AD专题汇总-操作主机管理

作者：曾垂鑫

51CTO专家讲师、微软MVP

背景

- ADDS数据库内绝大部分的复制是采用多主机复制模式（multi-master replication model），可以直接更新任何一台域控制器内绝大部分的ADDS对象，之后这个对象会被自动复制到其他域控。
- 而只有少部分的数据的复制是采用单主机复制的模式（single-master replication model），当提出更改对象的请求时，只会由其中一台被称为操作主机的域控制器负责接收与处理此请求，该对象先被更新在这台操作主机内，再由它将其复制到其他DC
- 操作主机角色（operations master roles）也被称为FSMO（flexible single master operations roles）。
- 多主复制模式中，为了避免复制冲突，通过让一个单域控制器负责操作

操作主机概述

五种操作主机介绍

林级别

- 架构操作主机
  - 负责更新与修改架构schema内的对象种类与属性数据
  - 隶属于schema admins组内的用户才有权利修改架构
  - 一个林只有一台架构操作主机
- 域命名主机
  - 负责林内域目录分区的新建与删除，即负责林内的域添加和删除工作
  - 负责应用程序目录分区的新建和删除
  - 一个林中只能有一台域命名主机
  - 防止多个域用同样的域名加入目录林
  - 域命名主机必须是GC，因为当域命名创建了新域时，查询GC核实是否有别的对象，包括域对象使用和新域对象相同的名字
  - 需要enterprise admins的权限

域级别

- RID操作主机
  - 发放RID（relative ID）给域内所有的域控制器
  - 当域内新建用户/计算机/组对象时，DC需要指派一个唯一的安全标识符（SID）给这个对象
  - 当在域间移动对象时，必须在当前包含该对象的RID主控上启动移动，这可避免对象可能的复制，当对象从一个域移动到另一个域时，RID主控将从域中删除对象
  - 对象SID=域SID（对于所有域中创建的安全规则都相同）+RID（对于域中创建的每个安全规则都是唯一的）
  - 每台域控制器需要RID时，它会向RID操作主机索取一些RID，RID用完后再向RID操作座机索取
  - 需要domain admins权限
- PDC模拟器操作主机
  - 支持旧版客户端
    - 如果域内有windows NT server 4.0 BDC（backup domain controller），它会要求从windows NT 4.0 PDC来复制用户账户和密码数据
    - 如果没有，这ADDS会通过PDC模拟器操作主机来扮演PDC角色
    - 只有当域处于混合模式时，拥有PDC的DC才需要和运行Windows NT 4.0或3.51的BDC保持同步
  - 减少因为密码复制延迟所造成的问题
    - 当用户密码变更后，这个密码会优先被复制到PDC模拟器操作主机，而其他域控制器仍然按照标准复制程序，也就是等待一段时间后才会收到新密码
    - 如果用户登录时，负责验证用户身份的域控制器发现密码不对，它会将验证身份的工作转发给拥有新密码的PDC模拟器操作主机，以便让用户可以登录
  - 负责整个域内时间的同步
    - PDC模拟器默认使用本地计算机的时间，也可以将其设置与外部时间源同步
    - 所有其他域的PDC模拟器主机会自动与林根域的PDC模拟器同步
    - 各个域内其他域控制器都会自动与该域的PDC模拟器同步
    - 域内成员计算机会与验证其身份的域控制器同步
    - 查看时间同步设置
    - 将PDC设置为与外部时间源同步
    - 时间同步使用的协议未SNTP（simple network time protocol），使用UDP 123端口
    - 加域和未加域的机器手动同步时间源
    - 客户端在图形界面设置时间源
  - 防止重写组策略对象GPO的可能
    - 默认情况下，组策略管理单元运行在PDC的DC上，这样可以减少潜在的复制冲突

场景介绍

- 例子1：部署exchange/lync服务器
- 例子2：迁移或升级DC服务器
- 只读域控制器无法扮演操作主机角色

操作主机放置最佳实践

- 基础结构主机放置
  - 所有DC都是GC：基础结构主机与全局编录不兼容。由于全局编录服务器会收到由每一个域所复制来的最新变动数据，故此时由那一台域控制器来扮演基础结构主机都无所谓
  - 只有一个域：若整个林中只有一个域，则基础结构主机不起作用，因为没有其他域对象可供参考，此时不需要理会基础结构主机由哪一台域控制器来扮演
  - 最佳实践：为了方便管理，可以将RID/PDC/基础结构主机放在一台机器上
  - 如果域中有RODC，则PDC必须是2008 R2或者2012R2以上
- PDC模拟器主机放置
  - 最佳实践：PDC所在的主机要求高性能/高稳定，因为PDC经常需要与网络上其他系统沟通，它的负担比其他操作主机都要重
  - 若要降低PDC的负担，可以调整PDC的权重，默认所有DC的权重都是100，默认被客户端定向查找的几率是相同的，可以把PDC调成50，则客户端被定向到这台PDC的概率就会降低，从而降低负担
  - 调整权重的方法
  - 最佳实践：如果网络中旧版系统比较多（windows2000之前版本），则PDC会使用比较多的RID，此时可以将PDC和RID放在一起，提高效率
  - 建议部署在用户集中的站点，能够降低网络流量
- RID主机放置
  - 需要高可用，不需要高性能，RID每次分发给其他DC500个RID
  - 在需要创建大量安全主体的站点上部署RID主控，降低网络连接失败造成的风险
  - 配置RID主控作为备用RID主控的直接复制伙伴，可降低占用主控时因为复制延迟引起的风险
- 林级别主机放置
  - 林中的第一台DC，自动成为架构主机和域命名主机，同时也是GC
  - 对负载要求不高，与GC兼容，可以并置
  - 将这两个角色迁移，也不会改善性能，所以保持原样即可
- 域级别主机放置
  - 每个域的第一台DC自动扮演域级别主机（RID/PDC/基础结构）
  - 林根域的第一台DC，默认扮演五个操作主机角色，两个林级别，三个域级别，同时也是GC
  - 最佳实践：单域环境，林级别放在一台DC，域级别放在一台DC

如何查看操作主机角色

通过图形MMC控制台

- 架构操作主机
  - AD架构控制台
    - regsvr32 schmmgmt.dll注册架构
    - 通过MMC打开AD架构控制台
- 域命名主机
  - AD域和信任关系
- RID操作主机
  - AD用户和计算机
- PDC主机
  - AD用户和计算机
- 基础结构主机
  - AD用户和计算机

通过powershell或cmd

- netdom query fsmo
- Get-ADDomain contoso.com | ft PDCEmulator,RIDMaster,InfrastructureMaster
- Get-ADForest contoso.com | ft SchemaMaster,DomainNamingMaster

转移操作主机角色

自动转移

- 当把扮演操作主机角色的DC降级为成员服务器时，系统会自动将其操作主机转移到另外一台适当的DC
- 建立ADDS域时，系统会自动选择DC放置操作主机

手动转移

- 使用AD用户和计算机转移RID/PDC/基础结构
- 使用AD架构控制台转移架构主机
- 使用AD域和信任关系转移域命名主机
- 利用powershell命令
  - 转移PDC到DC2
    - Move-ADDirectoryServerOperationMasterRole -identity "dc2" -OpertationMasterRole PDCEmulator
  - 转移其他角色
    - 将命令中的PDCEmulator改为RIDMaster/InfrastructureMaster/SchemaMaster/DomainNamingMaster
  - 通过代号转移
    - Move-ADDirectoryServerOperationMasterRole -Identity "DC2" -OperationMasterRole 0,1,2,3,4
    - 0：PDC/1：RID/2：基础结构/3：架构操作主机/4：域命名主机

注意事项

- 转移角色过程中不会有数据损失
- 可以将林级别的架构和域命名主机转移到同一个林中的任何一台DC
- 可以将域级别的RID/PDC转移到同一个域中的任何一台DC
- 基础架构不要和GC放在一起，除非只有一个域或者DC都是GC

占用操作主机角色

- 注意事项
  - 只有在无法转移的情况下，才使用夺取的方法
  - 在占用操作主机之前，确保新的操作主机已经完整接收到从其他DC复制过来的变更数据，新操作主机是根据其内的ADDS数据库来工作的
  - 夺取操作主机后，不要再将原来的操作主机角色的DC上线，否则会出现两台DC都各自认为是操作主机的现象，会影响ADDS的工作，严重情况下会损坏ADDS数据库
- 夺取的方法

操作主机停止服务的影响

- 架构操作主机
  - 对用户没有影响，因为用户不会直接与架构主机通信
  - 对管理员来说，除非他需要访问架构内的数据，例如安装exchange server，否则也暂时不需要使用架构主机
  - 上面两种情况，可以等待架构主机重新上线，不需要占用
  - 如果架构主机长时间停止服务，应该占用到其他DC
- 域命名主机
  - 对用户没有影响
  - 对管理员来说，除非要添加或者删除域，否则暂时也不需要使用域命名主机，等待域命名重新上线即可
  - 如果域命名长时间停止服务，应该占用
- RID主机
  - 对用户没有影响
  - 对管理员来说，除非要在域内新建对象，同时他们所连接DC之前索取的RID已经用完，否则暂时也不需要使用RID主机
  - 如果长时间停止服务，则占用
- PDC主机
  - 对网络登录用户会有影响
    - 旧版客户端因为无法与PDC主机通信而不能修改密码
    - 如果密码已经过期，也会因为无法修改密码，而无法登录
  - 应该尽快修复PDC主机，如果无法在短期内修复，应该占用
  - PDC被占用后，原旧的PDC还可以继续上线，但是因为角色已经被夺取，它会自动放弃PDC的角色
- 基础结构主机
  - 对用户没有影响
  - 对管理员来说，除非他最近移动大量账户或修改大量账户的名称，否则也不会感觉到基础结构主机已经停止服务
  - 基础结构主机被占用后，原旧的基础结构主机还可以继续上线，但是因为角色已经被夺取，它会自动放弃角色
  - 如果长时间离线，可以由其他DC占用，占用的DC不能是GC