

Microsoft IT 活动目录管理概要

余学俊
IT manager
Microsoft China, Beijing

主要议题

- 如何处理重要变更?
- 灾难恢复策略
- 域控制器的部署
- AD的配置和Exchange
- 怎样使用64-位 域控制器?
- 域控制器的监视和管理

怎样使用本演讲内容

- 微软的IT环境（或许）跟您的企业IT环境有很大不同
 - 并非所有推荐做法适用于您的环境
- Look for the “golden nuggets” that will help you
- 未包括的内容: 策略, 委派, 安全

Microsoft IT 环境一览



How Does Microsoft IT...

- Manage Significant Changes?
- Do Disaster Recovery?
- Deploy Domain Controllers?
- Configure AD for Exchange?
- Use 64-bit Domain Controllers?
- Monitor and Maintain DCs?

管理重要变更

- 变更的例子
 - 域森林功能模式的变化
 - Forestprep 或 Domainprep
 - Schema 变更
- 测试
 - 推荐作实验室测试
 - 建立并记录测试过程
 - 一次只处理一个重要变更
- 方法
 - 离线域控制器
 - 在私有网络上测试变更

管理不确定性 离线域控制器

- 比用备份数据恢复DC更为快速
- 把一个DC移出网络
- 用它作为种子恢复森林域
- 当变更生效后, 继续保持离线状态 48-72 小时
- 应尽可能使用DC而非GC
- 确保你可以正确登录!

管理不确定性 逐层剥离法

管理不确定性 逐层剥离法

管理不确定性 逐层剥离法

Managing Uncertainty Peel Off Method

管理不确定性 逐层剥离法

- 私有网络配置
 - DNS 变化
 - Seize FSMO roles (if necessary)
 - Don't seize the RID Master
 - IP 配置变化
 - 复制连接目标

*变更被复制!
(包括那些在私有网络上的变更)*

How Does Microsoft IT...

- Manage Significant Changes?
- Do Disaster Recovery?
- Deploy Domain Controllers?
- Configure AD for Exchange?
- Use 64-bit Domain Controllers?
- Monitor and Maintain DCs?

活动目录的服务恢复

目标: 最小化服务器故障引发的影响

- 业务的不间断性构建于
 - 精确掌握场点分布的拓扑结构
 - 对核心场点使用 *DNSAvoidRegisterRecords* 配置 DNS 记录 (Q306602)
- 远程重构
 - 所有本地域控制器配备远程管理板卡
 - Install From Media promotions
 - On disk system state backup via AT job with a batch file calling NTBackup

森林恢复

目标: 在灾难发生时能用最短时间恢复到森林的正常工作状态 Minimize time to "roll back" the forest in case of catastrophic failure

- 记录并演练森林域恢复
 - 至少要事前通读相关白皮书的内容
- 应考虑到每个域中至少有一台 DC (non-GC) 需要恢复
- 确保主要的应用软件维护人了解并测试森林域恢复动作。
- 遵循先恢复根/父节点域, 然后恢复子节点域的原则, 以确保完整的信任关系不被破坏

数据恢复

- 把关键业务数据置放于 AD 之外
 - 一旦森林需要恢复, 这些关键数据可以重新发布
 - 可以确保数据在多森林域环境中的一致性
 - MIIS 支持与多个管理工具的同步 (e.g., Via SQL, etc.)
- 附加的业务好处
 - 审计, 跟踪, 识别变更
 - 业务规则/逻辑 强化执行
 - 通过角色委派/分离提高了安全保障

How Does Microsoft IT...

- Manage Significant Changes?
- Do Disaster Recovery?
- Deploy Domain Controllers?
- Configure AD for Exchange?
- Use 64-bit Domain Controllers?
- Monitor and Maintain DCs?

DC 部署安排

- 接受每年两次审核
- 考略业务应用软件的需求
- 网络考略因素
 - 大于 99.5% 的可用性
 - 小于 90% 的平均使用率
 - 小于 750 ms 的往返包延迟
 - 带宽大于 512 Kbps
- 场点分类
 - 员工数
 - 用户类型
 - 把域控制器集中到数据中心

DC 集中管理

- 区域集中计划
 - 区域性数据中心整合集中
 - 应用软件的整合集中
 - 考量与区域用户的服务级别和性能级别协议规定
- 主工作森林
 - 整合前
 - 218 域控制器
 - 133 场点
 - 整合后
 - 138 域控制器 (减少了37%)
 - 64 场点

How Does Microsoft IT...

- Manage Significant Changes?
- Do Disaster Recovery?
- Deploy Domain Controllers?
- Configure AD for Exchange?
- Use 64-bit Domain Controllers?
- Monitor and Maintain DCs?

针对Exchange配置活动目录

- 纯粹 Exchange 2003 和 Office 2003 环境
 - Outlook 2003 缓存模式
- 全球4个Exchange 中心
 - 为总部 Redmond 的Exchange 服务器专门设计了一个场点
 - 其他3 个地点 - DC 同时承担认证职能

什么时间需要专门的场点 (Sites)

- 从无开始
 - 服务器数量增加
 - Increases security footprint
 - 附加的管理负荷
- 应用软件需求
- 应用软件的性能要求专用的硬件支持
- 网络需求
- 业务需求
 - 出错恢复, 容错, 冗余备份, 可用性

How Does Microsoft IT...

- Manage Significant Changes?
- Do Disaster Recovery?
- Deploy Domain Controllers?
- Configure AD for Exchange?
- Use 64-bit Domain Controllers?
- Monitor and Maintain DCs?

64-位域控制器部署概要

- 2002.10 上线3台IA64服务器
- 2004.12 上线12台AMD64服务器
- 2005.6部署另外12台 AMD64服务器和24台 EM64T 服务器
- 显著改进了查询为主的应用软件性能(如 Exchange)
- 对认证业务的性能改进不大
 - 此类业务的性能提高更多取决于增加新服务器, 升级更快速的CPU。内存增加对此影响不大。
- 只在出现>3GB DIT 文件的域中部署64位域控制器

服务器

- 所有域控制器遵从标准化的软硬件配置
 - 新的服务器全部为64位
- 尽可能减少可能的服务器功能分类
Minimum number of SKU's possible
 - 个可能的服务器分类
 - 区域性, 非Exchange服务 (EM64T)
 - 数据中心, 支持Exchange服务 (AMD64)
- 4 年硬件更新周期
- 同样的基础配置, 当技术发生变化时按照需求进行更新

How Does Microsoft IT...

- Manage Significant Changes?
- Do Disaster Recovery?
- Deploy Domain Controllers?
- Configure AD for Exchange?
- Use 64-bit Domain Controllers?
- Monitor and Maintain DCs?

服务器配置

- LDAP Policies (Q315071)
 - MaxQueryDuration set to 45 (default = 120)
 - MaxActiveQueries set to 32 (default = 20)
- NTDS\Diagnosics registry key
 - "15 Field Engineering" set to "5"
 - Logs events for expensive/inefficient queries
 - "6 Garbage Collection" set to "4"
 - Logs events for database size and whitespace
- Netlogon\Parameters registry key
 - LdapSrvPriority and LdapSrvWeight
 - Isolating or load balancing hardware

监视性能

- 收集历史性能数据
 - 诊断问题
 - 规划容量
 - 整合域控制器
 - 新的部署
- 周期性运行服务器性能顾问软件Run Server Performance Advisor periodically
 - 配置统一的编辑/报告服务器作为中心存储设施
 - 每天在业务繁忙时段收集性能快照数据并保留他们作基准性能参考
 - 当服务器正常运行时生成基准报告
- 不要让DC持续在超过60% CPU利用率状态下运行
 - 平均30-40%的CPU利用率是我们的目标“正常”状态
 - 平均 > 50%的CPU利用率或不断增长的趋势 - 需要审核服务器容量

复制

- 让 KCC 帮你管理复制环境
 - Windows Server 2003 的改进算法使你根本无需利用手工连接
- 借助场点和子网的划分及作用力精细控制复制Leverage the power of sites & subnets for granular control of replication
 - Faithful to the LAN = site definitions
 - 让你的复制拓扑与网络拓扑保持一致Keep your replication topology true to your network topology.
 - 越来越多的应用软件在参考这一原则 (SMS, DFS, etc...)
- Repadmin.exe - 学习他, 喜欢他, 利用它
 - repadmin /replsum /bysrc /bydest /sort:delta - health check
 - repadmin /showrepl * /csv - Import into Excel
 - repadmin /options * +disable_inbound_repl

监视FRS

- Deploy Ultrasound to monitor FRS
 - Watch out for Sharing Violations. They are the most common problem
 - Usually caused by incorrect permissions in SYSVOL or Applications opening SYSVOL with incorrect permissions
 - Watch for mangled named files/folders "ntfrs_xxxxx", "scripts_xxxxx"
- Use the Ultrasound management pack for Microsoft Operations Manager (MOM) ease monitoring

How Does Microsoft IT...

- Manage Significant Changes?
- Do Disaster Recovery?
- Deploy Domain Controllers?
- Configure AD for Exchange?
- Use 64-bit Domain Controllers?
- Monitor and Maintain DCs?

Resources

Microsoft IT Showcase:

<http://microsoft.com/itshowcase>

Creating a dedicated AD site for Exchange:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=6B263452-7A61-4253-9C9E-B337CB80D460&displaylang=en>

AD Forest Recovery White Paper:

<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=3EDA5A79-C99B-4DF9-823C-933FEB A08CFE>

Server Performance Advisor:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=61a41d78-e4aa-47b9-901b-cf85da075a73&DisplayLang=en>

