ỦY BAN NHÂN DÂN THÀNH PHỐ HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC SÀI GÒN

KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO ĐỒ ÁN CHUYÊN NGÀNH

MÔN HỌC: ẢO HÓA

Sinh viên: Trương Gia Thành

MSSV: 3121410456

GVHD: Lương Minh Huấn

TP. HỒ CHÍ MINH, THÁNG 10 NĂM 2024

LỜI MỞ ĐẦU

Trong thời đại công nghệ thông tin phát triển vượt bậc, việc quản lý và tối ưu hóa tài nguyên hệ thống trở thành một thách thức lớn đối với các doanh nghiệp. Công nghệ ảo hóa đã nổi lên như một giải pháp tiên tiến, giúp các tổ chức tiết kiệm chi phí, nâng cao hiệu suất và đảm bảo tính linh hoạt trong quản lý hệ thống. Trong số các nền tảng ảo hóa hiện nay, VMware vSphere được xem là một trong những giải pháp hàng đầu, cung cấp các tính năng mạnh mẽ và hiệu quả cho việc ảo hóa máy chủ.

VMware vSphere không chỉ giúp tối ưu hóa việc sử dụng tài nguyên phần cứng mà còn mang lại nhiều lợi ích khác như giảm thiểu thời gian downtime, tăng cường khả năng phục hồi sau thảm họa, và cải thiện hiệu suất làm việc của hệ thống. Với khả năng quản lý tập trung và tự động hóa cao, vSphere giúp các doanh nghiệp dễ dàng triển khai và quản lý các máy ảo, từ đó nâng cao hiệu quả hoạt động và giảm thiểu chi phí vận hành.

Đồ án này sẽ tập trung nghiên cứu và ứng dụng công nghệ ảo hóa VMware vSphere, nhằm cung cấp cái nhìn tổng quan về các tính năng, lợi ích và cách triển khai hệ thống ảo hóa này trong môi trường doanh nghiệp. Cụ thể, tôi sẽ đi sâu vào các khía cạnh sau:

Tổng quan về công nghệ ảo hóa: Giới thiệu về khái niệm ảo hóa, các loại ảo hóa phổ biến và lợi ích của việc sử dụng công nghệ ảo hóa trong quản lý hệ thống.

Giới thiệu về VMware vSphere: Trình bày tổng quan về nền tảng vSphere, các thành phần chính của vSphere như ESXi, vCenter Server, và các tính năng nổi bật của vSphere.

Lợi ích của việc sử dụng vSphere: Phân tích các lợi ích mà vSphere mang lại cho doanh nghiệp, bao gồm tối ưu hóa tài nguyên, giảm thiểu chi phí, nâng cao hiệu suất và khả năng phục hồi sau thảm họa.

Triển khai và cấu hình vSphere: Hướng dẫn chi tiết về cách cài đặt và cấu hình vSphere, từ việc chuẩn bị môi trường, cài đặt ESXi, cấu hình vCenter Server, đến việc tạo và quản lý các máy ảo.

Quản lý và giám sát hệ thống vSphere: Trình bày các công cụ và phương pháp quản lý, giám sát hệ thống vSphere, bao gồm việc sử dụng vSphere Client, vSphere Web Client, và các công cụ giám sát hiệu suất.

Bảo mật trong môi trường vSphere: Phân tích các vấn đề bảo mật trong môi trường ảo hóa và các biện pháp bảo mật mà vSphere cung cấp để bảo vệ hệ thống và dữ liệu.

Các trường hợp ứng dụng thực tế: Đưa ra các ví dụ và trường hợp ứng dụng thực tế của vSphere trong các doanh nghiệp, từ các doanh nghiệp nhỏ đến các tổ chức lớn.

Tôi hy vọng rằng, thông qua đồ án này, người đọc sẽ hiểu rõ hơn về công nghệ ảo hóa vSphere và có thể áp dụng những kiến thức này vào thực tiễn, góp phần nâng cao hiệu quả quản lý và vận hành hệ thống công nghệ thông tin. Việc nắm vững và triển khai thành công công nghệ ảo hóa không chỉ giúp doanh nghiệp tiết kiệm chi phí mà còn tạo ra một nền tảng vững chắc cho sự phát triển bền vững trong tương lai. Xin cảm ơn thầy Lương Minh Huấn đã tận tình hướng dẫn.

MỤC LỤC

Danh mục hình ảnh

Danh mục từ viết tắt

TT	Từ viết tắt	Ý nghĩa từ viết tắt
1	VM	Virtual Machine
2	ESXI	Phần mềm ảo hoá cơ bản do VMware phát triển cho vSphere
3	vDS	vSphere Distributed Switch
4	vSS	vSphere Standard Switch
5	SSO	Single Sign-On
6	NIC	Network Interface Card
7	LACP	Link Aggregation Control Protocol

Chương I. Tìm hiểu về các khái niệm vSphere, vCenter, Physical Infrastructure, Virtual Infrastructure, Virtual Machine (VM), vSphere (Component, User Interface,...)

vSphere là nền tảng ảo hóa của VMware, có vai trò quan trọng là tạo và quản lý máy ảo trên hạ tầng vật lý. Phần này giúp hiểu rõ hơn về vSphere và các thành phần liên quan như vCenter, Physical Infrastructure, Virtual Infrastructure và Virtual Machines (VMs). "vSphere"

I. Tổng quan về vSphere và các khái niệm cơ bản

Khái niệm: vSphere là nền tảng ảo hóa của VMware, dùng để tạo và quản lý máy ảo trên hạ tầng vật lý,. Hiện tại vSphere có 2 phiên bản:

- Vsphere Standard Edition: Phiên bản cơ bản, phù hợp cho các doanh nghiệp với nhu cầu ảo hóa vừa phải.
- Vsphere Enterprise Plus Edition: Phiên bản đầy đủ tính năng, hỗ trợ ảo hóa toàn diện cho trung tâm dữ liệu và điện toán đám mây.

Vai trò: vSphere giúp ảo hóa tài nguyên phần cứng, tối ưu hóa và đơn giản hóa việc quản lý hệ thống.

Tính năng nổi bật: Có nhiều phiên bản với các tính năng như quản lý tài nguyên, bảo mật và tự động hóa.

Lưu ý:

- vSphere 8.0 yêu cầu một giấy phép CPU cho tối đa 32 lõi vật lý. Nếu CPU có nhiều hơn 32 lõi, thì cần có thêm giấy phép CPU
- Ngừng sử dụng N-Port ID Virtualization (NPIV)

- Không còn hỗ trợ Common Information Model (CIM) và Service Location Protocol (SLP)
- Ngừng hỗ trợ cho nền tảng Apple Mac: ESXi 8.0 không hỗ trợ nền tảng Apple MacPro và Apple MacMini và macOS là hệ điều hành khách.

1. vCenter Server

Khái niệm: vCenter Server cung cấp nền tảng tập trung để quản lý, vận hành, cung cấp tài nguyên và đánh giá hiệu suất của máy ảo và máy chủ.

Vai trò: Quản lý và giám sát các máy ảo và tài nguyên ảo hóa.

Chức năng chính: Quản lý hiệu suất, phân bổ tài nguyên, tự động hóa quản trị.

- Các thành phần sau đây được bao gồm trong quá trình triển khai thiết bị vCenter Server :
- Các dịch vụ xác thực bao gồm vCenter Single Sign-On, dịch vụ cấp phép, dịch vụ tra cứu và VMware Certificate Authority.
- Nhóm dịch vụ vCenter Server bao gồm vCenter Server , vSphere Client , vSphere Auto Deploy và vSphere ESXi Dump Collector. Thiết bị vCenter Server cũng bao gồm dịch vụ VMware vSphere Lifecycle Manager Extension và VMware vCenter Lifecycle Manager.

Dịch vụ được cài đặt với vCenter Server:

- PostgreSQL: Phiên bản cơ sở dữ liệu đi kèm cho vSphere và các dịch vụ đám mây.
- vSphere Client: Giao diện HTML5 để quản lý vCenter Server qua trình duyệt.
- vSphere ESXi Dump Collector: Công cụ hỗ trợ thu thập dump của ESXi khi gặp lỗi nghiêm trọng.

- vSphere Auto Deploy: Công cụ triển khai ESXi cho nhiều máy chủ vật lý.
- VMware vSphere Lifecycle Manager: Quản lý cập nhật và phiên bản cho ESXi, máy ảo, và các ứng dụng ảo hóa.

2. Physical Infrastructure

Khái niệm: Là lớp hạ tầng vật lý bao gồm các máy chủ, hệ thống lưu trữ (như SAN, NAS, vSAN) và thiết bị mạng (như switch, router, firewall). Các thành phần này tương tác với nhau để tạo nên môi trường ảo hóa mạnh mẽ và linh hoạt.

Vai trò: Physical Infrastructure là nền tảng chính cho tất cả các tài nguyên ảo hóa trong vSphere. Các tài nguyên này được ảo hóa và phân bổ để phục vụ các ứng dụng và dịch vụ IT một cách hiệu quả, đảm bảo tính sẵn sàng cao và tối ưu hóa hiệu năng.

Quản lý: Đảm bảo tài nguyên phần cứng hoạt động tối ưu để hỗ trợ máy ảo.

- Server Hardware: Các máy chủ hiện đại với CPU nhiều lõi, bộ nhớ RAM lớn và lưu trữ nhanh chóng được sử dụng để hỗ trợ môi trường ảo hóa. Việc bảo trì định kỳ và kiểm tra tương thích phần cứng là yếu tố quan trọng để đảm bảo hiệu suất.
- Networking: Cấu hình mạng phức tạp nhưng linh hoạt, kết nối các máy chủ với nhau và với toàn bộ hệ thống qua các công nghệ như SDN (Software-Defined Networking) để tối ưu hóa hiệu năng và bảo mật.
- Storage: Hệ thống lưu trữ hiện đại như vSAN, hỗ trợ công nghệ NVMe và RAID, đảm bảo dữ liệu được truy cập nhanh chóng và an toàn. Việc quản lý lưu trữ bao gồm tối ưu hóa IOPS, độ trễ thấp và khả năng mở rộng linh hoạt.
- Tương thích phần cứng: Luôn đảm bảo phần cứng sử dụng tương thích với danh sách HCL (Hardware Compatibility List) của VMware để tránh các vấn đề hiệu suất và đảm bảo được hỗ trợ kỹ thuật từ VMware.

- Kiểm tra và bảo trì: Bảo trì định kỳ, bao gồm cập nhật firmware, kiểm tra hệ thống và dự phòng rủi ro, để đảm bảo phần cứng luôn hoạt động ổn định và sẵn sàng cho mọi tình huống.

3. Virtual Infrastructure

Khái niệm: Là lớp ảo hóa chạy trên hạ tầng vật lý. Virtual Infrastructure là lớp hạ tầng ảo hóa, bao gồm các máy ảo (VMs), mạng ảo (vSwitches), và các tài nguyên ảo hóa khác được quản lý bởi các phần mềm như VMware vSphere. Các tài nguyên phần cứng từ Physical Infrastructure được trừu tượng hóa để tạo ra môi trường ảo linh hoạt, có thể mở rộng và dễ dàng quản lý.

Mối liên hệ: Virtual Infrastructure được xây dựng từ các tài nguyên phần cứng. Cho phép tận dụng tối đa tài nguyên phần cứng, tạo ra nhiều máy ảo chạy các hệ điều hành và ứng dụng khác nhau trên cùng một máy chủ vật lý. Nó cung cấp khả năng linh hoạt cao trong quản lý tài nguyên và dễ dàng mở rộng hoặc thu hẹp quy mô hệ thống.

Lợi ích: Giúp quản lý linh hoạt, tiết kiệm chi phí, và dễ dàng mở rộng hệ thống.

Quản lý: Virtual Infrastructure quản lý các máy ảo (VMs) chạy trên tài nguyên phần cứng, cùng với mạng ảo và lưu trữ ảo hóa để tối ưu hóa hiệu năng, đảm bảo tính sẵn sàng cao và khả năng mở rộng linh hoạt. Nó tích hợp các công cụ như vSwitches để điều phối mạng, vSAN cho lưu trữ, và Resource Pools để phân bổ tài nguyên hiệu quả, tất cả đều giúp quản trị hệ thống dễ dàng và nhanh chóng

Kiến trúc:

- Host: Quản lý tài nguyên cho máy ảo và có thể kết hợp với các host khác để tạo thành một cụm.
- Hypervisor: Phần mềm cho phép một máy chủ vật lý chạy nhiều hệ điều hành ảo cùng lúc.

- Virtual machine: Máy tính ảo với hệ điều hành riêng, dễ dàng tạo và quản lý mà không cần phần cứng vật lý.
- User interface: Giao diện giúp quản trị viên quản lý hạ tầng ảo hóa qua kết nối trực tiếp hoặc trình duyệt web.

Các thành phần cơ sở hạ tầng ảo:

- Virtualized compute: Là khả năng ảo hóa tính toán, cho phép nhiều hệ điều hành và ứng dụng chạy trên cùng một máy chủ vật lý. Điều này giúp tối ưu hóa tài nguyên, làm cho các công nghệ như điện toán đám mây và container trở nên khả thi.
- Virtualized storage: Tạo ra một kho lưu trữ duy nhất từ nhiều thiết bị lưu trữ vật lý, giúp linh hoạt trong việc phân bổ tài nguyên cho các máy ảo. Các giải pháp lưu trữ phổ biến bao gồm SAN (Storage Area Network) và NAS (Network-Attached Storage).
- Virtualized networking and security: Ảo hóa các dịch vụ mạng, tách chúng khỏi phần cứng nền tảng, giúp quản lý tập trung dễ dàng hơn. Các tính năng bảo mật quan trọng bao gồm cô lập máy ảo và quản lý quyền truy cập.
- Management solution: Cung cấp một giao diện quản lý thân thiện để cấu hình, quản lý và tự động hóa cơ sở hạ tầng ảo hóa. Giúp di chuyển máy ảo giữa các máy chủ mà không bị gián đoạn, hỗ trợ tính sẵn sàng cao và quản lý khôi phục sau thảm họa.

4. Virtual Machines (VMs)

Khái niệm: Máy ảo là hệ thống giả lập chạy trên nền tảng ảo hóa. Mỗi máy ảo hoạt động như một hệ thống độc lập với hệ điều hành riêng, ngay cả khi chúng chạy trên cùng một phần cứng.

Vai trò: Đóng vai trò quan trọng trong việc triển khai và quản lý ứng dụng. Ngoài ra, máy ảo có thể thực hiện các tác vụ cụ thể được coi là quá rủi ro để thực hiện trong môi trường máy chủ, chẳng hạn như truy cập dữ liệu bị nhiễm vi-rút hoặc thử nghiệm hệ điều hành. Vì máy ảo được tách biệt khỏi phần còn lại của hệ thống, nên phần mềm bên trong máy ảo không thể can thiệp vào máy chủ.

Hai loại máy ảo chính là:

- Máy ảo tiến trình (Process Virtual Machine): Đây là loại máy ảo được thiết kế để chạy một tiến trình đơn lẻ như một ứng dụng trên máy chủ. Nó cung cấp một môi trường lập trình độc lập với nền tảng, giúp che giấu thông tin về phần cứng hoặc hệ điều hành nền tảng. Ví dụ điển hình là Máy ảo Java (JVM), cho phép chạy các ứng dụng Java trên bất kỳ hệ điều hành nào như thể chúng là ứng dụng gốc.
- Máy ảo hệ thống (System Virtual Machine): Đây là loại máy ảo được ảo hóa hoàn toàn để thay thế cho một máy vật lý. Nó cho phép chia sẻ tài nguyên vật lý của máy chủ giữa nhiều máy ảo, mỗi máy chạy một hệ điều hành riêng. Quá trình ảo hóa này dựa trên Trình quản lý ảo (Hypervisor), như VMware ESXi, có thể chạy trực tiếp trên phần cứng hoặc trên một hệ điều hành nền tảng.

Có 5 loại ảo hóa chính:

- Ảo hóa phần cứng (Hardware Virtualization): Đây là hình thức ảo hóa phổ biến nhất, nơi một máy chủ vật lý được chia thành nhiều máy ảo, mỗi máy có hệ điều hành riêng. Hypervisor là phần mềm chính giúp quản lý các máy ảo này.
- Ảo hóa phần mềm (Software Virtualization): Tập trung vào việc tạo ra môi trường phần mềm độc lập trong một hệ thống vật lý. Ví dụ, chạy nhiều ứng dụng độc lập trên cùng một máy mà không cần thay đổi hệ điều hành.

- Ảo hóa lưu trữ (Storage Virtualization): Hợp nhất nhiều thiết bị lưu trữ vật lý thành một không gian lưu trữ ảo, giúp tối ưu hóa việc quản lý và sử dụng dữ liệu.
- Ảo hóa mạng (Network Virtualization): Tạo ra các mạng ảo hoạt động độc lập với phần cứng mạng thực tế, giúp dễ dàng quản lý và phân phối tài nguyên mạng.
- Ảo hóa dữ liệu (Data Virtualization): Cho phép truy cập và quản lý dữ liệu từ nhiều nguồn mà không cần phải biết nơi dữ liệu thực sự lưu trữ, giúp việc tổng hợp và sử dụng dữ liệu trở nên linh hoạt hơn.

II. Kiến trúc và các thành phần của hệ thống

1. Kiến trúc của vSphere

- Thành phần cốt lõi: vSphere gồm có ESXi, vCenter, và vSphere Client. ESXi là hypervisor để chạy máy ảo, vCenter là công cụ quản lý và vSphere Client là giao diện để người dùng tương tác với hệ thống.
- Cấu trúc và liên kết: Các thành phần này kết hợp với nhau để tạo thành một hệ thống quản lý tập trung, nơi mọi máy ảo và tài nguyên được điều phối từ một nơi duy nhất.

2. Kiến trúc của Physical Infrastructure

- Thành phần phần cứng: Physical Infrastructure bao gồm CPU, RAM, Network và Storage. Đây là nền tảng vật lý hỗ trợ các máy ảo.
- Tích hợp và tối ưu hóa: Các tài nguyên này được tích hợp vào vSphere để đảm bảo hiệu suất cao nhất cho hệ thống ảo hóa, với khả năng quản lý và phân bổ linh hoạt.

3. Kiến trúc của Virtual Infrastructure

- Thành phần chính: Virtual Infrastructure được xây dựng từ các Datacenters, Clusters và Resource Pools. Datacenters là nơi chứa các tài nguyên ảo hóa,

Clusters nhóm các máy chủ lại để tăng khả năng sẵn sàng, còn Resource Pools giúp chia nhỏ tài nguyên để quản lý tốt hơn.

- Quản lý tài nguyên: Virtual Infrastructure cho phép điều phối tài nguyên dễ dàng, với các chính sách linh hoạt để tối ưu hóa hiệu năng.

4. Giao diện người dùng và công cụ quản lý

- vSphere Client và Web Client: Đây là hai giao diện chính để người dùng tương tác với hệ thống. vSphere Client cài trên máy tính, còn Web Client hoạt động qua trình duyệt web, cả hai đều dễ sử dụng và đầy đủ tính năng.
- Công cụ dòng lệnh và tự động hóa: vSphere cũng cung cấp các công cụ dòng lệnh để quản lý hệ thống hiệu quả hơn, đặc biệt là khi cần tự động hóa các tác vụ quản trị.

Chương II. Tìm hiểu các thành phần làm nên Vsphere

I. Giới Thiệu

Ở chương trước, chúng ta đã tìm hiểu về vSphere và các thành phần chính của nó, bao gồm ESXi, vCenter Server, vSphere Client, và vSphere Web Client. Trong chương này, chúng ta sẽ đi sâu vào tìm hiểu các thành phần tài nguyên làm nên vSphere, bao gồm CPU, RAM, Network, Storage, và GPU. Những thành phần này không chỉ quyết định hiệu suất của hạ tầng ảo hóa mà còn đóng vai trò quan trọng trong việc quản lý tài nguyên và tối ưu hóa chi phí.

II. CPU trong vSphere: Tầm Quan Trọng và Cách Quản Lý

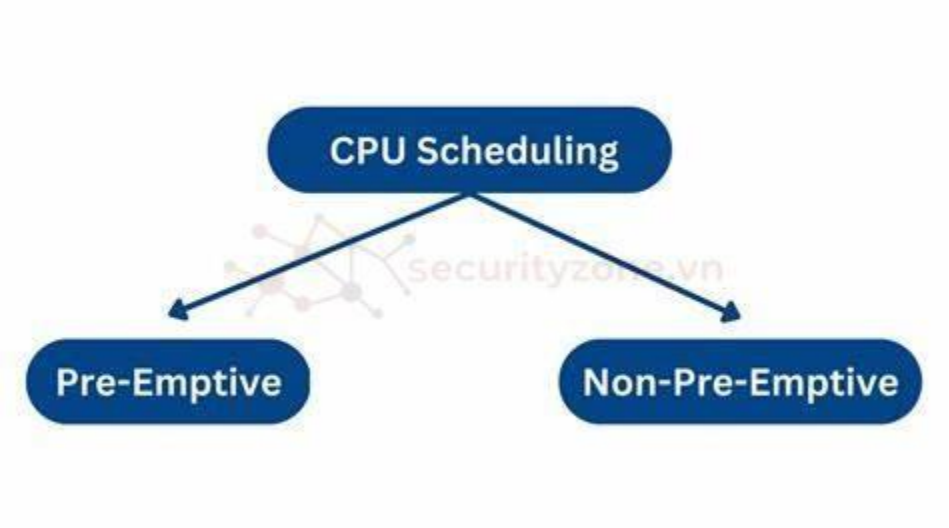
CPU (Central Processing Unit) là thành phần quan trọng trong mọi hệ thống, và trong môi trường vSphere, nó quyết định phần lớn đến hiệu suất của VM. Hiểu rõ cách thức hoạt động của CPU và các phương pháp quản lý nó sẽ giúp tối ưu hóa hiệu suất của hệ thống.

1. Tầm Quan Trọng của CPU

Trong vSphere, CPU xử lý tất cả các lệnh và thực hiện các tác vụ tính toán. Mỗi VM được gán một hoặc nhiều CPU ảo (vCPU) và có thể thực hiện các tác vụ tính toán tương tự như một máy tính vật lý. Để đảm bảo hiệu suất tối ưu, số lượng vCPU được phân bổ phải được cân nhắc cẩn thận dựa trên nhu cầu của ứng dụng và tài nguyên vật lý sẵn có.

2. Cơ Chế Hoạt Động của CPU trong vSphere

CPU Scheduling: vSphere sử dụng một cơ chế lập lịch tiên tiến để phân bổ thời gian CPU cho mỗi VM. Điều này giúp đảm bảo rằng tất cả các VM có cơ hội công bằng để sử dụng CPU, giảm thiểu độ trễ và tăng hiệu suất.



Hình 1 Cơ chế Preemptive and Non-Preemptive trong CPU Scheduling

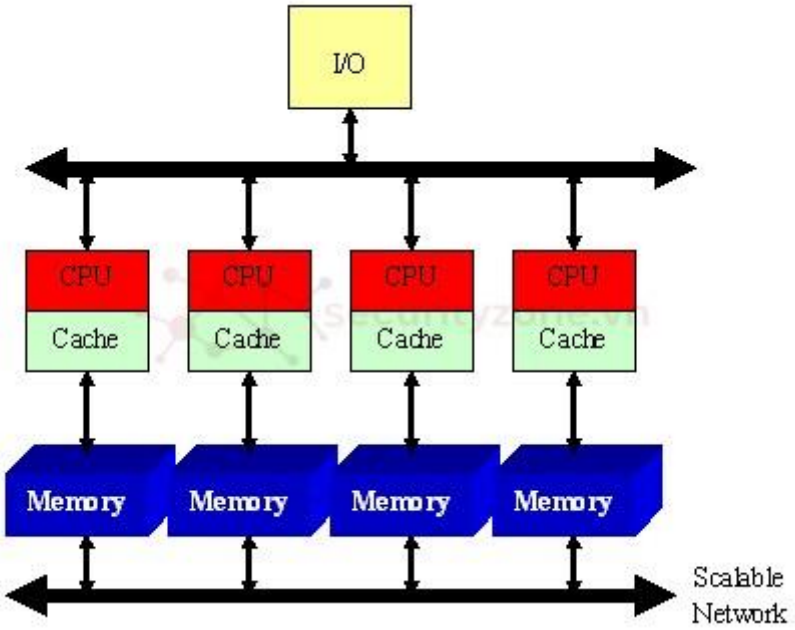
CPU Ready Time: Đây là một chỉ số quan trọng đo lường thời gian một VM phải chờ đợi để được CPU phục vụ. Thời gian này càng thấp, hiệu suất VM càng cao.

NUMA (Non-Uniform Memory Access): Trong các hệ thống với nhiều socket CPU, vSphere hỗ trợ NUMA để tối ưu hóa hiệu suất bộ nhớ và
CPU. NUMA cho phép một VM truy cập vào bộ nhớ gần nhất với CPU được gán, giảm độ trễ và tăng hiệu suất.

NUMA là một kiến trúc bộ nhớ trong đó thời gian truy cập bộ nhớ phụ thuộc vào vị trí tương đối của CPU và bộ nhớ. Thay vì tất cả các CPU truy cập vào một không gian bộ nhớ chung với tốc độ như nhau, trong kiến trúc NUMA, mỗi CPU có một "node cục bộ" - một vùng bộ nhớ được liên kết trực tiếp với CPU đó. Điều này có nghĩa là CPU có thể truy cập nhanh hơn vào bộ nhớ vật lý gần nhất so với bộ nhớ trên các node khác. Điều này giúp giảm độ trễ và tăng hiệu suất, đặc biệt là đối với các ứng dụng cần truy cập bộ nhớ liên tục và có khối lượng lớn. o Trong hệ thống NUMA, mỗi socket CPU đi kèm với một tập hợp các lõi (core) và một vùng bộ nhớ được liên kết trực tiếp. Khi một VM được gán vào một CPU trong một

node NUMA, hệ thống sẽ cố gắng đảm bảo rằng VM này sẽ truy cập vào bộ nhớ cục bộ của node đó.

Điều này giúp tối ưu hóa hiệu suất. Tuy nhiên, nếu bộ nhớ cục bộ không đủ, hệ thống sẽ phải truy cập bộ nhớ từ các node khác, gây tăng độ trễ và làm giảm hiệu suất tổng thể.



Hình 2 Cơ chế hoạt động của CPU trong ảo hóa vSphere

3. Phương Pháp Quản Lý CPU trong vSphere

- **CPU Affinity:** Cho phép quản trị viên gán một VM với các lõi CPU cụ thể. Điều này có thể tối ưu hóa hiệu suất cho các ứng dụng yêu cầu xử lý với độ trễ thấp.
- **Hot Add CPU:** Một tính năng cho phép thêm CPU vào một VM đang chạy mà không cần khởi động lại, giúp tăng tính linh hoạt trong quản lý tài nguyên.
- **Hyper-Threading:** Kỹ thuật này cho phép mỗi lõi CPU xử lý nhiều luồng đồng thời, tăng cường khả năng xử lý và cải thiện hiệu suất tổng thể của hệ thống.

III. RAM trong vSphere: Quản Lý Bộ Nhớ và Tối Ưu Hóa Hiệu Năng

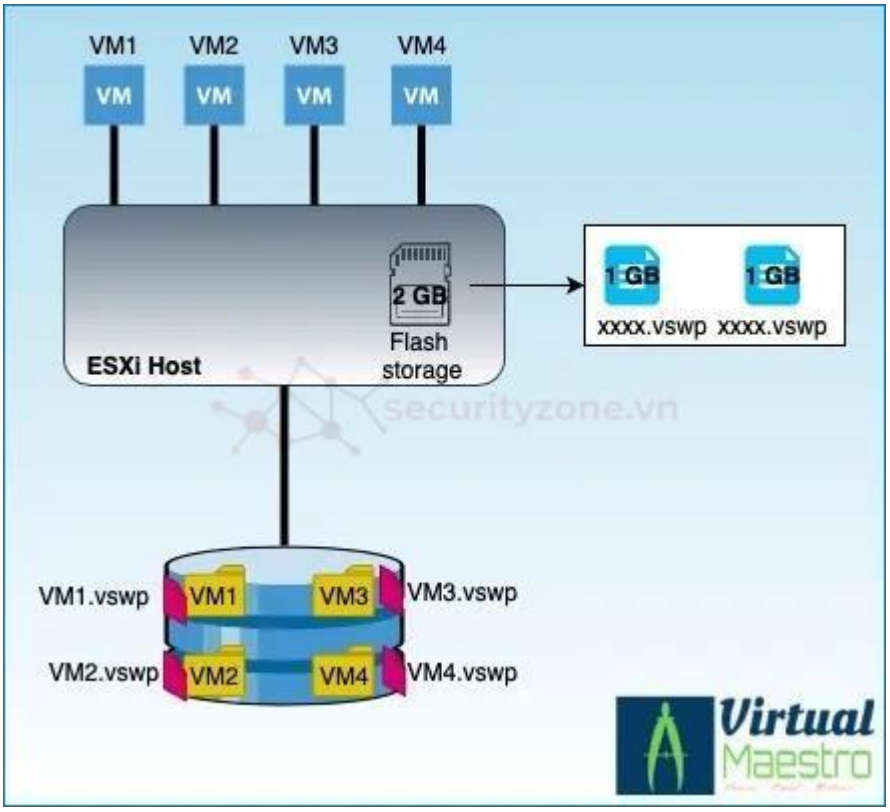
RAM (Random Access Memory) là một thành phần không thể thiếu, cung cấp bộ nhớ tạm thời cho các ứng dụng và dữ liệu đang được xử lý. Trong vSphere, quản lý bộ nhớ hiệu quả là điều cần thiết để đảm bảo rằng các VM hoạt động mượt mà và không gặp sự cố về bộ nhớ.

1. Tầm Quan Trọng của RAM

RAM đóng vai trò quyết định trong việc cung cấp bộ nhớ cho các VM và các ứng dụng chạy trên chúng. Việc quản lý bộ nhớ hiệu quả không chỉ giúp các VM chạy mượt mà, mà còn tránh tình trạng thiếu hụt bộ nhớ, gây ảnh hưởng đến toàn bộ hệ thống.

2. Cơ Chế Quản Lý Bộ Nhớ trong vSphere

- **Memory Overcommitment:** Cho phép phân bổ bộ nhớ ảo (vRAM) cho các VM nhiều hơn bộ nhớ vật lý có sẵn trên máy chủ. Điều này tận dụng khả năng rằng không phải tất cả các VM đều sử dụng hết bộ nhớ được cấp phát cùng một lúc.
- **Memory Ballooning:** Kỹ thuật này cho phép một VM "mượn" bộ nhớ không sử dụng từ các VM khác khi cần thiết, giúp tối ưu hóa việc sử dụng bộ nhớ trong toàn hệ thống.
- **Swapping:** Khi bộ nhớ vật lý bị cạn kiệt, vSphere sử dụng kỹ thuật swapping để chuyển dữ liệu từ RAM sang bộ nhớ lưu trữ trên đĩa cứng, mặc dù điều này có thể làm giảm hiệu suất do tốc độ truy cập dữ liệu trên đĩa cứng chậm hơn nhiều so với RAM.



Hình 3 Hình ảnh mô phỏng cơ chế quản lý bộ nhớ trong vSphere

3. Tính Năng Nâng Cao của RAM trong vSphere

- **Transparent Page Sharing (TPS):** Kỹ thuật này cho phép các VM chia sẻ các trang bộ nhớ giống nhau, giảm thiểu nhu cầu về bộ nhớ vật lý và tăng cường hiệu suất.

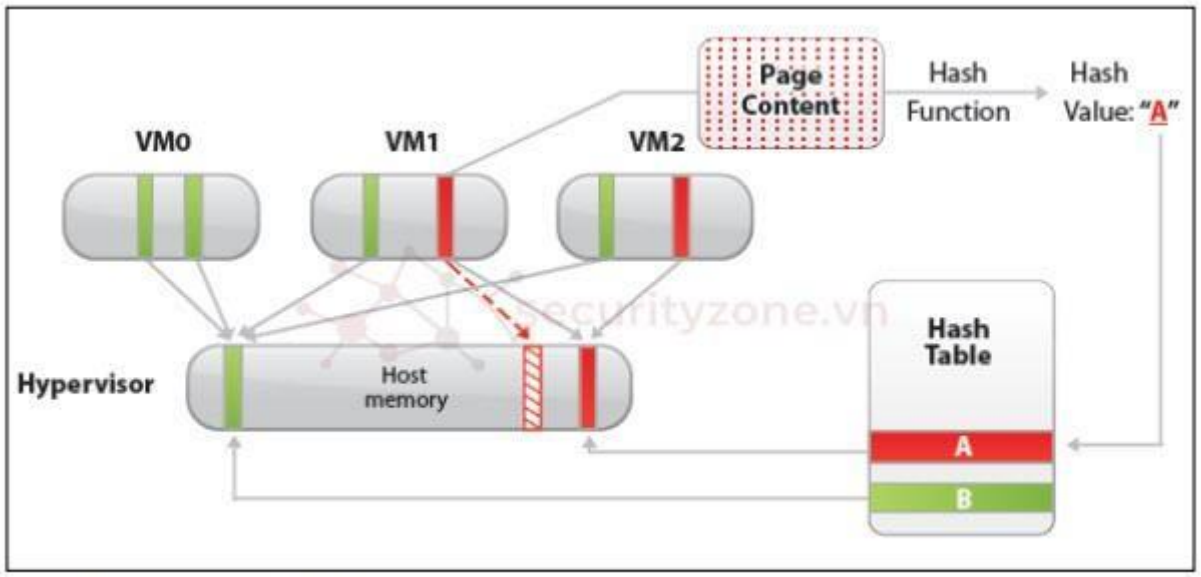
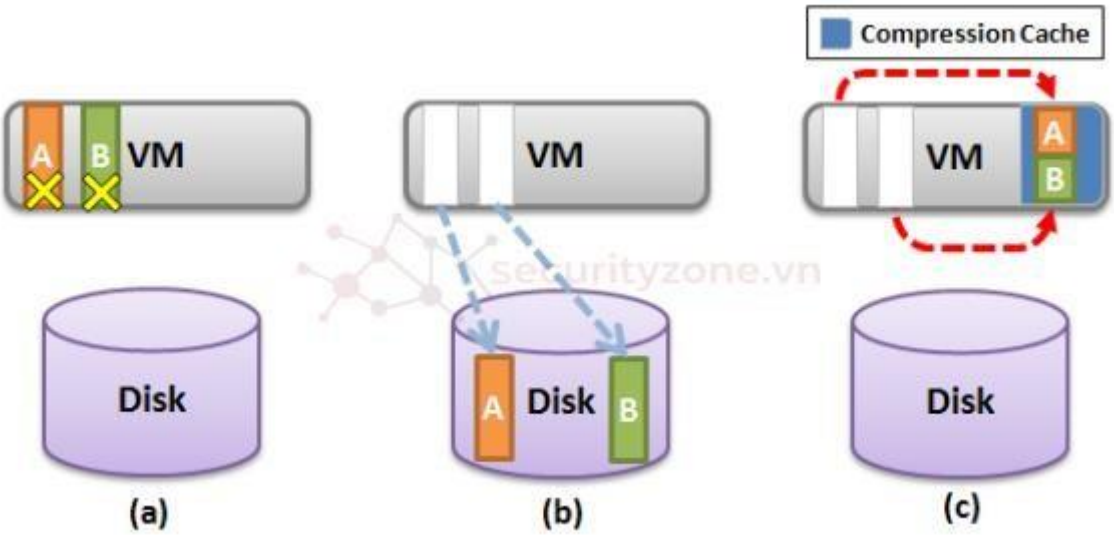


Figure 4. Content-Based Page Sharing in ESXi

Hình 4 Hình ảnh mô phỏng tính năng nâng cao của RAM

- **Memory Compression:** Khi bộ nhớ bị thiếu hụt, dữ liệu được nén lại trước khi chuyển sang ổ đĩa để tiết kiệm không gian lưu trữ và giảm thiểu tác động của swapping.



Hình 5 Hình ảnh mô phỏng tính năng nâng cao của RAM (tiếp theo)

- **Hot Add RAM:** Tính năng này cho phép thêm bộ nhớ vào một VM đang chạy mà không cần khởi động lại, giúp cải thiện hiệu quả hoạt động và linh hoạt trong quản lý tài nguyên.

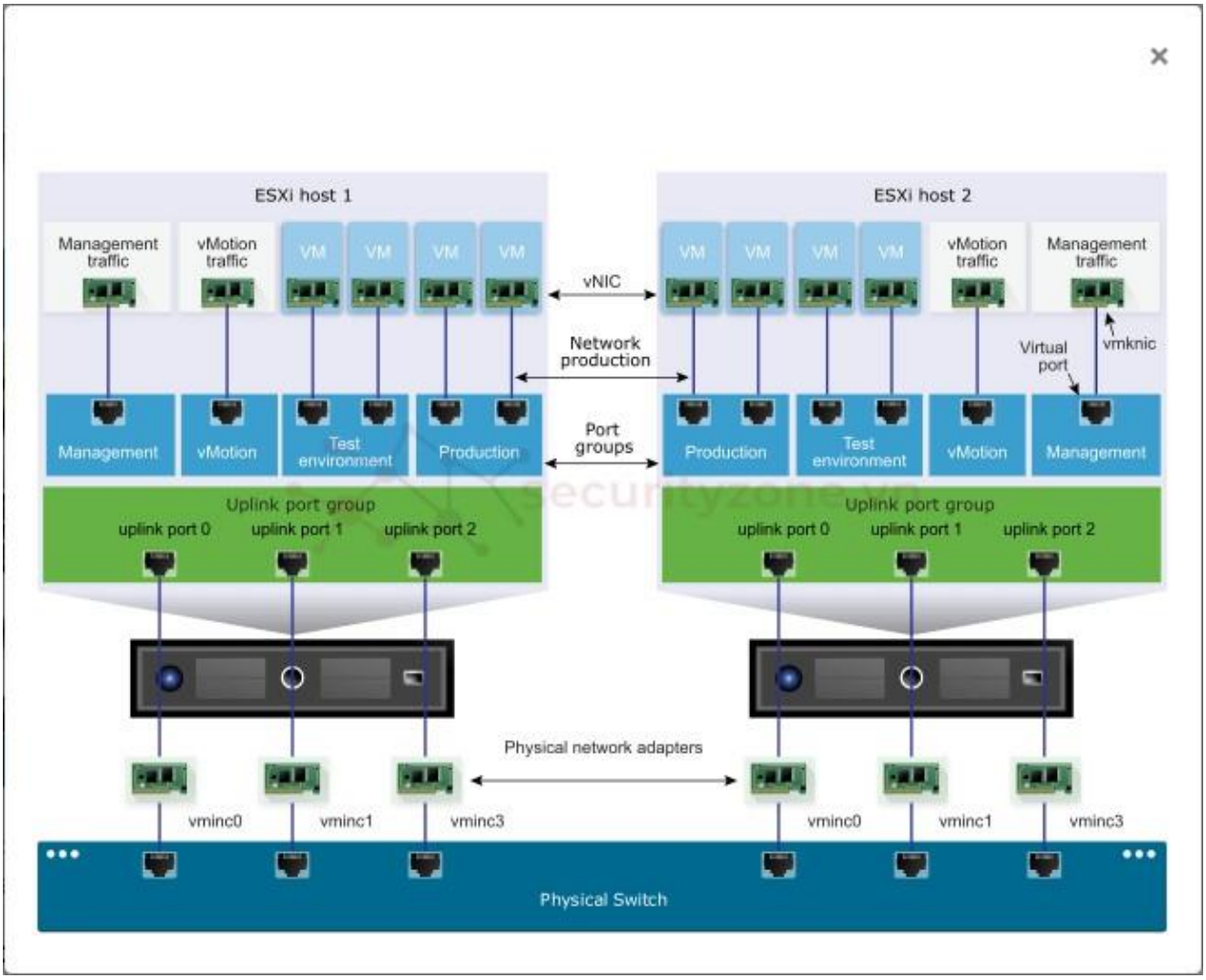
IV. Network trong vSphere: Kiến Trúc Mạng Ảo và Các Phương Pháp Quản Lý

Network (mạng) là một phần quan trọng trong môi trường vSphere, cung cấp khả năng kết nối giữa các VM và với các hệ thống bên ngoài. Quản lý mạng trong vSphere không chỉ liên quan đến việc cấu hình kết nối mà còn bao gồm việc đảm bảo an ninh và quản lý lưu lượng.

1. Kiến Trúc Mạng trong vSphere

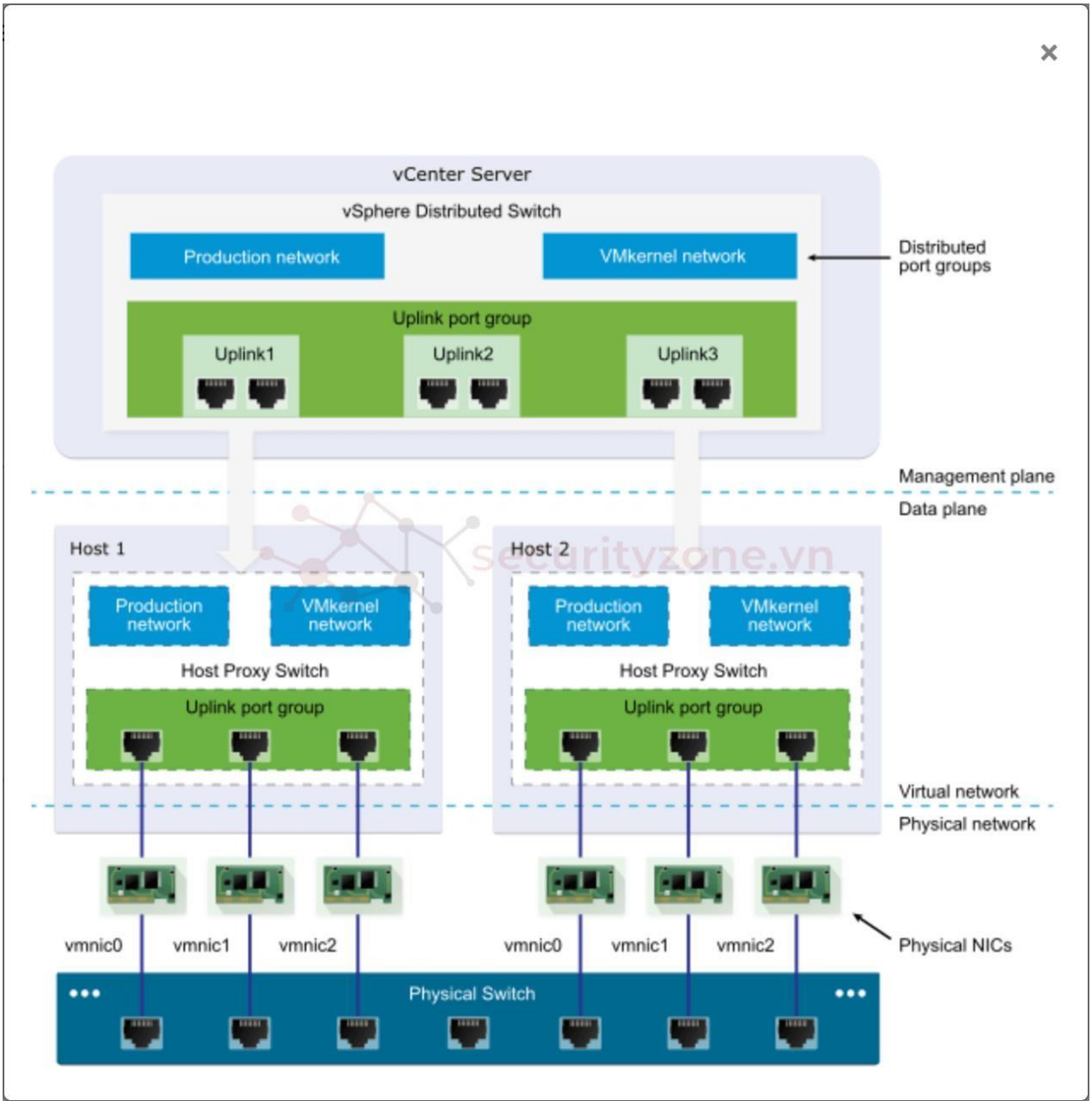
vSphere cung cấp hai loại switch ảo chính để quản lý mạng:

- **vSphere Standard Switch (vSS):** Đây là switch cơ bản cung cấp kết nối giữa các VM trên cùng một máy chủ vật lý và với mạng vật lý bên ngoài. vSS dễ dàng cấu hình và phù hợp cho các môi trường nhỏ.



Hình 6 Hình ảnh mô phỏng kiến trúc mạng trong vSphere

- **vSphere Distributed Switch (vDS):** Đây là switch nâng cao cung cấp quản lý tập trung và các tính năng nâng cao như QoS, bảo mật, và theo dõi lưu lượng. vDS được sử dụng trong các môi trường lớn và phức tạp.



Hình 7 Hình ảnh mô phỏng kiến trúc mạng trong vSphere(tiếp theo)

2. Quản Lý Mạng trong vSphere

- **Network I/O Control (NIOC):** Tính năng này cho phép quản lý băng thông mạng giữa các VM và các ứng dụng, đảm bảo rằng không có VM nào chiếm dụng quá nhiều tài nguyên mạng, gây ảnh hưởng đến hiệu suất của các VM khác.
- **Bảo Mật Mạng:**
    - **Port Group Security Policies:** Các chính sách này cho phép kiểm soát truy cập và bảo mật cho các VM, bao gồm chế độ promiscous, MAC address changes, và forged transmits.
    - **Virtual Private Networks (VPNs):** Hỗ trợ các kết nối mạng bảo mật giữa các môi trường ảo và các mạng bên ngoài.

3. Cấu Hình và Tối Ưu Hóa Mạng trong vSphere

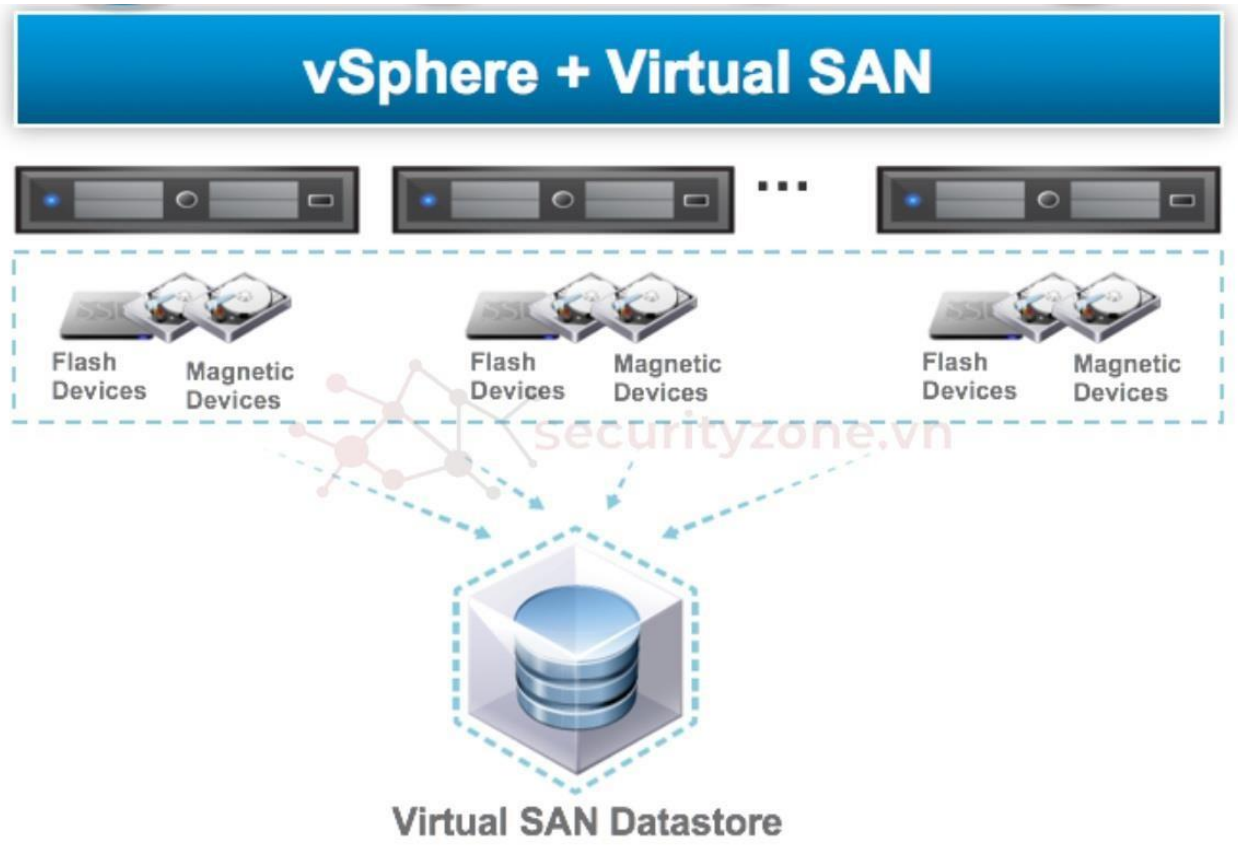
- **Load Balancing:** vSphere hỗ trợ nhiều phương pháp cân bằng tải để tối ưu hóa lưu lượng mạng, bao gồm IP Hash, Source MAC Hash, và LoadBased Teaming.
- **Jumbo Frames:** Sử dụng các gói dữ liệu lớn hơn để giảm tải mạng và cải thiện hiệu suất mạng cho các ứng dụng yêu cầu băng thông cao.
- **Traffic Shaping:** Cho phép kiểm soát lưu lượng mạng và đảm bảo rằng các ứng dụng quan trọng nhận được băng thông cần thiết.

V. Storage trong vSphere: Các Giải Pháp Lưu Trữ và Quản Lý Dữ Liệu

Storage (lưu trữ) trong vSphere là nền tảng cho việc lưu trữ dữ liệu VM và các ứng dụng, và cung cấp khả năng sao lưu, khôi phục, và bảo vệ dữ liệu. Với sự phát triển của công nghệ lưu trữ, vSphere hỗ trợ nhiều loại lưu trữ khác nhau, bao gồm SAN, NAS, và các giải pháp lưu trữ đám mây.

1. Các Loại Lưu Trữ trong vSphere

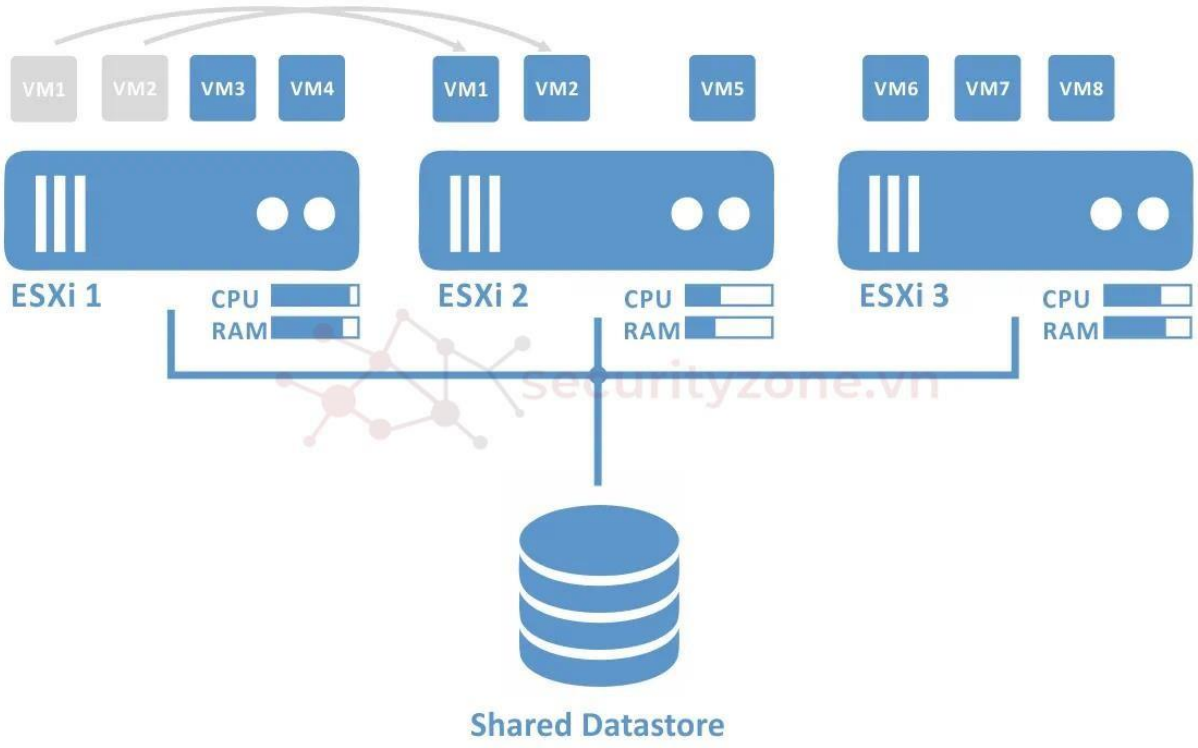
- **Local Storage:** Lưu trữ nội bộ trên máy chủ vật lý, thường được sử dụng cho các môi trường nhỏ hoặc để lưu trữ dữ liệu không quan trọng.
- **Shared Storage:** Bao gồm SAN (Storage Area Network) và NAS (Network Attached Storage), cho phép các máy chủ ESXi truy cập vào cùng một hệ thống lưu trữ, hỗ trợ các tính năng như vMotion và High Availability.
- **vSAN (Virtual SAN):** Một giải pháp lưu trữ phân tán tích hợp trong vSphere, sử dụng ổ cứng trên các máy chủ ESXi để tạo ra một lưu trữ chia sẻ ảo, tăng cường hiệu suất và độ tin cậy.



Hình 8 Hình ảnh mô phỏng ảo hóa lưu trữ vSAN

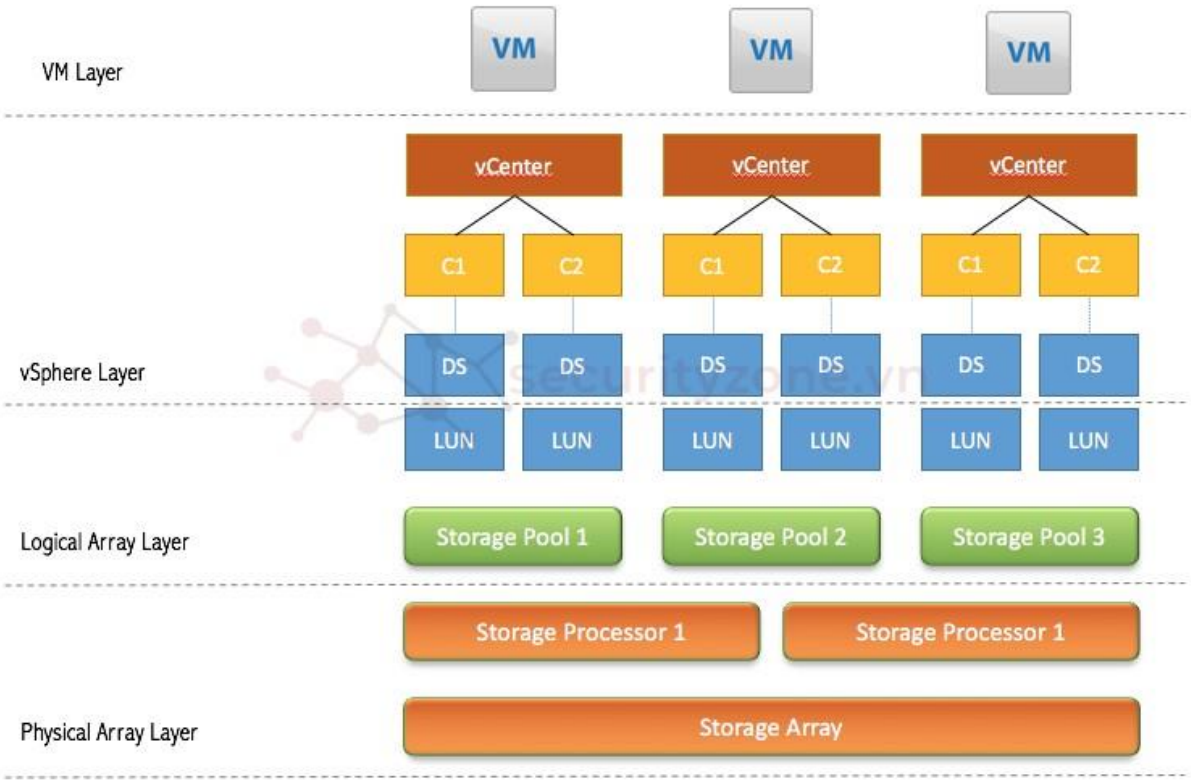
2. Quản Lý Lưu Trữ trong vSphere

- **Storage DRS (Distributed Resource Scheduler):** Tính năng này tự động quản lý và cân bằng tải lưu trữ giữa các datastore, đảm bảo rằng không có datastore nào bị quá tải.



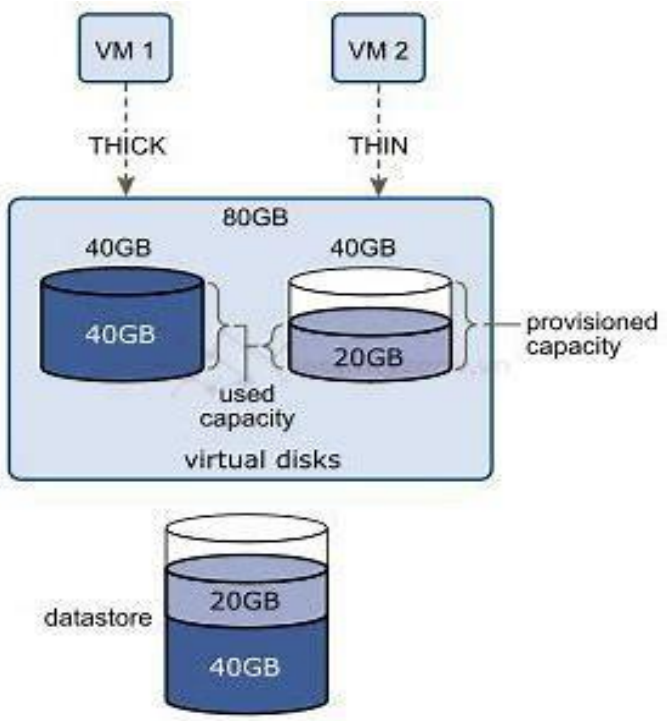
Hình 9 Hình ảnh mô phỏng quản lý lưu trữ giữa các ESXI Host

- **Storage I/O Control (SIOC):** Quản lý băng thông lưu trữ để ngăn chặn tình trạng nghẽn mạng lưu trữ và đảm bảo hiệu suất cho các ứng dụng quan trọng.



Hình 10 Hình ảnh giải thích cách ảo hóa lưu trữ trên vSphere

- **Thin Provisioning:** Kỹ thuật này cho phép VM sử dụng dung lượng lưu trữ nhỏ hơn dung lượng được phân bổ ban đầu, giúp tối ưu hóa việc sử dụng dung lượng lưu trữ.



Hình 11 Hình ảnh mô phỏng Thick và Thin Provisioning

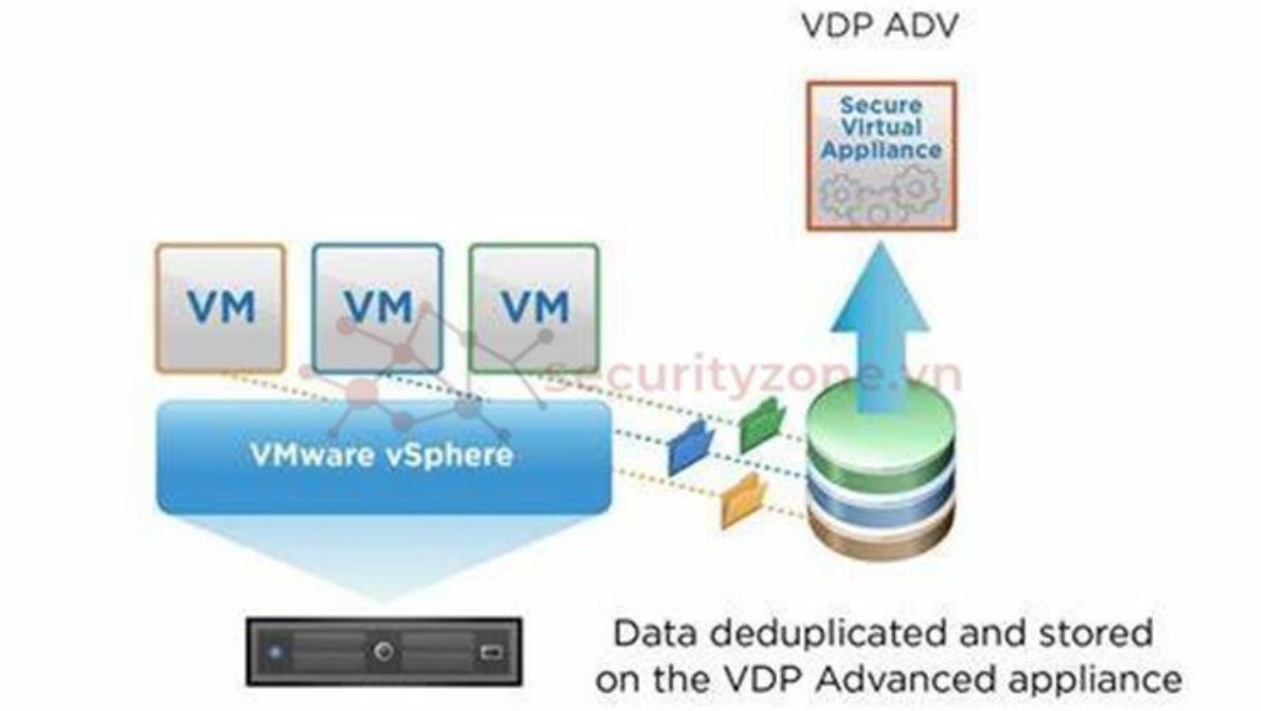
1. 3Cơ Chế Ghi/Đọc Dữ Liệu trong vSphere:

Trong hệ thống VMware, việc ghi/đọc dữ liệu chủ yếu dựa trên các giao thức lưu trữ như VMFS (Virtual Machine File System), NFS (Network File System) và iSCSI. Cơ chế này bao gồm các thành phần quan trọng như bộ nhớ đệm, hàng chờ I/O và đường truyền mạng. Các điểm dễ gây nghẽn, ảnh hưởng đến hiệu suất đọc/ghi dữ liệu bao gồm:

- **Băng thông của mạng lưu trữ:** Đường truyền mạng bị giới hạn có thể gây nghẽn khi dữ liệu cần truyền tải lớn, ảnh hưởng trực tiếp đến hiệu suất.
- **Cấu hình không đồng bộ giữa các thiết bị lưu trữ:** Nếu các thiết bị không được cấu hình đúng, việc truy cập có thể bị chậm trễ.
- **Số lượng IOPS (Input/Output Operations Per Second):** Nếu số lượng IOPS vượt quá khả năng của hệ thống, hiệu suất sẽ giảm.

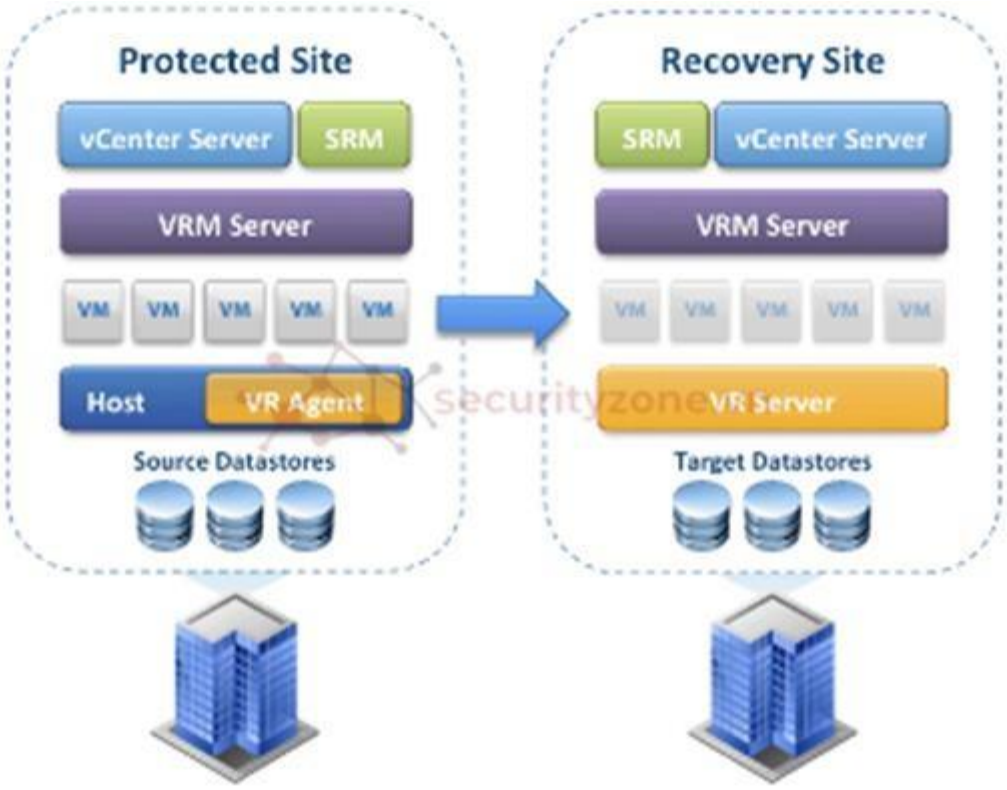
3. Sao Lưu và Khôi Phục Dữ Liệu trong vSphere

- **vSphere Data Protection (VDP):** Một giải pháp sao lưu và khôi phục dữ liệu tích hợp trong vSphere, hỗ trợ sao lưu cấp VM và các ứng dụng cụ thể.



Hình 12 Hình ảnh mô phỏng giải pháp bảo vệ dữ liệu của trung tâm dữ liệu

- **vSphere Replication:** Cung cấp khả năng sao chép dữ liệu từ một site sang site khác để đảm bảo an toàn dữ liệu và khôi phục sau thảm họa.



Hình 13 Hình ảnh mô phỏng giải pháp bảo vệ dữ liệu của trung tâm dữ liệu(tiếp theo)

VI. GPU trong vSphere: Sử Dụng trong Tính Toán Đồ Họa

GPU (Graphics Processing Unit) là một thành phần tài nguyên quan trọng trong các môi trường vSphere yêu cầu tính toán đồ họa cao hoặc xử lý dữ liệu lớn trong các ứng dụng AI và machine learning.

1. Tầm Quan Trọng của GPU

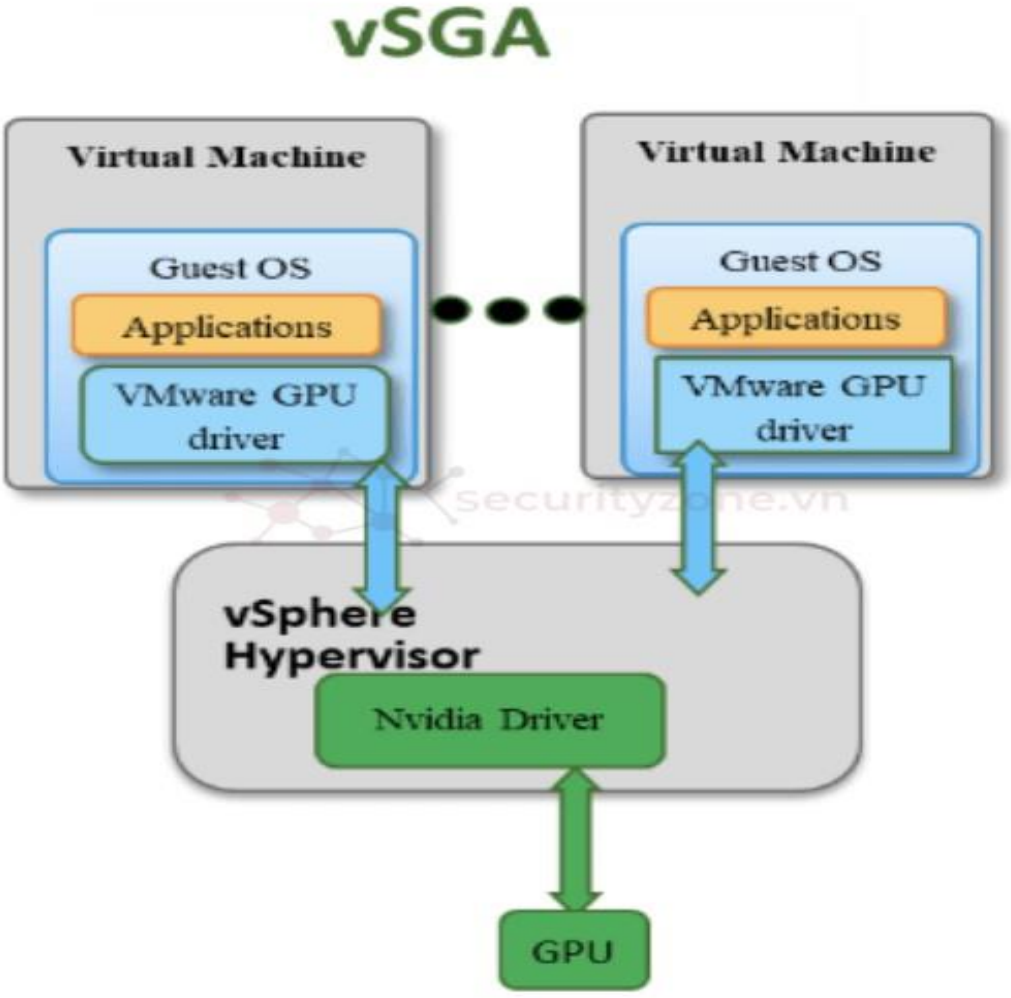
GPU cung cấp khả năng xử lý song song mạnh mẽ, giúp tăng tốc các tác vụ đồ họa và tính toán chuyên sâu. Trong vSphere, GPU có thể được chia sẻ giữa các VM hoặc được phân bổ độc quyền cho một VM cụ thể.

2. Cách Sử Dụng GPU trong vSphere

- **Virtual GPU (vGPU):** Công nghệ này cho phép nhiều VM chia sẻ cùng một GPU vật lý, tối ưu hóa việc sử dụng tài nguyên và giảm chi phí.
- **DirectPath I/O:** Cung cấp quyền truy cập trực tiếp của VM đến GPU vật lý, tối ưu hóa hiệu suất cho các ứng dụng yêu cầu đồ họa cao hoặc tính toán AI.

3. Các Tính Năng Nâng Cao của GPU trong vSphere

- **GPU Passthrough:** Cho phép một VM duy nhất sử dụng toàn bộ GPU vật lý, cung cấp hiệu suất tối đa cho các ứng dụng đồ họa hoặc tính toán nặng.
- **vSGA (Virtual Shared Graphics Acceleration):** Cung cấp khả năng tăng tốc đồ họa chia sẻ, cho phép nhiều VM sử dụng GPU cùng lúc mà không ảnh hưởng đến hiệu suất.



Hình 14 Hình ảnh mô phỏng GPU hoạt động trong vSphere Hypervisor

Chương III. Hướng dẫn cài đặt ESXI

I. Giới Thiệu Về ESXi

ESXi (VMware ESXi) là một phần mềm quản lý máy chủ, giúp quản lý và phân phối tài nguyên phần cứng của máy chủ cho các máy ảo (VM). Đây là một phần quan trọng của VMware vSphere, nền tảng ảo hóa hàng đầu của VMware.

Đặc điểm chính của ESXi:

- Kiến trúc nhỏ gọn: ESXi có kích thước rất nhỏ, chỉ chiếm một lượng nhỏ tài nguyên phần cứng, giúp tăng bảo mật và giảm nguy cơ bị tấn công.
- Bảo mật: ESXi cung cấp các tính năng bảo mật mạnh mẽ, bao gồm tự bảo vệ và quản lý chính sách bảo mật nghiêm ngặt.
- Quản lý tập trung: ESXi quản lý tập trung tài nguyên phần cứng của máy chủ, giúp dễ dàng phân bổ và giám sát tài nguyên cho các máy ảo.
- Khả năng mở rộng: ESXi có thể hỗ trợ hàng nghìn máy ảo và nhiều máy chủ vật lý, phù hợp với các môi trường từ nhỏ đến lớn.

II. Yêu Cầu Cài Đặt ESXi 7.0

1. Yêu Cầu Phần Cứng

- CPU: Máy chủ cần ít nhất hai lõi CPU và hỗ trợ bộ xử lý 64-bit x86 với tính năng ảo hóa (Intel VT-x hoặc AMD-V). Tính năng NX/XD cần được bật trong BIOS của CPU.
- RAM: ESXi 7.0 yêu cầu ít nhất 8 GB RAM vật lý và cần có ít nhất 8 GB RAM để chạy máy ảo trong môi trường sản xuất thông thường.

- Hỗ trợ ảo hóa phần cứng: Để hỗ trợ các máy ảo 64-bit, tính năng ảo hóa phần cứng (Intel VT-x hoặc AMD RVI) phải được bật.
- Bộ điều khiển Ethernet: Cần có một hoặc nhiều bộ điều khiển Ethernet Gigabit hoặc nhanh hơn.

2. Yêu cầu đĩa khởi động:

- Dung lượng: ESXi 7.0 yêu cầu đĩa khởi động có dung lượng ít nhất 32 GB. Điều này có thể là HDD, SSD, hoặc NVMe.
- Thiết bị boot: Chỉ sử dụng các thiết bị USB, SD, và phương tiện flash không phải USB cho phân vùng khởi động ESXi. Không được chia sẻ thiết bị khởi động giữa các máy chủ ESXi.
- Đĩa SCSI hoặc RAID: Cần có các đĩa SCSI hoặc RAID LUN cục bộ, không phải mạng, có không gian chưa phân vùng để lưu trữ máy ảo.
- Đĩa SATA: Nếu sử dụng Serial ATA (SATA), đĩa phải được kết nối thông qua bộ điều khiển SAS hoặc bộ điều khiển SATA tích hợp. Đĩa SATA được coi là từ xa, không phải cục bộ, và thường không được sử dụng làm phân vùng tạm thời vì tính chất "từ xa" của nó.

2. Yêu Cầu Lưu Trữ

- Dung lượng lưu trữ: Để có hiệu suất tốt nhất, sử dụng thiết bị lưu trữ liên tục có dung lượng tối thiểu là 32 GB. Đĩa cục bộ 128 GB hoặc lớn hơn sẽ hỗ trợ tối ưu cho ESXOSData.
- Thiết bị flash: Thiết bị flash phải có tối thiểu 128 terabyte được ghi (TBW) và cung cấp tốc độ ghi tuần tự ít nhất là 100 MB/giây.

- RAID: Nên sử dụng thiết bị sao chép RAID 1 để đảm bảo khả năng phục hồi trong trường hợp thiết bị bị lỗi.
- Hạn chế với thiết bị SD và USB: Thiết bị SD và USB chỉ được hỗ trợ cho phân vùng khởi động và không nên sử dụng để lưu trữ phân vùng ESX-OSData.

3. Yêu Cầu Khởi Động

- Khởi động UEFI: vSphere 7.0 hỗ trợ khởi động từ Giao diện chương trình cơ sở mở rộng hợp nhất (UEFI) và hỗ trợ khởi động mạng với vSphere Auto Deploy.
- Khởi động từ đĩa lớn hơn 2 TB: ESXi có thể khởi động từ đĩa lớn hơn 2 TB nếu chương trình cơ sở hỗ trợ.

III. Chuẩn Bị

1. Chuẩn Bị Trước Khi Cài Đặt

- Sao lưu dữ liệu: Sao lưu tất cả dữ liệu quan trọng trước khi cài đặt ESXi.
- Tài liệu cài đặt: Tải và đọc kỹ hướng dẫn cài đặt từ trang chủ VMware hoặc tài liệu đi kèm.
- Bootable Media: Chuẩn bị USB boot hoặc CD/DVD boot chứa bộ cài đặt ESXi.
- Thông tin mạng: Chuẩn bị các thông tin mạng như địa chỉ IP tĩnh, subnet mask, gateway, và DNS nếu cần cấu hình thủ công.

2. Quá Trình Nâng Cấp Lên ESXi 7.0

Phân vùng lại thiết bị khởi động: Quá trình nâng cấp sẽ phân vùng lại thiết bị khởi động và hợp nhất các phân vùng core dump, locker, và scratch vào ổ đĩa ESX-OSData.

Di chuyển các phân vùng: Phân vùng core dump và tệp nhật ký sẽ được di chuyển sang ESX-OSData, và phân vùng locker sẽ bị xóa.

Quản lý phân vùng sau nâng cấp: Nếu sử dụng thiết bị USB hoặc SD để nâng cấp, trình cài đặt sẽ cố gắng phân bổ ESX-OSData trên đĩa cục bộ. Nếu không có dung lượng trống, /scratch sẽ được đặt trên đĩa RAM.

3. Cấu Hình Sau Nâng Cấp

Cấu hình lại /scratch: Sau khi nâng cấp, cần cấu hình lại /scratch để sử dụng kho dữ liệu cố định hoặc thêm đĩa mới cho các ổ đĩa lưu trữ hệ thống.

Thêm đĩa cục bộ mới: Có thể thêm một đĩa cục bộ mới và bật tùy chọn autoPartition=TRUE để đĩa khởi động được phân vùng lại.

4. Chuẩn Bị Cho Môi Trường Auto Deploy và SAN

Cấu hình phân vùng /scratch: Trong môi trường Auto Deploy, phân vùng /scratch sẽ được đặt trên đĩa RAM nếu không tìm thấy đĩa cục bộ hoặc kho dữ liệu khả dụng.

Khởi động từ SAN: Mỗi máy chủ ESXi cần thiết lập ổ đĩa ESX-OSData trên một SAN LUN riêng. Tuy nhiên, có thể đồng định vị các vùng scratch cho nhiều máy chủ ESXi trên một LUN duy nhất, tùy theo số lượng máy chủ và kích thước LUN.

Chương IV. Hướng dẫn cài đặt vCenter và deploy vCenter Server

I. Giới Thiệu Về vCenter

vCenter là một thành phần chính trong bộ VMware vSphere, cung cấp một nền tảng quản lý tập trung cho toàn bộ hạ tầng ảo hóa, bao gồm các ESXi hosts và các máy ảo chạy trên chúng. Với vCenter, người quản trị có thể dễ dàng quản lý, giám sát và tự động hóa các hoạt động quản lý máy ảo và tài nguyên.

1. Đặc điểm chính của vCenter:

Quản lý tập trung: vCenter cho phép quản lý tất cả các ESXi hosts và máy ảo từ một giao diện duy nhất.

Tích hợp với các công cụ VMware: vCenter hoạt động liền mạch với các công cụ VMware khác như vSphere, vSAN, và NSX, mang lại giải pháp toàn diện cho ảo hóa.

Khả năng mở rộng: vCenter có thể quản lý hàng ngàn máy ảo và nhiều ESXi hosts, phù hợp cho cả các tổ chức lớn và nhỏ.

Bảo mật: vCenter cung cấp các tính năng bảo mật mạnh mẽ như phân quyền chi tiết, mã hóa dữ liệu và tích hợp với hệ thống quản lý nhận dạng.

2. Lợi ích khi sử dụng VMware vCenter Server trong hạ tầng vSphere

- **Triển khai dễ dàng:** VMware vCenter Server có thể dễ dàng triển khai qua vSphere Server Appliance (VCSA), giúp bạn nhanh chóng thiết lập và quản lý môi trường vSphere.
- **Quản lý và tối ưu hóa hiệu quả:** vCenter Server hỗ trợ hợp lý hóa quản lý tài nguyên và tối ưu hóa hiệu suất nhờ tích hợp với các công cụ như vSphere HA và DRS, đảm bảo tính khả dụng và tối ưu tài nguyên.

- **Mở rộng sang đám mây:** vCenter Server cho phép bạn mở rộng môi trường vSphere từ tại chỗ sang đám mây công cộng, như VMware Cloud trên AWS, mang lại sự linh hoạt và khả năng mở rộng cao.
- **Quản lý phân quyền:** Với vCenter Server, bạn có thể quản lý tập trung và phân quyền chi tiết cho các quản trị viên trong môi trường vSphere, đảm bảo an ninh và quản lý hiệu quả.
- **Tính sẵn sàng cao và bảo vệ dữ liệu:** VCSA hỗ trợ cấu hình ghép nối ActivePassive để dự phòng, giúp vCenter Server dự phòng sẵn sàng tiếp quản khi cần thiết. Ngoài ra, VCSA tích hợp sẵn giải pháp sao lưu dữ liệu, bảo vệ thông tin quan trọng.
- **Tích hợp bên thứ ba:** vCenter Server là nền tảng mạnh mẽ, được nhiều nhà cung cấp phần cứng tích hợp plugin để quản lý phần cứng ngay từ vSphere Client, như quản lý thiết bị lưu trữ. 3. Tại sao nên sử dụng vCenter Server?

Mặc dù VMware ESXi có thể hoạt động độc lập, nhưng với môi trường doanh nghiệp, vCenter Server là thành phần không thể thiếu. Nó cung cấp các tính năng quan trọng như vMotion, High-Availability (HA), và Distributed Resource Scheduler (DRS), giúp quản lý và tối ưu hóa tài nguyên, cũng như đảm bảo tính sẵn sàng và khả năng dự phòng khi có sự cố xảy ra.

Trong môi trường sản xuất, vCenter Server cho phép tạo các cụm vSphere, giúp kết nối và tối ưu hóa tài nguyên giữa các máy chủ ESXi. Nếu một máy chủ gặp sự cố, VMware HA sẽ tự động khởi động lại các máy ảo trên máy chủ khác trong cụm, đảm bảo dịch vụ không bị gián đoạn. Bên cạnh đó, vCenter Server hỗ trợ vMotion, cho phép di chuyển máy ảo giữa các máy chủ mà không cần dừng hoạt động, giúp thực hiện bảo trì mà không ảnh hưởng đến người dùng.

II.Yêu Cầu Cài Đặt vCenter

Điều kiện để triển khai vCenter Server Appliance 8

Yêu cầu hệ thống đối với trình cài đặt GUI và CLI:

Hệ điều hành	*Phiên bản được hỗ trợ*	*Cấu hình phần cứng tối thiểu để có hiệu suất tối ưu*
Các cửa sổ	• Windows 10, 11 • Windows 2016 x64bit • Windows 2019 x64bit • Windows 2022 x64bit	RAM 4 GB, 2 CPU 4 nhân tốc độ 2,3 GHz, ổ cứng 32 GB, 1 NIC
Linux	• SUSE 15 • Ubuntu 18.04, 20.04, 21.10	RAM 4 GB, 1 CPU 2 nhân tốc độ 2,3 GHz, ổ cứng 16 GB, 1 NIC Ghi chú: Trình cài đặt CLI yêu cầu hệ điều hành 64-bit.
Mac	• macOS 10.15, 11, 12 • macOS Catalina, Big Sur, Monterey	RAM 8 GB, 1 CPU 4 nhân tốc độ 2,4 GHz, ổ cứng 150 GB, 1 NIC

Hình 15 Điều kiện để triển khai vCenter Server Appliance 8

1. Yêu Cầu Phần Cứng

- CPU: vCenter yêu cầu CPU 64-bit với ít nhất 2 lõi vật lý. Hỗ trợ ảo hóa phần cứng (Intel VT-x hoặc AMD-V) là bắt buộc. Tùy thuộc vào quy mô môi trường (từ 2 đến 24 vCPU).
- RAM: Cần ít nhất từ 14GB đến 58GB. cho việc cài đặt vCenter. Tùy thuộc vào số lượng máy ảo và ESXi hosts được quản lý, yêu cầu RAM có thể tăng lên.
- Bộ điều khiển Ethernet: Cần có ít nhất một bộ điều khiển Ethernet Gigabit hoặc nhanh hơn để đảm bảo kết nối mạng hiệu quả.
- Bộ nhớ: Đĩa lưu trữ cần ít nhất 250 GB dung lượng, đặc biệt nếu sử dụng cơ sở dữ liệu tích hợp.

2. Yêu Cầu Lưu Trữ

- Dung lượng lưu trữ: vCenter yêu cầu dung lượng lưu trữ đủ lớn để chứa cơ sở dữ liệu, nhật ký và các thành phần khác của hệ thống nên tùy thuộc vào quy mô môi trường, với mức yêu cầu từ 579GB đến 4643GB
- Hỗ trợ RAID: Khuyến nghị sử dụng RAID 1 hoặc RAID 5 để đảm bảo khả năng dự phòng và tính sẵn sàng cao cho hệ thống.
- Hệ thống tệp: vCenter hỗ trợ các hệ thống tệp như VMFS, NFS và vSAN cho việc lưu trữ dữ liệu máy ảo và nhật ký hệ thống.

3. Yêu Cầu Mạng Và Cổng

- Kết nối mạng: vCenter yêu cầu ít nhất một kết nối mạng Gigabit. Để quản lý và sao lưu dữ liệu hiệu quả, có thể cần nhiều kết nối mạng.
- Địa chỉ IP tĩnh: Địa chỉ IP tĩnh là bắt buộc cho vCenter để đảm bảo rằng các dịch vụ mạng luôn được cung cấp một cách ổn định.
- DNS: DNS là một thành phần quan trọng cho việc cấu hình và quản lý vCenter. Đảm bảo rằng vCenter có thể giải quyết tên miền của các ESXi hosts và dịch vụ mạng khác.

III. Chuẩn Bị

1. Chuẩn Bị Trước Khi Cài Đặt

- Tải về source ISO: Chuẩn bị file ISO cài đặt từ các link tải chính thức của VMware.
- Kiểm tra máy chủ ESXi: Đảm bảo máy chủ không ở chế độ khóa hoặc bảo trì và không thuộc cụm DRS hoàn toàn tự động.
- Chuẩn bị thông tin mạng: Bao gồm IP tĩnh, subnet mask, gateway, và DNS.

- Sao lưu dữ liệu: Trước khi cài đặt vCenter, hãy đảm bảo rằng bạn đã sao lưu tất cả các dữ liệu quan trọng.
- Tài liệu cài đặt: Đọc kỹ tài liệu cài đặt của VMware để hiểu rõ các bước cần thực hiện.
- Bootable Media: Chuẩn bị USB hoặc CD/DVD boot chứa bộ cài đặt vCenter.
- Thông tin mạng: Chuẩn bị các thông tin mạng như địa chỉ IP tĩnh, subnet mask, gateway, và DNS.
- Các cổng cần thiết: Đảm bảo các cổng như 902, 443, 8080 được mở cho giao tiếp giữa vCenter và các thành phần khác.

2. Cài Đặt và Cấu Hình Ban Đầu

Chọn cấu hình phù hợp: Trong quá trình cài đặt, chọn cấu hình phù hợp với môi trường của bạn (vCenter Server Appliance hoặc vCenter trên Windows).

Cấu hình cơ sở dữ liệu: Nếu sử dụng cơ sở dữ liệu bên ngoài, đảm bảo rằng cơ sở dữ liệu đã được cài đặt và cấu hình chính xác trước khi bắt đầu cài đặt vCenter.

3. Quy Trình Triển Khai vCenter

Giai đoạn 1: Triển khai vCenter Server mới (8 bước)

- Chọn ngôn ngữ cài đặt.
- Chấp nhận thỏa thuận cấp phép.
- Chọn loại triển khai (tiny, small, medium...).
- Cấu hình tên miền và thiết lập DNS.
- Cấu hình mạng.
- Chọn ổ đĩa lưu trữ.
- Cấu hình tài khoản quản trị.
- Triển khai và kiểm tra.

Giai đoạn 2: Setup vCenter Server (5 bước)

- Đăng nhập và kiểm tra cấu hình ban đầu.
- Cấu hình NTP và đồng bộ thời gian.
- Kết nối vCenter với Active Directory.
- Cấu hình và kiểm tra các chính sách bảo mật.
- Triển khai các tính năng như vMotion, DRS, HA.

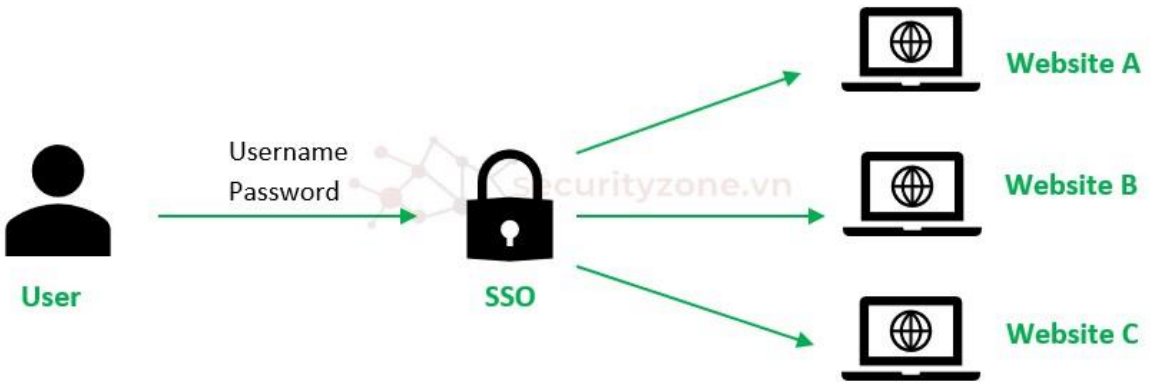
Chương V. Tìm hiểu về về Single Sign-On và vCenter Enhanced Linked Mode

Trong bối cảnh hiện đại, với sự gia tăng nhanh chóng của các ứng dụng và dịch vụ trực tuyến, việc quản lý thông tin đăng nhập trở thành một thách thức lớn đối với người dùng và quản trị viên hệ thống. Single Sign-On (SSO) và vCenter Enhanced Linked Mode (ELM) là hai giải pháp giúp đơn giản hóa quy trình đăng nhập và quản lý hạ tầng ảo hóa trong các doanh nghiệp. Nghiên cứu này sẽ phân tích chi tiết về SSO và ELM, cũng như đánh giá các ưu, nhược điểm của từng giải pháp.

I. Single Sign-On (SSO)

1. Tổng quan về Single Sign-On

Single Sign-On (SSO) là một cơ chế xác thực cho phép người dùng truy cập nhiều trang web hoặc ứng dụng chỉ với một lần đăng nhập duy nhất. Sau khi người dùng được xác thực tại một trang web hoặc ứng dụng cụ thể, họ có thể truy cập các trang web hoặc ứng dụng khác mà không cần phải nhập lại thông tin đăng nhập. Điều này giúp đơn giản hóa trải nghiệm người dùng và tăng cường bảo mật.



Hình 16 Hình ảnh mô phỏng cơ chế xác thực người dùng SSO

Các thành phần của SSO bao gồm:

- Identity Sources: Là nơi chứa thông tin user. Có các nguồn phổ biến như Active directory(AD), LDAP (Lightweight Directory Access Protocol và Local OS.
- SSO sever: Là nơi xử lý các request của user về xác thực và dịch vụ dựa trên thông tin được cung cấp bởi Identity Sources.
- Service providers: Các ứng dụng và dịch vụ yêu cầu xác thực như VCenter sever, vSphere web client và nhiều thành phần khác trong hệ sinh thái VMware

2. Ưu và Nhược điểm của SSO

Ưu điểm:

- Giảm thiểu số lượng username và password: Người dùng không cần phải ghi nhớ nhiều bộ thông tin đăng nhập cho nhiều ứng dụng khác nhau.
- Giảm số lần đăng nhập: Người dùng chỉ cần thực hiện thao tác đăng nhập một lần để truy cập nhiều dịch vụ khác nhau, tiết kiệm thời gian và tăng cường trải nghiệm.

- Tăng cường bảo mật: Việc giảm thiểu số lần người dùng phải nhập thông tin nhạy cảm giúp giảm nguy cơ lộ mật khẩu và thông tin cá nhân.

Nhược điểm:

- Chi phí phát triển cao: Việc triển khai SSO có thể tốn kém, đặc biệt khi tích hợp với các dịch vụ của bên thứ ba.
- Phụ thuộc vào dịch vụ bên ngoài: Nếu hệ thống SSO gặp sự cố, toàn bộ hệ thống ứng dụng liên kết cũng có thể bị ảnh hưởng, gây ra gián đoạn dịch vụ.

3. Cơ chế hoạt động của SSO

Hệ thống nhận dạng liên kết (Federated Identity System) là nền tảng của SSO, bao gồm 4 yếu tố chính:

- Xác thực (Authentication): Kiểm tra thông tin đăng nhập và xác định danh tính người dùng.
- Phân quyền (Authorization): Xác định quyền truy cập của người dùng dựa trên danh tính.
- Trao đổi thông tin người dùng (User attributes exchange): Chia sẻ thông tin người dùng giữa các hệ thống để tránh sự trùng lặp dữ liệu.
- Quản lý người dùng (User management): Quản trị viên có thể thực hiện các thao tác thêm, sửa, xóa thông tin người dùng trong các hệ thống liên kết.

Cách thức hoạt động: Khi người dùng đăng nhập vào một hệ thống (A), hệ thống này sẽ lưu thông tin xác thực vào cookie. Khi người dùng truy cập vào hệ thống khác (B), hệ thống B sẽ kiểm tra thông tin từ cookie đã được lưu để xác nhận danh tính mà không cần yêu cầu đăng nhập lại. Để chia sẻ thông tin này giữa các domain, một domain trung tâm (central domain) sẽ được sử dụng để chia sẻ thông tin cookie giữa các domain khác nhau.

Domain trung tâm này có thể tạo ra một JSON Web Token (JWT) và mã hóa nó. Khi người dùng truy cập vào các domain khác, họ sẽ được điều hướng đến domain trung tâm này, nhận lại token và tiếp tục sử dụng mà không cần đăng nhập lại.

Một ví dụ thực tế là khi một người dùng đăng nhập vào hệ thống A, thông tin đăng nhập được lưu trữ dưới dạng cookie tại domain của hệ thống A. Nếu người dùng sau đó truy cập hệ thống B, hệ thống này sẽ gửi yêu cầu đến domain trung tâm để xác thực người dùng thông qua token đã được tạo. Nhờ vậy, người dùng không cần phải nhập lại thông tin đăng nhập, mà vẫn được xác thực tự động.

4. Phân loại SSO

Single Sign-On (SSO) được triển khai qua nhiều giao thức và công nghệ khác nhau. Dưới đây là bốn loại SSO phổ biến:

SAML (Security Assertion Markup Language)

- Đặc điểm: SAML là một giao thức tiêu chuẩn dùng để trao đổi thông tin xác thực giữa các hệ thống, chủ yếu trong các ứng dụng web.
- Cách hoạt động: Người dùng đăng nhập một lần, sau đó có thể truy cập vào nhiều ứng dụng khác mà không cần phải đăng nhập lại.
- Ưu điểm: Khả năng tương thích cao, bảo mật mạnh mẽ.
- Nhược điểm: Phức tạp trong triển khai, có thể ảnh hưởng đến hiệu suất hệ thống.

OAuth (Open Authorization)

- Đặc điểm: OAuth cho phép các ứng dụng bên thứ ba truy cập vào tài nguyên của người dùng mà không cần chia sẻ mật khẩu của họ.
- Cách hoạt động: Sử dụng mã thông báo (token) để ủy quyền truy cập vào tài nguyên mà không cần biết mật khẩu.
- Ưu điểm: Bảo mật thông tin, linh hoạt trong sử dụng.

- Nhược điểm: Phức tạp trong quản lý mã thông báo, khó kiểm soát phạm vi quyền hạn.

OIDC (OpenID Connect)

- Đặc điểm: OIDC dựa trên OAuth 2.0, bổ sung thêm khả năng xác thực người dùng và quản lý danh tính.
- Cách hoạt động: Sử dụng mã thông báo (ID Token) để xác thực và quản lý thông tin người dùng.
- Ưu điểm: Kết hợp cả xác thực và ủy quyền, hỗ trợ rộng rãi bởi nhiều nhà cung cấp.
- Nhược điểm: Yêu cầu sự tương thích với OAuth 2.0 và các hệ thống hiện có.

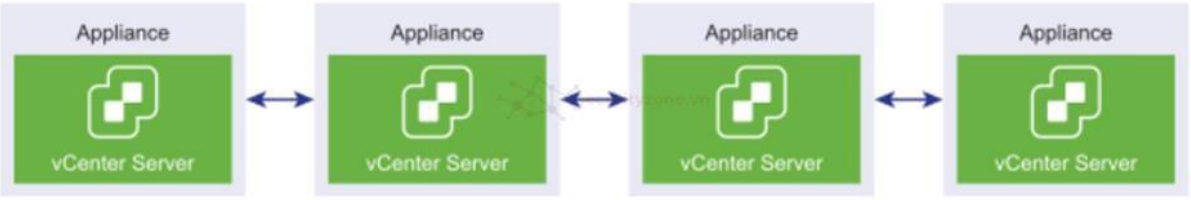
Kerberos

- Đặc điểm: Kerberos là một giao thức xác thực mạng phổ biến trong các môi trường doanh nghiệp.
- Cách hoạt động: Sử dụng các vé phiên (tickets) để xác thực và ủy quyền truy cập vào các dịch vụ mạng.
- Ưu điểm: Bảo mật mạnh mẽ, hiệu quả trong việc truy cập nhiều dịch vụ mà không cần đăng nhập lại.
- Nhược điểm: Phụ thuộc vào thời gian đồng bộ, triển khai phức tạp.

II. vCenter Enhanced Linked Mode (ELM)

1. Tổng quan về vCenter Enhanced Linked Mode

vCenter Enhanced Linked Mode (ELM) là một tính năng nâng cao của VMware vSphere, cho phép kết nối nhiều vCenter Server lại với nhau để cung cấp một giao diện quản lý duy nhất. Tính năng này giúp các quản trị viên dễ dàng quản lý và theo dõi các môi trường ảo hóa khác nhau từ một giao diện, mà không cần phải truy cập vào từng vCenter Server riêng lẻ.

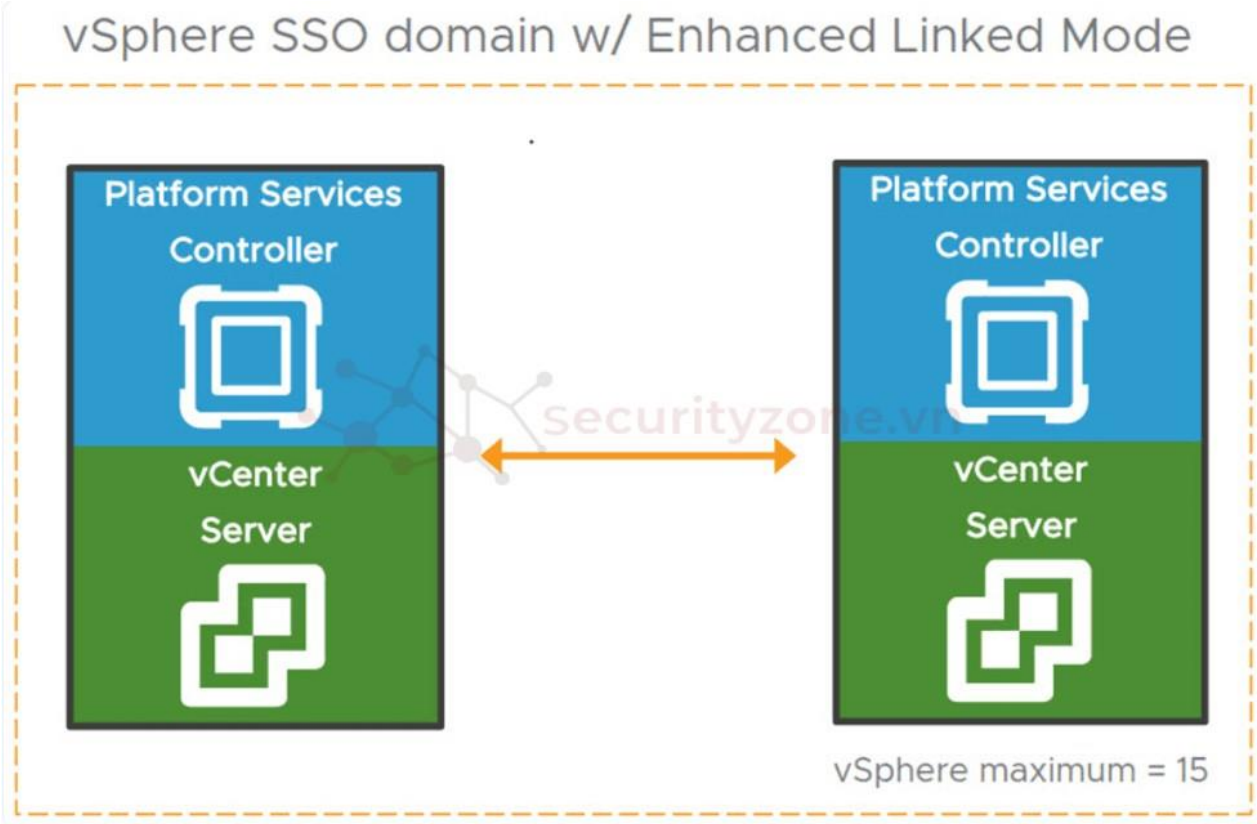


Hình 17 Hình ảnh mô phỏng cơ chế vCenter Enhanced Linked Mode

Cách thức hoạt động của ELM (Enhanced Link Mode)

ELM cung cấp một "giao diện duy nhất" (single pane of glass) cho nhiều vCenter Servers trong cùng một domain SSO vSphere. Tính năng này cho phép các kỹ sư hạ tầng ảo hóa dễ dàng quản lý các môi trường ảo khác nhau như môi trường máy tính ảo và máy chủ ảo trên nhiều site.

ELM chỉ được hỗ trợ trên vSphere Web Client. Khi ELM được kích hoạt, tất cả các vCenter Servers trong cùng một domain SSO sẽ được liên kết trong ELM và có thể truy cập từ một giao diện web duy nhất.



Hình 18 Sơ đồ mô tả cấu trúc của miền SSO trong vSphere với Enhanced Linked Mode

- Platform Services Controller: Cung cấp các dịch vụ như xác thực và quản lý người dùng.
- vCenter Server: Quản lý các máy ảo và tài nguyên trong môi trường ảo hóa.
- Enhanced Linked Mode: Cho phép quản lý nhiều vCenter Server từ một giao diện duy nhất, giúp dễ dàng hơn trong việc quản lý và giám sát.

Lợi ích của ELM với Embedded Platform Services Controller (PSC)

- Quy trình backup và khôi phục đơn giản: Không cần một thiết bị backup riêng biệt, giúp tiết kiệm tài nguyên và đơn giản hóa quy trình bảo trì.
- Kiến trúc domain đơn giản: ELM giúp quản lý nhiều site mà không cần phải sử dụng PSC ngoài, giảm thiểu sự phức tạp trong cấu trúc hệ thống.
- Khả năng mở rộng: vSphere 6.7 hỗ trợ tối đa 15 nodes với vCenter Server trong ELM, giúp hệ thống có thể dễ dàng mở rộng mà không cần thay đổi cấu trúc cơ bản.
- Đơn giản hóa quy trình High Availability (HA): Quản lý đến 15 vCenter Server Appliances trong Embedded Linked Mode mà không cần sử dụng load balancer, giúp tối ưu hóa quy trình HA.

Tính năng nâng cao của vCenter Enhanced Linked Mode với vCenter Server Appliance (VCSA)

- Khả năng liên kết tối đa: Bạn có thể liên kết tối đa 15 thiết bị vCenter Server với nhau bằng chế độ liên kết nâng cao, và tất cả đều được hiển thị trong một chế độ xem kho duy nhất. Điều này giúp quản trị viên có thể dễ dàng quản lý và điều phối các tài nguyên trên toàn bộ hạ tầng ảo hóa.
- Hỗ trợ sao lưu và khôi phục đơn giản: Quy trình sao lưu và khôi phục được đơn giản hóa đáng kể, đảm bảo rằng dữ liệu và cấu hình của hệ thống luôn được bảo vệ.
- Chế độ High Availability (HA) được tối ưu hóa: Trong cụm vCenter HA, ba nút được coi là một nút vCenter Server logic, giúp việc quản lý và vận hành trở nên dễ dàng hơn, đặc biệt là trong trường hợp có sự cố.
- Chế độ chỉ đọc cho các bản sao: Nếu một phiên bản vCenter High Availability (vCenter HA) được kết nối với một phiên bản vCenter Server khác có chế độ liên

kết nâng cao và vCenter HA chuyển đổi dự phòng sang nút thụ động và không thể giao tiếp với đối tác sao chép của mình trên nút vCenter Server khác, bản sao trên nút vCenter HA sẽ chuyển sang chế độ chỉ đọc, đảm bảo tính nhất quán dữ liệu trong trường hợp lỗi.

III. Kết luận

Single Sign-On (SSO) và vCenter Enhanced Linked Mode (ELM) là hai giải pháp công nghệ tiên tiến giúp đơn giản hóa quản lý hệ thống và cải thiện trải nghiệm người dùng. Trong khi SSO tập trung vào việc hợp nhất quy trình đăng nhập trên nhiều ứng dụng và dịch vụ, ELM mang lại khả năng quản lý tập trung cho các môi trường ảo hóa trong doanh nghiệp.

SSO cung cấp sự tiện lợi và tăng cường bảo mật cho người dùng cuối, nhưng cũng đòi hỏi đầu tư vào chi phí phát triển và phụ thuộc vào dịch vụ bên ngoài. Ngược lại, ELM hỗ trợ quản lý một cách hiệu quả các vCenter Server trong môi trường ảo hóa, giúp các tổ chức dễ dàng mở rộng và duy trì hệ thống với chi phí tối ưu hơn.

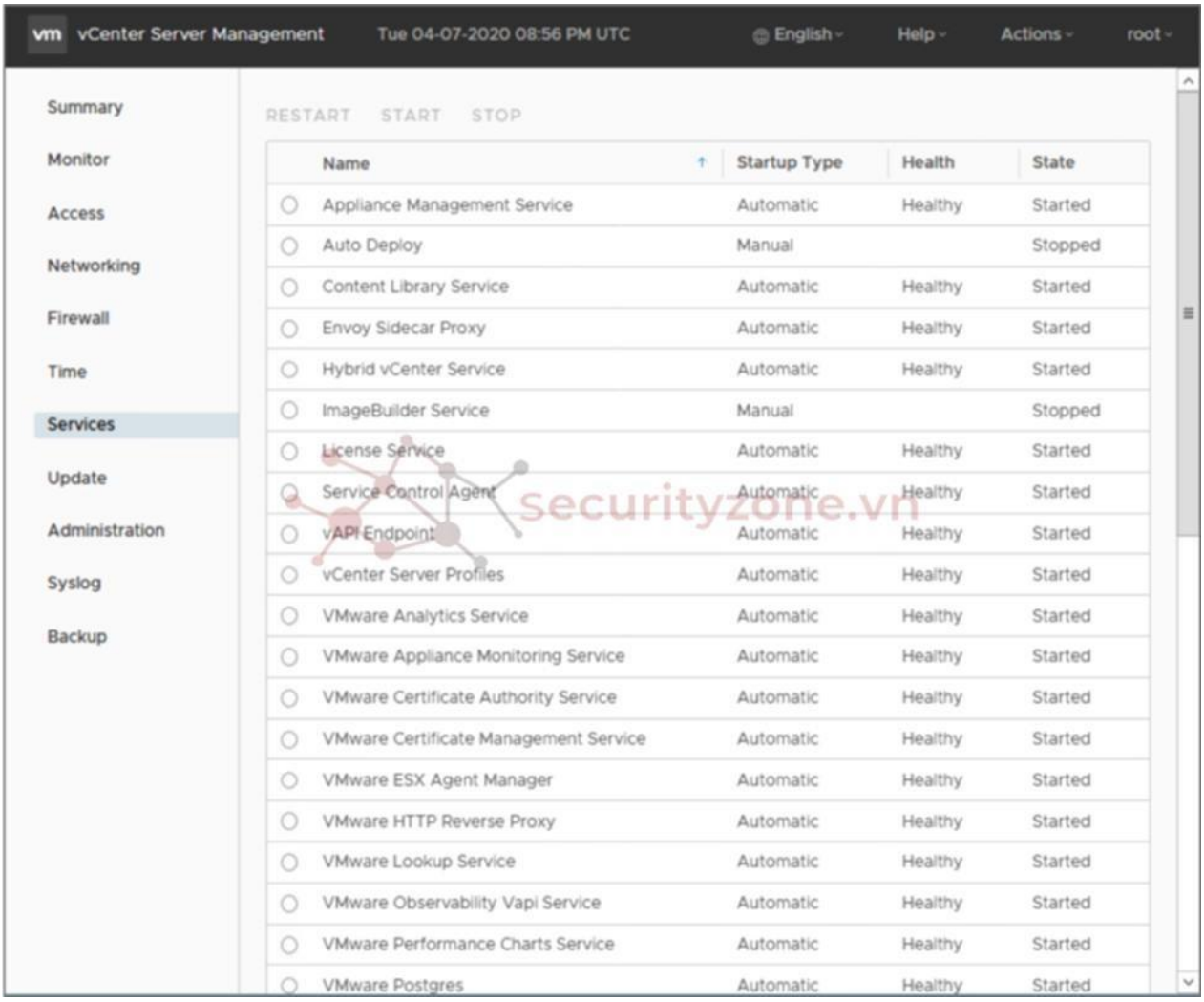
Sự kết hợp giữa SSO và ELM trong một môi trường ảo hóa doanh nghiệp có thể tạo ra một nền tảng quản lý toàn diện và bảo mật cao, đáp ứng nhu cầu ngày càng cao về tính hiệu quả và bảo mật trong quản lý hệ thống công nghệ thông tin.

Chương VI. Tìm Hiểu Về vCenter Service

I. Giới Thiệu vCenter Service

Khi cài đặt vCenter Server, nó sẽ cài đặt tất cả các thành phần cần thiết trên cùng một máy tính. Những thành phần này bao gồm các dịch vụ để xác thực người dùng, cấp giấy phép, và các công cụ quản lý khác.

vCenter Service là thành phần chính trong hệ thống quản lý ảo hóa của VMware, cung cấp một nền tảng tập trung cho việc quản lý, vận hành, cung cấp tài nguyên và đánh giá hiệu suất của các máy ảo và hosts.



Hình 19 Hình ảnh trực quan về vCenter Server

II. Dịch Vụ Chính Của vCenter Service

1. Dịch vụ xác thực

Đảm bảo rằng chỉ những người dùng được phép mới có thể truy cập vào hệ thống. Bao gồm:

vCenter Single Sign-On: Dịch vụ này cho phép đăng nhập vào tất cả các thành phần trong hệ thống vSphere mà không cần đăng nhập lại nhiều lần.

License Service: Quản lý các giấy phép sử dụng của hệ thống.

Lookup Service: Lưu trữ và quản lý thông tin cấu hình của các dịch vụ vCenter.

VMware Certificate Authority: Quản lý chứng chỉ bảo mật cho các kết nối trong hệ thống.

2. Dịch vụ quản lý

Giúp điều khiển và quản lý các máy ảo và máy chủ. Bao gồm:

vSphere Client: Giao diện dựa trên web cho phép quản lý hệ thống vSphere từ trình duyệt. vSphere Auto Deploy: Công cụ này giúp triển khai phần mềm ESXi lên nhiều máy chủ cùng lúc, giúp tiết kiệm thời gian và công sức khi cài đặt. vSphere ESXi Dump Collector: Công cụ thu thập thông tin khi hệ thống gặp sự cố, giúp chẩn đoán và khắc phục lỗi dễ dàng hơn.

III. Các Tính Năng Nổi Bật Của vCenter Service

1. Quản Lý Tập Trung (Centralized Management)

vCenter Service cho phép quản lý tất cả các máy chủ và máy ảo từ một nơi duy nhất, thay vì phải quản lý từng máy một cách riêng lẻ.

Lợi ích:Có thể quản lý hàng ngàn máy ảo và nhiều ESXi host (máy chủ cài đặt phần mềm ESXi) chỉ từ một giao diện duy nhất. Điều này giúp tiết kiệm thời gian và công sức khi vận hành hệ thống.

2. High Availability (HA) - Khả năng Sẵn Sàng Cao

Đây là tính năng giúp đảm bảo rằng các máy ảo của luôn hoạt động, ngay cả khi một trong các máy chủ vật lý (ESXi host) gặp sự cố.

Cách hoạt động: Nếu một ESXi host bị hỏng hoặc gặp vấn đề, máy ảo trên đó sẽ tự động được khởi động lại trên một host khác. Điều này giúp giảm thiểu thời gian ngừng hoạt động.

3. **vMotion:**

Tính năng này cho phép di chuyển một máy ảo từ một ESXi host sang một ESXi host khác mà không làm gián đoạn hoạt động của máy ảo đó.

Lợi ích: Có thể thực hiện bảo trì hoặc tối ưu hóa tài nguyên trên các host mà không cần tắt máy ảo, giúp duy trì sự liên tục của dịch vụ.

4. **Distributed Resource Scheduler (DRS) - Bộ Lập Lịch Tài Nguyên Phân Tán:**

DRS tự động phân phối các máy ảo giữa các ESXi host dựa trên tài nguyên hiện có và nhu cầu của từng máy ảo.

Lợi ích: Tính năng này giúp cân bằng tải, đảm bảo rằng không có host nào bị quá tải trong khi host khác lại rảnh rỗi. Điều này tối ưu hóa hiệu suất và duy trì tính sẵn sàng cao của hệ thống.

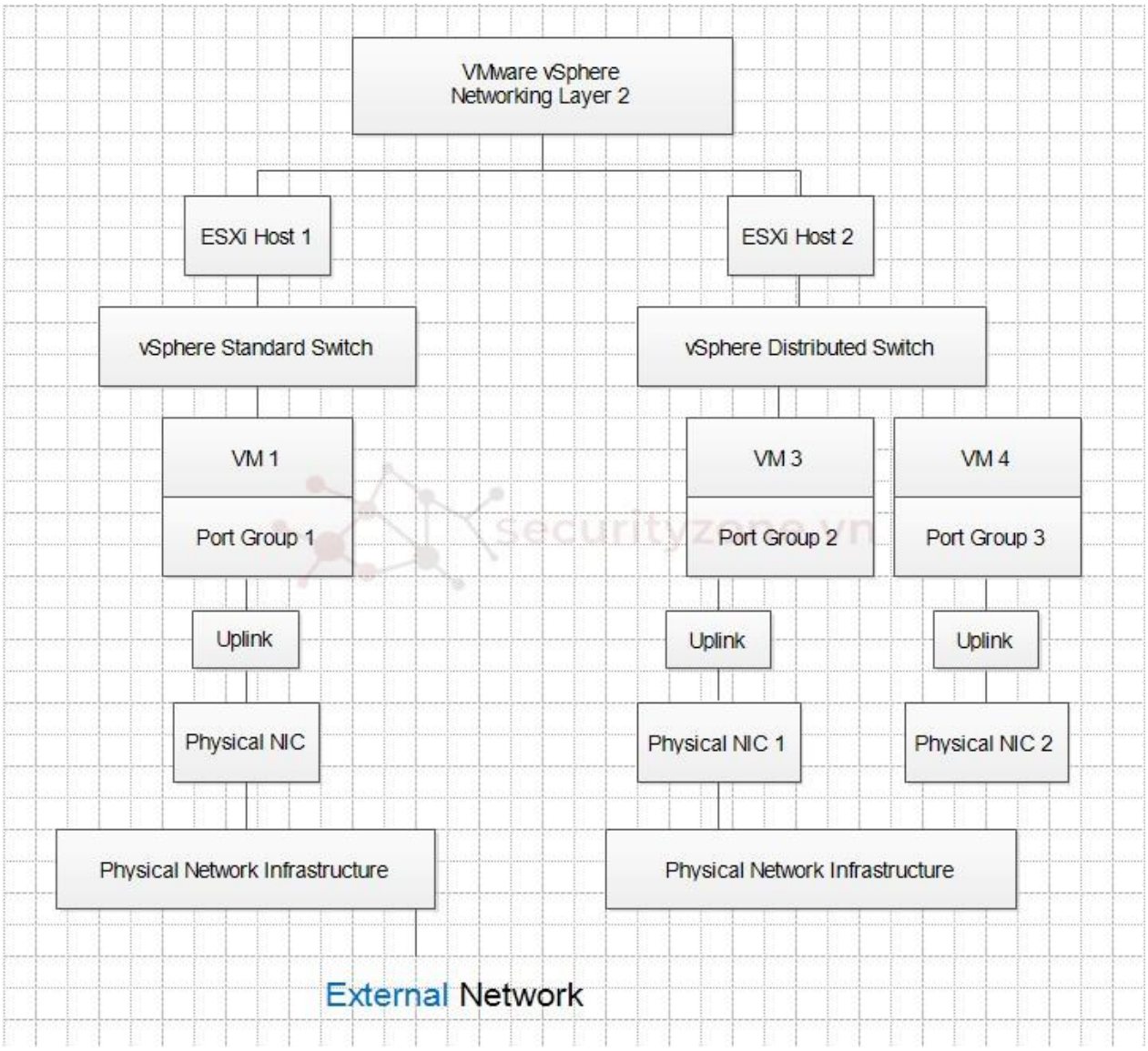
5. **vSphere Replication**

Đây là tính năng cho phép sao chép các máy ảo từ một site (vị trí) sang một site khác để đảm bảo rằng có thể khôi phục hệ thống nhanh chóng nếu có sự cố nghiêm trọng xảy ra.

Lợi ích: vSphere Replication giúp thiết lập các kịch bản DR (Disaster Recovery - Khôi phục sau thảm họa), bảo vệ dữ liệu và đảm bảo rằng có thể khôi phục hoạt động một cách nhanh chóng sau thảm họa.

Chương VII. Tìm hiểu về vSphere Layer 2 Networking

Giới thiệu về vSphere Networking vSphere Networking là một phần quan trọng của hệ thống ảo hóa VMware, cho phép các máy ảo (VM) trên cùng một host hoặc trên các host khác nhau giao tiếp với nhau và với mạng vật lý bên ngoài. Nó cung cấp cơ chế để quản lý lưu lượng mạng, bảo mật và hiệu năng, giúp tối ưu hóa việc sử dụng tài nguyên mạng trong môi trường ảo hóa.



Hình 20 Hình ảnh mô phỏng hệ thống Networking Layer 2

I. Cấu trúc và Chức năng của vSphere Networking

1. vSphere Standard Switch (vSS)

- **Cấu trúc**:
    - vSS là loại switch ảo cơ bản nhất trong VMware vSphere, tồn tại trên từng ESXi host riêng lẻ.
    - Mỗi vSS có thể chứa nhiều **Port Group** - nhóm cổng dùng để kết nối các máy ảo (VM) với mạng ảo hoặc mạng vật lý. o **Uplinks**: Đây là các card mạng vật lý (Physical NICs) gắn trên ESXi host, giúp kết nối vSS với mạng vật lý bên ngoài. o **NIC Teaming**: Cho phép sử dụng nhiều uplinks để cung cấp tính năng load balancing và failover cho vSS.
- **Chức năng**:
    - **Kết nối nội bộ**: vSS cho phép các VM trên cùng một ESXi host giao tiếp với nhau mà không cần phải qua mạng vật lý. o **Kết nối ra ngoài**: vSS kết nối các VM với mạng vật lý bên ngoài thông qua uplinks, cho phép các VM giao tiếp với các thiết bị khác trong mạng vật lý.
    - **Bảo mật**: vSS cung cấp các tùy chọn bảo mật như Promiscuous Mode, MAC Address Changes, và Forged Transmits, giúp kiểm soát việc truyền và nhận dữ liệu trong mạng ảo.
- **Ưu điểm**:
    - **Dễ dàng cấu hình**: Giao diện quản lý đơn giản, dễ thiết lập và sử dụng. o **Thích hợp cho môi trường nhỏ**: Không yêu cầu cấu hình phức tạp, phù hợp với các hệ thống nhỏ hoặc vừa.
- **Nhược điểm**:

- **Quản lý phân tán**: Mỗi vSS chỉ tồn tại trên một ESXi host, do đó cần phải cấu hình từng vSS riêng lẻ trên mỗi host, gây khó khăn khi quản lý và mở rộng. o **Giới hạn chức năng**: Không hỗ trợ các tính năng nâng cao như Network I/O Control (NIOC) hay Port Mirroring.

2. vSphere Distributed Switch (vDS)

- **Cấu trúc**:
  - vDS là một loại switch ảo tiên tiến hơn, được quản lý tập trung từ vCenter Server và áp dụng cho nhiều ESXi hosts cùng lúc. o **Distributed Port Groups**: Là các nhóm cổng được cấu hình trên vDS, cung cấp các kết nối mạng ảo đồng nhất trên tất cả các ESXi hosts kết nối với vDS.
  - **Uplinks**: Tương tự vSS, vDS cũng sử dụng uplinks để kết nối với mạng vật lý, nhưng việc cấu hình được thực hiện tập trung và áp dụng cho tất cả các host. o **Network I/O Control (NIOC)**: Quản lý băng thông mạng trên vDS, cho phép ưu tiên lưu lượng cho các dịch vụ quan trọng. o **Private VLAN (PVLAN)**: Cung cấp khả năng chia nhỏ thêm VLAN để cô lập lưu lượng giữa các máy ảo trong cùng một VLAN chính.
- **Chức năng**:
  - **Quản lý tập trung**: Tất cả các cấu hình mạng được quản lý từ vCenter Server và tự động áp dụng cho tất cả các ESXi host được kết nối với vDS. Điều này giúp dễ dàng quản lý và đảm bảo tính nhất quán.
  - **Load Balancing và Failover tiên tiến**: vDS hỗ trợ các phương pháp load balancing nâng cao và khả năng failover hiệu quả hơn so với vSS, giúp đảm bảo hiệu suất và độ tin cậy của hệ thống mạng. o **Giám sát và phân tích**: Với tính năng như Port Mirroring, vDS cho phép giám sát lưu lượng mạng, hỗ trợ cho việc phân tích và xử lý sự cố.

- **Ưu điểm**:
    - **Quản lý dễ dàng khi mở rộng**: Dễ dàng quản lý nhiều ESXi host từ một vị trí trung tâm, giảm thiểu công việc cấu hình khi hệ thống mở rộng. o **Hỗ trợ các tính năng nâng cao**: Với các tính năng như NIOC và PVLAN, vDS cung cấp khả năng kiểm soát băng thông và bảo mật cao hơn.
- **Nhược điểm**:
    - **Yêu cầu giấy phép cao cấp**: vDS chỉ có sẵn trong các phiên bản vSphere cao cấp, do đó không phù hợp cho các hệ thống với ngân sách hạn chế. o **Phức tạp hơn trong cấu hình**: Việc cấu hình và quản lý vDS đòi hỏi kiến thức và kinh nghiệm sâu hơn so với vSS.

3. VLANs (Virtual LANs)

- **Cấu trúc**:
    - **VLAN ID**: Mỗi VLAN trong môi trường vSphere được định danh bằng một số VLAN ID (thường từ 1 đến 4094). o **VLAN Tagging**: Khi lưu lượng di chuyển giữa các thiết bị trong một VLAN, nó được đánh dấu (tagged) bằng VLAN ID để đảm bảo nó chỉ được truyền trong phạm vi VLAN đó. o **Port Group**: Trong vSphere, mỗi VLAN được cấu hình trên một Port Group của vSS hoặc vDS, xác định các VM nào sẽ thuộc về VLAN đó.
- **Chức năng**:
    - **Phân đoạn mạng logic**: VLANs cho phép chia mạng vật lý thành các phân đoạn mạng logic, giúp tách biệt lưu lượng giữa các nhóm thiết bị khác nhau.
    - **Tăng cường bảo mật**: Bằng cách cô lập lưu lượng mạng giữa các VLAN, hệ thống mạng được bảo vệ tốt hơn trước các cuộc tấn công nội bộ và tránh hiện tượng broadcast storm. o **Tối ưu hóa băng thông**: Giảm thiểu lưu lượng broadcast không cần thiết, giúp tối ưu hóa băng thông trong mạng.

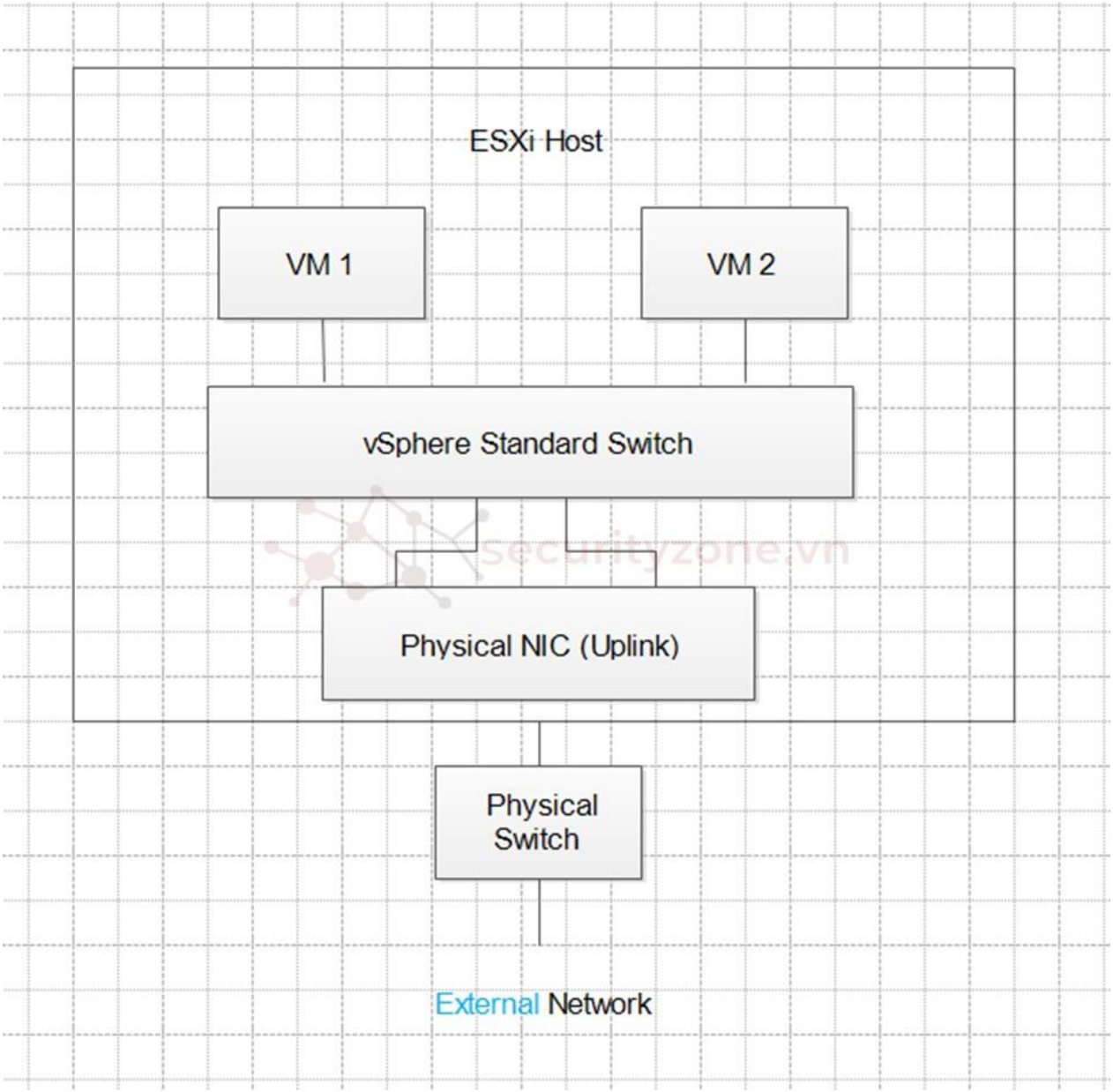
- **Ưu điểm**:
    - **Linh hoạt trong quản lý mạng**: Dễ dàng thêm hoặc xóa VLAN, điều chỉnh cấu hình mạng mà không cần thay đổi phần cứng vật lý. o **Tăng tính bảo mật**: Phân chia mạng một cách logic, giúp ngăn chặn truy cập trái phép giữa các phân đoạn mạng.
- **Nhược điểm**:
    - **Phức tạp trong quản lý**: Cần cấu hình cẩn thận để tránh xung đột VLAN ID và đảm bảo tính toàn vẹn của cấu trúc mạng. o **Cần có kiến thức chuyên sâu**: Việc cấu hình và quản lý VLAN yêu cầu kiến thức sâu về mạng, đặc biệt khi triển khai trên vDS.

III. Cách thức Hoạt động của Các Cấu Trúc Phổ Biến

1. vSphere Standard Switch (vSS)

- **Cách thức hoạt động**:
    - Khi một máy ảo (VM) trên ESXi host cần kết nối với mạng, nó sẽ sử dụng một **Port Group** được cấu hình trên vSS. Port Group này chứa các thiết lập về kết nối mạng, bao gồm cả VLAN nếu có.
    - **Uplinks** trên vSS kết nối với card mạng vật lý của ESXi host. Khi VM gửi gói dữ liệu, vSS sẽ chuyển tiếp gói này qua uplink tới mạng vật lý. Nếu gói dữ liệu được định tuyến đến một VM khác trên cùng một host, vSS sẽ chuyển gói này trực tiếp mà không cần qua mạng vật lý. o **NIC Teaming**: vSS hỗ trợ sử dụng nhiều uplinks cho một Port Group. Điều này cho phép chia sẻ lưu lượng mạng (load balancing) và đảm bảo kết nối liên tục nếu một uplink bị hỏng (failover).

- **Mô tả mô hình**: VM kết nối với vSS trên một ESXi host, với các đường dẫn từ vSS ra mạng vật lý thông qua uplinks (NICs).



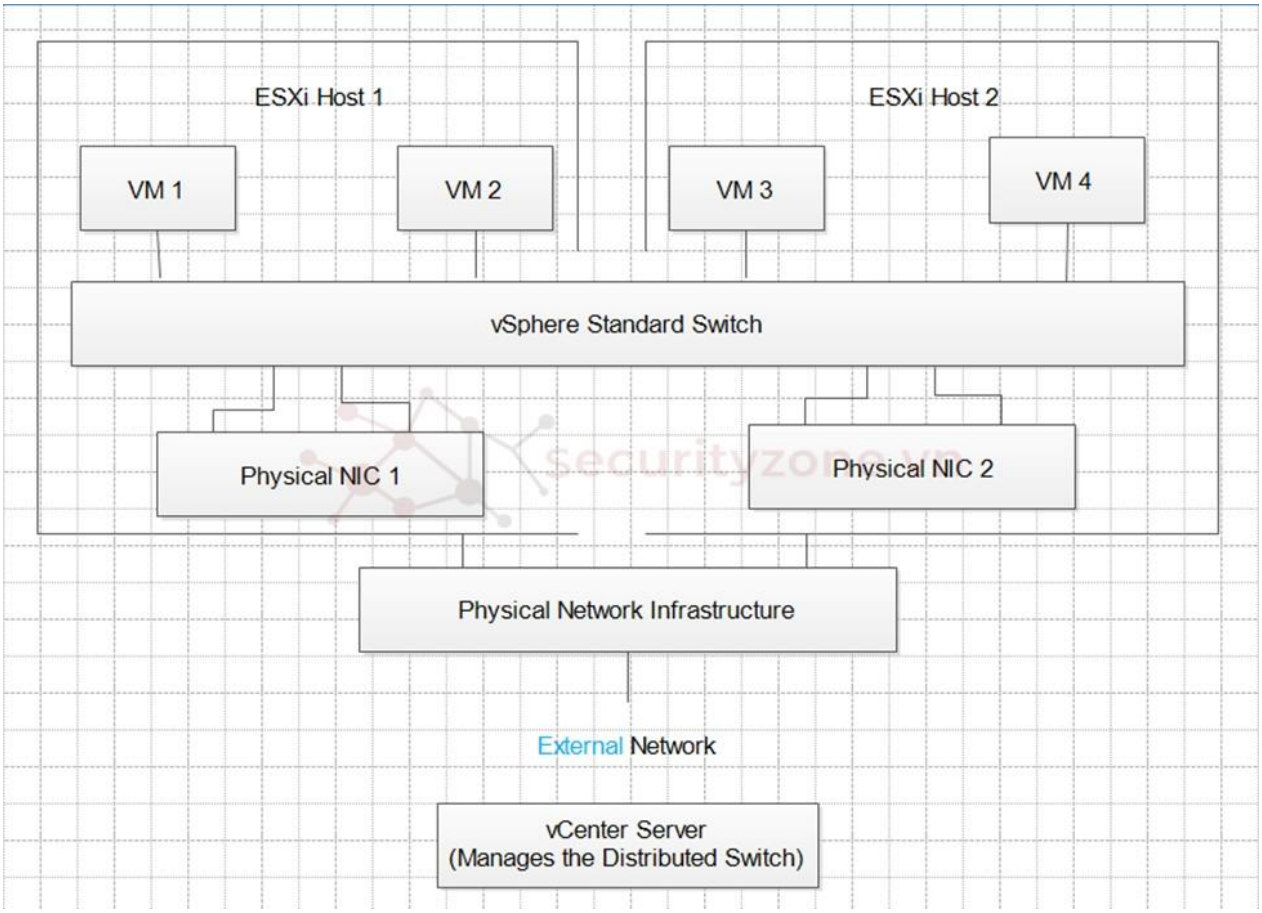
Hình 21 Hình ảnh mô phỏng cách thức hoạt động của vSS

vSS như một trung tâm chuyển mạch (switch) đơn giản nằm bên trong mỗi ESXi host, kết nối các VM với nhau và với mạng bên ngoài. Mỗi uplink đại diện cho một dây cáp kết nối switch ảo này với mạng vật lý.

2. vSphere Distributed Switch (vDS)

- **Cách thức hoạt động**:
    - vDS cung cấp một nền tảng quản lý mạng tập trung từ vCenter Server. Khi một VM cần kết nối mạng, nó sẽ kết nối thông qua một **Distributed Port Group** trên vDS.
    - Cấu hình của vDS (như VLAN, NIC Teaming, và Security Policies) được áp dụng đồng bộ trên tất cả các ESXi hosts kết nối với vDS. Điều này đảm bảo rằng tất cả các VM trên các hosts khác nhau có cấu hình mạng đồng nhất. o vDS sử dụng **Distributed Uplinks**, kết nối với các card mạng vật lý trên từng host. Khi một gói dữ liệu cần được gửi đi, vDS sẽ xác định đường đi tốt nhất dựa trên các chính sách đã được cấu hình và gửi gói dữ liệu đó thông qua uplink tương ứng.

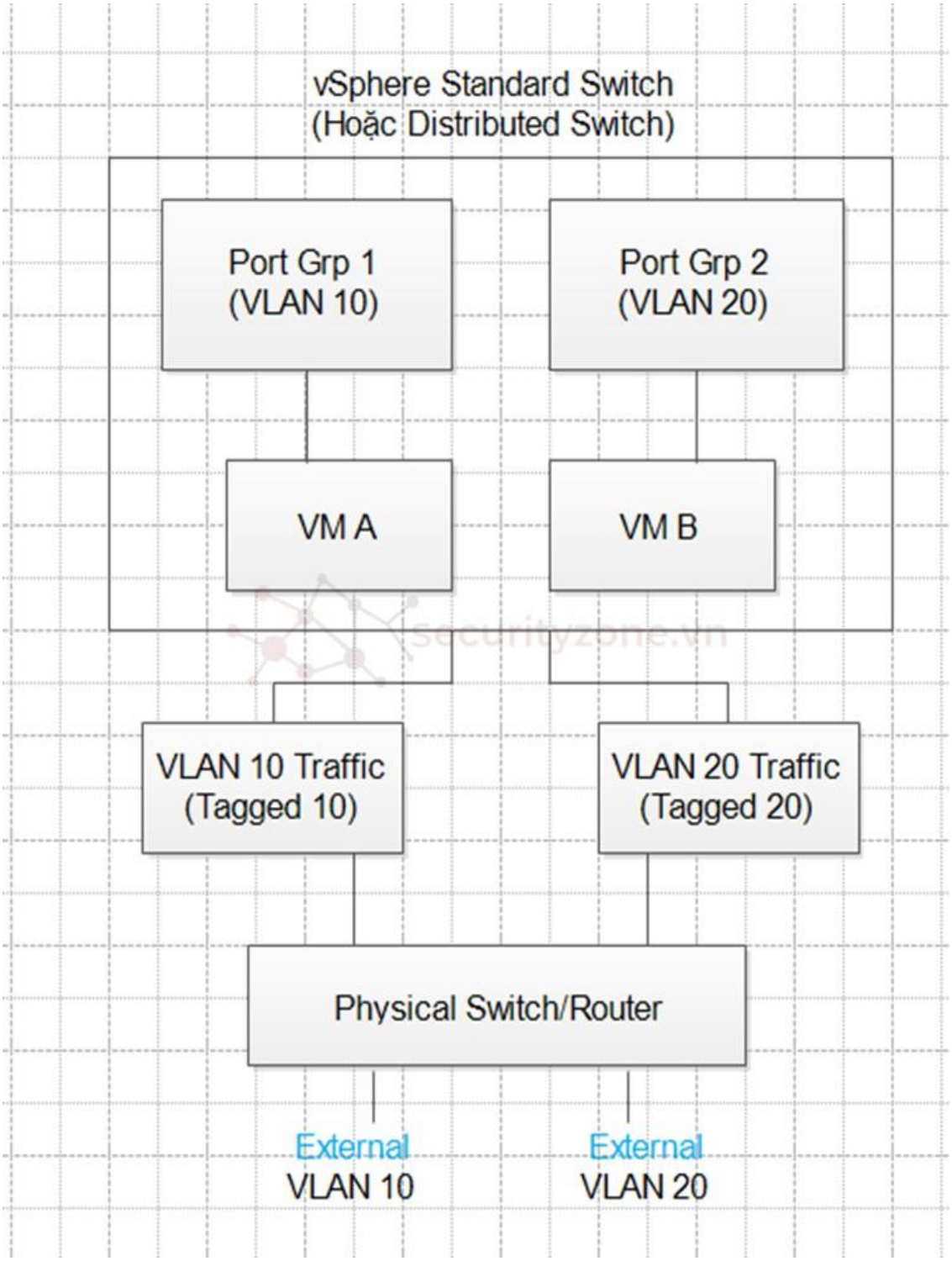
Mô tả mô hình: Nhiều ESXi hosts kết nối với một vDS thông qua Distributed Uplinks, thể hiện cách mà tất cả các hosts chia sẻ một cấu hình mạng chung.



Hình 22 Hình ảnh mô phỏng cách thức hoạt động của vDS

vDS như một switch ảo khổng lồ trải dài qua nhiều ESXi hosts, với vCenter Server như trung tâm điều khiển. Mỗi Port Group và Uplink trên vDS đại diện cho các cổng mạng và dây cáp kết nối các VM và hosts trong mạng.

3. VLANs



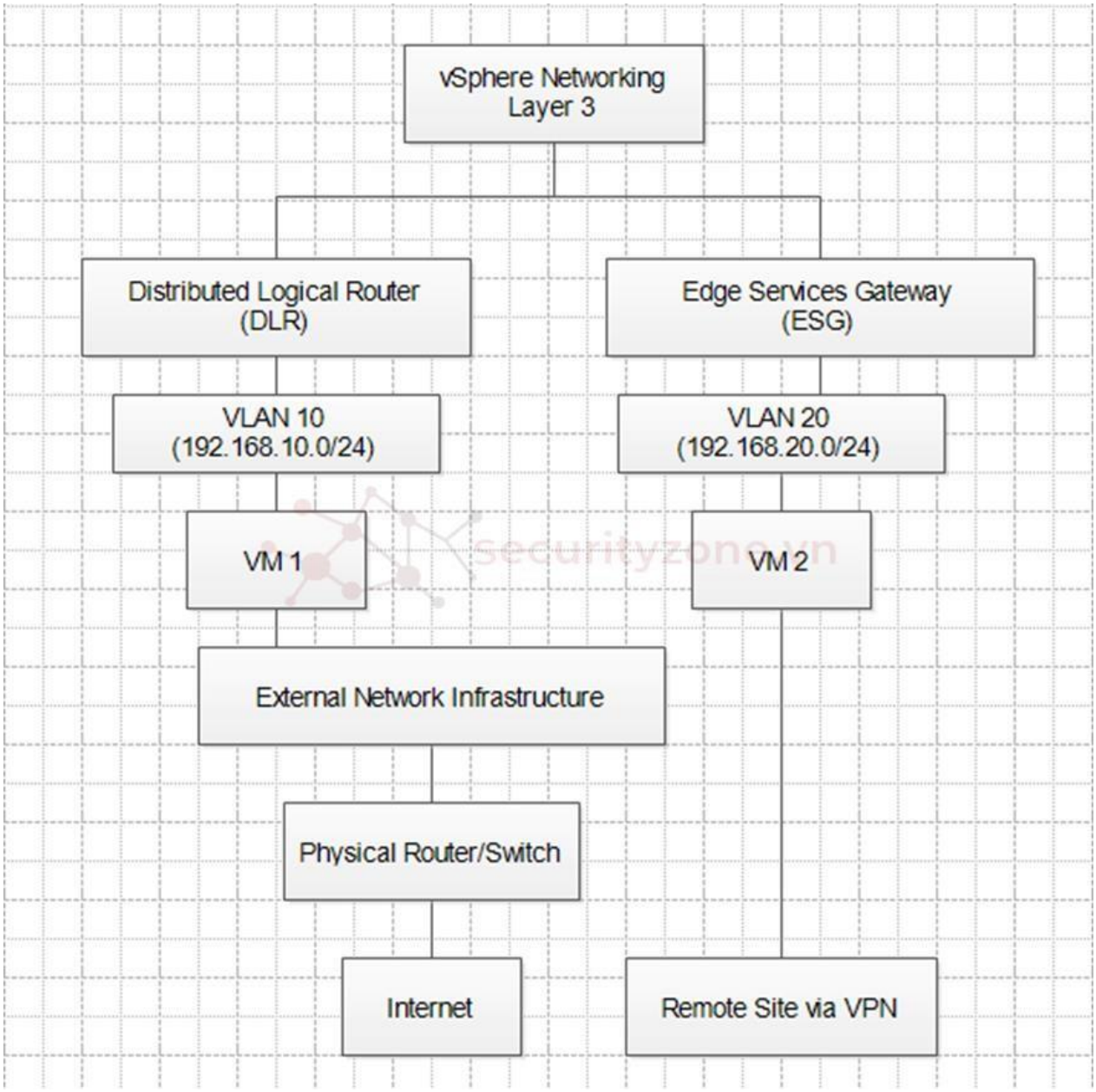
Hình 23 Hình ảnh mô phỏng cách VLAN hoạt động

VLAN như những "cộng đồng" khác nhau trong cùng một thành phố mạng, với mỗi cộng đồng chỉ có thể giao tiếp nội bộ trừ khi có cầu nối qua router.

Chương VIII. Tìm hiểu về vSphere Networking Layer 3

I. Giới thiệu về vSphere Networking Layer 3

vSphere Networking Layer 3 liên quan đến việc định tuyến lưu lượng giữa các mạng ảo, cho phép các máy ảo (VM) trên các mạng khác nhau giao tiếp với nhau thông qua các router ảo hoặc vật lý. Trong Layer 3, lưu lượng không chỉ bị giới hạn trong một mạng con (subnet) mà có thể được định tuyến giữa các mạng con khác nhau.



Hình 24 Hình ảnh mô phỏng về Vsphere Network Layer 3

II. Cấu trúc và Chức năng

1. Distributed Logical Router (DLR)

- **Cấu trúc**: DLR là một thành phần chính trong kiến trúc VMware NSX, cung cấp khả năng định tuyến giữa các mạng ảo (VLANs) trên cùng một ESXi host hoặc

trên nhiều ESXi hosts. DLR hoạt động ở Layer 3 và được tích hợp trực tiếp với hypervisor, giúp giảm thiểu độ trễ và tăng hiệu suất.

- **Chức năng**:
    - Định tuyến giữa các mạng ảo (VLANs).
    - Hỗ trợ các tính năng như Access Control Lists (ACLs) để kiểm soát truy cập giữa các mạng.
    - Tích hợp với NSX Firewall để cung cấp khả năng bảo mật.
- **Ưu điểm**: Giảm tải cho mạng vật lý, giảm độ trễ do việc định tuyến diễn ra ngay trên ESXi host.
- **Nhược điểm**: Phụ thuộc vào VMware NSX và phức tạp trong việc triển khai và quản lý.

2. Edge Services Gateway (ESG)

- **Cấu trúc**: ESG là một thành phần khác của VMware NSX, cung cấp các dịch vụ mạng Layer 3 như định tuyến, NAT (Network Address Translation), và VPN (Virtual Private Network). ESG thường được sử dụng để kết nối mạng ảo với mạng vật lý bên ngoài.
- **Chức năng**:
    - Định tuyến giữa các mạng ảo và mạng vật lý.
    - Cung cấp dịch vụ NAT để chuyển đổi địa chỉ IP.
    - Hỗ trợ VPN để bảo mật kết nối từ xa.
- **Ưu điểm**: Cung cấp các dịch vụ mạng toàn diện và mạnh mẽ, dễ dàng mở rộng và quản lý.
- **Nhược điểm**: Có thể gây ra bottleneck nếu không được cấu hình đúng cách.

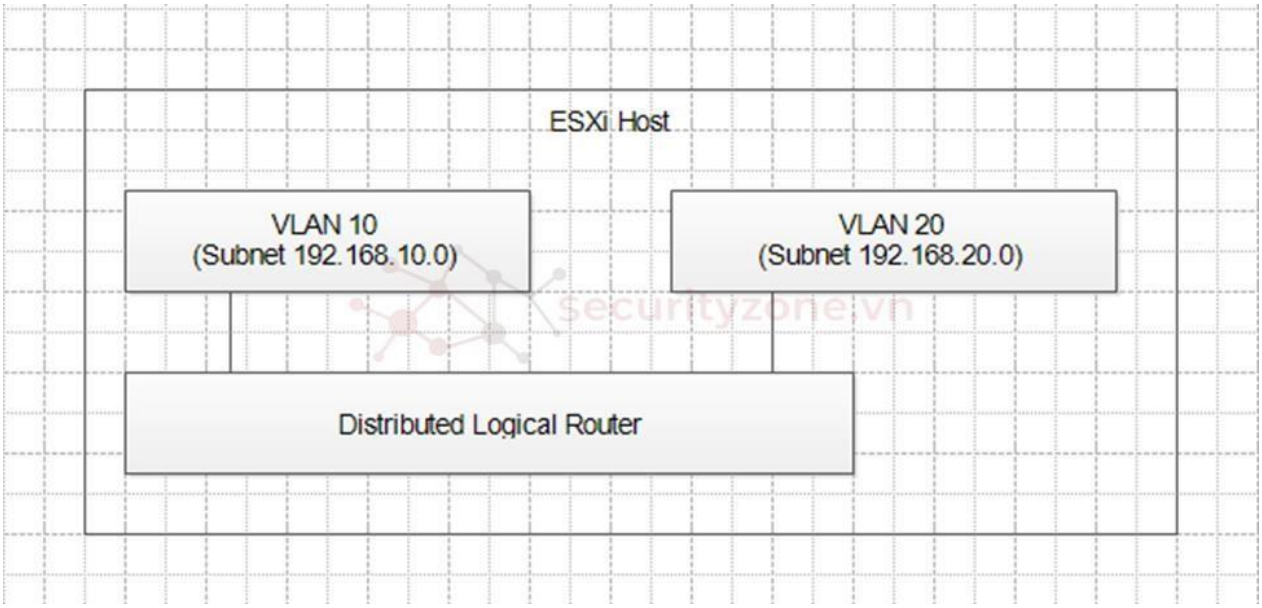
Cách thức Hoạt động của Layer 3 trong vSphere

1. Distributed Logical Router (DLR)

Cách thức Hoạt động:

- **Nội bộ Host**: Khi một máy ảo (VM) trên một ESXi host cần giao tiếp với một VM khác trên cùng host nhưng nằm trong một VLAN khác, DLR sẽ thực hiện quá trình định tuyến nội bộ mà không cần đi qua switch hoặc router vật lý bên ngoài. Điều này giúp giảm độ trễ và tăng tốc độ truyền dữ liệu.
- **Giữa các Host**: Nếu hai VM thuộc các VLAN khác nhau nhưng nằm trên các ESXi hosts khác nhau, DLR vẫn có thể định tuyến lưu lượng trực tiếp giữa các VLAN mà không cần phải chuyển dữ liệu ra ngoài mạng vật lý. DLR sử dụng bảng định tuyến nội bộ được chia sẻ trên các ESXi hosts để thực hiện việc này.
- **Chức năng chính**:
    - **Định tuyến liên VLAN**: DLR cho phép giao tiếp giữa các VLAN khác nhau mà không cần thiết phải có một router vật lý.
    - **Tiết kiệm tài nguyên mạng**: Bằng cách giữ lưu lượng nội bộ trong môi trường ảo hóa, DLR giảm thiểu việc sử dụng băng thông mạng vật lý và giảm tải cho các thiết bị mạng vật lý.

Mô hình mô tả:



Hình 25 Hình ảnh mô phong DLR

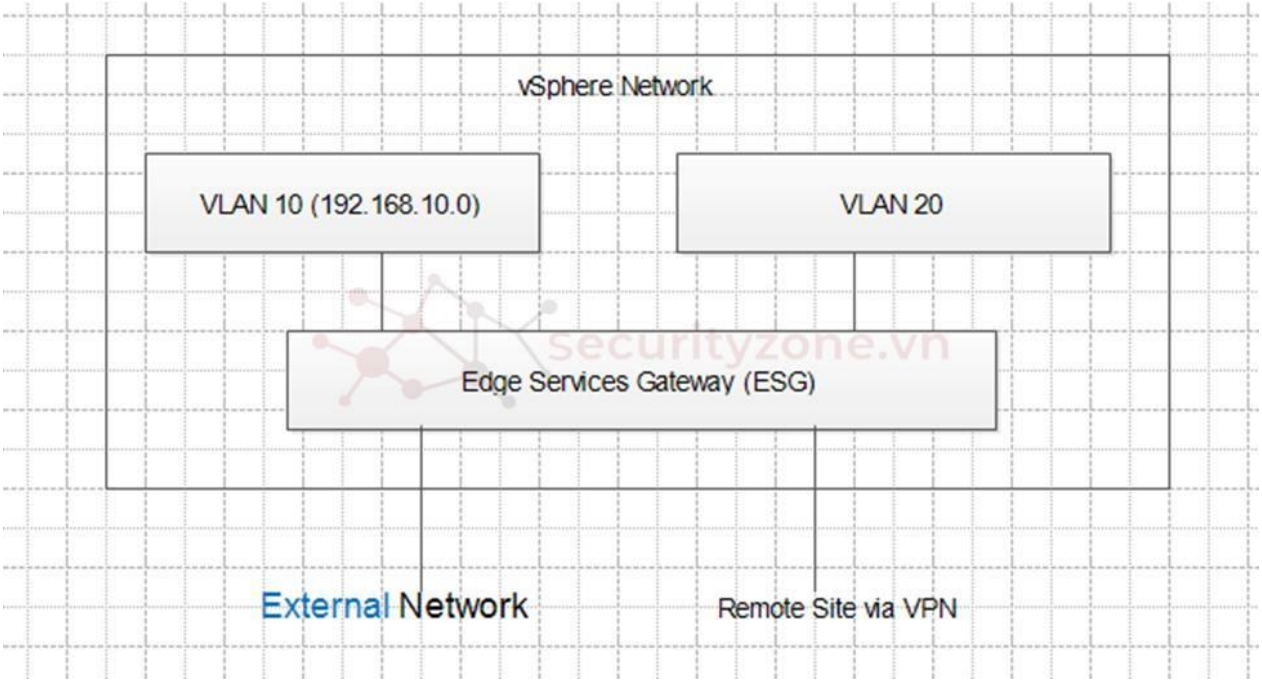
2. Edge Services Gateway (ESG)

Cách thức Hoạt động:

- **Kết nối với Mạng Vật Lý**: ESG đóng vai trò như một gateway định tuyến giữa môi trường mạng ảo và mạng vật lý bên ngoài. Khi VM cần kết nối ra Internet hoặc đến các mạng khác ngoài môi trường ảo hóa, ESG sẽ chịu trách nhiệm định tuyến lưu lượng đó.
- **Chức năng Bổ sung**:

  o **NAT (Network Address Translation)**: ESG có khả năng chuyển đổi địa chỉ IP từ mạng ảo sang địa chỉ IP công cộng hoặc ngược lại, giúp quản lý và bảo mật kết nối giữa các mạng. o **VPN (Virtual Private Network)**: ESG cung cấp khả năng tạo kết nối an toàn với các site từ xa hoặc với mạng doanh nghiệp từ ngoài môi trường ảo hóa thông qua các kênh VPN, đảm bảo rằng dữ liệu được mã hóa và bảo mật.

Mô hình mô tả:



Hình 26 Hình ảnh mô phong ESG

Chương IX. Tìm hiểu về Virtual Switch & Type of Virtual Switch (vSS, vDS)

I. Giới thiệu về Virtual Switch

Trong môi trường ảo hóa của VMware, Virtual Switch (Switch ảo) là một thành phần mạng quan trọng cho phép các máy ảo (VM) giao tiếp với nhau cũng như với mạng vật lý bên ngoài. Tương tự như switch vật lý, Virtual Switch có chức năng chuyển tiếp các gói dữ liệu giữa các thiết bị kết nối với nó, nhưng nó hoạt động hoàn toàn trong phần mềm và trên các ESXi hosts.

II. Các Loại Virtual Switch

VMware cung cấp hai loại Virtual Switch chính: vSphere Standard Switch (vSS) và vSphere Distributed Switch (vDS). Mỗi loại switch có cấu trúc và chức năng riêng biệt, phù hợp với các yêu cầu và quy mô khác nhau của hệ thống ảo hóa.

1. vSphere Standard Switch (vSS)

- Cấu trúc:
    - Tạo và Quản lý trên Từng Host: vSS được tạo và quản lý riêng lẻ trên từng ESXi host. Mỗi ESXi host trong môi trường vSphere sẽ có một hoặc nhiều vSS riêng biệt, và cấu hình của vSS này không được chia sẻ hoặc đồng bộ với các ESXi host khác.
    - Port Group: Một vSS có thể chứa nhiều Port Group. Port Group là một nhóm các cổng ảo được gán cho các VM, giúp định cấu hình cách các VM kết nối với switch. Port Group có thể được cấu hình với các thiết lập như VLAN ID, chính sách bảo mật, và băng thông.
    - Uplink: vSS kết nối với mạng vật lý thông qua một hoặc nhiều uplink (các NIC vật lý của ESXi host). Các uplink này cho phép lưu lượng từ VM đi ra ngoài hoặc lưu lượng từ mạng vật lý đến được chuyển tiếp vào mạng ảo.
    - Không có Quản lý Tập Trung: Mỗi vSS phải được cấu hình riêng lẻ trên từng host, và bất kỳ thay đổi nào cũng phải được thực hiện thủ công trên mỗi host. Điều này có thể gây khó khăn khi quản lý các môi trường lớn với nhiều ESXi hosts.
- Chức năng:
    - Kết nối các máy ảo trên cùng một ESXi host với nhau và với mạng vật lý bên ngoài.
    - Quản lý các Port Group, cho phép gắn các VM vào các VLAN khác nhau.
- Ưu điểm:
    - Đơn giản để triển khai và quản lý trong các môi trường nhỏ hoặc ít phức tạp. o Không yêu cầu vCenter Server để quản lý.

- Nhược điểm:
    - Không thể quản lý tập trung. Mỗi vSS trên từng host cần được cấu hình riêng biệt, gây khó khăn trong việc duy trì nhất quán cấu hình mạng khi số lượng ESXi host tăng lên.
    - Khả năng mở rộng và tính năng hạn chế so với vDS.

2. vSphere Distributed Switch (vDS)

- Cấu trúc:
    - Tạo và Quản lý Tập Trung: vDS được tạo và quản lý tập trung thông qua vCenter Server. Khi tạo một vDS, nó tồn tại như một thực thể duy nhất trong môi trường vSphere và có thể được áp dụng cho nhiều ESXi hosts cùng lúc.
    - Distributed Port Group: Tương tự như vSS, vDS sử dụng Distributed Port Group để quản lý các kết nối mạng cho VM. Tuy nhiên, các Distributed Port Group này được áp dụng đồng nhất trên tất cả các ESXi hosts tham gia vDS, đảm bảo cấu hình mạng nhất quán trên toàn bộ môi trường.
    - Uplink Ports: vDS cung cấp các Uplink Ports, cho phép kết nối với các NIC vật lý trên ESXi hosts. Các Uplink Ports này được cấu hình tập trung và chia sẻ giữa các ESXi hosts, giúp tối ưu hóa việc sử dụng băng thông mạng và đảm bảo tính sẵn sàng cao.
    - Tính Năng Nâng Cao: vDS hỗ trợ các tính năng nâng cao như Network I/O Control (NIOC) để quản lý băng thông, Port Mirroring để giám sát lưu lượng, và Private VLAN để tăng cường bảo mật. Những tính năng này giúp vDS phù hợp hơn cho các môi trường lớn và phức tạp.
- Chức năng:

- Cung cấp các tính năng nâng cao như Network I/O Control (NIOC), Port Mirroring, và Distributed Port Groups, cho phép quản lý băng thông và bảo mật chi tiết hơn. o Cho phép cấu hình và quản lý mạng tập trung từ vCenter Server, đảm bảo tính nhất quán và giảm thiểu lỗi cấu hình.

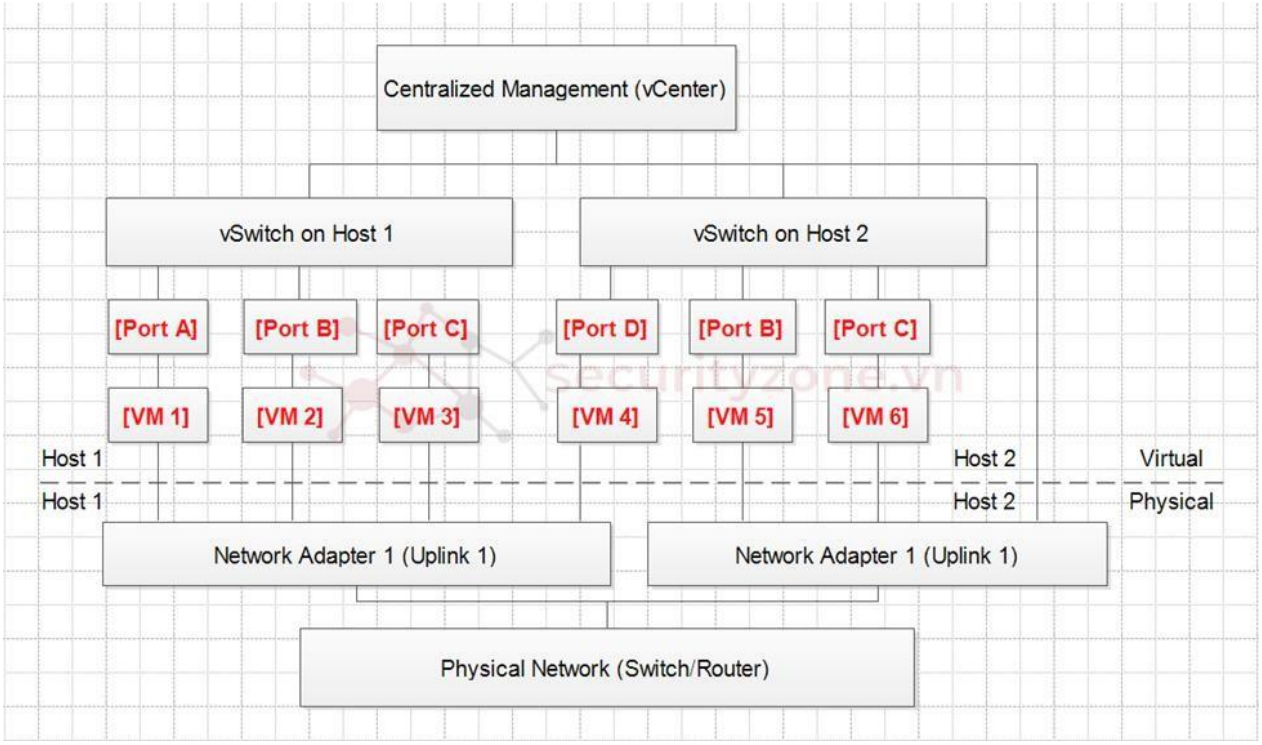
- Ưu điểm:
  - Quản lý tập trung, dễ dàng mở rộng và duy trì nhất quán cấu hình mạng trên nhiều ESXi hosts. o Cung cấp các tính năng nâng cao phù hợp cho các môi trường doanh nghiệp lớn và phức tạp.
- Nhược điểm:
  - Yêu cầu vCenter Server để quản lý, tăng chi phí và phức tạp cho việc triển khai. o Đòi hỏi sự hiểu biết sâu rộng về mạng ảo hóa để tận dụng hết các tính năng của vDS.

III. Cách thức Hoạt động của Virtual Switch

1. Cách thức hoạt động của vSphere Standard Switch (vSS)

- Khi một máy ảo gửi gói tin, vSS sẽ nhận và chuyển tiếp gói tin đến đích trong cùng một mạng ảo hoặc đến một uplink để truyền ra mạng vật lý.
- vSS không chia sẻ thông tin cấu hình với các vSS trên các ESXi hosts khác, do đó, cấu hình mạng phải được lặp lại trên mỗi host.

Mô hình quy trình hoạt động của vSS:



Hình 27 Hình ảnh mô phỏng quy trình hoạt động vSS

Quy trình hoạt động cơ bản:

- Máy ảo gửi/nhận dữ liệu qua Port Group và vSwitch.

- Nếu cùng máy chủ (Host1 hoặc Host2) và VLAN, dữ liệu được truyền ngay trên vSwitch.

- Nếu khác máy chủ hoặc VLAN, dữ liệu được truyền qua Uplink đến mạng vật lý.

- Mạng vật lý xử lý và truyền dữ liệu đến đích.

- vCenter quản lý toàn bộ cấu hình và giám sát lưu lượng mạng.

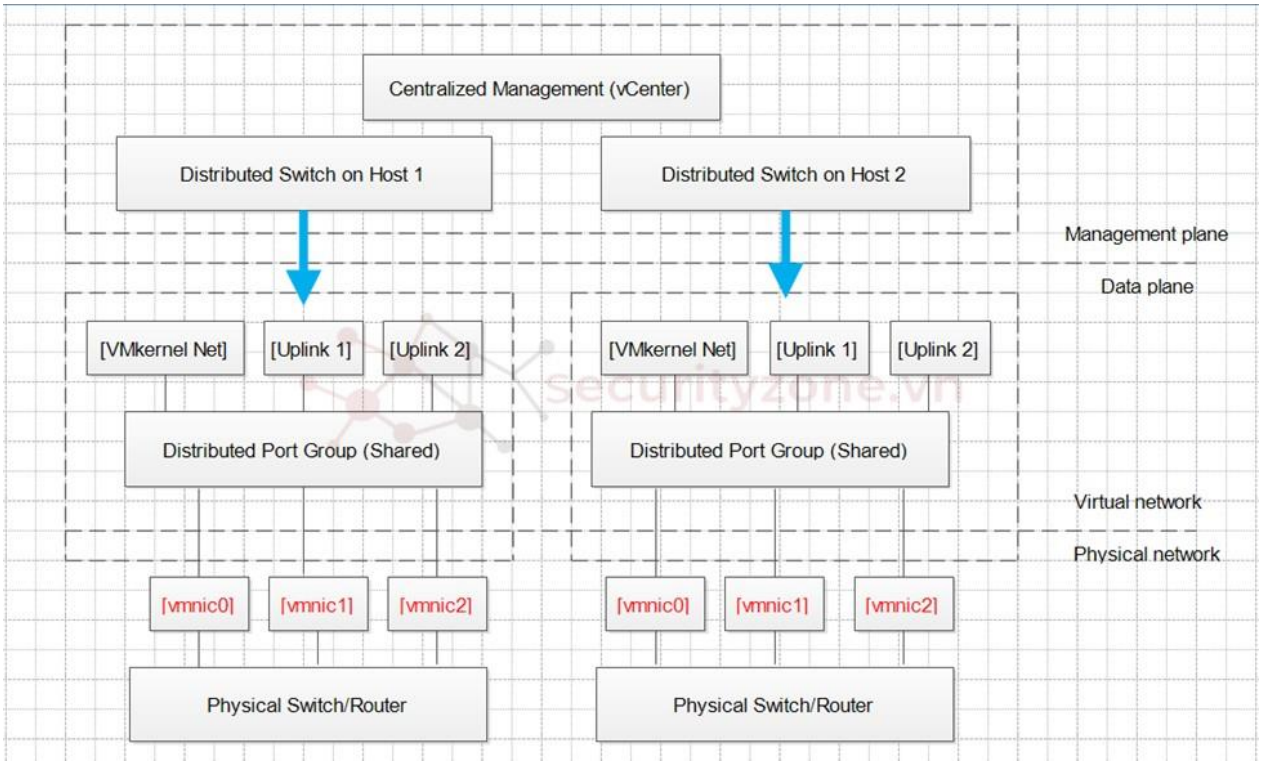
2. Cách thức hoạt động của vSphere Distributed Switch (vDS)

vDS hoạt động như một switch ảo duy nhất trên toàn bộ hệ thống, với các cấu hình và quy tắc mạng được áp dụng đồng nhất cho tất cả các ESXi hosts tham gia.

- Khi một máy ảo gửi gói tin, vDS quản lý và chuyển tiếp gói tin theo các quy tắc đã được cấu hình tập trung từ vCenter Server.

- Các tính năng nâng cao như Port Mirroring cho phép sao chép lưu lượng từ một cổng đến một cổng khác để giám sát và phân tích.

Mô hình quy trình hoạt động của vDS:



Hình 28 Hình ảnh quy trình hoạt động của vDS

Quy trình hoạt động cơ bản:

- VM1 trên Host1 gửi dữ liệu(Dữ liệu được gửi từ VM1 trên Host1, yêu cầu truyền thông qua mạng)
- Dữ liệu đi qua Distributed Port Group trên vDS của Host1 và được chuyển đến NIC vật lý thông qua Uplink (Dữ liệu từ VM1 được đưa vào Distributed Port Group, sau đó đi qua

Uplink trên vDS của Host1 để đến NIC vật lý "vmnic" trên Host1)

- Dữ liệu đi qua Physical Network (Sau khi rời khỏi NIC vật lý của Host1, dữ liệu di chuyển qua các thiết bị mạng vật lý như switch hoặc router để đến Host2)

- Khi đến Host2, dữ liệu đi vào qua NIC vật lý, thông qua Uplink và Distributed Port Group trên vDS của Host2 (Dữ liệu đến NIC vật lý trên Host2, sau đó đi qua Uplink và được chuyển vào Distributed Port Group tương ứng trên vDS của Host2)
- Dữ liệu cuối cùng đến VM đích trên Host2 (Dữ liệu được đưa đến VM đích trên Host2 thông qua Distributed Port Group và vDS, hoàn thành quá trình truyền thông)

Chương X. Tìm hiểu về Type of Virtual Switch Connections

I. Tổng Quát

Virtual switches (vSwitches) là các thành phần quan trọng trong môi trường ảo hóa, cho phép các máy ảo (VMs) và các thiết bị vật lý giao tiếp với nhau. Virtual switches cung cấp các kết nối mạng giữa VMs và cho phép quản lý lưu lượng mạng giữa các thành phần trong môi trường ảo hóa.

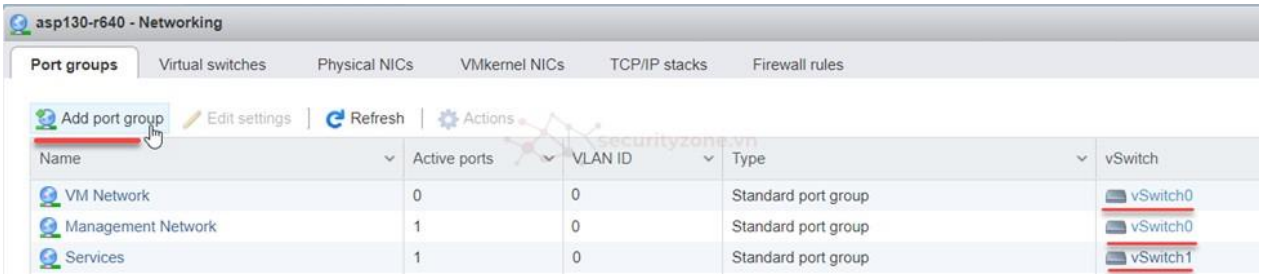
II. Các Loại Kết Nối của Virtual Switch

1. VM Port Group (Virtual Machine Port Group)

VM Port Group là nhóm các cổng mạng được thiết kế dành riêng cho máy ảo. Hãy hình dung nó như một "bảng cắm" nơi các máy ảo kết nối để trao đổi dữ liệu nội bộ hoặc truy cập mạng bên ngoài.

Chức năng: Cung cấp kết nối mạng cho các máy ảo. Bạn có thể áp dụng các chính sách quản lý như VLAN (mạng ảo) để kiểm soát cách các máy ảo giao tiếp với nhau hoặc kết nối ra bên ngoài.

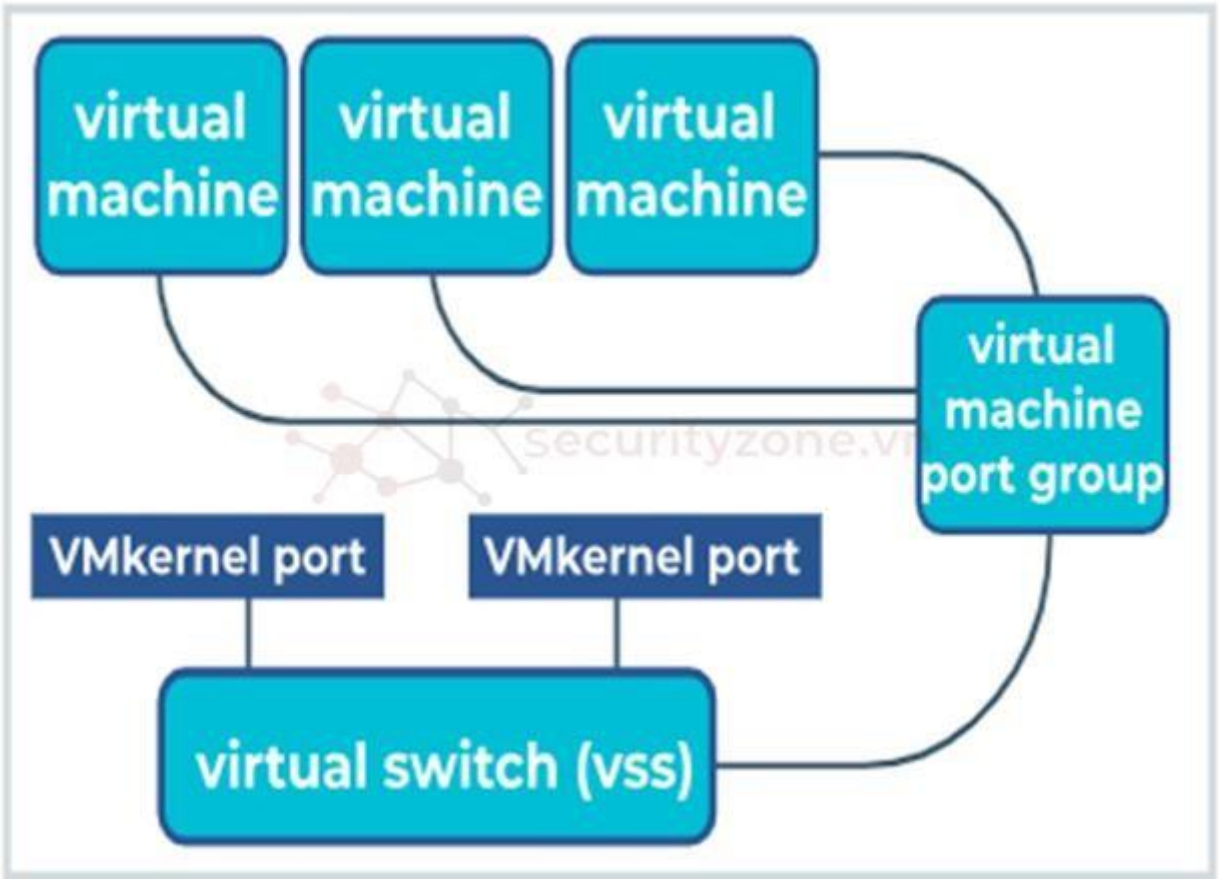
VM Port Group hữu ích khi bạn cần tạo một môi trường mạng chung cho nhiều máy ảo hoặc yêu cầu các máy ảo truy cập vào mạng vật lý, đồng thời áp dụng các chính sách bảo mật và quản lý đồng nhất.



Hình 29 Mô phỏng giao diện của Port Group trong vCenter

2. VMkernel Port (VMkernel Adapter)

VMkernel Port là cổng dành riêng cho các dịch vụ quản trị và hệ thống quan trọng như vMotion (di chuyển máy ảo giữa các host ESXi mà không cần tắt máy), truy cập lưu trữ mạng (iSCSI, NFS), hoặc quản lý ESXi host.



Hình 30 Hình ảnh mô phỏng cách hoạt động của Vmkernel Port

Chức năng: VMkernel Port quản lý các dịch vụ quan trọng của hệ thống như di chuyển máy ảo, kết nối với lưu trữ qua mạng, và cung cấp đường kết nối cho việc quản lý hệ thống.

Sử dụng VMkernel Port khi bạn cần cấu hình các tính năng quan trọng như vMotion, hoặc khi ESXi host cần kết nối đến hệ thống lưu trữ qua mạng một cách an toàn và ổn định.

Cổng VMkernel có thể xử lý lưu lượng từ đúng 6 dịch vụ: vMotion traffic, Fault tolerance (FT), Management traffic, vSphere replication traffic, iSCSI, NFS.

Uplink Port

Uplink Port là cổng kết nối giữa virtual switch và mạng vật lý bên ngoài như mạng LAN, WAN hoặc Internet.

Chức năng: Đảm nhiệm vai trò kết nối giữa máy ảo và hệ thống mạng vật lý. Uplink Port đóng vai trò như "cầu nối" giúp truyền tải dữ liệu giữa thế giới ảo và mạng thực. Khi bạn cần kết nối máy ảo với mạng bên ngoài hoặc Internet, Uplink Port sẽ là lựa chọn chính. Nó cũng giúp các máy ảo giao tiếp với các thiết bị vật lý.

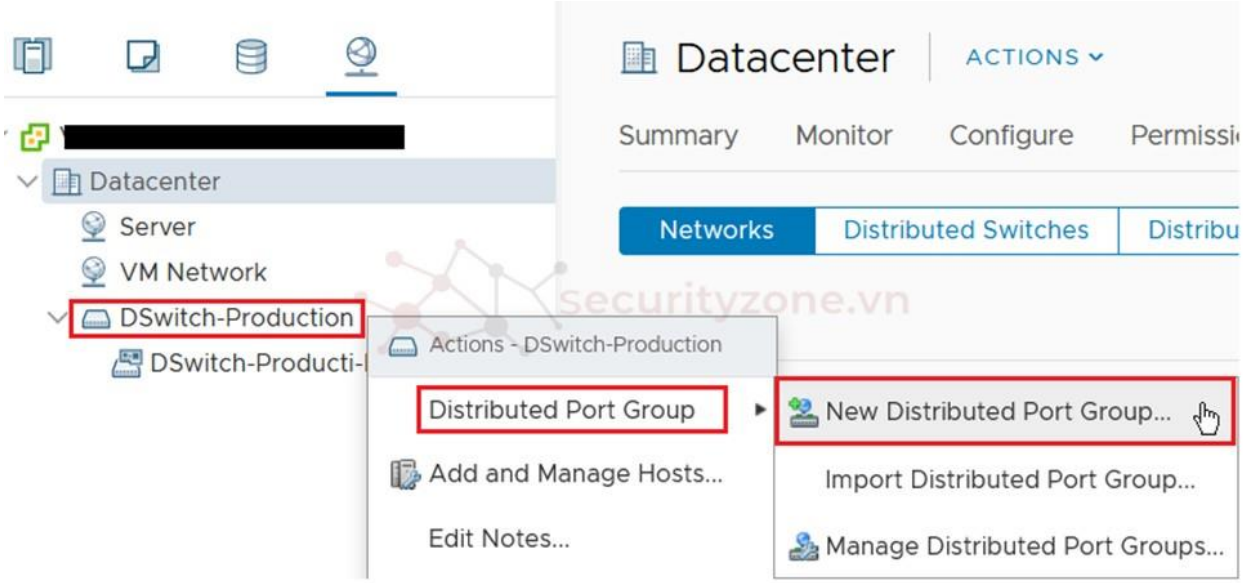
III. Distributed Port Group (DPG)

Distributed Port Group là phiên bản nâng cao của VM Port Group, hoạt động trên

Distributed Virtual Switch (vDS), một loại switch ảo có khả năng quản lý nhiều ESXi host cùng lúc.

Chức năng: Quản lý cấu hình mạng cho nhiều ESXi host từ một giao diện duy nhất. Distributed Port Group giúp việc áp dụng các chính sách mạng nhất quán và đồng bộ giữa các host trở nên dễ dàng.

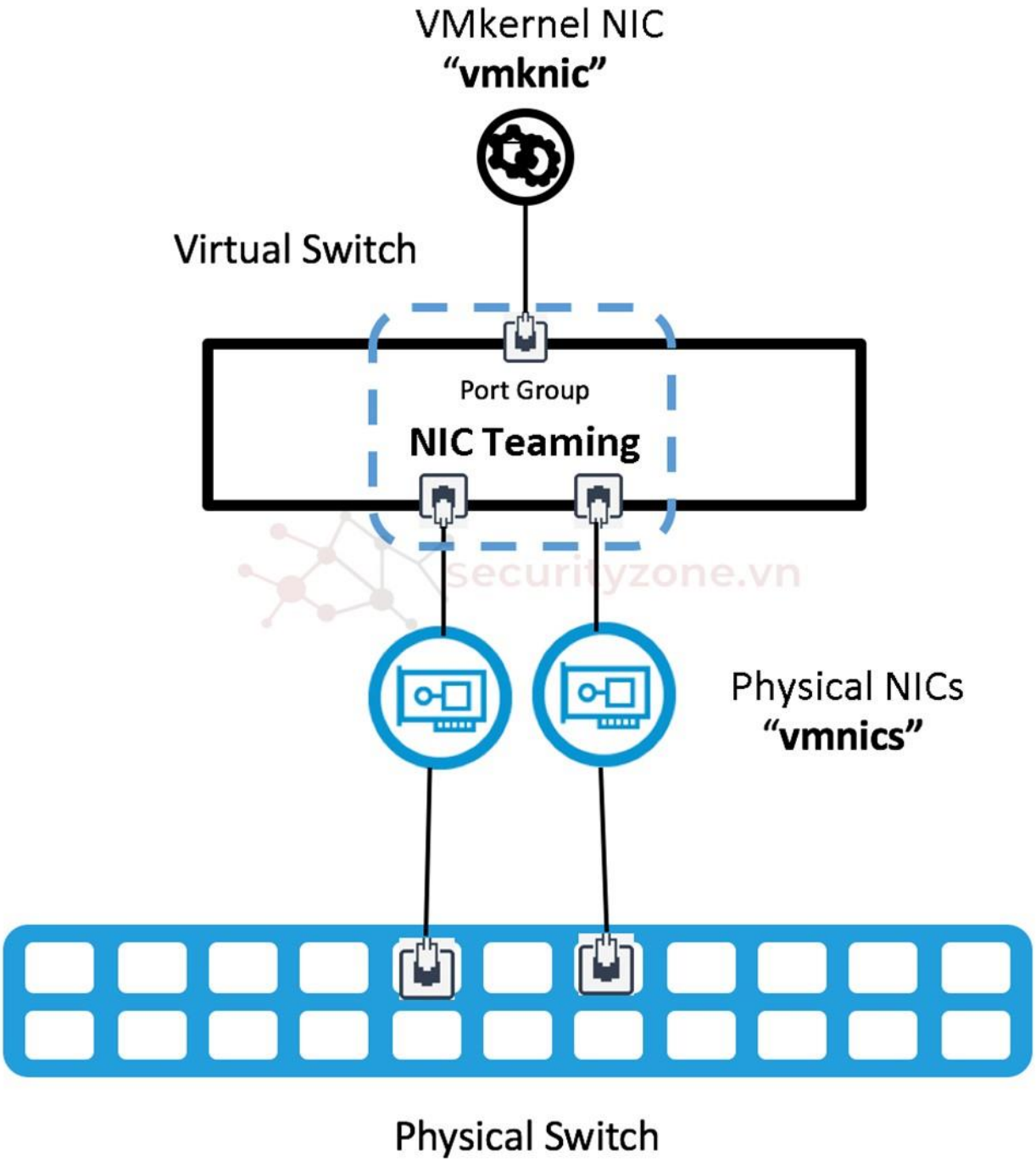
Khi bạn có môi trường với nhiều ESXi host và muốn quản lý mạng tập trung, hiệu quả, Distributed Port Group là lựa chọn tối ưu giúp quản lý và triển khai cấu hình mạng một cách đồng nhất.



Hình 31 Hình ảnh mô phỏng cách thêm một DPG vào Virtual Switch

IV. Physical Network Adapter (NIC Teaming)

NIC Teaming là việc kết hợp nhiều card mạng vật lý (NIC) lại với nhau để tạo một nhóm kết nối mạng có băng thông cao và dự phòng nếu có sự cố.



Hình 32 Hình ảnh mô phỏng cách hoạt động của một VMNic

Chức năng: Tăng cường băng thông mạng và cung cấp khả năng dự phòng trong trường hợp một kết nối vật lý bị lỗi.

Sử dụng NIC Teaming khi bạn cần tối ưu hóa hiệu suất mạng hoặc muốn đảm bảo hệ thống mạng luôn hoạt động liên tục ngay cả khi có sự cố về phần cứng.

Chương XI. Tìm hiểu về Vmkernel

I. Tổng quan về VMkernel

VMkernel là thành phần cốt lõi của hypervisor VMware ESXi, chịu trách nhiệm quản lý lớp ảo hóa của hệ thống máy chủ. Nó giúp ESXi quản lý và phân bổ tài nguyên vật lý, đồng thời cung cấp các dịch vụ quan trọng cho các máy ảo (VM) hoạt động trên máy chủ đó. VMkernel có các chức năng chính bao gồm quản lý tài nguyên, vận hành máy ảo, quản lý thiết bị, kết nối mạng, bảo mật và cách ly giữa các máy ảo.

1. **Quản lý tài nguyên**

VMkernel quản lý các tài nguyên phần cứng như CPU, bộ nhớ, lưu trữ và mạng, phân bổ chúng cho các máy ảo theo nhu cầu. Nó đảm bảo hiệu suất hoạt động của các VM và cung cấp tính năng tự động cân bằng tải tài nguyên khi có nhiều máy ảo cùng hoạt động trên một máy chủ vật lý.

2. **Vận hành máy ảo**

VMkernel chịu trách nhiệm quản lý toàn bộ vòng đời của máy ảo, bao gồm khởi động, tắt máy và quản lý snapshot. Điều này giúp duy trì sự ổn định và khả năng quản lý linh hoạt các hệ thống ảo hóa phức tạp.

3. Quản lý thiết bị

VMkernel cung cấp một khung làm việc để quản lý các thiết bị phần cứng và ảo, giúp kết nối các tài nguyên phần cứng với máy ảo. Các thiết bị này bao gồm cả các thiết bị mạng và lưu trữ ảo, giúp tăng cường khả năng linh hoạt và dễ dàng quản lý trong môi trường ảo hóa.

II. VMkernel Networking Layer

VMkernel Networking Layer cung cấp khả năng kết nối mạng cho các máy chủ ESXi và xử lý traffic hệ thống tiêu chuẩn như vSphere vMotion, IP Storage, Fault Tolerance và vSAN. VMkernel Networking cũng hỗ trợ cấu hình nhiều TCP/IP stack tùy theo các dịch vụ khác nhau, giúp quản lý mạng một cách hiệu quả hơn.

1. TCP/IP Stack của VMkernel

VMkernel hỗ trợ nhiều loại TCP/IP stack nhằm cô lập và tối ưu hóa traffic của các dịch vụ quan trọng:

Hình 33 Hình ảnh mô phỏng giao diện mô hình TCP/IP Stack trong Vmkernal

Default TCP/IP Stack: Hỗ trợ quản lý traffic giữa vCenter và các ESXi hosts, đồng thời cung cấp kết nối cho vMotion, IP Storage và Fault Tolerance. vMotion TCP/IP

Stack: Được thiết kế để tối ưu hóa traffic của dịch vụ vMotion, giúp tăng hiệu suất và đảm bảo tính cách ly giữa các traffic.

Provisioning TCP/IP Stack: Hỗ trợ traffic cho việc sao chép, di chuyển lạnh máy ảo và clone snapshot.

Custom TCP/IP Stacks: Quản trị viên có thể cấu hình các TCP/IP stack riêng để quản lý traffic cho các ứng dụng tùy chỉnh.

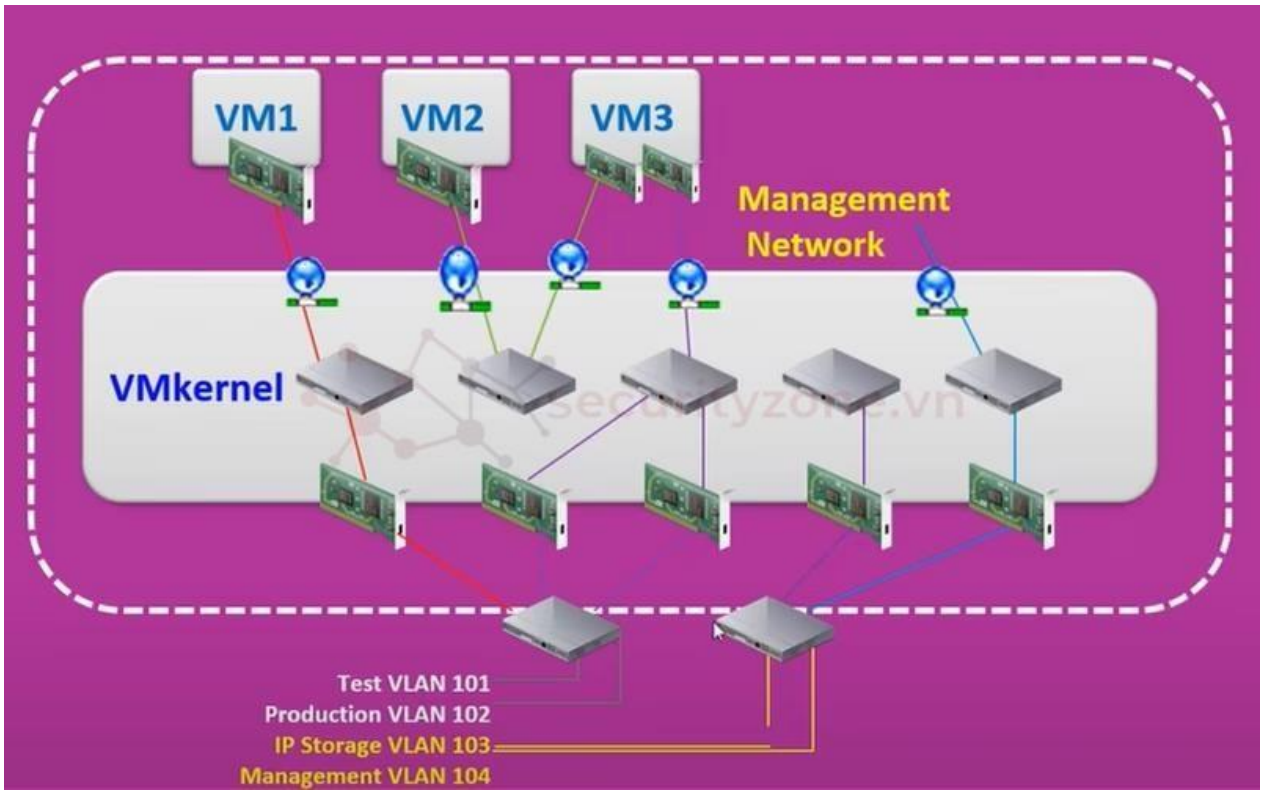
2. Các loại traffic hệ thống

Trong môi trường vSphere, mỗi loại traffic hệ thống yêu cầu một adapter VMkernel riêng để đảm bảo tính ổn định và bảo mật. Các loại traffic chính bao gồm:

- **Management Traffic**: Traffic quản lý giữa ESXi host và vCenter, sử dụng VMkernel adapter để đảm bảo quản lý liên tục và duy trì sự liên lạc giữa các hosts và dịch vụ quản lý trong hệ thống VMware.
- **vMotion Traffic**: Traffic này xử lý việc di chuyển nóng máy ảo giữa các ESXi hosts mà không cần phải tắt máy ảo. Để tối ưu hóa hiệu suất, quản trị viên có thể sử dụng Multi-NIC vMotion, nơi nhiều adapter vật lý được sử dụng để tăng băng thông cho quá trình di chuyển máy ảo.
- **Fault Tolerance Traffic**: Đảm bảo tính năng phân lớp lỗi cho các máy ảo có cấu hình Fault Tolerance, truyền dữ liệu từ máy ảo chính đến máy ảo thứ cấp, giúp duy trì tính toàn vẹn và liên tục cho các ứng dụng quan trọng.
- **IP Storage Traffic**: Traffic kết nối với các dịch vụ lưu trữ như iSCSI, NFS qua mạng TCP/IP. Quản trị viên có thể cấu hình iSCSI multipathing nếu có nhiều NIC vật lý, giúp tăng cường hiệu suất và tính ổn định cho kết nối lưu trữ.

- **vSAN Traffic**: Điều khiển traffic giữa các host trong một cụm vSAN, xử lý các hoạt động đồng bộ hóa và quản lý dữ liệu trong vSAN cluster.

  Replication Traffic: Traffic dành riêng cho vSphere Replication, bao gồm cả traffic ra và vào giữa các nguồn và đích replication.



Hình 34 Hình ảnh mô phỏng traffic của hệ thống

3. Định tuyến và Multihoming trong VMkernel

Định tuyến trong VMkernel:

VMkernel hỗ trợ việc định tuyến traffic qua các subnet khác nhau trong môi trường vSphere. Đây là một tính năng quan trọng để đảm bảo rằng các traffic quan trọng như

quản lý, vMotion, và storage có thể đi qua các mạng khác nhau một cách chính xác và hiệu quả.

a. Static Routing

VMkernel cho phép cấu hình các tuyến tĩnh để điều khiển đường đi của traffic qua các mạng cụ thể. Điều này đặc biệt hữu ích trong các môi trường đơn giản hoặc khi cần định tuyến các loại traffic cụ thể qua các đường dẫn được chỉ định.

b. Dynamic Routing (Optional)

Trong các môi trường phức tạp hơn, quản trị viên có thể tích hợp VMkernel với các giao thức định tuyến động thông qua việc sử

dụng các thành phần bổ sung như NSX. Điều này giúp tối ưu hóa việc định tuyến traffic và cải thiện tính linh hoạt của mạng.

c. Policy-Based Routing

VMkernel có thể hỗ trợ định tuyến dựa trên chính sách, cho phép quản trị viên định tuyến traffic dựa trên các tiêu chí như loại traffic, nguồn và đích, thay vì chỉ dựa trên địa chỉ IP.

Multihoming trong VMkernel:

Multihoming là khả năng của VMkernel để hỗ trợ nhiều adapter VMkernel, mỗi adapter có thể được cấu hình với một TCP/IP stack khác nhau hoặc nằm trong các subnet khác nhau. Tính năng này cung cấp sự linh hoạt trong việc quản lý mạng, nhưng cũng đòi hỏi sự cấu hình cẩn thận.

a. Lợi ích của Multihoming

- **Tăng cường Tính Sẵn Sàng**: Bằng cách sử dụng nhiều adapter VMkernel, hệ thống có thể đảm bảo tính liên tục của các dịch vụ quan trọng ngay cả khi một adapter hoặc đường truyền gặp sự cố. o **Cân Bằng Tải**: Multihoming cho phép phân phối traffic giữa nhiều adapter, giúp cân bằng tải và tối ưu hóa băng thông.

b. Thách thức của Multihoming

- **Routing Loops**: Sử dụng nhiều adapter trong cùng một subnet có thể dẫn đến các vòng lặp định tuyến, làm suy giảm hiệu suất mạng.
- **Kết Nối Không Ổn Định**: Nếu không cấu hình cẩn thận, multihoming có thể gây ra các vấn đề như kết nối không ổn định hoặc định tuyến không đối xứng, làm giảm hiệu suất hệ thống.

c. Best Practices

- Đảm bảo rằng mỗi adapter VMkernel được cấu hình đúng với subnet riêng biệt.

o Tránh sử dụng nhiều adapter trong cùng một subnet trừ khi cần thiết và có cấu hình định tuyến cụ thể. o Sử dụng các công cụ giám sát và phân tích mạng để đảm bảo rằng việc cấu hình multihoming không gây ra các vấn đề hiệu suất.

Chương XII. Tìm hiểu về VLANs, Virtual Switch Tagging và Trafic Follow trong Sphere Networking

I. Tổng quan lý thuyết

Trong môi trường vSphere Networking, mục tiêu chính là quản lý mạng ảo một cách hiệu quả, bảo đảm tính linh hoạt, khả năng mở rộng và bảo mật. Ba khái niệm chính cần tìm hiểu sâu hơn là:

- VLANs – Giúp chia nhỏ mạng thành các phân đoạn logic để tối ưu hóa lưu lượng và bảo mật.
- Virtual Switch Tagging (VST) – Cơ chế quản lý việc phân loại lưu lượng của các VLAN ở cấp độ virtual switch.
- Traffic Flow – Cách mà dữ liệu di chuyển qua lại giữa các máy ảo, host và mạng vật lý.

II. VLANs trong vSphere Networking

1. Khái niệm cơ bản:

VLAN (Virtual Local Area Network) cho phép chia nhỏ một mạng vật lý thành nhiều mạng logic. Điều này giúp cách ly lưu lượng, bảo mật tốt hơn và tối ưu hóa sử dụng tài nguyên mạng. Trong VMware vSphere, mỗi VLAN được gán một VLAN ID (từ 0 đến 4095) để xác định và phân biệt các lưu lượng khác nhau.

2. Vai trò trong vSphere:

- **Phân đoạn lưu lượng:** Giả sử bạn có nhiều máy ảo (VMs) trên cùng một host ESXi, bạn có thể sử dụng VLANs để cô lập lưu lượng giữa các máy ảo này. Điều này ngăn không cho lưu lượng từ một VLAN có thể truy cập các tài nguyên trên VLAN khác.
- **Tăng cường bảo mật:** Với VLANs, chỉ những máy ảo hoặc hệ thống thuộc cùng một VLAN mới có thể giao tiếp với nhau. Điều này giúp ngăn ngừa các tấn công lateral trong nội bộ mạng.
- **Giảm chi phí hạ tầng:** VLANs giúp tạo ra nhiều mạng logic mà không cần bổ sung switch vật lý mới.

Private VLANs (PVLANs): Private VLANs là một biến thể mở rộng của VLANs, cho phép cô lập các máy ảo ngay cả trong cùng một VLAN. Điều này giúp tăng cường bảo mật bằng cách hạn chế việc máy ảo này truy cập được vào máy ảo khác trong cùng một VLAN, nhưng vẫn có thể giao tiếp với hệ thống ngoài VLAN.

3. Loại Private VLANs:

- **Primary VLAN:** VLAN chính, nơi chứa các máy ảo.
- **Isolated VLAN:** Cách ly hoàn toàn lưu lượng giữa các máy ảo.
- **Community VLAN:** Các máy ảo có thể giao tiếp với nhau trong cùng một community VLAN nhưng không thể giao tiếp với các VLAN khác.

VLAN Trunking: Cho phép truyền nhiều VLAN cùng trên một đường truyền vật lý. Trong vSphere, khi máy chủ ESXi kết nối với switch vật lý, cổng kết nối sẽ được cấu hình ở chế độ trunk, cho phép chuyển tiếp lưu lượng của nhiều VLAN.

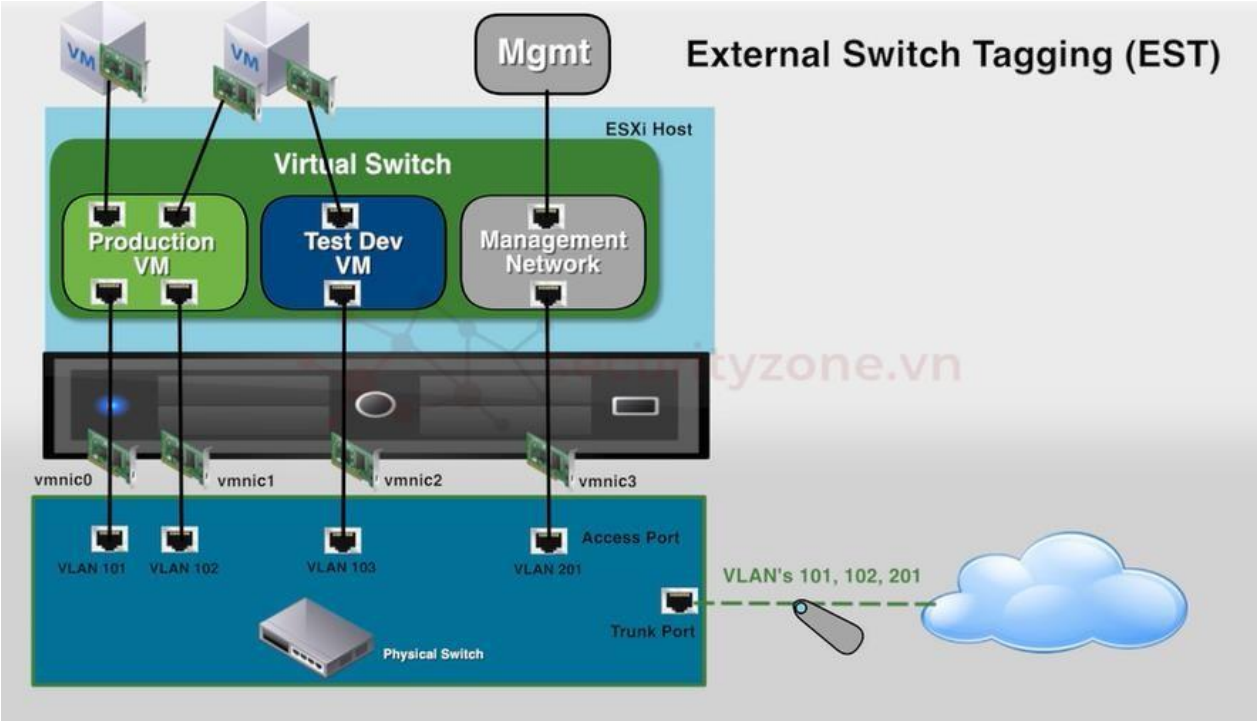
III. Virtual Switch Tagging (VST)

VLAN Tagging là quá trình gắn nhãn (tag) vào mỗi packet dữ liệu để chỉ định VLAN mà packet thuộc về. Khi dữ liệu di chuyển qua mạng có hỗ trợ nhiều VLAN, tag này giúp switch vật lý hoặc virtual switch nhận diện packet thuộc về VLAN nào.

Chế độ gắn thẻ	ID VLAN trên các nhóm cổng chuyển mạch	Sự miêu tả
EST	0	Bộ chuyển mạch vật lý thực hiện gắn thẻ VLAN. Bộ điều hợp mạng máy chủ được kết nối với các cổng truy cập trên bộ chuyển mạch vật lý.
VST	Giữa 1 và 4094	Bộ chuyển mạch ảo thực hiện gắn thẻ VLAN trước khi các gói tin rời khỏi máy chủ. Bộ điều hợp mạng máy chủ phải được kết nối với các cổng trunk trên bộ chuyển mạch vật lý.
VGT	▪ 4095 cho công tắc tiêu chuẩn ▪ Phạm vi và VLAN riêng lẻ cho chuyển mạch phân tán	Máy ảo thực hiện gắn thẻ VLAN. Bộ chuyển mạch ảo bảo toàn các thẻ VLAN khi chuyển tiếp các gói tin giữa ngăn xếp mạng máy ảo và bộ chuyển mạch bên ngoài. Bộ điều hợp mạng máy chủ phải được kết nối với các cổng trunk trên bộ chuyển mạch vật lý. vSphere Distributed Switch hỗ trợ sửa đổi VGT. Vì lý do bảo mật, bạn có thể cấu hình một bộ chuyển mạch phân tán để chỉ truyền các gói tin thuộc về các VLAN cụ thể. Ghi chú: Đối với VGT, bạn phải cài đặt trình điều khiển đường trục VLAN 802.1Q trên hệ điều hành khách của máy ảo.

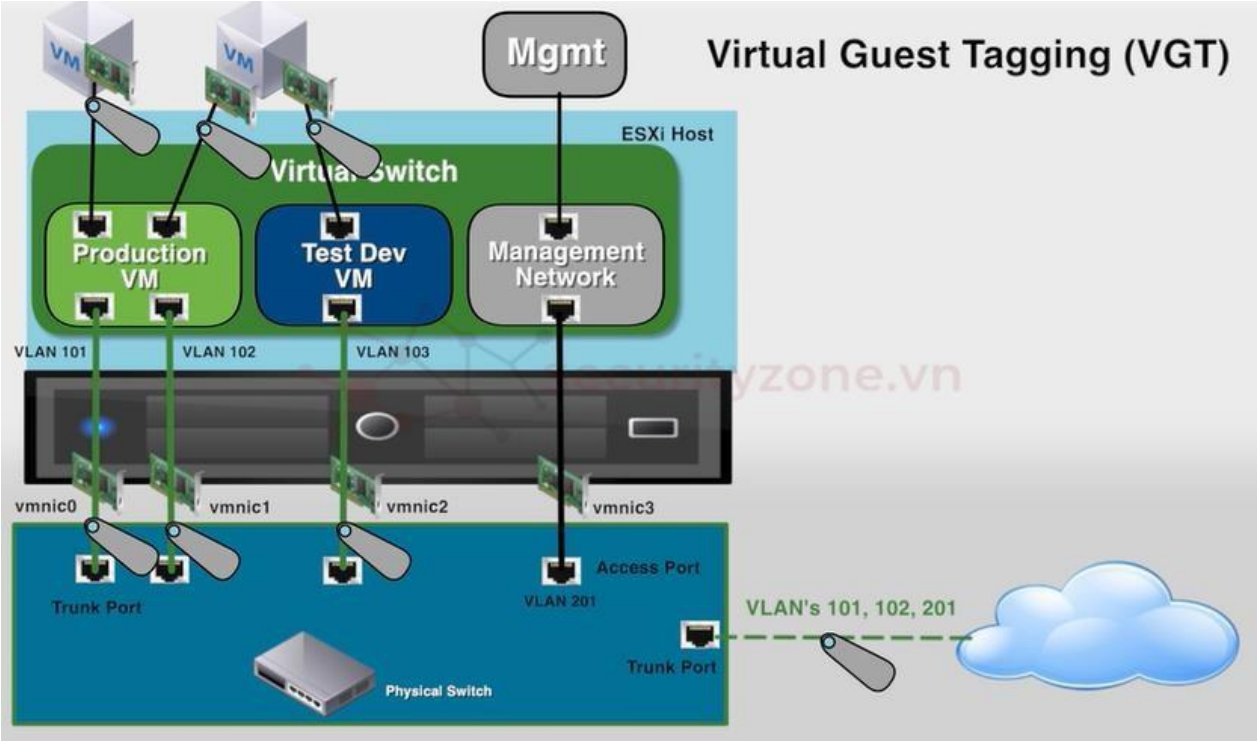
Hình 35 Hình ảnh mô phỏng chức năng VST gồm EST VST và VGT

1. **Các phương pháp Tagging:**
   - **External Switch Tagging (EST):** Việc tagging được thực hiện tại switch vật lý. vSwitch trong vSphere chỉ đơn giản là chuyển tiếp dữ liệu mà không can thiệp vào quá trình tagging. EST ít phổ biến trong môi trường vSphere.



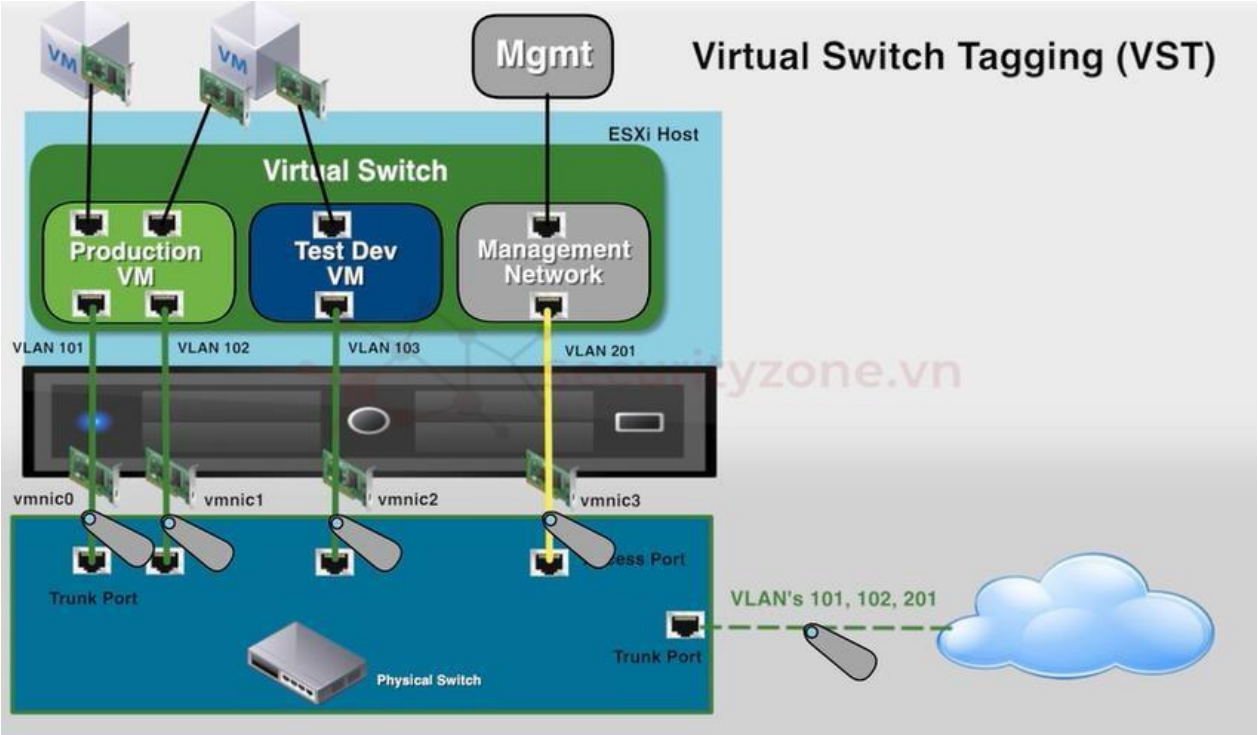
Hình 36 Hình ảnh mô phỏng chức năng EST

- **Virtual Switch Tagging (VST):** VST là phương pháp phổ biến nhất trong môi trường vSphere. Trong VST, virtual switch chịu trách nhiệm thêm và quản lý các VLAN tag. Khi dữ liệu di chuyển từ máy ảo ra ngoài mạng vật lý, virtual switch sẽ thêm tag trước khi gửi ra ngoài. Khi dữ liệu được chuyển lại vào máy ảo, virtual switch sẽ gỡ bỏ tag, vì máy ảo không cần biết về VLAN.



Hình 37 Hình ảnh mô phỏng chức năng VGT

- **Virtual Guest Tagging (VGT):** Đây là mô hình mà chính các máy ảo thực hiện tagging. Mô hình này chỉ áp dụng khi VM được yêu cầu quản lý nhiều VLAN. Tuy nhiên, nó phức tạp và ít được sử dụng so với VST.



Hình 38 Hình ảnh mô phỏng chức năng VST

2. **Hoạt động của VST:**
   - **Gắn Tag:** Khi một máy ảo gửi dữ liệu ra ngoài, virtual switch sẽ nhận biết VLAN ID của port group mà máy ảo kết nối.
   - **Thêm VLAN Tag:** Virtual switch thêm tag VLAN vào packet dữ liệu dựa trên VLAN ID của port group.
   - **Chuyển dữ liệu:** Dữ liệu đã được tag sẽ đi qua cổng uplink của ESXi, kết nối tới switch vật lý, và truyền đi qua mạng.
   - **Gỡ bỏ Tag:** Khi dữ liệu quay lại ESXi, virtual switch sẽ gỡ bỏ tag trước khi chuyển đến máy ảo.

Ưu điểm của VST:

- **Tập trung hóa quản lý:** VST tập trung việc quản lý VLAN ở cấp độ virtual switch, giúp giảm thiểu sự phức tạp và nguy cơ cấu hình sai tại máy ảo.

- **Hiệu suất:** Giảm tải cho switch vật lý khi phải xử lý tag VLAN, do công việc này đã được xử lý ở cấp độ virtual switch.

IV. Traffic Flow trong vSphere Networking

1. **Traffic Flow nội bộ (Internal Traffic Flow):**

Lưu lượng giữa các máy ảo trong cùng một VLAN trên cùng một host ESXi không cần phải đi qua mạng vật lý. Dữ liệu chỉ di chuyển qua lại giữa các máy ảo thông qua virtual switch, giúp tối ưu hóa hiệu suất và giảm tải cho hạ tầng vật lý.

2. **Traffic Flow giữa các VLAN (Inter-VLAN Traffic Flow):**

Khi lưu lượng di chuyển giữa các máy ảo thuộc các VLAN khác nhau, dữ liệu phải đi qua Layer 3 switch hoặc router để định tuyến lưu lượng. Đây là lúc tính năng routing giữa các VLAN được kích hoạt.

3. **Traffic Flow giữa các host ESXi:**

Nếu hai máy ảo thuộc cùng một VLAN nhưng nằm trên hai host ESXi khác nhau, lưu lượng sẽ được chuyển qua cổng uplink NIC của mỗi host. Điều này có nghĩa là lưu lượng sẽ di chuyển từ virtual switch của host này qua switch vật lý trước khi đến virtual switch của host khác.

4. **Cân bằng tải (Load Balancing):**

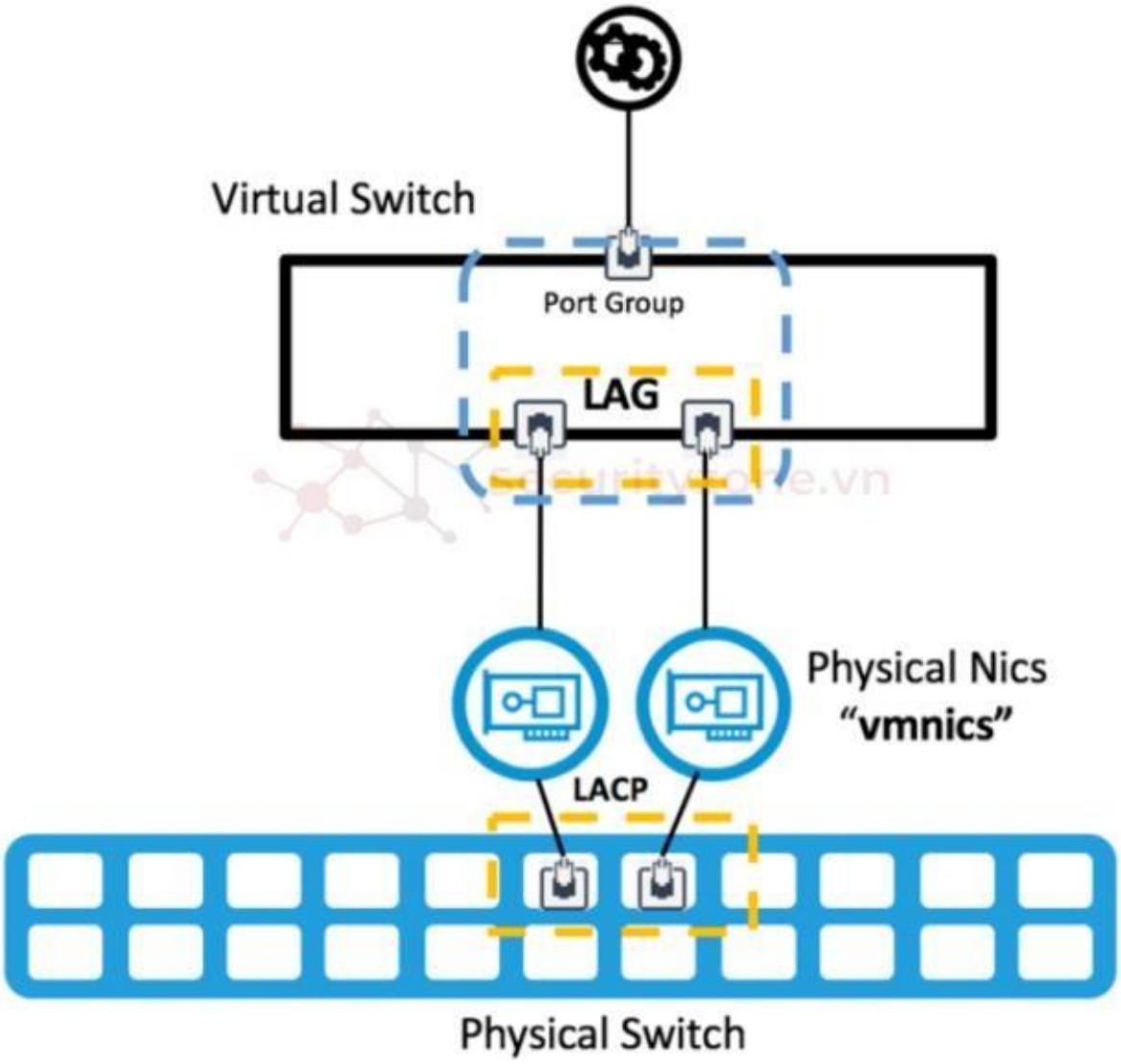
Distributed Switch (vDS) hỗ trợ tính năng load balancing giữa các uplink NICs, giúp phân phối đều lưu lượng qua nhiều NIC, tối ưu hóa hiệu suất và tránh tình trạng quá tải một uplink cụ thể. Điều này rất quan trọng trong các hệ thống lớn với nhiều máy ảo và yêu cầu lưu lượng lớn. **Traffic Shaping:**

Traffic Shaping là tính năng cho phép kiểm soát băng thông cho các port group trong virtual switch. Điều này giúp quản trị viên giới hạn và quản lý băng thông sử dụng, ngăn ngừa việc một máy ảo tiêu thụ toàn bộ băng thông của hệ thống, gây ảnh hưởng đến hiệu suất của các máy ảo khác.

Chương XIII. Tìm hiểu về LACP trên vDS

I.Giới thiệu về LACP

- LACP là một phần của tiêu chuẩn IEEE 802.3ad cho phép nhiều NIC vật lý hoạt động như một NIC ảo duy nhất.
- Nó giúp cân bằng tải trên nhiều đường truyền và tạo tính dự phòng.
- Khi sử dụng LACP, các ESXi hosts có thể tạo ra một nhóm nhiều uplinks để kết nối tới mạng vật lý với hiệu suất và độ ổn định cao hơn.



Hình 39 Hình ảnh mô phỏng chức năng của LACP

II. LACP trên vDS

1. Cách LACP hoạt động trên vDS

- Trên vSphere Distributed Switch (vDS), LACP được sử dụng để kết hợp nhiều uplinks từ các host khác nhau.
- vDS hỗ trợ LACP để cho phép cấu hình một **Link Aggregation Group (LAG)**.

  Mỗi LAG có thể chứa một hoặc nhiều uplinks từ các host ESXi.

- LACP xác định và điều phối các kết nối giữa các host ESXi và các switch vật lý hỗ trợ LACP, giúp tối ưu hóa luồng dữ liệu.

2. Các chế độ hoạt động của LACP

- **Active Mode**: ESXi host sẽ gửi yêu cầu LACP tới switch vật lý để thiết lập một LAG.
- **Passive Mode**: ESXi host sẽ chờ đợi yêu cầu từ switch vật lý để thiết lập kết nối.
- Trong hầu hết các trường hợp, **Active Mode** được sử dụng để ESXi chủ động gửi và nhận lưu lượng LACP.

Option	Description
Active	All LAG ports are in an Active negotiating mode. The LAG ports initiate negotiations with the LACP port channel on the physical switch by sending LACP packets.
Passive	The LAG ports are in Passive negotiating mode. The LAG ports respond to LACP packets they receive but do not initiate LACP negotiation.

Hình 40 Hình ảnh thể hiện cách hoạt động của một LACP

3. Ưu điểm - Nhược điểm và Giới hạn của LACP

Ưu điểm của việc sử dụng LACP

- Tăng băng thông: Kết hợp nhiều đường truyền thành một giúp tăng băng thông tổng thể.
- Tính dự phòng cao: Nếu một uplink bị lỗi, các uplinks khác trong nhóm LAG vẫn có thể hoạt động.
- Cân bằng tải: LACP tự động phân phối lưu lượng giữa các uplinks để tối ưu hóa băng thông sử dụng.

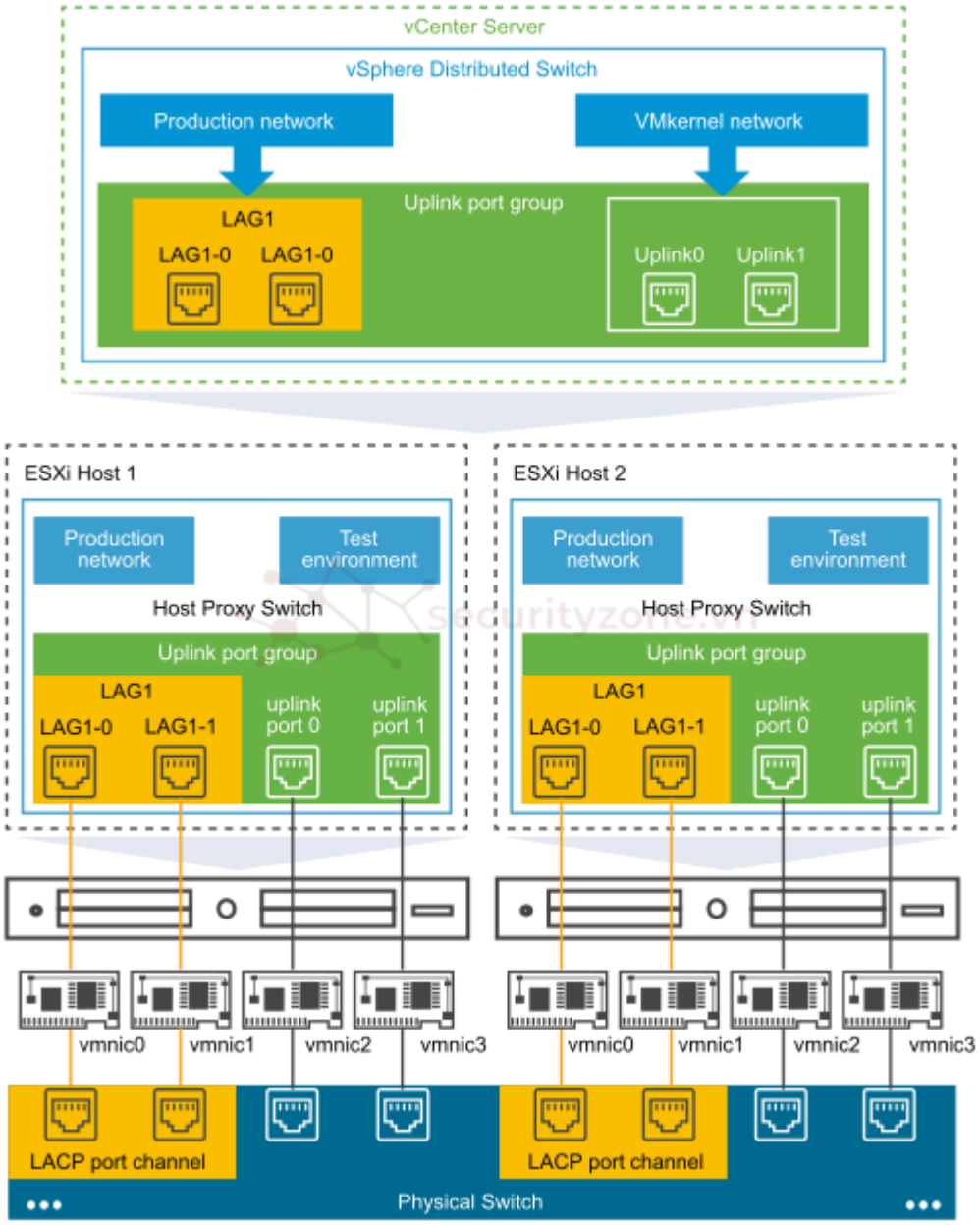
Nhược điểm và giới hạn

- Yêu cầu switch vật lý hỗ trợ LACP: Để sử dụng LACP, switch vật lý cũng phải hỗ trợ giao thức này.
- Cấu hình phức tạp hơn: Cần phải cấu hình đúng trên cả vSphere Distributed Switch và switch vật lý để đảm bảo tính tương thích.

4. Yêu cầu và Lưu ý khi triển khai LACP trên vDS

Yêu cầu trước khi triển khai

- Thiết bị mạng hỗ trợ LACP: Switch vật lý phải hỗ trợ và được cấu hình LACP.
- Card mạng tương thích: Các NIC trên ESXi host cần hỗ trợ teaming và LACP.
- Phiên bản vDS: Đảm bảo rằng phiên bản vDS đang sử dụng hỗ trợ LACP (thường là phiên bản mới nhất).



Hình 41 Hình ảnh mô phỏng cách triển khai LACP trên vDS và hình trên thể hiện 2 ESXI host hoạt động khi kết nối đến 1 vCenter

Lưu ý khi triển khai

- **Tương thích thiết bị**: Đảm bảo rằng cả switch vật lý và ESXi host đều hỗ trợ LACP và được cấu hình đúng cách.
- **Cấu hình đồng nhất**: Cấu hình LACP phải được thực hiện đồng nhất trên cả switch vật lý và vDS để tránh các lỗi kết nối.
- **Giám sát liên tục**: Theo dõi trạng thái của các liên kết để phát hiện và khắc phục sự cố kịp thời.
- **Số lượng uplinks**: Không nên gộp quá nhiều uplinks vào một nhóm LACP để tránh tăng độ phức tạp và khó quản lý.

Chương XIV. Tìm hiểu về Virtual Machine Hardware Deep Dive

I. Giới thiệu

Khi làm việc với các hệ thống ảo hóa, máy ảo (Virtual Machine - VM) đóng vai trò cực kỳ quan trọng trong việc mô phỏng phần cứng của một máy tính thực tế. Một máy ảo cung cấp một môi trường ảo nơi có thể chạy các hệ điều hành và phần mềm như trên một máy vật lý. Để hiểu rõ hơn về cách thức hoạt động của máy ảo, chúng ta sẽ đi sâu vào các thành phần phần cứng ảo của máy ảo, từ các tập tin cấu thành máy ảo, so sánh các phiên bản phần cứng của máy ảo, đến việc điều hướng và kiểm tra các cài đặt trong vSphere Client.

Bài viết này sẽ giúp bạn nắm vững kiến thức cơ bản về phần cứng máy ảo, các phương pháp để tương tác và kiểm tra chúng trên nền tảng vSphere, cũng như cách truy cập vào bảng điều khiển của máy ảo.

II.Nội dung chi tiết

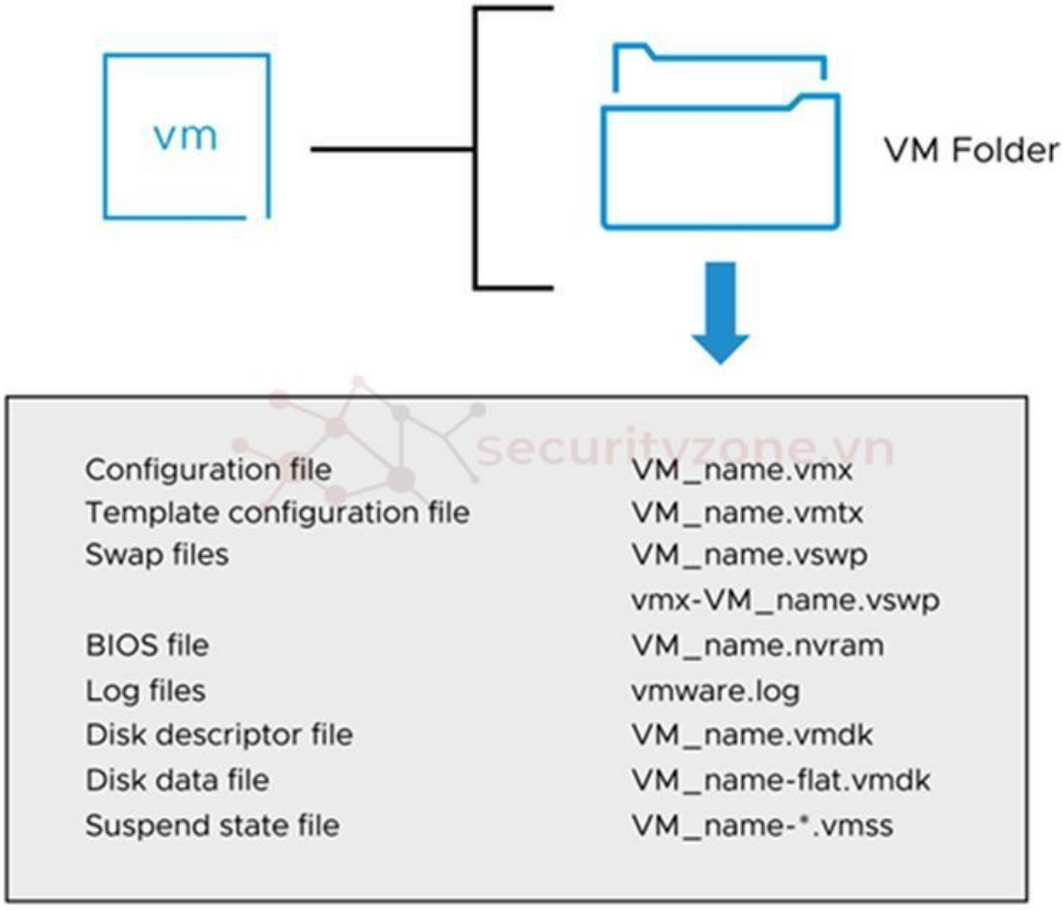
1. Về các tệp Máy Ảo (Virtual Machine Files)

Khi tạo ra một máy ảo, VMware sẽ tạo ra một loạt các tập tin khác nhau để lưu trữ trạng thái và thông tin cấu hình của máy ảo đó. Dưới đây là một số tệp phổ biến:

- Tập tin (.vmx): Đây là tập tin cấu hình chính của máy ảo. Nó chứa tất cả các thông tin về tài nguyên và cấu hình phần cứng ảo của máy ảo (CPU, RAM, ổ đĩa,...).
- **Tệp mẫu VM (.vmtx)**: Thay thế tệp .vmx khi VM được chuyển thành template.
- **Tệp swap (.vswp)**: Được sử dụng để quản lý bộ nhớ khi có tình trạng thiếu tài nguyên.
- **Tệp BIOS hoặc cài đặt EFI (.nvram)**: Chứa cấu hình BIOS hoặc EFI của VM.
- **Tệp nhật ký (.log)**: Lưu lại các bản ghi hoạt động của VM.

  Ngoài ra, mỗi VM còn có các tệp đĩa ảo như:

  - VM_name.vmdk(Đây là tập tin chứa dữ liệu ổ đĩa cứng ảo của máy ảo. Tập tin này mô phỏng ổ đĩa vật lý, và trong đó sẽ có dữ liệu mà máy ảo sử dụng) và VM_name-flat.vmdk cho đĩa ảo đầu tiên. o Nếu có nhiều đĩa ảo, tệp sẽ có dạng VM_name_#.vmdk và VM_name_#flat.vmdk.



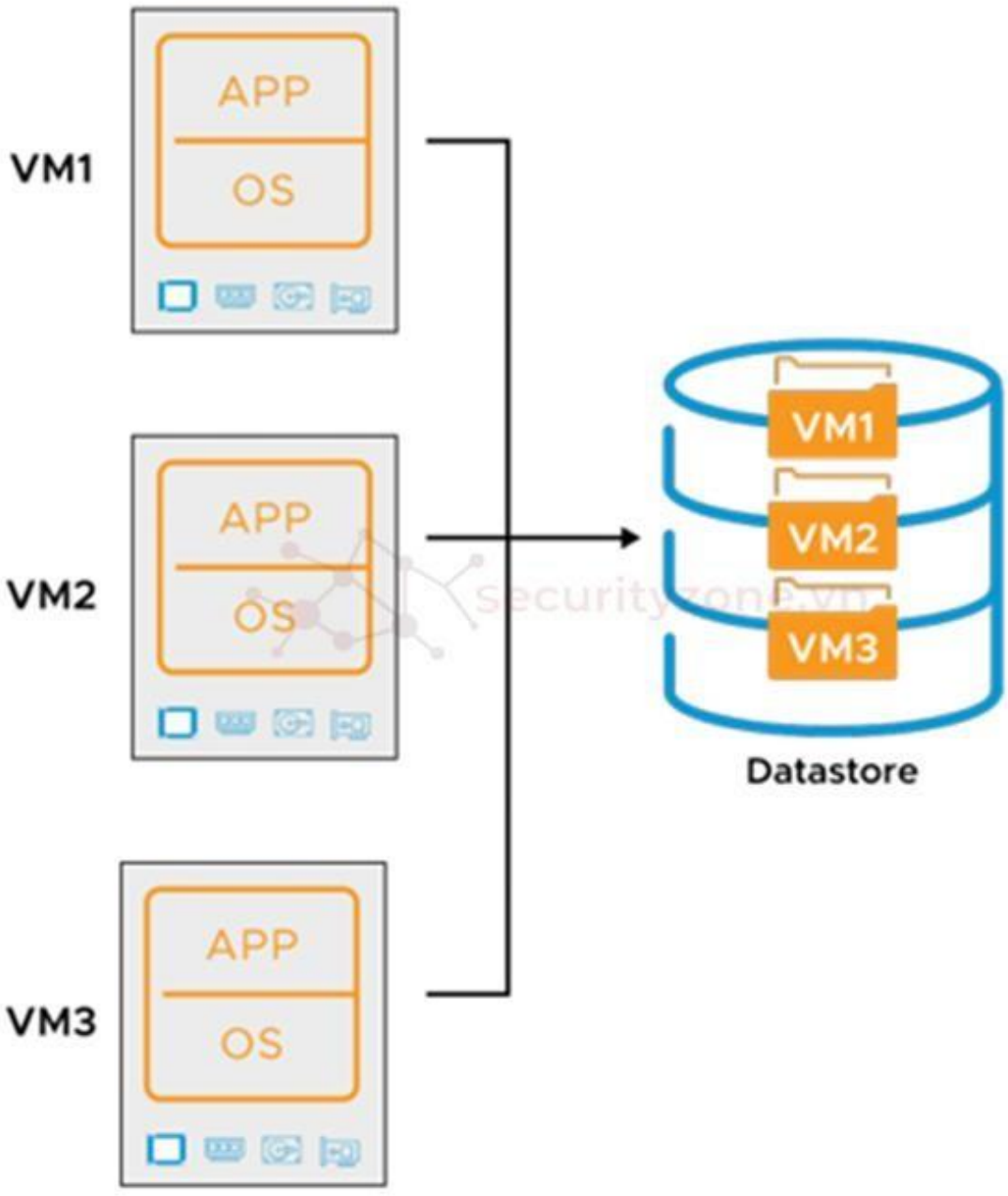
Hình 42 Hình ảnh giải thích cách tệp của một VM

Bao gói Máy Ảo (Virtual Machine Encapsulation)

Mỗi máy ảo (VM) được lưu trữ dưới dạng tập hợp các tệp hoặc đối tượng:

- Các tệp trong một thư mục trên datastore VMFS hoặc NFS
- Các đối tượng trên datastore vSAN hoặc vSphere Virtual Volumes

Mỗi đĩa ảo được bao gói thành một tệp hoặc đối tượng duy nhất. vSphere bao gói mỗi VM thành một vài tệp hoặc đối tượng, giúp quản lý và di chuyển VM dễ dàng hơn. Các tệp và đối tượng của mỗi VM được lưu trữ trong một thư mục riêng trên datastore.



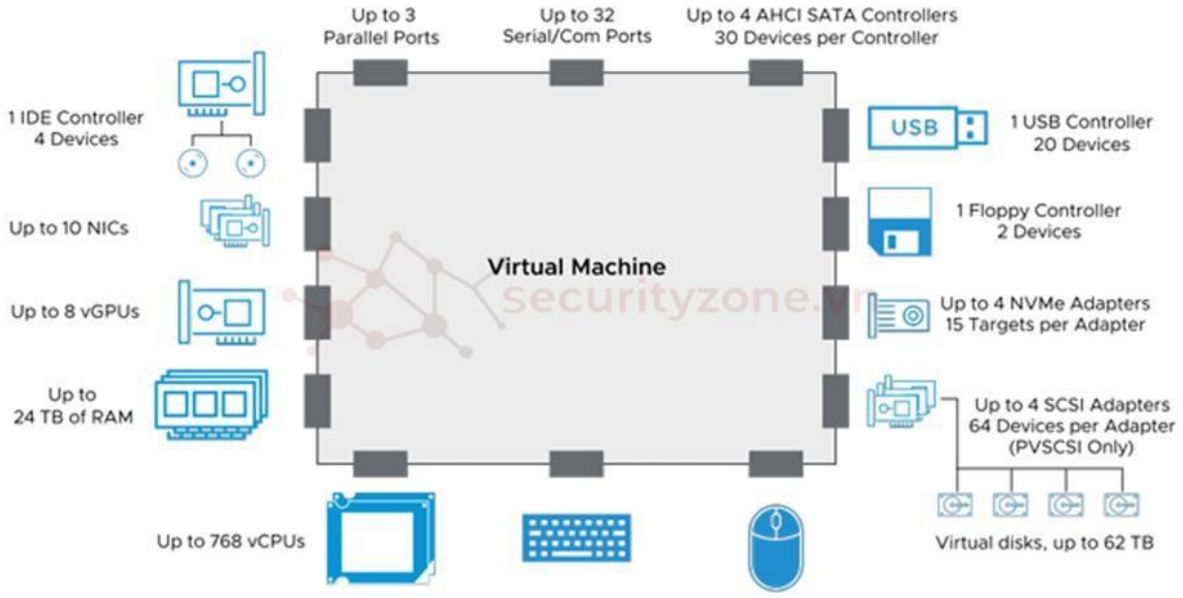
Hình 43 Hình ảnh mô phỏng cách thức file hoạt động từ VM lưu trữ ở Datastore

2. Về Phần Cứng Ảo (Virtual Hardware)

Hệ điều hành khách (Guest OS) truy cập các thiết bị phần cứng nhưng không nhận ra rằng chúng là ảo. Phần cứng ảo làm cho VM có thể di chuyển qua nhiều nền tảng VMware khác nhau.

Bạn có thể cấu hình bộ nhớ, CPU, thêm đĩa cứng ảo, NICs, và các thiết bị phần cứng ảo khác như CD/DVD, SCSI. Không phải tất cả các thiết bị đều có thể thêm vào hoặc cấu hình. Một số thiết bị như USB chỉ có thể sử dụng bởi một VM duy nhất tại một thời điểm. Một máy ảo có các thành phần phần cứng ảo mô phỏng tương tự các thành phần của một máy tính vật lý. Các thành phần này có thể được cấu hình và điều chỉnh tùy theo yêu cầu của bạn:

- **CPU ảo (vCPU)**: Là phiên bản ảo của bộ vi xử lý vật lý. Bạn có thể phân bổ số lượng vCPU tùy thuộc vào yêu cầu xử lý của ứng dụng chạy trên máy ảo.
- **RAM ảo**: Là bộ nhớ ảo mà máy ảo có thể sử dụng. Việc phân bổ RAM ảo phù hợp sẽ đảm bảo hiệu suất của máy ảo.
- **Ổ đĩa cứng ảo (vDisk)**: Ổ đĩa ảo lưu trữ hệ điều hành và dữ liệu cho máy ảo.
- **Card mạng ảo (vNIC)**: Được sử dụng để kết nối máy ảo với mạng. Bạn có thể thêm hoặc gỡ bỏ card mạng ảo tùy theo yêu cầu.
- **Thiết bị ảo khác**: Bao gồm các thiết bị như CD/DVD ảo, bộ điều khiển USB, và nhiều thành phần khác có thể được thêm vào máy ảo.



Hình 44 Hình ảnh mô phỏng phần mềm ảo hóa hỗ trợ mở rộng phần cứng

Phiên bản Phần Cứng Ảo (Virtual Hardware Versions)

Phiên bản phần cứng ảo (VM compatibility level) xác định các chức năng mà hệ điều hành khách có thể hỗ trợ. Bạn nên sử dụng phiên bản phần cứng tương thích với phiên bản ESXi của hệ thống.

So sánh các phiên bản phần cứng máy ảo

VMware cung cấp nhiều phiên bản phần cứng cho máy ảo, và mỗi phiên bản lại cung cấp các tính năng và cải tiến mới. Khi bạn nâng cấp hoặc tạo máy ảo mới, việc chọn phiên bản phần cứng phù hợp là rất quan trọng.

Dưới đây là một số phiên bản phần cứng máy ảo phổ biến:

- **Phiên bản 14**: Đây là phiên bản đi kèm với vSphere 6.7, hỗ trợ các cải tiến về bảo mật và tăng cường khả năng quản lý. Phiên bản này cũng hỗ trợ các thiết bị ảo mới như vTPM (Trusted Platform Module).
- **Phiên bản 20**: Được giới thiệu trong vSphere 8, cung cấp nhiều cải tiến về quản lý bộ nhớ, bảo mật, và hỗ trợ thiết bị ảo mới nhất.

- Một số phiên bản khác như: 19 - ESXi 7.0 U2 and later; 18 - ESXi 7.0 U1 and later; 17 - ESXi 7.0 and later; 15- ESXi 6.7 U2 and later…

3. Về CPU và Bộ Nhớ (About CPU and Memory)

Bạn có thể thêm, thay đổi, hoặc cấu hình tài nguyên CPU và bộ nhớ để cải thiện hiệu suất VM. Số lượng vCPU tối đa có thể gán cho một VM phụ thuộc vào số lượng CPU logic của máy chủ và loại hệ điều hành khách.

- Với ESXi 8.0, một VM có thể có tới 768 vCPU.
- Kích thước bộ nhớ tối đa của một VM với ESXi 8.0 là 24 TB.

Giới Hạn Tính Toán (Compute Maximums) là các giới hạn tối đa của phần cứng và cấu hình mà VMware vSphere hỗ trợ cho các tài nguyên tính toán như CPU, bộ nhớ, và lưu trữ trong môi trường ảo hóa. Các thông số này xác định mức tối đa mà một hệ thống vSphere có thể sử dụng hoặc quản lý trong một phiên bản cụ thể, bao gồm số lượng vCPU, bộ nhớ tối đa, số lượng máy ảo trên mỗi host, và các cấu hình phần cứng khác.

Các Compute Maximum thường được công bố bởi VMware cho mỗi phiên bản vSphere, giúp các quản trị viên hạ tầng hiểu rõ giới hạn của hệ thống để cấu hình và triển khai các dịch vụ ảo hóa một cách hiệu quả.

4. Tầm Quan Trọng của Compute Maximum:

- **Quản lý tài nguyên**: Giúp đảm bảo rằng hệ thống được cấu hình và sử dụng tài nguyên một cách hợp lý, không vượt quá giới hạn phần cứng của hạ tầng.
- **Tối ưu hóa hiệu suất**: Giới hạn compute maximum giúp đảm bảo hiệu suất của môi trường ảo hóa được duy trì, tránh tình trạng quá tải.

- **Lập kế hoạch mở rộng**: Cho phép các quản trị viên tính toán chính xác khi mở rộng hệ thống hoặc triển khai thêm máy ảo.

Một ví dụ về các giới hạn tính toán cho vSphere 8:

- Số vCPU tối đa trên mỗi VM: 768
- Bộ nhớ tối đa trên mỗi VM: 24 TB
- CPU tối đa trên mỗi host: 896
- Bộ nhớ tối đa trên mỗi host: 24 TB
- Số lượng host trên mỗi cluster: 96

5. **Về Lưu Trữ Ảo (About Virtual Storage)**

Đĩa ảo được kết nối với các bộ điều hợp lưu trữ ảo. ESXi cung cấp nhiều tùy chọn bộ điều hợp lưu trữ, bao gồm: SCSI, iSCSI, RAID, Fibre Channel, Fibre
ESXi truy cập bộ điều hợp trực tiếp thông qua trình điều khiển thiết bị trong VMkernel:

• BusLogic Parallel

• LSI Logic Parallel

• LSI Logic SAS

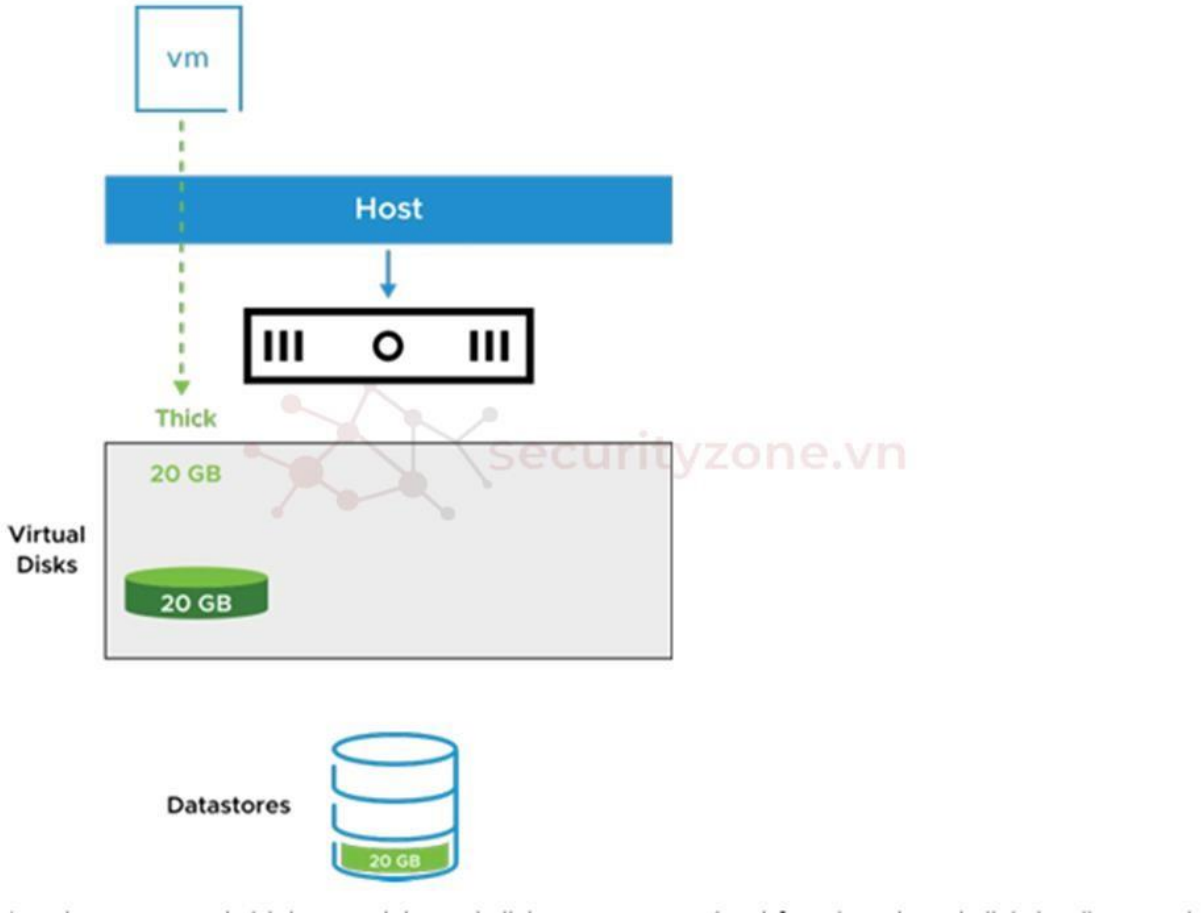
• VMware Paravirtual SCSI

• AHCI SATA controller

• NVMe ảo (Virtual NVMe)

Về Đĩa Dày (Thick-Provisioned Disks)

Sử dụng toàn bộ không gian đĩa được xác định khi tạo đĩa ảo, bất kể hệ thống tệp của hệ điều hành khách thực sự sử dụng bao nhiêu không gian đĩa.



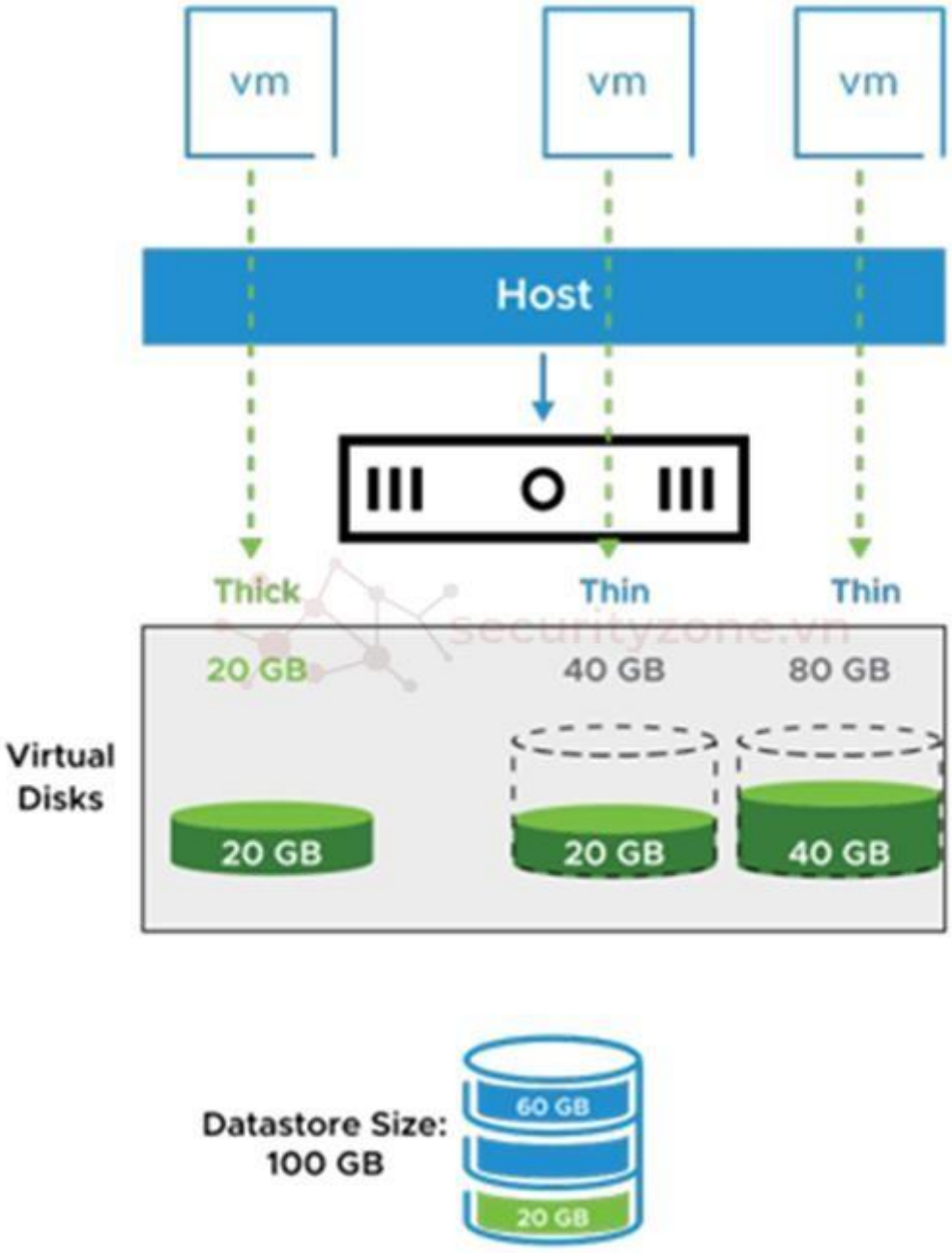
Hình 45 Hình ảnh mô phỏng về cách thức ảo hóa lưu trữ

Có hai loại đĩa dày:

- **Eager Zeroed**: Mọi khối dữ liệu được làm trống bằng số 0 trước khi dữ liệu được ghi.
- **Lazy Zeroed**: Khối dữ liệu chỉ được làm trống khi dữ liệu được ghi lần đầu tiên.

Về Đĩa Mỏng (Thin-Provisioned Disks)

Với đĩa mỏng, không gian chỉ được sử dụng khi cần thiết. VM luôn thấy kích thước đĩa đầy đủ nhưng chỉ sử dụng dung lượng cần thiết. Đĩa có thể mở rộng khi cần thêm dung lượng.



Hình 46 Hình ảnh mô phỏng về cách thức ảo hóa lưu trữ

6. **Quản lý Datastore chứa Đĩa Mỏng**

Đĩa mỏng giúp tối ưu hóa dung lượng lưu trữ nhưng cũng có thể gây ra tình trạng thiếu dung lượng nếu không quản lý cẩn thận. Cần thiết lập các cảnh báo và báo cáo để theo dõi việc sử dụng dung lượng và quản lý datastore hiệu quả.

So sánh ba loại cấp phát đĩa ảo trong VMware:

1. Thick Provisioned Lazy-Zeroed (Cấp phát dày, xóa chậm)

- **Thời gian tạo**: Nhanh, vì không cần xóa (zero out) các khối dữ liệu khi tạo đĩa.
- **Cấp phát khối**: Toàn bộ dung lượng đĩa được cấp phát ngay khi tạo đĩa.
- **Bố trí đĩa ảo**: Có khả năng cao các khối dữ liệu nằm liền nhau.
- **Xóa các khối dữ liệu được cấp phát**: Các khối dữ liệu chỉ được xóa khi có dữ liệu ghi lần đầu vào khối đó.

2. Thick Provisioned Eager-Zeroed (Cấp phát dày, xóa ngay)

- **Thời gian tạo**: Chậm hơn và tỷ lệ thuận với kích thước đĩa, do các khối dữ liệu được xóa ngay khi đĩa được tạo.
- **Cấp phát khối**: Tất cả khối dữ liệu được cấp phát trước.
- **Bố trí đĩa ảo**: Có khả năng cao các khối dữ liệu nằm liền nhau.
- **Xóa các khối dữ liệu được cấp phát**: Tất cả các khối dữ liệu được xóa ngay khi đĩa được tạo.

3. Thin Provisioned (Cấp phát mỏng)

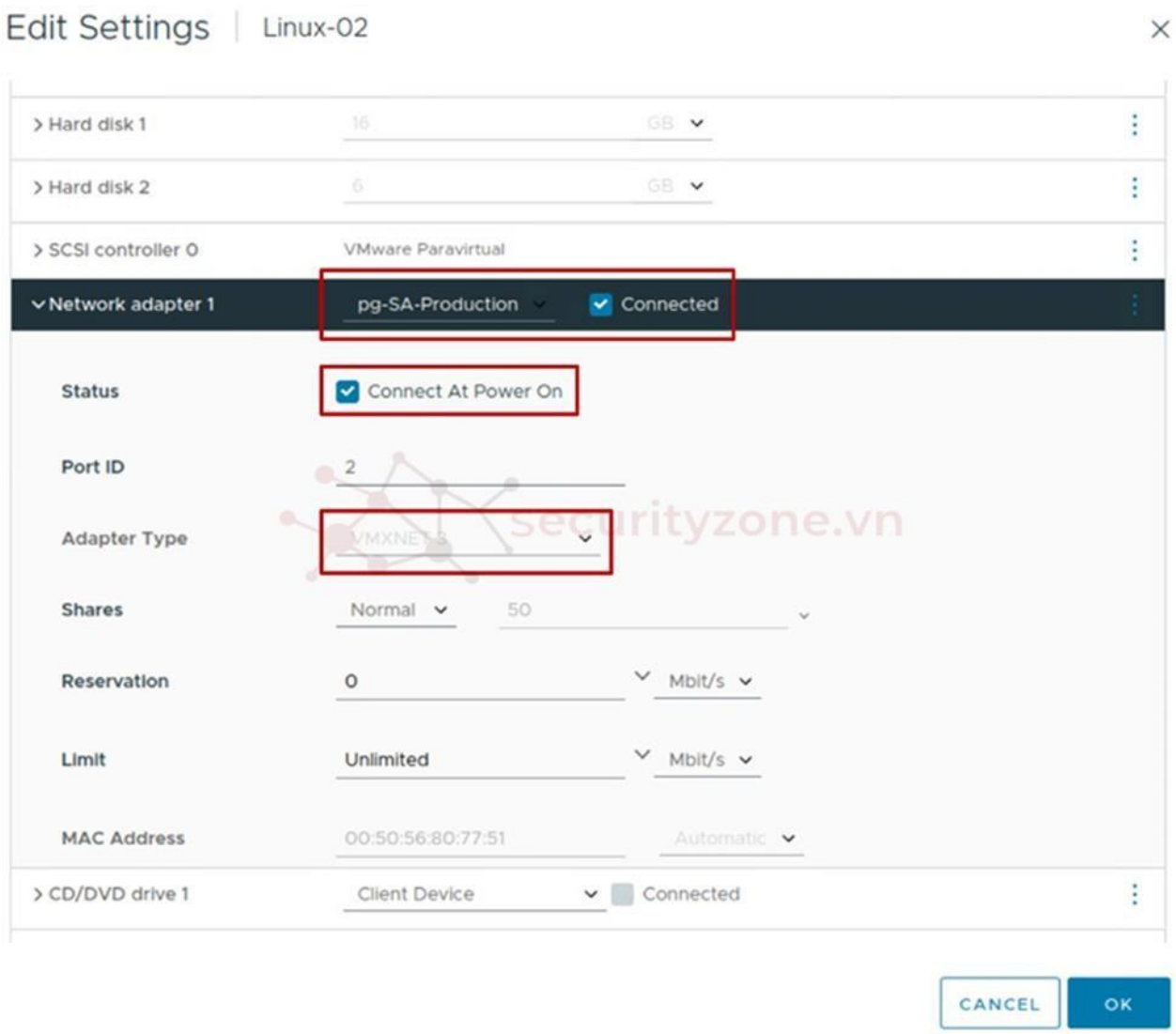
- **Thời gian tạo**: Nhanh nhất, vì đĩa chỉ cấp phát không gian khi dữ liệu thực tế được ghi vào.
- **Cấp phát khối**: Không gian được cấp phát và xóa dần dần khi có dữ liệu ghi vào khối.

- **Bố trí đĩa ảo**: Bố trí đĩa phụ thuộc vào trạng thái động của dung lượng tại thời điểm cấp phát khối.
- **Xóa các khối dữ liệu được cấp phát**: Các khối dữ liệu được xóa khi chúng được cấp phát.

5. Mạng ảo (Virtual Networks)

Mạng ảo cho phép các máy ảo (VM) và các thiết bị vật lý giao tiếp với nhau. Khi cấu hình mạng cho một VM, bạn có thể thiết lập hoặc thay đổi các thông số như loại adapter mạng, nhóm port (port group) mà VM kết nối, trạng thái kết nối mạng, và tùy chọn tự động kết nối khi VM được bật.

- **Network Adapter Type**: Lựa chọn loại adapter mạng mà máy ảo sẽ sử dụng, chẳng hạn như VMXNET3 hoặc E1000.
- **Port Group to Connect to**: Kết nối VM với một nhóm port ảo (port group) trên vSwitch hoặc vDS.
- **Network Connection State**: Trạng thái kết nối mạng của VM, có thể chọn kết nối hoặc không kết nối.
- **Auto-connect on Power On**: Tùy chọn kết nối tự động khi VM được bật.



Hình 47 Hình ảnh mô phỏng cách quản lý Thin Disk trong datastore

7. Các loại adapter mạng (NIC Types)

Khi cấu hình máy ảo, bạn có thể thêm các adapter mạng (NIC) và chỉ định loại adapter phù hợp.

- **E1000 và E1000E**: Phiên bản mô phỏng của card mạng Intel Gigabit Ethernet NIC, hỗ trợ các hệ điều hành khách mới.
- **VMXNET3**: Adapter NIC được thiết kế cho hiệu suất cao, yêu cầu VMware Tools và hỗ trợ nhiều tính năng như hỗ trợ đa hàng đợi (multiqueue), IPv6 offload, và gửi/nhận MSI/MSI-X interrupts.
- **Flexible**: Adapter có thể hoạt động như một Vlance hoặc VMXNET, tự động thay đổi tùy theo driver được cài đặt.
- **SR-IOV pass-through**: Cho phép máy ảo và adapter vật lý trao đổi dữ liệu trực tiếp, bỏ qua kernel VM, giảm thiểu độ trễ mạng.
- **PVRDMA**: Cung cấp hiệu suất cao thông qua giao diện RDMA (Remote Direct Memory Access), hỗ trợ truy cập thiết bị với độ trễ thấp và băng thông cao.

1. PCI Passthrough Devices

Các thiết bị PCI Passthrough cho phép máy ảo truy cập trực tiếp các tài nguyên vật lý để tối ưu hiệu suất.

- **vSphere DirectPath I/O**: Cho phép máy ảo truy cập trực tiếp thiết bị PCI hoặc PCIe trên host. Máy ảo bị ràng buộc với host cụ thể và không thể sử dụng các tính năng như vMotion hay snapshot.
- **vSphere Dynamic DirectPath I/O**: Thiết bị PCI không bị ràng buộc trực tiếp với VM, cho phép VMware DRS chuyển VM giữa các host có cùng thiết bị phần cứng.
- **NVIDIA GRID GPU**: GPU ảo hóa sử dụng công nghệ NVIDIA GRID, cho phép máy ảo thực hiện các tác vụ đồ họa phức tạp với hiệu suất cao.

2. Các thiết bị ảo khác (Other Virtual Devices)

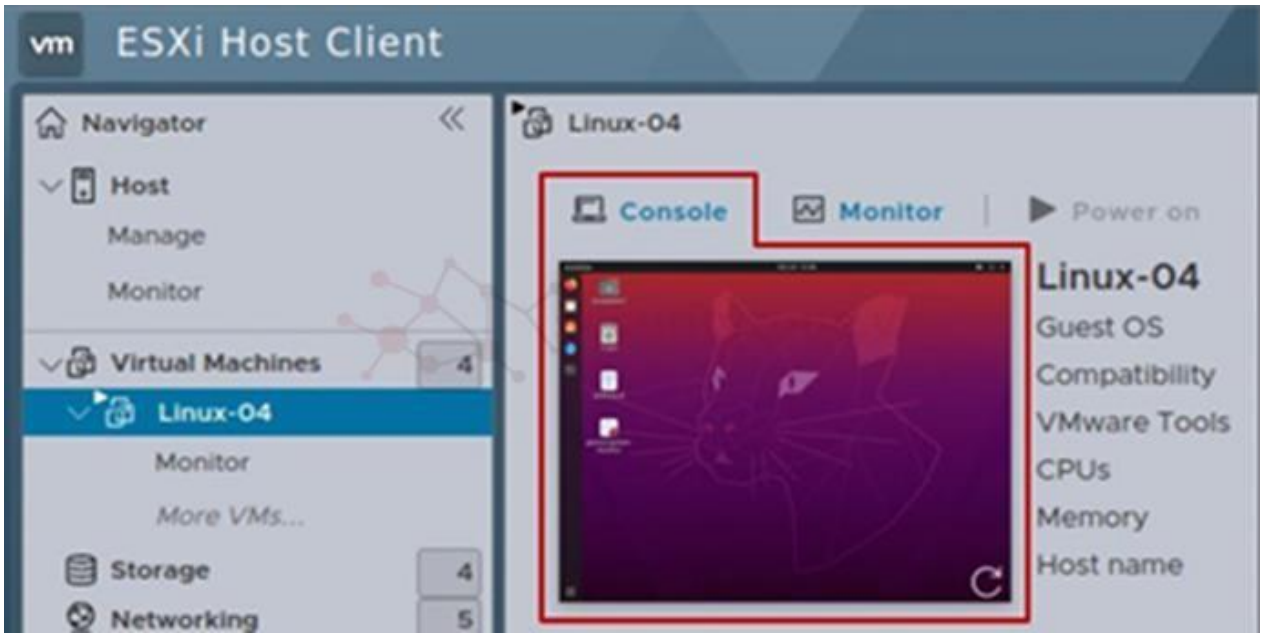
Máy ảo cần có các thiết bị cơ bản như vCPU và bộ nhớ ảo, nhưng việc thêm các thiết bị khác giúp máy ảo hoạt động hiệu quả hơn.

- **Thiết bị CD/DVD**: Kết nối VM với ổ CD, DVD hoặc file ISO.
- **USB 3.0 và 3.1**: Hỗ trợ kết nối các thiết bị USB với máy ảo.
- **vGPUs**: Cho phép VM sử dụng GPU vật lý để thực hiện các tác vụ tính toán cao.
- **vTPM**: Mô đun TPM ảo, cung cấp các chức năng bảo mật dựa trên phần cứng cho máy ảo.

3. Console máy ảo (Virtual Machine Console)

Console máy ảo cung cấp các chức năng điều khiển máy ảo như chuột, bàn phím, và màn hình hiển thị. Bạn có thể sử dụng console để cài đặt hệ điều hành, quản lý BIOS, hoặc khởi động lại máy ảo.

Console máy ảo thường không được sử dụng cho các tác vụ hàng ngày, thay vào đó, các công cụ kết nối từ xa như Remote Desktop Connection hay Virtual Network Connection sẽ được sử dụng.

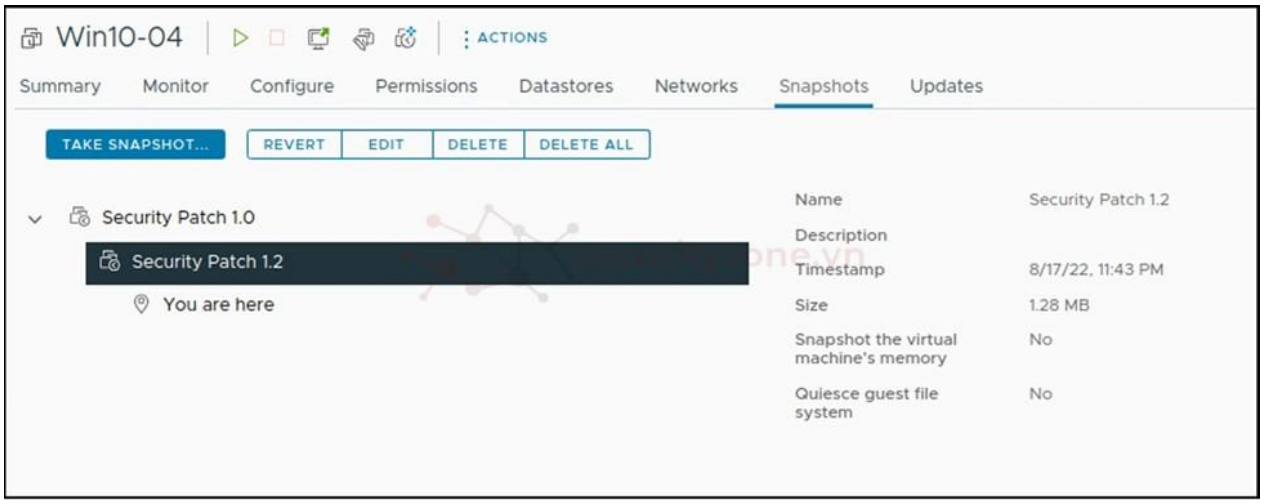


Hình 48 Hình ảnh mô phỏng console ở VM EXSI Host có một máy ảo là Ubuntu

Chương XV. Tìm hiểu về VM Snapshot

I. Tổng quan về VM Snapshot

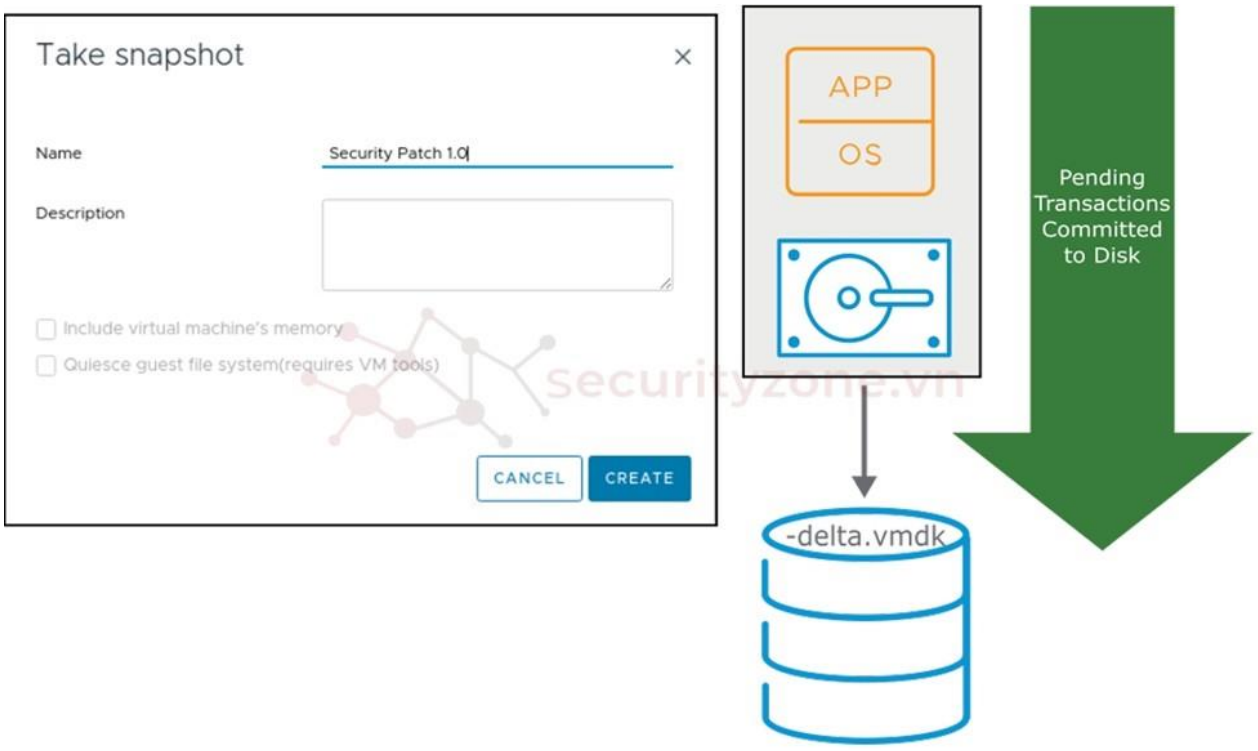
Snapshot là một công cụ hữu ích trong việc lưu giữ và bảo vệ trạng thái của VM, cho phép bạn quay lại trạng thái đã lưu trước đó nhiều lần. Điều này đặc biệt hữu ích trong quá trình nâng cấp hoặc cập nhật, khi có sự cố xảy ra, bạn có thể khôi phục lại trạng thái trước đó. Snapshot không thay thế được cho backup, vì backup đảm bảo lưu trữ dữ liệu trong thời gian dài và thường được thực hiện ngoài hệ thống đang chạy còn snapshot chỉ là một công cụ hỗ trợ cho các tình huống khôi phục nhanh trong thời gian ngắn ví dụ như khi bạn muốn quay lại trạng thái cũ nhiều lần mà không phải tạo nhiều máy ảo, cũng như trong quá trình vá lỗi hoặc nâng cấp Guest OS.



Hình 49 Hình ảnh mô phỏng giao diện VMSnapshot trong vCenter Management

Các snapshot được hiểu như một gốc cây có nhánh, trong đó mỗi snapshot xem như nhánh cây nên có một gốc và có thể có một hoặc nhiều nhánh trên cùng một cây, ngoại trừ snapshot cuối cùng không có nhánh. Snapshot được tạo ra bằng cách chụp ảnh nhanh khi máy ảo đang bật, tắt hoặc tạm dừng. Một snapshot bao gồm:

- Cấu hình của máy ảo
- Trạng thái bộ nhớ của máy ảo (tùy chọn)
- Đĩa ảo



Hình 50 Hình ảnh mô phỏng cách tạo một snapshot và cách thức hoạt động của phần cứng và phần mềm để tạo ra file snapshot .vmdk

Một snapshot tạo ra nhiều tệp tin khác nhau trên datastore, bao gồm:

-Snapshot#.vmsn: Trạng thái cấu hình.

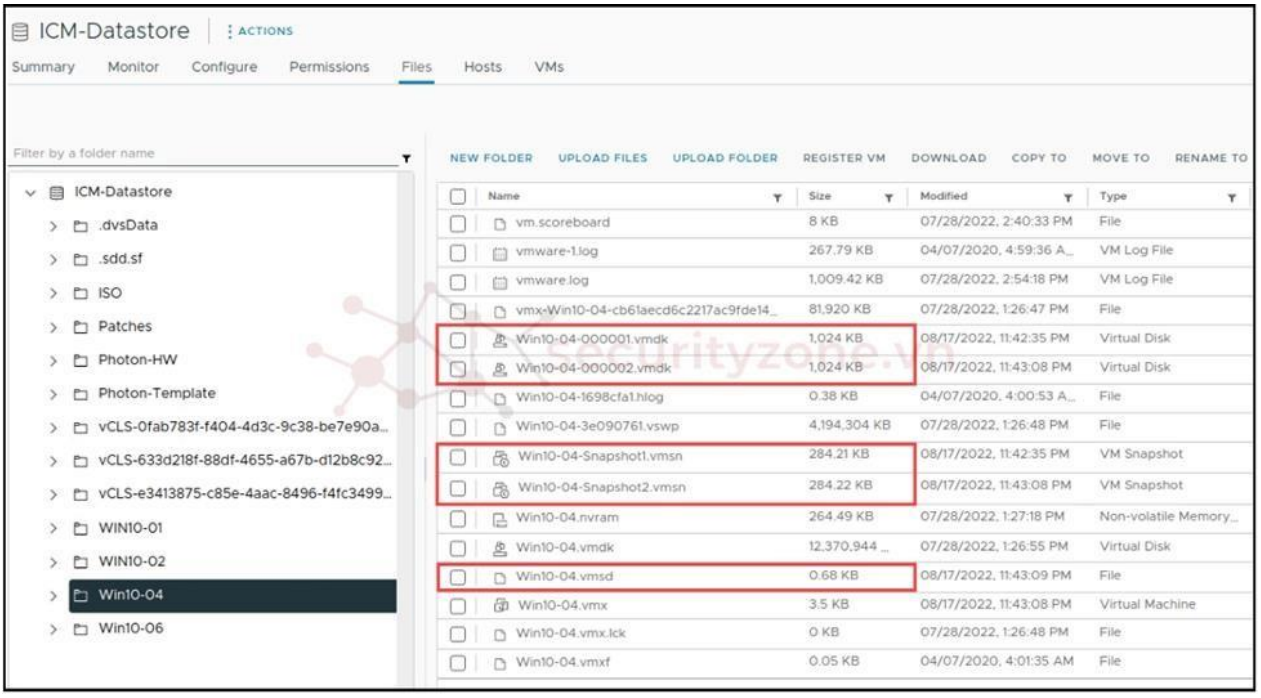
-Snapshot#.vmem: Trạng thái bộ nhớ (tùy chọn).

-00000#.vmdk: Tệp mô tả đĩa.

-00000#-delta.vmdk: Đĩa delta VMFS5.

-00000#-sesparse.vmdk: Đĩa delta VMFS6.

.vmsd: Lưu trữ tên, mô tả và mối quan hệ của các ảnh chụp nhanh.



Hình 51 Hình ảnh mô phỏng các file được tạo ra khi tạo mới một snapshot

II. Hiểu rõ hơn về VM Snapshot

1. Lợi ích của VM Snapshot

- **Lưu trữ trạng thái VM**: Snapshot lưu trữ trạng thái của VM tại thời điểm chụp, bao gồm cấu hình, bộ nhớ và ổ đĩa ảo.
- **Không cần tạo nhiều VM**: Bạn có thể sử dụng Snapshot khi cần khôi phục lại một trạng thái mà không cần tạo nhiều VM riêng biệt.
- **Phù hợp cho thử nghiệm và phát triển**: Rất hữu ích khi thực hiện các cập nhật, vá lỗi hoặc thay đổi cấu hình trên hệ điều hành của máy ảo.

Snapshot không bao gồm các đĩa ảo độc lập (persistent và nonpersistent) tức là snapshot không áp dụng cho các đĩa được đánh dấu là "độc lập" vì chúng không được ghi nhận vào các thay đổi snapshot. Nó ghi lại toàn bộ trạng thái của máy ảo tại thời điểm chụp, bao gồm:

- **Trạng thái bộ nhớ**: Nội dung của bộ nhớ máy ảo, chỉ được ghi lại nếu máy ảo đang bật và tùy chọn chụp bộ nhớ được chọn.
- **Trạng thái cấu hình**: Cài đặt của máy ảo.
- **Trạng thái đĩa**: Trạng thái của tất cả đĩa ảo của máy ảo.

Bạn cũng có thể tạm dừng hệ điều hành khách trước khi chụp ảnh (quiesce). Điều này chỉ áp dụng khi bạn không ghi lại trạng thái bộ nhớ của ảnh chụp nhanh.

2. Các loại Snapshot

Một đĩa delta hoặc đĩa con được tạo ra khi dùng chức năng snapshot. Đĩa delta là đĩa rỗng và được mở rộng khi dữ liệu thay đổi. Các định dạng đĩa khác nhau sẽ được sử dụng dựa trên loại datastore:

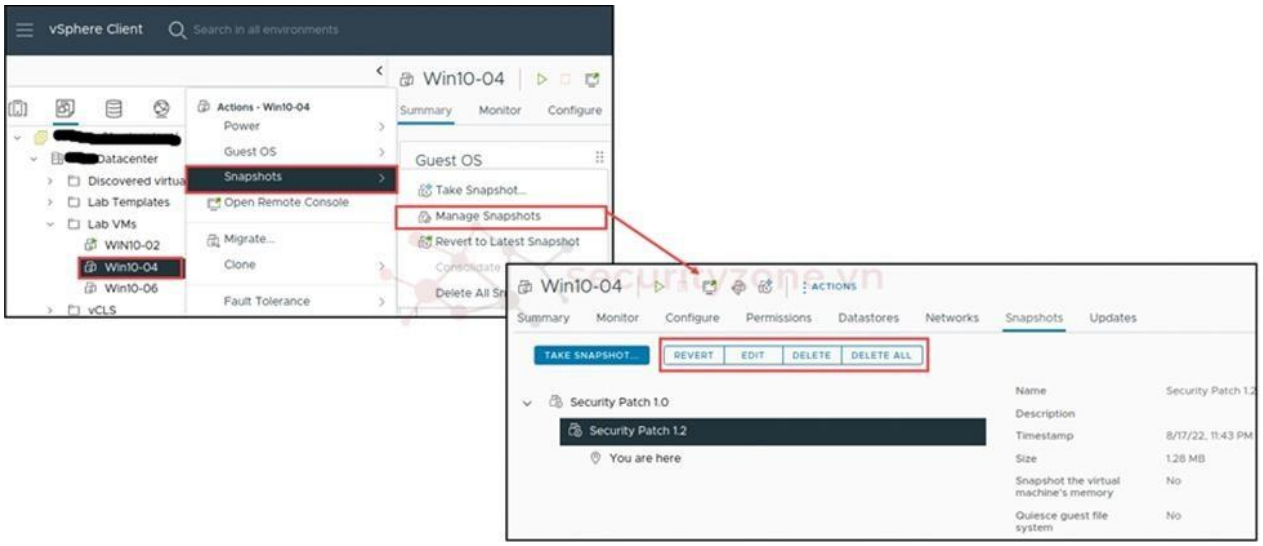
- **VMFSsparse**: Được sử dụng trên VMFS5 với ổ đĩa ảo nhỏ hơn 2 TB. Nó tạo một bản ghi lại (redo log) sau khi snapshot được tạo. VMFSsparse sử dụng kích thước khối 512 bytes và có định dạng “.vmdk”.
- **SEsparse**: Được sử dụng mặc định trên VMFS6 và VMFS5 với ổ đĩa lớn hơn 2 TB. SEsparse có khả năng thu hồi không gian (space reclamation) để giải phóng dung lượng đã sử dụng nhưng không còn cần thiết. SEsparse sử dụng kích thước khối 4 KB và có định dạng “.vmdk”.
- **vsanSparse**: Được tối ưu hóa cho **VMware vSAN**. Khi tạo snapshot trong môi trường vSAN, mỗi delta object sẽ có kích thước 4 MB.

Mỗi loại đĩa delta có sự khác biệt rõ rệt về tính năng và mục đích sử dụng. **VMFSsparse** phù hợp cho các ổ đĩa ảo nhỏ hơn 2 TB trên VMFS5, trong khi **SEsparse** là lựa chọn mặc định cho các ổ đĩa lớn hơn 2 TB, với khả năng thu hồi không gian. **vsanSparse** được thiết kế tối ưu hóa cho môi trường **vSAN**, giúp cải thiện hiệu suất lưu trữ và quản lý không gian trong các cụm vSAN.

3. Quản lý và Xóa Snapshot

Trong vSphere Client, người quản trị có thể thao tác một cách linh hoạt với VM Snapshot với các thao tác điển hình như:

- Chỉnh sửa: Chỉnh sửa tên và mô tả của ảnh.
- Xóa: Xóa ảnh, hợp nhất các tệp ảnh chụp với đĩa gốc.
- Xóa tất cả: Xóa toàn bộ ảnh chụp nhanh của máy ảo.
- Khôi phục lại: Khôi phục máy ảo về trạng thái đã chụp.

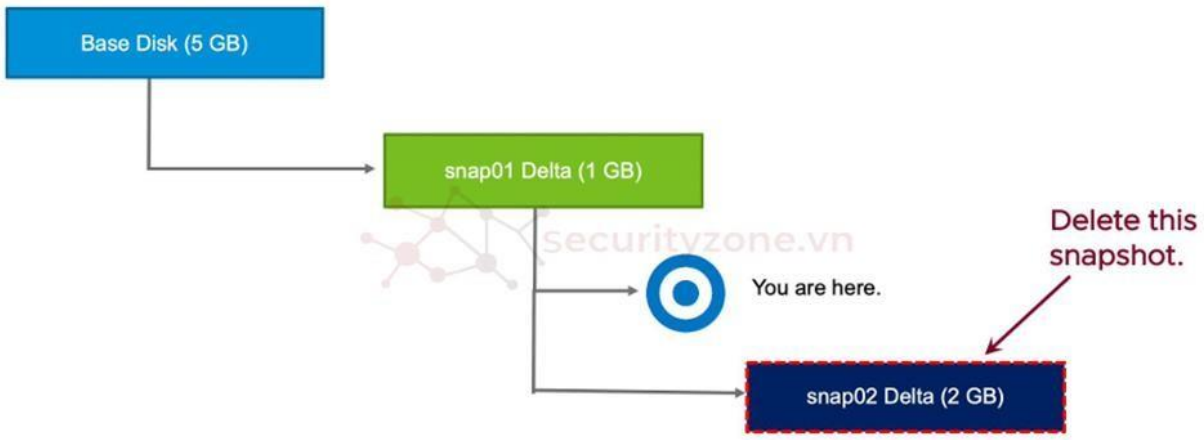


Hình 52 Hình ảnh mô phỏng giao diện khi tạo một snapshot trong vCenter

Lưu ý: Việc xóa các Snapshot quá lớn có thể gây ra thời gian ngừng hoạt động của VM, do quá trình hợp nhất dữ liệu (consolidation) yêu cầu tài nguyên hệ thống lớn. Vì vậy, quản trị viên nên thường xuyên xóa các snapshot không còn cần thiết và tránh để các ảnh chụp nhanh tồn tại trong thời gian dài.

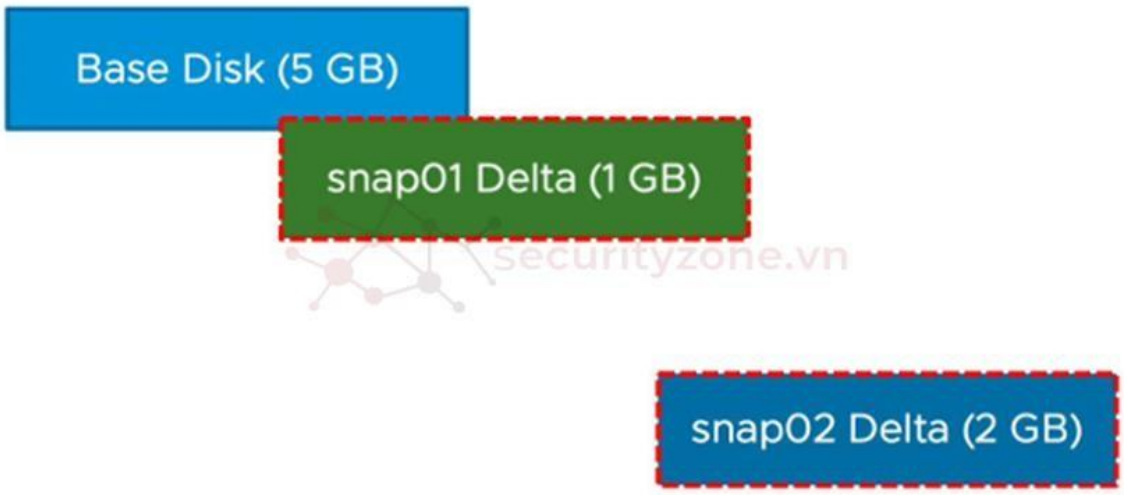
Khi xóa snapshot, các thay đổi sẽ được hợp nhất vào ổ đĩa chính. Nếu xóa tất cả snapshot, tất cả các thay đổi sẽ được hợp nhất vào ổ đĩa chính và các tệp snapshot sẽ bị xóa. Có thể xóa một hoặc tất cả ảnh chụp nhanh.

Xóa một vài:



Hình 53 Hình ảnh mô phỏng mô hình hoạt động của snapshot

Xóa tất cả ảnh chụp nhanh:



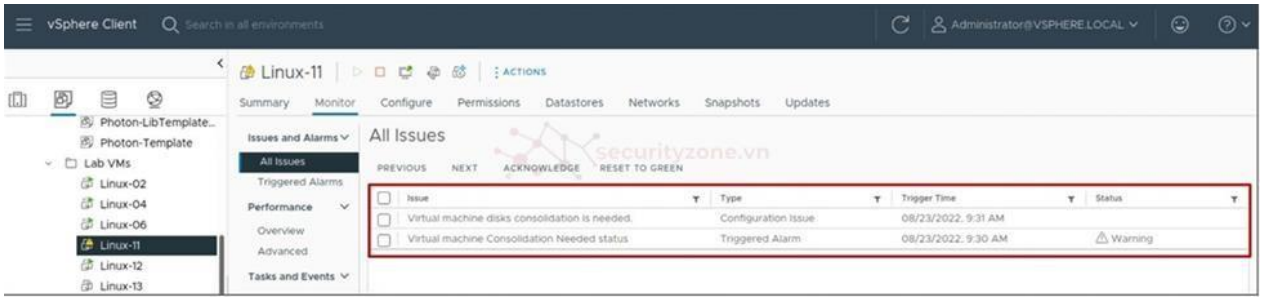
Hình 54 Hình ảnh basedisk(5gb) là ổ đĩa lưu hệ điều hành và snap01 là lần snapshot thứ nhất và snap02 là lần snapshot thứ 2

4. Hợp nhất các Snapshot (Consolidation)

Khi các tệp delta ngày càng phình to, chúng có thể ảnh hưởng đến hiệu suất của máy ảo và gây tiêu tốn tài nguyên lưu trữ không cần thiết. Hợp nhất các tệp delta với đĩa gốc thông qua quá trình **Consolidation** giúp giảm thiểu sự gia tăng kích thước của các tệp này, đồng thời đảm bảo hệ thống vận hành ổn định hơn. Việc hợp nhất thường xuyên là một biện pháp quan trọng để tránh tình trạng đầy datastore và đảm bảo hiệu suất của VM không bị suy giảm theo thời gian.

Dấu hiệu cần hợp nhất:

- Trong tab Monitor của vSphere Client, cảnh báo sẽ xuất hiện khi có sự không khớp giữa các tệp mô tả và các tệp ảnh chụp nhanh.
- Khi Snapshot Manager không hiển thị bất kỳ snapshot nào nhưng các tệp delta vẫn tồn tại.



Hình 55 Hình ảnh mô phỏng lỗi khi merge snapshot lại với nhau

Chương XVI. Tìm hiểu về vMotion

I. Giới thiệu về vSphere vMotion

vSphere vMotion là một tính năng trong VMware vSphere cho phép di chuyển một máy ảo (VM) đang chạy từ một máy chủ ESXi (compute resource) này sang một máy chủ ESXi khác mà không gây gián đoạn hoặc downtime cho hoạt động của VM. Điều này giúp hệ thống tiếp tục hoạt động mà không cần tắt hoặc khởi động lại các máy ảo, đồng thời cung cấp nhiều lợi ích quan trọng trong việc quản lý tài nguyên máy chủ.

vSphere vMotion mang lại những lợi ích chính sau:

- **Cải thiện hiệu suất sử dụng phần cứng**: Bằng cách cho phép di chuyển các máy ảo giữa các máy chủ, nên có thể tận dụng tối đa tài nguyên của các máy chủ vật lý mà không lo lắng về việc downtime.
- **Duy trì hoạt động liên tục cho các máy ảo**: Tính năng này cho phép di chuyển các VM trong khi bảo trì định kỳ hoặc khi hệ thống có thời gian ngừng hoạt động mà không gây gián đoạn cho các ứng dụng hoặc dịch vụ đang chạy.
- **Kết hợp với vSphere DRS (Distributed Resource Scheduler)**: vSphere DRS sử dụng vMotion để cân bằng tải giữa các máy chủ, đảm bảo rằng các máy ảo luôn có đủ tài nguyên để hoạt động hiệu quả.

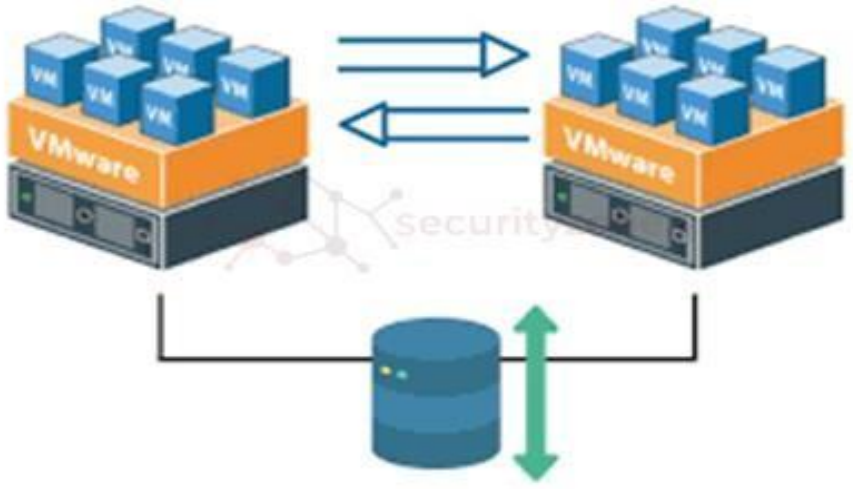
Hình 56 Hình ảnh mô phỏng cách thức hoạt động của vMotion

II. Cách thức hoạt động của vSphere vMotion

Khi bạn sử dụng vSphere vMotion để di chuyển một VM, toàn bộ trạng thái của máy ảo đó sẽ được di chuyển từ máy chủ ESXi nguồn sang máy chủ ESXi đích. Tuy nhiên, dữ liệu lưu trữ (storage) của VM vẫn được giữ nguyên trong cùng một datastore mà không thay đổi.

Trạng thái của VM bao gồm:

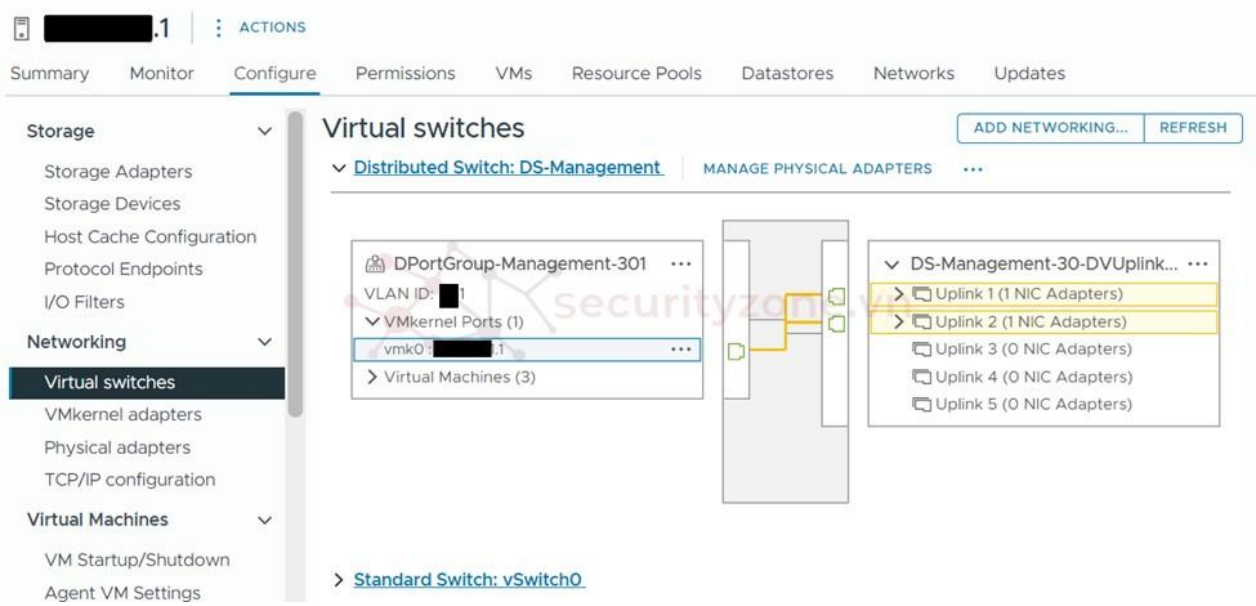
- Nội dung bộ nhớ hiện tại của máy ảo.
- Tất cả thông tin định danh và xác định VM, bao gồm dữ liệu ánh xạ phần cứng của máy ảo, BIOS hoặc EFI, các thiết bị, CPU, và địa chỉ MAC của các card Ethernet.



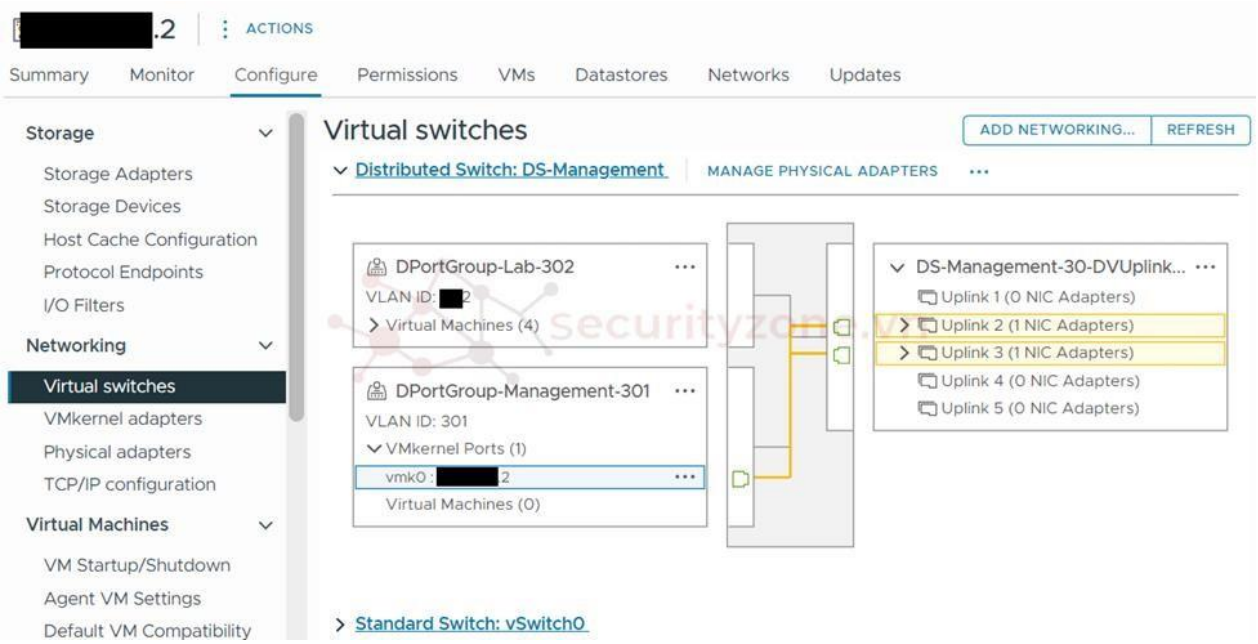
Hình 57 Hình ảnh mô phỏng cách hoạt động của vMotion lên 2 máy ảo

III. Cấu hình mạng vMotion cho các host

Để thực hiện quá trình di chuyển vMotion, bạn cần phải cấu hình đúng các adapter VMkernel trên cả máy chủ nguồn và máy chủ đích.



Hình 58 Hình ảnh mô phỏng giao diện quản lý Virtual Switch trong vCenter



Hình 59 Hình ảnh cách thức hoạt động giữa 2DPG đến 1NIC

Cấu hình vMotion mạng yêu cầu: Phải thiết lập một adapter VMkernel với dịch vụ vMotion được kích hoạt trên cả máy chủ nguồn và máy chủ đích. Các adapter VMkernel này sẽ giúp truyền tải dữ liệu bộ nhớ giữa hai máy chủ thông qua mạng vMotion.

1. Quy trình di chuyển với vSphere vMotion

Quá trình di chuyển một VM giữa các máy chủ ESXi thông qua vSphere vMotion gồm các bước sau:

1. Một **VM shadow** (bản sao máy ảo) được tạo trên máy chủ đích.

2. **Bộ nhớ của VM** trên máy chủ nguồn được sao chép qua mạng vMotion tới máy chủ đích. Trong khi sao chép, người dùng vẫn có thể truy cập và cập nhật bộ nhớ của VM. Mỗi trang bộ nhớ bị thay đổi được lưu trong một **memory bitmap** trên máy chủ nguồn.

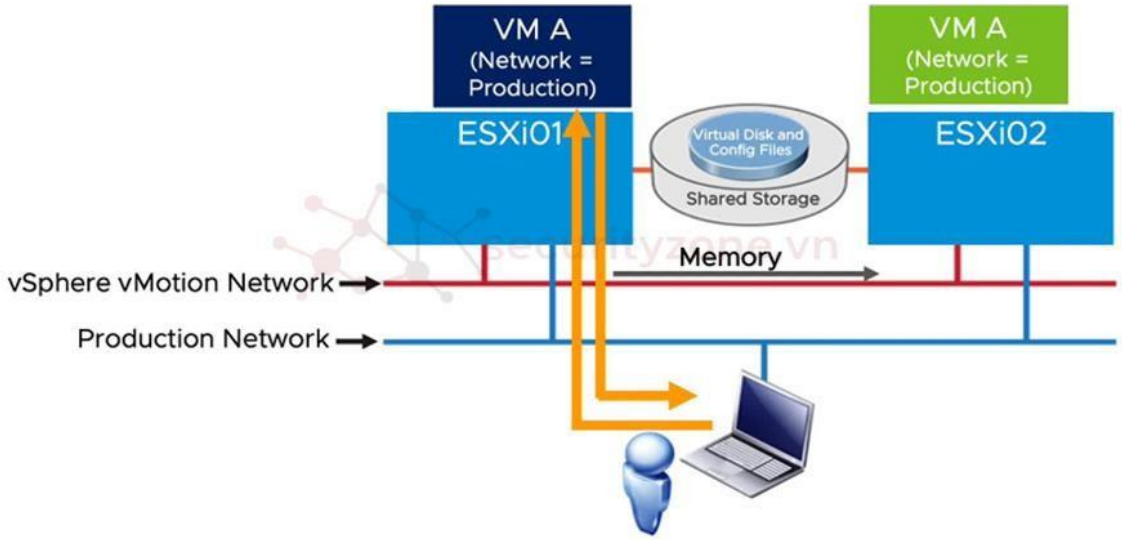
3. Sau khi bản sao chép bộ nhớ lần đầu tiên hoàn tất, một bản sao khác được thực hiện để sao chép các trang bộ nhớ đã thay đổi trong quá trình sao chép lần trước. Quá trình này tiếp tục cho đến khi số lượng trang thay đổi đủ nhỏ để có thể sao chép trong vòng 500 mili giây.

4. Khi hầu hết bộ nhớ của VM đã được sao chép từ máy chủ nguồn sang máy chủ đích, VM sẽ được **quiesce** (tạm dừng). Trong khoảng thời gian này, vMotion sẽ chuyển trạng thái thiết bị và bitmap bộ nhớ của VM sang máy chủ đích.

5. Ngay sau khi VM được quiesce trên máy chủ nguồn, VM sẽ khởi động trên máy chủ đích. Một yêu cầu **Gratuitous ARP (GARP)** sẽ được gửi để thông báo rằng địa chỉ MAC của VM đã chuyển sang một cổng switch vật lý khác. Lúc này, các file của VM sẽ được mở khóa trên máy chủ nguồn và bị khóa trên máy chủ đích.

6. Người dùng bắt đầu truy cập VM từ máy chủ đích thay vì máy chủ nguồn.

7. Các trang bộ nhớ mà VM đã sử dụng trên máy chủ nguồn sẽ được đánh dấu là trống.



Hình 60 Hình ảnh mô phỏng cách thức hoạt động của vMotion

V. Yêu cầu đối với VM và đối với host để vMotion

2. Yêu cầu đối với VM để sử dụng vMotion

Để có thể di chuyển một VM với vSphere vMotion, VM đó phải đáp ứng các yêu cầu sau:

- Nếu VM đang sử dụng đĩa cứng dạng RDM, thì máy chủ đích cũng phải có khả năng truy cập vào cùng thiết bị lưu trữ mà máy chủ nguồn đang sử dụng.
- Nếu máy ảo đang sử dụng file ISO hoặc hình ảnh đĩa từ máy chủ nguồn, thì bạn cần phải gỡ kết nối với các thiết bị ảo đó trước khi di chuyển bằng vMotion.
- Có thể sử dụng vMotion để di chuyển một VM có thiết bị được gắn thông qua giao diện điều khiển từ xa (remote console) như thiết bị vật lý hoặc hình ảnh đĩa.

3. Yêu cầu đối với host để thực hiện vMotion

Cả máy chủ nguồn và máy chủ đích phải đáp ứng các yêu cầu sau để thực hiện quá trình di chuyển vMotion:

- Máy chủ đích phải có quyền truy cập vào cùng bộ lưu trữ (datastore) nơi VM được lưu trữ. Bạn có thể thực hiện tới 128 lần di chuyển vMotion đồng thời cho mỗi datastore. Nếu vị trí file swap của máy chủ đích khác với máy chủ nguồn, file swap sẽ được sao chép tới vị trí mới.
- Cả hai máy chủ phải có cổng VMkernel với dịch vụ vMotion được kích hoạt để đảm bảo quá trình di chuyển có thể diễn ra.
- Máy chủ nguồn và đích phải có địa chỉ IP trong cùng một phiên bản mạng (IPv4 hoặc IPv6). Bạn không thể di chuyển một VM từ máy chủ đăng ký với địa chỉ IPv4 sang máy chủ đăng ký với địa chỉ IPv6.

  Số lượng tiến trình vMotion đồng thời bị giới hạn bởi tốc độ mạng:

- Mạng 1 Gbps cho phép tối đa 4 tiến trình vMotion đồng thời.
- Mạng 10 Gbps hoặc nhanh hơn cho phép tối đa 8 tiến trình vMotion đồng thời.

- Để có hiệu suất tốt hơn, bạn nên dành ít nhất hai nhóm port VMkernel cho lưu lượng vMotion.

CPU của máy chủ đích phải có khả năng hỗ trợ các lệnh hoặc tính năng giống như CPU của máy chủ nguồn. Nếu không, quá trình vMotion có thể gặp lỗi do không tương thích về phần cứng. EVC và Compatibility Masks là hai tính năng ẩn hoặc vô hiệu hóa các tính năng của CPU nhằm đảm bảo tương thích giữa các máy chủ có cấu hình phần cứng khác nhau.

- **Sử dụng Enhanced vMotion Compatibility (EVC):** Một tính năng trong vSphere cho phép bạn **ẩn đi** hoặc **giới hạn** các tính năng phần cứng cao cấp của CPU trên máy chủ nguồn. Điều này giúp đảm bảo rằng CPU của các máy chủ khác (với CPU cũ hơn hoặc ít tính năng hơn) vẫn có thể tương thích với VM trong quá trình di chuyển. **Ví dụ:** Nếu một máy chủ có CPU mới hơn, có các tính năng tiên tiến hơn, bạn có thể sử dụng EVC để ẩn các tính năng đó. Điều này làm cho CPU của máy chủ mới trông giống như CPU của máy chủ cũ hơn, giúp việc di chuyển VM trở nên dễ dàng mà không cần lo lắng về sự khác biệt về phần cứng.
- **Compatibility Masks (Mặt nạ tương thích):** Cho phép bạn tùy chỉnh và điều chỉnh các tính năng cụ thể của CPU. Bằng cách sử dụng các mặt nạ này, bạn có thể tắt một số tính năng của CPU, giúp cho các máy chủ ESXi với các loại CPU khác nhau có thể tương thích với nhau khi sử dụng vMotion. **Ví dụ:** Nếu máy chủ nguồn có CPU hỗ trợ một tính năng nào đó mà máy chủ đích không có, bạn có thể sử dụng mặt nạ tương thích để vô hiệu hóa tính năng đó. Điều này sẽ giúp việc di chuyển diễn ra suôn sẻ.

KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Kết luận

Công nghệ ảo hóa VMware vSphere đã chứng minh được vai trò quan trọng trong việc tối ưu hóa tài nguyên và nâng cao hiệu suất hệ thống. Qua quá trình nghiên cứu và triển khai, chúng ta có thể rút ra một số kết luận chính:

1. **Tối ưu hóa tài nguyên**: VMware vSphere cho phép các doanh nghiệp tận dụng tối đa tài nguyên phần cứng hiện có, giảm thiểu lãng phí và tăng hiệu suất sử dụng. Điều này đặc biệt quan trọng trong bối cảnh các doanh nghiệp luôn tìm kiếm các giải pháp tiết kiệm chi phí và nâng cao hiệu quả hoạt động.

2. **Khả năng mở rộng và linh hoạt**: Với VMware vSphere, các doanh nghiệp có thể dễ dàng mở rộng hệ thống mà không cần đầu tư lớn vào phần cứng mới. Khả năng linh hoạt trong việc quản lý và phân bổ tài nguyên giúp doanh nghiệp nhanh chóng đáp ứng các nhu cầu thay đổi của thị trường.

3. **An toàn và bảo mật**: VMware vSphere cung cấp các tính năng bảo mật tiên tiến, giúp bảo vệ dữ liệu và hệ thống khỏi các mối đe dọa từ bên ngoài. Các tính năng như mã hóa dữ liệu, kiểm soát truy cập và giám sát hệ thống giúp đảm bảo an toàn cho các ứng dụng và dữ liệu quan trọng.

4. **Quản lý dễ dàng**: Giao diện quản lý thân thiện và các công cụ hỗ trợ mạnh mẽ giúp việc quản lý hệ thống trở nên dễ dàng hơn. Các quản trị viên có thể giám sát và điều chỉnh hệ thống một cách hiệu quả, giảm thiểu thời gian và công sức cần thiết.

5. **Hỗ trợ đa dạng ứng dụng**: VMware vSphere hỗ trợ nhiều loại ứng dụng khác nhau, từ các ứng dụng doanh nghiệp truyền thống đến các ứng dụng hiện đại như trí tuệ nhân tạo và học máy. Điều này giúp doanh nghiệp dễ dàng tích hợp và triển khai các giải pháp công nghệ mới.

Hướng phát triển

Để tiếp tục phát triển và nâng cao hiệu quả của công nghệ ảo hóa VMware vSphere, chúng ta cần tập trung vào một số hướng phát triển chính sau:

1. **Nâng cao hiệu suất**:
    - **Tối ưu hóa các tính năng hiện có**: Liên tục cải tiến và tối ưu hóa các tính năng hiện có của VMware vSphere để đảm bảo hiệu suất cao nhất. Điều này bao gồm việc cải thiện khả năng xử lý, lưu trữ và kết nối mạng.
    - **Phát triển các tính năng mới**: Nghiên cứu và phát triển các tính năng mới để đáp ứng nhu cầu ngày càng cao của doanh nghiệp. Các tính năng như tự động hóa quản lý tài nguyên, tối ưu hóa năng lượng và quản lý tài nguyên động sẽ giúp nâng cao hiệu suất hệ thống.
2. **Tích hợp công nghệ mới**:
    - Trí tuệ nhân tạo (AI) và máy học (ML): Tích hợp các công nghệ AI và Machine Learning vào VMware vSphere để tự động hóa và tối ưu hóa quản lý tài nguyên. Các thuật toán AI có thể giúp dự đoán và điều chỉnh tài nguyên theo nhu cầu thực tế, giảm thiểu lãng phí và tăng hiệu quả sử dụng.
    - **Điện toán đám mây**: Kết hợp với các giải pháp điện toán đám mây để cung cấp các dịch vụ ảo hóa linh hoạt và hiệu quả hơn. Điều này giúp doanh nghiệp dễ dàng mở rộng và quản lý hệ thống mà không cần đầu tư lớn vào hạ tầng phần cứng.
3. **Mở rộng ứng dụng**:
    - **Internet of Things (IoT)**: Áp dụng công nghệ ảo hóa vào các hệ thống IoT để quản lý và phân tích dữ liệu từ các thiết bị kết nối. Điều này giúp doanh nghiệp tận dụng tối đa tiềm năng của IoT và cải thiện hiệu quả hoạt động.

- **Hệ thống phân tán**: Sử dụng VMware vSphere để quản lý các hệ thống phân tán, giúp đảm bảo tính nhất quán và hiệu suất cao cho các ứng dụng phân tán. Điều này đặc biệt quan trọng trong bối cảnh các doanh nghiệp ngày càng phụ thuộc vào các hệ thống phân tán để cung cấp dịch vụ.

4. **Đào tạo và phát triển nhân lực**:
   - **Đào tạo chuyên sâu**: Cung cấp các chương trình đào tạo chuyên sâu về công nghệ ảo hóa và VMware vSphere cho các quản trị viên hệ thống. Điều này giúp đảm bảo rằng nhân lực có đủ kiến thức và kỹ năng để quản lý và vận hành hệ thống một cách hiệu quả.
   - **Phát triển cộng đồng**: Xây dựng và phát triển cộng đồng người dùng VMware vSphere để chia sẻ kiến thức, kinh nghiệm và hỗ trợ lẫn nhau. Điều này giúp tạo ra một môi trường học tập và phát triển liên tục cho các chuyên gia công nghệ.
5. **Hợp tác và phát triển đối tác**:
   - **Hợp tác với các nhà cung cấp công nghệ**: Hợp tác với các nhà cung cấp công nghệ khác để tích hợp và phát triển các giải pháp ảo hóa tiên tiến. Điều này giúp mở rộng khả năng và ứng dụng của VMware vSphere trong nhiều lĩnh vực khác nhau.
   - **Phát triển đối tác kinh doanh**: Xây dựng mạng lưới đối tác kinh doanh để cung cấp các dịch vụ và giải pháp ảo hóa cho doanh nghiệp. Điều này giúp mở rộng thị trường và tăng cường sự hiện diện của VMware vSphere trên toàn cầu.

TÀI LIỆU THAM KHẢO

[1]. **Emilio Aguero, "Administering VMware vSphere 8 (Learn, Setup ESXi + vCenter)", Emilio Aguero/ Online Courses - Learn Anything, On Your Schedule | Udemy, 2024.**

[2]. Rick Crisci, Clear and Simple vSphere 8 Professional - VMware VCP DCV, Rick Crisci / **Online Courses - Learn Anything, On Your Schedule | Udemy, 2024**

[3]. Rick Crisci, "Clear and Simple VCTA VMware Technical Associate - vSphere 8", Rick Crisci / **Online Courses - Learn Anything, On Your Schedule | Udemy, 2024.**

[4]. HooangF4t, "vSphere Full Tutorial", HooangF4t / Lab Network System Security, 10/2024.

[5]. Wikipedia, "VMware vSphere - Wikipedia", 10/2024