FUNDAMENTALNO SISTEMSKO ADMINISTRIRANJE

Benjak, Mihael

VELEUČILIŠTE U RIJECI

Mihael Benjak

FUNDAMENTALNO SISTEMSKO ADMINISTRIRANJE

(specijalistički završni rad)

Rijeka, 2018.

VELEUČILIŠTE U RIJECI

Poslovni odjel

Specijalistički diplomski stručni studij Informacijske tehnologije u poslovnim sustavima

FUNDAMENTALNO SISTEMSKO ADMINISTRIRANJE

(specijalistički završni rad)

MENTOR

Elvis Kukuljan, dipl ing.

STUDENT

Mihael Benjak

MBS: 2422000134/14

Rijeka, srpanj 2018.

VELEUČILIŠTE U RIJECI

Poslovni odjel

Rijeka, 11.06. 2018.

ZADATAK
za specijalistički završni rad

Pristupniku Mihael Benjak **MBS: 2422000134/14**

Studentu specijalističkog diplomskog stručnog studija Informacijske tehnologije u poslovnim sustavima izdaje se zadatak specijalističkog završnog rada – tema specijalističkog završnog rada pod nazivom:

Fundamentalno sistemsko administriranje

Sadržaj zadatka:

Fundamentalno administriranje, instalacija, konfiguracija, implementacija i održavanje, serverskog okruženja kroz starije i novije Windows Server operativne sustave u realnom i testnom okruženju primjenom teorijskog i praktičnog pristupa.

Preporuka _____

Rad obraditi sukladno odredbama Pravilnika o završnom radu Veleučilišta u Rijeci.

Zadano: 11.06.2018

Predati do: 11.07.2018

Mentor:

Elvis Kukuljan, dipl ing

Pročelnik odjela:

mr. sc. Golob Marino, predavač

Zadatak primio dana:

Mihael Benjak

Dostavlja se:
- **mentoru**
- **pristupniku**

I Z J A V A

Izjavljujem da sam specijalistički završni rad pod naslovom Fundamentalno sistemsko administriranje izradio samostalno pod nadzorom i uz stručnu pomoć mentora Elvis Kukuljana, dipl ing.

Mihael Benjak

(potpis studenta)

Sažetak

Ovaj diplomski rad obuhvaća osnovne pojmove, konfiguraciju, implementaciju i administriranje računalnog i serverskog sustava u praktičnom i teorijskom obliku. Za izradu ovog rada upotrijebljeno je virtualno okruženje pomoću alata „Oracle VM VirtualBox“ i realno okruženje jednog poduzeća. U radu su obuhvaćene najčešće korištene tehnologije i strategije za implementiranje i administraciju računalnog sustava srednje velikog poduzeća opisano kroz starije i novije Windows Server operacijske sustave (Windows Server 2008R2 i Windows Server 2012R2) te može poslužiti kao dobar temelj za usvajanje znanja za MCSA certificiranje u serverskoj infrastrukturi.

Ključne riječi: Windows Server, administrator računalnog sustava, MCSA, konfiguracija i implementacija računalnog sustava.

SADRŽAJ

1. Uvod

Serveri su računala na mreži koja pružaju usluge ostalim računalima na mreži. Serveri mogu imati razne operacijske sustave poput Windows Server OS, Ubuntu, Red Hat ili čak mogu biti obični klijentski operativni sustavi poput Windows XP. Serveri su u svakom poduzeću najvažnija stavka koja mora biti konstantno dostupna te je potrebno redovno održavanje kako ne bi zastali u radu. Na njima se pohranjuju najvažnije informacije nad kojima se rukovode gotovo svi informatički servisi jer su to uređaji koji su vrlo robusni, stabilni i znatno sigurniji od običnih korisničkih računala. Serverske komponente su znatno skuplje od običnog korisničkog računala zbog njihove kompleksnosti i robusnosti kao i *software*-ski paketi za servere, ali u suštini se ne razlikuju previše po osnovnim funkcionalnostima.

Cilj ovog diplomskog rada je uvesti čitatelje u osnovne pojmove sistemskog administriranja i serverske arhitekture kao i njihove osnovne funkcionalnosti u mreži da bi se ostvarila što bolja, sigurnija i konstanta razmjena podataka i informacija između korisnika i centralnog računala- servera. U radu su opisane osnovne funkcionalnosti, načini rukovođenja nekih serverskih rola, puštanje u pogon te sigurnosni mehanizmi praćenja serverskog zdravlja i osiguravanje konstantne dostupnosti za lokalne i udaljene korisnike. Obuhvaćene cjeline prikazane u radu opisane su kroz realno okruženje jednog poduzeća te sadrže povjerljive informacije koje su cenzurirane iz sigurnosnih razloga. Pojedini pojmovi nisu prevedeni iz originalnog izvora jer prevođenjem se gubi smisao i koncept značenja određenih pojmova.

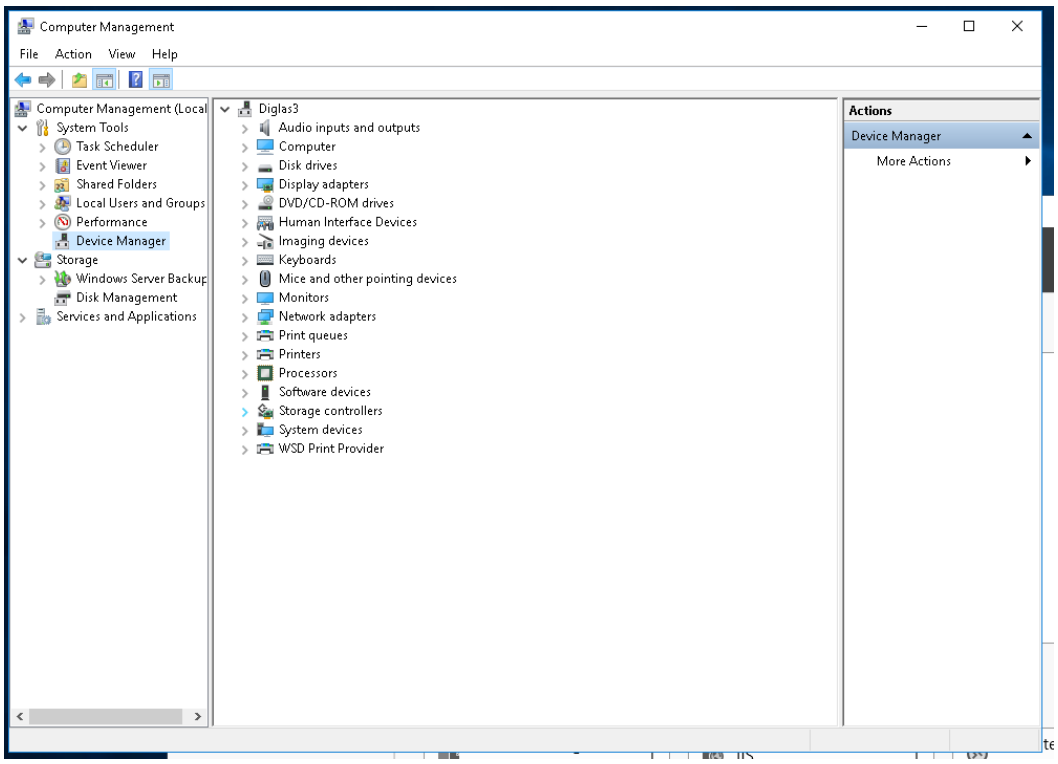
2. Upravljački programi

Upravljački programi (engl. „*Device Drivers*“) su *software*-ske komponente koje omogućuju komunikaciju *hardware*-skih uređaja sa operativnim sustavom. Upravljanje u serverskom okruženju gotovo je jednako kao i upravljanje nad osobnim računalom. Upravljački programi su programi napisani tako da operativni sustav prepozna konkretan uređaj te da mu se omogući međusobna komunikacija sa uređajem. Danas najčešće korišteni takozvani PnP (engl. *Plug and Play*) uređaji kojima nije potrebna ručna instalacija upravljačkih programa nego u svojoj *flash* memoriji imaju pohranjen program koji pokrene interakciju sa operativnim sustavom direktno iz samog uređaja.

Upravljački programi su dakle programi koji izvršavaju prijevod između samog fizičkog uređaja u Windows-u nativni jezik. Otkrivaju se pomoću „*Hardware ID*“ kojeg svaki uređaj posjeduje kao vlastiti identifikator pa se na osnovu toga provjerava u „.INF *file*“ upravljačkih programa ako odgovara samom uređaju te ako odgovara i samom operativnom sustavu, dozvoljava se instalacija uređaja na računalo. U serverskom okruženju administriranje nad upravljačkim programima je jedna od najlakših stavki za odraditi i održavati. Danas poznati upravljački programi u Windows okruženju su: .sws, .sys, .exe, .dll.

Postoje još zastarjele vrste koje se rjeđe koriste, a zovu se „*Legacy-non PNP* “ za koje je potrebno ručno pretraživanje za adekvatnim *software*-om te i sama instalacija. Najčešće takve vrste upravljačkih programa dolaze zajedno sa instalacijskim medijem (npr. CD., *Floppy Disk*…) ili ih je moguće preuzeti sa službenih web sjedišta proizvođača uređaja ili servera.

Slika 1. Konzola upravljanje uređajima

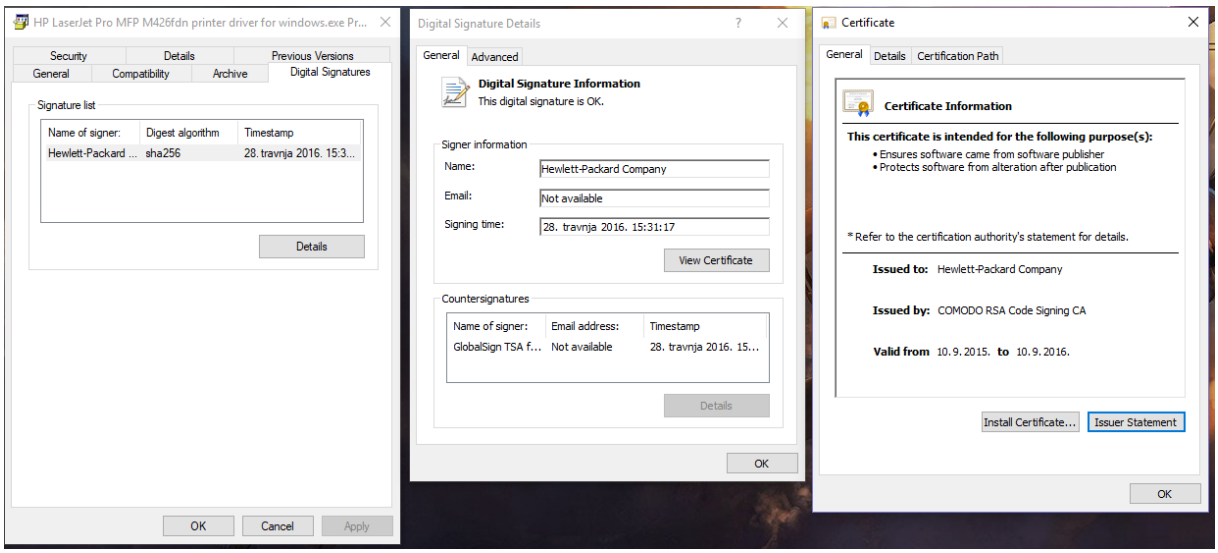


Izvor: Autor

Upravljački programi imaju mogućnost posjedovati potpisani i nepotpisani certifikat kao svojstvo. Potpisani upravljački programi sa važećim certifikatom su autorizirani paket *software*-a koje je dobavljač ili proizvođač potpisao certifikatom te da nisu naknadno prerađeni od neautorizirane osobe. To svojstvo programskog pokretača jedino se smatra stabilnim i sigurnim za serversko okruženje kao i za ostala računalna okruženja. Upravljački programi koji se naknadno prerađuju gube potpisani certifikat te ga nije moguće bez odobrenja proizvođača naknadno certificirati. Takvi nepotpisani upravljački programi nisu poželjni u realnom radnom okruženju jer mogu u najmanju ruku učiniti sustav nestabilnim, neupravljivim ili čak omogućiti zlonamjernim programima da se razvijaju u samoj serverskoj okolini i ostatku mreže. Dakle, prilikom preuzimanja upravljačkog programa potrebno je posebnu pozornost obratiti da li je preuzimanje izvršeno kod proizvođača te prije same instalacije provjeriti ako je upravljački program potpisan od strane samog proizvođača ili potvrđeno od strane Microsofta. Ukoliko korisnik nastavi sa instalacijom nepotpisanog upravljačkog programa, operativni sustav upozorava da postoji problem sa digitalnim certifikatom te traži suglasnost korisnika da svejedno instalira upravljački program. Programi od 3. stranke mogu sadržavati zlonamjerni sadržaj koji omogućuje

„*Backdoor entry*“ tj. pristup neautoriziranim aplikacijama i korisnicima u serversko okruženje poput „*Ransomware*“ virusa, „*Rootkit framework*“, „*Hijacked Computer*“ i ostalo.

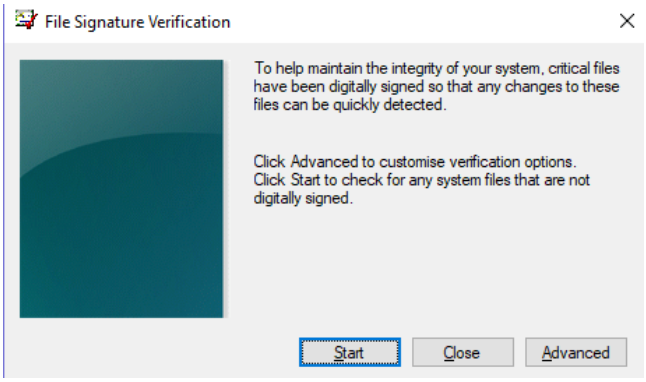
Slika 2. Pregled potpisa certifikata



Izvor: Autor

Alat „Sigverif.exe“ je aplikacija u Windows okruženju koja pregledava sve upravljačke programe na lokalnom računalu ili serveru za necertificiranim upravljačkim paketom te tako doprinosi rješavanju problema ukoliko se u sustavu nalazi neispravan ili čak zlonamjerni programski pokretač. Najjednostavniji način za pronalaženje ovog alata moguće je iz „*Start*“ izbornika ili „Pokreni“ dijaloga upisivanjem punog naziva alata zajedno sa njegovom ekstenzijom.

Slika 3. Alat „ Sigverif.exe"

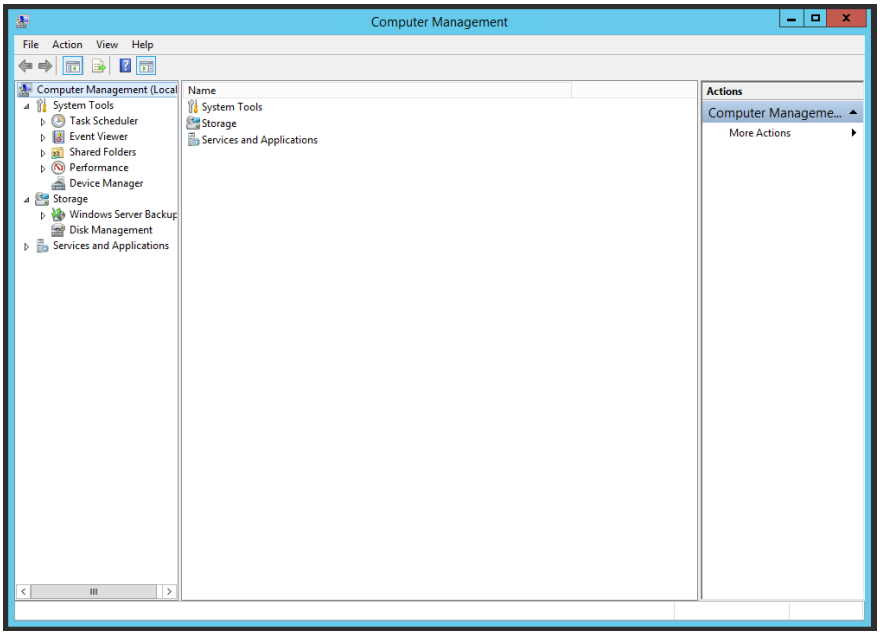


Izvor: Autor

3. Servisi

Jedna od najvažnijih serverskih komponenata su servisi. To su programi na računalima i serverima koji kontinuirano rade bez nadzora od samog pokretanja do gašenja uređaja te omogućuju serverske i računalne funkcionalnosti. Postoji i nekolicina servisa koji imaju mogućnost pokretanja kada je računalo i server isključeno poput „*Wake-on-lan*“ ili „*Schedule start up*“ koji se zapisuju u samom „BIOS-u“ računala te se pokreću na konkretan signal, poput impulsa na mrežnoj kartici kad dobije signal za paljenje ili u određenim vremenskim intervalima očitanih iz „BIOS“ sata koji je isprogramiran i odvija se u CMOS bateriji.

Slika 4. Pregled konzole upravitelj računala

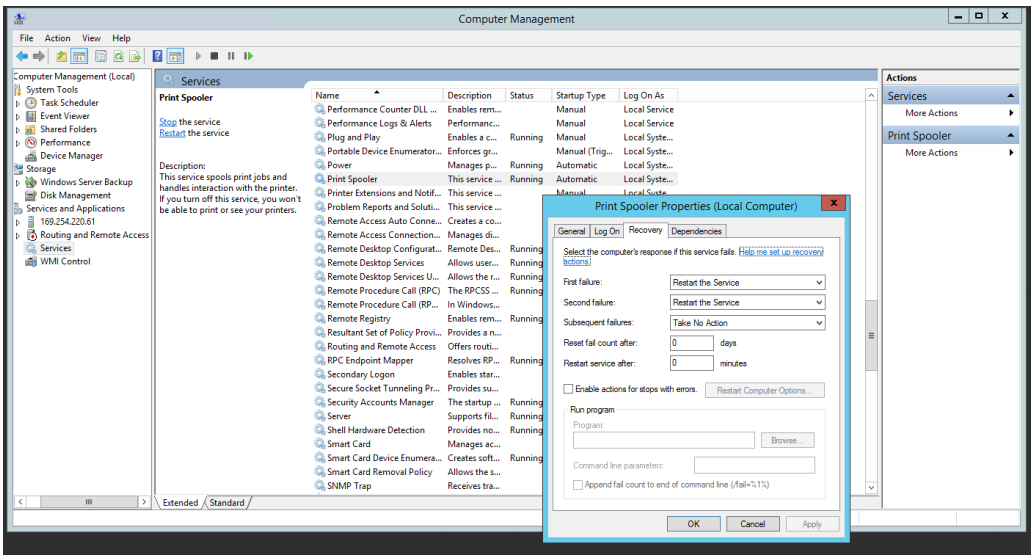


Izvor: Autor

Microsoft Windows posjeduje komponentu koja objedinjuje sve servise u jednoj konzoli pod nazivom „Microsoft Management Console“. Konzoli je moguće pristupiti putem pretraživanja punog naziva komponente „Services.msc“ ili pristupiti preko „Server manager“ konzole. Upravljanje nad servisima također moguće upravljanje putem „*Command Prompt*-a“ (skraćeno CMD). Primjer jedne naredbe u CMD: „NET STOP SPOOLER & NET START SPOOLER“. Ova naredba omogućuje ubrzano ponovo pokretanje tj. zaustavljanje i pokretanje

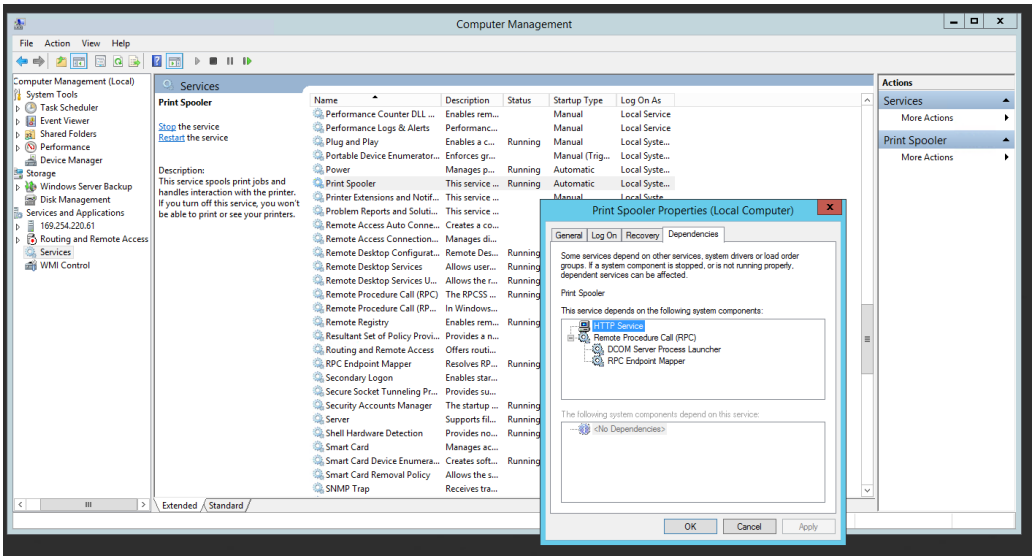
servisa „Spooler“ (puni naziv servisa je „Print Spooler“) koji je zadužen za komunikaciju operativnog sustava sa priključenim printerima.

Slika 5. Servisi i svojstvo oporavka servisa



Izvor: Autor

Slika 6. Pregled zavisnih servisa iz svojstava



Izvor: Autor

4. Instalacija

Prva faza u serverskom administriranju je sama instalacija servera i operativnog sustava. Potrebna je dobra priprema ovisno o potrebama za koje je server namijenjen kao i budući razvoj serverskog okruženja koji je proporcionalan razvoju organizacije u kojoj je smješten. Dobra priprema podrazumijeva preispitivanje potrebe, svrha, potencijalnih korisnika, koliko će se koristiti i u kojem smjeru vodi organizacija (npr. ako organizacija nema potrebu za geografsku ekspanziju u tom slučaju nije potrebno kupovati dodatne servere). Ovisno o svrsi, serveri se definiraju po svojim rolama, a to su: „Domain Controller“ (skraćeno DC), „Domain Name System“ (skraćeno DNS) , „Windows Internet Name Service“ (skraćeno WINS), „Dynamic Host Configuration Protocol“ server (skraćeno DHCP) , „File/Print server“, aplikacijski server, „Internet Information Server“ (skraćeno IIS), „Virtual Machine Server“ (skraćeno VMS, češće referenciran kao engl. „Host“) , „Itanium“ (serverska rola korištena za Datacentre), „Core“ (najprimitivniji oblik operativnog sustava koji posjeduje samo CMD u svojem sučelju što ga čini puno stabilnijim i sigurnijim), „Mail Server“, „Storage“ itd.

Slika 7. Data centar

Izvor: https://itpeernetwork.intel.com/data-center-design-tips, 1.2.2018.

Postoje razni načini koji pospješuju automatiziranu instalaciju Windows Server operativnog sustava. Jedna od mogućnosti je izrada slike (engl. „Image“) postojećeg sustava te ga replicirati na druge mašine. Najpopularniji alati za izradu slike replikacije su od proizvođača „Acronis“ i „Norton Ghost“. Drugi način je uporaba XML skripte smještene na prijenosni medij (najčešće USB *Flash* medij) koji se pokreće prema BOOT redoslijedu prije instalacijskog medija. XML skripta sadrži sve uvijete koje su potrebni za instalaciju, uključujući lokaciju instalacijskog medija, particioniranje, naziv računala, korisnika itd. Takav pristup se naziva „XML Unattended“ koji u potpunosti automatizira instalaciju servera.

Primjer:

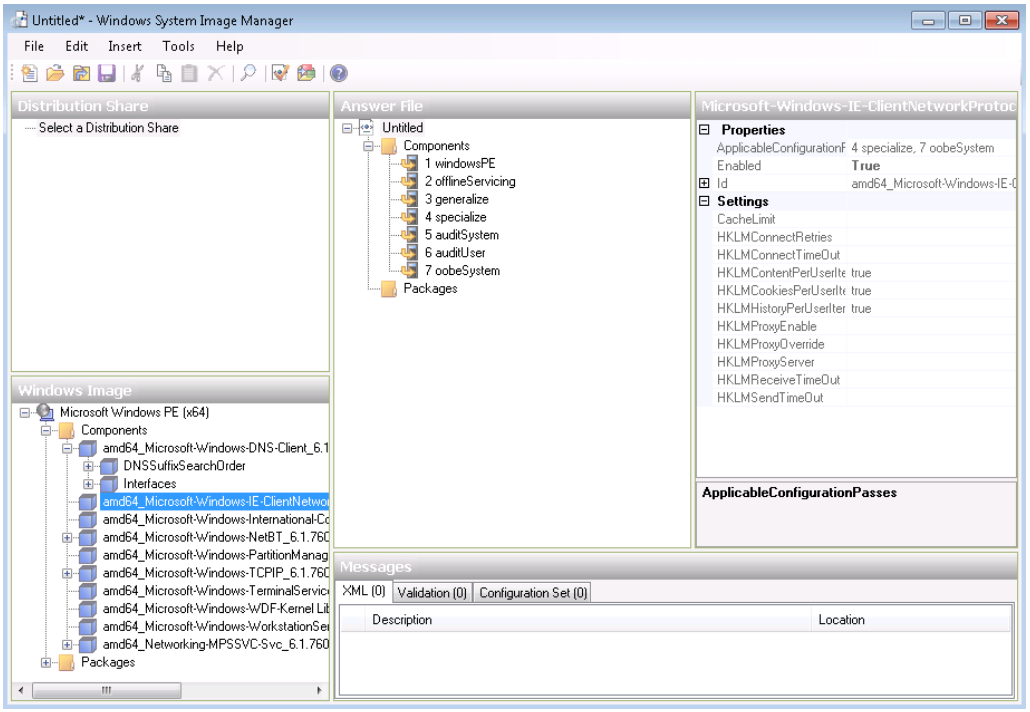
```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
   <settings pass="specialize">
      <component name="Microsoft-Windows-Deployment" processorArchitecture="amd64"
publicKeyToken="34b334f6ad355e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
         <ExtendOSPartition>
            <Extend>true</Extend>
         </ExtendOSPartition>
      </component>
      <component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64"
publicKeyToken="34b334f6ad355e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
         <ComputerName></ComputerName>
         <ProductKey>AAAAA-AAAAA-AAAAA-AAAAA-AAAAA</ProductKey>
         <RegisteredOrganization></RegisteredOrganization>
         <RegisteredOwner></RegisteredOwner>
         <TimeZone>Central Standard Time</TimeZone>
      </component>
      <component name="Microsoft-Windows-UnattendedJoin" processorArchitecture="amd64"
publicKeyToken="34b334f6ad355e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
         <Identification>
            <Credentials>
               <Domain>my_domain</Domain>
               <Password>password</Password>
               <Username>domain_admin</Username>
            </Credentials>
            <JoinDomain>my_domain</JoinDomain>
         </Identification>
      </component>
   </settings>
   <settings pass="oobeSystem">
      <component name="Microsoft-Windows-International-Core" processorArchitecture="amd64"
publicKeyToken="34b334f6ad355e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
         <InputLocale>en-US</InputLocale>
         <SystemLocale>en-US</SystemLocale>
         <UILanguage>en-US</UILanguage>
         <UserLocale>en-US</UserLocale>
      </component>
```

```
      <component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64"
publicKeyToken="34b334f6ad355e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
        <OOBE>
          <HideEULAPage>true</HideEULAPage>
          <HideOEMRegistrationScreen>true</HideOEMRegistrationScreen>
          <HideOnlineAccountScreens>true</HideOnlineAccountScreens>
          <HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>
          <NetworkLocation>Work</NetworkLocation>
          <SkipMachineOOBE>true</SkipMachineOOBE>
          <SkipUserOOBE>true</SkipUserOOBE>
          <HideLocalAccountScreen>true</HideLocalAccountScreen>
        </OOBE>
        <UserAccounts>
          <LocalAccounts>
            <LocalAccount wcm:action="add">
              <Password>
                <Value>ABCabcABCabcABCabcABCabcABCabcABCabc=</Value>
                <PlainText>false</PlainText>
              </Password>
              <Description>admin</Description>
              <DisplayName>admin</DisplayName>
              <Group>Administrators</Group>
              <Name>admin</Name>
            </LocalAccount>
          </LocalAccounts>
        </UserAccounts>
        <RegisteredOrganization>My Org</RegisteredOrganization>
        <RegisteredOwner>My Org</RegisteredOwner>
      </component>
    </settings>
    <cpi:offlineImage cpi:source="wim:c:/users/admin/desktop/install.wim#Windows 10 Pro" xmlns:cpi="urn:schemas-microsoft-
com:cpi" />
</unattend>
```

Izvor primjera: https://gist.githubusercontent.com/jacobsalmela/8d4a3084dd34719e5888eba43138bfc5/raw/ffcedfa24fff0e593715906dc35dee8822e6b415/unattend.xml 3.3.2018.

Jedan od načina repliciranja instalacija je putem alata na Windows Server operativnom sustavu pod nazivom „*System Image Manager*“ zajedno sa rolom „Windows Deployment Services“ koji imaju mogućnost izrade slike sustava i replicirati je putem mreže. Za ove potrebe nužno je prethodno zadati mašini *BOOT* poredak tako da je „PXE BOOT“ prvo svojstvo ili definiranje matičnog servera sa spremnom instalacijom. Kod čistih instalacija fizičkih servera koriste se automatizirani *software*-ski paketi poput „IBM“ alata „Server Guide“ koji u svojoj inicijalizaciji pregledava sve funkcionalnosti, upravljački programi, *firmware* i ostale postavke na samom serveru, pohranjuje ih na radnu memoriju radi naknadnog vraćanja istih te nakon toga izvršava čistu instalaciju Windows operativnog sustava.

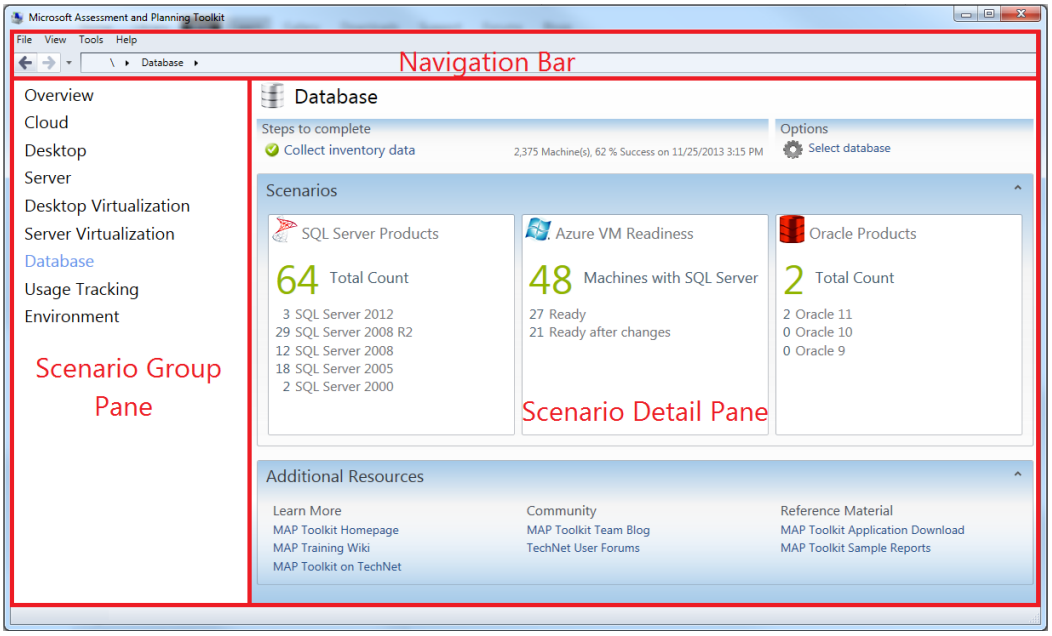
Slika 8. Alat „System Image Manager"



Izvor: https://4sysops.com/wp-content/uploads/2010/02/WindowsSystemImagerManager.png, 5.4.2018.

Također moguće je izvesti nadogradnju postojećeg sustava na noviji operativni sustav koji zadržava uglavnom sve funkcionalnosti i podatke koji se nalaze na postojećem sustavu. Neke funkcionalnosti se moraju ponovo definirati zbog njihove razlike u verzijama ili načinu pristupanja. Za nadogradnju potrebno je provjeriti ako postojeća mašina i operativni sustav podržavaju sve uvjete za nadogradnju. Alat „Maptoolkit“ omogućuje pregled trenutačnog stanja i provjerava koje su sve mogućnosti nadogradnje, koji uvjeti nisu podržani te koje promjene će se dogoditi na serveru nakon nadogradnje. Za nadogradnju starijih sustava poput W2003 (skraćeno za „Windows Server 2003“) na W12R2 potrebno je izvesti inkrementalnu nadogradnju svih Windows verzija po redoslijedu objavljivanja. Dakle, prva nadogradnja na W2008 pa zatim na W2012 te na kraju na W2012R2. Minimalni zahtjevi za instalaciju Windows Server W2012R2 su procesor sa najmanje 1.4Ghz frekvencije, 64bit arhitektura, 512MB prostora na radnoj memoriji te 32GB diskovnog prostora.

Slika 9. Alat „Microsoft Assessment and Planning Toolkit"

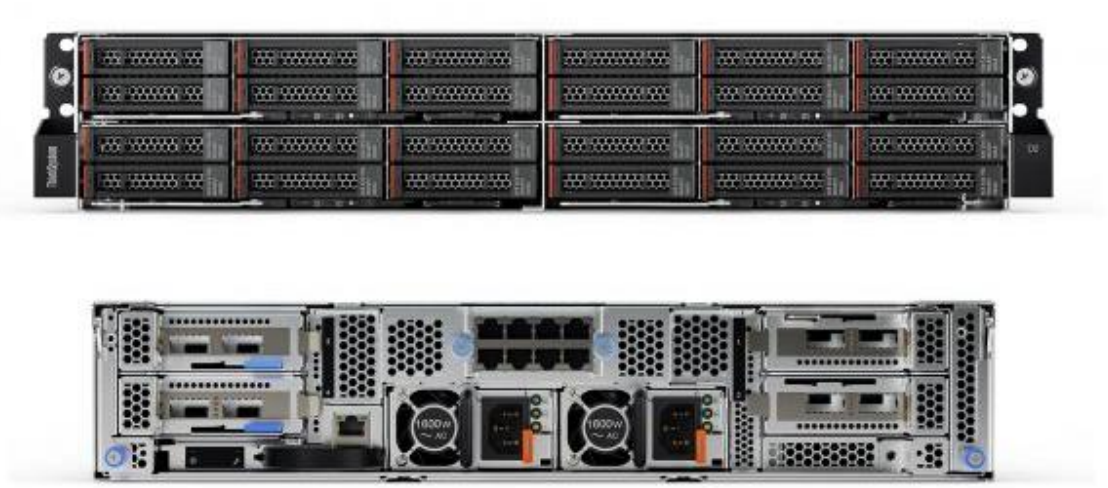


Izvor: https://social.technet.microsoft.com/wiki/contents/articles/21689.navigating-the-map-toolkit.aspx, 6.3.2018.

Jeftinija varijanta operativnog sustava „Windows Server Core“ koristi se najčešće na serverima nad kojima nema prevelike potrebe za izmjenama i upravljanjima već se koriste kao podloga za ostale servise i role poput DC,DNS,DHCP,File,Print ili čak kao *Host* za virtualne mašine. Neke od najčešći komandi koje administratori koriste na Core Serverima u CMD su: „netsh“, „netdom“, „slmgr“,“ocsetup“, „winrs/winrm“,“remote mmc“…

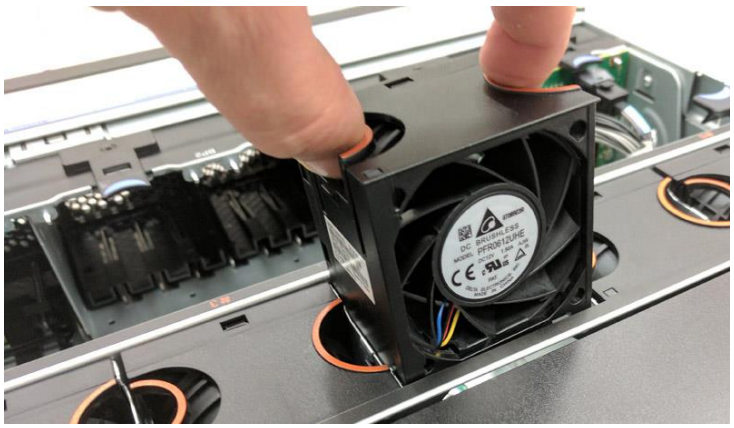
Skuplja varijanta za serversko okruženje koja zahtjeva više dostupnosti i upravljivosti nad grafičkim sučeljem te koja će posjedovati više serverskih rola je Windows Server Enterprise edicija koja ima mogućnost postavljanja multi-server *cluster* arhitekture. *„Hot swap“* je fizičko svojstvo na serverima koja omogućava vađenja i dodavanja *hardware*-skih komponenti poput radne memorije, jezgre ili diskova dok su serveri u uključeni i u radu.

Slika 10. Primjer fizičkog servera sa Hot i Cold Swap komponentama



Izvor: http://www.itpro.co.uk/server-storage/30208/lenovo-thinksystem-sd530-review , 7.3.2018.

Slika 11. Lako zamjenjiva komponenta



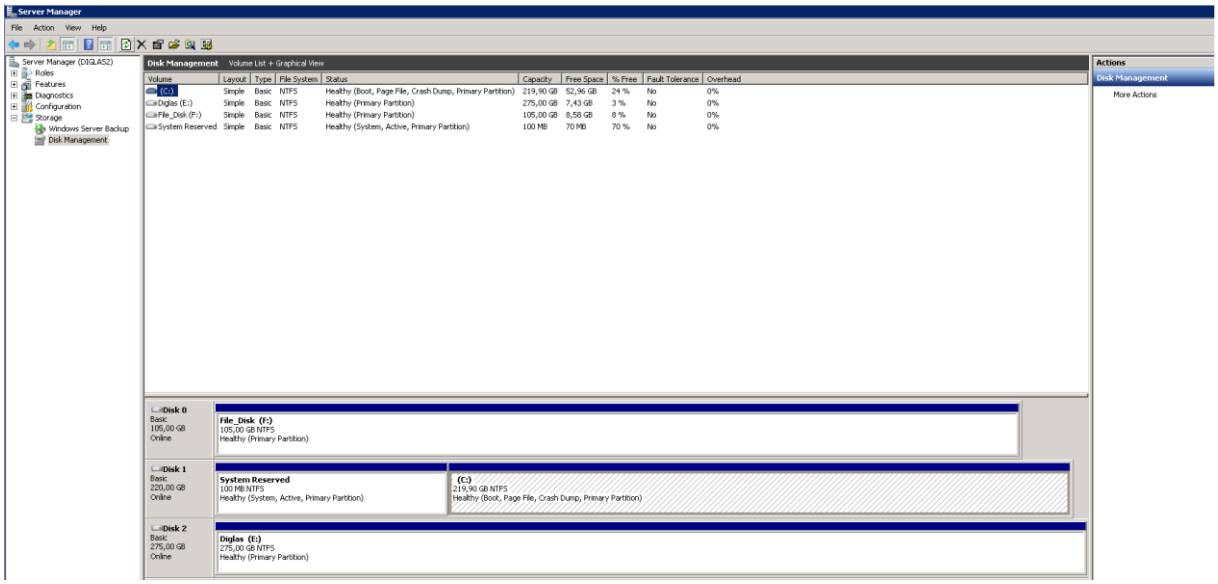
Izvor: https://www.servethehome.com/lenovo-system-x3650-m5-workhorse-2u-server-review/lenovo-x3650-m5-hot-swap-fans , 7.3.2018.

Firmware (tzv. „*on circuit programing"*) je set programa sličnih upravljačkim programima koji se zapisuju u *flash* memoriji *hardware*-skih komponenti kao npr. na „Raid controller" karticu , „Chipset", „BIOS", mrežnu karticu, a služe kao izvorni programi za pokretanje i komunikaciju komponenata sa operativnim sustavom te međusobnu razmjenu informacija.

4. Particioniranje

Particioniranje (engl. Particioning) je važno svojstvo kod instalacije operativnog sustava koji definira kako će se raspodijeliti i odvajati prostor na raspoloživim diskovima. Particije koje se primarne moraju biti definirane kao aktivne particije inače nije moguće izvesti instalaciju sustava. Postupak definiranja aktivne particije podešava se automatizmom prilikom instalacije i izabire se particija na koju će se izvršiti instalacija. Suvremene instalacije serverskog sustava podrazumijevaju instalaciju GPT vrstu particioniranja što omogućuje do 128 particija i preko 2TB diskovnog prostora što nije bilo moguće prema prethodnom MBR principu. Prilikom particioniranja, sustav odvaja barem 100MB prostora sa aktivne particije i smješta ga ispred sebe. U tih 100MB nalazi se tzv. „Partition Table“ koji je zadužen za pravilno pokretanje operativnog sustava. Svrha ovog pristupa jest da omogući disku da se može zaključati protiv krađe putem „BitLocker-a“ koji kriptira sav diskovni prostor osim „Partition Table“ particiju koja inače nebi bila čitljiva prilikom *BOOT*-anja sustava.

Slika 12. Pregled diskova i particija



Izvor: Autor

5. Aplikacijski serveri

Kao što samo ime govori služe kao serveri na kojima se smješta i upravlja nad aplikacijom. Postoje razne vrste aplikacijskih servera poput „Mail servera“, „Database server“, „Collaboration server“ , „System Center Opertaion Manager“, „Threat Management“ i ostale radne aplikacije poput raznih ERP i BI alata. *Mail* server upotrebljava se kod većih poduzeća, a najčešće korišten MS Exchange. Kod manjih poduzeća postoje „*Cloud“* rješenja poput Office365 Exchange koji omogućuje kupnju određenog broja mail licenci ili kupnja određenih licenci MS Exchange *mailova* kod 3. stranke.

Baza podataka je glavna informatička komponenta svakog poslovanja koja zahtjeva adekvatnu pohranu i skladištenje za što je potreban *Database* server za velike količine podataka. Ovaj server je od najveće važnosti i vrijednosti jer sadrži sve važne i relevantne informacije te zbog toga je potrebno odrađivanje redovitih *Backup-a* i omogućiti najveću dostupnost (engl. High availability). Najbolji primjer *Backup*-a je po „3-2-1-Backup“ principu: sveukupno 3 kopije, 2 na različitim medijima i 1 izvan lokacije. Najčešći korišten *Database* server su Oracle *database* server, a SQL serveri su Mssql server i Mysql.

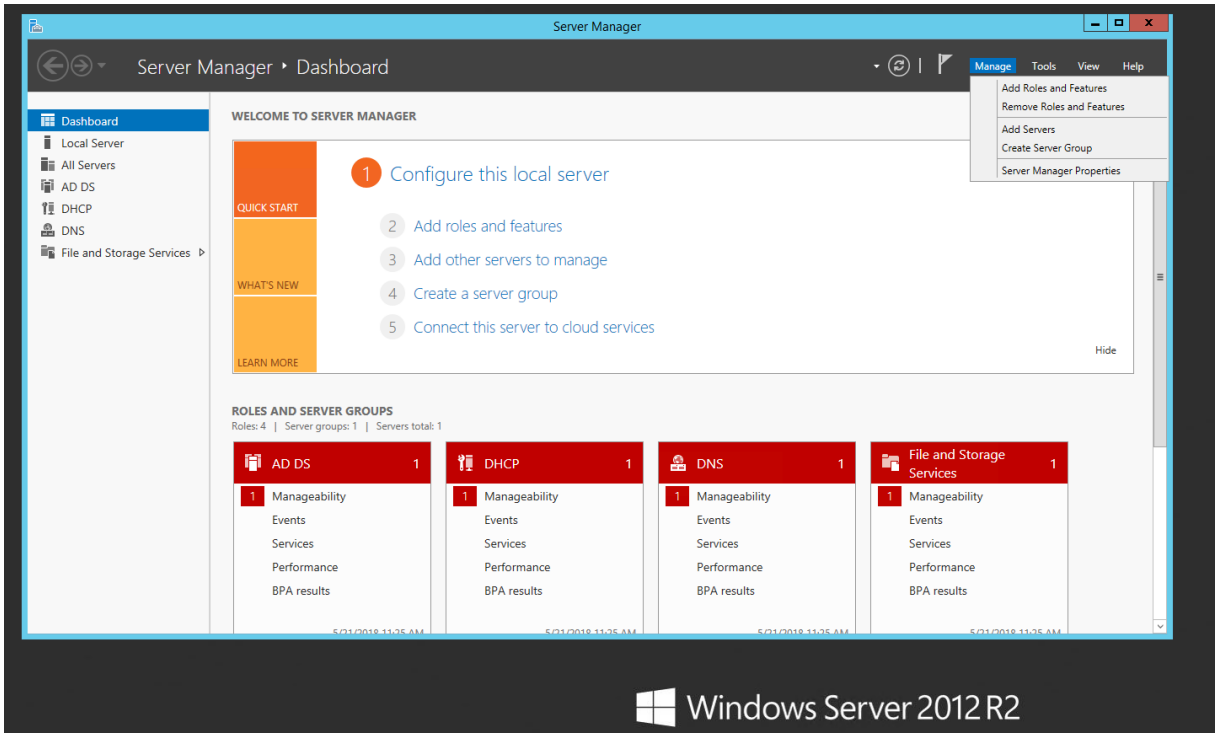
Collaboration serveri su najčešće korišteni kod *developer*-a zbog mogućnosti međusobne razmjene podataka i zajedničkog rada na istim projektima, kao i za Sharepoint servis od Microsofta kojeg koriste razna poduzeća. Takvi serveri uglavnom su *web* bazirani na lokalnoj i/ili globalnoj razini.

„System Center Operations Manager“ je menađment konzola koja brine za fizičko i virtualno stanje servera te vodi evidenciju svih događaja. Zahtjeva pristup Sql serveru da može zapisivati svoje događaje i *logove*. Posjeduje funkciju obavještavanja o bitnim i praćenim događajima, alarmira korisnika ili šalje obavijesti na unaprijed definiranu mail adresu.

6. Serverske role i značajke

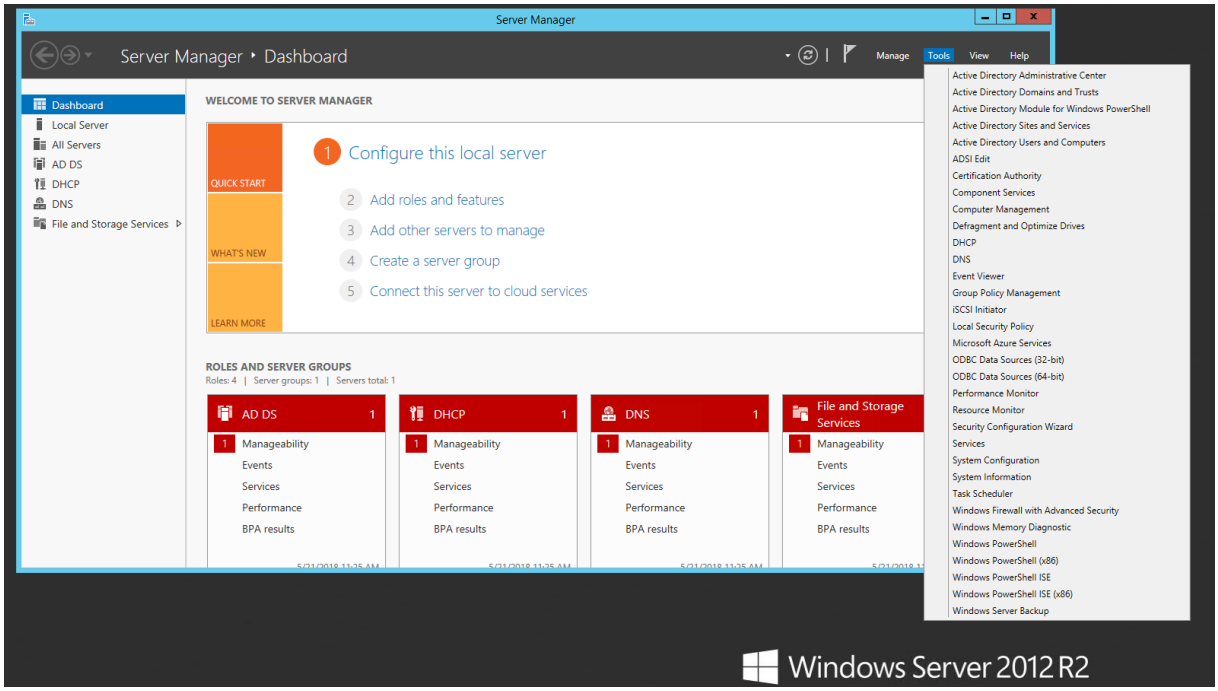
Serverske role (engl. *Roles*) su uloge *software*-skih paketa ili komponente koje omogućuju serverima izvršavanje određenih funkcionalnosti. To se odnosi na ostale servere, računala i korisnike. Serverima se može dodijeliti više uloga, npr. može biti i DC i DNS server. Značajke (engl. *Features*) su *software*-ske komponente koje omogućuje dodatne značajke određenim rolama. *Role* and *features* dodaju i izmjenjuju se putem *Server Manager* konzole.

Slika 13. „Server Manager“ konzola



Izvor: Autor

Slika 14. Pregled alata u „Server Manager“ konzoli



Izvor: Autor

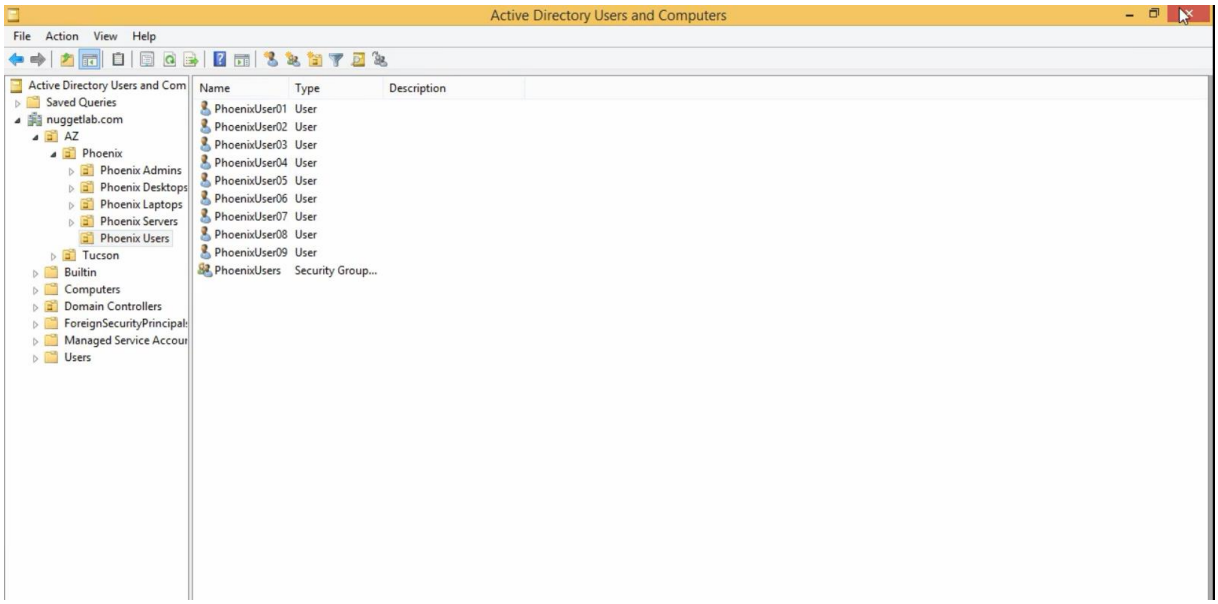
„*Remote Desktop Services*“ (skraćeno RDS) je serverska rola bolje poznata pod nazivom „Terminal Services“ te omogućava veći broj simultanih konekcija na isti operativni sustav. *Remote Access* (prevedeno: udaljeni pristup) je vrlo produktivan i jednostavan način za pristupanje serveru i lokalnoj mreži iz bilo koje lokacije. Najveća značajka je ušteda na vremenu i mogućnost rada direktno na serveru. Zadani *port* za udaljeni pristup je 3389. „Remote desktop gateway“ je serverska rola koja omogućuje autoriziranim korisnicima konekciju putem Interneta bez potrebe korištenja VPN konekcije. Koristi SSL *port* 443 na vatrozidu (engl.Firewall) koji je otvoren po zadanim postavkama. Korištenje HTTPS porta 443 stvara svojevrstan zaštitni tunel kao sigurnosna mjera od presretavanja.

„WINRM“ je mogućnost upravljanja nad serverom kojom se upravlja iz CMD konzole sa udaljenog računala ili servera. Konekcija ide putem HTTPS protokola. Najčešće je korišten u Windows core server ediciji. Nije praktičan zbog potrebnog izvrsnog poznavanja komandi u CMD-u.

„RSAT“ je mogućnost potpunog upravljanja nad serverom preko klijentskog računala.

Eliminira potrebu prisutnosti nad serverom. Potrebna je instalacija „Remote Server Administraton Tools“ alata za korisničko računalo koje će vršiti konekciju sa serverom te imati mogućnost menađmenta nad serverom. Koristan je zbog mogućnosti objedinjavanja kompletnog server *pool*-a na jednom mjestu te također i za Core instalacije koje nemaju svoje sučelje.

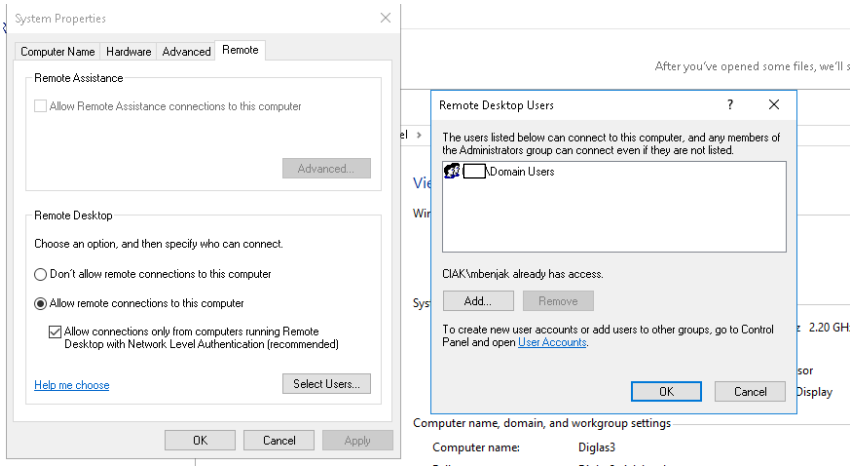
Slika 15. Pregled „Active Directory Users and Computers"



Izvor: Video tutorial, CBT Nuggets Microsoft Windows Server 2012 R2 70-410, 06. Introduction To Active Directory And Basic Installation

Prvi korak u konfiguraciji udaljenog pristupa potrebno je na serverskom okruženju dozvoliti pristup iz svojstava sustava (engl. „System Properties“) te odabirom na „Allow remote connections on this computer“ te definirati korisnike koji mogu pristupiti samo putem „Network Level Authentication“. Unutar dijaloga „Select Users“ odabiru se domenski korisnici što znači da pristup imaju samo korisnici koji su dio domene.

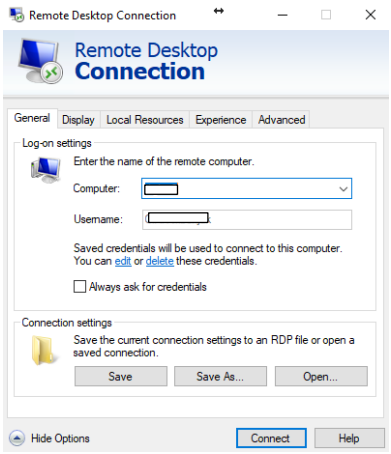
Slika 16. Uključivanje udaljenog pristupa iz svojstva sustava i autorizirani korisnici



Izvor: Autor

Na korisničkom računalu potrebno je konfigurirati konekciju. Konekcija udaljenih ručanala vrši se putem „mstsc.exe“ alata odnosno „Remote Desktop Connection“. U prvom tabu pod kategorijom „*General*“ definira se odredišno računalo na koje se vrši konekcija te se upisuju domena i korisničko ime. Navedenu konekciju moguće je pohraniti kao prečac na računalu odabirom „Save As…“ . „Save“ opcija pohranjuje sve promjene napravljene na konkretnom prečacu konekcije, dok opcija „Open“ otvara jednu od već prethodno pohranjenih prečaca.

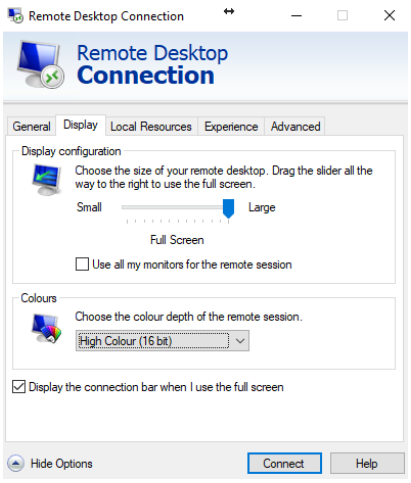
Slika 17. Opće postavke udaljene konekcije RDC



Izvor: Autor

U drugom tabu pod kategorijom „Display“ definira se kako će se grafički konekcija prikazivati na računalu. Postoji mogućnost izbora rezolucije prozora te kvalitetu prikaza boja.

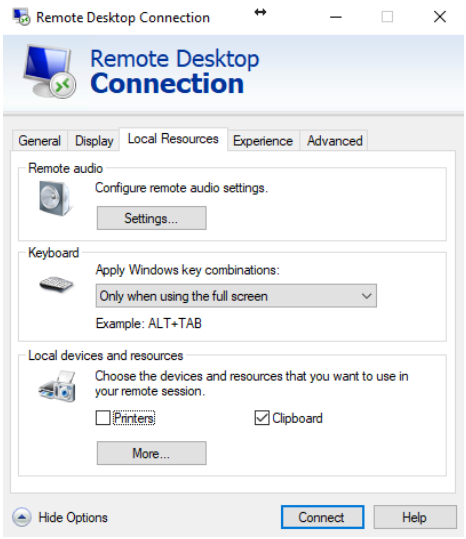
Slika 18. Grafičke postavke RDC



Izvor: Autor

U trećem tabu pod nazivom „Local Resources“ definiraju se resursi sa lokalnog računala koji se prenose u serversko okruženje poput lokalno instaliranog printera, način na koji se prenose komande sa tipkovnice ili zvučne postavke.

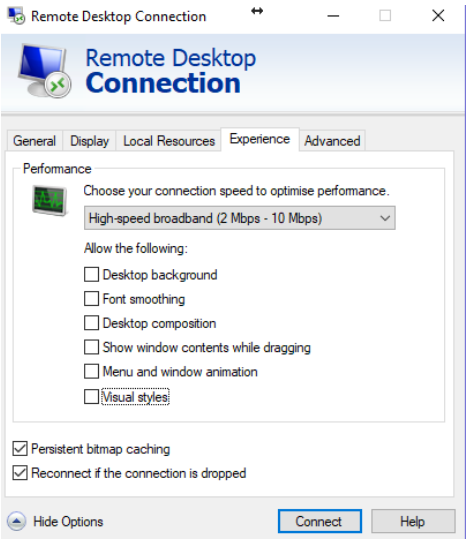
Slika 19. Lokalni resursi u RDC



Izvor: Autor

Četvrti tab „Experience“ definira performanse korisničkog rada u RDC konekciji. Izborom brzine prijenosa podataka i dodatnih stavki utječe na konačno korisničko zadovoljstvo u samom radu u serverskom okruženju.

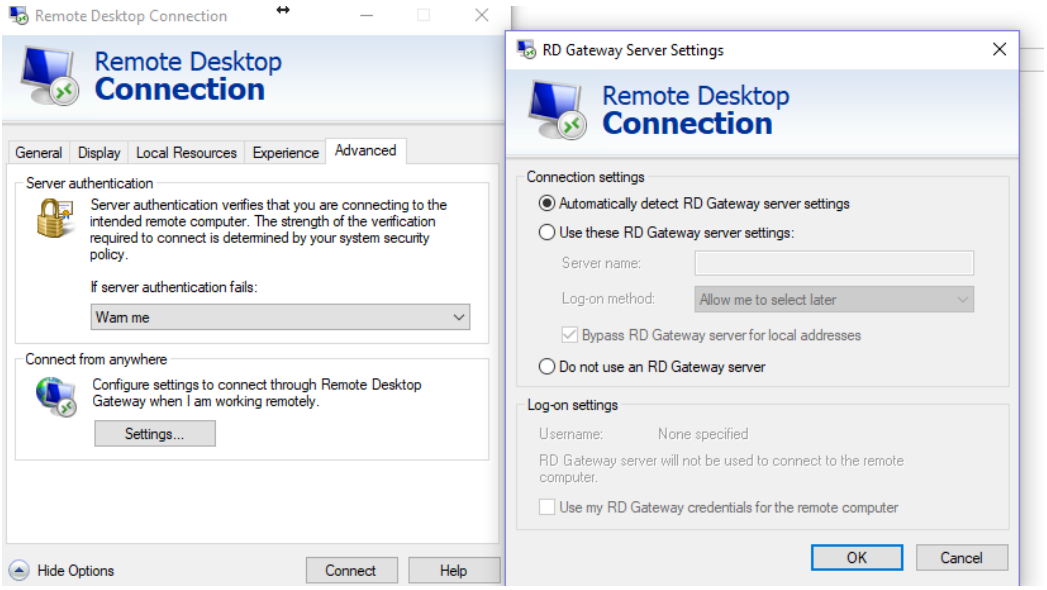
Slika 20. Korisničko iskustvu u RDC



Izvor: Autor

Peta stavka „Advanced“ definira dodatne postavke o uspostavljanju konekcije kao npr. definiranje Remote Desktop Gateway od kojeg servera će se koristiti postavke.

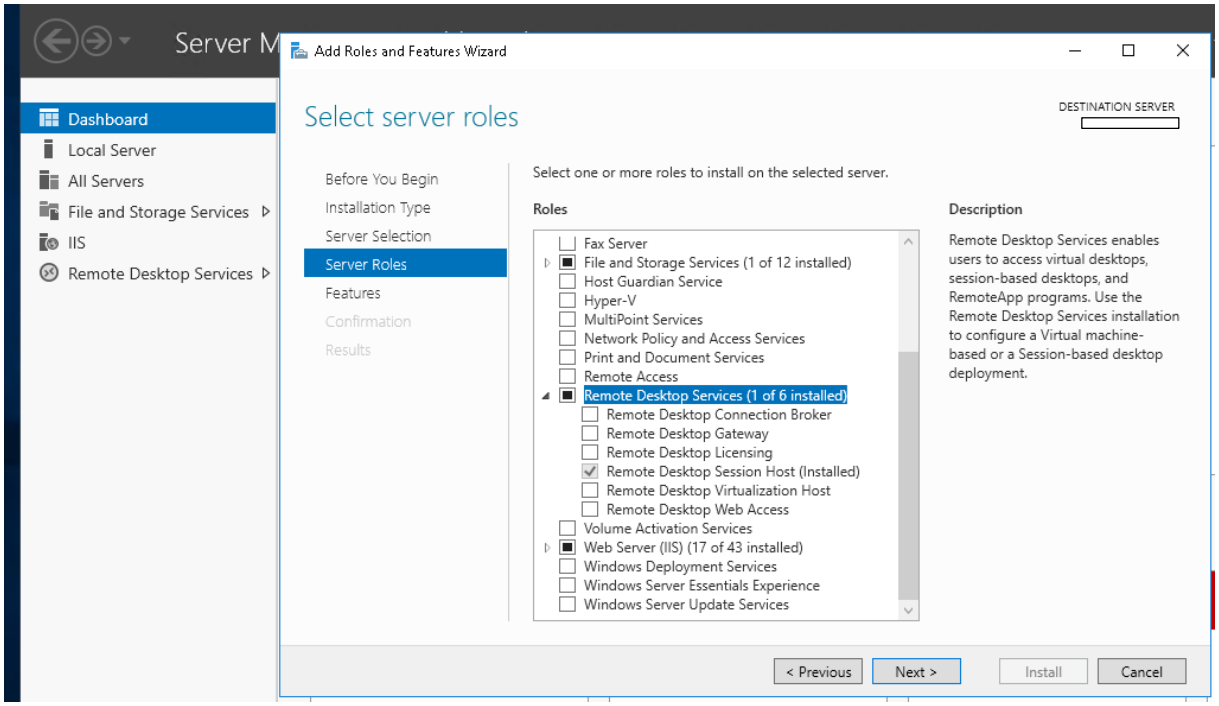
Slika 21. Napredne postavke RDC



Izvor: Autor

Instalacija tzv. „Terminal servis“ kao serversku rolu (engl. „*Remote Desktop Services*“) omogućava veći broj konekcija na jedan server i omogućuje „*Remote Desktop Gateway“*. „*Remote Desktop Gateway“* omogućuje konekcije putem interneta gdje nije potrebna VPN konekcija već koristi SSL *port* 443 po zadanim postavkama. Iz *Server Manager* konzole potrebno je dodati novu role pod nazivom „Remote Desktop Services“. Unutar te role nalaze se dodatne role koje dolaze zajedno sa RD servisima, a to su: Remote Destkop Connection Broker, RD Gateway, Licensing, Session Host, Virtualization Host i Web Access.

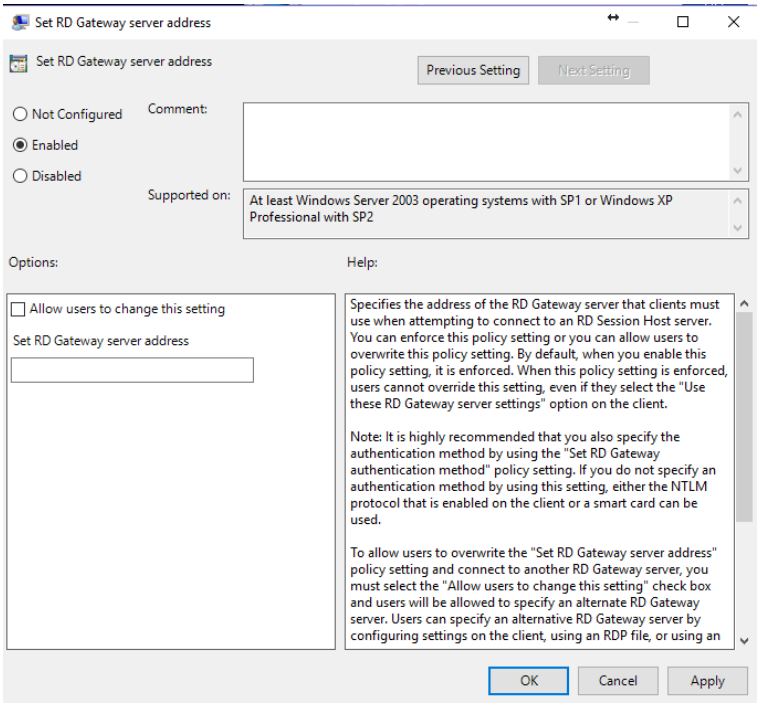
Slika 22. Dodavanje role



Izvor: Autor

„*Remote Desktop Connection Broker*“ omogućuje korisnicima re-konekciju na njihove postojeće sesije. Ujedno služi i za balansiranje opterećenja ako postoji više servera. „Remote Desktop Session Host“ je obavezan u konfiguraciji „Remote desktop“ role koji je ujedno i sama jezgra za terminalno spajanje više korisnika. „Remote Desktop Virtualization Host“ služi za RDC konekcije na Virtualne mašine. „Remote Desktop Licensing“ služi za praćenje licenci tj. broj korisnika koji ima dozvolu za spajanje. Licence se mogu kupovat zasebno i nazivaju se CAL-ovi (engl. Client Access Licence) i mogu se definirati kao korisničke licence ili licence za količinu uređaja. „Remote Desktop Web Access“ omogućava pristup putem *web* preglednika. „Remote Desktop Gateway“ omogučava konekciju putem Interneta bez potrebe za VPN konekcijama, definira tko se može *konektirati* i na koje servere. Kod postavljanja servera kako bi bio dostupan izvana potrebno je definirati u *Group Policy*-u pod *User Configuration, Administrative Templates, Windows Components, Remote Desktop Services* te unutar *RD Gateway* komponente „Set RD Gateway server address“ koja ima javnu IP adresu ili naziv servera koji je dostupan za RD Gateway.

Slika 23. Definiranje „RD Gateway“ adrese



Izvor: Autor

VPN (engl. Virtual Private Network) je skraćeni naziv za tzv. tuneliranje ili ostvarivanje sigurne konekcije između 2 uređaja preko interneta putem virtualnog tunela. Instalacija se vrši na Domain Controlleru. Potrebno je instalirati rolu pod nazivom „Network Policy and Access Services“. Tuneliranje omogućuje enkapsulaciju paketa na različite načine,a to su: PPTP, L2TP, SSTP, IPsec, IKEv2.

PPTP, L2TP, i SSTP definirani su po PPP (engl. Point to Point) protokolu koji prenosi enkapsulirane PPP pakete po PPP mreži te ujedno nije podržan IKEv2 protokolom. PPTP omogućava enkripciju i enkapsujaciju u IP zaglavlju koja se prenosi po javnoj mreži te se na odredištu dekriptira što znači da nema potrebe za javnim ključem. Nedostatak ovog protokola je što nema svojstvo podatkovnog integriteta odnosno nedostatak informacije ako je paket u procesu prijenosa izmijenjen. IKEv2 je protokol koji omogućava otpornost konekcije kada korisnik mijenja pristupnu mrežu. Koristi UDP *port* 500 te vrlo snažnu enkripciju.

7. Print servisi

Pisaći se mogu grupirati u dvije skupine: lokalni i mrežni. Lokalni pisaći su smješteni unutar lokalne mreže. Mogu biti direktno vezani na server ili na klijentskom računalu. Kada se instalira lokalni pisać potrebno ga je dodati u *Active Directory* iz njegovih svojstava, opcijom pod „*Sharing*“ tabom izborom na „list in directory“ (ovaj postupak je uglavnom automatiziran). Mrežni pisaći su spojeni na mrežu te ih je potrebno instalirati na serveru, zatim omogućiti im dijeljenje pisaća na mreži te na kraju instalirati i na klijentskom računalu. Ovom metodom se eliminiraju najveće greške u komunikaciji servera i print servera. Potrebno je da se naziv pisaća i upravljačkog programa zove isto na serveru i klijentskom računalu da se izbjegnu greške u komunikaciji.

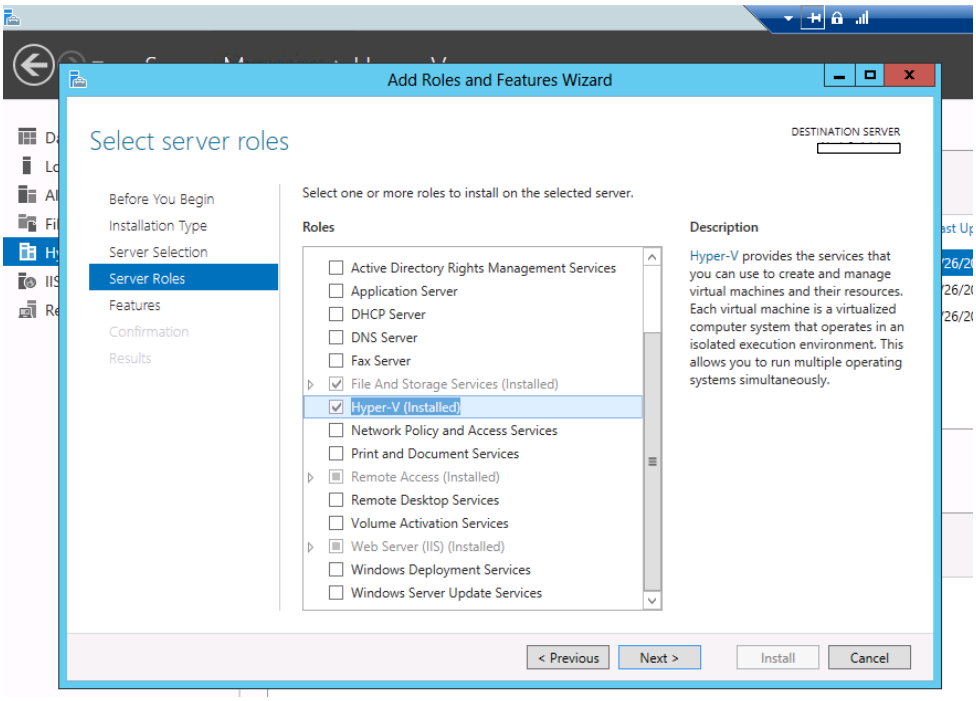
Također moguće je izvesti distribuiranu instalaciju pisaća putem GPO (engl. „Group Policy Object“) tako da se pristupi *Group Policy Management* konzoli, pod izbornikom *Policy*-izvršava se *edit*; *computer configuration, policies, windows settings, deploy printers- browse printer and add*. Zbog velikog broja *Terminal Service* konekcija sa raznih lokacija i raznolikim rasponom pisaća koji su u upotrebi, najjednostavnije rješenje je upotreba alata 3.stranke poput TS PRINTA, koji ukida potrebu za upravljanje i instalaciju nad svakim printerom da korisnik može ispisivati iz serverskog okruženja na svojem lokalnom računalu putem RDC konekcije.

8. Virtualizacija

Virtualizacija je jedna od fundamentalnih serverskih svojstava i operacija koja omogućava uštedu vremena, financija i posjeduje svojstvo visoke dostupnosti jer omogućava postavljanje više virtualnih sustava na istom fizičkom serveru. Princip rada osnovan je na MS Hyper-V programu koji na sebi drži sve operativne sustave preko jednog domaćina te stvara VHD objekt za svaki server. VHD (engl. „Virtual Hard Disk“) je virtualni dio na HD-u rezerviran samo za njegovu virtualku.

Postoje i drugi *hipervizori* od drugih proizvođača: VMware (workstation,fusion, esx server) i Parallels su najpopularniji. Virtualne mašine se obično postavljaju na „čiste“ *Host* servere te im se dodaje server rola „Hyper-V“.

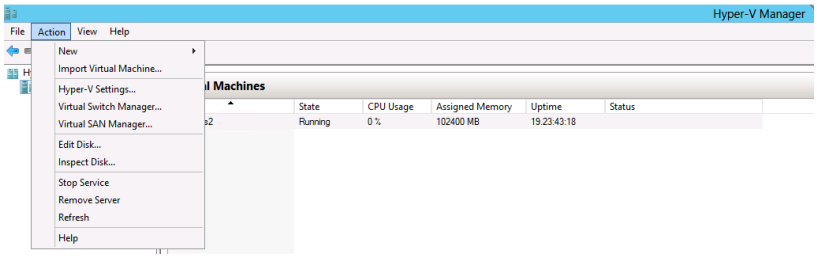
Slika 24. Dodavanje server role Hyper-V



Izvor: Autor

Nakon uspješne instalacije role vrši se instalacija virtualnih sustava iz Hyper-V Manager konzole. Konzola ima opcije dodavanja, uvoženja, konfiguracije virtualki, konfiguracije diskova, itd.

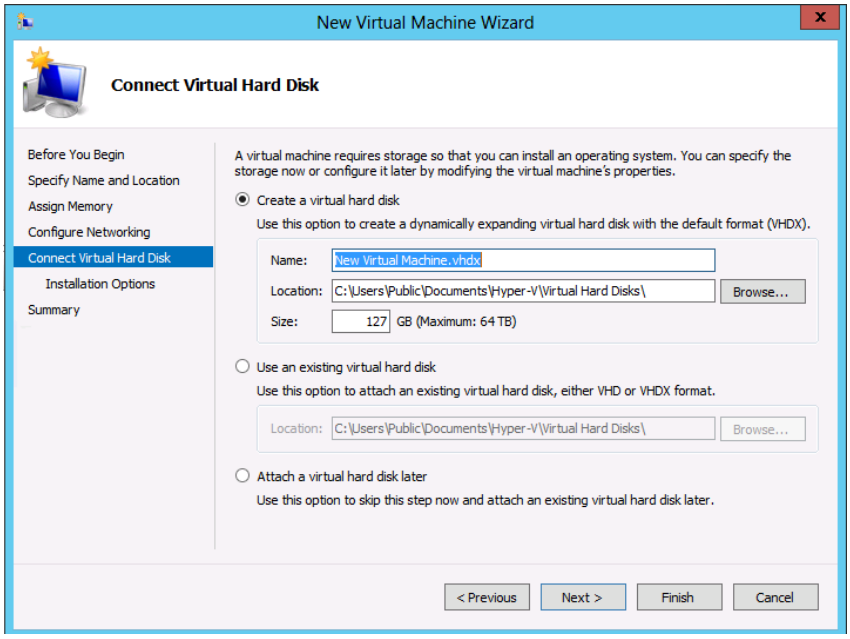
Slika 25. Hyper-V Manager konzola



Izvor: Autor

Instalacija nove virtualne vrši se putem VM čarobnjaka gdje se definiraju naziv servera, konfiguracija VHD, CPU, memorija i mrežni adapter.

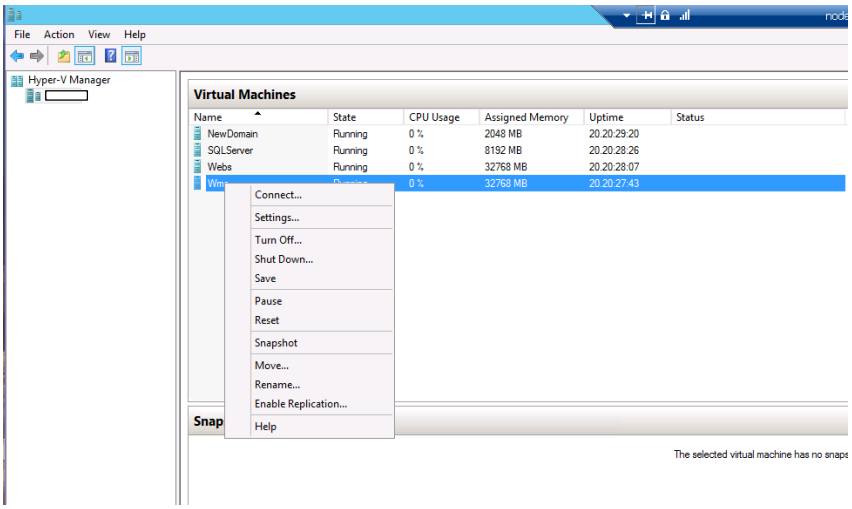
Slika 26. Čarobnjak za izradu virtualke



Izvor: Autor

Kod definiranja VHD-a moguće je odabrati jednu od opcija: izradu novog VHD-a te mu definirati lokaciju i veličinu, upotreba postojećeg VHD-a ili naknadno pridodavanje VHD-a. Prije same instalacije potrebno je na *Host* serveru uključiti svojstvo „*CPU Virtualisation*“ iz njegovog BIOS-a. Kod Intelovih procesora svojstvo se naziva VT, a kod AMD: amd-v. Također osim virtualne memorije može mu se dodijeliti i dio virtualne memorije na disku što nije preporučljivo jer može uzrokovati stalni rad HD-a te crpiti performanse i u konačnici usporiti rad samog servera. U konfiguraciji mreže može se konfigurirati na koje načine će komunicirati sa ostalima tj. na koji mrežni adapter se nova virtualka smješta. Također osim instalacije nove virtualke moguć je i uvoz već postojećih virtualnih servera pomoću njihovih VHD-a iz Hyper-V konzole.

Slika 27. Hyper-V konzola

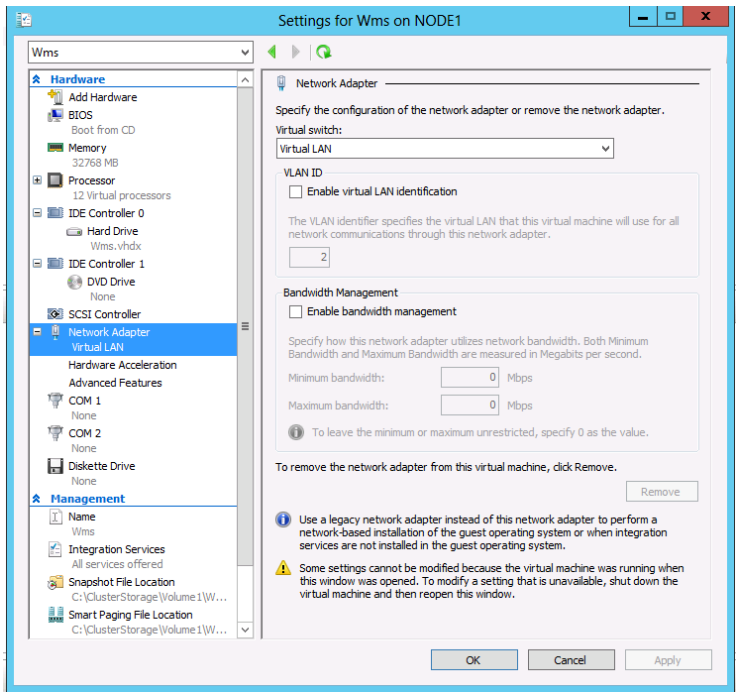


Izvor: Autor

Mogućnosti koje imamo iz Hyper-V konzole nad njenim virtulkama su: direktna konekcija, postavke, gašenje, pohranjivanje, pauziranje, resetiranje, „*Snapshot*“, premještanje, preimenovanje, replikacija i dodatna pomoć. „*Snapshot*“ opcija je jedna od bitnijih funkcionalnosti koje nudi virtualizacija. To je funkcija koja omogućava brzi *backup* u danom trenutku te omogućuje pripremu baze za izradu drugih virtualnih servera. Prilikom vračanja sustava u određeni „*Snapshot*“ gubi se sve naknadno konfigurirano na sustavu. Stanje „*Shut down*“ je gašenje sustava dok „*Turn off*“ je kompletno gašenje slično kao virtualno isključenje napajanja sustava. „*Paused*“ pauzira cpu, ali memorija ostaje u radu. „*Save*“ vrši pohranu

konfiguracije sa radne memorije na diskovni prostor. „*Save*“ se najčešće koristi ako je potrebno vraćanje informacije na radnu memoriju nakon ponovnog pokretanja sustava.

Slika 28. Postavke za virtualne uređaje



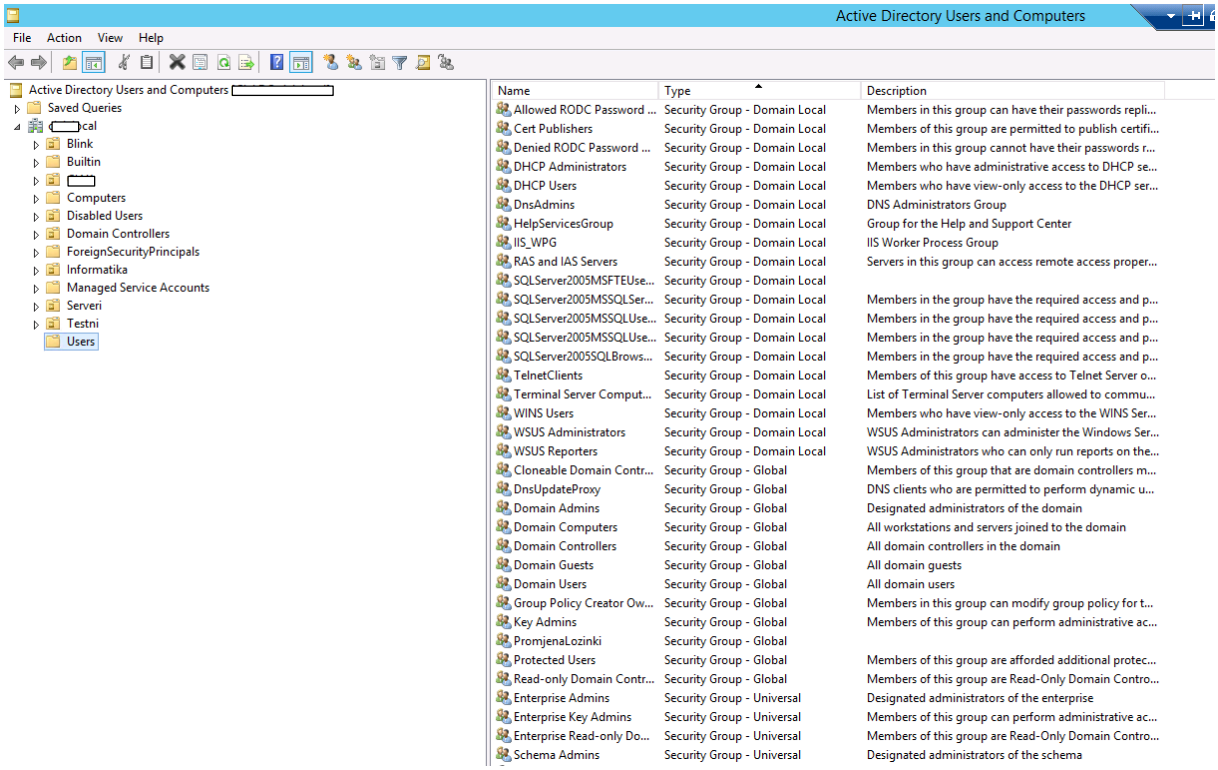
Izvor: Autor

Postavke koje se mogu definirati na virtualci dijele se na *Hardware* i *Management* . To uključuje upravljanje nad *Hardware*-skim komponentama, BIOS, radna memorija, VHD, optički pogon, SCSI *Controller*, mrežni adapteri, COM *portovi*, pogon za *Floppy*, naziv virtualke, servisi koji se integriraju u virtualci, *Snapshot*, lokacija pohranjivanja i ostale postavke. Kod postupka migracije fizičkog servera na virtualni server ostvaruje se ušteda fizičkog prostora, potrošnja energije, manje održavanje i centraliziranje što pospješuje lakši oporavak sustava nakon greške ili kvara. „System Centar Virtual Machine Manager“ je konzola za pretvaranje fizičkog u virtualni server. Pretvara fizički HD u VHD koji se kasnije lako uvozi u Hyper-V konzolu. Postoje i ostali alati od 3.stranke poput Acronis, VMware VCentar Converter, Starwind v2v converter (konvertira iz Hyper-V u VMware i obratno). Također moguće je migrirati virtualni server u fizički server. Najčešće se koristi kod redistribucije sustava na udaljene fizičke uređaje kojima je potreban već predefiniran sustav.

9. „Active Directory“ i „Domain Controller“

Jedna od funkcionalnosti koju omogućava DC jest upravljanje sa dozvolama nad određenim podacima. Dozvole se definiraju unutar same „Active Directory“ konzole. Potrebno je izraditi grupu, definirati dozvole te dodati korisnike u nju.

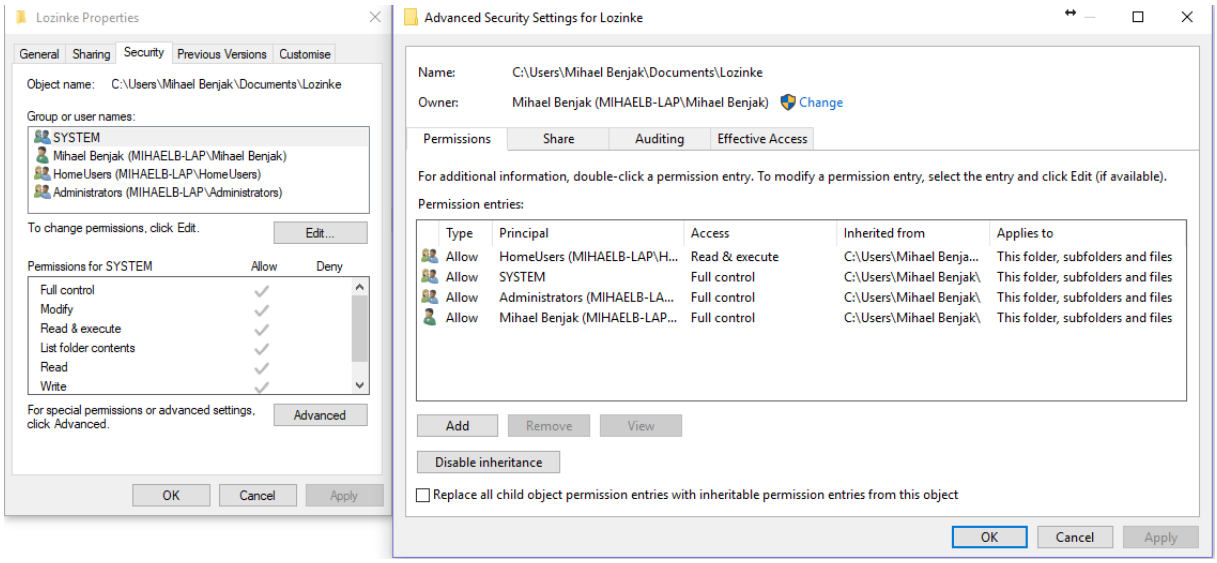
Slika 29. Pregled „Active Directory-a"



Izvor: Autor

Također moguće je eksplicitno napraviti dozvolu pod nazivom „NTFS Permision“ izborom svojstava nad konkretnim objektom te odabir „Edit user“ u „Security“ tabu.

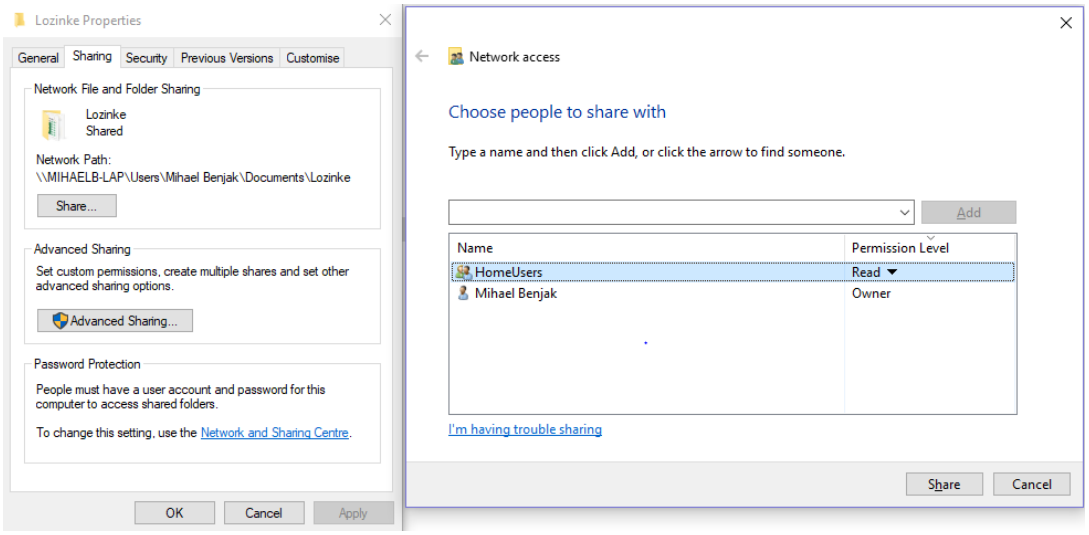
Slika 30. Podatkovna NTFS svojstva



Izvor: Autor

Ukoliko se radi o novom objektu potrebno ga je podijeliti sa korisnicama koji imaju dozvolu za rad nad njime izborom na svojstava samog objekta te iz drugog taba „Sharing“ izabrati ciljane korisnike i dodijeliti im prava na rad.

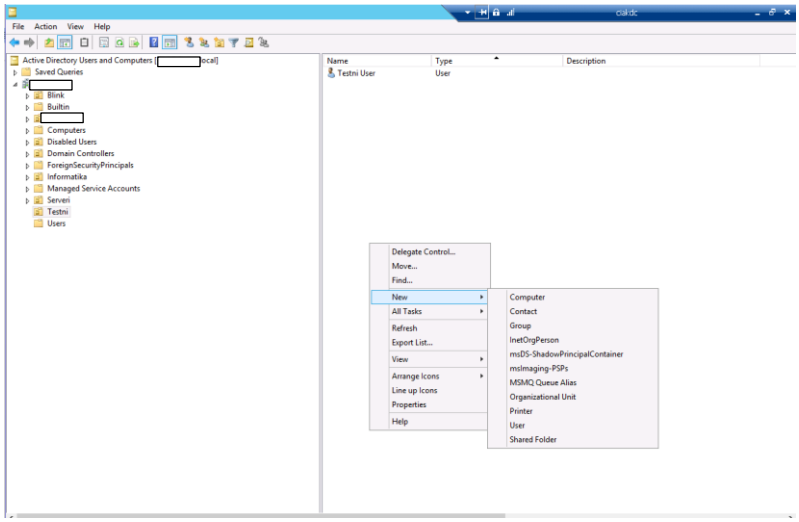
Slika 31. Dijeljenje podataka i dozvole iz svojstava



Izvor: Autor

Svaki novi korisnik dobiva atribut „*Globally unique*“ što znači da dobiva jedinstveni identifikator koji se ne može nikad podudariti sa niti jednim globalnim korisnikom. Korisnici dobivaju svojevrsni identifikator pod nazivom „SID“ uz svoje korisničko ime. Identifikatori na Windows domenama počinju sa S-1-5-21-xxx gdje xxx predstavlja jedinstveni broj za svakog novog korisnika. Ovaj postupak eliminira slučajna podudaranja korisnika sa istom autentifikacijom ili stručnim nazivom „*Passthroug autentication*“. „*Passthroug autentication*“ je nedostatak u kojem dvije osobe istih akreditacija posjeduju isto korisničko ime i lozinku te mogu pristupiti istom resursu kojem jedan od navedenih korisnika ima dozvolu pristupa dok drugi nema. Nedostatak je prisutan samo na lokalnoj razini te je tolerantan samo kod manjih lokalnih mreža od svega nekolicina računala gdje se može logički izbjeći podudaranja istih korisnika- pod uvjetom da administrator pozna sve korisnike i njihova korisnička imena. Takvi korisnici nazivaju se „*Local accounts*“ te vrijedi samo na jednom računalu odnosno na računalu na kojem je izrađen korisnik. Definirani su na lokalnoj razini odnosno bez domene. „*Domain accounts*“ ili domenski korisnici su za veće mreže. DC izrađuje korisničke račune i upravlja nad korisnicima tj. nad njihovima SID-ovima. Za izradu novih objekata na DC potrebno je izbrati opciju „*Action*“ ili desnim klikom na „*New*“. Nakon toga otvara se novi dijalog sa ponuđenim izbornikom za otvoriti novog: korisnika, računalo, kontakt, grupu, OU (engl. „*Organisation Unit*“) itd.

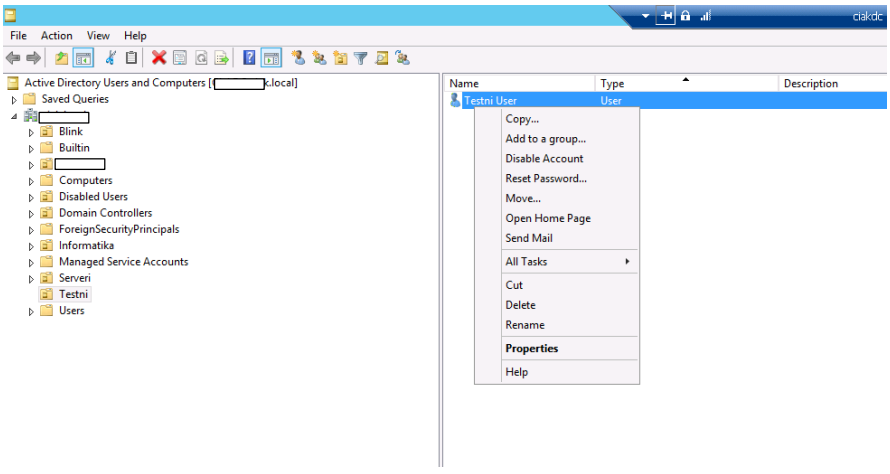
Slika 32. Izrada novih objekata u „Active Directory"



Izvor: Autor

Osim grafičkog unosa na sučelju, moguće je dodavanje putem „*Power Shell*“ i CMD komandi te automatizirani unosi pomoću alata u AD konzoli: LDIFDE (princip izvoza LDAP podatka) i CSVDE (princip CSV uvoza podataka) koji se unose pomoću komandi u „Powershell“ ili CMD. Dobra praksa ručnog unošenja korisnika jest putem predložaka, odnosno izrada predložaka u svakom OU po kojem se kopiraju konfiguracije za novog korisnika.

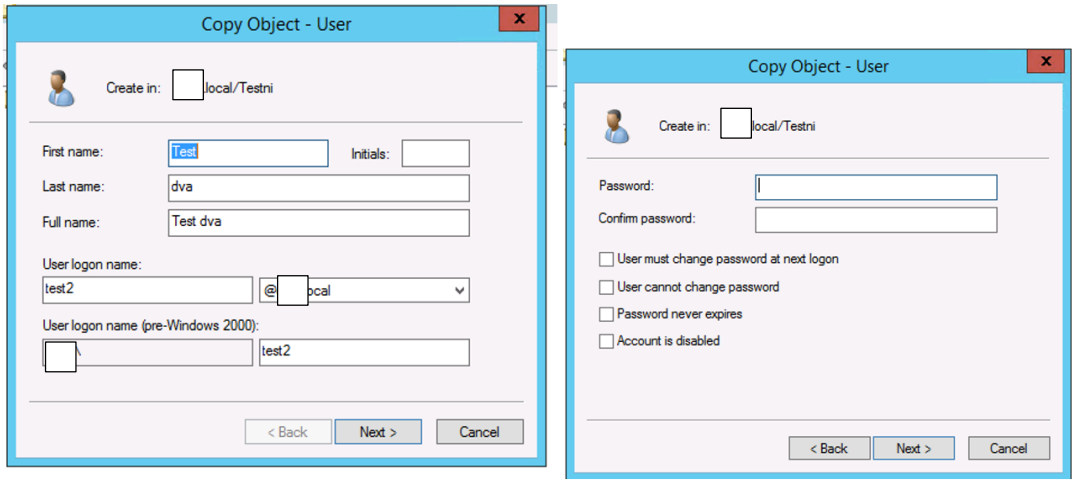
Slika 33. Postupak kopiranja postavki za izradu novog korisnika



Izvor: Autor

Kod otvaranja novog korisnika po principu kopiranja po prethodno otvorenim korisnicima, u prvom dijalogu definira se naziv korisnika, njegovo korisničko ime i domena u kojoj se nalazi, a u drugom dijalogu postavlja mu se lozinka za prijavu na domenski račun uz mogućnosti: korisnik može promijeniti lozinku kod prvog *logiranja*, da se onemogući promjena lozinke, onemogućenje roka valjanosti lozinke ili da se privremeno isključi novo kreirani korisnik.

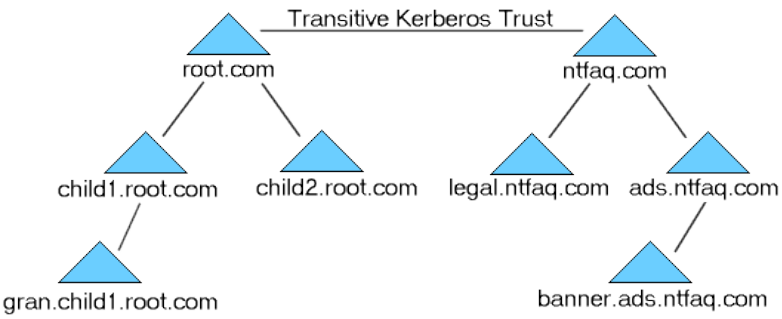
Slika 34. Definiranje korisnika



Izvor: Autor

Na slici broj **XX** su vidljivi „*Container*-i“ već prethodno definiranog DC. „*Container*“ je objekt koji sadrži grupe i korisnike te pospješuje generalnu raspodjelu svih objekata na domeni. Tako postoji sistemski zadani „*Container*“ pod nazivom „*Computer*“ koji ima unaprijed definiranu politiku smještanja svih računala u navedeni objekt koji se pojave na domeni. U većim poduzećima koji imaju više lokacija te potrebu da svaka lokacija ima svoju domenu, ali da ja moguće upravljanje nad svim domenama potrebno je napraviti vezu i odnose između njih. Spajanje više domena naziva se „*Forest*“ dok izrada novih pod-domena jedne domene naziva se „Child-Parent“ (prevedeno dijete-roditelj) ili „Branch“ (prevedeno grana) domene.

Slika 35. Hijerarhrija domene ili domenska šuma



Izvor: https://msandccna.blogspot.hr/2017/02/what-is-cdc.html , 6.3.2018.

Na vrhu svake šume nalazi se korijenski (engl. „Root“) DC koji je nadređeni za njegove grane te između njih ostvaruju se međusobne veze pod nazivom „*Trust Relationship*“. U takozvanim vezama postoji pojam „*Nesting*“ što omogućava smještanje jedne grupe iz jednog DC u druge grupe zbog omogućavanja i onemogućavanje prava nad zajedničkim podacima. U svrhu lakšeg upravljanja nad korisnicima i računalima koriste se „*Domain Local*“ , „*Global*“ i „*Universal*“ grupe. *„Domain Local“* grupa može sadržavati korisnike, a „*Global“* i „*Universal“* može sadržavati grupe iz bilo koje domene u „*Trusted forest*-u“ , ali može samo upravljati nad domenom u kojoj je definiran. Korisnici „*Global*“ grupe mogu upravljati nad istim šumom odnosno, globalne grupe se mogu *nestati* u lokalnim domenskim grupama iste šume. *„Universal“* grupe mogu upravljati nad svim domenama, ali im se ne mogu dodijeliti lokalne domenske grupe u njihovu grupu. U praksi postoji princip redoslijeda definiranja tih grupa pod nazivom AGDLP (skraćeno engl. „*account, global, domain local, permission"*) koji definira nadmoć nad ostalim grupama od najslabijeg do najjačeg: „*accounts*“> „*global group*“> „domain local group*"*> „*permision“*. „*Organisational units and Containers*“ su objekti koji sadrže ostale domenske objekte i korisnike. Njima se omogućuje centraliziranje, bolja preglednosti i pojednostavljeno upravljanje nad njenim objektima. Po zadano OU i *contrainers* posjeduju predhodno definirane sistemske objekte : „C*omputers“* (ulaze sva računala dodana u domeni); „*Domain controllers“ (* posjeduje unaprijed definirani GPO pod nazivom „*Default domain controler policy*“), „*Foreign security principals“* , „*Multiple domain envierments*“…

Active directory infrastruktura zapravo je jedna baza podataka koja smješta sve svoje objekte u jedan podatak pod nazivom „ntds.dit“.

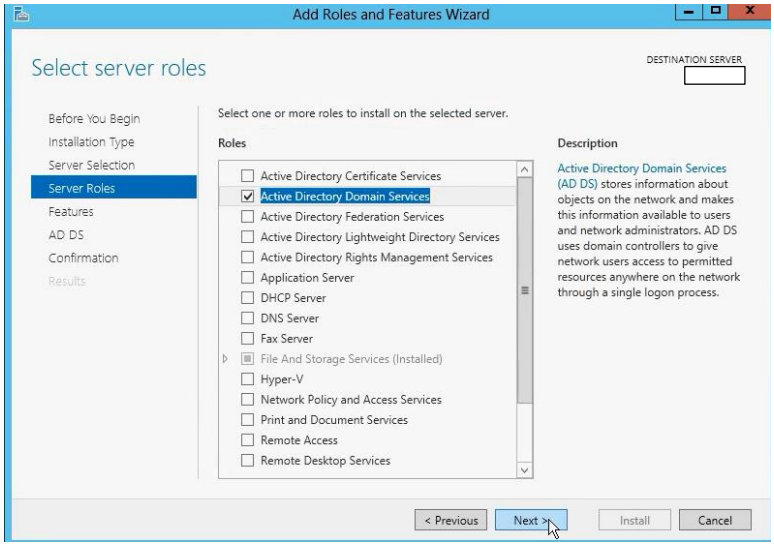
Unutra se nalaze:

1. AD objekti (*user,group,computer,dns zones,sites,site links,partial gpo*…)
2. N*amespace*
3. DNS server postavke
4. *Autenfikation Source*
5. ostale postavke pohranjene na DC

Preporuka kod većih i bitnih serverskih okruženja jest posjedovanje više DC zbog mogućnosti pada jednog. U okruženju sa više DC-a oni međusobno repliciraju „ntds.dit“ *podatak.* Ova akcija naziva se „*Peer replication*“. U procesu instalacije moguće je izabrati između: „*Full*“, „Read only dc“ (najčešće na Windows Core edicijama na udaljenim lokacijama i to uglavnom iz sigurnosnih razloga), „*Forest root*“ (glavni DC u šumi domeni), „*Child domain*“ (dio *Child* domene kad se radi *trusted domain* konekcija prema *korijen DC*), „*Peer dc*“ (sekundarni *failover controler* koji sinkronizira ntds.dit zbog dodatne sigurnosti domene).

Kod procesa same instalacije preporuča se čista instalacija koja će biti samo za potrebe DC-a. Server rola koju je potrebno instalirati je „Active Directory Domain Services“.

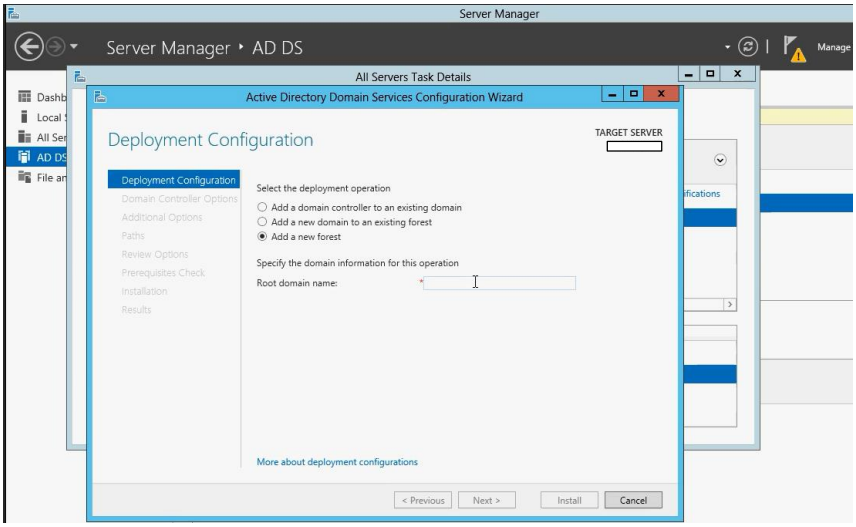
Slika 36. Dodavanje „Active Directory Domain Services“ role



Izvor: Autor

Nakon bazične instalacije potrebno je iskonfigurirati DC. Iz *Server Manager* konzole potrebno je aktivirati DC u domene. Prva stavka koja se definira za DC jest: ako se smješta u postojeću domenu, postojeći *forest* ili dodavanje novog *foresta.*

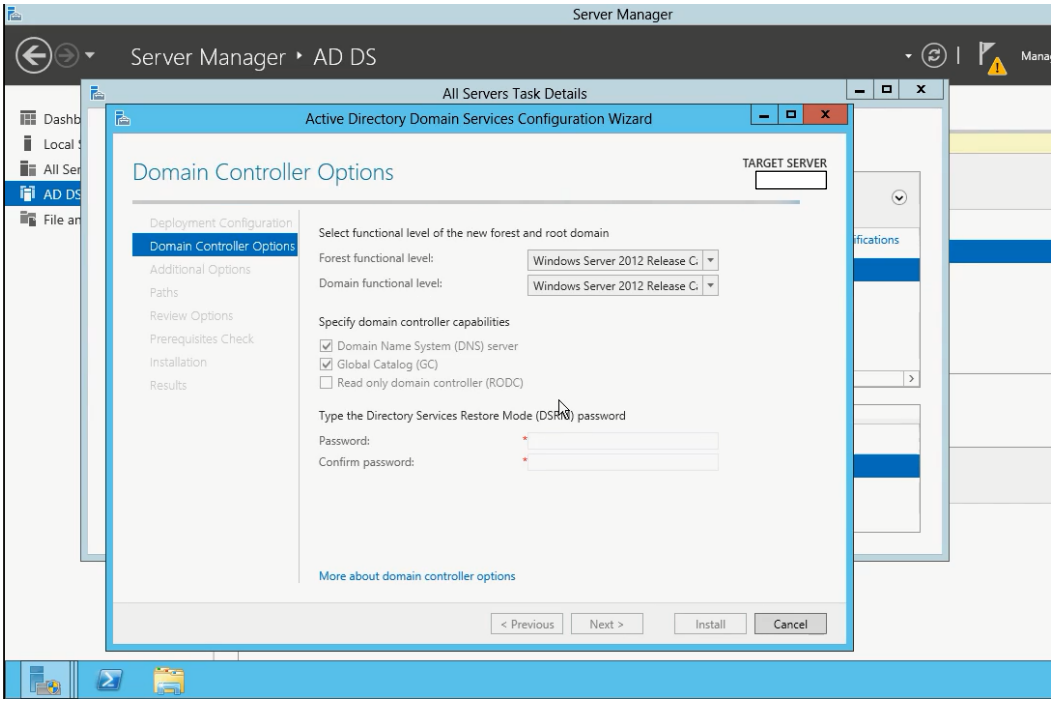
Slika 37. Postavljanje DC u domenu



Izvor: Autor

Kod definiranja samostalnog ili prvog DC potrebno je izabrati „*Add a new forest*“ te se specificira naziv DC-u koji će biti predstavljen kao *korijenski* DC u *forest-u.*

Slika 38. Opcije u postavljanju DC

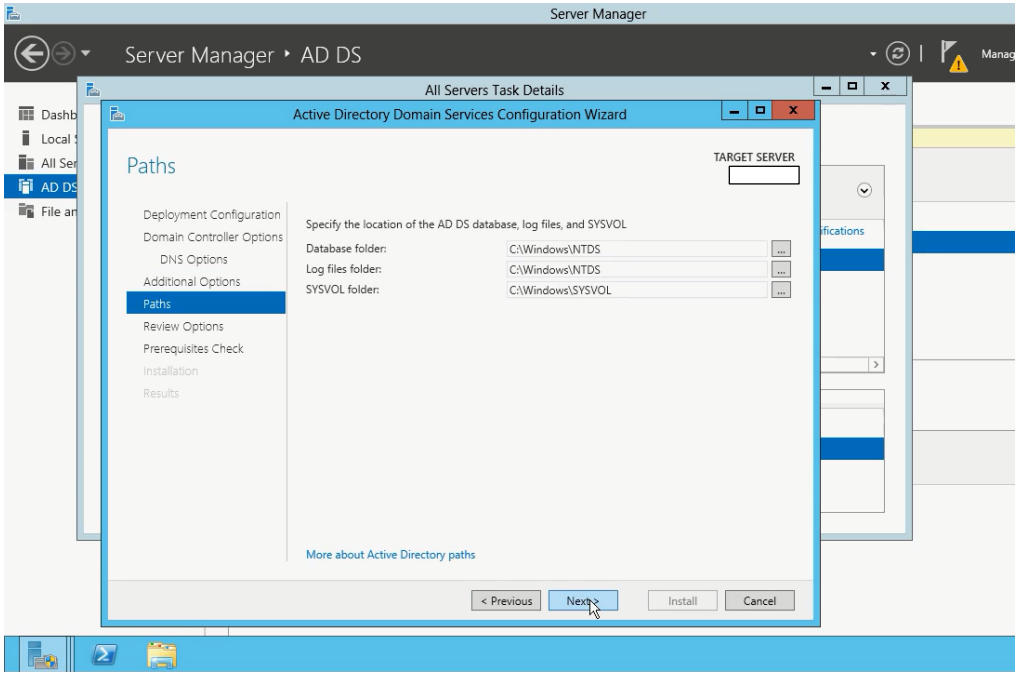


Izvor: Autor

U drugom dijelu definiraju se funkcionalnosti operacijskog sustava koje će biti na domeni. Nužno se definiraju prema ostalim budućim DC-ima tj. prema najstarijem operacijskom sustavu među DC-ima u domeni. Osim funkcionalnosti OS-a, definiraju se ako DC postaje i DNS server, posjeduje globalni katalog i/ili postaje samo *Read only* DC te se definira sigurnosna lozinka za potrebe oporavka. Globalni katalog je svojstvo DC koji na sebi nosi sve objekte ostalih domena što ga definira kao korijenski DC , odnosno izrađuje potpunu kopiju svojih objekata i vrijednosti u svrhu replikacije na druge DC. Dakle, kad se pretražuje po jednom od DC, a podatak nije definiran na njemu, pretraživanje ne mora ići do drugog domenskog upravljaća koji je izvor promjene već posjeduje svoju kopiju primarnog DC.

Read only DC služi za replikaciju i isključivo samo za čitanje podataka. Nije moguće vršiti izmjene DC objekata nad *Read only* DC-om, a najčešće se upotrebljava na udaljenim granama šume domene. U nastavku instalacije, pretražuje se ukoliko postoje već definirani DNS serveri te u dodatnim opcijama definira se „NetBIOS *name*"- predstavljanje servera na lokalnoj mreži.

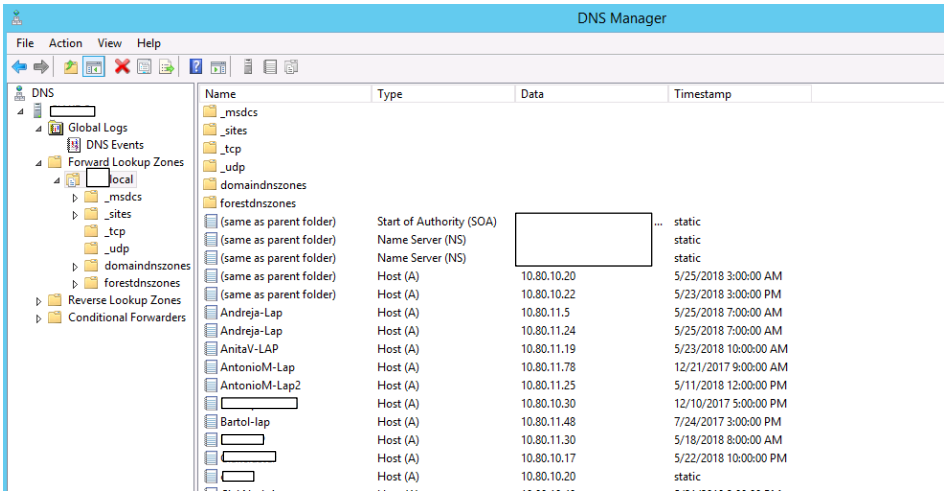
Slika 39. Putanje za pohranu podataka



Izvor: Autor

U petom dijelu instalacije definiraju se lokacije gdje DC pohranjuje svoju bazu podataka, *logove* i *Sysvol.* U nastavku slijedi pregled svih zatraženih funkcionalnosti i provjera kompatibilnosti okruženja i sustava te sama instalacija.

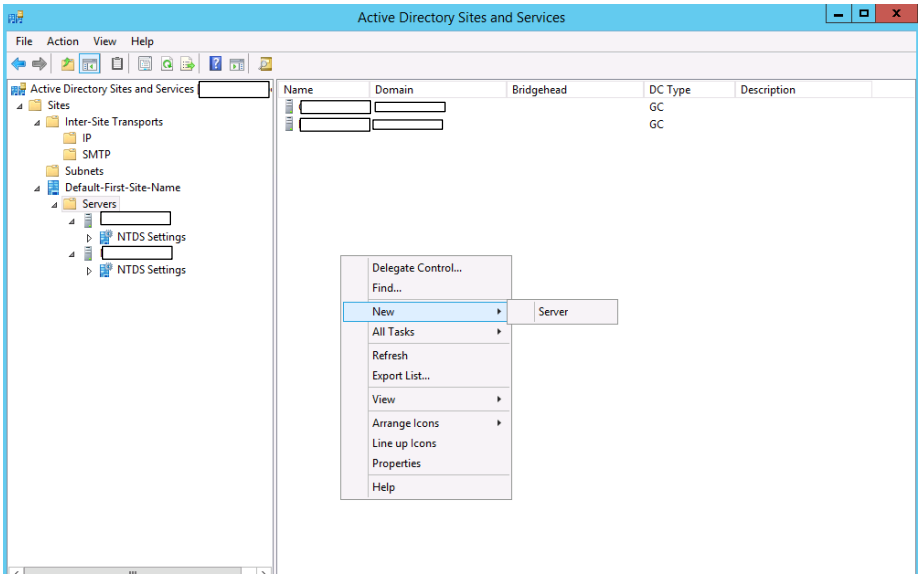
Slika 40. Pregled DNS Manager konzole i prijavljenih korisnika



Izvor: Autor

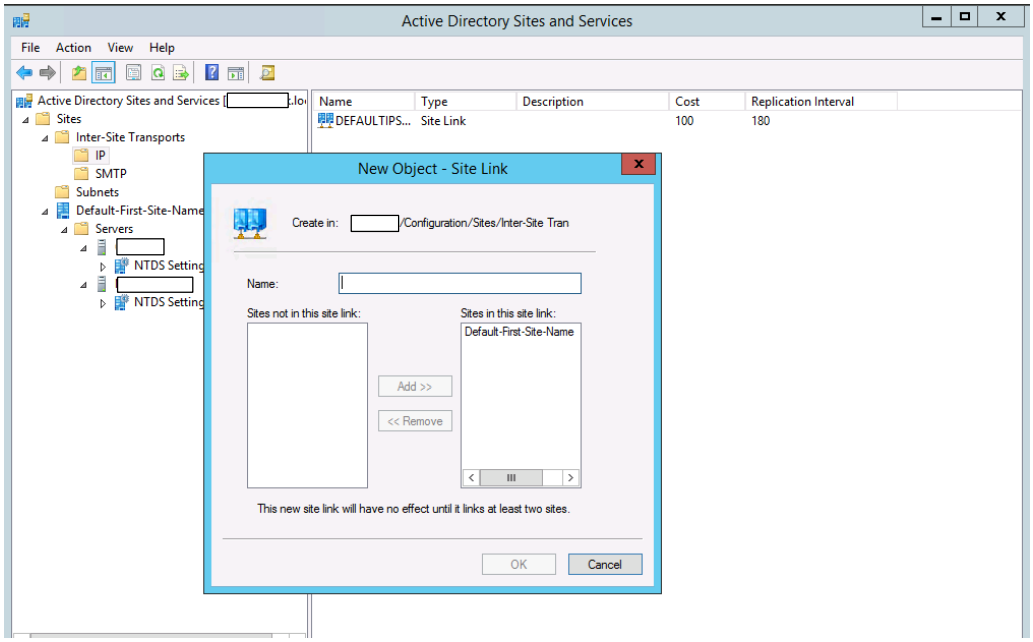
Za replikaciju informacija i podataka između DC-a potrebno je dodati ostale DC putem „*Active directory sites and services*“ konzole. Izvršava se akcija dodavanja novog servera te mu je potrebno definirati lokaciju iz IP foldera akcijom „*New site link*“.

Slika 41. Mogućnosti u "Active Directory Sites and Services"



Izvor: Autor

Slika 42. Dodavanje novog objekta „Site Link"



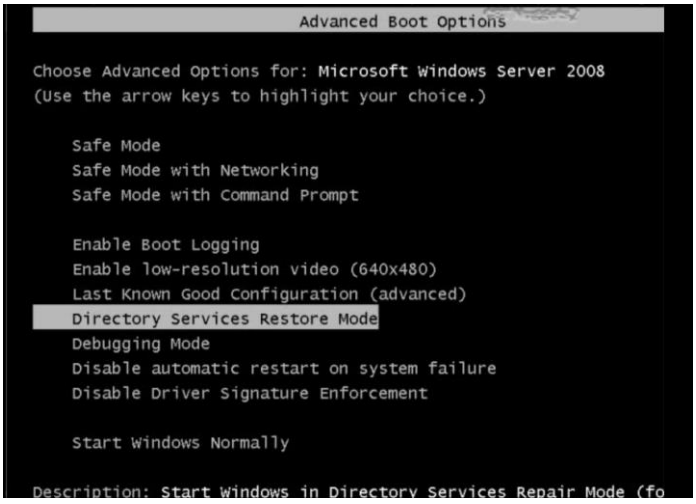
Izvor: Autor

„Trust Relationships“ odnosno veze između DC-a mogu biti jednosmjerni gdje se veza povjerava samo jednoj strani domene, dvosmjerna gdje se veza povjerava na obje strane, „*forest trust*“ gdje domene zajedno sa podomenama imaju povjerenje, „*shortcut trust*“ što je logički brža varijacija „*forest trust-a“ (* eliminira se potreba za „*walking up the tree“* da pronađe korisnika koji potražuje određeni resurs na drugom kraju šume, ali zahtijeva direktnu vezu).

Na DC postoje 5 tzv. „Total Master Opertions Roles“ tj. glavne funkcionalnosti *kontrolera*: 1. „*Domain naming role*“ (provjera imena da nisu redundantna), 2. „*Schema*“ (daje *scheme* u dijalozima tj. atribute, npr. MS Exchange se uvrštava u *schemu* tako da integrira neke svoje atribute i objekte u ostale objekte AD), 3. „*Infrastructure“* (brine o grupama, vlastitih i drugih domena) 4. „*Relative id master*“ (brine za SID-ove) i 5. „*PDC Emulator“* (smješten na primarnom DC- provjerava lozinke i pokreće replikaciju, upravlja nad GPO) Postoje još i dodatne role poput: „Domain browser master“ (drži listu resursa na mreži), „ Master time source“ (zadužen za sinkronizaciju vremena).

Noviji operativni sustavi za DC nude praktične funkcionalnosti poput „*Single sign on*“ funkcije (jedna prijava je dovoljna za sva ostala autentificiranja), upotreba „Kerberos“ sigurnosne tehnologije u razmjeni informacija koji ne prenosi lozinke preko mreže već radi po principu *ticket*-a ili *token*-a te ga ovom metodom predstavlja ostalim uređajima kao već autentificiranog korisnika. Starije verzije operativnog sustava nisu posjedovale mogućnost vraćanja izbrisanih korisnika (obično ljudskom greškom) već se proces vraćanja korisnika morao odraditi dužim putem što bi zahtijevalo konfiguriranje svih DC u *pool*-u te vraćanje korisnika iz BIOS „Advanced Boot Options“ izborom na „Directory Services Restore Mode“. Ukoliko je korisnik izbrisan i okruženje koje posjeduje više DC-a koji su uspjeli sinkronizirati akciju brisanja korisnika, taj navedeni korisnik se neće moći vratiti ručno iz „deleted items container-a“ jer ostali *domain controler*-i neće dozvoliti različiti inkrement verzije (koji je postupkom vraćanja postao manji za jednu verziju od ostalih repliciranih verzija). U tom slučaju bilo je potebno napraviti „directory services restore mode*“* iz „Advanced Boot Options“. U tom okruženju se otvara administratorski CMD, unosi se komanda: „wbadmin get version>wbadmin start systemstaterecovery –version:mm/dd/yyyy-hh:min“ te da se spriječi da ga ostali DC-i opet ne izbrišu, unosi se komanda: „ntdsutil>active instance ntds>auth rest>restore object „cn=korinisk, ou=organisation unit korisnika, ou= grupa ogranisation unita, OU=naziv container-a,dc=naziv domene“ . Ovaj postupak će napraviti inkrement verzije za 100000 tako da ne bude inkrement manji od ostalih repliciranih verzija na drugim DC.

Slika 43. Napredne BOOT postavke



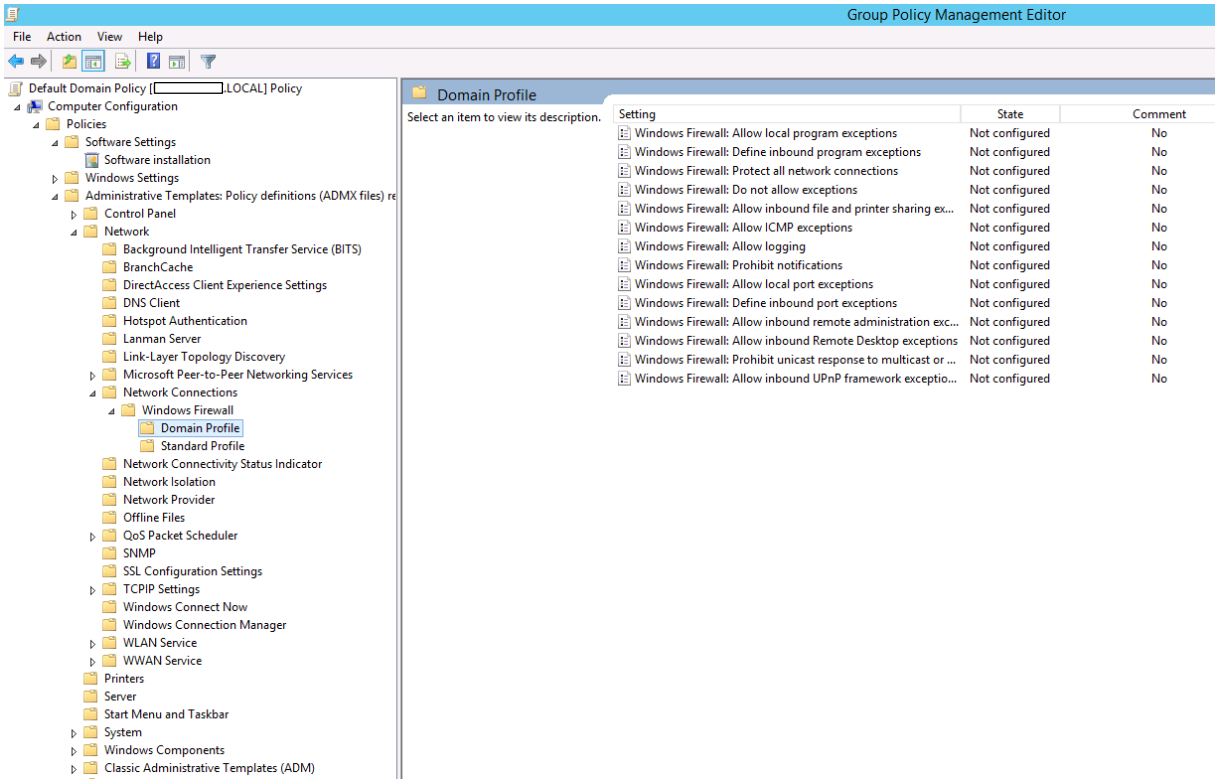
Izvor: Autor

Noviji operacijski sustavi patentirali su alat pod nazivom „AD Recycle bin“ koji ima funkcionalnost vračanja korisnika te mu se dodaje inkrementalna vrijednost +100000 na verziju tako da drugi DC mogu sinkronizirati na noviju verziju. Ovu funkciju potrebno je aktivirati u „Active Directory Administrative Ceneter“ te se pristupa „*Deleted objects*“ iz koje se vrši *restore* izbrisanog korisnika.

10. „Group policy“

„*Group policy*“ je funkcionalnost DC-a koja omogućuje centralizirano upravljanje nad grupnim pravilima i ograničenjima na domeni. Definiranje pravila odvija se u „*Group Policy Management Editor*-u“. Osnovna podjela dijeli se na računalnu konfiguraciju i na korisničku konfiguraciju. Na slici su prikazane postavke za vatrozid što se tiče računalne konfiguracije nad zadanim „*Default Domain Policy*“ objektom. Dobra praksa je otvaranje novog GPO za svaku kategoriju. Primjer: mrežne postavke u jedan GPO pod nazivom mreža, „Power management“ u drugi GPO pod nazivom ušteda energije, „Hide Internet explorer icon on desktop“ za korisničke postavke u treći GPO pod nazivom „Zasto nema Internet tipka na racunalu“. U radu sa GPO također preporuča se izbjegavati specijalna hrvatska slova i ostali simboli.

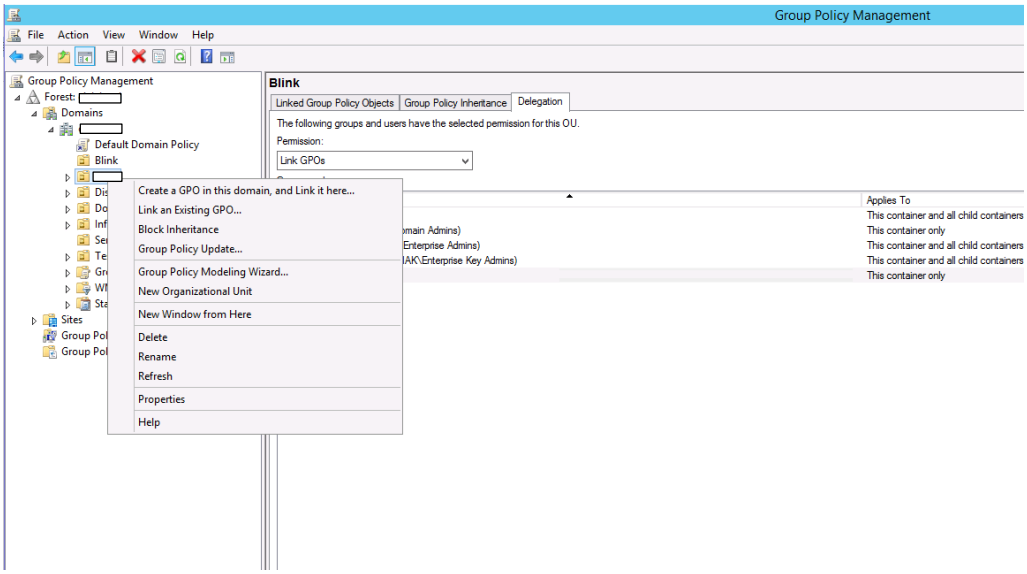
Slika 44. „Group Policy Management“ konzola



Izvor: Autor

Nakon izrađivanja GPO potrebno ih je dodijeliti korisnicima. Dodjeljivanje ili *linkanje* GPO objekta izvršava se putem „Group Policy Management“ konzole izborom na opciju „Link an Existing GPO“. Potrebno je obratiti pozornost gdje se linka GPO tako da adekvatni korisnici dobiju odgovarajuća prava i zabrane.

Slika 45. Opcije u Group Policy Management konzoli



Izvor: Autor

Korisnici ukoliko imaju ovlasti, mogu pristupiti i upravljati nad lokalnom politikom (engl. „*Local Policy*“) koja se nalazi na njihovim računalima. Ukoliko pravilo nije definirano na DC korisnik ju može izmijeniti, a ako se to isto pravilo naknadno definira na domeni, GP objekt će nadvladati pravila koja je korisnik vlastoručno definirao na svojoj *local policy*. Ukoliko se u GP objektu nalaze pravila vezana za istu postavku različito definiranim u „*Computer Configuration*“ od „*User Configuration*“, politika računalne konfiguracije nadvladava nad korisničkom konfiguracijom. GPO procesiranje vrši se tako DC provjerava svakih 5 minuta ako su se dogodile kakve promjene. Postupak uključuje provjeru verzije ukoliko se dogodila inkrementalna promjena verzije. Replikacija kod korisnika se izvršava kod pokretanja sustava, svakih 90 do 120min (zahtjevnije promjene traže odjavu ili ponovo pokretanje sustava) ili putem „gpupdate /force“ komande u CMD. Bitno je obratiti pažnju ukoliko se gpo objekt odnosi na korisnike da se ne dodjeli grupi koja sadrži računala jer GPO nema utjecaja zbog činjenice da se objekt odnosi isključivo na ciljanu grupu.

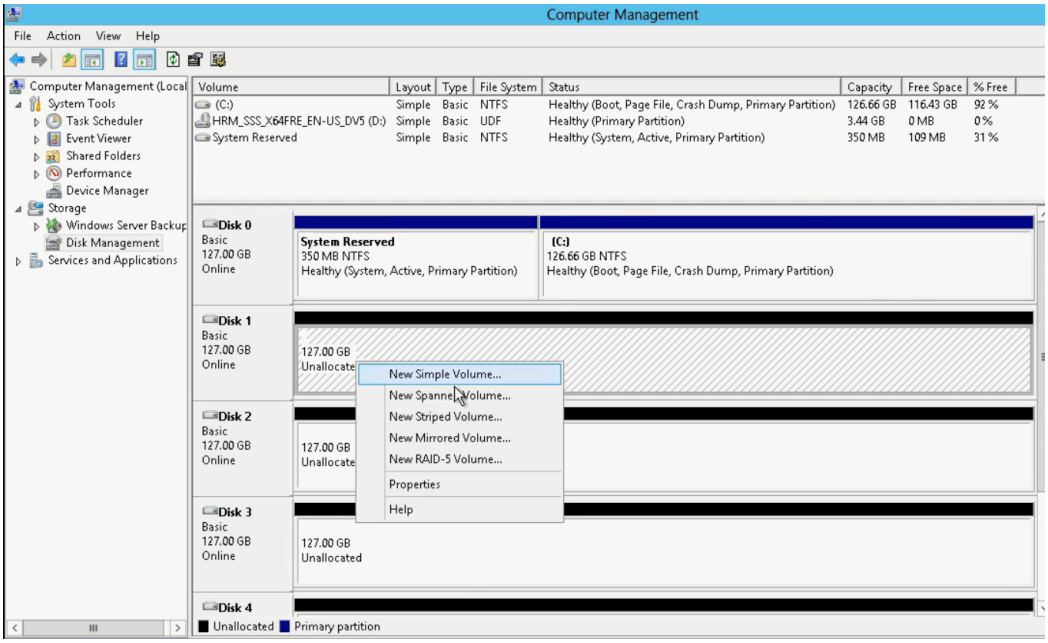
11. „*Storage*“

Storage je uređaj za pohranu, skladištenje i uređivanje bilo kakvih informacija ili podataka. U većim poduzečima sa velikom bazom podataka, informacije se pohranjuju na zasebni server. *Storage* server nije dostupan direktno ostalim korisnicima već pristupaju bazi preko aplikacijskog servera koji su međusobno povezani izvan LAN mreže putem SAS kablova (ili nekih drugi tipova) u SAN mreži. Pohrana baze vrši se na veliku količinu diskova u RAID-u koji zajedno grupirani čine „*Storage Pool“*. Vrste diskova prema funkcionalnosti mogu se podijeliti na:

1. *Basic Disk*- najosnovnija vrsta pohrane te je najkompatibilnija između svih operativnih sustava. Basic Disk je moguće konfigurirati sa najviše 4 primarnih particija.

2. *Dynamic Disk*- kod ovih vrsta stvaraju se „*Volumes*“ dok kod *Basic Disk*-a stvaraju se particije. Namjena im je za *Multi-Disk* konfiguracije kao npr. *Spanned Disk* (kombinacija više diskova gdje kada se popuni prostor jednog diska, automatizmom prelazi na drugi disk), *Striped* RAID Disk (RAID 0- pohrana podataka podijeljena između svih diskova), *Mirror* RAID *Disk* (RAID 1- pohrana podataka se kopira na druge diskove), *Striped* + *Parity Disk* (RAID 5 – pohrana podataka između više diskova sa jednim diskom koji služi kao paritetni disk za rekonstrukciju podataka).

Slika 46. Pregled diskova i particija u računalnom upravitelju

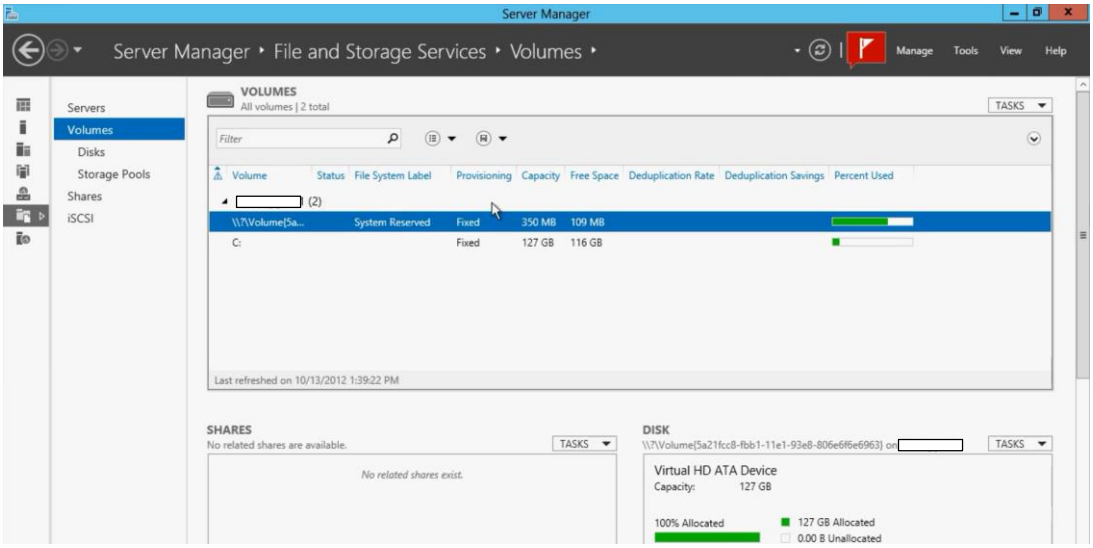


Izvor: Autor

3. VHD, VHDX – virtualni HD, smješta se na postojeći disk. Upotrebljava se najčešće kod virtualiziranih servera. Jednostavan je za distribuciju.

Za izradu *Storage* servera potrebno je adekvatno pripremiti diskove. Od fizičkih diskova stvaraju se „*Storage Pools*“ te iz njih virtualni diskovi (nisu vezani za VHD i VHDX). „*Storage Pool*“ čine 1 ili više grupiranih diskova te lako ga je nadograđivati sa dodatnim diskovima.

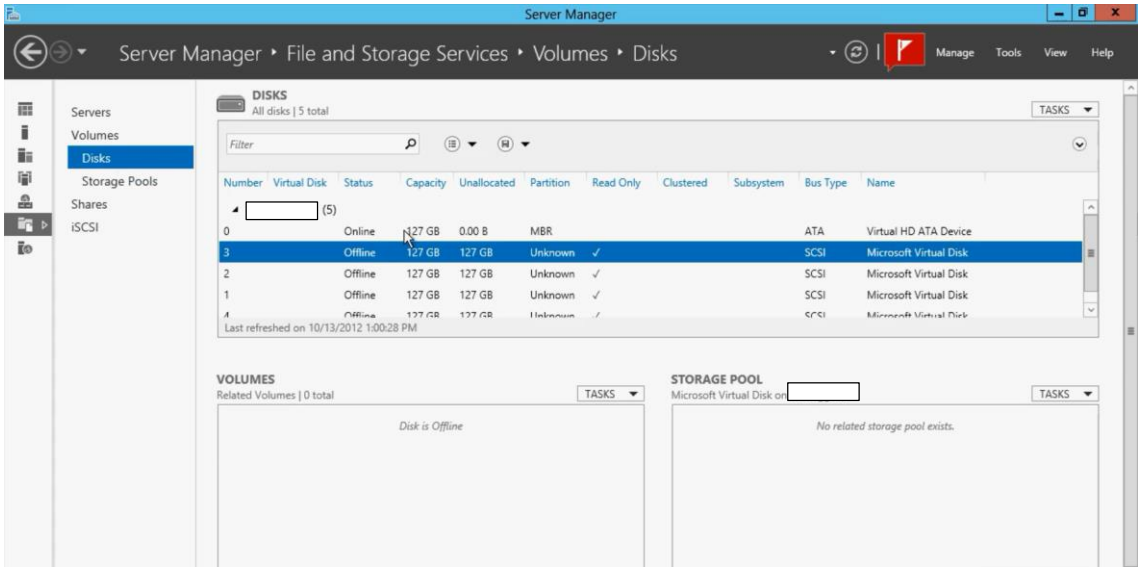
Slika 47. Pregled nad „*Volumes*“ u „*Server Manager*“ konzoli



Izvor: Autor

Pregled i konfiguracija virtualnih diskova i *Volumes* vrši se u *Server Manger* konzoli pod *File and Storage Services.* U kategoriji *Volumes* prikazani su postoječe dinamične particije.

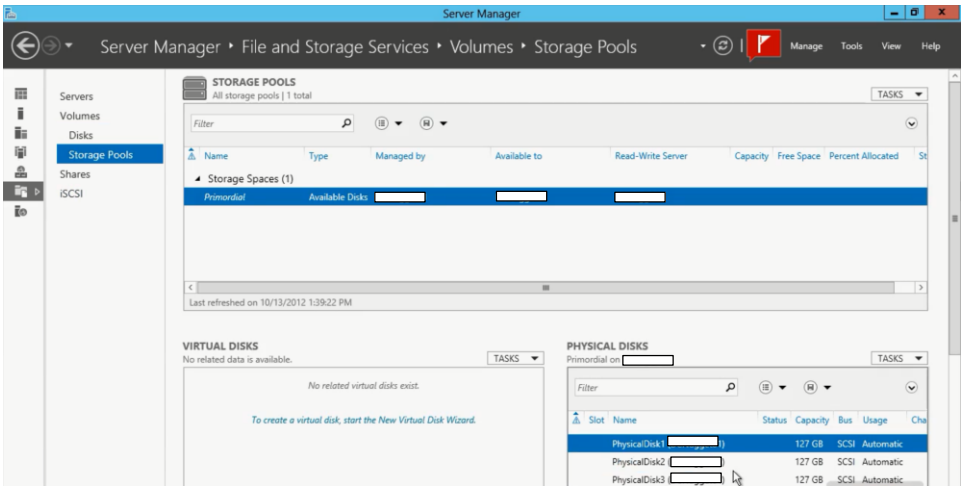
Slika 48. Pregled diskova u „*Server Manager*“ konzoli



Izvor: Autor

Pod Disk kategorijom vrši se pregled nad dostupnim diskovima, njihovi *Volumes* i *Storage Pools*.

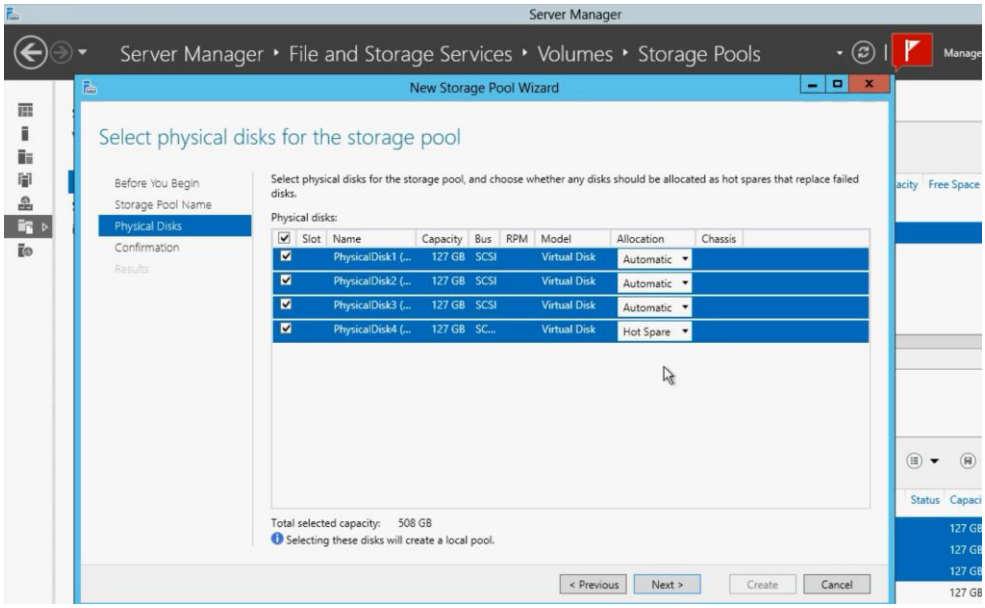
Slika 49. Pregled nad „*Storage Pools*“ u „*Server Manager*“ konzoli



Izvor: Autor

U kategoriji *Storage Pools* prikazani su grupirani diskovi u *Pool-u.* Za izradu novog *Pool-*a potrebno je izabrati diskove iz okvira fizičkih diskova te desnom tipkom miša izabrati „*New Storage Pool*“ .

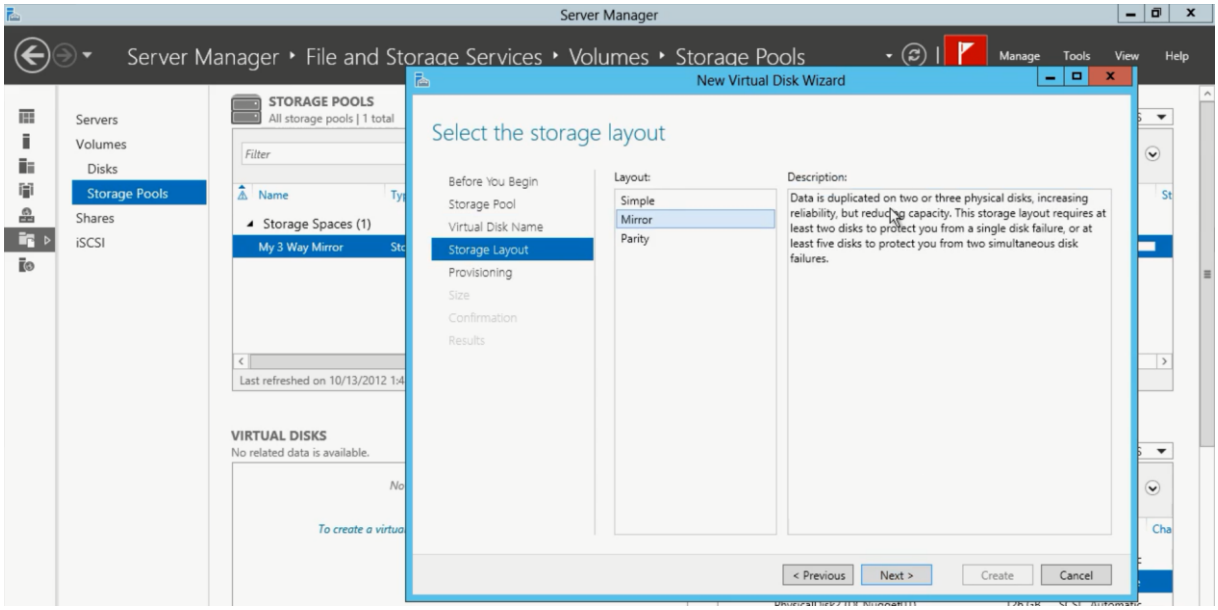
Slika 50. Izrada novog „*Storage Pool-a*“ grupiranjem dostupnih diskova



Izvor: Autor

Nakon unosa naziva *Pool*-a izabiru se diskovi te koju vrstu alokacije ili funkciju preuzimaju. Mogući je izbor između „*Automatic*“ koji je potreban za „*Mirroring*“ ili „*Hot Spare*“ koji služi kao rezervni disk u slučaju propadanja jednog od „*Automatic*“ diska. Nakon inicijalizacije *Pool*-a potrebno je napraviti VHD. Iz *Storage Pool*-a izabire se adekvatni *Pool* desnim klikom te se pokreće čarobnjak „*New Virtual Disk*“.

Slika 51. Izbor funkcionalnosti diskova u *„Pool-u“*



Izvor: Autor

U čarobnjaku definira se naziv virtualnog diska te mu se definira *Layout* (jednostavan, *Mirror* ili paritetni). Nakon „New Virtual Disk Wizard“ automatizmom otvara se „New Volume Wizard“ kojim se konfigurira *Volume*- naziv, *File System*, veličina, „*Drive Letter“* itd.

12. RAID

RAID (engl. „*Redundant Array of independant disks*“) je princip ili način grupiranja više diskova u svrhu povečanja prostora,redundancija i performansa (nije moguće implementirati sve 3 osobine). Konfigurira se direktno na RAID kartici najčešće iz BIOS-a servera.

OSNOVNI RAIDOVI:

RAID 0 čine 2 ili više diska- nema redundancije, dupla brzina i dupli smještaj.

RAID 1 čina najmanje 2 diska te uvijek moraju biti paran broj za svrhe „*mirroring*-a“. Stvaraju se redundantni podaci, kopiraju se sa primarnog diska na drugi. Gubi se na prostoru ali diskovi se lako nadomjeste.

RAID 5 čine 3 ili više diska. Radi na principu „*striping*-a“ sa paritetnim bitom. Podaci se zapisuju na dva diska dok se na treći disk zapisuje matematička informacija paritetnog bita koji će ponovo izgraditi podatke na novom disku u koliko se disk zbog kvara zamijeni. Paritetni disk konstantno cirkulira između 3 diska tako da svaki ima paritetni bit nekog podataka od oba diska. Troši CPU snagu za što je potrebna RAID kartica da rastereti tu funkciju sa servera. Gubi se na količini spremišta za jedan disk, tj. od 5 diska od 1 terabajt, preostaje 4 terabajta za pohranu.

RAID 10 čine 4 ili više (uvjet je paran broj) diska. Kombinira se raid 0 i raid 1 te osigurava najveću sigurnost.

„Hotswaping“ je svojstvo koje se koristi kod zamjene diskova (obično *koruptanih*) još dok su „vrući“, odnosno nije potrebno gasiti sustav. Također, koristi se još kod nekih tehnologija dodavanja memorije, procesora, pokvarenih napajanja itd.. Ova tehnologija kod nekih distributera prikazuje se grafički na samim *hardwares*-kim komponentama (plavo ili crveno).Diskovi moraju imati jednu količinu prostora pohrane, u suprotnom će za „*mirror“* uzeti veličinu najmanjeg diska. Preporuča se upotreba diskova istih modela i istog proizvođača.

13. SAN

„*Storage area network*“ je mreža bazirana na blok level protokolu te se najčešće koristi za razmjenu podataka sa „*storage*-om“. Diskovi na *storage*-u spojeni u SAN mreži daju prividno svojstvo kao da su lokalni *storage* odnosno nisu mapirani ili podijeljeni diskovi na drugom uređaju. Pristupanje uređajima u SAN mreži nije moguće preko LAN-a od drugih uređaja već imaju rezerviranu mrežu samo za svoje potrebe razmjene podataka. Načini na koje se mogu povezati uređaji u SAN mreži su putem SAS, iSCSI ili *Fiber* konekcija.

Slika 52. SAS kablovi

izvor: http://www.backupworks.com/HD-Mini-SAS-to-Mini-SAS-1m.aspx , 1.5.2018.

SAS konekcije ostvaruju se putem adekvatnih SAS kablova te mogu razvijati brzinu prijenosa do 12 Gb/s te najviše 4 spojenih servera. ISCSI konekcije nemaju ograničenje na broj spojenih servera, ali zahtjevaju Gigabit mrežni preklopnik. Mogu razmijenjivati prijenos podataka do 10 Gb/s uz adekvatni mrežni preklopnik kao posrednik i koriste se standardnim bakrenim mrežnim kablovima. *„Fiber Channel“* konekcije koriste optičke kablove koji su više pouzdani, eliminiraju smetnje te mogu razvijati brzinu prijenosa do 16Gb/s.
DFS (skraćeno engl. *Distributed File System)* je vrsta pohrane podataka kod kojeg se repliciraju podaci sa raznih lokacija na jednu centraliziranu lokaciju. Omogućuje lakše upravljanje i pretraživanje. NAS (skraćeno engl. *Network Attached Storage*) su zasebni mrežni uređaji koji služe za pohranu, razmijenu,skladištenje ili *backup* podataka. Bazirani su na Linuxu te im se pristupa putem *web-a* ili aplikacije. Koriste se : nfs,smb cifs protokolima.

Slika 53. NAS uređaj

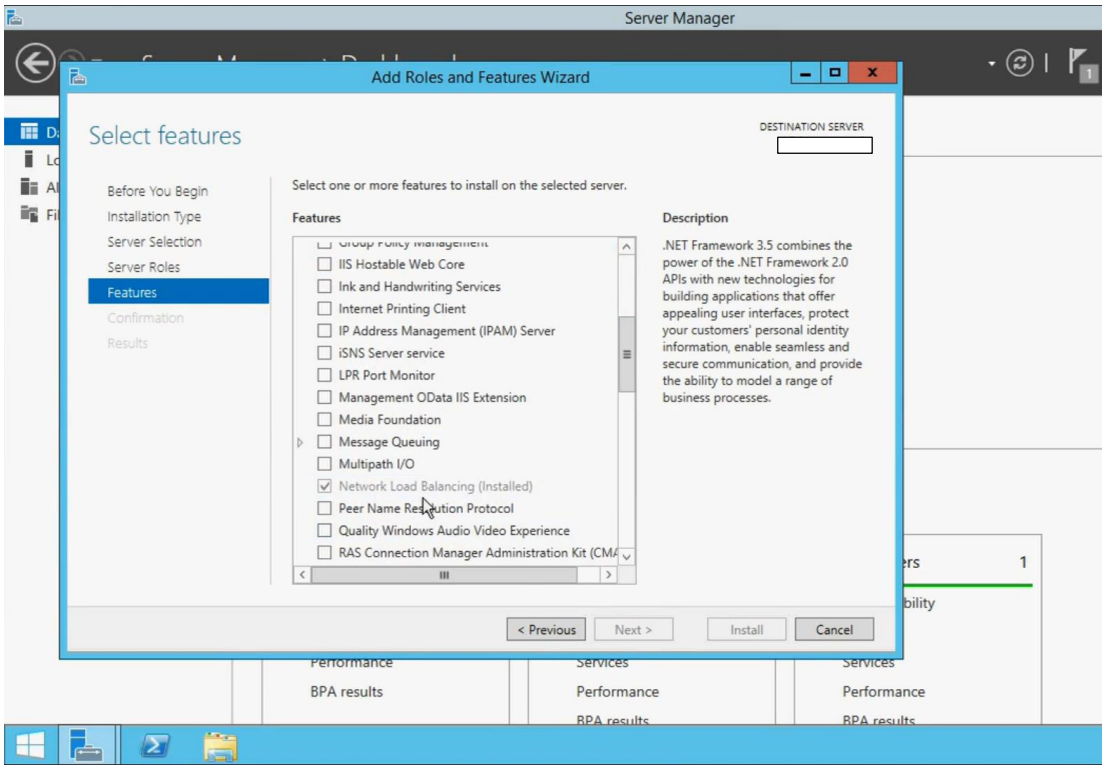
Izvor: http://www.storagereview.com/synology_releases_nas_ds416play , 1.5.2018.

14. „Load Balancing“

„Load Balancing“ je funkcionalnost servera koja omoguće raspodjelu resursa između više servera tako da ne dolazi do preopterećivanje jednog od servera. Upotrebljava se za IIS, RDS hostove, VPN servere, *Threat Management Gateways*…

Ovom funkcionalnosću ostvaruje se visoka dostupnost (engl. „*High Availability*“) korisnicima u radnoj okolini da mogu nesmetano nastavljati svoje aktivnosti bez prekida ukoliko dolazi do prekida jednog od servera. Za optimalnu konfiguraciju *Load Balance*-a preporuča se 2 mrežne kartice po svakom čvoru odnosno serveru sa različitim *subnet-ima* i ip adresama.

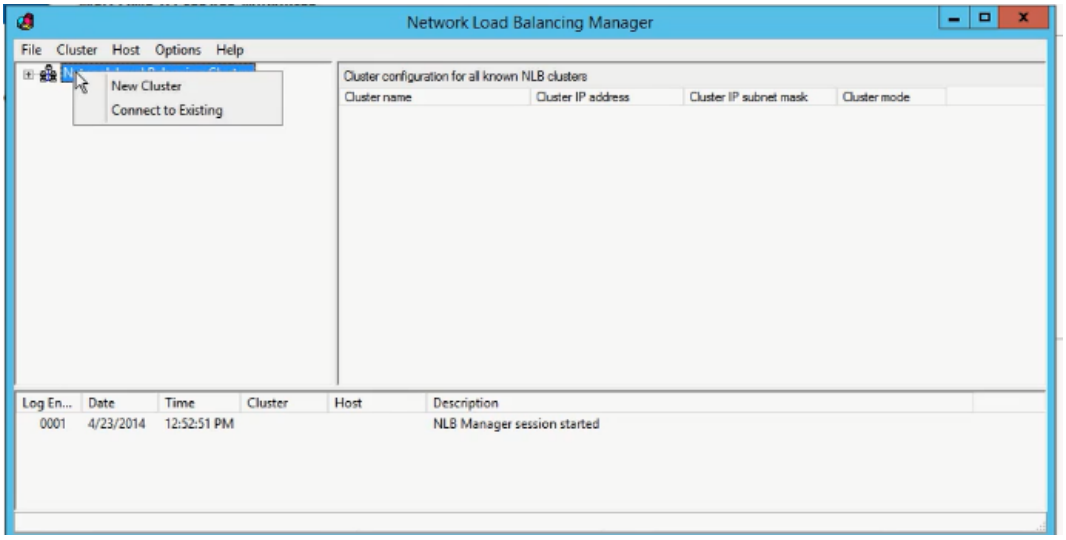
Slika 54. Dodavanje „*Network Load Balancing*" kao serversku rolu



Izvor: Autor

U prvom koraku potrebno je instalirati *Network Load Balancing* dodatak (engl. *Feature*) na servere putem „*Add Roles and Features Wizard“.* Nakon instalcije pokreće se „*Network Load Balancing Manager“* u *Server Manager*-u iz izbornika „*Tools“*.

Slika 55. Izrada novog NLB „*cluster-a“*



Izvor: Autor

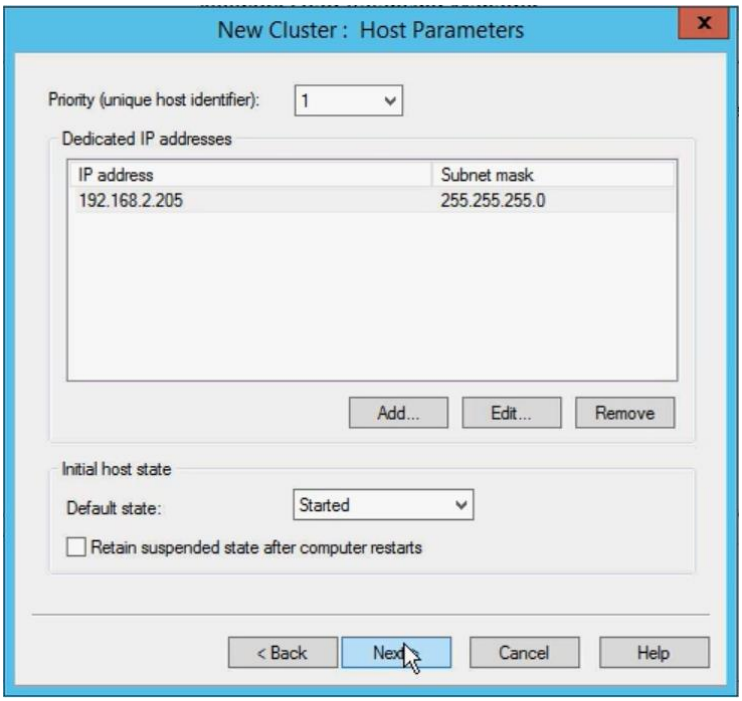
Prvi korak u NLB *Manager*-u potrebno je definirati koji serveri ulaze u *Network Load Balancing Cluster.* Desnim klikom otvaraju se opcije stvaranje novog *cluster*-a ili povezivanje već postojećeg „*cluster*-a“.

Slika 56. Definiranje servera koji ulaze u *NLB „cluster"*

Izvor: Autor

Prva mreža služi za korisnike koji pristupaju do ciljanog serevra preko NLB *cluster* mreže, a druga za direktan pristup administratorima ka konkretnom serveru. U „*New Cluster: Connect"* dijalogu definira se koji host ulazi u *cluster* i jedan od njegovih mrežnih *subnet*-a će se koristiti cluster.

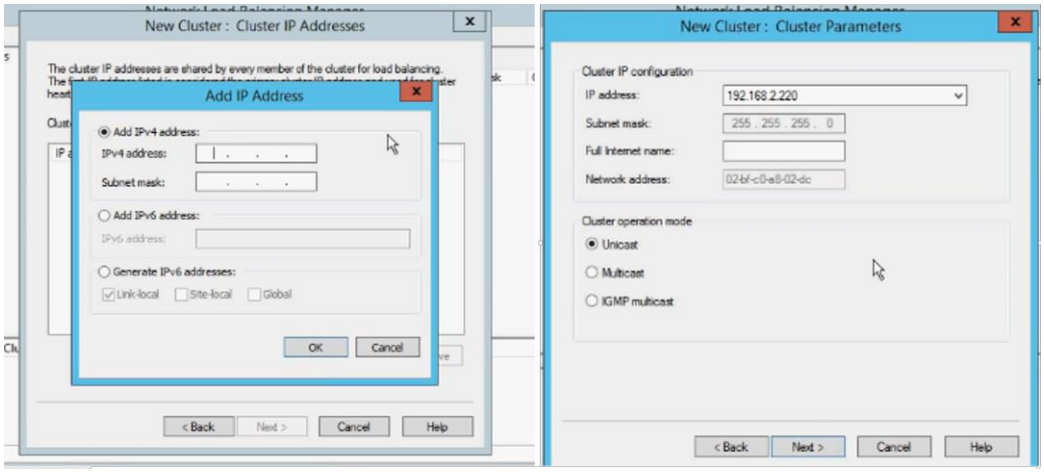
Slika 57. Definiranje prioriteta



Izvor: Autor

U drugom dijalogu definiraju se parametri na „*host*-u“. „*Unique host identifier*“ služi u *multi-cluster* okruženju za definiranje redoslijeda ili važnosti u slučaju prekida jednog od servera, kojim će se odrediti prioritet servera za preuzimanje korisnika. U slijedećem dijalogu definira se IP adresa virtualne cluster mreže i „*Full Internet name“* te izbor operacije *cluster*-a: *Unicast, Multicast ili IGMP multicast*. *Unicast* je standardna operacija i omogućuje zamjenu serverske MAC adrese da bude nadomještena sa *cluster* virtualnom MAC adresom. Prednost mu je veća količina *broadbanda* na raspolaganju. *Multicast* operacijom serveri zadržavaju svoje MAC adrese te popunjuje *broadband* prema *switchevima*. *IGMP multicast* mora biti podržan na mrežnim uređajima u serverskoj okolini koji imaju mogućnost *IGMP multicast* filtriranja prometa koji radi na principu praćenja traženih *port-ova* te tako rasterećuje *multicast* zahtjeve na mreži i oslobađa veći dio *broadband*-a.

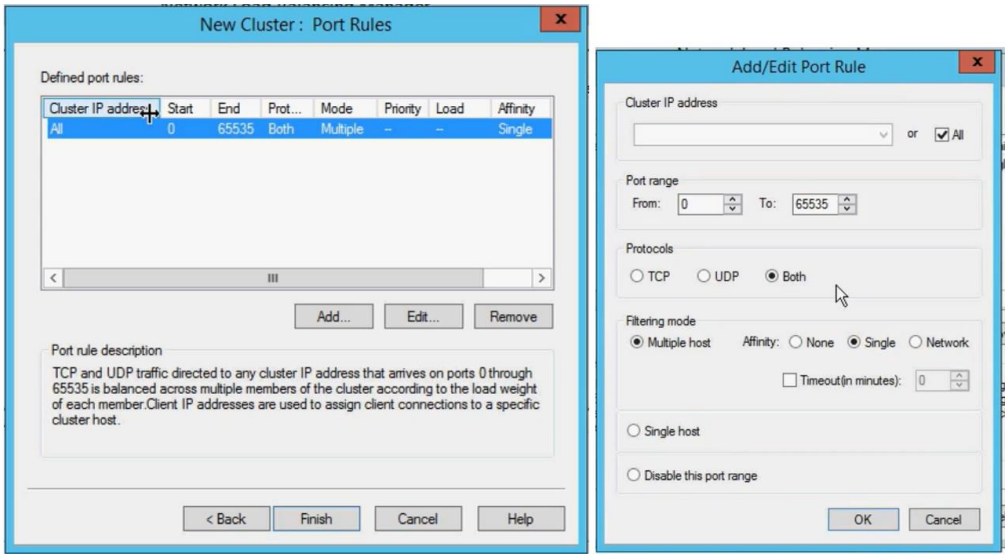
Slika 58. Definiranje virtualne mrežne postavke



Izvor: Autor

Zadnja točka *wizard*-a definira pravila za *port-ove*. U IP adresu unosi se adresa virtualne *cluster* mreže, raspon *port*-ova koji se *cluster*-iraju, protokoli, filtriranje korisnika prema više *host*-ova(*Single* – korisnika smješta na isti server, *None* – nasumični pristup serveru, *Network* – definirano po korisničkoj IP adresi) ili prema *Single host*-u odnosno na isti server (nema mogućnost *Load Balance* već brine samo ako konkretan host prestane raditi da korisnika preseli na drugi server i zadnja opcija je mogućnost izbora u potpunosti zatvoriti *portove* za ovaj *range)*.

Slika 59. Definiranje „*portova*“



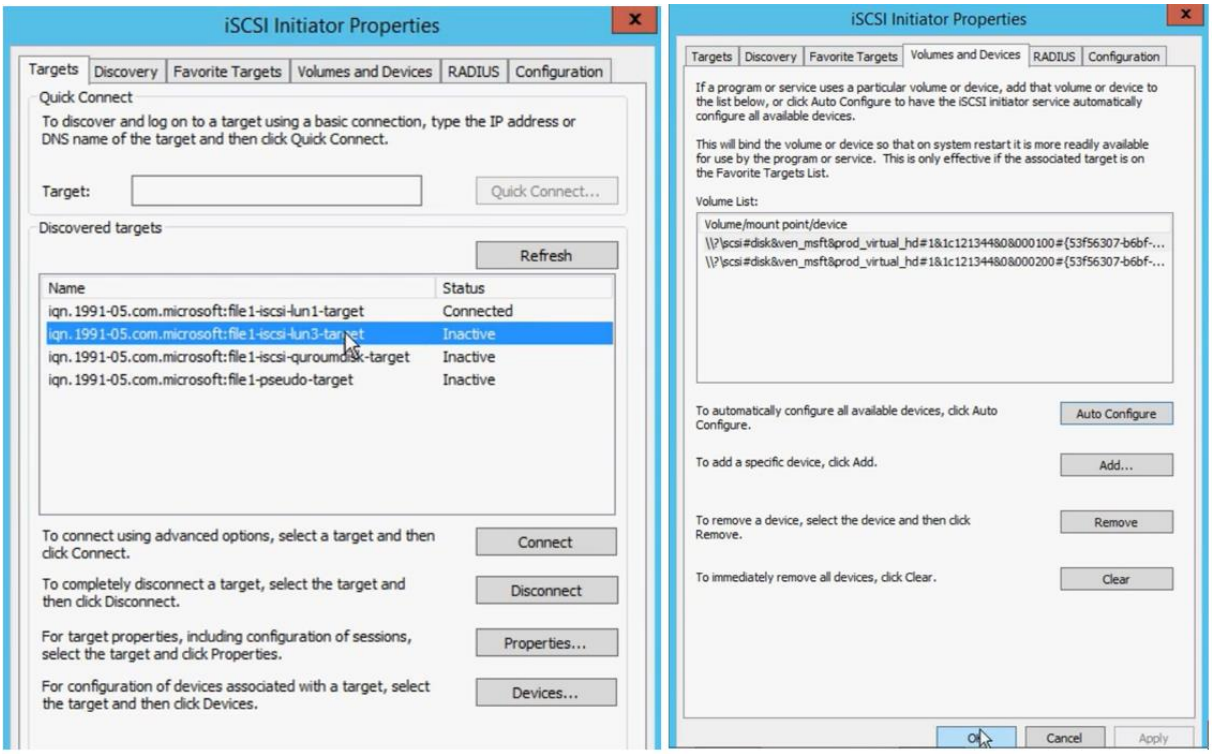
Izvor: Autor

Naknadno u svojstvima *cluster-a* moguće je definirati raspon opterećivanja svakog hosta. Nakon uspješnog dodavanja prvog *host*-a u *cluster* potrebno je dodati i ostale *host*-ove u *cluster*. Desnim klikom izabire se „*Add host to cluster*“, unosi se naziv *host*-a i odabire se adapter sa istim *subnet-om* u kojem je prvi host odnosno virtualna *cluster* mreža, prioritet u mreži i pravila sa *port*-ovima.

15. „*Failover cluster*“

Server „*Failover Cluster“* arhitektura je princip organizacije servera radi postizanja bolje dostupnosti, veće produktivnosti i sprječavanja stanke ili čak potpunog pada sustava. Sastoji se od najmanje 2 *cluster* servera i *storage* servera u SAN mreži i dodatnog *storage-a* pod nazivom „*Quorum*“ (određuje kako je cluster dostupan te ovisno o ishodu definira cluster model). „*Failover Cluster“* je prebacivanje svih resursa sa jednog servera na drugi server ukoliko jedan propada. Prije same instalcije potrebna je dobra priprema svih servera. Na svakom node-u nužno je definirati 3 mrežna adaptera: 1. za produkcijsku mrežu, 2. za „*Heartbeat*“ (komunikacija između *clustera node-ova*) i 3. za komunikaciju sa *storage* serverom. Preporuča se odvojiti svaki adapter u različite *subnet*-e. Nakon definiranja adaptera slijedi instalacija „*Failover Cluster“* značajke na svim serverima. Nakon instalacije potrebno je konektirati sve *node*-ove, npr. putem iSCSI konekcije. Prije same iSCSI konekcije obavezno je dobro pripremiti sve virtualne diskove na *storage* serveru da budu u *Pool*-u te definirati Quorum disk. Na storage je također nužno instalirati iSCSI protokol te nakon instalacije potrebno je iz „*Server Manager*-a“ pod iSCSI kategorijom u meniju „TASKS“ pokrenuti *wizard* za *new iSCSI Virtual Disk*. U *wizardu* odabira se virtualni disk koji će poslužiti za pohranu podataka, dodijeljuje mu se ime i veličina te u dijalogu „*Access Servers*“ puštaju se sve iSCSI konekcije instalirane na cluster serverima. Isti postupak mora se ponoviti i za „*Quorum“* disk. Nakon iSCSI inicijalizacije na *storage*-u se zaključuju konekcije na *cluster* serverima. Potrebno je otvoriti „iSCSI Initiator Properties“ te aktiviriti opcijom „*Connect“* nad virtualnim diskovima te u naprednim postavkama definirati sve potrebne atribute i varijable za adekvatnu konekciju (adapter koji se upotrebljava, IP adresa *storage*-a …) i pod „*Volumes and Devices*“ odabrati „*Auto Configure*“ ta dva virtualna diska na svakom *cluster* serveru.

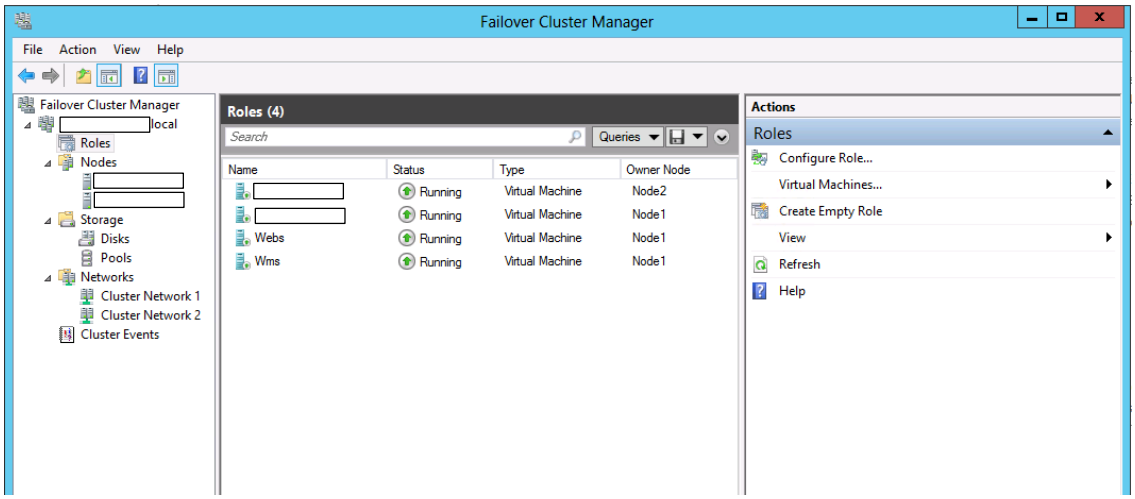
Slika 60. ISCSI konekcija i svojstva



Izvor: Autor

Nakon uspješne konekcije i inicijalizacije virtualnih diskova nužno je aktivirati i formatirati diskove u NTFS iz *Disk Management* konzole. Nakon iniciranja diskova obavezno je iz „*Failover Cluster Manager*“ konzole validirati prethodno konfigurirane clustere te se preporuća pustiti sve testove nad kompletnom konfiguracijom za *cluster*-e. Nakon uspješnih testiranja se iz te iste konzole pokreće *wizard* „Create Cluster Wizard“ gdje se definira naziv *cluster*-a te nova IP adresa za cluster (potrebno ga je dodati u produkcijski subnet).

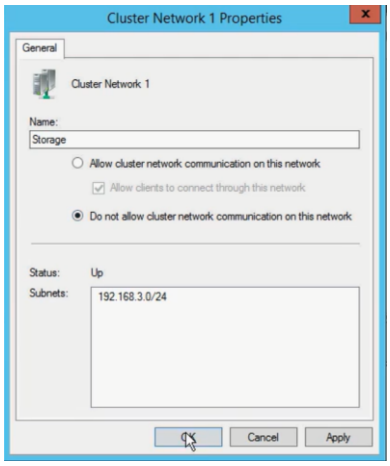
Slika 61. „*Failover Cluster Manager*“ konzola



Izvor: Autor

Nakon uspješne instalacije *cluster*-a zahtjeva se u istoj konzoli dodati virtualne diskove pod kategorijom „*Storage“* te onda pod *„Disks“*. Produkcijski virtualni disk se desnim klikom definira kao „*Cluster Shared Volume*“ umjesto zadanog „*Available Storage*“. Nakon diskova potrebno je definirati 3 mrežna adaptera za adekvatnu komunikaciju u *cluster*-u, odnosno zabraniti adapteru za *storage* komunikaciju da se upotrebljava za *cluster* komunikaciju izborom na „Do not allow cluster network communication on this network“.

Slika 62. Svojstva „*Cluster Network*“



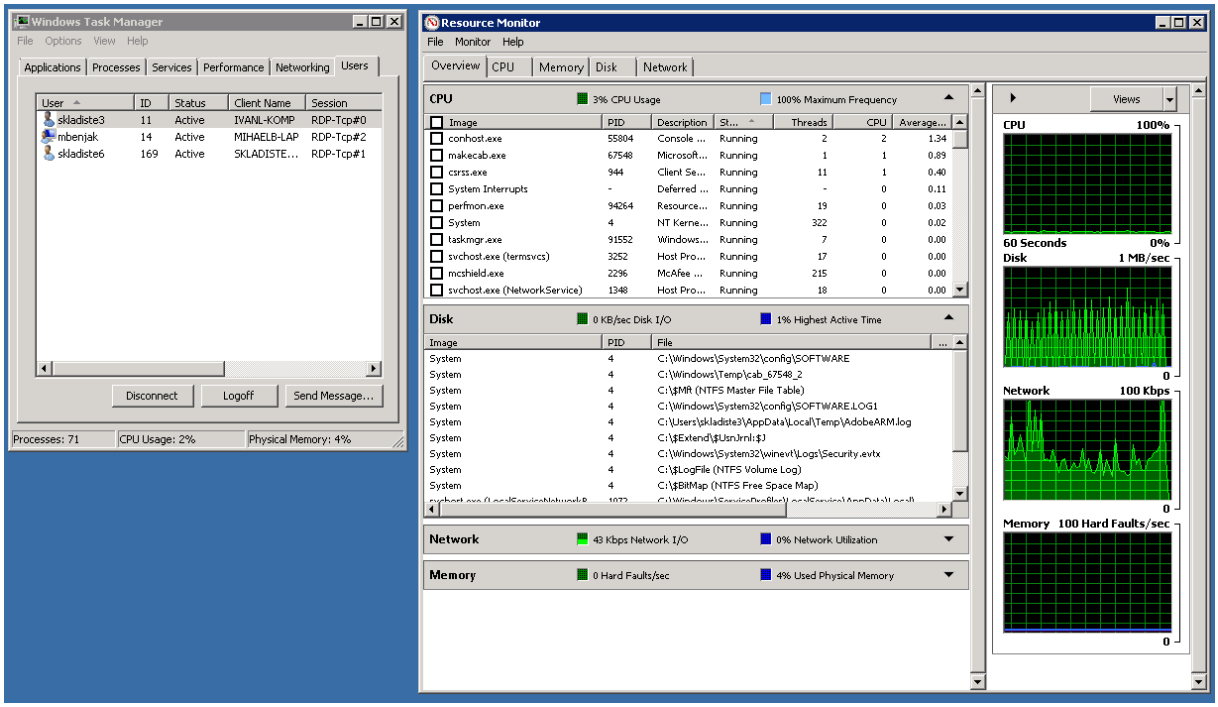
Izvor: Autor

Za drugi adapter koji služi za osluškivanje „*Heartbeat*“ konfigurira se „Allow cluster network communication on this network“, ali je nužno odznačiti „Allow clients to connect through this network“. Za treći adapter ostaju preddifinirane postavke dozvole komunikacije clustera i uporaba konekcija od strane klijenata. Nakon definiranje mreže potrebno je konfigurirati Quorum disk. *Dynamic Quorum* je nova MS tehnologija koja ima automatizam izbora cluster modela ovisno o broju raspoloživih servera u clusteru. *Quorum* može biti smješten kao zasebni disk na *storage*-u ili može biti smješten negdje u mreži kao *file share* nekog uređaja te se takav naziva *Witness disk. Quorum* disk se može definirati kao „*Node Majority*“ u clusterima sa neparnim brojem servera ili „*Node and Disk Majority*“ sa parnim brojem servera. Nakon padanja ili separacije nekih servera, *Quorum* disk je zadužen za definiranje koji serveri ostaju u clusteru, a koji se izbacuju iz njega.

16. Performance monitoring

Praćenje performansi i resursa sa kojima server raspolaže moguće je pratiti putem upravitelja zadataka (engl.“*Task Manager*“) i monitorom resursa (engl. „*Resource Monitor*“) uključenih u svim Windows Server okruženjima.

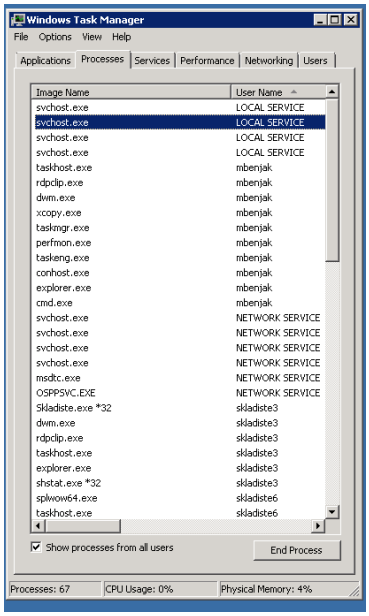
Slika 63. Upravitelj zadataka i resurs monitor



Izvor: Autor

Iz upravitelja zadataka moguće je vršiti pregled nad pokrenutim aplikacijama, njihov status (aktivni ili inaktivni status) te ih prisilno zaustaviti i prekinuti. Iz „Processes“ taba moguće napraviti uvid u sve procese koji se odvijaju na serveru od svih prijavljenih korisnika te ih je također moguće zaustaviti i prekinuti.

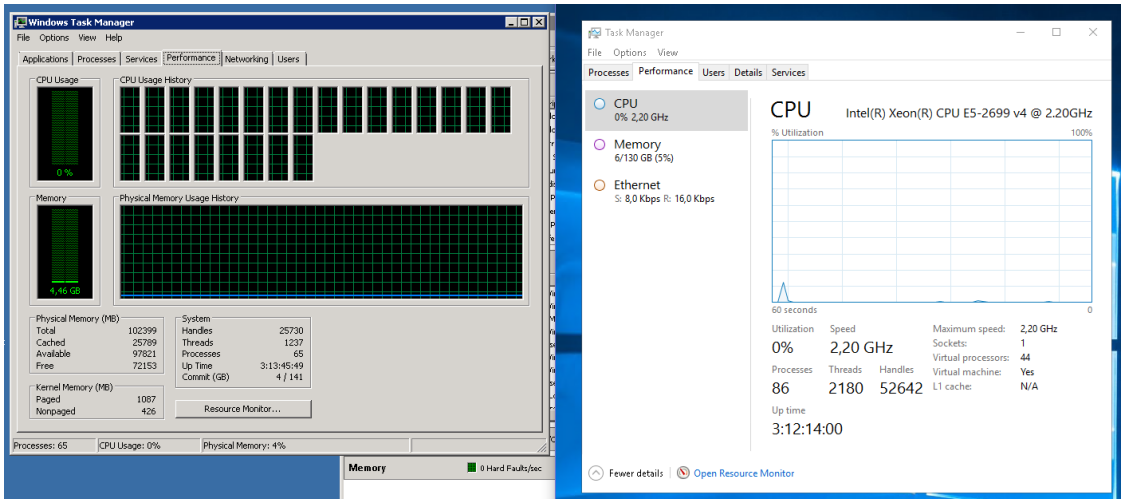
Slika 64. Pregled procesa u upravitelju zadataka



Izvor: Autor

Slijedeći tab su popis servisa koji su obrađeni prethodno u radu. U slijedećem tabu nalazi se osnovni pregled performansa koje se trenutno odvijaju nad serverom.

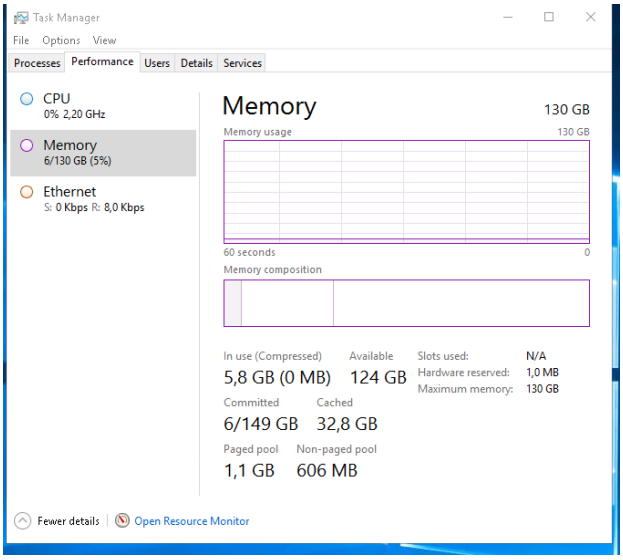
Slika 65. Razlika u kategoriji "*Performance*" starijeg i novijeg OS



Izvor: Autor

Iz ovog taba moguće je napraviti kratki uvid u stanje procesora, memorije i širokopojasne mreže *(engl. „Ethernet Broadband“)*. U starijoj verziji Windows Server operativnog sustava performansi prikazuju se u grafu u jedinici vremena osim širokopojasne mrežne potrošnje koja je naknadno dodana u novijim Windows Server verzijama. U CPU kategoriji prikazuje se vrsta procesora, graf aktivnosti u realnom vremenu i ostali performansi koju se odvijaju nad procesorom poput brzine izražene u frekvenciji, broj trenutnih procesa, dretvi, aktivno vrijeme...

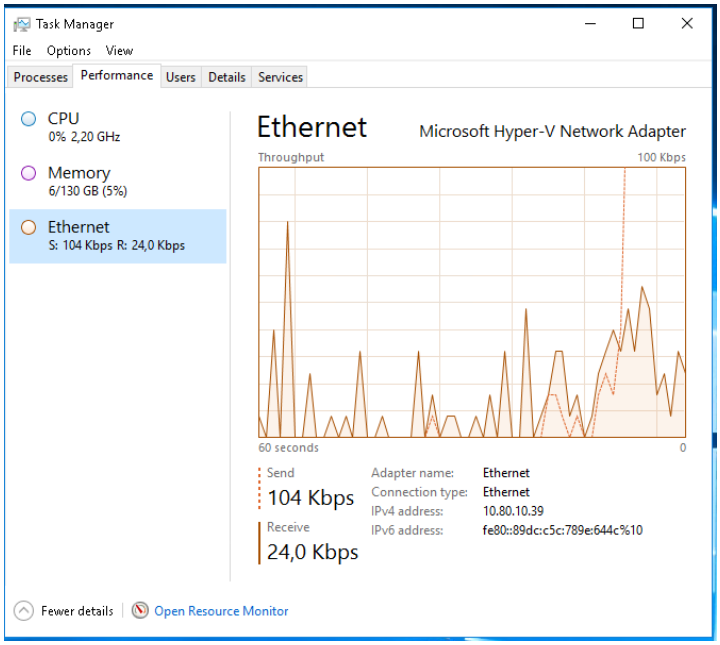
Slika 66. Pregled performansi radne memorije



Izvor: Autor

U drugoj kategoriji prikazuje se stanje radne memorije, odnosno količina zauzetosti/iskoristivosti od sveukupne količine radne memorije sa kojom server raspolaže.

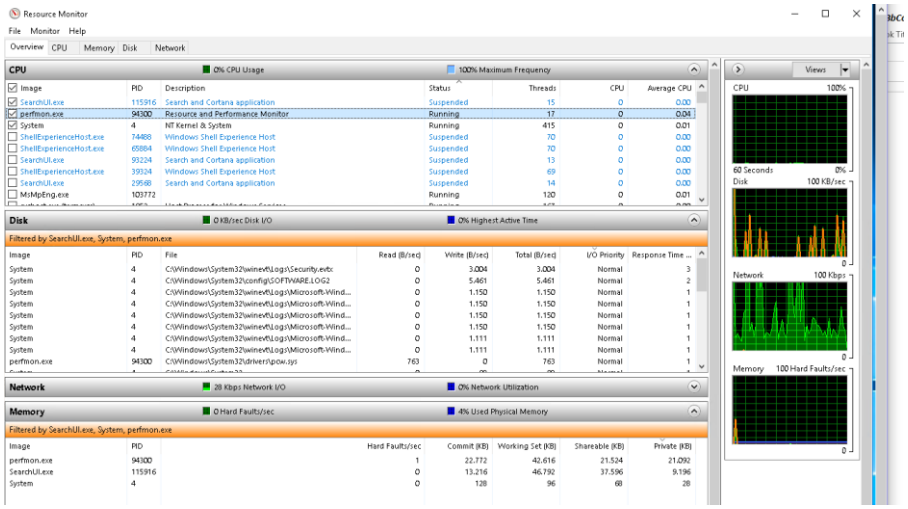
Slika 67. Pregled performasi mrežnog adaptera



Izvor: Autor

Iz treće kategorije vrši se uvid u potrošnju mrežnih resursa, naziv mrežnog adaptera, IP adrese te u trenutnu potrošnju u slanju i primanju podatkovnih paketa izraženu u numeričkoj vrijednosti. Iz „Performance“ *tab*a moguće je pristupiti monitoru resursa koji omogućuje detaljniji uvid u sve procese koji se odvijaju.

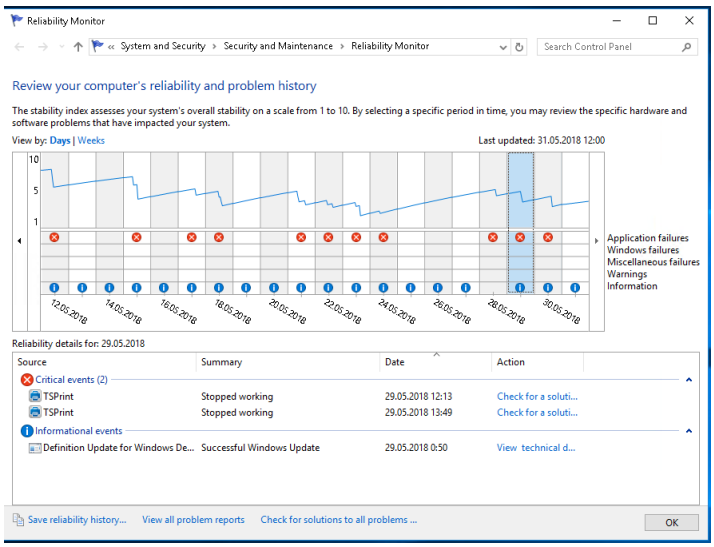
Slika 68. Pregled monitora resursa



Izvor: Autor

U monitoru resursa moguće je također vršiti pregled nad filtriranim objektima i servisima tako da se stvori detaljniji pregled što i koliko troši serverske resurse. Putem alata „Reliability Monitor“ iz upravljačke ploče pod kategorijom „Security and Maintenance“ moguće je napraviti uvid u aktivnosti koje se izvršavaju u jedinici vremena.

Slika 69. Pregled alata *„Realiability Monitor“*



Izvor: Autor

Ovaj alat nam omogućuje prikaz svih bitnih događaja u rasponu u od nekoliko tjedana. Baziran je također po grafikonu koji prikazuje informacije, upozorenja i greške koje su se dogodile u danim vremenskim intervalima. Osim događanja, prikazuje i indeks stabilnosti u danom trenutku na skali od 1 do 10. U ovom alatu moguće je pohranjivati povijest događaja, pregledati sve problematične izvještaje te pretraživanje za mogućim rješenjima.

17. „*Uninterruptible Power Supply*“ –UPS

Kao sigurnosni dodatak fizičkom serverskom okruženju preporuča se uporaba adekvatnih UPS uređaja koji brinu za distribuciju napona i struje do servera. Postavljaju se između servera i izvora napona i struje tako da sve naponske i strujne anomalije prolaze prvo kroz UPS koji regulira dobiveni ulaz u stabilan izlaz napona i struje. Također služe kao dodatni izvor napajanja u slučaju nestanka struje. Sadrže logički sklop koji ima mogućnost upravljanja nad UPS-om i njegovom integriranom baterijom kao izvor električne energije. Sofisticiranije izvedbe posjeduju i „*Menagement*“ priključak koji se veže uz server te omogućuje razmjenu podataka o statusu samog UPS-a, npr. kod nestanka struje, UPS momentalno prelazi u režim distribucije električne energije iz svojih baterija tako da ne ugrozi fizičko stanje i rad servera. U tom periodu šalje informacije serveru te se server može prilagođavati za nadolazeće događaje. Jedna od funkcionalnosti koje omogućava „*Management-a*“ jest smanjenje potrošnje naponskih resursa što relativno uspori performanse, ali omogućuje dužu dostupnost te u zadnjim trenucima raspoloživosti UPS-a sa distribucijom struje omogućuje serveru samostalnu pripremu za gašenje regularnim postupkom umjesto grubog prekida struje. Preporuča se snabdijevanje odvojenih UPS uređaja po svakom serverskom napajanju što je financijski vrlo opterećujuće, ali isplativo zbog sigurnosti fizičkog serverskog okruženja. UPS uređaji drže ograničeni broj ovisno o kapacitetu baterije i kompleksnosti zaštite od naponskih nepravilnosti.

Slika 70. Jednostavni UPS

Izvor: http://www.apc.com/shop/iq/en/products/APC-Smart-UPS-SC-620VA-230V/P-SC620I , 15.5.2018.

18. Windows server *backup*

Jedna od najbitnih sigurnosnih funkcijonalnosti je *Backup*. U sklopu Windows Server OS dolazi alat pod nazivom Windows Server Backup kao dodatak koji je potrebno instalirati iz „Server Manager“. Ovaj alat nam omogućuje više vrsta pohrane podataka: kopija cijelog *HD*-a, „*File level backup*“ koji kopira podatke kao svaki zasebni element i „*Block level backup*“ koji radi inkrementalnu razliku sa izmijenjenim podacima te ovim brzim i efikasnim rješenjem štedi na prostoru pohrane. Korisniku je omogućeno biranje između zakazanog ili trenutnog pokretanja kopiranja podataka. Povratak ili *Restore* posjeduje izbor vraćanja određenih datoteka, cijelovitog servera i DC *restore* ovisno o tipu *Backup*-a koji je izvršen.

Kao sigurnosa mjera postoji još funkcionalnost „*Volume shadow copy*“ koji služi za momentalna vraćanja određenih kopija nekog podatka, odnosno za *restore* u određenom vremenu nastajanja kopije. Može se definirati zakazani termin kada se vrši kopija ili ručno kada korisnik odluči.

19. Ažuriranja

Ažuriranja *(engl. „Updates“)* kao glavi izvor sigurnosnih zakrpa i stabilnosti sustava vrši se automatiziranom funkcijom provjere za raspoloživim ažuriranjima na Microsoft-ovim distribucijskim serverima. Ažuriranje je moguće izvršiti ručno pretaraživanjem na *web*-u, putem „Windows Update“ ili „Windows System Update Service“(skraćeno WSUS). U srednjim i većim poslovnim okruženjima sa ograničenom količinom širokopojasne mreže preporuča se uporaba vlasititog distribucijskog servera za ažuriranja : WSUS server. Primjenom WSUS servera ostvaruje centralno upravljanje nad ažuriranjima te se znatno štedi na širokopojasnoj mreži pogotovo u okruženju sa velikom količinom Windows 10 operativnih sustava do verzije 1711 koji nema mogućnost definiranja brzine i količine prijenosa ažuriranja. WSUS server u domenskom okruženju preuzima ažuriranja za sve Windows verzije koje su mu definirane u konfiguraciji te ih onda lokalno distribuira po računalima u određenim vremenskim intervalima. Posjeduje mogućnost sinkronizacije sa drugim raspoloživim WSUS serverima. Opcija „Sync schedule“ definira vrijeme kada će se sinkronizirati ažuriranja sa računalima, opcija „Automatic approvals“ definira koja ažuriranja nemaju potrebu biti prekontrolirana od strane administratora te ih automatizmom povlači i sinkronizira. Opcija „uvijek dozvoli“ ažuriranja se ne preporuča za upravljačke programe zbog njihove ranjivosti jer neadkvatni software može ugroziti sigurnost i stabilnost sustava. WSUS na korisničkoj strani definira se putem *Group policy*: „Specify intranet Microsoft Update service location“.

20. Zaključak

U ovom radu je teorijski i praktično prikazano kako se instaliraju, rukovode, implementiraju, administriraju i održavaju serveri i računala u umreženoj cjelini što čini jedan informatički sustav. Praktični rad baziran je na testnom virtualnom i realnom okruženju srednje velikog poduzeća koji zahtijeva konstantan pristup podacima skladištenim na serverima. Također, prikazani su načini kako spriječiti padove sustava implementacijom raznih *cluster* rješenja, ažuriranja upravljačkih programa i operativnog sustava, praćenja serverskog zdravlja i fizičke prevencije kvara nad *hardware*-skim komponentama. Ukoliko i dođe do padova sustava, potrebna je dobra pripremljenost administratora informatičkog sustava sa identičnim *hardware*-skim rezervama, ažurnim *backup*-ovima (uključujući podatkovne i sustavne) i dobrim razumijevanjem rada sustava radi otkrivanja problema i razloga pada sustava. Poduzeća i ostali informatički servisi koji upravljaju i raspolažu sa vlastitim serverima zahtijevaju svakodnevnu kontrolu svojih *haredware*-skih komponenti kao i nad samim zdravljem serverskog operativnog sustava uključujući i servisi koji su krucijalni za rad i razvoj poduzeća. Shodno tome, administratori sustava su ključna stavka svakog serverskog okruženja zbog omogućavanja i pružanja informatičkih usluga svojim korisnicima u što boljim uvjetima.

Popisa korištenih kratica u radu

PnP – *Plug and Play*

CMD- *Command Prompt*

DC- *Domain Controller*

DNS- *Domain Name System*

WINS- *Windows Internet Name Service*

DHCP- *Dynamic Host Configuration Protocol*

IIS- *Internet Information Server*

VMS- *Virtual Machine Server*

XML- *Extensible Markup Language*

PXE - *Preboot Execution Environment*

W2003- Windows Server 2003

W2008- Windows Server 2008

W12R2- Windows Server 2012R2

MB- Mega Byte

GB- Giga Byte

TB- Tera Byte

GHz- Giga Hertz

RAID- *Redundant Array of Independent Disks*

MBR- *Master Boot Record*

GPT- *GUID Partition Table*

ERP- *Enterprise Resource Planning*

BI- *Business Intellignce*

RD- *Remote Desktop*

RDC- *Remote Desktop Connection*

RDS- *Remote Desktop Service*

VPN- *Virtual Private Network*

SSL- *Secure Socets Layer*

HTTP- *Hypertext Transfer Protocol*

HTTPS- *Hypertext Transfer Protocol Secure*

WINRM- *Windows Remote Management*

RSAT- *Remote Server Administration Tools*

GP- *Group Policy*

GPO- *Group Policy Object*

IP- *Internet Protocol*

PPP- *Point to Point Protocol*

PPTP- *Point to Point Tunneling Protocol*

L2TP- *Layer 2 Tunneling Protocol*

SSTP- *Secure Socket Tunneling Protocol*

IPsec- *Internet Protocol Security*

IKEv2- *Internet Key Exchange*

UDP- *User Datagram Protocol*

AD- *Acitve Directory*

VHD- *Virutal Hard Disk*

HD- *Hard Disk*

CPU- *Central Processing Unit*

BIOS- *Basic Input/Outpust System*

SCSI- *Small Computer System Interface*

iSCSI- *Internet Small Computer System Interface*

NTFS- *New Technology File System*

SID- *System Identification Number*

OU- *Organisation Unit*

AGDLP- *A*ccount, Global, Domain Local, Permission

SAS- *Serial Attached SCSI*

LAN- *Local Area Network*

SAN- *Storage Area Network*

NAS- *Network Attached Storage*

Gb/s- Gigabit po sekundi

DFS- *Distibuted File System*

NLB- *Network Load Balancing*

MAC- *Medica Access Control*

OS- operacijski sustav

UPS- *Uninteruptible Power Supply*

WSUS- *Windows System Update Service*

Popisa literature

1. Conrad, James, CBT Nuggets Microsoft Windows Server 2012 R2 70-410, CBT Nuggets (video tutorial), 2016

2. Conrad, James, CBT Nuggets - 98-365 Windows Server Admin Fundamentals, CBT Nuggets (video tutorial), 2016

3. Shields, Greg, CBT Nuggets Microsoft Windows Server 2012 R2 70-412, CBT Nuggets (video tutorial), 2017

4. https://msdn.microsoft.com/en-us/library/dd184080.aspx , 22.2.2018.

5. https://docs.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/what-is-a-driver- , 1.4.2018.

6. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd469817(v=ws.10) , 24.4.2018.

7. https://msdn.microsoft.com/en-us/library/windows/desktop/ms681921(v=vs.85).aspx 1.5.2018.

8. https://msdn.microsoft.com/en-us/library/windows/desktop/ms685967(v=vs.85).aspx 5.5.2018.

9. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd469817(v=ws.10) , 15.5.2018.

10. https://en.wikipedia.org/wiki/Storage_area_network , 20.5.2018.

11.https://www.brianmadden.com/opinion/The-Ultimate-Guide-to-Terminal-Server-Printing-Design-and-Configuration , 1.6.2018.

Popis slika