



Chapter 10

活动目录的升级

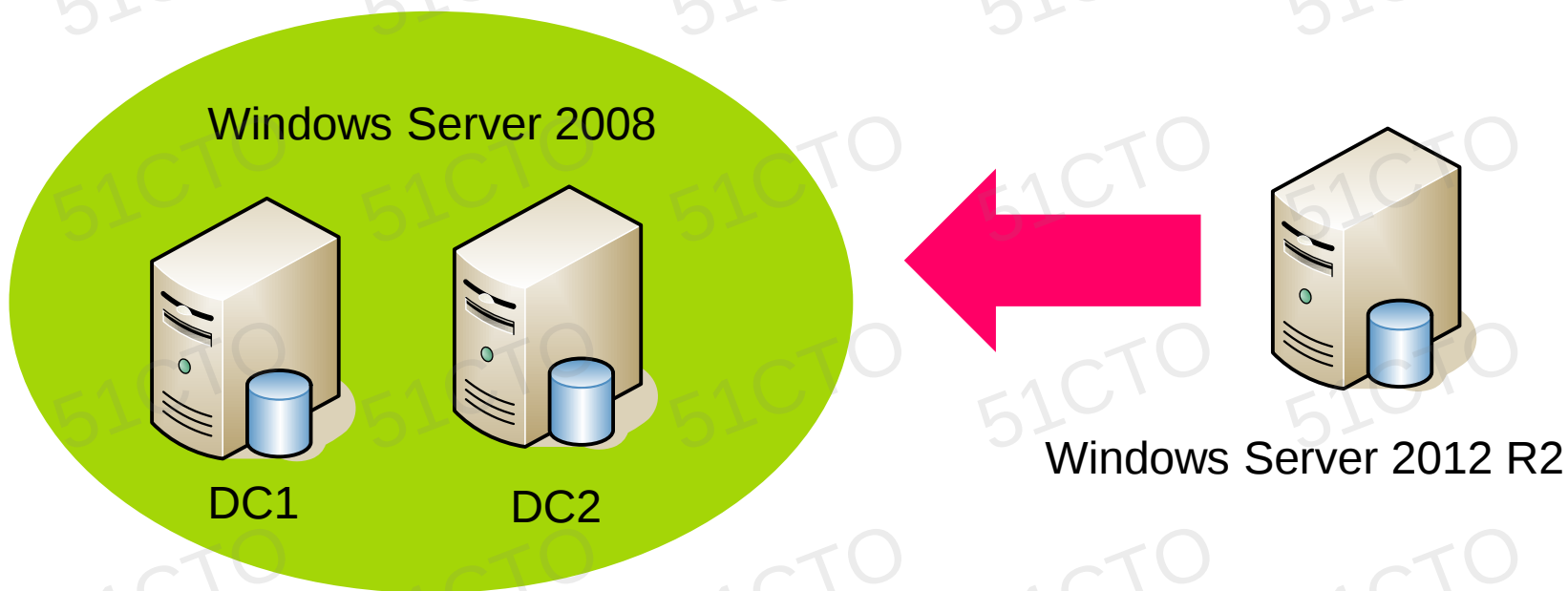
1

域控制器的升级

Domain Server upgrade

需求背景

- 公司现有的域环境中域控制器使用的是旧版本的Windows Server, 如何将域控制器提升为新版本的Windows Server?



林和域的功能级别

- 新的Window Server在AD和域的管理上提供新的Feature,但如果部署在多域和多DC的架构中,由于数据库的同步,必须考虑向下兼容
- 新林和域的功能级别提供了一种标识和属性,以便在数据同步中使新的Windows Server了解需禁用哪些新的Feature
- 功能级别的概念只影响域控制器,对成员服务器和PC终端无影响
- 林或域的功能级别一旦确定后,允许高版本的服务器加入成为域控制器,但不允许低版本的服务器加入成为域控制器

三种升级的方案

就地升级
(In-place upgrade)

摆动迁徙
(Swing Migration)

全新迁徙
(Clean and Pristine C&P)

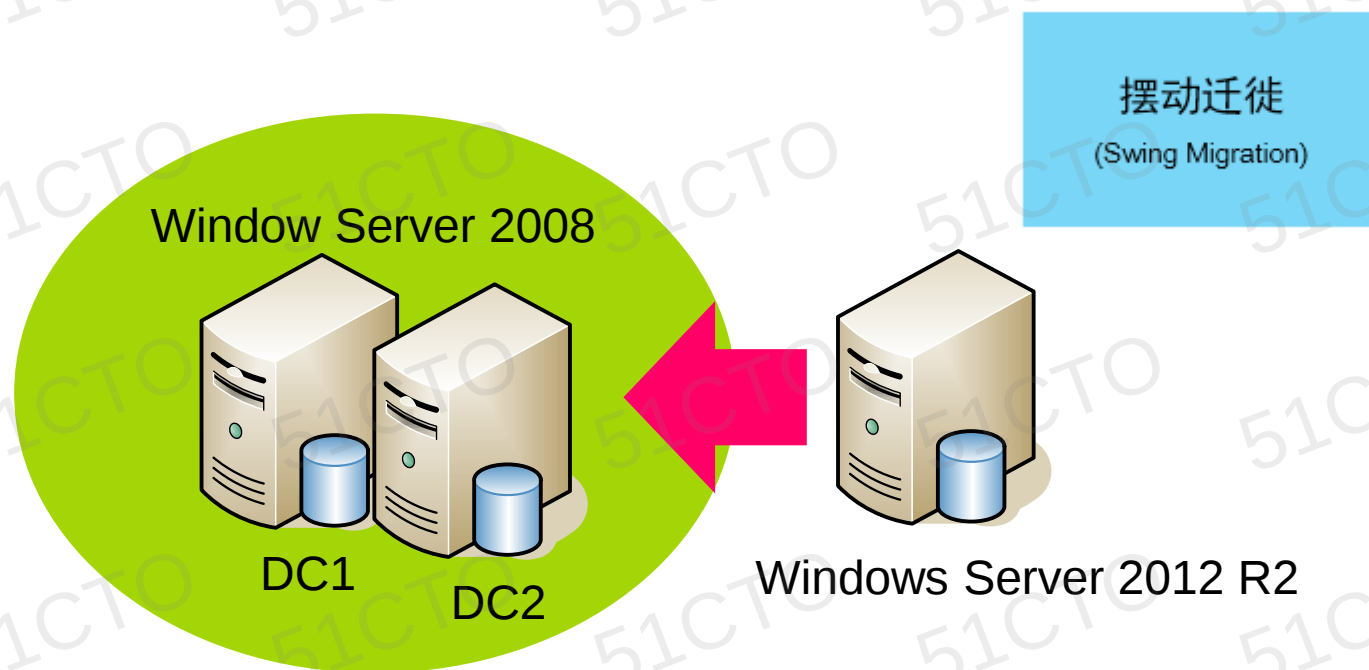
方案1：就地升级

- 操作步骤简单，物理服务器可利旧，但升级路径受限，且升级后结果的不确定性大，升级过程不提供回退
- 适用于小规模的单域控制器的环境或测试场景，可以在做好备份后尝试操作，如有问题及时恢复



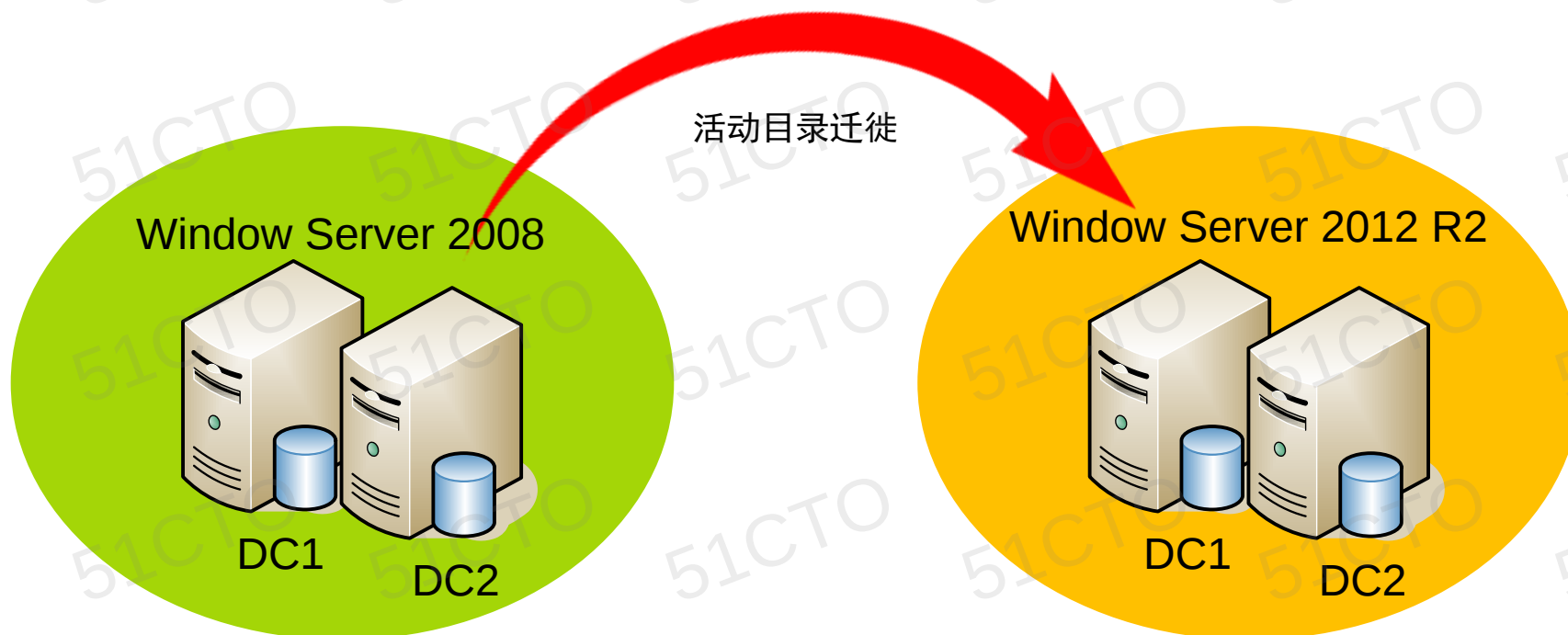
方案2：摆动迁徙

- 将高版本服务器加入域并提升为额外域控制器
- 将FSMO角色及GC功能转移到新的服务器后，陆续将所有旧版本的服务器降域（注意降域的操作步骤），最后提升林和域的功能级别到新版本



方案3：全新迁徙

- 用高版本服务器完全新建一个域（域名需是新名称），并与原有域建立信任关系
- 用专用的域和活动目录迁徙工具将原有域控制器的AD活动目录信息（用户/计算机帐号等）迁徙到新的域中
- 该方式可实现新旧域并存，并解决原有域的垃圾数据问题，适合域的大规模改造



AD迁徙的场景和工具

- AD迁徙的场景

域的升级：例如公司的域控制器需要从低版本升级到高版本

域的合并：例如公司并购，多个子公司原有AD账户需并入到母公司的AD中

域的拆分：例如公司重组，部分AD账户需要划归到新的AD中

- AD迁徙的工具

Active Directory Migration Tool (ADMT)



Domain Migration Administrator



Migration Manager for Active Directory



ADMT 简介

- ADMT (Active Directory Migration Tool) :
 - ADMT是微软的免费迁徙工具
 - AD的账户迁徙是复制操作，如出现问题，旧域中的帐号仍然可用
 - ADMT实施前需要新旧域之间建立信任关系，迁徙后信任关系可保留，账户可两边访问，提供给IT人员逐步迁徙其他共享资源的时间窗口
 - AD迁徙完成后，应实现终端计算机重启后自动加入新域，且保留原有用户的密码

ADMT 注意事项

ADMT工具的目前版本为3.2，暂时不支持Windows Server 2012及以上版本的服务器环境，实施过程中新的目标域需先引入一台Windows server 2008 R2的域控制器作为过渡，将数据迁徙至该过渡域控制器后，再利用AD的自动同步机制将数据复制到新域中的其他域控制器

2

域环境的名称及IP变更

Renaming and IP modification in Domain

域控制器IP修改与重命名

- 修改域控制器的IP地址

- 修改IP后，需停止并重启netlogon服务后，重启并用ipconfig/registerdns强制重新向DNS注册SRV记录，并删除DNS中原有的域控制器记录

- 修改域控制器的主机名

- 重命名后需执行一系列 **netdom** 相关的命令，并删除DNS中原有的域控制器记录

1. netdom computename 新DC主机名 /add 旧DC主机名
2. netdom computename 新DC主机名 /makeprimary 旧DC主机名
3. 重新启动后，输入 netdom computename 旧DC主机名 /remove 新DC主机名

- 如果不是唯一的域控制器，也可以先将域控制器降级为独立服务器（删除“Active Directory 域服务”，删除过程中系统提示降级），然后修改IP或重命名，再重新加入域

域的重命名

- 当域需要重命名时，需要用到域重名工具（**rendom**命令），该命令目前已集成在Windows Server的操作系统中。（执行rendom前需要手工创建新的DNS区域）
- 如果域环境比较复杂（如已部署Exchange, Sharepoint等应用），不建议采用域重命名的方法，而建议采用建新的域并通过数据迁徙的方式实现



本章小结

1

域和活动目录升级

2

域环境中名称及IP变更



Thanks

感谢聆听