Windows servery / CMD & POWERSHELL, užitečné příkazy

LDIFDE

Přidej OU

```
dn: OU=Printers,OU=Ostrava,DC=training,dc=te
changetype: add
objectClass: organizationalUnit
```

Export skupin z ...

```
ldifde -d "OU=Accounts,DC=domain,DC=tld" -r "(objectClass=group)" -l
"objectClass,cn,description,distinguishedName,name,sAMAccountName,groupType,
objectCategory" -f groups.ldif
```

Import skupin do ...

```
ldifde -i -v -k -f groups.ldif -c "OU=Accounts,DC=domain,DC=tld"
"OU=Accounts,DC=newDomain,DC=tld" -j logs
```

REPADMIN

Zobrazit chyby

```
repadmin /failcache
```

Zobrazit interSiteTopology generator servery

```
repadmin /istg
repadmin /kcc
```

Zobrazit latenci od vzniku zmeny po replikaci na DC

```
repadmin /latency servername
```

Detailní kontrola replikací u dané partition

```
repadmin /showvector /latency DN_partition (dn=atd..)
repadmin /notifyopt servername DN_domeny
```

Vynutit replikaci

```
repadmin /syncall
```

Vypnout odchozí replikace

```
repadmin /options servername + DISABLE_OUTBOUND_REPL
```

Zapnout odchozí replikace

```
repadmin /options servername - DISABLE_OUTBOUND_REPL
```

Stav replikace na daném serveru

```
repadmin /replsummary servername
```

Stav příchozích replikací, uložit do .csv

```
repadmin /showrepl /csv > %computername%.txt
```

Zobrazit čas v různých formátech

```
repadmin /showtime
```

NETDOM

Nalezení vlastníka FSMO rolí

```
netdom query /domain:jmeno_domeny fsmo
```

NET USER, NET LOCALGROUP

Přidat lokálního uživatele

```
net user username heslo /add
```

Lokálního uživatele přidat do lokální skupiny Administrators

```
net localgroup Administrators username /add
```

GPO, POLICY

Zobrazit nastavení auditování

```
auditpol /get /category:*
```

NLTEST

Vytvoření seznamu doménových trustů

```
nltest /domain_trusts
```

NSLOOKUP

Nalezení PDC serveru domény

```
nslookup -type=SRV _ldap._tcp.pdc._msdcs.domain.tld dns_server
```

Nalezení KDC (Kerberos server)

```
nslookup -q=SRV _kerberos._tcp.domain.tld dns_server
nslookup -q=SRV _kerberos._udp.domain.tld dns_server
```

Nalezení řadičů domény

```
nslookup -type=SRV _ldap._tcp.dc._msdcs.example.tld dns_server
```

DNSCMD

Vytvoření DNS zóny

```
dnscmd . /zoneadd domena.tld /forwarder IP_1 IP_2
```

Reload DNS zóny ze zónového souboru nebo AD

```
dnscmd . /zonereload domena.tld
```

Export DNS zóny do souboru

```
dnscmd . /zoneexport domain.tld file.txt
```

Vytvořit A záznam

```
dnscmd . /RecordAdd domain.tld servername A 10.1.1.2
```

Smazat A záznam

```
dnscmd . /recorddelete domain.tld hostname A
```

NTDSUTIL

Najít vlastníka FSMO rolí

```
Ntdsutil
roles
Connections
Connect to server %computername%
Quit
select Operation Target
List roles for connected server
Quit
Quit
Quit
```

WINDOWS TIME

Nastavit synchronizaci času s doménou

```
w32tm /config /syncfromflags:domhier /update
```

```
net stop w32time && net start w32time
```

Zapnout / vypnout logování služby w32time

```
w32tm /debug /enable /file:c:w32time.log /size:10000000 /entries:0-116
w32tm /debug /disable
```

Konverze času např. z atributu pwdLastSet

```
w32tm.exe /ntte 131001091660000000
```

NTFRS

Force FRS replikace

```
ntfrsutl forcerepl local_DC /r "domain system volume (sysvol share)" /p
remote_DC.contoso.com
```

NETBIOS over TCP/IP

Vylistovat aktuální stav

```
wmic nicconfig get caption,index,TcpipNetbiosOptions
```

Vypnutí

```
wmic nicconfig where index=8 call SetTcpipNetbios 2
```

Hodnoty

```
0 – Use NetBIOS setting from the DHCP server
1 – Enable NetBIOS over TCP/IP
2 – Disable NetBIOS over TCP/IP
```

NETSH

Zjistit velikost MTU

```
netsh interface ipv4 show subinterfaces
```

Nastavit MTU 1500

```
netsh interface ipv4 set subinterface "Network Name" mtu=1500
store=persistent
```

Přidat perzistentní záznam do ARP tabulky

```
netsh -c interface ipv4 add neighbors "jmeno_sítě" "(IP)x.x.x.x" "(MAC)xx-
xx-xx-xx-xx-xx" store=persistent
```

CMD

Přidat prefix do jmen souborů

```
for %a in (*.*) do ren "%a" "prefix_%a"
```

ROUTE

Přidat routu na interface (on-link)

```
route add -p 10.0.5.0/24 0.0.0.0 IF 37
```

BCDEDIT

Zakázat start do automatického recovery

```
bcdedit /set {default} recoveryenabled No
bcdedit /set {default} bootstatuspolicy ignoreallfailures
```

Instalace Telnet klienta

```
dism /online /Enable-Feature /FeatureName:TelnetClient
```

PATCHING

Vylistovat instalované patche, WMIC

```
wmic qfe list full /format:htable > hotfixes.htm
```

```
wmic qfe list full /format:csv > hotfixes.csv
```

Při zobrazení chyby '*Invalid XSL format (or) file name.*' je potřeba specifikovat cestu k .XSL souboru (jedná se o chybu ve WMIC):

```
wmic qfe list full /format:"%WINDIR%\System32\wbem\en-us\htable"
```

```
wmic qfe list full /format:"%WINDIR%\System32\wbem\en-us\csv"
```

Vylistovat instalované patche, DISM

```
dism /online /get-packages
```

Odinstalovat patch

Dotaz, zda má být patch odinstalován:

```
wusa /uninstall /kb:4483458
```

Bez interakce s uživatelem, server restartuje, pokud je to vyžadováno:

```
wusa /uninstall /kb:4483458 /quiet
```

Bez restartu:

```
wusa /uninstall /kb:4483458 /quiet /norestart
```

V kombinaci s `/quiet` se objeví informace před restartem:

```
wusa /uninstall /kb:4483458 /quiet /warnrestart
```

V kombinaci s ''/quiet'' jsou vynuceně ukončené aplikace a server restartuje:

```
wusa /uninstall /kb:4483458 /quiet /forcerestart
```

Certifikáty

Zkontrolovat AD certifikáty

```
certutil -dcinfo verify
```

Vytvořit self-signed certifikát

```
New-SelfSignedCertificate -KeyLength 2048 -KeyAlgorithm RSA -DnsName
```

```
"*.test01.local", "*.test02.local" -CertStoreLocation
"cert:\LocalMachine\My" -KeyExportPolicy Exportable -NotAfter (Get-
Date).AddMonths(120)
-DnsName // první je CNAME, další SANs
```

PODEPSÁNÍ POWERSHELL SCRIPTU

Vytvořit certifikát

```
New-SelfSignedCertificate -CertStoreLocation cert:\currentuser\my `
-Subject "CN=Jméno certifikátu" `
-KeyAlgorithm RSA `
-KeyLength 2048 `
-Provider "Microsoft Enhanced RSA and AES Cryptographic Provider" `
-KeyExportPolicy Exportable `
-KeyUsage DigitalSignature `
-Type CodeSigningCert `
-NotAfter $([datetime]::now.AddYears(10))
```

Kontrola certifikátu

```
get-childitem cert:\CurrentUser\my -codesigning
```

Podepsání scriptu

```
$cert = @(Get-ChildItem cert:\CurrentUser\My -codesigning)[0]
Set-AuthenticodeSignature -HashAlgorithm sha256 file.ps1 $cert
```

Enablovat / Disablovat Cipher Suites (PowerShell)

Enablovat

```
Enable-TlsCipherSuite -Name "TLS_DHE_RSA_WITH_AES_256_CBC_SHA"
```

Disablovat

```
Disable-TlsCipherSuite -Name "TLS_DHE_RSA_WITH_AES_256_CBC_SHA"
```

Odinstalovat Wireshark

```
"C:\Program Files\Wireshark\uninstall.exe" /S
```

Vytvořit checksum souborů ve složce a podsložkách

```
Get-ChildItem -Path c:\ -Recurse | Get-FileHash | Export-Csv C:\fileHash.txt
```

RDP, disablovat NLA

```
(Get-WmiObject -class Win32_TSGeneralSetting -Namespace
root\cimv2\terminalservices -Filter "TerminalName='RDP-
tcp'").SetUserAuthenticationRequired(0)
```

Shadow Copy

Spustit konzolu

```
diskshadow
```

Vylistovat dostupné snapshoty disku

```
list shadows all
```

Smazat snapshoty disku

```
DELETE SHADOWS all
```

- Twitter
- Facebook
- LinkedIn
- Email

cmd, netsh, repadmin, dnscmd, ldifde, ntdsutil, shadow copy, snapshot