



Chapter 7

操作主机（FSMO）

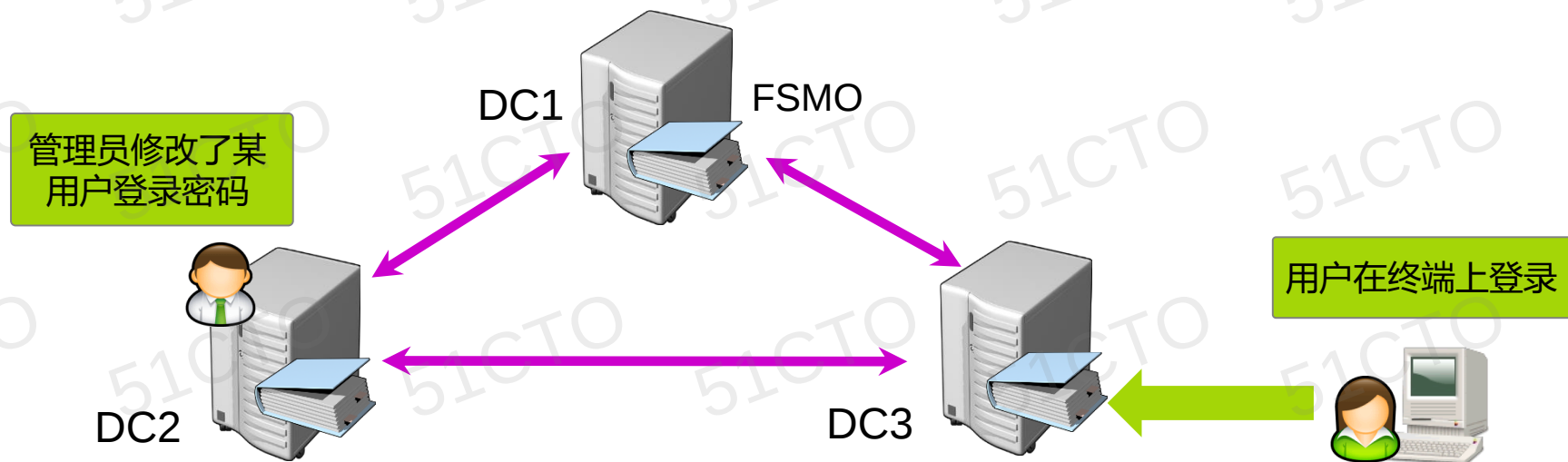
1

操作主机概述

FSMO Overview

什么是操作主机（FSMO）

- 域控制器之间需要同步AD的数据库
 - 大部分的数据同步采用**多主机复制机制**（Multi-master Replication Model）
 - 少部分的数据同步采用**单主机复制机制**（Single-Master Replication Model）
- 操作主机 **FSMO**（Flexible single master operation）即用于这类特殊的单主机复制机制，以满足特殊场景下更高效可控的数据同步（如用户密码修改）



操作主机的角色

- 操作主机是域控制器承担的一种特殊的角色
- 操作主机共有五类（两个林级别，三个域级别），每类一个
- 默认第一台安装的域控制器承担了所有的FSMO角色

林级别

- 架构主机 (Schema Master)
- 域命名主机 (Domain Naming Master)

域级别

- PDC模拟主机 (PDC Emulator Master)
- RID主机 (RID Master)
- 基础结构主机 (Infrastructure Master)

操作主机的作用 (林级别)

架构主机 (Schema Master)

- 负责更新和修改林中所有域中对象的种类和属性，类似数据库字段

域命名主机 (Domain Naming Master)

- 负责控制林中域/子域的添加和删除

操作主机的作用（域级别）

PDC模拟主机（PDC Emulator Master）

- 关键AD数据库信息的优先复制权（如组策略更新、密码更新）
- 整个域的时间同步
- 最重要的FSMO角色，可以理解为主域控制器

RID主机（RID Master）

- 向其他域控制器分配SID中的RID，一次500个（对象SID=域ID+RID）

基础结构主机（Infrastructure Master）

- 负责跨域对象的引用（如用户组包含其他域中的用户），通过GC传递并同步外域更新

操作主机角色的查看

- 命令行方式：**netdom query fsmo**（查询所有的FSMO角色）

```
C:\Windows\system32>netdom query fsmo
架构主机                DC1.ny.com
域命名主机              DC1.ny.com
PDC                    DC1.ny.com
RID 池管理器            DC1.ny.com
结构主机                DC1.ny.com
命令成功完成。
```

操作主机角色的查看

- 图形化方式：

FSMO级别	FSMO角色	FSMO的管理控制台
林级别	架构主机	Active Directory架构
	域命名主机	Active Directory 域和信任关系
域级别	PDC模拟主机	Active Directory 用户和计算机
	RID主机	Active Directory 用户和计算机
	基础架构主机	Active Directory 用户和计算机

2

操作主机的部署

FSMO Deployment

操作主机的部署建议和故障处理

- 林级别的“架构主机”和“域名空间主机”角色建议保留在默认的第一台根域控制器上
- 域级别的三种角色建议最好保留在同一台机器上
- 除了“PDC模拟主机”角色外，其他操作主机角色故障后不会对域的正常工作的域控制器接管相应的角色
- 当操作主机角色所在的域控制器出现故障时，可以通过“转移”或“抢占”等方式让其他正常工作的域控制器接管相应的角色
- 如果不是特别紧急的情况，建议在操作主机角色出现问题时，优先考虑修复原有机。如果是通过“抢夺”方式获得操作主机角色，则原有的机器建议不再上线

操作主机的转移和抢占

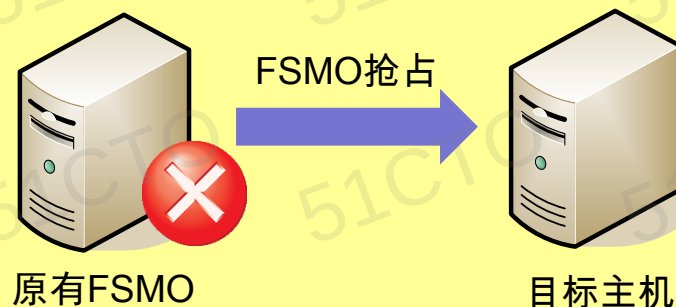
转移 (Transfer)

- “转移”要求原有的操作主机仍处于工作状态
- “转移”操作可以用图形化工具完成

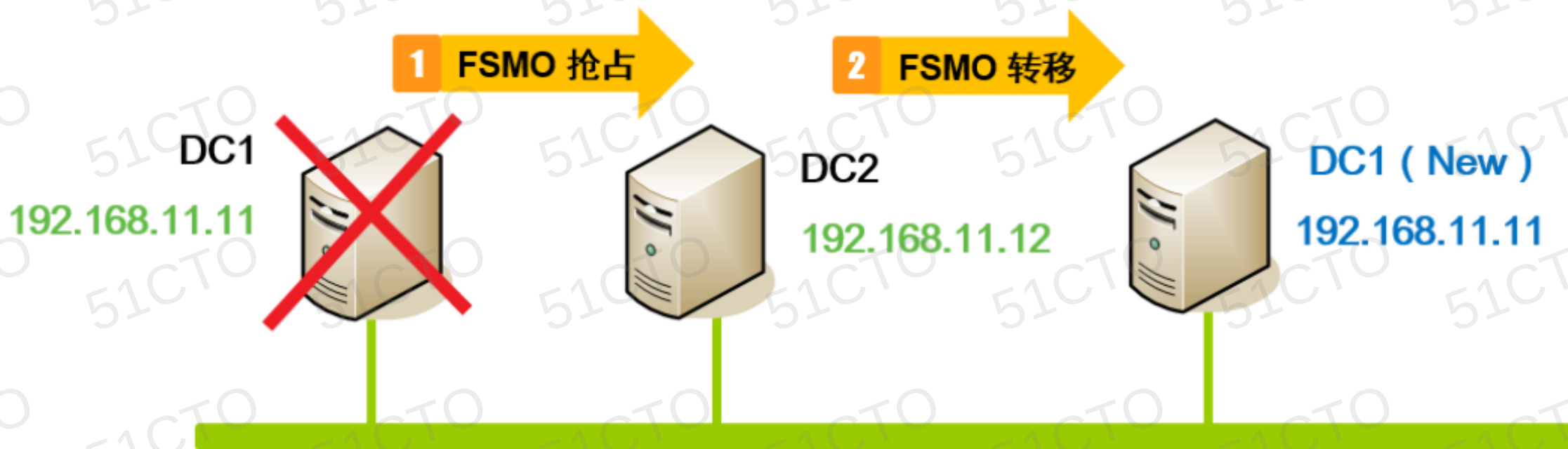


抢占 (Seize)

- “抢占”允许原有的操作主机已处于不在线状态（脱机）
- “抢占”操作只能用命令行完成（**Ntdsutil**命令）



FSMO故障处理演示



本章小结

1

操作主机概述

2

操作主机部署



Thanks

感谢聆听