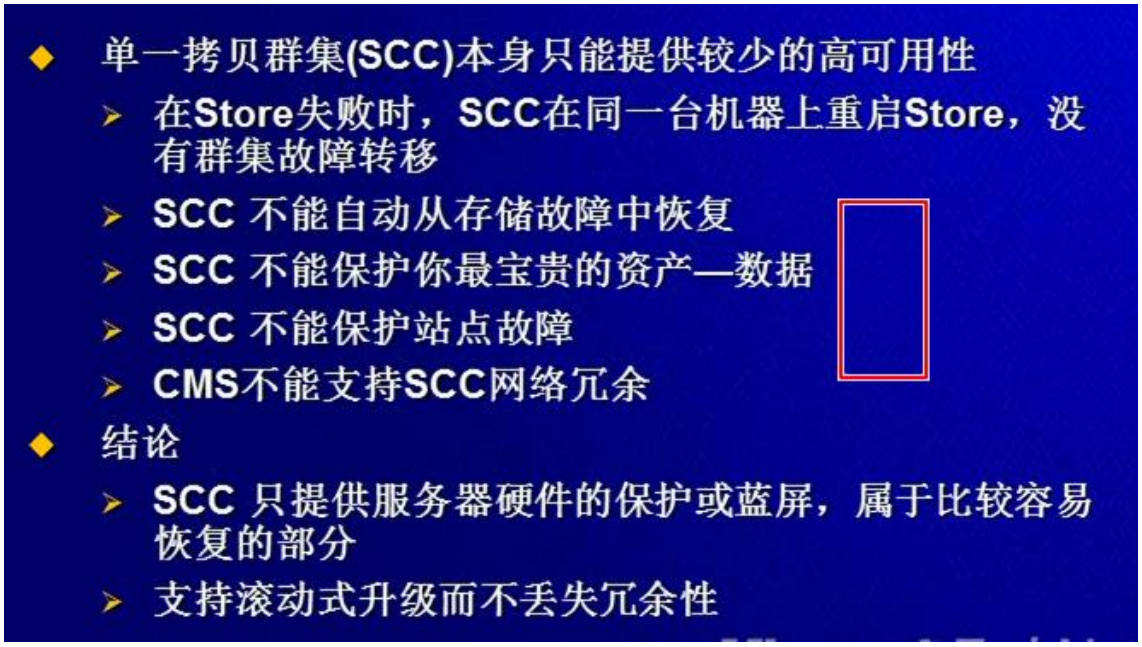
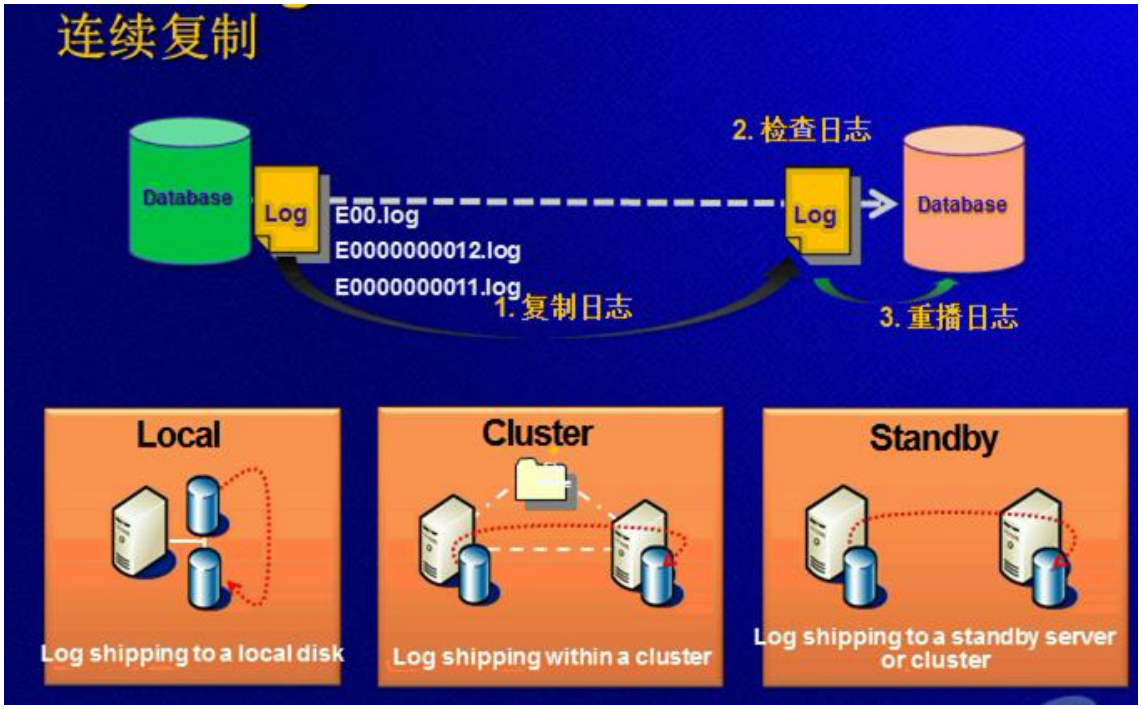
Exchange Server 2010精讲系列课程(7): Exchange Server 2010的高可用性-DAG(上)

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。



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。

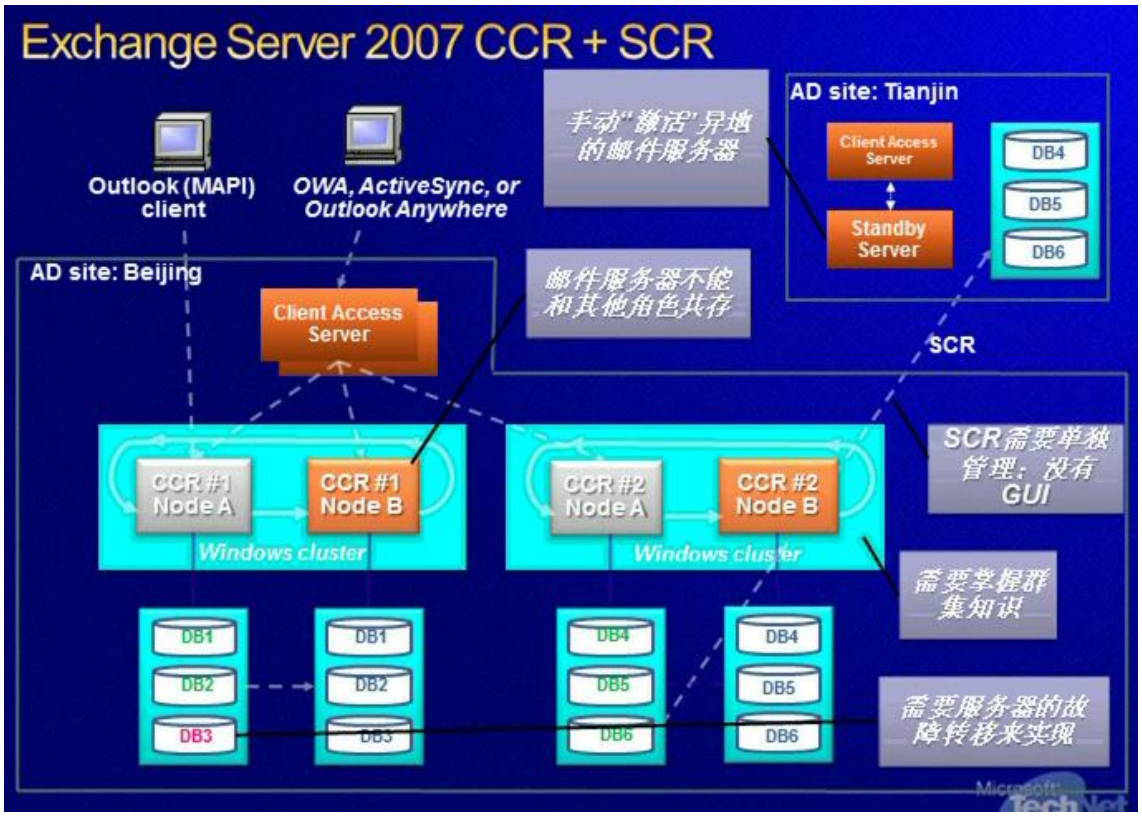
如果单个DB出问题了，那么也要进行服务器级别的切换，也就是说下图的DB1、DB2、DB3都需要切换，是服务器级别的切换。

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。

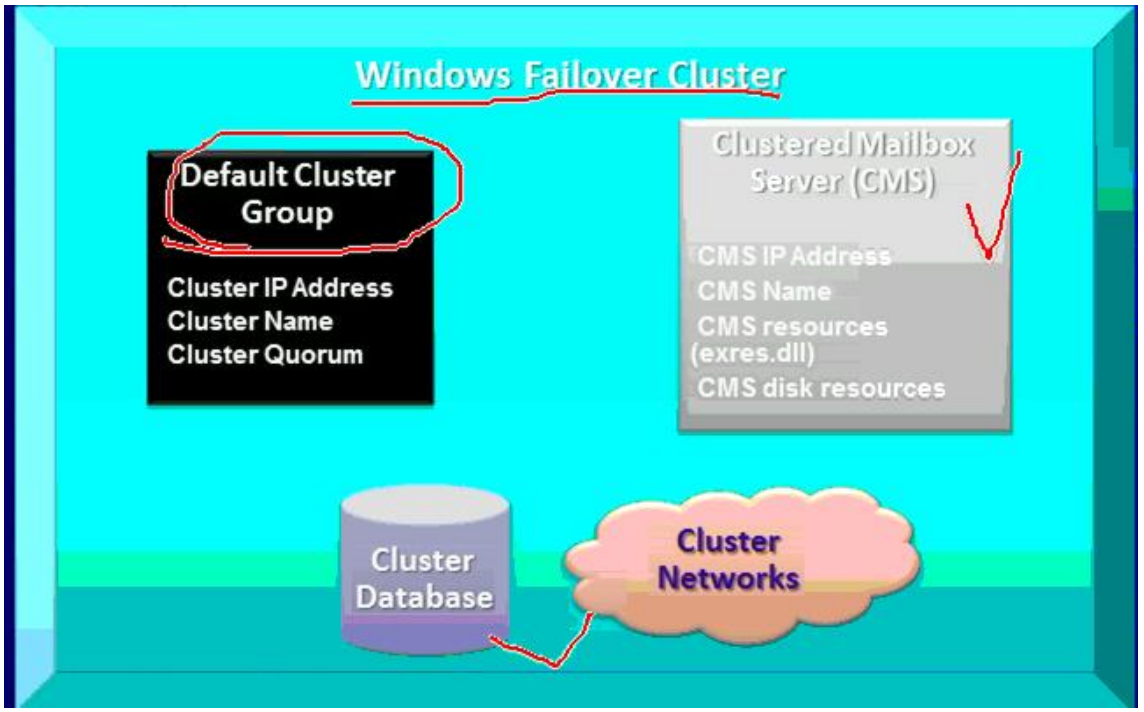
当前的CCR群集只支持2节点。只有一个节点是激活状态。另外一个节点是完全闲置的。

需要较好的存储支持，如果通过SATA磁盘实现性能相当差。

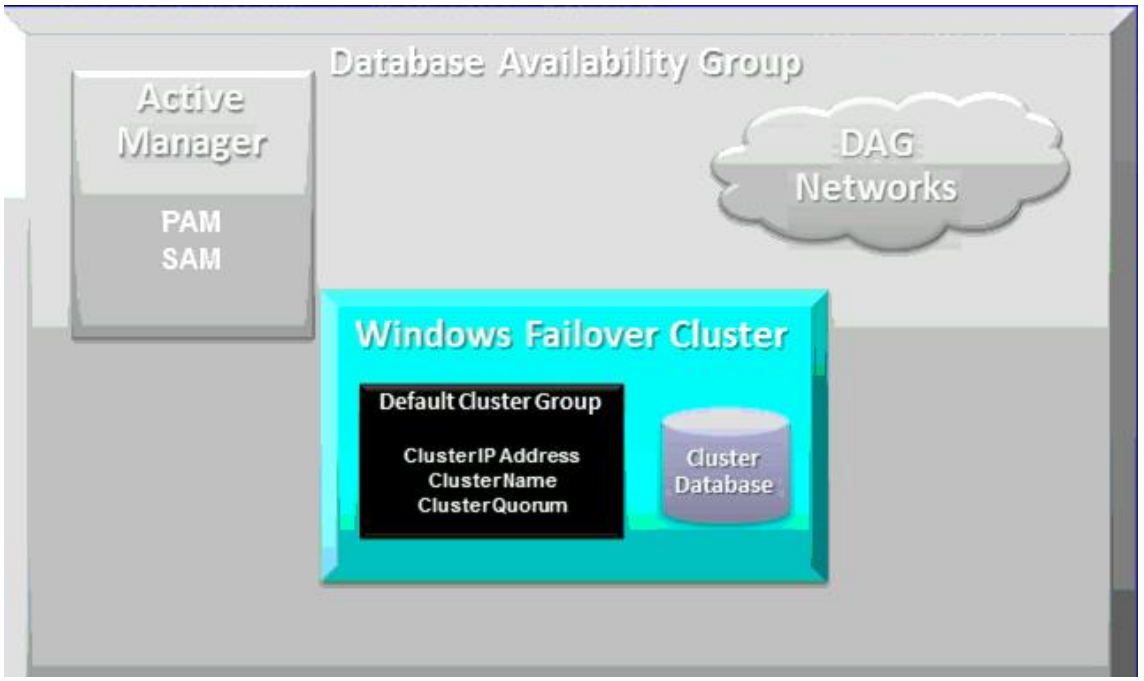


核心架构的改变。

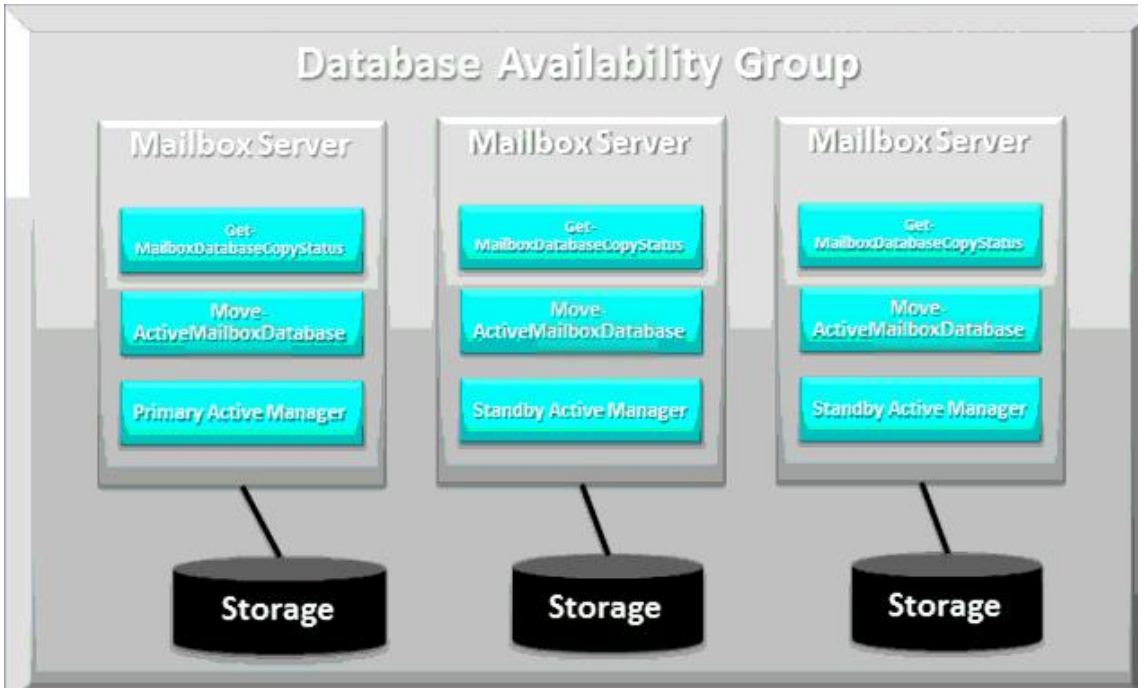
exchange 2007需要先配置cluster。



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。

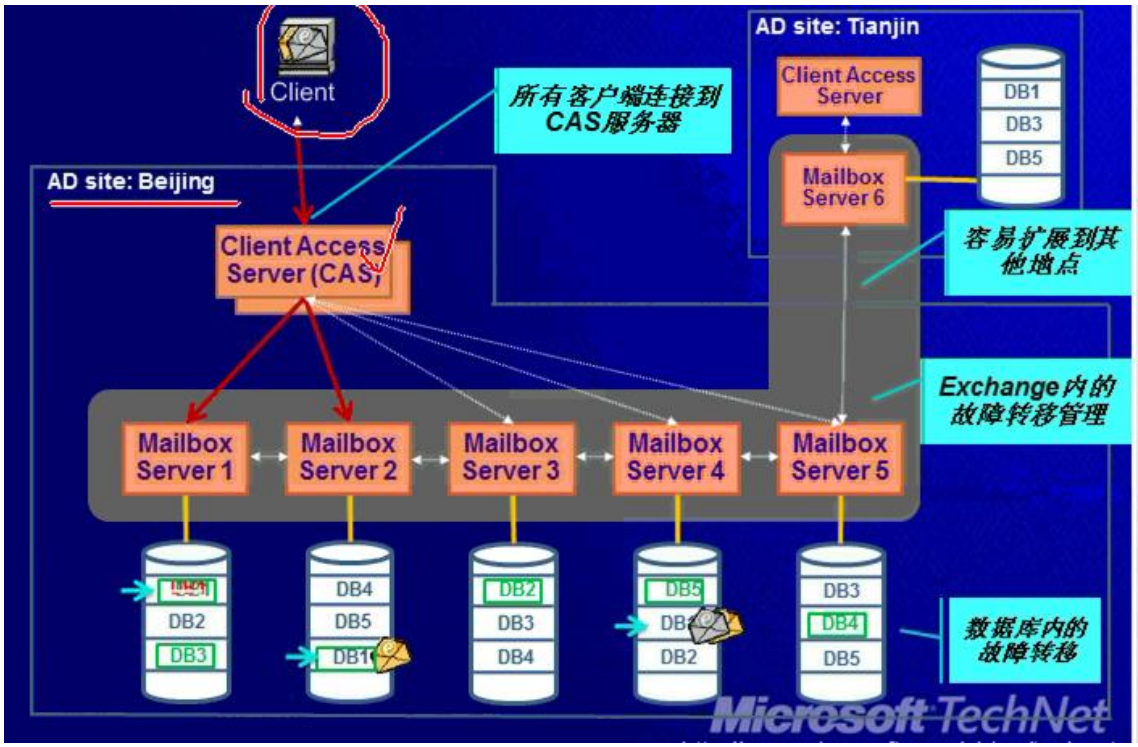
CAS服务器的高可用可以通过NLB或者硬件负载平衡。

exchange 2010的高可用性目标。

exchange 2010的增强

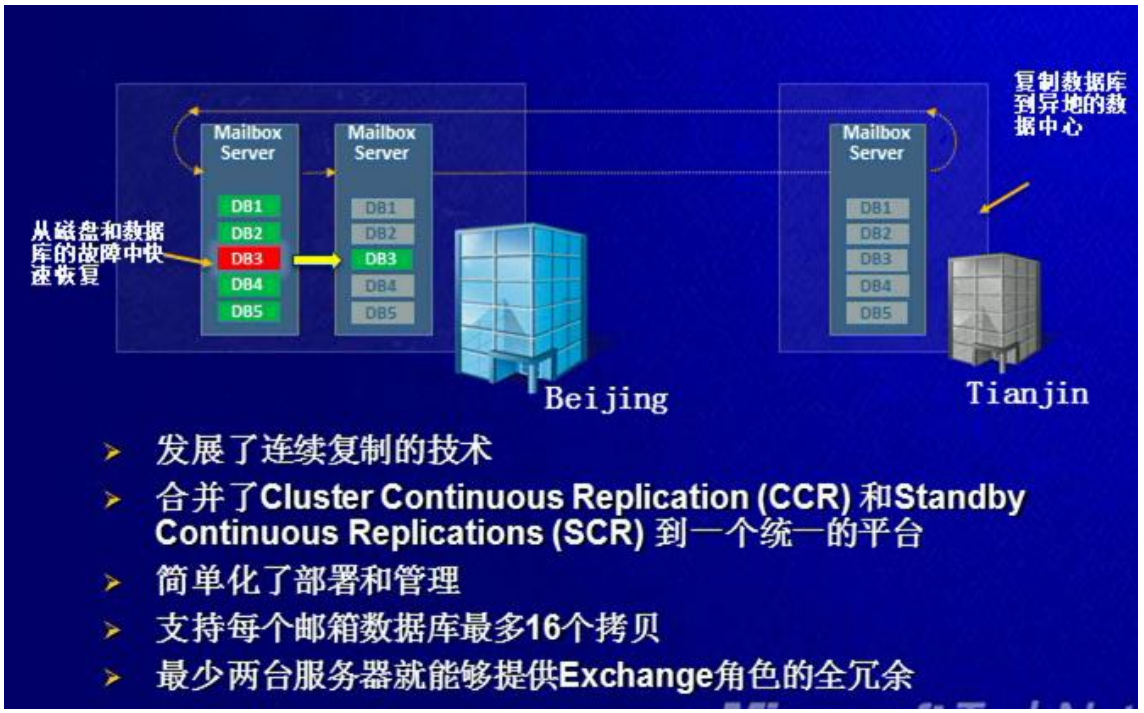
支持无RAID架构。

高可用架构图。

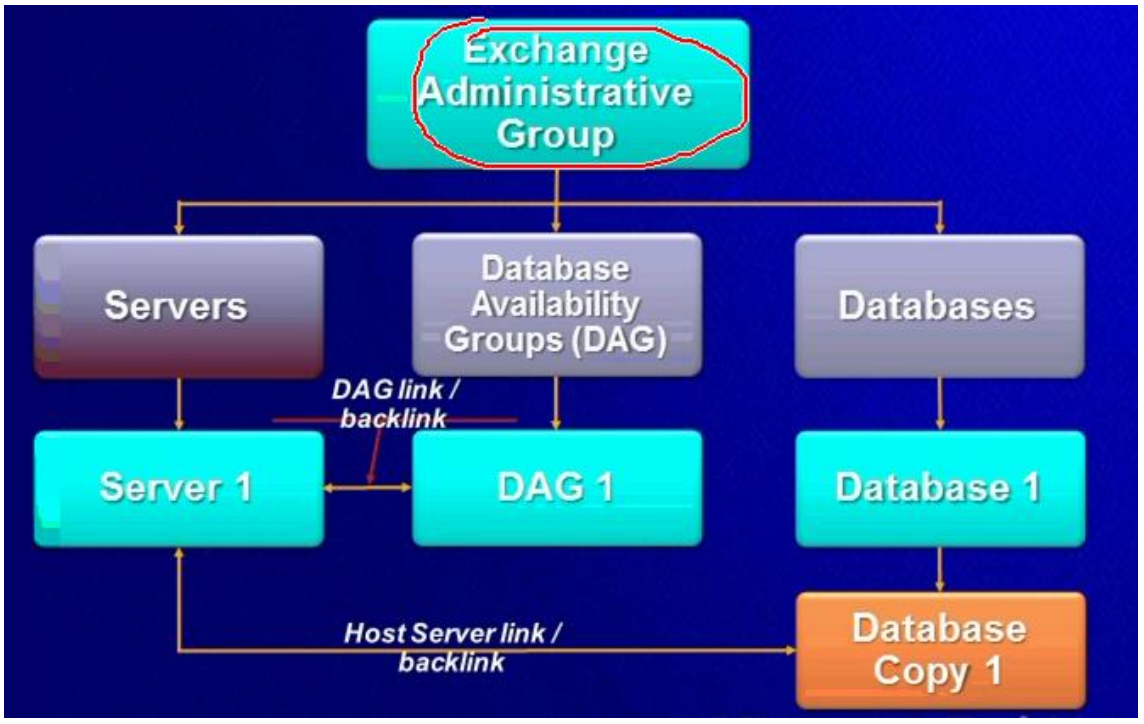


当某一个DB挂了，会自动切换到好的服务器上，由AM来做。

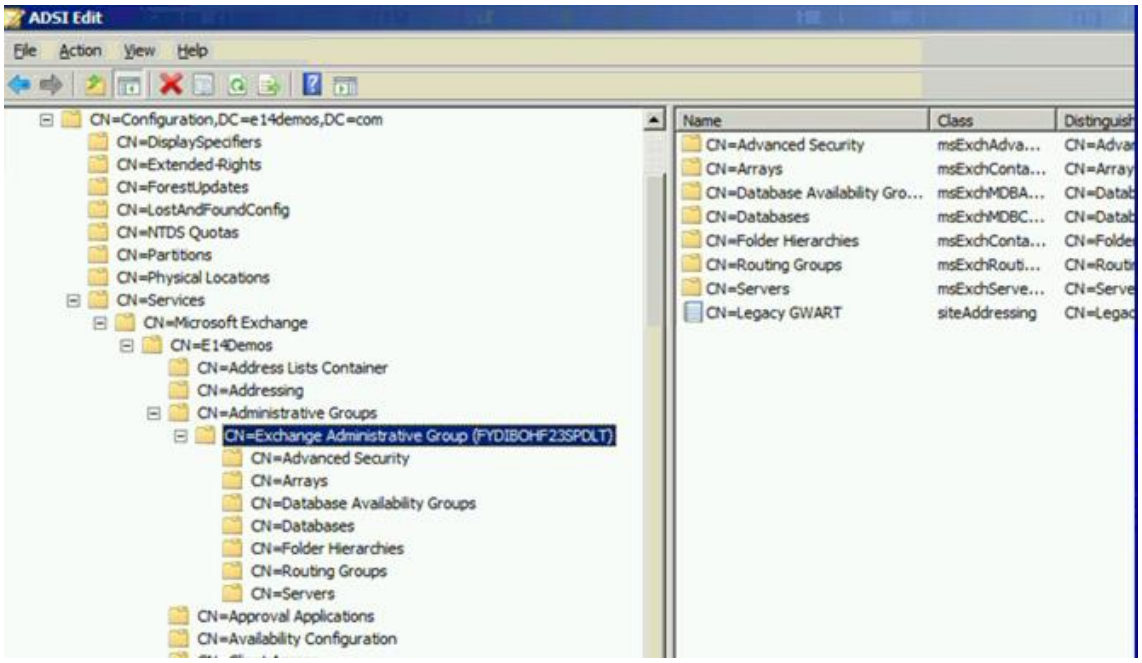
是高可用和灾难恢复的统一平台。



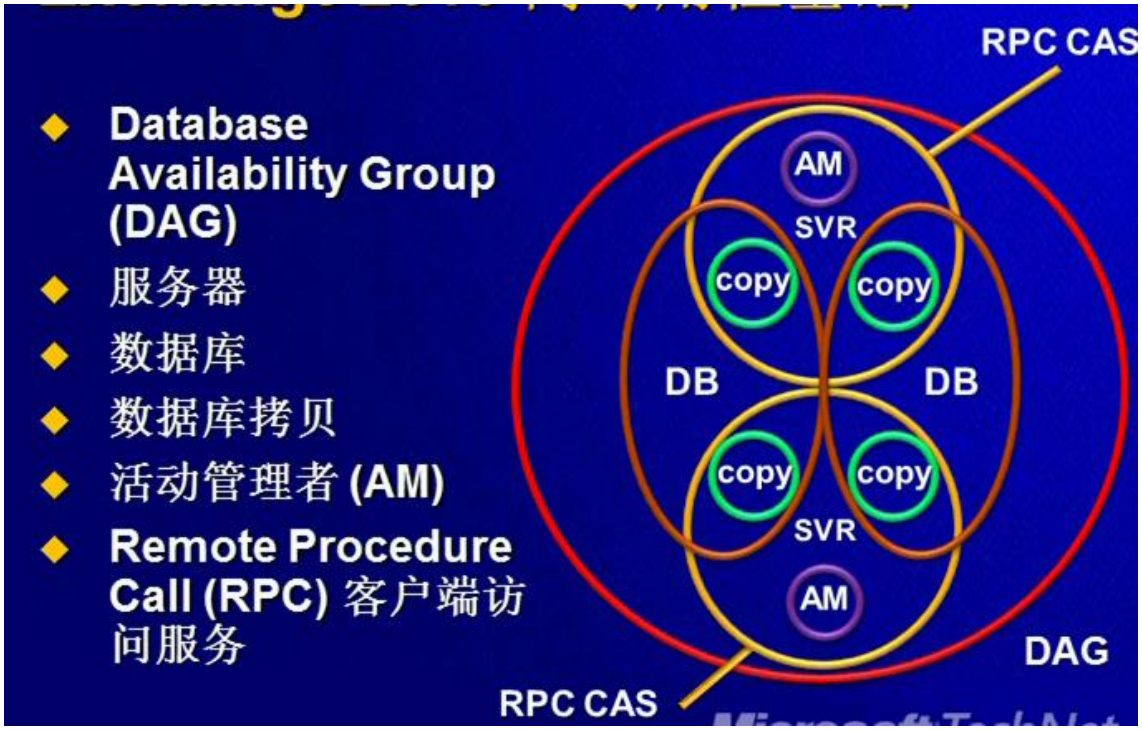
exchange 2010 AD域服务架构



使用ADSIEDIT查看exchange的架构。



基础概念。

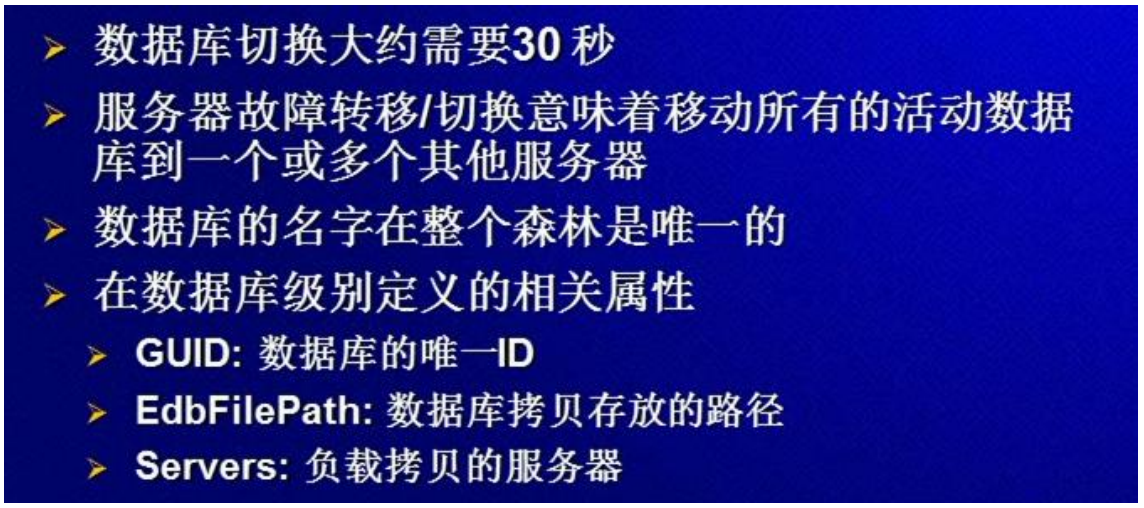


基础概念：DAG


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
Mailbox Server 1
Mailbox Server 2
Mailbox Server 3
Mailbox Server 4
Mailbox Server 16

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
Mailbox Server 1
Mailbox Server 2
Mailbox Server 3
DB1
DB2
DB3
DB4
DB1
DB2
DB3
DB4
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

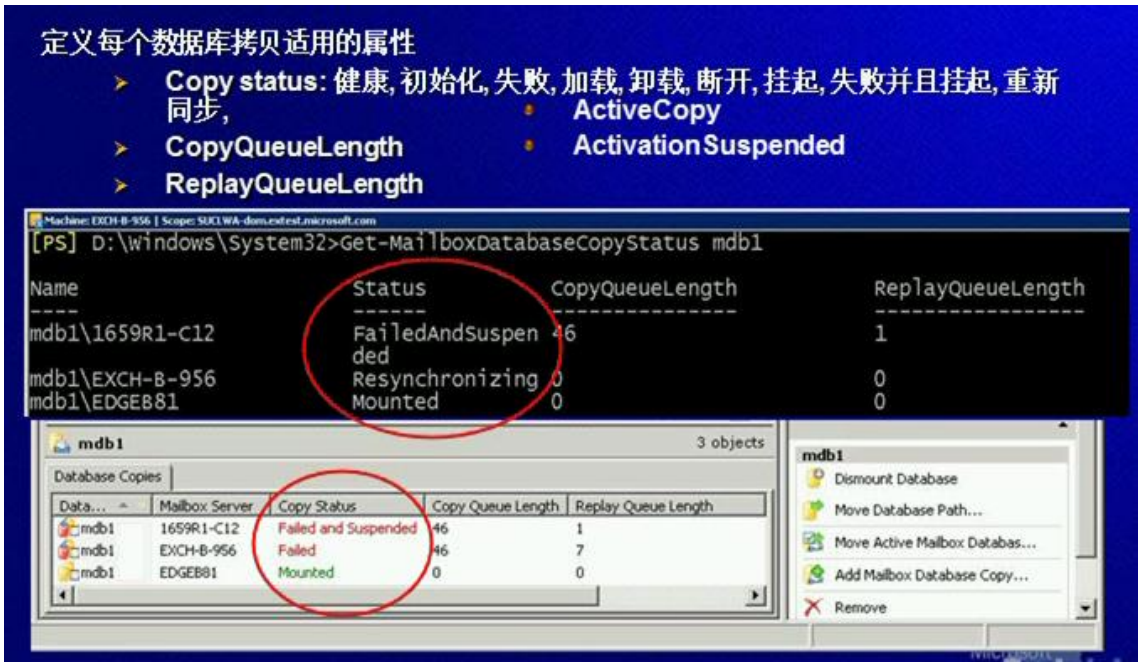


主动、被动

源、目标

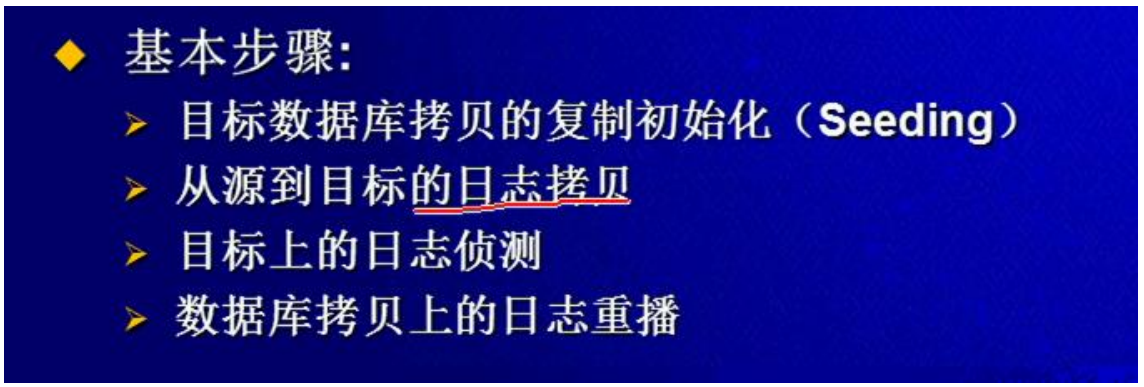
邮箱数据库的拷贝

查看拷贝复制的过程和属性

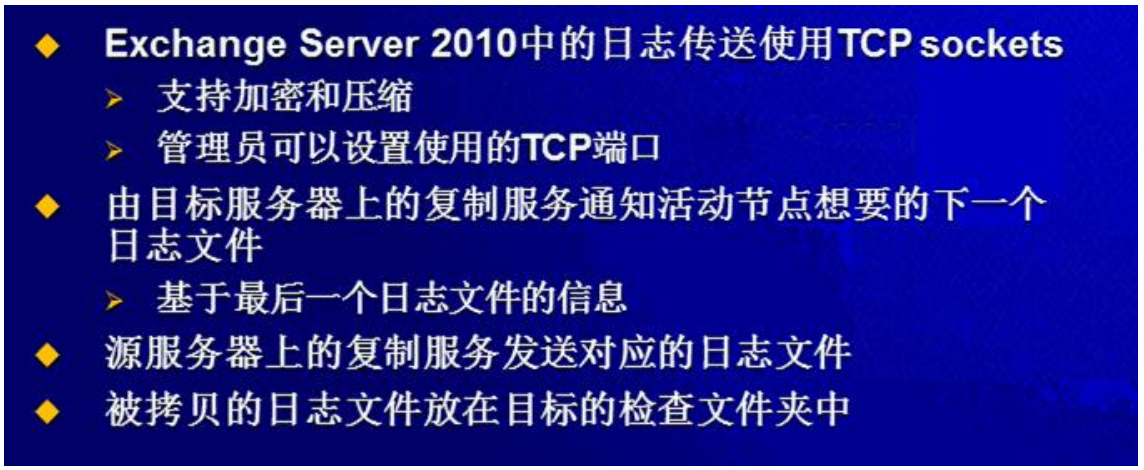


关于exchange的active manager

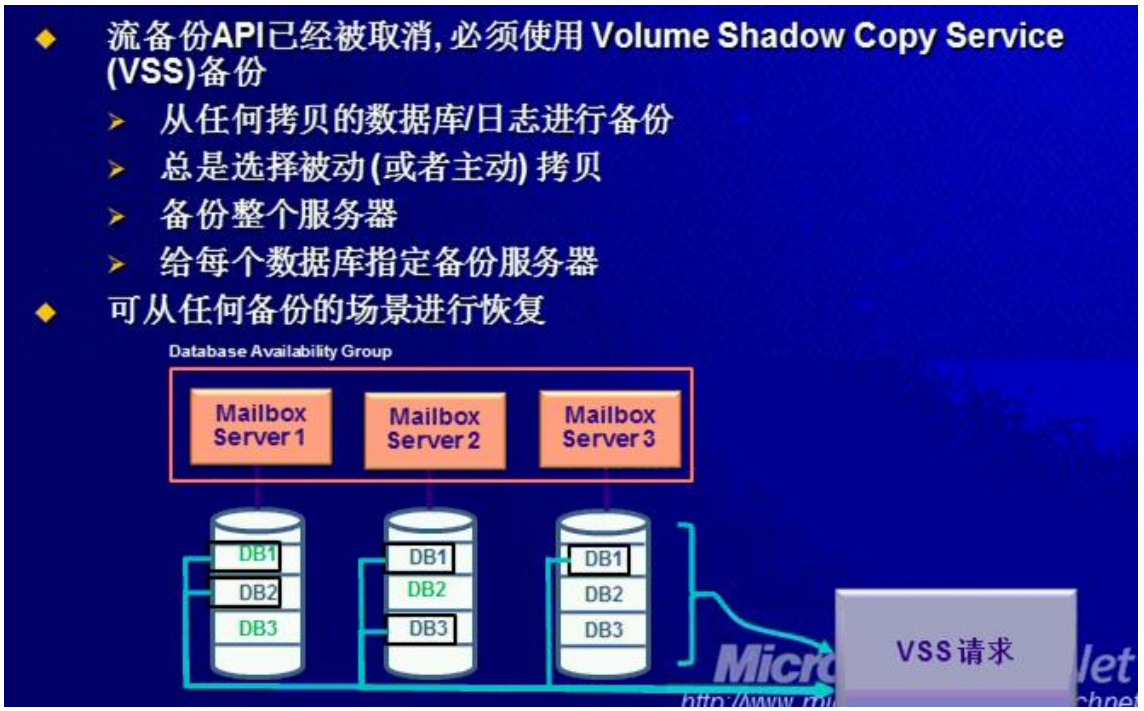
连续复制的过程



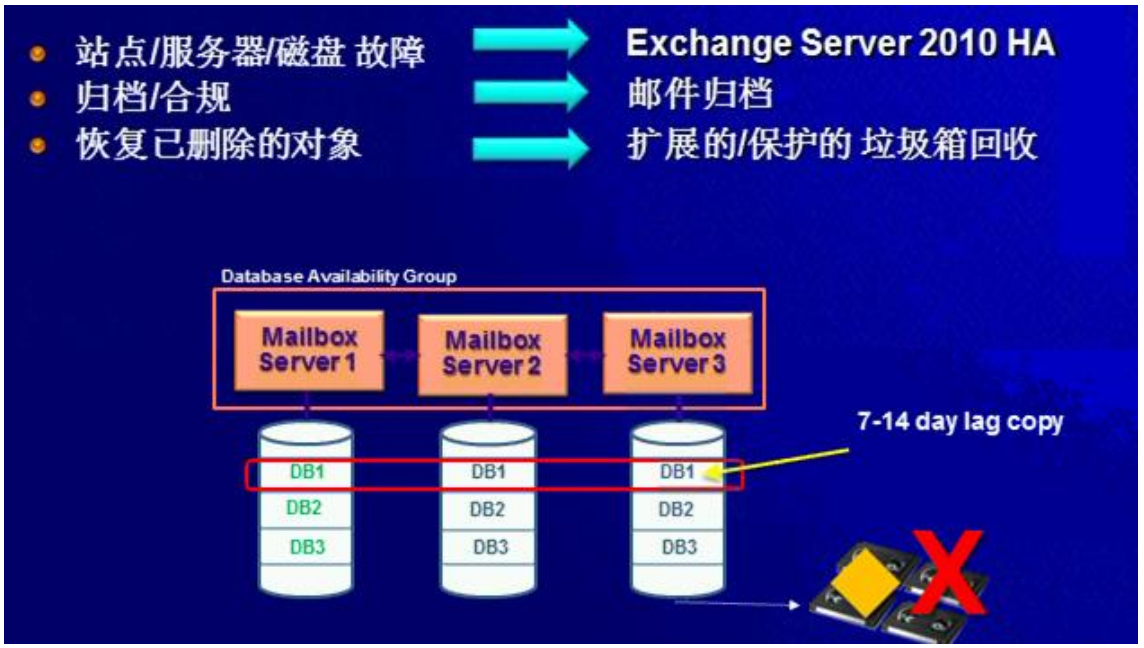
日志传输的过程



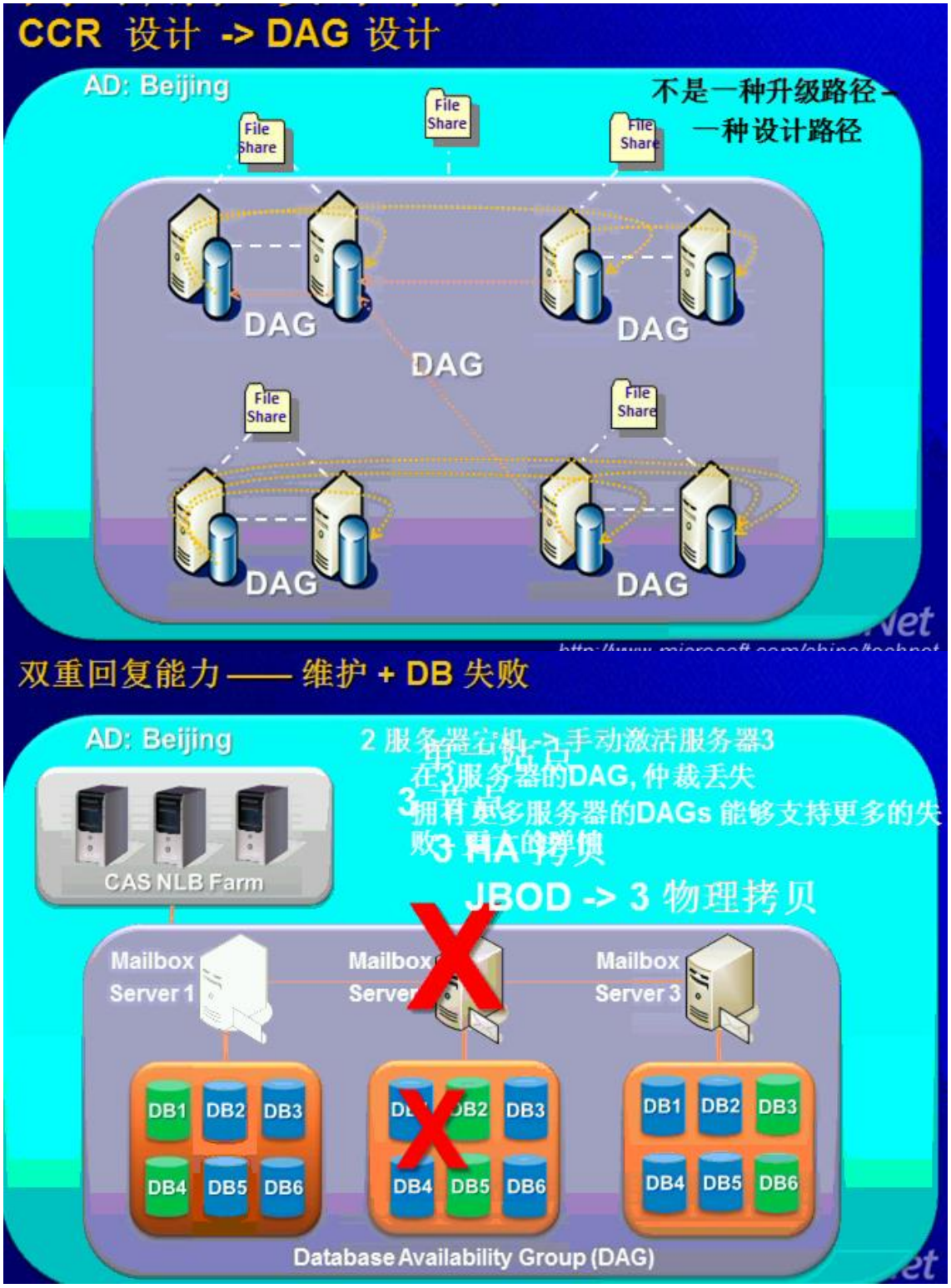
关于exchange的备份



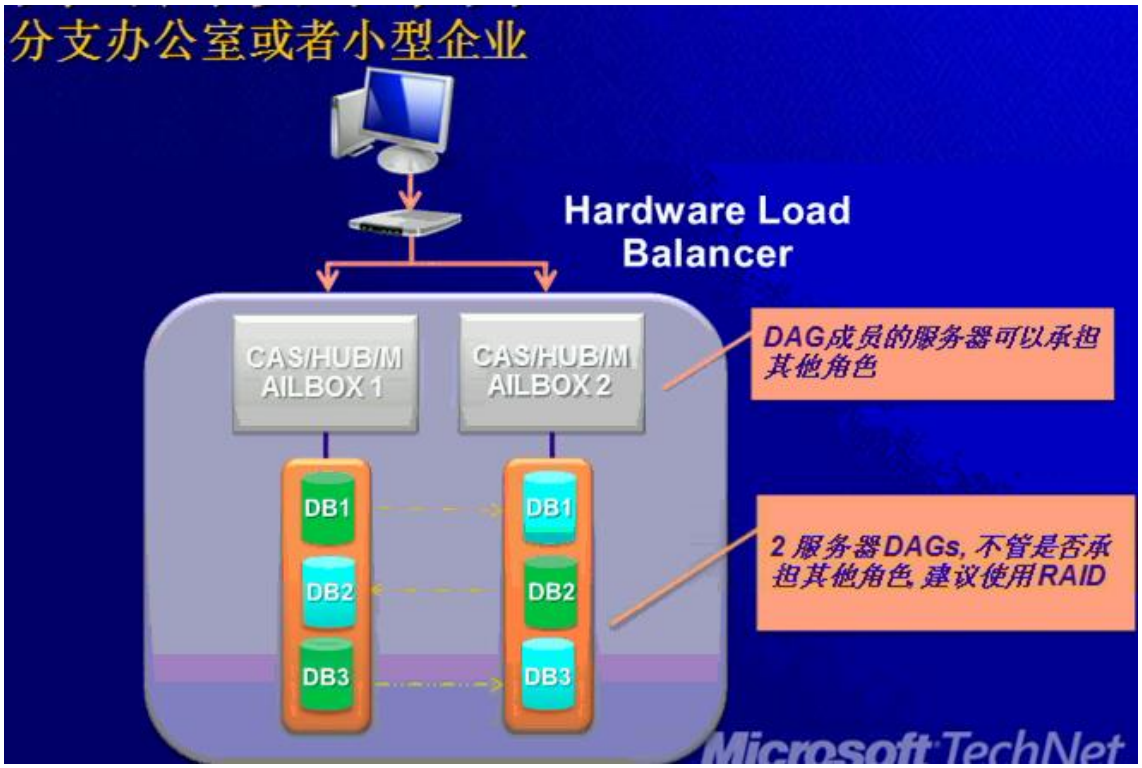
多数据库的拷贝可以实现无备份的配置



从exchange CCR到exchange DAG



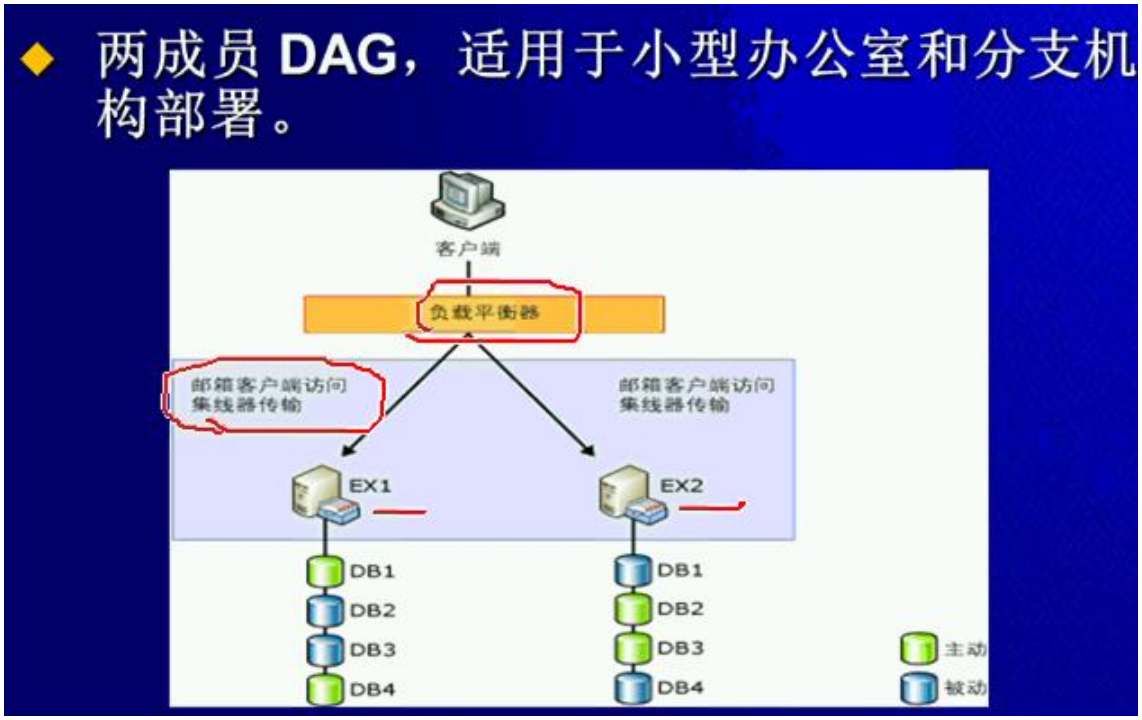
ALL in one部署只能使用硬件的NLB，因为微软的NLB和cluster不能共存。



==========

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。

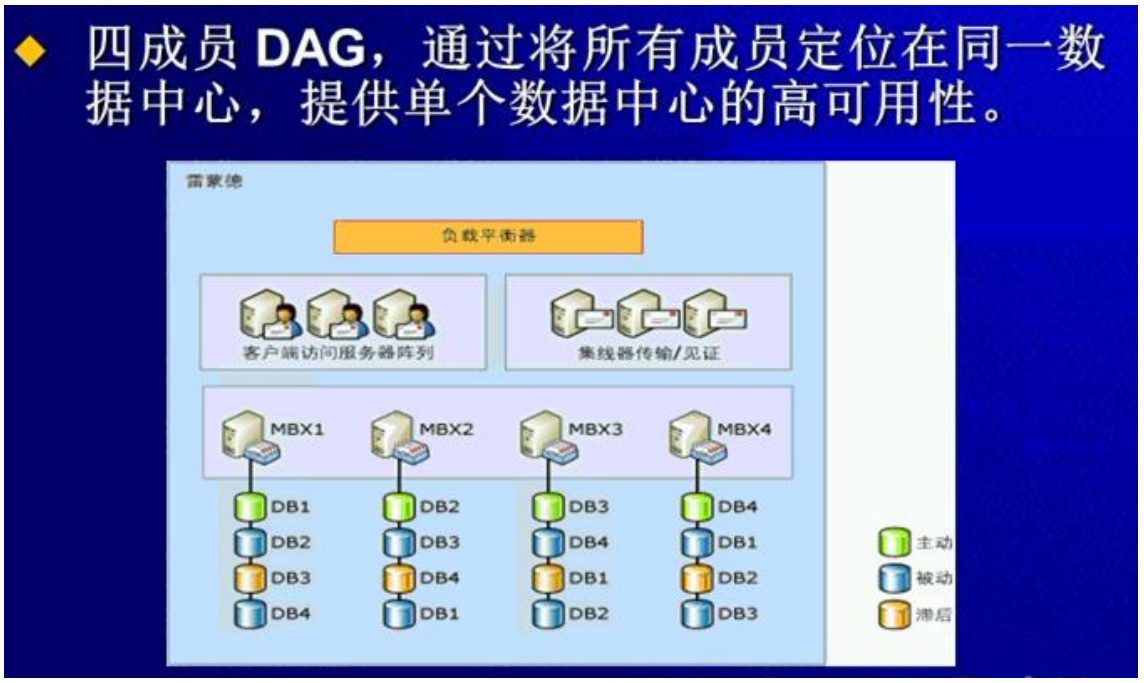


一个主动副本。

两个被动副本。

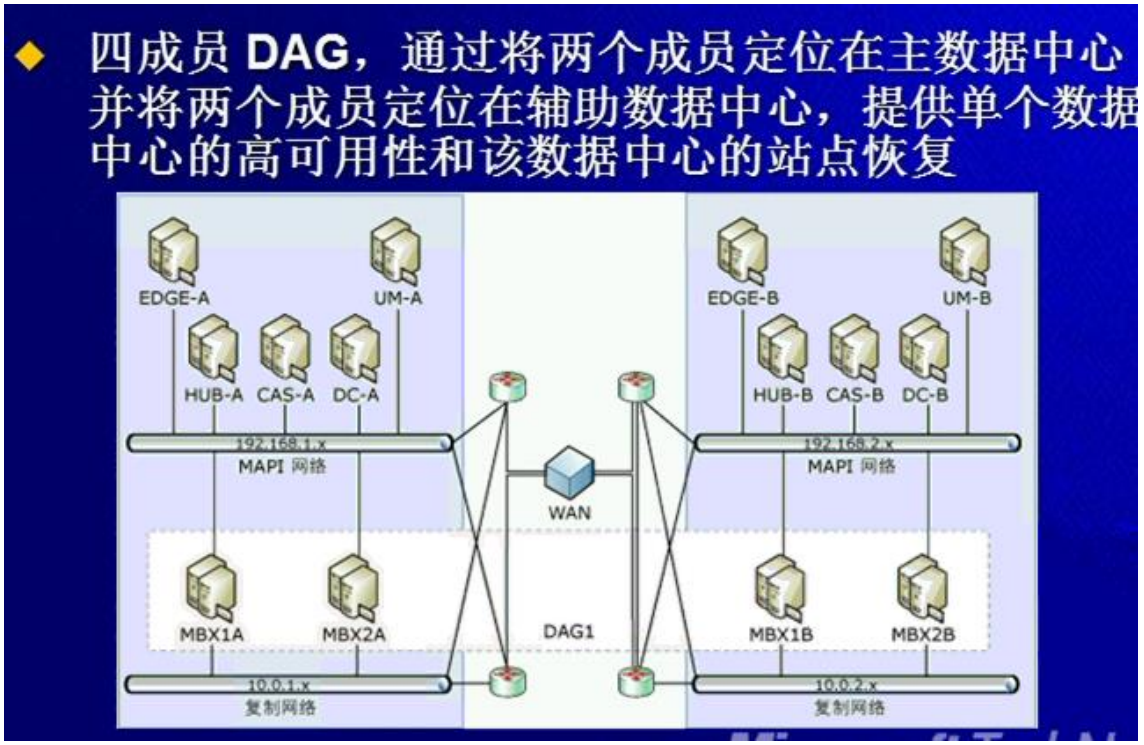
一个滞后副本。

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，数据中心的灾备。

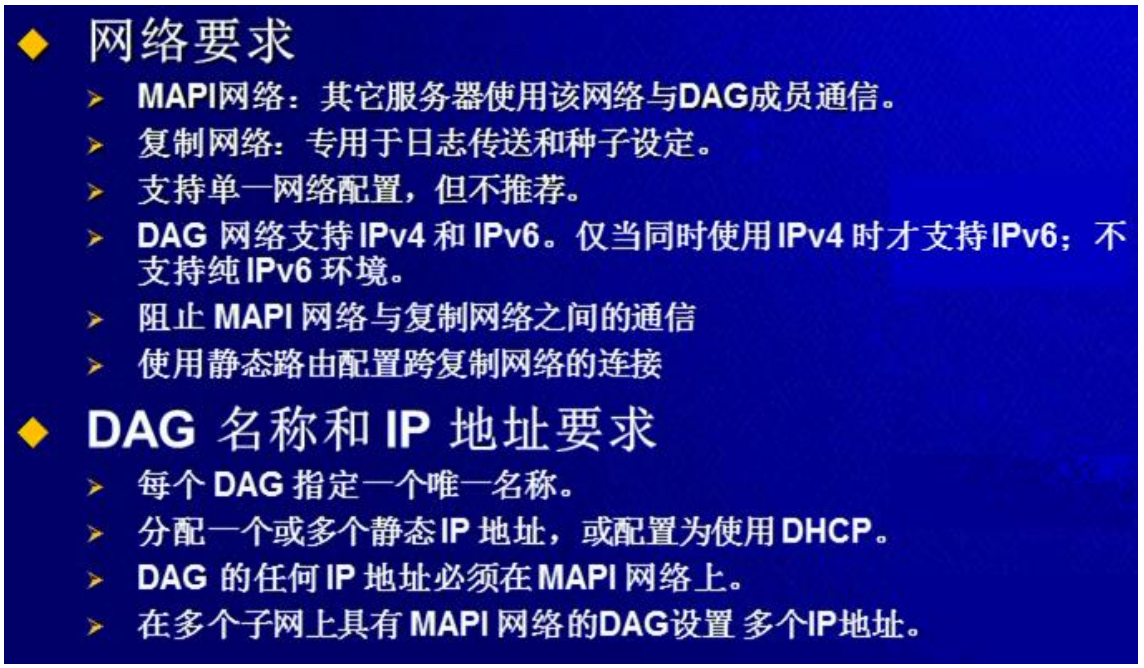
见证服务器放在总部，分支机构可以放置备用的见证服务器。



DAG的设计前提。

DAG不能跨域。

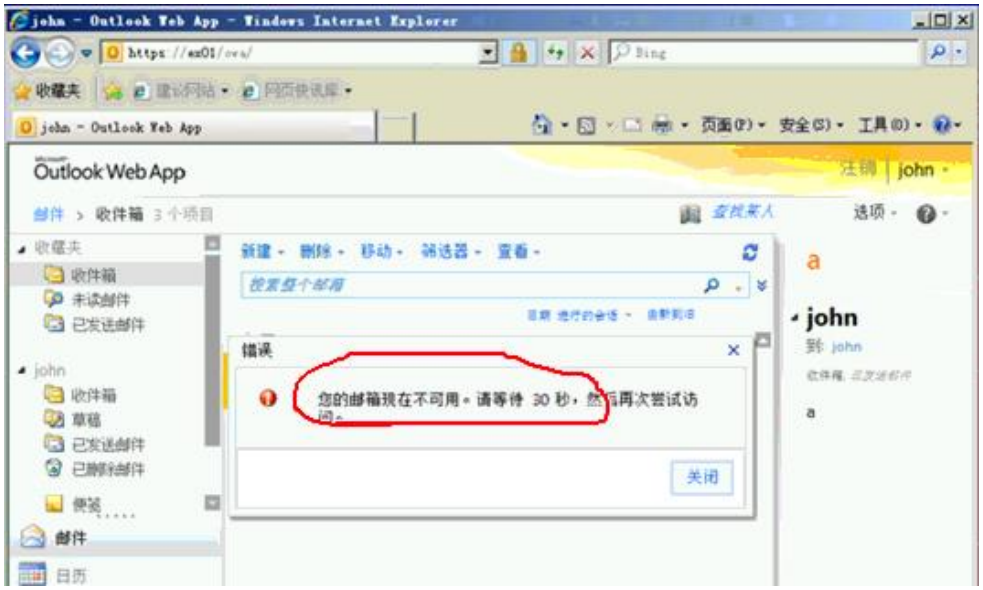
并置AD的邮箱角色不能做DAG。



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。

DAG的部署过程。

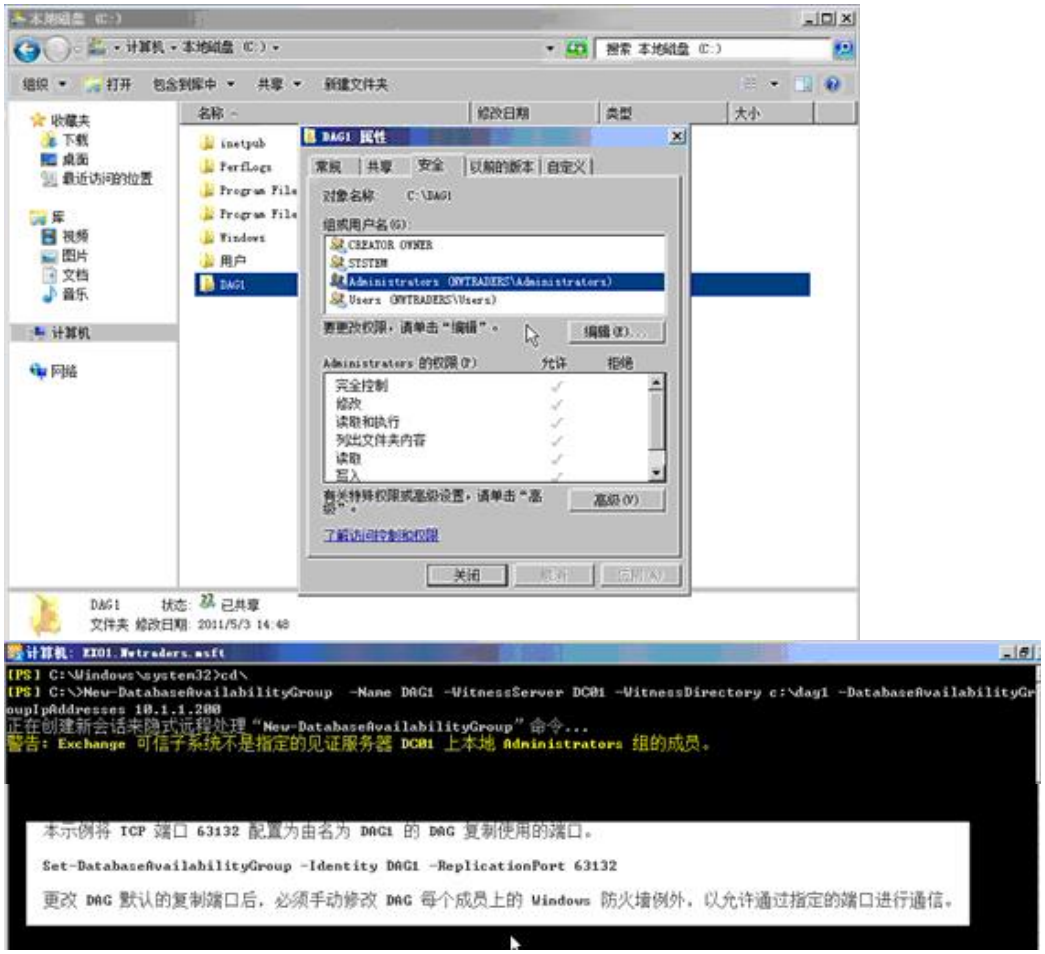
DAG出现故障切换时，OWA会提示出现故障，切换需要30秒。



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。

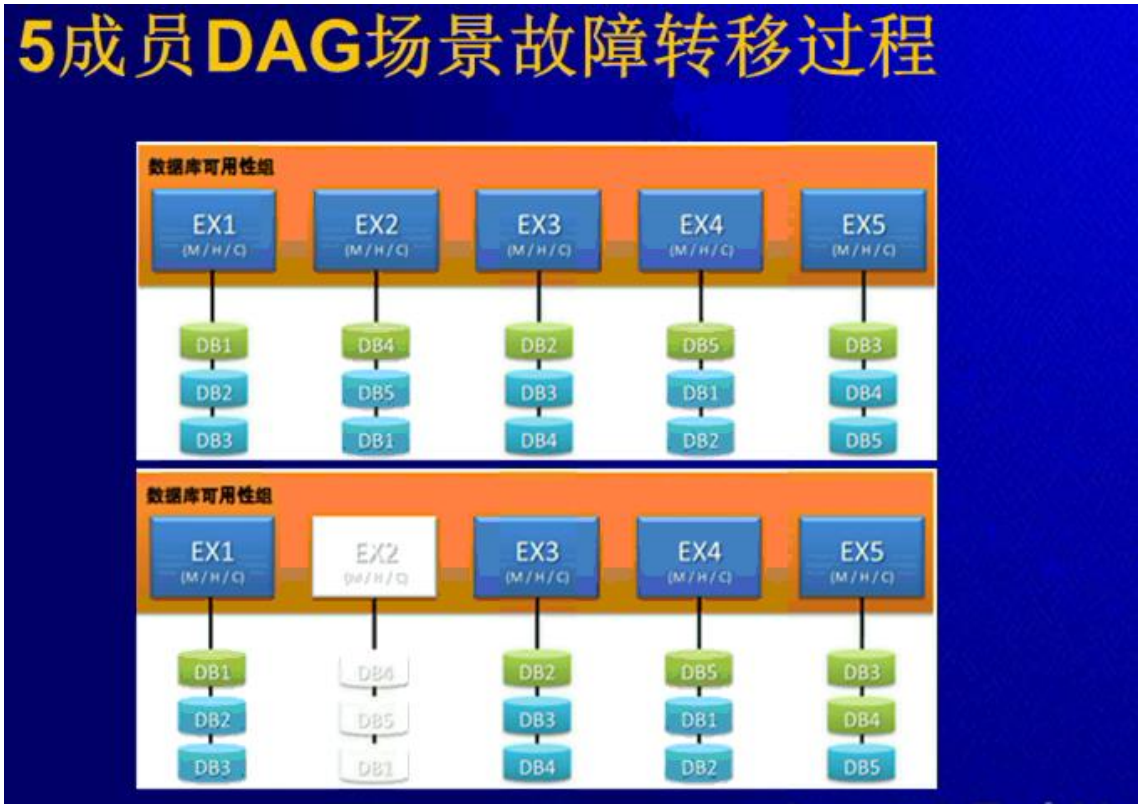
如果见证服务器不是exchange的成员，则还需要把一个角色加入到见证服务器的本地管理员组exchange trusted subsystem。



根据首选参数进行数据库的转移。

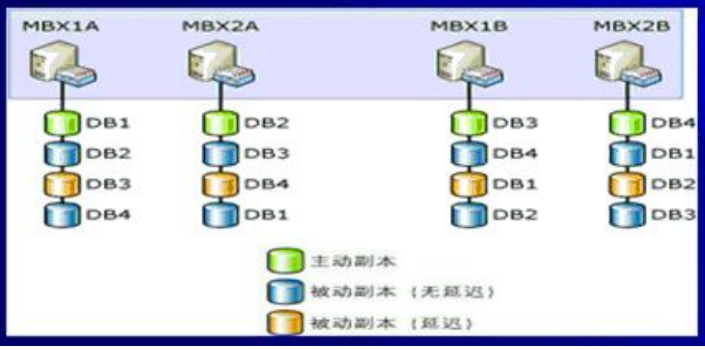
通过AM。

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。



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
```

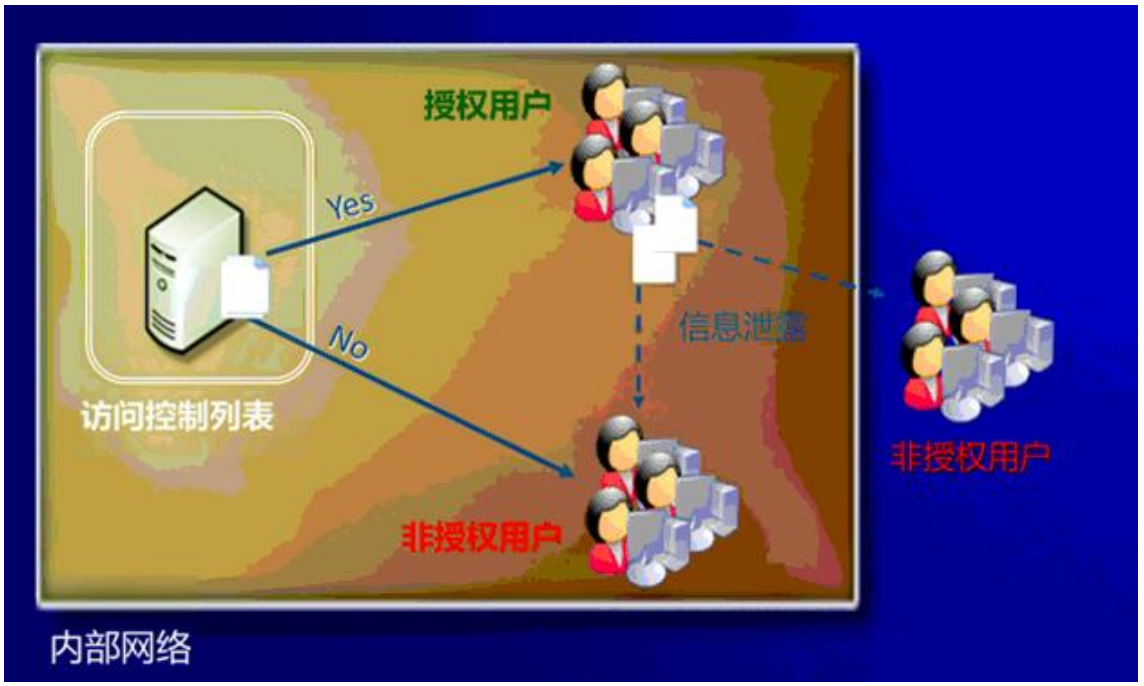
```
[PS] C:\Windows\system32>Test-ReplicationHealth

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。

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?

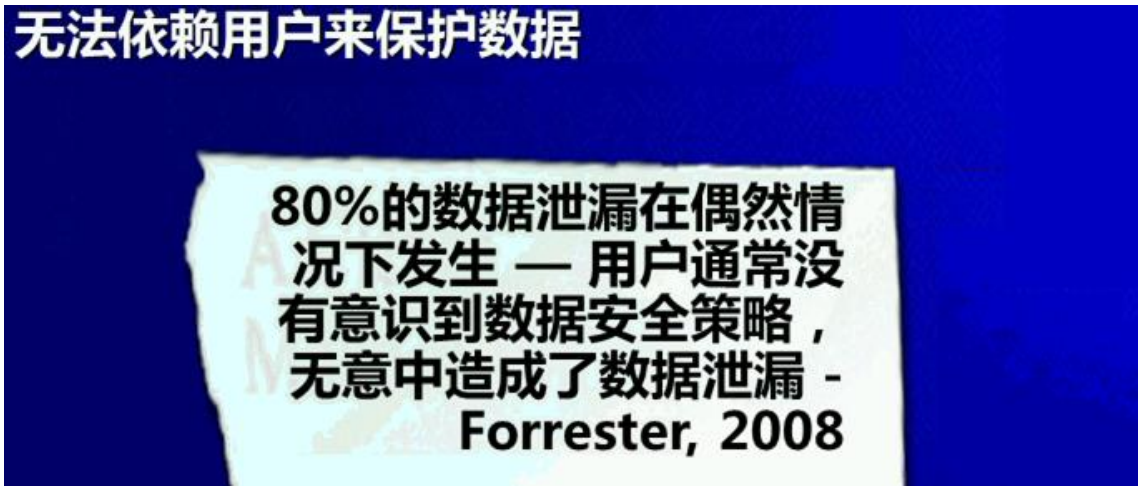
1）传输层安全性TLS。

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。



ADRMS技术。

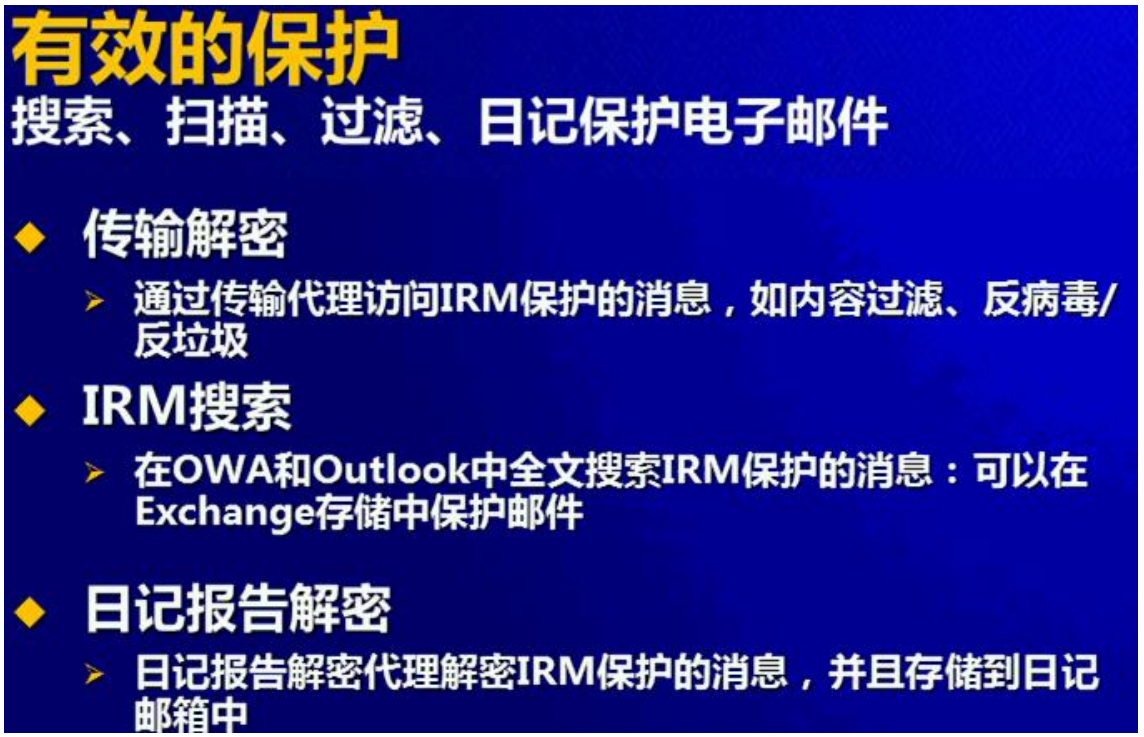
基于用户进行权限的设定。

IRM是基于ADRMS的。

集线器传输的规则使用。应用RMS模板，对邮件进行加密。

通过outlook保护规则进行自动加密设定。

解密和搜索机制。

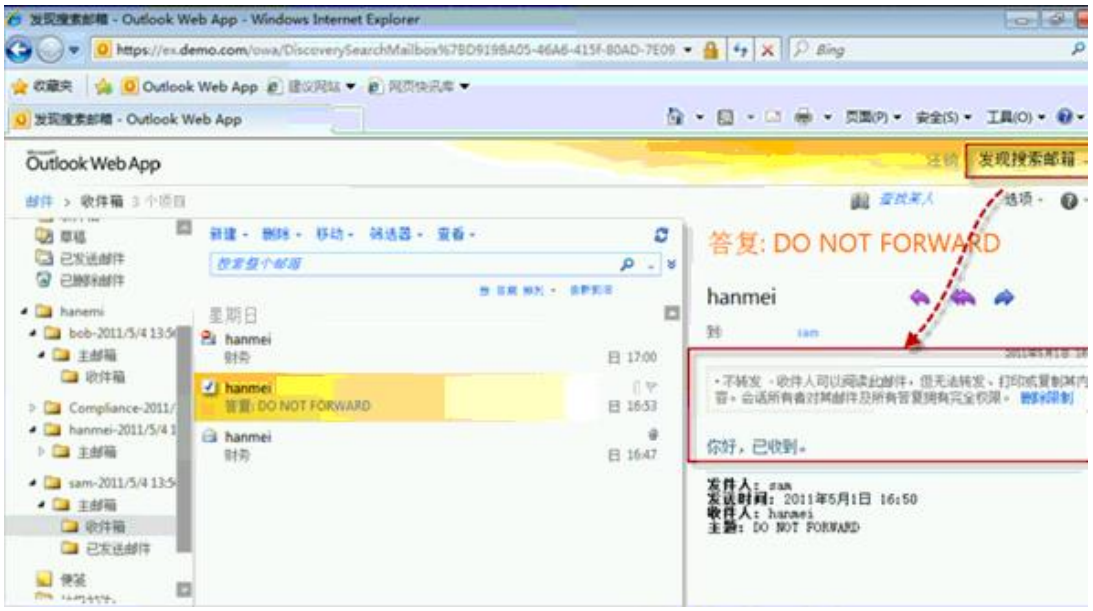


传输前先解密，传输后重新加密。

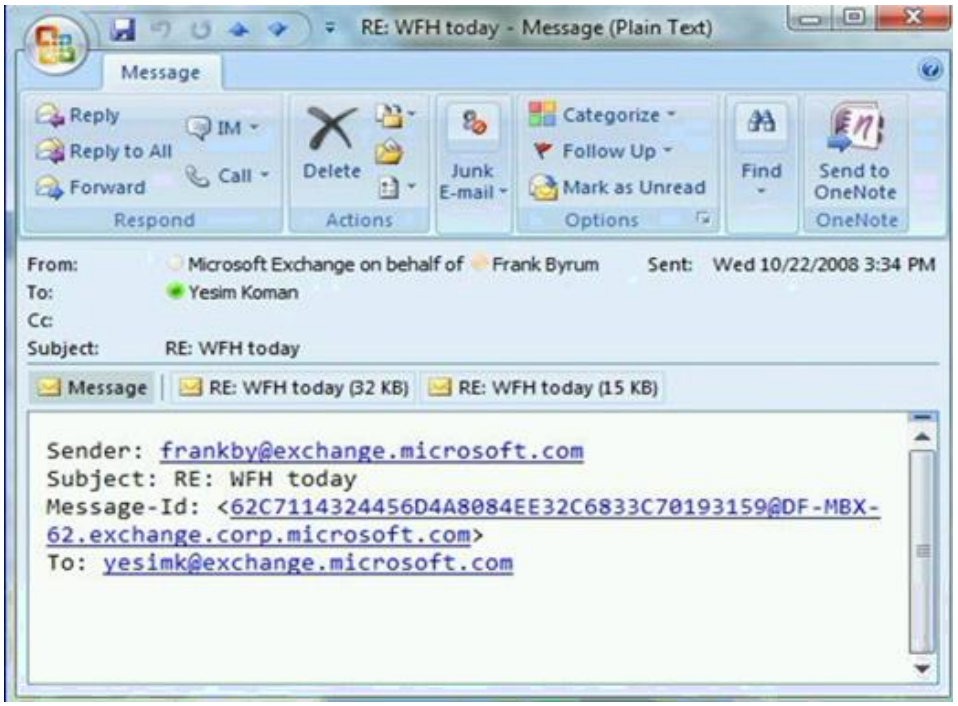
传输管道解密

- 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。


RE: WFH today - Message (Plain Text)
Message
Reply
Reply to All
Forward
IM
Call
Respond
Delete
Actions
Junk E-mail
Categorize
Follow Up
Mark as Unread
Options
Find
Send to OneNote
OneNote
From: Microsoft Exchange on behalf of Frank Byrum
Sent: Wed 10/22/2008 3:34 PM
To: Yesim Koman
Cc:
Subject: RE: WFH today
Message
RE: WFH today (32 KB)
RE: WFH today (15 KB)
Sender: frankby@exchange.microsoft.com
Subject: RE: WFH today
Message-Id: <62C7114324456D4A8084EE32C6833C70193159@DF-MBX-62.exchange.corp.microsoft.com>
To: yesimk@exchange.microsoft.com