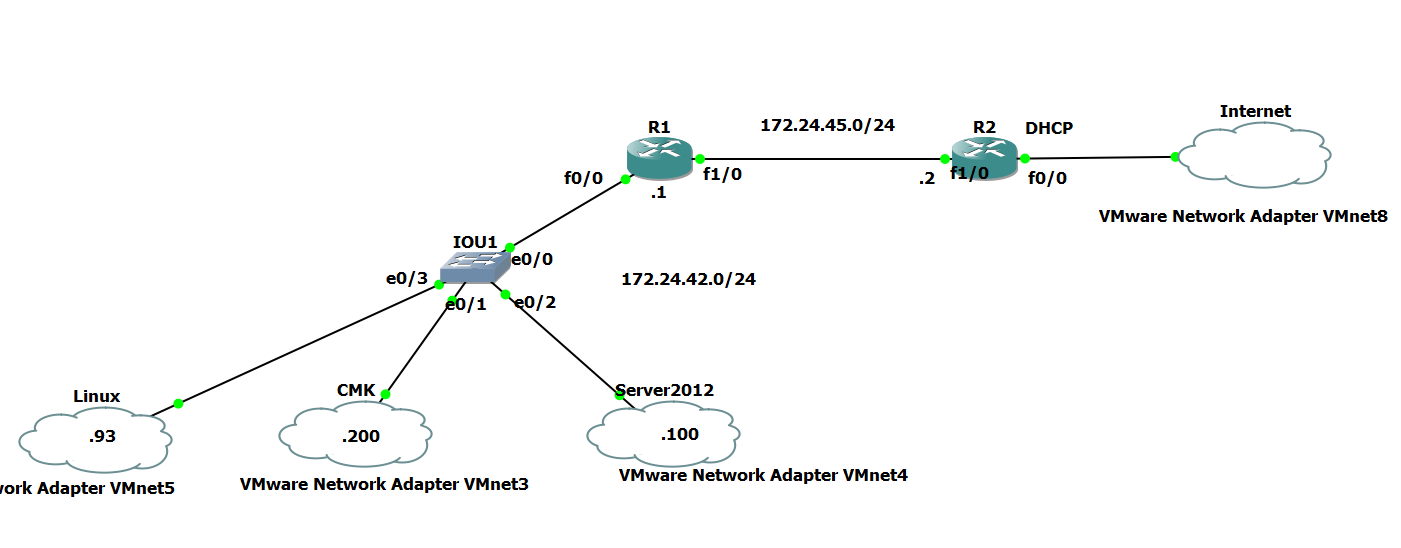
**Cấu Hình Và Cài Đặt CheckMK**

**I. Mô Hình:**

 \* Chuẩn bị:

- Hai Server CentOS 8 Server CMK / Agent

- Server 2012.

- Đặt IP và NAT mô hình trên.

**II. Cài Đặt Và Cấu Hình:**

Trên máy CentOS 8 Server:

Cài đặt Repo:

#dnf -y install epel-release

Cài Đặt Apache:

#dnf -y install httpd

#systemctl start httpd

#systemctl enable httpd

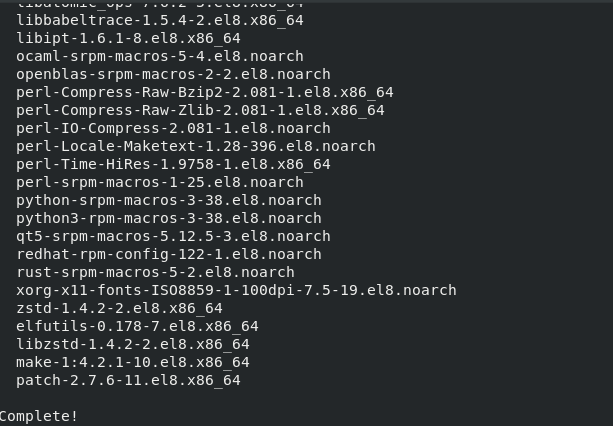
Cài đặt các gói cần thiết:

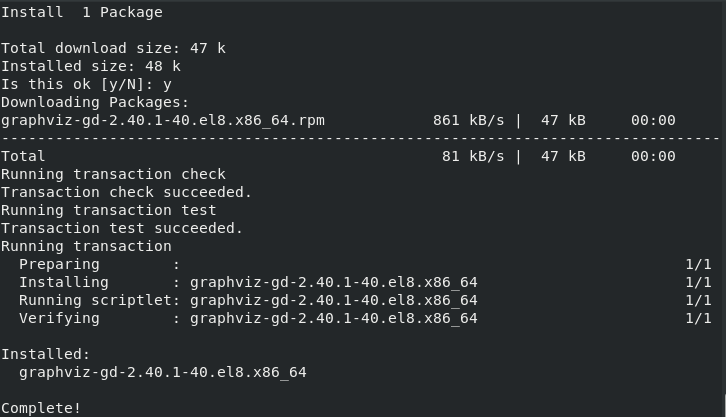
# wget <http://repo.openfusion.net/centos7-x86_64/openfusion-release-0.8-1.of.el7.noarch.rpm>

# rpm -Uvh openfusion-release\*rpm

# dnf -y install freeradius-utils graphviz libdbi perl-IO-Zlib perl-Locale-Maketext-Simple rpm-build traceroute uuid xinetd dialog

# dnf --enablerepo=PowerTools install graphviz-gd



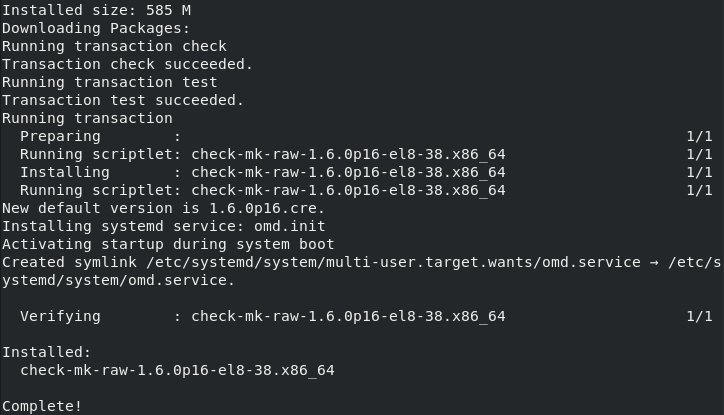


Sử dụng wget để download check\_mk:

# wget <https://checkmk.de/support/1.6.0p16/check-mk-raw-1.6.0p16-el8-38.x86_64.rpm>

Cài đặt check\_mk bằng link vừa download:

# dnf -y install check-mk-raw-1.6.0p16-el8-38.x86\_64.rpm



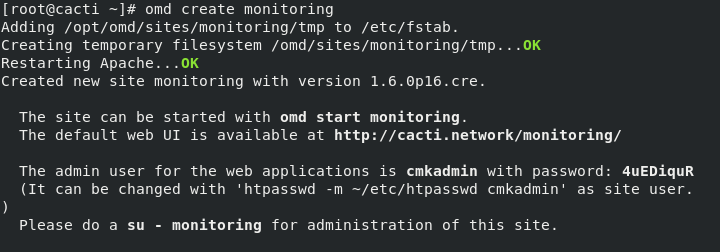
Mở port 80 để sử dụng dịch vụ httpd:

#firewall-cmd --permanent --add-port=80/tcp

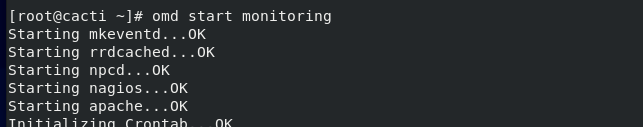
#firewall-cmd --reload

Tạo và khởi động site:

#omd create monitoring



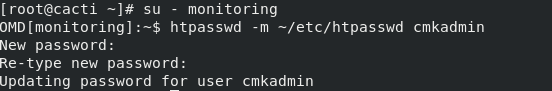
#omd start monitoring



Đặt mật khẩu cho site:

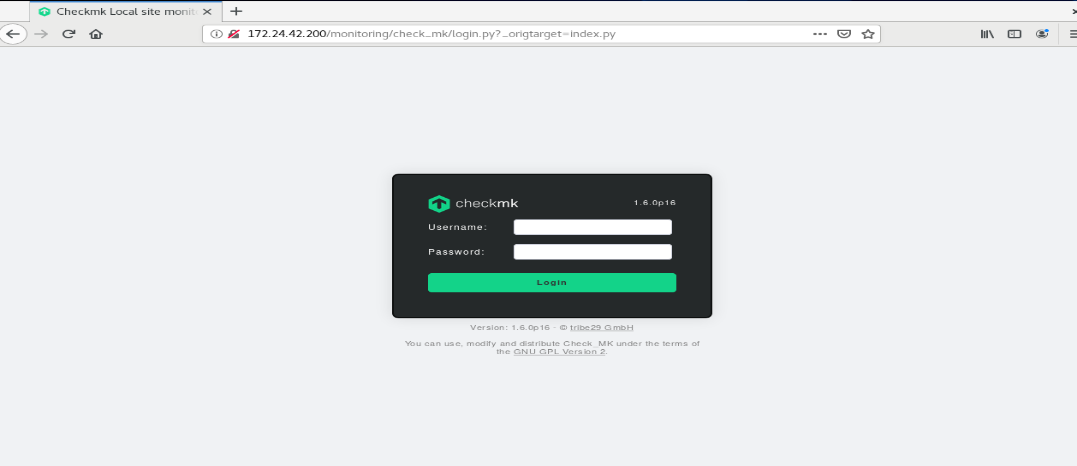
#su - monitoring

#htpasswd -m ~/etc/htpasswd omdadmin

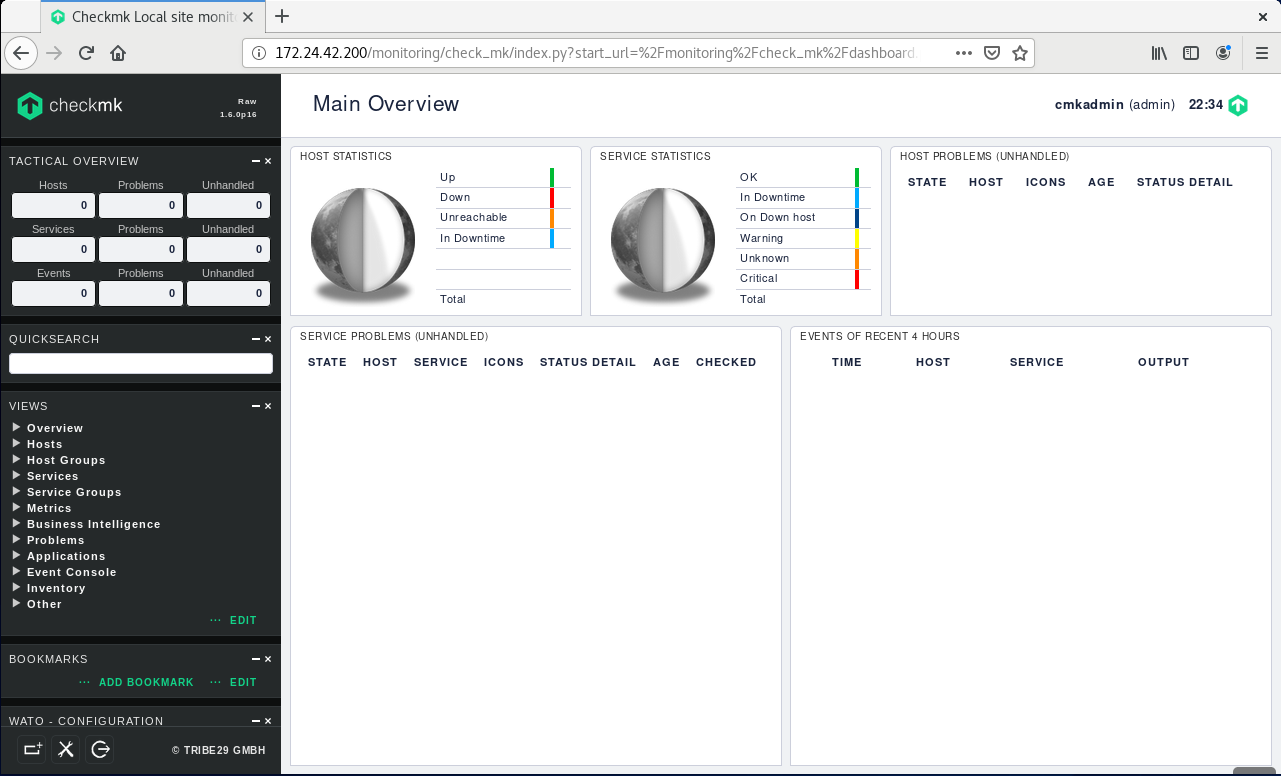


Đăng nhập vào trang web bằng tài khoản cmkadmin và passwd vừa tạo:

<http://Your-IP/monitoring>



Giao diện Dashboard:



**III. Thêm Host vào CheckMK:**

*1. Host Linux:*

Trên máy Server CheckMK:

Đầu tiên, chúng ta vào Web UI để tải Agent cho client. Ở giao diện Web, chúng ta kéo xuống phần WATO - Configuration, chọn tiếp Monitoring Agent:

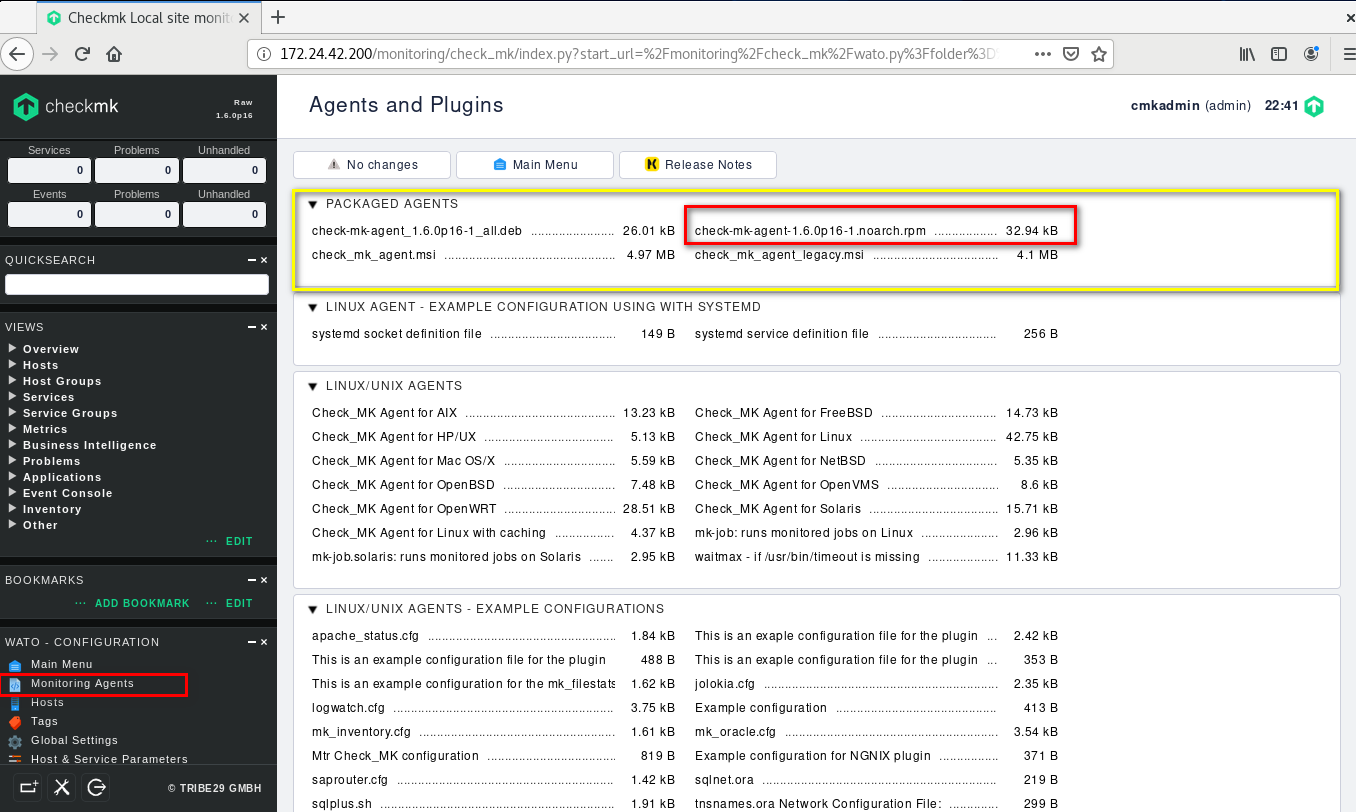
Ở đây chúng ta có 3 loại file cài đặt đó là :

\*.deb: Dành cho các host sử dụng DEBIAN.

\*.rpm: Dành cho các host sử dụng RHEL.

\*.msi: Dành cho các host sử dụng MS Windows.

Ở đây, agent là CentOS 8 thì chúng ta sẽ chọn \*.rpm: Dành cho các host sử dụng RHEL.

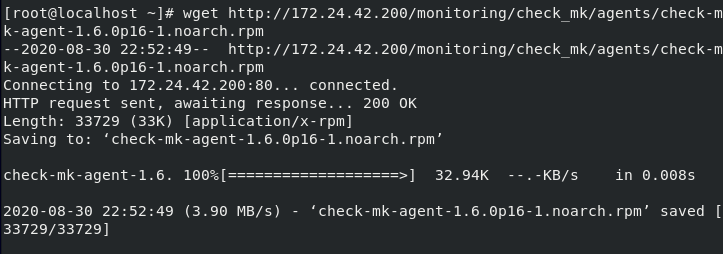


Coppy địa chỉ đường dẫn và dùng wget để tải file cài đặt về

**Trên Server CentOS Agent:**

Dán đường dẫn vừa copy bên Server và dùng Wget để tải file về:

wget <http://172.24.42.200/monitoring/check_mk/agents/check-mk-agent-1.6.0p16-1.noarch.rpm>

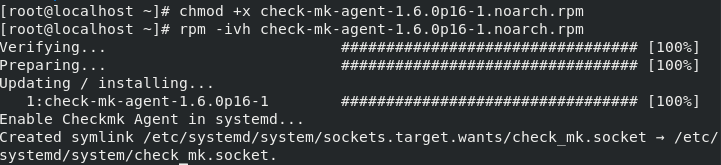


Cấp quyền thực thi cho file vừa download về:

# chmod +x check-mk-agent-1.6.0p16-1.noarch.rpm

Cài đặt agent:

# rpm -ivh check-mk-agent-1.6.0p16-1.noarch.rpm



Cài đặt xinetd:

# dnf install xinetd -y

Khởi động xinetd:

#systemctl start xinetd

#systemctl enable xinetd

Cài đặt gói net-tools để kiểm tra dễ dàng hơn:

# dnf install net-tools -y

Mở port trên client để có thể giao tiếp với check\_mk server:

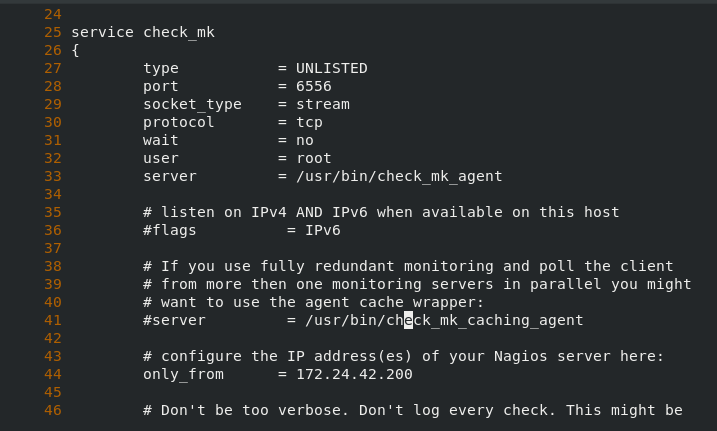
#vi /etc/xinetd.d/check\_mk

Sửa các thông số sau:

only\_from = 172.24.42.200 //IP Máy Server

disable = 0

port = 6556



Kiểm tra port mặc định của check\_mk sử dụng để giám sát được chưa:

#netstat -npl | grep 6556



Mở port trên firewall:

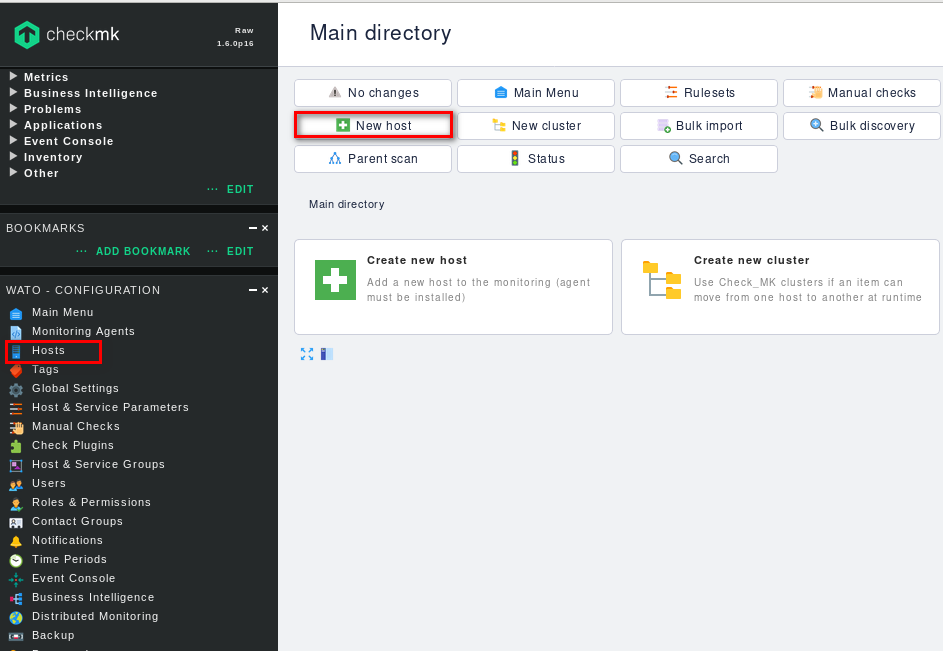
#firewall-cmd --add-port=6556/tcp --permanent

#firewall-cmd --reload

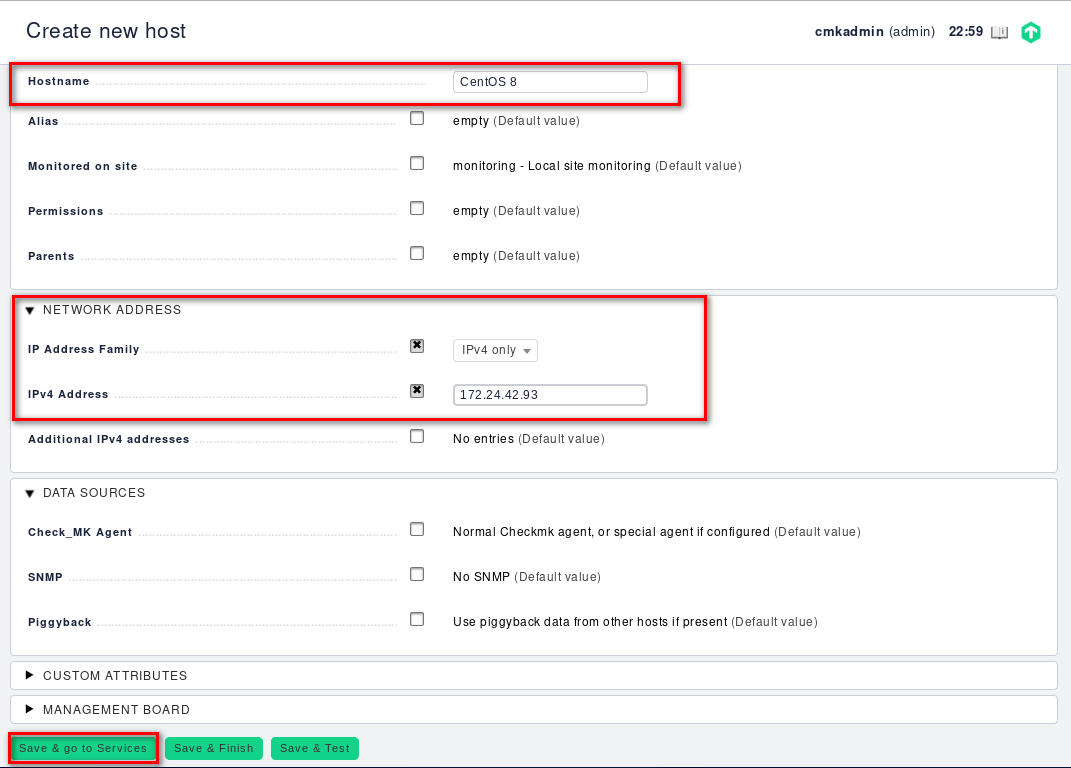
**Quay lại máy Server CheckMK tiến hành Add Host Linux:**

Log in vào Web UI:

Tại WATO – Configuration: Chọn Host -> New Host

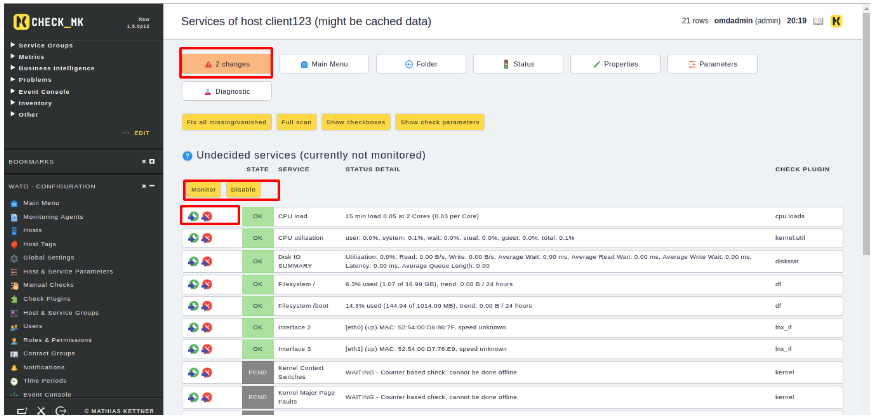


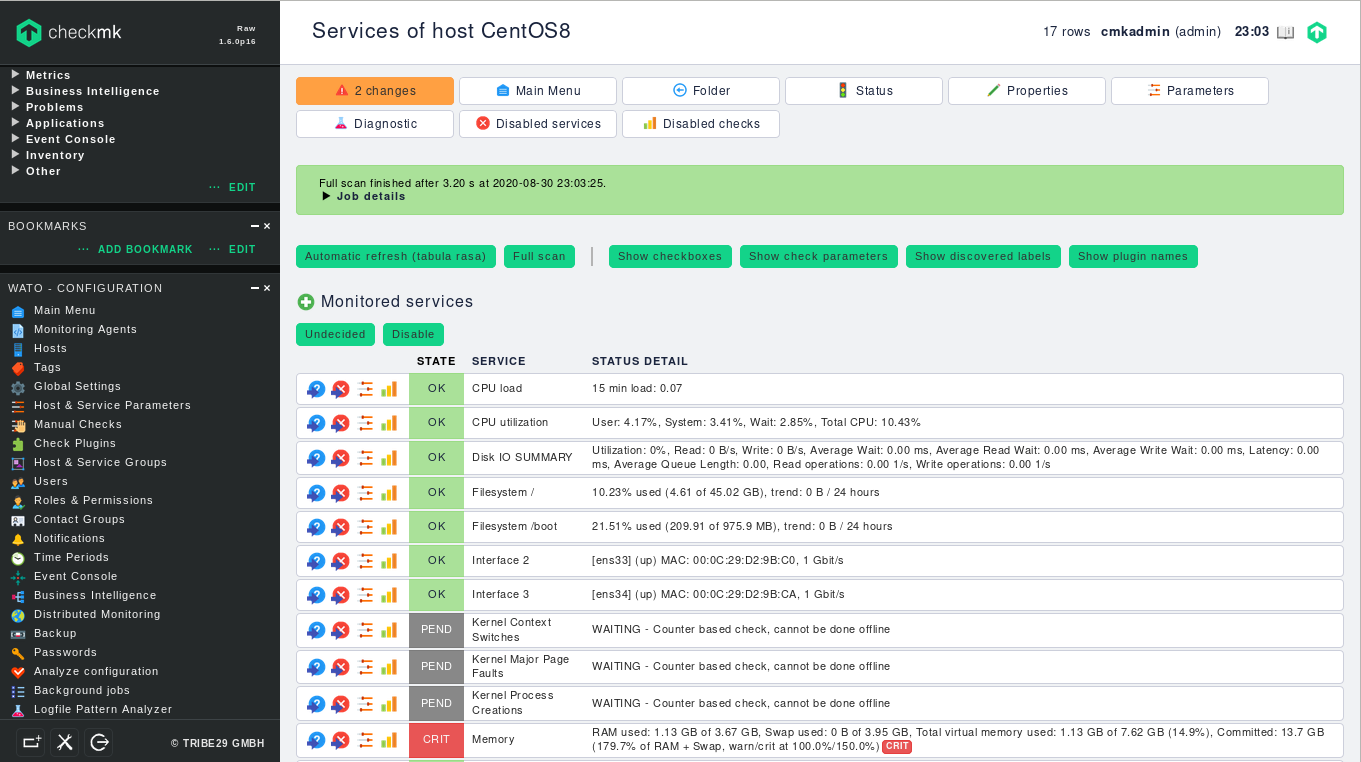
Nhập vào các thông số của máy Linux Agent:



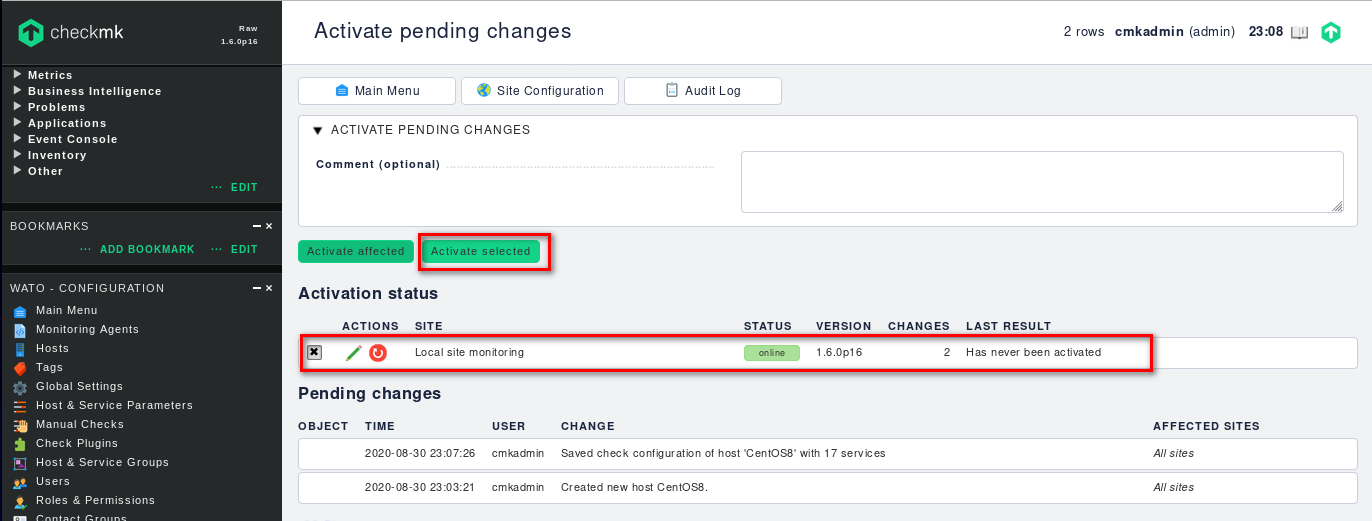
Chúng ta sẽ đi vào việc quyết định giám sát những service nào. Nếu muốn giám sát tất cả những service mà check\_mk phát hiện được hãy chọn **monitor** không thì hãy chọn **disable**. Còn nếu bạn muốn loại bỏ hay giám sát 1 service riêng lẻ nào đó hãy chọn dấu x hoặc tích nhé

Ở bài Lab này chúng ta sẽ Monitor tất cả nên chọn vào mục Monitor.

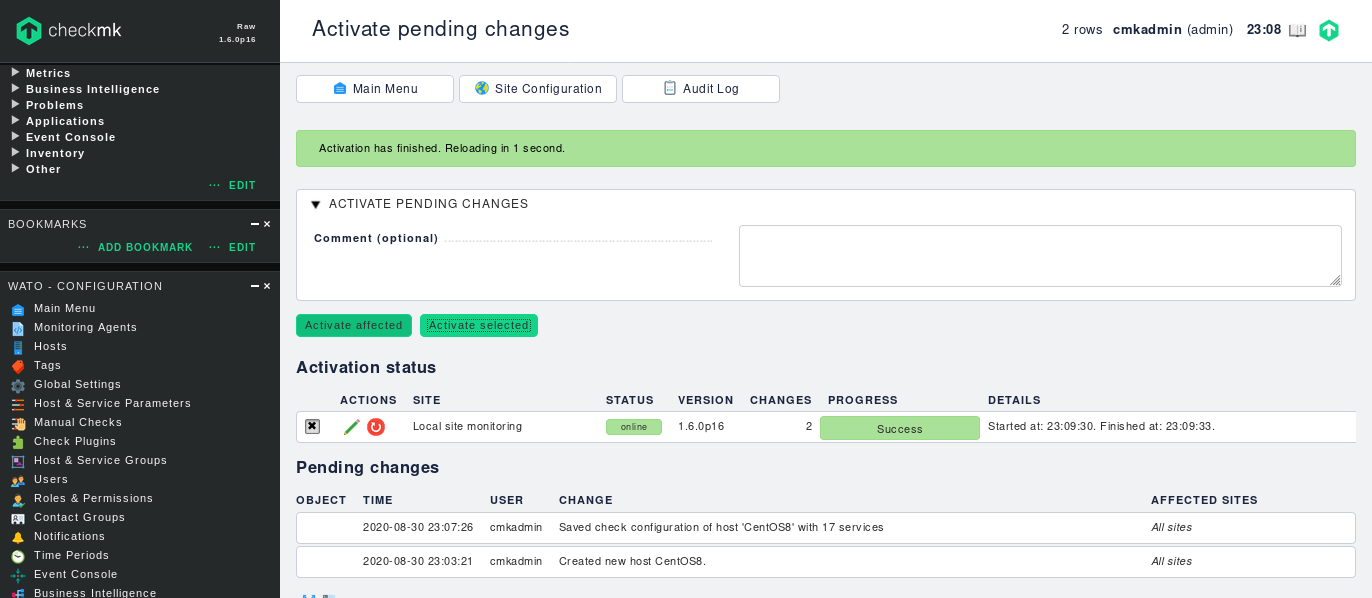




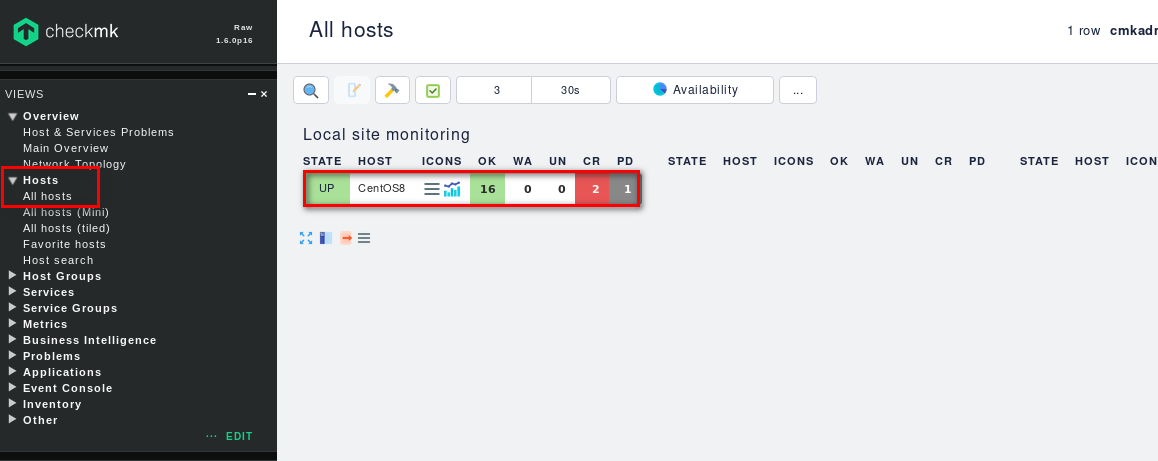
Sau đó chọn vào mục Changes phía trên. Chọn như hình để cập nhật các chỉnh sửa.

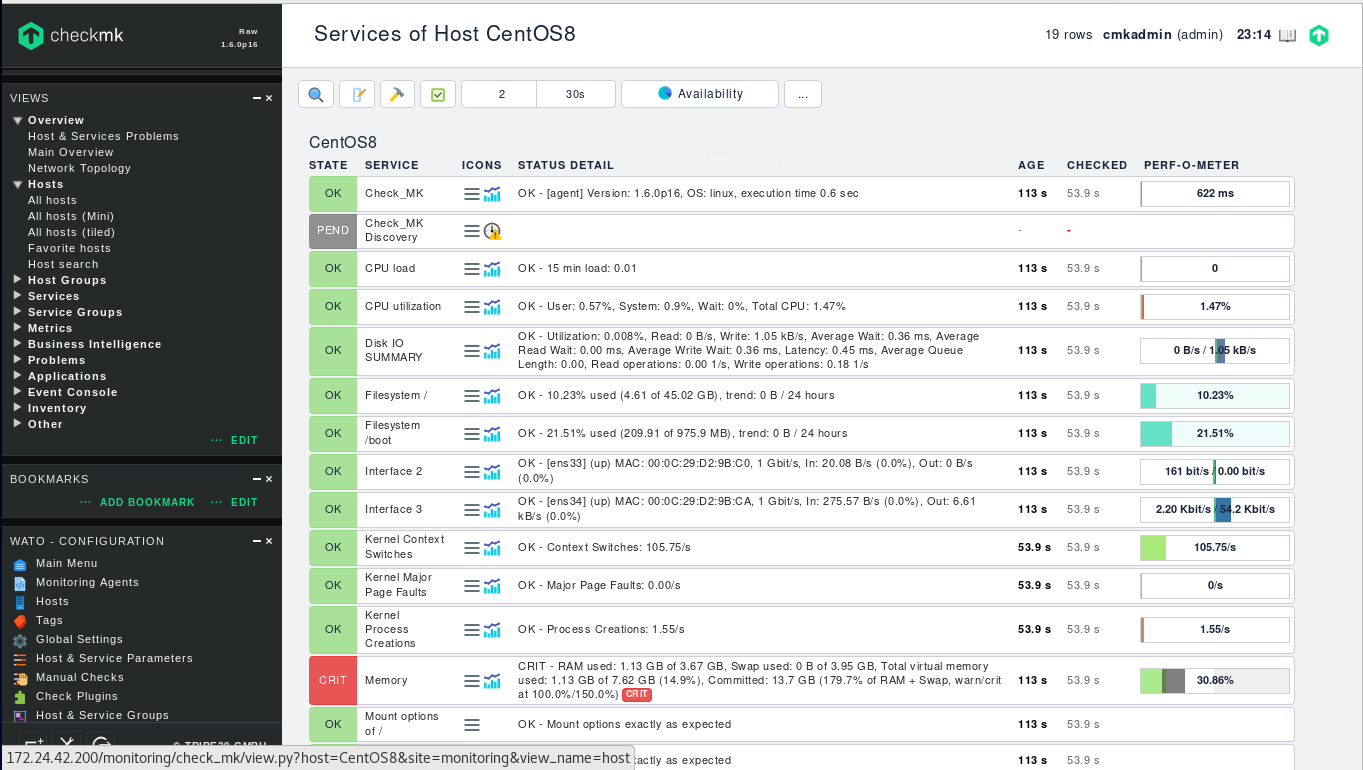


Cập nhật thành công



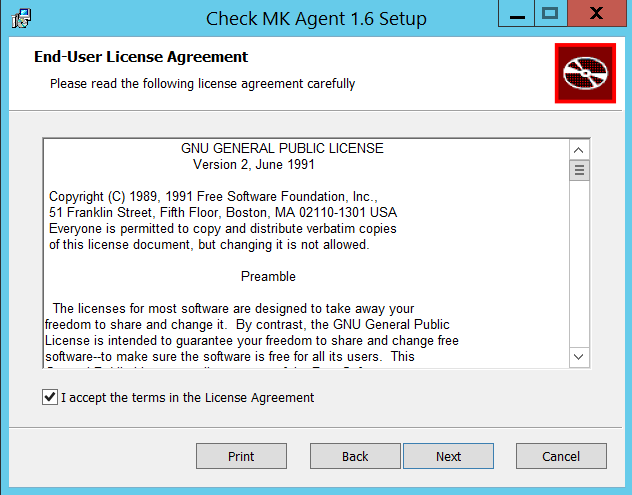
Kiểm tra lại host vừa mới thêm vào, tại Views, chọn Hosts rồi sau đó vào All host:



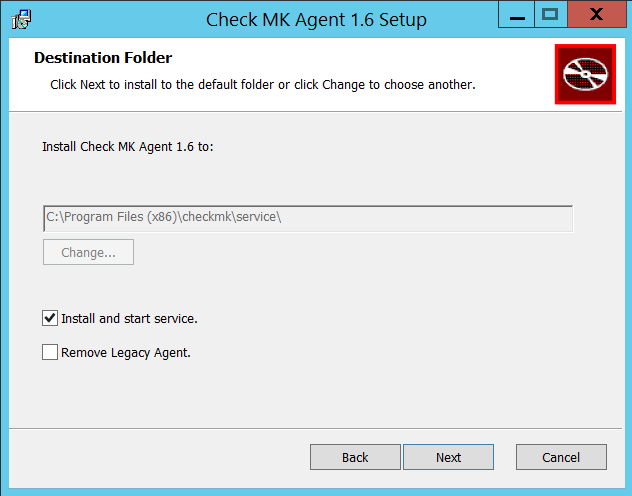


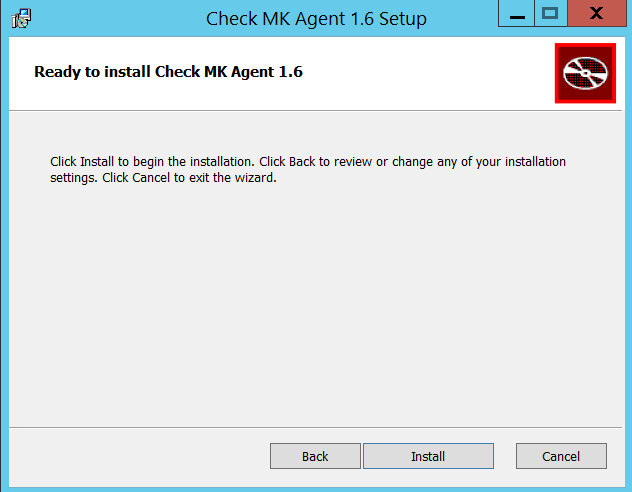
*2. Thêm Host Windows:*

Tiến hành tải agent dành cho Windows về máy Windows cần giám sát:



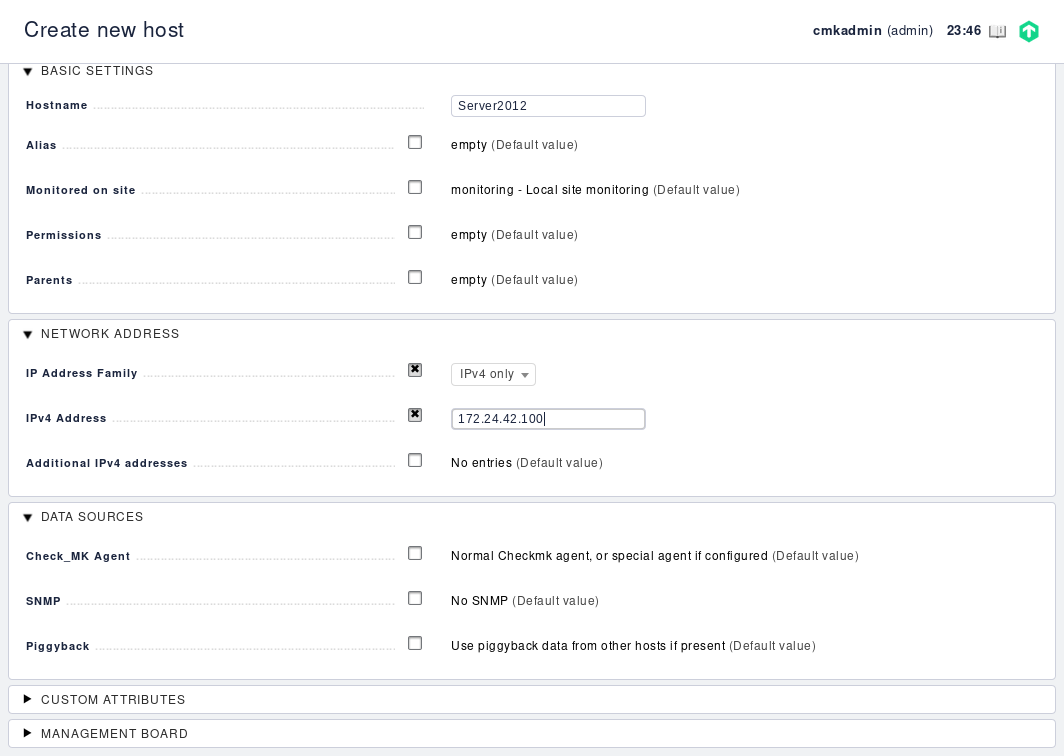
Cài đặt Agent này lên máy Windows:

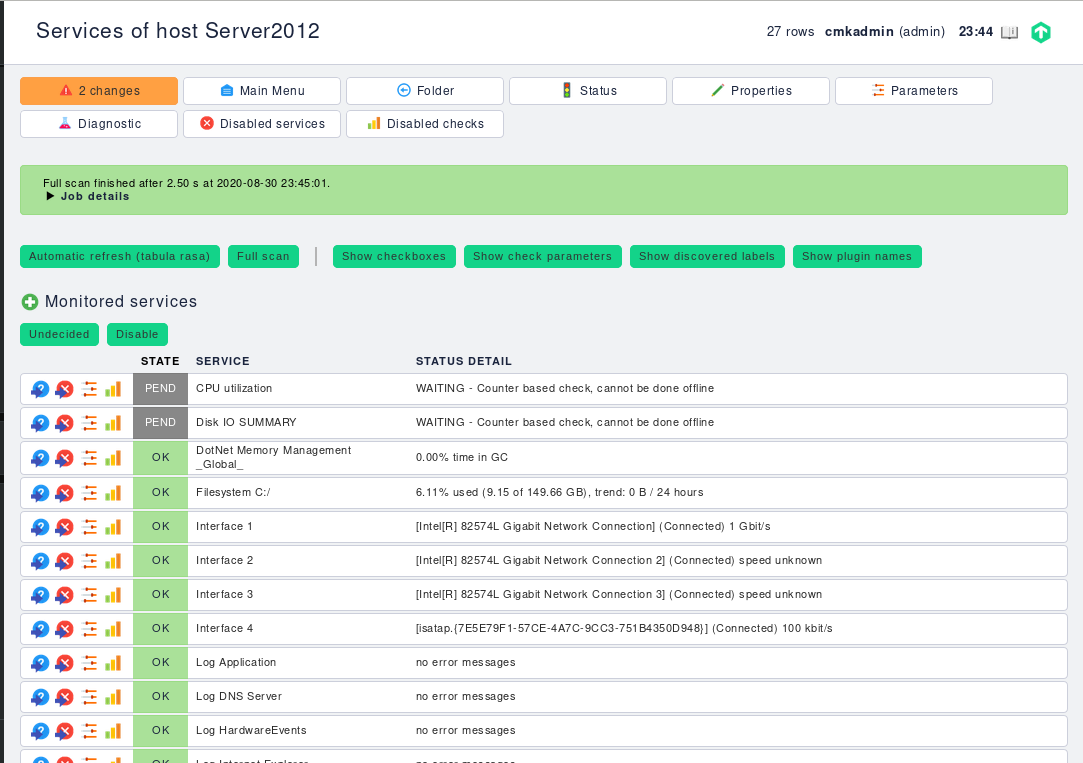




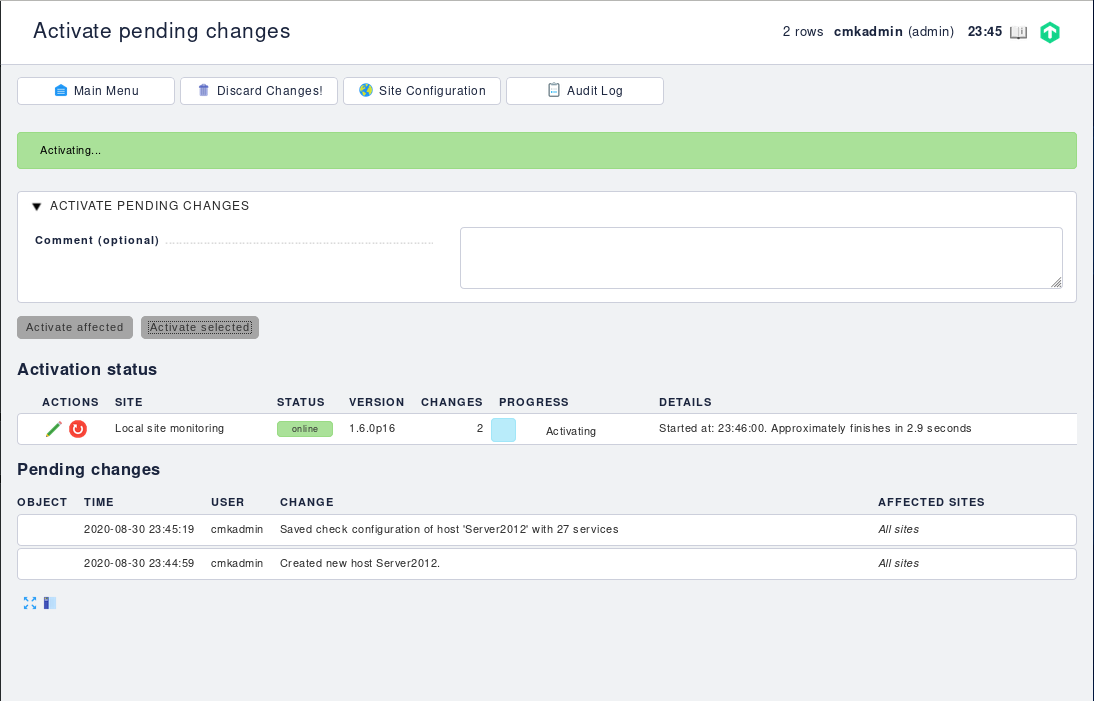
Sau khi cài đặt xong cho máy Windows quay trở lại máy Server CMK:

Vào Web UI và tiến hành thêm Host:





Cập nhật các thay đổi:



Quay lại VIEWS để xem Host Windows được thêm vào:



*3. Thêm Host Router:*

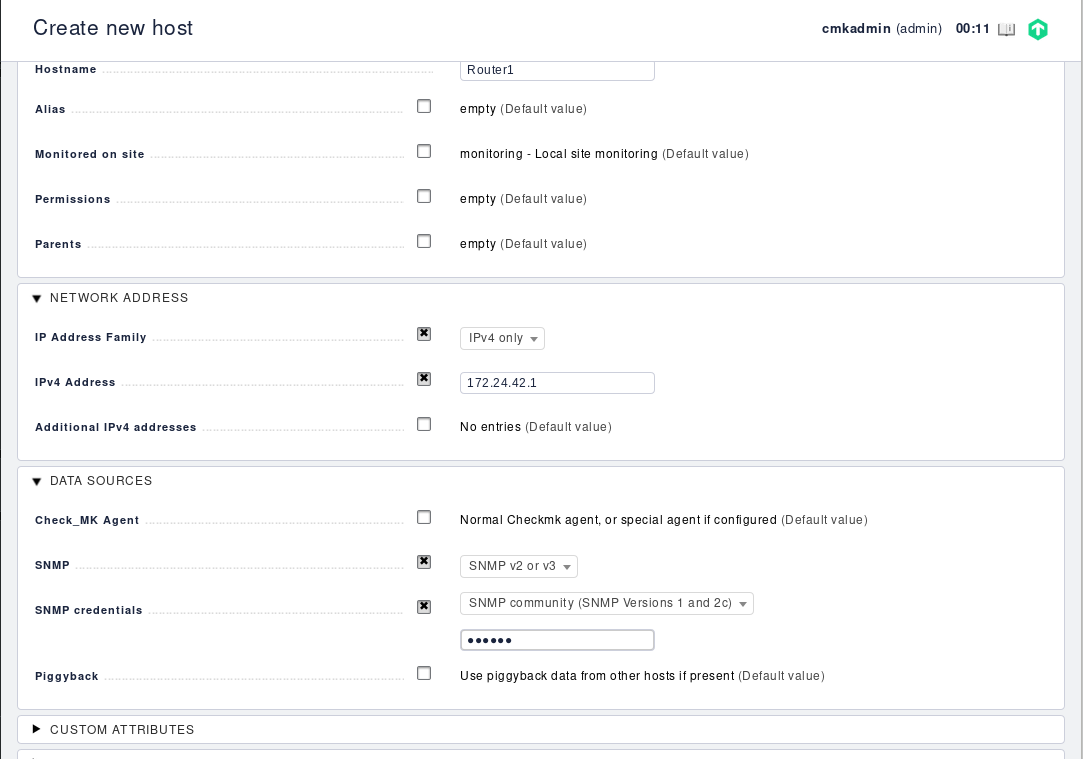
Trên Router cấu hình SNMP

**snmp-server community public RW**

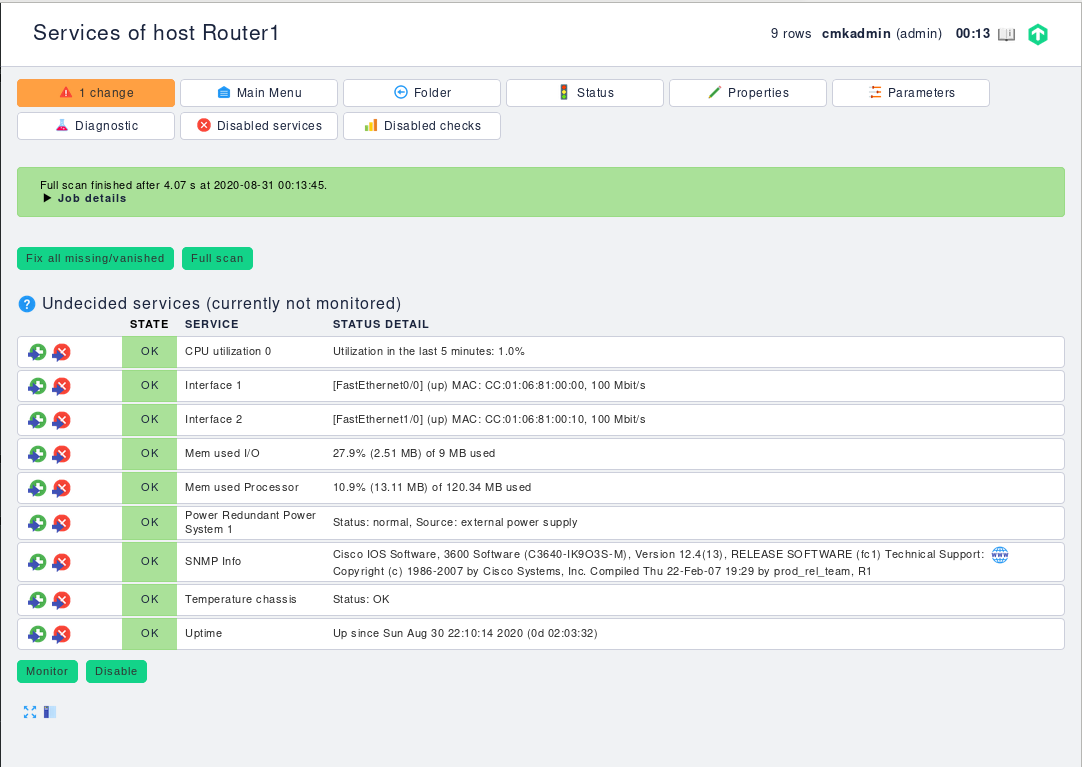
Quay lại máy Server CMK:

Tiến hành thêm Host:

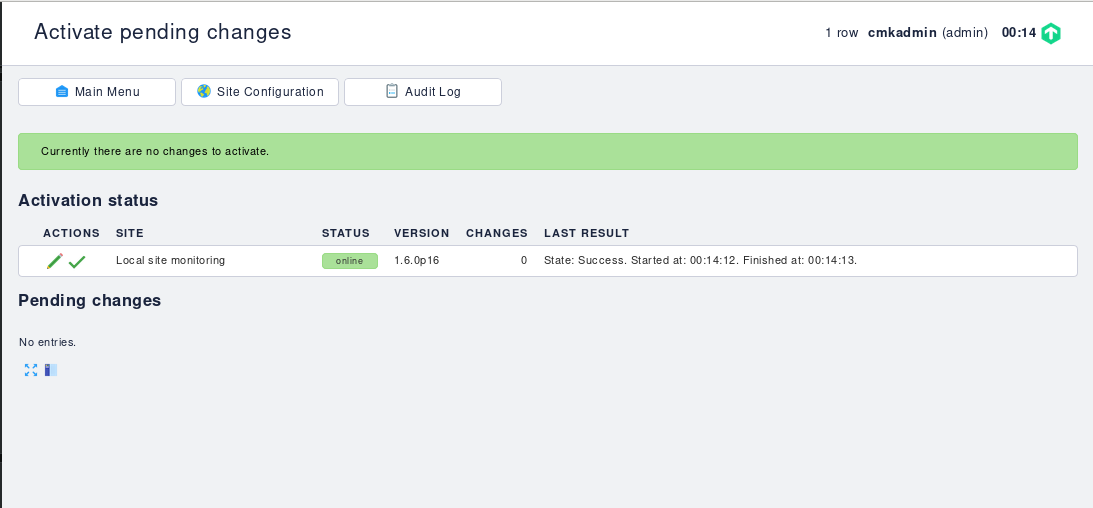
Phần SNMP nhập đúng chuỗi community mà chúng ta cấu hình trên Router



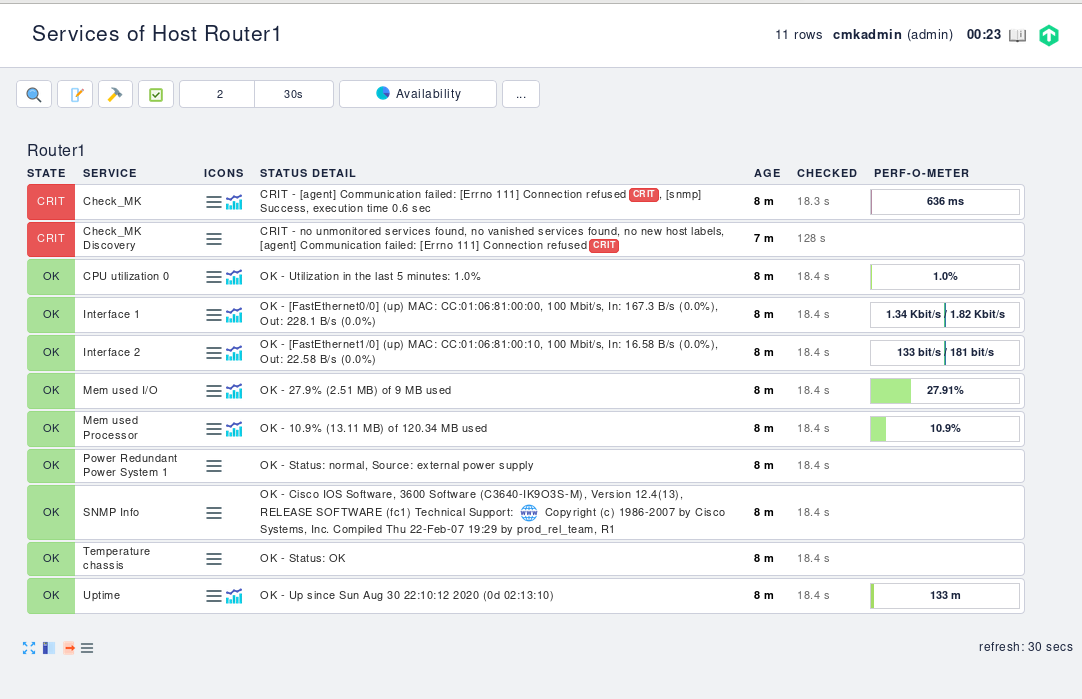
Chọn Services cho Router:



Cập nhật thay đổi:



Quay lại Tab VIEWS để kiểm tra host:

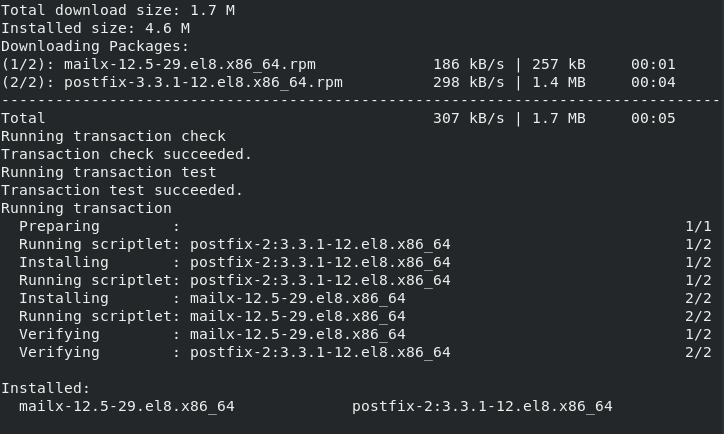


**IV. Cảnh báo qua Gmail:**

*1. Cấu hình relay gmail:*

Cài đặt gói postfix để relay gmail:

#dnf -y install postfix cyrus-sasl-plain mailx



*2. Cấu hình xác thực cho gmail:*

Các thông tin cấu hình của postfix được lưu trữ trong folder /etc/postfix. Vậy chúng ta sẽ tạo luôn thông tin của Gmail ở đây.

#vi /etc/postfix/sasl\_passwd

Thêm vào đó nội dung có cú pháp như sau:

[smtp.gmail.com]:587 username@gmail.com:password

*3. Khai báo địa chỉ lưu trữ thông tin của gmail trong file cấu hình của nó /etc/postfix/main.cf*

relayhost = [smtp.gmail.com]:587

smtp\_use\_tls = yes

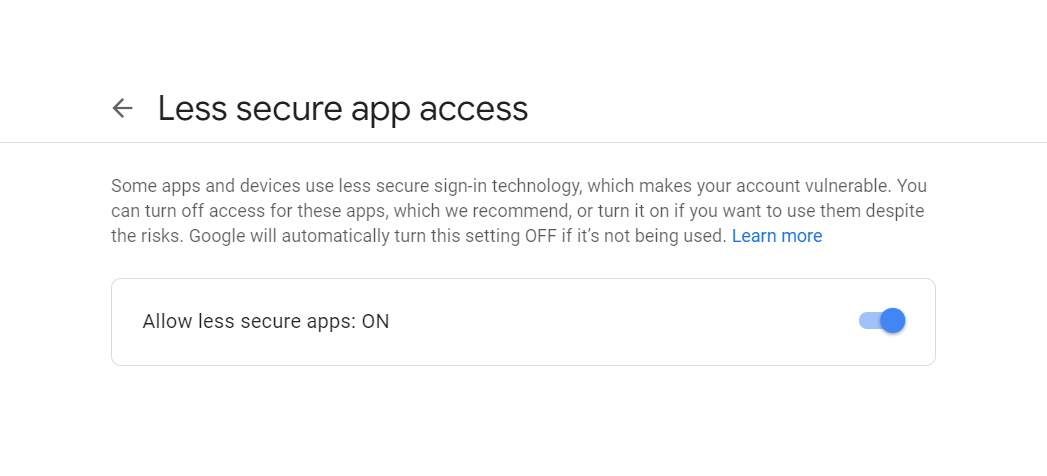
smtp\_sasl\_auth\_enable = yes

smtp\_sasl\_security\_options =

smtp\_sasl\_password\_maps = hash:/etc/postfix/sasl\_passwd

smtp\_tls\_CAfile = /etc/ssl/certs/ca-bundle.crt

Trong gmail có một chức năng chặn một số truy cập kém an toàn ta cần phải bật chức năng cho phép tất cả các truy cập đều có thể vào được. và ta làm điều đó tại link bên dưới:



*4. Cấp quyền sử dụng và đọc file lưu trữ thông tin của Gmai:*

#chown root:postfix /etc/postfix/sasl\_passwd\*

#chmod 600 /etc/postfix/sasl\_passwd

#postmap /etc/postfix/sasl\_passwd

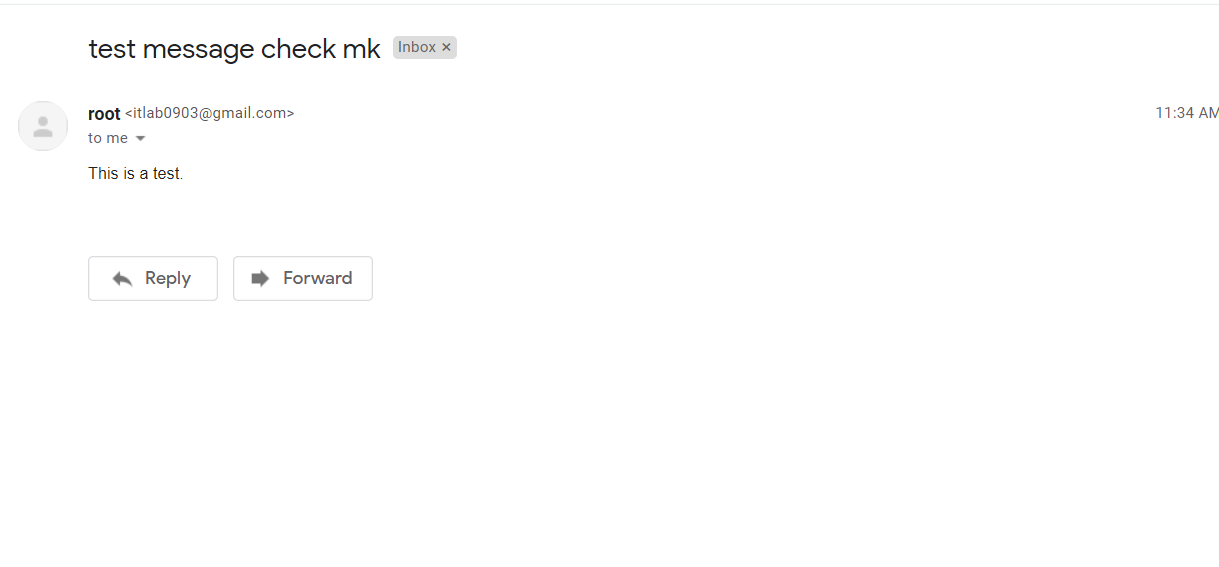
*5. Khởi động dịch vụ postfix:*

#systemctl start postfix

#systemctl enable postfix

*6. Kiểm tra xem dịch vụ đó đã được hoạt động hay chưa:*

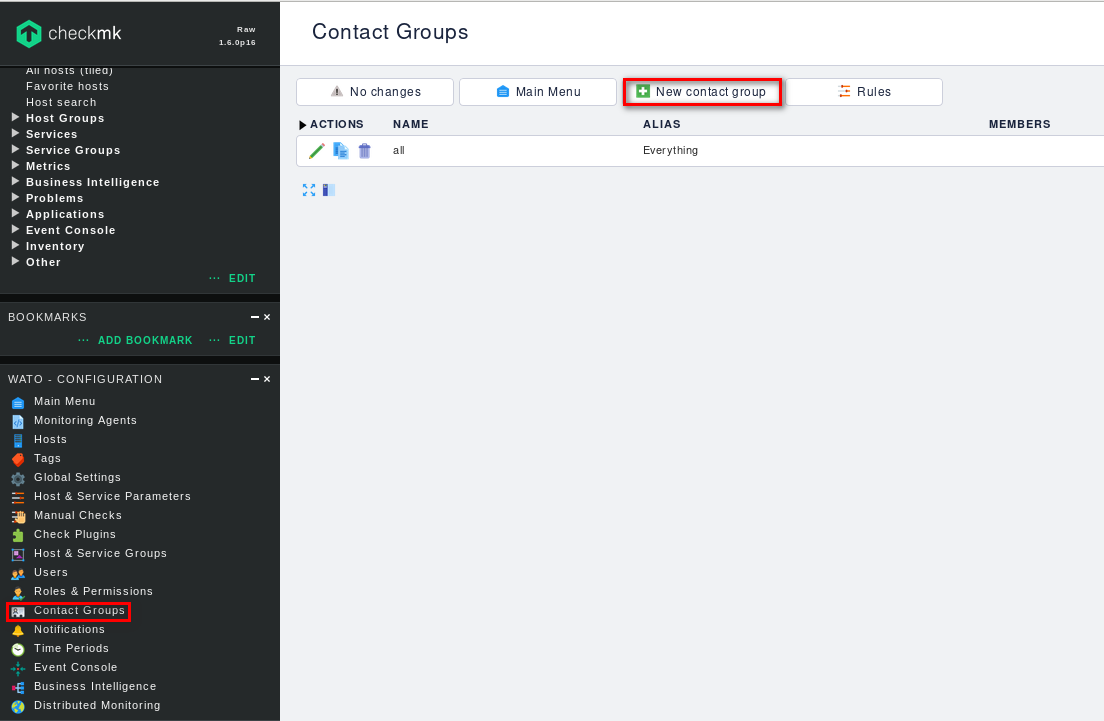
# echo "This is a test." | mail -s "test message check mk" [yourmail@gmail.com](mailto:yourmail@gmail.com)



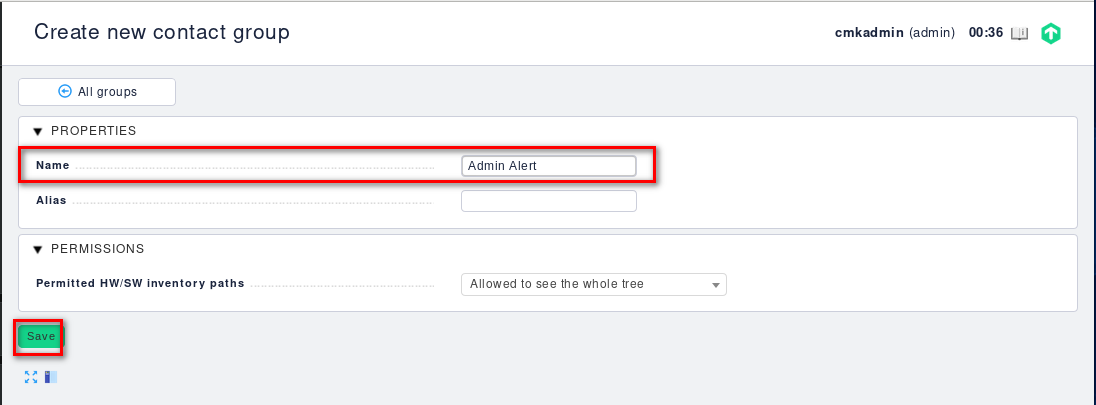
**V. Cấu hình gửi mail trong check\_mk:**

Tạo ra một group những người có thể nhận thông báo:

Đầu tiên sẽ vào contact groups sau đó nhấn vào new contact group để tạo ra một group mới

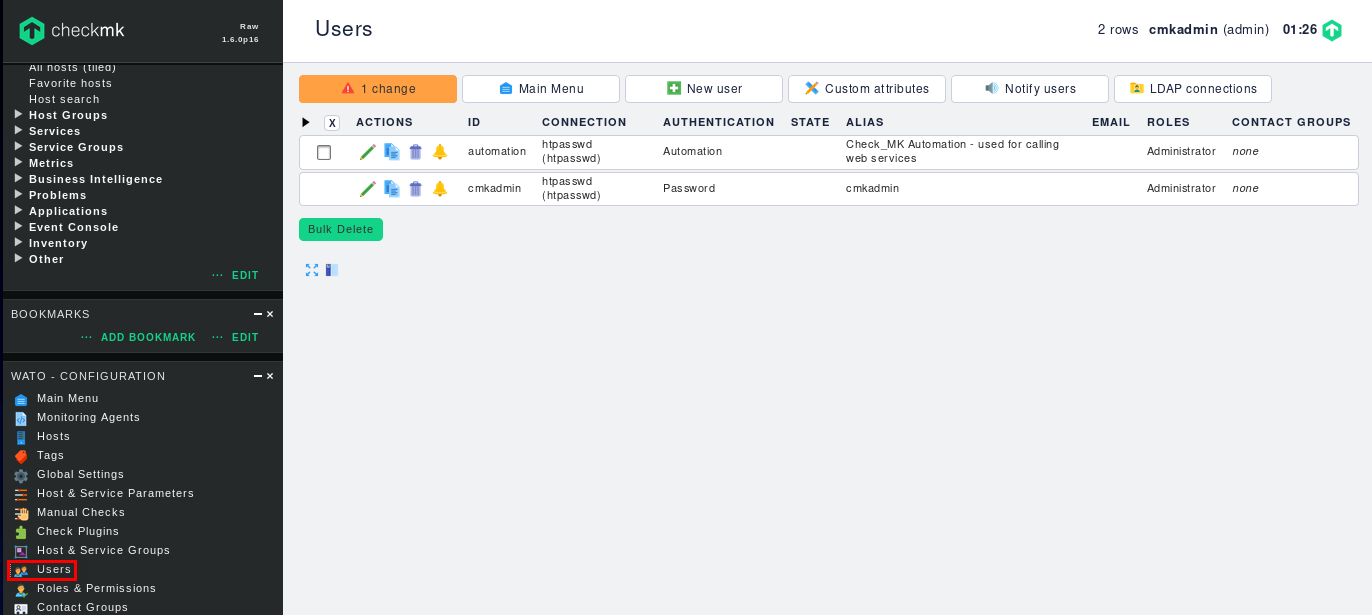


Đặt tên cho contact group này



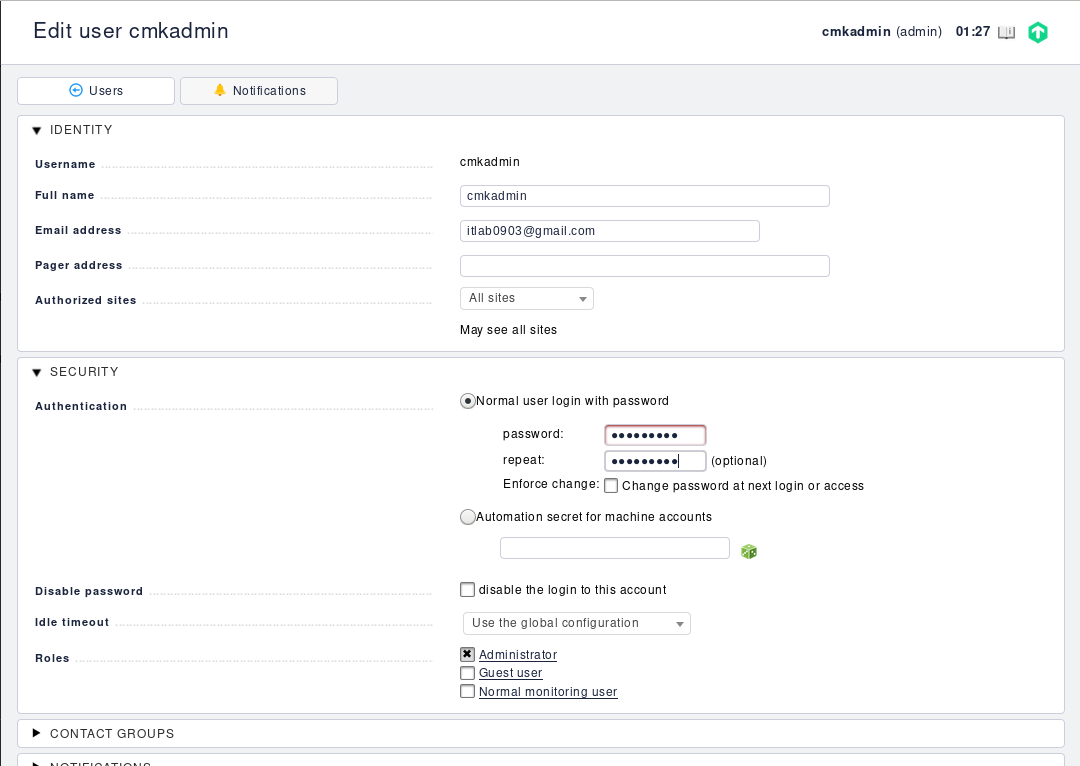
Tiếp theo chúng ta sẽ chọn User để nhận thông báo. Có thể tạo User mới hoặc dùng chính User cmkadmin

Chọn vào Users



Ở đây sử dụng chính cmkadmin nên sẽ chọn vào hình cây viết để edit User này:

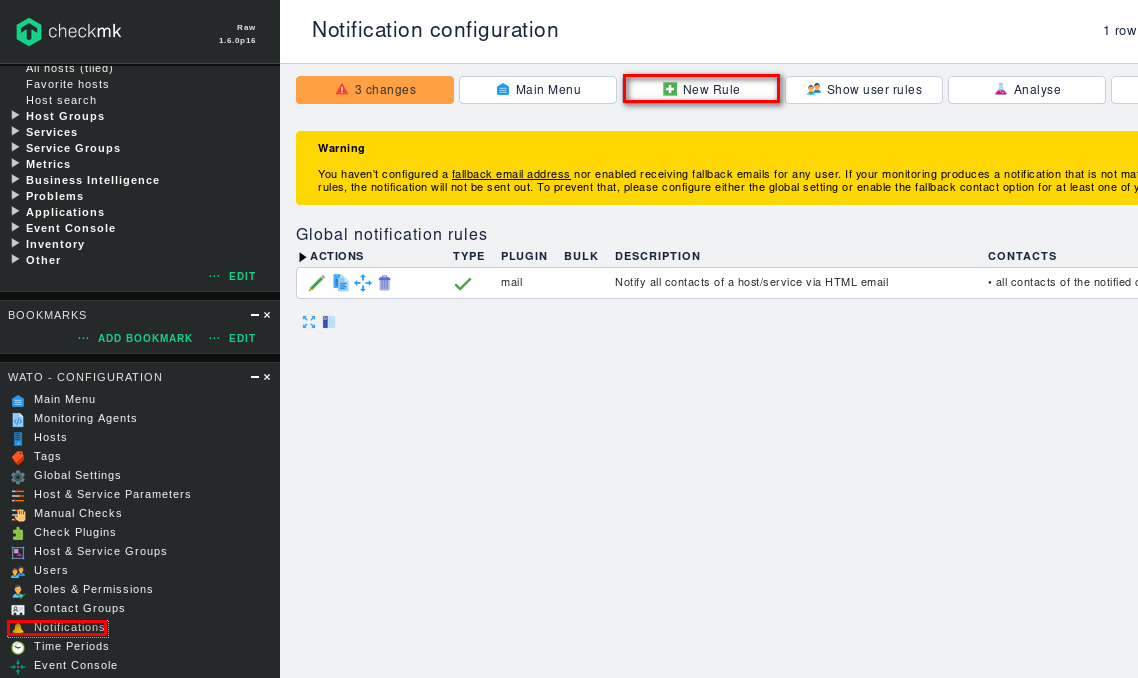
Nhập vào email nhận cảnh báo.



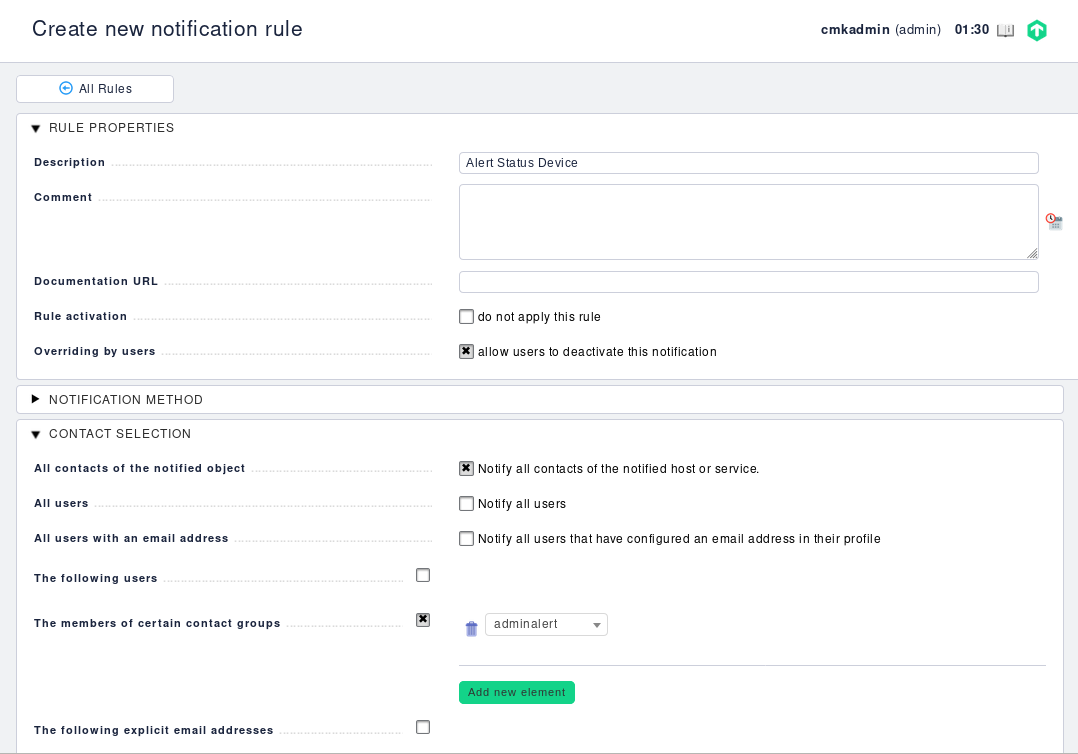
Kéo xuống chọn vào Contact Group vừa tạo



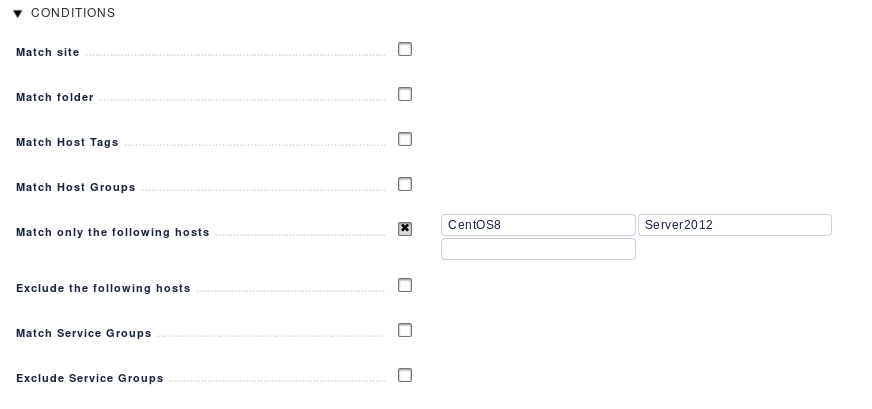
Chọn Notification -> New Rule:



Cấu hình như hình bên dưới



Có rất nhiều cách để mà cảnh báo này có thể match(cảnh báo theo ). Có thể là cảnh báo với 1 service nào đó nhưng ở đây chọn match theo host. Có rất nhiều option để chúng ta lựa chọn.



Tiến hành cập nhật các thay đổi

Thử tắt máy và nhận cảnh báo. Và hãy kiểm tra nội dung của nó:

