

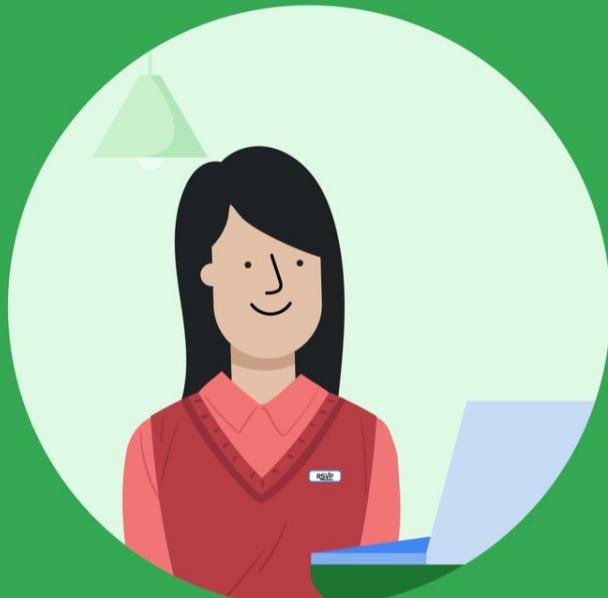


# Quản Trị Hệ Thống & Dịch vụ hạ tầng Công nghệ Thông tin

**Nhóm biên soạn:**

1. Lê Ngọc Thành
2. Phạm Trọng Nghĩa
3. Tạ Việt Phương
4. Trương Tấn Khoa

**Năm 2022**



# 1 Quản Trị Hệ Thống



# Quản trị viên hệ thống

- **Cơ sở hạ tầng CNTT** bao gồm **phần mềm, phần cứng, mạng** và các **dịch vụ** cần thiết để một tổ chức có thể hoạt động trong môi trường CNTT doanh nghiệp.
- **Quản trị viên hệ thống** (system administrator): người quản lý cơ sở hạ tầng CNTT của công ty.
- Quản trị viên hệ thống còn được gọi là **sysadmins**.



# Quản trị viên hệ thống

Sysadmins chịu trách nhiệm cho các dịch vụ CNTT của công ty:

- Email
- Lưu trữ tập tin
- Chạy trang web

**Máy chủ (Server):** nơi lưu trữ những dịch vụ này.

Sysadmins chịu trách nhiệm quản trị tất cả **máy chủ** của công ty.



# Máy chủ

**Máy chủ (Server):** phần mềm hoặc một máy cung cấp dịch vụ cho phần mềm khác hoặc máy khác.

Ví dụ:

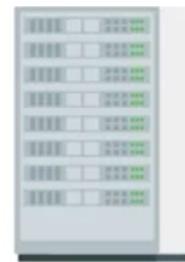
- Email server
- SSH server

**Máy khách (Client):** máy sử dụng dịch vụ của server.



# Máy chủ

- Bất kỳ máy tính nào cũng có thể là server.
- **Tower Server:** giống máy bàn.
- **Rack Server:** xếp chồng lên nhau bằng một giá đỡ.
- **Blade server:** mỏng hơn Rack.



Tower Server



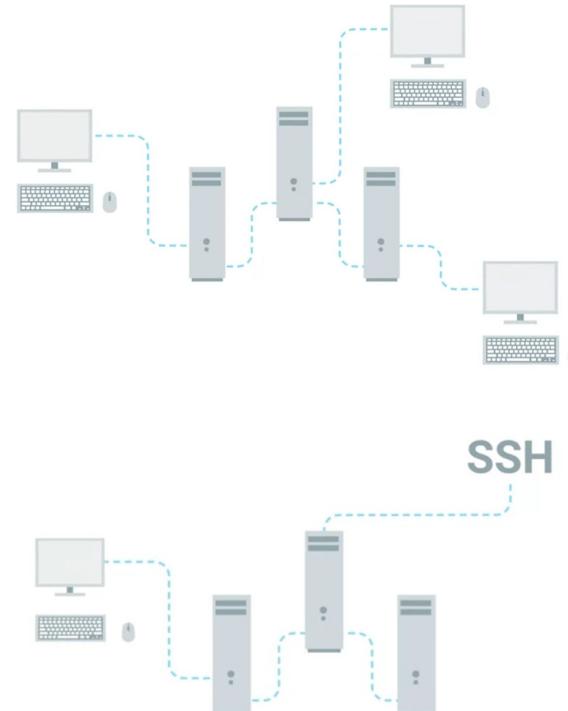
Rack Server



Blade Server

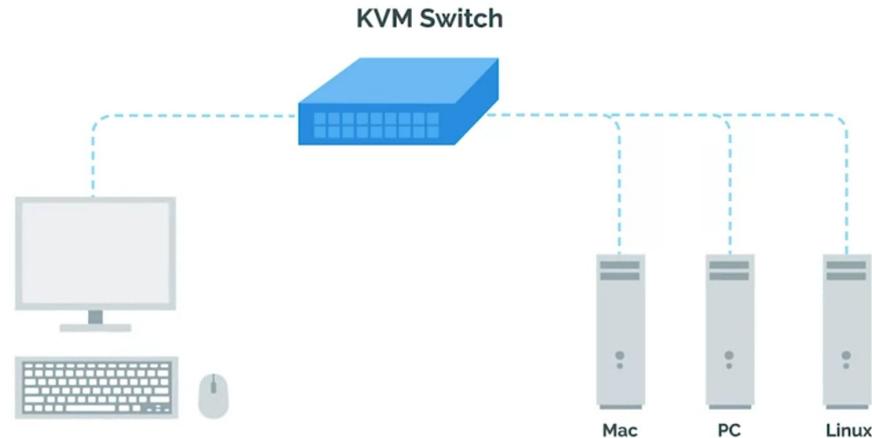
# Máy chủ

- Dùng bàn phím, chuột, màn hình để kết nối đến máy chủ.
- SSH: kết nối đến máy chủ từ xa.



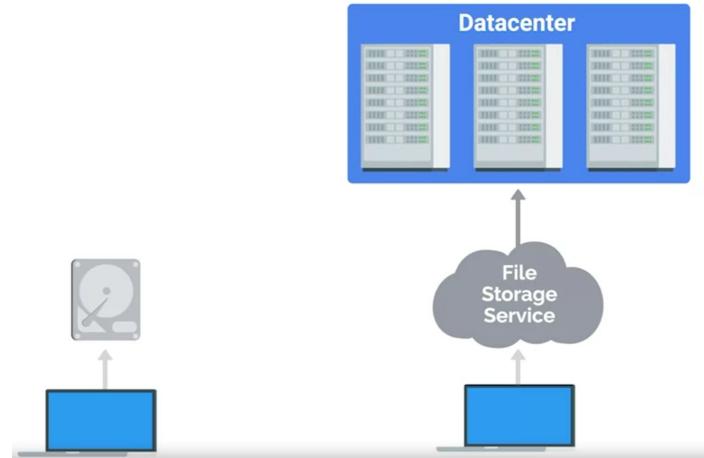
# KVM Switch

**KVM:** Keyboard (bàn phím), Video (màn hình), Mouse (chuột): thiết bị để kết nối nhiều máy tính và điều khiển bằng bàn phím, chuột và màn hình.



# Điện toán đám mây

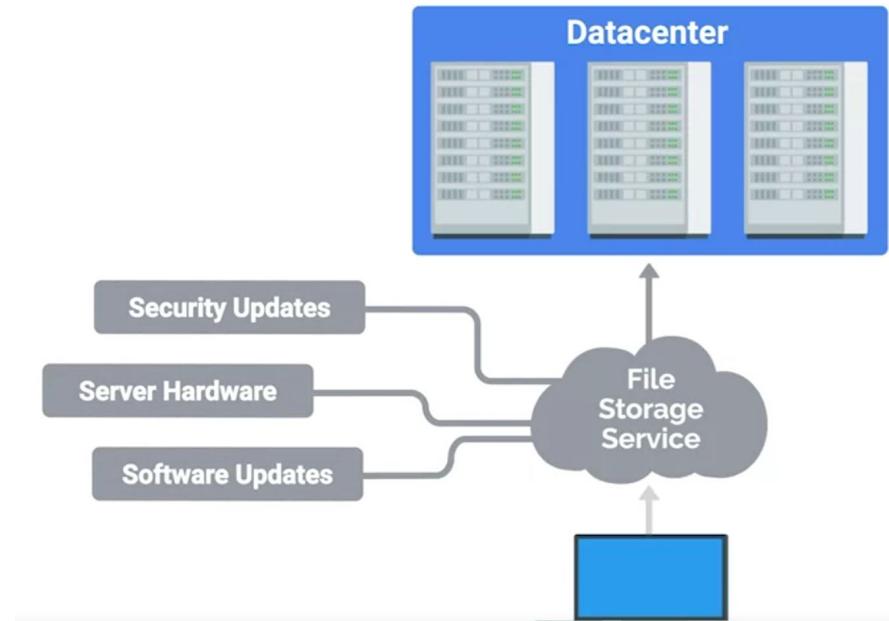
- **Điện toán đám mây:** có thể truy cập dữ liệu, sử dụng ứng dụng, lưu trữ file, v.v., từ mọi nơi trên thế giới miễn là bạn có kết nối internet.
- **Đám mây:** một mạng lưới các máy chủ lưu trữ và xử lý dữ liệu.
- **Trung tâm dữ liệu (data center):** cơ sở lưu trữ hàng trăm, hàng nghìn máy chủ.



# Điện toán đám mây

Sử dụng dịch vụ Internet để thực hiện các công việc của tổ chức như:

- Cập nhật bảo mật (security updates)
- Phần cứng máy chủ (server hardware),
- Cập nhật phần mềm (software update)



# Khuyết điểm của đám mây

## Chi phí:

- Tự xây dựng máy chủ: chi phí ban đầu cao, chi phí hàng tháng thấp.
- Dùng đám mây: chi phí ban đầu nhỏ hơn, nhưng tốn chi phí hàng tháng tương đối.

## Sự phụ thuộc

- Phụ thuộc vào bên cung cấp dịch vụ.

Nên sao lưu trên đám mây lẫn ổ cứng của chính mình.



# Chính sách của tổ chức

**Chính sách của tổ chức:** quy định về bảo mật máy tính và quyền truy cập cho các người dùng.

Ví dụ về chính sách:

- Người dùng không được phép tự cài đặt phần mềm.
- Người dùng nên có mật khẩu phức tạp với một số điều kiện: Ký hiệu, Số ngẫu nhiên, Ký tự...
- Có cho phép nhân viên xem các trang web không liên quan đến công việc như Facebook hay không?
- Thiết lập mật khẩu nếu giao điện thoại của công ty cho nhân viên.



# Quản trị người dùng và phần cứng

## Quản lý người dùng

- Tạo người dùng mới
- Cấp phép truy cập
- Xóa người dùng

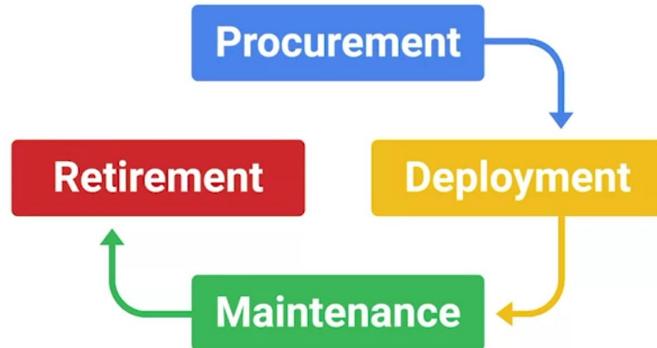
## Quản lý phần cứng

- Máy tính có khả năng đăng nhập
- Có đủ phần mềm cần thiết
- Máy tính được chuẩn hóa



# Vòng đời phần cứng

- **Mua sắm (Procurement)**: phần cứng được mua hoặc sử dụng lại.
- **Triển khai (Deployment)**: phần cứng được thiết lập, cài đặt.
- **Bảo trì (Maintenance)**: phần mềm được cập nhật và các sự cố phần cứng được khắc phục.
- **Nghỉ hưu (Retirement)**: loại bỏ phần cứng khi không còn sử dụng nữa.



# Bảo trì định kỳ

## Bảo trì định kỳ (Routine Maintenance)

- Cập nhật phần mềm bảo mật.

## Cập nhật hàng loạt (batch update)

- Cập nhật phần mềm cho tất cả các máy vào một khung thời gian xác định trước.



# Làm việc với nhà cung cấp

- Quản trị viên hệ thống cần mua sắm cài đặt các thiết bị CNTT:
  - Máy in, điện thoại, Máy fax, thiết bị nghe nhìn.
- Bảo đảm có người sửa chữa các thiết bị tại công ty.
- Tạo mối quan hệ với các nhà cung cấp thiết bị.
- Cần sự chấp thuận chính thức từ người quản lý để thiết lập mối quan hệ này.



# Khắc phục sự cố và quản lý lỗi

- Quản trị viên hệ thống: khắc phục sự cố và ưu tiên các vấn đề ở quy mô lớn.
- Hai kỹ năng quan trọng:
  - ❑ Tìm ra vấn đề: đặt câu hỏi, cô lập vấn đề, xem file log.
  - ❑ Dịch vụ khách hàng: thể hiện sự đồng cảm, giọng nói phù hợp,...
- Giám sát dịch vụ và thông báo trong trường hợp có sự cố.
- Theo dõi quá trình khắc phục sự cố
  - ❑ Hệ thống vé (ticketing system).



# Trách nhiệm của quản trị viên hệ thống

Quản trị viên hệ thống có trách nhiệm rất lớn.

Một số lưu ý:

- Tránh sử dụng quyền của quản trị viên cho các tác vụ không cần thiết.
- Tôn trọng quyền riêng tư của người khác.
- Suy nghĩ kỹ trước khi gõ.
- Lên kế hoạch trước khi tiến hành.
- Luôn sẵn sàng để rollback.



# Không thử nghiệm trong môi trường thực thi

- **Môi trường thực thi (production):** phần của cơ sở hạ tầng nơi các dịch vụ nhất định được thực thi và phục vụ cho người dùng.
- **Môi trường thử nghiệm (test environment):** máy ảo chạy cùng cấu hình với môi trường thực thi, nhưng không thực sự phục vụ bất kỳ người dùng nào?
- Kiểm tra trên môi trường thử nghiệm trước  môi trường thực thi.



# Không thử nghiệm trong môi trường thực thi

- **Máy phụ hoặc máy dự phòng:** giống hệt như máy thực thi, nhưng nó sẽ không nhận bất kỳ lưu lượng truy cập nào từ người dùng thực tế.
- Khi muốn thay đổi: Cập nhật máy phụ □ chuyển hoạt động từ máy chính sang máy phụ □ Cập nhật máy chính.
- Kỹ thuật thăm dò (canary):
  - ❑ Thực hiện thay đổi ở một nhóm nhỏ các máy chủ.
  - ❑ Nếu ổn, tiến hành thay đổi trên các máy chủ còn lại.
- **Lưu ý:** luôn thực hiện thay đổi ở môi trường thử nghiệm trước.



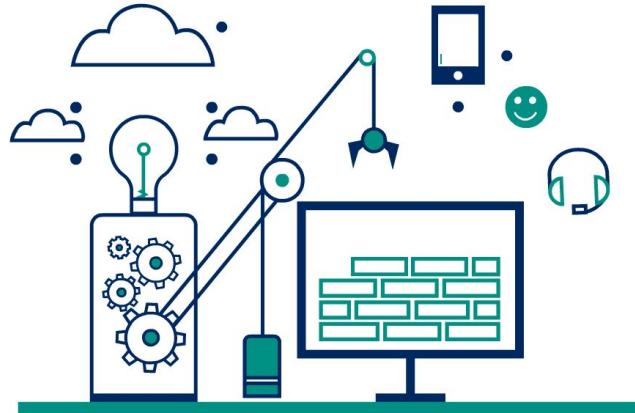
# Đánh giá rủi ro

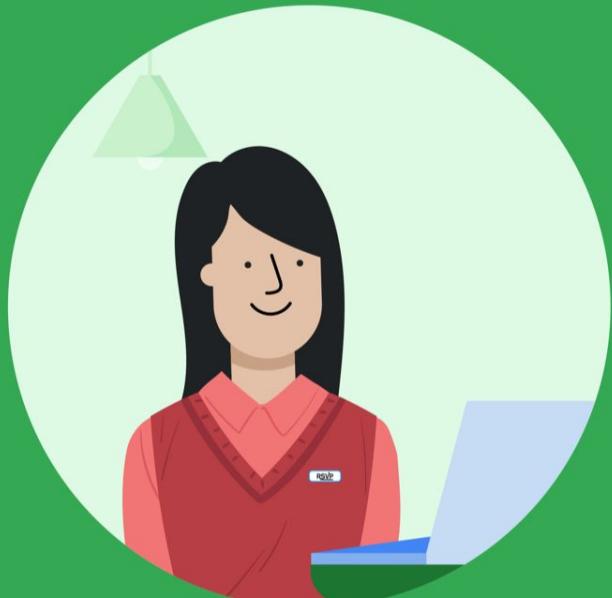
- **Đánh giá mức độ rủi ro:** mức độ quan trọng của các dịch vụ đối với cơ sở hạ tầng và số lượng người dùng bị ảnh hưởng nếu dịch vụ gặp sự cố.
  - ❑ Dịch vụ quan trọng: xác thực người dùng, hệ thống sao lưu.
  - ❑ Dịch vụ ít quan trọng hơn: hệ thống ticketing nội bộ.
- Dịch vụ càng nhiều người dùng, càng đảm bảo các thay đổi không gây gián đoạn.
- Dịch vụ càng quan trọng đối với hoạt động của công ty, càng làm việc nhiều hơn để duy trì dịch vụ.



# Phương pháp chung để khắc phục sự cố

- **Tái tạo vấn đề (Reproduction Case).** Tạo ra một lộ trình để dẫn đến kết quả không mong muốn.
  - ❑ Bạn đã thực hiện những bước nào để đến được trạng thái này?
  - ❑ Kết quả không mong muốn hoặc xấu là gì?
  - ❑ Kết quả mong đợi là gì?
- Sau khi áp dụng bản sửa lỗi: thực hiện lại các bước tương tự đã đưa bạn đến sự cố vào lúc trước để xem bản sửa lỗi có đúng hay chưa.





## 2 Dịch Vụ Mạng và Cơ Sở Hạ Tầng



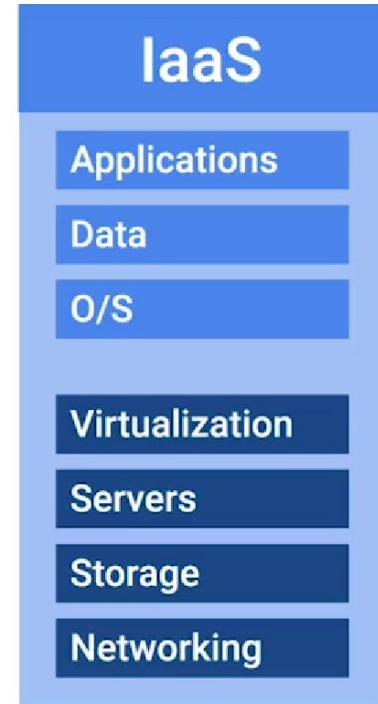
# Các loại dịch vụ cơ sở hạ tầng CNTT

- Dịch vụ cơ sở hạ tầng (Infrastructure as a Service - IaaS).
- Mạng dưới dạng dịch vụ (Networking as a Service - NaaS).
- Phần mềm dưới dạng dịch vụ (Software as a Service - SaaS).
- Nền tảng dưới dạng dịch vụ (Platform as a Service - PaaS).
- Thư mục dưới dạng Dịch vụ (Directory as a Service - DaaS).



# Dịch vụ cơ sở hạ tầng

- **Dịch vụ cơ sở hạ tầng (IaaS):** đám mây cung cấp tài nguyên cơ sở hạ tầng CNTT qua Internet.
- Nhà cung cấp IaaS: cung cấp máy ảo được cấu hình để sử dụng như máy vật lý.
- Các nhà cung cấp IaaS lớn:
  - ❑ Amazon Web Services
  - ❑ Linode
  - ❑ Windows Azure
  - ❑ Google Compute Engine



# Mạng dưới dạng dịch vụ

- **Mạng dưới dạng dịch vụ (NaaS):** dịch vụ Đám mây cho phép khách hàng thuê các dịch vụ mạng từ nhà cung cấp.
- Ví dụ về dịch vụ mạng:
  - ❑ Thiết lập bảo mật mạng
  - ❑ Quản lý việc định tuyến
  - ❑ Thiết lập mạng WAN, LAN



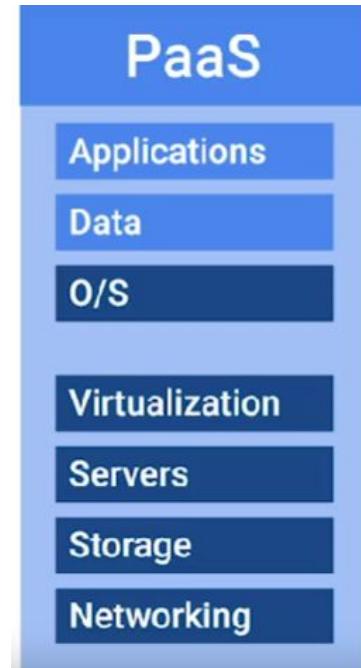
# Phần mềm dưới dạng Dịch vụ

- Phần mềm dưới dạng Dịch vụ (SaaS): dịch vụ đám mây cung cấp phần mềm cho bạn.
- Ví dụ SaaS:
  - ❑ Microsoft Office 365
  - ❑ Google G suite



# Nền tảng dưới dạng dịch vụ

- **Nền tảng dưới dạng Dịch vụ (PaaS):** Đám mây cung cấp nền tảng cho nhu cầu của bạn.
- Ví dụ về nền tảng để xây dựng trang web:
  - ❑ Môi trường lập trình.
  - ❑ Cơ sở dữ liệu
  - ❑ Máy chủ Web
- Nền tảng PaaS nổi tiếng: Heroku, Windows Azure, và Google App Engine



# Thư mục dưới dạng dịch vụ

- **Thư mục dưới dạng Dịch vụ (DaaS):** Đám mây cung cấp các dịch vụ thư mục.
- Ví dụ về dịch vụ thư mục:
  - ❑ Quản lý người dùng
  - ❑ Truy cập (access)
  - ❑ Xác thực (authorization)
- Phần mềm dịch vụ thư mục: Windows Active Directory, OpenLDAP.



# Hệ điều hành máy chủ

Hệ điều hành máy chủ (server operating system): hệ điều hành chuyên biệt, được tối ưu hóa cho máy chủ.

- Nhiều kết nối mạng hơn, dung lượng RAM lớn hơn.
- Bảo mật hơn.
- Đi kèm với nhiều dịch vụ có sẵn.

Ví dụ:

- Windows Server.
- Ubuntu server.
- Mac OS Server.



# Ảo hóa

Hai cách để chạy dịch vụ:

- Trên phần cứng chuyên dụng.
- Trên một phiên bản ảo hóa.

Ảo hóa một máy chủ:

- Đặt nhiều phiên bản ảo trên một máy chủ.
- Mỗi phiên bản chứa một dịch vụ.



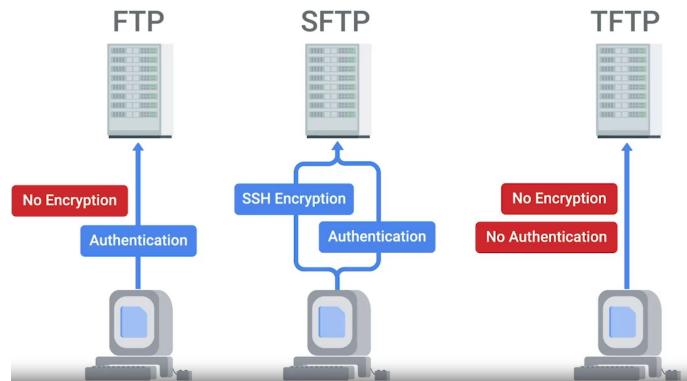
# Ảo hóa

- **Hiệu suất:** phần cứng chuyên dụng tốt hơn.
- **Chi phí:** ảo hóa tốt hơn.
  - Do tận dụng tài nguyên tốt hơn.
- **Bảo trì:** ảo hóa tốt hơn.
  - Nhanh chóng dừng dịch vụ hoặc di chuyển chúng sang một máy chủ vật lý khác.
- **Điểm thất bại (point of failure):** ảo hóa tốt hơn.
  - Dễ dàng di chuyển các dịch vụ ra khỏi một máy vật lý và tạo ra dịch vụ đó trên một máy khác.



# FTP, SFTP, và TFTP

- **Dịch vụ chia sẻ file:** dịch vụ chuyên biệt cho tác vụ chuyển file từ máy này sang máy khác trong tổ chức.
- FTP (File transfer protocol).
- SFTP (Secure FTP): phiên bản FTP bảo mật.
- TFTP (Trivial FTP): phiên bản đơn giản hơn của FTP, không yêu cầu xác thực người dùng.
  - ❑ Dùng cho PXE (Preboot Execution) boot.



# NTF

- Giao thức thời gian mạng (**Network Time Protocol - NTP**): đồng bộ hóa thời gian trên các máy được kết nối với mạng.
- Trong CNTT, máy móc cần có thời gian chính xác trên toàn mạng.
  - Dịch vụ bảo mật như Kerberos phụ thuộc vào thời gian nhất quán trên toàn hệ thống.
- Không thể phụ thuộc vào chính phần cứng: phải thiết lập một máy chủ NTP.



# NTF

Tự xây dựng máy chủ NTP.

- Cài đặt phần mềm máy chủ NTP trên máy chủ.
- Cài đặt các ứng dụng máy khách NTP và cho các máy tính đó biết dịch vụ NTP nào để đồng bộ.

Máy chủ NTP công cộng.

- Được quản lý bởi các tổ chức khác.
- Máy khách của bạn kết nối để đồng bộ hóa thời gian.

Phương pháp lai:

- Giống như phương pháp tự xây dựng máy chủ NTP.
- Máy chủ này liên kết với máy chủ NTP công cộng để đồng bộ thời gian.



# NTF

**Intranet:** là một **mạng nội bộ** bên trong một công ty.

- Truy cập được nếu bạn đang sử dụng mạng của công ty.
- Cung cấp cho nhân viên một phương tiện chia sẻ thông tin lớn hơn.

**Máy chủ proxy:** trung gian giữa mạng của công ty và Internet.

- Nhận lưu lượng mạng và chuyển tiếp đến mạng công ty.
- Truy cập mạng của công ty được giữ kín với Internet.
- Giám sát và ghi nhật ký hoạt động mạng nội bộ.
- Lọc truy cập trang web.
- Cung cấp quyền riêng tư và bảo mật trên Internet.

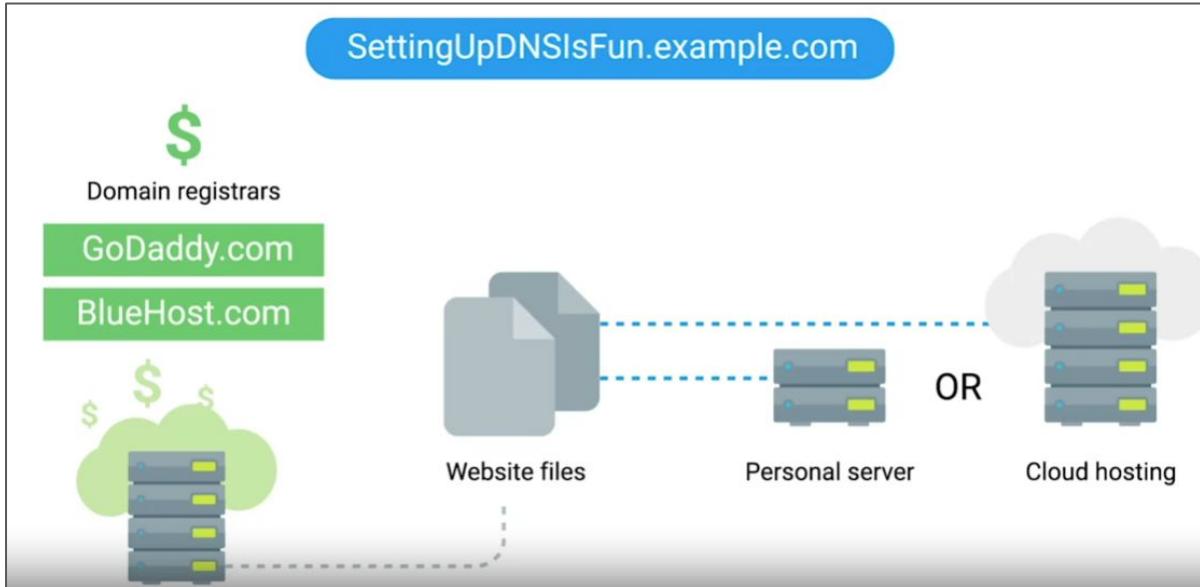


# DNS

- **Domain Name System (DNS)**: ánh xạ các tên dễ hiểu bởi con người sang các địa chỉ IP.
- Dịch vụ mạng tối quan trọng để thiết lập và duy trì khi quản lý cơ sở hạ tầng CNTT của công ty.
- Tại sao bạn cần thiết lập dịch vụ DNS của riêng mình:
  - Đang chạy một dịch vụ web
  - Kết nối từ xa (remote control)



# DNS cho máy chủ Web



# DNS cho mạng nội bộ

- Ánh xạ máy tính nội bộ tới các địa chỉ IP.
- Sử dụng local host file.
- Host file nằm ở etc/hosts. Nó có địa chỉ IP 127.0.0.1 trả đến localhost.

```
devan@devan-server: ~/Desktop
127.0.0.1      localhost
# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
~
~
```

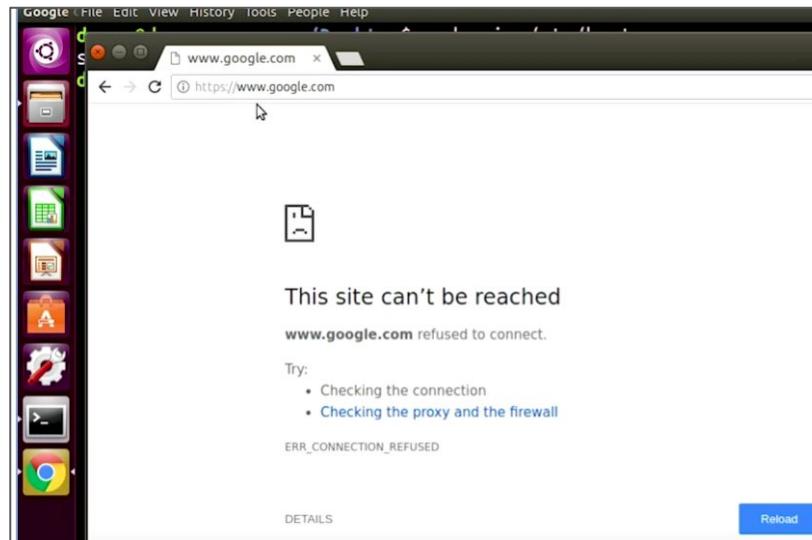
# DNS cho mạng nội bộ

Thay đổi localhost thành www.google.com như trong hình.

```
devan@devan-server: ~/Desktop
127.0.0.1      www.google.com
# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

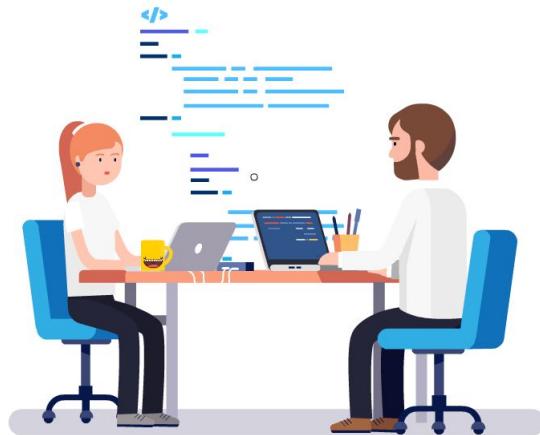
# DNS cho mạng nội bộ

Mở trình duyệt web và gõ vào www.google.com



# DNS cho mạng nội bộ

- Phương pháp dùng host file không thể mở rộng cho những hệ thống lớn.
- Thiết lập một máy chủ DNS cục bộ: lưu trữ thông tin tập trung hơn.
- Sau đó, thay đổi cài đặt mạng để các máy tính sử dụng máy chủ DNS này thay vì máy chủ DNS do ISP cung cấp.
- Máy chủ DNS cục bộ có thể được tích hợp với dịch vụ thư mục
  - ❑ Thực hiện tự động việc gán IP và tên.



# DHCP

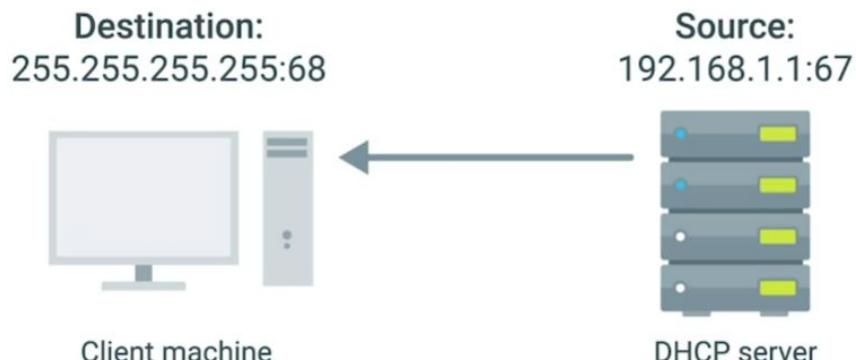
Địa chỉ IP tĩnh:

- Nhập thủ công địa chỉ IP vào cài đặt mạng.

Dùng DHCP: thuê địa chỉ IP từ máy chủ DHCP.

- Tự động nhận địa chỉ IP.

Khi mở rộng dải địa chỉ IP: diễn ra tự động.



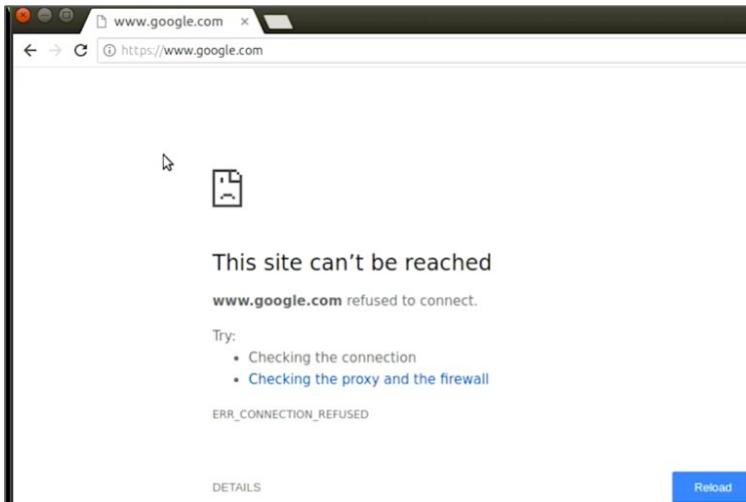
# DHCP

- Cấu hình máy chủ DHCP:
  - ❑ Xác định dải IP.
  - ❑ Địa chỉ của các máy chủ DNS cục bộ.
  - ❑ Gateway và subnet mask.
- Windows Server được tích hợp sẵn dịch vụ DHCP.
- Bật máy chủ DHCP + máy khách được thiết lập DHCP hoạt động.
- DHCP + DNS: DHCP cho thuê địa chỉ, DNS tự động cập nhật ánh xạ địa chỉ IP.



# Không thể phân giải tên máy chủ hoặc tên miền

Không thể truy cập đến Google



# Không thể phân giải tên máy chủ hoặc tên miền

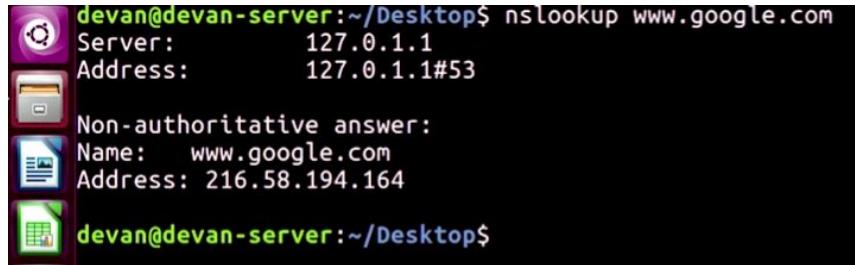
Gõ trong Terminal: `ping www.google.com`

```
devan@devan-server:~/Desktop$ ping www.google.com
PING www.google.com (127.1.1.3) 56(84) bytes of data.
64 bytes from www.google.com (127.1.1.3): icmp_seq=1 ttl=64 time=0.021 ms
64 bytes from www.google.com (127.1.1.3): icmp_seq=2 ttl=64 time=0.048 ms
64 bytes from www.google.com (127.1.1.3): icmp_seq=3 ttl=64 time=0.030 ms
64 bytes from www.google.com (127.1.1.3): icmp_seq=4 ttl=64 time=0.033 ms
^C
--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3065ms
rtt min/avg/max/mdev = 0.021/0.033/0.048/0.009 ms
devan@devan-server:~/Desktop$
```

Có nhận phản hồi

# Không thể phân giải tên máy chủ hoặc tên miền

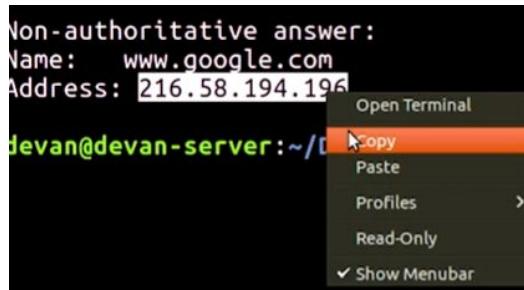
Gõ trong Terminal: `nslookup www.google.com`



```
devan@devan-server:~/Desktop$ nslookup www.google.com
Server:      127.0.1.1
Address:     127.0.1.1#53

Non-authoritative answer:
Name:   www.google.com
Address: 216.58.194.164

devan@devan-server:~/Desktop$
```



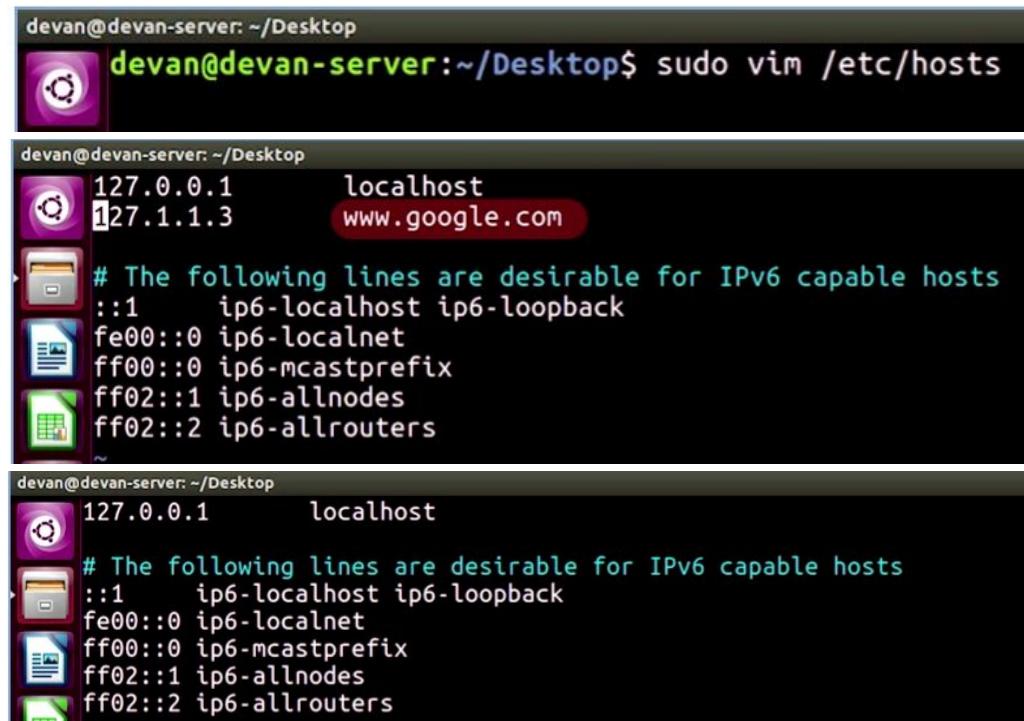
# Không thể phân giải tên máy chủ hoặc tên miền

Gõ trong Terminal: ping www.google.com

```
devan@devan-server: ~/Desktop
devan@devan-server:~/Desktop$ ping www.google.com
PING www.google.com (127.1.1.3) 56(84) bytes of data.
64 bytes from www.google.com (127.1.1.3): icmp_seq=1 ttl=64 time=0.022 ms
64 bytes from www.google.com (127.1.1.3): icmp_seq=2 ttl=64 time=0.038 ms
64 bytes from www.google.com (127.1.1.3): icmp_seq=3 ttl=64 time=0.039 ms
^C
--- www.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2025ms
rtt min/avg/max/mdev = 0.022/0.033/0.039/0.007 ms
devan@devan-server:~/Desktop$
```

# Không thể phân giải tên máy chủ hoặc tên miền

Mở host file

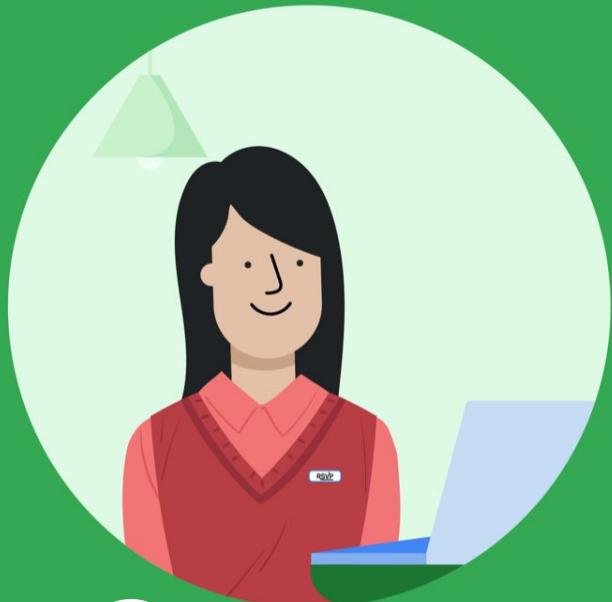


The screenshot shows a terminal session on a Linux system named 'devan'. The user has opened a terminal window and run the command `sudo vim /etc/hosts`. A dashed green box highlights the text 'Mở host file' (Open hosts file) on the left side of the slide, pointing to the terminal window.

```
devan@devan-server: ~/Desktop
devan@devan-server:~/Desktop$ sudo vim /etc/hosts

devan@devan-server: ~/Desktop
127.0.0.1      localhost
127.1.1.3      www.google.com
# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

devan@devan-server: ~/Desktop
127.0.0.1      localhost
# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

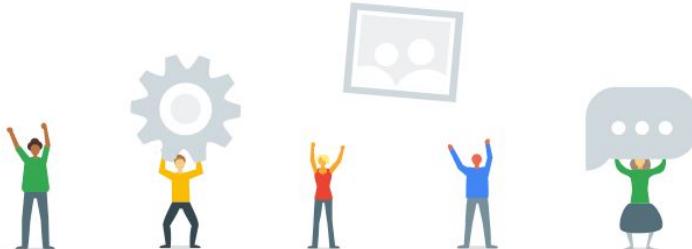


# 3 Các Dịch Vụ Nền Tảng và Phần Mềm



# Dịch vụ nền tảng và phần mềm

- **Dịch vụ phần mềm:** các dịch vụ mà nhân viên sử dụng để thực hiện các công việc hàng ngày.
- **Các dịch vụ nền tảng:** cung cấp nền tảng cho các nhà phát triển viết mã, xây dựng và quản lý các ứng dụng phần mềm.



# Các loại dịch vụ phần mềm

- **Dịch vụ giao tiếp** (communication services): cho phép nhân viên trong công ty trò chuyện với nhau.
- **Dịch vụ bảo mật** (security services): bảo mật an ninh cho cơ sở hạ tầng CNTT.
- **Dịch vụ năng suất của người dùng** (user productivity services).



# Dịch vụ giao tiếp

- **Giao tiếp tức thời (instant communication)**: trò chuyện với nhiều người khác nhau theo thời gian thực thông qua các phần mềm chat.
- **IRC (Internet Relay Chat)**: giao thức được sử dụng cho các thông điệp chat.
- **Tùy chọn trả tiền (Pay for options)**: loại ứng dụng trò chuyện phức tạp và tiên tiến hơn cung cấp hỗ trợ cho Doanh nghiệp
  - ❑ HipChat và Slack.
- **Open IM protocol**
- **XMPP (Extensible Messaging and Presence Protocol)**: Pidgin và Adium.



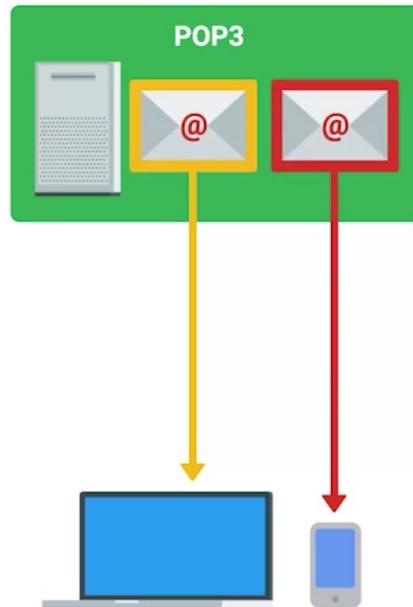
# Dịch vụ email

- **Sysadmin:** cấu hình các dịch vụ email cho công ty. Thiết lập một tên miền cho email. VD: devan@example.com
- Sử dụng máy chủ email tự quản lý: thiết lập phần mềm dịch vụ email trên máy chủ.
  - ❑ Khiến cho hệ thống email hoạt động, bảo vệ địa chỉ email của khỏi thư rác, lọc ra vi-rút.
- Sử dụng nhà cung cấp dịch vụ email: Google Suite, cần trả phí hàng tháng.
  - ❑ Liên kết bạn với ứng dụng Gmail và cho phép bạn truy cập email của mình từ mọi nơi, miễn là bạn được kết nối với Internet.



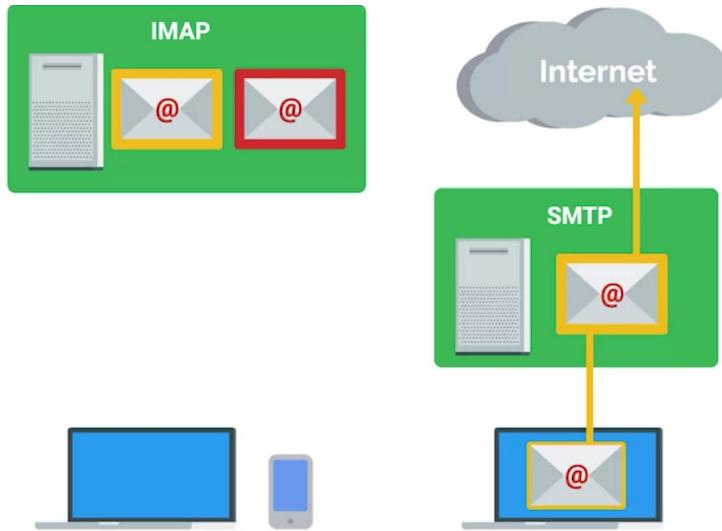
# Giao thức Email

- Giao thức email phổ biến: **POP3, IMAP và SMTP**.
- Post Office Protocol (POP3): tải email từ máy chủ email xuống thiết bị cục bộ. Sau đó, email sẽ bị xóa khỏi máy chủ.
- Lý do dùng POP3:
  - ❑ Dung lượng bộ nhớ email bị giới hạn.
  - ❑ Quyền riêng tư: Email chỉ có thể được xem từ thiết bị cục bộ của bạn.



# Giao thức Email - IMAP

- **IMAP** (Internet message access protocol): tải email từ máy chủ email của mình xuống nhiều thiết bị. Đồng thời giữ các email trên máy chủ email.
- **SMTP** (simple mail transfer protocol): giao thức được sử dụng để gửi email.



# Dịch vụ năng suất người dùng

- Phần mềm hỗ trợ nhân viên thực hiện công việc của mình. VD: chương trình phát triển phần mềm, xử lý văn bản, phần mềm tài chính.
- Sử dụng phần mềm dưới dạng cá nhân và doanh nghiệp có sự khác biệt.
  - ❑ Giấy phép phần mềm (Software licence)
  - ❑ Nhà phân phối phần mềm sẽ có một thỏa thuận riêng về giấy phép phần mềm.
- Tương tự cho dịch vụ phần mềm đám mây.
  - ❑ Mua thêm các tính năng bổ sung cho dành cho doanh nghiệp.



# Dịch vụ bảo mật

- HTTP (HyperText Transfer Protocol): định dạng và truyền nội dung web trên Internet.
- HTTPS (Hypertext Transfer Protocol Secure): phiên bản bảo mật của HTTP. Đảm bảo giao tiếp được bảo mật thông qua mã hóa
- Hai giao thức bảo mật:
  - ❑ TLS (Transport Layer Security protocol): cách phổ biến nhất hiện nay
  - ❑ SSL (Secure Socket Layer protocol). Cũ hơn và kém an toàn.



# Dịch vụ bảo mật

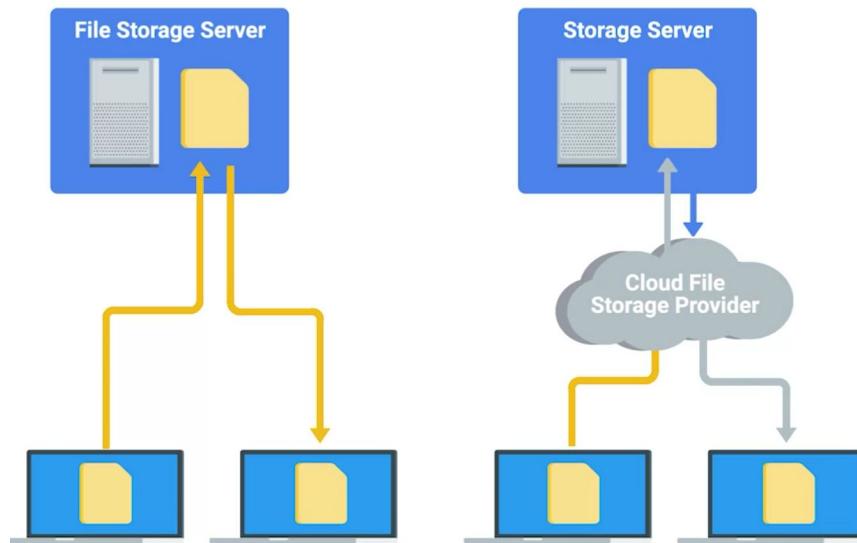
- Để dùng tính năng bảo mật TLS cần phải lấy chứng chỉ điện tử đáng tin cậy (digital certificate of trust)
- Chứng chỉ này được cấp bởi tổ chức phát hành chứng chỉ (certificate authority).
- Sau đó, bạn có thể cài đặt chứng chỉ trên máy chủ web của mình.



# Dịch vụ tập tin

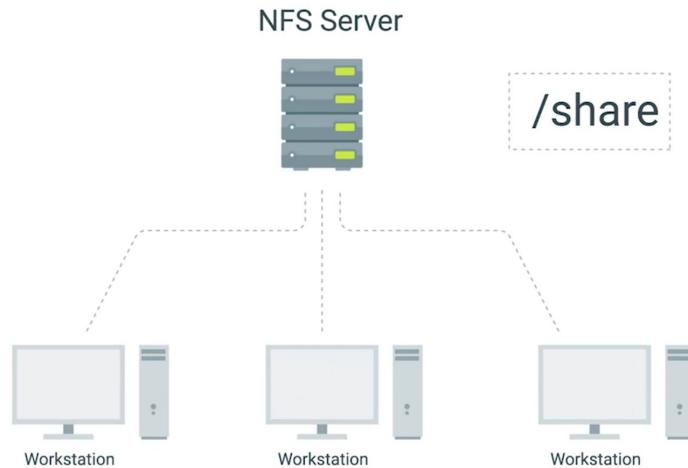
Dịch vụ tập tin (file services): dịch vụ lưu trữ tập tin cho phép chúng ta **lưu trữ** tập tin một cách tập trung và **quản lý quyền truy cập** giữa các tập tin và nhóm.

- Tự thiết lập một máy chủ lưu trữ tập tin
- Dịch vụ lưu trữ tập tin trên Đám mây.



# Dịch vụ tập tin

- FAT32: hệ thống tập tin tương thích với Windows, Linux và Mac OS.
- NFS (Network file system): giao thức cho phép các tập tin chia sẻ qua mạng.
- Thiết lập một máy chủ NFS là sử dụng môi trường Linux.
  - ❑ Bạn có thể cài đặt phần mềm máy chủ NFS
  - ❑ Máy khách muốn truy cập vào máy chủ, cần mount hệ thống tập tin theo cách bạn làm với bất kỳ hệ thống tập tin nào khác.



# Dịch vụ tập tin

- NFS gặp vấn đề tương thích với Windows.
- Sử dụng **Samba** cho Windows: chia sẻ và quản lý các dịch vụ tập tin một cách tập trung.
- Samba hoạt động tốt hơn với hệ điều hành Windows.
- Samba không đồng nghĩa với giao thức SMB.
  - ❑ Samba cài đặt giao thức SMB



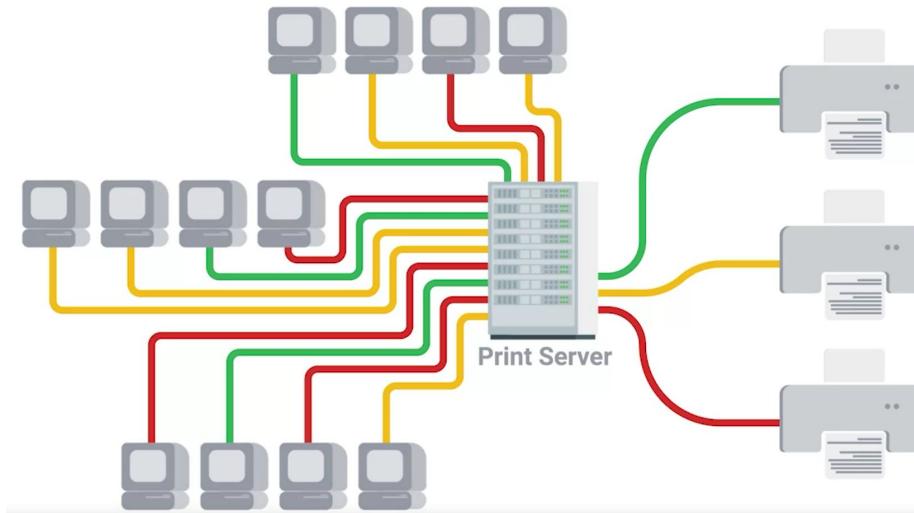
# Dịch vụ tập tin

- NAS (network attached storage): máy tính được tối ưu hóa để lưu trữ tập tin.
- Đi kèm với hệ hành chuyên dụng cho lưu trữ tập tin.
  - ❑ Loại bỏ nhiều tính năng khác.
  - ❑ Quản lý khối lượng lưu trữ lớn.
- Lưu trữ và quản lý tập tin trung tâm là một phần quan trọng của cơ sở hạ tầng CNTT của bất kỳ tổ chức nào.



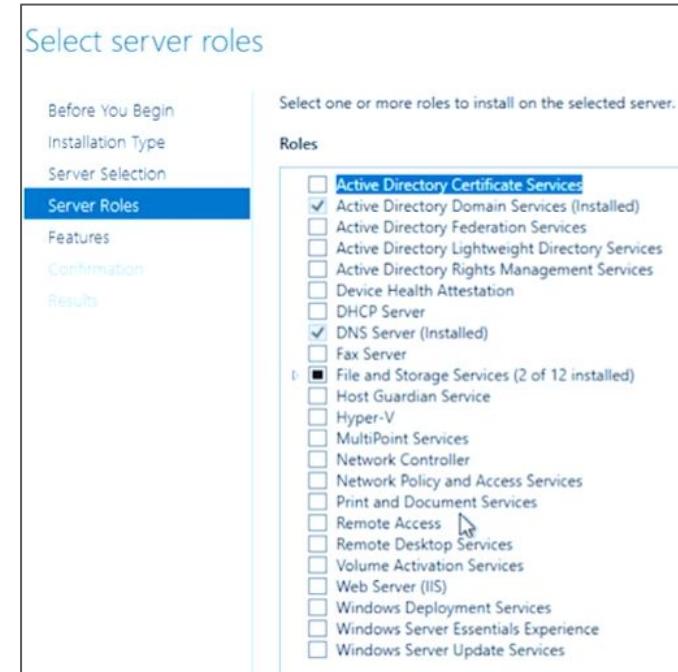
# Dịch vụ máy in

Quản lý tập trung tất cả các máy in



# Dịch vụ máy in

- Trên máy chủ: bật dịch vụ “Print and Document Services”.
- Cài đặt Driver cho máy in.



# Dịch vụ máy in

- Trong Linux: CUPS (Common UNIX Printing System).
- Quản lý máy in từ một trang web.



# Dịch vụ máy in

Sau khi dịch vụ in được thiết lập:

- Thêm máy in vào máy khách.
- Tìm kiếm tên máy chủ máy in
- Kết nối với thiết bị và bắt đầu in.

Sử dụng dịch vụ đám mây.

- Quản lý máy in qua trình duyệt web.
- In qua trình duyệt web



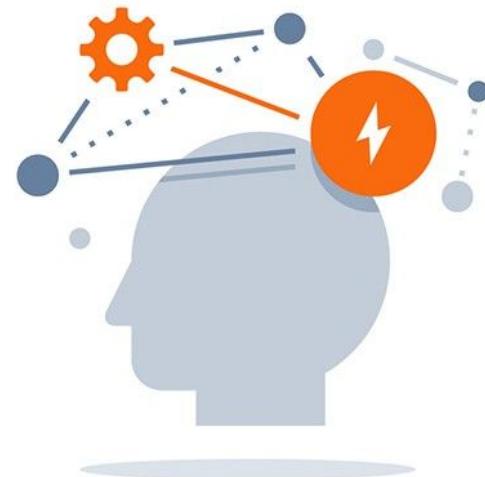
# Máy chủ Cơ sở dữ liệu

- Dữ liệu của trang web thường được lưu trong cơ sở dữ liệu (Database)
- **Cơ sở dữ liệu** cho phép **lưu trữ, truy vấn, lọc** và **quản lý** một lượng lớn dữ liệu.
- Cơ sở dữ liệu phổ biến: MySQL và PostgreSQL
- Yêu cầu kiến thức về các ngôn ngữ và cú pháp đặc biệt



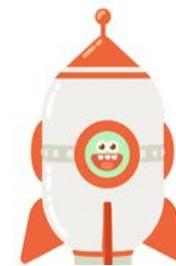
# Chuẩn đoán lỗi trang web

- **Mã trạng thái HTTP:** mã hoặc số cho biết một số loại lỗi hoặc thông báo về những gì đã xảy ra khi cố gắng truy cập tài nguyên web
- **404 Not Found:** URL không trả đến bất kỳ thứ gì
- Mã trạng thái HTTP bắt đầu bằng **4xx**: sự cố ở phía máy khách
- Mã trạng thái HTTP bắt đầu bằng **5xx**: sự cố ở phía máy chủ.
- Mã trạng thái HTTP bắt đầu bằng **2xx**: yêu cầu thành công



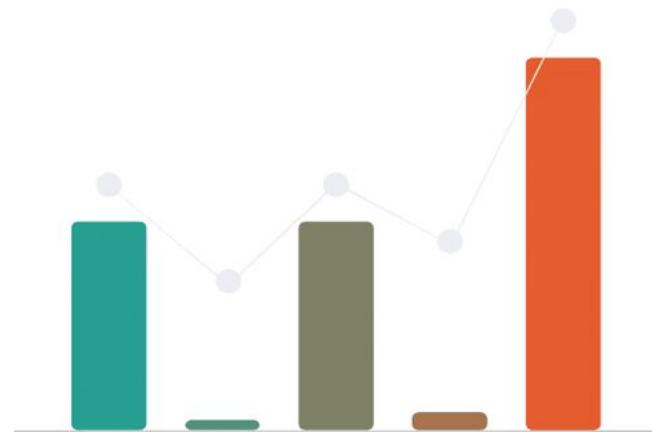
# Khái niệm Đám mây

- **Software as a Service (SaaS)**
- Phần mềm đã được cấu hình sẵn và người dùng không tham gia sâu vào cấu hình đám mây
- Nhà cung cấp đám mây quản lý mọi thứ liên quan đến dịch vụ:
  - ❑ Máy ảo có được lưu trữ hay không
  - ❑ Có đủ dung lượng hay không
  - ❑ Hoạt động thường xuyên
  - ❑ Đáng tin cậy.



# Khái niệm Đám mây

- Infrastructure as a Service – IaaS
- Bạn đang lưu trữ các dịch vụ của riêng mình trên đám mây.
- Bạn cần quyết định cách bạn muốn cơ sở hạ tầng như thế nào, tùy thuộc vào những gì bạn muốn chạy trên nó.
  - ❑ Dùng loại máy nào
  - ❑ Loại bộ nhớ nào



# Khái niệm Đám mây

- **Khu vực (Region)**: một vị trí địa lý có chứa một số trung tâm dữ liệu.
- **Vùng (zone)**: một trung tâm dữ liệu.
- Nếu một vùng gặp sự cố, các dịch vụ có thể được chuyển dời sang vùng khác mà không ảnh hưởng rõ ràng đến người dùng.
- Đám mây công cộng (public cloud).
- Đám mây dùng riêng (private cloud).
- Đám mây lai (hybrid cloud).



# Thiết lập cơ sở hạ tầng đám mây

- **Máy ảo** (virtual machine - VM): phục vụ cùng một trang web.
- **Bộ cân bằng tải** (load balancer): đảm bảo rằng mỗi máy ảo nhận được số lượng truy vấn cân bằng.
  - ❑ Tạo ra nhiều máy ảo hơn khi có nhiều truy vấn.
  - ❑ Tắt một số máy ảo khi số lượng truy vấn giảm.
- **Tự động thay đổi tỷ lệ** (Autoscaling): cho phép dịch vụ tăng hoặc giảm công suất khi cần thiết
- Dịch vụ Web đi kèm với Cơ sở dữ liệu trên đám mây.



# Thiết lập cơ sở hạ tầng đám mây

- Thiết lập giám sát và cảnh báo.
- Phát hiện và khắc phục bất kỳ sự cố nào trước khi người dùng nhận thấy.
- Đã bao gồm trong dịch vụ đám mây.
  - ❑ Khi nào được cảnh báo.
  - ❑ Cách thức được cảnh báo.
- Thiết lập tài nguyên đám mây có vẻ phức tạp nhưng hầu hết các nhà cung cấp hỗ trợ sẵn.



# Khi nào dùng Đám mây

Thiết lập cơ sở hạ tầng tạm thời không kéo dài.

- Dễ dàng chấm dứt cơ sở hạ tầng khi không còn nhu cầu.

Nhu cầu thay đổi nhiều trong năm.

- Dễ dàng tăng hay giảm số lượng máy cần với đám mây.

Vị trí địa lý.

- Chọn được trung tâm dữ liệu gần vị trí muốn phục vụ.

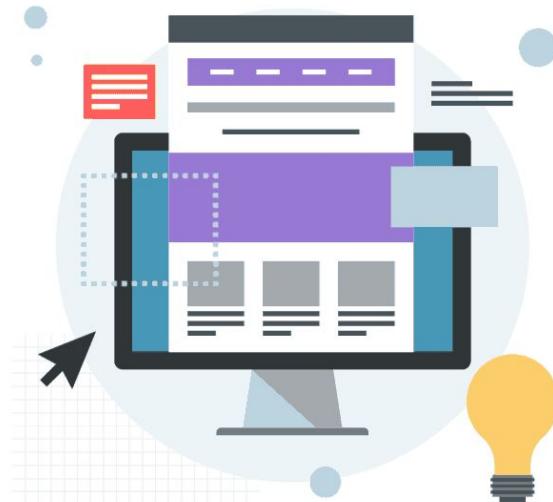


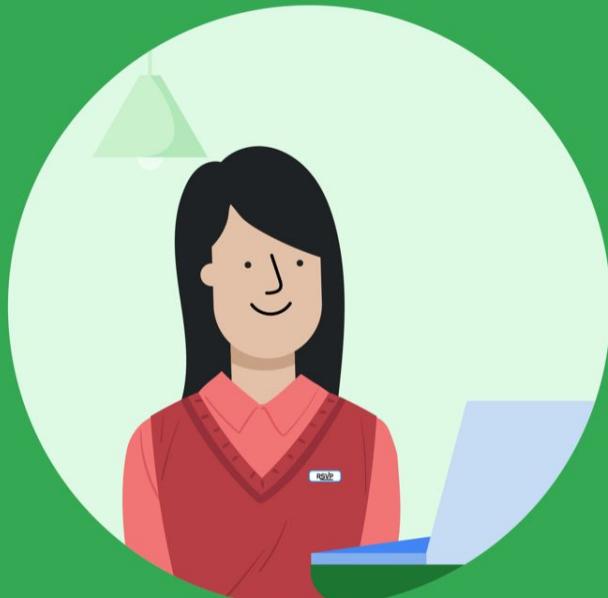
# Khi nào dùng Đám mây

Tận dụng bản dùng thử miễn phí.

- Xem đám mây có đáp ứng nhu cầu hay không.
- Kiểm tra cơ sở hạ tầng của công ty có thích hợp với đám mây hay không.

Luôn cập nhật những thay đổi mới nhất trong lĩnh vực này.





# 4 Các Dịch Vụ Thư Mục



# Máy chủ thư mục

- **Máy chủ thư mục** (directory server): chứa dịch vụ tra cứu cung cấp ánh xạ giữa các **tài nguyên mạng** và **địa chỉ mạng** của chúng.
- Quản lý tài khoản và thông tin máy tính trên máy chủ thư mục để dễ dàng truy cập và quản lý.
- Máy chủ thư mục phải hỗ trợ nhân bản (**replica**): dữ liệu thư mục lưu trữ được sao chép và phân phối trên một số máy chủ vật lý phân tán.
  - Replica cung cấp khả năng dự phòng.
  - Replica cũng làm giảm độ trễ khi bạn truy cập dịch vụ thư mục.



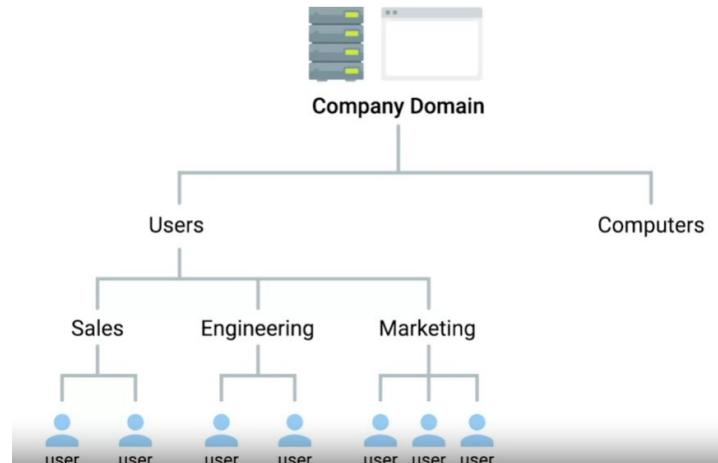
# Máy chủ thư mục

**Dịch vụ thư mục:** hữu ích cho việc tổ chức và tìm kiếm dữ liệu.

Thực hiện thông qua mô hình phân cấp gồm: các đối tượng và vùng chứa.

- Vùng chứa hay đơn vị tổ chức (organizational units - OU).
- Chúng có thể chứa các đối tượng hoặc các đơn vị tổ chức khác.

Tương tự như cấu trúc tập tin.



# Máy chủ thư mục

Cấu trúc này có thể truyền đạt sự khác biệt giữa những nhóm OU con.

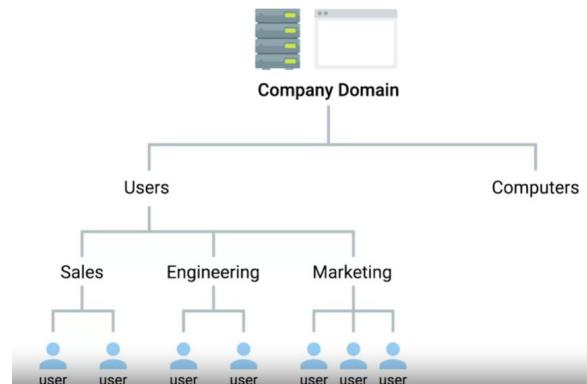
- Ví dụ: yêu cầu mật khẩu khắt khe hơn cho engineer, không ảnh hưởng đến sales và marketing.

Các OU con thừa hưởng các đặc điểm của OU cha.

- Thay đổi ở OU User sẽ ảnh hưởng đến : engineer, sales, và marketing.

Quản trị viên hệ thống: thiết lập, cấu hình và bảo trì máy chủ thư mục.

- Cài đặt hệ điều hành.
- Cài đặt và cấu hình của chính dịch vụ thư mục.



# Máy chủ thư mục

- Tiêu chuẩn thư mục (directory standard): **X.500**.
- Giao thức: **DAP** (Directory Access Protocol), **DSP** (Directory System Protocol), **DISP** (Directory Information Shadowing Protocol), **DOP** (Directory Operational Bindings Management Protocol).
- Các giải pháp ngoài **DAP**: **LDAP** (lightweight directory access protocol).



# Máy chủ thư mục

Phần mềm dịch vụ thư mục cho máy chủ:

- Active Directory (AD): hỗ trợ cho nền tảng Windows.
- OpenLDAP: mã nguồn mở.

Phần mềm dịch vụ thư mục cho máy khách:

- Microsoft Office Active Directory Users and Computers (ADUC), hoạt động tốt với Máy chủ Active Directory của Microsoft.

Các hệ điều hành lớn đều hỗ trợ máy chủ thư mục cho mục đích đăng nhập và xác thực.

Lựa chọn phần mềm: cần quan tâm đến hỗ trợ của hệ điều hành.

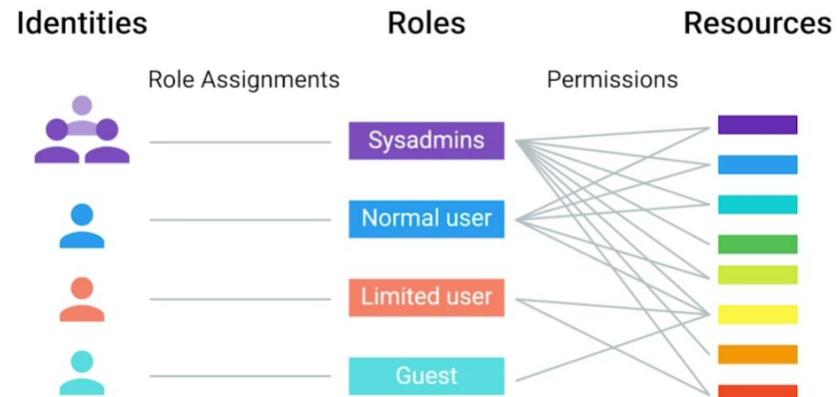
# Quản lý tập trung

- **Quản lý tập trung:** dịch vụ trung tâm cung cấp hướng dẫn cho tất cả các phần khác nhau trong cơ sở hạ tầng CNTT.
- Dịch vụ thư mục: chức năng **xác thực** (Authentication), **cấp quyền** (authorization) và **kế toán** (accounting), còn được gọi là AAA.
- Dịch vụ thư mục: cấp hoặc từ chối quyền truy cập vào máy tính, hệ thống tập tin và các tài nguyên khác.



# Quản lý tập trung

- Cấp quyền truy cập vào tài nguyên dựa trên vai trò (role) trong tổ chức.
- Ví dụ: cấp quyền tạo tài khoản và reset password cho vai trò Sysadmins. Bất kỳ ai có vai trò này sẽ có quyền này.
- Kiểm soát truy cập dựa trên vai trò (role-based access control - RBAC).



# Quản lý cấu hình tập trung

Quản lý cấu hình tập trung: thực hiện các cấu hình, cài đặt phần mềm từ một nơi tập trung.

- Cấu hình tài khoản người dùng, hay thiết lập máy in.

Tập lệnh đăng nhập.

Active Directory và các đối tượng chính sách nhóm.

Framework quản lý cấu hình chuyên dụng

- Chef
- Puppet
- SCCM.



# LDAP

LDAP (lightweight directory access protocol): được sử dụng để truy cập thông tin trong các dịch vụ thư mục qua mạng.

Dịch vụ thư mục sử dụng LDAP: Active Directory và OpenLDAP.

Thao tác có thể sử dụng trong LDAP:

- Thêm một mục mới (entry).
- Xóa một entry trong cơ sở dữ liệu máy chủ thư mục.
- Sửa đổi các entry.

Entry LDAP là một tập hợp thông tin được sử dụng để mô tả điều gì đó.



# Mục nhập LDAP

- **Mục nhập** (entry) LDAP: tập hợp thông tin được sử dụng để mô tả điều gì đó.

dn: CN=Devan Sri-Tharan,OU=Sysadmin,DC=example,DC=com

- dn: (distinguished name) tên mục nhập phân biệt.
- CN (common name): tên gọi chung của đối tượng. *Devan Sri-Tharan*.
- OU (organizational unit): nhóm. *Sysadmin*.
- DC (domain component): thành phần miền. *example.com* được tách thành *example* sau đó là *com*.

# Xác thực trong LDAP

Thao tác Bind: xác thực các máy khách đến máy chủ thư mục.

Đăng nhập vào trang web sử dụng dịch vụ thư mục.

- Điền thông tin đăng nhập tài khoản và mật khẩu
- Thông tin sẽ được gửi lại trang web.
- Nó sẽ sử dụng LDAP để kiểm tra xem tài khoản hợp lệ.
- Nếu hợp lệ, bạn sẽ được cấp quyền truy cập vào tài khoản đó.



# Xác thực trong LDAP

Ba cách phổ biến để xác thực:

- Ẩn danh (**Anonymous**): ai cũng có thể truy cập.
- Đơn giản (**Simple**): chỉ cần tên và mật khẩu, nhưng gửi đi qua kênh không bảo mật.
- **SASL** (Simple Authentication and Security Layer): gửi qua đường truyền bảo mật như TLS.

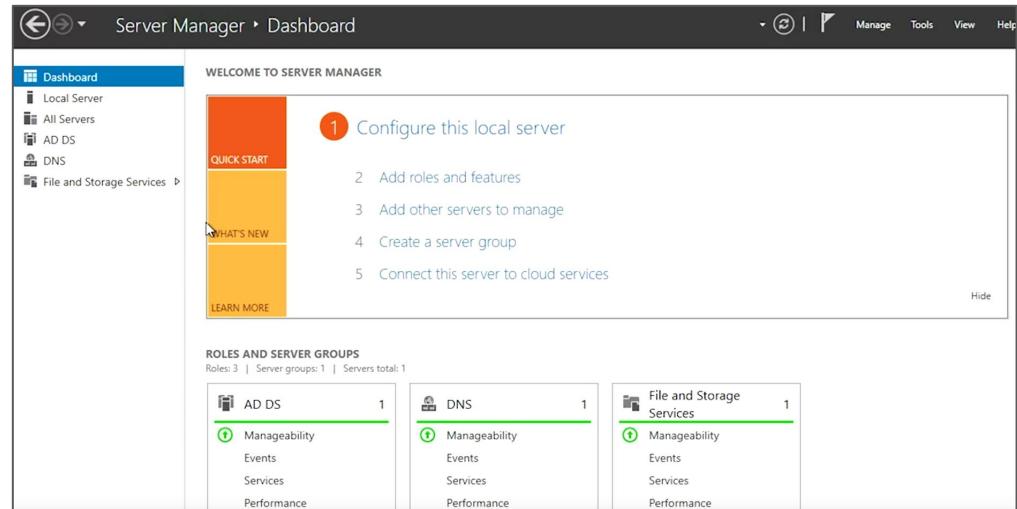
**Kerberos**: một giao thức xác thực mạng được sử dụng để xác thực danh tính người dùng, bảo mật việc chuyển thông tin đăng nhập của người dùng.

Sau khi đã xác thực thành công, người dùng sẽ được phép sử dụng cấp độ truy cập nào mà họ có.



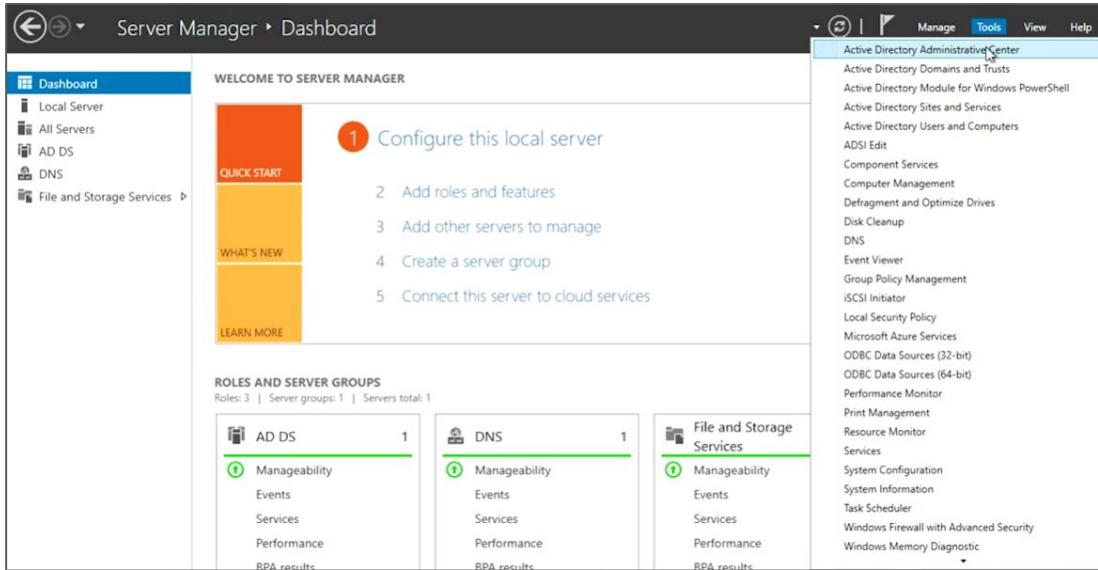
# Active Directory là gì?

- **Active Directory (AD):** dịch vụ thư mục dành riêng cho Microsoft Windows.
- **Đối tượng chính sách nhóm (group policy object – GPO):** cách để quản lý cấu hình của các máy Windows.
- Active Directory là kho lưu trữ GPO.



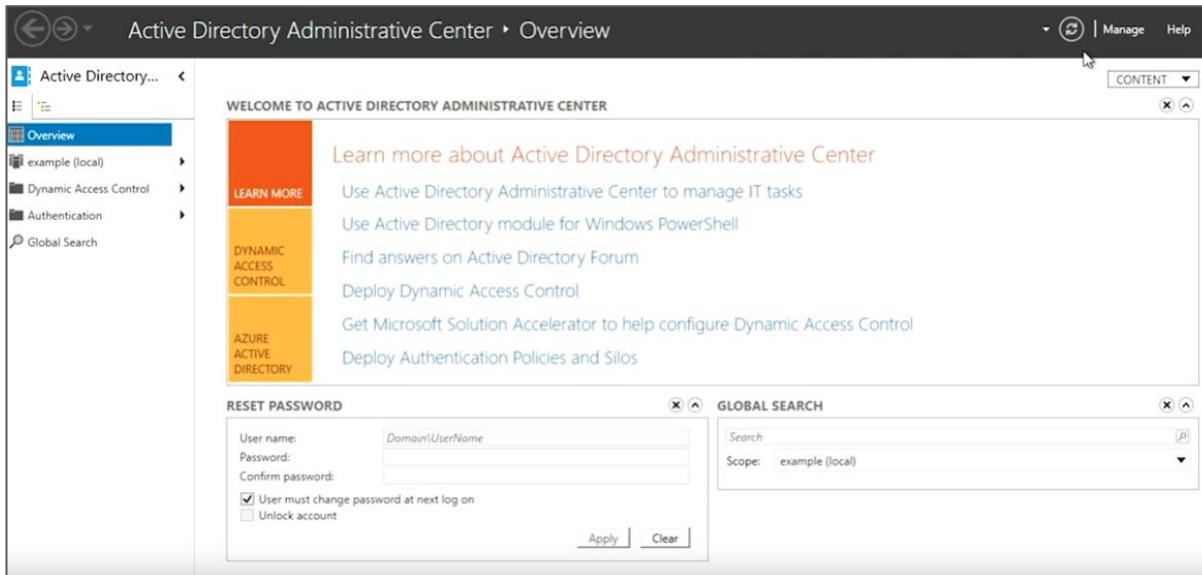
# Active Directory là gì?

Active Directory Administrative Center (ADAC)



# Active Directory là gì?

Active Directory Administrative Center (ADAC)



# Active Directory là gì?

- Mọi thứ trong Active Directory đều là **Đối tượng (object)**.
- **Vùng chứa** (container): đối tượng đặc biệt, có thể chứa các đối tượng khác.
- **Đơn vị tổ chức** (organizational unit - OU): vùng chứa đặc biệt, có thể chứa các OU khác.



# Active Directory là gì?

Miền (domain): example.

Rừng (forest): tập hợp nhiều miền.

The screenshot shows the Active Directory Administrative Center interface. The left navigation pane is collapsed, showing 'Active Directory...', 'Overview', 'example (local)', 'Dynamic Access Control', 'Authentication', and 'Global Search'. The main pane displays the 'example (local) (13)' container with a table of objects. The 'Builtin' container is selected, highlighted with a blue border. The table columns are 'Name', 'Type', and 'Description'. The 'Builtin' row is selected, showing its details: Name is 'builtinDomain...', Type is 'Container', and Description is 'Default container for upgr...'. The right pane shows a 'Tasks' menu with options like 'New', 'Delete', 'Properties', and specific actions for the 'example (local)' container such as 'Change domain controller', 'Raise the forest functional leve...', 'Raise the domain functional le...', 'Enable Recycle Bin ...', 'New', 'Search under this node', and 'Properties'.

Name	Type	Description
Builtin	Container	builtinDomain... Default container for upgr...
Computers	Container	Default container for upgr...
Domain Controllers	Organizational Unit	Default container for dom...
ForeignSecurityPrincipals	Container	Default container for secur...
Infrastructure	Container	infrastructu...
Keys	Container	Default container for key o...
LostAndFound	Container	lostAndFou... Default container for orph...
Managed Service Accounts	Container	Default container for man...
NTDS Quotas	Container	msDS-Quo... Quota specifications conta...
Program Data	Container	Default location for storag...
System	Container	Builtin system settings
Builtin	Container	Builtin

# Active Directory là gì?

- Bên trong miền Domain có Computer.
- Chứa các tài khoản máy tính Active Directory mới được tạo.

The screenshot shows the 'Active Directory Administrative Center' window. The left navigation pane displays a tree structure with 'Active Directory...' at the root, followed by 'example (local)', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipals', 'Keys', 'LostAndFound', 'Managed Service Account', 'NTDS Quotas', 'Program Data', 'System', 'TPM Devices', and 'Users'. The 'Computers' node is highlighted with a blue selection bar. The main pane shows a table titled 'Computers (1)' with one entry: 'WIN-DOMAIN' of type 'Computer'. The right pane, titled 'Tasks', contains a list of actions: 'Reset account...', 'Add to group...', 'Disable', 'Delete', 'Move...', and 'Properties'. Below the tasks, there are sections for 'Computers' with options 'New', 'Delete', 'Search under this node', and 'Properties'.

# Active Directory là gì?

Domain Controller (bộ điều khiển miền): nơi bộ điều khiển miền được tạo.

The screenshot shows the Active Directory Administrative Center interface. The left navigation pane is titled "Active Directory..." and contains the following items:

- Overview
- example (local)
- Builtin
- Computers
- Domain Controllers** (selected)
- ForeignSecurityPrincipals
- Keys
- LostAndFound
- Managed Service Accounts
- NTDS Quotas
- Program Data
- System
- TPM Devices
- Users

The main content area is titled "Domain Controllers (2)". It displays a table with the following columns: Name, Domain Contr..., Site, Type, and Description. Two entries are listed:

Name	Domain Contr...	Site	Type	Description
DC1	Global Catalog	Default-First-Si...	Domain Co...	
DC2	Global Catalog	Default-First-Si...	Domain Co...	

A context menu is open over the "DC1" entry, listing the following options:

- Add to group...
- Delete
- Move...
- Properties

Below the table, there is a "Tasks" section with the following options:

- Pre-create a Read-only domain...
- New
- Delete
- Search under this node
- Properties

# Active Directory là gì?

- users (người dùng)
- Vùng chứa này là nơi người dùng và nhóm AD mới được tạo theo mặc định.

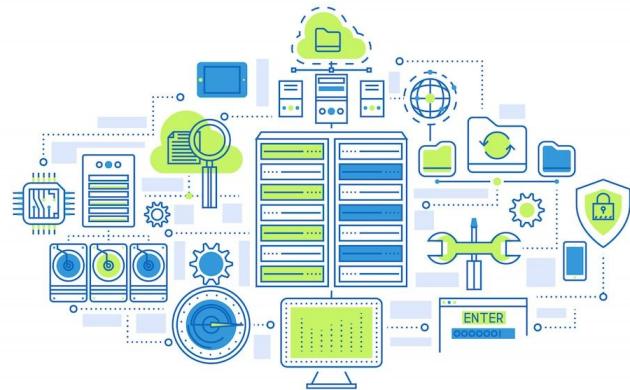
The screenshot shows the Active Directory Administrative Center interface. The left navigation pane is collapsed. The main area displays a list of users and groups under the 'example (local)' domain. The 'Administrator' user is selected, highlighted in blue. The right side features a 'Tasks' pane with options like 'Reset password...', 'View resultant password settin...', 'Add to group...', 'Disable', 'Delete', 'Move...', and 'Properties'. Below the tasks are buttons for 'New', 'Delete', and 'Search under this node'. At the bottom, there's a summary for the selected 'Administrator' user, including logon information and last logon details.

Name	Type	Description
Administrator	User	Built-in account for admin...
Cert Publishers	Group	Members of this group ar...
Cloneable Domain Control...	Group	Members of this group th...
DefaultAccount	User	A user account managed...
Denied RODC Password R...	Group	Members in this group ca...
DnsAdmins	Group	DNS Administrators Group
DnsUpdateProxy	Group	DNS clients who are perm...
Domain Admins	Group	Designated administrators...
Domain Computers	Group	All workstations and serve...
Domain Controllers	Group	All domain controllers in t...

User logon: Administrator  
Expiration: <Never>  
E-mail:  
Modified: 10/16/2017 2:36 PM

# Bộ điều khiển miền

- **Bộ điều khiển miền** (domain controllers - DC): dịch vụ lưu trữ bản sao của cơ sở dữ liệu Active Directory và các đối tượng chính sách nhóm.
- DC cũng đóng vai trò là máy chủ DNS.
- DC cung cấp xác thực tập trung.
- Quyết định quyền truy cập vào các tài nguyên được chia sẻ.
  - Hệ thống tập tin và máy in.



# Bộ điều khiển miền

- Mỗi bộ điều khiển có **bản sao hoàn chỉnh** của cơ sở dữ liệu AD và có thể thực hiện các thay đổi.
- Những thay đổi này được sao chép sang tất cả các bản sao khác.
- Một số thay đổi đối chỉ có thể được thực hiện bởi một DC tại một thời điểm. Dùng cơ chế hoạt động tổng thể linh hoạt **flexible single-master operations (FSMO)**.
- Liên kết máy tính với Active Directory.
  - AD biết về máy tính và đã cấp tài khoản máy tính cho nó.
  - Máy tính biết về miền Active Directory và xác thực với miền đó.



# Quản trị Active Directory

Miền Active Directory chứa: tài khoản người dùng mặc định, quản trị viên (administrator), một số nhóm người dùng mặc định.

The screenshot shows the Active Directory Administrative Center interface. On the left, there's a navigation pane with a tree view of the Active Directory structure, including Overview, example (local) (which is expanded to show Builtin, Computers, Domain Controllers, ForeignSecurityPrincipals, Keys, LostAndFound, Managed Service Account, NTDS Quotas, Program Data, System, TPM Devices, and Users), Dynamic Access Control, Authentication, and Global Search. The 'Users' node under example (local) is selected. The main pane displays a list of 24 users and groups. The 'Administrator' entry is highlighted with a blue selection bar. The right side of the screen has a 'Tasks' pane open, which includes options like Reset password..., View resultant password settings..., Add to group..., Disable, Delete, Move..., Properties, and a New button. Below the main list, there are details for the selected 'Administrator' user: User login: Administrator, E-mail: (empty), Modified: 10/16/2017 2:36 PM, Description: Built-in account for administering the computer/domain, and a note that it has an expiration date of <Never>. The last log on was 10/16/2017 2:29 PM.

# Domain admin

- Domain Admins: quản trị viên của miền Active Directory.
- Người dùng trong nhóm Domain Admins có thể thực hiện bất kỳ thay đổi nào họ muốn trên miền của mình.

The screenshot shows the Active Directory Administrative Center interface. The left navigation pane is collapsed. The main area displays a list of users and groups under the 'example (local)' domain. The 'Administrator' account is selected, highlighted in blue. A context menu is open on the right side of the screen, listing options like 'Reset password...', 'View resultant password setting...', 'Add to group...', 'Disable', 'Delete', 'Move...', 'Properties', 'Users', 'New', 'Delete', 'Search under this node', and 'Properties'. At the bottom of the user list, there is a summary for the 'Administrator' account, including details like User logon: Administrator, E-mail:, Expiration: <Never>, Last log on: 10/16/2017 2:29 PM, Modified: 10/16/2017 2:36 PM, and Description: Built-in account for administering the computer/domain.

# Enterprise Admins

- Enterprise Admins: quản trị viên của miền trong rừng Active Directory.
- Enterprise Admins chỉ nên dùng cần thiết trong trường hợp rất cần thiết.
- Domain Admins chỉ ảnh hưởng đến miền của mình.
- Enterprise Admins ảnh hưởng đến tất cả miền trong rừng.

The screenshot shows the 'Active Directory Administrative Center' interface. In the center, there is a table titled 'Users (24)' listing various groups. One group, 'Enterprise Admins', is highlighted with a blue selection bar. The table has columns for 'Name', 'Type', and 'Description'. The 'Enterprise Admins' entry is described as 'Designated administrators...' and is a 'Group' type. On the right side of the screen, there is a 'Tasks' sidebar with options like 'Manage', 'Help', 'Enterprise Admins', 'Add to another group...', 'Delete', 'Move...', 'Properties', 'Users', 'New', 'Delete', 'Search under this node', and 'Properties'. The 'Enterprise Admins' option is currently selected in the sidebar.

Name	Type	Description
DnsAdmins	Group	DNS Administrators Group
DnsUpdateProxy	Group	DNS clients who are perm...
Domain Admins	Group	Designated administrators...
Domain Computers	Group	All workstations and serve...
Domain Controllers	Group	All domain controllers in t...
Domain Guests	Group	All domain guests
Domain Users	Group	All domain users
<b>Enterprise Admins</b>	<b>Group</b>	<b>Designated administrators...</b>
Enterprise Key Admins	Group	Members of this group ca...
Enterprise Read-only Dom...	Group	Members of this group ar...
Group Policy Creator Own...	Group	Members in this group ca...

# Domain Users

- Domain Users: nhóm chứa mọi tài khoản người dùng trong miền.
- Cấp quyền cho Domain Users nếu bạn muốn cấp quyền truy cập vào tài cho mọi người trong miền.

Active Directory Administrative Center › example (local) › Users

Name	Type	Description
DnsAdmins	Group	DNS Administrators Group
DnsUpdateProxy	Group	DNS clients who are perm...
Domain Admins	Group	Designated administrators...
Domain Computers	Group	All workstations and serve...
Domain Controllers	Group	All domain controllers in t...
Domain Guests	Group	All domain guests
<b>Domain Users</b>	<b>Group</b>	<b>All domain users</b>
Enterprise Admins	Group	Designated administrators...
Enterprise Key Admins	Group	Members of this group ca...
Enterprise Read-only Dom...	Group	Members of this group ar...
Group Policy Creator Own...	Group	Members in this group ca...

E-mail: Type: Security  
Managed by: Scope: Global  
Modified: 10/16/2017 2:21 PM  
Description: All domain users

Tasks

Domain Users

- Add to another group...
- Delete
- Move...
- Properties

Users

- New
- Delete
- Search under this node
- Properties

# Domain Computers

Domain Computers chứa tất cả các máy tính được tham gia vào miền.

The screenshot shows the Active Directory Administrative Center interface. The left navigation pane is collapsed, and the main area displays a list of users under the 'example (local)' domain. A specific group, 'Domain Computers', is highlighted with a blue selection bar. The right side of the screen shows a 'Tasks' pane with options like 'Add to another group...', 'Delete', 'Move...', and 'Properties'. Below the tasks is a 'Users' section with 'New', 'Delete', and search functions. At the bottom, there is a summary of the selected group's details: E-mail, Managed by, Modified date (10/16/2017 2:21 PM), and Description (All workstations and servers joined to the domain).

Name	Type	Description
DnsAdmins	Group	DNS Administrators Group
DnsUpdateProxy	Group	DNS clients who are perm...
Domain Admins	Group	Designated administrators...
<b>Domain Computers</b>	<b>Group</b>	<b>All workstations and serve...</b>
Domain Controllers	Group	All domain controllers in t...
Domain Guests	Group	All domain guests
Domain Users	Group	All domain users
Enterprise Admins	Group	Designated administrators...
Enterprise Key Admins	Group	Members of this group ca...
Enterprise Read-only Dom...	Group	Members of this group ar...
Group Policy Creator Own...	Group	Members in this group ca...

# Domain Controllers

Domain Controllers chứa tất cả các bộ điều khiển miền trong miền.

The screenshot shows the Active Directory Administrative Center interface. The left navigation pane is collapsed, and the main area displays a list of users under the 'example (local)' domain. A specific group, 'Domain Controllers', is selected and highlighted with a blue bar. The right-hand pane contains a 'Tasks' section with options like 'Add to another group...', 'Delete', 'Move...', 'Properties', and a 'Users' section with 'New', 'Delete', and search functions. Below the main list, there is a detailed view of the 'Domain Controllers' group, showing its type as 'Security' and scope as 'Global'. The group has no members listed.

Name	Type	Description
DnsAdmins	Group	DNS Administrators Group
DnsUpdateProxy	Group	DNS clients who are perm...
Domain Admins	Group	Designated administrators...
Domain Computers	Group	All workstations and serve...
<b>Domain Controllers</b>	<b>Group</b>	<b>All domain controllers in t...</b>
Domain Guests	Group	All domain guests
Domain Users	Group	All domain users
Enterprise Admins	Group	Designated administrators...
Enterprise Key Admins	Group	Members of this group ca...
Enterprise Read-only Dom...	Group	Members of this group ar...
Group Policy Creator Own...	Group	Members in this group ca...

# Lưu ý khi quản trị Active Directory

- Quản trị viên hệ thống sẽ có vai trò domain admin hay enterprise admin.
- Không sử dụng tài khoản domain admin cho hoạt động hàng ngày của mình.
- Tài khoản domain admin chỉ nên dùng khi cần thiết.
- Dùng tài khoản bình thường cho hoạt động hàng ngày.
- Ủy quyền (delegation): cần thực hiện nhiệm vụ quản trị nhưng bạn không cần có quyền truy cập rộng rãi để thay đổi trong AD.



# Quản trị người dùng và nhóm

- Tài khoản người dùng: xác định bạn là ai và kiểm soát loại quyền truy cập đối với các tài nguyên CNTT.
- Quản trị kém: ngăn mọi người thực hiện những việc họ cần làm.
- Rủi ro cho tổ chức: có quá nhiều quyền truy cập hoặc không cần thiết.
- Nhiệm vụ của quản trị viên hệ thống:
  - Tài khoản người dùng được tạo
  - Duy trì
  - Xóa.



# Tạo tài khoản

Tạo tài khoản người dùng bằng Active Directory Administrative Center và đặt nó vào vùng chứa người dùng mặc định.

The screenshot shows the Active Directory Administrative Center interface. The left sidebar navigation tree is expanded to show the 'example (local)' domain, with 'Users' selected. The main pane displays a list of users and groups under 'example (local)'. A context menu is open over the 'Domain Controllers' group, with 'User' highlighted. A modal dialog box is open at the bottom, titled 'New User', showing fields for 'Name' (with 'User' typed), 'Type' (set to 'User'), and 'Scope' (set to 'Global'). The 'All domain controllers in the domain' checkbox is checked. The 'Tasks' pane on the right lists options for managing domain controllers and users.

# Tạo tài khoản

Nhập vào các trường cần thiết được đánh dấu hoa thị: Fullname và Username.

Create User: Kristi

* Account	Account
Organization	First name:
Member Of	Middle initials:
Password Settings	Last name:
Profile	Full name: * Kristi
Policy	User UPN logon:
Silo	User SamAccountName lo... example \* I
	Password:
	Confirm password:
	Create in: CN=Users,DC=example,DC=com Change...
	<input type="checkbox"/> Protect from accidental deletion
	<a href="#">Log on hours...</a> <a href="#">Log on to...</a>

# Tạo tài khoản

Chọn “user must change password at the next login”.

The screenshot shows a user account creation interface. On the left, there are several input fields for basic user information. On the right, there are configuration sections. The 'Password options:' section contains two radio buttons: one selected (blue outline) labeled 'User must change password at next log on' and another unselected (grey outline) labeled 'Other password options'. Below these are three checkboxes: 'Microsoft Passport or smart card is required for interactive log on' (unchecked), 'Password never expires' (unchecked), and 'User cannot change password' (unchecked). Further down are sections for 'Encryption options:' and 'Other options:', each containing a single checkbox (both unchecked).

Account expires:  Never  End of

Password options:

User must change password at next log on  
 Other password options

Microsoft Passport or smart card is required for interactive log on  
 Password never expires  
 User cannot change password

Encryption options:

Other options:

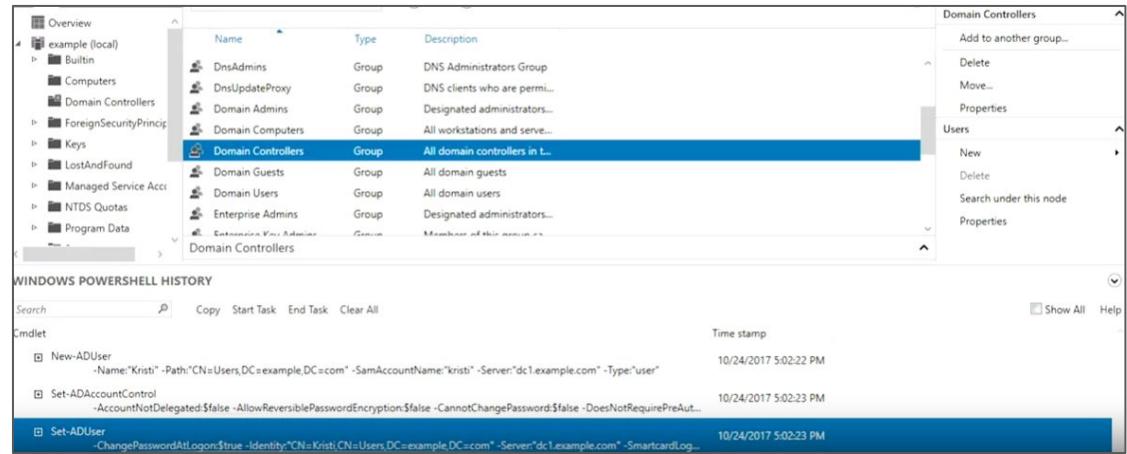
# Tạo nhiều tài khoản cùng một lúc

- Nhu cầu tạo nhiều tài khoản cùng một lúc.
  - Ví dụ: tạo hàng nghìn tài khoản sinh viên trong năm học mới.
- Nhấp qua các biểu mẫu ADAC như vừa rồi: tốn rất nhiều thời gian.
- Dùng trong giao diện dòng lệnh (command line): viết script chạy đi chạy lại các lệnh đó cho bạn.



# Tạo nhiều tài khoản cùng một lúc

- Mọi thứ bạn làm trong ADAC, được thực hiện trong PowerShell.
- Windows PowerShell: chứa các lệnh đang được chạy bởi ADAC.
- Tạo một script để lặp lại các lệnh tạo tài khoản.
- Đường dẫn đầy đủ của một đối tượng trong AD: ký hiệu LDAP.



# Tạo nhóm người dùng mới

Chọn Users > New > Group

The screenshot shows the Windows Active Directory Users and Computers management console. On the left, there's a navigation pane with a tree view of the local computer (example (local)) and various administrative and system containers like Built-in, Computers, Domain Controllers, and ForeignSecurityPrincipals. A context menu is open over the 'Users' container under 'example (local)'. The 'New' option in this menu is expanded, showing four choices: InetOrgPerson (selected), Group, User, and Computer. The main pane displays a list of existing users and groups. One user, 'Kristi', is highlighted. The columns in the list are Name, Type, and Description. The 'Type' column shows 'User' for Kristi and 'Group' for other entries like Enterprise Key Admins and Schema Admins.

Name	Type	Description
Enterprise Key Admins	Group	Members of this group ca...
Enterprise Read-only Dom...	Group	Members of this group ar...
Group Policy Creator Own...	Group	Members in this group ca...
Guest	User	Built-in account for guest...
Key Admins	Group	Members of this group ca...
krbtgt	User	Key Distribution Center Se...
Kristi	User	
Protected Users	Group	Members of this group ar...
RAS and IAS Servers	Group	Servers in this group can a...
Read-only Domain Control...	Group	Members of this group ar...
Schema Admins	Group	Designated administrators...

# Tạo nhóm người dùng mới

Gõ Researchers vào Group name.

Create Group: Researchers

Group	<p>Group</p> <p>Group name: * *</p>
Managed By	
Member Of	
Members	<p>Group type:</p> <p><input checked="" type="radio"/> Security</p> <p><input type="radio"/> Distribution</p> <p><input type="checkbox"/> Protect from accidental deletion</p>
Password Settings	<p>Group scope:</p> <p><input type="radio"/> Domain local</p> <p><input checked="" type="radio"/> Global</p> <p><input type="radio"/> Universal</p>
	<p>Managed By</p> <p>Managed by:</p> <p><input type="button" value="Edit..."/> <input type="button" value="Clear"/></p>

# Tạo nhóm người dùng mới

Thêm mô tả về nhóm

Create Group: Researchers

Group		Group	
Managed By	Group name: <input type="text" value="Researchers"/>	E-mail:	<input type="text"/>
Member Of	Group (SamAccountName... <input type="text" value="Researchers"/>	Create in: CN=Users,DC=example,DC=com	Change...
Members	Group type: <input checked="" type="radio"/> Security <input type="radio"/> Distribution	Group scope: <input type="radio"/> Domain local <input checked="" type="radio"/> Global <input type="radio"/> Universal	Description: <input type="text" value="A"/>
Password Settings	<input type="checkbox"/> Protect from accidental deletion		
Notes: <input type="text"/>			
Managed By			
Managed by:	<input type="checkbox"/> Manager can update membership list	<input type="button" value="Edit"/>	<input type="button" value="Clear"/>
Phone numbers:	Main:	Office:	<input type="text"/>
Mobile:	Fax:	<input type="text"/>	<input type="text"/>
		Address: <input type="text" value="Street"/>	<input type="text"/>
		City: <input type="text"/>	State/Province: <input type="text"/>
		Zip/Postal code: <input type="text"/>	Country/Region: <input type="text"/>
Member Of			
Filter <input type="text"/>		<input type="button" value="Add..."/>	
Name <input type="button" value="▼"/>	Active Directory...	<input type="button" value="Remove"/>	

# Tạo nhóm người dùng mới

Nhấn OK.

The screenshot shows the Windows Active Directory Users and Computers management console. On the left, the navigation pane is visible with various organizational units like 'example (local)', 'Computers', 'Domain Controllers', and 'Users'. The 'Users' node is currently selected. The main pane displays a list of users and groups under the heading 'Users (26)'. A new group, 'Researchers', has been created and is highlighted with a blue selection bar. Below the list, detailed information for the 'Researchers' group is shown, including its E-mail, managed by, modified date, and description. A dashed green rectangle highlights the text 'Nhấn OK.' (Press OK) at the top right of the main pane.

Name	Type	Description
Group Policy Creator Own...	Group	Members in this group ca...
Guest	User	Built-in account for guest...
Key Admins	Group	Members of this group ca...
krbtgt	User	Key Distribution Center Se...
Kristi	User	
Protected Users	Group	Members of this group ar...
RAS and IAS Servers	Group	Servers in this group ca...
Read-only Domain Control...	Group	Members of this group ar...
<b>Researchers</b>	<b>Group</b>	All members of the Resear...
Schema Admins	Group	Designated administrators...

**Researchers**

E-mail: Type: Security  
Managed by: Scope: Global  
Modified: 10/24/2017 5:10 PM  
Description: All members of the Research Dept.

# Dùng PowerShell

Mở PowerShell và gõ câu lệnh.

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> New-ADGroup -Description:"All members of the Research Dept." -GroupCategory:"Security" -GroupScope:
e,DC=com" -SamAccountName:"Researchers" -Server:"dcl.example.com"
```

GroupCategory và GroupScope.



# Loại nhóm (Group type)

- **Security Group (nhóm bảo mật):** chứa tài khoản người dùng, tài khoản máy tính hoặc các nhóm bảo mật khác.
  - Ví dụ: domain users hay domain admin.
  - Được sử dụng để cấp hoặc từ chối quyền truy cập vào các tài nguyên CNTT.
- **Distribution group (nhóm phân phối):** để nhóm các tài khoản và địa chỉ liên hệ để liên lạc qua email.
  - Không sử dụng distribution group để chỉ định quyền cho tài nguyên.
  - Tạo danh sách email bao gồm những người từ bên ngoài miền của bạn



# Phạm vi nhóm (Group scope)

- Group scope: cách các định nghĩa nhóm được sao chép trên các miền.
- Domain local (miền cục bộ): gán quyền truy cập cho một tài nguyên.
  - Tạo nhóm domain local: có quyền đọc vào một tài nghiên chia sẻ gọi là ResearchShareReaders Một nhóm khác có quyền ghi vào ResearchShareWriters.
- Global (Toàn cục). nhóm các tài khoản thành một vai trò (role).
  - Nhóm Research, Sale, Management.
- Universal (phổ quát). nhóm các vai trò global trong một khu rừng.
  - Sao chép bên ngoài miền mà chúng được định nghĩa
  - Nhóm global ResearchShareReaders cho mỗi miền.
  - Nhóm universal ResearchShareReaders có các thành viên là các nhóm global.

# Gắn nhóm cho người dùng

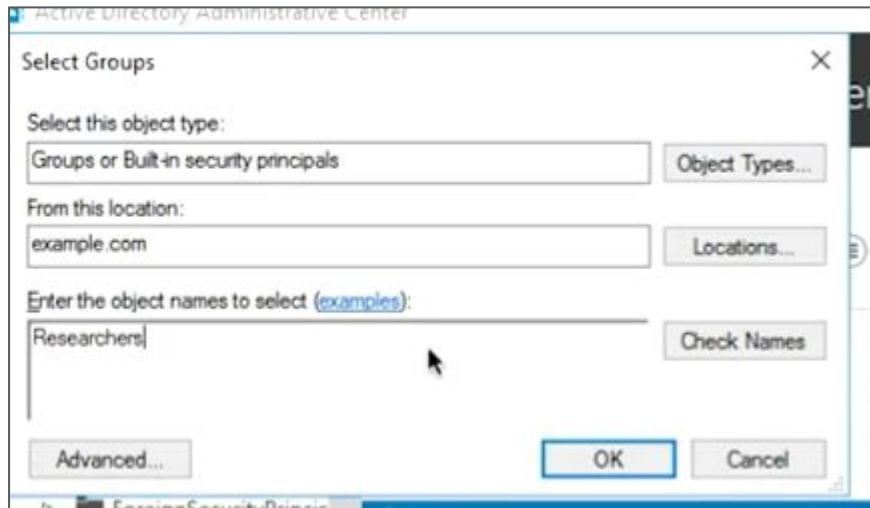
Nhấn chuột phải, chọn Add to group.

The screenshot shows the Active Directory Administrative Center interface. The left navigation pane shows the 'example (local)' domain with various containers like 'Builtin', 'Computers', and 'Domain Controllers'. The main area displays a list of users with 26 entries. One user, 'Kristi', is selected and has a context menu open. The menu includes options like 'Reset password...', 'View resultant password settings...', 'Add to group...', 'Enable', 'Delete', 'Move...', 'Properties', and 'Kristi (Disabled)'. The 'Add to group...' option is highlighted with a blue selection bar. To the right of the list, there's a 'Tasks' sidebar with options like 'Reset password...', 'View resultant password se...', 'Add to group...', 'Enable', 'Delete', 'Move...', 'Properties', and a 'Users' section with 'New', 'Delete', and 'Search under this node' options. At the bottom, there's a 'WINDOWS POWERSHELL HISTORY' section.

Name	Type	Description
Guest	User	Built-in account for guest...
Key Admins	Group	Members of this group ca...
krbtgt	User	Key Distribution Center Se...
Kristi	User	(Selected)
Protected Users		
RAS and IAS Se		
Read-only Dom		
Researchers		
Schema Admin		

# Gắn nhóm cho người dùng

Gõ tên nhóm. Chẳng hạn như researchers rồi nhấn OK.



# Thêm người dùng vào nhóm

Chọn nhóm, nhấp chuột phải, chọn Properties.

The screenshot shows the Active Directory Administrative Center interface. The left navigation pane is collapsed, and the main area displays a list of users under 'example (local) > Users (26)'. A context menu is open over the 'Researchers' group, listing options: 'Add members to the Research...', 'Add to another group...', 'Delete', 'Move...', and 'Properties'. The 'Properties' option is highlighted with a blue selection bar. The bottom of the screen shows a 'WINDOWS POWERSHELL HISTORY' section.

Name	Type	Description
Protected Users	Group	Members of this group ar...
RAS and IAS Servers	Group	Servers in this group can a...
Read-only Domain Control...	Group	Members of this group ar...
<b>Researchers</b>	Group	All members of the Resear...
Schema Admins	Group	Administrators...

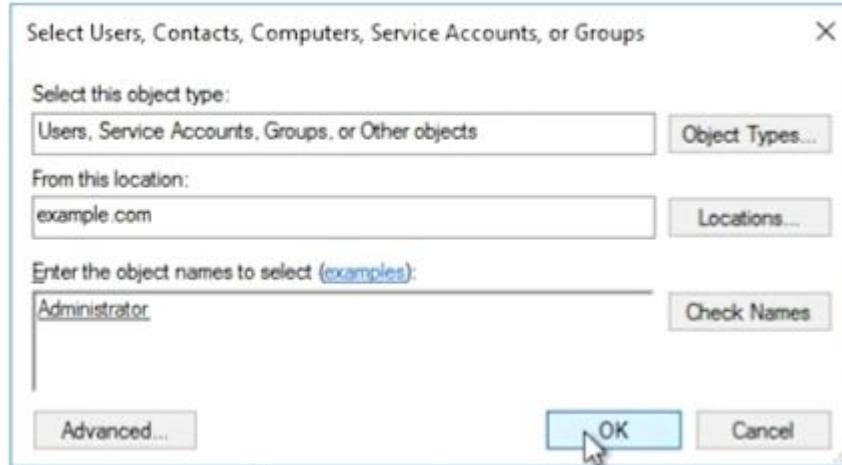
# Thêm người dùng vào nhóm

- Chọn Member.
- Chọn Add.

The screenshot shows the 'Researchers' group management interface. On the left, there's a sidebar with options: Group, Managed By, Member Of, Members, Password Settings, and Extensions. The 'Members' section is active, showing a table with a single row for 'Kristi' under 'example-Users...'. A blue bar highlights this row. To the right of the table are 'Add...' and 'Remove' buttons. Below the table are sections for 'Directly Associated Password Settings' and 'Extensions', each with their own tables and associated buttons like 'Assign...' and 'Clear'.

# Thêm người dùng vào nhóm

Gõ Administrator. Rồi OK



# Thêm người dùng vào nhóm

Kết quả:

The screenshot shows a Windows-based application window titled "Members". At the top left is a "Filter" input field with a magnifying glass icon. To its right is a dropdown menu set to "Name". Below the filter is a table with two rows. The first row contains "Administrator" and "example-Users...". The second row contains "Kristi" and "example-Users...". The "Administrator" row is highlighted with a thick blue bar. On the far right of the table are two buttons: "Add..." and "Remove". A mouse cursor is positioned over the "Remove" button. Above the table, a green dashed rectangular box encloses the word "Kết quả:".

# Xóa người dùng vào nhóm

The screenshot shows the 'Researchers' group management interface. On the left, there's a sidebar with options: Group, Managed By, Member Of, Members, Password Settings, and Extensions. The 'Members' section is active, showing a table with two rows:

Name	Active Directory...
Administrator	example-Users...
Kristi	example-Users...

At the bottom right of the 'Members' section, there are 'Add...' and 'Remove' buttons. The 'Remove' button is highlighted with a blue background and a cursor is pointing at it. Below the 'Members' section, there's another section titled 'Directly Associated Password Settings'.

# Tạo nhóm cha

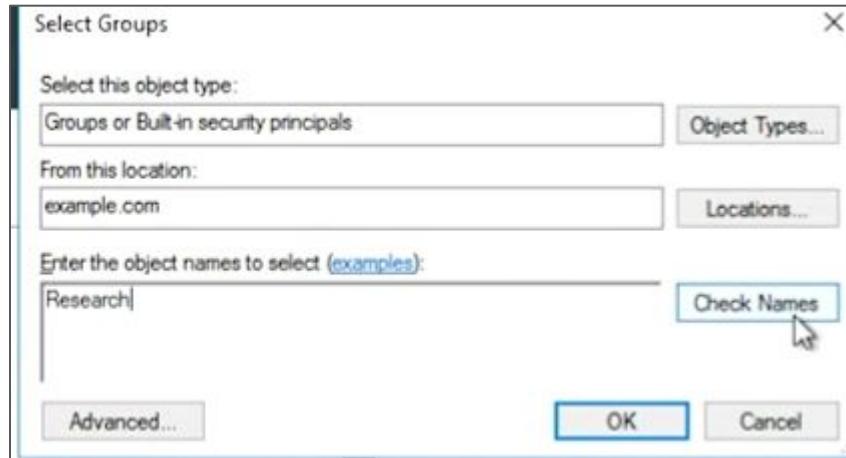
- Tạo nhóm “Research and Development” chứa nhóm Research và nhóm Development.
- Tạo nhóm cha.

Create Group: Research and Development

Group	<p>Group</p> <p>Managed By</p> <p>Member Of</p> <p>Members</p> <p>Password Settings</p>	<p>Group name: <input type="text" value="Research and Development"/></p> <p>Group (SamAccountName...): <input type="text" value="Research and Development"/></p> <p>Group type: <input checked="" type="radio"/> Security <input type="radio"/> Distribution</p> <p><input type="checkbox"/> Protect from accidental deletion</p> <p>Group scope: <input type="radio"/> Domain local <input checked="" type="radio"/> Global <input type="radio"/> Universal</p> <p>E-mail: <input type="text"/></p> <p>Create in: CN=Users,DC=example,DC=com <a href="#">Change...</a></p> <p>Description: All of the members of the Research and Development Group</p> <p>Notes:</p>	<p>TASKS ▾</p> <p>SECTIONS ▾</p>
Managed By	<p>Managed by:</p> <p><input type="checkbox"/> Manager can update membership list</p> <p>Phone numbers:</p> <p>Main:</p> <p>Mobile:</p> <p>Fax:</p>	<p><a href="#">Edit...</a> <a href="#">Clear</a></p> <p>Office:</p> <p>Address: Street</p> <p>City <input type="text"/> State/Province <input type="text"/> Zip/Postal code <input type="text"/></p>	

# Tạo nhóm cha

Chọn Add Member. Gõ vào “Researchers” để thêm nhóm.



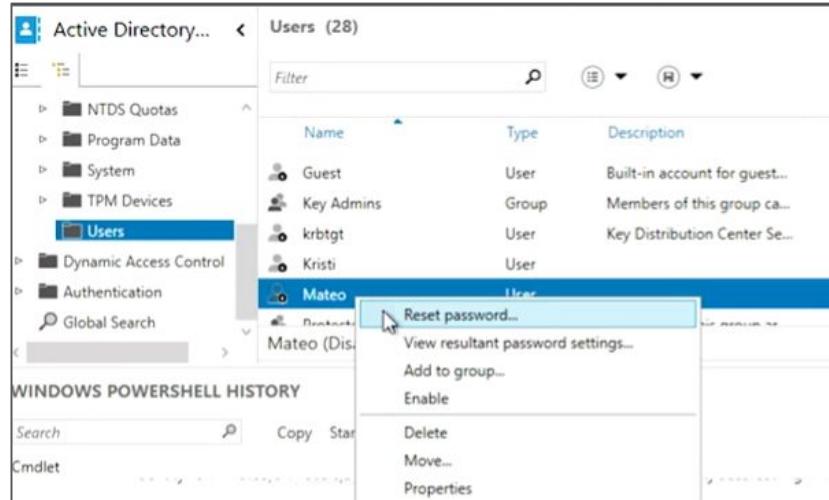
# Quản lý mật khẩu người dùng

- Chuyên gia hỗ trợ CNTT: hỗ trợ người dùng các vấn đề về mật khẩu.
- AD không lưu trữ mật khẩu của người dùng.
  - Dùng hàm băm mã hóa một chiều cho mật khẩu.
  - Mật khẩu có thể dễ dàng chuyển thành hàm băm, nhưng ngược lại hầu như không thể.
- Bạn (người quản lý hệ thống) không thể tra cứu mật khẩu của người dùng ngay cả khi bạn muốn.



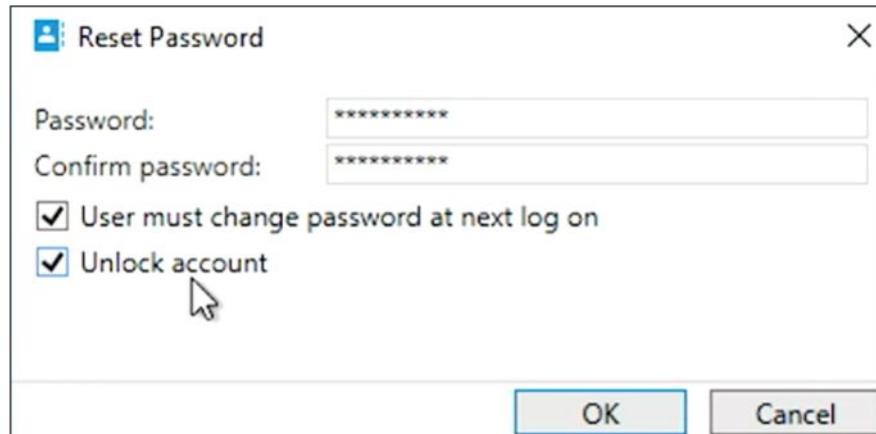
# Quản lý mật khẩu người dùng

- **Đặt lại mật khẩu (reset password):** việc thường gặp của SysAdmin.
- Trước hết phải xác nhận rằng họ đúng là chủ thật sự của tài khoản.
- Sau đó, thực hiện đặt lại mật khẩu trong Active Directory:
  - Nhấp chuột phải vào user, chọn Reset Password.



# Quản lý mật khẩu người dùng

- Gõ lại password tạm thời.
- Chọn “User must change password at next log on”.
- Chọn “Unlock account”.



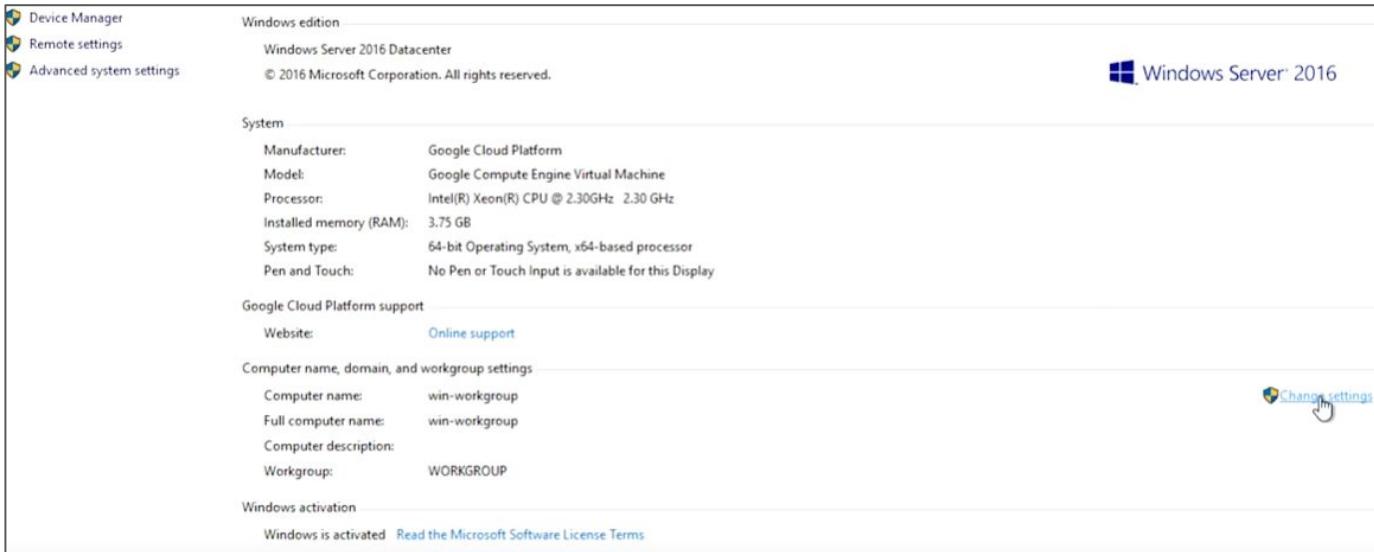
# Kết nối đến miền Active Directory

Máy tính không tham gia vào miền, hay còn gọi là máy tính Workgroup.

The screenshot shows the Windows Server 2016 Control Panel Home page. At the top, it displays basic computer information: Windows edition (Windows Server 2016 Datacenter), copyright (© 2016 Microsoft Corporation. All rights reserved.), and the Windows Server 2016 logo. Below this, the 'System' section provides detailed hardware specifications: Manufacturer (Google Cloud Platform), Model (Google Compute Engine Virtual Machine), Processor (Intel(R) Xeon(R) CPU @ 2.30GHz 2.30 GHz), Installed memory (RAM) (3.75 GB), System type (64-bit Operating System, x64-based processor), and Pen and Touch (No Pen or Touch input is available for this Display). The 'Google Cloud Platform support' section includes a 'Website' link to 'Online support'. Under 'Computer name, domain, and workgroup settings', the computer name is listed as 'win-workgroup' for both 'Computer name:' and 'Full computer name:', 'Computer description:' is empty, and 'Workgroup:' is set to 'WORKGROUP'. There is a 'Change settings' link next to the workgroup entry. At the bottom, it shows 'Windows activation' status ('Windows is activated') and the product ID ('Product ID: 00376-40000-00000-AA947'). A 'Change product key' link is also present. A 'See also' link is located at the very bottom left.

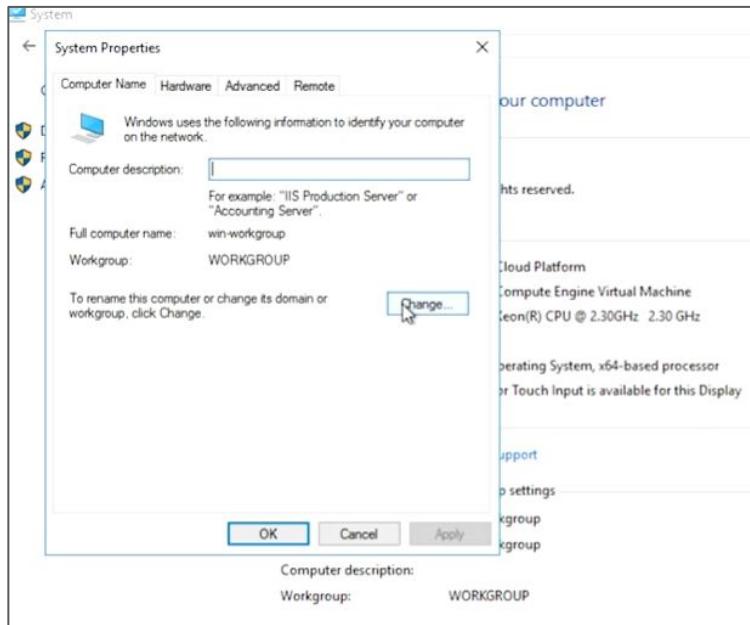
# Kết nối bằng giao diện đồ họa

Chọn Change Setting.



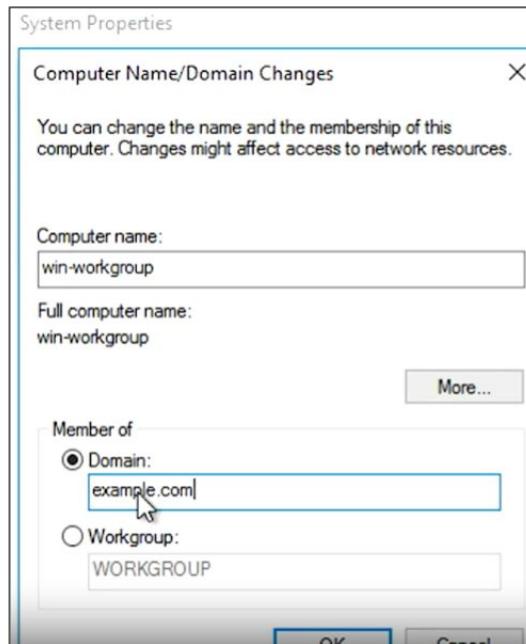
# Kết nối bằng giao diện đồ họa

Nhấp vào Change.



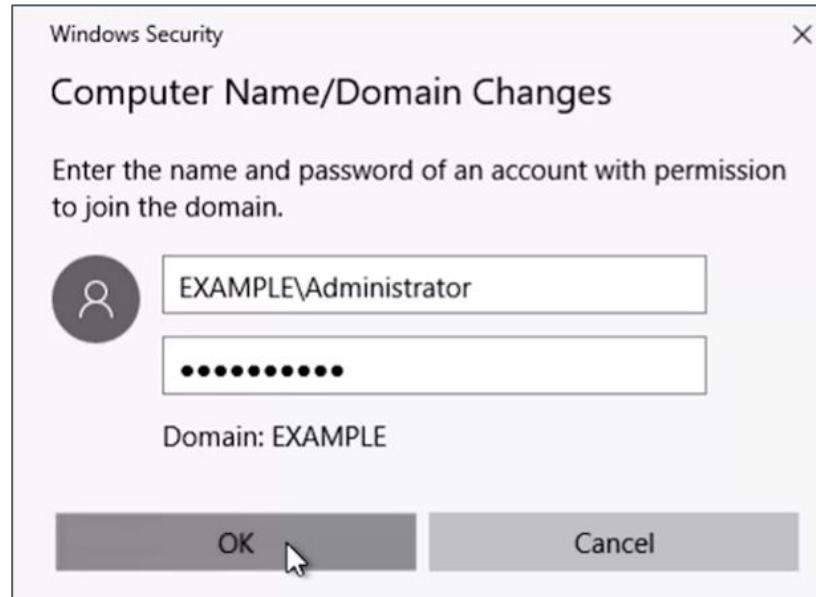
# Kết nối bằng giao diện đồ họa

Chọn Domain rồi nhập vào tên miền.



# Kết nối bằng giao diện đồ họa

Nhập username, password rồi OK.



# Kết nối bằng giao diện đồ họa

Máy tính đã được thêm vào domain.

The screenshot shows the Microsoft Active Directory Users and Computers (ADUC) interface. On the left, a navigation pane lists 'Overview', 'example (local)' (which is selected), 'Users', 'Domain Controllers', 'Computers', 'Dynamic Access Control', 'Authentication', and 'Global Search'. Below this is a search bar and a 'WINDOWS POWERSHELL HISTORY' section with a search bar and buttons for 'Copy', 'Start Task', 'End Task', and 'Clear All'. The main pane displays a table with columns 'Name', 'Type', and 'Description'. It contains two entries: 'WIN-DOMAIN' (Computer type) and 'WIN-WORKGROUP' (Computer type). A cursor is hovering over the 'WIN-WORKGROUP' entry. A dashed green box highlights the message 'Máy tính đã được thêm vào domain.' (The computer has been added to the domain.) at the top right of the main pane.

Name	Type	Description
WIN-DOMAIN	Computer	
WIN-WORKGROUP	Computer	

# Kết nối bằng Powershell

```
Administrator: Windows PowerShell
PS C:\Windows\system32> Add-Computer -DomainName 'example.com' -Server 'dc1'
cmdlet Add-Computer at command pipeline position 1
Supply values for the following parameters:
Credential
```

A screenshot of a Windows PowerShell window showing a credential request dialog. The title bar says "Windows PowerShell credential request". The dialog contains a key icon and the text "Enter your credentials.". It has two input fields: "User name:" with a placeholder icon and a dropdown arrow, and "Password:" with a redacted password field. At the bottom are "OK" and "Cancel" buttons.

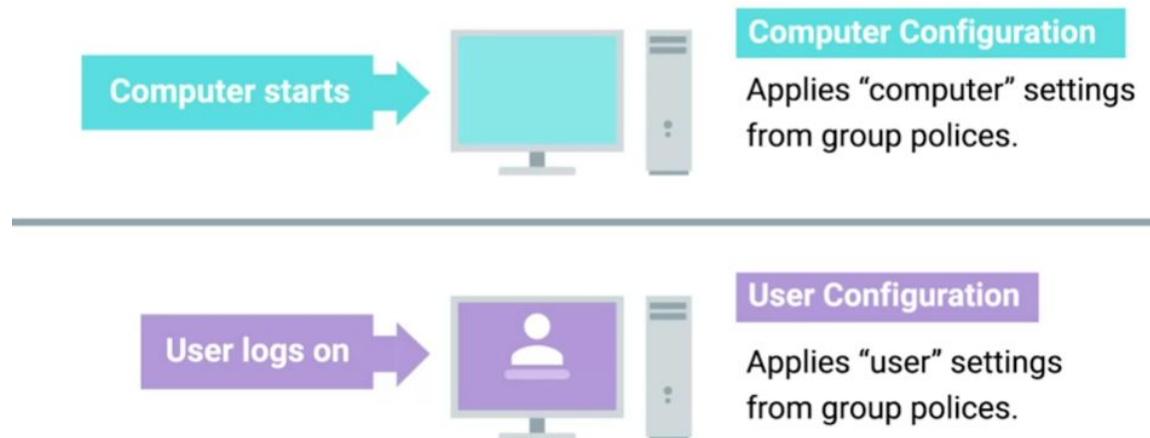
# Định nghĩa chính sách nhóm (GPO)

- **GPO (Group Policy Object):** một tập hợp các **chính sách (policy)** và **tùy chọn (preference)** có thể được áp dụng cho một nhóm đối tượng trong thư mục.
- Chính sách nhóm: giúp chuẩn hóa tùy chọn người dùng cho từng nhóm.
- Ví dụ về chính sách nhóm:
  - Cấu hình nhật ký sự kiện.
  - Số lần nhập sai mật khẩu cho phép.
  - Cài đặt phần mềm và chặn phần mềm.



# Tổng quan về GPO

- Khi bạn **liên kết** GPO, tất cả các máy tính hoặc người dùng trong miền, sites, hoặc OU sẽ được áp dụng chính sách đó.
- GPO có thể chứa **Cấu hình máy tính**, **Cấu hình người dùng** hoặc cả hai.



# Tổng quan về GPO

- **Cấu hình máy tính** (Computer configuration): được áp dụng khi máy tính đăng nhập vào miền Active Directory.
- **Cấu hình người dùng** (User configuration): được áp dụng khi tài khoản người dùng được đăng nhập vào máy tính.
- Khi GPO có hiệu lực, nó sẽ được kiểm tra và thực thi vài phút một lần.



# Tổng quan về GPO

- **GPO:** tập hợp các **chính sách** và **tùy chọn**.
- **Chính sách (policy)** là các cài đặt được áp dụng lại sau mỗi vài phút và không nên được thay đổi ngay cả bởi các quản trị viên cục bộ.
  - Chính sách trong GPO được áp dụng lại trên máy tính sau mỗi 90 phút.
- **Tùy chọn chính sách nhóm (Group policy preference)** là khuôn mẫu cho các cài đặt.
  - Người dùng có thể thay đổi cài đặt mà không bị ghi đè.

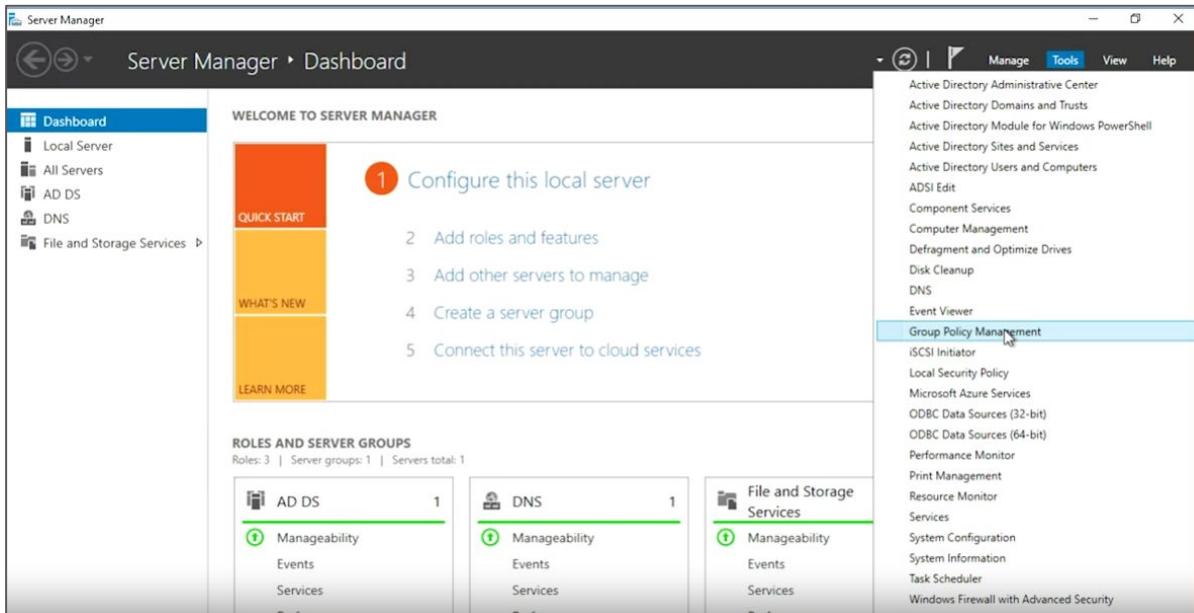
# Tổng quan về GPO

- Bộ điều khiển miền (domain controller) cung cấp GPO cho máy tính.
- Máy tính sẽ tải GPO từ một thư mục đặc biệt có tên là Sysvol.
- Khi máy tính đã tải xuống GPO, nó sẽ áp dụng chúng cho máy tính.
- Chính sách và tùy chọn trong GPO được thể hiện dưới dạng giá trị trong Windows Registry.



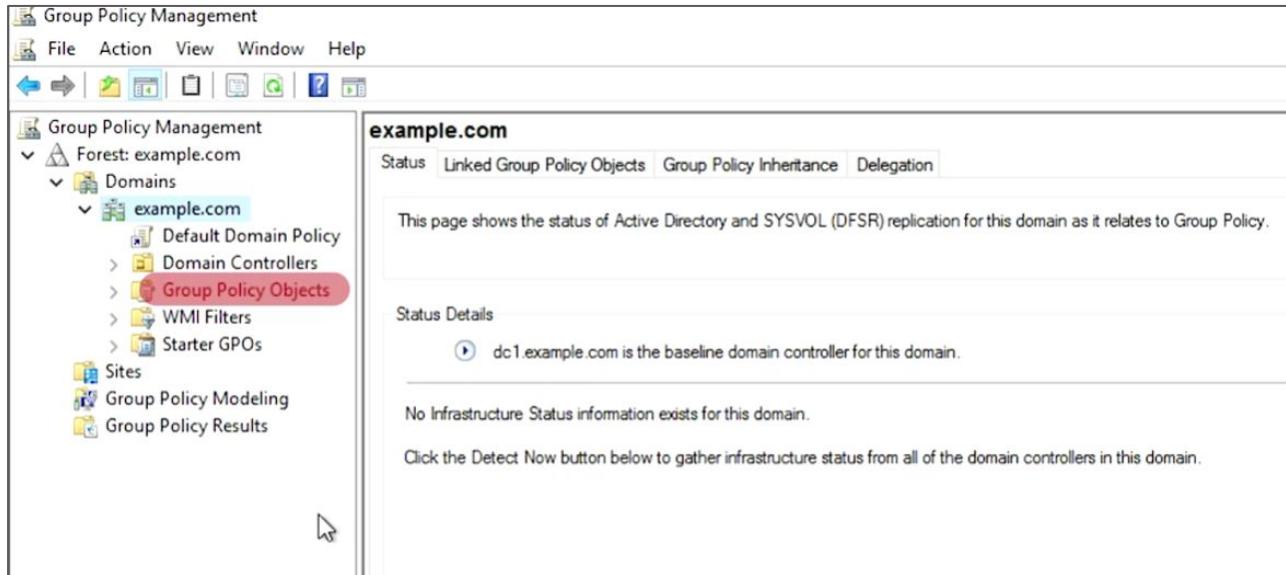
# Tạo và chỉnh sửa chính sách nhóm

Công cụ GPMC



# Tạo và chỉnh sửa chính sách nhóm

**Group Policy Objects:** chứa tất cả các GPO được xác định trong miền.



# Tạo và chỉnh sửa chính sách nhóm

**WMI Filters:** xác định các luật mục tiêu mạnh mẽ cho GPO.



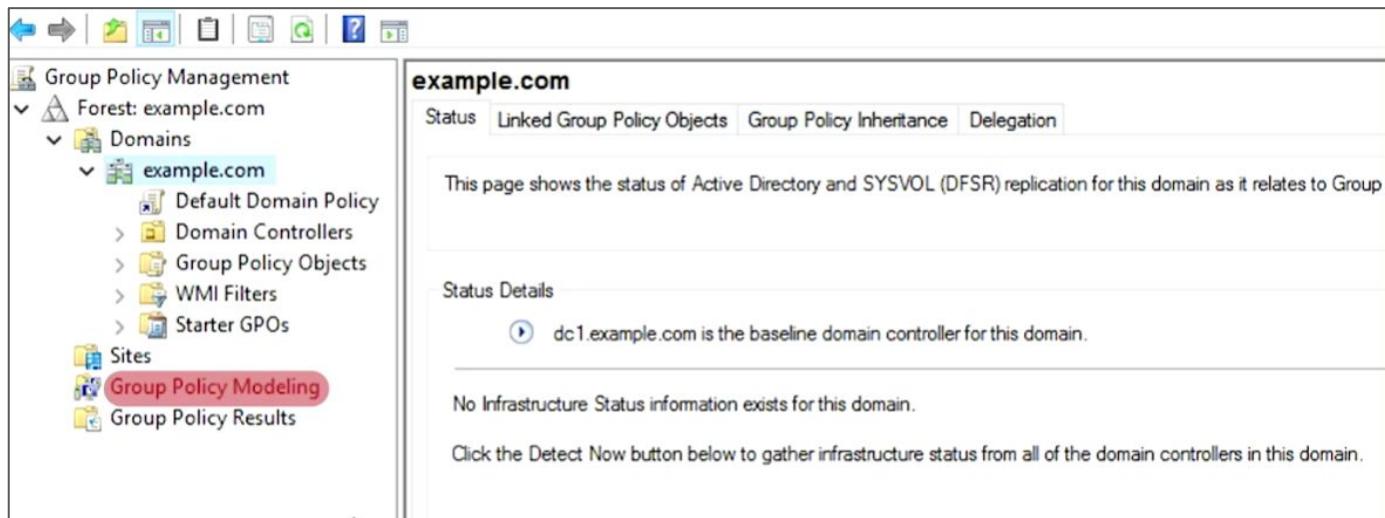
# Tạo và chỉnh sửa chính sách nhóm

**Group Policy Result:** công cụ khắc phục sự cố được sử dụng để tìm ra những chính sách nhóm nào áp dụng cho máy tính và người dùng.

The screenshot shows the Windows Group Policy Management console interface. On the left, the navigation pane displays a tree structure under 'Forest: example.com / Domains / example.com'. The 'Group Policy Results' node is highlighted with a red oval. The main pane shows the 'example.com' domain status page. The top navigation bar includes 'Status', 'Linked Group Policy Objects', 'Group Policy Inheritance', and 'Delegation'. Below the navigation bar, a message states: 'This page shows the status of Active Directory and SYSVOL (DFSR) replication for this domain as it relates to Group Policy'. Under 'Status Details', it says: 'dc1.example.com is the baseline domain controller for this domain.' A note below states: 'No Infrastructure Status information exists for this domain.' At the bottom, there is a button labeled 'Click the Detect Now button below to gather infrastructure status from all of the domain controllers in this domain.'

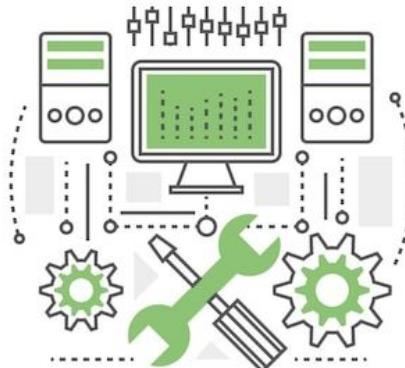
# Tạo và chỉnh sửa chính sách nhóm

Group Policy Modeling được sử dụng để dự đoán chính sách nhóm nào sẽ áp dụng cho máy tính hoặc người dùng trong mạng.



# Tạo và chỉnh sửa chính sách nhóm

- Vùng chứa user và vùng chứa computer không phải là OU.
- GPO chỉ có thể liên kết với **miền, sites** và **OU**.
- Để áp dụng GPO, cần tổ chức tài khoản người dùng và máy tính vào các OU



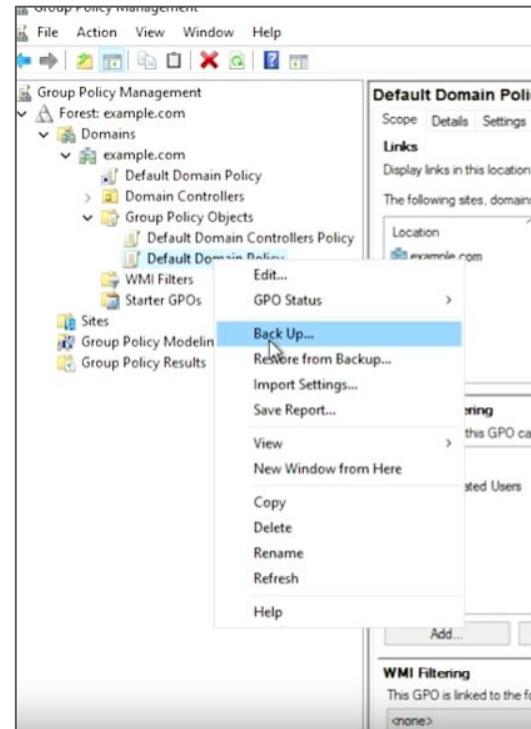
# Tạo và chỉnh sửa chính sách nhóm

Hai GPO được tạo tự động: **default domain controller policy** và **default domain policy**. Default Domain Policy là GPO mặc định được liên kết với miền. Nó áp dụng cho tất cả các máy tính và người dùng trong miền.

Default Domain Policy	
Scope Details Settings Delegation	
<b>Default Domain Policy</b>	
Data collected on: 10/24/2017 8:45:35 PM	
<b>Computer Configuration (Enabled)</b>	
<b>Policies</b>	
<b>Windows Settings</b>	
<b>Security Settings</b>	
<b>Account Policies/Password Policy</b>	
Policy	Setting
Enforce password history	24 passw
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 charact
Password must meet complexity requirements	Enabled

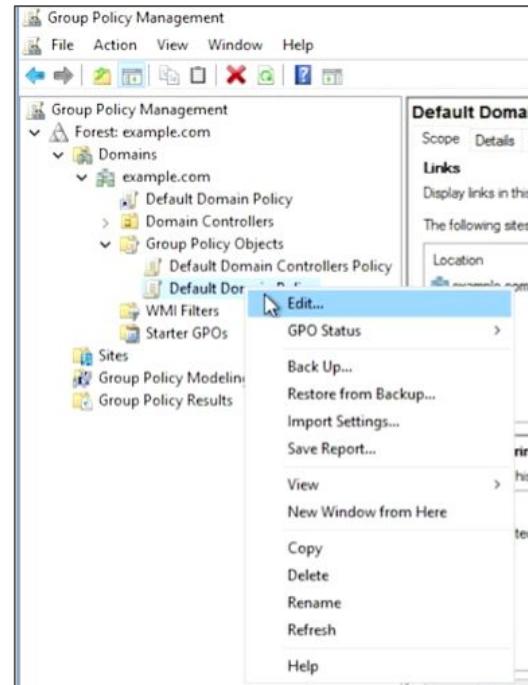
# Tạo và chỉnh sửa chính sách nhóm

- Sao lưu GPO trước khi thay đổi.
- Chọn Default Domain Policy > Nhấp chuột phải > Back up.

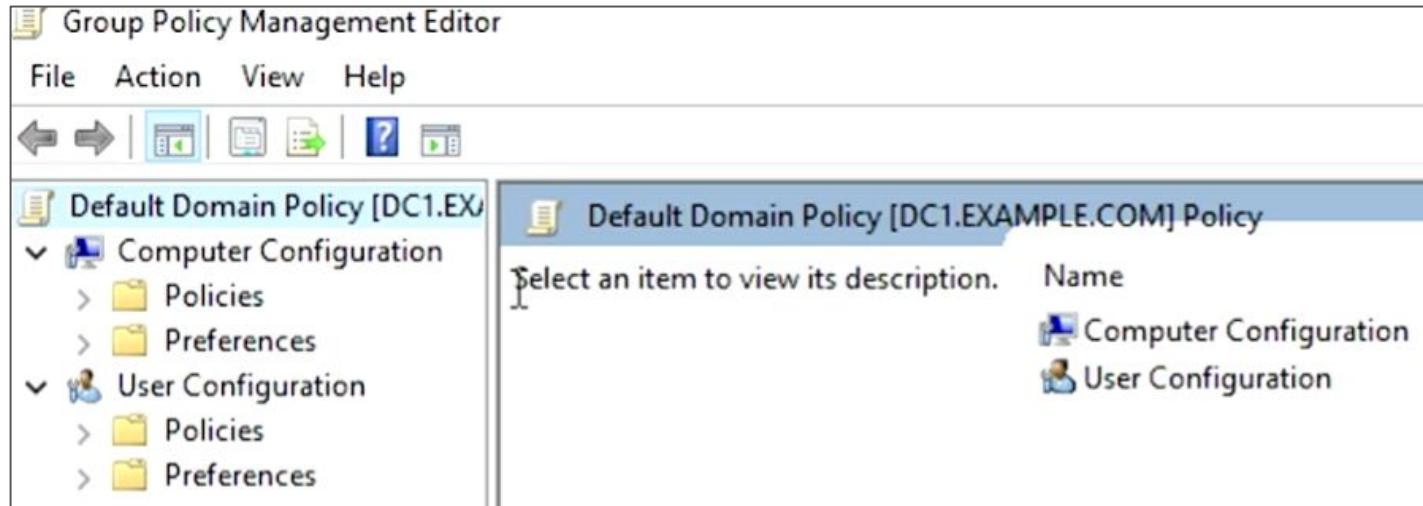


# Tạo và chỉnh sửa chính sách nhóm

- Để thay đổi, chọn chức năng Edit.
- Chọn Default Domain Policy > Nhập chuột phải > Edit.

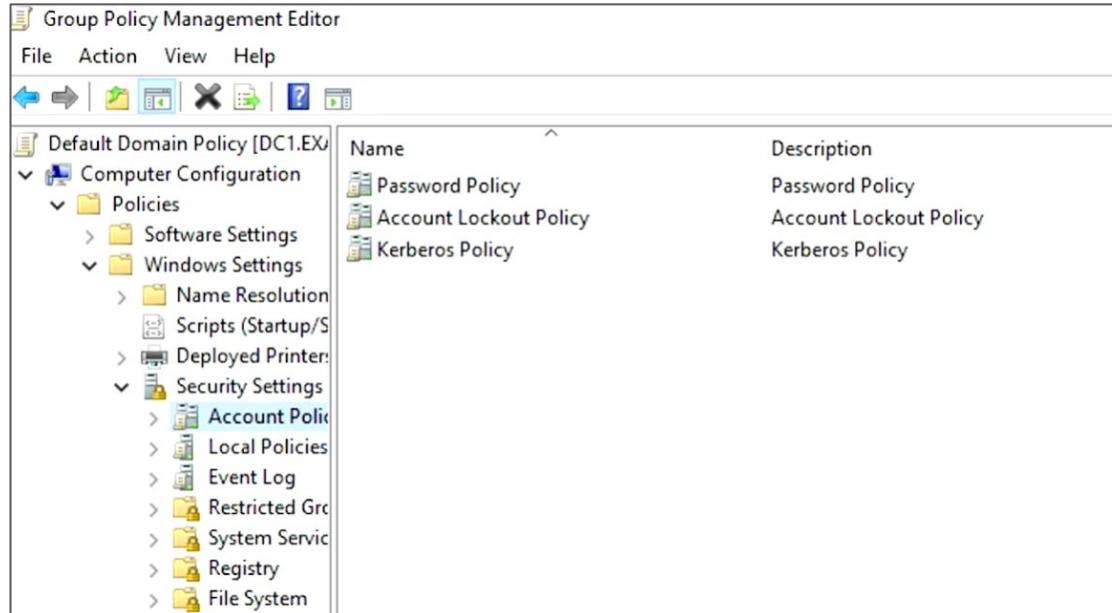


# Tạo và chỉnh sửa chính sách nhóm



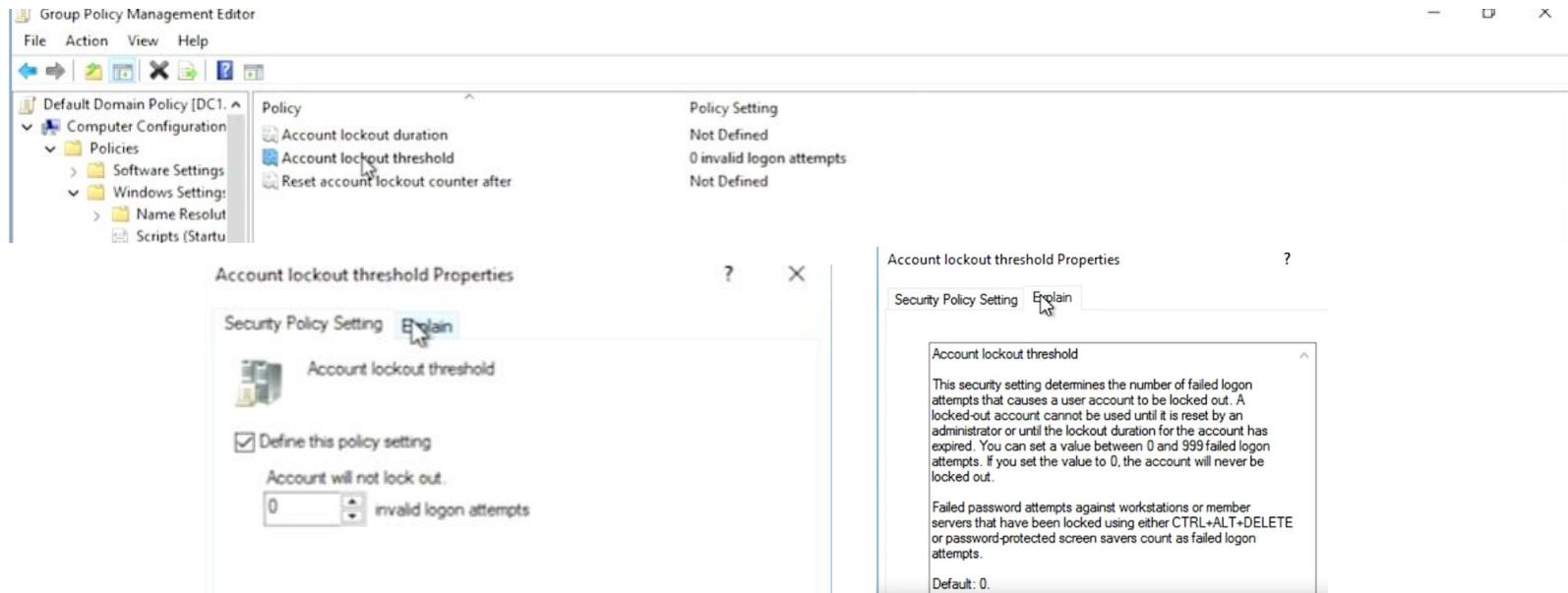
# Tạo và chỉnh sửa chính sách nhóm

Thay đổi account policy.



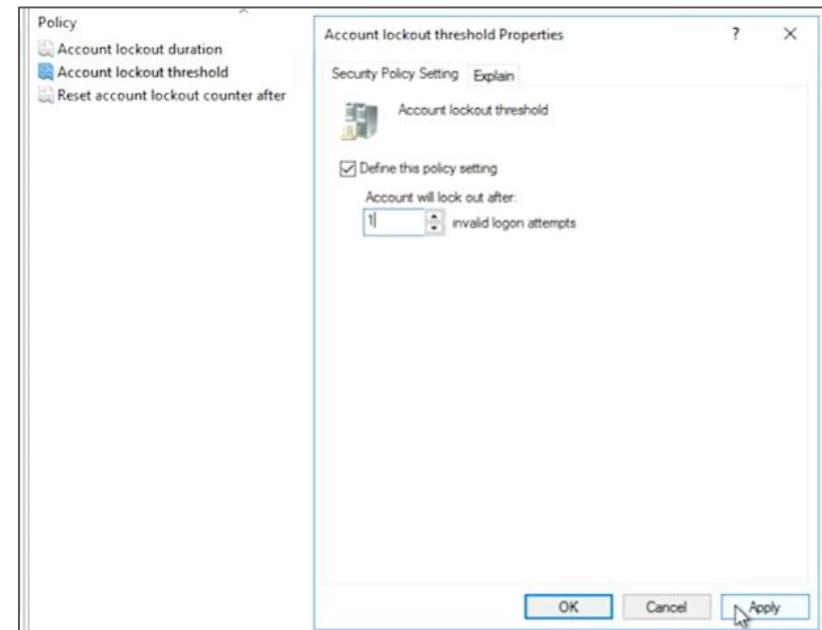
# Tạo và chỉnh sửa chính sách nhóm

Chọn Account lockout threshold.



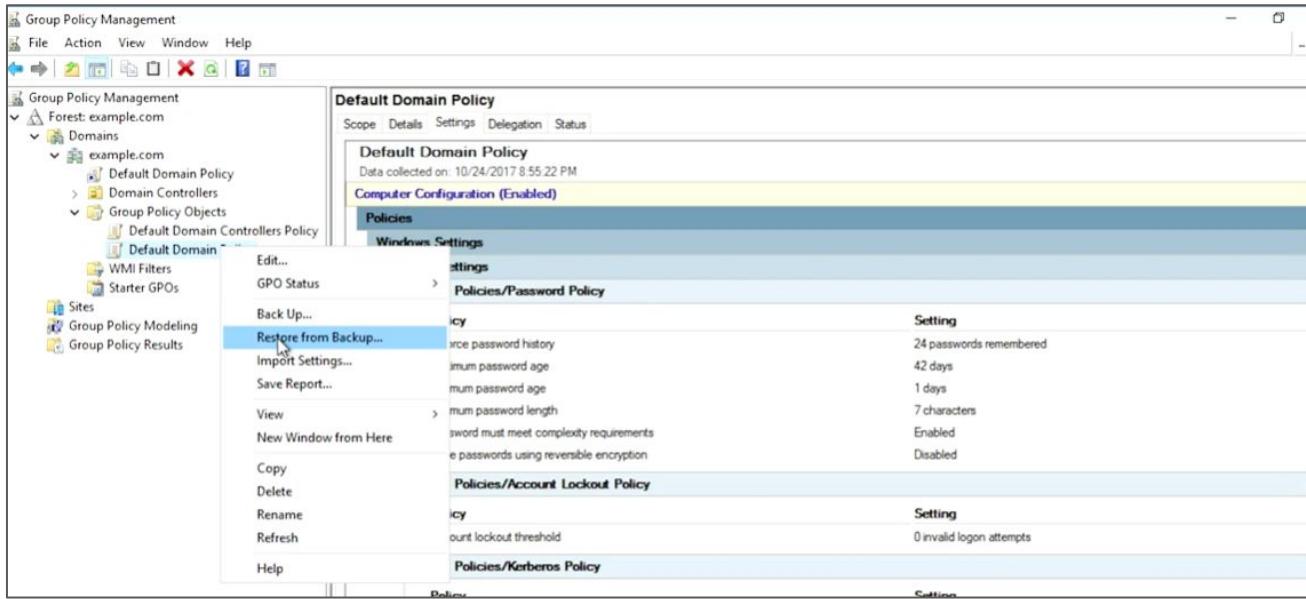
# Tạo và chỉnh sửa chính sách nhóm

- Thay đổi giá trị. Chọn Apply.
- Sự thay đổi GPO này có hiệu lực ngay lập tức.
- Các máy tính sẽ tải về bản cập nhật.



# Tạo và chỉnh sửa chính sách nhóm

Phục hồi Policy: chức năng Restore from Backup.



# Ưu tiên và kế thừa Chính sách Nhóm

- Khi áp dụng các GPO vào máy tính, tất cả các GPO này sẽ được áp dụng theo một thứ tự cụ thể dựa trên một tập **luật ưu tiên**.
- GPO của vùng chứa lớn nhất: áp dụng trước.
- GPO của vùng chứa nhỏ nhất: áp dụng sau cùng.
- Đầu tiên, GPO được liên kết tại AD **site** được áp dụng trước, sau đó là các liên kết tại miền (**domain**). Và sau đó là bất kỳ **OU** nào từ **cha mẹ** đến **con cái**.



# Ưu tiên và kế thừa Chính sách Nhóm

- Site: Australia, India
- Domain: example.com
- OU: IT, Sales

The screenshot shows the Windows Group Policy Management console. The left pane displays a tree structure of Group Policy Objects (GPOs) under the domain 'example.com'. The 'Sales' organizational unit (OU) is selected, which is highlighted in blue. The right pane shows a table of linked GPOs for the 'Sales' OU. There are two entries:

Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	Network Drives - Sales	No	Yes	Enabled	None	10/24/20...	example...
2	Network Printers - Sales	No	Yes	Enabled	None	10/24/20...	example...

# Ưu tiên và kế thừa Chính sách Nhóm

Thứ tự ưu tiên theo Link Order.

- Network Driver Sale  Network Printer Sale.

Sales							
Linked Group Policy Objects		Group Policy Inheritance		Delegation			
Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	Network Drives - Sal...	No	Yes	Enabled	None	10/24/20...	example...
2	Network Printers - S...	No	Yes	Enabled	None	10/24/20...	example...

# Ưu tiên và kế thừa Chính sách Nhóm

Group Policy Inheritance liệt kê tất cả GPO và thứ tự ưu tiên của nó.

## Computers

Linked Group Policy Objects    Group Policy Inheritance    Delegation

This list does not include any GPOs linked to sites. For more details, see Help.

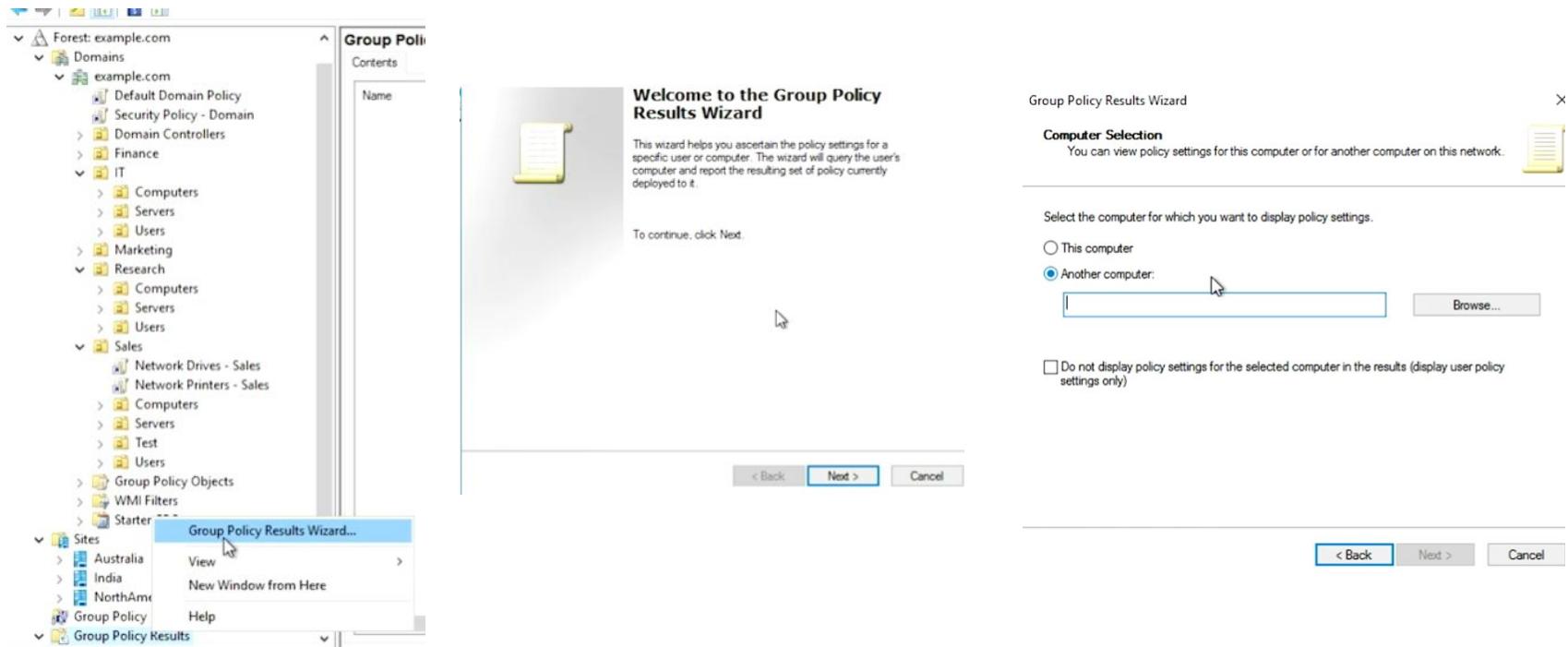
Precedence	GPO	Location	GPO Status	WMI Filter
1	Computer Security P...	Computers	Enabled	None
2	Network Drives - Sa...	Sales	Enabled	None
3	Network Printers - S...	Sales	Enabled	None
4	Security Policy - Do...	example.com	Enabled	None
5	Default Domain Policy	example.com	Enabled	None

# Ưu tiên và kế thừa Chính sách Nhóm

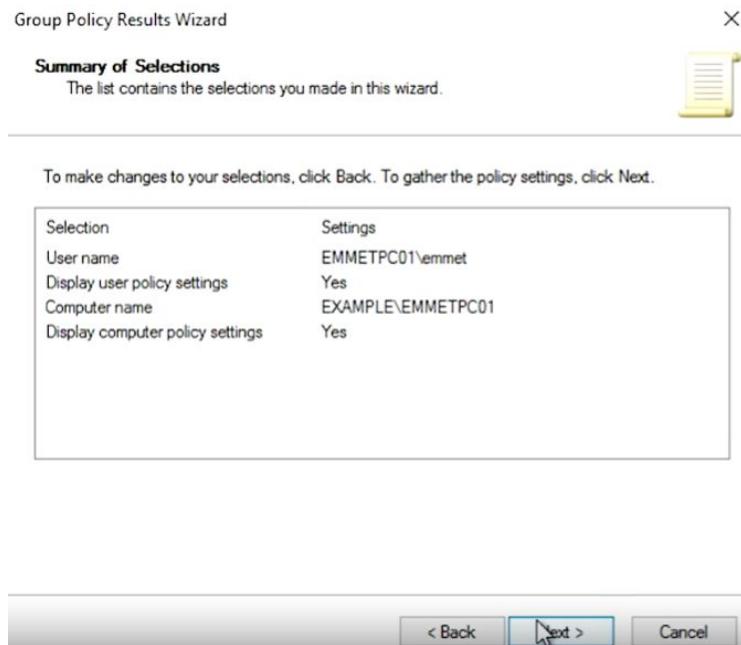
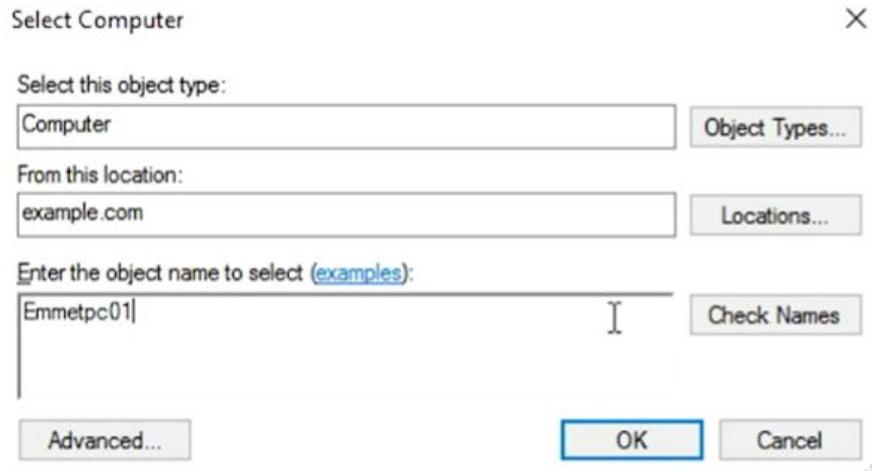
- **Resultant Set of Policy (RSoP)**: tất cả các chính sách và các quy tắc ưu tiên cho chúng.
- Khi khắc phục sự cố chính sách nhóm: bạn so sánh báo cáo RSoP với những gì mong đợi.



# Ưu tiên và kế thừa Chính sách Nhóm



# Ưu tiên và kế thừa Chính sách Nhóm



# Ưu tiên và kế thừa Chính sách Nhóm

The screenshot shows the 'Group Policy Results' window for a computer named 'emmet on EMMETPC01'. The window displays the following information:

- Computer Details:**
  - Computer name: EMMETPC01\emmet on EXAMPLE\EMMETPC01
  - Data collected on: 10/24/2017 10:39:54 PM
  - Domain: example.com
  - Site: (None)
  - Security Group Membership: show
- Component Status:**

Component Name	Status	Time Taken	Last Process Time	Event Log
Group Policy Infrastructure	Success	6 Second(s) 98 Millisecond(s)	10/24/2017 10:10:48 PM	<a href="#">View Log</a>
Registry	Success	16 Millisecond(s)	10/24/2017 10:10:45 PM	<a href="#">View Log</a>
Scripts	Success	94 Millisecond(s)	10/24/2017 10:10:46 PM	<a href="#">View Log</a>
Security	Success	2 Second(s)	10/24/2017 10:10:48 PM	<a href="#">View Log</a>
- Settings:**
  - Policies:** Windows Settings
  - Shutdown:** (Table view)

Name	Parameters	Last Run	Script Order in GPO	Winning GPO

# Gỡ rối chính sách nhóm

- Người dùng không thể đăng nhập vào máy tính của họ hoặc không thể xác thực miền Active Directory.
- Người dùng quên mật khẩu hoặc nhập sai.



# Lỗi không thể đăng nhập

- Lỗi có thể từ phía người dùng.
- Máy tính không thể định vị bộ điều khiển miền mà nó sử dụng để xác thực.
  - Kết nối mạng gặp trục trặc.
  - Lỗi liên quan đến DNS server. Không kết nối được đến DNS server hay DNS không có bản ghi SRV phù hợp.
- Vấn đề với đồng hồ.
  - Kerberos là giao thức xác thực mà AD nhạy cảm với sự khác biệt về thời gian.



# GPO không áp dụng được cho máy tính

- Máy tính trì hoãn việc cập nhật GPO mới.
  - Tối ưu hóa đăng nhập nhanh (Fast Logon Optimization).
  - Một số thay đổi GPO sẽ mất nhiều thời gian hơn để được tự động cập nhật.
- Buộc tất cả GPO được áp dụng hoàn toàn và ngay lập tức:  
`gpupdate/force`
- Tốt hơn, bạn có thể chạy:  
`gpupdate/force/sync.`

Thêm tham số `/sync` sẽ buộc đăng xuất và khởi động lại máy tính.



# GPO không áp dụng được cho máy tính

- Lỗi sao chép (Replication failure): khi thực hiện thay đổi đối với Active Directory, nó diễn ra trên một bộ điều khiển miền duy nhất.
- Sau đó phải được sao chép sang các bộ điều khiển miền khác.
- Nếu sao chép không thành công, sẽ tạo thành các GPO khác nhau, gây ra lỗi.



# Giới thiệu về OpenLDAP

- **OpenLDAP** (lightweight directory access protocol operates): nguồn mở và miễn phí.
- **Đa nền tảng**: Linux, macOS, thậm chí cả Microsoft Windows.
- Giao diện dòng lệnh (command line interface).
- Giao diện đồ họa: phpLDAPAdmin.

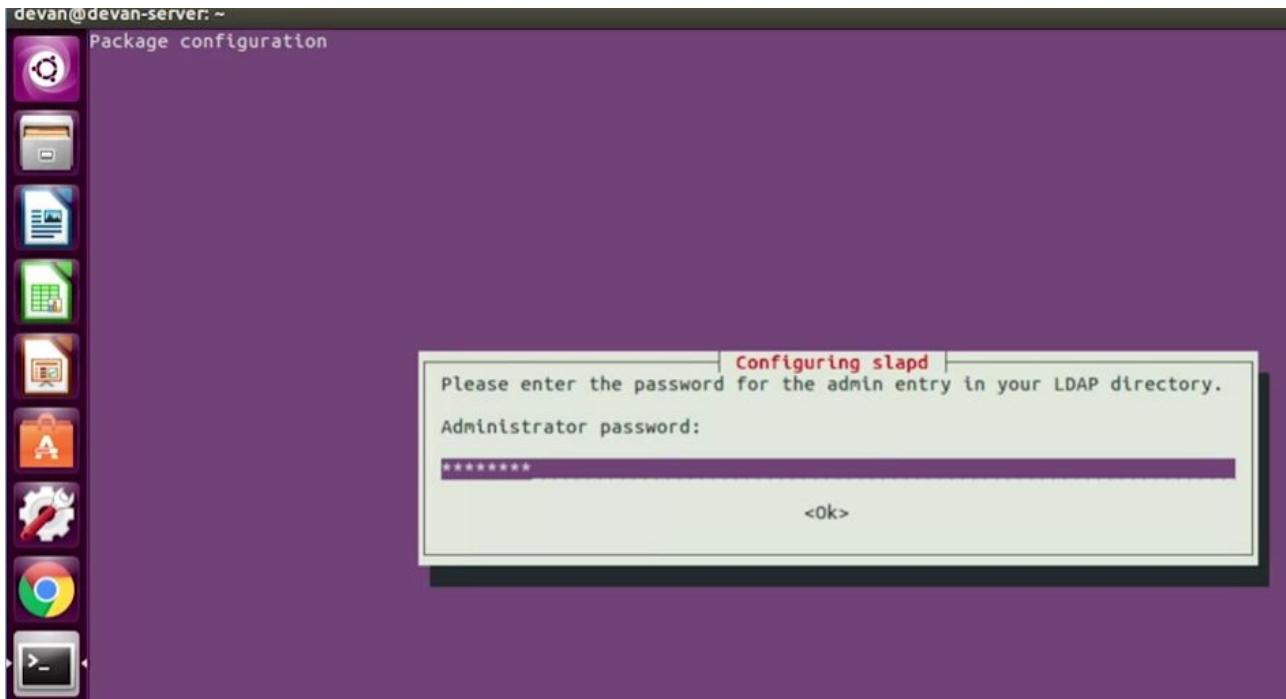


# Giới thiệu về OpenLDAP

Cài đặt: gõ lệnh *Sudo apt-get install slapd ldap-utils*

```
devan@devan-server: ~
devan@devan-server:~$ sudo apt-get install slapd ldap-utils
sudo: unable to resolve host devan-server
[sudo] password for devan:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libodbc1 libsasl1
Suggested packages:
  libsasl2-modules-gssapi-mit | libsasl2-modules-gssapi-heimdal libmyodbc odbc-postgres
The following NEW packages will be installed:
  ldap-utils libodbc1 libsasl1 slapd
0 upgraded, 4 newly installed, 0 to remove and 205 not upgraded.
Need to get 1,720 kB of archives.
After this operation, 17.1 MB of additional disk space will be used.
Do you want to continue? [Y/n] ■
```

# Giới thiệu về OpenLDAP



# Giới thiệu về OpenLDAP

Gõ `sudo dpkg-reconfigure slapd`

```
devan@devan-server: ~  
devan@devan-server:~$ sudo dpkg-reconfigure slapd
```

Một số câu hỏi

```
| Configuring slapd |  
If you enable this option, no initial configuration or database will be created for you.  
Omit OpenLDAP server configuration?
```

<Yes>

<No>

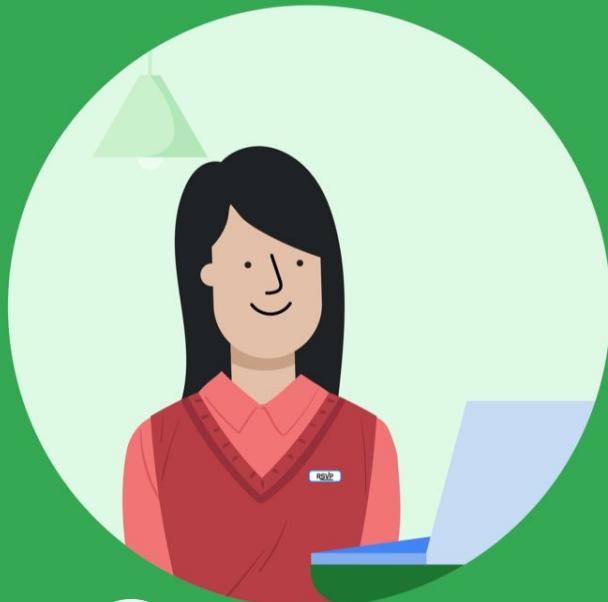
# Quản trị trong OpenLDAP

- Lệnh cho phép thêm, xóa, sửa các mục nhập trong thư mục.
- Tập tin LDIF: tập tin văn bản liệt kê các thuộc tính và giá trị.
- Ví dụ:  
`dn: uid=cindy,ou=Engineering,dc=example,dc=com  
objectClass: inetOrgPerson  
description: Cindy works in the Engineering department.  
cn: Cindy  
uid: cindy`
- Nhân viên tên là Cindy, làm việc trong bộ phận Engineer tại công ty example.com.

# Quản trị trong OpenLDAP

- **Ldapadd:** nhận đầu vào là tập tin LDIF và thêm ngữ cảnh của nó.
- **Ldapmodify:** sửa đổi một đối tượng hiện có.
- **Ldapdelete:** xóa đối tượng mà tập tin LDIF đề cập đến.
- **Ldapsearch:** tìm kiếm các mục nhập trong cơ sở dữ liệu thư mục của bạn.





# 5 Phục Hồi và Sao Lưu Dữ Liệu



# Phục hồi dữ liệu

- **Phục hồi dữ liệu** (data recovery): quá trình cố gắng khôi phục dữ liệu sau một sự kiện không mong muốn dẫn đến mất mát hoặc hỏng dữ liệu.
- Nguyên nhân:
  - Thiết bị chứa dữ liệu hư hỏng.
  - Bị tấn công phá hoại.
  - Phần mềm độc hại xóa dữ liệu quan trọng.



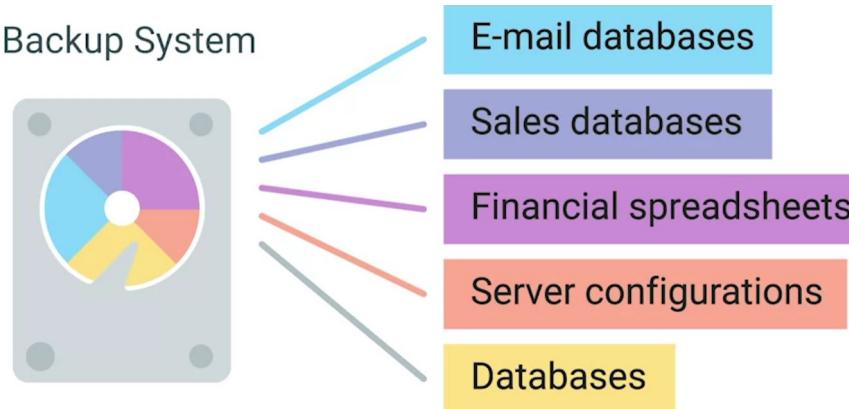
# Phục hồi dữ liệu

- Bản chất của dữ liệu bị mất
  - Thiết bị bị hỏng: khôi phục dữ liệu từ phần cứng.
- Có các bản sao lưu hay không.
  - Nếu có, bạn có thể khôi phục dữ liệu bị mất.
- Phục hồi dữ liệu là tác vụ quan trọng của hệ thống CNTT.
- Nếu có sự cố xảy ra, tổ chức có thể tiếp tục hoạt động kinh doanh của họ với mức gián đoạn tối thiểu.



# Sao lưu dữ liệu

- Xác định dữ liệu cần sao lưu: dữ liệu thực sự cần thiết và không thể tìm thấy ở nguồn khác.
  - E-mail, cơ sở dữ liệu bán hàng, bảng tính tài chính, cấu hình máy chủ và cơ sở dữ liệu.
- Quan tâm đến tổng số dữ liệu hiện có và tương lai để chọn giải pháp sao lưu phù hợp.



# Sao lưu dữ liệu

- **Sao lưu dữ liệu:** lên kế hoạch và quy trình xử lý thảm họa được suy nghĩ kỹ lưỡng.
- Sao lưu thường xuyên bất kỳ và tất cả các dữ liệu quan trọng.
- **Post-mortem:** ghi lại bất kỳ vấn đề nào phát hiện ra trong quá trình phục hồi dữ liệu.
- Dữ liệu có thể được sao lưu cục bộ hoặc sao lưu bên ngoài.



# Sao lưu dữ liệu – Cục bộ

- Ưu điểm:
  - Gần về mặt vật lý: truy cập dữ liệu nhanh hơn.
  - Cần ít băng thông.
- Khuyết điểm:
  - Mất dữ liệu nếu thảm họa xảy ra ở chính công ty.



# Sao lưu dữ liệu – Bên ngoài

- Lưu trữ ở một cơ sở khác, hay Đám mây.
- Ưu điểm:
  - Dữ liệu an toàn hơn do lưu tại nhiều vị trí khác.
- Khuyết điểm:
  - Cần cơ chế bảo mật và mã hóa.
  - Cần lượng băng thông lớn.



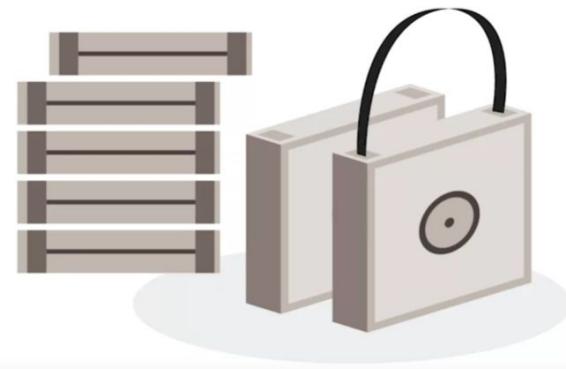
# Giải pháp sao lưu

- Tự xây dựng hệ thống sao lưu hay dùng đám mây.
- Tự xây dựng hệ thống:
  - Mua một thiết bị NAS.
  - Gắn hàng loạt ổ cứng vào NAS.
  - Gửi dữ liệu đến nó qua hệ thống mạng.
- Vấn đề với việc tự xây dựng:
  - Làm thế nào để bạn tăng dung lượng đĩa khi bạn cần thêm dung lượng lưu trữ?
  - Làm thế nào để bạn xử lý đĩa cứng bị lỗi?
- Bạn có thể triển khai cả hai: sao lưu tại chỗ và bên ngoài.
- Chú ý đến khoảng thời gian cần lưu dữ liệu sao lưu.



# Sao lưu dữ liệu – Phương tiện lưu trữ

- Cân bằng giữa chi phí và sự tiện lợi: lưu trữ chậm hơn nhưng rẻ.
- Dùng các băng từ dữ liệu (tape).
  - Lưu trữ bằng băng từ khá rẻ.
  - Không dễ hoặc nhanh chóng để truy cập như dữ liệu.
- Thường được sử dụng:
  - Lưu trữ lâu dài, xác xuất cần dùng dữ liệu thấp.
  - Chấp nhận sự chậm trễ khi muốn lấy lại dữ liệu.



# Sao lưu dữ liệu – Giải pháp sao lưu

- Tiện ích dòng lệnh **rsync**: tiện ích truyền tập tin được thiết kế để truyền và đồng bộ hóa các tập tin giữa các máy tính một cách hiệu quả.
  - Rsync hỗ trợ nén và SSH.
  - Đồng bộ hóa các tập tin giữa các máy từ xa.
- **Time Machine** của Apple: sử dụng một mô hình sao lưu gia tăng.
  - Khôi phục toàn bộ hệ thống từ các tập tin sao lưu hoặc từng tập tin riêng lẻ.
- **Backup and Restore** của Microsoft. Nó có hai chế độ hoạt động:
  - Phiên bản tập tin (file based version).
  - Ảnh hệ thống (system image).

# Kiểm tra sao lưu

- Kiểm tra quy trình phục hồi dữ liệu.
- Quy trình này cần lập thành văn bản cụ thể.
- Kiểm tra Khôi phục sau thảm họa (Disaster Recovery testing): đảm bảo hệ thống khôi phục hoạt động tốt khi sự kiện bất ngờ xảy ra như động đất, hỏa hoạn.
- Giúp phát hiện ra lỗ hổng trong kế hoạch.



# Các loại sao lưu

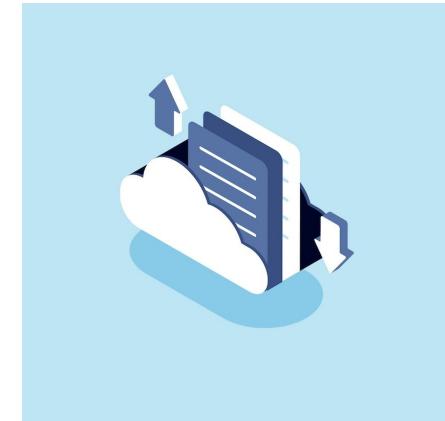
- **Sao lưu toàn bộ** (full backup): tạo một bản sao của toàn bộ dữ liệu
  - Sao lưu cho dù dữ liệu có được sửa đổi hay không.
  - Nếu dữ liệu ít thay đổi → không hiệu quả.
- **Sao lưu khác biệt** (differential backup): chỉ sao lưu các tập tin đã thay đổi hoặc được tạo kể từ lần **sao lưu toàn bộ cuối cùng**.
  - Không phải lưu trữ các bản sao lưu có dữ liệu trùng lặp.
  - **Sao lưu toàn bộ** không thường xuyên (hàng tuần), đồng thời thực hiện **sao lưu khác biệt** thường xuyên (hàng ngày).



# Các loại sao lưu

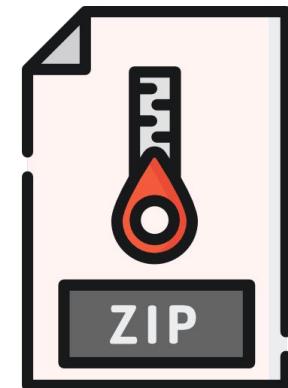
**Sao lưu gia tăng (incremental backup):** chỉ sao lưu các tập tin đã thay đổi hoặc được tạo kể từ lần **sao lưu (gia tăng) cuối cùng.**

- Chỉ sao lưu phần dữ liệu thay đổi □ tiết kiệm thời gian và không gian lưu trữ.
- Sao lưu gia tăng thường xuyên, đồng thời thực hiện bản sao lưu đầy đủ ít thường xuyên.
- Cần tất cả các bản sao lưu gia tăng để tái tạo lại toàn bộ tập tin.
- Nếu không, không thể khôi phục dữ liệu gần hơn lần **sao lưu đầy đủ** gần nhất.
- Khôi phục có thể tốn nhiều thời gian hơn.



# Các loại sao lưu – Nén dữ liệu

- **Nén dữ liệu khi sao lưu:** tiết kiệm dung lượng.
- **Nén dữ liệu:** cơ chế lưu trữ dữ liệu cần ít dung lượng ổ đĩa hơn bằng cách sử dụng các thuật toán nén phức tạp.
- Nên quan tâm đến **chi phí khôi phục**.
- Khôi phục dữ liệu từ bản sao lưu: cần được giải nén.
  - Cần nhiều thời gian và không gian đĩa.
- Lưu trữ dữ liệu sao lưu cục bộ: dung thiết bị NAS thương mại hoặc máy chủ tập tin.



# Các loại sao lưu – RAID

- **RAID** (Redundant Array of Independent Disks): phương pháp lấy nhiều đĩa vật lý và kết hợp chúng thành một đĩa ảo lớn.
- RAID là một cách tuyệt vời để lưu trữ dữ liệu, đồng thời giảm thiểu nguy cơ mất dữ liệu.
- **Lưu ý:** RAID không phải là một giải pháp sao lưu, nó là một giải pháp lưu trữ dữ liệu.
  - RAID không bảo vệ khỏi việc vô tình xóa tập tin.
  - Hoặc phần mềm độc hại làm hỏng dữ liệu của bạn.



# Sao lưu dữ liệu từ phía người dùng

Sao lưu dữ liệu từ phía người dùng.

Khó khăn:

- Nhiều thiết bị khác nhau.
- Tính di động của máy tính xách tay, điện thoại và máy tính bảng.

Giải pháp: sử dụng dịch vụ đám mây được thiết kế để đồng bộ hóa và sao lưu tập tin trên các nền tảng và thiết bị.

- Dropbox, Apple iCloud và Google Drive.
- Dễ sử dụng.



# Kế hoạch phục hồi sau thảm họa

- **Kế hoạch phục hồi sau thảm họa** (disaster recovery plan): tập hợp các quy trình và kế hoạch được lập thành văn bản về cách phản ứng và xử lý tình huống khẩn cấp hoặc thảm họa.
- **Bao gồm**: những việc nên làm trước, trong và sau thảm họa.
- **Mục tiêu**: giảm thiểu sự gián đoạn đối với hoạt động kinh doanh và CNTT.
- Kế hoạch phục hồi sau thảm họa:
  - **Biện pháp phòng ngừa**.
  - **Biện pháp phát hiện**.
  - **Biện pháp khắc phục**.

# Kế hoạch phục hồi sau thảm họa

- **Biện pháp phòng ngừa** (Preventative measures): bất kỳ quy trình hoặc hệ thống được áp dụng để chủ động giảm thiểu tác động của thảm họa.
  - Sao lưu thường xuyên.
  - Chuẩn bị hệ thống dự phòng.
- **Biện pháp phát hiện** (Detection measures): cảnh báo rằng một thảm họa đang xảy ra.
  - Cảm biến môi trường.
  - Cảm biến lũ lụt.
  - Cảm biến nhiệt độ và độ ẩm.
  - Thiết bị báo cháy và báo khói.
  - Quy trình sơ tán.

# Kế hoạch phục hồi sau thảm họa

**Biện pháp khắc phục hoặc phục hồi** (corrective, recovery measures): biện pháp được thực thi sau khi thảm họa xảy ra.

- Khôi phục dữ liệu bị mất từ bản sao lưu.
- Xây dựng lại và cấu hình lại hệ thống bị hỏng.

Sau khi phát hiện thảm họa và ngăn chặn sự cố: chúng ta sẽ bắt đầu khôi phục hoạt động đầy đủ của mọi thứ bị ảnh hưởng.



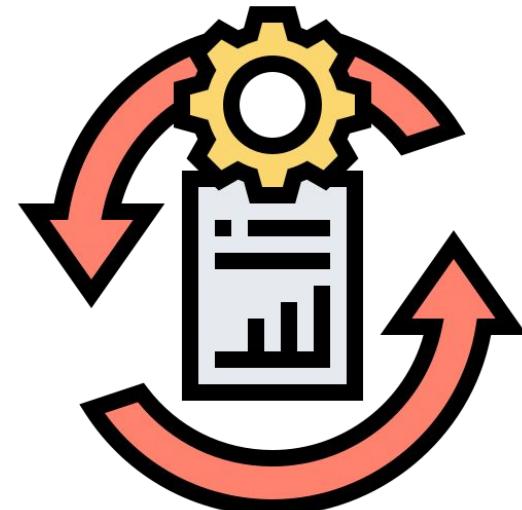
# Đánh giá rủi ro

- Đánh giá rủi ro: cho phép bạn tập trung hơn vào những phần có mức độ rủi ro cao.
- Thảo luận các tình huống giả định và phân tích các sự kiện để hiểu chúng sẽ tác động như thế nào đến tổ chức và công việc.
- Khi xem xét các biện pháp phòng ngừa, hãy chú ý đến các hệ thống thiểu dự phòng.
  - Có máy chủ dự phòng trong trường hợp máy chủ chính bị hư.



# Hệ thống sao lưu và phục hồi

- Hệ thống sao lưu và phục hồi, cùng với một chiến lược tốt.
- Sao lưu thường xuyên, tự động.
- Phải có quy trình khôi phục dữ liệu được ghi chép rõ ràng.
- Bảo đảm việc dự phòng:
  - Cung cấp điện, hệ thống thông tin liên lạc, liên kết dữ liệu và phần cứng.
- Kiểm tra tài liệu vận hành. Đảm bảo rằng mọi quy trình vận hành quan trọng đều được lập thành văn bản và có thể truy cập được.



# Biện pháp phát hiện, báo động và kiểm tra

Đảm bảo rằng bạn đã thiết lập một hệ thống có thể phát hiện và cảnh báo về sự cố hoặc các điều kiện môi trường bất thường.

Ví dụ:

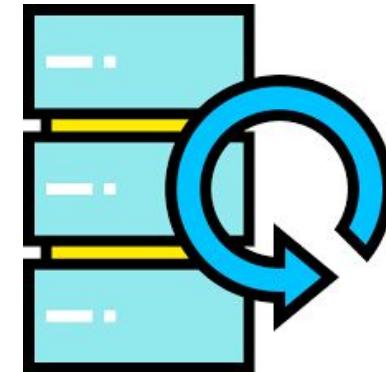
- Thông báo nếu đường truyền Internet gặp trục trặc.
- Nếu nhiệt độ trong phòng máy chủ tăng cao. Bạn cần được thông báo vấn đề để sớm giải quyết.

Hệ thống cảnh báo sớm cho phép đối phó với thảm họa trước khi nó thực sự xảy ra.



# Biện pháp phục hồi

- **Biện pháp phục hồi:** các hành động được thực hiện để khôi phục hoạt động như bình thường và phục hồi sau sự cố.
- Bao gồm: khôi phục cơ sở dữ liệu bị hỏng, cấu hình lại máy chủ.
- Tài liệu khôi phục sau thảm họa không cần phải chứa các chi tiết về các hành động.
- Chuẩn bị cho các tình huống chưa được ghi lại trong tài liệu.



# Post-mortem là gì?

- Chúng ta tạo ra **post-mortem** sau sự cố hay khi sự kiện diễn ra không như mong muốn.
- Post-mortem: ghi lại chi tiết, chính xác những gì đã xảy ra trước, trong và sau sự kiện, làm rõ những điều đã diễn ra.
- Mục đích của post-mortem: để học hỏi, không phải để trừng phạt hay chỉ trích
  - Tại sao sai lầm xảy ra và cách ngăn chúng tái diễn.
- Chia sẻ post-mortem khuyến khích văn hóa học hỏi từ những sai lầm.



# Cách viết Post-mortem

Post-mortem gồm các thành phần chính như sau:

- Tóm tắt ngắn gọn.
- Mốc thời gian chi tiết.
- Nguyên nhân vấn đề.
- Giải pháp và nỗ lực khôi phục.
- Hành động để ngăn tình huống lặp lại.



# Bảng tóm tắt

Đoạn ngắn để tóm tắt sự việc. Bao gồm:

- Sự cố là gì?
- Nó kéo dài bao lâu?
- Nó gây tác động gì?
- Nó đã được sửa như thế nào?

Ghi rõ múi giờ khi liệt kê thời gian và ngày tháng trong post-mortem.



# Mốc thời gian chi tiết

Mốc thời gian chi tiết cho các sự kiện chính. Bao gồm tất cả mọi thứ đã xảy ra:

- Khi nào sự kiện bắt đầu.
- Khi nào những người liên quan biết.

Mọi hành động được thực hiện nhằm giải quyết tình huống.

Thời gian, ngày tháng, múi giờ, và ai đã làm gì.

Tiến trình kết thúc với các hành động để giải quyết sự cố, báo hiệu sự kiện kết thúc.



# Nguyên nhân vấn đề

Bản tường trình chi tiết về các nguyên nhân gây ra vấn đề.

Ví dụ như:

Một sự thay đổi cấu hình không được kiểm tra đầy đủ.

- Cải thiện quy trình kiểm tra

Lỗi đánh máy.

- Tự động hóa quy trình nhập liệu



# Giải pháp và nỗ lực khôi phục

Giải thích chi tiết về giải pháp và nỗ lực khôi phục.

Tương tự như dòng thời gian ở bên trên, phải bao gồm ngày, giờ và múi giờ.

Chi tiết hơn về:

- Các bước đã được thực hiện để khôi phục.
- Cơ sở lý luận và lý do cho hành động đó.
- Kết quả của mỗi hành động bao gồm lý do.



# Hành động để ngăn tình huống lặp lại

Kết thúc báo cáo với danh sách các hành động cụ thể cần được thực hiện để tránh tình huống tương tự xảy ra lần nữa.

Bao gồm:

- Hành động nhằm cải thiện việc xử lý phản hồi.
- Cải thiện hệ thống giám sát.



# Những điều đã diễn ra tốt đẹp

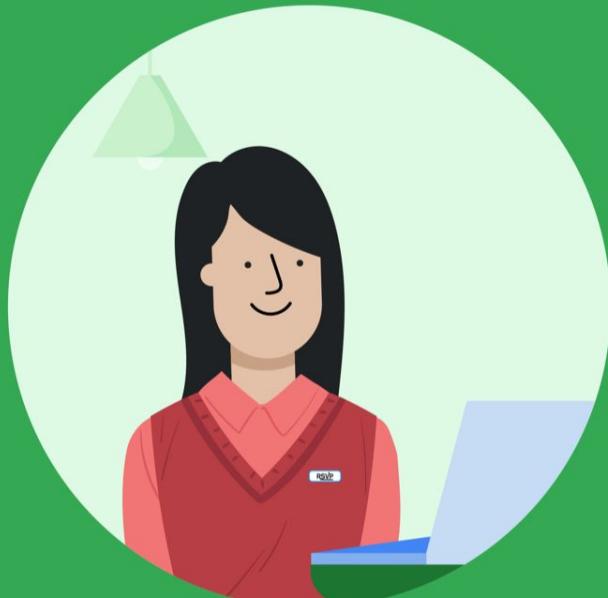
Trong quá trình phân tích sau sự cố: nên làm rõ những điều đã diễn ra tốt đẹp.

Bao gồm:

- Sự cố xảy ra một cách an toàn.
- Trong sự tính toán.
- Ngăn ngừa việc lan rộng sự cố.
- Giảm thiểu mức độ nghiêm trọng của sự cố.

Điều này chứng minh tính hiệu quả của hệ thống.





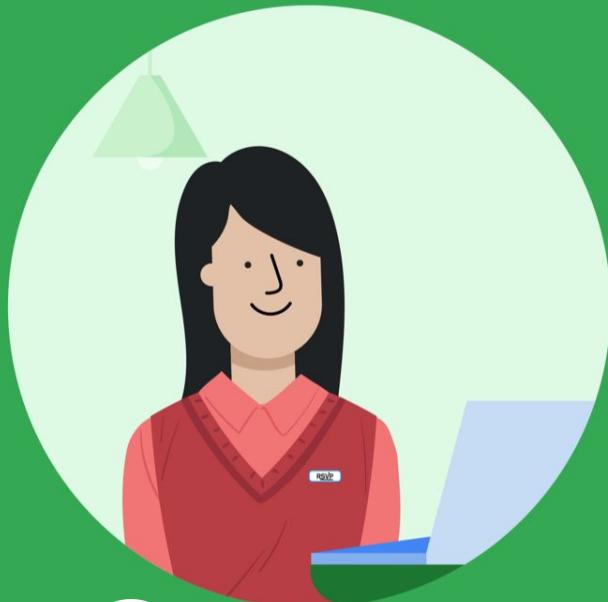
# Tổng kết



# Những điều cần nắm

- Những thông lệ tốt nhất để chọn phần cứng, nhà cung cấp và dịch vụ cho tổ chức của mình.
- Các dịch vụ cơ sở hạ tầng phổ biến nhất hoạt động và cách quản trị các máy chủ cơ sở hạ tầng.
- Hiểu cách tận dụng tối đa ưu thế của điện toán đám mây cho tổ chức của mình.
- Quản lý máy tính và người dùng của tổ chức bằng cách sử dụng các dịch vụ thư mục: Active Directory và OpenLDAP.
- Chọn và quản lý các công cụ mà tổ chức của bạn sẽ sử dụng.





# THANK YOU

