

C:\> systeminfo

Priručnik za upravljanje Windows **CORE** 2008 **R2 SP1** serverima

C:\>ver
verzija 2.7

C:\>whoami
Ratko Žižek, MCSE-MCITP



**DOPUNJENO
IZDANJE**

Priručnik je usmjeren ka IT profesionalcima koji žele ili moraju ovladati Windows Core 2008 R2 serverom a poznavatelji su Windows GUI servisa, alata i procedura.

Tematski, ovaj priručnik odgovara na nedoumice tipa „Kako to-i-to odraditi na Core serveru?“. Pojašnjenja su prisutna samo u potencijalno zbunjujućim situacijama. Nadalje, prvenstveno se bavimo Core instalacijom izvan domene, kad je server tzv. stand-alone, jer to je administrativno zahtjevnija situacija ali, naravno, prisutne su i brojne reference za Windows domenu.



PRIRUČNIK ZA UPRAVLJANJE WINDOWS CORE 2008 R2 SP1 SERVERIMA

SADRŽAJ

I. BITNE ZNAČAJKE CORE EDICIJA

Windows GUI vs Windows CLI
Podržane uloge (roles) i elementi (features)
Primarna namjena Server Core edicija

II. INSTALACIJA I AKTIVACIJA

Instalacija
Aktivacija

III. INICIJALNO PODEŠAVANJE NOVE INSTALACIJE

Alati za inicijalno podešavanje servera
Postaviti / izmijeniti password lokalnog Administratora
Kreirati rezervnog admina
Postaviti regionalne parametre
Preimenovati server
Postaviti statičke TCP/IP v4 i druge mrežne parametre
Konfigurirati Windows Time servis
O(ne)mogućiti pinganje servera
Učlaniti server u domenu
Iščlaniti server iz domene
Promijeniti radnu grupu (workgroup)
Pristupiti sa Core servera file-share resursu
Krpanje Core servera
Restartati ili isključiti server
Odjaviti se sa servera

IV. OSTALE UOBIČAJENE ADMINISTRATIVNE RADNJE

Ako server administriramo remotely, s tzv. admin stanice
Administriranje servera MMC konzolama
Administriranje servera RSAT konzolama
Administriranje servera RDC-om
Uporaba RDC klijenta za spajanje sa Core na druga računala
Kako (de)instalirati rolu i feature
Osnovne operacije s lokalnim grupama i korisnicima
Osnovne operacije sa servisima
Osnovne operacije s driverima
Osposobljavanje uređaja za koje Core nema driver

Osnove rada s lokalnim firewallom
Uvid u Event Viewer i druge logove
Uvid u volumene/particije sustava
Kreirati i obrisati (primarnu) particiju
Backupirati System State i podatke
Administrirati Pagefile.sys
Postaviti proxy server
Proizvoljno zaustaviti proces
Pokrenuti Task Manager
Defragmentirati disk
(De)instalirati MSU paket
(De)instalirati MSI paket
Raspakirati CAB paket
Izmijeniti display postavke
Disablrati User Account Control
Podesiti startup sekvencu
Anti-intruder zaštita servera
Pristupiti Web resursima sa Core servera
Core kao File Server
Core kao Print Server
Core kao DNS server
Core kao drugi Domain Controller
Core kao IP router
Core i Hyper-V
Core i IIS 7.5

[V. PREGLED KOMANDNOLINIJSKIH NAREDBI](#)

Uvodne napomene

Pregled naredbi

[VI. ZBLIŽIMO SE SA CLI OKRUŽENJEM!](#)

Za efikasniji rad u komandnoj linji...

Prompt (odzivni znak)

Varijable PATH i PATHEXT

Rad s direktorijima i datotekama

Džokeri (wildcards)

Redirekcija

Automatiziranje poslova skriptama

I. BITNE ZNAČAJKE CORE EDICIJA

Windows GUI vs Windows CLI

U odnosu na klasičnu (GUI baziranu) instalaciju Windows Server 2008 R2, Core ediciju karakteriziraju:

- izrazita orijentiranost na Command Line Interface (CLI)
- značajno smanjene potrebe za računalnim resursima
- značajno veća out-of-the-box razina zaštite
- izrazita modularnost tj. defaultno se instalira samo jezgra OS-a, potom je na administratoru da instalira sve potrebne uloge (roles) i elemente (features)
- nemogućnost direktnog upgradea Core edicije na GUI Windows ediciju
- otežano administriranje zbog nepostojanja GUI-a i Web browsera

Podržane uloge (roles) i elementi (features)

| ULOGJE | ELEMENTI |
|---|--|
| Active Directory Certificate Services | Failover Clustering Network Load Balancing Subsystem for UNIX-based applications Windows Server Backup Multipath IO BitLocker Drive Encryption Simple Network Management Protocol (SNMP) Windows Internet Name Service (WINS) Telnet client QWAVE Subset of .NET Framework 2.0 Subset of .NET Framework 3.0 and 3.5 Windows Communication Framework (WCF) Windows Workflow Framework (WF) LINQ Windows PowerShell Server Manager cmdlets Best Practices Analyzer (BPA) cmdlets WoW64 32-bit support for the Input Method Editor |
| Active Directory Domain Services | |
| Active Directory Lightweight Directory Services | |
| DHCP Server | |
| DNS Server | |
| File Services | |
| Media Services | |
| Hyper-V | |
| Print Services | |
| Web Services (trenutno s ograničenom podrškom za ASP.NET ali s punom podrškom za PHP i MySQL) | |

Sve podržane uloge i elemente vidjet ćemo naredbom `dism /online /get-features /format:table`.

Za dodatne informacije uvodnog karaktera vidi [http://technet.microsoft.com/en-us/library/cc753802\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc753802(WS.10).aspx).

Primarna namjena Server Core edicija

- Podrška servisima u high-security okolinama - tipično, internet-facing aplikativni ili infrastrukturni servisi, poput Web servera ili DNS-a.
- Podrška servisima koji bi, u skladu s preporukama proizvođača, trebali biti na dedicanom serveru - tipično, Hyper-V ili javni DNS; kombinacije RODC+DNS ili File & Print Services.

Windows 2008 R2 je pravi 64-bitni OS, dakle, ne radi na 32-bitnom HW i ne prihvaća 32-bitne sistemske drivere **ali** podržava 32-bitne user-mode drivere i aplikacije.

Detaljnije o Windows Server 2008 R2 edicijama, ulogama i elementima na <http://www.microsoft.com/windowsserver2008/en/us/R2-editions.aspx>.

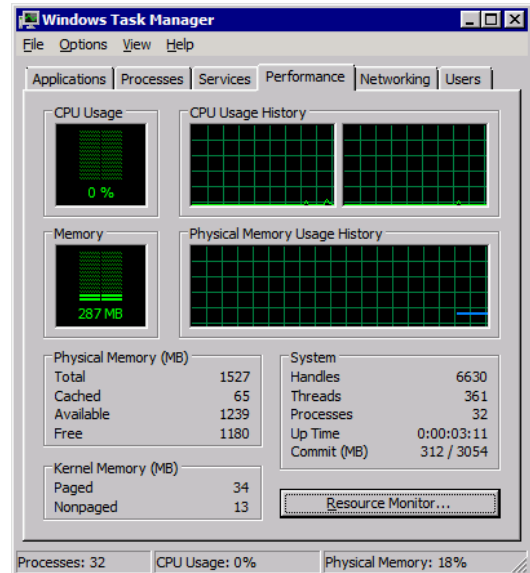
Aktualna startna točka za ovladavanje Windows Server 2008 R2: [http://technet.microsoft.com/hr-hr/evalcenter/dd459136\(en-us\).aspx](http://technet.microsoft.com/hr-hr/evalcenter/dd459136(en-us).aspx).

II. INSTALACIJA I AKTIVACIJA

INSTALACIJA

- Važan je odabir realnim potrebama primjerene edicije Windows Core (Web, Standard, Enterprise ili Datacenter) zbog ograničenja pojedinih edicija te, s druge strane, cijene konkretne edicije; Web edicija je najjeftinija ali s najviše ograničenja, vidi <http://www.microsoft.com/windowsserver2008/en/us/r2-compare-core-installation.aspx>.

Tek instaliran i pokrpan, Core R2 Enterprise zauzima oko 2.5 GB diskovnog prostora (bez Pagefile.sys ali s distribucijom kopiranom na disk tijekom Setupa), oko 250 MB RAM-a te radi na x64 procesoru bez obzira na njegovu brzinu.



- Core se može instalirati interaktivno (tzv. klasična instalacija) ili u unattended modu. Ako rabimo potonji način, moramo pripremiti datoteku instrukcija Unattend.xml i na budućem Core serveru startati jedan od OS-ova: Windows PE, Windows 2003 ili XP, vidi [http://technet.microsoft.com/en-us/library/cc753802\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc753802(WS.10).aspx).
- Za eventualni prekid interaktivne instalacijske procedure rabi se tipka Esc.
- Ako na računalu već imamo neki 64-bitni Windows OS, i želimo ga sačuvati, Core Setup pokrećemo iz te prve instalacije, ali na drugu particiju. Ovim pristupom zadržat ćemo postojeći raspored oznaka diskova.
- Osim uobičajenih operacija s particijama, Core Setup omogućava širenje (extend) postojeće particije (pored nje mora biti unallocated space) no s particijama se može raditi samo kad se Setup pokreće s instalacijskog medija a ne iz neke postojeće Windows instalacije.
- Ako Core nema driver za diskovni podsustav, istoga trebamo spremati u root diskete ili optičkog medija ili USB sticka pa kad se, tijekom Setup procedure, pojavi ekran za odabir diska, odaberemo Load Driver.
- Mudro je iz Setupa kreirati sve potrebne particije jer ako to odgodimo za kasnije morat ćemo rabiti komandnolinijski alat DISKPART koji nije baš user-friendly.
- Što ako Core Setup ne prepozna neki uređaj (odn. ne raspolaže adekvatnim driverom) poput mrežne ili grafičke kartice? Odgovori su u poglavlju Ostale uobičajene administrativne radnje.
- Nakon instalacije **ne** ukidati firewall (zbog zaštite i da bi mogao pratiti/pamtiti daljnja konfiguriranja servera), nadalje, što prije postaviti password za

Administratora, primijeniti zadnji Service Pack (Core prihvaća USB diskove) pa nastaviti dalje.

- Jednom instaliran Core R2 može se upgradeirati na višu Core R2 ediciju, npr. Core Standard na Core Enterprise. Više o toj temi na <http://technet.microsoft.com/en-us/library/dd744380%28WS.10%29.aspx>.

AKTIVACIJA

- Načelno, nakon dovršene instalacije slijedi upisivanje produkcijskog ključa (product key): `s\lmgr /ipk brojevni-izraz-sa-separatorima`, **ali** ako na mreži imamo lokalni KMS, product key **ne** upisujemo već primjenjujemo nižu proceduru.

Supozicija: Na korporativnoj mreži je aktivan KMS server; Core server je na korporativnoj mreži, postavljeni su mu interni DNS serveri (ili je KMS server upisan u lokalnu Hosts).

a) na Core serveru zadati: `s\lmgr /ato`

Ukoliko se pojavi poruka-greška, treba prijeći na korak b).

b) na Core serveru zadati: `s\lmgr /skms FQDN-KMS-servera`
`s\lmgr /ato`

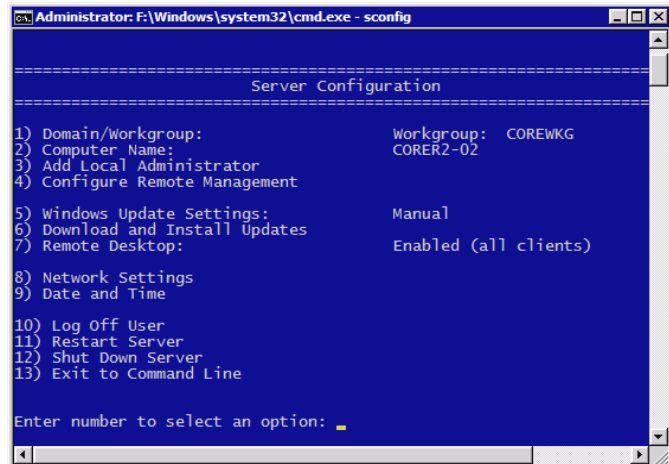
- Ukoliko se opet pojavi poruka s greškom, imate ili nepodešenu activation infrastrukturu ili specifičnu licensing-activation politiku (MS je razvio nekoliko politika). U potonjem slučaju, vašu situaciju trebate riješiti kontaktirajući MSH ili posredstvom adresa <http://www.microsoft.com/licensing/existing-customers/product-activation.aspx> i [http://technet.microsoft.com/en-us/library/cc770800\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc770800(WS.10).aspx).
- Aktivacijska licenca vrijedi 180 dana; ukoliko ju Windows računalo ne obnovi u tom intervalu, prelazi u stanje „neaktiviran“ tj. u grace period maksimalne duljine 30 dana. Nakon toga imamo izbor: ili računalo ipak aktivirati ili produžiti grace period. Potonje se može odraditi najviše dvaput, naredbom `s\lmgr /rearm`. Tijekom rada na neaktiviranoj instalaciji korisna je `s\lmgr /xpr` jer informira o krajnjem datumu aktualnog grace perioda.
- Ako Core server ostvaruje internet konekciju preko proxya koji mu nameće autentikaciju (vidi KB 921471), a na korporativnoj mreži **ne** postoji odgovarajuća licensing-activation infrastruktura, instalacija se može **aktivirati telefonom**:
 - a) zadati `s\lmgr /dti`
 - b) nazvati MS na 00800-300-300, birati 1, opet 1, priopćiti InstallationID
 - c) upisati od MS-ovog operatera priopćen Confirmation ID tako da zadamo naredbu: `s\lmgr /atp brojevni-izraz-bez-separatora`
- InstallationID i stanje aktivacije uvijek možemo provjeriti sa `s\lmgr /d\lv`.

III. INICIJALNO PODEŠAVANJE NOVE INSTALACIJE

Alati za inicijalno podešavanje servera

Core R2 ima alat SCONFIG (Visual Basic skripta) kojime se olakšavaju neke osnovne administrativne operacije. Postoje i third-party GUI-oriented alati iste namjene, poput već razvikanog Core Configuratora.

Glavni ekran SCONFIG skripte.



Postaviti / izmijeniti password lokalnog Administratora

Sustav traži od Administratora postavljanje passworda tijekom njegovog prvog ulogiravanja. Za naknadne izmjene passworda je naredba:

`net user administrator * ili Ctrl+Alt+Del pa Change a password`

OPREZ! Postavljeni password za Administratora vremenski je ograničen. Rečeno važi i za rezervnog admina. Uključenje opcije Password never expires najlakše se odradi remotely, vidi Administriranje servera MMC konzolama.

Kreirati rezervnog admina

- Kreirati korisnika Adminbck: `net user Adminbck * /add`
- Staviti korisnika Adminbck u lokalnu grupu Administrators:
`net localgroup Administrators /add Adminbck`
- Ukloniti korisnika Adminbck iz lokalne grupe Users:
`net localgroup Users /delete Adminbck`
- Učlaniti domenskog korisnika u lokalnu grupu Administrators (ako je server u domeni): `net localgroup Administrators /add domena\korisnik`
- Vidjeti članove lokalne grupe Administrators: `net localgroup Administrators`

Postaviti regionalne parametre

Zadati naredbu `control intl.cpl`, podesiti u skladu s aktualnom politikom firme, zadati logoff i ponovo se ulogirati.

* Posebnu pozornost dajte kartici Administrative, tu je gumb Copy settings kojime primjenjujemo regionalne postavke na accounte korisnika i servisa. Da bismo u Cmd prozoru prešli s kodne stranice 437 na 852, na istoj kartici odabrat ćemo gumb Change system locale.

* Ovisno o redosljedju podešavanja parametara za regionalne specifičnosti, da biste u Cmd prozoru dobili sva naša slova ponekad ćete morati napraviti logoff – logon.

Preimenovati server

- Ako je server stand-alone:

```
netdom renamecomputer aktualno-ime /newname:novo-ime
```

- Ako je server u domeni:

```
netdom renamecomputer aktualno-ime /newname:novo-ime /userd:domenski-admin /passwordd:*
```

* Ne zaboravite restartati server.

* Preimenovanje servera odnosi se na postavljanje tzv. NetBIOS imena odn. na *host label* dio FQDN imena; za definiranje primarnog DNS sufiksa vidi dalje.

* Aktualno ime najbrže ćemo doznati naredbama `hostname` ili `ipconfig /all`.

Preimenovanje servera člana domene; uočite upozorenje.

```
Administrator: C:\Windows\system32\cmd.exe - netdom renamecomput...
C:\>netdom renamecomputer corer2-01 /newname:CORER2-11 /user
d:ad\admin /passwordd:*
Type the password associated with the domain user:
This operation will rename the computer corer2-01
to CORER2-11.
Certain services, such as the Certificate Authority, rely on
a fixed machine
name. If any services of this type are running on corer2-01,
then a computer name change would have an adverse impact.
Do you want to proceed (Y or N)?
-
```

Postaviti statičke TCP/IP v4 i druge mrežne parametre

- Identificirati mrežne kartice:

```
netsh interface show interface
```

```
netsh interface ipv4 show interfaces
```

* Obratite pozornost na kolone Idx i Name jer su u njima prikazani identifikatori koje dalje rabimo u raznim naredbama.

- Postaviti IP adresu na preferirani mrežni interface:

```
netsh interface ipv4 set address name=Idx source=static
address=x.x.x.x mask=y.y.y.y gateway=x.x.x.x
```

- Postaviti prvi DNS:

```
netsh interface ipv4 add dnsservers name=Idx address=x.x.x.x index=1
```

* `netsh interface ipv4 set dnsservers` omogućuje nam upravljanje dynamic DNS registration značajkom te validacijom DNS servera.

- Postaviti drugi DNS:

```
netsh interface ipv4 add dnsservers name=Idx address=x.x.x.x index=2
```

- Postaviti ili ukloniti DNS sufikse:

a) pokrenuti Regedit

- b) smjestiti se u HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
 c) definirati sljedeće ključeve:

Domain (REG_SZ) - upišemo FQDN aktivne mrežne konekcije, poput **corp.hr**. Time smo definirali Primary DNS sufiks servera. Nije potreban restart.

SearchList (REG_SZ) - riječ je o sufiksima za pretraživanje kad se u upitu za resolving imena nekog mrežnog hosta rabe nekvalificirana DNS imena. Ako se postave sufiksi (npr.: internal.corp.hr,corp.hr) potreban je restart servera.

* Ako server učlanite u domenu, FQDN domene će mu biti postavljen kao Primary DNS suffix.

- Postaviti WINS server:

```
netsh interface ipv4 add winsservers name=Idx address=x.x.x.x index=1
```

- Dodijeliti opisno ime mrežnoj kartici:

```
netsh interface set interface name="aktualno-ime" newname="novo-ime"
```

- Provjeriti obavljeno konfiguriranje mrežnih parametara:

```
ipconfig /all ili netsh interface ipv4 show config
```

Za informiranje o mrežnim karticama potrebne su dvije naredbe.

```

Administrator: F:\Windows\system32\cmd.exe
F:\Users\Administrator>netsh interface show interface
Admin State      State           Type            Interface Name
-----
Disabled        Disconnected   Dedicated       Local Area Connection 2
Enabled         Connected      Dedicated       ActiveNIC

F:\Users\Administrator>netsh interface ipv4 show interfaces
Idx  Met  MTU  State      Name
----
  3   20   1500 connected ActiveNIC
  1   50 4294967295 connected Loopback Pseudo-Interface 1

F:\Users\Administrator>
  
```

- Poništiti postavljenu IP adresu

```
netsh interface ipv4 set address name=Idx
```

- Ukloniti sve DNS servere:

```
netsh interface ipv4 delete dnsservers name=Idx address=
```

- Vratiti mrežnu karticu na DHCP:

```
netsh interface ipv4 set address name=Idx source=dhcp
```

* U parametru source= upisuje se doslovce izraz DHCP.

- Disablirati (suvišnu) mrežnu karticu:

```
netsh interface set interface name="aktualno-ime" admin=disabled
```

* Za enabliranje kartice rabi se izraz admin=enabled.

- Disablirati IPv6 protokol: vidi <http://support.microsoft.com/kb/929852>.

- Detaljne info o mrežnim adapterima: wmic nic list /format:list.

Konfigurirati Windows Time servis

Ako je Core u domeni, servis se automatski starta te dogovara radne parametre i točno vrijeme s Domain Controllerom. Izvan domenskog prostora servis je u režimu rada Manual i stopiran, a interni okidač OS-a pokreće ga jednom tjedno kako bi se sinkronizirao s time.microsoft.com... ukratko, ovo je stanje nepoželjno na produkcijskom serveru.

OPREZ! Niže izloženo potrebno je samo ukoliko Core server **ne** učlanjujemo u domenu.

a) Postaviti Windows Time servis na Automatic:

```
sc config w32time start= auto (uočite razmak iza znaka jednakosti)
```

b) Startati WinTime servis: `sc start w32time`

c) Povezati WinTime servis sa stanjem mrežnog podsustava servera:

```
sc triggerinfo w32time start/networkon stop/networkoff
```

d) identificirati aktivnu mrežnu karticu, potom ju restartati (disable/enable) naredbom NETSH – vidi Postaviti statičke TCP/IP i druge mrežne parametre - ili jednostavno restartamo server

e) Definirati Time Source: `w32tm /config /manualpeerlist:IP-ili-FQDN-NTP-servera,0x8 /syncfromflags:manual /update`

f) Forsirati vremensku sinkronizaciju: `w32tm /resync /nowait`

* Poželjno je usmjeriti server na interni Time Source jer, prisjetimo se, NTP protokol ne autentificira NTP server.

* Za uobičajene kontrole / prilagodbe datuma i vremena rabi se naredba `control timedate.cpl` ili naredbe DATE i TIME. `Timedate.cpl` ima karticu Internet Time koju možemo iskoristiti za najosnovniju – za produkcijske servere nedostatnu – konfiguraciju i sinkronizaciju.

* Ako se Core vrti na Hyper-V, obratiti pozornost na stanje opcije Time synchronization u postavkama virtualne mašine (Settings > Integration Services).

Naredbom W32TM provjeravamo stanje vremenske sinkronizacije.

```
E:\>w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 4 (secondary reference - syncd by (S)NTP)
Precision: -6 (15.625ms per tick)
Root Delay: 0.0516968s
Root Dispersion: 7.8132740s
ReferenceId: 0x0A01FAD7 (source IP: 192.168.10.15)
Last Successful Sync Time: 13.8.2009 11:12:58
Source: 192.168.10.15,0x8
Poll Interval: 10 (1024s)
E:\>
```

O(ne)mogućiti pinganje servera

Defaultno se server ne može pingati zbog restriktivne politike lokalnog firewalla.

- Omogućiti pinganje: `netsh advfirewall firewall set rule name="File and Printer Sharing (Echo Request - ICMPv4-In)" new enable=yes`
- Onemogućiti pinganje: `netsh advfirewall firewall set rule name="File and Printer Sharing (Echo Request - ICMPv4-In)" new enable=no`

* Gornja naredba djeluje na sve profile vatrozida odjednom.

Učlaniti server u domenu

Prije učlanjenja, kao minimum postaviti ispravne DNS-ove (obično su to DC-i domene), te datum i regionalne specifičnosti.

```
netdom join ime-servera /domain:ime-domene /userd:domenski-admin  
/passwordd:*
```

* Ovisno o situaciji, parametar ime-domene može biti u NetBIOS ili FQDN obliku.

* Brza provjera punopravnosti članstva: netdom verify ime-servera /domain:FQDN-domene /usero:domenski-admin /passwordo:*. Ukoliko izvješće ukaže na grešku, tijekom tshootinga oslonite se na naredbu NLTEST i [http://technet.microsoft.com/en-us/library/cc776879\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc776879(WS.10).aspx).

Iščlaniti server iz domene

OPREZ! Prije iščlanjenja servera, provjerite možete li se ulogirati s lokalnim admin računom. Također, dobro je zadati naredbu netsh advfirewall firewall set rule name="remote desktop (tcp-in)" new profile=any enable=yes kako bismo zadržali RDC pristup bez obzira na to koji će se profil vatrozida aktivirati nakon prijelaza servera u radnu grupu.

```
netdom remove ime-servera /domain:FQDN-domene /userd:domenski-admin  
/passwordd:*
```

* Iz AD sustava ukloniti serverov objekt.

Promijeniti radnu grupu (workgroup)

```
wmic computersystem where name="ime-Core-servera" call  
joindomainorworkgroup name="ime-wkg"
```

* Ne zaboraviti restartati server.

Pristupiti sa Core servera file-share resursu

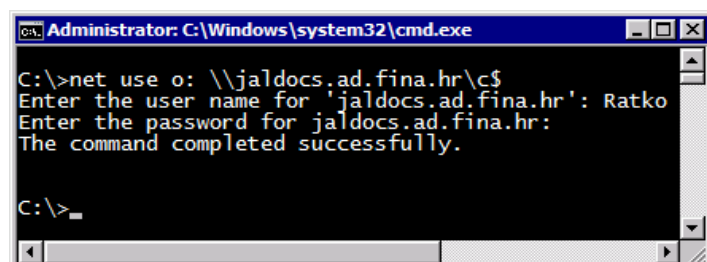
```
net use X: \\IP-adresa-cilja\share /user:ciljni-account
```

* Opcija /user: defaultno očekuje lokalni account no prihvaća i domenski ako izrijekom navedemo domenu, npr. /user:ad\ratko.

* Ako smo sigurni da radi resolving imena, u naredbi možemo rabiti NetBIOS ili FQDN ime ciljnog računala.

* Defaultno je na Core firewallu odlazna SMB konekcija dopuštena ali treba paziti na infrastrukturne firewalle te da je ciljno računalo podešeno za servisiranje SMB zahtjeva. Pristupačnost file-share servisa na ciljnom računalu možemo provjeriti naredbom telnet IP-adresa-cilja 445. Pretpostavka je instaliran element TelnetClient, vidi Kako (de)instalirati rolu i feature.

U naredbi rabimo FQDN ciljnog računala.



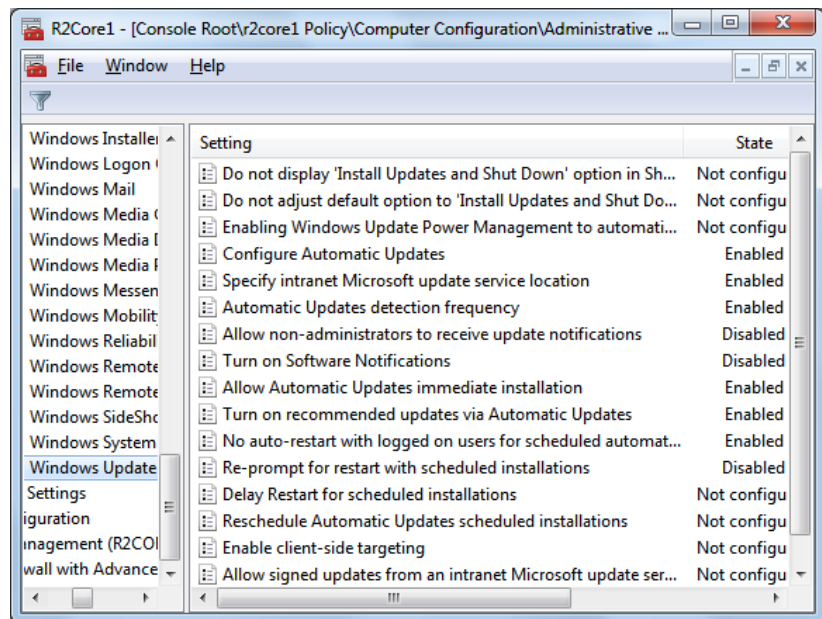
```
Administrator: C:\Windows\system32\cmd.exe  
C:\>net use o: \\jaldocs.ad.fina.hr\c$  
Enter the user name for 'jaldocs.ad.fina.hr': Ratko  
Enter the password for jaldocs.ad.fina.hr:  
The command completed successfully.  
C:\>
```

Krpanje Core servera

Trenutno Core server ne može izaći na Internet kroz proxy koji zahtijeva autentikaciju, vidi KB 921471.

Preferirani način krpanja Windows servera je s lokalnog WSUS-a. Ako je server u domeni, treba na njega primijeniti domenski WSUS GPO. Ako je stand-alone, i tako će ostati, usmjeravamo ga na WSUS posredstvom lokalne GPO; u ovom slučaju rabimo MMC konzolu Group Policy Object, vidi Administriranje servera MMC konzolama. U toj konzoli slijedimo smjer: Computer Configuration -> Administrative Templates -> Windows Components -> Windows Update. U oba slučaja treba računati s nemogućnošću izvršenja raznih WU notifikacija na koje smo navikli u GUI okolini te tako i podesiti opcije za Windows Update.

Pregled ključnih WU postavki za jednu Core instalaciju. Opcija Configure Automatic Updates mora biti na 4.



- Ako baš želimo/moramo krpati server direktno s Microsoft Update sitea, koristimo naredbe pod a) i b). Scregedit.wsf je u Windows\System32\.
- a) `cscript (put)scregedit.wsf /AU 4`
- b) `sc stop wuau serv pa sc start wuau serv`
- Isključivanje Automatic Updates: `cscript (put)scregedit.wsf /AU 1`
- Uvid u aktualnu postavku WU servisa: `cscript (put)scregedit.wsf /AU /v`
- Narediti trenutnu provjeru prisutnosti novih zakrpa na Windows Update serveru (MS-ovom ili internom): `wuauclt /detectnow`
- Pregled skinutih ali neinstaliranih zakrpa (i pratećih info): pogledati u datoteku WindowsUpdate.log
- Pregled instaliranih zakrpa: `wmic qfe list ili systeminfo`
- * WU će nas kroz System log (Event ID 22) izvijestiti o nužnosti restarta servera kad je to neophodno. Također, server neće krenuti u restart ako uključimo opciju No auto-restart with logged-on users... (vidi sliku).
- * Za primjenu pojedinačnih zakrpa na Core server rabimo alat WUSA.
- * Na adresi <http://msdn.microsoft.com/en-us/library/aa387102%28VS.85%29.aspx> i [http://msdn.microsoft.com/en-us/library/aa387101\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa387101(VS.85).aspx) nalaze se skripte koje značajno olakšavaju krpanje Core servera, bez obzira rabimo li WSUS ili WU.

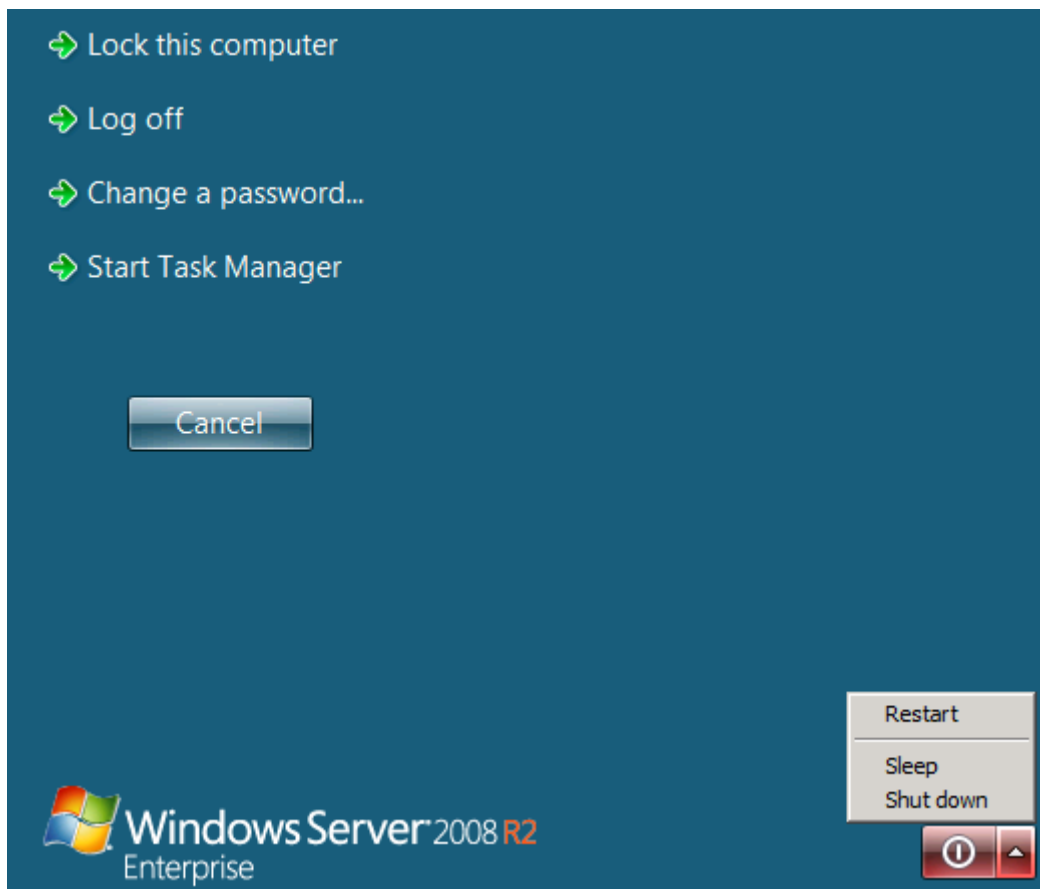
Restartati ili isključiti server

- Restart: shutdown /r ili (forsirani način) shutdown /r /f /t 0
 - Isključenje: shutdown /s ili (forsirani način) shutdown /s /f /t 0
- * Operacije se mogu obaviti i s admin stanice, npr.: shutdown /r /m \\Core-srv.

Odjaviti se sa servera

logoff

- * Ista naredba se rabi i za zatvaranje RDC sesije.



Nakon Ctrl+Alt+Del (Ctrl+Alt+End ako smo spojeni remotely) pojavljuje se ekran s važnim naredbama.

IV. OSTALE UOBIČAJENE ADMINISTRATIVNE RADNJE

Ako server administriramo remotely, s tzv. admin stanice

Admin stanica može biti GUI edicija Windows Server 2008 R2 i Windows 7.

Glede **Windows 2008 R2** GUI edicije, osim postojećih MMC konzola poput Computer Management, Windows Firewall with Advanced Security ... (opisano u Administriranje servera MMC konzolama), dodatne konzole i alate možemo dobiti na dva načina:

- a) Na server instaliramo ulogu ili element kojeg želimo administrirati na Core serveru.
- b) Na server instaliramo element Remote Server Administration Tools.

Slično, za **Windows 7** kao admin stanicu (preporučamo x64) imamo izbor: rabiti par postojećih MMC konzola poput Computer Manager, Print Manager... (opisano u Administriranje servera MMC konzolama) ili instalirati Remote Server Administration Tools Pack for Windows 7 with SP1, koji u taj operativni sustav ugnježđuje tucet dodatnih MMC konzola i CLI alata (opisano u Administriranje servera RSAT konzolama).

Uvijek vodite računa da su **minimalno** dva firewalla između admin stanice i Core instalacije – onaj na stanici i onaj na serveru – te da oba moraju biti podešena kako bismo mogli nesmetano administrirati server. Nadalje, tijekom rada posredstvom standardnih i RSAT admin konzola, na admin stanici otvaraju se **dinamički** portovi; na serverskoj strani težište je na TCP portovima poput 135, 445, 5985, 8172.... jer na njima slušaju servisi za udaljeno upravljanje serverom.

Ukoliko su Core server i admin stanica **u domeni, administriranje** servera je **olakšano** prvenstveno zbog transparentne autentikacije, centraliziranog upravljanja korisnicima te mogućnosti uporabe domenskih GPO.

Stand-alone Core server lakše ćemo administrirati ako na njemu i admin stanici rabimo iste accounte. Jasno, na Core serveru taj account mora imati administrativne privilegije.

Administriranje servera MMC konzolama

- Na Core serveru zadati:

a) `netsh advfirewall firewall set rule group="Remote Administration" new enable=yes`

b) `netsh advfirewall firewall set rule group="Windows Firewall Remote Management" new enable=yes` ili `netsh advfirewall set allprofiles settings remotemanagement enable`

Ovime je omogućena uporaba MMC konzola poput Computer Management, Windows Firewall With Advanced Security, Group Policy Object Editor, Print Management... (itd.), bez obzira na trenutno aktivan profil Core vatrozida.

- Da bismo iskoristili **Device Manager** snap-in, treba još učiniti sljedeće:

- a) na admin stanici pokrenuti Microsoft Management Console (Run: `mmc /a`)
- b) učitati Group Policy Object Editor i spojiti se njime na Core instalaciju

c) slijediti putanju: Computer Configuration -> Administrative Templates -> System -> Device Installation i ovdje enablirati opciju Allow remote access to the PnP interface

d) restartati Core

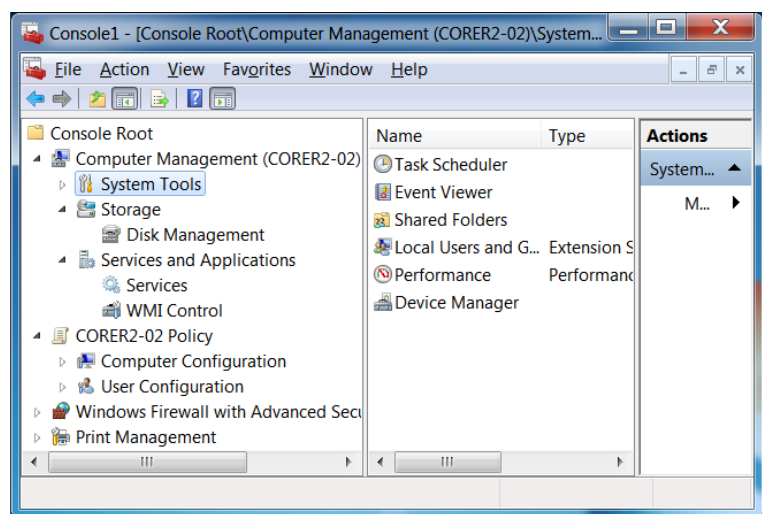
* Do daljnjega Device Manager snap-in može raditi samo u Read Only načinu, dodatno, na Core instalaciji možemo monitorirati Performance no ne možemo Reliability.

- Za uporabu snap-ina **Disk Management** treba dodatno odraditi:

a) na serveru pokrenuti servis Virtual Disk: `sc start vds`

b) na stanici i serveru zadati `netsh advfirewall firewall set rule group="Remote Volume Management" new enable=yes`

Nakon gornjih koraka, na admin stanici složimo si radnu MMC poput ove na slici.



- Da bismo s Windows 7 stanice upravljali **IIS-om 7.5**:

a) na stanicu instalirati IIS Management Console iz Windows 7 distribucije

b) s Interneta skinuti i na stanicu instalirati najnoviji IIS 7 Manager

c) na Core serveru instalirati i startati IIS Web Management Service (uočite da je taj servis u Manual stanju pa ga je dobro postaviti na Automatic)

d) na Core serveru, alatom Regedit, osposobiti udaljeni pristup na IIS:

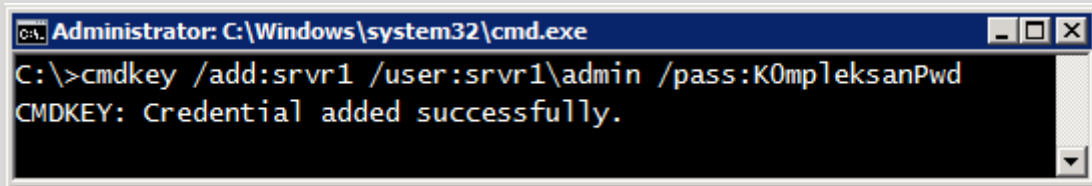
```
HKLM\Software\Microsoft\WebManagement\Server:
EnableRemoteManagement=1
```

* Budući da se za potrebe administriranja MMC metodom na Core firewallu redefinira nekoliko politika, za eventualno poništenje tih izmjena treba na serveru zadati:

a) `netsh advfirewall firewall set rule group="Remote Administration" new enable=no`

b) `netsh advfirewall firewall set rule group="Windows Firewall Remote Management" new enable=no` ili `netsh advfirewall set allprofiles settings remotemanagement disable`

Ako se na stand-alone Core spajamo accountom različitim od onoga s kojime smo se ulogirali na admin stanicu, treba na stanici zadati naredbu kako bismo se mogli transparentno autentificirati: `cmdkey /add:ime-servera /user:admin-account /pass:zaporka`. Nadalje, da biste izbjegli probleme sa spajanjem ako admin stanica i Core server rabe nepovezane DNS-ove, na stanici iskoristite Hosts.



```
Administrator: C:\Windows\system32\cmd.exe
C:\>cmdkey /add:svr1 /user:svr1\admin /pass:K0mpleksanPwd
CMDKEY: Credential added successfully.
```

Pripremamo se za spajanje MMC DNS konzolom s Win 2008 R2 Domain Controllera na stand-alone Core server Svr1 jer na DC-u rabimo drugačiji account.

Administriranje servera RSAT konzolama

Supozicija: Core server i admin stanica su u domeni; sve niže apostrofirane Windows edicije su sa SP1.

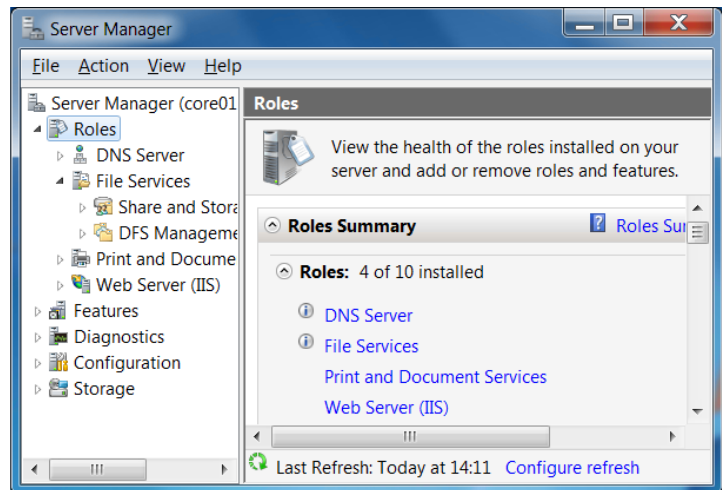
Razlog takve supozicije: Ukoliko admin stanica i Core server nisu u domeni, niže opisani postupci neće biti dovoljni. Tada imamo izbor: ili s HTTP transporta prijeći na HTTPS ili spustiti autentikaciju s Kerberos na Basic. Prvo rješenje (HTTPS) podrazumijeva upućenost u problematiku certifikata; drugo je u praksi besmisleno jer Core server postaje toliko ranjiv da se time ozbiljno narušava svaka politika anti-intruder zaštite servera. Posljedično, u nedomenskom prostoru do daljnjega je praktičnije rabiti standardne MMC konzole i RDC.

U opisu koji slijedi fokusiramo se na Windows 7 kao admin stanicu ali vrlo slično se za uporabu RSAT alata osposobljava i GUI edicija Windows Server 2008 R2. Ključna je razlika u tome što RSAT alate za Windows 7 sa SP1 treba skinuti s MS-ovog sitea, dok su u GUI serverskoj ediciji ti alati već prisutni pod Features kao instalabilna stavka.

1. Instalirati paket na Windows 7 admin stanicu i slijediti upute iz Helpa (da biste se informirali o paketu te u Administrative Tools dobili potrebne MMC konzole i prateće alate).
2. Na admin stanici postaviti servis Windows Remote Management na Automatic i startati ga.
3. Na Core serveru zadati:

```
dism /online /enable-feature /featurename:NetFx2-ServerCore
/featurename:MicrosoftWindowsPowerShell /featurename:ServerManager-
PSH-Cmdlets /featurename:BestPractices-PSH-Cmdlets
```
4. Restartati server, ulogirati se.
5. Zadati: powershell te u PS ljusci zadati:
 - a) `set-executionpolicy -executionpolicy remotesigned`
 - b) `configure-smremoting.ps1 -force -enable`
 - c) `exit`
6. Realizirati preduvjete za uporabu DevMana i DiskMana, kako je opisano u Administriranje servera MMC konzolama.

ServManom možemo administrirati uloge i pregledavati elemente ali ne možemo ih (de)instalirati.



* Ukoliko se RSAT konzolama ne uspijete konektirati na server, jedna od provjera treba biti usmjerena ka konačnom rezultatu djelovanja domenskih GPO na status servisa WinRM i Core vatrozida.

* Za razliku od izvornih Windows 7 ili GUI Server 2008 R2 MMC konzola, RSAT konzole i alati ne mogu raditi bez podrške Windows Remote Management protokola. Iako WinRM rabi HTTP protokol, promet je enkriptiran.

Administriranje servera RDC-om

- Omogućiti spajanje RDC-om:

```
cscript (put)scregedit.wsf /ar 0
```

* Podsjećamo: Scregedit.wsf je u Windows\System32\.

- Provjera učinka naredbe:

```
cscript (put)scregedit.wsf /ar /v, pa ako se u ispisu pojavi izraz View registry settings 0, dobro je.
```

Ako baš moramo pristupiti serveru sa starijim RDC klijentom, obvezni smo zadati naredbu kojom snižavamo security RDP-a (pa to treba izbjegavati):

```
cscript (put)scregedit.wsf /cs 0
```

- Otvoriti serverov firewall za RDC (opcija):

```
netsh advfirewall firewall set rule group="Remote Desktop" new enable=yes
```

- Preuzeti konzolu servera: mstsc /admin.

* Konfiguriranje Core RDC servisa obavlja se s GUI edicije Windows Server 2008 MMC konzolom Terminal Services Configuration.

* Za nesmetan rad na serveru putem RDC protokola važna je i podešenost Remote Desktop Connection **klijenta**. Svakako nastojte rabiti najnoviju verziju RDC klijenta, nadalje, u klijentu uključite Clipboard kako biste mogli kopirati naredbe s admin stanice u komandni redak servera (i obratno).

Uporaba RDC klijenta za spajanje sa Core na druga računala

Ova je funkcionalnost trenutno nepodržana od MS-a. Izbjegavajte instalirati RDC klijenta na javno dostupne Core servere.

| S GUI verzije Windows Server 2008 R2, iz X:\Windows\System32, kopirati na Core u X:\Windows\System32: | S GUI verzije Windows Server 2008 R2, iz X:\Windows\System32\en-us, kopirati na Core u X:\Windows\System32\En-us: |
|---|---|
| d3d10_1.dll | mstsmhst.dll.mui |
| d3d10_1core.dll | mstsmmc.dll.mui |
| dxgi.dll | mstsc.exe.mui |
| msacm32.dll | mstscax.dll.mui |
| mstsc.exe | msacm32.dll.mui |
| mstscax.dll | |
| mstsmhst.dll | |
| mstsmmc.dll | |

Kako (de)instalirati rolu i feature

- Uvid u sve raspoložive i već instalirane uloge (role) i elemente (features):
`dism /online /get-features /format:table`
- Instalirati ulogu DNS Server:
`dism /online /enable-feature /featurename:DNS-Server-Core-Role`
- Deinstalirati ulogu DNS Server:
`dism /online /disable-feature /featurename:DNS-Server-Core-Role`
- Instalirati element Windows Backup
`dism /online /enable-feature /featurename:WindowsServerBackup`
- Deinstalirati element Windows Backup:
`dism /online /disable-feature /featurename:WindowsServerBackup`

* **DISM je case-sensitive naredba.** Više o njoj na [http://technet.microsoft.com/en-us/library/dd772580\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/dd772580(Ws.10).aspx).

* Postoje moduli koji ovise o drugim modulima, npr. Microsoft PowerShell nema smisla instalirati prije instaliranja NetFx2 i 3 modula. Utoliko je prije instaliranja bilo kojeg modula dobro provjeriti ovisnosti naredbom OCLIST pa realizirati sve preduvjete.

* Da biste IIS 7.x pravilno instalirali (rabi se PKGMGR), konfigurirali i održavali, posjećujte mjesta poput <http://www.microsoft.com/windowsserver2008/en/us/iis-technical-resources.aspx> i <http://www.iis.net>.

Osnovne operacije s lokalnim grupama i korisnicima

- Postaviti minimalnu duljinu passworda: `net accounts /minpwlen:broj`
- Kreirati grupu: `net localgroup ime-grupe /add`
- Kreirati korisnika: `net user korisnik * /add`
- Učlaniti korisnika u grupu: `net localgroup ime-grupe /add korisnik`
- Iščlaniti korisnika iz grupe:

```
net localgroup ime-grupe /delete korisnik
```

- Obrisati grupu: net localgroup ime-grupe /delete
- Obrisati korisnika: net user korisnik /delete
- Učlaniti domenskog korisnika u lokalnu grupu (ako je server u domeni):

```
net localgroup ime-grupe /add domena\korisnik
```

- Podaci o lokalnim korisnicima: net user i net user korisnik
- Podaci o lokalnim grupama: net localgroup i net localgroup ime-grupe
- Dopunski podaci o lokalnim korisnicima (uključujući SID):

```
wmic useraccount list /format:list
```

- Dopunski podaci o lokalnim grupama: wmic group list /format:list
- * Politika accounta se pregledava i mijenja naredbom net accounts ili remotely MMC konzolom.
- * Defaultno password mora biti kompleksan.
- * Za grupe koje u imenu imaju razmak rabiti navodnike.

Osnovne operacije sa servisima

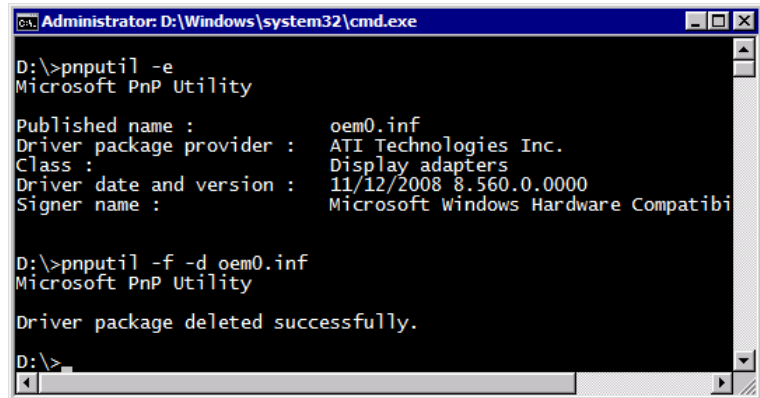
- Pregled bitnih info o svim servisima: sc query ili sc queryex
- Pregled bitnih info za pojedini servis:
sc queryex ime-servisa ili sc qc ime-servisa
- Startati servis: sc start ime-servisa ili net start ime-servisa
- Zaustaviti servis: sc stop ime-servisa ili net stop ime-servisa
- Postaviti servis u stanje Automatic: sc config ime-servisa start= auto
 - * uočite razmak iza znaka jednakosti
- Info o ovisnosti servisa o drugim servisima: sc enumdepend ime-servisa
 - * Ime servisa je u izvješću naredbe sc query(ex) u retku SERVICE_NAME.

Osnovne operacije sa driverima

- Pregled bitnih info o svim aktivnim driverima: sc query type= driver ili driverquery
 - * uočite razmak iza znaka jednakosti
- Pregled bitnih info za pojedini driver:
sc queryex ime-drivera ili sc qc ime-drivera
- Instalirati driver za komponentu za koju Core nema driver:
 - a) kopirati driver u neki folder (npr.: C:\drvinst)
 - b) pnputil -i -a C:\drvinst\driverov.inf
 - c) restart servera
- Ukloniti driver iz sustava:
 - a) pnputil -e

b) pnputil -f -d ime-drivera.inf

Upravo smo deinstalirali driver za grafičku karticu.



```
Administrator: D:\Windows\system32\cmd.exe
D:\>pnputil -e
Microsoft PnP Utility
Published name : oem0.inf
Driver package provider : ATI Technologies Inc.
Class : Display adapters
Driver date and version : 11/12/2008 8.560.0.0000
Signer name : Microsoft Windows Hardware Compatibi

D:\>pnputil -f -d oem0.inf
Microsoft PnP Utility
Driver package deleted successfully.
D:\>
```

- * Driveri se startaju, zaustavljaju i konfiguriraju naredbom SC (kao i servisi).
- * (De)instalaciju drivera PNPUTIL alatom Core bilježi u System log.
- * Windows Server 2008 R2 defaultno **ne** prihvaća digitalno nepotpisane kernel-mode i boot-start drivere. Tako se može desiti da instaliramo neki digitalno nepotpisani driver a OS ga potom odbije pokrenuti, što vrlo lako može destabilizirati sustav kao cjelinu. Da bismo ovakav driver uklonili iz sustava, treba privremeno isključiti značajku Driver Signature Enforcement:

- a) restartati server i tijekom startupa pritisnuti F8
- b) odabrati Advanced Boot Options
- c) odabrati Disable Driver Signature Enforcement
- d) podići Windows i deinstalirati nepotpisani driver

Više o toj temi na

<http://www.microsoft.com/whdc/winlogo/drvsign/kmsigning.msp>. Inače, naredbama SIGVERIF i VERIFIER možemo provjeriti koji su ključni driveri nepotpisani te kao takvi možda destabiliziraju sustav.

Osposobljavanje uređaja za koje Core nema driver

Ponekad Core ne može instalirati low-level SW podršku za neki uređaj, tipično, grafičku ili mrežnu karticu jer ne raspolaže odgovarajućim driverom. Ako nam nije poznat točan model neprepoznatog HW, morat ćemo zaviriti u server ili u tehničke specifikacije ili... ima još načina a jedan od praktičnijih je:

- a) na Core pokrenuti msinfo32
- b) otići u Components -> Problem Devices
- c) dio ili cijeli PNP Device ID problematičnog uređaja upisati u Web tražilicu poput Google
- d) kad tako doznamo model uređaja, na Core instaliramo odgovarajući driver (vidi Osnovne operacije s driverima)

* Ako imamo podešeno udaljeno administriranje servera, Device Manager će nam, karticom Details, dati niz dragocjenih podataka o neprepoznatom uređaju.

* Driver mora biti 64-bitni. U nuždi možemo iskoristiti driver pisan za Windows 7 ili Vistu ali tada je dobro provjeriti stanje sustava naredbama VERIFIER i SFC. Sve dok proizvođači HW ne počnu pisati drivere i njihove instalacije za Core kao specifičnu platformu, dešavat će nam se da se moramo dobrano potruditi kako bismo na Core

instalirali driver kojega smo bezbolno instalirali na GUI ediciju. Poanta: kad nabavljamo fizički server za Core, provjerit ćemo jesu li su driver-paketi za taj HW pisani baš za Core ediciju ili, minimalno, postoje li jasne upute kako potrebne drivere ugnijezditi u Core instalaciju.

* Sve gore rečeno **ne** vrijedi za pisače, vidi Core kao Print Server.

```
Administrator: D:\Windows\system32\cmd.exe
C:\swsetup\sp42394\Packages\Apps\VC8RTx64\vc8redist_x64>vc8redist.msi
C:\swsetup\sp42394\Packages\Drivers\Display\LH6A_INF>pnputil -i -a ch_72993.inf
Microsoft PnP Utility
Processing inf :          CH_72993.inf
Successfully installed the driver on a device on the system.
Driver package added successfully.
Published name :          oem0.inf

Total attempted:          1
Number successfully imported: 1
C:\swsetup\sp42394\Packages\Drivers\Display\LH6A_INF>
```

Primjer drivera koji neće raditi ukoliko nismo realizirali preduvjete, u ovom slučaju morali smo instalirati MS Visual C++ 2005 x64.

Osnove rada s lokalnim firewallom

- Vidjeti opće stanje FW: `netsh advfirewall show allprofiles`
 - Doznati koji je profil aktivan: `netsh advfirewall show currentprofile`
 - Isključiti FW: `netsh advfirewall set allprofiles state off`
 - Uključiti FW: `netsh advfirewall set allprofiles state on`
 - Isključiti/uključiti samo aktivan profil:
`netsh advfirewall set currentprofile state (off | on)`
 - Uključiti zapisivanje svih odbijenih konekcija u svim profilima:
`netsh advfirewall set allprofiles logging droppedconnections enable`
 - Vidjeti stanje pravila (rules):
`netsh advfirewall firewall show rule name=all`
 - Konfigurirati FW da prihvaća RDC konekcije samo kad je aktivan profil Private:
`netsh advfirewall firewall set rule name="remote desktop (tcp-in)" new profile=private enable=yes`
 - Kreirati vlastito pravilo, npr. omogućiti pinganje u svim profilima:
`netsh advfirewall firewall add rule name="Allow-ping4" protocol=icmpv4:8,any dir=in action=allow`
 - Izbrisati vlastito pravilo:
`netsh advfirewall firewall delete rule name="Allow-ping4"`
 - Vratiti inicijalne (defaultne) postavke vatrozida:
`netsh advfirewall set allprofiles firewallpolicy blockinbound,allowoutbound;` potom još zadati: `netsh advfirewall reset`
- * Povratak na inicijalne postavke je zadnje rješenje jer nakon toga moramo ponovo konfigurirati FW.

* Ponašanje vatrozida mijenja se ovisno o nizu faktora, npr. o ulogama servera, jesmo li naredbu formulirali za aktivan profil ili sve profile vatrozida odn. za grupu pravila (rule group) ili pojedinačno pravilo (rule name)... itd. Windows profesionalac mora njime ovladati, dobra osnova je na adresama:

[http://technet.microsoft.com/en-us/library/cc732283\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc732283(WS.10).aspx) i
<http://support.microsoft.com/kb/947709>.

Uvid u Event Viewer i druge logove

- Prikazati imena logova: `wevtutil e1`
- Vidjeti lokaciju i veličinu loga: `wevtutil gl ime-loga`
- Prikazati sadržaj loga: `wevtutil hqe /f:text ime-loga`
- Prikazati određeni događaj iz određenog loga:

```
wevtutil qe ime-loga /q:*[ime-loga[(EventID=broj)]] /f:text
```

- Eksportirati sadržaj loga:

```
wevtutil ep1 ime-loga lokacija-na-disku\ime-arhive.evtx
```

* primjer prikazivanja određenog događaja iz određenog loga (u primjeru je to EventID: 6009 koji se pojavljuje u System logu i posredno omogućuje analizu dinamike restartanja servera):

```
wevtutil qe System /q:*[System[(EventID=6009)]] /f:text
```

Uvid u volumene/particije sustava

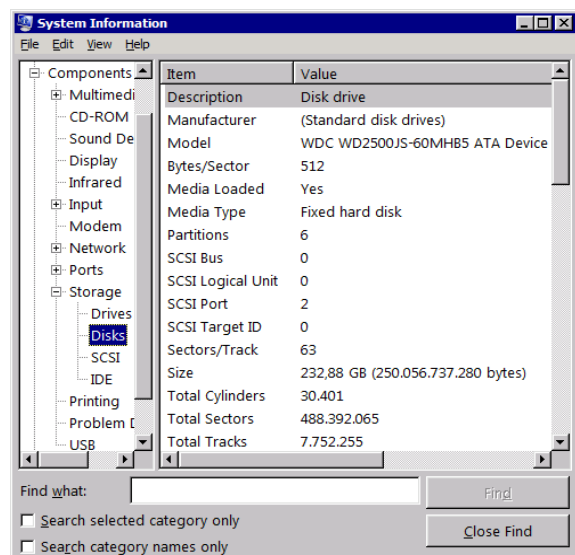
a) `fsutil fsinfo drives`

b) `fsutil fsinfo volumeinfo X:`

* Prvi izvještaj uključuje mapirane mrežne diskove i priključene USB flash memorije; drugi izvještaj se odnosi na značajke datotečnog sustava nekog volumena. Core admin treba dobro upoznati FSUTIL jer je riječ o naredbi koja djeluje na low-level i user-mode razinama datotečnog sustava.

* Da bismo se informirali o fizičkim diskovima sustava i diskovnim kontrolerima, pokrenuti ćemo System Information (msinfo32) i otići u Components > Storage. Alat obrađuje i USB te mrežne (mapirane) diskove. Možemo također instalirati element Windows Server Backup pa zadati `wbadmin get disks` – ova naredba, doduše, ignorira mrežne i USB flash diskove ali uvažava lokalne USB block-type diskove.

MSINFO32 pedantno odrađuje svoj posao informiranja admina o raznim značajkama datotečnih sustava, diskova, kontrolera....



Kreirati i obrisati (primarnu) particiju

DISKPART je interaktivan alat za upravljanje diskovima, volumenima i particijama servera. **OPREZ!** Potencijalno destruktivan alat; treba pažljivo pratiti njegove poruke.

1. Pokrenuti alat: diskpart
2. Informirati se o mogućnostima glede kreiranje volumena ili particije:
help create volume i help create partition
3. Informirati se o prisutnim volumenima: list volume
4. Informirati se o diskovima servera: list disk
5. Odabrati disk s kojim ćemo raditi: select disk broj-diska
6. Informirati se o particijama odabranog diska: list partition
7. Podsjetiti se na pravila kreiranja primarne particije: help create partition primary
8. Kreirati primarnu particiju na odabranom disku:
 - a) ako želimo dodijeliti particiji sav raspoloživi prostor: create partition primary
 - b) ako želimo particiji dodijeliti dio raspoloživog prostora, dodajemo brojčani parametar (jedinica je MB): create partition primary size=broj-u-MB
9. Pridružiti kreiranoj particiji slobodnu oznaku diska:
assign letter=slovo-bez-dvotočke
10. Formatirati particiju: format fs=ntfs label=ime-particije
11. Napustiti DISKPART sučelje: exit

Još uvijek je u fokusu (uoči asterisk) tek kreirana particija G, Partition no 4.

```
DISKPART> list volume

Volume ###  Ltr  Label          Fs          Type          Size         Status       Info
-----
Volume 0    F    XP              NTFS        DVD-ROM       0 B          No Media
Volume 1    C    Win2003EE      NTFS        Partition     49 GB        Healthy      System
Volume 2    D    Win2003EE      NTFS        Partition     39 GB        Healthy
Volume 3    E    WinC           NTFS        Partition     39 GB        Healthy      Boot
* Volume 4  G    Backups        NTFS        Partition     49 GB        Healthy

DISKPART> list partition

Partition ###  Type          Size         Offset
-----
Partition 1    Primary       49 GB        31 KB
Partition 2    Primary       39 GB        49 GB
Partition 3    Primary       39 GB        88 GB
* Partition 4  Primary       49 GB        127 GB

DISKPART>
```

* Naredba prepoznaje i USB flash odn. USB block-type diskove; ako takvi nisu prikazani, iskoristite opciju rescan.

* Podsjećamo da novokreiranoj particiji ne moramo nužno dodijeliti oznaku diska, možemo ju postaviti (mountati) u prazan direktorij prethodno kreiran na jednoj od postojećih particija; tada taj direktorij postaje Volume Mount Point. VMP particijama upravljamo MOUNTVOL alatom.

* Za **brisanje** primarne particije, preporučamo slijed:

help delete partition – dragocjene informacije o brisanju particije

select disk broj = moramo fokusirati disk na kojem je particija

list partition = da vidimo brojevu oznaku particije za brisanje

select partition broj = fokusiramo Diskpart na particiju za brisanje
 delete partition = Diskpart briše particiju bez obzira na to ima li na njoj podataka

* Primarna informacija o GPT, MBR i MSR particijama je na http://www.microsoft.com/whdc/device/storage/GPT_FAQ.msp.

Backupirati System State i podatke

Supozicija: Na disk D: backupirati SystemState i mape C:\Docs1 i C:\Docs2; potom obnoviti dokumente *.txt u mapi C:\Docs1.

1. Instalirati element WindowsServerBackup:

```
dism /online /enable-feature /featurename:WindowsServerBackup
```

2. Startati servis: sc start wbengine

2. Informirati se o diskovima i volumenima servera: wbadmin get disks

3. Backupirati System State:

```
wbadmin start systemstatebackup -backuptarget:d:
```

4. Backupirati mape Docs1 i Docs2:

```
wbadmin start backup -backuptarget:d: -include:c:\docs1,c:\docs2 -vssfull
```

5. Informirati se o backupima smještenim na backup lokaciji:

```
wbadmin get versions -backuptarget:d:
```

6. Obaviti restore mape Docs1:

```
wbadmin start recovery -version:09/01/2009-05:51 -itemtype:File -items:c:\docs1 -recursive
```

Restore mape Docs1; uočite da je procedura obnove sačuvala postojeće datoteke a obnovila izbrisane.

```
Administrator: C:\Windows\system32\cmd.exe
C:\>dir docs1
Volume in drive C is New Volume
Volume Serial Number is 38C1-AB56

Directory of C:\docs1

01.09.2009. 07:51 <DIR> .
01.09.2009. 07:51 <DIR> ..
18.08.2009. 10:22 86.020 2009-09-01 07-51 Copy of fwrules1.log
18.08.2009. 10:25 86.658 2009-09-01 07-51 Copy of fwrules2.log
18.08.2009. 10:39 86.020 2009-09-01 07-51 Copy of fwrules3.log
18.08.2009. 11:22 10.398 2009-09-01 07-51 Copy of okolina.log
20.08.2009. 17:43 31.276 driveri.txt
01.09.2009. 07:39 23.533 drivers.txt
28.08.2009. 09:01 96.499 ffww2.txt
28.08.2009. 09:46 86.019 fw3.txt
28.08.2009. 09:51 96.491 fw6.txt
18.08.2009. 10:22 86.020 fwrules1.log
18.08.2009. 10:25 86.658 fwrules2.log
18.08.2009. 10:39 86.020 fwrules3.log
18.08.2009. 11:22 10.398 okolina.log
01.09.2009. 07:34 16.996 servisi.txt
                14 File(s)            889,006 bytes
                 2 Dir(s) 43,844,161,536 bytes free

C:\>
```

* Backup lokacija može biti lokalni ili mrežni disk; backup lokacija se uvijek definira kao disk (D:, H:, Z: ...); na backup lokaciji naredba sama kreira direktorij WindowsImageBackup i u njega odlaže backup datoteke.

* WBADMIN ignorira lokalno priključene USB flash diskove ali prihvaća USB block-type diskove.

* wadmin enable backup omogućuje brzo kreiranje dnevnih backup zadataka, vidi [http://technet.microsoft.com/en-us/library/cc742130\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc742130(v=ws.10).aspx). Za stvaranje složenijih backup zadataka iskoristit ćemo naredbu SCHEDULETASKS (vidi [http://technet.microsoft.com/en-us/library/cc725744\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc725744(v=ws.10).aspx)), odn. njen GUI ekvivalent Task Scheduler. Potonjeg, dakako, rabimo tako da se MMC konzolom spojimo na Core, vidi Administriranje servera MMC konzolama.

Administrirati Pagefile.sys

Pagefile.sys managirajte lokalno ulogirani na server.

- Uvid u stanje Pagefile.sys:

```
wmic pagefile list /format:list i systeminfo
```

- Spriječiti OS da samostalno upravlja Pagefileom:

a) wmic computersystem where name="ime-servera" set AutomaticManagedPagefile=False

b) restartati server

- Premjestiti Pagefile.sys na D particiju i fiksirati veličinu na 3333 MB:

a) wmic pagefileset where name="D:\\pagefile.sys" set InitialSize=3333,MaximumSize=3333

b) restartati server

* dir /o/a = vidimo Pagefile na datotečnom sustavu

* attrib -a -s -h Pagefile.sys = skidamo joj attribute ako ju treba obrisati

Postaviti proxy server

a) osnovni oblik naredbe: netsh winhttp set proxy proxy-server:port

b) prošireni oblik naredbe: netsh winhttp set proxy proxy-server=proxy-server:port bypass-list="*.DNS-sufiks1;*.DNS-sufiks2;..."

c) vidjeti aktualnu postavku: netsh winhttp show proxy

* Drugu naredbu rabimo kako bismo serveru pokazali za koje DNS sufikse treba zaobići proxy server (to su redovito sufiksi lokalne mreže).

* Core trenutno ne podržava autenticiranje na proxy server, vidi KB 921471.

Proizvoljno zaustaviti proces

```
taskkill /PID ID-procesa
```

* ID procesa može se vidjeti naredbama tasklist ili sc queryex ili TaskManom.

* Postoje procesi koje nećemo moći prekinuti bez opcije /F (force). Utoliko je naredba Taskkill važna jer i TaskMan ima naredbu za prekidanje procesa ali bez mogućnosti forsiranja.

Pokrenuti Task Manager

```
taskmgr
```

* **Ne zaboravite** da TaskMan nije samo za monitoriranje servera, dobro će poslužiti i kao alat za upravljanje procesima – pokretanje, zaustavljanje, postavljanje prioriteta i angažiranih procesora; također, koristan je za start/stop operacije nad aplikacijama, servisima i korisnicima te, naposljetku, za praćenje mrežnog prometa. Na Core serveru je izrazito praktičan i GUI alat MSINFO32.

Defragmentirati disk

Preporučljivo je prije defragmentiranja upogoniti CHKDSK ili CHKNTFS da provjeri stanje datotečnog sustava na volumenima koje planiramo defragmentirati, npr. `chkdsk d:.` Ako naredba ukaže na nepravilnosti u strukturi datotečnog sustava, defragmentaciju odgađamo jer tada je imperativ backupirati taj volumen i riješiti uočene greške.

- Defragmentirati jedan volumen s konsolidiranjem slobodnog prostora uz praćenje aktivnosti i izvješće: `defrag X: /u /v /x`
- Defragmentirati sve volumene s konsolidiranjem slobodnog prostora i izvješćem: `defrag /c /v /x`

* Razumno je defragmentirati diskove servera kad su najmanje opterećeni, a tada možemo i ubrzati defragmentaciju opcijom /H, njome sustav daje Defragu kao procesu viši stupanj prioriteta.

(De)instalirati MSU paket

- Instalirati: `wusa ime-paketa.msu`
 - Ukloniti: `wusa ime-paketa.msu /uninstall`
 - Uvid u instalirane .msu pakete (zacrpe, alate, module...): `wmic qfe list format:list ||| systeminfo`.
- * Ističemo opcije /quiet, /forcerestart i /expand, vidi help WUSA naredbe.
* (De)instalaciju MSU paketa Core bilježi u Setup log.
* WUSA možemo rabiti za primjenu pojedinačnih zakrpi na server.

(De)instalirati MSI paket

- Instalirati: `msiexec /i ime-paketa.msi`
 - Deinstalirati: `msiexec /uninstall ime-paketa.msi`
 - Informacije o instaliranim MSI paketima: `wmic product list /format:list`
- * Ako (de)instalacija paketa pada, ili (de)instaliravamo pomoću skripte, dodati naredbi opciju /quiet. Microsoft preporuča i uporabu /qb opcije.
* (De)instalaciju MSI paketa Core bilježi u Application log.

Raspakirati CAB paket

- Uvid u paket: `expand -d ime-paketa.cab`
 - Raspakirati kompletan paket: `expand -f:* ime-paketa.cab ciljni-dir`
- * Opcijom -F možemo iz paketa izvlačiti i pojedinačne datoteke.
* Naredbom možemo raspakirati i pojedinačno komprimirane datoteke, npr.:

```
expand netapi32.dll_ netapi32.dll
```

Izmijeniti display postavke

Trenutno Core ne raspolaže jednostavnim načinom postavljanja rezolucije i dubine boja. Iako postoji mogućnost postavljanja željene rezolucije ručnom izmjenom određenih parametara u Registry bazi, praktičnije je iskoristiti alat Core Configurator. Rečeno vrijedi i da podešavanje Screen Saver-a.

Disablirati User Account Control

Defaultno je UAC na Core disabliran, ali ako se nehotice enablira (što se može desiti kad se na njega neplanirano primijeni neka domenska GPO) gotovo je nemoguće raditi na serveru. Tada treba alatima reg.exe ili regedit.exe stavku EnableLUA postaviti na 0. EnableLUA je u HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.

Podesiti startup sekvencu

Ako na računalu već imamo neku Windows 2008 instalaciju, pa instaliramo i Core (jasno, na drugu particiju), u startnom izborniku će obje instalacije imati isto ime. Da bismo ih razlikovali, moramo jednu instalaciju preimenovati.

a) zadamo samo bcdedit, da bismo vidjeli ID OS-a kojeg želimo preimenovati

b) zadamo: `bcdedit /set {ID-OS-a} description "opisno-ime"`

Iskoristili smo izvješće BCDEDIT naredbe da bismo svakoj instalaciji dodijelili adekvatno ime.

```
Administrator: C:\Windows\system32\cmd.exe
locale                en-US
inherit               {bootloadersettings}
osdevice              partition=D:
systemroot            \windows
resumeobject          {a46f9af3-98bf-11de-9954-f6782c794374}
nx                   OptOut

Windows Boot Loader
-----
identifier            {current}
device                partition=C:
path                  \windows\system32\winload.exe
description            Windows Server 2008 R2
locale                en-US
inherit               {bootloadersettings}
recoverysequence      {a46f9af1-98bf-11de-9954-f6782c794374}
recoveryenabled       Yes
osdevice              partition=C:
systemroot            \windows
resumeobject          {a46f9aef-98bf-11de-9954-f6782c794374}
nx                   OptOut

C:\>bcdedit /set {current} description "Win R2 RTM - GUI"
The operation completed successfully.

C:\>bcdedit /set {default} description "Win R2 RTM - CORE"
The operation completed successfully.

C:\>
```

* Sa BCDEDIT možemo mijenjati niz drugih parametara, tipično, koji će se OS defaultno učitati te vremenski interval prikazivanja boot izbornika. Dokument koji podrobno opisuje ovaj alat je (trenutno) na http://www.microsoft.com/whdc/system/platform/firmware/bcdedit_ref.msp.

Anti-intruder zaštita servera

Glede razine otpornosti na napade i provale s mreže, Core edicija je u startu superiornija GUI ediciji Windowsa. Ipak, i nadalje ćemo najviši stupanj zaštite

servera postići respektirajući Microsoftove Security Best Practices i Solution Accelerators, poput onih na adresama [http://technet.microsoft.com/en-us/library/cc772066\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc772066(WS.10).aspx) i [http://technet.microsoft.com/hr-hr/library/cc514539\(en-us\).aspx](http://technet.microsoft.com/hr-hr/library/cc514539(en-us).aspx).

Ako je Core instalacija u domeni, security postavljamo primjenom domenskih GPO, kombinirajući GPO i security predloške upakirane u Security Compliance Management Toolkit za Windows 2008 R2 (vidi gornji link).

Ako je server stand-alone, za konfiguriranje Local Security Policy moramo rabiti naredbu SECEDIT pri čemu možemo, dakako, iskoristiti spomenute security predloške.

Core nema SCWCMD, komandnolinijsku verziju Security Configuration Wizard alata, isti je slučaj i s MBSA alatom.

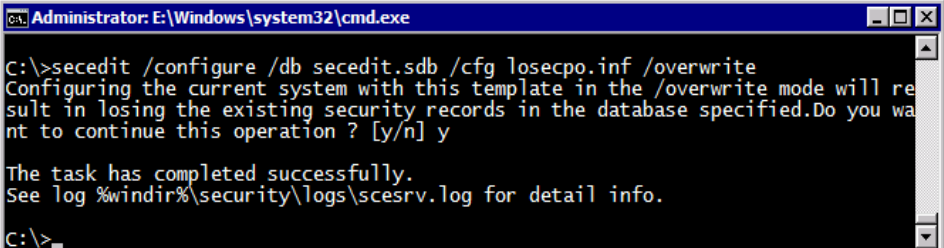
Najvažnije postavke, Password Policy i Audit Policy, možete redefinirati alatima NET ACCOUNTS i AUDITPOL, respektivno. Ukoliko ipak morate mijenjati postavke nedostupne navedenim naredbama, slijedite niže izloženu proceduru.

Supozicija: Server je stand-alone, OS je pravilno instaliran na disk C: i u njegovom rootu smo (prompt je C:\>); modificiramo lokalnu security politiku.

OPREZ! Loše odrađena izmjena security postavki može onesposobiti aplikacije i servise.

1. Exportirati aktualnu LSP: `secedit /export /cfg losecpo.inf /log losecpo.log`
 2. Losecpo.inf učitati u Notepad, editirati ju prema potrebama i spremiti u C:\.
 3. `secedit /import /db secedit.sdb /cfg c:\losecpo.inf /overwrite /quiet`
 4. `secedit /configure /db secedit.sdb /cfg c:\losecpo.inf /overwrite /quiet`
 5. `gpupdate /force`
- * Brza provjera: `auditpol /get /category:* i net accounts.`
 - * Temeljita provjera: ponovo exportirati LSP i proučiti je; pregledati `scesrv.log`; pregledati EV -> System.
 - * `gpresult /v` – dragocjen alat za domenski prostor, koristan i u workgroup sredini.
 - * Opis SECEDIT naredbe: [http://technet.microsoft.com/en-us/library/cc742472\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc742472(WS.10).aspx).

Primijenili smo modificiranu LSP.



```
Administrator: E:\Windows\system32\cmd.exe
C:\>secedit /configure /db secedit.sdb /cfg losecpo.inf /overwrite
Configuring the current system with this template in the /overwrite mode will result in losing the existing security records in the database specified. Do you want to continue this operation? [y/n] y
The task has completed successfully.
See log %windir%\security\logs\scesrv.log for detail info.
C:\>
```

Glede zaštite servera od raznog zloćudnog softvera, treba provjeriti kompatibilnost odabranog rješenja s Core edicijom. Aktualna izvedba Windows Defendera nije podržana ali možemo rabiti Malicious SW Removal Tool. Ukoliko nemamo nikakav zaštitni software na Core instalaciji, možemo se WinExploreroom spojiti na disk Core servera s admin stanice pa s nje odraditi skeniranje.

Raspolažemo i alatima poput SIGVERIF i SFC (korisni su za kontrolu svih datoteka važnih sustavu) ili naredbama poput netstat -a -b (pokazuje imena lokalnih procesa koji uspostavljaju konekcije s hostovima na mreži) i auditpol /set /subcategory:"logon" /success:enable /failure:enable (uključuje praćenje svih logon aktivnosti); tu su i route print, pathping, arp -a, potom TaskMan sa pregledom procesa te NetMon za analizu mrežnog prometa... – opisanim alatima i postupcima možemo indirektno zaključiti da li je server izložen nekim malicioznim radnjama. Promjene u ponašanju servera najlakše ćemo uočiti ako smo pravovremeno napravili baseline snimku servera, što je ujedno jedna od nezaobilaznih obveza administratora.

Već uobičajena mjera zaštite Windows servera je isključivanje NetBIOS interfeaca:

- a) wmic nicconfig get caption,index,TcpipNetbiosOptions - za detekciju indexa mrežnog sučelja
- b) wmic nicconfig where index=x call SetTcpipNetbios 2 - za disabliranje NetBIOSa na tom mrežnom sučelju

U području fizičke zaštite nema nikakvih specifičnosti u odnosu na GUI ediciju, Core je ipak samo Windows server.

Pristupiti Web resursima sa Core servera

Instalirati i podesiti Web preglednik poput Opere ili Firefoxa - odaberite Custom instalaciju preglednika i **isključite** opcije za kreiranje prečaca na raznim lokacijama radne površine. Glede lokalnog vatrozida, defaultno je dopušten HTTP-HTTPS odlazni promet.

Core kao File Server

Supozicija: Na stand-alone serveru bez drugih uloga obaviti dijeljenje mape F:\Fakture tako da na nju lokalna grupa Users ima pravo Read a lokalna grupa Fakturisti pravo Change.

Administriranje korisničkih računa i grupa opisano je pod Osnovne operacije s lokalnim grupama i korisnicima.

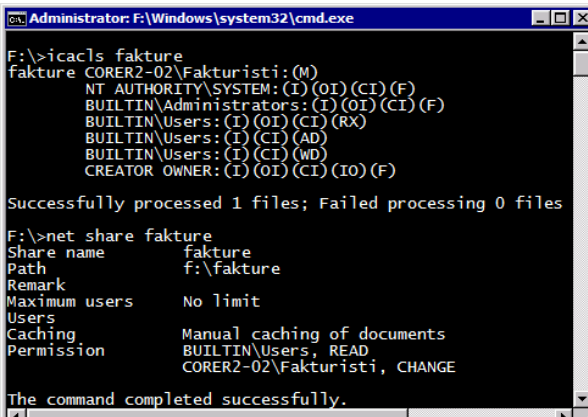
1. Instalirati rolu File Server:

```
dism /online /enable-feature /featurename:CoreFileServer
```

2. Postaviti primjerena prava na NTFS razini: icacls F:\Fakture /grant Fakturisti:M

3. Kreirati share: net share F:\Fakture=f:\Fakture /grant:Users,Read /grant:Fakturisti,Change

Provjeravamo prava na NTFS i file-share razinama.



```
Administrator: F:\Windows\system32\cmd.exe
F:\>icacls fakture
fakture CORER2-02\Fakturisti:(M)
NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
BUILTIN\Administrators:(I)(OI)(CI)(F)
BUILTIN\Users:(I)(OI)(CI)(RX)
BUILTIN\Users:(I)(CI)(AD)
BUILTIN\Users:(I)(CI)(WD)
CREATOR OWNER:(I)(OI)(CI)(IO)(F)

Successfully processed 1 files; Failed processing 0 files

F:\>net share fakture
Share name          fakture
Path                f:\fakture
Remark
Maximum users      No limit
Users
Caching            Manual caching of documents
Permission         BUILTIN\Users, READ
                  CORER2-02\Fakturisti, CHANGE

The command completed successfully.
```

* Posljedica gornjih koraka je otvaranje portova za File and Printer Sharing promet u aktivnom profilu firewalla što će, posljedično, omogućiti članu grupe Fakturisti da može na share odlagati dokumente, mijenjati ih i brisati; član grupe Users iste može samo čitati.

* Zatreba li, naredbama `fsutil quota enforce` i `fsutil quota modify` možemo postaviti diskovne kvote za pojedinačnog korisnika ili grupu, potom pratiti stanje opcijama `track` i `violations`. Auditing konfiguriramo AUDITPOL naredbom, npr.: `auditpol /set /subcategory:"file system" /success:enable /failure:enable`.

* Za pristup dijeljenom resursu na Windows računalu **nije** potreban NetBIOS over TCP/IP protokol. Dakle, ako disabliramo NBT protokol (ili konekcije na port TCP 139 zabranimo na FW), SMB promet će se transparentno preusmjeriti na TCP 445. Disablirati NetBIOS over TCP/IP možemo `wmic nicconfig` naredbom ili Regedit alatom, opisujemo potonji način:

a) `regedit`

b) `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetBT\ -> Parameters\Interfaces`

c) u popisu `Tcpip_GUID` mrežnih sučelja odabrati ciljnu stavku i parametar `NetbiosOptions` postaviti na **2**

d) nakon restarta servera ili `disable-enable` mrežnog sučelja, `ipconfig /all` će pokazati da je NetBIOS disabliran a `netstat -ano -p tcp` neće prikazati port TCP 139

* Povezano s gornjim, budući da je defaultno na vatrozidu Core servera omogućen promet kroz TCP port 445, odmah nakon instalacije Core servera možemo se, bez ikakvih dodatnih radnji (ali rabeći admin account definiran na Core serveru), spojiti s druge Windows instalacije na administrativne shareove poput `C$` i `Admin$`. Tako razne operacije s mapama i datotekama na Core serveru možemo odrađivati kroz GUI sučelje, Windows Explorerom.

* Uloga File Server, kojom Core instalaciju opremamo raznim admin alatima, **nije** neophodna ukoliko tek sporadično rabimo dijeljene mape na Core serveru. Dakle, i bez nje možemo kreirati file-share resurse, čime se ujedno otvaraju portovi za F&P Sharing u aktivnom profilu vatrozida.

* Kako bi se što lakše ucijepile u Windows okolinu, opremljenije Linux distribucije out-of-the-box podržavaju mape dijeljene na Windows računalu – dobrodošla info ako Windows shareima moraju pristupati i računala pod Linux OS-om.

* **OPREZ!** Nakon skidanja uloge CoreFileServer i ukidanja dijeljenih mapa, na lokalnom FW ostaju otvoreni portovi za File and Print Sharing inbound promet. Ukoliko zaista nemamo namjeru server nadalje rabiti kao File ili Print server, zadat ćemo naredbu: `netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=no`.

* **OPREZ!** Core nema Recycle Bin.

Core kao Print Server

Supozicija: Stand-alone serveru bez drugih uloga dodjeljujemo ulogu Print Server.

1. Instalirati Print Server ulogu:

```
dism /online /enable-feature /featurename:Printing-ServerCore-Role
```

2. Instalirati podršku za 32-bitne drivere odn. klijente:

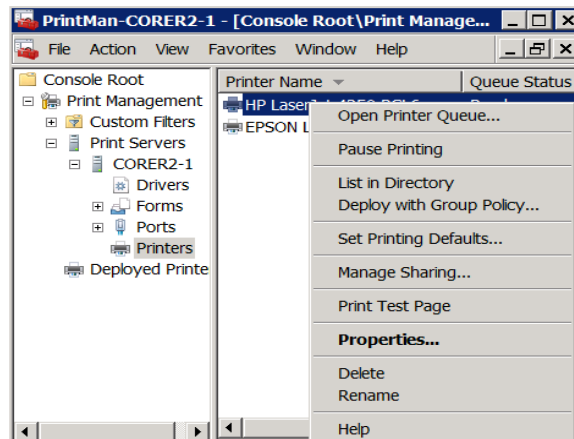
```
dism /online /enable-feature /featurename:Printing-ServerCore-Role-WOW64
```

3. Core vatrozid otvoriti za File & Printer Sharing promet: netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=yes

4. S Core servera pingom provjeriti pristupačnost mrežnog pisača.

5. Na admin stanici iskoristiti MMC snap-in Print Management kako bismo na Core instalirali potrebne drivere (rabimo funkciju Drivers), potom i definirali pisače (rabimo funkciju Printers).

Definirane pisače nadalje administriramo s admin stanice.



* Korak 3 nije potreban ukoliko smo ranije kreirali dijeljene mape.

* Mrežni pisači redovito rabe TCP/IP protokol, stoga tijekom definiranja mrežnog pisača treba odabrati opciju Add a TCP/IP or Web services printer.

* Postoje print-drivers paketi koje nije moguće raspakirati bez instaliranja. U tom slučaju instaliramo taj driver na admin stanicu, potom se PrintMan konzolom spojimo na Core i dodamo mu driver kroz Additional Drivers dijaloški okvir. Osobno preferiram kvazi-instalaciju na admin stanicu tj. „instaliram“ driver sve do pojavljivanja Windows čarobnjaka za instalaciju (Add Printer) – u tom je trenutku paket već raspakiran u neki direktorij – i tada se prebacim na Print Management konzolu pa kroz nju napadnem direktorij s driverom. U oba slučaja treba obratiti pozornost na arhitekturu procesora (x86 ili x64) admin stanice, kako bismo mogli instalirati driver koji je zaista potreban Core serveru.

* Core Print Server opslužit će i unixoidne klijente ako iskoristimo element Printing-LPDPrintService. Pritom, dobro je znati sljedeće: popularnije Linux distribucije imaju ugrađenu podršku za Windows kao File & Print server i tada server ne treba opremiti za opsluživanje Linux računala.

* Za disabliranje NetBIOS protokola vidi Osposobiti Core za ulogu File Server.

Core kao drugi DNS server

Supozicija: Primarni DNS je GUI edicija Windows 2008 R2; taj server je autoritativan za domenu corp.hr. Podižemo Core kao sekundarni DNS. Oba su servera stand-alone, Internet-facing (dakle, smješteni su u DMZ segmentu korporativne mreže).

! U stvarnosti, isplati se primarni DNS (prisjetimo se da taj, za razliku od sekundarnih, ima upisivu bazu) dignuti na nekoj VM minimalnih gabarita a na Internetu oglasiti (dakle, CARNetovoj DNS službi prijaviti) dva sekundarna Core DNS servera.

a) Ispravno konfigurirati DNS servis na GUI ediciji, uključujući: u karticu Name Servers upisati FQDN i IP adresu sekundarnog servera; također, karticom Zone Transfers omogućiti transfer zone ka svim DNS serverima prisutnim u Name servers kartici te uključiti notifikaciju.

b) Postaviti Core serveru njegovu vlastitu IP adresu kao prvi DNS (IP adresa primarnog DNS-a upisuje se kao drugi, sekundarni DNS), potom i Primary DNS Suffix – vidi Postaviti statičke TCP/IP v4 i druge mrežne parametre.

c) Restart (opcija).

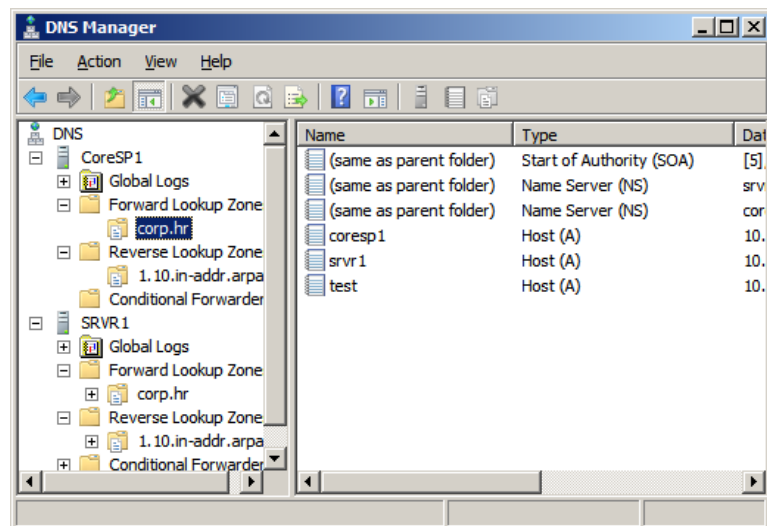
d) Instalirati DNS rolu:

```
dism /online /enable-feature /featurename:DNS-Server-Core-Role
```

* Na lokalnom FW se otvaraju portovi za DNS promet i pristup serveru MMC konzolom.

e) Slijedi konfiguriranje DNS servisa na Core serveru, prvenstveno kreiranje sekundarne domene corp.hr i postavljenje primarnog DNS-a kao tzv. Master servera. Glede alata kojime ćemo to obaviti, imamo izbor: ili rabiti CLI alat DNSCMD ili, praktičnije, spojiti se s primarnog DNS-a MMC konzolom i raditi u grafičkom sučelju. Potonji je način obrađen u cjelini Administriranje servera MMC konzolama.

S Windows 2008 R2 GUI edicije (SRVR1) administriramo Core R2 DNS MMC konzolom.



* Kad je Windows 2008 R2 DNS konfiguriran da rabi root hints, a unatoč dobroj internet vezi ne može resolvirati root servere (i/ili neke druge well-known internet hostove), zadati `dnscmd /config /EnableEDNSProbes 0`.

* Ako je DNS na IPv4 mreži, preporuka je disablrati IPv6 (vidi <http://support.microsoft.com/kb/929852>) ili namjestiti DNS da sluša samo na IPv4 adresi.

* Kad podižete Windows DNS na nesigurnoj mreži, odradite hardening servera, vidi Anti-intruder zaštita servera. Specifično za Internet-facing DNS, mudro ćemo postupiti ako, nakon obavljene konfiguracije Core servera DNS MMC konzolom, na firewallu oba DNS servera zabranimo dolazni promet ka DNS servisu kroz TCP portove RPC i RPC Endpoint Mapper (na znanje – time si ujedno onemogućujemo pristup DNS servisu standardnom DNS MMC konzolom); nadalje, zasigurno ćemo htjeti isključiti mogućnost dinamičkog upisivanja hostova.

* Glede DNSCMD – na Internetu je puno primjera, odličan početak je na [http://technet.microsoft.com/en-us/library/cc772069\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc772069(WS.10).aspx).

Core kao drugi Domain Controller

Supozicija: Već postoji tzv. glavni Domain Controller (taj je FSMO master, GC...), dignut na Windows 2008 R2 GUI ediciji. Na tom prvom DC je djelatna i DNS, zone su AD-integrirane, Core je kao DNS postavljen u Name Servers, zone su podešene za transfer na servere prisutne u Name Servers kartici... i sl. Forest je jednodomenski, u R2 native modu. Glede Core servera – „friško“ instaliran, punopravni je član domene.

1. Postaviti Core serveru prvi Domain Controller kao Preferred DNS; Alternate DNS treba biti sam sebi, vidi Postaviti statičke TCP/IP v4 i druge mrežne parametre.
 2. Instalirati NetFx-2, NetFx-3, potom i DNS ulogu:


```
dism /online /enable-feature /featurename:NetFx2-ServerCore
dism /online /enable-feature /featurename:NetFx3-ServerCore
dism /online /enable-feature /featurename:DNS-Server-Core-Role
```
 3. S prvog DC-a, snap-inom DNS spojiti se na Core i dotjerati DNS servis, npr. ukloniti root DNS servere, podesiti Scavenging, postaviti hijerarhijski nadređene DNS servere...
 4. Instalirati AD binaries:


```
dism /online /enable-feature /featurename:DirectoryServices-
DomainController-ServerFoundation
```
 5. Kreirati direktorije Sysvol, NTDS, Logs (npr., u C:\).
 6. U Notepadu kreirati datoteku dc2answers.txt sa sljedećim sadržajem:

! Sve što **nije** u <zagradama> zahtjevana je vrijednost, **ne** mijenjati to!
Vrijednosti izraza u <zagradama> upisivati **bez** tih zagrada!

```
[DCINSTALL]
UserName=<domena\administrator>
UserDomain=<NetBIOS-ime-domene>
Password=<K0mpleksna-Zap0rka>
SiteName=<Ime-Sitea>
ReplicaOrNewDomain=replica
ReplicaDomainDNSName=<FQDN-ime-domene>
DatabasePath=c:\NTDS
LogPath=c:\Logs
SYSVOLPath=c:\Sysvol
InstallDNS=yes
ConfirmGC=yes
SafeModeAdminPassword=<K0mpleksna-Zap0rka>
RebootOnCompletion=yes
```
 7. Smjestiti dc2answers.txt u C:\.
 8. Pozicionirani u C:\> zadajemo: `dcpromo /unattend:dc2answers.txt`
 9. Nakon restarta, postaviti Core serveru sebe kao primarni DNS a glavni DC kao sekundarni DNS; uvjeriti se da je na zoni uključena opcija za dynamic update.
- * Nakon instalacije Domain Controller funkcionalnosti, za provjeru konzistentnosti sustava iskoristit ćemo alate poput DCDIAG, NSLOOKUP, REPADMIN... te, jasno, MMC konzole na GUI DC-u.
- * DNS i Domain Controller servisi sami surađuju sa svojim lokalnim firewallom, stoga, načelno, nepotrebne su bilo kakve intervencije na toj razini.

* Svi vi skloni PowerShellu, prisjetite se da Core ima zaseban modul ActiveDirectory-PowerShell kojega možete instalirati te rabiti za managiranje Active Directory servisa. Brojne funkcionalnosti ovog modula opisane su na adresi <http://technet.microsoft.com/en-us/library/ee617195.aspx>.

Core kao IP router

Core kao router službeno je nepodržan od Microsofta. Nije moguća uporaba naredbe **netsh routing** s njenim brojnim opcijama. S druge strane, Core besprijekorno odrađuje posao preusmjeravanje paketa između IP mreža, lokalnim FW može se filtrirati promet... i dobro je znati kako ga upogoniti kao LAN router.

- instalirati i konfigurirati minimalno dvije mrežne kartice
- regedit -> HKLM -> CCS -> services -> Tcpip -> Parameters -> IPEnableRouter postaviti na **1**
- restart

* Mrežnim karticama nemojte postavljati Default Gateway.

* Dobro je znati da se na Coreu može rabiti MS-ov Network Monitor x64, samo odaberite Complete tip instalacije.

Core povezuje dvije mreže; uočite stalnu rutu prema mreži na kojoj nije fizički prisutan.

```

Administrator: E:\Windows\system32\cmd.exe
IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface
-----
10.1.190.2                 255.255.222.0   10.1.200.10     10.1.203.139
10.1.200.0                 255.255.222.0   On-link        10.1.203.139
10.1.203.139              255.255.255.255 On-link        10.1.203.139
10.1.203.255              255.255.255.255 On-link        10.1.203.139
127.0.0.0                 255.0.0.0       On-link        127.0.0.1
127.0.0.1                 255.255.255.255 On-link        127.0.0.1
127.255.255.255          255.255.255.255 On-link        127.0.0.1
192.168.10.0             255.255.255.0   On-link        192.168.10.1
192.168.10.1             255.255.255.255 On-link        192.168.10.1
192.168.10.255          255.255.255.255 On-link        192.168.10.1
224.0.0.0                 240.0.0.0       On-link        127.0.0.1
224.0.0.0                 240.0.0.0       On-link        192.168.10.1
224.0.0.0                 240.0.0.0       On-link        10.1.203.139
255.255.255.255          255.255.255.255 On-link        127.0.0.1
255.255.255.255          255.255.255.255 On-link        192.168.10.1
255.255.255.255          255.255.255.255 On-link        10.1.203.139

Persistent Routes:
Network Address        Netmask          Gateway Address  Metric
-----
10.1.190.2             255.255.252.0   10.1.200.10     1
  
```

Core i Hyper-V

Hyper-V za Microsoft nije samo još jedan od servisa Windows Server distribucije jer ga koristi kao infrastrukturnu osnovicu za tucet vlastitih komercijalnih usluga, preferirajući pri tome upravo Core ediciju kao Hyper-V host. Zbog toga temu „Core i Hyper-V“ nema smisla obrađivati u priručniku ovakvog profila jer sam Microsoft to odlično odrađuje na svojim službenim stranicama, vidi <http://www.microsoft.com/windowsserver2008/en-us/hyperv-technical-resources.aspx>.

Ovdje skrećemo pozornost na **besplatan** produkt Microsoft Hyper-V Server 2008 R2 SP1, softverski paket s dvije komponente: Windows Core edicijom i MS virtualizacijskim hipervizorom. Kao takav, besplatan, produkt ima i neka ograničenja u odnosu na komercijalnu Hyper-V inačicu no, budući da raspolaže administratorima važnim značajkama poput Host Clustering, Live Migration,

Dynamic Memory..., svakako je riječ o snažnom i visoko uporabljivom virtualizacijskom rješenju – o čemu se točno radi možete vidjeti u referentnoj tablici na adresi <http://www.microsoft.com/hyper-v-server/en/us/default.aspx>.

Core i IIS 7.5

Sve što trebate naći ćete na <http://technet.microsoft.com/en-us/library/cc771209.aspx> (instalacija) i <http://www.iis.net/> (sve ostale teme).

Podsjećamo na poglavlje Administriranje servera MMC konzolama jer je u njemu opisano podešavanje servera i stanice za udaljeno administriranje IIS-a.

Microsoftov security best practices preporuča Core ediciju kao osnovicu Internet-facing IIS-a.

V. PREGLED KOMANDNOLINIJSKIH NAREDBI

Slijedi **probrani** skup manje-više nezaobilaznih alata-naredbi. Svi niže navedeni alati dolaze s originalnom distribucijom Windows Core R2; nekoliko njih sastavni je dio **Cmd** ljuske; većinom su u \System32. Iako nije vezan striktno za Core, URL [http://technet.microsoft.com/hr-hr/library/cc754340\(en-us,WS.10\).aspx](http://technet.microsoft.com/hr-hr/library/cc754340(en-us,WS.10).aspx) publicira dragocjene informacije o Windows Server naredbama.

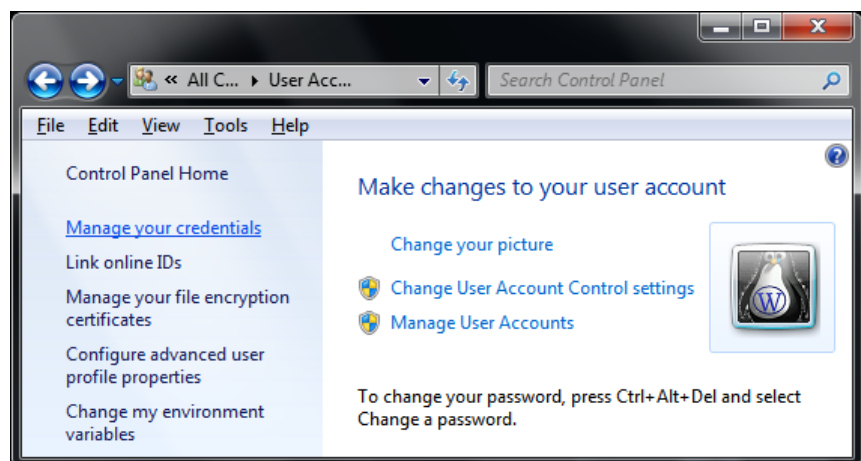
Instalacijom komponenata povećava se fond komandnolinijskih alata, npr. rola Domain Name System omogućit će nam uporabu DNSCMD naredbe, IIS donosi APPCMD a Core Backup naredbu WBADMIN.... itd. Dodatnim alatima opskrbit ćemo se instalirajući odgovarajuće administrativne pakete, npr. SysInternals Suite. Moćna komandna konzola i skriptni jezik Powershell zasebna je tema, vidi [http://technet.microsoft.com/hr-hr/library/cc731851\(en-us,WS.10\).aspx](http://technet.microsoft.com/hr-hr/library/cc731851(en-us,WS.10).aspx).

Poglavlje završava pregledom korisnih dodatnih alata.

* * *

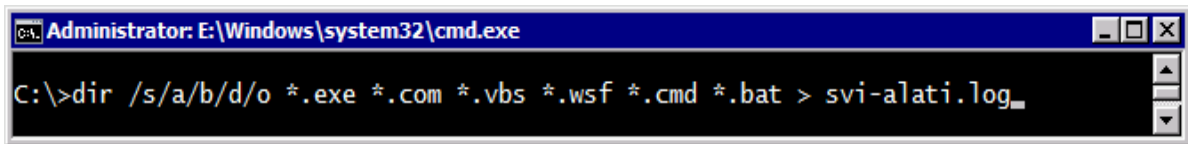
- * **ARP** = za administriranje tablice MAC adresa mrežnih hostova
- * **ATTRIB** = za administriranje A-H-I-R-S atributa datoteka i mapa
- * **AUDITPOL** = za upravljanje auditing politikama
- * **BCDEDIT** = Boot Configuration Data editor, konfigurator startup sekvence
- * **CERTREQ** i **CERTUTIL** – za administriranje digitalnih certifikata
- * **CHDIR** ili **CD** = za kretanje po strukturi direktorija (mapa) na disku
- * **CHKDSK** = u read-only modu korisne info o stanju volumena, korisna je i CHKNTFS
- * **CMDKEY** = upravljanje accountima za pristup mrežnim resursima / računalima

Windows 7 ima i GUI ekvivalent naredbi **CMDKEY**, *Manage your credentials*.



- * **COPY** = kopira datoteke, vidi i XCOPY
- * **DCGPOFIX** = obnavlja defaultne Domain i Domain Controller politike
- * **DCPROMO** = podiže Domain Controller funkcionalnost
- * **DEFRAG** = za defragmentiranje volumena/particija
- * **DEL** = briše (ne)zaštićene datoteke

- * **DIR** = razne vrste ispisa podataka o mapama i datotekama

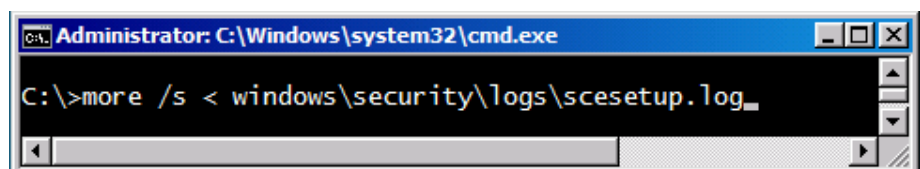


```
Administrator: E:\Windows\system32\cmd.exe
C:\>dir /s/a/b/d/o *.exe *.com *.vbs *.wsf *.cmd *.bat > svi-alati.log_
```

Stvaramo popis svih alata koji se nalaze na disku C:.

- * **DISM** = za pregledavanje i (de)instaliranje uloga (roles) i elemenata (features); za upravljanje WIM paketima
- * **DISKPART** = za upravljanje volumenima / particijama, vidi KB 325590
- * **DOSKEY** = unaprijeđuje rad u komandnoj liniji
- * **DRIVERQUERY** = prikazuje instalirane / aktivne drivere
- * **ECHO >>** = omogućuje dodavanje nekog teksta na kraj tekstualne datoteke direktno iz komandnog retka
- * **ESENTUTL** = za upravljanje ESE bazama
- * **EXPAND** = ekstrahira datoteke iz CAB i MSU kontejnera
- * **FINDSTR** = traga za specificiranim stringom u tekstualnim datotekama
- * **FORMAT** = formatira particiju tj. na RAW particiji stvara datotečni sustav
- * **FSUTIL** = za upravljanje datotečnim sustavom i informiranje o njemu
- * **FTP** = FTP klijent
- * **GPRESULT, GPOUPDATE** = za kontrolu primjene domenskih ili lokalnih GPO
- * **HELP** = pomoć za uporabu naredbi u CLI okolini
- * **ICACLS** = za upravljanje Access Control Listama odn. pravima na datotečni sustav
- * **INTL.CPL** = za podešavanje regionalnih postavki sustava (GUI), vidi i TZUTIL
- * **IPCONFIG** = za upravljanje mrežnim parametrima računala
- * **ISCSICLI** = MS-ov iSCSI inicijator za spajanje na iSCSI diskove (2008 R2 GUI edicija ima iSNS servis), vidi <http://www.microsoft.com/downloads/details.aspx?familyid=12CB3C1A-15D6-4585-B385-BEFD1319F825&displaylang=en>.
- * **ISCSICPL** = GUI baziran iSCSI klijent (Initiator)
- * **LABEL** = za imenovanje ili uvid u ime volumena
- * **LOGOFF** = prekida aktivnu sesiju
- * **MKDIR** ili **MD** = za kreiranje direktorija (mape)
- * **MORE** = ispisuje sadržaj tekstualne datoteke razvrstan po ekranima

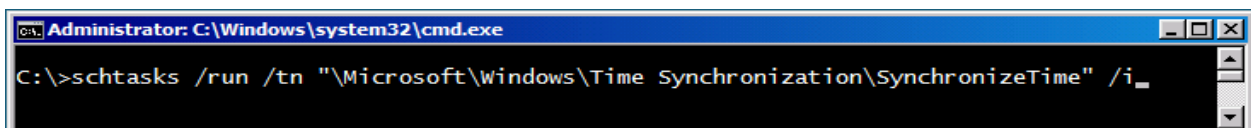
Koristimo MORE za čitanje jednog loga.



```
Administrator: C:\Windows\system32\cmd.exe
C:\>more /s < windows\security\logs\scesetup.log_
```

- * **MOVE** = za premještanje datoteka i preimenovanje direktorija
- * **MOUNTVOL** = za upravljanje Volume Mount Point značajkom
- * **MSG** = za slanje poruke konektiranom korisniku (ovisna o Messenger servisu)

- * **MSIEXEC** = (de)instalira i konfigurira MSI pakete
- * **MSINFO32** = detaljno izvješćuje o sustavu po različitim kategorijama (GUI); vidi i SYSTEMINFO, TASKMGR
- * **NBTSTAT** = upravlja tablicama NetBIOS imena; prikazuje podatke o NetBIOS over TCP/IP sesijama
- * **NET** = za upravljanje lokalnim korisnicima, grupama, servisima, dijeljenim resursima i mrežnim konekcijama
- * **NETDOM** = za managiranje Windows instalacije, prvenstveno u domeni
- * **NETSH** = shell za upravljanje mrežnim podsustavom, vidi [http://technet.microsoft.com/en-us/library/cc754516\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc754516(v=ws.10).aspx)
- * **NETSTAT** = za pregledavanje stanja TCP/IP portova i konekcija
- * **NOTEPAD** = tekstualni editor (GUI)
- * **NSLOOKUP** = za DNS dijagnostiku
- * **OCLIST** i **OCSETUP** – za (de)instaliranje rola i uloga, vidi i DISM
- * **OPENFILES** = prikazuje remotely otvorene datoteke i omogućuje forsirano diskonektiranje
- * **PATH** = pokazuje OS-u u kojim direktorijima i kojim slijedom treba tražiti izvršne programe (ako lokacija programa nije navedena u naredbi kojom se isti poziva)
- * **PATHPING** = dijagnostika komunikacijskog kanala do ciljnog hosta na IP razini, vidi i PING, TRACERT
- * **PING** = osnovna dijagnostika mrežne dostupnosti hosta
- * **PNPUTIL** = za (de)instalaciju drivera i pripremu drivera za naknadnu instalaciju
- * **QUERY** = prikazuje informacije o procesima, sesijama, userima i terminalskim serverima
- * **QWINSTA** = prikazuje info o terminalskim sesijama, vidi i RWINSTA
- * **REG** = komandnolinijski registry editor
- * **REGEDIT** i **REGEDT32** = GUI registry editori
- * **RELOG** = za konvertiranje i filtriranje performance logova
- * **RMDIR** ili **RD** = za brisanje direktorija (mape) u kojem se mogu ili ne moraju nalaziti poddirektoriji i/ili datoteke
- * **ROBOCOPY** = kopira/migrira mape i datoteke s mogućnošću nastavka nakon prekida i kreiranja loga o obavljenim radnjama; vidi i XCOPY
- * **ROUTE** = za administriranje lokalne tabele ruta
- * **RUNAS** = za pokretanje aplikacija s akreditivima različitim od aktualnih
- * **RWINSTA** = prekida uspostavljene sesije, vidi i QWINSTA
- * **SC** – preferirani alat za administriranje lokalnih servisa
- * **SCHTASKS** = za administriranje programabilnih zadataka (scheduled tasks)

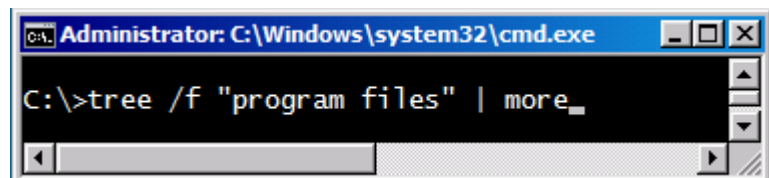


```
Administrator: C:\Windows\system32\cmd.exe
C:\>schtasks /run /tn "Microsoft\Windows\Time Synchronization\SynchronizeTime" /i
```

Namjeravamo pokrenuti jedan od postojećih zadataka, bez zadržke (/i).

- * **SCONFIG** = za osnovno konfiguriranje Core instalacije
- * **SCREGEDIT.WSF** = konfigurira AU servis, Remote Desktop, IPSec remote management i značajke Domain Controller SRV zapisa.
- * **SECEDIT** = za analizu, izmjenu, import i export... security postavki servera
- * **SET** = za administriranje sistemskih i korisničkih varijabli, vidi i SETX
- * **SETSPN** = za administriranje Service Principal Name-a računala odn. servisa
- * **SETX** = permanentno postavlja sistemske i korisničke varijable, vidi i SET
- * **SFC** = provjerava ispravnost i omogućuje zamjenu svih datoteka važnih sustavu
- * **SHUTDOWN** = za isključivanje ili restartanje računala
- * **SIGVERIF** = provjerava digitalne signature na sustavu važnim datotekama, vidi i VERIFIER
- * **SLMGR.VBS** = za managiranje licenci i aktivacija (naredba se ponekad referencira na SLUI.EXE ali taj ne postoji u R2)
- * **START** = starta određeni program u zasebnom prozoru sa zadanim prioritetom
- * **SYSTEMINFO** = verzija OS, RAM i pagefile, system uptime, hotfixovi..., vidi i MSINFO32
- * **TAKEOWN** = za preuzimanje i preraspodjelu vlasništva nad mapom/datotekom
- * **TASKKILL** = trenutno prekida djelatni proces
- * **TSKILL** = trenutno prekida proces terminalne sesije
- * **TASKLIST** = za pregled djelatnih procesa
- * **TASKMGR** = uvid u aktivne aplikacije i procese, real-time info o resursima sustava, pokretanje i zaustavljanje procesa (GUI), vidi i MSINFO32
- * **TELNET** = za konektiranje na Telnet server i za mrežnu dijagnostiku
- * **TIMEDATE.CPL, TIME** i **DATE** = GUI i komandnolinijski alati za podešavanje datuma i vremena sustava
- * **TRACERT** = za dijagnostiku komunikacijskog kanala do ciljnog hosta na IP razini, vidi i PATHPING
- * **TREE** = prikazuje stablo podmapa, može i sa imenima datoteka koje su u tim mapama

Vidjet ćemo stablasti prikaz direktorija i datoteka unutar C:\Program Files.



- * **TYPE** = na ekran ispisuje sadržaj tekstualne datoteke, vidi i MORE, NOTEPAD
- * **TZUTIL** = za postavljanje Time Zone, vidi i TIMEDATE.CPL
- * **VER** = prikazuje verziju OS-a
- * **VERIFIER** = ispituje stanje drivera po raznim kriterijima
- * **VSSADMIN** = za administriranje Volume Shadow Copy servisa
- * **W32TM** = za upravljanje vremenskom sinkronizacijom servera

- * **WECUTIL** i **WEVTUTIL** = za upravljanje logovima i eventima, vidi i EVENTCREATE
- * **WHOAMI** = prikazuje pod kojim accountom radimo
- * **WMIC** = snažna naredba za upravljanje sustavom na HW i SW razini
- * **WSCRIPT** i **CSCRIPT** = Windows Script Host interpreter, defaultni je wscript; više o tome na [http://msdn.microsoft.com/en-us/library/xazzc41b\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/xazzc41b(VS.85).aspx)
- * **WUSA** = Windows Update Standalone Installer, vidi KB 934307
- * **XCOPY** = za kopiranje/migriranje direktorija i datoteka, vidi i ROBOCOPY

* **KORISNI BESPLATNI ALATI**

Core Configurator = kombinacija PowerShella i Visual Basica u GUI-oriented alat za konfiguriranje Core servera

Microsoft Network Monitor x64 = za snimanje i analizu mrežnog prometa (GUI)

Sysinternals Suite = skup raznovrsnih CLI i GUI alata za Windows admina

Explorer++ x64 = upravitelj mapama i datotekama (GUI)

Microsoft Word Viewer = preglednik MS Word dokumenata (GUI)

Firefox ili **Opera** = Web browser (GUI)

Cool PDF Reader = GUI preglednik PDF dokumenata (skinuti all-in-one instalacijski paket, potom tijekom instalacije isključiti opcije za prečice a uključiti opciju za povezivanje aplikacije sa .pdf tipom)

VI. ZBLIŽIMO SE SA CLI OKRUŽENJEM!

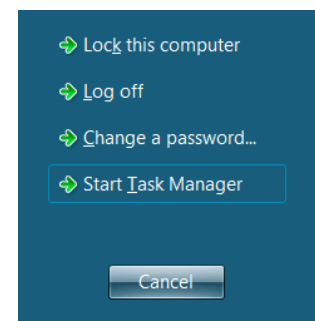
Za efikasniji rad u komandnoj liniji...

- Podesite komandnolinijski prozor: veličinu, buffer, font, boje... tako da, nakon desnog klika na zaglavlju prozora, odaberete naredbu Properties pa dalje. Usput, izbornik Edit sadrži skup važnih naredbi za efikasniju uporabu prozora.
- Rabite tipku TAB za auto-complete dovršenje započete naredbe; primjer: **C:\>cd p** pa pritisnate tipku TAB i ona će listati mape koje počinju sa slovom **p**.
- Za kretanje po prikazanoj naredbi su tipke usmjerivači lijevo-desno ili kombinacija tipaka Ctrl+usmjerivač lijevo-desno, a dobro će doći i tipke Home/End.
- Tipkom F7 prikazujemo popis naredbi zadanih računalu pa označavanjem + Enter možemo jednu od njih izvršiti (vidi sliku). Tipke usmjerivači gore-dolje služe za prizivanje već zadanih naredbi; prikazana naredba može se editirati pa izvršiti. Za pisanje preko prikazanog teksta pritisnite tipku Insert.
- Komandni redak brzo se čisti tipkom Esc a cijeli prozor naredbom `cls`.
- Naredbe iz ovog priručnika kopirajte u .txt datoteku, ovu spremite na Core, otvorite ju Notepadom te rabite Copy/Paste konkretne naredbe u naredbeni redak; ustreba li, prije izvršenja naredbu možete editirati.
- Praktično je podesiti Core da odmah nakon logona prikaže gore spomenuti dokument s naredbama i/ili administrativnim opaskama.
 - a) zadati `regedit` i smjestiti se u `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`
 - b) kreirati REG_SZ imena `Admindoc`, potom, nakon dvoklika na toj stavci, upisati `c:\admindoc.txt`
- Ako ste ispravno podesili RDC klijenta, kopirati možete s admin stanice na server i obratno.
- Samopomoć u komandnoj liniji je nužna, stoga rabite naredbu HELP odn. oblik `HELP <naredba>`; svaka naredba ima i lokalni help do kojega se najčešće dolazi opcijom `/?` ili slično tomu, npr.: `icaccls /?`.
- Ako zatvorimo komandnolinijski prozor, iskoristiti `Ctrl+Alt+Del` (iz remote sesije je `Ctrl+Alt+End`), pokrenuti Task Manager (vidi sliku) pa iz njega pokrenuti `cmd`. Drugi način otvaranja komandnolinijskog prozora: zadati `log off` pa se ulogirati na server. Ako smo lokalno na konzoli, TaskMan možemo dozvati i direktno sa `Ctrl+Shift+Esc`.
- Komandnom interpreteru je svejedno jeste li ime naredbe, mape ili datoteke upisali malim ili velikim slovima (prevodi ih u mala). Rečeno **ne** važi za opcije naredbi (npr. već općepoznata naredba PING razlikuje `-r` i `-R`), te za neke naredbe poput DISM – treba, dakle, voditi o tome račun.
- Često je praktično otvoriti više prozora; to se radi tako da u postojećem prozoru zadamo (osnovni oblik): `start cmd`.

```

0: netsh interface ipv4 show interfaces
1: control timedate.cpl
2: net use
3: systeminfo
4: copy *.log d:\
5: attrib
6: dir *.exe /o/a/s > svi-exe.txt
7: cls

```



Prompt (odzivni znak)

Uz pretpostavku da je Core instaliran na disk C:, defaultni oblik prompta koji se pojavljuje Administratoru izgleda ovako: **C:\Users\Administrator>** i doslovce nam govori: trenutno si u direktoriju (mapi, folderu) Administrator koji je poddirektorij direktorija Users a ovaj se, pak, nalazi u glavnom direktoriju diska C. Znak > u promptu ima simboliku sugestije „ovdje počni“.

Treba uočiti bitnu razliku između prvog i drugog znaka „\“: ako je taj znak uz oznaku diska, on se uvijek odnosi na glavni direktorij tog diska (npr. C:\); ako se opet pojavljuje u promptu (npr. Users\Administrator), on samo odjeljuje imena direktorija kako bi prompt kao cjelina bio čitljiviji.

Promptom nas OS podsjeća gdje se trenutno nalazimo u hijerarhiji (pod)direktorija određenog diska kako bismo mogli pravilno oblikovati naredbe za rad s diskovima, direktorijima i datotekama, lokalnim ili mrežnim.

Varijable PATH i PATHEXT

PATH govori OS-u u kojim direktorijima treba tražiti programe kako bismo ih mi admini (ili sustav, ovisi o konkretnom scenariju) mogli pozivati s bilo koje lokacije na disku. Naprimjer, programi-naredbe poput NOTEPAD i XCOPY uvijek će nam se odazvati zato jer su u \System32 a taj direktorij je defaultno u putu – zadajte naredbu path i uvjerite se.

Što ako direktorij u kojem imamo neke važne nam alate-programe nije u putu? Da bismo pokrenuli takav alat možemo:

- a) smjestiti se u njegov direktorij i pokrenuti alat

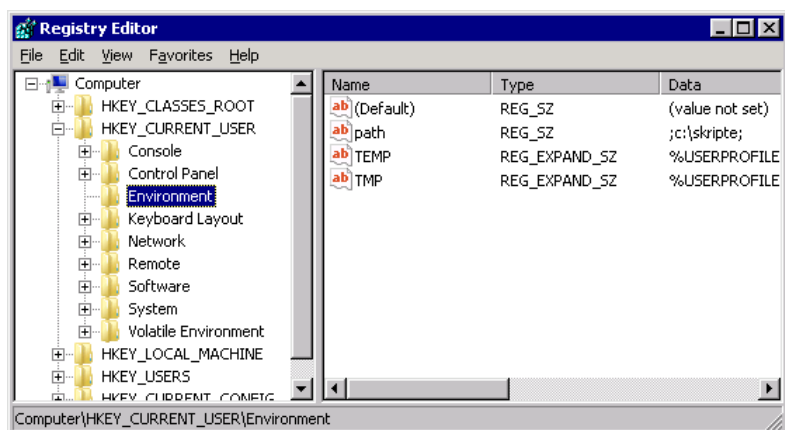
ili

- b) postaviti taj direktorij u put pa pozivati alat s bilo koje lokacije.

Rješenje a) donosi nam jednu važnu spoznaju: OS uvijek prvo traži program (i šire - datoteku) unutar direktorija u kojem trenutno jesmo pa tek ako ga tu ne nađe kreće u pretraživanje putanja definiranih varijablom PATH, i to redom kojim su u varijabli nevedene.

Za realizaciju točke b) rabit ćemo naredbe PATH, SET, SETX, REGEDIT..., ovisno o potrebi. Npr., da bismo postavili direktorij C:\Skripte u put, i to permanentno (tj. da instrukcija preživi restartanja servera), zadat ćemo naredbu (najjednostavniji oblik): `setx path ;c:\skripte;`. Potom odradimo `logoff` – `logon` da sustav prihvati dopunu puta.

Na slici vidimo gdje se prema korisnički dio varijable PATH.



Dobro je znati da postoje naredbe koje ne ovise o putu (COPY, DEL, DIR, CD, MD, RD, TYPE...) jer su integralni dio interpretera naredbi CMD.EXE.

PATHEXT govori OS-u koje tipove datoteka mora tretirati kao programe. Ovdje treba uočiti:

- **Izvršne** programe pokrećemo iz komandnog retka ili skripte pukim navođenjem njihovog imena (npr.: NOTEPAD, XCOPY) i oni kao takvi, izvršni, mogu biti samo tipova COM, EXE, BAT i CMD.
- **Neizvršne** programe, tipova poput VBS, WSF, JS, MSC... u načelu moramo pokrenuti posredstvom odgovarajućeg interpretera. Za programe tipa VBS i WSF to je Windows Script Host interpreter, poznat kao WSCRIPT.EXE. Srećom, WSH i CMD interpreteri su povezani pa programe poput SLMGR.VBS možemo pozvati baš kao izvršne, pukim navođenjem imena, npr. `s1mgr`. Drugi je način „pravilniji“: `wscript c:\windows\system32\slmgr.vbs`.

U jednom direktoriju OS traga za izvršnim programima ovim redom: COM, EXE, BAT i, naposljetku, CMD. Ukratko, ako u istom direktoriju imamo MOJALAT.EXE i MOJALAT.BAT, da bismo pokrenuli skriptu ne smijemo zadati naredbu `mojalat` (pokrenut će se MOJALAT.EXE) već `mojalat.bat`.

Rad s direktorijima i datotekama

Naredbe za rad s direktorijima i datotekama prisutne su u V. poglavlju. Opis džokera, kojima djelujemo na više datoteka ili direktorija odjednom, slijedi iza ove teme. Ako zaista razumijemo ulogu putanja i brojnih defaultnih postavki koje vrijede u komandnom retku, sve niže navedene operacije možemo izvesti na nekoliko načina. Zbog namjene ovog poglavlja, u primjerima koji slijede i koji zrcale par uobičajenih situacija, mi namjerno rabimo „školski“ pristup.

Primjeri:

C:\>dir /o/a/p = naredili smo sortirani ispis svih (i skrivenih) direktorija i datoteka koje sadrži glavni direktorij diska C:. Ako se radi o ispisu dužem od jedne stranice, naredba će popis formatirati po ekranskim stranicama.

C:\>md Temp = u glavnom direktoriju diska C: kreirali smo direktorij Temp.

C:\>copy windows*.log temp = iz direktorija C:\Windows kopirali smo sve .log datoteke u direktorij Temp.

C:\>cd temp = smjestili smo se u direktorij Temp.

C:\Temp>copy *.log d: = kopirali smo sve .log datoteke iz direktorija Temp u glavni direktorij diska D:.

C:\Temp>dir = gledamo sadržaj direktorija Temp

C:\Temp>del s*.log = iz direktorija Temp izbrisali smo .log datoteke ime kojih započinje slovom S.

C:\Temp>cd.. = izašli smo iz direktorija Temp i smjestili se u glavni direktorij diska C:.

C:\>rd temp /s = izbrisali smo direktorij Temp; opcijom /S naredili smo brisanje svega što se u njemu nalazi (bez te opcije naredba RD može izbrisati samo prazan direktorij).

C:\>d: = prelazimo na disk D: servera.

D:\>dir *.log = naredili smo prikazivanje svih datoteka tipa .log koje se nalaze u glavnom direktoriju diska D:. Ako su prikazane samo one datoteke koje želimo izbrisati, zadajemo naredbu `del *.log`.

D:\>c: = vraćamo se na disk C:.

C:\>attrib = dobijamo uvid u attribute datoteka smještenih u glavnom direktoriju diska C:. Ukoliko ih tijekom rada s datotekama previdimo, atributi **S**ystem, **H**idden i **R**ead-only mogu nas ozbiljno omesti – onemogućiti brisanja i kopiranja, manjkavima učiniti razne provjere ili ispise... zato je dobro upoznati se s opcijama naredbi poput ATTRIB, DEL, DIR, COPY i sl.

Džokeri (*wildcards*)

Džokeri su nezaobilazni u komandnolinijskom administriranju datoteka i direktorija pa je dobro pobliže se upoznati s načinima njihove primjene.

Džokeri su simboli ***** i **?**. Rabe se u naredbama u kojima navodimo imena direktorija ili datoteka i zamjenjuju neki niz znakova u imenu istih. Posredstvom džokera naredba djeluje na grupe direktorija ili datoteka. Simbol ***** zamjenjuje nekoliko znakova u imenu ili tipu datoteke (može i kompletno ime, vidi primjere). Simbol **?** uvijek zamjenjuje samo jedan znak ali se može više puta navesti.

Primjeri:

C:\>copy Windows\system32*.com = u glavni direktorij diska C kopiraju se sve datoteke tipa .com, koje se nalaze u direktoriju C:\Windows\System32.

C:\>dir *.exe /o/a/s > svi-exe.txt = budući da smo naredbu zadali pozicionirani u rootu volumena, bit će u tekstualnu datoteku svi-exe.txt upisani osnovni podaci o svim .exe programima (uključujući i skrivene) koji se nalaze na disku C; sve sortirano abecednim redom. Kreiranu .txt datoteku potom učitamo u Notepad.

C:\>xcopy windows\system32\w*.dll tempdll\ = iz System32 kopiramo sve dll-ove koji započinju slovom **w** u direktorij C:\tempdll; naredba sama tijekom izvršenja kreira taj direktorij jer smo ime tempdll završili s \.

C:\>xcopy windows\system32*.c* tempdll = u postojeći direktorij c:\tempdll kopiramo iz System32 sve datoteke kojima tip započinje slovom **c**.

C:\>del tempdll*.cp? = iz direktorija c:\tempdll brišemo sve datoteke kojima je zajednički slog **cp** u tipu.

C:\>cd pr* = primjer uporabe džokera u imenu direktorija.

Redirekcija

Redirekcija je preusmjeravanje izlaznih podataka neke naredbe s ekrana na neki drugi uređaj (datoteku, pisač) ili na neku drugu naredbu. Za redirekciju se koriste simboli **>**, **<**, **>&**, **<&**, **>>** i **|**. Redirekcije neće raditi ako ne mogu stvarati/brisati temp datoteke na disku.

Redirekcija je snažna i praktična komandnolinijska tehnika, više o njoj na <http://technet.microsoft.com/en-us/library/bb490982.aspx>.

Primjeri:

C:\>dir /o > root.txt = umjesto na ekran, naredba DIR u datoteku root.txt zapisuje nesakrivene stavke koje sadrži glavni direktorij diska C; mape i datoteke su razvrstane abecednim redom.

C:\>dir /o/a >> root.txt = sada smo na kraj datoteke root.txt **dodali** još jedan ispis naredbe DIR, ovoga puta upisane su zaista sve stavke koje se nalaze u C:\.

C:\>more < root.txt = root.txt usmjerili smo na naredbu MORE, stoga će ona na ekran ispisati sadržaj datoteke, izlistan po ekranskim stranicama.

C:\>dir /o/a | find "<JUNCTION>" > junctions.txt = ispis naredbe DIR predali smo na daljnju obradu naredbi FIND koja će u datoteku junctions.txt upisati sve pokazivače

koji se nalaze u C:\. Da bismo u datoteku zapisali sve pokazivače koji se nalaze na disku C, zadat ćemo vrlo sličnu naredbu: `dir /o/a/s | find "<JUNCTION>" > junctions.txt.`

C:\>netstat -ano -p tcp -t 5 >> netstat.log = svakih 5 sekundi naredba `netstat` zapisuje podatke o stanju TCP konekcija u datoteku `netstat.log`, ali tako da sačuva ranije zapise. Upisivanje prekidamo kombinacijom `Ctrl+C` (a `.log` datoteku učitamo u `Notepad`).

C:\>netsh advfirewall firewall show rule name=all > rules-all.log & rules-all.log = zapisujemo izvješće naredbe u datoteku te njen sadržaj odmah prikazujemo u `Notepadu`.

C:\>driverquery | clip = informacije o driverima pohranjuju se u `Clipboard` servera. Potom ih `RDP`-om prenesemo na admin stanicu tako da ih zalijepimo (`Paste`) u `Notepad`.

Automatiziranje poslova skriptama

Neizbježno je kreirati poneku skriptu kako bismo izbjegli ručno odrađivanje repetitivnih aktivnosti ili da bismo što brže obradili više diskova, datoteka, procesa... pa i servera. Od skriptnih jezika na raspolaganju su nam `PowerShell`, `Visual Basic` i „stari&dobri“ komandni (batch) jezik. Windows profesionalcima Microsoft preporuča `PowerShell`, intenzivno ga razvija i integrira sa svim novijim Windows OS-ovima i produktima poput `Exchange`, `Active Directory`, `Virtual Machine Manager`...; vidi

<http://www.microsoft.com/windowsserver2003/technologies/management/powershell/default.mspx>. Pravilna instalacija `PowerShell`a na Core R2 opisana je u artiklu KB 976736; podešavanje `PowerShell` ljsuke za izvršenje skripti naći ćete na <http://technet.microsoft.com/en-us/library/dd347628.aspx>.

Skripte, vlastoručno izrađene ili prikupljene s raznih strana (npr. s adrese [http://technet.microsoft.com/hr-hr/scriptcenter/dd742419\(en-us\).aspx](http://technet.microsoft.com/hr-hr/scriptcenter/dd742419(en-us).aspx)), smjestite u mapu `C:\Skripte`, potom se pobrinite da ih možete pozivati s raznih lokacija na disku odn. s raznih diskova sustava (vidi cjelinu `Varijable PATH` i `PATHEXT`).

Ovu temu, ujedno i priručnik, završavamo jednom zabavnom i poučnom batch skriptom – zabavnom stoga što se radi o maloj razbibrizi, poučnom utoliko što možete analizirati njen sadržaj pa ponešto naučiti glede pisanja takvih skripti. Dakle, skriptu prepišite, imenujte ju tako da ima nastavak `.bat`, kopirajte na svoj omiljeni Core server i... pravite se da radite! :-)

```
@echo off & setlocal enableextensions
cls
chcp | find "852" > nul
if errorlevel 1 (
echo. & echo.
echo    Kodna stranica u Command Promptu nije 852, PREKIDAM!) & goto izlaz
color E1
echo.
echo _____
echo.
echo    Ako broj kojega je skripta postavila tijekom pokretanja ne pogodiš u
echo    maksimalno 15 pokušaja, dobijaš "otkaz"; pogodiš li ga u 11 pokušaja -
echo    ja, bit ćeš pohvaljen(a) - nije puno, ali čovjeka veseli!
```

```
echo. & echo.
set /a pokusaji=0+0
:loop
set mojbr=%random%
:opet
if %pokusaji% GEQ 15 (
echo. & echo   Baj-baj, nabadalo-propadalo! Inače, broj je %mojbr%.) & goto izlaz
if %mojbr% GEQ 11111 (
goto loop
) else (
echo. & echo   Pogodi koji sam broj od 1 do 11111 zamislio!
set /p unos="* Upiši broj (Enter): "
)
set /a pokusaji=%pokusaji%+1
echo   %pokusaji%. pokušaj.
if %unos% GTR 11111 (echo. & echo   ::::: ne glupiraj se :::::) & goto opet
if %mojbr% GTR %unos% (echo. & echo   +++++ VEEĆIIIII +++++) & goto opet
if %mojbr% LSS %unos% (echo. & echo   ----- maanjiiii -----) & goto opet
if %mojbr% == %unos% if %pokusaji% LSS 12 (
echo.
rem start /min mplay32 /play /close %systemroot%\media\tada.wav
echo. & echo   . o O JE-JE-JEEEEE, TI SI GE-NI-JEEEEE! O o .
echo           * Tebi na čast, drugima kao uzor! *) & goto izlaz
if %mojbr% == %unos% (
echo. & echo.
echo   BRAVO TI, ŽIVIO JA!
echo   Ajd' probaj s 11 ili manje pokušaja, pliiiiz!) & goto izlaz
:izlaz
endlocal
echo.
echo   FINITO. Pikni razmaknicu...
pause > nul
exit
```

<kraj>