# Tuần 4: Xây dựng kế hoạch triển khai, chuẩn bị tài nguyên

## 4.1 Xác định yêu cầu phần cứng

### 4.1.1 Chức năng

* **Network Equipment:**
* 1 Router FPT
* 1 Firewall
* 1 Core Switch Layer 3
* 2-3 Switch Layer 2
* 6-8 Access Point WiFi 6
* **Thiết bị cho từng phòng ban:**
* Tổng số PC: ~78 chiếc
* IP Phone: ~15 chiếc
* Máy in: ~6 chiếc
* Máy chiếu: 2 chiếc
* Tivi: ~15 chiếc
* Máy chủ (Server): 6 chiếc
* **Chức năng của từng thiết bị:**
* **6 server 2016:** Trên mỗi server sẽ chạy một dịch vụ khác nhau để tiết kiểm chi phí.
* **Domain Controller (MVTC-DC):** Đây là server chính trong một mạng domain. Nhiệm vụ chính của Domain Controller là quản lý tài nguyên mạng, bao gồm việc xác thực người dùng, quản lý phân quyền, cấp phát địa chỉ IP, và quản lý các đối tượng trong domain như user accounts, group policies, và computer accounts.
* **Additional Domain (MVTC-DC-01):** Đây là server đồng cấp với server chính trong mạng domain. Nhiệm vụ chính của Additional Domain là hỗ trợ và tối ưu hóa hoạt động của hệ thống mạng, giúp cho Domain Controller hoạt động một cách hiệu quả nhất.
* **File Server:** File Server là nơi lưu trữ và chia sẻ các tệp tin và thư mục trong mạng domain. Các người dùng có thể truy cập vào các tệp tin này từ máy tính của họ trong mạng domain thông qua quyền truy cập được cấp phát bởi Domain Controller.
* **Mail Server:** Mail Server quản lý và phân phát thư điện tử trong mạng domain. Nó có thể cung cấp các dịch vụ như gửi và nhận thư, lưu trữ thư, bảo mật thư điện tử và quản lý danh sách đen/trắng.
* **Web Server:** Web Server cung cấp các dịch vụ truy cập các trang web và ứng dụng web trong mạng domain. Nó có thể được sử dụng để chạy các ứng dụng web nội bộ hoặc truy cập vào các tài nguyên web công cộng.
* **Database Server:** Database Server lưu trữ và quản lý dữ liệu trong mạng domain. Nó cung cấp các dịch vụ như lưu trữ dữ liệu, truy vấn dữ liệu, và cung cấp dữ liệu cho các ứng dụng khác trong mạng.
* **Switch:** là một thiết bị mạng được sử dụng để kết nối nhiều thiết bị mạng lại với nhau trong một mạng LAN, tuy nhiên, switch cung cấp nhiều ưu điểm hơn so với hub.
* **Chuyển Mạch (Switching):** Switch có khả năng phân loại dữ liệu và chỉ chuyển tiếp gói tin đến thiết bị đích mà nó định trước, điều này làm giảm tải trên mạng và tăng hiệu suất.
* **Băng Thông Lớn Hơn:** Switch thường có băng thông cao hơn so với hub, cho phép truyền dữ liệu nhanh hơn và hỗ trợ số lượng kết nối lớn hơn.
* **Bảo Mật Hơn:** Switch hỗ trợ các tính năng bảo mật như VLANs (Virtual Local Area Networks), cung cấp phương tiện để tách mạng thành các phần riêng biệt và giảm nguy cơ từ các cuộc tấn công mạng.
* **Hỗ Trợ Full Duplex:** Switch cho phép truyền và nhận dữ liệu đồng thời trên cùng một cổng, tăng tốc độ truyền dữ liệu so với half duplex như ở hub.
* **Quản Lý:** Một số switch cung cấp tính năng quản lý mạng như cấu hình VLANs, giám sát mạng và quản lý băng thông, giúp người quản trị mạng có khả năng điều chỉnh và tối ưu hóa mạng của họ.
* **Router:** là một thiết bị mạng quan trọng được sử dụng để chuyển tiếp các gói dữ liệu giữa các mạng máy tính. Nó thực hiện chức năng định tuyến, giúp các thiết bị trong mạng nội bộ (LAN) kết nối với nhau và với mạng bên ngoài như Internet.
* **Định tuyến dữ liệu:** Router xác định đường đi tốt nhất cho các gói dữ liệu từ nguồn đến đích qua các mạng khác nhau.
* **Kết nối mạng nội bộ với Internet:** Router kết nối mạng nội bộ (LAN) với mạng diện rộng (WAN) như Internet, cho phép các thiết bị trong mạng truy cập Internet.
* **Quản lý lưu lượng mạng:** Router quản lý và phân phối lưu lượng dữ liệu, giúp tối ưu hóa hiệu suất mạng và đảm bảo kết nối ổn định.
* **Bảo mật mạng:** Router cung cấp các tính năng bảo mật như tường lửa (firewall), lọc địa chỉ IP, lọc địa chỉ MAC, và VPN để bảo vệ mạng khỏi các mối đe dọa từ bên ngoài.
* **Cấp phát địa chỉ IP:** Router thường tích hợp máy chủ DHCP để cấp phát địa chỉ IP tự động cho các thiết bị trong mạng.
* **Firewall:** là một hệ thống an ninh mạng quan trọng được thiết kế để giám sát và kiểm soát lưu lượng mạng đến và đi dựa trên các quy tắc bảo mật đã được xác định trước. Nó hoạt động như một hàng rào bảo vệ giữa mạng nội bộ an toàn và các mạng không an toàn bên ngoài, chẳng hạn như Internet.
* **Kiểm soát truy cập:** Tường lửa cho phép hoặc chặn lưu lượng mạng dựa trên các tiêu chí đã được xác định trước, chẳng hạn như địa chỉ IP, cổng, giao thức và loại lưu lượng.
* **Bảo vệ chống lại các mối đe dọa bên ngoài:** Tường lửa ngăn chặn các cuộc tấn công từ bên ngoài như tấn công DDoS, truy cập trái phép, và các phần mềm độc hại.
* **Bảo mật mạng nội bộ:** Tường lửa bảo vệ các thiết bị và dữ liệu trong mạng nội bộ khỏi các mối đe dọa tiềm ẩn từ bên trong và bên ngoài.
* **Giám sát và ghi lại hoạt động:** Tường lửa theo dõi và ghi lại các hoạt động mạng, giúp phát hiện và phản ứng với các sự cố an ninh.

### 4.1.2 CPU

Quyết định sự thành công máy chủ ảo hóa trong môi trường có quy mô nhỏ hơn bắt đầu bằng máy chủ lưu trữ vật lý (host). Mặc dù nó sẽ chịu trách nhiệm cho việc lưu trữ hàng tá máy chủ ảo, nhưng lại yêu cầu tài nguyên trên bộ xử lý (CPU) khá ít.

Tùy theo phần mềm ảo hóa (chẳng hạn hypervisor), chúng ta sẽ có thể chạy máy chủ ảo hóa trên CPU 4 hoặc 6 nhân. Lý do là hầu hết máy chủ ảo hóa được vận hành gần như ở trạng thái duy trì (idle) trong phần lớn thời gian. Khi máy chủ ảo hóa bắt đầu chạy, tài nguyên của chúng có khuynh hướng chia ra cho CPU, RAM, đĩa cứng và truy xuất mạng vào/ra, trong đó chỉ một số máy chủ ảo yêu cầu tài nguyên CPU đáng kể. Bằng cách tận dụng ưu điểm này, chúng ta có thể phối hợp chặt chẽ nhiều máy chủ vật lý trên cùng một máy chủ lưu trữ duy nhất.

Tuy nhiên, đối với các máy chủ cơ sở dữ liệu, tải dữ liệu nhiều không thích hợp cài đặt trên máy chủ ảo hóa. Tất cả tùy thuộc vào tài nguyên phần cứng trên máy chủ lưu trữ, tính năng phần mềm ảo hóa, và cũng tùy thuộc vào những quy định của máy chủ ảo hóa. Việc thiết lập và kiểm tra các yêu cầu này trước khi thực hiện là điều không quá khó.

Chọn phần cứng, một nguyên tắc cần nhớ là chọn CPU đa nhân và có tốc độ xung nhịp lớn dành cho máy chủ lưu trữ; nếu có CPU 4 nhân tốc độ 2,93GHz và CPU 6 hoặc 12 nhân tốc độ 2,4GHz, chúng ta nên chọn CPU 6 hoặc 12 nhân. Bởi vì khả năng chia tải máy chủ ảo trên CPU đa nhân nhanh hơn, hiệu suất hoạt động đồng bộ hơn trên tất cả máy chủ ảo.

### 4.1.3 RAM

Máy chủ lưu trữ ảo hóa có thể luôn dùng nhiều bộ nhớ hệ thống (RAM), vì vậy hãy trang bị càng nhiều RAM càng tốt, và lựa chọn loại RAM nhanh nhất có thể. Mặt khác, việc phân bổ RAM cũng bị khống chế khắt khe hơn nhiều so với CPU. Càng nhiều RAM, bạn càng có thể có nhiều máy chủ ảo hóa.

Trong môi trường nhỏ hơn, bạn có thể không cần mạng lưu trữ hay thiết bị lưu trữ qua mạng để lưu ảnh máy chủ ảo hóa, vì máy chủ lưu trữ sẽ chịu trách nhiệm cho công việc này. Trong trường hợp đó, càng nhiều đĩa cứng càng tốt. Yêu cầu chung, ổ đĩa SATA chạy RAID 5 hay RAID 6 thì đủ đáp ứng, mặc dù ổ đĩa cứng SAS (Serial Attached SCSI) cung cấp hiệu suất hoạt động hiệu quả hơn.

### 4.1.4 HDD/SDD

Vì đây là một mô hình mạng khá lớn nên máy chủ cũng cần có một dung lượng bộ nhớ trong cũng phải lớn để đám ứng được nhu cầu cao về tốc độ truy cập file. Vậy nên khuyến cáo sử dụng ổ đĩa SSD cho hệ điều hành và ứng dụng đòi hỏi hiệu suất cao, chẳng hạn như cơ sở dữ liệu và máy chủ ứng dụng. Với mô hình trên 500 nhân sự, chúng ta cần ít nhất 5 TB SSD cho dung lượng cơ bản. Tuy nhiên, để đảm bảo hiệu suất và khả năng mở rộng, chúng ta có thể cân nhắc sử dụng các SSD dung lượng lớn hơn như 6-8 TB hoặc sử dụng nhiều ổ SSD và cấu hình RAID 10 để tăng hiệu suất và dự phòng.

### 4.1.5 Băng thông mạng

Trong nhiều trường hợp, máy chủ vật lý chỉ dùng 1 hay 2 card mạng để hỗ trợ toàn bộ môi trường ảo hóa, nhưng nếu bộ chuyển mạch mạng (switch) cho phép bạn gộp đường kết nối để tăng băng thông cho máy chủ ảo thì rất tốt. Việc gộp 2 hay nhiều card mạng tốc độ gigabit, giúp chúng ta tạo một card mạng ảo lớn hơn, hỗ trợ nhiều băng thông hơn cho người dùng và cho các máy chủ vật lý khác trên mạng. Nhiều bộ chuyển mạch tầm trung hỗ trợ tính năng này.

Nếu bộ chuyển mạch mạng thiếu tính năng gộp đường kết nối, chúng ta có thể dành một card mạng cho một máy chủ có tải nhiều nhất. Card mạng gigabit giờ cũng khá rẻ, vì vậy hãy trang bị ít nhất 4 card mạng gigabit cho máy chủ vật lý.

## 4.2 Triển khai

### 4.2.1 Phần mềm ảo hóa Hyper-V

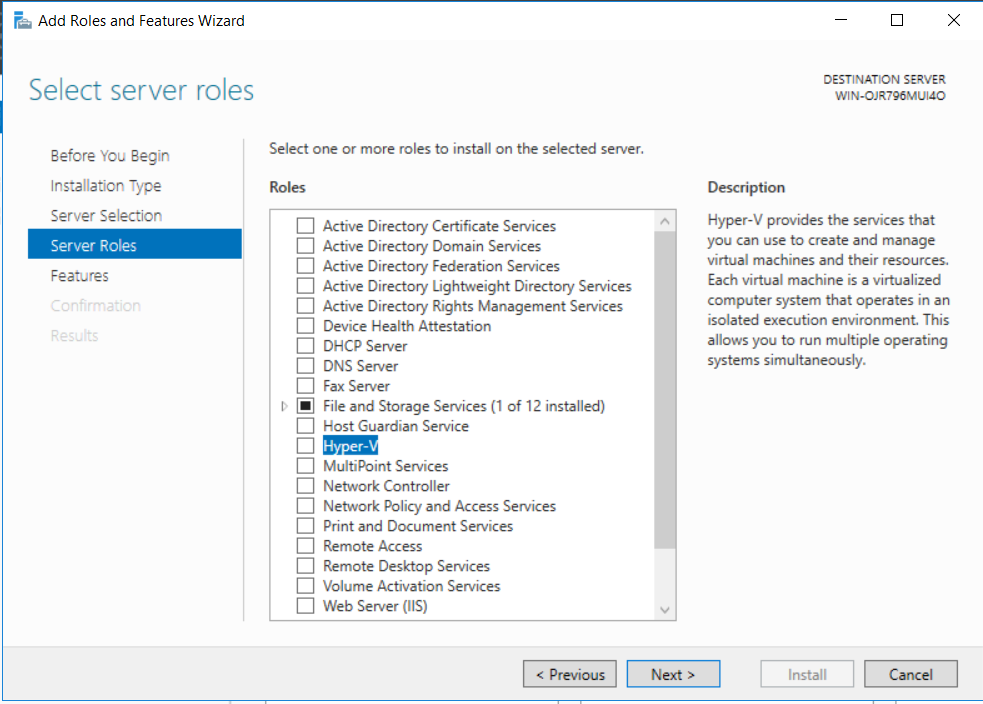
Hyper-V là một nền tảng ảo hóa mạnh mẽ được phát triển bởi Microsoft, cho phép người dùng tạo ra các máy chủ ảo trên một máy chủ vật lý. Với tính năng tạo máy chủ ảo, Hyper-V giúp tiết kiệm chi phí phần cứng và quản lý tài nguyên hiệu quả hơn. Cải thiện sự sẵn sàng và độ tin cậy: Hyper-V hỗ trợ các tính năng như live migration, clustering và load balancing để giúp tăng tính sẵn sàng và độ tin cậy của hệ thống máy chủ ảo. Giảm thời gian chết máy và tối ưu hóa tài nguyên: Hyper-V cho phép người dùng dễ dàng di chuyển các máy chủ ảo giữa các máy chủ vật lý và phân bổ tài nguyên (CPU, RAM, lưu trữ) cho các máy chủ ảo theo nhu cầu.

Tuy nhiên, vai trò của Hyper-V không chỉ dừng lại ở việc tạo máy chủ ảo. Nó còn cung cấp các tính năng quản lý tài nguyên và tính sẵn sàng, bao gồm Dynamic Memory, Live Migration và Failover Clustering, giúp tăng tính sẵn sàng và độ tin cậy của hệ thống máy chủ ảo.

Ngoài ra, Hyper-V còn hỗ trợ nhiều hệ điều hành khác nhau, bao gồm Windows, Linux và các hệ điều hành khác chạy trên kiến trúc x86 và x64.

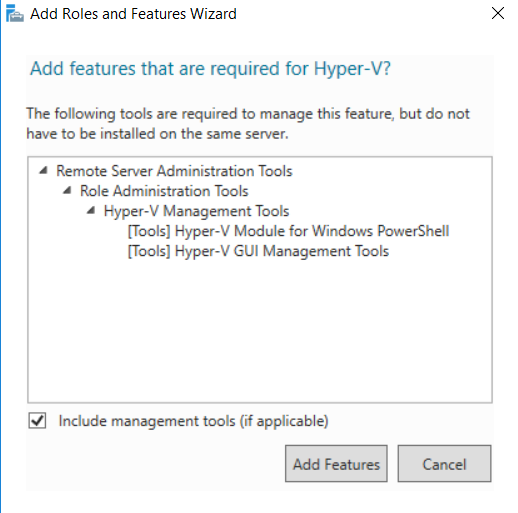
### 4.2.2 Cài đặt Hyper-V trên Windows Server 2016

* Thực hiện trên máy vật lý **MVTC-Host-01**, tại cửa sổ **Server Roles** click chọn vào dịch vụ **Hyper-V**



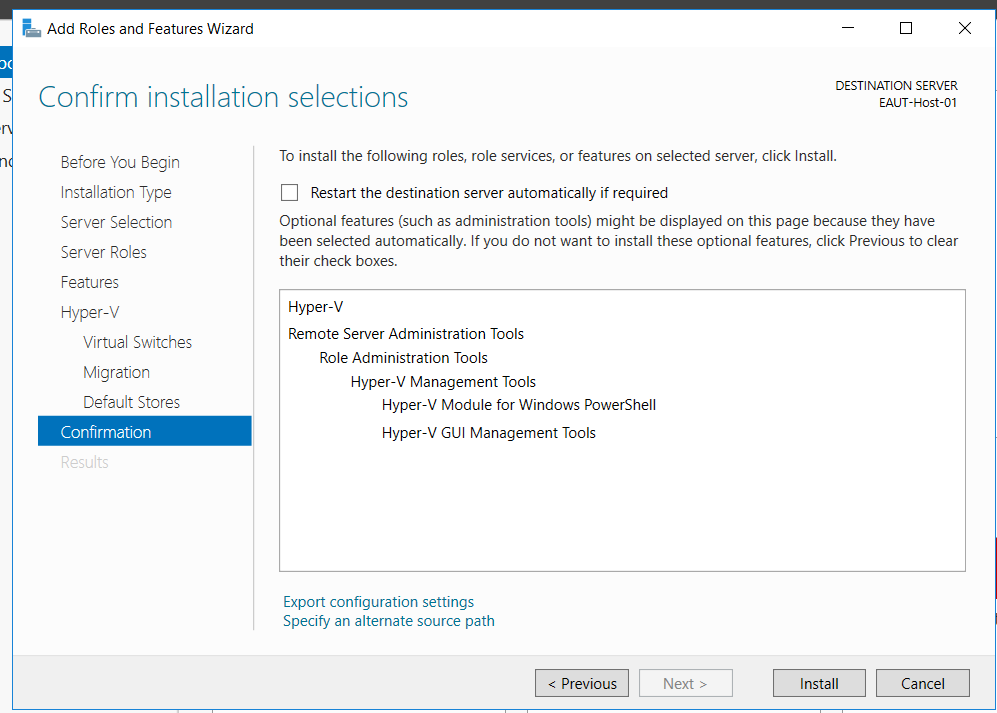
Hình . Cài đặt Hyper-V (hình 1)

* Cửa sổ **Add Roles and Features Wizard** hiện ra, chọn **Add Features**.



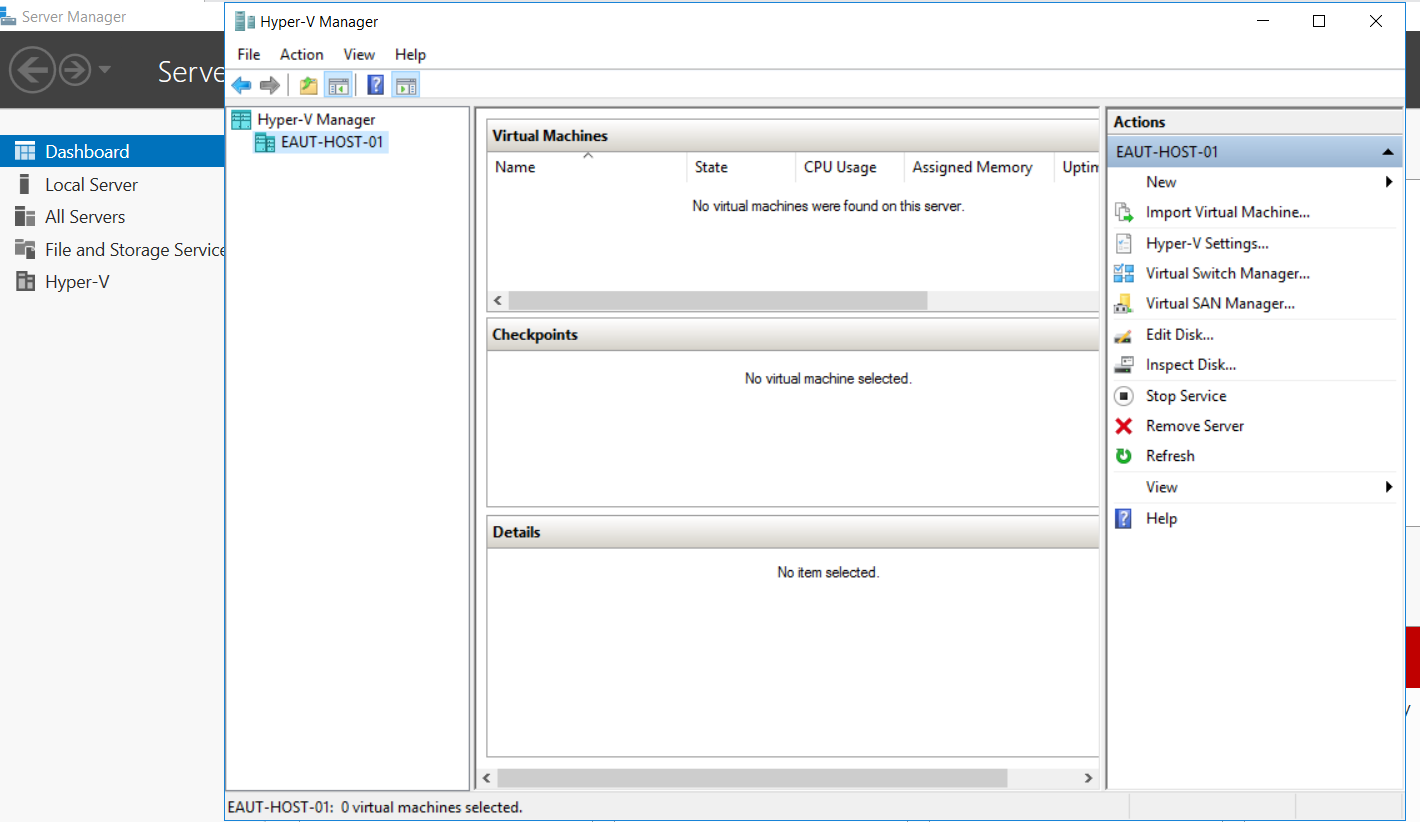
Hình . Cài đặt Hyper-V (hình 2)

* Tiếp tục ấn **Next**, tại cửa sổ **Confirm installation selections**, click vào **Install** để cài đặt dịch vụ.



Hình . Cài đặt Hyper-V (hình 3)

* Kết quả của cài đặt



Hình . Cài đặt thành công Hyper-Vin