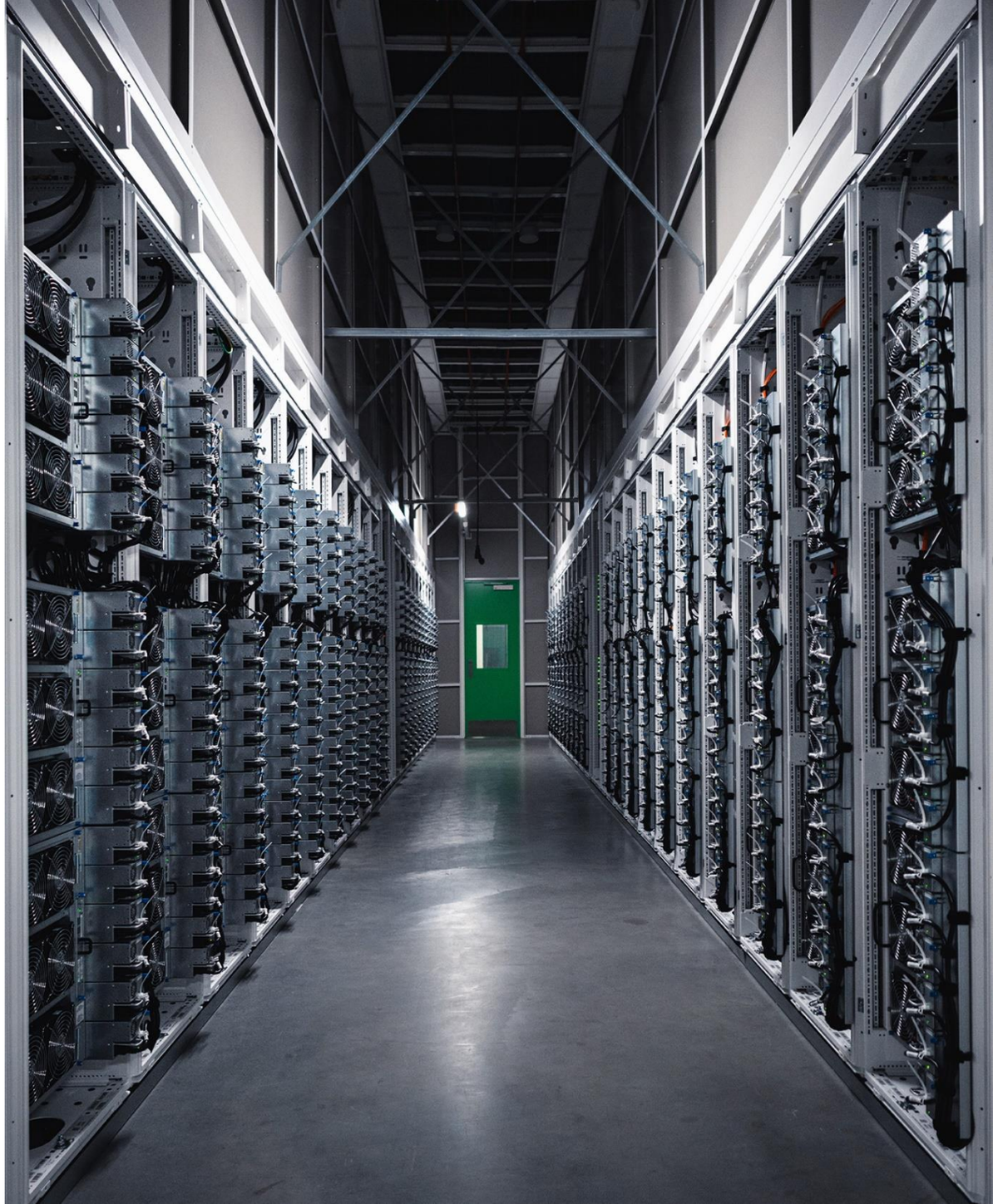
Microsoft

WS-011 Windows Server 2019 Administration



Module 2: Identity services in Windows Server

Module overview

Mô-đun này mô tả cách triển khai các dịch vụ trong môi trường Windows Server 2019

- Bài học:
  - Tổng quan về AD DS (Active Directory Domain Services: Dịch vụ miền Active Directory)
  - Triển khai Máy chủ điều khiển miền Windows Server (Domain Controllers: Máy chủ điều khiển miền)
  - Tổng quan về Azure AD (Giảm tải)
  - Thực thi chính sách nhóm (Group Policy)
  - Tổng quan về AD CS (AD Certificate Services) (Giảm tải)

Quản trị tài khoản người dùng

- Quản trị lớp học MMT và TTDL như sau: Máy chủ cấp tài khoản cho giảng viên và sinh viên để đăng nhập vào máy tính.
- Trên Windows Server, tạo 1 OU và tạo các tài khoản chứa trong OU đó:
  - Sinh viên 1 và 2:
    - Tên đăng nhập: **sv1**; Mật khẩu: **Sinhvien1**
    - Tên đăng nhập: **sv2**; Mật khẩu: **Sinhvien2**
  - Giảng viên 1 và 2:
    - Tên đăng nhập: **gv1**; Mật khẩu: **Giangvien1**
    - Tên đăng nhập: **gv2**; Mật khẩu: **Giangvien2**
- Trên máy Client:
  - Tham gia vào miền (**Lưu ý các thuộc tính TCP/IPv4**)
  - Đăng nhập bằng các tài khoản đã được cấp

Lesson 1: Overview of AD DS

Lesson 1 overview

Bài học này mô tả các thành phần logic cốt lõi và các thành phần vật lý để triển khai AD DS (Active Directory Domain Services)

- Chủ đề:
  - AD DS là gì?
  - Đối tượng AD DS
  - Rừng và miền AD DS (AD DS Forests and Domains)
  - Đơn vị tổ chức (OU: Organizational Unit)
  - Lược đồ AD DS (AD DS Schema)
  - Tổng quan về sao chép AD DS
  - Minh hoạ: Các công cụ để quản lý đối tượng, thuộc tính trong AD DS

What is AD DS? (1 of 2)

- Cơ sở dữ liệu Microsoft Active Directory Domain Services (AD DS) lưu trữ thông tin về danh tính người dùng, máy tính, nhóm, dịch vụ và tài nguyên trong một cấu trúc phân cấp, được gọi là directory.
- Máy chủ điều khiển miền AD DS cũng lưu trữ dịch vụ xác thực tài khoản người dùng và máy tính khi họ đăng nhập vào miền. Vì AD DS lưu trữ thông tin về tất cả các đối tượng miền và vì tất cả người dùng và máy tính phải kết nối với Máy chủ điều khiển miền AD DS khi đăng nhập, nên AD DS là cách chính để cấu hình và quản lý tài khoản người dùng và máy tính trong mạng.
- AD DS và các dịch vụ liên quan của nó tạo thành nền tảng cho mạng doanh nghiệp chạy hệ điều hành Windows.
- AD DS cung cấp một thư mục phân cấp, có thể tìm kiếm và một cách tiếp cận để áp dụng các cài đặt cấu hình và bảo mật cho các đối tượng trong doanh nghiệp.

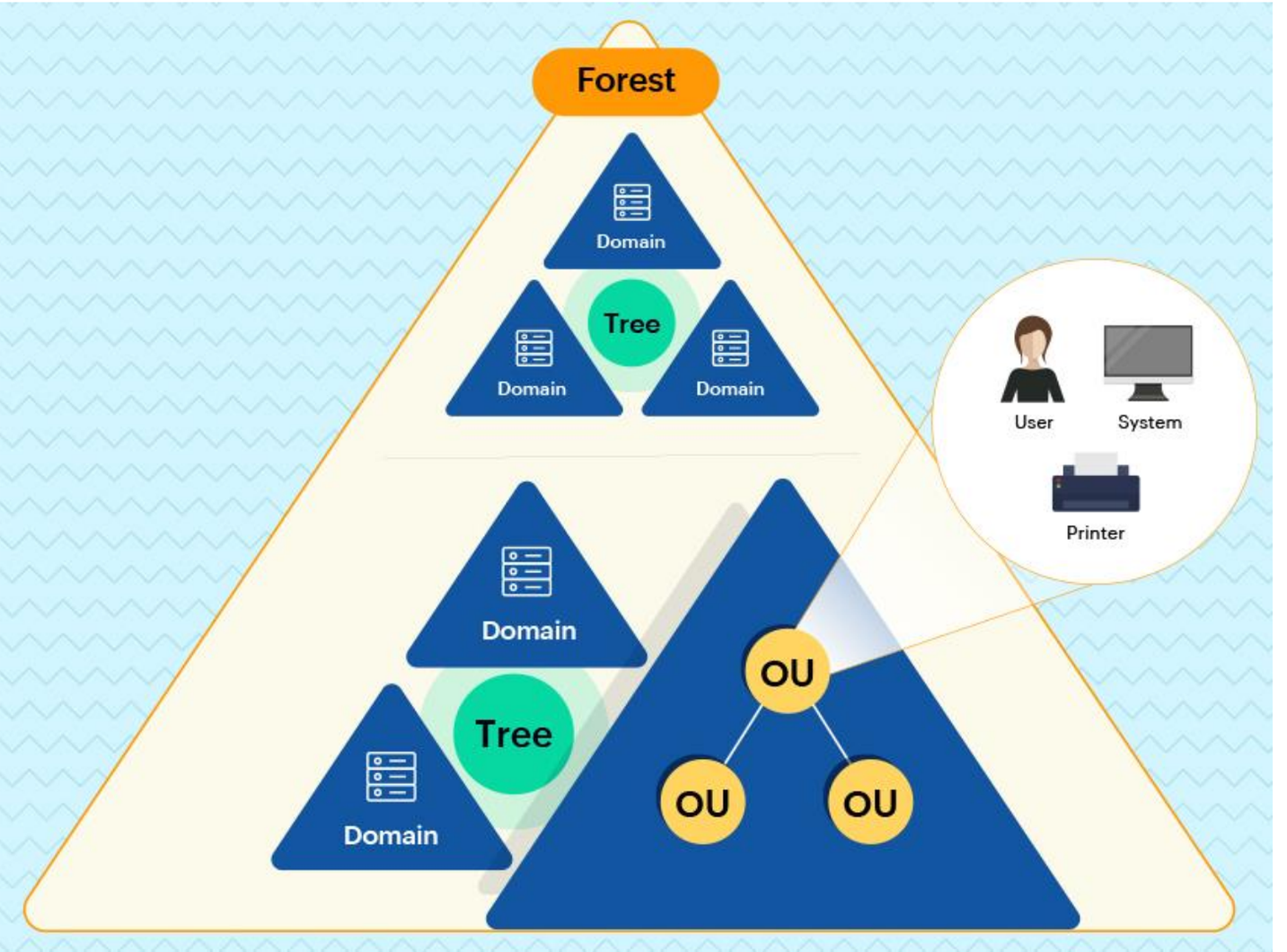
What is AD DS? (2 of 2)

AD DS bao gồm cả thành phần logic và vật lý

Thành phần logic	Thành phần vật lý
• Phân vùng (Partitions) • Lược đồ (Schema) • Miền (Domain) • Cây miền (Domain trees) • Rừng (Forests) • Đơn vị tổ chức (OU: Organizational Unit) • Bộ chứa (Containers)	• Máy chủ điều khiển miền (Domain controllers) • Kho dữ liệu (Data stores) • Máy chủ danh mục toàn cục (Global catalog servers) • Máy chủ điều khiển miền chỉ đọc (RODCs: Read-Only Domain Controller) • Địa điểm (Sites)

AD DS forests

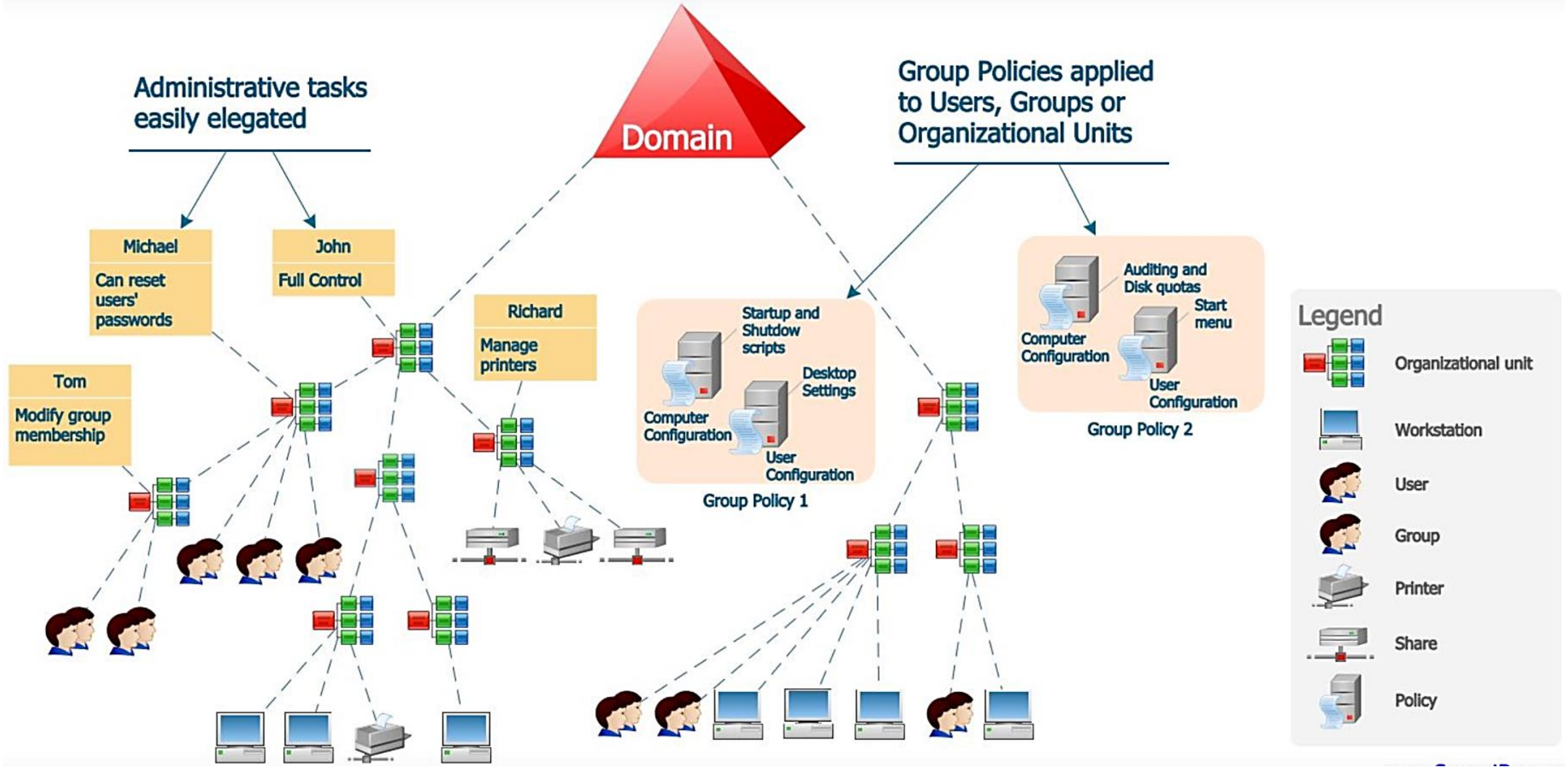
- Rừng (Forest): bộ chứa bậc cao
  - Ranh giới bảo mật
  - Ranh giới sao chép: phân vùng cấu hình, lược đồ, và danh mục toàn cục



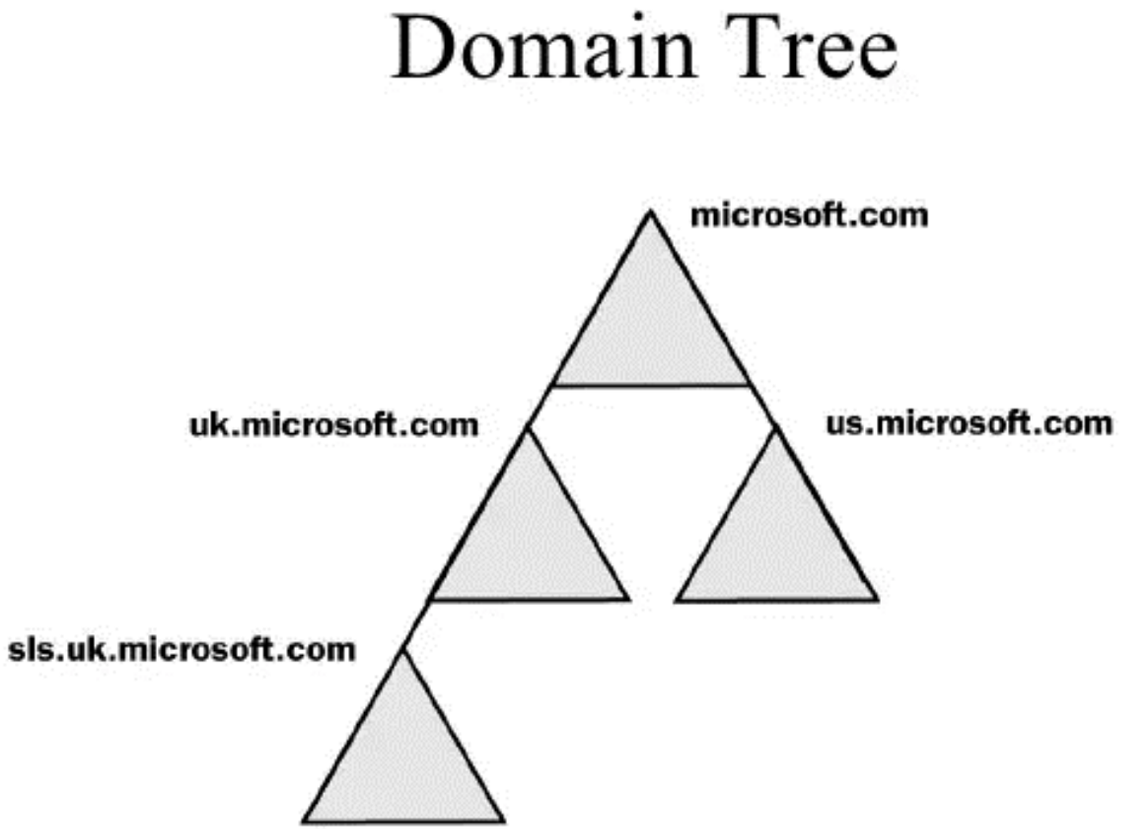
AD DS domains (1 of 2)

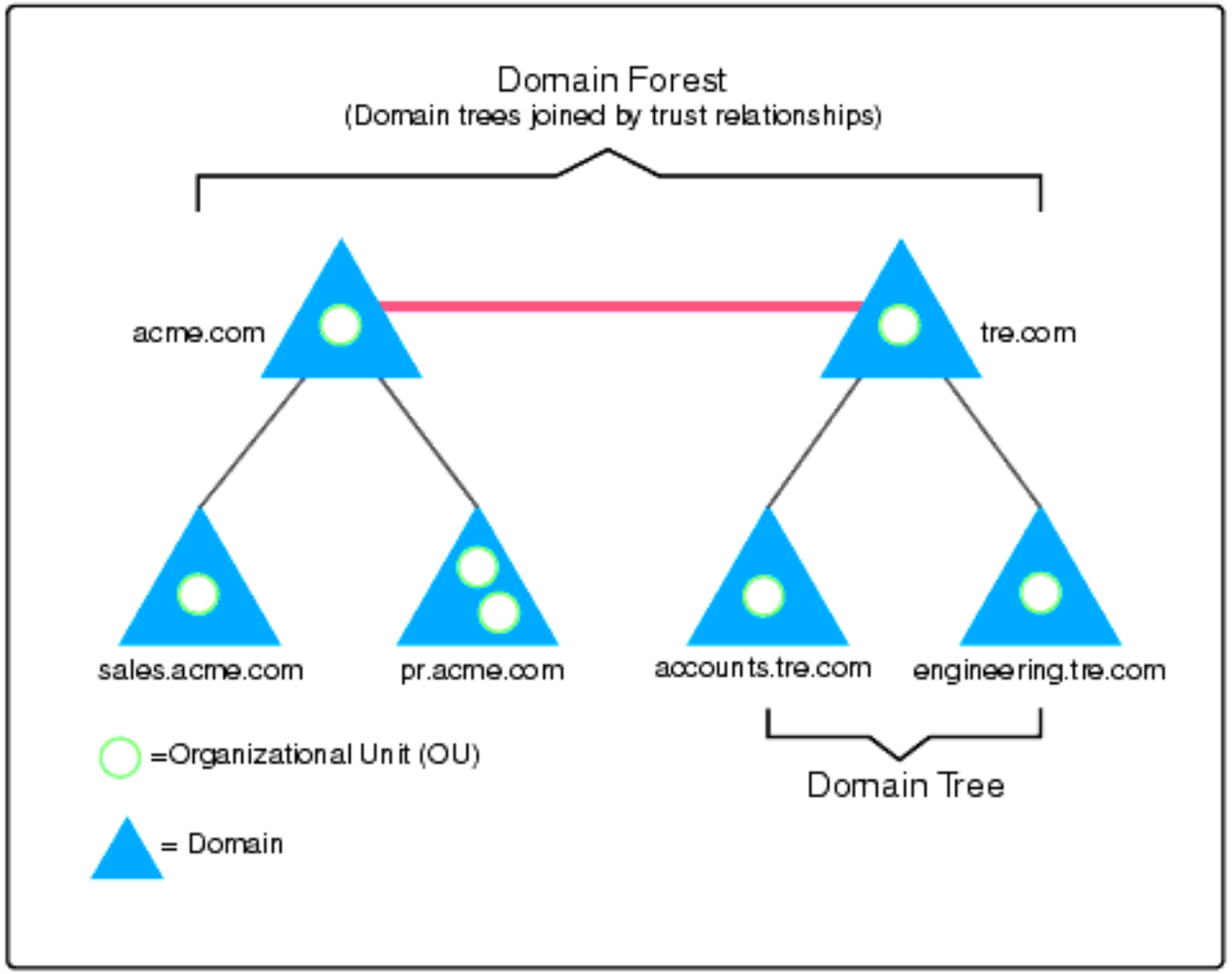
- Miền (Domain): bộ chứa logic để quản lý các đối tượng
  - Lưu trữ bản sao của cơ sở dữ liệu AD DS được đồng bộ hóa liên tục
  - Ranh giới sao chép: sao chép tất cả thay đổi tới bộ điều khiển khác trong miền
  - Trung tâm quản trị: Tài khoản Administrator, nhóm Domain Admins và nhóm Administrators
  - Cung cấp: Xác thực và ủy quyền
- AD DS yêu cầu một hoặc nhiều Máy chủ điều khiển miền
- Bất kỳ Máy chủ điều khiển miền nào cũng có thể xác thực bất kỳ đăng nhập nào bất cứ nơi nào trong miền

AD DS domains (2 of 2)



AD DS forests and domains



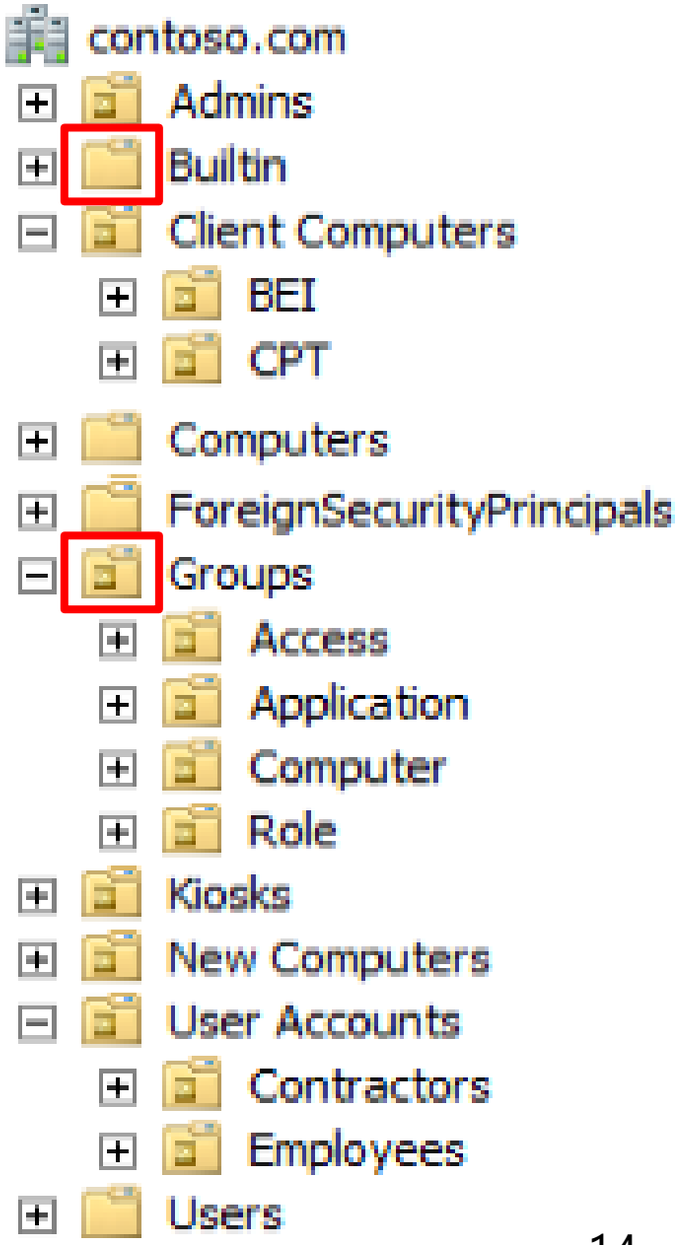


AD DS objects

- Đối tượng người dùng (User objects): xác thực tới miền AD DS và truy cập tài nguyên mạng với tài khoản đăng nhập, gồm tên người dùng và mật khẩu
- Đối tượng nhóm (Group objects)
  - Loại nhóm (Group types):
    - Bảo mật (Security): được kích hoạt bảo mật, gán quyền truy cập các tài nguyên
    - Phân phối (Distribution): không được kích hoạt bảo mật, ví dụ ứng dụng Email
  - Phạm vi nhóm (Group scopes): xác định phạm vi chức năng hoặc quyền của nhóm và thành viên của nhóm.
    - Local (chỉ tài nguyên cục bộ), Domain-local (chỉ tài nguyên cục bộ trong miền), Global (bất cứ nơi nào trong rừng, hợp nhất những người dùng có đặc điểm tương tự nhau), and Universal (bất cứ nơi nào trong rừng, thường được dùng trong mạng nhiều miền)
- Đối tượng máy tính (Computer objects)

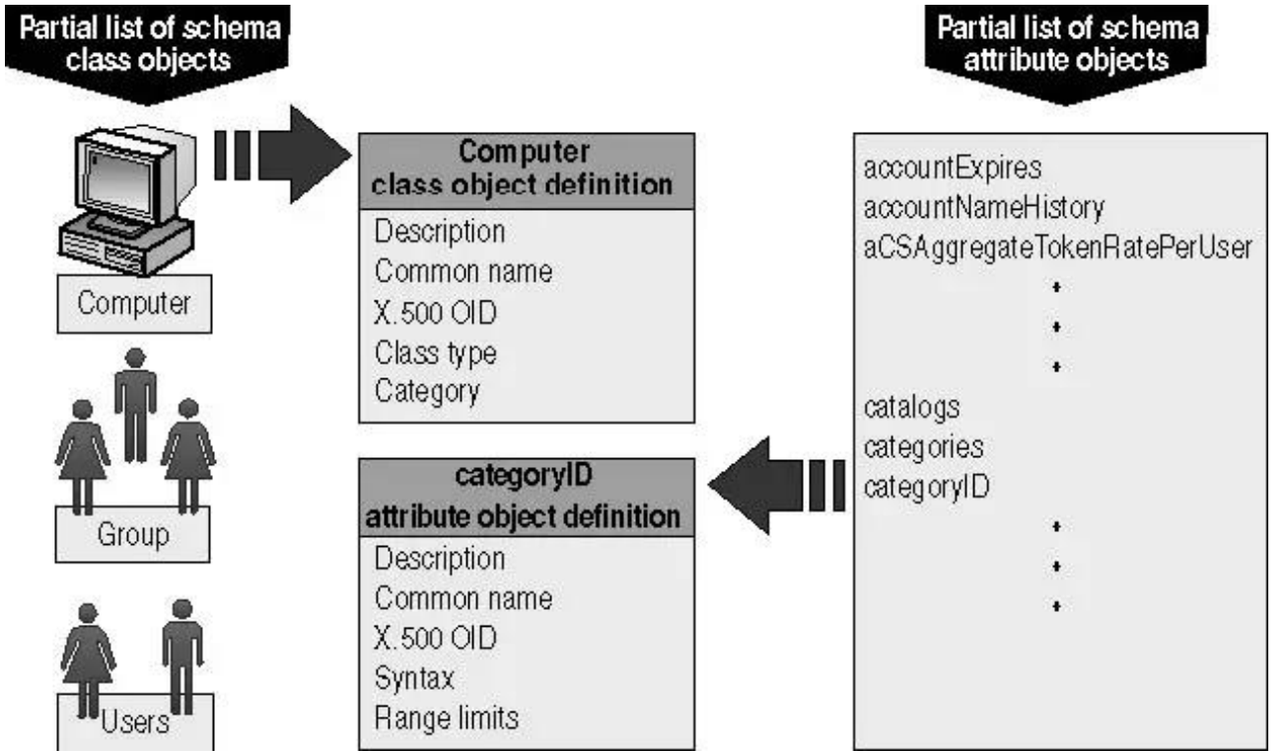
OUs

- Sử dụng bộ chứa (container) để nhóm đối tượng trong một miền:
  - Không thể áp dụng trực tiếp đối tượng chính sách nhóm (GPO: Group Policy Objects) vào bộ chứa
  - Bộ chứa được sử dụng cho các đối tượng hệ thống và làm vị trí mặc định cho các đối tượng mới
- Tạo OU (bộ chứa cho phép áp dụng GPO):
  - Nhóm các đối tượng với nhau để dễ dàng quản lý
  - Cấu hình các đối tượng bằng cách liên kết GPO cho chúng
  - Phân quyền quản trị

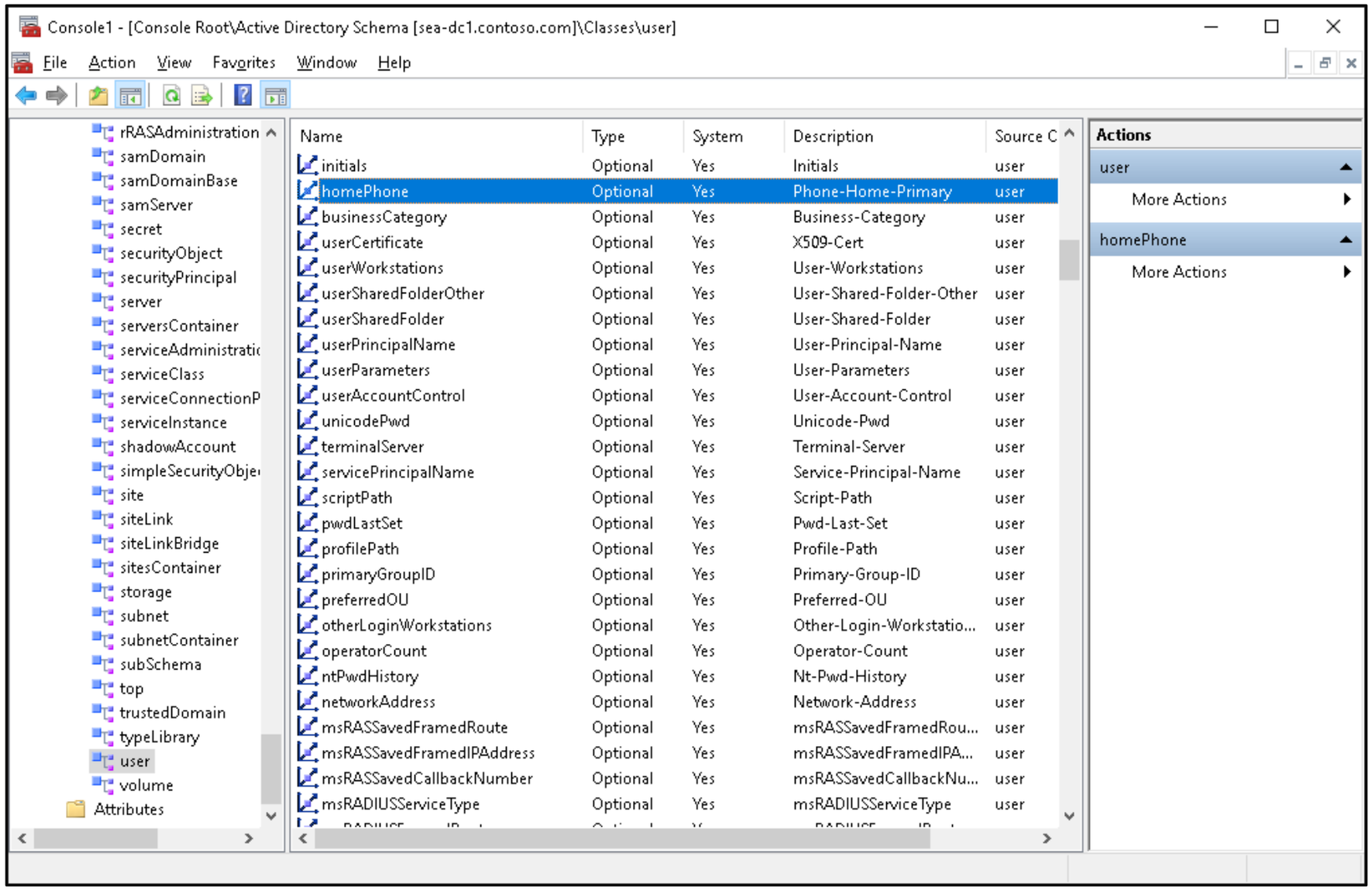


AD DS schema

- Lược đồ AD DS là thành phần xác định tất cả các lớp đối tượng và thuộc tính mà AD DS sử dụng để lưu trữ dữ liệu
- Tất cả các miền trong một rừng chứa một bản sao của lược đồ áp dụng cho rừng đó
- Mọi thay đổi trong lược đồ sẽ sao chép tới mọi Máy chủ điều khiển miền trong rừng thông qua các đối tác sao chép của chúng
- Tuy nhiên, các thay đổi bắt nguồn từ lược đồ chính, thường là Máy chủ điều khiển miền đầu tiên trong rừng



AD DS schema


Console1 - [Console Root\Active Directory Schema [sea-dc1.contoso.com]\Classes\user]
File Action View Favorites Window Help
rRASAdministration
samDomain
samDomainBase
samServer
secret
securityObject
securityPrincipal
server
serversContainer
serviceAdministratic
serviceClass
serviceConnectionP
serviceInstance
shadowAccount
simpleSecurityObje
site
siteLink
siteLinkBridge
sitesContainer
storage
subnet
subnetContainer
subSchema
top
trustedDomain
typeLibrary
user
volume
Attributes
Name Type System Description Source C
initials Optional Yes Initials user
homePhone Optional Yes Phone-Home-Primary user
businessCategory Optional Yes Business-Category user
userCertificate Optional Yes X509-Cert user
userWorkstations Optional Yes User-Workstations user
userSharedFolderOther Optional Yes User-Shared-Folder-Other user
userSharedFolder Optional Yes User-Shared-Folder user
userPrincipalName Optional Yes User-Principal-Name user
userParameters Optional Yes User-Parameters user
userAccountControl Optional Yes User-Account-Control user
unicodePwd Optional Yes Unicode-Pwd user
terminalServer Optional Yes Terminal-Server user
servicePrincipalName Optional Yes Service-Principal-Name user
scriptPath Optional Yes Script-Path user
pwdLastSet Optional Yes Pwd-Last-Set user
profilePath Optional Yes Profile-Path user
primaryGroupID Optional Yes Primary-Group-ID user
preferredOU Optional Yes Preferred-OU user
otherLoginWorkstations Optional Yes Other-Login-Workstatio... user
operatorCount Optional Yes Operator-Count user
ntPwdHistory Optional Yes Nt-Pwd-History user
networkAddress Optional Yes Network-Address user
msRASSavedFramedRoute Optional Yes msRASSavedFramedRou... user
msRASSavedFramedIPAddress Optional Yes msRASSavedFramedIPA... user
msRASSavedCallbackNumber Optional Yes msRASSavedCallbackNu... user
msRADIUSServiceType Optional Yes msRADIUSServiceType user
Actions
user
More Actions
homePhone
More Actions

Overview of AD DS replication

- Trong cấu trúc hạ tầng AD DS, Máy chủ điều khiển miền tiêu chuẩn sao chép thông tin Active Directory bằng cách sử dụng mô hình sao chép đa chủ
- Dữ liệu Active Directory được phân tách hợp lý thành nhiều phân vùng:
  - Phân vùng cấu hình
  - Phân vùng lược đồ
  - Phân vùng miền
  - Phân vùng ứng dụng

Các đặc điểm của sao chép AD DS:

- Sao chép đa chủ
- Dựa trên nguyên tắc kéo (Pull-based)
- Lưu trữ và chuyển tiếp
- Phân vùng lưu trữ dữ liệu
- Tự động tạo cấu trúc sao chép liên kết hiệu quả và mạnh mẽ
- Sao chép cấp thuộc tính
- Kiểm soát riêng biệt bản sao chép giữa các trang web
- Phát hiện và quản lý xung đột

Minh hoạ: Sử dụng công cụ để quản lý đối tượng và thuộc tính trong AD DS

- Active Directory Users and Computers
- Remote Server Administration Tools
- Windows Admin Center

Lesson 2: Deploying Windows Server domain controllers

Lesson 2 overview

Bài học này mô tả mục tiêu và chức năng của việc sử dụng Máy chủ điều khiển miền trong môi trường Windows Server

- Chủ đề:
  - Máy chủ điều khiển miền (DC: Domain Controllers) là gì?
  - Cài đặt Máy chủ điều khiển miền
  - Minh hoạ: Active Directory Domain Services và Domain Controllers
  - Hoạt động nhóm
  - Danh mục toàn cục là gì?
  - Làm chủ các hoạt động là gì?
  - Nâng cấp từ phiên bản trước của AD DS
  - Nhân bản DC

What is a DC? (1 of 2)

Máy chủ điều khiển miền:

- Xác thực tất cả người dùng và máy tính trong miền
- Là máy chủ xử lý các yêu cầu xác thực từ người dùng trong miền máy tính sử dụng Active Directory.
- Lưu trữ bản sao của cơ sở dữ liệu AD DS (Ntds.dit) và thư mục SYSVOL (chứa tất cả các cài đặt mẫu và tập tin cho đối tượng chính sách nhóm (GPO: Group Policy Objects))
- Có hai loại:
  - Read-only domain controllers (RODC): chứa bản sao chỉ đọc
  - Bộ điền khiển miền còn lại cho phép chỉnh sửa và sao lưu

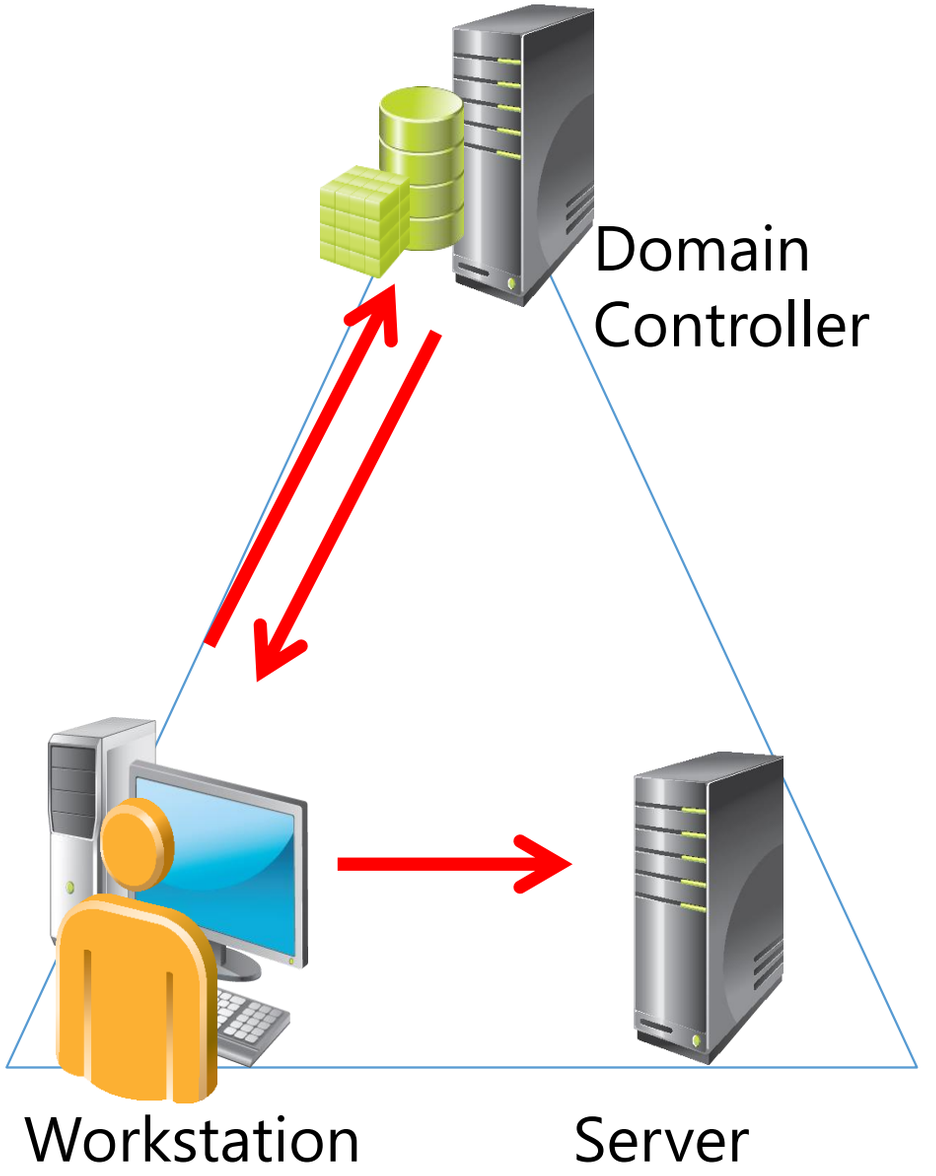
What is a DC? (2 of 2)

Đặc điểm Máy chủ điều khiển miền:

- Sử dụng quy trình sao chép đa chủ để sao chép dữ liệu từ Máy chủ điều khiển miền này sang Máy chủ điều khiển miền khác
- Dịch vụ sao chép AD DS sẽ đồng bộ hóa các thay đổi đối với cơ sở dữ liệu AD DS với tất cả các Máy chủ điều khiển miền khác trong miền
- Lưu trữ các dịch vụ liên quan đến AD DS: Dịch vụ xác thực Kerberos và dịch vụ KDC (Key Distribution Center) cho phép tài khoản xác thực và đăng nhập vào miền
- Giải pháp tốt nhất:
  - Khả dụng: Sử dụng ít nhất hai Máy chủ điều khiển miền trong một miền
  - Bảo mật: Sử dụng RODC hoặc BitLocker

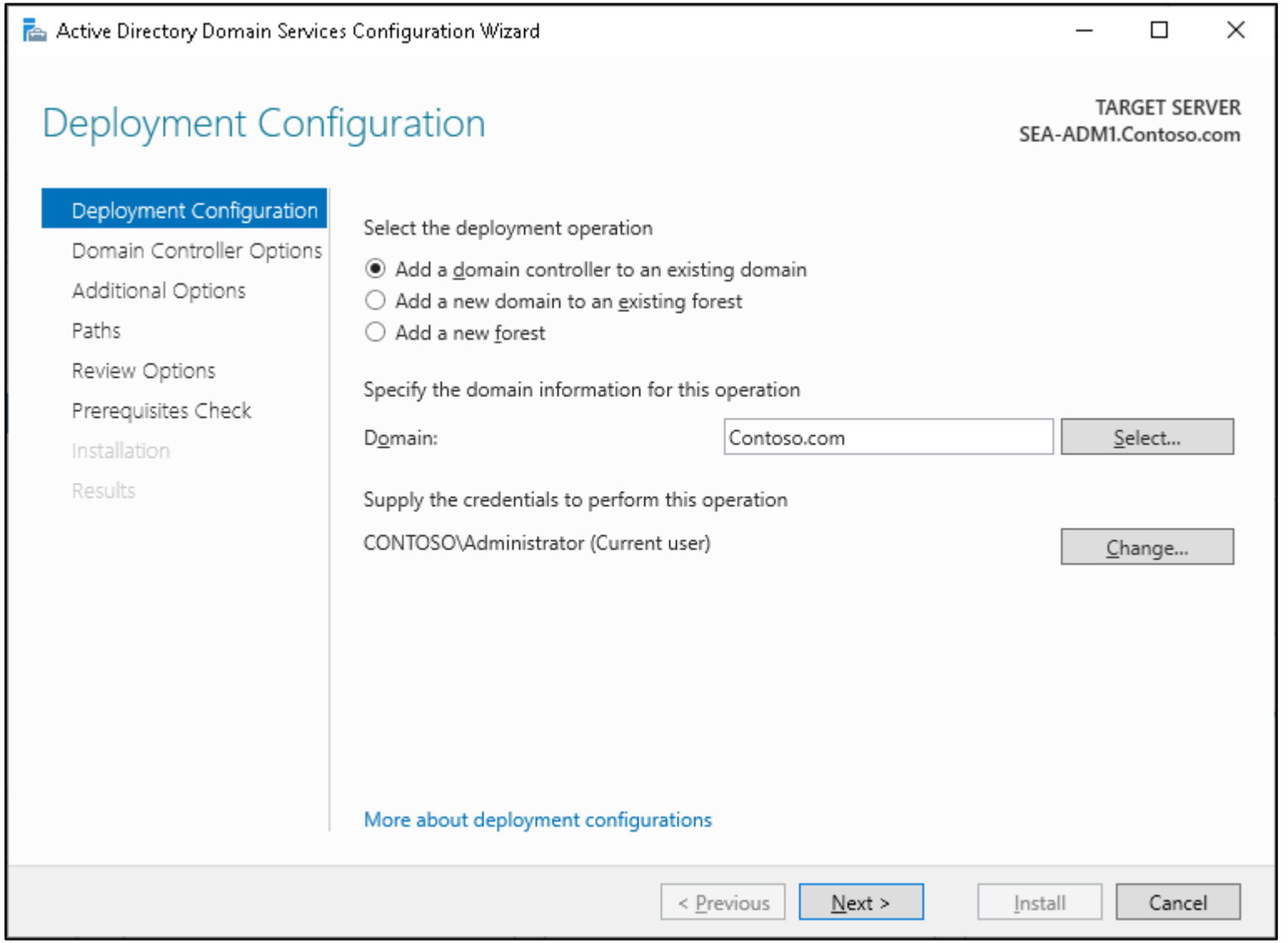
AD DS sign-in process

1. Tài khoản người dùng được xác thực với Máy chủ điều khiển miền
2. Máy chủ điều khiển miền trả lại "phiếu cấp vé" (TGT: Ticket Granting Ticket) cho máy khách
3. Máy khách sử dụng TGT để đăng ký quyền truy cập vào máy trạm
4. Máy chủ điều khiển miền cấp quyền truy cập vào máy trạm
5. Máy khách sử dụng TGT để đăng ký quyền truy cập vào máy chủ
6. Máy chủ điều khiển miền trả lại quyền truy cập vào máy chủ



Install a DC

- Cài đặt Máy chủ điều khiển miền trên Server Manager
- Cài đặt Máy chủ điều khiển miền trên bản cài đặt Server Core của Windows Server
- Cài đặt Máy chủ điều khiển miền bằng cách cài đặt từ phương tiện



Minh hoạ:
- Active Directory Domain Services
- Domain Controllers

- Cài đặt AD DS và Máy chủ điều khiển miền
- Quản trị người dùng sử dụng AD DS và Máy chủ điều khiển miền

Hoạt động nhóm số 1 – Cài đặt AD DS, DC

- Kiểm tra trạng thái Windows Server trước khi cài đặt Active Directory Domain Services (AD DS)
- Cài đặt AD DS và Máy chủ điều khiển miền
  - Tên miền: dhcnhn.com với mật khẩu: Dhcnhn1
- Làm quen với công cụ Server Manager và Active Directory Users and Computers

Hoạt động nhóm số 2 – Tham gia miền

- Quản trị lớp học MMT và TTDL của Trường ĐHCNHN dựa trên HĐH Windows với đặc điểm và yêu cầu như sau:
- Trên Windows Server, tạo 1 OU và tạo các tài khoản chứa trong OU đó:
  - Sinh viên 1 và 2:
    - Tên đăng nhập: sv1; Mật khẩu: Sinhvien1
    - Tên đăng nhập: sv2; Mật khẩu: Sinhvien2
  - Giảng viên 1 và 2:
    - Tên đăng nhập: gv1; Mật khẩu: Giangvien1
    - Tên đăng nhập: gv2; Mật khẩu: Giangvien2
- Trên máy Client:
  - Tham gia vào miền (**Lưu ý các thuộc tính TCP/IPv4**)
  - Đăng nhập bằng các tài khoản đã được cấp

Hoạt động nhóm số 3 – Người dùng

- Quản trị lớp học MMT và TTDL của Trường ĐHCNHN dựa trên HĐH Windows với đặc điểm và yêu cầu như sau:
  - Tạo 6 tài khoản (TK) sinh viên (SV) 1 đến 6 với cặp tên đăng nhập và mật khẩu:
    - sv1 – Sinhvien1; sv2 – Sinhvien2; …; sv6 – Sinhvien6
  - Mật khẩu TK SV 2-6 không bao giờ hết hạn
  - TK SV 1 yêu cầu đổi mật khẩu thành Student1 sau lần đăng nhập đầu tiên
  - TK SV 2 không thể đổi mật khẩu (Thử đổi mật khẩu của SV 2 thành Student2)
  - TK SV 3 chỉ được phép đăng nhập thứ 2-7 trong khung giờ 7h-11h và 13h -17h
  - TK SV 4 không được phép đăng nhập vào ngày hôm nay
  - TK SV 5 hết hạn vào ngày mai
  - TK SV 6 chỉ được đăng nhập trên máy tính Client1

Hoạt động nhóm số 4 – Đối tượng nhóm

- Quản trị lớp học MMT và TTDL của Trường ĐHCNHN dựa trên HĐH Windows với đặc điểm và yêu cầu như sau:
  - Tạo 2 tài khoản (TK) sinh viên (SV):
    - sv1 – Sinhvien1; sv2 – Sinhvien2
  - Tạo 2 TK giảng viên (GV)
    - gv1 – Giangvien1; gv2 – Giangvien2
  - Tạo 1 nhóm "Giang vien" gồm 2 TK GV và "Sinh vien" gồm 2 TK SV
  - Tạo 2 TK SV sau khi đăng nhập bằng tài khoản GV:
    - sv3 – Sinhvien3; sv4 – Sinhvien4
    - Thực hiện tạo TK trước và sau khi đưa nhóm GV làm thành viên của nhóm quản trị (Administrator)

Hoạt động nhóm số 5 – Uỷ quyền

- Quản trị lớp học MMT và TTDL của Trường ĐHCNHN dựa trên HĐH Windows với đặc điểm và yêu cầu như sau:
  - Tạo 1 đơn vị tổ chức (OU: Organizational Unit) "MMT va TTDL"
  - Tạo 2 tài khoản (TK) giảng viên (GV) thuộc nhóm "Giang vien"
    - gv1 – Giangvien1; gv2 – Giangvien2
  - Uỷ quyền cho nhóm "Giang vien" được phép tạo, xoá, quản lý TK sinh viên (SV)
  - Đăng nhập bằng TK GV và tạo 2 TK SV:
    - sv1 – Sinhvien1; sv2 – Sinhvien2

What is the global catalog?

- Danh mục toàn cục:
  - Lưu trữ bộ thuộc tính một phần cho các miền khác trong nhóm
  - Hỗ trợ truy vấn cho các đối tượng trong rừng
- Trong một miền duy nhất, nên định cấu hình tất cả các Máy chủ điều khiển miền giữ một bản sao của danh mục toàn cục
- Trong môi trường nhiều miền, chủ hạ tầng không nên là máy chủ danh mục toàn cục trừ khi tất cả các Máy chủ điều khiển miền trong miền cũng là máy chủ danh mục toàn cục
- Khi có nhiều địa điểm, nên đặt ít nhất một Máy chủ điều khiển miền tại mỗi địa điểm thành máy chủ danh mục toàn cục

What are operations masters?

- Trong mô hình sao chép đa chủ, một số hoạt động phải là hoạt động làm chủ đơn lẻ
- Nhiều thuật ngữ được sử dụng cho các hoạt động làm chủ đơn lẻ trong AD DS, bao gồm:
  - Làm chủ các hoạt động (hoặc vai trò kiểm soát các hoạt động)
  - Vai trò làm chủ duy nhất
  - FSMO

The five FSMOs (Flexible Single Master Operations)	
Forest: • Domain naming master • Schema master	Domain: • RID master • Infrastructure master • PDC emulator master

Upgrade from a previous version of AD DS

Có hai tùy chọn để nâng cấp AD DS lên Windows Server 2019:

- Thực hiện nâng cấp tại chỗ từ Windows Server 2012 R2 trở lên thành Windows Server 2019:
  - Lợi ích. Ngoại trừ các bước kiểm tra điều kiện tiên quyết, tất cả các tập tin và chương trình đều được giữ nguyên và không cần thực hiện thêm công việc nào
  - Rủi ro. Nó có thể để lại các tập tin lỗi thời và thư viện liên kết động
- Giới thiệu một máy chủ mới chạy Windows Server 2019 tham gia vào miền, sau đó nâng cấp nó thành Máy chủ điều khiển miền (tùy chọn này thường được ưu tiên):
  - Lợi ích. Máy chủ mới không có tập tin và cài đặt lỗi thời
  - Rủi ro. Nó có thể yêu cầu thêm tác vụ để di chuyển các tập tin và cài đặt của quản trị viên

DC cloning

- Có thể nhân bản Máy chủ điều khiển miền nhằm:
  - Nhanh chóng triển khai các Máy chủ điều khiển miền bổ sung
  - Nhanh chóng khôi phục tính liên tục của doanh nghiệp trong quá trình khắc phục thảm họa
  - Tối ưu hóa việc triển khai đám mây riêng
  - Cung cấp môi trường thử nghiệm nhanh chóng
  - Nhanh chóng đáp ứng nhu cầu năng lực gia tăng tại các văn phòng chi nhánh
- Để nhân bản Máy chủ điều khiển miền nguồn:
  - Thêm Máy chủ điều khiển miền vào nhóm Cloneable Domain Controllers
  - Xác minh tính tương thích của ứng dụng và dịch vụ
  - Tạo tập tin DCCloneConfig.xml
  - Trích xuất nó một lần, sau đó tạo bao nhiêu bản sao theo yêu cầu
  - Bắt đầu nhân bản

Lesson 3: Overview of Azure AD

Lesson 4: Implementing Group Policy

Lesson 4 overview

Bài học này mô tả cách quản lý môi trường Windows Server bằng cách sử dụng cấu trúc hạ tầng chính sách nhóm (Group Policy)

- Chủ đề:
  - GPO (Group Policy Object) là gì?
  - Phạm vi GPO, thứ tự xử lý GPO và tính kế thừa
  - GPO dựa trên miền là gì?
  - GPO miền mặc định
  - Minh hoạ: Công cụ quản lý chính sách nhóm
  - Hoạt động nhóm
  - Tổng quan về lưu trữ GPO và Starter GPO là gì?
  - Mẫu quản trị là gì? và Tổng quan về Central Store

Thực thi chính sách nhóm

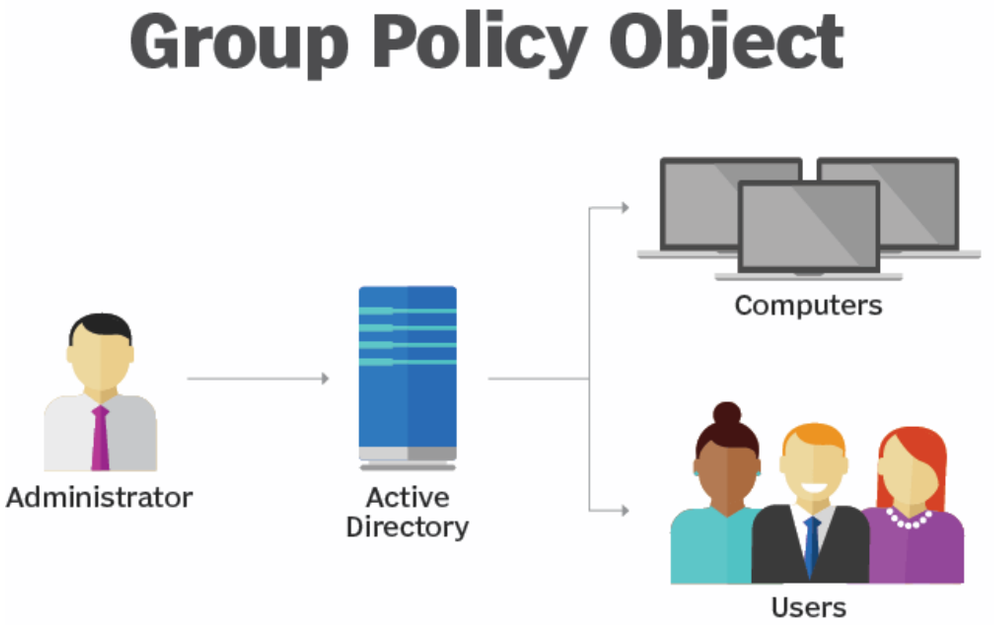
Quản trị lớp học MMT và TTDL của Trường ĐHCNHN dựa trên HĐH Windows với đặc điểm và yêu cầu như sau:

- Mỗi nhóm giảng viên và nhóm sinh viên được cấp các tài khoản:
  - gv1 – Giangvien1; gv2 – Giangvien2; sv1 – Sinhvien1; sv2 – Sinhvien2
- Chặn sinh viên mở Task Manager
- Cho phép giảng viên mở Task Manager

What are GPOs? (1 of 5)

- Chính sách nhóm là một bộ khung thông tin (framework) trong hệ điều hành Windows với các thành phần nằm trong dịch vụ miền Active Directory (AD DS), trên Máy chủ điều khiển miền, trên mỗi máy chủ và máy khách Windows

- Các cài đặt chính sách nhóm được định nghĩa trong đối tượng chính sách nhóm (Group Policy Object: GPO), chứa một hoặc nhiều cài đặt chính sách áp dụng cho một hoặc nhiều cài đặt cấu hình tới người dùng hoặc máy tính



What are GPOs? (2 of 5)

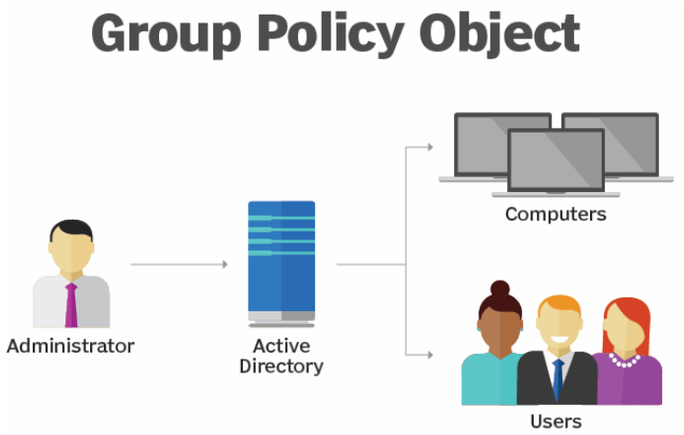
- Là một công cụ quản trị mạnh mẽ:
  - Áp dụng các cài đặt khác nhau tới một số lượng lớn người dùng và máy tính
  - Áp dụng cho các cấp độ khác nhau, từ máy tính cục bộ đến miền, ...
  - Cấu hình cài đặt mà không muốn người dùng tự cấu hình
  - Chuẩn hóa môi trường trên tất cả các máy tính trong một đơn vị tổ chức (OU) hoặc trong toàn bộ tổ chức
  - Cung cấp bảo mật bổ sung, để cấu hình một số cài đặt hệ thống nâng cao

What are GPOs? (3 of 5)

- Thông thường, GPO được sử dụng để:
  - Áp dụng cài đặt bảo mật (mật khẩu, tường lửa, quyền của người dùng)
  - Quản lý cài đặt ứng dụng máy tính (môi trường, ứng dụng được hỗ trợ GPO)
  - Triển khai phần mềm ứng dụng (ở định dạng .msi, tự động hoặc thủ công)
  - Quản lý chuyển hướng thư mục (sao lưu dữ liệu người dùng, tập trung hoá dữ liệu người dùng trên máy chủ, ví dụ, chuyển hướng thư mục Documents)
  - Cấu hình cài đặt mạng (chỉ cho phép người dùng kết nối tới Wi-Fi có tên được chỉ định trước, …)

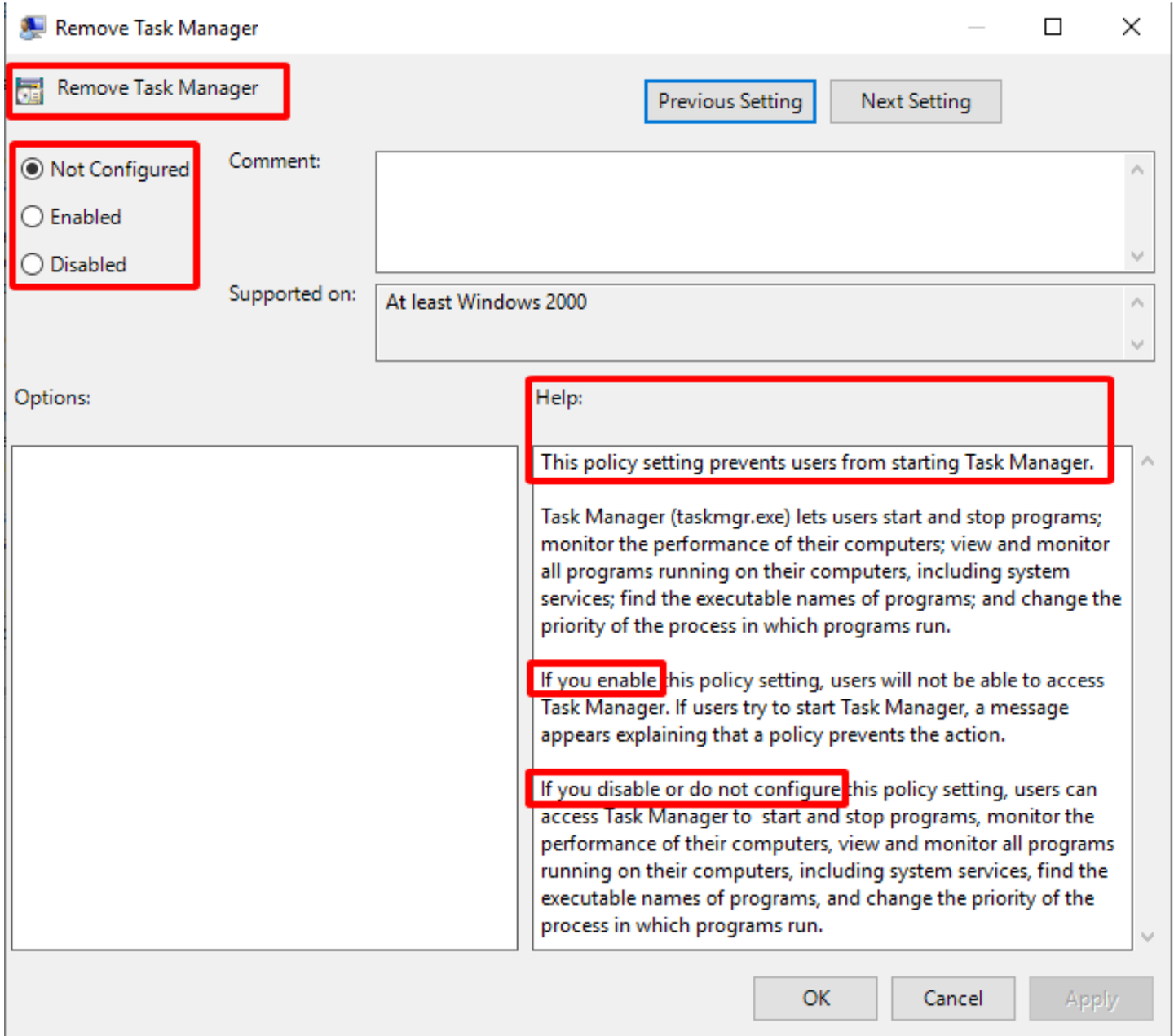
What are GPOs? (4 of 5)

- Thành phần chi tiết nhất của chính sách nhóm là một cài đặt chính sách riêng lẻ, định nghĩa cấu hình cụ thể, ví dụ chặn người dùng truy cập Task Manager
- Các cài đặt tác động đến người dùng, được gọi là cài đặt cấu hình người dùng hoặc chính sách người dùng
- Các cài đặt tác động đến máy tính, được gọi là cài đặt cấu hình máy tính hoặc chính sách máy tính



What are GPOs? (5 of 5)

- Chính sách nhóm quản lý các cài đặt chính sách khác nhau và khung chính sách nhóm có thể mở rộng. Có thể quản lý hầu hết mọi cài đặt bằng chính sách nhóm
- Hầu hết các cài đặt chính sách có thể có ba trạng thái: Not Configured (không được cấu hình), Enabled (được kích hoạt), và Disabled (không được kích hoạt)
- GPO lưu trữ cài đặt chính sách nhóm. Trong một GPO mới, mọi cài đặt chính sách đều được đặt mặc định là Not Configured



GPO scope

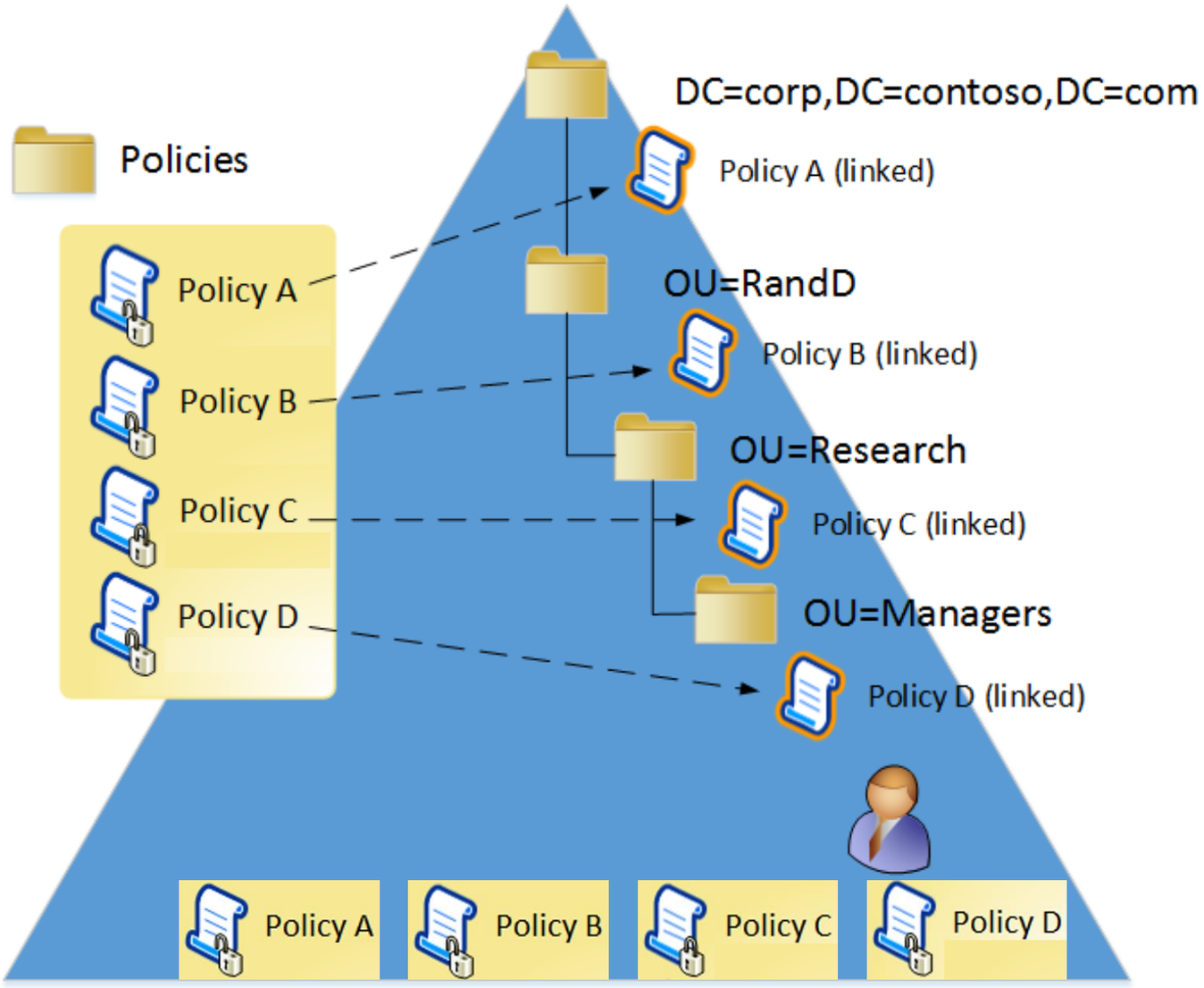
Phạm vi GPO được xác định bằng cách sử dụng:

- Liên kết GPO
  - Liên kết GPO với các địa điểm (site), miền (domain) và đơn vị tổ chức (OU) trong AD DS
  - Các cài đặt chính sách trong GPO chỉ định sẽ tác động đến tất cả máy tính và người dùng trong các địa điểm, miền hoặc OU, và các đối tượng của OU con.
  - Có thể liên kết một GPO với nhiều miền, OU hoặc địa điểm.
- Bộ lọc bảo mật: Chỉ định các nhóm bảo mật hoặc người dùng hoặc đối tượng máy tính liên quan đến phạm vi của GPO, nên hoặc không nên được áp dụng rõ ràng
- Bộ lọc WMI (Windows Management Instrumentation): sử dụng các đặc điểm của hệ thống, chẳng hạn như phiên bản hệ điều hành hoặc dung lượng bộ nhớ trống

Sử dụng bộ lọc bảo mật và bộ lọc WMI để thu hẹp hoặc chỉ định phạm vi áp dụng trong phạm vi ban đầu mà liên kết GPO đã tạo

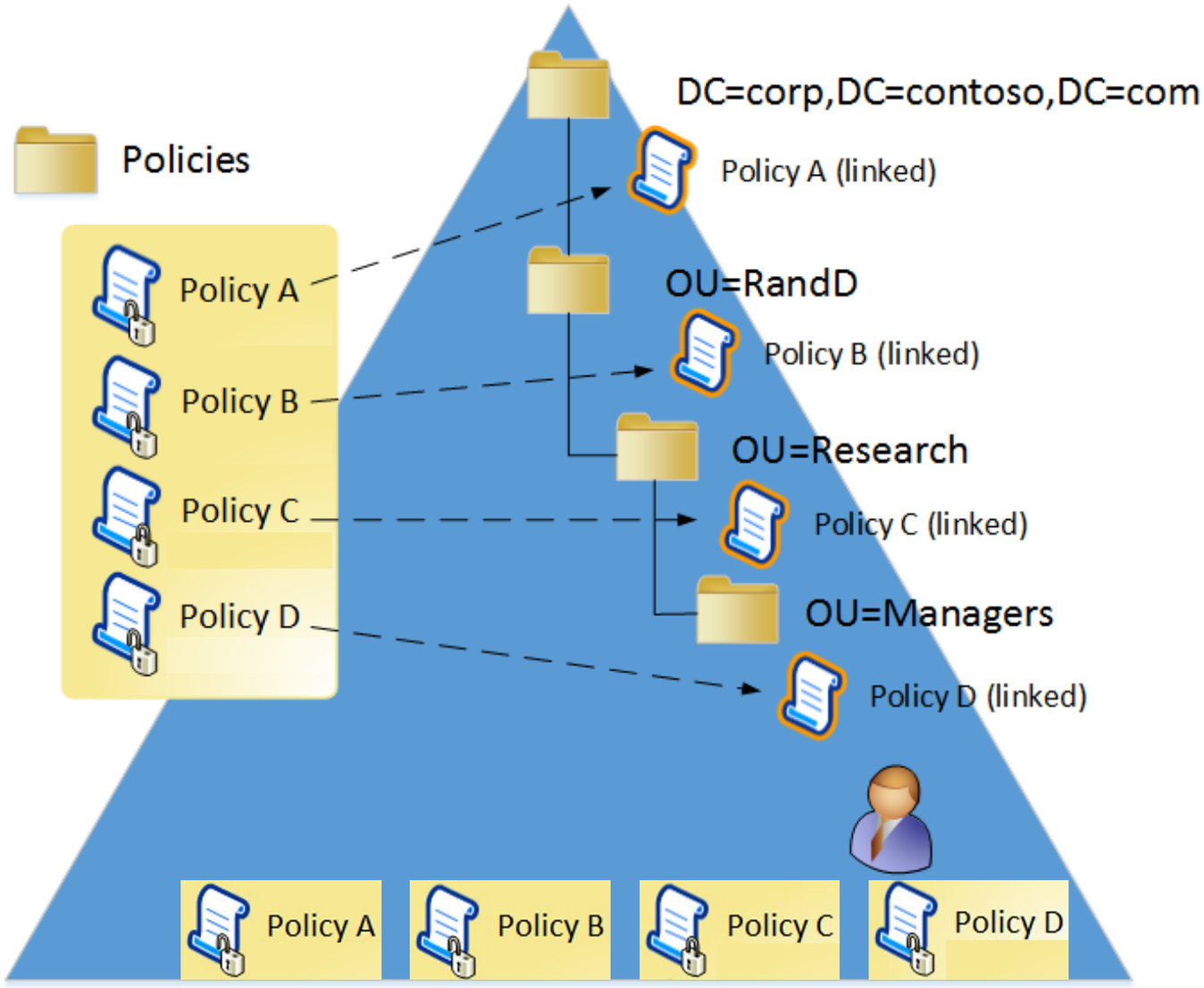
GPO processing order and inheritance (1 of 4)

- GPO áp dụng cho người dùng, máy tính hoặc cả hai không được áp dụng cùng một lúc
- Chính sách nhóm tuân theo bậc xử lý phân cấp:
  1. GPO cục bộ. Mỗi máy tính có ít nhất một chính sách cục bộ
  2. GPO được liên kết với địa điểm
  3. GPO được liên kết với miền
  4. GPO được liên kết với OU
  5. GPO được liên kết với OU con: Khi có nhiều cấp độ OU con, chính sách dành cho OU có độ ưu tiên cao hơn sẽ áp dụng trước



GPO processing order and inheritance (2 of 4)

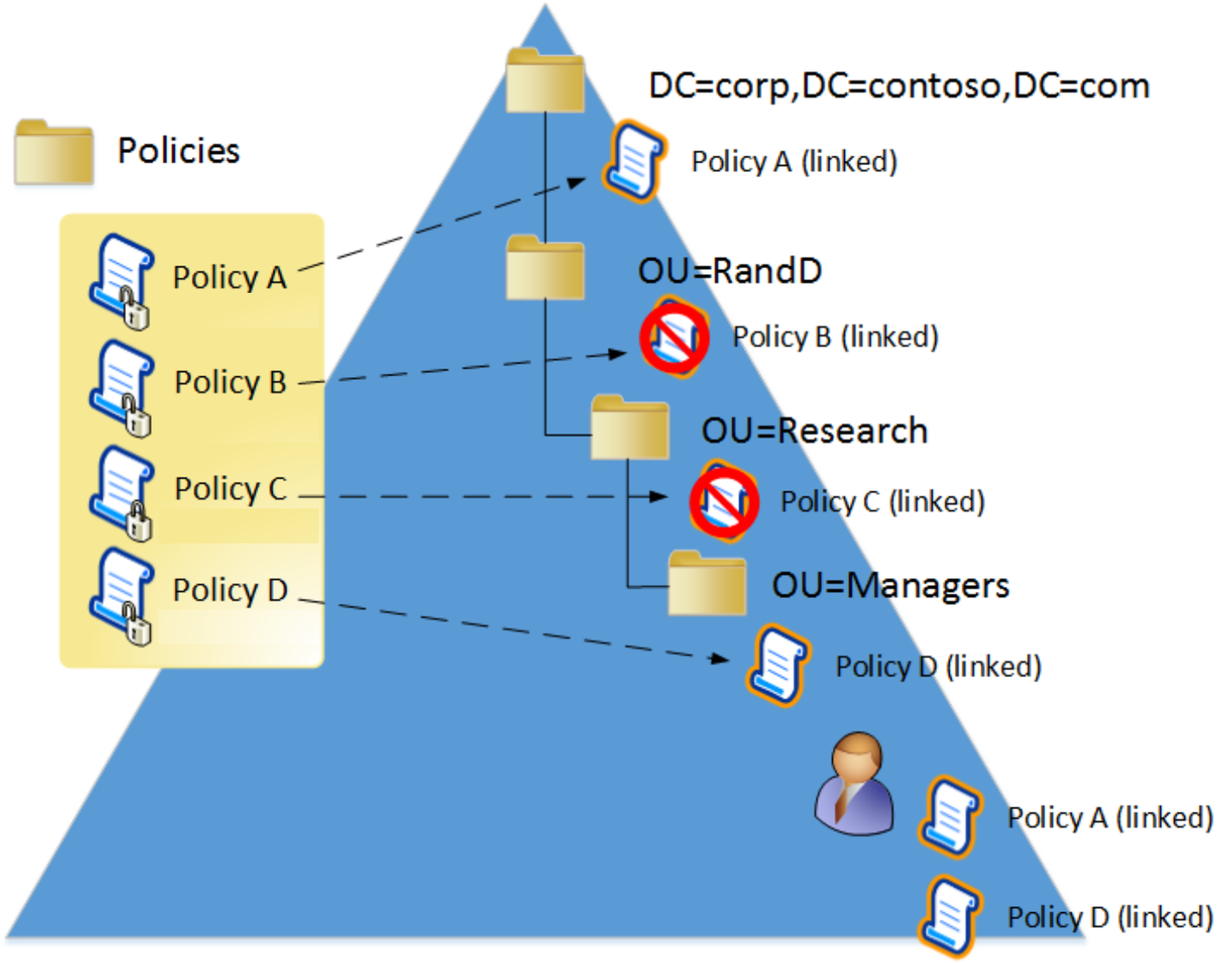
- Có thể cấu hình cài đặt chính sách trong nhiều GPO, nhưng điều này có thể dẫn đến việc các GPO xung đột với nhau
- Các cài đặt xung đột xử lý sau có thể ghi đè lên các cài đặt xử lý trước
- Nguyên tắc chung là chính sách sau được áp dụng sẽ có độ ưu tiên cao hơn



GPO processing order and inheritance (3 of 4)

- Thứ tự ưu tiên của các GPO xác định cài đặt chính sách mà người dùng/máy tính được áp dụng. GPO có độ ưu tiên cao hơn sẽ chiếm ưu thế so với GPO có độ ưu tiên thấp hơn
- Ví dụ: Chính sách A hạn chế truy cập vào Task Manager (TM) trong khi Chính sách D cho phép

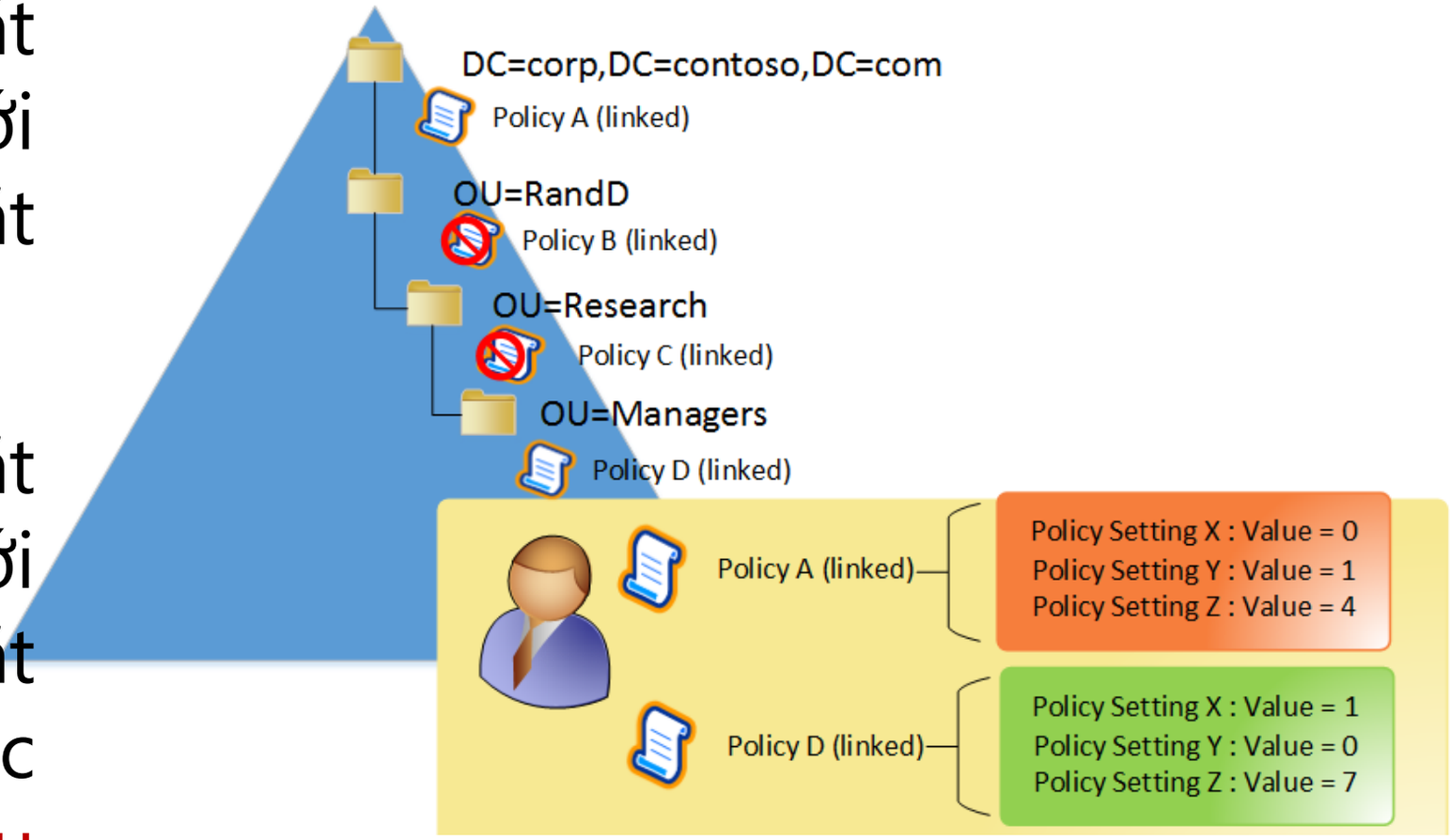
→ Chính sách A ở cấp miền bị ghi đè bởi chính sách D ở cấp OU



GPO processing order and inheritance (3 of 4)

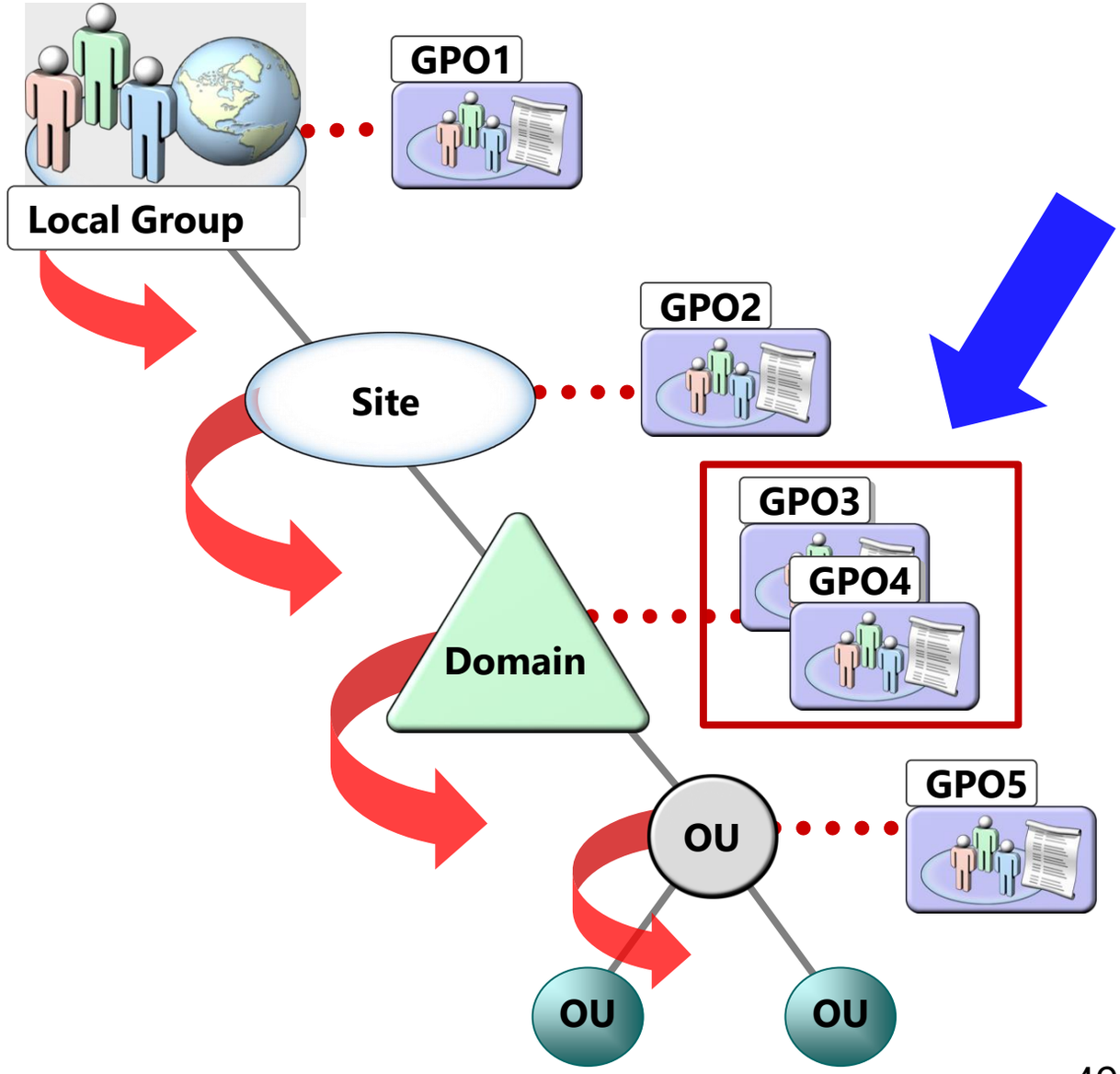
Khi bật hoặc tắt cài đặt chính sách trong GPO với độ ưu tiên cao hơn, cài đặt này sẽ có hiệu lực

Nếu không cấu hình cài đặt chính sách trong GPO với độ ưu tiên cao hơn, cài đặt chính sách, được bật hoặc tắt, trong GPO với độ ưu tiên thấp hơn sẽ có hiệu lực



GPO processing order and inheritance (4 of 4)

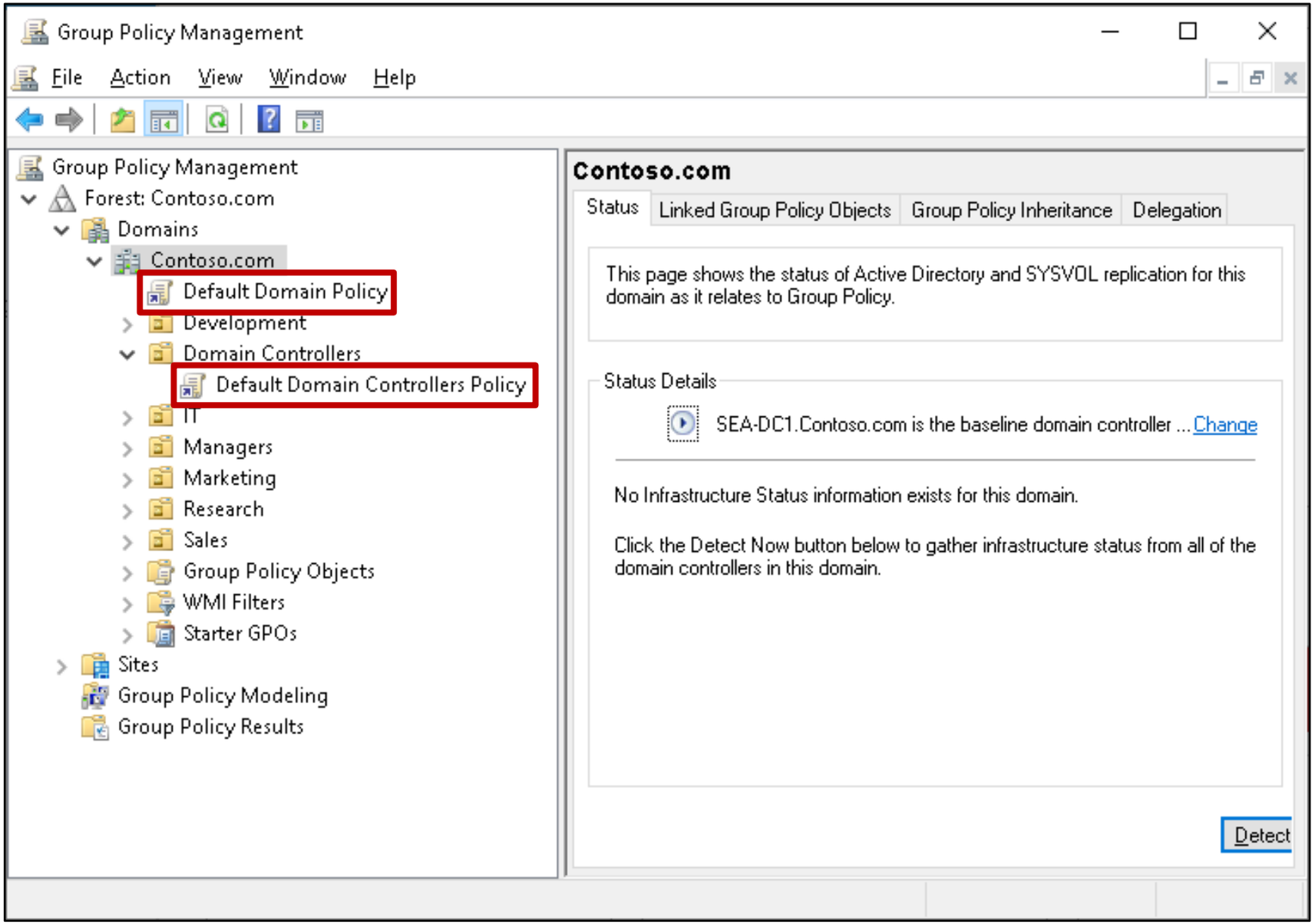
- Ví dụ: Cả hai GPO3 và GPO4 đều được áp dụng tại miền. GPO nào chiếm ưu thế (được ưu tiên trước)?
- Thứ tự ưu tiên của các chính sách được liệt kê trong **Group Policy Inheritance**, và điều chỉnh thứ tự ưu tiên cùng cấp tại **Linked GPO**
- Công cụ quản lý chính sách có chỉ số ưu tiên cho các chính sách. Số càng nhỏ, càng tiến về 1, độ ưu tiên càng cao



Block inheritance and Enforce a GPO link

- Có thể cấu hình miền hoặc OU để ngăn việc kế thừa cài đặt chính sách. Điều này được gọi là chặn kế thừa (Block Inheritance)
- Tùy chọn Block Inheritance là một thuộc tính của miền hoặc OU, do đó, nó chặn tất cả các cài đặt chính sách nhóm từ các GPO liên kết với cha-mẹ trong phân cấp chính sách nhóm
- Có thể đặt liên kết GPO được Enforced (thực thi với độ ưu tiên cao hơn so với những liên kết không được Enforced)
- Khi đặt một liên kết GPO thành Enforced, GPO sẽ có mức độ ưu tiên cao nhất. Cài đặt chính sách trong GPO đó sẽ chiếm ưu thế so với bất kỳ cài đặt chính sách xung đột nào trong các GPO khác. Hơn nữa, một liên kết được Enforced sẽ áp dụng cho các bộ chứa con ngay cả khi các vùng chứa đó được đặt Block Inheritance.

What are domain-based GPOs?



Default domain GPOs

- Chính sách miền mặc định
  - Liên kết với miền và áp dụng cho người dùng đã được xác thực
  - Tác động đến tất cả người dùng và máy tính trong miền
  - Chứa các cài đặt chính sách chỉ định mật khẩu, khóa tài khoản và chính sách giao thức xác thực Kerberos phiên bản 5
  - Không nên thêm các cài đặt chính sách không liên quan vào GPO này. Nếu cần các cài đặt khác để áp dụng trong miền, hãy tạo các GPO khác liên kết với miền
- Chính sách Máy chủ điều khiển miền mặc định
  - Liên kết với OU của Máy chủ điều khiển miền
  - GPO này chỉ tác động đến các Máy chủ điều khiển miền hoặc các đối tượng máy tính khác trong OU của Máy chủ điều khiển miền

Minh hoạ: Công cụ Group Policy Management

- GPO dựa trên miền và GPO mặc định
- Phạm vi GPO
- Thứ tự xử lý GPO và kế thừa
- Chặn kế thừa và Enforce liên kết GPO
- Tạo, chỉnh sửa và liên kết GPO

Hoạt động nhóm số 6 – GPO cơ bản

Quản trị lớp học MMT và TTDL của Trường ĐHCNHN dựa trên HĐH Windows với đặc điểm và yêu cầu như sau:

- Mỗi nhóm giảng viên và nhóm sinh viên được cấp các tài khoản:
  - gv1 – Giangvien1; gv2 – Giangvien2; sv1 – Sinhvien1; sv2 – Sinhvien2
- Chặn sinh viên mở Task Manager

Hoạt động nhóm số 7 – Phạm vi GPO

Quản trị lớp học MMT và TTDL của Trường ĐHCNHN dựa trên HĐH Windows với đặc điểm và yêu cầu như sau:

- Mỗi nhóm giảng viên và nhóm sinh viên được cấp các tài khoản:
  - gv1 – Giangvien1; gv2 – Giangvien2; sv1 – Sinhvien1; sv2 – Sinhvien2
- Chặn sinh viên mở Task Manager
- Cho phép giảng viên mở Task Manager
- Sử dụng 2 đơn vị tổ chức
- Kiểm tra kế thừa chính sách nhóm và thứ tự ưu tiên

Hoạt động nhóm số 8 – Thứ tự ưu tiên và kế thừa

Quản trị lớp học MMT và TTDL của Trường ĐHCNHN dựa trên HĐH Windows với đặc điểm và yêu cầu như sau:

- Mỗi nhóm giảng viên và nhóm sinh viên được cấp các tài khoản:
  - gv1 – Giangvien1; gv2 – Giangvien2; sv1 – Sinhvien1; sv2 – Sinhvien2
- Cho phép lớp học mở Task Manager (TM)
- Chặn sinh viên mở Task Manager
- Sử dụng 2 đơn vị tổ chức
- Sử dụng hai chính sách nhóm kích hoạt và không kích hoạt TM

Hoạt động nhóm số 9 – Chặn kế thừa, Enforce và ngắt liên kết GPO

Quản trị lớp học MMT và TTDL của Trường ĐHCNHN dựa trên HĐH Windows với đặc điểm và yêu cầu như sau:

- Mỗi nhóm giảng viên và nhóm sinh viên được cấp các tài khoản:
  - gv1 – Giangvien1; gv2 – Giangvien2; sv1 – Sinhvien1; sv2 – Sinhvien2
- Chặn lớp mở Task Manager (TM) nhưng cho phép giảng viên mở TM
- Sử dụng hai chính sách nhóm kích hoạt và không kích hoạt TM
- Chính sách không kích hoạt TM áp dụng vào toàn bộ lớp học
- Sau đó thực hiện: (1) chặn kế thừa tại OU sinh viên, (2) Enforce chính sách kích hoạt TM và (3) ngắt liên kết chính sách kích hoạt TM

Uỷ quyền tác vụ liên quan đến GPO

- Cho phép khối lượng công việc quản trị được phân phối trên toàn doanh nghiệp
- Tác vụ chính sách nhóm có thể được uỷ quyền độc lập trên người dùng hoặc nhóm người dùng, gồm:
  - Tạo GPOs
  - Chỉnh sửa GPOs
  - Quản lý liên kết chính sách nhóm cho địa điểm, miền, hoặc OU
  - Thực hiện phân tích mô hình hoá chính sách nhóm trong miền hoặc OU
  - Đọc dữ liệu kết quả chính sách nhóm trong miền hoặc OU
  - Tạo bộ lọc WMI trên miền

Hoạt động nhóm số 10 – Uỷ quyền

Quản trị lớp học MMT và TTDL của Trường ĐHCNHN dựa trên HĐH Windows với đặc điểm và yêu cầu như sau:

- Lớp học có 2 giảng viên và 4 sinh viên thuộc mỗi nhóm gồm 2 sinh viên, được cấp tài khoản:
  - sv1 – Sinhvien1; …; sv4 – Sinhvien4
  - gv1 – Giangvien1; gv2 – Giangvien2
- Tài khoản của giảng viên được uỷ quyền để thực hiện các vai trò sau:
  - Tạo, chỉnh sửa và liên kết chính sách nhóm tới lớp học
  - Chặn lớp mở Task Manager nhưng cho phép giảng viên mở TM
- Kiểm chứng tác vụ được và không được uỷ quyền

Hoạt động nhóm số 11 – Cài đặt bảo mật

Quản trị lớp học MMT và TTDL của Trường ĐHCNHN dựa trên HĐH Windows với đặc điểm và yêu cầu như sau:

- Mỗi nhóm giảng viên và nhóm sinh viên được cấp tài khoản theo chính sách bảo mật tài khoản sau:

Chính sách	Giảng viên	Sinh viên
Số lần đặt mật khẩu mới duy nhất trước khi có thể sử dụng lại mật khẩu cũ	5	10
Độ tuổi tối thiểu-tối đa của mật khẩu (ngày)	1->5	7->30
Số ký tự tối thiểu	11	10
Độ phức tạp của mật khẩu	Không	Có

- Kiểm chứng chính sách bằng cách tạo các tài khoản cho GV và SV

Hoạt động nhóm số 12 – Quản lý cài đặt ứng dụng máy tính

Quản trị lớp học MMT và TTDL của Trường ĐHCNHN dựa trên HĐH Windows với đặc điểm và yêu cầu như sau:

- Mỗi nhóm giảng viên và nhóm sinh viên được cấp các tài khoản:
  - gv1 – Giangvien1; gv2 – Giangvien2; sv1 – Sinhvien1; sv2 – Sinhvien2
- Thiết lập hình nền Desktop của tài khoản giảng viên và sinh viên khác nhau

Hoạt động nhóm số 13 – Triển khai cài đặt phần mềm

Quản trị lớp học MMT và TTDL của Trường ĐHCNHN dựa trên HĐH Windows với đặc điểm và yêu cầu như sau:

- Mỗi nhóm giảng viên và nhóm sinh viên được cấp các tài khoản:
  - gv1 – Giangvien1; gv2 – Giangvien2; sv1 – Sinhvien1; sv2 – Sinhvien2
- Triển khai cài đặt phần mềm 7-zip.msi xuống máy tính của giảng viên và tài khoản của sinh viên.

Hoạt động nhóm số 14 – Chuyển hướng thư mục

Quản trị lớp học MMT và TTDL của Trường ĐHCNHN dựa trên HĐH Windows với đặc điểm và yêu cầu như sau:

- Mỗi nhóm giảng viên và nhóm sinh viên được cấp các tài khoản:
  - gv1 – Giangvien1; gv2 – Giangvien2; sv1 – Sinhvien1; sv2 – Sinhvien2
- Thiết lập chính sách lưu trữ tập trung thư mục Documents của giảng viên và thư mục Downloads của sinh viên tại Máy chủ điều khiển miền

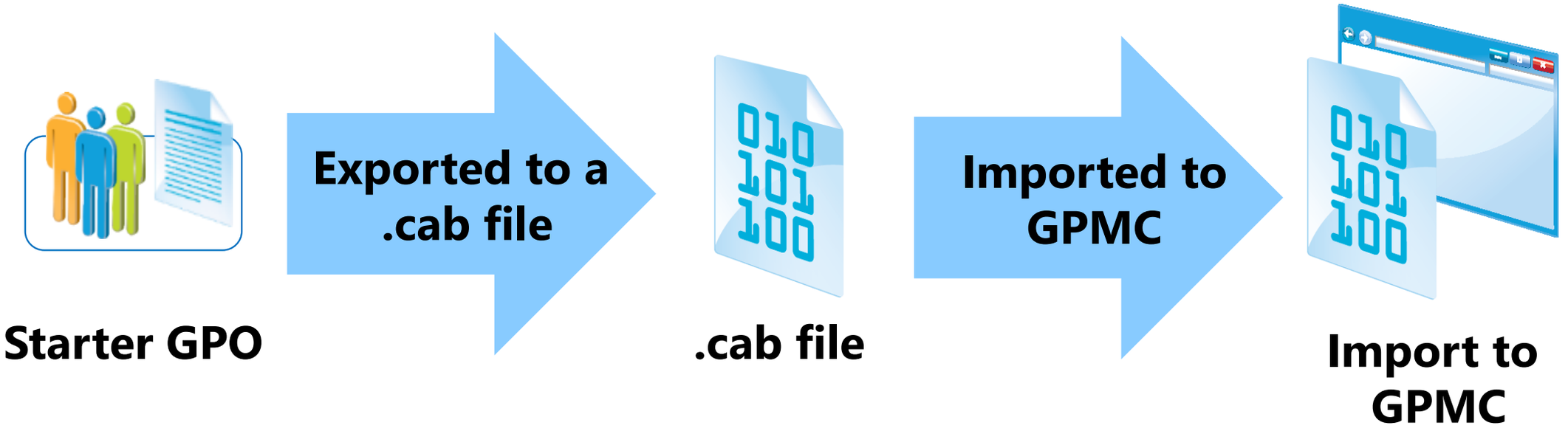
Overview of GPO storage and GPO replication

- Cài đặt chính sách nhóm được thể hiện dưới dạng GPO trong các công cụ giao diện người dùng AD DS, nhưng GPO thực sự gồm hai thành phần:
  - Bộ chứa chính sách nhóm (Group Policy container)
  - Mẫu chính sách nhóm (Group Policy template)
- Bộ chứa chính sách nhóm và mẫu chính sách nhóm đều sao chép giữa tất cả các Máy chủ điều khiển miền trong AD DS. Tuy nhiên, hai mục này sử dụng các cơ chế sao chép khác nhau:
  - Bộ chứa chính sách nhóm trong AD DS sao chép bởi Tác nhân sao chép thư mục (Directory Replication Agent)
  - Mẫu chính sách nhóm trong **SYSVOL** sao chép bằng cách sử dụng Sao chép hệ thống tập tin phân tán (Distributed File System Replication)
- Do bộ chứa chính sách nhóm và mẫu chính sách nhóm sao chép riêng biệt nên chúng có thể không đồng bộ trong một thời gian ngắn. Thông thường, khi điều này xảy ra, bộ chứa chính sách nhóm sẽ sao chép tới Máy chủ điều khiển miền trước

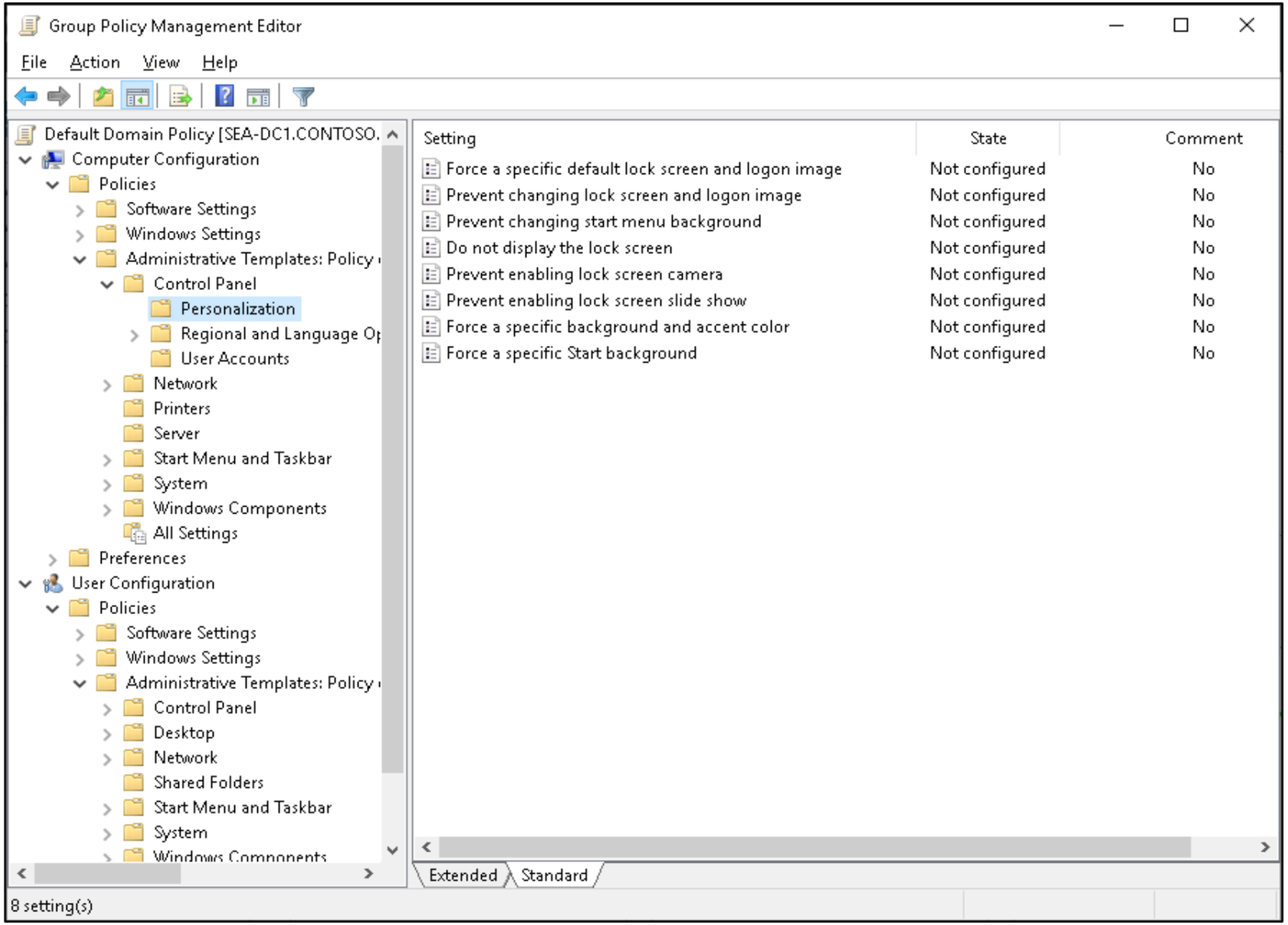
What are Starter GPOs?

Một Starter GPO:

- Lưu trữ các cài đặt mẫu quản trị mà các GPO mới sẽ dựa vào
- Có thể được xuất sang tệp .cab
- Có thể được nhập vào các khu vực khác của một tổ chức



What are administrative templates?



What are administrative templates?

- Các tệp mẫu quản trị cung cấp hầu hết các cài đặt GPO có sẵn, giúp sửa đổi các khóa đăng ký (registry keys) cụ thể
- Việc sử dụng các mẫu quản trị được gọi là chính sách dựa trên sổ đăng ký (registry-based policy), bởi vì tất cả các cài đặt cấu hình trong các mẫu quản trị đều dẫn đến các thay đổi tới sổ đăng ký (registry)
- Đối với nhiều ứng dụng, sử dụng chính sách dựa trên sổ đăng ký là cách đơn giản nhất và tốt nhất để hỗ trợ quản lý tập trung các cài đặt chính sách
- Có hai mẫu quản trị:
  - Cài đặt liên quan đến người dùng
  - Cài đặt liên quan đến máy tính
- Administrative Templates node: Control Panel, Network, Printers, Server, Start Menu and Taskbar, System, Windows Components, All Settings

Overview of the Central Store

Central Store:

- Là kho lưu trữ trung tâm cho các tệp .admx và .adml
- Được lưu trữ trong SYSVOL
- Phải được tạo thủ công
- Được phát hiện tự động bởi Windows Vista, Windows Server 2008 và các hệ điều hành mới hơn

Ưu điểm của việc tạo Central Store là:

- Bạn đảm bảo rằng bất cứ khi nào ai đó chỉnh sửa GPO, các cài đặt trong nút Mẫu quản trị luôn giống nhau
- Khi Microsoft phát hành các tệp .admx cho các hệ điều hành mới, bạn chỉ cần cập nhật các tệp .admx ở một vị trí

Lesson 5: Overview of AD CS

Thank you.