# IKT systemy - Windows

## Úvod virtualizácie

**Hypervisor** = softer code which is used for bare metal virtualization
**vHost** = virtualization host, physical computer with installed hypervisor
**VM** = virtual machine, is logical system with own guest OS running on vHost
**Uplink** = physical network adapter attached to vHost
**Datastore** = storage device used to store VMs, ISOS,..
**vCPU** = virtual CPU
**vRAM** = virtual RAM device of VM
**vDisk** = virtual HDD device of VM
**vNIC** = virtual NIC device of VM
**vSwitch** = virtual switch used by vNIC (left side) and Uplinks (right side)
**Appliance** = closed image (VM) with pre-installed guest OS and application

Virtualisation is technology, which allows to run multiple logical instances with own OS and Applications installed (VMs) on single or clustered physical.

**Pros:**

- System consolidation
- Hardware independent software
- High scalability and availability
- Better usage of hardware resources
- Lower costs of hosting, cooling, power supply
- Software based datacenter with central management
- Snaphshots (backup)

**Cons:**

- Higher investment
- Not all physical components can be connected to VM (special hardware no)
- Not all application can run on virtual platform

Virtualisation types - Bare metal (Type1) —> VM a hypervisor - Guest OS based
(Type 2) —> on ma virtualization SW a application az potom OP

Softer define datacenter - softverove riesenie

## Virtualisation - ESXi

**System Requirements (min)**

- 64 bit CPU dual core
- Intel or AMD Virtualisation tech. Enabled
- Data Execution Prevention (DEP), NX/XD bits enabled in BIOS
- 4 GD of Memory

NIC (1GB, 10GB, 40GB are supported) —> sietova karta

SLA —> pre zakaznika
OLA —> pre nas interne —> 1. Dostupnost, 2. Resolution time, 3. Reaction time

2 types: STANDARD
Needs to be configured per vHost
Not required VCS server for configuration

DISTRIBUTED
Required VCS server for configuration
Shared configuration across vHostgso

STORAGE VMware ESXi
**—> ESXi Hosts**
**—> Datastore Types** ( VMFS, NFS -> File systems )
**—> Storage Technologies** ( Direct attached, Fibre Channel -> optika, FCoE -> nieco medzi, iSCSI ->data posiekane po sieti , NAS-> storage box )

VM Files Vmware ESXi
**Configuration file .vmx / pri virtualke .vcm**
**Disk files .vmdk + -flat.vmdk .vhdx**
Bios file .nvram
Swap file .vswp
Snapshot files .vmsd (data) + .vmsn (state) + -delta.vmdk
Log file .log

# Installing and configuring: Hyper-V

**Hyper-Vserver**
Standalone product
is available for free

**Licensing Windows server**
Standar 2 OSEs
Datacenter unlimited OSEs

## Requirements vHost

**Hardware (min)**
64bit CPU with SLAT and support virtualisation tech
DEP enabled (XD or XN tech)
4 GB RAM
100 GB HDD
**Software**

Installed Windows server 2016 w Hyper-V feature or Hyper-V Server 2026

## Major/Core feature

**Production checkpoint**

Default option
Point in time image

**Standard Checkpoint**

Chose capturing SAVE state of VM
Usable for test, development, resistant APP

**Supported TECH**

1. iSCSI
2. FC
3. SMB 3.0 shares
4. Shared VHDX

**Supported partition format**

1. NTF
2. REFS

CSV musime vytvarat

**Software based layer 2 ethernet network switch**

**Traffic connectivity**

EXTERNAL
All communication outside
INTERNAL
Allow communication with VMs connection
PRIVATE
Same switch

**Limitations**

Needs to have at least one physical adapter
You cannot attache pNIC to multiple Switches
You can use VLAN taking

AVHDX
different
VMCX

**Naming convention** - pomenovanie podla toho na co sluzi
WS rc CPU - 2 —> Virtual WS CPU - 4

**OVERPROVISIONING** - 1GB:2 predavam nieco co nemam $ —> kapacitny monitoring

Disk provisioning - Thin provision —> postupne naplna storage, ked vymazeme vrati sa nam miesto
Thick provision —> rovno zaberie cely hard disk prázdnym miestom a ked vymazeme miesto sa nevrati

Ake typy workloadov moze byt na hyperv?

**Konfiguracne files** dalsi disk, zalohovanie, rychlost

Enhanced session policy policy -
Replication configuration - asynchronna

Generations

1. 32-bit pre stare systemy
2. 64-bit najnovsie generacie

**Dynamic memory** - vyuziva RAM naplno, prideluje sa mu RAM ako potrebuje a zvysok prideli inej AP = mozeme pridelit viacej Vm  8G ako mame RAM 4G

# AD DS - OWERVIEW

What are AD DS? - Active Directory, domain services
Why do company needs AD DS services - what are the benefits? Pre komfiguraciu
When do you need more than one domain? viacero dcerskych spolocnosti, test and production
Exist some relation with DNS? - domain naming, service location records, DCD, replication traffic, namespace consistency,
Forest vs Domain - spojenie viacerych domian - obsahuje v sebe klucove kontrolery 2
Administrators of forest/domain - prava vsade
Database and replication - v ramci domeny

## AD components

### Physical components

- **DC** | contains read-write copy of AD database
- **RODC** | special instance of DC with read-only database copy
- **Global catalogue** | special DC with host GC role which contains read

copy all objects in forests for speed up searching between domain
- Datastores | holds AD database Nods.dit and log files by default on all DC in C:\Windows\NTDS + Sysvol

**Logical components**

- **Domain** | security boundaries for users, computrrs, other objects
- **Domain tress** | collection of domains witch shares same root domain name and DNS namespaces
- **Site** | collection of object, defined by their physical location
- **Forest** | collection of domains witch share common AD DS
- **OU** | administrative object for group obj, delegate permission and applying GPOs
- **Containers** | same like OU, but it cannot be applying GPOs

```
Domena – domain admins –> prava na domene
Forest – enterprise admin –> maju prava vsade
```

## Post-dep-config

- Hostname
- DNS suffix
- IP (static)
- FS layout
- Local Users
- Softverovy firewalll
- Activation OS
- Domain Join
- Set TimeZone
- Set time

slmgr -xpr  —> na zistenie ci ze aktivovany system
slmgr -ato —> na aktivaciu systemu
cd \.  set-NetfirevallProfile - Enabled False -All
slmgr - ato
slmgr -rearm

Result set of policy -

192.168.118.18 -> moja IP

## DNS

- 3 domains (1 je root)
- Minimalne 2 musia nainstalovat ( s redudanciou 4)
- 2016 verzia priniesla nove ficurky - 2012 je stara verzia kde su vsetko domeny na jednej urovni a nie su tam fickurky
- Aspon 1 global controller

**Sposob obnovenia domain controller**
**Aut -** DC replikuje na existujuce -> ked chceme aby jeden prepisal ostatne
**Nout-** DC si zreplikuje z existujucich na seba -> pouzivame ak nam jeden vypadne, realne sa nepouziva

**NETBIOS NAME** zoberie prvych 15 znakov

Pri instalacii **promo controller** **je potrebny restart**
Na domain controllers sa nemozeme prihlasit ako normalny uzivatel ale ako admin

**V każdej domenę musi byt DNS a DC** - koli redunancii 4 (2 z kazdeho)
Aspon 2 foresty

VC.DUAL.SK-KOSICE.T-SYSTEMS.SK**.**

VC. - hostname
DUAL. - DNS
SK-KOSICE.
T-SYSTEMS.
SK. -
. - root

Inter replikacia - dnuka
Intra replikacie - vonku

**Geograficka poloha**
**Workload - test production**
**Administrativa - aby sme to nespravovali sami**

**Multi master mode** - DC funguju na <- z neho moze kontrolovat vsetky DC vo foreste —> musime mat zabezpecenu vysoku rychlost

**DSRM - f8** tlacitko -> zadat heslo -> cez comand

**Aky prikaz na restor potrebujeme? —>** ntdsutil

**Aky je rozdiel medzi kontainerom a OU**

**Prehladnost, administracia a ( aplikovat group polici ale iba na OU )**

**GP umoznuju nastavovat pasword polici, account polici , instalovat soubor .msi**

**Domain and trust** - na prepojenie dvoch domain trees—> ak chceme suport od

niekoho my ideme ku nemu takze zadavame cestu —> k nemu.

**Domain Site and servicer** - define SUB NET cez DC a hlada ho najprv u seba a potom inde cez IP adresu

**Active directory administrativ center** - nahradaza ciastocne zakladne ukony cez GUI
-> enable recycle bin

**Users and computers** - praca s objektami - kontajnery, OU

**TGT** - vytvara sa pri prihlasovani a ma tam informacie o pravach, groupe atd.

**SSO** - single site on —> vieme sa prihlasit cez mail

**Priradovanie viacej prav v domene US su komulativne - na kontrolu vsetkych sa kazdy dava do USERS**

**UG** — > pridelovanie opravneni
—> logicke zostupenie

**OU -** organisacion unit

## Powershell

**Zmenit meno a IP adresu -** DNS konci 10 a predtim 100 podla protokola

**C:\Widows\System32\....?**

**Group policy -** loral GP - computers settings, user settings
- domain GP

**Gpedit.msc**

**Windows settings - scripts - startup**
**- shutdown —>** pocas oboch mozeme dat nejakey skript
**- Security settings - account policies -** account lockout policy
- **Password policy** - kolko pismen atd.

Nektore politiky sa urobia po odhlaseni alebo po nejakom case (90 min) heslo, niektore az po reboot

**GROUPUPDATE | FORCE -** prejavia sa hend bez reboot

**GP result -** mozem si to vypracovat cez HTML

**Linkovanie novej policy mozeme na uzadi? -** child OU
- site
- domain
- OU

**Groupupdate -** aby som updatoval GP

**Ked mam viac policy ta mensia, spodnejsia vyhrava**

**Get-command** —> vypise vsetky mozne prikazi

## POWERSHELL

Objektovo orientovane
Zavisly .NET
Not case sensitive

### SYNTAX

Verb - Noun —> co? - s cim?
Parameter <value>
Get command - verb - noun

**VERB** - **NOUN**
**|> co chceme urobit?** **|> hladat cim?**

1. Get-localUser
2. Get-Volume
3. Get-Service
4. Get-Member - vypise vsetky mozne prikazy

Start-Transcript - Path C:\Temp\PowerSHell-Day2.txt —> zaznamenava logy co sa pise

Get-command Get Service —> Get-Service

### Ako pracovat s PS

1. Najst chdlet
2. HELP —> Get-Help (-ShowWindow) -Online

Get-service -name wuauserv , RpcEp...
Get-Host —> vypise verziu PS
WhatIf —> vypise co by sa stalo ak by sme pouzili konkretny command
Write-Host “I love PoweeShell with Dual members of APP group ”
-ForegroundColor Magenta
New-Variable —>

**PREMENNE**
$<NazovPremennej>
$Meno = "Stanislav"  - $Meno.GetType() —> na zistenie aky je to string
$Priezvisko = "Lukac"  -$Priezvisko | Get-Member —> ukaze metody
&Vek = 18  -Int32
$PSVersionTable

**ZADEFINOVANIE KODU CIM BUDE**
[int]$Vek = $null
[string]$Name = $null

PSP
-VAR
-ALIAS

## Praca s objektami

**command#1  | command#2**
**Musi mat vystup | musi vediet pracovat s vystupom**

**PLAN A - by value, musi dokazat s nimi pracovat**
**PLAN B - by property name**

Get-service -name wuauserv | stop-service -whatif

FILTROVANIE:

1. Krok —> Get-
2. Krok —> filtrovanie | select-object, where-object
3. Krok —> sort - object
4. Krok —> out | export

Bud jedno alebo druhe !

1. Krok —> format | format-list, format-table

Select-object —> dokace nam vyfiltrovat prvych alebo poslednych ….  Get-service | select-obj -last 2 | select onj - property -name, displayname | gm
Where-object —> vyfiltruje podla presnych parametrov… Get-Process | Where-Object {$_.CPU -gt 100}

Where-object—> na zaklade —> get-service | gm -membertype property
Get-service | where object {$_starttype}  —eq “automatic” } ) .count | where-object {$_status -ne “running”}

$_ -> plati na vsetky vystupy z lavej strany

Get-childitem -path C: | sort-object -prop length | select-object -first 5

Export-clixml —> dokaze pracovat s objektem, dokaze pracovat s polami
Export-Csv —> na ulozenie aby sme s tým potom vedeli dalej pracovat, zachovava member
Get-content —> nacitanie kontentu.. potom sa to meni na .txt (string), nedokaze nic

## PowerShell

SLUCKA FOR EACH
#foreach-object
#synatx: foreach ($obj in $objcoll) {<scriptCODE>}

```
$services = Get-Service

Foreach ($obj in $services) {
	write-hosts “services $obj.Name) has status $($obj.Status)”
}
```

#for
#syntax: for ($init; condition; $Ops_$I) { <code> }

```
For ($I = 0; $i -lt 5; $i++) {
	“[$I] Services $($services[$I].Name) has status $services[$I].Status”
}
```

#dowhile

```
$services = Get-Service
$i=0
Do
{
	write-hosts “[$I] Services $($services[$I].Name) has status $services[$I].Status”
	$I++
}
white ($i -lt 5)
```

#dountil

```
Do
{
		write-hosts “[$I] Services $($services[$I].Name) has status $services[$I].Status”
		$I++
}
until ($I -gt 4 )
```

#while

```
while ($x -lt 1)
{
        Write-Host “I hate PowerShell” -ForegroundColor Red
}
```

#Podmienovaci vyraz

```
If ($x -ee 99) {
    White-Host “[$I % complete] Analysing system, … please wait”
    $I++
}
elseif ( ) {
    codeB
}
else {
    codeC
}

SWITCH (R-premenna) {

X1    {codeA}
X2    {codeB}
Default    {code3}

}
```

## PS -layout

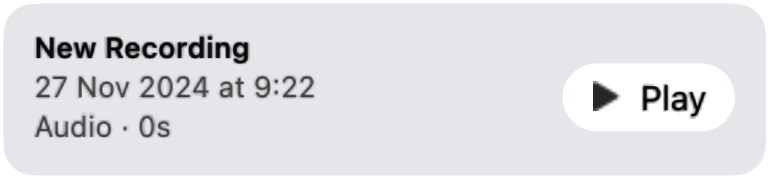
1. Capacity [GB]
2. Free space [%]
3. Free space [GB]

```
Get-volume | where-object {$_.Driveletter -ne $null} | select-object - property driveletter, Size*
```

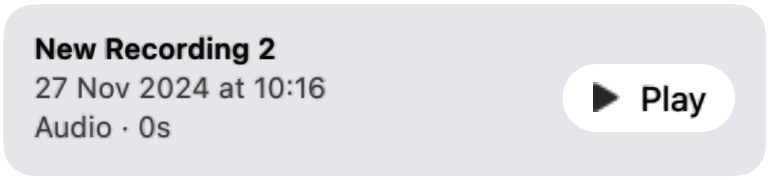
1. Get-volume | where-object {$_.Driveletter -ne $null} | select-object -property driveletter , @{name=“Capacity[GB]”; e={[math]::($_.Size/1Gb,2)}}
2. Get-volume | where-object {$_.Driveletter -ne $null} | select-object -property driveletter , @{name=“Freespace[%]”; e={[math]::(($_.SizeRemaining/$_.Size)*100,2)}}

3. Get-volume | where-object {$_.Driveletter -ne $null} | select-object -

property driveletter , @{name="Freespace[GB]"; e={[math]::
($_.SizeRemaining/1Gb,2)}}




CIM - celosvetovy standart —> pristup k info o hardvery alebo softvery —> powershell remouting 2 TCP porty
Port —> 5985
Ak ideme z vonku —> 5986
CIM-instance




One too many - invoke command —>
MTP session -

2025 - windows server

# VPN

**Protocol** - open VPN, ipsek (balik bezpecnostnych protocolov), autetifikacne protocoli,

**Open VPN** - Komunikacia s VPN serverom a VPN klientom, cez verejnu siet internetu, privatne pripojenie

**PAP** - pre developera ak skusaju nieco co nie je citlive, NEKONTROLUJE NAZACIATKU INFO O TOM KTO POSIELA

## Typy VPN

**Site to site** - prepojenie 2 a viacerych site
**Point to site** - pripojenie jednotlivcov do situ, vasinou nemaju dedikovane miesto

## Ake komponenty potrebujeme na POINT TO SITE

1.VPN server —>
2.VPN klient —-> inclu VPN tunel
3.DC
4.DHCP server (VPN samostatne moze mat dhcp v sebe a vie pridelovat ip adresy)

VPN server -> na neho sa pripaja klient cez internet
NPS - validacia ci ten kto sa pripaja ma up to date patche, ak nie prideli mu ip na, ktorej si doinstaluje patche a znova sa klient pripaja na NPS kde ho znova skontroluje a az po overeni ho pusta dalej do siete
DC
DHCP

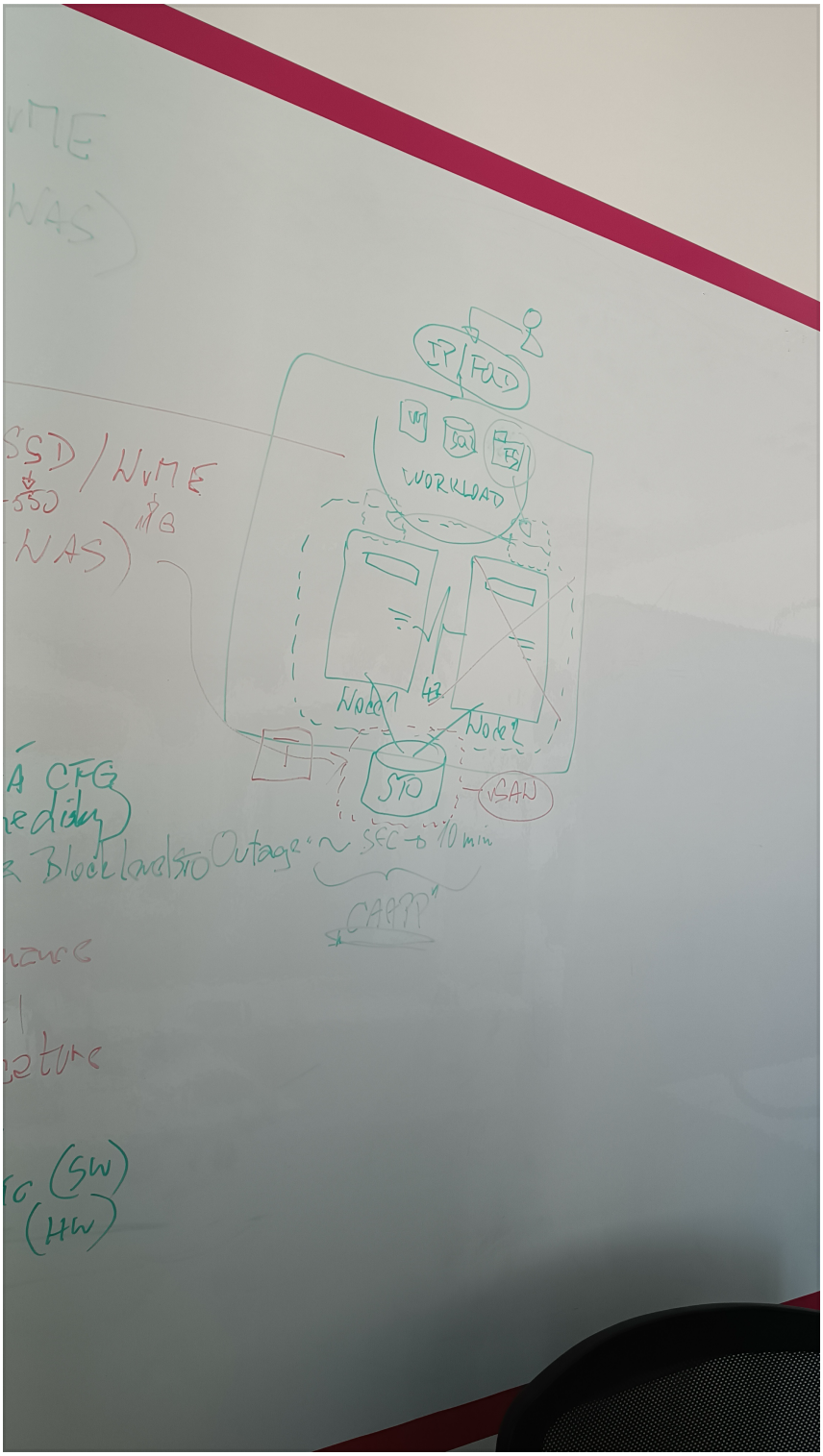
# WINDOWS SERVER STORAGE DOCUMENTATION

https://learn.microsoft.com/en-us/windows-server/storage/storage

Domace riesenia
- HDD / SSD / NvME
- Ext. NAS, synology
- Cloud

### Produkcia
- SAS (HDD) 15000 otacok, 24/7 / SSD / NvME
- Ext. SAN+NAS
- Cloud

Closet avare aplication




## ISCSI

**- ako keby nahradza 2. riesenie**

### VYHODY A NEVYHODY

1. Jednoducha konfig.
2. cena lokalny disk
3. Licence free, sucast windows servera and block level

- Rychlost / performance

- Kapacita
- Enterprise feature

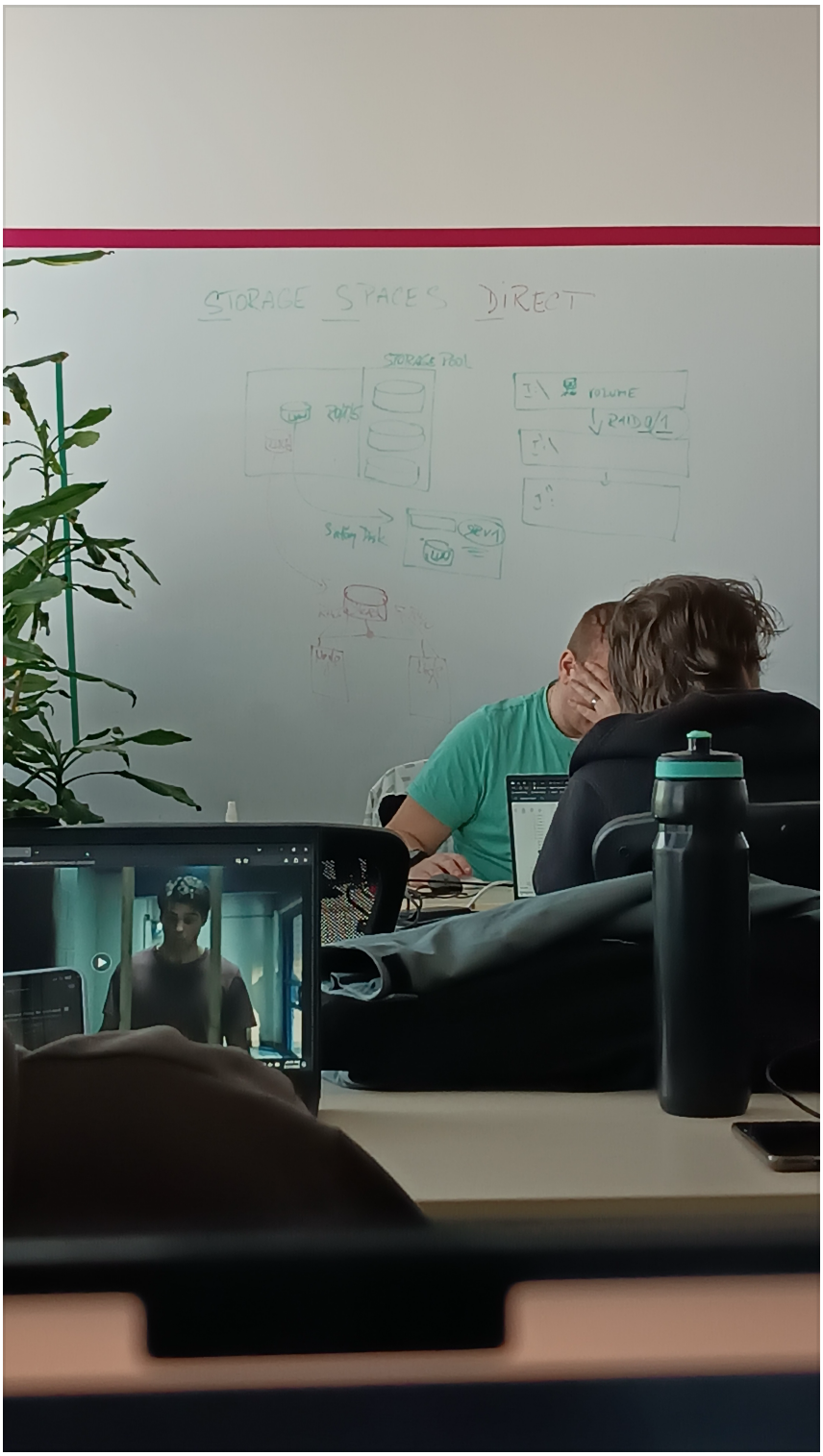
**REQUIRMENTS**

- Windows srv licencia
- Disk na, ktore sa budu ukladat data
- TCP IP - konekcia pre disky

I:/ volume —> raid 1 pre redundancy

## STORAGE SPACES

Storage pool —> disky su sucastou jedneho poolu kde mozu byt raidy 0/1/5. —> to cele sa pripaja ako sietovy disk




DFS - X —> DFS - N (centralne spravovanie), SMB shares Access Point

DFS - N -> logic groups kde je UNC Parth pre uzivatela. \\ 1 IP/FQDN \ 1 nameSMD
DFS - R -> replikuje SNB shares  1. HA without clu
2. Btw branch-offices
3. Central replication to sites
4. Easy management

# Klaster

Stav
- active/active
- active/passiv

Requirements :

Preco chceme mat 2 klastrovane serveri. Nod A/ nod B

Failover klaster
1. No single point of failure
2. Utilisation
3. Aby sme vedeli kde je kotra aplikacia

Witeness -> LUN from storage box (1GB)
SMB share
Azure storage account
Len aby mal 1 hlas , pri pade 1 klastra aby bol stav 2/3 a nie 1/2, vzdy je iba jeden ale more byt zdielany medzi klastre.

NLB klaster (network load balancer)
- pre webove aplikacie, autefikacne servre

Potrebujeme rozlozit load aby nespadli servere od zataženia od pouzivatelov
Max 32