5000个域用户怎么管理?

PowerShell几分钟搞定 AD 日常运维

在很多企业里，Active Directory（AD）已经运行了十几年。从员工账号管理，到电脑统一管理，再到ERP、MES、OA、PLM等系统的身份认证，AD几乎已经成为企业IT基础设施的重要组成部分。但我发现一个有趣的现象：很多IT工程师每天都在管理AD，却依然习惯：

- ??“AD??????”
- ??????????OU?
- ???????
- ????????
- ????????

人数少的时候问题不大。当企业规模达到：

- 1000???
- 5000???
- ?????

再继续靠鼠标运维，效率就会越来越低。这时候，PowerShell的价值就体现出来了。同样是账号管理，手工操作可能需要半天，PowerShell往往只需要几行命令。

例如：

- ??????
- ????????
- ???????
- ????????
- ?????????
- ????????

这些原本需要数小时完成的工作，几分钟就能处理完毕。

本篇文章结合实际运维经验，整理了**AD管理员最常用的PowerShell命令**

0. 准备工作

```
# 导入 AD 模块（PowerShell 7 需显式导入）
Import-Module ActiveDirectory

# 指定域控执行（避免连到非预期 DC）
Get-ADUser -Identity zhangsan -Server DC01.contoso.com
```

1. 用户管理

```
# 查询单个用户及属性
Get-ADUser -Identity zhangsan -Properties *

# 查找已禁用 / 已过期账户
Get-ADUser -Filter {Enabled -eq $false} -Properties whenChanged
Get-ADUser -Filter {AccountExpirationDate -lt (Get-Date)}

# 查找最近未登录账户（90天未登录）
$cutoff = (Get-Date).AddDays(-90)
Get-ADUser -Filter {lastLogonTimestamp -lt $cutoff} -Properties lastLogonTimestamp |

@{n='LastLogon';e={[datetime]::FromFileTime($_.lastLogonTimestamp)}}

# 新建用户
New-ADUser -Name "张三" -SamAccountName "zhangsan" -UserPrincipalName
"zhangsan@contoso.com" `
            -Path "OU=员工,DC=contoso,DC=com" -AccountPassword (ConvertTo-SecureStri
"P@ssw0rd!" -AsPlainText -Force) `
                                                -Enabled $true

# 启用 / 禁用 / 解锁
Enable-ADAccount zhangsan
Disable-ADAccount zhangsan
Unlock-ADAccount zhangsan

# 重置密码
Set-ADAccountPassword -Identity zhangsan -NewPassword (ConvertTo-SecureString
"NewP@ss!" -AsPlainText -Force) -Reset
Set-ADUser -Identity zhangsan -ChangePasswordAtLogon $true

# 下次登录强制改密

# 移动用户 / 删除（先禁用再删）
Move-ADObject -Identity "CN=zhangsan,OU=员工,DC=contoso,DC=com" -TargetPath "OU=离职
,DC=contoso,DC=com"
Remove-ADUser zhangsan -Confirm
```

2. 组管理

```
Get-ADGroup -Filter * -Properties Description
Get-ADGroupMember ”Domain Admins” -Recursive

# 递归查看成员
Add-ADGroupMember -Identity ”Domain Admins” -Members zhangsan
Remove-ADGroupMember -Identity ”Domain Admins” -Members zhangsan -Confirm
# 查看用户属于哪些组
Get-ADPrincipalGroupMembership zhangsan
```

3. 计算机账户

```
Get-ADComputer -Filter {Enabled -eq $false}
# 查停用计算机
Get-ADComputer -Identity WS001 -Properties LastLogonDate, OperatingSystem
# 清理失效计算机（30天未登录）
$cutoff = (Get-Date).AddDays(-30)
Get-ADComputer -Filter {LastLogonDate -lt $cutoff} | Remove-ADComputer -Confirm
```

4. 密码策略与锁定排查

```
# 默认域密码策略
Get-ADDefaultDomainPasswordPolicy
Set-ADDefaultDomainPasswordPolicy -MaxPasswordAge 90 -MinPasswordLength 12
# 排查账户锁定来源（核心：查 4740 事件）
$user = ”zhangsan”
Get-WinEvent -LogName Security -FilterXPath ”*[System[EventID=4740]]” -MaxEvents 20 |

Where-Object { $_.Properties[0].Value -eq $user } |
Select-Object TimeCreated, @{n='Source';e={$_.Properties[1].Value}} | Format-Table -
Auto
```

5. 复制与域控健康（日常必查）

```
# 复制汇总（最常用，一行看出全林复制状态）
repadmin /replsummary
# 单台 DC 入站/出站复制
repadmin /showrepl DC01
repadmin /queue DC01
# 强制立即复制
repadmin /syncall /AdeP
# 域控健康检查
dcdiag /v
dcdiag /test:replications
dcdiag /test:dns
# PowerShell 版复制状态
Get-ADReplicationPartnerMetadata -Target DC01 -Partition '*' -PartnerType Both |
    Select-Object Server, Partner, LastReplicationSuccess, ConsecutiveFailureCount
```

6. FSMO 角色

```
Get-ADDomainController -Filter * | Select-Object Name, Domain, OperationMasterRoles
Move-ADDirectoryServerOperationMasterRole -Identity DC02 -OperationMasterRole
SchemaMaster
# 或者用传统命令查看
netdom query fsmo
```

7. DNS 管理

```
Clear-DnsServerCache -ComputerName DC01
Get-DnsServerResourceRecord -ZoneName ”contoso.com” -Name ”web” -RRType A
Add-DnsServerResourceRecordA -ZoneName ”contoso.com” -Name ”web” -IPv4Address 10.0.0.10
Remove-DnsServerResourceRecord -ZoneName ”contoso.com” -RRType A -Name ”web” -Force
Get-DnsServerZone -ComputerName DC01

# 查看所有区域
Get-DnsServerDiagnostics | Select-Object EnableLoggingForQuery,
EnableLoggingForZoneTransfer
# 查看 DNS 记录变更
```

```
dnscmd DC01 /enumrecords contoso.com /continue
```

8. GPO 组策略

```
Get-GPO -All | Select-Object DisplayName, Owner, ModificationTime
Get-GPOReport -Name "默认域策略" -ReportType HTML -Path "C:\temp\gpo.html"

# 导出报告
Backup-GPO -Name "默认域策略" -Path "C:\backup\gpo"

# 备份
New-GPO -Name "禁用U盘" | New-GPLink -Target "OU=员工,DC=contoso,DC=com"

# 建策略并链接
# 强制刷新（客户端执行）
gpupdate /force
# 查看某机器生效的策略结果
gpresult /r /scope computer
```

9. 时间同步（域控时间错乱会直接导致 Kerberos 认证失败）

```
w32tm /query /status

# 查看同步状态
w32tm /query /source

# 查看时间源
w32tm /config /manualpeerlist:"ntp.aliyun.com,0x1" /syncfromflags:manual /update

# 改时间源
w32tm /resync

# 立即同步
Restart-Service w32time

# 重启时间服务
```

10. 站点与子网

```
Get-ADReplicationSite -Filter * | Select-Object Name, Options, SiteObjectBL
Get-ADReplicationSubnet -Filter *
New-ADReplicationSite -Name ”Shanghai-Site”
New-ADReplicationSubnet -Name ”10.10.0.0/24” -Site ”Shanghai-Site”
```

11. 日志与审计（常见事件 ID）

```
# 4740 账户被锁、4720 新用户、4732 加组、4724 改密码、4768 Kerberos 请求
Get-WinEvent -LogName Security -MaxEvents 1000 -FilterXPath ”*[System[EventID=4720]]”
|
Select-Object TimeCreated, @{n='User';e={$_.Properties[0].Value}}
# 查域控 DNS/系统错误日志
Get-EventLog -LogName System -EntryType Error -Newest 50 | Where-Object {$_.Source -
match 'DNS|NETLOGON|NTDS'}
```

12. 日常巡检脚本骨架

```
$report = @()
# 1. 复制状态
$report += repadmin /replsummary | Out-String
# 2. 无法登录的账户（密码过期）
$report += ”`n=== 密码快过期/已过期的账户 ===”
$report += Get-ADUser -Filter {Enabled -eq $true} -Properties msDS-
UserPasswordExpiryTimeComputed |
Where-Object { $_.msDS-UserPasswordExpiryTimeComputed -ne $nu
[datetime]::FromFileTime($_.msDS-UserPasswordExpiryTimeComputed) -lt (Get-
Date).AddDays(7) } |
Select-Object SamAccountName, @{n='Expiry';e={[datetime]::FromFileTime
UserPasswordExpiryTimeComputed)}} | Out-String
# 3. 时间同步
$report += ”`n=== 时间状态 ===”
$report += w32tm /query /status | Out-String
$report | Out-File ”C:\temp\dc_audit_$(Get-Date -Format yyyyMMdd).txt”
```

几点实用建议：

- ? `Import-Module ActiveDirectory`?PowerShell 5.1?Windows ???? 7 ????????????? 5.1?
- ??????????? 4740 ? `Caller Computer Name`??????
- ??????? 3 ????复制失败 ?repadmin??时间偏移 ?w32tm??账户大量锁定 ?4740 ????

PowerShell不仅仅是一门脚本语言，更是一名 Windows

运维工程师迈向自动化运维的必经之路。学会它之后，你会发现：

以前需要半天完成的工作，现在可能几分钟就能搞定；

以前需要熬夜处理的任务，现在可能定时脚本就能自动完成。

后续我还会持续分享：

- PowerShell自动化运维实战
- Active Directory最佳实践
- Windows Server运维技巧
- Exchange管理命令大全
- DNS与 DHCP故障排查
- □□□□□□□□□
- AD与 ERP、OA、企业微信统一身份认证实践

欢迎关注本公众号 。我会持续分享 **20**

多年制造业信息化实践中的真实经验、技术干货与避坑指南。让技术少走弯路，让数字化真正创造价值

。

Revision #3
Created 2026-08-29 05:31:18 UTC by Admin
Updated 2026-08-29 05:37:06 UTC by Admin