

第四节：exchange 2003管理收件人

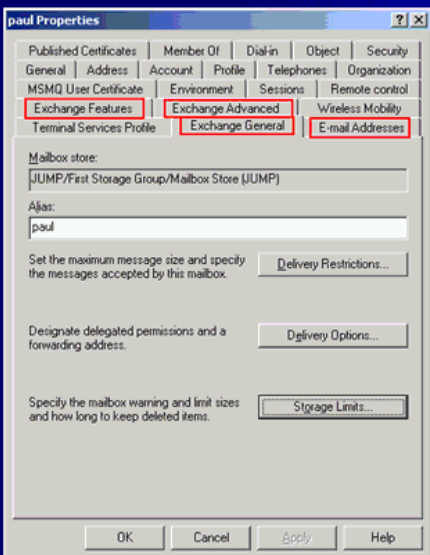
exchange server 2000收件人管理的特色

管理工具盒windows 2003 MMC 集成

4. MMC可以添加管理单元
5. ADUC对收件人的管理
6. 使用ESM管理单元对邮件系统进行管理

exchange 2000扩展的属性页：

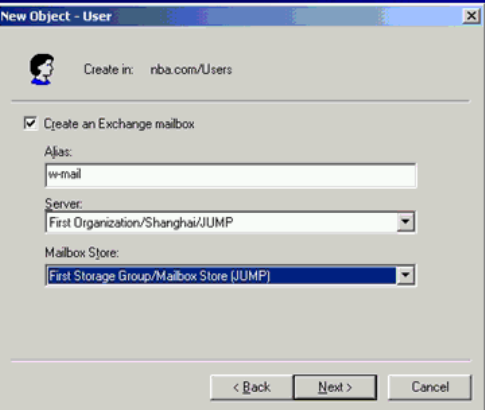
在exchange的属性页面里面可以做转发的操作。



- ◆ **Exchange Feature:**
用户具有哪些属性
- ◆ **Exchange General:**
常用的配置
- ◆ **E-mail Address:**
查看用户邮箱地址
- ◆ **Exch Advanced**
MMC->查看 -> 高级功能

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

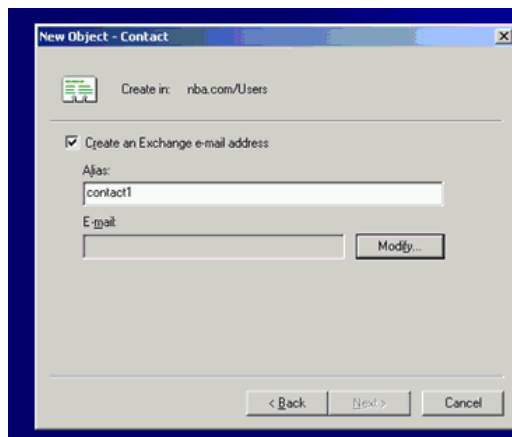
exchange可以创建带邮箱的用户、不带邮箱的用户（有AD账号，可以绑定外部的Email地址，创建一个外部的Email地址，这个用户虽然没有内部邮箱，但是在查找这个用户的时候，可以查找到他的外部邮件地址）、联系人、创建group



- ◆ **Username 和 Alias 的区别**
- ◆ **选择server**
“Org/AG/server”
- ◆ **选择Mailbox Store**

为了方便管理，邮箱的alias和登录名建议设置成一样的。

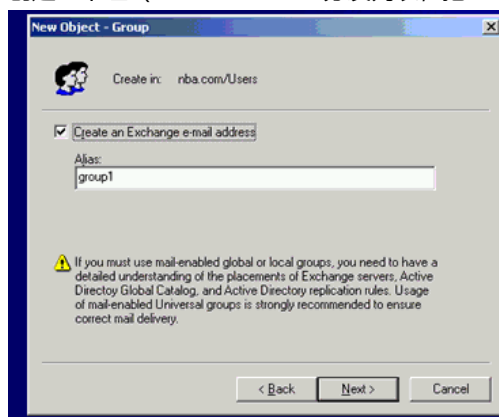
创建外部联系人（没有AD账号），可以关联外部的Email地址：



◆ **Contact:** 关联外部 email 地址

◆ **Ex2k中的Contact =Ex55中的Custom Recipient**

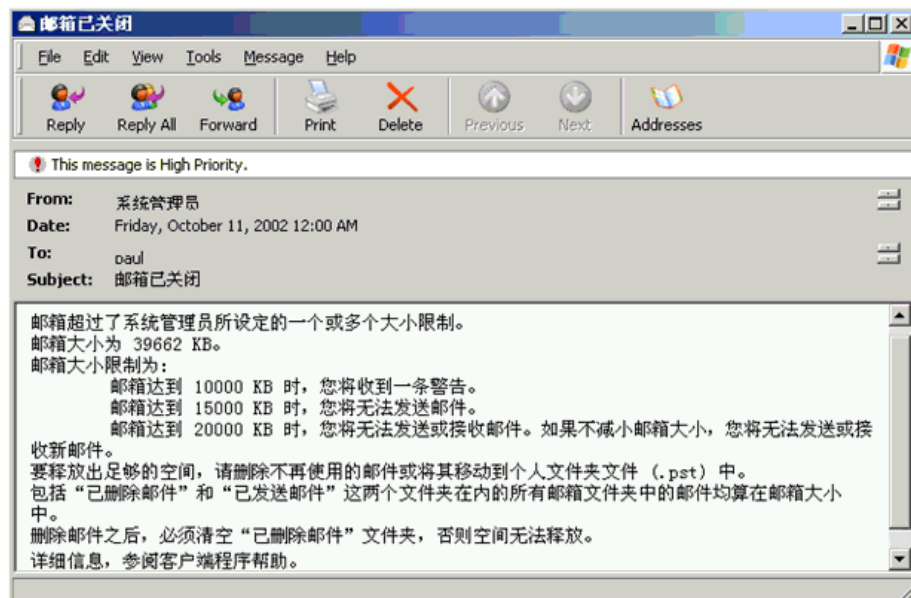
创建一个组（distribution list 分发列表，把一些人放到列表里）可以为组创建Email地址。



◆ **DL的作用**

◆ 把DL加入到**Public Folder**的的权限
ID no: 80004005
Q274046

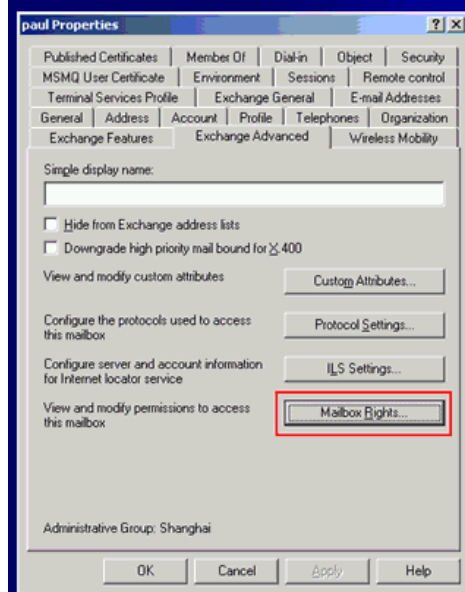
邮箱大小超过限制时的提示信息时可以修改的。



针对单个用户，赋予完全控制邮箱的权限，如图。

设置mailbox rights

针对单个用户配置



◆ Ex55 使用 **service account**

◆ Ex2k 使用 **ACL** 来授权邮箱权限

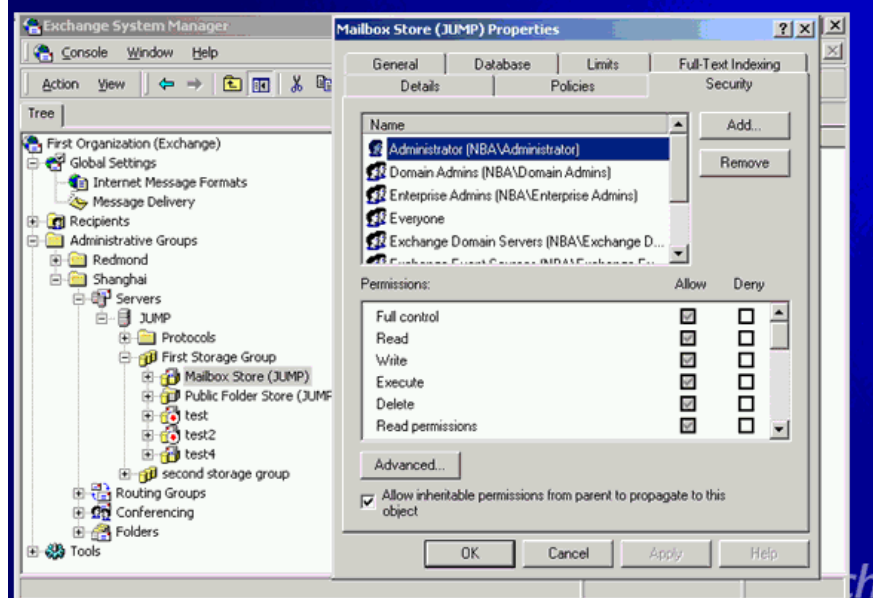
◆ Exchange Advanced Mailbox Rights

Q268754

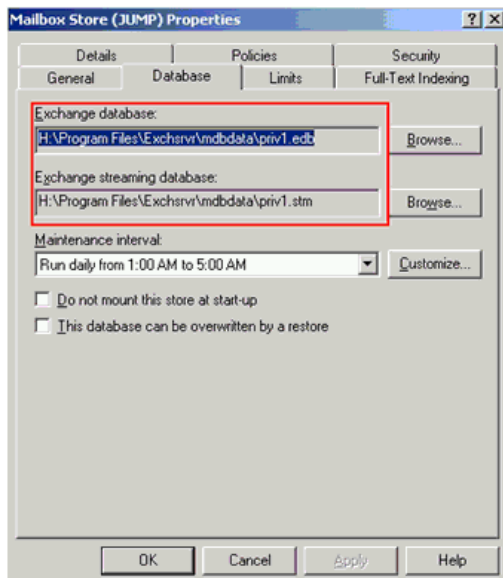
Microsoft TechNet
http://www.microsoft.com/china/technet

在mailbox store级别设置domain admins能够查看所有用户邮箱的权限。

针对Mailbox Store配置



如何移动数据库文件



如何防止垃圾邮件

不要把自己的Email地址放到网上发帖，论坛之中，以免被垃圾邮件组织利用，以免被收录到垃圾邮件数据库之中。
如果必须在网上用可以使用user#xxx.com把自己的Email地址伪装掉，让垃圾邮件系统检索不到。

◆避免在News Group(新闻组)使用邮件地址

◆使用SMTP Filter

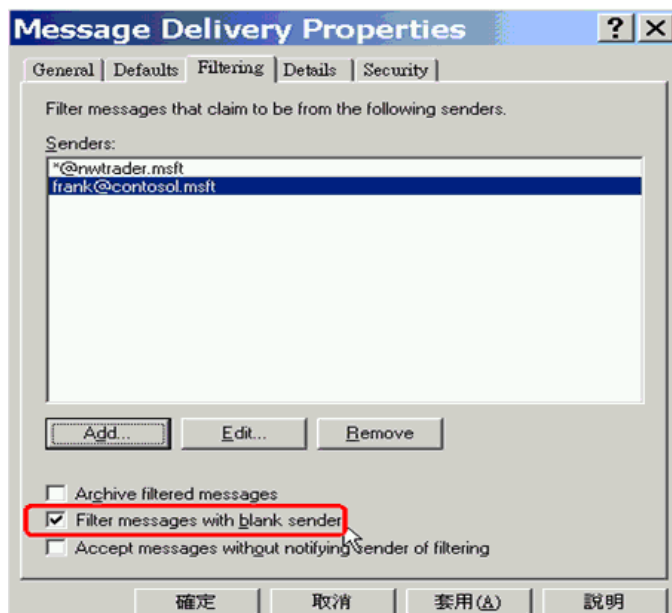
- 以e-mail地址过滤 (ex: tony@domain, *@domain)
- 过滤掉发件人是空白的邮件

◆使用IP地址限制

注：

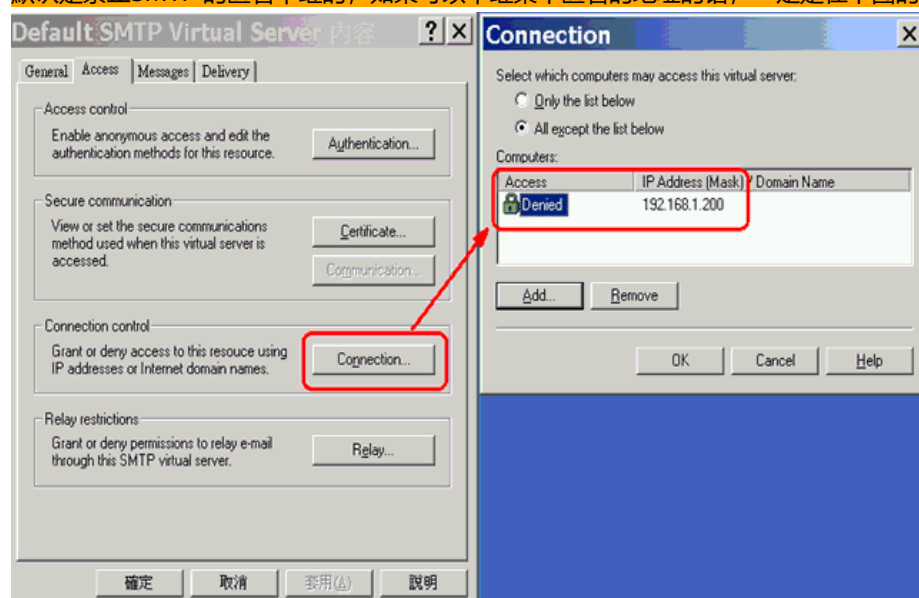
为避免产生太多的NDR，可以清除Global setting→
Internet Message Formats→ Default Properties→
Advanced→ Allow non-delivery reports的选项

SMTP筛选



限制IP连接

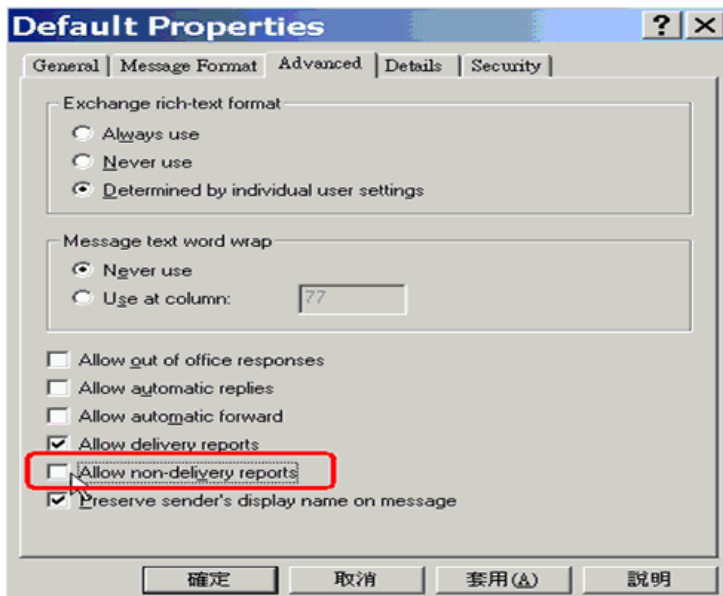
默认是禁止SMTP的匿名中继的，如果可以中继某个匿名的地址的话，一定是在下图的服务器中做过允许匿名中继的配置。



避免太多的NDR造成太多的queue

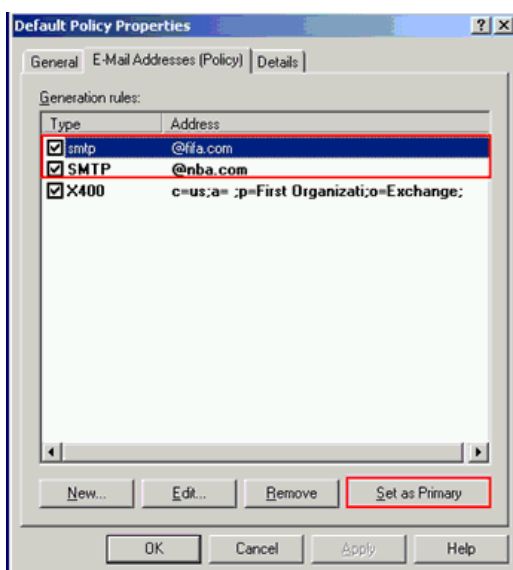
避免利用服务器退信式的垃圾邮件

关掉的好处是避免退信式垃圾邮件攻击，但是缺点是正常邮件的退信也收不到了。



如何接受多个域的邮件场景

4. AD域名和公网上DNS域名不一致时
5. 一个公司有多个域名时
6. 发邮件时以set as primary的地址发送



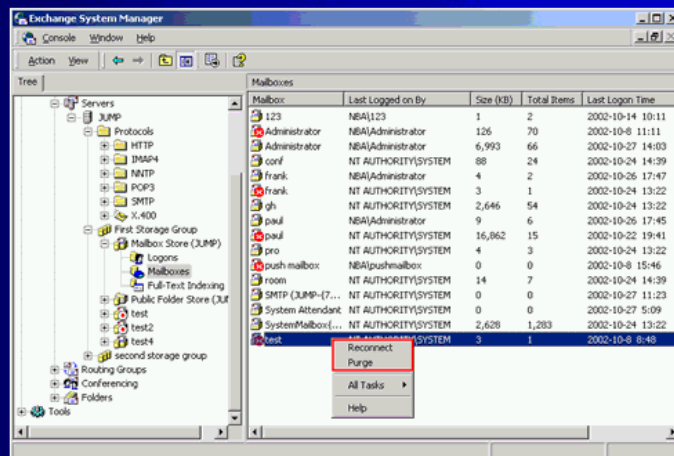
用户账号被删除后，邮箱并不是立即被删除的，默认被保存30天时间，过了30天才会被物理删除
 可以把邮箱再次关联到某个账号，被关联的账号不能是有邮箱的账号
 如果不想等到30天自动清除，可以右击已断开连接的邮箱，选择purge，手动清除
 可以使用mbconn.exe来批量关联用户和邮箱，这个命令在\support\utils\i386文件夹里面

用户帐号被删掉以后，邮箱并不是立刻被删除

Run Cleanup Agent

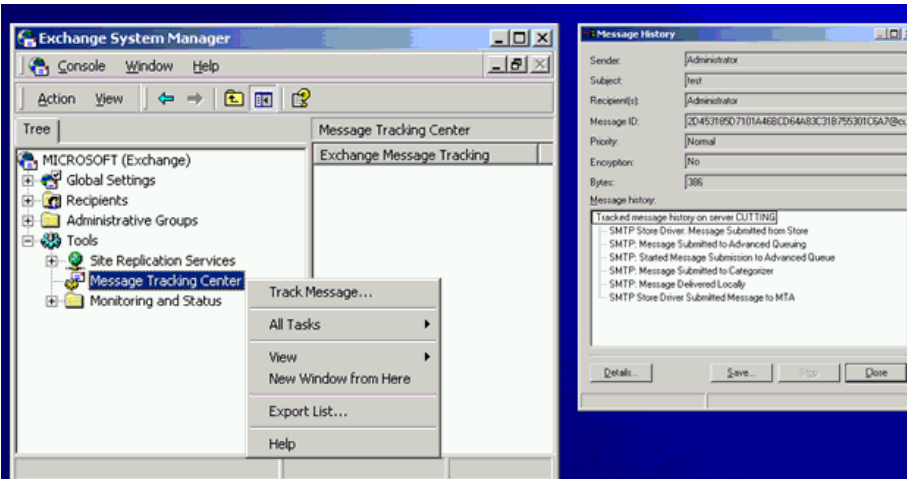
Reconnect

Purge



有用工具：message tracking center邮件追踪工具

日志功能需要在每台exchange服务器上手工启用



Exchange 2k的Message Tracking功能有所改进

邮件跟踪里面会把邮件的整个投递过程呈现出来。

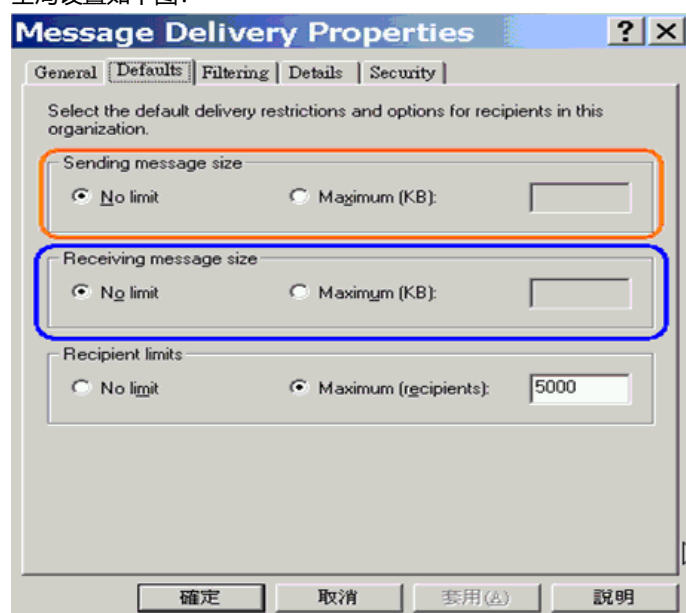
Event	Description
1019	SMTP submit message to Advanced Queuing
1020	SMTP begin outbound transfer
1021	SMTP bad mail
1022	SMTP Advanced Queuing failure
1023	SMTP local delivery
1024	SMTP submit message to categorizer
1025	SMTP begin submit message
1026	SMTP Advanced Queuing failed message
1027	SMTP submit message to Store Driver (SD)
1028	SMTP Store Driver (SD) local delivery
1029	SMTP Store Driver (SD) gateway delivery
1030	SMTP NDR all
1031	SMTP end outbound transfer

SMTP virtual server只负责进来的电子邮件

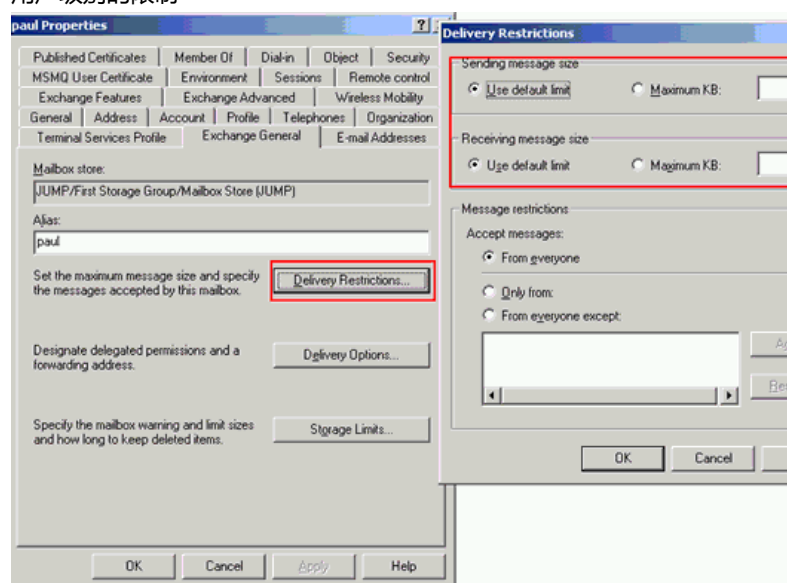
SMTP connectors只负责出去的邮件

用户级别的sending messaging size和receiving messaging size的设置优先级高于服务器级别的设置

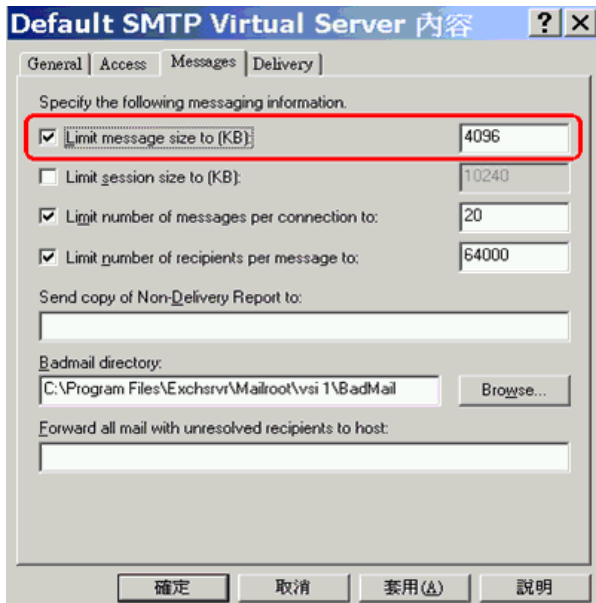
全局设置如下图：



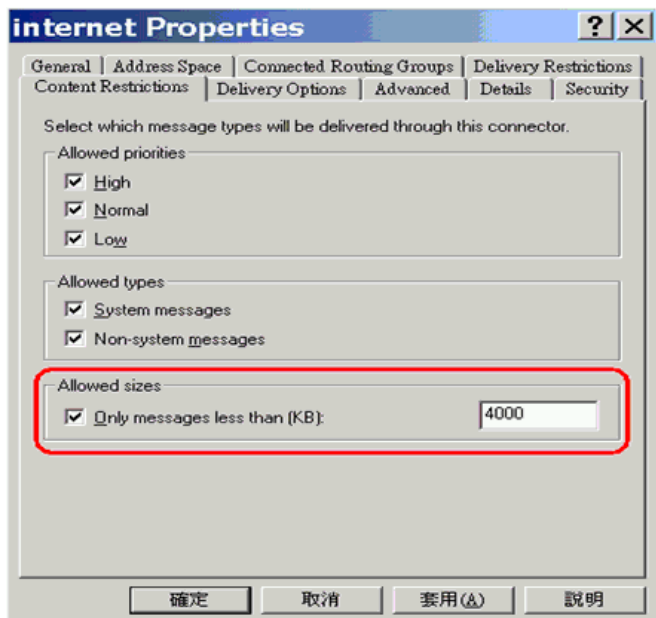
用户级别的限制



SMTP virtual server的限制，允许进来的信的大小

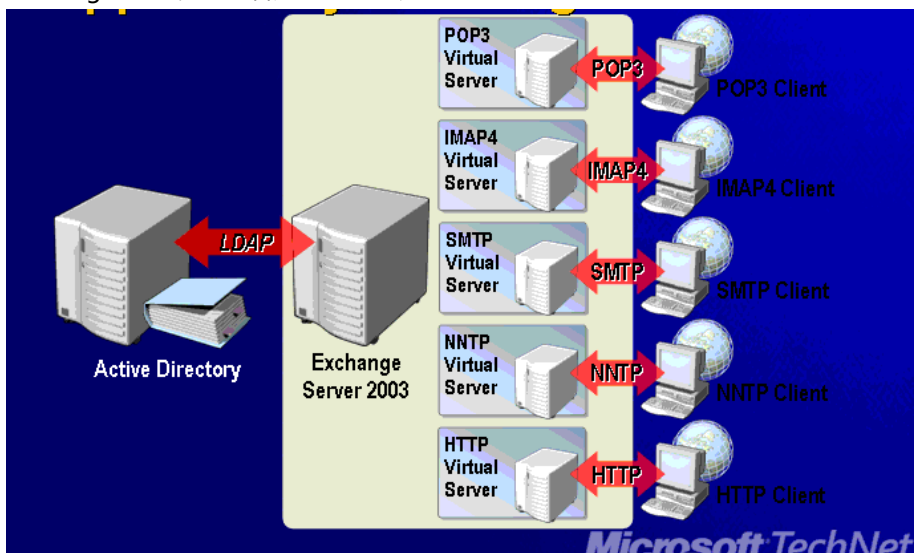


SMTP connectors的设置，允许发出去的信的大小



第五节：理解exchange server 2003客户端访问服务器

exchange 2003支持的客户端访问协议



使用virtual server来支持相关的客户端访问协议，好处是可以在exchange server对同一种协议创建多个虚拟服务器，因为某些用户可能需要身份验证访问，有些需要匿名访问，对不同的virtual server设置不同的身份验证方法

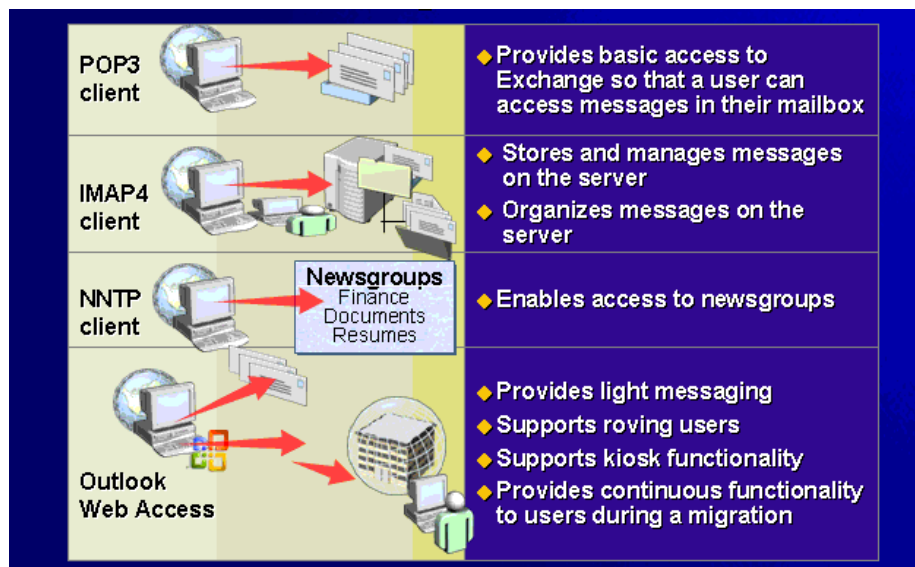
同时支持MAPI访问，支持RPC OVER HTTP访问，Internet上的客户端通过这种协议访问我们的服务器，中间会经过防火墙，防火墙只需要开放80和443端口。

通过LDAP协议与AD交互，活动目录的查询、修改。

LDAP也可以被我们的outlook客户端使用，来对活动目录进行查询。

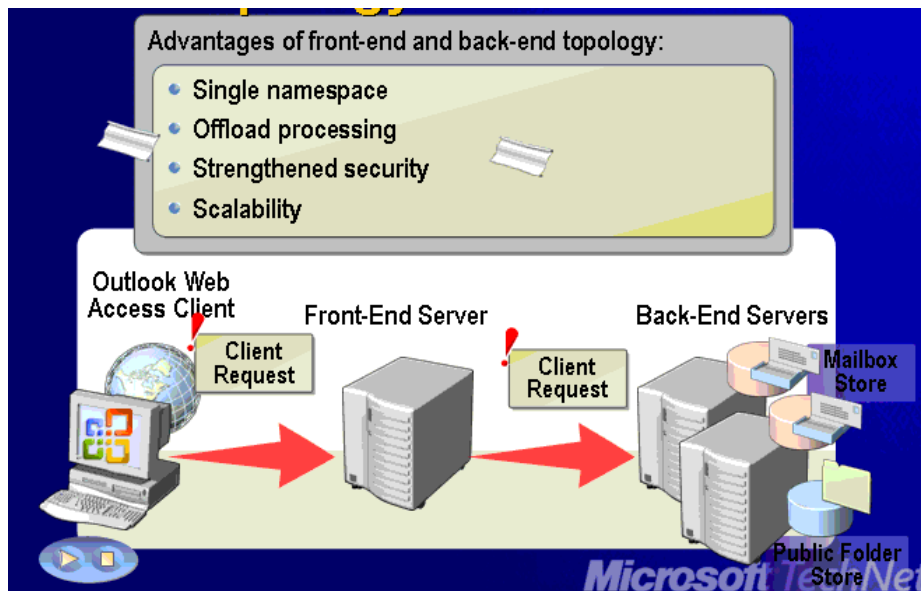
POP3会把邮件下载到本地，只提供基本的功能。配置pop协议可以做到不下载邮件到本地，实际上是outlook的功能，而不是pop3的功能。

IMAP提供了比POP3更高级的功能，在客户端上可以操作服务器上的邮件，在服务器上创建新的文件夹，标记邮件为已读，在客户端上操作，数据的变化在服务器上发生，可以连接到exchange服务器上的共用文件夹，而POP3是做不到的，还可以并不真正下载邮件，只是查看邮件头，如果邮件比较大的话，并不下载邮件到本地。



为什么要使用前后端的拓扑结构？

5. 单一命名空间
6. 处理客户端访问的负载
7. 增强的安全性
8. 扩展性



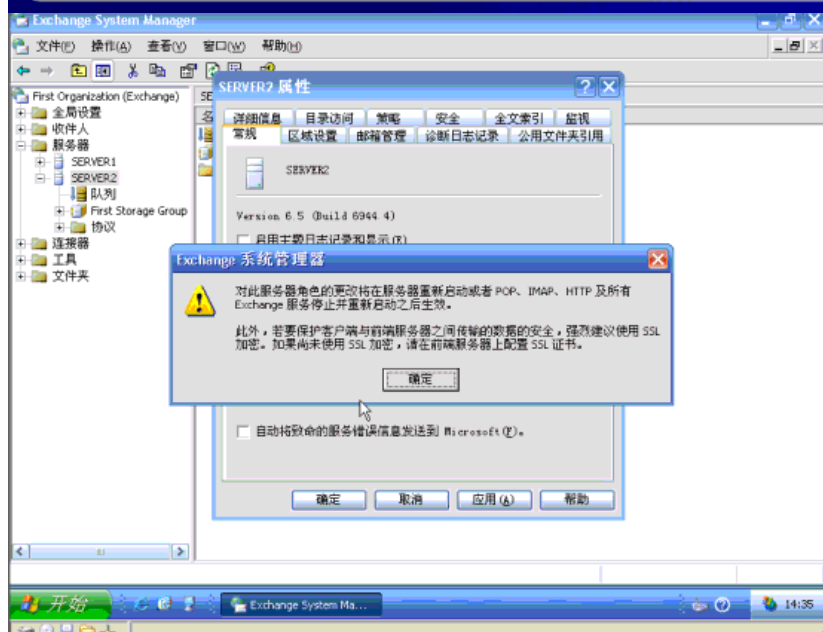
配置前端服务器的步骤如图。

前端服务器最好不要容纳DB或者共用文件夹，否则用户无法访问他们的DB或者公共文件夹。

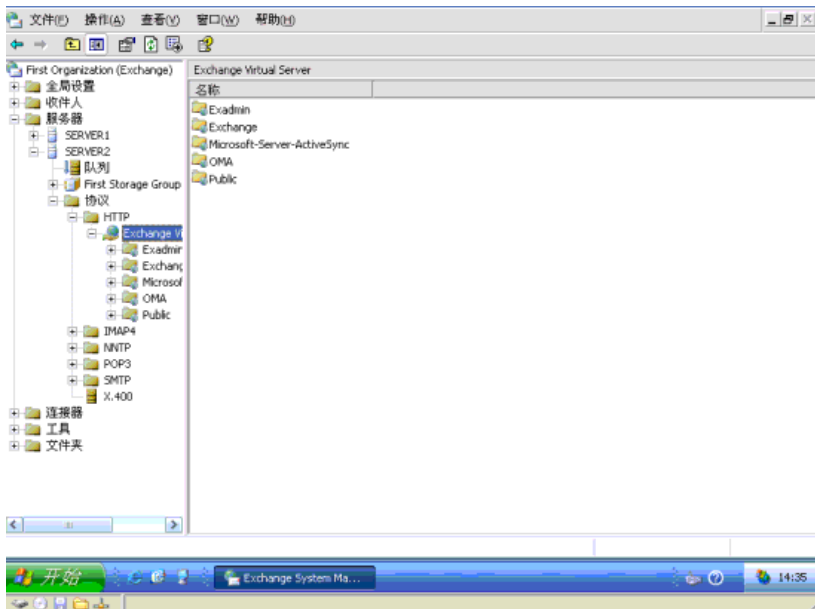
在提升服务器为前端之前，要迁移走上面的数据库和公共文件夹。

To set up a front-end server:

- 1 Install the server running Exchange in the organization
- 2 Use Exchange System Manager to browse to the server object, right-click the server object, and then click Properties
- 3 Select This is a front-end server, and then close the page
- 4 Restart the computer, or stop and restart the HTTP, POP3, and IMAP4 services



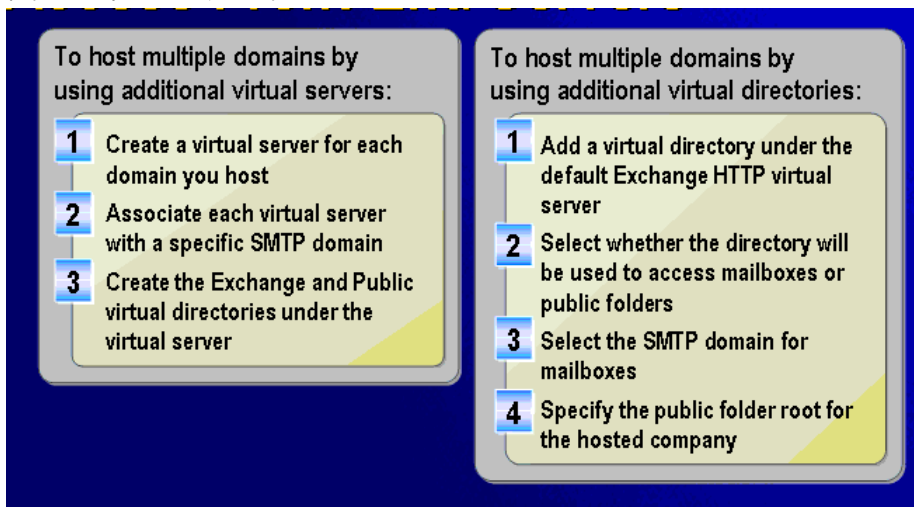
启用前端后，重启协议服务。



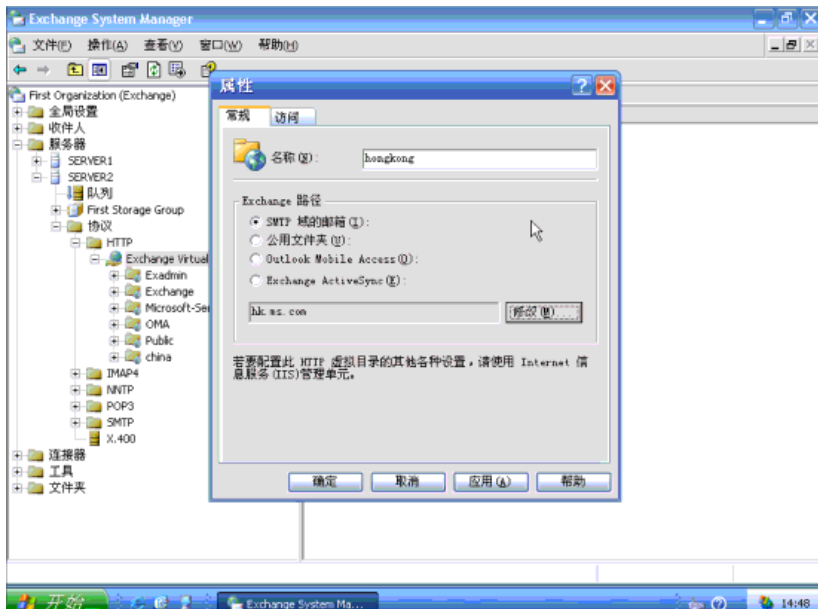
如何配置OWA的前端服务器，缺省情况下是没有必要配置的，但是在一些特殊场景，比如企业中驻留了多个域，需要去配置OWA能够访问的前端服务器。

下图是配置的两种方式。

- 1、在前端上添加多个虚拟服务器，让虚拟服务器对应多个域，需要多个IP；
- 2、第二种方式是在一个虚拟服务器里创建额外的虚拟目录，让不同的虚拟目录对应不同的域，这样用户访问一个固定的名称，下面不同的虚拟目录；



通过exchange 2003收件人策略来实现。创建电子邮件地址策略，然后关联到特定的OU。对于不同的域创建对应的虚拟目录，如图。



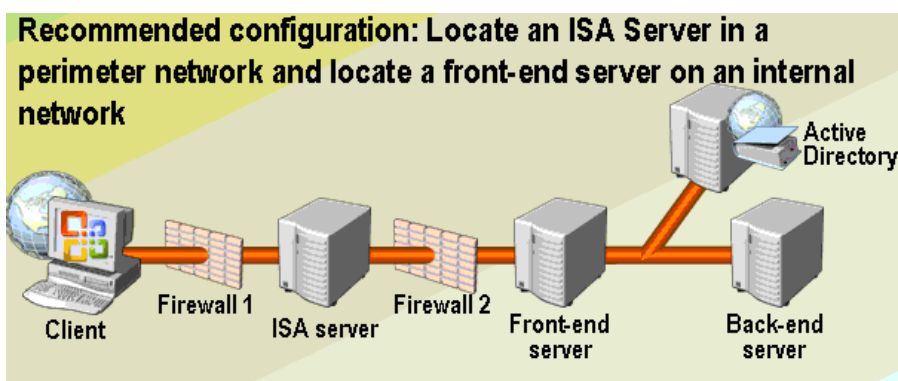
前端服务器修改完成后，后端服务器也要修改相应的配置，后端服务器的配置依赖于前端服务器的设置，如果在前端服务器配置了额外的虚拟服务器或者虚拟目录，那么在后端服务器上也要创建相应的虚拟目录或者虚拟服务器。

<p>To configure additional virtual servers on a back-end server:</p> <ol style="list-style-type: none"> 1 Specify a consistent name for the virtual server 2 Select the appropriate domain from the list 3 Add the appropriate host headers 	<p>To configure additional virtual directories on back-end servers:</p> <ol style="list-style-type: none"> 1 Configure the virtual directory structure on the back-end server to match the front-end server 2 Specify the appropriate SMTP domain for virtual directories associated with mailbox stores
---	---

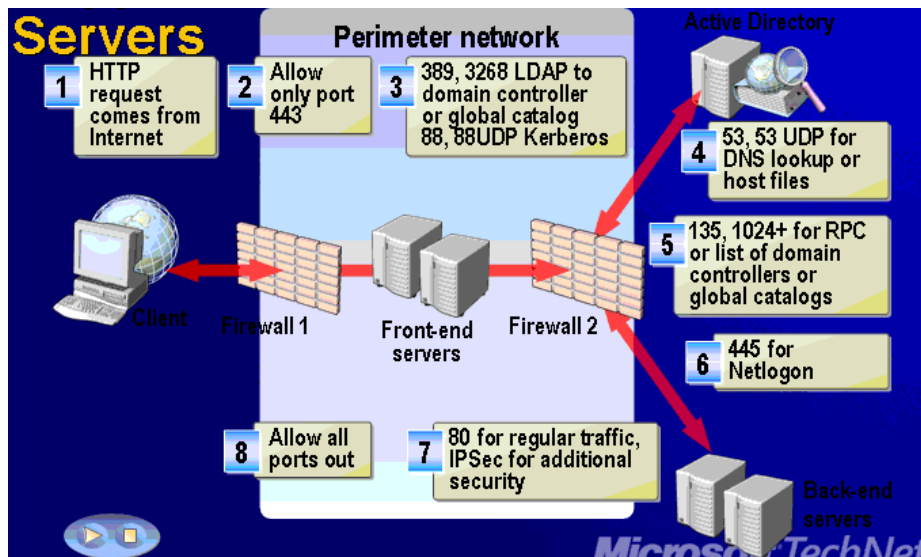
后端服务器所做的操作要**精确匹配**前端服务器的操作。

前后端防火墙的配置推荐方案是把前端服务器放到DMZ区域。

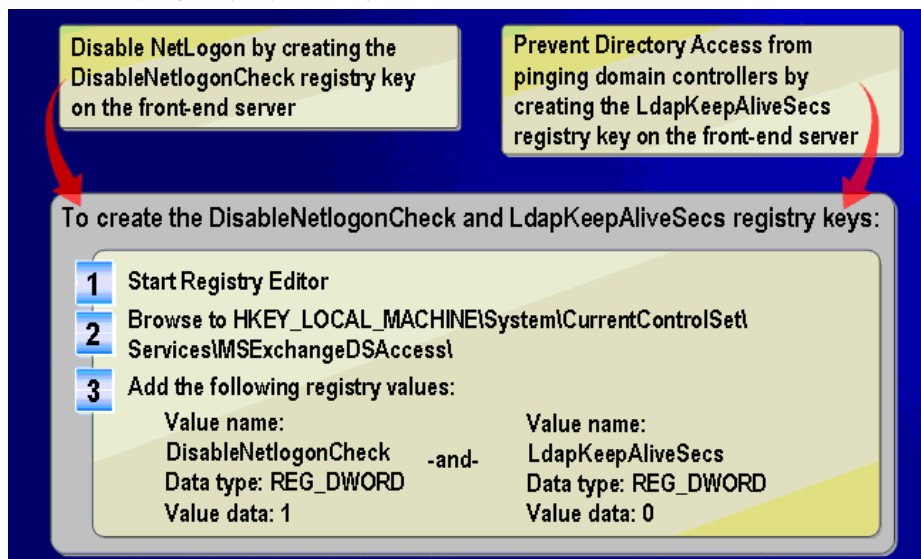
下图是都放到内网了，但是因为有ISAservice接受请求，所以相对来说比较安全，只需要开放80和443端口。



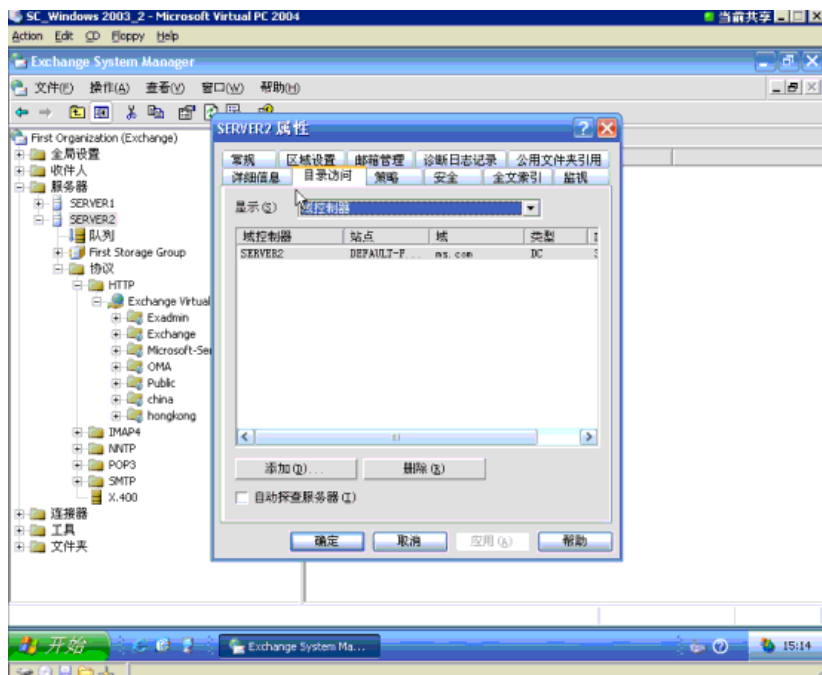
如果把前端服务器放在DMZ区的话，需要开放的防火墙的端口会特别多。



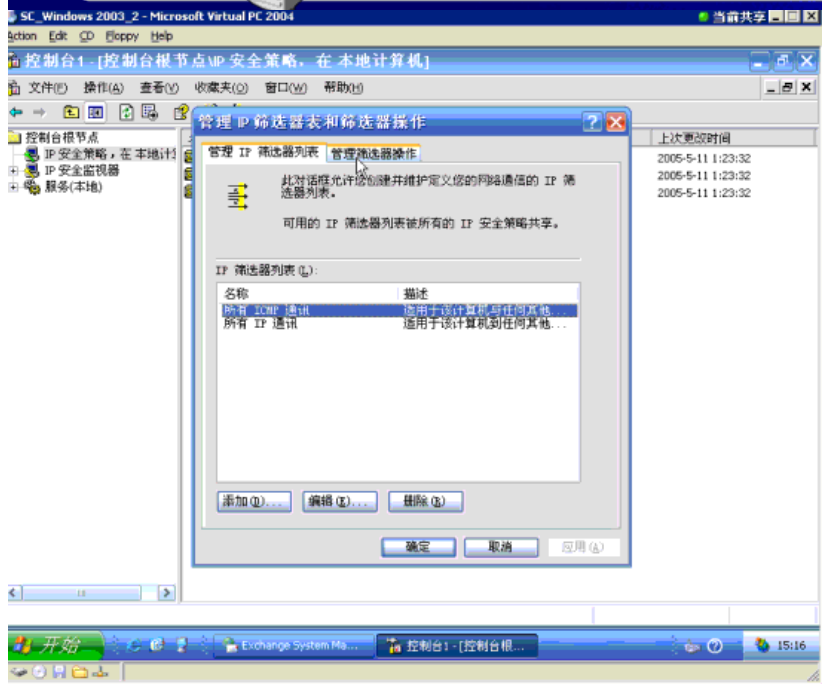
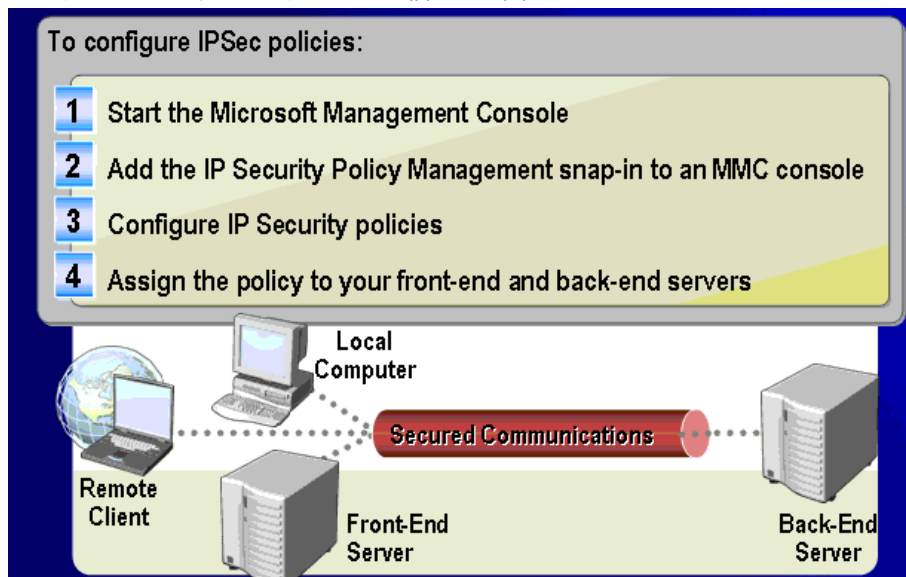
POP3和IMAP一般和SMTP配合使用，因为POP和MAP只能收邮件，发邮件需要依靠SMTP。
 所以如果上图中启用POP3和IMAP的话，还需要打开额外的端口。
 对于上面的场景，可以禁用前端服务器的DC查询。



可以取消前端服务器的自动探查功能，如图。



如何规划前后端服务器之间的IPSEC通信。如下图。



前后端服务器的性能优化建议。

考虑使用SSL的加速器设备，可以把服务器之间的加解密的负担卸载到加速器设备上。

不要删除前端的存储组，否则IIS会出问题。如果前端服务器使用IIS，至少确保有一个存储组存在。

Implement SSL Accelerators	Mitigate the impact encryption and decryption has on the server
Configure the correct server ratios	Configure one front-end processor for every four processors in your back-end servers
Configure the correct server hardware	Ensure that front-end servers have fast CPUs and a large amount of memory
Dismount and delete public and mailbox stores	Dismount and delete the public folder stores on the front-end server and the mailbox store unless you are using SMTP on the front-end server
Ensure high bandwidth between servers	Ensure high network connectivity between front-end, back-end, and global catalog servers for authentication

如果管理OWA访问服务器。

To modify Outlook Web Access settings for users: <ol style="list-style-type: none">1 Open Active Directory Users and Computers2 Modify the access settings for the user	To configure an Outlook Web Access server: <ul style="list-style-type: none">• Use Exchange System Manager• Use Internet Services Manager
---	---

选择使用OWA的版本。

To enable forms-based authentication: <ol style="list-style-type: none">1 Browse to Exchange Virtual Server for the server you want to configure2 Select Enable Forms Based Authentication for Outlook Web Access	To select an Outlook Web Access version: <ol style="list-style-type: none">1 Log on to Exchange 2003 Outlook Web Access by using the URL <code>https://ServerName/Exchange</code>2 Select a version of Outlook Web Access
---	--

Version	Why use?
Premium	<ul style="list-style-type: none">◆ Provides all of the Outlook Web Access features◆ Requires that clients use Microsoft Internet Explorer version 5.0 or later
Basic	<ul style="list-style-type: none">◆ Provides a subset of the rich client features◆ Works in any browser

保证OWA访问安全的选项。

可以通过修改注册表的方式来修改cookie的设置。

This option	Does this
Cookie authentication time-out	<ul style="list-style-type: none"> ◆ Keeps a user's account secure from unauthorized access ◆ Reduces the risk of unauthorized access if a session is accidentally left running on a public computer
Credentials cache	<ul style="list-style-type: none"> ◆ Clears browser's credentials cache when a user logs off from Outlook Web Access
S/MIME support	<ul style="list-style-type: none"> ◆ Allows users to send secure e-mail by digitally signing or encrypting e-mail messages

配置安全设置。

To set the Outlook Web Access cookie time-out value:

- 1 Browse to the registry key, valueHKey_local_machine\system\CurrentControlSet\Services\MSExchangeWeb\OWA\
- 2 Create a new Dword value named for either PublicClientTimeout or TrustedClientTimeout
- 3 Define a Decimal value between 1 and 432000

To deploy S/MIME with Outlook Web Access:

- 1 Install Windows Server 2003 Enterprise CA
- 2 Change any default configurations on the CA
- 3 Ask users to request the certificate
- 4 Install the Outlook Web Access S/MIME control
- 5 Configure default secure messaging settings
- 6 Send test messages

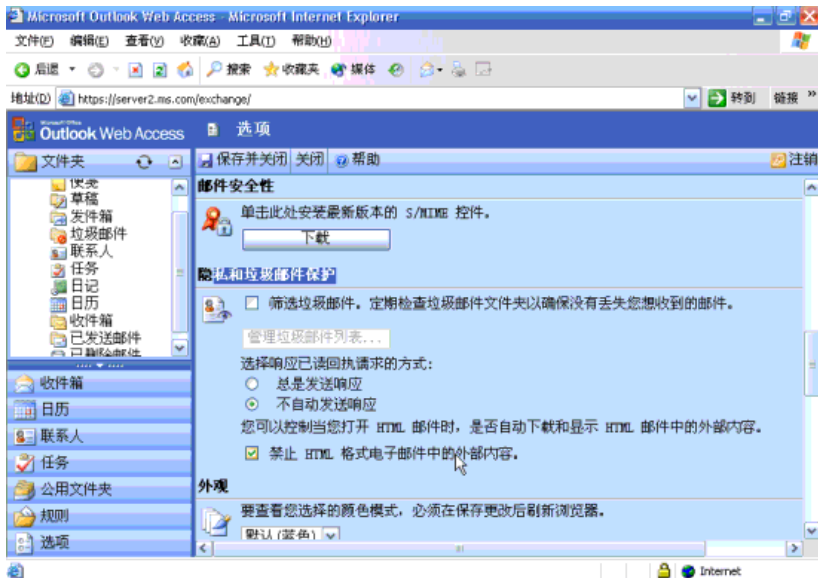
下图的第三点是通过ipsec来实现。

Guidelines for Securing Outlook Web Access Implementation

- Implement SSL between the Outlook Web Access client and Exchange
- Configure user authentication
- Configure authentication and encryption between front-end and back-end servers

如何启用SSL。

3. 安装CA。
4. IIS绑定CA证书。

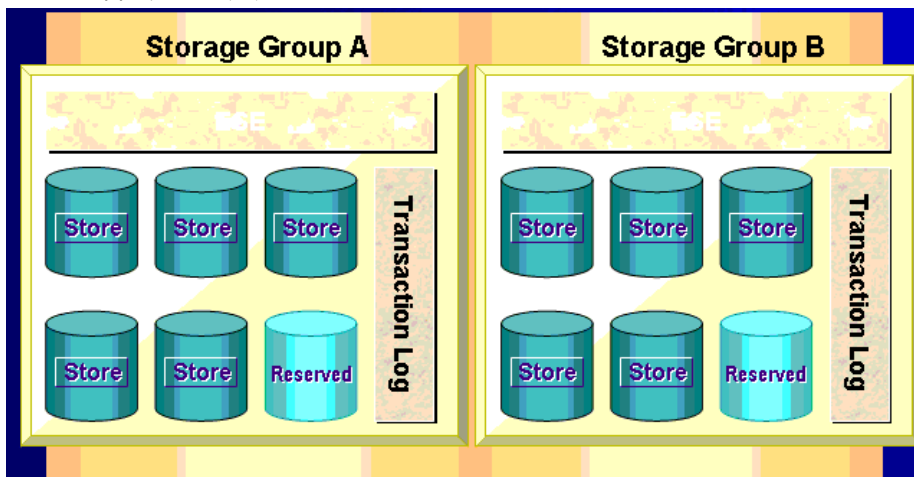


第六节：管理exchange数据库上

存储组和数据库的关系

单个数据库大小70GB最多。

企业版每台服务器可以放置四个存储组。



所有的database都是由Microsoft exchange information store服务管理的，在进程管理器里面有个store.exe进程。

每一个storage group对应一组log事务日志。然后可以在storage group里面创建mailbox store或者public store。

创建数据库之后，有两个文件：

3. exchange database文件，EDB格式；
4. exchange streaming database文件，stm格式；

这两个文件时一起使用的，密不可分。

exchange的备份时间要和联机维护的时间错开。

exchange日志文件。第一个日志文件时E00。

如果用户比较多的话，log文件会暴涨

对数据库的操作，会首先反映在内存里，然后写入到日志，最后写入到硬盘，才算最终完成。

磁盘的寻道时间和写入时间是10:1的关系。

日志文件是固定的5M大小，日志文件在磁盘上面是连续的.日志的作用是让内存的更改尽快写到磁盘，先写成日志比直接写到数据库要快十几倍。

清理日志文件的方法：对exchange做完全备份，在这次完全备份之前所有的日志文件都会被清除掉。

Name	Size	Type	Date Modified	Att
tmp.edb	1,032 KB	EDB File	6/10/2005 10:49 PM	A
res2.log	5,120 KB	Text Document	11/22/2004 6:53 PM	A
res1.log	5,120 KB	Text Document	11/22/2004 6:53 PM	A
pub1.stm	6,152 KB	STM File	6/10/2005 10:49 PM	A
pub1.edb	5,128 KB	EDB File	6/10/2005 10:49 PM	A
priv1.STM	8,200 KB	STM File	6/10/2005 10:49 PM	A
E000000B.log	5,120 KB	Text Document	12/28/2004 11:07 PM	A
E00.log	5,120 KB	Text Document	6/10/2005 10:49 PM	A
E00.chk	8 KB	Recovered File Fragment	6/10/2005 10:49 PM	A

res是保留日志文件。

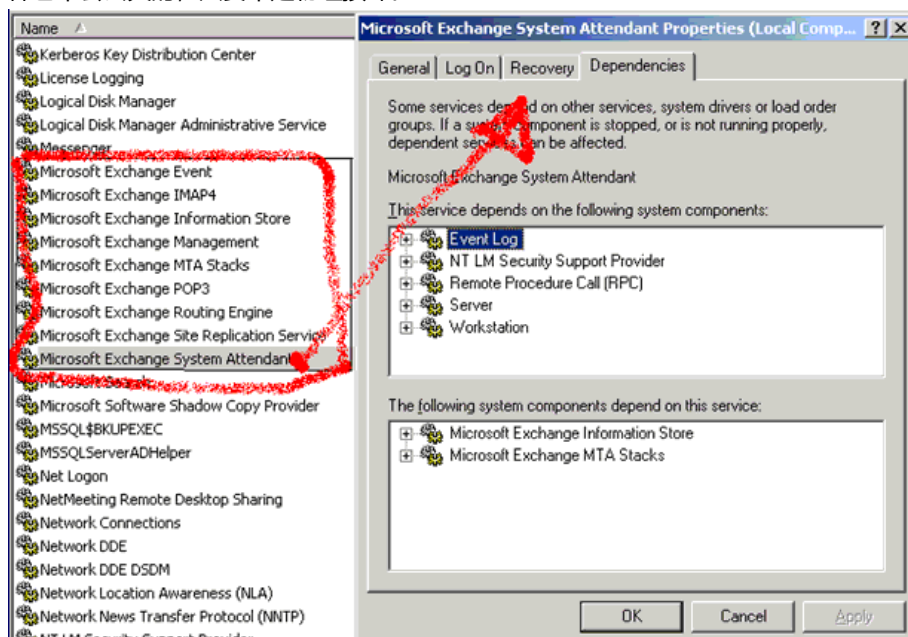
但是对于已经写入到硬盘的日志文件，是可以手动删掉的；问题是日志序列会变得不完整，只能恢复到上次备份的状态。因此建议：即使是检查点文件指针之前的日志已经写入到数据库的文件了，也不建议手动清除，建议通过做备份的方式清除。

- ◆ 作用一：确保对数据库邮箱的改动在第一时间写入硬盘
- ◆ 作用二：在进行灾难恢复的时候提供完整的数据序列，保证尽可能多的恢复数据
- ◆ 忠告一：永远不要手工的删除日志文件
- ◆ 忠告二：如果没有必要，不要开启循环日志
- ◆ 忠告三：日志和其对应的SG数据库分开存放在不同的物理阵列上
- ◆ 忠告四：不要让防病毒软件扫描数据库文件和日志文件
- ◆ 忠告五：定期的做全备份

NT backup提供exchange专用的备份接口，如果直接去备份文件盘符，是不会清除日志的。

如果information store不能启动，可以查看服务的依赖关系。

information store服务启动时会加载数据库文件，加载之前会先去查看与数据库相关的日志文件，看有没有还没写到数据库的，写完了之后，才开始数据库的使用。通过查看CHK文件的checkpoint指针。所以，即使重启或者断电，exchange的文件也不会丢失的，只要不是物理损坏。



当数据库正常运行的时候，永远都是inconsistent的状态，因为不停地有数据写入。

如果数据库正常的关闭了，那么数据库会处于consistent的状态。

- ◆ 数据库关闭时的状态
 - 使用 **eseutil /mh** 查看
 - **“Consistent”** 或者 **“Inconsistent”**
- ◆ **Inconsistent** 状态的数据库在下次 **mount** 的时候会自动地进行 **“software recovery”**

```

Event Type:      Information
Event Source:    ESE98
Event Category:  Logging and Recovery
Event ID:        301
Date:            10/17/2001
Time:            5:52:11 AM
User:            N/A
Computer:        <server_name>
Description:     Information Store (XXXX) The database engine has begun
                  replaying logfile ..\..\E0014553.log

```

关于M盘，就是把微软的数据库的EDB数据库文件映射为一个盘符。

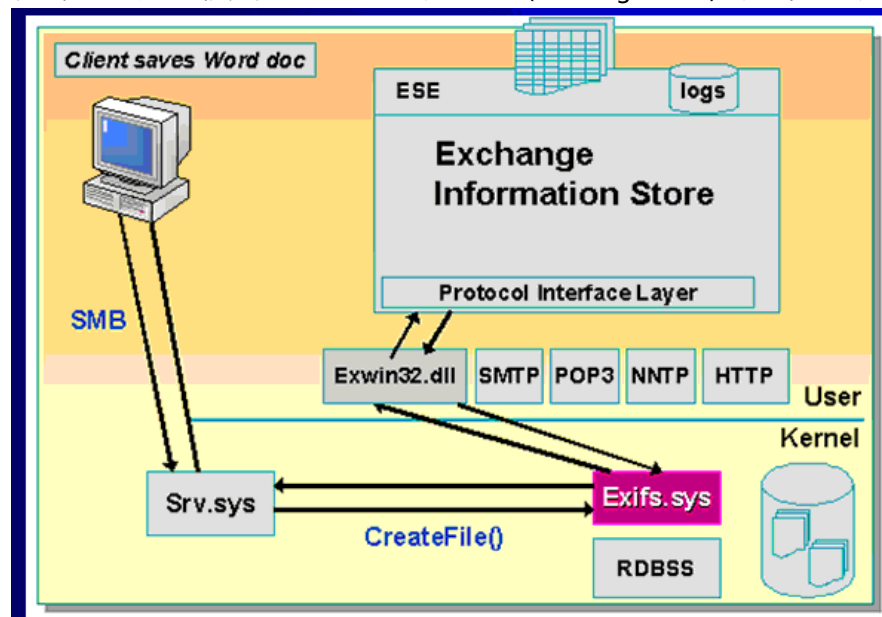
实际的用途并不是很大，有很大争议，所以在exchange 2003里面已经去掉了。

M盘是虚拟的。

永远不要对M盘进行扫描病毒

对M盘的备份是徒劳的

没有特殊需求的时候，没有必要把M盘映射出来（exchange 2003）默认不进行映射）



我们可以通过修改注册表的方式来改变 Exchange Server 所映射的盘符。

```
HLKM\System\CurrentControlSet\Services\ExIFS\Parameters
Name: DriveLetter
Data Type: REG_SZ
Value: Drive letter for IFS (盘符，不需要跟冒号)
```

在更改注册表以后，需要重启 Information Store Service 使更改生效。

我们也可以使用如下的命令行工具来改变 M 盘的映射：

```
Subst X: \\.\BackOfficeStorage 注释：把 Exchange Store 映射到 X 盘
Subst /d M: 注释：删除对 M 盘的映射
```

如果我们移除了 M 盘，我们还是可以通过\\.\BackOfficeStorage 这个共享名字来访问 Exchange Server 的数据库。

ExIFS 在 Windows 中是作为一个隐藏的服务来运行的。下面的注册表键值定义了这个服务的参数：

```
HLKM\System\CurrentControlSet\Services\ExIFS\Parameters
```

由于这是一个隐藏的服务，因此我们没有办法通过 Service 控制面板来对这个服务进行控制。但是我们可以通过命令行来做到：

```
NET Start ExIFS 注释：启动服务
NET Stop ExIFS 注释：停止服务
```

当对存储组级别为单位做数据备份的时候，会清除日志文件，就没有必要再单独备份数据库了。

