TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

VIỆN ĐIỆN TỬ - VIỄN THÔNG

BÁO CÁO BÀI TẬP LỚN

HỆ ĐIỀU HÀNH

Đề tài:

XÂY DỰNG PRIVATE IAAS CLOUD COMPUTING VỚI CLOUDSTACK VÀ KVM HYPERVISOR

Nhóm 7

Sinh viên thực hiện: Phạm Thái Hoà - 20182533
Trần Văn Chung - 20182388
Lê Quốc Việt - 20182885
Nguyễn Anh Bằng - 20182377
Nguyễn Thị Trang - 20182830
Trần Đức Ngọc - 20182709

Giảng viên hướng dẫn: TS. Phạm Doãn Tĩnh

Hà Nội, 1-2021

LỜI NÓI ĐẦU

Trong những năm gần đây, điện toán đam mây "Cloud Computing" đã xuất hiện như một trong những từ thường dùng trong ngành công nghiệp ICT. Nhiều nhà cung cấp CNTT được hứa hẹn cung cấp thiết bị, tính toán, lưu trữ và các dịch vụ ứng dụng, đồng thời cung cấp phạm vi vùng bảo mật tại một số châu lục, cung cấp dịch vụ cấp thoả thuận (SLA) thực hiện lời hứa ủng hộ về thời hạn hoạt động cho các dịch vụ của họ. Trong khi các "Đám mây" là sự tiến hoá tự nhiên của các trung tâm dữ liệu truyền thống, chúng được phân biệt bằng các cung cấp các tài nguyên(tính toán, dữ liệu, ứng dụng) như là điểm nổi trội dựa trên các dịch vụ web và làm theo một mô hình "Tiện ích" chi phí định giá mà khách hàng được tính dựa trên việc sử dụng các tài nguyên tính toán, lưu trữ, và chuyển dữ liệu. Họ cung cấp quyền truy cập dựa trên thuê bao cơ sở hạ tầng, nền tảng và các ứng dụng được phổ biến gọi là cơ sở hạ tầng như một dịch vụ IaaS, dịch vụ nền tảng PaaS và phần mềm như dịch vụ SaaS. Trong khi các dịch vụ này đang nổi lên tăng khả năng tương tác và khả năng sử dụng và giảm chỉ phí tính toán, ứng dụng lưu trữ, và cung cấp một số đơn đặt hàng các mức độ có ý nghĩa phức tạp liên quan đến việc đảm bảo rằng các ứng dụng và dịch vụ có thể mở rộng khi cần thiết để đạt được hoạt động phù hợp và đáng tin cậy theo vận hành tốt nhất.

MỤC LỤC

DANH MỤC KÝ HIỆU VÀ CHỮ VIẾT TẮT

CHỮ VIẾT TẮT	Ý NGHĨA
SaaS	Software as a Service
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
KVM	Kernel-based Virtual Machine
NFS	Network File System
VPN	Virtual Private Network
VM	Virtual Machine
CPU	Central Processing Unit
TCP	Transmission Control Protocol
IP	Internet Protocol
API	Application Programming Interface
UI	User Interface
DNS	Domain Name System
RFC	Request For Comments

DANH MỤC HÌNH VẼ

DANH MỤC BẢNG BIỂU

No table of figures entries found.

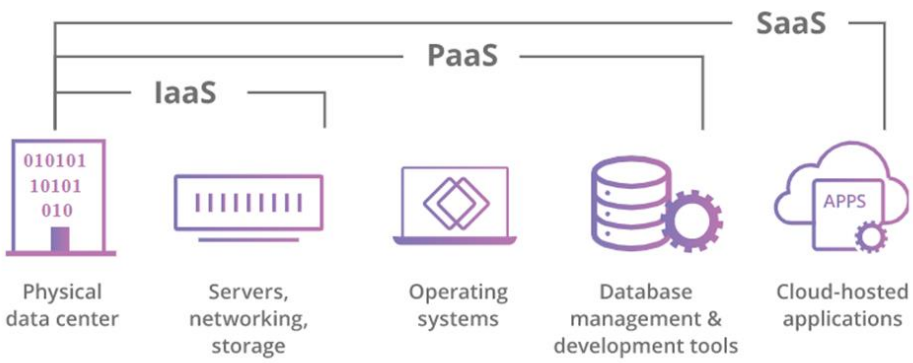
CHƯƠNG 1. KHÁI NIỆM VỀ CLOUD

1.1 Giới thiệu về Cloud

"Đám mây" đề cập đến các máy chủ được truy cập qua Internet, phần mềm và cơ sở dữ liệu chạy trên các máy chủ đó. Máy chủ đám mây được đặt tại trung tâm dữ liệu trên toàn thế giới. Điện toán đám mây là việc phân phối các tài nguyên CNTT theo nhu cầu qua Internet với chính sách thanh toán theo mức sử dụng. Thay vì mua, sở hữu và bảo trì các trung tâm dữ liệu và máy chủ vật lý, bạn có thể tiếp cận các dịch vụ công nghệ, như năng lượng điện toán, lưu trữ và cơ sở dữ liệu, khi cần thiết. Bằng cách sử dụng điện toán đám mây, người dùng và các công ty không phải tự quản lý các máy chủ vật lý hoặc chạy các ứng dụng phần mềm trên máy của chính họ. Đám mây cho phép người dùng truy cập các tệp và ứng dụng giống nhau từ hầu hết mọi thiết bị, vì quá trình tính toán và lưu trữ diễn ra trên các máy chủ trong trung tâm dữ liệu, thay vì cục bộ trên thiết bị của người dùng.

Điện toán đám mây có thể thực hiện được nhờ một công nghệ được gọi là ảo hóa. Ảo hóa cho phép tạo ra một máy tính "ảo" chỉ mô phỏng kỹ thuật số, hoạt động như thể nó là một máy tính vật lý với phần cứng của riêng nó. Thuật ngữ kỹ thuật cho một máy tính như vậy là máy ảo . Khi được triển khai đúng cách, các máy ảo trên cùng một máy chủ được phân chia với nhau, vì vậy chúng hoàn toàn không tương tác với nhau và các tệp và ứng dụng từ một máy ảo này sẽ không hiển thị với các máy ảo khác ngay cả khi chúng đang bật cùng một máy vật lý.

Các nhà cung cấp dịch vụ điện toán đám mây cung cấp các dịch vụ của họ theo ba mô hình cơ bản là hạ tầng dịch vụ (IaaS), nền tảng hướng dịch vụ (PaaS) và phần mềm hướng dịch vụ (SaaS).



Hình 1.1 Các mô hình dịch vụ trong Cloud

1.2 Các khái niệm cơ bản của Cloud

1.2.1 Software as a Service (SaaS)

Khái niệm:

Software as a service hay còn được gọi tắt là SaaS. Đây là một dịch vụ được các nhà cung cấp mang đến cho người dùng đầu cuối sử dụng dựa trên công nghệ đám mây. Nói đơn giản hơn nhà cung cấp tạo ra và duy trì một phần mềm chạy trên nền web và khách hàng có thể truy cập từ xa thông qua internet. Phần lớn các ứng dụng SaaS được chạy trực tiếp thông qua trình duyệt web, và không yêu cầu download hay cài đặt bất cứ thứ gì từ phía người dùng.

Các lợi ích của SaaS:

Mô hình SaaS cung cấp nhiều lợi ích cho khách hàng khi sử dụng. Đối với một doanh nghiệp kinh doanh, mô hình giúp tiếp kiệm về chi phí, thời gian, nhân lực vì SaaS dễ dàng truy cập mọi lúc mọi nơi. Bên cạnh đó, khách hàng luôn nhận được tính năng phần mềm tốt nhất vì việc bảo hệ máy chủ đều được nhà cung cấp chịu trách nhiệm.

Các đặc điểm của SaaS:

- Quản lý dịch vụ từ vị trí trung tâm
- Đặt trên máy chủ từ xa
- Khả năng truy cập qua internet
- Người dùng không có trách nhiệm cho việc cập nhật phần cứng và phần mềm

Ví dụ:

SaaS giống như thuê một ngôi nhà: chủ nhà duy trì ngôi nhà, nhưng người thuê chủ yếu được sử dụng nó như thể họ sở hữu nó. Ví dụ về các ứng dụng SaaS bao gồm Salesforce, MailChimp và Slack

1.2.2 Platform as a Service (PaaS)

Khái niệm:

Nền tảng là một dịch vụ (PaaS) là mô hình điện toán đám mây trong đó nhà cung cấp bên thứ ba cung cấp các công cụ phần cứng và phần mềm – thường là những công cụ cần thiết để phát triển ứng dụng – cho người dùng qua internet. Một nhà cung cấp PaaS lưu trữ phần cứng và phần mềm trên cơ sở hạ tầng của riêng mình . Do đó, PaaS giải phóng các nhà phát triển khỏi việc phải cài đặt phần cứng và phần mềm nội bộ để phát triển hoặc chạy một ứng dụng mới

Các lợi ích của PaaS:

Sẽ có rất nhiều lợi ích khác nhau cho việc sử dụng PaaS:

- Vì môi trường cần thiết cho sự phát triển đã được chuẩn bị trước, nên chi phí phát triển và thời gian làm việc có thể giảm đi rất nhiều.
- Bảo trì platform, sao lưu, v.v. được quản lý bởi đám mây, do đó người dùng không cần phải cài đặt cấu hình và quản lý chúng.
- Môi trường cơ sở hạ tầng được chuẩn bị trên đám mây, vì vậy nó có thể được sử dụng ngay lập tức.
- Các kỹ sư có thể tập trung vào phát triển vì toàn bộ môi trường cơ sở hạ tầng đã được cung cấp bởi các dịch vụ đám mây.
- Rất linh hoạt phát triển so với SaaS và khách hàng có thể sử dụng các chương trình của riêng họ.

Các đặc điểm của PaaS:

- Được xây dựng trên công nghệ ảo hóa, nghĩa là tài nguyên có thể dễ dàng mở rộng lên hoặc xuống khi doanh nghiệp bạn thay đổi.
- Các dịch vụ web và databases được tích hợp.
- Cung cấp nhiều dịch vụ để phát triển, kiểm thử, và triển khai ứng dụng.
- Nhiều người dùng có thể truy cập cùng một ứng dụng dịch vụ một lúc.

Ví dụ:

PaaS có thể được so sánh với việc thuê tất cả các công cụ và thiết bị cần thiết để xây dựng một ngôi nhà, thay vì thuê chính ngôi nhà đó. Các ví dụ về PaaS bao gồm Heroku và Microsoft Azure.

1.2.3 Infrastructure as a Service (IaaS)

Khái niệm:

Đây là một dịch vụ cho phép người dùng sử dụng cơ sở hạ tầng CNTT cần thiết cho việc xây dựng hệ thống, chẳng hạn như hệ thống mạng, máy chủ và hệ điều hành v.v. cần thiết cho hoạt động của hệ thống, thông qua Web.Với IaaS, người dùng chọn các thông số kỹ thuật phần cứng và phần mềm cần có, thiết lập hệ điều hành, v.v., xây dựng cơ sở hạ tầng CNTT và phát triển ứng dụng.Không giống như SaaS và PaaS, IaaS có tính linh hoạt cao hơn, cho phép người dùng chọn thông số kỹ thuật phần cứng và hệ điều hành tùy ý. Trong phạm vi đó, cần có kiến thức chuyên môn về hệ điều hành, phần cứng, mạng và phải xem xét các biện pháp bảo mật.

Các lợi ích của PaaS:

Có rất nhiều các lợi ích cho việc chọn IaaS như là:

- Không phải chuẩn bị môi trường phát triển riêng biệt.
- Cho phép linh hoạt lựa chọn các thông số kỹ thuật phần cứng và hệ điều hành cần thiết cho dịch vụ và sử dụng chúng từ hệ thống mạng.
- Cho phép mở rộng tài nguyên máy chủ về cả số lượng máy lẫn công năng máy một cách linh hoạt.
- Không phát sinh sửa chữa sự cố xảy ra trong phần cứng thực tế hoặc chi phí nâng cấp hệ thống.

Các đặc điểm của IaaS:

- Tài nguyên có sẵn như một dịch vụ
- Chi phí khác nhau phụ thuộc vào mức tiêu thụ
- Các dịch vụ có khả năng mở rộng cao
- Thường có nhiều người dùng trên một phần cứng cụ thể
- Cung cấp quyền kiểm soát hoàn toàn cơ sở hạ tầng cho tổ chức
- Linh động hơn rất nhiều so với SaaS, PaaS

Ví dụ:

Iaas giống như một công ty cho thuê một khu đất mà họ có thể xây bất cứ thứ gì họ muốn - nhưng họ cần phải cung cấp thiết bị và vật liệu xây dựng của riêng họ. Các nhà cung cấp IaaS bao gồm DigitalOcean, Google Compute Engine và OpenStack

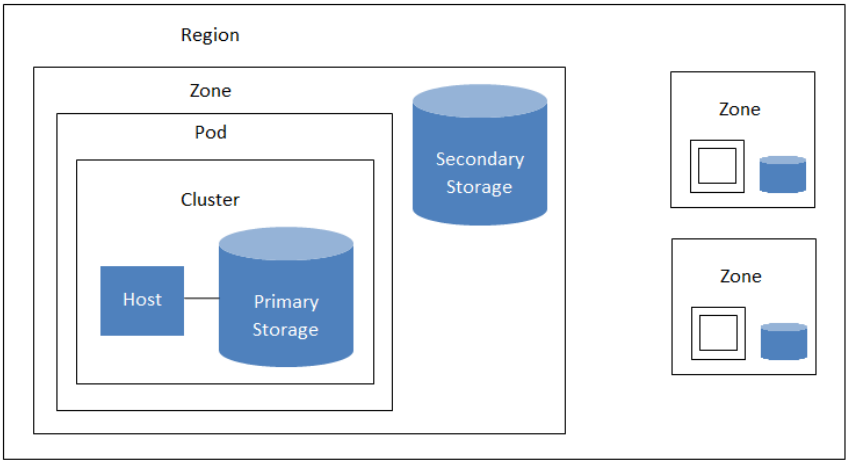
1.3 Tổng quan về cơ sở hạ tầng cloud

Tài nguyên trong đám mây được quản lý như sau:

- Regions
- Zones
- Pods
- Clusters
- Host
- Primary Storage
- Secondary Sotrage

1.3.1 Region

Một region là đơn vị tổ chức lớn nhất có sẵn trong triển khai CloudStack. Một region được tạo thành từ một số zones có sẵn, trong đó mỗi zone sẽ tương đương như một trung tâm dữ liệu (datacenter). Mỗi region được điều khiển bởi cụm máy chủ quản lý (Management Severs) của nó chạy ở một trong các zones.



Hình 1.2 Một region với nhiều zones

Bằng cách nhóm các zones thành các regions, đám mây có thể đạt được tính khả dụng và khả năng mở rộng cao hơn. Tài khoản người dụng có thể mở rộng các regions, do đó người dùng có thể triển khai máy ảo (Virtual Machine) ở nhiều regions phân tán rộng rãi. Ngay cả khi một trong các khu vực không khả dụng, các dịch vụ có sẵn cho

người dùng cuối thông qua các máy ảo được triển khai ở region khác. Và bằng cách nhóm cộng đồng các zones dưới máy chủ quản lý lân cận của chúng, độ trễ của thông tin liên lạc trong đám mây được giảm bớt so với việc quản lý các zones phần tán rộng rãi từ một máy chủ quản lý trung tâm duy nhất.

Hồ sơ sử dụng cũng có thể hợp nhất và theo dõi ở cấp region, tạo báo cáo hoặc hoá đơn cho từng khu vực địa lý.

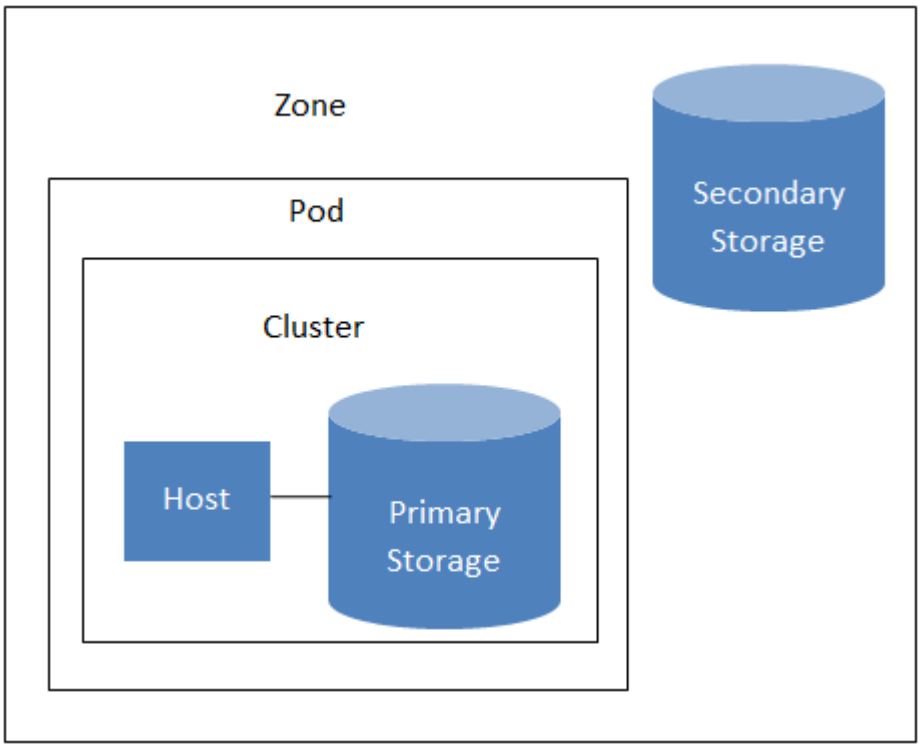
Các region được hiển thị cho người dùng cuối. Khi người dùng khởi động máy ảo khách trên một máy chủ quản lý CloudStack cụ thể, người dùng đang mặc định chọn khu vực đó cho khách của họ.. Người dùng cũng có thể được yêu cầu sao chép các mẫu riêng của họ sang các regions bổ sung để cho phép tạo các máy ảo của khách sử dụng mẫu của họ trong các reigion đó.

1.3.2 Zone

Zone là đơn vị tổ chức lớn thứ hai trong quá trình triển khải CloudStack. Một zone thường tương đương với một trung tâm dữ liệu, mặc dù có thể có nhiều zones trong một trung tâm dữ liệu. Lợi ích của việc tổ chức cơ sở hạ tầng thành các zones là cung câp sự cô lập và dự phòng. Ví dụ: mỗi zone có thể có nguồn cung cấp điện và đường mạng riêng biệt và các zones có thể được phần tách rộng rãi về mặt địa lý (mặc dù điều này không bắt buộc).

Một zone bao gồm:

- Một hoặc nhiều pods. Mỗi pod có chứa một hoặc nhiều cụm hosts và một hoặc nhiều máy chủ lưu chữ chính (primary storage sever)
- Một zone có thể chứa một hoặc nhiều máy chủ lữu chữ chính, được chia sẽ bởi tất cả các pods trong zone đó.
- Bộ nhớ thứ cấp (secondary storage), được chia sẽ bởi tất cả các pods trong zone.



Hình 1.3 Cấu trúc của một zone

Các zones được hiện thị cho người dùng cuối. Khi người dùng khởi động máy ảo khách, người dùng phải chọn một zone cho khách của họ. Người dùng cũng có thể được yêu cầu sao chép các mẫu riêng của họ sang các zones bổ sung để cho phép tạo máy ảo khách sử dụng các mẫu của họ trong các zone đó.

Các zones có thể là công khai hoặc riêng tư. Các zones công khai được hiển thị cho tất cả người dùng. Điều này có nghĩa là bất kỳ người nào cũng có thể tạo khách trong zone đó. Các zones riêng tư được dành riêng cho một miền cụ thể. Chỉ người dùng trong miền đó hoặc miền phụ của miền đó mới có thể tạo khác trong zone đó.

Các máy chủ trong cùng một zone có thể truy cập trực tiếp vào nhau mà không cần phải vượt qua tường lửa (firewall). Các hosts trong các zones khác nhau có thể truy cập lẫn nhau thông qua các đường hầm VPN được định cấu hình tính.

Đối với mỗi zone, quản trị viên phải quyết định những điều sau đây:

- Có bao nhiêu pods để đặt trong mỗi zone.
- Có bao nhiêu clusters để đặt trong mỗi pod.
- Có bao nhiêu hosts để đặt trong mỗi cluster.
- (Tuỳ chọn) Số lượng máy chủ lưu trữ chính cần đặ trong mỗi zone và tổng dung lượn cho các máy chủ lưu trữ này.

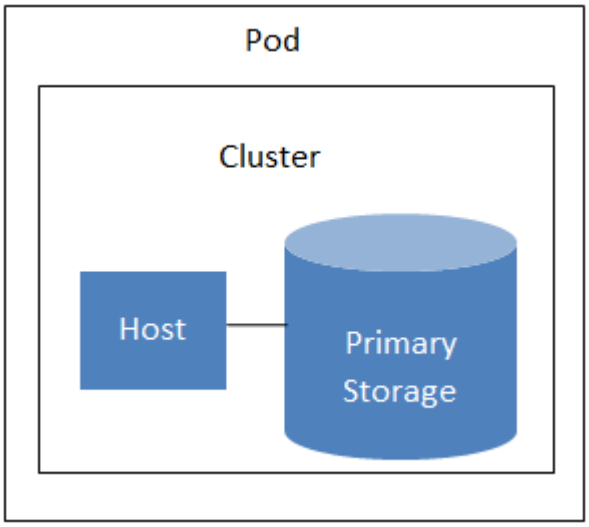
- Có boa nhiêu máy chủ lưu trữ chính cần đặt trong mỗi cluster và tổng dung lượng cho các máy chủ lưu trữ này.
- Có bao nhiêu bộ nhớ thứ cấp để triển khai trong một zone

Khi bạn thêm một zone mới bằng giao diện người dùng CloudStack, bạn sẽ được mặc định cấu hình mạng vật lý của zone đó và thêm pod, cluster, host, primary storage và secondary storage đầu tiên.

Để hỗ trợ các chức năng toàn zone cho VMware, CloudStack biết về Trung tâm dữ liệu VMware và có thể ánh xạ từng Trung tâm dữ liệu tới một zone CloudStack. Để kích hoạt các tính năng như di chuyển trực tiếp lưu trữ và lưu trữ chính trên toàn zone cho các hosts VMware, CloudStack phải đảm bảo rằng một zone chỉ chứa một Trung tâm dữ liệu VMware duy nhất. Do đó, khi bạn đang tạo một zone CloudStack mới, bạn có thể chọn Trung tâm dữ liệu VMware cho zone đó. Nếu bạn đang cung cấp nhiều Trung tâm dữ liệu VMware, mỗi Trung tâm dữ liệu sẽ được thiết lập thành một zone duy nhất trong CloudStack.

1.3.3 Pod

Một pod thường đại diện cho một giá đỡ duy nhất. Các hosts trong cùng một pod nằm trong cùng một mạng con. Pod là đơn vị tổ chức lớn thứ ba trong quá trình triển khai CloudStack. Pods được chứa trong các zones. Mỗi zone có thể chứa một hoặc nhiều pods. Một pod bao gồm một hoặc nhiều cụm máy chủ và một hoặc nhiều máy chủ lưu trữ chính. Người dùng cuối không nhìn thấy các nhóm.



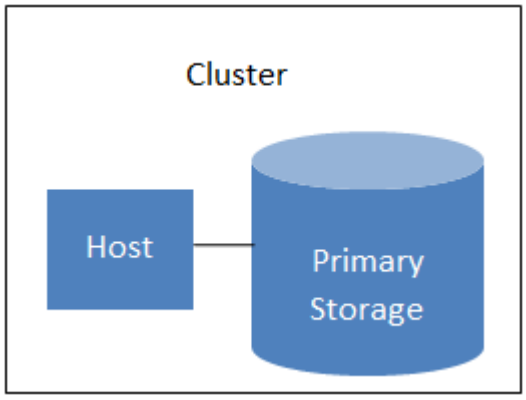
Hình 1.4 Một pod

1.3.4 Cluster

Một cluster cung cấp một cách để nhóm các hosts. Nói một cách chính xác, một cluster là một nhóm hosts XenServer, một tập hợp các máy chủ KVM hoặc một cụm VMware được cấu hình sẵn trong vCenter. Các hosts trong một cụm đều có phần cứng giống nhau, chạy cùng một trình giám sát, nằm trên cùng một mạng con và truy cập vào cùng một bộ nhớ chính được chia sẻ. Các phiên bản máy ảo (VM) có thể được di chuyển trực tiếp từ host này sang host khác trong cùng một cluster mà không làm gián đoạn dịch vụ cho người dùng.

Một cluster là đơn vị tổ chức lớn thứ tư trong quá trình triển khai CloudStack. Các cluster được chứa trong các pods và các pods được chứa trong các zones. Kích thước của cluster bị giới hạn bởi trình giám sát bên dưới.

Một cluster bao gồm một hoặc nhiều hosts và một hoặc nhiều máy chủ lưu trữ chính.



Hình 1.5 Một cluster

CloudStack cho phép nhiều cluster trong một triển khai đám mây.

Ngay cả khi bộ nhớ cục bộ được sử dụng riêng, các cluster vẫn được yêu cầu về mặt tổ chức, ngay cả khi chỉ có một host cho mỗi cluster.

Khi VMware được sử dụng, mọi cluster VMware được quản lý bởi một máy chủ vCenter. Quản trị viên phải đăng ký máy chủ vCenter với CloudStack. Có thể có nhiều máy chủ vCenter trên mỗi zone. Mỗi máy chủ vCenter có thể quản lý nhiều cluster VMware.

1.3.5 Host

Host là một máy tính duy nhất. Hosts cung cấp tài nguyên máy tính chạy các máy ảo khách. Mỗi host đều được cài đặt phần mềm siêu giám sát để quản lý các máy ảo khách. Ví dụ: host có thể là máy chủ Citrix XenServer, một host có thể hỗ trợ KVM Linux, máy chủ ESXi hoặc máy chủ Windows Hyper-V.

Host là đơn vị tổ chức nhỏ nhất trong quá trình triển khai CloudStack. Các hosts được chứa trong các clusters, các clusters được chứa trong các pods, các pods được chứa trong các zones và các zones có thể được chứa trong các regions.

Host trong triển khai CloudStack:

- Cung cấp tài nguyên CPU, bộ nhớ, bộ nhớ và mạng cần thiết để lưu trữ các máy ảo
- Kết nối bằng mạng TCP / IP băng thông cao và kết nối với Internet
- Có thể cư trú tại nhiều trung tâm dữ liệu trên các vị trí địa lý khác nhau
- Có thể có các dung lượng khác nhau (tốc độ CPU khác nhau, số lượng RAM khác nhau, v.v.), mặc dù các hosts trong một cluster phải đồng nhất

Các hosts bổ sung có thể được thêm vào bất kỳ lúc nào để cung cấp thêm dung lượng cho các máy ảo khách.

CloudStack tự động phát hiện lượng tài nguyên CPU và bộ nhớ do hosts cung cấp.

Hosts không hiển thị cho người dùng cuối. Người dùng cuối không thể xác định hosts khách của họ đã được chỉ định.

Để hosts hoạt động trong CloudStack, bạn phải thực hiện những việc sau:

- Cài đặt phần mềm hypervisor trên host
- Gán địa chỉ IP cho host
- Đảm bảo host được kết nối với máy chủ quản lý CloudStack.

1.3.6 Primary Storage

Bộ nhớ chính được liên kết với một cluster và nó lưu trữ các đĩa ảo cho tất cả các máy ảo đang chạy trên các hosts trong cluster đó. Trên KVM và VMware, bạn có thể cung cấp bộ nhớ chính trên cơ sở từng zone.

Bạn có thể thêm nhiều máy chủ lưu trữ chính vào một cluster hoặc zone. Ít nhất một cái được yêu cầu. Nó thường nằm gần host để tăng hiệu suất. CloudStack quản lý việc phân bổ các đĩa ảo khách cho các thiết bị lưu trữ chính cụ thể.

Với lưu trữ chính dựa trên cluster, dữ liệu trong bộ nhớ chính chỉ có sẵn trực tiếp cho các máy ảo trong cluster đó. Nếu một máy ảo trong một cluster khác cần một số dữ liệu, thì nó phải được sao chép từ cluster này sang cluster khác, sử dụng bộ nhớ thứ cấp của zone làm bước trung gian. Thao tác này có thể tốn thời gian một cách không cần thiết.

CloudStack được thiết kế để hoạt động với tất cả các máy chủ iSCSI và NFS tuân thủ tiêu chuẩn được hỗ trợ bởi trình siêu giám sát bên dưới, bao gồm:

- SolidFire cho iSCSI
- Dell EqualLogic ™ dành cho iSCSI
- Trình tập tin Thiết bị mạng cho NFS và iSCSI
- Tính toán quy mô cho NFS

1.3.7 Secondary Storage

Bộ nhớ thứ cấp lưu trữ những thứ sau:

- Mẫu – Hình ảnh hệ điều hành có thể được sử dụng để khởi động máy ảo và có thể bao gồm thông tin cấu hình bổ sung, chẳng hạn như các ứng dụng đã cài đặt
- Hình ảnh ISO – hình ảnh đĩa chứa dữ liệu hoặc phương tiện có thể khởi động cho hệ điều hành
- Ảnh chụp nhanh dung lượng đĩa – các bản sao đã lưu của dữ liệu VM có thể được sử dụng để khôi phục dữ liệu hoặc để tạo các mẫu mới.

Các mục trong bộ nhớ thứ cấp có sẵn cho tất cả các hosts trong phạm vi của bộ nhớ phụ, có thể được xác định theo zone hoặc theo region.

Để cung cấp các mục trong bộ nhớ thứ cấp cho tất cả các hosts trên toàn bộ đám mây, bạn có thể thêm bộ nhớ đối tượng ngoài kho lưu trữ thứ cấp NFS dựa trên zone. Không cần thiết phải sao chép các mẫu và ảnh chụp nhanh từ zone này sang vùng khác, như yêu cầu khi sử dụng riêng zone NFS. Mọi thứ đều có sẵn ở mọi nơi.

Đối với máy chủ Hyper-V, lưu trữ SMB / CIFS được hỗ trợ.

CHƯƠNG 2. CÁC SERVER CẤU THÀNH NÊN CLOUD

2.1 Management server là gì?

2.1.1 Tại sao management server lại được sử dụng ?

Quản lý và giám sát một máy chủ đám mây riêng yêu cầu các công cụ phần mềm giúp tạo ra một nhóm tài nguyên máy tính được ảo hóa, cung cấp cổng tự phục vụ cho người dùng cuối và xử lý bảo mật, phân bổ tài nguyên, theo dõi và thanh toán. Lúc đấy management server sẽ đảm nhiệm công việc đó.

Management Server thông thường sẽ chạy trên một máy tính chuyên biệt hoặc cũng có thể là máy ảo, ở đây nhóm chạy management server trên máy thực với IP là 192.168.1.10. Management Server của apache CloudStack chạy trên Apache tomcat server và cần một MySQL Database.

2.1.2 Vai trò chính của management server

Management Sever có những vai trò sau đây:

- Cung cấp dạo diện UI cho người dùng cuối cũng như Admin
- Quản lý việc phân công máy ảo khách cho host chứa tài nguyên Cloud
- Quản lý việc phân công các public và private IP
- Quản lý các disk images hay ISO images của máy ảo khách được lưu trong Secondary Storage

2.2 Hypervisor (KVM)

2.2.1 Hypervisor

Hypervisor hay còn gọi là phần mềm giám sát máy ảo: Là một chương trình phần mềm quản lý một hoặc nhiều máy ảo (VM). Nó được sử dụng để tạo, startup, dừng và reset lại các máy ảo. Các hypervisor cho phép mỗi VM hoặc “guest” truy cập vào lớp tài nguyên phần cứng vật lý bên dưới, chẳng hạn như CPU, RAM và lưu trữ. Nó cũng có thể giới hạn số lượng tài nguyên hệ thống mà mỗi máy ảo có thể sử dụng để đảm bảo cho nhiều máy ảo cùng sử dụng đồng thời trên một hệ thống. Hay nói một cách tổng

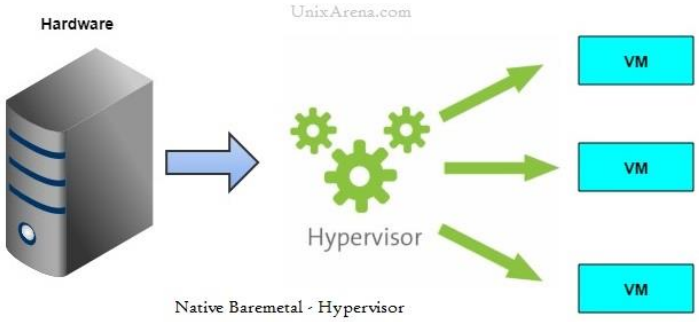
quát Hypervisor là các phần mềm công nghệ để tạo máy ảo và giám sát, điều khiển máy ảo.

Có 2 loại hypervisor là Native (hay còn gọi là Bare metal) và Host Based.

Loại-1: Native

Một hypervisor ở dạng native (hay còn gọi "bare-metal") chạy trực tiếp trên phần cứng. Nó nằm giữa phần cứng và một hoặc nhiều hệ điều hành khách (guest operating system). Nó được khởi động trước cả hệ điều hành và tương tác trực tiếp với kernel. Điều này mang lại hiệu suất cao nhất có thể vì không có hệ điều hành chính nào cạnh tranh tài nguyên máy tính với nó. Tuy nhiên, nó cũng đồng nghĩa với việc hệ thống chỉ có thể được sử dụng để chạy các máy ảo vì hypervisor luôn phải chạy ngầm bên dưới.

Các hypervisor dạng native này có thể kể đến như VMware ESXi, Microsoft Hyper-V và Apple Boot Camp.

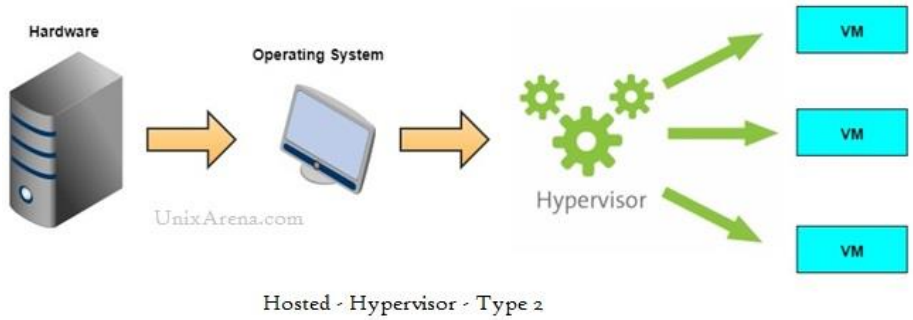


Hình 2.1 Native Baremental Hypervisor

Loại-2: Hosted

Một hypervisor dạng hosted được cài đặt trên một máy tính chủ (host computer), mà trong đó có một hệ điều hành đã được cài đặt. Nó chạy như một ứng dụng cũng như các phần mềm khác trên máy tính. Hầu hết các hypervisor dạng hosted có thể quản lý và chạy nhiều máy ảo cùng một lúc. Lợi thế của một hypervisor dạng hosted là nó có thể được bật lên hoặc thoát ra khi cần thiết, giải phóng tài nguyên cho máy chủ. Tuy nhiên, vì chạy bên trên một hệ điều hành, nó có thể đem lại hiệu suất tương tự như một hypervisor ở dạng native.

Ví dụ về các hypervisor dạng hosted bao gồm VMware Workstation, Oracle VirtualBox và Parallels Desktop for Mac.



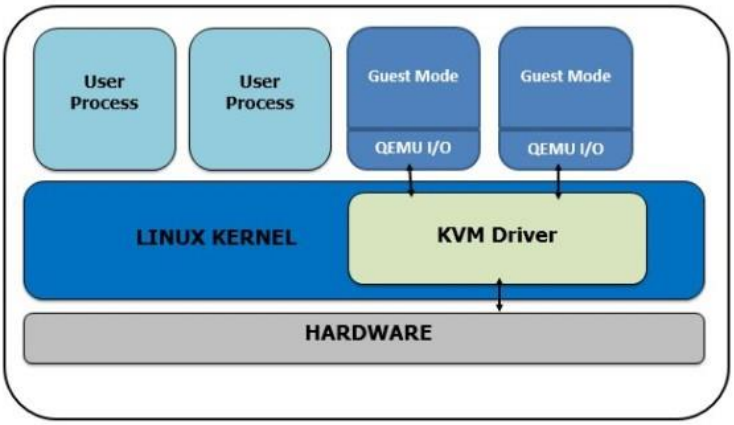
Hình 2.2 Hosted Hypervisor

2.2.2 KVM

KVM (Kernel-based Virtual Machine) được biết đến là một cơ sở hạ tầng ảo hóa cho nhân Linux dành cho những CPU hỗ trợ công nghệ ảo hóa như Intel VT hoặc ADM-V.

KVM ra đời phiên bản đầu tiên vào năm 2007 bởi công ty Qumranet tại Isarel, KVM được tích hợp sẵn vào nhân của hệ điều hành Linux bắt đầu từ phiên bản 2.6.20. Năm 2008, RedHat đã mua lại Qumranet và bắt đầu phát triển, phổ biến KVM Hypervisor.

KVM đi liền với QEMU. QEMU là 1 hyperviosr hoàn chỉnh thuộc loại 2 có khả năng giả lập tài nguyên phần cứng, trong đó bao gồm 1 CPU ảo.



Hình 2.3 KVM nằm trong kernel giao tiếp QEMU và phần cứng

KVM có một số đặc điểm sau:

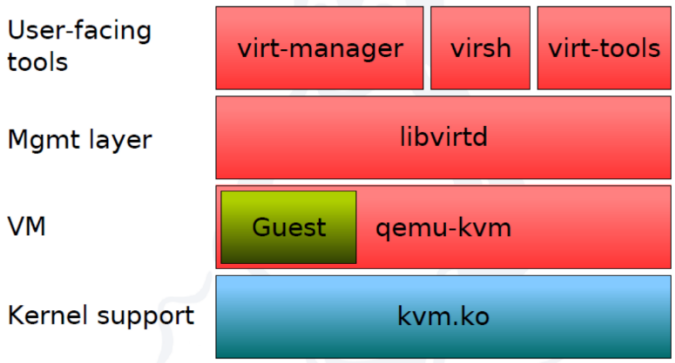
- Là giải pháp ảo hóa dạng toàn phần và hoàn toàn nguồn mở, miễn phí.
- Hỗ trợ các loại công nghệ phần cứng đa dạng và thông dụng như Intel-VT, AMD-V

- Cung cấp các máy ảo đa dạng, hỗ trợ nhiều loại hệ điều hành và không cần tinh chỉnh lại các ảnh của hệ điều hành
- Sử dụng cơ chế quản lý vùng nhớ của Linux (KSM) và các cơ chế bảo mật có sẵn của Linux (SELinux)

Với ưu điểm nguồn mở và độ tùy biến cao, KVM hypervisor được lựa chọn là nền tảng ảo hóa chính khi lựa chọn công nghệ ảo hóa nguồn mở. KVM cũng đồng thời là nền tảng của giải pháp điện toán đám mây nguồn mở nổi tiếng nhất hiện nay là OpenStack hoặc CloudStack.

2.2.2.1 KVM Stack

KVM Stack bao gồm 4 tầng:



Hình 2.4 KVM Stack

- Tầng User-facing tools: là các công cụ quản lý máy ảo hỗ trợ KVM. Các công cụ có giao diện đồ họa như virt-manager hay có giao diện dòng lệnh như virsh
- Tầng Management layer: là thư viện libivrt cung cấp API để các công cụ quản lý máy ảo hay hypervisor tương tác với KVM để thực hiện các thao tác quản lý tài nguyên ảo hóa, vì tự thân KVM không hề có khả năng giả lập tài nguyên như vậy.
- Tầng Virtual machine: chính là các máy ảo mà người dùng tạo ra.
- Tầng Kernel support: cung cấp 1 module làm hạt nhân cho hạ tầng ảo hóa mà 1 module đặc biệt hỗ trợ các vi xử lý VT-X và AMD-V

2.2.2.2 Kiến trúc của KVM

a) Về tính bảo mật

Trong kiến trúc KVM, máy ảo được xem như các tiến trình Linux thông thường, nhờ đó nó tận dụng được mô hình bảo mật của hệ thống Linux như SELinux, cung cấp khả năng cô lập và kiểm soát tài nguyên

SVirt project - dự án cung cấp giải pháp bảo mật MAC (Mandatory Access Control - Kiểm soát truy cập bắt buộc) tích hợp với hệ thống ảo hóa sử dụng SELinux để cung cấp một cơ sở hạ tầng cho phép người quản trị định nghĩa nên các chính sách để cô lập các máy ảo.

b) Về việc quản lý vùng nhớ

KVM thừa kế tính năng quản lý bộ nhớ mạnh mẽ của Linux. Vùng nhớ của máy ảo được lưu trữ trên cùng một vùng nhớ dành cho các tiến trình Linux khác và có thể swap. KVM hỗ trợ NUMA (Non-Uniform Memory Access - bộ nhớ thiết kế cho hệ thống đa xử lý) cho phép tận dụng hiệu quả vùng nhớ kích thước lớn.

c) Về mặt lưu trữ

KVM có khả năng sử dụng bất kỳ giải pháp lưu trữ nào hỗ trợ bởi Linux để lưu trữ các Images của các máy ảo, bao gồm các ổ cục bộ như IDE, SCSI và SATA, Network Attached Storage (NAS) bao gồm NFS và SAMBA/CIFS, hoặc

SAN thông qua các giao thức iSCSI và Fibre Channel.

KVM cũng hỗ trợ các images của các máy ảo trên hệ thống tệp tin chia sẻ như GFS2 cho phép các images có thể được chia sẻ giữa nhiều host hoặc chia sẻ chung giữa các ổ logic.

d) Về mặt hiệu năng

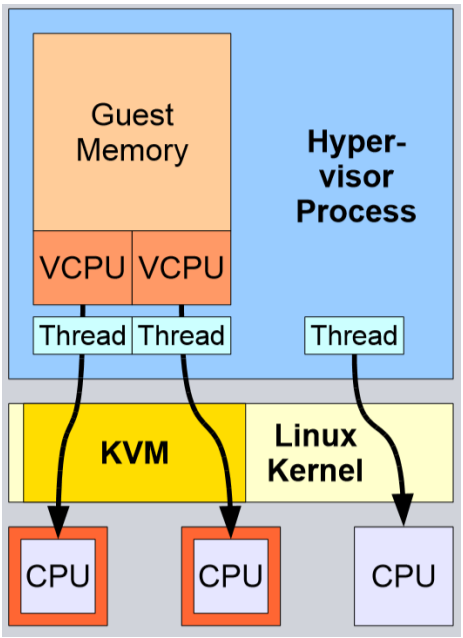
KVM kế thừa hiệu năng và khả năng mở rộng của Linux, hỗ trợ máy ảo với 16 CPUs ảo, 256GB RAM và hệ thống máy host lên tới 256 cores và trên 1TB RAM.

e) Về mặt khả năng tương thích với các môi trường

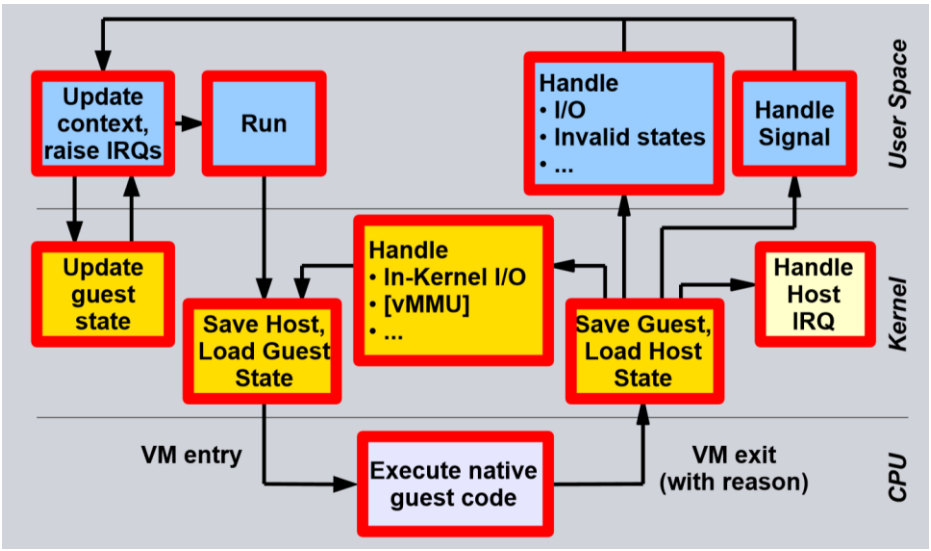
KVM hỗ trợ live migration cung cấp khả năng di chuyển ác máy ảo đang chạy giữa các host vật lý mà không làm gián đoạn dịch vụ. Khả năng live migration là trong suốt

với người dùng, các máy ảo vẫn duy trì trạng thái bật, kết nối mạng vẫn đảm bảo và các ứng dụng của người dùng vẫn tiếp tục duy trì trong khi máy ảo được đưa sang một host vật lý mới. KVM cũng cho phép lưu lại trạng thái hiện tại của máy ảo để cho phép lưu trữ và khôi phục trạng thái đó vào lần sử dụng tiếp theo.

f) Luồng hoạt động của mô hình KVM



Hình 2.5 Luồng hoạt động của mô hình KVM

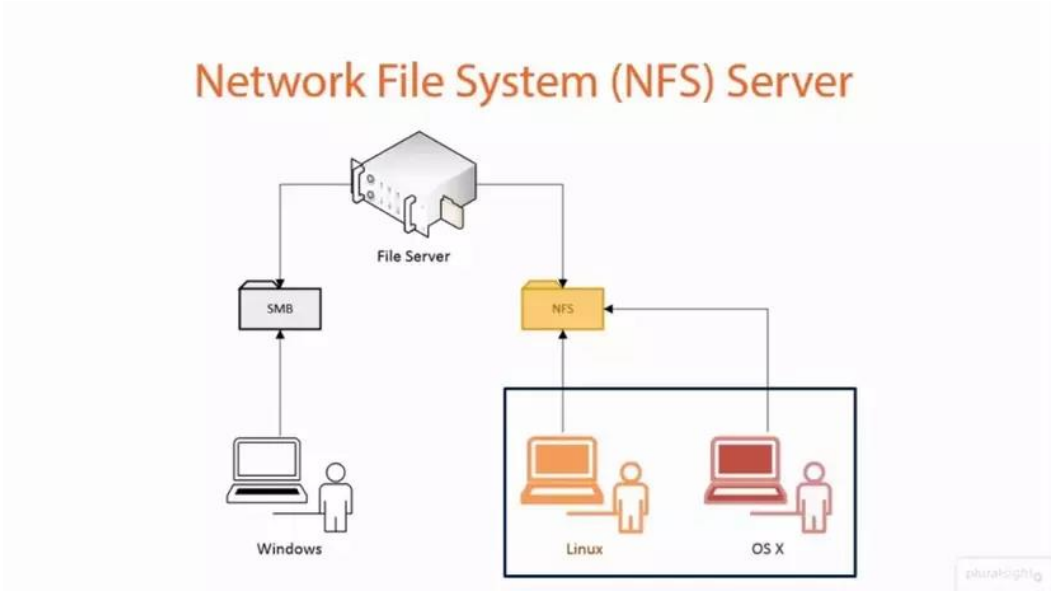


Hình 2.6 Luồng hoạt động của mô hình KVM

2.3 Network File System (NFS)

2.3.1 NFS server là gì?

NFS (Network File System) là một hệ thống giao thức chia sẻ file phát triển bởi Sun Microsystems từ năm 1984, cho phép một người dùng trên một máy tính khách truy cập tới hệ thống file chia sẻ thông qua một mạng máy tính giống như truy cập trực tiếp trên ổ cứng.



Hình 2.7 Network File System (NFS)

2.3.2 Những tính năng của NFS là gì?

NFS có những tính năng như sau:

- NFS cho phép truy cập cục bộ đến các tệp từ xa, cho phép nhiều máy tính sử dụng cùng một tệp để mọi người trên mạng có thể truy cập vào cùng một dữ liệu
- Với sự trợ giúp của NFS, chúng ta có thể cấu hình các giải pháp lưu trữ tập trung.
- Giảm chi phí lưu trữ bằng cách để các máy tính chia sẻ ứng dụng thay vì cần dung lượng ổ đĩa cục bộ cho mỗi ứng dụng của người dùng
- Giảm chi phí quản lý hệ thống và minh bạch hệ thống tập tin
- Cung cấp tính nhất quán và độ tin cậy của dữ liệu vì tất cả người dùng đều có thể đọc cùng một bộ tệp

- Có thể bảo mật với Firewalls và Kerberos

2.3.3 Cách hoạt động

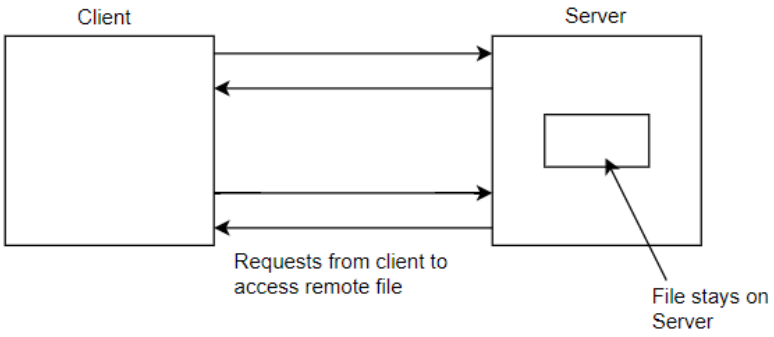
Để truy cập dữ liệu được lưu trữ trên 1 máy chủ, server sẽ triển khai các quy trình nền NFS để cung cấp dữ liệu cho khách hàng. Quản trị viên máy chủ xác định những gì cần cung cấp và đảm bảo có thể nhận ra các máy khách được xác nhận.

Từ client, yêu cầu quyền truy cập vào dữ liệu đã xuất, bằng cách sử dụng lệnh mount.

Server NFS tham chiếu tệp cấu hình /etc/export để xác định xem máy khách có được phép truy cập vào bất kỳ hệ thống nào không. Sau khi xác minh, tất cả hoạt động tập tin và thư mục được phép sử dụng trên Client.

a) Mô hình truy cập từ xa :

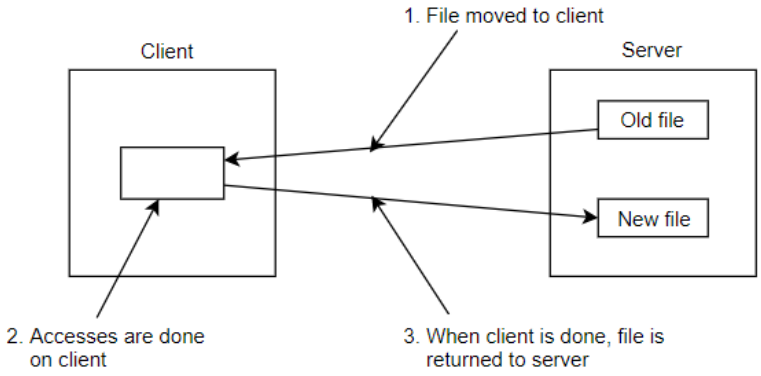
Client sẽ gửi yêu cầu từ xa để truy cập file trên Server



Hình 2.8 Mô hình truy cập từ xa

b) Mô hình tải lên tải xuống :

Client sẽ tải xuống old file để truy cập và thực hiện trên client, khi client thực hiện xong, file sẽ được tải về server.



Hình 2.9 Mô hình tải lên tải xuống

2.3.4 Ưu, nhược điểm

Ưu điểm :

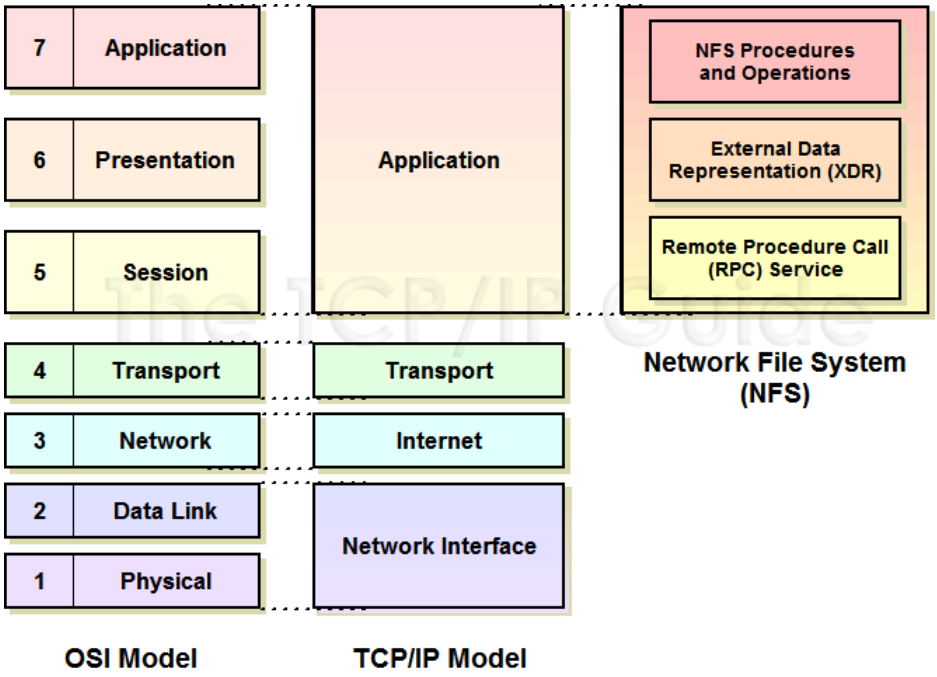
- NFS là 1 giải pháp chi phí thấp để chia sẻ tệp mạng.
- Dễ cài đặt vì nó sử dụng cơ sở hạ tầng IP hiện có
- Cho phép quản lý trung tâm, giảm nhu cầu thêm phần mềm cũ và dụng lượng đĩa trên các hệ thống người dùng cá nhân

Nhược điểm :

- NFS vốn không an toàn, chỉ nên sử dụng trên 1 mạng đáng tin cậy sau Firewall
- NFS bị chậm trong khi lưu lượng mạng lớn
- Client và server tin tưởng lẫn nhau vô điều kiện
- Tên máy chủ có thể là giả mạo (tự xưng là máy khác)

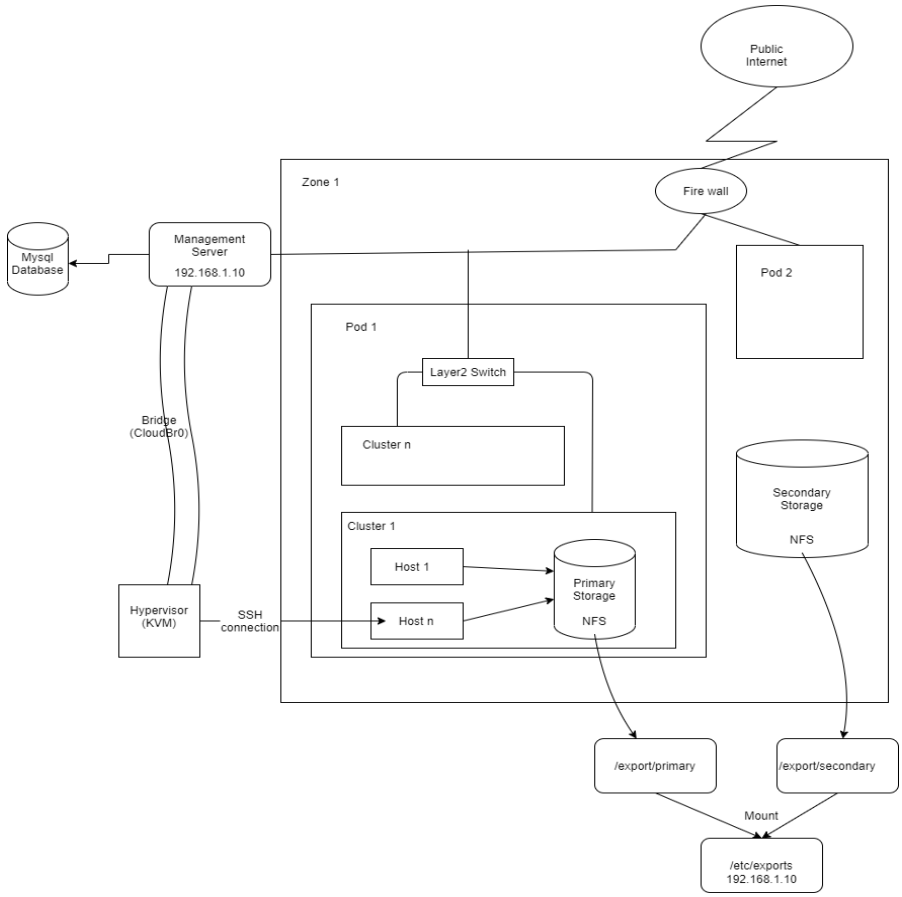
2.3.5 Các leyers NFS

- RPC leyer: Chuyển giữ liệu giữa các máy chủ [RFC 3010]
- XDR layer: Cung cấp tính độc lập của dữ liệu cho máy [RFC 1832]
- Lớp trên cùng bao gồm giao thức mount và giao thức NFS



Hình 2.10 Các Layers của NFS

2.4 Kiến trúc tổng quan Cloud Stack



Hình 2.11 Kiến trúc tổng quan CloudStack

CloudStack bao gồm 3 server chính : Management server, NFS server và KVM server. Thông thường với mục đích thương mại các server trên sẽ được cài đặt trên 3 phần cứng chuyên dụng khác nhau trong cũng một mạng LAN. Khi đó management server sẽ kết nối với KVM hypervisor qua SSH connection, trong khi NFS server sẽ cung cấp storage và mount đến management server tạo thành một kiến trúc hoàn chỉnh.

Nhưng với mục đích demo và test cũng như không đủ thiết bị phần cứng, 3 server trên vẫn có thể chạy trên cùng một thiết bị.Việc kết nối vẫn phải đảm bảo là KVM kết nối với Management server bằng ssh trên port 22. NFS server sẽ không mount share giữa 2 thiết bị mà là trên cũng một thiết bị với các đường dẫn được cấu hình trước.

Cấu trúc bên trong cloud sẽ được phân cấp từ Zone -> Host. Host là một máy tính chạy KVM hypervisor vừa cho phép giám sát các máy ảo sẽ deploy sau này vừa cung cấp tài nguyên tính toán. Trong khi đó tài nguyên lưu trữ sẽ được cung cấp bởi Primary storage và Secondary storage thông qua NFS server. Management server có vai trò cung cấp UI cho admin và User cũng như quản lý toàn bộ hệ thống.

CHƯƠNG 3. CÀI ĐẶT CLOUDSTACK MANAGEMENT, KVM HYPERVISOR VÀ NFS SERVER

3.1 Cài đặt Cloudstack management server

3.1.1 Cấu hình mạng bridges cho KVM

Thông thường KVM hypervisor sẽ được cái đặt trên một phần cứng riêng biệt với management server. Nhưng với mục đích demo và test của cloud, KVM server có thể chạy trên cùng một thiết bị với management server và dùng chung một mạng vật lý. Do đó trước tiên chúng ta phải cấu hình mạng của máy tính theo mode bridges(bắc cầu) để đồng thời KVM cũng như Management server có thể sử dụng được. Chúng ta sẽ cấu hình một địa chỉ IP chung cho 2 server trên là : 192.168.1.10 và là static IP. Đối với mạng wireless hay mạng ethernet sẽ có đôi chút khác biệt. Với ubuntu 20.04 ta có thể dễ dàng cấu hình mạng cho máy tính bằng cách sửa đổi file /etc/netplan/01-netcfg.yaml

File trên được định dạng yaml với quy tắc lùi dòng phân cấp do đó ta dễ dàng đọc và cấu hình.

3.1.2 Cấu hình mạng cho mạng wireless

Với mạng wireless đầu tiên cài package bridges-utils

```
$ sudo apt-get install bridge-utils
```

Sau đấy chỉnh sửa file yaml trong netplan với nội dung sau:

```
network:
  version: 2
  renderer: networkd
  wifis:
    wlp3s0:
      dhcp4: no
      dhcp6: no
      addresses: [192.168.1.10/24]
      gateway4: 192.168.1.1
      access-points:
        "Tên wifi":
          password: "***********"
  bridges:
   br0:
    dhcp4: no
    addresses: [192.168.1.10/24]
    interfaces: [wlp3s0]
```

```
    parameters:
      stp: true
      forward-delay: 4
```

Ở đây wlp3s0 là tên interface wireless trên máy tính một số máy có thể thay đổi vd: wlp0s3… Chữ " wl" là viết tắt của wireless còn p0 s3 chỉ các slot mạng .

Với "br0" là tên mạng bridge .

Thứ tự lùi dòng phải theo thứ hạng đảm bảo quy tắc một file .yaml

Sau khi cấu hình xong ta lưu lại và restart để mạng bắt đầu hoạt động theo mode bridges

```
$sudo netplan generate
$sudo netplan apply
$sudo reboot
```

Sau khi đã config ta có thể: $ip a để kiểm tra đã xuất hiện mạng bridges chưa

3.1.3 Cấu hình mạng cho mạng ethernet

Với mạng ethernet làm tương tự như mạng wireless với nội dung file .yaml như sau:

network:

```
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: false
      dhcp6: false
      optional: true
  bridges:
    cloudbr0:
      addresses: [192.168.1.10/24]
      gateway4: 192.168.1.1
      nameservers:
        addresses: [1.1.1.1,8.8.8.8]
      interfaces: [enp0s3]
      dhcp4: false
```

```
      dhcp6: false
      parameters:
        stp: false
        forward-delay: 0
```

Ở đây enp0s3 là interface mạng ethernet.

3.2 Cài đặt mysql server

Mỗi một management server cần kết nối với một mysql server thì mới có thể hoạt động được. Mysql server dùng để lưu username password của user cloud.

Đầu tiên tải package mysql:

```
$sudo apt-get install mysql-server
```

Sau đó mở file mysqld.cnf để thực hiện cấu hình:

```
$sudoedit  /etc/mysql/mysql.conf.d/mysqld.cnf
```

Sửa file trên với nội dung như sau:

```
server_id = 1
sql-
mode="STRICT_TRANS_TABLES,NO_ENGINE_SUBSTITUTION,ERROR_FOR_DIVISION_BY_ZE
RO,NO_ZERO_DATE,NO_ZERO_IN_DATE,NO_ENGINE_SUBSTITUTION"
innodb_rollback_on_timeout=1
innodb_lock_wait_timeout=600
max_connections=1000
log-bin=mysql-bin
binlog-format = 'ROW'
```

Sau khi thực hiện xong restart mysql:

```
$sudo systemctl restart mysql
```

3.3 Cài đặt management server và deploy lên local host

Sau các bước cấu hình mạng và cài mysql là các bước tiên quyết để cài management server.

Trước tiên ta đưa đường dẫn tải gói cloudstack management vào file cloudstack.list đã tạo mới.

```
$echodebhttp://download.cloudstack.org/ubuntufocal4.15>ru/etc/apt/sources
.list.d/cloudstack.list
```

Add key :

```
$ sudo wget -O - http://download.cloudstack.org/release.asc| sudo apt-key
add -

$sudo apt-get update
```

Thực hiện cài đặt:

```
$apt-get install -y cloudstack-management cloudstack-usage
```

Sau khi cài đặt xong deploy management server lên local host 192.168.1.10:8080

```
$sudo cloudstack-setup-databases cloud:cloud@localhost --deploy-
as=root:passw0rd
```

Passwor0rd: là password của user root mà ta set trong mysql server mặc định có thể để trống.

Kiểm tra việc deploy đã đúng chưa:

```
$cloudstack-setup-management
```

Quá trình deploy management server vào khoảng 2 tiếng trong thời gian đó file log sẽ được ghi ra liên tục, có thể check nó bằng command sau:

```
$tail -f /var/log/cloudstack/management/management-server.log
```

Sau khi cài xong đã có thể login vào ui cloudstack

http://192.168.1.10:8080/client/#/

Tuy nhiên hiện tại chưa có bất kì hạ tầng hay tài nguyên nào của máy. Để có được ta phải cài KVM hypervisor server .

3.4 Cài đặt KVM hypervisor

Quá trình cài đặt KVM hypervisor bao gồm:

- Chuẩn bị hệ điều hành
- Cài đặt và cấu hình libvirt
- Cấu hình Security Policies (AppArmor và SELinux)

- Cài đặt và cấu hình Agent

Cài đặt KVM host

CloudStack sử dụng libvirt để quản lý các máy ảo. Do đó, điều quan trọng là libvirt phải được định cấu hình chính xác. Libvirt là một phần phụ thuộc của cloudstack-agent và đã được cài đặt sẵn.

Thiết lập các tham số sau trong đường dẫn */etc/libvirt/conf*

```
listen_tls = 0
listen_tcp = 1
tcp_port = "16509"
auth_tcp = "none"
mdns_adv = 0
```

Bật "listening_tcp" trong libvirtd.conf là không đủ, chúng ta cũng phải thay đổi các thông số trong */etc/default/libvirt-bin*

```
env libvirtd_opts="-l"
```

Sau đó Restart libvirt

```
$ service libvirt-bin restart
```

CloudStack thực hiện nhiều thứ khác nhau có thể bị chặn bởi các cơ chế bảo mật như AppArmor và SELinux. Những điều này phải được tắt để đảm bảo Agent có tất cả các quyền cần thiết.

Để cấu hình Apparmor trước tiên cần kiểm tra xem AppArmor đã được cài đặc chưa bằng lệnh: $ dpkg --list 'apparmor' . Sau đó tắt cấu hình AppArmor cho libvirt :

```
$ ln -s /etc/apparmor.d/usr.sbin.libvirtd /etc/apparmor.d/disable/
$ ln -s /etc/apparmor.d/usr.lib.libvirt.virt-aa-helper /etc/apparmor.d/disable/
$ apparmor_parser -R /etc/apparmor.d/usr.sbin.libvirtd
$ apparmor_parser -R /etc/apparmor.d/usr.lib.libvirt.virt-aa-helper
```

CloudStack sử dụng cầu nối mạng kết hợp với KVM để kết nối các cá thể khách với nhau và với thế giới bên ngoài. Chúng cũng được sử dụng để kết nối System VMs với cơ sở hạ tầng (infrastructure). Theo mặc định, những cầu nối này được gọi là cloudbr0,

cloudbr1, …. Điều cần thiết là phải giữ cấu hình nhất quán trên tất cả các trình giám sát của mình. Đã được cấu hình ở phần đầu báo cáo.

Cài đặt KVM, CloudStack agent và cấu hình libvirt:

```
$ apt-get install qemu-kvm cloudstack-agent
```

Bật VNC cho proxy bảng điều khiển:

```
$ sed -i -e 's/\#vnc_listen.*$/vnc_listen = "0.0.0.0"/g' /etc/libvirt/qemu.conf
```

Bật libvirtd trong chế độ nghe:

```
$ sed -i -e 's/.*libvirtd_opts.*/libvirtd_opts="-l"/' /etc/default/libvirtd
```

Cấu hình libvirtd config mặc định:

```
$ echo 'listen_tls=0' >> /etc/libvirt/libvirtd.conf
$ echo 'listen_tcp=1' >> /etc/libvirt/libvirtd.conf
$ echo 'tcp_port = "16509"' >> /etc/libvirt/libvirtd.conf
$ echo 'mdns_adv = 0' >> /etc/libvirt/libvirtd.conf
$ echo 'auth_tcp = "none"' >> /sudoetc/libvirt/libvirtd.conf
$ systemctl restart libvirtd
```

Thiết lập duy nhất UUID máy chủ lưu trữ cụ thể trong cấu hình libvirtd:

```
$ apt-get install uuid
$ UUID=$(uuid)
$ echo host_uuid = \"$UUID\" >> /etc/libvirt/libvirtd.conf
$ systemctl restart libvirtd
```

Đối với Ubuntu phiên bản 20.04, socket/listen dựa trên cấu hình truyền thống có thể không hỗ trợ nên chúng ta có thể dùng bản cũ hơn:

```
$ systemctl mask libvirtd.socket libvirtd-ro.socket libvirtd-admin.socket
libvirtd-   tls.socket libvirtd-tcp.socket
$ systemctl restart libvirtd
```

3.5 Cấu hình firewall

Cấu hình firewall:

```
NETWORK=192.168.1.0/24
```

```
iptables -A INPUT -s $NETWORK -m state --state NEW -p udp --dport 111 -j ACCEPT
iptables -A INPUT -s $NETWORK -m state --state NEW -p tcp --dport 111 -j ACCEPT
iptables -A INPUT -s $NETWORK -m state --state NEW -p tcp --dport 2049 -j ACCEPT
iptables -A INPUT -s $NETWORK -m state --state NEW -p tcp --dport 32803 -j ACCEPT
iptables -A INPUT -s $NETWORK -m state --state NEW -p udp --dport 32769 -j ACCEPT
iptables -A INPUT -s $NETWORK -m state --state NEW -p tcp --dport 892 -j ACCEPT
iptables -A INPUT -s $NETWORK -m state --state NEW -p tcp --dport 875 -j ACCEPT
iptables -A INPUT -s $NETWORK -m state --state NEW -p tcp --dport 662 -j ACCEPT
iptables -A INPUT -s $NETWORK -m state --state NEW -p tcp --dport 8250 -j ACCEPT
iptables -A INPUT -s $NETWORK -m state --state NEW -p tcp --dport 8080 -j ACCEPT
iptables -A INPUT -s $NETWORK -m state --state NEW -p tcp --dport 9090 -j ACCEPT
iptables -A INPUT -s $NETWORK -m state --state NEW -p tcp --dport 16514 -j ACCEPT
```

```
$apt-get install iptables-persistent
```

```
# Disable apparmour on libvirtd
ln -s /etc/apparmor.d/usr.sbin.libvirtd /etc/apparmor.d/disable/
ln -s /etc/apparmor.d/usr.lib.libvirt.virt-aa-helper /etc/apparmor.d/disable/
apparmor_parser -R /etc/apparmor.d/usr.sbin.libvirtd
apparmor_parser -R /etc/apparmor.d/usr.lib.libvirt.virt-aa-helper
```

3.6 Cài nfs server, setup storage

Có hai cách để cài nfs server, cách đầu tiên là cài nfs server tách biệt với management server trên một phần cứng khác và mount đến management server. Ở đây nhóm sử dụng cách thứ hai là management server hoạt động như một nfs server có nghĩa là nfs server sẽ được cài lên cùng với management server trên cùng một thiết bị.

Đầu tiên install nfs server:

```
$apt-get install nfs-kernel-server quota
```

Tạo export:

```
$echo "/export  *(rw,async,no_root_squash,no_subtree_check)" > /etc/exports
```

Tạo hai đường dẫn mới một cho primary storage và một cho secondary storage:

```
$mkdir -p /export/primary /export/secondary
```

Tiến hành export:

```
$exportfs -a
```

Sau khi export hai đường dẫn mới đã được mount tới server nfs, sau này ta sẽ deploy hai đường dẫn này cho hai vùng lưu trữ primary storage và secondary storage của zone.

CHƯƠNG 4. DEPLOY MỘT ADVANCED ZONE HOÀN CHỈNH VÀ CHẠY CÁC MÁY ẢO TRÊN ZONE VỪA TẠO

4.1 Tạo advanced Zone

4.1.1 Setup zone

Sau khi đã login vào ui, đi tới infracstructure > zone click add Zone chọn Advanced và cung cấp các thông số sau:

Advanced Zone giúp cho việc định nghĩa các guest network một cách linh hoạt hơn Basic Zone:

- Name – bất kì
- Public DNS 1 - 8.8.8.8 (goole DNS)
- Internal DNS1 - 192.168.1.1 (IP gateway của máy tính)
- Hypervisor – KVM

4.1.2 Setup network

Cấu hình public traffic

Public traffic được tạo ra khi các máy ảo kết nối tới mạng internet.

- Gateway - 192.168.1.1
- Netmask - 255.255.255.0
- VLAN/VNI - (leave blank for vlan://untagged or in case of VXLAN use vxlan://untagged)
- Start IP - 192.168.1.20
- End IP - 192.168.1.50

Start-End IP là một loạt các địa chỉ IP có thể truy cập được từ Internet và sẽ được cấp phát để truy cập vào các guest VMs(máy ảo khách mà sao này sẽ chạy khi deploy Zone hoàn chỉnh)

4.1.3 Setup Pod

- Name – bất kì

- Gateway - 192.168.1.1
- Reserved system netmask – 255.255.255.0 (mặt nạ mạng cho phép định nghĩa mạng con trong Pod dùng quy tắc đánh theo CIDR)
- Start/end reserved system IPs - 192.168.1.51 - 192.168.1.80 (Một loạt các IP trong mạng quản lý cho phép CloudStack quản lý các loại System VMS (máy ảo hệ thống như là secondary Storage VM…)

Cấu hình Guest traffic (thông lượng khách)

- VLAN/VNI range: 700-900

4.1.4 Thêm tài nguyên máy tính cho Zone

Setup Cluster

- Name - bất kì
- Hypervisor - Choose KVM

Đưa KVM lên host

KVM sẽ giám sát các máy ảo được deploy lên Zone sau này

KVM cũng đồng thời cung cấp tài nguyên phần cứng nơi mà nó đang chạy (cùng 1 server với management server 192.168.1.10)

- Hostname - 192.168.1.10
- Username - root
- Password - <Mật khẩu của Root User >

Lưu ý phải Cài đặt Ssh server và kích hoạt cho phép root User sử dụng password trên KVM host.

SSH đảm bảo việc KVM và Management server kết nối được với nhau.Thông thường KVM Cũng như Management server sẽ được cài tách biệt trên hai phần cứng tuy nhiên với mục đích Test và Demo ta vẫn có thể cài cả hai trên 1 thiết bị nhưng vẫn cần SSH để kêt nối trên port 22.

Sau khi Setup Host thành công đã có KVM công việc còn lại là thiết lập 2 vùng lưu trữ Primary và Secondary Storage.

4.1.5 Primary Storage Setup

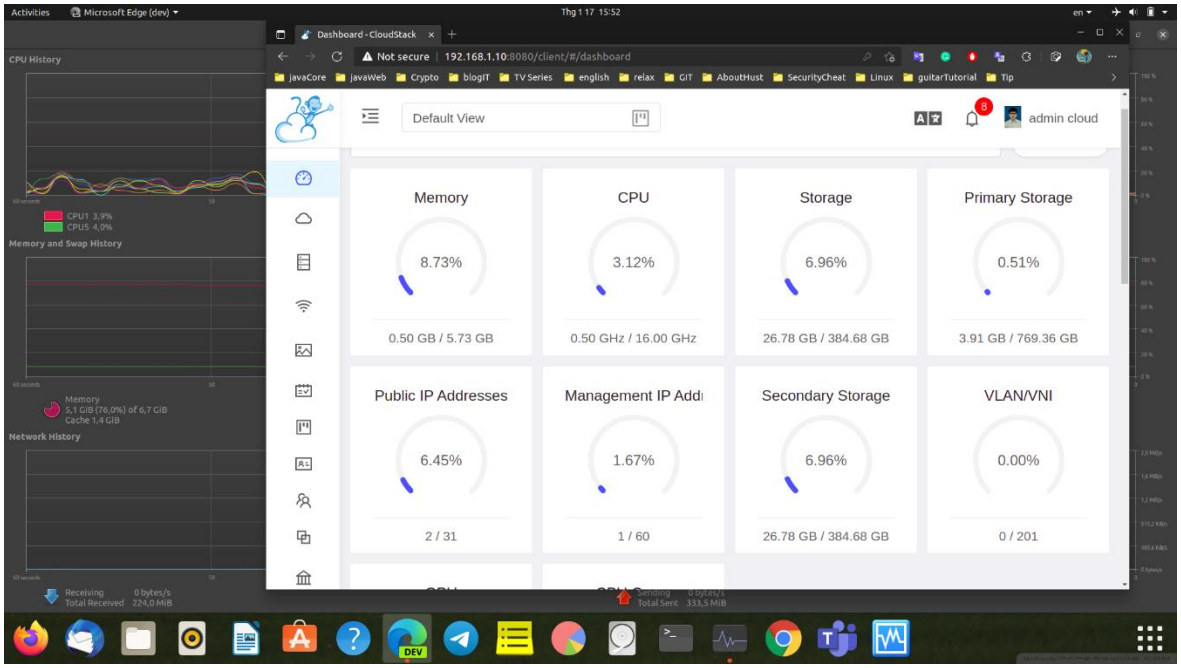
- Name – bất kì
- Scope - zone
- Protocol - NFS
- Server - 192.168.1.10 (nfs đang được cài trên cùng server với management server)
- Path - /export/primary (đường dẫn mount share đã được cấu hình từ trước)

4.1.6 Secondary Storage Setup

Tương tự như Primary Storage

- Provider - NFS
- Name - any name
- Server - 192.168.1.10
- Path - /export/secondary

Sau khi cài đặt các thành phần cần thiết ần Launch Zone và Các thông số phần cứng máy tính đã được deploy lên Zone.

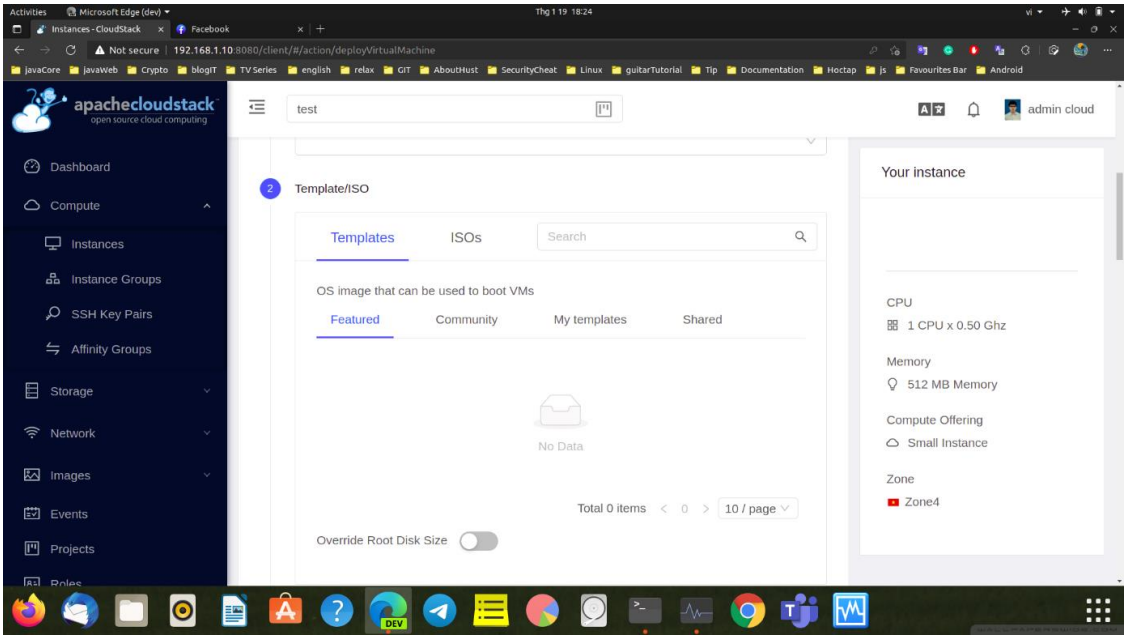


Hình 4.1 Thông số phần cứng được đưa lên Host

4.2 Deploy máy ảo lên Zone đã tạo

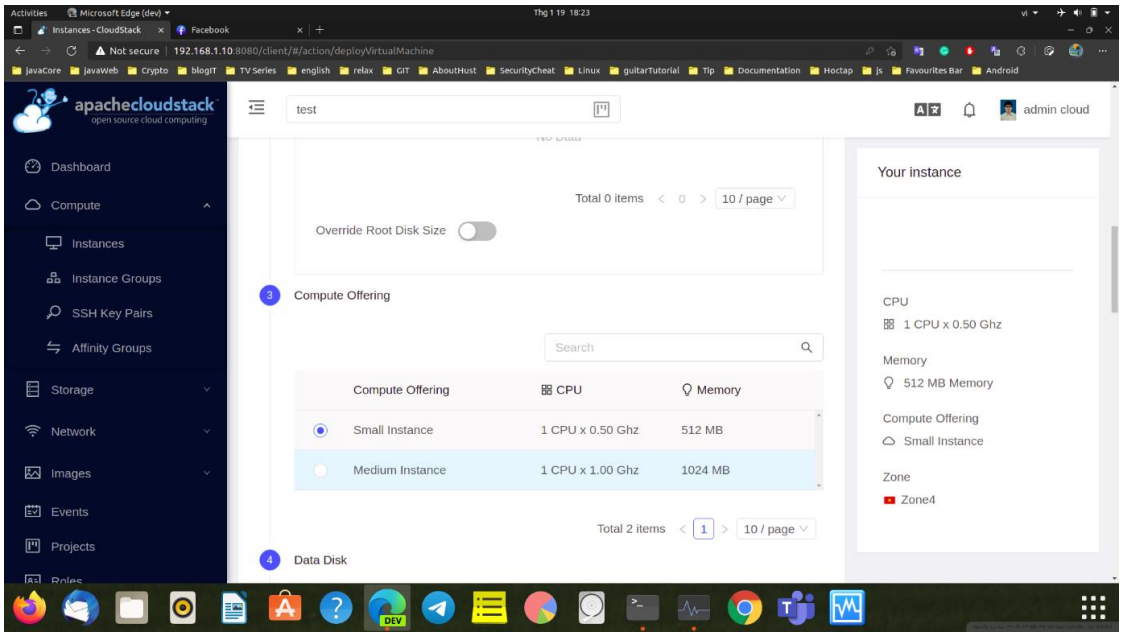
Việc Khởi chạy máy ảo trên Zone Chúng ta cần System VMS Template hoặc một ISO images hiểu đơn giản thì chúng là những images của một hệ điều hành mà ta cần cài cho máy ảo giống như virtual Box.

Đầu tiên ta chọn template vms hoặc ISO images đã được tải về giải nén và đưa vào secondary Storage. Ở đây hiện tại chưa có ISO images nào



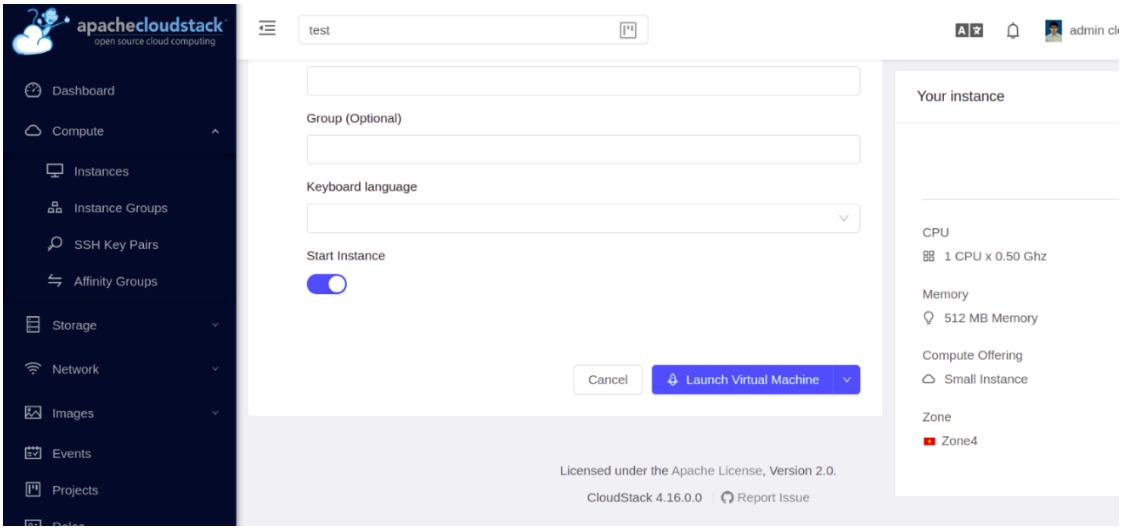
Hình 4.2 Chọn ISO Imgae cho máy ảo

Sau đó ta có thể cấp phát tùy ý tài nguyên của Zone mà ta vừa tạo:



Hình 4.3 Tuỳ chỉnh tài nguyên cho máy ảo

Cuối cùng là bước launch VMS trên Zone:



Hình 4.4 Launch VMS

Do vẫn có lỗi chưa thể thêm được VMS template nên phần chạy máy ảo trên nhóm sẽ cố gắng thực hiện trong tương lai.

Với kiến trúc 3 server chuyên biệt của CloudStack, một Datacenter có thể giảm thiểu số lượng máy tính vật lý xuống còn 3 máy mà vẫn đảm bảo có thể chạy được vô số máy ảo trên tài nguyên có sẵn.

CHƯƠNG 5. KẾT LUẬN

5.1 Kết luận chung

Qua đề tài xây dựng private Iaas Cloud với Cloud Stack và KVM hypervisor nhóm đã có them rất nhiều kiến thức về hệ điều hành ubuntu 20.04, về cách thức cấu hình mạng trong Ubuntu và cách Nfs server cũng như KVM server hoạt động. Bên cạnh những kiến thức nhỏ lẻ cụ thể chúng em còn hiểu hơn về kiến trúc tổng quan của một IaaS Cloud Computing. Hiểu được cách phân bổ các server chạy như thế nào chạy ở đâu và làm nhiệm vụ gì, cách mà tài nguyên máy tính được KVM quản lý và đưa lên các Host của Cloud

5.2 Hướng phát triển

Hiện tại tuy kiến trúc Cloud đã hoàn thiện cơ bản với mục đích Demo và Test. Nhưng có một số vấn đề hoàn toàn có thể khắc phục và phát triển trong tương lai:

- Tiến hành đưa ISO images hoặc system VMS template vào secondary storage, cấp phát tài nguyên và chạy thử một vài máy ảo trên Zone đã tạo
- Đưa các server nfs cũng như KVM tách biệt hoàn toàn với Management server trên một phần cứng riêng biệt để có được cái nhìn bao quát cũng như nâng cao khả năng mở rộng của hệ thống trong tương lai.

Do kiến thức còn hạn hẹp nên rất mong nhận được những góp ý của thầy và các bạn, nhóm chúng em xin trân thành cảm ơn!

TÀI LIỆU THAM KHẢO

[1] Welcome to Apache CloudStack's Documentation — Apache CloudStack 4.16.0.0 documentation.

[2] How to use bridge-utils on Ubuntu (linuxhint.com).

[3] Issues · apache/cloudstack · GitHub.

[4] How to check if port is in use on Linux or Unix - nixCraft (cyberciti.biz).

[5] Rohit Yadav - Apache CloudStack on Ubuntu with x86_64 KVM.

[6] Private Cloud Setup Step By Step Using Apache Cloud Stack » TechnologyRSS.

[7] Prepare NFS Server For CloudStack Management Server (technologyrss.com).