

VISOKO UČILIŠTE ALGEBRA

PROJEKTNI ZADATAK

Planiranje napredne infrastrukture

Antonio Janach

Zagreb, prosinac 2020.

Sadržaj

| | |
|---|----|
| 1. Sažetak | 1 |
| 2. Zahtjevi infrastrukture | 1 |
| 3. Topologija infrastrukture | 2 |
| 4. Opis infrastrukture | 3 |
| 5. Razrada projekta – projektno rješenje..... | 4 |
| 5.1. Podizanje domene na SERVERDC poslužitelju | 4 |
| 5.2. Dodavanje ostalih Windows računala u domenu | 5 |
| 5.3. Kreiranje korisnika | 6 |
| 5.4. Propagiranje sekundarne domene na SERVER1 računalu s DNS-om..... | 8 |
| 5.5. Konfiguracija DNS-a | 9 |
| 5.6. Storage spaces na SERVER1 poslužitelju..... | 11 |
| 5.7. Konfiguracija DAC-a na SERVER1 poslužitelju | 13 |
| 5.8. Konfiguracija DFS-R između SERVER2 i SERVER3..... | 19 |
| 5.9. CA konfiguracija na SERVER3 poslužitelju..... | 22 |
| 5.10. Instalirati IIS na SERVER1 i SERVER2 poslužitelj + SSL/TLS..... | 26 |
| 5.11. Konfiguracija DHCP-a na SERVER2 i SERVER3 | 29 |
| 5.12. Konfiguracija NLB uloge | 33 |
| 5.13. Internetska veza na SERVER3..... | 39 |
| 5.14. Konfiguracija reverse proxy na CentOS1 poslužitelju | 41 |
| 5.15. Docker na SERVER3 poslužitelju..... | 43 |
| 5.16. Nadogradnja SERVER3 poslužitelja na Windows server 2019 | 46 |
| 6. Zaključak..... | 54 |
| 7. Popis slika..... | 55 |
| 8. Reference | 57 |

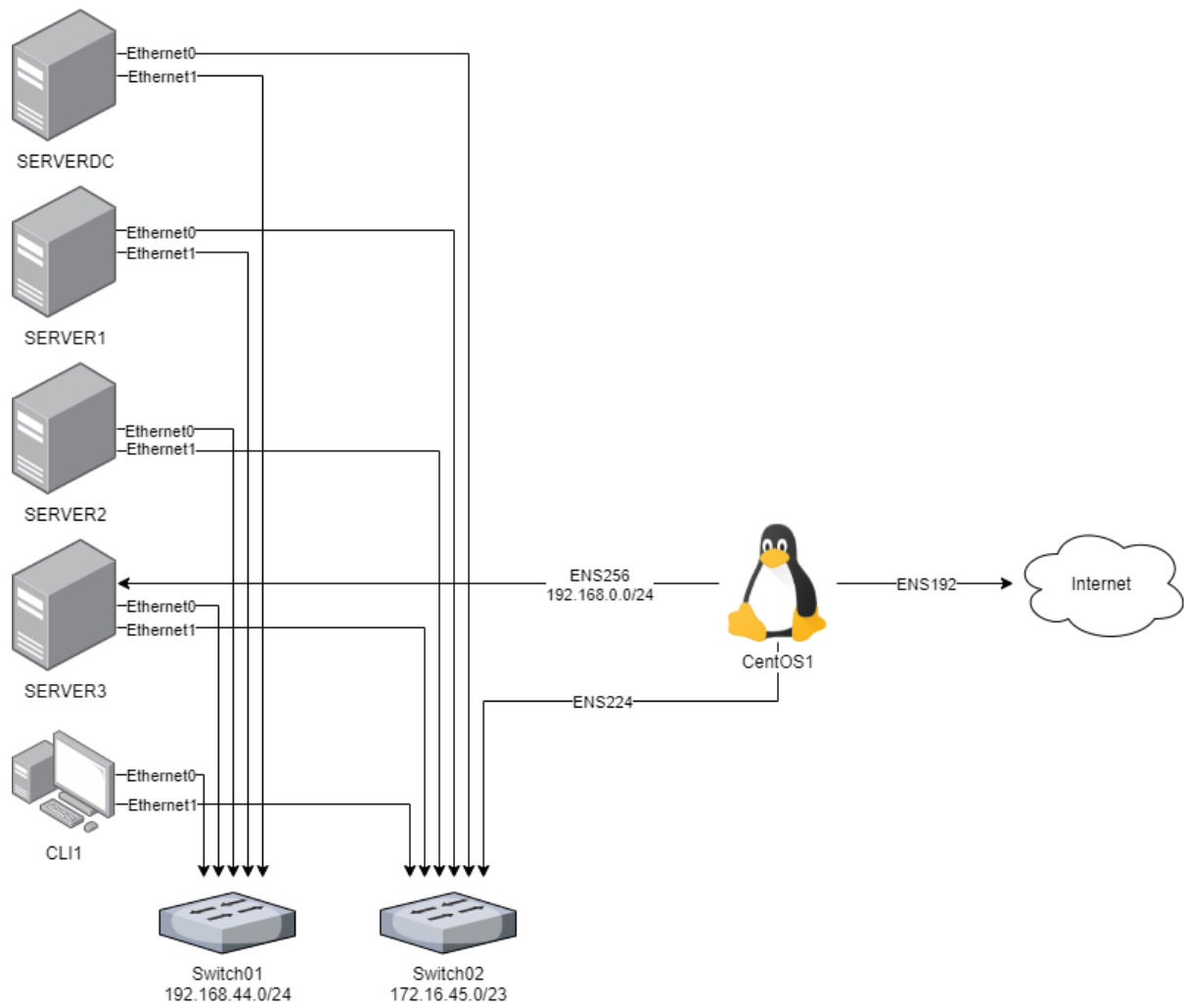
1. Sažetak

Za potrebe rješavanja zadataka koji su navedeni u projektu koristit će se računala: SERVERDC, SERVER1, SERVER2, SERVER3 i CLI1 od kojih je jedno linux računalo CentOS1. Cilj projektnog zadatak je od nule podići infrastrukturu prema zahtjevima klinike janach-klinika.hr.

2. Zahtjevi infrastrukture

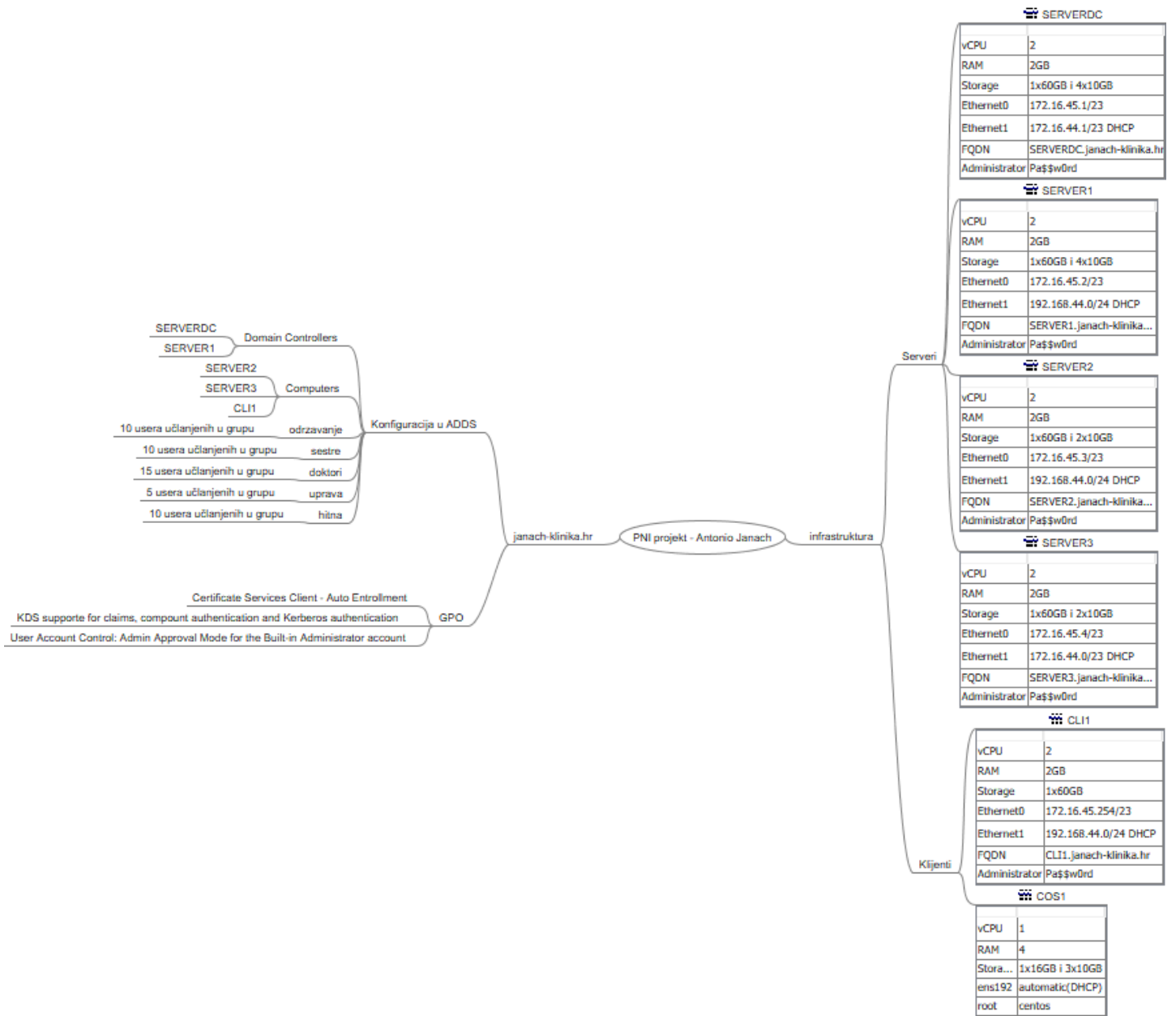
Zahtjevi tvrtke su podignuti domenu janach-klinika.hr na SERVERDC poslužitelju. Kreirati 50 korisnika koji su dodani u pripadajuće OU(organizational unit) i pripadajuće grupe. Podići sekundarni DNS i DC na SERVER1 poslužitelju zajedno s Storage Spaces-om i Dynamic Access Control datotečnim sustavom. Funkcionalan Destributed File System na SERVER2 i SERVER3 poslužitelju s replikacijom. Zatim SERVER3 dodati u domenu i instalirati CA i DHCP cluster koji je u paru sa SERVER2. Na SERVER1 i SERVER2 instaliran IIS i postavljena testna stranica koja koristi SSL/TLS enkripciju. Na SERVERDC instalirati NLB i konfigurirati ga za SERVER1 i SERVER2. Postaviti default gateway na SERVER3, default gateway je CentOS1 linux računalo. Zatim na CentOS1 privremeno omogućiti internet i instalirati reverse proxy poslužitelj za pristup web stranicama na NLB-u kad SERVER3 računalo izgubi vezu domenskog mrežnog adaptera. Kad je uspješno uspostavljena veza s internetom potrebno je podignuti Docker engine i preuzeti docker container, kad je docker container preuzet potrebno je zabraniti vezu s Internetom koja je uspostavljena pomoću CentOS1 računala. Za kraj na SERVER3 poslužitelju napraviti nadogradnju na Windows server 2019.

3. Topologija infrastrukture



Slika 1: Shematski prikaz topologije

4. Opis infrastrukture



Slika 2: za izradu umne mape u kojoj je opisana infrastrukturu korišten FreeMind software

5. Razrada projekta – projektno rješenje

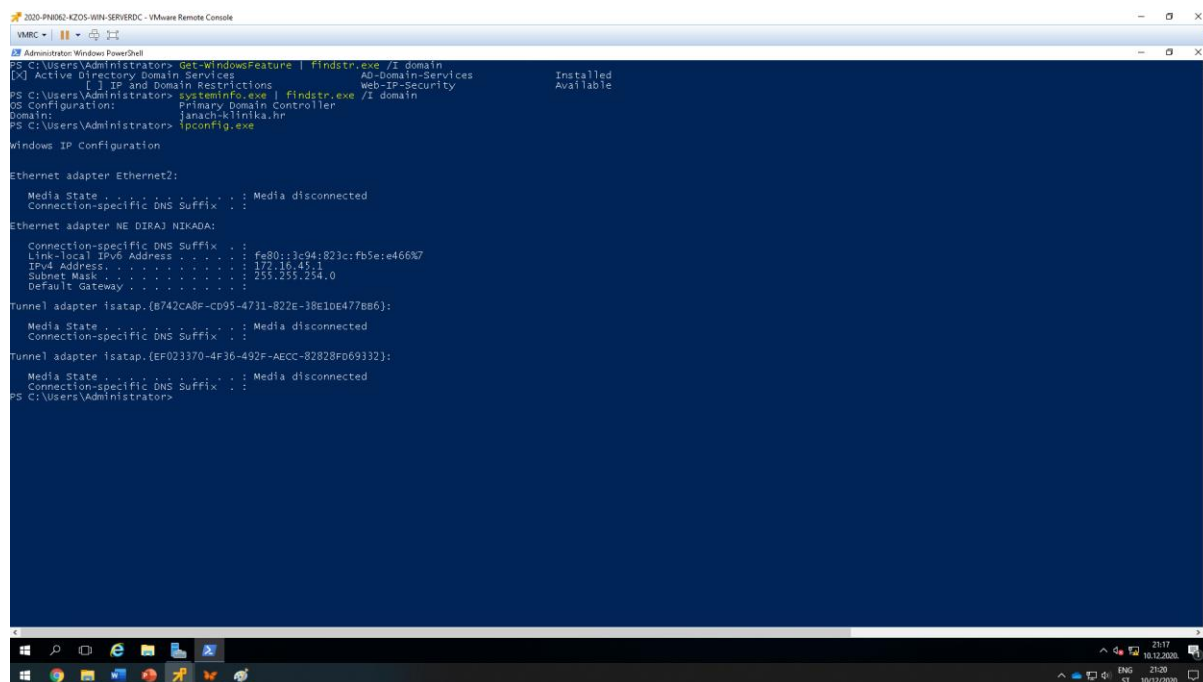
5.1. Podizanje domene na SERVERDC poslužitelju

Prije podizanja domene potrebno je promijeniti IP adrese mrežnim adapterima na Windows poslužiteljima i na Windows klijentskom računalu. Poslužiteljima i klijentskom računalu sam promijenio IP adrese koristeći subnet 172.16.45.0/23. Kad su adrese postavljene potrebno je napraviti dodatnu provjeru ping naredbom i ispitati da li računala mogu komunicirati jedni s drugima.

Promjenom IP adresa računalu SERVERDC spremno je za podizanje domene. Koristeći Server Manager potrebno je instalirati ADDS(Active Directory Domain Services) ulogu.

Add Roles and Features -> Server roles -> ADDS.

Kad je instalacije završena potrebno je propagirati SERVERDC u Domain Controller. Kod propagacije Domain Controller-a odabire se opcija dodavanje forest-a i u polje Root domain name upisujemo janach-klinika.hr. U Domain Controller opcijama functional level je Windows Server 2016, SERVERDC će ujedno koristiti DNS ulogu. U polje DSRM(Directory Services Restore Mode) upisati lozinku Pa\$\$w0rd. U nadolazećim koracima odabiru se default-ne postavke te kad se SERVERDC propagira bit će automatski pokrenuti s funkcionalnom domenom.



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-WindowsFeature | Findstr.exe /I domain
[D] Active Directory Domain Services                AD-Domain-Services                Installed
    [ ] IP and Domain Restrictions                  Web-IP-Security                    Available
PS C:\Users\Administrator> systeminfo.exe | findstr.exe /I domain
OS Configuration: Primary Domain Controller
Domain: janach-klinika.hr
PS C:\Users\Administrator> ipconfig.exe

Windows IP Configuration

Ethernet adapter Ethernet2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
Ethernet adapter NE DIRAJ NIKADA:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::3c94:823c:fb5e:e466%7
    IPv4 Address. . . . . : 172.16.45.1
    Subnet Mask . . . . . : 255.255.254.0
    Default Gateway . . . . . :

Tunnel adapter Isatap.{8742CA8F-CD95-4731-822E-38E1DE4778B6}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
Tunnel adapter Isatap.{EF023370-4F36-492F-AECC-82828FD69332}:

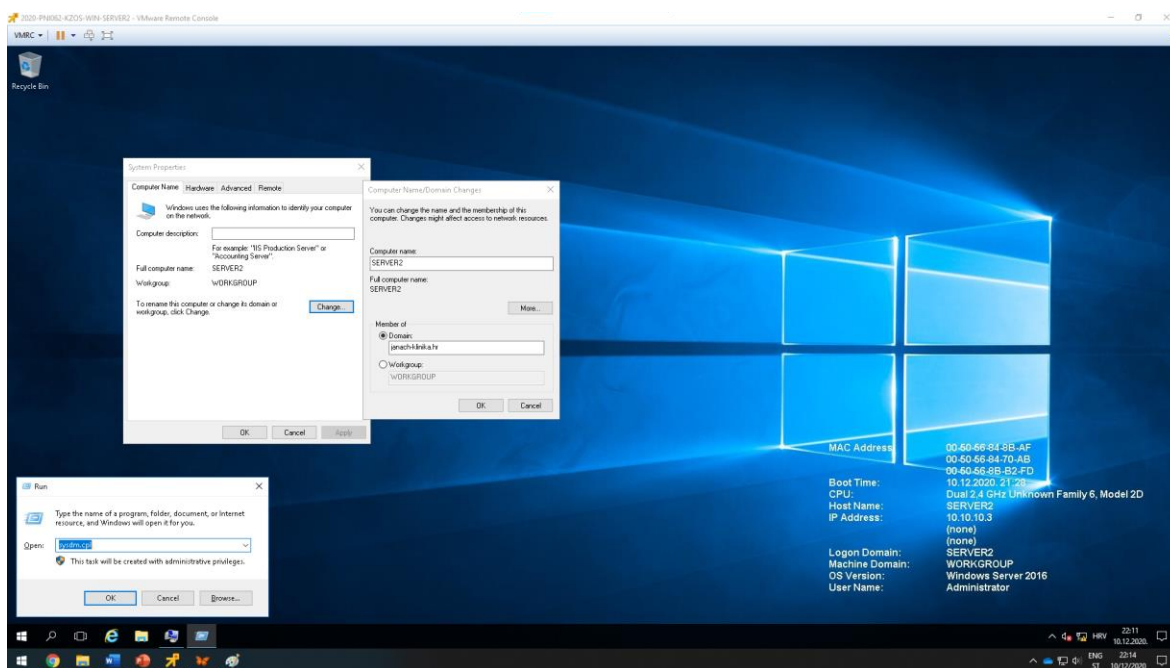
    Media state . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
PS C:\Users\Administrator>
```

Slika 3: prikaz podignute domene zajedno sa IP adresom na mrežnom adapteru

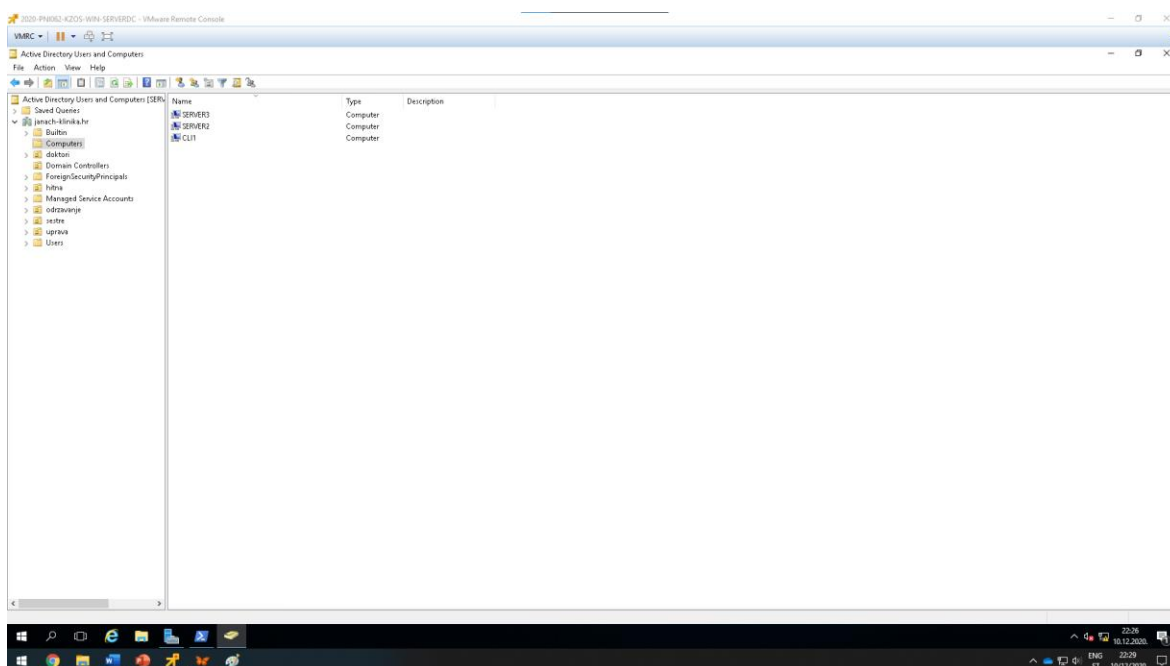
5.2. Dodavanje ostalih Windows računala u domenu

Funkcionalnom domenom ostala računala spremna su biti dodana u domenu osim SERVER1 poslužitelja koje služi kao sekundarni domain controller. Metoda za dodavanje računala je ista Windows računala.

Kad se prijavimo na jedan od računala koristi prečicu CTRL + R i upisati sysdm.cpl i kliknuti na gumb „Change“ i u domain polje upisati janach-klinika.hr, zatim se otvara prozor u kojeg se upisuju kredencijali domain administratora. Računalo zahtjeva restart te ga je potrebno reboot-at.



Slika 4: slika prikazuje dodavanje računala u domenu



Slika 5: prikaz dodanih računala u domenu

5.3. Kreiranje korisnika

Pošto zadatak traži da se kreira 50 usera odlučio sam ih kreirati pomoću .csv datoteke i PowerShella kako bi pomoću jedne skripte dodao svih 50 usera. Razlog zbog kojeg sam kreirao .csv datoteku je što ću se često susresti u produkciji sa importom podataka iz .csv datoteke, a i pretežito iz znatiželje.

```
#kreiranje OU:
New-ADOrganizationalUnit -Name održavanje
New-ADOrganizationalUnit -Name sestre
New-ADOrganizationalUnit -Name doktori
New-ADOrganizationalUnit -Name uprava
New-ADOrganizationalUnit -Name hitna

#kreiranje grupe u OU:
New-ADGroup -GroupScope Global -Name održavanje -Path "OU=održavanje,DC=janach-
klinika,DC=hr"
New-ADGroup -GroupScope Global -Name sestre -Path "OU=sestre,DC=janach-
klinika,DC=hr"
New-ADGroup -GroupScope Global -Name doktori -Path "OU=doktori,DC=janach-
klinika,DC=hr"
New-ADGroup -GroupScope Global -Name uprava -Path "OU=uprava,DC=janach-
klinika,DC=hr"
New-ADGroup -GroupScope Global -Name hitna -Path "OU=hitna,DC=janach-klinika,DC=hr"

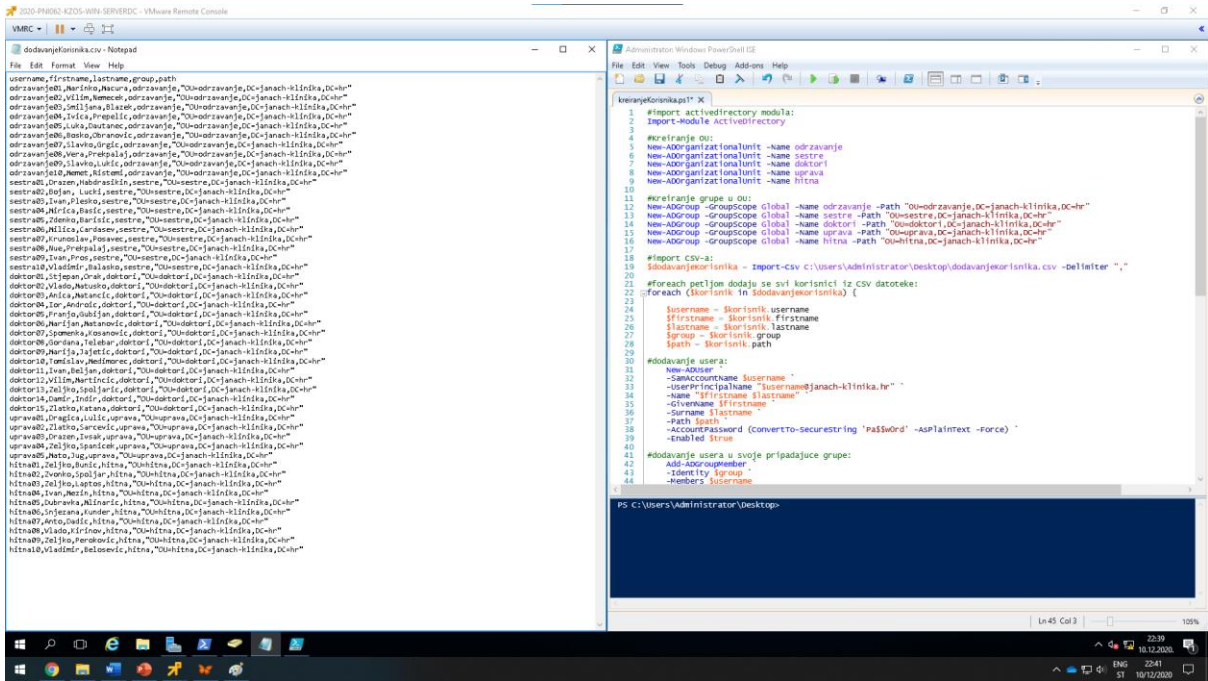
#import CSV-a:
$dodavanjeKorisnika = Import-Csv
C:\Users\Administrator\Desktop\dodavanjeKorisnika.csv -Delimiter ","

#foreach petljom dodaju se svi korisnici iz CSV datoteke:
foreach ($korisnik in $dodavanjeKorisnika) {

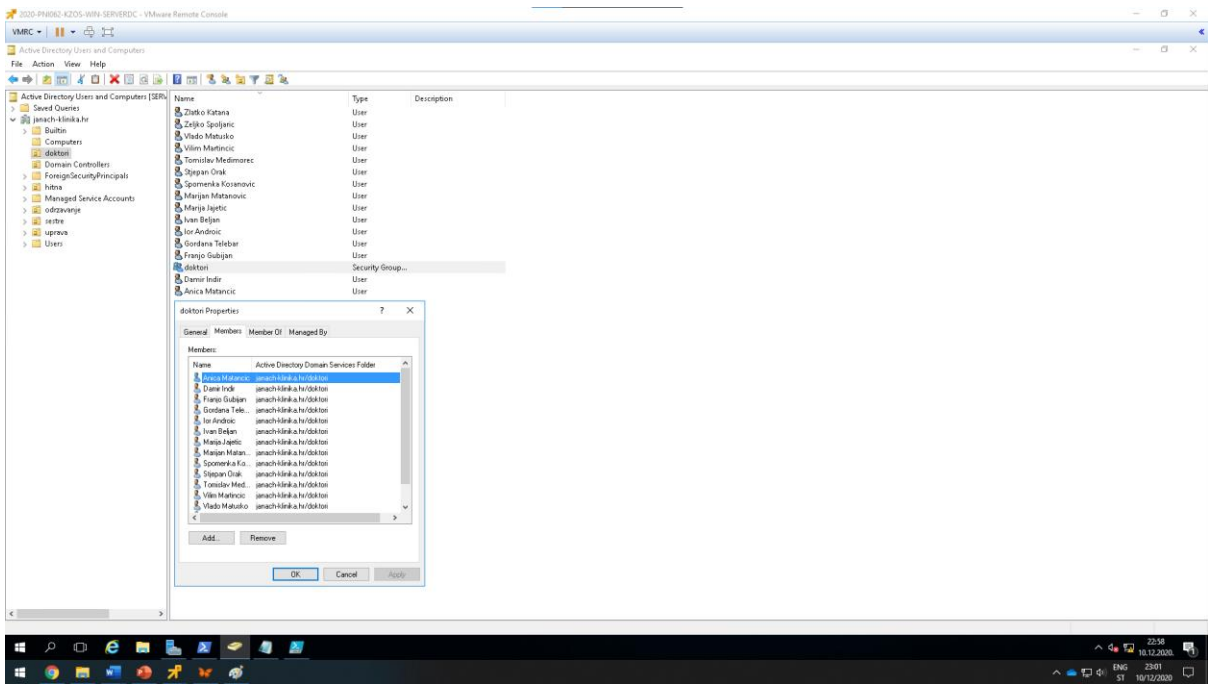
    $username = $korisnik.username
    $firstname = $korisnik.firstname
    $lastname = $korisnik.lastname
    $group = $korisnik.group
    $path = $korisnik.path

#dodavanje usera:
    New-ADUser
    -SamAccountName $username
    -UserPrincipalName "$username@janach-klinika.hr"
    -Name "$firstname $lastname"
    -GivenName $firstname
    -Surname $lastname
    -Path $path
    -AccountPassword (ConvertTo-SecureString 'Pa$$wOrd' -AsPlainText -Force)
    -Enabled $true

#dodavanje usera u svoje pripadajuće grupe:
    Add-AzureADGroupMember
    -Identity $group
    -Members $username
}
```

Slika 6: prikazuje dodavanje usera .csv datotekom pomoću PowerShell skripte



Slika 7: prikaz OU, usera koji su dodani u grupu

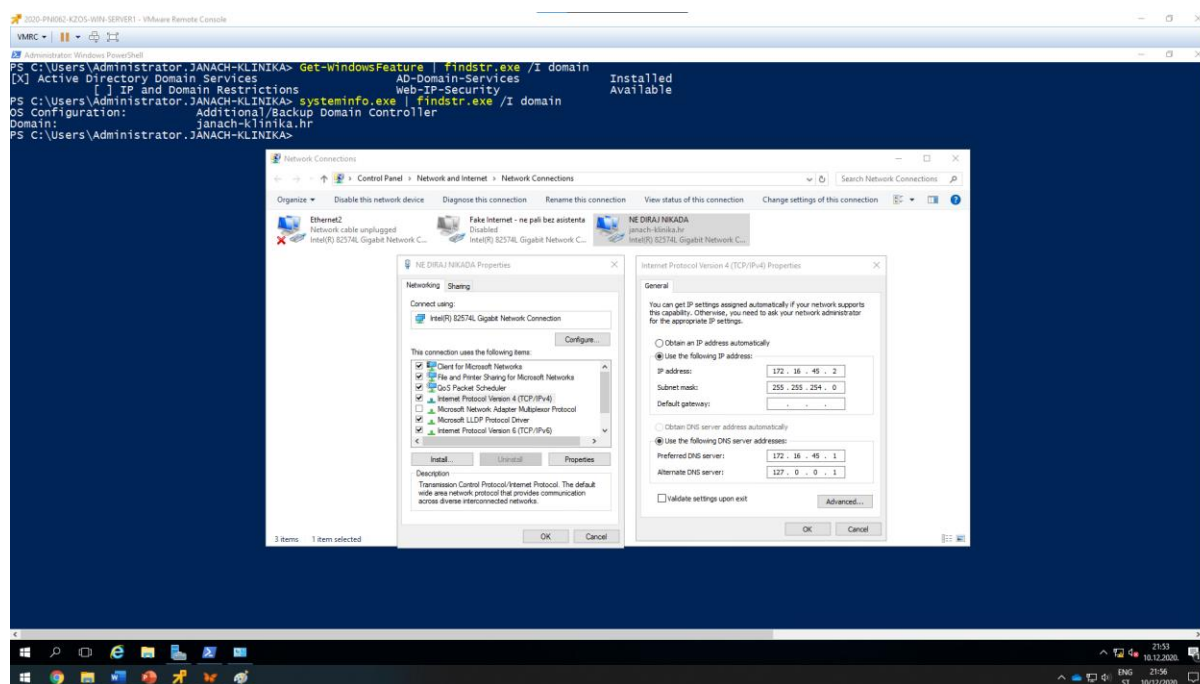
5.4. Propagiranje sekundarne domene na SERVER1 računalu s DNS-om

Prije instalacije ADDS(Active Directory Domain Services) uloge kod domenskog mrežnog adaptera dodati DNS server(172.16.45.1) od SERVERDC poslužitelja.

Koristeći Server Manager instalirati ADDS ulogu.

Add Roles and Features -> Server roles -> ADDS.

Kad je instalacije završena potrebno je propagirati SERVER1 u sekundarni Domain Controller. Kod propagacije sekundarnog Domain Controller-a odabrati opciju „add a domain controller to an existing domain“ zatim specificirati domenu u koju SERVER1 želimo dodati kao domain controller te kod odabira upisujemo kredencijale domenskog administratora kako bi odabrali domenu u kojoj će SERVER1 biti sekundarni DC. Kod kartice Domain Controller Options potrebno je omogućiti sve tri funkcije zajedno sa RODC(Read only domain controller) jer funkcija sekundarnog domain kontrolera će biti da replicira informacije sa SERVERDC poslužitelja. U polje DSRM upisati lozinku Pa\$\$w0rd. Sljedeći koraci ostaviti default-no te kad se SERVERDC propagira u sekundarni DC računalo će se samo pokrenuti s funkcionalnom domenom janach-klinika.hr.



Slika 8: prikaz instalirane ADDS uloge koja je propagirana u Additional/backup Domain Controller(sekundarni) i prikaz promjene IP adrese DNS servera nad mrežnim adapterom

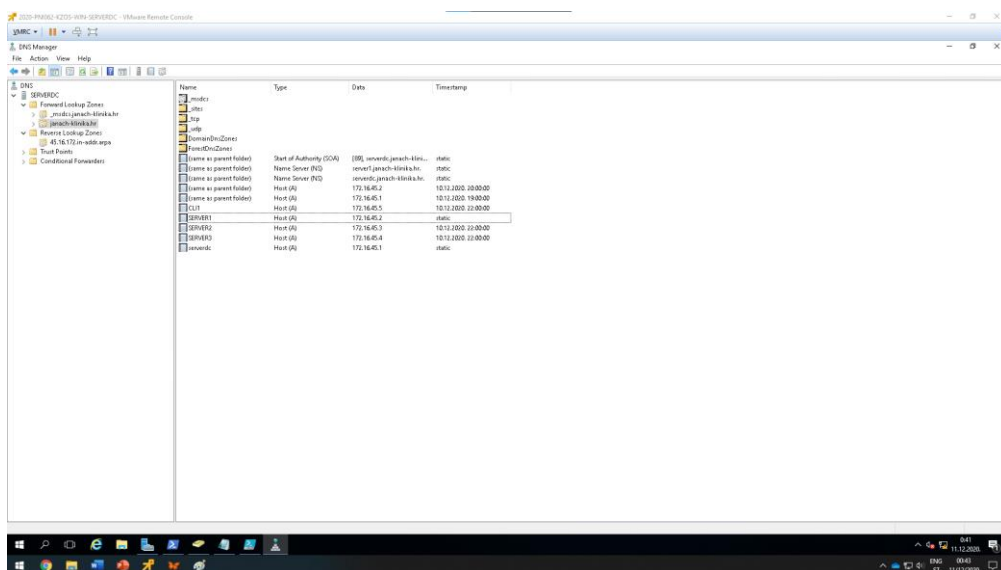
5.5. Konfiguracija DNS-a

Konfiguracijom funkcionalnog domenskog controller-a i sekundarnog domenskog kontrolera potrebno je konfigurirati DNS primarnu reverznu lookup zonu i postavljanje pointer (PTR) zapisa. Također konfigurirati reverznu lookup zonu na SERVER1 poslužitelju. Koristeći Server Manager konfigurirati DNS.

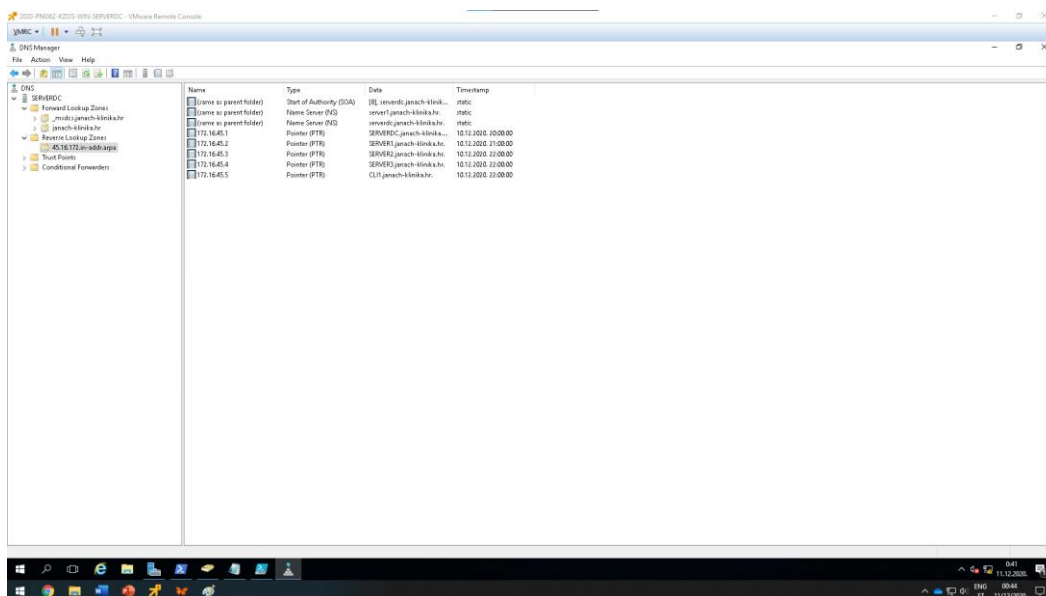
Tools -> DNS -> SERVERDC

Novu reverznu zonu kreiramo desnim klikom na Reverse Lookup Zones i klikom na New Zone.

Otvora se wizard u kojem kreiramo IPv4 primarnu reverznu zonu. U polje Network ID upisati 172.16.45 te dopustiti secure dynamic update. Kad se IPv4 primarna reverzna zona kreirala neophodno je ažurirati PTR zapise svih poslužitelja i klijenta u forward lookup zoni.



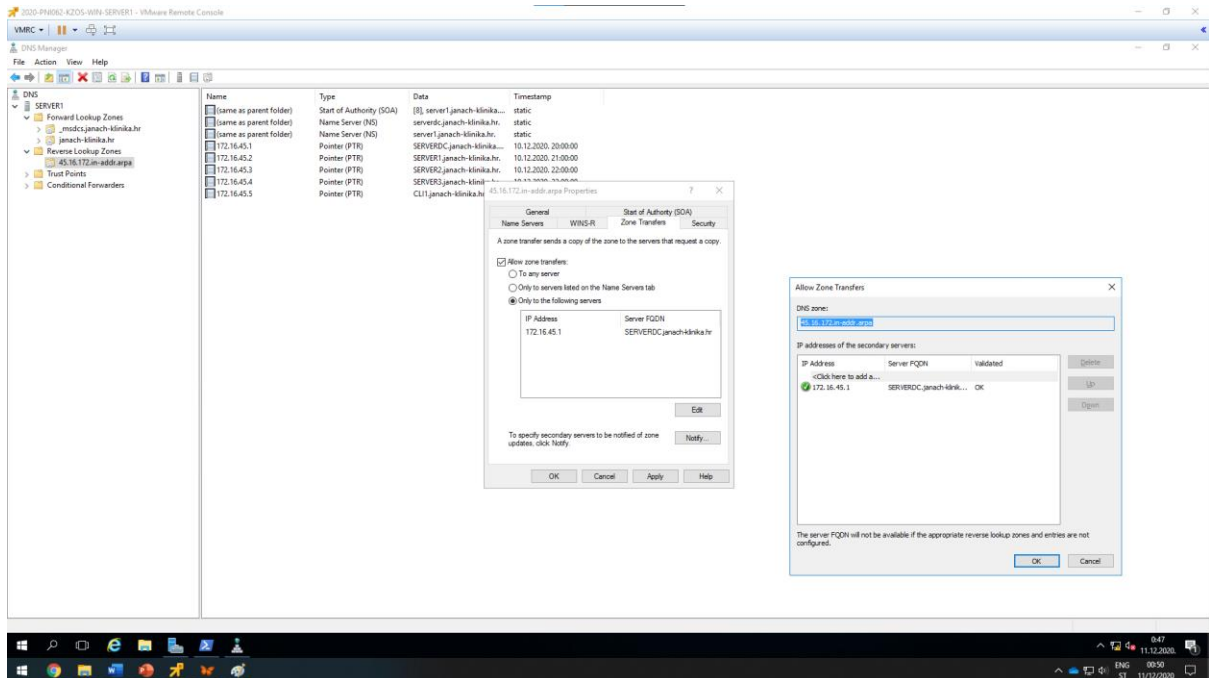
Slika 9: prikaz ažuriranih PTR zapisa u forward lookup zoni



Slika 10: prikaz zapisa IPv4 primarne reverzne lookup zone

Slijedi konfiguracija DNS zone na SERVER1 poslužitelju.

Kad otvorimo DNS Manager konzolu na SERVER1 računalu vidljivo je da se je reverzna lookup zona replicirala te je neophodno desnim klikom miša na reverznu zonu odabrati properties i kliknuti na karticu zone transfer i omogućiti zone transfer.



Slika 11: Shodno tome vidljivo je da su zapisi replicirani u reverznoj zoni na SERVER1 poslužitelju

5.6. Storage spaces na SERVER1 poslužitelju

Cilj je konfigurirati RAID5 polje od 4 dostupna diska od kojih je svaki kapaciteta 10GB. Kad se osvrnemo prethodno na vježbe iz ovog kolegija Storage Spaces se konfigurirao tako da je jedan od diskova bio u Hot Spare. Hot sparena je funkcionalan disk koji na sebi ne sadrži podatke te, ako jedan od diskova prestane raditi u volume grupi tada se automatski rekonstruiraju podaci sa ne funkcionalnog diska na hot spare što omogućuje višu dostupnost.

Prvi pothvat je postaviti diskove na SERVER1 poslužitelju u online stanje i inicijalizirati ih u GPT partijsku tablicu.

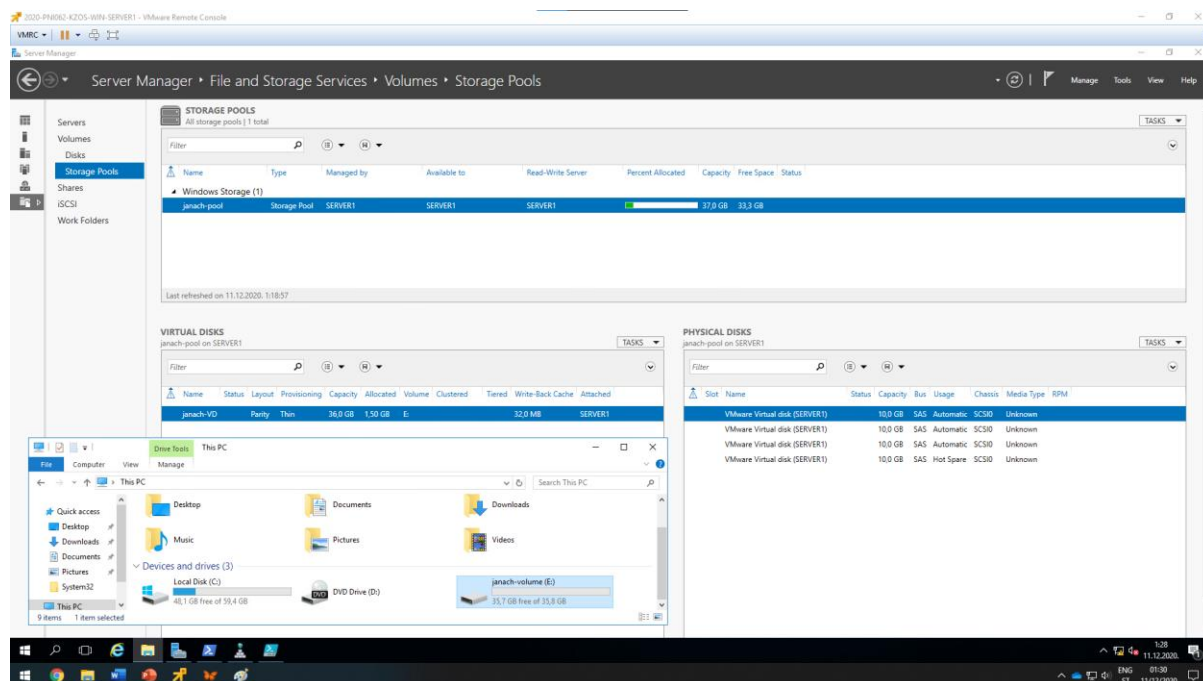
```
#postavljanje svih raspoloživih diskova u online stanje:
Get-Disk | ?{$_.OperationalStatus -eq "offline"} | %{Set-Disk -Number $_.Number
-IsOffline $false}

#inicijalizacija svih raspoloživih diskova u GPT partijsku tablicu:
Get-Disk | ?{$_.PartitionStyle -eq "RAW"} | %{Initialize-Disk -Number $_.Number
-PartitionStyle GPT}
```

Sljedeći podhvat je koristeći Server Manager kreirati Storage Pool od četiri diska.

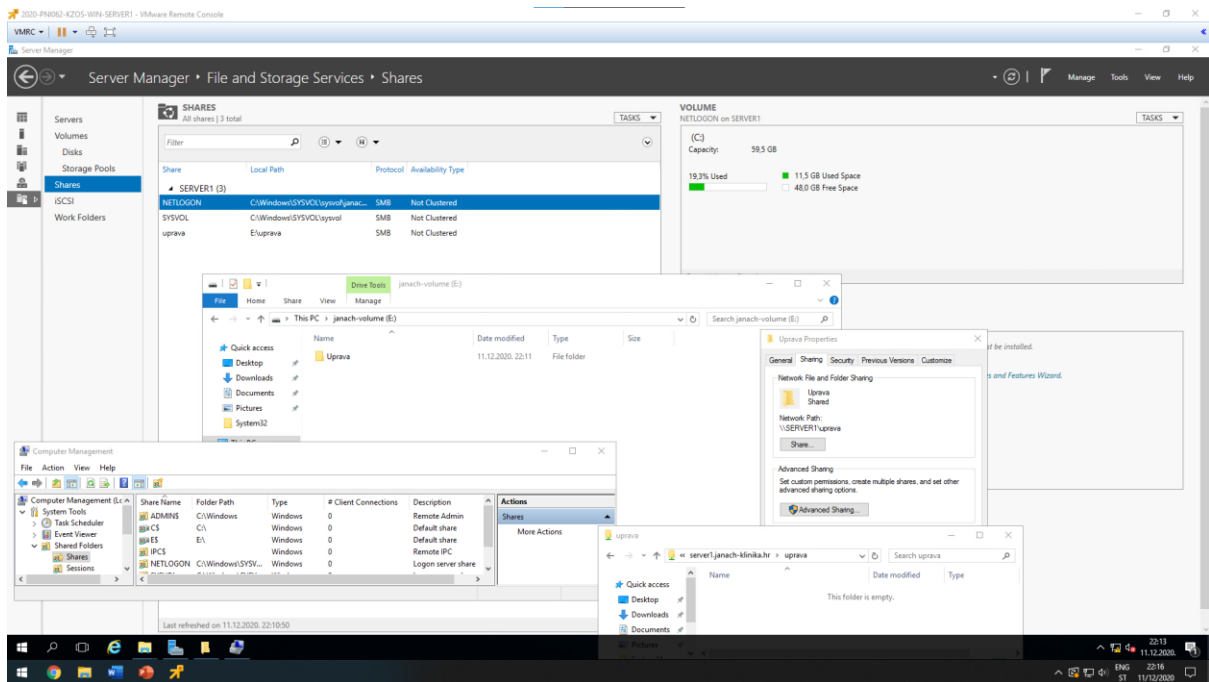
File and Storage Services -> Storage Pools -> New Storage Pool

Otvora se wizard za kreiranje Storage Pool-a, Storage Pool neophodno je imenovati(janach-pool). Sljedeće odabrati sve diskove od kojih jedan treba postaviti u Hot Spare. Time je kreiran Storage Pool. Zatim kreirati virtualni disk iz Storage Pool-a. Klikom na New Virtual Disk otvara se Wizard, virtualni disk neophodno je imenovati(janach-VD) potom kod Storage Layout koraka odabrati Parity. Provisioning Type odabrati na Thin kako bi koristili prostor iz Storage Poola po potrebi. Spesificirati veličinu diska(koristiti maksimalnu veličinu). Kad se virtualni disk kreira otvara se sljedeći wizard gdje se konfigurira volume, drive letter i format file system-a. Koraci kroz koje Wizard vodi mogu biti ostavljeni po default-u samo kod File System Settings imenovati label volumena(janach-volume).



Slika 12: Storage Spaces, Virtualni disk i volumen

Kad je funkcionalno konfiguriran volumen pomoću Storage Spaces-a potrebno je napraviti network share mape uprava. Nad permission-ima Network share mape uprava konfigurirat ćemo ih DAC(Dynamic Access Control)-om u sljedećem poglavlju.



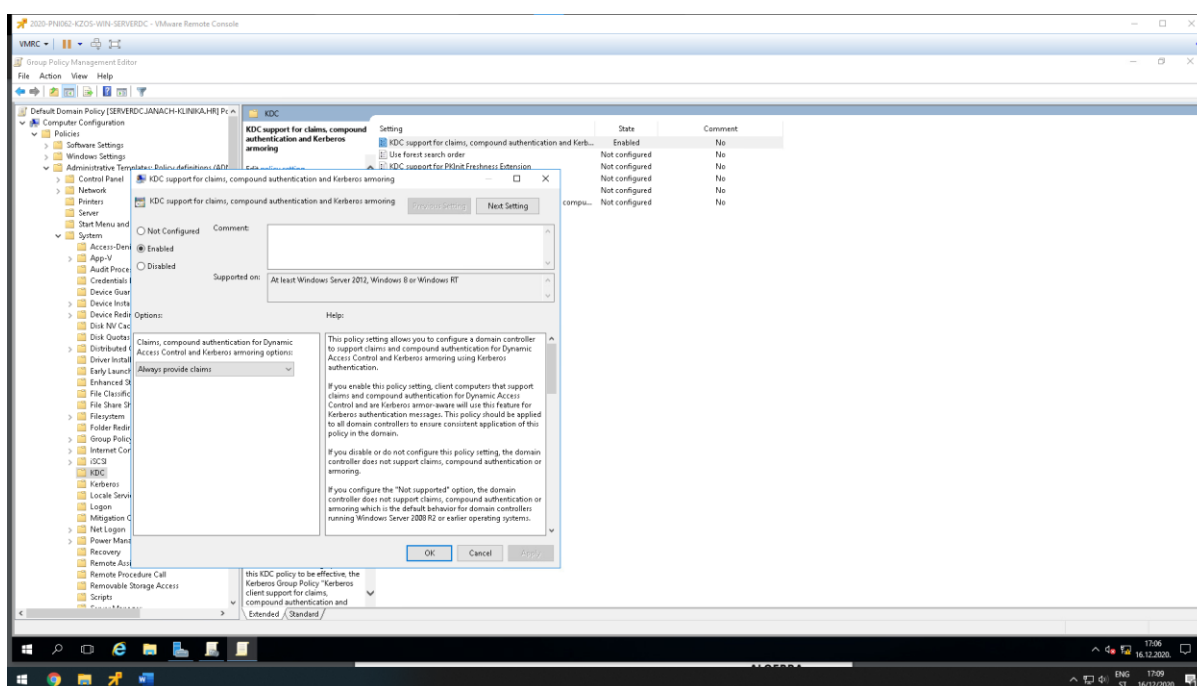
Slika 13:prikaz network share mape uprava

5.7. Konfiguracija DAC-a na SERVER1 poslužitelju

Kad je podignuto dijeljenje mape Uprava na kreiranom volumenu iz Storage Spaces R5 virtualnog diska. Potrebno je korištenjem DAC-a dodijeliti prava pristupa korisnicima iz Uprave. Dokumenti unutar foldera koji sadržavaju tekst „Secret“ neka bude klasificiran da mu mogu pristupiti samo Doktori.

Na SERVERDC nužno je u Group Policy Management-u pod Default Domain Policy omogućiti KDC supporte for claims, compound authentication and Kerberos Armoring i opciju promijeniti u Always provide claims.

Putanja: Computer Configuration -> Policies -> Administrative Templates -> System -> KDC -> KDC supporte for claims, compound authentication and Kerberos armoring

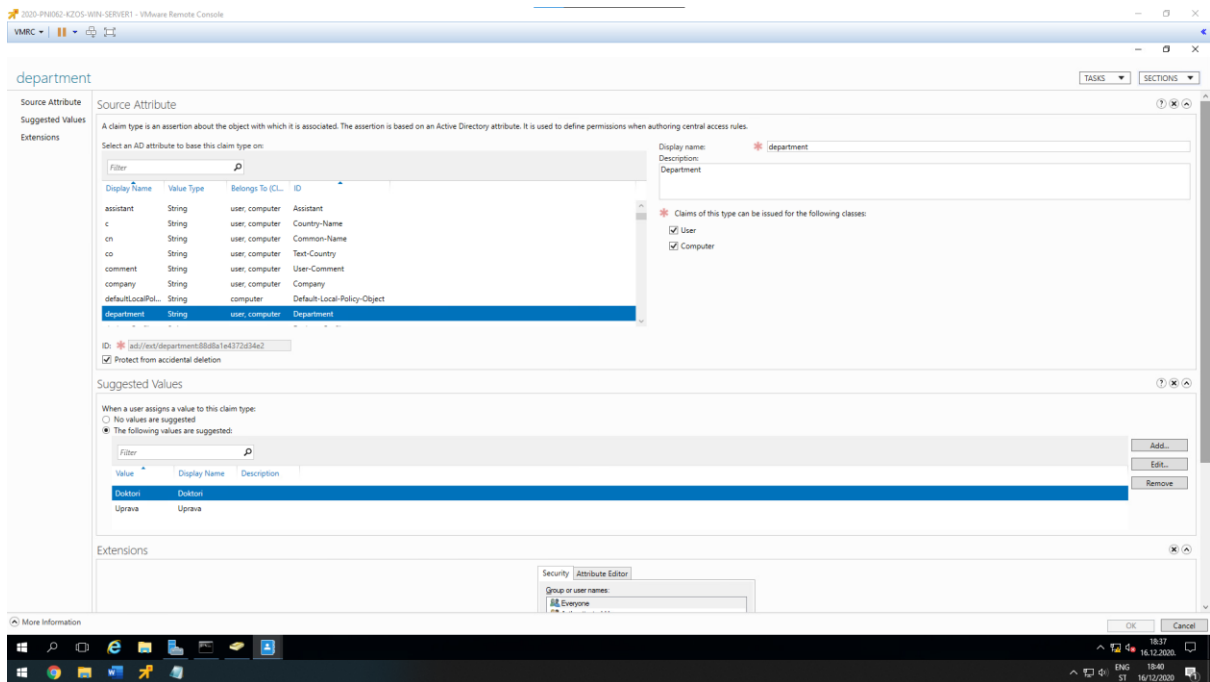


Slika 14: Prikaz setting-a KDC Supporte-a

Kad je omogućen KDC supporte potrebno je na svim poslužiteljima koji su u domeni napraviti gpupdate /force.

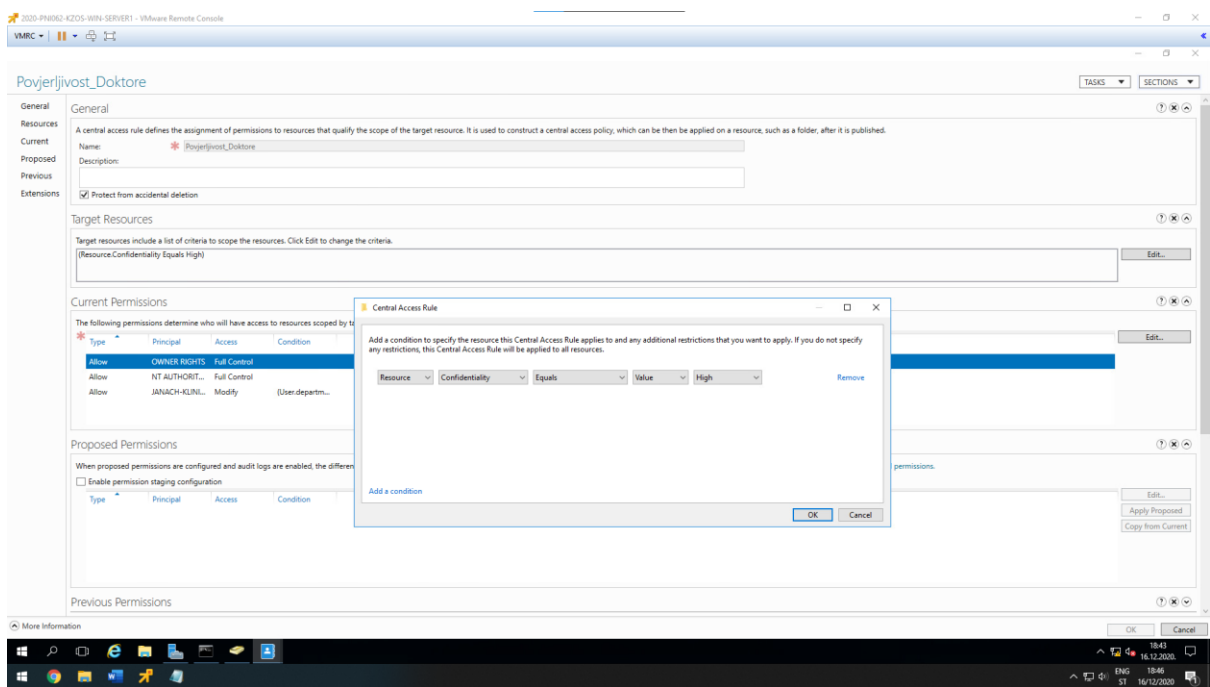
Za članove iz Uprave dodati Department Uprava, članovima u grupi doktori dodati department doktori i sestrama dodati department sestre kako bi isprobali funkcionalnost.

Sljedeće što je potrebno je upaliti Active Directory Administrative Center management i pod Dynamic Access Control -> Resource Properties i na ovoj putanji omogućiti Department i Confidentiality. U Department dodati department uprava i doktori. Zatim pozicionirati se na Claim Type i kreirati novi Claim Type department.

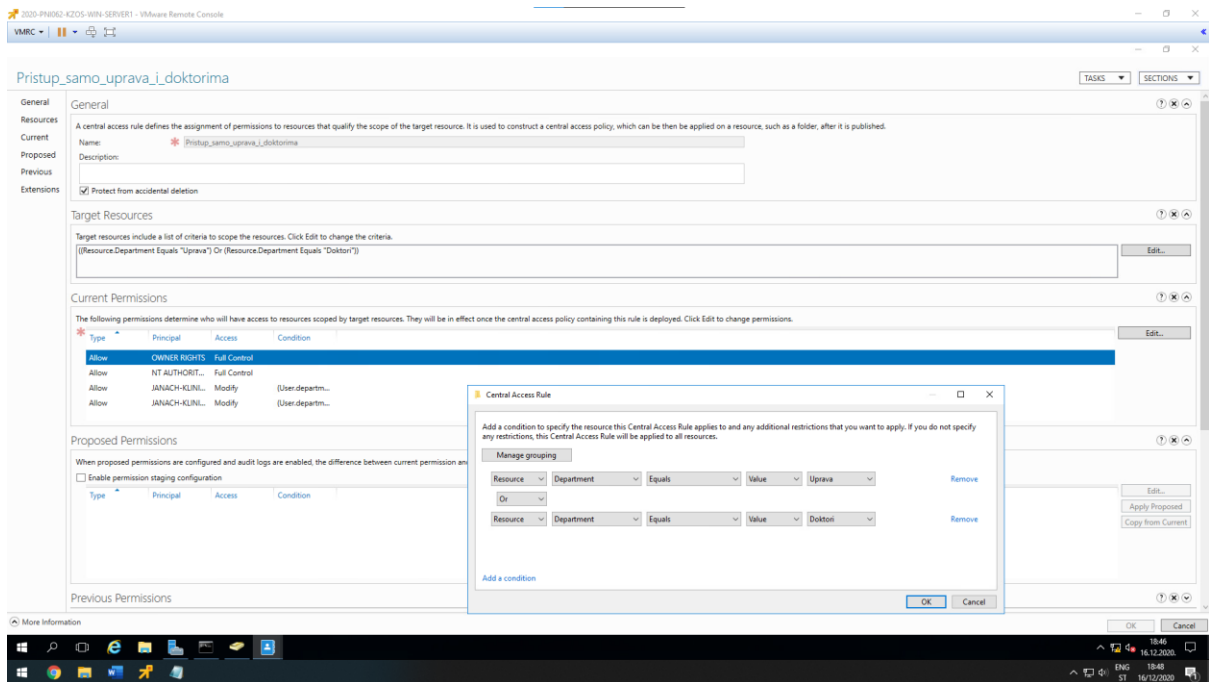


Slika 15: Prikaz setting-a postavljeneh novo kreirani Claim Type: department

Zatim u Central Access Rules kreirati dva rule-a jedan za doktore i jedan za upravu i doktore.



Slika 16: prikaz setting-a za novokreirani Central Access Rules za doktore koji su dodani u current permission

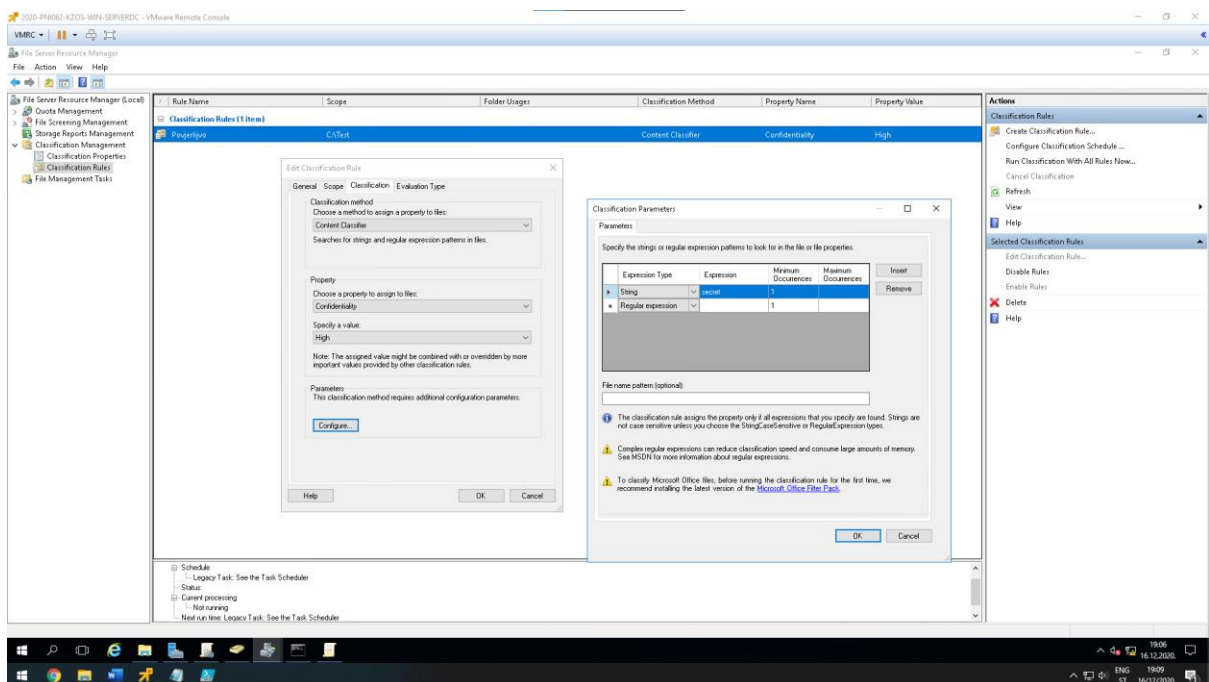


Slika 17: prikaz setting-a za novokreirani Central Access Rules za upravu i doktore koji su dodani u Current Permissions

Zatim instalirati FSRM (File Server Resource Manager) ulogu kako bi se kreiralo klasifikacijsko pravilo nad datotekom koja sadrži „secret“.

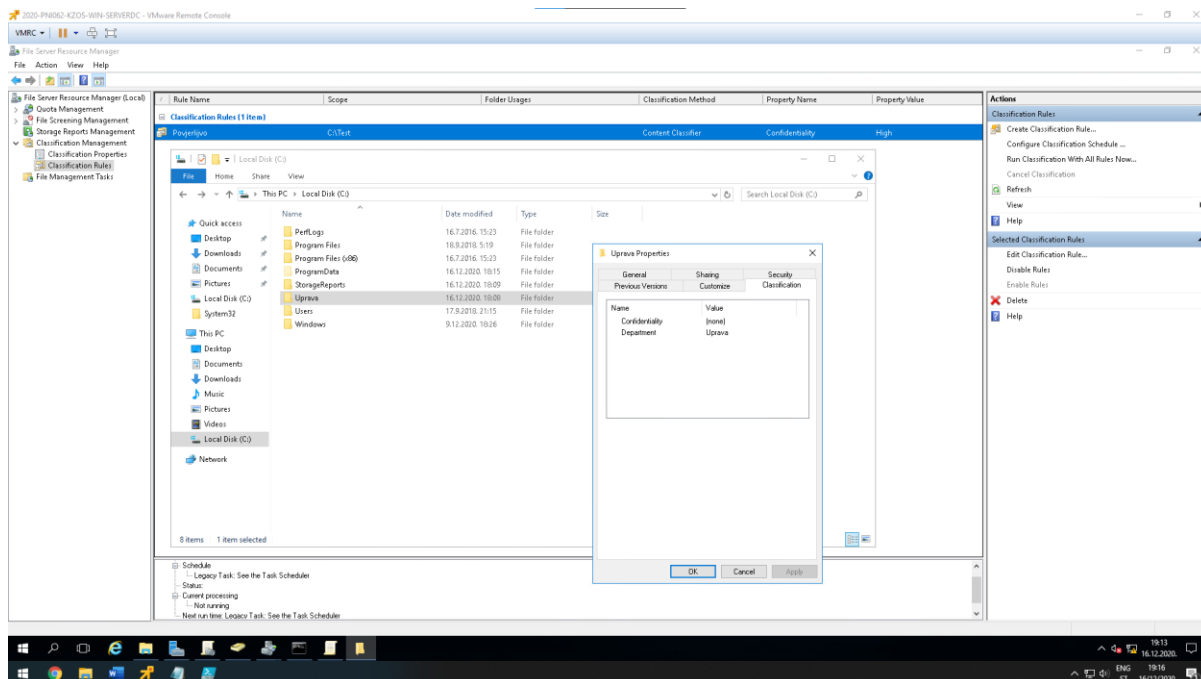
```
Install-WindowsFeature -Name FS-Resource-Manager
```

Otvoriti FSRM management iz Server Manager konzole. Zatim se pozicionirati u File Server Resource Manager (Local) -> Classification Management -> Classification Rules I kreirati novo pravilo za mrežno podijeljenu datoteku na putanji C:\Uprava.



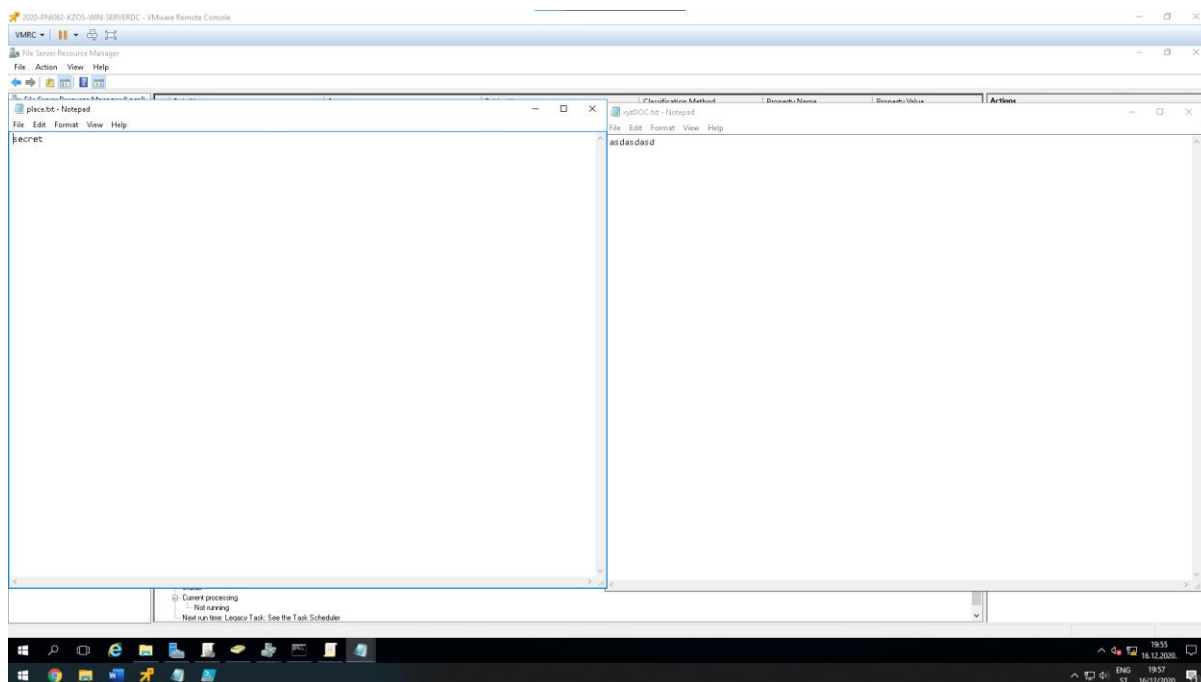
Slika 18: Prikaz setting-a kod kreiranja klasifikacijskog pravila

Kad je klasifikacijsko pravilo kreirano potrebno je nad datotekom koja je mrežno podijeljena dodati klasifikaciju Confidentiality I Department.

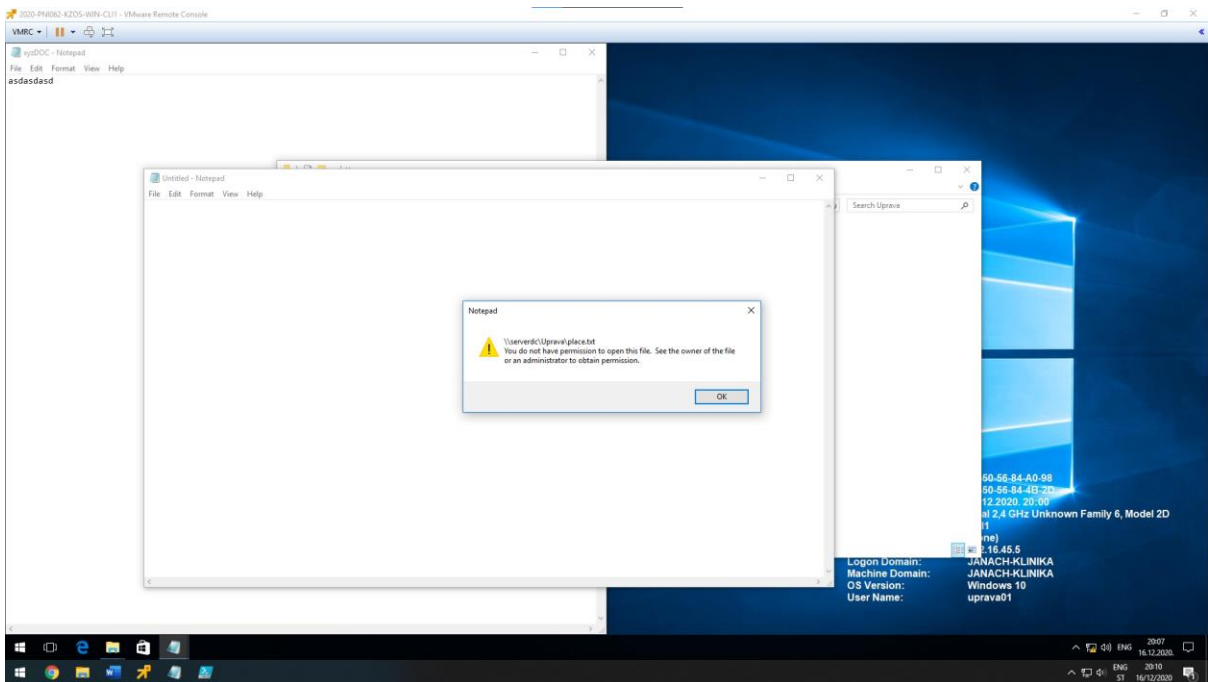


Slika 19: prikaz dodane klasifikacije Confidentiality i Department

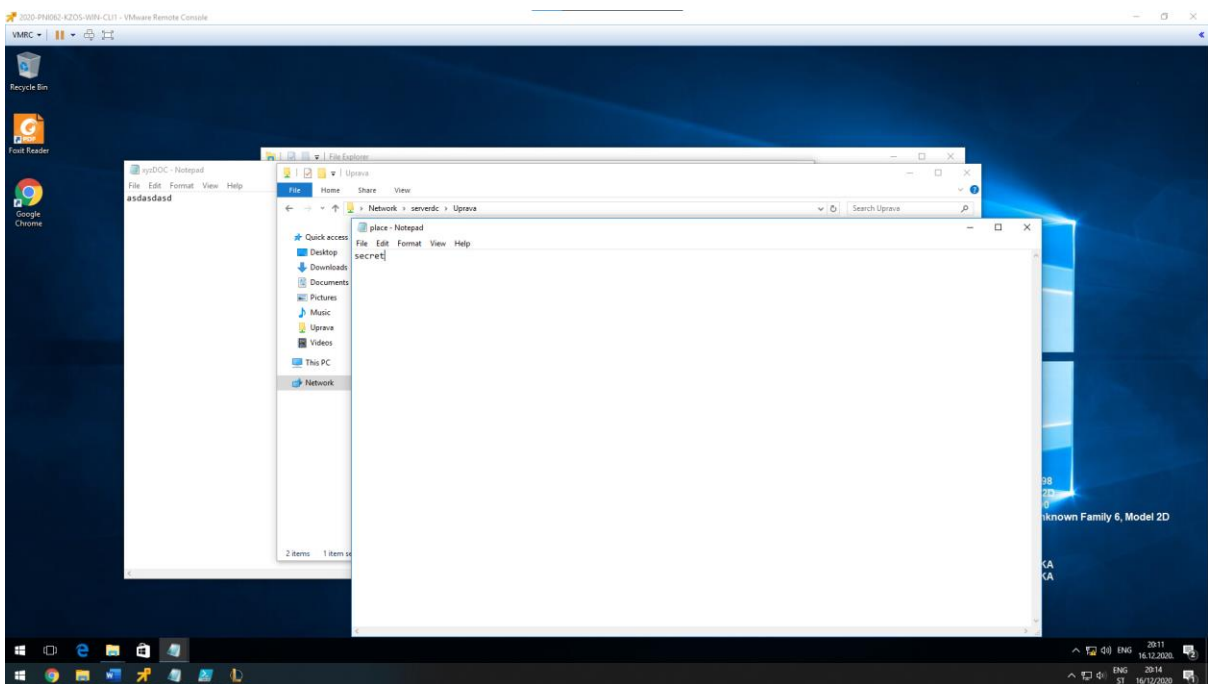
Na kraju testirati funkcionalnost sa CLI1 računala. Točnije prijaviti se sa CLI1 računala s korisnikom iz grupe doktori, zatim s korisnikom iz grupe uprava i s korisnikom iz sestre. Korisnici iz grupe doktori moraju imati pristup svim .txt datotekama, korisnik iz grupe uprave mora moći pristupiti samo datotekama koje ne sadrže u sebi tekst secret i korisnici iz grupe sestre ne smiju imati pristup.



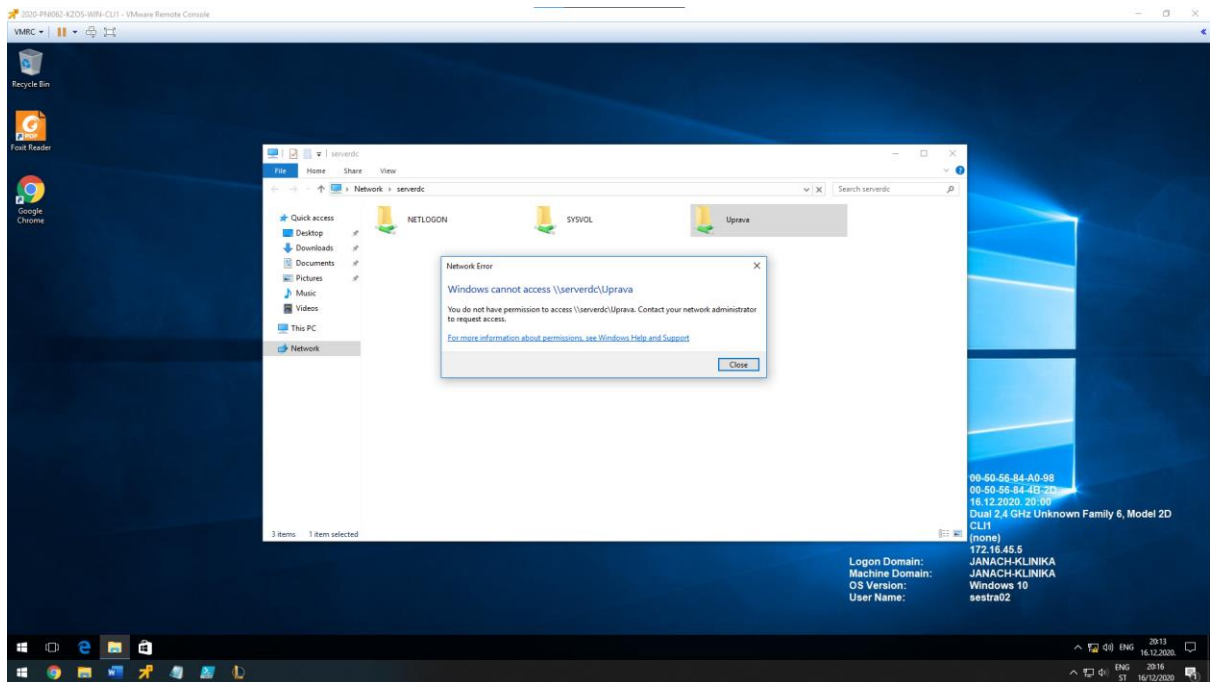
Slika 20: tekstualna datoteka koja sadrži secret kako bi se testirala funkcionalnost



Slika 21: test korisnika iz grupe uprava može ući u xyzDOC.txt datoteku, no ne može ući u place.txt datoteku



Slika 22: test korisnika iz grupe doktori može ući u obje datoteke



Slika 23: test korisnika iz grupe sestre ne može pristupiti datotekama

5.8. Konfiguracija DFS-R između SERVER2 i SERVER3

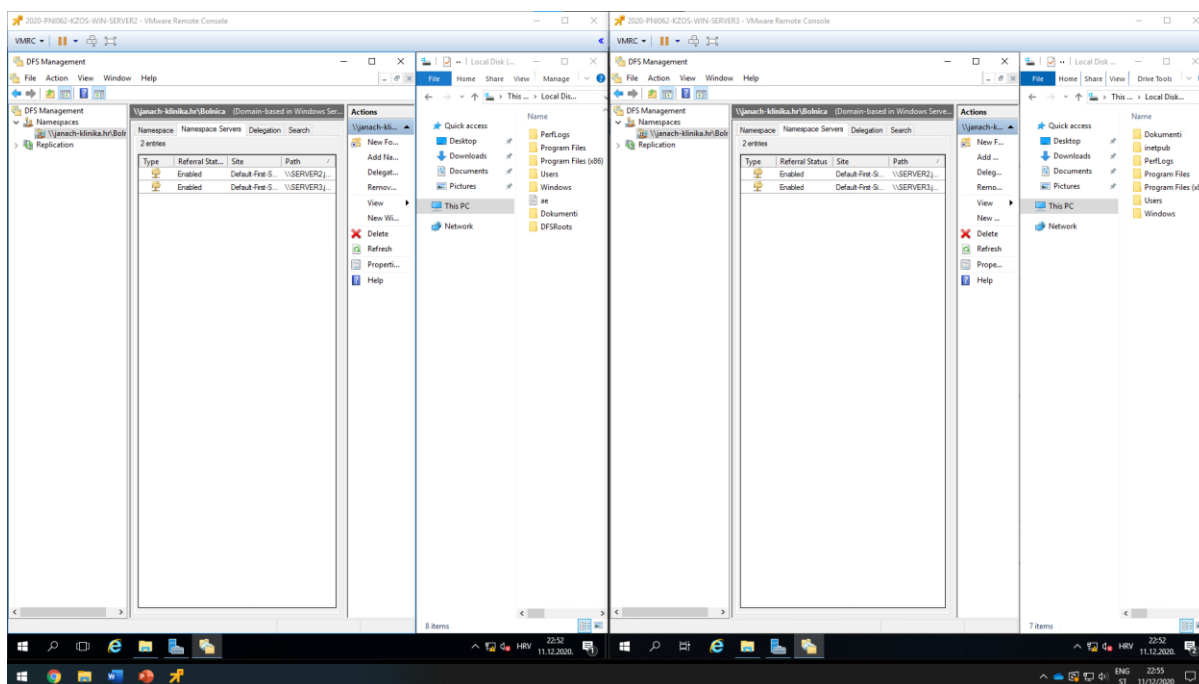
Cilj ovog poglavlja je konfigurirati funkcionalan DFS-R(Distributed File System) s replikacijom između SERVER2 i SERVER3.

Na SERVER1 i SERVER2 poslužitelj koristeći Server Manager instalirati DFS Namespaces i DFS Replication uloge.

Add Roles and Features -> Server roles -> File and Storage Services -> File and iSCSI Services -> DFS Namespaces i DFS Replication

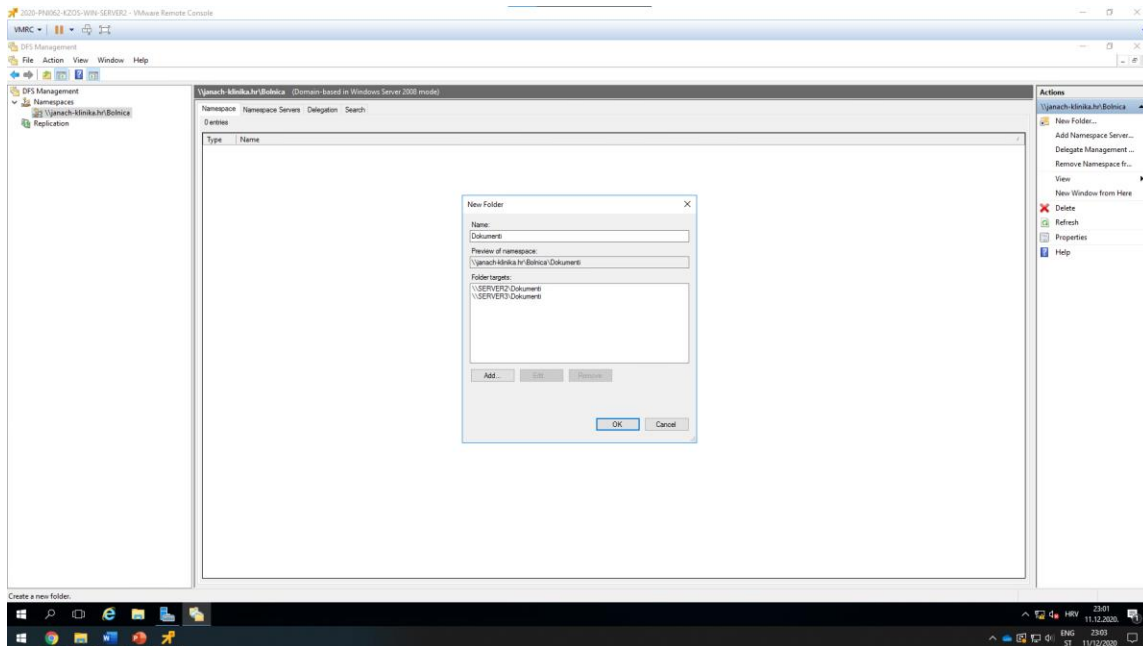
Kad su uloge instalirane kreirati na oba poslužitelja mapu „dokumenti“ koja će se kasnije koristiti u DFS-u. U oba poslužitelja kreirati namespace imena „Bolnica“ pritiskom na gumb New Namespace na traci Actions s desne strane DFS management-a. Otvara se Wizard gdje za server odabiremo SERVER2. Dodati ime namespace-u „Bolnica“, prava pristupa podesiti na custom -> everyone -> full control. Namespace Type bit će podešen na Domain-based namespaces.

Kreiranjem namespace-a u taj namespace dodajemo drugi namespace poslužitelj SERVER3 uz to podesiti prave na custom -> everyone -> full control.



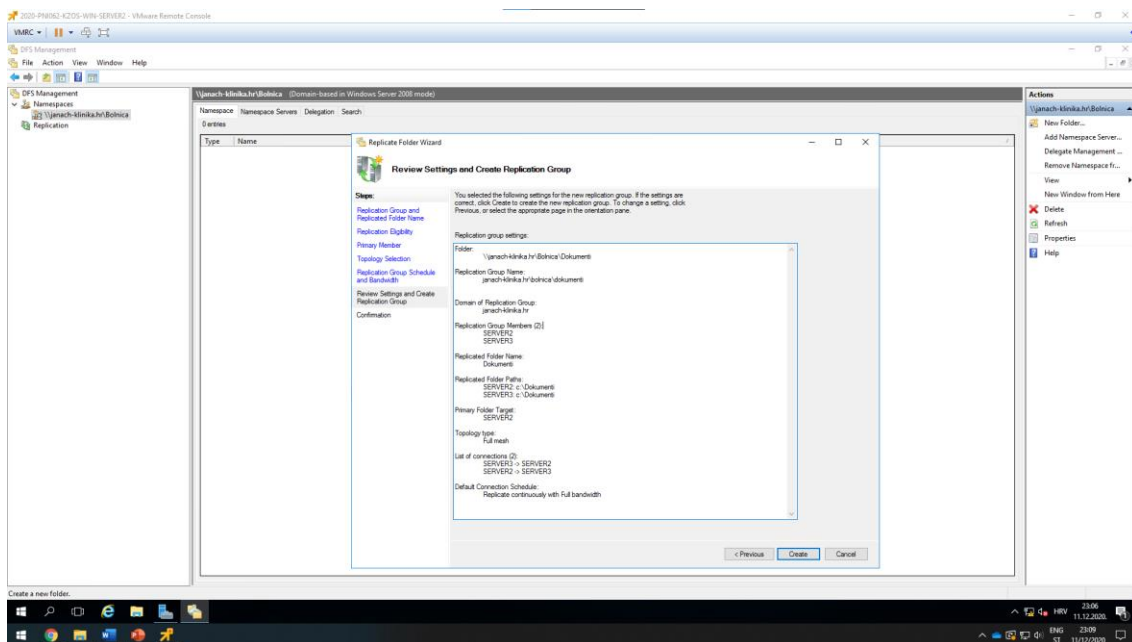
Slika 24: prikaz namespace-a i dodavanje namespace servera

Nakon dodanih namespace server-a kreirati novu mapu u novokreiranom namespace-u. Mapa će se zvati „Dokumenti“ te će toj mapi biti dodijeljena dva target-a, a to su SERVER2 i SERVER3. Pozicionirati se u novokreirani namespaces i s desne strane izbornika odabrati New Folder. Dodati folder-u ime „Dokumenti“ i dodati dva target-a.



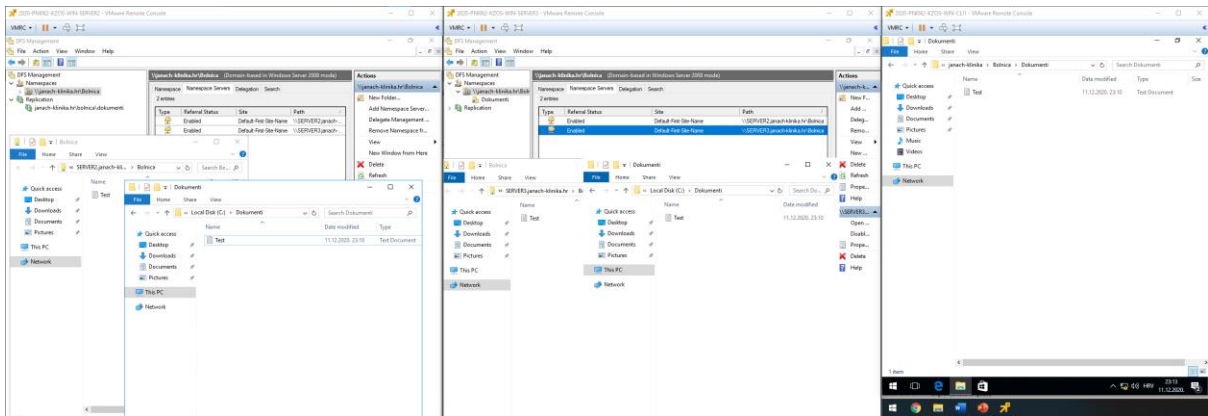
Slika 25: dodavanje novog foldera u namespace s dva target-a

Klikom na OK, DFS Management će automatski prepoznati da želimo konfigurirati DFS replikaciju. Otvara se prozor gdje DFS Management pita da li želimo napraviti replikacijsku grupu. Potrebno je odabrati „Yes“. Nakon toga otvara se Wizard za kreiranje replikacijske grupe. Kroz wizard prolazimo koristeći defaultne postavke no kod Primary membera potrebno je staviti SERVER2(svejedno je).



Slika 26: kreiranje replikacijske grupe

Provjeriti funkcionalnost replikacije sa klijentskog računala CLI1. Na klijentskom računalu spojiti se na network share <\\janach-klinika.hr\Bolnica\Dokumenti> i kreirati .txt dokument imena „Test“. Taj dokument treba se replicirati na sve network share-ove i lokalno na server računala SERVER2 i SERVER3.



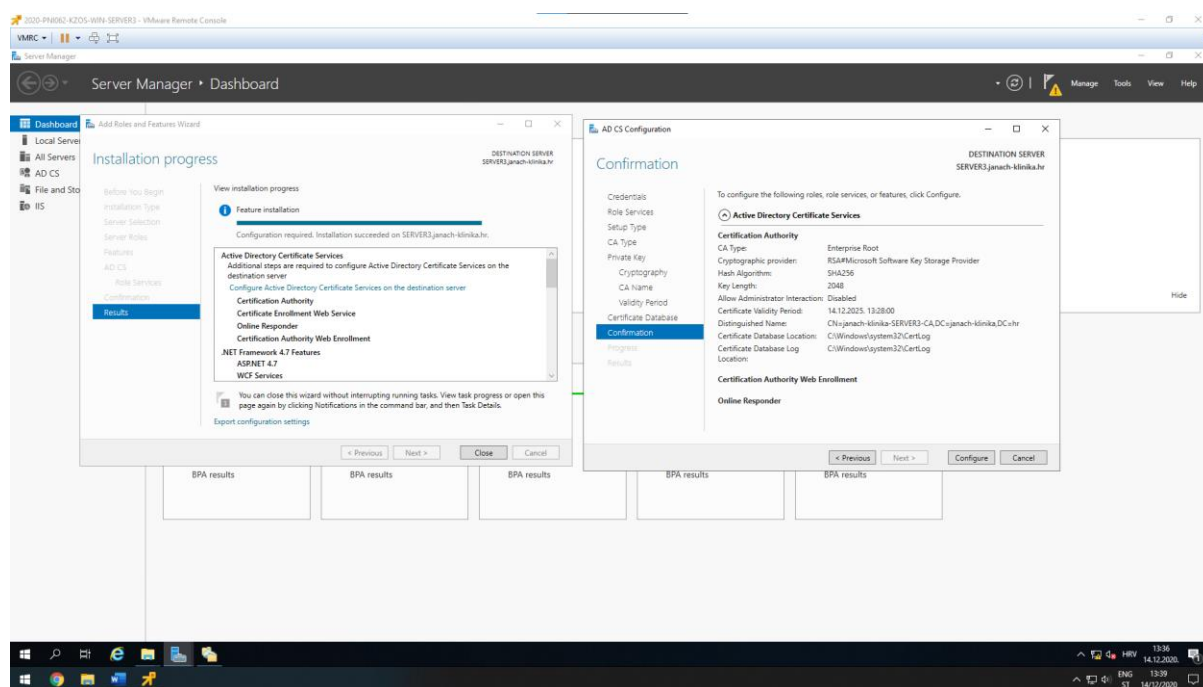
Slika 27: prikaz uspješne funkcionalnosti DFS replikacije između SERVER2 i SERVER3 računala

5.9. CA konfiguracija na SERVER3 poslužitelju

Konfiguracijom Certification Authority poslužitelja omogućiti će se postavljanje SSL/TLS certifikata na poslužitelje na kojima se pokreće web server. Na SERVER3 poslužitelj nužno je instalirati AD CS (Active Directory Certificate Services) ulogu.

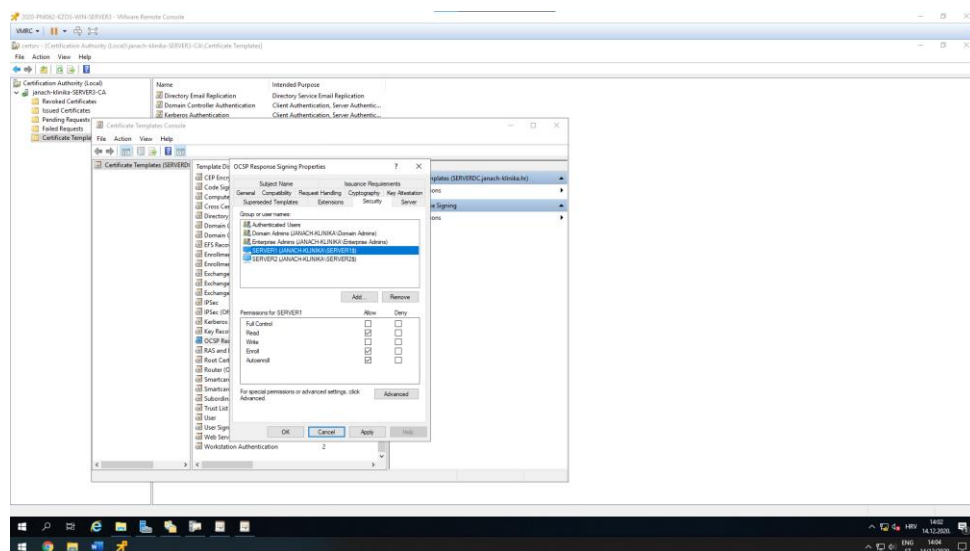
Add roles and Features -> Server roles -> AD CS

Na kartici AD CS, Role Services odabiremo Certification Authority, Certificate Enrollment Web Service, Certification Authority Web Enrollment i Online Responder i na kraju Wizard-a instalirati ulogu. Kad je uloga instalirana od nas se traži konfiguracija Active Directory Certificate Services na poslužitelju. Kredencijali koji će se koristiti će biti od domenskog administratora. Uloge koje će biti konfigurirane i koje treba odabrati na kartici Role Services: Certification Authority, Certification Authority Web Enrollment i Online Responder. Koristiti Enterprise CA zato što se radi o Domeni u kojoj se nalaze računala kojima će se izdavati certifikati. Za tip CA odabrati Root CA. Pošto je cilj kreirati privatni ključ, zato će se odabrati na kartici Private Key -> Create a new private key. Kriptografski provider je RSA#Microsoft Software Key Storage Provider s 2048 duljinom ključa i SHA256 algoritmom. Ostaviti pred definirani Common name (janach-klinika-SERVER3-CA). Također ostaviti default 5 godina validity period ključa. Na kraju Wizarda provjeriti konfiguraciju za kreiranje novog ključa i kliknuti na Configure.



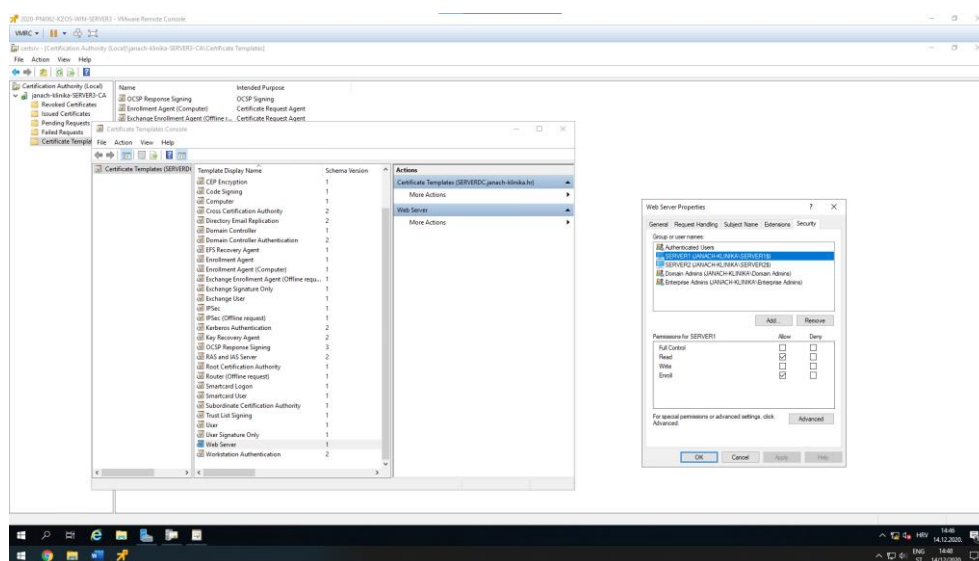
Slika 28: instalacija AD CS uloge i konfiguracija AD CS na poslužitelju

Izvršenom konfiguracijom ADCS na poslužitelj sljedeće što treba je konfigurirati Online Responder. Kreirati certifikat za IIS koji će se kasnije koristiti u konfiguraciji. Kako bi izvršili ovu konfiguraciju potrebno je otvoriti Certification Authority konzolu. Kad otvorimo CA konzolu, unutar nje kad se proširi forest nalazi se 5 mapa. Mapa nad kojom će se vršiti ova konfiguraciju biti će Certificate Templates. Desnim klikom miša na mapu Certificate Templates -> manage. Otvara se Certificate Templates konzola. Certifikat koji treba potražiti je OSCP Response Signing. Desni klik miša na OSCP Response -> properties. Odabrati karticu Security i dodati računala koja će biti IIS web poslužitelji. Poslužitelji koji su dodani pod dozvole staviti Enroll i Autoenroll.



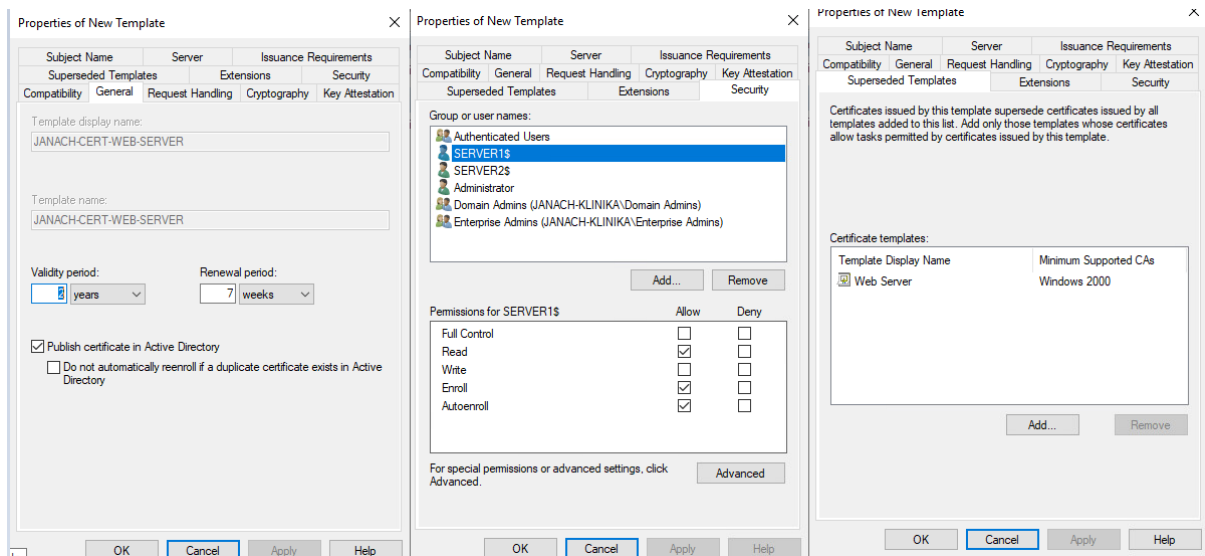
Slika 29: OSCP Response Signing Properties, prikaz dodanih poslužitelja koji će biti web serveri(IIS)

Podešenjem OSCP Response template-a odabiremo ponovno Certificate Templates -> desni klik miša -> odabrati New -> Certificate Template to Issue. Time izdajemo novi certifikat tako da da odaberemo u izborniku OSCP Response Signing i kliknuti OK. Nakon OSCP Response Signing kreiranog certifikata potrebno je kreirati još jedan certifikat za Web poslužitelj(IIS). Ponovno ući u manage konzolu od Certificate Templates i otvoriti properties od Web Server template-a. Odabrati karticu Security i dodati SERVER1 i SERVER2 te im dati dozvolu Enroll.



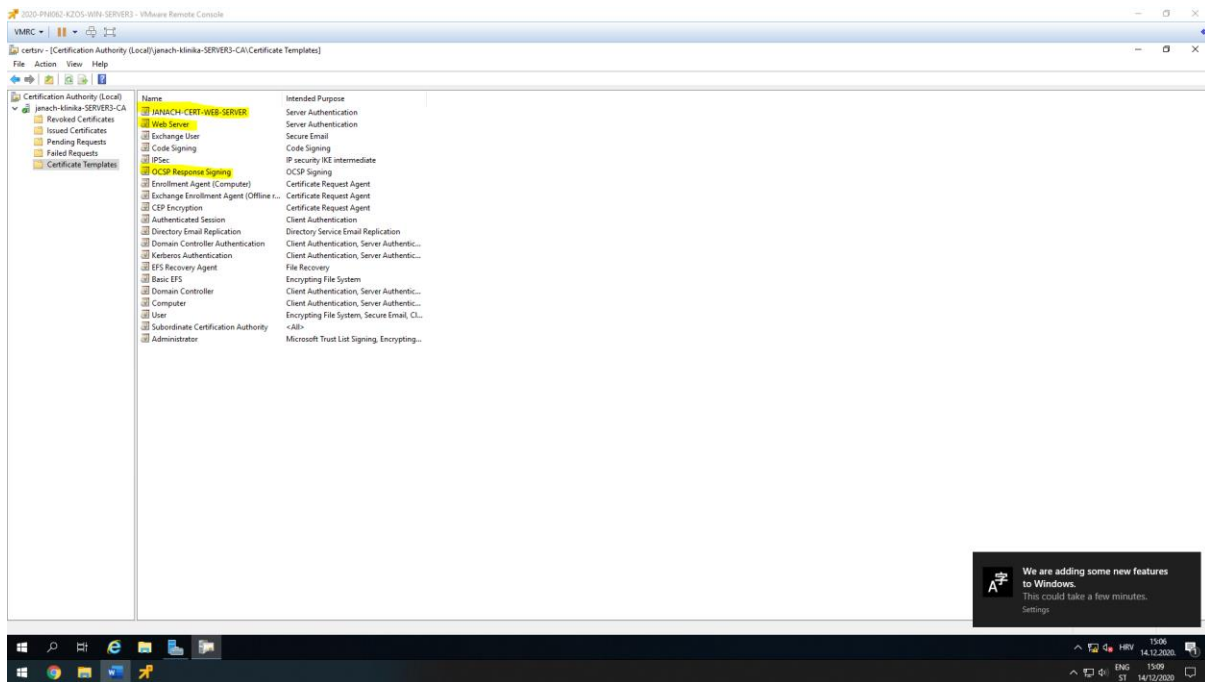
Slika 30: Web Server properties, prikaz dodanih poslužitelja koji će biti web serveri(IIS)

Ponovno treba izdati taj certifikat. Odabrati Certificate Template -> desni klik miša -> New -> Certificate Template to Issue -> Web Server -> OK. Zatim je potrebno duplicirati certifikat Web Server. To radimo u Manage na Certificate Templates. Kad dupliciramo template otvaraju se properties od novog template-a koji je baziran na Web Server Template-u. Dodati naziv template-u i odabrati opciju za objavljivanje certifikata u AD-u. Zatim kliknuti na karticu Security te poslužiteljima SERVER1 i SERVER2 označiti kvačicu na Autoenroll. Na kraju pozicionirati se na karticu Superseded Templates i dodati Web Server template.



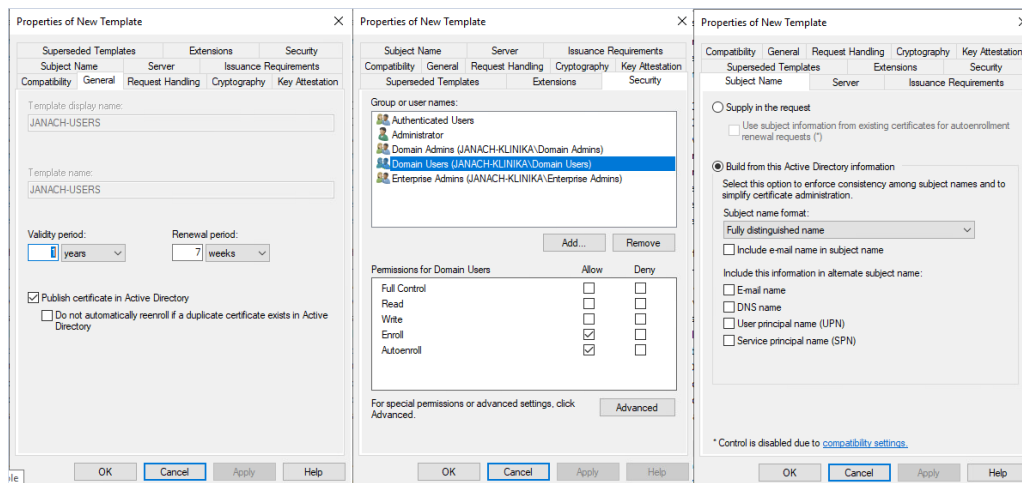
Slika 31: duplicated Web Server template, prikaz General, Security i Superseded setting-a

Dodati novokreirani template certifikata. Odabrati Certificate Template -> desni klik miša -> New -> Certificate Template to Issue -> JANACH-CERT-WEB-SERVER -> OK.



Slika 32: prikaz izdanih certifikata

Konfiguracija automatskog izdavanja certifikata(autoenroll). Odabrali manage na Certificate Templates konzolu i duplicirati User Template. Na kartici general dati ime certifikate template-u(JANACH-USERS). Zatim na kartici Security dodati Domain Users grupu te im za dozvole dati enroll i autoenroll. Zadnje na kartici Subject Name isključiti opciju E-mail name i User Principal Name.



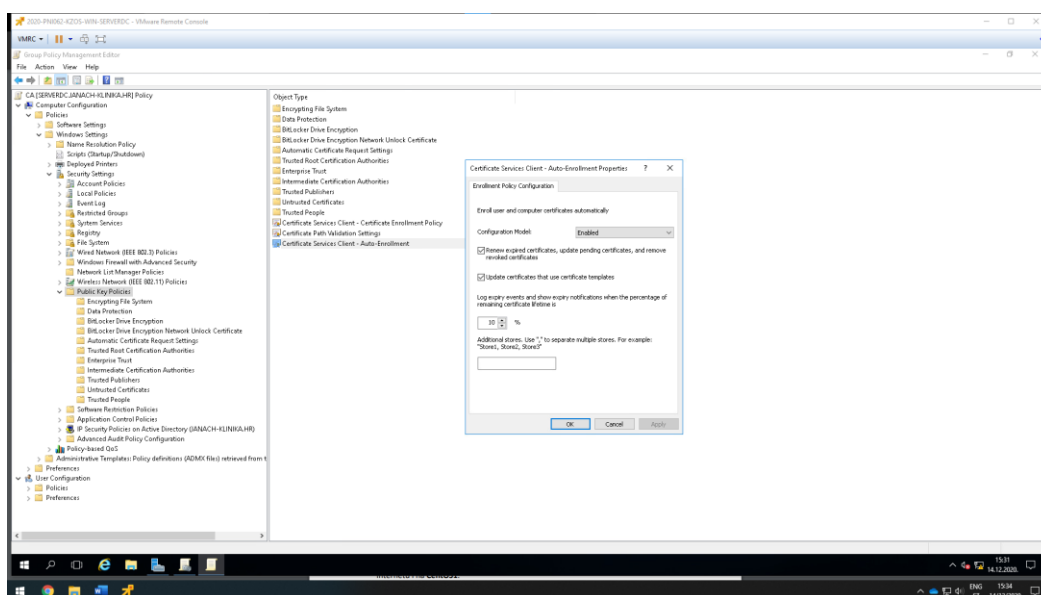
Slika 33: duplicate Users template, prikaz General, Security i Subject Name setting-a

Izdati novo napravljeni template certifikata naziva JANACH-USERS.

I zadnja stvar koju treba podesiti a to je group policy kako bi autoenroll funkcionalno radio. Za to se je potrebno preusmjeriti na SERVERDC poslužitelj i u Server Manager-u otvoriti GPO konzolu i kreirati novi GPO.

Forest: janach-klinika.hr -> Domains -> janach-klinika.hr -> desni klik Create a GPO in this domain.

Imenovati novi GPO CA kad se kreira novi GPO kliknuti na njega i odabrati Edit. Kad se otvori GPO Editor potrebno se pozicionirati u sljedeću putanju: Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Public Key Policies. Na ovoj putanji odabrati stavku Certificate Services Client – Auto-Enrollment. Nakon konfiguracije izvršiti gpupdate/force na svim računalima u domeni.



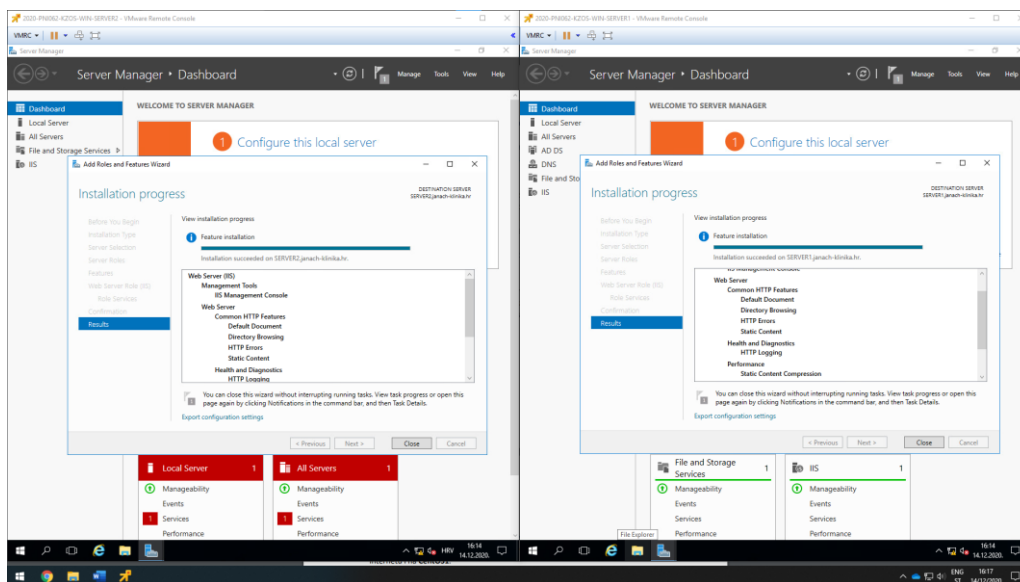
Slika 34: Certificate Services Client – Auto-Enrollment, prikaz konfiguracije nad stavkom, GPO raditi na SERVERDC

5.10. Instalirati IIS na SERVER1 i SERVER2 poslužitelj + SSL/TLS

Uspješnom konfiguracijom CA potrebno je instalirati Web Server(IIS) ulogu na SERVER1 i SERVER2. Instalacija uloge vrši se kroz Server Manager.

Add Roles and Features -> Server roles -> Web Server(IIS)

U kartici Role Services od Web Server Role(IIS) odabrati: Client Certificate Mapping Authentication i IIS Client Certificate Mapping Authentication.

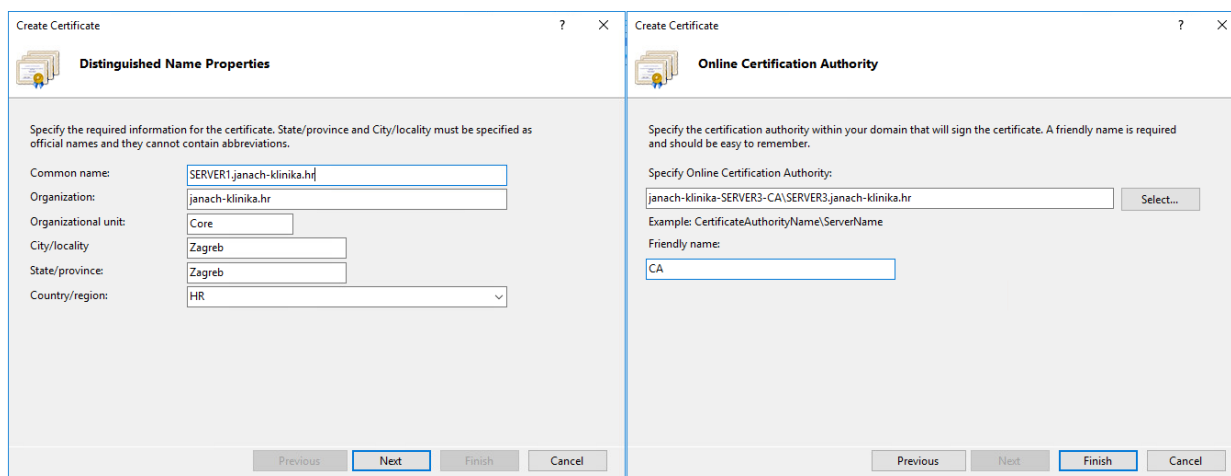


Slika 35: prikaz instalacije Web Server(IIS) uloge

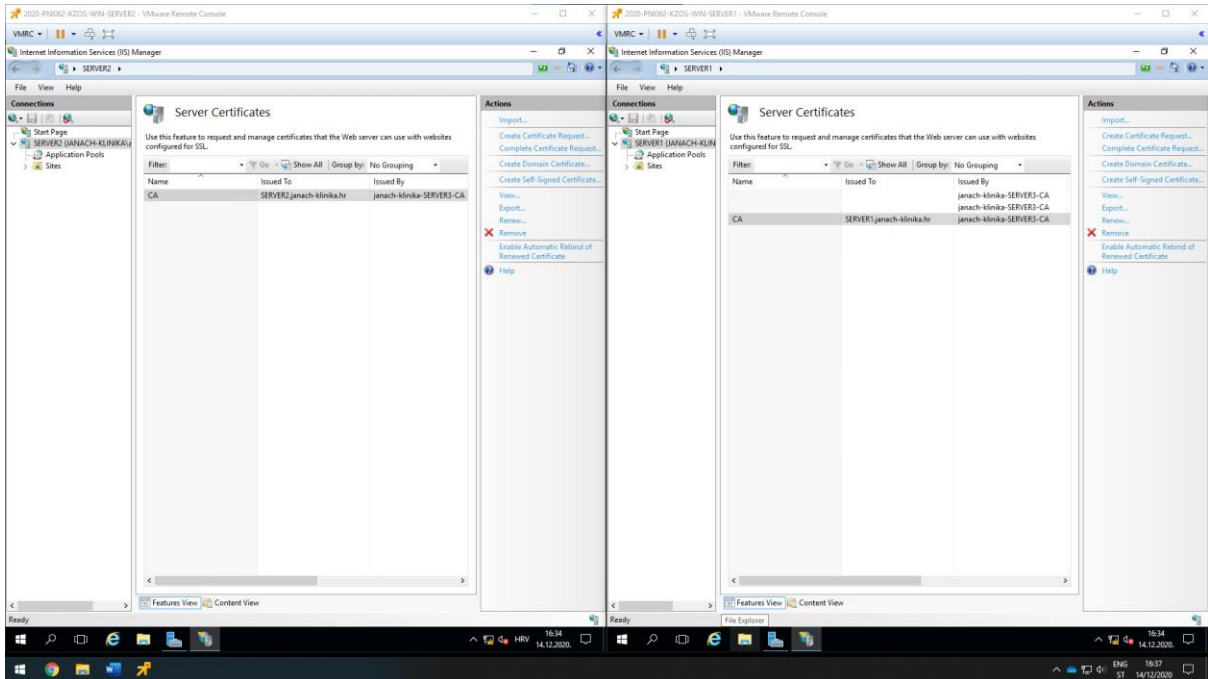
Konfiguracija koja slijedi radi se isto i na jednom i na drugom poslužitelju paralelno.

Nakon instalacije potrebno je otvoriti Internet Information Services (IIS) manager kroz Server Manager konzolu. Kad se otvori IIS konzola potrebno je kreirati novi Domain certifikat.

SERVER1 (JANACH-KLINIKA\Administrator) -> Server Certificate-s -> Create Domain Certificate

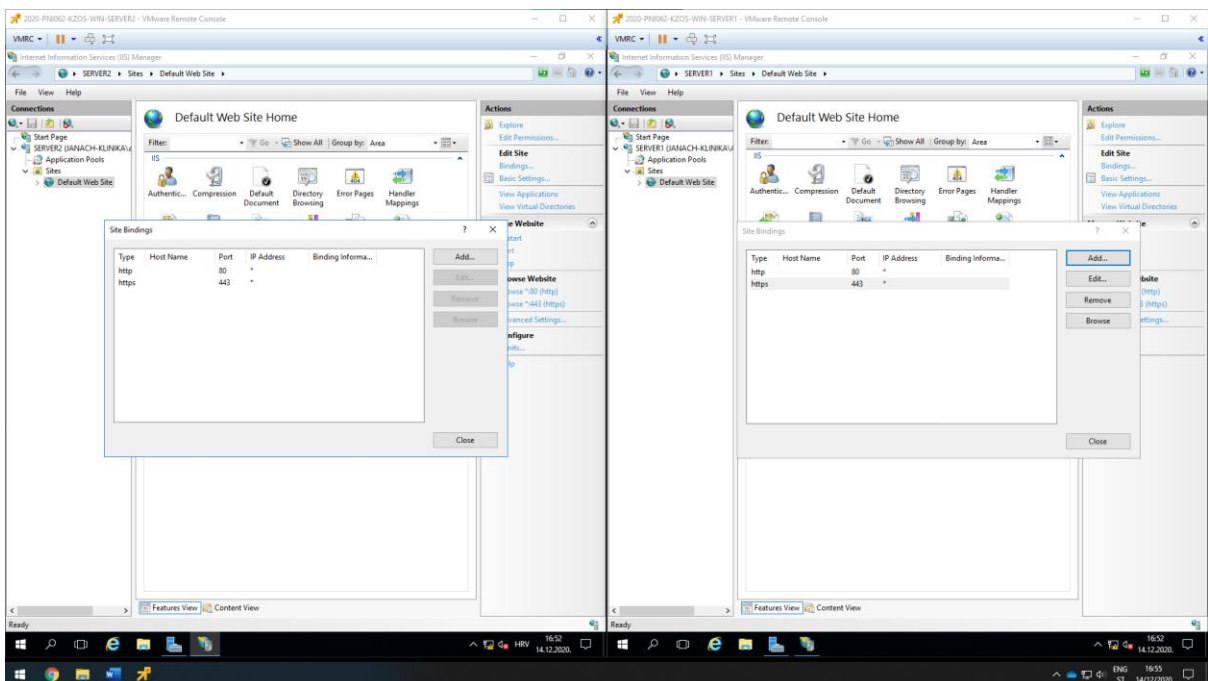


Slika 36: prikaz setting-a kreiranja Domain certifikata(Vrijedi i za SERVER1 i SERVER2 poslužitelj, friendly name zamijeniti s drugim imenom SERVERX-CERT



Slika 37: prikaz dodanih certifikata na SERVER1 i SERVER2 poslužitelju

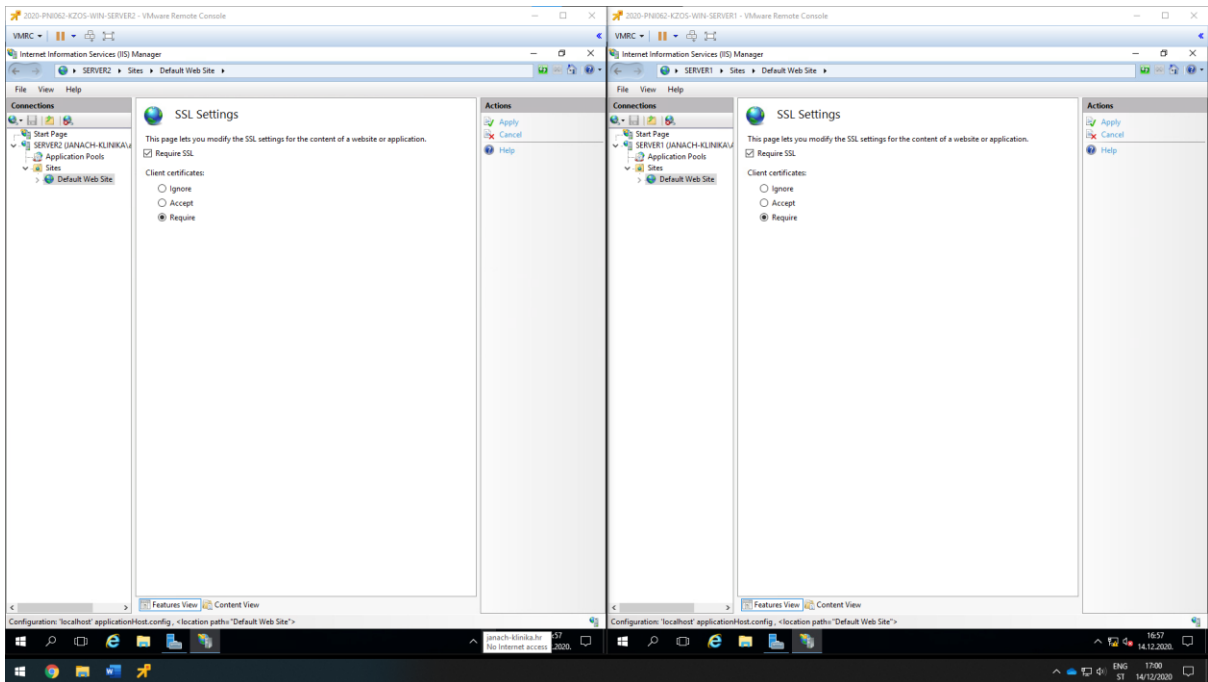
Nakon toga pozicionirati se u Default Web Site. Odabrati iz izbornika Default Web Site i s desne strane kliknuti na Bindings i tamo dodati HTTPS protokol koji radi na TCP portu 443 i za taj binding dodati prethodno kreirani certifikat.



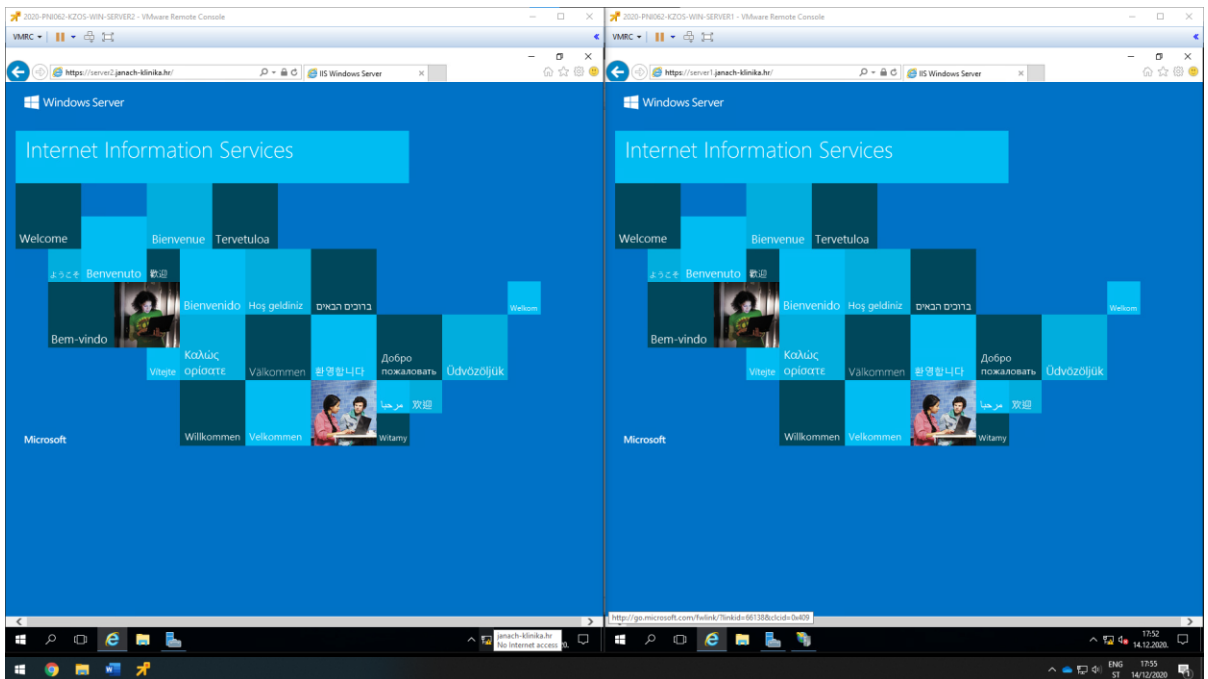
Slika 38: Prikaz konfiguracije Default Web Site, Site bindings

Dodatnu provjeru izvršiti na svim ostalim poslužiteljima i klijentskom računalu. S moje strane provjerio sam i sve radi.

I zadnje što je potrebno da bi SSL bio funkcionalan a to je da za Defaultni Web Site treba postaviti da automatski prihvaća SSL certifikat.



Slika 39: Default Web Site, Accept SSL



Slika 40: Dokaz da SSL certifikat funkcionalno radi

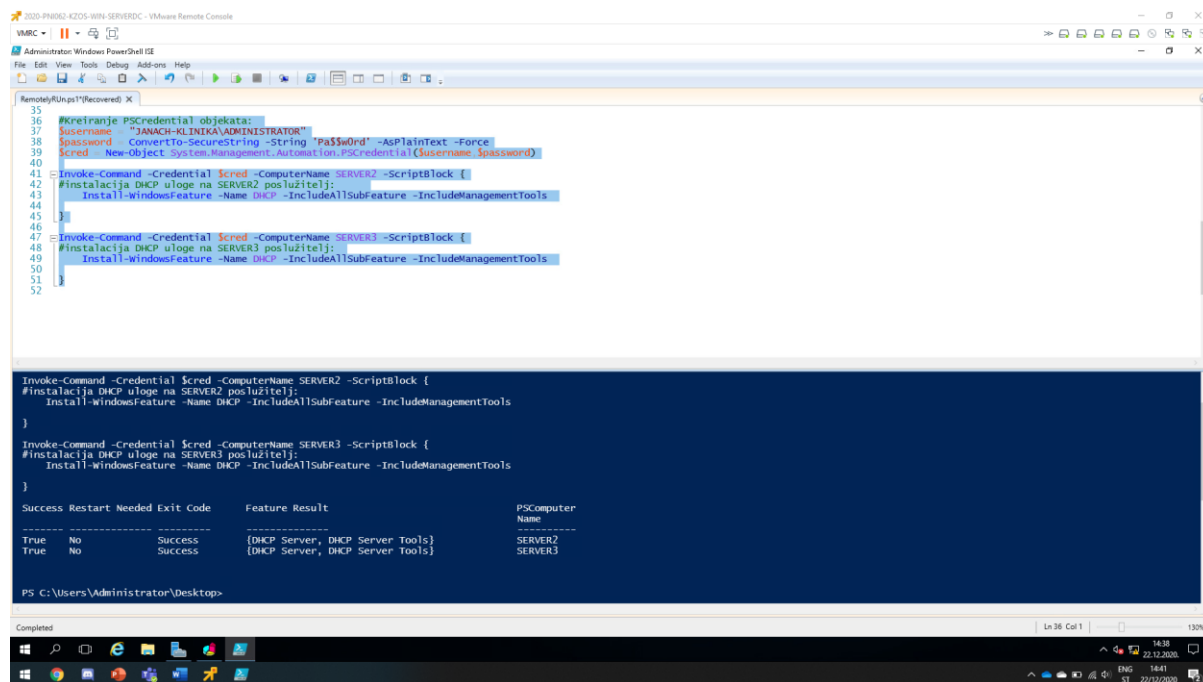
5.11. Konfiguracija DHCP-a na SERVER2 i SERVER3

DHCP služi automatiziranoj dodjeli IP postavki računalima na IP mreži. Te postavke, osim IP adrese i mrežne maske, uključuju zadani usmjernik(eng. Default Gateway) i adresu DNS poslužitelja. Cilj konfiguracije DHCP-a je instalirati DHCP ulogu na SERVER2 i SERVER3 poslužitelj. DHCP instalirati pomoću PowerShell skripte koja se pokreće remotely sa SERVERDC poslužitelja.

```
#kreiranje PSCredential objekata:
$username = "JANACH-KLINIKA\ADMINISTRATOR"
$password = ConvertTo-SecureString -String 'Pa$$w0rd' -AsPlainText -Force
$cred = New-Object System.Management.Automation.PSCredential($username,$password)

Invoke-Command -Credential $cred -ComputerName SERVER2 -ScriptBlock {
#instalacije NLB uloge na SERVER2 poslužitelj:
    Install-WindowsFeature DHCP -IncludeAllSubFeature -IncludeManagementTools
}

Invoke-Command -Credential $cred -ComputerName SERVER3 -ScriptBlock {
#instalacije NLB uloge na SERVER3 poslužitelj:
    Install-WindowsFeature DHCP -IncludeAllSubFeature -IncludeManagementTools
}
```



```
35
36 #kreiranje PSCredential objekata:
37 $username = "JANACH-KLINIKA\ADMINISTRATOR"
38 $password = ConvertTo-SecureString -String 'Pa$$w0rd' -AsPlainText -Force
39 $cred = New-Object System.Management.Automation.PSCredential($username,$password)
40
41 Invoke-Command -Credential $cred -ComputerName SERVER2 -ScriptBlock {
42 #instalacija DHCP uloge na SERVER2 poslužitelj:
43     Install-WindowsFeature -Name DHCP -IncludeAllSubFeature -IncludeManagementTools
44 }
45
46
47 Invoke-Command -Credential $cred -ComputerName SERVER3 -ScriptBlock {
48 #instalacija DHCP uloge na SERVER3 poslužitelj:
49     Install-WindowsFeature -Name DHCP -IncludeAllSubFeature -IncludeManagementTools
50 }
51
52

Invoke-Command -Credential $cred -ComputerName SERVER2 -ScriptBlock {
#instalacija DHCP uloge na SERVER2 poslužitelj:
    Install-WindowsFeature -Name DHCP -IncludeAllSubFeature -IncludeManagementTools
}

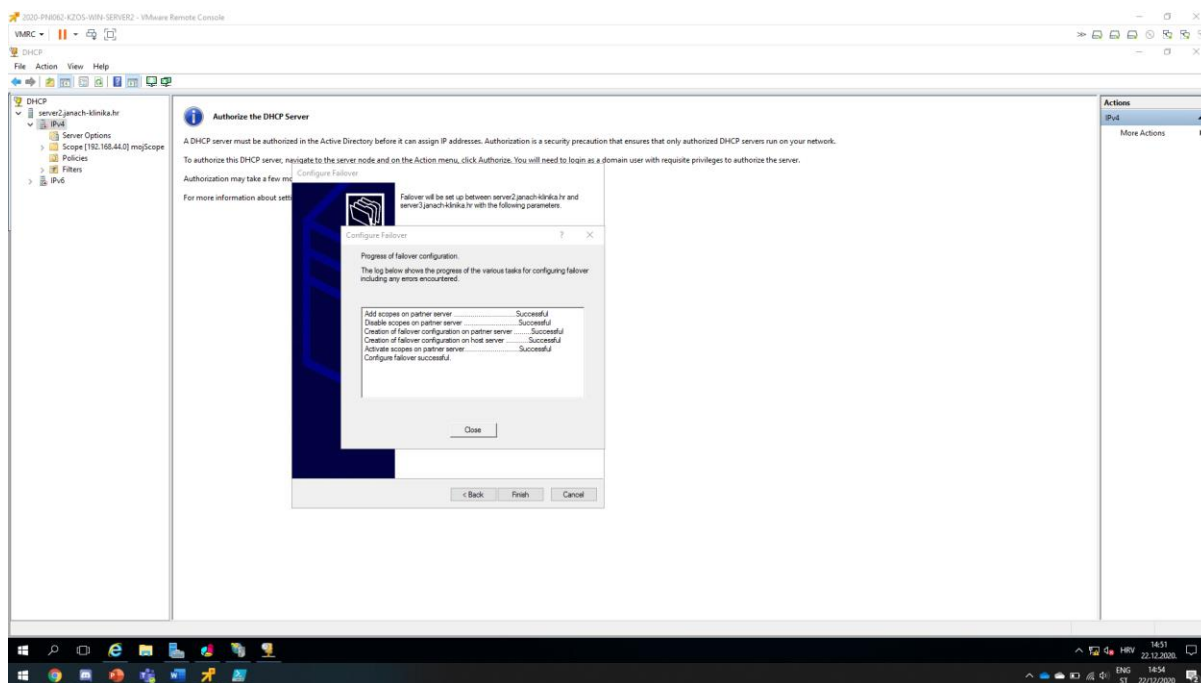
Invoke-Command -Credential $cred -ComputerName SERVER3 -ScriptBlock {
#instalacija DHCP uloge na SERVER3 poslužitelj:
    Install-WindowsFeature -Name DHCP -IncludeAllSubFeature -IncludeManagementTools
}

-----
Success Restart Needed Exit Code      Feature Result
-----
True      No          Success      [DHCP Server, DHCP Server Tools]
True      No          Success      [DHCP Server, DHCP Server Tools]
-----
PSComputer
Name
-----
SERVER2
SERVER3

PS C:\Users\Administrator\Desktop>
```

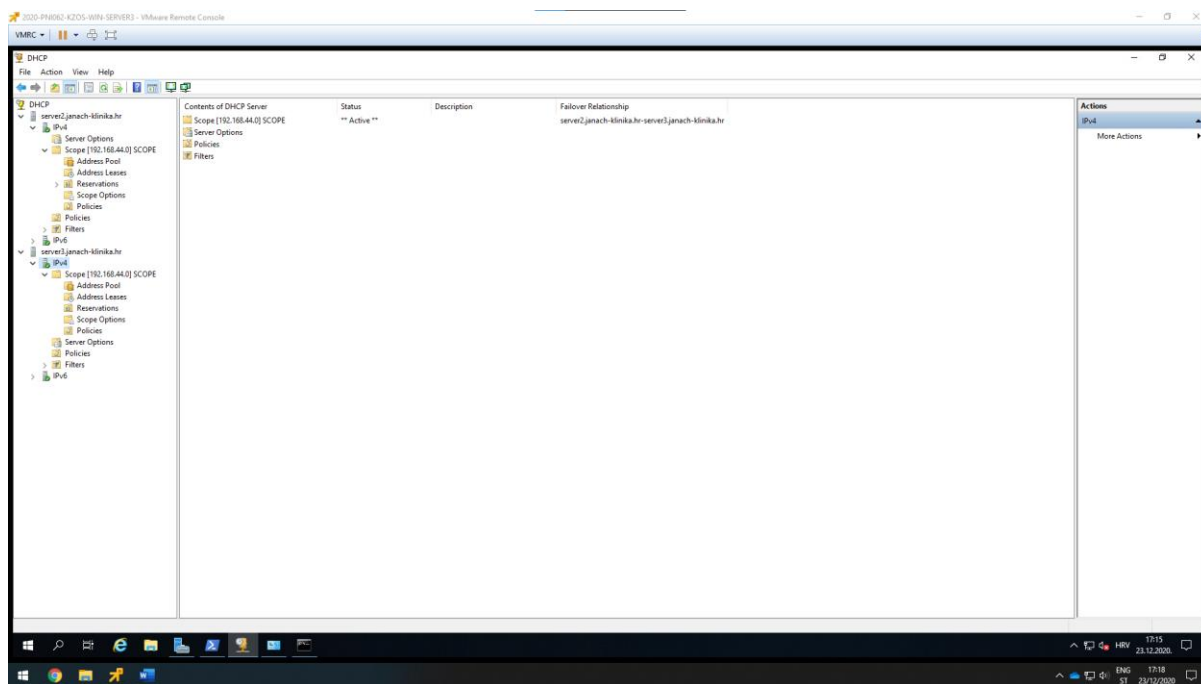
Slika 41: prikaz instalacije DHCP uloge na SERVER1 i SERVER2 poslužitelj

Kad je instalirana DHCP rola potrebno je pokrenuti DHCP management konzolu i kreirati novi scope subnet-a 192.168.44.0/24. Nakon kreiranog scope-a potrebno je konfigurirati failover i autorizirati DHCP Server desnim klikom na FQDN -> Authorize.



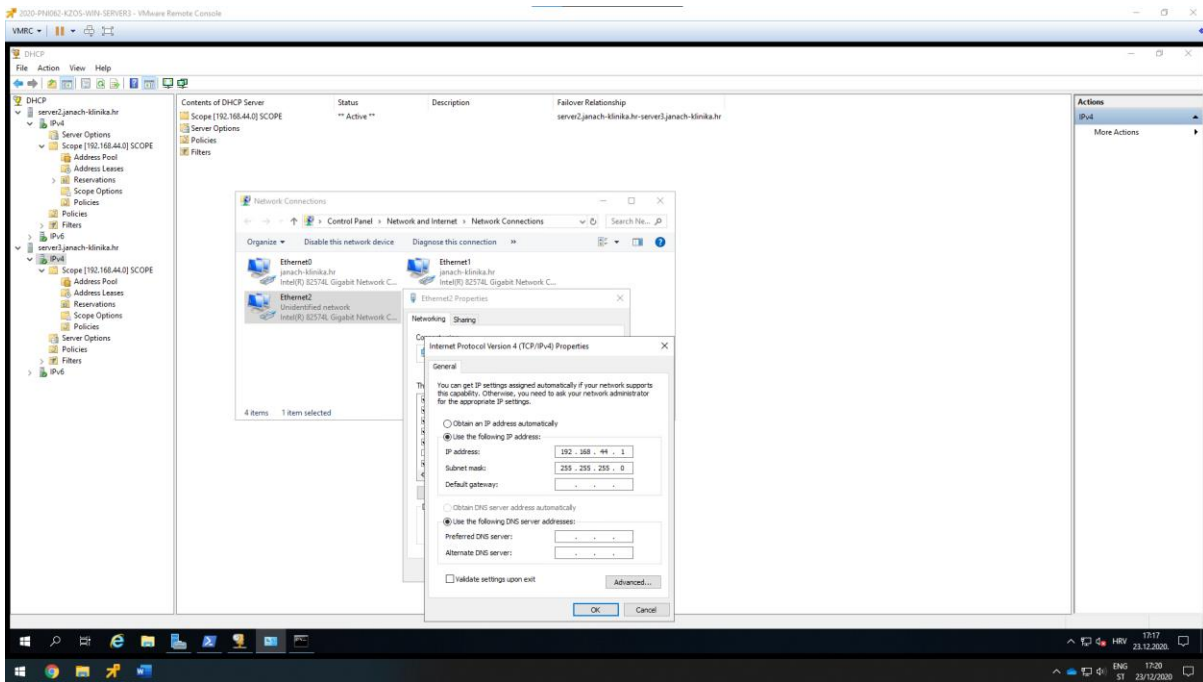
Slika 42: prikaz kreiranog scope-a i konfiguriranog failover-a

Zatim dodati drugo računalo(SERVER2 poslužitelj) u DHCP management konzolu(Cluster).



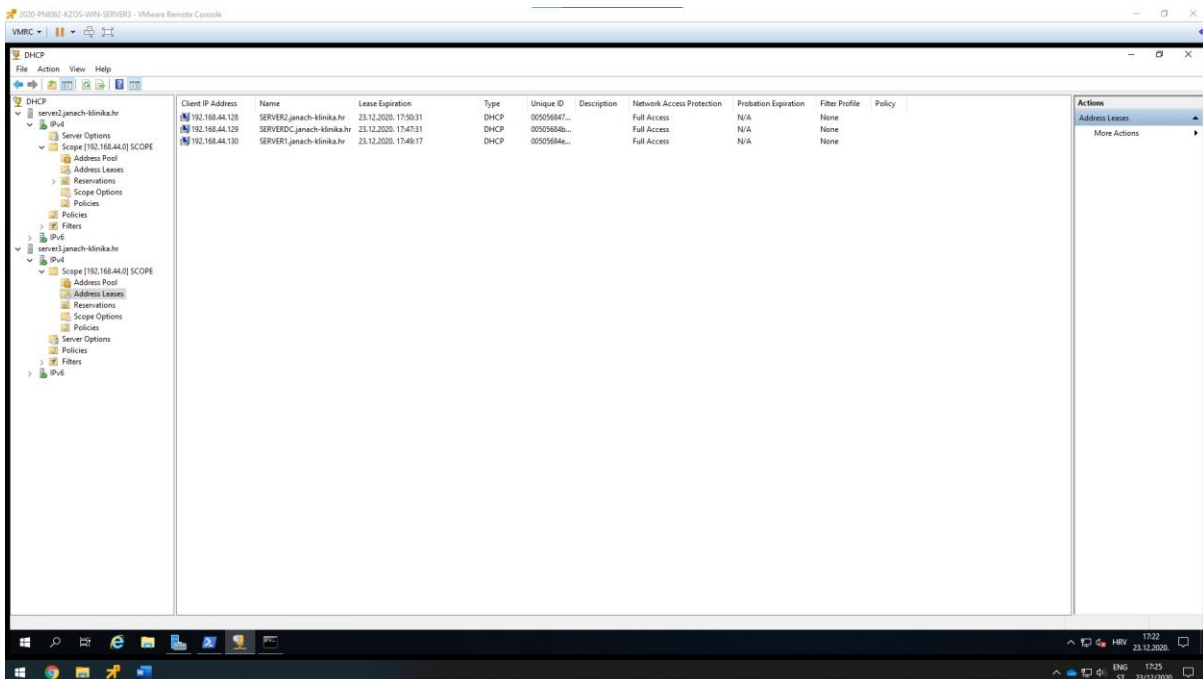
Slika 43: prikaz dodanog SERVER2 poslužitelja

Sad je sve spremno za dodjelu IP adresa mrežnim adapterima na računalima koja su u domeni, no prije toga potrebno je podesiti IP adresu na drugome mrežnome adapteru kako bi ostalima računalima bila dodjeljena IP adresa. Treći mrežni adapter je potrebno priključiti na sve virtualne mašine koje su u domeni koristeći vSphere.



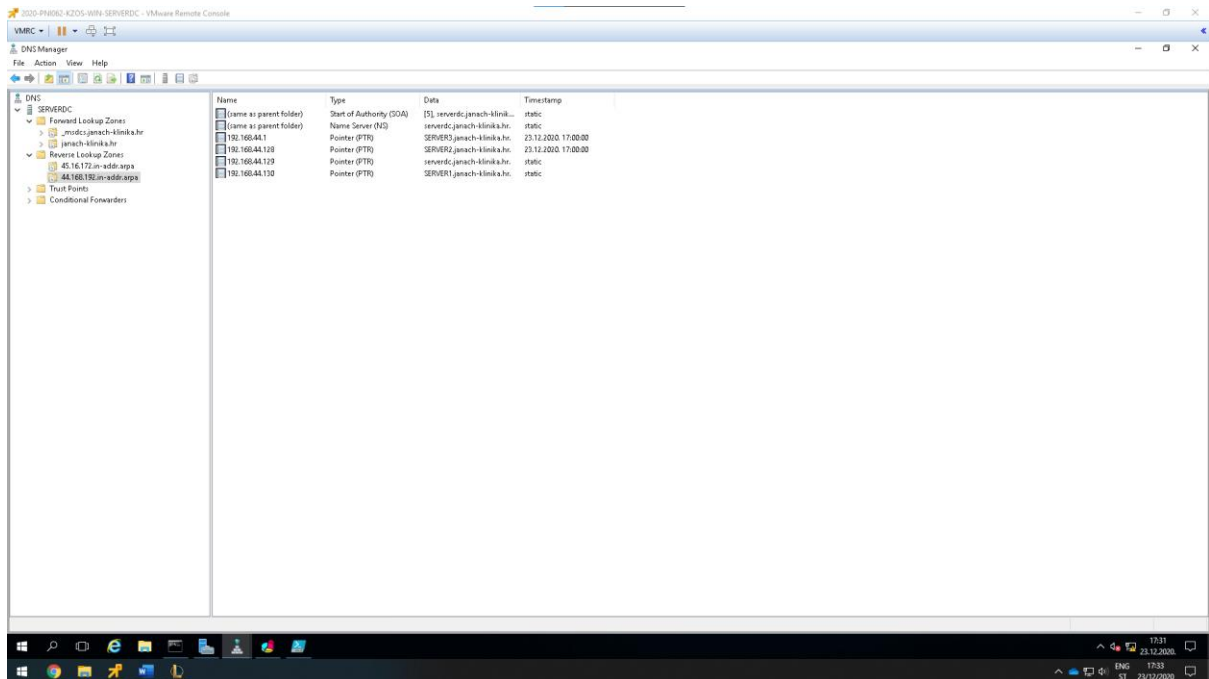
Slika 44: prikaz konfiguracije 3. mrežnog adaptera na SERVER3 poslužitelju kako bi IP adrese mogle biti dodijeljene ostalim računalima

Treći mrežni adapter koji se nalazim na SERVER2, SERVER1, SERVERDC i CLI računalu postaviti na opciju obtain an IP address automatically.



Slika 45: prikaz adresa koje su dodijeljene računalima

Kad su adrese dodijele potrebno je otvoriti DNS management konzolu na SERVERDC poslužitelju i kreirati reverznu zonu za subnet 192.168.44.0/24.



Slika 46: prikaz kreirane reverzne zone i dodanih PTR-a

5.12. Konfiguracija NLB uloge

Primarna uloga NLB-a je učinkovito balansirati veću količinu prometa (zahtjeva) koje korisnici generiraju pristupom na mrežne servise. Primjerice, ako poslovanje ima internetsku stranicu čiji se promet naglo povećao, web poslužitelj mogao bi se preopteretiti, čime padaju i njegove performanse. U ekstremnom slučaju, čak i sam web poslužitelj može prestati raditi. Kako bi se ovaj problem riješio, može se dodati još jedan web poslužitelj koji opslužuje isti sajt. No postavlja se jedno pitanje a to je kako biti siguran da će se ulazni promet jednako raspodijeliti na oba poslužitelja? Jedino moguće rješenje je NLB.

NLB klaster je logički subjekt vlastitog imena i IP adrese. Klijenti se povezuju s klasterom, a ne pojedinačnim računalima, a klaster raspodjeljuje ulazne zahtjeve u jednakoj mjeri među svojim poslužiteljima. S obzirom na to da svi poslužitelji NLB klastera mogu istovremeno aktivno uslužiti klijente, ova vrsta klastera nije odgovarajuća za aplikacije baza podataka i e-maila. Te aplikacije zahtijevaju isključiv pristup spremištu podataka. NLB je prikladniji za aplikacije koje imaju vlastita spremišta podataka, poput web poslužitelja.

Nakon izrade NLB klastera, klasteru se mogu dodati poslužitelji pomoću Network Load Balancing Manager-a. Kako se dodaju poslužitelji, servis NLB ih automatski inkorporira u klaster. No prije nego što se poslužitelji dodaju u klaster NLB uloga treba biti instalirana na svakog od njih.

Pošto je prethodno u projektu instalirani web server(IIS) s funkcionalnim SSL certifikatom koji učitava https web sajt na SERVER1 i SERVER2 poslužitelju. Sad je potrebno konfigurirati funkcionalni NLB.

Opis infrastrukture koja se želi postići:

SERVERDC: instalirana NLB uloga, te će se nad SERVERDC poslužiteljem kreirati klaster i dodavati ostali hostovi.

SERVER1: instalirana NLB uloga, SERVER1 poslužitelj bit će dodan u klaster koji je kreiran na SERVERDC poslužitelju.

SERVER2: instalirana NLB uloga, SERVER2 poslužitelj bit će dodan u klaster koji je kreiran na SERVERDC poslužitelju.

Instalacije NLB uloge PowerShell skriptom na sva tri poslužitelja:

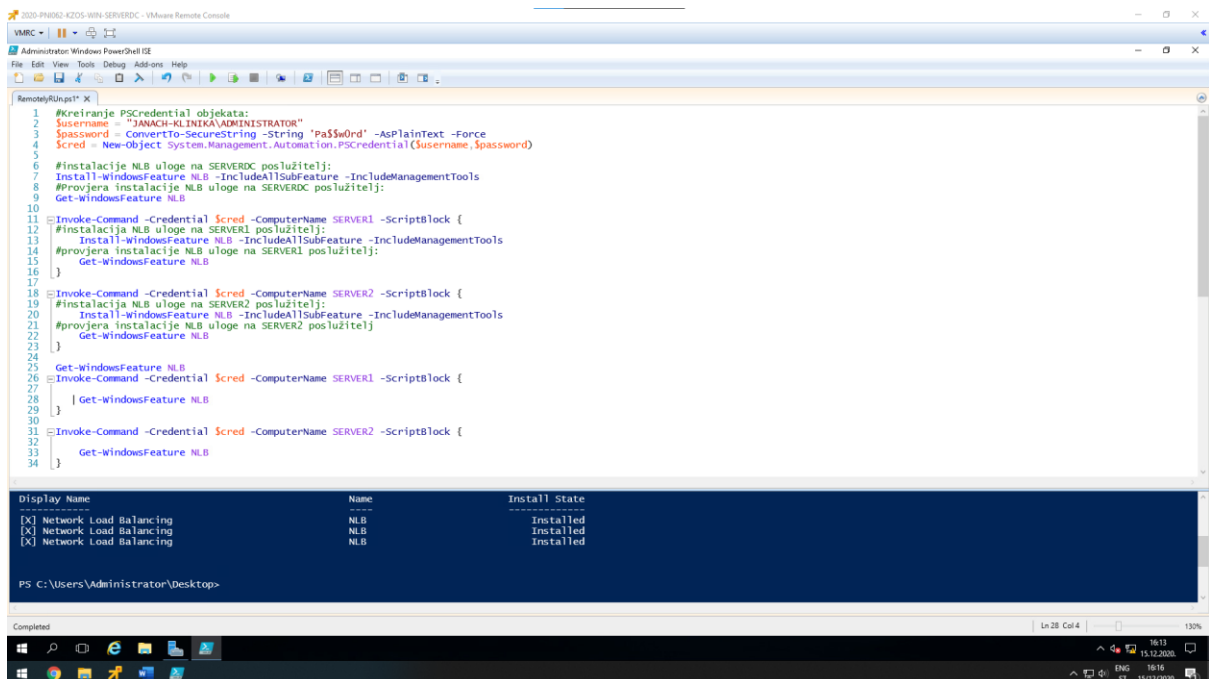
```
#kreiranje PScredential objekata:
$username = "JANACH-KLINIKA\ADMINISTRATOR"
$password = ConvertTo-SecureString -String 'Pa$$w0rd' -AsPlainText -Force
$cred = New-Object System.Management.Automation.PSCredential($username,$password)

#instalacije NLB uloge na SERVERDC poslužitelj:
Install-WindowsFeature NLB -InsluceAllSubFeature -IncludeManagementTools
#provjera instalacije NLB uloge na SERVERDC poslužitelj:
Get-WindowsFeature NLB

Invoke-Command -Credential $cred -ComputerName SERVER1 -ScriptBlock {
#instalacije NLB uloge na SERVER1 poslužitelj:
    Install-WindowsFeature NLB -InsluceAllSubFeature -IncludeManagementTools
#provjera instalacije NLB uloge na SERVER1 poslužitelj:
    Get-WindowsFeature NLB
}

Invoke-Command -Credential $cred -ComputerName SERVER2 -ScriptBlock {
#instalacije NLB uloge na SERVER2 poslužitelj:
    Install-WindowsFeature NLB -InsluceAllSubFeature -IncludeManagementTools
#provjera instalacije NLB uloge na SERVER2 poslužitelj:
    Get-WindowsFeature NLB
}

Get-WindowsFeature NLB
Invoke-Command -Credential $cred -ComputerName SERVER2 -ScriptBlock {
    Get-WindowsFeature NLB
}
}
Invoke-Command -Credential $cred -ComputerName SERVER2 -ScriptBlock {
    Get-WindowsFeature NLB
}
}
```



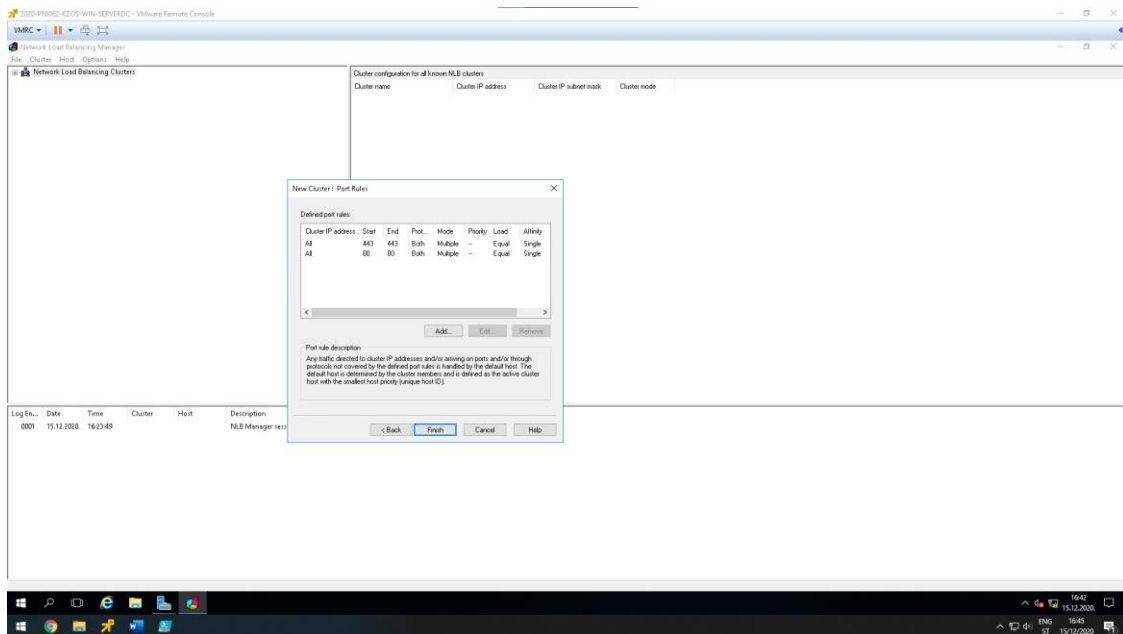
```
1 #kreiranje PScredential objekata:
2 $username = "JANACH-KLINIKA\ADMINISTRATOR"
3 $password = ConvertTo-SecureString -String 'Pa$$w0rd' -AsPlainText -Force
4 $cred = New-Object System.Management.Automation.PSCredential($username,$password)
5
6 #instalacije NLB uloge na SERVERDC poslužitelj:
7 Install-WindowsFeature NLB -IncludeAllSubFeature -IncludeManagementTools
8 #provjera instalacije NLB uloge na SERVERDC poslužitelj:
9 Get-WindowsFeature NLB
10
11
12 Invoke-Command -Credential $cred -ComputerName SERVER1 -ScriptBlock {
13 #instalacije NLB uloge na SERVER1 poslužitelj:
14     Install-WindowsFeature NLB -IncludeAllSubFeature -IncludeManagementTools
15 #provjera instalacije NLB uloge na SERVER1 poslužitelj:
16     Get-WindowsFeature NLB
17 }
18
19 Invoke-Command -Credential $cred -ComputerName SERVER2 -ScriptBlock {
20 #instalacije NLB uloge na SERVER2 poslužitelj:
21     Install-WindowsFeature NLB -IncludeAllSubFeature -IncludeManagementTools
22 #provjera instalacije NLB uloge na SERVER2 poslužitelj:
23     Get-WindowsFeature NLB
24 }
25
26 Get-WindowsFeature NLB
27
28 Invoke-Command -Credential $cred -ComputerName SERVER1 -ScriptBlock {
29     Get-WindowsFeature NLB
30 }
31
32 Invoke-Command -Credential $cred -ComputerName SERVER2 -ScriptBlock {
33     Get-WindowsFeature NLB
34 }
```

| Display Name | Name | Install State |
|----------------------------|------|---------------|
| [X] Network Load Balancing | NLB | Installed |
| [X] Network Load Balancing | NLB | Installed |
| [X] Network Load Balancing | NLB | Installed |

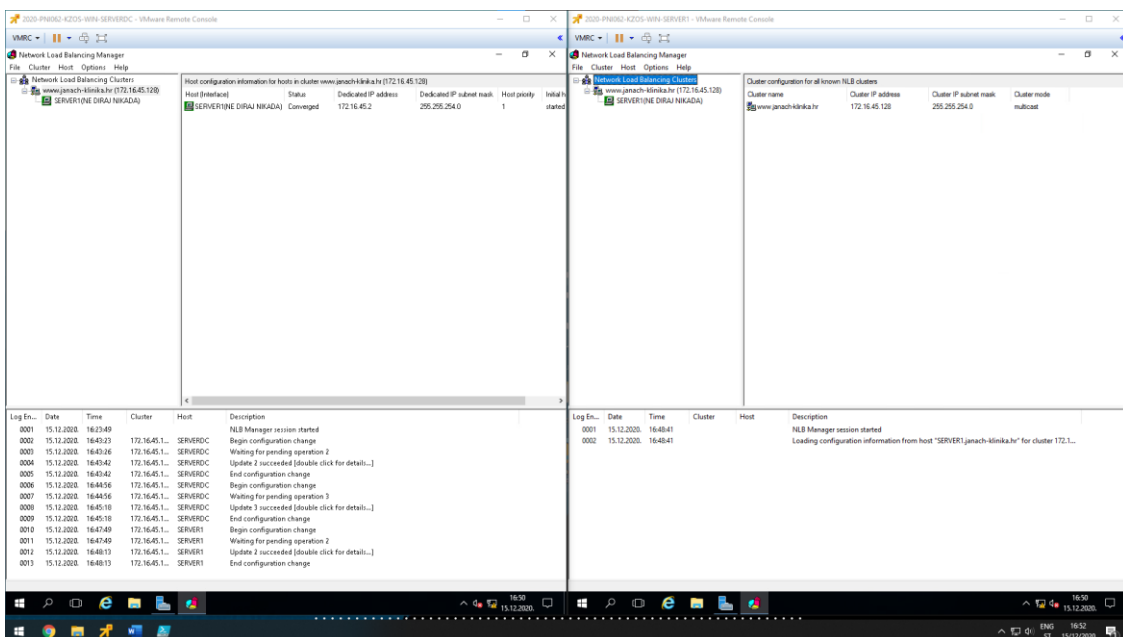
PS C:\Users\Administrator\Desktop>

Slika 47: prikaz instalacije NLB uloge s PowerShell skriptom

Kad je NLB uloga instalirana može se organizirati klaster. Klaster se konfigurira na SERVERDC poslužitelju tako da se pokrene Network Load Balancing Manager. U desnom dijelu NLB manager-a desnim klikom miša na Network Load Balancing Clusters -> New Cluster. Otvara se Wizard za kreiranje novog klastera. U polje host upisati ime poslužitelja nad kojim će se vršiti load balancing i u popisu mrežnih adaptera dodati domenski LAN mrežni adapter. New Cluster: Host Parameters ostaviti defaultne vrijednosti. New Cluster: Cluster IP Addresses dodati IP adresu klastera(Ona koja se ne koristi). New Cluster: Cluster Parameters postaviti Full Internet Name na www.janach-klinika.hr i operacijski mod klastera na multicast. New Cluster: izbrisati sva pravila i dodati nova za port 80 http(BOTH) i port 443 za https(BOTH).

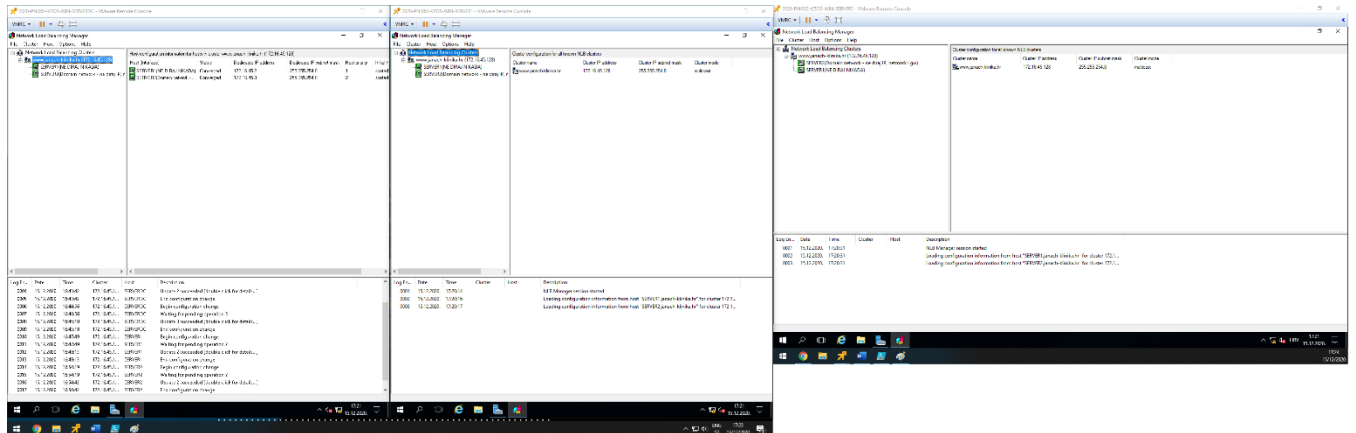


Slika 48: filtriranje portova

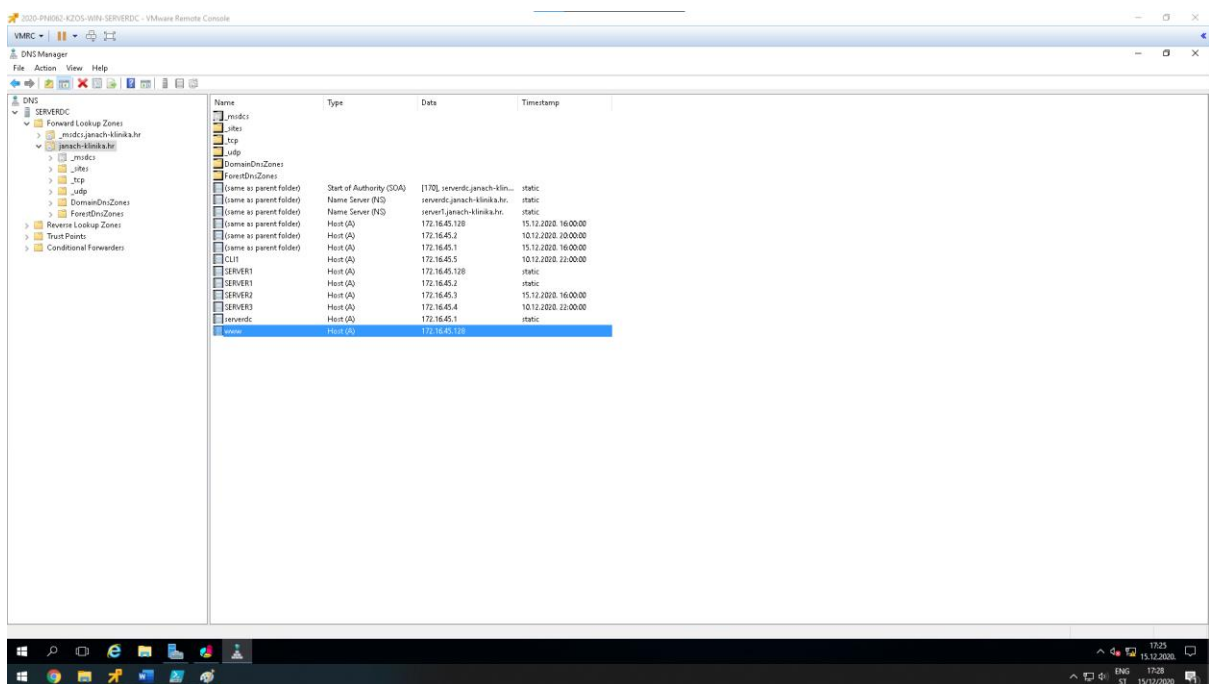


Slika 49: dodan je host(SERVER1) u klaster

Dodan je klaster i host u klaster, sad je potrebno dodati drugi host a to je SERVER2. Dodajemo da se desnim klikom miša klikne na klaster i odabere Add Host to Cluster. Otvara se Wizard Add Host to Cluster: Connect u polje host upisati drugi host koji se dodaje u ovom slučaju SERVER2 te iz izbornika mrežnih adaptera odabere domenski mrežni adapter. Add Host to Cluster: Host Parameters ostaviti default-no. I pravila filtriranja portova su već prethodno podešena kad se je dodavao prvi host.

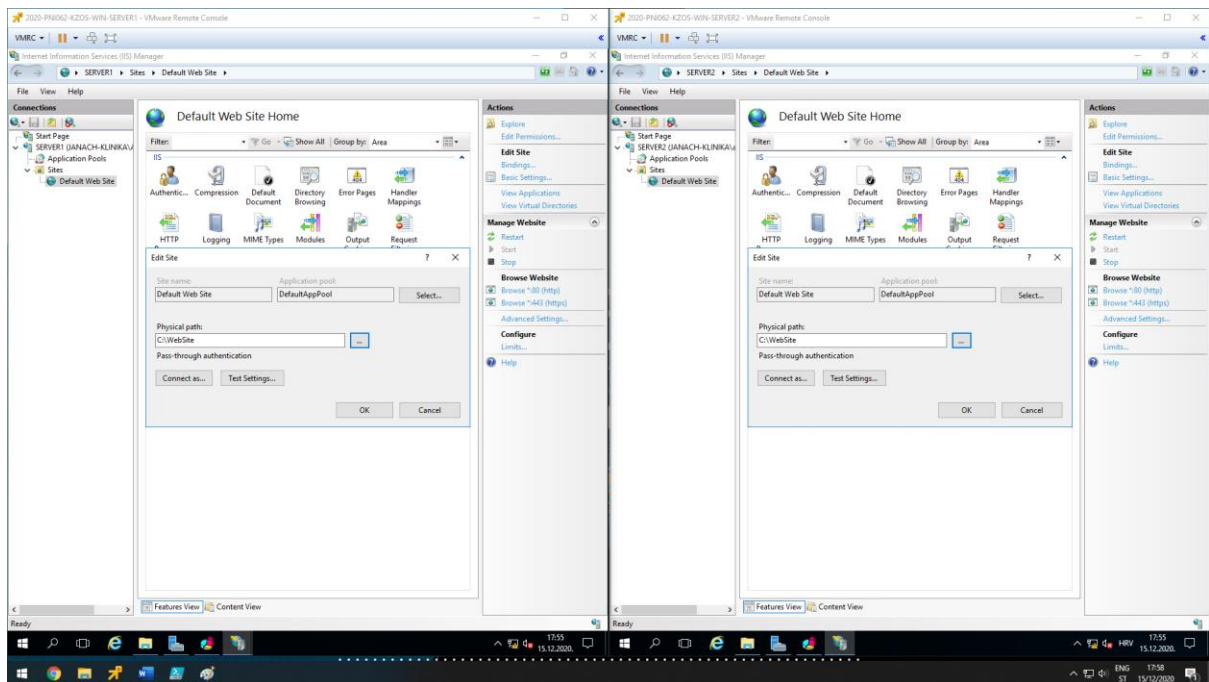


Slika 50: Prikaz kreiranog klastera i dodanih hostova SERVER1 i SERVER2



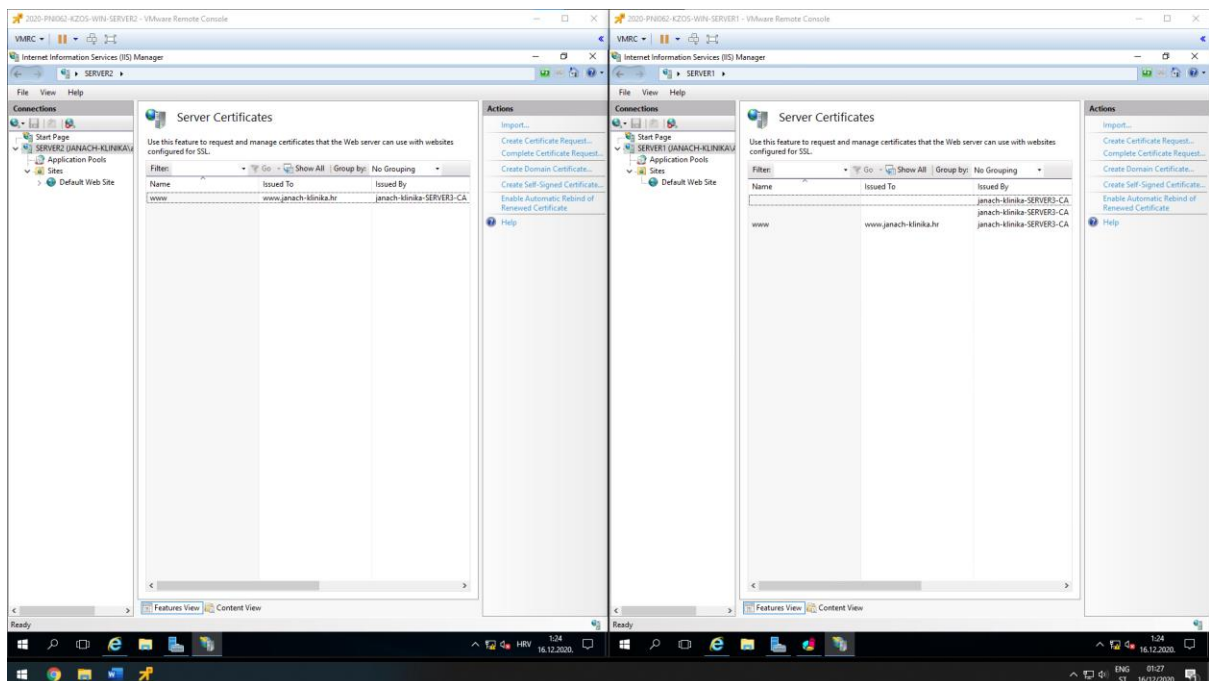
Slika 51: dodan DNS zapis klastera www

Provjera funkcionalnosti s računala CLI1. Tako da se na CLI1 računalu pokrene Internet Explorer i upiše www.racunarstvo.edu (ime klastera). No prije toga kad imamo dva IIS poslužitelja potrebno je napraviti i različite web stranice. Na SERVER1 i SERVER2 potrebno je kreirati website na putanji C:\WebSite\default.htm. Te taj novo kreirani vebsajt postaviti kao početnu stranicu IIS-a.

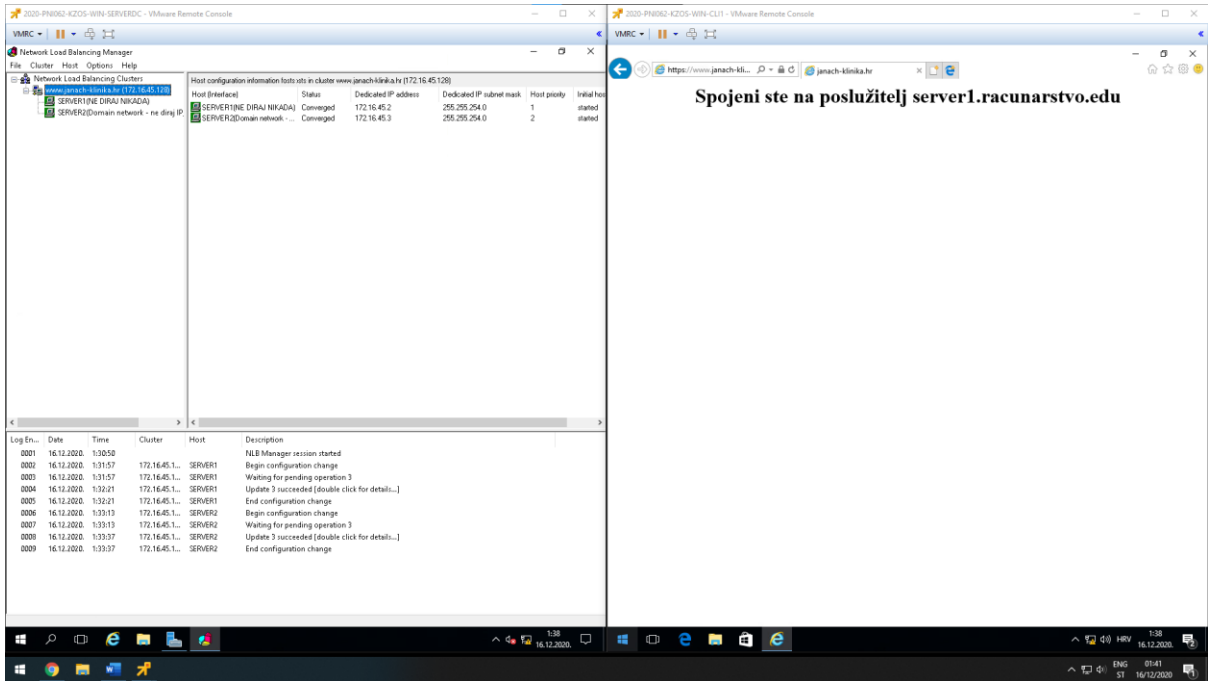


Slika 52: postavljanje novokreirane datoteke kao početnu stranicu IIS-a

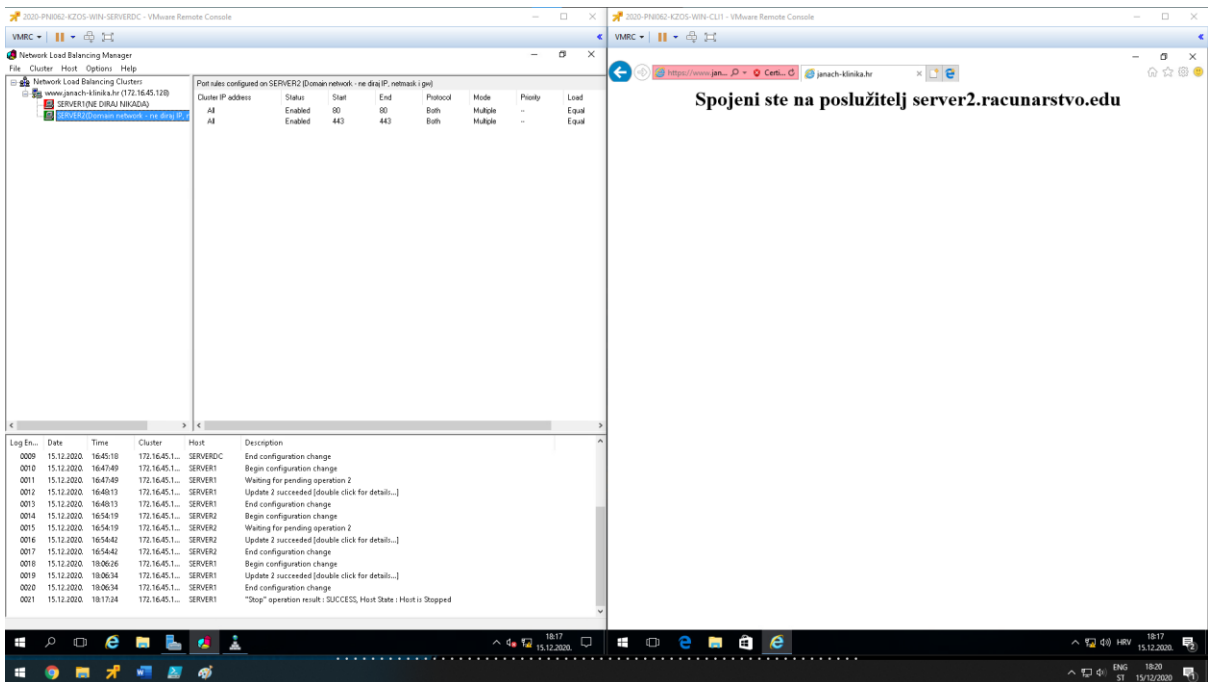
Kad je kreiran website potrebno je kreirati za taj website certifikat.



Slika 53: kreirani certifikati za www.janach-klinika.hr



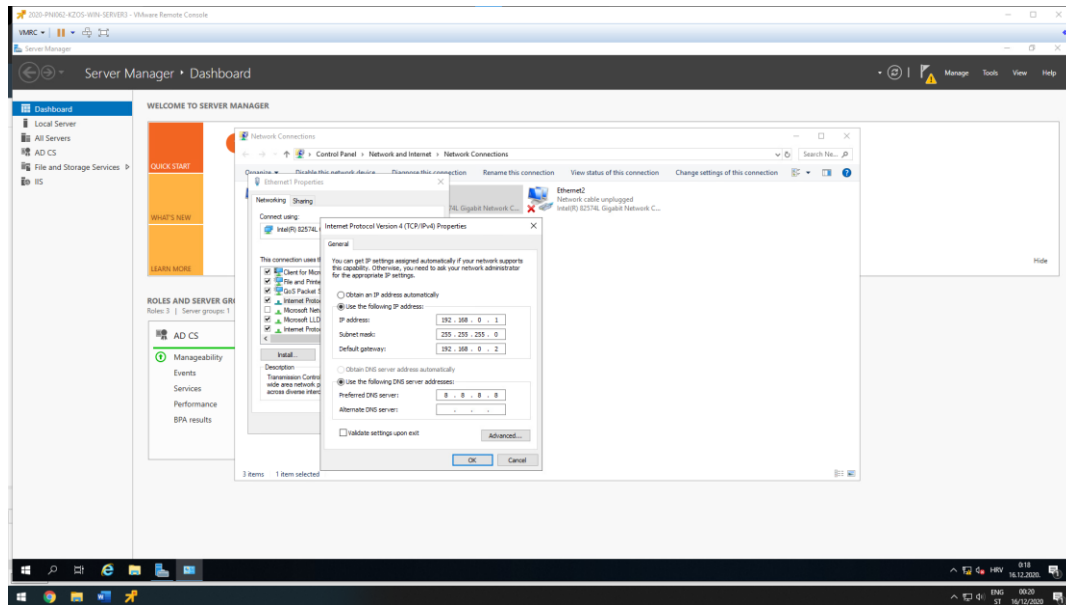
Slika 54: testiranje kad SERVER1 host u klasteru radi



Slika 55: testiranje kad SERVER1 host dodan u klaster ne radi

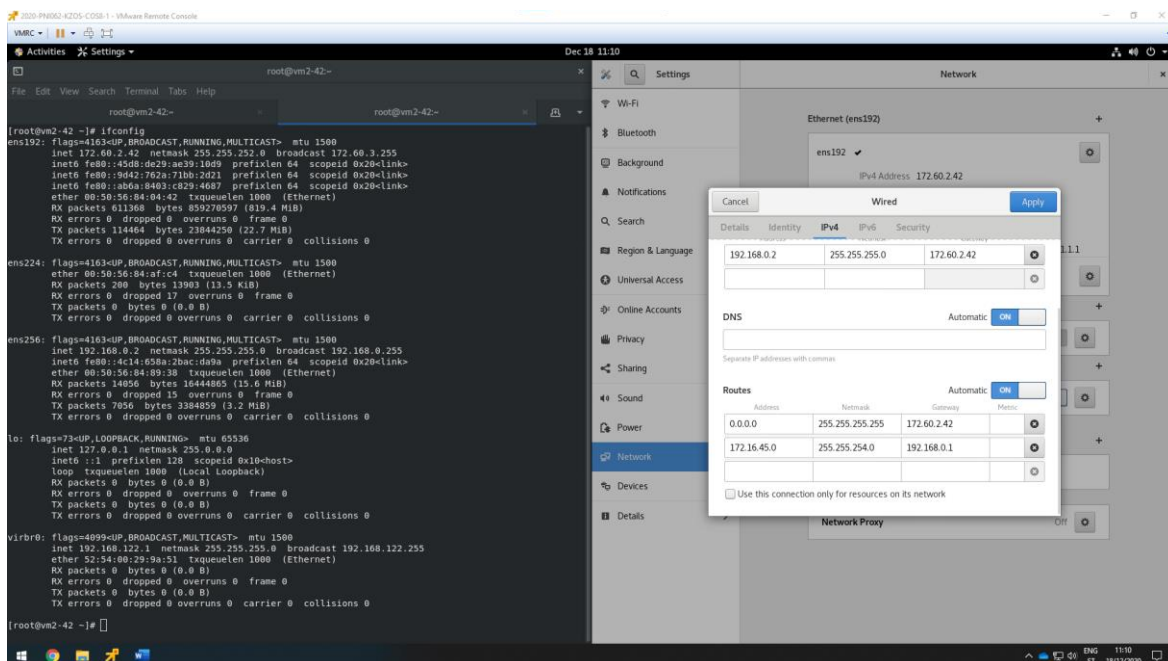
5.13. Internetska veza na SERVER3

Cilj je osposobiti internetsku vezu na SERVER3 poslužitelju koristeći CentOS1 računalo kao Gateway. Prije toga potrebno je konfigurirati drugi mrežni adapter na SERVER3 poslužitelju.



Slika 56: Prikaz konfiguracije drugog mrežnog adaptera na SERVER3 poslužitelju

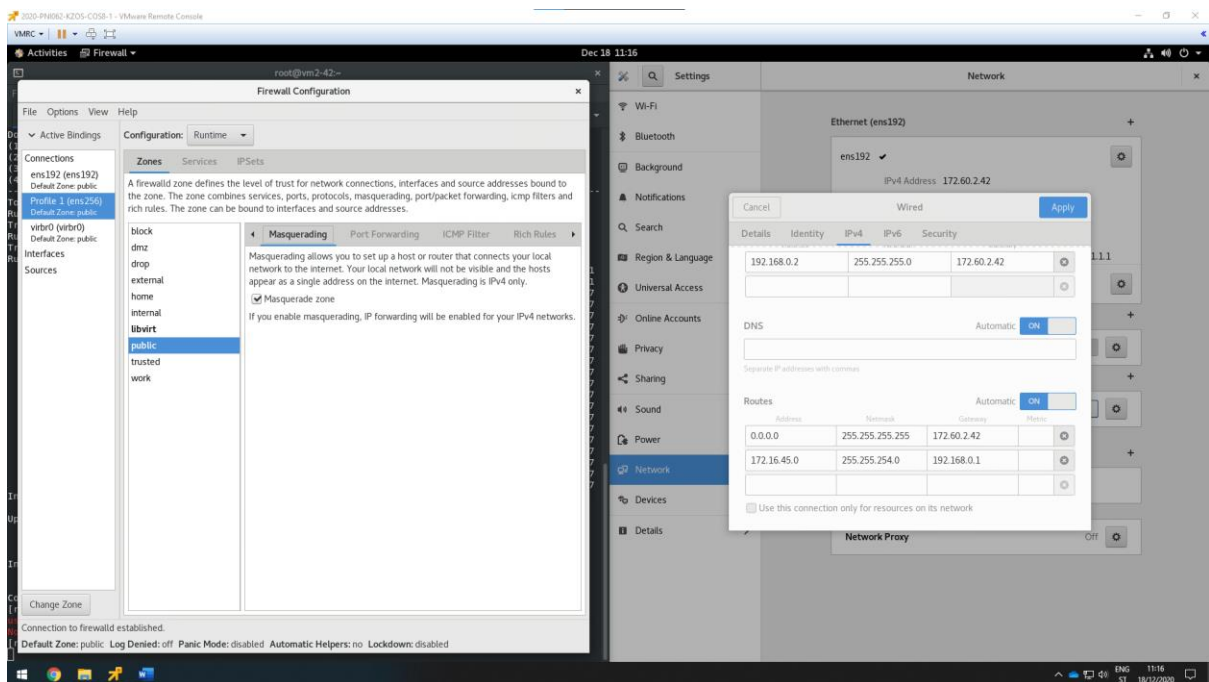
Na SERVER3 poslužitelj dodati default-nu rutu prema 192.168.0.2, ako nije dodana. Sljedeće što je potrebno, a to je konfigurirati drugi mrežni adapter ens256 kojem je potrebno dodati IP adresu zajedno sa Gateway-em koji će biti ens192 mrežni adapter. Dodati dvije rute. Jedna default-na ruta prema ens192 mrežnom adapteru i statička ruta domenskog mrežnog adaptera (na SERVER3) prema drugom mrežnom adapteru (na SERVER3).



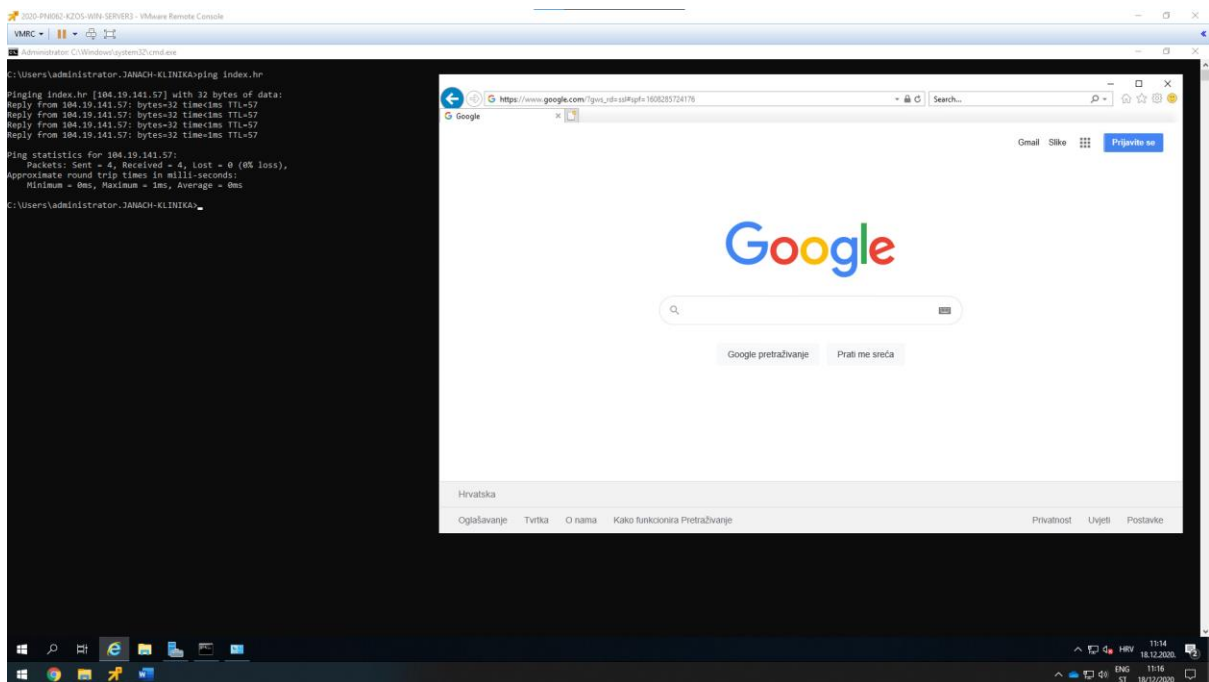
Slika 57: prikaz konfiguracije ens256 mrežnog adaptera na CentOS1 računalo

Na CentOS1 poslužitelj instalirati firewall-config, firewall-config potreban je zbog uključivanja MASQUERADE značajke koja omogućava lokalnoj mreži da se spoji na internet.

```
Yum install firewall-config -y
```



Slika 58: prikaz omogućene značajke MASQUERADE

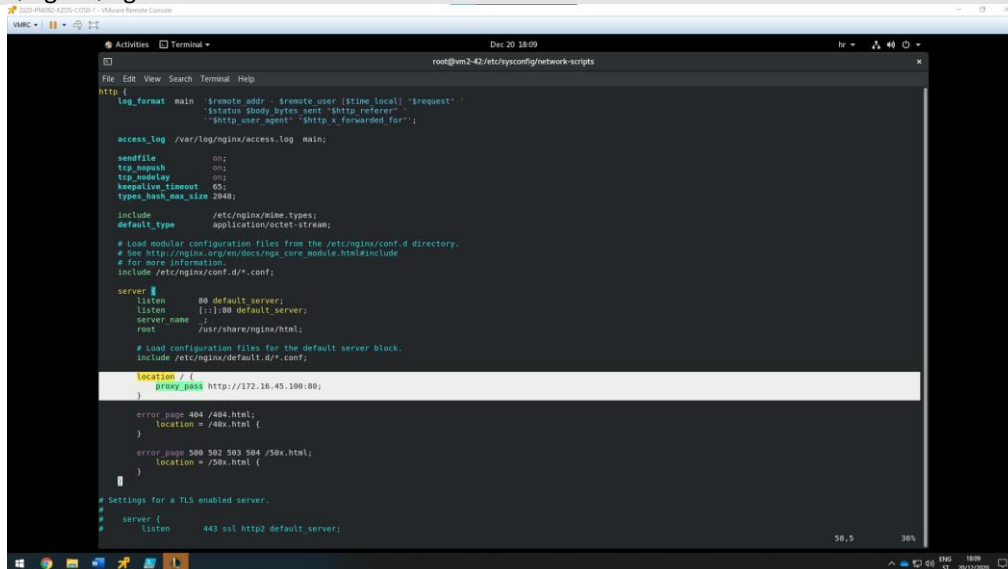


Slika 59: Testiranje internetske veze na SERVER3 računalu.

5.14. Konfiguracija reverse proxy na CentOS1 poslužitelju

Kako bi funkcionalno konfigurirali reverse proxy na CentOS1 poslužitelju potrebno je instalirati nginx servis te urediti VIM text uređivačem file na putanji /etc/nginx/nginx.conf.

```
Yum -y install nginx
Systemctl start nginx.service
Systemctl enable nginx.service
Vim /etc/nginx/nginx.conf
```



```
http {
    log_format main '$remote_addr - $remote_user [$time_local] "$request" '
        '$status $body_bytes_sent "$http_referer" '
        '"$http_user_agent" "$http_x_forwarded_for";

    access_log /var/log/nginx/access.log main;

    sendfile        on;
    tcp_nopush     on;
    tcp_nodelay    on;
    keepalive_timeout 65;
    types_hash_max_size 2048;

    include /etc/nginx/mime.types;
    default_type application/octet-stream;

    # Load modular configuration files from the /etc/nginx/conf.d directory.
    # See http://nginx.org/en/docs/nginx_core_module.html#include
    # For more information
    include /etc/nginx/conf.d/*.conf;
}

server {
    listen 80 default_server;
    listen [::]:80 default_server;
    server_name _;
    root /usr/share/nginx/html;

    # Load configuration files for the default server block.
    include /etc/nginx/default.d/*.conf;

    location / {
        proxy_pass http://172.16.45.100:80;
    }

    error_page 404 /404.html;
        location = /40x.html {
    }

    error_page 500 502 503 504 /50x.html;
        location = /50x.html {
    }

    # Settings for a TLS enabled server.
    #
    # server {
    #     listen 443 ssl http2 default_server;

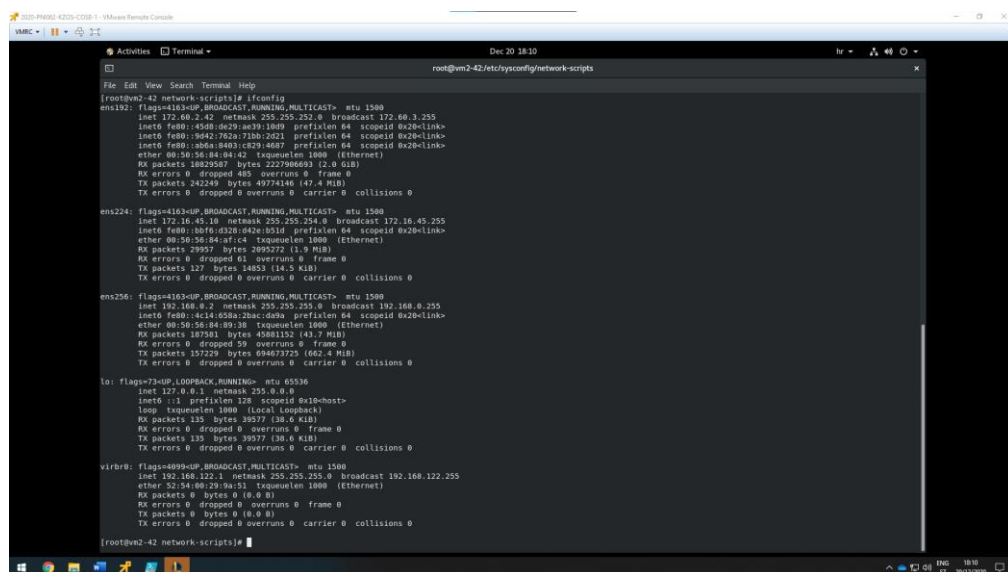
```

Slika 60: prikaz edit-iranog nginx.conf file-a

Uređivanjem nginx.conf fajla potrebno je ponovno pokrenuti nginx servis kako bi se primijenile promjene.

```
Systemctl restart nginx.service
```

Preostali mrežni adapterna CentOS1 računalu konfigurirati na tako da može komunicirati s računalima koja su u domeni.



```
[root@vm2-42 network-scripts]# ifconfig
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.0.42 netmask 255.255.252.0 broadcast 172.16.0.255
    inet6 fe80::4508:de29:ae39:1869 prefixlen 64 scopeid 0x2b<link>
    inet6 fe80::9642:762b:713b:2021 prefixlen 64 scopeid 0x2b<link>
    ether 08:00:50:56:84:04:ca txqueuelen 1000 (Ethernet)
    RX packets 1802807 bytes 222798600 (21.0 GiB)
    RX errors 0 dropped 485 overruns 0 frame 0
    TX packets 262249 bytes 49774140 (47.4 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.45.10 netmask 255.255.254.0 broadcast 172.16.45.255
    inet6 fe80::80f6:d328:442e:051d prefixlen 64 scopeid 0x2b<link>
    ether 08:00:50:56:84:04:ca txqueuelen 1000 (Ethernet)
    RX packets 29957 bytes 2895272 (1.9 MiB)
    RX errors 0 dropped 63 overruns 0 frame 0
    TX packets 127 bytes 14853 (14.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens256: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.2 netmask 255.255.252.0 broadcast 192.168.0.255
    inet6 fe80::4c14:658a:2bac:dab6 prefixlen 64 scopeid 0x2b<link>
    ether 08:00:50:56:84:04:38 txqueuelen 1000 (Ethernet)
    RX packets 187581 bytes 45881152 (43.7 MiB)
    RX errors 0 dropped 59 overruns 0 frame 0
    TX packets 157229 bytes 68683725 (65.4 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

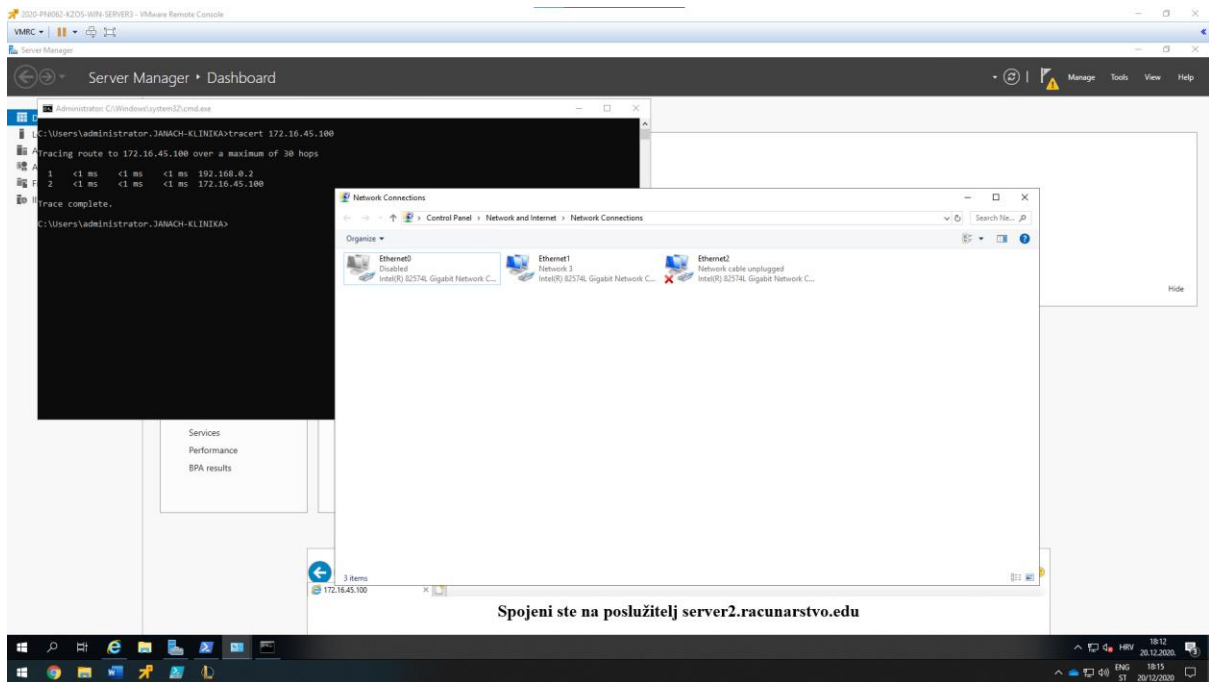
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 153 bytes 80572 (80.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 153 bytes 80572 (80.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

virbr9: flags=4899<UP,BROADCAST,MULTICAST> mtu 1500
    inet 192.168.122.1 netmask 255.255.252.0 broadcast 192.168.122.255
    ether 52:54:00:29:18:51 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@vm2-42 network-scripts]#
```

Slika 61: prikaz konfiguracija ens224 mrežnog adaptera u subnetu 172.16.45.0/23

Kako bi se testirala reverse proxy funkcionalnost potrebno je ugasiti domenski mrežni adapter na SERVER3 računalu. Kad je ugašen domenski mrežni adapter potrebno je pokušati konfiguracijom reverse proxy-a doći do web stranice koja se pokreće na IIS-u pomoću CentOS poslužitelja.

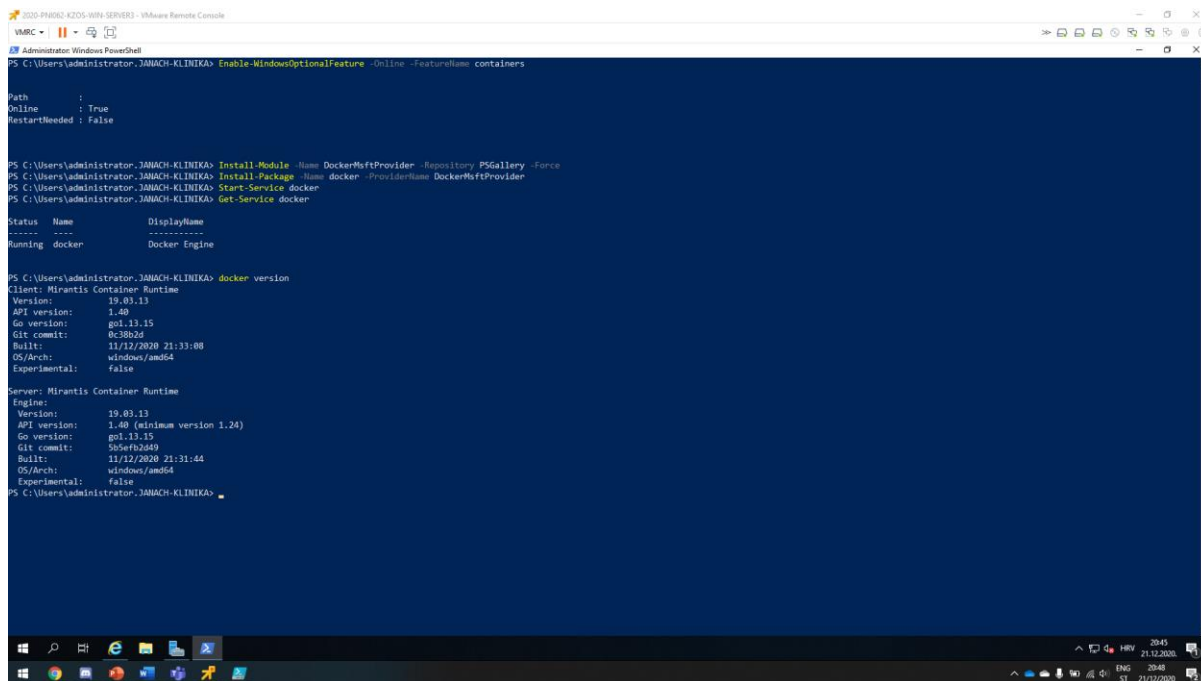


Slika 62: testiranje dostupnosti stranice 172.16.45.100 kad je ugašen domenski mrežni adapter

5.15. Docker na SERVER3 poslužitelju

Cilj je podignuti Docker engine i po izboru skinuti docker kontejner iz docker službenih repozitorija. Kad je kontejner preuzeti potrebno ga je pokrenuti i testirati rad.

```
#omogućiti značajku containers:  
Enable-WindowsOptionalFeature -Online -FeatureName Containers  
  
#instalirati module Docker(Docker Engine):  
Install-Module -Name DockerMsftProvider -Repository PSGallery -Force  
  
#instalirati paket imena Docker:  
Install-Package -Name docker -ProviderName DockerMsftProvider  
  
#omogućiti Docker(Docker Engine) servis:  
Start-Service docker  
  
#provjera stanja servisa:  
Get-Service docker
```



```
2020-PR0502-K205-WFN-SERVER3 - VMware Remote Console  
VMRC  
Administrator: Windows PowerShell  
PS C:\Users\Administrator\JAMACH-KLINIKA> Enable-WindowsOptionalFeature -Online -FeatureName containers  
  
Path :  
Online : True  
RestartNeeded : False  
  
PS C:\Users\Administrator\JAMACH-KLINIKA> Install-Module -Name DockerMsftProvider -Repository PSGallery -Force  
PS C:\Users\Administrator\JAMACH-KLINIKA> Install-Package -Name docker -ProviderName DockerMsftProvider  
PS C:\Users\Administrator\JAMACH-KLINIKA> Start-Service docker  
PS C:\Users\Administrator\JAMACH-KLINIKA> Get-Service docker  
  
Status Name Display Name  
-----  
Running docker Docker Engine  
  
PS C:\Users\Administrator\JAMACH-KLINIKA> docker version  
Client: Mirantis Container Runtime  
Version: 19.03.13  
API version: 1.40  
Go version: go1.13.15  
Git commit: 0c38b2d  
Built: 11/12/2020 21:33:08  
OS/Arch: windows/amd64  
Experimental: false  
  
Server: Mirantis Container Runtime  
Engine:  
Version: 19.03.13  
API version: 1.40 (minimum version 1.24)  
Go version: go1.13.15  
Git commit: 954fb2d49  
Built: 11/12/2020 21:31:44  
OS/Arch: windows/amd64  
Experimental: false  
PS C:\Users\Administrator\JAMACH-KLINIKA>
```

Slika 63: prikaz output-a pokrenutih CMDLET-a

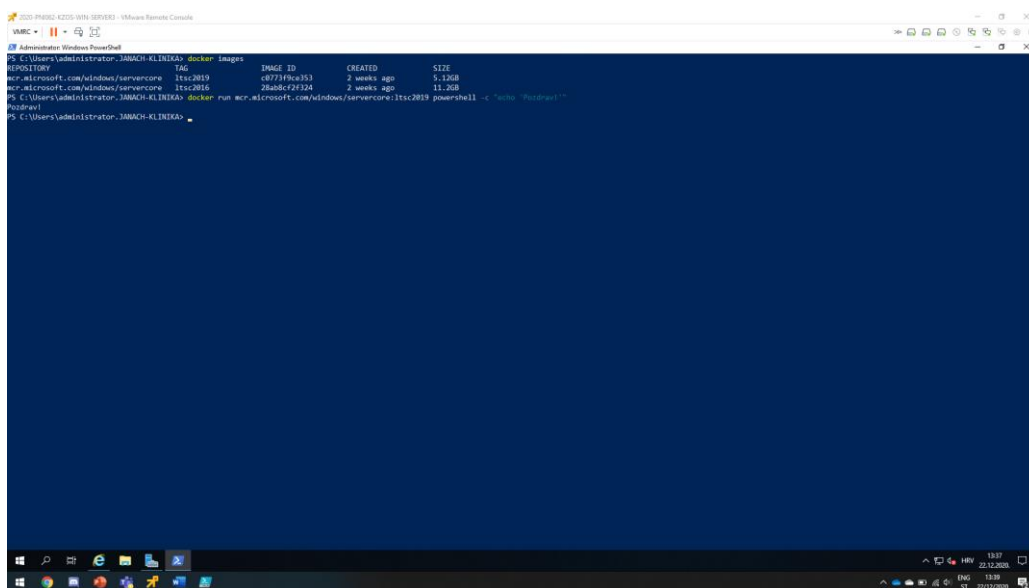
Kad je servis docker omogućen, mogu se pretraživati docker repozitoriji i povlačiti images s docker-ove službene stranice.

```
#pretražiti repozitorije dockera s ključnom riječi windows server, koristit će se prvi image s najviše review-a(zvijezdica):  
docker search windowsserver
```

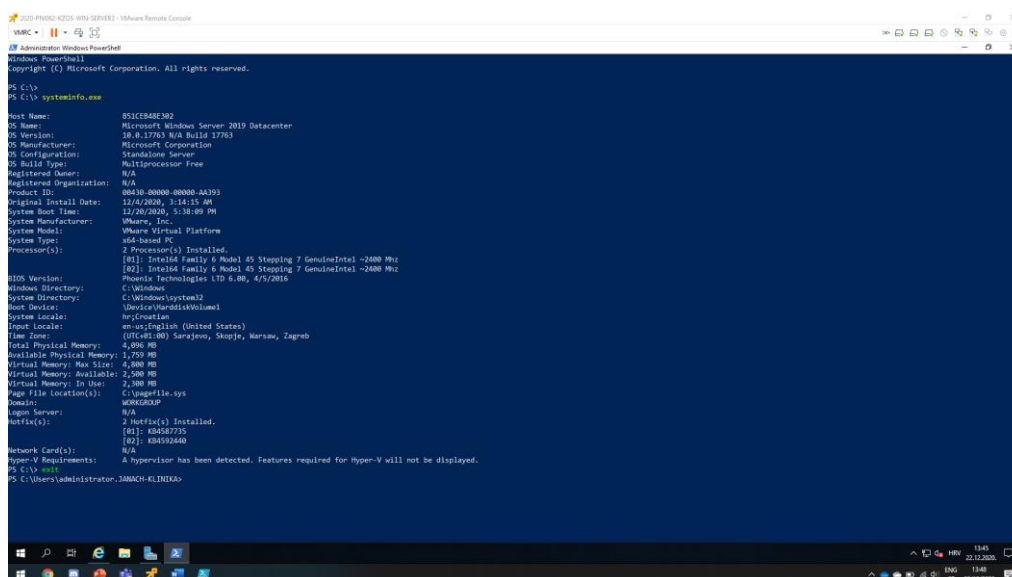
```
#Skinuti windows image sa službene stranice:  
docker pull mcr.microsoft.com/windows/servercore:ltsc2016  
docker pull mcr.microsoft.com/windows/servercore:ltsc2019
```

```
#pokrenuti echo naredbu unutar kontejnera  
docker run microsoft/windowsservercore powershell -c "echo Pozdrav!"
```

Kod preuzimanja docker-ovih image-a s njihovih službenih repozitorija, preuzeo sam Windows server 2016 i 2019. Kad su se preuzeli image-i pokrenut je Windows server Data Center 2019. Kroz pokrenuti image pokrenuta je echo naredba unutar tog kontejnera koja daje output. Time se testira rad kontejnera.



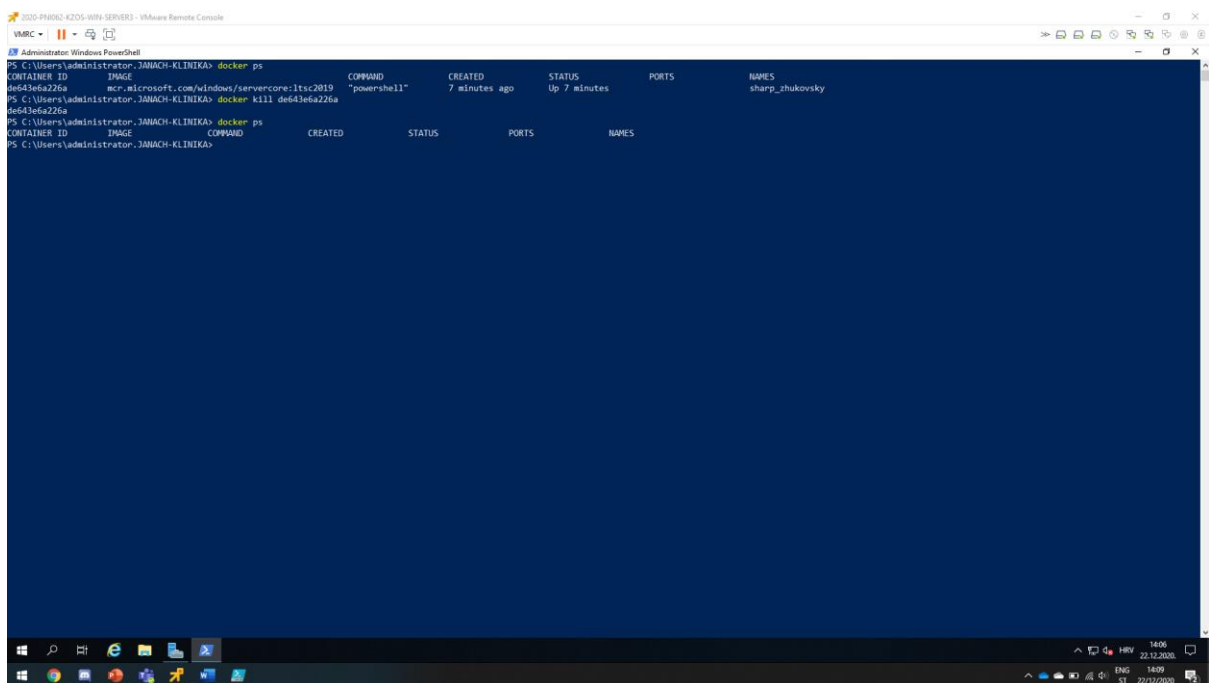
Slika 64: prikaz preuzetih image-a s docker-ovih službenih repozitorija i pokretanje echo naredbe unutar kontejnera



Slika 65: prikaz pokrenute sesije na Windows server 2019 Data Center image-u

Kako bi pokrenuli sesiju i kako bi sesija ostala pokrenuta kao proces koji se pokreće unutar docker-a. Potrebno je upisati naredbu koja je prikazana ispod ovog teksta. Kad je naredba pokrenuta otvara se sesija unutar koje je nužno pritisnuti CTRL + P ili CTRL + Q kako bi sesija ostala otvorena i pokretala se kao proces unutar docker-a.

```
#pokretanje sesije:  
docker run -it microsoft/windowsservercore powershell powershell  
  
#pritisnuti CTRL+Q ili CTRL+P  
  
#prikaz pokrenutih procesa unutar docker-a:  
docker ps  
  
#ako se želi spojiti ponovno sa sesijom:  
docker attach  
  
#ako se pokrenuti proces želi ugasiti iz host konzole:  
docker kill
```



```
Administrator: Windows PowerShell  
PS C:\Users\administrator_3AMACH-KLINIKA> docker ps  
CONTAINER ID        IMAGE               COMMAND             CREATED             STATUS              PORTS              NAMES  
de64366a226a       mcr.microsoft.com/windows/servercore:lts2019    "powershell"      7 minutes ago      Up 7 minutes        
de64366a226a       mcr.microsoft.com/windows/servercore:lts2019    "powershell"      7 minutes ago      Up 7 minutes        
de64366a226a       mcr.microsoft.com/windows/servercore:lts2019    "powershell"      7 minutes ago      Up 7 minutes      sharp_zhukovsky  
PS C:\Users\administrator_3AMACH-KLINIKA> docker ps  
CONTAINER ID        IMAGE               COMMAND             CREATED             STATUS              PORTS              NAMES  
PS C:\Users\administrator_3AMACH-KLINIKA> docker kill de64366a226a  
PS C:\Users\administrator_3AMACH-KLINIKA>
```

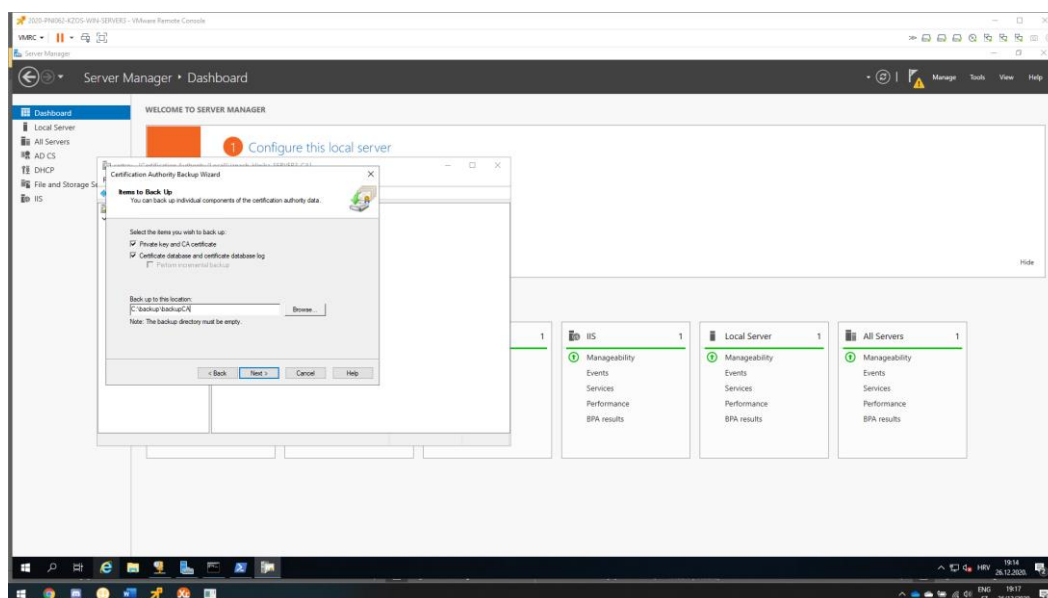
Slika 66: prikazane pokrenute sesije unutar docker servisa i gašenje pokrenute sesije unutar docker servisa

5.16. Nadogradnja SERVER3 poslužitelja na Windows server 2019

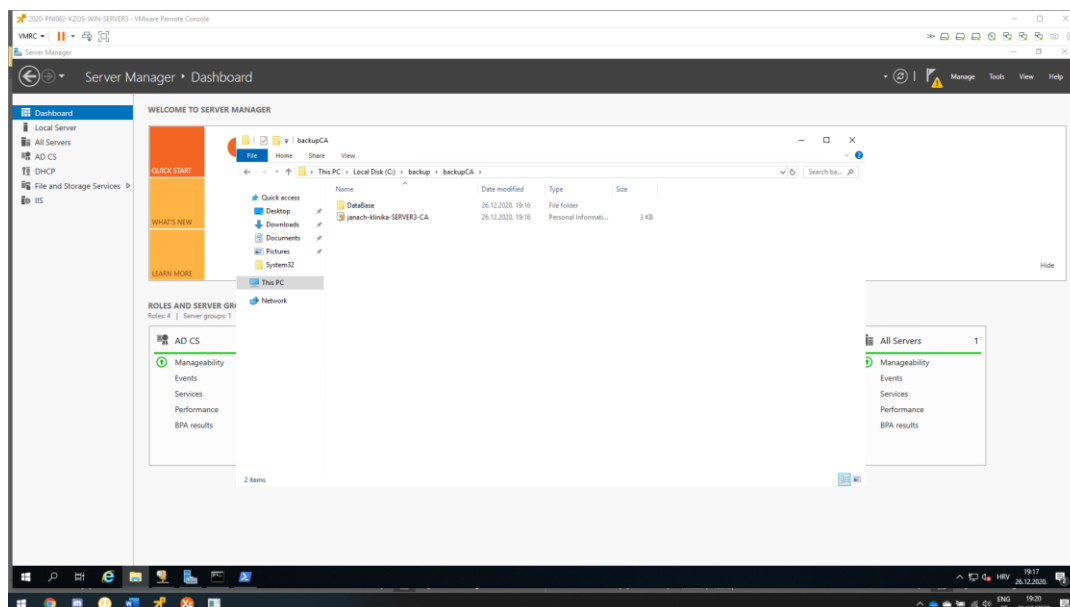
U navedenim zadacima na SERVER3 poslužitelju konfigurirani su CA, DHCP cluster koji je u paru sa SERVER2 poslužiteljem i DFS replikacija, što bi značilo da prije same nadogradnje sa Windows server 2016 na Windows server 2019 potrebno je napraviti backup CA i DHCP konfiguracije i remove-ati instalirane role. Tek nakon toga može se sigurno napraviti nadogradnja i kad se nadogradnja izvrši moguće je povratiti konfiguraciju koja je bila konfigurirana. Backup konfiguracija pohranjena je na putanji C:\backup.

CA backup:

Navigirati se u Certification Authority -> janach-klinika-SERVER3-CA -> All tasks -> Backup CA. Password kojim se štite datoteke je Pa\$\$w0rd.



Slika 67: prikaz Wizard-a za CA backup



Slika 68: prikaz kreiranih backup datoteka

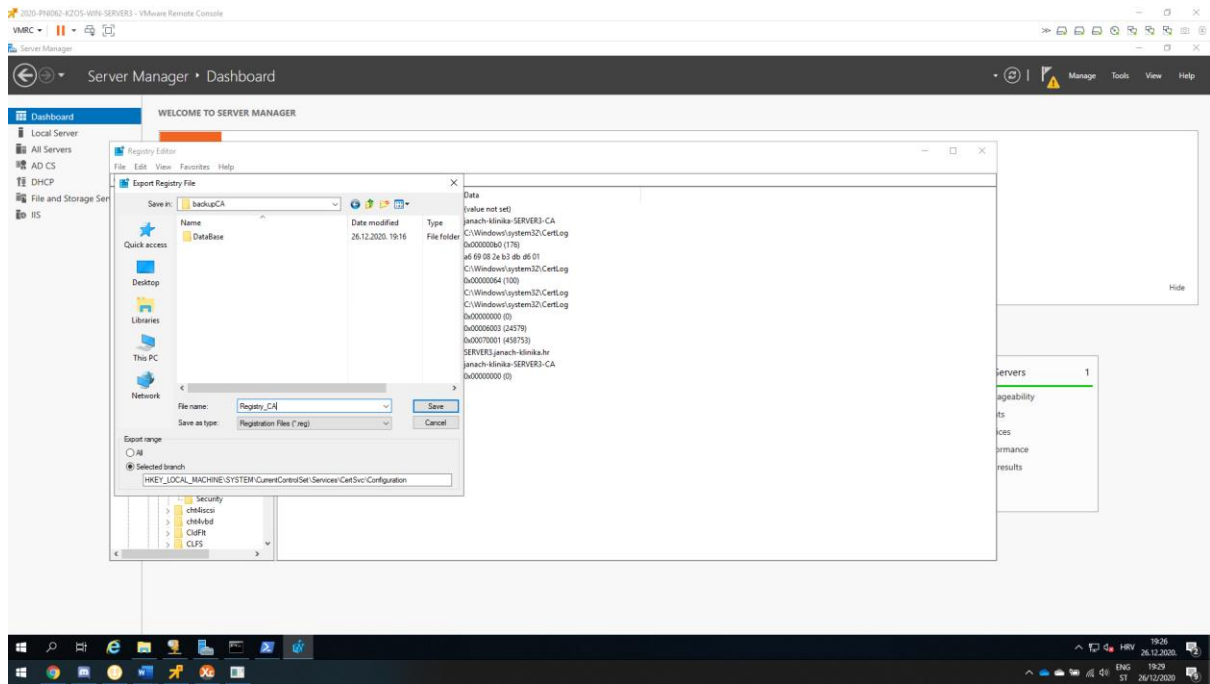
Sljedeće što je potrebno, a to je backupirati CA registry settingse.

CRTL+R -> regedit

Path u registry-u:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration

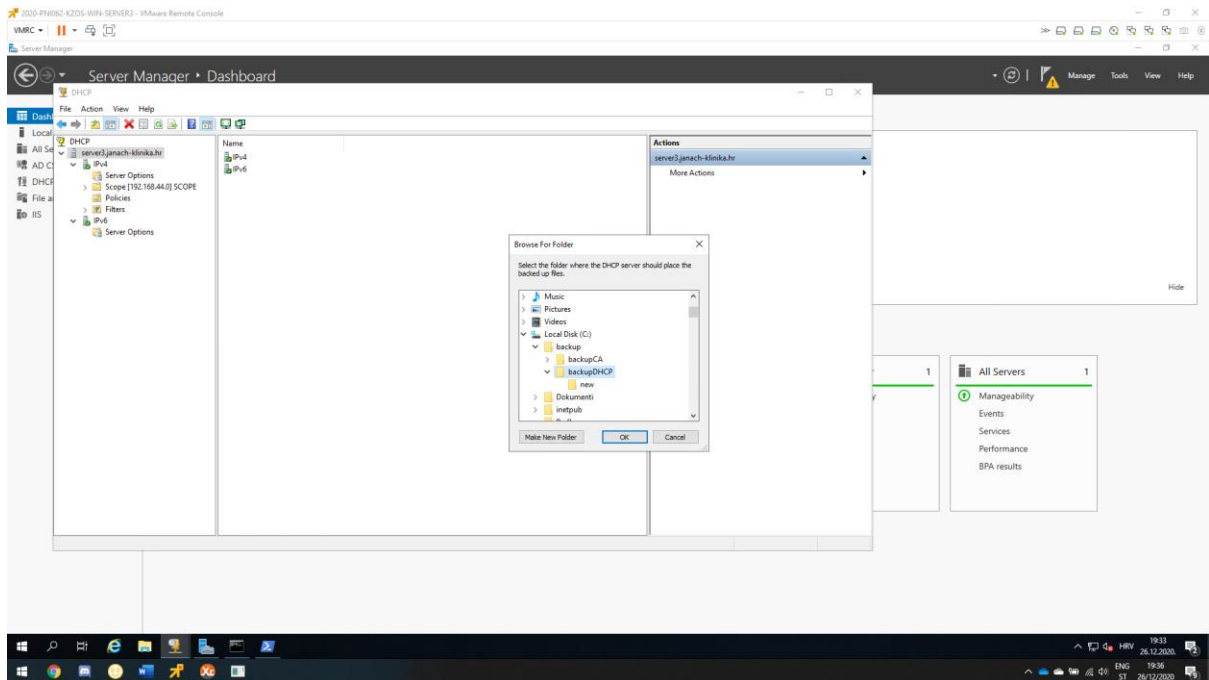
Desni klik na Configuration -> Export.



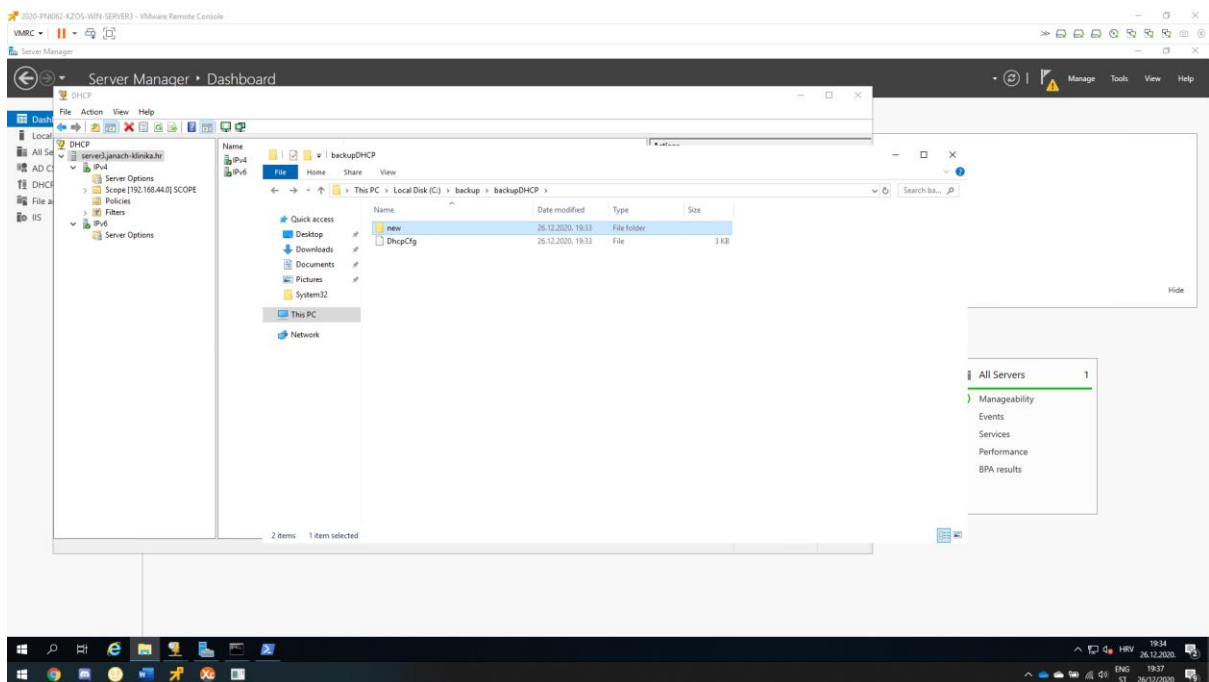
Slika 69: prikaz export-a CA konfiguracija iz registry-a

Kad je CA backup uspješno backupiran potrebno je napraviti DHCP backup tako da se navigiramo u DHCP konzolu na sljedeći način:

SERVER3.janach-klinika.hr -> Backup > odabrati putanju na kojoj će biti spremljeni backup.

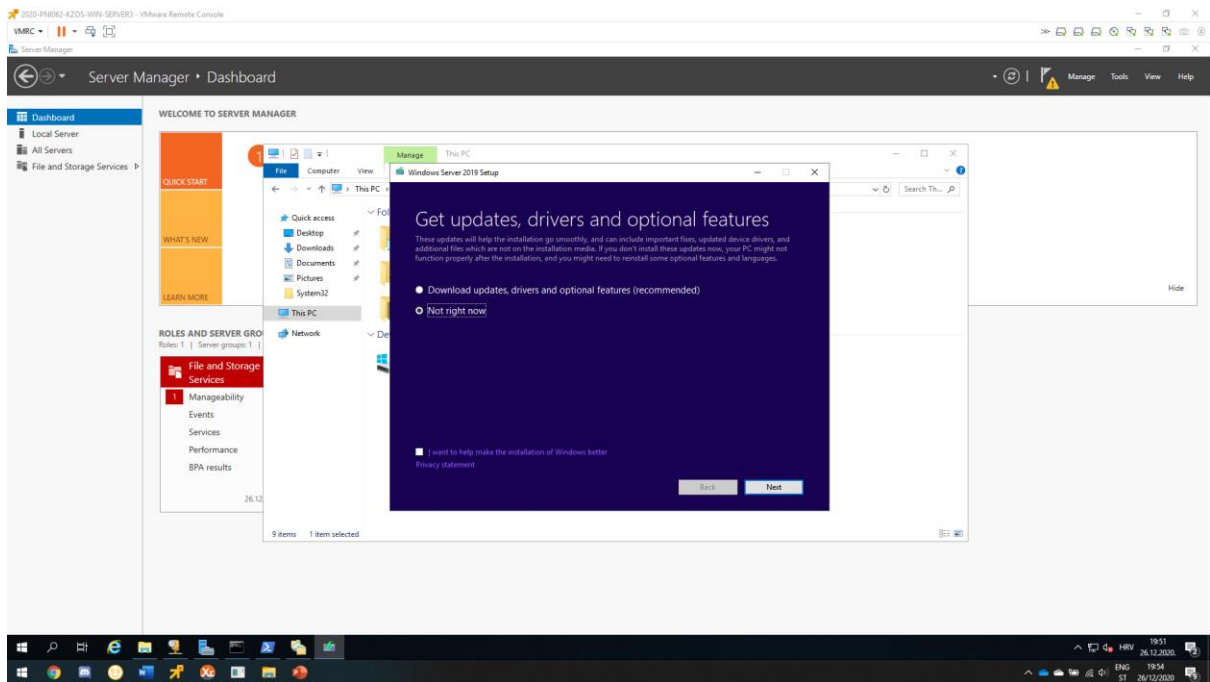


Slika 70: prikaz DHCP backup-a

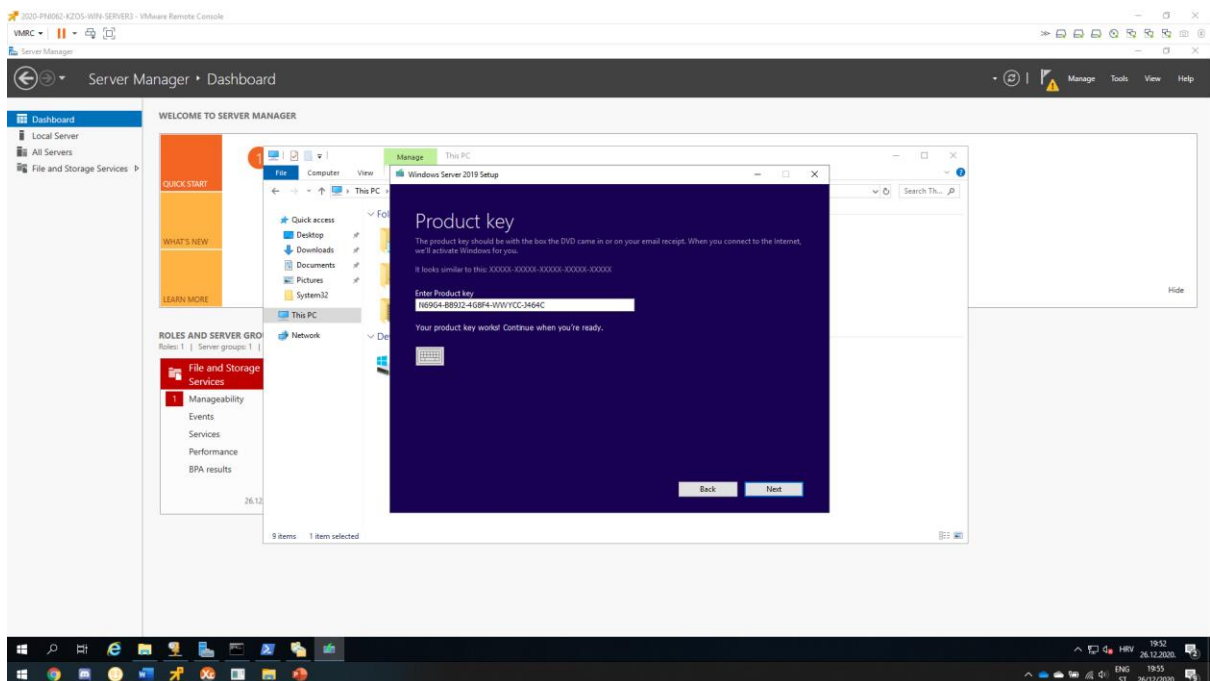


Slika 71: prikaz backup-iranih datoteka

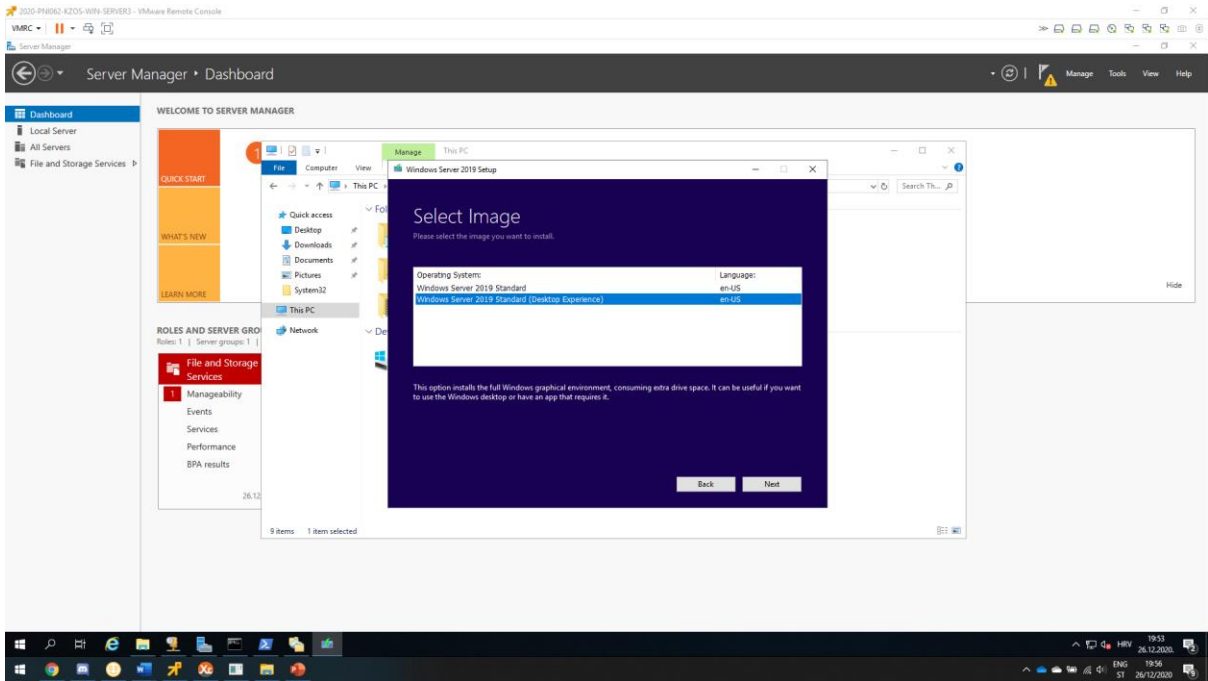
Prije nego se pokrene proces nadogradnje nužno je remove-ati sve instalirane role, a to su CA i DHCP. Koristeći server manager -> manage -> remove roles and features -> CA i DHCP. Zatim pokrenuti setup nadogradnje SERVER3 poslužitelja s Windows server 2016 na 2019.



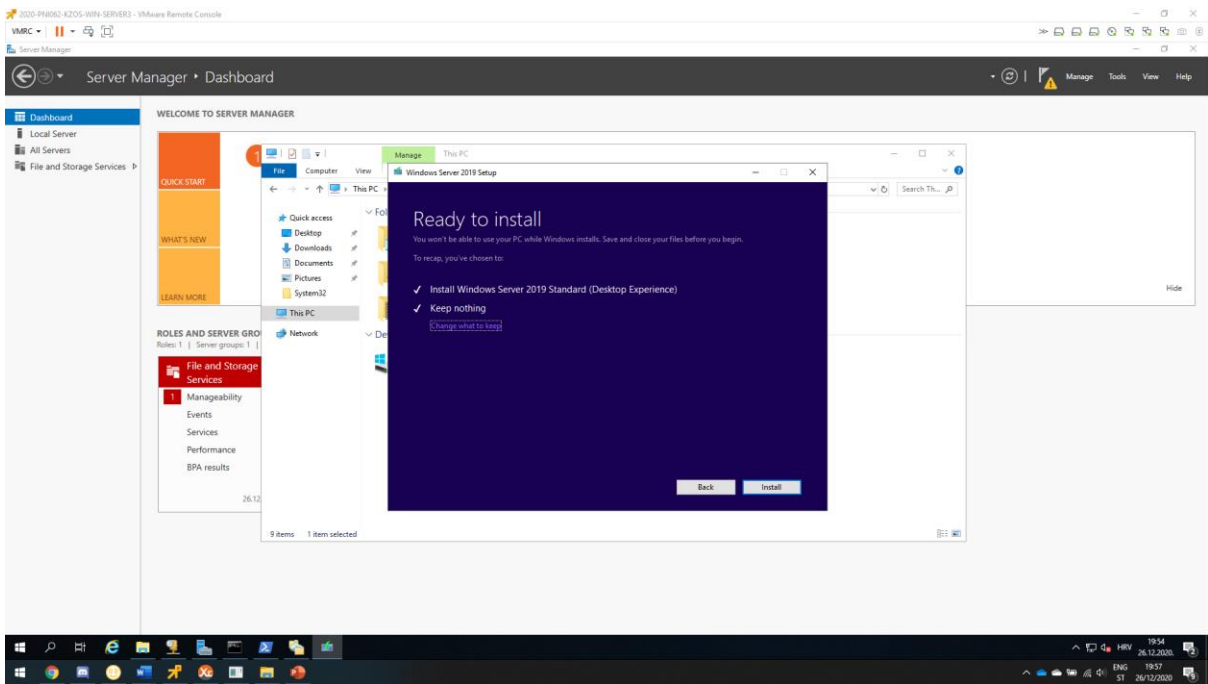
Slika 72: pokretanje setup-a



Slika 73: upisati product key

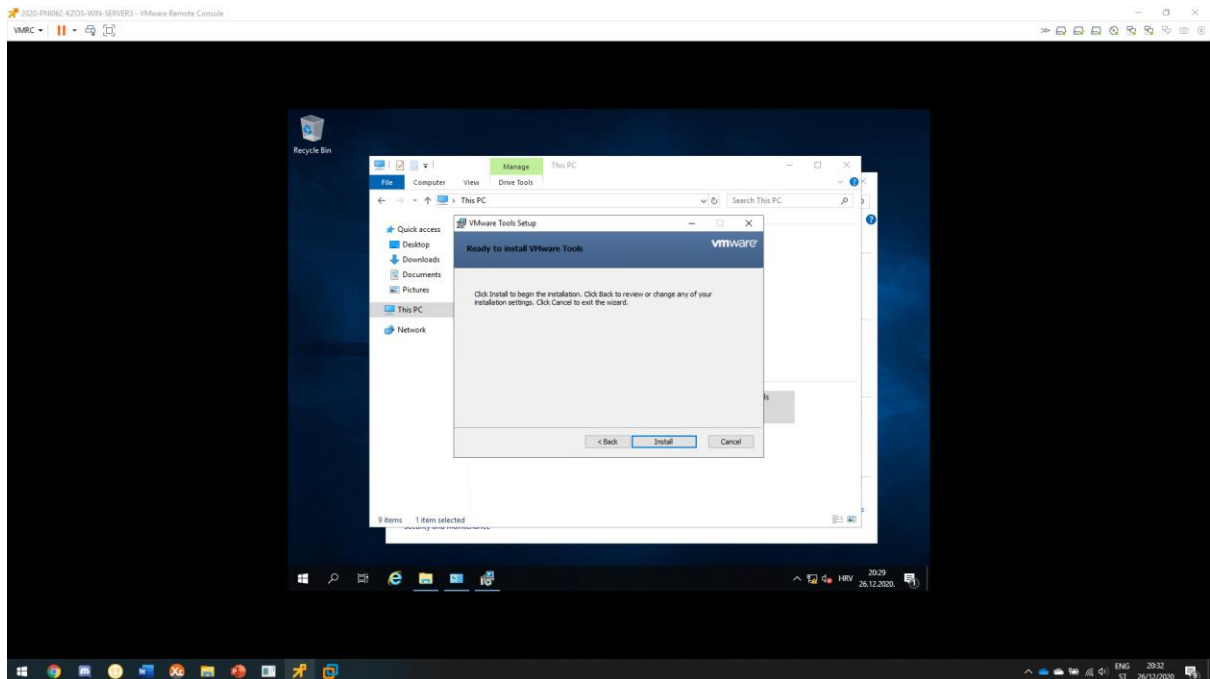


Slika 74: odabrali Desktop Experience

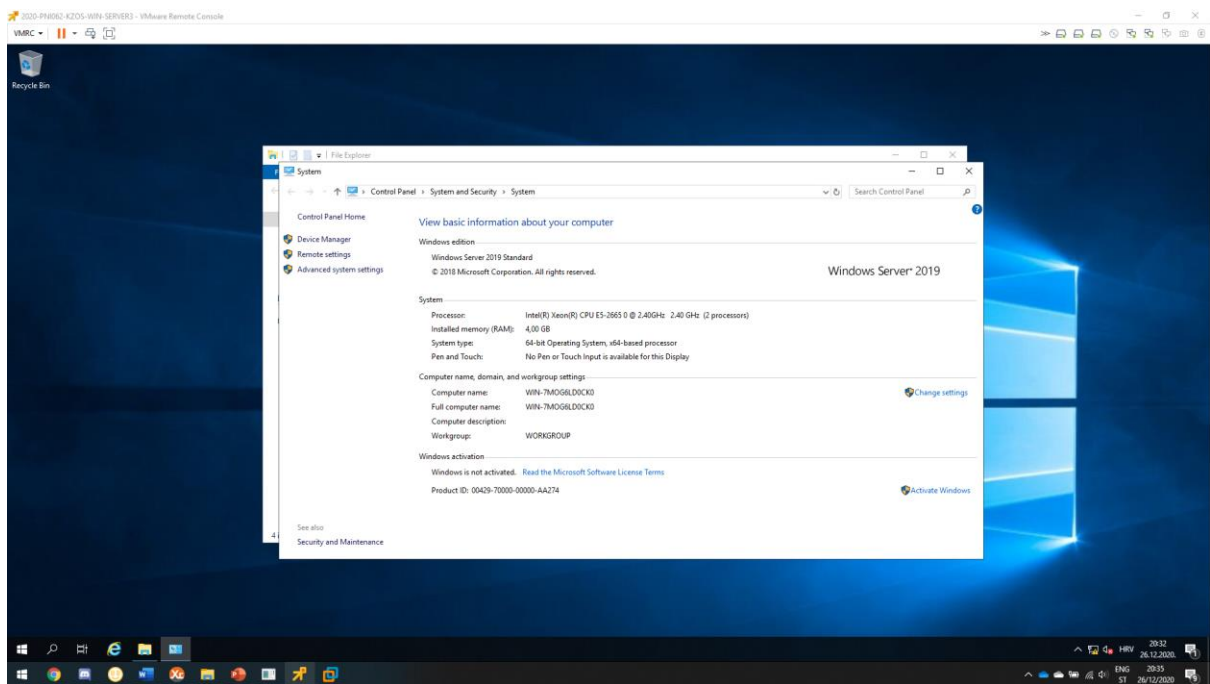


Slika 75: instalirati Windows server 2019

Kad je instaliran Windows server 2019 potrebno je instalirati VM tools, iz vSphere managera attachat VM tools na DC/DVD drive i instalirati ih ručno u virtualci.

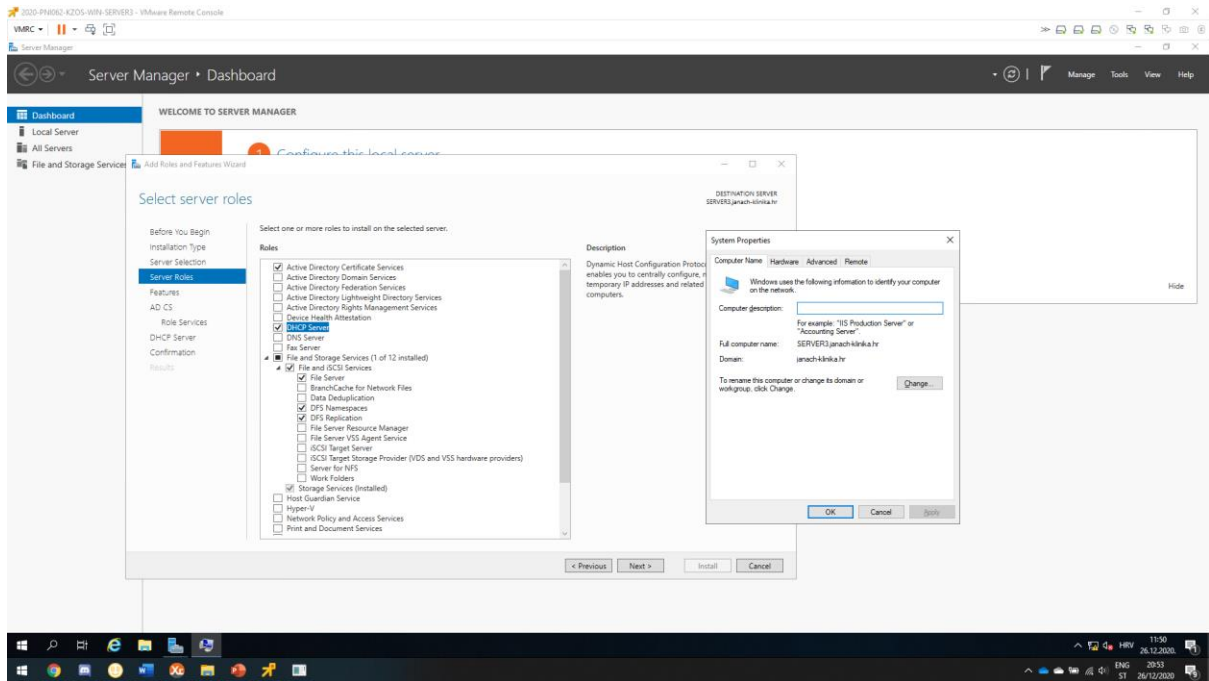


Slika 76: instalacija VM tools-a



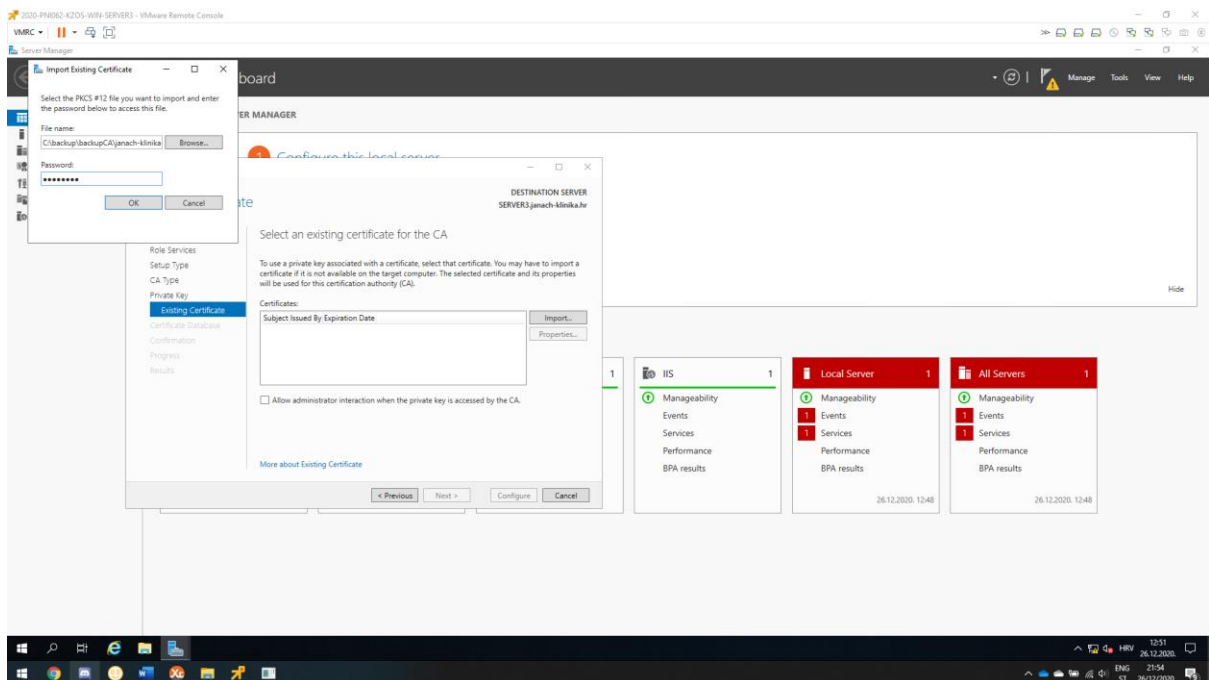
Slika 77: prikaz uspješne instalacije Windows server 2019

Kad je uspješno prošla nadogradnja s Windows servera 2016 na Windows server 2019 potrebno je računalo dodati u domenu i instalirati sve role koje su prethodno bile instalirane. Ako se javi problem black screena kod prijave domenskim administratorom potrebno je na SERVERDC u GPO omogućiti „User Account Control: Admin Approval Mode for the Built-in Administrator account“.

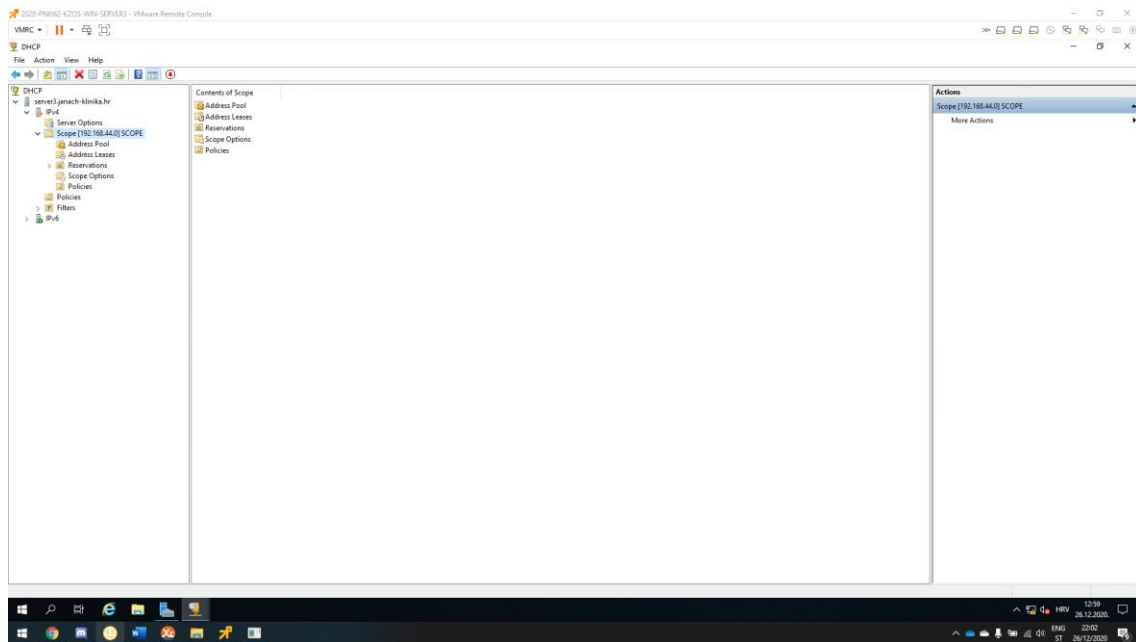


Slika 78: prikaz dodanog SERVER3 poslužitelja u domenu i instalacija rola

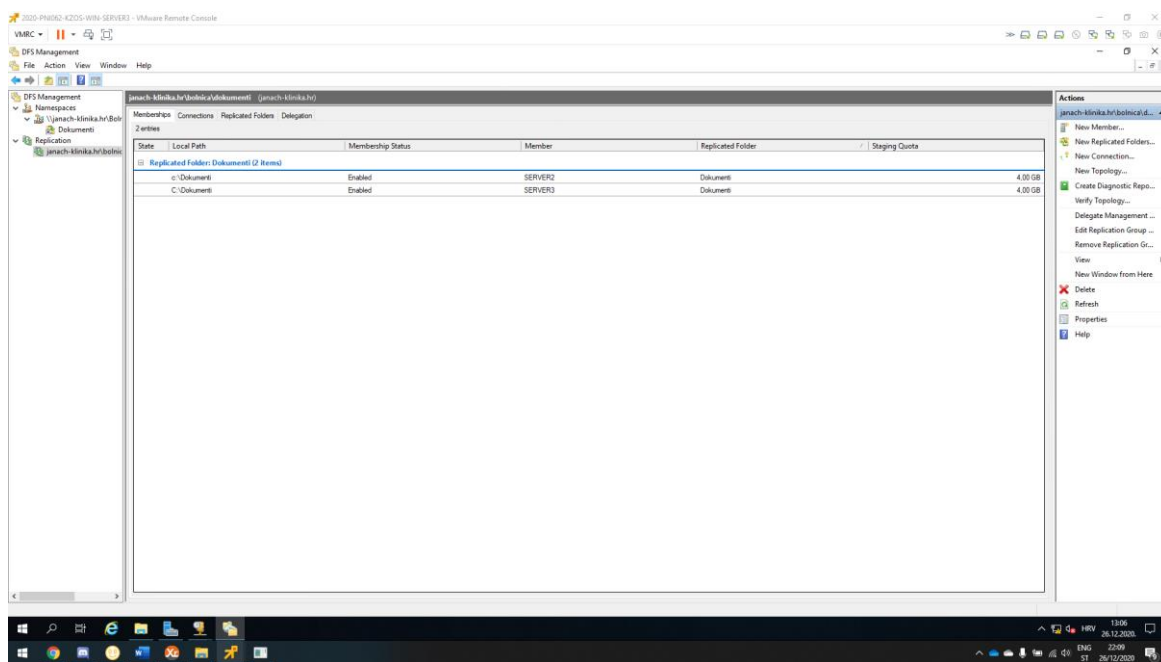
Kad su role instalirane potrebno je restore-ati konfiguraciju koja je prethodno backupirana.



Slika 79: restore CA certifikata



Slika 80: restoreDHCP konfiguracije



Slika 81: prikaz funkcionalnog DFS-a

Zadnja potrebna konfiguracija koju je potrebno napraviti, a to je konfigurirati preostala dva mrežna adaptera na SERVER3 poslužitelju. Prvi mrežni adapter je domenski, drugi mrežni adapter je veza s internetom(ako će u budućnosti postojati potreba za uključivanjem) i treći mrežni adapter služi poslužen je od strane DHCP servera adresom koja je u 192.168.44.0/24 subnet-u, ujedno treći mrežni adapter sprječava Single Point of Failure.

6. Zaključak

Dokumentacija obuhvaća rješenje projekta u kojem su korištena računala: SERVERDC, SERVER1, SERVER2, SERVER3 i CLI1 od kojih je jedno Linux računalo CentOS1. Ova dokumentacija obuhvaća podignutu infrastrukturu koja odgovara svim zahtjevima klinike janach-klinika.hr. U projektu je uspješno podignuta domena janach-klinika.hr na SERVERDC poslužitelju. Kreirano je 50 korisnika koji su dodani u pripadajuće OU i pripadajuće grupe. Podignut je sekundarni DNS i DC na SERVER1 poslužitelju zajedno s Storage Spaces-om i Dynamic Access Control datotečnim sustavom. Funkcionalan DFS na SERVER2 i SERVER3 poslužitelj s omogućenom replikacijom. Zatim SERVER3 je dodan u domenu na kojem je instaliran CA i DHCP klaster koji je u paru s SERVER poslužiteljem. Na SERVER1 u SERVER2 instaliran je IIS i postavljena je testna stranica koja koristi SSL/TLS enkripciju. Na SERVERDC instaliran NLB i konfiguriran za SERVER1 i SERVER2 u paru i rade u klasteru. Postavljen je default gateway na SERVER3, default gateway je CentOS1 linux računalo. Zatim je na SERVER3 poslužitelju omogućen internet preko CentOS1 računala i na CentOS1 računalu je konfiguriran reverse proxy za pristup web stranica NLB-a kad SERVER3 izgubi domensku vezu. Uspješnim pristupom na internet preko SERVER3 podignut je Docker Engine i preuzet je docker container. I za kraj SERVER3 poslužitelj je s Windows server 2016 nadograđen na Windows server 2019. Ovime završava projekt te se smatra da su svi zahtjevi tvrtke ispunjeni ovim rješenjem u ovoj dokumentaciji.

7. Popis slika

| | |
|--|----|
| Slika 1: Shematski prikaz topologije..... | 2 |
| Slika 2: za izradu umne mape u kojoj je opisana infrastrukturu korišten FreeMind software..... | 3 |
| Slika 3: prikaz podignute domene zajedno sa IP adresom na mrežnom adapteru..... | 4 |
| Slika 4: slika prikazuje dodavanje računala u domenu | 5 |
| Slika 5: prikaz dodanih računala u domenu | 5 |
| Slika 6: prikazuje dodavanje usera .csv datotekom pomoću PowerShell skripte..... | 7 |
| Slika 7: prikaz OU, usera koji su dodani u grupu..... | 7 |
| Slika 8: prikaz instalirane ADDS uloge koja je propagirana u Additional/backup Domain Controller(sekundarni) i prikaz promjene IP adrese DNS servera nad mrežnim adapterom | 8 |
| Slika 9:prikaz ažuriranih PTR zapisa u forward lookup zoni..... | 9 |
| Slika 10: prikaz zapisa IPv4 primarne reverzne lookup zone | 9 |
| Slika 11: Shodno tome vidljivo je da su zapisi replicirani u reverznoj zoni na SERVER1 poslužitelju ... | 10 |
| Slika 12: Storage Spaces, Virtualni disk i volumen..... | 11 |
| Slika 13:prikaz network share mape uprava..... | 12 |
| Slika 14: Prikaz setting-a KDC Supporte-a..... | 13 |
| Slika 15: Prikaz setting-a postavljenih novo kreirani Claim Type: department | 14 |
| Slika 16: prikaz setting-a za novokreirani Central Access Rules za doktore koji su dodani u current permission..... | 14 |
| Slika 17: prikaz setting-a za novokreirani Central Access Rules za upravu i doktore koji su dodani u Current Permissions..... | 15 |
| Slika 18: Prikaz setting-a kod kreiranja klasifikacijskog pravila..... | 15 |
| Slika 19: prikaz dodane klasifikacije Confidentiality i Department..... | 16 |
| Slika 20: tekstualna datoteka koja sadrži secret kako bi se testirala funkcionalnost | 16 |
| Slika 21: test korisnika iz grupe uprava može ući u xyzDOC.txt datoteku, no ne može ući u place.txt datoteku..... | 17 |
| Slika 22:test korisnika iz grupe doktori može ući u obje datoteke | 17 |
| Slika 23: test korisnika iz grupe sestre ne može pristupiti datotekama | 18 |
| Slika 24: prikaz namespace-a i dodavanje namespace servera | 19 |
| Slika 25: dodavanje novog foldera u namespace s dva target-a..... | 20 |
| Slika 26: kreiranje replikacijske grupe..... | 20 |
| Slika 27: prikaz uspješne funkcionalnosti DFS replikacije između SERVER2 i SERVER3 računala | 21 |
| Slika 28: instalacija ADCS uloge i konfiguracija ADCS na poslužitelju | 22 |
| Slika 29: OSCP Response Signing Properties, prikaz dodanih poslužitelja koji će biti web serveri(IIS) | 23 |
| Slika 30: Web Server properties, prikaz dodanih poslužitelja koji će biti web serveri(IIS) | 23 |
| Slika 31: duplicated Web Server template, prikaz General, Security i Superseded setting-a | 24 |
| Slika 32: prikaz izdanih certifikata..... | 24 |
| Slika 33: duplicate Users template, prikaz General, Security i Subject Name setting-a | 25 |
| Slika 34: Certificate Services Client – Auto-Enrollment, prikaz konfiguracije nad stavkom, GPO raditi na SERVERDC..... | 25 |
| Slika 35: prikaz instalacije Web Server(IIS) uloge | 26 |
| Slika 36: prikaz setting-a kreiranja Domain certifikata(Vrijedi i za SERVER1 i SERVER2 poslužitelj, friendly name zamijeniti s drugim imenom SERVERX-CERT | 26 |
| Slika 37: prikaz dodanih certifikata na SERVER1 i SERVER2 poslužitelju | 27 |
| Slika 38:Prikaz konfiguracije Default Web Site, Site bindings..... | 27 |

| | |
|--|----|
| Slika 39: Default Web Site, Accept SSL..... | 28 |
| Slika 40: Dokaz da SSL certifikat funkcionalno radi..... | 28 |
| Slika 41: prikaz instalacije DHCP uloge na SERVER1 i SERVER2 poslužitelj..... | 29 |
| Slika 42: prikaz kreiranog scope-a i konfiguriranog failover-a..... | 30 |
| Slika 43: prikaz dodanog SERVER2 poslužitelja..... | 30 |
| Slika 44: prikaz konfiguracije 3. mrežnog adaptera na SERVER3 poslužitelju kako bi IP adrese mogle biti dodijeljene ostalim računalima | 31 |
| Slika 45: prikaz adresa koje su dodijeljene računalima..... | 31 |
| Slika 46: prikaz kreirane reverzne zone i dodanih PTR-a | 32 |
| Slika 47: prikaz instalacije NLB uloge s PowerShell skriptom | 34 |
| Slika 48: filtriranje portova | 35 |
| Slika 49: dodan je host(SERVER1) u klaster | 35 |
| Slika 50: Prikaz kreiranog klastera i dodanih hostova SERVER1 i SERVER2 | 36 |
| Slika 51: dodan DNS zapis klastera www | 36 |
| Slika 52: postavljanje novokreirane datoteke kao početnu stranicu IIS-a..... | 37 |
| Slika 53: kreirani certifikati za www.janach-klinika.hr..... | 37 |
| Slika 54: testiranje kad SERVER1 host u klasteru radi..... | 38 |
| Slika 55: testiranje kad SERVER1 host dodan u klaster ne radi..... | 38 |
| Slika 56: Prikaz konfiguracije drugog mrežnog adaptera na SERVER3 poslužitelju | 39 |
| Slika 57: prikaz konfiguracije ens256 mrežnog adaptera na CentOS1 računalu | 39 |
| Slika 58: prikaz omogućene značajke MASQUERADE | 40 |
| Slika 59: Testiranje internetske veze na SERVER3 računalu. | 40 |
| Slika 60: prikaz edit-iranog nginx.conf file-a | 41 |
| Slika 61: prikaz konfiguracija ens224 mrežnog adaptera u subnetu 172.16.45.0/23..... | 41 |
| Slika 62: testiranje dostupnosti stranice 172.16.45.100 kad je ugašen domenski mrežni adapter | 42 |
| Slika 63: prikaz output-a pokrenutih CMDLET-a | 43 |
| Slika 64: prikaz preuzetih image-a s docker-ovih službenih repozitorija i pokretanje echo naredbe unutar kontejnera | 44 |
| Slika 65: prikaz pokrenute sesije na Windows server 2019 Data Center image-u | 44 |
| Slika 66: prikazane pokrenute sesije unutar docker servisa i gašenje pokrenute sesije unutar docker servisa | 45 |
| Slika 67: prikaz Wizard-a za CA backup..... | 46 |
| Slika 68: prikaz kreiranih backup datoteka | 46 |
| Slika 69: prikaz export-a CA konfiguracija iz registry-a | 47 |
| Slika 70: prikaz DHCP backup-a..... | 48 |
| Slika 71: prikaz backup-iranih datoteka | 48 |
| Slika 72: pokretanje setup-a | 49 |
| Slika 73: upisati product key | 49 |
| Slika 74: odabrati Desktop Experience | 50 |
| Slika 75: instalirati Windows server 2019..... | 50 |
| Slika 76: instalacija VM tools-a | 51 |
| Slika 77: prikaz uspješne instalacije Windows server 2019 | 51 |
| Slika 78: prikaz dodanog SERVER3 poslužitelja u domenu i instalacija rola | 52 |
| Slika 79: restore CA certifikata..... | 52 |
| Slika 80: restoreDHCP konfiguracije | 53 |
| Slika 81: prikaz funkcionalnog DFS-a | 53 |

8. Reference

- [1] Dakić, V. (2017) Planiranje mrežne infrastrukture: priručnik za polaznike. 2. izd. Zagreb: Algebra d.o.o.
- [2] Dokumentacija aplikacije iSCSI Software Target (tutoriali, upute i sl.)
[http://technet.microsoft.com/en-us/library/gg232606\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/gg232606(WS.10).aspx)
- [3] Alternativa Microsoft servisu – StarWind iSCSI SAN Free Edition
<http://www.starwindsoftware.com/starwind-free-features>
- [4] Technet dokumentacija PowerShell komandleta za upravljanje iSCSI-jem
<https://docs.microsoft.com/en-us/powershell/module/iscsi/?view=win10-ps>
- [5] Konfiguracija Storage Spaces značajke (korak po korak upute) kroz PowerShell
<http://blogs.technet.com/b/josebda/archive/2014/04/01/step-by-step-formirroredstorage-spaces-resiliency-using-powershell.aspx>
- [6] Konfiguracija mehanizma za uklanjanje duplikata kroz PowerShell, pohrana podataka
<http://technet.microsoft.com/en-us/library/hh831434.aspx>
- [7] Vodič (tutorial) za postavljanje DFS klastera: <https://www.vembu.com/blog/distributed-file-system-dfs-windows-server-2016-briefoverview/>
- [8] Popis čestih pitanja s odgovorima (eng. FAQ) za Microsoft DFS:
<https://docs.microsoft.com/en-us/windows-server/storage/dfs-replication/dfs-faq>
- [9] Dokumentacija za RDC tehnologiju: <https://docs.microsoft.com/en-us/previous-versions/windows/desktop/rdc/remotedifferential-compression?redirectedfrom=MSDN>
- [10] Opis DAC-a: <https://docs.microsoft.com/en-us/windows/security/identity-protection/accesscontrol/dynamic-access-control>
- [11] Upute za konfiguraciju pomoći pri odbijenom pristupu, DAC:
<http://technet.microsoft.com/en-us/library/hh831402.aspx>
- [12] Technet dokumentacija i tutoriala WDS uloga: [http://technet.microsoft.com/en-us/library/cc771670\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc771670(v=ws.10).aspx)
- [13] Portal aplikacije Microsoft Deployment Toolkit - MDT, naprednijeg alata za deployment Windowsa: <http://technet.microsoft.com/en-us/solutionaccelerators/dd407791.aspx>
- [14] Opis metode Lite Touch Deployment, Microsoftove strategije za maksimalnu automatizaciju alatom MDT: [http://technet.microsoft.com/en-us/library/dd919179\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/dd919179(v=ws.10).aspx)
- [15] Mrežna instalacija putem WDS uloga na 44 računala:
<https://www.youtube.com/watch?v=K6CpqOxw2Ss>
- [16] Upute za implementaciju NLB-a u produkcijskom okruženju:
[http://technet.microsoft.com/en-us/library/cc754833\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc754833(v=ws.10).aspx)
- [17] Live Migration, Hyper-V: <https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/manage/livemigration-overview>
- [18] Hyper-V Replica: <https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/manage/set-uphyper-v-replica>
- [19] Primjeri Docker:
<https://github.com/MicrosoftDocs/VirtualizationDocumentation/tree/live/virtualization/windowscontainers>
- [20] Reference, docker: <https://docs.docker.com/engine/reference/builder/>
- [21] Opcije, docker: <https://docs.docker.com/engine/reference/commandline/build/>
- [22] Optimizacija, docker: <https://docs.microsoft.com/en-us/virtualization/windowscontainers/managedocker/optimize-windows-dockerfile?redirectedfrom=MSDN>
- [23] Docker RUN: <https://docs.docker.com/engine/reference/run/>

- [24]Technet dokumentacija Windows klaster: <https://docs.microsoft.com/en-us/windows-server/failover-clustering/failover-clusteringoverview>
- [25]Opis nadogradnje: <https://docs.microsoft.com/en-us/windows-server/upgrade/upgrade-overview>
- [26]Nadogradnja CA uloge: <https://techcommunity.microsoft.com/t5/itops-talk-blog/step-by-step-migrating-theactive-directory-certificate-service/ba-p/697674>