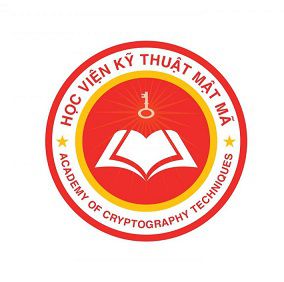
**HỌC VIỆN KỸ THUẬT MẬT MÃ**

**KHOA: AN TOÀN THÔNG TIN**

**----֎----**



**BÁO CÁO BÀI TẬP LỚN**

**TÌM HIỂU VÀ SO SÁNH BA MÔ HÌNH DỊCH VỤ IAAS, SAAS, PAAS**

**Sinh viên thực hiện : Trần Đức Lương – AT140131**

**Nguyễn Thị Hồng Quyên – AT140140**

**Bùi Anh Hiếu – AT140711**

**Phạm Thu Phương – AT140536**

**Lâm Thăng Long – AT140726**

**Thân Quang Phước – AT140437**

**Giảng viên hướng dẫn : Cô. Nguyễn Thị Thu Thủy**

**MỤC LỤC**

[Chương I: IAAS (Dịch vụ hạ tầng) 4](#_Toc83845291)

[1.1. Dịch vụ cơ sở hạ tầng (IAAS) 4](#_Toc83845292)

[1.1.1. Mô hình triển khai 5](#_Toc83845293)

[1.1.2. Ưu điểm và nhược điểm của IaaS 6](#_Toc83845294)

[1.2. Mục đích sử dụng IaaS 7](#_Toc83845295)

[1.3. Nhà cung cấp dịch vụ IaaS 8](#_Toc83845296)

[1.3.1. Khả năng triển khai 8](#_Toc83845297)

[1.3.2. UI và các phương thức truy cập đến Server 9](#_Toc83845298)

[1.3.3. Khả năng bảo tồn tài nguyên 10](#_Toc83845299)

[1.3.4. Chất lượng dịch vụ 11](#_Toc83845300)

[1.3.5. Lựa chọn trình giám sát và hệ điều hành 12](#_Toc83845301)

[1.3.6. Một số các nhà cung cấp dịch vụ IaaS chính. 12](#_Toc83845302)

[1.4. Quản lý bảo mật IaaS 15](#_Toc83845303)

[1.4.1. Bảo mật IaaS 15](#_Toc83845304)

[1.4.2. Các giải pháp bảo mật 15](#_Toc83845305)

[Chương II. SAAS (Dịch vụ nền tảng) 17](#_Toc83845306)

[2.1. Giới thiệu 17](#_Toc83845307)

[2.2. Ưu nhược điểm của mô hình Saas 18](#_Toc83845308)

[2.2.1. Ưu điểm của mô hình SaaS 18](#_Toc83845309)

[2.2.2. Nhược điểm của mô hình SaaS 21](#_Toc83845310)

[2.3. Vấn đề bảo mật trong SaaS 23](#_Toc83845311)

[2.3.1. Xác thực và ủy quyền 24](#_Toc83845312)

[2.3.2. Tính khả dụng 25](#_Toc83845313)

[2.3.3. Bảo mật dữ liệu 25](#_Toc83845314)

[2.3.4. Bảo mật máy ảo 26](#_Toc83845315)

[2.4. Những thách thức về bảo mật cụ thể trên đám mây 27](#_Toc83845316)

[2.4.1. Bảo mật thông tin 27](#_Toc83845317)

[2.4.2. An ninh mạng 27](#_Toc83845318)

[2.4.3 Tiêu chuẩn đám mây 27](#_Toc83845319)

[2.4.4. Truy cập dữ liệu 28](#_Toc83845320)

[2.4.5. Bảo mật ứng dụng web 29](#_Toc83845321)

[2.4.6. Vi phạm dữ liệu 30](#_Toc83845322)

[2.5. Giải pháp bảo mật hiện nay 30](#_Toc83845323)

[Chương III. PAAS (Dịch vụ phần mềm) 31](#_Toc83845324)

[3.1. Giới thiệu 31](#_Toc83845325)

[3.2. Các tính năng của PaaS 32](#_Toc83845326)

[3.3. Đặc điểm của PaaS 32](#_Toc83845327)

[3.4. Ưu điểm, nhược điểm của Paas 33](#_Toc83845328)

[3.4.1. Ưu điểm 33](#_Toc83845329)

[3.4.2. Nhược điểm 34](#_Toc83845330)

[3.5. Phân loại PaaS 34](#_Toc83845331)

[3.6. Ứng dụng PaaS trong công việc 35](#_Toc83845332)

[3.6.1. Cách sử dụng PaaS phổ biến 35](#_Toc83845333)

[3.6.2. Sử dụng PaaS trong các tổ chức 36](#_Toc83845334)

[3.6.3. Trường hợp sử dụng PaaS 37](#_Toc83845335)

[3.7. Bảo mật PaaS 37](#_Toc83845336)

[3.7.1. Thực tiễn bảo mật PaaS 37](#_Toc83845337)

[3.7.2. Giải pháp bảo mật PaaS 39](#_Toc83845338)

[Chương IV: So sánh vai trò và trách nhiệm của Nhà cung cấp và Khách hàng 41](#_Toc83845339)

[BẢNG PHÂN CÔNG NHIỆM VỤ CỦA TỪNG THÀNH VIÊN 45](#_Toc83845340)

**Chương I: IAAS (Dịch vụ hạ tầng)**

Các dịch vụ điện toán đám mây được chia thành ba lớp theo khả năng cung cấp và mô hình dịch vụ của các nhà cung cấp: Dịch vụ cơ sở hạ tầng (IaaS), dịch vụ nền tảng hệ thống (PaaS), dịch vụ ứng dụng (SaaS).

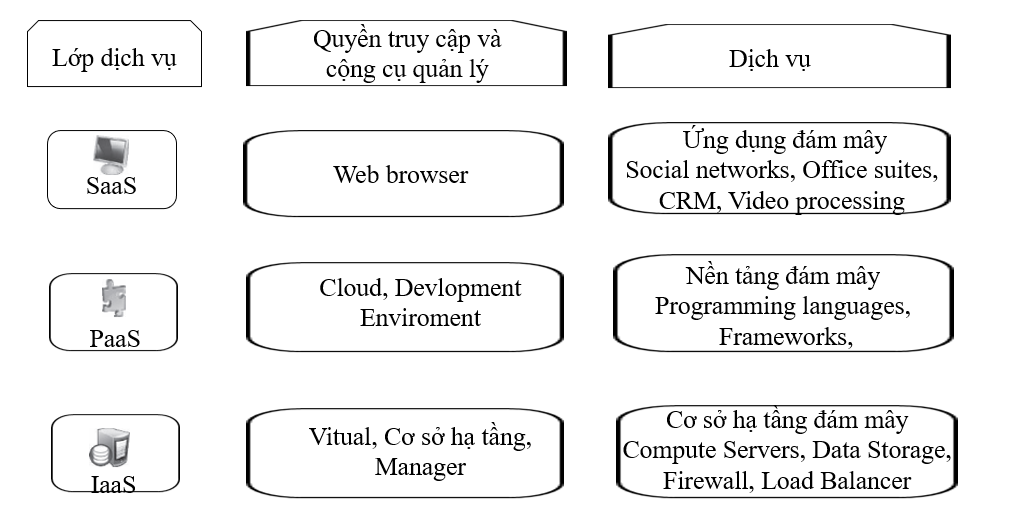
Các mức này cũng có thể xem như một kiến trúc phân lớp, nơi các dịch vụ lớp cao hơn có thể bao gồm các dịch vụ của lớp bên dưới. Môi trường phát triển đám mây được xây dựng dựa trên các dịch vụ cơ sở hạ tầng, cung cấp khả năng phát triển và triển khai ứng dụng. Các mô hình lập trình, thư viện, API ..cho phép tạo ra các ứng dụng kinh doanh, web…. Sau khi triển khai trên đám mây, những ứng dụng này có thể sử dụng bởi người dùng cuối.

**1.1. Dịch vụ cơ sở hạ tầng (IAAS)**

IaaS (Infrastructure as a Service) là dịch vụ cơ sở hạ tầng, cung cấp tài nguyên hạ tầng điện toán như máy chủ, mạng, không gian lưu trữ và các công cụ quản lý tài nguyên (tài nguyên được ảo hóa..)

Cơ sở hạ tầng đám mây cung cấp theo yêu cầu các máy chủ để chạy một số hoạt động trong hệ thống và một ngăn xếp phần mềm tùy chỉnh.

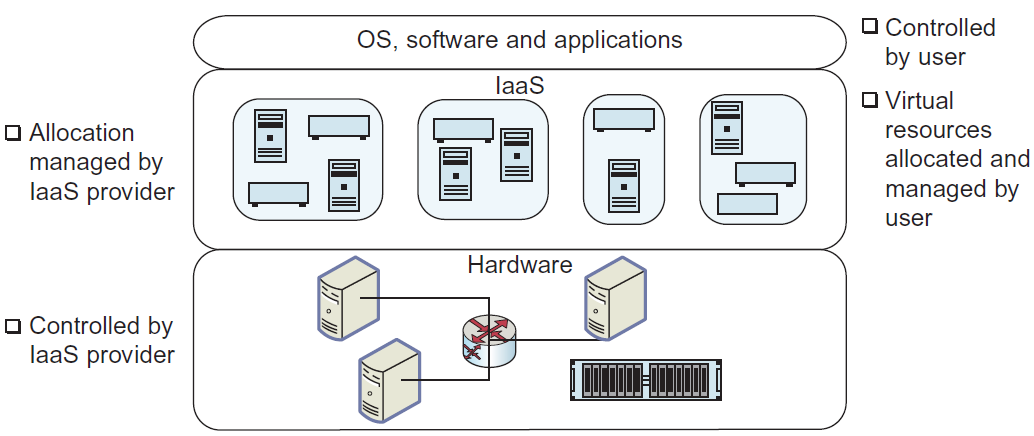
Các dịch vụ cơ sở hạ tầng nằm ở lớp dưới cùng của hệ thống điện toán đám mây:



*Phân lớp của đám mây*

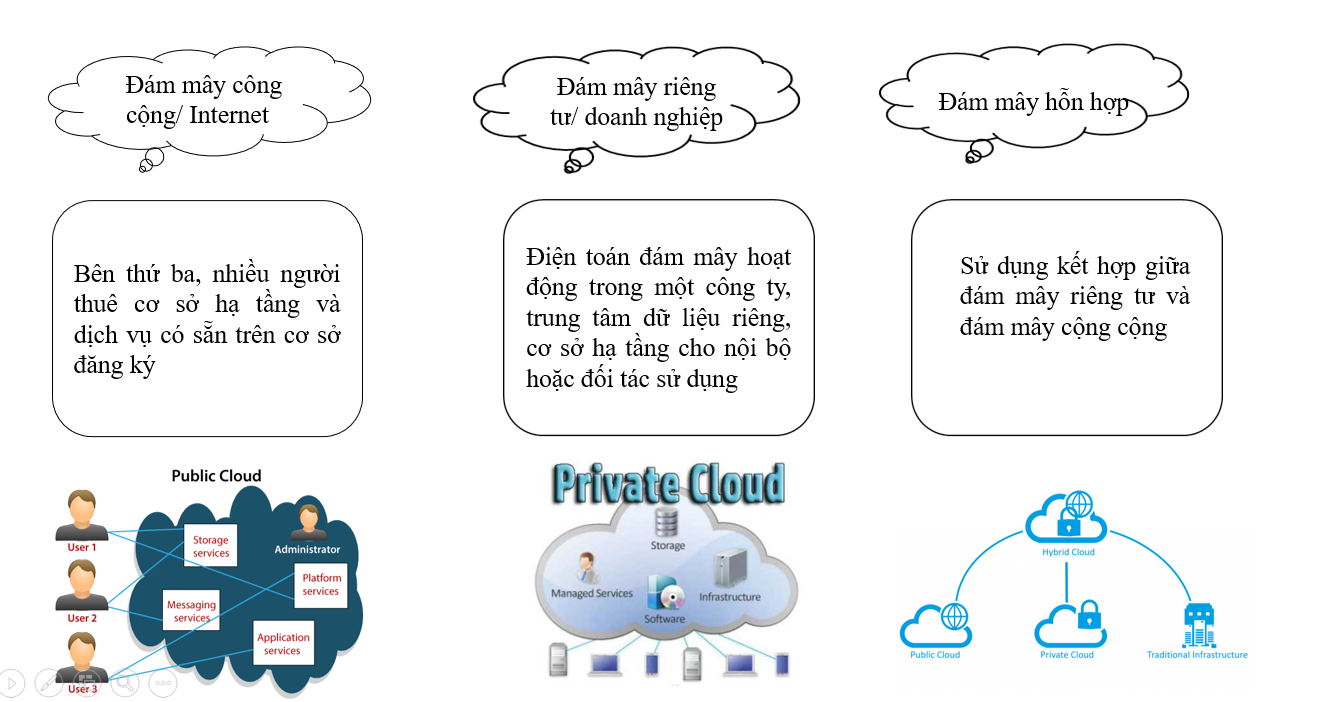
Amazon Web Services là dịch vụ chủ yếu của IaaS, nó cung cấp các máy ảo với một ngăn xếp phần mềm có thể được tùy chỉnh như một máy chủ vật lý thông thường. Người dùng được cấp quyền để thực hiện nhiều hoạt động với máy chủ như là: khởi động, tùy chỉnh bằng các cài đặt các gói phần mềm, cấu hình quyền truy cập và thiết lập các quy tắc tường lửa.

**Phạm vi kiểm soát:**



**1.1.1. Mô hình triển khai**

Điện toán đám mây xuất hiện khi các tiện ích máy tính, các mô hình phát triển khác với các thay đổi về vị trí vật lý và phân phối đã được thông qua. Điều đó bất kể lớp dịch vụ, mô hình triển khai điện toán đám mây như là: đám mây riêng, đám mây cộng đồng, đám mây hỗn hợp hay đám mây cộng đồng đều triển khai dựa trên mô hình như hình 1.1.2



*Mô hình triển khai dịch vụ, đám mây*

* Trong một đám mây lai, dữ liệu và ứng dụng có thể di chuyển giữa các đám mây riêng và đám mây công cộng để linh hoạt và có nhiều tùy chọn triển khai hơn.
* IaaS kết hợp với đám mây lai có thể là các giải pháp phù hợp cho nhu cầu các tổ chức khác nhau, riêng hoặc kết hợp nhiều mô hình cung cấp dịch vụ.
* Người dùng có thể quản lý, làm mới hoặc cập nhật phần cứng và bảo mật trên trung tâm dữ liệu tối ưu. Nó cung cấp các nguồn lực cần thiết để hỗ trợ phát triển dự án một cách nhanh chóng khi tăng hoặc giảm quy mô.
* Trong mô hình đám mây công cộng, các dịch vụ cơ sở hạ tầng bị giới hạn khá nhiều đối với các phiên bản hệ điều hành và các tùy chọn cấu hình mà nhà cung cấp cho phép, người dùng có thể lựa chọn máy chủ dựa trên máy ảo, lựa chọn hệ điều hành, có thể quản lý nhiều nhóm máy ảo với các quản trị viên, nhà khai thác riêng biệt nhưng chưa cung cấp bảng điều khiển tự phục vụ để quản lý máy ảo,…
* Đối với mô hình đám mây riêng tư, khi kết hợp với IaaS, người dùng có nhiều sự lựa chọn hơn như là: lựa chọn hệ điều hành, khả năng tự mở rộng tài nguyên (CPU, RAM..) khi cần, cấu hình cân bằng tải, tường lửa và mạng con, cài đặt các phiên bản hệ điều hành tùy chỉnh theo yêu cầu.

**1.1.2. Ưu điểm và nhược điểm của IaaS**

1.1.2.1. Ưu điểm IaaS

* Giúp dễ dàng vận hành khối lượng công việc.
* Tiết kiệm chi phí mua, quản lý cơ sở hạ tầng bên dưới.
* Dung lượng lớn và khả năng mở rộng tài nguyên tự động giúp việc giám sát dễ dàng, có thể chuyển từ một phiên bản của một ứng dụng hoặc công việc sang nhiều phiên bản.
* Giảm độ trễ và cải thiện hiệu suất.
* Hoạt động hiệu quả khi khối lượng công việc tạm thời, thử nghiệm hoặc thay đổi đột xuất
* Sau khi phần mềm mới được kiểm tra và tinh chỉnh, có thể xóa khỏi môi trường IaaS để triển khai nội bộ.

1.1.2.2. Nhược điểm của IaaS

* Quá trình thanh toán vẫn là một vấn đề đối với doanh nghiệp.
* Người dùng có thể thấy chi phí cao hơn dự kiến khi xem hóa đơn cho tất cả tài nguyên và dịch vụ liên quan đến việc triển khai ứng dụng.
* Có sự thiếu minh bạch trong các chi tiết cấu hình và hiệu suất cơ sở hạ tầng.
* Tính khả dụng và hiệu suất công việc phụ thuộc nhiều vào nhà cung cấp. Nếu nhà cung cấp dịch vụ gặp sự cố, người dùng sẽ bị ảnh hưởng.
* IaaS là một dịch vụ nhiều người thuê nên có thể ảnh hưởng đến hiệu suất công việc của người dùng.

**1.2. Mục đích sử dụng IaaS**

IaaS có thể được sử dụng cho nhiều mục đích khác nhau. Các trường hợp sử dụng phổ biến nhất để triển khai IaaS bao gồm:

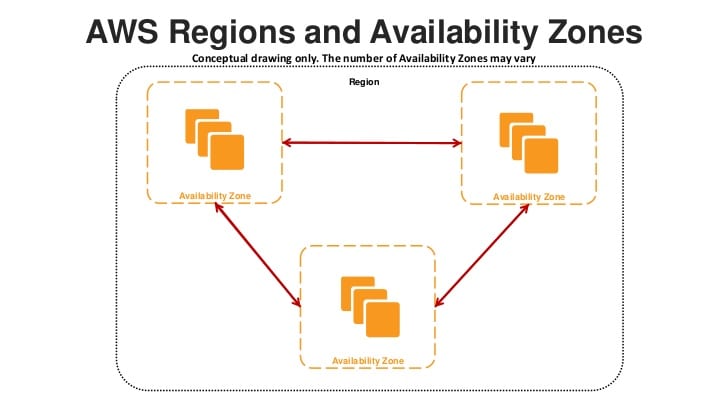
* + Môi trường thử nghiệm và phát triển. IaaS cung cấp cho các tổ chức sự linh hoạt khi nói đến các môi trường thử nghiệm và phát triển khác nhau. Chúng có thể dễ dàng được mở rộng hoặc thu nhỏ tùy theo nhu cầu.
  + Lưu trữ, sao lưu và phục hồi dữ liệu. IaaS có thể là cách dễ nhất và hiệu quả nhất để các tổ chức quản lý dữ liệu khi nhu cầu không thể đoán trước hoặc có thể tăng đều đặn. Hơn nữa, các tổ chức có thể tránh được nhu cầu về những nỗ lực sâu rộng tập trung vào các yêu cầu quản lý, pháp lý và tuân thủ của việc lưu trữ dữ liệu.
  + Ứng dụng web. cơ sở hạ tầng cần thiết để lưu trữ các ứng dụng web do IaaS cung cấp. Do đó, nếu một tổ chức đang lưu trữ một ứng dụng web, IaaS có thể cung cấp tài nguyên lưu trữ, máy chủ và mạng cần thiết. Việc triển khai có thể được thực hiện nhanh chóng và cơ sở hạ tầng đám mây có thể dễ dàng mở rộng hoặc thu nhỏ tùy theo nhu cầu của ứng dụng.
  + Máy tính hiệu suất cao (HPC), một số khối lượng công việc nhất định có thể yêu cầu tính toán mức HPC, chẳng hạn như tính toán khoa học, mô hình tài chính và công việc thiết kế sản phẩm.
  + Kho dữ liệu và phân tích dữ liệu lớn, IaaS có thể cung cấp sức mạnh tính toán và xử lý cần thiết để kết hợp thông qua các tập dữ liệu lớn.

**1.3. Nhà cung cấp dịch vụ IaaS**

* Các nhà cung cấp dịch vụ IaaS (Infrastructure as a Service) thường cung cấp các máy chủ ảo (VPS) chứa một hoặc nhiều CPU, chạy trên một số hệ điều hành bao gồm một tập các phần mềm tùy chọn, storage và các phương tiện liên lạc.
* Các nhà cung cấp dịch vụ IaaS thường tập trung vào tính sẵn sàng, đặc biệt là các tính năng mà đem lại lợi ích về kinh tế cho khách hàng khi chuyển sang sử dụng các dịch vụ đám mây. Các lợi ích phổ biến của Iaas bao gồm:
  + Không ảnh hưởng bởi phân bố địa lý của Data Center.
  + Nhiều loại UI và API để tương tác với hệ thống.
  + Hỗ trợ nhiều ứng dụng (Load Banlancer, Firewalls,…).
  + Đa dạng về hệ thống ảo hóa và hệ điều hành.
  + Thanh toán bằng nhiều phương thức khác nhau. (trả trước, trả sau, trả hàng giờ, trả hàng tháng).

**1.3.1. Khả năng triển khai**

Để cải thiện tính sẵn sàng và tính khả dụng, các nhà cung cấp dịch vụ đám mây sẽ xây dựng các Data Center và phân phối chúng trên khắp thế giới.

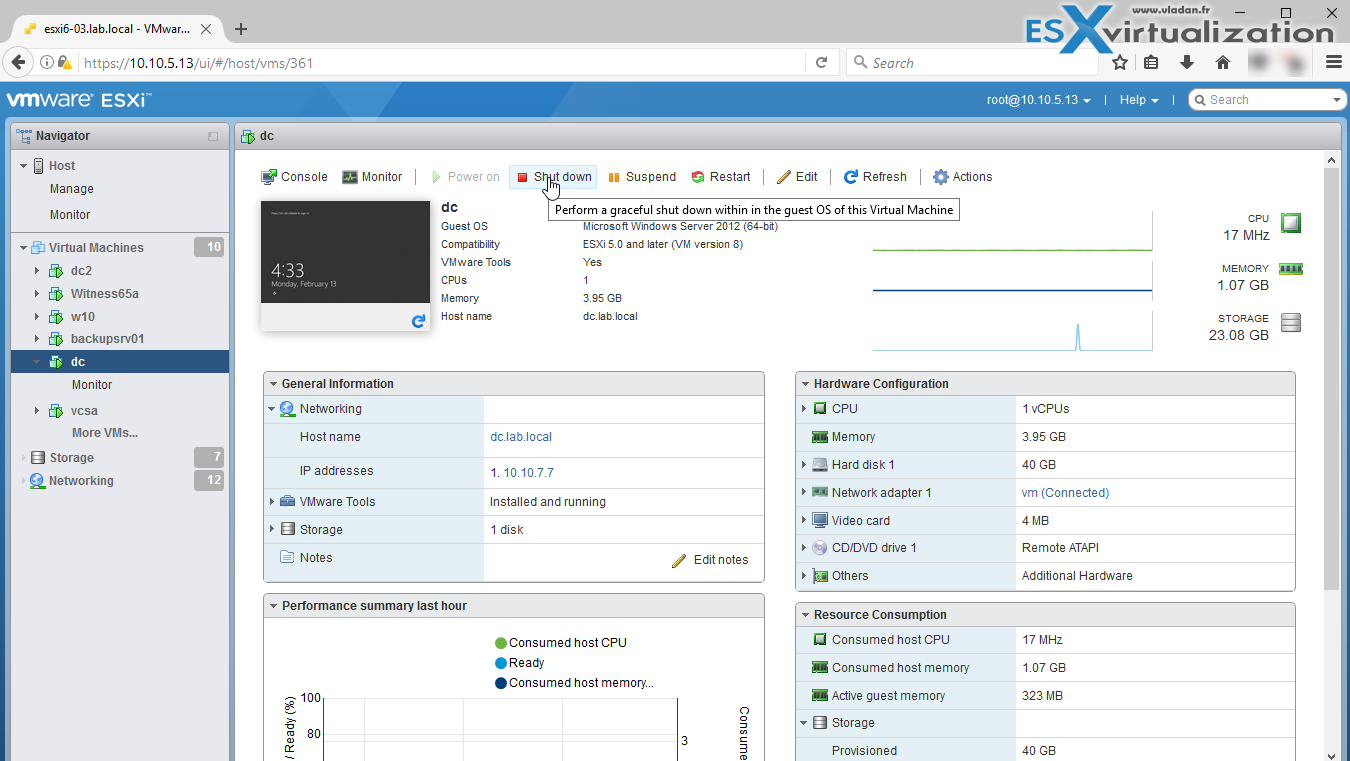


*AWS Region và Avaibility zones*

Ví dụ như Amazon Web Services đưa ra khái niệm “availability zones” và “regions” cho dịch vụ E2C của họ. Trong đó, “availability zones” được mô tả như là các vị trí riêng biệt được thiết kế để cách ly khỏi các sự cố ở các “availability zones” khác và cung cấp các kết nối mạng rẻ, độ trễ thấp với các vùng khác trong cùng khu vực. Còn “Regions” định nghĩa là là sự phân tán về mặt địa lý và nằm trong một khu vực hoặc quốc gia.

**1.3.2. UI và các phương thức truy cập đến Server**

Các nhà cung cấp dịch vụ IaaS thường cung cấp nhiều phương tiện khác nhau cho khách hàng để truy cập vào cloud của mình, do đó phục vụ được đa dạng các yêu cầu của khách hàng. Các loại giao diện người dùng (UI) khác nhau sẽ cung cấp các mức tương tác khác nhau cho khách hàng. Trong đó, phổ biến nhất là giao diện người dùng đồ họa (GUI), giao diện dòng lệnh (CLI) và Web Service API.

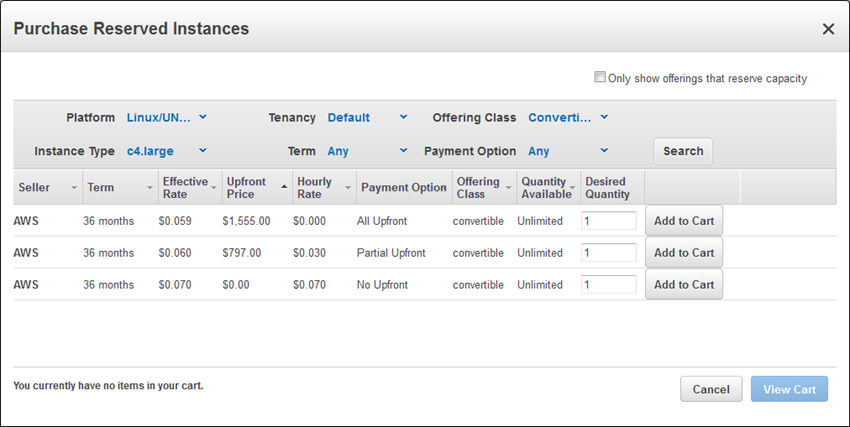


*Giao diện GUI của VMWare ESXi*

GUI thường được yêu thích bởi các khách hàng thông thường, những người mà chỉ cần chạy, tùy chỉnh và giám sát một vài máy chủ ảo. Mặt khác, CLI cung cấp nhiều tính năng hơn và khả năng tự động hóa các tác vụ thông qua câu lệnh (VD: start và shutdown theo lịch đã đặt). Các API WS cung cấp truy cập vào cloud bằng cách sử dụng các HTTP request tiêu chuẩn. Các dịch vụ có tính phức tạp cao có thể được xây dựng trên các IaaS Cloud.

**1.3.3. Khả năng bảo tồn tài nguyên**

Khách hàng có thể yêu cầu các nhà cung cấp IaaS bảo tồn một phần tài nguyên cho một khoảng thời gian cụ thể trong tương lai, đảm bảo tài nguyên này sẽ sẵn sàng tại thời điểm đó. Amazon Reserved Instance là một phương thức bảo tồn tài nguyên, nó cho phép người dùng trả trước một khoản tiền để đảm bảo tài nguyên luôn sẵn sàng bất kỳ lúc nào trong khoảng thời gian đã thỏa thuận. Tuy nhiên, khoảng thời gian này chỉ từ 1 đến 3 năm.



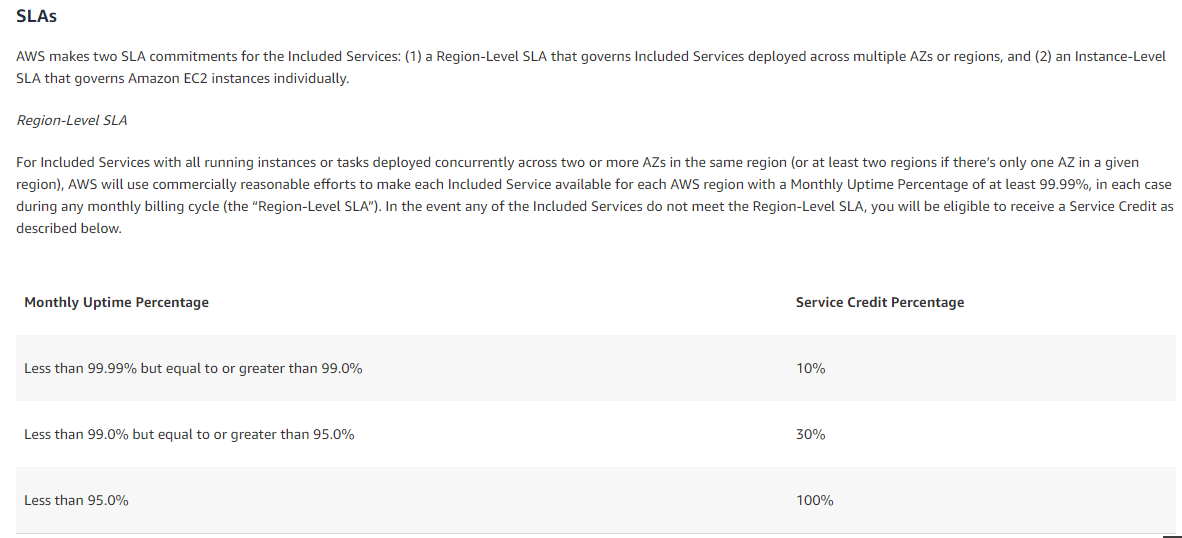
*Bảng giá Reversed Instances của AWS*

**1.3.3. Tự động chia tỷ lệ và cân bằng tải**

Trong mô hình điện toán đám mây các tài nguyên vật lý là có giới hạn, vậy nên tính đàn hồi là một trong những tính năng quan trong của mô hình này. Các ứng dụng thường cần tăng và giảm quy mô để đáp ứng các điều kiện tải khác nhau. Khả năng tự động chia tỷ lệ là một tính năng rất hiệu quả của các dịch vụ IaaS. Nó cho phép người dùng thiết lập các điều kiện khi họ muốn ứng dụng của mình tăng hoặc giảm quy mô, dựa trên các chỉ số của ứng dụng (transacion/s, số lượng người dùng đồng thời, độ trễ của các request,…). Khi số lượng các máy chủ ảo được tăng lên, lượng truy cập đến phải được phân bố tự động giữa các máy chủ này. Hoạt động này cho phép các ứng dụng đáp ứng kịp thời với sự gia tăng lưu lượng, đồng thời đạt được khả năng chịu lỗi cao hơn.

**1.3.4. Chất lượng dịch vụ**

  Cam kết chất lượng dịch vụ (SLAs) được đưa ra bởi nhà cung cấp dịch vụ IaaS để thể hiện cam kết của họ trong việc cung cấp dịch vụ với một QoS nhất định. Đối với khách hàng, nó sẽ được hiểu như là một phiếu bảo hành. SLAs thường bao gồm tính sẵn sàng và sự đảm bảo về mặt hiệu suất, các chỉ số và các hình phạt khi vi phạm những chỉ số này phải được tất cả các bên thỏa thuận và đồng ý. Hầu hết các nhà cung cấp dịch vụ IaaS đều tập trung các điều khoản trong SLAs của họ vào việc đảm bảo tính sẵn sàng, đảm bảo tỷ lệ thời gian hệ thống sẵn sàng trong một khoảng thời gian nhất định.



*SLAs của AWS E2C cho Region-Level*

  Ví dụ: Amazon E2C tuyên bố rằng: “Nếu thời gian sẵn sàng hoạt động của khách hàng hàng năm giảm xuống dưới 99,95%  thì khách hàng đó sẽ nhận được ưu đãi 10% dựa trên tổng số hóa đơn của họ.

**1.3.5. Lựa chọn trình giám sát và hệ điều hành**

Các dịch vụ IaaS truyền thống được triển khai trên các Xen mã nguồn mở được tùy chỉnh rất nhiều. Các nhà cung cấp IaaS cần có kiến thức chuyên môn về Linux, Mạng, Ảo hóa, đo lường, quản lý tài nguyên và nhiều khía cạnh khác để triển khai và duy trì thành công các dịch vụ đám mây của họ. Gần đây, với sự xuất hiện của các nền tảng IaaS như VMWare vCloud và Citrix Cloud Center (C3) đã hạ thấp rào cản về các kiến thức kể trên, dẫn đến sự mở rộng nhanh chóng trên thị trường IaaS.

**1.3.6. Một số các nhà cung cấp dịch vụ IaaS chính.**

**Amazon Web Service**. AWS là một trong những ông lớn trong thị trường điện toán đám mây và là người tiên phong trong việc giới thiệu dịch vụ điện toán đám mây đến người dùng (2006). AWS cung cấp nhiều dịch vụ đám mây khác nhau, trong đó đáng chú ý nhất là: S3 (storage), EC2 (virtual servers), Cloudfront (content delivery), Cloudfront Streaming (Video Streaming), SimpleDB (CSDL có cấu trúc), RDS (CSDL quan hệ), SQS và Elastic MapReduce. The Elastic Computer Cloud (EC2) cung cấp các máy chủ ảo dựa trên Xen và có thể được khởi tạo từ Amazon Machine Images (AMI) với các phiên bản có sẵn với nhiều kích cỡ, hệ điều hành, kiến trúc và giá cả. Dung lượng CPU của các phiên bản được đo bằng Amazon Compute Units và sẽ có sự khác nhau giữa các phiên bản từ 1 đến 20. Mỗi một phiên bản cung cấp một dung lượng ổ đĩa nhất định và dịch vụ Elastic Block Storage cho phép gắn các đĩa ảo có dung lượng lên đến 1TB vào các phiên bản. Tóm lại EC2 cung cấp các tính năng như sau: Nhiều Datacenter được đặt ở Mỹ, Châu Á và Châu Âu; CLI; Web service (SOAP và Query); Web GUI; Truy cập thông qua SSH (Linux) và Remote Desktop (Windows); Các phiên bản dự trữ trong 1 đến 3 năm; SLAs lên đến 99,5%; Tính giá theo giờ; Automatic Scaling; Load Balancing.

Flexiscale. Flexiscale là một nhà cung cấp có trụ sở đặt tại Anh và cung cấp các dịch vụ tương tự như Amazon Web Service. Tuy nhiên, các máy chủ ảo của nó cung cấp một số tính năng khác biệt: Lưu trữ liên tục, địa chỉ IP được điều chỉnh, VLAN, kích thước máy chủ lớn hơn, CPU bursting. Tường tự như các nhà cung cấp khác, dịch vụ của Flexiscale cũng được tính phí theo giờ. Tóm lại, Flexiscal cung cấp các tính năng sau: khả dụng tại Anh; Web service (SOAP); Web GUI; Truy cập vào máy chủ bằng SSH (Linux) và Remote Desktop (Window); SLAs lên tới 100% với khả năng tự động khôi phục máy ảo trong trường hợp bị lỗi phần cứng; Tính phí theo giờ; automatic scaling.

**Joyent**. Dịch vụ đám mây công cộng của Joyent cung cấp các máy chủ dựa trên công nghệ ảo hóa của Soloris. Các máy chủ này cho phép triển khai nhiều phần mềm chuyên dụng khác nhau dựa trên phiên bản tùy chỉnh của hệ điều hành Open Solaris và mặc định bao gồm một công cụ kiểm tra dựa trên Web và một số phần mềm được cài đặt sẵn như Apache, MySQL, PHP, Ruby on Rails và Java. Load Balancer cho phần mềm có sẵn ngoài bộ Load Balancer phần cứng. Một tính năng đáng chú ý của Joyent là tự động chi tỷ lệ lõi CPU theo chiều dọc, có nghĩa là máy chủ ảo có thể tự động sử dụng các CPU bổ sung đến khi chạm đến số lõi tối đa của máy chủ vật lý. Tóm lại, Joyent cung cấp các tính năng sau: Nhiều DC tại Mỹ; Web GUI; Truy cập vào máy chủ bằng SSH (Linux); SLA lên đến 100%; Tính phí theo tháng; Hệ điều hành  OpenSolaris; Automatic scaling.

**GoGrid**. GoGrid cũng giống như tất cả các nhà cung cấp dịch vụ IaaS khác đều cho phép khách hành của mình sử dụng các hệ điều hành Windows và Linux với các tùy chỉnh khác nhau. Đồng thời, GoGrid cũng cấp các ngăn xếp cho các ứng dụng như web với lượng truy cập lớn, e-Commerce, kho cơ sở dữ liệu và một số các tính năng đáng chú ý như hybird hosting (kết hợp các máy chủ truyền thống với hạ tầng máy chủ đám mây). Ngoài ra, GoGrid còn cung cấp tính năng cân bằng tải phần cứng miễn phí, auto-scaling, …

**Rackspace Cloud Servers**. Rackspace Cloud Servers là một nhà cung cấp giải pháp IaaS với các phiên bản được chỉnh sửa. Cloud Servers cung cấp một loạt các image của Linux được tạo sẵn. Người dùng có thể yêu cầu các image có kích thước khác nhau (tùy chỉnh RAM, không phải CPU). Giống như GoGrid, Cloud Servers có thể kết hợp các máy chủ chuyên dụng với hạ tầng đám mây. Cloud Servers cho phép khách hàng đặt IP tĩnh, lưu trữ liên tục và cân bằng tải (bằng A-DNS) được cung cấp miễn phí.

 Ngoài ra còn có nhiều doanh nghiệp nhỏ hơn như:

* + Rackspace Managed Cloud
  + IBM Cloud Private
  + Máy chủ ảo đám mây của IBM
  + Đám mây CenturyLink

**1.4. Quản lý bảo mật IaaS**

**1.4.1. Bảo mật IaaS**

* Mã hóa dữ liệu: dữ liệu di chuyển giữa các tài nguyên trên nền tảng đám mây và giữa các ứng dụng đám mây khác nhau, nên việc mã hóa là điều cần thiết. Người dùng có thể mã hóa bằng khóa riêng của mình hoặc sử dụng mã hóa theo nhà cung cấp IaaS.
* Tối ưu hóa cấu hình: Nguyên nhân phổ biến của các sự cố bảo mật đám mây là định cấu hình sai cho tài nguyên đám mây. Theo báo cáo của McAfee, tổ chức trung bình có ít nhất 14 trường hợp IaaS được định cấu hình sai. Điều này dẫn đến trung bình 2,269 sự cố cấu hình sai mỗi tháng. Ví dụ: 5,5% nhóm Amazon Web Services (AWS) S3 đang được định cấu hình sai, điều này có thể dẫn đến mất dữ liệu đáng kể.
* Phân quyền truy cập: chỉ cho phép truy cập đối với các tài khoản nhất định, phân quyền truy cập tới tài nguyên dựa trên vai trò của người dùng

**1.4.2. Các giải pháp bảo mật**

Bốn giải pháp quan trọng cho bảo mật IaaS là:

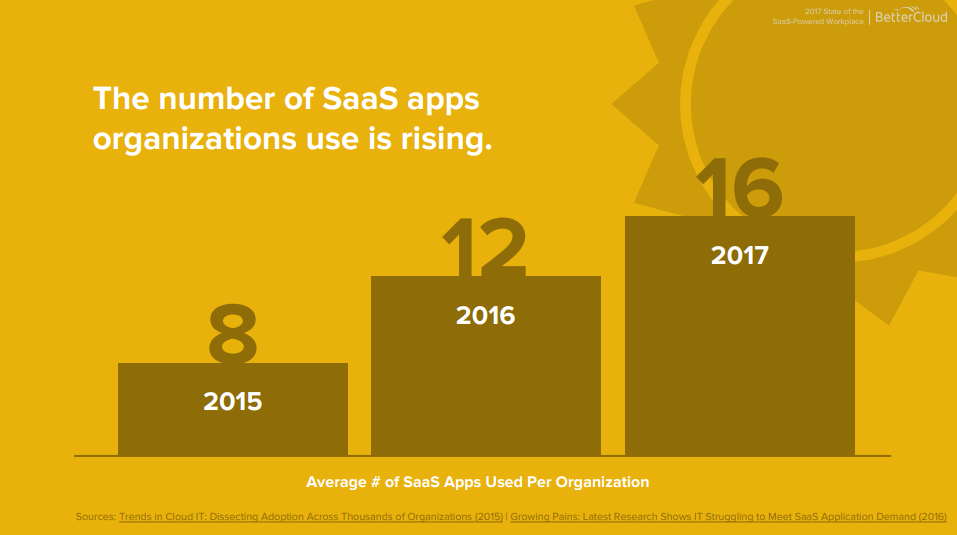
* CloudAccess Security Broker: Còn được gọi là cổng bảo mật đám mây (CSG), cung cấp nhiều dịch vụ bảo mật khác nhau, chẳng hạn như giám sát các dịch vụ đám mây. thực thi các chính sách bảo mật dữ liệu bao gồm ngăn chặn mất dữ liệu (DLP), hạn chế quyền truy cập vào dịch vụ đám mây dựa trên người dùng, thiết bị và ứng dụng và kiểm tra cấu hình đám mây để tuân thủ và rủi ro
* Community Wildfire Protection Plans (CWPPs): Các dịch vụ CWPP cũng áp dụng tính năng bảo vệ chống phần mềm độc hại và đơn giản hóa việc quản lý bảo mật giúp phát hiện và giám sát các vùng chứa dữ liệu
* Các nền tảng an ninh mạng ảo (VNSP). Các giải pháp của VNSP quét lưu lượng mạng di chuyển giữa các phiên bản trong môi trường IaaS. Giúp phát hiện và ngăn chặn xâm nhập mạng để bảo vệ tài nguyên ảo.
* Cloud security posture management (CSPM): Người quản lý bảo mật đám mây kiểm tra môi trường đám mây IaaS để tìm các vấn đề về bảo mật và tuân thủ, cũng như cung cấp biện pháp khắc phục thủ công hoặc tự động

**Chương II. SAAS (Dịch vụ nền tảng)**

**2.1. Giới thiệu**

SaaS (viết tắt của Software-as-a-Service) - một trong những dạng điện toán đám mây phổ biến nhất - được định nghĩa là mô hình phân phối dịch vụ ứng dụng phần mềm; trong đó nhà cung cấp không bán sản phẩm phần mềm mà bán dịch vụ dựa trên phần mềm đó. 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 sau khi trả một khoản phí đăng ký định kỳ (hàng tháng, quý, năm). SaaS được coi là mô hình 4.0 ưu việt hơn so với phần mềm on-premise - dạng phần mềm được doanh nghiệp mua lại thông qua một giấy phép vĩnh viễn.

Xu hướng hội nhập của mô hình SaaS trên toàn thế giới: Chắc chắn rằng bạn đang sử dụng ít nhất một dịch vụ phần mềm, chỉ là bạn có để tâm đó thực sự là một mô hình SaaS hay không mà thôi. Có thể liệt kê một vài phần mềm được phát triển rộng rãi bởi những nhà cung cấp SaaS hàng đầu thế giới như Amazone Web Services, Oracle, Adobe Creative Cloud, Slack, Dropbox, Google, IBM, Microsoft, ServiceNow,... Có thể thấy, SaaS gần như đã chiếm được độc quyền trong thị trường công nghệ.

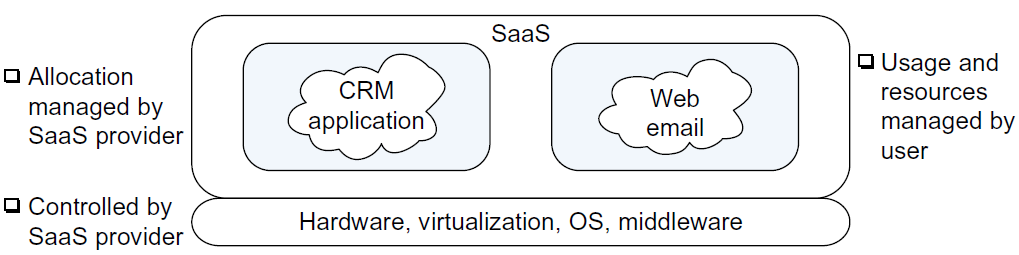


*Số lượng ứng dụng SaaS được sử dụng trong một doanh nghiệp tăng liên tục qua các năm*

Trong một báo cáo mới có tên Thị trường phần mềm dịch vụ: Công nghệ và thị trường toàn cầu đến năm 2022, BCC Research dự đoán rằng ngành công nghiệp dựa trên mô hình SaaS được định giá $44,4 tỷ vào năm 2017. Trong khi đó, người ta ước tính giá trị đó sẽ đạt được $94,9 tỷ vào năm 2022, nghĩa là tốc độ tăng trưởng hàng năm (CAGR) của thị trường SaaS vào khoảng 16,4% - một con số "khủng" cho thấy tiềm năng và cơ hội rộng mở cho ngành dịch vụ phần mềm này. Bởi lẽ các phần mềm dịch vụ SaaS có thể đến từ rất nhiều nhà cung cấp, nên xu hướng hiện đại của mô hình SaaS trên thế giới chính là gia tăng tích hợp giữa các phần mềm này để chúng cùng vận hành trơn tru, tạo ra sức mạnh tổng hợp cho toàn doanh nghiệp. Điều này lý giải cho việc một doanh nghiệp có thể sử dụng đồng thời nhiều phần mềm SaaS. Theo dữ liệu thống kê năm 2017 của BCC Research, con số trung bình được tính trên thế giới là 16 phần mềm/doanh nghiệp.

**Phạm vi kiểm soát:**

* + Nhà cung cấp dịch vụ SaaS quản lý thiết lập vị trí các ứng dụng
  + Khách hàng quản lý việc sử dụng tài nguyên, và sử dụng các ứng dụng dịch vụ
  + Phần cứng, ảo hóa, hệ điều hành và các phần sụn hoàn toàn do nhà cung cấp dịch vụ SaaS quản lý và kiểm soát.



**2.2. Ưu nhược điểm của mô hình Saas**

**2.2.1. Ưu điểm của mô hình SaaS**

Nhờ biết cách vận dụng tối ưu internet kết nối tài nguyên, mô hình SaaS ngày càng chiếm lĩnh thị trường công nghệ bởi hàng loạt lợi ích thiết thực.

* Tiết kiệm chi phí cho doanh nghiệp

Có một sự thật là mô hình SaaS giúp doanh nghiệp tiết kiệm được cả chi phí tiền mặt, thời gian, nhân lực, chi phí chuyển đổi và chi phí cơ hội.

Với mô hình SaaS, bạn không cần cài đặt và chạy các phần mềm trên hệ thống của doanh nghiệp. Điều đó giúp bạn tiết kiệm được một khoản chi phí rất lớn liên quan tới việc mua giấy phép phần mềm, lắp đặt phần cứng cũng như xây dựng hệ cơ sở dữ liệu mới. Trong suốt quá trình sử dụng, mô hình SaaS không đòi hỏi bạn phải trả thêm phí hỗ trợ và bảo trì định kỳ giống như phần mềm on-premise (khoảng 15 - 20%).

Hầu hết các mô hình SaaS hiện nay đều tập trung vào và bán các dịch vụ phần mềm dưới hai dạng: Freemium - cho phép bạn dùng miễn phí trước rồi trả thêm tiền để sử dụng các tính năng nâng cao, và Premium - bán theo gói dựa trên số lượng tài khoản và thời gian sử dụng. Trong cả hai trường hợp, bạn đều có quyền lựa chọn ngừng đăng ký dịch vụ SaaS bất cứ khi nào bạn muốn, và chi phí cũng ngừng luôn tại thời điểm đó.

Thời gian và nhân lực cần thiết để triển khai một phần mềm SaaS cũng tiết kiệm hơn hẳn so với giải pháp on-premise truyền thống. Doanh nghiệp phải tốn tới 6 tháng hoặc lâu hơn vào việc tạm ngưng hoạt động một số bộ phận để lắp đặt hoàn chỉnh một hệ thống on-premise cồng kềnh, đồng thời huy động tất cả nhân viên kỹ thuật tốt nhất đến hỗ trợ. Còn với đội ngũ hỗ trợ (thường chỉ gồm 1-2 thành viên) của nhà cung cấp SaaS, họ chỉ cần tối đa là 2 ngày để thiết lập tài khoản và training sử dụng phần mềm cho toàn bộ nhân viên trong doanh nghiệp.

Mô hình SaaS cũng giúp doanh nghiệp giải bài toán chi phí chuyển đổi khi lắp đặt và áp dụng công nghệ. Giả sử phần mềm on-premise gặp phải sự cố phát sinh trong quá trình vận hành, tất cả hệ thống sẽ "chết"; mà khi phần mềm đó đã thực sự lỗi thời, doanh nghiệp cũng khó dứt khoát loại bỏ nó vì chi phí ban đầu bỏ ra quá lớn. Còn phần mềm SaaS được ví như một chiếc xe bus, bạn chỉ cần bỏ ra số tiền vừa phải để được chở đi đến bất cứ nơi nào bạn muốn mà không cần mua chiếc xe mới hay quá lo lắng cho việc chiếc xe bị hỏng hóc giữa đường.

* Tính năng phần mềm

Là khách hàng sử dụng SaaS, bạn không cần một bộ phận IT luôn túc trực để xử lý vấn đề kỹ thuật trong quá trình vận hành phần mềm nữa. Từ việc đảm bảo hệ thống máy chủ chạy tốt, duy trì bảo mật đến fix các bugs phát sinh,... đều được nhà cung cấp chịu trách nhiệm. Đội ngũ tester và IT của họ làm rất tốt phần này, và bạn sẽ luôn được sử dụng dịch vụ tốt nhất từ phía họ.

Doanh nghiệp cũng được hưởng lợi từ việc các nhà cung cấp SaaS luôn thường xuyên tự động cập nhật phần mềm, bao gồm cả việc tối ưu các tính năng cũ và bổ sung thêm các tính năng cao cấp hơn. Bạn không cần lo lắng tìm mua phiên bản mới được phát hành hoặc các bản vá công nghệ.

* Dễ dàng sử dụng ở mọi lúc, mọi nơi

Vì các nhà cung cấp SaaS triển khai dịch vụ qua internet nên người dùng dễ dàng truy cập phần mềm từ bất kỳ thiết bị và trình duyệt nào có kết nối internet.

Với SaaS, bạn không cần phải đến văn phòng, mở chiếc máy tính được cài sẵn phần mềm thì mới có thể sử dụng nó. Khi doanh nghiệp đăng ký sử dụng phần mềm, bạn được phép tạo thêm tài khoản (với giới hạn số lượng tuỳ theo gói đã mua) cho nhân viên trong doanh nghiệp. Bạn và nhân viên có thể ngồi ở bất cứ đâu, tại bất cứ thời gian nào, thực hiện thao tác đăng nhập đơn giản và sử dụng các tính năng không giới hạn.



*Với SaaS và internet, bạn và nhân viên có thể sử dụng phần mềm ở bất cứ đâu, tại bất cứ thời gian nào*

Hầu hết các nhà cung cấp SaaS đều đang cố gắng phát triển ứng dụng trên đa hệ điều hành (Windows, MacOS, iOS và Android) và trên nhiều trình duyệt (Microsoft Internet Explorer, Google Chrome, Apple Safari, Mozilla Firefox,...) để hỗ trợ tối đa trải nghiệm người dùng. Thông thường, bạn có thể cùng lúc đăng nhập trên nhiều thiết bị.

* Khả năng tích hợp

Các phần mềm on-premise thường được thiết kế để giải quyết bài toán một cách biệt lập và không cần liên quan tới các ứng dụng ngoài. Nhưng trên thực tế, bạn luôn cần trao đổi dữ liệu qua lại giữa các phần mềm với nhau để hệ thống hoá quy trình và tiết kiệm thời gian, công sức làm việc. Hiểu được nhu cầu thiết yếu này, các nhà cung cấp đã phát triển khả năng tích hợp thành thế mạnh vượt trội của mô hình SaaS trên toàn thế giới.

Hầu hết các phần mềm SaaS hiện nay đều được tối ưu hệ thống API - giao diện lập trình ứng dụng mở cho phép đồng nhất và trao đổi dữ liệu qua lại giữa các ứng dụng đến từ nhiều bên cung cấp khác nhau. Đó chính là cơ hội để bạn và doanh nghiệp hội nhập nhanh hơn với các công nghệ mới ngay trên chính hệ thống hiện tại của mình.

* Quy mô sử dụng

Một ưu điểm lớn của dữ liệu đám mây nói chung và SaaS nói riêng là khả năng mở rộng. Bạn dễ dàng tăng gấp đôi, gấp ba,... số lượng tài khoản hoặc tích hợp thêm các phần mềm mới mà không ảnh hưởng tới cơ sở hạ tầng hay cơ sở dữ liệu có sẵn của doanh nghiệp. Điều này đặc biệt quan trọng đối với các doanh nghiệp đang trên đà tăng trưởng nóng hoặc bạn đang có dự định mở rộng quy mô trong tương lai.

**2.2.2. Nhược điểm của mô hình SaaS**

Không có giải pháp công nghệ nào là hoàn hảo, và mô hình SaaS cũng vậy. Những vấn đề này không hẳn là nhược điểm mà đôi khi chỉ là những yêu cầu bắt buộc đối với người sử dụng phần mềm mà bạn hoàn toàn hiểu và có biện pháp khắc phục. Dưới đây là một số điểm đang được các nhà cung cấp SaaS hoàn thiện thêm.

* Tính bảo mật hệ thống

Chính bởi tập trung vào sự linh hoạt, gọn nhẹ và dễ dàng triển khai mà mô hình SaaS có một điểm yếu so với giải pháp on-premise - đó là vấn đề bảo mật. Với SaaS, server của phần mềm sẽ được đặt ở bên phía nhà cung cấp chứ không đặt tại doanh nghiệp, còn dữ liệu được ký gửi trên “đám mây” (cloud) nên bạn có thể có cảm giác không an toàn, lo sợ thông tin rò rỉ hoặc bị lấy cắp.

Khi nền điện toán đám mây 4.0 càng phát triển thì vấn đề này càng bớt lo ngại. Đó là nhờ các nhà cung cấp SaaS chú trọng hơn vào mã hoá dữ liệu và có các điều khoản cam kết bảo mật chặt chẽ hơn trong Cam kết mức độ dịch vụ (SLA). Bạn nên kiểm tra lại một lượt về bảo mật trước khi đưa ra bất cứ quyết định triển khai phần mềm SaaS nào.

* Yêu cầu bắt buộc về kết nối internet

Người dùng cần phải kết nối internet để đăng nhập và sử dụng phần mềm SaaS. Trong trường hợp thiết bị sử dụng không kết nối được, hoặc khi đang ở những nơi internet không khả dụng như di chuyển trên máy bay, việc sử dụng sẽ bị gián đoạn.

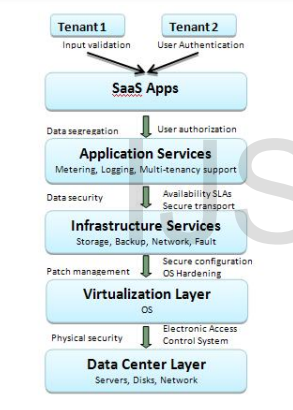
Đây có thể coi là một điểm trừ của SaaS trong đánh giá của những nhà lãnh đạo doanh nghiệp khó tính. Còn đối với số đông còn lại, những người luôn thường xuyên cập nhật thông tin trên Facebook, chat, gửi Email, nghe nhạc online,... thì internet giống như một trợ thủ song hành, chứ không phải yêu cầu khắt khe từ phía nhà cung cấp. Trên tất cả, các nhà cung cấp hiện đang phát triển tính năng hỗ trợ sử dụng ngoại tuyến cho các phần mềm này.

* Chưa sẵn sàng với phiên bản mới cập nhật

Lợi ích được tự động cập nhật miễn phí phiên bản mới của phần mềm cũng có thể mang lại sự bất tiện. Đó là khi bạn hoặc một số nhân viên trong doanh nghiệp có thể cảm thấy bỡ ngỡ với các thay đổi trong giao diện hay tính năng nâng cao của phần mềm.

**2.3. Vấn đề bảo mật trong SaaS**

Trong mô hình Phần mềm dưới dạng Dịch vụ (SaaS), máy khách phải phụ thuộc vào nhà cung cấp dịch vụ cho phù hợp các biện pháp an ninh. Nhà cung cấp phải đảm bảo rằng nhiều người dùng không thể nhìn thấy nhau dữ liệu. Vì vậy, điều quan trọng đối với người dùng là đảm bảo các biện pháp an ninh phù hợp và cũng đảm bảo rằng ứng dụng sẽ có sẵn khi cần thiết. Trong khi sử dụng Mô hình SaaS, theo định nghĩa, khách hàng sẽ được thay thế các ứng dụng phần mềm mới cho những phần mềm cũ. Nhà cung cấp phần mềm SaaS có thể lưu trữ ứng dụng trên máy chủ riêng của họ hoặc triển khai nó trên một dịch vụ cơ sở hạ tầng điện toán đám mây được cung cấp bởi nhà cung cấp bên thứ ba (ví dụ: Amazon, Google, v.v.). Việc sử dụng điện toán đám mây đi đôi với với phương pháp 'trả tiền khi bạn di chuyển' giúp nhà cung cấp dịch vụ ứng dụng giảm đầu tư trong các dịch vụ cơ sở hạ tầng và cho phép nó tập trung vào việc cung cấp các dịch vụ tốt hơn cho khách hàng. Hầu hết các doanh nghiệp đều quen thuộc với mô hình truyền thống, nơi dữ liệu tiếp tục cư trú trong ranh giới doanh nghiệp, tùy thuộc vào chính sách của họ.



*Các vấn đề bảo mật trong SaaS*

**2.3.1. Xác thực và ủy quyền**

Các ứng dụng xác thực và ủy quyền đối với môi trường doanh nghiệp có thể cần phải đã thay đổi, để làm việc với môi trường đám mây an toàn. Nhiệm vụ pháp y có thể trở nên khó khăn hơn nhiều vì các nhà điều tra có thể không truy cập được phần cứng hệ thống về mặt vật lý. Thiết kế được đề xuất bởi Pratap Murukutla cho phép người dùng sử dụng một tập hợp các thông tin xác thực. Họ đã đề xuất một giải pháp với các tiêu chuẩn thực tế về ủy quyền mở trong mà có một kiểm toán viên của bên tin cậy duy trì tất cả thông tin đăng nhập và nhà cung cấp đám mây có thể phân biệt duy nhất người dùng này với người dùng khác. Các mô hình được đề xuất trong tài liệu xác minh người dùng tính xác thực bằng cách sử dụng hai bước. Xác minh, đó là dựa trên mật khẩu, thẻ thông minh và ngoài băng tần (tức là hai yếu tố mạnh mẽ) xác thực. Ngoài ra, chương trình cũng cung cấp xác thực lẫn nhau, quản lý danh tính, thiết lập khóa phiên, quyền riêng tư của người dùng và bảo mật chống lại nhiều các cuộc tấn công. Tuy nhiên, việc kiểm tra bảo mật chính thức vẫn chưa được chính thức hóa.

**2.3.2. Tính khả dụng**

Tính khả dụng đảm bảo sự đáng tin cậy và kịp thời truy cập vào dữ liệu đám mây hoặc tài nguyên điện toán đám mây bởi các nhân viên thích hợp. Sự sẵn sàng của các nhà cung cấp dịch vụ đám mây cũng là một mối quan tâm lớn, vì nếu dịch vụ đám mây bị gián đoạn, nó ảnh hưởng nhiều hơn khách hàng so với mô hình truyền thống. Ví dụ như sự gián đoạn gần đây của Amazon dịch vụ đám mây vào năm 2011, đã hạ gục một số lượng trang web bao gồm Reedit, Foursquare... Các nhà cung cấp ứng dụng SaaS là cần thiết để đảm bảo rằng hệ thống đang chạy thích hợp khi cần thiết và doanh nghiệp được cung cấp với các dịch vụ suốt ngày đêm. Cái này liên quan đến việc thực hiện các thay đổi kiến trúc tại cấp độ ứng dụng và cơ sở hạ tầng để thêm khả năng mở rộng và tính sẵn sàng cao. Khả năng phục hồi lỗi phần cứng/phần mềm, cũng như từ chối các cuộc tấn công dịch vụ, cần được xây dựng từ bên ngoài tới trong ứng dụng. Đồng thời, một kế hoạch hành động thích hợp để hoạt động kinh doanh liên tục và khôi phục sau thảm họa cần được xem xét để bất kỳ yêu cầu nào theo hướng dẫn được cung cấp. Điều này là cần thiết để đảm bảo sự an toàn của dữ liệu doanh nghiệp trong khi vẫn duy trì mức tối thiểu thời gian chết cho các doanh nghiệp. Với Amazon là một ví dụ: API Amazon Web Services (AWS) điểm cuối được lưu trữ trên cùng một quy mô Internet, cơ sở hạ tầng đẳng cấp thế giới hỗ trợ các trang web bán lẻ Amazon. Từ chối phân tán tiêu chuẩn của các kỹ thuật giảm thiểu dịch vụ (DDoS) như cookie đồng bộ và giới hạn kết nối là đã sử dụng. Để giảm thiểu hơn nữa ảnh hưởng đến tiềm năng tấn công DDoS, Amazon duy trì nội bộ băng thông vượt quá do nhà cung cấp của nó cung cấp Băng thông Internet.

**2.3.3. Bảo mật dữ liệu**

Bảo mật đề cập đến việc ngăn chặn cố ý hoặc vô ý trái phép tiết lộ thông tin. Bảo mật trên đám mây hệ thống liên quan đến các lĩnh vực trí tuệ quyền tài sản, kênh bí mật, phân tích lưu lượng truy cập, mã hóa và suy luận. Điện toán đám mây liên quan đến việc chia sẻ hoặc lưu trữ thông tin trên máy chủ từ xa do người khác sở hữu hoặc điều hành, trong khi truy cập qua Internet hoặc bất kỳ cách nào khác kết nối. Dịch vụ điện toán đám mây tồn tại trong nhiều biến thể, bao gồm các trang web lưu trữ dữ liệu, trang video, trang khai thuế, sức khỏe cá nhân ghi lại các trang web và nhiều hơn nữa. Toàn bộ nội dung của thiết bị lưu trữ của người dùng có thể được lưu trữ với một nhà cung cấp đám mây duy nhất hoặc với nhiều các nhà cung cấp đám mây. Bất cứ khi nào một cá nhân, một doanh nghiệp, cơ quan chính phủ hoặc bất kỳ tổ chức nào khác chia sẻ thông tin trên đám mây, quyền riêng tư hoặc câu hỏi bảo mật phát sinh.

**2.3.4. Bảo mật máy ảo**

Là quyền kiểm soát của quản trị viên đối với server và client các hệ điều hành. Nhiều lỗi đã được tìm thấy mặc dù toàn cầu việc áp dụng ảo hóa là một tương đối gần đây hiện tượng, các mối đe dọa đối với cơ sở hạ tầng đang phát triển nhanh chóng. Các hypervisor và các máy ảo được sử dụng trong đám mây các nhà cung cấp cũng có thể có lỗ hổng bảo mật. Ảo hóa là một trong những các thành phần của đám mây, nhưng điều này lại đặt ra các vẫn đề liên quan tới rủi ro bảo mật. Các vẫn đề bảo mật trên để đảm bảo rằng các trường hợp khác nhau chạy trên cùng một máy vật lý bị cô lập từ nhau là một nhiệm vụ chính của ảo hóa điều này không được đáp ứng hoàn toàn trong kịch bản ngày nay. Vấn đề khác là tất cả các VMM phổ biến cho phép thoát khỏi VM. Màn hình máy ảo phải là "root secure", nghĩa là không có đặc quyền trong môi trường khách ảo hóa cho phép can thiệp vào hệ thống máy chủ. Một vài lỗ hổng bảo mật đã được tìm thấy trong tất cả ảo hóa phần mềm có thể bị khai thác bởi phần mềm độc hại, cục bộ người dùng để vượt qua các hạn chế bảo mật nhất định hoặc đạt được các đặc quyền. Ví dụ, lỗ hổng bảo mật của Microsoft Virtual PC và Microsoft Virtual Server có thể cho phép người dùng hệ điều hành khách chạy mã trên máy chủ lưu trữ hoặc một khách khác đang điều hành hệ thống. Lỗ hổng trong Virtual PC và Virtual Máy chủ có thể cho phép nâng cao đặc quyền. Do đó, các nhà cung cấp có thể cần phải xem xét lại các vấn đề về an ninh truyền thống từ nhiều góc độ khác nhau.

**2.4. Những thách thức về bảo mật cụ thể trên đám mây**

**2.4.1. Bảo mật thông tin**

Trong một ứng dụng truyền thống các mô hình triển khai, dữ liệu nhạy cảm của mỗi doanh nghiệp tiếp tục sử dụng trong doanh nghiệp ranh giới và phụ thuộc vào vật lý, logic và chính sách an ninh nhân sự và kiểm soát truy cập. Tuy nhiên, trong mô hình SaaS, dữ liệu doanh nghiệp được lưu trữ bên ngoài ranh giới của doanh nghiệp, mà tại đó SaaS của nhà cung cấp kết thúc phiên làm việc. Do đó, nhà cung cấp SaaS phải áp dụng các biện pháp kiểm tra bảo mật bổ sung để đảm bảo dữ liệu bảo mật và ngăn chặn vi phạm do bảo mật lỗ hổng trong ứng dụng hoặc thông qua nhân viên độc hại. Điều này liên quan đến việc sử dụng kỹ thuật mã hóa mạnh mẽ để bảo mật dữ liệu và ủy quyền chi tiết để kiểm soát quyền truy cập vào dữ liệu.

**2.4.2. An ninh mạng**

Trong mô hình triển khai SaaS, dữ liệu nhạy cảm là thu được từ các doanh nghiệp, được xử lý bởi Ứng dụng SaaS và được lưu trữ tại nhà cung cấp SaaS IJSER Tạp chí Quốc tế Nghiên cứu Khoa học & Kỹ thuật Tập 8, Số 5, Tháng 5-2017 37 ISSN 2229-5518 IJSER © 2017 http://www.ijser.org kết thúc. Tất cả luồng dữ liệu qua mạng cần phải được bảo mật để ngăn ngừa rò rỉ thông tin. Điều này liên quan đến việc sử dụng các kỹ thuật mã hóa lưu lượng mạng như Lớp cổng bảo mật (SSL) và lớp truyền tải Bảo mật (TLS) để bảo mật. Trong trường hợp của Amazon Web Dịch vụ (AWS), lớp mạng cung cấp bảo vệ đáng kể chống lại mạng truyền thống các vấn đề bảo mật, chẳng hạn như các cuộc tấn công MITM (Man-In-TheMiddle), giả mạo IP, quét cổng, gói tin đánh hơi, v.v. Để bảo mật tối đa, Amazon S3 là có thể truy cập thông qua các điểm cuối được mã hóa SSL.

**2.4.3 Tiêu chuẩn đám mây**

Để đạt được khả năng tương tác giữa các đám mây và tăng tính ổn định và bảo mật của chúng, các tiêu chuẩn đám mây là cần thiết trên các tiêu chuẩn khác nhau phát triển các tổ chức. Ví dụ, hiện tại dịch vụ lưu trữ của một nhà cung cấp đám mây có thể không tương thích với của nhà cung cấp khác. Theo thứ tự để giữ chân khách hàng của họ, các nhà cung cấp dịch vụ đám mây có thể giới thiệu cái gọi là '' dịch vụ cố định '' tạo ra khó khăn cho người dùng nếu họ muốn di chuyển từ nhà cung cấp này đến nhà cung cấp khác, ví dụ: Amazon’s S3 là không tương thích với Blue Cloud của IBM, Open Grid Forum, v.v. Đến việc thúc đẩy sử dụng rộng rãi điện toán đám mây, các cơ quan tiêu chuẩn cần ngồi xuống và làm việc cùng nhau để thiết lập các tiêu chuẩn chung. Các tiêu chuẩn ''liên đám mây'' trong các miền sau cần thiết để tăng khả năng tương tác với đám mây và di chuyển dữ liệu tự do giữa các đám mây:

* Kiến trúc mạng,
* Định dạng dữ liệu,
* Đo sáng và thanh toán,
* Chất lượng dịch vụ,
* Nguồn lực cung cấp,
* Bảo mật, quản lý danh tính và sự riêng tư.

**2.4.4. Truy cập dữ liệu**

Vấn đề truy cập dữ liệu chủ yếu liên quan đến bảo mật các chính sách được cung cấp cho người dùng khi truy cập vào dữ liệu. Trong một tình huống điển hình, một doanh nghiệp nhỏ tổ chức có thể sử dụng đám mây do một số nhà cung cấp khác để thực hiện công việc kinh doanh của mình các quy trình. Tổ chức này sẽ có chính sách bảo mật dựa trên đó mỗi nhân viên có thể có quyền truy cập vào một tập hợp dữ liệu cụ thể. Các chính sách bảo mật có thể cho phép một số lựa chọn, trong đó, một số nhân viên không được cho truy cập vào một lượng dữ liệu nhất định. Các chính sách bảo mật này phải được đám mây tuân thủ tránh xâm nhập dữ liệu của người dùng trái phép. Mô hình SaaS phải đủ linh hoạt để kết hợp các chính sách cụ thể do tổ chức. Trong bất cứ một mô hình nào cũng phải có khả năng cung cấp giới hạn của tổ chức trong đám mây bởi vì nhiều tổ chức sẽ triển khai quy trình kinh doanh của họ trong một môi trường đám mây duy nhất.

**2.4.5. Bảo mật ứng dụng web**

SaaS là phần mềm được triển khai qua internet hoặc được triển khai để chạy sau tường lửa trong khu vực cục bộ mạng hoặc máy tính cá nhân. Chìa khóa các đặc điểm bao gồm quyền truy cập dựa trên mạng vào và quản lý, có sẵn trên thị trường phần mềm và quản lý các hoạt động từ trung tâm thay vì tại trang web của mỗi khách hàng, cho phép khách hàng truy cập ứng dụng từ xa qua Web. Phát triển ứng dụng SaaS có thể sử dụng nhiều loại thành phần phần mềm khác nhau và các khuôn khổ. Những công cụ này có thể giảm thời gian marketing và chi phí chuyển đổi sản phẩm hoặc công trình phần mềm là tiền đề để triển khai giải pháp SaaS mới. Những ví dụ bao gồm các thành phần để quản lý đăng ký, mạng lưới phần mềm máy tính, khuôn khổ ứng dụng web và hoàn thiện các sản phẩm nền tảng SaaS. Một trong những các yêu cầu ''phải có'' đối với ứng dụng SaaS là nó phải được sử dụng và quản lý trên web. Phần mềm được cung cấp dưới dạng dịch vụ tồn tại trên cloud mà không ràng buộc với người dùng thực tế. Điều này cho phép thay đổi phần mềm mà không cần gây bất tiện cho người dùng. Các lỗ hổng bảo mật trên web các ứng dụng do đó tạo ra lỗ hổng cho ứng dụng SaaS. Trong trường hợp này, lỗ hổng bảo mật có thể có khả năng có tác động bất lợi đối với tất cả khách hàng sử dụng đám mây. Thử thách với Bảo mật SaaS không khác gì so với bảo mật của bất kỳ công nghệ ứng dụng web nào khác. Tuy vậy một trong những vấn đề là mạng truyền thống các giải pháp bảo mật như tường lửa mạng, phát hiện và ngăn chặn xâm nhập mạng hệ thống (IDS & IPS), không giải quyết đầy đủ vấn đề này. Các ứng dụng web giới thiệu mới các rủi ro bảo mật không thể được bảo vệ một cách hiệu quả chống lại ở cấp độ mạng và yêu cầu cấp độ ứng dụng.

**2.4.6. Vi phạm dữ liệu**

Vì dữ liệu từ nhiều người dùng và doanh nghiệp khác nhau các tổ chức hợp tác với nhau trong môi trường đám mây, xâm nhập vào môi trường đám mây sẽ có khả năng tấn công dữ liệu của tất cả người dùng. bên trong các báo cáo vi phạm của Verizon Business blog nó đã được tuyên bố rằng tội phạm bên ngoài là kẻ lớn nhất mối đe dọa (73%), nhưng lại được ít tác động nhất (30.000 bản ghi bị xâm phạm), dẫn đến lỗ hổng ảo hóa.

**2.5. Giải pháp bảo mật hiện nay**

OWASP liệt kê danh sách các lỗ hổng bảo mật hàng đầu dựa trên đám mây hoặc các mô hình SaaS được cập nhật là mối đe dọa tài nguyên của một số công trình nghiên cứu xảy ra trong lĩnh vực bảo mật đám mây. Các nhóm và tổ chức quan tâm đến phát triển các giải pháp và tiêu chuẩn bảo mật cho đám mây. CSA là tập hợp các nhà cung cấp giải pháp, tổ chức phi lợi nhuận và các cá nhân tham gia thảo luận về thực tiễn tốt nhất hiện tại và tương lai cho thông tin đảm bảo trên đám mây. Tiêu chuẩn đám mây trang web thu thập và điều phối thông tin về các tiêu chuẩn liên quan đến đám mây đang được phát triển bởi các nhóm thay đổi. Giải pháp bảo mật tốt nhất cho các ứng dụng SaaS là để phát triển một kiến trúc bảo mật cứng rắn.

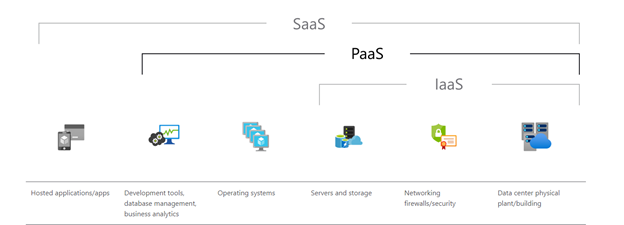
**Chương III. PAAS (Dịch vụ phần mềm)**

**3.1. Giới thiệu**

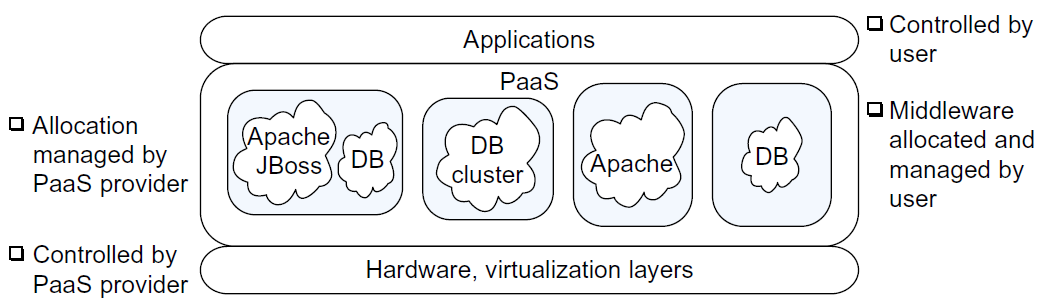
**Platform as a service:** Nền tảng dưới dạng dịch vụ (PaaS) là một môi trường phát triển và triển khai hoàn chỉnh trên đám mây, với các tài nguyên cho phép bạn cung cấp mọi thứ từ các ứng dụng dựa trên đám mây đơn giản đến các ứng dụng doanh nghiệp phức tạp, hỗ trợ đám mây. Người dùng mua các tài nguyên họ cần từ một nhà cung cấp dịch vụ đám mây trên cơ sở trả tiền khi họ di chuyển và truy cập chúng qua kết nối Internet an toàn.

 Giống như IaaS, PaaS bao gồm cơ sở hạ tầng máy chủ, lưu trữ và mạng nhưng cũng có phần mềm trung gian, công cụ phát triển, dịch vụ kinh doanh thông minh (BI), hệ thống quản lý cơ sở dữ liệu, v.v. PaaS được thiết kế để hỗ trợ một vòng đời ứng dụng web hoàn chỉnh: xây dựng, thử nghiệm, triển khai, quản lý và cập nhật.

 PaaS cho phép người sử dụng giảm chi phí và sự phức tạp của việc mua và quản lý giấy phép phần mềm, cơ sở hạ tầng ứng dụng cơ bản và phần mềm trung gian, bộ điều phối vùng chứa như Kubernetes hoặc các công cụ phát triển và các tài nguyên khác. Bạn quản lý các ứng dụng và dịch vụ bạn phát triển và nhà cung cấp dịch vụ đám mây thường quản lý mọi thứ khác.



**Phạm vi kiểm soát:**



**3.2. Các tính năng của PaaS**

Các khả năng cụ thể của PaaS có thể khác nhau giữa các nhà cung cấp và sản phẩm khác nhau. Tuy nhiên, bộ tính năng cốt lõi của PaaS thường bao gồm cơ sở hạ tầng, công cụ phát triển, phần mềm trung gian, hệ điều hành và công cụ quản lý cơ sở dữ liệu.

**Infrastructure (Cơ sở hạ tầng)**:PaaS bao gồm mọi thứ mà IaaS có. Điều này có nghĩa là các nhà cung cấp PaaS sẽ quản lý các máy chủ, bộ lưu trữ, trung tâm dữ liệu và tài nguyên mạng.

**Application design, testing and development tools** ( Các công cụ thiết kế, kiểm tra và phát triển ứng dụng ):PaaS cung cấp cho khách hàng mọi thứ họ cần để xây dựng và quản lý ứng dụng. Các công cụ này có thể được truy cập qua internet thông qua trình duyệt, bất kể vị trí thực tế. Các công cụ phát triển phần mềm cụ thể thường bao gồm, nhưng không giới hạn ở trình gỡ lỗi, trình chỉnh sửa mã nguồn và trình biên dịch.

**Middleware (Phần mềm trung gian):** PaaS cũng thường bao gồm phần mềm trung gian, phần mềm thu hẹp khoảng cách giữa hệ điều hành và các ứng dụng của người dùng cuối. Do đó, người đăng ký PaaS không phải cam kết các nhà phát triển nội bộ và tài nguyên của họ để xây dựng phần mềm trung gian.

**Operating systems (Các hệ điều hành)**: Nhà cung cấp PaaS cung cấp hệ điều hành cho các ứng dụng cũng như để các nhà phát triển xây dựng ứng dụng.

**Databases (Cơ sở dữ liệu)**:Các nhà cung cấp PaaS thường sẽ vừa duy trì cơ sở dữ liệu, vừa cung cấp cho các nhà phát triển của tổ chức khách hàng các công cụ quản lý cơ sở dữ liệu.

**3.3. Đặc điểm của PaaS**

• Xây dựng và phát triển trên công nghệ ảo hóa, điều đó đồng nghĩa là tài nguyên sử dụng tăng giảm một cách dễ dàng dựa vào sự thay đổi của nhu cầu.

• Cung cấp nhiều dịch vụ khác nhau, hỗ trợ phát triển, triển khai, thử nghiệm ứng dụng.

• Cho phép truy cập cùng một lúc nhiều người dùng vào ứng dụng.

• Tích hợp cả các dịch vụ web và cơ sở dữ liệu.

**3.4. Ưu điểm, nhược điểm của Paas**

**3.4.1. Ưu điểm**

• Thời gian tiếp cận thị trường nhanh

Công dụng đầu tiên của PaaS phải nhắc đến đó là nó giúp xây dựng nhanh ứng dụng. Người phát triển không cần quá lo về các vấn đề xây dựng, cấu hình, vấn đề tự cung cấp cơ sở hạ tầng,…Khi sử dụng PaaS, họ chỉ cần quan tâm đến việc viết code, check ứng dụng, các vấn đề khác sẽ được phía nhà cung cấp PaaS chịu trách nhiệm.

• Một môi trường trọn vẹn đầu tới cuối

Các quá trình từ việc xây dựng, thử nghiệm, sau đó fix lỗi, lưu trữ và cập nhật ứng dụng người dùng đều có thể làm trọn vẹn từ đầu tới cuối trên PaaS. Việc này rất quan trọng, vì khi đó nhà phát triển có thể chắc chắn rằng các ứng dụng web của họ đã hoạt động trơn tru, sẵn sàng ra mắt, đơn giản hóa quá trình nâng cấp ứng dụng.

• Chi phí giá cả rẻ

Chi phí để sử dụng PaaS rẻ hơn nhiều, lại mang lại hiệu quả hơn nhiều so với IaaS. Việc không phải quản lý máy chủ với PaaS đã giúp làm giảm tổng chi phí quản lý được giảm đi rất nhiều. Hơn nữa, bạn có thể chọn hình thức thanh toán là dùng đến đâu, thanh toán đến đấy (pay as you go). Khi đó doanh nghiệp chỉ cần phải trả tiền cho nguồn lực của máy tính mà ứng dụng đó tiêu hao, lại tiết kiệm thêm được một khoản tiền cho nhà phát triển. Lưu ý là vẫn có những nhà cung cấp thu một khoản phí mặc định hàng tháng và mỗi công ty có khung giá khác nhau.

• Bản quyền

Các nhà cung cấp PaaS sẽ đăng ký toàn bộ bản quyền cho các công cụ phát triển, hệ điều hành, các ứng dụng khác trên nền tảng.

• Linh hoạt môi trường sử dụng

Chỉ cần có kết nối với Internet là bạn có thể truy cập PaaS, ngồi ở đâu bạn cũng có khả năng tiến hành xây dựng ứng dụng trình duyệt web. Trong môi trường ứng dụng không lưu trữ cục bộ nên việc tương tác với ứng dụng rất linh hoạt. Tạo điều kiện giải quyết công việc đa quốc gia. Nhưng cũng vì thế mà các nhà phát triển có ít quyền kiểm soát môi trường thiết kế sản phẩm một chút.

• Hỗ trợ nhiều ngôn ngữ

PaaS hỗ trợ nhiều ngôn ngữ khác nhau: Node.js, Java, Ruby, C#, Go, Python, hoặc PHP, tùy thuộc vào nhà cung cấp giải pháp điện toán đám mây. Linh hoạt cho việc sử dụng các library, framework

**3.4.2. Nhược điểm**

* Không có sự quản lý, kiểm soát chuyên sâu đối với dữ liệu. Các dữ liệu và tài nguyên trên PaaS đều được quản lý bởi bên thứ ba (nhà cung cấp), nên việc tự kiểm soát dữ liệu rất khó khăn và có khả năng bị leak (tiết lộ) ra ngoài.
* Khó khăn khi thay đổi nhà cung cấp. Ví dụ, phần mềm của bạn đang được xây dựng bằng Azure, sau đó bạn muốn chuyển sang AWS thì phải điều chỉnh lại cho tương thích, điều này có thể làm mất khá nhiều thời gian và công sức.
* Đáp ứng với bản cập nhật của nhà cung cấp. Ví dụ, bạn đang sử dụng ngôn ngữ PHP nhưng nhà cung cấp đột nhiên đưa ra một bản cập nhật mới, yêu cầu bạn phải sử dụng ngôn ngữ Java để viết tiếp, điều này có thể gây ra một rắc rối không nhỏ cho bạn.

**3.5. Phân loại PaaS**

Các loại PaaS khác nhau hiện có sẵn cho các nhà phát triển bao gồm các loại sau:

**Public Paas (PaaS công cộng)**: phù hợp nhất để sử dụng trong đám mây công cộng, cho phép người dùng kiểm soát việc triển khai phần mềm trong khi nhà cung cấp đám mây quản lý việc phân phối tất cả các thành phần CNTT chính khác cần thiết cho việc lưu trữ các ứng dụng, bao gồm hệ điều hành, cơ sở dữ liệu, máy chủ và mạng hệ thống lưu trữ.

**Private PaaS** **(PaaS doanh nghiệp)**: thường được phân phối dưới dạng thiết bị hoặc phần mềm trong tường lửa của người dùng và được duy trì trong trung tâm dữ liệu tại chỗ của công ty.

**Hybrid Paas** **(Lai PaaS)**: kết hợp PaaS công cộng và PaaS tư nhân để cung cấp cho các công ty tính linh hoạt của năng lực vô hạn được cung cấp bởi PaaS công cộng và hiệu quả chi phí của việc sở hữu cơ sở hạ tầng nội bộ trong PaaS tư nhân. Lai PaaS sử dụng một đám mây lai.

**Communications PaaS** **(Truyền thông PaaS)**: là một nền tảng dựa trên đám mây cho phép các nhà phát triển thêm giao tiếp thời gian thực vào ứng dụng của họ mà không cần cơ sở hạ tầng và giao diện phụ trợ.

**Mobile PaaS** **(PaaS di động)**: là việc sử dụng môi trường phát triển tích hợp trả phí để cấu hình các ứng dụng di động, được phân phối thông qua trình duyệt web và thường hỗ trợ đám mây công cộng, đám mây riêng và lưu trữ tại chỗ.

**OpenPaaS**: là một nền tảng cộng tác hướng tới doanh nghiệp, là mã nguồn mở, miễn phí, hấp dẫn trên tất cả các thiết bị và cung cấp các ứng dụng web hữu ích, bao gồm lịch, danh bạ và ứng dụng thư.

**3.6. Ứng dụng PaaS trong công việc**

**3.6.1. Cách sử dụng PaaS phổ biến**

Sử dụng trong việc phát triển các ứng dụng di động. Ngoài ra, nhiều nhà phát triển và công ty còn sử dụng PaaS để xây dựng các ứng dụng đa nền tảng vì nó cung cấp giải pháp linh hoạt và năng động, đặc biệt có khả năng tạo một ứng dụng có thể hoạt động trên hầu hết mọi thiết bị.

Trong các công cụ DevOps, PaaS cung cấp các tính năng quản lý vòng đời ứng dụng cũng như các tính năng cụ thể để phù hợp với các phương pháp phát triển sản phẩm của công ty. Đặc biệt, các công ty theo mô hình thác nước có thể cập nhật bằng cách sử dụng cùng bảng điều khiển họ sử dụng để quản lý hàng ngày.

Tự động hóa hoặc loại bỏ hoàn toàn các nhiệm vụ bảo trì và bảo trì để giảm thời gian ứng dụng ra thị trường. Không chỉ vậy, PaaS có thể giảm quản lý cơ sở hạ tầng bằng cách giúp giảm gánh nặng quản lý cơ sở hạ tầng có thể mở rộng. PaaS loại bỏ sự phức tạp của cân bằng tải, đồng thời nhân rộng và phân phối các dịch vụ phụ thuộc mới thay cho các nhà phát triển kiểm soát các nhiệm vụ này.

PaaS cung cấp cho các ngôn ngữ và công nghệ lập trình mới hơn, điển hình như các chức năng và bộ chứa không có máy chủ. Khi đó, các nhà phát triển có thể sử dụng mô hình để giới thiệu các kênh phát triển kỹ thuật mới.

PaaS đặc biệt phù hợp với các ngành công nghiệp mà sự thay đổi kỹ thuật là một quá trình chậm chạp như ngân hàng và sản xuất bởi PaaS cho phép các tổ chức này thích ứng với các dịch vụ mới nhất mà không thay đổi hoàn toàn quy trình kinh doanh của họ.

**3.6.2. Sử dụng PaaS trong các tổ chức**

**Development framework** (Khung phát triển):PaaS cung cấp một khuôn khổ mà các nhà phát triển có thể xây dựng để phát triển hoặc tùy chỉnh các ứng dụng dựa trên đám mây. Tương tự như cách bạn tạo macro Excel, PaaS cho phép các nhà phát triển tạo ứng dụng bằng cách sử dụng các thành phần phần mềm tích hợp sẵn. Các tính năng đám mây như khả năng mở rộng, tính khả dụng cao và khả năng nhiều người thuê được bao gồm, giảm số lượng mã hóa mà các nhà phát triển phải thực hiện.

**Analytics or business intelligence** (Phân tích hoặc thông tin kinh doanh)**:** Các công cụ được cung cấp dưới dạng dịch vụ với PaaS cho phép các tổ chức phân tích và khai thác dữ liệu của họ, tìm hiểu thông tin chi tiết và các mẫu cũng như dự đoán kết quả để cải thiện dự báo, quyết định thiết kế sản phẩm, lợi nhuận đầu tư và các quyết định kinh doanh khác

**Additional services** (Các dịch vụ bổ sung): Các nhà cung cấp PaaS có thể cung cấp các dịch vụ khác để nâng cao ứng dụng, chẳng hạn như quy trình làm việc, thư mục, bảo mật và lập lịch.

**3.6.3. Trường hợp sử dụng PaaS**

* Startup công nghệ đang có nhu cầu xây dựng hệ thống.
* Doanh nghiệp phần mềm đang có nhu cầu phát triển, mở rộng một cách dễ dàng, nhanh chóng.

PaaS cũng cực kỳ hữu ích nếu bạn muốn tạo một ứng dụng tùy chỉnh cho riêng mình. Dịch vụ điện toán đám mây này có thể giúp làm giảm đáng kể chi phí và đơn giản hóa các thách thức xuất hiện nếu bạn cần triển khai nhanh chóng một ứng dụng.

**3.7. Bảo mật PaaS**

**3.7.1. Thực tiễn bảo mật PaaS**

Trong đám mây, bảo mật là trách nhiệm được chia sẻ giữa nhà cung cấp đám mây và khách hàng. Khách hàng của PaaS chịu trách nhiệm bảo mật các ứng dụng, dữ liệu và quyền truy cập của người dùng. Nhà cung cấp PaaS bảo mật hệ điều hành và cơ sở hạ tầng vật lý.

Dưới đây là bảy phương pháp hay nhất về bảo mật PaaS để bảo mật dữ liệu và ứng dụng của tổ chức trên đám mây.

Nghiên cứu bảo mật của nhà cung cấp**:** Năm 2019, Theo báo cáo của McAfee Chỉ 8% trong số 25,000 dịch vụ đám mây đang được sử dụng hiện nay, đáp ứng các yêu cầu bảo mật dữ liệu được xác định trong Chương trình CloudTrust. Chỉ 1/10 mã hóa dữ liệu ở trạng thái mới và chỉ 18% hỗ trợ xác thực đa yếu tố. Kiểm tra các quy trình bảo mật để nhân viên truy cập vào hệ thống CNTT và các cơ sở vật chất. Đặt câu hỏi về kế hoạch ứng phó sự cố khi vi phạm bảo mật xảy ra hay không, cũng như kế hoạch khôi phục dữ liệu khi toàn bộ hệ thống ngừng hoạt động. Nếu dịch vụ PaaS gặp sự cố, điều gì sẽ xảy ra với các ứng dụng và dữ liệu đang chạy trên đó?

Sử dụng mô hình mối đe dọa**:** Phần lớn các lỗi bảo mật được đưa ra trong giai đoạn đầu của quá trình phát triển phần mềm. Các nhà phát triển có ý thức bảo mật,  có thể xác định và sửa chữa các lỗ hổng tiềm ẩn trong thiết kế ứng dụng, bằng cách sử dụng các công cụ và thực hành mô hình hóa mối đe dọa. Dự án Bảo mật ứng dụng Web Mở (OWASP) có thông tin về mô hình hóa mối đe dọa và Microsoft cung cấp công cụ và thông tin mô hình hóa mối đe dọa miễn phí.

Kiểm tra các lỗ hổng phần mềm kế thừa**:** Các nền tảng và thư viện của bên thứ ba thường có lỗ hổng bảo mật. Các nhà phát triển có thể kế thừa chúng, nếu họ tìm không thấy các lỗ hổng bảo mật tiềm năng.

Triển khai các kiểm soát truy cập dựa trên nhiệm vụ:Quản lý danh tính và quyền truy cập dựa trên nhiệm vụ, giúp đảm bảo nhà phát triển và người dùng khác có quyền truy cập vào các tài nguyên và công cụ mà họ cần, chứ không phải các tài nguyên khác.

Quản lý các tài khoản không hoạt động: Các tài khoản không được sử dụng cung cấp cơ hội tiềm năng cho tin tặc. Hủy cấp phép các tài khoản nhân viên cũ và các tài khoản không hoạt động khác. Tin tặc tìm kiếm những người gần đây, đã rời khỏi hoặc gia nhập các công ty, như LinkedIn là một nguồn tuyệt vời cho việc đó  và chiếm lấy các tài khoản. Ngoài ra, khóa thông tin đăng nhập tài khoản gốc, để ngăn truy cập trái phép vào tài khoản quản trị.

Tận dụng tài nguyên của nhà cung cấp: Hầu hết các nhà cung cấp PaaS lớn đều đưa ra các nguyên tắc và phương pháp hay nhất, để xây dựng trên nền tảng của họ. Nhiều người cũng cung cấp hỗ trợ kỹ thuật, thử nghiệm, tích hợp và trợ giúp khác cho các nhà phát triển.

**3.7.2. Giải pháp bảo mật PaaS**

Các tổ chức có thể triển khai các công nghệ bảo mật của riêng họ, để bảo vệ dữ liệu và ứng dụng của họ khỏi bị đánh cắp hoặc truy cập trái phép. Ba giải pháp bảo mật đám mây quan trọng là: Chương trình bảo mật truy cập đám mây, nền tảng bảo vệ dữ liệu công việc trên đám mây và quản lý tư thế bảo mật đám mây.

Chương trình giới bảo mật truy cập đám mây (CASB): Còn được gọi là cổng bảo mật đám mây (CSG), cung cấp nhiều dịch vụ bảo mật khác nhau, chẳng hạn như giám sát các dịch vụ đám mây trái phép, thực thi các chính sách bảo mật dữ liệu bao gồm ngăn chặn mất dữ liệu (DLP), hạn chế quyền truy cập vào các dịch vụ đám mây dựa trên người dùng, thiết bị và ứng dụng và kiểm tra cấu hình đám mây để tuân thủ và rủi ro.

Nền tảng bảo vệ dữ liệu công việc trên đám mây (CWPP): Các khối lượng công việc và vùng chứa không được bảo mật, cung cấp cho tội phạm mạng một đường dẫn vào môi trường đám mây, do đó, các nền tảng bảo vệ dữ liệu công việc trên đám mây phát hiện và giám sát các vùng chứa và các dữ liệu công việc. Các dịch vụ CWPP cũng áp dụng tính năng bảo vệ chống phần mềm độc hại và đơn giản hóa việc quản lý bảo mật trên nhiều môi trường PaaS.

Quản lý tư thế bảo mật đám mây (CSPM):Người quản lý tư thế bảo mật liên tục kiểm tra môi trường đám mây, để tìm các vấn đề về bảo mật và tuân thủ, cũng như cung cấp biện pháp khắc phục thủ công hoặc tự động. Ngày càng có nhiều CASB bổ sung thêm chức năng CSPM.

Bảo mật đám mây tiếp tục được cải thiện với những tiến bộ mới trong kiến ​​trúc và công nghệ bảo mật. Ví dụ, sự ra đời của các vùng chứa, gói các ứng dụng riêng lẻ và sự phụ thuộc của chúng, giúp phát triển PaaS an toàn hơn, bằng cách cô lập các phiên bản ứng dụng riêng lẻ, khỏi các lỗ hổng trong các ứng dụng khác trên cùng một máy chủ.

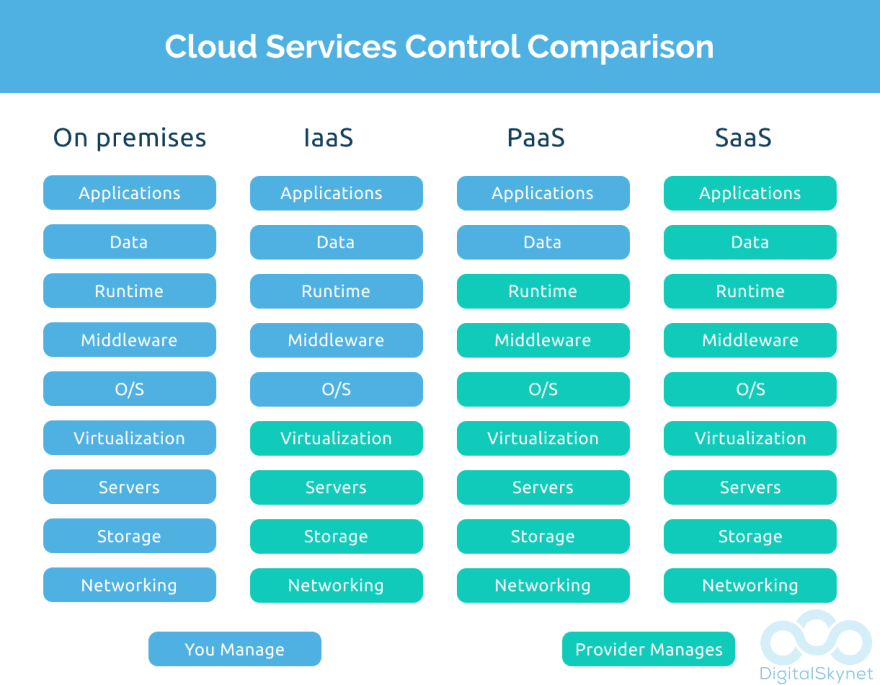
Khi nhiều ứng dụng doanh nghiệp di chuyển vào đám mây, sẽ có nhiều nhà phát triển sử dụng PaaS, để tạo các ứng dụng gốc đám mây và kích hoạt các ứng dụng tại chỗ trên đám mây. Để giảm thiểu nguy cơ bị tấn công mạng, vi phạm dữ liệu và các sự cố bảo mật khác, các nhà quản lý CNTT nên tuân theo các phương pháp hay nhất về bảo mật ứng dụng và triển khai các công nghệ bảo mật đám mây tiên tiến, cập nhật.

Các giải pháp bảo mật đám mây của McAfee cho phép các tổ chức đẩy nhanh tốc độ phát triển kinh doanh và chuyển đổi kỹ thuật số, bằng cách cung cấp cho họ khả năng hiển thị và kiểm soát dữ liệu của họ trên đám mây. Tìm hiểu thêm về công nghệ bảo mật đám mây McAfee.

# **Chương IV: So sánh vai trò và trách nhiệm của Nhà cung cấp và Khách hàng**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **IaaS** | **SaaS** | **PaaS** |
| **Nhà cung cấp** | - Cung cấp cho khách hàng tài nguyên hạ tầng điện toán như máy chủ, mạng , không gian lưu trữ và các công cụ quản trị tài nguyên đó.  - Có thể cung cấp các tài nguyên bổ sung như thư viện ảnh đĩa máy ảo , lưu trữ khối thô, lưu trữ tệp hoặc đối tượng , tường lửa, bộ cân bằng tải, địa chỉ IP, mạng cục bộ ảo (VLAN) và các gói phần mềm.  - Hỗ trợ số lượng lớn máy ảo và khả năng mở rộng quy mô dịch vụ lên và xuống theo các yêu cầu khác nhau của khách hàng.  - Lập hóa đơn cho các dịch vụ IaaS trên cơ sở điện toán tiện ích: chi phí phản ánh lượng tài nguyên được phân bổ và tiêu thụ.  - Nhà cung cấp kiểm soát toàn bộ ngăn xếp máy tính mà bạn có thể truy cập bằng trình duyệt web. Các ứng dụng này chạy trên đám mây. | - Quản lý thiết lập vị trí các ứng dụng.  - Quản lý và kiểm soát phần cứng, ảo hóa, hệ điều hành và các phần mềm sụn.  - Cho phép khách hàng cung cấp (thông qua một giao diện tự phục vụ hoặc bằng cách làm việc với nhân viên nhà cung cấp ứng dụng) logo tùy chỉnh và đôi khi là một bộ màu tùy chỉnh.  - Không phải tốn tài nguyên để cập nhật và duy trì các phiên bản phần mềm đã lỗi thời, vì chỉ có một phiên bản duy nhất.  - Có quyền truy cập vào tất cả dữ liệu của khách hàng, tiến hành kiểm tra thiết kế và hồi quy.  - Có quyền truy cập vào hành vi của người dùng trong ứng dụng (thường thông qua phân tích trang web), giúp dễ dàng xác định các khu vực xứng đáng để cải thiện.  - Có thể cung cấp các tính năng cho phép người dùng của họ cộng tác và chia sẻ thông tin. | - Cung cấp nền tảng điện toán.  - Cung cấp mạng, máy chủ , bộ nhớ , hệ điều hành (OS), phần mềm trung gian (ví dụ: thời gian chạy Java , thời gian chạy .NET , tích hợp, v.v. .), cơ sở dữ liệu và các dịch vụ khác để lưu trữ ứng dụng của người tiêu dùng.  - Cung cấp dịch vụ lưu trữ ứng dụng và môi trường triển khai, cùng với các dịch vụ tích hợp khác nhau. Các dịch vụ cung cấp các mức độ khác nhau về khả năng mở rộng và bảo trì.  - Cho phép các khách hàng thêm các tính năng liên lạc theo thời gian thực (thoại, video và nhắn tin) trong các ứng dụng của riêng họ mà không cần xây dựng cơ sở hạ tầng và giao diện back-end. |
| **Khách hàng** | - Có thể triển khai và chạy phần mềm tùy ý, có thể bao gồm hệ điều hành và ứng dụng.  - Không quản lý hoặc kiểm soát cơ sở hạ tầng đám mây bên dưới nhưng có quyền kiểm soát hệ điều hành, bộ nhớ và các ứng dụng đã triển khai; và có thể hạn chế kiểm soát các thành phần mạng được chọn (ví dụ: tường lửa máy chủ).  - Có thể sử dụng Internet hoặc đám mây của nhà cung cấp dịch vụ (mạng riêng ảo chuyên dụng).  - Để triển khai các ứng dụng, khách hàng có thể cài đặt hình ảnh hệ điều hành và phần mềm ứng dụng của họ trên cơ sở hạ tầng đám mây.  - Có thể tự vá và bảo trì hệ điều hành và phần mềm ứng dụng. | - Quản lý việc sử dụng tài nguyên và sử dụng các ứng dụng dịch vụ.  - Có thể thay đổi tập hợp các tùy chọn cấu hình (còn gọi là tham số) ảnh hưởng đến chức năng và giao diện của phần mềm được cung cấp. | - Quản lý các ứng dụng và dữ liệu.  - Kiểm soát việc triển khai phần mềm với các tùy chọn cấu hình tối thiểu.  - Có thể viết một ứng dụng và tải nó lên một PaaS hỗ trợ ngôn ngữ phần mềm mà họ lựa chọn và ứng dụng chạy trên PaaS đó.  - Được sử dụng bất kỳ ngôn ngữ lập trình, cơ sở dữ liệu, hệ điều hành hoặc máy chủ nào để triển khai các ứng dụng của họ. |

Một cách khác để so sánh IaaS, PaaS và SaaS là ​​dựa trên lượng quản lý được để lại cho khách hàng (màu xanh lam) so với lượng quản lý còn lại cho nhà cung cấp dịch vụ đám mây (màu xanh lá).



|  |  |
| --- | --- |
| **BẢNG PHÂN CÔNG NHIỆM VỤ CỦA TỪNG THÀNH VIÊN** | |
| Tìm hiểu về IaaS:   * Dịch vụ cơ sở hạ tầng * Mục đích sử dụng IaaS * Nhà cung cấp dịch vụ IaaS * Quản lí bảo mật IaaS | Bùi Anh Hiếu |
| Phạm Thu Phương |
| Tìm hiểu về SaaS:   * Giới thiệu về SaaS * Vấn đề bảo mật trong SaaS * Những thách thức về bảo mật * Giải pháp bảo mật hiện nay * Ưu nhược điểm của SaaS * Phát triển SaaS tại Việt Nam | Trần Đức Lương |
| Nguyễn Thị Hồng Quyên |
| Tìm hiểu về PaaS:   * Giới thiệu về PaaS * Các tính năng của PaaS * Đặc điểm của PaaS * Ưu nhược điểm của PaaS * Phân loại PaaS * Ứng dụng của PaaS * Bảo mật PaaS | Lâm Thăng Long |
| Thân Quang Phước |

**Tài liệu tham khảo**

* Syngress.Securing.The.Cloud.Cloud.Computer.Security.Techniques.And.Tactics.Apr.2011.ISBN.1597495921
* Cloud Computing - Implementation, Management and security
* Secure Cloud Computing ( PDFDrive.com )
* <https://www.ijser.org/researchpaper/Security-issues-in-SaaS-of-cloud-computing.pdf>
* <https://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service>
* <https://azure.microsoft.com/en-us/overview/what-is-paas/>
* <https://www.bigcommerce.com/blog/saas-vs-paas-vs-iaas/#the-three-types-of-cloud-computing-service-models-explained>
* https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/