Josip Torbar

Planiranje napredne infrastrukture

PROJEKT

Sadržaj

[Sadržaj 1](#_Toc59309104)

[1. Sažetak 2](#_Toc59309105)

[2. Opis infrastrukture 2](#_Toc59309106)

[3. Priprema infrastrukture 5](#_Toc59309107)

[3.1. Inicijalizacija diskova 5](#_Toc59309108)

[3.2. Postavljanje IP adresa 5](#_Toc59309109)

[4. Razrada projekta – projektno rješenje 5](#_Toc59309110)

[4.1. Kreiranje domene na SERVERDC poslužitelju 5](#_Toc59309111)

[4.2. Dodavanje ostalih poslužitelja i klijentskog računala u domenu 6](#_Toc59309112)

[4.3. Kreiranje korisnika 7](#_Toc59309113)

[4.4. Promocija SERVER1 poslužitelja u sekundarni DC i DNS 10](#_Toc59309114)

[4.5. Konfiguracija DNS-a 11](#_Toc59309115)

[4.6. Konfiguracija Storage Spaces-a na SERVER1 12](#_Toc59309116)

[4.7. Konfiguracija DAC-a (Dynamic Access Control-a) na SERVER1 14](#_Toc59309117)

[4.8. Konfiguracija DFS (Distributed File System) replikacije na SERVER 2 i SERVER3 20](#_Toc59309118)

[4.9. Konfiguracija CA (Certification Authority) na SERVER3 22](#_Toc59309119)

[4.10. Konfiguracija IIS-a (Internet Information Services-a) na SERVER1 i SERVER2 29](#_Toc59309120)

[4.11. Konfiguracija NLB (Network Load Balancing) clustera na SERVER1 i SERVER2 32](#_Toc59309121)

[4.12. Konfiguracija DHCP (Dynamic Host Configuration Protocol) failover clustera na SERVER 2 i SERVER3 34](#_Toc59309122)

[4.13. Instalacija Docker kontejnera na SERVER3 36](#_Toc59309123)

[4.14. Nadogradnja SERVER3 na Windows Server 2019 38](#_Toc59309124)

[5. Zaključak 38](#_Toc59309125)

[6. Reference 38](#_Toc59309126)

1. Sažetak

Cilj projekta iz Planiranja napredne infrastrukture jest napraviti dizajn rješenja, plan implementacije te samu implementaciju infrastrukture prema zadanim klijentskim zahtjevima. Klijentu Torbar Klinika d.o.o. potrebno je osposobiti infrastrukturu od 4 Windows servera 2016 u domeni torbar-klinika.hr, jednog klijentskog Windows 10 računala te jednog CentOS 8 računala.

1. Opis infrastrukture

**VM SERVERDC – WS2016**

FQDN: serverdc.torbar-klinika.hr

vCPUs: 2CPUs

Memory: 2GB

Storage disks:

Disk 0 – 60GB

Disk 1 – 10GB

Disk 2 – 10GB

Disk 3 – 10GB

Disk 4 – 10GB

eth0: 192.168.44.1/24

eth1: auto (192.168.44.0/24)

**VM SERVER1 – WS2016**

FQDN: server1.torbar-klinika.hr

vCPUs: 2CPUs

Memory: 2GB

Storage disks:

Disk 0 – 60GB

Disk 1 – 10GB

Disk 2 – 10GB

Disk 3 – 10GB

Disk 4 – 10GB

eth0: 192.168.44.2/24

eth1: auto (192.168.44.0/24)

**VM SERVER2 – WS2016**

FQDN: server2.torbar-klinika.hr

vCPUs: 2CPUs

Memory: 2GB

Storage disks:

Disk 0 – 60GB

Disk 1 – 10GB

Disk 2 – 10GB

eth0: 192.168.44.3/24

eth1: auto (192.168.44.0/24)

**VM SERVER3 – WS2016 (2019[[1]](#footnote-1))**

FQDN: server3.torbar-klinika.hr

vCPUs: 2CPUs

Memory: 4GB

Storage disks:

Disk 0 – 60GB

Disk 1 – 10GB

Disk 2 – 10GB

eth0: 192.168.44.4/24

eth1: 172.16.10.254/24; GW: 172.16.10.1 (COS1, ens256)

**VM CLI1 – Win10**

FQDN: client1.torbar-klinika.hr

vCPUs: 2CPUs

Memory: 4GB

Storage disk:

Disk 0 – 60GB

eth0: auto (192.168.44.0/24)

**VM COS1 – CentOS8**

Hostname: CentOS1.torbar-klinika.local

vCPUs: 1CPU

Memory: 4GB

Storage disks:

/dev/sda – 16GB

/dev/sdb – 10GB

/dev/sdc – 10GB

/dev/sdd – 10GB

ens192: 172.60.2.43/24

ens224: 172.16.10.1/24; GW 172.60.2.43

**Role:**

SERVERDC – Domain controller, primary DNS server

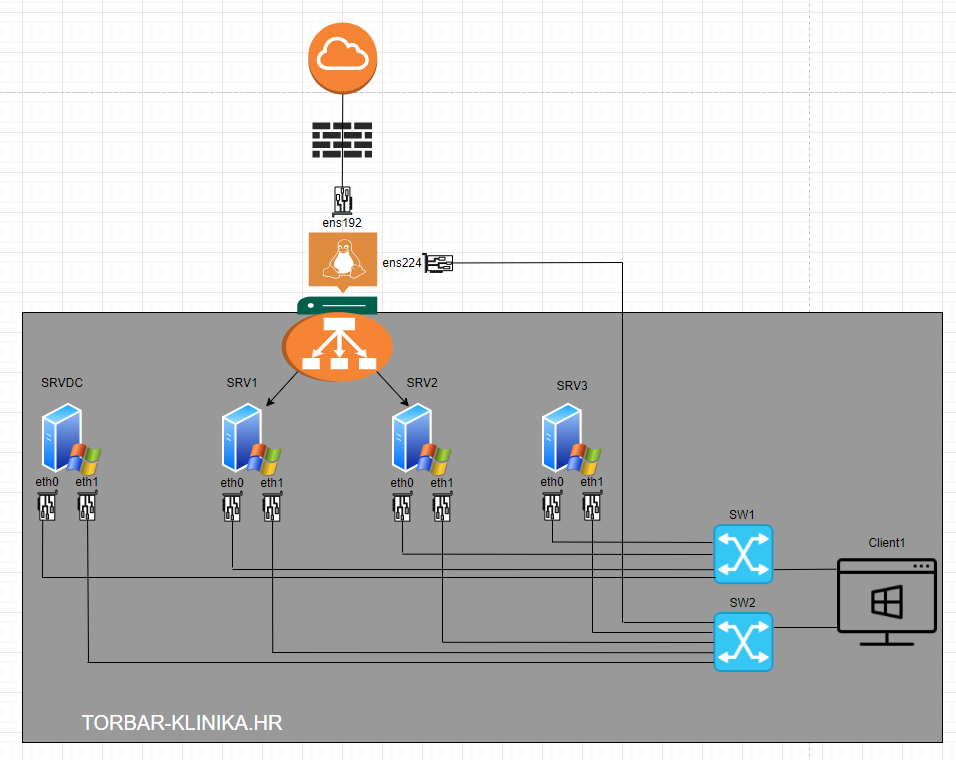
SERVER1 – Secondary domain controller, secondary DNS server, DAC server, IIS, NLB

SERVER2 – Member server, DFS server, DHCP server, IIS, NLB

SERVER3 – Member server, DFS server, DHCP server, CA

Client1 – Klijentsko računalo

COS1 – reverse proxy poslužitelj za NLB cluster



Slika – Skica infrastrukture

1. Priprema infrastrukture
   1. Inicijalizacija diskova

Prije bilo kakve konfiguracije infrastrukture, inicijalizirat ćemo diskove na svim Windows serverima. To ćemo učiniti pomoću powershella.

Get-disk | ?{$\_.number -ne 0} | Set-Disk -IsOffline $false

Get-disk | ?{$\_.number -ne 0} | Set-Disk -IsReadOnly $false

Get-disk | ?{$\_.number -ne 0} | Initialize-Disk -PartitionStyle GPT

* 1. Postavljanje IP adresa

Nakon inicijalizacije diskova, postavit ćemo IP adrese na svim eth0 mrežnim adapterima Windows poslužitelja i Windows klijentskom računalu kako je navedeno u opisu infrastrukture. Svim poslužiteljima članovima domene i klijentskom računalu za DNS server ćemo postaviti **192.168.44.1**.

1. Razrada projekta – projektno rješenje
   1. Kreiranje domene na SERVERDC poslužitelju

Sada je sve spremno za podizanje domene torbar-klinika.hr. Na SERVERDC poslužitelju kroz Server Manager instaliramo AD DS rolu.

Add Roles and Features 🡪 Server roles 🡪 AD DS (Active Directory Domain Services)

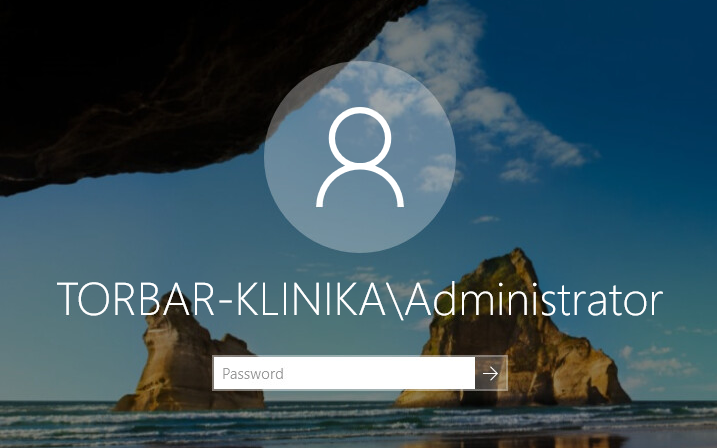
Na kraju instalacije promoviramo poslužitelj u DC (Domain Controller).

Otvara se novi prozor Deployment Configuration. Odabiremo opciju *Add a new forest* i u polje *Root domain name* upisujemo torbar-klinka.hr.

U Domain Controller opcijama *functional level* je Windows Server 2016, ovaj poslužitelj će ujedno biti *DNS server* i *Global catalog* te ćemo kao DSRM (Directory Services Restore Mode) lozinku postaviti „Pa$$w0rd“.

U sljedećim koracima odabiremo defaultno zadane postavke.

Kada promocija poslužitelja završi, on će se sam ponovno pokrenuti te će time biti podignuta funkcionalna domena torbar-klinka.hr.

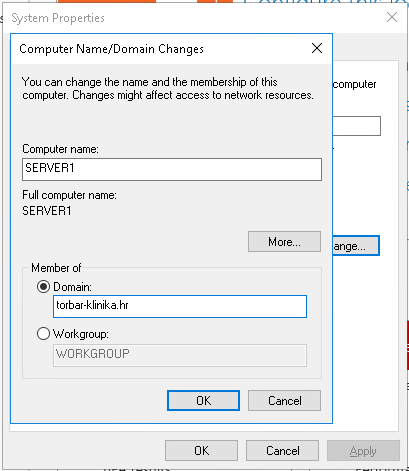


Slika – login screen na SERVERDC nakon podizanja domene torbar-klinka.hr

* 1. Dodavanje ostalih poslužitelja i klijentskog računala u domenu

Nakon što se poslužitelj SERVERDC ponovno pokrenuo, spremni smo za dodavanje ostalih poslužitelja u domenu. To ćemo napraviti jednostavnom procedurom koju ćemo ponoviti na svim poslužiteljima i klijentskom računalu.

Kada se prijavimo na poslužitelj/klijentsko računalo, u Windows tražilicu upisujemo „Change Workgroup Name“. Otvara nam se prozor System Properties i unutar njega kartica Computer Name. Pritiskom na gumb *Change…* otvara nam se novi prozor u kojem su informacije o računalu, konkretno njegovo ime i članstvo u domeni/workgroup-u. Odabiremo Domain i upisujemo ime domene.



Slika – SERVER1 Computer Name/Domain Changes unutar System Properties-a

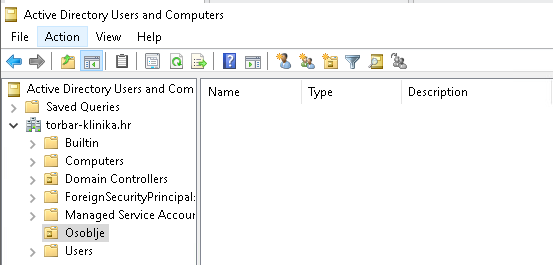
Pritiskom na gumb OK otvara nam se prozor koji zahtjeva autentikaciju domenskog administratora kako bi računalo dodali u domenu. Unosimo credentials-e te nakon poruke o dobrodošlici u domenu ponovno pokrećemo računalo. Ovu proceduru ponovimo na preostalim Windows poslužiteljima i Windows 10 klijentskom računalu.

* 1. Kreiranje korisnika

Prije nego što krenemo s kreiranjem korisnika, napravit ćemo organizacijsku jedinicu *Osoblje.* To ćemo napraviti kroz Powershell, koji pokrećemo s administratorskim pravima.

New-ADOrganizationalUnit -Name „Osoblje“ -Path „DC=TORBAR-KLINIKA,DC=HR“

Izvršenje naredbe provjerit ćemo u alatu Active Directory Users and Computers.



Slika – OU Osoblje unutar Active Directory Users and Computers

Sada ćemo kreirati korisnike 1-10 - održavanje, 11-20 - sestre, 21-35 - doktori, 36-40 - uprava, 41-50 hitna. To ćemo odraditi putem par jednostavnih powershell skripti.

U varijablu $path stavit ćemo putanju OU-a, u varijablu $username korisničko ime (npr. održavanje) te u varijablu $count brojeve od 1 do 10. Te varijable ćemo koristiti u foreach petlji te si time olakšati kreiranje korisnika. Svi korisnici će kao lozinku imati postavljeno „Pa$$w0rd“.

**Skripta za kreiranje korisnika 1-10:**

$path=“OU=Osoblje,DC=TORBAR-KLINIKA,DC=HR“

$username="odrzavanje"

$count=1..10

foreach ($i in $count)

{ New-AdUser -Name $username$i -Department Odrzavanje -Path $path -Enabled $True `

-ChangePasswordAtLogon $true -AccountPassword (ConvertTo-SecureString `

"Pa$$w0rd" -AsPlainText -force) -passThru }

**Skripta za kreiranje korisnika 11-20:**

$path=“OU=Osoblje,DC=TORBAR-KLINIKA,DC=HR“

$username="sestra"

$count=1..10

foreach ($i in $count)

{ New-AdUser -Name $username$i -Department Sestre -Path $path -Enabled $True `

-ChangePasswordAtLogon $true -AccountPassword (ConvertTo-SecureString `

"Pa$$w0rd" -AsPlainText -force) -passThru }

**Skripta za kreiranje korisnika 21-35:**

$path=“OU=Osoblje,DC=TORBAR-KLINIKA,DC=HR“

$username="doktor"

$count=1..15

foreach ($i in $count)

{ New-AdUser -Name $username$i -Department Doktori -Path $path -Enabled $True `

-ChangePasswordAtLogon $true -AccountPassword (ConvertTo-SecureString `

"Pa$$w0rd" -AsPlainText -force) -passThru }

**Skripta za kreiranje korisnika 36-40:**

$path=“OU=Osoblje,DC=TORBAR-KLINIKA,DC=HR“

$username="uprava"

$count=1..5

foreach ($i in $count)

{ New-AdUser -Name $username$i -Department Uprava -Path $path -Enabled $True `

-ChangePasswordAtLogon $true -AccountPassword (ConvertTo-SecureString `

"Pa$$w0rd" -AsPlainText -force) -passThru }

**Skripta za kreiranje korisnika 41-50:**

$path=“OU=Osoblje,DC=TORBAR-KLINIKA,DC=HR“

$username="hitna"

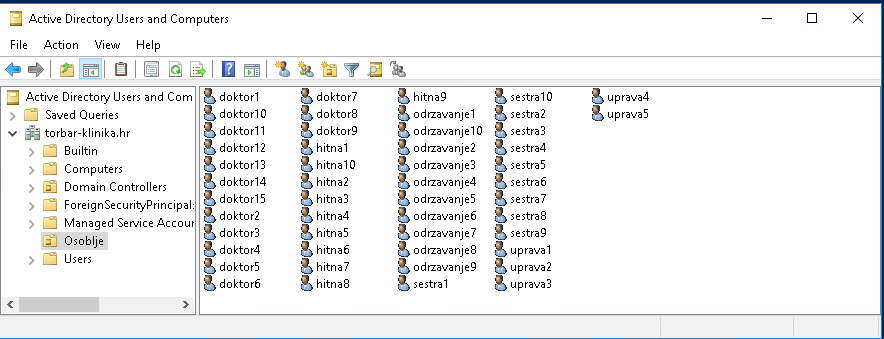
$count=1..10

foreach ($i in $count)

{ New-AdUser -Name $username$i -Department Hitna -Path $path -Enabled $True `

-ChangePasswordAtLogon $true -AccountPassword (ConvertTo-SecureString `

"Pa$$w0rd" -AsPlainText -force) -passThru }



Slika – kreirani korisnici 1-50

Kada smo uspješno kreirali korisnike, kreirat ćemo im i pripadajuće grupe te ih dodati u iste.

**Odrzavanje:**

New-ADGroup -Name "Odrzavanje" -SamAccountName Odrzavanje -GroupCategory Security`

-GroupScope Global -Path "OU=Osoblje,DC=TORBAR-KLINIKA,DC=HR"

**Sestre:**

New-ADGroup -Name "Sestre" -SamAccountName Sestre -GroupCategory Security`

-GroupScope Global -Path "OU=Osoblje,DC=TORBAR-KLINIKA,DC=HR"

**Doktori:**

New-ADGroup -Name "Doktori" -SamAccountName Doktori -GroupCategory Security`

-GroupScope Global -Path "OU=Osoblje,DC=TORBAR-KLINIKA,DC=HR"

**Uprava:**

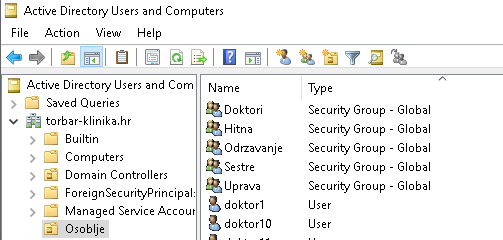
New-ADGroup -Name "Uprava" -SamAccountName Uprava -GroupCategory Security`

-GroupScope Global -Path "OU=Osoblje,DC=TORBAR-KLINIKA,DC=HR"

**Hitna:**

New-ADGroup -Name "Hitna" -SamAccountName Hitna -GroupCategory Security`

-GroupScope Global -Path "OU=Osoblje,DC=TORBAR-KLINIKA,DC=HR"



Slika – Kreirane grupe Odrzavanje, Sestre, Doktori, Uprava i Hitna

Korisnike ćemo dodati u grupe kroz Active Directory Users and Computers. Jednostavno označimo korisnike koje želimo staviti u pojedinu grupu, pritisnemo na njih desnim klikom miša, odaberemo opciju *Add to group…* i u prozor koji nam se otvori upišemo ime grupe.

* 1. Promocija SERVER1 poslužitelja u sekundarni DC i DNS

Kada smo završili s dodavanjem korisnika u AD, krećemo s promocijom poslužitelja SERVER1 u sekundarni Domain Controller i DNS server.

Ovaj postupak sličan je onome u poglavlju *4.1*, gdje smo kreirali domenu.

Add Roles and Features 🡪 Server roles 🡪 AD DS (Active Directory Domain Services)

Na kraju instalacije promoviramo poslužitelj u DC.

Otvara se novi prozor Deployment Configuration. Odabiremo opciju *Add a domain controller to an existing domain*, specificiramo domenu u koju ga želimo dodati kao DC te odabiremo credentials-e domenskog administratora kako bi izvršili promociju.

U Domain Controller opcijama *functional level* je Windows Server 2016, ovaj poslužitelj će ujedno biti *DNS server* i *Global catalog*. SERVER1 će replicirati sve informacije sa poslužitelja SERVERDC. Kao DSRM lozinku postavit ćemo „Pa$$w0rd“.

U sljedećim koracima odabiremo defaultno zadane postavke.

Kada promocija poslužitelja završi, on će se sam ponovno pokrenuti te će time biti podignuta funkcionalna domena torbar-klinka.hr.

* 1. Konfiguracija DNS-a

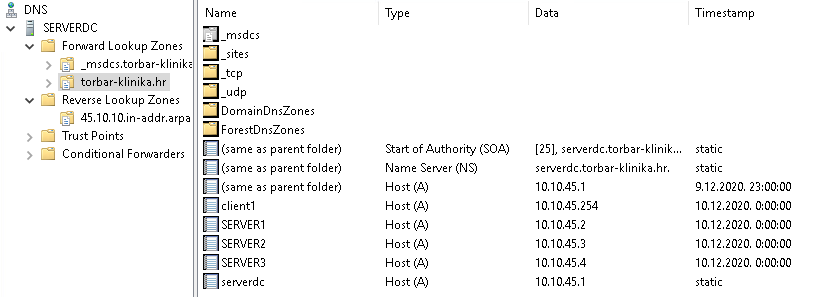
Kada smo završili s promocijom poslužitelja SERVER1 u RODC, krećemo s konfiguracijom primarne reverse lookup zone i postavljanjem pointer (PTR) zapisa. Također, trebat ćemo konfigurirati sekundarnu reverse lookup zonu na poslužitelju SERVER1. DNS konfiguriramo kroz Server Manager.

Tools 🡪 DNS 🡪 SERVERDC

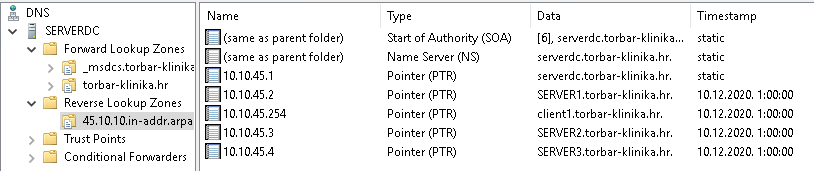
Novu zonu kreiramo desnim klikom miša na Reverse Lookup Zones i klikom na *New Zone…*

Otvara nam se New Zone Wizard u kojem ćemo kreirati novu IPv4 primarnu zonu koju ćemo pospremiti u AD i replicirat ćemo ju na sve DNS servere u našem forestu. Network ID zone će biti 10.10.45. Dopustit ćemo samo secure dynamic update.

Nakon što smo uspješno kreirali zonu, moramo ažurirati PTR zapise svih poslužitelja i klijenata u forward lookup zoni.



Slika – SERVERDC Forward Lookup Zones, torbar-klinika.hr



Slika – SERVERDC Reverse Lookup Zones, 45.10.10.in-addr-arpa

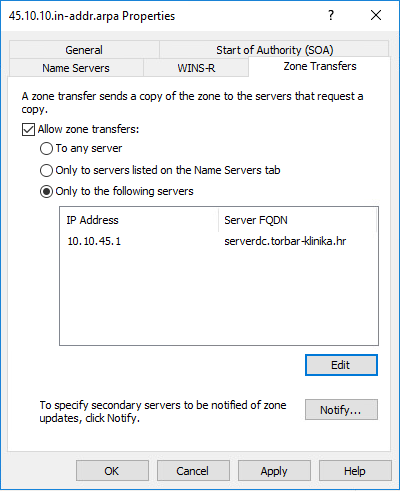
Ovime smo završili DNS konfiguraciju primarne zone na SERVERDC, sada ćemo konfigurirati sekundarnu na SERVER1. To ćemo također konfigurirati kroz Server Manager.

Tools 🡪 DNS 🡪 SERVER1

Novu zonu kreiramo desnim klikom miša na Reverse Lookup Zones i klikom na *New Zone…*

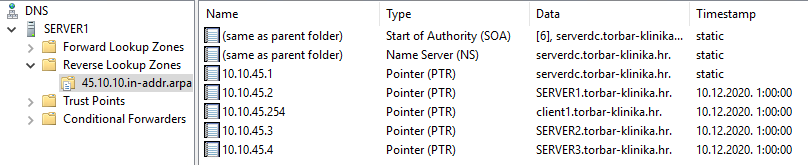
Otvara nam se New Zone Wizard u kojem ćemo kreirati novu IPv4 sekundarnu zonu. Network ID zone će biti 10.10.45. Master DNS server će nam biti 10.10.45.1 (SERVERDC).

Kada smo dodali zonu, još moramo konfigurirati Zone Transfers. To ćemo konfigurirati u propertiesima kreirane zone na SERVER1.



Slika – SERVER1 Reverse Lookup Zones, 45.10.10.in-addr.arpa Properties, Zone Transfers

Kada postavimo Zone Transfers, napravimo reload zone i osvježimo cijeli DNS server. Provjerimo jesu li zapisi u reverznoj zoni.



Slika – SERVER1 Reverse Lookup Zones, 45.10.10.in-addr.arpa

* 1. Konfiguracija Storage Spaces-a na SERVER1

Sada ćemo konfigurirati Storage Spaces. Konkretno, RAID 5 polje od 4 dostupna diska, svaki od 10GB, od kojih će jedan biti Hot-Spare[[2]](#footnote-2).

Prvi korak koji moramo napraviti jest dodati diskove u Storage Pool. To ćemo učiniti kroz powershell.

$diskovi = (Get-PhysicalDisk -CanPool $true | Select-Object -First 3)

New-StoragePool -FriendlyName POOL1 -StorageSubSystemFriendlyName "Windows `

Storage\*" -PhysicalDisks $diskovi

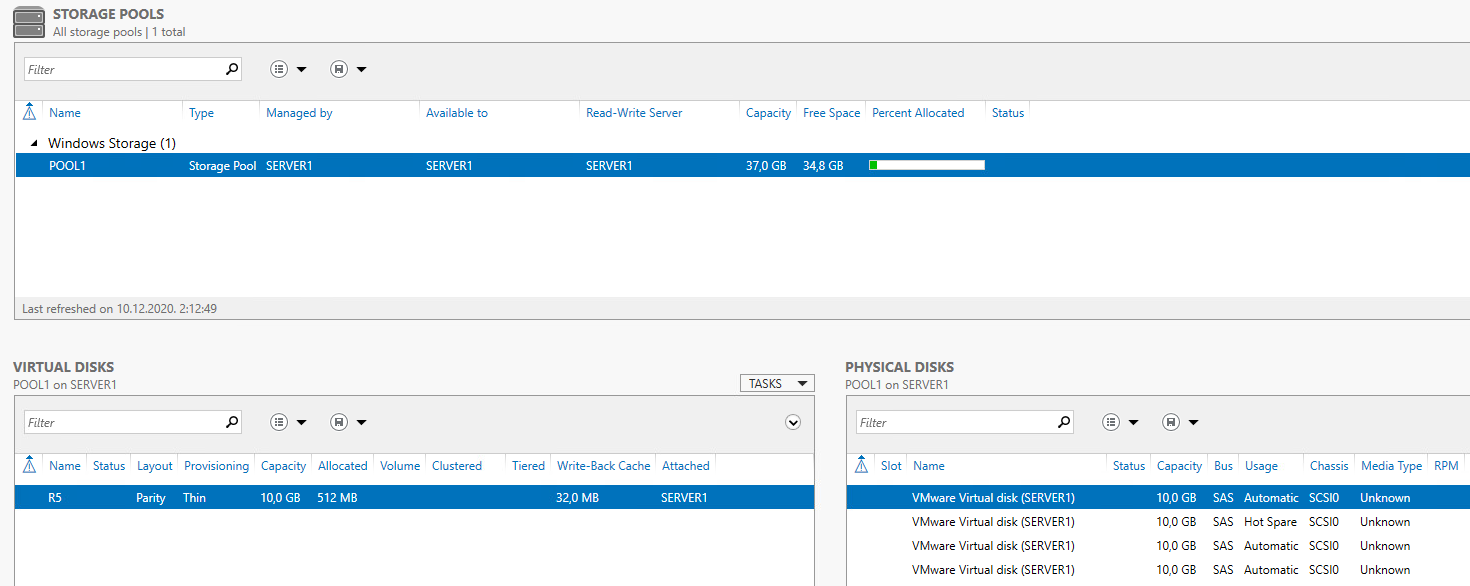
Add-PhysicalDisk -StoragePoolFriendlyName "POOL1" -PhysicalDisks `

(Get-PhysicalDisk -CanPool $true) -Usage HotSpare

Nakon što smo kreirali Storage Pool, napravit ćemo virtualni disk veličine 10GB prema zahtjevima navedenim u projektnom zadatku.

New-VirtualDisk -StoragePoolFriendlyName "POOL1" -FriendlyName "R5" -Size 10GB `

-ProvisioningType Thin -ResiliencySettingName Parity



Slika – SERVER1 Storage Pools nakon konfiguracije R5

Sada kada imamo virtualni disk, moramo ga inicijalizirati te mu dodjeliti slovo i formatirati ga.

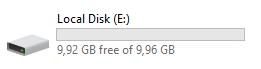
get-disk | ?{$\_.number -eq 5} | set-disk -Isoffline $false

get-disk | ?{$\_.number -eq 5} | set-disk -IsReadOnly $false

get-disk | ?{$\_.number -eq 5} | initialize-disk -PartitionStyle GPT

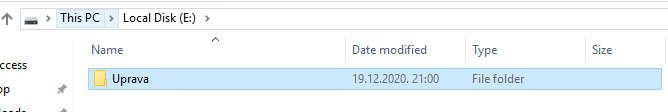
New-Partition -DiskNumber 5 -UseMaximumSize -DriveLetter E

Format-Volume -DriveLetter E -FileSystem NTFS



Slika – SERVER1 E: disk

Još ćemo napraviti na K: disku mapu Uprava koju ćemo podijeliti na mreži.



Slika – Direktorij E:\Uprava

* 1. Konfiguracija DAC-a (Dynamic Access Control-a) na SERVER1

Nakon storage spaces-a krećemo na konfiguraciju DAC-a (Dynamic access control) na poslužitelju SERVER1.

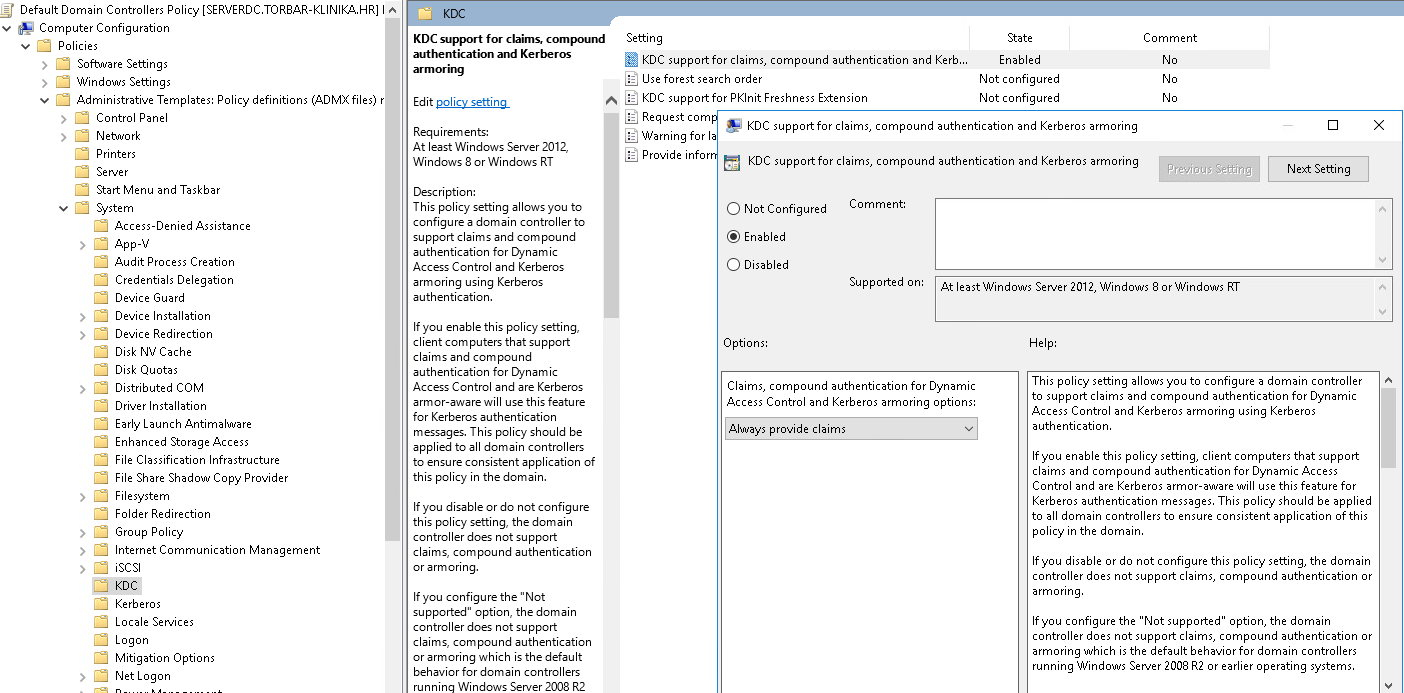
Na SERVER1 poslužitelju kroz Server Manager instaliramo File Server Resource Manager rolu.

Add Roles and Features 🡪 Server roles 🡪 File and Storage Services 🡪 File and iSCSI Services 🡪

File Server Resource Manager

Nakon instalacije role odlazimo u Group Policy Management i tamo ćemo konfigurirati KDC (Key Distribution Center) tako da on uvijek provide-a claim-ove.

Tools 🡪 Group Policy Management



Slika – Default Domain Controllers Policy

Nakon što smo konfigurirali GPO, na domenskim kontrolerima forsiramo ažuriranje group policy-a.

gpupdate /force

Sada idemo u Active Directory Administrative Center i tamo konfiguriramo DAC.

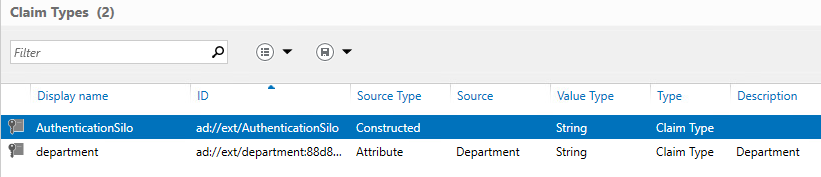
Tools 🡪 Active Directory Administrative Center 🡪 Dynamic Access Control

Prvo što trebamo napraviti je dodati u Department resource property odjele Uprava i Doktori te nakon toga omogućiti resource properties Confidentiality i Department.



Slika – DAC Enabled Resource Properties

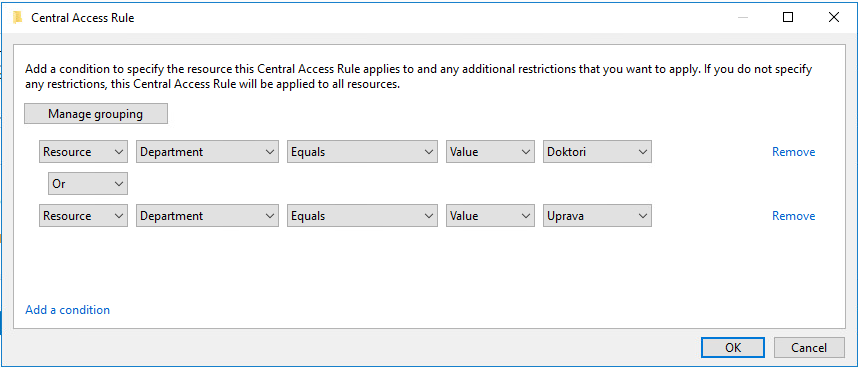
Nakon toga ćemo napraviti Claim type department koji će za izvor koristiti Department resource property.



Slika – DAC Claim Types

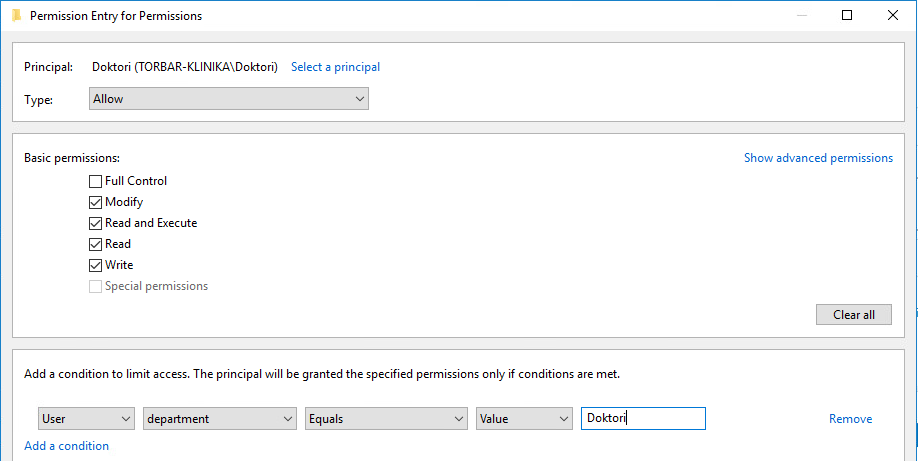
Sada ćemo kreirati dva Central Access pravila, jedno za pristup direktorijima određenim odjelima, a drugo za pristup povjerljivim datotekama.

Prvo ćemo kreirati Central Access Rule Odjeli. Postavit ćemo da resurs Department mora biti jednak Doktorima ili Upravi.

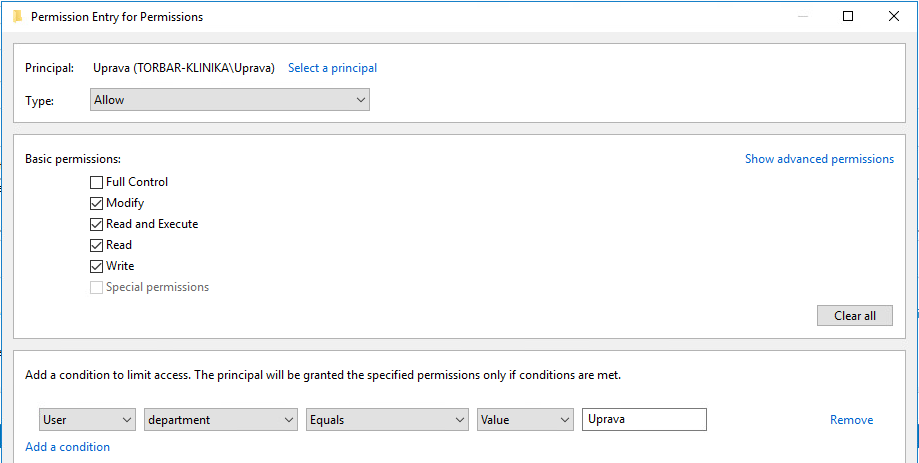


Slika – Odjeli conditions

Isto tako, moramo konfigurirati dozvole pristupa za dva navedena odjela.

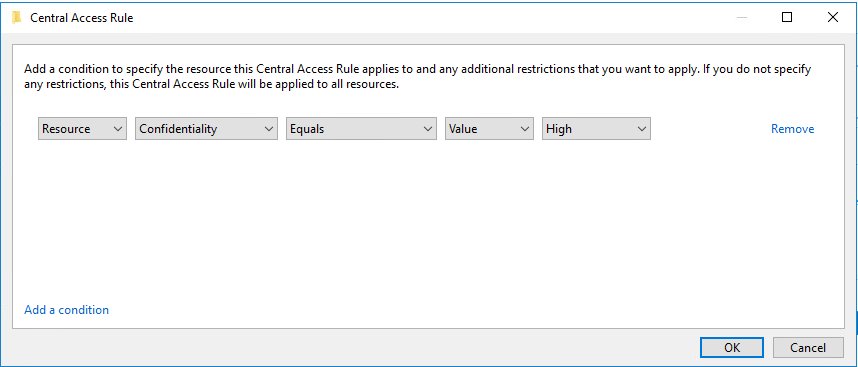


Slika – dozvole pristupa Doktori



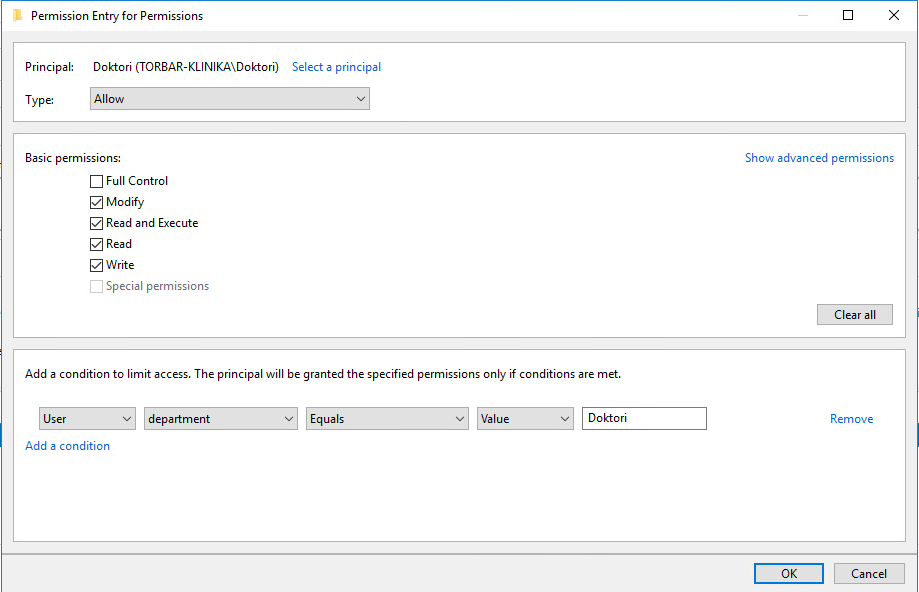
Slika – dozvole pristupa Uprava

Drugo ćemo kreirati Central Access Rule PovjerljivostDatoteka. Postavit ćemo da resurs Confidentiality mora biti jednak High.

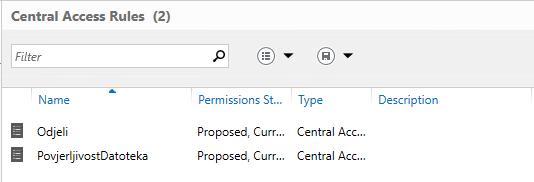


Slika – PovjerljivostDatoteka conditions

Isto kao i kod kreiranja prvog pravila, moramo konfigurirati dozvole pristupa povjerljivim datotekama za Doktore.

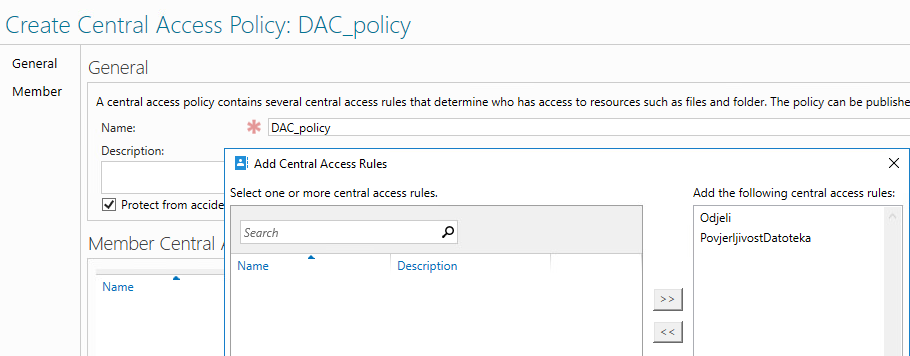


Slika – dozvole pristupa Doktori



Slika – DAC Central Access Rules

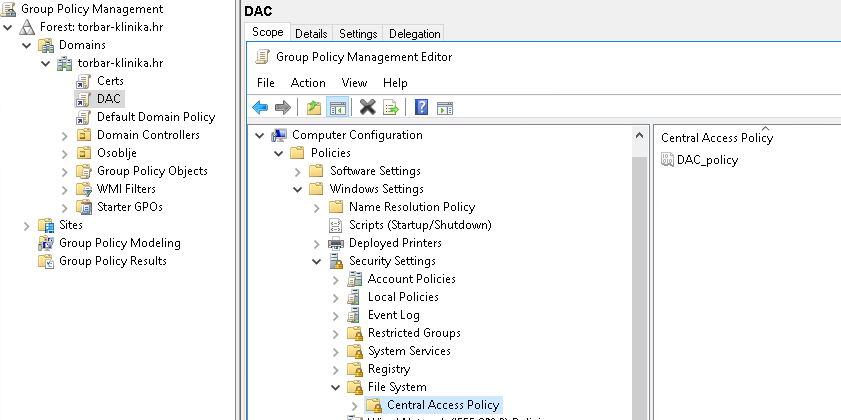
Nakon što smo definirali pravila Odjeli i PovjerljivostDatoteka, kreiramo politiku koja će sadržavati ta dva pravila.



Slika – kreiranje DAC\_policy centralne politike

Sada moramo primijeniti tu politiku u našoj domeni, to ćemo napraviti kroz Group Policy Management na poslužitelju SERVERDC gdje ćemo kreirati novi GPO naziva DAC.

Tools 🡪 Group Policy Management

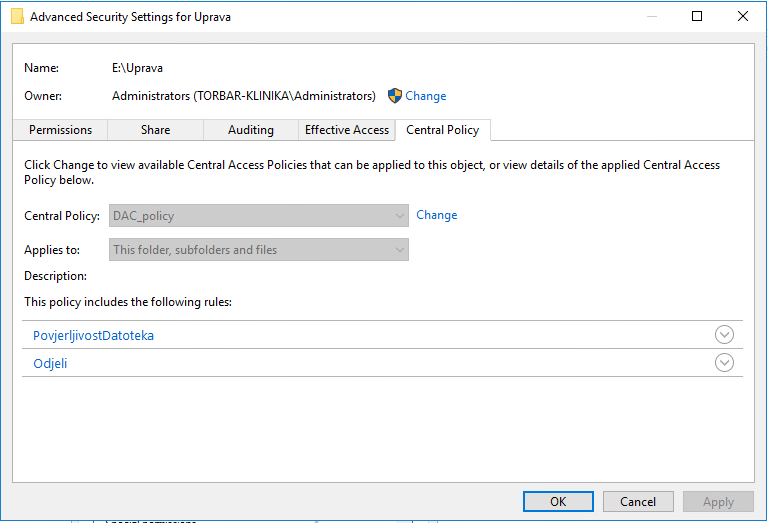


Slika – DAC GPO sa primijenjenom DAC\_policy centralnom politikom

Nakon što smo konfigurirali GPO, na svim računalima u domeni forsiramo ažuriranje group policy-a.

gpupdate /force

Nakon što se group policy ažurirao, postavit ćemo u sigurnosne postavke direktorija E:\Uprava kreiranu centralnu politiku.



Slika – Advanced Security Settings for Uprava, Central Policy

Sada ćemo na poslužitelju SERVER1 napraviti classification pravilo koje će primjenjivati razinu povjerljivosti podataka. To radimo u File Server Resource Manager-u.

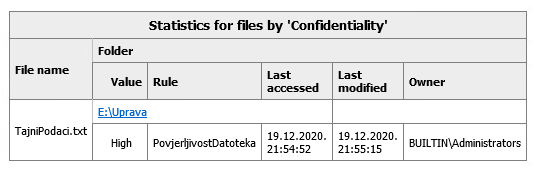
Tools 🡪 File Server Resource Manager

Classification pravilo zvat će se PovjerljivostDatoteka, radit će nad E:\Uprava direktorijem te će kao jako povjerljive datoteke smatrati one koje u sebi sadrže string „Tajno“.



Slika – File Server Resource Manager, Classification Rules

Kada smo kreirali pravilo, desnim klikom i odabirom *Run all classification rules now…* pokrenut ćemo kreirano pravilo.



Slika – Statistika pokrenutog classification pravila

* 1. Konfiguracija DFS (Distributed File System) replikacije na SERVER 2 i SERVER3

Kada smo uspješno konfigurirali DAC, krećemo na konfiguraciju DFS-a (Distributed File System) i njegove replikacije na poslužiteljima SERVER2 i SERVER3.

Na oba poslužitelja kroz Server Manager instaliramo DFS Namespaces i DFS Replication role.

Add Roles and Features 🡪 Server roles 🡪 File and Storage Services 🡪 File and iSCSI Services 🡪

DFS Namespaces + DFS Replication

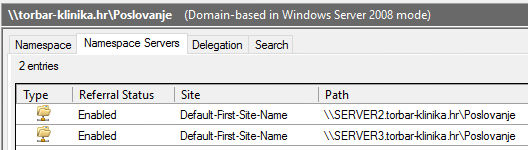
Nakon instalacije rola ponovno pokrenemo poslužitelje te kad se oni podignu napravimo direktorij C:\Dokumenti na oba poslužitelja.

Svu daljnju konfiguraciju radimo unutar DFS Managementa na navedenim poslužiteljima.

Sada ćemo kreirati namespace Poslovanje na poslužitelju SERVER2. To radimo pritiskom na gumb *New Namespace* na traci *Actions* s desne strane DFS management-a.

Kao server odabiremo SERVER2. Namespace ćemo nazvati Poslovanje, prava pristupa će glasiti tako da administratori imaju potpuni pristup, dok korisnici imaju RW prava. Tip namespace-a će biti Domain-based.

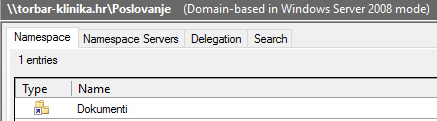
Kada smo kreirali namespace, u taj namespace dodajemo drugi namespace server (SERVER3) te na njega postavljamo ista prava pristupa kao i kod SERVER2.



Slika - \\torbar-klinika.hr\Poslovanje Namespace Servers

Sada kad smo dodali namespace servere, kreiramo novu mapu u namespace-u.

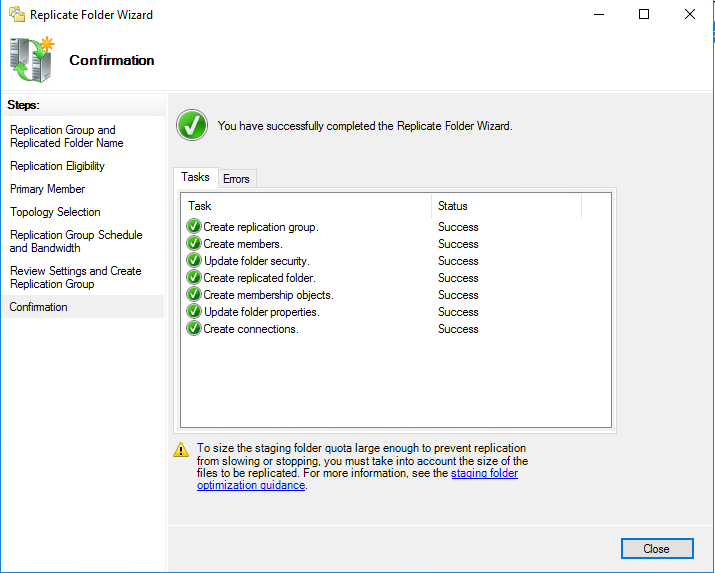
Nova mapa će se zvati Dokumenti, te će joj target biti kreirana lokalna mapa istog imena. Prava pristupa će biti identična onima na namespace-u.



Slika - \\SERVER2\Dokumenti

Sada ćemo dodati novi target, istoimenu mapu na poslužitelju SERVER3. Nakon što dodamo taj target, DFS nam odmah nudi mogućnost postavljanja replikacije. Napravit ćemo replikaciju (replikacijsku grupu).

Otvara nam se Replicate Folder Wizard. Ostavimo defaultni naziv replikacijske grupe, odabrati ćemo SERVER2 kao poslužitelja koji replicira sadržaj svoje datoteke na ostale, full mesh topologija, kontinuirana replikacija koja koristi 512Kbps.



Slika – uspješna konfiguracija DFS replikacijske grupe

* 1. Konfiguracija CA (Certification Authority) na SERVER3

Sada ćemo konfigurirati Certification Authority poslužitelja za našu domenu.

Kroz Server Manager instaliramo AD CS (Active Directory Certificate Services) rolu.

Add Roles and Features 🡪 Server roles 🡪 AD CS

U kartici role services odabiremo Certification Authority, Certificate Enrollment Web Service, Certification Authority Web Enrollment i Online Responder.

Na kraju instalacije moramo dodatno konfigurirati Active Directory Certificate Services na poslužitelju.

Za credentials-e ćemo koristiti domenskog administratora.

Role servise koje ćemo sada konfigurirati su Certification Authority, Certification Authority Web Enrollment i Online Responder. Setup type će biti Enterprise CA. Tip CA će biti Root. Kreiramo novi privatni ključ.

Kriptografski provider će nam biti RSA#Microsfot Software Key Storage Provider, duljina ključa 2048 te hash algoritam SHA256.

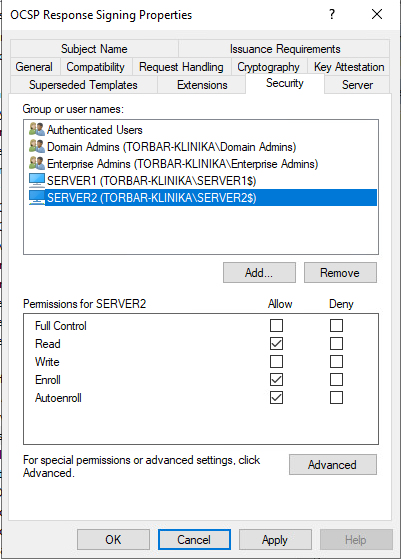
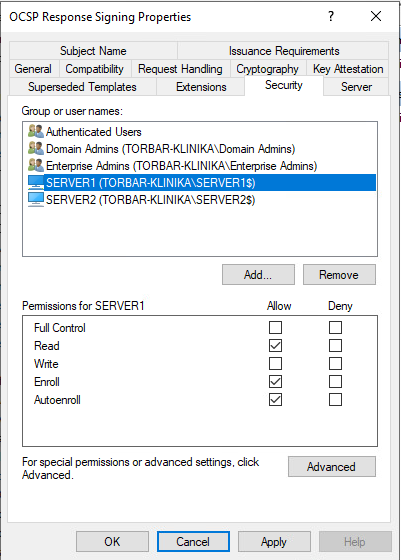
Common name CA će biti torbar-klinika-SERVER3-CA.

Validity period će biti 5 godina.

Nakon što smo uspješno podigli CA, trebamo konfigurirati online responder te kreirati certifikat za IIS koji ćemo kasnije konfigurirati. Otvaramo Certification Authority management konzolu.

Unutar torbar-klinika-SERVER3-CA nalazi se 5 mapa. Nama će sada trebati Certificate Templates kako bi iz template-a izradili svoje certifikate za obavještavanje klijenata o opozvanim certifikatima i certifikat za IIS. Na Certificate Templates pritisnemo desnim klikom miša, Manage.

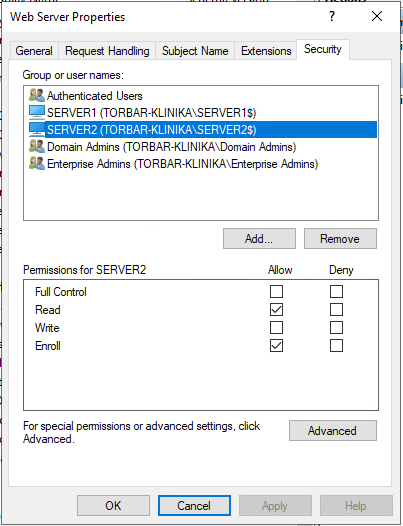
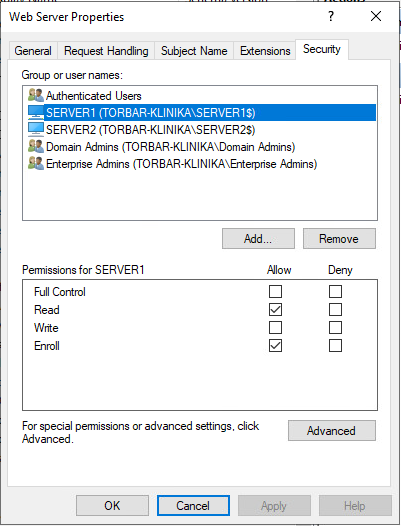
Otvara nam se Certificate Templates konzola. Potražimo template certifikata koji se zove OCSP Response Signing i desnim klikom miša odemo na Properties. Kada otvorimo Properties, idemo na karticu security te dodajemo računala koja će nam biti IIS (web poslužitelji). Njima ćemo dati dozvole pristupa za Enroll i Autoenroll.



Slika – OCSP Response Signing Properties, Security, SERVER1 & SERVER2 permissions

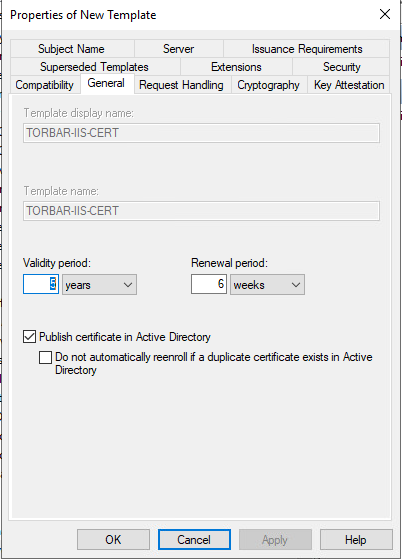
Nakon što smo podesili template, primjenimo promjene i izlazimo iz Certificate Templates konzole. Sada desnim klikom miša na Certificate Templates pritiskom na gumb New izdajemo novi certifikat. Potražimo OCSP Response Signing i kliknemo na gumb OK.

Sada ćemo još kreirati certifikat za naše web poslužitelje. Ponovno ulazimo u Certificate Templates konzolu, ulazimo u Web Server Properties, kartica Security. Dodajemo SERVER1 i SERVER2 te im dajemo dozvolu za Enroll.



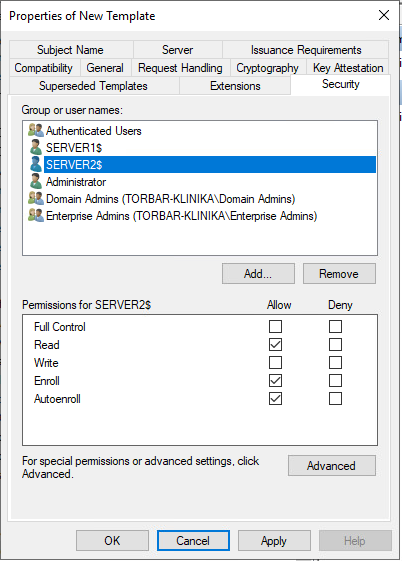
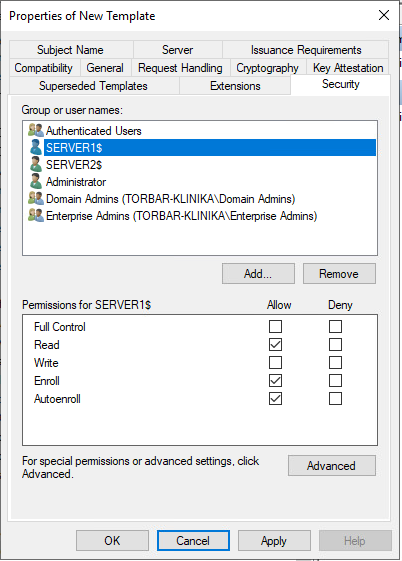
Slika – Web Server Properties, Security, SERVER1 & SERVER2 permissions

Primjenimo promjene i vraćamo se u Certificate Templates konzolu. Dupliciramo certifikat Web Server, otvara se prozor Properties of New Template. Odlazimo na karticu General i dajemo naziv novom template-u, TORBAR-IIS-CERT. Odaberemo opciju objavljivanja certifikata u AD. Primjenimo promjene i prelazimo na karticu Security.



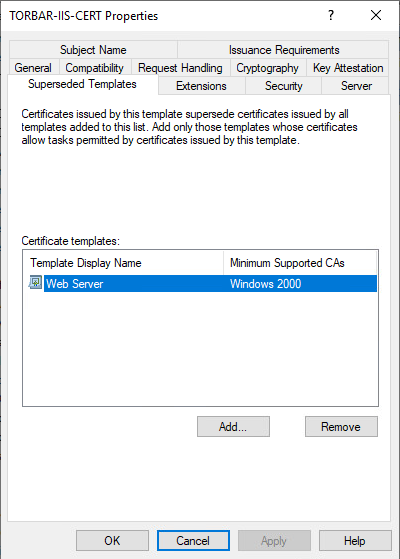
Slika – Properties of New Template, General

Na kartici Security poslužiteljima SERVER1 i SERVER2 dajemo dozvolu za Autoenroll. Primjenimo promjene i idemo na karticu Superseded Templates.



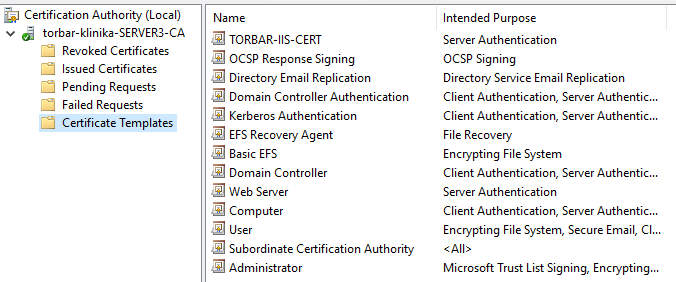
Slika – Properties of New Template, Security, SERVER1 & SERVER2 permissions

Na kartici Superseded Templates pritisnemo na gumb *Add* i odaberemo Web Server. Primjenimo promjene i izlazimo iz Certificate Templates koznole.



Slika – TORBAR-IIS-CERT Properties, Superseded Templates

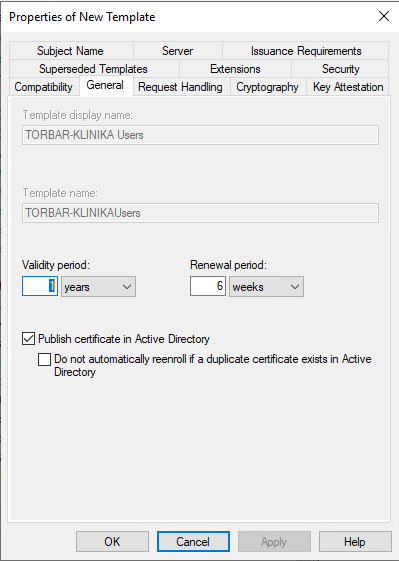
Sada desnim klikom miša na Certificate Templates pritiskom na gumb New izdajemo novi certifikat. Potražimo TORBAR-IIS-CERT i kliknemo na gumb OK.



Slika – CA Issued Certificates nakon kompletne konfiguracije CA

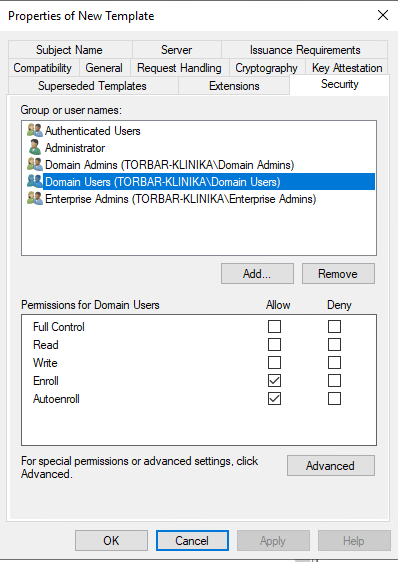
Sada još moramo konfigurirati automatsko izdavanje certifikata (autoenroll). Vraćamo se u Certificate Templates konzolu. Dupliciramo User template.

Na kartici General kao ime template-a stavimo TORBAR-KLINIKA Users.



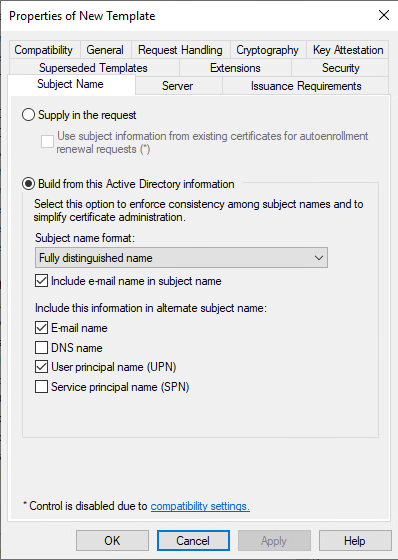
Slika – Properties of New Template, General

Na kartici Security dodamo Domain Users grupu i damo im dozvole za enroll i autoenroll.



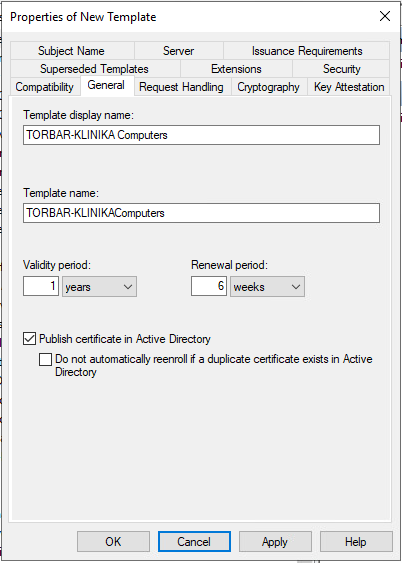
Slika – Properties of New Template, Security

I na kartici Subject Name isključujemo opcije E-mail name i User Prinicipal Name.



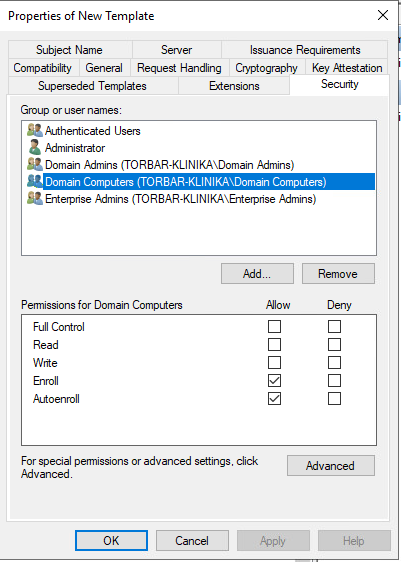
Slika – Properties of New Template, Subject Name

Primjenimo promjene i pritisnemo OK. Sada ćemo isti postupak ponoviti za računala.



Slika – Properties of New Template, General

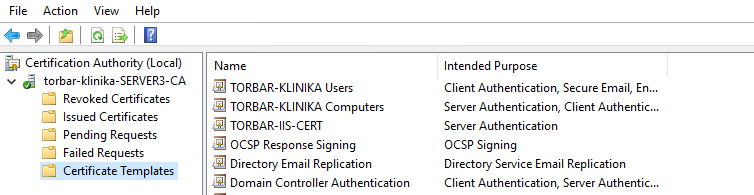
Na kartici Security dodamo Domain Computers grupu i damo im dozvole za enroll i autoenroll.



Slika – Properties of New Template, Security

Primjenimo promjene i pritisnemo OK. Izlazimo iz Certificate Templates konzole.

Sada izdamo oba prethodno napravljena certifikata.



Slika – torbar-klinika-SERVER3-CA issued certificates

Još nam samo preostaje konfigurirati group policy kako bi autoenroll radio kako treba.

Prelazimo na poslužitelj SERVERDC i otvaramo Group Policy Management.

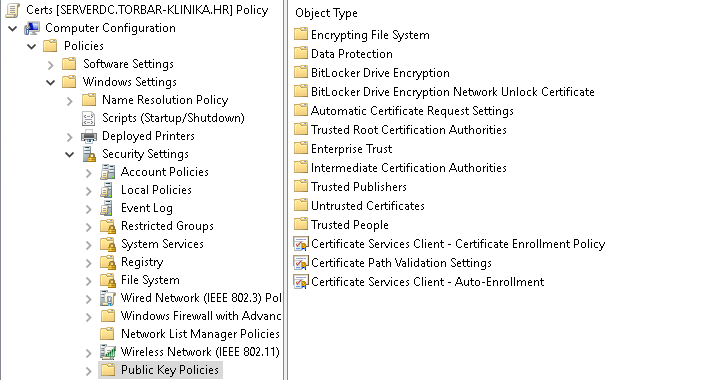
Forest: torbar-klinika.hr 🡪 Domains 🡪 torbar-klinika.hr

Unutar domene torbar-klinika.hr kreiramo novi GPO imena Certs. Sada ćemo desnim klikom na Certs editirati GPO. Otvara nam se Group Policy Management Editor. Idemo na sljedeću putanju:

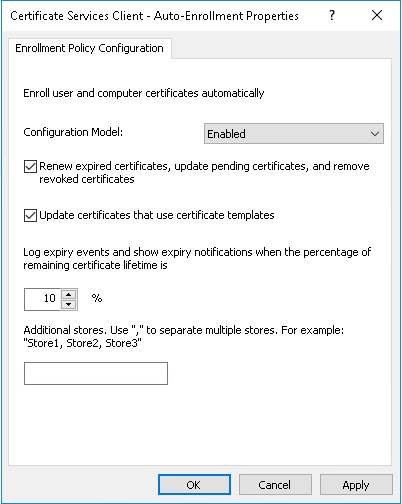
Computer Configuration-> Policies-> Windows Settings-> Security Settings-> Public Key Policies

Unutar Public Key Policies nalazi se stavka Certificate Services Client – Auto-Enrollment, nju ćemo konfigurirati.

Kada završimo s konfiguracijom Group Policy-a, izvršimo naredbu gpupdate /force na svim poslužiteljima i klijentskom računalu.



Slika – Certs 🡪 Public Key Policies



Slika – Certificate Services Client – Auto-Enrollment nakon konfiguracije

Sada ćemo testirati konfiguraciju putem korisnika certtest s klijentskog računala client1.

* 1. Konfiguracija IIS-a (Internet Information Services-a) na SERVER1 i SERVER2

Nakon što smo konfigurirali CA, konfigurirat ćemo web servere (IIS-ove) SERVER1 i SERVER2.

Kroz Server Manager instaliramo Web Server (IIS) rolu.

Add Roles and Features 🡪 Server roles 🡪 Web Server (IIS)

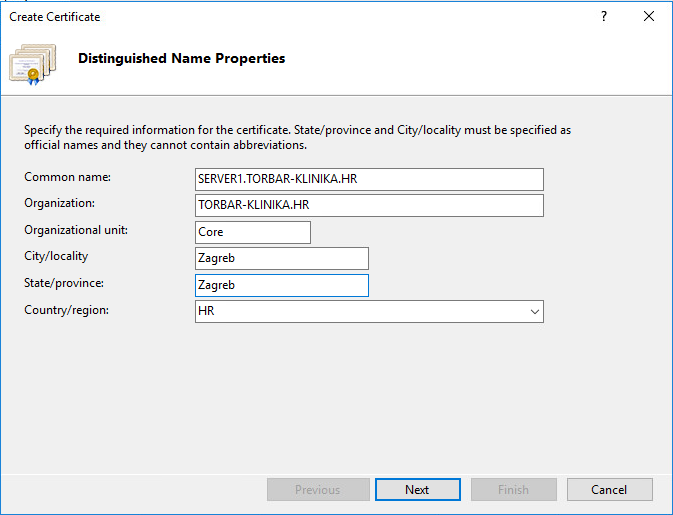
U kartici role services odabiremo Client Certificate Mapping Authentication i IIS Client Certificate Mapping Authentication.

Sljedeću konfiguraciju radimo na oba poslužitelja usporedno.

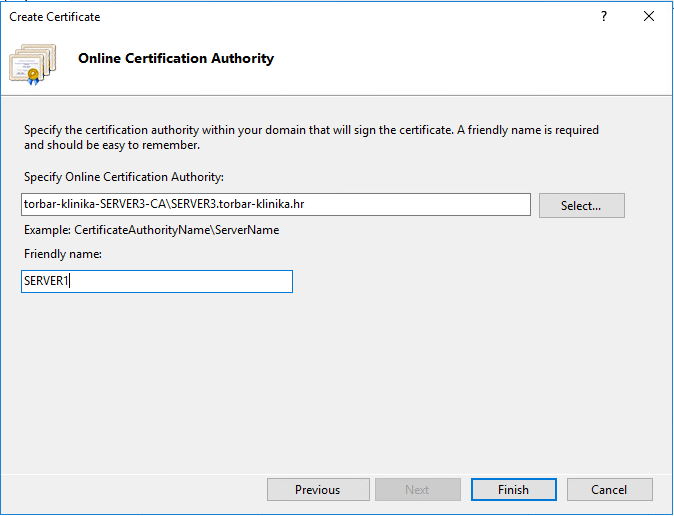
Kroz Server Manager ulazimo u Internet Information Services (IIS) Manager.

Prvo ćemo napraviti domenske certifikate za web poslužitelje.

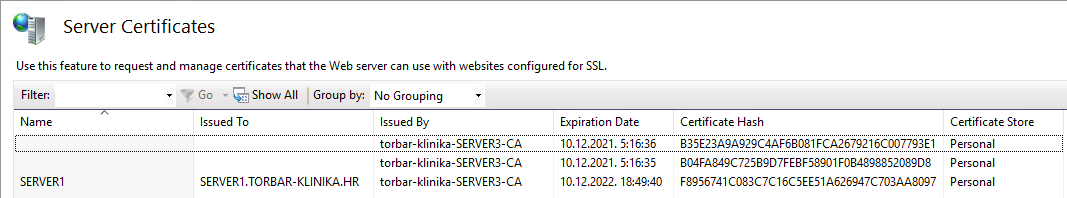
SERVER1 🡪 Server Certificates 🡪 Create Domain Certificate



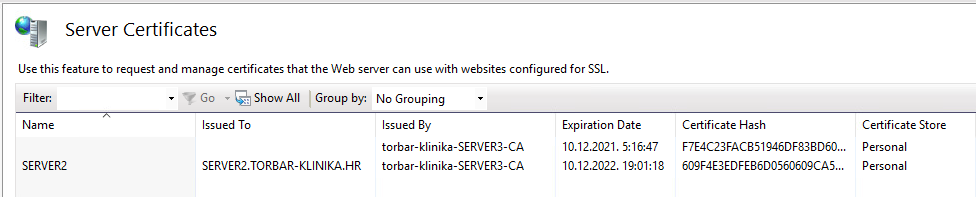
Slika – Create Certificate, Certificate Information



Slika – Create Certificate, Certification Authority

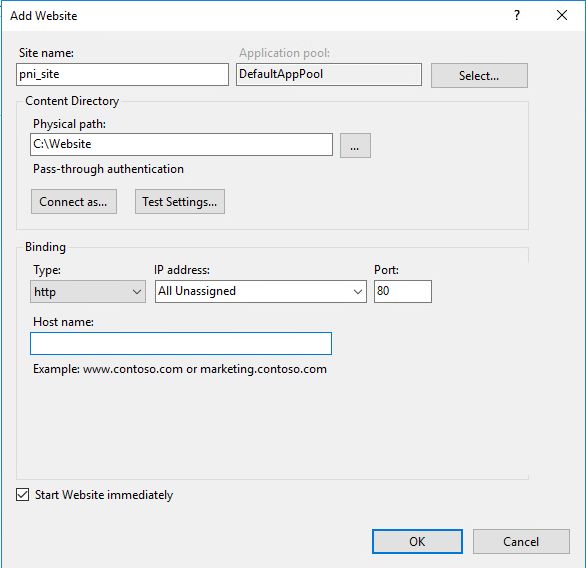


Slika – SERVER1 IIS, Server Certificates



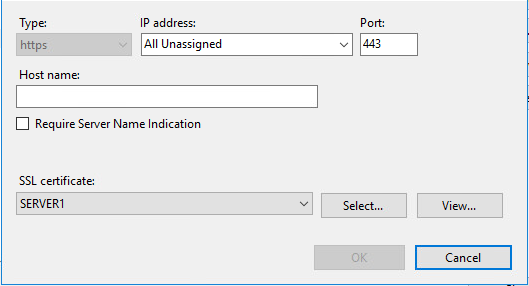
Slika – SERVER2 IIS, Server Certificates

Sada odlazimo u mapu Sites koju možemo vidjeti unutar okna s lijeve strane. Tamo ćemo napraviti novi website pni\_site koji koristi fizičku putanju C:\Website za direktorij iz kojeg pruža sadržaj.



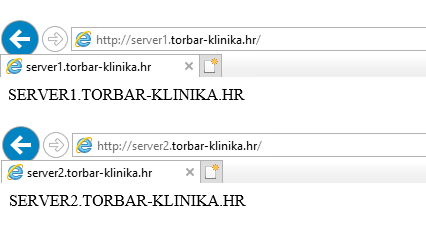
Slika – Add Website pni\_site

Sada ćemo još dodati https binding na pni\_site. To radimo desnim klikom na pni\_site, *Edit Bindings…* Pritisnemo na gumb *add* i dodamo https binding koji će raditi s certifikatom koji smo prethodno kreirali.



Slika – SERVER1 Add Site Binding

Testirajmo pristup web stranicama sa poslužitelja SERVER3.



Slika – SERVER3 test funkcionalnosti IIS-a

* 1. Konfiguracija NLB (Network Load Balancing) clustera na SERVER1 i SERVER2

Nakon što smo konfigurirali web poslužitelje, konfigurirat ćemo NLB na SERVERDC poslužitelju koji će preusmjeravati zahtjeve za pristup *www.jtorbar-klinika.hr* na poslužitelje server1 i server2.

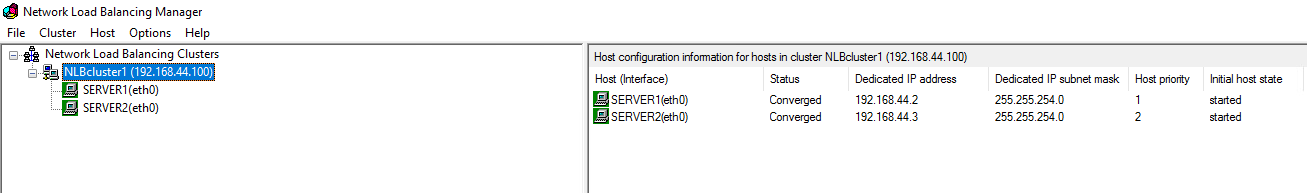
Kroz Server Manager instaliramo NLB feature na sve navedene poslužitelje.

Add Roles and Features 🡪 Features 🡪 NLB

Nakon instalacije kroz server manager ulazimo u NLB Manager na SERVERDC poslužitelju.

SERVERDC 🡪 Tools 🡪 Network Load Balancing Manager

Kada uđemo u NLB Manager, dodat ćemo novi cluster koji će koristiti eth0 adaptere poslužitelja SERVER1 i SERVER2 za balansiranje prometa prema web stranicama na tim poslužiteljima. IP adresa clustera bit će 192.168.44.100/24. Operativni mode clustera je multicast. Port pravila će biti definirana tako da rade na portovima 80 i 443.



Slika – SERVER2 NLB Manager

Sada ćemo još dodati na poslužitelju SERVERDC u DNS-u napraviti host zapis naziva www koji pokazuje na IP adresu 192.168.44.100.



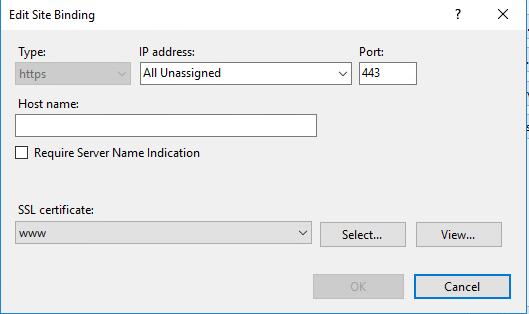
Slika – www host record na SERVERDC poslužitelju

Kada smo uspješno konfigurirali NLB cluster i dodali host zapis u DNS, napravit ćemo domenski certifikat za svakog od web poslužitelja kako bi on ispravno radio na FQDN-u www.torbar-klinika.hr.



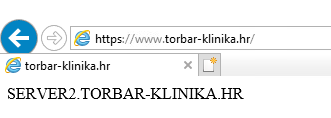
Slika – novo kreirani www.torbar-klinika.hr domenski certifikat

Nakon što smo kreirali certifikat još ga trebamo dodati u website binding za https.



Slika – Edit Site Binding

Testirajmo funkcionalnost NLB clustera sa poslužitelja SERVER3 i računala client1.



Slika – www.torbar-klinika.hr – test pristupa stranici sa poslužitelja SERVER3



Slika - www.torbar-klinika.hr – test pristupa stranici sa računala client1

* 1. Konfiguracija DHCP (Dynamic Host Configuration Protocol) failover clustera na SERVER 2 i SERVER3

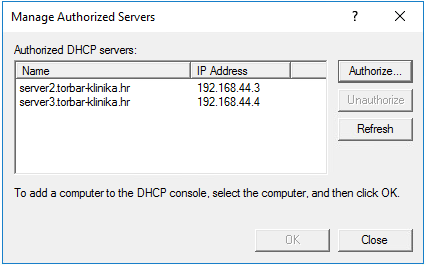
Nakon što smo konfigurirali NLB, konfigurirat ćemo DHCP cluster na poslužiteljima SERVER2 i SERVER3.

Kroz Server Manager instaliramo DHCP Server rolu na oba poslužitelja.

Add Roles and Features 🡪 Server roles 🡪 DHCP Server

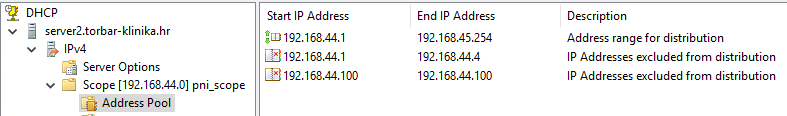
Na kraju instalacije moramo dodatno konfigurirati DHCP Server. DHCP Server u AD DS autoriziramo putem računa domenskog administratora.

Desnim klikom miša na DHCP i pritiskom na gumb *Manage Authorized Servers*… možemo vidjeti autorizirane DHCP servere u domeni.

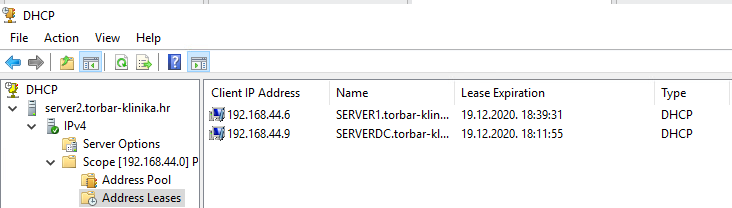


Slika – DHCP Manage Authorized Servers

Konfigurati ćemo novi IPv4 raspon od 192.168.44.1 do 192.168.45.254. Lease duration ćemo postaviti na 1 dan. Kao DNS servere navest ćemo SERVERDC i SERVER1, u tom redoslijedu. Izostavit ćemo adrese od 192.168.44.1 do 192.168.44.4 i adresu 192.168.44.100 pošto su te adrese već dodijeljene našim poslužiteljima.



Slika – DHCP Server SERVER3, Address Pool



Slika – DHCP Server SERVER3, Address Leases

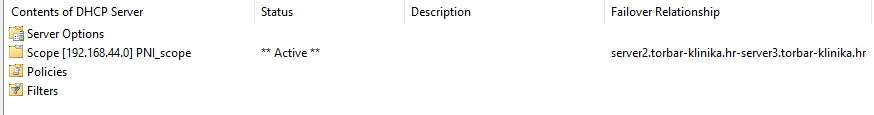
Kao što možemo vidjeti iz slike, DHCP server je ispravno konfiguriran i funkcionalan. Sada ćemo prijeći na konfiguraciju failover-a.

Failover konfiguriramo tako da desnim klikom miša na IPv4 pritisnemo na *Configure Failover…*

Failover konfiguriramo za scope 192.168.44.0/24, kao partner server specificiramo poslužitelja SERVER3, failover mode će biti *Load balance* te će omjer biti 80%(SERVER2):20%(SERVER3). Dijeljeni secret će glasiti „Pa$$w0rd“.

Sada možemo vidjeti kako je scope 192.168.44.0/24 u Failover odnosu:

server2.torbar-klinika.hr-server3.torbar-klinika.hr



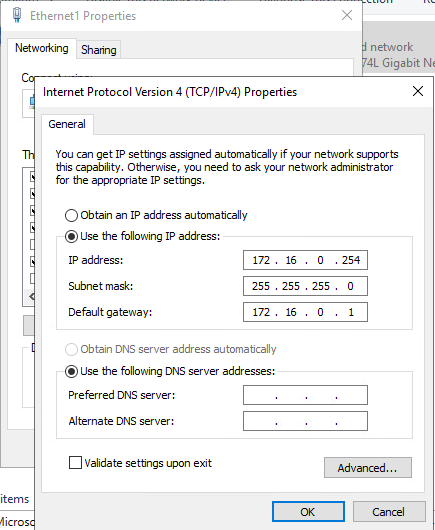
Slika – Failover Relationship za scope 192.168.44.0/24

Ovime smo uspješno konfigurirali DHCP failover cluster između poslužitelja SERVER2 i SERVER3.

* 1. Instalacija Docker kontejnera na SERVER3

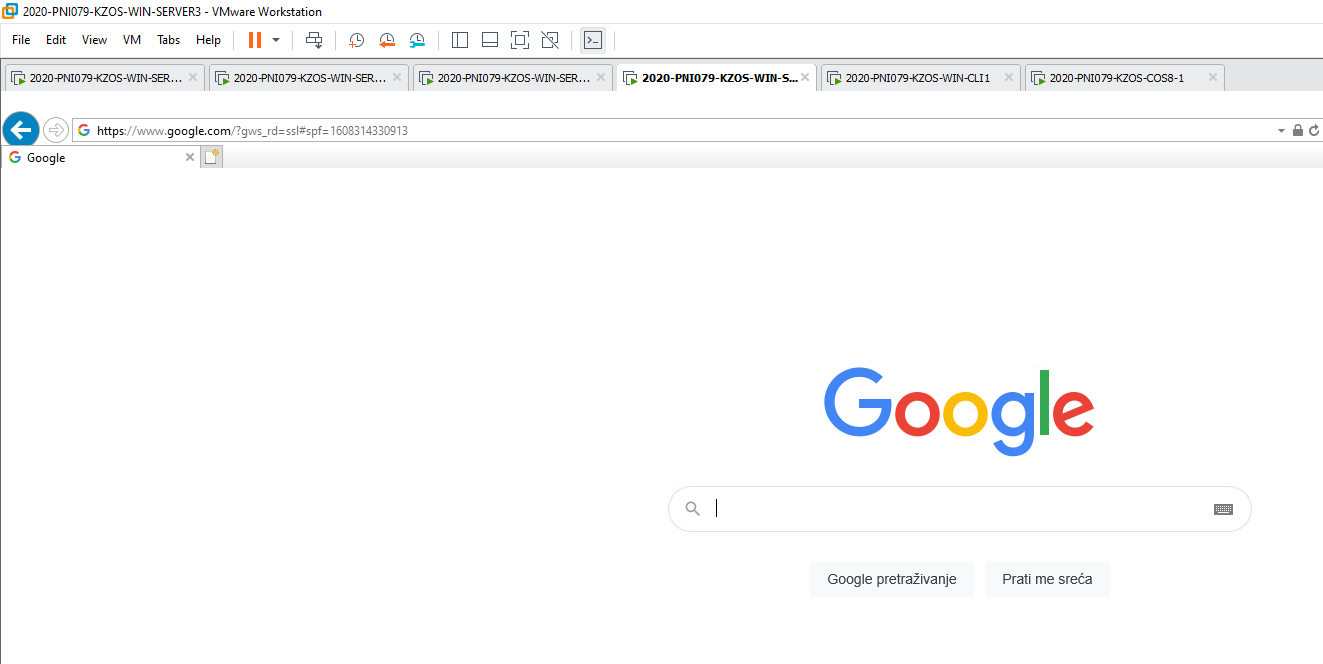
Prije nego što krenemo u konfiguraciju docker engine-a na poslužitelju SERVER3, moramo mu omogućiti pristup internetu preko COS1 poslužitelja.

Prvo ćemo na mrežni adapter eth1 na poslužitelju SERVER3 kao defaultni GW postaviti IP adresu ens224 mrežnog adaptera na poslužitelju COS1.



Slika – postavke eth1 mrežnog adaptera na poslužitelju SERVER1

Nakon toga moramo omogućiti masquerade na svim mrežnim adapterima na računalu COS1. Kako bi provjerili konfiguraciju testiramo pristup www.google.com stranici s poslužitelja SERVER3.



Slika – pristup www.google.com sa poslužitelja SERVER3

Sada ćemo instalirati nginx na poslužitelju COS1 te ga potom konfigurirati kao reverse proxy za naš NLB cluster.

yum -y install nginx

systemctl enable nginx

systemctl start nginx

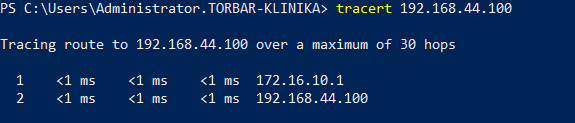
vim /etc/nginx/nginx.conf



Slika – /etc/nginx/nginx.conf

systemctl restart nginx

Provjerit ćemo radi li reverse proxy tako da na poslužitelju SERVER3 privremeno onemogućimo mrežni adapter eth0 te napravimo tracert prema NLB-u.



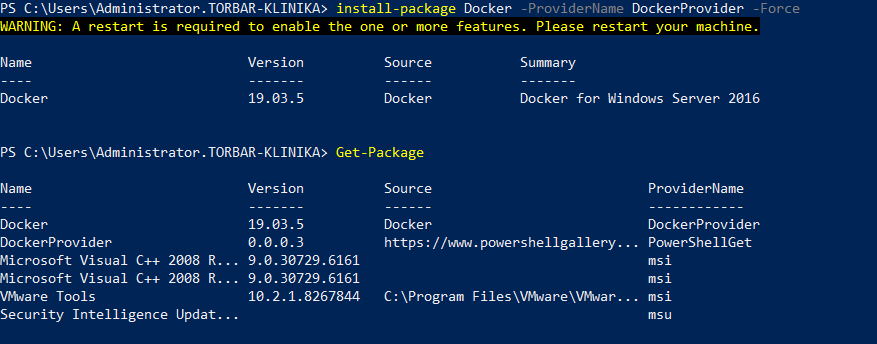
Slika – test reverse proxy-a

Nakon što smo konfigurirali reverse proxy, vratit ćemo se na SERVER3 i podići Docker engine.

Kroz powershell instaliramo *DockerProvider* module te nakon njega paket Docker.

install-module DockerProvider -Force

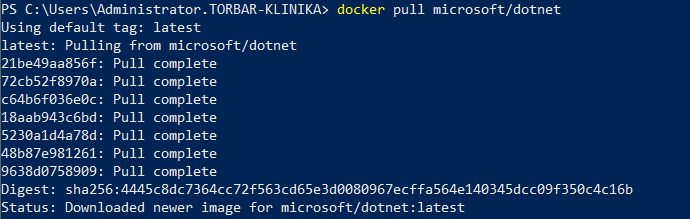
install-package Docker -ProviderName DockerProvider -Force



Slika – instalirani paketi na poslužitelju SERVER3

Kada se poslužitelj ponovno pokrene, skinut ćemo IIS kontejner image iz default docker microsoft repozitorija.

docker pull microsoft/dotnet



Slika – skinut dotnet:latest image



Slika – lista image-a

Ovime smo uspješno skinuli container image iz docker repozitorija. Onemogućit ćemo Internet pristup poslužitelju SERVER3 (onemogućit ćemo eth1 mrežni adapter).

* 1. Nadogradnja SERVER3 na Windows Server 2019

Za kraj ćemo napraviti nadogradnju operacijskog sustava poslužitelja SERVER3 sa WS2016 na WS2019. Kako bi svi servisi koji su trenutno aktivni bili aktivni i funkcionalni nakon nadogradnje, morat ćemo ih sigurno pohraniti prije nadogradnje. Servisi koje ćemo sigurno pohraniti su CA i DHCP.

Za sigurnosnu pohranu navedenih servisa kreirat ćemo dva direktorija na C:\ disku imena CA\_Backup i DHCP\_Backup.

Prvo ćemo krenuti sa sigurnosnom pohranom CA.

Tools 🡪 Certification Authority

Desnim klikom na torbar-klinika-SERVER3-CA odabiremo *All Tasks…* i od ponuđenih opcija kliknemo na *Backup CA…*

Sigurnosno ćemo pohraniti privatni ključ i CA certifikat zajedno s bazom podataka i njezinim log zapisima. Lokacija na koju ćemo to pospremiti je C:\CA\_Backup. Lozinka kojom ćemo zaštiti privatni ključ i CA certifikat će biti „Pa$$w0rd1234“.

Sada ćemo to napraviti i za DHCP.

Tools 🡪 DHCP

Desnim klikom na server3.torbar-klinika.hr odabiremo *Backup…* Lokacija na koju ćemo to pospremiti je C:\DHCP\_Backup.

Nakon što smo napravili sigurnosnu pohranu za servise, krećemo u deinstalaciju rola. To radimo kroz Server Manager.

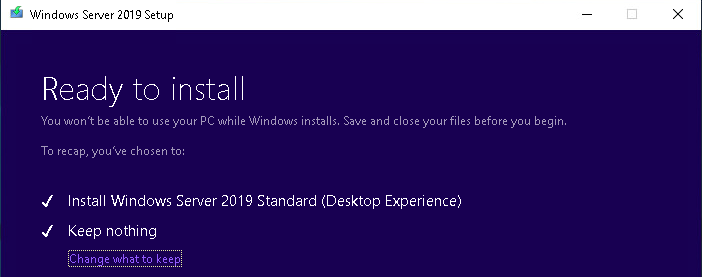
Manage 🡪 Remove Roles and Features

Prvo ćemo deinstalirati neke role unutar AD CS-a. Konkretno, Certificate Enrollment Web Service, Certification Authority Web Enrollment i Online Responder. Ostale korake u wizard-u ne radimo ništa (next, next i finish).

Nakon što smo uklonili te role ponovno ćemo pokrenuti Remove Roles and Features wizard te ukloniti AD CS, DHCP Server, DFS Namespaces i DFS Replication. Ostale korake u wizard-u ne radimo ništa (next, next i finish).

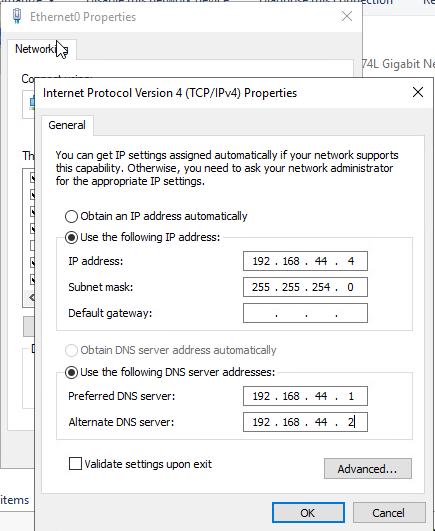
Kada smo uspješno uklonili i te role, ponovno pokrećemo poslužitelj. Nakon što se poslužitelj pokrenuo, krećemo s setup-om za nadogradnju.

U setup-u nećemo koristiti ažuriranja, upisujemo ključ za WS2019, instalirat ćemo WS2019 Standard (Desktop Expirience) te nećemo zadržavati datoteke. Nakon pritiska gumba *Install* kreće proces nadogradnje i on traje cca 20-30 minuta. Nakon što instalacija završi ponovno postavimo lozinku lokalnog administratora na „Pa$$w0rd“



Slika – informacije o nadogradnji

Kada završi nadogradnja, ponovno moramo postaviti pravilne postavke na mrežni adapter eth0.



Slika – eth0 properties, IPv4

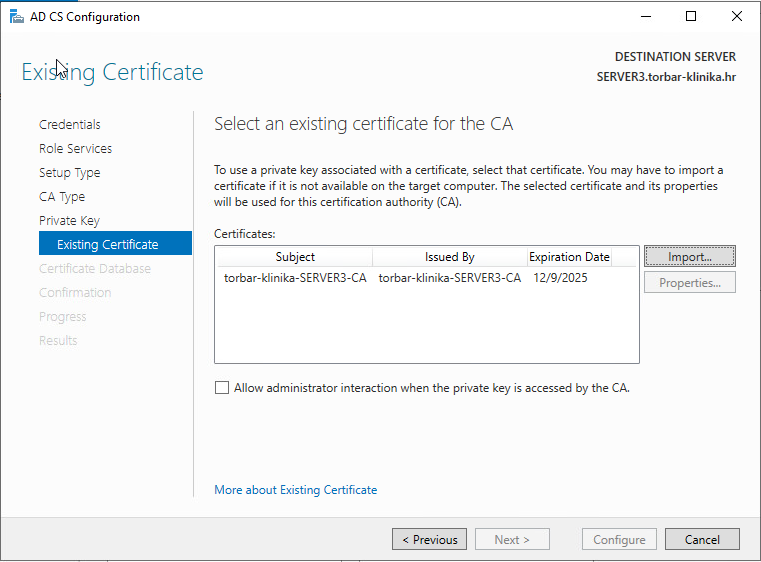
Nakon što smo ispravno konfigurirali mrežni adapter, mijenjamo ime poslužitelja nazad u SERVER3 te ga ponovno pokrenemo. Kada se on ponovno pokrene dodat ćemo ga u domenu torbar-klinika.hr. Ta radnja će također zahtijevati restart poslužitelja. Nakon što se on ponovno pokrene ulogirat ćemo se kao domenski administrator kako bi instalirali role koje smo sigurnosno pohranili. DFS ćemo morati ručno ponovno konfigurirati sa poslužitelja SERVER2.

Prva rola koju ćemo instalirati bit će AD CS. Od Role Services-a odabrat ćemo Certificate Enrollment Web Service, Certification Authority Web Enrollment i Online Responder.

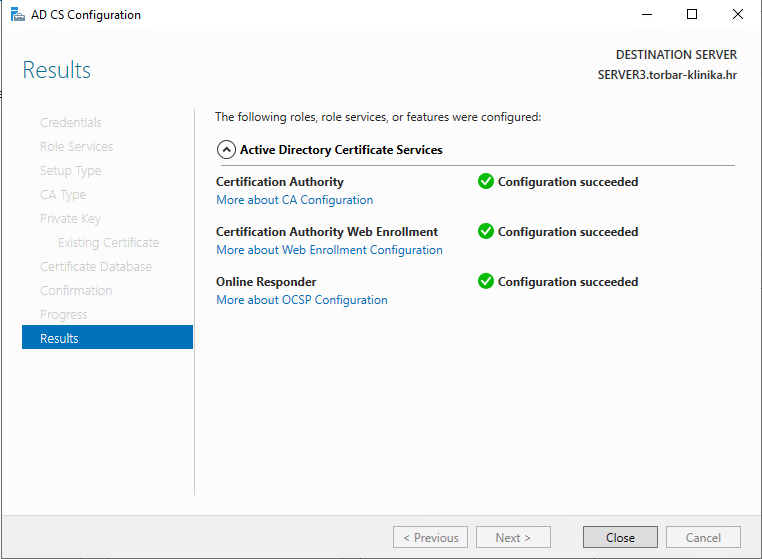
Manage 🡪 Add Roles and Features 🡪 AD CS

Kada se završi instalacija role, moramo dodatno ju konfigurirati. Kliknemo na *Configure Active Directory Certificate Services on the destination server*.

Otvara se novi wizard za konfiguraciju Role Servisa. Koristimo credentials-e domenskog administratora, konfiguriramo sve role servise koje smo instalirali (jedan nećemo moći dok ne instaliramo CA), CA će biti enterprise tipa te će poslužitelj biti root CA za našu domenu. U sljedećem koraku „Private key“ odabiremo certifikat s privatnim ključem koji smo sigurnosno pohranili na C:\ disku.



Slika – AD CS Configuration, Import Existing Certificate



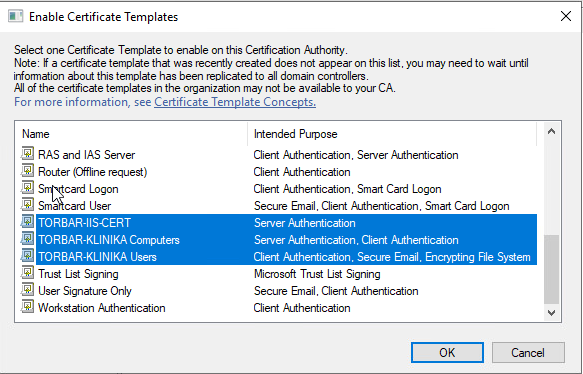
Slika – AD CS Configuration, Results

Nakon što smo to napravili, potrebno je konfigurirati još jedan role servis koji nismo mogli instalirati prije nego što je podignut CA, a to je Certificate Enrollment Web Service.

Kada završi konfiguracija, odlazimo u Certification Authority kako bi ponovno izdali certifikate koje smo kreirali u poglavlju 4.9.

Tools 🡪 Certification Authority

Pod torbar-klinika-SERVER3-CA desnim klikom na Certificate Templates kliknemo na *New Certificate Template to Issue* te ponovno izdamo prethodno navedene certifikate*.*



Slika 73 – Enable Certificate Templates

Ovime smo uspješno podigli CA rolu nakon nadogradnje. Prelazimo na DHCP.

Manage 🡪 Add Roles and Features 🡪 DHCP Server

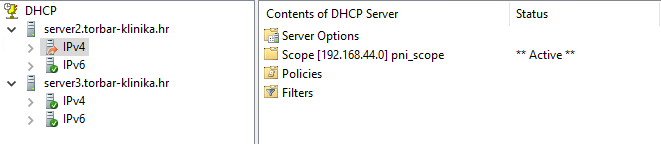
Na kraju instalacije moramo dodatno konfigurirati DHCP Server. DHCP Server u AD DS autoriziramo putem računa domenskog administratora.

Nakon instalacije odlazimo u DHCP.

Tools 🡪 DHCP

Desnim klikom miša na server3.torbar-klinika.hr odabiremo opciju *Restore…* te odabiremo direktorij C:\DHCP\_Backup u koji smo sigurno pohranili konfiguraciju našeg DHCP poslužitelja.

Sada ćemo otići na poslužitelj SERVER2 kako bi provjerili radi li DHCP kako treba.



Slika 74 – DHCP na poslužitelju SERVER2

Sa slike možemo vidjeti kako su svi IPv4 i IPv6 rasponi u redu te da je na IPv4 konfiguriran failover.

Još je ostao DFS za konfiguraciju. Pošto nam je sve konfigurirano na poslužitelju SERVER2, na poslužitelju SERVER3 ćemo samo prije instalacije role provjeriti je li još uvijek postoji direktorij C:\Dokumenti. Nakon što smo se uvjerili da postoji, instaliramo DFS Namespaces i DFS Replication role.

Add Roles and Features 🡪 DFS Namespaces, DFS Replication

Kada instalacija završi, idemo u DFS Management.

Tools 🡪 DFS Management

Na početnoj stranici DFS Management-a pritisnemo na *Add namespaces to Display…* i dodamo namespace [\\torbar-klinika.hr\Poslovanje](file:///\\torbar-klinika.hr\Poslovanje).

Nakon dodavanja namespace-a, dodat ćemo i replikacijsku grupu imena torbar-klinika.hr\poslovanje\dokumenti.

Funkcionalnost replikacije provjerit ćemo tako da kreiramo datoteku na poslužitelju SERVER2 te pratimo promjene na poslužitelju SERVER3. Možemo vidjeti kako kreiranjem datoteke na poslužitelju SERVER2 replikacija odrađuje svoj posao te istu datoteku možemo vidjeti i na poslužitelju SERVER3.

1. Zaključak
2. Reference

Windows Server 2016 Inside Out, Thomas, Orin, Pearson Education Inc.

<http://technet.microsoft.com/en-us/library/gg232606(WS.10).aspx>

[Step-by-Step for Mirrored Storage Spaces Resiliency using PowerShell | Microsoft Docs](https://docs.microsoft.com/en-us/archive/blogs/josebda/step-by-step-for-mirrored-storage-spaces-resiliency-using-powershell)

<https://www.vembu.com/blog/distributed-file-system-dfs-windows-server-2016-brief-overview/>

[Dynamic Access Control Overview (Windows 10) - Microsoft 365 Security | Microsoft Docs](https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/dynamic-access-control)

<http://technet.microsoft.com/en-us/library/cc754833(v=ws.10).aspx>

[Network Load Balancing Deployment Guide | Microsoft Docs](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc754833(v=ws.10)?redirectedfrom=MSDN)

[Virtualization-Documentation/virtualization/windowscontainers at live · MicrosoftDocs/Virtualization-Documentation · GitHub](https://github.com/MicrosoftDocs/Virtualization-Documentation/tree/live/virtualization/windowscontainers)

[Docker run reference | Docker Documentation](https://docs.docker.com/engine/reference/run/)

[Overview of Windows Server upgrades | Microsoft Docs](https://docs.microsoft.com/en-us/windows-server/upgrade/upgrade-overview)

[Step-By-Step: Migrating The Active Directory Certificate Service From Windows Server 2008 R2 to 2019 (microsoft.com)](https://techcommunity.microsoft.com/t5/itops-talk-blog/step-by-step-migrating-the-active-directory-certificate-service/ba-p/697674)

1. Nakon nadogradnje u zadnjem koraku, operacijski sustav je WS2019 [↑](#footnote-ref-1)
2. Hot Spare – failover mehanizam koji nam omogućava pouzdanost sustava [↑](#footnote-ref-2)