



Chapter 9

活动目录的备份与维护

1

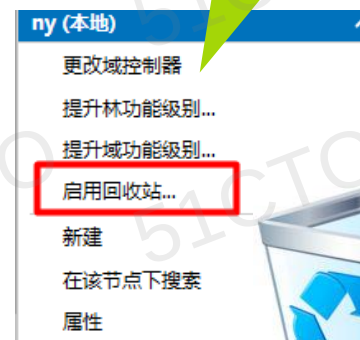
AD的备份与恢复

AD Backup & Recovery

AD回收站

- AD回收站功能默认未启用，需要在“AD管理中心”中启用，一旦启用无法再关闭
- AD回收站功能的启用需要域所在的林功能级别为Windows Server 2008 R2以上
- AD回收站的对象默认保留180天，调整该默认值需要使用Set-ADObject命令
- AD回收站无法恢复在该功能启用前删除的帐号

删掉的AD用户
帐号还能从回收
站恢复出来！



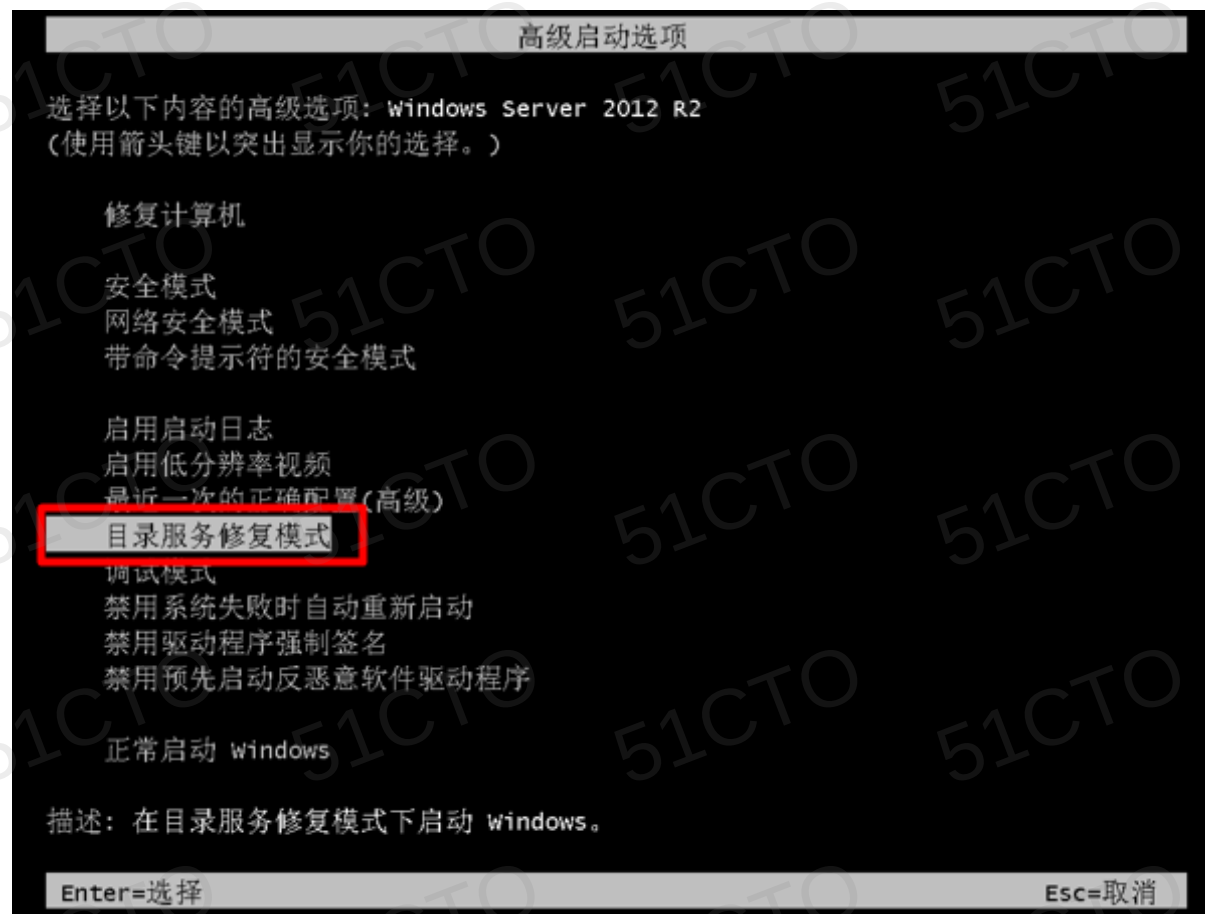
AD活动目录的备份

- 安装Windows Server Backup 工具
- 备份时选择备份项目为“系统状态”
- 备份数据的存放可以是本地硬盘或网络共享文件夹



AD活动目录的恢复 (Window Server Backup)

- 重启按F8进入“目录服务修复”模式
- 系统登录时不能再用域管理员登录，用户名为 .\administrator, 密码安装AD时的配置恢复管理员密码
- 启动Windows Server backup工具，选择恢复“系统状态”，当域中存在多台DC时，需要考虑“授权还原”和“非授权还原”的选项



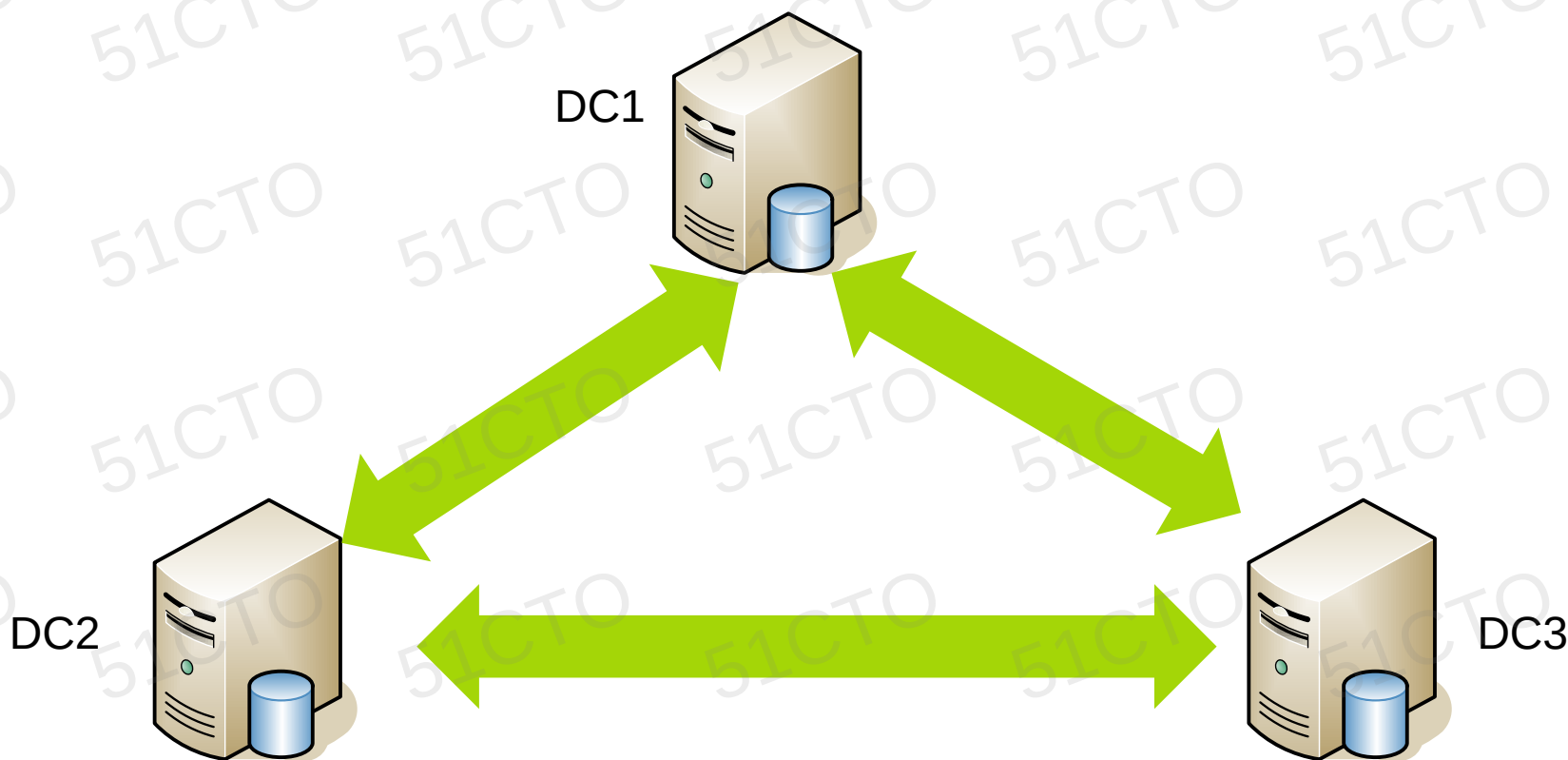
2

AD数据库的维护

Maintain AD Database

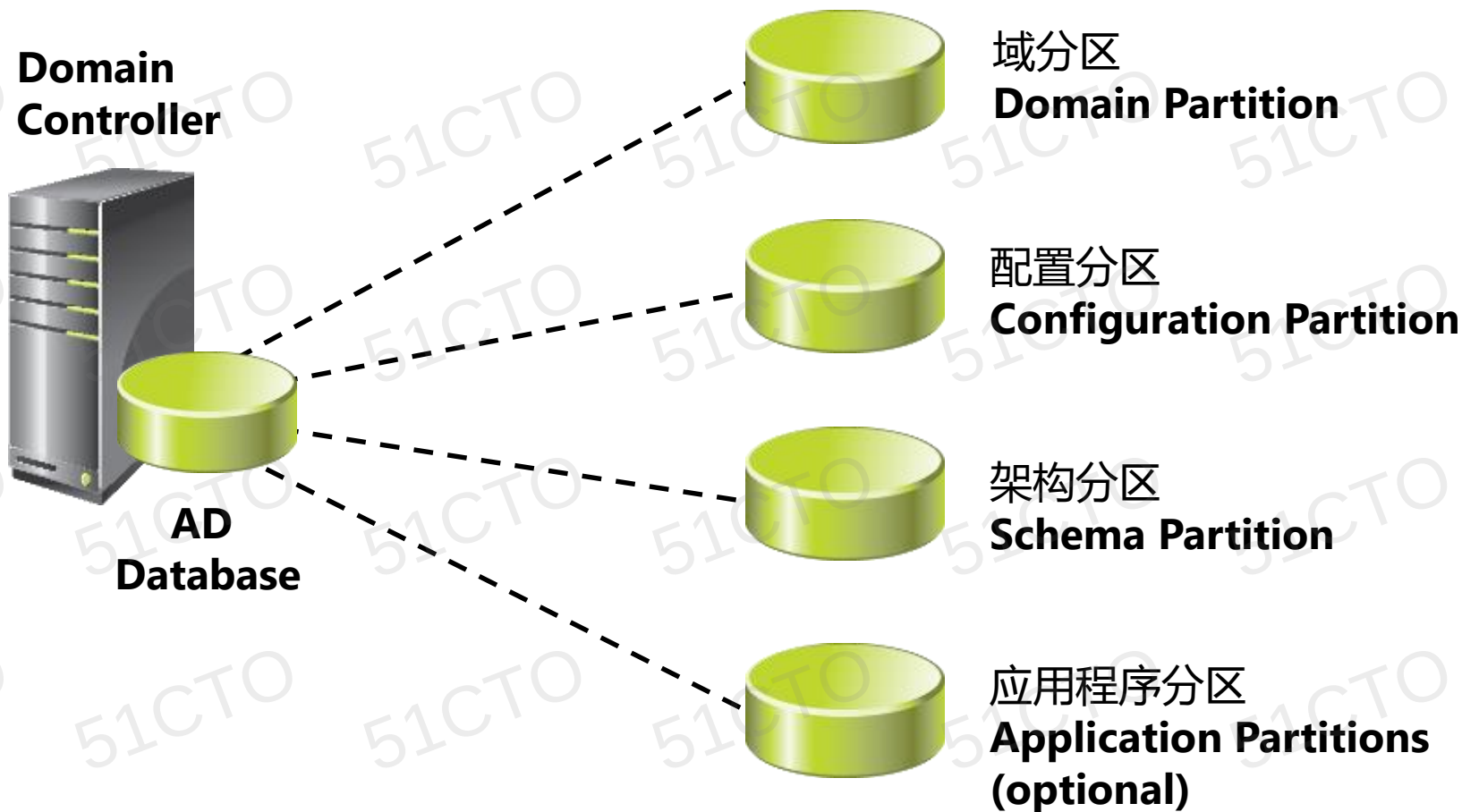
AD数据库的存储与同步

- AD数据库会在每台DC的本地保存，且定时或在发生改变时自动在DC之间相互同步复制，同步复制的频率和时间窗口可以配置和定义
- AD数据库文件默认保存在的C:\Windows\NTDS目录中，主文件为ntds.dit



AD数据库的结构

- AD数据库包含四个分区 (Partition)的数据，不同分区的数据复制和同步的范围不同
- 一个DC中的数据库应至少包含三个分区：本域的域分区，全局的配置分区和架构分区



ADDS服务的启动/停止

- AD数据库维护过程中必要时需进行文件夹重定向、脱机整理等操作，但必须先停止ADDS服务，完成操作后再启动ADDS服务

- 命令行: `net stop ntds , net start ntds`
- Powershell: `stop-service ntds -force , start-service ntds`
- 服务控制台

名称	描述	状态	启动类型	登录为
 Active Directory Domain Services	AD DS 域控制器服务。如果停止此服...	正在运行	自动	本地系统
 Active Directory Web Services	此服务提供指向此服务器上本地运行...	正在运行	自动	本地系统
 App Readiness	当用户初次登录到这台电脑和添加新...		手动	本地系统
 Application Experience	在应用程序启动时为应用程序处理应...		手动(触...	本地系统
 Application Identity	确定并验证应用程序的标识。禁用此...		手动(触...	本地服务
 Application Information	使用辅助管理权限便于交互式应用程...		手动(触...	本地系统
 Application Layer Gateway Service	为 Internet 连接共享提供第三方协议...		手动	本地服务
 Application Management	为通过组策略部署的软件处理安装、...		手动	本地系统
 AppX Deployment Service (AppXSVC)	为部署应用商店应用程序提供基础结...		手动	本地系统
 Background Intelligent Transfer Service	使用空闲网络带宽在后台传送文件。...		手动	本地系统

AD数据库的维护和优化：ntdsutil

Ntdsutil命令集

- 重置AD活动目录还原的管理员密码

```
ntdsutil.exe " set DSRM password "
```

- AD数据库文件的移动

```
ntdsutil.exe "activate instance ntds" files "move db to e:\ntds " quit quit
```

- AD数据库的离线整理优化

```
ntdsutil.exe "activate instance ntds" files "compact to c:\ " quit quit
```

- 修复活动目录数据库

```
ntdsutil.exe "activate instance ntds" "semantic database analysis" "verbose on" "go  
fixup" quit quit
```

- 清除与AD相关的垃圾文件

```
Ntdsutil "metadata cleanup" "remove selected server <ServerName>"
```

3

文档维护与健康巡检

Documenting and Health Check

域环境文档

域环境文档应包含版本号，定期更新并标明每次修订的具体时间和内容

- 林和域的整体架构（域的数量、层次、名称）
- 网络部署和站点规划（物理/逻辑拓扑图）
- 域控制器列表（域控制器数量、操作系统、IP地址等）
- 特殊域控制器（RODC、GC）和操作主机（FSMO）角色分布
- DNS服务器列表（DNS数量、Zone的分布等）
- OU规划及用户/计算机命名原则
- 用户和计算机数量清单（OU归属、操作系统、IP地址等）
- 共享资源目录及权限列表（共享文件夹、打印机等）
- 组策略配置及部署日志
- 关键的管理员帐号分配及职责说明



日常健康巡检

健康巡检建议配合操作文档并写明具体操作步骤, 部分任务可编写为脚本

- 域控制器的网络连通性检查 (用ping, telnet, 官方检查工具PortqryUI)
- 域控制器的性能情况检查 (CPU, 内存、磁盘空间)
- AD相关核心服务检查 (如ADDS,DNS,Server,KDC, Netlogon等服务)
- AD相关的默认共享检查 (用Net share命令)
- DNS中SRV记录及其他记录解析检查
- FSMO角色状态检查 (用netdom query FSMO)
- AD数据库状态检查 (文件大小、错误日志等)
- AD数据库复制状态检查 (用Repadmin命令)
- BPA最佳实践分析程序



AD诊断的专业工具：DcDiag

Dcdiag -e >c:/dcdiag.txt 可重定向导出

- Dcdiag诊断内容包括：

- 连通性
- 复制
- 拓扑完整性
- 登录权
- DC位置
- 安全边界
- FSMO角色
- DNS

```
Domain Controller Diagnosis

Performing initial setup:
  Done gathering initial info.

Doing initial required tests

  Testing server: Default-First-Site-Name\RESKIT-DC1
    Starting test: Connectivity
    ..... RESKIT-DC1 passed test Connectivity

Doing primary tests

  Testing server: Default-First-Site-Name\RESKIT-DC1
    Starting test: Replications
    ..... RESKIT-DC1 passed test Replications
    Starting test: NCSecDesc
    ..... RESKIT-DC1 passed test NCSecDesc
    Starting test: NetLogons
    ..... RESKIT-DC1 passed test NetLogons
    Starting test: Advertising
    Fatal Error:DsGetDcName (RESKIT-DC1) call failed, error 1722
    The Locator could not find the server.
    ..... RESKIT-DC1 failed test Advertising
    Starting test: KnowsOfRoleHolders
    ..... RESKIT-DC1 passed test KnowsOfRoleHolders
    Starting test: RidManager
    ..... RESKIT-DC1 passed test RidManager
    Starting test: MachineAccount
    ..... RESKIT-DC1 passed test MachineAccount
    Starting test: Services
    NETLOGON Service is stopped on [RESKIT-DC1]
    ..... RESKIT-DC1 failed test Services
    Starting test: ObjectsReplicated
    ..... RESKIT-DC1 passed test ObjectsReplicated
    Starting test: frssysvol
    ..... RESKIT-DC1 passed test frssysvol
    Starting test: kccevent
    ..... RESKIT-DC1 passed test kccevent
```

4

第三方AD管理工具

3rd Party AD Management Tools

ManageEngine的产品

<http://demo.admanagerplus.com>

AD域管理

ADManager Plus

轻松执行各项复杂的AD域管理工作；
批量创建、管理和删除AD对象；
指派操作权限，降低帮助台负荷；
提供丰富的AD报表，满足合规性审计需要。

<http://demo.adselfserviceplus.com>

AD域用户自助服务

ADSelfService Plus

为用户提供的自助服务门户，便于重置密码、解锁账户和更新个人信息；
有效缓解帮助台符合并降低安全风险；
通过邮件或短信自动通知用户密码即将到期；
提供手机App。

<http://demo.adauditplus.com>

AD变更审计与报表

ADAudit Plus

跟踪所有AD对象，包括用户、组、计算机、GPO以及组织单元的变更；
审计Windows文件服务器，记录文件的创建、更改与删除操作；
监控用户的登录和退出，包括每一次登录成功和失败；
提供150多种审计报表。

<http://demo.recoverymanagerplus.com>

AD备份与恢复

RecoveryManager Plus

自动备份AD域对象的变更；
轻松恢复到正确配置版本；
提供AD回收站，一键还原删除的对象和属性；
全面记录历史版本。

本章小结

1

AD的备份和恢复

2

AD数据库的维护

3

文档维护和日常巡检

4

第三方AD管理工具



Thanks

感谢聆听