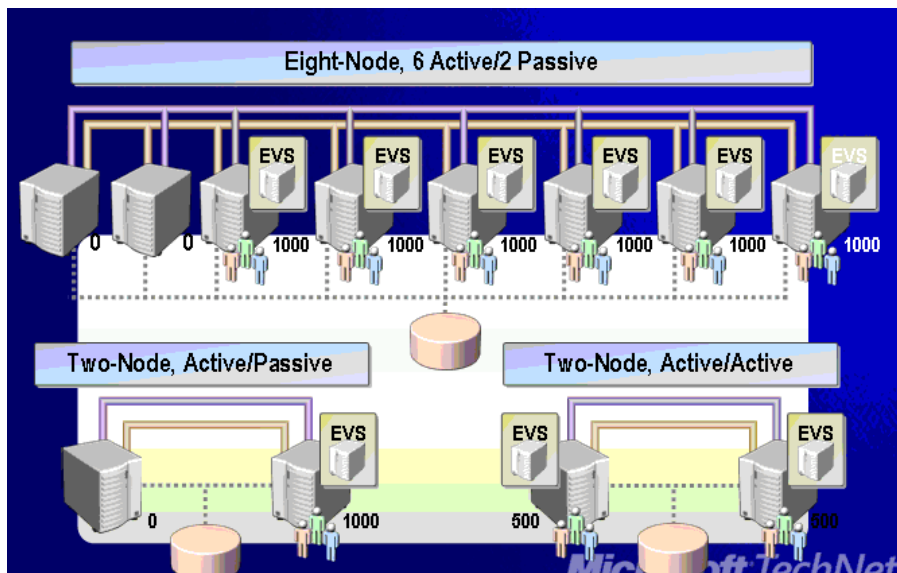
2. back end server后端服务器

后端服务器的高可用群集，故障转移，A/P模式或者A/A模式

主动/被动模式的资源利用率不高

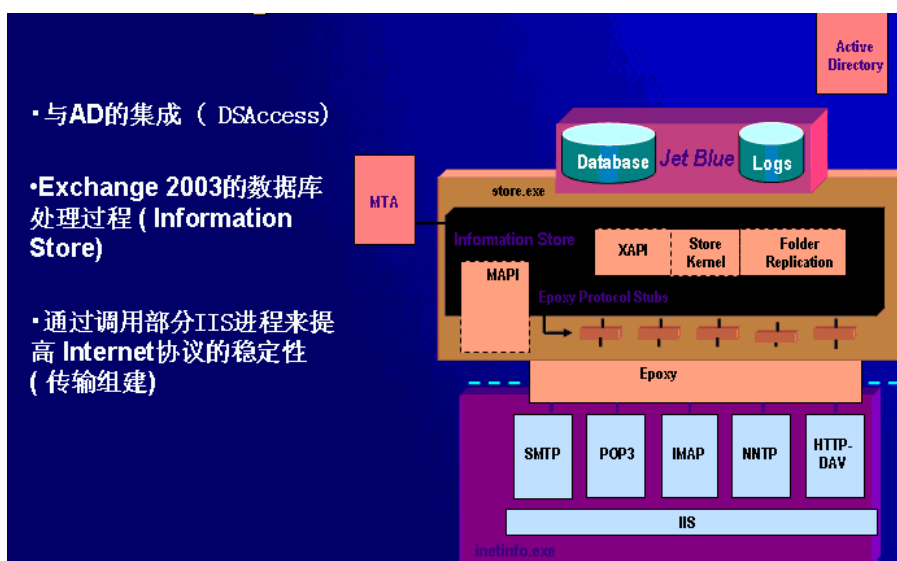
A/A模式利用率高，但是可用性会有影响，一旦一个节点失败，那么服务器都会转到一台机器上
在一台物理服务器上，只能支持4个存储组

使用SCSI共享磁盘只支持两个节点的群集，DAS设备做不了，推荐ISCSI或者SAN



exchange 2003内部架构

4. DSAccess主要负责同活动目录的集成，身份标识信息都放在AD里，统一身份标识，DSAccess去获取活动目录信息等
5. information store，下图的store.exe里面黑色的部分，数据库存储，存储用户收件箱、日历、联系人信息
6. 传输组件，提供MAPI接口（outlook通过MAPI方式），然后通过Epoxy同IIS进行沟通，利用IIS的SMTP/POP3/IMAP/NNTP/HTTP-DAVA



服务器可以在路由组之间移动，但是无法在管理组之间移动，所以在部署前一定要规划好，一旦把服务器指定到特定的管理组，就不建议再调整了。

安装exchange 2003的时候，可以选择安装一些可选组件，同第三方的邮件系统互联

- **Microsoft Exchange Messaging and Collaboration Services**
 - Microsoft Exchange Connector for Lotus Notes
 - Microsoft Exchange Connector for Novell GroupWise
 - Microsoft Exchange Calendar Connector
- **Microsoft Exchange System Management Tools**
 - Microsoft Exchange 5.5 Administrator

使用POP3/IMAP这种Internet的协议和客户端，只能使用部分exchange的功能，而使用MAPI客户端可以使用exchange的所有功能。

超过三个节点一定要有一个被动节点，只能配置A/P群集。

两个节点可以使用A/A群集。

第二节: exchange 2003部署与体系结构

8. dcdiag一般是在DC上运行，他会测试DC的架构分区和配置分区，这个对exchange会有影响的，也会测试系统日志是不是有异常，如果系统日志有错误，也不代表会影响exchange的安装。

9. netdiag可以在客户端或者成员服务器上运行；

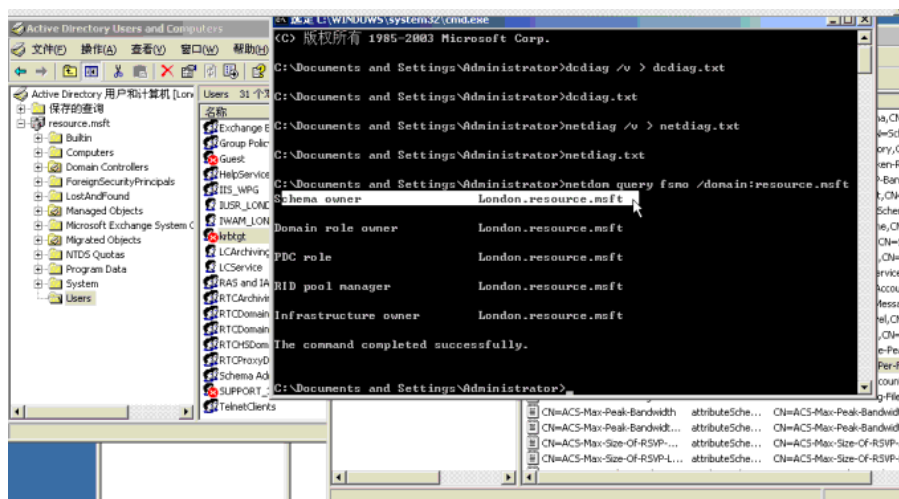
10. AD UC对应于domain分区。

11. AD SS对应于配置分区下的site

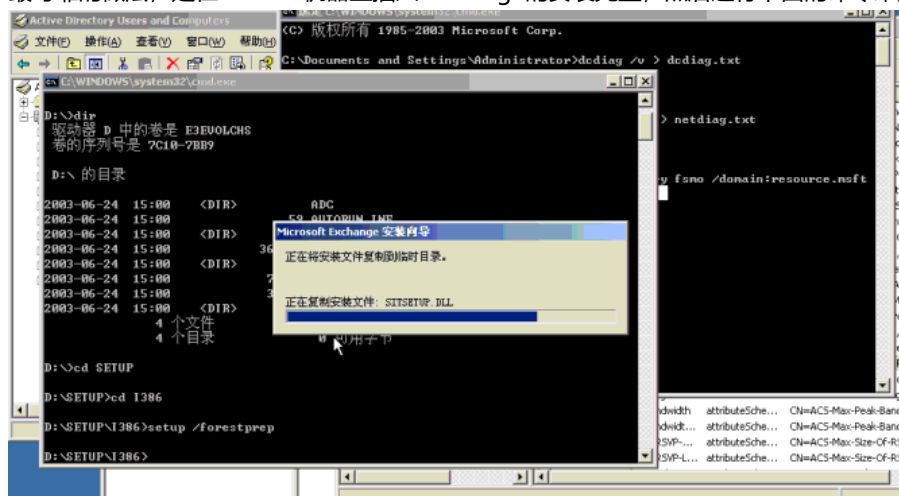
12. AD架构对应于架构schema分区

13. 默认只有schema admins可以修改架构，而默认只有默认的builtin的administrator属于schema admins

14. 那么默认会在哪台DC修改schema呢？默认永远只能在一台DC修改schema，我们可以通过下面的命令来查看哪台DC是schema owner



最可靠的做法，是在schema机器上插入exchange的安装光盘，然后运行下面的命令来扩展架构



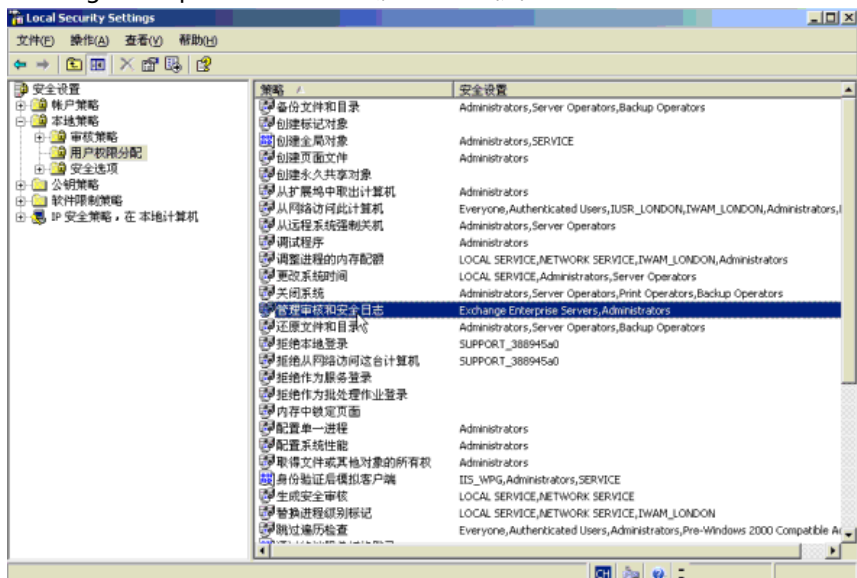
DC上面的remote registry一定不能停，否则exchange扩展不了架构，也装不上去。也可以在其他DC上扩展架构，但是要考虑DC的负载和之间的网络情况。

在安装光盘里有schemaLDF的文件，架构准备是把这些文件导入到AD中。

如何验证schema是否扩展成功？在架构中找到cn=ms-schema-version-Pt，然后在这个值的属性中找到rangeupper的值为6870

域扩展会建两个组：exchange domain server和exchange enterprise server（域内所有的exchange服务器都会属于这个组）

exchange enterprise server一定要属于管理审核和安全日志这个组



域扩展还会修改windows用来为本地domain administrator组的成员设置权限的adminsldholder模板

在域的根位置设置exchange enterprise servers组的权限，使收件人更新服务有正确的权限来处理收件人对象

创建“exchange系统对象”容器（exchange system object），该容器用于存放已启用邮件的共用文件夹

将全局exchange domain servers组嵌套到exchange enterprise server组中

如何确保域扩展已完成？运行安装光盘support\exdeploy下面的polcytest.exe程序，如果结果right found已找到，则代表域扩展已经完成

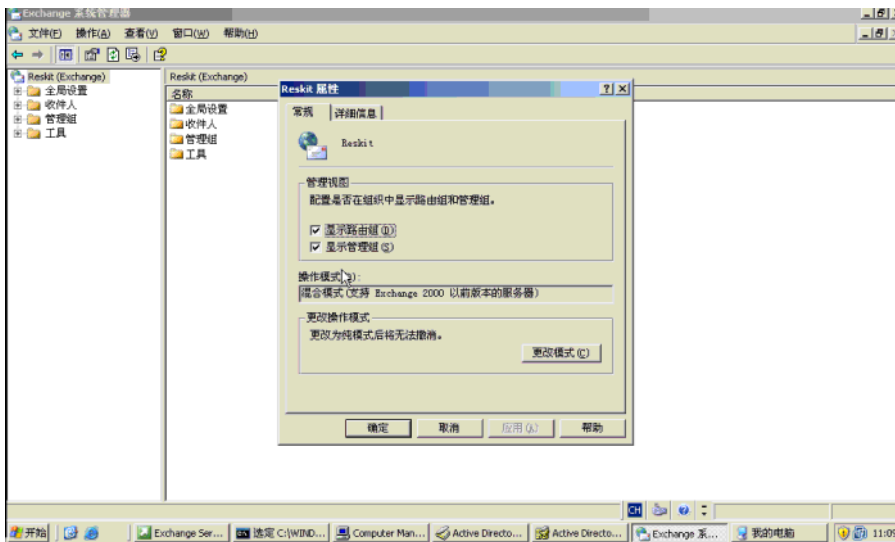
exchange的两个组默认的位置不要改变，否则exchange会有问题。

域扩展在每个域都要做，而架构扩展整个森林只做一次

- 正确安装和配置Active Directory和DNS（require）
- 有相应的Active Directory访问权限（企业管理员和架构管理员）
- 服务器加入Active Directory域
- 属于同一个ORG的Exchange服务器在相同的AD森林里
- 在升级Windows Server 2003之前安装Exchange 2003
- 系统必须是Windows 2000 SP3以上或Windows Server 2003系列
- 运行ForestPrep（Schema拓展和Configuration拓展）
- 指定一个Exchange Full Administrator用户帐号
- 安装Exchange之前创建Exchange管理组结构（先forestprep，再装esm，就可以在安装exchange前设定管理组，因为默认情况下所有服务器都加入第一个ag，且服务器加入ag后不能再移动）
- 运行DomainPrep（添加Exchange Domain Server和Exchange Enterprise Server）
- 安装和配置相应服务（www,smtp,nntp）

exchange 2003的管理工具室“exchange系统管理器”

默认情况下exchange系统管理器是不显示管理组和路由组的，需要我们在下面的位置勾选

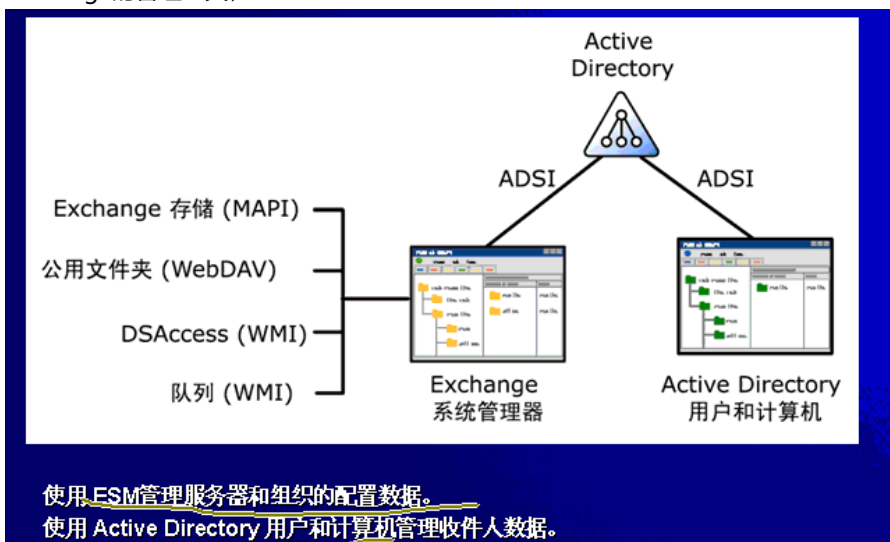


可以新建管理组，新建路由组

也可以通过windows explorer (drive M) 来验证exchange是否安装成功，exchange 2003已经不使用M盘，我们可以使用 subst \\.\backackom: /d来挂载M盘，从而可以直接通过文件系统来访问exchange的数据库

不要显示M盘，否则有可能磁盘管理工具或者杀毒软件，第三方碎片整理程序会搞坏M盘

exchange的管理工具，



exchange的系统管理器可以做什么

容器	描述
全局设置	包括用于配置系统范围设置的功能。这些设置应用于 Exchange 组织中的所有服务器和收件人。
收件人	包括用于管理组织中的收件人对象和设置的功能。您可以管理地址列表、脱机地址列表、收件人更新服务、收件人策略、邮箱管理设置、详细信息模板和地址模板。
管理组	包括用于管理管理组的功能。每个组都是为权限管理而组织在一起的 Active Directory 对象的集合。每个管理组都可以包含策略、路由组、公用文件夹层次结构以及服务器。
服务器	存放服务器特定的配置对象，例如队列、邮箱存储、公用文件夹存储以及协议信息。
系统策略	包含影响系统配置设置的策略。策略是应用于 Active Directory 中一个或多个 Exchange 对象的配置设置的集合。
路由组	定义 Exchange 服务器的物理网络拓扑。Exchange 邮件系统或组织包含一台或多台运行 Exchange 的服务器。除非您规划的是小型 Exchange 安装，否则可能会有多台 Exchange 服务器。在某些组织中，这些服务器通过可靠的永久连接相连。以这种方式链接在一起的服务器组应组织到同一个路由组中。
文件夹	显示公用文件夹层次结构。公用文件夹用于存储可以被组织内所有指定的用户共享的邮件或信息。公用文件夹可以包含从简单邮件到多媒体剪辑、再到自定义表单等各种类型的信息。
工具	包含有助于您监视 Exchange 组织、跟踪邮件以及恢复邮箱的工具。

收件人更新服务可以更新收件人策略，收件人策略里面可以设置用户的多个电子邮件地址。

使用 Exchange 系统管理器执行下列操作	使用 Active Directory 用户和计算机执行下列操作
管理 Exchange 组织。	管理 Active Directory 对象 (收件人)。
管理服务器。	管理用户。
将所有邮箱从一台服务器移动到另一台服务器。	将单个用户的邮箱从一台服务器移动到另一台服务器。
创建公用文件夹。	创建通讯组。

可能会使用或者涉及到的exchange管理工具如下

- ◆ Exchange System Manager
- ◆ Active Directory Users and Computers
- ◆ Cluster Administrator
- ◆ ADSI Edit
- ◆ LDP utility
- ◆ Active Directory Schema snap-in
- ◆ IIS snap-in
- ◆ DNS snap-in
- ◆ ESEUTIL / ISINTEG
- ◆ Windows Support Tools
- ◆ Exchange All Tools Pack
- ◆ ExchMBX

ExchMBX是exchange的命令行管理工具，是MVP写的。

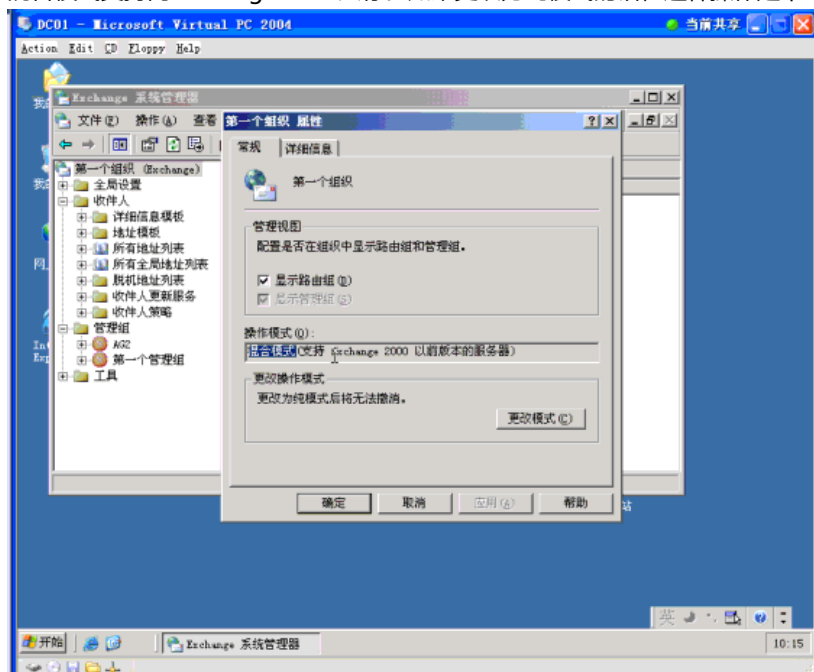
为什么exchange上面的ADUC可以看到exchange的属性，而AD上的ADUC看不到呢？因为exchange的ADUC和AD的ADUC是不同版本的。解决的办法是可以到AD上安装exchange的管理工具。

exchange 2003的邮件跟踪不能用，有可能是邮件跟踪依赖的日志共享文件夹不可访问或者权限被修改。

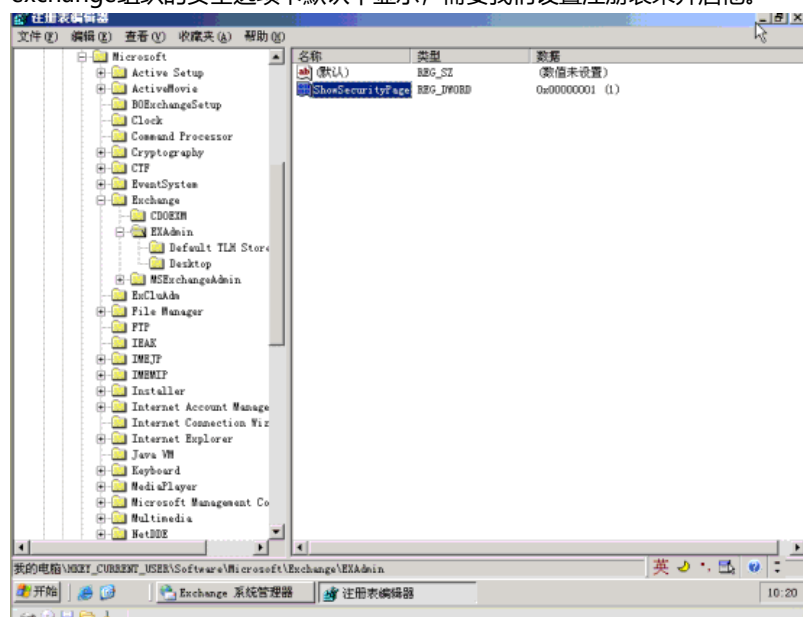
第三节：管理exchange组织和服务器

如果存在多个exchange的管理组，那么下图的管理组复选框就是灰色的。

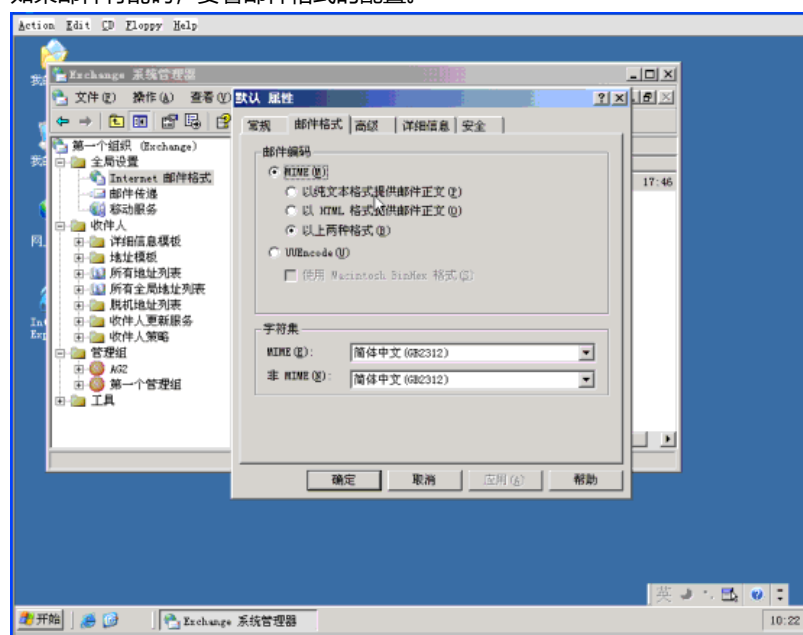
混合模式支持同exchange 2000共存。如果更改为纯模式的话，这种操作是不可逆转的。



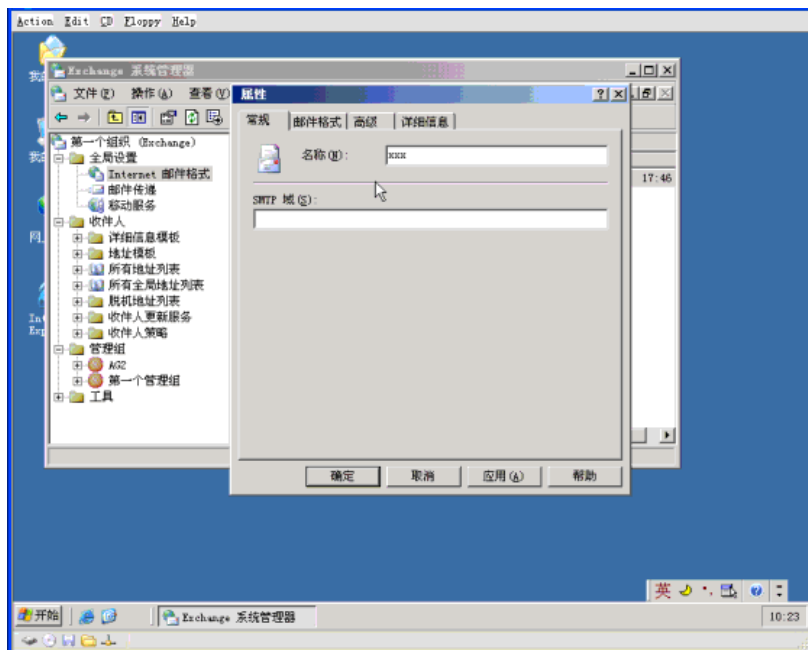
一个管理组下面可以有多个路由组，但是路由组是不能跨多个管理组的。但是在纯模式下路由组之间是可以移动服务器的，而混合模式为了兼容早期的服务器，兼容“站点”的概念，就不能移动服务器。
exchange组织的安全选项卡默认不显示，需要我们设置注册表来开启他。



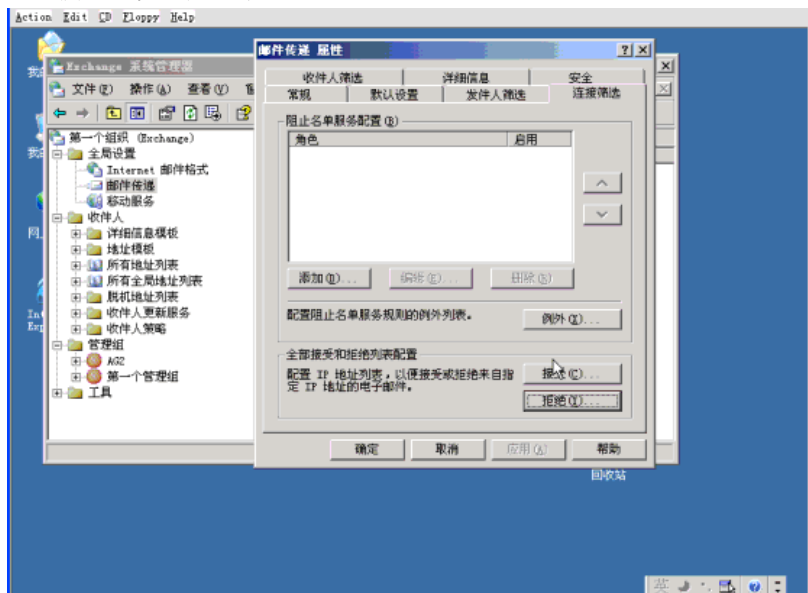
如果邮件有乱码，要看邮件格式的配置。



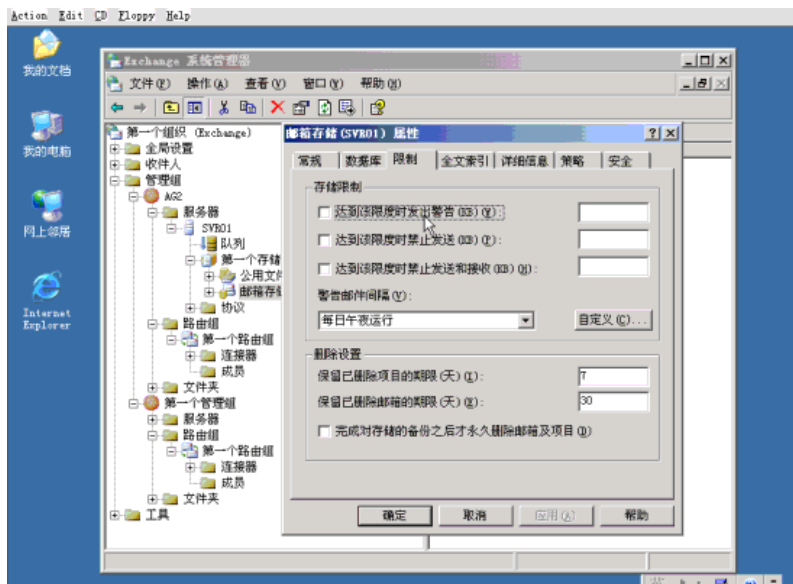
可以右击“Internet邮件格式”选择新建域，为不同的域配置邮件格式，字符集等等。



组织级别的邮件传递选项。



邮箱存储选项卡。



当企业规模比较大的时候，需要注意安全性的管理，进行权利的分配，不同地区的管理员的权限分配。

exchange的权限类型

Standard Permissions

- Full control
- Read
- Write
- Delete
- Read permissions
- Change permissions
- Take ownership
- Create children
- Delete children
- List contents
- Read properties
- Write properties
- List objects

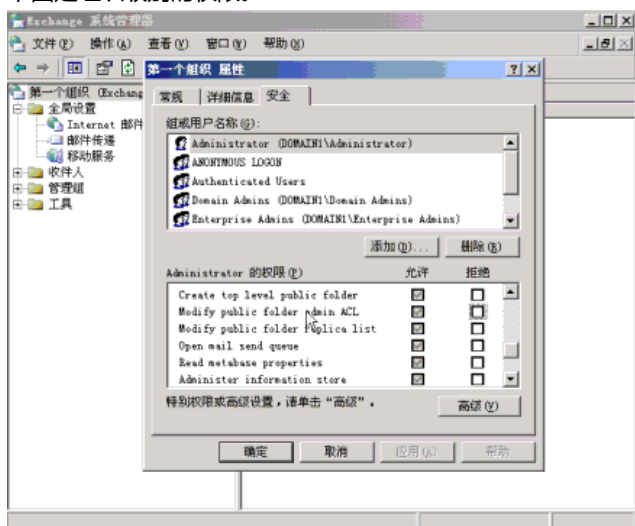
Extended Permissions

- Add PF to admin group
- Create public folder
- Open mail send queue
- Read metabase properties
- Administer information store
- View information store status
- Receive As
- Send As

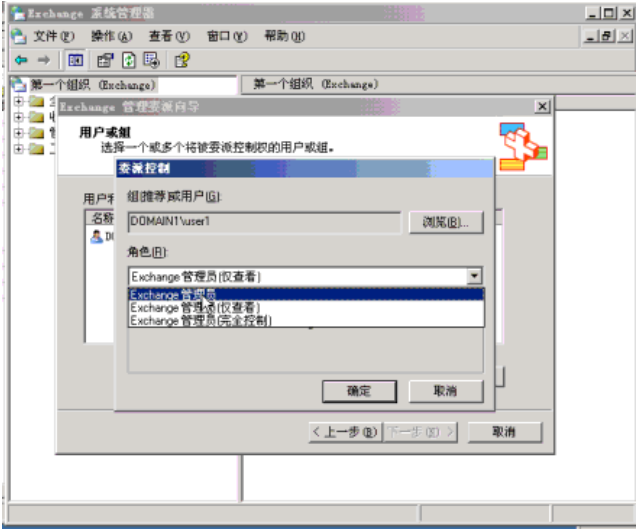
<http://www.microsoft.com/china/technet>

exchange有很多对象，对象提供很多功能，每种功能对应不同的权限。

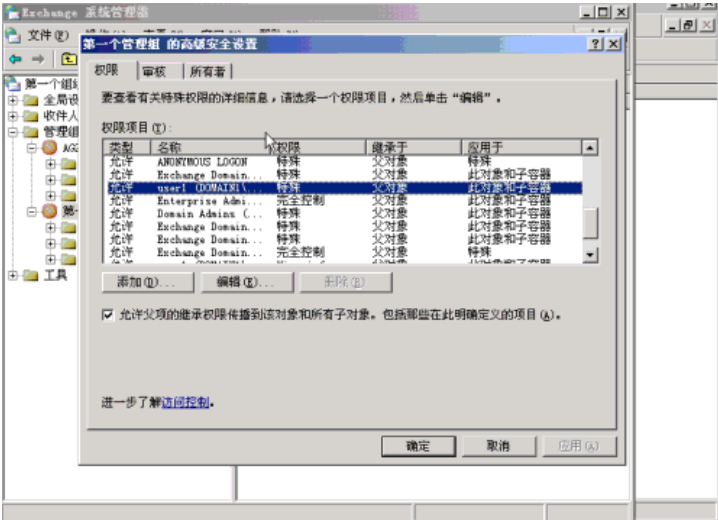
下图是组织级别的权限。



在组织级别和管理组级别都可以进行权限的委派。把这些委派同AD账户的委派结合起来，比如在AD里面委派用户只能在人力资源部OU进行管理，比如新建用户，修改密码等。



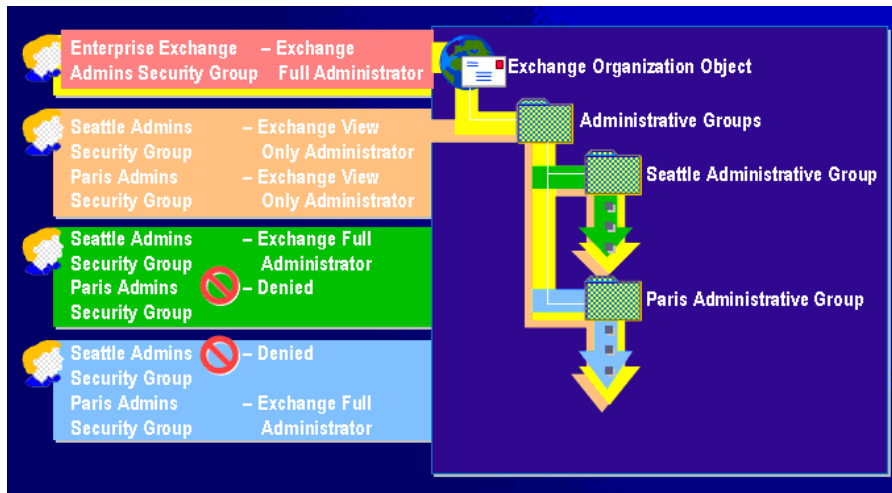
下图user1的权限是从父对象继承的，也就是user1的权限是从组织级别继承的。



当然我们也可以打破这种继承。
建议大家使用基于角色的权限控制，不建议直接去修改安全属性页面。
可以委派的三种角色：

Permission	What you can do	Delegate this role to
Exchange Full Administrator	配置Exchange系统，包括修改权限	对系统访问进行控制的管理员
Exchange Administrator	配置Exchange系统，不包括修改权限	进行日常维护的管理员
Exchange View Only Administrator	查看Exchange系统的配置	只需查看系统配置的管理员

使用委派的用户user1在客户端计算机上登录，然后使用AD用户和计算机工具去创建用户邮箱。

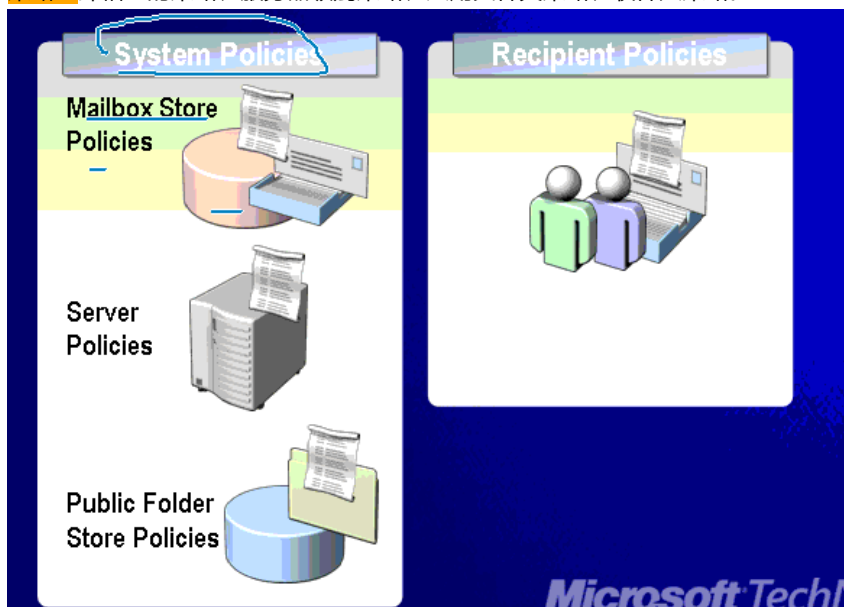


什么是exchange policy?

可应用到一个或多个相同exchange对象的一组配置的集合

使对大量exchange对象的管理更加方便和灵活

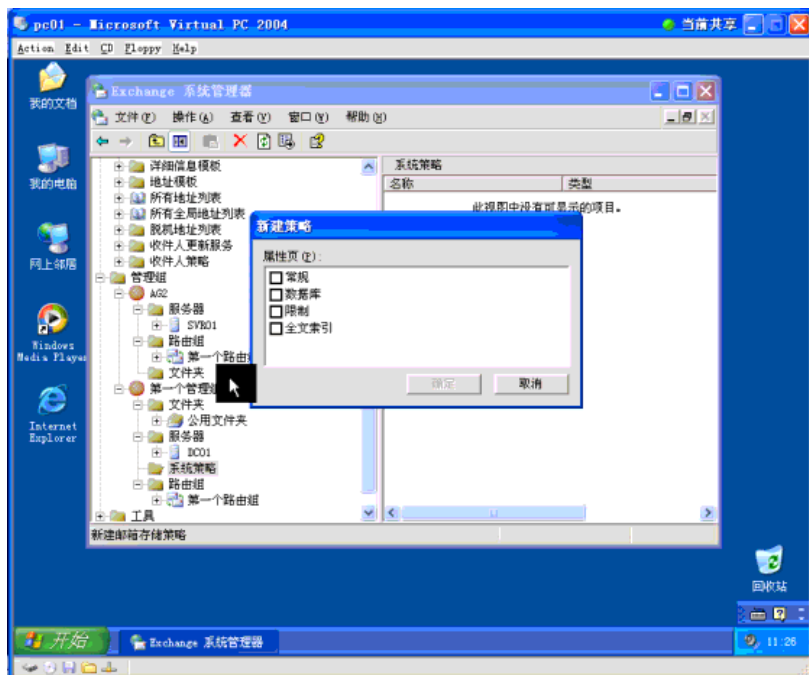
策略: 邮箱上的策略、服务器级别策略、共用文件夹策略、收件人策略。



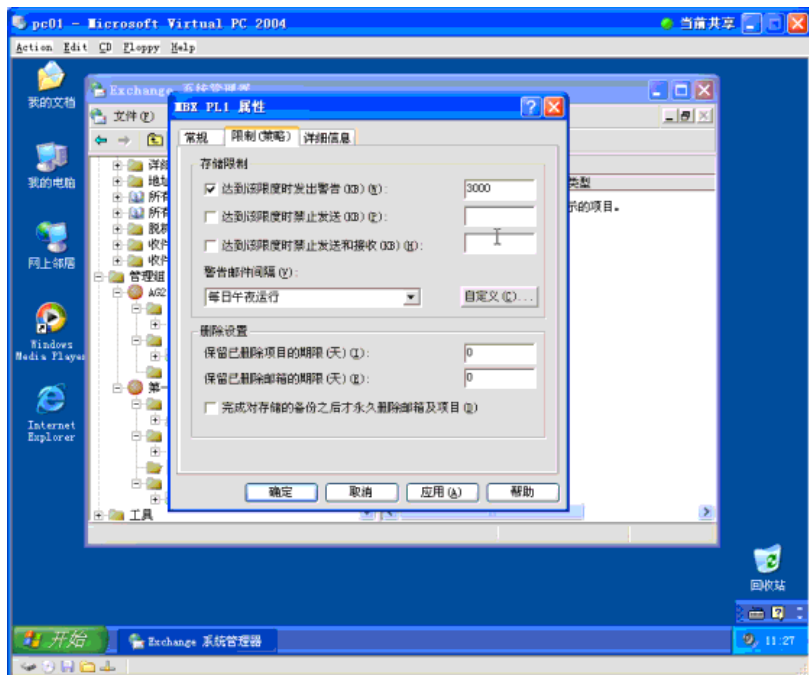
如何创建策略，前提条件

必要的权限	<ul style="list-style-type: none"> ◆AG或组织级别有“创建策略”的权限 ◆对策略要应用的对象有“写”权限
创建策略容器	<ul style="list-style-type: none"> ◆在每个AG创建“策略”容器
避免策略冲突	<ul style="list-style-type: none"> ◆可以通过减少策略绑定的属性页减少多策略冲突的问题，

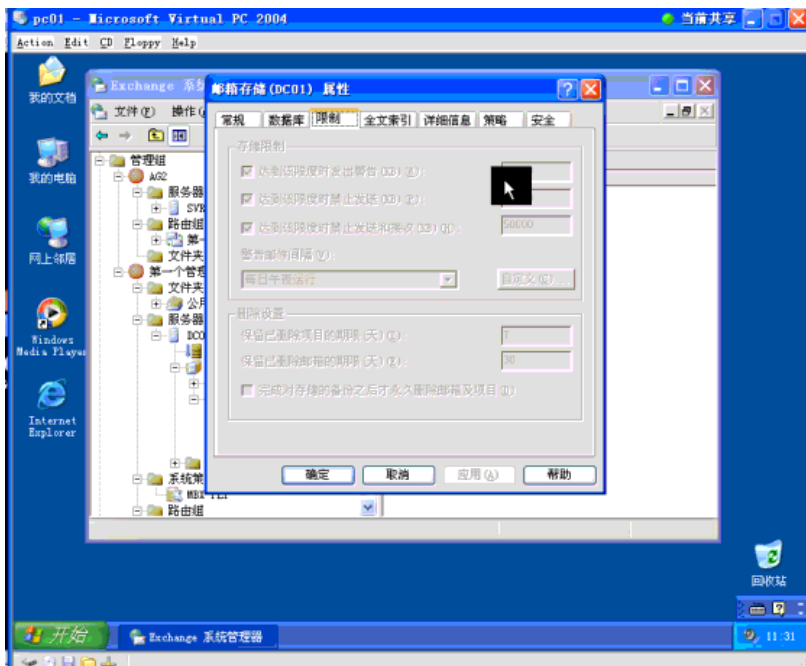
创建和应用策略



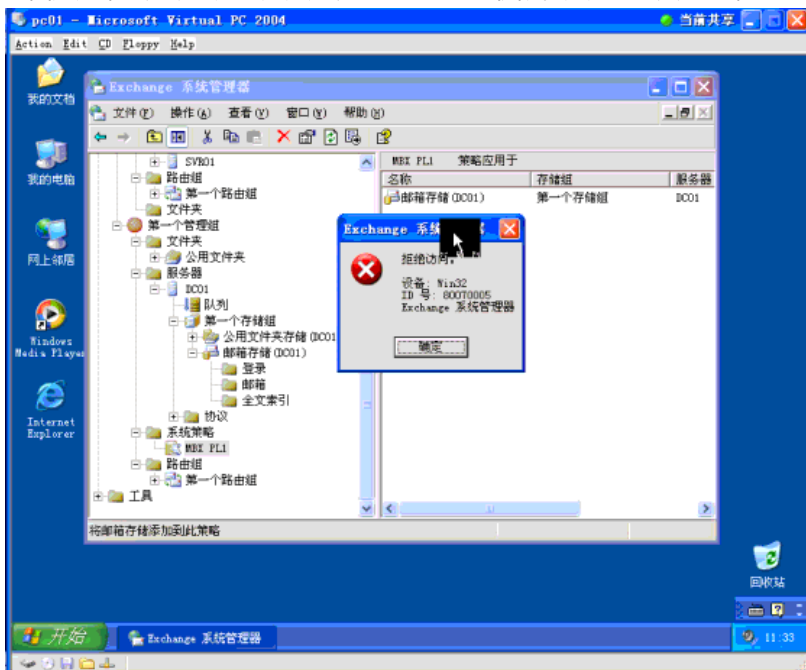
下图是设置限制策略的例子。




策略新建完成后，需要把策略应用到服务器上的DB上。
应用策略之后，邮箱存储的限制是无法修改的，由策略配置。



下图应用策略失败的原因是用户没有该管理组的权限，用户需要具有把策略绑定到特定对象的权限。



地址列表的定义：

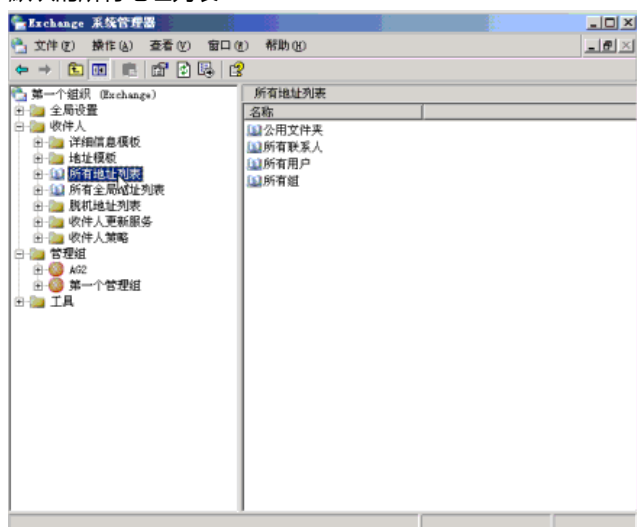


- 按照对象的目录属性归类的收件者对象的集合. **Address lists (AL)** :
 - 可包含多种类型的收件者对象
 - 对象是动态的
- 创建AL，方便用户快速定位其他用户

地址列表的类型

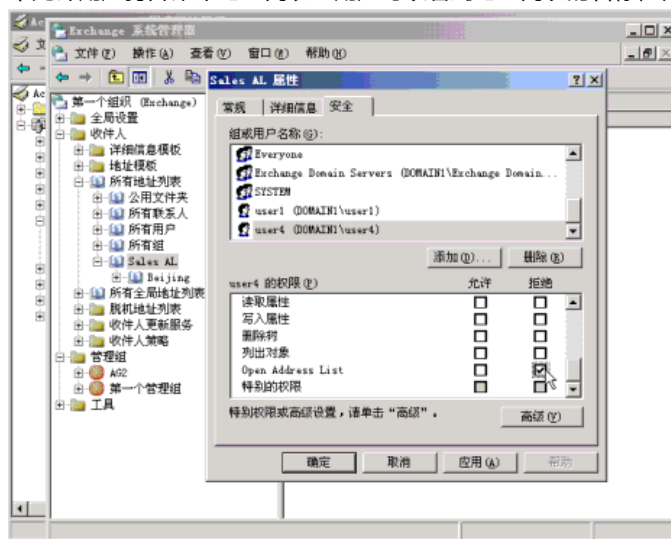
Type	Description	When to use it
Default	自动创建	用户无需定制的AL
Global	包括组织中所有的 recipients	用户可见的主要AL
Offline	可脱机使用的AL	是用户可脱机使用AL
Custom	根据需求定制的AL	是用户更加方便地使用AL

默认的所有地址列表：



可以通过outlook来查看这些地址列表

不允许用户打开某个地址列表：用户可以看到地址列表的名称，但是看不到里面的用户。



如果想让用户连地址列表的名称也看不到，那么可以创建一个空的地址列表，然后拒绝某个用户对该地址列表的读权限，然后把相应的地址列表拖动到这个空的地址列表中，那么用户不但看不到地址列表的用户，也看不到地址列表的名称。