

exchange 2010的管理工具

EMC、powershell、ECP

exchange管理的历史

exchange 2003的管理手段

Exchange Server 2003

- ◆ Exchange System Manager 和 Active Directory® Domain Services (AD DS) Users and Computers 用于管理所有邮件相关属性
- ◆ 管理工具依赖于分配在AD DS的Recipient和Configuration对象上的权限
- ◆ 管理组建立在Organization/Administration Group级别
- ◆ 3个可用的管理组
 - Exchange Full Administrator
 - Exchange Administrator
 - Exchange View-Only Administrator

exchange 2007的管理手段

Exchange Server 2007

- ◆ Exchange Server 2007提供了新的工具来丰富管理手段
 - Exchange Management Shell (EMS)
 - Exchange Management Console 和 Management Shell提供了更丰富的管理手段
- ◆ 管理工具依赖于分配在AD DS的Recipient和Configuration对象上的权限
- ◆ 5个可用的管理组
 - Exchange Organization Administrator
 - Exchange Recipient Administrator
 - Exchange View Only Administrator
 - Exchange Public Folder Administrator
 - Exchange Server Administrator

exchange server 2010的管理手段

ECP的web管理，用户自助服务。

- ◆ 新的基于Web的简单管理窗口
- ◆ 面向最终用户，主机租户和专门人员

Administrator



Client logon



使用remote powershell

可以在windows764位客户端上安装exchange的管理工具。

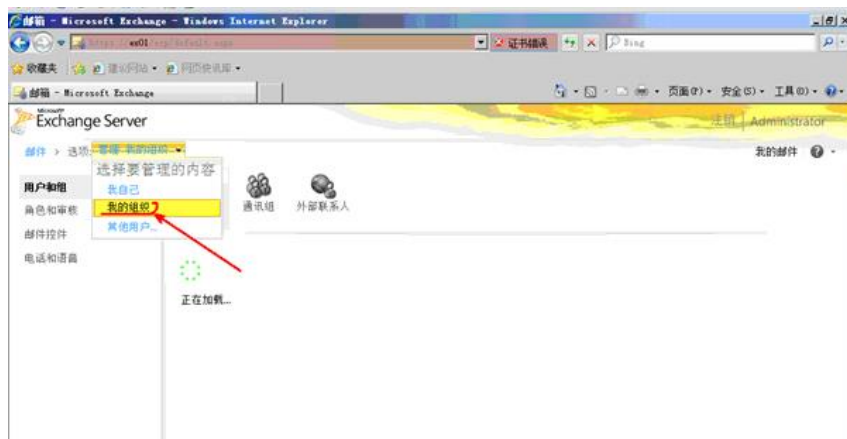
- ◆ **\$UserCredential = Get-Credential**
- ◆ **\$rs = New-PSSession**
-ConfigurationName Microsoft.Exchange
-ConnectionUri https://<Exchange 2010 servername>/PowerShell
-Credential \$UserCredential
- ◆ **Import-PSSession \$rs**
- ◆ **Or... for on-premise, just run the Exchange Management Shell icon!**

在EMC里面可以完成90%左右的任务。

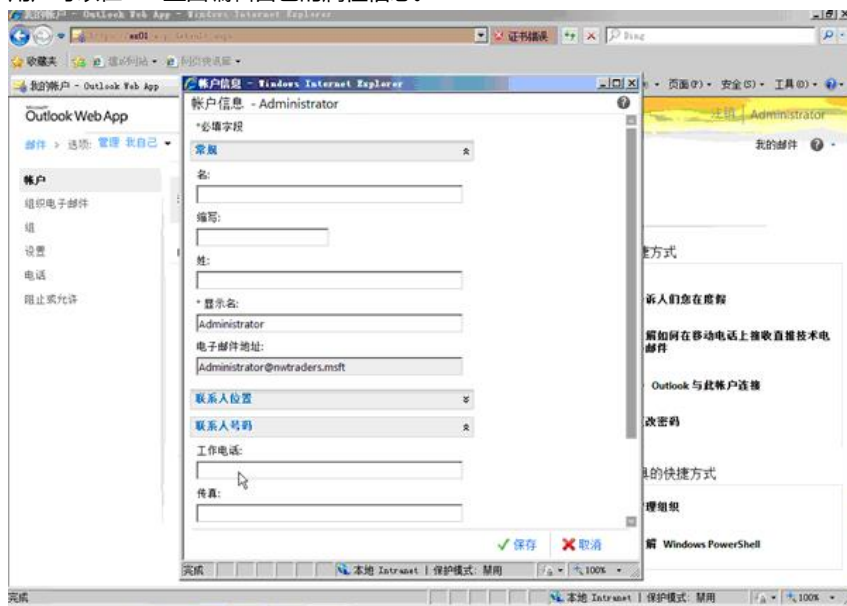
在ECP里面如果输入的是管理员用户，则不仅可以管理自己的邮箱，还可以管理其他用户的邮箱，如果是普通用户，则只能管理自己的邮箱。

在OWA里面有个选项，实际上就是ECP的内容。

具有管理员权限的人才可以选择我的组织。



用户可以在ECP里面编辑自己的属性信息。



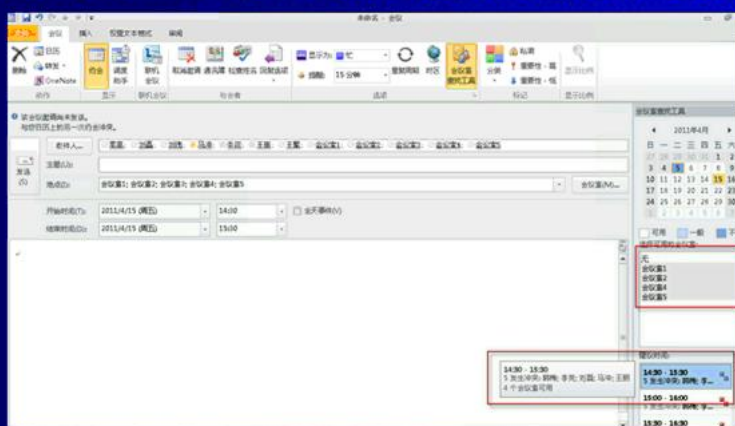
exchange邮箱管理的新增功能

◆ Exchange 2010新增和改进功能

- 用户共享信息的能力，如共享日历忙/闲信息以及位于不同组织中的用户的联系人
- 改进的资源邮箱日历处理的调度和配置功能
- 在最终用户访问邮箱时移动邮箱的能力
- 扩展的批量收件人管理功能，允许您批量管理收件人属性
- **EMC** 向收件人发送邮件的能力

单台mailbox数据库用户数建议不超过4000个。

◆ 改进的资源邮箱日历处理的调度和配置功能



exchange邮箱数据库的文件类型

文件类型	描述
<Log Prefix>.chk	检查点文件
<Log Prefix>.log	当前的事务日志文件
<Log Prefix>xxxxxxx.log	已被重命名的事务日志文件
<Log Prefix>res00001.jrs	保留事务日志文件
<Log Prefix>res00002.jrs	保留事务日志文件
Tmp.edb	处理交易的临时工作区文件
<Log Prefix>tmp.log	临时工作区的日志文件
<File Name>.edb	数据库文件(存储邮箱和公共文件夹)

exchange 2010的日志文件时1M，之前是10M

数据库更新过程

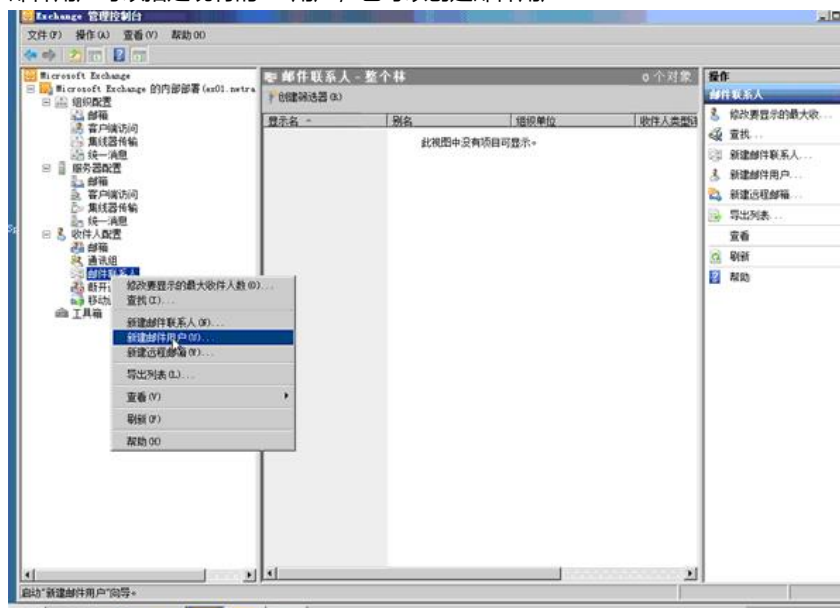
exchange 2010 SP1之后可以支持远程托管的存档，可以指定别的数据库。

存档邮箱是个高级功能，客户必须购买exchange的企业版CAL。



在邮件联系人界面，可以新建邮件用户。

邮件用户可以指定现有的AD用户，也可以创建邮件用户

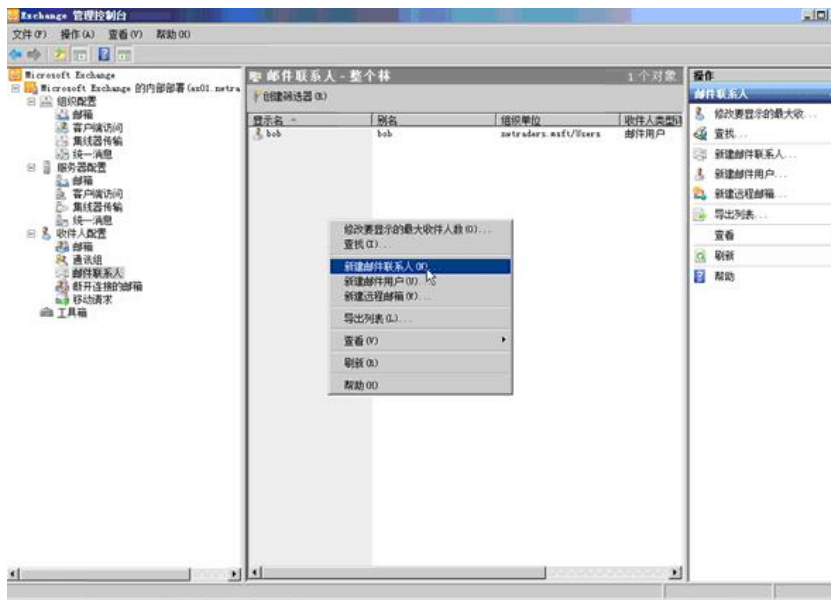


邮件用户指定的地址为外部的电子邮件地址。

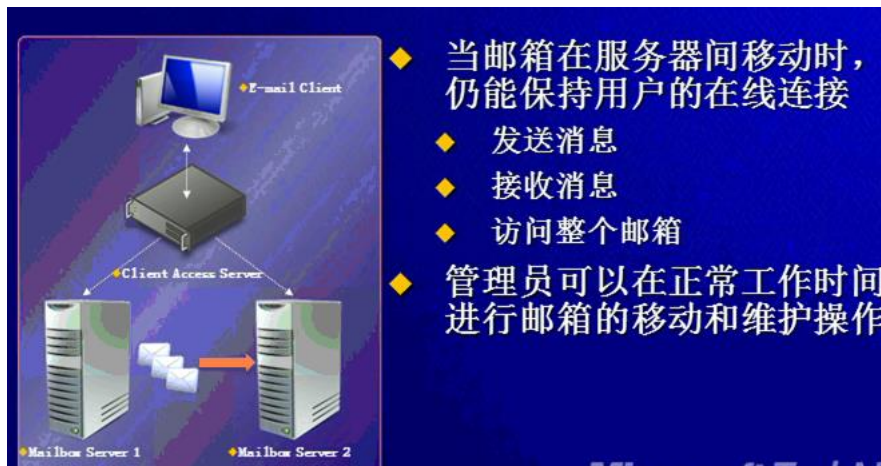


创建的邮件联系人，会被保存到AD数据库之中，然后客户端更新地址簿，邮件联系人的信息会出现在地址簿之中，方便用户使用。

即外部的联系人启用邮件地址。



在邮箱移动和维护时，仍保持用户访问邮箱的能力。



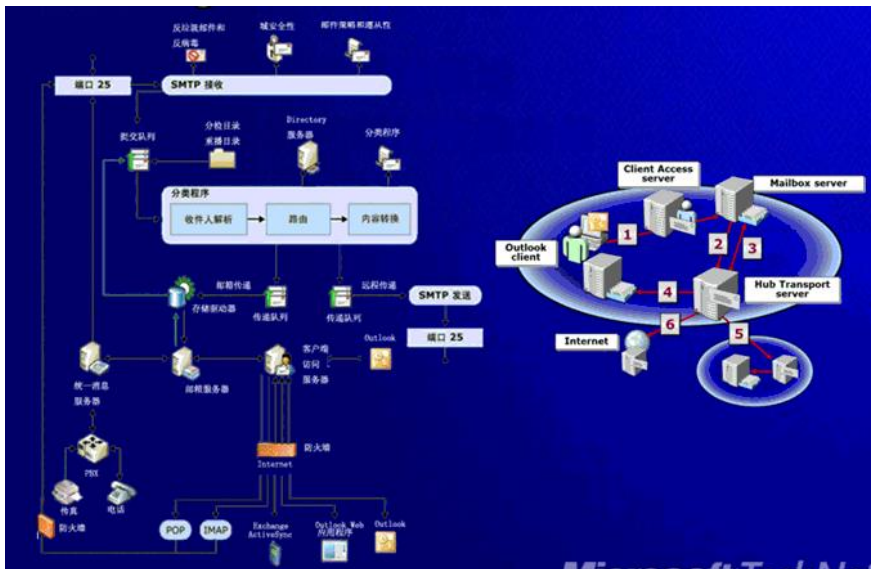
批量的收件人管理功能。

批量的功能建议使用powershell来实现。

- ◆ 可以在结果窗格中选择多个收件人，然后在操作窗格中单击“属性”。无法进行批量编辑的属性不可用。

Exchange Server 2010精讲系列课程(5): Exchange Server 2010的传输规则

exchange server 2010传输拓扑



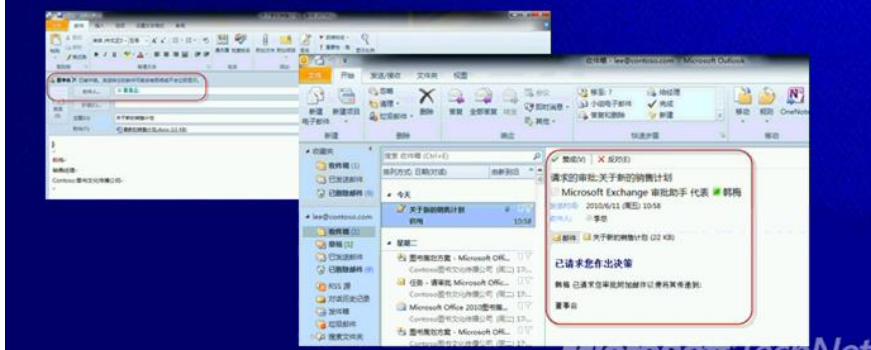
提交队列一次只能处理一封邮件，然后提交到分类程序。
非常类似于邮局的分拣邮件。

exchange 2010传输服务器的新功能

- ◆ Mail Tips
- ◆ 仲裁传输
- ◆ 传输规则和RMS集成
- ◆ 端到端的邮件跟踪
- ◆ 卷影冗余
- ◆ 支持对 WAN 拓扑禁用 TLS
- ◆ 延迟管理
- ◆ 反压的改进

仲裁传输功能。

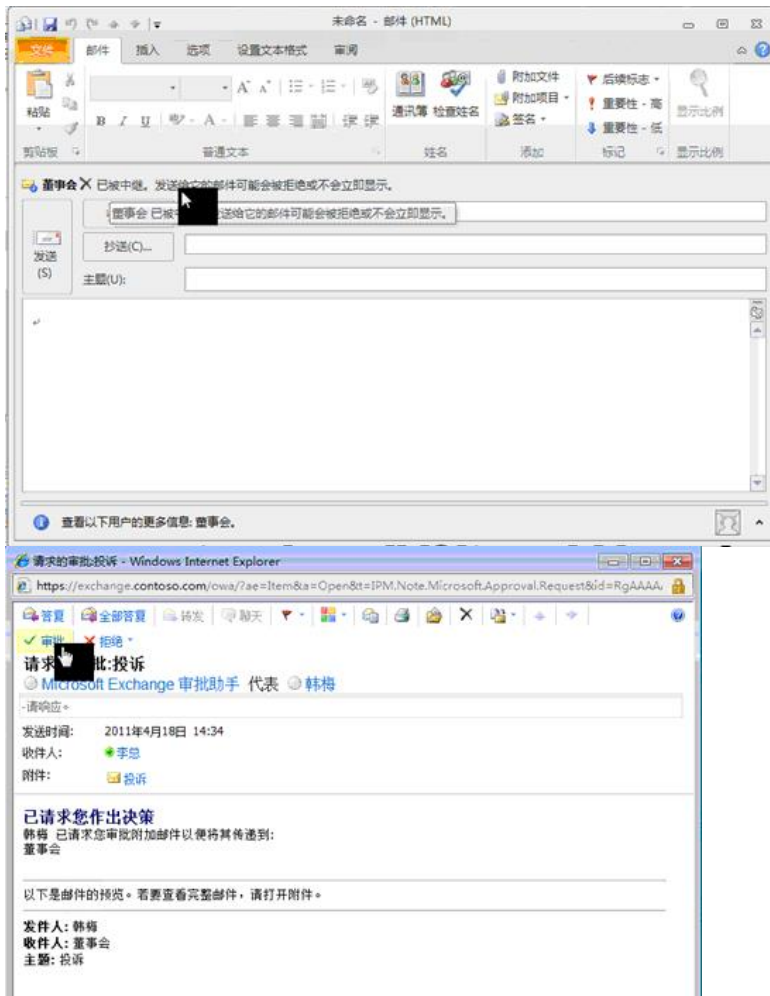
- ◆ 当前很多企业都面临着普通用户越级申报或者越级审批的难题，我们可以通过**Exchange**服务器对企业内部的邮件流进行自动控制。



端到端的邮件跟踪，可以查看outlook或者ECP的送达报告。

对于mailtips，在OWA和outlook里面都支持提醒功能。

对于需要审批的邮件，当越级发邮件的时候，也会有mailtips信息。如果非要越级发送，那么董事会是不会受到邮件的，邮件会先被审批人部门领导收到。

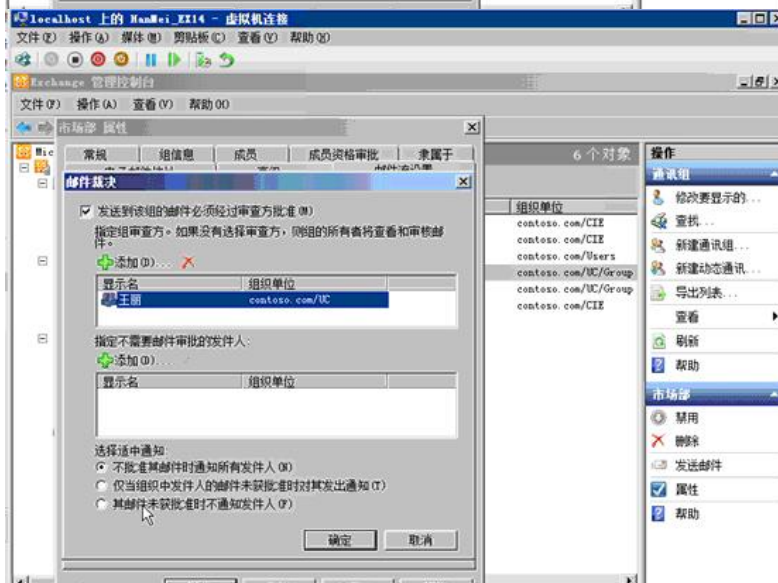
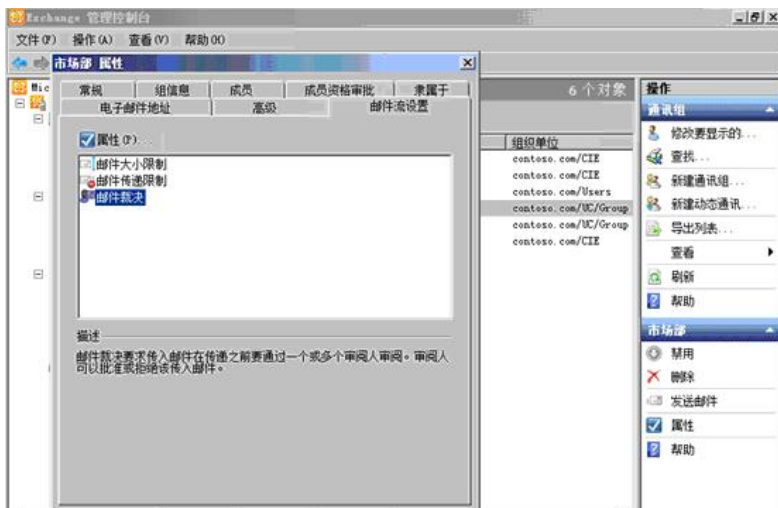


通过服务器配置，集线器传输，来新建传输规则，通过传输规则可以设置审批流程。

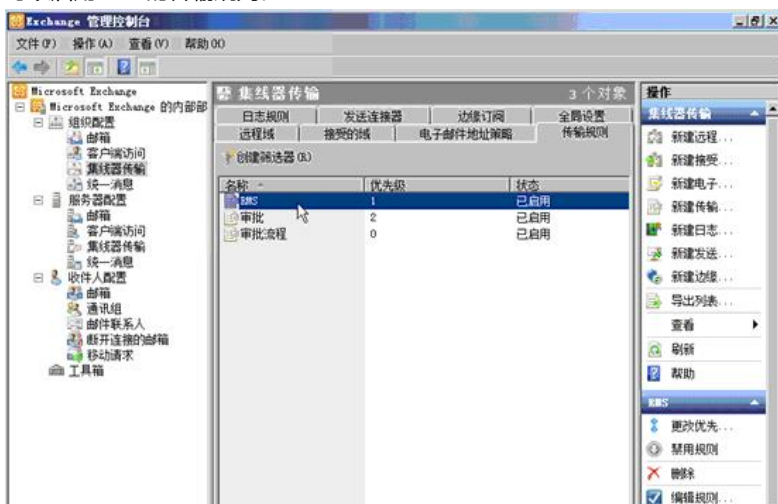
可以选择多人进行审批。任何一个人都可以审批，只要有任何一个人审批，邮件就可以被发送或者被拒绝，不需要全部都审批。



通过图形界面，也可以进行邮件裁决功能的设置。



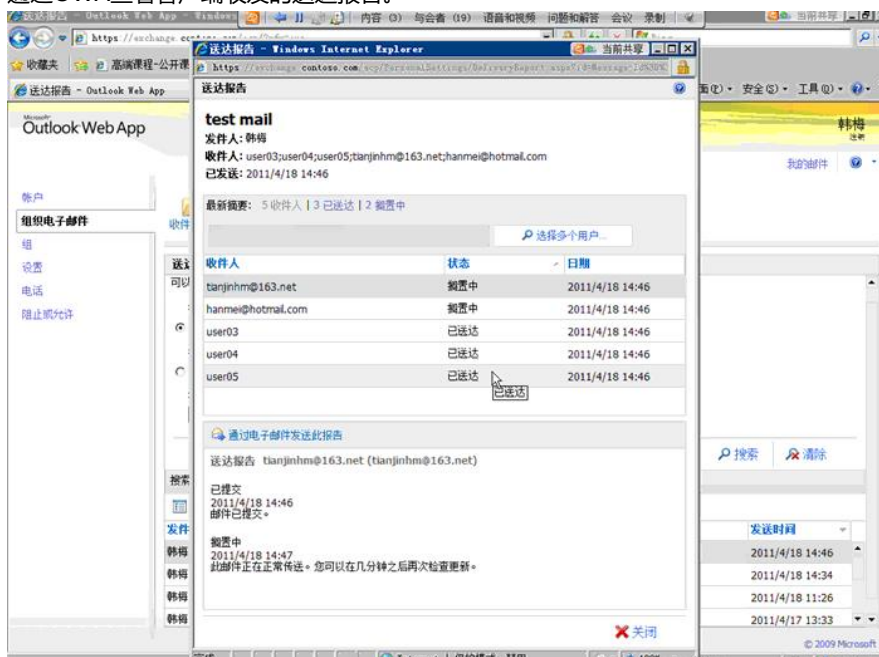
可以启用RMS的传输规则。



可以设置包含特定关键字的邮件，自动应用特定的RMS模板。



我们可以自己自由组合设定不同的RMS的模板。然后结合传输规则。
通过OWA查看客户端收发的送达报告。



卷影冗余

提供了比传输转储更可靠的机制。

- ◆ 影子冗余类似**Transport Dumpster**
- ◆ 增强可靠性的同时而不增加硬件成本
- ◆ 缺省是启用的
- ◆ 数据会被保留在上一跳服务器上直到转发成功
- ◆ 当下一跳传输失败被侦测到，上一跳会重新提交传输
- ◆ 如果传输服务器出现故障，您可以将其从生产环境中删除，而不会清空其队列或丢失邮件。

邮件会先放到自己的影子队列里面。

卷影冗余默认每隔五分钟检测一次，重试间隔为3次。

在卷影队列里面放置两天后，邮件会被丢弃。

◆ 查看全局卷影冗余配置

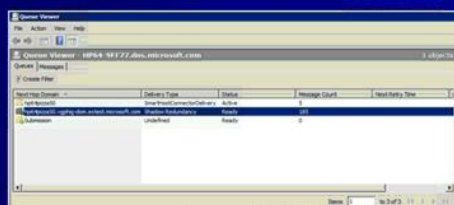
```
[PS] D:\>get-TransportConfig | Fl Shadow*

ShadowRedundancyEnabled      : True
ShadowHeartbeatTimeoutInterval : 00:05:00
ShadowHeartbeatRetryCount    : 3
ShadowMessageAutoDiscardInterval : 2.00:00:00
```

◆ 启用全局卷影冗余配置

```
[PS] D:\>Set-TransportConfig -ShadowRedundancyEnabled $true
```

◆ 卷影队列



支持对WAN拓扑禁用TLS。

- ◆ 在 **Microsoft Exchange Server 2007** 中，传输层安全性 (TLS) 加密对于集线器传输服务器之间的所有 **SMTP** 通信都是强制性的。这将强化集线器到集线器通信的总体安全性。但在某些使用 **WAN 优化控制器 (WOC)** 设备的拓扑中，可能不需要 **SMTP** 通信的 TLS 加密。**Exchange Server 2010** 支持为这些特定方案禁用集线器到集线器通信的 TLS。

测量传递的延迟

Service Level Agreement (SLA)

- ◆ 使用 **Exchange 2010** 传输，可以度量传递的相对于服务级别协议 (SLA) 目标的服务级别。**Exchange 2010** 提供度量每个跃点延迟以及端到端延迟的能力。
- ◆ **Exchange Server 2010** 对这些延迟进行测量，并使用邮件跟踪日志和 **PerfMon** 指标进行报告

针对反压的改进。

反压是 **Microsoft Exchange** 传输服务的一种系统资源监视功能

- 监测系统资源例如可用的硬盘空间、驱动器空间、内存
- 如果系统资源超过一个指定的级别，那么将限制新的连接和邮件
- 防止服务器完全过载

资源使用率级别

描述

正常

资源的使用未过度。服务器可以接受新的连接和邮件。

中等

资源的使用稍微过度。此时将以有限的方式对服务器应用反压功能。来自权威域中的发件人的邮件可以流动。但是，根据具有压力的特定资源，服务器会使用缓送技术延迟服务器响应或拒绝来自其他源的传入邮件。

高

资源的使用严重过度。此时将充分应用反压功能。所有邮件都停止流动，服务器将拒绝一切邮件传入。

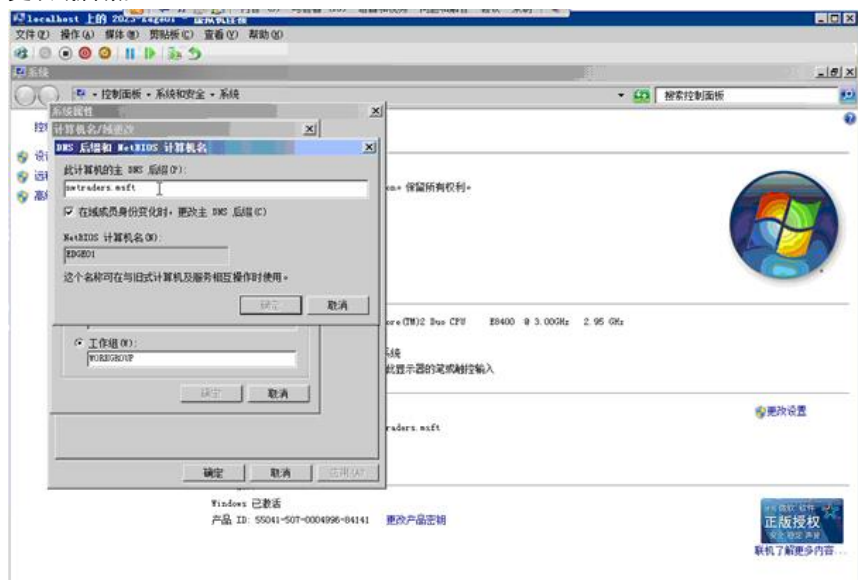
Microsoft TechNet

Exchange Server 2010精讲系列课程(6): Exchange Server 2010的边缘服务器的实施

边缘传输服务器的基础架构要求

- ◆ 在内部和外部防火墙上开放相应的端口
- ◆ 必须配置域后缀
- ◆ 在公网申请并注册相应的**FQDN**的**A**记录
- ◆ **Edge**和**HUB**可以相互通过名字解析
- ◆ **Edge**上安装**AD LDS**

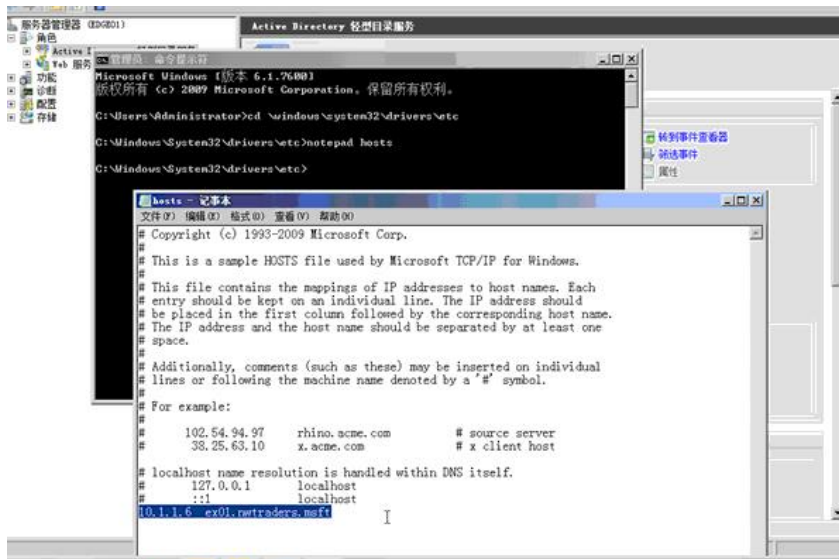
更改域后缀。



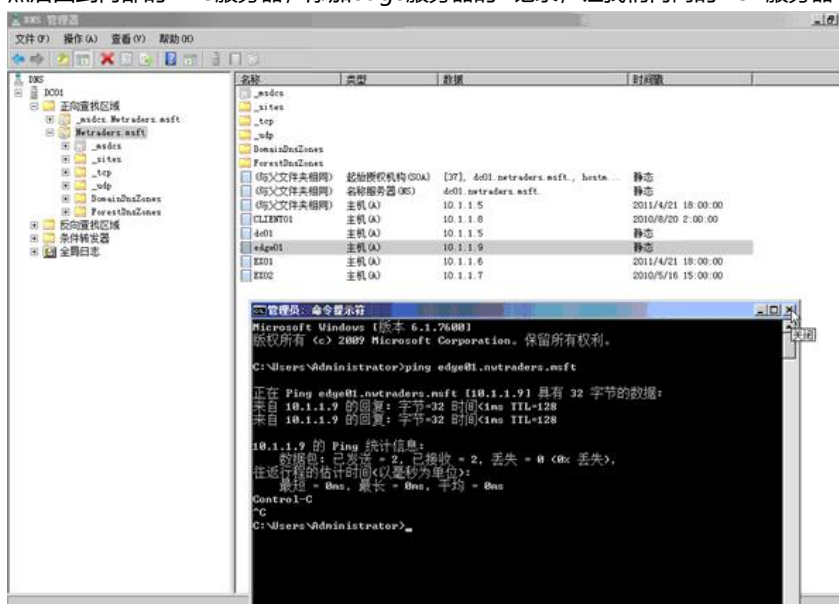
安装轻型目录服务。



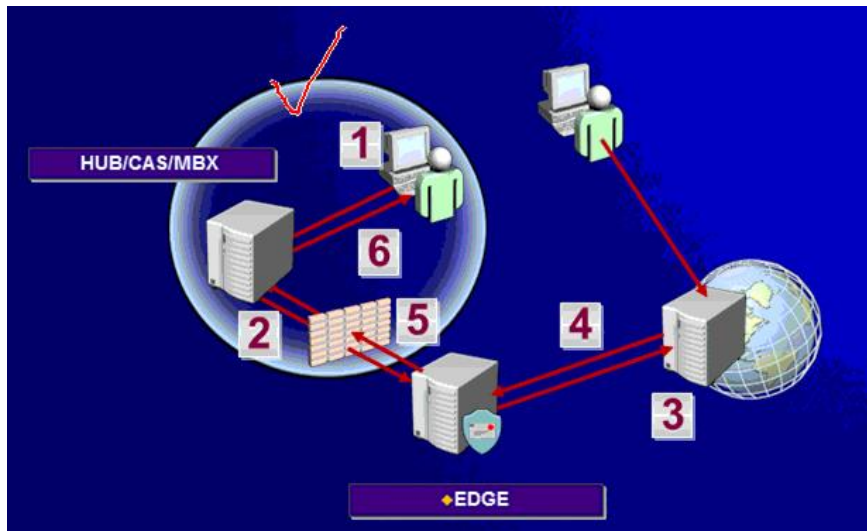
修改hosts文件。让边缘能够解析HUB服务器。



然后回到内部的DNS服务器，添加edge服务器的A记录，让我们内网的HUB服务器可以解析EDGE服务器。



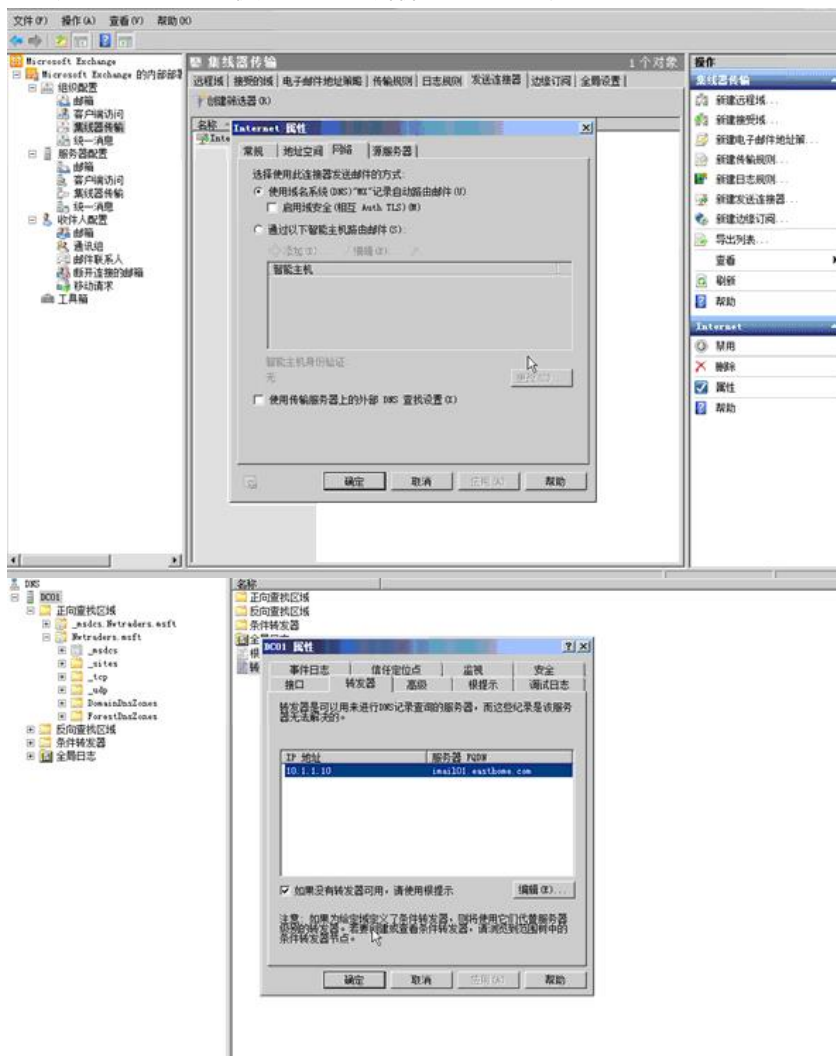
Internet邮件流过程



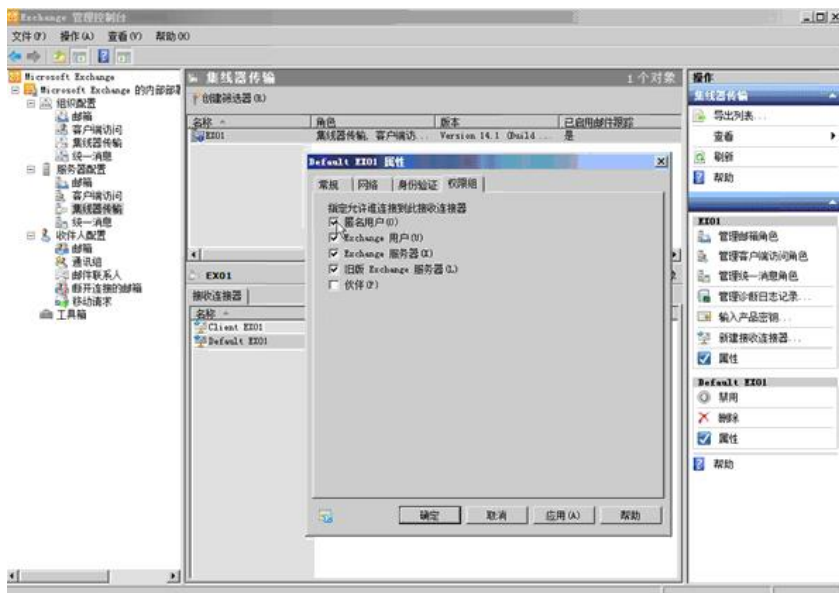
如果内外网域名不一致，需要为外网域名创建接受域和电子邮件地址策略。

如果往公网发送，需要在HUB上创建发送连接器。

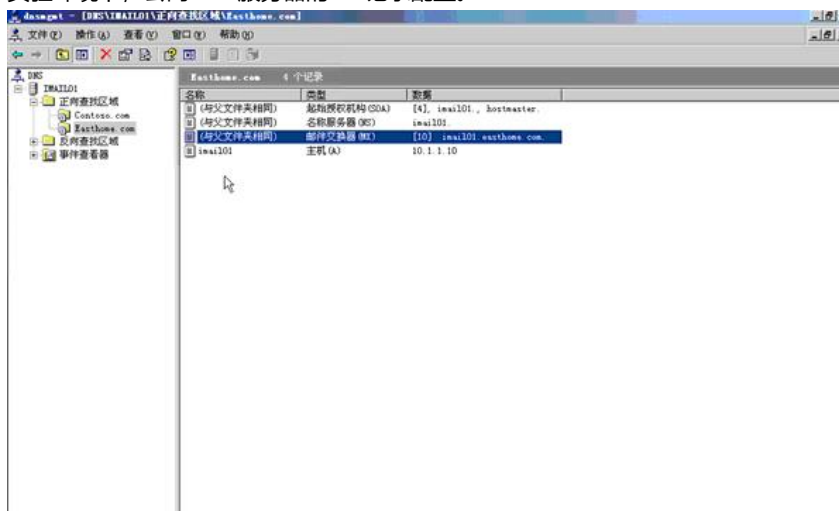
如果发送连接器指定了使用内部DNS解析MX记录的话，需要然后需要到内部的DNS上配置转发器，将请求转到公网的DNS。



如果需要接收互联网发来的匿名邮件，还需要修改接收连接器。



实验环境下，公网DNS服务器的MX记录配置。



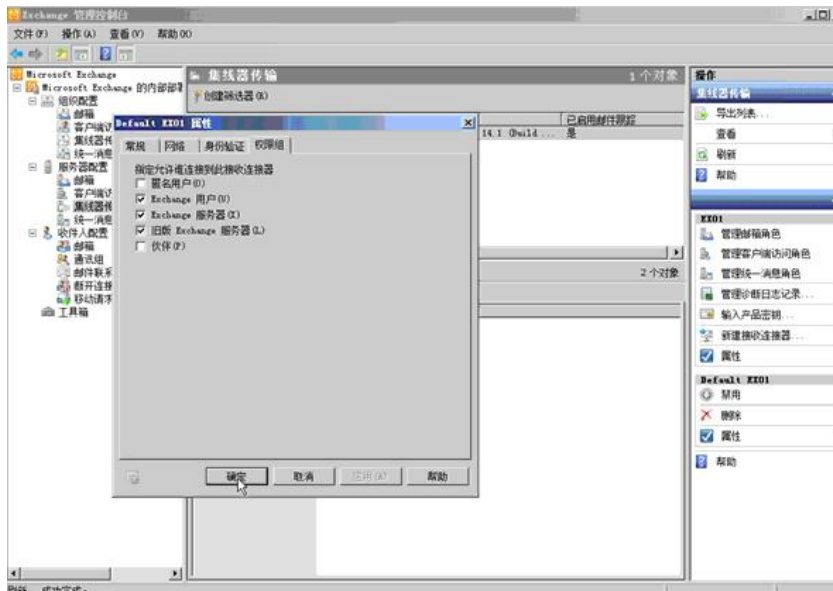
配置完上面的项目后，在只有一台HUB的情况下，也可以往外网发送接收邮件了。

下面是HUB+edge的配置情况。

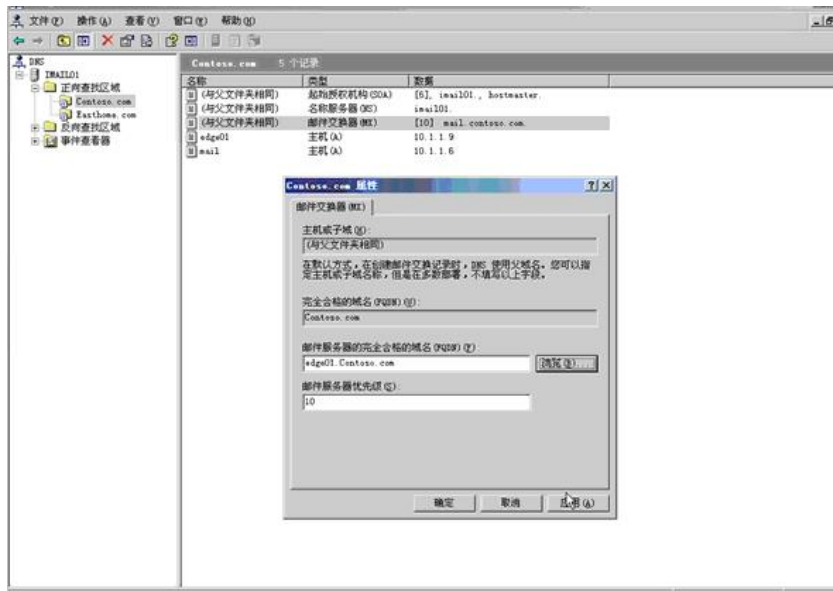
首先要回到HUB，删除Internet的连接器。因为由EDGE来发送Internet邮件。



取消HUB的匿名接收。因为由EDGE接收匿名。



修改公网的DNS记录。把MX记录指向EDGE服务器。



edge服务器默认情况下，只有接收连接器，没有发送连接器，没有接收域。



我们需要做EDGE和HUB之间的边缘同步，来把HUB的配置信息同步到EDGE。

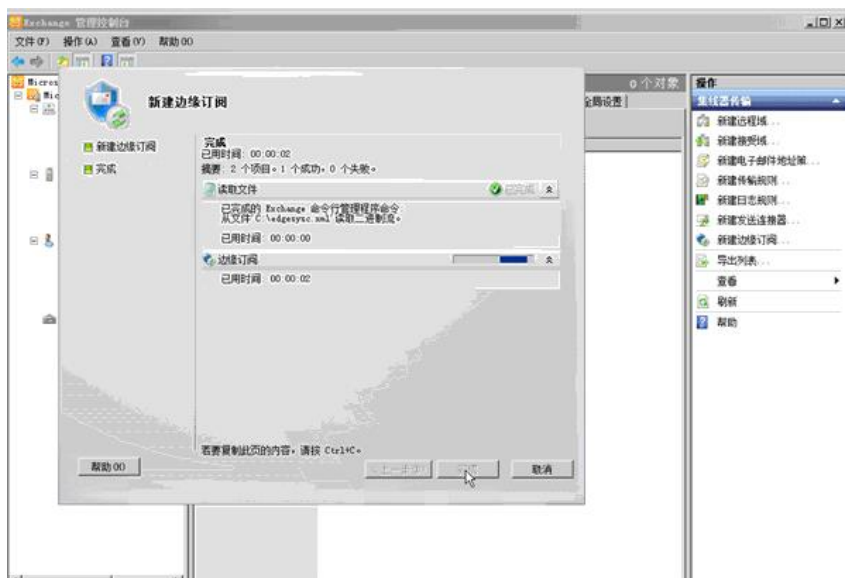
在边缘服务器生成订阅文件，包含边缘服务器的一系列信息，然后拷贝到HUB，在HUB服务器上进行导入，导入的同时生成相应的发送连接器，然后让HUB和EDGE之间进行同步。

首先生成订阅文件。

```
(PS) C:\Windows\system32>New-EdgeSubscription -FileName c:\edgesync.xml

确认
如果您创建“边缘订阅”，则可以此边缘传输服务器方便地通过 EdgeSync
进行管理。作为结果，将删除手动创建的以下任何类型的对象：
接受域、邮件分配、传输域和发送连接器。在创建“边缘订阅”后，必须从组织内部管理这些对象，并且允许 EdgeSync
更新边缘传输服务器。而且，在同步过程中 TransportConfig 对象的 InternalSMTPServers 列表将被覆盖。
EdgeSync 要求此边缘传输服务器能够解析 Active Directory
站点(该站点为该边缘传输服务器订阅到的站点)内集线器传输服务器的完全限定的域名(FQDN)。这些集线器服务器必须能够解析
传输服务器的 FQDN。您应在随后的“1440”分钟内完成组织内部的边缘订阅。“1440”分钟 bootstrap 帐户将过期。
(Y) 是(Y) (N) 全否(N) (L) 全否(L) (G) 挂起(G) (F) 帮助 <默认值为“Y”>: a
```

然后把文件拷贝到HUB上，进行导入。在组织配置，集线器传输，选择新建边缘订阅。



然后生成两个发送连接器。会同步到edge服务器，同时HUB上的接受域也会同步到EDGE。



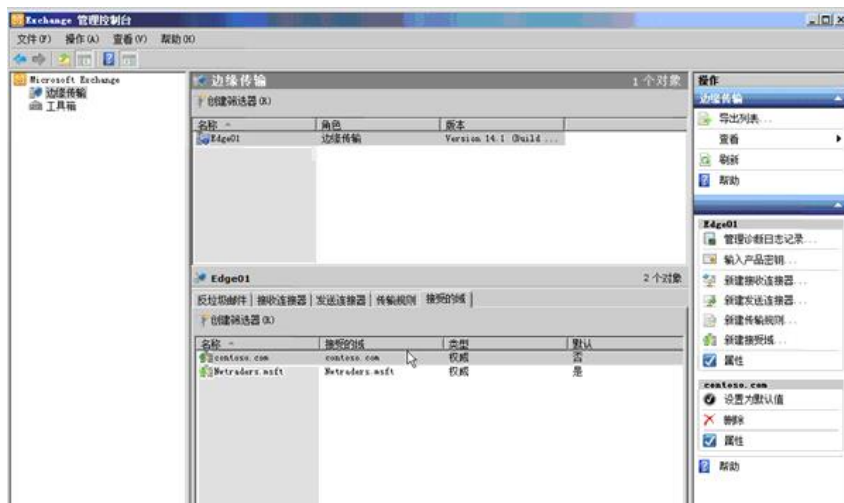
可以进行手动同步。否则在exchange 2007需要4小时，exchange 2010需要等待30秒同步到EDGE服务器。同步了配置信息和收件人信息。


```
计算机: Edge01.Metradex.mst
[PC] C:\Windows\system32>Start-EdgeSynchronization

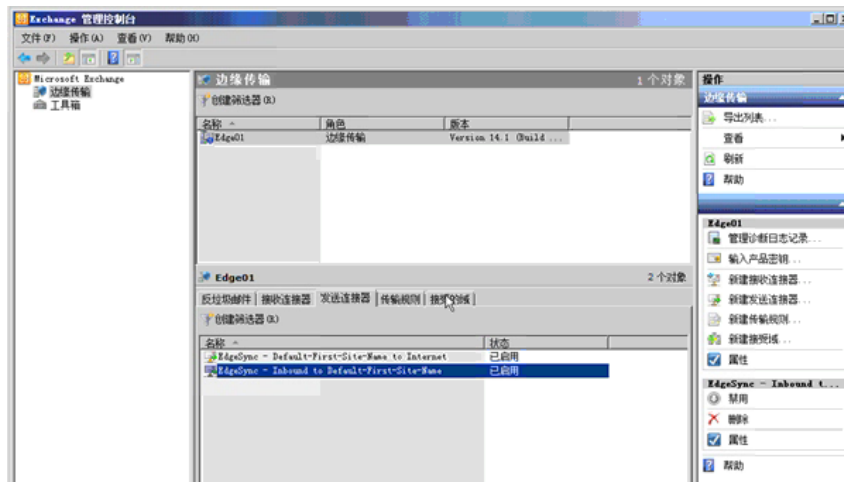
RunspaceId : 12f1b075-afa2-47d7-9929-ee0b5d40c967
Result      : Success
Type        : Recipients
Name        : Edge01
FailureDetails :
StartUTC    : 2011/4/22 6:53:32
EndUTC      : 2011/4/22 6:53:33
Added       : 0
Deleted     : 0
Updated     : 0
Scanned     : 0
TargetScanned : 0

RunspaceId : 12f1b075-afa2-47d7-9929-ee0b5d40c967
Result      : Success
Type        : Configuration
Name        : Edge01
FailureDetails :
StartUTC    : 2011/4/22 6:53:32
EndUTC      : 2011/4/22 6:53:33
Added       : 0
Deleted     : 0
```

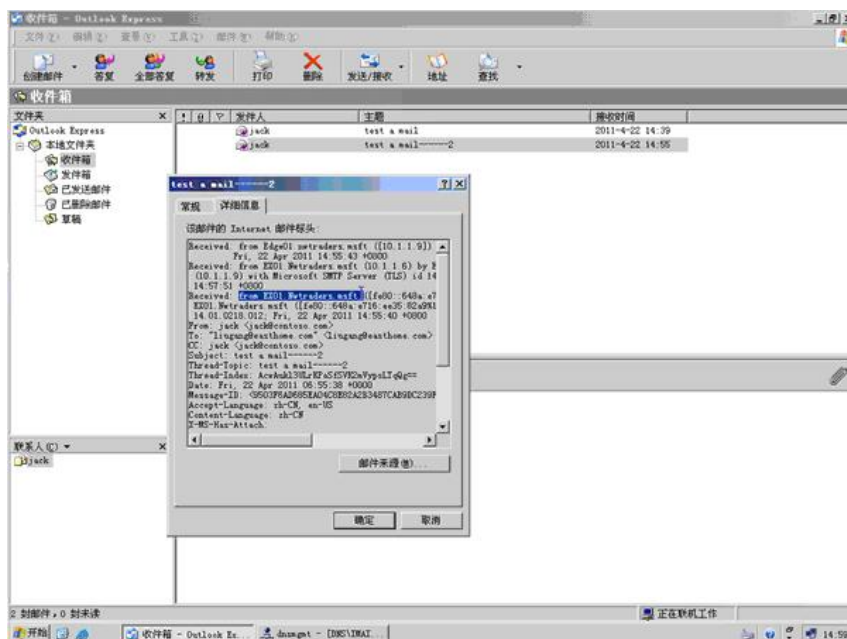
信息已经同步过来了。



连接器信息也过来了。



可以查看客户端邮件的投递信息，从哪些服务器到哪些服务器。



对于EDGE服务器的高可用技术如何实施？

边缘克隆

- ◆ 配置多个边缘服务器是实施高可用的一种解决方案。
- ◆ 使用**ExportEdgeConfig** 脚本从第一台边缘服务器上导出配置信息
- ◆ 使用**ImportEdgeConfig** 脚本把导出的配置信息导入第二台或其它边缘服务器。

边缘克隆做起来比较麻烦。

上图的两个脚本文件的位置在哪里？

