|  |
| --- |
| HỌC VIỆN KỸ THUẬT MẬT MÃ  **AN TOÀN THÔNG TIN**  ¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯  Logo HvKTMM  Phân tích & thu thập An ninh mạng |
| **Hệ thống giám sát tập trung**  **sử dụng zabbix** |
| Nhóm: Nguyễn Văn Minh  Nguyễn Tuấn Anh  Nguyễn Quốc Thành  Vũ Minh Vương    Hà Nội, 2019 |

Mục lục

[I. Giới thiệu về Monitoring 3](#_Toc7698490)

[II. Tổng quan về Zabbix 5](#_Toc7698491)

[1. Ưu điểm của Zabbix 5](#_Toc7698492)

[2. Các thành phần cơ bản của Zabbix 6](#_Toc7698493)

[Zabbix server 6](#_Toc7698494)

[Zabbix Proxy 6](#_Toc7698495)

[Zabbix Agent 6](#_Toc7698496)

[Web interface 7](#_Toc7698497)

[3. Cơ chế thu thập dữ liệu: 7](#_Toc7698498)

[3.1. Zabbix Passive Check 7](#_Toc7698499)

[3.2. Zabbix Active Check 8](#_Toc7698500)

[III. Hướng dẫn cài đặt 9](#_Toc7698501)

[1. Mô hình cài đặt 9](#_Toc7698502)

[Mô hình: 9](#_Toc7698503)

[IP Planing: 10](#_Toc7698504)

[2. Các bước cài đặt 10](#_Toc7698505)

[Bước 1: Cài đặt zabbix-server 10](#_Toc7698506)

[Bước 2: Cấu hình Mysql cho zabbix 11](#_Toc7698507)

[Bước 3: Cấu hình PHP cho zabbix 12](#_Toc7698508)

[Bước 4: Cấu hình cho Zabbix Web Interface 13](#_Toc7698509)

[Bước 5: Cấu hình zabbix agent 16](#_Toc7698510)

[Bước 6: Cấu hình zabbix agent trên window 17](#_Toc7698511)

[IV. Hướng dẫn quản trị 23](#_Toc7698512)

[1. Thêm host 23](#_Toc7698513)

[2. Thêm Template cho host 25](#_Toc7698514)

[3. Thêm item cho host 26](#_Toc7698515)

[4. Thêm trigger 29](#_Toc7698516)

[V. Demo 31](#_Toc7698517)

I. Giới thiệu về Monitoring

1. Một số khái niệm cơ bản

Để một hệ thống mạng hoạt động tốt nó bao gồm rất nhiều thành phần, hoạt động trên các nền tảng và mỗi trường khác nhau

* Các máy trạm
* Các máy chủ
* Các thiết bị hạ tầng mạng: Router, switch, Hub…
* Các thiết bị, hệ thống phát hiện và phòng chống xâm nhập: IDS/IPS, Snort, FireWall…
* Các ứng dụng chạy trên các máy chủ và máy trạm.

Giám sát An ninh mạng: Giám sát an ninh mạng là việc thu thập các thông tin trên các thành phần của hệ thống, phân tích các thông tin, dấu hiệu nhằm đánh giá và đưa ra các cảnh báo cho người quản trị hệ thống.

Đối tượng của giám sát an ninh mạng là tất cả các thành phần, thiết bị trong hệ thống mạng

* Các máy trạm
* Cơ sở dữ liệu
* Các ứng dụng
* Các server
* Các thiết bị mạng

2. Các bước thực hiện của một hệ thống giám sát

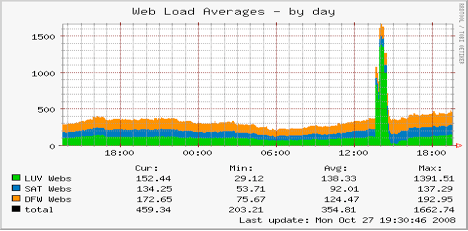
a.Thu thập dữ liệu

Việc thu thập dữ liệu ở đây chính là việc lấy các thông tin liên quan đến tình trạng hoạt động của các thiết bị trong hệ thống mạng. Tuy nhiên, trong những hệ thống mạng lớn thì các dịch vụ hay các thiết bị không đặt tại trên máy, một địa điểm mà nằm trên các máy chủ, các hệ thống con riêng biệt nhau. Các thành phần hệ thống cũng hoạt động trên những nền tảng hoàn toàn khác nhau. Mô hình Log tập trung được đưa ra để giải quyết vấn đề này. Cụ thể, là tất cả Log sẽ được chuyển về một trung tâm để phân tích và xử lý.

Với mỗi thiết bị có những đặc điểm riêng và các loại log cũng khác nhau. Như log của các thiết bị mạng như: Router, Swich. Log của các thiết bị phát hiện xâm nhập: IDS, IPS, Snort … Log của các Web Server, Application Server, Log Event, Log Registry của các Server Windows, Unix/Linux.

b.Phân tích dữ liệu

Khi đã thu thập được những thông tin về hệ thống thì công việc tiếp theo là phân tích thông tin, cụ thể là việc thực hiện chỉ mục hóa dữ liệu, phát hiện những điều bất thường, những mối đe dọa của hệ thống. Dựa trên những thông tin về lưu lượng truy cập, trạng thái truy cập, định dạng request… Ví dụ như lưu lượng truy cập bỗng dưng tăng vọt tại một thời điểm. Đây có lẽ là nơi thích hợp để Big data lên tiếng.



c.Cảnh báo

Sau khi đã thực hiện việc phân tích dữ liệu từ các thông tin thu thập được việc tiếp theo là thực hiện việc đánh giá, đưa thông tin cảnh báo tới người quản trị và thực hiện những công tác nhằm chống lại những mỗi đe dọa, khắc phục các sự cố có thể sảy ra.

Cảnh báo có thể thông qua email, SMS, hoặc thực thi các mã script nhằm hạn chế hậu quả của sự cố. Khi xảy ra sự cố, hệ thống sẽ tự động gửi email, sms cho người quản trị và cũng có thể chạy script để thêm một địa chỉ IP có biểu hiện tấn công và danh sách đen của Firewall. Việc này đòi hỏi người lập trình phải có hiểu biết sâu và kinh nghiệm về hệ thống.

II. Tổng quan về Zabbix

Zabbix là một phần mềm giám sát mã nguồn mở. Nó tập trung giám sát hàng nghìn máy chỉ, , máy ảo và các thiết bị mạng được thu thập và gửi về ở bất kì đâu và ở mọi lúc. Các chỉ số này có thể giúp bạn xác định tình trạng hiện tại của cơ sở hạ tầng CNTT của bạn và phát hiện sự cố với các thành phần phần cứng hoặc phần mềm trước khi khách hàng phản ánh. Các thông tin hữu ích này được lưu lại trong cơ sở dữ liệu để các chuyên gia có thể phân tích dữ liệu và cải thiện dịch vụ cung cấp hoặc lên kế hoạch nâng cấp hệ thống.

Zabbix sử dụng kiến trúc client-server, các máy client được cài đặt agent lên để thu thập thông số metric sau đó gửi kết quả về phía server. Zabbix phiên bản 3 hỗ trợ việc mã hóa thông tin trên đường truyền giữa máy chủ và máy khách, vì vậy dữ liệu được bảo vệ trong khi nó truyền qua môi trường mạng không an toàn.

Zabbix sử dụng database là Mysql, PostgreSQL, or Oracle. Nó còn có giao diện web để xem dữ liệu giám sát và cấu hình.

## 1. Ưu điểm của Zabbix

- Giám sát được cả server và thiết bị mạng

- Dễ dàng thao tác và cấu hình

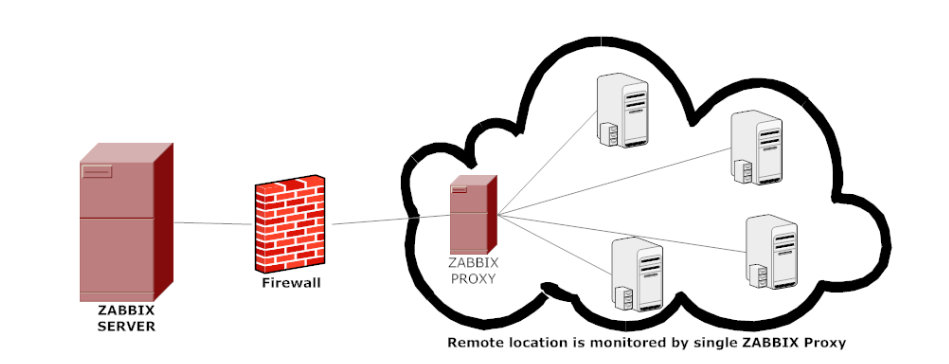
- Hỗ trợ máy chủ Linux, Solaris, FreeBSD …

- Đáng tin cậy trong việc chứng thực người dùng

- Giao diện web đẹp mắt

- Mã nguồn mở và chi phí thấp

## 2. Các thành phần cơ bản của Zabbix



### Zabbix server

Đây là thành phần trung tâm của phần mềm Zabbix. Zabbix Server có thể kiểm tra các dịch vụ mạng từ xa thông qua các báo cáo của Agent gửi về cho Zabbix Server và từ đó nó sẽ lưu trữ tất cả các cấu hình cũng như là các số liệu thống kê.

### Zabbix Proxy

Là phần tùy chọn của Zabbix. Nó có nhiệm vụ thu nhận dữ liệu, lưu trong bộ nhớ đệm và chuyển đến Zabbix Server.  
 Zabbix Proxy là một giải pháp lý tưởng cho việc giám sát tập trung của các địa điểm từ xa, chi nhánh công ty, các mạng lưới không có quản trị viên nội bộ.  
 Zabbix Proxy cũng được sử dụng để phân phối tải của một Zabbix Server.

### Zabbix Agent

Để giám sát chủ động các thiết bị cục bộ và các ứng dụng (ổ cứng, bộ nhớ, …) trên hệ thống mạng. Zabbix Agent sẽ được cài lên trên Server và từ đó Agent sẽ thu thập thông tin hoạt động từ Server mà nó đang chạy và báo cáo dữ liệu này đến Zabbix Server để xử lý.

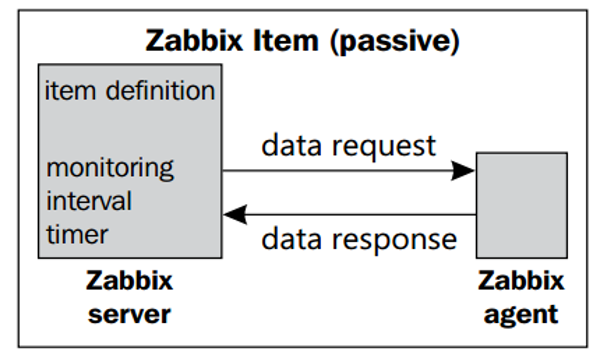
### Web interface

Để dễ dàng truy cập dữ liệu theo dõi và sau đó cấu hình từ giao diện web cung cấp. Giao diện là một phần của Zabbix Server, và thường chạy trên các máy chủ.

## 3. Cơ chế thu thập dữ liệu:

Như chúng ta đã được biết, Zabbix server thu thập thông tin từ Agent thông qua các item tương ướng. Các item có nhiều loại, tuy nhiên 2 loại chính là Active Item (Item chủ động) và Passive Item (Item bị động). Vậy nên việc kiểm tra phân loại chủ động (active) hay bị động (passive) dựa vào giá trị item đang sử dụng ở dạng active hay passive.

### 3.1. Zabbix Passive Check

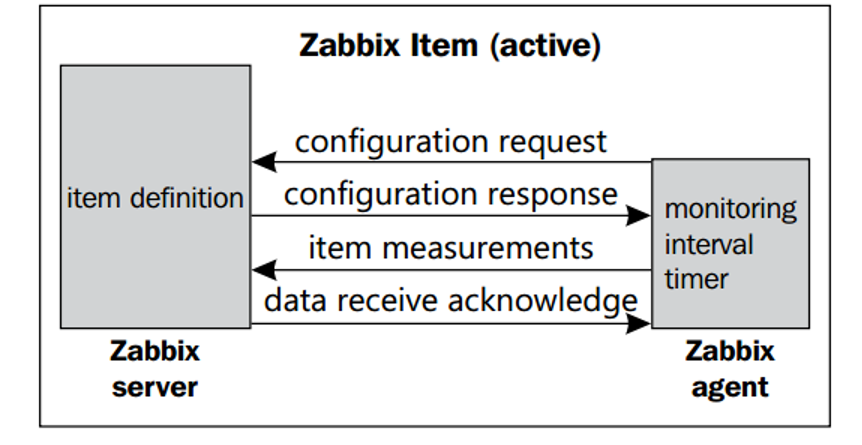


* Đây là kiểu kiểm tra tương ứng với Item Zabbix Passive, kiểu này có đặc tính là công việc ưu cầu thông tin cần giám sát thuộc về Zabbix Server.
* Zabbix Server sẽ request thông tin cần tìm kiếm đến các Agent theo các khoảng thời gian (interval time) đã được cấu hình trong item tương ứng, lấy thông tin monitor và báo cáo lại về hệ thống ngay lập tức. Server khởi tạo kết nối, Agent luôn ở chế động lắng nghe kết nối từ Server.

Tiến trình:

* Server mở kết nối TCP đến Zabbix Agent
* Server gửi ưu cầu thu thập thông tin với item tương ứng. Ví dụ : "agent.ping"
* Agent nhận ưu cầu, phân tích, thu thập dữ liệu và gửi trả về Server. Với item "agent.ping", kết quả trả về ở đây sẽ là "0" hoặc "1".
* Kết nối TCP đóng lại

### 3.2. Zabbix Active Check



* Đây là kiểu kiểm tra tương ứng với Item Active (chủ động), đặc tính của kiểu này là công việc chủ động request thông tin cần giám sát thuộc về Zabbix Agent. Kiểu kiếm tra này hay dùng khi Zabbix Server không thể kết nối trực tiếp đến Zabbix Agent (có thể do chính sách firewall...)
* Zabbix Agent sẽ chủ động gửi request đến Zabbix Server nhằm lấy thông tin về các Item được Server chỉ định sẵn. Sau khi lấy được danh sách item thì Agent sẽ xử lý động lập rồi gửi tuần tự thông tin về cho Server. Server sẽ không khởi tạo kết nối nào mà chỉ trả lời request item list và nhận lại thông tin được trả về. Tuy nhiên nếu Agent trei hoặc chết thì Server sẽ không nhận được bất kỳ kết nối nào.

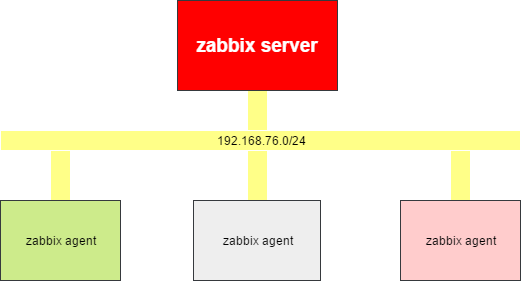
Tiến trình :

* Agent mở kết nối TCP đến Zabbix Server
* Agent yêu cầu danh sách item cần thu thập
* Server phản hồi với danh sách item tương ứng ( danh sách này đã được định sẵn trước đó, gồm item key, delay).
* Kết nối TCP đóng lại.
* Agent bắt đầu thu thập thông tin tương ứng với danh sách item nhận được.

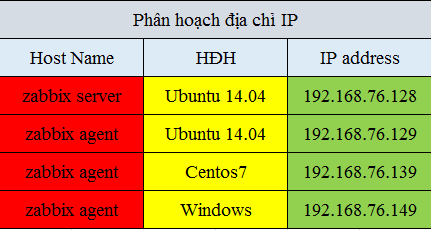
# III. Hướng dẫn cài đặt

## 1. Mô hình cài đặt

### Mô hình:



### IP Planing:

****

## 2. Các bước cài đặt

Sử dụng zabbix server và zabbix agent có OS là CentOS 7

### Bước 1: Cài đặt zabbix-server

- SSH hoặc Login vào zabbix-server bằng tài khoản root

- Install package tử repo zabbix trên CentOS7

|  |
| --- |
| sudo rpm -ivh http://repo.zabbix.com/zabbix/3.0/rhel/7/x86\_64/zabbix-release-3.0-1.el7.noarch.rpm |

- Kết quả của output

|  |
| --- |
| Retrieving http://repo.zabbix.com/zabbix/3.0/rhel/7/x86\_64/zabbix-release-3.0-1.el7.noarch.rpm warning: /var/tmp/rpm-tmp.qLbOPP: Header V4 DSA/SHA1 Signature, key ID 79ea5ed4: NOKEY Preparing... ################################# [100%] Updating / installing...  1:zabbix-release-3.0-1.el7 ################################# [100%] |

- Cài đặt Zabbix server và web frontend

|  |
| --- |
| sudo yum install zabbix-server-mysql zabbix-web-mysql |

- Tải zabbix agent

|  |
| --- |
| sudo yum install zabbix-agent |

### Bước 2: Cấu hình Mysql cho zabbix

- Đăng nhập vào MySQL với tư cách người dùng root mà bạn đã thiết lập trong quá trình cài đặt máy chủ MySQL:

|  |
| --- |
| mysql -uroot -p |

- Tạo database cho zabbix

|  |
| --- |
| create database zabbix character set utf8;  grant all privileges on zabbix.\* to zabbix@localhost identified by 'your\_password';  flush privileges;  quit; |

- Import cấu trúc cơ sở dữ liệu vào database vừa tạo

|  |
| --- |
| cd /usr/share/doc/zabbix-server-mysql-3.0.4/  zcat create.sql.gz | mysql -uzabbix -p zabbix |

Nhập mật khẩu zabbix mà bạn vừa tạo lúc create database

- Để máy chủ Zabbix sử dụng cơ sở dữ liệu này, bạn cần đặt mật khẩu cơ sở dữ liệu trong tệp cấu hình máy chủ Zabbix.

|  |
| --- |
| sudo vi /etc/zabbix/zabbix\_server.conf |

|  |
| --- |
| ### Option: DBPassword  # Database password. Ignored for SQLite.  # Comment this line if no password is used. #  # Mandatory: no  # Default:  DBPassword=your\_zabbix\_mysql\_password |

### Bước 3: Cấu hình PHP cho zabbix

- Chỉnh sửa file /etc/httpd/conf.d/

|  |
| --- |
| sudo vi /etc/httpd/conf.d/zabbix.conf |

|  |
| --- |
| <IfModule mod\_php5.c>  php\_value max\_execution\_time 300  php\_value memory\_limit 128M  php\_value post\_max\_size 16M  php\_value upload\_max\_filesize 2M  php\_value max\_input\_time 300  php\_value always\_populate\_raw\_post\_data -1  # php\_value date.timezone Europe/Riga </IfModule> |

- Khởi động lại http

|  |
| --- |
| sudo systemctl restart httpd |

- Khởi động lại zabbix server

|  |
| --- |
| sudo systemctl start zabbix-server |

- Kiểm tra status zabbix server bằng lệnh

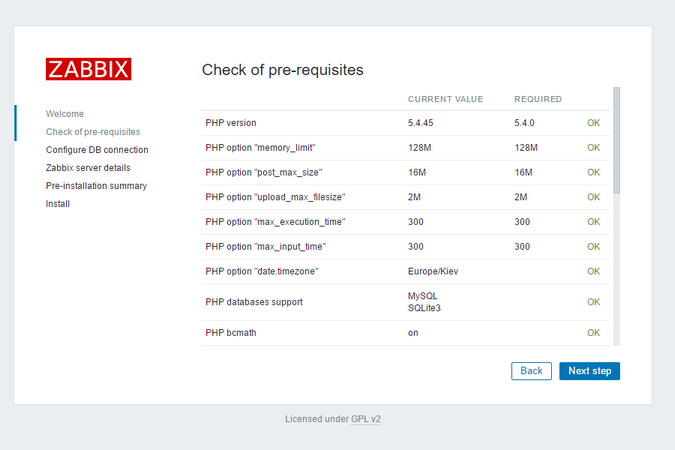
|  |
| --- |
| sudo systemctl status zabbix-server |

- Cho phép khởi động zabbix server cùng thệ thống

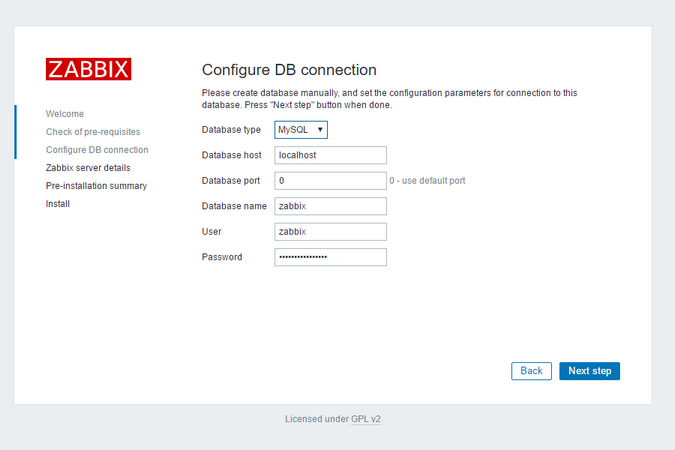
|  |
| --- |
| sudo systemctl enable zabbix-server |

### Bước 4: Cấu hình cho Zabbix Web Interface

Bây giờ hãy truy cập vào địa chỉ: http://your\_zabbix\_server\_ip\_address/zabbix/



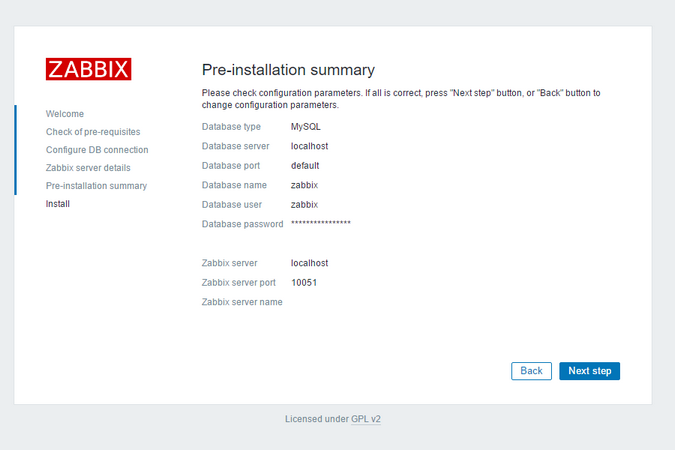
Click next step



* Datatype ở đây chọn MySQL
* Database host: vì ở đây mình cài mysql server trên chính zabbix nên khai báo là localhost
* Database port : 3306
* Database name : Đặt theo tên database mình tạo ở bước 2
* User và Password : Đặt theo tên database mình tạo ở bước 2



* Name: có thể khai báo tùy ý
* Host và Port để mặc định



Click next step

### Bước 5: Cấu hình zabbix agent

- SSH hoặc Login vào zabbix agent

- Tải package từ repo

|  |
| --- |
| sudo rpm -ivh <http://repo.zabbix.com/zabbix/3.0/rhel/7/x86_64/zabbix-release-3.0-1.el7.noarch.rpm> |

- Install zabbix agent

|  |
| --- |
| sudo yum install zabbix-agent |

- Sửa file cấu hình

|  |
| --- |
| vi /etc/zabbix/zabbix\_agentd.conf |

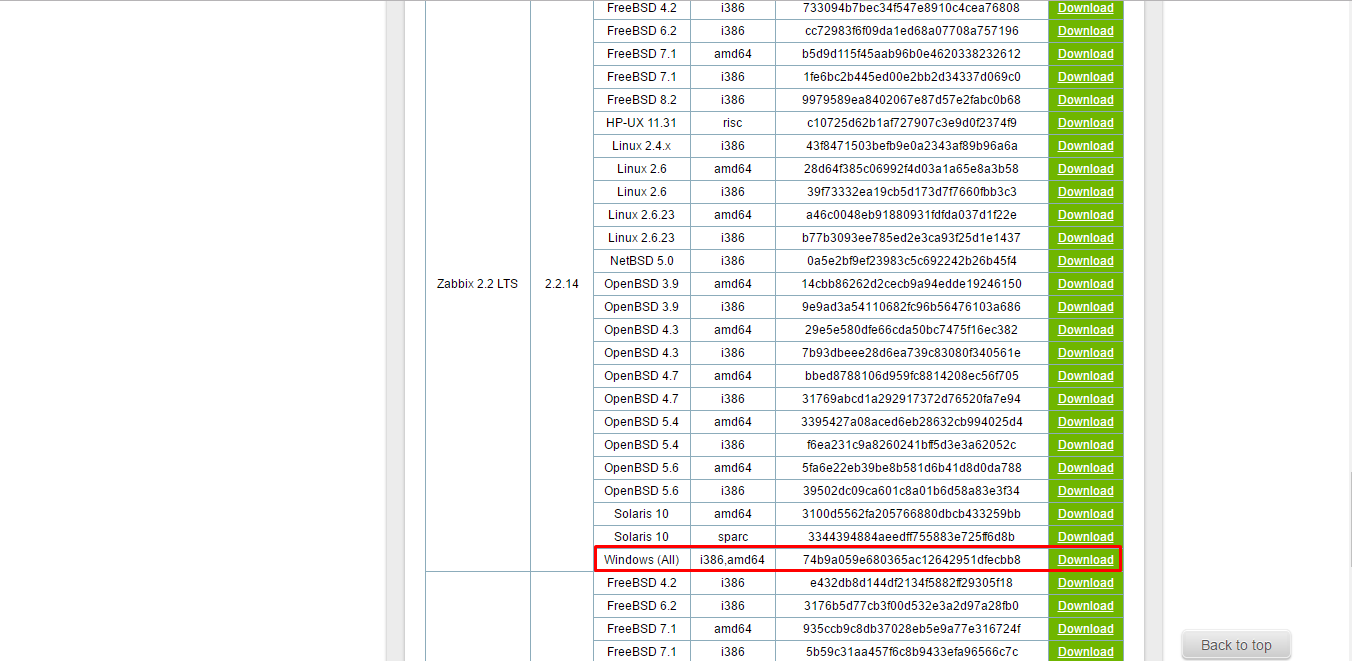
Như sau

|  |
| --- |
| Server=Zabbix-SRV-IP ServerActive=Zabbix-SRV-IP Hostname= client1  - Khởi động lại zabbix agent  sudo systemctl start zabbix-agent  sudo systemctl enable zabbix-agent |

### Bước 6: Cấu hình zabbix agent trên window

- Tải gói cài đặt Zabbix-agent tại đây

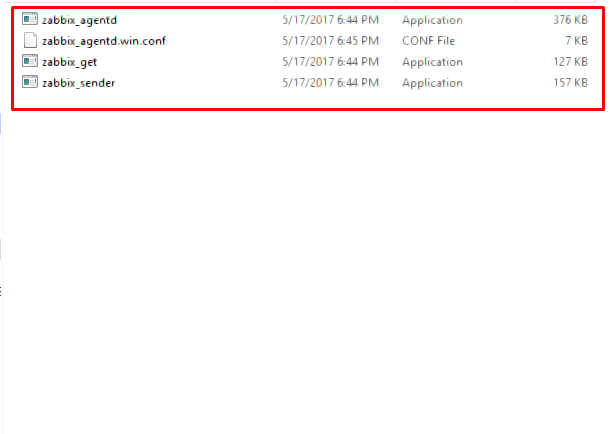
|  |
| --- |
| http://www.zabbix.com/download |



- Sau khi tải gói Zabbix-agent cần giải nén

- Tạo 1 thư mục có tên zabbix trong ổ C

- Tìm và Copy những file như hình sau vào thư mục zabbix vừa tạo. Lưu ý là chọn những file thuộc thư mục Win64 nếu dùng Windows 64 bits



- Sau khi copy mở cmd và thực hiện câu lệnh sau để cài zabbix-agent

|  |
| --- |
| C:\zabbix\zabbix\_agentd.exe --config C:\zabbix\zabbix\_agentd.win.conf --install |

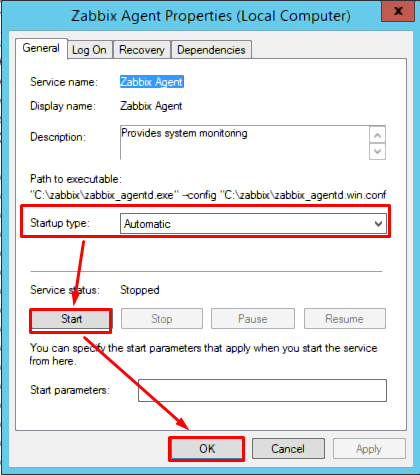
- Sửa file cấu hình C:\zabbix\zabbix\_agentd.win.conf. Sửa các dòng sau

|  |
| --- |
| Server=<IP\_Zabbix\_SRV> ServerActive=<IP\_Zabbix\_SRV> Hostname=<Hostname\_Windows> |

- Sử dụng nút Windows để tìm kiếm tab Services và tìm dịch vụ Zabbix-agent

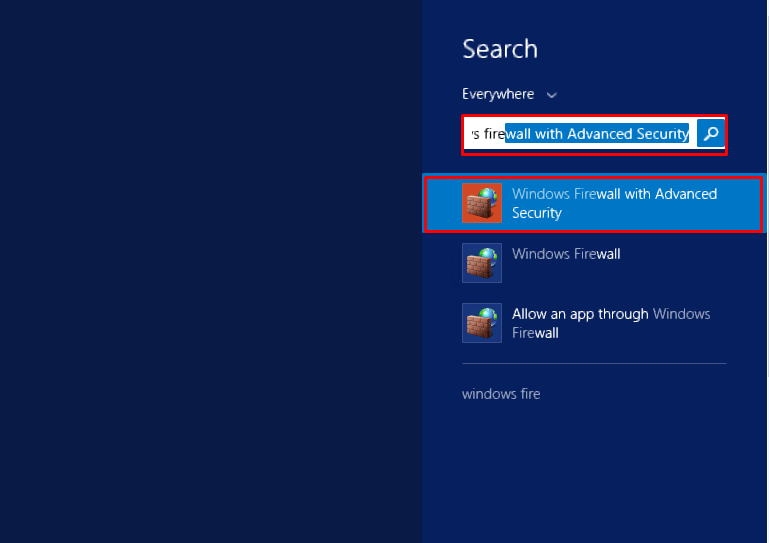


- Khởi động dịch vụ

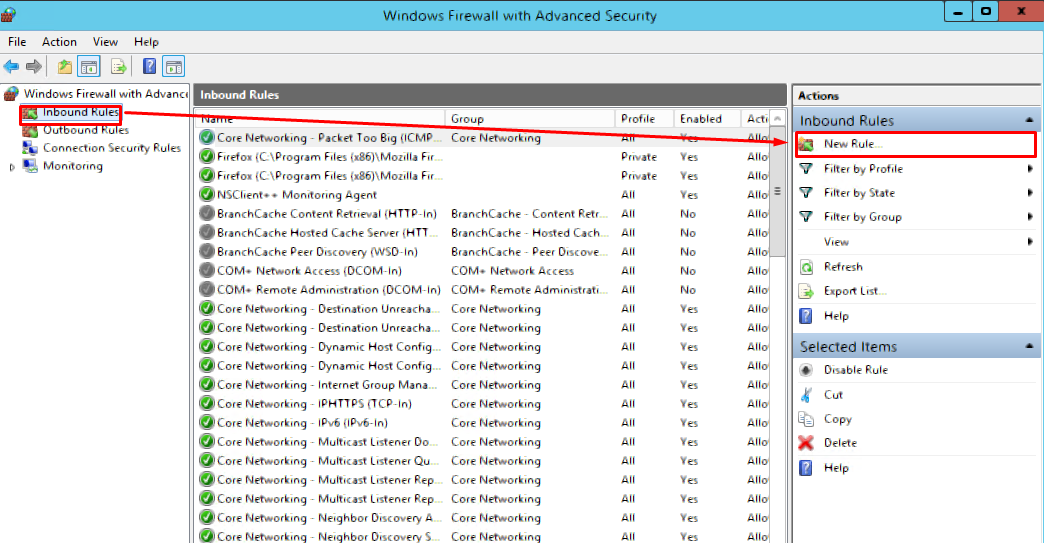


- Mở rule cho Windows

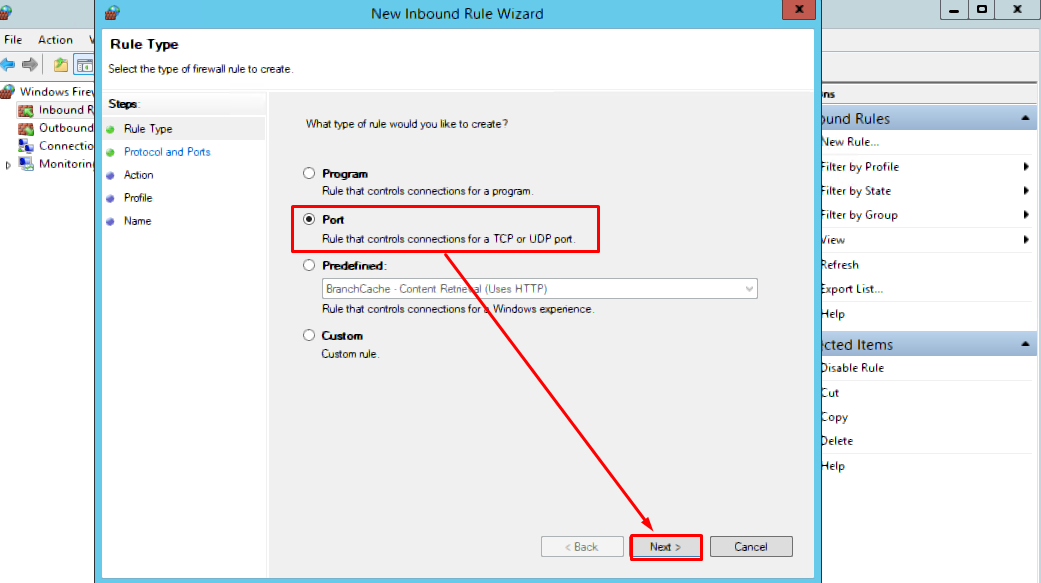
Tìm kiếm windows firewall with advanced security trên nút Windows



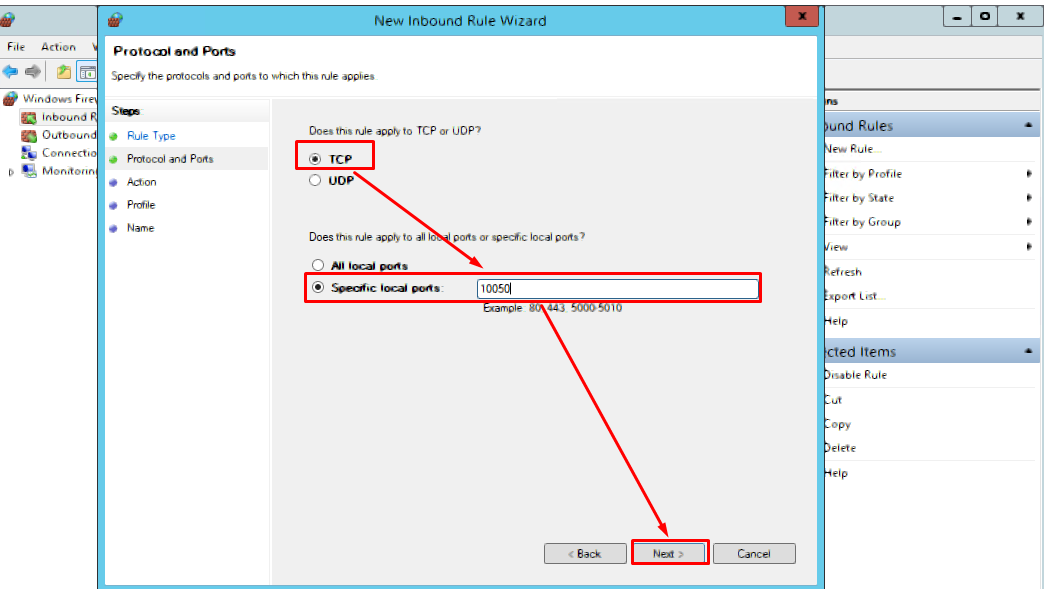
Tạo Rule cho chiều inbound Rules



Tạo Rule theo port

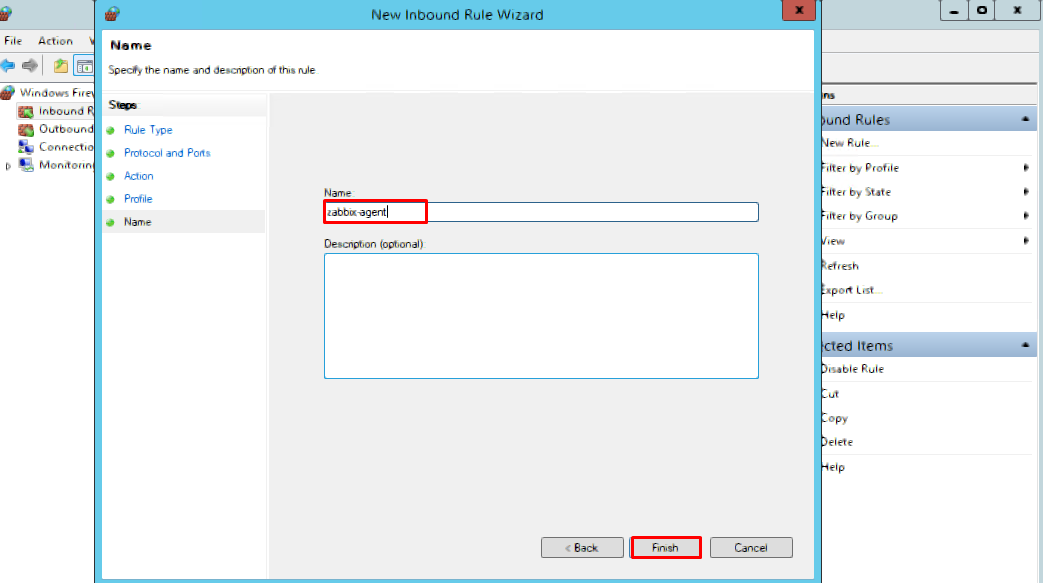


Tạo port sử dụng giao thức TCP



Chọn Allow the Connection và ấn Next. Ấn Next ở bước kế tiếp

Đặt tên cho Rule



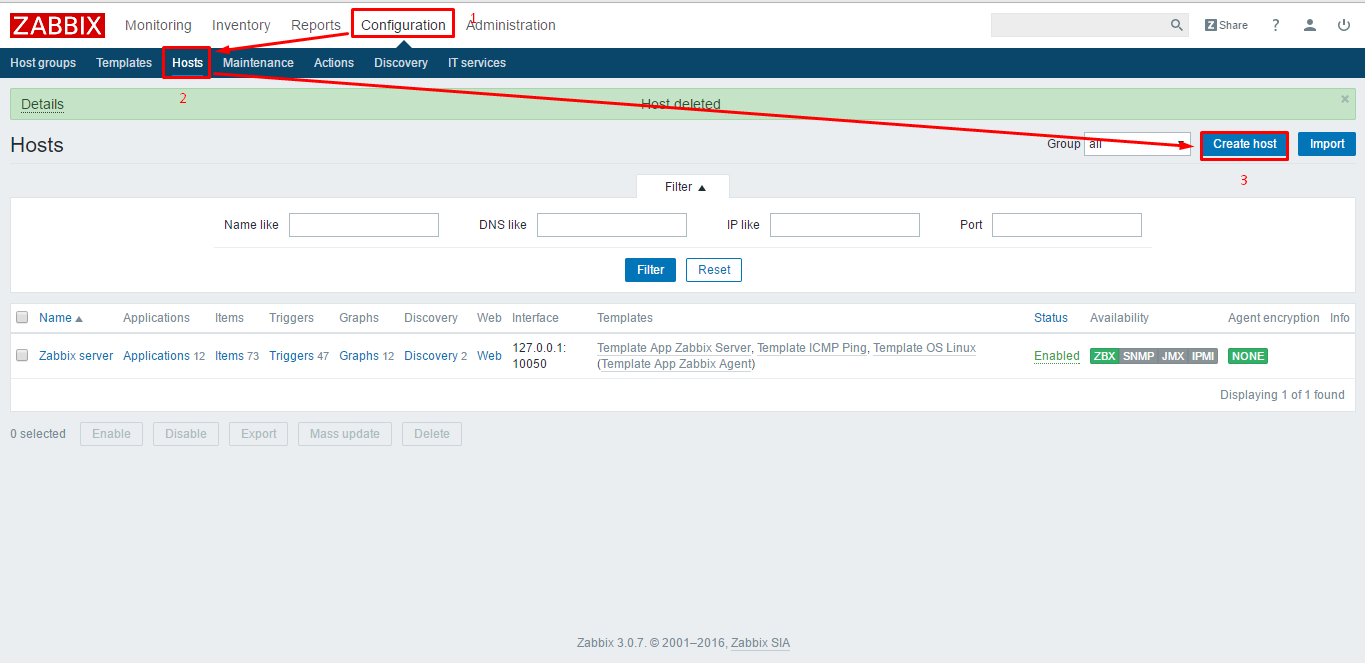
Bây giờ truy cập vào http://your\_zabbix\_server\_ip\_address/zabbix/ với user/password là Admin/zabbix

# IV. Hướng dẫn quản trị

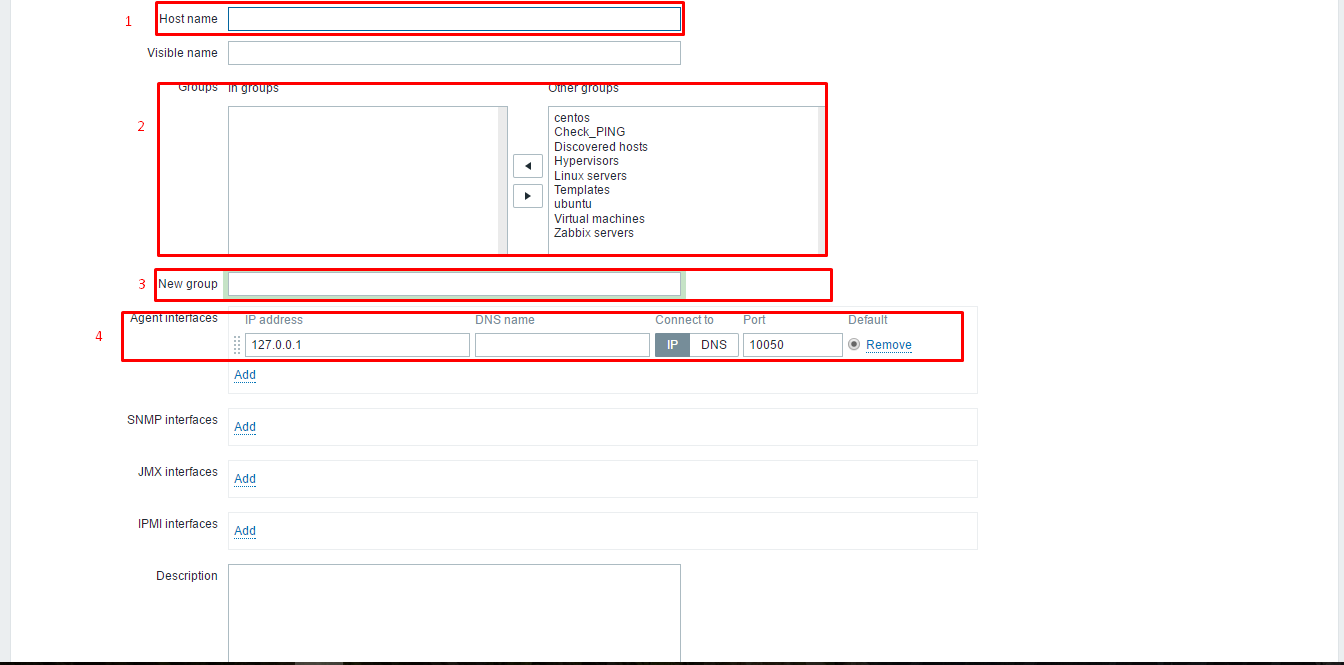
### 1. Thêm host

Để thêm 1 host mới trên dashboard Zabbix, làm theo các bước sau

* Bước 1: Thực hiện add host theo các bước sau



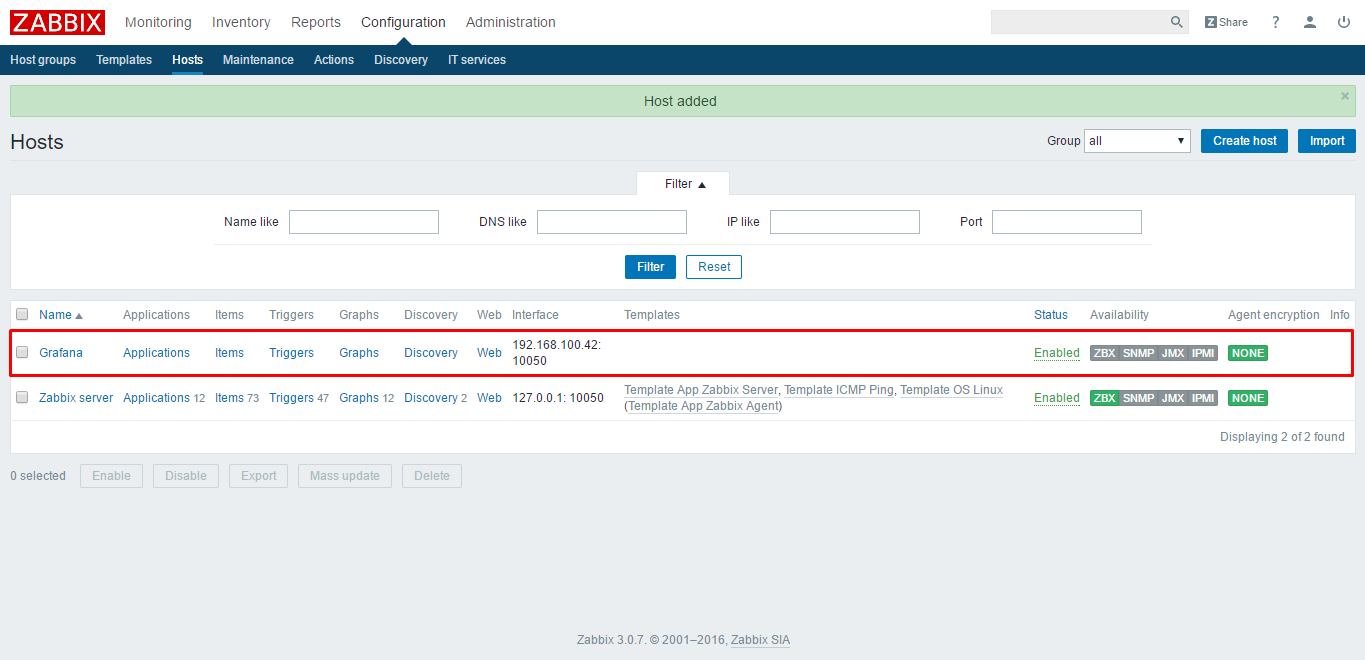
* Bước 2: Nhập các thông số sau



- Mục 1: Nhập vào tên host trên dashboard  
- Mục 2: Thêm host giám sát vào các host group có sẵn mà  
- Mục 3: Thêm host giám sát vào 1 group mới  
- Mục 4: Nhập địa chỉ IP của host giám sát

Sau khi hoàn thành các bước trên chọn Add

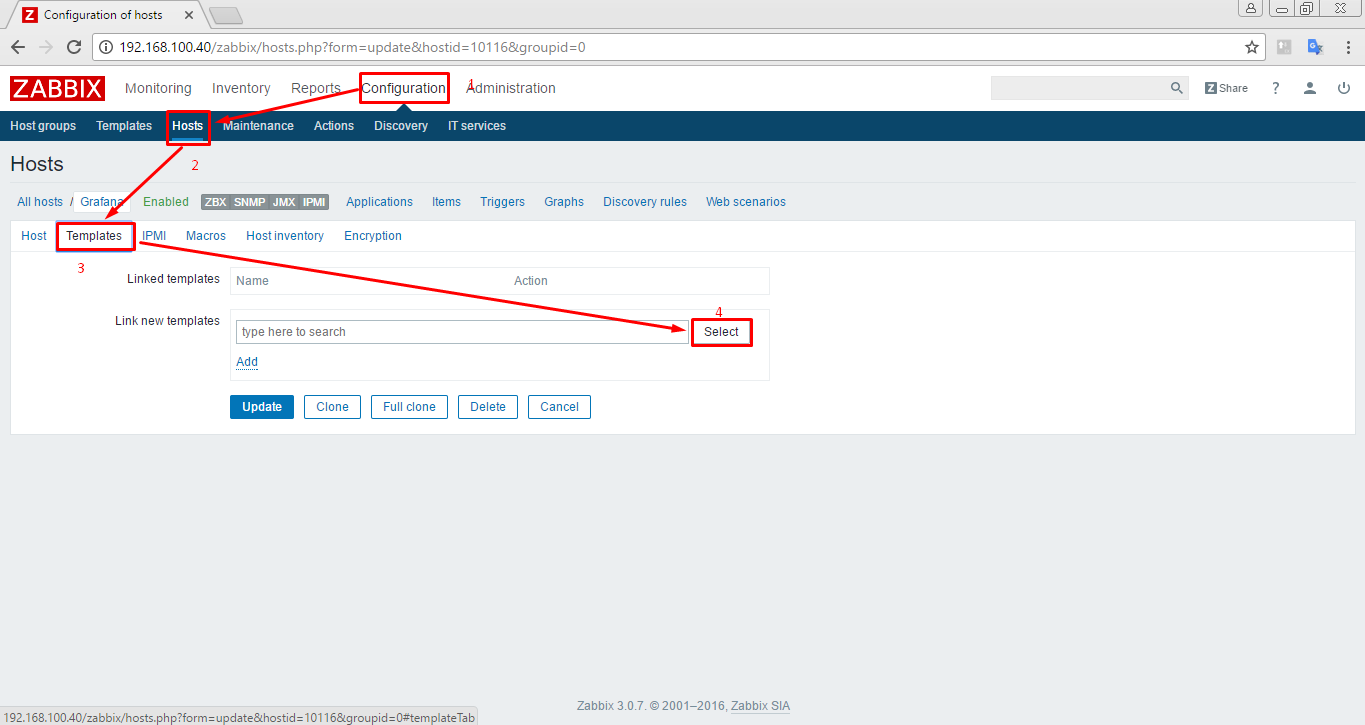
* Bước 3: Kiểm tra trên Dashboard



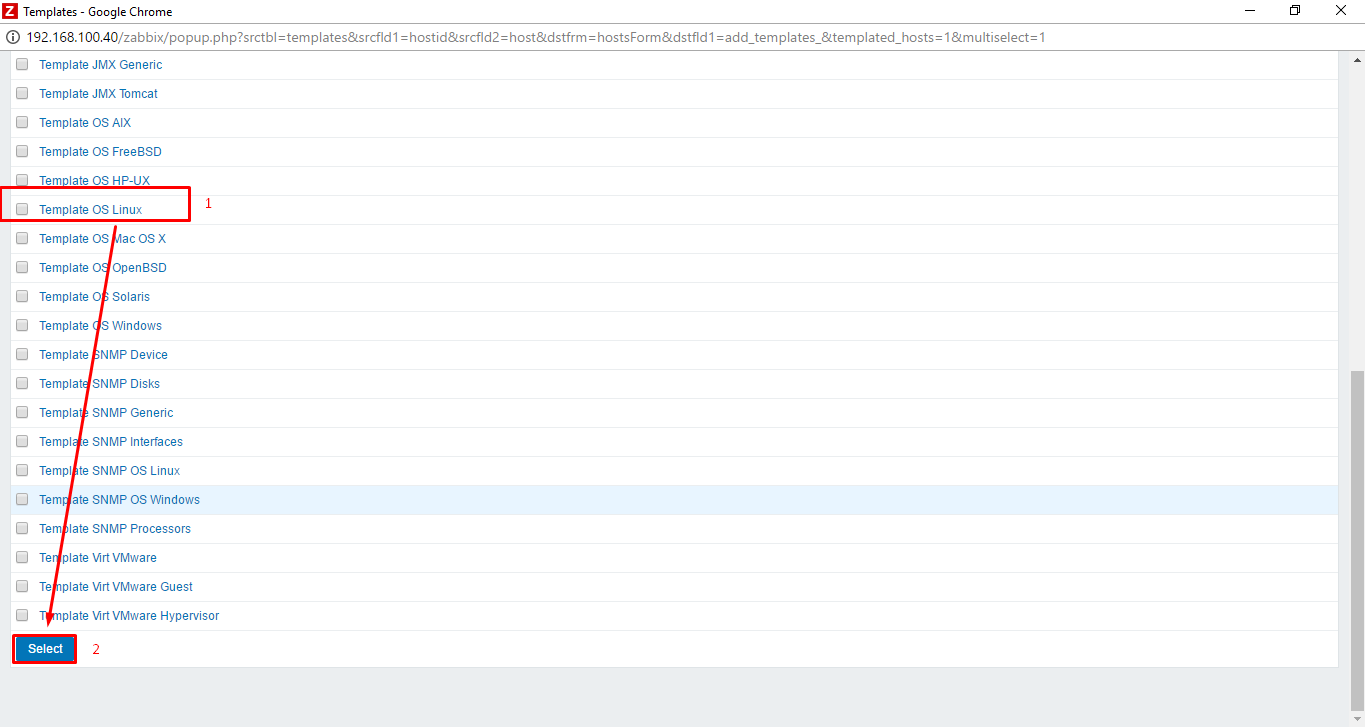
### 2. Thêm Template cho host

Trong Zabbix đã có sẵn các mẫu để giám sát các thông số tài nguyên hệ thống như giám sát với máy chủ có OS Linux, Windows...Khi thêm các templates này vào host giám sát, các templates sẽ có sẵn các item, trigger, graph..

Bước 1: Làm theo các bước sau để thêm template vào host giám sát



Bước 2: Chọn template, do ở đây host giám sát của tôi sử dụng Ubuntu14 nên tôi sẽ thêm template OS Linux

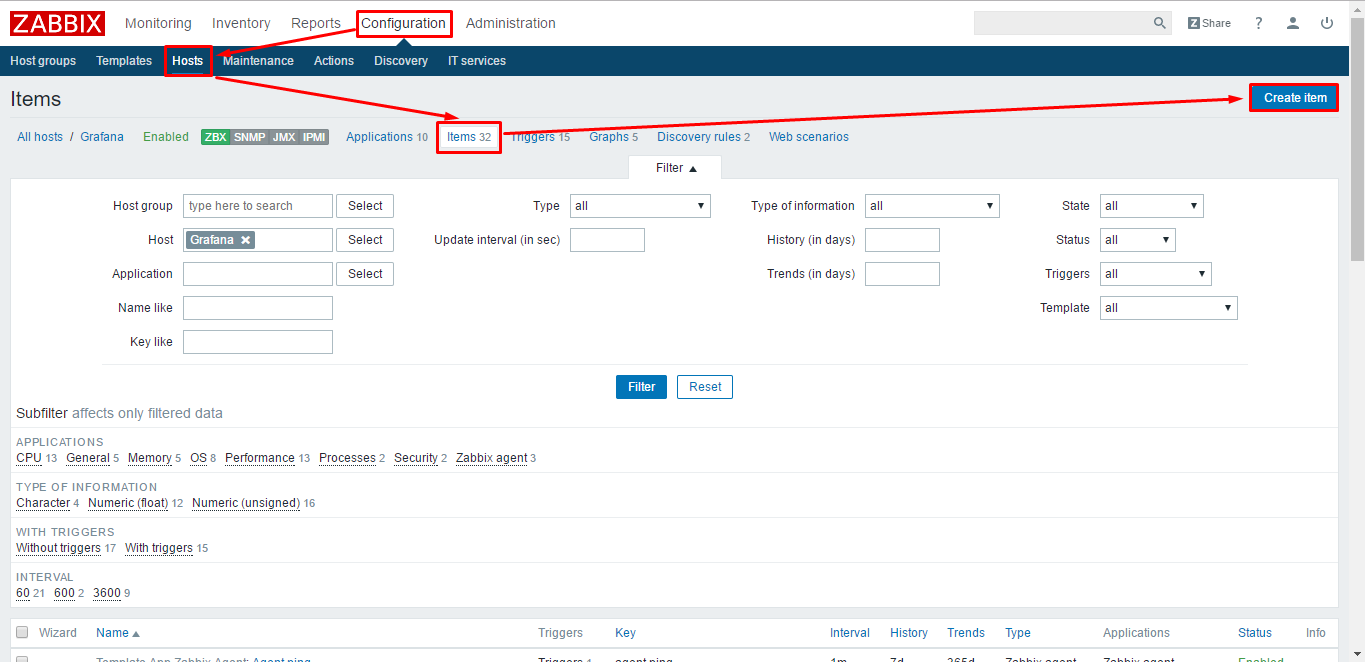


Sau đó chọn nút Add và Update trạng thái

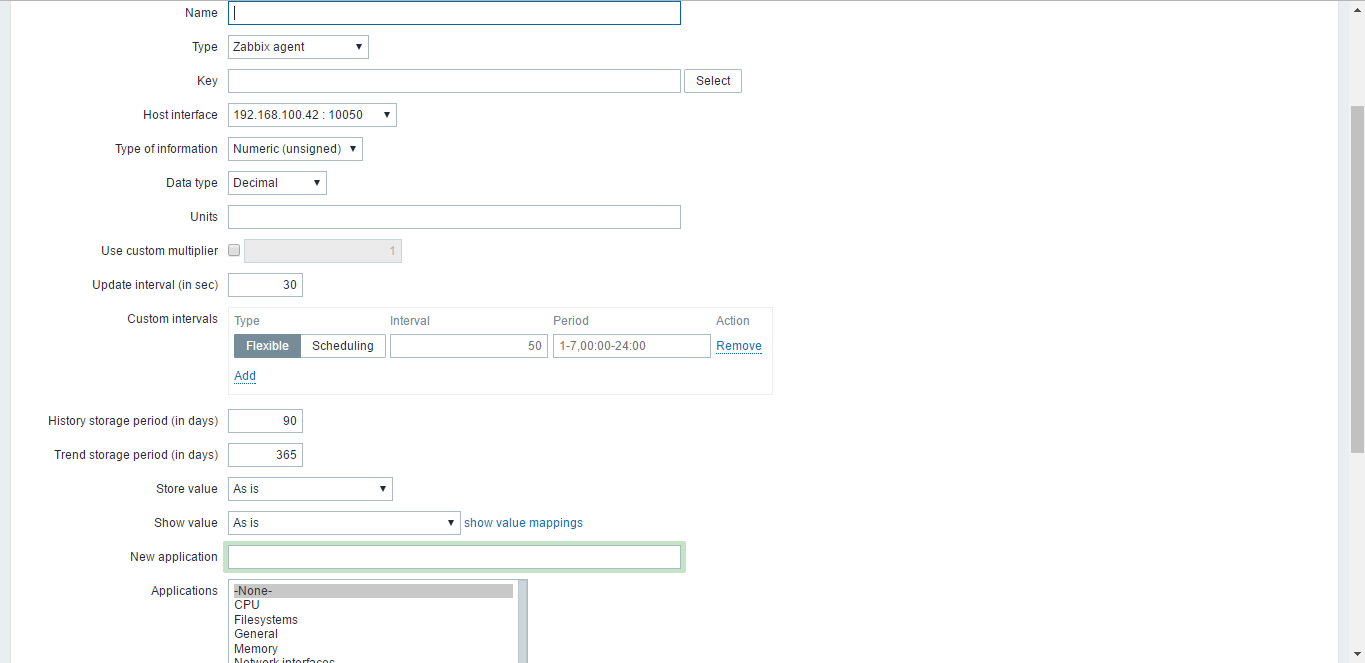
### 3. Thêm item cho host

Item của Zabbix là những key có sẵn (hoặc có thể tự viết) để thu thập dữ liệu từ các host được giám sát. Cách thêm như sau:

Bước 1: Tạo 1 item



Bước 2: Điền các thông tin item

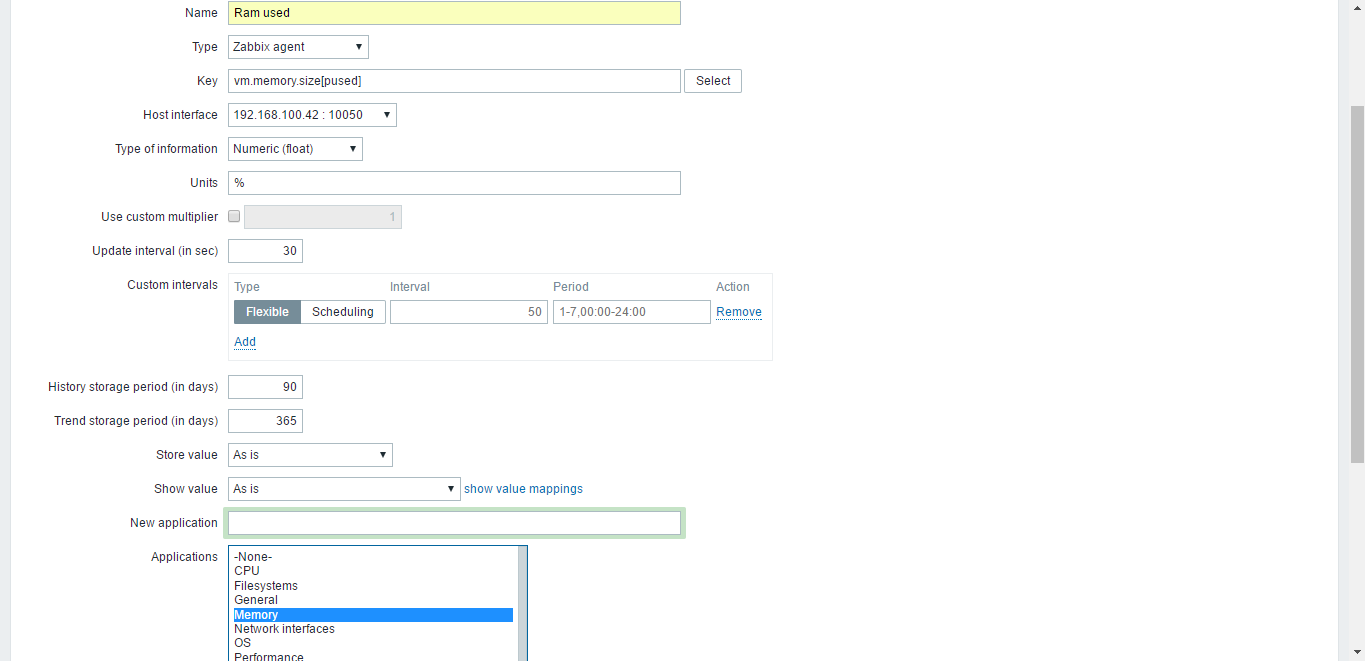


trong đó:

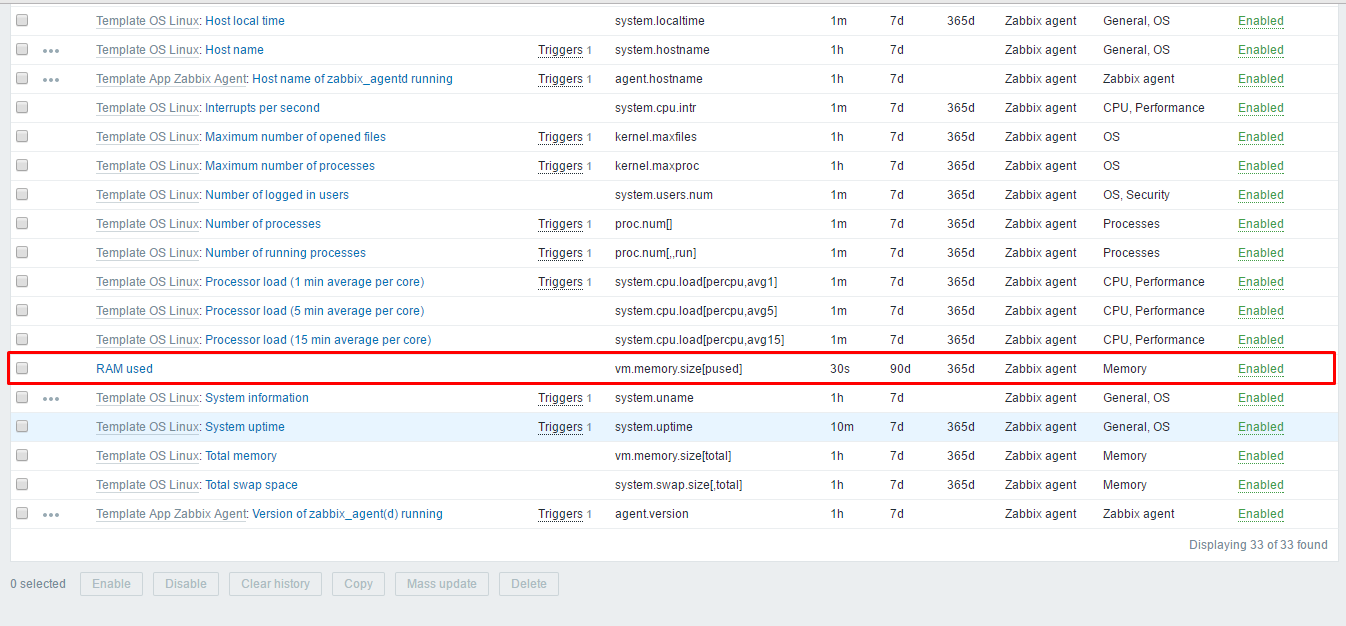
* Name: là tên được đặt cho item
* Type: Loại item này thuộc Zabbix-agent
* Key: Đây là các key được quy định sẵn trong zabbix-agent, chọn key phù hợp
* Host interface: Là địa chỉ IP của host giám sát với port 10050
* Type of information: Đây là loại dữ liệu item trả về
* Data type: Loại dữ liệu
* Units: Đơn vị của dữ liệu, đây là thông số cực kì quan trọng. Cần xác định đúng đơn vị của dữ liệu trả về để giám sát đúng
* Applications: Tầng ứng dụng, nơi mà item sẽ nằm trong đó. Ví dụ, RAM used sẽ nằm trong ứng dụng là Memory

Sau khi điền xong các thông số cơ bản trên, chọn Add

Ví dụ: Tôi sẽ tạo 1 item giám sát phần trăm RAM đã sử dụng



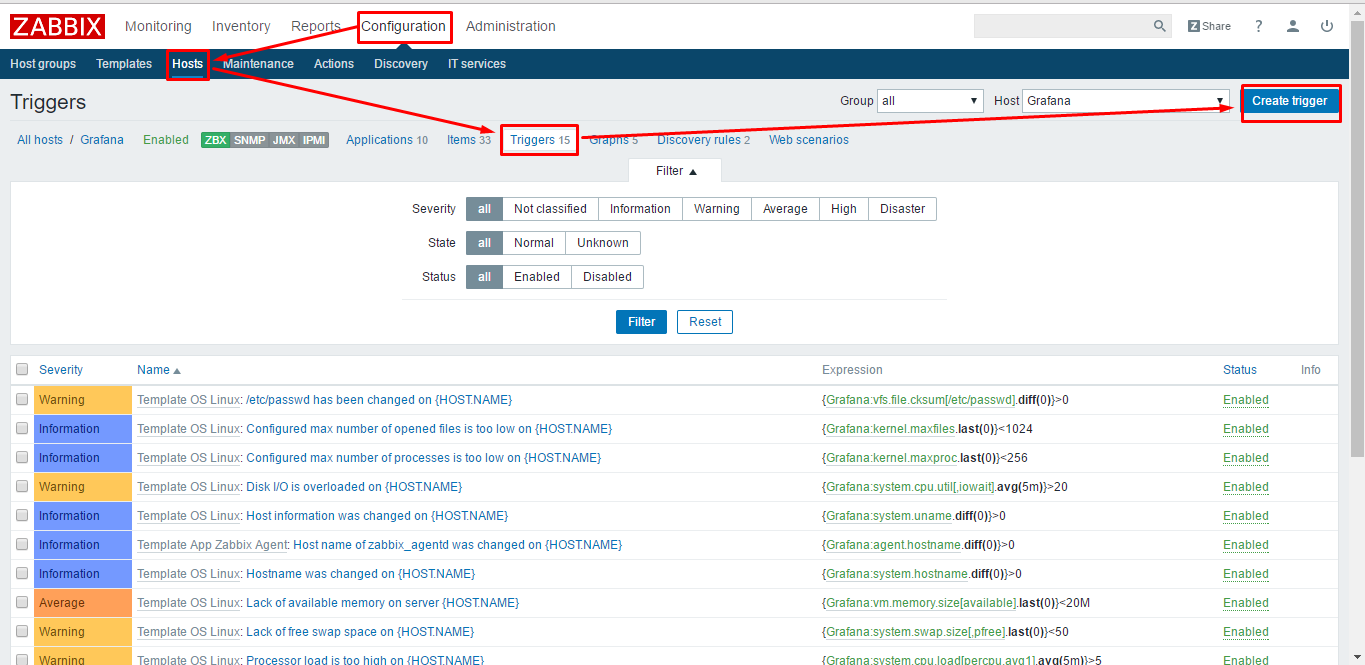
Trên dashboard



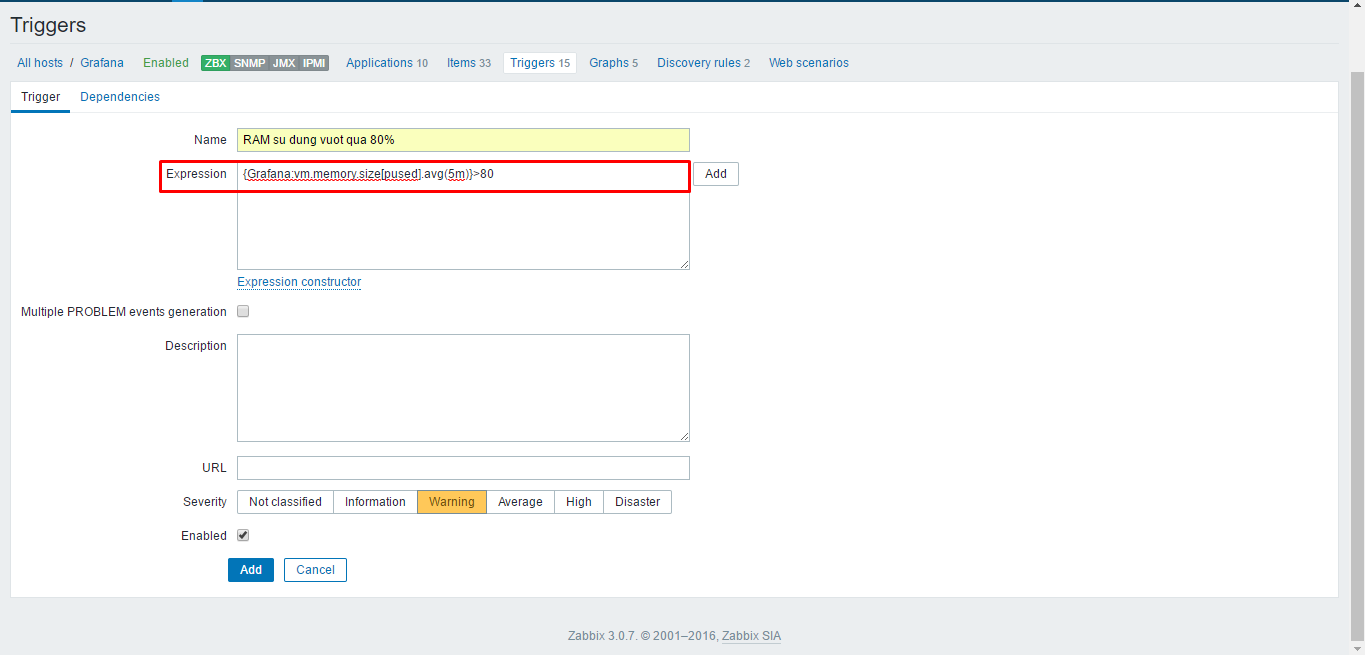
### 4. Thêm trigger

Trigger là các ngưỡng cảnh báo được đặt ra dựa theo thông số mà các item thu được từ host giám sát. Để add các trigger làm theo các bước sau\

Bước 1: Thực hiện thêm trigger



Bước 2: Điền các thông số sau



* Name: tên của trigger
* Expression: Là các biểu thức tính toán để đưa ra cảnh báo
* Severity: Là các mức độ nghiêm trọng của cảnh báo

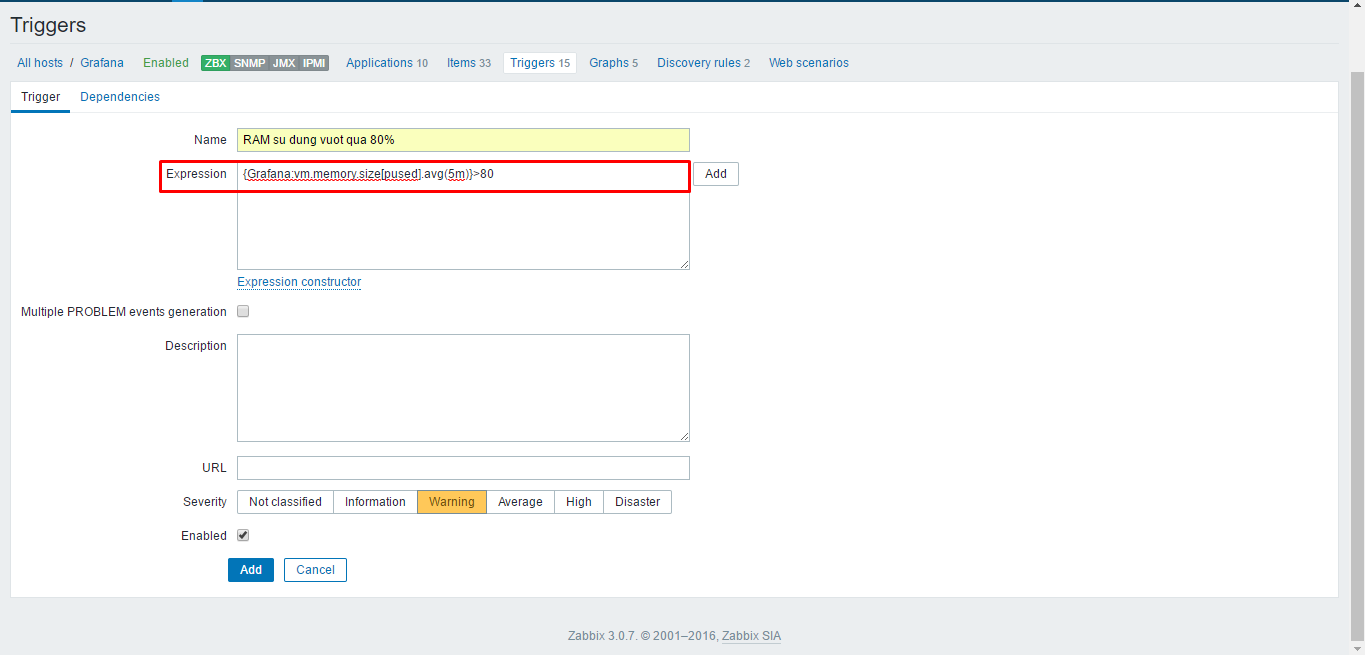
Bước 2.1: Sử dụng các Expression



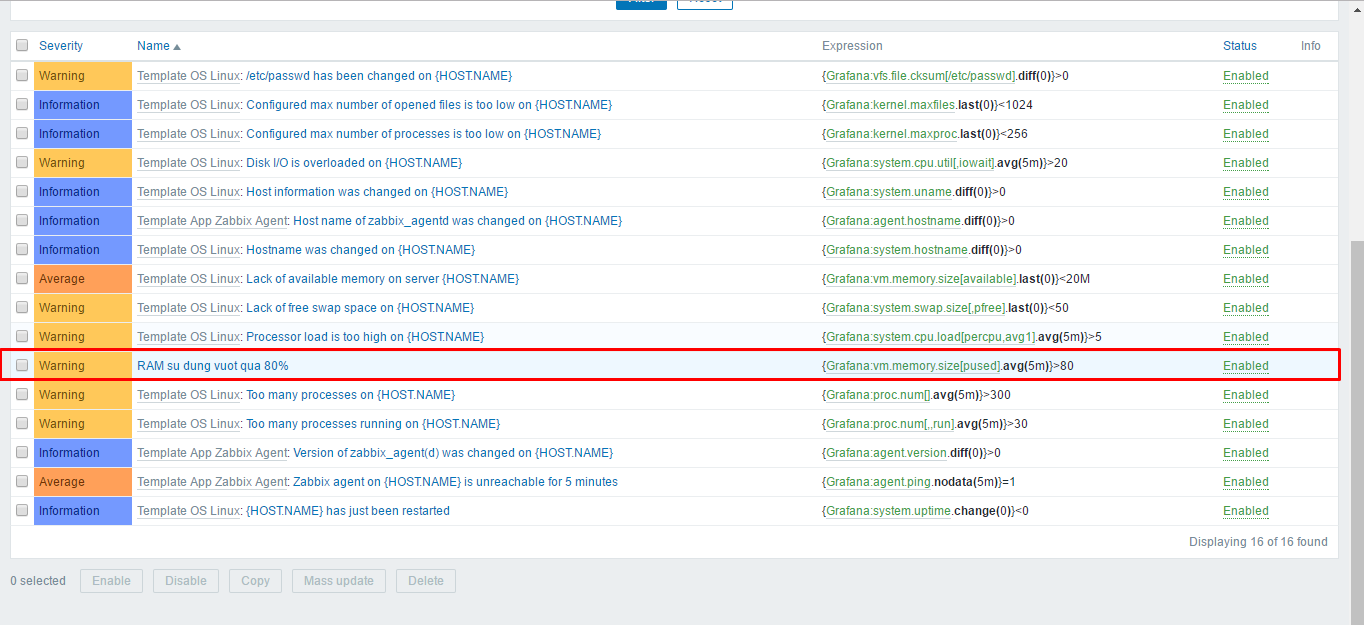
* Item: Là các item thu thập dữ liệu, chọn 1 item muốn cảnh báo
* Function: Là biểu thức tính giá trị của dữ liệu thu được. Ví dụ, lần cuối cùng lớn hơn giá trị N, giá trị trung bình của dữ liệu…
* Last of (T): Khoảng thời gian check cuối cùng
* N: Là giá trị xác định ngưỡng, nếu quá ngưỡng giá trị này sẽ cảnh báo

Sau khi thực hiện xong các bước, chọn **Insert**

Bước 3: Kiểm tra trên Dashboard

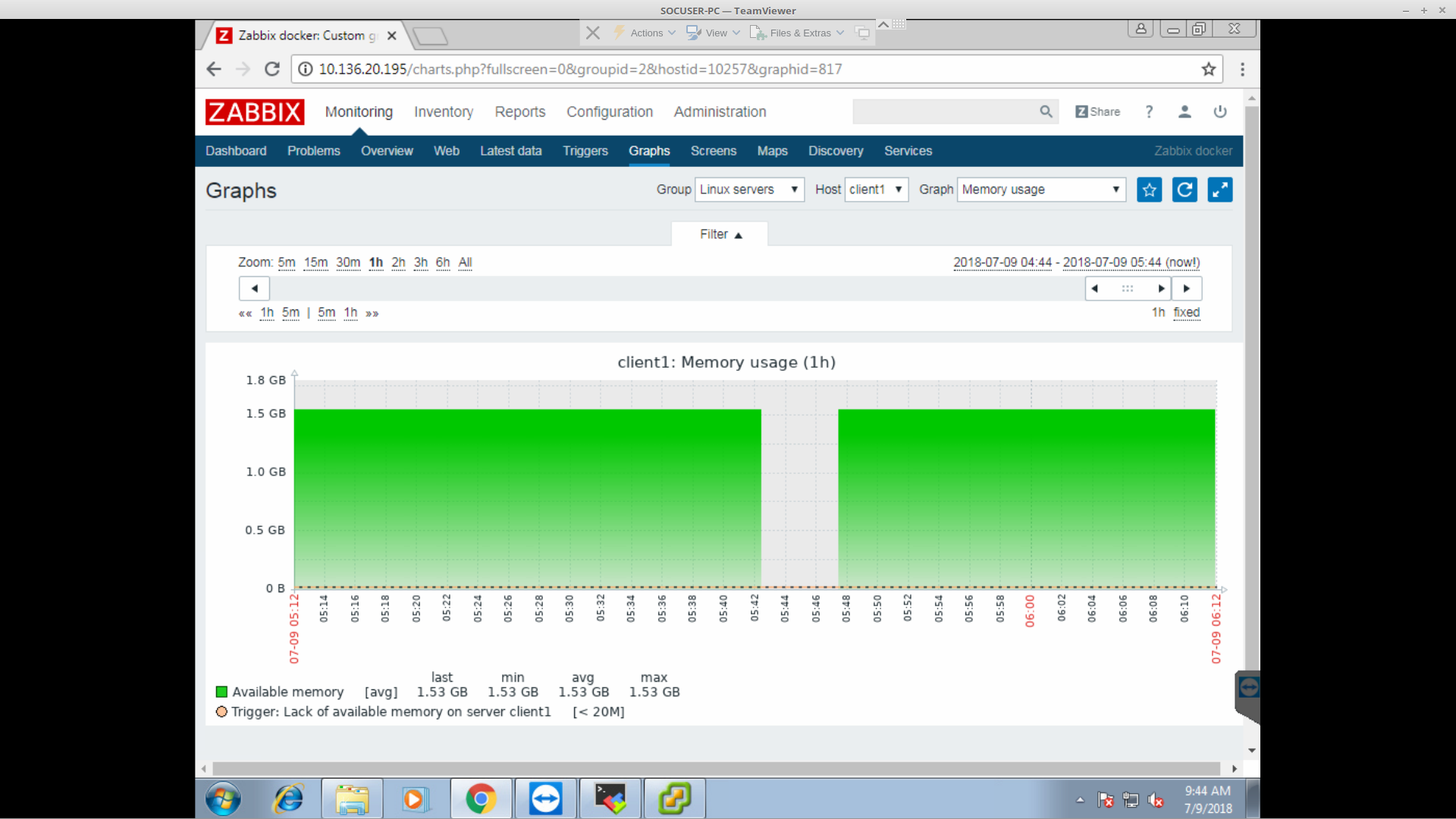


Bước 4: Chọn Add và kiểm tra

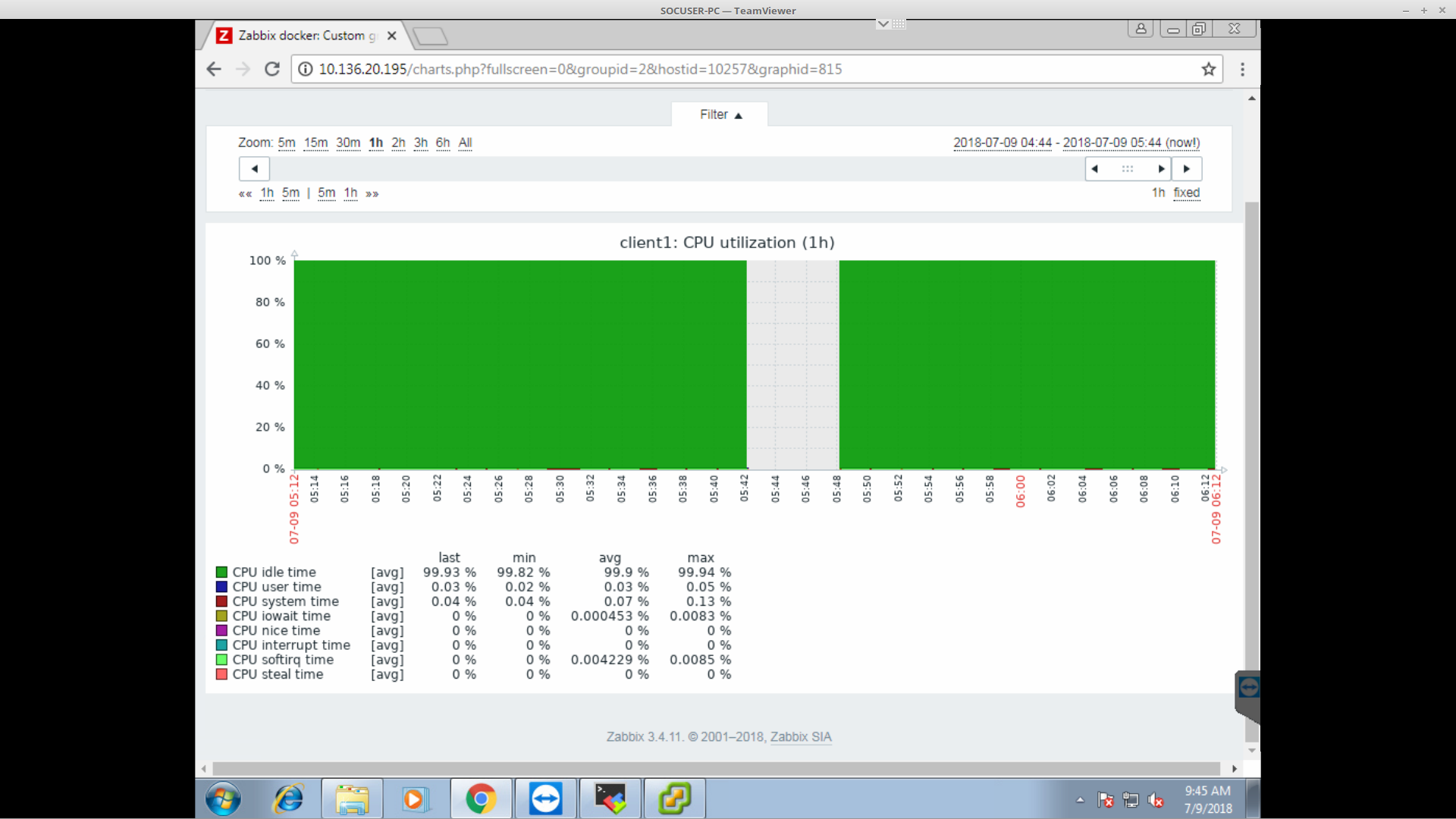


# V. Demo

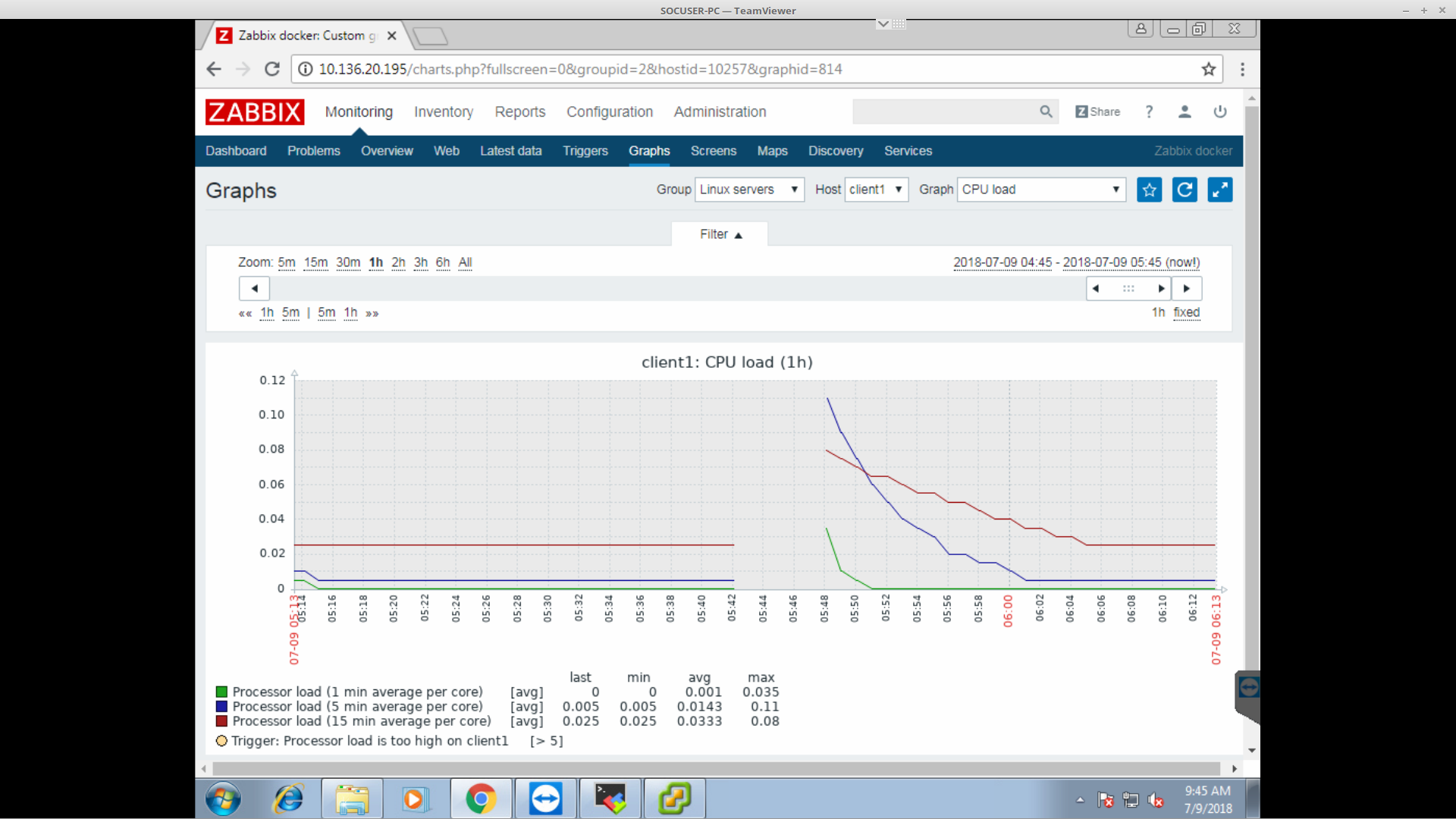
1. Theo dõi thông số về ram



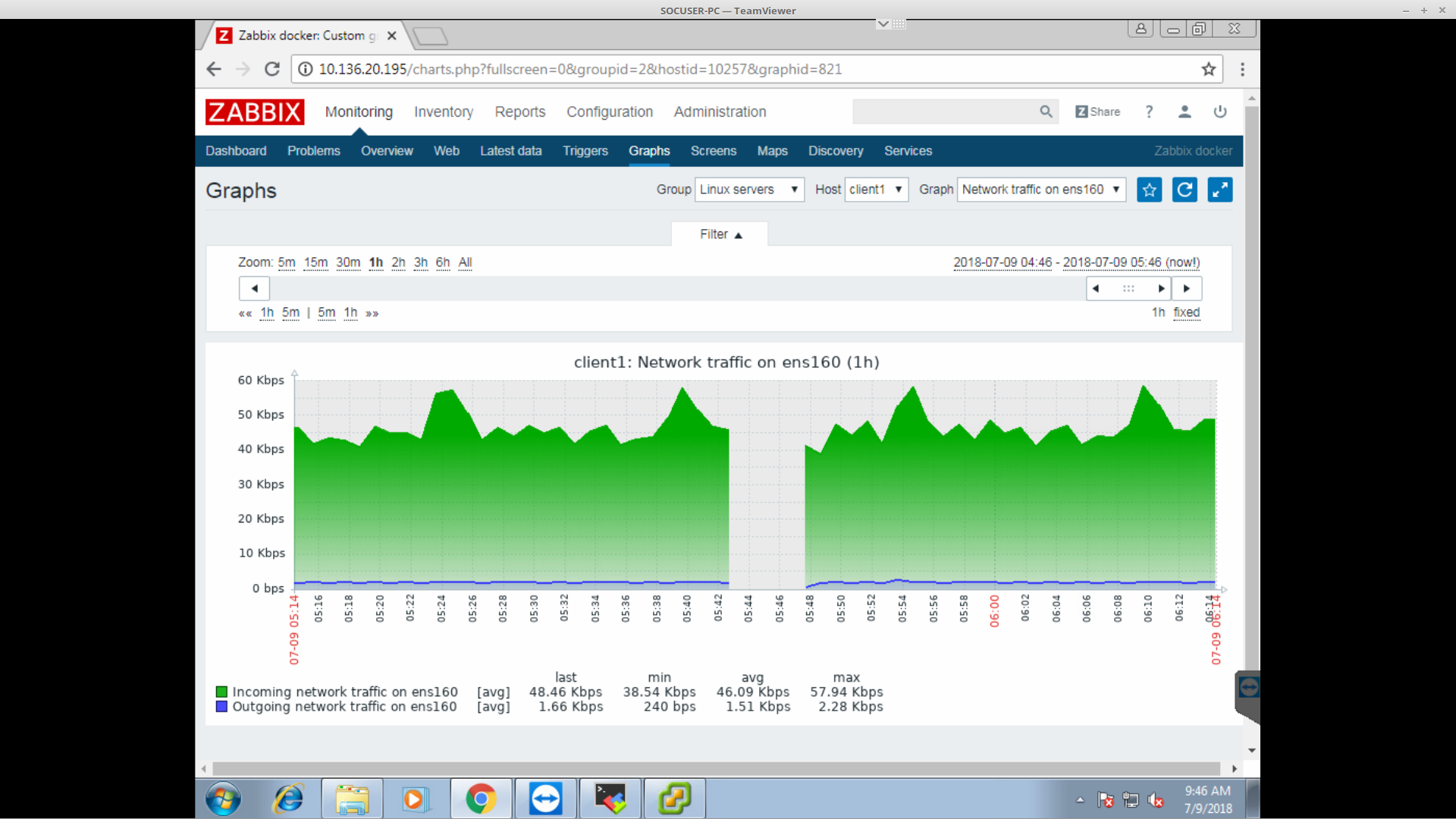
2. Theo dõi thông số cpu



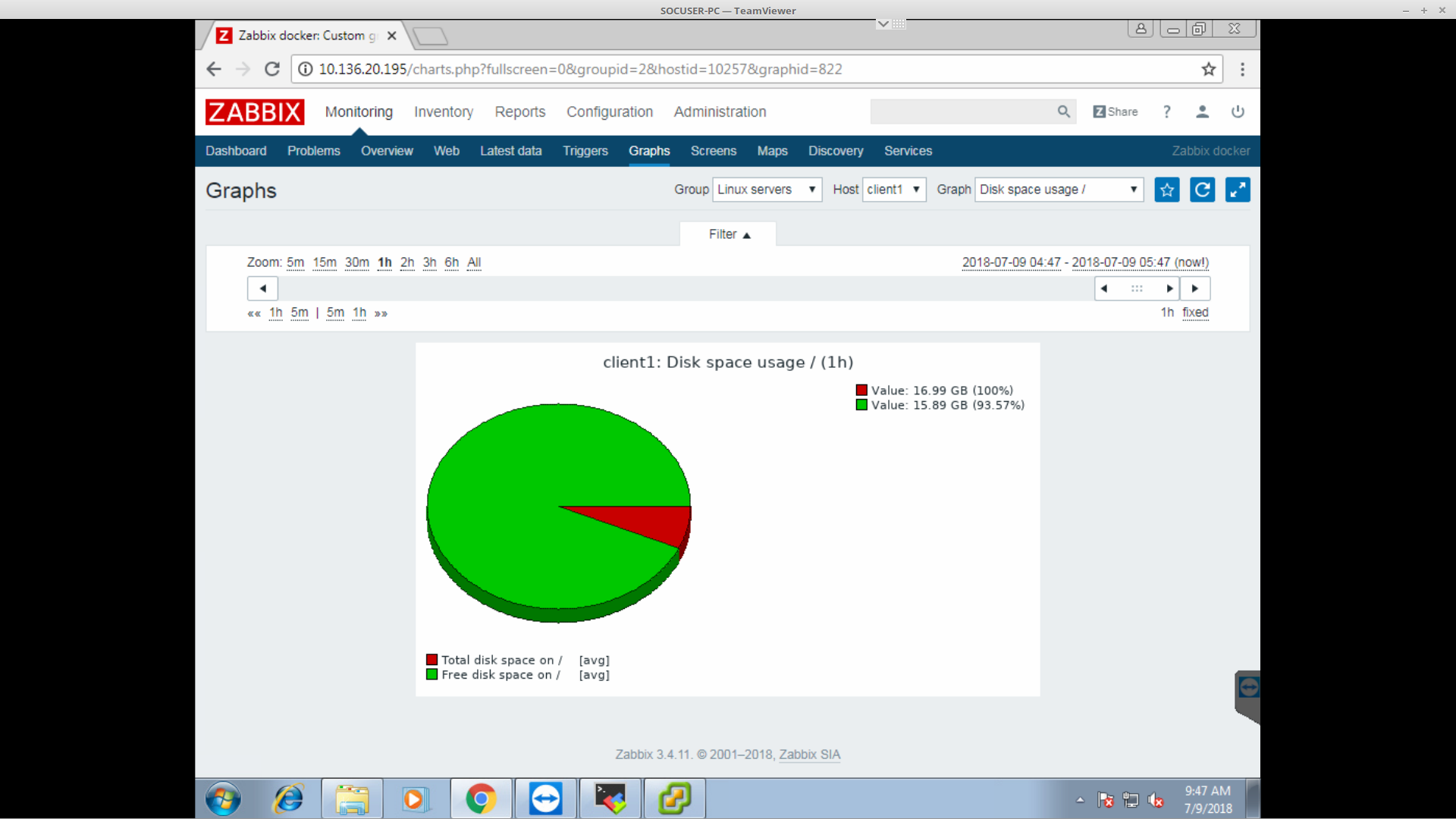
3. Theo dõi thông số cpu load



4. Theo dõi network traffic



5. Theo dõi disk



6. Theo dõi thông qua grafana

