

VISOKO UČILIŠTE ALGEBRA

PROJEKTNI ZADATAK

Sigurnosna pohrana i oporavak IT sustava

Antonio Janach

Zagreb, siječanj 2021.

Sadržaj

1. Uvod.....	1
2. Zahtjevi infrastrukture	2
3. Opis infrastrukture.....	3
4. Topologija infrastrukture	4
5. Priprema infrastrukture	5
5.1. Konfiguracija mrežnog adaptera.....	5
5.2. iSCSI initiator.....	6
5.3. Formatiranje diska	7
5.4. Konfiguracija Veeam Backup repozitorija.....	8
6. Razrada projekta - projektno rješenje	9
6.1. Linux datotečni poslužitelj	9
6.1.1. Konfiguracija NFS datotečnog sustava.....	9
6.1.2. Konfiguracija SMB datotečnog sustava.....	11
6.2. Procedura za izradu sigurnosne pohrane	13
6.3. Izrada sigurnosne kopije konfiguracije	14
6.4. Upravljanje korisničkim podacima.....	16
6.5. Dodavanje Windows i Linux poslužitelja u Veeam	17
6.5.1. Dodavanje poslužitelja po tipu.....	18
6.5.2. Dodavanje poslužitelja u Veeam infrastrukturu	19
6.6. Dodavanje mrežnih datotečnih sustava u Veeam infrastrukturu.....	21
6.7. Dodavanje File Server-a na SQL poslužitelju.....	22
6.8. Kreiranje zadataka za izradu sigurnosnih kopija.....	23
6.8.1. Kreiranje zadataka izrade sigurnosnih kopija dijeljenih mapa.....	24
6.8.2. Raspored izrade sigurnosnih kopija	25
6.9. Mjerenje vremena izrade sigurnosne kopije	27
6.10. Procedura za oporavak iz sigurnosne pohrane.....	28
6.10.1. Oporavak domenskog kontrolera	29
6.10.2. Oporavak Exchange poslužitelja na razini aplikacije.....	32
6.10.3. Oporavak SQL poslužitelja na razini aplikacije.....	35
7. Popis slika.....	38
8. Zaključak.....	39
8.1. Preporuke za sigurnosnu pohranu.....	39
8.2. Prednosti i mane cloud backup rješenja.....	39
9. Literatura.....	41

1. Uvod

Sigurnosna pohrana i oporavak IT sustava definira postupke stvaranja i pohranjivanja kopija podataka koje se mogu koristiti kao sredstvo zaštite od gubitka podataka i brži oporavak usluga koje sustav pruža. Oporavak iz sigurnosnih kopija obično uključuje vraćanje podataka na izvorno mjesto ili na neko drugo mjesto koje se može koristiti umjesto izgubljenih ili oštećenih podataka. Ispravna sigurnosna kopija pohranjena je na zasebnom sustavu ili mediju, radi zaštite od mogućnosti gubitka podataka zbog greške primarnog hardvera ili softvera. Svrha sigurnosne pohrane je stvoriti kopiju podataka koje se mogu oporaviti u slučaju nedostupnosti. Nedostupnost može biti rezultat grešaka u hardveru ili softveru, oštećenje podataka ili događaji uzrokovani korisničkim akcijama, poput zlonamjernog napada (maliciozni programi) ili slučajnim brisanjem podataka. Rezervne kopije omogućuju obnavljanje podataka iz ranijeg vremenskog razdoblja kako bi se oporavili od neplaniranih događaja.

Spremanje kopije podataka na zasebni medij je kritično za zaštitu od gubitka ili korupcije podataka. Dodatni medij može biti jednostavan poput vanjskog pogona ili USB stick-a ili nešto kompleksniji, poput sustava za pohranu diskova, usluga u cloudu ili podatkovnih traka. Dodatni medij može biti spremljen na istom ili udaljenom mjestu. Sigurnosna pohrana pokreće se u redovnim intervalima kako bi se smanjila količina podataka koji se mogu izgubiti. Jednako tako zadržavanje višestrukih kopija podataka pruža osiguranje i fleksibilnost kod vraćanje podataka u određeno vrijeme koje nije pod nekim negativnom utjecajem. Jednako tako potrebno je redovito raditi provjere vraćanja podataka da bi bili sigurni da će i u slučaju oštećenja taj postupak proći kako je planirano.

2. Zahtjevi infrastrukture

Tvrtka X u svom poslovanju koristi hibridnu okolinu (Windows-Linux). Na različitim poslužiteljima nalaze se različite uloge te je potrebno izraditi i implementirati sustav za sigurnosnu pohranu i oporavak sustava.

Poslužitelji koji se trebaju backupirati:

L1 – Linux datotečni poslužitelj (instalirati SMB, NFS, i napravite 10ak datoteka i direktorija koji se koristi za serviranje kroz SMB, i 10ak datoteka i direktorija koji se koristi za serviranje kroz NFS)

L2 – Linux poslužitelj s KVM virtualizacijom

SDC – Windows poslužitelj s AD DC i DHCP ulogom

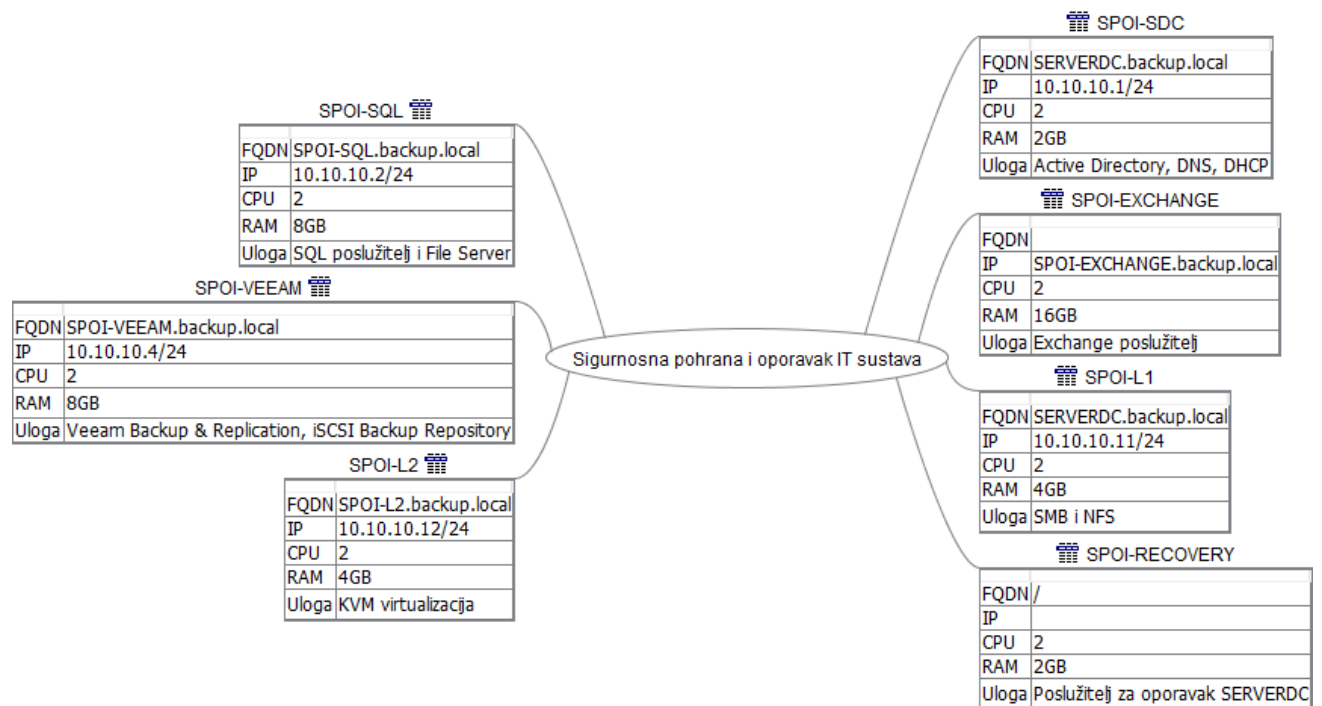
S1 – Windows poslužitelj sa SQL poslužiteljem i File Server ulogom (za datotečni poslužitelj, isti scenarij kao kod poslužitelja L1 – napraviti 10ak datoteka i direktorija koji moraju biti uključeni u backup)

S2 – Windows poslužitelj s Exchange poslužiteljem

S3 – Windows poslužitelj s instaliranim Veeam manager-om Enterprise Plus Edition licence

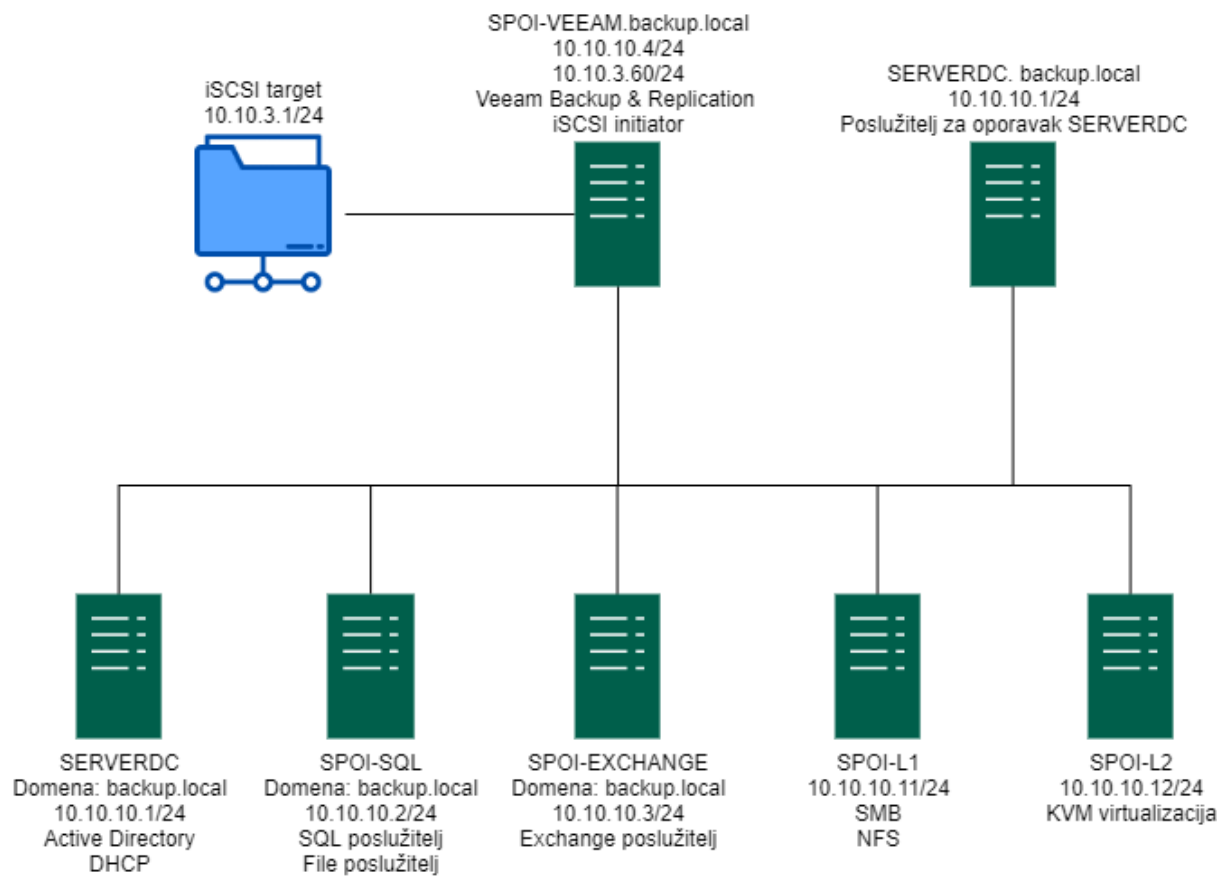
S4 – prazna virtualna mašina u kojoj je montiran bootabilan Veeam RE environment

3. Opis infrastrukture



Slika 1: prikaz opisa infrastrukture kroz umnu mapu

4. Topologija infrastrukture

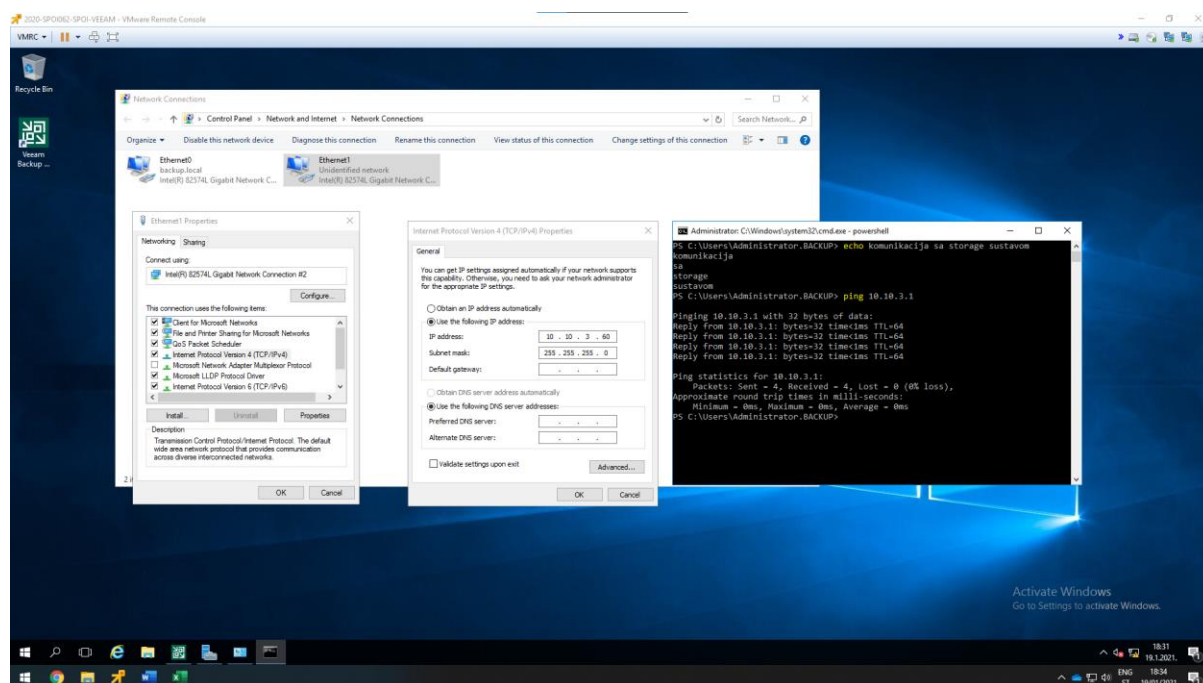


Slika 2: prikaz topologije infrastrukture

5. Priprema infrastrukture

5.1. Konfiguracija mrežnog adaptera

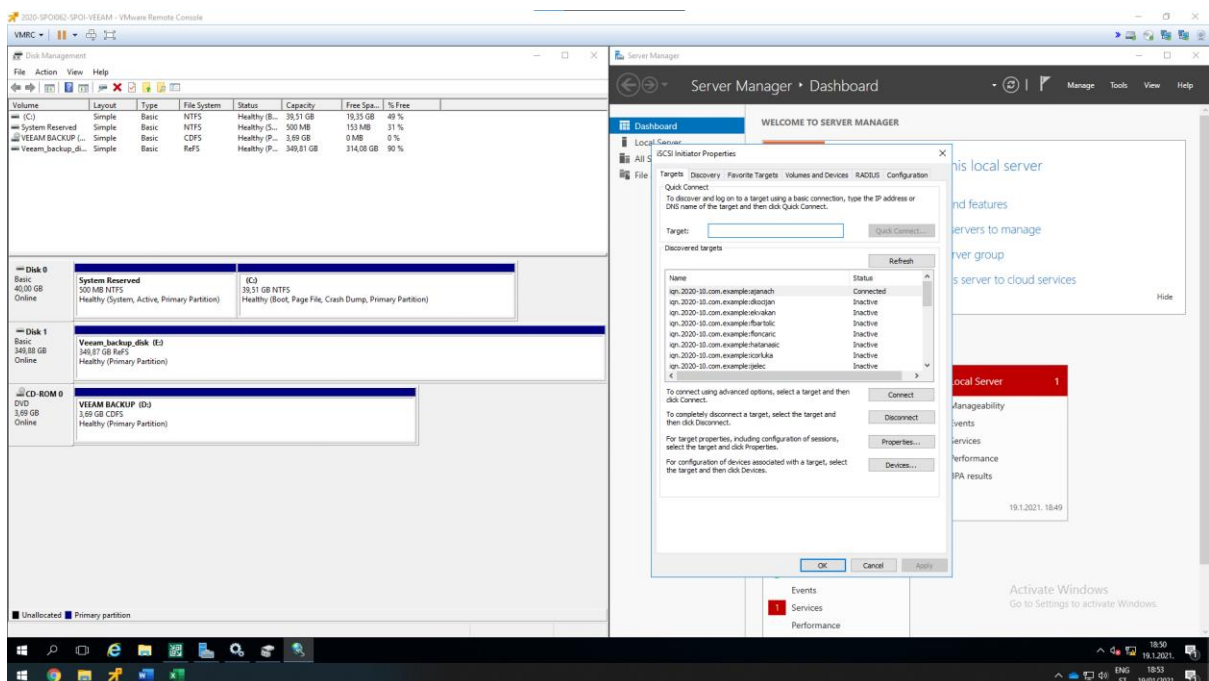
Polazimo od virtualne mašine koja ima instaliran Veeam management FQDN-a SPOI-VEEAM.backup.local. Virtualna mašina na sebi ima dva mrežna adaptera. Prvi mrežni adapter je domenski i služi za komunikaciju s ostalim računalima koja su u domeni backup.local. Drugi mrežni adapter namijenjen je za storage i služi za komunikaciju s iSCSI diskom. Preporuka je imati posebno mrežni adapter za storage promet što bi značilo da drugi mrežni adapter treba konfigurirati tako da on može komunicirati sa storage sustavom koji na sebi pokreće iSCSI protokol. IP adresa storage sustava je 10.10.3.1, a LUN na koji se SPOI-VEEAM.backup.local virtualna mašina spaja ima IP adresu 10.10.3.60.



Slika 3: konfiguracija mrežnog adaptera

5.2. iSCSI initiator

Uspješnom konfiguracijom drugog mrežnog adaptera virtualne mašine FQDN-a SPOI-VEEAM.backup.local nužno je pokrenuti iSCSI initiator servis kako bi inicirali konekciju sa storage sustavom. iSCSI Initiator servis dolazi default-no instalacijom Windows server poslužitelja. Kako bi se pokrenuo servis i inicirala konekcija sa storage sustavom potrebno se je pozicionirati u Server Manager konzolu, zatim u gornjem desnom izborniku lijevim klikom odabrati Tools i iz padajućeg izbornika odabrati iSCSI Initiator. Ako se prvi puta pokreće iSCSI Initiator opcija Windows server poslužitelj pitat će nas da li želimo prije same konfiguracije initiator-a uključiti trajno servis, na poruku se odgovara sa „da“. Nakon toga otvaraju se značajke iSCSI initiator-a. U karticu Targets upisati IP adresu storage sustava koja je 10.10.3.1 i spojiti se na LUN imena „iqn.2020-10.com.example:ajanach“. Nakon spajanja pozicionirati se na karticu Volumes and Devices i pritisnuti na opciju Auto Configure. Nakon toga disk koji je dodijeljen od strane storage sustava spreman je na korištenje i priključen je u sustav virtualne mašine.

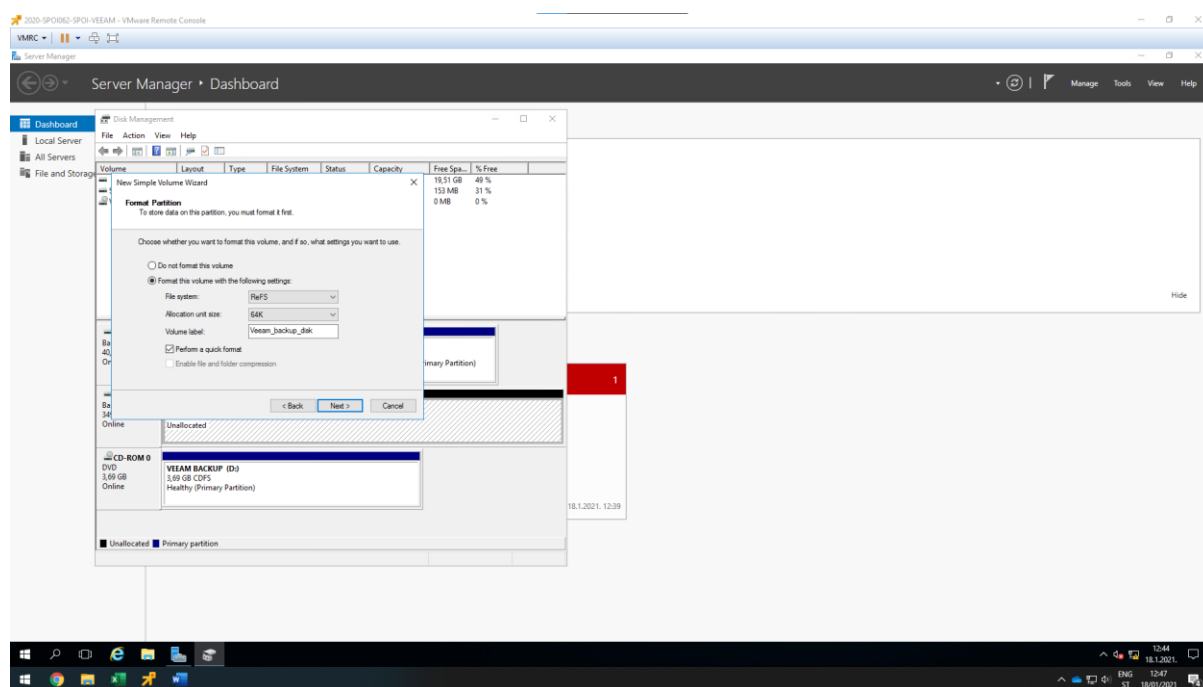


Slika 4: spajanje na storage sustav koristeći iSCSI protokol

5.3. Formatiranje diska

Disk koje je dodijeljen na korištenje, kapaciteta je 350GB. Disk je inicijaliziran u GPT partijsku tablicu. Zatim je kreiran volumen file system-a ReFS, allocation unit size-om 64K i naziva „Veeam_backup_disk“. File system i allocation unit size namjerno su podešeni prema ovim parametrima jer ako damo na korištenje drugi file system s drugačijim parametrom allocation unita, kod dodavanja Backup repozitorija u Veeam Manager-u javit će grešku da ti parametri nisu preporučljivi već ovi koji su prethodno navedeni a to su file system diska ReFS s allocation unit size-om 64K.

Kad se govori o tome koji file system koristiti NTFS ili ReFS, odgovor leži u tome da se mogu koristiti oba file system-a za Veeam Repository. No kad se govori o prednostima i manama treba uzeti u obzir da ReFS file system omogućava Veeam software-u korištenje „Fast Clone“ značajke za bržu izradu sintetičkih operacija full backup-a. Dok NTFS omogućava brži restore iz full backup-a. Shodno tome odabran je ReFS file system iz razloga jer se češće obavlja zadatak full backup-a, nego restore-a. Što se tiče blokova veličine s razlogom su odabrani 64KB veličine. Razlog odabira ove veličine bloka je zato što, ako je manja veličina bloka prostor na disku neće biti potraćen bez veze uz performanse koje rezultiraju boljima.

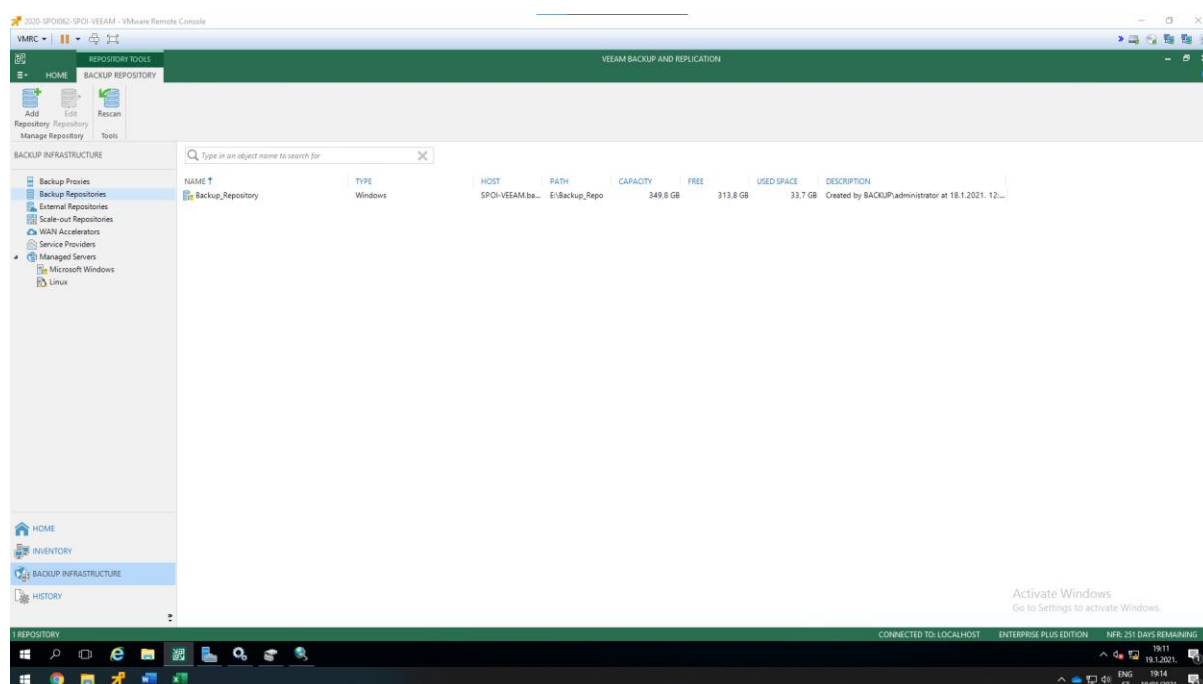


Slika 5: formatiranje diska file system-a ReFS

5.4. Konfiguracija Veeam Backup repozitorija

Dodavanje novog repozitorija na E:\ disk koji je priključen putem iSCSI protokola i brisanje zadanog repozitorija koji ima putanju na C:\ disku.

Kako bi se konfigurirao Veeam Backup repozitorij potrebno je upaliti Veeam management konzolu s prečaca koji se nalazi na radnoj površini Windows server poslužitelja. Kod paljenja Veeam management konzole potrebno se je prijaviti s domenskim administratorom. Zatim kliknuti na Backup Infrastructure kako bi se otvorio konfiguracijski panel. Desnim klikom kliknti na Backup Repositories iz lijevog izbornika i odabrati Add Backup Repository. Otvara se čarobnjak naziva New Backup Repository s konfiguracijskim prozorom. Repozitoriju je dodano ime „Backup_Repository“ i kliknuti next, pošto se radi o Microsoft Windows poslužitelju možemo ostaviti preddefinirane postavke. Zaustaviti se na dijelu „Repository“ gdje treba dodati putanju diska. Putanja disk u ovom slučaju je E:\Backup_Repo. Dalje ostaviti sve preddefinirane postavke i kliknuti na finish. Ako primjećujemo, sada u Veeam managemen konzoli postoje dva Backup Repository-a gdje je jedan zadani, a drugi je kreiran od strane korisnika. Defaultni je nužno obrisati jer nema nikakvu svrhu. Prije nego ga se može obrisati potrebno je postaviti novokreirani repozitorij kao defaultni za izvršavanje backup-a. Kad je to postavljeno može se obrisati default-ni repozitorij koji ima putanju C:\Backup.



Slika 6: Kreiranje novog Backup repozitorija

Ovima završava dio koji opisuje pripremu infrastrukture. Sljedeća poglavlja opisuju razradu projekta koji se sastoji od procedure za izradu sigurnosne pohrane, procedure za oporavak cjelokupnih ili pojedinih dijelova sustava.

6. Razrada projekta - projektno rješenje

6.1. Linux datotečni poslužitelj

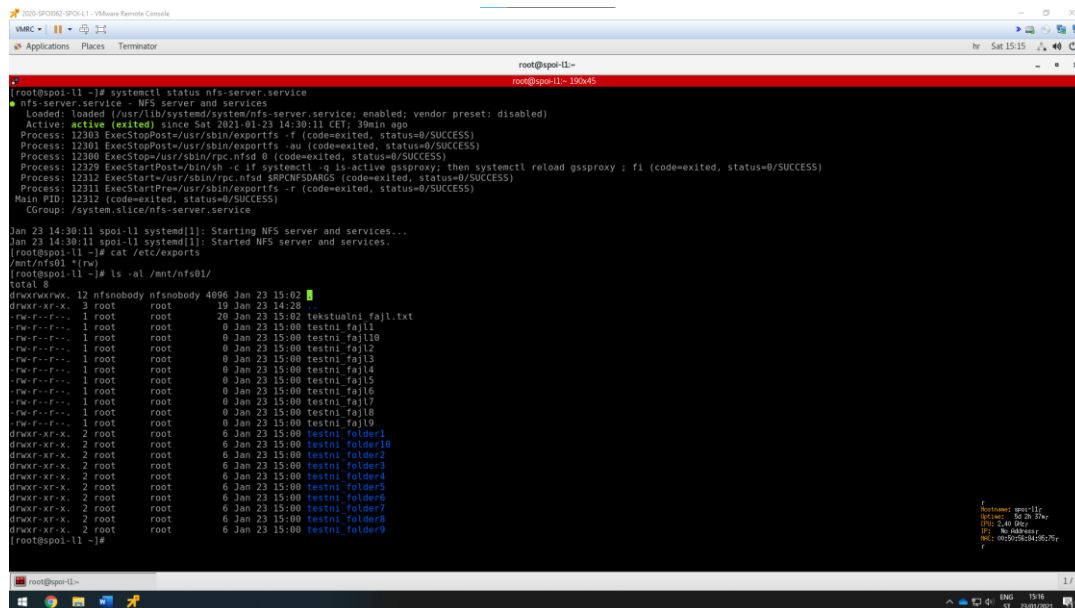
Svaka tvrtka ima potrebu za pohranom i razmjenom podataka. Tako podaci moraju biti osigurani od gubitaka i visokodostupni. Da bi se ti podaci osigurali od gubitaka, potrebno je osmisliti strategiju i implementirati rješenje za sigurnosno kopiranje. Naime, dijeljenje podataka ostvaruje se pomoću datotečnih poslužitelja koji omogućuju centralnu pohranu podataka i lakše upravljanje pravima pristupa. Datotečni poslužitelji obično koriste jedan od dva protokola, a to su Network File System(NFS) ili Server Message Block(SMB). Obično se korištenje NFS protokola koristi u Linux okruženjima, a SMB protokol u Windows okruženjima. Također valja napomenuti da je moguće korištenje SMB protokola u Linux okruženju i NFS protokola u Windows okruženju.

Ulogu Linux datotečnog poslužitelja obavljat će L1 Linux poslužitelj. Na L1 linux poslužitelj instalirani su SMB i NFS mrežne datotečne sustave za pristupanje udaljenim uređajima preko mreže. Navedena dva datotečna sustava koja su uspostavljena na L1 Linux računalu *backupirati* koristeći Veeam software.

6.1.1. Konfiguracija NFS datotečnog sustava

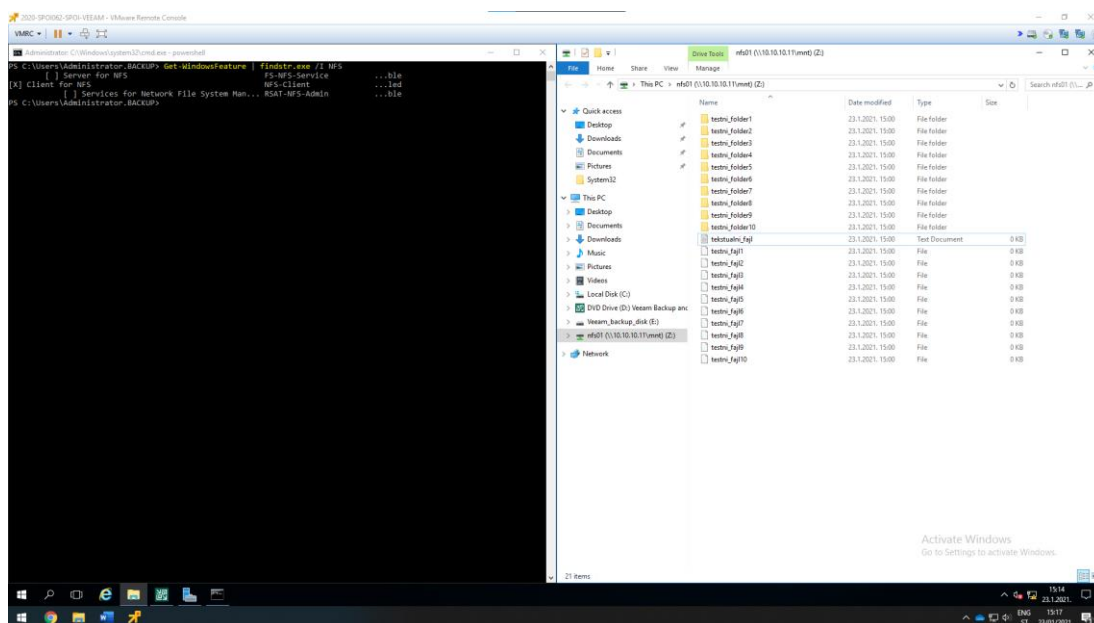
Prikaz izvršenih radni za uspostavu uspješne uspostave NFS datotečnog sustava.

```
#instalacija NFS servisa:
yum install nfs-utils
#omogućeno pokretanje i pokretanje pri paljenju za nfs servis:
systemctl enable nfs-server
systemctl start nfs-server
#datoteka kontrolira koji se datotečni sustavi izvoze na udaljene hostove:
echo „/mnt/nfs01 *(rw)“ >> /etc/exports
#postavljena prava nad datotekom:
chown nfsnobody:nfsnobody /nfsshare
chmod 777 /mnt/nfs01
#kreirati 10 foldera i 10 datoteka
Mkdir testni_folder{1..10}
Touch testni_fajl{1..10}
```



Slika 7: prikaz NFS konfiguracije na Linux L1 poslužitelj

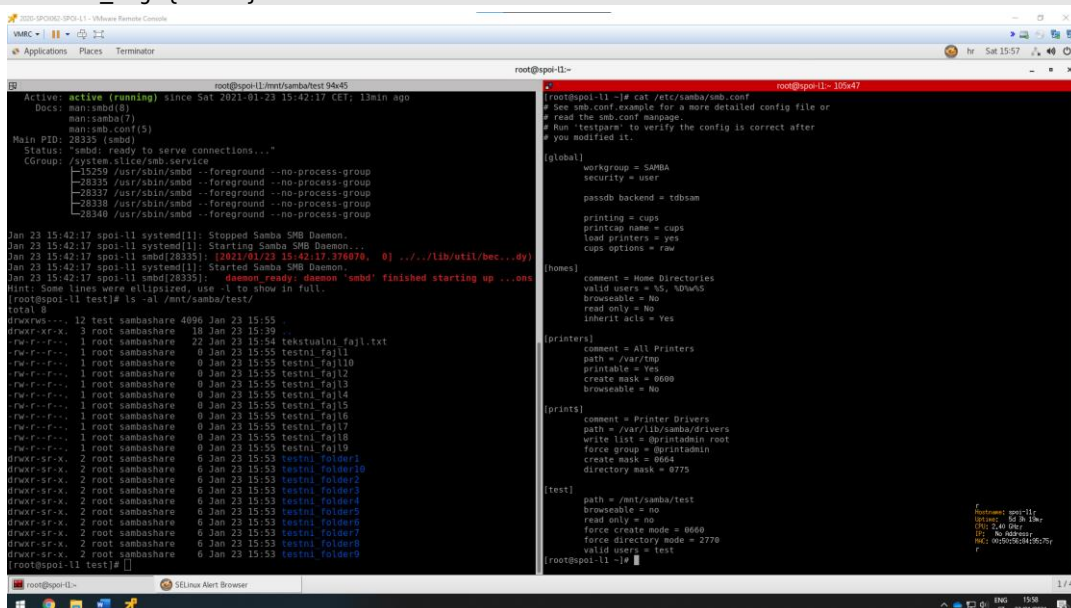
Kako bi dokazali da mrežni datotečni sustav NFS radi bit će montiran na Windows poslužitelj s instaliran Veam software-om. Stoga je potrebno na Windows poslužitelj instalirati značajku Client for NFS i potom mapirati mrežni disk.



Slika 8: NFS mrežni datotečni sustav radi

6.1.2. Konfiguracija SMB datotečnog sustava

```
#instalacija NFS servisa:
Yum -y install samba samba-client
#omogućeno pokretanje i pokretanje pri paljenju za nfs servis:
systemctl enable smb
systemctl start smb
#kreiranje direktorija koji će biti dijeljeni
Mkdir /mnt/samba
#dodavanje grupe za smb share
Groupadd sambashare
Chgrp sambashare /mnt/samba
Useradd -M -d /mnt/samba/test -s /usr/sbin/nologin -G sambashare test
#kreiranje direktorija u share-u
Mkdir /mnt/samba/test
#podešavanje prava nad direktorijem
Chown test:sambashare /mnt/samba/test
Chmod 2770 /mnt/samba/test
#kreiranje password-a za pristup smb share-u
Smbpasswd -a test
Smbpasswd -e test
#unos parametra u konfiguracijsku datoteku
Vim /etc/samba/smb.conf
[test]
    path = /mnt/samba/test
    browseable = no
    read only = no
    force create mode = 0660
    force directory mode = 2770
    valid users = test
#kreirati 10 foldera i 10 datoteka
Mkdir testni_folder{1..10}
Touch testni_fajl{1..10}
```



```
root@spoi-l1:~# systemctl status smb
Active: active (running) since Sat 2021-01-23 15:42:17 CET; 13min ago
Docs: man:smbd(8)
      man:samba(7)
      man:smb.conf(5)
Main PID: 28335 (smbd)
Status: "smbd: ready to serve connections..."
Group:
├─system.slice/smb.service
├─15250 /usr/sbin/smbd --foreground --no-process-group
├─28335 /usr/sbin/smbd --foreground --no-process-group
├─28337 /usr/sbin/smbd --foreground --no-process-group
├─28338 /usr/sbin/smbd --foreground --no-process-group
└─28340 /usr/sbin/smbd --foreground --no-process-group

Jan 23 15:42:17 spoi-l1 systemd[1]: Stopped Samba SMB Daemon.
Jan 23 15:42:17 spoi-l1 systemd[1]: Starting Samba SMB Daemon...
Jan 23 15:42:17 spoi-l1 smbd[28335]: [2021/01/23 15:42:17:0.000000] ../../lib/util/bec...dy)
Jan 23 15:42:17 spoi-l1 systemd[1]: Started Samba SMB Daemon.
Jan 23 15:42:17 spoi-l1 smbd[28335]: daemon ready; daemon 'smbd' finished starting up ...ont
Hint: Some lines were ellipsized, use -l to show in full.
[root@spoi-l1 test]# ls -ol /mnt/samba/test/
total 8
drwxr-xr-x. 3 root sambashare 4096 Jan 23 15:55
drwxr-xr-x. 1 root sambashare 22 Jan 23 15:55 tekstualni_fajl.txt
-rw-r--r--. 1 root sambashare 0 Jan 23 15:55 testni_fajl1
-rw-r--r--. 1 root sambashare 0 Jan 23 15:55 testni_fajl10
-rw-r--r--. 1 root sambashare 0 Jan 23 15:55 testni_fajl2
-rw-r--r--. 1 root sambashare 0 Jan 23 15:55 testni_fajl3
-rw-r--r--. 1 root sambashare 0 Jan 23 15:55 testni_fajl4
-rw-r--r--. 1 root sambashare 0 Jan 23 15:55 testni_fajl5
-rw-r--r--. 1 root sambashare 0 Jan 23 15:55 testni_fajl6
-rw-r--r--. 1 root sambashare 0 Jan 23 15:55 testni_fajl7
-rw-r--r--. 1 root sambashare 0 Jan 23 15:55 testni_fajl8
-rw-r--r--. 1 root sambashare 0 Jan 23 15:55 testni_fajl9
drwxr-sr-x. 2 root sambashare 6 Jan 23 15:53 testni_folder1
drwxr-sr-x. 2 root sambashare 6 Jan 23 15:53 testni_folder10
drwxr-sr-x. 2 root sambashare 6 Jan 23 15:53 testni_folder2
drwxr-sr-x. 2 root sambashare 6 Jan 23 15:53 testni_folder3
drwxr-sr-x. 2 root sambashare 6 Jan 23 15:53 testni_folder4
drwxr-sr-x. 2 root sambashare 6 Jan 23 15:53 testni_folder5
drwxr-sr-x. 2 root sambashare 6 Jan 23 15:53 testni_folder6
drwxr-sr-x. 2 root sambashare 6 Jan 23 15:53 testni_folder7
drwxr-sr-x. 2 root sambashare 6 Jan 23 15:53 testni_folder8
drwxr-sr-x. 2 root sambashare 6 Jan 23 15:53 testni_folder9
[root@spoi-l1 test]#
```

```
root@spoi-l1:~# vim /etc/samba/smb.conf
[global]
    workgroup = SAMBA
    security = user
    passdb backend = tdbsam
    printing = cups
    printcap name = cups
    load printers = yes
    cups options = raw

[homes]
    comment = Home Directories
    valid users = %S, %S%w
    browseable = No
    read only = No
    inherit acls = Yes

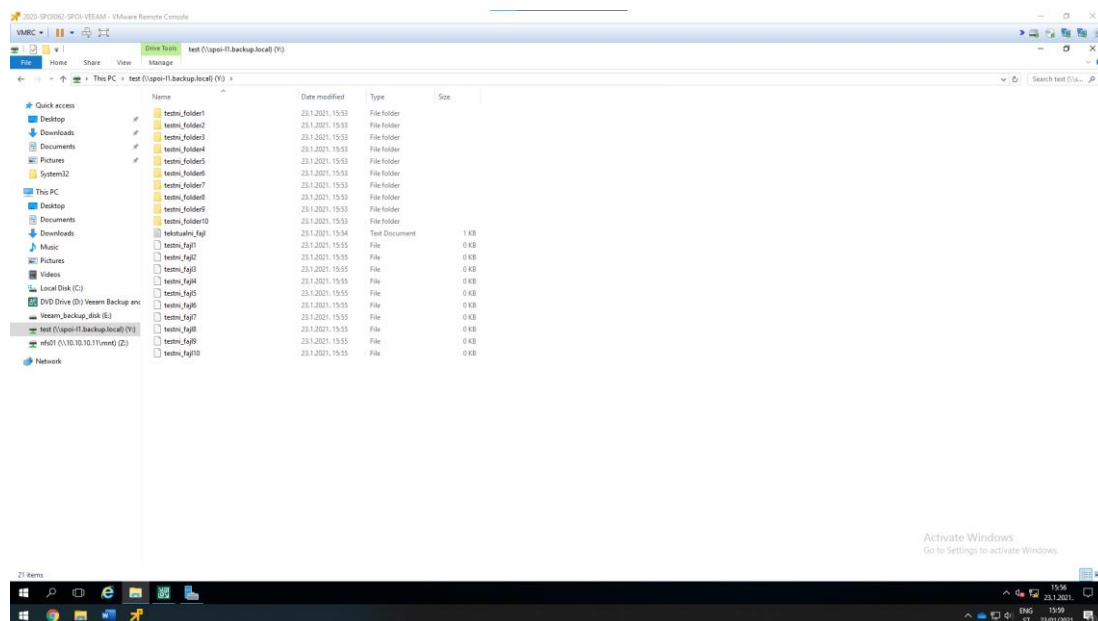
[printers]
    comment = All Printers
    path = /var/tmp
    printable = Yes
    create mask = 0600
    browseable = No

[print$]
    comment = Printer Drivers
    path = /var/lib/samba/drivers
    write list = @printadmin root
    force group = @printadmin
    create mask = 0664
    directory mask = 0775

[test]
    path = /mnt/samba/test
    browseable = no
    read only = no
    force create mode = 0660
    force directory mode = 2770
    valid users = test
    root@spoi-l1:~#
```

Slika 9: prikaz SMB konfiguracije na Linux L1 poslužitelju

Kako bi dokazali da mrežni datotečni sustav SMB radi bit će montiran na Windows poslužitelj s instaliranim Veeam software-om. Stoga je potrebno mapirati mrežni disk.



Slika 10: SMB datotečni sustav radi

6.2. Procedura za izradu sigurnosne pohrane

Za izradu procedure sigurnosne pohrane na ispravan način nužno je da su uređaji dodani prema Veeam infrastrukturi. Bitno je naglasiti da se pohrana radi van produkcijskih sati kako bi se omogućilo zaposlenicima da neometano rade na infrastrukturi. Razlog tome je što sigurnosna pohrana oduzima resurse na poslužiteljima kako bi bila izrađena.

Zahtjevi tvrtke X su sljedeći:

- Korištenje maksimalne kompresije pri izradi svakog backupa radi štednje prostora
- Svi serveri osim KVM hosta moraju imati item-level recovery (dakle, moguć recovery datoteke, objekta, tablice, baze, maila, mailboxa, ovisno o servisu o kojem je riječ)
- Backup mora biti podešen tako da se radi dva puta na dan
- Item-level backup za SQL i Exchange moraju biti podešeni da rade tri puta na dan
- Backup mora biti složen tako da ne radi korupciju podataka za vrijeme backupa, ili za vrijeme recovery procedure
- Veeam mašinu ne backupirati samu na sebe –Veeam mašina se koristi samo za backup

Zahtjevi jasno govore kako je nužno poslužiteljima SPOI-SQL i SPOI-EXCHANGE izraditi zadatak sigurnosne pohrane 3 puta na dan, dok ostalim poslužiteljima 2 puta na dan. Trenutno sigurnosnoj infrastrukturi postavljena je sigurnosna pohrana koja pohranjuje svih pet servera sa „item-level recovery“ funkcijom i „health check“ procedurom. Što se tiče synthetic full backup-a i inkremental backupa oni se izrađuju na sljedeći način: synthetic full backup se radi tijekom ne radnog dana u tjednu, a to je nedjelja. Inkrementalni backup se radi svim ostalim danima u tjednu sve do sljedeće nedjelje. Također, valja naglasiti da se radi i backup same konfiguracije Veeam software-a frekvencije svakog dana.

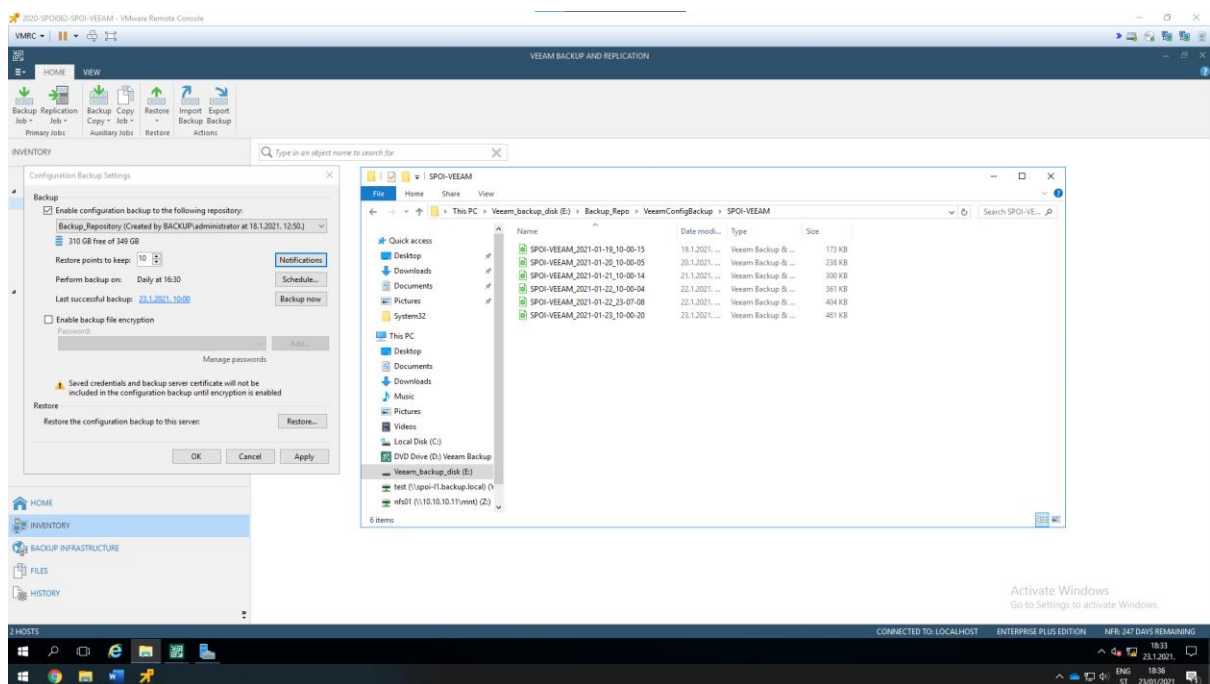
6.3. Izrada sigurnosne kopije konfiguracije

Veeam backup software omogućava sigurnosnu kopiju konfiguracije. Time se osigurava sprječavanje ne željenih akcija koje su se provele nad Veeam backup software-om. Neki od primera su ako Veeam backup poslužitelj iz nekog razloga prestane raditi, on može se ponovno instalirati na neki drugi poslužitelj i na njega se može učitati konfiguraciju iz sigurnosne kopije.

Tijekom sigurnosne kopije konfiguracije, Veeam Backup software izvozi podatke iz baze podataka same konfiguracije i sprema ih u datoteku sigurnosne kopije u spremištu sigurnosnih kopija tj. sam Backup Repository. Preporuča se redovita izrada sigurnosne kopije konfiguracije na dnevnoj bazi.

Sigurnosna kopija konfiguracije konfigurira se na sljedeći način. Potrebno je otvoriti Veeam backup software na Veeam poslužitelju. Zatim u lijevom gornjem ćošku samog sučelja kliknuti na hamburger meni, te iz padajućeg izbornika odabrati „Configuration Backup“. Otvara se prozor „Configuration Backup“ Setting gdje se daljnja konfiguracija odvija.

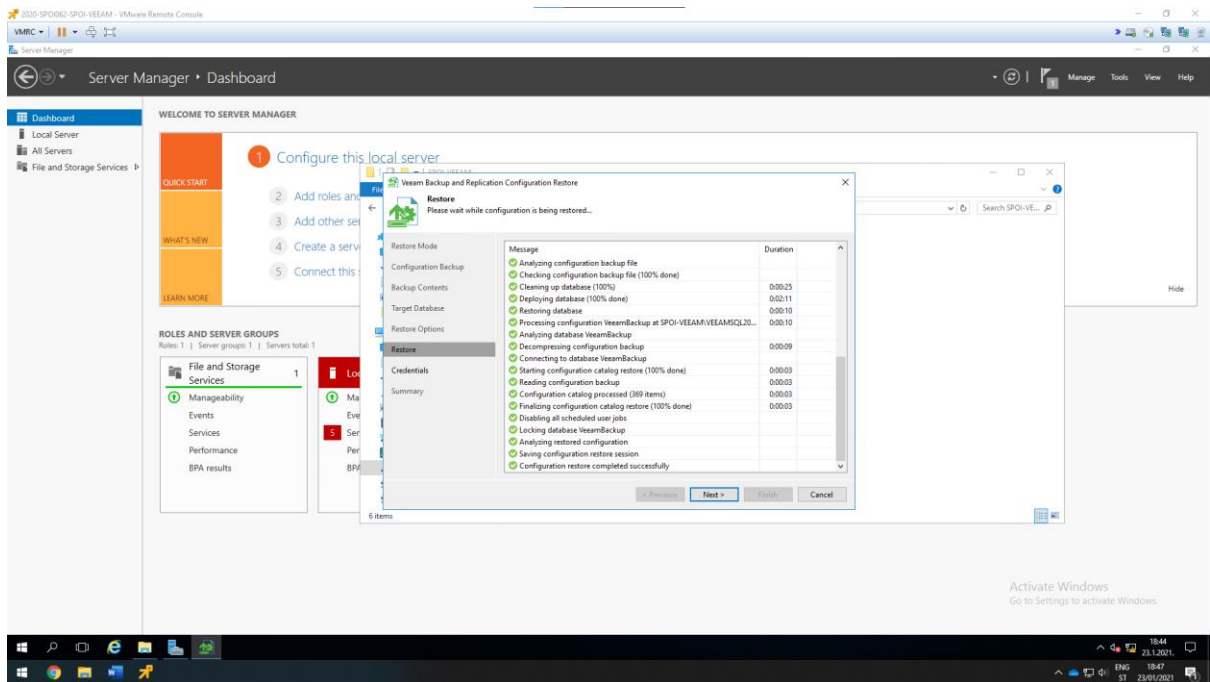
Izrada sigurnosne kopije konfiguracije izrađuje se svakim danom u 16:30 s držanjem do 10 točaka oporavka. Razlog odabira ove frekvencije izrade sigurnosne kopije konfiguracije je zato što se smatra da radno vrijeme Administratora Veeam infrastrukture završava u 16:00. Te ne drugo poslije radnog vremena izrađuje se sigurnosna pohrana.



Slika 11: Postavke izrade sigurnosne kopija

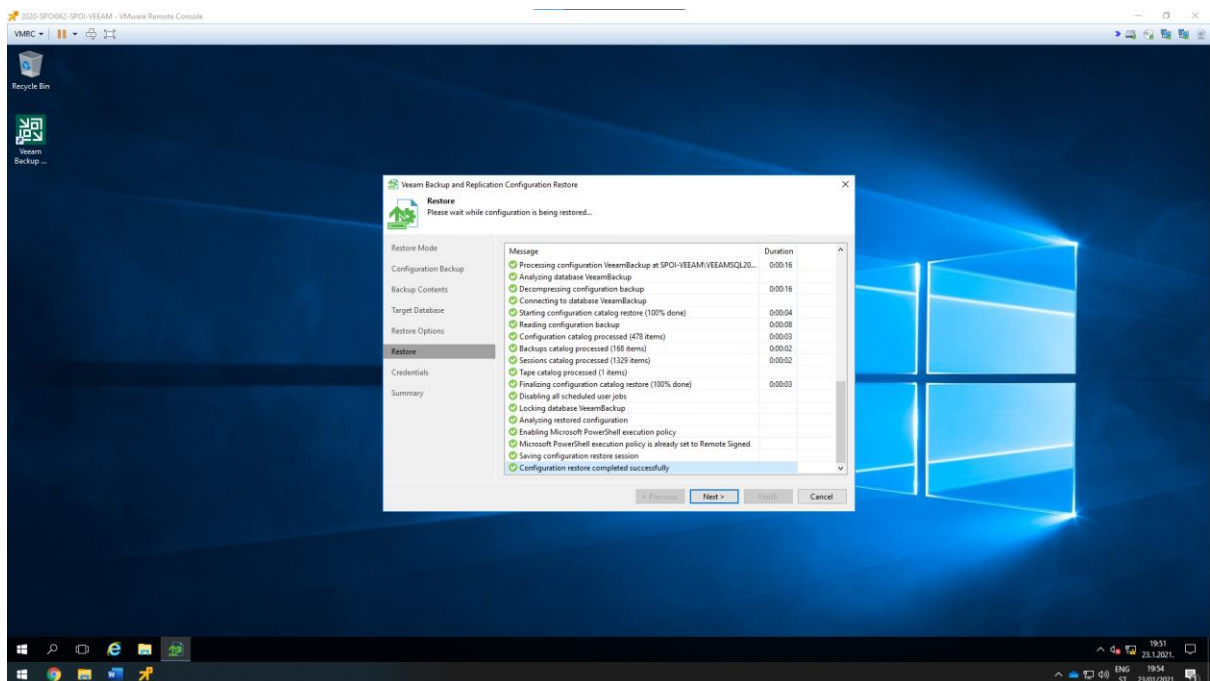
Kao što je vidljivo iz slike 9 sigurnosna kopija konfiguracije sprema se u Backup Repository na E:\ disku.

Za oporavak sigurnosne kopije konfiguracije potrebno je iz otvorenog prozora Configuration Backup Setting-a odabrati Restore. Otvara se Wizard gdje je moguće odabrati Restore ili Migrate metodu. Kako bi se testiralo uspješan restore sigurnosne kopije konfiguracije nužno je odabrati metodu Restore. Nakon toga odabrati Backup Repository i jedan od backup datoteka sigurnosne kopije konfiguracije. Te ostale postavke ostaviti na zadanom stanju i kliknuti na restore. Veeam software se gasi sve dok se oporavak sigurnosne pohrane ne povrti, kad je radnja izvršena on se ponovno pali.



Slika 12: oporavka sigurnosne kopije konfiguracije na početno stanje

Za potrebe ovog demo-a vratit ću Veeam software konfiguracijsko stanje na ono koje je bilo koristeći istu metodu oporavka sigurnosne kopije konfiguracije.

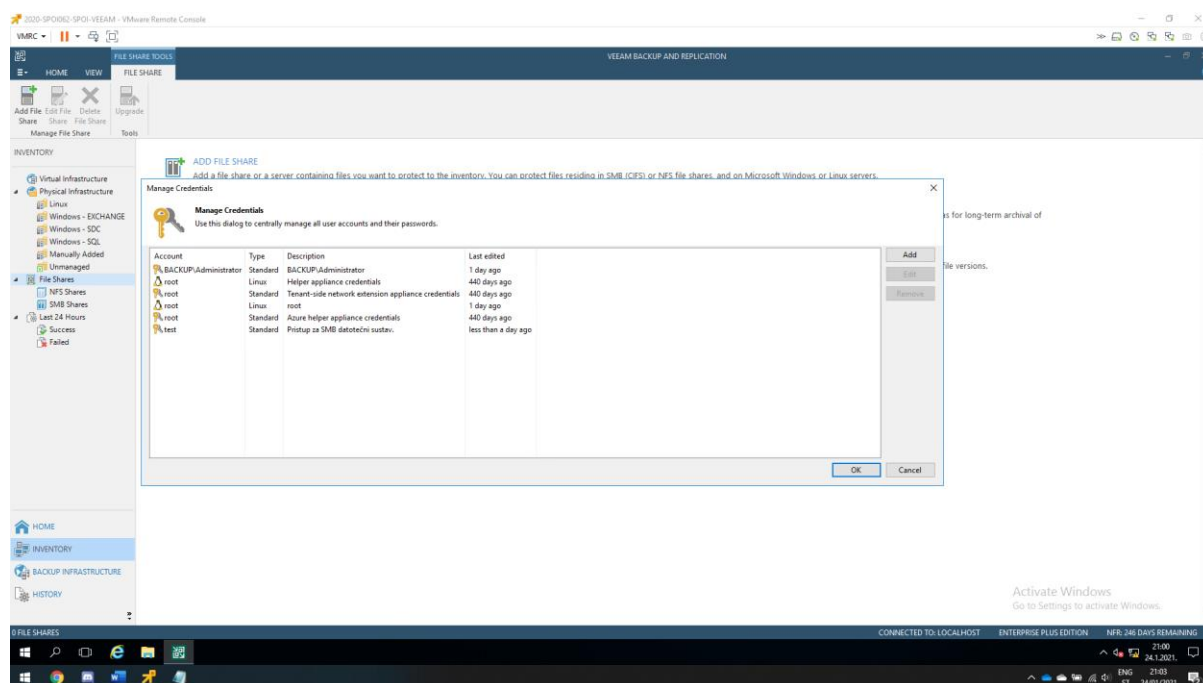


Slika 13: oporavak sigurnosne kopije konfiguracije na trenutno stanje

6.4. Upravljanje korisničkim podacima

Korak upravljanja korisničkim podacima dostupan je za upravljanje korisničkim podacima računalima u domeni ili posebno za svakoga računala. Upravljanje korisničkim podacima omogućava lakšu administraciju računala koja su npr. U domeni. To bi značilo da kad se jednom doda korisničkim račun u ovom slučaju od domenskog administratora, taj korisnički podatak može se koristiti za sva računala koja su u toj domeni i nije nužno kod kreiranja novog zadatka za izrade sigurnosnih kopija ili dodavanja poslužitelja u Veeam infrastrukturu, ponovno upisivati korisničke podatke domenskog administratora već ga odabrati iz izbornika s ostalim dodanim korisničkim podacima.

Dodavanje korisničkih podataka se dodaje na sljedeći način, u lijevom gornjem kutu nalazi se hamburger ikona, klikom na nju otvara se padajući izbornik iz kojeg je potrebno odabrati Manage Credentials. Otvara se prozor Manage Credentials i s desne strane prozora se nalazi gum Add, pritiskom na taj gumb dodaju se korisnički podaci za domenska računala i Linux računala. Kad se dodaju korisnički podaci klikom na OK spremaju se podaci i gasi se otvoreni prozor. Ovim postupkom značajno se skraćuje vrijeme kad će se izrađivati Job-ovi sigurnosnih kopija računala.



Slika 14: dodavanje korisničkih podataka

Korisnički podaci koji su dodani su korisnički računi BACKUP\Administrator, root i test. Prvi korisnički račun služi za prijavu na domenska računala, odnosno SERVERDC.backup.local, SPOI-SQL.backup.local, SPOI-EXCHANGE.backup.local i SPOI-VEEAM.backup.local. Drugi korisnički račun služi za prijavu na Linux računala SPOI-L1.backup.local i SPOI-L2.backup.local. Dok treći korisnički račun služi za pristup na SMB datotečni sustav dijeljenih foldera.

6.5. Dodavanje Windows i Linux poslužitelja u Veeam

Kako bi bilo moguće izrađivati sigurnosne kopije, nužno je dodati poslužitelje u Veeam infrastrukturu. Treba napomenuti da bi uopće bilo moguće dodati poslužitelje u Veeam infrastrukturu mrežno dijeljenje datoteka mora biti propušteno kroz Vatro zid, točnije za računala koja su u domeni Backup svi poslužitelji moraju moći pristupiti dijeljenim datotekama drugih servera koje su zadano kreirane.

Kod dodavanja poslužitelja u Veeam infrastrukturu instaliraju se sljedeće komponente na poslužitelje, a to su:

- Veeam Backup Transport
- Veeam Installer Service
- Ovisno o operacijskom sustavu:
 - Veeam Agent for Microsoft Windows Redistributable
 - Veeam Agent for Linux Redistributable

Veeam Backup Transport instalirava se na poslužitelj kako bi se učinkovitost posla i vrijeme potrebno za izradu sigurnosnih kopije uvelike pospješilo. Ova metoda omogućuje način transporta za dohvaćanje podataka s poslužitelja.

Veeam Installer Service se kod dodavanja poslužitelja u Veeam infrastrukturu instalira. To je softverski program koji sve svoje radnje koje su zadane od strane Veeam management obavlja u pozadini.

Veeam Agent je rješenje za zaštitu podataka i oporavak od katastrofe za fizičke i virtualne strojeve. Veeam Agent može se koristiti za različitu vrstu računala i uređaja: stolnih računala, prijenosnih računala i tableta. Veeam agent nudi razne značajke za zaštitu podataka sa:

- Eksternih načina pohrane od CD-a do vanjskih jedinica tvrdih diskova
- Stvaranje cijele sigurnosne kopije sustava, sigurnosne kopije određenih računala ili pojedinačnih mapa s datotekama

Značajke koje su nabrojane također mogu se pohraniti na vanjske tvrde diskove, dijeljene mape, u Veeam Backup Repository, Veeam Cloud Connect, pa čak i na Microsoft OneDrive.

U slučaju katastrofe pomoću ove značajke mogu se izvršiti sljedeće operacije:

- Vraćanje podataka iz sigurnosnih kopija na prvobitno mjesto ili na novo mjesto
- Izvršenje Bare-Metal Restore-a

Kod dodavanja poslužitelja u Veeam infrastrukturu koristit će se korisnički podaci koji su prethodno dodani u Veeam infrastrukturu. Te su nužna administrativna prava nad svim računalima kod dodavanja poslužitelja u Veeam infrastrukturu, što bi značilo imati prava nad pristupom korisničkom disku.

6.5.1. Dodavanje poslužitelja po tipu

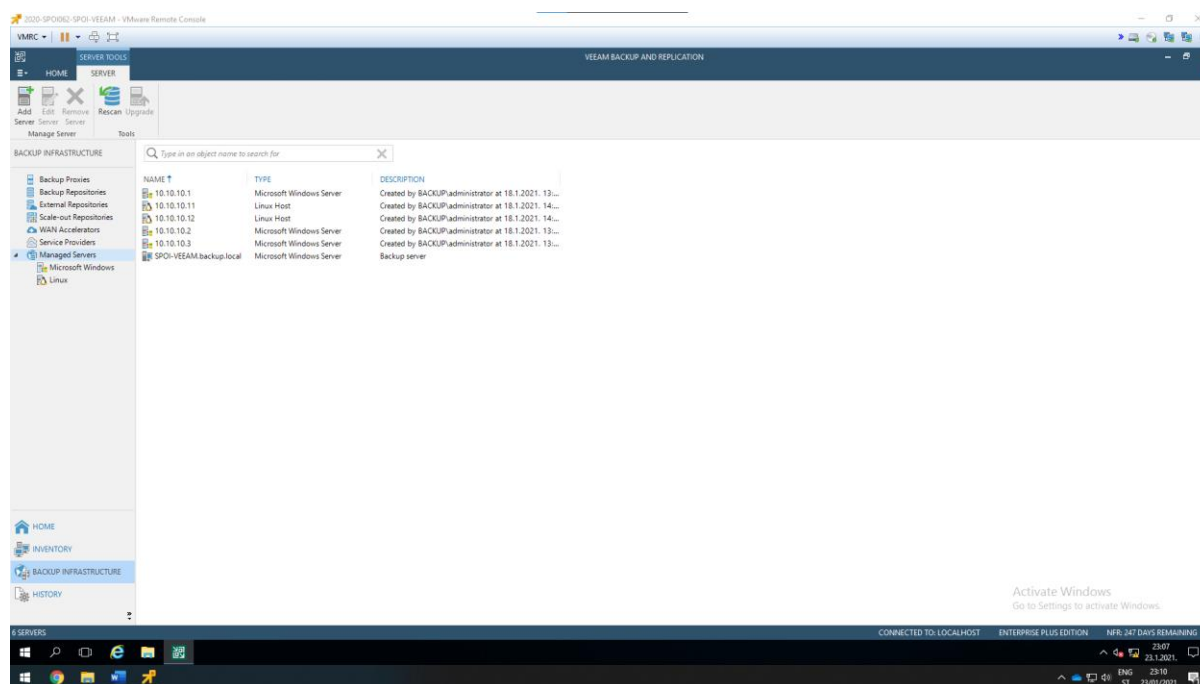
Dodavanje poslužitelja u Managed Servers. U Managed Servers dodaju se poslužitelji po tipu npr. Vmware vSphere, Microsoft Hyper-V, Microsoft Windows ili LnuX. U doljnjem lijevom kutu kliknuti na Backup Infrastructure i iz izbornika odabrati managed servers i odabrati opciju Add Server. Otvara se Wizard koji traži da se unese DNS ime poslužitelja ili Ipv4 adresa. Valja napomenuti IP adrese računala koja će biti dodana u infrastrukturu:

- 10.10.10.1 - SERVERDC.backup.local
- 10.10.10.2 - SPOI-SQL.backup.local
- 10.10.10.3 - SPOI-EXCHANGE.backup.local
- 10.10.10.11 - SPOI-L1.backup.local
- 10.10.10.12 - SPOI-L2.backup.local

Klikom na „Next“ otvara se kartica „Credentials“ potrebno je odabrati odgovarajuće korisničke podatke za određeni poslužitelj, npr. Za Windows računala koristiti BACKUP\Administrator, a za Linux računala koristiti root. Kliknut na „Next“.

Otvora se kartica Review gdje se jasno vidi da će se na dodani poslužitelj instalirati komponenta imena „Transport“. Klikom na „Apply“ i na kraju „Finish“ završava dodavanje poslužitelja u Veeam Managed Servers.

Ovaj postupak ponoviti za sva računala koja će biti dodana u Managed Servers.



Slika 15: prikaz dodanih računala u Managed Servers

6.5.2. Dodavanje poslužitelja u Veeam infrastrukturu

Kad su poslužitelji dodani po tipu u „Managed Servers“ sad se ta računala mogu staviti u zaštitne grupe kako bi se olakšala implementacija i izrada zadatka za izradu sigurnosnih kopija. Odlukom, Windows poslužitelji stavljeni su u odvojene grupe, dok je Linux poslužitelj stavljen u jednu.

Da bi se dodali poslužitelji u zaštitne grupe potrebno se je iz lijevog donjnjeg izbornika pozicionirati na „Inventory“. Desnim klikom miša odabrati „Physical Infrastructure“ i pritisnuti na „Add Protection Group“. Zatim se otvara „Wizard“ gdje je potrebno dati ime grupi zatim, klikom na Next otvara se kartica „Type“. U ovu karticu za Windows poslužitelje odabrati opciju „Microsoft Active Directory objects“, dok je za Linux računala nužno odabrati „Individual Computers“. Ako se odabere opcije „Microsoft Active Directory objects“ klikom na „Next“ pojavljuje se okvir za dodavanje računala iz „Active Directory“, ovdje je potrebno odabrati poslužitelj koji se želi dodati u Veeam infrastrukturu. Klikom na „Next“ otvara se kartica „Exclusion“ ovdje je potrebno maknuti sve opcije koje su vezane za „Exclude“. Sve ostale postavke ostaviti na zadano sve do kartice „Options“. Kartica „Options“ vrlo je važna i odnosi se na dio koji ulazi u proceduru za izradu sigurnosne kopije. U ovoj kartici podešavaju se postavke frekvencije vezane za skeniranje zaštitne grupe koja omogućava otkrivanje novo dodanih računala u zaštitnu grupu, ali i za otkrivanje dostupnosti samog poslužitelja u zaštitnoj grupi. Klikom na „Advanced“ moguće je postaviti i slanje dnevnog izvještaja na specifičnu E-mail adresu, što omogućava Veeam administratoru, u slučaju događaja neke anomalije detekciju problema s dostupnosti poslužitelja na vrijeme. Klikom na „Next“ može se vidjeti koje komponente su sve instalirane na računalo, a to su „Veeam Backup Transport“, „Veeam Distribution Service“ i „Veeam Agent“. Ovime završava dodavanje poslužitelja u Veeam infrastrukturu.

Odabirom „Individual Computers“ nužno je samo navesti IP adresu poslužitelja, a sve ostale postavke odabrati da odgovaraju zahtjevima infrastrukture.

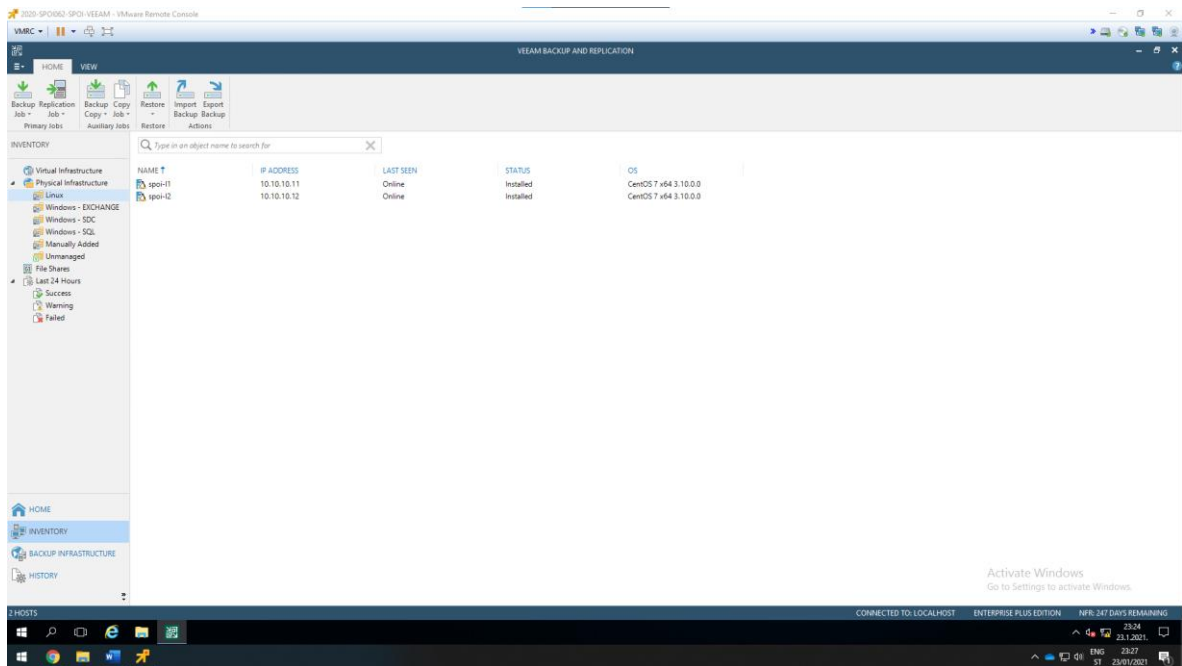
Naziv zaštitne grupe	Frekvencije skeniranja zaštitne grupe
Windows – SDC	Svakih 8 sati
Windows – SQL	Svakih 8 sati
Windows – EXCHANGE	Svakih 8 sati
Linux	Svakih 24 sata

Tablica 1: tablica prikazuje frekvenciju skeniranja zaštitnih rupa za navedene zaštitne grupe

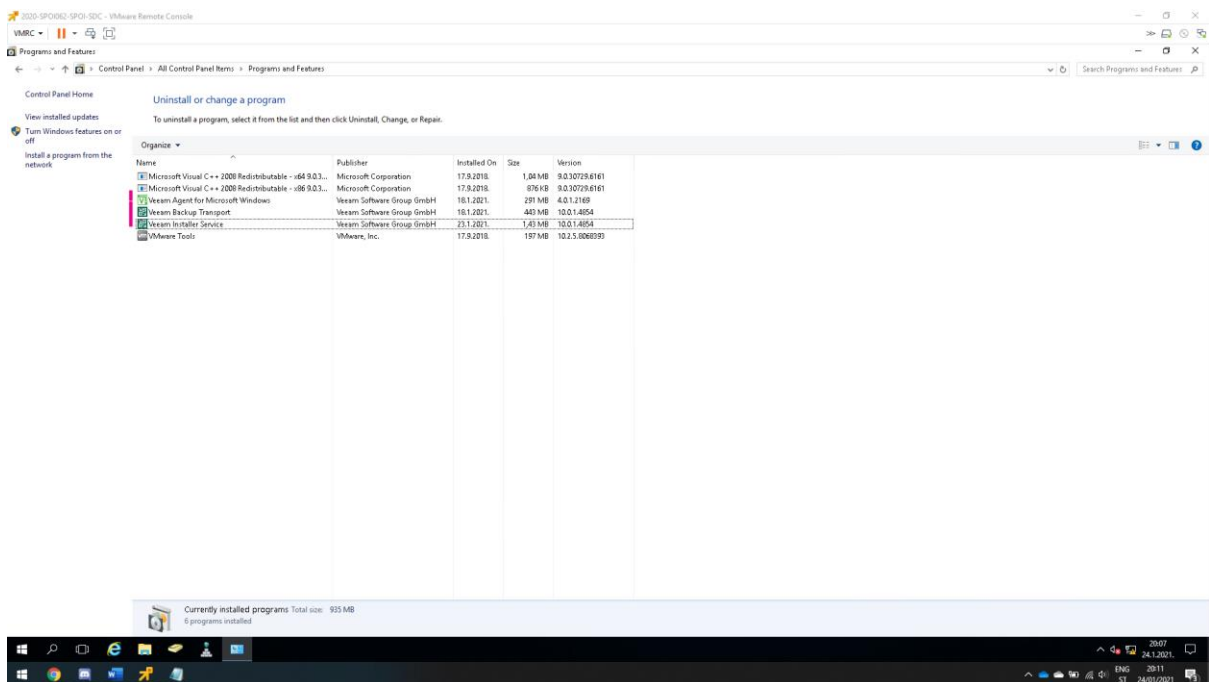
Razlog zbog kojeg su navedene opcije odabrane, a to je jer smatram da tvrtka ne može biti u svojem operativnom stanju bez Active Directory, SQL i Exchange poslužitelja. Iz tog razloga frekvencija skeniranja zaštitne grupe podešena je na svakih 8 sati. Dok je kod Linux računala svakih 12 sati jer tvrtka može biti u operativnom stanju i bez njih.

Bitna stavka koju je potrebno naglasiti, a to je prije nego se Linux poslužitelji dodaju u Veeam infrastrukturu potrebno je pokrenuti sljedeće naredbe na oba poslužitelja:

```
Yum clean all
Yum install kernel-devel dkms -y
Yum update -y
Reboot
```



Slika 16: prikaz dodanih poslužitelja u "Protection Group"



Slika 17: prikaz instaliranih komponenti na SERVERDC.backup.local poslužitelj (instalirane na svako dodano računalo)

Vrijeme koje je potrebno za uspješno dodavanje poslužitelja u infrastrukturu je od 2 - 5 minuta ovisno o kojoj kompleksnosti instaliranih servisa je riječ. Ovime završava dio dodavanja poslužitelja u Veeam infrastrukturu.

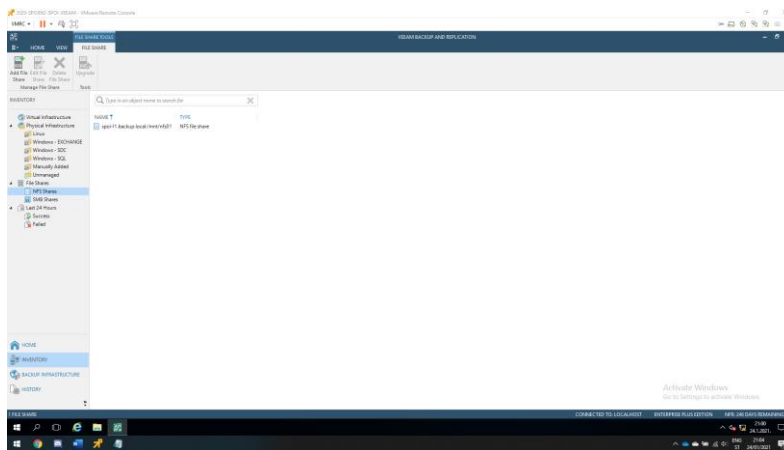
6.6. Dodavanje mrežnih datotečnih sustava u Veeam infrastrukturu

I poglavlja „Linux datotečni poslužitelj“ konfigurirano je mrežno dijeljenje datotečnih sustava protokola NFS i SMB. Prema zahtjevima tvrtke nad ovim datotečni sustavima moraju biti izrađene sigurnosne kopije. Kako bi bilo moguće izrađivati sigurnosne kopije datotečnih sustava, nužno ih je dodati u Veeam infrastrukturu.

Koraci koje je potrebno izvršiti da bi datotečni sustavi bili dodani u Veeam infrastrukturu su sljedeći: pošto su opisani koraci dodavanja poslužitelja u infrastrukturu u istoj toj kartici desnim klikom miša pritisnuti na „File Shares“ i odabrati „Add file share“. Otvara se „Wizard“ u kojem je prvo potrebno odabrati o kojem tipu datotečnog sustava se radi. Za dodavanje NFS datotečnog sustava odabrati opciju „NFS share“, dok je za dodavanje SMB datotečnog sustava potrebno odabrati opciju „SMB share“.

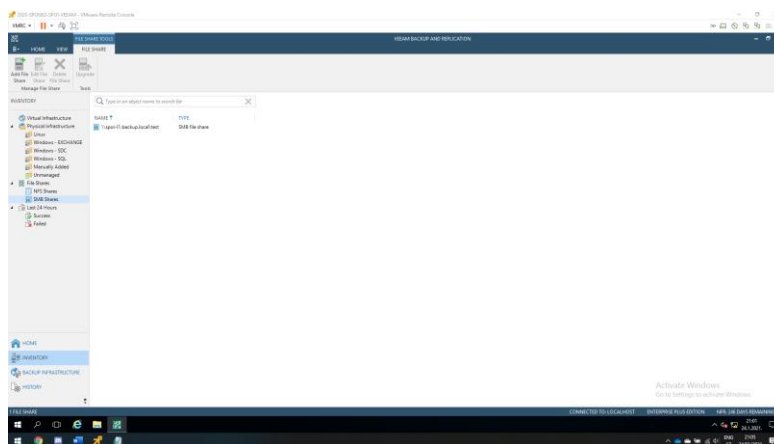
Daljnji koraci bit će posebno opisani za oba datotečna poslužitelja:

- a) Dodavanje NFS datotečnog poslužitelja: otvara se prozor u koji je potrebno upisati putanju NFS dijeljenog foldera, u ovom slučaju to je `spoi-l1.backup.local:/mnt/nfs01`. Ostale postavke ostaviti zadano.



Slika 18: prikaz dodanog NFS datotečnog sustava u Veeam infrastrukturu

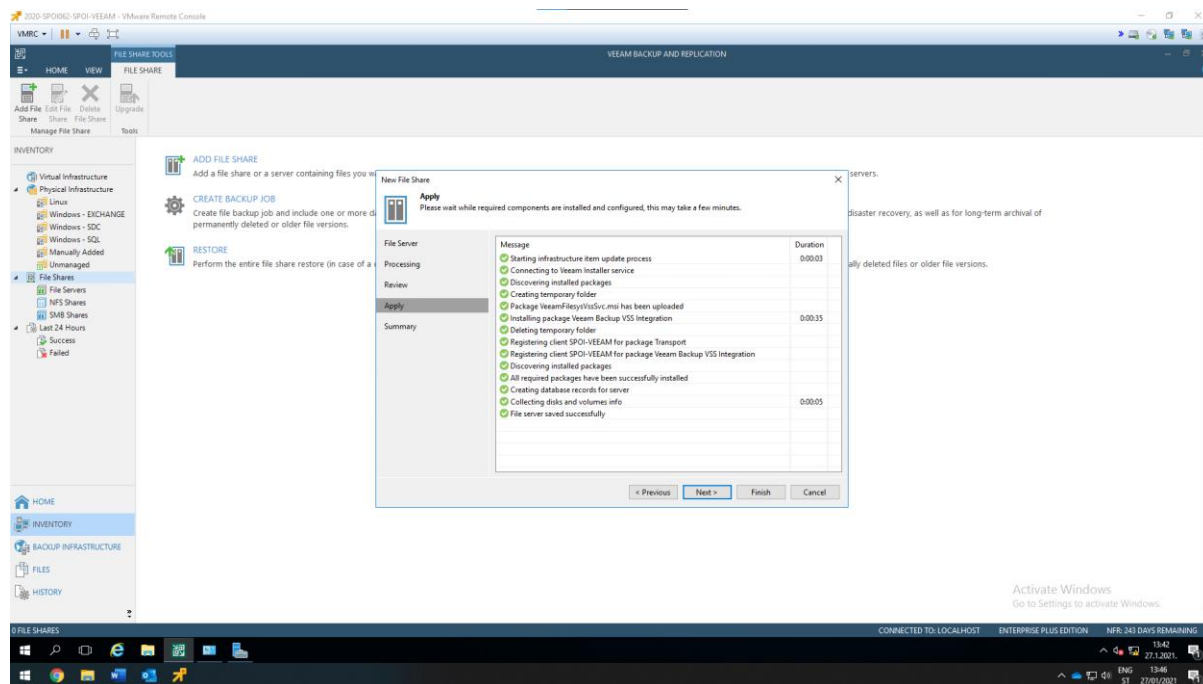
- b) Dodavanje SMB datotečnog sustava: otvara se prozor u koji je potrebno upisati putanju SMB dijeljenog foldera, u ovom slučaju to je `\\spoi-l1.backup.local\test`. Kao i korisničke podatke za pristup dijeljenom folderu. Ostale postavke ostaviti zadano.



Slika 19: prikaz dodanog SMB datotečnog sustava u Veeam infrastrukturu

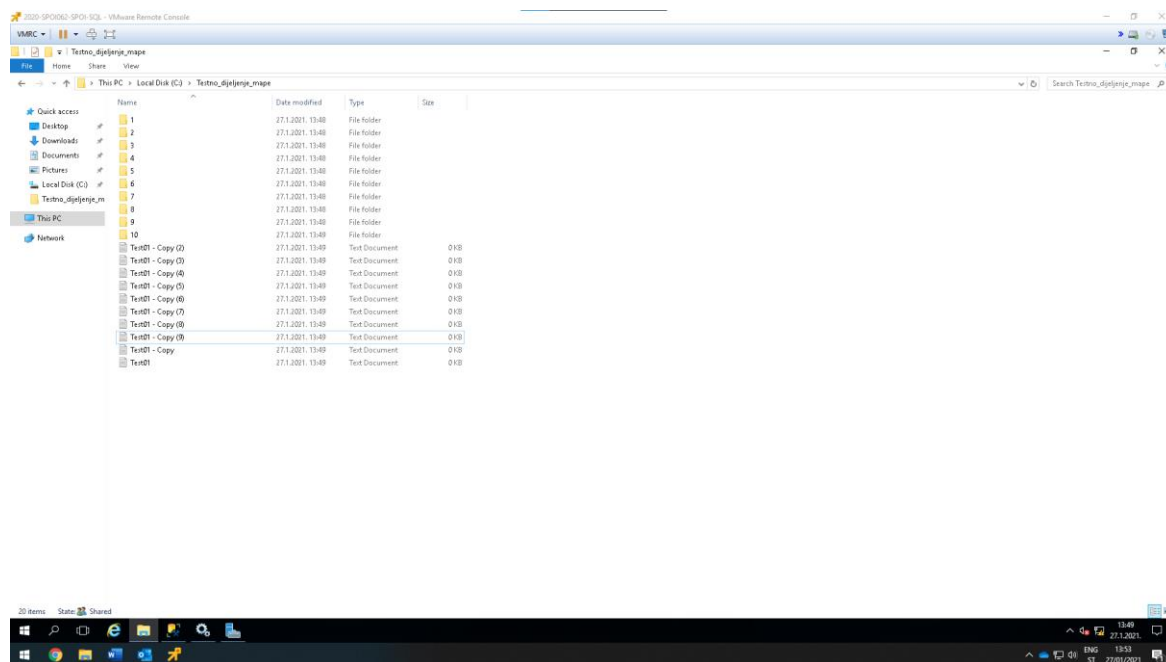
6.7. Dodavanje File Server-a na SQL poslužitelju

File Server se dodaje istim postupkom kao i dodavanje mrežnih datotečnih sustava SMB i NFS u Veeam infrastrukturu. Kod dodavanja File Server-a potrebno je paziti da se odabere opcije „File Server“. Zatim dalje slijediti čarobnjak za dodavanje File Server-a u Veeam infrastrukturu. Dodavanjem File Server-a u Veeam infrastrukturu na SPOI-SQL.backup.local računala instalira se paket „Veeam Backup VSS Integration“.



Slika 20: "File Share" dodan je u Veeam infrastrukturu

Kada je „File Share“ dodan u Veeam infrastrukturu nužno je u dijeljenoj mapi kreirati 10 mapa i 10 datoteka.



Slika 21: prikaz kreiranih mapa i datoteka u dijeljenom folderu

6.8. Kreiranje zadataka za izradu sigurnosnih kopija

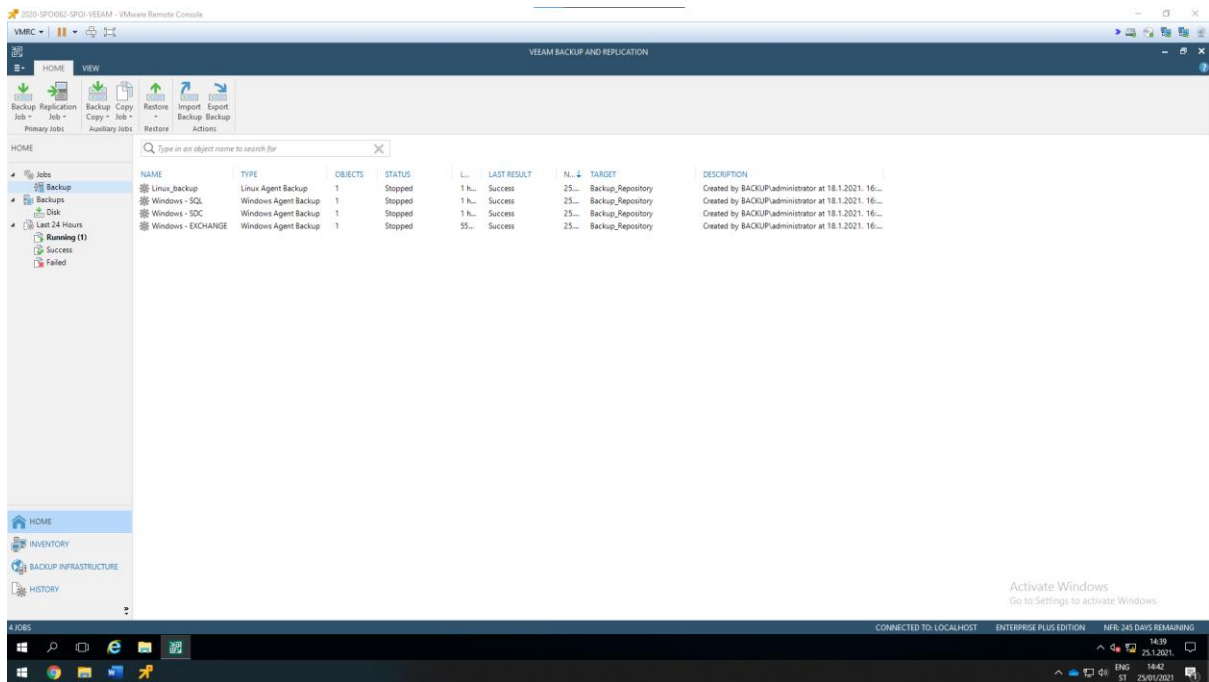
Zadatak sigurnosne kopije procesuirao „Veeam Agent“ izvodi se na poslužitelju za izradu sigurnosnih kopija na sličan način kao i uobičajeni posao za sigurnosnu kopiju podataka. Zadaća se može dodati na jednu ili više zaštitnih grupa ili pojedinačnih računala i uputiti Veeam backup software-u da kreira sigurnosne kopije „Veeam Agent“ u „Backup Repository“. „Veeam Agent“ koji je pokrenut na poslužitelju djeluje pod nadzorom Veeam backup software-a i izvodi samo sigurnosne kopije podataka, poput stvaranja snimke volumena, čitanja sigurnosno kopiranih podataka, prijenosa sigurno kopiranih podataka na ciljano mjesto.

Da bi se konfigurirao zadatak sigurnosne kopije, potrebno je pokrenuti „Wizard“ za posao izrade sigurnosne kopije novog agenta i odabrati opciju „Manage by backup server“ u koraku „Job mode“. Za sigurnosne kopije ove vrste, Veeam backup software nudi postavke slične postavkama VM zadataka sigurnosne kopije, kao i postavljen specifične za Veeam agente.

U Veeam backup software-u, u doljnjem lijevom kutu odabrati „Home“ i iz lijevog izbornika desnim klikom odabrati na „Jobs“, „Backup“ -> „Windows Computer“. „Backup“ opcija sadržava par opcija koja se sastoji od „Virtual machine“, „Windows Computer“, „Linux Computer“ i „File Share“ ovisno o tipu odabrati opciju koja odgovara navedenom uređaju.

Otvora se „Wizard“ imena „New Agent Backup Job“, u prvom dijelu imena prozora „Job Mode“ ostaviti postavke na zadano. Klikom na „Next“ otvara se prozor imena „Name“, u toj kartici dodati ime zadatku proizvoljno, ali prepoznatljivo tako da odgovara infrastrukturi. Klikom na „Next“, odabrati zaštitnu grupu nad kojom će zadatak izrade sigurnosne kopije biti pokrenut. Klikom na „Next“, odabrati opciju „Entire computer“ i pritisnuti „Next“. Otvora se kartica „Storage“ u dijelu „Retention policy“ odabrana je politika zadržavanja do 8 dana zadržavanja točki vraćanja. Klikom na „Advanced“ dolazi se do bitnog dijela koji je opisan u proceduri za izradu sigurnosne pohrane. Klikom na „Advanced“ otvara se prozor imena „Advanced Settings“. U prozoru „Advanced Settings“ pod karticom „Backup“ odabrati opciju „Create synthetic full backups periodically“ svaku nedjelju. Pod karticom „Maintenance“ odabrati opciju „Perform backup files health check“ značajka koja omogućava da se kod vremena izrade sigurnosnih kopija i vremena procedure oporavka ne radi korupcija podataka, značajka se pokreće svake nedjelje. Pod karticom „Storage“ odabrati Compression level „Extreme“ zbog toga što jer nam ova mogućnost nudi korištenje maksimalne kompresije izrade sigurnosnih kopija kako se štedjelo na prostoru. Kad su ove postavke primijenjene nužno je pritisnuti OK i „Next“. Otvora se kartica „Guest Processing“ gdje je nužno omogućiti obje značajke „Enable application-aware processing“ i „Enable guest file system indexing“. Klikom na „Next“ dolazi se do kartice „Schedule“ koji je ključan kreiranje rasporeda izrade sigurnosnih kopija van radnog vremena tvrtke.

Postupak za dodavanje zadataka izrade sigurnosne kopije može se primijeniti s navedenih postavkama na sva računala. Postavke „Schedule“ kartice nužno je prilagoditi prema načinu poslovanje tvrtke. I za SQL poslužitelj kod kartice „Guest Processing“ nužno je pritisnuti na „Applications“ zatim na „Edit“ korisničkih postavka i u kartici „SQL“ podesiti domenski administrator na spajanje na SQL server jer domenski administrator ima Sysadmin rolu. Također, omogućiti opcije „Backup logs periodically“ opcijom osigurava se da se svakih 12 minuta pohranjuju logovi.

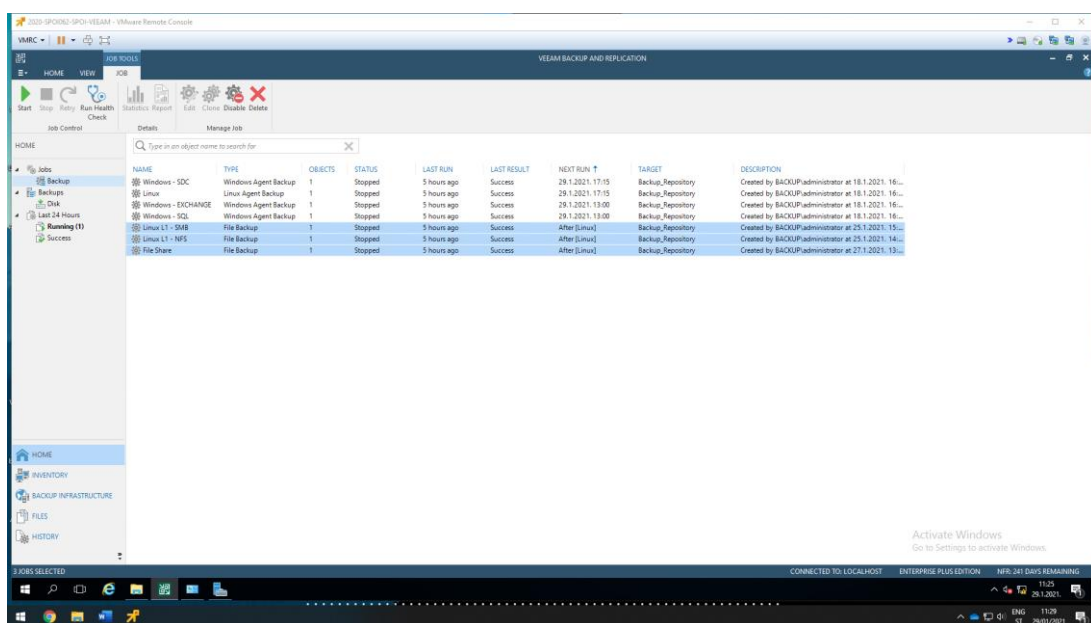


Slika 22: prikaz dodanih zadataka za izradu sigurnosnih kopija

6.8.1. Kreiranje zadataka izrade sigurnosnih kopija dijeljenih mapa

Zahjevni tvrtke su da je nužno izraditi sigurnosne kopije datotečnih sustava koji su dodani u Veeam infrastrukturu.

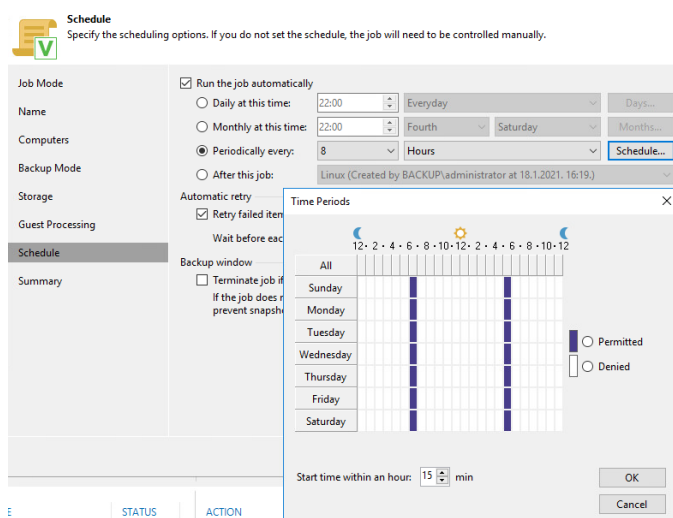
Desnim klikom na „Backup“ odabrali opciju „File Share“. Zatim se otvara „Wizard“ imena „New File Backup Job“ gdje je nužno dodati ime zadatku za izradu sigurnosnih kopija koji odgovara infrastrukturi. Klikom na „Next“ otvara se kartica „Files and Folders“ gdje je potrebno dodati dijeljeni disk. Klikom na „Next“ otvara se kartica „Storage“, postaviti postavke koje su prethodno navedena za ovu karticu. Karticu „Secondary“ ostaviti na zadanim postavkama. I zadnje na kartici „Schedule“ podesiti raspored izrade sigurnosnih kopija koji odgovara poslovanju tvrtke.



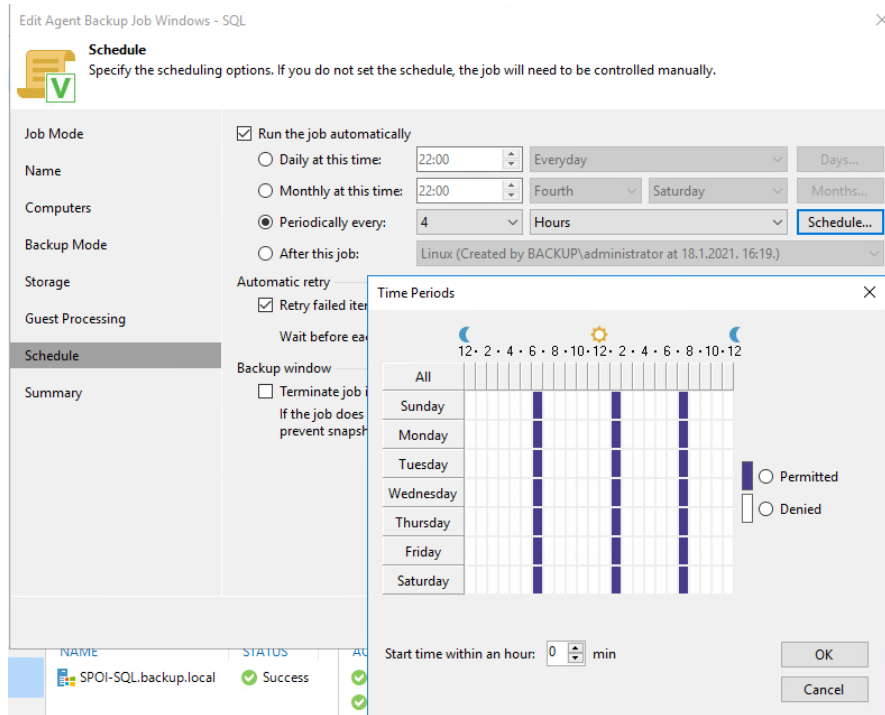
Slika 23: prikaz kreiranih zadataka izrade sigurnosnih kopija dijeljenih diskova

6.8.2. Raspored izrade sigurnosnih kopija

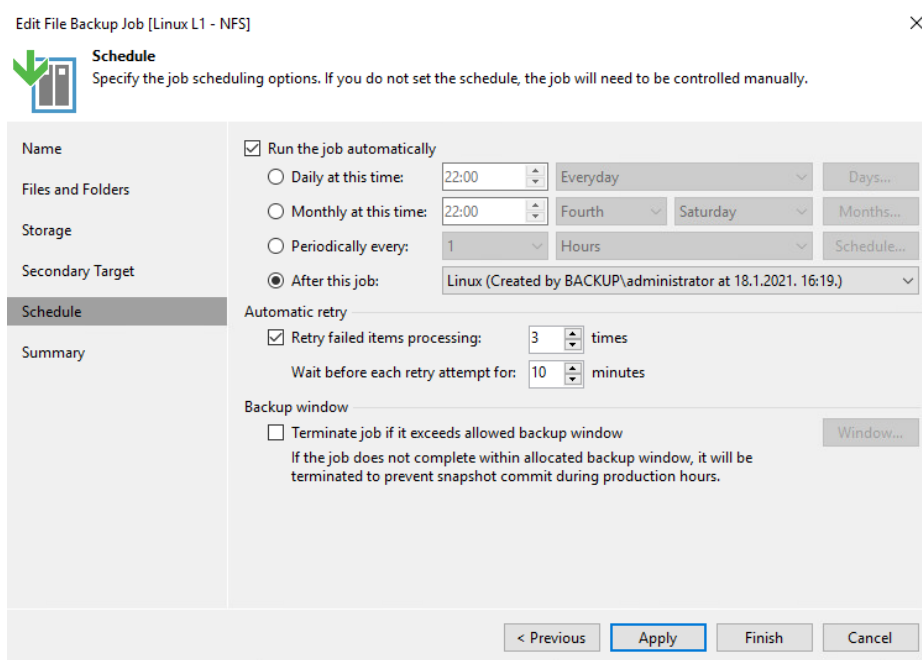
Job Name	Raspored - backup	Raspored - files health check
Windows - SDC	Svaki dan u tjednu Dva puta dnevno 6:15 - 6:59 17:15 - 17:59	Svake nedjelje
Windows - SQL	Svaki dan u tjednu Tri puta dnevno 6:00 - 6:59 13:00 - 13:59 19:00 - 19:59	Svake nedjelje
Windows - EXCHANGE	Svaki dan u tjednu Tri puta dnevno 6:00 - 6:59 13:00 - 13:59 19:00 - 19:59	Svake nedjelje
Linux	Svaki dan u tjednu Dva puta dnevno 6:15 - 6:59 17:15 - 17:59	Svake nedjelje
Linux L1 - NFS	Izvršava se poslije izvršenja sigurnosne kopije Linux poslužitelja, zato što jer se na L1 poslužitelju nalazi dijeljena mapa	Svake nedjelje
Linux L1 - SMB	Izvršava se poslije izvršenja sigurnosne kopije Linux poslužitelja, zato što jer se na L1 poslužitelju nalazi dijeljena mapa	Svake nedjelje
File Share	Izvršava se poslije izvršenja sigurnosne kopije Linux server-a	Svake nedjelje



Slika 24: raspored izrade sigurnosne kopije za SDC i Linux zaštitne grupe



Slika 25: raspored izrade sigurnosne kopije za SQL i EXCHANGE sigurnosnu grupu



Slika 26: raspored izrade sigurnosne kopije za NFS i SMB datotečne sustave

6.9. Mjerenje vremena izrade sigurnosne kopije

Prilikom izrade strategije sigurnosne kopije na pojedinim poslužiteljima isprobano je mjerenje izrade sigurnosne kopije s pohranom cijelog računala i pohranom specifične samo za pojedine usluge. Odnosno kad je uključena opcija „application-aware processing“ i kad je ta opcija isključena. Zaključno mjerenjima u tablici nešto duže je trajala izrada sigurnosne kopije s isključenom opcijom.

Job Name	Application-aware uključen	Application-aware isključen
Windows - SDC	4:52	8:16
Windows - SQL	5:07	6:36
Windows - EXCHANGE	5:17	7:26
Linux	5:18	5:53

6.10. Procedura za oporavak iz sigurnosne pohrane

Za izradu procedure za oporavak iz sigurnosne pohrane na ispravan način potrebno je imati jasnu strategiju koji poslužitelj u infrastrukturi je prioritet. Zatim sljedeće što je potrebno da bi se razvila kvalitetna procedura za oporavak iz sigurnosne pohrane je scenarij koji se može dogoditi, zbog kojeg je potrebno napraviti oporavak iz sigurnosne kopije.

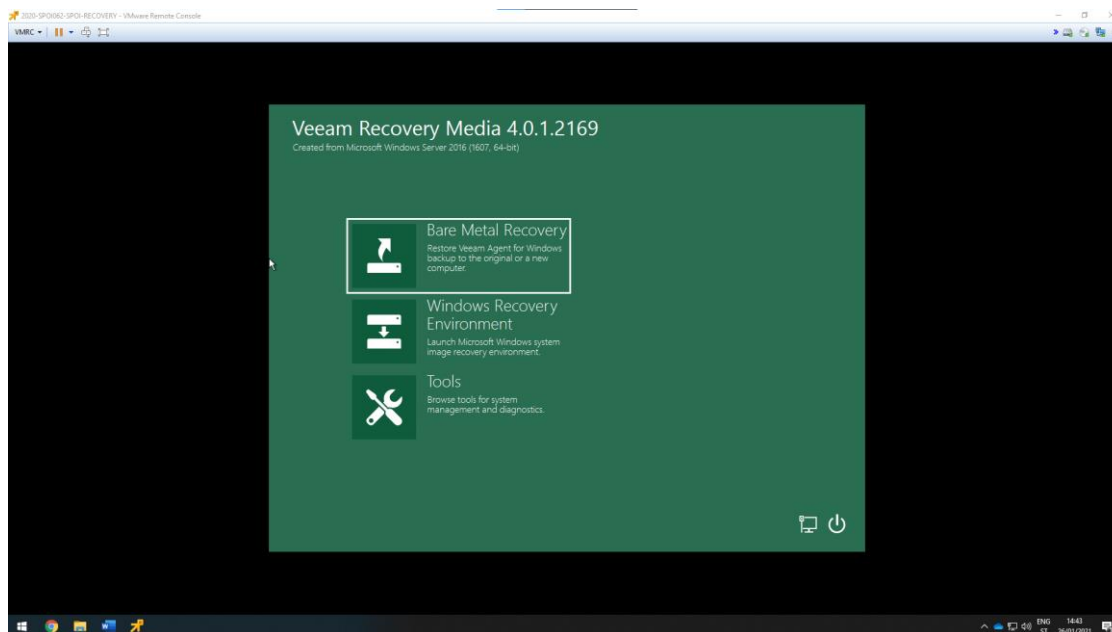
Prioriteti

U slučaju potrebe za oporavkom iz sigurnosne pohrane, nužno je osigurati sigurnosnu pohranu koja je ispravna i aktualna. Kako bi se rezultiralo osiguranje ispravne i aktualne sigurnosne pohrane treba konfigurirati dobar raspored sigurnosnih pohrana uz izradu zdravstvene provjere (eng. Health Check) pohrana na tjednoj bazi. Zdravstvene provjere uvelike su važne jer provjeravaju točke vraćanja i time se osigurava da će daljnje vraćanje biti moguće.

Bitno je naglasiti da Veeam backup software omogućava Bare-metal Recovery. Bare-metal Recovery je postupak izrade sigurnosne kopije podataka cijelog sustava, a to nisu samo korisnički podaci i postavke, već cijeli sustav koji uključuje upravljačke programe, servise, strukturu informacije, pa čak i sam operacijski sustav. Bare-metal Recovery omogućava oporavak računala na drugu mašinu u slučaju da je prva oštećena. Uz korištenje ove mogućnosti kompletan oporavak operacijskog sustava je moguć tako da drugo (prazno računalo) preuzme zadaću prvog računala koji je oštećen.

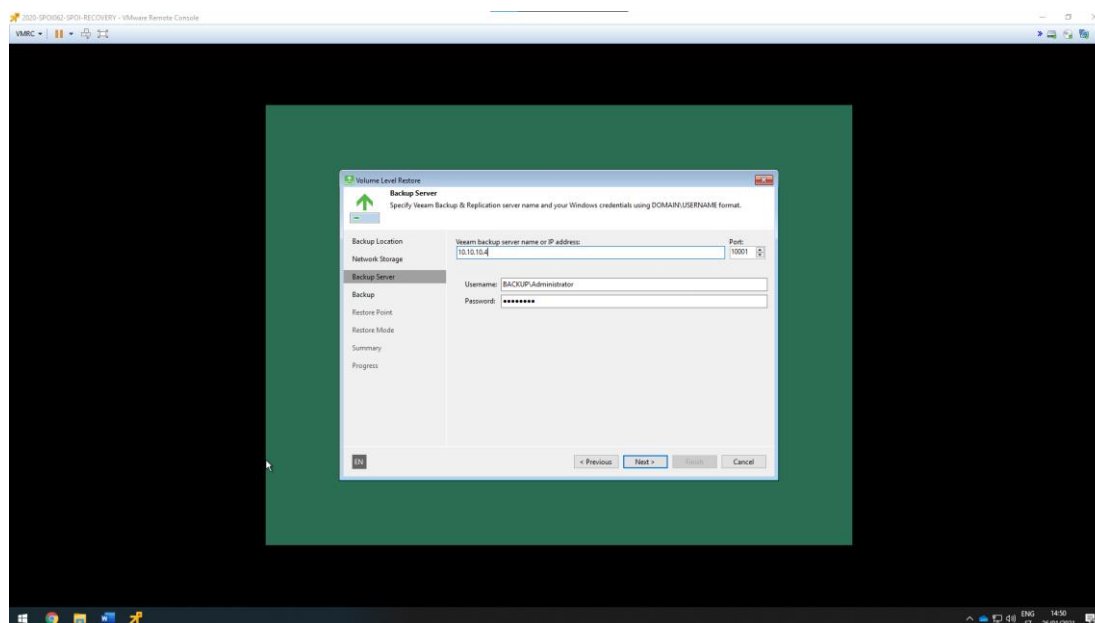
6.10.1. Oporavak domenskog kontrolera

Kako bi simulirali ne funkcionalan domenski kontroler nužno ga je ugasiti. Kad je ugašen domenski poslužitelj potrebno je upaliti RECOVERY prazno računalo koje na sebi pokreće image VEEAM RE(Veeam Recovery Media).



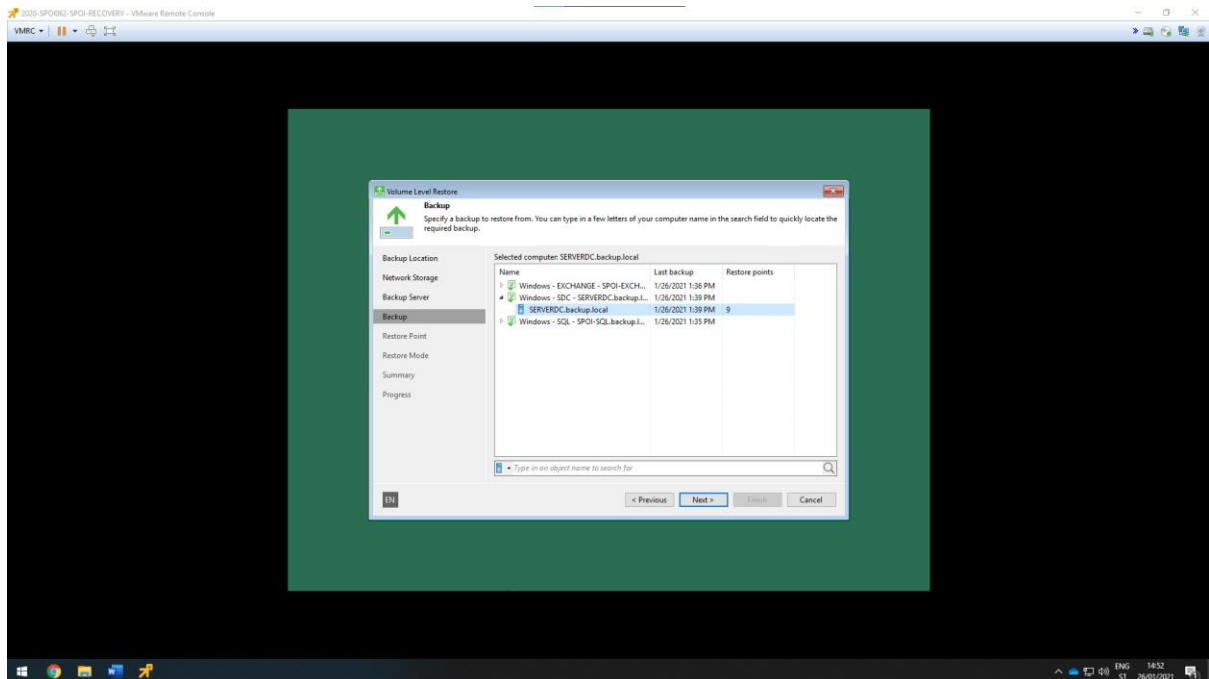
Slika 27: Veeam Recovery Media

Prvo je potrebno konfigurirati mrežni adapter na IP adresu koju je imao domenski poslužitelj 10.10.10.1/24 i gateway IP adrese Veeam backup software-a 10.10.10.4/24 kako bi se moglo pristupiti Veeam management konzoli. Odabrati „Bare Metal Recovery“ -> „Network Storage“ -> „Veeam backup repository“. Kad je IP adresa unesena i dodan odgovarajući korisnički račun može se krenuti dalje s procedurom.



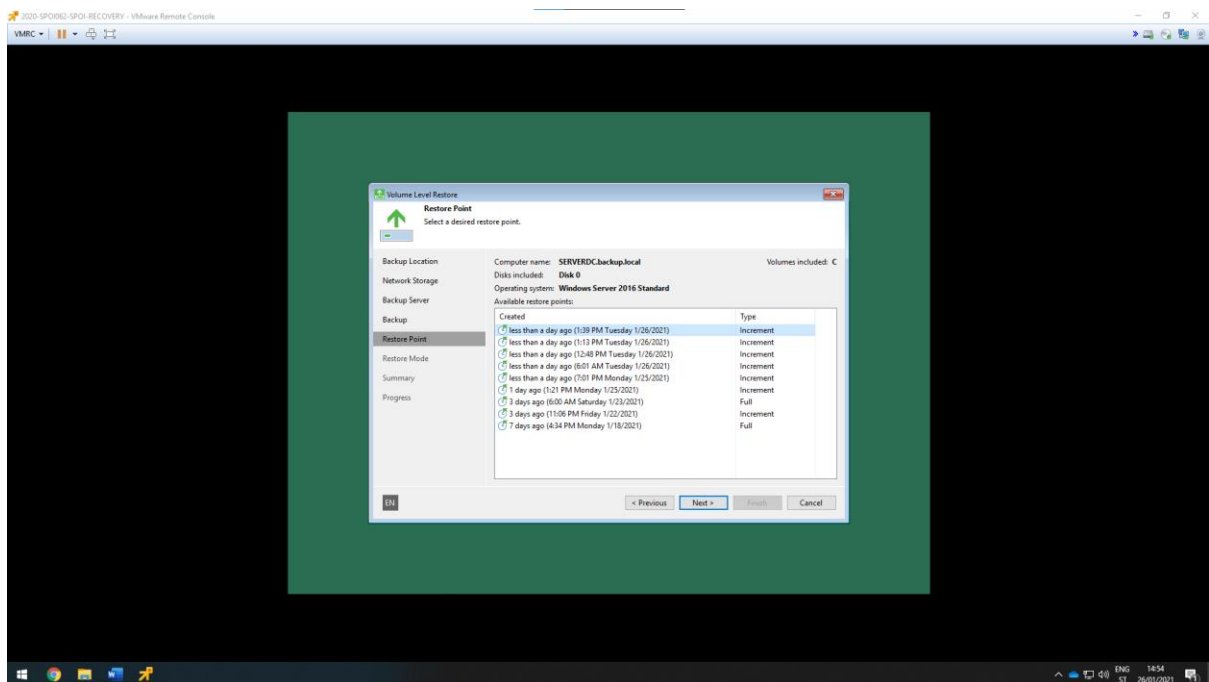
Slika 28: autorizacija na Veeam poslužitelj

Zatim odabрати Windows - SDC zadatak izrade sigurnosne kopije kao i SERVERDC.backup.local.



Slika 29: odabir sigurnosne kopije za oporavak

Nakon toga otvara se kartica s točkama vraćanja gdje je potrebno odabrati zadnju funkcionalnu sigurnosnu kopiju inkrementa.

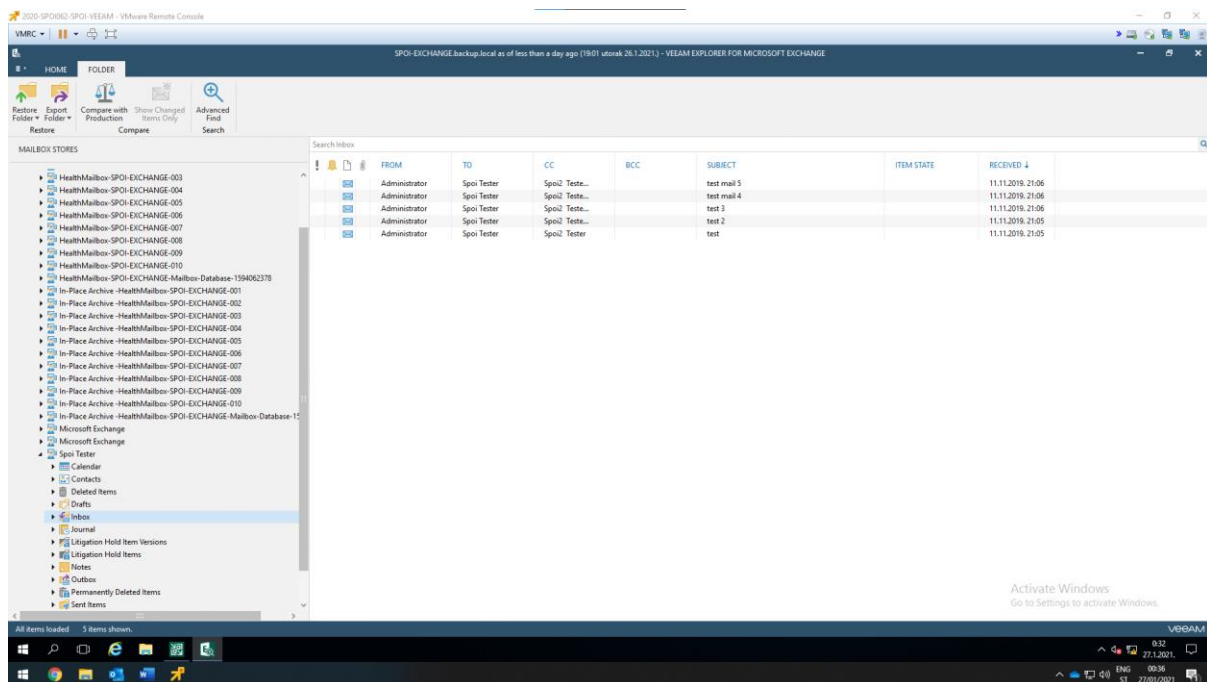


Slika 30: odabir točke vraćanja

6.10.2. Oporavak Exchange poslužitelja na razini aplikacije

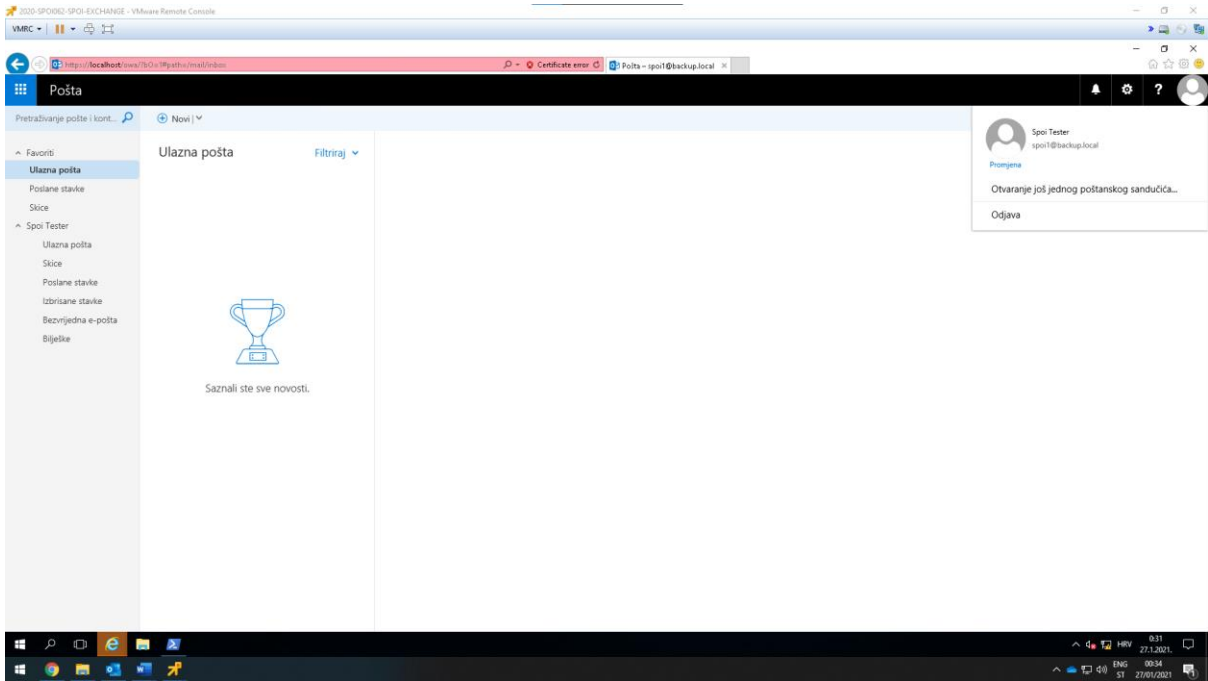
Veeam backup software uz oporavak cijelih sustava daje mogućnost oporavka određenih datoteka, sadržaja na volumenu diska, kao i oporavka na razini aplikacije. Veeam oporavak na razini aplikacije bilježi stanje podataka aplikacije u vrijeme izrade sigurnosne kopije, uključujući podatke u memoriji, što olakšava vraćanje aplikacije za daljnju uporabu. Točnije kad se izrađuje sigurnosna kopija na razini aplikacije, aplikacija zaustavlja svoj rad i tada kreira „software snapshot“ svih podataka aplikacije. Kad je kreiran „software snapshot“ aplikacija nastavlja svoj rad. Druga mogućnost koju Veeam software backup nudi je „Gust file system indexing“. Ova funkcija omogućava oporavak pojedinačnog maila u Exchange-u.

Oporavak na razini aplikacije radi se tako da se u Veeam sučelju potrebno pozicionirati u „Home“, zatim pritisnuti „Backup“, pojavljuje se alatna traka iz koje je nužno pritisnuti na „Restore“ i odabrati „Agent“. Otvara se „Wizard“ u kojem je nužno odabrati „Application item restore“, kad je odabrana navedena opcija potrebno je odabrati opciju za oporavak Exchange poslužitelja „Microsoft Exchange“. Odabrati poslužitelj koji ima instaliranu ulogu MS Exchange i pritisnuti na „Next“. Otvara se kartica imena „Restore Point“ te je potrebno odabrati najnovije kreiranu točku vraćanja i završiti sa „Wizard“ prozorom. Završetkom čarobnjaka otvara se „Veeam Explorer for Microsoft Exchange“ sučelje koje nudi mnogo mogućnosti za oporavak i do najsitnijih detalja.



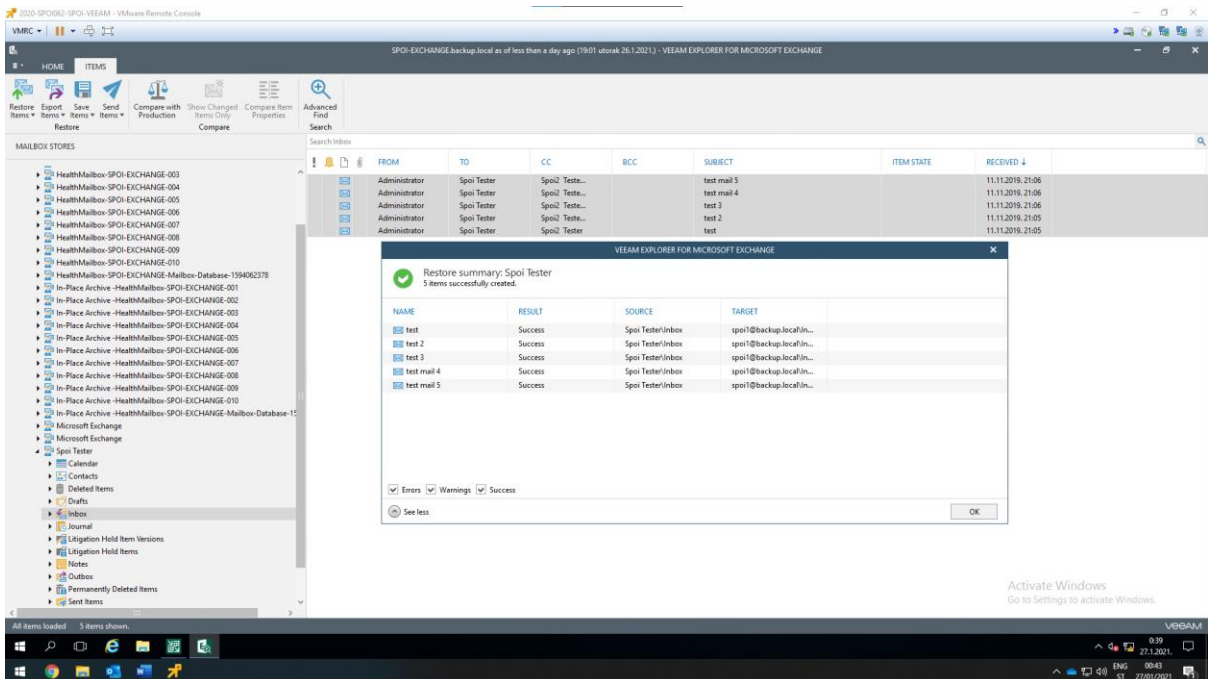
Slika 33: prikaz sučelja Veeam Explorer-a

Za demonstracije ove mogućnosti potrebno se je prijaviti u „Outlook“ s korisničkim računom korisnika spoi1@backup.local i izbrisati sve poruke koje ima u sandučiću. Kad su poruke izbrisane one će biti oporavljene na razini aplikacije koristeći Veeam backup software.



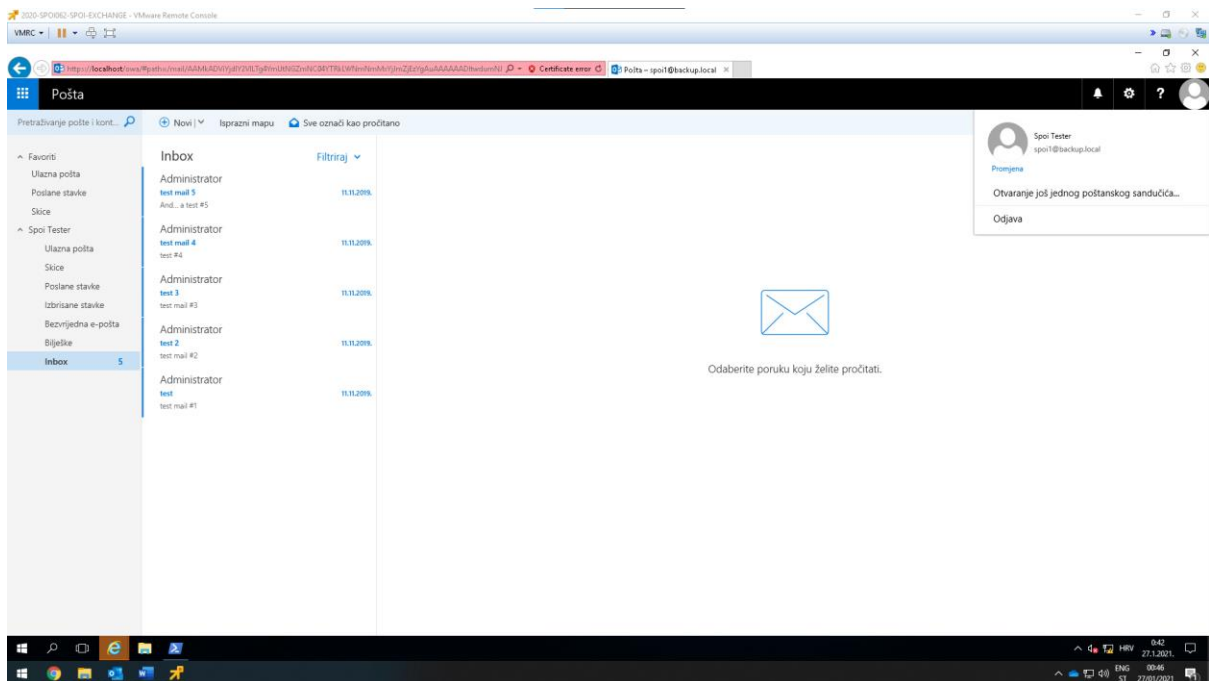
Slika 34: prikaz obrisanih mailova korisniku spo1@backup.local

U Veeam Explorer konzoli odabrati mailbox bazu i unutar baze mailova odabrati željenog korisnika nad kojim se želi napraviti oporavak na razini aplikacije u ovom slučaju korisniku spo1@backup.local izbrisan je sandučić sa svim mailovima te će se nad ovim korisnikom izvršiti oporavak mailova. Nužno je odabrati sve mailove koje je korisnik spo1@backup.local imao u svojoj bazi mailova i desnim klikom miša otvara se izbornik iz kojeg je potrebno odabrati opciju „Restore to spo1@backup.local“. Iz otvorenog izbornika nudi se mogućnost i oporavka na proizvoljno mjesto na koje je moguće oporaviti mailove.



Slika 35: prikaz uspješno oporavljenih mailova spo1@backup.local korisnika

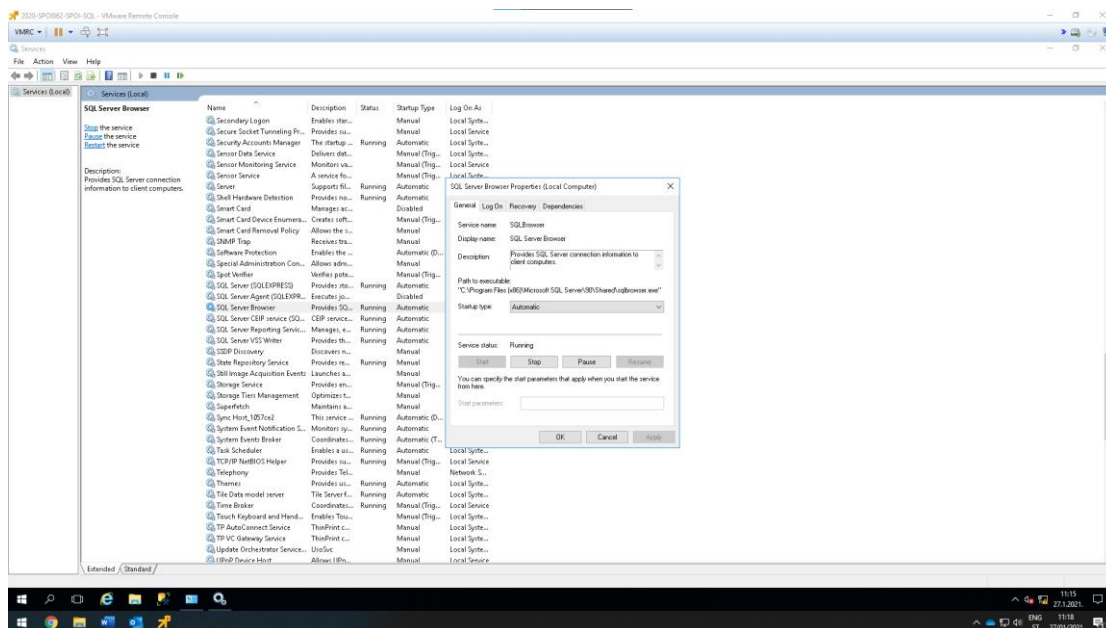
Kad su mailovi oporavljeni nužno je testirati kako ti izgleda sa strane korisnika. Korisnik bi morao moći vidjeti kad se prijavi u „Outlook“ svoje mailove koji su prethodno bili obrisani.



Slika 36: oporavljeni mailovi vidljivi su sa strane korisnika u aplikaciji „Outlook“

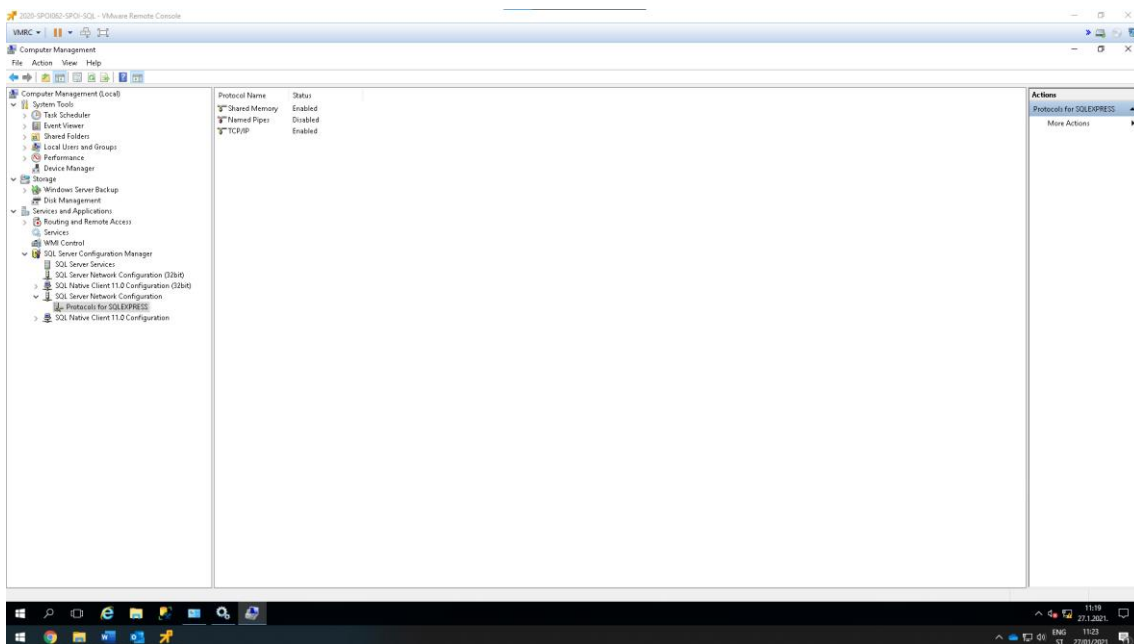
6.10.3. Oporavak SQL poslužitelja na razini aplikacije

Kako bi se demonstrirao oporavak SQL poslužitelja potrebno je upaliti servis „SQL Server Browser“ među servisima koji rade na SQL poslužitelju.



Slika 37: Pokrenuti servis "SQL Server Browser"

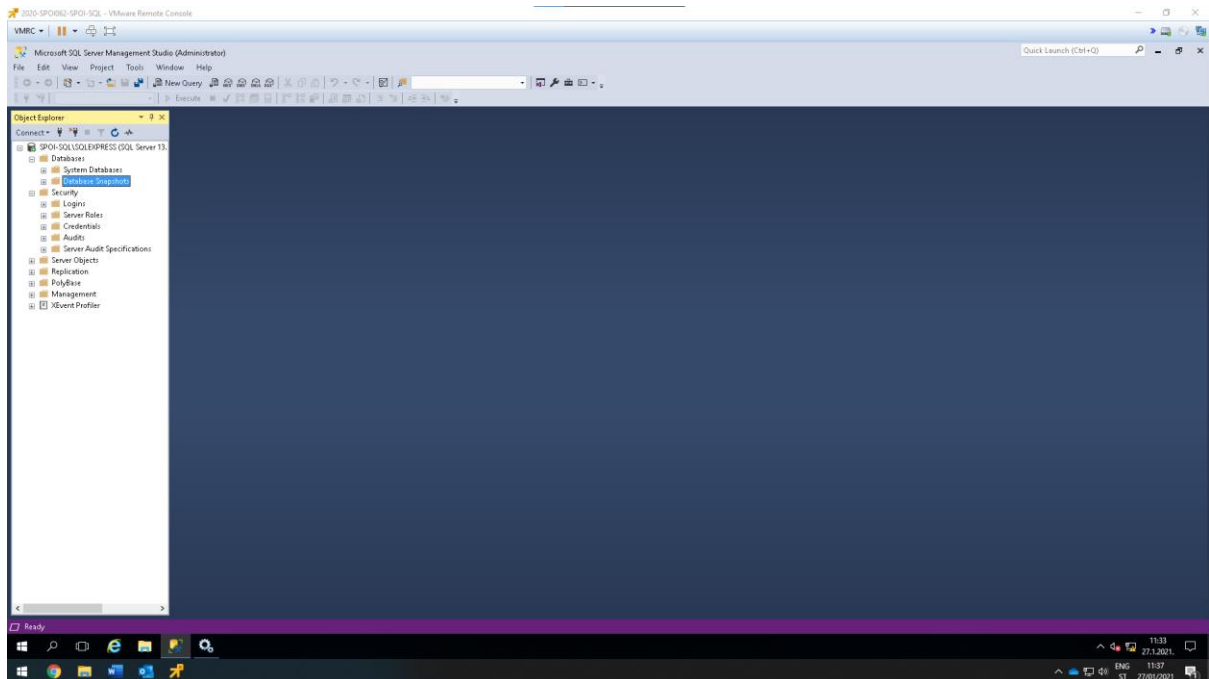
Također potrebno je u „SQL Server Configuration“ manager-u omogućiti TCP/IP protokol za SQLEXPRESS bazu podataka. Omogućenjem ove značajke može se putem mreže pomoću Administrativnog korisničkog računa pristupiti bazi podataka iz „Veeam Explorer“ manager-a i tako oporaviti dio ili cijelu bazu podataka.



Slika 38: TCP/IP protokol za SQLEXPRESS bazu podataka

Kako bi promjena bila omogućena na nužno je napraviti restart SQLEXPRESS baze i oporavak sigurnosne kopije sličan je onome kao i za Exchange.

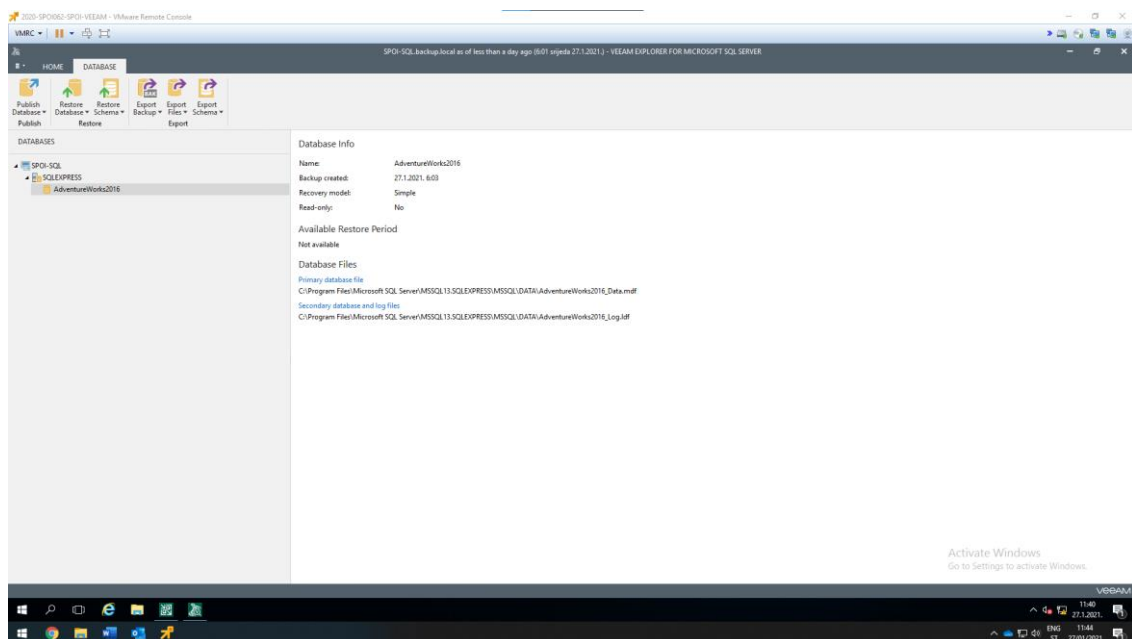
Za potrebe ove demonstracije obrisat ću bazu podataka „AdventureWorks2016“ i napraviti oporavak cijele baze podataka.



Slika 39: prikaz izbrisane baze "AdventureWorks2016"

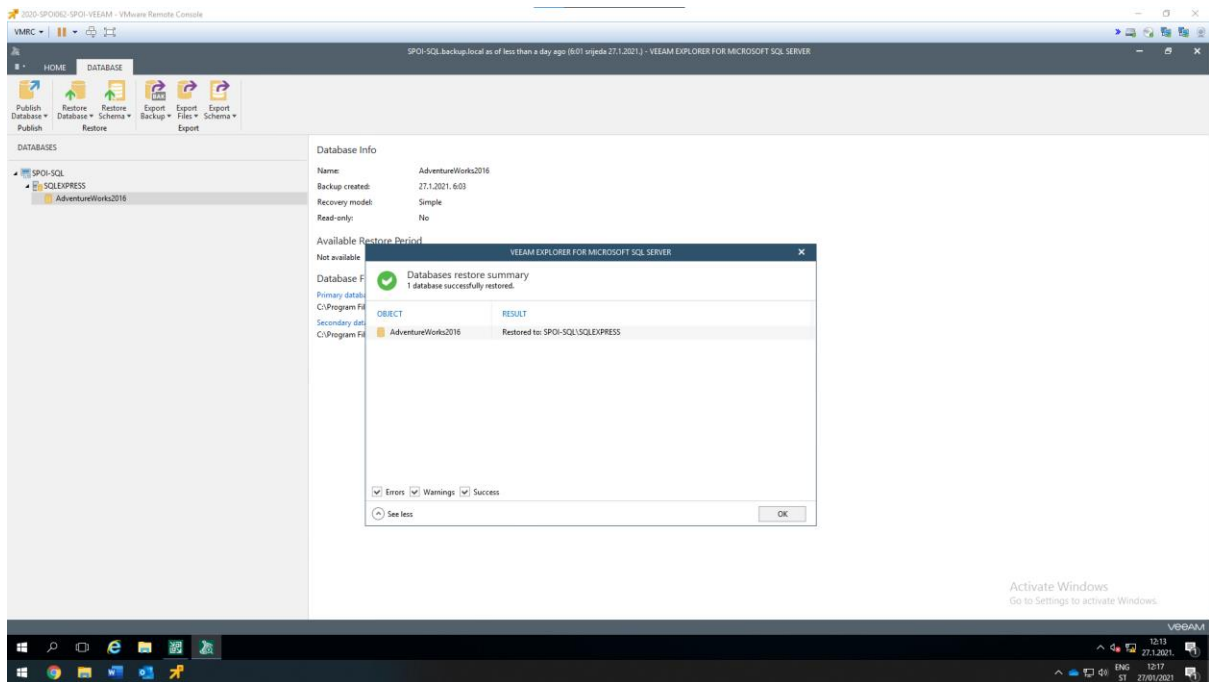
Oporavak sigurnosne kopije baze podataka nakon što se izbriše baza podataka „AdventureWorks2016“ na njeno mjesto stavlja onu verziju baze podataka iz inkrementalne točke vraćanja. Premda je kod konfiguracije zadatka sigurnosne kopije uključena mogućnost „Application-Aware processing“, „Guest file system indexing“ i pohranjivanje transakcijskih logova nudi se mogućnost „Restore Schema“ gdje se može oporaviti bilo koja promjena zapisana u bazu podataka.

Home -> Backup -> Restore -> Agent -> Application items restore -> Microsoft SQL Server -> odabrati SQL poslužitelja -> odabir točke vraćanja -> otvaranje „Veeam Explorer for Microsoft SQL Server“.

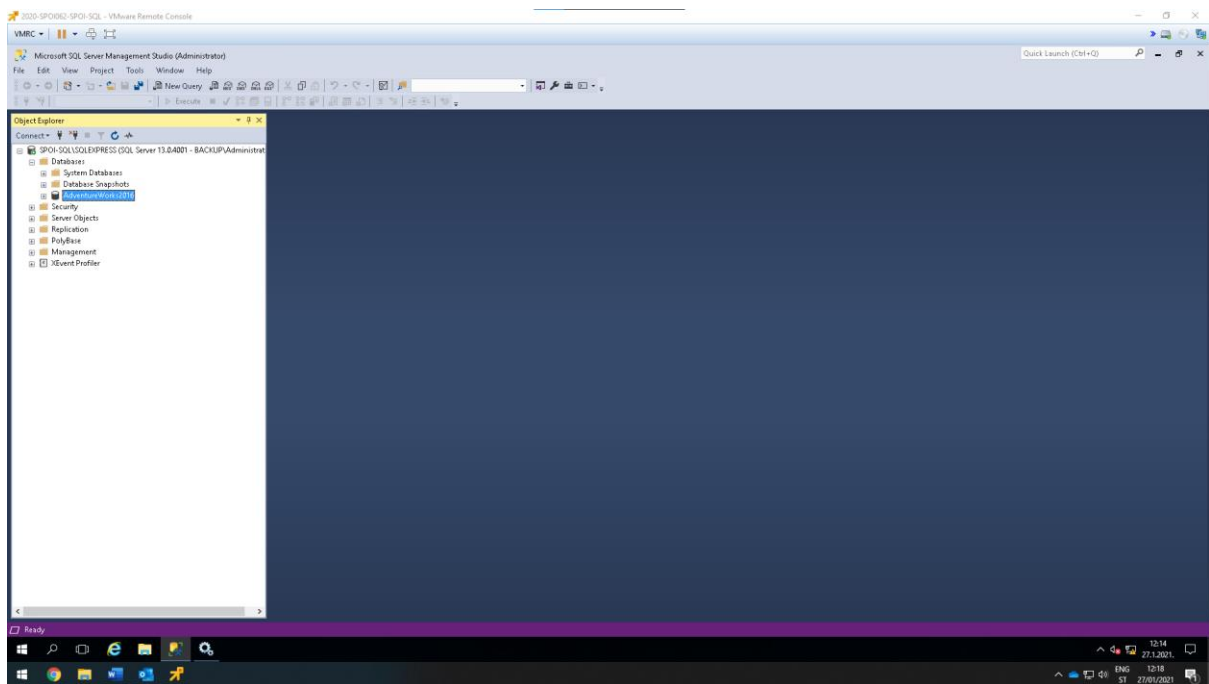


Slika 40: Veeam Explorer for Microsoft SQL Server

Kako bi se oporavak baze podataka izvršio potrebno je denim klikom pritisnuti na „AdventureWorks2016“ i izbornika odabrati „Restore database“ -> „Restore latest state to SPOI\SQLSERVER“.



Slika 41: oporavak baze podataka "AdventureWorks2016"



Slika 42: prikaz oporavka baze podataka koji je vidljiv u SQL poslužitelju

7. Popis slika

Slika 1: prikaz opisa infrastrukture kroz umnu mapu	3
Slika 2: prikaz topologije infrastrukture	4
Slika 3: konfiguracija mrežnog adaptera.....	5
Slika 4: spajanje na storage sustav koristeći iSCSI protokol.....	6
Slika 5: formatiranje diska file system-a ReFS	7
Slika 6: Kreiranje novog Backup repozitorija	8
Slika 7: prikaz NFS konfiguracije na Linux L1 poslužitelj	10
Slika 8: NFS mrežni datotečni sustav radi	10
Slika 9: prikaz SMB konfiguracije na Linux L1 poslužitelju	11
Slika 10: SMB datotečni sustav radi	12
Slika 11: Postavke izrade sigurnosne kopija.....	14
Slika 12: oporavka sigurnosne kopije konfiguracije na početno stanje	15
Slika 13: oporavak sigurnosne kopije konfiguracije na trenutno stanje.....	15
Slika 14: dodavanje korisničkih podataka	16
Slika 15: prikaz dodanih računala u Managed Servers	18
Slika 16: prikaz dodanih poslužitelja u "Protection Group"	20
Slika 17: prikaz instaliranih komponenti na SERVERDC.backup.local poslužitelj(instalirane na svako dodano računalo).....	20
Slika 18: prikaz dodanog NFS datotečnog sustava u Veeam infrastrukturu	21
Slika 19: prikaz dodanog SMB datotečnog sustava u Veeam infrastrukturu.....	21
Slika 20: "File Share" dodan je u Veeam infrastrukturu	22
Slika 21: prikaz kreiranih mapa i datoteka u dijeljenom folderu	22
Slika 22: prikaz dodanih zadataka za izradu sigurnosnih kopija	24
Slika 23: prikaz kreiranih zadataka izrade sigurnosnih kopija dijeljenih diskova.....	24
Slika 24: raspored izrade sigurnosne kopije za SDC i Linux zaštitne grupe.....	25
Slika 25: raspored izrade sigurnosne kopije za SQL i EXCHANGE sigurnosnu grupu	26
Slika 26: raspored izrade sigurnosne kopije za NFS i SMB datotečne sustave	26
Slika 27: Veeam Recovery Media.....	29
Slika 28: autorizacija na Veeam poslužitelj.....	29
Slika 29: odabir sigurnosne kopije za oporavak.....	30
Slika 30: odabir točke vraćanja	30
Slika 31: Sažetak postavljenih postavka oporavka.....	31
Slika 32: potvrda funkcionalnog oporavka Windows - SDC računala	31
Slika 33: prikaz sučelja Veeam Explorer-a.....	32
Slika 34: prikaz obrisanih mailova korisniku spoi1@backup.local	33
Slika 35: prikaz uspješno oporavljenih mailova spoi1@backup.local korisnika	33
Slika 36: oporavljeni mailovi vidljivi su sa strane korisnika u aplikaciji „Outlook“	34
Slika 37: Pokrenuti servis "SQL Server Browser"	35
Slika 38: TCP/IP protokol za SQLEXPRESS bazu podataka.....	35
Slika 39: prikaz izbrisane baze "AdventureWorks2016"	36
Slika 40: Veeam Explorer for Microsoft SQL Server.....	36
Slika 41: oporavak baze podataka "AdventureWorks2016"	37
Slika 42: prikaz oporavka baze podataka koji je vidljiv u SQL poslužitelju.....	37

8. Zaključak

Ako je organizacija velika i složena, trošak njene uspostave ne prekinutog poslovanja može doseći velike brojke. Kada se gleda na prvi pogled, može biti jednostavnije ne činiti ništa po tom pitanju i živjeti u nadu da organizacija neće doživjeti katastrofalne događaje. Uspoređujući danas, krize i neželjeni događaji gotovo su ne izbjegli i samo je pitanje vremena kada će i koliko snažno pogoditi organizaciju. Zbog navedenog razloga potrebno je planirati poslovni kontinuitet i prilagoditi ga njegovoj veličini. Gledano iz perspektive planiranja poslovnog kontinuiteta ono se ne odnosi samo na neprekidnost poslovnih operacije već i na efikasan oporavak od poremećaja. Ovaj proces ne samo da daje uvid u poslovne procese i njihove slabe točke poslovanja, već omogućava bolje razumijevanje organizacije i njenih prijetnji kao i rizika. Iz pogleda ekonomije može se reći da kvalitetan plan kontinuiteta poslovanja čini konkurentsku prednost organizacije.

Ovim projektnim zadatkom predstavljena je aplikacija koja podupire koncept upravljanja kontinuiteta poslovanja i oporavka od katastrofalnih događaja. No s druge strane poznata je činjenica da nijedan informacijski sustav nije 100% siguran, kao i procesi, aplikacije unutar organizacijske strukture. Zbog toga važno je implementirati softverska rješenja za izradu sigurnosnih kopija, replikacija i oporavka kako bi se eliminirali poremećaji u poslovanju.

8.1. Preporuke za sigurnosnu pohranu

Prema zahtjevima infrastrukture naveden je zahtjev izrađivanje sigurnosne kopije 2 puta za sva računala osim SQL i Exchange poslužitelja za koje je potrebno izrađivati sigurnosnu kopiju 3 puta na dan. Zahtjevi infrastrukture Tvrtke X su zadovoljeni no izrađivanje sigurnosne kopije moglo se i drugačije provesti, no to sve ovisi o složenosti organizacije, predviđanja rizika, radnome vremenu kao i slabostima tvrtke za koju se implementira jedno od rješenja.

Raspored izrade sigurnosnih kopija za računala kojima se izrađuje sigurnosna kopija 2 puta na dan, se izrađuje prije početka radnog vremena i na kraju radnog vremena, ako smatramo da poslovanje ima svoje radno vrijeme od 8:00 - 16:00. U ovome slučaju izrada sigurnosne kopije provodi se od 6:15 - 6:59 i od 17:15 - 17:59. Raspored za ova računala još se je mogao podesiti da se izrada sigurnosne kopije izrađuje za vrijeme pauze i nakon radnog vremena, ili prije početka radnog vremena i za vrijeme pauze. Raspored izrade sigurnosnih kopije za računala kojima se izrađuje sigurnosna kopije 3 puta na dan, se izrađuje prije početka radnog vremena, za vrijeme pauze i na kraju radnog vremena. Odnosno 6:00 - 6:59, 13:00 - 13:59 i od 19:00 - 19:59. Odabran je ovaj raspored kakav je prethodno naveden zbog toga što smatram da najbolje odgovara poslovnom okruženju. Što se tiče izrade sigurnosne kopije nad datotekama ona se izrađuje 2 puta na dan, poslije Linux zadataka za izradu sigurnosne kopije. Ovaj koncept za izradu sigurnosne kopije nad datotekama odabran je iz razloga da se stvori lanac zadataka za izradu sigurnosnih kopija i pojednostavi izrada kreiranja rasporeda. Također korištenje ove opcije štede se resursi Veeam poslužitelja jer se tada ne koriste svi resursi u isto vrijeme već kad jedan završi drugi nastavlja.

8.2. Prednosti i mane cloud backup rješenja

Cloud backup rješenje uključuje slanje sigurnosnih kopija pružateljima usluge u „Cloud“ infrastrukturi. „Cloud“ pružatelji usluga čuvaju podatke sigurnosnih kopija u zamjenu za naknadu koja ovisi o kojem pružatelju usluge je riječ. Uz rješenje „Cloud“ infrastrukture pružatelji usluga osiguravaju da se osjetljive informacije sigurnosnih kopija mogu vratiti u slučaju katastrofe. Bitno je napomenuti kako „Veeam Backup & Recovery“ softver nudi ovu mogućnost svojim korisnicima u

realizaciji boljih rješenja. Mogućnost koju Veeam nudi za Cloud backup rješenja je značajka imena „Cloud Connect“. „Veeam Cloud Connect Backup“ sigurnosna pohrana šalje se putem sigurnosne konekcije do poslužitelja „Cloud“ usluge. Funkcionira tako da se sigurnosne pohrane ne vrše na jednak način kao one kod lokalne sigurnosne pohrane. Razlika koja se pojavljuje je da se nakon prve izrade cijele sigurnosne kopije, pohranjuje razlika ostalih izrada cijelih sigurnosnih kopija koja se spaja u jednu kako bi se prijenos obavio brže. Točnije kod izrade cijelih sigurnosnih kopija one se sintetiziraju u jednu. Još jedna od prednosti „Veeam Cloud Connect Backup“ je WAN akceleracija koja omogućava obavljanje deduplikacije nad datotekama koje se šalju u „Cloud“ infrastrukturu kako bi se optimalno iskoristio prostor za pohranu. Negativne strane „Veeam Cloud Connect Backup“ su da „Transaction log backup“ nije podržan za „Cloud Repository“. Kao i instantan oporavak Virtualnih mašina, „multi-os file-level restore“, oporavak na Microsoft Azure, oporavak na Amazon EC2 kao i oporavak na Nutanix AHV nije podržan. Također sigurnosna kopija NAS pohrane nije podržana.

Što se tiče generalnog osvrta na „Cloud“ backup rješenje neke od prednosti i mana su dostupnost podataka s bilo kojeg mjesta u bilo koje vrijeme. To znači da sigurnosne kopije koje su spremljene u „Cloud“ infrastrukturu čini dostupnima bilo kada, sve dok god je pristup internetskoj vezi omogućen. Sljedeća prednost koju Cloud backup nudi je učinkovitost i pouzdanost, a to bi značilo da pružatelji „Cloud“ usluga brinu za nadogradnje softvera, nadogradnje hardvera kao i troškovima održavanja u koje spadaju hlađenje i električna energija. Na ovaj način korisnik ne mora brinuti o ovim aspektima. Druga pak prednost je sigurnost gdje pružatelji usluga osiguravaju podatke sigurnosnih kopija sigurnim. Podatkovni centri za pohranu podataka koriste šifriranje podataka vojne namjene u svrhu poboljšane sigurnosti kao i zaštitare koji sigurnosnim kamerama nadgledaju cijeli kampus podatkovnog centra. Nedostaci sigurnosne pohrane u „Cloud“ infrastrukturi su da se podacima ne može pristupiti bez internetske veze koja mora imati odgovarajuću propusnost kako bi se podaci prenesli s jednog mjesta na drugo. Još jedan od nedostataka je problem kod potpunog oporavka koji bi mogao potrajati i trajati duže nego onaj koji je pohranjen na lokalnoj pohrani.

9. Literatura

- [1] Mohn, M. (2014) Learning Veeam Backup & Replication for VMware vSphere. 1. izd. Pakt Publishing Ltd.
- [2] Veeam Backup & Replication, User Guide for VMware vSphere, Version 10, September, 2020
- [3] Veeam Backup Enterprise Manager, User Guide, Version 10, August, 2020
- [4] Radić I. (2019.) Oporavak od katastrofe i upravljanje kontinuitetom poslovanja: usporedba softvera za izradu sigurnosnih kopija. Diplomski rad. Sveučilište u Zagrebu, Ekonomski fakultet
- [5] https://helpcenter.veeam.com/docs/backup/cloud/cloud_overview.html?ver=100
- [6] <https://www.veeam.com/>
- [7] https://www.youtube.com/watch?v=iRqAxTm9EVw&list=PLcRhKiWZmM8hxxTgixVP1OzCtwAC5s7W&ab_channel=LabsHandsOn