Windows server 2019

Les 2

Standalone server

- Ook al wordt het niet veel gebruikt … alles begint hier …
- Alvorens een server in een domein opgenomen wordt of zelf een domein controller wordt, is het en standalone server

- Op deze standalone server wordt gewerkt met lokale gebruikers en lokale groepen
  - lokaal op de server
  - Hoe aanmaken
    - Tools => computer management

Active Directory

- AD is een implementatie van LDAP, Kerberos en DNS in een Windows-omgeving
  - Kerberos: authenticatieprotocol dat ervoor zorgt dat gebruikers van een netwerk zich op een veilige manier kunnen aanmelden en hun identiteit kunnen bewijzen, zonder zich telkens opnieuw te moeten aanmelden. Dit maakt “single sign-on” mogelijk.
  - LDAP: ‘Lightweight Access Protocol’ is een netwerkprotocol dat beschrijft hoe gegevens uit een directoryservice benaderd moeten worden. Een directory is informatie die op een hiërarchische manier, gegroepeerd naar een bepaald attribuut, is opgeslagen.
  - DNS

ntds.dit

- Een domein is een groep netwerkobjecten zoals computers, printers, … die centraal beheerd worden
  - ieder netwerkobject moet een unieke naam krijgen

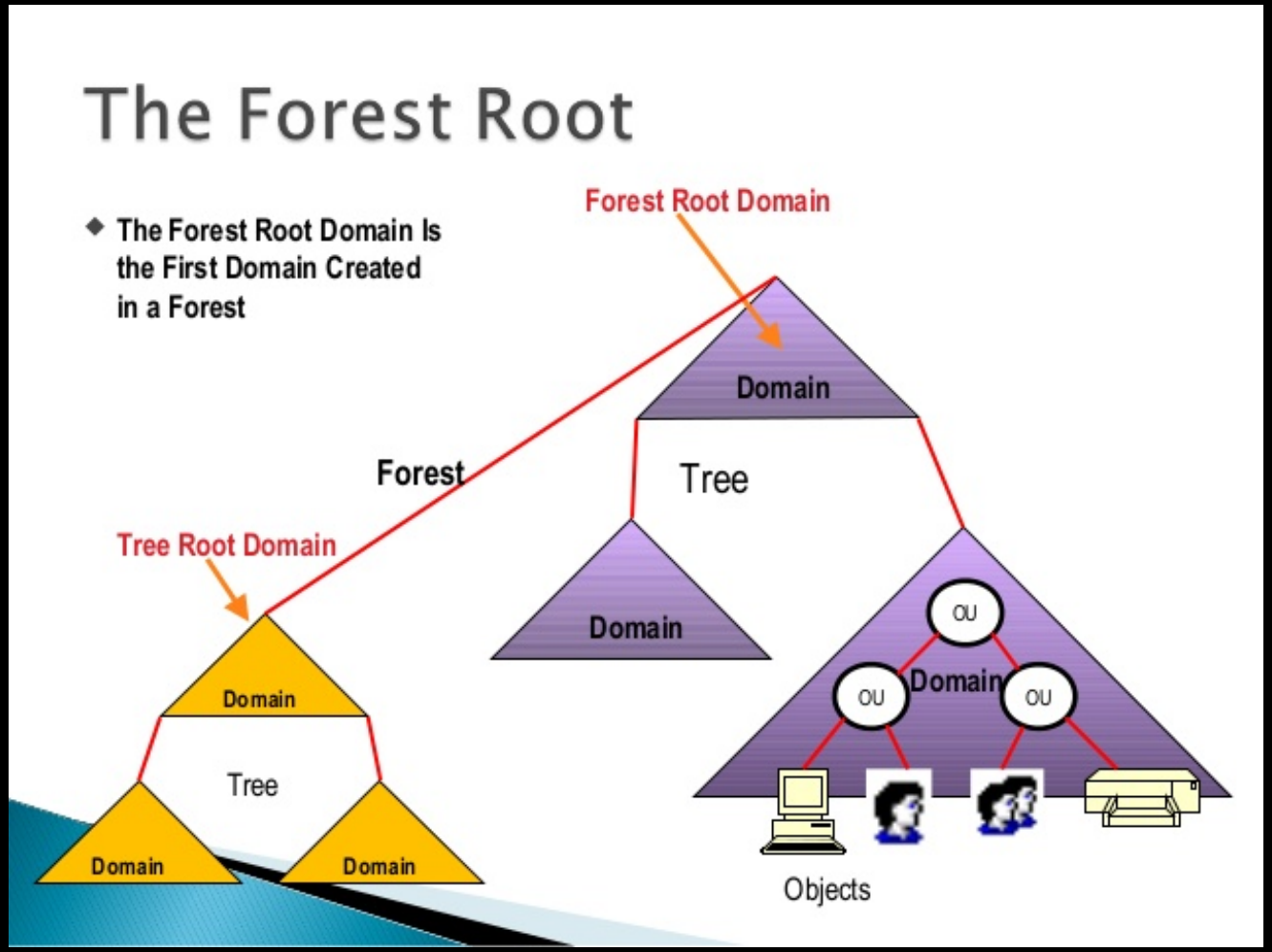
- Gegevens over deze netwerkobjecten worden bewaard in een databank-bestand, nl. ntds.dit opgeslaan in %SystemRoot%\ntds\
  - New Technology Directory Services
  - Data Information Table

ntds.dit

- Ntds.dit bevat drie tabellen
  - Schema
    - Hierin staat welke soorten objecten in een active directory kunnen worden gemaakt/gebruikt.
    - Hierin staat welke objecten “een relatie hebben” tot welke ander objecten
    - Hierin staat welke “objectkenmerken” verplicht of facultatief zijn
  - Link
    - Hierin staat welke objecten “verbonden zijn” met welke andere objecten
  - Gegevens
    - Bevat de gegevens van alle objecten

Forest - Tree

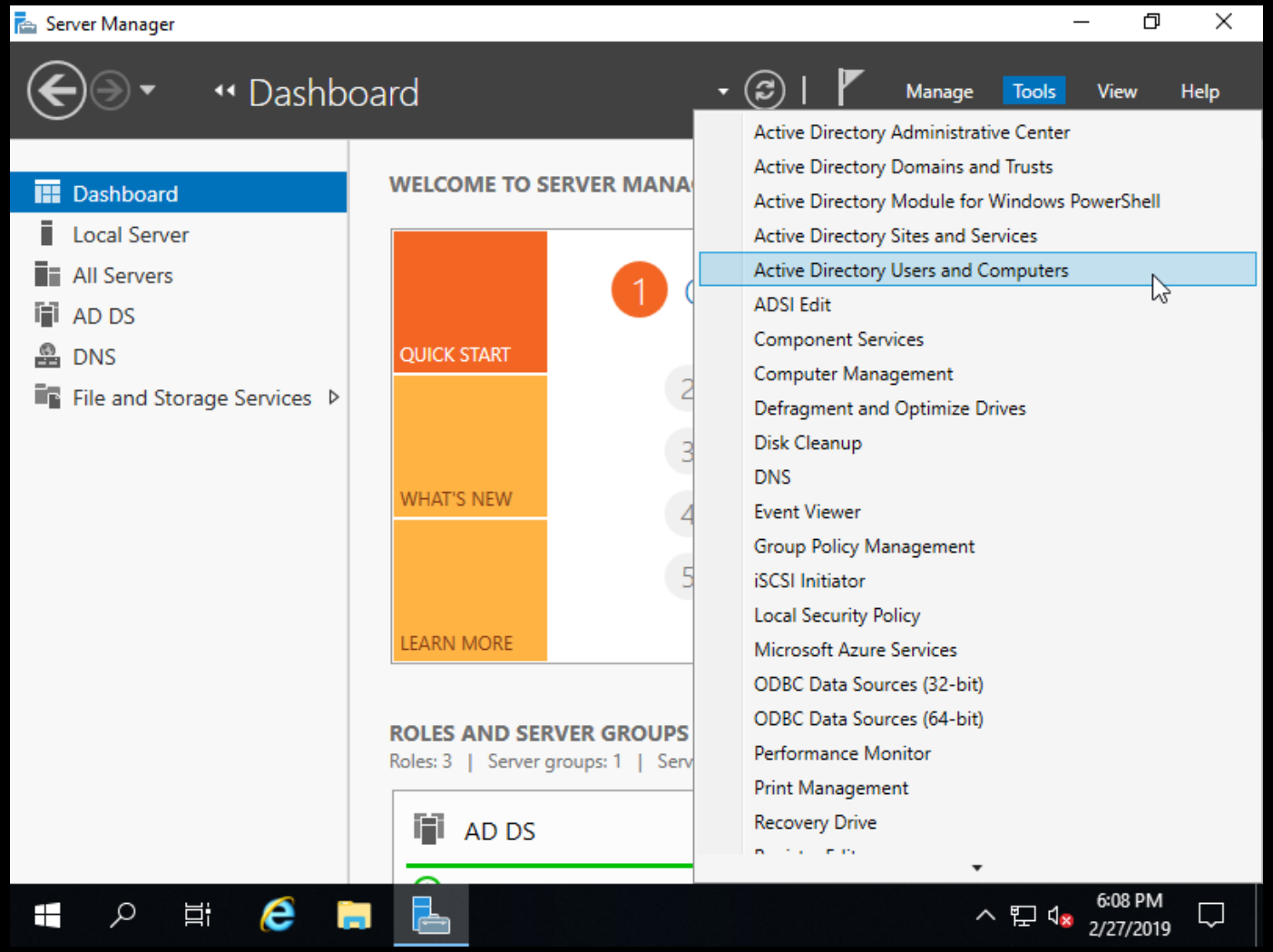
- Een parent domain of root domain is het eerste domain
- Cosci.be is het root domain
- Cosci.be is ook het parent domain voor de child domains tokyo.cosci.be en madrid.cosci.be
- De users binnen de AD van tokyo.cosci.be kunnen ook inloggen bij cosci.be, ook zit deze account niet in de AD van cosci.be



Sites

- Een domein is een logische eenheid van netwerkobjecten
- Een site is een fysiek geografische eenheid, nl. een locatie
- Het bedrijf Cosci.be kan een domein hebben waarbij de kantoren/gebouwen zich op verschillende geografisch verspreide locaties of sites bevinden
- Een site wordt gedefinieerd door een of meerdere IP-subnetten
- Zijn ontstaan om het replicatieverkeer over WAN-linken te verminderen

On PC?
Remote Server Administration Tools (RSAT)



Objectenklassen in AD

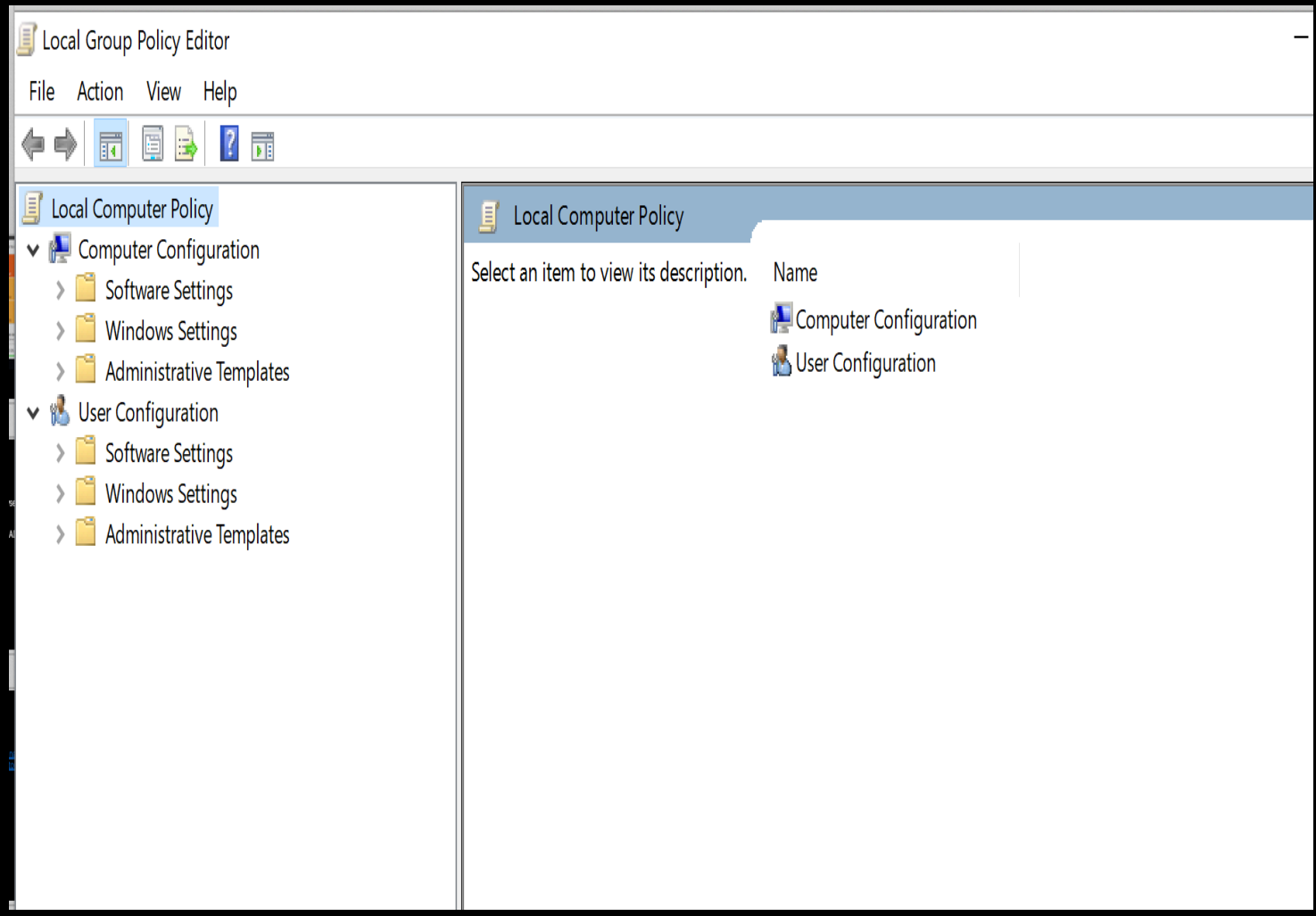
- AD is een objectgeoriënteerde directoryservice
- Objecten zijn instanties van klassen
- Welke ingebouwde objectklassen heeft AD?
  - Gebruikers
  - Computers
  - Groepen (container objecten) => verschil? De scope
    - Universal Group
      - Bereik gehele forest
      - Users/computers/… uit alle domeinen van het forest kunnen lid zijn
    - Global Group
      - Bereik gehele forest
      - Users/computers/… uitsluitend uit het eigen domeinen kunnen lid zijn
    - Domain Local Group:
      - Bereik domein
      - Users/computers uit alle domeinen van het forest kunnen lid zijn
    - Organizational Unit

Groepsbeleid

- Beleid beschrijft regels (beperkingen) die gelden:
  - User policies
    - Uitgevoerd tijdens inloggen user
    - Beperkingen gelden niet meer na uitloggen
  - Computer policies
    - Uitgevoerd tijdens opstart van computer
    - Blijven gelden bij elke user die inlogt
- We spreken meestal niet van beleid maar van groepsbeleid
- Twee soorten groepsbeleid
  - Lokaal => opgeslaan op de lokale computer, geldend voor een computer
  - Niet lokaal => centraal opgeslaan, geldend voor een AD netwerk

Lokaal groepsbeleid

- Aanpasbaar als computer niet in een domein zit
- gpedit.msc



Niet lokaal groepsbeleid

- Het groepsbeleid wordt vastgelegd in een Group Policy Object in AD
- Groepsbeleidobjecten zijn van toepassing op objecten in AD van de site, domein of OU waaraan ze zijn gekoppeld
- GPO’s uitvoer volgorde
  - Lokale
  - Site
  - Domein
  - OU (en sub-OU …)

Group Policy Management

- GPO’s op sites worden standaard niet getoond => Show Sites
- GPO is altijd gekoppeld aan een site, domein of OU

Voorbeeld oefening

- Maak een policy die alle icoontjes op de desktop verwijdert voor een user van Marketing
- Maak een policy die configuratiescherm blokkeert voor een user van Boekhouding
- Maak een policy die de C- schijf blokkeert voor een user van Sales
- Maak een policy die de Internet Explorer homepage instelt op www.ucll.be voor alle gebruikers
- Pas het wachtwoord beleid aan voor alle users zodat er geen complex wachtwoord nodig is en min 4 tekens. Ze mogen altijd alle wachtwoorden herbruiken en hoeven nooit hun wachtwoord te veranderen
- Testen? => reboot of gpudate /force

PowerShell

Wat studeren?

- begrijpen en kunnen gebruiken als referentiemateriaal
  - Book 1
  - Book 2
  - Book 3