TỔNG QUAN GIẢI PHÁP GIÁM SÁT MẠNG TRÊN NỀN TẢNG MÃ NGUỒN MỞ

Lê Minh Quang[1]; Nguyễn Huyền Quang[1]

[1]Cục Công nghệ thông tin và dữ liệu tài nguyên môi trường, Bộ Tài nguyên và Môi trường

Email: lmquang_ccntt@monre.gov.vn; nhquang2@monre.gov.vn.

Tóm tắt: *Trong bài báo này, chúng tôi tập trung nghiên cứu về vấn đề giám sát hoạt động của một hệ thống mạng dựa trên phần mềm mã nguồn mở; đưa ra mô hình hoạt động tổng quan của một hệ thống giám sát thông qua một trong những phần mềm phổ biến nhất là Zabbix. Từ đó đề xuất hướng ứng dụng các giải pháp giám sát này vào trong hoạt động quản lý, giám sát thực tiễn tại các đơn vị thuộc Bộ Tài nguyên và Môi trường.*

Từ khóa: *Giám sát mạng; Mã nguồn mở; Zabbix.*

1. Đặt vấn đề

Cùng với sự phát triển của công nghệ thông tin, sự đầu tư cho hạ tầng mạng trong mỗi cơ quan, đơn vị ngày càng tăng cao, dẫn đến việc quản trị sự cố một hệ thống mạng gặp rất nhiều khó khăn. Đi cùng với những lợi ích khi phát triển hạ tầng mạng như băng thông cao, khối lượng dữ liệu trong mạng lớn, đáp ứng được nhu cầu của người dùng, hệ thống mạng phải đối đầu với rất nhiều thách thức như các cuộc tấn công bên ngoài, tính sẵn sàng của thiết bị, tài nguyên của hệ thống,… Một trong những giải pháp hữu hiệu nhất để giải quyết vấn đề này là thực hiện việc giải pháp giám sát hệ thống mạng, dựa trên những thông tin thu thập được thông qua quá trình giám sát, các cán bộ quản trị mạng có thể phân tích, đưa ra những đánh giá, dự báo, giải pháp nhằm giải quyết những vấn đề trên. Để thực hiện giám sát hệ thống mạng có hiệu quả, một chương trình giám sát phải đáp ứng được các yêu cầu sau: phải đảm bảo chương trình luôn hoạt động, tính linh hoạt, chức năng hiệu quả, đơn giản trong triển khai, chi phí thấp. Hiện nay, có khá nhiều phần mềm mã nguồn mở hỗ trợ việc giám sát mạng có hiệu quả như Nagios, Zabbix, Zenoss, Cacti,… Trong bài báo này chúng tôi sẽ giúp cho mọi người có cái nhìn tổng quan về một hệ thống giám sát mạng hoàn chỉnh thông qua việc tìm hiểu một trong những phần mềm giám sát phổ biến nhất là Zabbix.

2. Đối tượng và Phương pháp nghiên cứu

Đối tượng nghiên cứu của bài báo này là cách thức triển khai giải pháp giám sát mạng bằng phần mềm mã nguồn mở thông qua phần mềm zabbix, từ đó nêu lên được các ưu nhược điểm của giải pháp này. Để đạt được mục tiêu trên cần có những nghiên cứu về:

- Giám sát mạng là gì, cần giám sát những gì trong hệ thống mạng.
- Mô hình hoạt động tổng quan hệ thống giám sát mã nguồn mở Zabbix.
- Thử nghiệm tích hợp và đánh giá kết quả

3. Kết quả và bàn luận

3.1. Khái niệm giám sát mạng[1]

3.1.1. Khái niệm

Giám sát mạng Là một thuật ngữ dùng để chỉ việc sử dụng liên tục một hệ thống (có thể là một chương trình hoặc một thiết bị) để theo dõi tất cả các hoạt động của các thiết bị, các dịch vụ trong một hệ thống mạng.

3.1.2. Cần giám sát những gì và tại sao?

Đối với hệ thống mạng, điều quan trọng nhất là nắm được những thông tin chính xác nhất vào mọi thời điểm. Những thông tin cần nắm bắt khi giám sát một hệ thống mạng bao gồm:

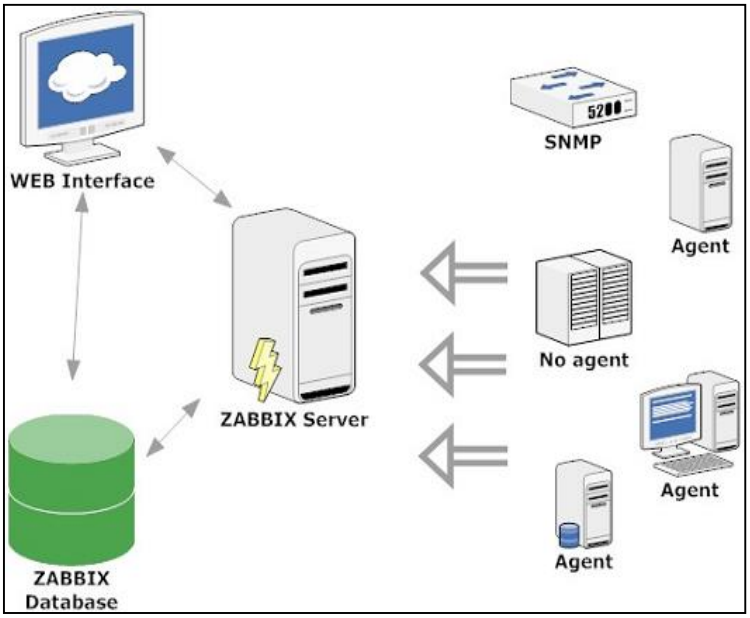
- Tính sẵn sàng của thiết bị (Router, Switch, Server,…): những thiết bị giữ cho mạng hoạt động.
- Các dịch vụ trong hệ thống (dns, ftp, http,…): những dịch vụ này đóng vai trò quan trọng trong một cơ quan, tổ chức, nếu các dịch vụ này không được đảm bào hoạt động bình thường và liên tục, nó sẽ ảnh hưởng nghiêm trọng đến cơ quan, tổ chức đó.
- Tài nguyên hệ thống: Các ứng dụng đều đòi hỏi tài nguyên hệ thống, việc giám sát tài nguyên sẽ đảm bảo cho chúng ta có những can thiệp kịp thời, tránh ảnh hưởng đến hệ thống.
- Lưu lượng trong mạng: nhằm đưa ra những giải pháp, ngăn ngừa hiện tượng quá tải trong mạng.
- Các chức năng về bảo mật: nhằm đảm bảo an ninh trong hệ thống.
- Nhiệt độ, thông tin về máy chủ, máy in: giúp tránh những hư hỏng xảy ra.

- Tạo file log: thu được những thông tin về những thay đổi trong hệ thống.

3.2. Mô hình hoạt động tổng quan của phần mềm giám sát mã nguồn mở zabbix

a. Đề xuất mô hình triển khai[1]

Zabbix là công cụ mà mã nguồn mở giải quyết vấn đề giám sát. Zabbix sử dụng một cơ chế thông báo linh hoạt cho phép người dùng cấu hình email cảnh báo dựa cho sự kiện bất kỳ. Điều này cho phép giải quyết nhanh của các vấn đề Server. Zabbix cung cấp báo cáo và dữ liệu chính xác dựa trên cơ sở dữ liệu.Điều này khiến cho Zabbix trở lên lý tưởng hơn. Zabix gồm các thành phần cơ bản sau:



Hình 1. Mô hình Zabbix

- **Zabbix server:**

Đây là thành phần trung tâm của phần mềm Zabbix. Server có thể kiểm tra các dịch vụ mạng từ xa (web server và mail server). Agent sẽ báo cáo toàn bộ thông tin và số lượng thống kê cho server. Server sẽ lưu trữ tất cả cấu hình và dữ liệu thống kê.

- **Zabbix proxy:**

  - Proxy là phần tuỳ chọn của Zabbix. Proxy sẽ thu nhận dữ liệu , lưu trong bộ nhớ đệm và được chuyển đến Zabbix server.
  - Zabbix Proxy là một giải pháp lý tưởng cho một giám sát tập trung của địa điểm từ xa, chi nhánh, mạng lưới không có các quản trị viên địa phương.
  - Zabbix proxy cũng có thể được sử dụng để phân phối tải của một đơn Zabbix Server.

- **Zabbix agent:**

Để giám chủ động giám sát các thiết bị cục bộ và các ứng dụng (ổ cứng, bộ nhớ, bộ xử lý số liệu thống kê, …) trên hệ thống mạng, các hệ thống phải chạy Zabbix Agent. Agent sẽ thu thập thông tin hoạt động từ hệ thống mà nó đang chạy và báo cáo dữ liệu này đến Zabbix server để xử lý tiếp. Trong trường hợp lỗi (ổ cứng đầy hoặc dịch vụ của một quá trình chết), các Zabbix server báo cho quản trị viên sự cố này.

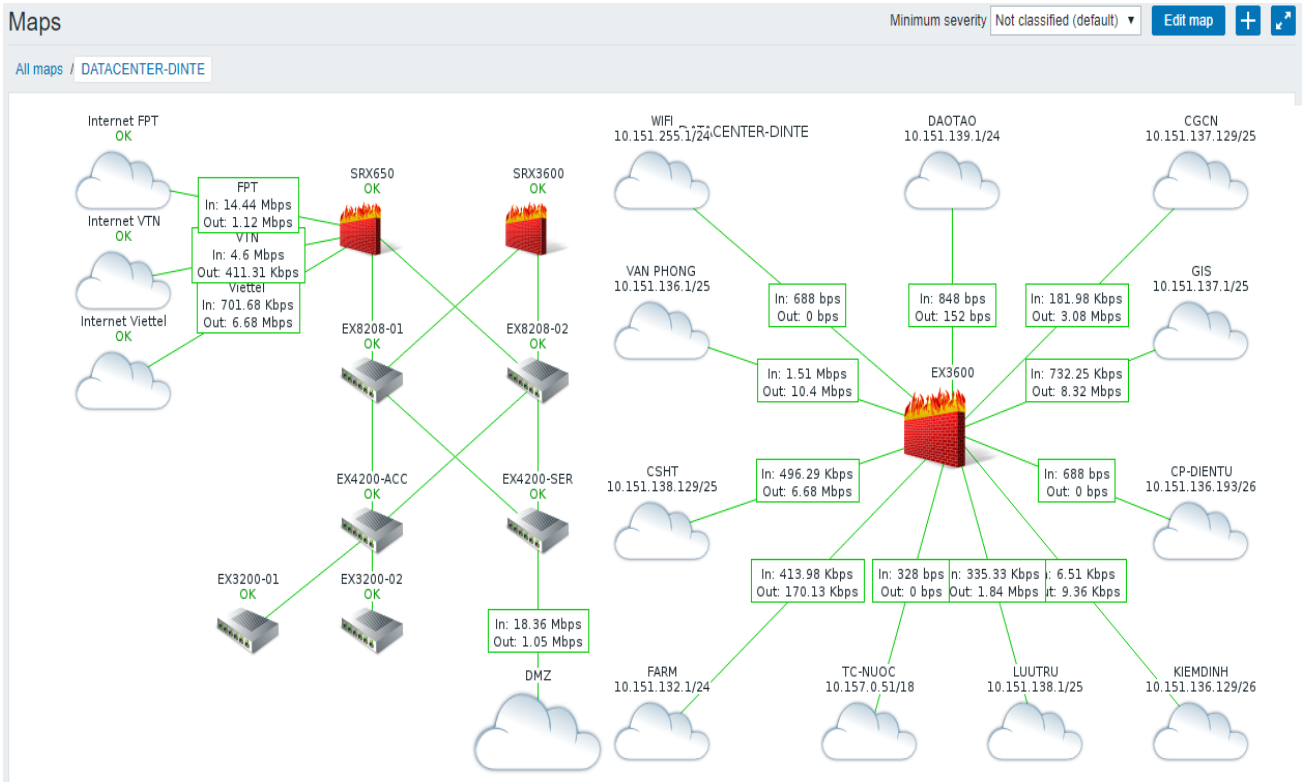
- **Web interface:**

Để dễ dàng truy cập dữ liệu theo dõi và sau đó cấu hình Zabbix từ bất cứ giao diện web cung cấp. Giao diện là một phần của Zabbix server, và thường chạy trên các máy vật lý giống như đang chạy một trong các Zabbix server.

Để triển khai và đánh giá hoạt động của phần mềm Zabbix, chúng tôi đã đưa vào thử nghiệm tại mô hình thực tế đang hoạt động tại Trung tâm dữ liệu Trụ sở Bộ Tài nguyên và Môi trường.

Các bước tiến hành như sau:

- Cài đặt các thành phần của Zabbix gồm: Zabbix server, Zabbix proxy, Zabbix agent và Web Interface[2]:



Hình 2. Mô hình triển khai thực tế

- Tạo CSDL Zabbix (Trong bước cài đặt Zabbix server):

```
shell> mysql -u<username> -p<password>
mysql> create database zabbix character set utf8;
mysql> quit;
shell> cd create/schema
shell> cat mysql.sql | mysql -u<username> -p<password> zabbix
shell> cd ../data
shell> cat data.sql | mysql -u<username> -p<password> zabbix
shell> cat images_mysql.sql | mysql -u<username> -p<password>
zabbix
```

- Cài đặt Zabbix agent:

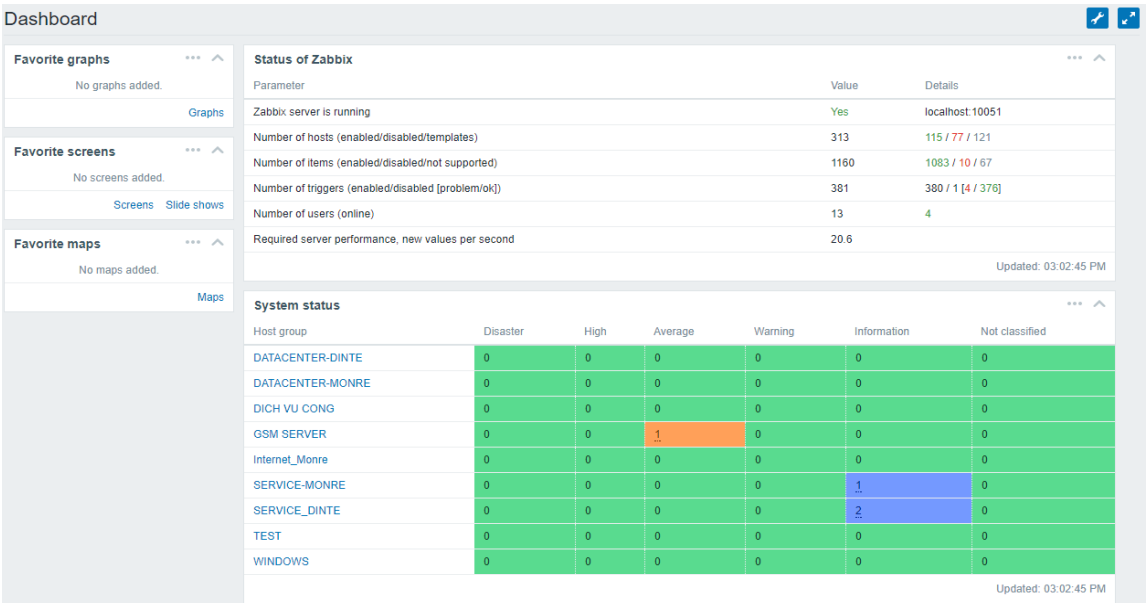
```
Shell> useradd zabbix
shell> gunzip zabbix-1.6.tar.gz && tar -xvf zabbix-1.6.tar
shell> ./configure --enable-agent
shell> make
zabbix_agent 10050/tcp
zabbix_agent stream tcp nowait.3600 zabbix /opt/zabbix/bin/zabbix_agent
shell> killall -HUP inetd
shell> /opt/zabbix/bin/zabbix_agentd
```

- Theo dõi, giám sát mạng thông qua Web interface[1]:

Sau khi cài đặt xong các thành phần của phần mềm, chúng ta có thể dễ dàng theo dõi, giám sát các thông số của hệ thống thông qua giao diện web:

- Bảng điều khiển:

Bảng 1. Bảng điều khiển (Dashboard)



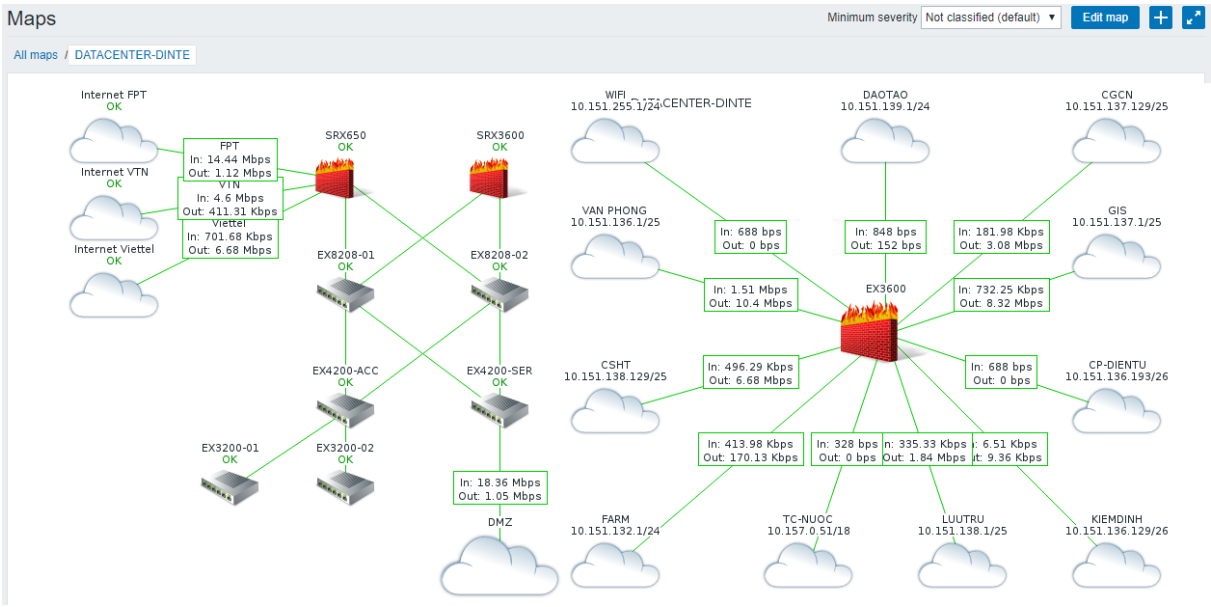
- Các thông số kỹ thuật của thiết bị theo dõi như: CPU, RAM, nhiệt độ…
- Trạng thái hoạt động của thiết bị, đường truyền;
- Bảng cảnh báo khi có các thông số vượt quá ngưỡng cho phép;
- Các sự kiện diễn ra trong hệ thống mạng;
- Sơ đồ hệ thống;
- Cảnh báo qua email, SMS

Bảng 2. Bảng trigger cảnh báo

Severity	Status	Info	Last change ▾	Age	Ack	Host	Name	Description
Average	PROBLEM		08/27/2017 07:03:00 PM	24d 20h 2m	No 1	Máy chủ giám sát mang	Zabbix agent on Máy chủ giám sát mang is unreachable for 5 minutes	Add
Information	PROBLEM		08/03/2017 10:38:31 AM	1m 19d 4h	No 1	CSDLQG - standby database	ORACLE service	Add
Information	PROBLEM		08/03/2017 10:38:02 AM	1m 19d 4h	No 1	CSDLQG - primary database	ORACLE service	Add
Information	PROBLEM		08/03/2017 10:37:02 AM	1m 19d 4h	No 1	HQ-DB	POSTGESQL service	Add

Displaying 4 of 4 found

Bảng 3. Bảng sự kiện



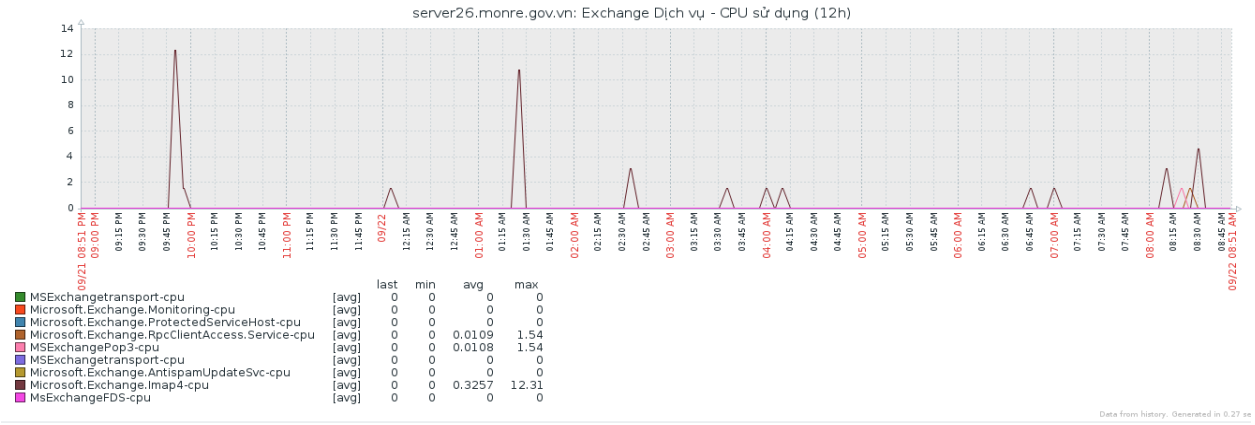
Hình 3. Sơ đồ hệ thống

b. Đánh giá kết quả triển khai

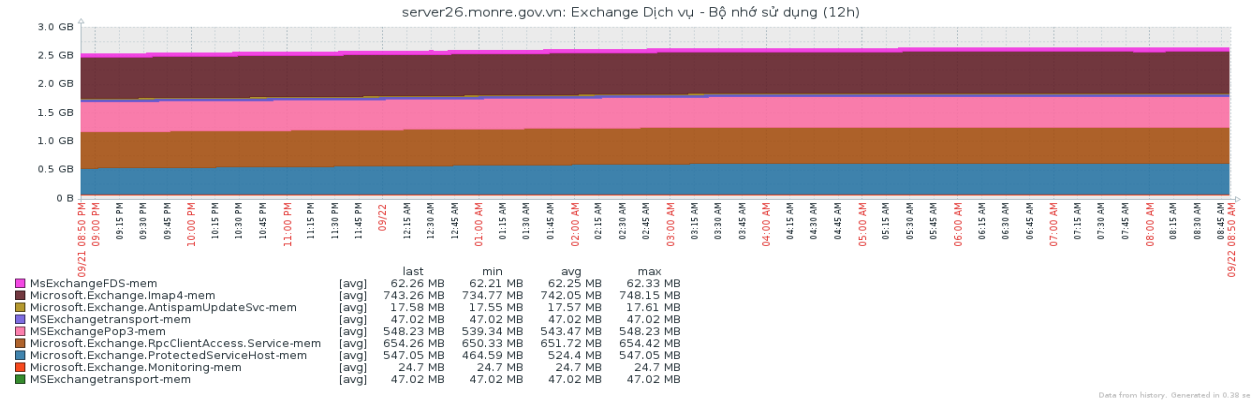
- Kết quả triển khai:

Chúng tôi đã triển khai thử nghiệm phần mềm giám sát trên mô hình thực tế đang triển khai tại Trung tâm dữ liệu Trụ sở Bộ Tài nguyên và Môi trường. Một số nội dung chính giám sát như sau:

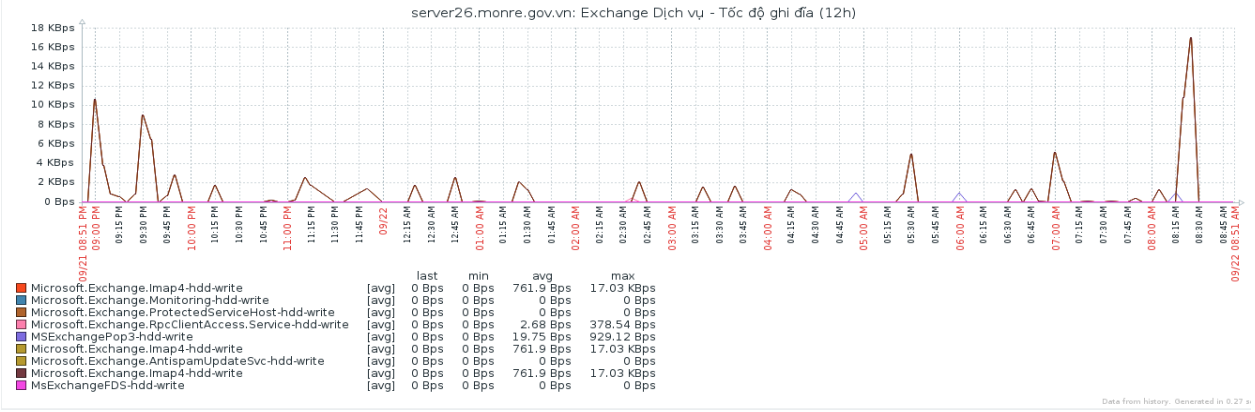
+ Giám sát tài nguyên của các máy chủ, ứng dụng, dịch vụ như CPU, RAM, tốc độ đọc, ghi ổ cứng…



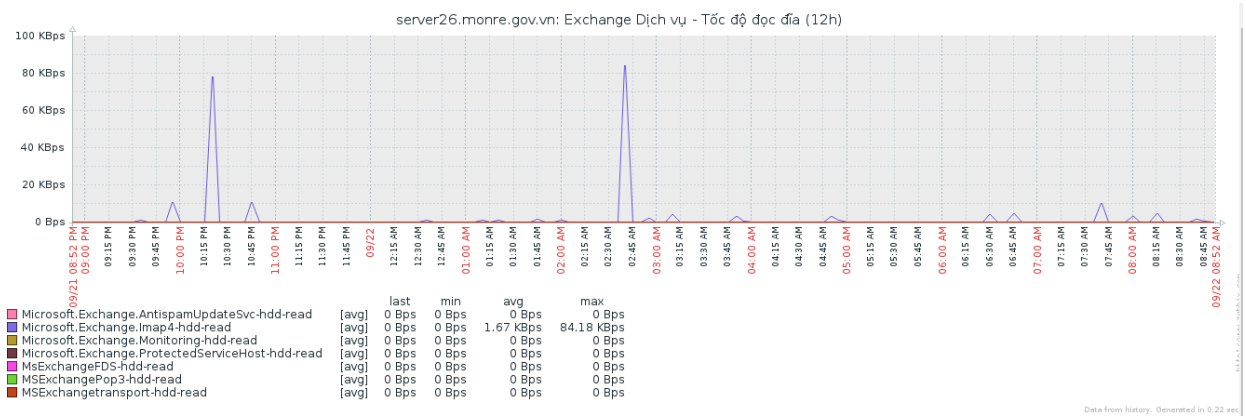
Hình 4: Biểu đồ % CPU sử dụng của các dịch vụ mail



Hình 5: Biểu đồ dung lượng RAM sử dụng

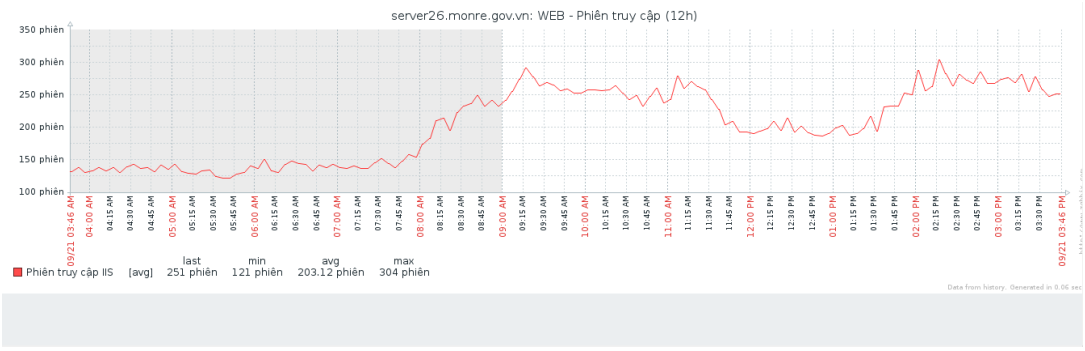


Hình 6: Tốc độ ghi ổ đĩa

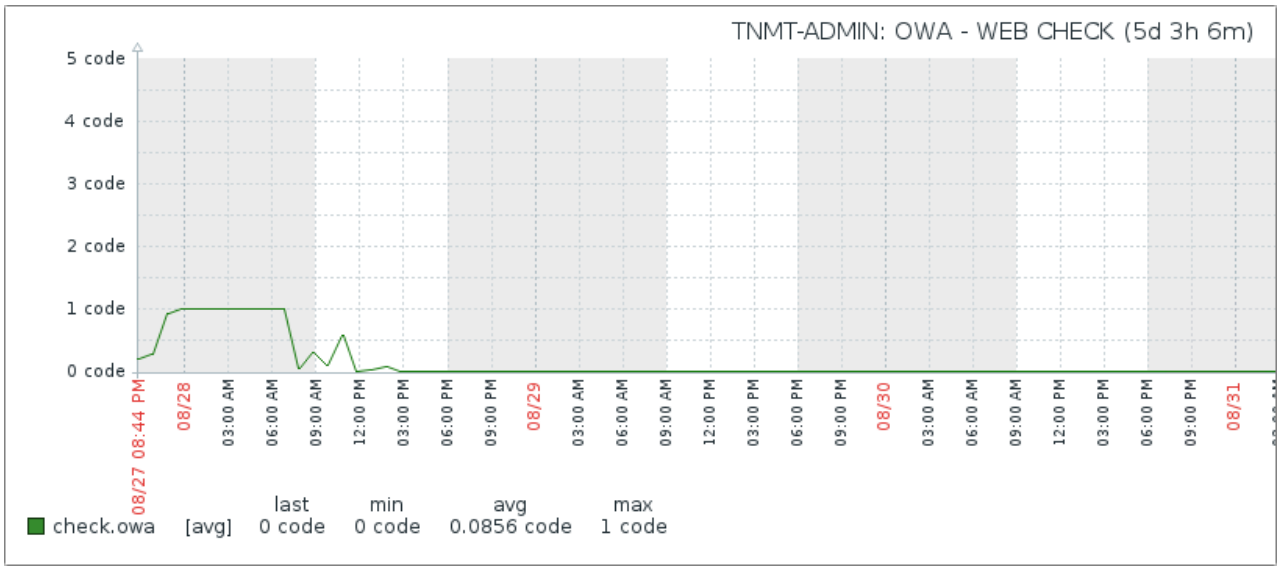


Hình 7: Tốc độ đọc ổ đĩa

+ Giám sát dịch vụ thư điện tử công vụ mail.monre.gov.vn:

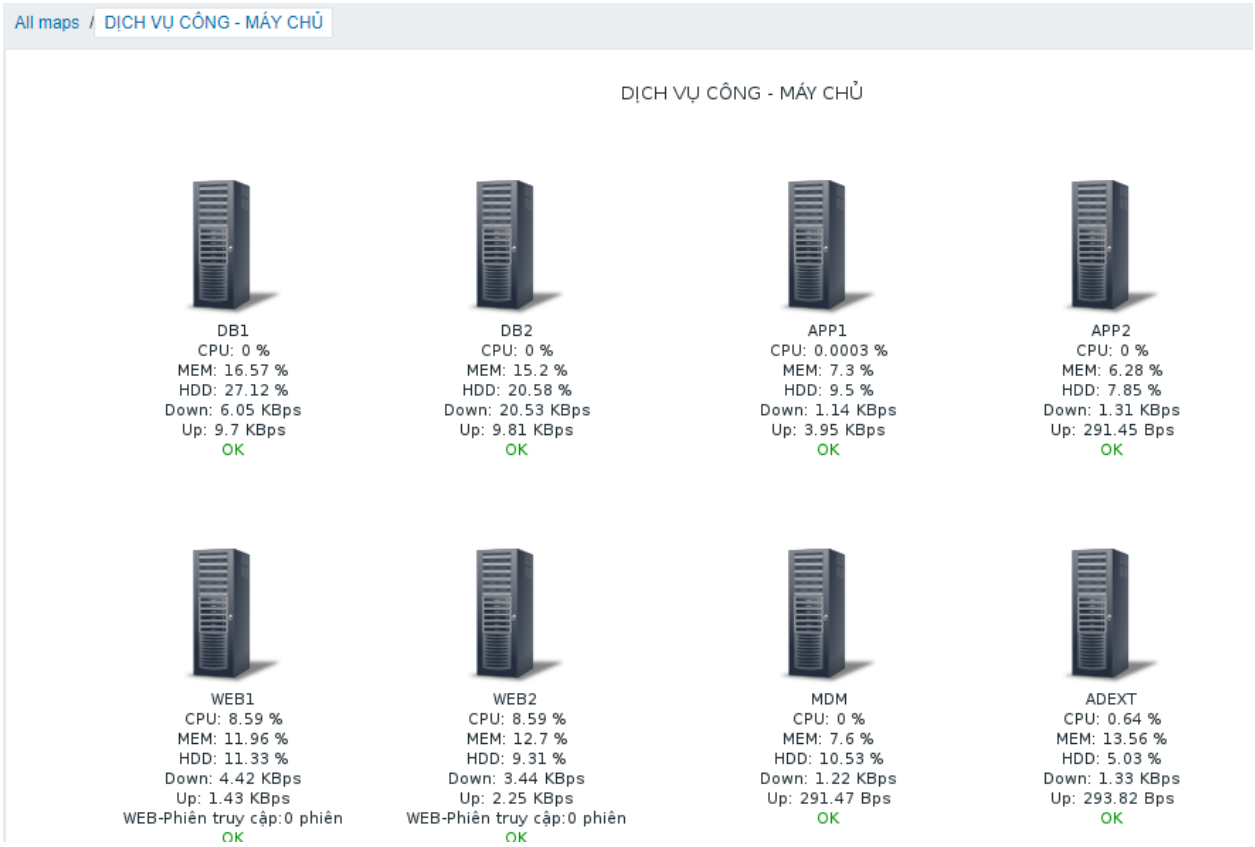


Hình 8: Phiên truy cập Wab mail.monre.gov.vn

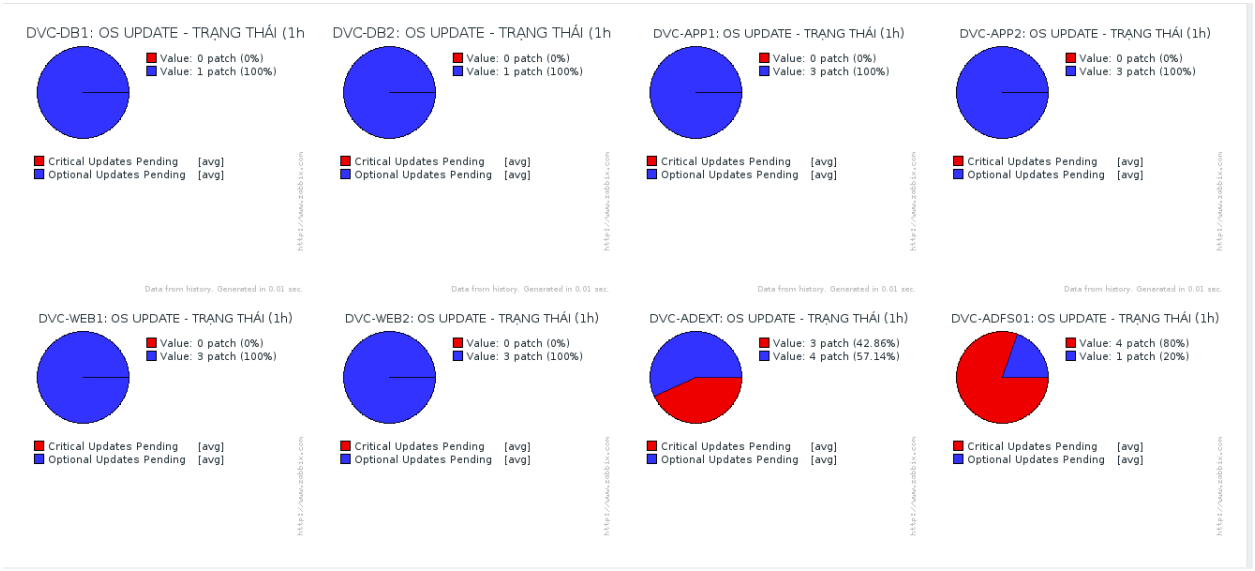


Hình 9: Giám sát dịch vụ Web mail theo tiêu chí

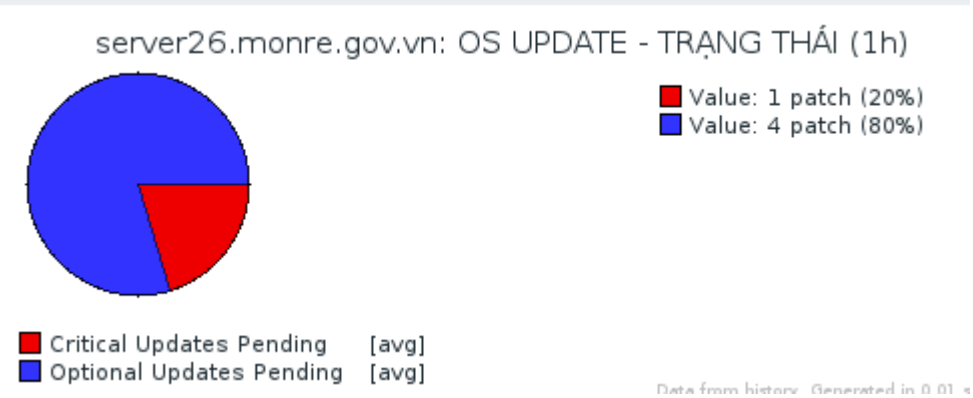
+ Giám sát hệ thống máy chủ Dịch vụ công:



Hình 10:Máy chủ dịch vụ công



Hình 11a: Biểu đồ % và số bản vá hệ điều hành (máy chủ Dịch vụ công)



Hình11 b: Biểu đồ % và số bản vá hệ điều hành

- Đánh giá kết quả triển khai:

Sau thử nghiệm phần mềm Zabbix để giám sát mô hình mạng trên, chúng tôi đã so sánh, phân tích, đánh giá với thời điểm hệ thống mạng chưa được giám sát và đưa ra các kết luận như sau:

+ Các hệ thống được giám sát đã chạy ổn định và an toàn hơn rất nhiều so với trước đây;

+ Hệ thống giám sát đã giúp cho cán bộ kỹ thuật theo dõi được rất nhiều các thông tin của hệ thống mạng, giảm thiểu thời gian, thao tác quản trị so với lúc chưa triển khai hệ thống;

+ Giúp người quản trị phản ứng nhanh hơn, hiệu quả hơn trước các mối nguy hiểm cũng như các sự cố có thể xảy ra;

+ Việc sử dụng phần mềm giám sát cũng giúp người quản trị hiểu rõ, sâu sắc hơn về toàn bộ hệ thống mạng;

+ Triển khai phần mềm giám sát là vấn đề tất yếu đối với việc đảm bảo hệ thống hoạt động liên tục, ổn định, an ninh, an toàn.

Ngoài ra chúng tôi cũng nghiên cứu và so sánh phần mềm Zabbix với các phần mềm giám sát mã nguồn mở tương đương như Cacti, Zenoss, Nagios và đưa ra đánh giá ưu, nhược điểm của phần mềm này nói riêng và phần mềm giám sát mã nguồn mở nói chung như sau:

- Ưu điểm:

- Cài đặt, cấu hình dễ dàng: Zabbix làm việc như thế nào, tập tin cấu hình ở đâu, các luật như thế nào người quản trị đều có thể biết và cấu hình theo ý mình được. Kể cả việc tạo ra các luật mới.

- Sử dụng mã nguồn mở nên chi phí triển khai thấp
- Tất các các thông tin (cấu hình, hiệu suất) được lưu trong cơ sở dữ liệu.
- Hỗ trợ rất nhiều giao thức giám sát như SNMP (v1, v2), ICMP, WMI

dẫn đến có thể giám sát rất nhiều các thông số của hệ thống

- Giao diện trực quan.
- Hỗ trợ rất nhiều hệ điều hành máy chủ, máy
- Được phân phối theo dõi bởi admin
- Đáng tin cậy trong việc chứng thực người dùng.
- Linh hoạt trong việc phân quyền người dùng
- Có thể thông báo sự cố qua email,SMS

- Nhược điểm:

- Không có sự hỗ trợ kỹ thuật một cách chính thức, ít tài liệu, giao diện không được chăm chút nhiều.
- Hạn chế tính năng:theo giới chuyên môn, các phần mềm mã nguồn mở vẫn còn kém xa về chất lượng so với các phần mềm có thu phí.
- Thiếu sáng tạo: các phiên bản của phần mềm này thường chỉ có một nhiệm vụ duy nhất là bắt chước y hệt các tính năng của bản nâng cấp của các phần mềm có thu phí.

4. Kết luận

Qua các phân tích ở trên chúng ta có thể nhận thấy rằng giám sát mạng là vô cùng quan trọng. Trong đó giải pháp giám sát mạng bằng các phần mềm mã nguồn mở là một trong các lựa chọn hàng đầu bởi vì nó có rất nhiều các ưu điểm:

- Quản lý tập trung log, từ đó đưa ra những cảnh báo sớm (bằng email hoặc tin nhắn) gửi cho quản trị mạng khi có sự cố xảy ra (như đứt đường truyền, chết dịch vụ, hỏng ổ cứng, hỏng card mạng, quá tải RAM, quá tải CPU, vv)
- Dễ dàng mở rộng và quản lý đến hàng vài ngàn thiết bị
- Miễn phí, chỉ mất chi phí triển khai trên máy tính
- Có sẵn nhiều mẫu Template được viết sẵn cho các loại thiết bị mạng, máy chủ và các hệ điều hành khác nhau.
- Dễ dàng tạo các Templates cho các thiết bị
- Cho phép bổ sung nhiều chương trình plugin tiện ích, cho phép triển khai nhanh chóng hệ thống quản lý tài nguyên mạng với chi phí hợp lý.

Qua triển khai thử nghiệm trên mô hình thực tế tại trụ sở Bộ Tài nguyên và môi trường chúng tôi nhận thấy việc áp dụng các giải pháp giám sát bằng phần mềm mã nguồn mở trong các đơn vị thuộc Bộ Tài nguyên và Môi trường là hoàn toàn khả thi trên nhiều phương diện: Tài chính, độ phức tạp kỹ thuật, nguồn nhân lực thực hiện… Do đó chúng tôi dự kiến hướng phát triển tiếp theo là sẽ kiến nghị

các đơn vị có thẩm quyền tạo điều kiện để nhân rộng mô hình giám sát này trong cũng như ngoài Bộ Tài nguyên và Môi trường.

TÀI LIỆU THAM KHẢO

[1]. Kết quả nghiên cứu các chuyên đề trong đề tài "Nghiên cứu, thiết kế, xây dựng phần mềm giám sát hệ thống mạng thông tin ngành tài nguyên và môi trường sử dụng giải pháp mã nguồn mở" chủ nhiệm Lê Minh Quang (đề tài đang trong quá trình thực hiện).

[2]. Nguyễn Thị Thanh Vân (2008), *Hệ điều hành mạng Unix*, Trường Đại Học Sư Phạm Kỹ Thuật Tp.HCM.

[3]. *Zabbix Monitoring Solution, Zabbix Solution in Government* , Zabbix LLC, truy cập ngày 04 tháng 9 năm 2017, http://www.zabbix.com/.

OVERVIEW OF OPENSOURCE-BASED NETWORK MONITORING SOLUTION

Le Minh Quang[1]; Nguyen Huyen Quang[1]

[1]Department of Information Technology and Environment Resources Data

Abstract: *In this article, we focus on the subject of monitoring operation of network components - based on open source solution; present the overview of deploy model from zabbix - a popular monitoring solution. Propose a method to apply the solution for managing, monitoring at units under the Ministry of Natural Resources and Environment.*

Keywords: *network monitoring; opensource code; zabbix.*