HUỲNH QUYẾT THẮNG (Chủ biên)
NGUYỄN HỮU ĐỨC - DOÃN TRUNG TÙNG
NGUYỄN BÌNH MINH - TRẦN VIỆT TRUNG

ĐIỆN TOÁN ĐÁM MÂY

NHÀ XUẤT BẢN BÁCH KHOA HÀ NỘI

HUỲNH QUYẾT THẮNG (Chủ biên)
NGUYỄN HỮU ĐỨC - DOÃN TRUNG TÙNG
NGUYỄN BÌNH MINH - TRẦN VIỆT TRUNG
ĐIỆN TOÁN ĐÁM MÂY

HUỲNH QUYẾT THẮNG (Chủ biên)
NGUYỄN HỮU ĐỨC – DOÃN TRUNG TÙNG
NGUYỄN BÌNH MINH – TRẦN VIỆT TRUNG

ĐIỆN TOÁN ĐÁM MÂY

(Xuất bản lần thứ hai)

NHÀ XUẤT BẢN BÁCH KHOA HÀ NỘI

Biên mục trên xuất bản phẩm của Thư viện Quốc gia Việt Nam

Điện toán đám mây / Huỳnh Quyết Thắng (ch.b.), Nguyễn Hữu Đức, Doãn Trung Tùng... - H. : Bách khoa Hà Nội, 2020. - 138tr. : hình vẽ, bảng ; 24cm

Thư mục: tr. 135

1. Điện toán đám mây 2. Giáo trình

004.6782 - dc23

BKD0005p-CIP

LỜI MỞ ĐẦU

Với sự phát triển bùng nổ hiện nay của công nghệ thông tin và ứng dụng trong đời sống, điện toán đám mây trở nên có tầm quan trọng thời sự. Giáo trình ***Điện toán đám mây*** được biên soạn cho đối tượng là học viên cao học các chuyên ngành Công nghệ thông tin. Sinh viên năm cuối của các trường đại học kỹ thuật cũng có thể sử dụng giáo trình như một tài liệu tham khảo để phát triển các ứng dụng cho nghiên cứu, cho đồ án tốt nghiệp.

Các tác giả hy vọng thông qua giáo trình sẽ cung cấp cho người đọc một tiếp cận tổng thể tới các khái niệm cơ bản về điện toán đám mây, các vấn đề về lưu trữ và xử lý dữ liệu, các vấn đề về an toàn và bảo mật, các dịch vụ, kiến trúc dịch vụ, hệ giám sát, một số chủ đề nâng cao gợi mở các vấn đề nghiên cứu hiện nay trong lĩnh vực điện toán đám mây.

Giáo trình là kết quả tổng hợp các nội dung nghiên cứu trong khuôn khổ đề tài tiến sỹ của các tác giả khi học tập tại nước ngoài, một số kết quả nghiên cứu khi triển khai đề tài khoa học công nghệ cấp Nhà nước: "Nghiên cứu làm chủ công nghệ dịch vụ đám mây (tạo lập và cung cấp dịch vụ, cung cấp nội dung số, quản lý truy cập)" mã số KC.01.01/11–15 và các kiến thức, kinh nghiệm qua nhiều năm giảng dạy tại Đại học Bách Khoa Hà Nội. Một số nội dung đã được giảng dạy thử nghiệm cho các khóa thạc sỹ 2012, 2013 của Viện Công nghệ Thông tin & Truyền thông và sau đó đã được chỉnh sửa để phù hợp với sự thay đổi công nghệ.

Giáo trình được xuất bản lần đầu nên không tránh khỏi những khiếm khuyết nhất định. Ngoài ra, do tính chất đặc thù phát triển nhanh chóng của lĩnh vực điện toán đám mây, nên nội dung giáo trình chưa hoàn toàn cập nhật, cô đọng, thiếu các diễn giải chi tiết, nhiều vấn đề chỉ nêu mà chưa minh họa. Chúng tôi mong nhận được nhiều ý kiến đóng góp cụ thể của các bạn độc giả để có thể sửa chữa, bổ sung và làm tốt hơn trong các lần xuất bản sau.

Tập thể tác giả xin bày tỏ sự cám ơn chân thành tới Bộ Khoa học và Công nghệ, Bộ Giáo dục và Đào tạo, Trường Đại học Bách Khoa Hà Nội đã tạo điều kiện để phát triển các nghiên cứu chuyên sâu. Chúng tôi cũng đặc biệt cám ơn các bạn đồng nghiệp ở Viện Công nghệ Thông tin & Truyền thông đã có những góp ý chân thành để giáo trình được hoàn thiện.

Mọi ý kiến đóng góp xin gửi về tập thể tác giả theo địa chỉ sau:

PGS. TS. Huỳnh Quyết Thắng, TS. Nguyễn Hữu Đức

Phòng 504, nhà B1, Viện Công nghệ Thông tin & Truyền thông, Trường Đại học Bách Khoa Hà Nội, số 1 Đại Cồ Việt, Hai Bà Trưng, Hà Nội.

Email: thang.huynhquyet@hust.edu.vn

duc.nguyenhuu@hust.edu.vn

tung.doantrung@hust.edu.vn

minh.nguyenbinh@hust.edu.vn

trung.tranviet@hust.edu.vn

Các tác giả

MỤC LỤC

Chương mở đầu
TỔNG QUAN ĐIỆN TOÁN ĐÁM MÂY

A. LỊCH SỬ RA ĐỜI CỦA ĐIỆN TOÁN ĐÁM MÂY

Khái niệm điện toán đám mây ra đời từ những năm 1950 khi máy chủ tính toán quy mô lớn (large-scale mainframe computers) được triển khai tại một số cơ sở giáo dục và tập đoàn lớn. Tài nguyên tính toán của các hệ thống máy chủ được truy cập từ các máy khách cuối (thin clients, terminal computers), từ đó khai sinh khái niệm "chia sẻ thời gian" (time-sharing) đặc tả việc cho phép nhiều người sử dụng cùng chia sẻ đồng thời một tài nguyên tính toán chung.

Trong những năm 1960 – 1990, xuất hiện luồng tư tưởng coi máy tính hay tài nguyên công nghệ thông tin có thể được tổ chức như hạ tầng dịch vụ công cộng (public utility). Điện toán đám mây hiện tại cung cấp tài nguyên tính toán dưới dạng dịch vụ và tạo cảm giác cho người dùng về một nguồn cung ứng là vô tận. Đặc tính này có thể so sánh tới các đặc tính của ngành công nghiệp tiêu dùng dịch vụ công cộng như điện và nước. Khi sử dụng điện hay nước, người dùng không cần quan tâm tới tài nguyên đến từ đâu, được xử lý, phân phối như thế nào, họ chỉ việc sử dụng dịch vụ và trả tiền cho nhà cung cấp theo lượng tiêu dùng của mình.

Những năm 1990, các công ty viễn thông từ chỗ cung ứng kênh truyền dữ liệu điểm tới điểm (point-to-point data circuits) riêng biệt đã bắt đầu cung ứng các dịch vụ mạng riêng ảo với giá thấp. Thay đổi này tạo tiền đề để các công ty viễn thông sử dụng hạ tầng băng thông mạng hiệu quả hơn. Điện toán đám mây mở rộng khái niệm chia sẻ băng thông mạng này qua việc cho phép chia sẻ cả tài nguyên máy chủ vật lý bằng việc cung cấp các máy chủ ảo.

Amazon cung cấp nền tảng Amazon Web Services (AWS) vào năm 2006, đánh dấu việc thương mại hóa điện toán đám mây. Từ đầu năm 2008, Eucalyptus được giới thiệu là nền tảng điện toán đám mây mã nguồn mở đầu tiên, tương thích với API của AWS. Tính tới thời điểm hiện tại, có rất nhiều các sản phẩm điện toán đám mây được đưa ra như Google App Engine, Microsoft Azure, Nimbus,...

B. KHÁI NIỆM VỀ ĐIỆN TOÁN ĐÁM MÂY

Điện toán đám mây (cloud computing) là một xu hướng công nghệ nổi bật trên thế giới trong những năm gần đây và đã có những bước phát triển nhảy vọt cả về chất lượng, quy mô cung cấp và loại hình dịch vụ, với một loạt các nhà cung cấp nổi tiếng như Google, Amazon, Salesforce, Microsoft,...

Điện toán đám mây là mô hình điện toán mà mọi giải pháp liên quan đến công nghệ thông tin đều được cung cấp dưới dạng các dịch vụ qua mạng Internet, giải phóng người sử dụng khỏi việc phải đầu tư nhân lực, công nghệ và hạ tầng để triển khai hệ thống. Từ đó điện toán đám mây giúp tối giản chi phí và thời gian triển khai, tạo điều kiện cho người sử dụng nền tảng điện toán đám mây tập trung được tối đa nguồn lực vào công việc chuyên môn.

Lợi ích của điện toán đám mây mang lại không chỉ gói gọn trong phạm vi người sử dụng nền tảng điện toán đám mây mà còn từ phía các nhà cung cấp dịch vụ điện toán. Theo những đánh giá của nhóm IBM CloudBurst năm 2009, trên môi trường điện toán phân tán có đến 85% tổng năng lực tính toán trong trạng thái nhàn rỗi, thiết bị lưu trữ tăng 54% mỗi năm, khoảng 70% chi phí được dành cho việc duy trì các hệ thống thông tin. Công nghiệp phần mềm mất đi 40 tỷ USD hằng năm vì việc phân phối sản phẩm không hiệu quả, khoảng 33% khách hàng phàn nàn về các lỗi bảo mật do các công ty cung cấp dịch vụ. Những thống kê này đều chỉ đến một điểm quan trọng: mô hình hệ thống thông tin hiện tại đã lỗi thời và kém hiệu quả, cần phải chuyển sang một mô hình điện toán mới – đó là điện toán đám mây.

Theo định nghĩa của Viện Quốc gia Tiêu chuẩn và Công nghệ Mỹ (US NIST), điện toán đám mây là mô hình cho phép truy cập trên mạng tới các tài nguyên được chia sẻ (ví dụ: hệ thống mạng, máy chủ, thiết bị lưu trữ, ứng dụng và các dịch vụ) một cách thuận tiện và theo nhu cầu sử dụng. Những tài nguyên này có thể được cung cấp một cách nhanh chóng hoặc thu hồi với chi phí quản lý tối thiểu hoặc tương tác tối thiểu với nhà cung cấp dịch vụ.

C. CÁC ĐẶC TÍNH CỦA ĐIỆN TOÁN ĐÁM MÂY

Định nghĩa của US NIST chứa đựng kiến trúc, an ninh và chiến lược triển khai của đám mây. Năm đặc tính cốt lõi của điện toán đám mây được thể hiện rõ như sau:

– Tự phục vụ theo yêu cầu (on-demand self-service): Khách hàng với nhu cầu tức thời tại những thời điểm thời gian xác định có thể sử dụng các tài nguyên tính toán (như thời gian CPU, không gian lưu trữ mạng, sử dụng phần mềm,...) một cách tự động, không cần tương tác với con người để cấp phát.

– Sự truy cập mạng rộng rãi (broad network access): Những tài nguyên tính toán này được phân phối qua mạng Internet và được các ứng dụng client khác nhau sử dụng với những nền tảng không đồng nhất (như máy tính, điện thoại di động, PDA).

– Tập trung tài nguyên: Những tài nguyên tính toán của nhà cung cấp dịch vụ đám mây được tập trung với mục đích phục vụ đa khách hàng sử dụng mô hình ảo hóa với những tài nguyên vật lý và tài nguyên ảo được cấp phát động theo yêu cầu. Động lực của việc xây dựng một mô hình tập trung tài nguyên tính toán nằm trong hai yếu tố quan trọng: tính quy mô và tính chuyên biệt. Kết quả của mô hình tập trung tài nguyên là những tài nguyên vật lý trở nên trong suốt với người sử dụng. Ví dụ, người sử dụng không được biết vị trí lưu trữ cơ sở dữ liệu của họ trong đám mây.

– Tính mềm dẻo: Đối với người sử dụng, các tài nguyên tính toán được cung cấp tức thời hơn là liên tục, được cung cấp theo nhu cầu để mở rộng hoặc tiết giảm không hạn định tại bất kỳ thời điểm nào.

– Khả năng đo lường: Mặc dù tài nguyên được tập trung và có thể chia sẻ cho nhiều người sử dụng, hạ tầng của đám mây có thể dùng những cơ chế đo lường thích hợp để đo việc sử dụng những tài nguyên đó cho từng cá nhân.

D. SƠ LƯỢC CÁC CÔNG NGHỆ ỨNG DỤNG TRONG ĐIỆN TOÁN ĐÁM MÂY

Công nghệ ảo hoá

Công nghệ ảo hóa (virtualization) là công nghệ quan trọng nhất ứng dụng trong điện toán đám mây. Công nghệ ảo hóa là công nghệ cho phép tạo ra các thực thể ảo có tính năng tương đương như các thực thể vật lý, ví dụ như thiết bị lưu trữ, bộ vi xử lý,... Ảo hóa phần cứng (hardware virtualization) tham chiếu tới việc tạo ra các máy ảo (virtual machine) mà hoạt động với hệ điều hành được cài đặt như một máy tính vật lý thực. Ví dụ, một máy ảo chạy hệ điều hành Ubuntu có thể được tạo ra trên một máy tính thực cài hệ điều hành Windows.

Ảo hoá phần cứng cho phép chia nhỏ tài nguyên vật lý để tối ưu hóa hiệu năng sử dụng. Điều này được thể hiện qua việc có thể khởi tạo nhiều máy ảo với năng lực tính toán và năng lực lưu trữ bé hơn trên duy nhất một máy chủ vật lý. Máy chủ vật lý được gọi là host machine còn máy ảo (virtual machine) được gọi là máy khách (guest machine). Khái niệm "host" và "guest" được sử dụng để phân biệt phần mềm chạy trên máy tính vật lý hay phần mềm chạy trên máy ảo. Phần mềm hay firmware tạo máy ảo được gọi là hypervisor hay virtual machine manager.

Công nghệ tự động hóa giám sát điều phối tài nguyên (automation, dynamic dynamic orchestration)

Công nghệ giám sát điều phối tài nguyên động là nền tảng để điện toán đám mây thực hiện cam kết chất lượng cung cấp dịch vụ điện toán. Với công nghệ điều phối tài nguyên động, việc lắp đặt thêm hay giảm bớt các tài nguyên máy chủ vật lý hoặc máy

chủ lưu trữ dữ liệu được thực hiện tự động để hệ thống điện toán luôn đáp ứng được giao kèo trong hợp đồng dịch vụ đã ký với bên người sử dụng.

Công nghệ tính toán phân tán, hệ phân tán

Điện toán đám mây là một dạng hệ phân tán xuất phát từ yêu cầu cung ứng dịch vụ cho lượng người sử dụng khổng lồ. Tài nguyên tính toán của điện toán đám mây là tổng thể kết hợp của hạ tầng mạng và hàng nghìn máy chủ vật lý phân tán trên một hay nhiều trung tâm dữ liệu số (data centers).

Công nghệ Web 2.0

Web 2.0 là nền tảng công nghệ phát triển các sản phẩm ứng dụng hướng dịch vụ trên nền điện toán đám mây. Công nghệ Web 2.0 phát triển cho phép phát triển giao diện ứng dụng web dễ dàng và nhanh chóng và trên nhiều thiết bị giao diện khác nhau. Web 2.0 phát triển làm xóa đi khoảng cách về thiết kế giao diện giữa ứng dụng máy tính thông thường và ứng dụng trên nền web, cho phép chuyển hóa ứng dụng qua dịch vụ trên nền điện toán đám mây mà không ảnh hưởng đến thói quen người sử dụng.

E. ƯU NHƯỢC ĐIỂM CỦA ĐIỆN TOÁN ĐÁM MÂY

Ưu điểm của điện toán đám mây

Triển khai nhanh chóng: So với phương pháp thông thường triển khai một ứng dụng trên internet, người dùng phải thực hiện một loạt các công việc như mua sắm thiết bị (hoặc thuê thiết bị từ bên thứ ba), cài đặt và cấu hình phần mềm, đưa các ứng dụng vào đám mây, việc sử dụng điện toán đám mây giúp loại bỏ một số công việc đòi hỏi thời gian lớn, ví dụ người dùng chỉ việc quan tâm phát triển triển khai các ứng dụng của mình lên "mây" (internet) khi sử dụng các đám mây nền tảng. Bên cạnh đó, khả năng tăng hoặc giảm sự cung cấp tài nguyên nhanh chóng theo nhu cầu tiêu dùng của ứng dụng tại các thời điểm khác nhau nhờ công nghệ ảo hóa của điện toán đám mây cũng là một trong những đặc điểm vượt trội của công nghệ này, thể hiện khả năng triển khai nhanh đáp ứng đòi hỏi tài nguyên tức thời của ứng dụng.

Giảm chi phí: Chi phí được giảm đáng kể do chi phí vốn đầu tư được chuyển sang chi phí duy trì hoạt động. Điều này làm giảm những khó khăn khi người dùng cần tính toán xử lý các tác vụ trong một lần duy nhất hoặc không thường xuyên do họ có thể đi thuê cơ sở hạ tầng được cung cấp bởi bên thứ ba.

Đa phương tiện truy cập: Sự độc lập giữa thiết bị và vị trí làm cho người dùng có thể truy cập hệ thống bằng cách sử dụng trình duyệt web mà không quan tâm đến vị trí của họ hay thiết bị nào mà họ đang dùng, ví dụ như PC, mobile. Vì cơ sở hạ tầng off-site (được cung cấp bởi đối tác thứ ba) và được truy cập thông qua Internet, do đó người dùng có thể kết nối từ bất kỳ nơi nào.

Chia sẻ: Việc cho thuê và chia sẻ tài nguyên giữa các người dùng với nhau làm giảm chi phí đầu tư hạ tầng tính toán giữa một phạm vi lớn người dùng. Sự chia sẻ này cũng cho phép tập trung cơ sở hạ tầng để phục vụ các bài toán lớn với chi phí thấp hơn việc đầu tư hệ thống máy chủ tính toán từ đầu.

Khả năng chịu tải nâng cao: Về lý thuyết, tài nguyên tính toán trên đám mây là vô hạn. Việc thêm vào năng lực tính toán để chịu tải cao có thể được thực hiện chỉ bằng các thao tác kích chuột hoặc đã được tự động hoá.

Độ tin cậy: Người sử dụng điện toán đám mây được ký hợp đồng sử dụng với điều khoản chất lượng dịch vụ rất cao ghi sẵn trong hợp đồng. Chất lượng dịch vụ đám mây đơn giản được đánh giá ổn định hơn hệ thống tự triển khai do nền tảng đám mây được thiết kế và bảo trì bởi đội ngũ chuyên gia nhiều kinh nghiệm về hệ thống. Hơn nữa, việc luôn làm việc với hệ thống lớn và gặp nhiều lỗi tương tự nhau nên quá trình khôi phục hệ thống sau thảm họa thông thường là nhanh chóng.

Tính co giãn linh động: Tính co giãn thể hiện sự linh động trong việc cung cấp tài nguyên tính toán theo nhu cầu thực tế của người dùng hoặc các ứng dụng dịch vụ. Theo đó tài nguyên sẽ được đáp ứng một cách tự động sát với nhu cầu tại thời gian thực mà không cần người dùng phải có kỹ năng cho quá trình điều khiển này.

Bảo mật: Tính bảo mật trong điện toán đám mây từ trước đến nay vẫn là câu hỏi lớn cho người dùng tiềm năng. Tuy nhiên, hiện nay, khả năng bảo mật trong môi trường đám mây đã được cải thiện đáng kể, nhờ vào một số lý do chính sau đây: do dữ liệu tập trung trong các đám mây ngày càng lớn nên các nhà cung cấp luôn chú trọng nâng cao công nghệ và đặt ra những rào cản để tăng tính an toàn cho dữ liệu. Bên cạnh đó, các nhà cung cấp đám mây có khả năng dành nhiều nguồn lực cho việc giải quyết các vấn đề bảo mật mà nhiều khách hàng không có đủ chi phí để thực hiện. Các nhà cung cấp sẽ ghi nhớ các nhật ký truy cập, nhưng việc truy cập vào chính bản thân các nhật ký truy cập này có thể cũng rất khó khăn do chính sách của nhà cung cấp đám mây khi người dùng tự mình muốn xác minh rõ hệ thống của mình có an toàn không. Mặc dù vậy, mối quan tâm lo ngại về việc mất quyền điều khiển dữ liệu nhạy cảm cũng ngày càng tăng cao.

Nhược điểm của điện toán đám mây

Chi phí: Giảm chi phí đầu tư ban đầu là ưu điểm của điện toán đám mây. Tuy nhiên, nó cũng là một vấn đề phải tranh cãi khi người sử dụng điện toán đám mây luôn phải duy trì trả phí sử dụng dịch vụ. So với tự chủ đầu tư hạ tầng, người sử dụng điện toán đám mây không có tài sản sau khấu hao chi phí đầu tư.

Các công cụ giám sát và quản lý: Công cụ giám sát và bảo trì chưa hoàn thiện và khả năng giao tiếp với các đám mây là có giới hạn, mặc dù thông báo gần đây của BMC, CA, Novell cho rằng các ứng dụng quản lý trung tâm dữ liệu đang được cải tiến

để cung cấp kiểm soát tốt hơn dữ liệu trong điện toán đám mây Amazon EC2 và các dịch vụ đám mây.

Chuẩn hóa đám mây: Chuẩn hóa giao tiếp và thiết kế đám mây chưa được thông qua. Mỗi nền tảng cung cấp các giao diện quản lý và giao tiếp ứng dụng API khác nhau. Hiện nay, các tổ chức như Distributed Management Task Force, Cloud Security Alliance và Open Cloud Consortium đang phát triển các tiêu chuẩn về quản lý tương thích, di chuyển dữ liệu, an ninh và các chức năng khác của điện toán đám mây.

Tính sẵn sàng: Tính sẵn sàng là ưu điểm của đám mây trong lý thuyết. Tuy nhiên, trên thực tế với các đám mây hiện thời, tính sẵn sàng đôi khi không được đảm bảo và cũng là một trở ngại hiện nay, khi chỉ có một số ít nhà cung cấp dịch vụ cam kết được về sự sẵn sàng và liên tục của dịch vụ, về thời gian sửa chữa và phục hồi dữ liệu.

Vấn đề tuân thủ hợp đồng cũng trở nên phức tạp: Những nhà cung cấp dịch vụ điện toán đám mây có thể chuyển dữ liệu tới quốc gia khác có giá điện rẻ hơn, nhưng luật lỏng lẻo hơn mà người sử dụng dịch vụ điện toán không được thông tin. Điều này hoàn toàn có thể vì đám mây là trong suốt với người dùng.

Tính riêng tư: Hầu hết các hợp đồng thể hiện giao kèo giữa nhà cung cấp và người dùng điện toán đám mây hứa hẹn một viễn cảnh trong đó dữ liệu khách hàng luôn an toàn và riêng tư. Tuy nhiên, tính riêng tư trong điện toán đám mây cũng là một vấn đề đáng quan tâm vì hạ tầng an toàn thông tin cho đám mây hiện vẫn đang là một chủ đề nghiên cứu trong giới khoa học.

Cấp độ dịch vụ: Điện toán đám mây cung cấp dịch vụ theo yêu cầu, tuy nhiên trong thực tế, các gói dịch vụ thường được định nghĩa trước và người sử dụng căn cứ vào nhu cầu và khả năng để chọn dịch vụ sẵn có. Ví dụ, việc tự cấu hình chi tiết thông số các máy ảo hiện tại chưa thực hiện được. Như vậy, khả năng để thích ứng yêu cầu cấp dịch vụ cho các nhu cầu cụ thể của một doanh nghiệp là ít hơn so với các trung tâm dữ liệu xây dựng riêng với mục đích là để tiếp tục mục tiêu nâng cao khả năng kinh doanh của công ty.

Khả năng tích hợp với hạ tầng thông tin sẵn có của tổ chức: Việc tích hợp điện toán đám mây vào hạ tầng sẵn có của khách hàng chưa có mô hình và cách thức thực hiện cụ thể. Các mô hình kết nối đám mây riêng và đám mây thương mại vẫn đang được nghiên cứu.

F. GIỚI THIỆU MỘT SỐ ĐÁM MÂY ĐƯỢC SỬ DỤNG/ TRIỂN KHAI PHỔ BIẾN HIỆN NAY

Microsoft Azure: Microsoft Azure là đám mây cung cấp hạ tầng và nền tảng điện toán xây dựng bởi Microsoft và đưa vào khai thác từ 2010. Về mặt hạ tầng, Azure cung cấp các máy chủ ảo có thể chạy hệ điều hành Windows hoặc Unix. Về mặt nền tảng

điện toán, Azure hỗ trợ đa ngôn ngữ lập trình cho phép triển khai trên Azure nhiều ứng dụng phát triển trên các công cụ và framework khác nhau. Phổ biến là các ứng dụng viết trên nền .Net của Microsoft.

Amazon Web Service (AWS): AWS được đưa ra vào năm 2006 với khởi đầu là tập lợp các dịch vụ tính toán như dịch vụ máy ảo EC2 và dịch vụ lưu trữ S3. AWS là nền tảng đám mây thương mại đầu tiên và phổ biến nhất hiện nay. Nhiều khách hàng lớn sử dụng AWS có thể nói đến như NASA, Pinterest, Netflix.

Nimbus: Nimbus là đám mây mã nguồn mở cung cấp hạ tầng máy chủ hướng theo dịch vụ thông qua giao diện kết nối dựa trên chuẩn kết nối của AWS.

Google App Engine (GAE): GAE là nền tảng đám mây mà trên đó Google cung cấp hỗ trợ cho cơ sở dữ liệu, các thư viện lập trình và các môi trường thực thi cho các ngôn ngữ lập trình phổ biến. Các ứng dụng trên các ngôn ngữ hỗ trợ sau khi triển khai trên GAE sẽ chạy trên các máy chủ ảo của Google.

G. NỘI DUNG CƠ BẢN CỦA GIÁO TRÌNH

Giáo trình giới thiệu tổng quan về công nghệ điện toán đám mây, cung cấp những kiến thức cơ bản về điện toán đám mây bao gồm các công nghệ được áp dụng và thành phần thiết kế của nó. Các chủ đề liên quan đến công nghệ nền tảng của điện toán đám mây bao gồm: các trung tâm dữ liệu lớn, công nghệ ảo hóa, các giao thức quản lý và điều khiển các dịch vụ đám mây, cơ sở dữ liệu và lưu trữ trong môi trường đám mây, bảo mật và an toàn khi sử dụng ứng dụng đám mây, các phương pháp đảm bảo chất lượng dịch vụ, hợp đồng dịch vụ. Các chủ đề liên quan đến việc triển khai và phát triển các dịch vụ đám mây bao gồm các kiến thức về dịch vụ web, các môi trường lập trình trong đám mây, cấu trúc và thiết kế các dịch vụ đám mây.

Trong Chương mở đầu, giáo trình đề cập đến lịch sử ra đời của điện toán đám mây, từ đó đưa ra khái niệm, định nghĩa về nền tảng đám mây. Chương mở đầu tập trung nêu rõ các đặc tính và ưu nhược điểm của nền tảng.

Trong Chương 1, các dạng điện toán đám mây sẽ được phân tích trên cơ sở hiểu rõ trung tâm dữ liệu lớn và công nghệ ảo hoá. Các mô hình mô phỏng môi trường đám mây cũng sẽ được giới thiệu.

Chương 2 giới thiệu một trong những dịch vụ điện toán đám mây cốt lõi là dịch vụ lưu trữ và xử lý dữ liệu. Chương 2 bắt đầu với tổng quan về các hệ quản lý tập tin phân tán, đi sâu vào phân tích hệ thống tập tin HDFS và mô hình tính toán MapReduce. Các cơ sở dữ liệu không quan hệ NoSQL cũng sẽ được đề cập đến.

Chương 3 phân tích khía cạnh bảo mật của điện toán đám mây. Chương gồm ba phần lớn: các thách thức về bảo mật và an toàn dịch vụ đám mây, các phương pháp bảo đảm an toàn cho dịch vụ đám mây và giải pháp thiết kế cấu trúc của đám mây an toàn.

Trong Chương 4, cách thức xây dựng dịch vụ trên nền tảng đám mây điển hình Azure sẽ được giới thiệu cụ thể.

Chương 5 phân tích khía cạnh giám sát và đảm bảo chất lượng các dịch vụ đám mây.

Chương 6 đưa ra các chủ đề nâng cao như đám mây liên bang, mô hình môi giới dịch vụ,...

Chương 1
NỀN TẢNG VÀ PHÂN LOẠI

Trong chương này, chúng ta sẽ làm quen với các khái niệm khái quát chung của nền tảng và phân loại điện toán đám mây. Người đọc sẽ được trang bị các kiến thức về khái niệm và mô hình của Trung tâm dữ liệu, trên cơ sở đó tiếp thu các kiến thức về công nghệ ảo hóa. Một phần nội dung của chương trình bày phân loại các mô hình điện toán đám mây và các kiến trúc, nền tảng điện toán đám mây đang được cung cấp trên thị trường hiện nay. Một số công cụ và giải pháp mô phỏng điện toán đám mây tại các trung tâm nghiên cứu cũng được giới thiệu để người đọc có thể tiếp cận các công cụ này.

1.1. TRUNG TÂM DỮ LIỆU LỚN

Khái niệm Trung tâm dữ liệu

Về mặt kỹ thuật, trung tâm dữ liệu (TTDL) hay data center có nguồn gốc từ các phòng máy tính lớn (main frames) thời sơ khai của ngành công nghiệp máy tính trong những năm 1960. Tại thời kỳ này, các hệ thống máy tính đầu tiên được coi là những thành tựu lớn lao của công nghệ tính toán tự động dựa trên kỹ thuật điện tử (electronic computing). Các hệ thống này là những hệ thống có những yêu cầu cực kỳ phức tạp trong vận hành, bảo trì, và môi trường hoạt động đặc biệt về nguồn điện, điều hòa không khí.

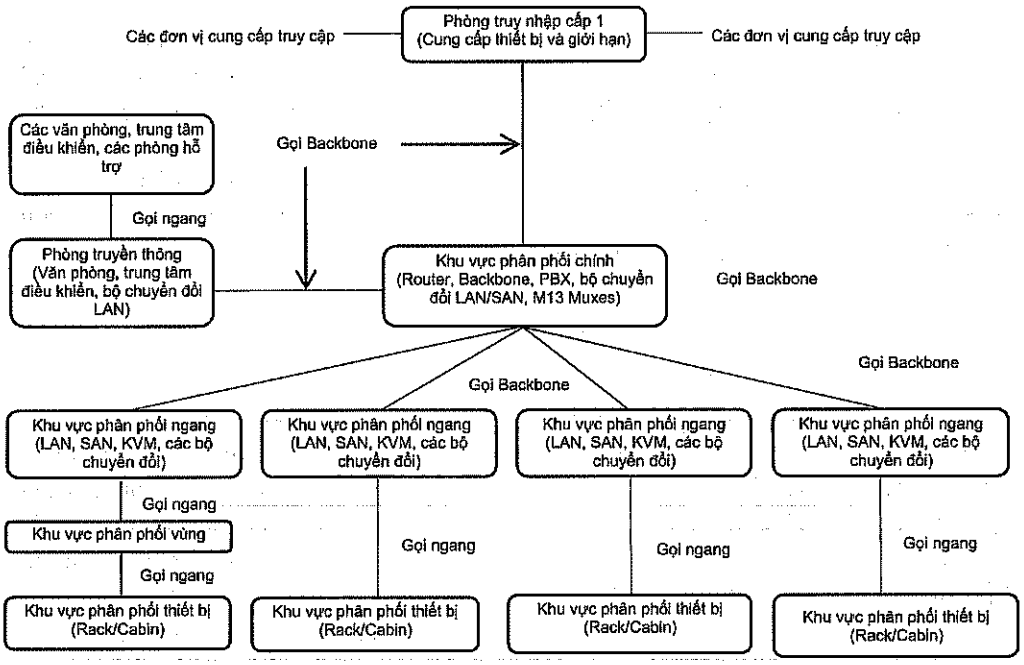
Với sự ra đời của mô hình tính toán "khách – chủ" trong những năm 1990, các máy chủ (server) đã thay thế dần các máy tính lớn trong các phòng máy tính tại các trường đại học và cơ sở nghiên cứu khoa học. Với sự giảm giá mạnh của phần cứng server, các thiết bị kết nối mạng và sự chuẩn hóa các hệ thống cáp mạng, các hệ thống tính toán "client-server" đã dần dần có chỗ đứng riêng trong môi trường của các tổ chức và doanh nghiệp để phục vụ công tác quản lý và kinh doanh. Thuật ngữ TTDL dùng để chỉ các phòng máy tính được thiết kế riêng bên trong tổ chức, doanh nghiệp với những yêu cầu đặc biệt về nguồn điện, điều hòa không khí, cấu trúc liên kết thiết bị và mạng,... bắt đầu đạt được sự công nhận phổ biến trong khoảng thời gian này.

TTDL là giải pháp hoàn chỉnh về một trung tâm điều phối hoạt động, trung tâm lưu trữ, nó có thể cung cấp các ứng dụng cho một tổ chức doanh nghiệp hay phục vụ cho hàng ngàn người cần truy cập, trao đổi thông tin. Mọi hoạt động của TTDL đều có ảnh hưởng rất lớn đến việc kinh doanh, tài chính, cũng như sự sống còn của một doanh nghiệp như các ngân hàng, công ty tài chính, sàn chứng khoán, công ty bảo hiểm,...

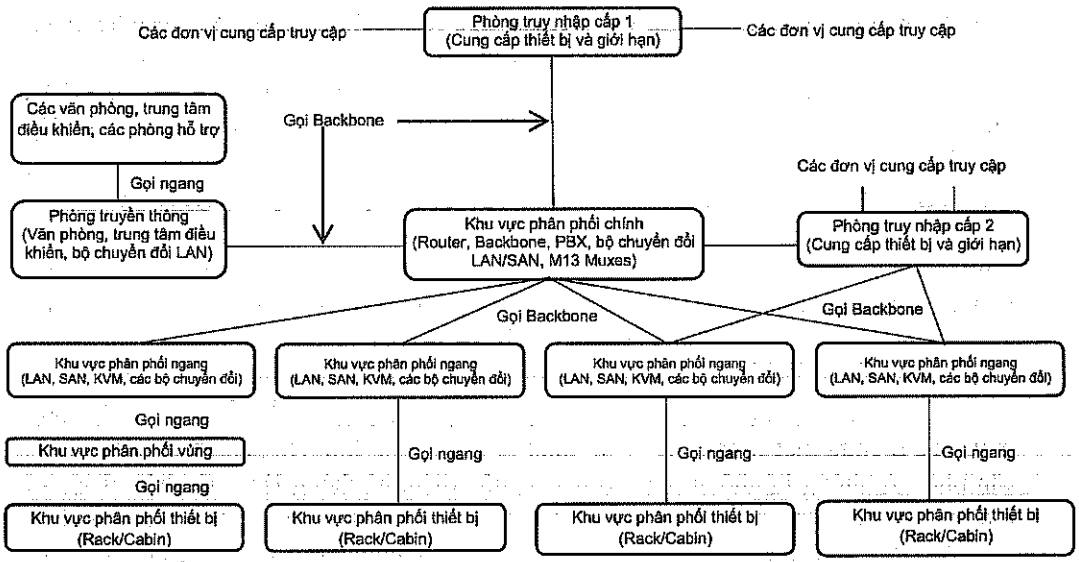
TTDL là một hệ thống máy tính cực kỳ quan trọng và rất dễ bị tổn hại, trong một TTDL chứa một lượng máy chủ, thiết bị lưu trữ rất lớn. Để hoạt động tốt, TTDL cần phải có những hệ thống phụ trợ như nguồn điện, hệ thống làm mát, báo cháy, an ninh bảo mật,..., cho dù kích cỡ như thế nào thì các TTDL vẫn có chung những chức năng là xử lý và lưu trữ dữ liệu. TTDL có thể là một phòng của một tầng lầu, hay một tầng của một toà nhà, hoặc được xây một toà nhà riêng.

Trung tâm dữ liệu đã trải qua nhiều bước phát triển về công nghệ và cấu trúc, cho đến nay tiếp tục phát triển dựa trên điện toán đám mây là xu hướng mới nhất nhằm hiện đại hóa trung tâm dữ liệu, tăng cường hiệu năng tính toán, nâng cao hiệu quả sử dụng năng lượng của thiết bị, giảm chi phí đầu tư và vận hành hạ tầng cho khách hàng.

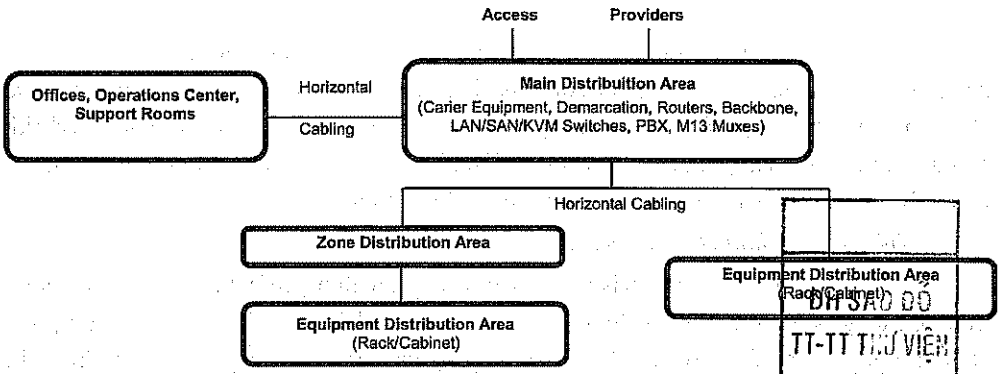
Các mô hình của Trung tâm dữ liệu



Hình 1.1. Mô hình Trung tâm dữ liệu cơ bản



Hình 1.2. Trung tâm dữ liệu có nhiều điểm kết nối đường vào



Hình 1.3. Mô hình trung tâm dữ liệu đơn giản

1.2. CÔNG NGHỆ ẢO HÓA

Khái niệm

Ảo hóa (Virtualization) là công nghệ tiên tiến nhất trong một loạt các cuộc cách mạng công nghệ nhằm tăng mức độ ảo hóa hệ thống, cho phép tăng hiệu suất làm việc của máy tính lên một cấp độ chưa từng có.

Ảo hóa hệ thống tức là tiến hành phân chia một máy chủ thành nhiều máy chủ ảo hoặc kết hợp nhiều máy chủ vật lý thành một máy chủ logic, đối với người sử dụng họ nhận biết và sử dụng các server ảo giống như một máy vật lý độc lập có đủ các tài nguyên cần thiết (bộ vi xử lý, bộ nhớ, kết nối mạng,...), trong khi các server ảo không hề có những tài nguyên độc lập như vậy, nó chỉ sử dụng tài nguyên được gán từ máy chủ vật lý. Ở đây, bản chất thứ nhất là các server ảo sử dụng tài nguyên của máy chủ vật lý, bản chất thứ hai là các server ảo có thể hoạt động như một server vật lý độc lập.

Lợi ích của ảo hóa

Thông thường việc đầu tư cho một trung tâm công nghệ thông tin rất tốn kém. Chi phí mua các máy chủ cấu hình mạnh và các phần mềm bản quyền là rất đắt. Doanh nghiệp luôn luôn muốn cắt giảm và hạn chế tối đa các chi phí không cần thiết trong khi vẫn đáp ứng được năng suất và tính ổn định của hệ thống. Vậy nên việc ứng dụng ảo hóa trở thành nhu cầu cần thiết của bất kỳ doanh nghiệp nào dù lớn hay nhỏ. Thay vì mua 10 máy chủ cho 10 ứng dụng thì chỉ cần mua 1 hoặc 2 máy chủ có hỗ trợ ảo hóa cũng vẫn có thể chạy tốt 10 ứng dụng này. Điều này cho thấy sự khác biệt giữa hệ thống ảo hóa và không ảo hóa. Bên cạnh đó, việc ứng dụng ảo hóa còn đem lại những lợi ích sau:

– Quản lý đơn giản;

– Triển khai nhanh;

– Phục hồi và lưu trữ hệ thống nhanh;

– Cân bằng tải và phân phối tài nguyên linh hoạt;

– Tiết kiệm chi phí;

– Ảo hóa góp phần tăng cường tính liên tục, hạn chế ngắt quãng.

Kiến trúc ảo hóa

Xét về kiến trúc hệ thống, các kiến trúc ảo hóa hệ thống máy chủ có thể ở các dạng chính là: Host–based, Hypervisor–based (còn gọi là bare mental hypervisor, được chia nhỏ làm hai loại là Monothic hypervisor và Microkernel hypervisor), Hybrid. Ngoài ra, tùy theo sản phẩm ảo hóa được triển khai (như VMWare, Microsoft HyperV, Citrix XEN Server) và mức độ ảo hóa cụ thể sẽ khác nhau.

Kiến trúc ảo hóa Hosted–based

Còn gọi là hosted hypervisor, kiến trúc này sử dụng một lớp hypervisor chạy trên nền tảng hệ điều hành, sử dụng các dịch vụ được hệ điều hành cung cấp để phân chia tài nguyên tới các máy ảo. Nếu ta xem hypervisor là một phần mềm riêng biệt, thì các hệ điều hành khách của máy ảo sẽ nằm trên lớp thứ ba so với phần cứng máy chủ.

Nhìn vào hình 1.4, ta có thể thấy mô hình này được chia làm bốn lớp hoạt động như sau:

– Nền tảng phần cứng;

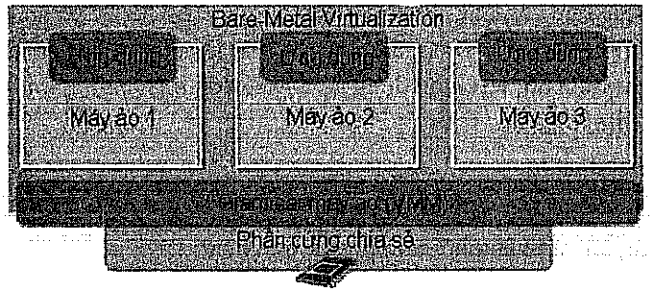
– Hệ điều hành Host;

– Hệ thống virtual machine monitor (hypervisor);

– Các ứng dụng máy ảo: sử dụng tài nguyên do hypervisor quản lý.

Hình 1.4. Mô hình ảo hóa Hosted–based

Kiến trúc ảo hóa Hypervisor–based



Hình 1.5. Kiến trúc Hypervisor–based

Trong mô hình này, ta thấy lớp phần mềm hypervisor chạy trực tiếp trên nền tảng phần cứng của máy chủ, không thông qua bất kỳ một hệ điều hành hay một nền tảng nào khác. Qua đó, các hypervisor này có khả năng điều khiển, kiểm soát phần cứng của máy chủ. Đồng thời nó cũng có khả năng quản lý các hệ điều hành chạy trên nó.

Một hệ thống ảo hóa máy chủ sử dụng nền tảng Bare – Mental hypervisor bao gồm ba lớp chính:

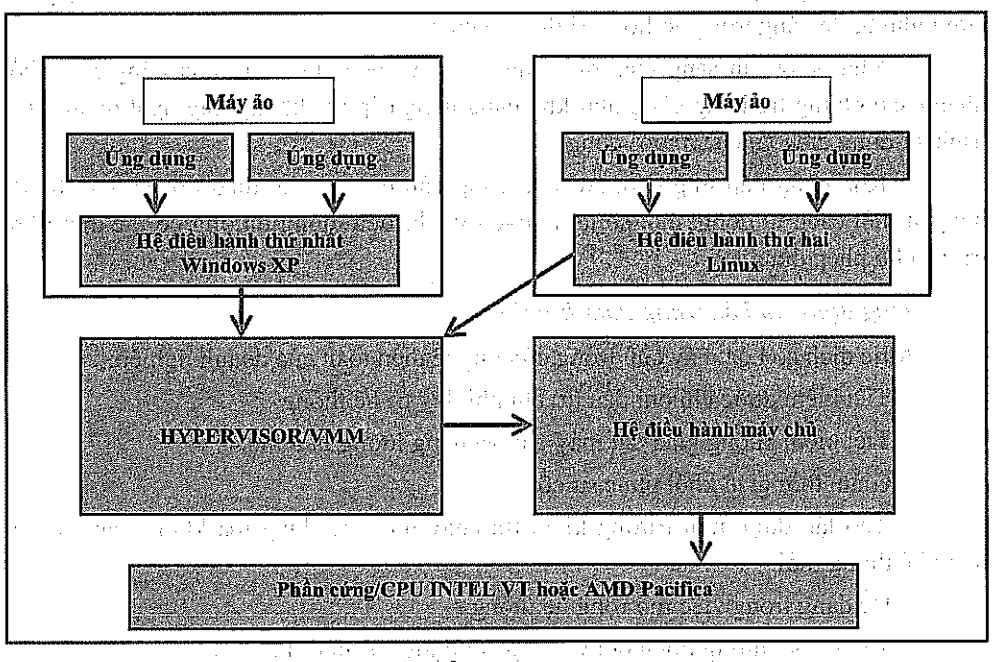
– Nền tảng phần cứng: bao gồm các thiết bị nhập xuất, thiết bị lưu trữ (Hdd, Ram), bộ vi xử lý CPU và các thiết bị khác (các thiết bị mạng, vi xử lý đồ họa, âm thanh…).

– Lớp nền tảng ảo hóa: Virtual Machine Monitor thực hiện việc liên lạc trực tiếp với nền tảng phần cứng phía dưới, quản lý và phân phối tài nguyên cho các hệ điều hành khác nằm trên nó.

– Các ứng dụng máy ảo: các máy ảo này sẽ lấy tài nguyên từ phần cứng, thông qua sự cấp phát và quản lý của hypervisor.

Kiến trúc lai Hybrid

Hybird là một kiểu ảo hóa mới hơn và có nhiều ưu điểm. Trong đó lớp ảo hóa hypervisor chạy song song với hệ điều hành máy chủ. Tuy nhiên, trong cấu trúc ảo hóa này, các máy chủ ảo vẫn phải đi qua hệ điều hành máy chủ để truy cập phần cứng nhưng khác biệt ở chỗ cả hệ điều hành máy chủ và các máy chủ ảo đều chạy trong chế độ hạt nhân.



Hình 1.6. Kiến trúc ảo hóa Hybrid

Ảo hóa trong điện toán đám mây

Trong điện toán đám mây, một trong những vấn đề nền tảng và cơ bản nhất là tính ảo hóa (virtualization) của hạ tầng bên dưới. Trên Linux, các gói phần mềm nguồn mở cung cấp các giải pháp xây dựng các tầng IaaS (đôi khi là cả PaaS) đều đã được đóng gói kèm theo một công nghệ ảo hóa riêng biệt. Ví dụ: Nimbus với Xen (và cả KVM), OpenStack với KVM/QEMU, VMWare với VMWare Hypervisor, OpenVZ Linux Container với công nghệ OpenVZ... Điện toán đám mây và ảo hóa giúp tối ưu hóa tài nguyên về mặt sử dụng năng lượng, sử dụng theo yêu cầu và kèm theo khả năng mở rộng linh hoạt.

Ảo hóa là một phần không thể thiếu trong mọi đám mây dựa trên khả năng trừu tượng hóa và bao đóng. Ảo hóa cung cấp mức độ trừu tượng cần thiết như việc các tài nguyên tính toán, lưu trữ, tài nguyên mạng được đồng nhất thành kho tài nguyên để cấp phát theo nhu cầu. Ảo hóa cung cấp tính bao đóng vì mọi thao tác cài đặt cập nhật trên nguồn tài nguyên ảo hóa chỉ diễn ra trong phạm vi máy ảo mà không ảnh hưởng hay tác động tới các máy ảo khác, tài nguyên khác không được cấp phát.

Công nghệ điện toán đám mây dựa mạnh mẽ vào công nghệ ảo hóa vì các nhân tố sau đây:

– Nhiều ứng dụng có thể chạy trên cùng một server, tài nguyên có thể được sử dụng hiệu quả hơn.

– Khả năng cấu hình cao: Nhiều ứng dụng yêu cầu tài nguyên khác nhau như số lượng core, dung lượng bộ nhớ. Việc cấu hình này khó thực hiện được ở mức độ phần cứng nhưng dễ dàng trong ảo hóa. Ví dụ VMWare.

– Khả năng sẵn sàng của ứng dụng cao: Ảo hóa cung cấp khả năng phục hồi nhanh sau những hư hỏng cũng như khả năng nâng cấp mà không gây ngắt quãng quá trình sử dụng dịch vụ của người dùng.

– Khả năng đáp ứng cao: Ảo hóa cung cấp các cơ chế theo dõi và bảo trì tài nguyên một cách tự động, một số tài nguyên về dữ liệu thông thường có thể được lưu trữ và cho phép dùng lại.

Ứng dụng ảo hóa trong doanh nghiệp

Mục đích ảo hóa máy chủ trong công nghệ điện toán của doanh nghiệp:

– Tiết kiệm được chi phí đầu tư, chi phí duy trì hệ thống.

– Tiết kiệm không gian đặt máy chủ và năng lượng tiêu thụ.

– Giảm thời gian khôi phục sự cố.

– Tạo lập được môi trường kiểm tra chạy thử ứng dụng mà không cần đầu tư thêm hệ thống mới.

– Dễ dàng trong việc mở rộng hệ thống.

– Tạo lập sự tương thích đối với việc sử dụng các chương trình cũ.

Xét ví dụ sau, một bài toán đưa ra cho doanh nghiệp khi họ cần thêm tài nguyên điện toán mới:

a. Lựa chọn 1

– Đầu tư và mở rộng cơ sở hạ tầng của tổ chức.

– Thường xuyên bổ sung thêm máy chủ, thiết bị lưu trữ và kết nối.

b. Lựa chọn 2

– Tập trung hóa và ảo hóa các tài nguyên hiện có.

– Nâng cao mức độ sử dụng tài nguyên vượt qua những hạn chế vật lý.

c. Lựa chọn 3

– Sử dụng cơ sở hạ tầng điện toán đám mây.

– Mở rộng ảo hóa vượt khỏi phạm vi trung tâm dữ liệu doanh nghiệp.

– Thuê các tài nguyên điện toán từ các dịch vụ đám mây.

– Trả tiền theo mức độ sử dụng.

Các bước áp dụng công nghệ ảo hóa

Doanh nghiệp có rất nhiều máy chủ, mỗi máy chủ được đặt ở nhiều nơi khác nhau, vì vậy việc truy xuất hay bảo trì dữ liệu là rất khó khăn. Do đó tất cả các dữ liệu đều được ảo hóa trong đám mây giúp doanh nghiệp giảm thiểu chi phí vận hành bảo trì bảo dưỡng.

Tiếp nhận yêu cầu: ghi nhận lại các thông tin chi tiết về yêu cầu hỗ trợ như: loại yêu cầu, thông tin khách hàng hoặc người yêu cầu, hình thức tiếp nhận (điện thoại, email, chat...).

Phân công người xử lý: Người tiếp nhận có thể trực tiếp xử lý hoặc chuyển cho các bộ phận chức năng xử lý yêu cầu hỗ trợ. Đối với các yêu cầu đơn giản, người xử lý có thể xử lý và nhập thông tin phản hồi trực tiếp cho yêu cầu. Đối với các yêu cầu phức tạp đòi hỏi nhiều người tham gia xử lý, có thể sử dụng phân hệ quản lý công việc để tiến hành phân công công việc và theo dõi kết quả thực hiện qua hệ thống báo cáo ngày.

Quản lý kho tri thức (knowlegde base): Quản lý các giải pháp xử lý các tình huống sẵn có để người tiếp nhận, xử lý có thể tìm kiếm và trả lời ngay cho các tình huống đã có trên hệ thống cũng như cập nhật giải pháp cho các tình huống đặc trưng vừa xử lý vào kho tri thức chung.

Ví dụ về dịch vụ ứng dụng trên nền tảng hạ tầng ảo hóa – ứng dụng CloudOffice

Quản lý công việc:

– Giao việc, lập kế hoạch thực hiện.

– Báo cáo công việc, theo dõi tiến độ và mức độ hoàn thành công việc.

– Danh sách nhân viên chưa báo cáo.

– Lịch làm việc.

Quản lý Hành chính: Quản lý công văn giấy tờ; Quản lý tài nguyên, tài sản; Quản lý văn phòng phẩm, công cụ dụng cụ; Quản lý chấm công, báo cáo ngày; Quản lý tài liệu dùng chung; Quản lý tin tức nội bộ; Quản lý ngày làm việc; Quản lý thời gian làm việc, nghỉ phép.

CloudHelpdesk – Hỗ trợ khách hàng: Hệ thống cung cấp các tính năng hỗ trợ khách hàng, tiếp nhận và xử lý các vấn đề liên quan đến dịch vụ chăm sóc khách hàng tại các tổ chức, doanh nghiệp. Kiểm soát chặt chẽ quy trình hỗ trợ khách hàng. Qua đó sẽ không còn hiện tượng bỏ quên, không xử lý kịp thời các yêu cầu hỗ trợ, nâng cao năng suất làm việc của nhân viên hỗ trợ khách hàng. Tổng hợp đánh giá được chất lượng sản phẩm, dịch vụ của doanh nghiệp.

CloudHRM – Quản lý nhân sự: Cung cấp các tính năng quản lý xuyên suốt các thông tin về cán bộ từ khi bắt đầu tuyển dụng cho đến khi kết thúc quá trình làm việc. Quy trình quản lý xuyên suốt qua đó đánh giá được đúng năng lực nhân viên, kịp thời ban hành các chính sách thúc đẩy nhân lực phát triển.

Các chức năng của CloudHRM: Quản lý đợt đánh giá, Đánh giá, Tổng hợp báo cáo, Quản lý tuyển dụng, Quản lý hồ sơ, Quản lý hợp đồng, Quản lý nhân viên, Quản lý nhóm nhân viên, Quản lý đào tạo.

CloudAccounting – Quản lý tài chính kế toán: Cung cấp các tính năng phục vụ các nghiệp vụ tài chính kế toán của tổ chức, doanh nghiệp, cập nhật các chế độ tài chính kế toán mới nhất, các quy trình nghiệp vụ kế toán tự động giúp nâng cao hiệu quả bộ phận tài chính kế toán của doanh nghiệp, quy trình quản lý tập trung giúp lãnh đạo kiểm soát được tình hình tài chính, các luồng tiền, công nợ của doanh nghiệp.

Các chức năng chính của CloudAccounting: Quản lý tạm ứng, Quản lý tiền mặt, tiền gửi ngân hàng, Quản lý bán hàng, Quản lý mua hàng, Quản lý lương, Quản lý kho, Quản lý thuế, Quản lý tài sản.

Kết luận

Về cơ bản, mô hình ảo hóa đám mây trong doanh nghiệp đã được đề ra có tính khả thi và đáp ứng được các yêu cầu như:

– Vận dụng lý thuyết về công nghệ ảo hóa: Raid, San, High Availability và những công nghệ liên quan có chức năng hỗ trợ để áp dụng cho doanh nghiệp của mình.

– Vận dụng được các thành phần, cấu trúc và chức năng từng phần của hệ thống ảo hóa. Triển khai mô hình ảo hóa máy chủ có các lợi ích khi ứng dụng mô hình ảo hóa vào trong thực tế như tiết kiệm chi phí, tăng hiệu suất, dễ quản lý,...

1.3. PHÂN LOẠI CÁC MÔ HÌNH ĐIỆN TOÁN ĐÁM MÂY

Điện toán đám mây có ba mô hình cung cấp dịch vụ, tùy theo các đối tượng khách hàng như sau:

Infrastructure as a Service – Dịch vụ hạ tầng: Mô hình dịch vụ này cung cấp cho khách hàng tài nguyên xử lý, lưu trữ, mạng và các tài nguyên máy tính cơ bản khác.

Từ đó, khách hàng có thể triển khai và chạy phần mềm tùy ý, bao gồm hệ điều hành và các ứng dụng. Khách hàng không quản lý hoặc kiểm soát các cơ sở hạ tầng điện toán đám mây nằm bên dưới, nhưng có kiểm soát hệ thống điều hành, lưu trữ và các ứng dụng được triển khai đồng thời kiểm soát có giới hạn của các thành phần mạng.

Platform as a Service – Dịch vụ nền tảng: Mô hình dịch vụ này cung cấp cho khách hàng khả năng triển khai trên hạ tầng điện toán đám mây các ứng dụng của họ bằng việc sử dụng các ngôn ngữ lập trình, các thư viện, dịch vụ, công cụ được hỗ trợ từ bên thứ ba. Người dùng không cần quản lý hoặc kiểm soát các cơ sở hạ tầng điện toán đám mây bên dưới như máy chủ ảo, mạng, hệ điều hành, lưu trữ, nhưng có thể cấu hình cho môi trường chạy ứng dụng của họ.

Software as a Service – Dịch vụ phần mềm: Mô hình dịch vụ này cung cấp cho phép khách hàng sử dụng các dịch vụ phần mềm của nhà cung cấp ứng dụng được triển khai trên hạ tầng điện toán đám mây. Các ứng dụng có thể truy cập từ các thiết bị khác nhau thông qua giao diện "mỏng" (thin client interface), chẳng hạn như một trình duyệt web (ví dụ như email trên web), hoặc qua giao diện của chương trình. Khách hàng không quản lý hoặc kiểm soát cơ sở hạ tầng điện toán đám mây nằm bên dưới bao gồm mạng, máy chủ, hệ điều hành, lưu trữ,..., với ngoại lệ có thể thiết lập cấu hình ứng dụng hạn chế người sử dụng cụ thể.

1.4. KIẾN TRÚC ĐÁM MÂY HƯỚNG THỊ TRƯỜNG

Một trong những bài toán quan trọng của điện toán đám mây là định giá cho tài nguyên trên đám mây để cho thuê. Có một số cách định giá cơ bản như sau:

Định giá cố định: Nhà cung cấp sẽ xác định rõ đặc tả về khả năng tính toán cố định (dung lượng bộ nhớ được cấp phát, loại CPU và tốc độ...).

Định giá theo đơn vị sử dụng: được áp dụng phổ biến cho lượng dữ liệu truyền tải, dung lượng bộ nhớ được cấp phát và sử dụng,... cách này uyển chuyển hơn cách trên.

Định giá theo thuê bao: ứng dụng phần lớn trong mô hình dịch vụ phần mềm (SaaS) người dùng sẽ tiên đoán trước định mức sử dụng ứng dụng cloud (cách tính này thường khó đạt được độ chính xác cao).

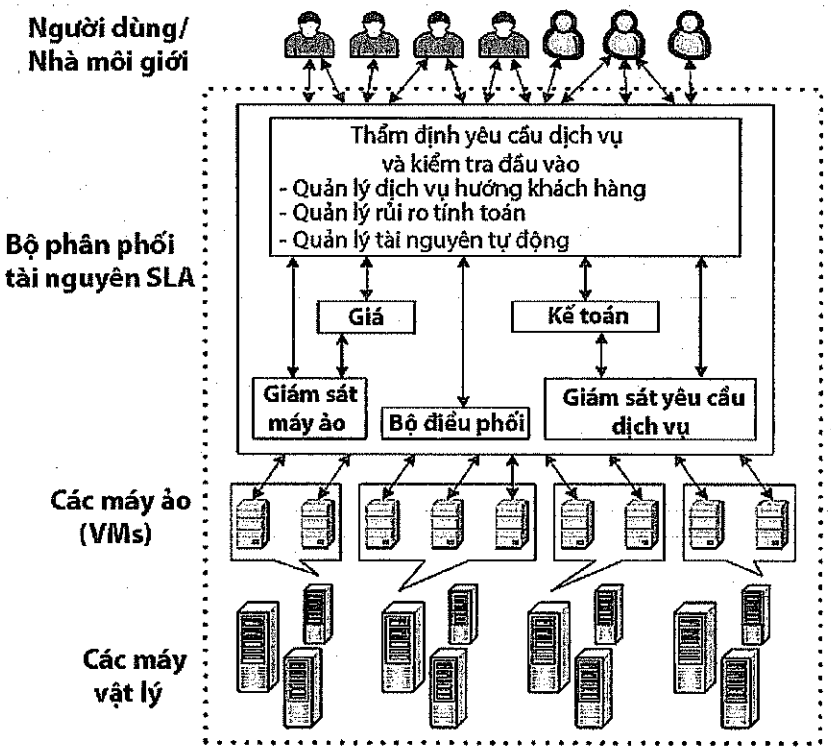
Với các cách định giá như trên, nhà cung cấp dịch vụ và người sử dụng cần có những thỏa thuận cụ thể về việc áp dụng cách định giá với tài nguyên. Điều này phải được nêu trong SLA (Service Level Agreement) trong đó xác định về yêu cầu chất lượng dịch vụ QoS (Quality of Service). Kiến trúc Market-oriented cloud bao gồm bốn thành phần chủ yếu:

User/Broker (Người dùng/Nhà môi giới): Người dùng hay nhà phân phối sử dụng quyền ủy thác để gửi yêu cầu dịch vụ từ bất kỳ đâu trên thế giới tới trung tâm dữ liệu hay Cloud để được xử lý.

SLA Resource Allocator (Bộ phân phối tài nguyên SLA): đóng vai trò như một trung gian giữa các nhà cung cấp Cloud với người dùng/nhà môi giới bên ngoài.

VMs (các máy ảo virtual machine): Nhiều máy ảo có thể được mở và tắt tự động trên một máy vật lý để phù hợp với yêu cầu dịch vụ từ phía người dùng/nhà môi giới bên ngoài cũng như phù hợp với việc sử dụng hiệu quả tài nguyên từ phía nhà cung cấp cloud. Cơ chế cung cấp máy ảo, như đã phân tích, là một trong những công nghệ chủ chốt cho phép tham số hóa cấu hình máy chủ ảo để phù hợp với điều luật sử dụng được ký kết.

Physical Machines (các máy vật lý): Các máy vật lý chính là tài nguyên hạ tầng của nhà cung cấp cloud. Các máy tính vật lý này chạy firmware hypervisor để cấp phát và chạy các máy ảo theo yêu cầu.



Hình 1.7. Kiến trúc Market-Oriented Cloud

Đi vào chi tiết, bộ phân phối tài nguyên SLA gồm các thành phần sau đây:

Service Request Examiner and Admission Control: Khi một yêu cầu dịch vụ được gửi lên lần đầu sẽ được phiên dịch thành các yêu cầu về chất lượng dịch vụ QoS trước khi xác định xem yêu cầu đó được chấp nhận hay từ chối. Điều này đảm bảo rằng không có tình trạng quá tải dịch vụ khi các yêu cầu dịch vụ không thể được đáp ứng đầy đủ vì giới hạn của tài nguyên hệ thống sẵn có. Dịch vụ này cần thông tin trạng thái cuối cùng về tình trạng sẵn sàng của tài nguyên (từ cơ chế VM Monitor) và khả năng xử lý tải (từ cơ chế Service Request Monitor) theo thứ tự để quyết định việc phân phối

tài nguyên một cách hiệu quả. Sau đó dịch vụ này sẽ phân yên cầu cho các máy ảo VM và xác định đặc tả tài nguyên cho máy ảo được cấp phát.

Pricing: Cung cấp cơ chế quyết định cách các yêu cầu dịch vụ được tính phí sử dụng. Ví dụ như dịch vụ được tính phí sử dụng dựa theo thời gian thực thi các nhiệm vụ, tỷ lệ giá cả (cố định/thay đổi) hay tính sẵn sàng của tài nguyên (sẵn có/yêu cầu). Cơ chế định giá thích hợp có mục đích là nhằm cân bằng chi phí cho người sử dụng và nhà cung cấp dịch vụ cloud.

Accounting: Cung cấp cơ chế theo dõi lưu lượng tài nguyên được sử dụng để tính chi phí cho người dùng.

VM Monitor: Cung cấp cơ chế lưu vết, giám sát những máy ảo đang sử dụng và các thông tin về tài nguyên của chúng.

Dispatcher: Cung cấp cơ chế bắt đầu thực thi việc cấp phát máy ảo cho những yêu cầu dịch vụ đã được chấp nhận.

Service Request Monitor: Cung cấp cơ chế lưu vết tiến trình yêu cầu dịch vụ.

1.5. CÁC CÔNG CỤ MÔ PHỎNG ĐÁM MÂY

Hiện nay, bên cạnh các hệ thống đám mây thương mại, các phần mềm cài đặt đám mây mã nguồn mở còn có một số công cụ có chức năng mô phỏng môi trường đám mây. Các công cụ này có ưu điểm là giúp người sử dụng, các nhà nghiên cứu công nghệ có thể thử nghiệm các sản phẩm công nghệ của mình trên "mây" mà không cần phải tự mình quản lý một đám mây thật. Tiêu biểu nhất trong các công cụ mô phỏng đám mây đó là CloudSim.

Kiến trúc CloudSim

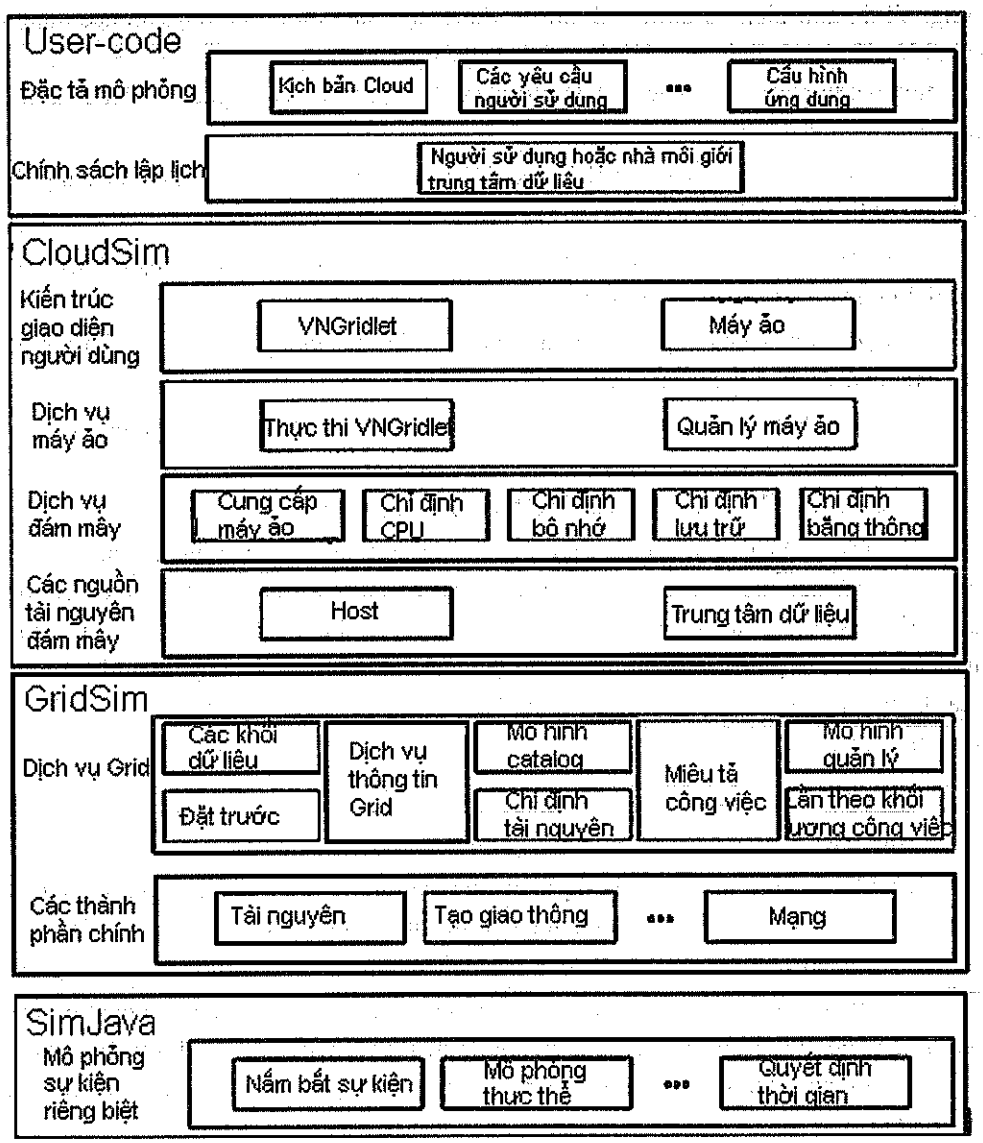
Một cách tổng thể, CloudSim bao gồm bốn lớp (xem hình 1.8):

SimJava: Mức thấp nhất trong kiến trúc bao gồm những công cụ mô phỏng sự kiện dùng để hiện thực những chức năng cốt lõi cần thiết cho việc mô phỏng ở lớp cao hơn như sắp xếp và xử lý sự kiện, khởi tạo các thành phần, quản lý mô phỏng đồng hồ.

GridSim: Bộ công cụ hỗ trợ các thành phần phần mềm cấp cao hơn để mô hình hóa nhiều nền tảng lưới, bao gồm cả hệ thống mạng và liên kết đồng bộ những thành phần cơ bản của lưới như tài nguyên, tập dữ liệu, dịch vụ giám sát và lưu vết, dịch vụ thông tin.

CloudSim: là phần hiện thực ở mức tiếp theo do việc mở rộng tự động các tính năng cơ bản được cung cấp bởi lớp GridSim. CloudSim cung cấp hỗ trợ cho việc mô hình và mô phỏng hóa môi trường nền tảng Cloud. Lớp CloudSim quản lý việc khởi tạo và thực thi các thực thể cốt lõi (máy ảo, thiết bị lưu trữ, ứng dụng) trong suốt quá trình mô phỏng. Lớp này có khả năng khởi tạo đồng thời và quản lý mở rộng trong suốt với những nền tảng Cloud bao gồm hàng nghìn thành phần hệ thống. Những vấn đề

cơ bản như triển khai máy ảo VM dựa trên yêu cầu người dùng, quản lý quá trình thực thi ứng dụng và theo dõi tự động đều được quản lý bởi lớp này.



Hình 1.8. Kiến trúc lớp của CloudSim

User-code: đây là lớp trên cùng của hệ thống mô phỏng cho phép cấu hình những chức năng liên quan đến các máy chủ (số lượng, đặc tả máy chủ ảo), liên quan đến ứng dụng (số lượng các tác vụ và yêu cầu đặc tả), các máy ảo VM, số lượng người dùng. Một người phát triển ứng dụng mô phỏng Cloud có thể tùy chọn và tham số cấu hình ứng dụng, ngữ cảnh thực nghiệm ở lớp này.

Mô hình mô phỏng Cloud

Kiến trúc dịch vụ nền tảng liên quan đến Cloud được mô hình hóa trong chương trình mô phỏng bởi thành phần Data center. Data center được tạo bởi các tập hợp các Host, có trách nhiệm quản lý các máy ảo VM trong chu kỳ sống của chúng. Các Host là các nút trong Cloud: nó được tham số khả năng xử lý của bộ vi xử lý trung tâm CPU (biểu diễn qua đơn vị MIPS = milion of instruction per second), bộ nhớ, khả năng lưu trữ và chính sách định thời để xử lý việc cấp phát lõi tính toán cho các máy ảo. Các thành phần máy Host của nền tảng mô phỏng hỗ trợ mô phỏng vi xử lý một nhân và đa nhân.

Việc phân phối máy ảo phục vụ cho ứng dụng cụ thể nào đó đến các thành phần Host là trách nhiệm của thành phần Virtual Machine Provisioner. Thành phần này cung cấp một tập các phương thức cho người sử dụng, với nhưng chính sách điều phối tài nguyên hướng tới mục tiêu tối ưu hiệu quả sử dụng. Những chính sách mặc định hiện có sẵn rất giản đơn theo hướng ai đến trước sẽ được phục vụ trước.

Với mỗi thành phần Host, sự cấp phát các vi xử lý CPU tới các máy ảo được thực hiện theo chính sách điều phối cụ thể dựa theo số lượng yêu cầu và số lượng vi xử lý sẵn có. Do vậy, có thể có các chính sách như cấp phát CPU dành riêng cho máy ảo hay phân tán động giữa các máy ảo (chia sẻ theo thời gian).

Mô hình cấp phát máy ảo VM

Một trong những ý tưởng khiến Cloud computing khác biệt với Grid computing là việc triển khai tối đa công nghệ và các công cụ ảo hoá.

Để cho phép giả lập những chính sách khác nhau, CloudSim hỗ trợ việc cấp phát máy ảo VM ở hai mức: trước tiên tại mức Host và sau đó là mức máy ảo VM. Ở mức đầu tiên, có thể xác định rõ tổng năng lực xử lý của mỗi nhân trong Host sẽ được gán cho mỗi máy ảo. Tại mức tiếp theo, các máy ảo VM sẽ được phân rõ tổng năng lực xử lý cụ thể cho mỗi tác vụ được thực thi. Tại mỗi mức, CloudSim hiện thực chính sách cấp phát tài nguyên theo thời gian và không gian.

Mô hình chợ Cloud

Mô hình chợ Cloud đóng vai trò như người môi giới giữa nhà cung cấp dịch vụ Cloud và khách hàng là điểm nhấn của Cloud computing. Hơn thế nữa, những dịch vụ này cần cơ chế để xác định chi phí dịch vụ và các chính sách về giá.

Mô hinh chính sách, chi phí và giá cả là một ý tưởng được xem xét khi thiết kết chương trình mô phỏng Cloud, bốn thuộc tính được xem xét đến là:

– Chi phí mỗi bộ xử lý;

– Chi phí mỗi đơn vị bộ nhớ;

– Chi phí mỗi đơn vị lưu trữ;

– Chi phí mỗi đơn vị băng thông sử dụng.

Chi phí mỗi đơn vị bộ nhớ và lưu trữ được kèm theo trong quá trình khởi tạo máy ảo. Chi phí mỗi đơn vị băng thông sử dụng có trong quá trình truyền dữ liệu. Bên cạnh đó, các chi phí sử dụng bộ nhớ, lưu trữ và các chi phí liên quan có mối liên hệ với việc sử dụng tài nguyên tính toán. Do vậy, nếu máy ảo VM được tạo mà không có tác vụ nào thực thi trên chúng, thì chỉ có chi phí về bộ nhớ và lưu trữ. Những vấn đề này có thể được thay đổi bởi người dùng.

1.6. CÂU HỎI VÀ BÀI TẬP

1. Nêu các đặc trưng của trung tâm dữ liệu.
2. So sánh các mô hình trung tâm dữ liệu. Đánh giá ưu, nhược điểm của từng mô hình khi áp dụng cho các doanh nghiệp.
3. Trình bày đặc thù của công nghệ ảo hóa và vai trò trong điện toán đám mây.
4. So sánh các kiến trúc ảo hóa. Đánh giá ưu/nhược điểm của từng kiến trúc.
5. Các phân loại mô hình điện toán đám mây có những đặc điểm gì giống và khác nhau.
6. Phân biệt vai trò của các thành phần trong kiến trúc đám mây hướng thị trường.
7. Nêu các đặc điểm của bộ phân phối tài nguyên SLA trong kiến trúc đám mây thị trường. Tìm hiểu và trình bày một số kiến trúc SLA cụ thể.
8. Tìm hiểu và trình bày chi tiết về công cụ mô phỏng đám mây: CloudSim.

Chương 2
LƯU TRỮ VÀ XỬ LÝ DỮ LIỆU

2.1. HỆ THỐNG LƯU TRỮ PHÂN TÁN VÀ ĐỒNG NHẤT BỘ NHỚ NFS, AFS

Trong phần này, chúng ta sẽ đi vào tìm hiểu kiến trúc các hệ thống lưu trữ phân tán cơ bản như hệ thống quản lý tập tin phân tán NFS và AFS. Đặc tính chung của các hệ lưu trữ phân tán là nhằm mục đích lưu trữ tập trung và chia sẻ thông tin cho các máy tính trong cùng mạng nội bộ.

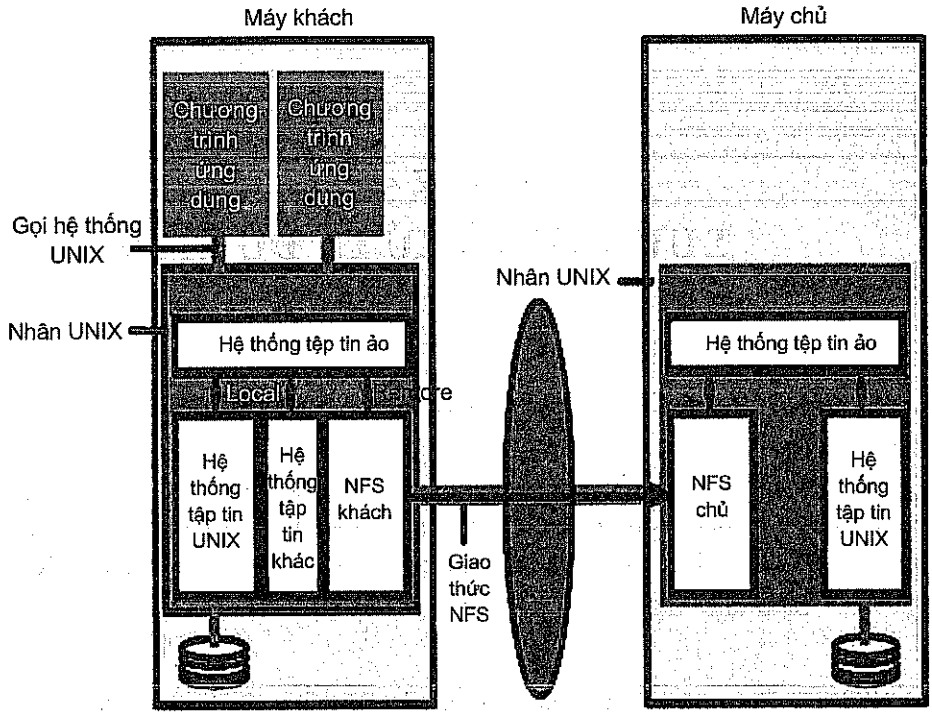
NFS

NFS hay Network File System là kiến trúc hệ thống tập tin phân tán mà một máy chủ trong hệ thống đóng vai trò là máy chủ lưu trữ, cung cấp năng lực lưu trữ của các ổ đĩa cứng cục bộ, hệ thống RAID cho các máy tính khác qua giao thức mạng. NFS là kiến trúc hệ quản lý tập tin phân tán rất phổ biến, được hỗ trợ bởi hầu hết các nền tảng hệ điều hành như Windows, Unix.

Ưu điểm của NFS là tính trong suốt cho người dùng cuối về cách thức truy cập tập tin hay vị trí nơi tập tin được lưu trữ. Hệ thống tập tin NFS được ánh xạ như một thư mục trong hệ thống quản lý tập tin cục bộ và không có sự khác biệt. Yếu điểm của NFS là tính khả mở thấp do mọi thao tác đọc ghi dữ liệu đều thực hiện qua kết nối mạng với máy chủ lưu trữ NFS. Trong trường hợp nếu có truy cập tương tranh vào cùng một tệp, hiệu năng của NFS suy giảm rõ rệt.

AFS

AFS cũng là một hệ thống tập tin phân tán nhằm mục đích chia sẻ tập tin cho một lượng lớn người dùng mạng. So với NFS, AFS có tính khả mở cao hơn, đáp ứng được số lượng người dùng lớn hơn nhờ vào đặc trưng sau đây: Khi truy cập tập tin, toàn bộ tập tin sẽ được sao chép về phía máy người sử dụng và các thao tác đọc ghi được thực hiện trên tập tin đó. Khi tập tin được đóng, nội dung tập tin sẽ được cập nhật về phía máy chủ lưu trữ. Chính vì vậy, quá trình đọc ghi tương tranh là trong suốt đối với từng người sử dụng nhưng tính nhất quán của tập tin không được đảm bảo.



Hình 2.1. Kiến trúc hệ thống tập tin NFS

2.2. HỆ THỐNG LƯU TRỮ HDFS, GFS

HDFS

Hadoop framwork của Apache là một nền tảng dùng để phân tích các tập dữ liệu rất lớn mà không thể xử lý trên được trên một máy chủ duy nhất. Hadoop trừu tượng hóa mô hình tính toán MapReduce, làm nó trở nên dễ tiếp cận hơn với các nhà phát triển. Hadoop có khả năng mở rộng vô số các nút lưu trữ và có thể xử lý tất cả hoạt động và phân phối liên quan đến việc phân loại dữ liệu.

Tổng quan thiết kế của HDFS

HDFS (Hadoop distributed file system) ra đời trên nhu cầu lưu trữ dữ liệu của Nutch, một dự án Search Engine nguồn mở. HDFS kế thừa các đặc tính chung của các hệ thống tập tin phân tán thế hệ trước như độ tin cậy, khả năng mở rộng và hiệu suất hoạt động. HDFS được thiết kế với những giả định như dưới đây:

Thứ nhất, các lỗi về phần cứng sẽ thường xuyên xảy ra. Hệ thống HDFS sẽ chạy trên các cluster với hàng trăm hoặc thậm chí hàng nghìn nút. Các nút này được xây dựng từ các phần cứng thông thường, giá rẻ, tỷ lệ lỗi cao. Chất lượng và số lượng của các thành phần phần cứng như vậy sẽ tất yếu dẫn đến tỷ lệ xảy ra lỗi trên hệ thống cluster cao. Có thể điểm qua một số lỗi như lỗi của ứng dụng, lỗi của hệ điều hành,

lỗi đĩa cứng, bộ nhớ, lỗi của các thiết bị kết nối, lỗi mạng, lỗi về nguồn điện... Vì thế, khả năng phát hiện lỗi, chống chịu lỗi và tự động phục hồi phải được tích hợp vào trong hệ thống HDFS.

Thứ hai, do đặc thù lưu trữ dữ liệu có dung lượng lớn, HDFS được thiết kế để tối ưu cho bài toán lưu trữ các tập tin có kích thước lớn hàng GB, thậm chí TB. Để giải quyết bài toán này, dữ liệu của các tập tin lớn sẽ được chia nhỏ thành các khối lớn (ví dụ 64MB) và phân tán trên các nút lưu trữ. So với các hệ thống tập tin khác, HDFS không tối ưu cho bài toán lưu trữ hàng tỉ tập tin nhỏ với kích thước mỗi tập tin chỉ vài KB. Ưu điểm của thiết kế tập tin lớn là giảm tải cho hệ thống quản lý không gian tập tin, giảm thời gian thao tác trên các thư mục hay tìm kiếm tập tin.

Thứ ba, HDFS ban đầu được thiết kế chỉ cho phép thay đổi nội dung các tập tin được lưu trữ qua phép toán thêm "append" dữ liệu vào cuối tập tin hơn là ghi đè lên dữ liệu hiện có. Việc ghi dữ liệu lên một vị trí ngẫu nhiên trong tập tin không được hỗ trợ. Một khi đã được tạo ra, các tập tin sẽ trở thành file chỉ đọc (read-only). Thiết kế này khác căn bản so với các hệ thống quản lý tập tin truyền thống do khác biệt về mục đích sử dụng. HDFS được thiết kế để tối ưu cho bài toán lưu trữ dữ liệu cho việc phân tích khi mà đầu vào có thể là các tập tin nhật ký logs hay dữ liệu liên tục đến từ các cảm biến. Với đầu vào dữ liệu này thì thao tác ghi ngẫu nhiên hay ghi đè dữ liệu là không cần thiết. Hơn nữa, đơn giản hóa hỗ trợ ghi dữ liệu cũng là nhân tố để HDFS tối ưu và tăng hiệu năng hệ thống.

Ngày nay, Hadoop cluster và HDFS rất phổ biến trên thế giới. Nổi bật nhất là hệ thống của Yahoo với một cluster lên đến 1100 nút với dung lượng HDFS là 12 PB. Các công ty khác như Facebook, Adode, Amazon cũng đã xây dựng các cluster chạy HDFS với dung lượng hàng trăm, hàng nghìn TB.

Kiến trúc HDFS

Giống như các hệ thống tập tin khác, HDFS duy trì một cấu trúc cây phân cấp các tập tin, thư mục mà các tập tin sẽ đóng vai trò là các nút lá. Trong HDFS, vì kích thước mỗi tập tin lớn, mỗi tập tin sẽ được chia ra thành các khối (block) và mỗi khối này sẽ có một block ID để nhận diện. Các khối của cùng một file (trừ khối cuối cùng) sẽ có cùng kích thước và kích thước này được gọi là block size của tập tin đó. Mỗi khối của tập tin sẽ được lưu trữ thành nhiều bản sao (replica) khác nhau vì mục đích an toàn dữ liệu. Các khối được lưu trữ phân tán trên các máy chủ lưu trữ cài HDFS. HDFS có một kiến trúc chủ/khách (master/slave). Trên một cluster chạy HDFS, có hai loại nút (node) là Namenode và Datanode. Một cluster có duy nhất một Namenode và có một hoặc nhiều Datanode.

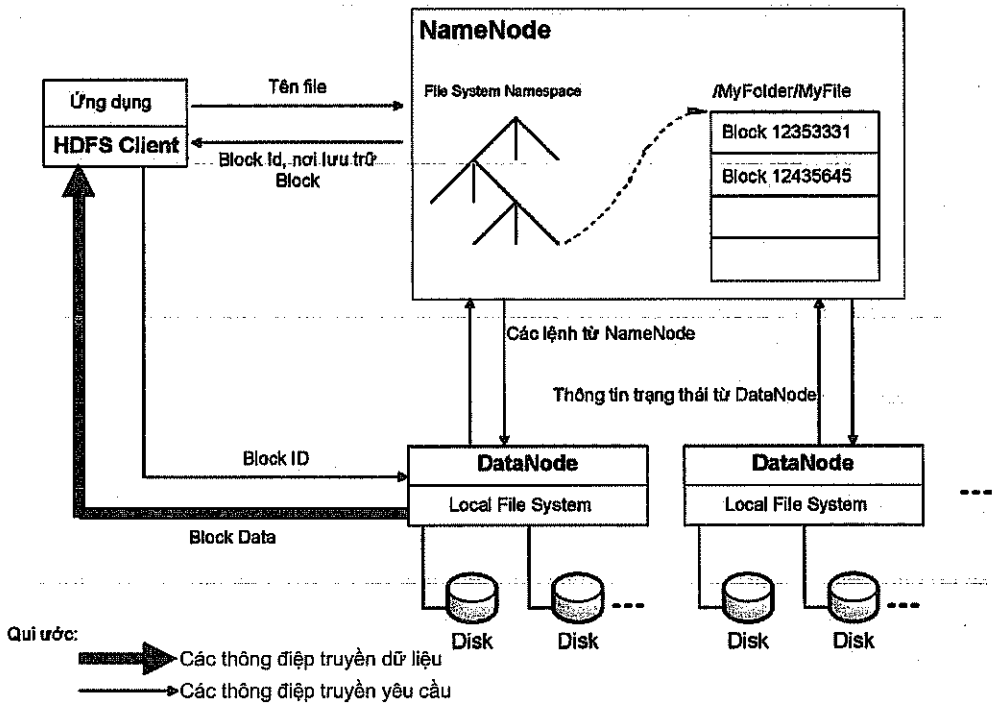
Namenode đóng vai trò là master, chịu trách nhiệm duy trì thông tin về cấu trúc cây phân cấp các tập tin, thư mục của hệ thống tập tin và các siêu dữ liệu (metadata) khác của hệ thống tập tin. Cụ thể, các metadata mà Namenode lưu trữ gồm có:

– *File system namespace (không gian tên tập tin):* là hình ảnh cây thư mục của hệ thống tập tin tại một thời điểm nào đó. Không gian tên tập tin thể hiện tất cả các file, thư mục có trên hệ thống file và quan hệ giữa chúng.

– *Thông tin để ánh xạ từ tên tập tin ra thành danh sách các khối:* Với mỗi tập tin, ta có một danh sách có thứ tự các khối block của tập tin đó, mỗi khối đại diện bởi Block ID.

– *Nơi lưu trữ các khối:* Các khối được đại diện một Block ID. Với mỗi block, ta có một danh sách các DataNode lưu trữ các bản sao của khối đó.

Các DataNode sẽ chịu trách nhiệm lưu trữ các khối thật sự của từng tập tin của HDFS. Mỗi một khối sẽ được lưu trữ như một tập tin riêng biệt trên hệ thống tập tin cục bộ của DataNode. Trong ngữ cảnh MapReduce, các DataNode này còn có chức năng tính toán với dữ liệu là chính các khối được lưu trữ. Kiến trúc của HDFS được thể hiện trong hình 2.2.



Hình 2.2. Kiến trúc HDFS

Về cơ bản, Namenode sẽ chịu trách nhiệm điều phối các thao tác truy cập (đọc/ghi dữ liệu) của người sử dụng (client) lên hệ thống HDFS. Khi client của hệ thống muốn đọc một tập tin trên hệ thống HDFS, client này sẽ thực hiện một yêu cầu thông qua RPC đến Namenode để lấy các metadata của tập tin cần đọc. Từ metadata này, client sẽ biết được danh sách các block của tệp tin và vị trí của các DataNode chứa

các bản sao của từng block. Client sẽ truy cập vào các DataNode để thực hiện các yêu cầu đọc các block.

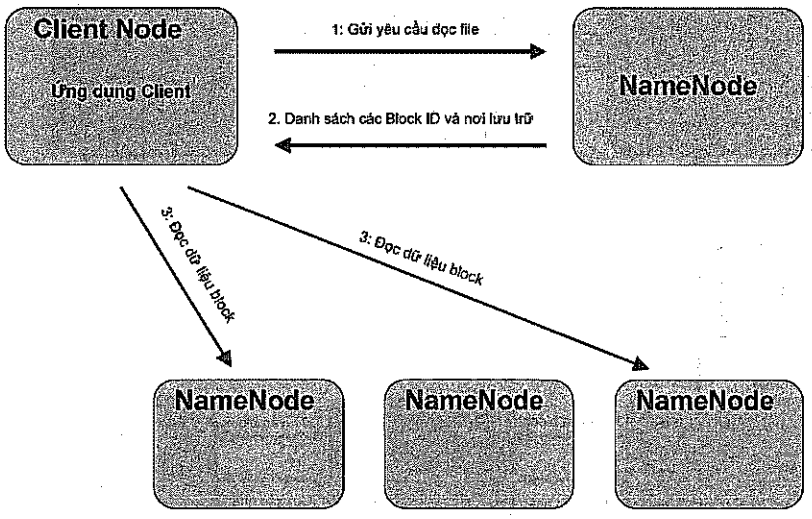
Định kỳ, mỗi DataNode sẽ báo cáo cho NameNode biết về danh sách tất cả các block mà nó đang lưu trữ, NameNode sẽ dựa vào những thông tin này để cập nhật lại các metadata trong nó. Cứ sau mỗi lần cập nhật lại như vậy, metadata trên NameNode sẽ đạt được tính nhất quán với dữ liệu trên các DataNode. Toàn bộ trạng thái của metadata khi đang ở tình trạng thống nhất này được gọi là một checkpoint. Chỉ khi nào metadata ở trạng thái checkpoint mới có thể được nhân bản cho mục đích phục hồi lại NameNode.

NameNode và quá trình tương tác giữa client và HDFS

Việc tồn tại duy nhất một NameNode trên một hệ thống HDFS đã làm đơn giản hóa thiết kế của hệ thống và cho phép NameNode ra những quyết định thông minh trong việc sắp xếp các block dữ liệu lên trên các DataNode dựa vào các kiến thức về môi trường hệ thống như: cấu trúc mạng, băng thông mạng, khả năng của các DataNode... Tuy nhiên, một nhu cầu đặt ra là cần phải tối thiểu hóa sự tham gia của NameNode vào các quá trình đọc/ghi dữ liệu lên hệ thống để tránh tình trạng nút thắt cổ chai (bottle neck). Client sẽ không bao giờ đọc hay ghi dữ liệu lên hệ thống thông qua NameNode. Thay vào đó, client sẽ hỏi NameNode về thông tin các DataNode có các block cần truy cập hoặc các DataNode có thể ghi các block mới. Sau đó, client sẽ lưu trữ lại tạm thời các thông tin này và kết nối trực tiếp với các DataNode để thực hiện các thao tác truy xuất dữ liệu.

Quá trình đọc file

Sơ đồ sau miêu tả quá trình client đọc một tập tin trên HDFS.



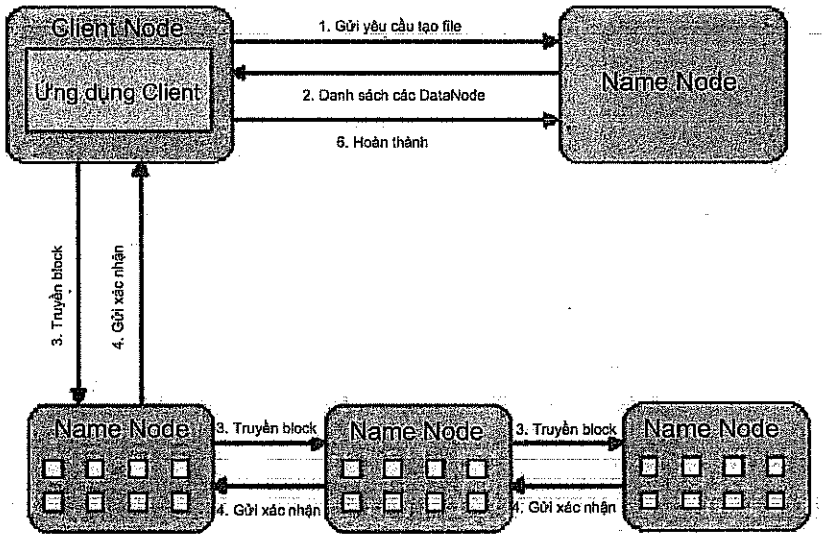
Hình 2.3. Quá trình đọc tập tin trên HDFS

Đầu tiên, client sẽ mở tập tin cần đọc bằng cách gửi yêu cầu đọc tập tin đến NameNode (1). NameNode sẽ thực hiện một số kiểm tra xem file được yêu cầu đọc có tồn tại không. Nếu không có vấn đề gì xảy ra, NameNode sẽ gửi danh sách các block (đại diện bởi Block ID) của tệp tin cùng với địa chỉ các DataNode chứa các bản sao của block này (2). Tiếp theo, client sẽ mở các kết nối tới DataNode, thực hiện một yêu cầu RPC để yêu cầu nhận block cần đọc và đóng kết nối với DataNode (3). Lưu ý là với mỗi block, ta có thể có nhiều DataNode lưu trữ các bản sao của block đó. Client sẽ chỉ đọc bản sao của block từ DataNode theo thứ tự ưu tiên được cấu hình trong hệ thống. Client sẽ thực hiện việc đọc các block lặp đi lặp lại cho đến khi block cuối cùng của file được đọc xong.

Như vậy, trong quá trình một client đọc một file trên HDFS, ta thấy client sẽ trực tiếp kết nối với các DataNode để lấy dữ liệu chứ không cần thực hiện gián tiếp qua NameNode. Điều này sẽ làm giảm đi rất nhiều việc trao đổi dữ liệu giữa client và NameNode, khối lượng luân chuyển dữ liệu sẽ được trải đều ra khắp cluster, tình trạng bottle neck "thắt cổ chai" sẽ không xảy ra. Do đó, cluster chạy HDFS có thể đáp ứng đồng thời nhiều client cùng thao tác tại một thời điểm.

Quá trình ghi file

Quá trình ghi tập tin bắt đầu với việc client sẽ gửi yêu cầu tạo một chỉ mục tập tin (file entry) lên không gian tên của hệ thống tập tin đến NameNode (1). Tập tin mới được tạo sẽ rỗng, tức chưa có một block nào. Sau đó, NameNode sẽ quyết định danh sách các DataNode sẽ chứa các block của tập tin và gửi lại cho client (2). Client sẽ chia dữ liệu của tập tin cần tạo ra thành các block, mỗi block sẽ được lưu ra thành nhiều bản sao trên các DataNode khác nhau (tùy vào chỉ số độ nhân bản của tập tin).



Hình 2.4. Quá trình tạo và ghi dữ liệu lên tập tin HDFS

Client gửi block cho DataNode thứ nhất, DataNode thứ nhất sau khi nhận được block sẽ tiến hành lưu lại bản sao thứ nhất của block. Tiếp theo DataNode thứ nhất sẽ gửi block này cho DataNode thứ hai để lưu ra bản sao thứ hai của block. Tương tự, DataNode thứ hai sẽ gửi packet cho DataNode thứ ba. Cứ như vậy, các DataNode cũng lưu các bản sao của một block. Quá trình này được hình dung như là một ống dẫn dữ liệu *data pile*. Sau khi DataNode cuối cùng nhận được thành công block, nó sẽ gửi lại cho DataNode thứ hai một gói xác nhận rằng đã lưu thành công (4). Và gói thứ hai lại gửi gói xác nhận tình trạng thành công của hai DataNode về DataNode thứ nhất.

Client sẽ nhận được các báo cáo xác nhận từ DataNode thứ nhất cho tình trạng thành công của tất cả DataNode trên *data pile*. Nếu có bất kỳ một DataNode nào bị lỗi trong quá trình ghi dữ liệu, client sẽ tiến hành xác nhận lại các DataNode đã lưu thành công bản sao của block và thực hiện một hành vi ghi lại block lên trên DataNode bị lỗi.

Sau khi tất cả các block của tập tin đều đã được ghi lên các DataNode, client sẽ thực hiện một thông điệp báo cho NameNode nhằm cập nhật lại danh sách các block của tập tin vừa tạo. Thông tin ánh xạ từ BlockID sang danh sách các DataNode lưu trữ sẽ được NameNode tự động cập nhật qua giao thức điểm danh mà định kỳ các DataNode sẽ gửi báo cáo cho NameNode danh sách các block mà nó quản lý.

Như vậy, cũng giống như trong quá trình đọc, client sẽ trực tiếp ghi dữ liệu lên các DataNode mà không cần phải thông qua NameNode. Một đặc điểm nổi trội nữa là khi client ghi một block với chỉ số nhân bản là n, tức nó cần ghi n block lên n DataNode, nhờ cơ chế luân chuyển block dữ liệu qua ống dẫn (pipe) nên lưu lượng dữ liệu cần write từ client sẽ giảm đi n lần, phân đều ra các DataNode trên cluster.

Kích thước khối block

Như ta đã biết, trên đĩa cứng, đơn vị lưu trữ dữ liệu nhỏ nhất không phải là byte, bit hay KB mà là một block. Kích thước block (block size) của đĩa cứng sẽ quy định lượng dữ liệu nhỏ nhất mà ta có thể đọc/ghi lên đĩa. Các hệ thống tập tin như của Windows hay Unix cũng sử dụng block như là đơn vị trao đổi dữ liệu nhỏ nhất, block size trên các file system này thường là khoảng nhiều lần block size trên đĩa cứng.

HDFS cũng chia file ra thành các block, và mỗi block này sẽ được lưu trữ trên Datanode thành một file riêng biệt trên hệ thống file local của nó. Đây cũng là đơn vị trao đổi dữ liệu nhỏ nhất giữa HDFS và client của nó. Block size là một trong những điểm quan trọng trong thiết kế HDFS. Block size mặc định của HDFS là 64 MB, nhưng thông thường trên các hệ thống lớn, người ta dùng block size là 128 MB, lớn hơn block size của các hệ thống file truyền thống rất nhiều.

Việc sử dụng block size lớn, tức sẽ giảm số lượng block của một tập tin, mang lại một số thuận lợi. Đầu tiên, nó sẽ làm giảm nhu cầu tương tác với NameNode của client vì việc đọc/ghi trên một block chỉ cần một lần tương tác với NameNode để lấy Block ID và nơi lưu block đó. Thứ hai, với block size lớn, client sẽ phải tương tác với DataNode ít hơn. Mỗi lần client cần đọc một BlockID trên DataNode, client phải tạo một kết nối TCP/IP đến DataNode. Việc giảm số lượng block cần đọc sẽ giảm số lượng

kết nối cần tạo, client sẽ thường làm việc với một kết nối bền vững hơn là tạo nhiều kết nối. Thứ ba, việc giảm số lượng block của một tập tin sẽ làm giảm khối lượng metadata trên NameNode. Điều này giúp MasterNode có thể đưa toàn bộ metadata vào bộ nhớ chính mà không cần phải lưu trữ trên đĩa cứng.

Mặt khác, việc sử dụng block size lớn sẽ dẫn đến việc một tập tin nhỏ chỉ có một vài block, thường là chỉ có một. Điều này dẫn đến việc các DataNode lưu block này sẽ trở thành điểm nóng khi có nhiều client cùng truy cập vào tập tin. Tuy nhiên, hệ thống HDFS đa phần chỉ làm việc trên các file có kích thước lớn với nhiều block như đã đề cập ở phần trên nên sự bất cập này là không đáng kể trong thực tiễn.

GFS

GFS hay Google file system là hệ thống tập tin phân tán phát triển bởi Google và ra đời trước HDFS. GFS có kiến trúc tương tự HDFS, là hình mẫu để cộng đồng phát triển nên HDFS. GFS thường được cấu hình với MasterNode và các shadow Master nhằm mục đích chịu lỗi. Trong quá trình hoạt động, nếu MasterNode gặp sự cố, một shadow Master sẽ được lựa chọn thay thế MasterNode. Quá trình này hoàn toàn trong suốt với client và người sử dụng. Ngoài ra, trong quá trình lưu trữ các block, GFS sử dụng các kỹ thuật kiểm tra lỗi lưu trữ như checksum nhằm phát hiện và khôi phục block bị lỗi một cách nhanh chóng. GFS là nền tảng phát triển các hệ thống khác của Google như BigTable hay Pregel.

2.3. CƠ SỞ DỮ LIỆU NOSQL

Các hệ quản trị dữ liệu quan hệ (RDBMS) từ lâu đã được xem như là giải pháp số một trong lưu trữ và truy vấn dữ liệu cấu trúc trong nhiều thập kỷ qua. RDBMS cung cấp mô hình dữ liệu quan hệ mà với mô hình này có thể đặc tả hầu hết mối quan hệ giữa các tập dữ liệu lưu trữ. Một trong những đặc tính cơ bản của RDBMS là bảo đảm ngữ nghĩa ACID cho phép xử lý các giao dịch dữ liệu một cách tin cậy. Điều này giải phóng ứng dụng khỏi khối lượng công việc khổng lồ đảm bảo tính toàn vẹn của dữ liệu trong truy cập tương tranh.

Khi lượng dữ liệu được lưu trữ ngày càng lớn và vượt ra khỏi giới hạn xử lý của một máy chủ RDBMS duy nhất, rất nhiều các kỹ thuật được đưa ra để mở rộng hiệu năng của hệ thống RDBMS. Một trong những kỹ thuật phổ biến là "database sharding" thực hiện bằng cách chia cơ sở dữ liệu tổng thể thành các phần "shards" và phân tán trên cụm RDBMS cluster. Tuy nhiên, do độ phức tạp cao của cơ chế bảo đảm ACID, các cụm RDBMS cluster thường chỉ được triển khai trên quy mô nhỏ vài chục nốt.

Từ năm 2005, cộng đồng nghiên cứu về cơ sở dữ liệu trên thế giới đồng ý rằng sự thống trị của RDBMS đã kết thúc và kêu gọi cần phải thiết kế các cơ sở dữ liệu chuyên biệt hóa với tính khả mở cao để phù hợp với nhu cầu thực tế. Lớp các hệ cơ sở dữ liệu mới này được gọi dưới tên chung là NoSQL. Hiện tại có các hệ cơ sở NoSQL điển hình như Amazon Dynamo, Cassandra, CouchDB,...

Đặc điểm chung của các hệ NoSQL là tính khả mở cao, so với RDBMS có những khác biệt cơ bản như dưới đây:

Mô hình dữ liệu đơn giản hoá: NoSQL không tổ chức dữ liệu dưới các bảng quan hệ. NoSQL có mô hình tổ chức dữ liệu dưới bốn nhóm chính: key/value, hướng văn bản (document-oriented), hệ cột (column-familly store) và cơ sở dữ liệu đồ thị (Graph database).

Cơ sở dữ liệu (DBMS) key/value cung cấp mô hình dữ liệu và giao diện ứng dụng API đơn giản nhất giống với bảng băm (hashtable). Ứng với mỗi khóa, DBMS key/value chỉ cho phép đọc, ghi và xóa giá trị được định danh bởi khóa đó. Ví dụ kiểu NoSQL key/value là: Amazon Dynamo, Riak.

DBMS hướng văn bản được thiết kế để quản trị dữ liệu nửa cấu trúc (semistructured data) tổ chức dưới dạng tập hợp các văn bản. Giống như DBMS key/value, mỗi văn bản trong DBMS được định danh bằng một khóa duy nhất. Tuy nhiên, vì văn bản có cấu trúc gồm nhiều thuộc tính, DBMS hướng văn bản cho phép tạo chỉ mục tìm kiếm cho các trường thuộc tính này. Ví dụ của DBMS hướng văn bản bao gồm: CouchDB và MongoDB.

DBMS hệ cột tổ chức cấu trúc dữ liệu dưới dạng các bảng ánh xạ đa chiều thưa như mô hình Google Bigtable. Về cơ bản, dữ liệu tồn tại dưới dạng bảng như trong RDBMS nhưng các dòng trong bảng không nhất thiết có cùng tập các cột. Hơn nữa, DBMS hệ cột này phần lớn không hỗ trợ phép toán JOIN như trong DBMS.

Độ phức tạp được đơn giản hóa: RDBMS với đặc tính ACID đảm bảo dữ liệu luôn được toàn vẹn và nhất quán trong giao dịch. Tuy nhiên, đặc tính này trong thực tiễn với các ứng dụng internet như hiện nay trở nên không cần thiết. NoSQL lựa chọn tính khả mở thay vì cam kết bảo đảm ACID. Để có thể mở rộng tới mô hình triển khai phân tán trên hàng ngàn máy chủ lưu trữ, NoSQL phần lớn chỉ hỗ trợ mô hình nhất quán sau cùng (eventual consistency model) như là các thao tác đọc có thể được trả về dữ liệu cũ chưa được cập nhật với thay đổi mới với điều kiện đảm bảo sau cùng thì các thao tác đọc luôn nhận về dữ liệu mới nhất đã cập nhật.

Mô hình mở rộng ngang trên phần cứng phổ thông: Không giống như RDBMS, các DBMS NoSQL có tính khả mở cao trên các phần cứng phổ thông. Các nốt lưu trữ của NoSQL có thể gia nhập hay ra khỏi hệ thống tùy theo nhu cầu mà không làm ảnh hưởng đến sự hoạt động của hệ thống.

2.4. ĐIỆN TOÁN ĐÁM MÂY VÀ DỮ LIỆU LỚN

Các kho lưu trữ dữ liệu phân tán là thành phần không thể thiếu trong điện toán đám mây. Ngoài tính năng lưu trữ dữ liệu tập trung cho người sử dụng điện toán đám mây, các kho lưu trữ dữ liệu này còn đảm nhận vai trò lưu trữ và cung cấp các tập tin ảnh máy ảo phục vụ cho chính nền tảng ảo hóa của điện toán đám mây. Trong chương này,

chúng ta sẽ đi vào tìm hiểu thiết kế các kho lưu trữ Openstack Swift, Amazon S3, thiết kế của các hệ quản trị dữ liệu mới phổ biến trên nền điện toán đám mây và phân tích cụ thể mô hình tính toán MapReduce/Hadoop.

Một đặc điểm chung của hệ quản trị dữ liệu cho điện toán đám mây là giao diện tương tác HTTP API, không sử dụng giao diện hệ thống quản lý tập tin thông thường.

Amazon S3

Amazon S3 là dịch vụ kho lưu trữ dữ liệu trên nền điện toán đám mây Amazon Web Service, được đưa ra giới thiệu vào năm 2006. S3 cung cấp giao diện tương tác ứng dụng API đơn giản cho phép lưu trữ và truy cập dữ liệu bất cứ khi nào và ở bất cứ đâu có kết nối Internet. Các nhà phát triển ứng dụng hay người sử dụng S3 không phải trả bất kỳ khoản phí cài đặt nào, chỉ trả phí dựa trên dung lượng lưu trữ và băng thông sử dụng.

Khi ra công bố, Amazon tính phí cho người sử dụng là 0,15 USD một gigabyte mỗi tháng, với chi phí thêm cho băng thông được sử dụng để gửi và nhận dữ liệu, tính phí cho mỗi yêu cầu (nhận hay gửi). Amazon tuyên bố ngay chính Amazon cũng sử dụng nền tảng S3 với tính khả mở cao để chạy mạng lưới thương mại điện tử toàn cầu của họ.

Amazon S3 được báo cáo đã lưu trữ hơn một nghìn tỷ thực thể tính đến tháng 6 năm 2012. Con số này tăng lên từ 102 tỷ thực thể trong tháng 3 năm 2010, 64 tỷ thực thể trong tháng 8 năm 2009, 52 tỷ tháng 3 năm 2009,29 tỷ trong tháng 10 năm 2008, 14 tỷ trong tháng 1 năm 2008 và 10 tỷ trong tháng 10 năm 2007. S3 được sử dụng cho web hosting, image hosting và lưu trữ cho các hệ thống backup. Hợp đồng dịch vụ cho S3 kèm theo một đảm bảo 99,9% thời gian hoạt động hằng tháng, tương đương với khoảng 43 phút thời gian chết mỗi tháng.

Các khái niệm cơ sở trong Amazon S3

Đối tượng dữ liệu (Objects): Các đối tượng dữ liệu được coi như khái niệm các tập tin trong hệ thống quản lý tập tin thông thường. Mỗi đối tượng được lưu trữ với siêu dữ liệu đặc tả đi kèm như ngày chỉnh sửa, ngày khởi tạo,... Số lượng các đối tượng mà người sử dụng có thể lưu trữ là vô hạn và mỗi đối tượng có thể chứa 5TB dữ liệu.

Thùng (buckets): Mỗi đối tượng được lưu trữ trong một thùng, được hiểu như là một thư mục trên hệ quản lý tập tin. Tuy nhiên, khác với hệ quản lý tập tin, các thùng chỉ chứa các đối tượng dữ liệu, không chứa các thùng con.

Khóa (keys): Mỗi đối tượng dữ liệu trong Amazon S3 được định danh bởi một khóa duy nhất ứng với thùng có chứa đối tượng đó. S3 hỗ trợ tính phiên bản, do vậy định danh của mỗi một phiên bản (version) của đối tượng dữ liệu được xây dựng từ tên thùng, khóa và mã phiên bản.

Vùng địa lý kho lưu trữ (Regions): Người sử dụng S3 khởi tạo thùng theo khu vực địa lý nơi triển khai hệ thống S3. Việc cho phép lựa chọn vùng lưu trữ là để tối ưu độ trễ đường truyền tăng tốc độ truy cập. S3 hiện nay được triển khai trên các vùng địa lý như Mỹ, châu Âu, khu vực châu Á,...

Thiết kế

Amazon không công bố thông tin chi tiết thiết kế của S3. Theo Amazon, thiết kế của S3 nhằm mục đích cung cấp khả năng mở rộng, tính sẵn sàng cao và độ trễ thấp với chi phí.

S3 lưu trữ các đối tượng hay thực thể dữ liệu kích thước lên đến 5 terabyte. Các đối tượng được tổ chức thành các thùng bucket (mỗi thùng thuộc sở hữu của một dịch vụ Web Amazon hoặc tài khoản AWS). Mỗi thực thể được định danh trong mỗi nhóm bằng một khóa duy nhất gán với người sử dụng. Các thùng và các đối tượng có thể được tạo ra, được liệt kê và lấy ra bằng cách sử dụng hoặc một giao diện HTTP kiểu REST hoặc giao diện SOAP. Ngoài ra, các đối tượng có thể được tải về bằng cách sử dụng giao diện giao thức BitTorrent.

S3 hỗ trợ các giao thức bảo mật, chính sách quyền truy cập đến các đối tượng và các thùng. Tên và khóa thùng được lựa chọn nên các đối tượng có thể được đánh địa chỉ thông qua URL:

http://s3.amazonaws.com/bucket/key

http://bucket.s3.amazonaws.com/key

Vì các đối tượng có thể truy cập qua giao thức HTTP, S3 có thể được sử dụng để thay thế đáng kể cơ sở hạ tầng lưu trữ web tĩnh hiện có. Cơ chế xác thực AWS Amazon cho phép chủ sở hữu nhóm tạo ra một URL xác thực với thời gian tồn tại được định sẵn. Ví dụ như, người sử dụng có thể xây dựng một URL mà có thể được giao cho một bên thứ ba để truy cập trong một thời gian như trong 30 phút tiếp theo, hoặc 24 giờ tiếp theo.

Mỗi mục trong một thùng cũng có thể được phục vụ như là một nguồn cấp dữ liệu BitTorrent. Các kho dữ liệu của S3 có thể hoạt động như một máy chủ lưu trữ nguồn cho một torrent và client BitTorrent bất kỳ có thể lấy lại tập tin qua giao thức BitTorrent. Điều này làm giảm đáng kể chi phí băng thông cho việc tải xuống của các thực thể phổ biến vì các client BitTorrent trong quá trình tải về đối tượng dữ liệu cũng đóng góp vào việc làm trung gian đưa dữ liệu tới các client khác.

Dịch vụ lưu trữ web tĩnh

Tính đến ngày 18 tháng 2 năm 2011, S3 Amazon cung cấp các tùy chọn để lưu trữ các trang web tĩnh với sự hỗ trợ tài liệu trang chủ chỉ mục (index.html) và hỗ trợ tài liệu báo lỗi. Sự hỗ trợ này đã được thêm vào như một kết quả từ yêu cầu của người sử dụng từ năm 2006. Ví dụ, trong trường hợp Amazon S3 đã được cấu hình với các bản ghi CNAME để lưu trữ http://subdomain.example.com/. Trong quá khứ, một người

truy cập vào URL này sẽ chỉ là một danh sách định dạng XML của các đối tượng thay vì một trang chủ index để phù hợp với khách truy cập ngẫu nhiên. Tuy nhiên, ngày nay, các trang web lưu trữ trên S3 có thể chỉ định một trang chủ mặc định để hiển thị và một trang khác để hiển thị trong trường hợp trang mặc định này không tồn tại.

Ưu điểm và tính năng của S3

Tính ổn định: Người sử dụng S3 được ký thỏa thuận cung cấp dịch vụ với mức duy trì tính sẵn sàng của hệ thống đạt 99,99%. S3 được thiết kế chịu lỗi và phục hồi hệ thống nhanh trong thời gian tối thiểu.

Tính đơn giản, dễ dùng: S3 cung cấp giao diện kết nối Rest API và các thư viện giao tiếp trên các ngôn ngữ phổ biến như JAVA, Python,...

Tính mở rộng: S3 chỉ tính phí dịch vụ trên dung lượng và băng thông sử dụng. Người sử dụng có toàn quyền tăng hoặc giảm số lượng các đối tượng dữ liệu được lưu trữ để tối ưu chi phí sử dụng.

Tính rẻ: Theo tính toán thống kê, chi phí sử dụng S3 rất cạnh tranh với các giải pháp tự thiết kế lưu trữ trên máy chủ riêng.

OpenStack Swift

OpenStack Swift là hệ thống kho lưu trữ đối tượng có tính khả mở cao, được thiết kế để lưu trữ khối lượng lớn các dữ liệu phi cấu trúc với chi phí thấp thông qua giao diện ứng dụng Restful. Hệ thống OpenStack Swift có thể triển khai mở rộng từ một vài nốt (node) lưu trữ với dung lượng lưu trữ giới hạn lên tới hàng ngàn nốt lưu trữ phân tán với dung lượng tổng thể lên tới hàng ngàn Petabytes. OpenStack Swift được thiết kế chịu lỗi, trong hệ thống không có bất cứ thành phần nào là điểm chết duy nhất (single point of failure) mà hỏng hóc của thành phần này kéo theo việc dừng hoạt động của toàn bộ hệ thống. Như các kho lưu trữ điện toán đám mây khác, OpenStack swift được thiết kế để có thể lưu trữ và phục vụ dữ liệu nội dung đồng thời nhiều người dùng dịch vụ.

Đặc trưng của OpenStack Swift

OpenStack Swift lưu trữ dữ liệu dưới dạng các đối tượng dữ liệu được truy xuất qua định danh URL.

Tất cả các đối tượng lưu trữ đều được nhân bản ra ít nhất ba vùng chịu lỗi được định nghĩa như là nhóm các ổ đĩa cứng, nhóm các nốt lưu trữ,... Mục đích của việc nhân bản ra các vùng chịu lỗi khác nhau là để giúp đối tượng lưu trữ vẫn có thể truy cập tới được khi có sự cố trên một hoặc hai vùng chịu lỗi.

Tất cả các đối tượng có thông tin siêu dữ liệu đi kèm như quyền người sử dụng, thời gian khởi tạo...

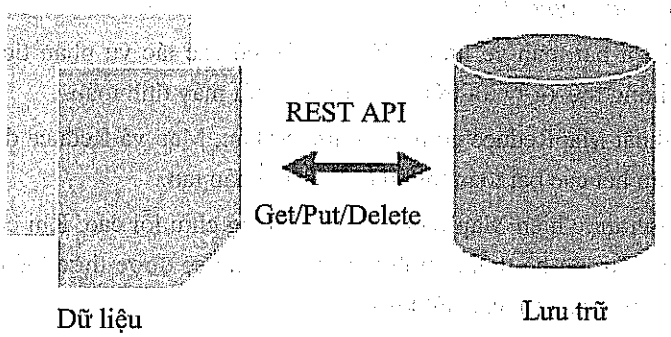
OpenStack Swift cung cấp giao tiếp RestFul API để truy xuất đối tượng dữ liệu.

Đối tượng dữ liệu được phân tán trên hệ thống mà không phụ thuộc vào định danh URL của đối tượng.

OpenStack Swift mở rộng hay thu hẹp hệ thống bằng việc thêm bớt các nốt lưu trữ nhưng không ảnh hưởng đến hiệu năng của hệ thống. Quá trình thêm bớt các nốt là hoàn toàn trong suốt và không ảnh hưởng đến hoạt động của toàn hệ thống.

Các nốt lưu trữ là phần cứng máy chủ phổ biến như Dell, HP,...

Các lập trình viên hoặc người sử dụng nền tảng OpenStack Swift có thể sử dụng trực tiếp giao tiếp API cung cấp bởi OpenStack Swift, hoặc sử dụng các thư viện giao tiếp trên các ngôn ngữ lập trình phổ biến như Java, Python, Ruby và C#.



Hình 2.5. Truy cập dữ liệu qua Rest API

Xử lý dữ liệu lớn MapReduce/Hadoop

Theo thống kê, lượng dữ liệu được tạo ra hiện nay tăng gấp đôi sau chu kỳ 2 năm. Đóng góp vào sự tăng trưởng khổng lồ này là các văn bản, tập tin video, audio được chia sẻ trên các mạng xã hội như twitter, facebook. Ngoài ra còn phải kể đến dữ liệu sinh ra trong nghiên cứu khoa học và các loại dữ liệu lấy từ thiết bị cảm biến lắp đặt khắp nơi trên thế giới. Trong ngữ cảnh này, từ khóa "big data" hay dữ liệu lớn trở thành từ khóa được nhắc đến nhiều nhất trong giới công nghệ. Dữ liệu lớn đặt ra nhiều thách thức cho việc thiết kế lại hệ thống lưu trữ và xử lý, cũng như mang lại nhiều lợi ích nếu được khai thác như một nguồn tài nguyên trong kỷ nguyên số.

Dữ liệu lớn được đặc tả bằng 4V: Volume, Velocity, Variety và Value. Volume nói tới dung lượng khổng lồ của dữ liệu lớn, velocity nói tới lớp dữ liệu lớn đòi hỏi phải xử lý nhanh và liên tục. Variety tham chiếu tới sự đa dạng của các loại dữ liệu cấu trúc và phi cấu trúc tồn tại hiện nay. Value là về giá trị quý báu có thể có được khi khai thác dữ liệu lớn.

Một vấn đề cần phải thấy, đó là điện toán đám mây là nền tảng cơ bản cho phép lưu trữ và khai thác dữ liệu lớn trở nên phổ biến. Như đã phân tích, với ứng dụng điện toán đám mây, các doanh nghiệp tổ chức có thể thuê máy chủ hoặc dịch vụ lưu trữ phân tích dữ liệu lớn với chi phí thấp mà không phải đầu tư hạ tầng và con người để

quản trị hệ thống. Trong phần này, chúng ta sẽ đi vào tìm hiểu xử lý dữ liệu lớn với Hadoop MapReduce.

MapReduce là một trong những công nghệ tạo khả năng của cuộc cách mạng dữ liệu lớn, một mô hình lập trình và công cụ được Google đưa ra giới thiệu vào năm 2004. Mapreduce có thể hiểu là một phương thức thực thi để giúp các ứng dụng có thể xử lý nhanh một lượng dữ liệu lớn trên môi trường phân tán. Các máy tính này sẽ hoạt động song song nhưng độc lập với nhau, mục đích là làm rút ngắn thời gian xử lý toàn bộ dữ liệu.

Ưu điểm của MapReduce

– Xử lý tốt bài toán về lượng dữ liệu lớn có các tác vụ phân tích và tính toán phức tạp mà không thể xử lý tốt trên môi trường một máy tính toán.

– Giải thuật MapReduce gồm hai bước cơ bản, Map và Reduce đơn giản nhưng có thể đặc tả hầu hết các bài toán trên môi trường phân tán.

– Mô hình thực hiện MapReduce có khả năng chịu lỗi cao. Khi có lỗi xảy ra tại một nút tính toán trong hệ thống, tính toán tại nút đó sẽ được thực hiện lại mà không ảnh hưởng tới tính toán trên các nút khác.

– Tính toán MapReduce được phân tán trên các nút lưu trữ. So với các mô hình tính toán khác mà dữ liệu được sao chép đến các nút tính toán và thực hiện trên các nút đó, mô hình tính toán MapReduce khác biệt ở chỗ mã chương trình được sao chép tới các nút lưu trữ để thực thi. Đây là một trong những điểm mấu chốt tiên tiến của MapReduce vì quan điểm di chuyển mã chương trình tiết kiệm và hiệu quả hơn di chuyển dữ liệu mà có thể lên tới hàng TB.

– Nền tảng tính toán MapReduce được thiết kế để thực thi với các máy chủ phổ thông, không cần năng lực tính toán và lưu trữ lớn như mô hình tính toán song song MPI. Điều này đạt được nhờ vào thiết kế chịu lỗi cao.

Nguyên tắc hoạt động của MapReduce

MapReduce hoạt động trên một nguyên tắc đơn giản. Các phép toán lấy đầu vào là một tập các cặp khóa/giá trị và đưa ra một tập khóa/giá trị đầu ra. MapReduce biểu diễn tính toán chỉ bằng hai hàm: Map và Reduce.

Hàm Map, lấy đầu vào là một cặp khóa/giá trị và đưa đầu ra là một tập các cặp khóa/giá trị trung gian. Các cặp khóa/giá trị trung gian này sau đó được gộp lại và các cặp khóa/giá trị trung gian có cùng khóa sẽ được chuyển cho hàm Reduce. Từ đó hàm Reduce tính toán trên các cặp này nhằm đưa ra các giá trị tổng quan hơn là kết quả cuối cùng.

Tính toán MapReduce trong thực tiễn

Với nguyên tắc hoạt động của MapReduce giới thiệu bên trên, có nhiều phương pháp hiện thực hóa mô hình tính toán MapReduce như phát triển nền tảng trên các máy tính chia sẻ bộ nhớ trong, trên các máy tính đa xử lý NUMA, trên cluster tính toán... Trong phần này, chúng ta sẽ đi vào tìm hiểu tính toán MapReduce triển khai trên cluster. Một cluster gồm hàng trăm tới hàng ngàn máy chủ phổ thông kết nối với nhau qua mạng LAN thông thường 100 Mbs hoặc 1 Gbs. Phần cứng lưu trữ trên các máy chủ này không đòi hỏi hiệu năng cao, chỉ là các đĩa cứng thông thường kết nối qua chuẩn IDE. Đơn vị công việc trong chương trình MapReduce gọi là gói công việc (job), mỗi job gồm nhiều tác vụ được điều chuyển thông qua hệ thống phân phối chung tới các máy chủ thuộc cluster.

Tác vụ Map được thực hiện phân tán trên các nút lưu trữ. Quá trình phân tán được thực hiện tự động thông qua việc dữ liệu đầu vào được chia nhỏ. Tác vụ Reduce cũng được phân tán thông qua việc các cặp khóa/giá trị trung gian được nhóm lại thành các cặp có khóa giống nhau. Luồng thực thi một gói công việc MapReduce bao gồm các bước sau (hình 2.6):

– MapReduce cluster về cơ bản gồm một nút Master và các nút Worker. Nút Master làm nhiệm vụ quản lý và điều tiết các Worker.

– Thư viện MapReduce phía người sử dụng gửi mã biên dịch của tác vụ Map tới các nút tính toán thường là các nút chứa dữ liệu của tệp tin đầu vào. Số lượng các tác vụ Map được chạy song song thường bằng số các block của tệp đầu vào.

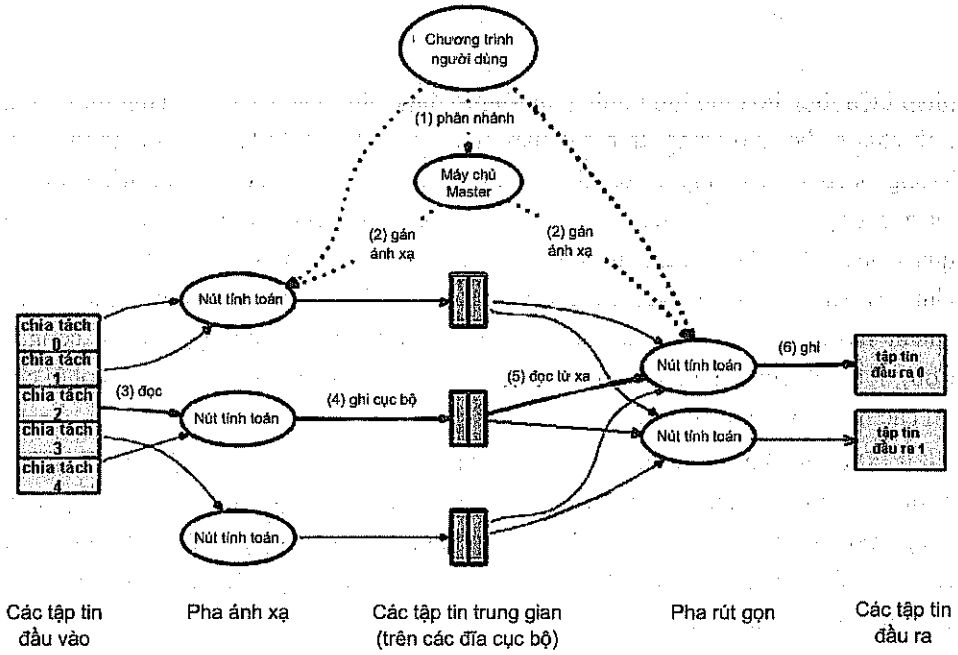
– Các nút tính toán là các worker đọc dữ liệu từ tệp tin đầu vào, thường là từ chính block được lưu trữ trên ổ đĩa cục bộ. Tác vụ Map sinh ra tập các cặp khóa/giá trị trung gian lưu trên bộ nhớ trong.

– Theo định kỳ được cấu hình, các cặp khóa/giá trị trung gian này được ghi vào ổ đĩa cứng cục bộ, chia thành R nhóm (R là số lượng các nút chạy tác vụ Reduce). Vị trí của các cặp này được thông báo cho máy chủ Master để Master làm nhiệm vụ đưa lại địa chỉ này cho các máy chủ làm tác vụ Reduce.

– Khi Worker thực hiện tác vụ Reduce được thông báo về vị trí các cặp khóa/giá trị trung gian, các Worker này sử dụng RPC để đọc dữ liệu này. Khi quá trình đọc kết thúc, Worker sắp xếp lại các cặp khóa/giá trị trung gian theo khóa.

– Worker thực hiện Reduce tính toán tuần tự trên các dữ liệu được sắp xếp. Đầu ra của tác vụ Reduce được ghi vào tệp tin đầu ra.

– Khi tất cả các tác vụ Map và Reduce được kết thúc, Master thông báo lại kết quả cho chương trình của người sử dụng.



Hình 2.6. Mô tả quá trình thực thi gói công việc

2.5. CÂU HỎI VÀ BÀI TẬP

1. Nêu các đặc điểm của hệ thống lưu trữ phân tán.
2. Nêu các đặc điểm của hệ thống lưu trữ HDFS.
3. Phân biệt và so sánh cơ sở dữ liệu NOSQL và hệ cơ sở dữ liệu quan hệ.
4. Tìm hiểu về kiến trúc Amazon S3 và so sánh với OpenStack swift.
5. So sánh kỹ thuật lưu trữ trên điện toán đám mây với kỹ thuật lưu trữ truyền thống.
6. Phân tích ưu nhược điểm của HDFS.
7. So sánh mô hình thực thi MapReduce và mô hình thực thi MPI.
8. Phân tích nhược điểm của MapReduce.
9. Giới thiệu các xu thế tính toán cải tiến MapReduce.

Chương 3
AN TOÀN VÀ BẢO MẬT

Trong một hệ thống thông tin, an toàn và bảo mật (ATBM) là sự đảm bảo tính bí mật, tính toàn vẹn và tính sẵn dùng của hệ thống dưới những đe dọa đến từ các sự cố phần cứng/phần mềm hoặc đến từ sự tấn công có chủ đích của con người. Với các hệ thống đám mây, nơi dữ liệu và các tiến trình xử lý thông tin của người dùng được giao phó cho sự quản lý của các nhà cung cấp dịch vụ, thì vấn đề đảm bảo tính an toàn và bảo mật càng trở nên cấp thiết. Chương này sẽ trình bày những vấn đề đặt ra về ATBM và giới thiệu một số giải pháp đảm bảo tính ATBM cho các hệ thống đám mây. Các chủ đề chính của chương bao gồm: Các vấn đề về ATBM trong điện toán đám mây; Một số phương pháp đảm bảo tính ATBM cho các dịch vụ đám mây; Giải pháp thiết kế kiến trúc hệ thống đám mây nhằm đảm bảo ATBM.

3.1. CÁC VẤN ĐỀ VỀ AN TOÀN VÀ BẢO MẬT TRONG ĐIỆN TOÁN ĐÁM MÂY

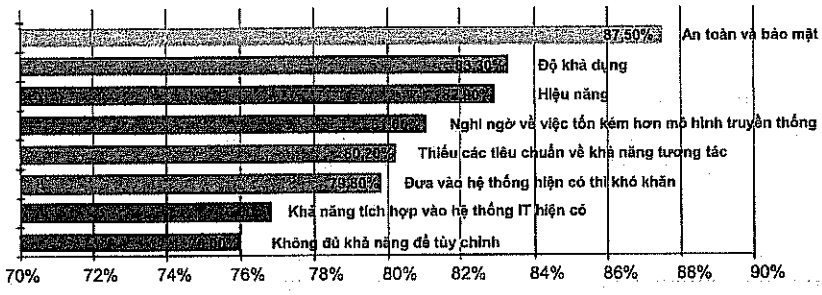
Điện toán đám mây được xem như giải pháp giúp khách hàng tiết kiệm được nhiều chi phí đầu tư cũng như công sức quản lý và vận hành hệ thống. Tuy vậy, do tính chất phân tán và trực tuyến, tích hợp nhiều tầng dịch vụ với nhiều công nghệ đặc thù, giải pháp này đồng thời cũng bộc lộ nhiều nguy cơ mới về ATBM. Năm 2009, tổ chức khảo sát và phân tích thị trường International Data Corporation (IDC) tiến hành khảo sát ý kiến của các giám đốc thông tin (CIO) từ nhiều công ty hàng đầu về những trở ngại trong việc chuyển đổi sang mô hình dịch vụ đám mây. Kết quả khảo sát (minh họa trong hình 3.1) cho thấy vấn đề ATBM đang là lo lắng hàng đầu của các tổ chức thuê dịch vụ đám mây.

Trong phần này, chúng tôi trước tiên tóm tắt một số vấn đề liên quan tới ATBM trên các tầng dịch vụ khác nhau của điện toán đám mây. Sau đó giới thiệu một số lỗ hổng ATBM và nguy cơ về ATBM trên các hệ thống đám mây.

Các vấn đề về an toàn và bảo mật trên các tầng dịch vụ đám mây

Như đã đề cập đến trong chương 1, mô hình điện toán đám mây cung cấp ba tầng dịch vụ chính: dịch vụ phần mềm (SaaS), dịch vụ nền tảng (PaaS) và dịch vụ hạ tầng (IaaS).

Với SaaS, gánh nặng về ATBM thuộc về phía nhà cung cấp dịch vụ. Các dịch vụ phần mềm thường đặt trọng tâm vào việc tích hợp chức năng đồng thời tối thiểu hóa khả năng can thiệp và mở rộng của người sử dụng. Trong khi đó, các dịch vụ nền tảng hỗ trợ nhiều hơn khả năng can thiệp và mở rộng. Và dưới cùng, các dịch vụ hạ tầng cho phép người sử dụng có khả năng can thiệp và đồng thời chịu trách nhiệm lớn nhất về ATBM.



Hình 3.1. Kết quả khảo sát của IDC về những quan ngại của khách hàng với mô hình điện toán đám mây

An toàn và bảo mật trong các dịch vụ phần mềm

SaaS cung cấp các dịch vụ phần mềm theo nhu cầu như thư điện tử, hội thảo trực tuyến, ERP, CRM,... Nội dung tiếp theo sẽ trình bày một số vấn đề về an toàn và bảo mật trong tầng dịch vụ này.

Vấn đề 1. Bảo mật ứng dụng

Người sử dụng thường truy nhập các ứng dụng đám mây thông qua trình duyệt web. Sai sót trong các trang web có thể tạo nên những lỗ hổng của dịch vụ SaaS. Tin tặc từ đó có thể gây thương tổn tới các máy tính của người sử dụng để thực hiện các hành vi ác ý hoặc ăn trộm các thông tin nhạy cảm. ATBM trong dịch vụ SaaS không khác với trong các ứng dụng web thông thường. Có thể tham khảo thêm về những vấn đề ATBM ứng dụng web thông qua bài viết "The most critical web application security risks" do OWASP (Open Web Application Security Project) xuất bản.

Vấn đề 2. Nhiều người thuê đồng thời (multi-tenancy)

Các dịch vụ SaaS có thể được xây dựng theo ba mô hình:

– Mô hình khả mở (scalability model): Mỗi người sử dụng được cấp một thể hiện đã chuyên biệt hóa của phần mềm. Mặc dù có nhiều nhược điểm, nhưng mô hình này lại không tạo nên những vấn đề lớn về an toàn và bảo mật.

– Mô hình cấu hình qua siêu dữ liệu (configurability via metadata): Mỗi người cũng có một thể hiện riêng của phần mềm, tuy nhiên các thể hiện này dùng chung một mã nguồn, sự khác biệt chỉ là cấu hình của phần mềm thông qua các siêu dữ liệu.

– Mô hình nhiều người thuê đồng thời: Trong mô hình này, một thể hiện duy nhất của ứng dụng được chia sẻ cho nhiều người thuê. Khi đó tài nguyên sẽ được sử dụng hiệu quả (mặc dù tính khả mở sẽ giảm đi). Trong mô hình này, do dữ liệu của các người dùng được lưu trữ trên cùng một cơ sở dữ liệu nên nguy cơ về rò rỉ dữ liệu có thể xảy ra.

Vấn đề 3. Bảo mật dữ liệu

Trong SaaS, dữ liệu thường được xử lý dưới dạng bản rõ và được lưu trữ trên đám mây. Nhà cung cấp dịch vụ SaaS sẽ phải chịu trách nhiệm về bảo mật dữ liệu trong khi chúng được xử lý và lưu trữ. Việc sao lưu dữ liệu rất phổ biến trong các hệ thống đám mây cũng tạo nên những vấn đề phát sinh cho bảo mật dữ liệu, nhất là khi nhà cung cấp dịch vụ ký hợp đồng sao lưu lại với một đối tác thứ ba không đáng tin cậy.

Vấn đề 4. Truy cập dịch vụ

Việc các dịch vụ SaaS hỗ trợ khả năng truy cập thông qua trình duyệt mang lại nhiều thuận lợi, ví dụ như chúng có thể dễ dàng được truy cập từ các thiết bị kết nối mạng khác PC như điện thoại hay máy tính bảng. Tuy nhiên, điều này lại tạo nên những nguy cơ mới về ATBM như các phần mềm ăn trộm dữ liệu trên di động, mạng Wifi không an toàn, kho ứng dụng không an toàn,...

An toàn và bảo mật trong các dịch vụ nền tảng

PaaS hỗ trợ việc xây dựng các ứng dụng đám mây mà không cần quan tâm tới vấn đề thiết lập và duy trì hạ tầng phần cứng hay môi trường phần mềm. Vấn đề ATBM trong PaaS liên quan tới hai khía cạnh: bảo mật trong nội tại của dịch vụ PaaS và bảo mật trong phần mềm của khách hàng triển khai trên nền dịch vụ PaaS. Nội dung tiếp theo giới thiệu một số vấn đề về ATBM trong tầng dịch vụ nền tảng.

Vấn đề 5. An toàn và bảo mật của bên thứ ba

Dịch vụ PaaS thường không chỉ cung cấp môi trường phát triển ứng dụng của nhà cung cấp dịch vụ mà đôi khi cho phép sử dụng những dịch vụ mạng của bên thứ ba. Những dịch vụ này thường được đóng gói dưới dạng thành phần trộn (mashup). Chính vì vậy, ATBM trong các dịch vụ PaaS cũng phụ thuộc vào ATBM của chính các mashup này.

Vấn đề 6. Vòng đời của ứng dụng

Giống như các loại hình ứng dụng khác, các ứng dụng trên dịch vụ đám mây cũng có thể liên tục nâng cấp. Việc nâng cấp ứng dụng đòi hỏi nhà cung cấp dịch vụ PaaS phải hỗ trợ tốt cho những thay đổi của ứng dụng. Đồng thời, người phát triển cũng cần phải lưu ý rằng sự thay đổi của các thành phần ứng dụng trong quá trình nâng cấp đôi khi gây ra các vấn đề về ATBM.

An toàn và bảo mật trong các dịch vụ hạ tầng

IaaS cung cấp một vùng chứa tài nguyên như máy chủ, mạng, kho lưu trữ bao gồm cả các tài nguyên được ảo hóa. Khách hàng có toàn quyền kiểm soát và

quản lý các tài nguyên họ thuê được. Các nhà cung cấp dịch vụ IaaS phải bảo vệ hệ thống khỏi những ảnh hưởng liên quan tới vấn đề ATBM phát sinh từ các tài nguyên cho thuê của khách hàng. Nội dung tiếp theo liệt kê một số vấn đề về ATBM trong tầng dịch vụ IaaS.

Vấn đề 7. Ảo hóa

Công nghệ ảo hóa cho phép người sử dụng dễ dàng tạo lập, sao chép, chia sẻ, di trú và phục hồi các máy ảo trên đó thực thi các ứng dụng. Công nghệ này tạo nên một tầng phần mềm mới trong kiến trúc phần mềm của hệ thống. Chính vì vậy nó cũng mang đến những nguy cơ mới về ATBM.

Vấn đề 8. Giám sát máy ảo

Thành phần giám sát máy ảo (virtual machine monitor – VMM) hay còn gọi là supervisor có trách nhiệm giám sát và quản lý các máy ảo được tạo trên máy vật lý. Chính vì vậy, nếu VMM bị tổn thương, các máy ảo do nó quản lý cũng có thể bị tổn thương. Di trú máy ảo từ một VMM này sang một VMM khác cũng tạo nên những nguy cơ mới về ATBM.

Vấn đề 9. Tài nguyên chia sẻ

Các máy ảo trên cùng một hệ thống chia sẻ một số tài nguyên chung như CPU, RAM, thiết bị vào ra,... Việc chia sẻ này có thể làm giảm tính ATBM của mỗi máy ảo. Ví dụ, một máy ảo có thể đánh cắp thông tin của máy ảo khác thông qua bộ nhớ chia sẻ. Hơn nữa nếu khai thác một số kênh giao tiếp ngầm giữa các máy ảo, các máy ảo có thể bỏ qua mọi quy tắc bảo mật của VMM.

Vấn đề 10. Kho ảnh máy ảo công cộng

Trong môi trường IaaS, ảnh máy ảo là một mẫu sẵn có để tạo nên các máy ảo. Một hệ thống đám mây có thể cung cấp một số ảnh máy ảo trong một kho công cộng để người dùng có thể dễ dàng tạo nên máy ảo theo nhu cầu của mình. Đôi khi hệ thống đám mây có thể cho phép người sử dụng tự tải ảnh máy ảo của mình lên kho công cộng này. Điều này tạo nên một nguy cơ về bảo mật khi tin tặc tải lên những ảnh máy ảo có chứa mã độc và người sử dụng có thể dùng những ảnh này để tạo máy ảo của họ. Hơn nữa, qua việc tải ảnh máy ảo lên kho công cộng, người dùng cũng có nguy cơ mất đi những dữ liệu nhạy cảm của mình trong ảnh máy ảo đã tải. Ảnh máy ảo cũng tạo ra nguy cơ về bảo mật khi chúng không được vá lỗi giống như các hệ thống đang vận hành.

Vấn đề 11. Phục hồi máy ảo

Người sử dụng có thể phục hồi máy ảo về một trạng thái đã được lưu trữ trước đó. Tuy nhiên, nguy cơ về ATBM lại phát sinh khi những lỗi được vá mới không áp dụng cho trạng thái máy ảo cũ.

Vấn đề 12. Mạng ảo

Mạng ảo có thể được chia sẻ bởi nhiều người thuê trong một vùng chứa tài nguyên. Khi đó, các vấn đề ATBM có thể phát sinh giữa các người thuê chia sẻ chung

mạng ảo này như việc một máy ảo có thể nghe trộm các bản tin gửi cho máy ảo khác trên cùng mạng.

Một số lỗ hổng về an toàn và bảo mật trong các hệ thống đám mây

Để giải quyết những vấn đề về ATBM đã đặt ra như trong phần trước, công việc đầu tiên của các nhà cung cấp dịch vụ đám mây là phải xác định được những lỗ hổng có thể tồn tại về ATBM trong hệ thống của mình. Bảng 3.1 tổng kết một số lỗ hổng điển hình về ATBM trong các hệ thống đám mây.

Bảng 3.1. Các lỗ hổng an toàn bảo mật trong hệ thống đám mây

STT	*Lỗ hổng*	*Mô tả*
1	Giao diện người sử dụng và API được cung cấp không an toàn	Phần lớn các nhà cung cấp dịch vụ đám mây cung cấp dịch vụ thông qua các giao diện HTTP, SOAP, hoặc REST. Những vấn đề bảo mật gắn với các giao diện này bao gồm: – Chứng nhận sử dụng hợp lệ yếu; – Việc kiểm tra xác quyền không đủ; – Thiếu kiểm tra tính hợp lệ của dữ liệu.
2	Tài nguyên phân bổ không giới hạn	– Hệ thống có thể gặp phải tình huống dành sẵn quá nhiều tài nguyên nếu như việc đánh giá về tài nguyên sử dụng không chính xác.
3	Các lỗ hổng liên quan tới dữ liệu	– Khả năng phân tách yếu cho những dữ liệu có nguồn gốc khác nhau (chẳng hạn của các đối tượng cạnh tranh, hoặc của tin tặc) dẫn đến chúng dễ bị đánh cắp. – Dữ liệu không được xóa hoàn toàn. – Dữ liệu được sao lưu bởi một bên thứ ba không tin cậy. – Người sử dụng thường không biết vị trí lưu trữ dữ liệu. – Dữ liệu thường được lưu trữ, lưu chuyển và xử lý dưới dạng bản rõ.

4	Lỗ hổng trong máy ảo	– Tồn tại những kênh giao tiếp không tường minh. – Cấp phát và giải phóng tài nguyên không hạn chế trong máy ảo. – Di trú không được kiểm soát. – Không kiểm soát các snapshot có thể dẫn đến rò rỉ dữ liệu. – Các máy ảo có IP có thể quan sát được bên trong đám mây, do vậy tin tặc có thể định vị được một máy ảo cần tấn công.
5	Lỗ hổng trong ảnh máy ảo	– Ảnh máy ảo được đặt trên kho lưu trữ công cộng một cách không kiểm soát. – Ảnh máy ảo không thể vá lỗi vì chúng không hoạt động.
6	Lỗ hổng trong hypervisor	– Khả năng cấu hình linh động của hypervisor có thể khiến chúng bị khai thác.
7	Lỗ hổng trong mạng ảo	– Lỗ hổng khi chia sẻ các cầu nối ảo giữa các máy ảo.

Những nguy cơ về an toàn và bảo mật trong các hệ thống đám mây

Tháng 11 năm 2008, liên minh an toàn bảo mật trong điện toán đám mây (Cloud Security Alliance – CSA) được thành lập dưới hình thức một tổ chức phi lợi nhuận. Nhiệm vụ chính của CSA là xác định các vấn đề liên quan tới ATBM đám mây, sau đó cung cấp những kinh nghiệm và giải pháp hỗ trợ giải quyết các vấn đề đó. Tổ chức này đã nhận được sự ủng hộ của trên một trăm hai mươi nhà cung cấp dịch vụ đám mây, bao gồm những nhà cung cấp hàng đầu như Google, Amazon hay Saleforce.

Năm 2013, trong tài liệu "The Notorious Nine: Cloud Computing Top Threats in 2013", CSA công bố 9 nguy cơ lớn nhất về ATBM trong các hệ thống đám mây. Các nguy cơ này bao gồm:

– *Rò rỉ dữ liệu.* Rò rỉ dữ liệu là việc dữ liệu của người dùng hoặc tổ chức thuê dịch vụ đám mây bị thất thoát vào tay những đối tượng không mong đợi. Đây có lẽ là một trong những đe dọa nghiêm trọng nhất đối các tổ chức sử dụng dịch vụ. Trong một hệ thống đám mây, việc tích hợp những công nghệ mới tạo nên những nguy cơ mới về thất thoát dữ liệu. Ví dụ, vào tháng 11 năm 2012, các nghiên cứu viên ở trường Đại học North Carolina, trường Đại học Wisconsin và tổ chức RSA đã công bố một công trình, trong đó mô tả phương thức sử dụng một máy ảo để trích xuất các khóa riêng tư từ máy ảo khác trên cùng một máy vật lý.

– *Mất mát dữ liệu.* Mất mát dữ liệu là việc dữ liệu của người dùng hoặc tổ chức thuê dịch vụ bị phá hủy hoặc không thể truy nhập được. Đối với khách hàng, mất mát dữ liệu là một điều tồi tệ, nó không những khiến khách hàng mất đi thông tin mà đôi khi khiến các hoạt động của khách hàng trên hệ thống dịch vụ bị gián đoạn hoặc thậm chí sụp đổ. Nguyên nhân cho việc mất mát dữ liệu có thể đến từ những tấn công của tin tặc; từ trục trặc của hệ thống phần mềm/phần cứng; hoặc do các thảm họa như cháy nổ, động đất. Đôi khi mất mát dữ liệu còn do phía người dùng, ví dụ như khi người dùng gửi bản mã hóa của dữ liệu lên đám mây nhưng lại quên mất khóa để giải mã chúng.

– *Bị đánh cắp tài khoản hoặc thất thoát dịch vụ.* Hiện tượng người sử dụng bị đánh cắp tài khoản hoặc thất thoát dịch vụ có thể nói khá phổ biến trong các loại hình dịch vụ trực tuyến. Nhiều người sử dụng bị đánh cắp tài khoản do "dính bẫy" phishing hoặc do các lỗ hổng phần mềm trong hệ thống bị tin tặc khai thác. Môi trường điện toán đám mây đang là miền đất mới cho các kỹ thuật tấn công dạng này. Khi quyền truy nhập của một hệ thống dịch vụ đám mây rơi vào tay tin tặc, chúng có thể can thiệp vào các hoạt động của hệ thống, thay đổi các giao dịch của hệ thống, dẫn hướng khách hàng của hệ thống tới những liên kết của chúng, biến tài nguyên của khách hàng trên đám mây thành một căn cứ tấn công mới của chúng,...

Một ví dụ điển hình là sự kiện dịch vụ đám mây của Amazon gặp lỗi XSS (Cross-site Scripting) vào tháng 4 năm 2010. Lỗi này khiến khách hàng mất đi quyền truy nhập vào hệ thống và tài nguyên của khách hàng trên hệ thống trở thành các botnet của mạng lưới tấn công Zeus.

– *Giao diện và API không an toàn.* Các nhà cung cấp dịch vụ đám mây thường cung cấp cho khách hàng một tập giao diện phần mềm (API) nhằm giúp khách hàng có thể quản lý và tương tác với dịch vụ một cách tự động. Các API được tổ chức thành nhiều nhóm theo từng tầng dịch vụ. API thuộc các tầng khác nhau phụ thuộc vào nhau giống như sự phụ thuộc giữa các tầng dịch vụ. Khi lỗ hổng bảo mật trong các API bị tin tặc khai thác, tính ATBM của hệ thống sẽ bị xâm phạm. Lỗ hổng trong các API tầng thấp sẽ ảnh hưởng đến các API thuộc tầng cao hơn. Do vậy, vấn đề ATBM của hệ thống đám mây gắn bó mật thiết tới việc bảo mật cho các API này.

Bên cạnh đó, các tổ chức sử dụng dịch vụ đám mây đôi khi tự xây dựng những tầng dịch vụ mới cho khách hàng của họ dựa trên các API của nhà cung cấp dịch vụ đám mây. Điều này càng làm tăng thêm những rủi ro về ATBM từ hệ thống API của đám mây.

– *Từ chối dịch vụ.* Tấn công từ chối dịch vụ là cách thức hạn chế khả năng truy nhập vào dữ liệu và ứng dụng của người sử dụng dịch vụ. Phương thức thường dùng trong việc tấn công từ chối dịch vụ là việc tạo ra một số lượng yêu cầu lớn bất thường tới các dịch vụ bị tấn công khiến cho tài nguyên hệ thống (RAM, CPU, HDD, băng thông,...) cạn kiệt. Khi đó hệ thống trở nên chậm chạp, đáp ứng kém hoặc không đáp ứng được các yêu cầu từ khách hàng khiến cho họ bất bình và quay lưng lại với dịch vụ.

– *Nguy cơ từ bên trong.* Nguy cơ từ bên trong ám chỉ những nguy cơ đến từ các cá nhân có ác ý nằm trong tổ chức cung cấp dịch vụ, ví dụ như một quản trị viên của hệ thống đám mây. Khi các đối tượng này có quyền truy nhập vào mạng, dữ liệu, các máy chủ của hệ thống đám mây, các dữ liệu quan trọng của khách hàng có thể bị đánh cắp; ứng dụng của khách hàng có thể bị sửa đổi khiến chúng vận hành theo chiều hướng gây thiệt hại tới khách hàng.

– *Sự lạm dụng dịch vụ đám mây.* Một trong những lợi ích mà điện toán đám mây mang lại là nó cho phép một tổ chức nhỏ cũng có khả năng sử dụng một hạ tầng lớn. Một tổ chức nhỏ có thể gặp khó khăn khi xây dựng và duy trì hàng chục ngàn máy chủ. Tuy nhiên, với mô hình điện toán đám mây, họ lại có thể thuê được chúng trong một khoảng thời gian nhất định. Với nguyên tắc như vậy, một tin tặc có thể thuê một hệ thống hàng chục ngàn máy chủ của dịch vụ hạ tầng đám mây để nhằm mục đích xấu như giải mã dữ liệu, tấn công DDoS, hay phát tán các thông tin hoặc phần mềm độc hại.

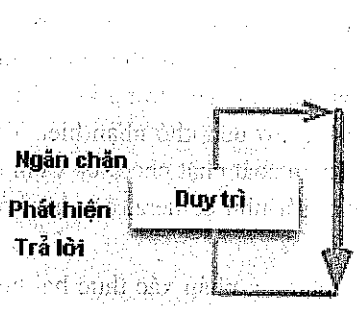
– *Khảo sát không đầy đủ.* Nhiều doanh nghiệp lựa chọn việc chuyển đổi sang sử dụng các dịch vụ đám mây do những hứa hẹn về việc giảm chi phí đầu tư, tăng hiệu quả vận hành,... Tuy nhiên, doanh nghiệp sẽ chịu nhiều rủi ro tiềm tàng nếu họ thiếu sự hiểu biết về môi trường công nghệ mới này. Ví dụ khi một doanh nghiệp chuyển đổi một hệ thống ứng dụng đang vận hành trên một mạng cục bộ lên đám mây. Nếu hệ thống ứng dụng này áp dụng một số giả định về chính sách ATBM cho mạng cục bộ thì khi chuyển đổi ứng dụng lên môi trường điện toán đám mây, các chính sách này sẽ không còn hiệu lực nữa và khi đó ứng dụng sẽ nằm dưới nguy cơ mất an toàn.

– *Lỗ hổng trong các công nghệ sử dụng chung.* Hệ thống đám mây thường cung cấp các dịch vụ một cách linh hoạt thông qua việc chia sẻ hạ tầng, nền tảng và ứng dụng. Tuy nhiên, trong hệ thống thường có một số thành phần (chủ yếu từ hạ tầng như bộ đệm cache của CPU, bộ xử lý đồ họa GPU,...) không được thiết kế cho việc chia sẻ này. Các đặc điểm này khi bị tin tặc khai thác có thể tạo nên những lỗ hổng bảo mật mới.

Có thể nói, đa phần những nguy cơ kể trên đến từ những công nghệ cấu thành nên hệ thống đám mây như dịch vụ web, trình duyệt web, ảo hóa,...

3.2. MỘT SỐ PHƯƠNG PHÁP ĐẢM BẢO AN TOÀN CHO DỊCH VỤ ĐÁM MÂY

Để đảm bảo an toàn và bảo mật cho hệ thống đám mây, các nhà quản lý dịch vụ đám mây cần những chiến lược và quy trình hoàn chỉnh thay vì áp dụng những kỹ thuật ứng phó đơn lẻ, rời rạc. Nếu chúng ta xem xét các sự cố an toàn và bảo mật là một dạng rủi ro với hệ thống thì việc đảm bảo an toàn và bảo mật cho hệ thống có thể được thực hiện theo một quy trình quản lý rủi ro như trong hình 3.2.



Giai đoạn	Hoạt động
Lập kế hoạch	Phân loại tài nguyên thông tin Chọn cơ chế kiểm soát an toàn và bảo mật Đánh giá rủi ro
Triển khai	Cài đặt cơ chế kiểm soát
Đánh giá	Đánh giá Xem xét định kỳ

Hình 3.2. Quy trình quản lý rủi ro về an toàn và bảo mật

Các bước thực hiện chính trong quy trình bao gồm:

Bước 1. Lập kế hoạch: Mục tiêu của bước này là nhận định những nguy cơ về an toàn và bảo mật; xác định các *cơ chế kiểm soát an toàn và bảo mật* (security controls) hiệu quả nhằm giải quyết các nguy cơ; lên kế hoạch cho việc thực hiện các cơ chế kiểm soát an toàn và bảo mật này.

Bước 2. Triển khai. Bao gồm việc cài đặt và cấu hình cho các cơ chế kiểm soát an toàn và bảo mật.

Bước 3. Đánh giá: Đánh giá tính hiệu quả của của các cơ chế kiểm soát và định kỳ xem xét tính đầy đủ của cơ chế kiểm soát.

Bước 4. Duy trì: Khi hệ thống và các cơ chế kiểm soát đã vận hành, cần thường xuyên cập nhật những thông tin mới về các nguy cơ ATBM.

Cơ chế kiểm soát an toàn và bảo mật (security controls) được hiểu như một kỹ thuật, một hướng dẫn hay một trình tự được định nghĩa tường minh giúp ích cho việc phát hiện, ngăn chặn, hoặc giải quyết các sự cố về an toàn bảo mật.

Năm 2013, liên minh an toàn và bảo mật trong điện toán đám mây (CSA) xuất bản tài liệu CSA Cloud Control Matrix phiên bản 3.0 (viết tắt là CSA CCM v3.0). Tài liệu này đề xuất một tập hợp bao gồm hơn một trăm hai mươi cơ chế kiểm soát an toàn và bảo mật nhằm trợ giúp các nhà cung cấp dịch vụ đám mây dễ dàng ứng phó với các nguy cơ về ATBM.

Trong khuôn khổ cuốn sách này, chúng tôi không có ý định giới thiệu lại tất cả các cơ chế kiểm soát đó. Thay vì vậy, cuốn sách giới thiệu một số biện pháp đảm bảo ATBM được áp dụng phổ biến trong các hệ thống đám mây.

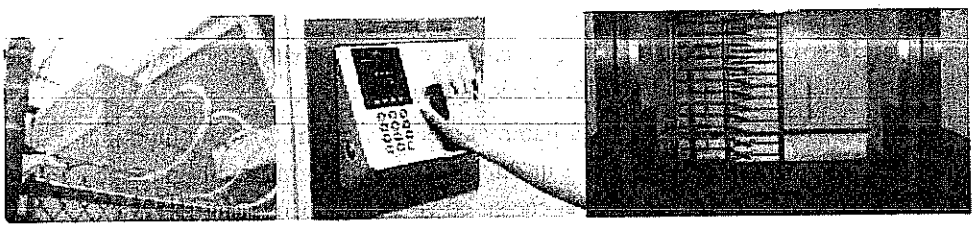
Bảo mật trung tâm dữ liệu

Bảo mật mức vật lý: Các công ty như Google, Microsoft, Yahoo, Amazon và một số nhà khai thác trung tâm dữ liệu đã có nhiều năm kinh nghiệm trong việc thiết kế, xây dựng và vận hành các trung tâm dữ liệu quy mô lớn. Những kinh nghiệm này

đã được áp dụng cho chính nền tảng cơ sở hạ tầng điện toán đám mây của họ. Kỹ thuật tiên tiến trong việc bảo mật mức vật lý là đặt các trung tâm dữ liệu tại các cơ sở khó nhận biết với những khoảng sân rộng và vành đai kiểm soát được đặt theo tiêu chuẩn quân sự cùng với các biên giới tự nhiên khác. Các tòa nhà này nằm trong khu dân cư không đặt biển báo hoặc đánh dấu, giúp cho chúng càng trở nên khó nhận biết. Truy cập vật lý được các nhân viên bảo vệ chuyên nghiệp kiểm soát chặt chẽ ở cả vành đai kiểm soát và tại các lối vào với các phương tiên giám sát như camera, các hệ thống phát hiện xâm nhập và các thiết bị điện tử khác.

Những nhân viên được cấp phép phải sử dụng phương pháp xác thực hai bước không ít hơn ba lần mới có thể truy cập vào tầng trung tâm dữ liệu. Thông thường, tất cả khách tham quan hay các nhà thầu phải xuất trình căn cước và phải đăng ký. Sau đó họ tiếp tục được hộ tống bởi đội ngũ nhân viên được cấp phép.

Các công ty cung cấp dịch vụ đám mây đôi khi thiết lập trung tâm dữ liệu với mức độ tiên tiến vượt xa so với các trung tâm dữ liệu của các công ty dịch vụ tài chính. Máy chủ của các trung tâm dữ liệu này được đặt vào hầm trú ẩn kiên cố không dễ dàng vượt qua như chúng ta vẫn thấy trong các bộ phim gián điệp. Trong trung tâm dữ liệu Fort Knox của Salesforce.com, các nhân viên an ninh áp dụng phương pháp tuần tra vòng tròn, sử dụng máy quét sinh trắc học năm cấp độ, hay thiết kế lồng bẫy có thể rơi xuống khi chứng thực không thành công. Hình 3.3 minh họa một số biện pháp bảo mật vật lý.



Hình 3.3. Bảo mật mức vật lý

Để tránh các cuộc tấn công nội bộ, hệ thống ghi nhật ký và kiểm tra phân tích cho các kết nối cục bộ được kích hoạt thường xuyên. AICPA (American Institute of Certified Public Accountants) cung cấp những tiêu chuẩn kỹ thuật liên quan tới bảo mật kể trên trong chứng nhận SAS 70.

Chứng nhận SAS 70: Phần lớn các đám mây công cộng đều cần chứng nhận này. Chứng nhận này không phải là một danh mục để kiểm tra tại một thời điểm. Nó yêu cầu các tiêu chuẩn phải được duy trì trong ít nhất 6 tháng kể từ khi bắt đầu đăng ký. Thông thường chi phí để đạt được chứng nhận này rất lớn mà chỉ các nhà cung cấp hàng đầu mới đạt được.

Các biện pháp kiểm soát truy nhập

Tiếp theo vấn đề bảo mật mức vật lý là các kỹ thuật kiểm soát những đối tượng có thể truy nhập vào đám mây. Dĩ nhiên điều này là cực kỳ cần thiết, bởi vì thiếu nó, tin tặc có thể truy nhập vào các máy chủ của người sử dụng, đánh cắp thông tin hoặc sử dụng chúng cho các mục đích xấu. Chúng ta hãy lấy ví dụ về cách thức kiểm soát truy nhập của Amazon Web Services (cũng tương tự như với một số đám mây khác). Cách thức kiểm soát này được thức hiện qua nhiều bước, thường bắt đầu với thông tin thẻ tín dụng của khách hàng.

Xác nhận bằng hóa đơn thanh toán: Nhiều dịch vụ thương mại điện tử sử dụng hóa đơn thanh toán cho mục đích xác thực với người dùng. Ở môi trường trực tuyến, hóa đơn thanh toán thường gắn liền với thẻ tín dụng của khách hàng. Tuy nhiên thẻ tín dụng thì thường không có nhiều thông tin gắn với khách hàng nên một số biện pháp khác có thể được áp dụng.

Kiểm tra định danh qua điện thoại: Mức độ tiếp theo của kỹ thuật kiểm soát truy cập là phải xác định đúng đối tượng truy cập. Để tránh rủi ro trong việc xác nhận, một hình thức xác nhận qua các kênh liên lạc khác như điện thoại là cần thiết. Thông thường nhà cung cấp sẽ liên hệ với khách hàng và yêu cầu khách hàng trả lời số PIN được hiển thị trên trình duyệt.

Giấy phép truy nhập: Hình thức giấy phép truy nhập đơn giản nhất chính là mật khẩu. Khách hàng có thể lựa chọn cho mình một mật khẩu mạnh hoặc có thể lựa chọn những giấy phép truy nhập nhiều bước như RSA SecurID. Người sử dụng cần dùng giấy phép truy nhập khi họ muốn sử dụng dịch vụ trực tiếp. Trong trường hợp người sử dụng dịch vụ qua API, họ cần phải có khóa truy nhập.

Khóa truy nhập: Để gọi bất kỳ API nào của hệ thống đám mây, người sử dụng phải có một khóa truy nhập. Khóa này được cung cấp cho người sử dụng trong quá trình thiết lập tài khoản. Người sử dụng cần bảo vệ khóa truy nhập này để tránh sự rò rỉ dịch vụ.

Giấy phép X.509: Giấy phép X.509 dựa trên ý tưởng về hạ tầng khóa công khai (PKI). Một giấy phép X.509 bao gồm một giấy phép (chứa khóa công khai và nội dung cấp phép) và một khóa bí mật. Giấy phép được sử dụng mỗi khi tiêu thụ dịch vụ, trong đó khóa bí mật được sử dụng để sinh ra chữ ký số cho mỗi yêu cầu dịch vụ. Dĩ nhiên, khóa bí mật cần phải được giữ kín và không được phép chia sẻ. Tuy nhiên, do giấy phép X.509 thường được các nhà cung cấp sinh ra và chuyển cho người sử dụng nên không thể đảm bảo 100% rằng khóa bí mật không bị rò rỉ.

Để sử dụng giấy phép X.509, khi yêu cầu dịch vụ, người sử dụng sinh chữ ký số bằng khóa bí mật của mình, sau đó gắn chữ ký số, giấy phép với yêu cầu dịch vụ. Khi hệ thống nhận được yêu cầu, nó sẽ sử dụng khóa công khai trong giấy phép để giải mã chữ ký số và chứng thực người dùng. Hệ thống cũng sử dụng giấy phép để khẳng định các yêu cầu đặt ra là hợp lệ.

Cặp khóa: Cặp khóa là yếu tố quan trọng nhất trong việc truy nhập vào các thể hiện của AWS. Mỗi dịch vụ cần một cặp khóa riêng biệt. Cặp khóa cho phép hệ thống đảm bảo người dùng hợp lệ. Mặc dù không thể thay thế cặp khóa, tuy nhiên người sử dụng có thể đăng ký nhiều cặp khóa.

AWS tạo cặp khóa bằng AWS Management Console nếu người sử dụng không tự tạo ra cho mình. Khóa bí mật sẽ được gửi đến người sử dụng và sau đó hệ thống sẽ không lưu trữ lại chúng.

Bảo mật dữ liệu và mạng

Bảo mật hệ điều hành: Bảo mật mức hệ thống có nhiều cấp độ: bảo mật cho hệ điều hành của máy chủ vật lý; bảo mật cho hệ điều hành của các máy ảo chạy trên nó; tường lửa và bảo mật cho các API.

Để bảo mật cho máy chủ vật lý, Amazon yêu cầu người quản trị sử dụng khóa SSH để truy nhập vào các máy *bastion*. Bastion là các máy được thiết kế đặc biệt và không cho phép người sử dụng truy nhập tới chúng. Sau khi đã truy nhập được vào bastion, người quản trị có thể thực hiện một số lệnh với mức ưu tiên cao lên các máy chủ vật lý. Khi người quản trị đã hoàn tất công việc, quyền truy nhập của họ vào các máy bastion sẽ bị rút.

Bảo mật mạng: Các đám mây công cộng thường cung cấp một hệ thống tường lửa để ngăn chặn các truy nhập trái phép. Hệ thống tường lửa nội bộ được sử dụng để kiểm soát sự trao đổi nội tại bên trong đám mây. Thông thường người sử dụng cần định nghĩa tường minh các cổng cần mở cho các giao dịch nội bộ này. Việc kiểm soát và thay đổi các luật tường lửa do mỗi máy ảo tự đảm nhận, tuy nhiên hệ thống đám mây sẽ yêu cầu giấy phép X.509 khi người sử dụng thực hiện các thay đổi này trên máy ảo. Trong mô hình cung cấp dịch vụ của Amazon EC2, quản trị viên của hệ thống đám mây và quản trị viên của các máy ảo là hai đối tượng khác nhau. AWS khuyến khích người sử dụng tự định nghĩa thêm các luật tường lửa cho các máy ảo của mình.

Thông thường, tường lửa cho mỗi máy ảo mặc định sẽ từ chối mọi kết nối tới các cổng, người sử dụng sẽ phải cân nhắc cẩn thận cho việc mở cổng nào phù hợp với ứng dụng của mình. Các đám mây công cộng thường là đích ngắm của các tấn công trên mạng internet như DDoS.

Bảo mật cho môi trường cộng sinh: Trong hệ thống đám mây Amazon EC2, một máy ảo không thể chạy dưới chế độ hỗn tạp (promiscuous mode) để có thể "ngửi" gói tin từ các máy ảo khác. Kể cả khi người sử dụng có ý thiết lập chế độ hỗn tạp này cho máy ảo thì các gói tin tới các máy ảo khác cũng không thể gửi đến máy ảo đó được. Chính vì vậy, các phương pháp tấn công theo kiểu ARP cache poisoning không có hiệu lực trong Amazon EC2. Tuy nhiên, một khuyến cáo chung cho khách hàng là họ nên mã hóa những giao dịch qua mạng quan trọng cho dù chúng đã được bảo vệ cẩn thận bởi EC2.

Các nhà cung cấp dịch vụ đám mây cũng thường cung cấp không gian lưu trữ trên một kho dữ liệu dùng chung. Các đối tượng được lưu trữ thường được kèm theo mã băm MD5 để xác nhận tính toàn vẹn. Không gian lưu trữ cho từng người sử dụng cũng được ảo hóa thành các đĩa ảo và chúng thường được xóa mỗi khi khởi tạo. Chính vì vậy, vấn đề rò rỉ dữ liệu do sử dụng chung không gian lưu trữ vật lý không quá lo ngại. Tuy vậy, các nhà cung cấp dịch vụ đám mây thường khuyến cáo người sử dụng hệ thống tệp được mã hóa trên các thiết bị lưu trữ ảo này.

Bảo mật cho các hệ thống giám sát: Các hệ thống giám sát thường được sử dụng để bật/tắt các máy ảo, thay đổi tham số về tường lửa,... Mọi hành động này đều yêu cầu giấy phép X.509. Hơn nữa, khi các hành vi này được thực hiện qua các API, có thể bổ sung thêm một tầng bảo mật nữa bằng cách mã hóa các gói tin, ví dụ sử dụng SSL. Khuyến cáo của các nhà cung cấp dịch vụ là nên luôn luôn sử dụng kênh SSL cho việc thực thi các API của nhà cung cấp dịch vụ.

Bảo mật lưu trữ dữ liệu: Các dịch vụ lưu trữ đám mây thường kiểm soát quyền truy nhập dữ liệu thông qua một danh sách kiểm soát truy nhập (ACL – access control list). Với ACL, người sử dụng có toàn quyền kiểm soát tới những đối tượng được phép sử dụng dịch vụ của họ.

Một lo lắng khác cho vấn đề bảo mật dữ liệu là chúng có thể bị đánh cắp trong quá trình truyền thông giữa máy của người sử dụng dịch vụ và đám mây. Khi đó các API được bảo vệ bởi SSL sẽ là giải pháp cần thiết. Khuyến cáo chung với người dùng là trong mọi trường hợp, nên mã hóa dữ liệu trước khi gửi đến lưu trữ trên đám mây.

3.3. THIẾT KẾ KIẾN TRÚC HỆ THỐNG ĐÁM MÂY NHẰM ĐẢM BẢO AN TOÀN BẢO MẬT

Thiết kế kiến trúc là bước quan trọng trong quy trình xây dựng một hệ thống phức tạp. Mục tiêu chính của bước này là xác định được một (hoặc nhiều) cấu trúc tổng thể của hệ thống với những thành phần và mối quan hệ giữa chúng.

Trong phần này, chúng ta tập trung quan tâm tới cấu trúc vật lý (trung tâm dữ liệu, mạng kết nối,...) và cấu trúc thành phần phần mềm (các phân hệ) của hệ thống đám mây trong mục tiêu đáp ứng tính an toàn và bảo mật. Đầu tiên, chúng ta sẽ nhận định một số yêu cầu kiến trúc liên quan tới an toàn và bảo mật. Sau đó giới thiệu một số mẫu kiến trúc điển hình cho an toàn và bảo mật đám mây. Phần cuối cùng giới thiệu một số ví dụ về kiến trúc các hệ thống đám mây.

Những yêu cầu an toàn và bảo mật cho kiến trúc đám mây

Một trong những mục tiêu cho việc thiết kế kiến trúc là việc đảm bảo sự đáp ứng của hệ thống với những yêu cầu đặt ra, trong đó bao hàm cả các yêu cầu về an toàn và bảo mật. Các yêu cầu này thường xuất phát từ một số yếu tố cần cân nhắc như chi phí, độ tin cậy, hiệu năng, các ràng buộc pháp lý,... Nội dung tiếp sau đây tóm tắt một số yêu cầu bảo mật cho các hệ thống đám mây.

Yêu cầu bảo mật mức vật lý

Hệ thống đám mây được xây dựng từ một hoặc một vài trung tâm dữ liệu. Việc đảm bảo ATBM cho các trung tâm dữ liệu này cũng chính là một yêu cầu quan trọng cho hệ thống đám mây. Công việc này chủ yếu liên quan tới hai nhóm yêu cầu:

– Phát hiện và phòng chống sự thâm nhập trái phép vào trung tâm dữ liệu, các thiết bị phần cứng.

– Bảo vệ hệ thống khỏi các thảm họa tự nhiên.

Yêu cầu bảo mật với các thành phần hệ thống

Quản lý định danh: Quản lý định danh là chìa khóa của việc đảm bảo ATBM của hệ thống. Thông tin về định danh phải chính xác và sẵn sàng cho các thành phần khác của hệ thống. Những yêu cầu cho thành phần này bao gồm:

– Phải có cơ chế kiểm soát để đảm bảo tính bí mật, tính toàn vẹn và tính sẵn dùng của thông tin định danh.

– Phân hệ quản lý định danh cũng phải được sử dụng cho mục đính chứng thực người dùng của hệ thống đám mây (thường với tải yêu cầu cao).

– Cân nhắc cơ chế sử dụng hoặc tương tác với các hệ thống quản lý định danh của bên thứ ba.

– Kiểm tra định danh của người sử dụng khi đăng ký khớp các yêu cầu của pháp luật.

– Lưu thông tin định danh của người sử dụng, kể cả khi họ rút khỏi hệ thống, phục vụ cho công tác kiểm tra, báo cáo (với các cơ quan pháp luật).

– Khi một định danh được xóa bỏ, sau đó tái sử dụng, cần đảm bảo người sử dụng mới không thể truy cập vào các thông tin của định danh trước đó.

Quản lý truy cập. Quản lý truy cập là thành phần sử dụng thông tin định danh để cho phép và đặt ràng buộc với các truy cập dịch vụ đám mây. Các yêu cầu liên quan tới quản lý truy cập bao gồm:

– Quản trị viên của đám mây chỉ có quyền truy cập hạn chế tới dữ liệu của khách hàng. Quyền truy cập này phải được ràng buộc chặt chẽ và được công bố rõ ràng trong hợp đồng sử dụng dịch vụ (SLA).

– Cần có cơ chế chứng thực nhiều bước cho những thao tác yêu cầu mức ưu tiên cao. Cần có cơ chế xác quyền đủ mạnh để đảm bảo các thao tác này không ảnh hưởng trên toàn đám mây.

– Không cho phép chia sẻ một số tài khoản đặc biệt (ví dụ tài khoản root), thay vì vậy, sử dụng các cơ chế khác như sudo.

– Cài đặt các cơ chế như LPP (least privilege principal) khi gán quyền truy nhập hay RBAC (role-based access control) để thiết lập các ràng buộc truy nhập.

– Thiết lập danh sách trắng (white list) về IP cho các quản trị viên.

Quản lý khóa. Trong đám mây, việc mã hóa dữ liệu là phương tiện chính để đảm bảo an toàn thông tin. Quản lý khóa là phân hệ phục vụ công tác lưu trữ và quản lý khóa cho việc mã hóa và giải mã dữ liệu của người sử dụng. Yêu cầu chính cho phân hệ này là:

– Có cơ chế kiểm soát và giới hạn các truy cập vào khóa.

– Với mô hình đám mây có cơ sở hạ tầng trên nhiều trung tâm dữ liệu, cần đảm bảo việc hủy bỏ khóa phải có hiệu lực tức thì trên các trạm.

– Đảm bảo việc khôi phục cho các khóa khi có lỗi.

– Mã hóa dữ liệu và máy ảo khi cần thiết.

Ghi nhận sự kiện và thống kê. Các sự kiện liên quan tới an toàn bảo mật của mạng và hệ thống cần được ghi nhận (logs) và thống kê cho nhu cầu kiểm tra, đánh giá. Những yêu cầu chính cho phân hệ này là:

– Ghi nhận sự kiện ở nhiều mức: từ các thành phần hạ tầng vật lý như máy chủ vật lý, mạng vật lý, tới những thành phần ảo hóa như máy ảo, mạng ảo.

– Các sự kiện được ghi nhận với đầy đủ thông tin để phân tích: thời gian, hệ thống, người dùng truy cập,...

– Các sự kiện cần được ghi nhận gần tức thời.

– Thông tin ghi nhận cần liên tục và tập trung.

– Thông tin ghi nhận cần được duy trì cho tới khi chúng không còn cần thiết.

– Thông tin ghi nhận được có thể được cung cấp tới khách hàng như một dạng dịch vụ.

– Tất cả các thao tác ghi nhận đều phải đảm bảo tính bí mật, nhất quán và sẵn sàng của thông tin ghi nhận được.

Giám sát bảo mật. Giám sát bảo mật là phân hệ liên quan tới việc khai thác các thông tin ghi nhận (logs), thông tin giám sát mạng hay thông tin bảo mật từ hệ thống giám sát vật lý. Yêu cầu cho phân hệ này bao gồm:

– Là dạng dịch vụ có tính sẵn sàng cao, có thể truy cập cục bộ hoặc từ xa trên một kênh bảo mật.

– Bao gồm một số chức năng chính:

+ Cảnh báo sự cố bảo mật dựa trên phân tích tự động các thông tin thu thập được.

+ Gửi cảnh báo bằng nhiều phương tiện như email, sms.

+ Cho phép người quản trị khai thác và phát hiện nguyên nhân của các sự cố.

+ Có cơ chế phát hiện xâm nhập hoặc bất thường của hệ thống.

+ Cho phép khách hàng có thể tự xây dựng cơ chế cảnh báo khi sử dụng PaaS hoặc IaaS.

Quản lý sự cố. Quản lý sự cố và phản ứng khi có sự cố là công tác quan trọng với bảo mật hệ thống. Các yêu cầu cho công tác này bao gồm:

– Có quy trình đầy đủ cho việc phát hiện, ghi nhận và xử lý sự cố.

– Có các cơ chế hỗ trợ người sử dụng thông báo về sự cố.

– Việc kiểm tra sự cố cần được thực hiện thường xuyên.

Kiểm tra an toàn và vá lỗi. Đây là công tác được thực hiện mỗi khi triển khai hoặc nâng cấp một dịch vụ mới. Các yêu cầu cho công việc này bao gồm:

– Có môi trường cô lập để phát triển, kiểm tra và điều chỉnh trước khi đưa dịch vụ vào sử dụng.

– Có quy trình vá lỗi cho các thành phần của hệ thống.

– Theo dõi thường xuyên các lỗ hổng bảo mật.

Kiểm soát mạng và hệ thống. Hệ thống kiểm soát mạng và các máy chủ được áp dụng cho cả các hạ tầng vật lý và hạ tầng ảo. Các yêu cầu cho hệ thống này bao gồm:

– Đảm bảo khả năng cô lập, khả năng cấu hình và tính bảo mật cho các thành phần bảo mật.

– Đảm bảo khả năng cô lập về mạng cho các vùng chức năng của hệ thống đám mây.

– Phân tách truy nhập thiết bị vật lý với thiết bị ảo.

– Phân tách vùng thiết bị ảo của các khách hàng khác nhau.

– Đảm bảo tính nhất quán của máy ảo, hệ điều hành,... cho ứng dụng của khách hàng.

Quản lý cấu hình. Trong một hệ thống đám mây với hạ tầng linh động, việc duy trì một danh sách thông tin về các tài nguyên của hệ thống và cấu hình của chúng là cần thiết. Các yêu cầu cho công tác này bao gồm:

– Sử dụng một hệ thống cơ sở dữ liệu cấu hình CMDB.

– Phân loại các tài nguyên theo chức năng, tính nhạy cảm, độ quan trọng,...

Các yêu tố kiến trúc và mẫu bảo mật

Phòng ngự chiều sâu (defence in-depth). Thuật ngữ phòng ngự chiều sâu lần đầu tiên được đề cập đến trong lĩnh vực an ninh mạng và máy tính là trong bài báo "Information warfare and dynamic information defence" vào năm 1996. Tiếp cận này trước đó được gọi bằng nhiều tên trong đó có "phòng ngự theo lớp" (layered defence). Tư tưởng chung của tiếp cận này là sử dụng nhiều tầng kiểm soát bảo mật để tạo nên một giải pháp đầy đủ, hoàn chỉnh hơn.

Trên quan điểm kiến trúc, kỹ thuật phòng ngự theo chiều sâu có thể được xem như một mẫu thiết kế hiệu quả cho vấn đề bảo mật. Ứng dụng của mẫu này có thể thấy ở nhiều hệ thống thực tiễn. Ví dụ như phòng ngự chiều sâu cho phân hệ kiểm soát truy nhập bao gồm nhiều lớp: lớp 1 – mạng riêng ảo (VPN); lớp 2 – bộ định tuyến cổng vào với cơ chế lọc IP; lớp 3 – token bảo mật.

Hũ mật ong (honeypots). "Hũ mật ong" là một kỹ thuật bẫy nổi tiếng. Trong một hệ thống mạng doanh nghiệp, "hũ mật ong" tạo nên một hệ thống không tồn tại hoặc không có giá trị nhằm thu hút sự tấn công. Khi đã thu hút thành công, "hũ mật ong" lại được sử dụng để quan sát, phân tích và cảnh báo. Dù thế nào thì kỹ thuật này cũng khiến cho bên tấn công tiêu phí thời gian và sức lực.

Hộp cát (sandbox). Hộp cát (sandbox) là một lớp trừu tượng nằm giữa phần mềm với hệ điều hành nhằm tạo môi trường độc lập cho việc thực thi ứng dụng. Tác dụng của hộp cát cũng giống như hypervisor trong việc cung cấp các máy ảo. Với hộp cát, hệ thống có thêm một tầng bảo vệ theo mô hình phòng ngự chiều sâu.

Cô lập máy ảo. Hạ tầng chuyển mạch trong một hệ thống đám mây không thể cô lập được các gói tin truyền thông giữa các máy ảo nằm trên cùng một môi trường phần cứng. Do vậy, nếu các gói tin không được mã hóa, máy ảo có thể theo dõi, quan sát các gói tin gửi đến/gửi đi từ máy ảo khác trong cùng một mạng. Cô lập máy ảo là kỹ thuật:

– Ứng dụng công nghệ ảo hóa để cô lập các máy ảo trong cùng một mạng vật lý;

– Mã hóa các gói tin gửi đến/gửi đi từ máy ảo;

– Kiểm soát truy cập đến máy ảo, đặc biệt là các cổng dịch vụ;

– Lọc gói tin đến máy ảo qua các cơ chế tường lửa.

Tạo dư thừa và đảm bảo tính sẵn sàng. Một trong những mẫu thiết kế thường được ứng dụng rộng rãi trong việc đảm bảo tính sẵn sàng cao của dịch vụ, trong đó bao gồm cả các dịch vụ bảo mật như quản lý định danh, quản lý truy cập,... là tạo dư thừa cho những thành phần hệ thống, bao gồm máy chủ, thiết bị mạng,... Tùy thuộc vào mức độ đảm bảo tính sẵn sàng mà kiến trúc có thể thiết lập dư thừa tương ứng. Tuy nhiên, cần lưu ý rằng sự dư thừa bao giờ cũng kéo theo những hệ quả như: tăng chi phí, tăng độ phức tạp của hệ thống.

Nội dung mục này giới thiệu một số kiến trúc đám mây điển hình, trong đó có bao hàm các thành phần đảm bảo tính an toàn và bảo mật.

Kiến trúc đám mây cung cấp dịch vụ PaaS (dịch vụ định danh, dịch vụ cơ sở dữ liệu)

Hình 3.4 giới thiệu kiến trúc một hệ thống đám mây cung cấp các dịch vụ PaaS (dịch vụ định danh, dịch vụ cơ sở dữ liệu).

Trong kiến trúc này, người sử dụng thông thường truy nhập vào dịch vụ của hệ thống thông qua mạng công cộng. Bên cạnh đó, hệ thống cũng cung cấp một mạng riêng biệt – mạng OOB (out-of-band) nhằm phục vụ công tác quản trị. Việc kiểm soát truy nhập vào mạng OOB này có thể được thực hiện thông qua một danh sách IP trắng – IP của các quản trị viên hệ thống. Thêm vào đó, quản trị viên cần thực hiện xác thực mỗi khi thao tác. Cơ chế xác thực hai bước (token và pin) có thể giúp hệ thống trở nên an toàn. Đây cũng là ví dụ về việc áp dụng cơ chế phòng ngự chiều sâu.

Hệ thống mạng cục bộ chia làm ba mạng chính:

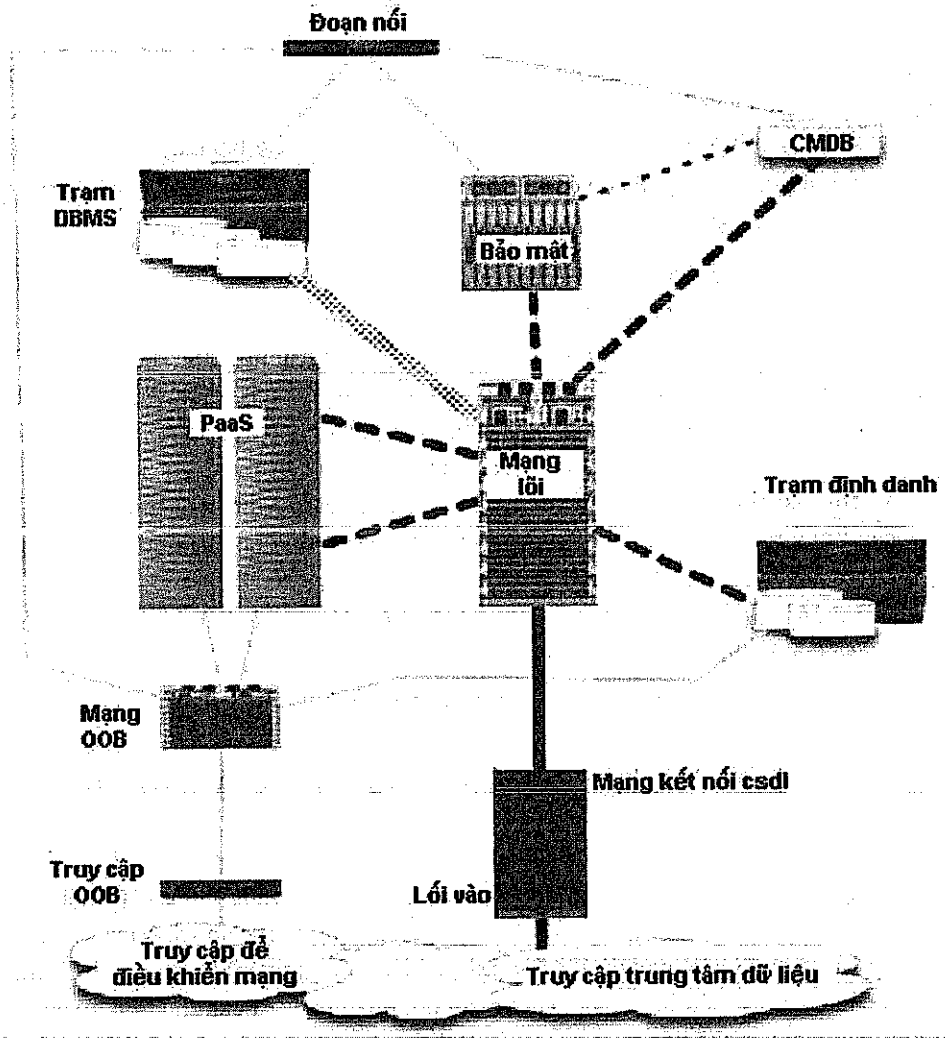
– Mạng OOB: sử dụng để quản trị các thành phần khác trong hệ thống.

– Mạng lõi: sử dụng để cung cấp dịch vụ.

– Mạng kết nối với cơ sở dữ liệu: bao gồm nhiều kết nối đảm bảo tính sẵn sàng.

Các thành phần của hệ thống cũng được thiết kế để cô lập các dịch vụ khác nhau của hệ thống như dịch vụ cơ sở dữ liệu và dịch vụ định danh. Một thành phần quản trị cấu hình (CMDB) cũng được đưa vào trong kiến trúc nhằm quản lý cấu hình các tài nguyên cung cấp bởi hệ thống.

Một số kiến trúc đám mây điển hình đáp ứng yêu cầu an toàn và bảo mật

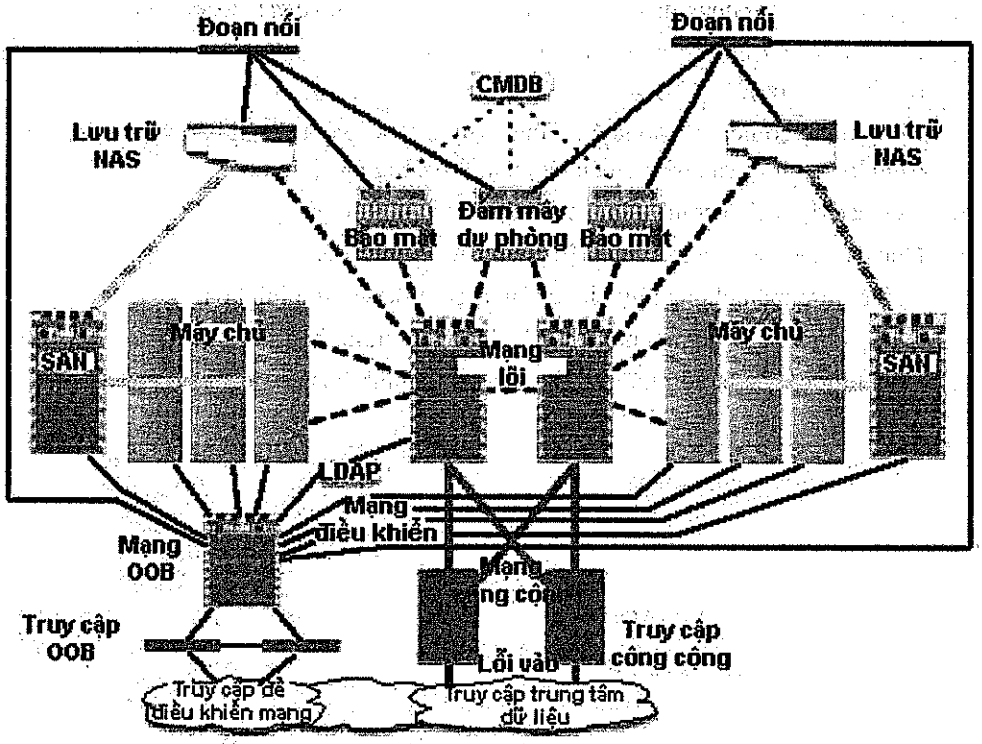


Hình 3.4. Kiến trúc đám mây cung cấp dịch vụ định danh và dịch vụ cơ sở dữ liệu

Kiến trúc đám mây cung cấp kho lưu trữ và dịch vụ tính toán

Hình 3.5 minh họa một ví dụ khác về kiến trúc đám mây với các loại hình dịch vụ cung cấp là dịch vụ tính toán và dịch vụ lưu trữ dữ liệu. Trong kiến trúc này, hệ thống đám mây cung cấp một số lượng lớn tài nguyên tính toán được ảo hóa trên các máy chủ, cũng như các kho lưu trữ trên các thiết bị SAN. Hơn nữa, kiến trúc này hỗ trợ tính sẵn sàng cao cho người sử dụng thông qua việc tạo lập dư thừa cho mạng kết nối công cộng và mạng OOB. Để đảm bảo tính sẵn sàng cho việc truy nhập vào kho lưu trữ SAN, mạng SAN được thiết lập với các kết nối giữa kho lưu trữ SAN và các máy chủ tính toán.

Để đảm bảo tính sẵn sàng cao, bản thân các máy chủ và kho lưu trữ SAN cũng được thiết kế dư thừa. Ở đây chúng ta có thể áp dụng một số chiến lược khác nhau để cân đối giữa chi phí đầu tư và tính sẵn sàng của hệ thống.



Hình 3.5. Kiến trúc đám mây cung cấp dịch vụ tính toán và lưu trữ

Với các tài nguyên tính toán, để đảm bảo khả năng đáp ứng tốt cho dịch vụ, hệ thống cần có những thiết kế cho việc dành sẵn tài nguyên (provision). Các máy chủ phục vụ cho việc này được thiết kế độc lập. Việc dành sẵn tài nguyên này cũng đòi hỏi sự kiểm soát và quản lý của một phân hệ quản lý cấu hình tài nguyên CMDB. Kết nối trên sơ đồ đã thể hiện điều này.

Một điểm đặc biệt khác trong sơ đồ kiến trúc của hình là hai phân hệ bảo mật được thiết kế theo mẫu dư thừa. Các phân hệ này cung cấp những dịch vụ bảo mật như:

– Jumphost và VPN: cho phép tạo lập các mạng riêng ảo và cho phép các quản trị viên có thể truy nhập trực tiếp vào các máy chủ cần quản lý.

– Trung tâm điều hành bảo mật: cho phép giám sát các vấn đề liên quan tới an toàn bảo mật, quét các lỗi bảo mật của hệ thống, phân tích nguyên nhân và báo cáo.

– Ghi nhật ký về các sự kiện của hệ thống và cảnh báo nếu có.

– Giám sát thông tin mạng (quét lỗ hổng, giám sát băng thông mạng, ...)

Có thể nói thành phần bảo mật này là công cụ giám sát bảo mật chính của các quản trị viên trong hệ thống đám mây.

3.4. CÂU HỎI VÀ BÀI TẬP

1. Tại sao người sử dụng dịch vụ đám mây thường lo ngại về vấn đề an toàn – bảo mật?
2. Hãy trình bày những nguy cơ về an toàn bảo mật trong mô hình đa người thuê (multi-tenancy)?
3. Công nghệ ảo hóa có tạo nên những nguy cơ mới về an toàn bảo mật không? Hãy trình bày những vấn đề an toàn bảo mật với công nghệ ảo hóa.
4. Nêu các đặc điểm chính của biện pháp bảo mật mức vật lý.
5. Nêu các đặc điểm chính của biện pháp bảo mật dữ liệu.
6. Chiến lược/mẫu phòng ngự chiều sâu là gì? Cho ví dụ minh họa.
7. Chiến lược/mẫu "hũ mật ong" là gì? Cho ví dụ minh họa.
8. Chiến lược/mẫu tạo dư thừa là gì? Cho ví dụ minh họa.

Chương 4
SỬ DỤNG DỊCH VỤ

Nền tảng là dịch vụ (PaaS) là dạng điện toán đám mây thường bị nhầm lẫn với Cơ sở hạ tầng là dịch vụ hoặc Phần mềm là dịch vụ. PaaS cho phép các nhà phát triển xây dựng và triển khai các ứng dụng web trên một cơ sở hạ tầng lưu trữ trên máy chủ. Nói cách khác, PaaS cho phép tận dụng tài nguyên tính toán dường như vô hạn của một cơ sở hạ tầng đám mây. Điều này có được là do tính chất co dãn của nền tảng đám mây dành cho PaaS, nó có thể mở rộng khi cần thiết để cung cấp tài nguyên máy tính nhiều hơn. Xu hướng phát triển và triển khai các dịch vụ dựa vào PaaS trên các đám mây hiện nay đang gặp phải những thách thức to lớn. Hầu hết các đám mây PaaS hiện đang giới hạn vào một nền tảng cụ thể cũng như các giao diện lập trình ứng dụng (Application Programming Interface –API) của chúng. Đám mây PaaS cung cấp nền tảng để lưu trữ và API để lập trình các ứng dụng này. Nền tảng PaaS cũng quản lý các hoạt động của ứng dụng và hỗ trợ một vài tính năng như tự động mở rộng tài nguyên cho dịch vụ,... Đối với các ứng dụng có sẵn, người lập trình sẽ phải viết lại chương trình cho phù hợp với các API cung cấp bởi PaaS, việc này đòi hỏi thời gian, tiền bạc và công sức rất lớn khiến nó trở thành mối e ngại thực sự trong quyết định chuyển ứng dụng lên đám mây. Ngoài khó khăn về mặt công nghệ, còn có những khó khăn về mặt kinh tế khi các dịch vụ PaaS nổi tiếng hiện nay như Google App Engine, Azure, Amazon Web Services đều thu phí hoặc miễn phí với nhiều giới hạn và ngay khi người dùng sử dụng tài nguyên vượt qua giới hạn thì sẽ bị tính phí.

Chương này sẽ trình bày ba nội dung chính: Giới thiệu một số dịch vụ phần mềm IaaS điển hình trong môi trường đám mây; Giới thiệu Windows Azure, một trong những dịch vụ nền tảng PaaS giúp các nhà phát triển phần mềm trên đám mây; Giới thiệu một số dịch vụ hạ tầng trong môi trường đám mây.

4.1. SỬ DỤNG DỊCH VỤ PHẦN MỀM

Hiện nay, với số lượng ngày càng nhiều các công ty triển khai các dịch vụ phần mềm lên đám mây, thật khó có thể kể ra hết các loại hình dịch vụ của điện toán đám mây cũng như những lợi ích mà chúng đem lại cho người dùng cá nhân.

Việc sử dụng các dịch vụ điện toán đám mây cũng đồng nghĩa với việc dữ liệu của bạn được lưu trên các hệ thống đĩa cứng lớn trong các máy chủ khổng lồ được kết

nối với mạng Internet. Bên cạnh đó, điều đó còn là việc có thể sử dụng các ứng dụng nền web và truy cập chúng qua mạng – bất kể từ máy tính cá nhân, máy tính bảng hay thậm chí là điện thoại di động. Bạn có thể nhanh chóng làm việc cho dù đang ngồi ở máy mình hay hệ thống lạ, truy cập dữ liệu từ bất kỳ đâu và sử dụng nhiều dịch vụ hấp dẫn khác. Các tác vụ bảo trì hệ thống, bảo mật... thậm chí có thể giao trọn cho nhà cung cấp dịch vụ điện toán đám mây nếu muốn.

Sử dụng "đám mây" sẽ cho phép bạn có kho lưu trữ dữ liệu trực tuyến và khả năng truy cập nhiều dịch vụ để đáp ứng nhu cầu riêng. Một ví dụ quen thuộc là Dropbox – công cụ lưu trữ trực tuyến cho phép mọi người dùng mới đăng ký có 2 GB khoảng trống. Các dịch vụ khác như Amazon mặc định cho 5 GB rộng rãi hơn. Bên cạnh lưu trữ, các dịch vụ như Google còn cho phép tạo tài liệu, các bảng tính, lịch... và sử dụng nhiều công cụ văn phòng hữu ích một cách miễn phí. Trong khi đó, Spotify lại là dịch vụ lưu nhạc trực tuyến với hàng triệu bài hát cho phép sử dụng miễn phí thời gian đầu.

Khả năng truy cập dữ liệu ở mọi nơi đồng thời cho phép bạn tiếp tục công việc đúng ở chỗ trước đó dừng lại, điều này là một lợi thế lớn trong công việc. Hiện nay, những dịch vụ như iCloud của Apple đã cho phép đồng bộ các thiết bị cùng lúc bất cứ khi nào người dùng cập nhật nội dung của các tập tin. Như thế, dù là sử dụng thiết bị nào, bạn cũng có thể truy cập ngay tới cùng một tập tin dữ liệu. Dĩ nhiên, với các dịch vụ miễn phí kiểu như thế, cái giá phải trả chính là độ "riêng tư" của dữ liệu.

Thực tế, điện toán đám mây là giải pháp giúp tiết kiệm đáng kể chi phí trong khi vẫn tận dụng được những tính năng hiện đại nhất. Những khía cạnh "tiết kiệm" có thể đạt được như năng lượng vận hành máy chủ, chi phí cho bản quyền phần mềm... khi người dùng chuyển từ việc sử dụng phần mềm email riêng (kiểu như Outlook) sang mail trên web, đưa cơ chế phòng virus sang dạng trực tuyến, sử dụng các dịch vụ lưu trữ đám mây thay cho máy chủ riêng. Việc tận dụng tối đa các dịch vụ đám mây sẽ cho phép bạn tiết kiệm đáng kể chi phí.

Với số lượng ngày càng nhiều các công ty triển khai các dịch vụ phần mềm lên đám mây, thật khó có thể kể ra hết các loại hình dịch vụ của điện toán đám mây hay các nhà cung cấp SaaS cho người dùng cá nhân. Có thể trong tương lai không xa, các phần mềm cơ bản của người dùng sẽ được đưa hết lên đám mây.

Những nhà sản xuất điện thoại/máy tính bảng lớn như Apple, Samsung, HTC,... đều đưa ra các dịch vụ đám mây của riêng mình để phục vụ khách hàng lưu trữ dữ liệu, đồng bộ hóa dữ liệu, danh bạ, đa phương tiện,...

Về lưu trữ dữ liệu, hiện có rất nhiều nhà cung cấp dịch vụ này, ngoài những dịch vụ gắn liền với thiết bị điện tử như điện thoại hay máy tính bảng. Google có Google Drive. Các hãng khác như Dropbox, Sharefile, Egnyte,...

Những phần mềm văn phòng trước đây là lãnh địa riêng của Microsoft với bộ Microsoft Office thì nay cũng đã phải chia sẻ thị phần với những dịch vụ trên đám mây như Google Docs hay Zoho.

Ngay cả những phần mềm chuyên dụng trước đây như phần mềm chỉnh sửa ảnh, thì nay cũng có thể tìm thấy dịch vụ tương ứng trên đám mây như Picasa của Google. Hoặc thậm chí chính công ty từng rất thành công với phần mềm chỉnh sửa ảnh Photoshop cũng đưa dịch vụ tương ứng lên đám mây là Adope Photoshop Express. Thậm chí những phần mềm đòi hỏi máy tính cấu hình mạnh để làm phim, xuất ảnh cỡ lớn cũng đã được đưa lên đám mây để tận dụng sức mạnh tính toán khổng lồ của nó như Blender 3D.

Danh sách những nhà cung cấp SaaS còn rất dài, trong đó có những cái tên rất quen thuộc với người dùng mạng như: Linkedin, Flickr, Yahoo, Facebook,... Từ những phần mềm cơ bản cho đến những phần mềm chuyên dụng, chưa kể đến những phần mềm dành riêng cho doanh nghiệp, tổ chức, tất cả đều đã và đang được đưa dần lên đám mây.

Các tiểu mục sau đây sẽ giới thiệu những lợi ích của các dịch vụ đám mây và một số dịch vụ đám mây tiêu biểu.

Các lợi ích của các dịch vụ đám mây

Cải tiến quy trình: Với những công ty SME, với sự xuất hiện của SaaS, những hệ thống như CRM, Helpdesk mới trở nên "vừa túi tiền" và trong tầm với của doanh nghiệp. Từ đó việc đưa hệ thống IT vào để cải tiến hoạt động kinh doanh hiện tại trở nên dễ dàng và tiện lợi hơn nhiều. Tất nhiên, giữa việc phải dùng Excel để lưu trữ danh sách khách hàng và dễ bị sai sót với một hệ thống CRM hoàn chỉnh và hàng loạt chức năng tuyệt vời thì quả thật doanh nghiệp như được "lắp thêm cánh".

Tự động hóa: Có nhiều hoạt động trước đây phải làm thủ công, nay với sự giúp sức của IT thì có thể tự động hóa, tiết kiệm chi phí cũng như tăng hiệu quả.

Tập trung vào công việc đem lại giá trị lớn nhất: Bởi vì hệ thống IT gần như được "out-source" và lo lắng đầy đủ, công ty bây giờ hoàn toàn có thể tinh gọn và chỉ tập trung vào những nhân sự đúng lĩnh vực kinh doanh của mình, đem lại giá trị lớn nhất cho doanh nghiệp.

Thống nhất dữ liệu: Bởi vì toàn bộ thông tin dữ liệu đều được lưu trữ tại một chỗ (và được truy cập bởi nhiều nhân viên, theo nhiều cách khác nhau), cho nên bạn có thể "consolidate" thông tin của mình và không phải lo lắng dữ liệu của mình ở chỗ này một tí, chỗ kia một tí, hoặc khi có nhân viên nghỉ thì không biết làm sao lấy lại dữ liệu mà nhân viên đó đang giữ.

Chi phí đầu tư thấp: Thay vì phải đầu tư vài trăm triệu để có một phần mềm hoàn chỉnh, bạn có thể chia nhỏ ra và trả theo tháng (thông thường chi phí mỗi tháng tính theo mức độ sử dụng, hoặc số lượng nhân viên, hoặc số lượng khách hàng,...). Vì vậy, với SaaS, gần như bạn có thể bắt đầu sử dụng bất kỳ lúc nào thay vì phải đợi có đủ tiền.

Phân tích thông tin doanh nghiệp (Business Intelligence): Vì khi mọi dữ liệu, thông tin liên quan đến hoạt động của công ty đều được ghi lại thì bước tiếp theo sẽ là những phần mềm/hệ thống giúp phân tích những thông tin này và đem lại cho doanh nghiệp những hiểu biết thấu đáo về chính hoạt động kinh doanh của mình. Ví dụ: trước đây doanh nghiệp chỉ có thể nắm doanh thu, lợi nhuận,... hằng năm, hằng quý, hằng tháng; nhưng nếu có thêm hệ thống CRM thì doanh nghiệp biết được mình có bao nhiêu khách hàng, trong những phân khúc nào, bao nhiêu % khách hàng thân thiết thường hay mua sản phẩm, bao nhiêu % khách hàng giới thiệu bạn bè người thân đến mua,... và hàng loạt những "insight" bổ ích khác.

Ở trên là vài lợi ích lớn nhất, ngoài ra còn hàng loạt lợi ích khác và còn tùy theo dịch vụ SaaS là gì sẽ có những lợi ích khác nhau.

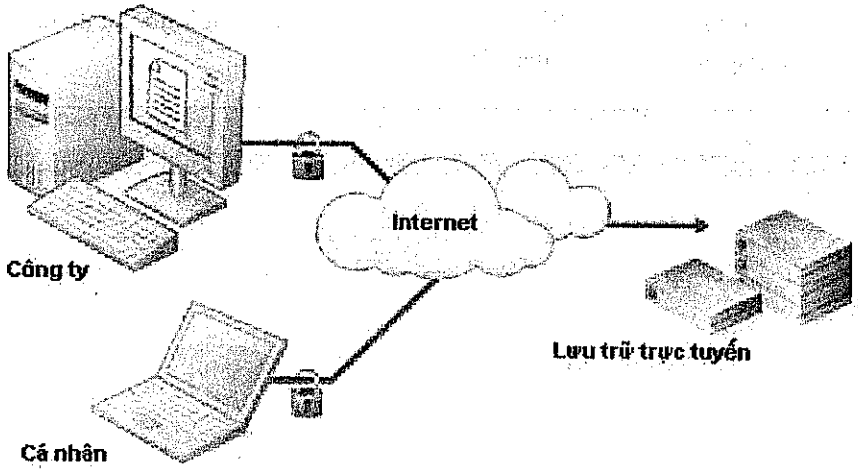
Ứng dụng Google Apps

Google Apps là một dịch vụ từ Google dùng cho việc kết hợp tên miền của cá nhân với các sản phẩm của Google. Các tính năng của nó bao gồm các ứng dụng Web tương tự với bộ office, như Gmail, Google Calendar, Google Talk, Google Docs và Google Sites. Google Apps được xây dựng trên nền tảng điện toán đám mây, cho phép người dùng sử dụng các ứng dụng trực tuyến từ bất cứ đâu có kết nối Internet. Ngoài các ứng dụng có sẵn nêu trên, Google Apps còn cho phép người dụng tích hợp các ứng dụng từ bên thứ ba tại Google Apps Marketplace. Google Apps được cho là bộ sản phẩm cạnh tranh với bộ sản phẩm Microsoft Office của Microsoft.

Gmail, hay còn gọi là Google Mail ở Đức và Anh là một dịch vụ e-mail trên nền web và e-mail POP3 miễn phí do Google cung cấp. Bản beta được đưa vào hoạt động vào ngày 01 tháng 4 năm 2004, với hình thức chỉ dành cho thư mời và được mở rộng thành bản beta cho tất cả mọi người vào tháng 2 năm 2007.

Gmail hỗ trợ POP3 và hơn 7.0 Gigabyte không gian lưu trữ, một công cụ tìm kiếm và đàm thoại trực tuyến hoặc chat, khả năng bảo mật tốt và cảnh báo virus. Gmail nổi tiếng với việc sử dụng công nghệ Ajax trong thiết kế. Gmail hỗ trợ nhiều trình duyệt (browser) và hỗ trợ đa ngôn ngữ (multi languages), địa chỉ người gửi đến và người gửi đi tự động nhập lưu vào sổ. Năm 2005, Gmail là sản phẩm đứng thứ hai sau Mozilla Firefox trong 100 sản phẩm tốt nhất được tạp chí PC World bình chọn.

Google Docs là bộ tổ hợp các công cụ xử lý dữ liệu văn bản và trình chiếu, bao gồm: Document, Drawing, Presentation, Spreadsheet và Form. Bất kỳ văn bản tài liệu hoặc trình chiếu nào được tạo bằng Google Docs (hoặc chuyển định dạng thành Doc) đều được lưu trữ trên hệ thống máy chủ của Google bằng tài khoản của người sử dụng. Theo thông tin từ trang hỗ trợ của Google, hãng không giới hạn số lượng văn bản người sử dụng có thể làm việc với Google Docs (mặc dù vẫn còn tồn tại một số giới hạn nhất định). Bên cạnh đó, người dùng có thể lưu trữ tới 1 GB các định dạng dữ liệu chưa được chuyển đổi hoàn toàn miễn phí và lưu lượng thực sự Google hỗ trợ người dùng còn lên tới 10 GB (có bao gồm các dịch vụ trực tuyến có trả phí).



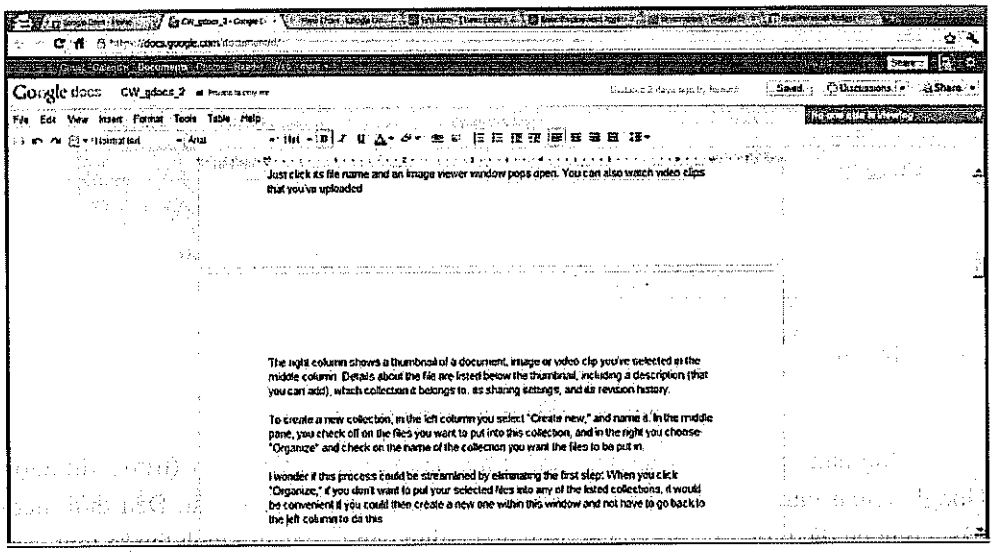
Hình 4.1. Ứng dụng Google Docs

Ứng dụng xử lý văn bản này được khởi đầu với cái tên Writely (trước khi được Google chính thức mua lại) và có toàn bộ các tính năng cơ bản nhất. Đến thời điểm này, công cụ đã được tích hợp nhiều tính năng định dạng, thay đổi kích thước font, căn lề, cách dòng, tạo mục lục, danh sách... tương tự như Microsoft Word. Ngoài ra, chúng ta còn có thể chèn thêm những đối tượng hỗ trợ vào văn bản như phần Header, Footer, bảng cũng như các công thức toán học, ảnh, video trình chiếu...

Bên cạnh đó, chức năng chuyển đổi định dạng của Google Docs cũng đã được cải thiện rất nhiều, hỗ trợ văn bản Microsoft Word, OpenOffice, rich text (RTF), HTML hoặc text đơn thuần (.txt). Ví dụ, một văn bản tài liệu Word sau khi được import có chứa nhiều thành phần ký tự toán học, đánh dấu... sẽ giữ nguyên những thành phần này. Chỉ có những phần ngoại lệ thay đổi mới được ghi lại thông tin, cụ thể là những đối tượng không được chuyển đổi sang định dạng phù hợp của Google Docs. Do vậy, tính năng này của Google cũng khác hẳn so với những chương trình xử lý văn bản hiện nay. Mặt khác, chúng ta có thể trích xuất định dạng chuẩn của văn bản thành những file phổ biến khác như RTF, ODT, Word hoặc HTML. Ngoài ra, Google Docs còn hỗ trợ người dùng bằng công nghệ OCR – Optical Character Recognition (nhận dạng ký tự qua hình ảnh) giúp chuyển các file PDF hoặc ảnh (JPG, GIF và PNG)... mà họ đăng tải lên thành file văn bản có thể chỉnh sửa được. Tính năng này hoạt động rất ổn định và vô cùng hiệu quả, vì toàn bộ nội dung text trong file PDF hoặc các bức ảnh được hiển thị rất rõ ràng.

Một công cụ hỗ trợ chuyển đổi khác vô cùng tiện lợi ở đây là ngôn ngữ (hệ thống Google Docs hỗ trợ tới hơn 50 ngôn ngữ phổ biến khác nhau) và lưu trữ văn bản đã được dịch thành file Google Docs trực tiếp trên tài khoản, còn file gốc của người dùng vẫn được giữ nguyên. Các văn bản tại đây luôn được áp dụng và xử lý dựa trên tính năng kiểm tra real – time, các từ ngữ sai chính tả được đánh dấu gạch chân bằng

những dấu chấm màu đỏ, khi nhấn chuột phải vào những từ ngữ đó, hệ thống sẽ hiển thị những phương án phù hợp để thay đổi.



Hình 4.2. Ứng dụng Google Docs

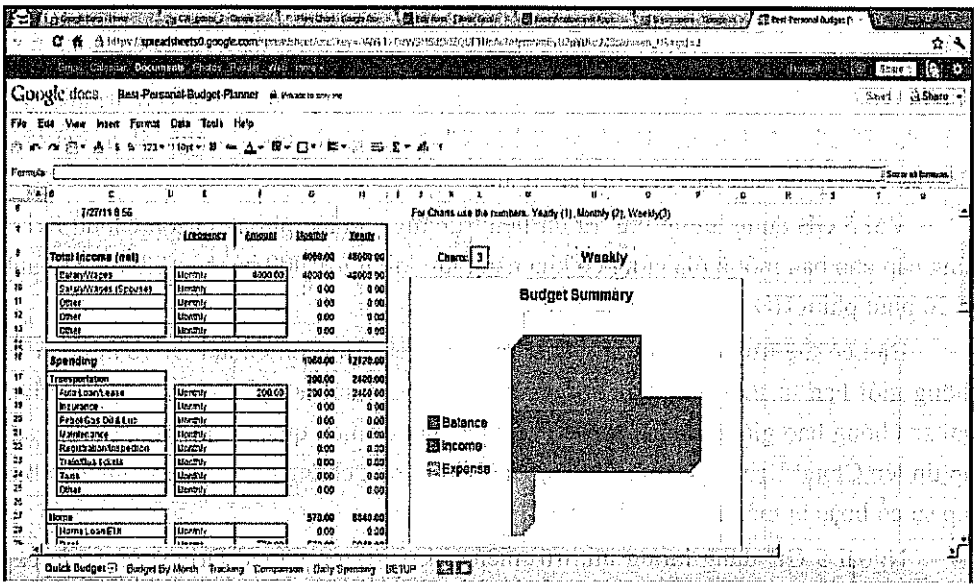
Tính năng được thay đổi gần đây nhất là Pagination – cho phép người dùng xem văn bản theo từng trang riêng biệt khác nhau. Tuy nhiên, chúng ta vẫn chưa thể chèn thêm (hoặc định dạng lại) số trang trong một văn bản, thay vào đó khi muốn in thì có thể thiết lập Google Docs in số trang này tại nhiều vị trí khác nhau như góc trên bên trái, giữa, phải, góc dưới bên trái, giữa và phải trên tất cả các trang.

Công cụ **Spreadsheet** của Google với chức năng tương tự như như ứng dụng Spreadsheet của OpenOffice, Excel của Microsoft Office. Về cụ thể, nó còn được tích hợp sẵn nhiều chức năng tính toán khác như kỹ thuật, tài chính, kế toán, thống kê, phân tích...

Trong năm 2010, các nhà phát triển Google Docs đã cải tiến một số chức năng khác như lọc dữ liệu và quan trọng hơn là PivotTable – nhanh chóng giúp người sử dụng trích xuất và liệt kê từng mảng dữ liệu trên bản báo cáo, bao gồm các bảng chứa và mối dữ liệu có liên quan... Bên cạnh đó, Spreadsheet còn có thể tạo biểu đồ dựa trên mô hình dữ liệu cụ thể của từng hệ thống, được phân chia rõ ràng theo hàng, cột, các mẫu biểu đồ, nhưng không được nhiều mẫu đa dạng như của OpenOffice hoặc Microsoft Excel.

Spreadsheet còn có cơ chế import hỗ trợ nhiều định dạng dữ liệu khác nhau, bao gồm: XLS và XLSX (Excel), ODS (OpenOffice), CSV, TXT, TSV và TAB. Nhưng về cơ chế hoạt động cụ thể, công cụ Spreadsheet của OpenOffice không import file dữ liệu

chuẩn xác theo cách thông thường, điển hình nhất là chế độ màu nền của các file văn bản thường xuyên bị mất. Bên cạnh đó, các công thức tính toán trong nhiều trang văn bản khác nhau bị sai lệch hoặc không hoạt động... Nhưng các bạn hãy yên tâm, vì Spreadsheet của Google Docs xử lý quá trình này chuẩn xác hơn nhiều so với OpenOffice.



Hình 4.3. Ứng dụng Google Spreadsheet

Mỗi một bảng tính trong Spreadsheet được hiển thị như 1 tab riêng biệt ở phía dưới của chương trình. Bởi vì đây là ứng dụng trực tuyến, cho nên quá trình chuyển tiếp giữa những thành phần này sẽ lâu hơn thông thường, khoảng 1 – 2 giây để hệ thống tải đủ dữ liệu cần thiết. Nếu không có đủ số dòng cần thiết trên một bảng tính, hãy kéo chuột xuống phía dưới và chọn chức năng Add để thêm, điền số dòng tại đây và nhấn Enter, hệ thống sẽ bổ sung đúng số dòng theo giá trị trong ô. Tuy nhiên, hiện tại Google vẫn chưa bổ sung chức năng tương tự để thêm số cột. Để chèn thêm nhiều dòng hoặc cột, các bạn hãy đánh dấu một vài dòng, cột, sau đó nhấn chuột phải để thêm số lượng.

Không giống như ứng dụng Drawing và Presentation, Spreadsheet không hỗ trợ tính năng phóng to hoặc thu nhỏ bản ghi (Document cũng không có tính năng này). Đây sẽ trở thành vấn đề khá nghiêm trọng khi chúng ta làm việc đối với những bản tính lớn. Mặt khác, người sử dụng còn có thể download file Spreadsheet với nhiều định dạng khác nhau, bao gồm XLS (Excel), ODS (OpenOffice), PDF, CSV, HTML hoặc TXT.

Ngoài ra trong bộ Google App Suits còn có những phần mềm như: Presentation (trình diễn), Drawing (vẽ),... Phiên bản cho các hệ điều hành di động như Android, iOS cũng có những phần mềm tương ứng. Tất cả đều được đồng bộ trên đám mây của Google.

Ứng dụng Amazon Apps

Có chức năng gần tương đồng với Dropbox, CX hay SpiderOak, Amazon Cloud Drive là một "ổ đĩa cứng trên mây" của bạn, giúp bạn lưu trữ âm thanh, video, hình ảnh và tài liệu lên máy chủ an toàn của Amazon. Tất cả những gì bạn cần là một trình duyệt web như Firefox 4, Internet Explorer 9 hay Chrome 11 để update, download và truy cập vào các tập tin của bạn từ mọi máy tính.

Với 5 GB dung lượng lưu trữ dữ liệu trực tuyến miễn phí, Amazon Cloud Drive cung cấp cho bạn một ổ đĩa cứng có khả năng lưu lại hơn 1.000 bài hát, 2.000 hình ảnh và 20 phút phim HD.

Bạn có thể truy cập vào dữ liệu được lưu trên Amazon Cloud Drive an toàn và không giới hạn từ mọi máy tính. Ngoài ra, bằng việc sử dụng Amazon Cloud Drive, bạn sẽ không bao giờ còn phải lo lắng về việc mất dữ liệu quan trọng nữa, lưu lại các tập tin lên Cloud Drive và bạn sẽ không bao giờ bị mất chúng cho dù máy tính của bạn gặp sự cố hoặc bị mất hoặc bị đánh cắp.

Ngoài 5 GB dung lượng lưu trữ miễn phí, Amazon Cloud Drive còn cung cấp cho bạn 6 gói lưu trữ trả phí khác bao gồm: 20 GB, 50 GB, 100 GB, 200 GB, 500 GB và 1000 GB.

Đặc biệt, nếu bạn mua bất kỳ một album nhạc có trong Amazon MP3 Store, bạn sẽ được miễn phí 20 GB dung lượng lưu trữ trong 1 năm tính từ ngày bạn đặt mua album và những bài hát có trong album này sẽ được lưu miễn phí trong Amazon Cloud Drive của bạn, có nghĩa là dung lượng còn lại của Amazon Cloud Drive sẽ không bị ảnh hưởng bởi dung lượng album nhạc mà bạn đã mua.

Các ứng dụng đám mây cho doanh nghiệp

Thường gặp nhất là các nhà cung cấp Hệ thống quản lý quan hệ khách hàng (Customer Relationship Management – CRM), hệ thống Email Marketing, hệ thống quản trị nội dung (Content Management System – CMS), hệ thống HelpDesk,... Thông thường những dịch vụ này sẽ được "nằm trên mây" (on the Cloud), tức là đưa vận hành và lưu trữ trực tiếp từ điện toán đám mây (Cloud Computing).

Ưu điểm lớn nhất của SaaS là mọi vấn đề phát sinh và gánh nặng kỹ thuật để phần mềm vận hành tốt đều sẽ do nhà cung cấp dịch vụ chịu trách nhiệm, từ việc đảm bảo hệ thống server chạy tốt, đến việc cập nhật thường xuyên, duy trì bảo mật,... Tức là

doanh nghiệp chỉ cần mua dịch vụ và sử dụng, không cần phải duy trì một bộ phận IT để lo như trước đây nữa. Một số nhà cung cấp SaaS:

Saleforces – là hệ thống CRM lớn nhất hiện giờ, ngoài ra còn có dịch vụ help desk, marketing,...

Mailchimp – là một trong những hệ thống Email Marketing phổ biến nhất hiện nay.

Desk.com – là hệ thống chăm sóc khách hàng (Helpdesk).

Trong nước có:

Biaki – cũng là hệ thống quản trị quan hệ khách hàng (CRM), có thể sử dụng cả trên máy tính và smartphone.

Misa – vừa có CRM, HRM (quản trị nguồn nhân lực), kế toán, chứng từ,...

Avoca – cũng là hệ thống quản lý quan hệ khách hàng CRM.

Dễ thấy là có rất nhiều nhà cung cấp dịch vụ CRM trên đám mây. Chúng ta hãy cùng xem xét dưới đây một ví dụ cụ thể về dịch vụ CRM cung cấp bởi công ty Oracle.

Oracle On–demand: Oracle là một trong những công ty hàng đầu thế giới trong việc cung cấp các giải pháp quản lý quản lý quan hệ khách hàng – CRM. Đặc biệt với phần mềm Oracle CRM On Demand cung cấp các khả năng rộng nhất và sâu nhất có thể để giúp các tổ chức ở tất các các mặt như bán hàng, tiếp thị, phân tích, quản lý quan hệ với đối tác, quản lý mối quan hệ với khách hàng... trong tất cả các lĩnh vực như bán hàng, tài chính ngân hàng, công nghiệp ôtô, dược phẩm, y tế...

– Oracle CRM On Demand Analytics (phân tích nhu cầu khách hàng): hỗ trợ lập các báo cáo một cách khá chính xác, đưa ra các quyết định kinh doanh dựa trên số dữ liệu thời gian thực. Với khả năng phân tích tương tác đầy đủ, Oracle CRM On Demand cho doanh nghiệp một cái nhìn sâu sắc và toàn diện về các hoạt động của mình. Với Oracle CRM On Demand, doanh nghiệp sẽ có được cái nhìn sâu sắc giúp nhanh chóng nhận diện một cách chính xác và kịp thời để có thể đáp ứng được với điều kiện thay đổi của thị trường. Bằng cách hợp thời gian thực, hành động kinh doanh thông minh có sẵn thông qua các biểu đồ tương tác, báo cáo tùy chỉnh và xu hướng phát triển cho phép doanh nghiệp khám phá những cơ hội mới và xác định các vấn đề trước khi chúng ảnh hưởng tới doanh nghiệp.

Các tính năng và lợi ích:

– Kinh doanh thông minh nhờ việc truy cập thời gian thực (Access real-time business intelligence).

– Phân tích lịch sử và xu hướng trong tương lai thông qua chức năng kho dữ liệu... (Create historical and trend analysis via high-powered data warehouse functionality).

– Đưa ra những phân tích với độ chính xác cao (Create powerful ad hoc analysis).

Giải pháp của Oracle cung cấp các tính năng như kênh bán hàng tự động, marketing, dịch vụ khách hàng và bao gồm tổng đài tích hợp cho phép các công ty quản lý thông tin liên lạc thông qua các kênh thông tin cố định và di động. Các tính năng quan trọng khác gồm khả năng tích hợp với Lotus Notes và Microsoft Outlook; hệ thống trả lời tương tác (interactive voice response – IVR) tích hợp với với hệ thống trung gian, đưa ra sự lựa chọn cho phép các công ty giữ lại thông tin về công ty của họ khi gửi đi các hướng dẫn hay khi theo dõi các dự án và bán hàng chung. Với việc sử dụng một giao diện thông dụng, các công ty có thể truy nhập vào các dữ liệu về lĩnh vực bán hàng, marketing và dịch vụ để tìm kiếm các chức năng, các bảng chỉ số và các báo cáo thông qua trình duyệt web. Tính năng chính của kênh bán hàng tự động bao gồm tính năng tạo ra các bản kê khai để việc quản lý lượng khách hàng lớn trở nên dễ dàng hơn. Một tính năng khác cho phép các công ty có thể theo dõi sự tương tác của khách hàng và lưu lại mọi số liệu về khách hàng. Tuy nhiên, điểm nổi bật thật sự trong phiên bản này là việc tổng đài đang sử dụng "Engine" (một phần của chương trình máy tính được thiết kế để thực hiện những nhiệm vụ riêng biệt) Telephonya Work's CallCenter Anywhere. Dịch vụ cung cấp VoIP (Voice over Internet Protocol) tích hợp và hướng cuộc gọi đến các số Off – Premise như điện thoại di động hay phòng làm việc ở nhà và các công cụ cho việc phát triển IVR và định hướng liên lạc.

Với On – Demand, các đại diện tổng đài được chỉ định theo khả năng của họ. Các nhà quản lý có thể giám sát lượng thông tin thu về và cung cấp hướng dẫn sử dụng các tính năng giám sát và ghi nhận, hướng dẫn ngoại tuyến (off-line) và hội đàm qua điện thoại.

4.2. SỬ DỤNG DỊCH VỤ NỀN TẢNG

Lợi ích của các mô hình nền tảng như dịch vụ PaaS đối với các công ty phát triển phần mềm bao gồm tiết kiệm chi phí, giảm bảo dưỡng kỹ thuật và tăng tính di động. Chi phí trả trước để mua máy chủ, phần cứng khác và giấy phép cho phần mềm cần thiết được loại bỏ. Với các máy chủ lưu trữ ngoại vi thì nhân viên hỗ trợ kỹ thuật cũng ít được yêu cầu. PaaS cũng cung cấp các công cụ đắt tiền nhưng chỉ sử dụng trong một thời gian ngắn trong quá trình phát triển phần mềm như là một phần của gói tổng thể PaaS, do đó cũng tiết kiệm được chi phí. Tính di động của nhân viên được tăng lên, vì tất cả mọi thứ có thể truy cập thông qua các công cụ dựa trên nền web. Hàng loạt các công cụ có sẵn trên PaaS làm cho nó có thể thích ứng với môi trường lập trình ngày càng phát triển.

Hai trong số những lợi ích kinh doanh chính của PaaS trong điện toán đám mây là giảm chi phí và tăng tốc độ phát triển và triển khai. Các công ty có thể sử dụng một

dịch vụ PaaS trong phát triển và triển khai thay vì phải mua nhiều công cụ độc lập khác nhau nên tiết kiệm được rất nhiều chi phí.

Trong một môi trường lai, khi cùng một môi trường PaaS có thể hỗ trợ cả hai dịch vụ công cộng và riêng tư, các doanh nghiệp có thể được hưởng lợi bởi đặc tính linh hoạt và nhanh nhẹn này. Bằng cách cung cấp một nền tảng đồng nhất, chúng ta có thể dễ dàng chuyển tải công việc từ một đám mây riêng tới một đám mây công cộng cho việc triển khai và nhân rộng hiệu quả. Điều này cho phép các tổ chức có được một mức độ kiểm soát cao tại nơi một ứng dụng cụ thể đang chạy.

Dưới đây liệt kê tóm tắt một số nhà cung cấp PaaS:

Amazon Web Services

Amazon đã xây dựng dịch vụ PaaS với tên gọi Amazon Web Service (AWS) Elastic Beanstalk, dựa trên cơ sở vững chắc của cơ sở hạ tầng, EC2, một dịch vụ IaaS cũng của Amazon. Dù cho PaaS của Amazon không hẳn là một nền tảng PaaS theo đúng định nghĩa truyền thống, AWS Elastic Beanstalk của Amazon thay đổi cách các nhà phát triển đẩy ứng dụng của họ vào điện toán đám mây của Amazon. Các nhà phát triển tải lên các ứng dụng và AWS Elastic Beanstalk xử lý các chi tiết về triển khai, khả năng cung cấp, cân bằng tải, tự động mở rộng quy mô và theo dõi tình trạng ứng dụng. Cho đến nay, danh mục dịch vụ của PaaS từ AWS bao gồm AWS Toolkit cho Eclipse (một plug-in cho Java của môi trường phát triển tích hợp Eclipse), AWS CloudFormation (một dịch vụ cho phép các nhà phát triển tạo ra và cung cấp các nguồn tài nguyên của Amazon), một số tùy chọn cơ sở dữ liệu dựa trên đám mây và SDK cho Android và Apple cho máy điện thoại di động, ERuby, Java, PH và. Net.

Salesforce.com

Salesforce là một trong những nhà cung cấp SaaS hàng đầu nay cũng đã chuyển sang cung cấp PaaS với AppExchange của Force.com và nền tảng Heruko. Hiện nay, theo IDC, Salesforce đang là một trong những nhà cung cấp chiếm lĩnh thị trường điện toán đám mây lớn nhất. Năm 2011, Salesforces công bố 3.000 ứng dụng được xây dựng, lắp đặt mỗi 24 giờ và rằng các nền tảng Force.com thực hiện hơn 650 triệu giao dịch mỗi ngày.

Microsoft

Đã có nhiều bất ổn đối với nền tảng PaaS Azure của Microsoft và Azure không nhận được sự thu hút như công ty đã hy vọng. Danh mục các dịch vụ PaaS của Microsoft bao gồm các môi trường máy tính Windows Azure cho các ứng dụng và lưu trữ liên tục cho cả dữ liệu có cấu trúc và phi cấu trúc; Windows Azure AppFabric cung cấp một loạt các dịch vụ kết nối người sử dụng và các ứng dụng thông thường tới các ứng dụng trên điện toán đám mây, quản lý xác thực, thực hiện quản lý dữ liệu và SQL Azure, một dịch vụ cơ sở dữ liệu điện toán đám mây. Tất cả sử dụng Windows làm trung tâm.

RedHat

OpenShift là một nền tảng điện toán đám mây như một sản phẩm dịch vụ của RedHat. Một phiên bản cho điện toán đám mây riêng được đặt tên là OpenShift Enterprise.

Đặc điểm của OpenShift khác với các dịch vụ PaaS khác là các phần mềm chạy dịch vụ là mã nguồn mở dưới tên OpenShift Origin và có sẵn trên GitHub. Những nhà phát triển có thể sử dụng Git để triển khai các ứng dụng web bằng các ngôn ngữ khác nhau trên nền tảng này.

OpenShift cũng hỗ trợ các chương trình nhị phân là các ứng dụng web, miễn là chúng có thể chạy trên RedHat Enterprise Linux. Điều này cho phép sử dụng ngôn ngữ lập trình tùy ý. OpenShift chăm sóc duy trì các dịch vụ cơ bản của ứng dụng và nhân rộng các ứng dụng khi cần thiết trên nền tảng đám mây.

Google

Google App Engine (thường được gọi là GAE hoặc đơn giản là App Engine) là một nền tảng điện toán đám mây để phát triển và lưu trữ các ứng dụng web trong trung tâm dữ liệu của Google quản lý. GAE lần đầu tiên được phát hành như là một phiên bản xem trước vào tháng 4 năm 2008 và chính thức ra mắt vào tháng 9 năm 2011. Ứng dụng được sandbox và chạy trên nhiều máy chủ. App Engine cung cấp tính năng tự động mở rộng quy mô cho các ứng dụng web, khi số lượng yêu cầu tăng lên đối với một ứng dụng, App Engine tự động phân bổ thêm tài nguyên cho các ứng dụng web để xử lý các nhu cầu bổ sung.

Google App Engine được cung cấp miễn phí cho đến một mức độ nhất định của các nguồn tài nguyên tiêu thụ. Sau đó GAE sẽ tính phí cho lưu trữ bổ sung, băng thông, hoặc thời gian chạy của ứng dụng.

Cloud Foundry

Cloud Foundry là dịch vụ PaaS mã nguồn mở giống OpenShift được đưa ra lần đầu năm 2011 bởi VMware và xung quanh đó công ty có kế hoạch xây dựng một sản phẩm thương mại trong tương lai. Như với sáng kiến của RedHat, VMware đang thu hút các nhà phát triển là những người muốn một nền tảng mở cho phép họ xây dựng trong ngôn ngữ mà họ muốn và chạy ứng dụng trên nhà cung cấp IaaS mà họ thích. Theo VMware, dự án có được sức hút rất lớn bởi hơn 2.100 nhà phát triển đang tích cực theo dõi sửa đổi trong mã nguồn mở của Cloud Foundry. Một ví dụ, AppFog là nhà cung cấp PaaS toàn diện đầu tiên đã dựa trên mã Cloud Foundry.

IBM

IBM gia nhập khá muộn vào thị trường PaaS với SmartCloud được giới thiệu vào tháng 10 năm 2013. Nhưng nền tảng này đã quen thuộc với IBM cũng như doanh nghiệp khách hàng của IBM qua bộ công cụ tin cậy WebSphere – cho phép các doanh

nghiệp xây dựng các ứng dụng dựa trên Java có thể chạy trong các đám mây công cộng, được gọi là IBM Smart Cloud Enterprise. IBM đang tìm cách để giữ khách hàng của họ trong một môi trường quen thuộc đồng thời thúc đẩy họ đưa ứng dụng ra điện toán đám mây.

CloudBees

CloudBees là một trong những nhà cung cấp dịch vụ PaaS dựa trên Java đầu tiên cho phép các doanh nghiệp có thể dễ dàng để di chuyển các ứng dụng Java hiện tại vào đám mây. Đám mây RUN@ là nơi chạy ứng dụng thời gian thực của CloudBees, cung cấp chức năng máy chủ ứng dụng truyền thống cho các ứng dụng web, Java và Spring. Khách hàng của CloudBees có thể lựa chọn chạy ứng dụng trên IaaS cơ bản của họ hoặc thậm chí trên đám mây riêng. Ứng dụng chạy trên RUN@ có thể được xây dựng bằng cách sử dụng công cụ phát triển Java EE truyền thống hoặc sử dụng dịch vụ do PaaS của CloudBees cung cấp, gọi là DEV@. Đám mây DEV@ là một môi trường phát triển, xây dựng và thử nghiệm dựa trên đám mây. Doanh nghiệp lựa chọn CloudBees vì có rất nhiều chi phí chìm trong các ứng dụng Java hiện có, do đó các doanh nghiệp bất đắc dĩ mới bỏ đi.

Các mục tiếp theo sẽ giới thiệu chi tiết về một dịch vụ PaaS của nhà cung cấp Microsoft là Windows Azure.

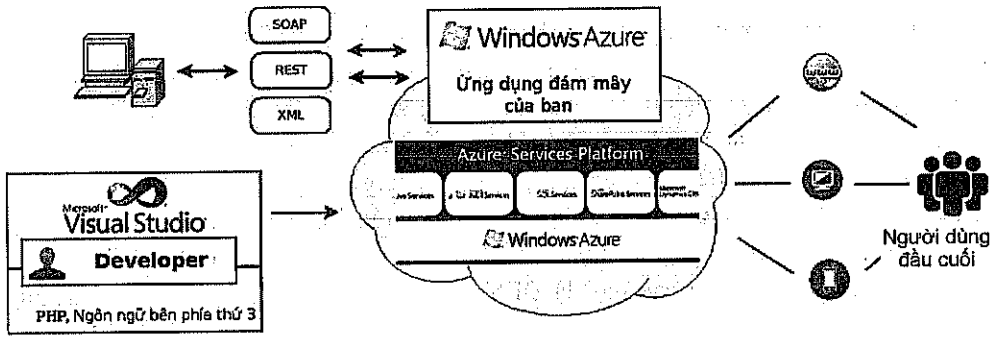
Tổng quan về Windows Azure

Nhìn một cách tổng quan, Windows Azure là một hệ điều hành dùng để chạy các ứng dụng Windows và lưu dữ liệu của nó trên đám mây. Nhưng khác với một hệ điều hành bình thường, người dùng phải cài đặt và chạy trên máy tính của mình, Windows Azure là một dịch vụ: Khách hàng dùng nó để chạy ứng dụng và lưu trữ dữ liệu trên các máy chủ ở trung tâm dữ liệu của Microsoft, có thể truy cập qua Internet. Các ứng dụng này có thể cung cấp dịch vụ cho doanh nghiệp và khách hàng.

Azure là một nền tảng đám mây được đặt trong trung tâm dữ liệu của Microsoft, cung cấp hệ điều hành và tập các dịch vụ phát triển, có thể sử dụng độc lập hoặc kết hợp với nhau để xây dựng các ứng dụng mới, chạy các ứng dụng trên đám mây hoặc phát triển các ứng dụng đã có lấy đám mây làm cơ sở. Azure có cấu trúc mở, cho phép lập trình viên chọn lựa xây dựng các ứng dụng web, chạy các ứng dụng trên các thiết bị, máy tính, máy chủ nối mạng.

Azure giúp giảm thiểu nhu cầu mua công nghệ, cho phép lập trình viên nhanh chóng và dễ dàng tạo ra các ứng dụng chạy trên đám mây bằng cách sử dụng các kỹ thuật có sẵn với môi trường phát triển là Visual Studio và Microsoft .NET framework, hỗ trợ nhiều ngôn ngữ lập trình và môi trường phát triển. Azure đơn giản hóa việc duy trì và vận hành ứng dụng bằng cách cung cấp việc chạy ứng dụng hoặc lưu trữ khi có nhu cầu. Việc quản lý cơ sở hạ tầng được tiến hành tự động. Azure cung cấp một môi trường mở, chuẩn, hỗ trợ nhiều giao thức mạng gồm HTTP, REST, SOAP, XML. Nếu như Windows Live, Microsoft Dynamics và những dịch vụ Microsoft trực tuyến

cho thương mại khác như Microsoft Exchange Online, SharePoint Online cung cấp các ứng dụng đám mây có sẵn cho người sử dụng thì Azure cho phép lập trình viên cung cấp cho khách hàng những thành phần tính toán, lưu trữ, xây dựng các khối dịch vụ và tạo các ứng dụng đám mây.



Hình 4.4. Tổng quan Microsoft Windows Azure

Các thành phần của Windows Azure Platform:

– Windows Azure: cung cấp môi trường nền tảng Windows để chạy ứng dụng và lưu trữ dữ liệu trên máy chủ trong trung tâm dữ liệu của Microsoft.

– SQL Azure: cung cấp dịch vụ lưu trữ dữ liệu quan hệ trên đám mây dựa trên SQL Server.

– AppFabric: cung cấp các dịch vụ đám mây để kết nối các ứng dụng chạy trên đám mây hoặc on-premise.

Windows Azure

Windows Azure là một nền tảng để chạy các ứng dụng Windows và lưu trữ dữ liệu của các ứng dụng này trên đám mây. Windows Azure chạy trên rất nhiều máy, tất cả đều được đặt trong trung tâm dữ liệu của Microsoft và có thể truy cập nhờ mạng Internet. Kết cấu Windows Azure liên kết các trạng thái xử lý thành một khối thống nhất. Các dịch vụ lưu trữ và chạy ứng dụng của Windows Azure được xây dựng phía trên các kết cấu này.

Trong phiên bản Windows Azure được đưa ra tại buổi hội thảo của các chuyên gia tổ chức vào mùa thu năm 2008, lập trình viên có thể tạo ra các phần mềm dựa trên công nghệ .NET như các ứng dụng ASP.NET và các dịch vụ Windows Communication Foundation (WCF). Để làm được điều này, họ có thể sử dụng C# và những ngôn ngữ .NET khác, cùng với các công cụ phát triển truyền thống như Visual Studio 2008. Họ cũng có thể sử dụng phiên bản này của Windows Azure để tạo ra các ứng dụng Web.

Cả ứng dụng Windows Azure và các ứng dụng chạy trên máy cá nhân có thể truy cập các dịch vụ lưu trữ của Windows Azure theo cùng một cách: sử dụng phương thức REST. Tuy nhiên, thành phần lưu trữ dữ liệu không phải là Microsoft

SQL Server, cũng không phải là một hệ thống quan hệ và ngôn ngữ truy vấn của nó không phải là SQL. Thành phần này được thiết kế để hỗ trợ chạy các ứng dụng của Windows Azure, nó cung cấp các kiểu lưu trữ đơn giản hơn, linh động hơn. Nó cũng cho phép lưu các đối tượng dữ liệu lớn (blobs), cung cấp hàng đợi để giao tiếp giữa các thành phần của ứng dụng Windows Azure và thậm chí cung cấp các bảng với ngôn ngữ truy vấn dễ hiểu.

Chạy ứng dụng và lưu dữ liệu trên đám mây rất có ý nghĩa. Thay vì phải mua sắm, cài đặt và xử lý chính hệ thống của mình, một tổ chức có thể chỉ phụ thuộc vào nhà cung cấp đám mây. Khách hàng cũng chỉ phải trả cho việc chạy ứng dụng và lưu trữ mà họ sử dụng thay vì phải duy trì rất nhiều máy chủ chỉ để phục vụ một số nhu cầu nào đó. Và nếu được viết chính xác, các ứng dụng có thể được thay đổi dễ dàng, tận dụng được những tính năng của trung tâm dữ liệu mà đám mây cung cấp.

Trong Windows Azure, mỗi ứng dụng có một file cấu hình. Bằng việc thay đổi thông tin lưu trong file này, chủ sở hữu của ứng dụng có thể thay đổi số lượng các thể hiện mà Windows Azure sẽ chạy. Kết cấu Windows Azure giám sát ứng dụng để duy trì trạng thái mong muốn của ứng dụng đó.

Để cho phép khách hàng tạo ra, cấu hình và giám sát các ứng dụng, Windows Azure cung cấp một cổng có thể truy cập được qua trình duyệt. Mỗi khách hàng được cung cấp một tài khoản Windows Azure ID, một tài khoản để chạy ứng dụng, một tài khoản để lưu trữ dữ liệu.

Windows Azure có thể được ứng dụng theo nhiều cách khác nhau. Một số ứng dụng tiêu biểu:

– Tạo ra một trang web mới: Windows Azure hỗ trợ cả các dịch vụ web và các tiến trình bên dưới, ứng dụng có thể cung cấp giao diện người dùng tương tác cũng như xử lý công việc để đồng bộ người dùng.

Một nhà bán lẻ phần mềm độc lập (ISV) tạo ra phiên bản phần mềm hoạt động như là dịch vụ (SaaS) của một ứng dụng đã có. Ứng dụng .NET có thể được xây dựng trên Windows Azure. Vì Windows Azure cung cấp một môi trường .NET chuẩn nên việc chuyển các ứng dụng .NET lên đám mây không gây ra nhiều vấn đề. Xây dựng ứng dụng trên một nền tảng đã tồn tại cho phép ISV hướng đến việc kinh doanh của họ thay vì mất thời gian cho cơ sở hạ tầng.

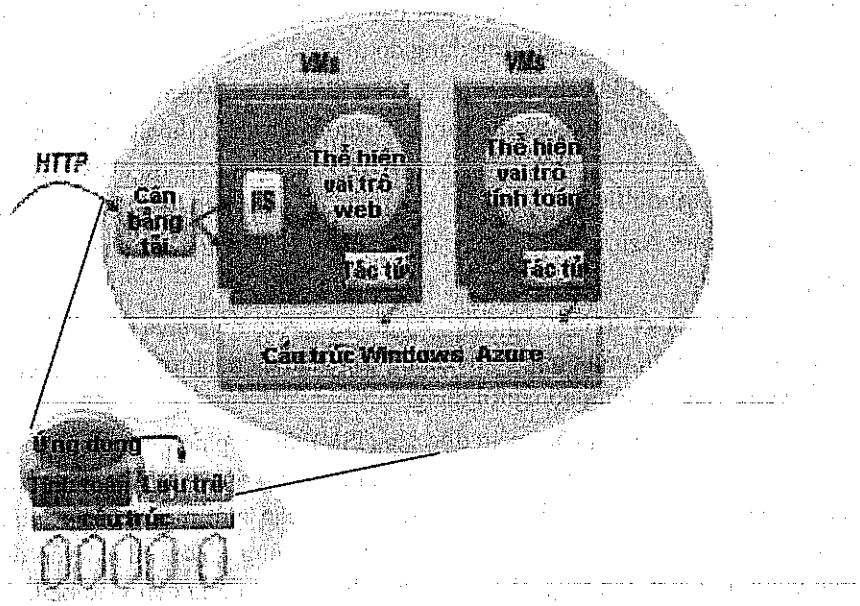
– Một ứng dụng doanh nghiệp: Chọn các ứng dụng trong trung tâm dữ liệu của Microsoft giúp các doanh nghiệp không phải trả tiền cho việc quản lý máy chủ mà tập trung toàn bộ chi phí vào việc xử lý.

Chạy ứng dụng trên đám mây là một trong những xu hướng quan trọng nhất của điện toán đám mây. Với Windows Azure, Microsoft cung cấp một nền tảng để làm việc này, cùng với cách thức lưu trữ dữ liệu. Windows Azure làm hai việc chính: chạy ứng dụng và lưu trữ dữ liệu.

– Chạy ứng dụng: Trong Windows Azure, một ứng dụng có nhiều thể hiện, mỗi thể hiện chạy một phần của mã ứng dụng.

Mỗi thể hiện chạy trên máy ảo của nó. Những máy ảo này chạy Windows Server 2008 64 bit, chúng được thiết kế đặc biệt để sử dụng trên đám mây. Một ứng dụng Windows Azure không thể thấy được máy ảo mà nó đang chạy trong đó. Lập trình viên không được phép cung cấp hình ảnh máy ảo của mình cho Windows Azure, cũng không cần quan tâm về cách duy trì bản sao của hệ điều hành Windows. Thay vào đó, phiên bản đầu tiên cho phép lập trình viên tạo ra ứng dụng .NET 3.5 với Web role và/hoặc Worker role.

Mỗi web role chấp nhận các yêu cầu HTTP hay HTTPS đến qua IIS7. Một web role có thể thực thi sử dụng ASP.NET, WCF hay các công nghệ .NET framework khác làm việc với IIS. Windows Azure cung cấp cân bằng tải có gắn sẵn để mở rộng các yêu cầu qua web role như một phần của ứng dụng.



Hình 4.5. Windows Azure cung cấp các dịch vụ lưu trữ và tính toán cho đám mây

Một worker role, ngược lại, không thể chấp nhận các yêu cầu trực tiếp từ bên ngoài, nó không cho phép các kết nối đến và IIS không chạy trên máy ảo của nó. Thay vào đó, nó nhận dữ liệu vào từ web role, qua hàng đợi trong Windows Azure Storage.

Kết quả của việc này có thể được ghi vào Windows Azure Storage hoặc được gửi ra ngoài. Không giống như web role được tạo ra để xử lý một yêu cầu HTTP đến và kết thúc khi yêu cầu đã được xử lý, một worker role có thể chạy mãi mãi. Một worker role được thực thi sử dụng bất kỳ công nghệ .NET nào.

Bất kể là chạy web role hay worker role, mỗi máy ảo chứa một tác nhân Windows Azure (Windows Azure Agent) cho phép ứng dụng tương tác với kết cấu Windows Azure.

Phiên bản đầu tiên của Windows Azure duy trì một mối quan hệ một – một giữa máy ảo và nhân xử lý vật lý của nó. Vì vậy, hiệu suất của ứng dụng có thể được đảm bảo. Để tăng hiệu suất của ứng dụng, có thể tăng số lượng thể hiện trong file cấu hình. Kết cấu Windows Azure sẽ chuyển sang máy ảo mới, gán chúng với nhân và bắt đầu chạy nhiều thể hiện của ứng dụng hơn. Kết cấu cũng phát hiện xem khi nào web role hoặc worker role bị lỗi, để bắt đầu một cái mới.

Các trạng thái của web role sẽ được ghi vào Windows Azure Storage hoặc được chuyển về cho khách qua cookie.

Cả web role và worker role đều được thực thi sử dụng công nghệ .NET chuẩn. Ứng dụng truy cập dữ liệu theo các cách khác nhau. Truy cập vào dữ liệu Windows Azure sử dụng dịch vụ web ADO.NET. Worker role phụ thuộc vào hàng đợi trong Windows Azure Storage để lấy thông tin đầu vào, một hạn chế khác là ứng dụng Windows Azure không chạy trên môi trường tin cậy, chúng bị hạn chế bởi cái mà Microsoft gọi là Windows Azure Trust.

Với lập trình viên, xây dựng một ứng dụng Windows Azure trong phiên bản PDC giống như xây dựng một ứng dụng .NET truyền thống. Microsoft cung cấp khuôn mẫu (template) project Visual Studio 2008 để tạo ra web role, worker role hoặc cả hai. Lập trình viên tự do sử dụng bất kỳ ngôn ngữ .NET nào. Gói phát triển phần mềm Windows Azure gồm phiên bản của môi trường Windows Azure chạy trên máy của lập trình viên. Gói này bao gồm Windows Azure Storage, một Windows Azure Agent và bất kỳ ứng dụng gì có thể thấy trên đám mây. Lập trình viên có thể tạo ra và sửa ứng dụng bằng hệ thống này, sau đó triển khai trên đám mây khi đã sẵn sàng. Tuy nhiên không thể đưa bộ gỡ lỗi lên đám mây, vì vậy sửa lỗi trên đám mây phụ thuộc vào việc viết ra bản ghi (log) thông tin Windows Azure qua Windows Azure Agent.

Windows Azure cũng cung cấp những dịch vụ khác cho lập trình viên. Ví dụ: một ứng dụng Windows Azure có thể gửi một chuỗi thông báo qua Windows Azure Agent và Windows Azure sẽ chuyển tiếp thông báo đó qua thư, thông điệp tức thời hay một cơ chế nào đó tới người nhận cụ thể. Nếu muốn, Windows Azure có thể phát hiện xem ứng dụng nào lỗi và gửi thông báo. Windows Azure Platform cũng cung cấp thông tin chi tiết về tài nguyên ứng dụng, gồm thời gian xử lý, băng thông đi và đến, lưu trữ.

Truy cập dữ liệu: Cách đơn giản nhất để lưu dữ liệu là sử dụng blob.

Một tài khoản lưu trữ có thể có một hoặc nhiều container, mỗi container có một hoặc nhiều blob. Blob có thể lớn (50 gigabytes) và để sử dụng blob hiệu quả, mỗi blob có thể được chia thành các khối (block). Nếu có lỗi xảy ra, việc chuyển dữ liệu có thể được khôi phục lại với khối gần nhất thay vì phải gửi lại toàn bộ blob.

Blob được lưu trong phạm vi Blob Container. Trong cùng một container, mỗi blob có tên riêng. Dữ liệu trong một blob là các cặp <tên, giá trị>, có kích thước khoảng 8 KB.

Blob chỉ thích hợp cho một số kiểu dữ liệu. Để ứng dụng làm việc với dữ liệu hiệu quả hơn, Windows Azure Storage cung cấp bảng (table). Dữ liệu chứa trong bảng gồm các thực thể với các thuộc tính. Các khái niệm liên quan đến bảng:

– Thực thể (hàng): là những đối tượng dữ liệu cơ bản được lưu trong bảng. Một thực thể chứa tập hợp các thuộc tính. Mỗi bảng có hai thuộc tính tạo thành khóa riêng cho thực thể. Mỗi thực thể có nhiều nhất 255 thuộc tính gồm cả các thuộc tính hệ thống như khóa phân vùng (PartitionKey), khóa hàng (RowKey), thời gian lưu lại thay đổi (Timestamp).

– Thuộc tính (cột): thể hiện một giá trị đơn trong một thực thể. Tên thuộc tính có phân biệt chữ hoa, chữ thường.

– Khóa phân vùng (partitionkey): thuộc tính khóa đầu tiên của mọi bảng. Hệ thống sử dụng khóa phân vùng để tự động phân bố các thực thể của bảng trên nhiều nút lưu trữ khác nhau. Khóa phân vùng có kiểu string.

– Khóa hàng (rowkey): thuộc tính khóa thứ hai của mọi bảng. Đây là định danh riêng của mọi thực thể trong phân vùng chứa thực thể đó. Khóa phân vùng và khóa hàng xác định cụ thể một thực thể trong bảng. Khóa hàng có kiểu string.

– Thời gian lưu lại thay đổi: thời gian hệ thống lưu lại phiên bản của thực thể.

– Phân vùng: tập hợp các thực thể trong bảng có cùng khóa phân vùng.

– Thứ tự sắp xếp: mỗi thực thể trong bảng được sắp xếp theo khóa phân vùng và khóa hàng để truy vấn dựa theo những khóa này hiệu quả hơn, kết quả trả về được sắp xếp theo những khóa này.

Một bảng không có giản đồ định nghĩa sẵn (defined schema), thuộc tính có nhiều loại khác nhau: int, string, bool, DateTime. Thay vì sử dụng SQL, ứng dụng truy cập dữ liệu bảng sử dụng lệnh truy vấn với cú pháp LINQ. Một bảng có thể lớn, với hàng tỉ thực thể lưu hàng triệu byte dữ liệu, nếu cần thiết, Windows Azure có thể phân chia các bảng trên nhiều máy chủ để cải thiện hiệu suất.

Blob và bảng đều được dùng để lưu dữ liệu. Lựa chọn thứ ba là hàng đợi (queue). Hàng đợi cung cấp cách để web role giao tiếp với worker role. Một hàng đợi có thể chứa nhiều thông điệp. Tên của hàng đợi có phạm vi trong tên tài khoản. Số lượng các thông điệp lưu trong hàng đợi không bị giới hạn. Mỗi thông điệp được lưu nhiều nhất là một tuần, sau đó hệ thống sẽ tự thu dọn những thông điệp lâu hơn một tuần. Dữ liệu trong hàng đợi cũng có dạng <tên, giá trị> và mỗi hàng đợi chứa tối đa 8 KB dữ liệu.

Thông điệp được lưu trong hàng đợi. Khi được đưa vào hàng đợi, thông điệp có thể có dạng nhị phân nhưng khi lấy thông điệp ra khỏi hàng đợi, đáp ứng trả về có dạng XML còn thông điệp được mã hóa base64. Thông điệp được trả về từ hàng đợi không

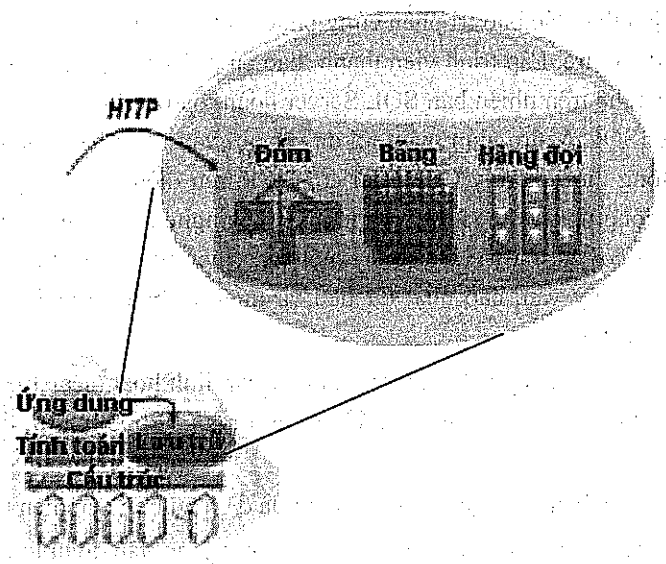
theo thứ tự, mỗi thông điệp có thể được trả về nhiều hơn một lần. Một số tham số được sử dụng trong hàng đợi của Azure là:

MessageID: giá trị định danh thông điệp trong hàng đợi.

VisibilityTimeout: số thực xác định thời gian chờ tính bằng giây có thể thấy được thông điệp. Giá trị cực đại là 2 giờ. Thời gian mặc định là 30 giây.

PopReceipt: chuỗi được trả về khi truy vấn thông điệp. Chuỗi này cùng với MessageID là những giá trị bắt buộc khi muốn xóa một thông điệp khỏi hàng đợi.

MessageTTL: xác định thời gian sống tính bằng giây của thông điệp. Thời gian sống cực đại là 7 ngày, giá trị mặc định là 7 ngày. Nếu trong thời gian sống mà thông điệp không bị chủ tài khoản xóa khỏi hàng đợi, hệ thống lưu trữ sẽ tự động xóa thông điệp.



Hình 4.6. Windows Azure cho phép lưu dữ liệu trong blob, table và queue theo kiểu REST qua giao thức HTTP

Windows Azure Storage có thể truy cập ứng dụng Windows Azure hoặc một ứng dụng chạy ở một nơi nào đó. Trong cả hai trường hợp, các kiểu lưu trữ của Windows Azure sử dụng tiêu chuẩn REST để xác định và lấy dữ liệu. Mọi thứ được đặt tên sử dụng URIs và được truy cập với chuẩn HTTP. Một máy khách .NET có thể sử dụng dịch vụ dữ liệu ADO.NET và LINQ.

SQL Azure

SQL Azure là ứng dụng chạy trên trung tâm dữ liệu, cung cấp khả năng lưu trữ dữ liệu cho các cả các ứng dụng điện toán đám mây và các ứng dụng khác. SQL Azure cung cấp tập các dịch vụ đám mây hỗ trợ lưu trữ và làm việc với nhiều loại thông tin.

Hiện tại, Microsoft đưa ra 2 thành phần chính của SQL Azure: SQL Azure Database và "Huron" Data Sync. SQL Azure Database cung cấp một RDBMS trong "đám mây". Nó cho phép ứng dụng đám mây và ứng dụng có sẵn (on-premises) có thể lưu trữ cơ sở dữ liệu quan hệ hoặc dạng khác trên các máy chủ tại trung tâm dữ liệu. Chi phí sẽ được tính dựa trên những gì sử dụng, thay đổi tùy theo nhu cầu sử dụng.

Thành phần thứ hai trong SQL Azure được giới thiệu là "Huron" Data Sync, xây dựng dựa trên Microsoft Sync Framework và SQL Azure Database, công nghệ này cho phép đồng bộ dữ liệu thông qua các on–premises DBMS. Người sử dụng và sở hữu dữ liệu sẽ xác định những gì cần đồng bộ, giải quyết các xung đột như thế nào,...

SQL Azure giúp đơn giản hóa công tác kế hoạch dự phòng và triển khai của nhiều CSDL khác nhau. Trên Azure, lập trình viên không còn phải cài đặt, cấu hình, nâng cấp, hay vá lỗi phần mềm máy chủ CSDL như trước đây. Khả năng sẵn sàng, chịu lỗi cao và tối giản thao tác bảo trì phần cứng phục vụ CSDL là yêu cầu mặc định – tiên quyết trong SQL Azure. Lập trình viên thành thạo cú pháp T-SQL (Transact-SQL), mô hình dữ liệu quan hệ trên phiên bản SQL Server hoàn toàn có thể dùng lại kỹ năng này với SQL Azure. SQL Azure giúp giảm tối đa chi phí vận hành bằng tích hợp tập công cụ có sẵn để đồng thời quản lý CSDL tại cơ sở và trên điện đoán mây. Ngoài ra, lập trình viên web công nghệ Microsoft, hay từ các công nghệ khác như PHP, Java, có thể sử dụng công cụ có tên mã là Houston – một giao diện web gọn nhẹ, giao diện thân thiện để quản trị, truy vấn, cập nhật dữ liệu và thiết kế bảng trên SQL Azure. SQL Azure có các chức năng:

– Phát triển ứng dụng web đáp ứng tải truy cập linh hoạt (scalable), phù hợp với các doanh nghiệp cỡ nhỏ (< 100 người) đến trung bình (< 2000 người, theo tiêu chuẩn của Microsoft).

– Phát triển và bán ứng dụng đóng gói như là dịch vụ trên nền điện toán đám mây.

– Xây dựng những ứng dụng cỡ phòng ban trong một tập đoàn lớn.

– Thông qua các chuẩn mở như WCF Service hay RESTful để tổng hợp dữ liệu từ nhiều nguồn khác nhau trên điện toán đám mây và cho phép truy cập dữ liệu an toàn từ nhiều địa điểm, thiết bị điện toán khác nhau.

SQL Azure có thể đem lại các lợi ích lớn:

– Tối thiểu quản trị (không phải cài đặt, vá lỗi, hay bảo trì phần cứng).

– Tự động chống lỗi, khắc phục sự cố – tối đa tính sẵn sàng.

– Đơn giản hóa công tác lập kế hoạch dự phòng phần cứng, phần mềm khi triển khai nhiều CSDL khác nhau.

– Co dãn linh hoạt tuy biến theo nhu cầu sử dụng thực tế.

– Có thể đặt ở nhiều địa điểm khác nhau trên thế giới để rút ngắn tuyến truy cập.

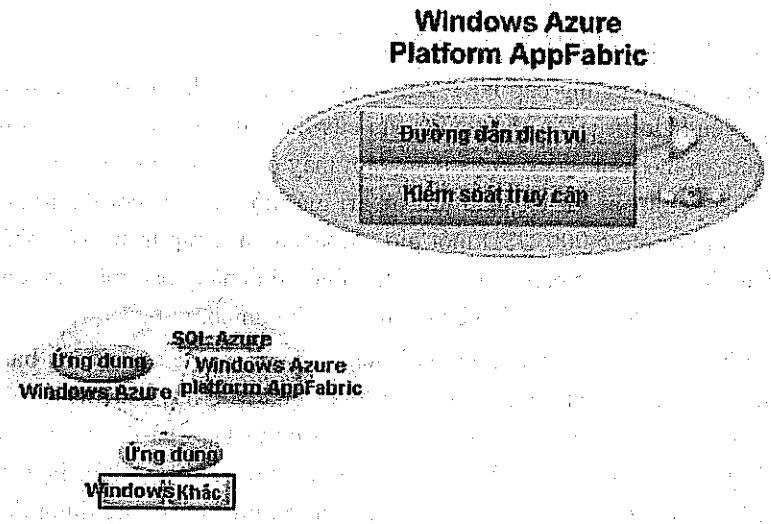
– Tích hợp sẵn với các công cụ phổ biến SQL Server và Visual Studio. Ngoài ra có giao diện web cho các lập trình viên sử dụng công nghệ không phải Microsoft truy vấn tới.

– Hỗ trợ T-SQL trên mô hình tương tự với dữ liệu quan hệ truyền thống.

Apps Fabric

Windows Azure platform AppFabric cung cấp dịch vụ cơ sở hạ tầng dựa trên đám mây.

Windows Azure platform AppFabric cung cấp cơ sở hạ tầng dựa trên đám mây được sử dụng bởi ứng dụng đám mây và ứng dụng on-premise.



Hình 4.7. Windows Azure Platform AppFabric

Các thành phần của Windows Azure platform AppFabric:

– Service Bus: Mục tiêu của Service Bus là cho phép ứng dụng expose các endpoint có thể được truy xuất bởi các ứng dụng khác. Mỗi exposed endpoint được gán một URI. Client sử dụng URI này để xác định vị trí và truy xuất dịch vụ. Service Bus cũng xử lý việc chuyển đổi địa chỉ mạng và vượt qua tường lửa mà không cần mở port mới để expose ứng dụng.

– Access Control: Dịch vụ này cho phép ứng dụng client chứng thực chính nó và cung cấp một ứng dụng server với thông tin xác thực. Máy chủ sau đó có thể sử dụng thông tin này để quyết định những gì ứng dụng này được phép làm.

Các dịch vụ này có thể được sử dụng trong nhiều cách khác nhau như sau:

Giả sử một doanh nghiệp muốn cho phần mềm được truy cập bởi các đối tác thương mại đến một trong các ứng dụng của nó. Nó có thể expose các chức năng của ứng dụng qua dịch vụ Web: SOAP hoặc REST, sau đó đăng ký các endpoint của họ với

Service Bus. Các đối tác thương mại có thể sử dụng Service Bus để tìm các endpoint này và truy xuất các dịch vụ.

Một ứng dụng chạy Windows Azure có thể truy xuất dữ liệu lưu trữ trong cơ sở dữ liệu on-premise. Để làm được điều này, có thể giải quyết bằng cách tạo một service truy xuất dữ liệu, sau đó expose service này qua Service Bus.

Hãy tưởng tượng một doanh nghiệp expose nhiều dịch vụ ứng dụng cho các đối tác kinh doanh của mình. Nếu những dịch vụ đó được expose bằng cách sử dụng REST, ứng dụng có thể dựa vào các Access Control để xác thực và cung cấp thông tin nhận dạng cho mỗi ứng dụng khách hàng. Thay vì duy trì thông tin nội bộ về từng ứng dụng đối tác thương mại, thông tin này có thể được lưu trữ trong dịch vụ Access Control.

4.3. SỬ DỤNG DỊCH VỤ HẠ TẦNG IAAS

Trong các nhà cung cấp IaaS, Amazon luôn đứng đầu trong gần như mọi bảng xếp hạng. Nếu SalesForce là công ty đi đầu của SaaS thì có thể coi Amazon là công ty đầu tiên đưa ra mô hình IaaS. Điện toán đám mây của Amazon cung cấp một loạt các lựa chọn. Từ cung cấp không gian lưu trữ trị giá một vài xu một tháng đến cho thuê siêu máy tính với giá 5.000 USD/một giờ. Amazon đang tập trung vào phân khúc các khách hàng doanh nghiệp bằng việc bổ sung nhiều tính năng bảo mật hơn cho đám mây của mình và tuyển dụng nhân viên bán hàng doanh nghiệp.

Hai hãng lớn trong công nghệ là Microsoft và Google cũng đang bắt đầu đi vào cung cấp IaaS sau khi đã thành công với PaaS qua Microsoft Azure và Google App Engine. Microsoft vừa mở rộng Azure vào thị trường IaaS và thậm chí còn cho phép người dùng chạy Linux trên đám mây của mình với mức giá hứa hẹn sẽ thấp hơn Amazon. Bên cạnh đó, Microsoft cũng cung cấp rất nhiều các ứng dụng doanh nghiệp trên đám mây của mình từ cơ sở dữ liệu SQL Server đến Microsoft Office 365. Google đã rất thành công với các ứng dụng trong SaaS và Google App Engine trong PaaS thì giữa năm 2012 cũng tung ra dịch vụ IaaS của riêng mình là Google Compute Engine.

Ngoài ra còn có các tên tuổi khác như IBM, Rackspace với công nghệ đám mây OpenStack; Citrix và Apache với CloudStack.

Trong một số bảng xếp hạng các dịch vụ IaaS, dù theo tiêu chí nào thì Amazon cũng dẫn đầu. Điều đó cho thấy vị thế của Amazon trong lĩnh vực điện toán đám mây, cụ thể là IaaS. Ngoài ra, có thể thấy rất nhiều tên tuổi lớn nữa như Microsoft, Google, HP, AT&T, Rackspace.

Nói đến IaaS là nói đến hạ tầng phần cứng, các nhà cung cấp dịch vụ IaaS thông thường sẽ đưa ra những dịch vụ: cung cấp máy ảo – từ máy tính cấu hình thông thường nhất đến các máy chủ chuyên biệt, cung cấp dung lượng lưu trữ cho các máy ảo, các địa chỉ IP, các đám mây riêng,... Các dịch vụ này có thể được cung cấp riêng lẻ hoặc

được cung cấp cùng nhau theo từng gói dịch vụ. Dưới đây sẽ liệt kê một số chức năng của các dịch vụ cung cấp bởi IaaS.

Lưu trữ: Cung cấp lưu trữ liên tục cho các máy ảo. Dung lượng lưu trữ thường tồn tại độc lập với thời gian sống của máy ảo. Dung lượng lưu trữ thường mang tính sẵn sàng cao, độ tin cậy cao, có thể được sử dụng như phân vùng khởi động một máy ảo hoặc gắn liền với một máy ảo như một thiết bị lưu trữ tiêu chuẩn. Khi được sử dụng như một phân vùng khởi động, các máy ảo có thể được dừng lại và sau đó khởi động lại, cho phép chỉ phải trả cho các tài nguyên lưu trữ sử dụng trong khi duy trì trạng thái của máy ảo. Với những doanh nghiệp muốn lưu trữ với độ bền cao, các nhà cung cấp sẽ cung cấp khả năng tạo ra bản sao tại những thời điểm nhất định của dữ liệu, sau đó chúng được lưu trữ và tự động sao chép trên nhiều nơi khác trong đám mây. Những bản sao có thể được sử dụng như là điểm khởi đầu cho một khối lưu trữ mới và có thể bảo vệ dữ liệu của doanh nghiệp cho độ bền lâu dài. Doanh nghiệp cũng có thể dễ dàng chia sẻ các bản sao này. Có hai loại dung lượng lưu trữ thường được các nhà cung cấp IaaS đưa ra là dung lượng tiêu chuẩn và dung lượng IOPS. Dung lượng tiêu chuẩn cung cấp chi phí lưu trữ hiệu quả rất phù hợp cho các ứng dụng với các yêu cầu giao tiếp dữ liệu vừa phải. Dung lượng IOPS được dùng cho các yêu cầu hiệu suất cao hoặc các ứng dụng như cơ sở dữ liệu.

Máy ảo đa địa điểm: Một số nhà cung cấp IaaS cung cấp khả năng đặt máy ảo tại nhiều địa điểm. Do các địa điểm được thiết kế và cài đặt riêng biệt nên chúng được cách ly khỏi những lỗi/hỏng. Với máy ảo đa địa điểm riêng biệt, ứng dụng được bảo vệ khỏi lỗi/hỏng của một địa điểm duy nhất với máy ảo đa địa điểm riêng biệt, ứng dụng tránh được các lỗi hay hỏng hóc gây ra bởi một địa điểm duy nhất.

Địa chỉ IP mềm dẻo: là dịch vụ cung cấp địa chỉ IP tĩnh nhưng được thiết kế riêng cho điện toán đám mây để đảm bảo tính năng động. Một địa chỉ IP mềm dẻo sẽ gắn với tài khoản của doanh nghiệp chứ không phải với máy ảo được thuê.

Khách hàng kiểm soát địa chỉ đó cho đến khi không sử dụng dịch vụ nữa. Tuy nhiên, không giống như địa chỉ IP tĩnh truyền thống, địa chỉ IP mềm dẻo sử dụng kỹ thuật ánh xạ lại cho phép ánh xạ từ địa chỉ IP công cộng của khách hàng tới bất kỳ máy chủ ảo nào. Thay vì chờ đợi vào một kỹ thuật viên dữ liệu để cấu hình lại hoặc thay thế máy chủ của bạn, hoặc chờ đợi DNS để tuyên truyền cho tất cả các khách hàng của bạn, địa chỉ IP mềm dẻo cho phép khách hàng giải quyết khi vấn đề/lỗi xảy ra bằng cách nhanh chóng ánh xạ lại địa chỉ IP đó tới máy ảo thay thế.

Đám mây riêng ảo: Dịch vụ đám mây riêng ảo cung cấp cho doanh nghiệp một đám mây riêng nằm trong đám mây của nhà cung cấp IaaS trong một mạng ảo do khách hàng quyết định. Doanh nghiệp hoàn toàn kiểm soát môi trường mạng ảo, bao gồm lựa chọn các dải địa chỉ IP của riêng họ, tạo ra các mạng con, cấu hình bảng định tuyến và cổng mạng. Doanh nghiệp cũng có thể tạo ra một kết nối bằng mạng riêng ảo

(VPN) giữa trung tâm dữ liệu của công ty với đám mây riêng ảo và tận dụng điện toán đám mây như một phần mở rộng của trung tâm dữ liệu của công ty.

Với đám mây riêng ảo, doanh nghiệp có thể:

– Cho thuê ứng dụng web cơ bản nhưng được bảo mật qua một lớp bổ sung của đám mây.

– Có thể cho thuê ứng dụng web đa tầng với các máy chủ web, máy chủ ứng dụng, máy chủ cơ sở dữ liệu.

– Cho thuê các ứng dụng web mở rộng được trên mây kết nối tới trung tâm dữ liệu của doanh nghiệp.

– Mở rộng hệ thống mạng, ứng dụng cộng tác sang đám mây.

– Khôi phục dữ liệu khi thảm họa xảy ra với trung tâm dữ liệu.

Cụm tính toán hiệu năng cao (High Performance Computing Clusters): Khách hàng có nhu cầu cần khối lượng công việc tính toán phức tạp như các bài toán lập trình song song giao tiếp nhiều, hoặc với các ứng dụng nhạy cảm với hiệu suất mạng, có thể sử dụng dịch vụ này để đạt được hiệu năng tính toán cao và mạng lưới hoạt động ổn định nhưng lại tận dụng các tính đàn hồi, linh hoạt và lợi thế về chi phí của điện toán đám mây. Với các dịch vụ cung cấp tính toán phân cụm, tính toán phân cụm dùng GPU và tính toán phân cụm bộ nhớ cao đã được thiết kế đặc biệt để cung cấp khả năng mạng hiệu năng cao và có thể được lập trình đưa ra thành các cụm – cho phép các ứng dụng có được hiệu suất mạng có độ trễ thấp cần thiết cho giao tiếp giữa các luồng.

Dịch vụ tính toán GPU: Khách hàng đòi hỏi khả năng hoạt động song song cao sẽ được hưởng lợi từ các dịch vụ tính toán GPU, trong đó cung cấp quyền truy cập vào các GPU từng lên đến 1.536 lõi CUDA và 4 GB bộ nhớ video. Với các phiên bản driver mới nhất, các GPU hỗ trợ cho OpenGL, DirectX, CUDA, OpenCL và SDK GRID. Dịch vụ tính toán GPU rất lý tưởng cho các ứng dụng đồ họa 3D, bao gồm cả trò chơi trực tuyến và tính toán khối lượng công việc, bao gồm cả hóa học tính toán, mô hình tài chính, thiết kế kỹ thuật.

Các dịch vụ đặc biệt:

– Máy chủ truy xuất dữ liệu vào ra mức cao: Dịch vụ này có thể cung cấp cho khách hàng với tỉ lệ vào/ra ngẫu nhiên trên 100.000 IOPS. Dịch vụ này được hỗ trợ bởi công nghệ ổ đĩa thể đặc (Solid State Disk – SSD), rất phù hợp cho khách hàng cần hiệu suất cao và cơ sở dữ liệu quan hệ NoSQL.

– Xuất nhập máy ảo (VM): cho phép bạn dễ dàng nhập khẩu hình ảnh máy ảo từ môi trường hiện tại vào một đám mây mới và xuất khẩu chúng trở lại bất cứ lúc nào. Bằng cách nhập các máy ảo đã sẵn sàng để sử dụng trong đám mây, doanh nghiệp vừa có thể tận dụng các khoản đầu tư hiện tại trong các máy ảo vừa có thể đáp ứng bảo mật,

quản lý cấu hình,... Tương tự, khách hàng có thể xuất các máy chủ ảo để sau này có thể dùng lại bất cứ lúc nào.

Các dịch vụ hỗ trợ

Ngoài ra, các nhà cung cấp IaaS cũng có các dịch vụ hỗ trợ cho các dịch vụ chính liệt kê ở trên:

– Giám sát: là một dịch vụ web cung cấp giám sát đối với các nguồn tài nguyên điện toán đám mây và các ứng dụng. Dịch vụ giám sát cung cấp khả năng hiển thị việc sử dụng tài nguyên, hiệu suất hoạt động và tổng nhu cầu mô hình, bao gồm cả số liệu như sử dụng CPU, ổ đĩa đọc và viết, lưu lượng mạng. Khách hàng có thể nhận được số liệu thống kê, xem đồ thị, và thiết lập hệ thống báo động cho dữ liệu số liệu của mình.

– Co dãn tự động: cho phép doanh nghiệp tự động thay đổi quy mô hạ tầng tăng lên hoặc giảm xuống tùy theo điều kiện xác định trước. Với Auto Scaling, doanh nghiệp có thể đảm bảo rằng hạ tầng phần cứng đang sử dụng có khả năng tăng quy mô liên tục khi có nhu cầu để duy trì hiệu suất trong khi quy mô xuống tự động theo nhu cầu để giảm thiểu chi phí. Co dãn tự động theo quy mô đặc biệt rất thích hợp cho các ứng dụng chạy thay đổi theo thời gian ngắn hạn như hằng giờ, hằng ngày, hoặc hằng tuần.

– Cân bằng tải mềm dẻo: dịch vụ này tự động phân phối lưu lượng ứng dụng đến các máy ảo trên đám mây. Điều này cho phép đạt được khả năng chịu lỗi lớn hơn trong các ứng dụng của doanh nghiệp, chúng liên tục cung cấp số lượng tải công suất cân bằng cần thiết để đáp ứng với lưu lượng truy cập ứng dụng đến. Cân bằng tải mềm dẻo phát hiện các máy chủ bị quá tải và tự động định tuyến lại lưu lượng truy cập đến các máy chủ khỏe mạnh chịu được tải cao cho đến khi các máy chủ quá tải đã được khôi phục. Có thể cấu hình cho phép cân bằng tải mềm dẻo trong một khu sẵn có hoặc qua nhiều khu vực cho phù hợp hơn với hiệu suất ứng dụng.

– Mạng tăng cường: cho phép đạt được hiệu năng truyền gói tin cao hơn một cách đáng kể để làm giảm tải của mạng. Tính năng này sử dụng một mạng lưới mới ngăn xếp ảo cung cấp hiệu suất vào ra I/O cao hơn và sử dụng CPU thấp hơn so với máy chủ truyền thống.

4.4. CÂU HỎI VÀ BÀI TẬP

1. Nêu các đặc điểm giống/khác giữa các phần mềm trên đám mây như Google App Suits và các phần mềm truyền thống.
2. Tìm hiểu mô hình SaaS ứng dụng cho doanh nghiệp. Lấy một trong các công cụ điển hình Salesforce minh họa. Tìm hiểu về sản phẩm của MISA – doanh nghiệp Việt Nam để minh họa (MISA CRM, MISA HRM).

3. Tìm hiểu và so sánh Windows Azure với một số nhà cung cấp PaaS khác như Amazon Webservices và Google App Engine.
4. Tìm hiểu thêm về Windows Azure và nêu rõ vai trò của: Blob, Table, Queues.
5. Nêu các đặc điểm trong sử dụng dịch vụ nền tảng.
6. Nêu các đặc điểm trong sử dụng dịch vụ phần mềm.
7. Nêu các đặc điểm trong sử dụng dịch vụ IaaS.
8. Tìm hiểu thêm về Microsoft Office 365 và mô tả hiệu quả trong sử dụng dịch vụ IaaS.

Chương 5
GIÁM SÁT, TRÁNH LỖI VÀ ĐẢM BẢO CHẤT LƯỢNG

Trong chương này, chúng ta làm quen với các khái niệm khái quát chung để có một cái nhìn tổng thể về lĩnh vực đảm bảo chất lượng dịch vụ đám mây. Mặc dù mục tiêu chung của giáo trình là giới thiệu kỹ thuật cơ sở, riêng trong chương này, để có một cái nhìn bao quát, ta sẽ thử thâm nhập vào lĩnh vực dưới con mắt của một chuyên gia cấp cao đảm bảo chất lượng cho người sử dụng đám mây, người có trách nhiệm phải xây dựng một giải pháp an toàn tổng thể cho một hệ thống. Với cách tiếp cận này, người đọc sẽ được trang bị một tầm nhìn bao quát, trên cơ sở đó có thể chủ động liên hệ các kiến thức học thuật và kỹ thuật cụ thể ở các chương sau vào các bài toán thực tế.

5.1. CÁC HỆ THỐNG, DỊCH VỤ GIÁM SÁT

Các khái niệm

Điện toán đám mây cho phép các công ty và cá nhân thuê tài nguyên theo yêu cầu từ một cái "bể" hầu như không giới hạn. Mô hình thanh toán "dùng bao nhiêu trả bấy nhiêu" được tính phí dựa trên khối lượng tài nguyên sử dụng trong 1 đơn vị thời gian. Bằng cách này, một doanh nghiệp có thể tối ưu hóa khoản tiền đầu tư vào công nghệ thông tin và cải thiện tính sẵn sàng cũng như khả năng mở rộng của hệ thống.

Trong khi điện toán đám mây có rất nhiều hứa hẹn cho điện toán doanh nghiệp, vẫn có một số thiếu sót trong dịch vụ hiện nay như:

– Khả năng mở rộng vốn dĩ hạn chế của các nhà cung cấp dịch vụ đám mây đơn lẻ, mặc dù hầu hết các nhà cung cấp cơ sở hạ tầng đám mây hiện nay yêu cầu khả năng mở rộng vô hạn. Trong thực tế thì ngay cả những nhà cung cấp lớn nhất cũng có nguy cơ đối mặt với vấn đề về khả năng mở rộng khi tỷ lệ sử dụng điện toán đám mây tăng. Về lâu dài, vấn đề về khả năng mở rộng có thể sẽ trở nên tồi tệ hơn khi các nhà cung cấp điện toán đám mây phục vụ một số lượng dịch vụ online ngày càng tăng, thêm vào đó, mỗi dịch vụ lại được truy cập bởi số lượng lớn người dùng trên toàn cầu vào mọi thời điểm.

– Thiếu khả năng tương tác giữa các nhà cung cấp dịch vụ. Công nghệ đám mây hiện tại không được thiết kế để có khả năng tương tác. Kết quả là các nhà cung cấp dịch vụ đám mây không thể mở rộng thông qua quan hệ đối tác kinh doanh. Ngoài ra, nó cũng ngăn cản các nhà cung cấp cơ sở hạ tầng đám mây vừa và nhỏ xâm nhập thị trường cung cấp điện toán đám mây. Nhìn chung, nó đã ngăn cản sự cạnh tranh cũng như trói buộc khách hàng với một nhà cung cấp duy nhất.

– Không hỗ trợ xây dựng trong quản lý dịch vụ kinh doanh. Quản lý dịch vụ kinh doanh (System management business – SMB) là một chiến lược quản lý cho phép doanh nghiệp sắp xếp quản lý CNTT theo mục tiêu cao cấp của họ. Một mặt quan trọng của SMB là quản lý hợp đồng dịch vụ (SLA). Giải pháp điện toán đám mây hiện tại không được thiết kế để hỗ trợ cho các hoạt động SMB được thành lập trong quản lý hằng ngày của doanh nghiệp ngành CNTT. Kết quả là các doanh nghiệp tìm kiếm sự chuyển đổi từ các hoạt động CNTT sang công nghệ dựa vào đám mây sẽ phải đối mặt với một bước đi không tăng và có khả năng gây rối.

Để giải quyết những vấn đề này, hiện nay mô hình liên kết kinh doanh cho các nhà cung cấp dịch vụ điện toán đám mây, trong đó mỗi nhà cung cấp có thể mua hoặc bán dung lượng từ các nhà cung cấp khác, tùy theo nhu cầu.

Các yêu cầu của hệ thống, dịch vụ giám sát

Những yêu cầu chính sau đây cho một hệ thống hạ tầng điện toán đám mây nhằm đảm bảo chất lượng dịch vụ cung cấp cho người dùng đầu cuối:

– *Triển khai tự động và nhanh chóng.* Đám mây nên hỗ trợ hệ thống kích hoạt dự phòng tự động cho những ứng dụng dịch vụ phức tạp, dựa trên một hợp đồng chính thức xác định cụ thể hợp đồng dịch vụ cơ sở hạ tầng. Hợp đồng tương tự cũng cần được tái sử dụng để cung cấp nhiều trường hợp của cùng một ứng dụng cho người thuê khác nhau với các tùy chỉnh khác nhau.

– *Co dãn tự động.* Đám mây nên tự động điều chỉnh các thông số phân bố nguồn tài nguyên (bộ nhớ, CPU, băng thông, lưu trữ) của môi trường thực thi ảo của mỗi cá nhân một cách liên tục. Hơn nữa, số lượng các môi trường ảo thực hiện phải được tự động và điều chỉnh liên tục để thích ứng với sự thay đổi tải.

– *Tối ưu tự động liên tục.* Đám mây nên liên tục tối ưu sự sắp xếp của việc quản lý nguồn tài nguyên cơ sở hạ tầng với mục đích cao cấp của doanh nghiệp.

Trong phần này, chúng ta sẽ làm sáng tỏ một tập hợp các nguyên tắc cho phép các dịch vụ điện toán đám mây được giám sát. Các nguyên tắc này làm nổi bật các yêu cầu cơ bản từ các nhà cung cấp điện toán đám mây cho phép các ứng dụng ảo được di chuyển một cách tự do, phát triển và thu nhỏ.

Tính liên minh trong hệ thống: Tất cả các nhà cung cấp dịch vụ điện toán đám mây, bất kể lớn đến đâu, đều có một khả năng hữu hạn. Để phát triển vượt khỏi giới

hạn đó, các nhà cung cấp dịch vụ điện toán đám mây nên hình thành liên minh các nhà cung cấp để cộng tác và chia sẻ tài nguyên. Sự cần thiết của những sản phẩm điện toán đám mây có khả năng liên kết cũng có nguồn gốc từ xu hướng công nghiệp, trong việc áp dụng các mô hình điện toán đám mây nội bộ trong công ty để tạo ra các đám mây riêng và sau đó có thể mở rộng đám mây với các nguồn tài nguyên cho thuê theo yêu cầu từ các đám mây công cộng. Mỗi liên minh của các nhà cung cấp dịch vụ điện toán đám mây nên cho phép các ứng dụng ảo được triển khai trên các địa điểm liên kết. Hơn thế nữa, các dịch vụ ảo cần một địa điểm hoàn toàn tự do và cho phép di chuyển một phần hoặc toàn bộ giữa các địa điểm. Đồng thời, sự riêng tư bảo mật và độc lập của các thành viên liên bang phải được duy trì để cho phép các nhà cung cấp cạnh tranh nhằm liên hiệp.

Tính độc lập của các dịch vụ: Cũng như các tiện ích khác, nơi chúng ta sử dụng dịch vụ mà không biết gì về hệ thống bên trong với các thiết bị tiêu chuẩn, không phụ thuộc vào bất kỳ nhà cung cấp nào, để các dịch vụ điện toán đám mây thực sự đáp ứng các tính toán như một tầm nhìn tiện ích, chúng ta cần cung cấp cho người dùng một sự độc lập hoàn toàn. Người dùng nên được trao khả năng sử dụng dịch vụ đám mây mà không cần phải dựa vào bất kỳ công cụ đặc biệt nào của nhà cung cấp dịch vụ và nhà cung cấp dịch vụ điện toán đám mây nên có khả năng quản lý cơ sở hạ tầng của mình mà không phơi bày các chi tiết bên trong cho khách hàng hoặc đối tác. Như một hệ quả của nguyên tắc độc lập, tất cả các dịch vụ điện toán đám mây cần được đóng gói và tổng quát để người sử dụng có thể có nguồn tài nguyên tương đương tại các nhà cung cấp khác nhau.

Tính tách biệt của các dịch vụ: Dịch vụ điện toán đám mây, theo định nghĩa, được tổ chức bởi một nhà cung cấp đồng thời sẽ tổ chức các ứng dụng từ nhiều người sử dụng khác nhau. Đối với những người dùng di chuyển những tính toán của họ vào đám mây, họ cần sự đảm bảo từ nhà cung cấp điện toán đám mây sao cho công cụ của họ là hoàn toàn tách biệt những người khác. Người dùng phải được đảm bảo rằng tài nguyên của họ không thể bị truy cập bởi những người chia sẻ cùng một đám mây và không có người dùng khác có thể có khả năng trực tiếp ảnh hưởng đến các dịch vụ cấp cho ứng dụng của họ.

Tính mềm dẻo: Một trong những ưu điểm chính của điện toán đám mây là khả năng cung cấp hoặc phát hành nguồn tài nguyên theo yêu cầu. Những khả năng mềm dẻo nên được ban hành tự động bởi các nhà cung cấp điện toán đám mây để đáp ứng nhu cầu thay đổi, giống như các công ty điện có thể (trong trường hợp hoạt động bình thường) tự động đối phó với chênh lệch trong mức tiêu thụ điện. Hành vi và giới hạn của việc tăng cũng như thu hẹp tự động cần được thúc đẩy bởi hợp đồng và các quy tắc thống nhất giữa các nhà cung cấp điện toán đám mây và người sử dụng.

Tình hướng doanh nghiệp: Có lẽ vấn đề quan trọng nhất để giải quyết trước khi điện toán đám mây có thể trở thành mô hình điện toán ưa thích là làm sao thiết lập được sự tin tưởng. Cơ chế để xây dựng và duy trì lòng tin giữa người tiêu dùng và các nhà cung cấp, cũng như giữa các nhà cung cấp với nhau, là yếu tố cần thiết cho sự thành công của bất kỳ sản phẩm điện toán đám mây nào.

Mô hình hệ thống dịch vụ giám sát

Trong mô hình hệ thống giám sát dịch vụ điện toán đám mây, chúng ta xác định hai đối tượng chính: Nhà cung cấp dịch vụ (Service Providers – SPs) là các nhân tố cần tài nguyên để cung cấp một vài dịch vụ. Tuy nhiên SPs không sở hữu tài nguyên, thay vào đó, họ thuê của các nhà cung cấp cơ sở hạ tầng (Infrastructure Providers – IPs), nơi cung cấp cho họ một không gian tài nguyên tính toán, mạng và lưu trữ gần như vô hạn.

Một ứng dụng dịch vụ là một tập hợp các thành phần phần mềm làm việc cùng nhau để đạt được một mục tiêu chung. Mỗi thành phần của ứng dụng dịch vụ như thực hiện trong một VEE chuyên dụng. Các nhà cung cấp dịch vụ triển khai các ứng dụng dịch vụ trên đám mây bằng việc cung cấp một IP, được gọi là các trang web chính với một dịch vụ Manifest–có nghĩa là, một tài liệu xác định cấu trúc của ứng dụng cũng như hợp đồng và SLA giữa các SP và IP.

Để tạo ra những ảo ảnh của một không gian tài nguyên vô hạn, các nhà cung cấp cơ sở hạ tầng chia sẻ công suất không sử dụng của họ với nhau để tạo ra một liên bang đám mây. Một khung hiệp định là một văn bản định nghĩa hợp đồng giữa hai IPs – thông báo các điều khoản và điều kiện để một nhà cung cấp này có thể sử dụng tài nguyên của một nhà cung cấp khác.

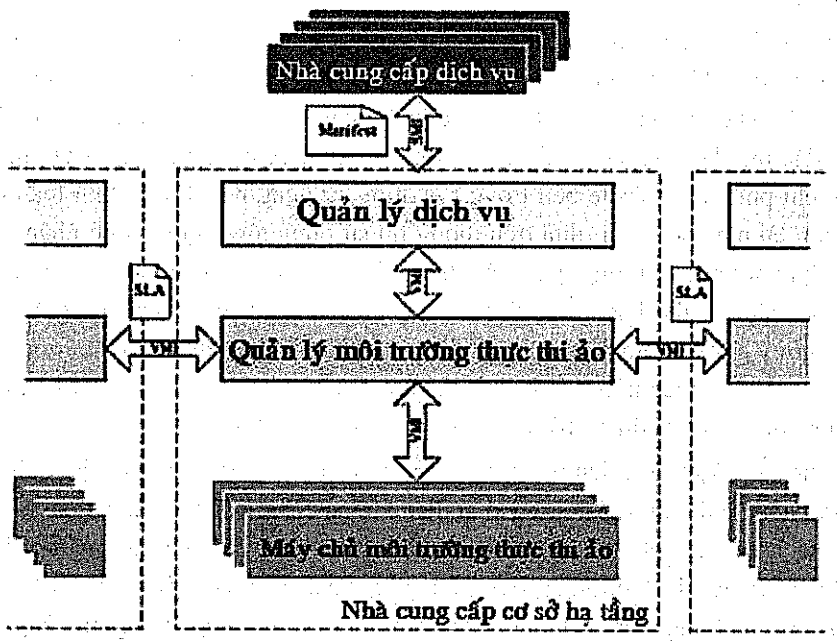
Với mỗi nhà cung cấp cơ sở hạ tầng, tối ưu hóa tài nguyên sử dụng đạt được bằng việc phân vùng các tài nguyên vật lý, thông qua một lớp ảo tới môi trường thực thi ảo (Virtual Execution Environments – VEEs) – môi trường thực thi hoàn toàn tách biệt. Chúng ta cũng đề cập đến nguồn tài nguyên tính toán ảo hóa, bên cạnh là các lớp ảo hóa và tất cả các thành phần quản lý như môi trường thực hiện máy chủ ảo (Virtual Execution Evironment Host – VEEH).

Thiết kế và miêu tả của kiến trúc này là mục đích chính của dự án nghiên cứu RESERVOIR European. Kiến trúc RESERVOIR (xem hình 5.1) xác định các thành phần chức năng chính cần một IP để hỗ trợ hoàn toàn mô thức điện toán đám mây. Lý do đằng sau sự phân lớp đặc biệt này là để tách biệt rõ ràng các mối quan tâm và trách nhiệm, để ẩn các chi tiết cơ sở hạ tầng ở mức độ thấp, nhận quyết định từ quản lý cấp cao và các nhà cung cấp dịch vụ.

Quản lý dịch vụ là một thành phần duy nhất với một IP có thể tương tác với các nhà cung cấp dịch vụ (SPs). Nó nhận các danh sách dịch vụ, điều đình giá cả và quản lý hóa đơn. Hai nhiệm vụ quan trọng nhất của nó là triển khai, cung cấp VEEs dựa trên

các danh sách dịch vụ và giám sát, thực thi sự tuân thủ theo SLA bằng cách điều chỉnh khả năng của một ứng dụng dịch vụ.

Quản lý môi trường thực thi ảo (VEEM) chịu trách nhiệm cho các vị trí tối ưu của các VEE vào các máy chủ phụ thuộc vào ràng buộc được xác định bởi quản lý dịch vụ (Service Manager). Quá trình tối ưu hóa liên tục được thúc đẩy bởi một chức năng tiện ích lập trình vị trí cụ thể. Quản lý môi trường thực thi ảo được tự do đặt và di chuyển các môi trường khắp mọi nơi, thậm chí là ở những địa điểm điều khiển từ xa (tùy thuộc vào thỏa thuận tổng thể), miễn là các vị trí đáp ứng được các ràng buộc. Như vậy, ngoài việc phục vụ các yêu cầu nội bộ (từ quản lý dịch vụ nội bộ), VEEM còn chịu trách nhiệm cho sự liên kết của các site từ xa.



Hình 5.1. Kiến trúc RESERVOIR: Các thành phần và giao diện chính

Máy chủ môi trường thực thi ảo (VEEH) chịu trách nhiệm cho việc điều khiển cơ bản và giám sát các VEEs và tài nguyên của chúng (ví dụ: tạo ra một VEE, sắp xếp thêm các nguồn tài nguyên cho một VEE, giám sát một VEE, di chuyển một VEE, tạo một mạng ảo và không gian lưu trữ,...). Cho rằng các VEE thuộc cùng một ứng dụng có thể đặt ở nhiều máy chủ và thậm chí được mở rộng vượt ra khỏi phạm vi một site, máy chủ phải hỗ trợ các mạng ảo tách biệt vượt qua các máy chủ và site. Hơn nữa, các máy chủ phải hỗ trợ di dân VEE minh bạch cho bất kỳ máy chủ nào tương thích trong các đám mây liên kết, bất kể vị trí trang web cho mạng và lưu trữ cấu hình.

Quản lý dịch vụ (SM). Hệ thống dịch vụ là một kịch bản liên minh gần như cơ bản nhất, thậm chí ở đây SM cũng phải được cho phép hạn chế các vị trí cụ thể khi dịch vụ được triển khai. Hạn chế việc triển khai có liên quan đến một VEE cụ thể (mặc dù các biểu hiện hạn chế có thể liên quan đến các VEE khác, như có thể thấy trong những hạn chế mối quan hệ ở trên) và truyền lại cho các quản lý VEE cùng với bất kỳ siêu dữ liệu VEE cụ thể khác khi VEE được ban hành để tạo thông qua VMI. Chúng chỉ định một tập các ràng buộc phải được tiến hành khi VEE được tạo ra, để có thể được xem như một số loại "điều kiện đường viền" nhằm xác định lĩnh vực có thể được sử dụng bởi các thuật toán sắp xếp chạy ở lớp quản lý các VEE. Hai loại hạn chế triển khai được hình dung là: đầu tiên, có những hạn chế mối quan hệ, liên quan đến mối quan hệ giữa các VEEs; thứ hai, có thể có những hạn chế trang web, liên quan đến các trang web.

Trong kịch bản liên minh, sử dụng thỏa thuận khung (FA) giữa các tổ chức để thiết lập các điều khoản và điều kiện cho liên kết. Hiệp định khung được đàm phán và được xác định bởi các cá nhân, nhưng chúng được mã hóa ở cuối trong quản lý dịch vụ (SM) – đặc biệt là trong cơ sở dữ liệu thông tin kinh doanh (BIDB). Ví dụ, thông tin quản lý chi phí cho Website bên trong FA được sử dụng bởi SM để tính toán chi phí các nguồn tài nguyên từ xa (dựa trên thông tin sử dụng tổng hợp mà nó nhận được từ VEEM địa phương) và tương quan các thông tin này với những chi phí từ những trang web khác. SM có thể bao gồm như là một phần của siêu dữ liệu trong VEE, một "Vector gợi ý giá" bao gồm một chuỗi các con số, mỗi người đại diện một ước tính chi phí tương đối của việc triển khai các VEE trên mỗi trang web liên kết. SM tính toán vector này dựa trên FA được thành lập với các trang web khác.

Cho rằng kịch bản liên minh cao cấp hỗ trợ di chuyển, hạn chế vị trí phải được kiểm tra không chỉ ở thời gian triển khai dịch vụ mà còn để di chuyển. Ngoài ra, SM có thể cập nhật các hạn chế triển khai trong thời gian tuổi thọ dịch vụ, qua đó thay đổi "điều kiện đường viền" được sử dụng bởi các thuật toán sắp xếp. Khi VEE được di chuyển trên các trang web, hạn chế việc triển khai của nó được bao gồm cùng với bất kỳ siêu dữ liệu khác liên quan đến VEE. Mặt khác, cần phải không có chức năng bổ sung từ người quản lý dịch vụ để thực hiện các liên đoàn đầy đủ tính năng.

Quản lý môi trường thực thi ảo. Ít cần trong kịch bản cơ bản của liên dịch vụ VEEM. Yêu cầu duy nhất sẽ là khả năng triển khai một VEE trong các trang web từ xa, vì vậy nó sẽ cần một plug-in có thể giao tiếp với đám mây từ xa bằng cách gọi các API công cộng để đáp ứng yêu cầu vị trí cơ hội. VEEM sẽ cần thỏa thuận khung để các tính năng khác nhau được cung cấp bởi các kịch bản liên minh cơ bản, vì các VEEM cần tham dự vào việc đánh giá SLA được quy định trong FA, cho dù có quan tâm tới VEE hay không. Các mô đun tốt nhất trong VEEM dành cho việc đánh giá SLA kiểm soát sự chính xác của các chính sách với người dùng. Ngoài ra, cần phải có di chuyển lạnh;

do đó VEEM cần khả năng báo hiệu hypervisor để lưu trạng thái VEE (điều này là một phần của các môđun vòng đời VEEM) và cũng cần khả năng chuyển các tập tin nhà nước cho trang web từ xa. Ngoài ra, VEEM có thể gửi tín hiệu tới hypervisor (tầng ảo hóa) để khôi phục lại trạng thái VEE và tiếp tục thực hiện của nó (cũng là một phần của môđun vòng đời VEEM). Liên quan đến hỗ trợ dự phòng tài nguyên tạm thời, các công cụ chính sách phải có khả năng dự trữ một không gian trong cơ sở hạ tầng vật lý để đưa ra một khung thời gian cho các VEE cụ thể.

Trong kịch bản liên minh nâng cao, khả năng tạo ra các mạng ảo cross-site cho các VEE có thể đạt được bằng cách sử dụng chức năng cung cấp bởi các mạng ứng dụng ảo (VAN) như một phần của các máy chủ ảo giao diện API. Do đó, VEEM cần giao diện một cách chính xác với VAN và có thể thể hiện các đặc điểm mạng ảo trong một kết nối VEEM-to-VEEM. Trong kịch bản liên minh đầy đủ tính năng, tính năng di chuyển trực tiếp cần phải được hỗ trợ trong API VHI. Các VEEM sẽ chỉ cần gọi các chức năng của di chuyển trực tiếp đến phần hypervisor của API VHI để đạt được chuyển đổi trực tiếp qua các domain.

Máy chủ môi trường thực thi ảo. Cần có khả năng giám sát cả liên minh. Các dịch vụ giám sát của RESERVOIR hỗ trợ việc theo dõi không đồng bộ một trung tâm dữ liệu đám mây VEEHs, VEEs của họ và các ứng dụng chạy bên trong VEEs. Để hỗ trợ liên bang, các trung tâm dữ liệu có nguồn gốc phải có khả năng theo dõi VEEs và các ứng dụng của họ chạy ở một trang web từ xa. Khi một sự kiện xảy ra liên quan đến một VEE chạy trên một trang web từ xa, nó được công bố và proxy từ xa chuyển tiếp yêu cầu đến proxy địa phương đăng ký, do đó công bố sự kiện này cho các thuê bao tại địa phương chờ đợi. Khuôn khổ giám sát độc lập với loại hình và nguồn gốc của dữ liệu đang được theo dõi và hỗ trợ linh hoạt việc tạo chủ đề mới.

Cần bỏ các chức năng khác cho các liên đoàn cơ bản trong VEEH ngoài các tính năng được mô tả trong kịch bản cơ sở. Mặt khác, đối với một liên đoàn nâng cao, có một số tính năng cần thiết. Đầu tiên, nó phải có khả năng thực hiện dịch vụ mạng liên mạng với ứng dụng ảo, một mạng lưới lớp phủ mới cho phép các dịch vụ mạng ảo trên mạng con và qua các biên giới hành chính. Ứng dụng ảo cho phép thiết lập mạng ảo quy mô lớn, miễn phí không phụ thuộc vị trí và cho phép các mạng ảo hoàn toàn "có khả năng di chuyển". (1) Các dịch vụ mạng ảo được cung cấp là hoàn toàn bị cô lập; (2) nó cho phép chia sẻ các máy chủ, thiết bị mạng và các kết nối vật lý; (3) giấu mạng liên quan đến đặc tính vật lý như thông lượng liên kết, vị trí của máy chủ,...

Ngoài ra, khả năng để làm di chuyển liên minh với dịch vụ lưu trữ không chia sẻ được yêu cầu. RESERVOIR tăng cường khả năng chuyển đổi tiêu chuẩn VM thường có sẵn trong mỗi hypervisor hiện đại với sự hỗ trợ cho các môi trường trong đó nguồn và các máy chủ đích không chia sẻ lưu trữ; ổ cứng thường của máy ảo di cư cư trú hủy bỏ việc chia sẻ lưu trữ.

Với những kịch bản liên minh đầy đủ tính năng, các yêu cầu từ VEEH hầu hết tập trung vào di chuyển nóng. Nguyên tắc chia tách của tách RESEVOIR yêu cầu mỗi trang web RESERVOIR là một thực thể tự trị. Cấu hình trang web, cấu trúc liên kết và những gì tương tự không được chia sẻ giữa các trang web. Vì vậy, một trang web không nhận thức được các địa chỉ của máy chủ từ một trang web khác. Tuy nhiên, hiện nay, máy ảo di chuyển giữa các máy chủ yêu cầu nguồn và đích hypervisors biết địa chỉ của nhau và chuyển một VM trực tiếp từ các máy chủ nguồn đến đích. Để khắc phục mâu thuẫn rõ ràng này, RESEVOIR giới thiệu một kênh di chuyển liên kết mới chuyển một VEE từ một máy chủ đến máy chủ khác mà không trực tiếp giải quyết các máy chủ đích. Thay vì chuyển VEE trực tiếp đến các máy chủ đích, nó đi qua proxy tại trang web nguồn và trang web đích, giải quyết vấn đề không rõ vị trí hypervisor.

5.2. GIÁM SÁT DỊCH VỤ

Giám sát dịch vụ

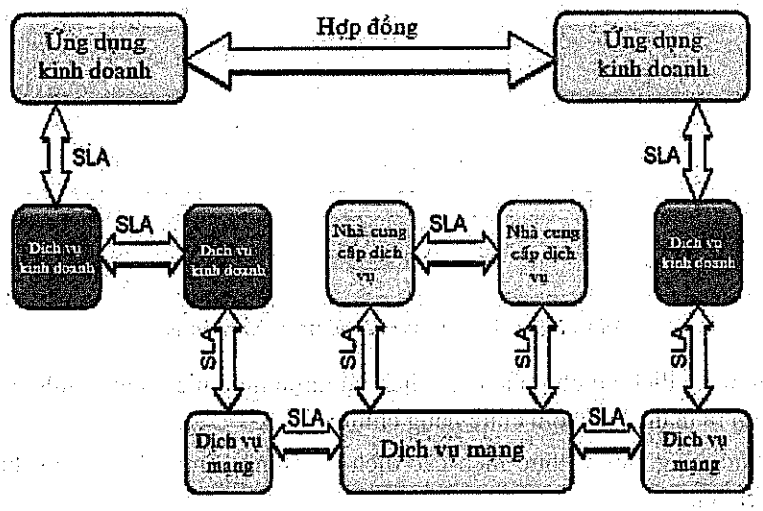
Việc tích hợp giám sát dịch vụ của dịch vụ đám mây với các quy trình nội bộ của doanh nghiệp cung cấp dịch vụ giám sát (SPs) đòi hỏi thiết kế và lập kế hoạch một cách cẩn thận. Thông thường, dịch vụ giám sát là độc quyền và hạn chế cung cấp cho các đại lý bên ngoài. Do đó, việc các doanh nghiệp chuyển đổi sang sử dụng dịch vụ đám mây đòi hỏi việc sử dụng giám sát đại lý giữa các mạng doanh nghiệp và dịch vụ đám mây. Các đại lý phải được thiết kế để phân biệt giữa mức độ dịch vụ được cung cấp bởi dịch vụ đám mây và mức độ dịch vụ được cung cấp bởi chính các mạng doanh nghiệp. Các đại lý sau đó cần phải xử lý được với mức chất lượng theo những cách thích hợp để đảm bảo rằng dịch vụ đám mây cung cấp những thỏa thuận về số liệu chất lượng cho doanh nghiệp và sau đó quản lý các cấp độ chất lượng này để thực hiện theo cam kết của các doanh nghiệp. Ngoài chất lượng dịch vụ giám sát, các đại lý cần phải quản lý tài sản doanh nghiệp. Tài sản của các đại lý phải được lưu giữ trong một bản kiểm kê các tài sản cố định và tài sản biến động đang sử dụng hoặc có thể được cung cấp theo yêu cầu người sử dụng và các dịch vụ. Tài sản của các đại lý cũng làm việc với các dịch vụ của các đại lý để yêu cầu giám sát và phân bổ nguồn lực trong việc bảo trì ở dạng cố định hoặc biến động với mức độ chất lượng dịch vụ cần có.

SLAs đã là một sản phẩm phổ biến trong hỗ trợ các dịch vụ viễn thông được cung cấp bởi SP trong nhiều năm. Như đã thảo luận ở mục 5.1, SLAs xác định hiệu suất thỏa thuận và QoS hoặc các số liệu sản phẩm. Để đạt được chất lượng và hiệu suất theo mục tiêu cho các sản phẩm hoặc dịch vụ, có thể cần yêu cầu doanh nghiệp thành lập và quản lý một số SLAs. Sự phức tạp của dịch vụ toàn cầu là tập hợp vô số các dịch vụ, nhà cung cấp và công nghệ, tất cả đều có yêu cầu hiệu suất khác nhau. Như vậy, mục tiêu của doanh nghiệp SLAs là để cải thiện kinh nghiệm khách hàng (CE) của dịch vụ hoặc sản phẩm cho khách hàng doanh nghiệp, dù là bên trong hay bên ngoài để tổ chức.

CE là một thuật ngữ chung để tạo thành một thước đo chất lượng của dịch vụ hoặc sản phẩm và bao gồm tất cả các khía cạnh dịch vụ: hiệu suất, mức độ hài lòng của khách hàng trong tổng số kinh nghiệm, trước và sau bán hàng, việc cung cấp các sản phẩm và dịch vụ. Xác định CE cung cấp sự phân biệt giữa các loại dịch vụ khác nhau hoặc các sản phẩm mà một doanh nghiệp cung cấp, từ đó dẫn đến cơ hội cân bằng mức độ chất lượng cung cấp tương ứng với giá và kỳ vọng của khách hàng.

Mối quan hệ giữa CE và SLA là CE liên quan đến nhận thức chất lượng của một sản phẩm hay dịch vụ, trong khi một SLA đề cập đến định nghĩa, đo lường và báo cáo của mục tiêu của dịch vụ hoặc sản phẩm. Như vậy, CE và SLA có liên quan trong đó nếu nhận thức về dịch vụ hoặc sản phẩm là chưa đầy đủ, nhưng các thông số dịch vụ nằm trong giới hạn quy định của SLA, SLA phải được khắc phục. Các khái niệm quan trọng là ghép nối các phương pháp nhận thức từ CE vào các biện pháp khách quan cho SLA. Việc ghép nối này có thể là đa chiều, thực nghiệm, chức năng, hoặc phức tạp trong tự nhiên.

Các ứng dụng hỗ trợ doanh nghiệp hoặc kinh doanh, tạo điều kiện thuận lợi cho dịch vụ kinh doanh. Ví dụ, trong một tổng đài (ứng dụng), một dịch vụ kinh doanh rõ ràng là thông tin liên lạc bằng giọng nói. Dịch vụ kinh doanh tự nó thường không tăng doanh thu, nhưng nó hỗ trợ các mục tiêu kinh doanh và hiệu quả của một ứng dụng doanh nghiệp. Một hoặc nhiều dịch vụ kinh doanh có thể cần thiết để hỗ trợ ứng dụng doanh nghiệp. Dịch vụ kinh doanh lần lượt sử dụng một số tài nguyên dịch vụ, chẳng hạn như dịch vụ mạng. Đặc biệt, dịch vụ kinh doanh hỗ trợ Tầng 4 trong mô hình OSI được phân loại như các dịch vụ mạng. Các dịch vụ mạng có thể là hỗ trợ nội bộ hay bên ngoài để cung cấp dịch vụ cho bên ngoài, chẳng hạn như các nhà cung cấp đám mây.

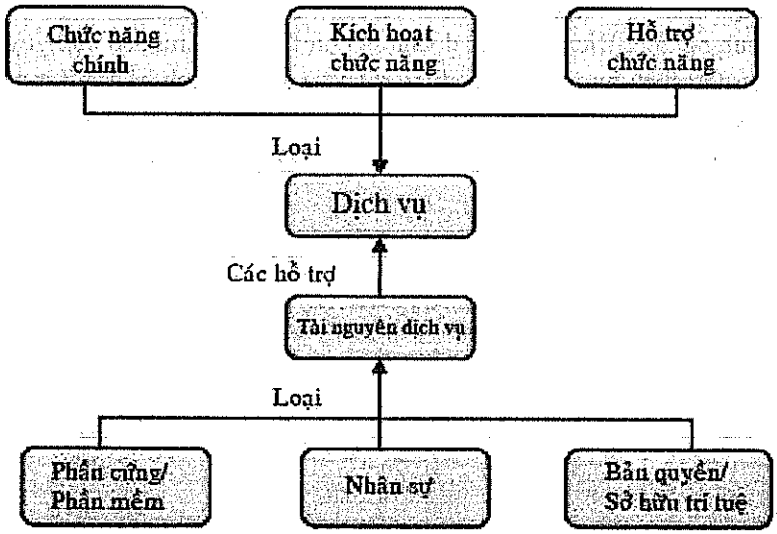


Hình 5.2. End-to-End SLA

Hình 5.2 là một ví dụ của end-to-end SLA. Vấn đề quan trọng cần lưu ý trong hình là các ứng dụng kinh doanh, ví dụ như, tổng đài hoặc môi giới chứng khoán trực tuyến, được hỗ trợ bởi một số dịch vụ kinh doanh, ví dụ, giọng nói và cơ sở dữ liệu, mà lần lượt được hỗ trợ bởi dịch vụ mạng, ví dụ như IP. Có thể có các dịch vụ mạng nội bộ hoặc các dịch vụ mạng bên ngoài từ các nhà cung cấp đám mây. Một số dịch vụ kinh doanh, chẳng hạn như vận chuyển, không yêu cầu các dịch vụ mạng để thực hiện các ứng dụng kinh doanh của họ, chẳng hạn như chuyển phát bưu kiện, nhưng ngày càng dựa vào các dịch vụ mạng cung cấp giá trị dịch vụ gia tăng, chẳng hạn như theo dõi bưu kiện trực tuyến.

Để tăng giá trị cho một SLA trong việc cung cấp các ứng dụng kinh doanh cho doanh nghiệp, cơ sở hạ tầng doanh nghiệp cần phải được gắn đầy đủ số liệu để có thể xác định đảm bảo sự phù hợp, ngăn chặn hoặc cảnh báo không phù hợp và các đánh giá mức độ không phù hợp. Một bản ghi kiểm toán cũng có thể cần thiết cho việc lập kế hoạch năng lực, kiểm soát chi phí và giải quyết tranh chấp.

Thông thường, việc thực hiện, giám sát dịch vụ hoặc giám sát sản phẩm đòi hỏi phải ứng dụng các chức năng dịch vụ và các nguồn lực trong một mối quan hệ tương tự như những gì thể hiện trong hình 5.3.



Hình 5.3. Các dịch vụ và tài nguyên dịch vụ

Chức năng dịch vụ cho phép các dịch vụ được thực hiện mang tính vật lý và có thể phân tách ra thành ba nhóm chức năng chính:

– Chức năng chính: thực hiện các dịch vụ chính. Email là một ví dụ của một chức năng chính.

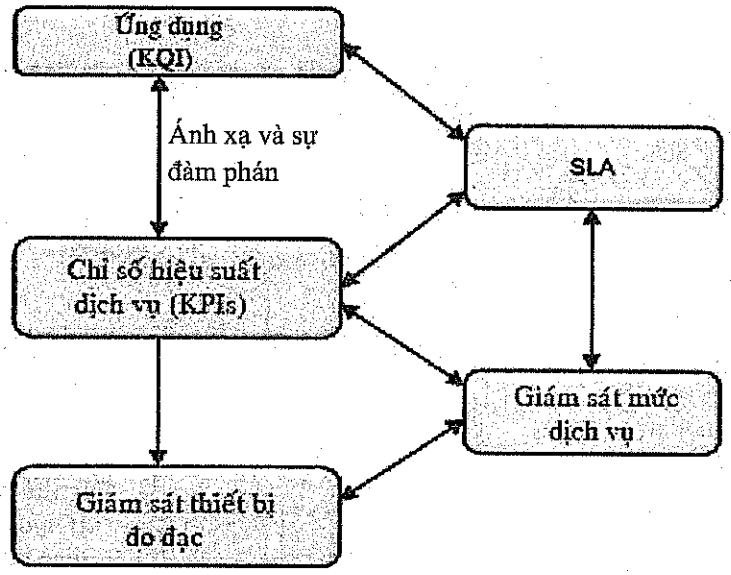
– Kích hoạt chức năng: cho phép các chức năng chính được thực hiện. Ví dụ các chức năng cho phép bao gồm hệ điều hành, sưởi ấm, thông gió và điều hòa nhiệt độ (HVAC).

– Hỗ trợ chức năng: hỗ trợ và mở các chức năng chính. Ví dụ về chức năng hỗ trợ bao gồm tài khoản, tiếp tân, nhóm thực thu, người quản lý và bảo trì.

Mặt khác, tài nguyên bao gồm tài sản như phần cứng, phần mềm, nhân sự và đào tạo, bản quyền và sở hữu trí tuệ, cơ sở vật chất và ngân sách.

Các chỉ số chất lượng quan trọng và các chỉ số hiệu suất chính

Có thể đánh giá và báo cáo dễ dàng về khó khăn trong ghép nối các thông số dịch vụ cụ thể với thông số công nghệ. Kết quả là, SLAs truyền thống đã tập trung gần như hoàn toàn vào việc thực hiện hỗ trợ dịch vụ. Ngược lại, KQIs và KPIs tập trung vào chất lượng dịch vụ chứ không phải vào hiệu suất mạng. KQIs và KPIs cung cấp phép đo các khía cạnh cụ thể của việc thực hiện các ứng dụng hoặc dịch vụ. Một KQI có nguồn gốc từ một số nguồn tin, bao gồm cả số liệu hiệu suất của một dịch vụ hoặc KPIs dịch vụ hỗ trợ cơ bản. Như một dịch vụ hay ứng dụng được hỗ trợ bởi một số yếu tố dịch vụ, một số KPIs khác nhau có thể cần phải được xác định để tính toán một KQI cụ thể. Ghép nối giữa KPI và KQI có thể đơn giản hay phức tạp và việc ghép nối này có thể là thực nghiệm hoặc chính thức.



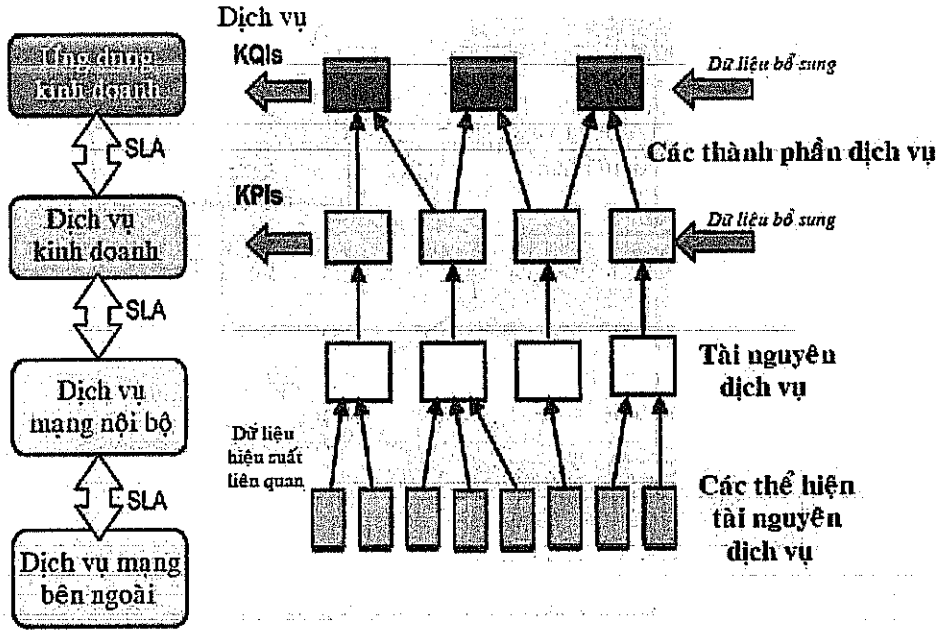
Hình 5.4. Quan hệ giữa SLA, KQI và KPI

Theo tính chủ quan, một số thông số KQI có thể gặp khó khăn để thêm vào như là một hợp đồng yêu cầu trong một SLA. Tuy nhiên, có một số KQIs có liên quan đến

CE và nên cần được thêm vào trong một SLA. Để đáp ứng những KQIs, một số KPIs cũng phải được xác định, đánh giá và thống nhất trong các SLA. Những mối quan hệ này được mô tả trong hình 5.4. Trong hình 5.4, KPIs có thể được quy định tại SLAs, KQIs có nguồn gốc và được theo dõi trong một quá trình SLM. Mỗi KPI hoặc KQI có ngưỡng cảnh báo trên và dưới và một ngưỡng lỗi trên và dưới. Các KPIs sau đó được kết hợp bởi một số chức năng thực nghiệm hay lý thuyết để đạt được biện pháp KQIs.

Báo cáo và quản lý dịch vụ

Sự phù hợp với một SLA được đảm bảo bằng cách sử dụng công cụ trong hệ thống cung cấp KPI thích hợp và các biện pháp KQI ở mức mẫu cần thiết. Điều quan trọng trong quá trình thiết kế là để đảm bảo rằng quá trình đo lường chính nó không tạo ra hoặc làm trầm trọng thêm tình trạng hệ thống bằng cách thêm tải trọng cho hệ thống, ví dụ, bằng cách sử dụng sức mạnh xử lý bổ sung hoặc bổ sung thêm quản lý lưu lượng chi phí. Nếu một KQI cho một dịch vụ đầu tiên được xác định bởi tương quan KPI hoặc dữ liệu KQI từ một dịch vụ thứ hai, thông tin từ các dịch vụ thứ hai có thể được yêu cầu trong thời gian thực. Điều này sẽ cho phép đo được sự thực hiện quản lý chủ động của dịch vụ đầu tiên, do đó cho phép phòng ngừa lỗi chứ không phải là thông tin tổng hợp được lưu trữ. Như vậy, một SLA nên được theo dõi liên tục với tốc độ phù hợp với yêu cầu cho một dịch vụ để đảm bảo rằng hành động khắc phục có thể được thực hiện và đối chiếu để tạo các báo cáo quản lý.



Hình 5.5. Quan hệ giữa các tài nguyên dịch vụ, KQI và KPI

Khi một SLA được đặt ra, sự phù hợp với các SLA được thể hiện bằng các sự trình bày báo cáo. Như với các SLA, màn hình hiển thị và giải thích các dữ liệu báo cáo phải rõ ràng và súc tích, nó phải rõ ràng khi SLA ra khỏi sự phù hợp và không ẩn chứa trong vô số các dữ liệu phù hợp. Cho mỗi dịch vụ, dữ liệu hiệu suất liên quan đến được lấy từ các trường hợp có liên quan của tài nguyên dịch vụ. Đây là những đối chiếu và kết hợp để tạo KQI cho mỗi tài nguyên và tiếp tục kết hợp để hình thành các dịch vụ và sản phẩm KQI, như thể hiện trong hình 5.5.

Bằng cách sử dụng thiết bị trong một hệ thống để đo lường KPI và KQI, dữ liệu về hiệu suất dịch vụ được thu thập và đối chiếu thành một dạng có thể được thao tác để cho phép chẩn đoán và hình thành báo cáo. Thiết bị đo đạc có thể bao gồm các khảo sát sự hài lòng của người sử dụng; ứng dụng thử nghiệm, bao gồm các ứng dụng như gọi ảo; tác nhân màn hình khách; tác nhân màn hình máy chủ và các tác nhân màn hình mạng. Các SLA cần xác định các giai đoạn thu thập và cung cấp thông tin cốt lõi cần thiết để đảm bảo rằng các SLA đáp ứng yêu cầu của họ. Dữ liệu thiết bị có thể cần phải được thông qua trên các điểm truy cập dịch vụ để nó có thể được sử dụng như dữ liệu KQI và KPI để xác định KQI hoặc KQI cho các dịch vụ khác. Ngoài ra, để chủ động quản lý, hệ thống cần phải thu thập thông tin thời gian thực để có thể thực hiện chủ động quản lý phòng chống lỗi. Đối với quản lý phản ứng, hệ thống có thể thu thập thời gian gần thực hoặc ngoại tuyến, dữ liệu thời gian đánh dấu để nó có thể tương quan với các dữ liệu thời gian đánh dấu khác nhằm cải thiện hiệu suất thông tin. Ngoài ra, hệ thống có thể liên quan đến ngoại tuyến, thông tin tổng hợp với dữ liệu tổng hợp khác để cung cấp phân tích xu hướng quản lý phản ứng. Điều quan trọng là phải phân biệt giữa các sự kiện hoạt động và thông số hoạt động, như sau:

– Sự kiện là hiện tượng tức thời hoặc gần tức thời xảy ra trong một dịch vụ hoặc môi trường của nó có ảnh hưởng đến KQI của dịch vụ. Ví dụ như bị mất hoặc sai địa chỉ gói tin, mất tín hiệu, mất điện. Sự kiện có thể được báo hiệu thông qua các cơ chế như bẫy SNMP và ngắt hoặc có thể được suy ra bởi sự mất mát nghiêm trọng của dịch vụ.

– Thông số có nguồn gốc bằng cách xử lý một loạt các phép đo hoặc các sự kiện trong khoảng thời gian đo lường trong một số liệu được xác định có thể được thông báo. Đây có thể là thời gian liên quan, tỷ lệ hoặc mức sự kiện. Ví dụ có tính sẵn sàng, băng thông, sử dụng, thời gian đáp ứng cuộc gọi trung bình và tỷ lệ xung đột mạng Ethernet cho mỗi gói.

– Hệ thống có thể thu thập dữ liệu hiệu suất SLA để tạo thành các báo cáo nội bộ, cái mà có thể được sử dụng để chẩn đoán hiệu suất của các hệ thống cho cả chẩn đoán nội bộ và cả các báo cáo khách hàng. Việc thu thập có thể yêu cầu kết hợp KQI hoặc KPI từ các dịch vụ hoặc sản phẩm, bao phủ bởi các SLA khác nhau, từ các nhà cung cấp tiềm năng khác nhau. Việc thu thập có thể được thực hiện trực tiếp bởi các công cụ thu thập hoặc bằng cách sử dụng các ứng dụng trung gian sử dụng ngôn ngữ

giao diện thông thường như CORBA, XML, hoặc SQL. Thời gian lấy mẫu có thể là thời gian thực, bán thời gian thực, hoặc có liên quan đến lịch sử.

Các báo cáo nội có thể là trong một định dạng khác với các báo cáo bên ngoài để phù hợp với các thủ tục và các công cụ nội bộ. Ngoài ra, hệ thống có thể thiết lập các ngưỡng phù hợp tại các giá trị tích cực hơn so với những định nghĩa trong SLA để đảm bảo hành động khắc phục có thể được thực hiện trước khi nảy sinh sự không phù hợp. Vì lý do này, các báo cáo nội bộ có khả năng tạo ra một cách đều đặn hơn so với các báo cáo bên ngoài, để cho phép hành động khắc phục hậu quả phải được thực hiện để cải thiện hoặc tăng cường hệ thống. Trong một ứng dụng doanh nghiệp đòi hỏi phải có một SLA đa tầng, hệ thống có thể cần phải chứng minh làm thế nào một dịch vụ đã được thực hiện gần đây (thường là một vài giờ) là kết quả của một cuộc gọi hỗ trợ hoặc trong chẩn đoán không phù hợp ở một tầng khác.

Hệ thống nên trình bày báo cáo bên ngoài cho khách hàng trong những khoảng thời gian thích hợp và trong các định dạng đã thống nhất một cách ưu tiên. Doanh nghiệp có thể sử dụng các báo cáo bên ngoài để cung cấp bảo đảm sự phù hợp và phân tích xu hướng phát triển trong tương lai hoặc những cơ hội mới.

Một số nhóm chức năng khác nhau có thể muốn xem các báo cáo quản lý SLA. Đây có thể bao gồm các nhóm quản lý cấp cao có thể được quan tâm với các mục tiêu thành tích cao, nhóm tài chính có thể sẽ được quan tâm đến sự thanh toán và thu phí, nhóm kỹ thuật có thể được quan tâm với chẩn đoán và lập kế hoạch, các nhóm người dùng cuối có thể được quan tâm với CRM. Do đó, định dạng, ngôn ngữ và phong cách của mỗi báo cáo phải phù hợp với từng đối tượng. Ví dụ, đối với quản lý cấp cao, các báo cáo có thể bao gồm các bài trình bày với màu sắc và biểu đồ bảng xếp hạng. Ngược lại, các báo cáo tài chính sẽ bao gồm các bảng tính có thể đọc được bằng máy. Đối với kỹ thuật, các báo cáo sẽ bao gồm các đồ thị xu hướng và dữ liệu thô, cho người dùng cuối thì các báo cáo sẽ bao gồm các báo cáo dựa trên Web.

Quy trình phát triển SLA

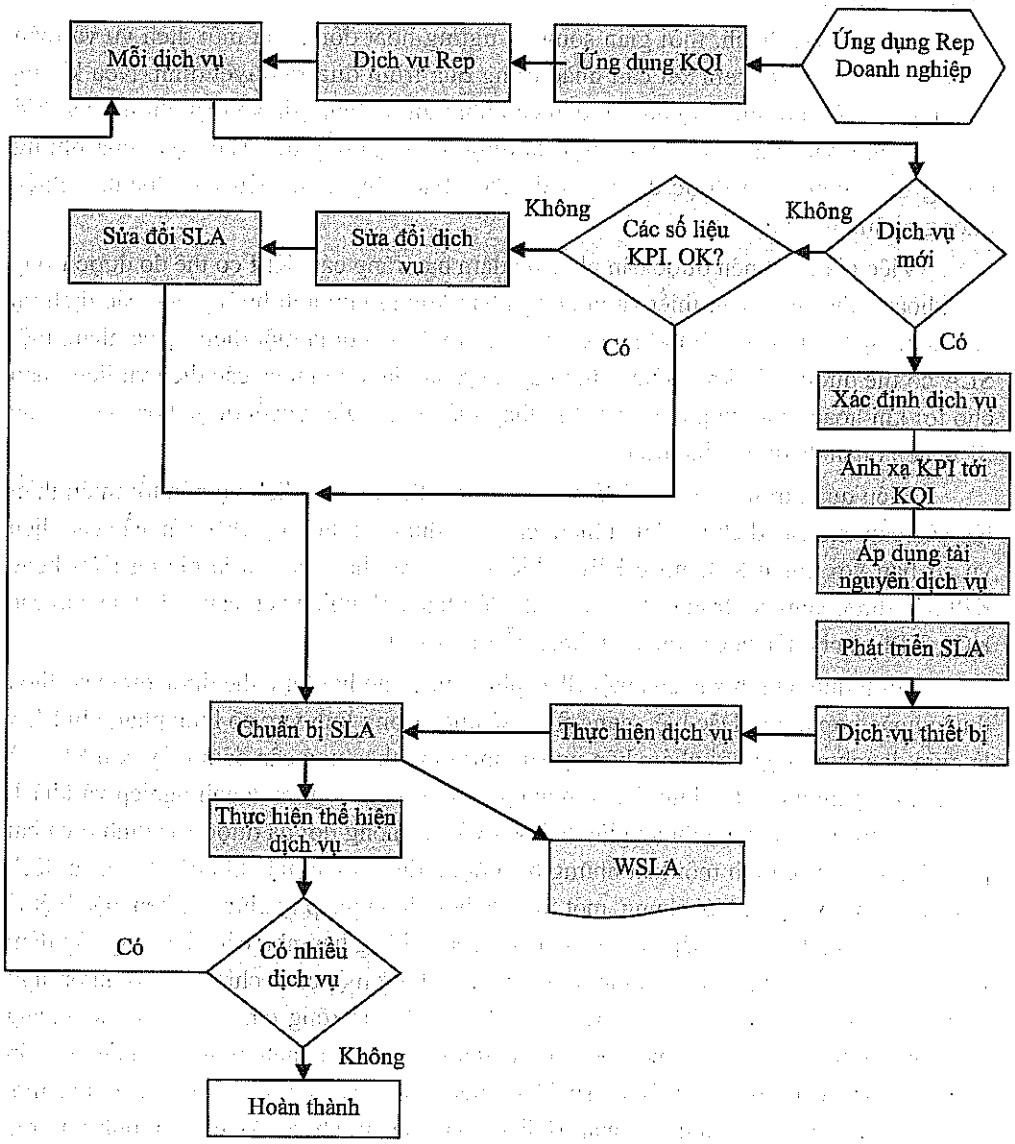
SLAs phụ thuộc rất lớn vào các mục tiêu của doanh nghiệp. Do đó, khó tạo được một định dạng SLA chung áp dụng tới tất cả các doanh nghiệp và các mục tiêu.

Doanh nghiệp làm việc hướng tới những mục tiêu mức cao như một SLA hoặc tập hợp các hỗ trợ SLAs. Quá trình kinh doanh đánh giá lại các mục tiêu đó. Sự xung đột có thể dẫn đến sự sửa đổi các mục tiêu ứng dụng hoặc các yêu cầu, hoặc trong một số trường hợp có thể có những thay đổi tới chính những mục tiêu của doanh nghiệp. Hình 5.6 mô tả một quy trình phát triển của SLA.

Quy trình bắt đầu với sự quyết định kinh doanh, ví dụ từ một người quản lý sản phẩm hoặc mức độ hội đồng, để theo đuổi một cơ hội bằng cách cung cấp một ứng dụng, có thể nói một sản phẩm hoặc dịch vụ tới những khách hàng hoặc đối tác. Trong quy trình kinh doanh thông thường, các mục tiêu của các ứng dụng được xác định. Do vậy các yêu cầu cho ứng dụng là có nguồn gốc. Các yêu cầu ứng dụng được hoàn thành

từ việc thu hồi các sản phẩm và dịch vụ, phát triển một sản phẩm hay dịch vụ mới, sắp xếp các nguồn tài nguyên ngoài, nâng cao sản phẩm và dịch vụ hiện có, hay tích hợp với các sản phẩm dịch vụ mới hoặc đã có.

Nói chung, các ứng dụng cần thiết cho việc kinh doanh và các dịch vụ mạng. Các dịch vụ liên quan được xác định sau đó. Nếu một dịch vụ chưa được sử dụng, khi đó dịch vụ được bắt đầu và một thể hiện được tạo ra cho ứng dụng. Ở đâu dịch vụ đã tồn tại, một thể hiện mới được tạo. Số liệu SLA khi đó có thể được áp dụng tới toàn bộ dịch vụ hoặc thể hiện một phần nào đó.



Hình 5.6. Quy trình xây dựng SLA

Đối với mỗi dịch vụ hoặc thể hiện đã yêu cầu, KQIs của một ứng dụng được xác định và ánh xạ tới các yêu cầu dịch vụ. Điều này cho phép sự định nghĩa của KPIs cho thể hiện dịch vụ, nó có thể được sử dụng trong giám sát và trình bày báo cáo. Những chỉ số khác có thể được bắt nguồn và giám sát cho chuẩn đoán, đề phòng lỗi và giải quyết. Nếu dịch vụ không tồn tại hoặc có yêu cầu sửa đổi các dịch vụ hiện có, các khoảng thời gian, giá và ảnh hưởng tới những ứng dụng và dịch vụ khác thì nên được cân nhắc. Nếu có một xung đột với các yêu cầu cho dịch vụ từ ứng dụng khác, theo quy định của ứng dụng doanh nghiệp, cái đó phải được leo thang thông qua quản lý để giải quyết xung đột.

Chi phí vận hành, thời gian sống và ngừng hoạt động của mỗi dịch vụ và toàn bộ dịch vụ cần được xem xét cân nhắc trong quá trình đưa ra quyết định. Nếu không có xung đột tồn tại, mức độ hướng dẫn cần phải được đánh giá về mặt chi phí và thời gian để đảm bảo nhân viên thích hợp là được đào tạo đầy đủ. Tác động của những hướng dẫn thêm phải được đánh giá để đảm bảo rằng mục tiêu của doanh nghiệp không bị ảnh hưởng.

Việc giám sát nên được cân nhắc để đảm bảo rằng các KPI có thể đo được trong các khoảng thời gian cần thiết và phương pháp không làm ảnh hưởng đến các dịch vụ này hoặc dịch vụ khác. Một khi tất cả các yếu tố được coi là một dịch vụ cá nhân, một SLA có thể được triển khai. Quy trình này được lặp lại cho tất cả các dịch vụ liên quan cho tới khi hoặc một xung đột được tìm thấy mà không giải quyết được hoặc tất cả các SLA liên quan đã được phát triển.

Điều quan trọng cần lưu ý là các KQI và KPI cho các dịch vụ nên tối thiểu thiết lập yêu cầu cho các dịch vụ. Tuy nhiên, các ứng dụng và dịch vụ khác yêu cầu các dịch vụ cơ bản với nhiều KQI hoặc KPI nghiêm ngặt và chặt chẽ, đó là những KQI hoặc KPI nên được xem xét trong SLA. SLA do đó phản ánh nhiều yêu cầu khắt khe cho các KQI, KPI và cho tất cả các dịch vụ được hỗ trợ bởi SLA.

Hình thức chính xác của một SLA phụ thuộc vào hai thực thể được đưa vào thỏa thuận hoặc hợp đồng. Đặc biệt, dạng SLA sẽ khác trong lĩnh vực có hình phạt, khi SLA là giữa doanh nghiệp với nhóm bên ngoài, như một nhà cung cấp đám mây, khi SLA là trong nội bộ giữa các tổ chức doanh nghiệp và khi SLA là giữa doanh nghiệp và khách hàng của họ. SLA là thỏa thuận giữa hai bên với sự mong đợi đã được xác định ở cả hai phía. Nó cũng xác định một loạt những hoạt động được thực hiện khi có những sai lệch xảy ra so với kỳ vọng. Nói chung, một SLA là hợp đồng pháp lý giữa các bên, đặc biệt là cho SLAs giữa doanh nghiệp và đối tác bên ngoài, chẳng hạn như các nhà cung cấp đám mây. Do đó tư vấn pháp lý về hình thức của hợp đồng một cách chính xác và ngôn ngữ được sử dụng là điều rất quan trọng. Nếu SLA là để mở rộng ranh giới quốc tế, chẳng hạn như có thể xảy ra trong một môi trường đám mây, các doanh nghiệp cần đến tư vấn pháp lý cũng cần có hiểu biết về sự khác biệt trong các quy định về hợp đồng, môi trường, việc làm và các thủ tục pháp lý liên quan. Thậm chí SLAs nội bộ, lĩnh vực mà SLA mở rộng ranh giới quốc tế, có thể sẽ cần phải được quan tâm nhiều hơn.

Ngôn ngữ và thuật ngữ đã sử dụng trong SLA nên phù hợp với khán giả. Một danh mục có thể là cần thiết để giải thích các thuật ngữ phổ biến. Nhưng về nguyên tắc, SLA nên được viết theo cách mà nó có thể đọc bởi một số người quan tâm trong dịch vụ hoặc công nghệ cụ thể. Điều này cũng áp dụng cho nhiều tư vấn pháp lý thực hiện trong việc chuẩn bị và đàm phán của một SLA. Nếu SLA được viết giữa các doanh nghiệp hoặc giữa một doanh nghiệp và một nhà cung cấp đám mây, nó như là một ngôn ngữ pháp lý với các điều khoản. Mặt khác, loại ngôn ngữ này có thể cung cấp một cái nhìn không tích cực của doanh nghiệp trong các điều khoản của CE nếu ngôn ngữ này được sử dụng trong SLA giữa doanh nghiệp và người dùng cuối.

Pháp luật có liên quan nên được nêu và xem xét trong việc đàm phán và chuẩn bị của một SLA. Nếu mối quan hệ nhằm mục đích lâu dài và chiến lược, khi đó giao ước chấp thuận giữa hai bên nên được xem xét; nếu chiến thuật khôn khéo, thì nó có thể giúp cho hai bên tạo ra được dự thảo ban đầu. SLA nên rõ ràng, ngôn ngữ dễ hiểu, mục đích của ứng dụng này là cung cấp dịch vụ. Mặc dù không là một phần của hợp đồng chính nhưng điều này có thể giúp cả hai bên hiểu các yêu cầu hơn.

SLA cũng nên chỉ rõ những thành phần của SLA, như sự tồn tại của các mối quan hệ, hợp đồng chính, những báo cáo SLA nên cân nhắc bảo mật vì có thể có lợi thế cạnh tranh trong dịch vụ cung cấp hoặc ứng dụng hỗ trợ. Những phạm vi được cân nhắc bảo mật nên xác định rõ ràng cả về thời hạn của bảo mật đó.

Khi một nhà cung cấp định nghĩa một dịch vụ lần đầu tiên, một mẫu SLA được định nghĩa để hình thành tất cả các thể hiện cơ bản của SLA.

Một bản phác thảo những chủ đề chính để đưa vào SLA được thảo luận trong những mục chấm tròn dưới đây. Hình thức chính xác của SLA phụ thuộc vào một số yếu tố, bao gồm cả khi SLA là một hợp đồng riêng biệt theo đúng nghĩa của nó hoặc là một phần hay phụ lục của một hợp đồng lớn. Nó có thể dễ dàng đàm phán hơn nếu phụ lục được thêm vào SLA cho những dịch vụ mới mà không cần phải đàm phán thương lượng lại các thành phần chính. Trong trường hợp này, SLA nên được viết một cách phù hợp cho dịch vụ đầu tiên.

Giới thiệu: Các tài liệu phần này làm rõ các bên liên quan tham gia vào thỏa thuận SLA. Việc giới thiệu cũng nên có cái nhìn tổng quan ngắn gọn về sự cần thiết của SLA và các ứng dụng và dịch vụ nó phục vụ. Thông tin này nên bao gồm KQI cho ứng dụng và làm thế nào KPIs của dịch vụ hỗ trợ khai báo cho KQI ứng dụng.

Các yêu cầu khách hàng: Các tài liệu phần này nói rõ làm thế nào người dùng sử dụng dịch vụ, nó giải thích rõ ràng những cái gì dịch vụ hỗ trợ. Ví dụ, nếu yêu cầu là hỗ trợ thời gian một vòng đi nhỏ hơn 1 s cho một giao dịch, khi đó nó sẽ cần thiết để hiểu được giá trị cực đại và chiều dài những bùng phát xảy ra của giao dịch đã được dự đoán. Nó có thể là cần thiết để xác định các dịch vụ nên đáp ứng khi nào, trong ví dụ này tỷ giá giao dịch là đã vượt quá.

Tổng quan của dịch vụ: Phần này mô tả dịch vụ bao gồm vị trí vật lý và những giao diện logic giữa hai bên, những người sở hữu đó là một phần của giao diện, số lượng các vị trí và các thông tin khác mô tả dịch vụ hoặc sản phẩm một cách đầy đủ.

Điều khoản: Phần này giới thiệu chi tiết khoảng thời gian SLA có hiệu lực.

Trách nhiệm: Phần này nói chi tiết các trách nhiệm vừa của khách hàng với nhà cung cấp để đảm bảo phù hợp và vừa của nhà cung cấp đối với khách hàng. Kỳ vọng của cả hai bên có thể được trình bày chi tiết trong phần này.

Các chi tiết của dịch vụ: Phần này mô tả các thông số dịch vụ trong điều khoản của KPI vì chúng sẽ được báo cáo cho khách hàng. Phần này có thể làm thành một bảng. Nên hiển thị rõ ràng mức độ hiệu suất có thể chấp nhận được hoặc không phù hợp cùng các điều kiện đặc trưng ngoài.

Các ngoại lệ: Nó là các ngoại lệ cần phải được bao hàm và có tài liệu rõ ràng trong SLA. Khoảng thời gian chết dùng cho việc nâng cấp và bảo trì thường xuyên có thể là cần thiết nhưng cần phải được mô tả với tham số như thời gian thông báo. Trong các môi trường đa web, phải cẩn thận để đảm bảo thời gian chết là rõ ràng. Ví dụ, nếu SLA là giữa doanh nghiệp và nhà cung cấp đám mây, cung cấp giữa trụ sở công ty và văn phòng chi nhánh của nó và tổng số thời gian chết tối đa là 10 giờ mỗi tháng. Nó giống như SLA có thể xác định thời gian chết tối đa của trụ sở chính và các chi nhánh khác.

Mẫu và báo cáo: SLAs xác định tần suất KPIs như một biện pháp phù hợp và thường xuyên được đối chiếu trong hình thức một bản báo cáo để tính toán KQI ứng dụng. Phương pháp báo cáo, ví dụ thông qua web hoặc giấy cũng có thể rất cần thiết. Những báo cáo không phù hợp có thể yêu cầu tần suất khác nhau từ quy trình đối chiếu thông thường. Phương pháp báo cáo không phù hợp cũng có thể khác từ những KPIs bình thường và nên được ghi lại thành tài liệu. Tương tự như vậy, các báo cáo của các sự kiện không đồng bộ như báo động, cảnh báo, bẫy cũng có thể khác nhau và nó có thể là cần thiết để hình thành tần số tối đa của các sự kiện không đồng bộ từ khách hàng hoặc nhà cung cấp.

Báo cáo mẫu cần được thống nhất và đi kèm với tài liệu SLA. Nếu dữ liệu hiệu suất SLA là cần thiết để xác định số liệu hiệu năng KQI và KPI trong thời gian thực hoặc thời gian gần thực, khi đó định dạng của dữ liệu này, giao diện,..., SQL, XML, hoặc CORBA và sự hỗ trợ, tính sẵn sàng, tính toán vẹn, bảo mật cho giao diện cần được xác định. Ngoài ra, nó có thể là lớp các báo cáo cung cấp sẵn với hình thức online hoặc offline. Ví dụ, khách hàng có thể xem các báo cáo SLA cho riêng họ sử dụng. Do vậy, kiểm soát truy cập sẽ phải được đồng ý trong SLA, cùng với khoảng thời gian bao lâu báo cáo này được lưu trữ online hoặc như là một kho chứa.

Các hình thức phạt: Các hình thức phạt không phù hợp nên được chi tiết. Ví dụ như hình thức phạt bao gồm những phí mất, phí phải trả, bồi thường cho thu nhập bị mất và hủy bỏ.

Giải quyết tranh chấp và leo thang: Các tài liệu phần này nói về sự khác biệt giữa các quan điểm trên SLA trong hợp đồng, báo cáo, hoặc hành động được giải quyết. Nó có thể là cần thiết để cung cấp các thông tin liên lạc chi tiết cho những trường hợp đó và cũng để ghi lại những tình huống có thể leo thang để quản lý cấp cao nếu tình huống đó không thể giải quyết được. Đối với SLA giữa các khách hàng hoặc người sử dụng bên ngoài, việc trọng tài có thể là cần thiết. Đối với SLA nội bộ, phần này có thể không có và được giải quyết trong quá trình quản lý thông thường.

Thay đổi các yêu cầu: Phần này chi tiết các thủ tục cho việc thay đổi yêu cầu để SLA có thể thực hiện và xử lý, với nhiều chi tiêu được chi tiết. Tần số tối đa của yêu cầu thay đổi nên được chi tiết. Thời gian thông báo cho các yêu cầu thay đổi nên được ghi lại. Thực hiện các yêu cầu thay đổi có thể gặp phải các điều khoản phạt.

Sự hủy bỏ: Các tài liệu phần này nói về lý do tại sao chấm dứt SLA cùng với thời gian thông báo chấm dứt và các chi phí liên quan. Thời gian thông báo có thể là khác nhau cho SLAs nhà cung cấp tới khách hàng và khách hàng tới nhà cung cấp. SLA cũng nên chỉ rõ những cái sẽ xảy ra trong trường hợp một trong các bên được mua lại bởi một bên khác hoặc doanh nghiệp khác, như vậy các yêu cầu dịch vụ có thể khác với những gì được quy định trong SLAs. Nên xem xét cân nhắc cho việc SLAs nên chấm dứt, tiếp tục hay thương lượng lại.

Pháp luật liên quan: Phần này chi tiết về các luật liên quan sẽ được xem xét trong SLA và quyền hạn giải quyết những vi phạm hợp đồng. Phần này có thể bị thiếu trong hai bên trừ khi hai bên ở hai đất nước khác nhau, có sự khác biệt đáng kể trong hệ thống luật liên quan và thực hiện dịch vụ giữa các nước khác nhau.

Bảo mật: Phần này chi tiết và làm nổi bật rõ những khía cạnh của SLA như là sự tồn tại của nó, hiệu suất, các báo cáo, dữ liệu báo cáo, chúng là bí mật.

Bảo hành: Phần này chi tiết về các phạm vi được bảo hành. Những nơi bảo hành đã có sẵn một số tài nguyên dịch vụ, làm thế nào để chi tiết những hiệu lực của SLA.

Bồi thường và hạn chế trách nhiệm pháp lý: Phần này chỉ rõ ai là người chịu trách nhiệm trong kết quả thất bại của SLA, hoặc là nhà cung cấp hoặc là khách hàng.

Các ký kết: SLA nên đề ngày và được ký bởi các bên liên quan tới SLA.

5.3. ĐẢM BẢO CHẤT LƯỢNG DỊCH VỤ

Các ngành công nghiệp dịch vụ truyền thông kỹ thuật số cung cấp dịch vụ thông qua một chuỗi giá trị hoặc một hệ sinh thái của các bên đối tác và các nhà cung cấp dịch vụ. Cung cấp trải nghiệm chất lượng cao cho khách hàng trên chuỗi giá trị phức tạp được hỗ trợ bởi một hệ sinh thái đòi hỏi các bên đối tác để đo lường sự hài lòng của khách hàng, kiểm soát thỏa thuận cấp độ dịch vụ, xác định các vấn đề trên toàn chuỗi giá trị hoặc hệ sinh thái và phân bổ các khoản thanh toán trong khi duy trì sự an toàn. Vì vậy, một khung quản lý chất lượng dịch vụ cần phải xác định một khung toàn diện

để đo lường và quản lý hiệu quả chất lượng dịch vụ; số liệu chất lượng dịch vụ quan trọng tại mỗi điểm dọc theo mạng lưới cung cấp dịch vụ; vấn đề chất lượng dịch vụ và kế toán cần thiết; thông tin hạ giá, thông tin sử dụng và các thông tin giải quyết vấn đề; khả năng quản lý để hỗ trợ từng bước trong mạng lưới phân phối dịch vụ; giao diện thích hợp và giao diện ứng dụng để cho phép trao đổi thông tin điện tử giữa các nhà cung cấp khác nhau trong mỗi chuỗi giá trị dịch vụ.

Trong một chuỗi giá trị, mỗi mối quan hệ giữa một nhà cung cấp và một khách hàng có thể được mô hình hóa như một khách hàng có những nhu cầu cụ thể. Những nhu cầu này thường được lấy trong một số mẫu của một thỏa thuận cấp độ dịch vụ. Những thỏa thuận cấp độ dịch vụ đã được thảo luận chi tiết trong chương 5.

Trong một môi trường đám mây, các doanh nghiệp mong đợi chất lượng tốt nhất có thể từ các nhà cung cấp đám mây để vượt qua một chất lượng tương tự như các khách hàng doanh nghiệp. Hơn nữa, những dịch vụ mới dự kiến sẽ có độ phức tạp cao hơn trong chuỗi cung cấp dịch vụ end-to-end (coi trọng đến điểm đầu và điểm cuối, không quan tâm nhiều đến các bước trung gian) hơn những dịch vụ hiện tại. Chất lượng của kinh nghiệm mà khách hàng nhận thức được thì phụ thuộc vào nhiều yếu tố, chẳng hạn như các yếu tố về hành vi và hình ảnh, tiếp thị, các thành phần cài đặt dịch vụ, các quá trình kinh doanh liên quan đến dịch vụ, nguồn tài nguyên được hỗ trợ, hiệu suất của mạng và các ứng dụng cơ bản. Vì vậy, để định lượng chất lượng cảm nhận của kinh nghiệm, các nhà cung cấp dịch vụ nên biết khách hàng chủ chốt các số liệu để đánh giá CE, KQI (chỉ số chìa khóa chất lượng), KPI (chỉ số chìa khóa hiệu suất) cho các mạng và dịch vụ.

Mục 5.1 và mục 5.2 đã thảo luận về các dịch vụ và SDFs (các khung phân phối dịch vụ). Mô hình quản lý cho các mạng và dịch vụ công nghệ thông tin trình bày mô hình tài nguyên gần gũi hơn với một cái nhìn dịch vụ hơn là một tiếp xúc đơn giản của các thành phần chi tiết được sử dụng để thực hiện các dịch vụ. Bằng cách sử dụng các mô hình tài nguyên, các mô hình quản lý có thể cung cấp khả năng dự báo về năng lực và dịch vụ lập kế hoạch, dịch vụ dự phòng tài nguyên đưa vào tài khoản CE và các mục tiêu, bao gồm cả dịch vụ bảo đảm cảnh báo vi phạm SLA (thỏa thuận cấp độ dịch vụ) và vượt ngưỡng, sử dụng và thanh toán dịch vụ.

Chuỗi giá trị quản lý chất lượng dịch vụ

Từ một quan điểm chuỗi giá trị, một SQM (quản lý chất lượng dịch vụ) hỗ trợ một tập các APIs và các số liệu cho các bên đối tác, chẳng hạn như một doanh nghiệp và các đối tác cung cấp đám mây của mình, để thu thập, xử lý và trao đổi thông tin. Dữ liệu này được sử dụng để quản lý và báo cáo chất lượng dịch vụ end-to-end cung cấp cho người dùng cuối tại các điểm truy cập dịch vụ và hỗ trợ quản lý các thỏa thuận cấp độ dịch vụ giữa các đối tác và khách hàng cuối. Hình 5.5 biểu diễn các thành phần cần thiết của quan điểm chuỗi giá trị của quản lý chất lượng phần mềm. Quan điểm các miêu tả về vài ứng dụng như sau:

– CRM Applications: Các ứng dụng này giữ các thông tin về khách hàng và các mối quan hệ hoặc nhóm trong số đó. Các ứng dụng này cũng có một lịch sử các sự cố và các số liệu đánh giá sự hài lòng của khách hàng.

– Value add CE/SQM Applications: Các ứng dụng này có thể lấy được nhiều mẫu khác nhau. Một mẫu là cho các ứng dụng đơn giản để tổng hợp thông tin từ nhiều nguồn và hiển thị chúng dưới dạng phù hợp trong một khoảng thời gian phù hợp trên một bảng điều khiển quản lý. Mục tiêu là để đánh dấu tầm quan trọng của các sự cố và quan sát các xu hướng. Một mẫu khác thì dành cho các ứng dụng phỏng đoán hoặc thuật toán xử lý các phép đo nguồn lực để dự đoán hiệu suất dịch vụ,..., hiệu suất của tính năng sản phẩm. Còn có mẫu khác nữa thì dành cho các ứng dụng tương quan và tối ưu hóa các nguồn lực, các phép đo dịch vụ có nguồn gốc từ lịch sử sự cố của khách hàng để tối ưu hóa các hoạt động dịch vụ đó. Mục tiêu là để nâng cao sự hài lòng của khách hàng và đánh giá số liệu CE.

– Resource Management Applications: Các ứng dụng này cung cấp các dịch vụ mạng trừu tượng, ứng dụng CNTT và nguồn lực CNTT.

– Edge Application Probes: Các ứng dụng này hỗ trợ giám sát chủ động sự trải nghiệm dịch vụ bởi khách hàng tại các điểm truy cập dịch vụ.

– Network Probes: Các ứng dụng này giám sát hiệu suất kỹ thuật của tài nguyên mạng và cung cấp chức năng chẩn đoán. Ví dụ, các chức năng giám sát chất lượng mạng, chẳng hạn như tỷ lệ lỗi hoặc sự tiềm tàng lỗi trong các giai đoạn phân tích, cờ báo xuất hiện khi các phép đo hiệu suất vượt quá ngưỡng quy định, áp dụng điều kiện kiểm tra chẩn đoán và báo cáo lại các kết quả của các kiểm tra chẩn đoán.

– Applications Probes: Các ứng dụng này giám sát hiệu suất kỹ thuật của tài nguyên ứng dụng, cung cấp một tập hợp các tiêu chuẩn giám sát và chức năng chẩn đoán tương tự như cho mạng. Nó có thể bao gồm các biện pháp trì hoãn ứng dụng, xử lý, và lưu trữ sử dụng.

Số liệu quản lý chất lượng dịch vụ (SQM)

Số liệu SQM hiện nay được sử dụng để tạo đầu vào cho việc giám sát và phân tích các ứng dụng doanh nghiệp lái xe hoặc bảng điều khiển SP trong việc hỗ trợ các chức năng dịch vụ và quản lý khách hàng. Số liệu nhằm vào việc bảng điều khiển chỉ cần thể hiện xu hướng đáng tin cậy, không cần phải hoàn toàn chính xác, một số đo lường giả tạo hoặc lỗi có thể chấp nhận được.

Số liệu thì trao đổi giữa doanh nghiệp và các nhà cung cấp đám mây, nhưng các số liệu cần phải được xác định đến mức mà các phép đo được thực hiện bởi một tổ chức với một công cụ có thể so sánh trực tiếp với các phép đo được thực hiện bởi tổ chức khác sử dụng một công cụ khác. Điều này không chỉ bao hàm việc xác định các phương pháp đo lường, mà còn đòi hỏi kiểm định cả công cụ và tổ chức để đảm bảo rằng các phép đo tạo ra có thể so sánh được.

CE và số lượng chất lượng được thu thập trong khối lượng rất cao và vì những lý do thực tế, nó là cần thiết để tổng hợp chúng trong một số hình thức thích hợp. Thông thường, các số liệu tổng kết đại diện cho các giá trị trung bình, tỷ lệ phần trăm theo thời gian hoặc giá trị các biện pháp dưới đây hoặc trên một ngưỡng và tỷ lệ chung. Thông thường, các số liệu được sử dụng để hỗ trợ chức năng hoạt động như mạng lưới hoạt động và các hoạt động dịch vụ cho các đại diện dịch vụ khách hàng và quản lý sản phẩm, nơi những tóm tắt thống kê được sử dụng trong các báo cáo và bảng điều khiển trên đường thiết lập xu hướng và các mẫu. Nơi các số liệu từ các tổ chức cá nhân được trao đổi qua các giao diện để ước tính hiệu suất tổng thể quá trình đầu – cuối trong một chuỗi giá trị, như trái ngược với trực tiếp đo với đầu dò, các số liệu cần phải được trình bày khác so với trung bình và ngưỡng truyền thống. Ví dụ, nếu dịch vụ hoặc sản phẩm có sẵn tính năng số liệu, cần được tính toán từ một số biện pháp nguồn lực có sẵn, như đã thấy trong SDF thảo luận ở chương 5, sau đó tính toán nhu cầu thông tin về phụ thuộc giữa các nguồn lực và các sản phẩm hoặc các tính năng dịch vụ. Tương tự như vậy, nó cần cơ chế khả năng phục hồi nguồn lực để ngăn chặn thất bại của một nguồn tài nguyên ảnh hưởng đến tính năng của sản phẩm, xác suất có điều kiện trong các sự kiện từ các nguồn tài nguyên, chẳng hạn như mức độ độc lập của các sự kiện thống kê... Tính toán thống kê có giá trị cần phân phối được các đặc trưng và xác suất có điều kiện để được ước tính. Lý tưởng nhất là dữ liệu thô được cung cấp như thực tế nhưng một số cắt giảm dữ liệu thì có thể cần thiết.

Để tính toán tổng thể trung bình quá trình đầu – cuối từ giá trị trung bình các miền phụ cá nhân, điều này bao gồm việc so sánh các số đo với các chuẩn đo lường; ước lượng cho các chức năng phân phối xác suất bằng cách sử dụng các phương pháp như phân bổ xác suất cụ thể (Binomial, Poisson, Normal) hoặc phân phối tổng quát (Kurtosis); và ước lượng cho xác suất có điều kiện, mức độ độc lập của các bản phân phối độ miền phụ được đánh giá trong các tổ chức khác nhau. Ví dụ, các báo cáo SLA phải có số liệu vượt quá hiệu suất, trong hiệu suất và dưới tỷ lệ phần trăm hiệu suất. Mặt khác, để trình bày cho mạng và các hoạt động dịch vụ, thông tin chi tiết, hoặc thậm chí dữ liệu thô và một số dấu hiệu của sự sai lệch của phân phối sự kiện là cần thiết.

Hệ thống khảo sát đánh giá dịch vụ

Hệ thống khảo sát là một công cụ cơ bản cho các nhà khai thác mạng và các nhà cung cấp dịch vụ SPs để giám sát và quản lý QoS. Khảo sát có thể được đặt ở bất kỳ điểm nào trong mạng, do đó họ cung cấp một sự linh hoạt lớn hơn các hệ thống dựa trên các thành phần mạng hoặc các nguồn dữ liệu khác. Hoạt động khảo sát đánh giá đưa lưu lượng truy cập vào trong mạng và gửi yêu cầu đến các máy chủ dịch vụ như một người dùng cuối. Chúng thường được sử dụng để cung cấp một cái nhìn end-to-end. Mặt khác, các gói tin thăm dò thụ động được phát hiện từ các dịch vụ khác nhau. Chúng chỉ có thể cung cấp cái nhìn của một phần của mạng ở nhiều cấp độ giao thức khác nhau. Việc khảo sát tạo ra một công cụ giám sát duy nhất cho tất cả các dịch vụ

cho phép các hệ thống để đánh giá QoS và có thể liên quan đến các thông tin từ các biện pháp và dịch vụ khác nhau. Đặc biệt, khảo sát cung cấp các chức năng sau:

– Giám sát mạng thời gian thực: Bằng cách liên tục theo dõi tình trạng của các thành phần mạng và lưu lượng, chất lượng các thông số, thất bại có thể được phát hiện và phân tích tác động của chúng trong thời gian thực.

– Quy hoạch mạng dựa trên dữ liệu cập nhật: Dữ liệu lưu lượng truy cập đạt được thông qua thăm dò chi tiết có thể được sử dụng để lập dự toán quy hoạch mạng như khả năng định tuyến.

– Kiểm soát chi tiết sử dụng mạng: Khảo sát có thể giám sát các loại và lưu lượng truy cập, cái mà có thể giúp ngăn chặn việc lạm dụng sử dụng từ khách hàng hoặc đối tác.

– Quản lý hiệu năng: Khảo sát có thể đo các thông số như số lượng cuộc gọi, chuyển vùng nỗ lực, yêu cầu để được tư vấn đến các nền tảng mạng thông minh và thống kê thất bại. Bằng cách này, trong trường hợp một tham số chất lượng vượt quá ngưỡng được xác định trước, hệ thống có thể thông báo cho người sử dụng và cung cấp đầy đủ dữ liệu để mô tả chính xác vấn đề.

Dữ liệu cho dịch vụ thanh toán: Khảo sát có thể hoạt động như một hệ thống hỗ trợ thanh toán bổ sung. Kể từ khi thăm dò được tiếp cận với lưu lượng mạng, hệ thống thăm dò cơ sở có thể tái tạo lại các dịch vụ được thực hiện bởi một người dùng và do đó sẽ xác minh được hóa đơn.

Hệ thống khảo sát cơ sở diễn ra tại các điểm cụ thể trên các hệ thống mạng, nơi mà các thông tin được tạo ra bởi mẫu dò nhận được và trước khi xử lý trong các trang web từ xa, thường thăm dò theo cách tự nhiên, do đó các trang web từ xa đã xây dựng các lưu lượng và chất lượng đo lường cụ thể. Ngoài ra, khung lấy được một số lượng cấu hình thời gian cũng được lưu trữ trong các trang web từ xa, bởi vậy sau đó họ có thể truy cập để phục vụ cho việc nghiên cứu của những báo cáo bất thường. Đo từ các trang web từ xa được gửi đến một hệ thống trung tâm để xử lý, nhóm và tương quan. Ngoài ra, dữ liệu từ các trang web từ xa được hợp nhất trong một cơ sở dữ liệu trong hệ thống trung tâm.

Kiến trúc này liên quan đến việc thăm dò sự hỗ trợ từ xa, một mặt là các giao diện card mạng thụ động, mặt khác là thăm dò hoạt động tạo ra từ đầu đến cuối phiên. Ngoài ra còn thăm dò thụ động việc giám sát lưu lượng truy cập trực tiếp qua mạng và tiến hành một loạt các phép đo chất lượng cuộc gọi. Hai loại của các đơn vị thăm dò có thể được hình dung: tổ chức thăm dò khách hàng, trong đó mô phỏng hành vi của dịch vụ khách hàng và các thực thể mạng thăm dò. Mạng này không xâm nhập thu thập bên trong mạng lưu lượng thực tế mà khách hàng tạo ra khi sử dụng các dịch vụ. Cả hai đơn vị cung cấp khai thác với khả năng lập kế hoạch đầy đủ để thiết kế tự kiểm tra. Kiểm tra dịch vụ sau đó có thể được sử dụng để xây dựng các báo cáo QoS.

5.4. KIỂM SOÁT LỖI DỊCH VỤ VÀ ĐỘ TIN CẬY

Kiểm soát lỗi dịch vụ

Business Service Fabric (BSF) là một mô hình cho sự ảo hóa không đồng bộ và sự trừu tượng hóa của các dịch vụ, ứng dụng, chính sách, khả năng, tài nguyên, cơ sở hạ tầng và con người. Trong mô hình BFS, những thực thể được đề cập đến có thể được phân một cách hợp lý và thực tế tới các vùng ảo đã phân phối của Business Service Sub-Fabrics (VBSFs). Một BSF có thể nối công ty, địa lý, các ranh giới công nghệ, các đám mây công cộng hoặc riêng tư và các trung tâm dữ liệu doanh nghiệp. Cầu nối giữa VBSFs được cung cấp bởi các dịch vụ hòa giải trung gian. Quản lý và điều khiển các tương tác inter-sub-fabric, quản lý các giao thức, bao gồm các chuyển đổi giao thức và giám sát quản lý sub-fabric cơ bản. Trong kinh doanh, các dịch vụ hòa giải sub-fabric quản lý tương tác giữa các môi trường đối tác.

Các khái niệm BSF và VBSF là một tập hợp ảo các dịch vụ kinh doanh, từ các nguồn khác nhau, trong môi trường các dịch vụ mạng cho phép nhất quán sử dụng, quản lý và khả năng hoạt động. Trong một VBSF, các thiết lập đa dạng, riêng biệt của dịch vụ làm việc cùng với nhau để thực hiện một vài nhiệm vụ trong khi đang giao tiếp trên ngăn xếp giao thức các dịch vụ kinh doanh.

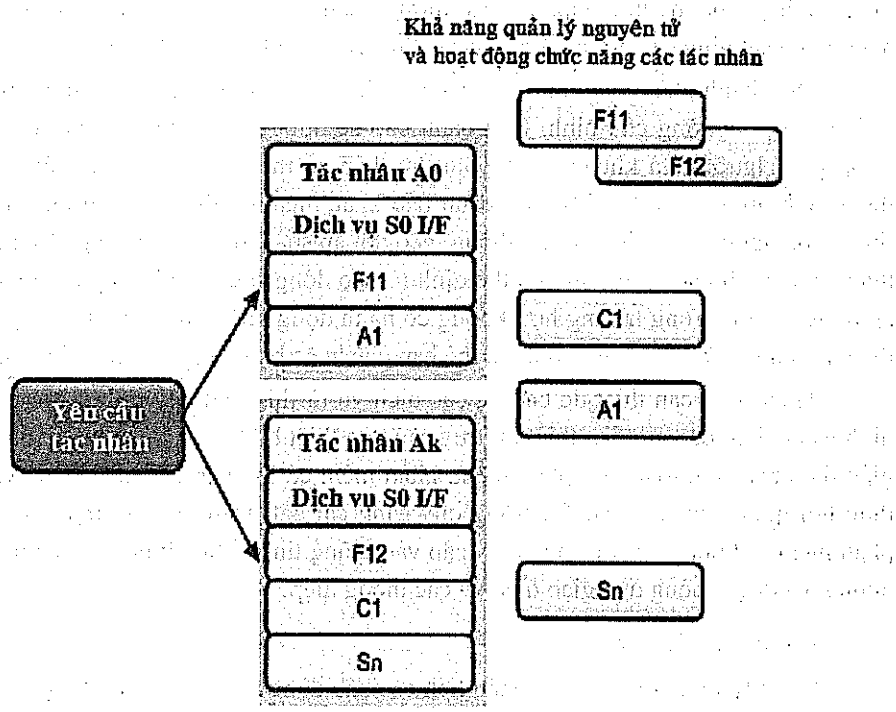
Trong mô hình BSF, mọi người dùng,..., người dùng cuối của dịch vụ, các nhà phát triển dịch vụ, hoặc người quản trị hoạt động trong BFSs cho phép và mỗi BSF người dùng được cấu hình bao gồm các VBSFs cần thiết. Một BSF ẩn các đặc điểm của những nguồn tài nguyên cơ bản từ các hệ thống dịch vụ, ứng dụng và người dùng cuối khác với các tài nguyên đó. Người sử dụng là cô lập, môi trường dịch vụ đầy đủ chức năng dựa trên quyền lợi và vai trò của họ.

Một phương pháp phổ biến để tạo máy ảo (VM) trong môi trường đám mây chia tách hệ điều hành tới những hệ thống rời rạc, một *hypervisor* quản lý các VMs và một SDF cho việc quản lý ứng dụng và cung cấp các dịch vụ cần thiết. Dịch vụ kinh doanh liên kết hoặc chỉ sử dụng các dịch vụ cần thiết từ các hệ thống BPM, hệ thống cơ sở dữ liệu, middleware frameworks,... Các dịch vụ kinh doanh cũng sử dụng các dịch vụ hoạt động và quản lý kinh doanh như quản lý lỗi, cấu hình, tài khoản, hiệu suất và bảo mật.

Một quy trình là một bộ điều phối các hoạt động hợp tác để cung cấp một số đầu ra cụ thể. Các quy trình có thể bao gồm tương tác, cộng tác với các quy trình khác. KPI có thể được giám sát để xác minh các hành động trong quy trình kinh doanh là đang được thực hiện, mục tiêu mong đợi và kết quả đạt được. Các màn hình KPI là các dịch vụ có thể là trong hoặc ngoài. Hành động, chính sách định hướng hoàn hảo và được tự động được thực hiện khi có khoảng cách giữa sự mong đợi và kết quả đạt được. Các quy trình, tài nguyên, thông điệp và con người cũng thường được coi như dịch vụ. Sub-fabrics hạn chế các sự tương tác có thể, các loại tài nguyên, vị trí và tùy chọn khả năng quản lý, hoạt động. Như vậy, tính di động có thể được giới hạn tới việc thực hiện

dịch vụ hoặc tác nhân, middleware, các phân đoạn mạng, các thiết bị khách hàng, các máy chủ tính toán và máy chủ dữ liệu. Một dịch vụ có thể được thực hiện bởi nhiều tác nhân, những tác nhân có khả năng nhất định. Ví dụ, các tác nhân sẽ khác nhau theo luật của các nước khác nhau. Sự lựa chọn các tác nhân cung cấp phụ thuộc vào khả năng, hiệu suất, chính sách quản lý và các cân nhắc chi phí của tác nhân.

Các chính sách ràng buộc các hành vi và việc sử dụng nguồn tài nguyên áp dụng cho các tác nhân. Các dịch vụ thực hiện bởi các tác nhân bên ngoài hoặc kết hợp với một dịch vụ quản lý thực thi các chính sách. Một tác nhân (A0) thực hiện một dịch vụ (S0) có thể bao gồm một số tác nhân dịch vụ quản lý tập hợp các khả năng của tác nhân (A0) như trong hình 5.7 và thiết lập của các tác nhân dịch vụ quản lý bên ngoài.



Hình 5.7. Kiểm soát lỗi dịch vụ

Chỉ những chính sách nhất định là quản lý nội bộ, trong khi những chính sách khác có thể yêu cầu điều phối và quản lý ngoài. Ví dụ, các tác nhân quản lý ngoài có thể thực thi các chính sách cho ứng dụng mang tính di sản kế thừa.

Các nền tảng đa dịch vụ trình bày các nhu cầu duy nhất trên các hệ thống quản lý sự kiện vì khối lượng giao thông chúng xử lý và số lượng báo động có thể tạo ra. Một thành phần quản lý sự kiện trong một dịch vụ quản lý có thể hỗ trợ sự kiện tương quan và lọc chúng để giảm bớt những sự kiện không cần thiết. Lọc sự kiện và các

chính sách tương quan xác định lọc và thực hiện mối tương quan. Một chính sách tương quan có thể được xác định liên kết tất cả các sự kiện tới một sự kiện gốc đã có trong một khoảng thời gian quy định. Kết quả là, chỉ sự kiện gốc là được chuyển tiếp, do đó làm giảm tình trạng quá tải báo động về trên hệ thống quản lý.

Thiết bị đo đạc và giao diện quản lý của một dịch vụ là những khía cạnh quan trọng của quản lý. Dịch vụ sẽ không thể quản lý được nếu không có các thiết bị phù hợp để cung cấp thông tin và kiểm soát. Một hệ thống quản lý ngoài có thể cấu trúc và khởi tạo một truy vấn cho tất cả các thiết bị đo lường trạng thái và phân tích. Giám sát hoạt động tập trung và định hướng là khó để biểu diễn năng động, quy mô lớn trong môi trường phân phối. Trong các hệ thống giám sát tập trung, khối lượng dữ liệu được cung cấp sẵn từ một số lượng lớn các dịch vụ, có thể là quá cho cho các thành phần giám sát hiệu suất để thu thập, lưu trữ, tương quan và xử lý. Bằng cách phân vùng khả năng giám sát giữa các nơi ảo, khối lượng dữ liệu sẽ có thể quản lý được.

Một thành phần màn hình của các màn hình người quản lý sự kiện có thể không phù hợp với ngưỡng cấu hình. Một cảnh báo sẽ được đưa ra bất cứ lúc nào ngưỡng vượt quá. Ngưỡng và khoảng thời gian thu thập có thể được cấu hình riêng cho mỗi thuộc tính được theo dõi. Mức độ cảnh báo khác nhau có thể tăng lên khi một thuộc tính có đa ngưỡng. Ví dụ, một hệ thống theo dõi áp suất có thể có các ngưỡng: rất thấp, thấp, cao và rất cao. Quy định có thể định rõ báo động sau khi ngưỡng điều kiện được áp dụng. Ví dụ, trong trường hợp không có hành động khắc phục, giá trị thuộc tính có thể lên trên ngưỡng, các quy định có thể hạn chế hoặc báo động hơn nữa được tạo ra.

Thiết bị là cần thiết để bảo vệ các dịch vụ từ thiệt hại gây ra bởi các vấn đề an ninh và để đảm bảo an toàn thiết bị, truy cập vào thiết bị đó cũng phải được bảo vệ. Để giúp đảm bảo tính toàn vẹn phần mềm, phần mềm có thể nạp các chữ ký số và chứng thực bởi người quản lý cài đặt trong quy trình cài đặt. Nếu không được xác thực thì phần mềm sẽ không chạy được. Truy cập vào thông tin và điều khiển kích hoạt thiết bị nhúng đạt được thông qua giao diện và các thông điệp.

Độ tin cậy dịch vụ

Quản lý lỗi là thu thập và phân tích các báo động và lỗi trong dịch vụ. Các lỗi có thể là tạm thời hoặc lâu dài. Lỗi tạm thời sẽ không báo động nếu nó xảy ra mà không vượt quá ngưỡng. Ví dụ, thông điệp không thường xuyên hoặc chậm trễ. Tuy nhiên, những sự kiện này đã được ghi vào nhật ký hoạt động (log). Một vài vấn đề tạm thời có thể tự động sửa chữa ngay bên trong dịch vụ, trong khi những cái khác có thể yêu cầu các mức độ giải quyết khác nhau của dịch vụ quản lý. Lỗi có thể được xác định từ tin nhắn báo động hoặc bằng cách phân tích Log.

Phân tích quản lý lỗi và lọc thông báo lỗi, điều phối các thông điệp, do vậy số các sự kiện thực tế phản ánh điều kiện thực tế của dịch vụ. Nguyên nhân nguồn gốc gây ra là được báo cáo, trong khi bỏ qua các thông báo lỗi có liên quan. Trong khi

tất cả các lỗi được ghi lại trong log và quản lý lỗi ở một số lớp có thể giải quyết được các lỗi, người quản lý giải quyết lỗi tạo ra một bản ghi ghi lại chi tiết các lỗi và các hành động khắc phục đã thực hiện. Ví dụ, trong khi quản lý lỗi có thể có quyết định một tài nguyên dịch vụ riêng Ra bị thất bại và thay vào đó là sử dụng tài nguyên Rb. Khi đó Ra vẫn cần phải được sửa lại. Đối với mỗi dịch vụ, có một ánh xạ tới các dịch vụ cơ bản và tài nguyên để theo dõi những lỗi, thất bại của dịch vụ và tài nguyên đó. Ví dụ, trong trường hợp của thông điệp đầu vào được xây dựng từ các dịch vụ chức năng khác. Lỗi có thể được sửa hoặc giảm nhẹ bằng cách cung cấp một hoặc nhiều các thể hiện dịch vụ và phân phối giữa các bản sao khác nhau. Tuy nhiên, nếu hàng đợi thông điệp đầu ra đang phát triển, khi đó lỗi có thể là các dịch vụ nhận, dịch vụ tin nhắn, một hoặc nhiều tài nguyên cơ bản thực hiện các dịch vụ tin nhắn. Chuẩn đoán của các dịch vụ khác nhau có thể xác định được dịch vụ cần được giải quyết. Do đó, nếu lỗi là do tắc nghẽn mạng, khi đó cung cấp một đường dẫn mạng thay thế có thể khắc phục được sự cố.

Ảnh hưởng của lỗi làm kết quả sai hoặc kết quả không đáp ứng được yêu cầu hiệu suất. Hai phương pháp thường được sử dụng để phát hiện lỗi là: chấp nhận kiểm thử và so sánh kiểm thử.Trong chấp nhận kiểm thử, dịch vụ được chạy với đầu vào đã biết, kết quả thực tế được so sánh với kết quả mong đợi với các đầu vào nhất định. Kiểm thử so sánh được sử dụng trong một môi trường mà nhiều phiên bản của dịch vụ được chạy đồng thời, kết quả từ tất cả các phiên bản với cùng một đầu vào được so sánh, kết quả phần lớn hơn sẽ được chấp nhận.

Một dịch vụ quản lý lỗi đang hoạt động, có thể đang ở mức độ kém đi trong việc hiển thị các lỗi. Đối với dịch vụ mà lỗi của nó còn khoan dung được nếu nó còn có khả năng phát hiện, chẩn đoán, chứa, bồi thường và phục hồi từ các lỗi,... nghĩa là nó phải có khả năng tự quản lý.

Cô lập lỗi là quá trình xác định nguyên nhân gây ra lỗi hoặc chính xác thành phần nào bị lỗi. Trong kiểm thử so sánh, cô lập lỗi yêu cầu một số lẻ các phiên bản chạy đồng thời, và sau đó đa số phiếu sẽ dùng để cô lập phiên bản bị lỗi. Trong thiết kế tốt, các dịch vụ chịu lỗi. Lỗi được chứa trước khi họ tuyên truyền quảng bá mức độ ảnh hưởng của dịch vụ cung cấp. Điều này khiến một phần dịch vụ không sử dụng được vì các lỗi còn sót lại. Nếu lỗi tiếp theo xảy ra, dịch vụ không thể đối phó vì mất các tài nguyên, trừ khi các nguồn tài nguyên được thu hồi thông qua các quy trình phục hồi. Một dịch vụ có thể che khuất lỗi ngay cả trong khi lỗi xảy ra, chỉ những kết quả hợp lệ được truyền vào dịch vụ nơi mà người dùng tác động ảnh hưởng. Ví dụ trong trường hợp của một cuộc điều tra số dư tài khoản, dữ liệu hợp lệ cuối cùng, ngày và thời gian là được trình bày cho người dùng. Nếu một lỗi xảy ra và giới hạn trong một thành phần nào đó, nó có thể cần thiết cho dịch vụ để cung cấp các hồi đáp cho đầu ra của thành phần bị lỗi. Điều này có thể có trong những tình huống nhất định, chẳng hạn như khi

báo cáo cân nặng, khi đó thành phần cân bằng được xác định để nhất quán trả về cân nặng thực tế cộng với một số lượng cố định đã biết.

Khi một dịch vụ hoàn toàn thất bại, phục hồi có thể dẫn tới khởi động lại dịch vụ. Cấu hình quản lý khởi động lại dịch vụ dựa trên quy trình phục hồi xác định cho dịch vụ đó. Cấu hình quản lý có thể cung cấp một dịch vụ phục hồi sẽ thực thi các ràng buộc phục hồi trên trình tự thông điệp, tình trạng nhất quán và tiến hành giao tiếp với các bên liên quan.

Khả năng quản lý là kết quả tổng hợp của một số khía cạnh khác nhau, bao gồm, tính sẵn có, khả năng mở rộng, tối ưu hóa hiệu suất, độ tin cậy, quản lý rủi ro, quản lý kinh doanh và quản lý thay đổi. Nhiều hệ thống cần được thường xuyên quản lý, có nhiều bước trong hoạt động quản lý. Các bước có thể dài hoặc ngắn.

Các dịch vụ kinh doanh thích ứng với môi trường thông qua các thành phần hoặc bằng cách tương tác với các dịch vụ thích hợp. Các chính sách dịch vụ là có sẵn và yêu cầu khả năng mở rộng, tối ưu hóa hiệu suất, giám sát và an ninh. Các dịch vụ có khả năng mở rộng liên tục và tính sẵn sàng cao thông qua việc nhân rộng dịch vụ. Dịch vụ cung cấp trực quan hiệu suất của chúng, đặc biệt cùng với KPI thông qua sự kết hợp các thành phần và các dịch vụ giám sát bên ngoài.

Một dịch vụ có thể quản lý được khi nó cho thấy một tập các hoạt động quản lý hỗ trợ cho khả năng quản lý. Những hoạt động này chỉ có thể tiếp xúc với các dịch vụ với sự phân quyền cần thiết. Các hoạt động quản lý cung cấp cho giám sát, kiểm soát và báo cáo chức năng, ngoài khả năng quản lý chính sách, tác nhân có thể báo động trên những hành vi vi phạm chính sách. Thông tin có thể được cung cấp để đáp ứng một truy vấn quản lý trên số yêu cầu và hồi đáp, thời gian bắt đầu và kết thúc,... Giao diện của dịch vụ chỉ rõ khả năng quản lý được hỗ trợ lên màn hình. Mặc dù việc cung cấp khả năng quản lý cho phép một dịch vụ có thể quản lý được, phạm vi và mức độ quản lý được quy định trong chính sách quản lý được liên kết với dịch vụ. Do đó, chính sách quản lý sử dụng để xác định quyền, nghĩa vụ, quản lý dịch vụ.

Khả năng quản lý và hoạt động của dịch vụ được đơn giản hóa khi dịch vụ hoạt động trong các môi trường có quản lý và xác định. Một hệ sinh thái quản lý hỗ trợ tập hợp quá trình và hoạt động cần thiết để chuyển giao dịch vụ và vận hành chúng nhằm đáp ứng một số mục tiêu của dịch vụ. Trong một hệ sinh thái quản lý, có ít nhất một tác nhân làm người quản lý và ít nhất một tác nhân khác là tác nhân được quản lý. Người quản lý yêu cầu thông tin hoặc thực hiện một số hành động. Người quản lý tác nhân tạo điều kiện thuận lợi cho việc thực hiện yêu cầu bằng cách tương tác với tác nhân bị quản lý thông qua một liên kết giữa tác nhân quản lý và tác nhân được quản lý. Trong hệ sinh thái quản lý, tác nhân có thể giả định vai trò người quản lý hoặc vai trò tác nhân được quản lý.

Các tác nhân cho phép các dịch vụ kinh doanh tương tác với tác nhân thực hiện các yếu tố của dịch vụ và làm cho nó có thể đồng bộ hóa nhiều sự kiện khác

hoặc hoạt động có thể áp dụng. Tác nhân cho phép việc thực hiện các hoạt động phức tạp trên nhóm tác nhân hoạt động và đa dạng và kiểm soát các hành vi thay đổi trong khi hoạt động.

Khả năng hoạt động là khả năng vận hành hệ thống khi thực hiện các chức năng đã dự định trong khoảng thời gian của nó. Nó bao gồm độ tin cậy, tính bảo trì, khả năng hỗ trợ, tính linh hoạt, an toàn, chi phí hoạt động và tính dễ sử dụng. Độ tin cậy là tổng hợp của tính sẵn có và khả năng khôi phục nhanh chóng, đầy đủ trạng thái hệ thống. Khả năng hỗ trợ là khả năng hoạt động hệ thống và thích ứng với nhu cầu thay đổi. Khả năng bảo trì là khả năng nhanh chóng thay đổi dịch vụ và giữ những thứ không cung cấp của dịch vụ ở mức tối thiểu. Khả năng hoạt động xác định các chi phí bao gồm chi phí cho hỗ trợ, bảo trì, đào tạo, các ấn phẩm kỹ thuật, phụ tùng, thiết bị hỗ trợ và một số các tiện ích.

Sau đây cho thấy tập con của các bước trong quy trình tạo dịch vụ ưu đãi với khả năng hoạt động.

Tạo dịch vụ: Dịch vụ có thể được tạo ra bằng cách sử dụng công cụ phát triển dịch vụ tạo ra một dịch vụ mới, bằng cách thích ứng với các dịch vụ đã có hoặc bằng cách đóng gói một ứng dụng hiện có trong dịch vụ. Trong quy trình tạo dịch vụ, các khả năng phi chức năng cũng sẽ tạo cùng dịch vụ. Các thuộc tính phi chức năng có thể được cung cấp bằng cách kết hợp các tác nhân quan lý đã có và các chính sách quản lý được kết hợp.

Dịch vụ Sổ đăng ký: Quy trình đăng ký thì phải khám phá ra các mô tả, giao diện, khả năng,... Nó cũng đòi hỏi định rõ khả năng quản lý và giao diện. Dịch vụ đăng ký để có thể nhìn thấy rõ trong một số mạng định rõ tùy vào người tạo dịch vụ và thông tin dịch vụ, như là giấy chứng nhận khả năng quản lý và khả năng hoạt động. Khả năng quản lý và khả năng hoạt động của dịch vụ xác định các mô hình tương tác giữa dịch vụ và tác nhân quản lý bên ngoài.

Hoạt động Dịch vụ: Một dịch vụ có thể tương tác với dịch vụ khác bằng cách sử dụng dịch vụ trung gian. Dịch vụ trung gian quản lý xác thực và tương tác cũng như hỗ trợ giao thức chuyển đổi, ví dụ như mã hóa và quản lý chính sách.

5.5. CÂU HỎI VÀ BÀI TẬP

1. Làm rõ các thành phần của mô hình hệ thống dịch vụ giám sát RESERVOIR: VEEM, VEEH, SM.
2. Phân tích vai trò của các nhà cung cấp dịch vụ, vai trò của điện toán đám mây trong cung cấp dịch vụ giám sát.
3. Phân tích đánh giá các chỉ số chất lượng và phương pháp xác định các chỉ số này trong giám sát dịch vụ.

4. Phân tích các giải pháp đảm bảo chất lượng dịch vụ và phương pháp khảo sát đánh giá.
5. Phân tích đặc điểm của quy trình xây dựng SLA và khả năng kinh doanh các dịch vụ.
6. Phân tích các thành phần của chuỗi giá trị quản lý chất lượng dịch vụ. Tìm hiểu mô hình thực tế tại các doanh nghiệp lớn: ví dụ các hệ SCM, ERP.
7. Nêu bản chất của khái niệm Business Service Fabric. Tìm một số công cụ điển hình hỗ trợ mô hình này.
8. Phân tích các giải pháp kiểm soát lỗi dịch vụ. Nghiên cứu đề xuất một số biện pháp nâng cao độ tin cậy của các dịch vụ.
9. Tìm và mô tả một số dịch vụ thực tế các sản phẩm phần mềm – dịch vụ giám sát đã triển khai ở Việt Nam.

Chương 6
CÁC CHỦ ĐỀ NÂNG CAO

Chương này sẽ cập nhật một số hướng nghiên cứu và phát triển cho công nghệ đám mây. Nội dung của chương sẽ được bố cục thành các chủ đề tương ứng với các hướng nghiên cứu hiện nay. Bên trong từng chủ đề, chúng tôi sẽ đưa ra những phân tích cụ thể theo quan điểm định hướng cho các nghiên cứu mở rộng sau này. Chúng tôi hy vọng thông qua các chủ đề đó, bạn đọc sẽ có được bức tranh toàn cảnh cũng như có thể định hình và tìm cho mình một hướng đi khi đi sâu nghiên cứu về công nghệ này. Các nội dung trình bày trong chương này bao gồm: Khả năng tương tác của các đám mây và các dịch vụ đám mây; Các tiêu chuẩn và tiêu chuẩn hóa đám mây; Liên bang đám mây; Bảo mật dữ liệu và an toàn dịch vụ/ứng dụng trên các đám mây; Mô hình môi giới dịch vụ đám mây; Các ứng dụng hỗ trợ cho điện toán đám mây.

Đây là các chủ đề có tính chất thời sự hiện nay, giúp người đọc tìm hiểu thêm về một số định hướng nghiên cứu trong công nghệ điện toán đám mây.

6.1. TÍNH TƯƠNG KẾT CỦA CÁC ĐÁM MÂY VÀ DỊCH VỤ ĐÁM MÂY

Khả năng tương tác (interoperability) sẽ mang lại nhiều lợi ích quý giá cho cả các doanh nghiệp cung cấp dịch vụ đám mây và cộng đồng khoa học sử dụng công nghệ này. Sự thiếu hụt khả năng tương tác giữa các đám mây với nhau cũng như giữa các dịch vụ đám mây đã và đang cản trở sự phát triển của mô hình điện toán này trong việc mở rộng dịch vụ hướng tới người sử dụng tiềm năng. Mặc dù vậy, các nghiên cứu liên quan đến khả năng tương tác đều gặp phải nhiều khó khăn do nhà cung cấp dịch vụ đám mây thường khóa công nghệ để buộc người dùng gắn bó với dịch vụ của họ. Khả năng tương tác trong môi trường đám mây được nhìn nhận từ hai góc độ khác nhau nhưng có liên quan mật thiết với nhau: khả năng tương tác của các đám mây và khả năng tương tác của các dịch vụ được triển khai trên mây.

Khả năng tương tác của các đám mây

Như đã nhắc đến ở trên, việc nhà cung cấp "khóa công nghệ" của họ (vendor lock-in) là một trong những tác động quan trọng vào việc phát triển của điện toán đám mây. Vấn đề ở đây là mỗi một nhà cung cấp dịch vụ đám mây lại sử dụng các công

nghệ của riêng họ và các công nghệ này về mặt cấu trúc là hoàn toàn khác nhau. Lấy ví dụ: các đám mây công cộng dạng IaaS có thể sử dụng các *hypervisor* khác nhau (XEN, KVM, VMware,...) để cho phép người dùng tạo các mây ảo. Bên cạnh đó, họ thường triển khai các hạ tầng mạng, các cơ sở dữ liệu, các API quản lý và các phần mềm hỗ trợ khác nhau. Theo hướng này, người sử dụng dịch vụ đám mây trong trường hợp muốn chuyển các ứng dụng của họ tới các đám mây khác hoặc muốn triển khai một ứng dụng mới lên nhiều đám mây khác nhau sẽ gặp phải vấn đề tương tác này. Chính vì vậy, một giải pháp hoặc một hướng tiếp cận cho phép khả năng tương tác giữa các đám mây trở thành nhu cầu cấp thiết phía từ người sử dụng.

Khả năng tương tác cho phép các đám mây khác nhau (IaaS, PaaS, SaaS, công cộng, riêng tư, cộng đồng, lai) làm việc hoặc liên kết với nhau. Trên một định nghĩa rộng về khả năng tương tác, sự liên kết giữa các đám mây là phức tạp. Ví dụ: một đám mây dạng IaaS không chỉ tương tác (hay liên kết) với một (hoặc nhiều) đám mây IaaS khác mà còn có khả năng liên kết thành một hệ sinh thái với các đám mây PaaS hoặc SaaS. Ví dụ khác về độ phức tạp khi liên kết nhiều đám mây là khi đám mây dạng công cộng PaaS liên kết với một đám mây dạng riêng tư IaaS,... Mô hình lý tưởng cho phép tương tác giữa các đám mây này sẽ cung cấp khả năng mềm dẻo về tài nguyên hơn so với mô hình đơn đám mây thông thường. Về phía người dùng dịch vụ, họ sẽ được hưởng lợi nhờ khả năng chọn cũng như sử dụng nhiều đám mây tùy theo nhu cầu mà không cần quan tâm tới sự khác biệt về công nghệ mà các nhà cung cấp đưa ra. Các nghiên cứu tập trung vào giải quyết bài toán tương tác hiện nay chủ yếu đưa ra giải pháp cho các đám mây cung cấp cùng một dạng dịch vụ. Một cách cụ thể là giữa hai hay nhiều đám mây IaaS, đám mây PaaS và đám mây SaaS...

Như bản thân điện toán đám mây với rất nhiều các định nghĩa khác nhau, khả năng tương tác giữa các đám mây cũng có rất nhiều định nghĩa với ý nghĩa cũng khác nhau. Ở tầng thấp của hệ thống đám mây, khả năng tương tác có thể hiểu là khả năng sử dụng cùng một công cụ để quản lý một ứng dụng hay dịch vụ trong môi trường đám mây. Ở tầng cao hơn, khả năng tương tác có thể hiểu là khả năng cho phép triển khai hoặc di chuyển một ứng dụng trên nhiều đám mây khác nhau. Có nhiều hướng nghiên cứu hiện nay tập trung giải quyết vấn đề này. Theo như kết quả mong đợi của các giải pháp này, chúng được chia thành nhiều hướng nhỏ, bao gồm: tạo các chuẩn cho ảnh của máy ảo; tạo các API thống nhất cho phép quản lý, điều khiển, sử dụng các tài nguyên đám mây và tạo ra các middleware hoặc nền tảng đám mây mã nguồn mở kết hợp nhiều chuẩn thống nhất trong môi trường điện toán đám mây.

Chuẩn hóa ảnh cho máy ảo (VM standard images). Mục đích của hướng tiếp cận này là cho phép triển khai các ứng dụng và cơ sở dữ liệu trên nhiều đám mây mà không yêu cầu bất kỳ thay đổi nào phía máy ảo, ứng dụng và cơ sở dữ liệu. Các ảnh của máy ảo thông thường được tạo ra và cung cấp bởi bên phát triển lớn như VMware Disk (VMDK), Microsoft Virtual Hard Disk (VHD),.... Theo hướng này, các nhà nghiên cứu tập trung vào việc xây dựng một chuẩn định dạng cho phép đóng

gói và trao đổi các ảnh máy ảo giữa các nền tảng ảo hóa khác nhau của các đám mây khác nhau.

API cho phép quản lý, điều khiển và sử dụng. Các API này cung cấp cho người dùng một công cụ để lấy trao đổi thông tin với dịch vụ đám mây. Nói cách khác, đây là một giao diện thống nhất để quản lý, điều khiển và sử dụng các dịch vụ thuộc nhiều đám mây khác nhau. Các API chung này thường bao gồm các chức năng về cung cấp, cấu hình tài nguyên tính toán như máy ảo, nền tảng và ứng dụng. Các nghiên cứu hoặc giải pháp theo hướng này được chia thành hai phần riêng biệt:

– Đề xuất một chuẩn API cho các đám mây dạng IaaS.

– Phát triển một lớp API trừu tượng (abstraction) nhằm cung cấp một phương tiện truy cập, sử dụng cho các đám mây IaaS, PaaS và SaaS mà không cần sự hỗ trợ (về mặt công nghệ) từ phía nhà cung cấp.

Xây dựng nền tảng đám mây mã nguồn mở kết hợp nhiều chuẩn công nghệ. Thay vì cố gắng đạt được khả năng tương tác bằng cách tạo các lớp trừu tượng hóa API từ các nền tảng đám mây khác nhau hoặc tạo ra các chuẩn áp dụng cho mọi đám mây, hiện nay xu hướng phát triển để tập hợp nhiều chuẩn công nghệ hoặc giải pháp có sẵn nhằm xây dựng một mô hình đám mây mã nguồn mở cũng đang được đẩy mạnh. Lợi ích của các mô hình này là khả năng thích ứng với nhiều công nghệ được chấp nhận rộng rãi. Lấy ví dụ, OpenStack là nền tảng đám mây mã nguồn mở cho phép sử dụng các chuẩn ảnh máy ảo Open Virtualization Format (OVF), chuẩn API điều khiển Open Cloud Computing Interface (OCCI),... Điều này cho phép bản thân OpenStack có khả năng tương tác với các đám mây hoặc nền tảng đám mây khác nếu áp dụng các chuẩn trên.

Khả năng tương tác của các dịch vụ đám mây

Hướng nghiên cứu về khả năng tương tác của các dịch vụ đám mây hiện nay tập trung vào việc xây dựng các ứng dụng có khả năng triển khai giữa các đám mây khác nhau. Mặc dù vậy, bản thân việc cho phép tính tương tác cho ứng dụng cũng phải phụ thuộc rất nhiều vào công nghệ mà các đám mây cung cấp. Lấy ví dụ, các ứng dụng được phát triển trên nền tảng của Google (GAE) bằng ngôn ngữ Go, yêu cầu đặt ra cho các ứng dụng này là triển khai được trên các đám mây khác như Ruby on Rails, Heroku hỗ trợ các ngôn ngữ khác không phải Go. Để thực hiện việc này, các nhà phát triển thường hướng tới xây dựng một API trung gian giữa hai đám mây dựa trên các API có sẵn của nhà cung cấp (hoặc bộ thư viện trung gian). Azure hiện nay đã cho phép một giải pháp như vậy, các ứng dụng viết bằng Java có thể triển khai trên đám mây của Microsoft thay vì phải viết bằng .NET hoặc một ngôn ngữ lập trình nào đó được hỗ trợ bởi Microsoft. Giải pháp này có được là nhờ bộ thư viện hỗ trợ mà nhà cung cấp đưa ra. Bên cạnh đó, giải pháp xây dựng nền tảng cho phép phát triển và triển khai độc lập không yêu cầu nhà cung cấp dịch vụ đám mây hỗ trợ cũng được nghiên cứu. OCCI là một mô hình hướng tới giải pháp dịch vụ đó. Trong khi bước đầu của sản phẩm là cho

phép khả năng điều khiển nhiều đám mây một lúc, thì trong bước hai, OCCI sẽ tập trung cho phép nhà lập trình viết các phần mềm theo dạng định nghĩa (software defined) bằng cách tạo một OCCI framework. Một ví dụ khác có thể kể đến là SAGA API, được phát triển đầu tiên cho việc tạo và triển khai các ứng dụng vào lưới (grid computing), sau đó mở rộng cho các hệ phân tán bao gồm cả đám mây. SAGA API sử dụng cơ cấu xếp hàng đợi của lưới để đưa các công việc (jobs) vào hệ thống phân tán. Tuy nhiên, còn nhiều hạn chế khi áp dụng cơ chế này vào môi trường đám mây.

Vấn đề khác của việc cho phép khả năng tương tác (nói cách khác là khả năng di chuyển các ứng dụng) giữa các đám mây đó là cho phép khả năng di chuyển của dữ liệu ứng dụng giữa các đám mây đó. Một loạt các ý tưởng mới cho vấn đề này đang được nghiên cứu bao gồm thành lập một chuẩn API để quản trị dữ liệu. Ví dụ như chuẩn Cloud Data Management Interface (CDMI) hoặc Microsoft's Open Data Protocol (ODP), hay xây dựng một nền tảng dữ liệu trung gian làm nhiệm vụ chuyển đổi định dạng dữ liệu giữa các đám mây.

Có thể thấy rằng, làm việc với dữ liệu trong môi trường hỗn tạp của điện toán đám mây hiện nay đang là thách thức lớn với các nhà nghiên cứu phát triển. Họ không chỉ gặp phải vướng mắc khi phát triển, triển khai ứng dụng có khả năng tương tác mà còn gặp phải vấn đề lớn với các ứng dụng có sẵn (legacy applications) khi triển khai chúng vào nhiều đám mây khác nhau. Các ứng dụng này thường đã được viết và sử dụng trước đây, việc mây hóa chúng phù hợp với hạ tầng, nền tảng của nhà cung cấp dịch vụ đám mây đòi hỏi chi phí cao, trong một số trường hợp là không thực tế. Ví dụ như việc đưa ứng dụng phần mềm từ dạng "cài đặt trên máy bàn – desktop application" lên máy chủ đám mây của GAE hoặc Azure hiện nay còn là công việc khó khăn với người sử dụng.

6.2. CÁC TIÊU CHUẨN CỦA ĐIỆN TOÁN ĐÁM MÂY

Một trong số những giải pháp để giải quyết vấn đề tương tác trong môi trường đa đám mây đó là xây dựng các chuẩn có thể áp dụng cho mọi nhà cung cấp. Ý tưởng của việc tạo ra chuẩn công nghệ hoặc các tiêu chuẩn hóa các đám mây là thông qua các chuẩn này, các ứng dụng và dữ liệu có thể di chuyển (để triển khai) giữa các đám mây mà không gặp trở ngại về mặt công nghệ. Bên cạnh đó, người dùng cũng sẽ được cung cấp một giao diện duy nhất để quản lý và sử dụng các dịch vụ trên mây.

Bản thân việc nghiên cứu đưa ra các tiêu chuẩn (không chính thức) cho điện toán đám mây cũng được chia thành các hướng tiếp cận khác nhau phụ thuộc vào sản phẩm mà các nghiên cứu này đưa ra. Ở hướng tiếp cận ở tầng cao trong cấu trúc dịch vụ đám mây, các nhà nghiên cứu đưa ra giải pháp cung cấp một chuẩn giao diện cho phép các đám mây hoặc các cơ sở dữ liệu trong môi trường đám mây có thể được quản lý và điều khiển chung. Ở hướng tiếp cận ở tầng thấp hơn, các nhà nghiên cứu đang cố gắng đưa ra các tiêu chuẩn hóa trong quá trình phát triển ứng dụng. Ví dụ các trình duyệt, các ngôn ngữ mô tả dữ liệu, phần mềm runtime, nhận gửi thông điệp bên trong

ứng dụng, các giao thức, công nghệ bảo mật,... Ở hướng tiếp cận ở tầng thấp nhất, các nhà nghiên cứu đã đưa ra chuẩn cho ảnh của máy ảo nhằm giúp các ứng dụng và dữ liệu kèm máy ảo có thể di chuyển được giữa các đám mây.

OCCI là một giải pháp được giới thiệu của Open Grid Forum. Đây là một API dựa trên giao thức RESTful phục vụ mọi tác vụ quản lý các đám mây, đặc biệt là các đám mây dạng IaaS. Về mặt kỹ thuật, người sử dụng sẽ gửi các yêu cầu HTTP tuần tự tới OCCI web service với các "action" và thông số để quản lý và điều khiển tài nguyên trên mây. Các thông số được chuẩn hóa và định nghĩa trong các tệp mô tả dữ liệu dạng XML và JSON và được gửi kèm cùng yêu cầu. Khi nhận được các yêu cầu từ phía người sử dụng, OCCI web service sẽ trả về cho người dùng một nội dung XML, bao gồm các thông tin của tài nguyên vừa được yêu cầu. Lấy ví dụ một yêu cầu GET để liệt kê danh sách các tài nguyên sau khi gửi cho OCCI server như sau:

```
GET /compute HTTP/1.1
Authorization: Basic xxxxxxxxx
User-Agent: occi-client/1.0 (linux) libcurl/7.19.4 OCCI/1.0
Host: example.com
Accept: text/uri-list
```

Khi đó OCCI server sẽ trả về nội dung như sau:

```
HTTP/1.1 200 OK
Server: occi-server/1.0 (linux) OCCI/1.0
Date: Wed, 27 Jan 2012 17:26:40 GMT
Content-type: text/uri-list
/compute/node1
```

Tuy nhiên, mục đích chính của OCCI là tạo ra một môi trường hybrid quản lý các đám mây một các độc lập. Trong kịch bản của sản phẩm này, OCCI sẽ được chia thành hai phần riêng biệt, OCCI *core* và OCCI *interface*, trong đó phần interface đã và đang được ứng dụng trên một số đám mây IaaS như: OpenNebula, OpenStack, ElasticHost, GoGrid,... *Core* định rõ các dạng cơ bản, bao gồm: *Entity*, *Resource*, *Link* và *Action*. *Entity* là một dạng trừu tượng hóa của dạng *Resource* và *Link*; *Resource* mô tả cụ thể các tài nguyên như các đối tượng (object); *Link* định nghĩa mối quan hệ giữa *Resource*; *Action* định nghĩa các hoạt động phù hợp cho *Entity*. Mô hình OCCI được phát triển trên UML, nhưng các dạng cơ bản trên được mô tả như một cấu trúc hình học tương tự như OWL.

Ngoài OCCI, hiện nay Amazon EC2 API cũng được coi là một trong các chuẩn không chính thức của các đám mây dạng IaaS. EC2 API đang được rất nhiều các đám mây mã nguồn mở hỗ trợ như là giao diện lập trình thứ hai cho người dùng, bên cạnh các API được cung cấp chính thức của nhà phát triển đám mây đó. Các đám mây hỗ trợ EC2 phải kể đến: OpenStack, OpenNebula, Eucalyptus, CloudStack,...

Dữ liệu tương tác trao đổi ra và vào giữa các nền tảng đám mây khác nhau cũng là chủ đề nghiên cứu thu hút hiện nay. Ngoài các phương pháp trao đổi dữ liệu như SCP hoặc WebDAV và các cơ sở dữ liệu quan hệ, hiện nay khá nhiều các đám mây

cho phép một phương pháp mới để truy cập và lưu trữ dữ liệu nhằm đạt được hiệu năng và tính khả mở cho việc xử lý dữ liệu người dùng. Một số ý tưởng mới cố gắng tiếp cận khả năng tương tác bằng cách tiêu chuẩn hóa các API quản lý dữ liệu trên mây. Ví dụ như chuẩn CDMI.

Trong môi trường đám mây, các chuẩn cho việc lập trình ứng dụng và dịch vụ rất quan trọng đối với các lập trình viên bởi nhiều nguyên nhân khác nhau. Ví dụ như, theo một số nhà nghiên cứu, nhìn chung, 80% chi phí cho một sản phẩm phần mềm là vào việc bảo trì nó. Trong khi đó, đối việc chỉnh sửa lỗi xảy ra trong quá trình hoạt động lại là nhiệm vụ khó khăn bởi người vá lỗi không phải là người phát triển ứng dụng. Trên cơ sở đó, các chuẩn lập trình giúp tăng tính dễ đọc cho phần mềm, cho phép nhà phát triển hiểu các mã mới nhanh chóng và triệt để hơn. Một số chuẩn có thể sử dụng vào tiêu chuẩn hóa bao gồm (không đầy đủ):

– Mô tả dữ liệu XML, JSON;

– Môi trường runtime: LAMP (Linux, Apache, MySQL, PHP hoặc Perl hoặc Python), LAPP (Linux, Apache, PostgreSQL, PHP hoặc Perl hoặc Python), Tomcat.

– Giao thức gửi/nhận thông điệp: SMTP (Simple Message Transfer Protocol), POP (Post Office Protocol), IMAP (Internet Messaging Access Protocol), REST (Representational State Transfer), SOAP (Simple Object Access Protocol). An toàn: SAML (sercurity Assertion Markup Language), OAuth (Open Authentication), OPENID, SSL/TLS (Transport Layer Sercuriy/Secure Sockets Layer).

Như đã giới thiệu ở phần trước, ở tầng thấp nhất trong cấu trúc của dịch vụ đám mây, chuẩn OVF cho ảnh của máy ảo cũng được coi là chuẩn không chính thức trong môi trường điện toán đám mây.

6.3. LIÊN BANG ĐÁM MÂY

Các khái niệm cơ bản

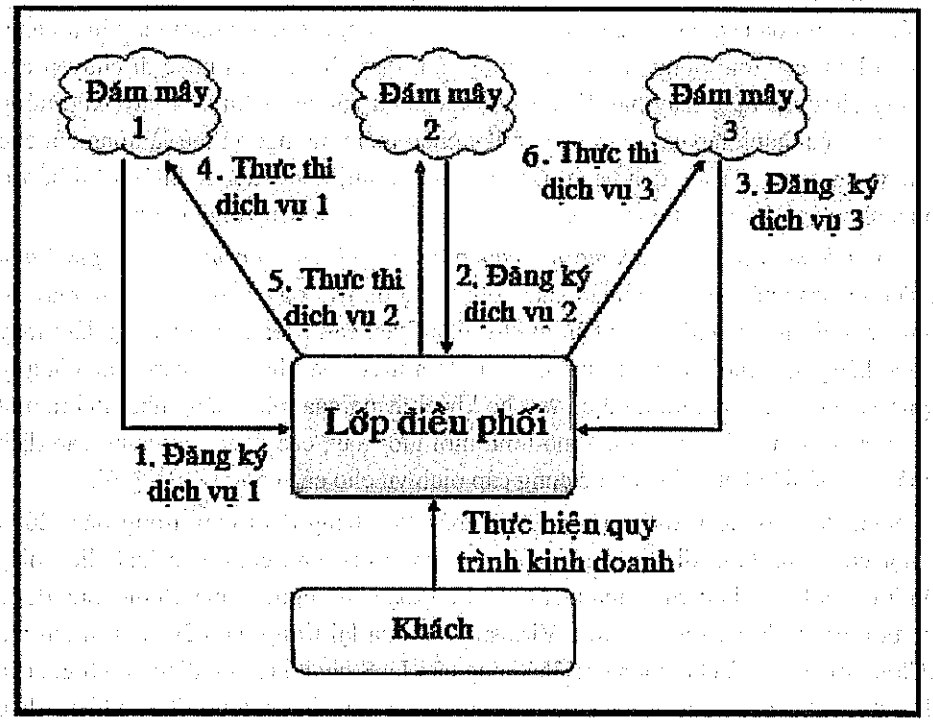
Xây dựng một Cloud Federation (còn gọi là liên bang đám mây) là việc triển khai và quản lý nhiều dịch vụ điện toán đám mây để phù hợp với nhu cầu sử dụng. Nói cách khác, đây là sự kết hợp của một số bộ phận nhỏ hơn (các đám mây thành viên) nhằm thực hiện một hành động chung. Đám mây liên bang đòi hỏi các nhà cung cấp tài nguyên tính toán kết hợp lại với nhau theo một cách nào đó và chịu sự quản lý chung về mặt kỹ thuật bởi một giải pháp tích hợp hệ thống. Những nguồn tài nguyên góp chung này trở thành một phần mở rộng tạm thời hoặc vĩnh viễn trong môi trường điện toán đám mây của người sử dụng. Việc liên kết các đám mây lại với nhau hoàn toàn tùy thuộc vào thỏa thuận cụ thể giữa các nhà cung cấp.

Đám mây liên bang cung cấp nhiều lợi ích đáng kể so với mô hình dịch vụ đám mây thông thường, các lợi ích chính bao gồm:

– Cho phép các nhà cung cấp tăng khả năng cấp tài nguyên tính toán cho người sử dụng từ các tài nguyên nhàn rỗi của các đám mây khác.

– Cho phép một nhà cung cấp có thể liên kết để phục vụ được nhiều khách hàng tiềm năng ở những vùng dịch vụ đám mây của họ chưa phát triển hoàn chỉnh. Cho phép người dùng sử dụng được nguồn tài nguyên gần như vô hạn, bất kể họ sử dụng tài nguyên, dịch vụ của đám mây thành viên nào thuộc liên bang nhằm phục vụ các bài toán từ lớn đến cực lớn của họ.

– Cho phép khả năng tránh lỗi (fault-tolerance), tránh thảm họa (disaster recovery) đối với dữ liệu của người dùng.



Hình 6.1. Orchestration layer trong các liên bang đám mây

Như đã trình bày ở trên, thông thường một liên bang đám mây sẽ được quản lý, điều khiển bởi một công cụ chung (gọi là orchestration layer). Về mặt cấu trúc, công cụ này được mô hình hóa như là một lớp độc lập so với các dịch vụ đám mây thành viên của liên bang. Lớp này ngoài việc chịu trách nhiệm quản lý còn có trách nhiệm là giao diện tương tác với người sử dụng đám mây liên bang. Chính vì vậy, nó phải có các chức năng quản lý người dùng, phân chia tài nguyên, bảo mật,... Mô hình đám mây liên bang được trình bày ở hình 6.1.

Liên kết trở thành đám mây liên bang

Mô hình đám mây liên bang sẽ tạo ra sức mạnh về số lượng. Điều này đặc biệt đúng đối với các nhà cung cấp dịch vụ vừa và nhỏ và là thành viên của một đám mây liên bang. Các đám mây thành viên này khi tham gia vào một liên bang nào đó có thể cung cấp các dịch vụ tiên tiến hơn, phổ biến hơn và khả năng mở rộng hơn so với phát triển độc lập. Về mặt kinh tế, liên bang đám mây cho phép các nhà cung cấp nhỏ cải thiện triển vọng của họ cho tăng trưởng dài hạn và bền vững nhờ có vị trí để họ cạnh tranh với những gã khổng lồ của ngành công nghiệp này như Amazon hay Microsoft.

Xu hướng liên kết các đám mây chắc chắn phải dựa nhiều vào các tiêu chuẩn và việc tiêu chuẩn hóa các công nghệ. Lý do là ở góc độ người dùng đám mây liên bang, việc triển khai các ứng dụng vào bất kỳ một đám mây thành viên hoặc di chuyển các ứng dụng giữa các đám mây này là nhu cầu tối thiểu của họ. Chính vì vậy, xu hướng khác trong việc thành lập các đám mây là lấy phần mềm mã nguồn mở là nòng cốt cho đám mây liên bang. Trong quá trình mở rộng của mình, liên bang sẽ hướng tới hỗ trợ kỹ thuật cho các đám mây thương mại. Một số ví dụ về liên bang đám mây:

SpotCloud: Liên bang thông qua thị trường dịch vụ đám mây của người môi giới. Theo hướng này, một tác nhân xuất hiện trong thị trường các dịch vụ đám mây đó là công ty môi giới. Họ sẽ đảm nhận vai trò nhận yêu cầu triển khai dịch vụ đám mây từ khách hàng đầu cuối và triển khai nó trên đám mây của nhà cung cấp. Các công ty môi giới sẽ đảm bảo chất lượng dịch vụ cho khách hàng của mình cũng như đưa ra một mức phí cạnh tranh. Khi xuất hiện mô hình môi giới này, các đám mây cung cấp dịch vụ thuần có thể liên kết với nhau để cung cấp dịch vụ cho các công ty môi giới.

SpotCloud bước vào thị trường điện toán liên bang đám mây trong năm 2010 như một cơ sở hạ tầng dịch vụ môi giới cho phép các nhà cung cấp IaaS liên hiệp nguồn lực của họ và bán vượt quá khả năng tính toán cho người mua. SpotCloud được tài trợ bởi Enomaly và sau đó được Virtustream mua lại trong năm 2011. Lợi ích mà SpotCloud mang lại là cho phép các nhà cung cấp IaaS nhanh chóng điều chỉnh giá của họ dựa trên nhu cầu thực tế của thị trường thông qua SpotCloud. Tuy nhiên, theo Reuven Cohen, người sáng lập và hiện là chủ tịch phó Virtustream, sự xuất hiện của một hệ sinh thái đám mây liên bang là không thể tránh khỏi, nhưng phải thừa nhận nó vẫn chưa thực sự đáp ứng được kỳ vọng của cả hai bên – nhà cung cấp IaaS và người sử dụng.

Bên cạnh SpotCloud, *EGI Federated Cloud* cũng là một liên bang đám mây lớn thu hút tới gần hơn 50 tổ chức nghiên cứu thuộc gần 40 quốc gia trên toàn thế giới tham gia chia sẻ tài nguyên chung. Liên bang đám mây này chủ yếu được xây dựng dựa trên các công nghệ và giải pháp mã nguồn mở hiện nay. Tiêu biểu như OpenStack, OpenNebula, OCCI, CDMI, OVF và một số các công nghệ khác. Mục đích của EGI Federated Cloud là cung cấp một môi trường đám mây với lượng lớn tài nguyên được đóng góp từ nguồn tài nguyên đám mây nhàn rỗi của các tổ chức nghiên cứu đến từ

khắp nơi trên toàn thế giới. Hiện đây được coi là một liên bang đám mây thành công nhất nhờ tính phi lợi nhuận và các giải pháp mã nguồn mở mà nó áp dụng.

OnApp: Liên bang đám mây nhằm chia sẻ nội dung số trên mạng mạng, quản lý các dịch vụ đám mây trên các máy chủ CDN. OnApp là một liên bang đám mây ra đời năm 2011 với mục tiêu xây dựng các công cụ quản lý đám mây, liên kết các hệ thống máy chủ lớn phân phối nội dung số trên internet (CDN – Content Delivery Network). Bắt đầu từ việc liên kết các máy chủ của các nhà cung cấp CDN, OnApp nhận ra rằng tới 20% cơ sở hạ tầng của họ luôn trong tình trạng nhàn rỗi. Do đó, OnApp đã xây dựng một liên bang đám mây giúp các nhà cung cấp máy chủ CDN kiếm tiền từ tài nguyên đó thông qua dịch vụ đám mây IaaS. OnApp theo đó đã ra mắt dịch vụ điện toán đám mây CDN của nó, mang nhãn hiệu Liên bang đám mây OnApp CDN, trong tháng 8 năm 2011 để cạnh tranh trực tiếp với cung cấp dịch vụ CloudFront CDN của Amazon. Trong liên bang của OnApp, các nhà cung cấp đám mây chạy nền tảng CDN đều có thể tham gia. Giải pháp của OnApp đưa ra là tập trung vào hoạt động quản lý các dịch vụ, phục vụ như một trung gian và môi giới để theo dõi việc sử dụng quản lý và quyết toán tài chính giữa người mua và người bán tài nguyên.

6.4. MÔ HÌNH MÔI GIỚI DỊCH VỤ ĐÁM MÂY

Hiện nay, mô hình môi giới dịch vụ đám mây trong thị trường kinh doanh điện toán này được chia thành ba hướng chính, đó là:

– Dịch vụ trung gian (service intermediation).

– Kết hợp các dịch vụ (service aggregation).

– Buôn bán dịch vụ (service arbitrage).

Dịch vụ trung gian trong mô hình này, một nhà cung cấp dịch vụ cầu nối sẽ đóng vai trò kết nối hai dịch vụ đám mây lại với nhau. Lấy ví dụ, một doanh nghiệp kinh doanh SaaS có nhu cầu triển khai ứng dụng của họ lên nền tảng đám mây IaaS nào đó do không muốn đầu tư về cơ sở hạ tầng của các trung tâm dữ liệu. Theo hướng này, một nhà cung cấp trung gian (môi giới) sẽ cung cấp giải pháp, nền tảng cho phép ứng dụng SaaS được triển khai dễ dàng nhanh chóng vào đám mây IaaS của một doanh nghiệp thứ ba. Animoto là ví dụ cụ thể cho ứng dụng SaaS triển khai trên máy chủ ảo của AWS. Để đưa ứng dụng chỉnh sửa video của mình lên các nền tảng hạ tầng đám mây của AWS, Animoto sử dụng giải pháp dịch vụ của RightScale. RightScale cho phép ứng dụng Animoto triển khai trên máy ảo nhanh chóng, bảo mật dữ liệu người dùng. Ở đây, RightScale đóng vai trò như một nhà môi giới dịch vụ đám mây nhờ việc cung cấp giải pháp toàn diện cho cả Animoto và AWS.

Kết hợp các dịch vụ mô hình này đưa ra giải pháp cho phép các dịch vụ kết hợp lại với nhau trở thành đám mây liên bang. Ở đám mây này, có thể có nhiều nhà cung cấp các dịch vụ khác nhau bao gồm IaaS, PaaS và SaaS tạo thành một hệ sinh thái (ecosystem) phục vụ nhu cầu của người sử dụng. Ví dụ, khách hàng của một dịch vụ

đám mây IaaS có thể thông qua nhà cung cấp của mình sử dụng các dịch vụ PaaS và SaaS của đám mây khác (dịch vụ này không được cung cấp bởi đám mây IaaS). Ở đây, nhà cung cấp IaaS sẽ đóng vai trò môi giới giữa khách hàng và dịch vụ PaaS, SaaS. Ở phía nhà cung cấp, họ sẽ thu được lợi nhuận nhờ sự tiêu dùng của khách hàng. Trong khi đó, ở phía ngược lại, người dùng chỉ cần có hợp đồng với duy nhất đám mây IaaS nhưng vẫn được sử dụng các tiện ích có được từ các đám mây khác. Mô hình này đòi hỏi các nghiên cứu nhằm đưa ra giải pháp cho khả năng tương tác không những theo chiều ngang của các dịch vụ đám mây (giữa hai, ba hay nhiều hơn đám mây IaaS với nhau, hoặc giữa các đám mây PaaS,...) mà còn đòi hỏi khả năng tương tác theo chiều dọc (giữa các đám mây IaaS và PaaS, SaaS). Bên cạnh đó, nhà cung cấp cũng phải đảm bảo chất lượng dịch vụ của các dịch vụ cho người sử dụng. Từ đó đưa ra các hướng nghiên cứu về các hệ kiểm tra chất lượng các dịch vụ được cung cấp,... Việc tạo ra một đám mây liên bang cũng là một trong những thách thức khi cần một giải pháp tổng thể cho các đám mây thương mại như đã trình bày ở phần trên.

Buôn bán dịch vụ mô hình này hình thành bắt nguồn từ nhu cầu sử dụng các dịch vụ đám mây của người dùng đầu cuối. Trong thời đại các dịch vụ đám mây bùng nổ như hiện nay, vấn đề mà người dùng tiềm năng các dịch vụ đám mây đau đầu là chọn cho mình một dịch vụ phù hợp với nhu cầu thực tế. Một số nhà môi giới dịch vụ đám mây sẽ làm điều này cho khách hàng của họ. Giải pháp của họ đưa ra là phân tích như cầu của khách hàng, đưa ra lựa chọn về dịch vụ đám mây phù hợp. Khác với mô hình đầu tiên về môi giới dịch vụ đám mây, ở đây các nhà môi giới sẽ thay mặt khách hàng của mình mua dịch vụ của nhà cung cấp đám mây, sau đó bán lại cho khách hàng. Mô hình môi giới này đòi hỏi nhà cung cấp đám mây, nhà môi giới phải có thỏa thuận về lợi ích, đảm bảo quyền lợi cho cả hai bên và chất lượng dịch vụ cho khách hàng. Nhà cung cấp dịch vụ đám mây theo đó cũng sẽ đưa dịch vụ của họ tới được nhiều người sử dụng hơn và thu lợi nhuận trên tổng số người dùng nhiều hơn. Phía người sử dụng, ngoài việc thuận lợi hơn trong quá trình chọn dịch vụ đám mây phù hợp với nhu cầu, họ thậm chí được sử dụng dịch vụ với giá bán ra của nhà cung cấp nhưng vẫn được hưởng đầy đủ các ưu điểm và chức năng của mô hình dịch vụ điện toán này.

Việc xây dựng một mô hình trung gian môi giới giữa các nhà cung cấp dịch vụ và khách hàng đầu cuối hiện nay đang là xu thế của các công ty công nghệ thông tin vừa và nhỏ. Có rất nhiều hướng phát triển các nghiên cứu nhằm đưa ra giải pháp cho mô hình này. Một số yêu cầu đặt ra khi xây dựng mô hình môi giới đó là:

– Đảm bảo chất lượng dịch vụ (QoS) dựa trên SLA.

– Xây dựng giải pháp cho khả năng tương tác của dịch vụ, ứng dụng và dữ liệu trong môi trường đa đám mây.

– Xây dựng cơ cấu triển khai các ứng dụng vào môi trường đa đám mây. Đảm bảo an toàn bảo mật thông tin giữa khách hàng – nhà môi giới – nhà cung cấp.

– Xây dựng giải pháp tổng thể cho đám mây liên bang.

Bên cạnh đó, vấn đề khác nảy sinh khi xây dựng một mô hình môi giới là cần phải có các dịch vụ giám sát thực thi SLA và QoS khi sử dụng dịch vụ trung gian. Các dịch vụ hướng tới giám sát này cũng là những hướng nghiên cứu hiện nay cho điện toán đám mây, bao gồm:

– Giám sát chức năng và khả năng an toàn bảo mật của toàn hệ thống, dịch vụ đám mây.

– Giám sát tính riêng tư của dữ liệu người dùng khi đưa lên mây với sự tham gia của nhiều bên cung cấp dịch vụ, môi giới. Đảm bảo dữ liệu không bị đưa cho các tổ chức, cá nhân khác.

– Giám sát hiệu năng của hệ thống và dịch vụ khi có sự xuất hiện trung gian của nhà môi giới. Đánh giá hiệu năng nhằm đảm bảo chất lượng dịch vụ QoS và SLA.

6.5. CÁC ỨNG DỤNG HỖ TRỢ CHO ĐIỆN TOÁN ĐÁM MÂY

Những năm trở lại đây, cùng với sự phát triển của công nghệ điện toán đám mây, rất nhiều các ứng dụng hoặc giải pháp ra đời với mục đích hỗ trợ cho các dịch vụ này. Bên cạnh một số giải pháp hướng tới việc đưa ra các chuẩn và tiêu chuẩn hóa đám mây như OCCI, CDMI, OVF, một số ứng dụng khác lại hướng tới giúp người dùng dễ dàng hơn trong việc sử dụng điện toán đám mây. Hầu hết các dịch vụ này đều hướng vào mô hình dịch vụ IaaS và một số dịch vụ PaaS, chúng có thể chia thành hai hướng chính như sau:

– Các giải pháp trừu tượng hóa API (API abstraction) của các đám mây.

– Các giải pháp triển khai ứng dụng trong các hệ phân tán.

Các giải pháp trừu tượng hóa API tập trung vào hướng cho phép điều khiển, quản lý các dịch vụ đám mây thông qua một giao diện duy nhất. Ban đầu các giải pháp này phục vụ cho các đám mây IaaS, sau đó mở rộng chức năng cho phép phát triển và triển khai ứng dụng lên IaaS và PaaS. Một số ví dụ về các giải pháp này bao gồm:

– Simple Cloud API là một thư viện PHP trừu tượng hóa API của nhiều đám mây để cung cấp giao diện lập trình thống nhất cho người dùng. Một giải pháp tương tự là Apache LibCloud, cung cấp thư viện Python. Tuy nhiên, khác với OCCI, các bộ thư viện này không yêu cầu sự hỗ trợ về công nghệ và kỹ thuật từ phía nhà cung cấp.

– Deltacloud định nghĩa REST API để quản lý tài nguyên từ các đám mây. Các API của Deltacloud được xây dựng và hoạt động thông qua các yêu cầu/trả lời HTTP tới một service của Deltacloud. Để dễ sử dụng, giải pháp này cung cấp một giao diện dòng lệnh (command line). Khác với các giải pháp khác như Simple Cloud API hay Apache Libcloud, trong đó trói buộc người sử dụng sử dụng một ngôn ngữ lập trình cụ thể nào đó, Deltacloud cho phép người dùng gọi các yêu cầu HTTP bằng bất kỳ ngôn ngữ lập trình nào cũng như nhận trả lời là các tệp mô tả dữ liệu dạng XML. Đây là cá chuẩn được chấp nhận rộng rãi.

Bên cạnh các giải pháp trên còn có một loạt các công cụ khác như: jCloud, boto, enStartus, Dasein Cloud, Scalr, SAGA API đưa ra giải pháp tạo abstraction API tương tự. Một số giải pháp cho phép phát triển và triển khai ứng dụng dạng phần mềm định nghĩa (software defined) lên các đám mây mà nó hỗ trợ.

Các giải pháp triển khai ứng dụng trong các hệ phân tán. Các giải pháp này hướng vào việc cho phép triển khai tự động các ứng dụng vào môi trường phân tán các máy chủ, trong đó các máy ảo đám mây cũng là các máy chủ ở môi trường phân tán. Lấy ví dụ, để xây dựng dịch vụ đám mây Hadoop-as-a-service, người quản trị hệ thống cần phải cài đặt hàng chục hoặc thậm chí hàng trăm máy ảo chứa Hadoop để chứa một khối lượng dữ liệu lớn của các ứng dụng. Theo kiểu thông thường, người quản lý phải cài đặt bằng tay và cấu hình tuần tự từng máy ảo một. Công việc này sẽ tốn rất nhiều thời gian và có thể dẫn đến khả năng xảy ra lỗi. Nhờ có giải pháp tự động cài đặt, các nhà quản trị hệ thống chỉ việc định nghĩa các tệp cấu hình bằng ngôn ngữ dễ đọc, dễ mô tả và các thành phần của Hadoop sẽ tự động được cài đặt trên các nút (các máy ảo). Các sản phẩm tiêu biểu cho hệ thống này gồm:

CFEngine là một phần mềm mã nguồn mở được viết bằng ngôn ngữ C. CFEngine sử dụng mô hình server/client. Bất kỳ trạng thái nào của máy khách (client) khác với máy chủ (server) (được người dùng định nghĩa trong tệp mô tả) sẽ tự động cấu hình để trở thành trạng thái mong muốn.

Puppet được thiết kế bởi Puppet Labs. Puppet cũng là một công cụ mã nguồn mở được viết bằng ngôn ngữ Ruby. Phần hạt nhân của giải pháp này cũng hoạt động giống CFEngine: cung cấp cho người sử dụng ngôn ngữ mô tả cho phép họ viết các mã miêu tả trạng thái máy chủ dễ đọc và hiểu dưới dạng các đối tượng (object). Về kỹ thuật, máy chủ cài Puppet là tập hợp các tài nguyên đối tượng có các thuộc tính. Máy khách cài Puppet giao tiếp với máy chủ thông qua certificate được chứng thực SSL. Sau khi giao tiếp được kết nối, cấu hình được mô tả trong tệp trạng thái sẽ được tự động áp dụng trên các máy khách. Thêm vào đó, cả máy chủ Puppet và máy khách đều có API để quản lý và điều khiển các hoạt động cài đặt. Tuy nhiên, thông thường chỉ có máy chủ nghe các liên kết API. Điều này là phù hợp vì các máy khách không cần thiết phải đưa ra các lệnh gọi đồng bộ hóa.

Chef cũng là một công cụ mã nguồn mở được phát triển bởi Opscode. Thiết kế của nó rất giống với Puppet mặc dù nó không phải là một sản phẩm xuất phát từ mã phát triển của Puppet. Theo hướng này, Chef cũng được viết bằng ngôn ngữ Ruby và cũng được thiết kế lấy cảm hứng từ CFEngine.

Bcfg2 cũng là công cụ cấu hình tự động cho các máy chủ ở môi trường phân tán được phát triển bởi bộ môn toán và khoa học máy tính thuộc phòng thí nghiệm quốc gia Argonne. Bcfg2 được viết bằng Python, cấu hình của công cụ này sử dụng mô hình miêu tả dữ liệu XML.

Hiện nay, các hướng nghiên cứu liên quan đến các ứng dụng của điện toán đám mây này tập trung vào việc sử dụng các giải pháp trừu tượng để có thể triển khai nhanh

chóng các ứng dụng lên mây. Sau đó, mô hình này sẽ cung cấp dịch vụ nền tảng triển khai ứng dụng IT cho phép khả năng tương tác giữa các đám mây với nhau (chỉ cần phát triển ứng dụng một lần nhưng triển khai được ứng dụng đó trên các đám mây khác nhau). Bên cạnh đó, giải pháp theo hướng này cũng mở ra khả năng cho phép các phần mềm có sẵn đưa vào đám mây mà không cần phải phát triển lại. Song song với việc phát triển các giải pháp trừu tượng, việc sử dụng các công cụ triển khai ứng dụng trên các hệ phân tán cũng đang thu hút các nhà nghiên cứu về điện toán đám mây hiện nay. Các công cụ này về bản chất cho phép khả năng triển khai các ứng dụng có sẵn vào nhiều đám mây khác nhau. Tuy nhiên, hạn chế duy nhất là mô hình này đòi hỏi khả năng tạo ra nền tảng phát triển ứng dụng cho người dùng. Hiện tại, ngoài việc định nghĩa các tệp cấu hình cho máy khách, người dùng vẫn chưa có phương pháp nào phát triển hiệu quả các ứng dụng để đưa lên mây.

6.6. CÂU HỎI VÀ BÀI TẬP

1. Trình bày khả năng tương tác (interoperability) của đám mây và khả năng tương tác của các dịch vụ đám mây.
2. Open Virtualization Format (OVF) là gì? Trình bày mô hình hoạt động của OVF?
3. OCCI là gì? Trình bày mô hình hoạt động của OCCI.
4. Vai trò của OVF và OCCI trong việc cho phép khả năng tương tác của các đám mây là gì?
5. Thế nào là khả năng tương tác các đám mây theo chiều dọc của dịch vụ và khả năng tương tác theo chiều ngang của dịch vụ.
6. Thế nào là chuẩn và tiêu chuẩn hóa trong môi trường dịch vụ đám mây?
7. CDMI là gì? Trình bày mô hình hoạt động của CDMI.
8. Trình bày về các chuẩn đề nghị cho công nghệ điện toán đám mây hiện nay, bao gồm các chuẩn công nghệ phát triển dịch vụ điện toán đám mây.
9. Thế nào là một đám mây liên bang?
10. Trình bày về cấu trúc chung của một đám mây liên bang.
11. Nêu một số ví dụ về đám mây liên bang.
12. Các yếu tố cản trở sự hình thành đám mây liên bang là gì?
13. Trình bày sự khác biệt giữa đám mây riêng và đám mây công cộng, đám mây lai, đám mây cộng đồng dưới góc nhìn về bảo mật an toàn dữ liệu.
14. Trình bày một số rủi ro chính gặp phải với dữ liệu trong môi trường đám mây.
15. Trình bày về kỹ thuật mã hóa cho Public Key Infrastructure (KPI). Trình bày về các kỹ thuật mã hóa dữ liệu đám mây.
16. Trình bày về các kỹ thuật bảo đảm an toàn truy cập dịch vụ đám mây.
17. Trình bày phương pháp chính đảm bảo an toàn tránh thảm họa xảy ra đối với các máy chủ dữ liệu đám mây.

18. Trình bày về mô hình môi giới dịch vụ đám mây.
19. Các yêu cầu đặt ra trong mô hình môi giới dịch vụ đám mây là gì?
20. Trình bày về dịch vụ giám sát cho môi hình môi giới dịch vụ đám mây.
21. Trình bày các giải pháp và công cụ phục vụ cho điện toán đám mây.
22. Nêu ví dụ và đặc điểm của một trong số các công cụ phục vụ cho điện toán đám mây. So sánh công cụ này và các công cụ có chức năng tương đương.

TÀI LIỆU THAM KHẢO

1. Rosenberg, Jothy, and Arthur Mateos. *The cloud at your service.* Manning Publications Co., 2010.
2. Buyya, Rajkumar, James Broberg, and Andrzej M. Goscinski, eds. *Cloud computing: Principles and paradigms.* Vol. 87. Wiley. com, 2010.
3. Douglas K. Barry and David Dick. *Web Services, Service-Oriented Architectures, and Cloud Computing.* Morgan Kaufmann, 2013.
4. Marinescu, Dan C. *Cloud Computing: Theory and Practice.* Working paper. Computer science Division, Department of electrical engineering & Computer science, University of Central Florida, Orlando, fl, 2012.
5. Chuck Lam. *Hadoop in Action* (1st ed.). Manning Publications Co., Greenwich, CT, USA, 2010.
6. J. Lin and C. Dyer. *Data-Intensive Text Processing with MapReduce.* Morgan & Claypool Publishers, 2010.
7. J. Han, M. Kamber, and J. Pei. *Data Mining: Concepts and Techniques* (3rd Ed), Morgan Kaufmann, 2012.
8. Ashford, Warwick. *Securing the cloud.* Computer Weekly, 2011.
9. Hay, Chris and Brian Prince. *Azure in action.* Manning Publications Co., 2010.
10. Chang, William Y., Hosame Abu-Amara, and Jessica Feng Sanford. *Transforming enterprise cloud services.* Springer, 2010.
11. Hwang, Kai, J. J. Dongarra, and Geoffrey C. Fox. *Distributed and Cloud Computing.* Elsevier/Morgan Kaufmann, 2012.

MỤC TỪ

ĐIỆN TOÁN ĐÁM MÂY

NHÀ XUẤT BẢN BÁCH KHOA HÀ NỘI
Ngõ 17 Tạ Quang Bửu – Hai Bà Trưng – Hà Nội
ĐT: 024. 38684569; Fax: 024. 38684570
http://nxbbk.hust.edu.vn

Chịu trách nhiệm xuất bản:
Giám đốc – Tổng biên tập: TS. BÙI ĐỨC HÙNG

Phản biện: PGS. TS. ĐẶNG VĂN CHUYẾT
PGS. TS. NGÔ HỒNG SƠN
Biên tập: ĐỖ THANH THÙY
Sửa bản in: TRẦN THỊ PHƯƠNG
Trình bày bìa: DƯƠNG HOÀNG ANH

In 500 cuốn khổ (16 × 24) cm tại Công ty In Giao thông, chi nhánh Công ty TNHH MTV NXB Giao thông vận tải. Số 80B Trần Hưng Đạo, Hoàn Kiếm, Hà Nội.
Số xuất bản: 3658 – 2020/CXBIPH/04 – 68/BKHN; ISBN: 978-604-9982-91-0.
Số QĐXB: 261/QĐ – ĐHBK – BKHN ngày 15/9/2020.
In xong và nộp lưu chiểu quý III năm 2020.