Josip Torbar

SIGURNOSNA POHRANA I OPORAVAK IT INFRATRUKTURE

PROJEKT

Sadržaj

[1. Sažetak 3](#_Toc61913691)

[2. Opis infrastrukture 4](#_Toc61913692)

[2.1. Priprema infrastrukture 1](#_Toc61913693)

[2.1.1. Spajanje poslužitelja SPOI-VEEAM na iSCSI Target 1](#_Toc61913694)

[2.1.2. Kreiranje i konfiguracija SMB-a i NFS-a na poslužitelju SPOI-L1 3](#_Toc61913695)

[2.1.3. Kreiranje i konfiguracija dijeljenih datoteka na poslužitelju SPOI-SQL 6](#_Toc61913696)

[2.2. Procedura za izradu sigurnosne pohrane sustava 7](#_Toc61913697)

[2.3. Procedura za oporavak 9](#_Toc61913698)

[3. Razrada projekta – projektno rješenje 11](#_Toc61913699)

[3.1. Dodavanje managed servera u Veeam infratrukturu 11](#_Toc61913700)

[3.2. Dodavanje Protection Group-a u Veeam Inventory 12](#_Toc61913701)

[3.3. Izrada backup job-ova 14](#_Toc61913702)

[3.3.1. DC\_PG\_Backup 14](#_Toc61913703)

[3.3.2. SQL\_PG\_Backup 16](#_Toc61913704)

[3.3.3. MBX\_PG\_Backup 19](#_Toc61913705)

[3.3.4. LX\_FS\_Backup 21](#_Toc61913706)

[3.3.5. LX\_KVM\_Backup 23](#_Toc61913707)

[3.4. Mjerenja backup job-ova 27](#_Toc61913708)

[4. Oporavak poslužitelja SPOI-SDC 28](#_Toc61913709)

[5. Oporavak dijelova sustava 33](#_Toc61913710)

[5.1. Oporavak AD objekta 34](#_Toc61913711)

[5.2. Oporavak SQL baze 35](#_Toc61913712)

[5.3. Oporavak mail-a 36](#_Toc61913713)

[6. Osvrt na konfiguraciju sigurnosne pohrane 37](#_Toc61913714)

[7. Cloud backup vs Local backup 37](#_Toc61913715)

[8. Zaključak 40](#_Toc61913716)

[9. Reference 41](#_Toc61913717)

1. Sažetak

Cilj projekta Sigurnosna pohrana i oporavak IT sustava ( „SPOIT“ ) je uspješno isplanirati i implementirati plan sigurnosne pohrane i oporavka IT sustava za tvrtku X uz pomoć VEEAM platforme. Potrebno je uz pomoć VEEAM-a napraviti backup heterogene okoline. Konkretno, okolina se sastoji od 3 Windows servera te 2 Linux servera. Na različitim poslužiteljima nalaze se različite uloge. Projekt se smatra u potpunosti uspješnim ako domena nakon oporavka Domain Controllera ponovno kompletno funkcionalna (svi servisi rade kako treba).

1. Opis infrastrukture

Svi poslužitelji nalaze se u domeni „backup.local“.

**VM SPOI-SDC – WS2016**

FQDN: serverdc.backup.local

**vCPUs**: 2CPUs

**Memory**: 2GB

**Storage disks**:

Disk 0 – 60GB

**eth0**: 10.10.10.1/24

**VM SPOI-EXCHANGE – WS2016**

FQDN: spoi-exchange.backup.local

**vCPUs**: 2CPUs

**Memory**: 16GB

**Storage disks**:

Disk 0 – 60GB

**eth0**: 10.10.10.3/24

**VM SPOI-L2 – CentOS 7**

FQDN: spoi-l2.backup.local

**vCPU**: 1CPU

**Memory**: 4GB

**Storage disks**:

/dev/sda – 16GB

**eth0**: 10.10.10.12/24

**VM SPOI-SQL – WS2016**

FQDN: spoi-sql.backup.local

**vCPUs**: 2CPUs

**Memory**: 8GB

**Storage disks**:

Disk 0 – 60GB

**eth0**: 10.10.10.2/24

**VM SPOI-L1 – CentOS 7**

FQDN: spoi-l1.backup.local

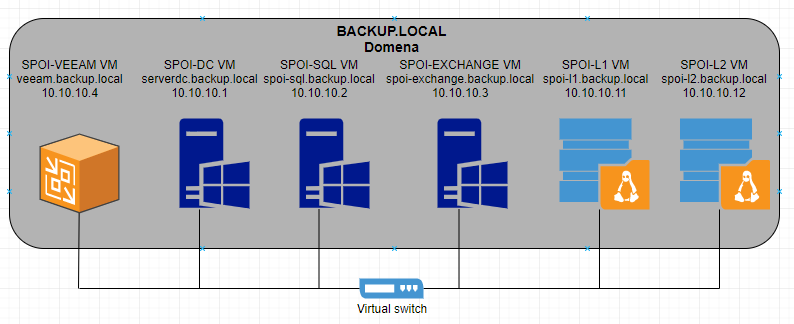
**vCPU**: 1CPU

**Memory**: 4GB

**Storage disks**:

/dev/sda – 16GB

**eth0**: 10.10.10.11/24



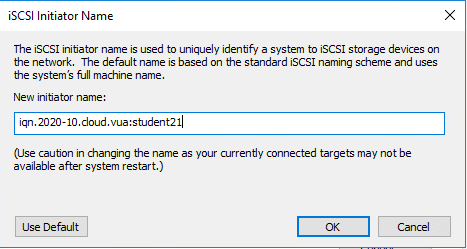
Slika 1 – Skica infrastructure

* 1. Priprema infrastrukture
     1. Spajanje poslužitelja SPOI-VEEAM na iSCSI Target

Prije početka izrade procedura za sigurnosnu pohranu i oporavak klijentskog sustava, moramo na SPOI-VEEAM VM priključiti iSCSI disk na koji ćemo spremati backup-ove. Također, napraviti ćemo novi Veeam repozitorij koji će korstiti taj disk.

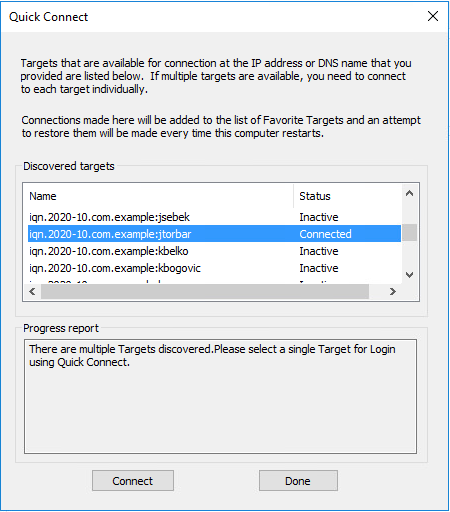
Prvo što trebamo napraviti jest podesiti iSCSI initiator name.

iSCSI initiator 🡪 Configuration 🡪 iSCSI initiator name



Slika 2 – iSCSI initiator name

Nakon što smo postavili iSCSI initiator name prema zadanoj tablici, spajamo se na iSCSI target iqn.2020-10.cloud.vua:jtorbar.

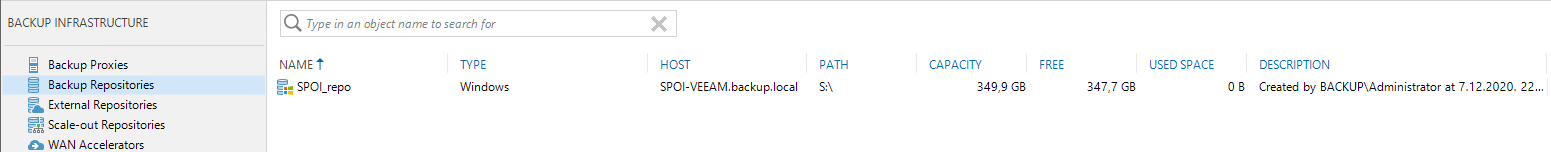


Slika 3 – iSCSI initiator targets

Kada smo spojeni na target pokrećemo automatsku konfiguraciju uređaja te nakon toga formatiramo disk u ReFS format, allocation unit veličine 64kB te mu dodjeljujemo slovo S:.

Nakon što smo formatirali disk moramo napraviti novi Veeam repozitorij koji će ga koristiti za pohranu backup-ova. Ulogirat ćemo se u Veeam konzolu i pod karticom Backup Infrastructure ćemo kreirati novi repozitorij My\_repo.

Backup Infrastructure 🡪 Backup repositories 🡪 Add repository



Slika 4 – Veeam Backup Repositories

* + 1. Kreiranje i konfiguracija SMB-a i NFS-a na poslužitelju SPOI-L1

Na poslužitelju SPOI-L1 ( 10.10.10.11 ) kreirat ćemo jedan dijeljeni NFS direktorij s 10 .txt datoteka veličine 50MiB.

[root@spoi-l1]#systemctl enable nfs-server

[root@spoi-l1]#systemctl start nfs-server

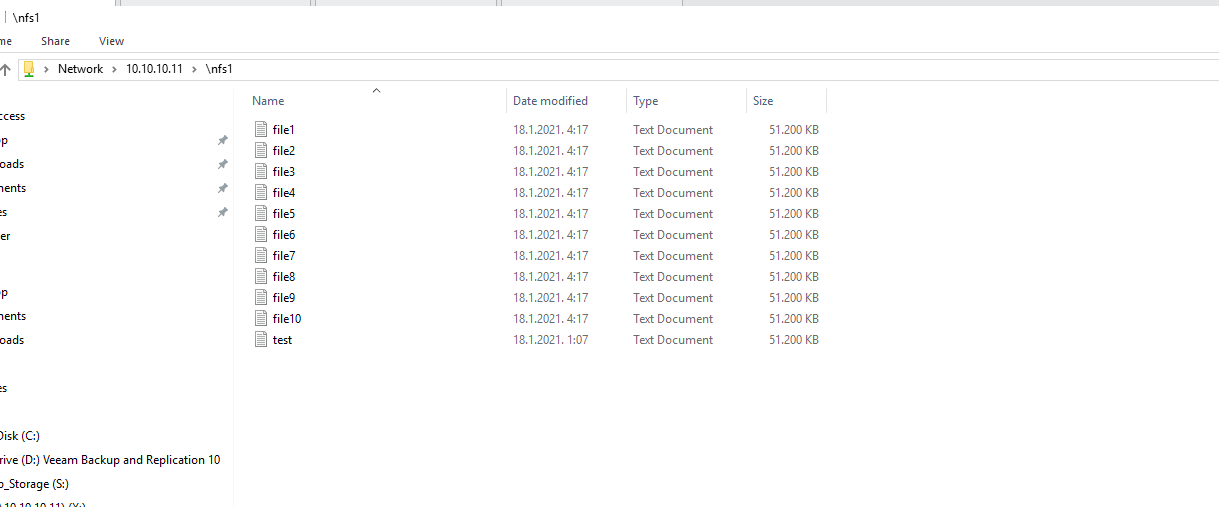
[root@spoi-l1]#mkdir /nfs1

[root@spoi-l1]#echo “/nfs1 10.10.10.0/24(rw)” >> /etc/exports

[root@spoi-l1]#systemctl restart nfs-server

[root@spoi-l1]#exportfs -arv

[root@spoi-l1]#exportfs -s



Slika 5 – Pristup NFS share-u sa poslužitelja SPOI-VEEAM

Nakon što smo podigli NFS share, konfigurirat ćemo I jedan SMB share koji sadrži 10 .txt datoteka veličine 50MiB I 5 direktorija.

[root@spoi-l1]#yum -y install samba samba-client

[root@spoi-l1]#systemctl enable smb

[root@spoi-l1]#systemctl enable nmb

[root@spoi-l1]#systemctl start smb

[root@spoi-l1]#systemctl start nmb

[root@spoi-l1]#mkdir /samba

[root@spoi-l1]#groupadd sambashare

[root@spoi-l1]#chgrp sambashare /samba

[root@spoi-l1]#useradd -M -d /samba/smbuser -s /usr/bin/nologin -G sambashare smbuser

[root@spoi-l1]#mkdir /samba/smbuser

[root@spoi-l1]#chown test:sambashare /samba/smbuser

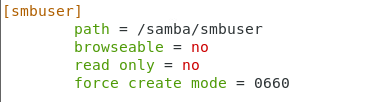
[root@spoi-l1]#chmod 2770 /samba/smbuser

[root@spoi-l1]#smbpasswd -a smbuser

[root@spoi-l1]#smbpasswd -e smbuser

[root@spoi-l1]#cp /etc/samba/smb.conf /etc/samba/smb.conf.orig

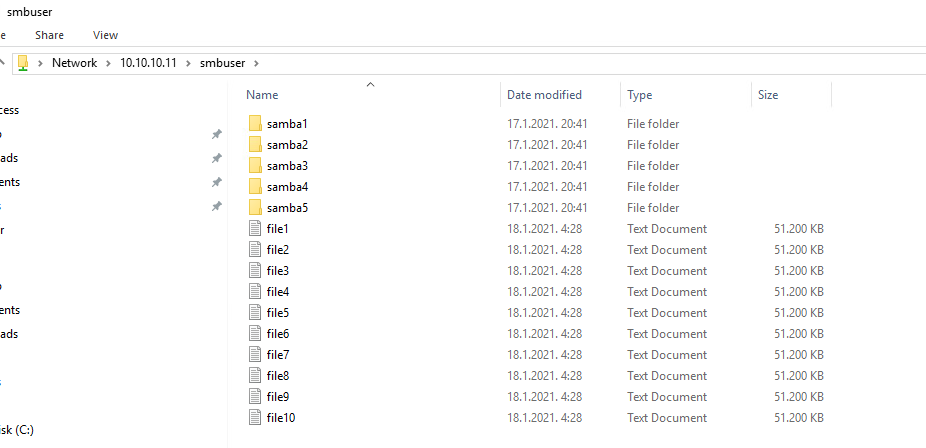
[root@spoi-l1]#vim /etc/samba/smb.conf



Slika 6 - /etc/samba/smb.conf nakon uređivanja

[root@spoi-l1]#mkdir /samba/smbuser/samba{1..5}

[root@spoi-l1]#truncate -s 50MiB /samba/smbuser/file{1..10}.txt

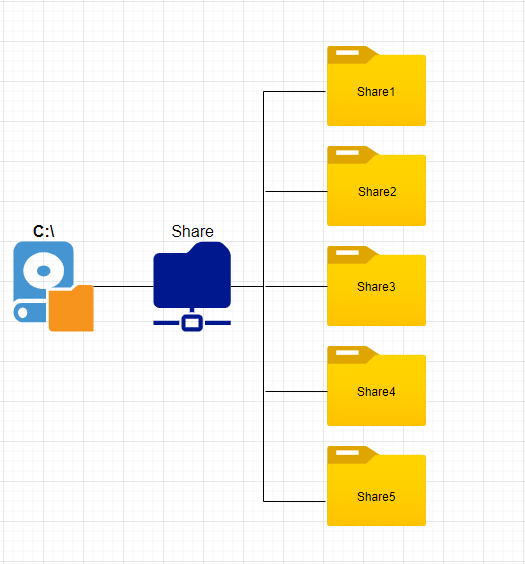


Slika 7 – Pristup SMB share-u s poslužitelja SPOI-VEEAM

* + 1. Kreiranje i konfiguracija dijeljenih datoteka na poslužitelju SPOI-SQL

Na poslužitelju SPOI-SQL ( 10.10.10.2 ) kreirat ćemo jedan dijeljeni direktorij s 5 poddirektorija koji u sebi imaju neke datoteke.

Slike opisuje konfiguraciju direktorija.



Slika 8 – opis dijeljenog direktorija \\10.10.10.2\Share

* 1. Procedura za izradu sigurnosne pohrane sustava

Procedura za izradu sigurnosne pohrane temelji se na važnosti pojedinih dijelova sustava za kontinuiran i neometan rad poslovanja.

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 s 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

Tvrtka X navela je sljedeće zahtjeve za izradu backup plana:

* 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 recovery 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

Budući da su svi poslužitelji u infrastrukturi klijenta od neophodni za poslovanje sigurnosna pohrana svih poslužitelja izvršavat će se **2 puta dnevno**.

Item-level backup poslužitelja S1 i S2 ( SQL i Exchange ) izvršavat će se **3 puta dnevno.**

Svake subote izvršavat će se **synthetic full backup**. To znači da će se svake subote napraviti **full backup** te će svi sljedeći poslovi sigurnosne pohrane kreirati **incremental backup** do sljedećeg synthetic full backup-a.

Raspored izvršavanja poslova sigurnosne pohrane prikazan je tablicom na sljedećoj strani.

Tablica 1 – Raspored izvršavanja poslova sigurnosne pohrane

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Protection Group | Ponedjeljak | Utorak | Srijeda | Četvrtak | Petak | Subota | Nedjelja |
| DC\_PG | Incremental  08:00  16:00 | Incremental  08:00  16:00 | Incremental  08:00  16:00 | Incremental  08:00  16:00 | Incremental  08:00  16:00  Backup files health check  21.00 | Incremental  08:00  16:00  Synthetic Full | Incremental  08:00  16:00 |
| SQL\_PG | Incremental  06:00  14:00  22:00 | Incremental  06:00  14:00  22:00 | Incremental  06:00  14:00  22:00 | Incremental  06:00  14:00  22:00 | Incremental  06:00  14:00  22:00  Backup files health check  21.00 | Incremental  06:00  14:00  22:00  Synthetic Full | Incremental  06:00  14:00  22:00 |
| MBX\_PG | Incremental  06:00  14:00  22:00 | Incremental  06:00  14:00  22:00 | Incremental  06:00  14:00  22:00 | Incremental  06:00  14:00  22:00 | Incremental  06:00  14:00  22:00  Backup files health check  21.00 | Incremental  06:00  14:00  22:00  Synthetic Full | Incremental  06:00  14:00  22:00 |
| LX\_FS | Incremental  Izvršava se nakon SDC\_PG | Incremental  Izvršava se nakon SQL\_PG | Incremental  Izvršava se nakon SQL\_PG | Incremental  Izvršava se nakon SQL\_PG | Incremental  Izvršava se nakon SQL\_PG  Backup files health check  21.00 | Incremental  Izvršava se nakon SQL\_PG  Synthetic Full | Incremental  Izvršava se nakon SQL\_PG |
| LX\_KVM | Incremental  Izvršava se nakon DC\_PG | Incremental  Izvršava se nakon DC\_PG | Incremental  Izvršava se nakon DC\_PG | Incremental  Izvršava se nakon DC\_PG | Incremental  Izvršava se nakon DC\_PG  Backup files health check  21.00 | Incremental  Izvršava se nakon DC\_PG  Synthetic Full | Incremental  Izvršava se nakon DC\_PG |
| File\_Shares | Incremental  Izvršava se nakon LX\_FS | Incremental  Izvršava se nakon LX\_FS | Incremental  Izvršava se nakon LX\_FS | Incremental  Izvršava se nakon LX\_FS | Incremental  Izvršava se nakon LX\_FS  Backup files health check  21.00 | Incremental  Izvršava se nakon LX\_FS  Synthetic Full | Incremental  Izvršava se nakon LX\_FS |

* 1. Procedura za oporavak

Proceduru za oporavak smišljamo ovisno o scenariju koji se dogodio. Najjednostavnija podjela procedura za oporavak je na Data Recovery i Disaster Recovery.

* Data Recovery – gubitak podataka, ali računala i spremišta podataka čitavi
* Disaster Recovery – gubitak podataka I nemogućnost korištenja računala i spremišta podataka

Za klijentsku infrastrukturu važnost podataka na pojedinim poslužiteljima definirana je sljedećim popisom ( 1. je od najveće važnosti ):

1. SPOI-SDC
2. SPOI-SQL
3. SPOI-EXCHANGE
4. SPOI-L1
5. SPOI-L2

Sljedeći koraci mogu vrijediti za svaki od gore navedenih scenarija.

Nakon što smo identificirali problem i koje smo podatke izgubili, postavljamo si pitanja:

* „Zašto je došlo do gubitka podataka?“ – Analiza uzroka gubitka podataka, izrada plana implementacije zakrpi
* “Je li vrijedi raditi oporavak izgubljenih podataka?” – Koliko gubitak podataka utječe na svakodnevne poslovne operacije

Bitna stavka koju valja navesti za proceduru oporavka jest stanje backup datoteka. Backup ciklusi se MORAJU odvijati u planiranim intervalima. Od iznimne je važnosti i da backup datoteke budu redovno provjerene ( tjedni health check ).

Veeam Backup & Replication nam nudi nekolicinu opcija za različite scenarije Disaster Recovery-a. Pošto mi koristimo Veeam za sigurnosnu pohranu fizičkih poslužitelja, oporavak cijelog sustava radit ćemo pomoću **VRM** ( **Veeam Recovery Media** ).

To je alat kojim možemo napraviti **Bare-Metal Recovery** Windows poslužitelja na bilo koji dostupni restore point. To znači da možemo napraviti oporavak kompletnog računala sa svim njegovim funkcijama ( OS, Applikacije i datoteke).

Također, VRM nam omogućava oporavak Windows poslužitelja iz nekog System image-a ili DVD arhive koja sadrži System image-e. VRM sadrži alate za dijagnostiku i otklanjanje problema.

VE Suite ( Veeam Explorer Suite ) koristimo za oporavak pojedinih manjih dijelova sustava, kao što su AD objekti, SQL tablice, mail-ovi i slično. VE Suite podržava sljedeće aplikacije:

* Veeam Explorer for Microsoft Active Directory
* Veeam Explorer for Microsoft SQL
* Veeam Explorer for Oracle
* Veeam Explorer for Microsoft Exchange
* Veeam Explorer for Microsoft SharePoint
* Veeam Explorer for Microsoft OneDrive for Business

Od ovih navedenih u korisničkoj infrastrukturi za oporavak nekog dijela sustava koristimo:

* Veeam Explorer for Microsoft Active Directory
* Veeam Explorer for Microsoft SQL
* Veeam Explorer for Microsoft Exchange

1. Razrada projekta – projektno rješenje
   1. Dodavanje managed servera u Veeam infratrukturu

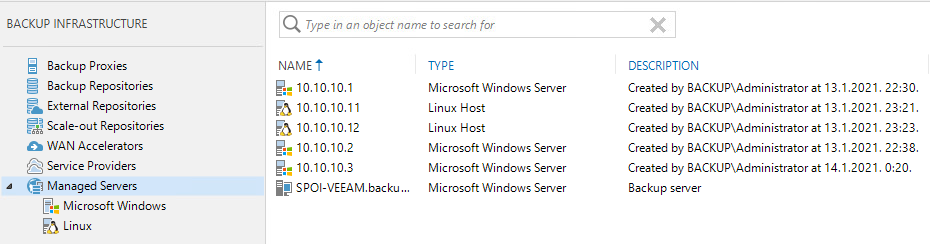
Za početak, dodat ćemo servere za koje ćemo kreirati backup job-ove. To ćemo napraviti kroz Veeam Backup Infrastructure.

Backup Infrastructure 🡪 Managed Servers 🡪 Add Server

Za svaki server moramo specificirati njegov OS, njegovu IP adresu i credential-se. Na linux poslužiteljima korsitimo autentikaciju putem privatnih ključeva.

Za domenska računala korisnik je **BACKUP\Administrator** te je njegova lozinka „**Pa$$w0rd**“.

Nakon što smo dodali sve servere stanje bi trebalo izgledati kao na screenshotu:



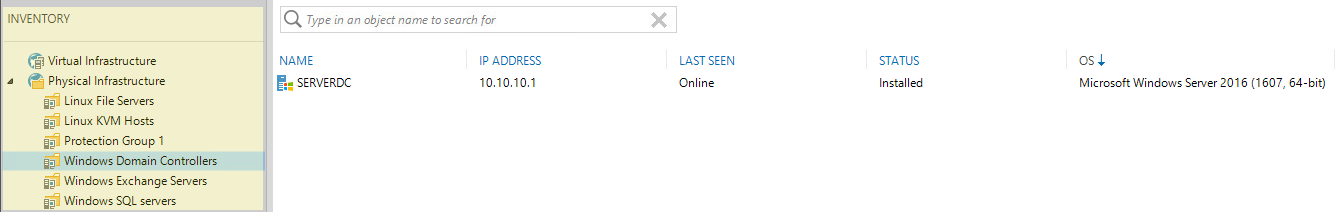
Slika 9 – Backup Infrastructure, Managed Servers

* 1. Dodavanje Protection Group-a u Veeam Inventory

Kada smo dodali servere, kreiramo Protection Group kako bi imali bolji pregled i sistematiku naše infrastrukture, a i instalirali Veeam agente na poslužitelje. Kreirat ćemo sljedeće grupe: **Domain Controllers**, **SQL Servers**, **Exchange Servers**, **Linux File Servers**, **Linux KVM Hosts**.

Inventory 🡪 Physical Infrastructure ( *desni klik* ) 🡪 Add Protection Group…

Poslužitelje, pošto ih nemamo puno dodat ćemo kao individualna računala. Poslužitelje ćemo podijeliti u grupe tako da nazivi grupa odgovaraju rolama poslužitelja. Rescan protection grupe radit će se svaki dan u 21.00. Za Credentials-e koristimo one koji su spremljeni od dodavanja Managed poslužitelja. Distribucijski poslužitelj je SPOI-VEEAM.backup.local te će on instalirati backup agente automatski te će iste automatski ažurirati kada to bude potrebno.

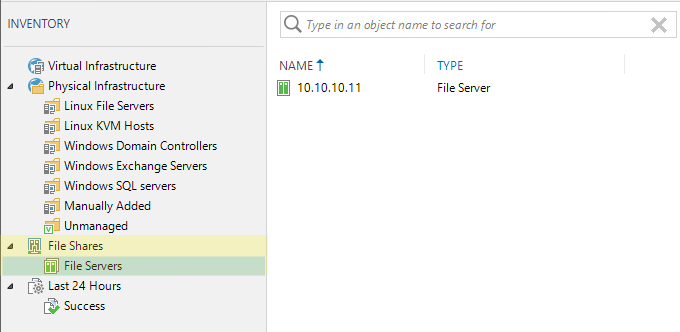


Slika 10 – Inventory, Domain Controllers Protection group

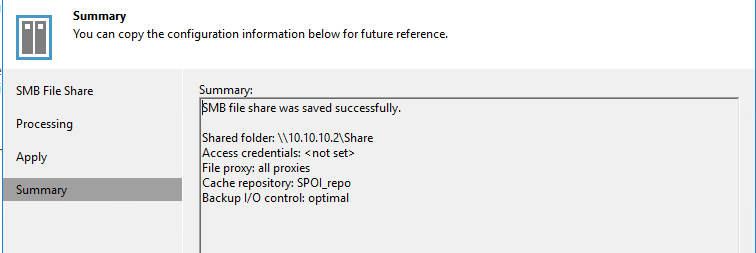
Također ćemo dodati I dijeljene direktorije na poslužitelju **SPOI-L1** putem SMB ( “Server Message Block” ) i NFS ( “Network File System” ) protokola.

Backup Infrastructure 🡪 File Share ( *desni klik* ) 🡪 Add File Share…

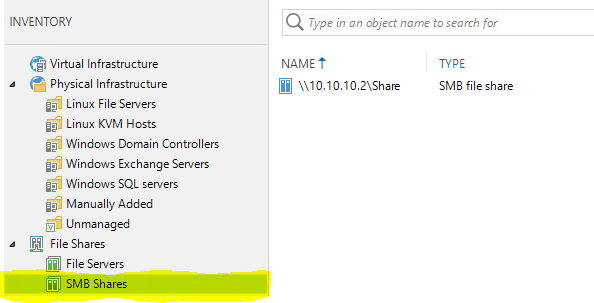
Dodat ćemo File Server, poslužitelj **SPOI-L1** ( **10.10.10.11** ) i dijeljeni direktorij *Share* koji se nalazi na poslužitelju **SPOI-SQL** ( **10.10.10.2** ). Za poslužitelj **SPOI-L1** odabrat ćemo dijeljene direktorije /samba i /nfs1.



Slika 11 – Inventory, File Shares 🡪 File Servers



Slika 12 - [\\10.10.10.2\Share](file:///\\10.10.10.2\Share) SMB Share Summary



Slika 13 – VeeamInventory, File Shares 🡪 SMB Shares

* 1. Izrada backup job-ova

Poslove za izradu sigurnosne pohrane kreiramo na kartici Home. Kreiramo redom poslove kako su navedene Protection grupe u tablici 1 u poglavlju 0.

* + 1. DC\_PG\_Backup

Prvi backup job koji ćemo kreirati biti će sigurnosna pohrana DC-ova.

Home 🡪 Jobs ( desni klik ) 🡪 Backup 🡪 Windows computer…

Otvara nam se New Agent Backup Job wizard.

Job mode

Tip backup agenta je Server, a mod u kojem će raditi je Managed by backup server

Name

Ime backup job-a bit će DC\_PG\_Backup.

Computers

Na koraku *Computers* odabiremo Windows Domain Controllers Protection grupu. Backup mode je Entire Computer. To znači da će naš backup moći oporaviti i datoteke potrebne za rad operacijskog sustava i diskovne volumene te pojedine datoteke.

Storage

Na koraku *Storage* kao Backup repository odabiremo SPOI\_repo, Retention policy će biti 7 restore point-ova. Što znači da ćemo moći oporaviti poslužitelje u trenutle kada su izvršeni svaki od zadnjih 7 backup job-ova.

Konfigurirat ćemo i GFS ( Grandfather – Father - Son) retention policy. GFS je stupnjevita shema retention policy-a. Koristi nekoliko ciklusa kako bi zadržali pojedine backup-ove različiti vremenski period. GFS politika koju implementiramo sprema tjedne full backup-ove 7 dana, mjesečne 1 mjesec, kvartalne 3 mjeseca.

Storage 🡪 Advanced Settings

Za *Storage* ćemo konfigurirati i i neke napredne postavke. Sintetički full backup kreirat će se svaku subotu. Storage-level corruption guard će raditi health check backupiranih datoteka svaki petak. Compression level je Extreme. Storage optimization je Local Target.

Guest Processing

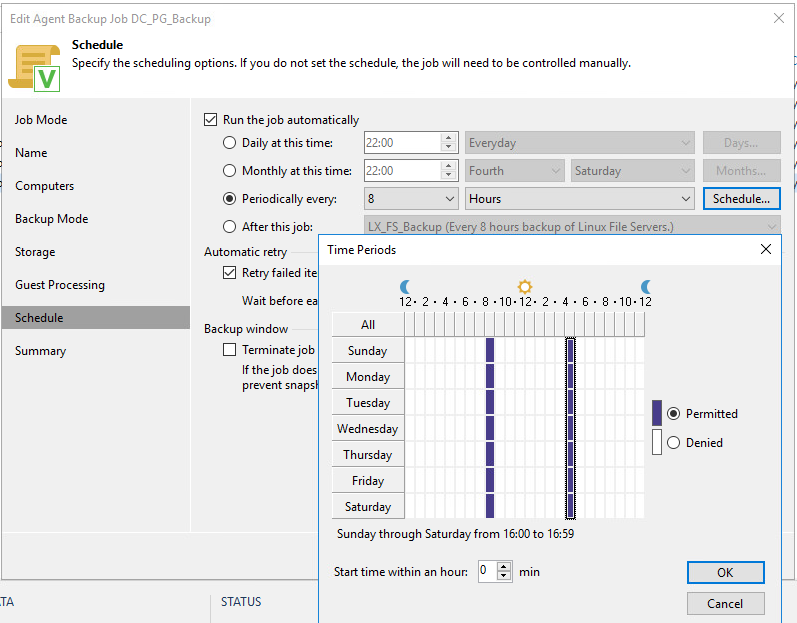
U ovom koraku ćemo konfigurirati procesiranje aplikacija koje se vrte na DC-ovima. Omogućit ćemo i Application-aware Processing i Guest File System Indexing. Za ove poslužitelje ostavit ćemo default-ne postavke za ove dvije opcije.

**App-aware processing** – detektira i priprema aplikaciju za konzistentni backup, procesira transakcijske logove i konfigurira operacijski sustav da odradi određene korake za oporavak pri prvom paljenju

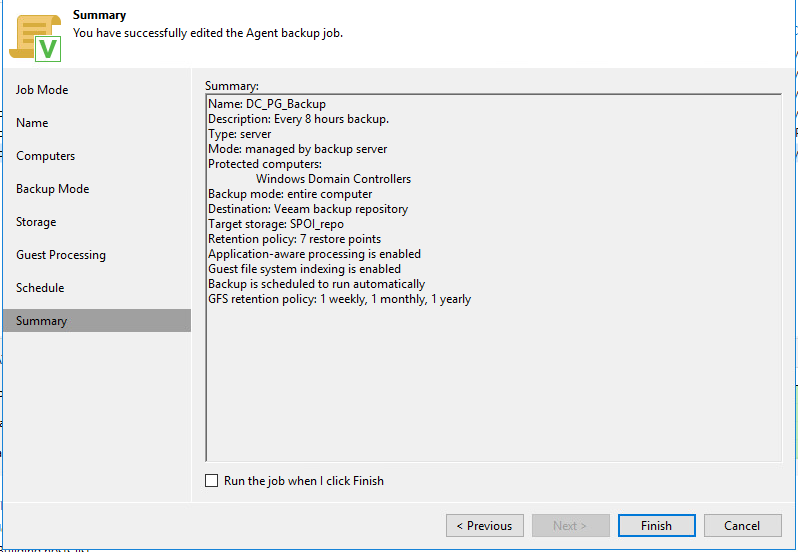
**Guest File System Indexing** – kreira katalog gostovih datoteka te time omogućuje „1-click“ oporavak individualnih datoteka.

Schedule

Ovaj backup job kao i većinu ostalih izvršavat ćemo periodički, svakih 8 sati.



Slika 14 – DC\_PG\_Backup, Backup Job Schedule



Slika 15 – DC\_PG\_Backup, Backup Job Summary

* + 1. SQL\_PG\_Backup

Sljedeći backup job koji ćemo kreirati bit će sigurnosna pohrana SQL servera.

Home 🡪 Jobs ( desni klik ) 🡪 Backup 🡪 Windows computer…

Otvara nam se New Agent Backup Job wizard.

Job mode

Tip backup agenta je Server, a mod u kojem će raditi je Managed by backup server.

Name

Ime backup job-a bit će SQL\_PG\_Backup.

Computers

Na koraku *Computers* odabiremo Windows SQL Servers Protection grupu. Backup mode je Entire Computer. To znači da će naš backup moći oporaviti i datoteke potrebne za rad operacijskog sustava i diskovne volumene te pojedine datoteke.

Storage

Na koraku *Storage* kao Backup repository odabiremo SPOI\_repo, Retention policy će biti 7 restore point-ova. Što znači da ćemo moći oporaviti poslužitelje u trenutle kada su izvršeni svaki od zadnjih 7 backup job-ova.

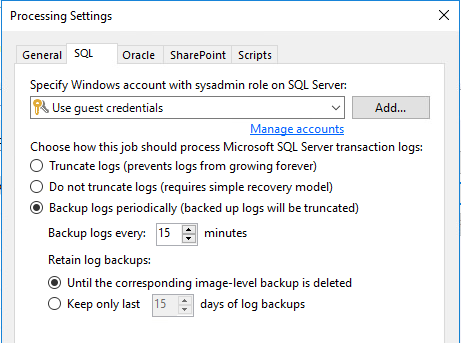
Konfigurirat ćemo i GFS ( Grandfather – Father - Son) retention policy. GFS je stupnjevita shema retention policy-a. Koristi nekoliko ciklusa kako bi zadržali pojedine backup-ove različiti vremenski period. GFS politika koju implementiramo sprema tjedne full backup-ove 7 dana, mjesečne 1 mjesec, kvartalne 3 mjeseca.

Storage 🡪 Advanced Settings

Za *Storage* ćemo konfigurirati i i neke napredne postavke. Sintetički full backup kreirat će se svaku subotu. Storage-level corruption guard će raditi health check backupiranih datoteka svaki petak. Compression level je Extreme. Storage optimization je Local Target.

Guest Processing

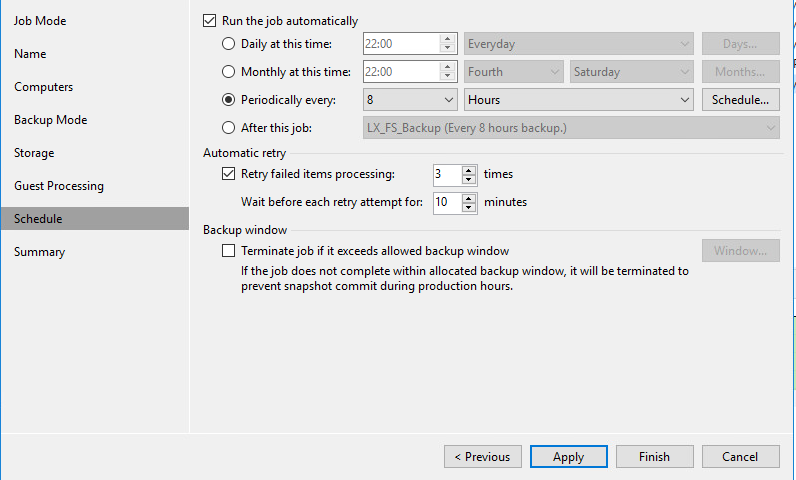
U ovom koraku ćemo konfigurirati procesiranje aplikacija koje se vrte na SQL Serverima. Omogućit ćemo i Application-aware Processing i Guest File System Indexing. Za ove poslužitelje konfigurirat ćemo backup SQL transakcijskih logova koji će se pri kreiranju backup datoteke trunkirati[[1]](#footnote-1). Credentials-i koje koristimo su guest credentials, backup logova vrši se svakih 15 minuta, logovi se zadržavaju dok se odgovarajući image-level backup ne izbriše.



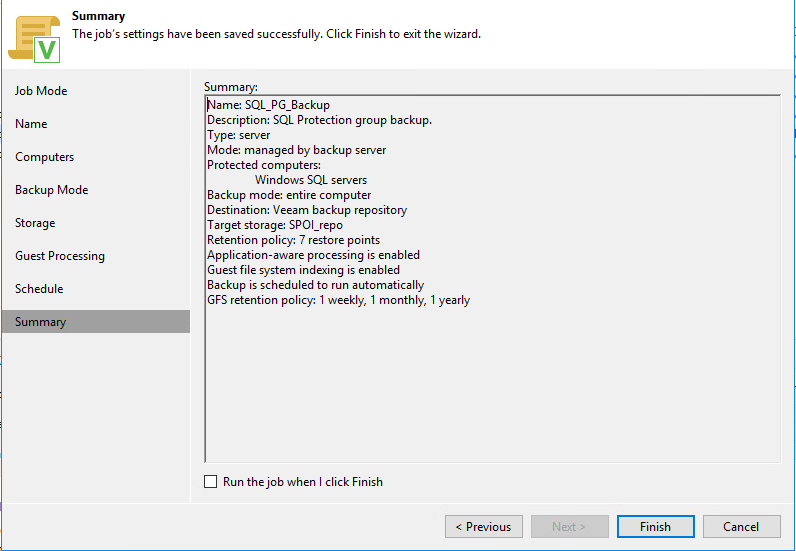
Slika 16 – SQL\_PG\_Backup, SQL Processing Settings

Schedule

Ovaj backup job kao i većinu ostalih izvršavat ćemo periodički, svakih 8 sati.



Slika 17 – SQL\_PG\_Backup, Backup Job Schedule



Slika 18 – SQL\_PG\_Backup, Backup job Summary

* + 1. MBX\_PG\_Backup

Treći backup job koji ćemo kreirati biti će sigurnosna pohrana Exchange servera.

Home 🡪 Jobs ( desni klik ) 🡪 Backup 🡪 Windows computer…

Otvara nam se New Agent Backup Job wizard.

Job mode

Tip backup agenta je Server, a mod u kojem će raditi je Managed by backup server.

Name

Ime backup job-a bit će MBX\_PG\_Backup.

Computers

Na koraku *Computers* odabiremo Windows Exchange Servers Protection grupu. Backup mode je Entire Computer. To znači da će naš backup moći oporaviti i datoteke potrebne za rad operacijskog sustava i diskovne volumene te pojedine datoteke.

Storage

Na koraku *Storage* kao Backup repository odabiremo SPOI\_repo, Retention policy će biti 7 restore point-ova. Što znači da ćemo moći oporaviti poslužitelje u trenutle kada su izvršeni svaki od zadnjih 7 backup job-ova.

Konfigurirat ćemo i GFS ( Grandfather – Father - Son) retention policy. GFS je stupnjevita shema retention policy-a. Koristi nekoliko ciklusa kako bi zadržali pojedine backup-ove različiti vremenski period. GFS politika koju implementiramo sprema tjedne full backup-ove 7 dana, mjesečne 1 mjesec, kvartalne 3 mjeseca.

Storage 🡪 Advanced Settings

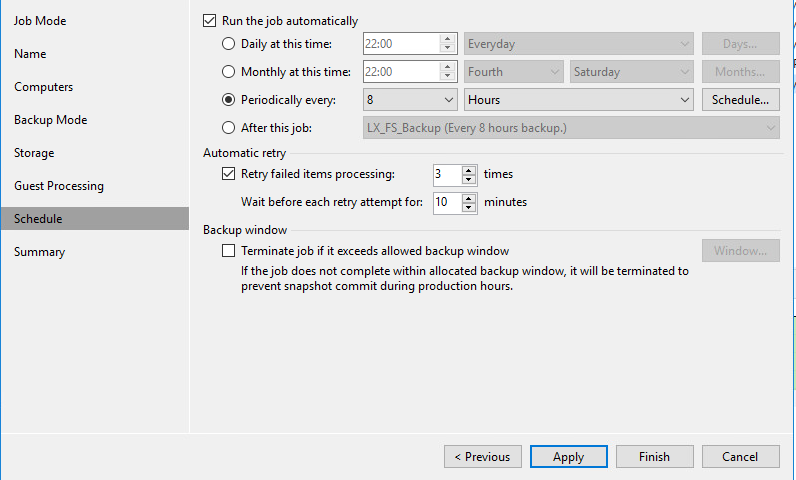
Za *Storage* ćemo konfigurirati i i neke napredne postavke. Sintetički full backup kreirat će se svaku subotu. Storage-level corruption guard će raditi health check backupiranih datoteka svaki petak. Compression level je Extreme. Storage optimization je Local Target.

Guest Processing

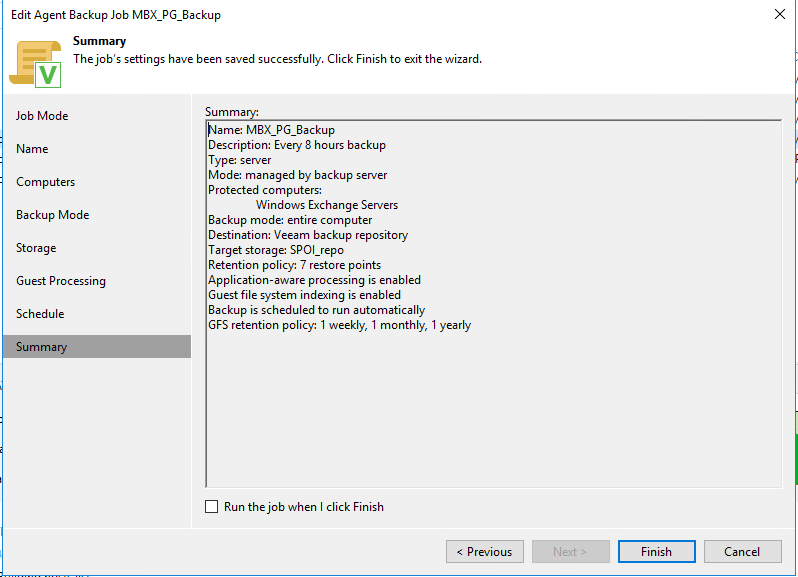
U ovom koraku ćemo konfigurirati procesiranje aplikacija koje se vrte na Microsoft Exchange Serverima. Omogućit ćemo i Application-aware Processing i Guest File System Indexing. Za ove poslužitelje ostavit ćemo default-ne postavke za ove dvije opcije.

Schedule

Ovaj backup job kao i većinu ostalih izvršavat ćemo periodički, svakih 8 sati.



Slika 19 – MBX\_PG\_Backup, Backup Job Schedule



Slika 20 – MBX\_PG\_Backup, Backup Job Summary

* + 1. LX\_FS\_Backup

Sljedeći backup job koji ćemo kreirati biti će sigurnosna pohrana Linux datotečnih servera.

Home 🡪 Jobs ( desni klik ) 🡪 Backup 🡪 Linux computer…

Otvara nam se New Agent Backup Job wizard.

Job mode

Tip backup agenta je Server, a mod u kojem će raditi je Managed by backup server.

Name

Ime backup job-a bit će LX\_FS\_Backup.

Computers

Na koraku *Computers* odabiremo Linux File Servers Protection grupu. Backup mode je Entire Computer. To znači da će naš backup moći oporaviti i datoteke potrebne za rad operacijskog sustava i diskovne volumene te pojedine datoteke.

Storage

Na koraku *Storage* kao Backup repository odabiremo SPOI\_repo, Retention policy će biti 7 restore point-ova. Što znači da ćemo moći oporaviti poslužitelje u trenutle kada su izvršeni svaki od zadnjih 7 backup job-ova.

Konfigurirat ćemo i GFS ( Grandfather – Father - Son) retention policy. GFS je stupnjevita shema retention policy-a. Koristi nekoliko ciklusa kako bi zadržali pojedine backup-ove različiti vremenski period. GFS politika koju implementiramo sprema tjedne full backup-ove 7 dana, mjesečne 1 mjesec, kvartalne 3 mjeseca.

Storage 🡪 Advanced Settings

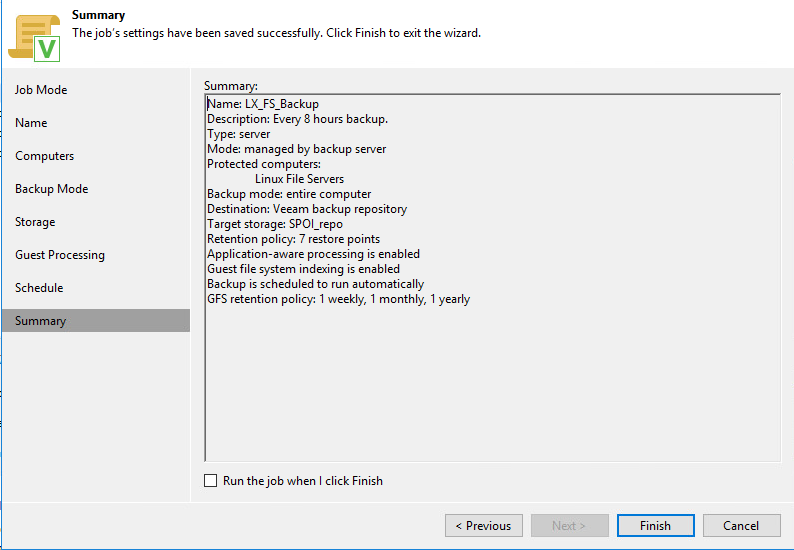
Za *Storage* ćemo konfigurirati i i neke napredne postavke. Sintetički full backup kreirat će se svaku subotu. Storage-level corruption guard će raditi health check backupiranih datoteka svaki petak. Compression level je Extreme. Storage optimization je Local Target.

Guest Processing

U ovom koraku ćemo konfigurirati procesiranje aplikacija koje se vrte na Linux datotečnim poslužiteljima. Omogućit ćemo i Application-aware Processing i Guest File System Indexing. Za ove poslužitelje ostavit ćemo default-ne postavke za ove dvije opcije.

Schedule

Ovaj backup job kao i većinu ostalih izvršavat ćemo periodički, nakon svakog odrađenog DC\_PG\_Backup job-a.



Slika 21 – LX\_FS\_Backup, Backup Job Summary

* + 1. LX\_KVM\_Backup

Peti backup job koji ćemo kreirati biti će sigurnosna pohrana Linux KVM host-ova.

Home 🡪 Jobs ( desni klik ) 🡪 Backup 🡪 Linux computer…

Otvara nam se New Agent Backup Job wizard.

Job mode

Tip backup agenta je Server, a mod u kojem će raditi je Managed by backup server.

Name

Ime backup job-a bit će LX\_KVM\_Backup.

Computers

Na koraku *Computers* odabiremo Linux KVM Hosts Protection grupu. Backup mode je Entire Computer. To znači da će naš backup moći oporaviti i datoteke potrebne za rad operacijskog sustava i diskovne volumene te pojedine datoteke.

Storage

Na koraku *Storage* kao Backup repository odabiremo SPOI\_repo, Retention policy će biti 7 restore point-ova. Što znači da ćemo moći oporaviti poslužitelje u trenutle kada su izvršeni svaki od zadnjih 7 backup job-ova.

Konfigurirat ćemo i GFS ( Grandfather – Father - Son) retention policy. GFS je stupnjevita shema retention policy-a. Koristi nekoliko ciklusa kako bi zadržali pojedine backup-ove različiti vremenski period. GFS politika koju implementiramo sprema tjedne full backup-ove 7 dana, mjesečne 1 mjesec, kvartalne 3 mjeseca.

Storage 🡪 Advanced Settings

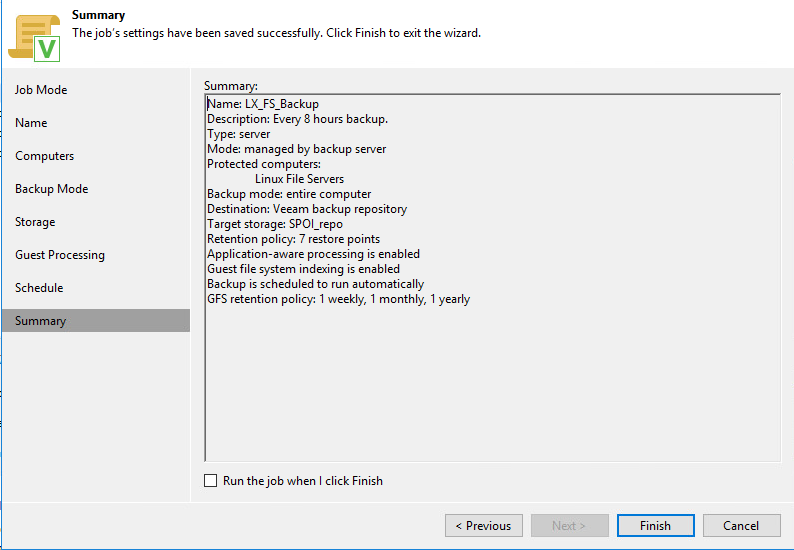
Za *Storage* ćemo konfigurirati i i neke napredne postavke. Sintetički full backup kreirat će se svaku subotu. Storage-level corruption guard će raditi health check backupiranih datoteka svaki petak. Compression level je Extreme. Storage optimization je Local Target.

Guest Processing

U ovom koraku ćemo konfigurirati procesiranje aplikacija koje se vrte na KVM Host-ovima. KVM host-ovima ćemo samo omogućiti Application-aware Processing.

Schedule

Ovaj backup job kao i većinu ostalih izvršavat ćemo periodički, nakon svakog odrađenog SQL\_PG\_Backup job-a.



Slika 22 – LX\_KVM\_Backup, Backup Job Summary

* + 1. File\_Shares\_Backup

Sljedeći backup job koji ćemo kreirati biti će sigurnosna pohrana Linux datotečnog poslužitelja SPOI-L1 i SMB share-a na poslužitelju SPOI-SQL.

Home 🡪 Jobs ( desni klik ) 🡪 Backup 🡪 File Share…

Otvara nam se New Agent Backup Job wizard.

Name

Ime backup job-a bit će File\_Shares\_Backup.

Files and Folders

Direktorije koje želimo sigurno pohraniti su **/nfs** i **/samba**.

Storage

Na koraku *Storage* kao Backup repository odabiremo SPOI\_repo, Retention policy će biti zadnjih 28 dana. Što znači da ćemo moći oporaviti poslužitelje u sve spremljene verzije od zadnjih 28 dana.

Storage 🡪 Advanced Settings

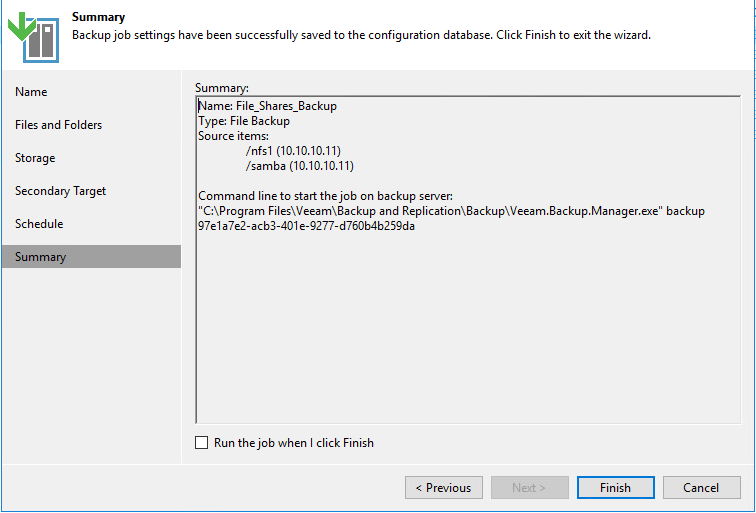
Za *Storage* ćemo konfigurirati i i neke napredne postavke. Backup dozvola pristupa i atributa će raditi samo na folder-levelu. Storage-level corruption guard će raditi health check backupiranih datoteka svaki petak. Compression level je Extreme. Storage optimization je Local Target.

Secondary Target

U ovom koraku nećemo dodavati sekundarni storage target.

Schedule

Ovaj backup job kao i većinu ostalih izvršavat ćemo periodički, nakon svakog odrađenog LX\_FS\_Backup job-a.

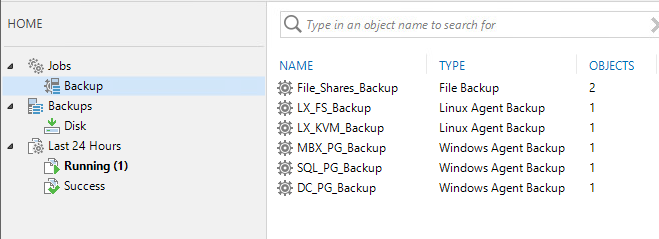


*Slika 23 – File\_Shares\_Backup, Backup Job Summary*

Home 🡪 Jobs ( desni klik ) 🡪 Backup 🡪 File Share…

Otvara nam se New Agent Backup Job wizard.

Nakon izrade backup job-ova kartica Home izgleda ovako:



Slika 24 – Veeam Backup & Replication Home

* 1. Mjerenja backup job-ova

Prilikom izrade strategije za sigurnosnu pohranu sustava na pojedinim poslužiteljima isprobati opcije potpune pohrane cijelog računala i pohrane specifične samo za pojedine usluge.

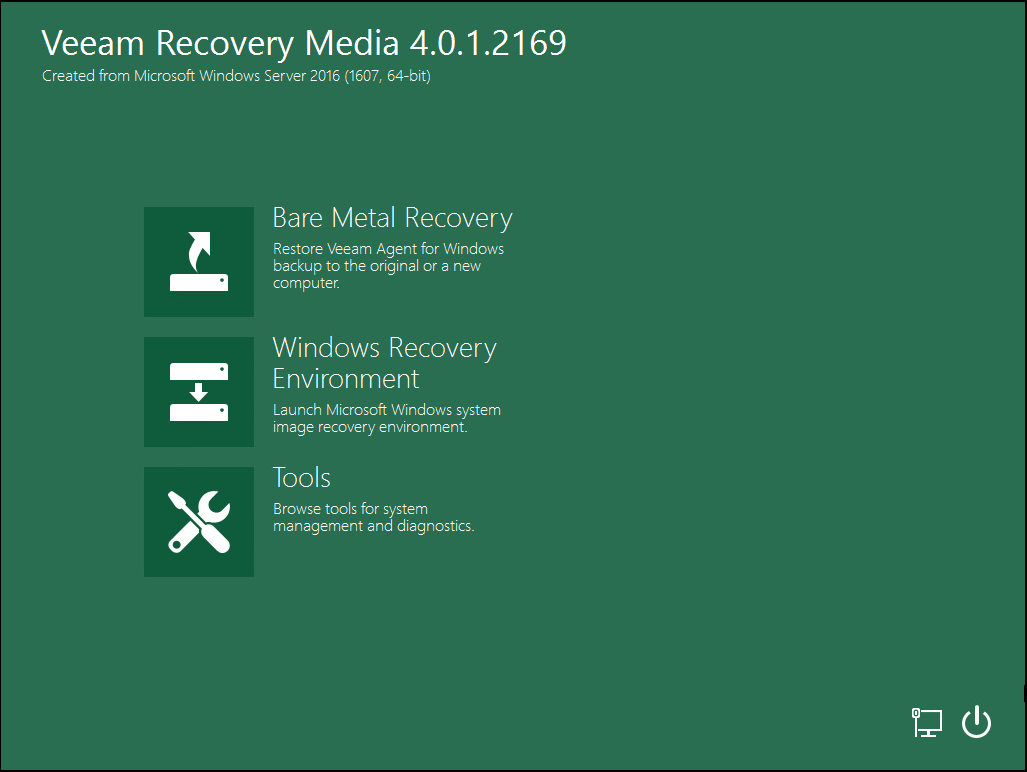
Sva mjerenja rađena su sa Extreme Compression level-om i vrijednosti su aritmetička sredina izvedena iz 3 različita mjerenja.

Tablica 2 – Mjerenja za različite vrste backup-a

|  |  |  |
| --- | --- | --- |
| Job Name | Entire Computer | Volume level |
| **DC\_PG\_Backup** | 05:08 min  5,7 GB Synthetic Full  120 MB Incremental | 05:01 min  5,7 GB Synthetic Full  120 MB Incremental |
| **SQL\_PG\_Backup** | 05:11 min  11.2 GB Synthetic Full  115 MB Incremental | 05:21 min  11,2 GB Synthetic Full  75 MB Incremental |
| **MBX\_PG\_Backup** | 09:34 min  12,1 GB Synthetic Full  513 MB Incremental | 09:32 min  12,1 GB Synthetic Full  388 MB Incremental |
| **LX\_FS\_Backup** | 05:30 min  3,02 GB Synthetic Full  90 MB Incremental | 03:02 min  3,02 GB Synthetic Full  77 MB Incremental |
| **LX\_VM\_Backup** | 04:25 min  3,95 GB Synthetic Full  90 MB Incremental | 5:11 min  3,95 GB Synthetic Full  87 MB Incremental |

1. Oporavak poslužitelja SPOI-SDC[[2]](#footnote-2)

Za potrebe ovog zadatka koristit ćemo poslužitelj SPOI-RECOVERY koji pokreće VRM verzije 4.0.1.2169. Također, isključit ćemo poslužitelj SPOI-SDC.

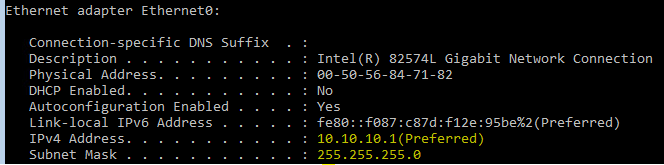


Slika 25 – SPOI\_SDC, Veeam Recovery Media

Radimo Bare-Metal oporavak fizičkog poslužitelja SERVER-DC. Prvo što trebamo napraviti je provjeriti IP adresu mrežnog adaptera na poslužitelju, ako je ona ista kao i ona od poslužitelja SERVERDC, možemo krenuti u proces oporavka.

Tools 🡪 Command Prompt

ipconfig /all



*Slika 26 – SPOI-RECOVERY CMD, ipconfig /all*

Pokrećemo Volume Level Restore wizard – Bare-Metal Recovery.

Backup Location

Kao *Backup Location* odabrat ćemo Network Storage jer se naš backup nalazi unutar Veeam Backup Repository-a.

Network Storage

Na koraku *Network* *Storage* kao Backup repository odabiremo Veeam Backup Repository.

Backup Server

Veeam backup IP = 10.10.10.4:10001

Username = BACKUP\Administrator

Password = Pa$$w0rd

Backup

DC\_PG\_Backup 🡪 10.10.10.1

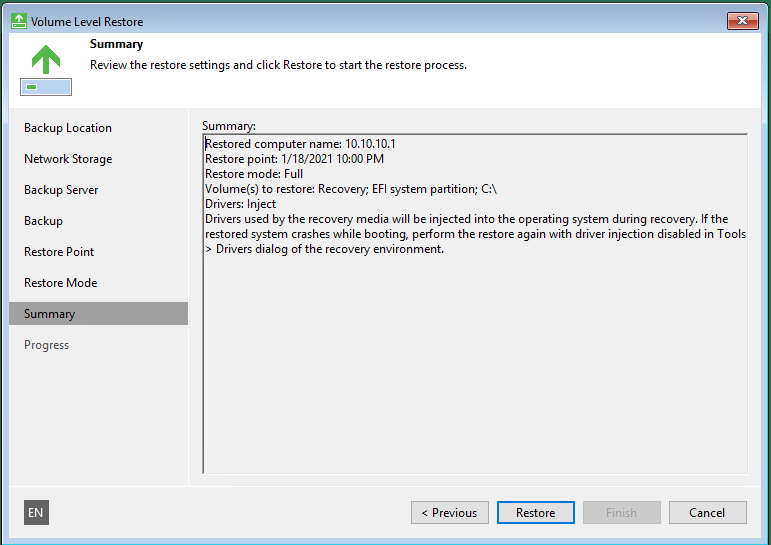
Restore Point

Odabiremo zadnji restore point (10:00 PM Monday 18/01/2021).

Restore Mode

Odabiremo Entire Computer.

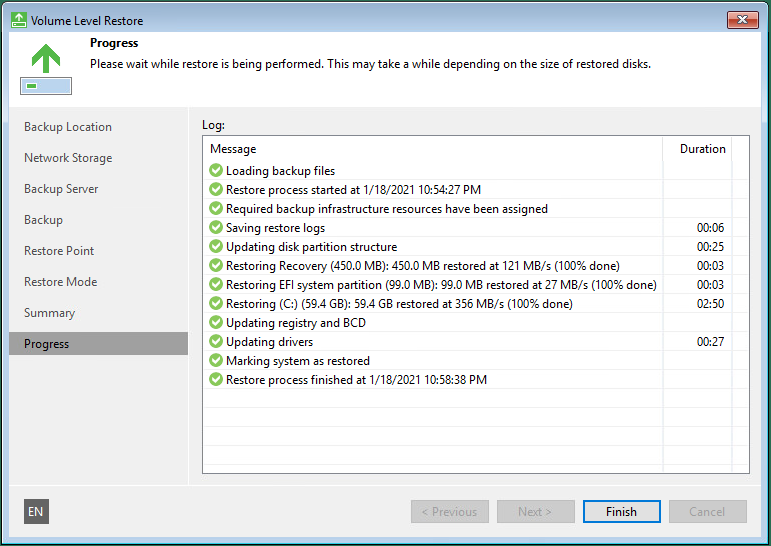
Summary



*Slika 27 – Volume Level Restore Summary*

Progress

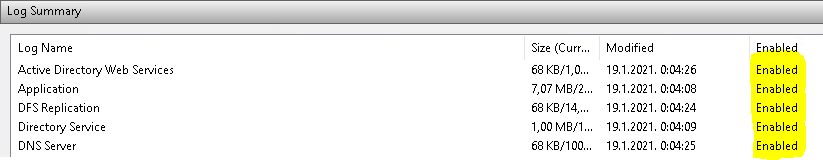
Nakon što proces završi, ponovno ćemo pokrenuti računalo. Nakon reboot-a ćemo testirati rade li sve funkcionalnosti AD-a kako treba.



*Slika 28 – Volume Level Restore Progress*

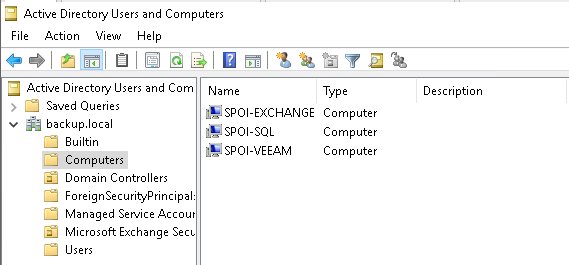
Kada se računalo pokrenulo, prijavit ćemo se s računom domenskog administratora te provjeriti Event Viewer, DNS i AD Users and Computers.

U Event Viewer-u ćemo pogledati jesu li svi servisi koji su potrebni za potrebne funkcionalnosti omogućeni.

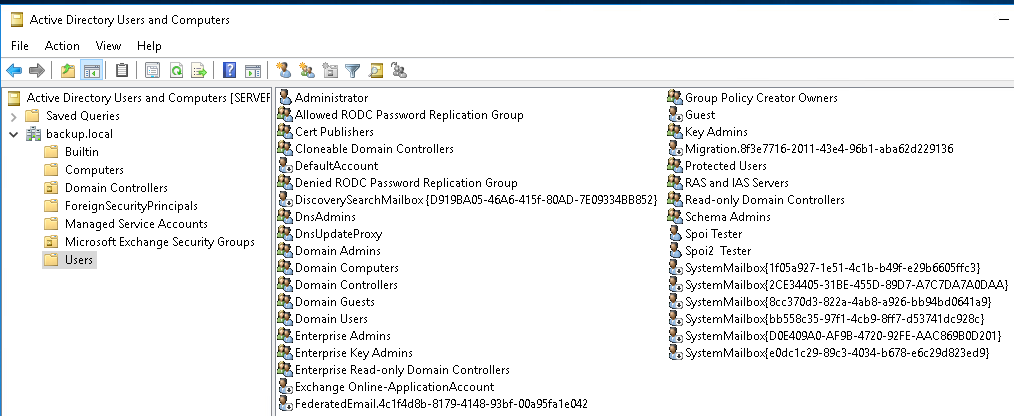


Slika 29 – SPOI-RECOVERY ( SPOI-SDC ), Event Viever Log Summary

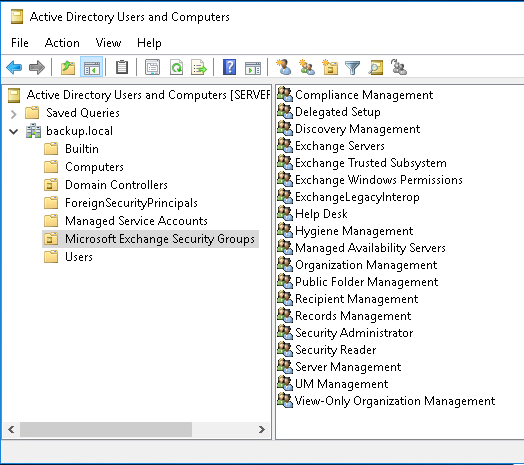
U ADUC-u ćemo pogledati postoje li objekti za sve poslužitelje i korinsike te Exchange Security grupe.



Slika 30 - SPOI-RECOVERY ( SPOI-SDC ), ADUC Computers

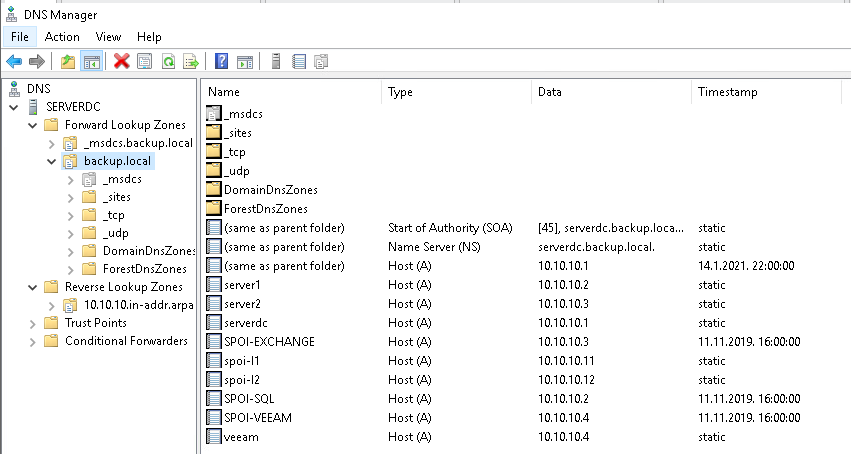


Slika 31 - SPOI-RECOVERY ( SPOI-SDC ), ADUC Users

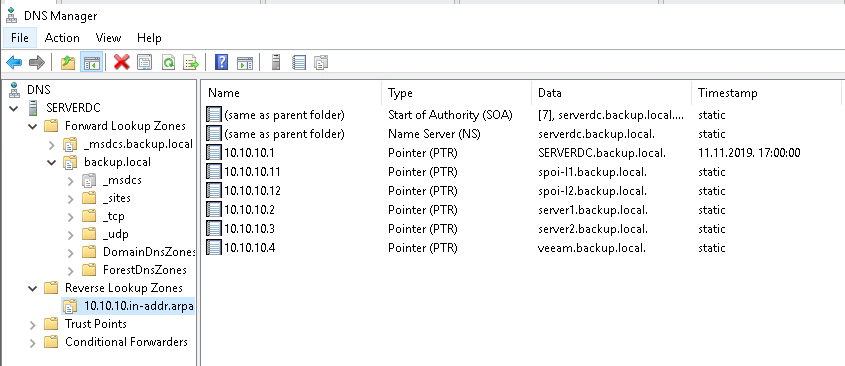


Slika 32 - SPOI-RECOVERY ( SPOI-SDC ), ADUC MS Exchange Security Groups

U DNS Manager-u ćemo pogledati postoje li sve forward i reverse zone te postoje li zapisi za sve poslužitelje.



Slika 33 – SPOI-RECOVERY ( SPOI-SDC ), DNS, Forward Lookup Zones, backup.local



Slika 34 – SPOI-RECOVERY ( SPOI-SDC ), DNS, Reverse Lookup Zones, 10.10.10.in-addr.arpa

Za zadnju provjeru izvršit ćemo sljedeću naredbu kroz powershell na poslužiteljima SPOI-SQL i SPOI-EXCHANGE.

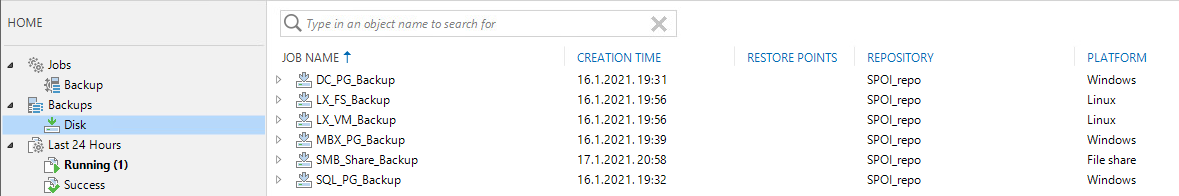
Test-ComputerSecureChannel

Naredba mora vratiti vrijednost true na oba poslužitelja ako je domena funkcionalna.

1. Oporavak dijelova sustava

U ovom poglavlju vraćamo se na poslužitelj SPOI-VEEAM i u Veeam Backup & Replication konzoli na kartici Home otvaramo:

Backups 🡪 Disk

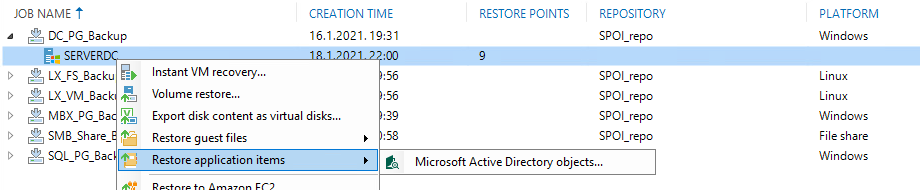


Slika 35 – Veeam Backup and Replication Home, Backups, Disk

* 1. Oporavak AD objekta

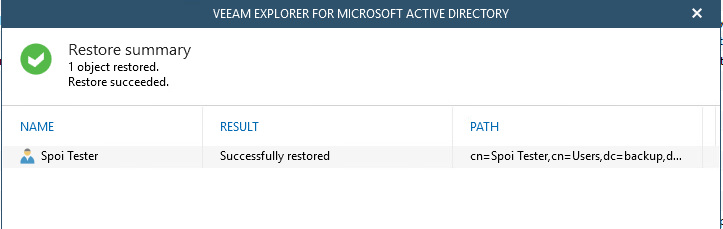
Kako bi testirali oporavak AD objekta, pobrisat ćemo korisnika Spoi Tester iz AD-a te ga vratiti kroz Veeam Explorer for Microsoft Active Directory. Otvaramo job imena DC\_PG\_Backup.

SERVERDC ( desni klik ) 🡪 Restore application items 🡪 Microsoft Active Directory objects…



Slika 36 – SERVERDC, Restore application items, Microsoft Active Directory objects

Otvara se Microsoft Active Directory Object Restore wizard, odabiremo zadnji restore point. Nakon završetka wizarda otvara se Veeam Explorer for Microsoft Active Directory. Potražimo korisnika Spoi Tester te pritisnemo na njega desnim klikom i odaberemo Restore objects to SERVERDC.backup.local.

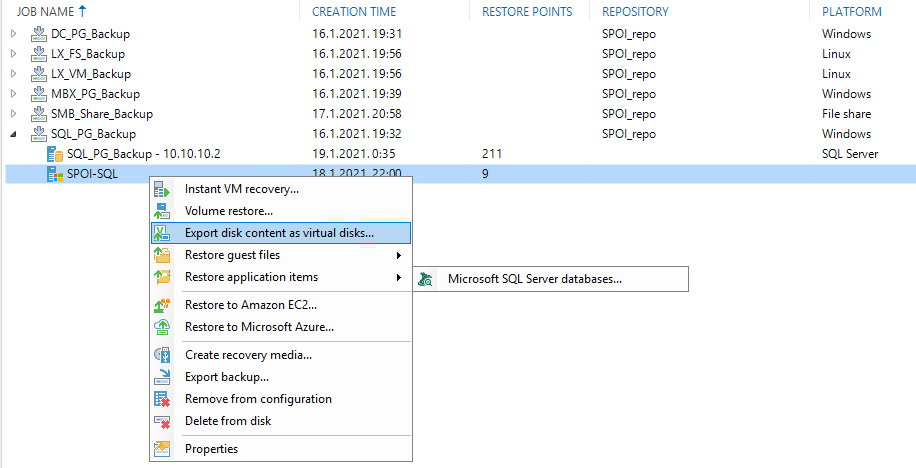


Slika 37 – Uspješan oporavak AD korisničkog objekta

* 1. Oporavak SQL baze

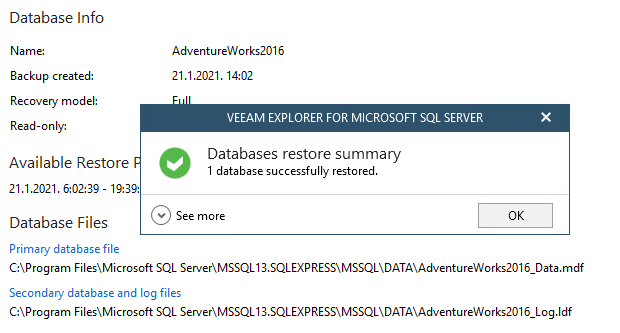
Kako bi testirali oporavak SQL baze, pobrisat ćemo bazu podataka AdventureWorks2016 te ju vratiti kroz Veeam Explorer for Microsoft SQL. Otvaramo job imena SQL\_PG\_Backup.

SPOI-SQL ( desni klik ) 🡪 Restore application items 🡪 Microsoft SQL Server databases…



Slika 38 – SPOI-SQL, Restore application items, Microsoft SQL Server databases

Otvara se Microsoft SQL Server Database Restore wizard, odabiremo zadnji restore point. Nakon završetka wizarda otvara se Veeam Explorer for Microsoft SQL. Potražimo bazu „AdventureWorks2016“ te pritisnemo na nju desnim klikom i odaberemo Restore point-in-time state to SPOI-SQL\SQLEXPRESS. Veeam Explorer nam nudi fine-tuning oporavka gdje možemo odabrati točno vrijeme prije ili poslije neke transakcije ( brisanje baze ).

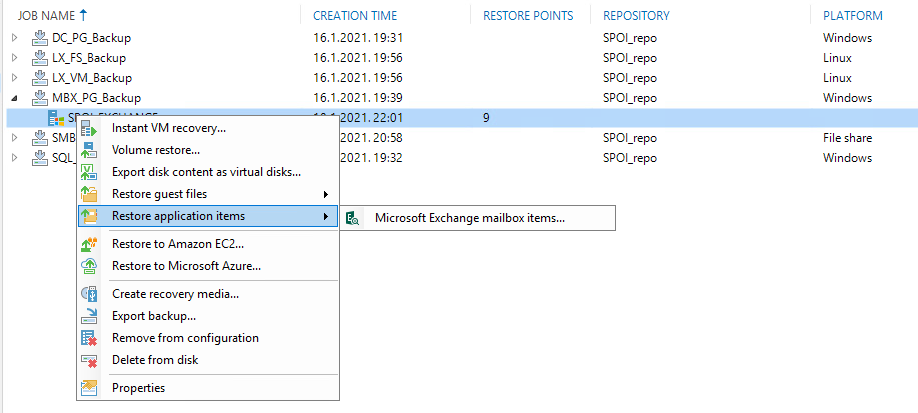


Slika 39 - Uspješan oporavak korisničke baze podataka

* 1. Oporavak mail-a

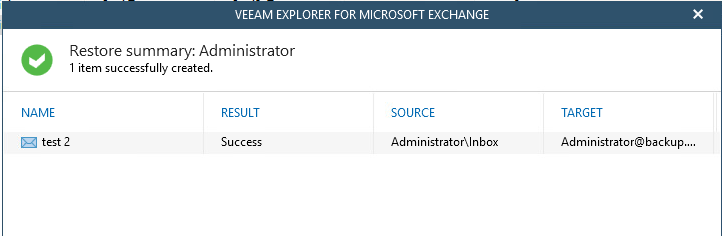
Kako bi testirali oporavak mail-a, pobrisat ćemo mail „test 2“ iz inbox-a administratora te ga vratiti kroz Veeam Explorer for Microsoft Exchange. Otvaramo job imena MBX\_PG\_Backup.

SPOI-MBX ( desni klik ) 🡪 Restore application items 🡪 Microsoft Exchange mailbox items…



Slika 40 - SPOI-EXCHANGE, Restore application items, Microsoft Exchange mailbox items

Otvara se Microsoft Exchange Mailbox Item Restore wizard, odabiremo zadnji restore point. Nakon završetka wizarda otvara se Veeam Explorer for Microsoft Exchange. Otvorimo mailbox bazu koja se kreirala te potražimo Administrator inbox, na njega pritisnemo desni klik i odaberemo „Restore to Administrator@backup.local“.



Slika 41 - Uspješan oporavak korisničkog mail-a

1. Preporuke za dodatnu konfiguraciju sustava

Izvedena konfiguracija sigurnosne pohrane i oporavka zadovoljava sve klijentske zahtjeve. Međutim, u budućnosti bi svakako trebalo nadograditi i bolje osigurati kompletni sustav sigurnosne pohrane kako bi se napravio bolje upotpunjen Disaster Recovery. Neke od preporuka za nadogradnju sustava su sljedeće:

* Konfigurirati na svakom od poslužitelja još barem po jedan dodatni mrežni adapter kako bi se postigla redundantna komunikacija između poslužitelja
* Dodati još dva storage poslužitelja kako bi se sigurnosne pohrane spremale na tri fizički odvojena poslužitelja, sljedeći pravilo 3-2-1
* Podaci bi se trebali nalaziti barem na 2 različita medija između ta 3 poslužitelja ( Disk + Tape )
* Konfigurirati backup copy i tape job-ove

1. Local Backup vs Cloud Backup

Idealni sustav pohrane podataka trebao bi biti lako dostupan. Sigurnosna pohrana podataka je nužna jer omogućava oporavak u slučaju gubitka podataka. Jako dugo vremena, trake i diskovi bili su prvi i najbolji izbor medija za pohranu. Danas, dolaskom cloud backup-a, opcije kreiranja strategija sigurnosne pohrane i oporavka su bezbrojne. Što točno onda znače local i cloud backup te kako odlučiti na koji način organizacija planira izvršavanje poslova sigurnosne pohrane?

Local Backup

Lokalni backup je dugovječniji oblik sigurnosne pohrane te se najčešće koristi na primarnoj lokaciji poslovanja. Za ovaj tip backup-a najčešće se koriste diskovi. U procesu backup-a još se koristi neki dana reduction softver poput onoga za deduplikaciju.

Traka je bila puno češći medij za sigurnosnu pohranu do ranih 2000.-ih. Koristi se i danas, najčešće za offline pospremanje kako bi se zaštitili od ransomware i sličnih tipova napada.

Cloud Backup

Cloud backup je novi oblik sigurnosne pohrane. To je postupak kojim kopiramo podatke preko mreže na neki off-site poslužitelj nekog service provider-a ( SP-a ). Cloud backup SP naplaćuje u skladu s uslugom koju isporučuje. To znači da cijena ovisi o karakteristikama sustava koji je korisniku potreban. U ovu računicu ulaze kapacitet, bandwidth, broj korisnika…

Cloud backup nam uvelike pomaže i olakšava postizanje 3-2-1 backup pravila. Podaci su off-site i medij se broji kao drugi medij za pohranu, drugačiji od tradicionalnog diska. Postoje i cloud-to-cloud backup planovi također.

Tablica uspoređuje lokalni i cloud backup.

Tablica 3 – Usporedba Local I Cloud Backup-a

|  |  |  |
| --- | --- | --- |
|  | **Local Backup** | **Cloud Backup** |
| **Troškovi usluge** | On-prem hardware, diskovi su skupi te ih treba mijenjati prije nego trake, ali pružaju bolje brzine. | Backup male količine podataka je jeftin, ali povećanjem opsega usluge, brzo poskupljuje i njena cijena. |
| **Skalabilnost** | Pri nadogradnji backup setup-a, treba biti svjestan količine prostora, novca i konfiguracije nadogradnje on-prem backup sustava | Cloud Backup-e je lako skalirati te nema nekog realnog limita mjesta za pohranu, ali također treba pripaziti na cijenu nadogradnje usluge |
| **Dostupnost** | On-prem hardware je lako dostupan jedino ako katastrofa nije zahvatila tu fizičku lokaciju. Brzine ovise o tipu medija. | Cloud Backup-i su laki za pristup pošto nam je za to potrebna samo Internet konekcija. Međutim, brzina prijenosa ovisi o kvaliteti te konekcije. |
| **Sigurnost** | Većina Local backup proizvoda ima sigurnosne featur-e. | U najboljim Cloud backup proizvodima koristi se end-to-end enkripcija. |
| Management | IT osoblje mora održavati backup sustav.  Neka poslovanja preferiraju da njihovi ljudi obavljaju taj posao. | Cloud Provider tipično održava sustav. Veoma korisno za korisnike koji nemaju potrebne ljudske resurse za obavljanje takivh zadataka. |

Local Backup

Prednosti:

**On-site dostupnost** – ovdje local backup sigurno ima prednost, jako jednostavan pristup podacima

**Brzina** – disk koji je on-site pruža najbolje brzine prijenosa

**Kontrola sigurnosti** – organizacija ima više kontrole nad podacima

Mane:

**Visoka inicijalna cijena** – puno skuplji za početi od nule

**Problemi sa skalabilnošću** – treba platiti zamjenu ili dodavanje dodatnih diskova, također, ako treba dodati još ormara treba imati mjesta

**Održavanje** – također treba platiti ljude koji će održavati i pregledavati sustav

**Problemi sa sigurnosti i Disaster Recovery procedurom** – ako ne postoji off-site backup = Single Point of Failure ( SPOF )

Cloud Backup

Prednosti:

**Low entry cost** – puno jeftinija za poslovanja koja ne mogu priuštiti off-site backup

**Laka skalabilnost** – kapacitet se poveća pomoću nekoliko klikova miša, dok bi na lokalnom storage-u morali dodati fizički disk

**Lak management** – u puno slučajeva management odrađuje SP uz konzultacije s korisnikom

**Jednostavan Distaster Recovery** – DRaaS omogućava dosta povoljniji Disaster Recovery nego što je on bio prije

Mane:

**Akumulacija troškova** – velika količina podataka tijekom dužeg vremenskog perioda uzrokuje postepeni porast troškova

**Latencija** – pošto korisnik ovisi o mrežnoj konekciji sa SP-om, nužno je da osigura nisku latenciju i dobar BW, kako on tako i SP

**Problemi sa sigurnosti** – jako je bitno da SP ima end-to-end ekripciju, ako su podaci u oblaku ne znači da su 100% sigurni

Nakon svega navedenog, kao zaključak je li bolji cloud ili lokalni backup, morat ću reći kako je najčešće najoptimalnije raditi neki hibridni plan sigurnosne pohrane i oporavka te tako izvući najbolje od jedne i druge strane te samim time na najbolji način osigurati podatke organizacije.

1. Zaključak

Implementacijom ovog projekta tvrtka X ima isplaniran i implementiran plan sigurnosne pohrane i oporavka svog IT sustava.

Isplanirane su i dokumentirane procedure za sigurnosnu pohranu i oporavak.

Poslužitelji se backup-iraju u grupama, prema svojim ulogama u korisničkoj infrastrukturi.

Sigurnosna pohrana pokreće se u redovnim intervalima kako bi se smanjila količina podataka

koji se mogu izgubiti.

Sigurnosna pohrana vrši se 2 puta dnevno za poslužitelje:

* SPOI-SDC
* SPOI-L1
* SPOI-L2

Sigurnosna pohrana vrši se 3 puta dnevno za poslužitelje:

* SPOI-SQL
* SPOI-EXCHANGE

Health-check backup datoteka za sve backup poslove vrši se svaki zadnji petak u mjesecu.

Za sve poslužitelje osim SPOI-L2 KVM Hosta, konfiguracijom poslova sigurnosne pohrane omogućen je item-level recovery pojedinih objekata sa poslužitelja.

Navedene su preporuke za dodatnu konfiguraciju sustava koje bi povisile dostupnost i poboljšale njegovu pouzdanost.

1. Reference

Learning Veeam Backup & Replication for VMware vSphere, Mohn, Christian, Packt Publishing Ltd., 2014

<https://helpcenter.veeam.com/docs/backup/vsphere/>

<https://helpcenter.veeam.com/docs/backup/em/>

<https://helpcenter.veeam.com/docs/backup/agents/>

<https://helpcenter.veeam.com/docs/backup/cloud/>

<https://helpcenter.veeam.com/docs/backup/cloud/cloud_overview.html?ver=100>

<https://www.disastersolutions.bz/cloud-backup-vs-local-backup/>

https://aisn.net/cloud-backup-vs-traditional-backup/

1. truncating – sprječava beskonačni rast transakcijskih logova [↑](#footnote-ref-1)
2. Prije izrade ovog poglavlja napravljen je snapshot virtualnih mašina imena „*Backupirano*“ [↑](#footnote-ref-2)