

GÓI DỊCH VỤ KIỂM THỬ PHẦN MỀM HƯỚNG CLOUD

ThS. Trịnh Thuỳ Linh

Phòng NCPT Dịch vụ bưu chính viễn thông

Tóm tắt: Bất cứ loại phần mềm nào cũng đều tiềm ẩn bên trong nó những nguy cơ nhất định. Phần mềm hướng cloud cũng vậy, do đặc điểm đặc trưng là kiến trúc nhiều bên thuê nên cũng ẩn chứa nhiều rủi ro mà nếu không được lưu ý trong quá trình phát triển cũng như kiểm thử thì có thể gây hậu quả rất lớn. Đây chính là những khía cạnh chính mà những người làm kiểm thử phải lưu ý tới. Trong khuôn khổ bài báo này, chúng tôi sẽ trình bày các nguy cơ có thể xảy ra đối với loại phần mềm hướng cloud để từ đó đưa ra khung kiểm thử cũng như các bài kiểm thử cụ thể.

Abstract: Any kind of software are hidden within it certain risks. Cloud-based software as well, due to its multi-tenant architectural features that should also hidden risks that otherwise noted in the development well as testing, they can cause huge consequences. This is the main aspect that test manager have to pay attention to the test. In this article, we will present the probable risk for cloud-based software in order to offer the testing framework as well as specific tests for it.

1. GIỚI THIỆU

Từ năm 2007, Công nghệ thông tin đã bắt đầu một mẫu hình mới — điện toán đám mây. Mặc dù điện toán đám mây chỉ là một cách khác để cung cấp các tài nguyên máy tính, chứ không phải là một công nghệ mới, nhưng nó đã châm ngòi một cuộc cách mạng trong cách cung cấp thông tin và dịch vụ của các tổ chức. Cũng từ đó việc cung cấp phần mềm đã có những bước chuyển mình rõ rệt. Xu hướng chuyển các phần mềm truyền thống thành các dịch vụ phần mềm trên đám mây đặt ra cho các nhà cung cấp nhiều thách thức hơn.

Cũng như các nhà cung cấp phần mềm tại Việt Nam, VNPT cũng đang tận dụng thế mạnh của các đơn vị trực thuộc từng bước đưa những phần mềm dùng chung của các bưu điện trên khắp các tỉnh/ thành trở thành các dịch vụ phần mềm dưới dạng phần mềm hướng cloud based. Bên cạnh đó còn tích cực đẩy mạnh việc cung cấp, kinh doanh các dịch vụ CNTT ra ngoài thị trường. Đây là mảng hứa hẹn nhiều tiềm năng nhưng cũng bị cạnh tranh gay gắt không kém các dịch vụ Viễn thông. Với vai trò kinh doanh các dịch vụ như vậy, Tập đoàn có hai phương thức để tạo các sản phẩm dịch vụ: tự phát triển hoặc mua để kinh doanh dịch vụ. Cả hai phương thức này đều đặt ra yêu cầu kiểm định phần mềm

chặt chẽ bởi việc kinh doanh các dịch vụ CNTT cũng giống như các dịch vụ Viễn thông, cần đảm bảo cam kết chất lượng phần mềm, dịch vụ tới khách hàng. Với những yêu cầu như vậy, cộng với xu thế các phần mềm, hệ thống được cung cấp dưới dạng cloud nêu yêu cầu kiểm định phần mềm cloud là một bài toán cần phải giải quyết ngay.

Nắm bắt được yêu cầu đó, CDiT đã đưa ra gói kiểm thử phần mềm hướng cloud. Với khung kiểm thử CDiT đưa ra cho loại phần mềm này thì tất cả các phần mềm cần kiểm thử được đối chiếu qua để biết được những rủi ro mà phần mềm có thể gặp phải. Từ những phân tích rủi ro sẽ đưa ra mức ưu tiên về kiểm thử các khía cạnh phần mềm. Với gói dịch vụ kiểm thử phần mềm hướng cloud, CDiT đưa ra các bài kiểm thử cụ thể để đảm bảo tất cả các khía cạnh cần thiết được kiểm tra nhằm đạt chất lượng tốt nhất.

2. NỘI DUNG VÀ PHƯƠNG PHÁP NGHIÊN CỨU

2.1. Đặc điểm khác biệt giữa phần mềm hướng cloud với các phần mềm truyền thống

Phần mềm hướng cloud có nhiều đặc điểm khác so với phần mềm và ứng dụng web truyền thống. Đây là phần mềm có kiến trúc multi-tenant (nhiều bên thuê) trong đó

tất cả người dùng và các ứng dụng được chia sẻ trong một cơ sở hạ tầng và một nền code chung được duy trì tập trung. Đây là một điểm mạnh của phần mềm hướng cloud vì nó tiết kiệm được khá nhiều chi phí cho cả nhà cung cấp lẫn người sử dụng. Ngoài ra, nó còn thuận tiện trong việc triển khai trên diện rộng và dễ dàng trong việc sửa chữa, bảo trì, v.v... Tuy nhiên, bên cạnh những điểm mạnh thì phần mềm hướng cloud cũng ẩn chứa một số rủi ro, nguy cơ do những đặc điểm kiến trúc phần mềm của mình. Một số rủi ro mà các phần mềm hướng cloud thường gặp phải bao gồm: rủi ro về mặt hiệu năng, bảo mật, khả năng sẵn sàng hay khả năng bảo trì, v.v....

2.2. Một số nguy cơ cần kiểm soát đối với phần mềm hướng cloud

Những nguy cơ liên quan đến hiệu năng là mục tiêu quan trọng trong một thời gian dài. Với điện toán đám mây, càng nhiều kết nối được thực hiện trên Internet thì rủi ro về hiệu năng càng nhiều hơn. Khi nhiều hệ thống khác được sử dụng với sự trợ giúp của đám mây thì việc sử dụng internet có thể dẫn đến nguy cơ về hiệu năng đối với tất cả các quy trình nghiệp vụ. Một hướng quan trọng trong lựa chọn điện toán đám mây là khả năng mở rộng của dịch vụ. Khi nhu cầu tăng thì năng lực của hệ thống tự động tăng một cách nhanh chóng, sau đó khi nhu cầu giảm thì năng lực hệ thống cũng sẽ giảm đi. Đây chính là khả năng đàn hồi, một khía cạnh test riêng trong cloud.

Những rủi ro xuất hiện đối với hiệu năng cũng đi cùng với bảo mật: đây cũng chính là điều mà người quản lý kiểm thử luôn luôn quan tâm. Khi sử dụng đám mây có nghĩa là những nguy cơ về bảo mật phải được giải quyết một cách rõ ràng. Sự cố bảo mật có thể dẫn đến thiệt hại ngay lập tức cho doanh nghiệp và có thể dẫn đến vi phạm pháp luật. Có rất nhiều các quy định về an toàn thông tin và bảo mật. Việc chia sẻ tài nguyên CNTT với các khách hàng khác cũng sẽ dẫn đến các vấn đề an ninh. Trong tất cả các mô hình thực hiện điện toán đám mây thì sự nguy hiểm nhất là một nhân viên không được quyền nhưng lại truy cập được vào các dữ liệu nhạy cảm. Đây chính là vấn đề cần phải được kiểm soát. Một đặc điểm quan trọng

khác của các dịch vụ trên đám mây là việc không khóa Internet, thông qua các dịch vụ có thể thu được ở khắp mọi nơi và trên tất cả các loại nền tảng. Hiện nay có một xu hướng mới, đó là nhân viên sử dụng các thiết bị của mình để làm việc. Mọi người thường làm việc ở nhiều địa điểm khác nhau, hầu hết là ngoài văn phòng và sử dụng thiết bị riêng của mình. Điều này dẫn đến một lỗ hổng mới. Vậy làm thế nào để giữ an toàn cho các thiết bị và làm thế nào để người dùng sử dụng một cách an toàn. Đó cũng là điều mà các bài kiểm thử cần phải đưa ra để kiểm tra.

Rủi ro về tính sẵn sàng và liên tục ảnh hưởng trực tiếp ngay đến quá trình kinh doanh của người sử dụng. Một số vấn đề có thể xảy ra như mất kết nối Internet, một thiết bị bị lỗi trong dịch vụ riêng của mình, hoặc không truy cập được vào dữ liệu công ty. Việc phân tích rủi ro sẽ đánh giá được những gián đoạn có thể xảy ra và lường trước được hậu quả của nó. Tùy thuộc vào nguy cơ để đưa ra các biện pháp kiểm thử nhằm làm giảm nhẹ các rủi ro đó.

2.3. Các khía cạnh kiểm thử của phần mềm hướng cloud

a) Kiểm thử bảo mật

Mục đích: nhằm đảm bảo hệ thống phòng chống được các sự tấn công từ bên ngoài, đảm bảo an ninh dữ liệu của các bên thuê.

b) Kiểm thử hiệu năng

Mục đích: nhằm kiểm tra hiệu suất hoạt động, phản ứng của hệ thống trong các trường hợp tải khác nhau, trường hợp quá tải cũng như khi hệ thống sử dụng tải lớn trong một thời gian đủ dài.

c) Kiểm thử chức năng

Mục đích: nhằm đảm bảo các quy trình nghiệp vụ được thực hiện chuẩn xác, có thể cấu hình theo từng bên thuê.

d) Kiểm thử tương thích

Mục đích: nhằm bảo đảm khả năng tương thích của ứng dụng với các mục tiêu khác nhau như trình duyệt web, các nền tảng phân cứng, người dùng (ngôn ngữ, vùng miền khác nhau) hay hệ điều hành, v.v...

e) Kiểm thử Live

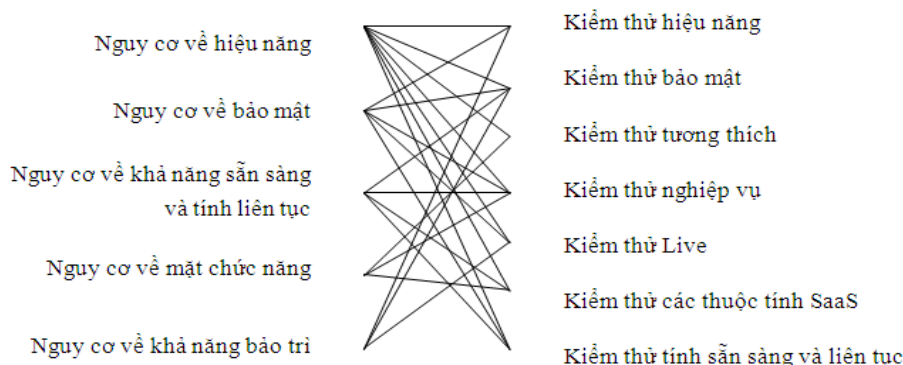
Mục đích: Mục đích của kiểm thử live nhằm đảm bảo ứng dụng được test trong một môi trường thực sự. Có hai loại kiểm thử live cần được quan tâm là:

- Kiểm thử khả năng phục hồi sau thảm hoạ

- Kiểm thử khả năng nâng cấp trực tuyến

f) Kiểm thử các thuộc tính SaaS

Mục đích của việc kiểm thử các thuộc tính SaaS chính là đảm bảo cho ứng dụng SaaS thoả mãn các đặc điểm mà một SaaS cần phải có.



Hình 1. Bảng ánh xạ giữa nguy cơ phần mềm và các khía cạnh kiểm thử

Khía cạnh kiểm thử	Bài kiểm tra
Kiểm thử hiệu năng	Kiểm thử tải (Load test) Kiểm thử quá tải (Stress test) Kiểm thử độ bền hoặc kiểm thử khối lượng Kiểm thử tính mềm dẻo và khả năng mở rộng
Kiểm thử bảo mật	Đánh giá bảo mật mạng Kiểm tra bảo mật thông tin khách hàng Kiểm thử khả năng mã hóa Kiểm thử khả năng xác thực Kiểm thử khả năng ủy quyền Kiểm thử bảo mật chống lại những tấn công từ Internet. Kiểm thử những bản vá bảo mật
Kiểm thử tương thích	Kiểm thử khả năng tương thích của dịch vụ với các quy trình nghiệp vụ Kiểm thử tính tương thích với các trình duyệt Kiểm thử tính tương thích với các hệ điều hành khác nhau Kiểm thử khả năng nội địa hoá (Localization) Kiểm thử khả năng quốc tế hoá (Internationalization testing): Kiểm thử khả năng tương thích ngược về mặt giao diện
Kiểm thử nghiệp vụ	Kiểm thử chất lượng dịch vụ

	Kiểm thử tính thân thiện với người dùng Kiểm thử giao diện với các hệ thống khác Kiểm thử khả năng cấu hình dịch vụ Kiểm thử khả năng tùy biến đối với nhà cung cấp Kiểm thử khả năng tùy biến đối với khách hàng Kiểm thử các web service Kiểm thử trên nhiều nền tảng Kiểm tra và thử nghiệm với các ứng dụng Kiểm thử khả năng làm việc offline
Kiểm thử Live	Kiểm thử khả năng khôi phục sau thảm họa Kiểm thử nâng cấp trực tuyến (Live upgrade)
Kiểm thử các thuộc tính SaaS	Kiểm thử sự tách biệt giữa các bên thuê Kiểm thử sự tích hợp giữa các API Kiểm thử cơ chế tính phí
Kiểm thử tính sẵn sàng và liên tục	Kiểm thử độ tin cậy của phần cứng Kiểm thử độ tin cậy của phần mềm Kiểm tra kết nối internet Kiểm thử dự phòng

Hình 2. Khung kiểm thử và các bài kiểm thử tương ứng

3. KẾT QUẢ

Từ những phân tích rủi ro và các khía cạnh kiểm thử cho phần mềm hướng cloud, chúng tôi đưa ra khung để đánh giá, kiểm tra nhằm xác định các bài kiểm thử cụ thể cho từng phần mềm với đặc điểm riêng của nó.

4. THẢO LUẬN

Với khung kiểm thử như trên, có thể thấy rằng có rất nhiều bài kiểm thử cần phải tiến hành trên mỗi phần mềm hướng cloud. Điều đó sẽ dẫn đến sự tốn kém về mặt thời gian, chi phí và công sức. Vậy có thực sự phải qua tất cả các bài kiểm tra như vậy hay không?

Chúng ta đều biết rằng, mỗi một phần mềm khi được xây dựng đều có mục tiêu, đối tượng, tính chất riêng của nó. Do vậy, chúng ta hoàn toàn có thể dựa vào đó để đưa ra mức ưu tiên đánh giá các khía cạnh kiểm thử để giảm bớt thời gian và chi phí kiểm thử phần mềm mà vẫn đạt hiệu quả cao. Ví dụ: Đối

với phần mềm Kế toán cần được kiểm soát về mặt bảo mật và riêng tư dữ liệu cao thì việc đánh giá phải được làm thật kỹ với nhiều kịch bản. Mỗi kịch bản phải được xây dựng dựa trên các công việc thực tế mà khách hàng vẫn tiến hành, kiểm tra sự tách biệt giữa các khách hàng. Xây dựng các kịch bản tấn công dạng cloud để kiểm soát khả năng bảo mật của phần mềm. Còn đối với phần mềm mang tính đại chúng như VnEdu thì lại cần được kiểm tra kỹ lưỡng về mặt hiệu năng, sự tách biệt về hiệu năng giữa các bên thuê khác nhau. Cụ thể là nếu một trường (bên thuê) có sự kiện gì đó khiến lượng người dùng bỗng nhiên tăng đột biến thì khi đó hiệu năng của hệ thống phải đáp ứng được số lượng người dùng lớn, đồng thời tốc độ truy cập của các bên thuê còn lại không được bị ảnh hưởng.

5. KẾT LUẬN

Với kết quả nghiên cứu và xây dựng nên các bài kiểm tra cụ thể, gói dịch vụ kiểm thử phần mềm hướng cloud có thể được triển khai thực hiện trước hết cho các phần mềm của VNPT và hướng ra mở rộng thực hiện cho các nhà cung cấp, các nhà đầu tư vào phần mềm hướng cloud có nhu cầu trên thị trường.

6. TÀI LIỆU THAM KHẢO

1. *Avneesh Vashistha, Pervez Ahmed, SaaS Multi-Tenancy Isolation Testing-*

Challenges and Issues - International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-5, November 2012

2. *Vijayanathan Naganathan, Sreesankar Sankarayya, Overcomming Challenges associated with SaaS Testing, Infosys, October 2011*

3. *Kees Blokland, Jeroen Mengerink, Martin Pol, Testing cloud service, Edwards Brothers Malloy, 2013*

Thông tin tác giả:



Trịnh Thuỳ Linh

Năm sinh: 1979

Lý lịch khoa học:

- Tốt nghiệp Trường Đại học Bách Khoa Hà nội năm 2002,
- Tốt nghiệp cao học Công nghệ thông tin năm 2009 tại Học viện Công nghệ Bru chính Viễn thông.

Hướng nghiên cứu: Kiểm thử các loại phần mềm trong lĩnh vực Công nghệ thông tin

Email: ttlinh@ptit.edu.vn