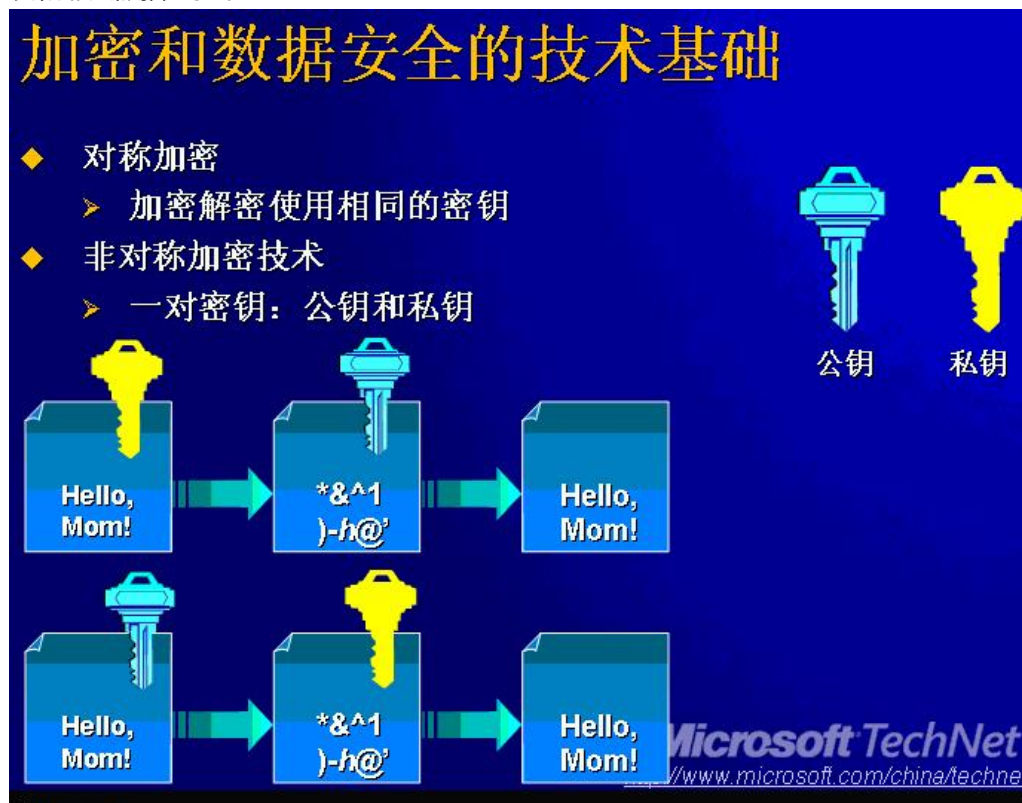


电子邮件的安全需求：传送过程中不能够被窃取和更改、证明发件人身份、邮件保存的安全、针对邮件内容再分发和非法散播的控制。



S/MIME在安全方面的功能又进行了扩展，它可以把MIME实体(比如数字签名和加密信息等)封装成安全对象。RFC 2634定义了增强的安全服务，例如具有接收方确认签收的功能，这样就可以确保接收者不能否认已经收到过的邮件。微软将在未来的Office 2000新版本中包含这些服务。S/MIME增加了新的MIME数据类型，用于提供数据保密、完整性保护、认证和鉴定服务等功能，这些数据类型包括“应用 /pkcs7-MIME” (application/pkcs7-MIME)、“复合/已签名” (multipart/signed) 和“应用 /pkcs7-签名” (application/pkcs7-signature) 等。如果邮件包含了上述MIME复合数据，邮件中将带有有关的MIME附件。在邮件的客户端，接收者在阅读邮件之前，S/MIME应用处理这些附件。如表1所示，附件的扩展名因复合数据类型所提供的S/MIME服务的不同而异。在MIME的头部，标识了MIME附件的名字。一些邮件客户端，如果没有安装具有S/MIME能力的系统，或安装的是早期S/MIME的版本，也需要通过这些附件来识别邮件中和S/MIME有关的内容。其他邮件客户端则更是完全依靠复合数据信息识别MIME实体。

使用S/MIME保证邮件安全

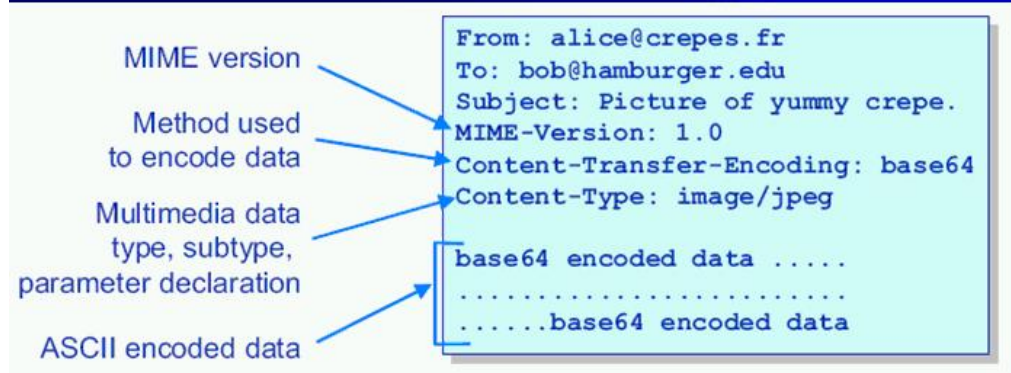
- ◆ 证明发件人的身份
- ◆ 信息的完整性
- ◆ 隐私保护和数据的安全性



默认邮件再编码过程中，是非加密的MIME。

邮件的内容是如何被传送的

- ◆ SMTP要求所有传输的内容必须都为 7-bit ASCII码
 - 所有非ASCII内容在传送前都要经过编码
- ◆ 在邮件头中的额外空行用来标示MIME类别



Secure MIME的原理。

什么是S/MIME

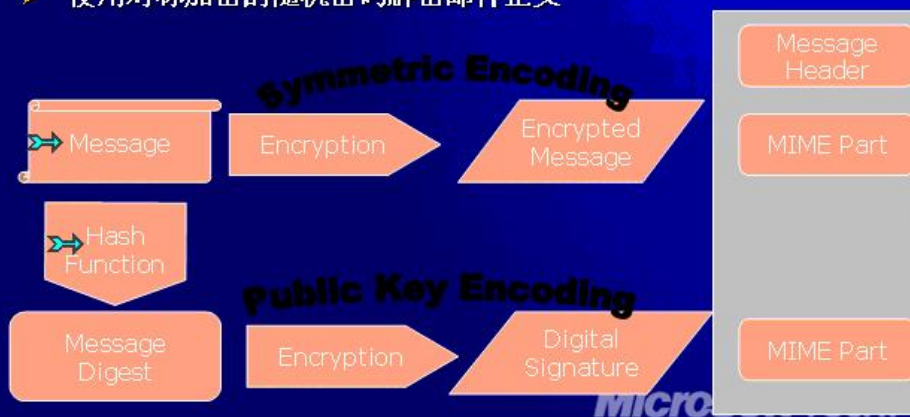
- ◆ 基于**MIME**的一种邮件加密技术
- ◆ 工作原理
 - 同时使用对称加密和非对称加密
 - 对称加密的密钥随着邮件一起传送
 - 使用收件人的公钥加密邮件头和包含对称加密密钥的共享敏感数据
 - 使用数字签名来保证邮件内容不被篡改

S/MIME的加密过程

- ◆ 对邮件正文进行散列计算，并声称一个散列值(message digest)
- ◆ 使用发信人的私钥加密散列值
 - 如果收信人根据邮件正文计算出来的散列值跟原始值不匹配，这邮件内容在传输过程中可能被篡改
- ◆ 使用对称加密密钥(随机生成)加密邮件正文
- ◆ S/MIME邮件由三部分组成
 - 邮件散列值，**Message Digest (digital signature)**
 - 对称加密随机密钥 (**transmitted with message**)
 - 加密的正文

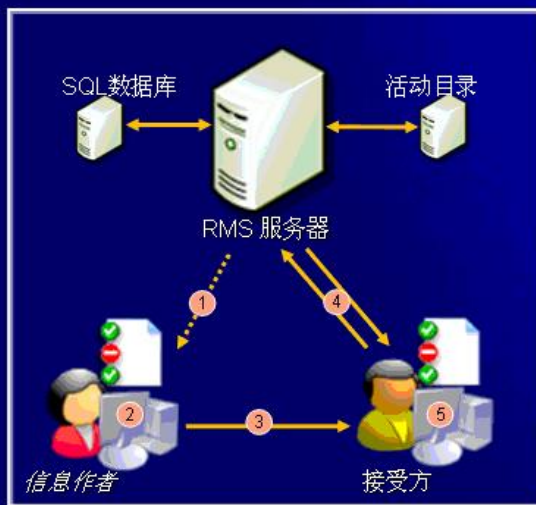
S/MIME的解密过程

- ◆ 使用发信人的公钥解密邮件的散列值
 - 确保邮件传送过程中没有被篡改
- ◆ 使用收件人的私钥解密对称加密的随机密码
 - 获取对称加密随机密码
 - 使用对称加密的随机密码解密邮件正文



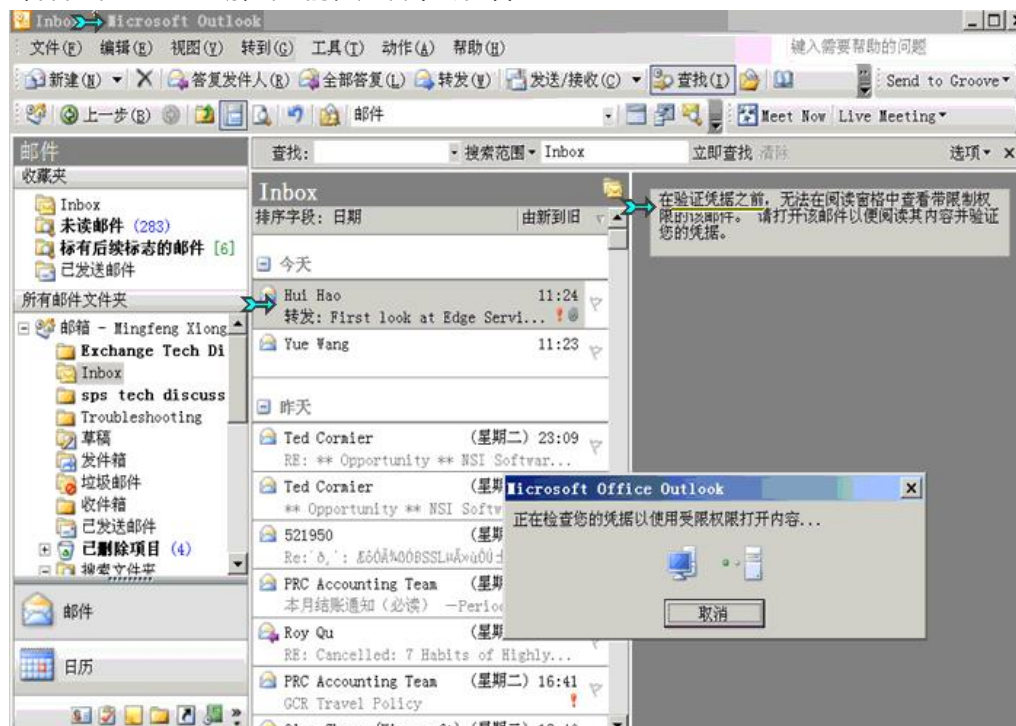
使用S/MIME的两种方式：1) 使用私有CA颁发的证书；2) 使用public证书。

Windows RMS的工作流程



1. 原作者在第一次配制内容权限保护时收到一个识别身份证书。
2. 作者对内容定义一系列的使用权限，兼容的应用程序在文档中实现设定，并嵌入加密部分。
3. 作者分发文件。
4. 接受方收到文件后，应用程序在打开时连接RMS服务器，并验证所有的设置。
5. 应用程序现实文档内容并实现所有的限制。

邮件在未经过RMS解密之前，是看不到内容的。



反病毒软件一定要设置好，否则会导致服务器不正常工作，比如数据库损坏。

CAS/HUB服务器上没有必要安装针对邮箱的防病毒软件。

反病毒软件安装建议和优化步骤

◆→各司其职

- 系统级别的防病毒软件
- 邮件专用的防病毒软件(针对邮件数据库)

◆ OWA服务器，SMTP网关上没必要安装针对邮箱的防病毒软件

◆ 把Exchange文件夹从系统防病毒软件中移除

如果邮件数据巨大，那么病毒扫描会占用大量资源和时间。扫描的时候会做大量的CPU运算。
通过性能计数器来查看监控防病毒扫描对服务器的总体影响。

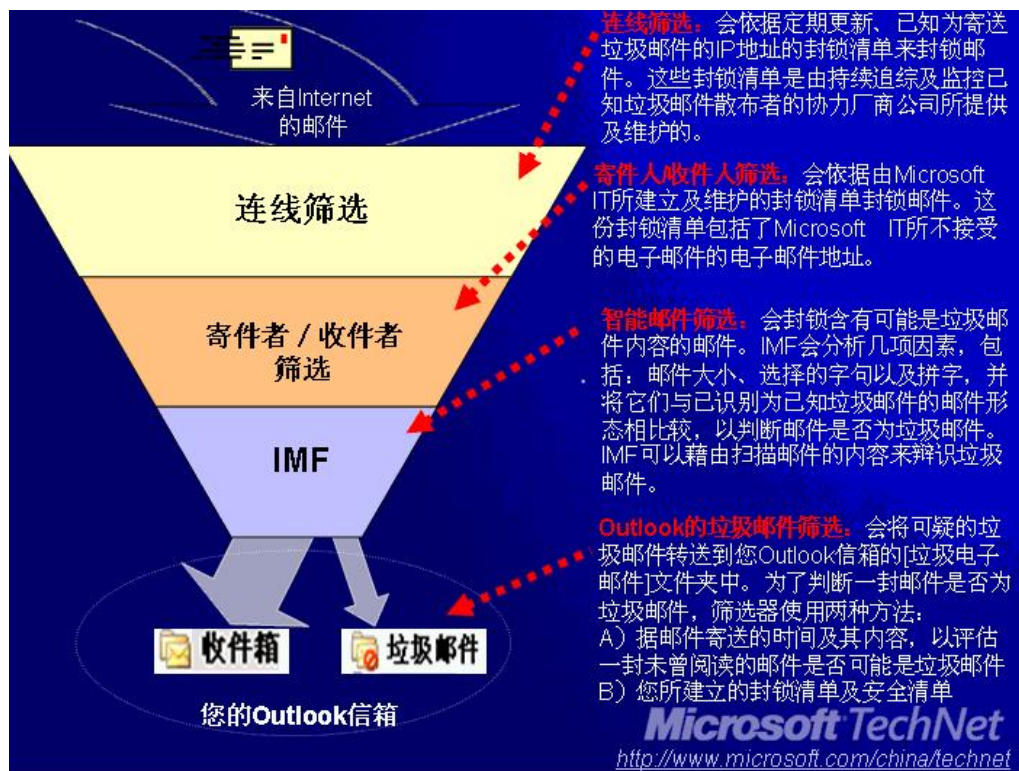
病毒扫描和系统性能的平衡

MSExchangeIS	
Virus Scan Bytes Scanned	0
Virus Scan Files Cleaned	0
Virus Scan Files Cleaned/sec	0.000
Virus Scan Files Quarantined	0
Virus Scan Files Quarantined/sec	0.000
Virus Scan Files Scanned	0
Virus Scan Files Scanned/sec	0.000
Virus Scan Folders Scanned in Background	0
Virus Scan Messages Cleaned	0
Virus Scan Messages Cleaned/sec	0.000
Virus Scan Messages Deleted	0
Virus Scan Messages Deleted/sec	0.000
Virus Scan Messages Processed	0
Virus Scan Messages Processed/sec	0.000
Virus Scan Messages Quarantined	0
Virus Scan Messages Quarantined/sec	0.000
Virus Scan Messages Scanned in Background	0
Virus Scan Queue Length	0

如果系统没有特别严重的瓶颈，比如CPU慢，那防病毒软件对服务器的性能不会有太大的影响。

Exchange反垃圾邮件和IMF最佳实践

- ◆ 立体的防御结构
- ◆ 平衡垃圾邮件过滤和正常邮件的误判
- ◆ 需要用户的配合，客户端的操作
- ◆ 灵活的调整和白名单策略



IMF智能邮件筛选。

分值越高, 越有可能是垃圾邮件。可以在邮件服务器上配置相应的SCL的分值。

建议: 1-3的放到用户邮箱。3-5的放到用户的垃圾邮件收件夹里。

如果设置了归档垃圾邮件, 那要规划归档目录, 最好手动移动到非系统盘, 归档的邮件为eml格式, 可以通过IMF archive manager来查看, 可以很快找出来误判的邮件。

IMF也会有一些更新, 比如检测垃圾邮件的方式, 可以通过windows update进行更新, 如果配置IMF自动更新, 需要更改注册表。

充分发挥IMF的威力

◆ IMF的微调

- 调整服务器端归档邮件保存文件夹路径
- 配置IMF在保存邮件时一同保存邮件的SCL等级

◆ 自定义IMF关键字

- regsvr32 Drive_letter:\Program Files\Exchsrvr\bin\MSCFV2\MSEExchange.UceContentFilter.dll
- MSEExchange.UceContentFilter.xml

◆ IMF引擎和定义文件的自动更新

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Exchange\ContentFilterState

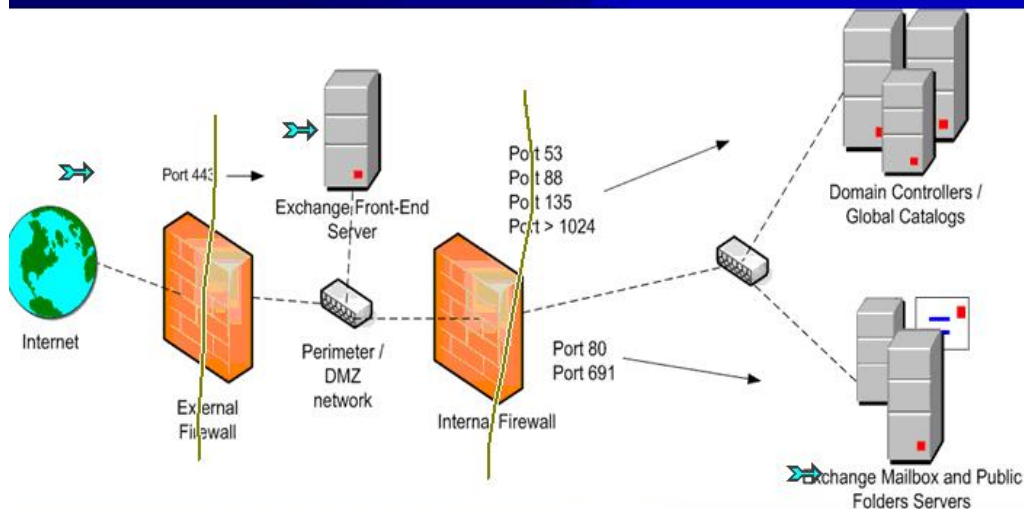
◆ 使用IMF归档邮件查看器

- IMF Archive Manager

可以在第一道和第二道防火墙之间放置exchange的SMTP和前端服务器。

IMF针对有图片的邮件, 也会有相应的措施, 比如把邮件的SCL级别识别的较高。

Front-end servers in DMZ



51CTO下载-14ExchangeServer白手起家系列之十四：存储备份策略

数据存储和备份是邮件系统平稳可靠运行的保证，也是灾难恢复的前提。

关于Exchange数据存储的一些建议

◆ 每服务器支持500和5000个邮箱的区别

优点

显著降低管理成本
对存储硬件的利用率高
充分利用数据中心的硬件基础架构

顾虑

备份完成的速度
灾难恢复的高要求

分区尽量以物理的RAID为区分。

低价位的硬盘作为备份硬盘。

关于Exchange数据存储的一些建议

◆ RAID，RAID，RAID！

- ◆ 分区尽量以物理的RAID阵列为单位
- ◆ 每个分区的功能要明确，并尽可能单一
- ◆ 禁用NTFS高级特性，禁用压缩和磁盘配额
- ◆ 大型系统尽可能使用SAN来节省远期投入
- ◆ 高速磁盘和低价位磁盘混合使用，各司其职

对齐磁盘扇区以获取最大的性能。

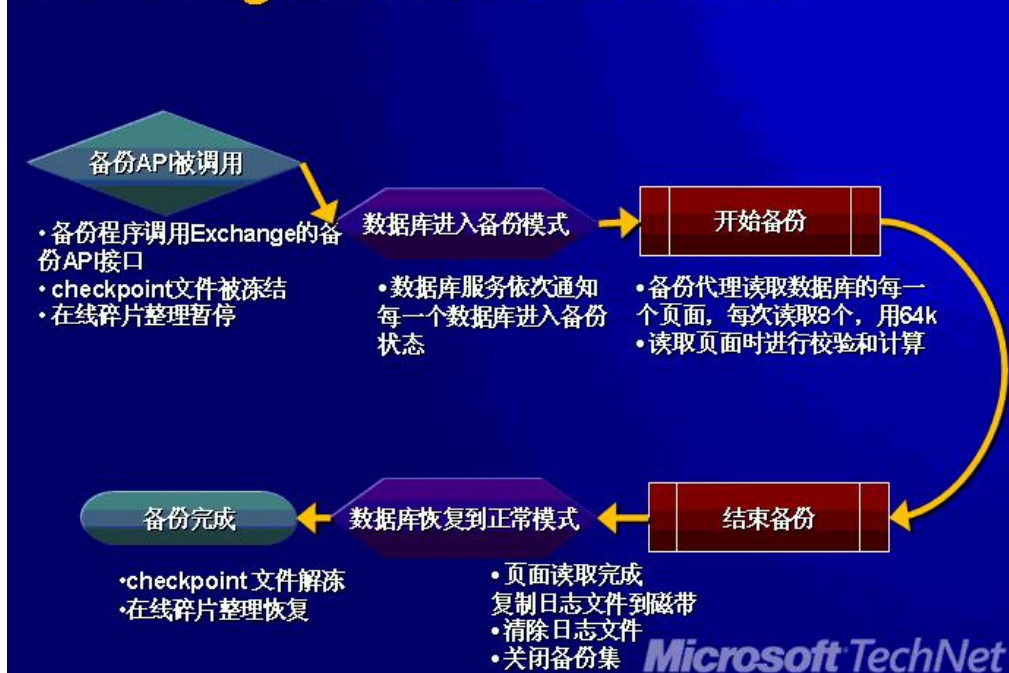
windows 2000使用diskpar，包含在resourceKIT里面。

大多数情况下，应使用 **DiskPar** 来使硬盘磁道与物理磁盘分区对齐。由于 Windows 2000 和 Windows Server 2003 将最大隐藏扇区数限制为 63，因此，对于每个磁道具有 63 个以上扇区的磁盘，其默认启动扇区是第 64 个扇区。Windows 2000 和 Windows Server 2003 所创建的所有分区都从第 64 个扇区开始，这使得写入磁盘的每八个数据块中有一个数据块会跨越两个磁道。要使用 DiskPar 来对齐硬盘，请执行以下步骤。

- 备份硬盘上的所有数据，然后删除所有分区。
- 在命令提示符处，键入 **diskpart -s <驱动器号>**，然后确认您要对磁盘分区。
- 键入该硬盘的新起始偏移量和分区大小。由于 Exchange 以 4 KB 数据块为单位写入数据，因此所键入的起始偏移量的值必须是 4 KB 的倍数。
- DiskPar 对齐磁盘之后，在命令提示符处，键入 **diskpart -i <驱动器号>**，以验证磁盘已正确对齐。
- 使用磁盘管理器对硬盘进行分区。将分区配置为使用 NTFS，并使用 4096 (4 KB) 作为分配单位大小。
- 使用 DiskPar 提高磁盘性能并格式化磁盘分区。使用 DiskPar 之前，务必备份想要保留的所有数据。DiskPar 是 Windows 2000 资源工具包的一部分。有关使用 Diskpart.exe 的详细信息，请参阅 Microsoft Windows 2000 资源工具包的帮助。

磁盘分区对齐后，对于exchange来说性能会有15%-20%的性能提升。

Exchange的备份的幕后细节



一定会导致checkpoint冻结，也就是checkpoint指向的某个文件一部分已经同步到数据库，一部分还没有写入到数据库。

但是备份进程依然会把checkpoint指向的那个文件完全拷贝到备份集里面。因为虽然一个文件的一部分写到数据库，一部分没写到数据库，但是备份进程没有办法把一个文件分开。

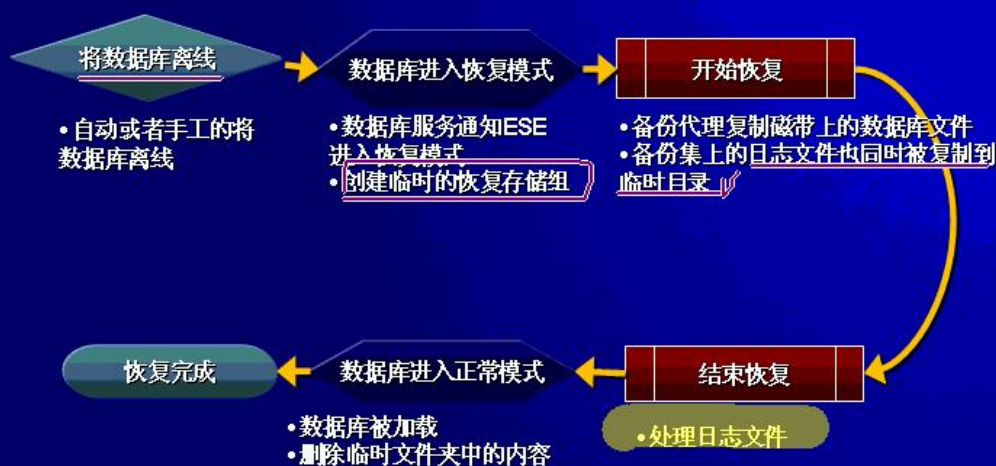
在恢复的时候，会发现，恢复的那个文件只有一半（也就是写到数据库的那个部分）。

- ◆ Information Store服务必须启动，所有数据库都要被Mount
- ◆ 可以备份整个存储组，也可以备份单一的数据库
- ◆ 支持同时进行备份和恢复(针对不同的数据库)
- ◆ 事务日志文件的清除
- ◆ 长时间等待的备份任务可能导致数据库离线或停止工作
 - 超过1024个未提交日志会使数据库离线

备份类型比较

Type	Copies DB	Copy Logs	Truncates Logs
Full(Normal)	X	X	X
Copy/Daily	X	X	
Incremental		X	X
Differential		X	
Snapshot		X	X
Offline	X		Not recommended

Exchange的恢复的幕后细节



恢复过程的要点

- ◆ **MSExchangeIS**服务在恢复时必须正常运行
- ◆ 被恢复的数据库需要离线
 - 手工设置数据库的可覆盖属性
- ◆ 其余的数据库不受影响，可以正常使用
- ◆ **System Attendant** 服务不参与恢复过程
- ◆ **Restore.env**文件
- ◆ 使用命令行进行硬恢复(**Hard recovery**)
 - **Eseutil /cc**

恢复数据库时**Log**文件的重演过程

- ◆ 检查**Log**文件的签名
- ◆ 重演(**replay**)日志文件
 - 首先从临时文件夹中被恢复的日志开始
 - 接着从存储组的日志中进行**Replay**
 - 如果启用了循环日志，则不进行任何**Replay**
 - In this case the database will be rolled back to the date of backup
- ◆ 如果仅恢复存储组中的一个数据库，程序会选择从日志序列中恢复跟此数据库有关的日志

微软内部**Exchange**系统的备份方案

Situation

- ◆ As part of the internal rollout of Microsoft® Exchange 2003 and the Microsoft Windows Server System™ at Microsoft, Microsoft IT began to consolidate messaging servers to reduce operating costs. High availability requirements for the clustered server redesign prompted Microsoft IT to examine its backup and restore solution.

Solution

- ◆ Microsoft IT implemented a two-step backup solution and the Exchange 2003 Recovery Storage Group (RSG) feature that minimizes user downtime during a database recovery. The new solution supports server consolidation with high availability while providing greater backup and restore flexibility.

Benefits

- ◆ Increased server ability during single node failures
- ◆ Reduced operating costs from server consolidation
- ◆ Minimized impact to users during backup using an alternate passive node in the clustered configuration
- ◆ Flexible recovery solution allowed users to continue working while restoration of mailbox/database was done offline and merged later

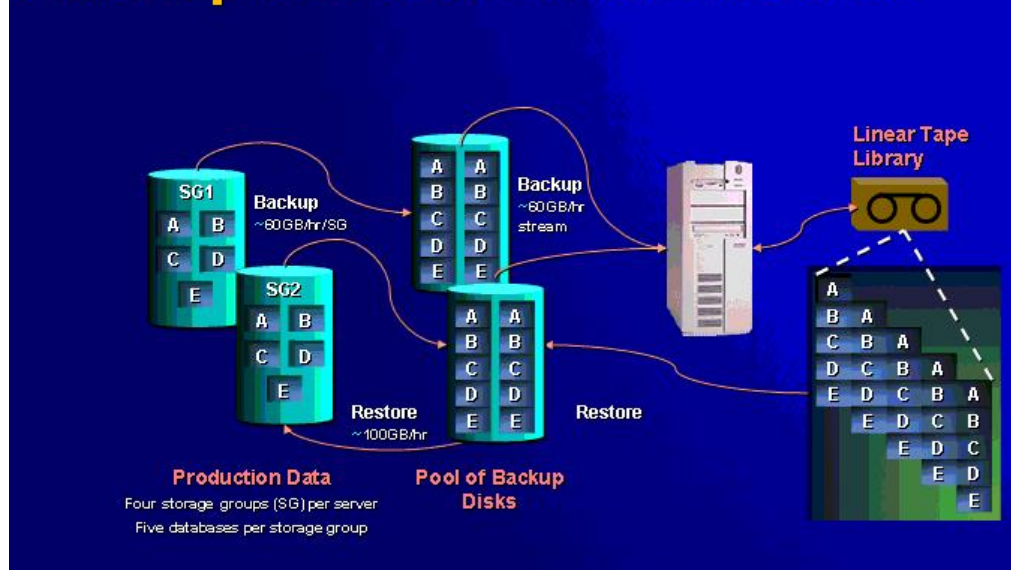
恢复的时候要考虑用户，先为用户恢复服务，比如先让用户可以收发邮件，然后再给用户做数据恢复、导出和合并。

总结：备份和恢复的原则

- ◆ Restore mail service immediately; restore data later.
- ◆ New e-mail vs. historical data
- ◆ Why swap databases?
 - When should you use this method?
 - Q282496: Considerations and Best Practices When Resetting an Exchange Mailbox Database
 - Dramatically reduce EXMerged data
 - Preserve single instance storage and avoid database bloat
- ◆ Send immediate status email
 - Data is being recovered, but service has been restored in the meantime
 - Time expectations
 - If you intend to swap back in the original database, users should not reconfigure rules, views, offline files
 - Merge process

压力比较大或者用户比较频繁的时候，建议备份窗口越短越好。这样恢复的时间也相对较短。

Backup Solution Architecture



15Exchange Server白手起家系列之十五：你的系统可靠性有几个9？

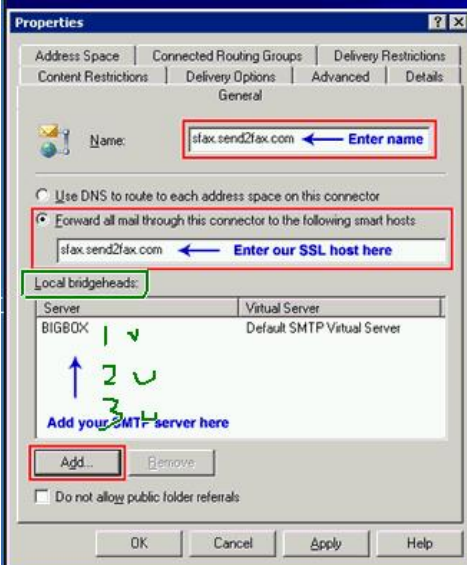
收邮件的冗余设计。

可以通过三个MX记录，权重一样，那会随机选择一个MX记录。

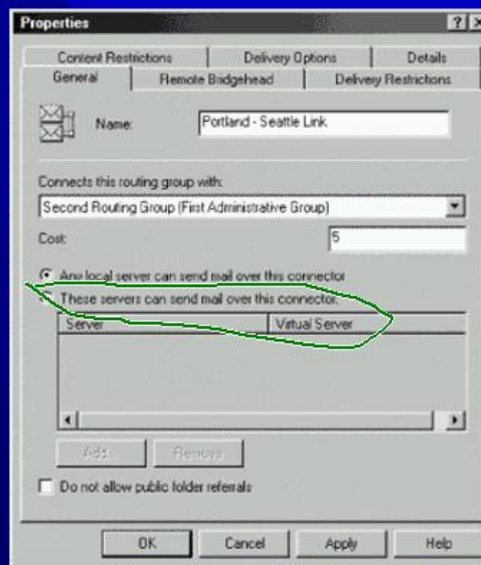
SMTP和桥头堡服务器的冗余设计

- ◆ 通过DNS的方式实现SMTP接收邮件的冗余
- ◆ 通过为SMTP连接器配置多个桥头堡的方式实现外部邮件发送冗余
- ◆ 通过为路由组连接器配置多个桥头堡的方式实现内部邮件发送冗余

→ SMTP连接器



→ 路由组连接器



每个路由组都有一个桥头堡服务器，负责邮件的发送和接收。

微软集群技术概述

- ◆ Network Load Balancing Cluster (NLB)
- ◆ Component Load Balancing (CLB)
- ◆ Server Cluster
- ◆ Compute Cluster
- ◆ NLB和CLB是基于局域网的负载平衡技术，不需要额外的硬件支持
- ◆ Server Cluster是面向容错的集群技术，在硬件上需要网络共享存储和双网卡的支持
- ◆ Computer Cluster是数据处理和科学计算上使用的集群技术，在硬件上至少需要双网卡的支持

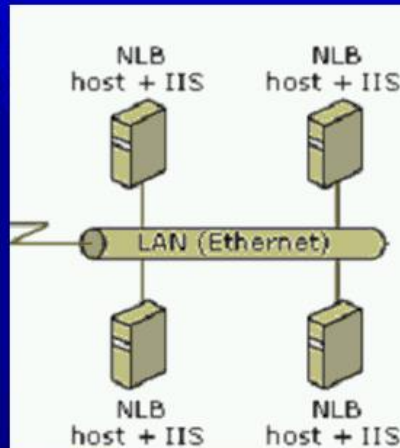
一般SMTP连接器有一个就够了，除非对一些邮件组织有特殊的要求。桥头堡服务器配置SMTP连接器。

SMTP和路由组是在exchange应用里面的路由，和跨网段路由器的那种路由是没有关系的。

NLB的每台机器都可以独自处理访问请求，不需要与其他的机器进行协商，采用散列算法的技术。

Network Load Balancing (NLB)

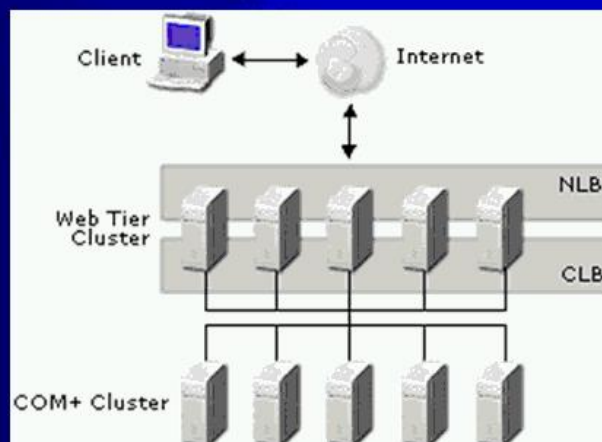
- ◆ **NLB** 是无状态的
- ◆ **Web, Terminal**和 **VPN** 服务可以使用**NLB**作冗余和负载平衡
- ◆ 通过**MAC**地址共享的方式组成集群



CLB做COM+组件的负载平衡，也是基于NLB的。

Component Load Balancing (CLB)

- ◆ **CLB**是无状态的
- ◆ **Web COM+** 服务可以通过**CLB**作冗余和负载平衡
- ◆ 基于**NLB**

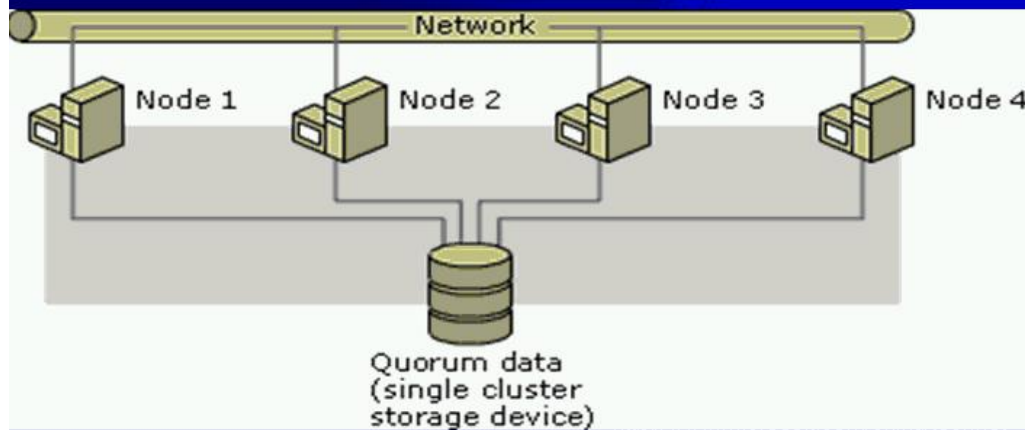


仲裁盘保存了一些cluster的全局信息。

在私有网络里通过心跳网卡完成彼此间的通信。

Server Cluster

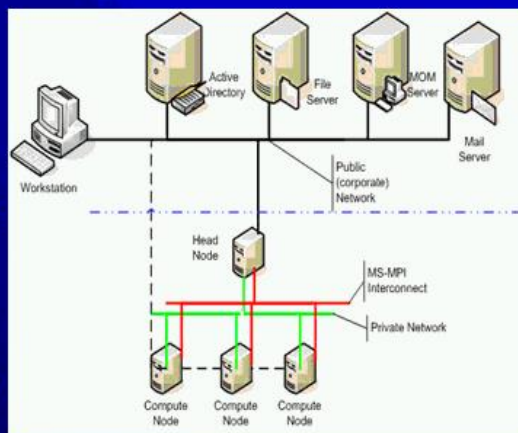
- ◆ 集群的状态保存在共享的仲裁磁盘上(quorum disk)
- ◆ SQL, Exchange, 文件和打印共享可以借助Server Cluster环境来实现冗余和故障转移
- ◆ 集群通过在私有网络上的TCP/UDP进行通信



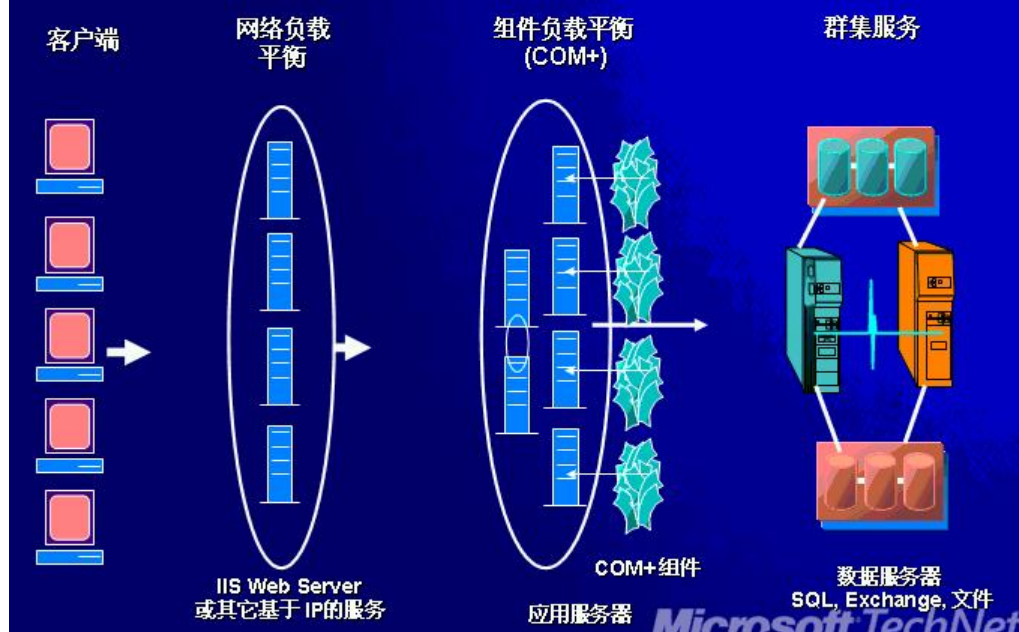
把大的计算量分拆到多个节点上进行计算。需要专门的windows compute cluster版本。

Compute Cluster

- ◆ 至少一个核心节点必须运行 Windows Compute Cluster版本的操作系统,其余计算节点可以运行 Windows x64
- ◆ 可以通过Windows 2003或Windows XP进行远程管理和任务计划
- ◆ 使用MS-MPI C语言, Fortran77, 和Fortran90
- ◆ 可以使用PXE进行计算节点的部署



Windows下的集群全家福

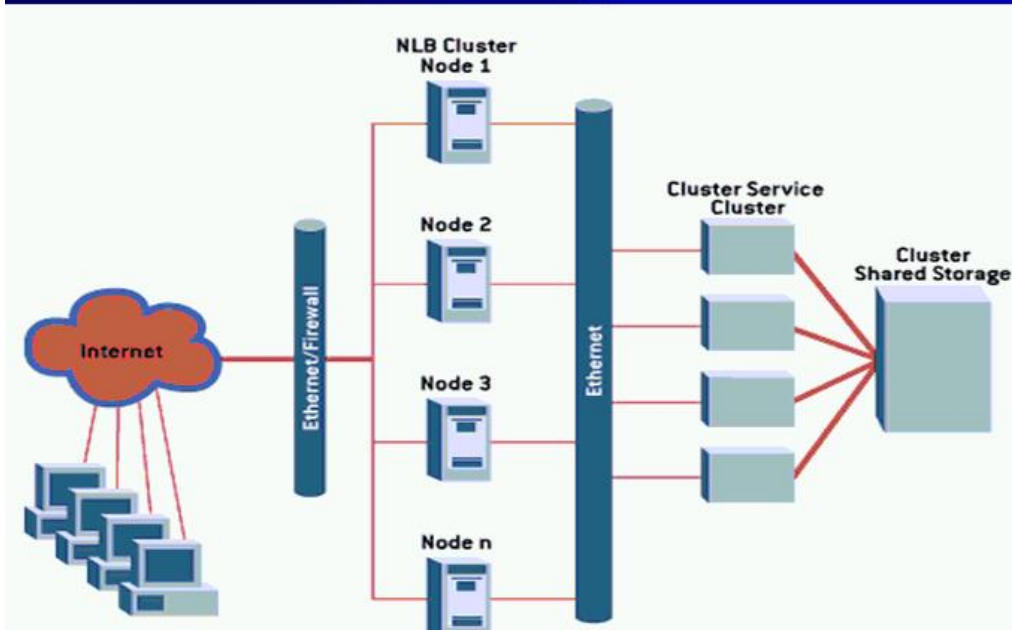


NLB不能跨三层设备。

Windows NLB在Exchange系统中的应用

- ◆ IP 连接最多可延伸至32台机器
 - www.microsoft.com 和 www.msn.com 每个群集有18-24台机器
- ◆ 所有在同一个 NLB 群集中的机器共享一个虚拟 IP 地址
- ◆ 这些机器通过发送一个规则的脉冲信号来检测机器故障
- ◆ 对其它群集技术进行补充
 - SQL Server™, Exchange, 文件/打印, 等等
- ◆ NLB的实现
 - UDP/2504 注册端口应被用于 NLB
 - 只能用 TCP 或 UDP 连接 — 也就是说, 不能用 ICMP 或其它
 - 群集的网络信息中心必须在相同的广播域内 — 也就是说, 如果使用交换器的话, 只能用两层的交换器而不能用三层的

NLB架构概述

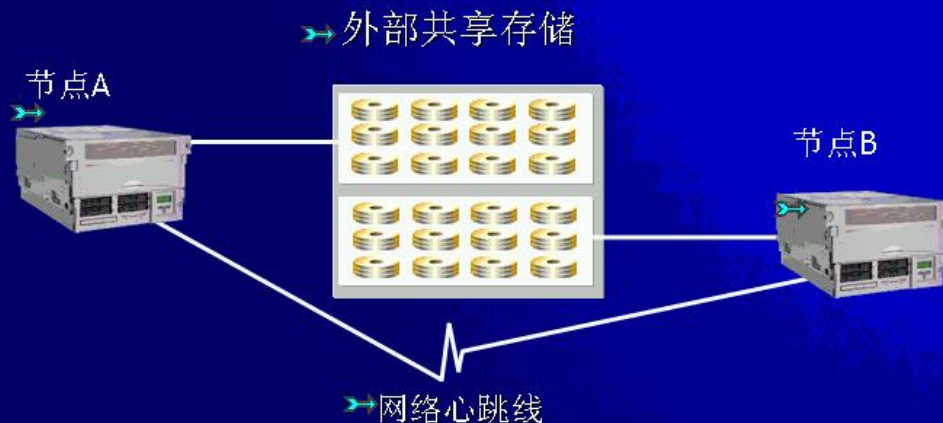


Windows NLB在Exchange系统中的应用

◆ 最佳实践

- 它只对所有应用程序的第一层，也就是介绍层有作用
- 用两个以上的网络信息中心能够提高整体的性能
- 如果存在一个以上的网络适配器—要确保 NLB 有效，并只在其中的一块网卡上进行配置
- 在群集适配器上—除了TCP/IP不要安装其它任何协议
- 确保不同的群集适配器上保持一致的配置和端口规则
- 确保主机参数唯一
- 确保群集的 IP 地址也在 TCP/IP 设置中列出
- 确保专用的 IP 地址总是列在群集的 IP 地址前
- 即使你能把“AliveMsgPeriod”设置为十分之一秒—也绝对不要把它设置为小于一秒（或一千毫秒）
- 不能把“AliveMsgTolerance”设置为少于五个周期
- 如果因为 IP 地址冲突而在“拨号连接”中去掉“网络负载平衡”选项，这并不是个好方法—应该用“wlbs.exe”来启用或禁止端口

服务器集群的概念



为什么要做集群

◆ 提供高可用性

- 在出现硬件故障时，通过故障转移来减轻由此带来的负面影响
- 通过冗余设计来提高可靠性
- 你的系统有几个9？

9的数目	每年的停机时间
99.999	5 minutes
99.99	52 minutes
99.9	8.7 hours
99	3.7 days

◆ 可管理的升级和迁移

- 滚动升级

◆ 服务器集群无法在下列情况出现时提供保护

- 共享存储损坏
- 网络故障
- 应用程序故障或数据库损坏
- 自然灾害

◆ 无法像NLB那样提供负载均衡

◆ 无法移动正在运行的应用，故障转移会导致应用状态的丢失

群集资源包括磁盘驱动器和网卡等物理硬件设备以及 Internet 协议 (IP) 地址、应用程序、应用数据库等逻辑实体。群集中的每个节点都有自己的本地资源。但群集也有共用资源，比如共用的数据存储阵列和专用的群集网络。群集中的每个节点都可以访问这些共用资源。一个特殊的共用资源是 仲裁资源，这是指共用的群集磁盘阵

列中对群集运行有着关键性作用的物理磁盘。它是节点操作（比如构成群集或加入群集）得以发生所必须具备的。

资源组 是指群集服务作为一个逻辑单元进行管理的资源集合。通过将逻辑上相关的资源分成资源组，可以非常容易地管理应用资源和群集实体。对资源组执行群集服务操作时，操作对于该组内包含的各个资源都有效。通常来说，创建资源组的目的是为了将特定应用程序服务器和客户端正常使用该应用程序而所需的全部元素都包括在一起。

下图的virtual server是指在安装exchange群集的时候，会让安装exchange为virtual server模式。

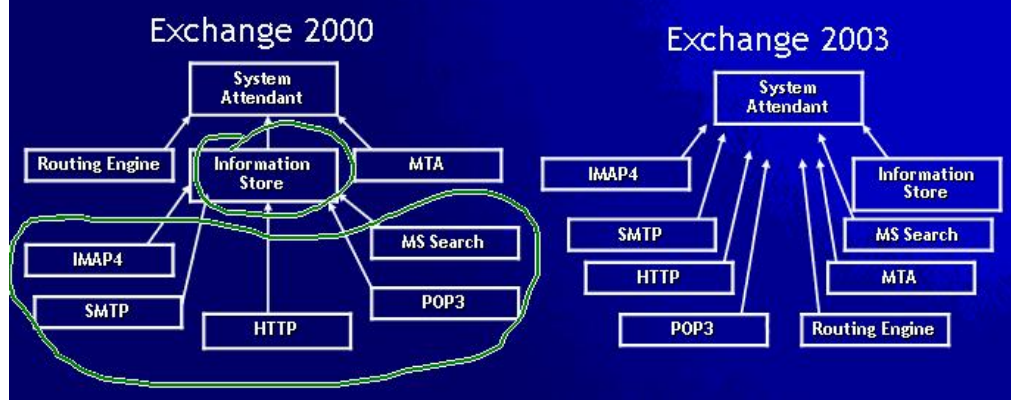
术语

◆ 有关服务器集群的重要术语

- Active/Passive
- Active/Active
- Failover / Failback
- Heartbeat
- Quorum
- Shared Storage
- Resources and Resource Groups
- Virtual Server

Exchange Server 2003集群的特色

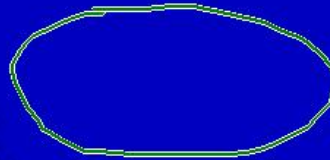
- ◆ 在前一个版本的Exchange中，除了SA以外，所有的服务都依赖于Information Store服务，必须要等Store启动完成后，剩余的服务才能依次启动，严重影响了故障转移的效率



Exchange集群的模式

◆ Exchange 集群的模式

- **Active/Passive** 是强烈推荐的集群模式
 - 集群中EVS的数量小于节点的数量
- **Active/Active**
 - 集群中EVS的数量等于甚至大于节点的数量
 - 每节点的MAPI用户数量必须小于1900
 - 每节点的CPU利用率必须小于40%
 - 故障转移可能存在潜在的问题
 - MAPI 客户端可能在故障转移时需要重新启动



◆ Exchange Virtual Server的限制

- 2个节点的情况下，EVS不能大于2个
- 多于2个的集群节点(假设为N个)情况下，EVS的数量为N-1

下面一些比较旧的服务，windows集群无法支持。

集群无法支持的服务

- ◆ ADC
- ◆ EDK Connectors
- ◆ Exchange Event Service
- ◆ NNTP
- ◆ Site Replication Service

Exchange集群的外部存储设计

- ◆ 每个节点上最多4个存储组
 - 每个存储组5个数据库
- ◆ 物理的RAID阵列 (RAID 1 or RAID 0+1)
- ◆ 共享磁盘必须为Basic NTFS分区
- ◆ 在每个EVS中，使用独立的物理磁盘做数据库和日志分区
- ◆ 每一个集群组使用专用的仲裁磁盘
- ◆ 在Win2003环境下可以使用卷安装点，有利于大型集群的管理

搭建Exchange集群

◆ 集群网络环境的设计

- 至少两块网卡，集群节点使用专用的网络做心跳信号通信
- 严禁使用网卡teaming或DHCP
- IP地址和计算机名称的分配
 - 每一个物理节点(XXX-cl01)
 - 每一个集群资源组(XXX-clr01)
 - 每一个EVS(XXX-cex01)

◆ 步骤1 - Prepare Hardware

- Apply latest system BIOS
- Apply latest device firmware
- Gather latest software drivers
- Disable unnecessary hardware

◆ 步骤2 - Install OS and Pre-Reqs

- Install desired OS (Windows Server 2003 preferred)
 - SMTP, W3SVC and NNTP services
- Add Nodes to Domain as member servers
 - DCs not supported in Exchange 2003 clusters
- Windows Update / Security Hotfixes
- Administration Tools - ADMINPAK.MSI

◆ 步骤4 - Install Cluster Service on each node. Set Quorum Log file to reset at 4096KB.

◆ 步骤5 - Install MS DTC on each node by running COMCLUST.EXE

◆ 步骤6 - Install Exchange 2003

- Unattended setup not supported
- Binaries installed locally in same location on each node
- Install one node at a time and reboot each node when finished

◆ 步骤7 - Install Exchange 2003 Service Packs and Updates

- Always update one node at a time

◆ 步骤8 - Create Exchange Virtual Server

- Create Resource Group
 - Disk Resource
 - IP Address Resource
 - Network Name Resource
 - Exchange System Attendant Resource

◆ 步骤9 - (Optional) Repeat Step 8 if using Active/Active model

◆ 步骤10 - Configure EVS Resources

- Increase pending timeout on A/A clusters

◆ 步骤11 - Bring Resources Online

◆ 在投入生产环境之前的工作

- 全面的测试故障转移
- 模拟所有可能的硬件故障
- 使用LoadSim2003作压力测试
 - Test under heavy network loads
 - Test under heavy disk I/O
 - Test under heavy services load
 - Test under large number of simultaneous logon attempts

APM/ACPI高级电源管理功能不要开启，避免进入节能模式。

- ◆ 不要在默认的Cluster Group中安装任何集群应用
- ◆ 不要将默认的Cluster Group更名，也不要删除默认的Cluster Group
- ◆ 不要在集群节点上开启和使用 APM/ACPI节点功能
- ◆ 不要使用域管理员组中的账号作为集群服务帐号

高可用性架构规划

Exchange + DC 的部署

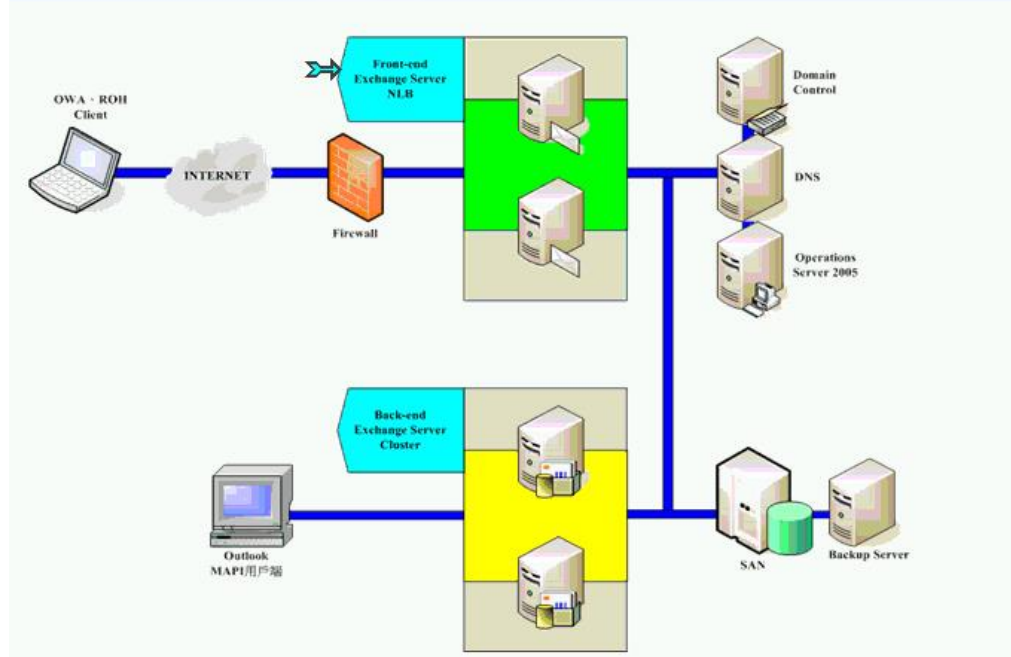
- ◆ 当DC出故障时，Exchange会自动连接另外的可用DC
- ◆ 如果只有单一的DC，在系统用户大量登陆和使用时，可能造成瓶颈
- ◆ 如果在DC上安装Exchange，并启用3GB参数，可能会使DC的性能下降
- ◆ 任何AD有关的安全问题，都可能对Exchange造成影响
- ◆ 如果在DC上安装Exchange，会发生关机时间长的问題，因为AD的服务先于Exchange服务关闭，导致Exchange的服务无法正常的结束

高可用性架构规划

前后端高可用性规划

- ◆ 前端(Front-end)可采用NLB架构
 - 有效的分散来自用户访问的压力
 - 可以避免由于网络或单机故障引起的服务中断
 - 最多32个节点
- ◆ 后端(Back-end)可采用服务器集群架构
 - 自动完成的故障转移
 - 防止应用程序和服务失败
 - 防止系统及硬件失败

典型的高可用性Exchange架构



=====