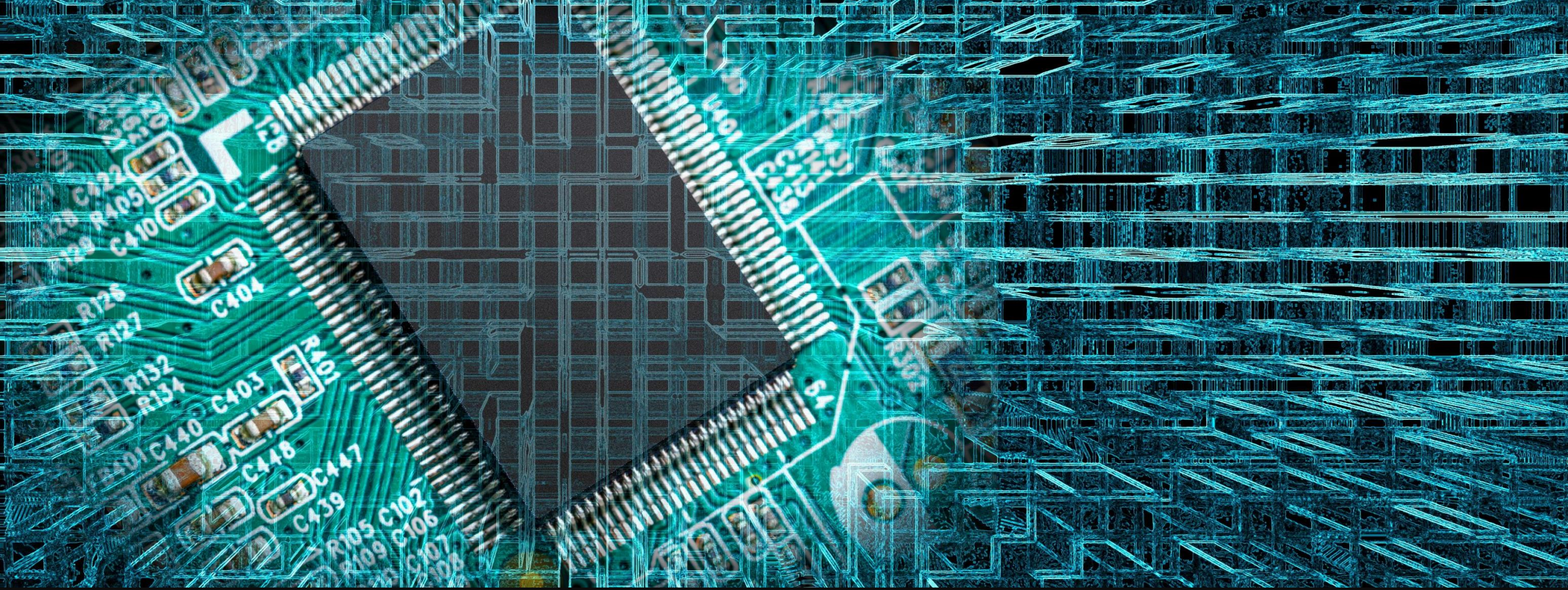




Ako na zálohu a obnovu doménových radičov

Mgr. Michal Dobšovič

MCP | MCSA | MCTS | MCT

whoami

- Trainer @ IT LEARNING SLOVAKIA
- Day-to-day experience:
 - IT LEARNING SLOVAKIA
 - ~ 100 workstations
 - ~ 20 servers (MS, Linux)
 - Ext. site admin & IT staff coach @ Chipita
 - > 10 000 employees, 18 sites
 - IT Administrator @ Nalgoo
 - ~ 20 servers (MS, Linux)
- Admin experience:
 - Windows Server 2003 - 2016
 - Exchange Server 2010 - 2016
 - SQL Server 2005 - 2016
 - Office 365 & Azure
 - Linux (Debian, Ubuntu Server, RHEL)
 - Zabbix

Microsoft
CERTIFIED
Professional

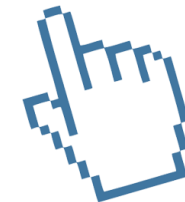
Microsoft
CERTIFIED
Solutions Associate

Windows Server 2012

Microsoft
CERTIFIED
Systems Administrator

Windows Server 2003

Microsoft
CERTIFIED
Trainer



IT LEARNING
SLOVAKIA
AKREDITOVANÉ POČÍTAČOVÉ KURZY
SKOLENIA A IT SEMINÁRE

Prečo sme dnes tu?

1

Prerequisites

- Replikácia AD DS
- FSMO roles

2

Záloha AD DS

- Prečo?
- Ako?
- Kedy?

3

Obnova zo zálohy

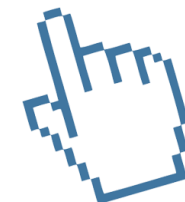
- Ako nie?
- Ako áno?

4

Čo ak DC náhle odíde?

5

Vaše otázky a diskusia



1. Prerequisites

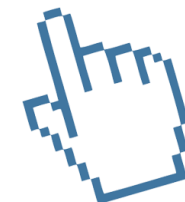
Replikácia AD DS

- Proces synchronizácie dát, prináša dáta bližšie k užívateľovi
- Slúži na zabezpečenie HA (High Availability)
- Replikácia v AD je tzv. multi-master
- 5 FSMO rolí
 - Schema Master
 - Domain Naming Master
 - Infrastructure Master
 - PDC Emulator
 - RID Master



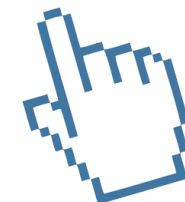
Schema master

- Jediný DC vo foreste, kt. môže zapisovať do AD Schema
- LDAP://CN=Schema,CN=configuration,DC= <root-domain>
- Zmena Forest Functional Level



Domain Naming Master

- Jediný DC vo foreste, kt. je zodpovedný za správu domain namespace
- LDAP://CN=Partitions, CN=Configuration, DC= <root-domain>
- Jediný DC, ktorý môže pridávať/odoberať doménu



Infrastructure Master

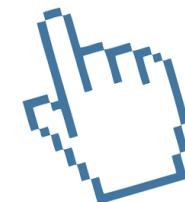
- Zabezpečuje cross-domain reference
- Napr. užívateľ je členom skupiny v inej doméne
- Keď zmažeme užívateľa, IM zabezpečí jeho zmazanie zo skupiny v inej



Infrastructure master by nemal byť nainštalovaný na Global Catalog serveri, pokiaľ všetky DC zároveň nie sú aj GC.



Ak je povolený AD Recycle Bin (FFL $\geq$ 2008 R2), každé DC si aktualizuje svoje cross-domain references, ak objekt presúva, premenováva alebo maže. V takom prípade sa Infrastructure master vôbec nepoužíva a je jedno, na ktorom DC sa nachádza.



RID Master

- Jedný DC v doméne zodpovedný za pridelovanie RID poolov pre jednotlivé DC v doméne
- SID objektu = jednoznačný identifikátor objektu v rámci forestu
- SID objektu = SID domény + RID

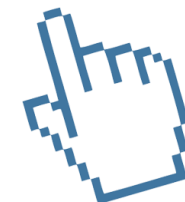


PDC Emulator

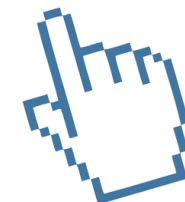
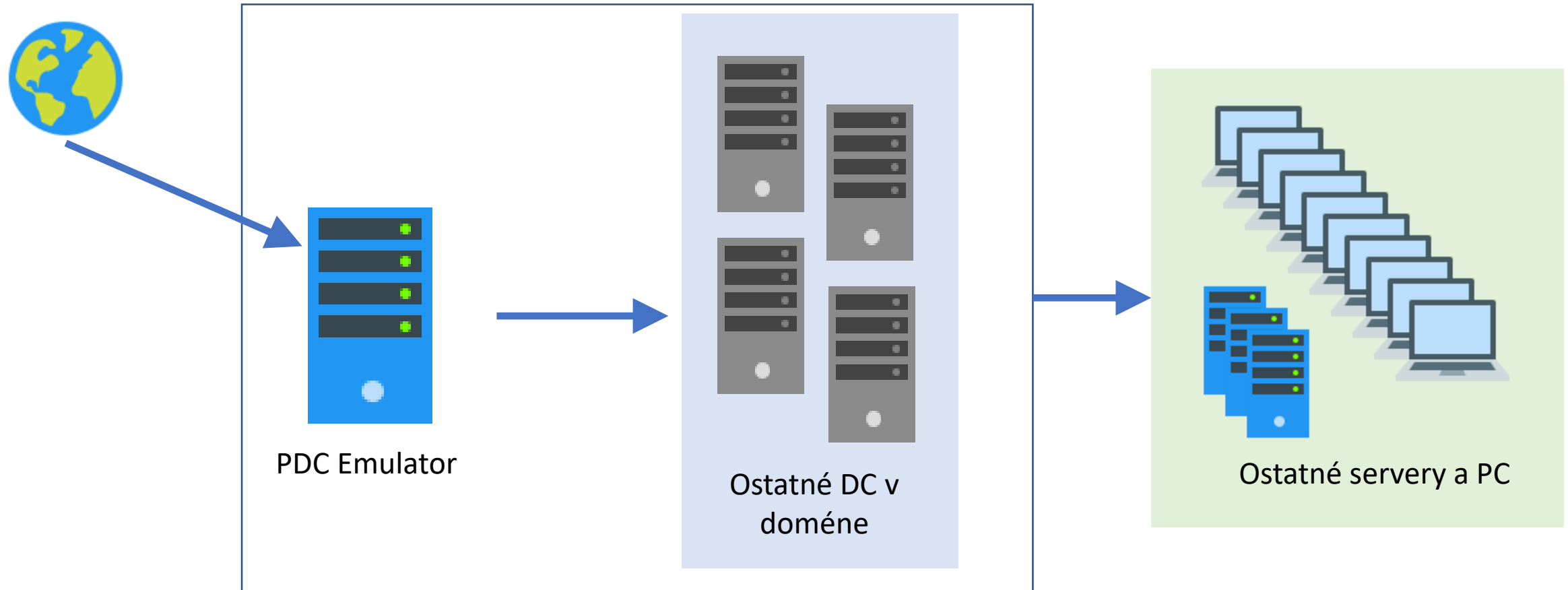
- Veľmi dôležitý DC, pretože ho veľmi často využívajú klientske stanice
- Synchronizácia času
- Zmena hesla
- Account Lockout



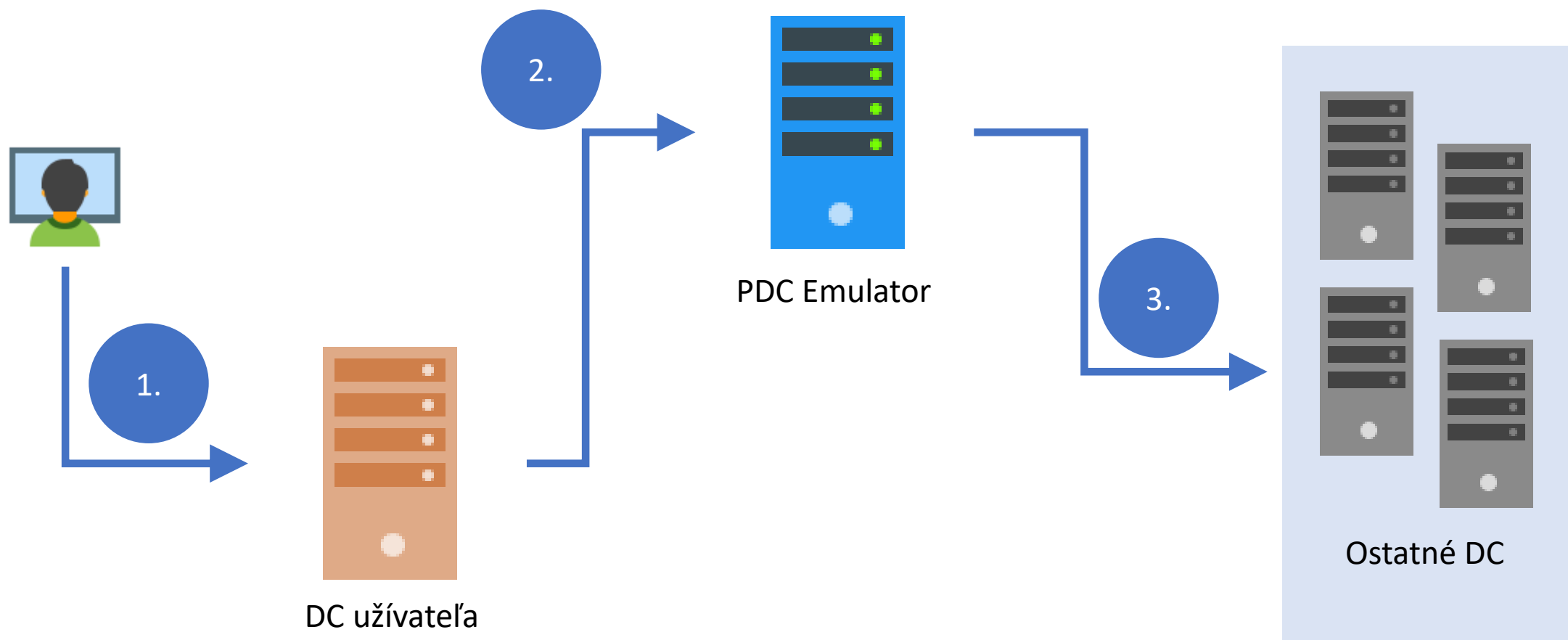
História: PDC Emulator vykonával všetky role primárneho DC v prostredí Windows NT 4.0 (toto zaniklo s upgradom na Windows 2000)



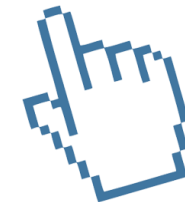
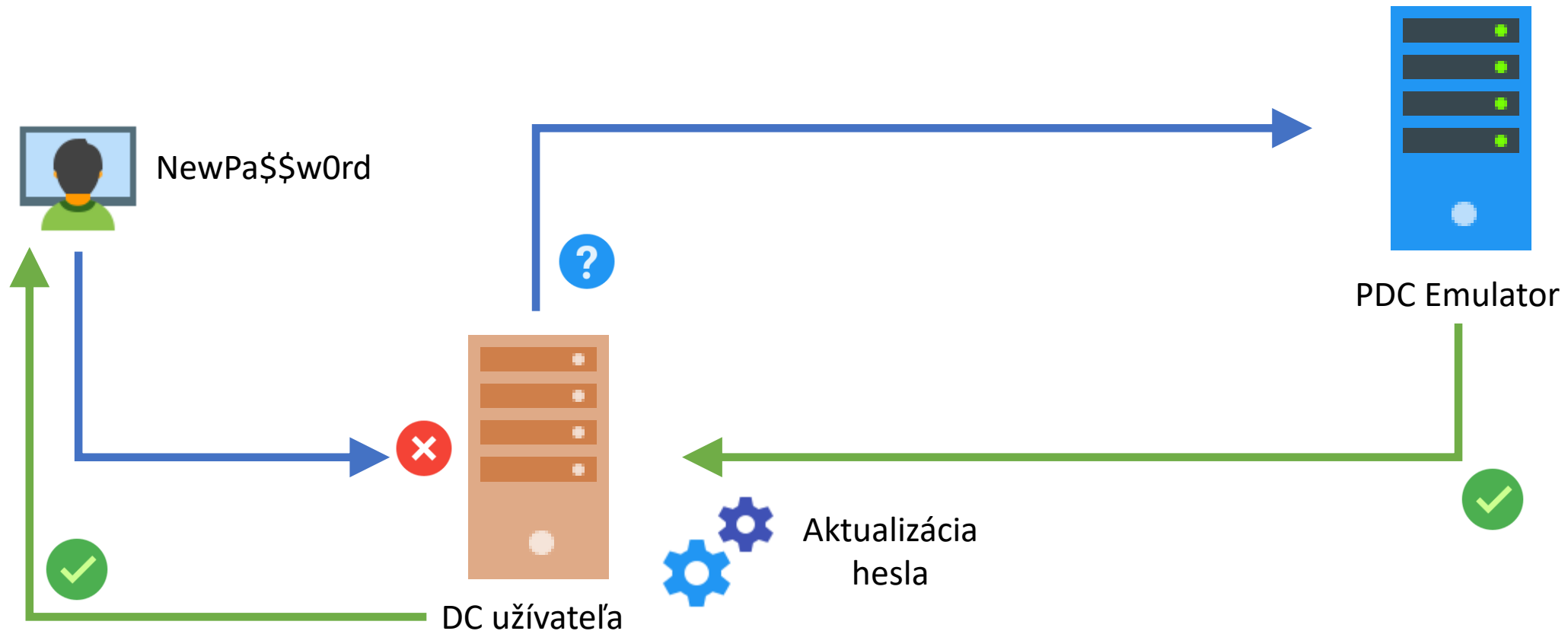
PDC Emulator – synchronizácia času



PDC Emulator – zmena hesla



PDC Emulator – prihlásenie po zmene hesla



2. Záloha AD DS

C:\Windows\NTDS

Súbor	Význam
Ntds.dit	Databáza AD DS
Edb.log	Transakčný log k databáze (10 MB)
EdbXXXXX.log	Doplnkové transakčné logy (á 10 MB), iba ak sa zaplní Edb.log
Edb.chk	Checkpoint súbor pre transakčný log
Res1.log Res2.log	Ich úlohou je rezervovať voľné miesto na disku pre transakčný log
Temp.edb	Dočasné úložisko pre rôzne operácie v AD DS databáze a logu



Ako nezálohovať?

- Nekopírovať súbory „zaživa“
- Ani pomocou Volume Shadow Copy
- Ani pri vypnutej službe AD DS
- Nepoužívať exotické zálohovacie nástroje
- DC je najdôležitejší server v sieti, tak mu doprajme patričnú úctu ☺

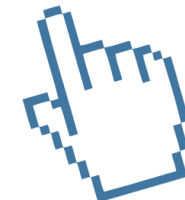


Because you **could**,
it doesn't mean
you **should**!



Ako teda zálohovať?

- Windows Server Backup
 - Bezplatný nástroj – súčasť Windows Server
 - Treba doinštalovať ako Feature
`PS> Install-WindowsFeature Windows-Server-Backup`
- System Center Data Protection Manager
 - Platený nástroj
- Azure Backup Server
 - Bezplatný nástroj, k dispozícii iba pre Azure užívateľov
 - Vychádza z DPM
- Third-party backup software
 - Musí vedieť zálohovať System state, resp. byť Active Directory-aware



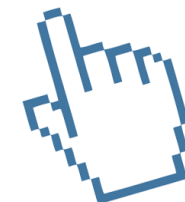
DEMO – Windows Server Backup

- Inštalácia
- Typy záloh
- Konfigurácia jednorazovej vs. plánovanej zálohy



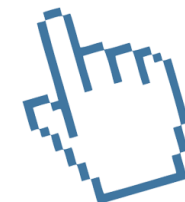
Kedy zálohovať?

- „Vždy po tom, ako sa v databáze vykoná nejaká dôležitá zmena“
- V databáze AD sa dejú dôležité zmeny prakticky neustále
 - Zmena hesla užívateľa
 - Zmena hesla počítača
 - Pridanie / Úprava účtu
 - MS Exchange tiež pracuje s AD databázou
 - A možno aj iný software...
- RPO – Recovery Point Objective
- RTO – Recovery Time Objective



Ktoré DC zálohovať?

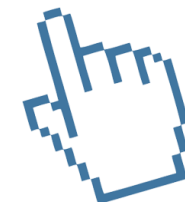
- Netreba všetky – databáza na nich je predsa rovnaká (replikácia)
- Je dobré mať zálohu
 - DC s FSMO rolami
 - Global Catalog Server
 - Ľubovoľný writable DC
 - Ak používate RODC, tieto netreba zálohovať vôbec



Odporúčania

- Zálohujte aspoň jeden DC
- Zálohujte aj po zmene v Exchange Serveri
 - Pridanie nového servera, presun užívateľov, nastavenie Mailbox databáz
- Zálohujte pravidelne
 - Stará záloha sa nemusí dať obnoviť!
- Majte Disaster Recovery Plan
 - Proces, ktorý definuje, ako sa zálohujú a obnovujú jednotlivé služby (nielen AD DS)
- Overte si, či záloha funguje – či je čitateľná a použiteľná
 - Obnova do iného umiestnenia a skontrolovať súbory
- Zapnite AD Recycle Bin
 - nebudete musieť obnovovať DC zo zálohy kvôli omylom zmazanému kontu

Na DC nemajte iné
role, ako AD DS!



PowerShell náš každodenný...

```
Install-WindowsFeature Windows-Server-Backup `
    -IncludeAllSubfeature -IncludeManagementTools
```

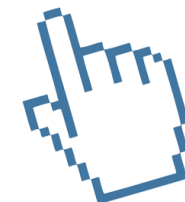
```
$policy = New-WBPolicy
```

```
Add-WBSystemState -Policy $policy
```

```
$target = New-WBBackupTarget -VolumePath "D:"
```

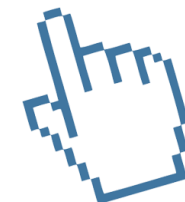
```
Add-WBBackupTarget -Policy $policy -Target $target
```

```
Start-WBBackup -Policy $policy
```



DEMO – Záloha DC

- Najprv vygenerujeme nejaké zmeny...
- Zmeny zreplikujeme na ostatné DC
- Jeden DC zazálohujeme



Prestávka...

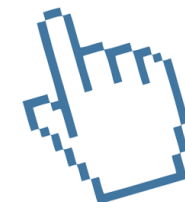
3. Obnova zo zálohy

Úvod do obnovy AD DS

- „Re-create the failed domain controller and populate its copy of Active Directory through replication from the unaffected domain controllers in your organization, **instead of restoring your data from a backup.**”
- „Neobnovujte zlyhaný DC zo zálohy, ale urobte čistú inštaláciu a nechajte AD DS, aby nareplikovalo všetky potrebné zmeny.”
- Non-authoritative restore
- Authoritative restore

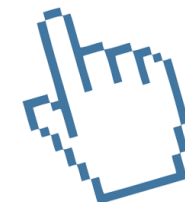


Nie je možné obnoviť zálohu staršiu ako tombstoneLifetime



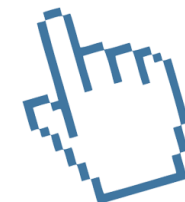
Postup obnovy zo zálohy – Non-authoritative

1. Naštartovať DC v Directory Services Restore Mode (DSRM)
2. Zadať heslo DSRM účtu
3. Spustiť Windows Server Backup
4. Obnoviť System state
5. Reštartovať DC do normálnej prevádzky



DEMO: Reset DSRM Password

1. `ntdsutil`
2. `set dsrm password`
3. `reset password on server {null | SERVERNAME}`
4. `q`
5. `q`

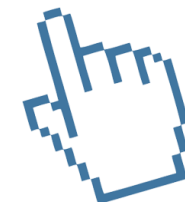


Tombstone lifetime

- Čas od zmazania objektu po jeho odstránenie z databázy AD DS
- Aby ostatné DC mali čas nareplikovať si info, že objekt bol zmazaný

CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=DomainName

- WS2003: 60 days; $\geq$ WS2003SP1: 180 days



Postup obnovy zo zálohy – Authoritative

1. Naštartovať DC v Directory Services Restore Mode (DSRM)
2. Zadať heslo DSRM účtu
3. Spustiť Windows Server Backup
4. Obnoviť System state
5. Označiť objekty, na ktorých sa má vykonať authoritative restore
6. Reštartovať DC do normálnej prevádzky
7. Spustiť LDIFDE



4. Čo ak DC odíde?

Scenár

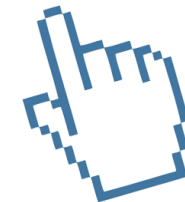
- Zhorel hardware, bol zmazaný disk, niekto skúšal a doskúšal, ...
- Predpokladáme, že takto odídený DC **nebudeme obnovovať** zo zálohy
- Metadáta o starom DC musíme z domény zmazať
- Predpoklad: V doméne je aspoň jeden funkčný **writable** DC

Nikdy nemažte DC tak, že ho iba sformátujete!



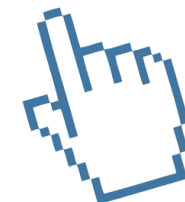
Čo opraviť?

- Odstrániť konto DC v doméne
- FSMO roles
- Replikácia
- Metadáta
- Konfiguráciu klientov (PC & ostatné servery)



Odstránenie konta DC

- Active Directory Users and Computers
- OU Domain Controllers
- Zmazať konto DC – pozor, zmazať **správne** konto 😊
- Potvrdiť, že ho naozaj chceme zmazať
- Potvrdiť, že ho naozaj chceme zmazať
- Ak DC mal FSMO role, bude možné ich presunúť na iný DC (seize)



Oprava replikácie

- Active Directory Sites and Services
- Vybrať Site, v ktorej bol DC
- Rozkliknúť Servers a zmazať správny server



Odstránenie metadát

```
ntdsutil
```

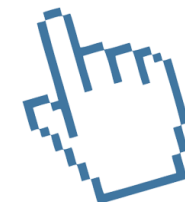
```
metadata cleanup
```

```
remove selected server NAZOVDC
```

```
Yes
```

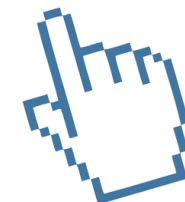
```
quit
```

```
quit
```



Konfigurácia klientov

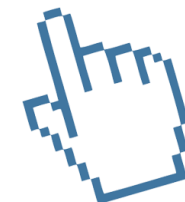
- DHCP konfigurácia (DNS Server)
- Statické DNS
- Clear DNS Client Cache
 - `ipconfig /flushdns`
 - Efektívnejšie je reštartovať PC



Otázky?

Kurzy v IT LEARNING SLOVAKIA

- www.itlearning.sk
- Microsoft Windows Server 2012/2016 - Active Directory základný kurz
 - 18. - 20. 10. 2017
- Microsoft Windows Server 2012/2016 - Active Directory pokročilý kurz a cloud computing
 - 25. - 27. 10. 2017
- MOC 20742 – Windows Server 2016 - správa účtov Active Directory, Group Policy, ADFS, ADCS, ADRMS
 - od 04. 12. 2017
 - Microsoft Official Course (5 dní)





Ďakujem za
pozornosť

Mgr. Michal Dobšovič

dobsovic@itlearning.sk

<https://dobsovic.itlearning.sk>