Active Directory Domain Services

Windows Server

FUTURE-PROOF

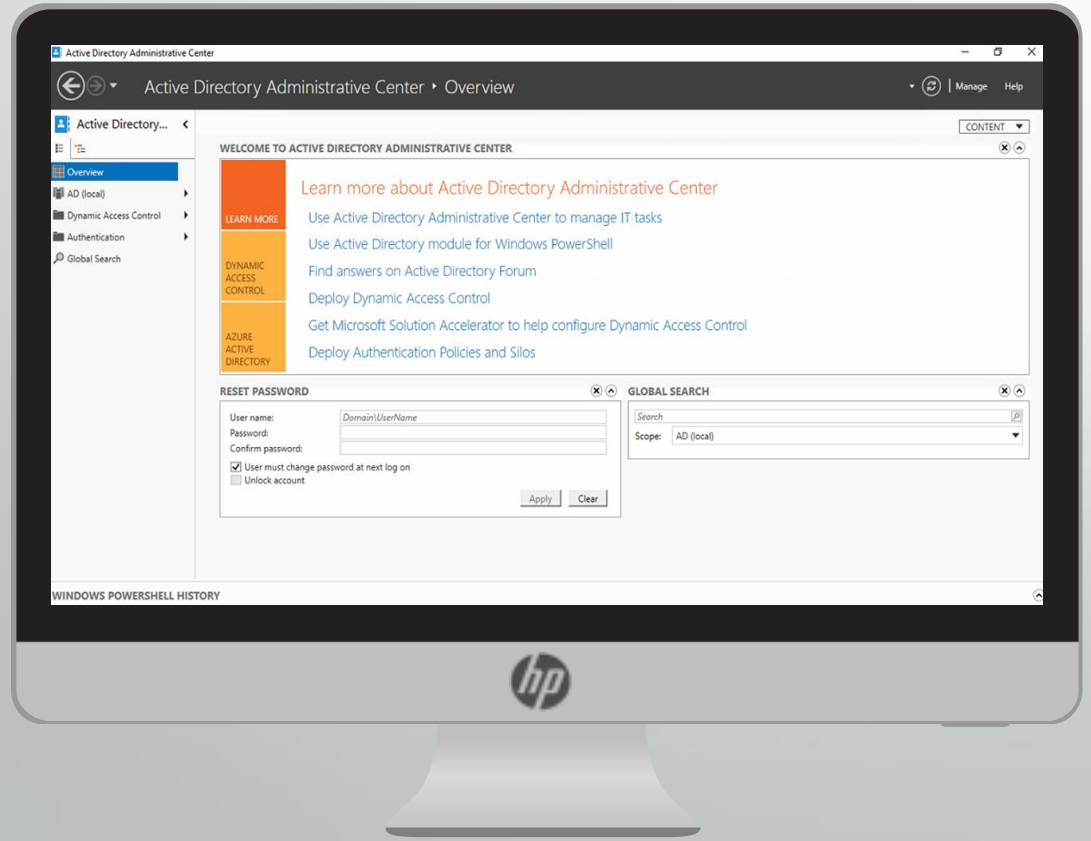
PEOPLE-CENTRIC

- Active Directory Administrative Center
- Active Directory Recycle Bin
- Read-Only Domain Controller
- Cloning Domain Controllers
- FSMO
- Active Directory maintenance

Active Directory Administrative Center

FUTURE-PROOF

PEOPLE-CENTRIC



= Console voor beheer AD-objecten

= Opvolger van ADUC

→ Gebouwd op Windows Powershell

Active Directory Administrative Center

FUTURE-PROOF

PEOPLE-CENTRIC

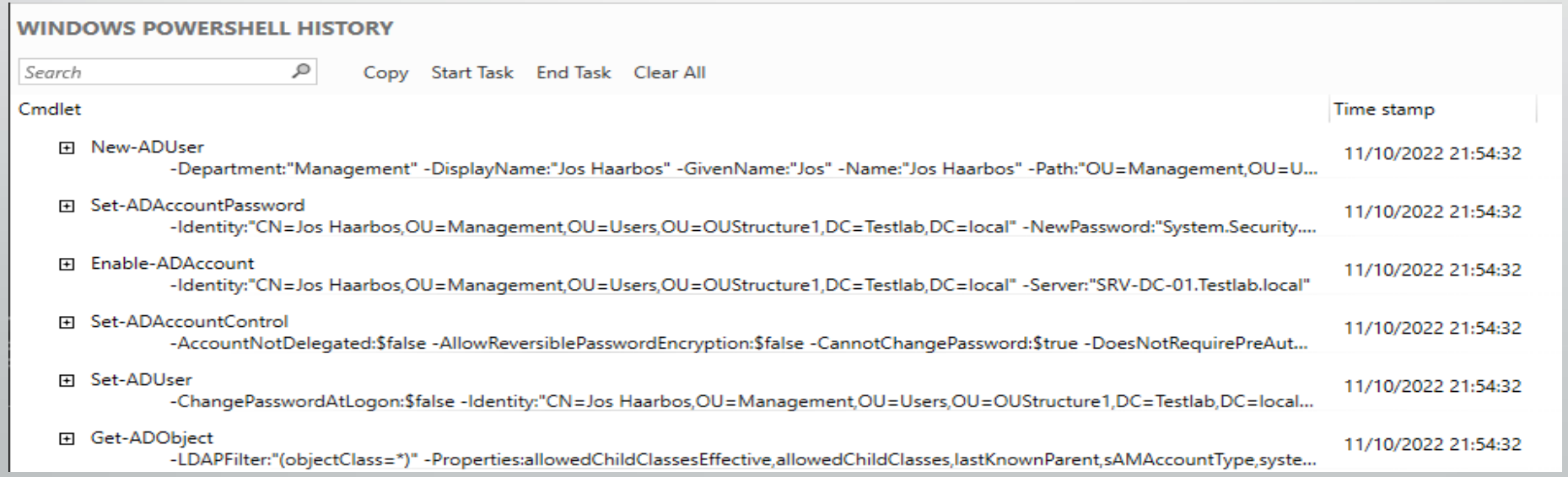
- Bepaalde verbeteringen t.o.v. Active Directory Users & Computers
  - ✓ Betere filteropties
  - ✓ Gemakkelijker queries voor AD configureren
  - ✓ Algemene tool password reset
  - ✓ Nieuwe features komen enkel uit op ADAC

Active Directory Administrative Center

FUTURE-PROOF

PEOPLE-CENTRIC

- Nieuwe feature in ADAC = Powershell History



Active Directory Recycle Bin

FUTURE-PROOF

PEOPLE-CENTRIC

- Object verwijderen in AD
  - ⇒ Niet permanent verwijderd
  - ⇒ Kan nog teruggezet worden
- Geen Recycle Bin aanwezig…
  - ⇒ Back-up is enige oplossing !

Eens ingeschakeld kan het niet meer uitgeschakeld worden

Active Directory Recycle Bin

FUTURE-PROOF

PEOPLE-CENTRIC

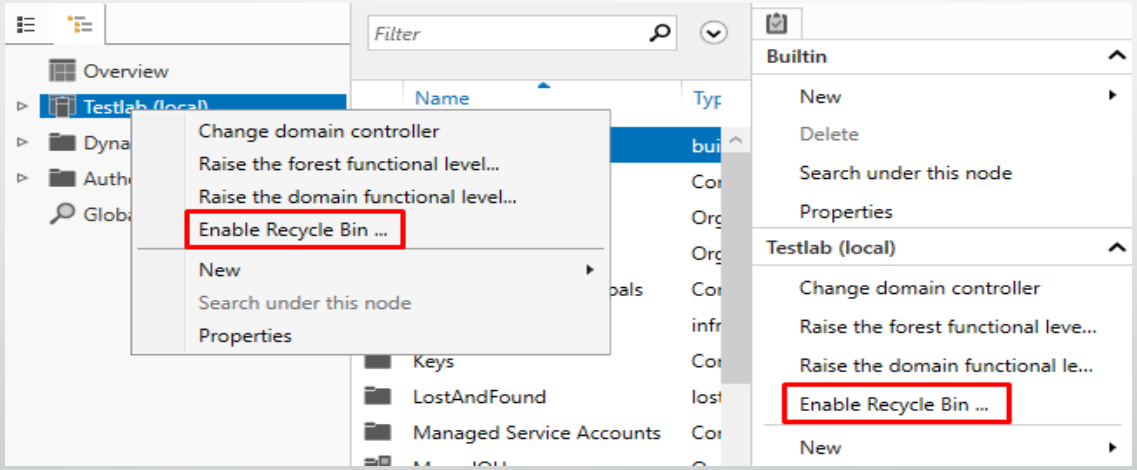
- Vereisten
  - ✓ OS = Windows Server 2008 R2 of later
  - ✓ Forest Functional Level = Minimum Windows Server 2008 R2 Mode
- Inschakelen via Powershell

Recycle Bin

```
Enable-ADOptionalFeature –Identity “Recycle Bin Feature”
–Scope ForestConfigurationSet –Target “<domain name>”
```

Active Directory Recycle Bin

- Inschakelen via ADAC



AD Recycle Bin step-by-step guide

FUTURE-PROOF

PEOPLE-CENTRIC

FUTURE-PROOF

PEOPLE-CENTRIC

- [x] LAB – Recycle Bin

Labs – Active Directory

Read-Only Domain Controller

FUTURE-PROOF

PEOPLE-CENTRIC

= Domain Controller in Read-Only modus

Standaard DC
=
Writable

Specifiek ontworpen voor branch offices

- ✓ Weinig personeel
- ✓ Geen IT-medewerkers aanwezig
- ✓ Meestal slechte fysieke beveiliging
- ✓ Netwerkbandbreedte minder goed

Read-Only Domain Controller

FUTURE-PROOF

PEOPLE-CENTRIC

Vereisten

- ✓ Forest Functional Level = Minstens Windows Server 2003
- ✓ Minstens 1 DC met Windows 2008 of hoger
- ✓ OS van RODC = Windows Server 2008 of hoger

Voor “Prepopulate Passwords” moet FFL minstens Windows Server 2008 zijn

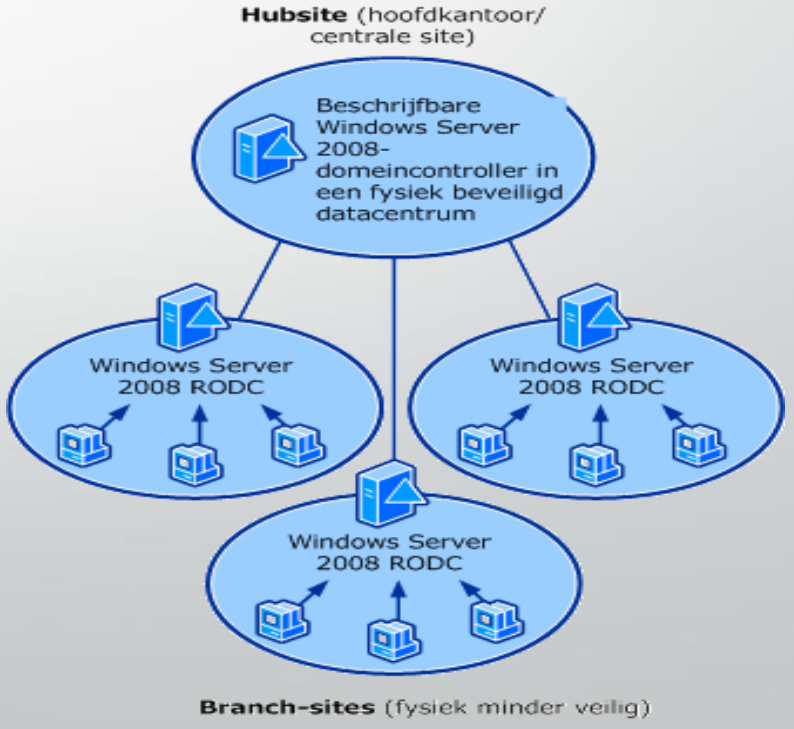
Read-Only Domain Controller

FUTURE-PROOF

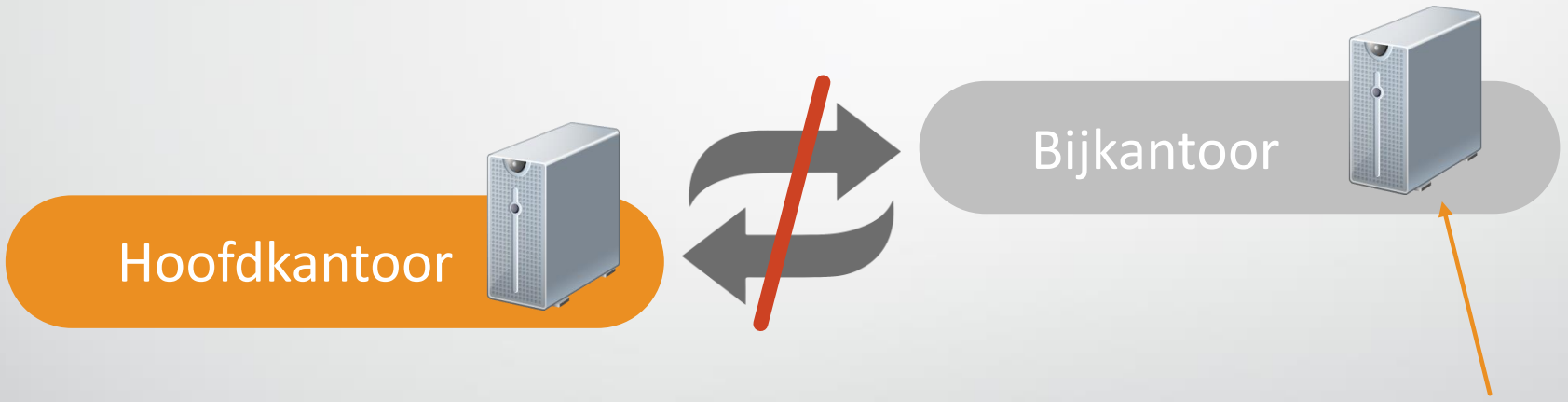
PEOPLE-CENTRIC

Prepopulate Passwords

- ✓ Wachtwoorden van gebruikers en computers die werkzaam zijn in branch office ‘cachen’
- ✓ Bepalen van wie wachtwoorden moeten bewaard worden
  - ◊ Allowed RODC Password Replication Group
  - ◊ Denied RODC Password Replication Group



Read-Only Domain Controller



Alle computers en gebruikers authenticeren naar RODC

⇒ Prepopulate Passwords is vereist !!

✓ DNS-zone is ook Read-Only op RODC !!

FUTURE-PROOF

PEOPLE-CENTRIC

FUTURE-PROOF

PEOPLE-CENTRIC

- [x] LAB – S2SVPN
- [x] LAB – RODC

talentlms

Labs – Networking

Labs – Active Directory

Domain Controller Cloning

FUTURE-PROOF

PEOPLE-CENTRIC

= Klonen van gevirtualiseerde DC's

→ Redenen

- ✓ Snelle uitrol van extra DC
- ✓ Snelle restore bij disaster recovery
- ✓ Verbetering uitbreiding bij private cloud
- ✓ Testlabs (situatie dezelfde als productie)

Domain Controller Cloning

FUTURE-PROOF

PEOPLE-CENTRIC

Vereisten

- ✓ Hyper-V moet VM-GenerationID ondersteunen
- ✓ DC moet minstens Windows Server 2012 of hoger zijn
- ✓ PDC Emulator moet online zijn en minstens Windows Server 2012
- ✓ Source DC moet lid zijn van groep “Cloneable Domain Controllers”

Domain Controller Cloning

FUTURE-PROOF

PEOPLE-CENTRIC

- DC Cloning
- DC Cloning step-by-step
- ADDS Virtualization

FSMO Roles

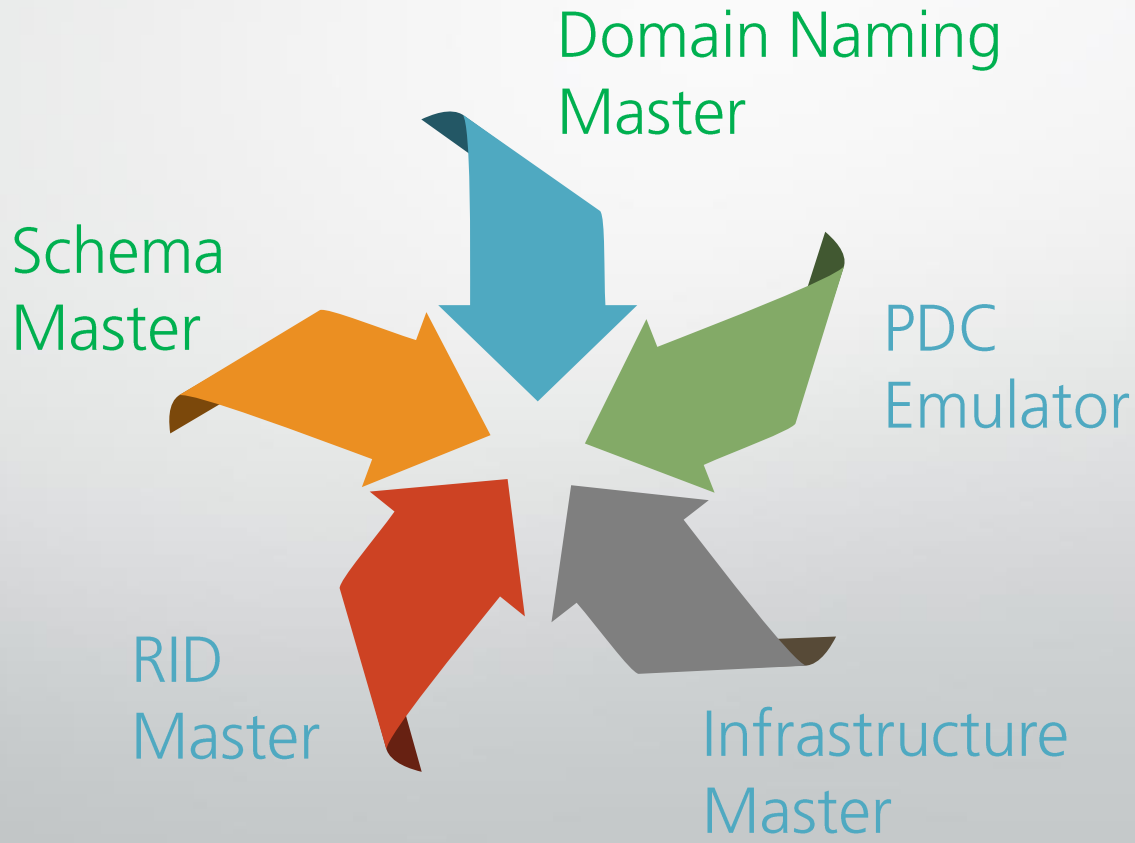
FUTURE-PROOF

PEOPLE-CENTRIC

= Flexible Single Master Operation

- Bepalen welke DC's "baas" zijn in een domein of forest
- 5 operation masters in AD forest ⇒ Multimaster Model
  - ✓ 2 operation masters op FOREST level
  - ✓ 3 operation masters op DOMAIN level

FSMO Roles



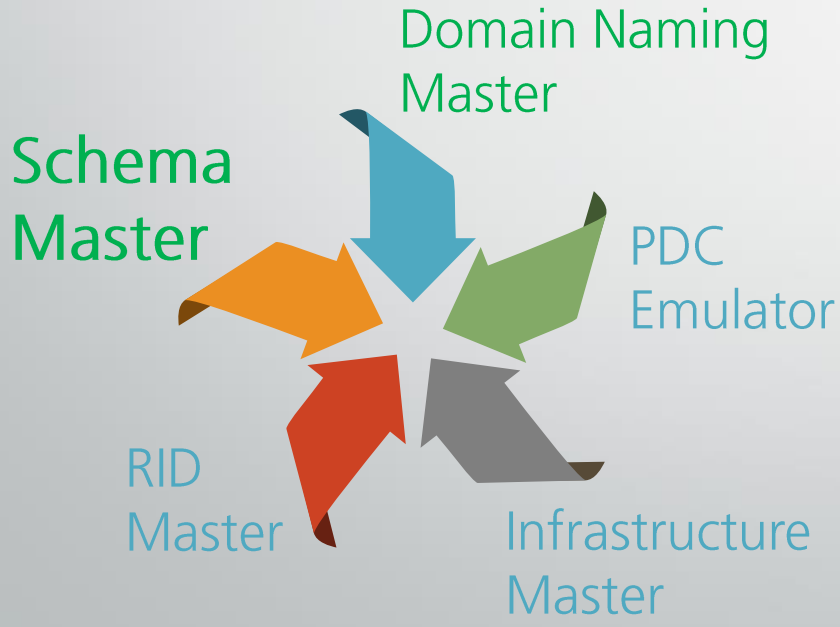
FUTURE-PROOF

PEOPLE-CENTRIC

FSMO Roles

FUTURE-PROOF

PEOPLE-CENTRIC



- Beschrijft het “uiterlijk” van alle objecten in AD
- Bepaalt welke attributen object heeft
- Aanpassingen vaak door software

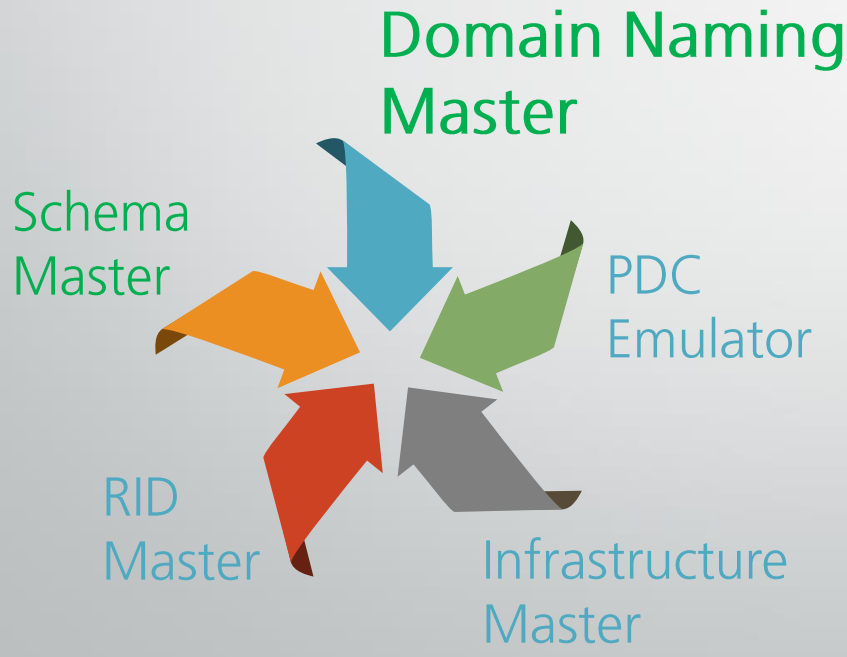
Bvb. Installatie van Exchange

⇒ Bepaalde attributen user object aangepast

FSMO Roles

FUTURE-PROOF

PEOPLE-CENTRIC

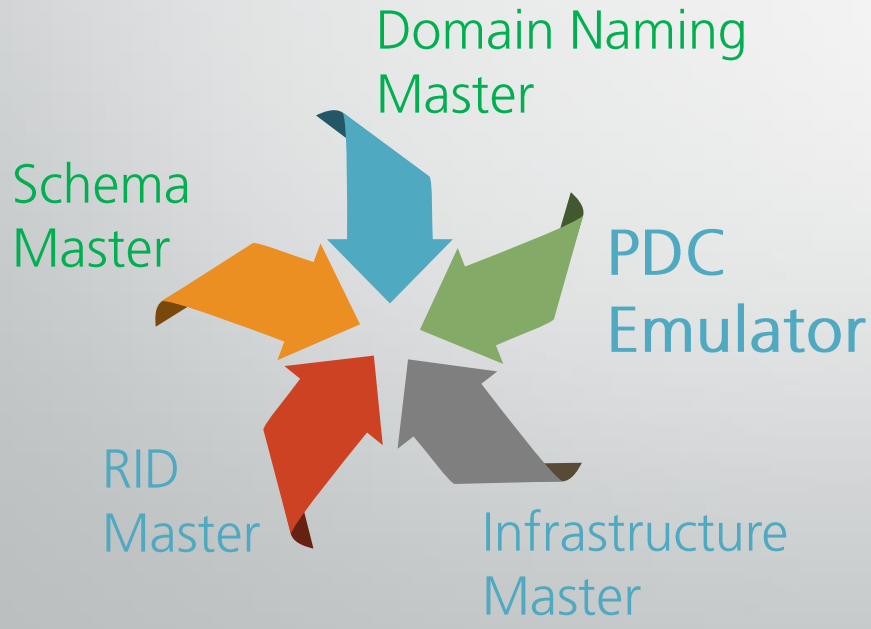


- Bewaakt alle domeinen in de forest
  - ⇒ Er kan niet zomaar domein toegevoegd of verwijderd worden
- Verantwoordelijk voor de trusts binnen de forest

FSMO Roles

FUTURE-PROOF

PEOPLE-CENTRIC

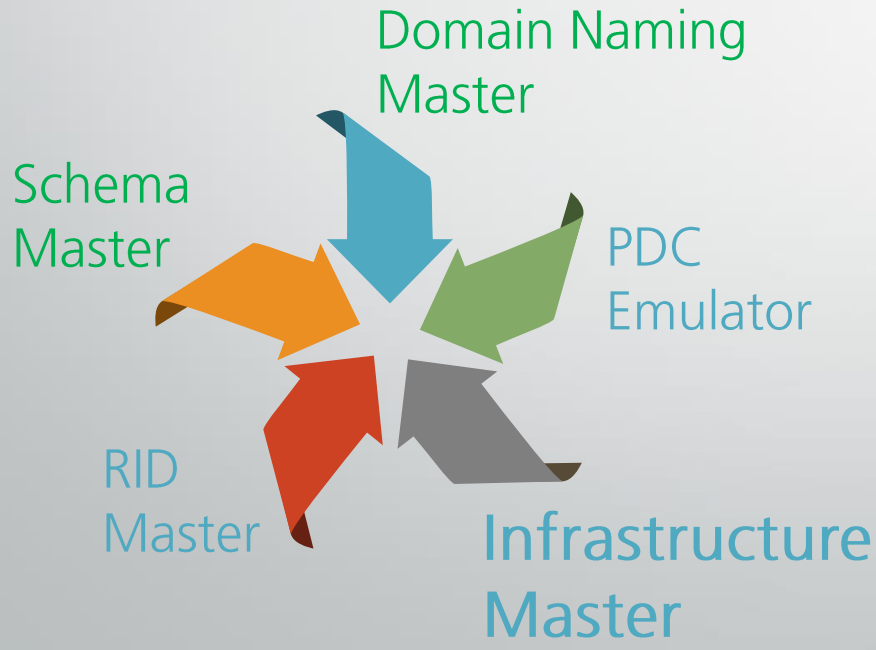


- Zorgt voor replicatie naar andere DC's als wachtwoorden veranderen
- Tijdssynchronisatie voor domain members
- Voorziet lijst van workgroups en domeinen als een client door het netwerk zou browsen

FSMO Roles

FUTURE-PROOF

PEOPLE-CENTRIC

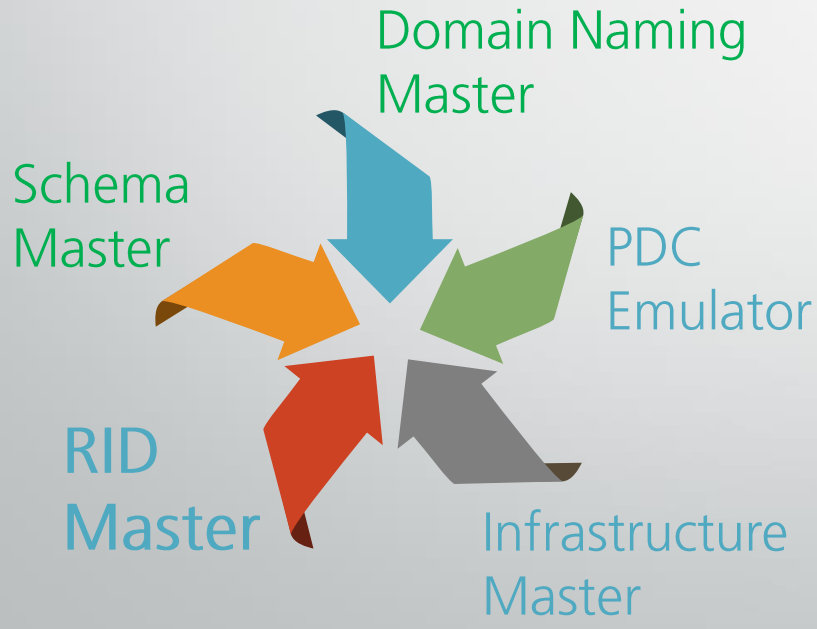


- Zorgt voor replicatie naar andere DC's
  - ✓ SID, GUID, DN, …
- Onderhoudt Global Catalog

FSMO Roles

FUTURE-PROOF

PEOPLE-CENTRIC



- Alle objecten hebben een SID (= Security Identifier)
  - ✓ Eerste deel is "Domain ID" (hetzelfde voor alle objecten binnen een domein)
  - ✓ Tweede deel is "Relative ID" (uniek!)
- Elke DC krijgt pool met RID-nummers toegewezen
  - ⇒ RID master wijst pools toe

FSMO Roles

FUTURE-PROOF

PEOPLE-CENTRIC

- Standaard worden roles automatisch toegewezen aan een DC

alle roles

1ste DC van forest

3 domain roles

1ste DC van domein

FSMO Roles

FUTURE-PROOF

PEOPLE-CENTRIC

- Verplaatsen van roles kan op 2 manieren

Verplaatsen van roles tussen DC's wanneer er geen issues zijn

Transfer roles

Roles overnemen van gefaalde DC wanneer er issues zijn

Seize roles

FSMO Roles

FUTURE-PROOF

PEOPLE-CENTRIC

Best Practice vanaf 2 DC's → Spreiden van de rollen !!!

DOMAIN ROLES

- PDC Emulator
- Infrastructure Master
- RID Master

1ste DC

FOREST ROLES

- Schema Master
- Domain Naming Master

2de DC

FUTURE-PROOF

PEOPLE-CENTRIC

- [x] LAB – FSMO Roles

Active Directory Maintenance

FUTURE-PROOF

PEOPLE-CENTRIC

- Opschonen van AD kan op 2 manieren

Offline
defragmentatie

Metadata
Cleanup

Active Directory Maintenance

FUTURE-PROOF

PEOPLE-CENTRIC

Offline defragmentatie

= Eeuwenoude techniek in Active Directory

- "defragmentatie" van Active Directory database
- NTDS.dit blijft maar groeien
- Objecten verwijderen in AD ⇒ NTDS.dit verkleint niet !!

AD Services mogen niet draaien ⇒ Moet offline gebeuren

Active Directory Maintenance

FUTURE-PROOF

PEOPLE-CENTRIC

Offline defragmentatie

1. DC opstarten in DSRM (= Directory Service Repair Mode)
2. Command Prompt → *"NTDSUtil"* ⇒ NTDSUtil Prompt
    1. *"Activate instance NTDS"*
    2. *"Files"* (opent file maintenance) ⇒ *"info"*
    3. *"Compact to …"* (bestand defragmenteren naar locatie)
3. Nieuwe NTDS.dit kopiëren naar bestaande NTDS.dit

Active Directory Maintenance

FUTURE-PROOF

PEOPLE-CENTRIC

Metadata Cleanup

= Opkuisen van oude informatie die blijft hangen in AD

- Nodig wanneer DC geforceerd uit Active Directory is verwijderd
- Nodig bij DC's die operation master roles hebben
- Kan via console of via CMD-line uitgevoerd worden

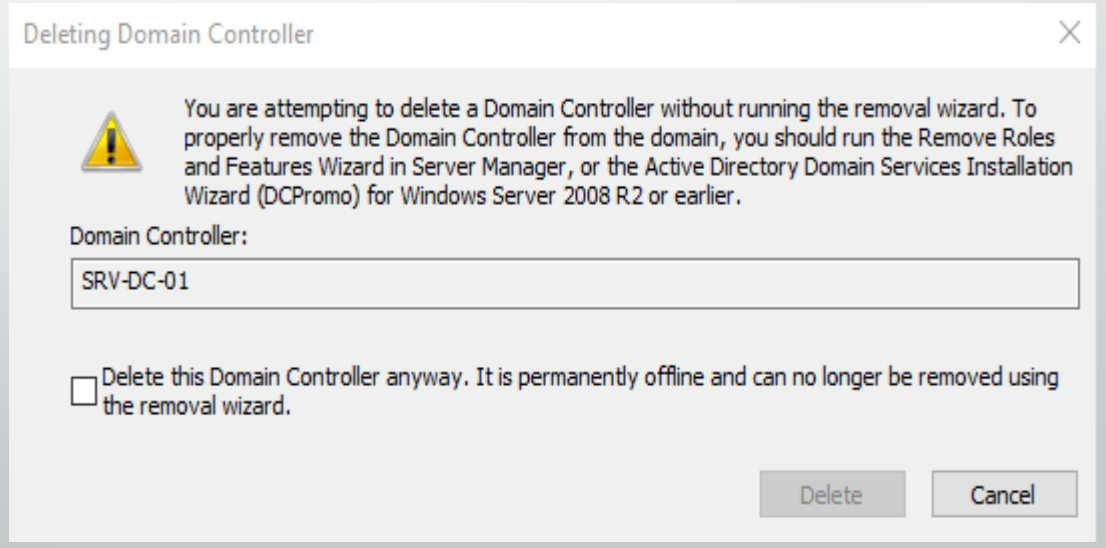
Active Directory Maintenance

FUTURE-PROOF

PEOPLE-CENTRIC

Metadata Cleanup

- Via ADUC-console



Central Store

FUTURE-PROOF

PEOPLE-CENTRIC

- Nieuw(e) OS, software pakketten,... binnen netwerk
  - ⇒ Group Policy Management bijwerken

Central Store updaten met administrative templates

Administrative templates bestaan uit:

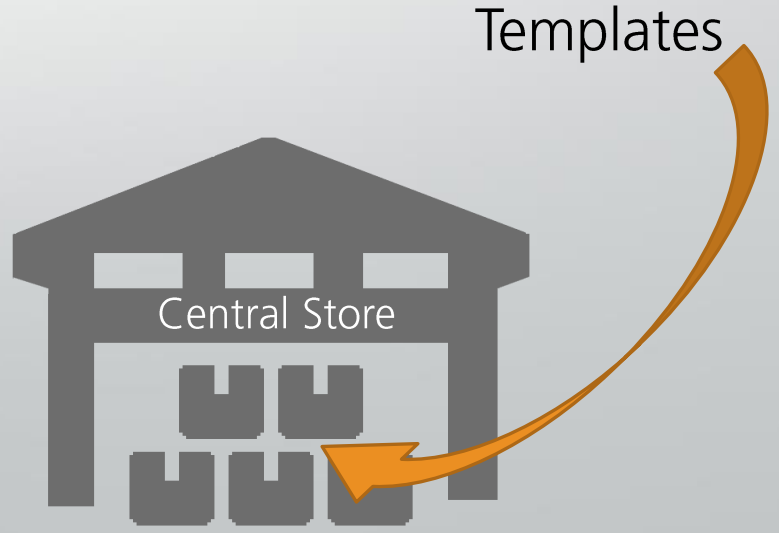
- ADMX-files = Algemene GPO-configuraties
- ADML-files = Taalspecifieke GPO-configuraties

Central Store

FUTURE-PROOF

PEOPLE-CENTRIC

1. Aanmaken Central Store:
   \\<domain>\SYSVOL\<domain>\Policies**PolicyDefinitions**
2. ADMX files onder deze folder plaatsen
3. ADML files onder juiste subfolder plaatsen
   (Bvb.: en-us, nl-nl)



FUTURE-PROOF

PEOPLE-CENTRIC

- [x] LAB – Central Store

Labs – Active Directory