ĐẠI HỌC ĐÀ NẴNG
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG VIỆT - HÀN
Vietnam - Korea University of Information and Communication Technology

GIÁM SÁT MẠNG

Giảng viên: Lê Tự Thanh
Email : ltthanh@vku.udn.vn
Website : www.vku.udn.vn

CHƯƠNG 5. TRIỂN KHAI HỆ THỐNG GIÁM SÁT

5.1. Yêu cầu chung của hệ thống giám sát

- ✓ Quản lý lỗi (Fault management):

Các vấn đề mạng được phát hiện và sửa chữa. Các vấn đề tiềm tàng được xác định và có các biện pháp hữu hiệu kịp thời để ngăn chặn chúng xảy ra hoặc tái diễn. Với mô đun Fault management, mạng lưới sẽ hoạt động và thời gian chết của thiết bị cũng như hệ thống mạng được giảm tối thiểu.

5.1. Yêu cầu chung của hệ thống giám sát

✓ Quản lý cấu hình (Configuration management):

Mô đun này sẽ thực hiện giám sát và kiểm soát hoạt động của mạng lưới. Điều phối các thay đổi về phần cứng và chương trình, bao gồm cả việc bổ sung thiết bị mới và chương trình mới, sửa đổi các hệ thống hiện có và xóa bỏ các hệ thống chương trình lỗi thời. Ở mức độ này thì tài nguyên của các thiết bị và chương trình được lưu giữ và cập nhật thường xuyên.

CHƯƠNG 5. TRIỂN KHAI HỆ THỐNG GIÁM SÁT

5.1. Yêu cầu chung của hệ thống giám sát

- ✓ Quản lý tài khoản (Accounting management) :

Mô đun này được sử dụng để phân phối các tài nguyên một cách tối ưu và công bằng giữa các người dùng mạng. Điều này giúp sử dụng hiệu quả nhất các hệ thống sẵn có, giảm thiểu chi phí vận hành.

5.1. Yêu cầu chung của hệ thống giám sát

✓ Quản lý hiệu năng (Performance management):

Mô đun này liên quan đến việc quản lý toàn bộ hiệu năng của toàn mạng. Thông lượng tối đa, tắc nghẽn mạng và các vấn đề tiềm tàng cần được xác định. Một phần quan trọng khi quản lý hiệu năng là cần mang lại hiệu suất tổng thể lớn nhất.

5.1. Yêu cầu chung của hệ thống giám sát

✓ Security management (Quản lý bảo mật):

Mô đun này chịu trách nhiệm xử lý và đảm bảo an ninh mạng lưới bởi tin tặc, những người dùng trái phép, hoặc các thiết bị phá hoại. Tính bảo mật thông tin người dùng cần được duy trì được đảm bảo. Hệ thống an ninh cũng cho phép quản trị viên kiểm soát từng cá nhân có thể (và không thể) được làm những gì với hệ thống.

5.2. Hạ tầng cho hệ thống giám sát

✓ Yêu cầu về thiết bị: Cần có cấu hình phù hợp để vận hành và xây dựng hệ thống giám sát tập trung.

+ Core Switch: phải có tốc độ xử lý cao, hỗ trợ cổng có băng thông lớn. Một số dòng đáp ứng nhu cầu như: Switch Cisco 3750, 3850,... Port 1Gbps.

+ Server phân tích thông tin: cần quan tâm đến cấu hình của CPU, Memory, Storage tùy theo nhu cầu bài toán đặt ra. Về CPU thì nên chọn CPU có nhiều lõi (từ 4-8 lõi) với tốc độ trung bình từ 3.6GHz đến 3.9GHz (nên chọn số lõi ưu tiên hơn tốc độ xử lý để gia tăng khả năng xử lý).

5.2. Hạ tầng cho hệ thống giám sát

Bộ nhớ: tùy theo nhu cầu, nên từ 16-64GB. Riêng Disk thì ta phải xem xét lượng dữ liệu thu thập sẽ "đổ về" server.

Ví dụ: trong 1 ngày trung bình khoảng 1GB dữ liệu đổ về và ta cần lưu trữ dữ liệu thu thập được trong ít nhất 30 ngày (trên 30 ngày tự động xóa) thì ít nhất ổ cứng phải có dung lượng 50GB trở lên (gồm dung lượng hệ điều hành, dữ liệu thu thập được và một khoảng dung lượng phát sinh nếu có).

5.2. Hạ tầng cho hệ thống giám sát

✓ Yêu cầu về băng thông đường truyền:

Lượng thông tin cần truyền qua lại giữa các thiết bị trong hệ thống giám sát tập trung là rất nhiều nên băng thông đường truyền phải đủ lớn để các luồng dữ liệu di chuyển trong hệ thống không bị tắc nghẽn. Tùy theo tình hình thực tế, cần sử dụng những dây có băng thông lớn từ 1 Gbps đến 10 Gbps.

5.3. Mô hình hệ thống giám sát

Mô hình hệ thống giám sát tập trung

5.3. Mô hình hệ thống giám sát

Mô hình tập trung: là quá trình tập trung, thu thập, phân tích... các log cần thiết từ nhiều nguồn khác nhau về một nơi an toàn để thuận lợi cho việc phân tích, theo dõi hệ thống.

Lợi ích của mô hình tập trung:

- Giúp quản trị viên có cái nhìn chi tiết về toàn bộ hệ thống
- Mọi hoạt động của hệ thống được ghi lại và lưu trữ ở một nơi an toàn đảm bảo tính toàn vẹn phục vụ cho quá trình phân tích điều tra các cuộc tấn công vào hệ thống (nếu có).
- Dễ phân tích cùng lúc khi sử dụng công cụ phân tích

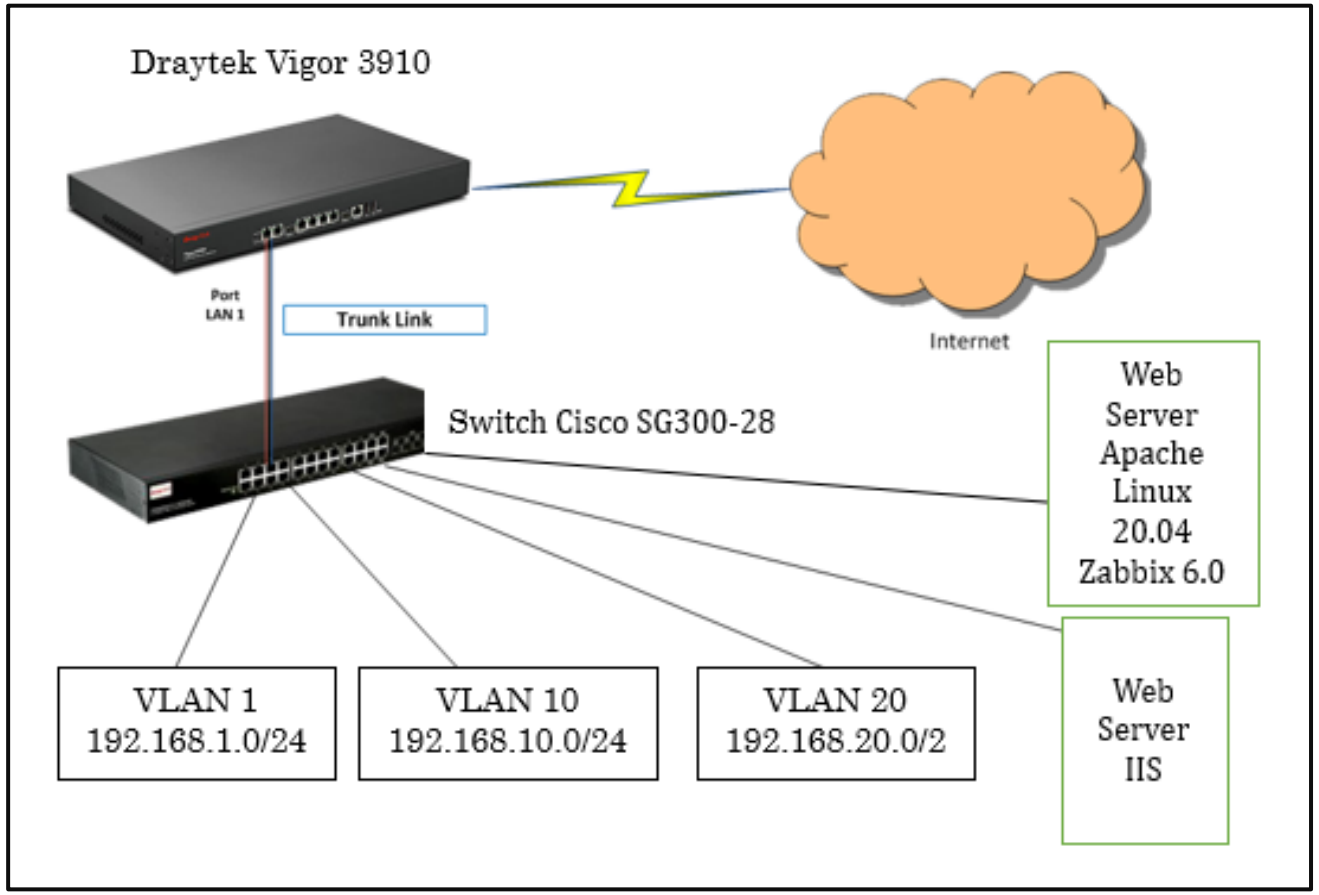
CHƯƠNG 5. TRIỂN KHAI HỆ THỐNG GIÁM SÁT

Mô hình hệ thống giám sát phân tán

Trong mô hình này Log chỉ lưu lại bản thân các Server riêng biệt.

- Khó sử lý, phân tích đồng thời
- Quản trị viên khó nhìn tổng quát về hệ thống thông qua log

5.4. Các thành phần cần giám sát



5.4. Các thành phần cần giám sát

Giám sát hạ tầng mạng

- Xác định thiết bị hạ tầng mạng cần giám sát

+ Router
+ Switch
+ Access Point
+ Tài nguyên máy chủ

- Xác định các thông số cần giám sát của thiết bị

+ CPU
+ RAM
+ Nhiệt độ

5.4. Các thành phần cần giám sát

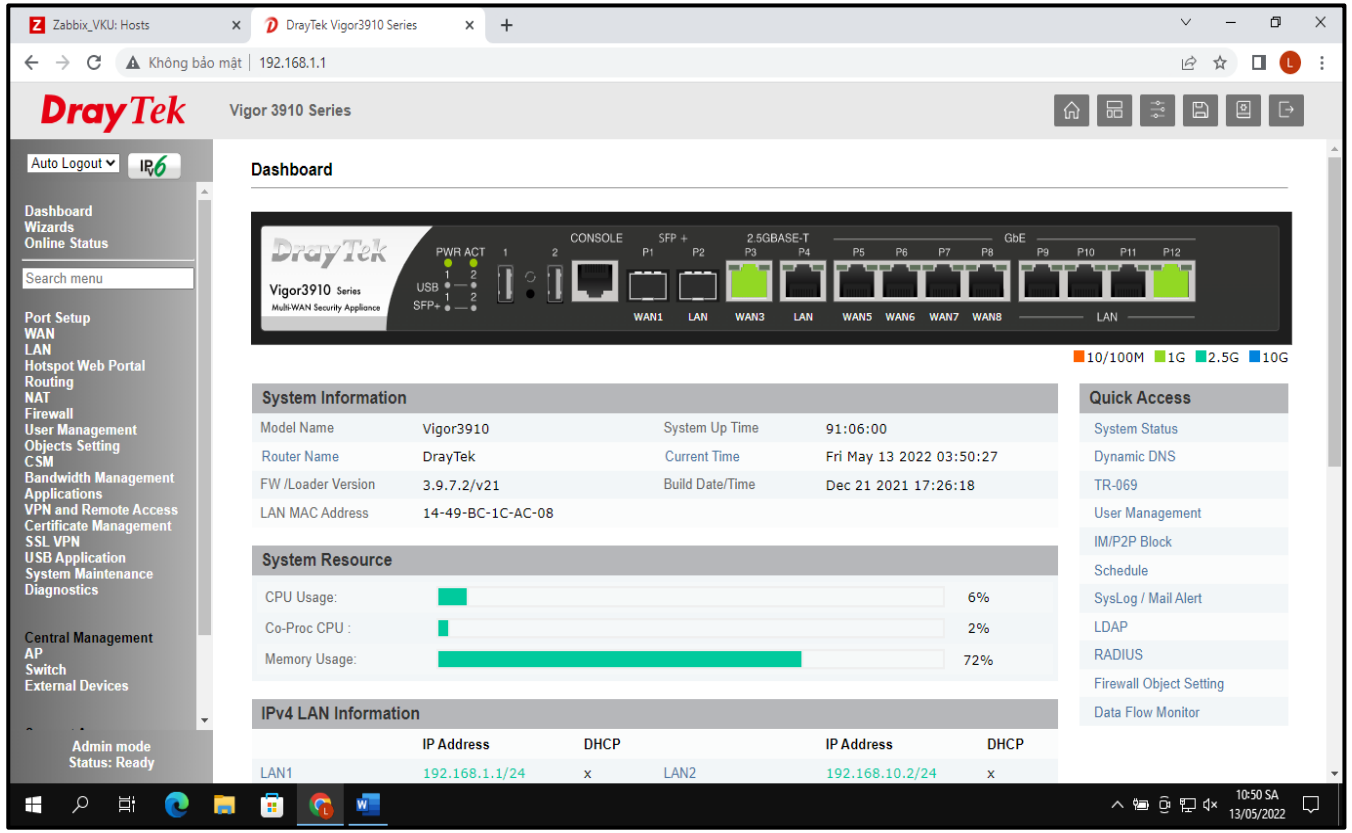
Giám sát dịch vụ mạng

- Xác định dịch vụ mạng cần giám sát

+ Web Server
+ DNS Server
+ DHCP Server
+ …..

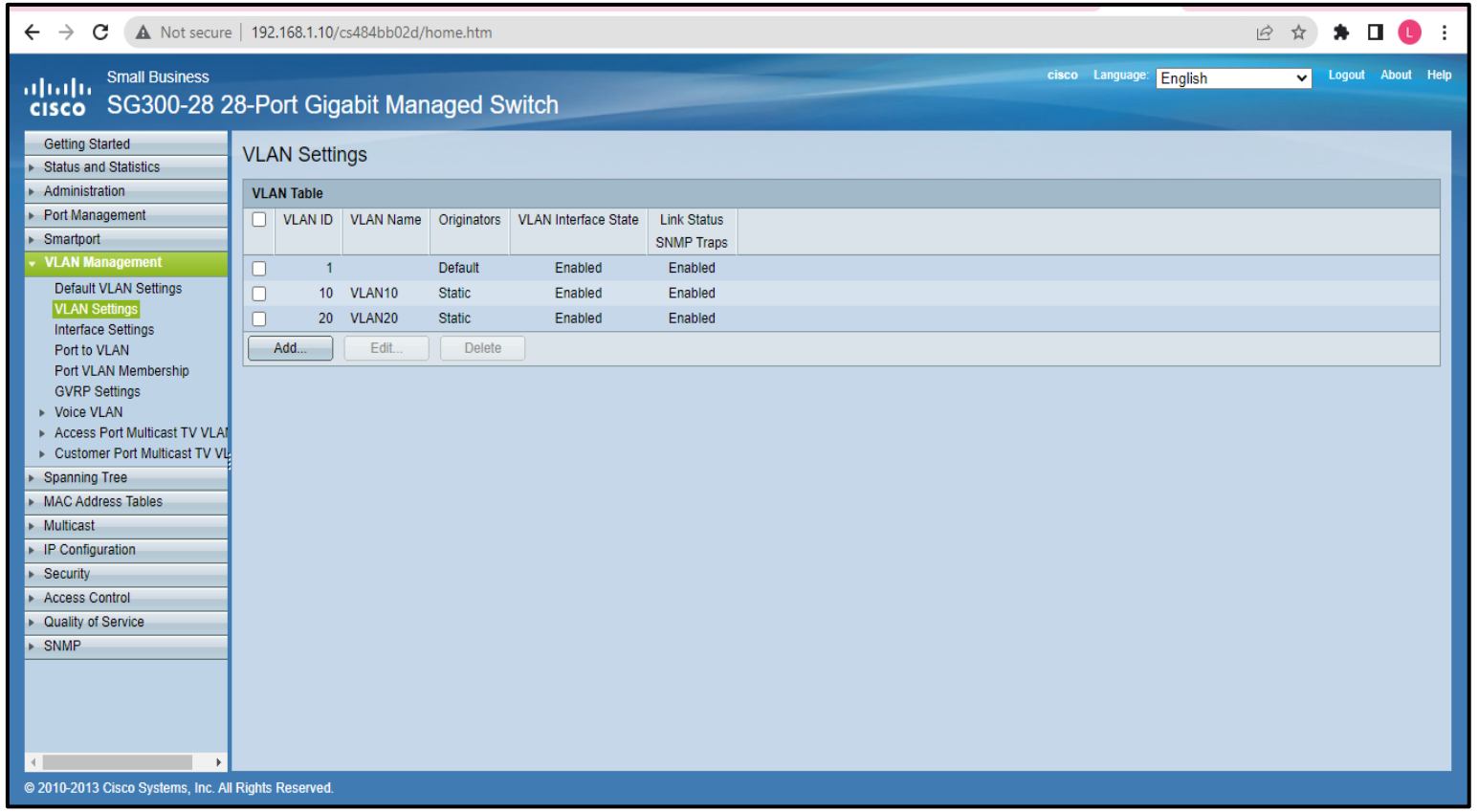
CHƯƠNG 5. TRIỂN KHAI HỆ THỐNG GIÁM SÁT

- Giám sát router: Giám sát port, bang thông, bộ nhớ,…



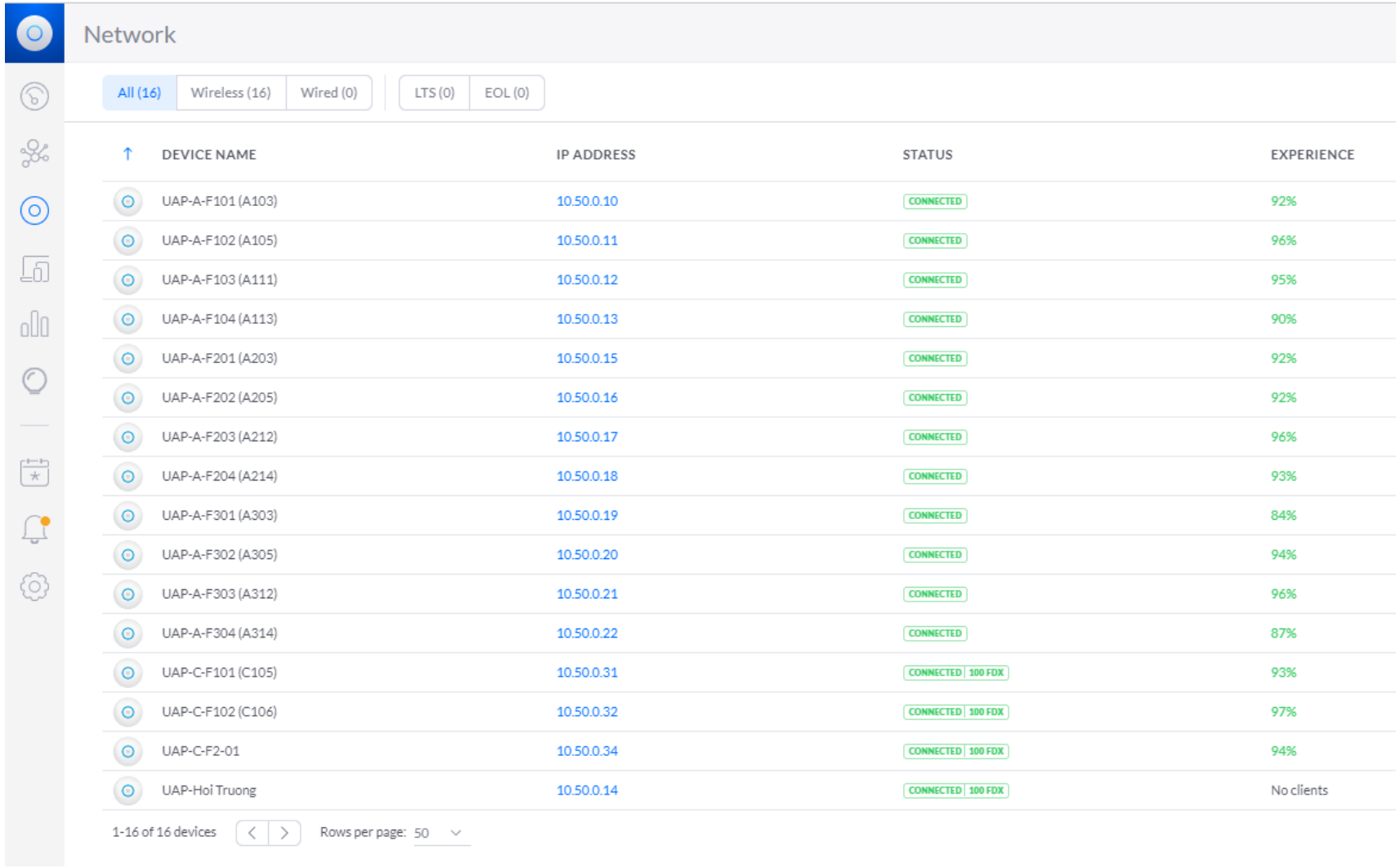
CHƯƠNG 5. TRIỂN KHAI HỆ THỐNG GIÁM SÁT

- Giám sát Switch: Giám sát port, Traffic, ….



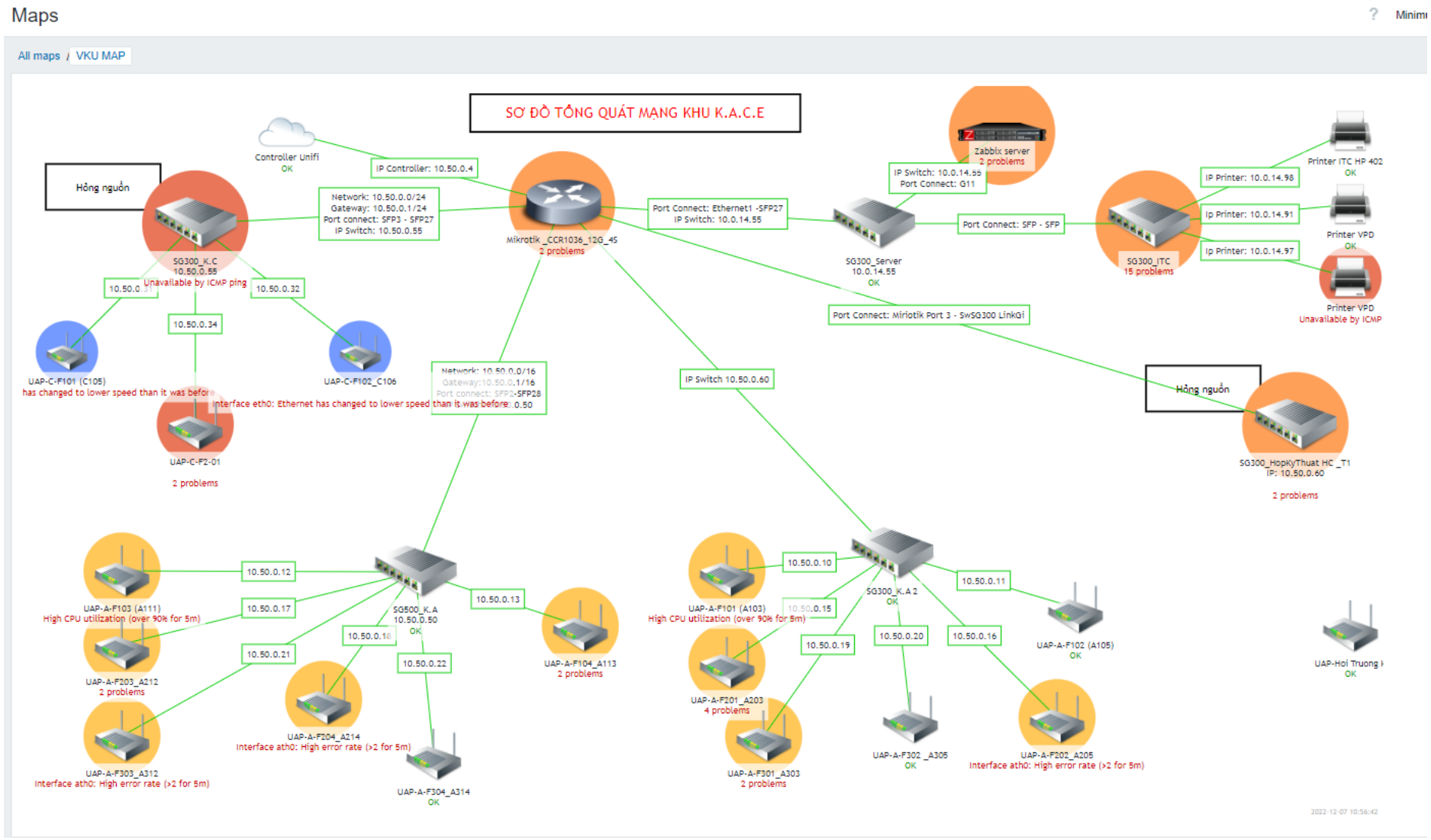
CHƯƠNG 5. TRIỂN KHAI HỆ THỐNG GIÁM SÁT

- Giám sát AP: Số lượng connect, traffic,…



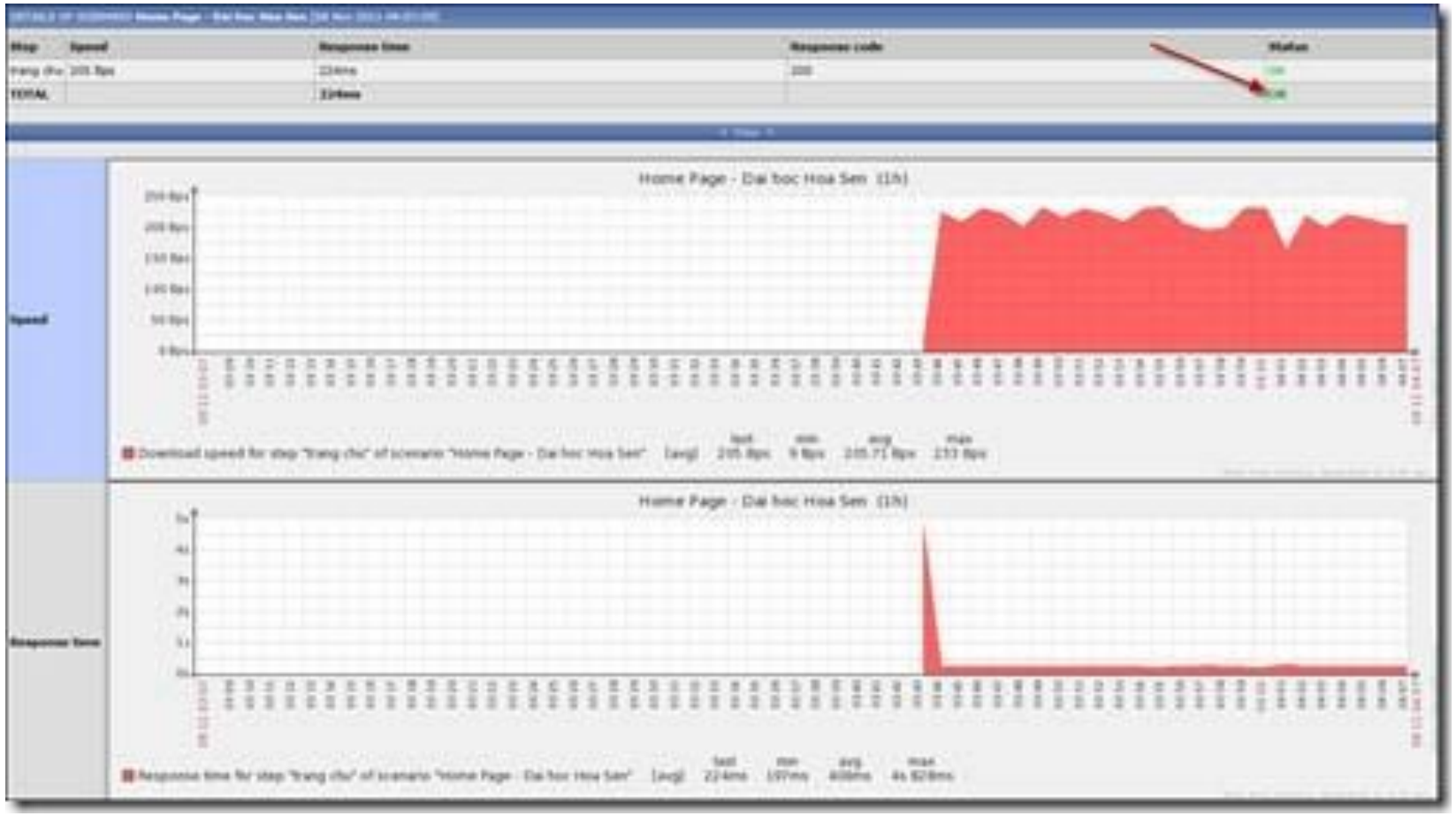
CHƯƠNG 5. TRIỂN KHAI HỆ THỐNG GIÁM SÁT

Ví dụ: Sơ đồ mạng cần giám sát



CHƯƠNG 5. TRIỂN KHAI HỆ THỐNG GIÁM SÁT

- Giám sát dịch vụ Web server

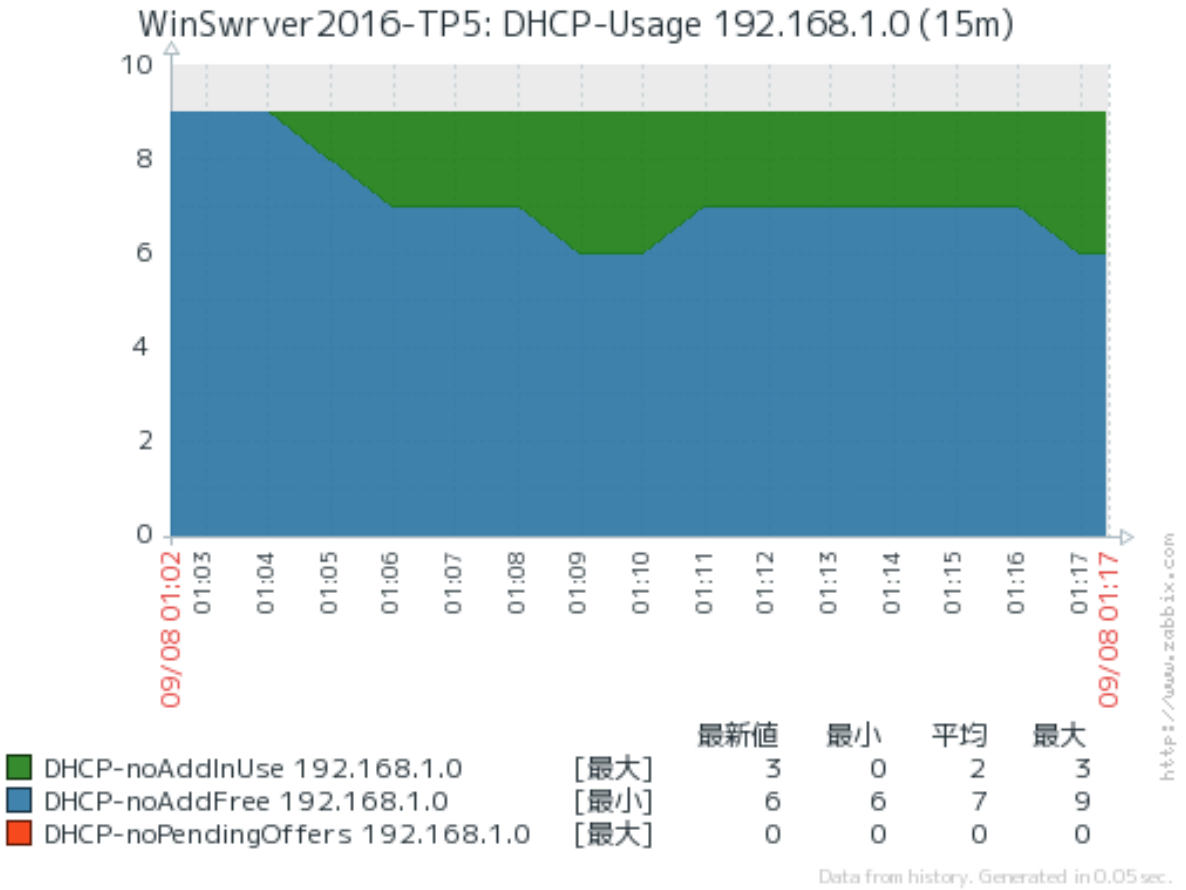


CHƯƠNG 5. TRIỂN KHAI HỆ THỐNG GIÁM SÁT

- Giám sát dịch vụ Web server

CHƯƠNG 5. TRIỂN KHAI HỆ THỐNG GIÁM SÁT

- Giám sát dịch vụ DHCP server



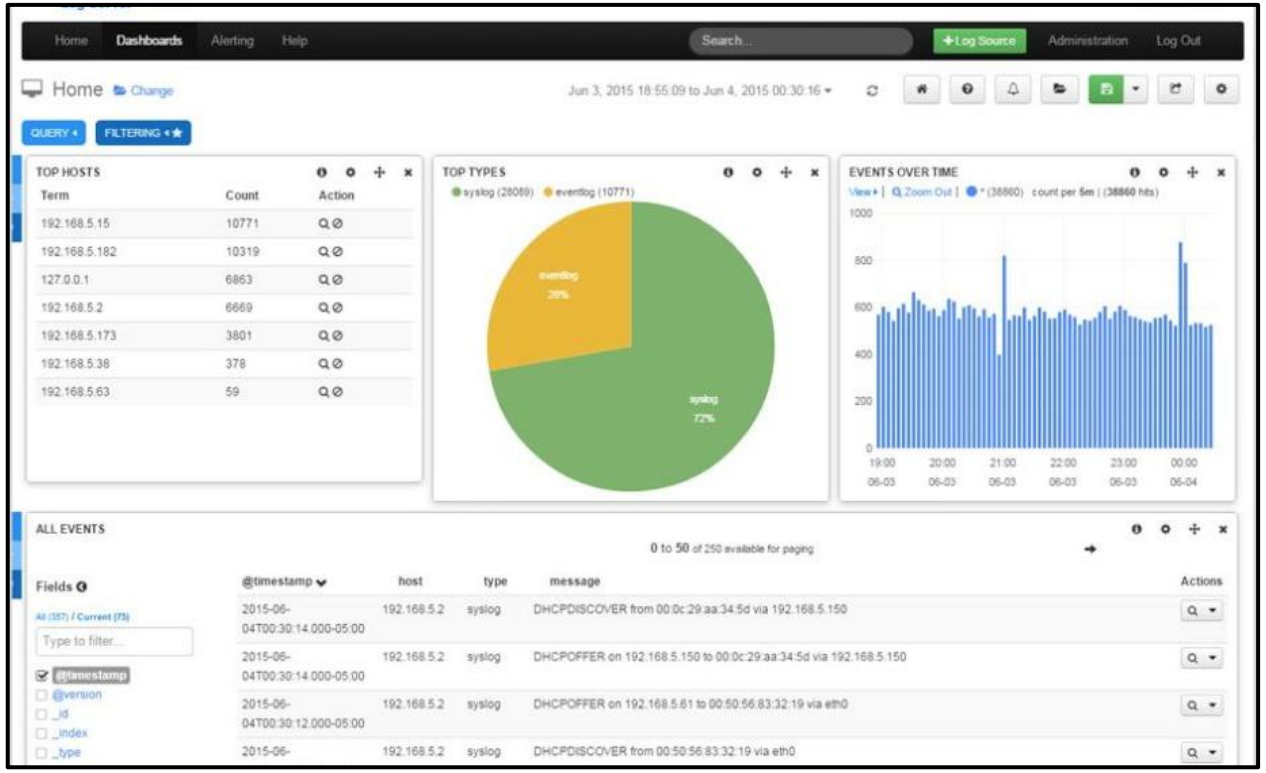
5.5. Một số phần mềm hệ thống giám sát

Hiện nay trên thị trường có rất nhiều phần mềm cho phép triển khai hệ thống giám sát mạng với nhiều cách thức, hiệu năng cũng như chi phí khác nhau.

5.5. Một số phần mềm hệ thống giám sát

Hệ thống giám sát nguồn mở

Phần mềm Nagios



Website tham khảo và thông tin thêm :
https://www.nagios.org

5.5. Một số phần mềm hệ thống giám sát

Hệ thống giám sát nguồn mở

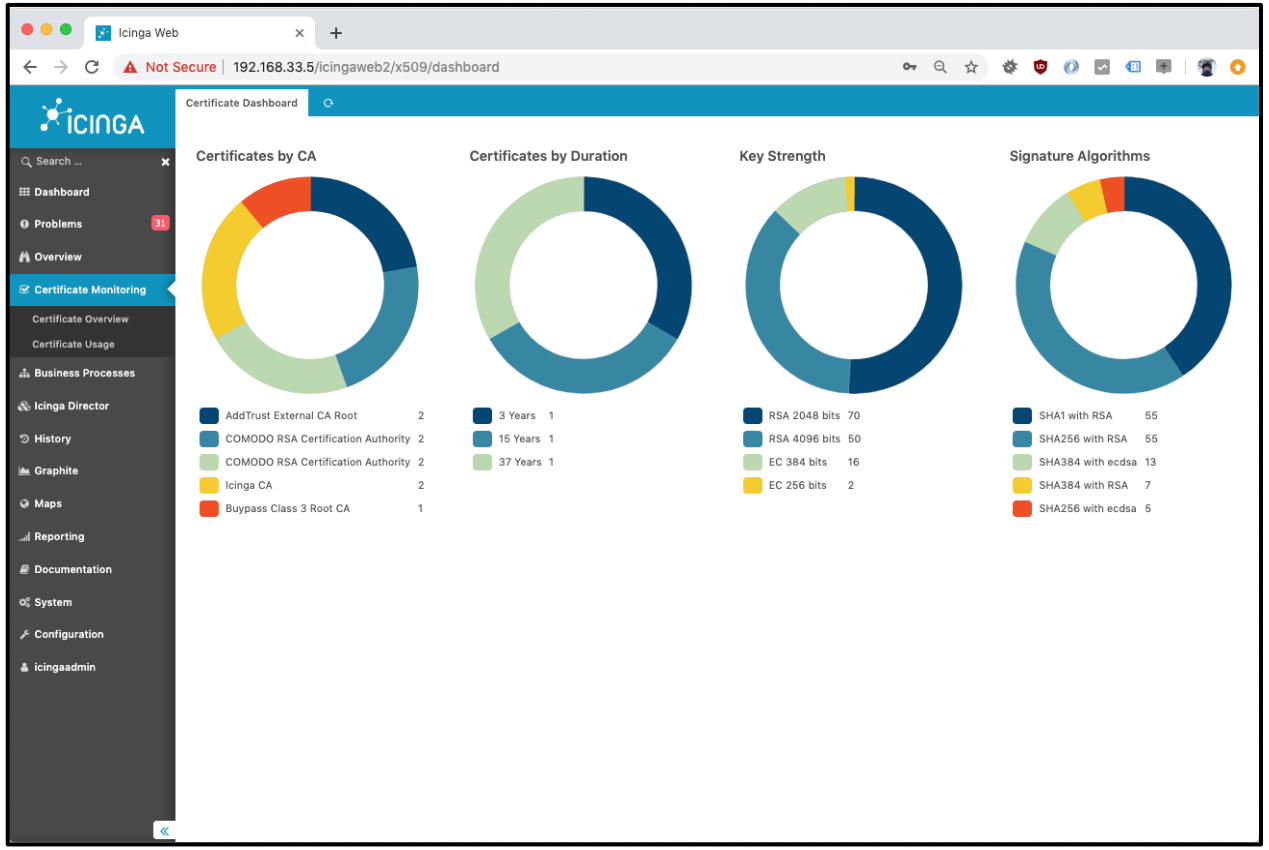
Nagios là một phần mềm mã nguồn mở dùng cho việc giám sát hệ thống mạng. Phần mềm thực hiện theo dõi và đưa ra các cảnh báo về trạng thái của các thiết bị, các máy chủ và các dịch vụ thông qua các Agent cũng như giao thức mạng SNMP.

Phần mềm cung cấp phiên bản miễn phí chạy trên hệ điều hành Linux, phần mềm hỗ trợ rất nhiều chức năng hữu ích cho người quản trị mạng. Tuy nhiên việc cài đặt, cấu hình phần mềm khá phức tạp. Giao diện sử dụng chưa được thân thiện.

5.5. Một số phần mềm hệ thống giám sát

Hệ thống giám sát nguồn mở

Phần mềm Incinga



Website tham khảo và thông tin thêm:

https://www.icinga.com

5.5. Một số phần mềm hệ thống giám sát

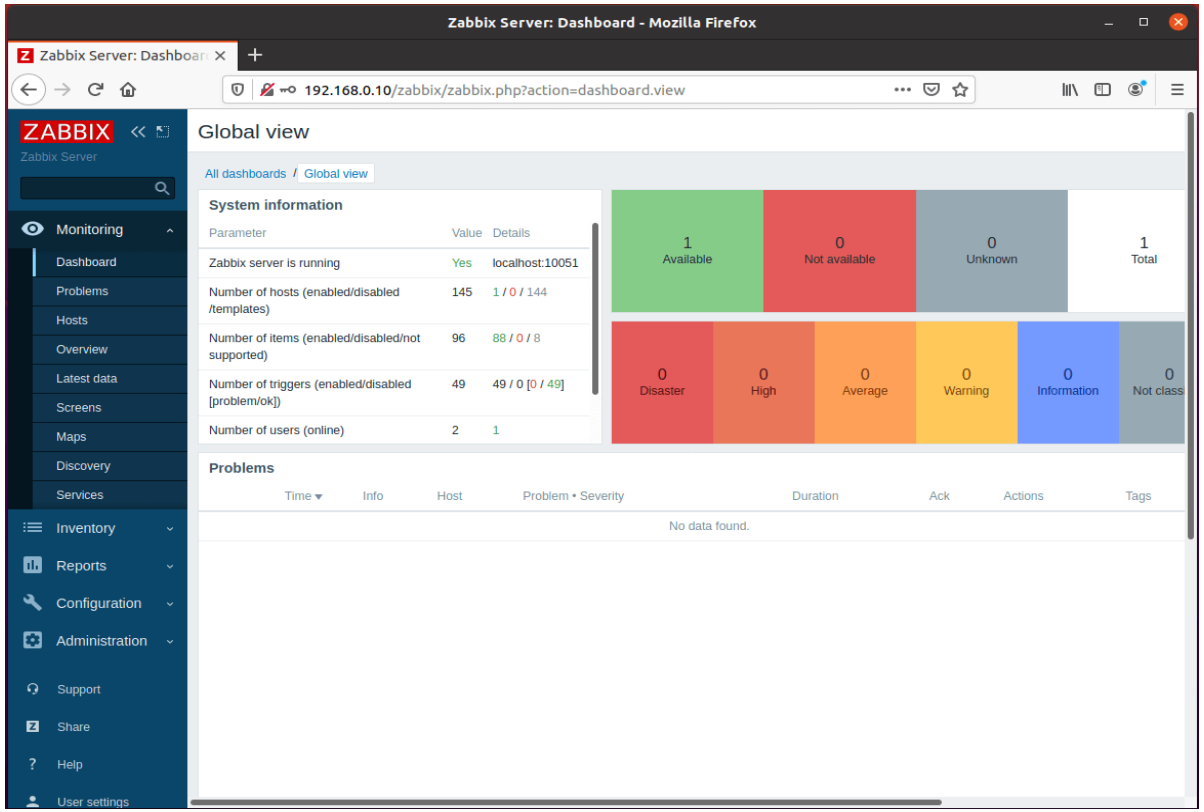
Icinga được phát triển vào năm 2009 bởi cùng một nhóm các nhà phát triển Nagios. Nó là một công cụ rất dễ sử dụng và linh hoạt cho các mạng SMB và doanh nghiệp. Phần mềm tập trung mạnh vào cơ sở hạ tầng và dịch vụ giám sát. Công cụ này cũng bao gồm phân tích ngưỡng tuyệt vời và các chức năng báo cáo / cảnh báo.

Icinga cung cấp các báo cáo và thay đổi về tình trạng chung của cơ sở hạ tầng CNTT của bạn.

5.5. Một số phần mềm hệ thống giám sát

Hệ thống giám sát nguồn mở

Phần mềm Zabbix



Website tham khảo và thông tin thêm :
https://www.zabbix.com/

5.5. Một số phần mềm hệ thống giám sát

Zabbix được sáng lập bởi Alexei Vladishev, hiện tại được hỗ trợ và phát triển bởi Zabbix SIA. Zabbix là công cụ mã nguồn mở giải quyết vấn đề giám sát. Zabbix là phần mềm liệt kê các tham số của một mạng, tình trạng và tính toàn vẹn của server, router, switch... Zabbix sử dụng một cơ chế thông báo linh hoạt các thông tin của các thành phần mạng cho phép người dùng cấu hình cảnh báo qua email, tin nhắn

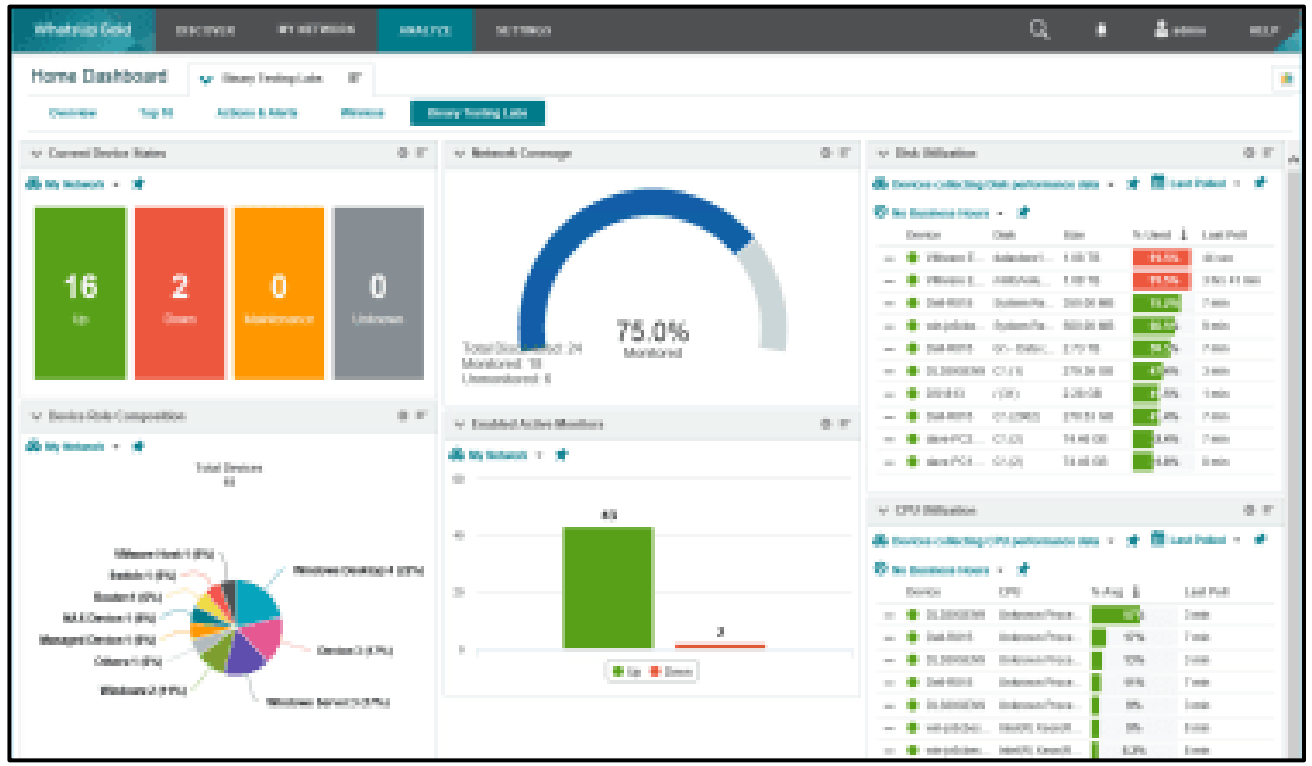
5.5. Một số phần mềm hệ thống giám sát

Hệ thống giám sát thương mại

Phần mềm giám sát mạng WhatsUp Gold (WUG)

Website tham khảo và thông tin thêm:

https://www.ipswitch.com/application-and-network monitoring/whatsup-gold



5.5. Một số phần mềm hệ thống giám sát

WhatsUp Gold (WUG) là một phần mềm giám sát mạng nổi tiếng của Ipswitch. Nó là một trong những phần mềm giám sát mạng dễ sử dụng nhất. Các bảng điều khiển thân thiện với người dùng và hấp dẫn trực quan.

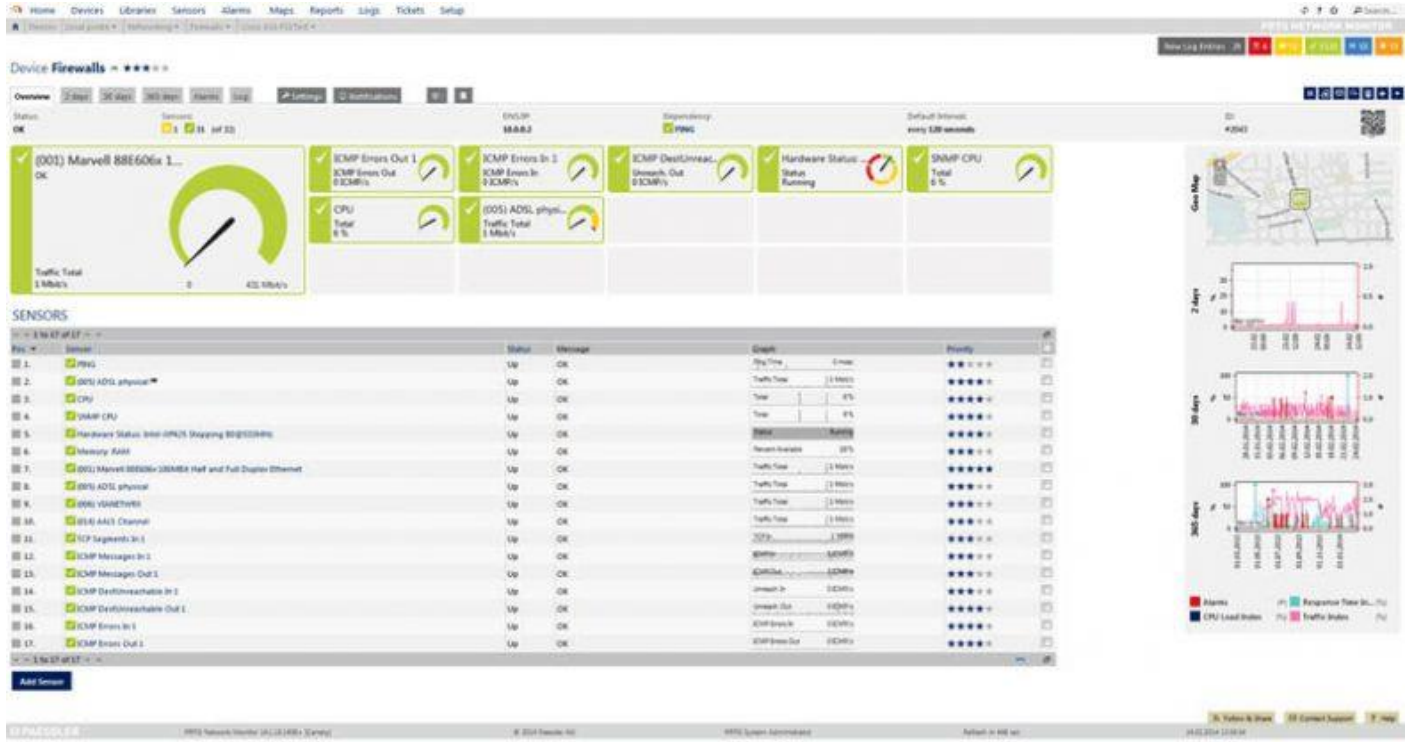
Các điểm nổi bật của phiên bản mới nhất là giám sát đám mây kết hợp, giám sát hiệu suất thời gian thực, chuyển đổi dự phòng tự động và thủ công và mở rộng khả năng hiển thị cho các mạng phân tán.

WhatsUp Gold là phần mềm thương mại, chỉ được hỗ trợ trên hệ điều hành Windows.

5.5. Một số phần mềm hệ thống giám sát

Hệ thống giám sát thương mại

Phần mềm giám sát mạng PRTG



Website tham khảo và thông tin thêm:

https://www.paessler.com/prtg

5.5. Một số phần mềm hệ thống giám sát

Phần mềm PRTG Network Monitor thường được biết đến với khả năng quản lý cơ sở hạ tầng tiên tiến. Tất cả các thiết bị, hệ thống, lưu lượng truy cập và ứng dụng trong mạng của bạn có thể dễ dàng hiển thị trong chế độ xem phân cấp tóm tắt hiệu suất và cảnh báo. PRTG giám sát cơ sở hạ tầng CNTT sử dụng công nghệ như SNMP, WMI, SSH, Flows / Packet Sniffing, HTTP request, REST APIs, Pings, SQL và nhiều hơn nữa.

Đây là một trong những lựa chọn tốt nhất cho các tổ chức có kinh nghiệm giám sát mạng thấp. Giao diện người dùng thực sự mạnh mẽ và rất dễ sử dụng.

CÁC KHÁI NIỆM CƠ BẢN VỀ QUẢN TRỊ MẠNG

Q & A