

回顾exchange server 2007的高可用解决方案

SCC使用共享存储。可以实现服务器级别的故障转移。

只有一台提供服务。使用SCC的企业比较少。

- ◆ 单一拷贝群集(SCC)本身只能提供较少的高可用性
 - 在Store失败时，SCC在同一台机器上重启Store，没有群集故障转移
 - SCC 不能自动从存储故障中恢复
 - SCC 不能保护你最宝贵的资产—数据
 - SCC 不能保护站点故障
 - CMS不能支持SCC网络冗余
- ◆ 结论
 - SCC 只提供服务器硬件的保护或蓝屏，属于比较容易恢复的部分
 - 支持滚动式升级而不丢失冗余性

第二种是LCR本地连续复制：在一台服务器上有两个存储，我们的数据可以存两份，放到两个存储里，但是服务器是一个单一故障点，LCR可以实现存储高可用，但是不能实现服务器的高可用。

第三种是CCR，群集连续复制，即实现了存储高可用，也实现了服务器的高可用，在同一个时间点只能有一台服务器提供工作。

第三种是SCR，在异地放置服务器，作为高可用备份。



缺陷。

作为CCR的成员，不能安装其他角色。必须在规划之初就考虑清楚，后期部署完成了，exchange 2007不支持在当前的生产环境基础上实施高可用，只能推倒重建。

必须搭建failover cluster群集，需要管理员具备较高的群集知识。

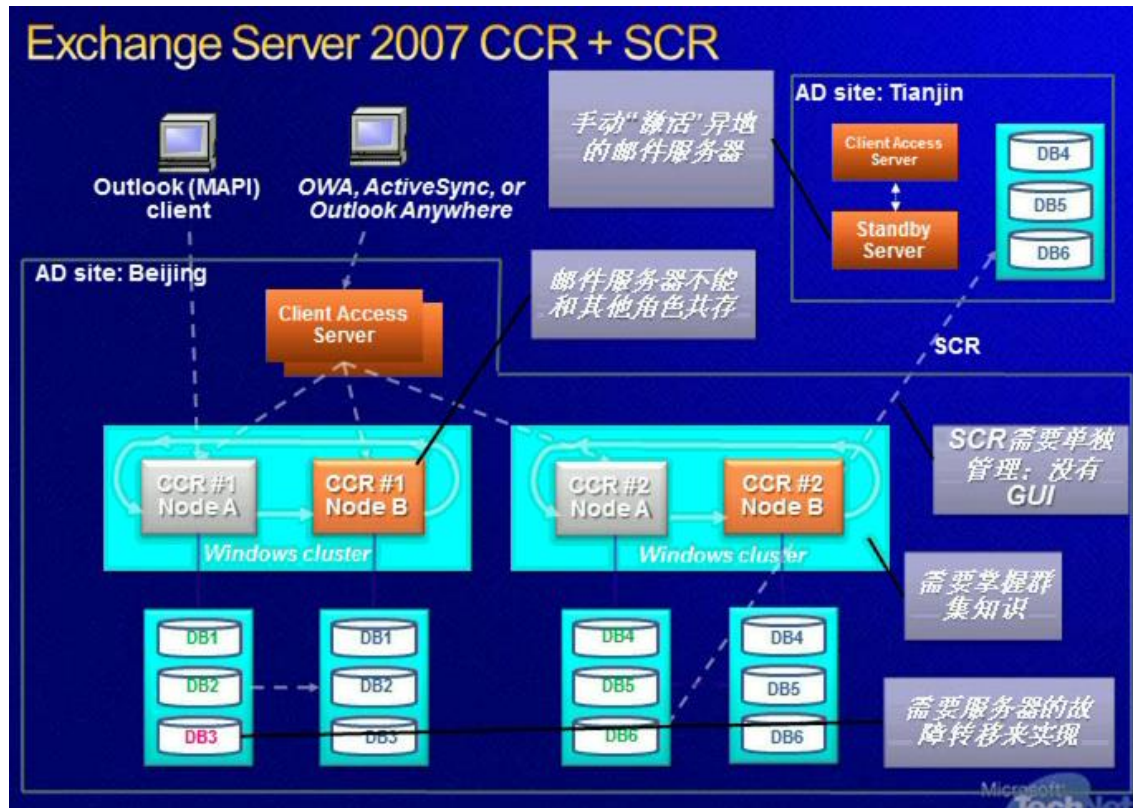
如果单个DB出问题了，那么也要进行服务器级别的切换，也就是说下图的DB1、DB2、DB3都需要切换，是服务器级别的切换。

SCR需要单独管理：没有GUI界面。

异地的邮件服务器需要手动激活。

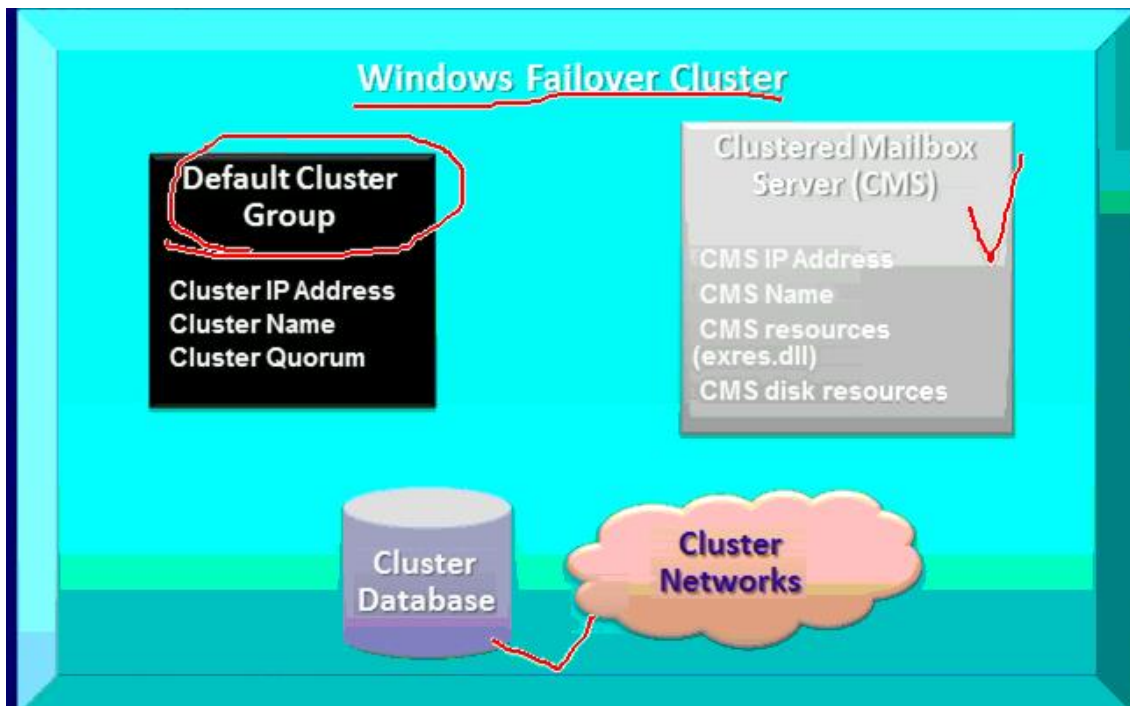
当前的CCR群集只支持2节点。只有一个节点是激活状态。另外一个节点是完全闲置的。

需要较好的存储支持，如果通过SATA磁盘实现性能相当差。

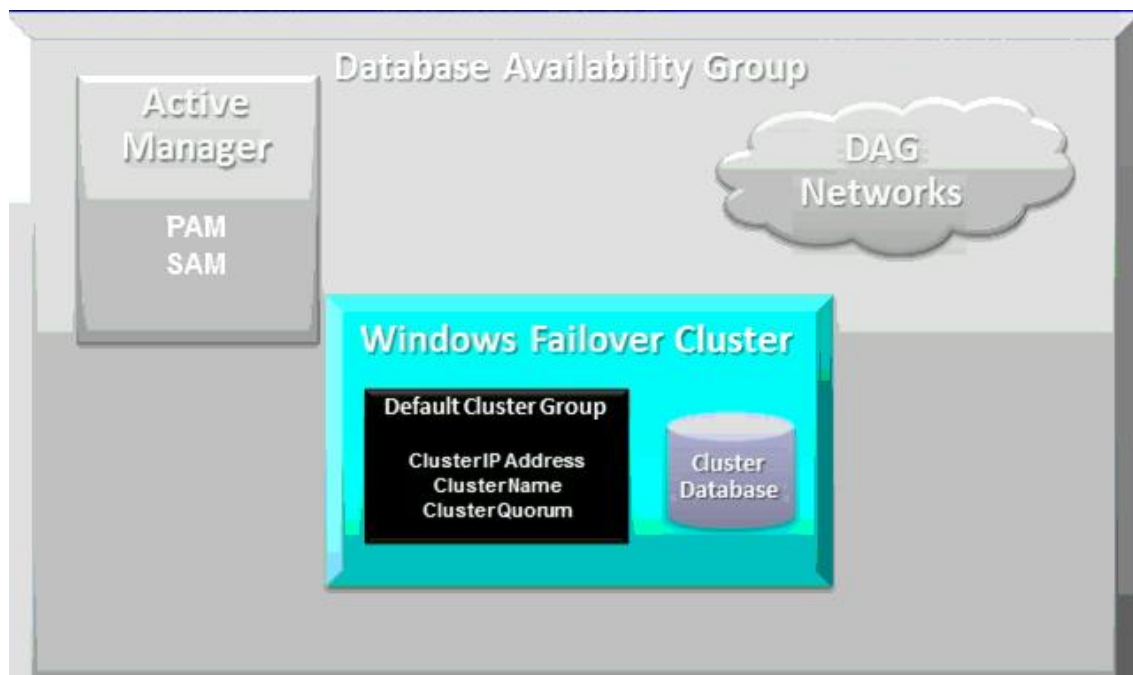


核心架构的改变。

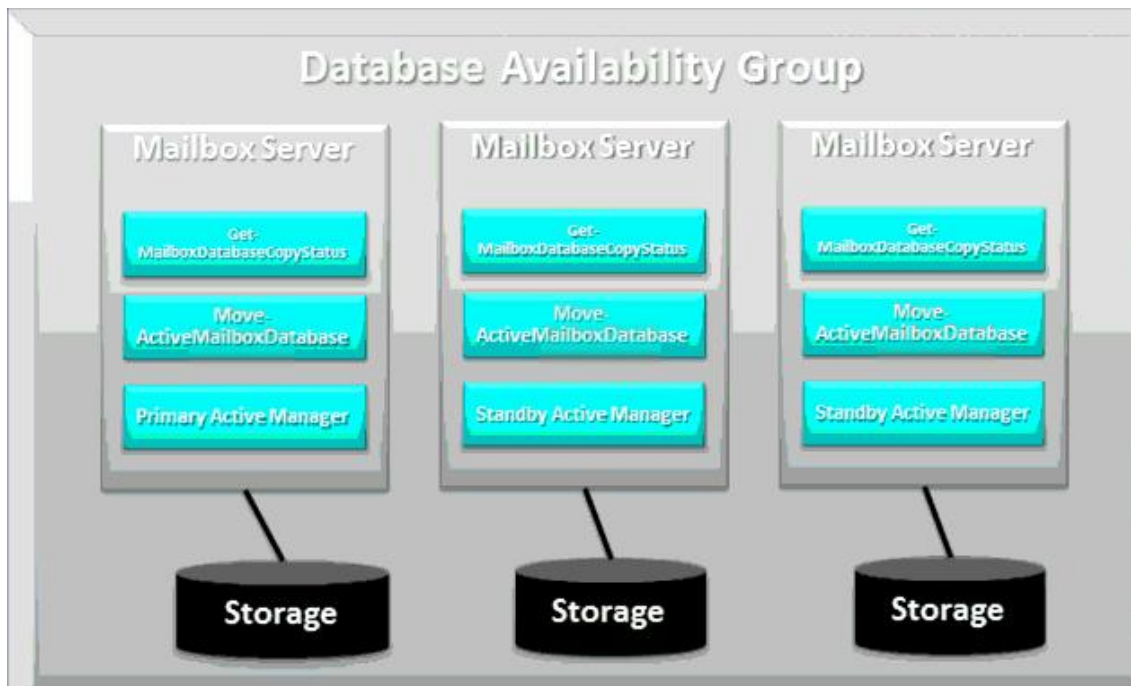
exchange 2007需要先配置cluster。



exchange server 2010的架构。在配置DAG的过程中，会自动配置故障转移群集。群集可以看成是DAG需要的一个组件。



DAG实现的是数据库级别的故障转移。



exchange 2010其他角色的高可用技术总结

HUB服务器可以自动实现负载平衡。

UM在企业环境中部署多台，可以通过AD实现高可用。

边缘服务器可以通过边缘克隆来实现高可用。

CAS服务器的高可用可以通过NLB或者硬件负载平衡。

exchange 2010的高可用性目标。

- ◆ 降低复杂度
- ◆ 降低成本
- ◆ 消除单点故障点
- ◆ 减少恢复的时间
- ◆ 支持更大的邮箱
- ◆ 支持大规模部署

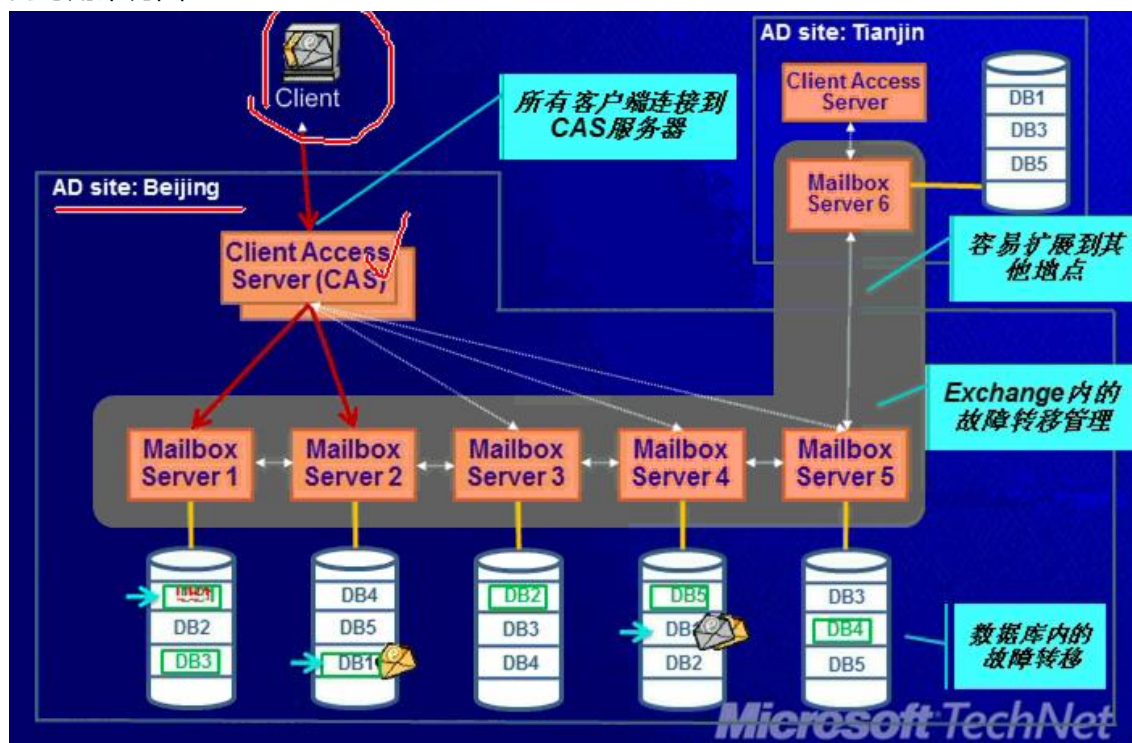
使高可用性成为**Exchange**部署的主流！

exchange 2010的增强



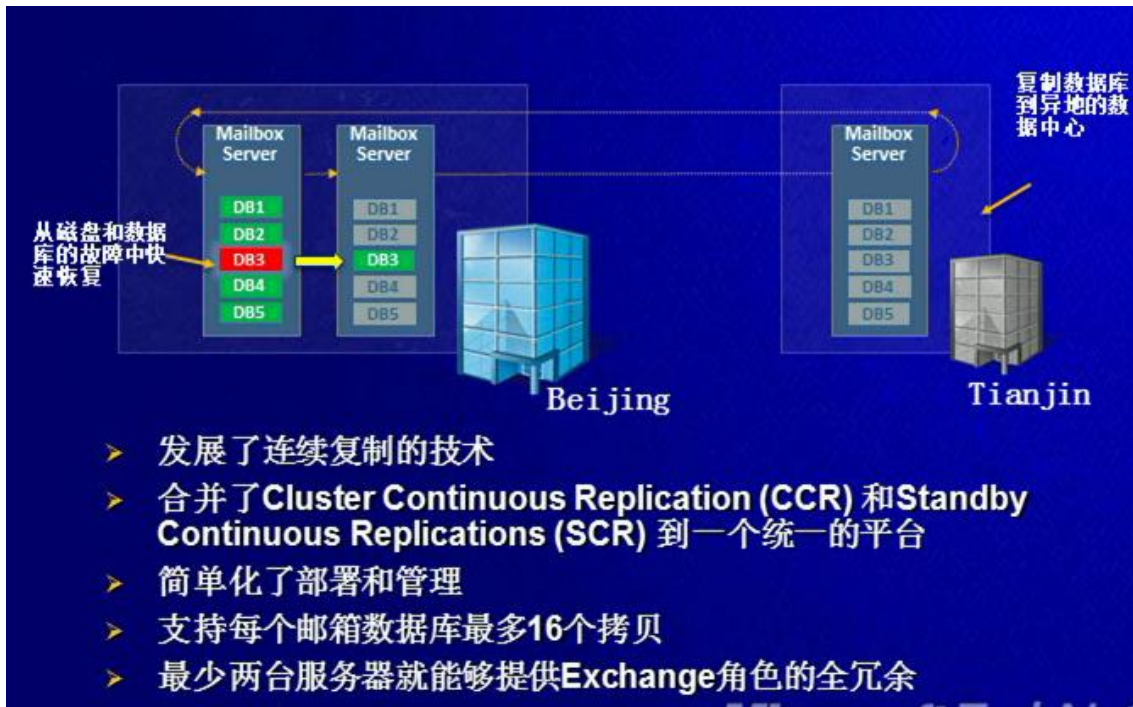
支持无RAID架构。

高可用架构图。

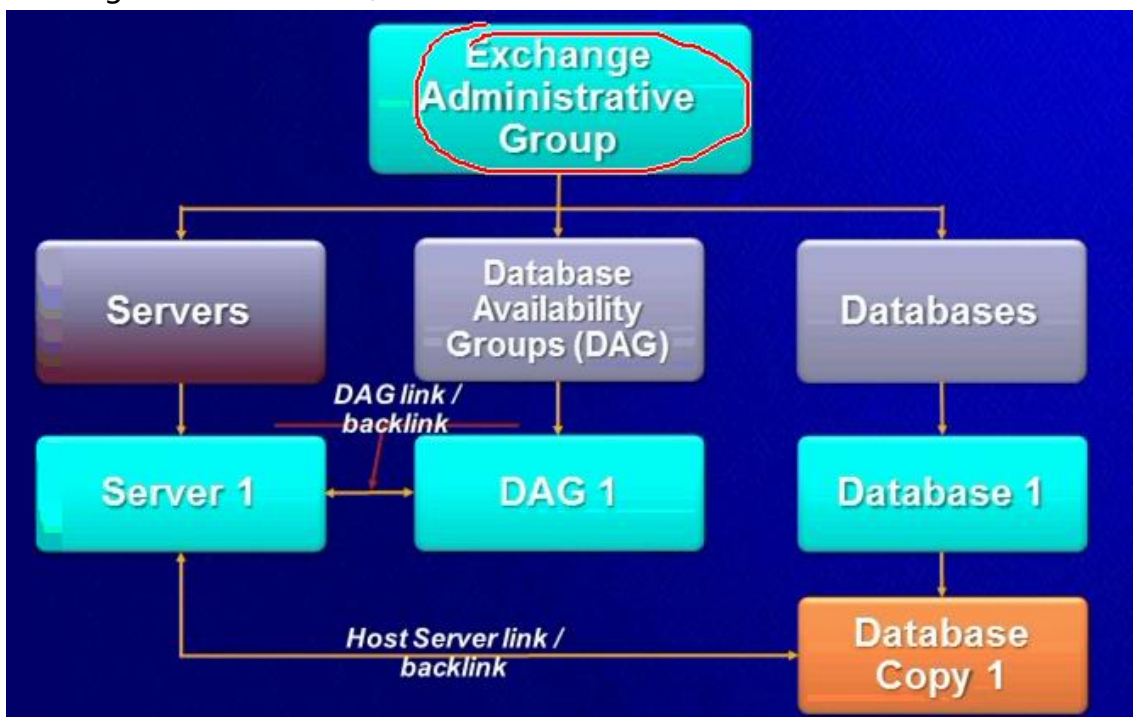


当某一个DB挂了，会自动切换到好的服务器上，由AM来做。

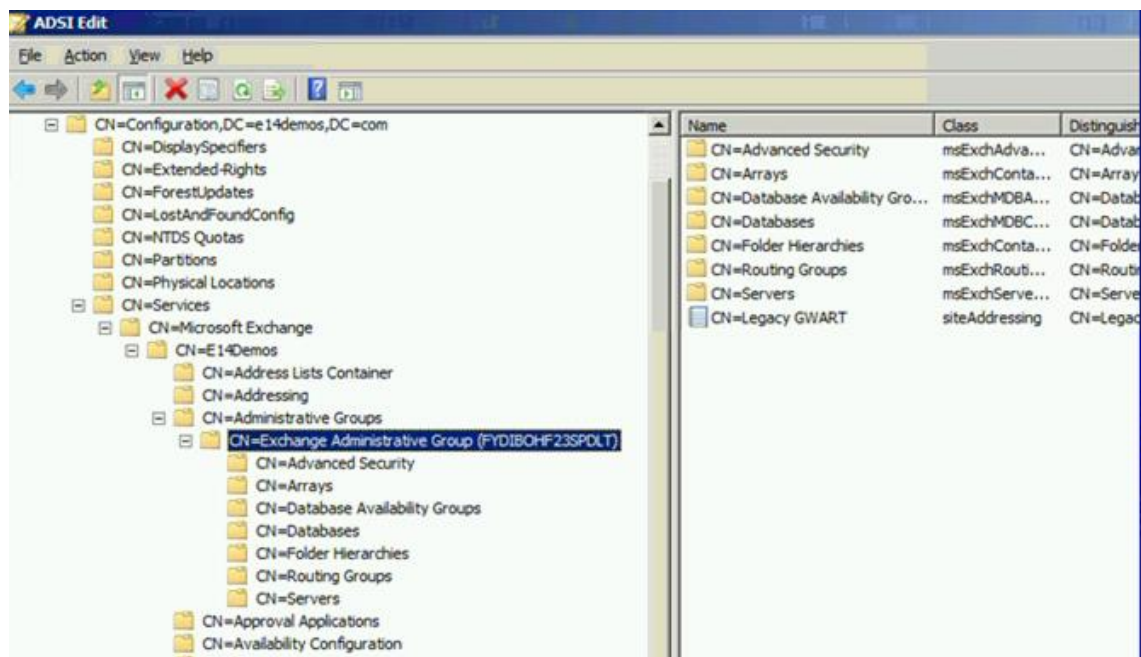
是高可用和灾难恢复的统一平台。



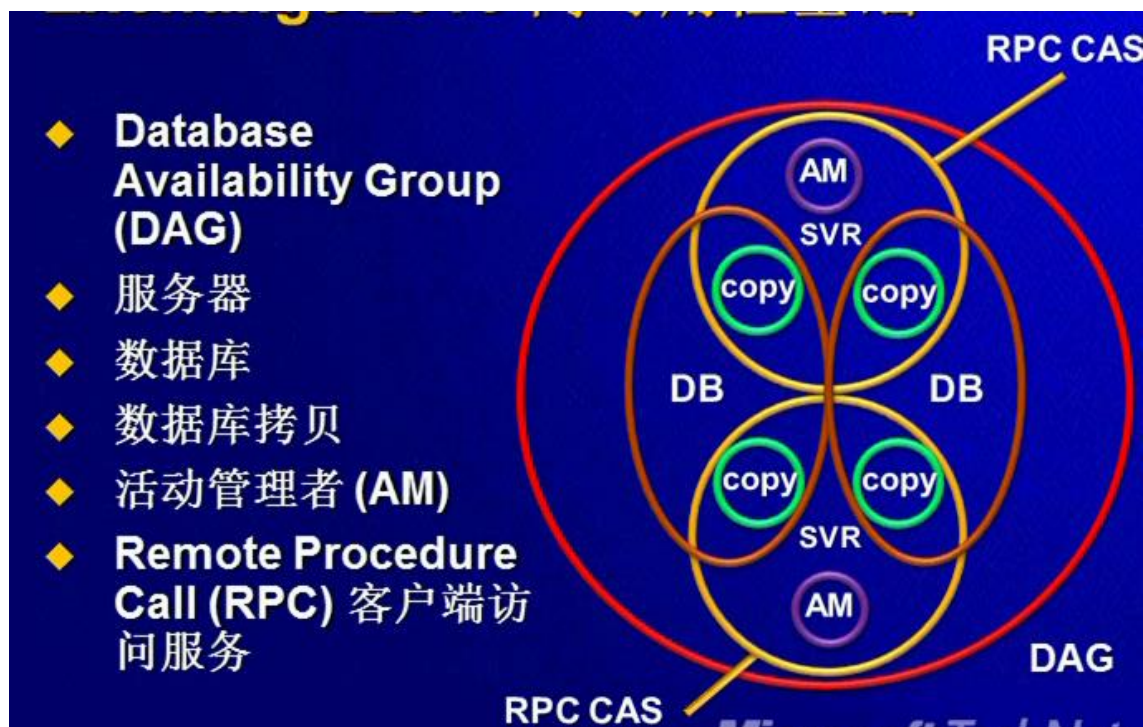
exchange 2010 AD域服务架构



使用ADSIEDIT查看exchange的架构。



基础概念。



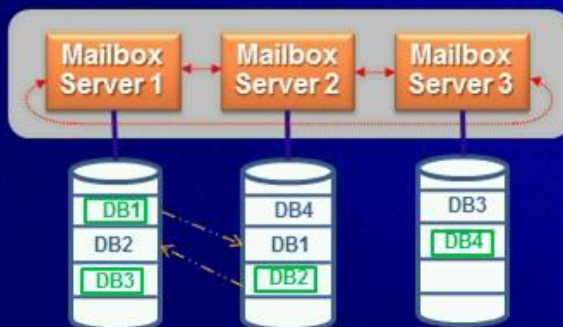
基础概念：DAG

- ◆ 一个包含了一组最多在16台服务器之间复制的数据库的组
- ◆ 替代了Windows Failover Cluster
 - 在组中管理服务器的成员
 - 心跳服务器，仲裁，群集数据库
- ◆ 定义了数据库复制的边界
- ◆ 定义了故障转移/切换的边界
- ◆ 定义了DAG Active Manager的边界



基础概念：服务器

- ◆ DAG的一个成员
- ◆ 承载多个邮箱数据库的主动和被动拷贝
- ◆ 在主动邮箱拷贝上运行 Information Store, CI, Assistants等服务
- ◆ 在被动邮箱数据库拷贝上运行复制服务



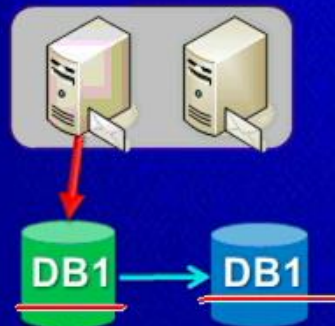
- ◆ 一个故障转移的单元
- ◆ 每个数据库有一个活动拷贝，活动拷贝可以被加载或者卸载
- ◆ 最大的被动节点数目 = DAG 中的服务器数目 - 1

- 数据库切换大约需要**30 秒**
- 服务器故障转移/切换意味着移动所有的活动数据库到一个或多个其他服务器
- 数据库的名字在整个森林是唯一的
- 在数据库级别定义的相关属性
 - **GUID**: 数据库的唯一ID
 - **EdbFilePath**: 数据库拷贝存放的路径
 - **Servers**: 负载拷贝的服务器

主动、被动

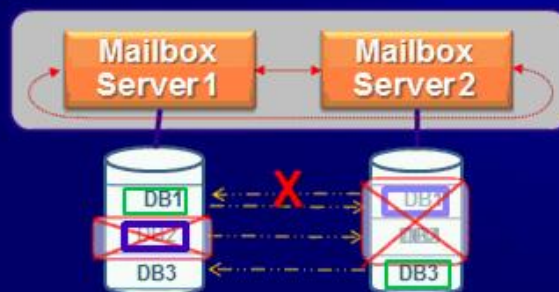
源、目标

- ◆ 可用性角度
 - 主动: 提供电子邮件服务给用户
 - 被动: 如果主动节点失败可提供服务给用户
- ◆ 复制角度
 - 源: 提供拷贝用的数据给其他地点
 - 目标: 接受从源来的数据



邮箱数据库的拷贝

- 复制的范围
- 在任何时间，一个拷贝要么是源要么是目标，但不能同时
- 在任何时间，一个拷贝要么是主动的要么是被动的
- 任何时刻一个**DAG**中的每个数据库只有一个拷贝是主动的
- 每个服务器不能有一个数据库超过1个的拷贝



查看拷贝复制的过程和属性

定义每个数据库拷贝适用的属性

- Copy status: 健康, 初始化, 失败, 加载, 卸载, 断开, 挂起, 失败并且挂起, 重新同步, ActiveCopy
- CopyQueueLength ActivationSuspended
- ReplayQueueLength

The screenshot shows a Windows command prompt window with the command `Get-MailboxDatabaseCopyStatus mdb1` executed. The output is a table with four columns: Name, Status, CopyQueueLength, and ReplayQueueLength. The Status column is circled in red. Below the command prompt is a screenshot of the Exchange Management Console (EMC) showing the 'Database Copies' tab for the 'mdb1' mailbox database. The table in the EMC also has a 'Copy Status' column circled in red.

Name	Status	CopyQueueLength	ReplayQueueLength
-----	-----	-----	-----
mdb1\1659R1-C12	FailedAndSuspended	46	1
mdb1\EXCH-B-956	Resynchronizing	0	0
mdb1\EDGE881	Mounted	0	0

Data...	Mailbox Server	Copy Status	Copy Queue Length	Replay Queue Length
...
...	...	Failed and Suspended	46	1
...	...	Failed	46	7
...	...	Mounted	0	0

关于exchange的active manager

- ◆ Exchange内的资源管理器（高可用性的大脑）
 - 在DAG中的每一台服务器上运行
 - 负责管理哪个拷贝是主动的，哪个是被动的
 - 定义数据库被激活和加载时所需的源信息
 - 将信息提供给其他Exchange组件(例如RPC Client Access和Hub Transport)
 - 信息存放在群集数据库中

连续复制的过程

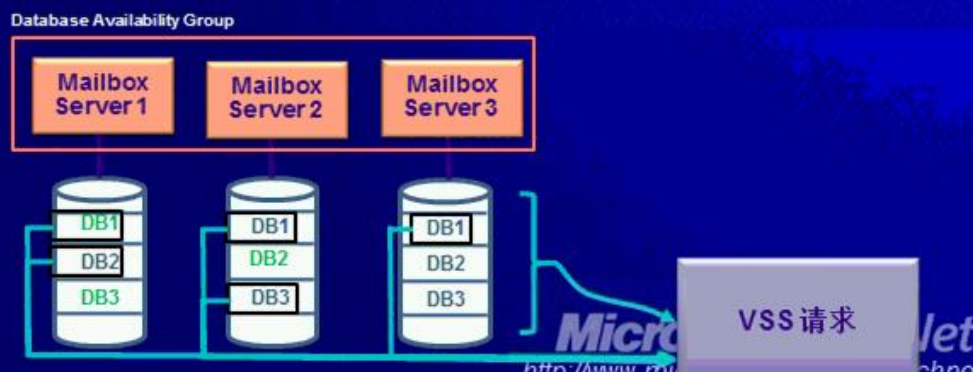
- ◆ 基本步骤：
 - 目标数据库拷贝的复制初始化（Seeding）
 - 从源到目标的日志拷贝
 - 目标上的日志侦测
 - 数据库拷贝上的日志重播

日志传输的过程

- ◆ **Exchange Server 2010中的日志传送使用TCP sockets**
 - 支持加密和压缩
 - 管理员可以设置使用的TCP端口
- ◆ 由目标服务器上的复制服务通知活动节点想要的下一个日志文件
 - 基于最后一个日志文件的信息
- ◆ 源服务器上的复制服务发送对应的日志文件
- ◆ 被拷贝的日志文件放在目标的检查文件夹中

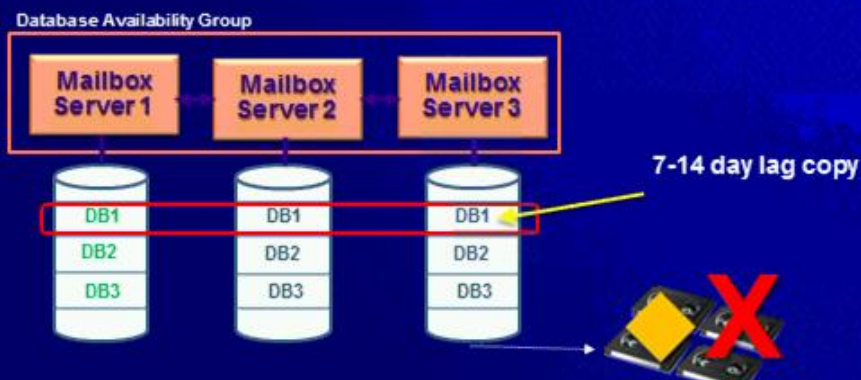
关于exchange的备份

- ◆ 流备份API已经被取消, 必须使用 **Volume Shadow Copy Service (VSS)** 备份
 - 从任何拷贝的数据库/日志进行备份
 - 总是选择被动 (或者主动) 拷贝
 - 备份整个服务器
 - 给每个数据库指定备份服务器
- ◆ 可从任何备份的场景进行恢复



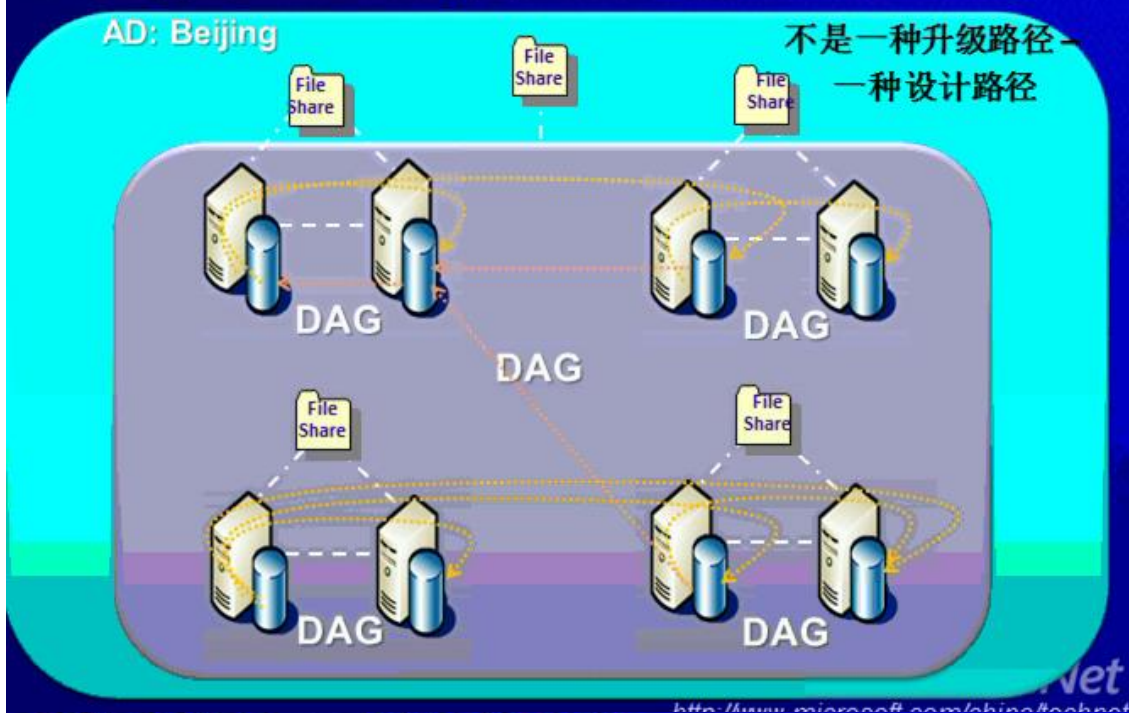
多数据库的拷贝可以实现无备份的配置

- 站点/服务器/磁盘 故障 → **Exchange Server 2010 HA**
- 归档/合规 → 邮件归档
- 恢复已删除的对象 → 扩展的/保护的 垃圾箱回收

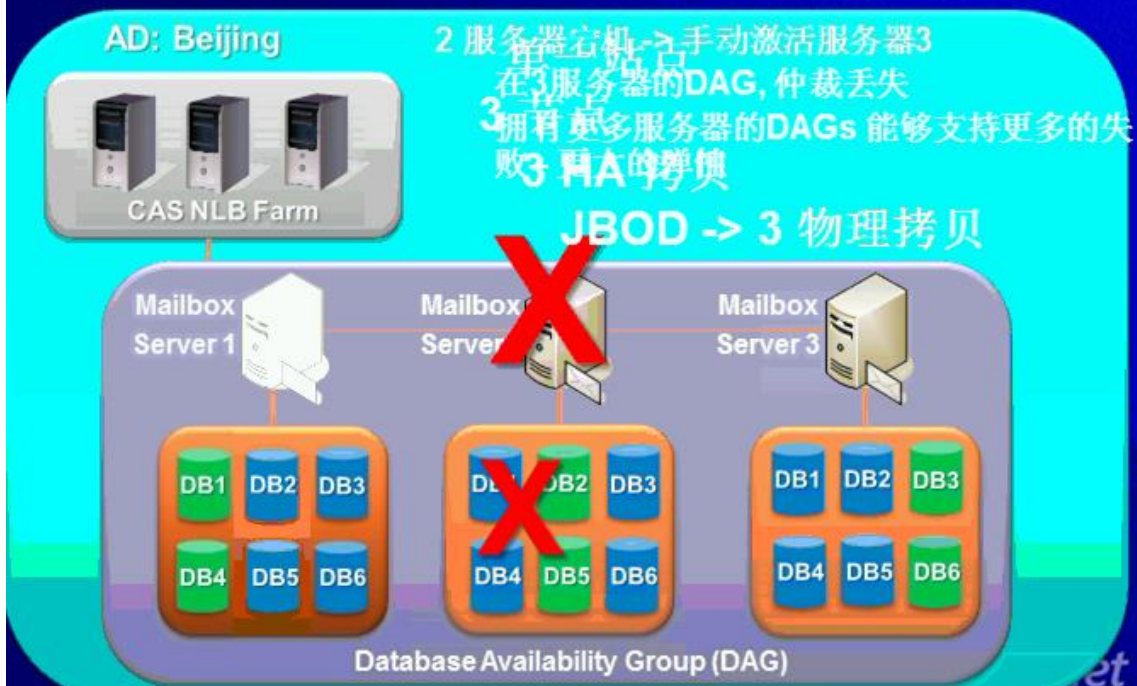


从exchange CCR到exchange DAG

CCR 设计 -> DAG 设计

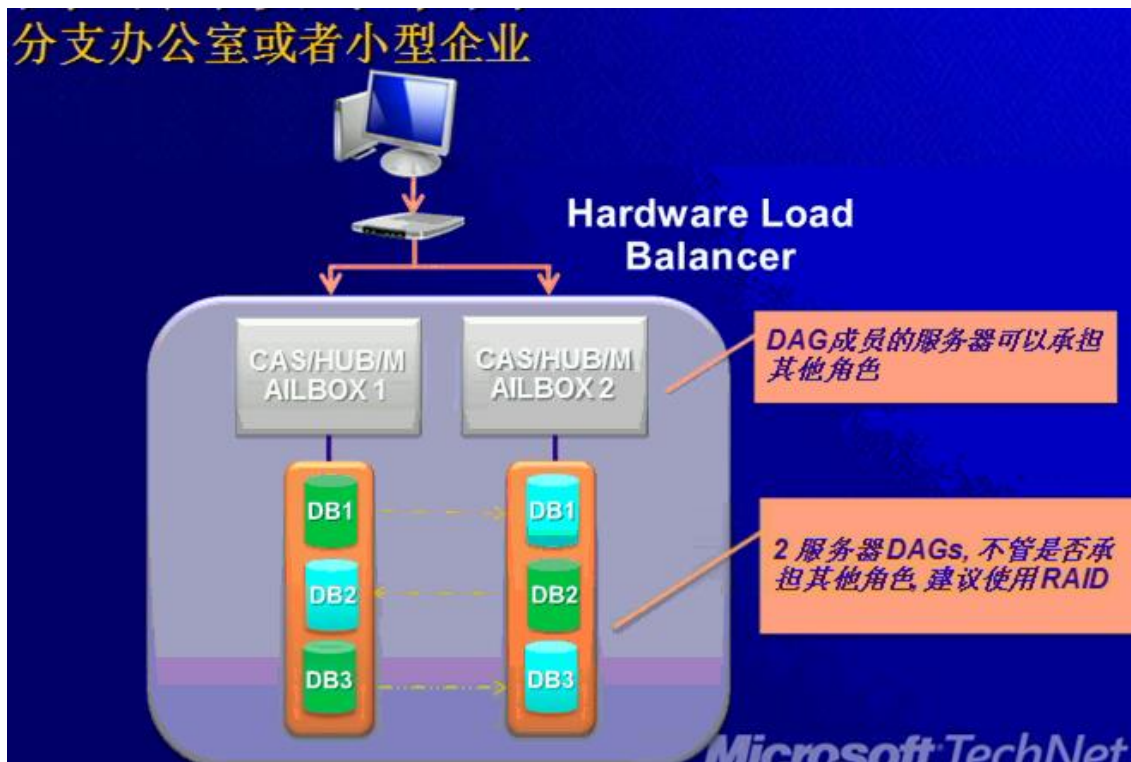


双重回复能力——维护 + DB 失败



ALL in one部署只能使用硬件的NLB，因为微软的NLB和cluster不能共存。

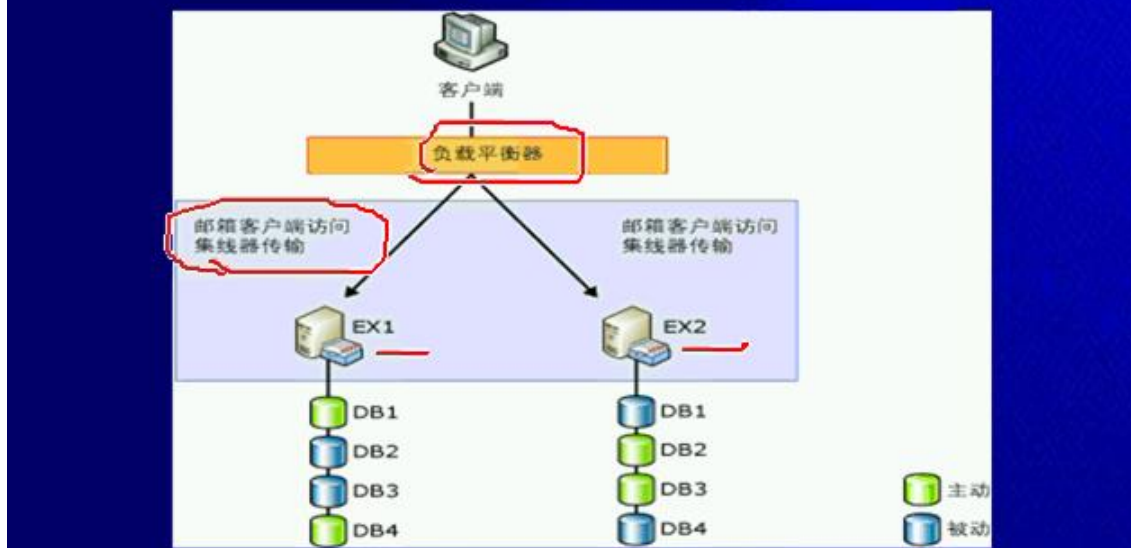
分支办公室或者小型企业



Exchange Server 2010精讲系列课程(8)_ Exchange Server 2010的高可用性-DAG(下)

CAS需要通过硬件负载平衡设备。因为NLB和cluster不能共存。

◆ 两成员 DAG，适用于小型办公室和分支机构部署。



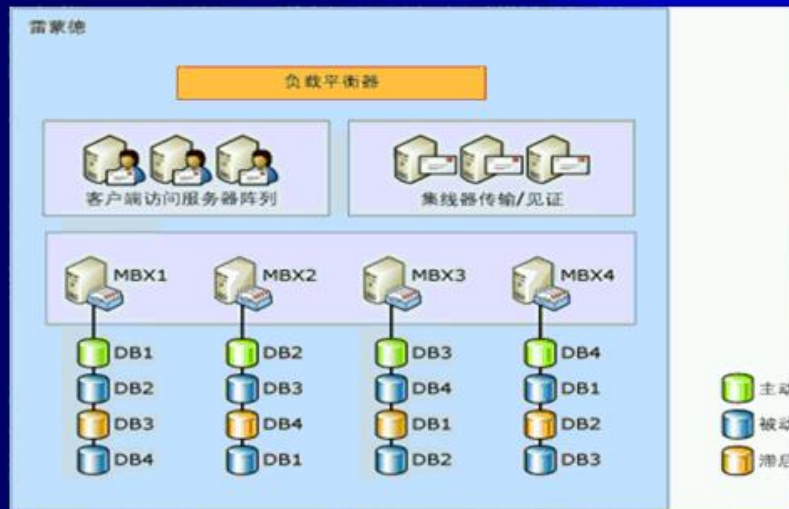
一个主动副本。

两个被动副本。

一个滞后副本。

四节点最多可以承担两个故障点。下图有见证服务器，如果DAG成员是偶数的话，需要部署见证。

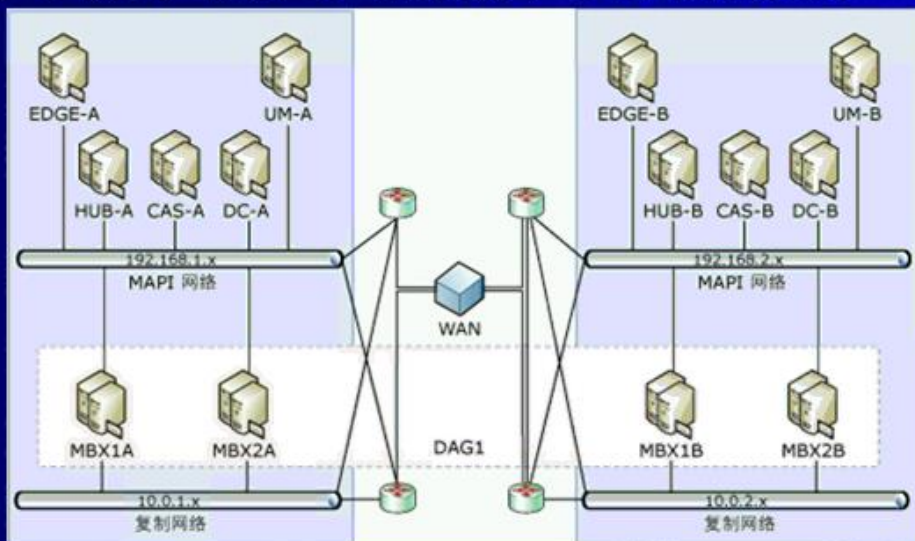
- ◆ 四成员 **DAG**，通过将所有成员定位在同一数据中心，提供单个数据中心的高可用性。



四成员DAG，数据中心的灾备。

见证服务器放在总部，分支机构可以放置备用的见证服务器。

- ◆ 四成员 **DAG**，通过将两个成员定位在主数据中心并将两个成员定位在辅助数据中心，提供单个数据中心的高可用性和该数据中心的站点恢复



DAG的设计前提。

◆ 常规要求

- 需要有DNS
- DAG 中的每个邮箱服务器必须是相同域中的成员服务器。
- 不支持将同时作为目录服务器的 Exchange 2010 邮箱服务器添加到 DAG。
- 分配给 DAG 的名称必须是不超过 15 个字符的有效、可用和唯一的计算机名称。

◆ 软件要求

- Exchange 2010标准版和企业版或混合服务器。
- DAG成员的操作系统必须是Windows Server 2008或 2008 R2，不能是混合环境。
- Windows Server 2008 或 2008 R2必须是企业版。

DAG不能跨域。

并置AD的邮箱角色不能做DAG。

◆ 网络要求

- MAPI网络：其它服务器使用该网络与DAG成员通信。
- 复制网络：专用于日志传送和种子设定。
- 支持单一网络配置，但不推荐。
- DAG 网络支持 IPv4 和 IPv6。仅当同时使用 IPv4 时才支持 IPv6；不支持纯 IPv6 环境。
- 阻止 MAPI 网络与复制网络之间的通信
- 使用静态路由配置跨复制网络的连接

◆ DAG 名称和 IP 地址要求

- 每个 DAG 指定一个唯一名称。
- 分配一个或多个静态 IP 地址，或配置为使用 DHCP。
- DAG 的任何 IP 地址必须在 MAPI 网络上。
- 在多个子网上具有 MAPI 网络的DAG设置 多个IP地址。

不建议在复制网络上配置网关，所以可以使用静态路由的方式来完成复制网络之间的通信。

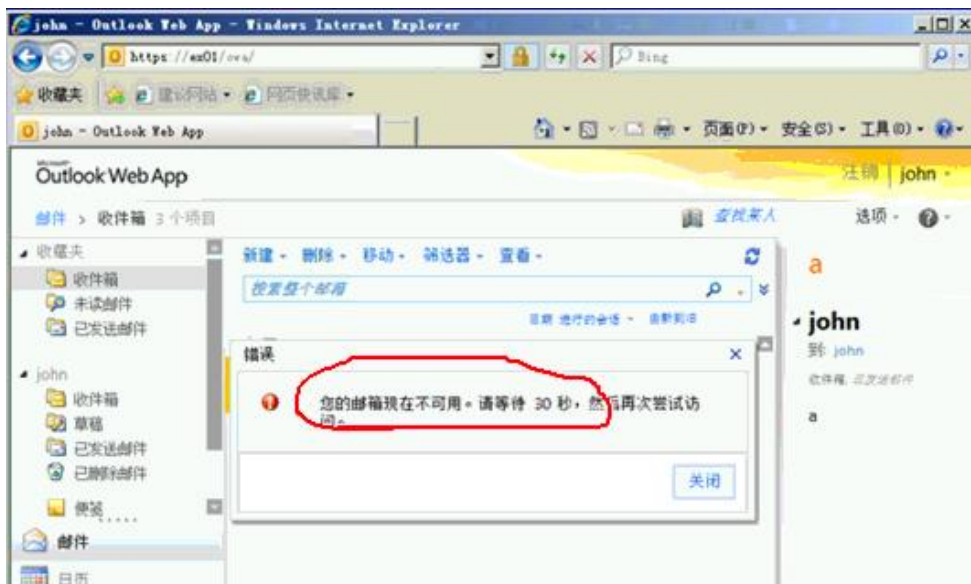
◆ 见证服务器要求

- 当 DAG 的成员数为偶数时，使用见证服务器可实现和维护仲裁。DAG 的成员数为奇数时，则不使用见证服务器。
- 见证服务器不能是 DAG 的成员。一般建议HUB充当见证服务器。
- 见证服务器必须与 DAG 位于同一个 Active Directory 林中。
- 见证服务器必须运行 Windows Server 2008 R2、Windows Server 2008、Windows Server 2003 R2 或 Windows Server 2003。
- 一台服务器可以充当多个 DAG 的见证；但是，每个 DAG 都需要拥有自己的见证目录。

DAG的部署过程。

- ◆ 安装第二台或更多的MBX
- ◆ 创建一个 DAG
 - New-DatabaseAvailabilityGroup
- ◆ 向 DAG 添加两个或多个邮箱服务器
 - Add-DatabaseAvailabilityGroupServer
- ◆ 根据需要配置 DAG 属性
 - Set-DatabaseAvailabilityGroup
- ◆ 在 DAG 中跨邮箱服务器添加邮箱数据库副本
 - Add-MailboxDatabaseCopy

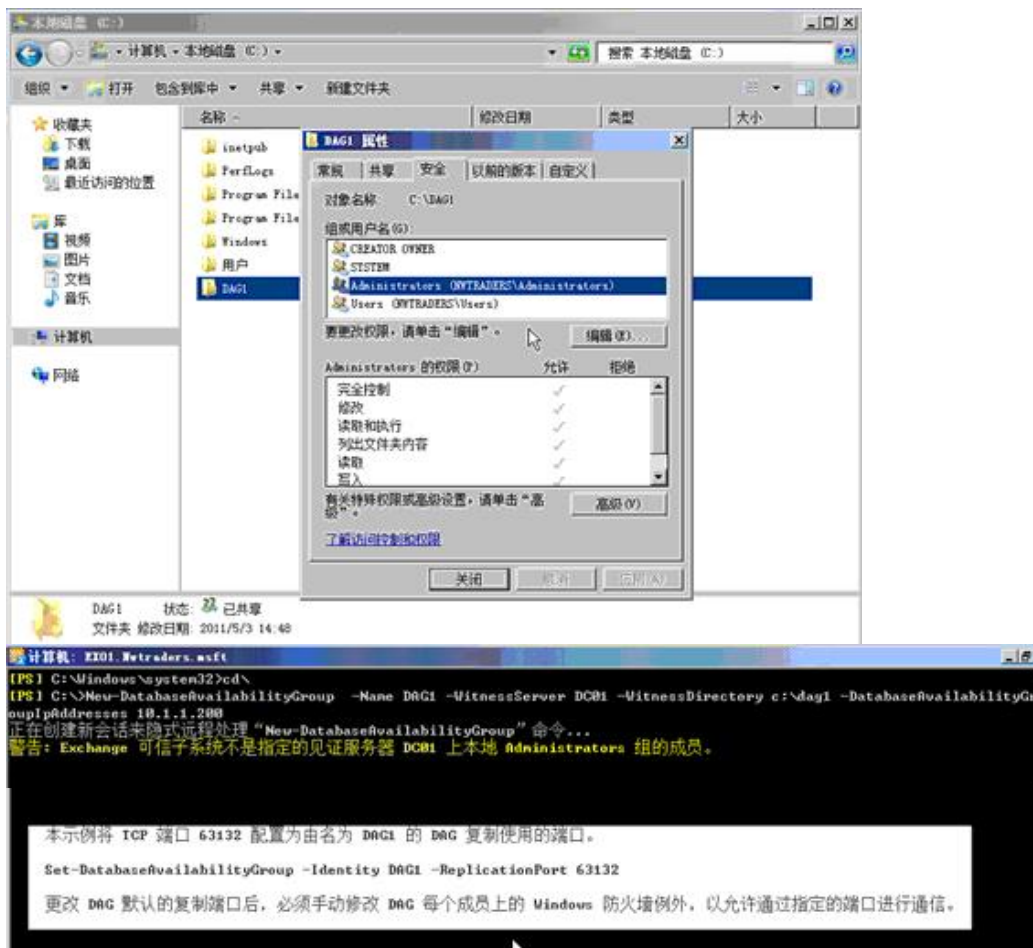
DAG出现故障切换时，OWA会提示出现故障，切换需要30秒。



调整DAG两个网络的优先级，原则上让MAPI网络优先。

建立见证服务器共享。

如果见证服务器不是exchange的成员，则还需要把一个角色加入到见证服务器的本地管理员组 exchange trusted subsystem。



根据首选参数进行数据库的转移。

通过AM。

当主数据库所在的服务器恢复运行后，需要手动将数据库回切。

5成员DAG场景故障转移过程



跨两个站点扩展的DAG部署

- ◆ 其中MBX1A、MBX2A位于中心站点，而MBX1B、MBX2B位于分支站点。
- ◆ 每个邮箱服务器承载一个活动邮箱数据库副本、两个非延迟被动数据库副本和一个延迟被动数据库副本。其他站点中的邮箱服务器上承载每个活动邮箱数据库的延迟副本。



可以认为控制复制的来源，复制是实时复制还是延迟复制。

跨两个站点扩展的DAG部署

- ◆ `Add-MailboxDatabaseCopy -Identity DB1 -MailboxServer MBX2A`
- ◆ `Add-MailboxDatabaseCopy -Identity DB1 -MailboxServer MBX2B`
- ◆ `Add-MailboxDatabaseCopy -Identity DB1 -MailboxServer MBX1B -ReplayLagTime 3.00:00:00 -SeedingPostponed`
- ◆ `Suspend-MailboxDatabaseCopy -Identity DB1\MBX1B -SuspendComment "Seed from MBX2B" -Confirm:$False`
- ◆ `Update-MailboxDatabaseCopy -Identity DB1\MBX1B -SourceServer MBX2B`
- ◆ `Suspend-MailboxDatabaseCopy -Identity DB1\MBX1B -ActivationOnly`



- ◆ 主动监视
 - `Get-MailboxDatabaseCopyStatus`
 - `Test-ReplicationHealth`

```
[PS] C:\PST001>Test-ReplicationHealth
正在创建新会话来隐式远程处理 "Test-ReplicationHealth" 命令...
服务器 CAS01 没有安装邮箱服务器角色。只能从邮箱服务器运行 Test-ReplicationHealth cmdlet，或者在将邮箱服务器指定为目标时，
从非邮箱服务器运行此命令。
+ CategoryInfo          : NotInstalled: (:) [Test-ReplicationHealth], NoMailboxRoleInstalledException
+ FullyQualifiedErrorId : D3D3397A,Microsoft.Exchange.Monitoring.TestReplicationHealth
```

```
[PS] C:\Windows\system32>Test-ReplicationHealth
```

Server	Check	Result	Error
DAG01	ClusterService	已通过	
DAG01	ReplayService	已通过	
DAG01	ActiveManager	已通过	
DAG01	TasksRpcListener	已通过	
DAG01	TcpListener	已通过	
DAG01	ServerLocatorService	已通过	
DAG01	DagMembersUp	已通过	
DAG01	ClusterNetwork	已通过	
DAG01	QuorumGroup	已通过	
DAG01	FileShareQuorum	已通过	

=====

Exchange Server 2010精讲系列课程(9): Exchange Server 2010信息保护和控制

信息泄露的威胁。



法律，法规和财务

- 每年数字的泄漏成本是 \$Billions
- 这个数字还在增加，并且越来越复杂
- 不遵守规章或者数据丢失都将导致法律费用，财物损失或者更多的问题



损坏形象和可信度

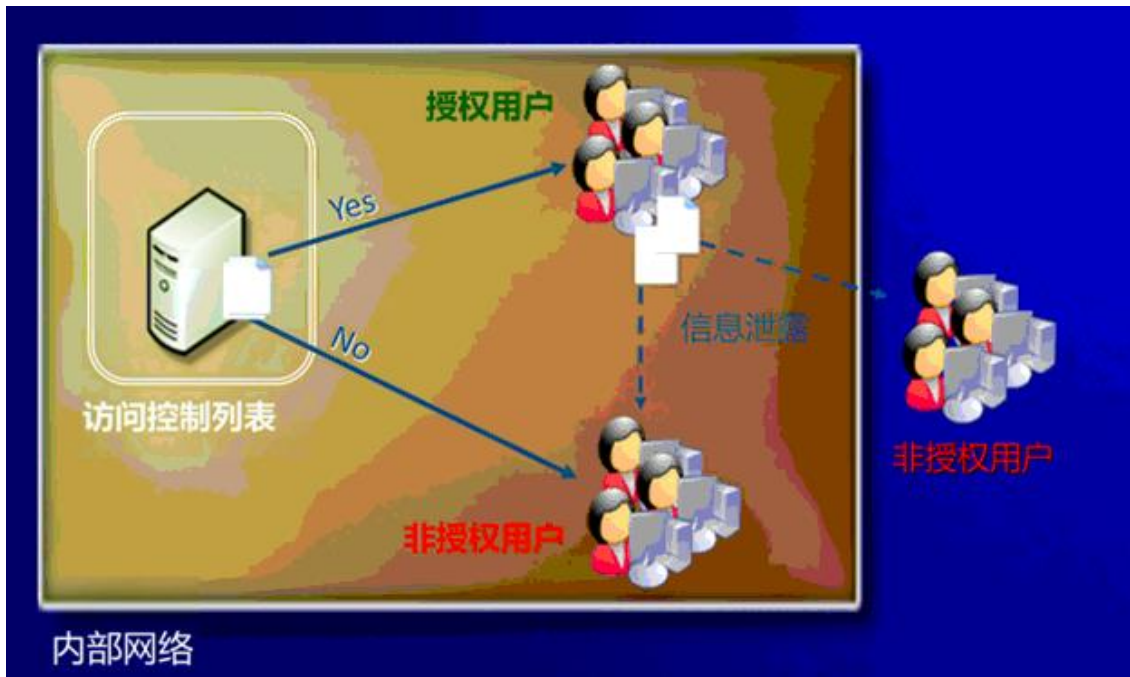
- 损坏公众形象和客户的信任度
- 对于公司来说会有可能造成金融方面的损失



失去竞争优势

- 战略计划的披露，并购信息的可能导致收入和市场资本总额的损失
- 损失研究，分析数据，以及其他智力资本

传统的NTFS访问控制不能保证文件的持续保护，如图。



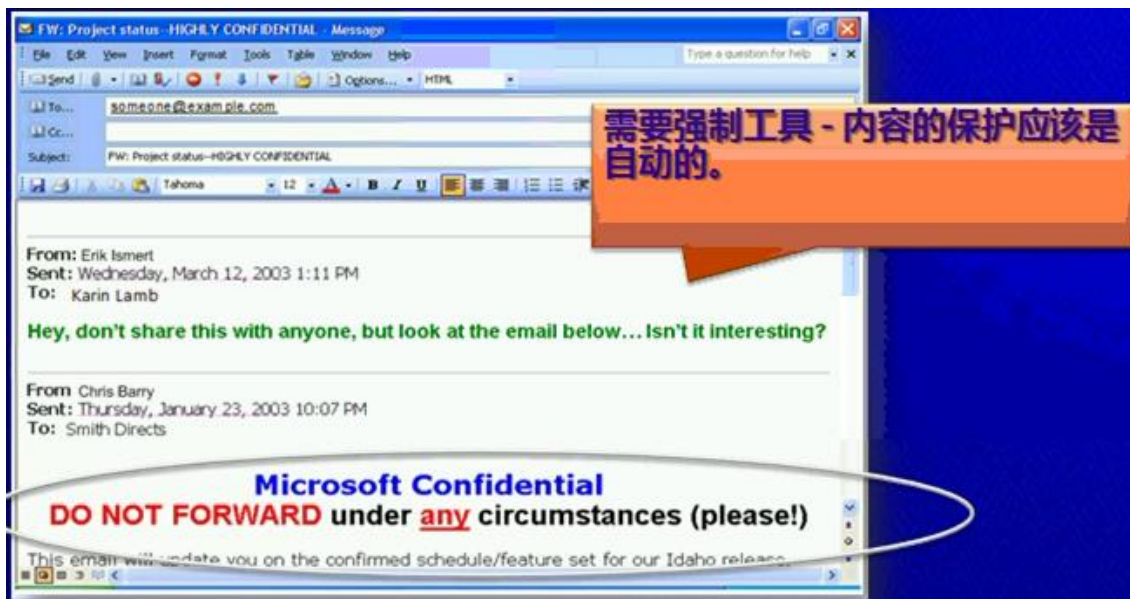
EFS加密文件系统只能阻止未授权的访问，但是依然不能阻止信息的泄露。

如何保证邮件传输过程的安全？

- 1) 传输层安全性TLS。
- 2) 借助于电子邮件的加密和签名技术。证书。

邮件的持续保护要求：我们不但要着眼于企业内部，也要着眼企业外部。

邮件的私密性声明：



信息泄露大部分是无意识的行为。

无法依赖用户来保护数据

80%的数据泄漏在偶然情况下发生 — 用户通常没有意识到数据安全策略，无意中造成了数据泄漏 -
Forrester, 2008

AD RMS技术。

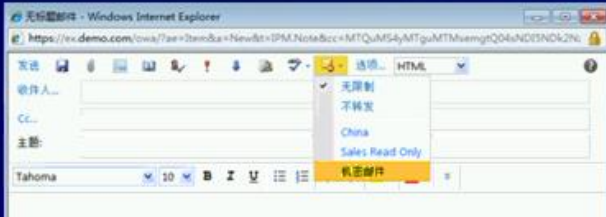
基于用户进行权限的设定。

- ◆ **RMS (Rights Management Services)**
- ◆ **Windows 平台的信息保护技术**
- ◆ **敏感信息的好护卫**
 - 防止未授权的查看，编辑，拷贝，打印或者转发
 - 限制文件访问只给授权用户
 - 审核跟踪被保护文件的使用
- ◆ **固化的保护**
 - 保护敏感信息，无论它到哪里
 - 增强组织策略的技术
 - 作者可以定义收件人如何使用信息
- ◆ **IRM**
 - IRM 使用了 Active Directory 权限管理服务 (AD RMS)
 - 信息权限管理 (IRM) 功能对邮件和附件应用持久保护

IRM是基于AD RMS的。

对邮件进行IRM保护

- ◆ 由 Outlook 用户手动进行
- ◆ 由 Outlook Web App 用户手动进行
- ◆ 在集线器传输服务器上自动进行
- ◆ 在 Outlook 2010 中自动进行



集线器传输的规则使用。应用RMS模板，对邮件进行加密。

自动保护-传输保护规则

Exchange Server 2010
提供了控制和保护电
子邮件信息的唯一途
径



通过outlook保护规则进行自动加密设定。

Outlook 保护规则

- ◆ 允许一个Exchange管理员定义自动在outlook里面执行的客户端规则，用来保护敏感信息

- 规则根据需要可以强制也可以选择

- ◆ 规则基于以下判断：

- 发件人的部门 (HR, R&D, etc.)

- 收件人的身份 (特定的用户或者邮件组)

- 收件人的范围 (所有人都在组织内, 外部, etc.)

- 命令举例：

```
New-OutlookProtectionRule -Name "Sales Demo" -SentTo "salesgroup@demo.com" -  
ApplyRightsProtectionTemplate "Sales Read Only"
```

- ◆ 规则从Exchange 使用Autodiscover和Exchange Web Service自动获得

解密和搜索机制。

有效的保护

搜索、扫描、过滤、日记保护电子邮件

- ◆ 传输解密

- 通过传输代理访问IRM保护的消息，如内容过滤、反病毒/反垃圾

- ◆ IRM搜索

- 在OWA和Outlook中全文搜索IRM保护的消息：可以在Exchange存储中保护邮件

- ◆ 日记报告解密

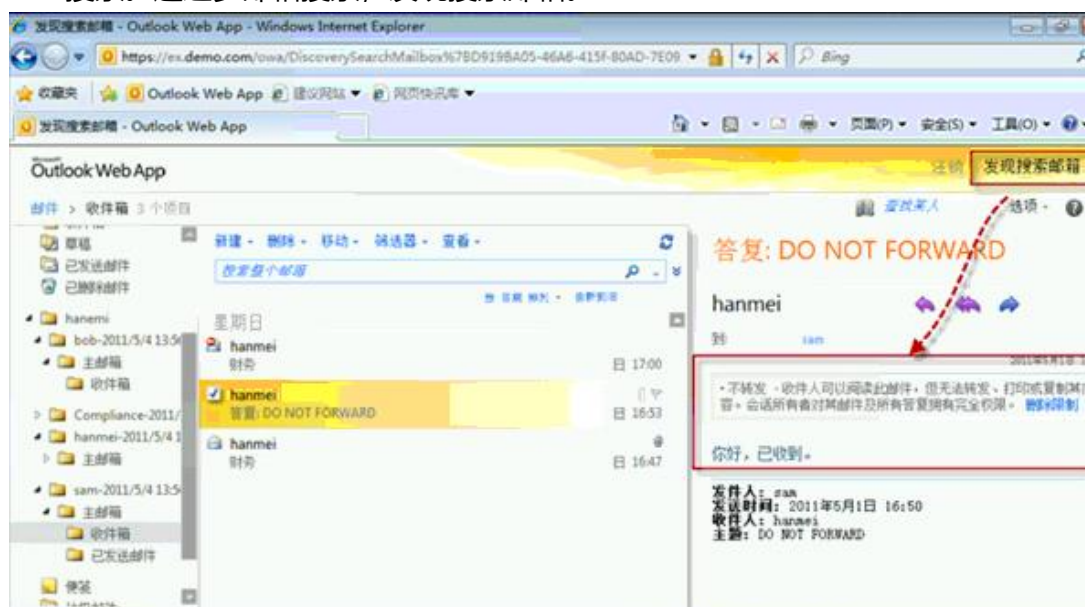
- 日记报告解密代理解密IRM保护的消息，并且存储到日记邮箱中

传输前先解密，传输后重新加密。

传输管道解密

- ◆ 使得集线器传输代理能够扫描和修改RMS保护的信息
 - 防病毒，传输规则或者第三方的代理需要
- ◆ 解密代理
 - 使用RMS超级用户权限解密邮件和附件
 - 每个森林只解密一次，在第一台集线器服务器上。这样能够提高性能
- ◆ 加密代理
 - 使用原始的发布证书重新加密邮件、附属邮件和NDR

IRM搜索。通过多邮箱搜索，发现搜索邮箱。



日志报告解密。

