

Osnove administracije operacijskog sustava na poslužitelju

Kristanović, Antonio; Mlinar, Romeo; Golubić, Kruno; Novak Milić, Jasna

Educational content / Obrazovni sadržaj

Publication status / Verzija rada: **Accepted version / Završna verzija rukopisa prihvaćena za objavljivanje (postprint)**

Publication year / Godina izdavanja: **2016**

Permanent link / Trajna poveznica: <https://urn.nsk.hr/urn:nbn:hr:102:938372>

Rights / Prava: [Attribution-NonCommercial-ShareAlike 4.0 International](#)/[Imenovanje-Nekomercijalno-Dijeli pod istim uvjetima 4.0 međunarodna](#)

Download date / Datum preuzimanja: **2024-05-03**



Repository / Repozitorij:

[Digital repository of the University Computing Centre \(SRCE\)](#)





srce

Sveučilište u Zagrebu
Sveučilišni računski centar

Windows Server 2012 R2

Osnove administracije operacijskog sustava na poslužitelju

**Priručnik za
polaznika**

SA1-120

Ovu inačicu priručnika izradio je autorski tim Srca u sastavu:

Autor: Antonio Kristanović

Recenzent: Romeo Mlinar

Urednik: Kruno Golubić

Lektor: dr. sc. Jasna Novak Milić

Sveučilište u Zagrebu

Sveučilišni računski centar

Josipa Marohnića 5, 10000 Zagreb

edu@srce.hr

ISBN 978-953-8172-21-2 (meki uvez)

ISBN 978-953-8172-23-6 (meki uvez)

ISBN 978-953-8172-22-9 (PDF)

Inačica priručnika: 20160530



Ovo djelo dano je na korištenje pod licencom *Creative Commons*
Imenovanje-Nekomercijalno-Dijeli pod istim uvjetima 4.0

međunarodna. Licenca je dostupna na stranici:
<http://creativecommons.org/licenses/by-nc-sa/4.0/>.

Sadržaj

Uvod	1
1. Instalacija i konfiguracija poslužitelja.....	3
1.1. Iz predavanja.....	3
1.2. Važni pojmovi.....	4
1.3. Korisne naredbe	4
1.4. Vježba: Instalacija <i>Server Core</i>	5
1.5. Vježba: <i>Server Core</i> u sučelju GUI.....	5
1.6. Vježba: <i>Server Manager</i>	5
1.7. Vježba: Rad s <i>Disk Managementom</i>	5
1.8. Pitanja za ponavljanje	6
2. Konfiguriranje poslužiteljskih uloga i značajki	9
2.1. Iz predavanja.....	9
2.2. Važni pojmovi.....	10
2.3. Vježba: Izrada dijeljene mape pomoću <i>Server Managera</i>	10
2.4. Vježba: Dijeljenje printera.....	11
2.5. Dodatna vježba: Privilegirani ispis	11
2.6. Pitanja za ponavljanje	11
3. Konfiguriranje <i>Hyper-V</i> uloge.....	13
3.1. Iz predavanja.....	13
3.2. Važni pojmovi.....	14
3.3. Korisne naredbe	14
3.4. Vježba: Instalacija i konfiguracija uloge <i>Hyper-V</i>	14
3.5. Vježba: Izrada virtualnog stroja	14
3.6. Vježba: Izrada virtualnog diska.....	15
3.7. Dodatna vježba: Izrada virtualnog preklopnika	15
3.8. Pitanja za ponavljanje	16
4. Implementacija i konfiguriranje osnovnih mrežnih servisa.....	19
4.1. Iz predavanja.....	19
4.2. Važni pojmovi.....	20
4.3. Korisne naredbe	20
4.4. Vježba: CIDR-dijeljenje mreža na podmreže	21
4.5. Vježba: Izrada zona na DNS-poslužitelju.....	21
4.6. Vježba: Konfiguriranje DHCP-a	22
4.7. Pitanja za ponavljanje	23

5. Instalacija i administriranje <i>Active Directorya</i>.....	25
5.1. Iz predavanja.....	25
5.2. Važni pojmovi.....	26
5.3. Korisne naredbe.....	26
5.4. Vježba: Instalacija nove šume	27
5.5. Vježba: Izrada AD-objekata.....	27
5.6. Dodatna vježba: Provjera DNS-registracije	28
5.7. Pitanja za ponavljanje	28
6. Izrada i upravljanje pravilnicima skupine (<i>Group Policy</i>).....	31
6.1. Iz predavanja.....	31
6.2. Važni pojmovi.....	32
6.3. Korisne naredbe.....	33
6.4. Vježba: Konfiguriranje <i>Central Storea</i>	33
6.5. Vježba: Definiranje lokalnih pravilnika	33
6.6. Vježba: Izrada GPO-a i povezivanje na OU.....	33
6.7. Vježba: Izvoz i uvoz pravila <i>Windows Firewalla</i>	33
6.8. Dodatna vježba: <i>Default Domain Controllers Policy</i>	34
6.9. Pitanja za ponavljanje	35
7. Odgovori na pitanja.....	37
8. Popis literature	40

Uvod

Ovaj se priručnik koristi za izvođenje praktičnog dijela tečaja „Osnove administracije operacijskog sustava na poslužitelju (*Windows Server 2012*)“.

Rješavanjem predviđenih vježbi polaznik će moći isprobati postupke obrađene u teorijskom dijelu tečaja koji je dostupan preko sustava za e-učenje.

Priručnik se sastoji od šest cjelina. Na početku svake cjeline dostupni su sažetak teorijskog dijela i popis važnijih pojmova i naredbi potrebnih za rješavanje vježbi. Nakon rješavanja vježbi pripremljena su pitanja za ponavljanje.

U ovom se priručniku za označavanje važnijih pojmova i naredbi rabe **podebljana slova**.

Za odvajanje naredbi u nizu naredbi rabi se oznaka →.

Put do naredbe piše se kurzivom, a naredba podebljana, na primjer *Prikaz* → *Prozor* → **Promijeni prozor**.

Nazivi datoteka napisani su **podebljanim slovima i kurzivom**.

Prečaci na tipkovnici označeni su ovako: [Ctrl]+[Alt]+[Del], [F1].

Savjeti, upozorenja i zanimljivosti nalaze se u okvirima sa strane.

Programski kôd napisan je ovako:

```
Install-WindowsFeature Server-Gui-Mgmt-  
Infra,Server-Gui-Shell -Source wim  
:D:\sources\install.wim:2
```


1. Instalacija i konfiguracija poslužitelja

Nakon ove cjeline moći ćete:

- obaviti instalaciju *Windows Servera 2012 R2*
- konfigurirati poslužitelj nakon instalacije
- upravljati *Server Managerom* – upraviteljem poslužitelja
- konfigurirati diskove u *Disk Managementu*.

1.1. Iz predavanja

Planiranjem instalacije odlučujemo koje će se izdanje operacijskog sustava instalirati: hoće li to biti potpuno grafičko sučelje ili instalacija *Server Core*, hoće li se i koja virtualizacijska strategija primijeniti te koje će se poslužiteljske uloge implementirati.

Server Core nije poseban operacijski sustav ili izdanje – to je instalacijska mogućnost uključena u *Windows Server 2012 R2 Standard* i *Datacenter*.

Poboljšanje koje je donio *Windows Server 2012 R2* u odnosu na *Windows Server 2008 R2* je mogućnost pretvaranja između GUI-sučelja i *Server Corea* bez potrebe za reinstalacijom operacijskog sustava.

Upravitelj poslužitelja ili *Server Manager* može instalirati uloge i značajke na bilo koji poslužitelj na mreži. Također pruža pristup servisima pokrenutim na svim poslužiteljima na mreži.

Windows Server Migration Tools je značajka (*feature*) koja se sastoji od naredbi *PowerShell* i uputa kojima se administratoru pomaže preseliti uloge između poslužitelja.

Što se tiče pohrane na diskove, *Windows Server 2012 R2* podržava dvije vrste particija (*MBR* i *GPT*) i dvije vrste diskova (*Basic* i *Dynamic*), pet vrsti volumena i tri vrste datotečnih sustava (*NTFS*, *ReFS*, *FAT*).

Sve instalacije *Windows Server 2012 R2* uključuju ulogu *File And Storage Services*, kojom se u *Server Manageru* nudi izbornik s pristupom upravljanju volumenima, diskovima, dijeljenim mapama itd.

1.2. Važni pojmovi

pojam	kratak opis
<i>Storage Spaces</i>	To je diskovna virtualizacijska tehnologija koja omogućuje objedinjenje diskovnog prostora sa zasebnih fizičkih diskova u virtualne diskove bilo kojih veličina, a koje su hardverski podržane.
<i>Storage Pools</i>	To je skup resursa za diskovnu pohranu, odnosno nedodijeljen (<i>unallocated</i>) diskovni prostor <i>Storage Spacesa</i> , kojem prema potrebi možemo dodavati ili oduzimati fizičke diskove.
ReFS	ReFS je novi datotečni sustav koji se prvi puta pojavljuje s <i>Windows Serverom 2012 R2</i> , a pruža praktično neograničene veličine datoteka i mapa te povećava otpornost podataka na pogreške.

1.3. Korisne naredbe

naredba	kratak opis naredbe
Install - WindowsFeature	Naredba <i>PowerShell</i> za dodavanje punog grafičkog sučelja. Primjer: <pre>Install-WindowsFeature Server-Gui-Mgmt-Infra,Server-Gui-Shell -Source wim :<drive>:\sources\install.wim:<index></pre>
Uninstall - WindowsFeature	Naredba <i>PowerShell</i> za isključenje grafičke ljske uz brisanje datoteka iz mape WinSxS. Primjer: <pre>Uninstall -WindowsFeature Server-Gui-Shell -Remove</pre>
Sconfig.cmd	<i>Server Configuration</i> , alat za konfiguriranje i upravljanje osnovnim postavkama instalacije <i>Server Core</i> .
Netdom	Naredba za promjenu imena poslužitelja. Primjer: <pre>Netdom renamecomputer %ComputerName% /NewName: <NovoIme></pre>

1.4. Vježba: Instalacija *Server Core*

1. Instalirajte instalaciju *Windows Servera 2012 R2 Server Core* na particiju veličine 50 GB. Particiju treba izraditi tijekom instalacijskog postupka i pritom dio diskovnog prostora ostaviti nedodijeljenim. Kao administratorsku zaporku kroz cijeli tečaj rabite **Pa55word!**.
2. Po završenoj instalaciji obavite inicijalnu konfiguraciju poslužitelja alatom **sconfig**:
 - promijenite ime poslužitelja iz inicijalnog u **SRV-LABxx**
 - omogućite pristup udaljenoj radnoj površini (*Remote Desktop*)
 - provjerite i prema potrebi podesite točan datum i vrijeme
 - ponovno pokrenite poslužitelj (*Restart Server*).

1.5. Vježba: *Server Core* u sučelju GUI

1. Prebacite instalaciju *Server Core* u puno grafičko sučelje odgovarajućom naredbom. Za parametar **<drive>** koristite se slovom **D**, a za **<index>** brojem **2** (*Standard*).

Upišite naredbu kojom ste se koristili:

1.6. Vježba: *Server Manager*

1. Pomoću *Server Managera* prebacite poslužitelj iz inicijalne radne skupine u radnu skupinu naziva **LAB**. Obavite potrebno ponovno pokretanje poslužitelja.
2. U *Server Manageru*, pomoću čarobnjaka *Add or Remove Features*, dodajte ulogu **File Server**.
3. U *Server Manageru*, pomoću čarobnjaka *New Volume Wizard* stvorite novi volumen veličine 80 GB i oznake H, a druge mogućnosti ostavite na pretpostavljenim vrijednostima.

1.7. Vježba: Rad s *Disk Managementom*

1. Rabeći preostali prostor na disku, proširite ranije stvoren volumen H na **50 GB**. Za rješavanje zadatka rabite *Disk Management*.

1.8. Pitanja za ponavljanje

1. **Koja se od navedenih procesorskih arhitektura može rabiti za instalaciju *Windows Servera 2012 R2*?**
 - A. Samo 32-bitni procesori.
 - B. Samo 64-bitni procesori.
 - C. I 32-bitni i 64-bitni procesori.
 - D. 64-bitni procesori i procesori Itanium.
2. **Kako se naziva mapa u koju poslužitelj sprema module koji se mogu naknadno rabiti pri instalaciji uloga i značajki?**
 - A. *WindowsBin*
 - B. *InstallerLog*
 - C. *WinSxS*
 - D. *System32*
3. **Kojom se naredbom *Powershell* koristimo za deinstalaciju uloga i značajki s poslužitelja?**
 - A. *Remove-WindowsFeature*
 - B. *Remove-WindowsRole*
 - C. *Uninstall-WindowsRole*
 - D. *Uninstall-WindowsFeature*
4. **Kojom se izvedbom udruživanja NIC (*NIC Teaming*) koristimo kada želimo bolju toleranciju pogrešaka (*fault tolerance*)?**
 - A. *Switch Independent Mode*
 - B. *Switch Dependent Mode*
 - C. *Router Alternate Mode*
 - D. *Switched Route Mode*
5. **Kojom se naredbom možemo koristiti za dodavanje poslužitelja *Server Core* u domenu?**
 - A. *ipconfig.exe*
 - B. *netsh.exe*
 - C. *netdom.exe*
 - D. *dcpromo.exe*

6. Koja dva od ovih volumena osiguravaju toleranciju pogrešaka (*fault tolerance*)?

- A. Rastegnuti (*spanned*) volumen
- B. Isprugani (*striped*) volumen
- C. Zrcaljeni (*mirrored*) volumen
- D. Volumen RAID-5

2. Konfiguriranje poslužiteljskih uloga i značajki

Nakon ove cjeline moći ćete:

- izraditi dijeljene mape i upravljati dozvolama na resursima datotečnog sustava
- dijeliti printere i upravljati dokumentima za ispis.

2.1. Iz predavanja

Izrada dijeljenih mapa omogućuje da su podaci koji se nalaze na diskovnim prostorima poslužitelja dostupni korisnicima na mreži.

Važno je da administrator razumije da su dozvole na dijeljenim mapama potpuno odvojene od prava na NTFS-u. Za pristup datoteci na dijeljenoj mapi korisnik mora imati odgovarajuća prava NTFS-a i odgovarajuća prava na dijeljenoj mapi.

Svaka datoteka i mapa na disku NTFS imaju svoju pristupnu kontrolnu listu – ACL (*Access Control List*), koja se sastoji od ACE (*Access Control Entry*), zapisa koji se sastoje od principala i dodijeljenih mu dozvola. Sigurnosni principali su korisnici i skupine na koje se *Windows*i referiraju pomoću sigurnosnih identifikatora (SID).

Datotečni sustav NTFS ima 14 naprednih dozvola koje možemo pridružiti datoteci ili mapi. Kombiniranjem naprednih dozvola izvedeno je šest osnovnih dozvola: *fullcontrol*, *modify*, *read & execute*, *list folder contents*, *read* i *write*.

Nasljeđivanje dozvola (*inheriting permissions*) znači da će nadređeni element predati svoje dozvole podređenom elementu. Prema potrebi se nasljeđivanje dozvola može isključiti.

Prednost je dijeljenog mrežnog ispisa u tome što su svi poslovi za ispis pohranjeni u jednom redu za čekanje pa klijenti i administratori mogu vidjeti cjeloviti popis poslova koji čekaju red na ispis. Uz to, administratori mogu implementirati napredne značajke za ispis te s udaljenog mjesta upravljati sigurnošću i pravima ispisa, nadgledanjem poslova i zapisa o pogreškama itd.

Napomena

U izdanjima prije *Windows Servera 2012*, osnovne (*basic*) dozvole nazivale su se standardnim dozvolama (*standard permissions*), a napredne (*advanced*) posebnim dozvolama (*special permissions*).

2.2. Važni pojmovi

pojam	kratak opis
SMB	<i>Server Message Blocks</i> – protokol za dijeljenje datoteka na svim inačicama <i>Windowsa</i>
NFS	<i>Network File System</i> – protokol koji se rabi na većini <i>Unixovih</i> i <i>Linuxovih</i> distribucija
ABE	<i>Access-based enumeration</i> , značajka koja onemogućuje korisnicima da vide dijeljene mape na koje nemaju prava
<i>Print device</i>	Pisač, uređaj za ispis – hardver koji proizvodi dokumente ispisane na papir ili na neki drugi medij za ispis.
<i>Printer</i>	<i>Printer</i> je softversko sučelje kroz koje računalo komunicira s uređajem za ispis.

2.3. Vježba: Izrada dijeljene mape pomoću *Server Managera*

Napomena

Prije nego što se može izraditi i upravljati dijeljenjima **SMB** (**SMB shares**) pomoću *Server Managera*, treba instalirati servis uloge **File Server**.

1. Pomoću *Server Managera*, *File and Storage Services*, izradite dijeljenu mapu s ovim postavkama:

- Local path: C:\Shares\Dijeljenje1
- Share name: Dijeljenje1
- Protocol: SMB
- ABE: enabled
- Caching: enabled
- BranchCache: disabled
- Encrypt data: disabled.

Dozvole u mapi uredite tako da se doda ugrađeni (*builtin*) sigurnosni principal *Power Users* s pravima *Modify*.

2.4. Vježba: Dijeljenje printera

1. Na poslužitelj instalirajte lokalni printer *Microsoft PCL6 Print Driver* na port **LPT1**. Printer će biti dijeljen s pretpostavljenim postavkama i predloženim dijeljenim imenom (*share name*).
2. Zbog potreba privilegiranog ispisa za lokalnu skupinu korisnika **Power Users**, instalirajte još jedan printer pridružen istom pisaču. Printer treba imati naziv *Microsoft PCL6 Print Driver (Power Users)*. Podesite prioritet ispisa i prava na ispis tako da skupina *Power Users* ima prednost pri ispisu dokumenata.

2.5. Dodatna vježba: Privilegirani ispis

1. U prethodnom primjeru, ako za printer koji je namijenjen ispisu za skupinu *Power Users*, ostavimo prava ispisa i za skupinu *Everyone*, u kojem slučaju korisnik koji nije član skupine *Power Users* može ispisivati na privilegirani pisač?
-
-

2.6. Pitanja za ponavljanje

1. **Koji od ovih pojmova najbolje opisuje postupak davanja pristupa korisnicima dokumentu na dijeljenoj mapi, na osnovi danih prava?**
 - A. autentikacija
 - B. autorizacija
 - C. renderiranje
 - D. enumeracija
2. **Koja od ovih izjava najbolje opisuje ulogu sigurnosnog principala pri dodjeli dozvola na resurs datotečnog sustava?**
 - A. Sigurnosni principal je osoba koja ima *Write* prava na resurs.
 - B. Sigurnosni principal je osoba koja je vlasnik (*owner*) resursa.
 - C. Sigurnosni principal je osoba koja dodjeljuje dozvole pristupa.
 - D. Sigurnosni principal je osoba kojoj dodjeljujemo dozvolu pristupa.

3. **Koji je maksimalan broj kopija u sjeni po volumenu koje *Windows Server 2012 R2* može održavati?**
- A. 8
 - B. 16
 - C. 64
 - D. 128
4. **Koji od ovih pojmova najbolje opisuje softversko sučelje kojim računalo komunicira s uređajem za ispis?**
- A. Printer server
 - B. Printer
 - C. Printer driver
 - D. PCL
5. **Jedan od uređaja za ispis se pokvario pa je potrebno privremeno onemogućiti da korisnici šalju dokumente na printer koji ispisuje na pokvareni pisač. Što od navedenog treba poduzeti?**
- A. Isključiti dijeljenje printera.
 - B. Ukloniti printer iz *Active Directorya*.
 - C. Promijeniti printerski port.
 - D. Preimenovati dijeljenje printera (*share name*).

3. Konfiguriranje *Hyper-V* uloge

Nakon ove cjeline moći ćete:

- rabiti *Hyper-V Manager* kroz izradu ili podešavanje virtualnih strojeva i određivati hardverske resurse koji će im se dodijeliti
- izraditi novi virtualni stroj
- izraditi novi virtualni disk.

3.1. Iz predavanja

Virtualizacija je proces koji dodaje sloj apstrakcije između stvarnog, fizičkog hardvera, i sustava koji se njime koristi. Umjesto poslužitelja koji ima izravni pristup računalnom hardveru, komponenta naziva hipernadzor stvara okruženje u kojem se pokreće operacijski sustav poslužitelja.

Virtualizacija je postupak implementacije i održavanja višestrukih instanci operacijskog sustava koje nazivamo virtualnim strojevima (VM) i to na jednom fizičkom stroju.

Microsoftov *Hyper-V* je hipernadzor instaliran između hardvera i operacijskog sustava i glavna je komponenta koja upravlja virtualnim računalima. Dodavanjem uloge *Hyper-V* operacijski sustav (u ovom slučaju *Windows Server 2012 R2*) se konvertira u nadređenu particiju, a hipernadzor se učitava prije operacijskog sustava.

Primarni alat za izradu i upravljanje virtualnim strojevima je konzola *Hyper-V Manager*. Postoji također i niz *Hyper-V* orijentiranih naredbi *PowerShell*.

VHD-slika diska ograničena je na maksimalnu veličinu od 2 TB i kompatibilna je sa svim starijim hipernadzorskim proizvodima. VHDX-slika diska može biti velika 64 TB, nije unazad kompatibilna te može biti čitana samo s *Windows Server 2012 (R2)* i *Windows 8(.1)* *Hyper-V* poslužitelja. Moguće je konvertirati format VHD u VHDX i VHDX u VHD sve dok je disk veličine do 2 TB.

Izrada kontrolne točke (*checkpoint*) predstavlja sliku stanja sustava, podataka i hardverske konfiguracije virtualnog stroja određenog trenutka u vremenu. Broj kontrolnih točaka (*checkpointa*) koje možemo napraviti za svaki virtualni stroj je 50.

Postoje tri vrste virtualnih mrežnih preklopika koje moramo izraditi kroz *Virtual Switch Manager* da bismo na njih spojili virtualne strojeve: to su vanjski (*external*), unutarnji (*internal*) i privatni (*private*) preklopnik.

Napomena

Izraz **checkpoint** istovjetan je izrazu **snapshot** koji se rabio za isti postupak u inačicama *Hyper-V*-a prije *Windows Server 2012 R2*.

Microsoft preporuča rabiti najmanje dvije fizičke mrežne kartice na *Hyper-V* poslužitelju, tako da jedna poslužuje nadređenu (*parent*), a druga podređenu (*child*) particiju.

3.2. Važni pojmovi

pojam	kratak opis
<i>Hyper-V Server</i>	Izdanje <i>Windows Servera 2012</i> koje sadrži samo ulogu <i>Hyper-V</i> i ograničeni dio <i>File and Storage Services</i> , kao i mogućnosti <i>Remote Desktop</i> . Besplatan je i može se skinuti s Microsoftovih stranica, no za svaki gostujući operacijski sustav potrebna je licenca.
<i>Guest Integration Services</i>	Softverski paket koji se instalira na virtualne strojeve za potrebe kompatibilnosti.
<i>VLAN ID</i>	VLAN-identifikator, na mrežnoj kartici virtualnog stroja određuje virtualni LAN kojim će se virtualni stroj koristiti za svu mrežnu komunikaciju kroz tu mrežnu karticu.

3.3. Korisne naredbe

naredba	kratak opis naredbe
<code>Install-WindowsFeature -Name Hyper-V</code>	Naredba <i>PowerShell</i> za instalaciju uloge <i>Hyper-V</i> . Primjer: <code>Install-WindowsFeature -Name Hyper-V -ComputerName <ime> -IncludeManagementTools -Restart</code>

3.4. Vježba: Instalacija i konfiguracija uloge *Hyper-V*

1. Pokrenite instalaciju uloge *Hyper-V* pomoću čarobnjaka *Add Roles And Features* u *Server Manageru*.
2. Konfigurirajte ulogu tako da pretpostavljene lokacije virtualnih diskova i konfiguracijskih datoteka ukazuju na volumen H; u fazi instalacije uloge ne treba izraditi virtualni preklopnik.
3. Nakon što je uloga instalirana, u *Hyper-V* manageru izradite privatni virtualni preklopnik naziva **Privatni Preklopnik LAB**.

3.5. Vježba: Izrada virtualnog stroja

1. U *Hyper-V Manageru*, pomoću čarobnjaka *New Virtual Machine*, izradite novi virtualni stroj naziva **VM-LAB01**. Lokaciju datoteka

ostavite na pretpostavljenim vrijednostima. Operacijski će se sustav instalirati na virtualni stroj poslije.

2. Odaberite drugu generaciju virtualnog stroja (*Generation 2*), dodijelite mu **512 MB** početne memorije i uključite mogućnost dinamičke memorije. Kod konfiguracije mreže odaberite virtualni preklopnik koji ste već izradili, **Privatni Preklopnik LAB**.
 3. Za taj virtualni stroj treba izraditi novi virtualni disk veličine **32 GB**. Druge postavke virtualnog diska ostavite na ponuđenim vrijednostima.
 4. Nakon što je napravljen virtualni stroj, u postavkama za memoriju postavite vrijednost za *Startup RAM* na **1024 MB**. Što smo postigli tom promjenom?
-
-

3.6. Vježba: Izrada virtualnog diska

1. U *Hyper-V Manageru*, pomoću čarobnjaka *New Virtual Hard Disk*, izradite novi dinamičko proširivi virtualni disk u formatu **VHDX** veličine **10 GB**. Disk ostavite na ponuđenoj lokaciji, a nazovite ga **vHD01-LAB01**.
2. Nakon izrade novog praznog virtualnog diska, spojite ga kao dodatni disk na SCSI-kontrolor virtualnog stroja VM-LAB01.
3. Za provjeru pokrenite virtualni stroj VM-LAB01, obavite inicijalizaciju novog diska s **GPT**-particioniranjem i novim volumenom pune veličine u formatu **NTFS**.
4. Funkcionalnost provjerite izradom nove mape i datoteke.txt u *File Exploreru*.

3.7. Dodatna vježba: Izrada virtualnog preklopnika

1. U *Hyper-V Manageru*, pomoću *Virtual Switch Managera*, napravite novi virtualni preklopnik naziva **Novi Preklopnik LAB**. Novi virtualni preklopnik smije imati pristup samo za virtualne strojeve na podređenoj particiji. Koju vrstu virtualnog preklopnika treba odabrati da bismo zadovoljili taj uvjet?
-
-
2. Konačno, na virtualnom stroju napravljenom u vježbi 3.4 (VM-LAB01) stvorite novu mrežnu karticu te ju spojite na virtualni preklopnik **Novi Preklopnik LAB**.

3.8. Pitanja za ponavljanje

1. **Koja od ovih vrsti virtualizacije daje najbolje performanse za poslužitelje velikih propusnosti u produkcijskom okruženju?**
 - A. Tip I
 - B. Tip II
 - C. Prezentacijska virtualizacija
 - D. *RemoteApp*
2. **Koja od ovih značajki *Hyper-V*-a nije nužna da bi virtualni stroj radio na manjoj količini RAM-a nego kad je pokrenut?**
 - A. *Smart paging*
 - B. *Dynamic Memory*
 - C. *Memory Weight*
 - D. *Guest Integration Services*.
3. **Kada se *Hyper-V* instalira na *Windows Server 2012 R2*, na koji element sustava se konvertira OS?**
 - A. Na hipernadzor.
 - B. Na nadređenu (*parent*) particiju.
 - C. Na podređenu (*child*) particiju.
 - D. Na UEFI-hardver.
4. **Koja su dva od navedenih valjani razlozi da se ne rabi kontrolna točka (*checkpoint*)?**
 - A. Veliko zauzeće diskovnog prostora.
 - B. Velika potrošnja fizičke memorije.
 - C. Dugotrajna izrada.
 - D. Smanjenje performansi virtualnih strojeva.
5. **Koji je najveći broj portova koje podržava preklopnik *Hyper-V*?**
 - A. 16
 - B. 32
 - C. 48
 - D. Neograničeno.

6. Koja od ovih vrsta virtualnih preklopnika ne dopušta komunikaciju između gostujućeg OS-a i nadređene particije?

- A. *External* – vanjski.
- B. *Internal* – interni.
- C. *Private* – privatni.
- D. *Isolated* – izolirani.

4. Implementacija i konfiguriranje osnovnih mrežnih servisa

Nakon ove cjeline moći ćete:

- dijeliti podmreže metodom CIDR
- napraviti zone i zapise na DNS-poslužitelju
- konfigurirati DHCP-poslužitelj.

4.1. Iz predavanja

Adresni prostor IPv4 sastoji se od 32-bitnih adresa, koje se bilježe kao četiri 8-bitne decimalne vrijednosti u rasponu od 0 do 255. Zasebne 8-bitne decimalne vrijednosti nazivaju se okteti ili bajtovi, a odvojene su točkom.

IPv4-adresa je logički podijeljena na dva dijela. Jedan dio odnosi se na mrežu u kojoj se adresa nalazi (*network identifier*), a drugi dio označava sam uređaj (*host identifier*) kojem dodjeljujemo IPv4-adresu. Maska podmreže (*subnet mask*) pokazuje koji je mrežni dio, a koji je dio uređaja u IPv4-adresi.

IPv6 se koristi obilježavanjem koje se naziva *colon-hexadecimal*, odnosno, sastoji se od osam 16-bitnih heksadecimalnih brojeva odvojenih dvotočkom.

U svojem osnovnom obliku, postupak DNS-zahtjeva sastoji se od klijenta (resolvera) koji upućuje upit svojem određenom DNS-poslužitelju. Kada poslužitelj nema tražene podatke, proslijeđuje upit drugom DNS-poslužitelju na mreži. Drugi poslužitelj vraća prvom odgovor koji sadrži traženo ime i IP-adresu, a on ga zatim predaje klijentu.

Postupak implementacije DNS-poslužitelja na *Windows Server 2012 R2* zapravo je instalacija uloge *DNS Server* pomoću *Add Roles And Features Wizarda* u *Server Manageru*. Instalacija ne zahtijeva dodatne parametre, a u čarobnjaku nema dodatnih stranica ni servisa uloge koje treba odabrati.

DNS-poslužitelj u *Windowsima* podržava tri vrste zona, kojima se određuje kamo poslužitelj pohranjuje baze podataka i kakvu vrstu informacija u njima čuva. Tu su: primarna, sekundarna i stub zona.

DHCP (*Dynamic Host Configuration Protocol*) je servis koji automatski konfigurira IP-adresu i druge TCP/IP-postavke na mrežna računala. Adresa se dodjeljuje iz bazena (*pool*) adresa, zvanog opseg (*scope*), a vraća se nakon što joj najam (*lease*) istekne.

4.2. Važni pojmovi

pojam	kratak opis
<i>CIDR – Classless Inter-Domain Routing</i>	Metoda koja administratorima omogućuje postavljanje oznake mreže ili uređaja na bilo kojem mjestu u adresi, a ne samo među oktetima.
<i>Subnet Mask</i>	Maska podmreže, označuje koji bitovi IP-adrese određuju uređaj, a koji bitovi mrežu na kojoj uređaj obitava.
<i>Router</i>	IP-adresa usmjernika (<i>router</i>) ili zadanog pristupnika (<i>default gateway</i>)
<i>Domain Name Server</i>	IP-adresa DNS-poslužitelja kojim će se klijent koristiti za DNS-upite.
<i>Host Name</i>	DNS-ime kojim će se klijent koristiti.
<i>Domain Name</i>	Ime DNS-domene na kojoj će klijent obitavati.
<i>Scope</i>	Opseg (<i>scope</i>) je raspon IP-adresa na posebnoj podmreži (<i>subnet</i>) koju opslužuje DHCP-poslužitelj.

4.3. Korisne naredbe

naredba	kratak opis naredbe
Ipconfig /all	Naredba kojom lako možemo provjeriti dodijeljenu IPv4- i IPv6-adresu mrežnim adapterima na računalu.
Add-DnsServerPrimaryZone	<p><i>Cmdlet</i> za izradu primarne zone u <i>Active Directoryu</i> pomoću <i>Windows PowerShella</i>.</p> <p>Primjer:</p> <pre>Add-DnsServerPrimaryZone -Name "imezone.lab.local" -ReplicationScope "Domain" -PassThru</pre>

4.4. Vježba: CIDR-dijeljenje mreža na pod mreže

1. Pogledajmo ovaj scenarij: administrator mreže 172.16.6.0/24 ima potrebu razdijeliti mrežu na barem tri pod mreže u kojoj za svaku očekuje do 50 uređaja.

Koje će raspone IP-adresa za uređaje svaka od mreža imati i kojim će se maskama pod mreže klijenti koristiti?

Adresa mreže	Početna IP-adresa	Završna IP-adresa	Maska pod mreže

4.5. Vježba: Izrada zona na DNS-poslužitelju

1. Primarnoj mrežnoj kartici na poslužitelju dodijelite sljedeće postavke:
IP: 10.4.0.100; SM: 255.255.0.0; DG: 10.4.0.1
2. Ako na poslužitelju ne postoji DNS-uloga, instalirajte ju.
3. U *DNS Manageru* napravite novu primarnu zonu DNS za prosljeđivanje (*forward*) naziva **zona1.lab.local**. Datoteka zone neka se zove **zona1.lab.local.dns**. Zona ne smije podržavati dinamičko ažuriranje.
4. Nakon izrade primarne zone, napravite standardnu primarnu zonu za obrnuto razlučivanje (*reverse lookup*). *Network ID* zone treba biti **10.4.4**. Ime datoteke zone može ostati ponuđena vrijednost, a zona ne smije podržavati dinamičko ažuriranje.
5. U zona1.lab.local napravite novi **Host (A)** zapis: **pc-lab01** s IP-adresom **10.4.4.125**. Ostavite uključenu mogućnost za izradu pridruženog PTR-zapisa. Provjerite izradu zapisa *Pointer* (PTR).

Kako glasi FQDN izrađenog PTR-zapisa?

4.6. Vježba: Konfiguriranje DHCP-a

1. Ako na poslužitelju ne postoji uloga **DHCP Server**, instalirajte ju. Potvrdite izradu sigurnosnih skupina i ponovno pokrenite poslužitelj.
2. Pomoću **konzole DHCP** izradite novi opseg s ovim postavkama:
 - ime opsega: lab
 - raspon adresa za distribuciju: 10.4.4.120 - 10.4.4.200
 - maska mreže 255.255.255.0 (/24)
 - iz raspona isključiti adresu 10.4.4.125.

Druge postavke ostaviti na pretpostavljenim vrijednostima, a mogućnosti opsega ostavite za naknadno konfiguriranje. Aktivirajte opseg.

4.7. Pitanja za ponavljanje

1. **Koju vrstu IP-adrese sustav mora imati da bi bio vidljiv na Internetu?**
 - A. Binarnu.
 - B. Registriranu.
 - C. Privatnu.
 - D. Klasu B.
2. **Koja je od navedenih IPv6 ekvivalent privatnim adresama u IPv4?**
 - A. *Link* – adresa *local unicast*.
 - B. Adresa *global unique unicast*.
 - C. Adresa *unique-local unicast*.
 - D. Adresa *anycast*.
3. **Kojom se od ovih maski podmreže treba koristiti za konfiguraciju TCP/IP-a na klijentu za 172.16.32.0/19 mrežu?**
 - A. 255.255.224.0
 - B. 255.255.240.0
 - C. 255.255.255.224
 - D. 255.255.255.240
4. **Koja je od navedenih primarna metoda za prijenos prometa IPv6 kroz mrežu IPv4?**
 - A. *contracting*
 - B. *supernetting*
 - C. *subnetting*
 - D. *tunneling*
5. **Koji od navedenih nije jedan od elemenata DNS-a?**
 - A. *resolver*
 - B. *relay agent*
 - C. *name server*
 - D. *namespace*

6. **Koja od ovih vrsta zapisa sadrži informaciju da DNS-poslužitelj treba obaviti obrnuto razlučivanje imena (*reverse name lookup*)?**
- A. A
 - B. SOA
 - C. CNAME
 - D. PTR
7. **Što od navedenog sadrži kontrole kojima reguliramo DNS-predmemoriranje (*caching*)?**
- A. Kartica *Forwarders* na svojstvima poslužitelja.
 - B. Čarobnjak *New Zone*.
 - C. Kartica *Root Hint* na svojstvima poslužitelja.
 - D. Kartica *Start of Authority* (SOA) na svojstvima zone.
8. **Koji se od ovih TCP/IP-parametara obično predaje klijentu kao DHCP-mogućnost opsega (*scope option*)?**
- A. Maska pod mreže (*subnet mask*)
 - B. Duljina najma (*lease duration*)
 - C. Zadani pristupnik (*default gateway*)
 - D. DNS-poslužitelj.

5. Instalacija i administriranje *Active Directory*

Nakon ove cjeline moći ćete:

- instalirati novu šumu instalacijom prvog domenskog kontrolora u domeni
- izraditi objekte AD DS-a: računala, korisnike i skupine.

5.1. Iz predavanja

Active Directory je skup servisa koji se rabi za upravljanje identitetima i kontrolom pristupa resursima na mreži. *Active Directory Domain Services* (AD DS) je imenički servis koji omogućuje administratorima izraditi organizacijske oblasti koje nazivamo domenama (*domains*).

Kod nove instalacije AD DS-a, prvi je korak izrada šume (*forest*), tako da se napravi prva domena u šumi, na prvom domenskom kontroloru (*domain controller*). Nakon toga se mogu izraditi dodatni domenski kontrolori u toj domeni ili se mogu dodati nove domene u šumu.

S *Windows Serverom 2012 R2* može se instalirati AD DS na instalaciju *Server Core*, a poslužitelj se može promovirati u domenskog kontrolora, sve pomoću *PowerShella*.

Dodavanje računala u domenu mora se inicirati na strani računala i mora ga obaviti člana lokalne skupine *Administrators*.

Korisnici (*users*) i računala (*computers*) osnovni su objekti u AD DS-u, a organizacijska je jedinica najmanja jedinica na koju implementiramo postavke pravilnika skupine (*Group Policy*) ili na koju delegiramo administrativna prava za upravljanje.

Korisnike, računala i organizacijske jedinice izrađujemo i njima upravljamo pomoću posebnih alata kao što su to npr. *Active Directory Users & Computers* (AD U&C) ili *Active Directory Administrative Center* (AD AC).

Gniježđenje skupina je izraz kojim se koristimo kad skupine postavljamo kao članove neke druge skupine.

5.2. Važni pojmovi

pojam	kratak opis
šuma (<i>forest</i>)	Šuma je vršno spremište koje udomačuje jednu ili više domena unutar svojih sigurnosnih granica.
korijenska domena šume (<i>forest root domain</i>)	To je prva domena u šumi, a njezino ime se odnosi na samu šumu.
Domena (<i>domain</i>)	Domena je logičko spremište mrežnih objekata s kojima dijeli imeničku bazu, sigurnosnu politiku i pouzdan odnos između drugih domena.
domenski kontrolor (<i>domain controller</i>)	Domenski kontrolor sadrži informacije o domenskim objektima i replicira ih na druge kontrolore u domeni.
globalni katalog (<i>global catalog</i>)	Globalni katalog je indeks svih AD DS-ovih objekata u šumi. Kad objekt domene traži informaciju o objektu iz druge domene, kontaktira se globalni katalog.

5.3. Korisne naredbe

naredba	kratak opis naredbe
dcdiag	<p>Za potvrdu da je domenski kontrolor registriran u DNS-u rabi se naredba dcdiag. Puna naredba koju treba izvršiti s administratorskim ovlastima glasi:</p> <pre>dcdiag /test:registerindns /dnsdomain:<domain name> /v</pre> <p>Naredba dcdiag inače analizira stanje domenskih kontrolora te izvještava o problemima prikazujući izlaz u prozoru naredbenog retka. Izlaz se može preusmjeriti u datoteku koristeći se parametarom <code>/f:<LogFile></code>.</p> <p>Naredba dcdiag mora se pokrenuti s povišenim ovlastima (<i>elevated command prompt</i>) tako da naredbeni redak pokrećemo uz odabir mogućnosti <i>Run As Administrator</i> ili kroz administratorski naredbeni redak <i>Command Prompt (Admin)</i>.</p>

5.4. Vježba: Instalacija nove šume

1. Poslužitelj s instaliranim *Windows Serverom 2012 R2* član je radne skupine i ima statičku IP-adresu. U mreži ne postoji DNS-poslužitelj. Poslužitelj nema instaliranih rola i uloga osim početnih.

Na poslužitelj instalirajte novu šumu s ovim zahtjevima:

1. Ime nove šume: **lab.local**.
2. U šumi neće biti domenskih kontrolora prijašnjih inačica *Windows Servera*.
3. Potrebno je zadovoljiti uvjete složene zaporke, npr. **Passw0rd!**.
4. Ponovno pokrenuti poslužitelj kad se to traži u postupku i na kraju se prijaviti u domenu.

Ako zahtjevom nije drugačije određeno, sve druge postavke ostavite na ponuđenim vrijednostima.

5.5. Vježba: Izrada AD-objekata

1. U domeni **lab.local** alatom *Active Directory Users & Computers* izradite ove objekte:
 1. U korijenu domene izradite organizacijsku jedinicu (OU) naziva **Lab**.
 2. U OU **Lab**-u napravite nove OU-e naziva **LabRacunala** i **LabKorisnici**.
 3. U OU-u **LabRacunala** napravite novi objekt računala naziva **labpc1**.
 4. U OU-u **LabKorisnici** izradite predložak korisnika, korisničkog imena **predlozak1**, proizvoljnog imena i prezimena. Predložak mora imati isključenu mogućnost *User Must Change Password At Next Logon*, a uključene mogućnosti *Password Never Expires* i *Account Is Disabled*. Potrebno je zadovoljiti uvjete složene zaporke, npr. **Passw0rd!**.
 5. U OU-u **LabKorisnici** iz predloška napravite dva korisnika korisničkih imena **labkorisnik1** i **labkorisnik2**, proizvoljnih imena i prezimena.
 6. Označite korisničke račune **labkorisnik1** i **labkorisnik2** te im u zajedničkom prozoru sa svojstvima promijenite atribut *Description* u „Lab korisnici za testiranje“.
2. Zatvorite konzolu AD U&C.

3. Otvorite konzolu *Active Directory Administrative Center*:
 1. Za korisnika **labkorisnik1** resetirajte zaporku u **Pa2sword!**.
 2. Za korisnika **labkorisnik2** omogućite korisnički račun.
 3. U OU-u **Lab** izradite novu skupinu naziva **labgrupa1** s inicijalnim postavkama.
 4. Dodajte korisnika **labkorisnik2** u skupinu **labgrupa1**.
4. Zatvorite konzolu AD AC.

5.6. Dodatna vježba: Provjera DNS-registracije

1. Provjerite je li domenski kontrolor uspješno registrirao svoj zapis u DNS-u. Za tu potrebu, s administratorskim ovlastima pokrenite naredbu **dcdiag** s potrebnim parametrima.

Kako glasi puna sintaksa naredbe za ime domene iz primjera (lab.local)?

5.7. Pitanja za ponavljanje

1. Što od ovog ne možemo reći za AD DS?
 - A. Pruža prilagodljiv servis za izdavanje i upravljanje certifikatima.
 - B. Pohranjuje i upravlja informacijama o mrežnim resursima.
 - C. Omogućuje upravljanje iz jednog središta.
 - D. Daje podršku za imeničko-omogućene aplikacije poput *Exchangea*.
2. Točno ili netočno: printeri i dijeljene mape mogu biti pohranjene u AD-u?
 - A. Točno.
 - B. Netočno.
3. Koji akreditiv mora biti priložen kad se instalira nova šuma?
 - A. Lokalni korisnik.
 - B. Domenski korisnik.
 - C. Lokalni administrator.
 - D. Domenski administrator.

4. **AD DS zahtijeva DNS-infrastrukturu.**
- A. Točno.
 - B. Netočno.
5. **Što od navedenog klijent domene *Active Directory* rabi za lociranje objekta druge domene?**
- A. DNS.
 - B. DHCP.
 - C. *Global Catalog*.
 - D. GPO.
6. **U *Windows Serveru 2012 R2* nužno je pokretanje naredbe *Adprep.exe* prije svake instalacije domenskog kontrolora.**
- A. Točno.
 - B. Netočno.

6. Izrada i upravljanje pravilnicima skupine (*Group Policy*)

Nakon ove cjeline moći ćete:

- izraditi GPO u konzoli *Group Policy Management*
- mijenjati postavke GPO-a kroz *Group Policy Management Editor*
- mijenjati i upravljati postavkama u *Windows Firewallu*.

6.1. Iz predavanja

Group Policy ili pravilnici skupine sastoje se od korisničkih i računalnih postavki koje se mogu primijeniti za npr. vrijeme pokretanja računala ili za vrijeme korisnikove prijave u sustav (*logon*). Te postavke mogu se primijeniti za prilagođavanje korisnikove okoline, za primjenu sigurnosnih okvira i kao pomoć u pojednostavljenju korisničke i računalne administracije.

U AD DS-u pravilnici skupine mogu se pridružiti *site*ovima, domenama i organizacijskim jedinicama. Na svakom računalu početno postoji jedan lokalni pravilnik čije se postavke prepisuju postavkama iz Active Directory pravilnika skupine.

Konzola *Group Policy Management* je alat koji se rabi za izradu i izmjene objekata pravilnika skupine (GPO, *Group Policy Objects*) i njihovih postavki.

Central Store je kopija datoteka ADMX pohranjena na domenskom kontroloru SYSVOL. Izrađuje se tako da se mapa C:\Windows\PolicyDefinitions kopira na C:\Windows\SYSVOL\sysvol\<domena>\Policies na domenskom kontroloru.

Većina sigurnosno orijentiranih postavki može se naći unutar čvora *Windows Settings* u čvoru *Computer Configuration* GPO-a.

Postavke lokalnih pravilnika upravljaju radnjama koje korisnici mogu izvesti na određenom računalu i određuju hoće li se te radnje zabilježiti u zapisniku događaja.

Nadgledanje se može konfigurirati tako da se nadgleda uspješna radnja (*success*), pogrešna (*failure*) ili oboje.

Administratori se mogu koristiti sigurnosnim predlošcima za konfiguraciju lokalnih pravilnika, članstava u skupinama, postavkama zapisnika događaja i za druge postavke.

Windows Server 2012 R2 sve korisnike drži dalje od administratorskog pristupa sustavu, sve dok se ne pojavi potreba za izvođenjem

administrativne zadaće. Mehanizam kojim se to čini naziva se *User Account Control* (UAC) – kontrola korisničkog računa, a inicijalno je uključena u svim instalacijama *Windows Servera 2012*, no može se konfigurirati ili posve isključiti (nije preporučljivo).

Vatrozid (*firewall*) je softverski program koji štiti računalo tako da dopušta određenu vrstu mrežnog prometa u sustav i iz sustava, a blokira sav drugi promet.

Vatrozid je u osnovi niz filtera koji ispituju sadržaj paketa i prometnih uzoraka koji dolaze i izlaze iz mreže da bi se odredilo koji se paketi mogu propustiti.

Početna pravila vatrozida dopuštaju promet koji se rabi za standardne mrežne funkcije *Windowsa*, kao što je dijeljenje datoteka i printera. Za izlazni mrežni promet *Windows Firewall* dopušta izlaz cjelokupnom prometu, osim onome koji je zabranjen pravilom.

Windows Firewall iz upravljačke ploče (*control panel*) dizajniran je tako da omogući administratoru osnove vatrozidne konfiguracijske zadaće.

Za puni pristup konfiguracijskim postavkama *Windows Firewalla* mora se rabiti *Windows Firewall With Advanced Security*.

6.2. Važni pojmovi

pojam	kratak opis
<i>Central Store</i>	Jednostruka kopija datoteka ADMX pohranjena na domenskom kontroloru.
<i>Starter GPO</i>	Početni GPO, u osnovi predložak (<i>template</i>) za izradu domenskih GPO-a koji se temelje na standardnoj kolekciji postavki.
<i>Network Discovery</i>	Skup vatrozidnih pravila koji određuju portove koje <i>Windowsi</i> rabe za pretraživanje mreže.
<i>.wfw - policy file</i>	Datoteka s nastavkom <i>.wfw</i> u koju se izvoze sve postavke instalacije <i>Windows Firewall</i> i sva pravila uključujući početna i ona koje je napravio administrator.

6.3. Korisne naredbe

naredba	kratak opis naredbe
New-GPO	<i>cmdlet u Windows PowerShellu koji se može rabiti za kopiranje postavki iz početnog (starter) GPO-a u novi GPO.</i>
gpupdate /force	Osvježava lokalne ili postavke <i>AD Group Policya</i> , uključujući sigurnosne postavke.

6.4. Vježba: Konfiguriranje *Central Storea*

1. Konfigurirajte *Central Store* tako da se administrativni predlošci **AMDX** rabe iz volumena domenskog kontrolora **SYSVOL**. Ispravno konfiguriranje *Central Storea* treba utvrditi u *Group Policy Management Editoru*.

6.5. Vježba: Definiranje lokalnih pravilnika

1. U *Default Domain Policyu* uredite postavku *Audit Policy* naziva *Audit Directory Service Access* tako da se nadziru svi pristupi **Failure**.

6.6. Vježba: Izrada GPO-a i povezivanje na OU

1. U AD U&C napravite novu organizacijsku jedinicu naziva **Kiosk** i izradite novi GPO povezan na OU **Kiosk**.
2. U GPO-u treba odabrati postavke: omogućiti račun **Guest** i preimenovati ga u **Gost**.

6.7. Vježba: Izvoz i uvoz pravila *Windows Firewalla*

1. U konzoli *Windows Firewall With Advanced Security* napravite ove radnje:
 - izvezite (*export*) postavke *Windows Firewalla*
 - omogućite pravilo *Inbound Remote Desktop – User Mode (TCP-In)*
 - izadite novo pravilo *Inbound* s postavkama: Rule Type: **Port**; Protocol And Port: **TCP 5555**; Action: **Allow the Connection**; Profile: **Domain**; Name: **TCP 5555 In**.
 - uvezite (*import*) prije izvezenih postavki.

Što se dogodilo s prije omogućenim pravilom i s novim pravilom „TCP 5555 In“ nakon uvoza prije izvezenih postavki?

- A. Izmijenjene i novododane postavke ostale su definirane, jer prije nisu bile postavljene.

- B. Izmijenjene i novododane postavke izgubile su se, jer se pri izvozu i uvozu postavki u *Windows Firewall* izvozi i uvozi cijela datoteka neovisno o statusu pojedinačnih pravila.

6.8. Dodatna vježba: *Default Domain Controllers Policy*

1. Za sve domenske kontrolore (koji se nalaze u spremištu *Domain Controllers*) treba izraditi poruku koja će se prikazivati na konzoli poslužitelja pri prijavi u sustav (*logon*). Budući da se ne preporuča izravno mijenjanje *Default Domain Controlles Policya*, napravite novi GPO i povežite ga na spremište (OU) *Domain Controllers*.
2. U novoizrađenom GPO-u uredite postavku *Interactive logon: Message text for users attempting to log on* i postavku *Interactive logon: Message title for users attempting to log on* tako da naslov prozora (*title*) i poruka (*text*) upozoravaju na zabranu neovlaštenog ulaska u sustav (proizvoljno).

6.9. Pitanja za ponavljanje

1. **Kojoj vrsti datoteka alati pravilnika skupine (Group Policy) pristupaju na *Central Store*?**
 - A. Sigurnosnim predlošcima.
 - B. Datotekama ADM.
 - C. Datotekama ADMX.
 - D. Objektima pravilnika skupine.
2. **Koja od navedenih lokalnih GPO-a uzima prednost u sustavu s više lokalnih GPO-a?**
 - A. *Local Group Policy*.
 - B. *Administrators Group Policy*.
 - C. *Non-administrators Group Policy*.
 - D. *User-specific Group Policy*.
3. **Koja se tehnika može primijeniti za primjenu postavki GPO-a na određenu skupini korisnika u nekom OU-u?**
 - A. GPO-povezivanje (*linking*).
 - B. Administrativni predlošci.
 - C. Sigurnosno filtriranje (*security filtering*).
 - D. Početni (*starter*) GPO.
4. **Kad se objekt pravilnika skupine (GPO) s vrijednošću *Not Configured* (nije postavljeno) primjeni u sustavu u kojem je ta postavka isključena, kakav je rezultat?**
 - A. Dolazi do konfiguracijske pogreške.
 - B. Postavka prima vrijednost *Not Configured* (nije postavljeno).
 - C. Postavka se mijenja u *Enabled* (omogućeno).
 - D. Postavka ostaje isključena.
5. **Koji se od alata rabe za promjenu postavki sigurnosnih predložaka?**
 - A. *Group Policy Object Editor*
 - B. *Security Templates snap-in*
 - C. *Active Directory Users & Computers*
 - D. Konzola *Group Policy Management*.

6. **Koje dvije od navedenih su lokalne skupine u koje se mogu dodati korisnici pomoću upravljačke ploče *Windows*?**
- A. *Users*.
 - B. *Power Users*.
 - C. *Administrators*.
 - D. *Guests*.
7. **Koja je od ovih tvrdnji točna za *User Access Control (UAC)* u *Windows Serveru 2012 R2*?**
- A. UAC se ne može ni prilagoditi ni isključiti.
 - B. UAC se može i prilagoditi i isključiti.
 - C. UAC se može samo prilagoditi, a ne možemo ga isključiti.
 - D. UASC se može samo isključiti.
8. **Koje su dvije od ovih tvrdnji vezanih uz *Windows Firewall* točne?**
- A. Primjena vatrozidnih pravila pomoću *Group Policya* prepisuje sva postojeća pravila na ciljanom računalu.
 - B. Primjena vatrozidnih pravila pomoću *Group Policya* kombinira pravila s postojećima pravilima na ciljanom računalu.
 - C. Uvoz vatrozidnih pravila s drugog računala prepisuje sva postojeća pravila na ciljnom računalu.
 - D. Uvoz vatrozidnih pravila s drugog računala kombinira se s postojećim pravilima na ciljanom računalu.

7. Odgovori na pitanja

U ovoj cjelini nalaze se odgovori na pitanja za ponavljanje.

1. Instalacija i konfiguracija poslužitelja

1. Točan odgovor je B, samo 64-bitni sustavi.
2. Točan odgovor je C, *WinSxS*.
3. Točan odgovor je D, *Uninstall-WindowsFeature*.
4. Točan odgovor je A, *Switch Independent Mode*.
Izvedba neovisna o preklopniku osigurava toleranciju na pogrešku.
5. Točan odgovor je C, *netdom.exe*.
6. Točni odgovori su C i D, zrcaljen volumen i RAID 5 volumen.

2. Konfiguriranje poslužiteljskih uloga i značajki

1. Točan odgovor je B, autorizacija. Autorizacija je postupak kojim se korisniku daju prava na resurs prema dodijeljenim mu dozvolama. Autentikacija je postupak identifikacije korisnika.
2. Točan odgovor je D. Sigurnosni principal je korisnik, skupina ili računalo kojem je dodijeljena dozvola.
3. Točan odgovor je C, 64. Prije nego što počne prepisivati najstarije kopije u sjeni, po volumenu se može pohraniti 64 kopija.
4. Točan odgovor je B, printer.
5. Točan odgovor je A, isključiti dijeljenje printera. Prestanak dijeljenja printera onemogućit će slanje dokumenata na ispis. Isključenje iz liste *Active Directory* onemogućiti će nalaženje printera pretraživanjem, ali i dalje će biti dostupan. Promjena porta onemogućit će slanje na pisač, ali ne i na printer. Promjena dijeljenog imena otežat će nalazak printera, ali kad se nađe, bit će moguć ispis na printer.

3. Konfiguriranje *Hyper-V*-a

1. Točan odgovor je A, Tip I virtualizacije.
2. Točan odgovor je C, *Windows Memory Weight* kontrolira alociranje memorije virtualnim strojevima, ali ne i količinu memorije za podizanje sustava.
Smart paging je potreban za privremenu memoriju na disku, *Dynamic Memory* omogućuje određivanje manje radne memorije nego startne memorije, a *Guest Integration Services* je uvjet da gostujući OS rabi *Dynamic Memory*.
3. Točan odgovor je B, u nadređenu (*parent*) particiju.
4. Točni odgovori su A i D.

5. Točan odgovor je D, neograničen.
6. Točan odgovor je C, privatni preklopnik ne može komunicirati ni s nadređenom particijom ni s vanjskom mrežom, samo s drugim gostujućim OS-om.

4. Implementacija i konfiguriranje osnovnih mrežnih servisa

1. Točan odgovor je B, registriranu kod IANA.
2. Točan odgovor je C, *unique-local unicast adresa*.
3. Točan odgovor je A, 255.255.224.0.
Oznaka /19 označava tri bita mreže u trećem oktetu, što daje $128+64+32 = 224$. Prva dva okteta su 255, četvrti je 0, što daje masku podmreže: 255.255.224.0.
4. Točan odgovor je D, tuneliranje.
5. Točan odgovor je B, *relay agent* usmjerava DHCP-promet na druge mreže.
6. Točan odgovor je D, PTR.
7. Točan odgovor je D, SOA kartica sadrži TTL-kontrole.
8. Točan odgovor je C, mogućnost *Router* tipičan je primjer mogućnosti opsega, jer klijentski zadani pristupnik (*default gateway*) mora biti na istoj podmreži kao i klijentska IP-adresa.

5. Implementacija i administriranje *Active Directory*a

1. Točan odgovor je A, AD DS nije servis za certifikate.
2. Točan odgovor je A, printeri i dijeljene mape mogu biti pohranjene u AD.
3. Točan odgovor je C, lokalni administrator.
4. Točan odgovor je A, AD DS zahtijeva DNS-infrastrukturu.
5. Točan odgovor je C, *Global Catalog*.
6. Točan odgovor je B, netočno. Adprep.exe više ne treba pokretati u *Windows Serveru 2012 R2* prije instalacije domenskog kontrolora.

6. Izrada i upravljanje pravilnicima skupine (*Group Policy*)

Odgovor uz vježbu 6.7: točan odgovor je B.

1. Točan odgovor je C, pretpostavljeno traže XML-administrativne predloške (ADMX) u *Central Storeu*.
2. Točan odgovor je D, među lokalnim GPO-vrstama, *User-specific* se primjenjuje posljednja.
3. Točan odgovor je C, sigurnosnim filtriranjem možemo ograničiti primjenu pravilnika skupine na određene korisnike nekog AD DS-spremišta (OU).

4. Točan odgovor je D, postavka *Not Configured* nema utjecaja na postojeću vrijednost u sustavu.
5. Točan odgovor je B. *Security Templates snap-in* se koristi za uređivanje postavki sigurnosnih predložaka.
6. Točan odgovor je A, C. *Users* i *Administrators* su skupine u koje se dodaju korisnici kad ih izradimo pomoću upravljačke ploče.
7. Točan odgovor je B. UAC se može i prilagoditi i isključiti.
8. Točni odgovori su B i C. Pravila primijenjena pravilnikom skupine kombiniraju se s postojećima, a pravila vatrozida koja su uvezena s drugog računala prepisuju se preko postojećih.

8. Popis literature

1. *Microsoft Technet*, <https://technet.microsoft.com/>
2. *Microsoft Virtual Academy*, <https://www.microsoftvirtualacademy.com/>