

Contents

LỜI CẢM ƠN	4
LỜI NÓI ĐẦU	5
CHƯƠNG 1: MỞ ĐẦU	6
1.1 Lý do chọn đề tài :	6
1.2 Mục tiêu đề tài:.....	7
1.3 Nội dung đề tài:	7
CHƯƠNG 2: HỆ THỐNG GIÁM SÁT MẠNG	8
2.1 Giám sát mạng là gì?	8
2.2 Giám sát mạng quan trọng như thế nào?	9
2.3 Giám sát mạng có thể giám sát gì?.....	9
2.4 Hệ thống giám sát mạng có thể giám sát những loại mạng nào?	10
2.5 Hệ thống giám sát mạng có thể làm nhiệm vụ chiến lược gì?	10
2.6 Giám sát mạng có thể trả lời những câu hỏi gì?.....	11
2.7 Giám sát mạng có thể làm gì cho chúng ta?	11
2.8 Hệ thống giám sát mạng có những công cụ gì?	12
2.9 Những loại hệ thống giám sát mạng có giá trị?	12
2.10 Chi phí cho chúng là gì?	14
CHƯƠNG 3: TÌM HIỂU PHẦN MỀM ZABBIX.....	16
3.1 Giới thiệu về Zabbix:	16
3.1.1 Zabbix là gì:.....	16
3.1.2 Ưu điểm của Zabbix:	16
3.1.3 Tại sao sử dụng Zabbix:	17
3.1.4 Đối tượng sử dụng Zabbix:	17

3.2 Cài đặt Zabbix:	17
3.2.1 Yêu cầu:	17
3.2.1.1 Yêu cầu phần cứng:	17
3.1.1.1 Yêu cầu phần mềm:	18
3.2.2 Thành phần của hệ thống giám sát Zabbix:	18
3.2.2.1.1 Zabbix server:	18
3.2.2.1.2 Zabbix proxy:	18
3.2.2.1.3 Zabbix agent:	19
3.2.2.1.4 Web interface:	19
3.2.3 Cấu trúc của Zabbix:	21
3.2.4 Cài đặt:	21
3.2.4.1 Zabbix Server:	21
3.2.4.2 Zabbix Proxy:	26
3.2.4.3 Zabbix Agent:	29
3.2.4.4 Cài đặt Web Zabbix:	32
3.3 Giới thiệu giao diện web zabbix:	37
3.3.1 Dashboard:	37
3.3.2 Latest data:	38
3.3.3 Triggers:	39
3.3.4 Events:	40
3.3.5 Graphs:	41
Thông tin giám sát được biểu diễn dưới dạng biểu đồ	41
3.3.6 Media types:	42
CHƯƠNG 4: THỰC NGHIỆM.....	43
4.1 Mô hình thực nghiệm:	43

4.2 Mô tả, yêu cầu:	44
4.3 Cấu hình:	44
4.3.1 Cấu hình máy Windows server:	44
4.3.2 Cấu hình máy Linux server:.....	45
4.3.3 Cấu hình máy Zabbix server:	45
4.4 Kết quả:	49
4.4.1 Máy Zabbix server:	50
4.4.2 Máy Windows server:.....	52
4.4.3 Máy Linux server:	53
CHƯƠNG 5: KẾT LUẬN.....	54
5.1 Kết quả đạt được:	54
5.2 Ưu điểm – khuyết điểm:	54
5.3 Hướng phát triển:	54
5.4 Khó khăn:	55

LỜI CẢM ƠN

Trước tiên em xin gửi lời cảm ơn chân thành tới Thầy Huỳnh Nguyên Chính, đã trực tiếp hướng dẫn và tận tình chỉ bảo, truyền đạt kinh nghiệm giúp nhóm hoàn thành đề tài.

Trong suốt quá trình thực hiện đề tài, nhóm đã nhận được rất nhiều sự hỗ trợ, giúp đỡ từ phía nhà trường và các thầy cô.

Cuối cùng, nhóm xin cảm ơn tất cả các bạn sinh viên trong lớp đã giúp nhóm trong những buổi trao đổi về các ý tưởng cũng như công nghệ để phát triển đề tài.

TP. Hồ Chí Minh, ngày ... tháng 06 năm 2010

LỜI NÓI ĐẦU

Trong vai trò là người quản trị hệ thống hay là một chuyên gia bảo mật thông tin thì công tác giám sát luôn là một việc cần thiết. Giám sát mạng cho chúng ta biết được tình trạng băng thông được sử dụng trên mạng, xác định được người dùng nào đang chạy các ứng dụng chia sẻ file, hoặc có virus/ trojan nào đang âm thầm hoạt động trên mạng hay không.

Có rất nhiều công cụ có thể dùng cho quá trình giám sát mạng và Zabbix cũng nằm trong số các công cụ đó.

Mục tiêu của đê tài là tìm hiểu về Hệ thống giám sát mạng và phát triển ứng dụng sử dụng phần mềm nguồn mở Zabbix. Nhưng cho đến nay, phần mềm Zabbix chưa được ứng dụng rộng rãi tại Việt nam. Chính vì thế nhóm muốn nghiên cứu phần mềm Zabbix để góp phần khai thác và phát triển phần mềm mã nguồn mở tại Việt Nam.

CHƯƠNG 1: MỞ ĐẦU

1.1 Lý do chọn đề tài :

Ngày nay do tốc độ phát triển như vũ bão của các ngành khoa học kỹ thuật, đặc biệt là sự bùng nổ trong lĩnh vực công nghệ thông tin làm cho số lượng tri thức nhân loại tăng lên một cách “chóng mặt”, cùng với việc Việt Nam chính thức là thành viên của tổ chức thương mại thế giới WTO. Nền kinh tế tài chính ngày càng phát triển khởi sắc, đồng nghĩa với việc dữ liệu thông tin vô cùng quan trọng, quyết định đến sự sống còn của doanh nghiệp. Chính vì thế quan niệm về bảo mật an ninh mạng ngày được quan tâm hơn. Giám sát an ninh mạng chính là phương thức giúp chúng ta có thể thực hiện việc này một cách tối ưu nhất.

Một trong những công việc cơ bản của người quản trị là giám sát mạng. Giám sát mạng là kiểm tra máy tính, hệ thống, dịch vụ.... Điều này làm cho việc quản trị hệ thống mạng máy tính càng được ổn định và hoàn thiện hơn.

Bạn sẽ không bao giờ biết khi nguồn cung cấp điện bị cháy hoàn toàn, hoặc là khi máy chủ bị sụp đổ, băng thông mạng kẹt, một router bị ngưng hoạt động, khi mạng LAN của bạn bị tấn công, và còn nhiều vấn đề nữa. Bạn sẽ không bao giờ biết những thứ này khi nào xảy ra, nhưng bạn có thể chuẩn bị cho những tình huống như vậy. Hiệu quả của giám sát mạng giúp bạn đối phó với tình huống như vậy và giảm thời gian xuống. Nó cũng sẽ cho biết thông tin định kỳ của mạng, nó sẽ tạo cho bạn những file tổng quan và biểu diễn những biểu đồ về hiệu suất của hệ thống và khả năng phản ứng với những thông tin như thế, bạn có thể tối ưu cơ sở hạ tầng mạng và hiệu suất.

Để làm việc này hiệu quả, ISO (International Organization for Standardization) đã thiết kế mô hình gọi là FCAPS để hỗ trợ hiểu biết về các chức năng chính trong hệ thống quản lý mạng:

- Quản lý lỗi

- Quản lý cấu hình
- Quản lý tài khoản
- Quản lý thực hiện
- Quản lý bảo mật

Bằng việc thực hiện phần mềm giám sát mạng, hệ thống quản lý có thể thu thập đủ dữ liệu và báo cáo định kỳ, nó giúp chúng ta quản lý mạch lạc và dễ dàng. Có một số phần mềm thương mại cũng như phần mềm mã nguồn mở để giám sát mạng rất mạnh cùng với những công cụ hỗ trợ như là Nagios,Cacti.... Zabbix cũng thuộc nhóm những công cụ này, tuy không phổ biến rộng rãi bằng Nagios và Cacti nhưng Zabbix cũng là một trong những công cụ giám sát mạng khá mạnh.

1.2 Mục tiêu đề tài:

Mục tiêu nghiên cứu của đề tài này bao gồm các điểm sau:

- Tìm hiểu hệ thống giám sát mạng.
- Tìm hiểu về phần mềm nguồn mở Zabbix.
- Cài đặt và sử dụng Zabbix giám sát hệ thống mạng.

1.3 Nội dung đề tài:

Để hoàn thành được mục tiêu, nhóm tập trung nghiên cứu các nội dung sau:

- Nghiên cứu vai trò của hệ thống giám sát mạng
- Nghiên cứu về các giao thức, phần mềm hỗ trợ giám sát mạng.
- Nghiên cứu về hệ thống giám sát mạng sử dụng phần mềm nguồn mở Zabbix.

CHƯƠNG 2: HỆ THỐNG GIÁM SÁT MẠNG

2.1 Giám sát mạng là gì?

Giám sát mạng cho mạng của một công ty là một chức năng quan trọng, nó có thể tiết kiệm tiền thông qua việc làm tăng hiệu quả của mạng lưới, năng suất nhân viên và chi phí cơ sở hạ tầng. Một hệ thống giám sát mạng giám sát cho nhiều vấn đề. Nó có thể tìm và giúp đỡ giải quyết việc tải trang web snail-paced, mất mát email, hoạt động của người truy vấn và truyền tải file, nguyên nhân do quá tải, sự cố server, kết nối mạng delay hoặc các thiết bị khác.

Các hệ thống giám sát mạng (NMSs) thì khác với các hệ thống phát hiện xâm nhập (IDSs) hoặc các hệ thống phòng chống xâm nhập (IPSs). Những hệ thống khác phát hiện break-ins và ngăn chặn người dùng trái phép. Tập chung của NMS không phải cho vấn đề an ninh cho mỗi lần đăng nhập.

Giám sát mạng có thể đạt được bằng cách sử dụng phần mềm khác nhau hoặc kết hợp giữa các plug và play, thiết bị phần cứng và giải pháp phần mềm. Hầu hết bất kì loại mạng nào cũng có thể được giám sát. Nó không quan trọng là có dây hay không có dây, một mạng LAN công ty, VPN hoặc dịch vụ cung cấp WAN. Bạn có thể giám sát thiết bị trên các hệ điều hành khác nhau với vô số chức năng , từ BlackBerrys và điện thoại di động, tới servers, routers và switches. Những hệ thống này có thể giúp bạn xác định các hoạt động cụ thể và số liệu hiệu xuất, đưa ra kết quả cho phép doanh nghiệp giải quyết các yêu cầu khác nhau, đưa ra các mối đe dọa an ninh nội bộ và cung cấp nhiều hiển thị hoạt động hơn.

Việc quyết định dùng cái gì để giám sát mạng thì rất quan trọng. Bạn phải chắc rằng cấu trúc sơ đồ mạng của công ty bạn thì luôn cập nhật. Đó là bản đồ chính xác để đưa ra các loại mạng khác nhau nhằm đáp ứng việc giám sát, server đang chạy trên hệ điều hành nào, có bao nhiêu máy tính để bàn và có bao nhiêu thiết bị từ xa có thể truy cập cho mỗi

mạng. Trả lời cho các câu hỏi trên sẽ làm cho việc lựa chọn công cụ giám sát trở nên đơn giản hơn.

2.2 Giám sát mạng quan trọng như thế nào?

Bạn có thể nghĩ rằng nếu mạng đưa ra và chạy, không có lý do để gây rối với nó. Tại sao bạn lại quan tâm về việc thêm một dự án cho các nhà quản lý mạng của bạn. Lý do để khẳng định việc giám sát mạng là nhằm duy trì sức khỏe của mạng lưới, đảm bảo sẵn sàng và cải thiện hiệu suất. NMS cũng có thể giúp bạn xây dựng cơ sở dữ liệu thông tin quan trọng mà bạn có thể dùng để lên kế hoạch trong sự phát triển trong tương lai.

Giám sát mạng giống như sự viếng thăm của chuyên gia tim mạch. Nếu bác sĩ của bạn đang theo dõi dấu hiệu nguy hiểm như chảy máu qua các mạch, van và buồng của tim, thì hệ thống giám sát mạng của bạn đang theo dõi dữ liệu chuyên qua dây cáp thông qua server, switches, các kết nối và routers.

Dĩ nhiên, giám sát mạng ở các công ty không giải quyết cho ảnh chụp nhanh hàng năm của hiệu năng hệ thống. Họ không chỉ theo dõi sau khi xuất hiện các triệu chứng đáng lo ngại. Họ giám sát mạng của họ 24 giờ một ngày và mỗi ngày.

2.3 Giám sát mạng có thể giám sát gì?

Người ta dùng hệ thống giám sát mạng thường để kiểm tra băng thông sử dụng, kiểm tra hiệu suất của ứng dụng và hiệu suất của máy chủ.

Giám sát lưu lượng là nhiệm vụ cơ bản, một trong những việc xây dựng hệ thống mạng và duy trì các nhiệm vụ cơ bản. Nó thường tập chung vào các vấn đề hỗ trợ người dùng nội bộ. Vì vậy hệ thống giám sát mạng tiến hóa để giám sát các loại thiết bị như:

- BlackBerrys
- Cell phones
- Servers and desktops
- Routers
- Switches

Một số hệ thống mạng đi kèm với việc phát hiện tự động, khả năng ghi lại thiết bị liên tục khi chúng được thêm vào, gỡ bỏ hoặc trải qua những thay đổi cấu hình. Những công cụ này tách riêng các thiết bị tự động:

- IP address
- Service
- Type (switch, router, etc.)
- Physical location

Ngoài những lợi thế hiển nhiên của việc biết chính xác và thực tế những gì bạn đã khai triển, hệ thống giám sát mạng còn có thể tự động phát hiện và phân loại công đoạn, giúp bạn có kế hoạch phát triển.

2.4 Hệ thống giám sát mạng có thể giám sát những loại mạng nào?

Hệ thống giám sát mạng có thể giám sát các mạng có kích thước lớn, nhỏ, trung bình. Một số loại mạng như là:

- Wireless or wired
- Lan
- VPN
- WAN

Thị trường kinh doanh luôn đòi hỏi các chức năng trang web mới để sử dụng nội bộ và bên ngoài. Hiệu suất các chức năng nhạy cảm (hay còn gọi là băng thông) bao gồm tiếng nói qua IP (VoIP), Internet Protocol TV (IPTV) và video theo yêu cầu (VOD). Giám sát cho phép các nhà quản lý phân bổ nguồn lực để duy trì tính toàn vẹn của hệ thống.

2.5 Hệ thống giám sát mạng có thể làm nhiệm vụ chiến lược gì?

Một hệ thống giám sát (NMS) sẽ giúp định hướng trong môi trường phức tạp, đưa ra các báo cáo, người quản lý có thể sử dụng các báo cáo này để:

- Xác nhận việc tuân thủ quy định và chính sách
- Tiết kiệm chi phí tiềm lực bằng cách tìm nguồn dữ liệu dư thừa.
- Giải quyết hiệu quả việc bị lây cắp thông tin

- Trợ giúp xác định năng suất của nhân viên
- Spot quá tải thiết bị trước khi nó có thể mang xuống một mạng lưới
- Xác định liên kết mạng diện rộng yếu và thắt cổ chai
- Do độ trễ, hoặc do chuyển tải dữ liệu bị trễ
- Tìm bất thường trong mạng nội bộ có thể cho biết một mối đe dọa an ninh.

Nhưng một NMS không phải là hệ thống phát hiện (IDS) hoặc hệ thống phòng chống (IPS). Một NMS có thể phát hiện các hành động khó chịu, nhưng đó không phải là nhiệm vụ của nó.

2.6 Giám sát mạng có thể trả lời những câu hỏi gì?

Một báo cáo giám sát sẽ giúp bạn trả lời câu hỏi khó khăn:

- Giúp các nhà thiết làm đơn giản hóa và đồng nhất hệ thống với chi phí thấp, giúp đưa ra quyết định thay thế các phân đoạn mạng với chi phí chấp nhận được ?
- Hệ điều hành và ứng dụng nào chạy trên server, và chúng cần thiết?
- Người sử dụng đại diện cho ai, và cái gì được họ gửi?
- Làm thế nào để gần với công suất của máy chủ?
- Thiết bị từ xa gì được sử dụng, và chúng được sử dụng gì?
- Làm thế nào và từ đâu thiết bị từ xa gia nhập vào hệ thống?
- Ai và Những nguồn gì đang quản lý hệ thống?

Dĩ nhiên, bỏ qua thông tin này và báo cáo tình trạng tốt, như thế có thể có kết luận rằng không có vấn đề gì, có nghĩa là không có lý do thay đổi mọi thứ. Đó thường là kết luận sai vì doanh nghiệp không tồn tại một trạng thái ổn định.

2.7 Giám sát mạng có thể làm gì cho chúng ta?

Giám sát mạng cẩn thận cho phép giám đốc điều hành tất cả thông tin họ cần để chứng minh việc nâng cấp mạng và mở rộng mạng là cần thiết để hỗ trợ doanh nghiệp thành công trong tương lai.

Service-level agreements(SLA) khó thực thi bên bộ phận khách hàng bởi vì nó đưa ra những điều khoản rất là khắt khe.

Hệ thống giám sát mạng làm việc hiệu quả sẽ thông cho nhà quản lý biết thiết bị, dịch vụ, hoặc ứng dụng được phép hoạt động ở mức độ nào.

2.8 Hệ thống giám sát mạng có những công cụ gì?

Bản thân những hệ thống giám sát mạng có thể là phần mềm hoặc firmware, đơn giản hay phức tạp.

Một trong những công cụ đơn giản nhất là gửi tín hiệu đến thiết bị và xem thời gian trả về là bao lâu(digital echolocation). Thích hợp hơn với hầu hết các nhà quản lý là các công cụ liên quan đến các kiểm tra thông tin thường và các kịch bản theo dõi và có thể đưa ra nhiều báo cáo đa dạng với các đồ họa, với điều kiện tổng kết từ thiết bị cụ thể trong mạng lưới rộng khắp.

Các công cụ mã nguồn mở có tính mở rộng cao, không tồn. Và chúng làm việc với hầu hết các công cụ và phù hợp với hầu hết các nền tảng.

Không có vấn đề gì đáng lo khi bạn chọn công cụ, mặc dù tích cực tìm hiểu xem chúng làm tốt như thế nào trong môi trường của bạn, đặc biệt với các hệ điều hành trên mạng của bạn.

Nếu như mạng của bạn trở nên quá phức tạp và bạn không thể kiểm soát được những gì đang xảy ra, bạn có thể theo dõi outsource. Outsourcers tạo ra các mức của dịch vụ và các gói chức năng để bao quát nhiều môi trường mạng và ngân sách.

Sản phẩm giám sát mạng có thể miễn phí hoàn toàn(như với ứng dụng mã nguồn mở) hoặc chúng cũng có thể vô cùng tốn kém.

2.9 Những loại hệ thống giám sát mạng có giá trị?

Công cụ mạng giám sát đến tất cả các khía cạnh và các mức phức tạp. Rất nhiều công cụ giao diện command (CLI) có giá trị. Một trong những cái có giá trị là ping, một công cụ khá tin cậy trong hoạt động lý thuyết "KISS". Ping để kiểm tra một máy chủ cụ thể có thể truy cập mạng qua I, nó làm việc bằng cách gửi gói ICMP echo yêu cầu tới máy chủ mục tiêu chờ phản hồi. Ping ước lượng thời gian khứ hồi trong milli giây, hồ sơ bắt kì gói tin mát mẻ và in ra một bảng tóm tắt khi hoàn tất.

Rõ ràng là rất tiện lợi cho những người không chuyên, hệ thống giám sát mạng với những biểu đồ các vấn đề quan hệ với công cụ CLI. Một sự phong phú của giải pháp giao

diện web bao gồm chi tiết và các tính năng biểu đồ có sẵn. Những công cụ này có thể dễ dàng cài đặt và sử dụng. Nhiều người đến với cấu hình trước kịch bản. Plus, các bản đồ chúng đưa ra thì rất là quan trọng khi đặt cùng với bộ giám sát đại diện cho một nút mạng quan trọng.

Công cụ mã nguồn mở luôn được ưa chuộng trong giới IT, có rất nhiều cho nhu cầu giám sát mạng. Chúng linh động và tốt hơn, tất cả hầu như là miễn phí hoặc rẻ. Ngoài ra, công cụ mã nguồn mở thì tương thích với hầu hết các công cụ hoặc nền tảng. Dữ liệu cho những công cụ mã nguồn mở hầu hết là XML. Ví dụ: một công cụ miễn phí theo GNU GPL bắt đầu như kịch bản khó diễn tả tới việc sử dụng đồ họa của một trường đại học kết nối với internet. Sau đó nó được sử dụng như là công cụ cho việc vẽ đồ họa cho các nguồn dữ liệu khác nhau như tốc độ, điện áp, nhiệt độ và số lượng bản in. Sau đó công dân mạng bắt đầu dùng phần mềm để thăm dò mạng, lấy lại MIB (Management Information Base) và SNMP (Simple Network Management Protocol), và dùng kịch bản Perl để đưa ra kết quả bằng đồ thị trên trang web. Công cụ nhanh chóng được sử dụng không chỉ công dân mạng mà nguồn mở giải pháp riêng của họ với nhau mà còn bởi các nhà cung cấp độc quyền lớn, những người vay mượn một số khả năng của công cụ để làm phong phú thêm các giải pháp riêng của họ.

Nếu bạn đang ở nơi buôn bán thiết bị mới, các hàng sản xuất thiết bị mạng đã cung cấp rất chi tiết thông tin cho thiết bị của họ, cộng thêm trị giá để mua. Việc của bạn là phải kiểm tra tính tương thích của công cụ, đặc biệt là với hệ điều hành trên mạng của bạn, xác định rõ độ hữu ích của công cụ cho kế hoạch tổng thể của bạn. Cuối cùng là giá cả. Ví dụ: bạn không muốn thấy bạn trong hoàn cảnh, nơi bạn mua server mới với công cụ giám sát cho một khu vực và công cụ giám sát không chạy tốt với sever của bạn, không hỗ trợ hệ điều hành.

Nếu bạn có nhiều thiết bị khác nhau, với khả năng làm việc không đồng đều và một đường cong học hỏi rộng lớn. Có những ứng dụng giám sát trên thị trường có thể kết hợp lại và làm đơn giản việc quản lý giám sát mạng lại. Họ làm được điều này bằng cách quản lý lưu lượng đến các công cụ riêng, cho dù chúng là thiết bị hay ứng dụng. Các thiết bị cung cấp ứng dụng cân bằng tải trên các mạng con khác nhau. Theo lý thuyết, quy

trình này làm linh hoạt hơn và giảm bớt nghẽn tắc mạng gây ra bởi giám sát, làm chậm đường truyền kiểm tra nó. Đường cong học tập cũng giảm đi.

Mạng trở nên phức tạp, vì thế phải dùng hệ thống giám sát. Hội tụ, hoặc "triple play" mạng, kết hợp voice, video và truyền dữ liệu tốc độ cao qua một ống duy nhất. Những điều này cần quản lý và giám sát hiệu quả. Những loại mạng loại này cần hệ thống khảo sát rung động của mỗi gói, độ trễ và mất gói tin, và đó là dành cho người mới bắt đầu. Cách quản lý mạng truyền thống-sử dụng SNMP agents để thăm dò các thiết bị mỗi lần cách nhau 5 giây để xác định liệu mạng lưới có vấn đề. Có nhiều giải pháp có giá trị để giải quyết nhiều nhiệm vụ như hoạt động không an toàn trong khi mất nguồn, cung cấp hỗ trợ cho switch ports và VLANs, và chính xác giống như một màn hình LCD để khắc phục sự cố.

Nếu mạng của bạn trở lên quá phức tạp và bạn không thể kiểm soát những gì đang xảy ra, Những người khác có thể làm cho bạn. Có những công ty mà bạn có thể thuê để giám sát, quản lý, phân tích. Ví dụ, một dịch vụ cung cấp ở châu âu cung cấp các module khác nhau tới khách hàng mạng và các công ty sử dụng cả ba mạng. Một module của dịch vụ bao gồm thông tin của khách hàng trong một khoảng thời gian xác định, và đưa ra báo cáo hiệu xuất giao thông và ứng dụng. Một module khác lấy các thông tin và đưa ra khuyến nghị để cải thiện mạng hiệu quả. Module thứ 3 theo dõi liên tục, báo cáo, và hiệu suất báo cáo.

2.10 Chi phí cho chúng là gì?

Giải pháp giám sát mạng có thể hoàn toàn miễn phí hoặc rất tốn kém. Hầu hết các công cụ mã nguồn mở là miễn phí, như những công cụ có thể được mua kèm với cơ sở hạ tầng. Ứng dụng, phần mềm-giải pháp và các dịch vụ chỉ giao động trong khoảng từ 50 đô la đến hàng ngàn đô la.

Với các nhà cung cấp dịch vụ, bạn có thể tùy chọn trong danh mục các dịch vụ giám sát; có thể tiết kiệm thông qua lấy các thiết bị phát sinh phụ thuộc vào mạng. Có những trao đổi khác nhau. Mua dịch vụ có thể cung cấp cho bạn tiếp cận với công nghệ giám sát mới nhất; tương phản, lấy được thiết bị cung cấp nhiều chức năng hơn.

Một trong những điều chắc chắn khi nói đến giám sát mạng là chi phí mà bạn phải bỏ ra nếu không sử dụng những công nghệ này có thể sẽ lớn hơn bạn nghĩ rất nhiều, nếu bạn không nhận được hiệu suất và tính sẵn sàng. Bạn buộc lòng phải chịu tổn kém để chắc rằng mạng của bạn khỏe mạnh và an toàn. Giá trị của nó là công việc của bạn.

CHƯƠNG 3: TÌM HIỂU PHẦN MỀM ZABBIX

3.1 Giới thiệu về Zabbix:

3.1.1 Zabbix là gì:

Zabbix được sáng lập bởi Alexei Vladishev, và hiện tại được phát triển và hỗ trợ bởi Zabbix SIA.

Zabbix là công cụ mã nguồn mở giải quyết vấn đề giám sát. Zabbix là phần mềm các tham số của một mạng, tình trạng và tính toàn vẹn của Server. Zabbix sử dụng một cơ chế thông báo linh hoạt cho phép người dùng cấu hình e-mail 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 nên lý tưởng hơn.

Tất cả các báo cáo, thống kê cũng như các thông số cấu hình của Zabbix được truy cập thông qua giao diện web. Giao diện giúp ta theo dõi được tình trạng hệ mạng và server. Cấu hình đúng, Zabbix đóng một vai trò quan trọng trong việc theo dõi cơ sở hạ tầng công nghệ thông tin. Điều này phù hợp cho các tổ chức nhỏ có một server và các công ty lớn với nhiều server.

Zabbix được viết và phát hành với General Public License GPL phiên bản 2.

3.1.2 Ưu điểm của Zabbix:

- Tự động phát hiện server và thiết bị mạng
- Được phân phối theo dõi bởi admin
- Hỗ trợ máy chủ Linux, Solaris, HP-UX, AIX, Free BSD, Open BSD, OS X
- Hỗ trợ máy trạm Linux, Solaris, HP-UX, AIX, Free BSD, Open BSD, OS X, Tru64/OSF1, Windows NT4.0, Windows 2000, Windows 2003, Windows XP, Windows Vista.
- Đáng tin cậy trong việc chứng thực người dùng.
- Linh hoạt trong việc phân quyền người dùng
- Giao diện web
- Có thể thông báo sự cố qua email
- Có xem báo cáo, biểu đồ qua giao diện web.
- Kiểm tra theo dõi việc đăng nhập.

3.1.3 Tại sao sử dụng Zabbix:

- Mã nguồn mở.
- Hiệu quả cao đối với Unix và Win32.
- Chi phí thấp.
- Cấu hình đơn giản.
- Tất cả các thông tin (cấu hình, hiệu suất) được lưu trong cơ sở dữ liệu.
- Cài đặt dễ dàng.
- Hỗ trợ SNMP (v1, v2).
- Giao diện trực quan.

3.1.4 Đối tượng sử dụng Zabbix:

Tất cả các tổ chức lớn nhỏ trên thế giới có nhu cầu sử dụng Zabbix cho công việc giám sát.

3.2 Cài đặt Zabbix:

3.2.1 Yêu cầu:

3.2.1.1 Yêu cầu phần cứng:

Zabbix yêu cầu về tối thiểu về RAM là 128MB, 256MB không gian đĩa cứng. Tuy nhiên số lượng bộ nhớ đĩa yêu cầu phụ thuộc vào số lượng host và các thông số được giám sát.

Zabbix và các dữ liệu zabbix đặc biệt yêu cầu tài nguyên CPU đáng kể phụ thuộc vào các tham số được giám sát.

Name	Platform	CPU/Memory	Database	Monitored hosts
Small	Ubuntu Linux	PII 350MHz 256MB	MySQL MyISAM	20
Medium	Ubuntu Linux 64 bit	AMD Athlon 3200+ 2GB	MySQL InnoDB	500
Large	Ubuntu Linux 64 bit	Intel Dual Core 6400 4GB	RAID10 MySQL InnoDB or PostgreSQL	>1000
Very large	RedHat Enterprise	Intel Xeon 2xCPU 8GB	Fast RAID10 MySQL InnoDB or PostgreSQL	>10000

Hình 3.1: Yêu cầu phần cứng

3.1.1.1 Yêu cầu phần mềm:

Cần một số packet sau:

- zlib-devel
- mysql-server
- mysql-devel (for MySQL support)
- php-mysql
- php-gd
- php-bcmath
- php-mbstring
- glibc-devel
- curl-devel (for web monitoring)
- libidn-devel (curl-devel might depend on it)
- openssl-devel (curl-devel might depend on it)
- net-snmp-devel (for SNMP support)
- popt-devel (net-snmp-devel might depend on it)
- rpm-devel (net-snmp-devel might depend on it)
- OpenIPMI-devel (for IPMI support)
- libssh2-devel (for direct SSH checks)

3.2.2 Thành phần của hệ thống giám sát Zabbix:

Gồm 4 thành phần cơ bản:

3.2.2.1.1 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.

3.2.2.1.2 Zabbix proxy:

Proxy là phần tùy 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

3.2.2.1.3 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.

3.2.2.1.4 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.

3.2.3 Cấu trúc của Zabbix:

- docs: Thư mục chứa file hướng dẫn pdf
- src: Thư mục chứa tất cả source cho các tiến trình Zabbix.
- src/zabbix_server: Thư mục chứa file tạo và source cho zabbix_server.
- src/zabbix_agent: Thư mục chứa file tạo và source cho zabbix_agent và zabbix_agentd.
- src/zabbix_get: Thư mục chứa file tạo và source cho zabbix_get.
- src/zabbix_sender: Thư mục chứa file tạo và source cho zabbix_sender.
- include: Thư mục chứa các thư viện Zabbix.
- misc
 - misc/init.d: Thư mục chứa các tập lệnh khởi động trên các nền khác nhau.
- frontends
 - frontends/php: Thư mục chứa các file PHP
- create: Thư mục chứa các tập lệnh SQL để tạo cơ sở dữ liệu ban đầu.
 - create/schema: Thư mục tạo biểu đồ cơ sở dữ liệu.
- create/data: Thư mục chứa dữ liệu cho việc tạo cơ sở dữ liệu ban đầu.
- upgrades: thư mục chứa các thủ tục nâng cấp cho phiên bản khác nhau của Zabbix.

3.2.4 Cài đặt:

3.2.4.1 Zabbix Server:

Cài đặt bên máy server

Bước 1: Tạo tài khoản

User: zabbix

Password: zabbix

```
Shell> useradd zabbix
```

Bước 2: Giải nén source zabbix-1.6.tar.gz

```
shell> gunzip zabbix-1.6.tar.gz && tar -xvf zabbix-1.6.tar
```

Bước 3: Tạo cơ sở dữ liệu Zabbix

Zabbix sử dụng tập lệnh SQL để tạo ra các lược đồ cơ sở dữ liệu cần thiết và cũng có thể chèn vào một câu hình mặc định.

Đối với MySQL:

```
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
```

D

```
shell> cd create
shell> sqlplus zabbix/password
sqlplus> set def off
sqlplus> @schema/oracle.sql
sqlplus> @data/data.sql
sqlplus> @data/images_oracle.sql
sqlplus> exit
```

Đối với PostgreSQL:

```
shell> psql -U <username>
psql> create database zabbix;
psql> \q
shell> cd create/schema
shell> cat postgresql.sql | psql -U <username> zabbix
shell> cd ../data
shell> cat data.sql | psql -U <username> zabbix
shell> cat images_pgsql.sql | psql -U <username> zabbix
```

Đối với SQLite:

```
shell> cd create/schema  
shell> cat sqlite.sql | sqlite3 /var/lib/sqlite/zabbix.db  
shell> cd ../data  
shell> cat data.sql | sqlite3 /var/lib/sqlite/zabbix.db  
shell> cat images_sqlite3.sql | sqlite3 /var/lib/sqlite/zabbix.db
```

Chú ý: Cơ sở dữ liệu sẽ tự động được tạo ra nếu nó chưa tồn tại.

Bước 4: Cấu hình và biên dịch mã nguồn zabbix-1.6

Mã nguồn phải được biên dịch cho cả server (máy giám sát) cũng như client (máy được giám sát). Để cấu hình mã nguồn cho server bạn phải chỉ định cơ sở dữ liệu nào sẽ được sử dụng.

Đối với MySQL:

```
shell> ./configure --enable-server --with-mysql --with-net-snmp --with-jabber --with-libcurl
```

Đối với Oracle:

```
shell> ./configure --enable-server --with-oracle=/home/zabbix/sqlora8 --with-net-snmp --with-jabber --with-libcurl
```

Đối với PostgreSQL:

```
shell> ./configure --enable-server --with-pgsql --with-net-snmp --with-jabber --with-libcurl
```

Bước 5: Make install

```
shell> make install
```

Mặc định make install sẽ được cài đặt theo đường dẫn /usr/local/bin, /usr/local/lib, /etc. Bạn cũng có thể chỉ định đường dẫn khác với --prefix.

Bước 6: Cấu hình file /etc/service

Bước này là tùy chọn. Tuy nhiên, trên máy client nên thêm những dòng sau vào /etc/service

```
zabbix-agent    10050/tcp  Zabbix Agent
zabbix-agent    10050/udp  Zabbix Agent
zabbix-trapper  10051/tcp  Zabbix Trapper
zabbix-trapper  10051/udp  Zabbix Trapper
```

Bước 7: Cấu hình /etc/inetd.conf

Nếu bạn có kế hoạch sử dụng zabbix_agent thay cho zabbix_agentd để nghị thêm dòng sau đây:

```
zabbix_agent stream tcp nowait.3600 zabbix
/opt/zabbix/bin/zabbix_agent
```

Khởi động inetd

```
shell> killall -HUP inetd
```

Bước 8: Cấu hình file /etc/zabbix/zabbix_server.conf

```
Shell> mkdir /etc/Zabbix
Shell> cd ../..
Shell> cp misc/conf/zabbix_server.conf /etc/zabbix/
```

Đối với hệ thống nhỏ (giám sát 10 host) các thông số mặc định đã phù hợp. Tuy nhiên, bạn nên thay đổi thông số mặc định để tối đa hóa hiệu suất của Zabbix.

```
Shell> vi /etc/zabbix/zabbix_server.conf
```

```
DBName=zabbix  
DBUser=zabbix  
DBPassword=your-zabbix-mysql-password
```

Bước 9: Cấu hình /etc/zabbix/zabbix_agentd.conf

Bạn cần cấu hình file này cho tất cả các host đã cài đặt zabbix_agentd. File này có chứa địa chỉ IP của server. Các kết từ các host khác sẽ bị cấm. Bạn có thể sửa file misc/conf/zabbix_agentd.conf như sau:

```
Shell> cp misc/conf/zabbix_agentd.conf /etc/zabbix/
```

Bước 10: Cấu hình /etc/zabbix/zabbix_agentd.conf

Bạn cần cấu hình file này cho tất cả các host đã cài đặt zabbix_agent. File này có chứa địa chỉ IP của server. Các kết từ các host khác sẽ bị cấm. Bạn có thể sửa file misc/conf/zabbix_agent.conf như sau:

```
Shell> cp misc/conf/zabbix_agent.conf /etc/zabbix/
```

Bước 11: Chạy máy server

Chạy zabbix_server bằng các lệnh sau;

```
shell> cd sbin  
shell> ./zabbix_server
```

Bước 12: Chạy máy agent

Chạy zabbix_agentd cần thiết bằng các lệnh sau:

```
shell> cd bin  
shell> ./zabbix_agentd
```

3.2.4.2 Zabbix Proxy:

Bước 1: Tạo tài khoản

User: zabbix
Password: zabbix

```
Shell> useradd zabbix
```

Bước 2: Giải nén source zabbix-1.6.tar.gz

```
shell> gunzip zabbix-1.6.tar.gz && tar -xvf zabbix-1.6.tar
```

Bước 3: Tạo cơ sở dữ liệu Zabbix

Zabbix sử dụng tập lệnh SQL để tạo ra các lược đồ cơ sở dữ liệu cần thiết và cũng có thể chèn vào một cấu hình mặc định.

Đối với MySQL:

```
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
```

Đối với Oracle:

```
shell> cd create/schema  
shell> cat oracle.sql | sqlplus zabbix/password >out.log
```

Đối với PostgreSQL:

```
shell> psql -U <username>  
psql> create database zabbix;  
psql> \q  
shell> cd create/schema  
shell> cat postgresql.sql | psql -U <username> zabbix
```

Đối với SQLite:

```
shell> cd create/schema  
shell> cat sqlite.sql | sqlite3 /var/lib/sqlite/zabbix.db
```

Chú ý: Cơ sở dữ liệu sẽ tự động được tạo ra nếu nó chưa tồn tại.

Bước 4: Cấu hình và biên dịch mã nguồn zabbix-1.6

Mã nguồn phải được biên dịch cho cả server (máy giám sát) cũng như client (máy được giám sát). Để cấu hình mã nguồn cho server bạn phải chỉ định cơ sở dữ liệu nào sẽ được sử dụng.

Đối với MySQL:

```
shell> ./configure --enable-proxy --with-mysql --with-net-snmp --with-libcurl
```

Đối với Oracle:

```
shell> ./configure --enable-proxy --with-oracle=/home/zabbix/sqlora8 --with-net-snmp --with-libcurl
```

Đối với PostgreSQL:

```
shell> ./configure --enable-proxy --with-pgsql --with-net-snmp --with-libcurl
```

Bước 5: Make install

```
shell> make install
```

Mặc định make install sẽ được cài đặt theo đường dẫn /usr/local/bin, /usr/local/lib, /etc. Bạn cũng có thể chỉ định đường dẫn khác với --prefix.

Bước 6: Cấu hình file /etc/service

Bước này là tuỳ chọn. Tuy nhiên, trên máy client nên thêm những dòng sau vào /etc/service

```
zabbix_agent 10050/tcp  
zabbix_trap 10051/tcp
```

Bước 7: Cấu hình /etc/inetd.conf

Nếu bạn có kế hoạch sử dụng zabbix_agent thay cho zabbix_agentd để nghị thêm dòng sau đây:

```
zabbix_agent stream tcp nowait.3600 zabbix  
/opt/zabbix/bin/zabbix_agent
```

Khởi động inetd

```
shell> killall -HUP inetd
```

Bước 8: Cấu hình file /etc/zabbix/zabbix_proxy.conf

Đối với hệ thống nhỏ (giám sát 10 host) các thông số mặc định đã phù hợp. Tuy nhiên, bạn nên thay đổi thông số mặc định để tối đa hóa hiệu suất của Zabbix proxy. Hãy chắc chắn rằng bạn thiết lập đúng các tham số Hostname và Server. Bạn có thể xem misc/conf/zabbix_proxy.conf như ví dụ mẫu.

Bước 9: Chạy Proxy

Chạy zabbix_proxy

```
shell> cd sbin  
shell> ./zabbix_proxy
```

3.2.4.3 Zabbix Agent:

Cài đặt bên máy client.

Bước 1: Tạo tài khoản

User: zabbix
Password: zabbix

```
Shell> useradd zabbix
```

Bước 2: Giải nén source zabbix-1.6.tar.gz

```
shell> gunzip zabbix-1.6.tar.gz && tar -xvf zabbix-1.6.tar
```

Bước 3: Cấu hình và biên dịch mã nguồn zabbix-1.6

Mã nguồn phải được biên dịch cho client.

```
shell> ./configure --enable-agent
```

Bước 4: Xây dựng

```
shell> make
```

Sao chép tạo ra những chương trình từ bin/ sang /opt/zabbix/bin hoặc bất kỳ thư mục khác. Thư mục khác thường là /usr/local/bin or /usr/local/zabbix/bin.

Bước 5: Cấu hình file /etc/service

Bước này là tuỳ chọn. Tuy nhiên, trên máy client nên thêm những dòng sau vào /etc/service

```
zabbix_agent 10050/tcp  
zabbix_trap 10051/tcp
```

Bước 6: Cấu hình /etc/inetd.conf

Nếu bạn có kế hoạch sử dụng zabbix_agent thay cho zabbix_agentd để nghị thêm dòng sau đây:

```
zabbix_agent stream tcp nowait.3600 zabbix  
/opt/zabbix/bin/zabbix_agent
```

Khởi động inetd

```
shell> killall -HUP inetd
```

Bước 7: Cấu hình file /etc/zabbix/zabbix_agent.conf

Bạn cần phải cấu hình tập tin này cho mỗi máy chủ có zabbix_agent cài đặt. Các tập tin nên chứa địa chỉ IP của Zabbix server. Kết nối từ các host khác sẽ bị từ chối.

Lưu ý: trong tập tin không có ký tự kết thúc dòng.

Bạn có thể xem misc/conf/zabbix_agent.conf như ví dụ mẫu.

Bước 8: Cấu hình file /etc/zabbix/zabbix_agentd.conf

Bạn cần phải cấu hình tập tin này cho mỗi máy chủ có zabbix_agentd cài đặt. Các tập tin nên chứa địa chỉ IP của Zabbix server. Kết nối từ các host khác sẽ bị từ chối. Bạn có thể xem misc/conf/zabbix_agentd.conf như ví dụ mẫu.

Bước 9: Chạy Agent

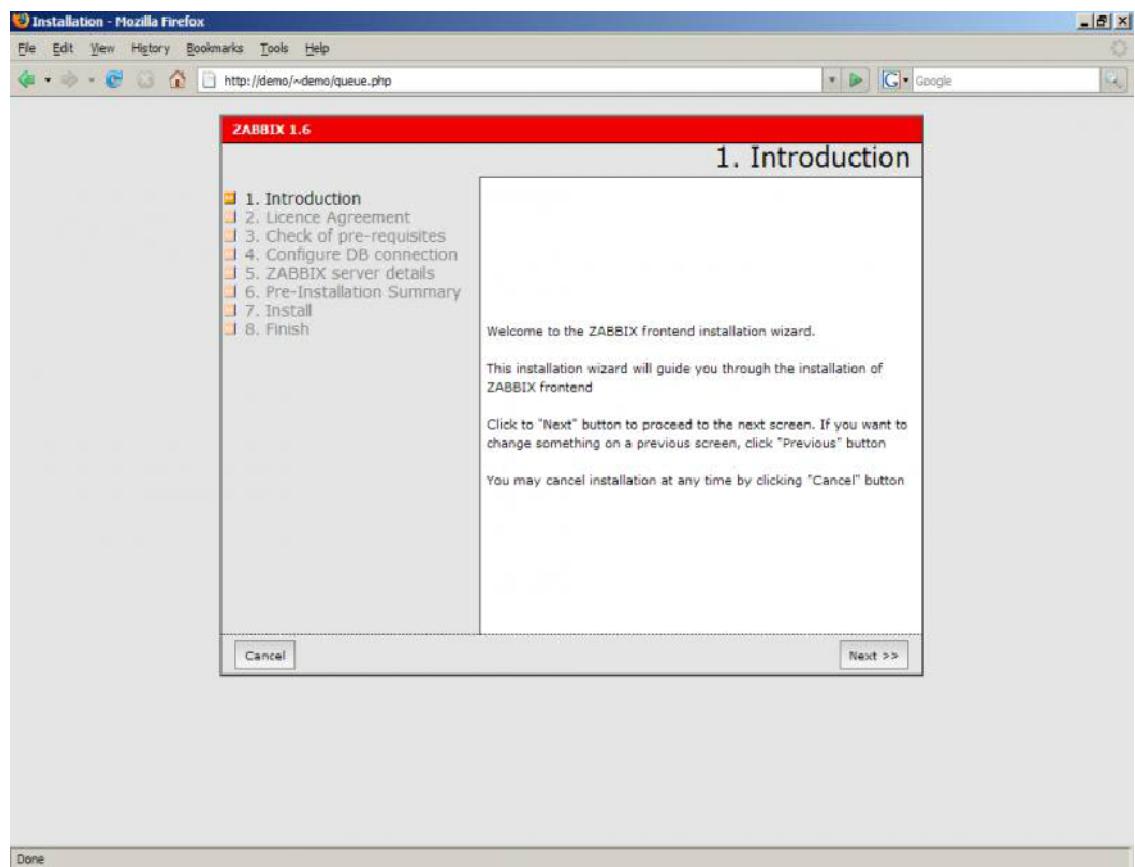
Chạy zabbix_agentd trên tất cả các máy được giám sát.

```
shell> /opt/zabbix/bin/zabbix_agentd
```

Chú ý: Bạn không nên chạy zabbix_agentd khi đã sử dụng zabbix_agent.

3.2.4.4 Cài đặt Web Zabbix:

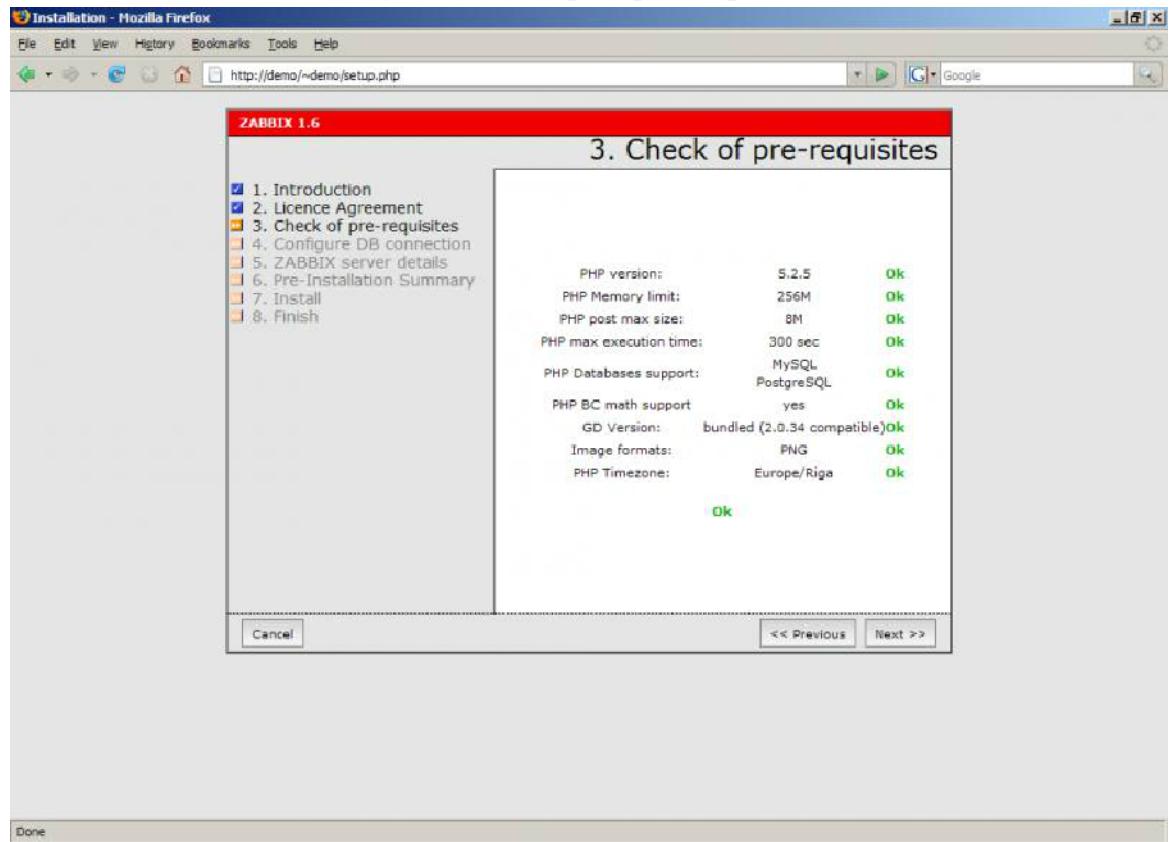
Bước 1: Truy cập đến giao diện web



Hình 3.2: Giới thiệu phần cài đặt Zabbix

Bước 2: Đóng ý phiên bản, next.

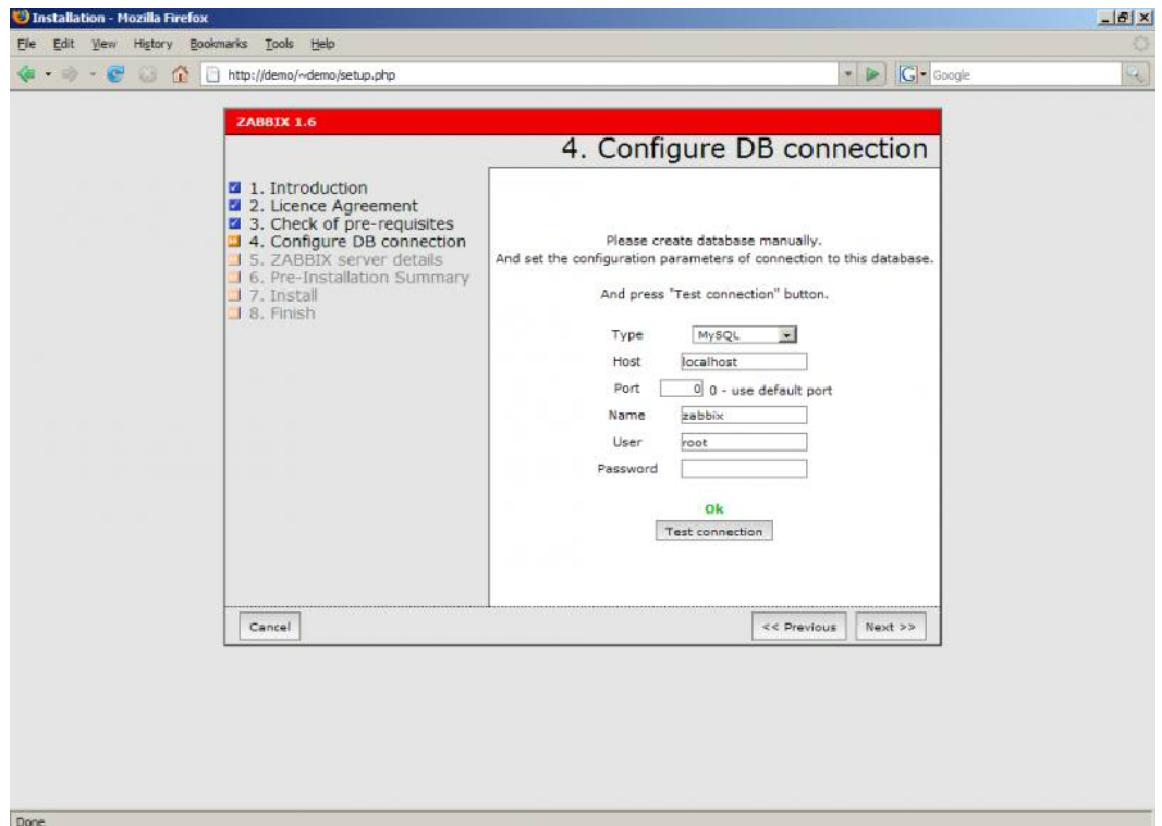
Bước 3: Hãy chắc chắn rằng các yêu cầu phải phù hợp.



Hình 3.3: Kiểm tra các yêu cầu

Pre-requisite	Minimum value	Description
PHP version	5.0	
PHP Memory limit	8MB	In php.ini: memory_limit = 128M
PHP post max size	8MB	In php.ini: post_max_size = 8M
PHP max execution time	300 seconds	In php.ini: max_execution_time = 300
PHP database support	One of: MySQL, Oracle, PostgreSQL, SQLite	One of the following modules must be installed: php-mysql, php-sqlora8, php-pgsql, php-sqlite3
PHP BC math	Any	Compiled in PHP5.
GD Version	2.0 or higher	Module php-gd.
Image formats	At least PNG	Module php-gd.

Bước 4: Cấu hình cơ sở dữ liệu. Cơ sở dữ liệu Zabbix phải tạo ra trước đó.



Hình 3.4: Cấu hình Database

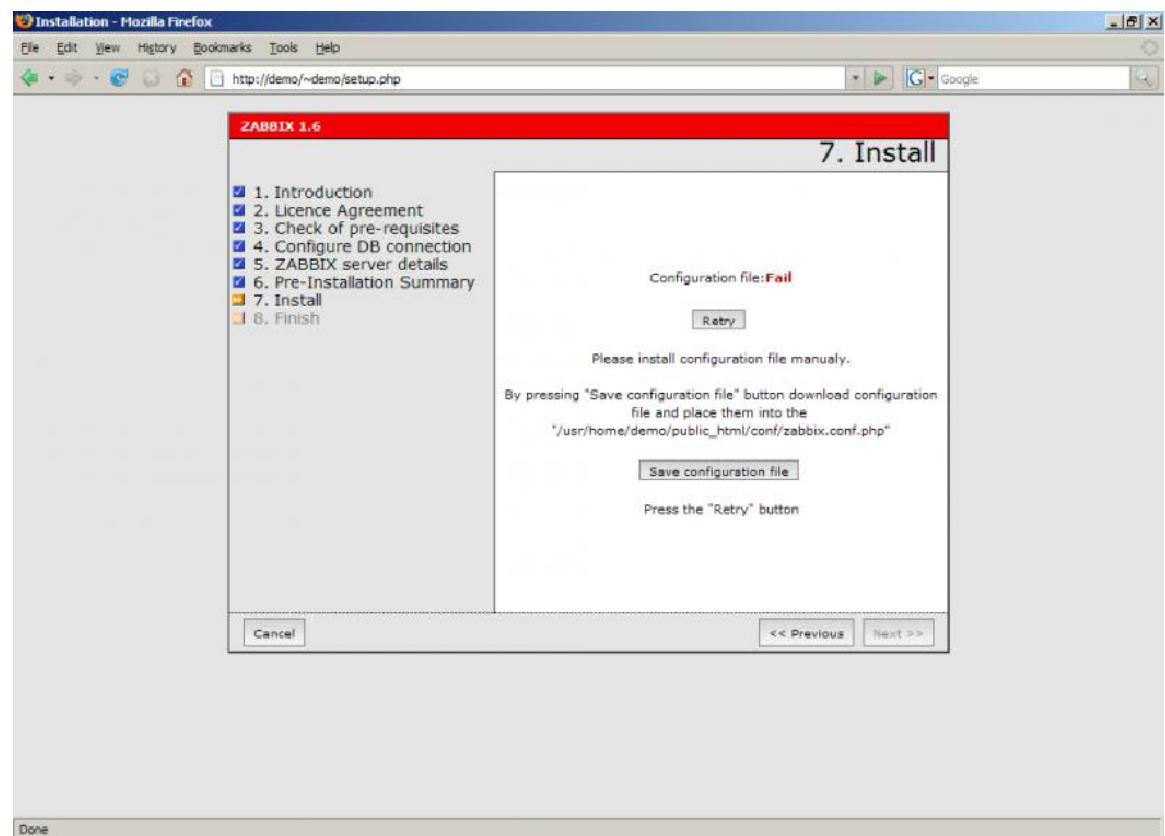
Bước 5: Thông số host và port Zabbix server

Host: localhost

Port: 10050

Bước 6: Tóm tắt thông số cấu hình Zabbix

Bước 7: Tải file cấu hình và đặt vào
/usr/home/demo/public_html/conf/zabbix.conf.php



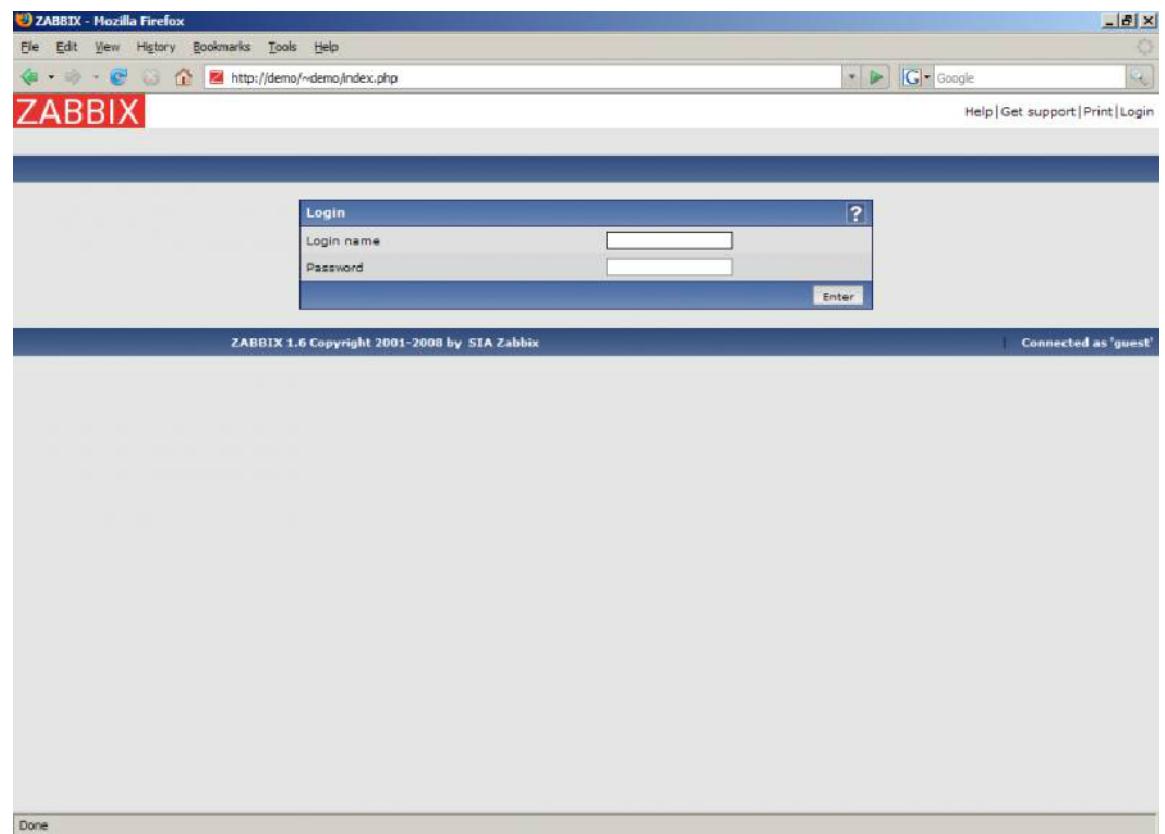
Hình 3.5: Cài đặt

Bước 8: Kết thúc

Bước 9: Đăng nhập

User: admin

Password: zabbix



Hình 3.6: Đăng nhập

3.3 Giới thiệu giao diện web zabbix:

3.3.1 Dashboard:

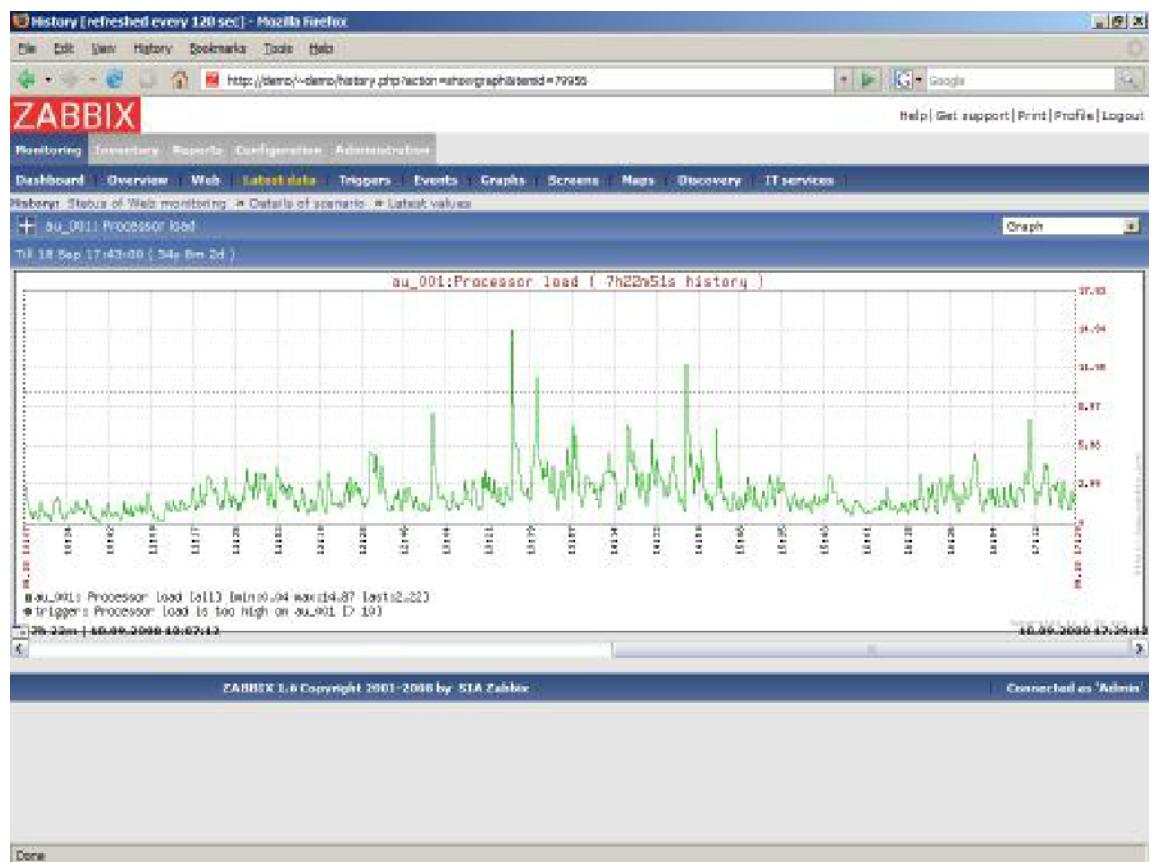
Bảng điều khiển cung cấp cho cá nhân chi tiết về giám sát môi trường.
Đây là phần trung tâm của Zabbix.

The screenshot shows the Zabbix Dashboard page. At the top, there's a navigation bar with links for Monitoring, Inventory, Reports, Configuration, Administration, Dashboard, Overview, Web, Latest data, Triggers, Events, Graphs, Screens, Maps, Discovery, IT services, Help, Get support, Print, Profile, and Logout. Below the navigation bar, the URL in the address bar is http://demo.v-demo/dashboard.php. The main content area is titled "PERSONAL DASHBOARD". It features several sections: "System status" showing parameters like "ZABBIX server is running" (Value: Yes), "Number of hosts (monitored/not monitored/templates)" (Value: 10024), "Number of items (monitored/disabled/not supported)" (Value: 100126), "Number of triggers (enabled/disabled)[true/unknown/false]" (Value: 10042), "Number of users (online)" (Value: 602), and "Required server performance, new values per second" (Value: 542.0434). Below this is a section for "Last 20 issues" with a table showing host, issue, last change, age, ack, and actions. The first row shows "ZABBIX Server" with an issue about the SMTP server being down. The final section is "Discovery status" with a table for "Discovery rule" showing "Local network" with 10 up and 0 down hosts. The bottom of the dashboard has a "Done" button.

Hình 3.7: Tab Dashboard

3.3.2 Latest data:

Chúng ta có thể kiểm tra dữ liệu đầu vào ở tab Monitoring | Latest data. Items này cho chúng ta thấy tổng thời gian của tất cả các CPU chạy trên máy tính , vì vậy hãy xem tab Monitoring | Latest data, chúng ta có thể thấy dữ liệu được trực tiếp lấy từ hệ thống.



Hình 3.8: Tab Latest data

3.3.3 Triggers:

Để kiểm tra trigger mới thêm, mở tab Monitoring | Triggers. Nếu đã được cập nhật thì ở cột Status có chữ OK màu xanh. Sẽ có 4 phút để bạn kích hoạt trigger tính từ lúc mới thêm trigger. Sau 4 phút nếu chưa kích hoạt sẽ có 3 phút báo động màu đỏ ở cột Status

Severity	Status	Last change	Host	Name	Acknowledged	Comments
Average	PROBLEM	18 May 11:13:22	ZABBIX Server	Email (SHTTP) server is down on ZABBIX Server	No	Add

Hình 3.9: Tab Triggers

3.3.4 Events:

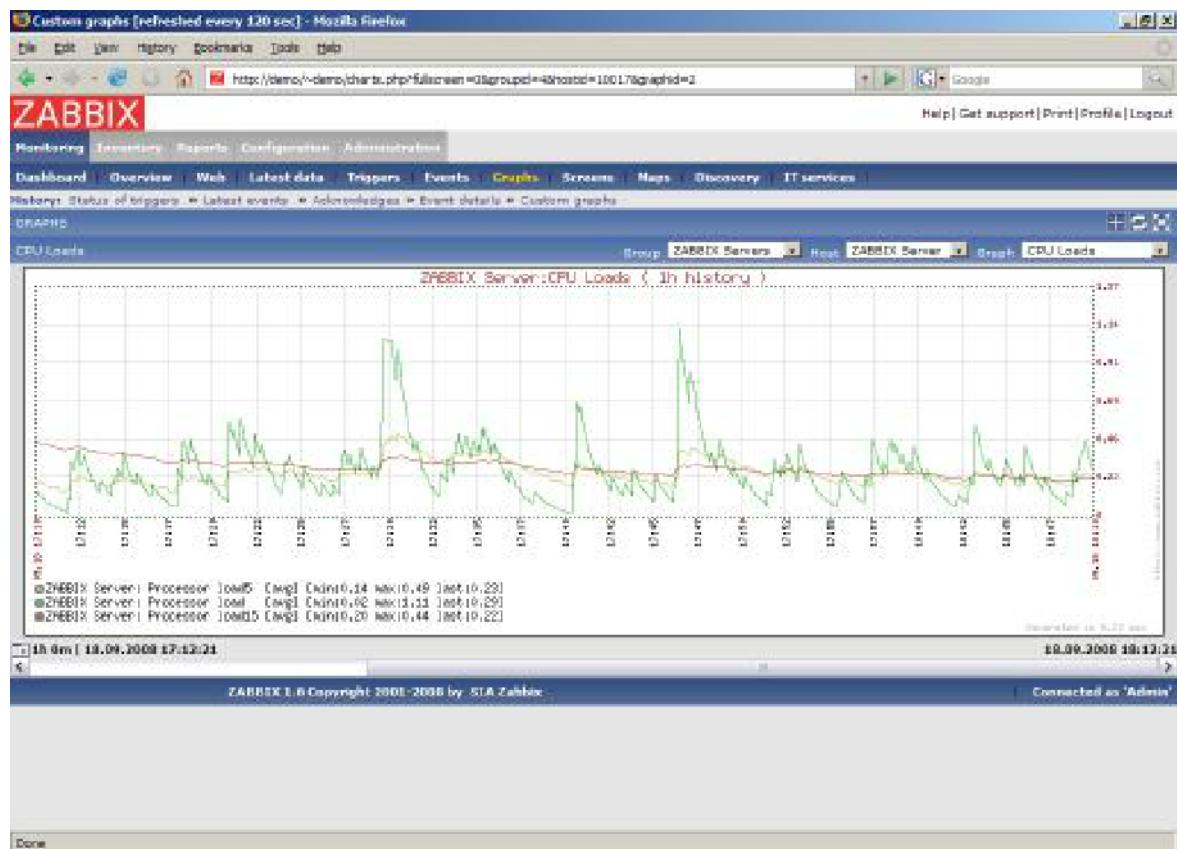
Có thể kiểm tra danh sách các sự kiện ở Tab Monitoring | Events

Time	Description	Status	Severity	Duration	Ack	Actions
2008-Sep-18 14:39:12	Processor load is too high on au_001	OK	Warning	3h 8m 49s	No	Failed
2008-Sep-18 14:39:41	Processor load is too high on au_001	PROBLEM	Warning	31s	No	Failed
2008-Sep-18 14:42:29	Processor load is too high on au_001	OK	Warning	3m 2s	No	Failed
2008-Sep-18 14:52:10	Processor load is too high on au_001	PROBLEM	Warning	29s	No	Failed
2008-Sep-18 14:48:40	Processor load is too high on au_001	OK	Warning	3m 30s	No	Failed
2008-Sep-18 14:49:15	Processor load is too high on au_001	PROBLEM	Warning	29s	No	Failed
2008-Sep-18 14:47:38	Processor load is too high on au_001	OK	Warning	37s	No	Failed
2008-Sep-18 14:46:12	Processor load is too high on au_001	PROBLEM	Warning	1m 26s	No	Failed
2008-Sep-18 14:41:11	Processor load is too high on au_001	OK	Warning	5m 1s	No	Failed
2008-Sep-18 14:40:40	Processor load is too high on au_001	PROBLEM	Warning	31s	No	Failed
2008-Sep-18 14:32:13	Processor load is too high on au_001	OK	Warning	8m 27s	No	Failed
2008-Sep-18 14:31:43	Processor load is too high on au_001	PROBLEM	Warning	30s	No	Failed
2008-Sep-18 14:34:13	Processor load is too high on au_001	OK	Warning	7m 31s	No	Failed
2008-Sep-18 14:23:41	Processor load is too high on au_001	PROBLEM	Warning	31s	No	Failed
2008-Sep-18 14:22:10	Processor load is too high on au_001	OK	Warning	1m 31s	No	Failed
2008-Sep-18 14:21:12	Processor load is too high on au_001	PROBLEM	Warning	98s	No	Failed
2008-Sep-18 14:13:43	Processor load is too high on au_001	OK	Warning	7m 29s	No	Failed
2008-Sep-18 14:13:12	Processor load is too high on au_001	PROBLEM	Warning	31s	No	Failed
2008-Sep-18 14:00:09	Processor load is too high on au_001	OK	Warning	13m 3s	No	Failed
2008-Sep-18 13:59:14	Processor load is too high on au_001	PROBLEM	Warning	58s	No	Failed

Hình 3.10: Tab Events

3.3.5 Graphs:

Thông tin giám sát được biểu diễn dưới dạng biểu đồ

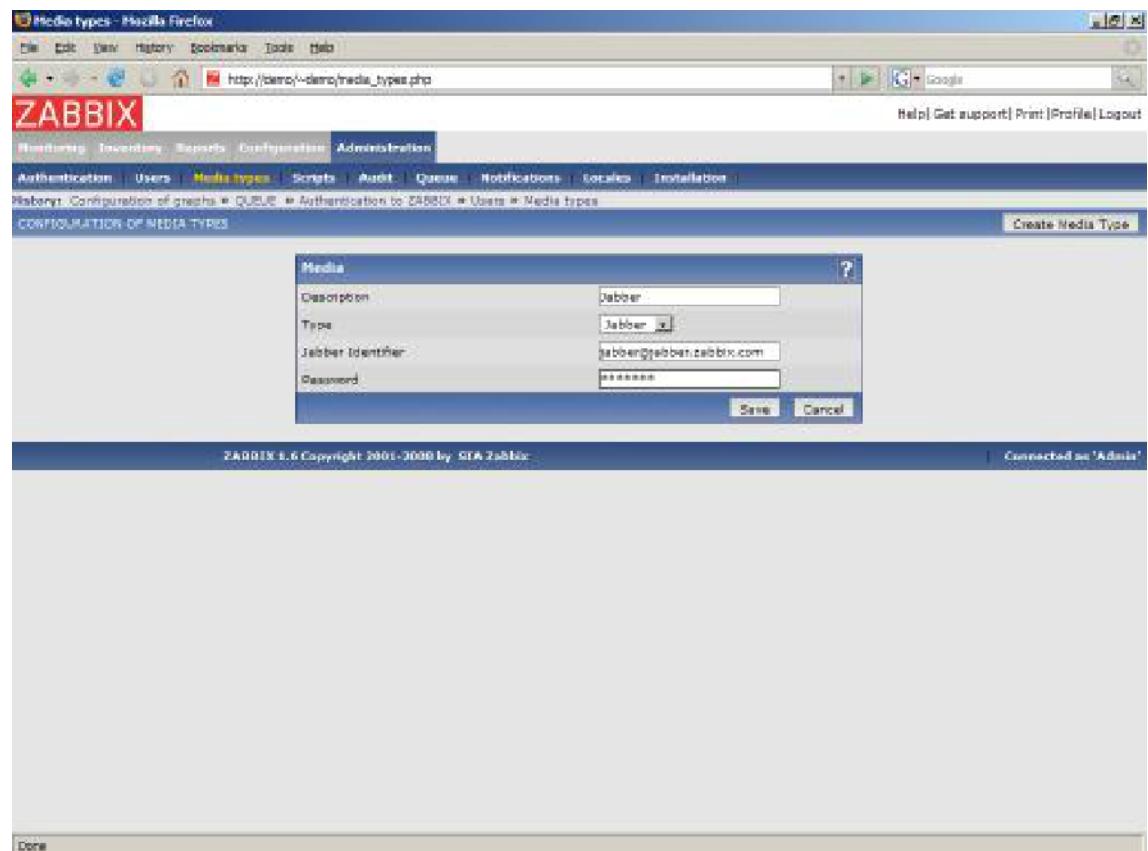


Hình 3.11: Tab Graphs

3.3.6 Media types:

Có 3 loại giúp cảnh báo với người quản trị:

- + Gửi email
- + Nhắn tin SMS đến điện thoại di động
- + Jabber

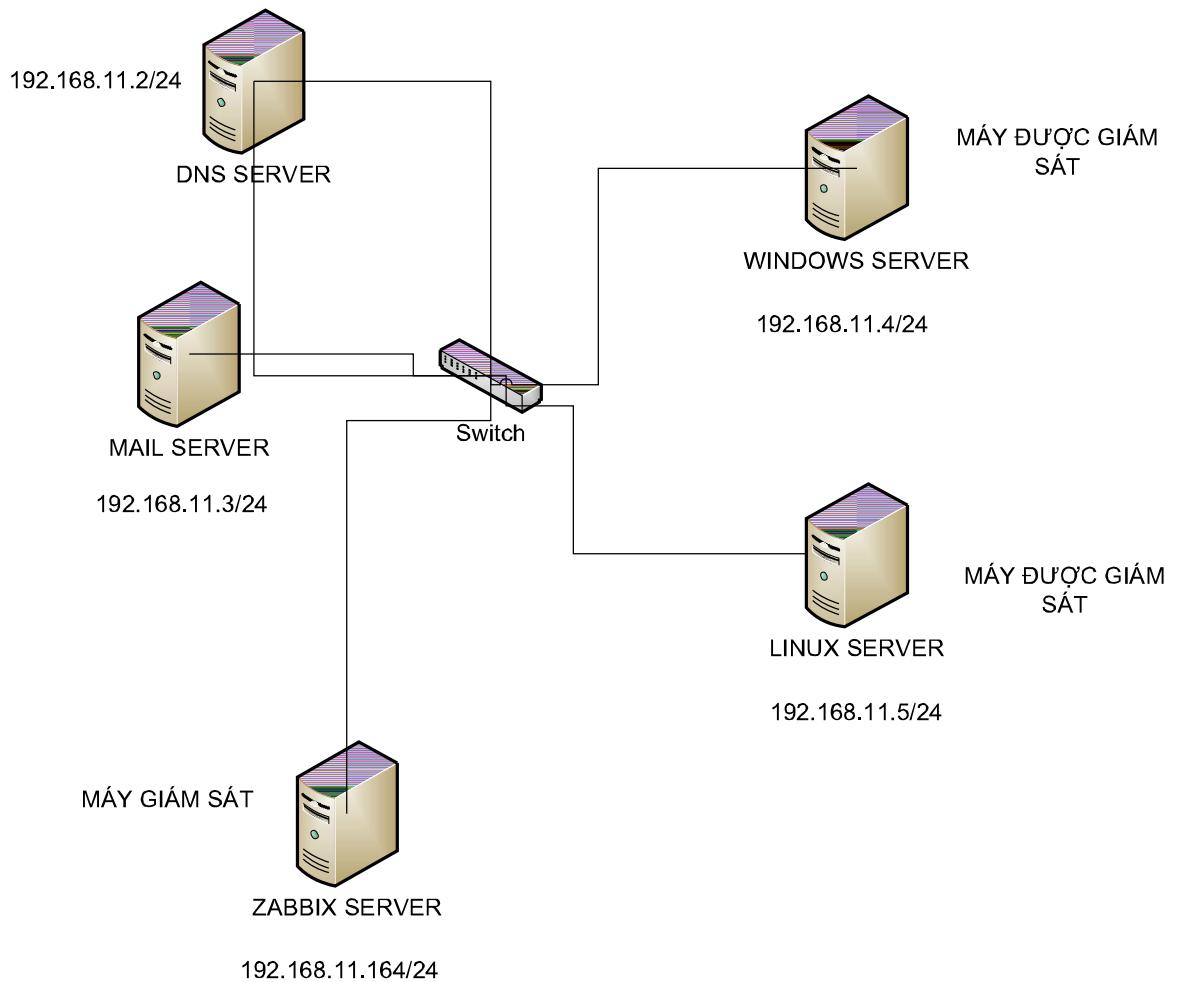


Hình 3.12: Tab Medias types

CHƯƠNG 4: THỰC NGHIỆM

GIÁM SÁT MẠNG LAN

4.1 Mô hình thực nghiệm:



Hình 4.1: Mô hình thực nghiệm

4.2 Mô tả, yêu cầu:

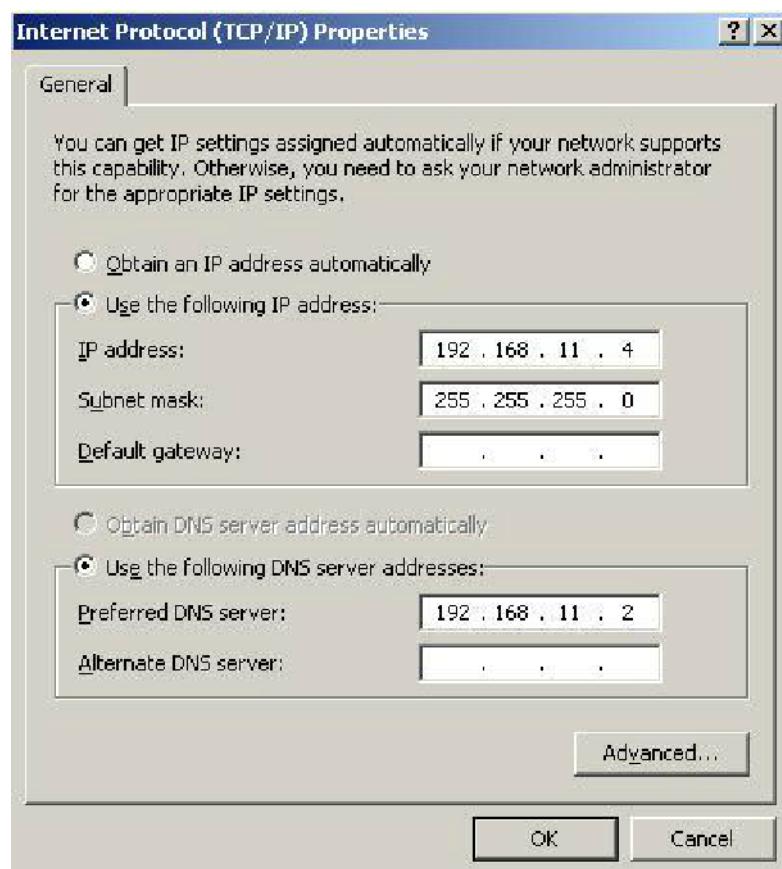
- Mô hình thực nghiệm được xây dựng gồm 5 máy được nối với nhau thông qua switch.
- Domain name là zabbix.com.vn, thuộc lớp mạng 192.168.11.0/24
- Zabbix server có địa chỉ IP = 192.168.11.164/24, chức năng giám sát thiết bị mạng, chương trình ứng dụng, tài nguyên các máy server khác.
- DNS server có địa chỉ IP = 192.168.11.2/24
- Mail server có địa chỉ IP = 192.168.11.3/24
- Windows server có địa chỉ IP = 192.168.11.4/24, Linux server có địa chỉ IP = 192.168.11.5/24 là hai máy được giám sát.
- Máy Zabbix server giám sát hai máy Linux server và Windows server.

4.3 Cấu hình:

4.3.1 Cấu hình máy Windows server:

Chuẩn bị: Gói zabbix_agents_1.8.2.win.zip

Bước 1: Cấu hình địa chỉ IP



Hình 4.2: Cấu hình địa chỉ IP

IP address: 192.168.11.4

Subnet mask: 255.255.255.0

Preferred DNS server: 192.168.11.2

Bước 2: Tạo file C:\zabbix_agentd.conf

Cấu hình file zabbix_agentd.conf tương tự với file zabbix_agentd.conf của Zabbix server

Bước 3: Cài đặt agent

```
Zabbix_agentd.exe --install
```

Bước 4: Chạy agent

```
Zabbix_agentd.exe --start
```

4.3.2 Cấu hình máy Linux server:

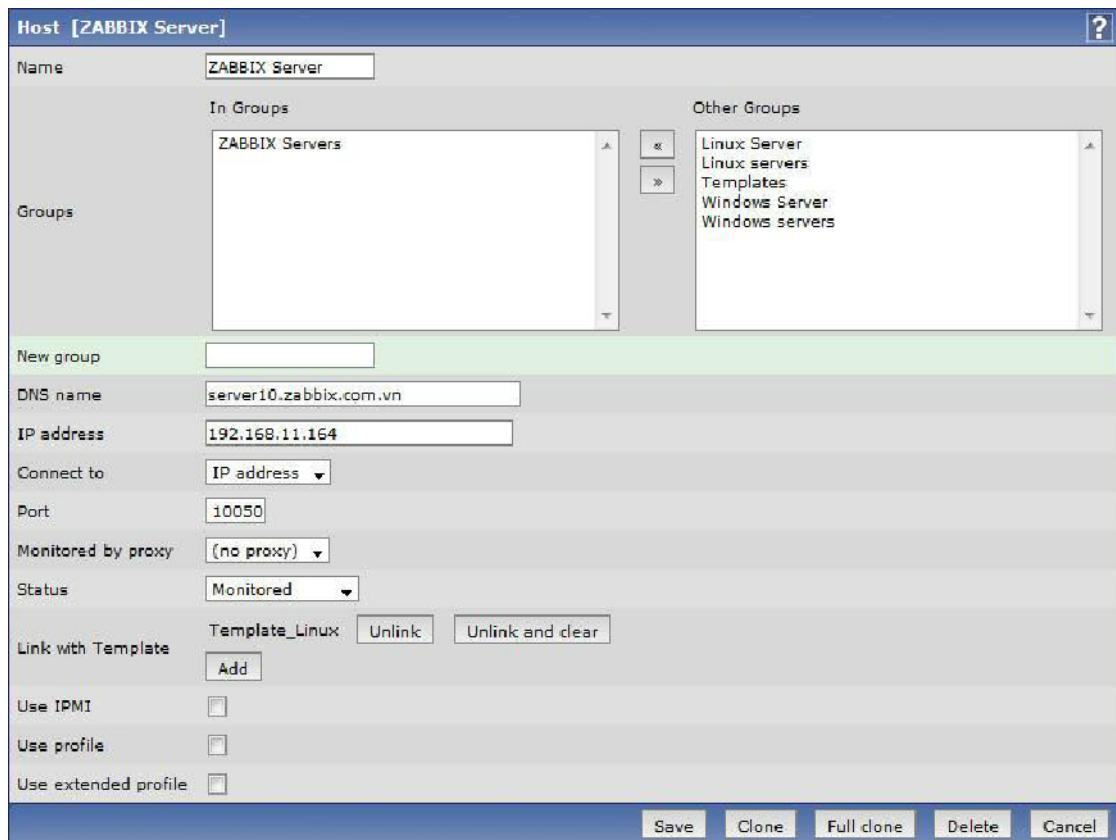
Xem phần cài đặt zabbix_agent mục 3.2.4.3

4.3.3 Cấu hình máy Zabbix server:

Tạo 3 host giám sát Zabbix server, Windows server và Linux server.

4.3.3.1 Cấu hình host Zabbix server:

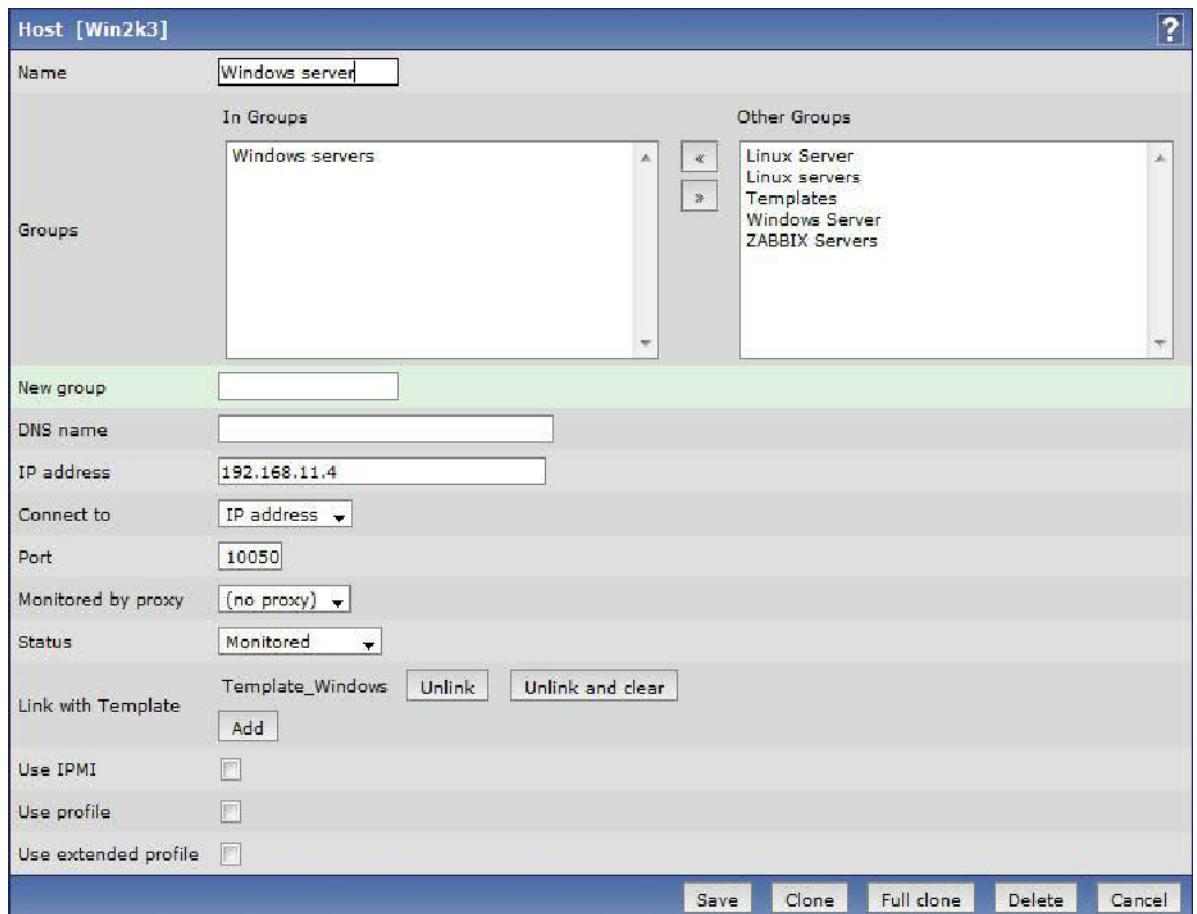
Tab Configuration -> Hosts -> Create Hosts



Hình 4.3: Cấu hình host Zabbix server

Name: ZABBIX server
Groups: ZABBIX server
DNS name: server10.zabbix.com.vn
IP address: 192.168.11.164
Connect to: IP address
Port: 10050
Monitored by proxy: No proxy
Status: Monitored
Link with Template: Template_Linux

4.3.3.2 Cấu hình host Windows server:



Hình 4.4: Cấu hình host Windows server

Name: Windows server

Groups: Windows server

DNS name:

IP address: 192.168.11.4

Conect to: IP address

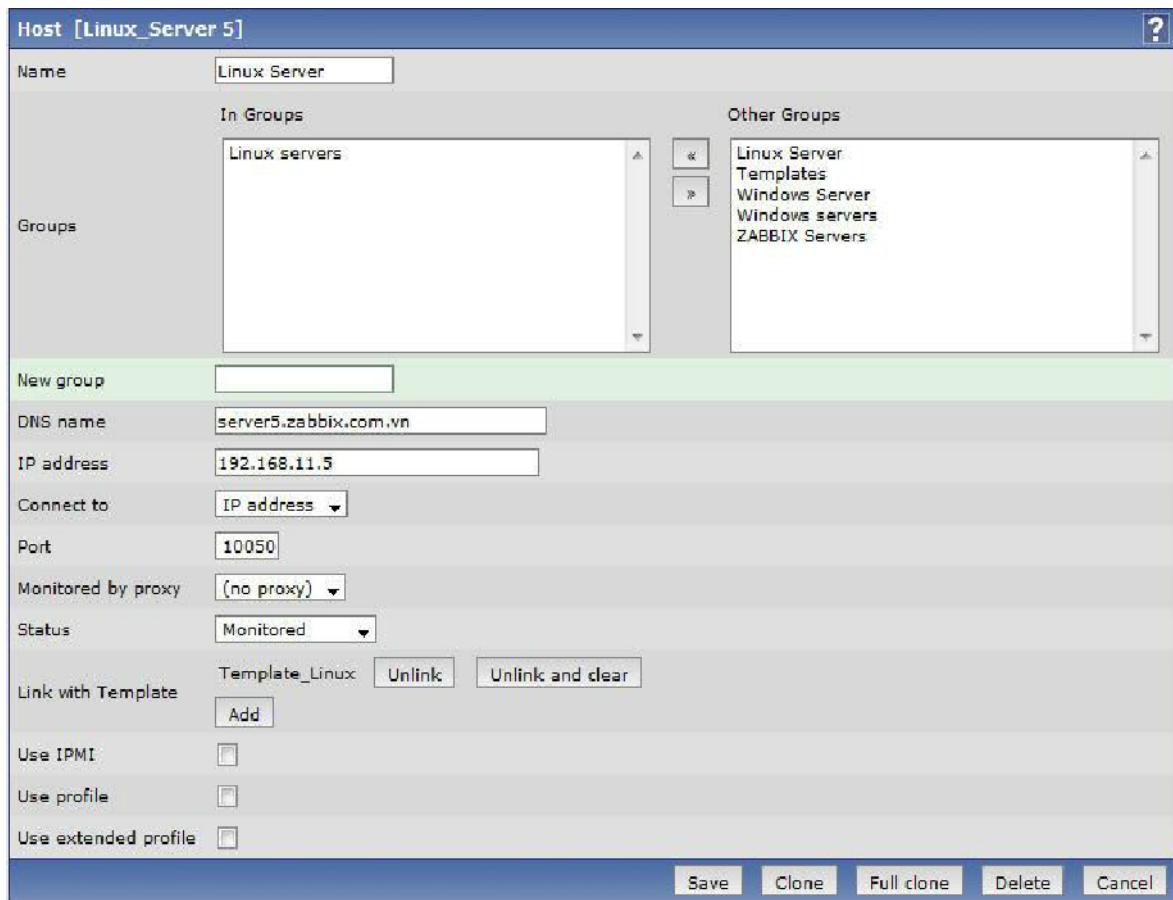
Port: 10050

Monitored by proxy: No proxy

Status: Monitored

Link with Template: Template_Windows

4.3.3.3 Cấu hình host Linux server:



Hình 4.5: Cấu hình host Linux server

Name: Linux server
Groups: Linux server
DNS name: server5.zabbix.com.vn
IP address: 192.168.11.5
Connect to: IP address
Port: 10050
Monitored by proxy: No proxy
Status: Monitored
Link with Template: Template_Linux

4.4 Kết quả:

Zabbix server giám sát hoạt động của máy chủ CentOS Linux, Windows Server 2003, Switch cisco, Router cisco... Giám sát bao gồm theo dõi hoạt động của các thiết bị mạng, tài nguyên của máy (CPU, Memory, Disk,...), theo dõi traffic trên các cổng kết nối của thiết bị. Việc giám sát tạo ra các thống kê về việc sử dụng mạng, thiết bị mạng đưa ra cảnh báo với biểu đồ đồ họa.

Monitoring -> Dashboard

Sơ đồ giúp cho người quản trị có cái nhìn tổng thể về hệ thống, lưu lượng thời gian thực trên đường link, giúp người quản trị nhanh chóng phát hiện sự cố.

The screenshot shows the Zabbix Monitoring Dashboard. The top navigation bar includes links for Monitoring, Inventory, Reports, Configuration, Administration, Dashboard, Overview, Web, Latest data, Triggers, Events, Graphs, Screens, Maps, Discovery, IT services, and Help. The main content area is titled "PERSONAL DASHBOARD". It features three main sections: "System status", "Status of ZABBIX", and "Last 20 issues".

System status:

Host group	Disaster	High	Average	Warning	Information	Not classified
Linux servers	0	0	9	0	0	0
Windows servers	0	0	0	0	0	0
ZABBIX Servers	0	0	5	0	0	0

Status of ZABBIX:

Parameter	Value	Details
ZABBIX server is running	Yes	-
Number of hosts (monitored/not monitored/templates)	45	3 / 0 / 42
Number of items (monitored/disabled/not supported)	233	208 / 0 / 25
Number of triggers (enabled/disabled)[true/unknown/false]	92	92 / 0 [14 / 0 / 78]
Number of users (online)	3	1
Required server performance, new values per second	7.1481	-

Last 20 issues:

Host	Issue	Last change	Age	Ack	Actions
Linux Server	IMAP server is down on Linux Server	30 May 21:33:19	1h 4m 15s	No	-
Linux Server	Inetd is not running on Linux Server	30 May 21:33:18	1h 4m 16s	No	-
Linux Server	POP3 server is down on Linux Server	30 May 21:33:18	1h 4m 16s	No	-
Linux Server	Mysql is not running on Linux Server	30 May 21:33:17	1h 4m 17s	No	-
Linux Server	Apache is not running on Linux Server	30 May 21:33:17	1h 4m 17s	No	-
Linux Server	News (NNTP) server is down on Linux Server	30 May 21:33:17	1h 4m 17s	No	-
Linux Server	WEB (HTTP) server is down on Linux Server	30 May 21:33:17	1h 4m 17s	No	-
Linux Server	FTP server is down on Linux Server	30 May 21:33:15	1h 4m 19s	No	-
Linux Server	Zabbix_server is not running on Linux Server	30 May 21:33:15	1h 4m 19s	No	-
ZABBIX Server	POP3 server is down on ZABBIX Server	30 May 20:28:47	2h 8m 47s	No	-
ZABBIX Server	IMAP server is down on ZABBIX Server	30 May 20:28:47	2h 8m 47s	No	-
ZABBIX Server	Inetd is not running on ZABBIX Server	30 May 20:28:47	2h 8m 47s	No	-
ZABBIX Server	News (NNTP) server is down on ZABBIX Server	30 May 20:28:46	2h 8m 48s	No	-
ZABBIX Server	FTP server is down on ZABBIX Server	30 May 20:28:46	2h 8m 48s	No	-

Hình 4.6:

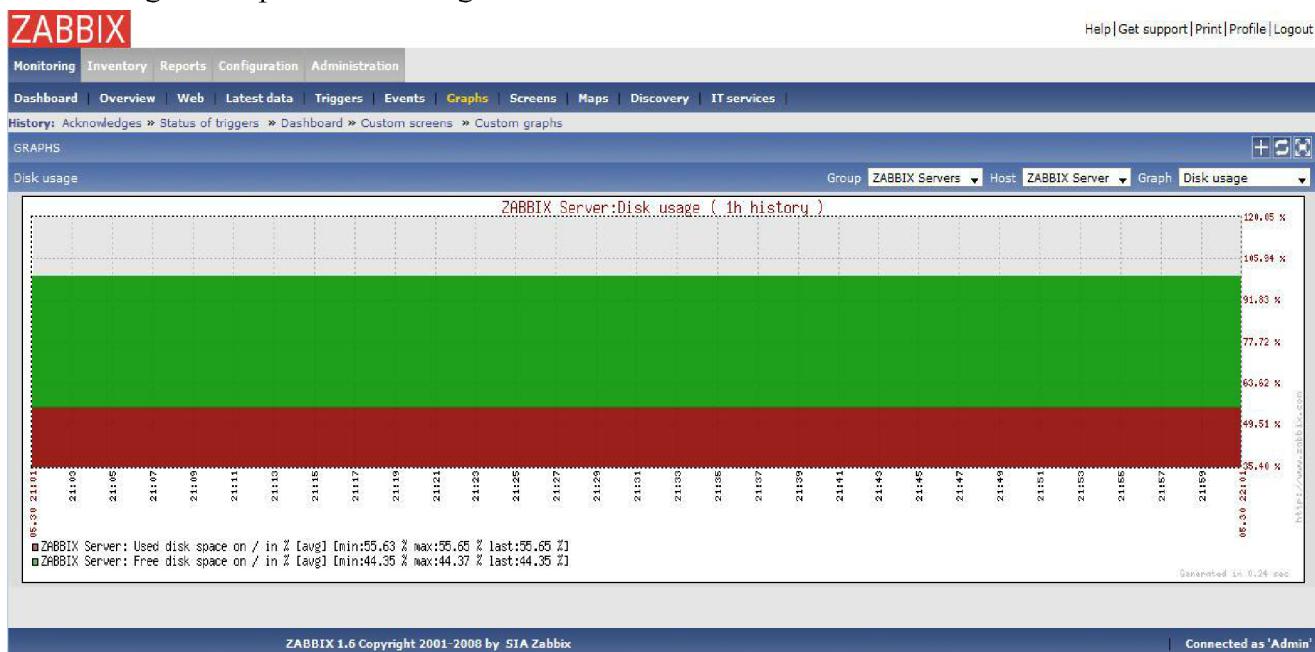
4.4.1 Máy Zabbix server:

Monitoring -> Graph -> CPU Loads
Biểu đồ trạng thái hoạt động của CPU



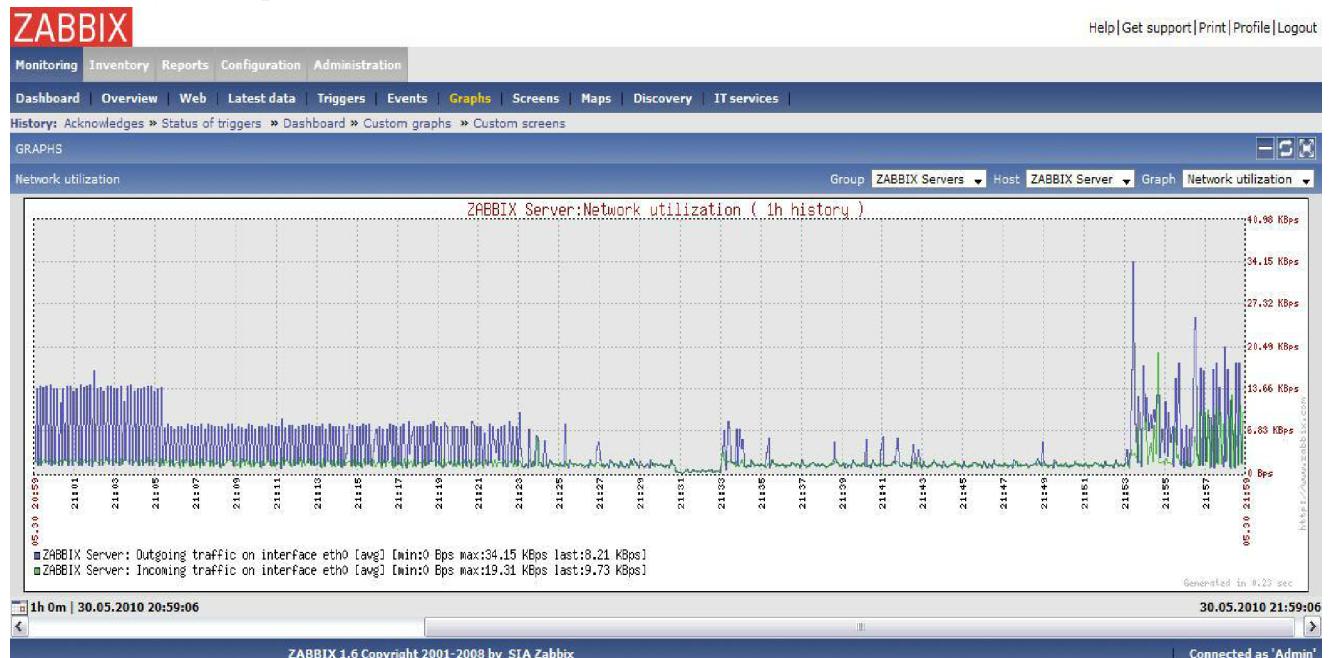
Hình 4.7: Biểu đồ trạng thái của CPU

Monitoring -> Graph -> Disk usage



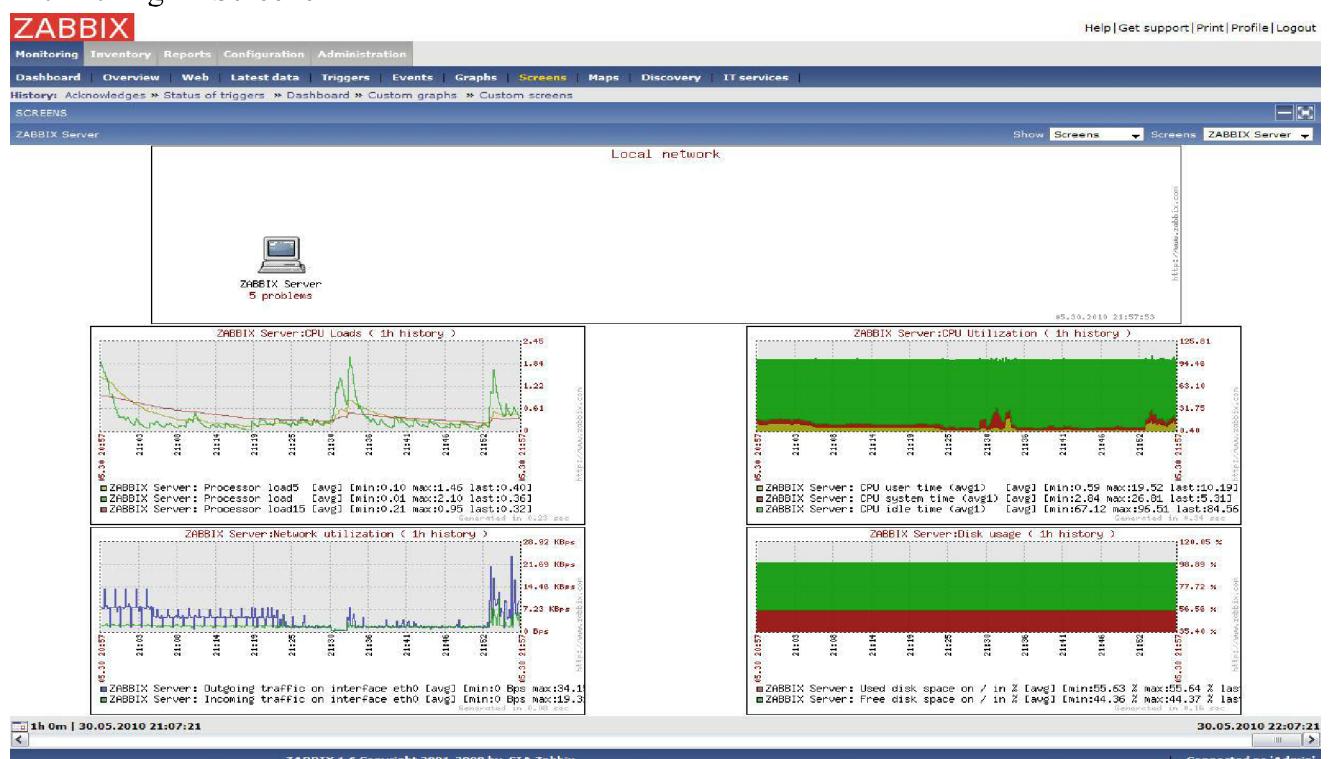
Hình 4.8: Biểu đồ trạng thái của ổ cứng

Monitoring -> Graph -> Network utilization



Hình 4.9: Biểu đồ trạng thái card mạng

Monitoring -> Screens



Hình 4.10: Biểu đồ tổng thể trạng thái CPU, card mạng, ổ cứng.

4.4.2 Máy Windows server:

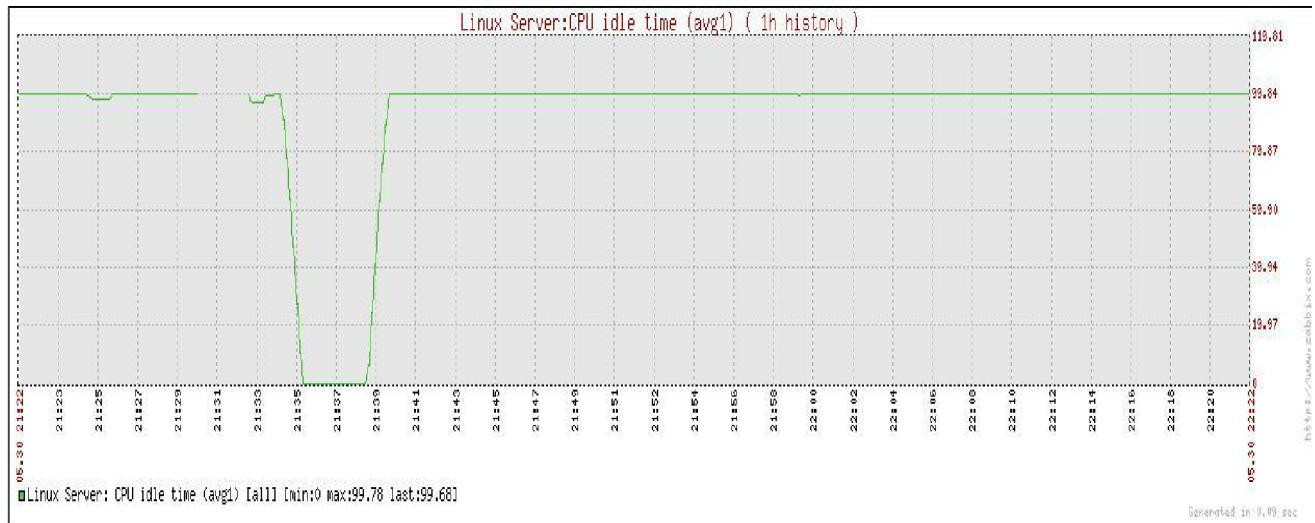
Monitoring -> Latest data -> CPU -> Graph



Hình 4.11: Biểu đồ trạng thái CPU của Windows server

4.4.3 Máy Linux server:

Monitoring -> Latest data -> CPU -> Graph



Hình 4.12: Biểu đồ trạng thái CPU của Linux server

CHƯƠNG 5: KẾT LUẬN

5.1 Kết quả đạt được:

- Phần mềm Zabbix giám sát dựa trên cơ chế agent/server. Với cơ chế này khả năng giám sát toàn diện hơn nhờ có agent.
- Hệ thống có cấu trúc mở cho phép phát triển, tùy biến, tích hợp với các hệ thống khác một cách linh hoạt, dễ dàng.
- Hệ thống cho phép giám sát trạng thái, các thông số thống kê của thiết bị cũng như các dịch vụ theo thời gian.
- Tự động phát hiện một số sự cố thường gặp và cảnh báo cho người quản trị mạng thông qua việc gửi Email, nhắn tin SMS đến điện thoại di động.
- Tuy nhiên nhóm đã có gắng hết sức chỉ dừng ở mức độ theo dõi, giám sát máy chủ như giám sát tài nguyên máy, dung lượng traffic.

5.2 Ưu điểm – khuyết điểm:

Ưu điểm:

- Hiển thị tham số thống kê: CPU, RAM, không gian lưu trữ, các tiến trình, lưu lượng trên các interface, ... của thiết bị theo thời gian, trực quan.
- Giám sát được hầu hết các thiết bị mạng, các ứng dụng dịch vụ (SMTP, POP3, HTTP, FTP, ...)
- Phát hiện sự cố, phát hiện tấn công nhanh chóng đưa ra cảnh báo cho người quản trị mạng.

Khuyết điểm:

Cài đặt phức tạp, khó khăn.

5.3 Hướng phát triển:

- Nghiên cứu sâu hơn về hệ thống giám sát mạng Zabbix và các công cụ hỗ trợ giám sát mạng.
- Phát triển các chức năng trên Zabbix như : chức năng cảnh báo SMS qua điện thoại động.

5.4 Khó khăn:

- Do chưa có nhiều kinh nghiệm, mới làm quen nên việc cài đặt phần mềm gặp rất nhiều khó khăn, vướng mắt.
- Tài liệu hạn hẹp, rất ít sách đề cập đến vấn đề giám sát mạng bằng Zabbix.

TÀI LIỆU THAM KHẢO

- [1] Nguyễn Thị Thanh Vân, Hệ điều hành mạng Unix, Trường Đại học Sư Phạm Kỹ Thuật Tp.HCM 2008.
- [2] Zabbix Manual v1.6, Copyright © 2008 ZABBIX SIA
- [3] Rihards Olups, Zabbix 1.8 Network Monitoring, Copyright © 2010 Packt Publishing
- [4] <http://www.zabbix.com>
- [5] <http://www.zabbix.com/forum>
- [6] <http://www.zabbix.com/wiki/howto/install/centos/centosinstall>
- [7] <http://www.nhatnghe.com/forum>
- [8] <http://library.linode.com>

.....