Microsoft

Chapter 3

活动目录中的对象管理

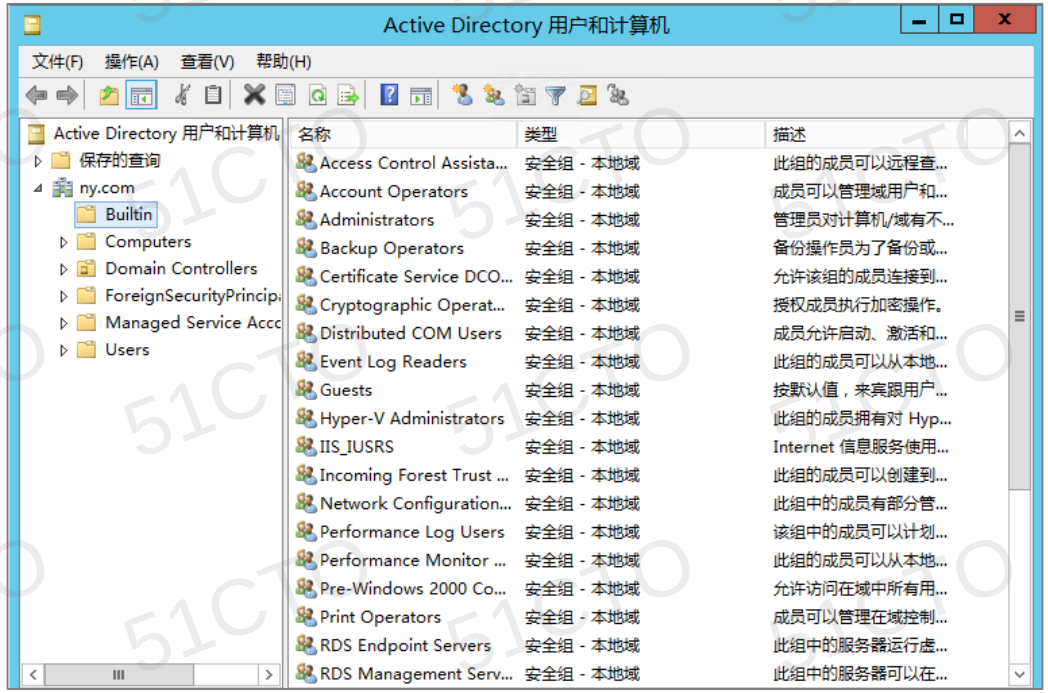
Microsoft

1 活动目录对象管理工具

AD Objects Management Tools

图形化管理工具

- Active Directory 用户和计算机



- Active Directory 管理中心

命令行管理工具

- DS 系列命令集
  - dsquery、dsadd、 dsmod、 dsmove、 dsrm 等
- Powershell 系列命令集
  - Get-ADDomain、 New-Aduser、 Search-ADAccount 等

举例：用 Powershell 创建AD用户账户

```
New-aduser
-name "hr01"
-userprincipalname "hr01@ny.com"
-accountpassword (ConvertTo-SecureString -AsPlainText "123.com" -Force)
-Path "ou=hr,dc=ny,dc=com"
-enabled $true
```

AD管理中心的“Powershell历史记录”功能可用于学习和熟悉命令的语法

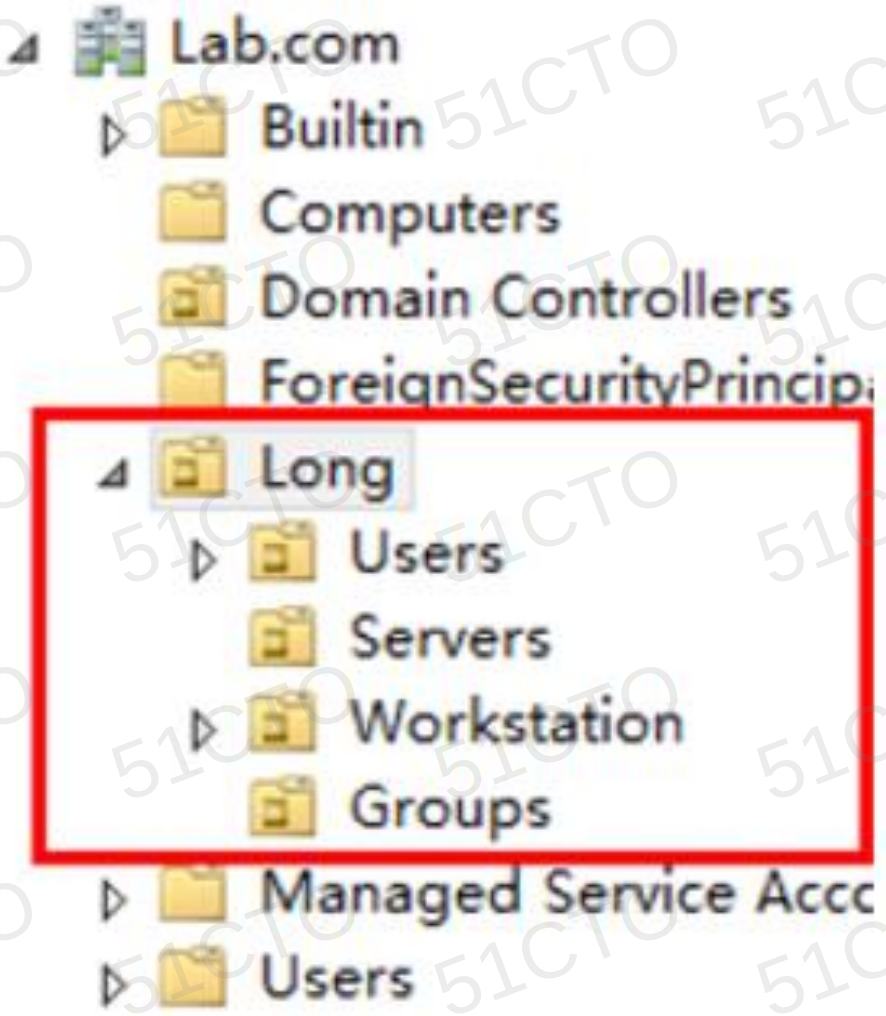
Microsoft

2 活动目录中的对象

Objects in Active Directory

活动目录中的术语

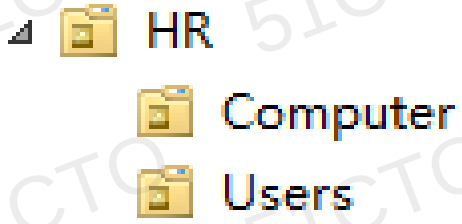
- 对象（Objects）
  - 常见的对象类型包括：用户、组、计算机等
- 容器（Container）
  - 系统内置，是部分对象的默认逻辑存放位置
  - 不能删除或编辑，无法进一步层次化
- 组织单位（OU）
  - 用户创建，用于自定义对象的逻辑存放位置
  - 支持层次化结构、允许编辑



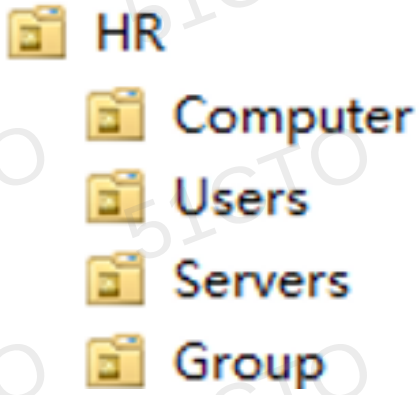
OU（组织单位）的规划

- OU一般需体现企业组织架构或地理特征
- OU中的对象类型是否混合取决与管理的需要
- OU的主要作用是控制组策略部署范围和活动目录的管理权限委派

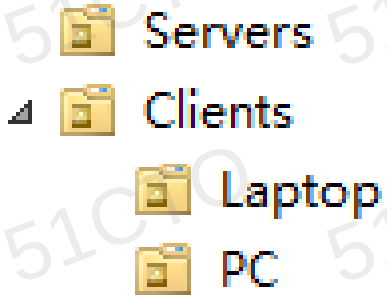
Example 1



Example 2



Example 3



对象类型1：用户

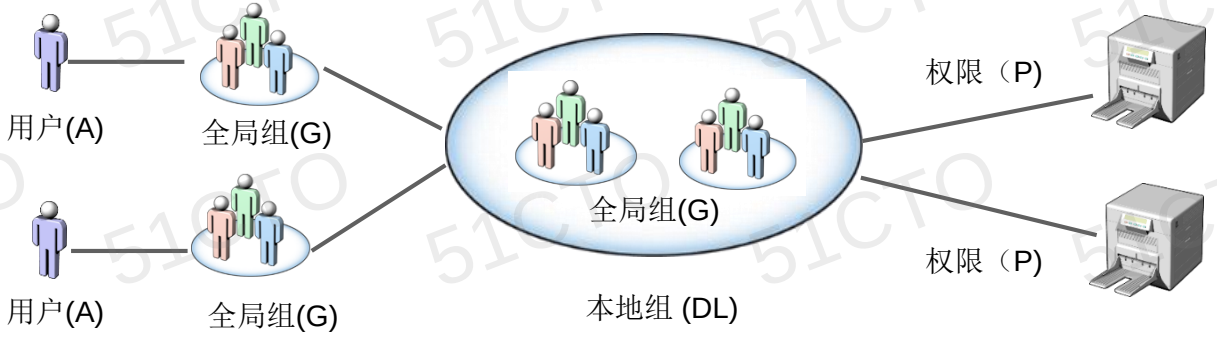
- 域用户的登录
  - 域用户名@域名　　（如 tester@abc.com）
  - 域名\域用户名　　（如 abc\tester）
- 用户单个用户的创建和管理方式：
  - AD用户和计算机
  - AD管理中心
- 批量用户的创建和管理方式：
  - 服务器内置命令行工具（如csvde和ldifde）
  - 编写Powershell脚本

理解 SID

- 域中每个对象都有全局唯一的安全标识符(Security Identifier)
- 用户重命名不会影响SID
- 删除账户后重建与之前相同的用户名的账户，会使用不同SID
- 建议删除账户先将账户禁用一段时间，并移入专门的OU以便管理

对象类型2：组

- 组的用途：批量设置用户的权限(Permission) 或者 权利（Right)
- 组的分类：
  - 按是否内置： 内置组、自定义组
  - 按作用范围： 本地组、全局组、通用组
- 组的规划建议：
  - AGDLP原则： 基于资源规划本地组，基于组织行政架构规划全局组



对象类型3：计算机

- 计算机被动加域：
  - 活动目录中事先未创建计算机帐号，加域后计算机账户自动保存在默认的Computer容器中
- 计算机主动加域：
  - 活动目录中事先已由管理员在指定的OU中创建好计算机帐号，加域后将根据对应的计算机关联事先创建在指定的OU中的计算机账户

提问

哪些用户有权限将计算机加域？如何控制？

计算机账户密码 / 安全通道

- 加入域的计算机与域控制器之间通讯的安全通道（Secure Channel)建立需要密码，由客户端计算机本地生成后上传到域控制器的活动目录中保存，默认每隔30天自动更换该密码

- 如果客户端计算机超过30天未能和域控制器通信，则域控制器允许使用之前保存在活动目录中上一次已过期的计算机账户密码维系安全通道，但时间最多不能超过两个密码更新周期（默认最长60天），否则安全通道将被破坏，客户端将自动脱域，导致用户无法登录

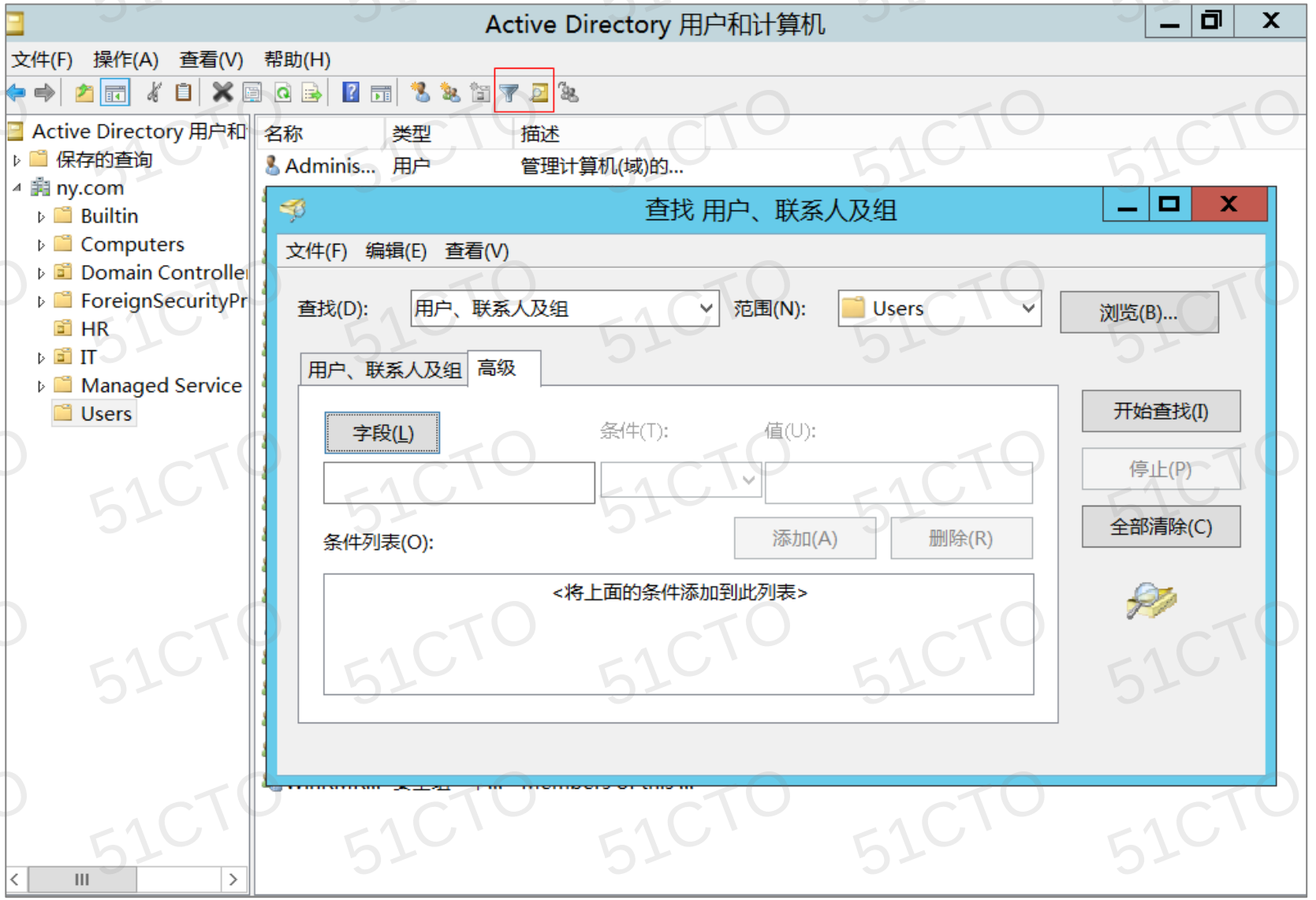
- 计算机密码的更新周期和有效性等参数可通过组策略调整

Microsoft

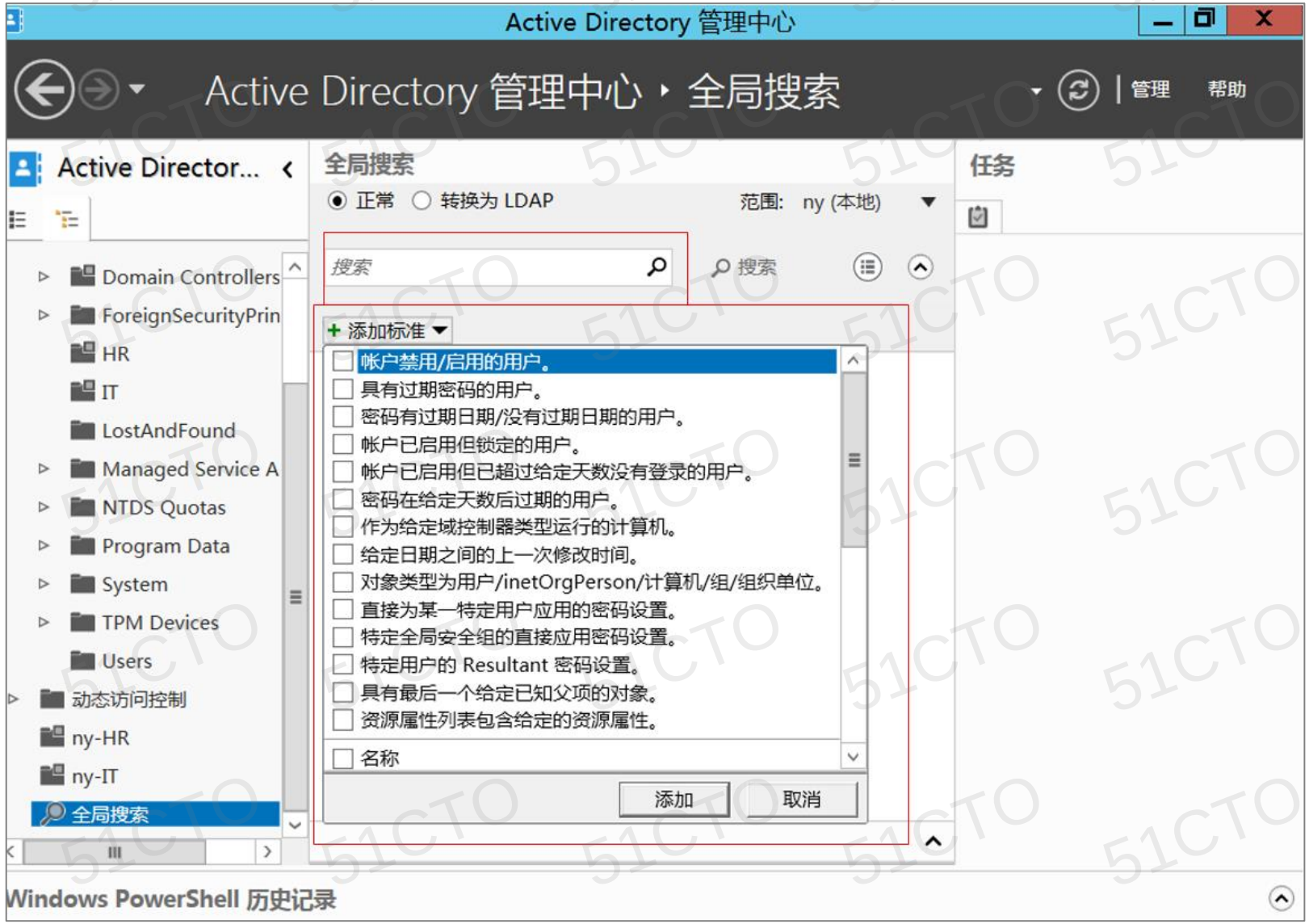
3 对象的筛选和查找

AD Object Filter and Search

手段1：Active Directory 用户和计算机



手段2：Active Directory 管理中心



手段3：DS系列命令

- dsquery命令可以按多种筛选条件查询活动目录中各类对象

```
dsquery computer     - 查找目录中的计算机
dsquery user         - 查找目录中的用户
dsquery group        - 查找目录中的组
dsquery ou           - 查找目录中的组织单位
dsquery site         - 查找目录中的站点
dsquery server       - 查找目录中的 AD DC
dsquery *            - 查找目录中的任何对象
```

- dsquery命令的结果通过管道输出，可作为其他DS命令的输入（dsmod,dsrm等）

举例： 查找超过4个星期处于未活动状态的计算机并从活动目录中删除

dequery computer –inactive 4 | dsrm

手段4：PowerShell命令或脚本

- 例1： 找出长时间（如90天）未被登录的计算机

PowerShell

```
# Gets time stamps for all computers in the domain that have NOT logged in since after specified
  date
# Mod by Tilo 2013-08-27
import-module activedirectory
$domain = "domain.mydom.com"
$DaysInactive = 90
$time = (Get-Date).Adddays(-($DaysInactive))

# Get all AD computers with lastLogonTimestamp less than our time
Get-ADComputer -Filter {LastLogonTimeStamp -lt $time} -Properties LastLogonTimeStamp |

# Output hostname and lastLogonTimestamp into CSV
select-object Name,@{Name="Stamp"; Expression={[DateTime]::FromFileTime($_.lastLogonTimestamp)}} | export-
csv OLD_Computer.csv -notypeinformation
```

- 例2： 将CSV文件中列出的用户账户移动到指定的OU

PowerShell

```
# Import CSV
$MoveList = Import-Csv -Path "C:\Temp\Acc_MoveList.csv"
# Specify target OU.This is where users will be moved.
$TargetOU = "OU=SWC_Users,OU=VA,DC=TekPros,DC=com"
# Import the data from CSV file and assign it to variable
$Imported_csv = Import-Csv -Path "C:\temp\Acc_MoveList.csv"

$Imported_csv | ForEach-Object {
        # Retrieve DN of User.
        $UserDN    = (Get-ADUser -Identity $_.Name).distinguishedName
        Write-Host " Moving Accounts ..... "
        # Move user to target OU.
        Move-ADObject    -Identity $UserDN    -TargetPath $TargetOU

 }
 Write-Host " Completed move "
 $total = ($MoveList).count
 Write-Host "    $total accounts have been moved succesfully..."
```

去哪里找Powershell脚本资源

- 访问 Technet资源库
  - https://gallery.technet.microsoft.com

Microsoft

TechNet 面向 IT 专业人员的资源

- 根据主题分类或关键字寻找完成任务的脚本:

（1）显示指定用户最后登录的时间（last login time)

（2）显示域中当前所有在线的计算机 （Online computers)

（3）……

- 执行脚本

方式1：在ISE调试环境中粘贴脚本代码后执行

方式2：在Powershell命令行下输入 ISE .\xxxxx.ps1

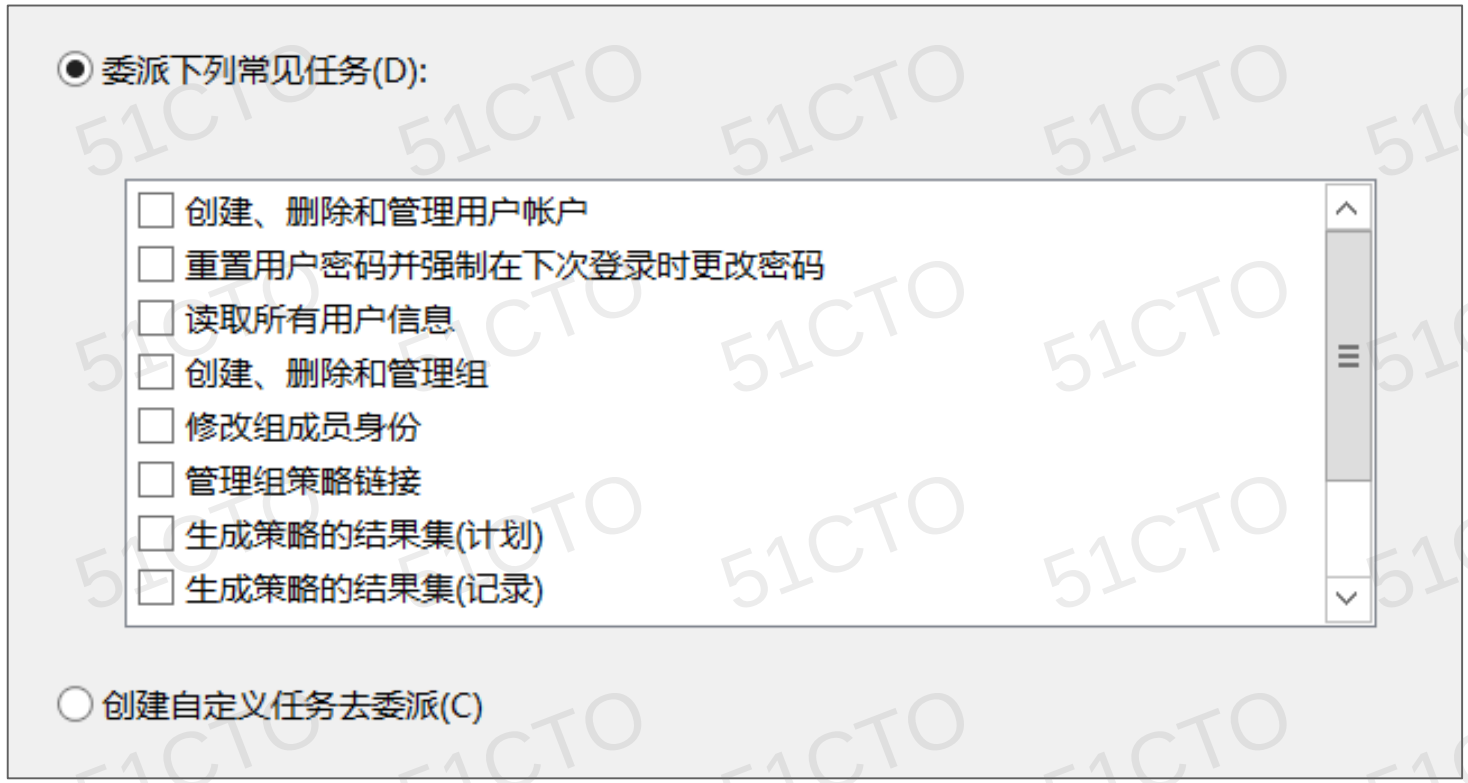
Microsoft

4 AD管理的权利委派

AD Management Delegation

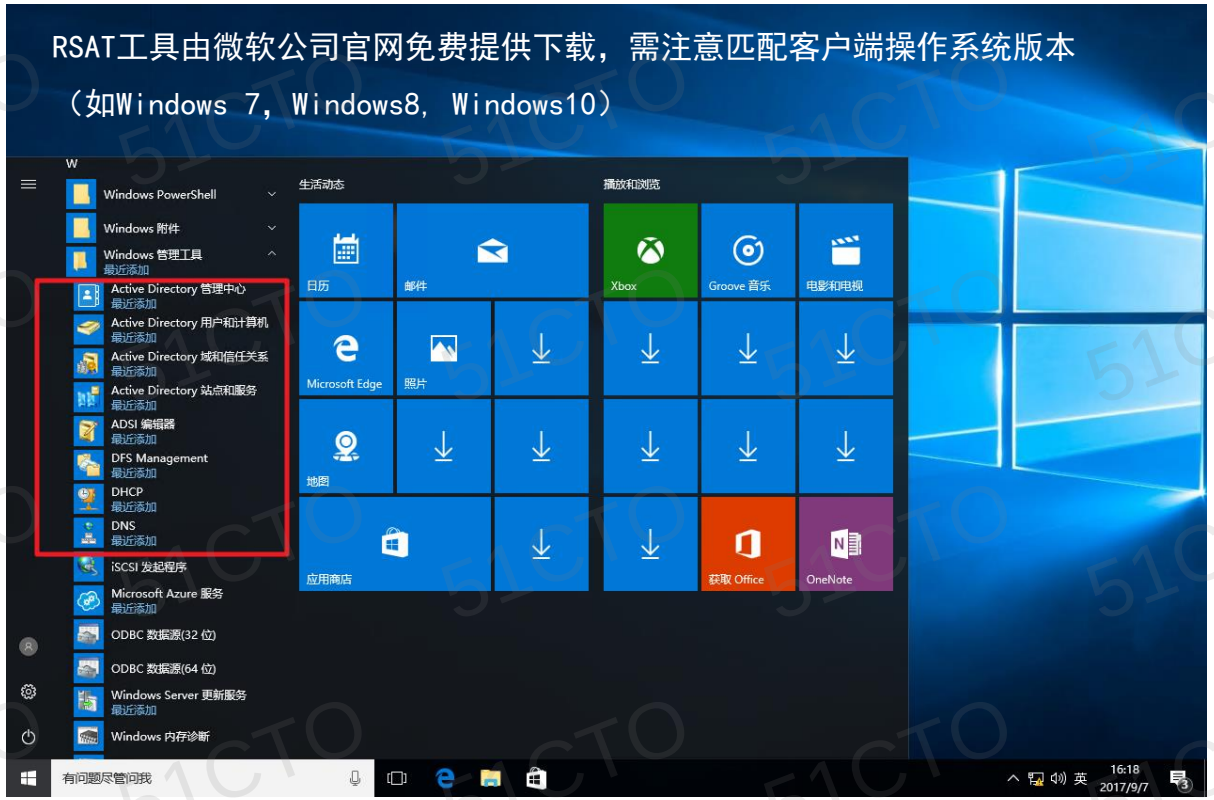
AD管理的权利委派

- 对AD的操作委派可以在OU层面配置，以分配对该OU内对象的常见管理任务给指定的用户或组，减轻域管理员工作负荷（比如修改部门账户的属性，解除帐号锁定，重置账户密码等）



RSAT 工具

- RSAT（Remote Server Administration Tool) 可配合AD权利委派，用于在客户端操作系统上进行AD域服务的远程操作（如重置密码，解禁密码等）



- Active Directory 域服务（ADDS) 工具
- Active Directory 证书服务工具
- DHCP服务器工具
- DNS服务器工具
- 文件服务器工具
- 组策略管理工具
- 网络策略和访问服务工具
- 故障转移群集工具
- Windows 系统资源管理器工具
- .....

本章小结

1. ADDS管理工具介绍
2. 管理活动目录中的对象
3. AD对象的筛选和查找
4. AD管理的权利委派

Microsoft

Thanks

感谢聆听