Active Directory aktivně

Active Directory
Automatizace správy

Patrik Malina
patrikmalina.eu

O čem bude řeč

- Active Directory – způsoby správy
- Možnosti automatizace – dříve a dnes
- Různé vymoženosti PowerShellu
- Bezprostřední hromadné změny
- Dávkový import a export
- Záloha a obnova objektů

Jak na správu AD

- Grafická rozhraní
  - Klasické provedení
  - Moderní přístupy
    - PowerGUI
    - Active Directory Administrative Center
- Nástroje pro automatizaci
  - Cmd.exe
  - WSH/VBS
  - PowerShell

Automatizace dříve a dnes

- Změny/nastavení atributů
  - Ldifde.exe

```
dn: CN=Jane Doe,OU=Staff,DC=microsoft,DC=com
changetype: modify
replace: extensionAttribute1
extensionAttribute1: Staff
-
dn: CN=John Doe,OU=Staff,DC=microsoft,DC=com
changetype: modify
replace: extensionAttribute1
extensionAttribute1: Staff
-
```

  - Csvde.exe

Automatizace dříve a dnes

- Exporty dat/sestavy
  - Logparser.exe

```
LogParser "SELECT cn,samaccountname,description FROM
LDAP://foundation.int" -i:ADS -objclass:user
```

```
LogParser "SELECT cn,samaccountname,description Into d:\data\ad_ex.csv
FROM LDAP://foundation.int" -i:ADS -objclass:user
```


Automatizace dříve a dnes

- Úpravy objektů – rodinka Ds*

```
for /F "tokens=1" %h IN (users.txt) Do dsquery user forestroot -name
"%h" | dsmod user -desc "Popisek"
```

```
for /F "tokens=1" %h IN (users.txt) Do dsquery user forestroot -name
"%h" | dsmod user -disabled yes
```

```
For /f "tokens=1 delims= " %i in (MyUsers.Txt) do Dsquery user
"cn=%i,OU=sales,DC=domena,DC=abc" | dsmove -newparent
"OU=sales2,DC=domena,DC=abc“
```

Automatizace dříve a dnes

- Skripty: WSH + ADSI

```
Const ADS_SCOPE_SUBTREE = 2

Set objConnection = CreateObject("ADODB.Connection")
Set objCommand = CreateObject("ADODB.Command")
objConnection.Provider = "ADsDSOObject"
objConnection.Open "Active Directory Provider"
Set objCommand.ActiveConnection = objConnection

objCommand.Properties("Page Size") = 1000
objCommand.Properties("Searchscope") = ADS_SCOPE_SUBTREE

strValue = strAttributeValue
objCommand.CommandText = "SELECT aDSPath FROM 'LDAP://" & strADPath & "' WHERE '"
& strAttributeName & "'='" & strValue & "'"

   err.clear
   Set objRS = objCommand.Execute
```


Automatizace dříve a dnes

- PowerShell – Quest AD Cmdlets
  - Win XP a dále
  - PSH 1 i 2
  - Výborná dokumentace

Automatizace dříve a dnes

- Active Directory PowerShell
  - Win 7 & Win 2008 R2
  - Jen PSH 2
  - Hlavně nápověda

Různé vymoženosti PowerShellu

- Objekty a roura

```
Get-QADUser | Where-Object {$_.name -like "*modry*"}

Get-QADGroup -Identity oddeleni* | Get-QADGroupMember

cat .\cns.txt | Get-QADUser

cat .\cns.txt | Add-QADGroupMember -Identity oddeleni1

(Get-QADObject -Identity *demo* | Where-Object {$_.type -like "*org*"}).dn
```

Různé vymoženosti PowerShellu

- Manipulace s texty

```
cat D:\data\cns.txt | ForEach-Object `
{"cn=$_,ou=demo_bck,dc=foundation,dc=int"} | Set-Content Dns.txt

Import-Csv D:\data\users.csv | ForEach-Object `
{$_.jm + "." + $_.Pr + "@domena.xyz"}

'cn=jnovacek,ou=demo_bck,dc=foundation,dc=int' -split ","
('cn=jnovacek,ou=demo_bck,dc=foundation,dc=int' -split ",")[0] -replace "cn="

(([regex]::match('cn=jnovacek,ou=demo_bck,dc=foundation,dc=int',"ou=.*dc=")).
value).Substring(3)
```


Bezprostřední hromadné změny

- Vyhledání účtů

```
Get-QADUser -SearchRoot "foundation.int/demo"

Get-QADUser -PasswordNeverExpires
Get-QADUser -AccountNeverExpires
Get-QADUser -AccountExpiresBefore

Get-QADUser -AccountExpiresAfter ((get-date).adddays(30))

Get-QADUser -MemberOf oddeleni1
Get-QADUser | Where-Object {$_.memberof -like "*oddeleni1*"}
```

Bezprostřední hromadné změny

- Vyhledání účtů

```
Get-ADUser -Filter {name -like "*"}

Get-ADUser -Filter {name -like "*"} -Properties *

Get-ADGroup -Filter {name -like "odd*"}

Get-ADUser -LDAPFilter
Get-ADUser -LDAPFilter "(samaccountname=*)"
Get-ADUser -LDAPFilter "(samaccountname=j*)"
```


Bezprostřední hromadné změny

- Zapnutí/vypnutí účtů

```
Get-QADUser -SearchRoot "foundation.int/demo" -Disabled

$domena = "foundation.int"
Get-QADUser -SearchRoot "foundation.int/demo" -Disabled -Service $domena

Get-QADUser -SearchRoot "ou=demo,dc=foundation,dc=int" | Enable-QADUser

$ou_dn = (Get-QADObject -Identity *demo* | Where-Object {$_.type -like `
"*org*"}).dn
data>Get-QADUser -SearchRoot $ou_dn | Enable-QADUser

cat .\cns.txt | Disable-QADUser -WhatIf
```

Bezprostřední hromadné změny

- Reset hesla a odemčení

```
Get-QADUser -SearchRoot 'foundation.int/demo' | Set-QADUser ` -
UserPassword "Heslo123heslo" -UserMustChangePassword $true
```

```
Get-QADUser -Locked
Get-QADUser -Locked | Unlock-QADUser
```


Bezprostřední hromadné změny

- Hromadná změna atributu

```
cat .\cns.txt | Set-QADUser -Description "Popisek"
```

Bezprostřední hromadné změny

- Členství ve skupinách

```
Get-QADGroupMember -Identity oddeleni1

Get-QADGroupMember -Identity oddeleni1 | Add-QADGroupMember -Identity `
oddeleni2

$groups = (Get-QADUser tnov*).memberof
$user = Get-QADUser Novy* -SearchRoot "OU=Demo_bck,DC=foundation,DC=int"

$groups | ForEach-Object {Add-QADGroupMember -Identity $_ -Member $user}
Get-QADGroup oddeleni2 | Get-QADGroupMember
```


Bezprostřední hromadné změny

- Informování uživatelů

```
$emailfrom = "odesilatel@domena.abc"
$subject = 'Udrzba domeny'

$path = Join-Path (pwd) -ChildPath "\priloha1.rtf"
$attach = new-object Net.Mail.attachment($path)

$emailbody = cat message_1.htm
$emailto = 'prijemce@domena.xyz'

$smtpServer = "smtp.domena.ijk"
$mailer = new-object Net.Mail.SMTPclient($SMTPserver)

$msg = new-object Net.Mail.MailMessage($emailfrom, $emailto, $subject, $emailbody)
$msg.IsBodyHTML = $True

$msg.Attachments.Add($attach)

$mailer.send($msg)
$msg.Dispose()
```

Dávkový import a export

- Datový zdroj/úložiště – CSV, XML

```
import-csv .\users.csv
import-csv .\users.csv | Get-Member
```

```
Import-Csv .\users.csv | ForEach {New-QADUser -name $_.sam `
-Email $_.upn -FirstName $_.jm -LastName $_.pr `
-UserPrincipalName $_.upn -SamAccountName $_.sam `
-ParentContainer 'OU=demo,DC=foundation,DC=int'}
```


Dávkový import a export

- Ldifde reloaded

```
cat cns.txt | % {ldifde.exe -f "$((pwd).ToString())\$_-AD_backup_$(get-
date -UFormat %m-%d-%y-%H-%M-%S).ldif" -r "cn=$_" -p subtree}
```

Záloha a obnova objektů

- Export-import
  - Pozor na limity AD – SID, GUID atd.

```
Get-QADUser -identity jnovacek -IncludeAllProperties -SerializeValues |
Export-Csv jnovacek.csv
```

```
Import-Csv .\jnovacek.csv | New-QADUser -ParentContainer `
"foundation.int/demo_bck" -DeserializeValues -name novyuzivatel ` -
SamAccountName novyuzivatel -UserPassword "NoveHeslo!@#3"
```


Záloha a obnova objektů

- Obnova smazaných (tombstoned) objektů
  - Před W2008 R2 – Deleted
  - Nově – Recycle Bin

Záloha a obnova objektů

- Obnova smazaných (tombstoned) objektů

```
Get-QADUser -Tombstone

Get-QADUser -Tombstone | Restore-QADDeletedObject

Get-QADObject -name "Divize*" -Tombstone | Restore-QADDeletedObject ` -
RestoreChildren
```


Záloha a obnova objektů

- AD Recycle Bin

```
Set-ADForestMode –Identity foundation.int -ForestMode
Windows2008R2Forest

Enable-ADOptionalFeature –Identity ‘CN=Recycle Bin Feature,CN=Optional
Features,CN=Directory Service,CN=Windows
NT,CN=Services,CN=Configuration, DC=foundation,DC=int’ –Scope
ForestOrConfigurationSet –Target ‘foundation.int’

Get-ADObject -Filter {cn -like "tnovak*"} -IncludeDeletedObjects

Get-ADObject -Filter {cn -like "tnovak*"} -IncludeDeletedObjects |
Restore-ADObject
Get-ADObject -Filter {cn -like "tnovak*"} -IncludeDeletedObjects
```

Zdroje informací

Internet

- MS Active Directory PowerShell
  - Blog vývojového týmu
  - http://blogs.msdn.com/adpowershell/default.aspx
- Quest – PowerShell cmdlets
  - Sada cmdletů
  - http://www.quest.com/activeroles-server/arms.aspx
- PowerGUI/AD cmdlets info
  - Blog
  - http://dmitrysotnikov.wordpress.com/

Dotazy

- … a diskuse

Další informace

- Autor
  www.patrikmalina.eu
- Kontat
  it@patrikmalina.eu

17. 12. 2009