**** TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

VÀ TRUYỀN THÔNG VIỆT - HÀN

**KHOA KỸ THUẬT MÁY TÍNH VÀ ĐIỆN TỬ**

**BÁO CÁO**

**THỰC TẬP TỐT NGHIỆP**

**TÊN ĐỀ TÀI**

**XÂY DỰNG HỆ THỐNG MẠNG TỰ ĐỘNG HÓA**

**VỚI ANSIBLE KẾT HỢP PROMETHEUS VÀ GRAFANA**

**Sinh viên thực hiện : Nguyễn An Phúc**

**Lớp : 21NS**

**Giảng viên hướng dẫn : THS. Trần Thu Thủy**

**Đơn vị thực tập : VNNIC**

**Người hướng dẫn : Nguyễn Văn Bình**

***Đà Nẵng, tháng 8 năm 2025***

**** TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

VÀ TRUYỀN THÔNG VIỆT - HÀN

**KHOA KỸ THUẬT MÁY TÍNH VÀ ĐIỆN TỬ**

**BÁO CÁO**

**THỰC TẬP TỐT NGHIỆP**

**TÊN ĐỀ TÀI / CÔNG VIỆC**

**XÂY DỰNG HỆ THỐNG MẠNG TỰ ĐỘNG HÓA**

**VỚI ANSIBLE KẾT HỢP PROMETHEUS VÀ GRAFANA**

**Sinh viên thực hiện : Nguyễn An Phúc**

**Lớp : 21NS**

**Giảng viên hướng dẫn : THS. Trần Thu Thủy**

**Đơn vị thực tập : VNNIC**

**Người hướng dẫn : Nguyễn Văn Bình**

***Đà Nẵng, tháng 8 năm 2025***

NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN

…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

Đà Nẵng, ngày 8 tháng 9 năm 2025

Giảng viên hướng dẫn

LỜI CẢM ƠN

Để đề tài đạt được kết quả như hiện tại, em đã nhận được sự hỗ trợ, giúp đỡ, chỉ bảo tận tâm của cô. Với tình cảm sâu sắc, chân thành, cho phép em được bày tỏ lòng biết ơn sâu sắc đến tất cả quý thầy cô đã tạo điều kiện giúp đỡ em trong quá trình học tập và nghiên cứu.

Trước hết, em xin gửi tới đội ngũ giảng viên trường Đại học Công nghệ thông tin và truyền thông Việt – Hàn lời chào trân trọng, lời chúc sức khỏe và lời cảm ơn sâu sắc nhất. Với sự quan tâm, chỉ bảo tận tình chu đáo, cũng như vốn kiến thức về nhiều lĩnh vực của mình, đội ngũ giảng viên của trường đã truyền tải cho chúng em được nhiều kiến thức, cũng như kỹ năng cần thiết, để đến ngày hôm nay, chúng em đã có thể hoàn thành được Đề tài của mình.

Đặc biệt, em xin gửi lời cảm ơn chân thành tới THS.TRẦN THU THỦY và anh NGUYỄN VĂN BÌNH, giảng viên và người hướng dẫn đã quan tâm, giúp đỡ, chỉ bảo tận tình để em có thể hoàn thành tốt đề tài này trong suốt thời gian vừa qua.

Với điều kiện thời gian cũng như kinh nghiệm còn hạn chế, đề tài này không thể tránh được những thiếu sót. Em rất mong nhận được sự chỉ bảo, đóng góp ý kiến của các thầy/cô, để chúng em có điều kiện bổ sung, nâng cao kiến thức, kỹ năng của mình, phục vụ tốt hơn cho công tác thực tế sau này.

Em xin trân trọng cảm ơn!

*Sinh viên,*

Nguyễn An Phúc

MỤC LỤC

[NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN i](#_Toc208329952)

[LỜI CẢM ƠN ii](#_Toc208329953)

[MỤC LỤC iii](#_Toc208329954)

[DANH MỤC HÌNH ẢNH vi](#_Toc208329955)

[DANH MỤC CÁC TỪ VIẾT TẮT viii](#_Toc208329956)

[MỞ ĐẦU xii](#_Toc208329957)

[1. Giới Thiệu xii](#_Toc208329958)

[2. Mục tiêu xii](#_Toc208329959)

[3. Đối Tượng, PHạm vi Và Phương pháp tiếp cận xiii](#_Toc208329960)

[4. Kết quả Của đề Tài xiii](#_Toc208329961)

[5. Bố cục của đề tài xiv](#_Toc208329962)

[CHƯƠNG 1: GIỚI THIỆU CÔNG TY VNNIC 1](#_Toc208329963)

[1.1. Giới thiệu tổng quát công ty VNNIC 1](#_Toc208329964)

[1.2. Lịch sử hình thành và phát triển 2](#_Toc208329965)

[1.3. Tầm nhìn, sứ mệnh, giá trị cốt lõi và cơ cấu tổ chức 3](#_Toc208329966)

[1.4. Các trụ cột chiến lược phát triển 6](#_Toc208329967)

[1.5. Mục tiêu phát triển của công ty 8](#_Toc208329968)

[1.5.1. Mục Tiêu Tổng Quát 8](#_Toc208329969)

[1.5.2. Mục Tiêu Cụ Thể 9](#_Toc208329970)

[1.6. Nhiệm vụ trọng tâm của VNNIC 11](#_Toc208329971)

[CHƯƠNG 2: NGHIÊN CỨU KIẾN TRÚC VÀ CÔNG NGHỆ ANSIBLE – PROMETHEUS – GRAFANA 14](#_Toc208329972)

[2.1. Giới thiệu chương 14](#_Toc208329973)

[2.2. Tổng quan về Ansible 14](#_Toc208329974)

[2.2.1. Khái niệm và vai trò 14](#_Toc208329975)

[2.2.2. Kiến trúc Ansible 15](#_Toc208329976)

[2.2.3. Ưu điểm của Ansible 15](#_Toc208329977)

[2.3. GIỚI THIỆU TỔNG QUAN VỀ PROMETHEUS VÀ GRAFANA 16](#_Toc208329978)

[2.3.1. Kiến trúc và cơ chế hoạt động của Prometheus 17](#_Toc208329979)

[2.3.2. Thành phần chính của Prometheus 17](#_Toc208329980)

[2.3.3. Kiến trúc hoạt động của Prometheus 18](#_Toc208329981)

[2.3.4. Giới thiệu chi tiết về Grafana 18](#_Toc208329982)

[2.4. Mối quan hệ và tích hợp giữa Ansible – Prometheus – Grafana 19](#_Toc208329983)

[2.5. Kết luận chương 20](#_Toc208329984)

[CHƯƠNG 3: XÂY DỰNG VÀ TRIỀN KHAI LAB 21](#_Toc208329985)

[3.1. Thiết kế mô hình lab 21](#_Toc208329986)

[3.1.1. Phân vùng mạng chi tiết: 22](#_Toc208329987)

[3.2. Triển khai hệ thống tự động hóa với Ansible 23](#_Toc208329988)

[3.2.1. Cấu trúc thư mục làm việc 23](#_Toc208329989)

[3.2.2. Tự động hóa backup thiết bị mạng 24](#_Toc208329990)

[3.2.3. Tự động tích hợp với Teleport Server 26](#_Toc208329991)

[3.2.4. Tự động hóa cài đặt dịch vụ Nginx 27](#_Toc208329992)

[3.3. Cấu hình Prometheus thu thập metric 28](#_Toc208329993)

[3.3.1. Thu thập trạng thái backup của thiết bị: 28](#_Toc208329994)

[3.3.2. Thu thập trạng thái của dịch vụ Nginx: 29](#_Toc208329995)

[3.3.3. Thu thập sử dụng node\_exporter 30](#_Toc208329996)

[3.3.4. Thu thập sử dụng giao thức SNMP 31](#_Toc208329997)

[3.3.5. Cấu hình file Prometheus.yml 34](#_Toc208329998)

[3.4. Tích hợp hệ thống và tạo Dashboard 35](#_Toc208329999)

[3.4.1. Thêm Prometheus vào Grafana 35](#_Toc208330000)

[3.4.2. Tạo Dashboard giám sát sử dung node\_exporter 36](#_Toc208330001)

[3.4.3. Tạo dashboard giám sát sử dụng SNMP walk 38](#_Toc208330002)

[3.4.4. Tự tạo dashboard để giám sát các thiết bị switch 39](#_Toc208330003)

[3.4.5. Cấu hình tích hợp alertmanager gửi cảnh báo 41](#_Toc208330004)

[3.4.6. Kết nối cấu hình cảnh báo đến telegram 42](#_Toc208330005)

[3.4.7. Quy tắc cảnh báo (Alert Rules) 43](#_Toc208330006)

[3.4.8. Cơ chế gửi cảnh báo 47](#_Toc208330007)

[3.5. Kết luận chương 50](#_Toc208330008)

[KẾT LUẬN 53](#_Toc208330009)

[1. KẾT QUẢ ĐẠT ĐƯỢC 53](#_Toc208330010)

[2. NHẬN XÉT SAU THỜI GIAN THỰC TẬP TẠI CÔNG TY VNNIC 54](#_Toc208330011)

[TÀI LIỆU THAM KHẢO 57](#_Toc208330012)

DANH MỤC HÌNH ẢNH

[Hình 1.1: Logo công ty VNNIC 1](#_Toc207292804)

[Hình 1.2: Kiến Trúc Tổ Chức của VNNIC 4](#_Toc207292805)

[Hình 1.3: Tổ Chức bộ máy trong công ty 5](#_Toc207292806)

[Hình 1.4: Bảy Trụ Cột Chiến Lược của VNNIC 6](#_Toc207292807)

[Hình 2.1: Logo Ansible 14](#_Toc207292808)

[Hình 2.2: Kiến trúc của Ansible 15](#_Toc207292809)

[Hình 2.3: Logo Prometheus 16](#_Toc207292810)

[Hình 2.4: Logo Grafana 16](#_Toc207292811)

[Hình 2.5: Kiến trúc hoạt động của Prometheus 18](#_Toc207292812)

[Hình 2.6: Grafana DashBoard 19](#_Toc207292813)

[Hình 3.1. Sơ đồ mô hình hệ thống 21](#_Toc207292814)

[Hình 3.2: Cấu trúc thư mục làm việc 23](#_Toc207292815)

[Hình 3.3: File Playbook backup Pfsense 24](#_Toc207292816)

[Hình 3.4: File Playbook backup switch 25](#_Toc207292817)

[Hình 3.5: File Playbook tự động tích hợp với Teleport Server 27](#_Toc207292818)

[Hình 3.6: File Playbook tự động cài đặt Nginx 28](#_Toc207292819)

[Hình 3.7: Trạng thái backup của thiết bị 29](#_Toc207292820)

[Hình 3.8: Cấu hình trên Prometheus.yml 29](#_Toc207292821)

[Hình 3.9: Trạng thái hiển thị của Nginx 30](#_Toc207292822)

[Hình 3.10. Kiểm tra trạng thái hoạt động của node\_exporter 31](#_Toc207292823)

[Hình 3.11. Kiểm tra cấu hình 32](#_Toc207292824)

[Hình 3.12. Cấu hình SNMP trên Pfsense 33](#_Toc207292825)

[Hình 3.13. Gom các metrics thành các module phù hợp 33](#_Toc207292826)

[Hình 3.14. Cấu hình file Prometheus.yml 34](#_Toc207292827)

[Hình 3.15. Kiểm tra trạng thái hoạt động của từng thiết bị 35](#_Toc207292828)

[Hình 3.16. Tích hợp Prometheus vào Grafana 35](#_Toc207292829)

[Hình 3.17. Import Dashboard có sẵn từ Grafana Lab 36](#_Toc207292830)

[Hình 3.18. Thông tin chung về hệ thống 36](#_Toc207292831)

[Hình 3.19. Hiệu suất 37](#_Toc207292832)

[Hình 3.20. Network traffic trên từng cổng 38](#_Toc207292833)

[Hình 3.21: Xem giám sát thông qua Grafana 39](#_Toc207292834)

[Hình 3.22. Giao diện tùy chỉnh 39](#_Toc207292835)

[Hình 3.23. Tổng lưu lượng mạng In/Out 40](#_Toc207292836)

[Hình 3.24. Bảng trạng thái từng cổng 40](#_Toc207292837)

[Hình 3.25. Hệ thống gửi cảnh báo Alertmanager 42](#_Toc207292838)

[Hình 3.26. Cấu hình alertmanager.yml 43](#_Toc207292839)

[Hình 3.27. Trạng thái dịch vụ Alertmanager 43](#_Toc207292840)

[Hình 3.28. Rule cảnh báo trạng thái cổng mạng 44](#_Toc207292841)

[Hình 3.29. Rule cảnh báo trạng backup khi không backup thành công 45](#_Toc207292842)

[Hình 3.30. Rule cảnh báo khi có lưu lượng In/Out tăng cao 46](#_Toc207292843)

[Hình 3.31. Rule gửi cảnh báo theo tình trạng mức sử dụng bộ nhớ 47](#_Toc207292844)

[Hình 3.32. Ví dụ về template mẫu của cảnh báo Up/Down trên cổng mạng 47](#_Toc207292845)

[Hình 3.33. Cảnh báo khi trạng thái cổng down 48](#_Toc207292846)

[Hình 3.34. Cảnh báo khi trạng thái cổng được khôi phục trở lại 48](#_Toc207292847)

[Hình 3.35. Cảnh báo khi backup failed 49](#_Toc207292848)

[Hình 3.36. Cảnh báo khi lượng memory đạt 74.55% 50](#_Toc207292849)

DANH MỤC CÁC TỪ VIẾT TẮT

|  |  |  |
| --- | --- | --- |
| TỪ VIẾT TẮT | ĐẦY ĐỦ | NỘI DUNG |
| IP | Internet Protocol | Giao thức định địa chỉ và truyền dữ liệu giữa các thiết bị mạng. |
| LAN | Local Area Network | Mạng cục bộ – kết nối các thiết bị trong phạm vi gần (như văn phòng, nhà ở). |
| WAN | Wide Area Network | Mạng diện rộng – kết nối các mạng LAN ở khoảng cách lớn. |
| NAT | Network Address Translation | Cơ chế chuyển đổi địa chỉ IP trong mạng nội bộ ra địa chỉ công cộng. |
| SNMP | Simple Network Management Protocol | Giao thức giám sát và quản lý thiết bị mạng. |
| MIB | Management Information Base | Cơ sở dữ liệu quản lý dùng trong SNMP để lưu thông tin thiết bị. |
| pfSense | Packet Filter Sense | Hệ điều hành tường lửa mã nguồn mở dùng để định tuyến và bảo mật mạng. |
| DNS | Domain Name System | Hệ thống phân giải tên miền thành địa chỉ IP. |
| DHCP | Dynamic Host Configuration Protocol | Giao thức cấp phát địa chỉ IP động cho các thiết bị. |
| GUI | Graphical User Interface | Giao diện người dùng đồ họa, dễ sử dụng. |
| RRD | Round Robin Database | Cơ sở dữ liệu dạng vòng dùng để lưu trữ số liệu theo thời gian (dùng cho biểu đồ). |
| ACL | Access Control List | Danh sách điều khiển truy cập để giới hạn quyền của người dùng hoặc dịch vụ. |
| IDS | Intrusion Detection System | Hệ thống phát hiện xâm nhập mạng. |
| IPS | Intrusion Prevention System | Hệ thống ngăn chặn xâm nhập mạng. |
| HA | High Availability | Độ sẵn sàng cao – đảm bảo hệ thống luôn hoạt động ngay cả khi có sự cố. |
| CPU | Central Processing Unit | Bộ xử lý trung tâm – thành phần chính xử lý dữ liệu. |
| RAM | Random Access Memory | Bộ nhớ truy xuất ngẫu nhiên – lưu trữ dữ liệu tạm thời. |
| VM | Virtual Machine | Máy ảo – mô phỏng máy tính chạy trên phần mềm ảo hóa. |
| API | Application Programming Interface | Giao diện lập trình ứng dụng – cho phép các phần mềm giao tiếp với nhau. |
| TLS | Transport Layer Security | Giao thức mã hóa bảo mật cho truyền thông mạng. |
| HTTP | HyperText Transfer Protocol | Giao thức truyền tải siêu văn bản – nền tảng của World Wide Web. |
| HTTPS | HyperText Transfer Protocol Secure | Phiên bản bảo mật của HTTP với mã hóa TLS/SSL. |
| Prometheus | Prometheus Monitoring System | Hệ thống giám sát mã nguồn mở thu thập và lưu trữ dữ liệu dạng chuỗi thời gian. |
| Grafana | Grafana Visualization Tool | Nền tảng trực quan hóa dữ liệu, xây dựng dashboard từ dữ liệu Prometheus và nhiều nguồn khác. |
| Alertmanager | Prometheus Alertmanager | Thành phần quản lý cảnh báo của Prometheus, hỗ trợ gửi thông báo đến nhiều kênh. |
| Exporter | Metric Exporter | Thành phần trung gian thu thập số liệu từ hệ thống hoặc thiết bị để gửi về Prometheus. |
| Node Exporter | Prometheus Node Exporter | Exporter phổ biến dùng để giám sát tài nguyên máy chủ (CPU, RAM, Disk). |
| SNMP Exporter | Prometheus SNMP Exporter | Exporter hỗ trợ thu thập số liệu từ thiết bị mạng qua SNMP. |
| Webhook | Webhook | Cơ chế gửi dữ liệu tự động từ hệ thống này sang hệ thống khác qua HTTP POST. |
| Backup | Backup Process | Quá trình sao lưu dữ liệu hoặc cấu hình hệ thống để phục hồi khi xảy ra sự cố. |
| Load Balancing | Load Balancing | Cân bằng tải – phân phối lưu lượng giữa nhiều máy chủ để tối ưu hiệu suất. |
| QoS | Quality of Service | Chính sách quản lý băng thông và ưu tiên dữ liệu trong mạng. |

MỞ ĐẦU

1. Giới Thiệu

Trong bối cảnh số hóa và toàn cầu hóa hiện nay, hệ thống mạng đóng vai trò then chốt trong hoạt động của doanh nghiệp. Tuy nhiên, cùng với sự phát triển của công nghệ thông tin, các mối đe dọa an ninh mạng ngày càng tinh vi, đòi hỏi hạ tầng CNTT không chỉ được cấu hình chính xác, đồng bộ mà còn phải giám sát liên tục để kịp thời phát hiện và xử lý sự cố.

Việc quản trị thủ công hệ thống mạng thường tiềm ẩn rủi ro sai sót, tốn kém thời gian và khó mở rộng khi quy mô doanh nghiệp phát triển. Do đó, giải pháp tự động hóa cấu hình kết hợp với giám sát tập trung trở thành xu hướng tất yếu nhằm nâng cao hiệu quả quản trị và đảm bảo an toàn thông tin.

Trong đó, Ansible – công cụ tự động hóa cấu hình mã nguồn mở – cho phép quản trị viên triển khai, cấu hình và quản lý thiết bị mạng một cách nhanh chóng, đồng bộ và an toàn. Đồng thời, bộ công cụ giám sát Prometheus và Grafana mang lại khả năng thu thập dữ liệu linh hoạt, trực quan hóa mạnh mẽ và tích hợp cảnh báo theo thời gian thực.

Nhận thấy tầm quan trọng của sự kết hợp này, nhóm chúng em lựa chọn thực hiện đề tài:

"Xây dựng hệ thống mạng tự động hóa cấu hình và giám sát toàn diện với Ansible và Prometheus".

Mục tiêu là nghiên cứu, thiết kế và triển khai mô hình mạng có khả năng tự động hóa cấu hình, theo dõi trạng thái hoạt động và cảnh báo kịp thời sự cố, qua đó mang lại một giải pháp toàn diện, hiệu quả và tiết kiệm chi phí cho doanh nghiệp.

1. Mục tiêu

Đề tài được thực hiện với các mục tiêu chính sau:

Tìm hiểu Ansible: Nghiên cứu kiến trúc, nguyên lý hoạt động và khả năng ứng dụng của Ansible trong tự động hóa cấu hình hệ thống mạng.

Nghiên cứu Prometheus – Grafana: Khảo sát cơ chế thu thập dữ liệu, trực quan hóa và cảnh báo trong giám sát hệ thống mạng.

Xây dựng hệ thống tích hợp: Triển khai mô hình kết hợp Ansible với Prometheus – Grafana trong môi trường mạng mô phỏng, nhằm vừa tự động hóa cấu hình, vừa giám sát và cảnh báo theo thời gian thực.

Đánh giá hiệu quả: Phân tích khả năng giảm thiểu sai sót cấu hình, phát hiện sự cố nhanh chóng, và hỗ trợ vận hành ổn định của giải pháp tích hợp này.

1. Đối Tượng, PHạm vi Và Phương pháp tiếp cận

Đối tượng nghiên cứu: Hệ thống tự động hóa cấu hình và giám sát mạng sử dụng Ansible, Prometheus, Grafana, Alertmanager và các Exporter.

Phạm vi nghiên cứu:

* Tìm hiểu kiến trúc, nguyên lý hoạt động của Ansible, Prometheus và Grafana.
* Triển khai hệ thống trong môi trường mô phỏng doanh nghiệp.
* Thiết lập tự động hóa cấu hình mạng (Ansible) và giám sát – cảnh báo (Prometheus – Grafana – Alertmanager).
* Đánh giá hiệu quả qua các tình huống thử nghiệm.

Phương pháp tiếp cận:

* Nghiên cứu tài liệu lý thuyết, hướng dẫn triển khai.
* Thực nghiệm triển khai trong môi trường mô phỏng.
* Đánh giá bằng so sánh trước/sau khi áp dụng giải pháp.

1. Kết quả Của đề Tài

Sau khi hoàn thành, đề tài dự kiến mang lại các đóng góp:

* Xây dựng báo cáo chi tiết về giải pháp kết hợp tự động hóa cấu hình (Ansible) và giám sát mạng (Prometheus – Grafana).
* Triển khai thành công hệ thống mạng có khả năng cấu hình tự động, giám sát tập trung và cảnh báo sự cố.
* Đánh giá hiệu quả trong việc nâng cao tính ổn định, an toàn và khả năng quản trị hệ thống mạng.
* Cung cấp tài liệu tham khảo, hướng dẫn triển khai cho cá nhân và tổ chức có nhu cầu áp dụng giải pháp này.

1. Bố cục của đề tài

Ngoài phần Mở đầu, báo cáo được trình bày qua ba chương chính:

Chương 1: Giới thiệu công ty VNNIC

Chương 2: Kiến trúc và công nghệ Ansible – Prometheus – Grafana

Chương 3: Xây dựng và triển khai hệ thống mạng tự động hóa cấu hình và giám sát

Cuối cùng là Kết luận, Tài liệu tham khảo và Phụ lục.

# GIỚI THIỆU CÔNG TY VNNIC

## Giới thiệu tổng quát công ty VNNIC

Trung tâm Internet Việt Nam (VNNIC) là một đơn vị trực thuộc Bộ Thông tin và Truyền thông Việt Nam, được thành lập vào ngày 28 tháng 4 năm 2000. Với vai trò là cơ quan quản lý nhà nước về tài nguyên Internet tại Việt Nam, VNNIC có trách nhiệm quản lý, cấp phát, và giám sát hoạt động sử dụng các tài nguyên quan trọng như tên miền quốc gia ".vn", địa chỉ IP (IPv4, IPv6), hệ thống máy chủ tên miền (DNS), và các tài nguyên liên quan khác.



Hình .1: Logo công ty VNNIC

VNNIC đóng vai trò quan trọng trong việc phát triển hạ tầng kỹ thuật của Internet Việt Nam, đảm bảo sự ổn định, an toàn, và bền vững cho hệ thống Internet quốc gia. Trung tâm cũng là cơ quan đầu mối trong việc hợp tác quốc tế về Internet, tham gia vào các tổ chức, diễn đàn quốc tế như ICANN (Tổ chức quản lý số hiệu mạng Internet) và APNIC (Trung tâm thông tin mạng Châu Á - Thái Bình Dương).

Ngoài ra, VNNIC còn thực hiện các hoạt động nghiên cứu, phát triển và triển khai các giải pháp công nghệ tiên tiến nhằm tăng cường an ninh, bảo mật cho hạ tầng Internet. Trung tâm cũng cung cấp các dịch vụ liên quan đến Internet cho cộng đồng, tổ chức các khóa đào tạo, hội thảo nhằm nâng cao nhận thức và kỹ năng về quản lý, sử dụng tài nguyên Internet.

Trong suốt quá trình hoạt động, VNNIC đã và đang đóng góp quan trọng vào việc thúc đẩy sự phát triển của Internet tại Việt Nam, hỗ trợ doanh nghiệp và người dùng trong việc tiếp cận và khai thác hiệu quả các tài nguyên mạng, từ đó góp phần vào sự phát triển kinh tế, xã hội của đất nước.

## Lịch sử hình thành và phát triển

Lịch sử hình thành và phát triển của Trung tâm Internet Việt Nam (VNNIC) :

Trung tâm Internet Việt Nam (VNNIC) được thành lập vào ngày 28 tháng 4 năm 2000 theo Quyết định số 372/QĐ-TCBĐ của Tổng cục Bưu điện (nay là Bộ Thông tin và Truyền thông). VNNIC ra đời trong bối cảnh Internet đang dần trở thành một yếu tố quan trọng, mở ra kỷ nguyên mới cho công nghệ thông tin và truyền thông tại Việt Nam. Ngay từ khi thành lập, VNNIC đã được giao nhiệm vụ quản lý, cấp phát tài nguyên Internet, bao gồm tên miền quốc gia ".vn" và địa chỉ IP tại Việt Nam.

Giai đoạn đầu (2000-2005): Thiết lập cơ sở hạ tầng và hoạt động ban đầu

Trong những năm đầu hoạt động, VNNIC tập trung vào việc thiết lập cơ sở hạ tầng kỹ thuật cần thiết cho việc quản lý và cấp phát tài nguyên Internet tại Việt Nam. Một trong những thành tựu đáng chú ý là việc triển khai hệ thống đăng ký tên miền ".vn" và cấp phát địa chỉ IP cho các tổ chức trong nước. Đồng thời, VNNIC cũng tích cực tham gia vào các tổ chức quốc tế như APNIC và ICANN, khẳng định vị thế của Việt Nam trên bản đồ Internet toàn cầu.

Giai đoạn phát triển mạnh mẽ (2005-2015): Mở rộng quy mô và dịch vụ

Từ năm 2005, VNNIC bắt đầu mở rộng quy mô hoạt động với việc tăng cường quản lý và phát triển các dịch vụ liên quan đến tài nguyên Internet. Giai đoạn này đánh dấu sự phát triển mạnh mẽ của hệ thống máy chủ tên miền quốc gia (DNS) và triển khai thành công hệ thống quản lý địa chỉ IP phiên bản IPv6. VNNIC cũng đã đẩy mạnh hoạt động đào tạo, tổ chức các hội thảo và sự kiện nhằm nâng cao nhận thức và kỹ năng của cộng đồng về quản lý tài nguyên Internet.

Giai đoạn hiện đại (2015-nay): Đổi mới và hội nhập quốc tế

Trong những năm gần đây, VNNIC đã tập trung vào việc đổi mới và nâng cao chất lượng dịch vụ nhằm đáp ứng nhu cầu ngày càng cao của thị trường và cộng đồng Internet tại Việt Nam. Trung tâm đã triển khai nhiều dự án quan trọng, bao gồm việc xây dựng hệ thống DNSSEC (Domain Name System Security Extensions) nhằm tăng cường an ninh cho hệ thống tên miền quốc gia, và phát triển các giải pháp quản lý tài nguyên Internet dựa trên nền tảng điện toán đám mây.

VNNIC cũng đã tăng cường hợp tác quốc tế, tham gia vào nhiều diễn đàn và tổ chức toàn cầu, đóng góp vào việc xây dựng các tiêu chuẩn và chính sách chung về quản lý tài nguyên Internet. Nhờ những nỗ lực này, VNNIC đã khẳng định vai trò quan trọng của mình trong việc bảo đảm sự ổn định và an toàn cho Internet tại Việt Nam, đồng thời góp phần vào sự phát triển chung của Internet toàn cầu.

## Tầm nhìn, sứ mệnh, giá trị cốt lõi và cơ cấu tổ chức

Tầm nhìn

* Internet kết nối toàn thế giới, bao phủ rộng khắp, an toàn, ổn định, là hạ tầng của chuyển đổi số.
* Việt Nam là quốc gia phát triển về hạ tầng số, Internet; hưởng lợi từ sự phát triển của Internet nhưng đảm bảo lợi ích, chủ quyền quốc gia trên không gian mạng và có sự đóng góp tích cực cho sự phát triển chung của Internet.
* VNNIC tiên phong, dẫn dắt thúc đẩy phát triển Internet Việt Nam, kết nối khu vực.

Sứ mệnh

* Là NIC quốc gia, cung cấp các nền tảng hạ tầng, dịch vụ thiết yếu, tài nguyên Internet (ccTLD, NIR, DNS, Internet Exchange, Whois …) cho hoạt động ổn định, an toàn, phát triển bền vững Internet Việt Nam, bảo vệ chủ quyền quốc gia trên Internet.
* Dẫn dắt, định hướng, cung cấp thông tin tin cậy, dịch vụ mới trên nền tài nguyên Internet; kết nối cộng đồng, thúc đẩy phát triển, đảm bảo an toàn mạng Internet Việt Nam.



Hình .2: Kiến Trúc Tổ Chức của VNNIC

Định Danh : Trái Tim Internet của Việt Nam

VNNIC xây dựng và phát triển trên các giá trị cốt lõi sau:

* Tiên phong và dẫn dắt: Luôn chủ động, sáng tạo và đón đầu xu hướng.
* Đáng tin cậy: Hoạt động dựa trên các chuẩn mực quốc tế, luôn nhận được sự tin cậy từ cộng đồng.
* Văn hóa tổ chức: Tự tin, nhiệt huyết, chu đáo, tinh thần đồng đội và gắn kết cộng đồng.
* Internet for all (IFA): Phát triển Internet trở nên hiện đại, an toàn và kết nối với mọi người, mọi nhà.

VNNIC hướng đến việc phát triển hạ tầng số Việt Nam, đảm bảo an toàn Internet và bảo vệ chủ quyền quốc gia. Với vai trò NIC quốc gia, VNNIC cung cấp tài nguyên và dịch vụ thiết yếu, dựa trên các giá trị tiên phong, tin cậy và kết nối toàn diện.

Tổ chức bộ máy, biên chế của Trung tâm bao gồm Hội đồng quản lý, Ban Giám đốc, 7 Phòng, Ban và 02 Chi nhánh:

- Phòng Tổ chức - Hành chính

- Phòng Tài chính - Kế toán

- Phòng Hợp tác - Quản lý tài nguyên

- Phòng Kỹ thuật

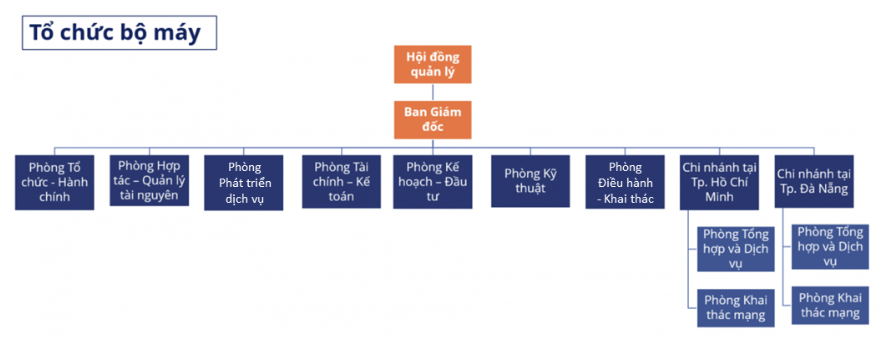
- Phòng Kế hoạch - Đầu tư

- Phòng Phát triển dịch vụ

- Phòng Điều hành - Khai thác

- Chi nhánh tại Thành phố Hồ Chí Minh

- Chi nhánh tại Thành phố Đà Nẵng



Hình .3: Tổ Chức bộ máy trong công ty

Địa chỉ công văn: 18 Nguyễn Du, Phường Bùi Thị Xuân, Quận Hai Bà Trưng, Hà Nội

Trụ sở liên hệ: Tòa nhà Cục Viễn Thông, đường Dương Đình Nghệ, phường Yên Hòa, quận Cầu Giấy, thành phố Hà Nội

Điện thoại: 024.35564944 - Fax: 024. 37821462

Website: <http://www.vnnic.vn>

Chi nhánh tại TP Hồ Chí Minh: Lô U15B-17A, đường số 20, Khu chế xuất Tân Thuận, Quận 7

Chi nhánh tại TP Đà Nẵng: Lô 21, Đường số 7, Khu công nghiệp An Đồn

## Các trụ cột chiến lược phát triển

VNNIC phát triển và thực hiện sứ mệnh dựa trên 07 trụ cột chiến lược.



Hình .4: Bảy Trụ Cột Chiến Lược của VNNIC

1. Hạ tầng (Infrastructure) - Các hạ tầng lõi của mạng Internet Việt Nam: hệ thống DNS quốc gia, Trạm trung chuyển Internet quốc gia VNIX đóng vai trò kết nối liên thông, đảm bảo hoạt động liên tục mạng Internet trong nước, quốc tế. - Hạ tầng CNTT của Bộ được quản lý, vận hành đảm bảo chất lượng, an toàn. - Phát triển hạ tầng hiện đại, đón đầu, chuẩn mực quốc tế. - Đảm bảo an toàn, độc lập của mạng Internet Việt Nam.
2. Quản lý tài nguyên Internet (Registry) - Với vai trò NIC, NIR quốc gia theo mô hình quốc tế, VNNIC đề xuất, xây dựng và thực thi các chính sách về tài nguyên Internet, cung cấp các dịch vụ, nền tảng, ứng dụng, dịch vụ, giám sát trên tài nguyên Internet cho cộng đồng. - Các hoạt động, dịch vụ cung cấp theo mô hình, chuẩn mực quốc tế. Đảm bảo tin cậy, xác thực, hiệu quả trong hoạt động thực tế, thúc đẩy chuyển đổi số. - Tên miền quốc gia “.vn” phổ cập và sử dụng rộng rãi cho người dân, doanh nghiệp và các cơ quan, tổ chức.
3. Mạng lưới thành viên (Membership) - Tổ chức hoạt động của mạng lưới thành viên trên cơ sở tin cậy, cùng xây dựng, phát triển, cung cấp các dịch vụ cho cộng đồng, tham gia xây dựng chính sách, thúc đẩy phát triển. - Các thành viên bao gồm: Các nhà đăng ký tên miền “.vn’’; Các thành viên địa chỉ; Các thành viên VNIX …
4. Cộng đồng (Community) - Xây dựng, dẫn dắt cộng đồng công nghệ (DNS, mạng, dịch vụ) Internet Việt Nam, mở rộng khu vực. - Kết nối cộng đồng, thúc đẩy phát triển, đảm bảo an toàn mạng Internet Việt Nam.
5. Thông tin và thúc đẩy phát triển (Information & Development) - Dữ liệu, thông tin là nhiên liệu để thúc đẩy phát triển và sáng tạo dịch vụ mới). - Dẫn dắt, định hướng, chủ động cung cấp thông tin tin cậy, dịch vụ mới trên nền tài nguyên Internet. - Tổ chức triển khai các hoạt động phát triển nghiên cứu phát triển, đào tạo, xây dựng nguồn lực, cung cấp cho cộng đồng, cơ quan quản lý.
6. Mạng lưới quốc tế (Int’l network) - Là thành viên tích cực, có vai trò trong các tổ chức quốc tế về Internet, khẳng định vị thế, bảo vệ lợi ích quốc gia trong lĩnh vực Internet. - Phối hợp, sử dụng hiệu quả nguồn lực quốc tế trong phát triển Internet Việt Nam.
7. Nguồn lực (Capability) - Nguồn nhân lực nội tại chất lượng cao, cơ chế hợp lý, cạnh tranh, thúc đẩy sáng tạo, phát triển. - Khai thác nguồn lực chuyên gia từ thành viên, cộng đồng. - Đơn vị sự nghiệp tự chủ toàn bộ, chủ động nguồn lực tài chính, không phụ thuộc vào ngân sách, đóng góp trực tiếp vào ngân sách

## Mục tiêu phát triển của công ty

### Mục Tiêu Tổng Quát

Phát triển Internet Việt Nam đạt tầm quốc tế : VNNIC đặt mục tiêu đưa Internet Việt Nam phát triển ngang bằng với các nước tiên tiến trong khu vực và trên thế giới. Điều này không chỉ liên quan đến việc xây dựng hạ tầng số hiện đại và mạnh mẽ mà còn đảm bảo an toàn, độc lập của mạng Internet quốc gia. Bên cạnh đó, VNNIC cam kết bảo vệ chủ quyền quốc gia trên không gian mạng, đóng góp tích cực vào sự phát triển chung của cộng đồng Internet toàn cầu.

Đảm bảo an toàn và độc lập : Một trong những nhiệm vụ trọng tâm của VNNIC là đảm bảo an toàn, bảo mật cho hệ thống mạng Internet Việt Nam. Điều này bao gồm việc phát triển các hệ thống máy chủ tên miền DNS quốc gia với công nghệ và tiêu chuẩn mới nhất, đảm bảo an toàn tuyệt đối cho hoạt động của tên miền quốc gia ".vn", cùng các dịch vụ trực tuyến khác.

Trở thành NIC hàng đầu khu vực : VNNIC đặt mục tiêu trở thành tổ chức quản lý tài nguyên Internet (NIC) số một Đông Nam Á, ngang tầm với các NIC của các quốc gia phát triển trong khu vực Châu Á - Thái Bình Dương và thế giới. Tổ chức sẽ tiên phong và dẫn dắt việc phát triển Internet Việt Nam, đồng thời thúc đẩy kết nối khu vực, cung cấp dịch vụ tốt nhất cho cộng đồng.

Chuyển đổi số toàn diện : VNNIC cam kết thực hiện chuyển đổi số toàn diện từ cốt lõi, bao gồm việc xây dựng mô hình tổ chức và quản trị nội bộ khoa học, minh bạch, và hiệu quả. Tất cả các hệ thống quản lý tài nguyên Internet sẽ được nâng cấp và xây dựng mới, hoạt động trực tuyến, tự động theo yêu cầu quản lý và quy trình nghiệp vụ, phù hợp với các tiêu chuẩn quốc tế.

Phát triển chính sách và hạ tầng số : VNNIC sẽ xây dựng và đổi mới các chính sách, mô hình quản lý tài nguyên Internet phù hợp với xu hướng phát triển toàn cầu. Điều này bao gồm chuẩn bị tài nguyên Internet đáp ứng nhu cầu và xu thế phát triển của công nghệ 5G, IoT và IPv6, từ đó xây dựng hạ tầng số và phát triển hệ sinh thái số Việt Nam.

Phổ cập và thương hiệu hóa tên miền quốc gia ".vn" : VNNIC sẽ thúc đẩy việc sử dụng rộng rãi tên miền quốc gia ".vn", biến nó thành thương hiệu quốc gia phổ biến. Mục tiêu là đưa tên miền này trở thành lựa chọn ưu tiên của công dân và các doanh nghiệp Việt Nam, cũng như khuyến khích cộng đồng chuyển đổi số sử dụng các dịch vụ số "Make In Việt Nam".

Phát triển trạm trung chuyển Internet quốc gia VNIX : VNIX sẽ được phát triển thành hạ tầng số chủ chốt, kết nối các nền tảng số, thúc đẩy phát triển nội dung và hệ sinh thái số Việt Nam. Điều này sẽ hỗ trợ các doanh nghiệp nhỏ/mới tham gia thị trường, đảm bảo an toàn, chất lượng dịch vụ, đồng thời giảm chi phí và giá thành dịch vụ, tạo nền tảng để Việt Nam trở thành trung tâm (HUB) Internet khu vực.

Xây dựng hạ tầng dữ liệu Internet đạt chuẩn quốc tế : VNNIC sẽ phát triển hạ tầng, nền tảng trung tâm dữ liệu Internet theo chuẩn mực quốc tế, nhằm phục vụ triển khai và đảm bảo an toàn cho các hệ thống DNS quốc gia, trạm trung chuyển Internet quốc gia VNIX, quản lý tài nguyên Internet quốc gia và cung cấp các dịch vụ cho cộng đồng.

Kết nối và phát triển cộng đồng Internet : VNNIC sẽ xây dựng và dẫn dắt cộng đồng Internet Việt Nam trên tinh thần tin cậy, kết nối, chia sẻ và cùng phát triển. VNNIC cũng sẽ gắn kết với cộng đồng Internet quốc tế, hợp tác song phương bình đẳng với các tổ chức quốc tế, từ đó sáng tạo ra các giá trị mới.

Đảm bảo tự chủ và phát triển bền vững : VNNIC sẽ đảm bảo nguồn lực tự chủ hoàn toàn, đảm bảo sự phát triển bền vững và chủ động trong mọi hoạt động của tổ chức.

### Mục Tiêu Cụ Thể

Hoàn thiện hành lang pháp lý cho tên miền ".vn" : VNNIC sẽ hoàn thiện các quy định pháp lý mở rộng không gian phát triển cho tên miền quốc gia ".vn", bao gồm việc bổ sung các quy định về quản lý đăng ký và sử dụng tên miền quốc tế, cũng như dịch vụ xuyên biên giới.

Chuyển đổi mạng Internet sang IPv6 : VNNIC đặt mục tiêu chuyển đổi hoàn toàn mạng Internet Việt Nam sang IPv6, với 100% người sử dụng Internet truy cập qua IPv6 và 100% các Bộ, Ngành, địa phương ban hành và thực hiện thành công kế hoạch chuyển đổi IPv6. Việt Nam sẽ đứng vào top 10-20 quốc gia có tỷ lệ chuyển đổi IPv6 cao nhất thế giới.

Mở rộng và phát triển tên miền ".vn" : VNNIC đặt mục tiêu đạt tối thiểu 1 triệu tên miền ".vn" vào năm 2025, và xây dựng chính sách hỗ trợ để đạt từ 3 đến 4 triệu tên miền. Việt Nam sẽ duy trì vị trí số 1 trong khối ASEAN, top 10 Châu Á - Thái Bình Dương và top 20-30 quốc gia có số lượng tên miền mã quốc gia lớn nhất trên thế giới. Tên miền ".vn" sẽ chiếm ưu thế, với tỷ lệ tên miền ".vn" so với tên miền quốc tế đạt ít nhất 60/40.

Phát triển hệ thống VNIX : VNNIC sẽ mở rộng số lượng thành viên kết nối với VNIX, mục tiêu đạt từ 110 đến 165 thành viên, chiếm 20-30% tổng số thành viên số hiệu mạng AS ở Việt Nam. VNIX sẽ được mở rộng tại 5 trung tâm dữ liệu lớn nhất tại Việt Nam và kết nối với các IX trong khu vực.

Đảm bảo chất lượng và an toàn hệ thống kỹ thuật : Các hệ thống kỹ thuật quan trọng như DNS, VNIX sẽ đạt mức SLA 99,999% và được chứng nhận ISO 27001. Các hệ thống quản lý tài nguyên Internet sẽ được xây dựng để đảm bảo tương thích hoàn toàn với các chuẩn quốc tế.

Xác thực và giám sát mạng Internet : VNNIC sẽ đảm bảo hoạt động của mạng Internet Việt Nam được xác thực và giám sát bởi các hệ thống, nền tảng quản lý tài nguyên theo chuẩn quốc tế. Điều này sẽ bao gồm việc vận hành, giám sát, và đánh giá hiệu quả hoạt động qua các nền tảng như VNNIC Internet Atlas và i-Speed. Các điểm đo và giám sát sẽ được đặt tại 100% mạng của top 10 các ISP, IDC và Cloud tại Việt Nam, với mục tiêu đạt 45-50 điểm đo.

Xây dựng và duy trì các hoạt động cộng đồng : VNNIC sẽ chủ trì xây dựng và duy trì các hoạt động cộng đồng thường niên, đồng thời xây dựng mạng lưới chuyên gia Internet có tổ chức thông qua các sự kiện như VNNIC Internet Conference, VNNIC Internet Academy, VNIX-NOG, VN-NOG.

Tham gia và dẫn dắt các tổ chức quốc tế về Internet : VNNIC sẽ là thành viên đầy đủ của các tổ chức quốc tế về Internet, đồng thời liên kết và tham gia các vị trí quan trọng trong các tổ chức như APNIC, ICANN, APTLD, APIX. Tổ chức cũng sẽ đàm phán để tổ chức tối thiểu một sự kiện quốc tế lớn của các tổ chức này tại Việt Nam.

Tự chủ và mở rộng các hoạt động dịch vụ sự nghiệp : VNNIC cam kết đảm bảo tự chủ hoàn toàn trong hoạt động, đồng thời mở rộng các dịch vụ sự nghiệp. Tổ chức đặt mục tiêu tăng thu từ 7-10% và hoàn thành 100% nghĩa vụ tài chính, tăng thu ngân sách nhà nước.

## Nhiệm vụ trọng tâm của VNNIC

Nhiệm vụ trọng tâm của VNNIC trong việc đổi mới tổ chức, quản trị và truyền thông bao gồm nhiều hoạt động quan trọng nhằm đảm bảo sự phát triển bền vững và hiệu quả của tổ chức. Các nhiệm vụ chính được liệt kê như sau:

Đổi mới tổ chức, quản trị và truyền thông :

* Điều chỉnh tên/chức năng của các đơn vị trong Trung tâm để phù hợp với chiến lược phát triển và các nhiệm vụ được giao.
* Cập nhật, ban hành mới các quy chế nội bộ nhằm tháo gỡ các hạn chế và thu hút nhân lực chất lượng cao.
* Áp dụng các mô hình quản trị hiện đại như OKR, tổ chức mềm, và xây dựng môi trường làm việc sáng tạo, cạnh tranh.
* Thực hiện chuyển đổi số toàn diện trên các trụ cột: Con người, Chính sách/quy trình, Công nghệ.
* Triển khai chương trình truyền thông để lan tỏa cộng đồng và thúc đẩy phát triển.
* Phát triển nguồn nhân lực chất lượng cao :
* Ban hành đề án vị trí việc làm và kế hoạch phát triển nhân lực có chuyên môn cao.
* Thiết lập quy chế trả thu nhập theo vị trí việc làm để thu hút nhân lực chất lượng.
* Tăng cường năng lực đội ngũ thông qua đào tạo, phổ cập kỹ năng số và an ninh mạng.
* Phát triển đội ngũ chuyên gia có ảnh hưởng trong nước và quốc tế.
* Xây dựng, đổi mới chính sách, tiêu chuẩn, hướng dẫn :
* Đánh giá và điều chỉnh hành lang pháp lý, tập trung vào các chính sách đột phá.
* Xây dựng các tiêu chuẩn và hướng dẫn liên quan đến tài nguyên Internet và kết nối Internet.
* Tổ chức các chương trình đào tạo và tập huấn.
* Đảm bảo an toàn, độc lập của mạng Internet Việt Nam :
* Xây dựng và thử nghiệm các giải pháp kỹ thuật mới.
* Đàm phán với các tổ chức quốc tế để đưa hệ thống DNS Root về Việt Nam.
* Phát triển các giải pháp chống tấn công DDoS cho các thành viên VNIX.
* Thúc đẩy hệ sinh thái số Việt Nam và các kết nối trao đổi lưu lượng trong nước.
* Đảm bảo chất lượng, an toàn hệ thống DNS quốc gia “.vn” :
* Ban hành quy định quản lý an toàn thông tin hệ thống kỹ thuật và dịch vụ, tuân thủ các tiêu chuẩn quốc tế.
* Đầu tư phát triển hạ tầng kỹ thuật và tăng cường phương án bảo vệ an toàn hệ thống DNS, VNIX.
* Tổ chức đảm bảo an toàn thông tin theo mô hình 4 lớp và thực hiện SLA với mục tiêu đạt 99,999%.
* Phát triển các hạ tầng, nền tảng lõi, ứng dụng phát triển Internet
* Phát triển hệ thống DNS quốc gia và trạm trung chuyển Internet quốc gia VNIX theo tiêu chuẩn quốc tế.
* Nâng cấp nền tảng quản lý tên miền “.vn” và xây dựng nền tảng quản lý IP, định tuyến Internet theo chuẩn quốc tế.
* Triển khai nền tảng thu thập, phân tích dữ liệu lớn và xây dựng hồ dữ liệu về tài nguyên Internet.
* Phát triển tài nguyên Internet, VNIX, các dịch vụ, mở rộng thị trường:
* Xây dựng thương hiệu tên miền quốc gia “.vn” và đẩy mạnh truyền thông, quảng bá.
* Mở rộng và hỗ trợ sử dụng hiệu quả tài nguyên địa chỉ IP, phát triển thị trường và tăng số lượng thành viên kết nối VNIX.
* Cung cấp dịch vụ đăng ký, duy trì tài nguyên Internet theo chuẩn mực quốc tế.
* Dẫn dắt, thúc đẩy chuyển đổi Internet Việt Nam sang IPv6 :
* Thúc đẩy chuyển đổi mạng Internet Việt Nam sang IPv6 và nâng cao thứ hạng quốc gia.
* Ban hành và triển khai Chương trình IPv6 For Gov và hỗ trợ các tổ chức, doanh nghiệp trong việc chuyển đổi sang IPv6.

Các nhiệm vụ trên nhằm đảm bảo VNNIC phát triển mạnh mẽ, thích ứng với xu thế mới và đóng góp vào sự phát triển của Internet Việt Nam.

# NGHIÊN CỨU KIẾN TRÚC VÀ CÔNG NGHỆ ANSIBLE – PROMETHEUS – GRAFANA

## Giới thiệu chương

Trong chương này, báo cáo tập trung trình bày cơ sở lý thuyết và nguyên lý hoạt động của các công cụ được sử dụng trong đề tài, bao gồm Ansible – công cụ tự động hóa cấu hình, và Prometheus – Grafana – bộ công cụ giám sát và trực quan hóa dữ liệu. Nội dung chương sẽ giúp làm rõ vai trò, kiến trúc, các thành phần chính và khả năng tích hợp giữa chúng để tạo thành một giải pháp hoàn chỉnh cho việc tự động hóa và giám sát hệ thống mạng.

## Tổng quan về Ansible

### Khái niệm và vai trò

Ansible là một công cụ mã nguồn mở dùng để tự động hóa cấu hình hệ thống, triển khai phần mềm và quản lý hạ tầng CNTT. Với cơ chế hoạt động theo mô hình agentless (không cần cài đặt phần mềm client trên máy đích), Ansible giúp giảm thiểu sự phức tạp trong quản trị hệ thống mạng và máy chủ.



Hình .1: Logo Ansible

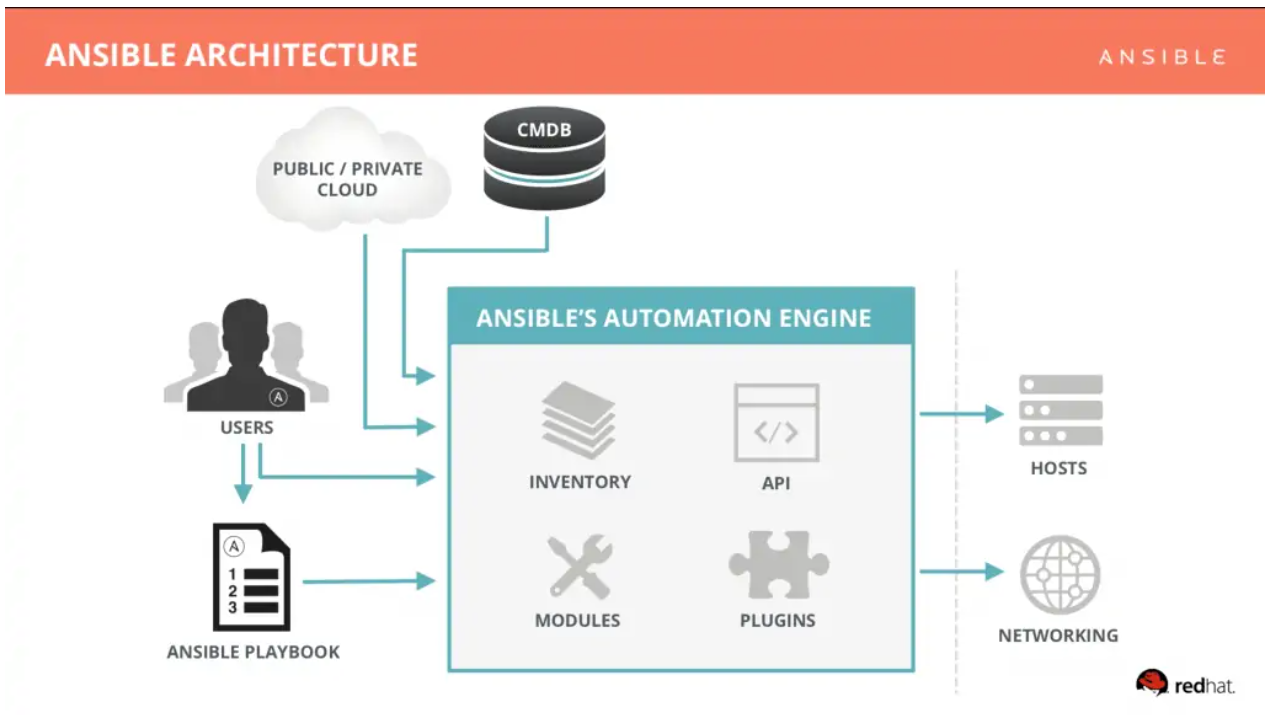
Vai trò của Ansible trong hệ thống mạng:

* Tự động hóa cấu hình thiết bị (router, switch, firewall, máy chủ).
* Quản lý tập trung, giảm thiểu sai sót do thao tác thủ công.
* Tái sử dụng kịch bản (playbook) giúp tiết kiệm thời gian triển khai.

### Kiến trúc Ansible

Ansible gồm các thành phần chính:

* Control Node: máy chủ quản lý, nơi cài đặt Ansible và chạy playbook.
* Managed Node: các thiết bị/ máy chủ được quản lý.
* Inventory: tệp lưu trữ danh sách các máy chủ/thiết bị cần quản lý.
* Playbook: tệp YAML định nghĩa các tác vụ tự động hóa.
* Module: tập hợp các chức năng được Ansible cung cấp sẵn (cấu hình dịch vụ, sao lưu, quản lý user,…).



Hình .2: Kiến trúc của Ansible

Ansible hoạt động thông qua giao thức SSH (Linux) hoặc WinRM (Windows), không cần cài đặt agent.

### Ưu điểm của Ansible

Dễ học, dễ triển khai.

Không cần agent, giảm tải tài nguyên trên thiết bị.

Có thể mở rộng và tích hợp với nhiều công cụ DevOps.

Hỗ trợ đa dạng hệ điều hành và thiết bị mạng.

## GIỚI THIỆU TỔNG QUAN VỀ PROMETHEUS VÀ GRAFANA

Prometheus và Grafana là hai công cụ mã nguồn mở phổ biến được sử dụng trong giám sát hạ tầng CNTT và cảnh báo mạng.



Hình .3: Logo Prometheus

Prometheus đóng vai trò thu thập và lưu trữ dữ liệu dạng chuỗi thời gian (time series), đồng thời cung cấp cơ chế cảnh báo linh hoạt thông qua Alertmanager.



Hình .4: Logo Grafana

Grafana đảm nhiệm việc trực quan hóa dữ liệu, hiển thị biểu đồ và dashboard, giúp người quản trị dễ dàng theo dõi tình trạng hệ thống.

Sự kết hợp của hai công cụ này mang đến giải pháp giám sát hiện đại, nhẹ, linh hoạt và dễ mở rộng, phù hợp cho cả doanh nghiệp vừa và lớn.

### Kiến trúc và cơ chế hoạt động của Prometheus

Prometheus được dùng để giám sát hệ thống thông qua các daemon cài sẵn trên các node, qua đó thu thập các thông tin cần thiết. Prometheus giao tiếp với node qua giao thức http/https và lưu trữ data theo dạng time-series database (TSDB).

Time series database (TSDB) là những database được lưu trữ theo các mốc thời gian. Nghĩa là mỗi dữ liệu luôn được gắn với một mốc thời gian nhất đinh từ đó tạo thành chuỗi dữ liêu theo thời gian từ đó giúp chúng ta có thể xem lại dữ liệu cho một khoảng thời gian 1 giờ hay 1 tiếng.

### Thành phần chính của Prometheus

Prometheus bao gồm các thành phần cốt lõi sau:

Prometheus Server: Thành phần trung tâm, chịu trách nhiệm thu thập, lưu trữ dữ liệu và xử lý truy vấn PromQL.

Exporter: Ứng dụng hoặc plugin giúp xuất dữ liệu từ hệ thống hoặc dịch vụ (như Node Exporter cho máy chủ, Blackbox Exporter cho HTTP/TCP ping, v.v.).

Alertmanager: Thành phần quản lý cảnh báo, gửi thông báo qua email, Slack, webhook,… khi xảy ra sự cố.

Pushgateway (tùy chọn): Cho phép nhận dữ liệu từ các ứng dụng không thể bị Prometheus “pull” trực tiếp, ví dụ job chạy ngắn hạn.

PromQL (Prometheus Query Language): Ngôn ngữ truy vấn dữ liệu mạnh mẽ để phân tích và lọc thông tin theo yêu cầu.

### Kiến trúc hoạt động của Prometheus



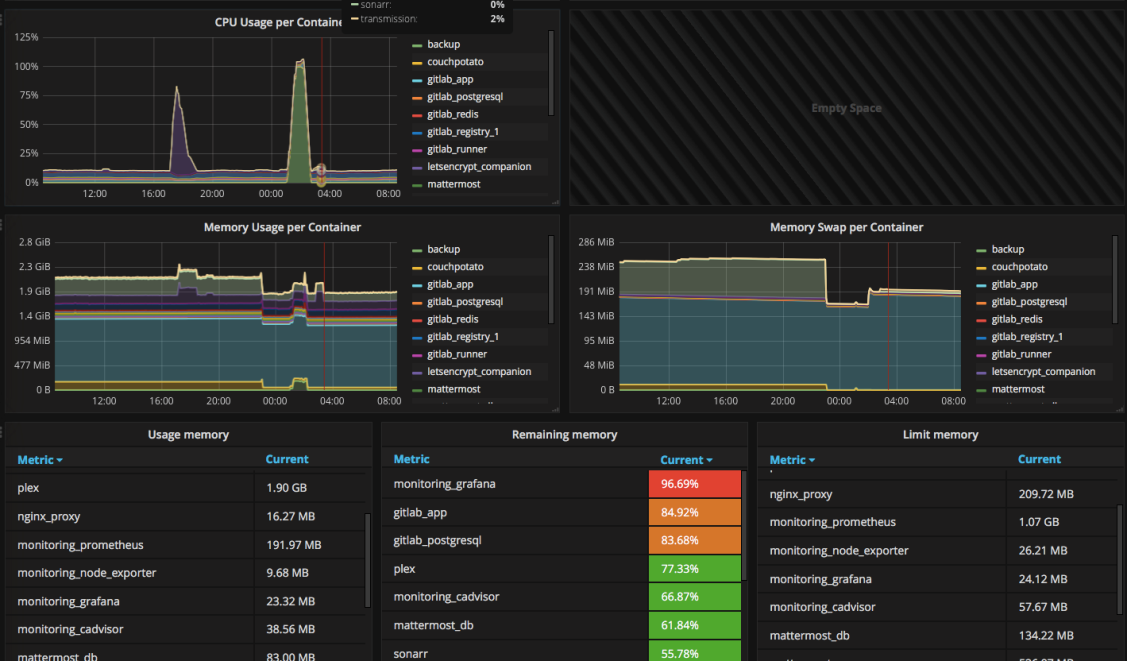
Hình .5: Kiến trúc hoạt động của Prometheus

Kiến trúc của Prometheus hoạt động theo mô hình pull-based:

* Prometheus Server định kỳ “kéo” dữ liệu từ các exporter thông qua HTTP endpoint.
* Dữ liệu được lưu trữ dưới dạng chuỗi thời gian trong cơ sở dữ liệu nội bộ TSDB (Time Series Database).
* Khi xảy ra sự kiện vượt ngưỡng đã cấu hình, Alertmanager sẽ gửi cảnh báo tới người quản trị.
* Người dùng sử dụng PromQL để truy vấn hoặc kết hợp với Grafana để hiển thị trực quan.

### Giới thiệu chi tiết về Grafana

Grafana là một vizualizer hiển thị các metric dưới dạng các biểu đồ (chart) hoặc đồ thị (graph), được tập hợp lại thành dashboard có tính tùy biến cao, giúp dễ dàng theo dõi tình trạng của node. Đơn giản cho các bạn dễ hiểu là sau khi lấy được metric từ các thiết bị, grafana sẽ sử dụng metric đó để phân tích và tạo ra dashboard mô tả trực quan các metric cần thiết cho việc monitoring như CPU, RAM, disks, IO operations...



Hình 2.6: Grafana DashBoard

Chức năng chính:

* Tích hợp nhiều nguồn dữ liệu: Prometheus, InfluxDB, MySQL, ElasticSearch,…
* Trực quan hóa dữ liệu bằng dashboard tùy chỉnh.
* Cung cấp cơ chế cảnh báo ngay trong giao diện đồ họa.
* Hỗ trợ quản lý người dùng, phân quyền và chia sẻ dashboard.

Vai trò trong hệ thống giám sát:

Grafana không thực hiện việc thu thập dữ liệu, mà đóng vai trò hiển thị thông tin từ các nguồn dữ liệu khác nhau. Trong mô hình Prometheus – Grafana:

* Prometheus chịu trách nhiệm lưu trữ và cung cấp dữ liệu.
* Grafana truy vấn dữ liệu từ Prometheus và hiển thị biểu đồ trực quan.

## Mối quan hệ và tích hợp giữa Ansible – Prometheus – Grafana

Ansible: đảm nhận vai trò tự động hóa cấu hình thiết bị mạng và hệ thống.

Prometheus: giám sát tình trạng thiết bị và dịch vụ sau khi được cấu hình.

Grafana: trực quan hóa dữ liệu thu thập từ Prometheus, giúp quản trị viên theo dõi tình trạng hệ thống dễ dàng.

Khi kết hợp:

* Ansible triển khai và cấu hình hệ thống.
* Prometheus giám sát các dịch vụ, thiết bị đã được cấu hình.
* Grafana cung cấp dashboard để quản trị viên quan sát trạng thái mạng.
* Alertmanager gửi cảnh báo khi phát hiện sự cố.

Mô hình này giúp doanh nghiệp có giải pháp toàn diện: vừa tự động hóa cấu hình, vừa giám sát liên tục, vừa cảnh báo kịp thời.

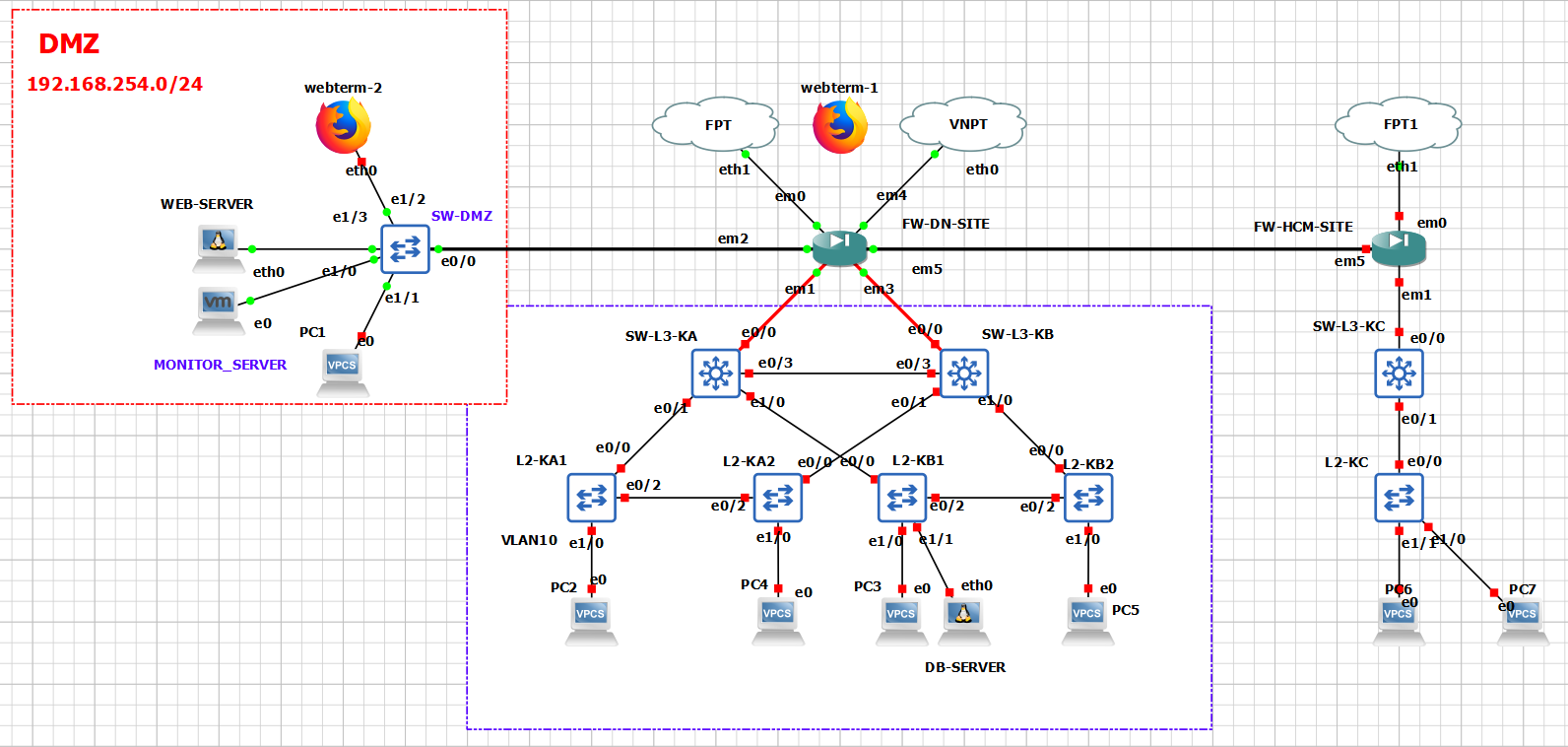
## Kết luận chương

Chương này đã trình bày tổng quan về Ansible, Prometheus và Grafana, các thành phần kiến trúc, vai trò và ưu điểm. Đồng thời, nội dung cũng chỉ ra cách thức kết hợp các công cụ này để hình thành hệ thống quản lý mạng hiệu quả. Đây là nền tảng lý thuyết quan trọng cho quá trình triển khai thực tế được trình bày ở Chương 3.

# XÂY DỰNG VÀ TRIỀN KHAI LAB

## Thiết kế mô hình lab

Hệ thống được thiết kế nhằm tự động hóa việc cấu hình và giám sát các thiết bị trong mạng, đồng thời giảm thiểu thao tác thủ công của quản trị viên. Các thành phần chính bao gồm:



Hình .1. Sơ đồ mô hình hệ thống

Ansible: Công cụ tự động hóa cấu hình và quản lý tập trung.

Teleport Server: Hỗ trợ xác thực, quản lý truy cập và kết nối an toàn đến các thiết bị/host.

DB Server & Client: Được phân bố trong các VLAN khác nhau.

Switch DMZ: Quản lý kết nối đến vùng DMZ, nơi chứa các dịch vụ công khai và giám sát.

Monitor Server (192.168.254.254/24): Đóng vai trò theo dõi hoạt động mạng và tài nguyên hệ thống, được đặt trong vùng DMZ.

Teleport Server chỉ phục vụ nội bộ, các người dùng có quyền sẽ có thể truy cập

### Phân vùng mạng chi tiết:

#### Vùng LAN (quản lý qua switch L3)

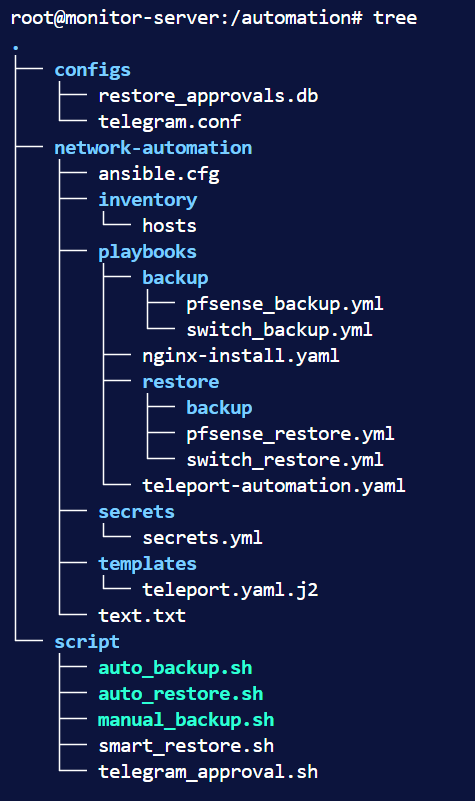
|  |  |  |
| --- | --- | --- |
| SWITCH | Địa chỉ IP | Mô tả |
| SW-L3-KA  SW-L3-KB | 10.10.20.1 | Switch core layer 3 khu A - B |
| SW-L2-KA1  SW-L2-KA2 | 192.168.10.2  192.168.20.2 | Switch layer 2 khu A |
| SW-L2-KB1  SW-L2-KB2 | 192.168.30.2  192.168.40.2 | Switch layer 2 khu B |

#### Vùng DMZ

|  |  |  |
| --- | --- | --- |
| Thành phần | Địa chỉ IP | Mô tả |
| Switch DMZ | 192.168.254.1 | Quản lý thiết bị vùng DMZ |
| Monitor Server | 192.168.254.254 | Giám sát hệ thống |
| Teleport Server | 192.168.254.100 | Nội bộ phục vụ người dùng |

## Triển khai hệ thống tự động hóa với Ansible

### Cấu trúc thư mục làm việc



Hình .2: Cấu trúc thư mục làm việc

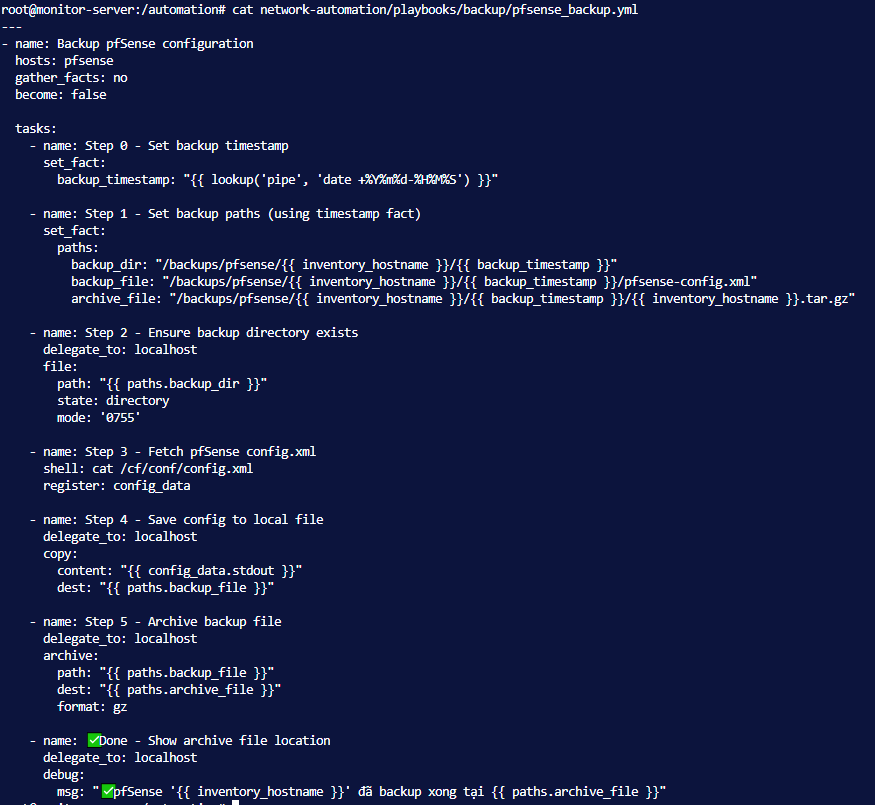
### Tự động hóa backup thiết bị mạng

Trong hệ thống, việc backup cấu hình của các thiết bị mạng (router, switch, firewall) là vô cùng quan trọng để đảm bảo khả năng khôi phục khi xảy ra sự cố. Để loại bỏ thao tác thủ công và giảm thiểu rủi ro, nhóm đã triển khai cơ chế backup hoàn toàn tự động sử dụng Ansible kết hợp với Shell script.

1. Playbook backup pfSense:

Nhiệm vụ của playbook pfsense\_backup.yml là thu thập file cấu hình config.xml từ thiết bị pfSense, lưu trữ vào thư mục “/backups/pfsense/<hostname>/<timestamp>/” và nén lại thành file .tar.gz.

Quá trình này đảm bảo mỗi lần backup đều có bản lưu trữ riêng biệt với dấu thời gian (timestamp), dễ dàng quản lý và phục hồi.



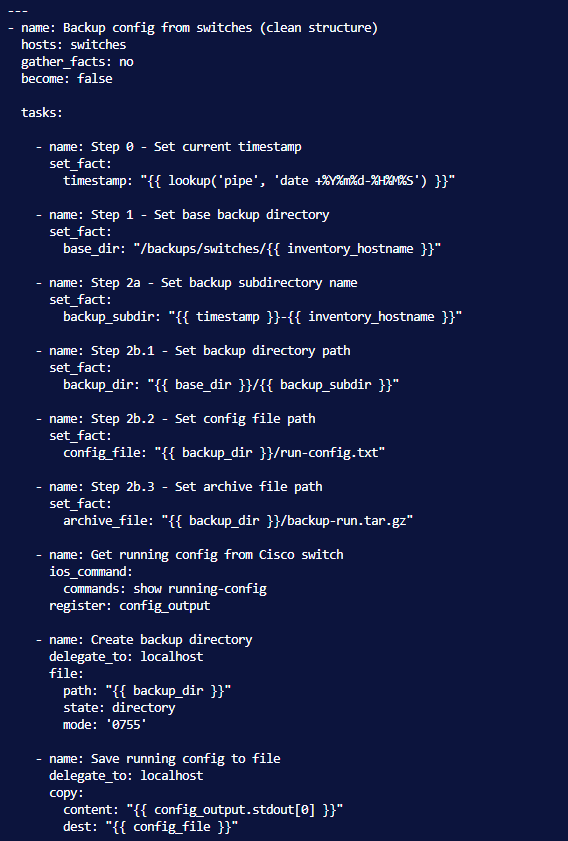
Hình .3: File Playbook backup Pfsense

b) Playbook backup Switch

Với switch Cisco, playbook switch\_backup.yml sử dụng module ios\_command để trích xuất running-config của thiết bị.

File cấu hình sau đó được lưu vào thư mục /backups/switches/<hostname>/<timestamp>/ và nén lại để dễ quản lý.

Việc phân chia thư mục theo thiết bị và thời gian giúp việc tra cứu, so sánh cấu hình ở các thời điểm khác nhau trở nên thuận tiện.



Hình .4: File Playbook backup switch

c) Script tự động hóa backup (auto\_backup.sh)

Để đảm bảo quá trình backup diễn ra định kỳ và hoàn toàn tự động, một script Bash (auto\_backup.sh) được xây dựng với các chức năng chính:

Đọc danh sách thiết bị từ file inventory của Ansible.

Thực thi các playbook backup tương ứng cho pfSense và switches.

Ghi log chi tiết quá trình backup vào /var/log/backups\_auto/auto\_backup.log.

Xuất kết quả backup dưới dạng Prometheus metrics trong file /var/lib/node\_exporter/textfile\_collector/auto\_backup\_status.prom, bao gồm:

auto\_backup\_status: trạng thái backup (0 = thành công, 1 = thất bại).

auto\_backup\_duration: thời gian thực hiện backup cho từng host.

### Tự động tích hợp với Teleport Server

Để giảm thiểu thao tác thủ công và đảm bảo tính nhất quán khi triển khai nhiều máy chủ, nhóm tiến hành xây dựng **Ansible Playbook** nhằm tự động cài đặt và tích hợp các node vào Teleport Server. Quy trình được thực hiện như sau:

1. Cài đặt gói phụ thuộc: Trên các hệ thống Debian/Ubuntu, playbook sẽ tự động cài đặt công cụ curl phục vụ quá trình tải script cài đặt Teleport.
2. Kiểm tra trạng thái Teleport: Playbook kiểm tra xem binary teleport đã tồn tại trên hệ thống chưa. Nếu chưa có, nó sẽ tải và chạy script cài đặt từ Teleport Server thông qua HTTPS, đồng thời sử dụng token đã cấu hình sẵn để đăng ký node.
3. Triển khai file cấu hình Teleport: Một file template teleport.yaml.j2 được sử dụng để sinh file cấu hình chính /etc/teleport/teleport.yaml. File này chứa:

* nodename: tên node, lấy tự động từ hostname của hệ thống.
* auth\_server: địa chỉ Teleport Server và cổng xác thực (3025).
* auth\_token: token dùng để đăng ký node.
* ssh\_service: bật dịch vụ SSH để Teleport có thể quản lý và truy cập node.

1. Cấu hình dịch vụ systemd: Playbook tạo service teleport.service trong /etc/systemd/system/, chỉ định đường dẫn binary Teleport và file cấu hình. Các handlers được gọi để reload daemon, enable và khởi động lại dịch vụ.
2. Tự động hoá quá trình đăng ký node: Sau khi hoàn tất, node sẽ tự động kết nối tới Teleport Server, xác thực bằng token và xuất hiện trong Teleport Web UI. Quản trị viên không cần thao tác thủ công cài đặt hay cấu hình trên từng node riêng lẻ.



Hình .5: File Playbook tự động tích hợp với Teleport Server

Với cơ chế này, việc mở rộng hạ tầng trở nên đơn giản: chỉ cần thêm node mới vào inventory của Ansible, chạy playbook, node sẽ tự động cài đặt Teleport, cấu hình, và kết nối tới Teleport Server.

### Tự động hóa cài đặt dịch vụ Nginx

Trong mô hình triển khai, Ansible được sử dụng để tự động hóa quá trình cài đặt và quản lý dịch vụ Nginx trên các máy chủ cần thiết. Thay vì phải đăng nhập thủ công vào từng máy chủ để thực hiện lệnh cài đặt, playbook Ansible sẽ giúp:

* Kiểm tra tình trạng Nginx có sẵn trên hệ thống.
* Nếu chưa có, Ansible sẽ tự động cài đặt Nginx.
* Đảm bảo dịch vụ Nginx luôn được kích hoạt và khởi động cùng hệ thống.
* Cung cấp báo cáo trạng thái sau khi cài đặt, bao gồm phiên bản Nginx và trạng thái dịch vụ.



Hình .6: File Playbook tự động cài đặt Nginx

## Cấu hình Prometheus thu thập metric

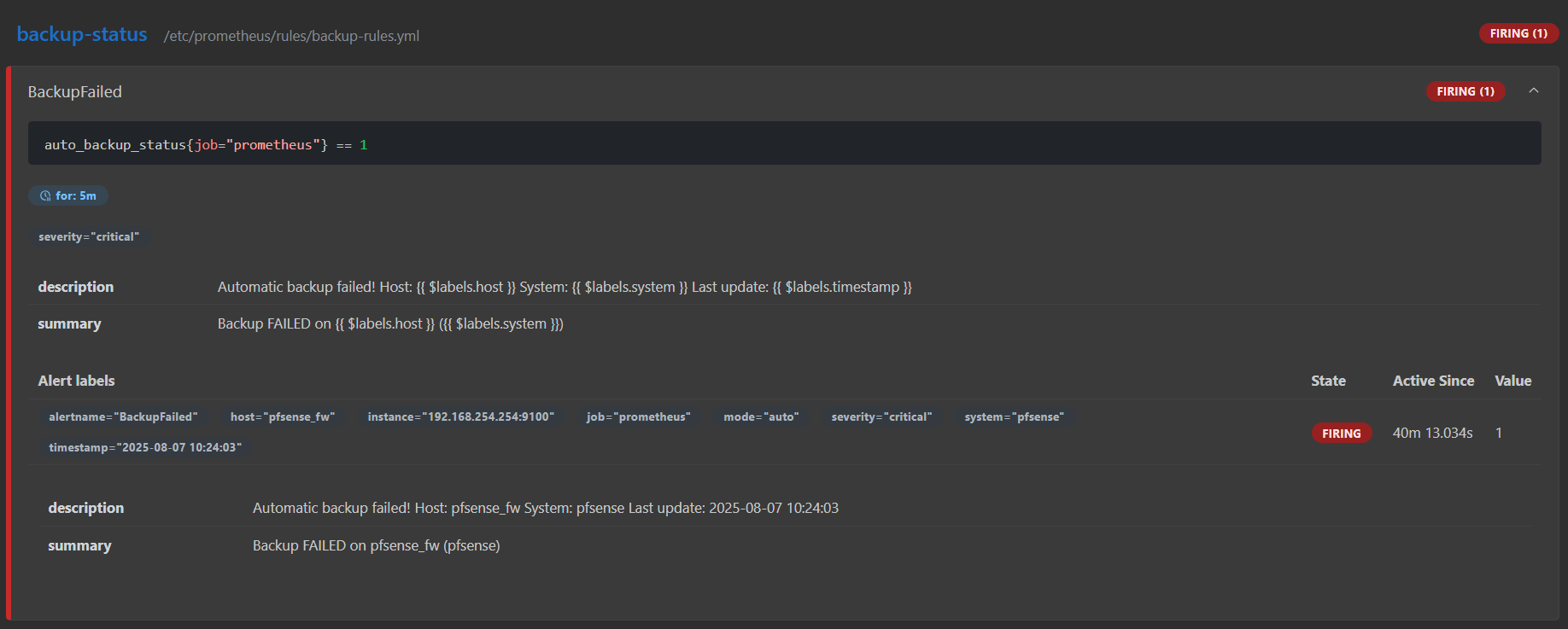
### Thu thập trạng thái backup của thiết bị:

Khi backup thành công hoặc thất bại, sẽ lưu metrics vào file “/var/lib/node\_exporter/textfile\_collector/auto\_backup\_status.prom”

auto\_backup\_status{host="pfsense\_fw",system="pfsense",mode="auto",timestamp="2025-08-07 10:24:03"} 1

Lưu ở dạng:

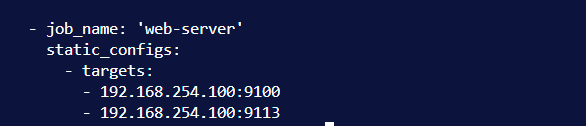
* auto\_backup\_status → trạng thái của backup (1 = thành công, 0 = thất bại).
* auto\_backup\_duration → thời gian chạy backup (tính bằng giây).
* Các label (host, system, mode, timestamp) giúp phân biệt host nào, loại thiết bị nào, chạy lúc nào.



Hình .7: Trạng thái backup của thiết bị

### Thu thập trạng thái của dịch vụ Nginx:

Sử dụng file Prometheus.yml để kết nối đến node\_exporter và nginx\_exporter trên các thiết bị cài đặt dịch vụ



Hình .8: Cấu hình trên Prometheus.yml

Để thu thập dữ liệu giám sát từ các dịch vụ trong hệ thống, Prometheus được cấu hình kết hợp với các Exporter chuyên dụng:

Node Exporter: Thu thập các metric về hệ thống (CPU, RAM, Disk, Network, Process, Load Average, v.v.).

Nginx Exporter: Thu thập trạng thái và thông số từ dịch vụ Nginx (Active connections, Request rate, Reading/Writing/Waiting connections, v.v.).

Các exporter này chạy dưới dạng tiến trình riêng và cung cấp dữ liệu qua các endpoint /metrics mà Prometheus sẽ định kỳ scrape để lưu trữ và hiển thị trên Grafana.



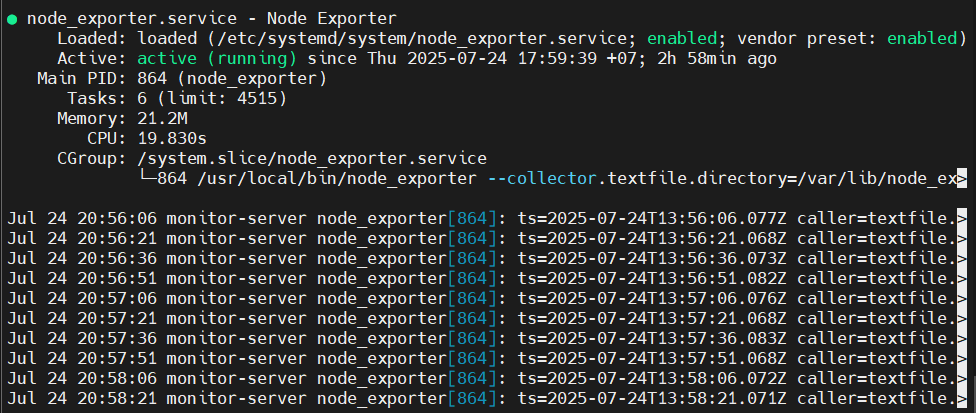
Hình .9: Trạng thái hiển thị của Nginx

### Thu thập sử dụng node\_exporter

Cài đặt node\_exporter trên từng thiết bị cần được giám sát

* cd /tmp
* wget https://github.com/prometheus/node\_exporter/releases/download/v1.7.0/node\_exporter-1.7.0.linux-amd64.tar.gz
* tar xvf node\_exporter-1.7.0.linux-amd64.tar.gz
* sudo mv node\_exporter-1.7.0.linux-amd64/node\_exporter /usr/local/bin/
* sudo useradd --no-create-home --shell /bin/false node\_exporter
* sudo chown node\_exporter:node\_exporter /usr/local/bin/node\_exporter

Tạo file dịch vụ và kiểm tra trạng thái



Hình .10. Kiểm tra trạng thái hoạt động của node\_exporter

### Thu thập sử dụng giao thức SNMP

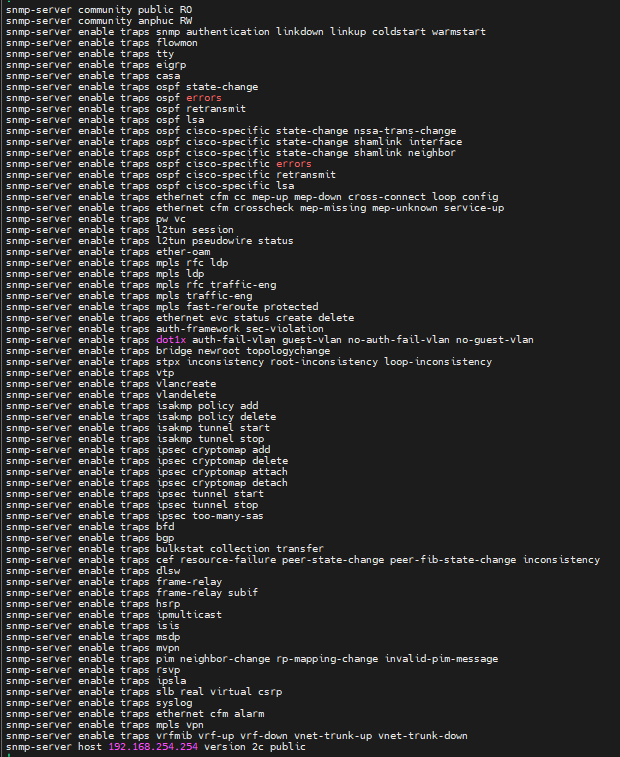
Xác định và cấu hình các thiết bị cần được cấu hình SNMP, như switch, firewall

1. Trên switch cisco

Cấu hình SNMP sử dụng các câu lệnh:

* snmp-server community public RO
* snmp-server community anphuc RW
* snmp-server host 192.168.254.254 public
* snmp-server enable traps

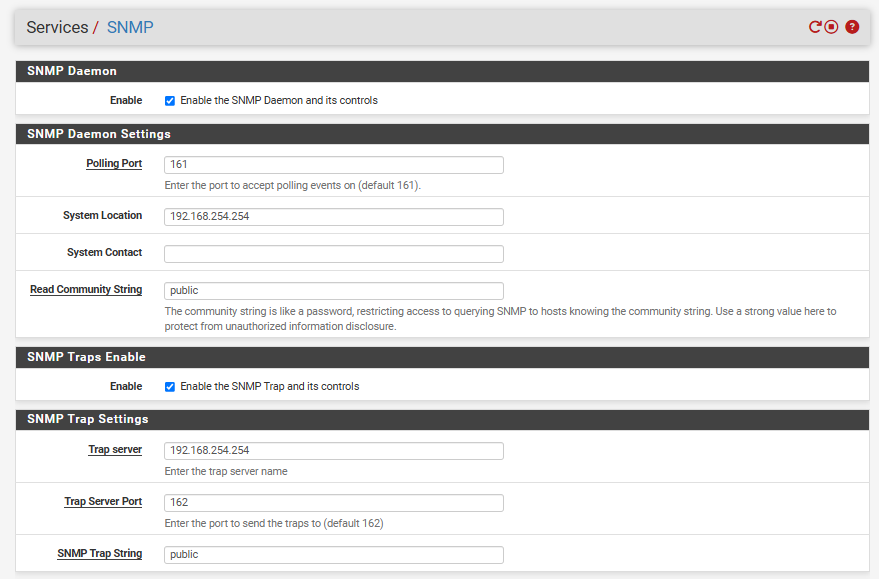
Kiểm tra thông tin:



Hình .11. Kiểm tra cấu hình

1. Trên firewall pfsense

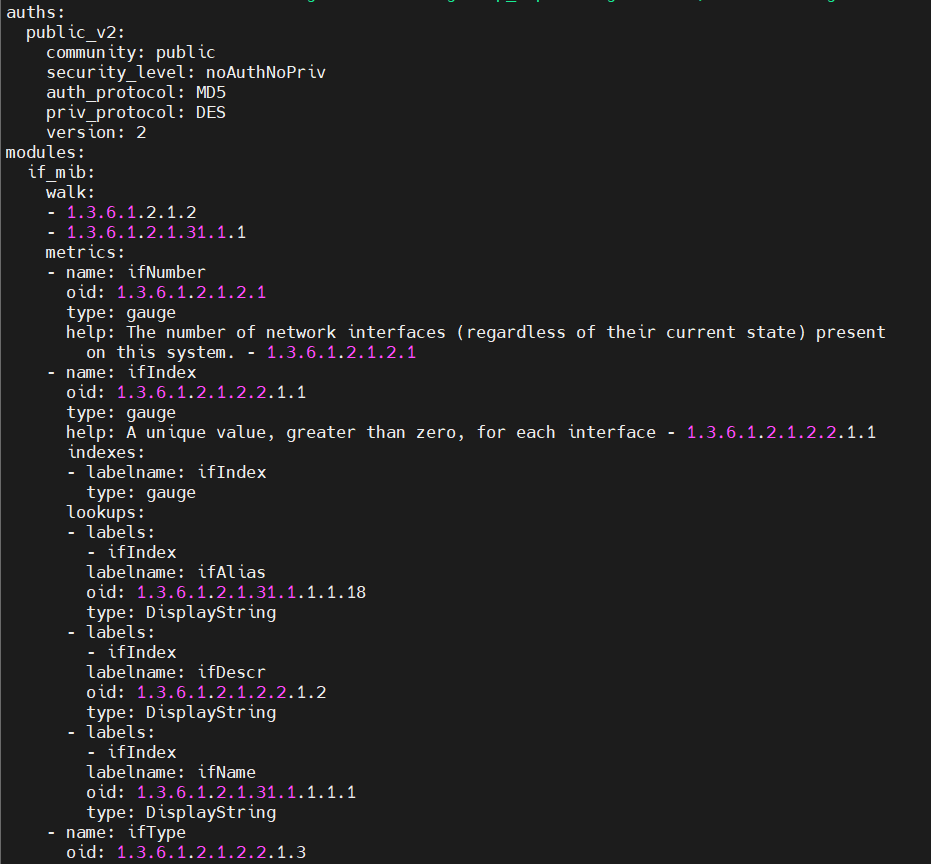
Vào Services -> SNMP



Hình .12. Cấu hình SNMP trên Pfsense

Bật trạng thái SNMP, sử dụng port 161 mặc định, snmp server 192.168.254.254 và community string là public

Sau khi đã cấu hình snmp xong thì ta cần tạo file /etc/prometheus/snmp.yml để lưu các metric thành 1 module để dễ dàng cấu hình



Hình .13. Gom các metrics thành các module phù hợp

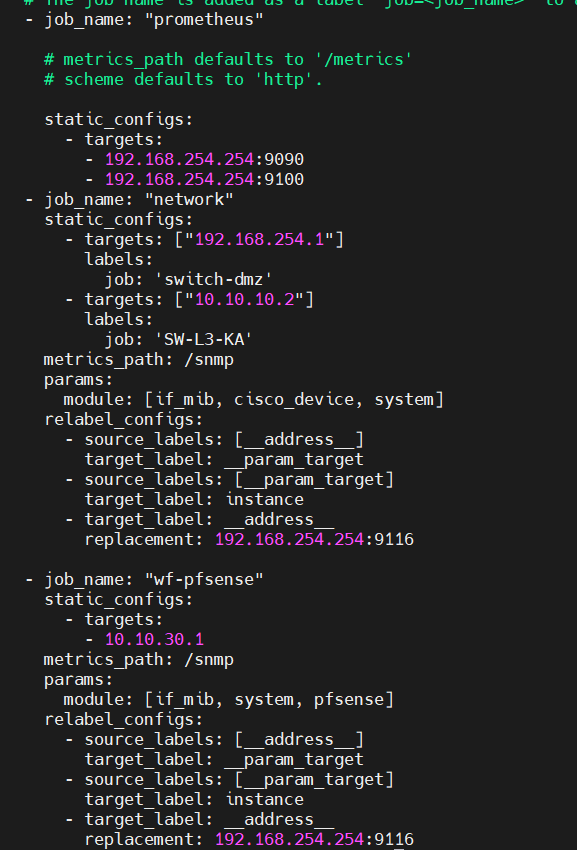
### Cấu hình file Prometheus.yml

Sau khi ta đã xác định và thu thập được metrics ở các thiết bị ta bắt đầu tạo file /etc/prometheus/prometheus.yml để Prometheus xác định được chính xác các đối tượng cần thu thập thông tin và sử dụng modules phù hợp

Xác định các targets

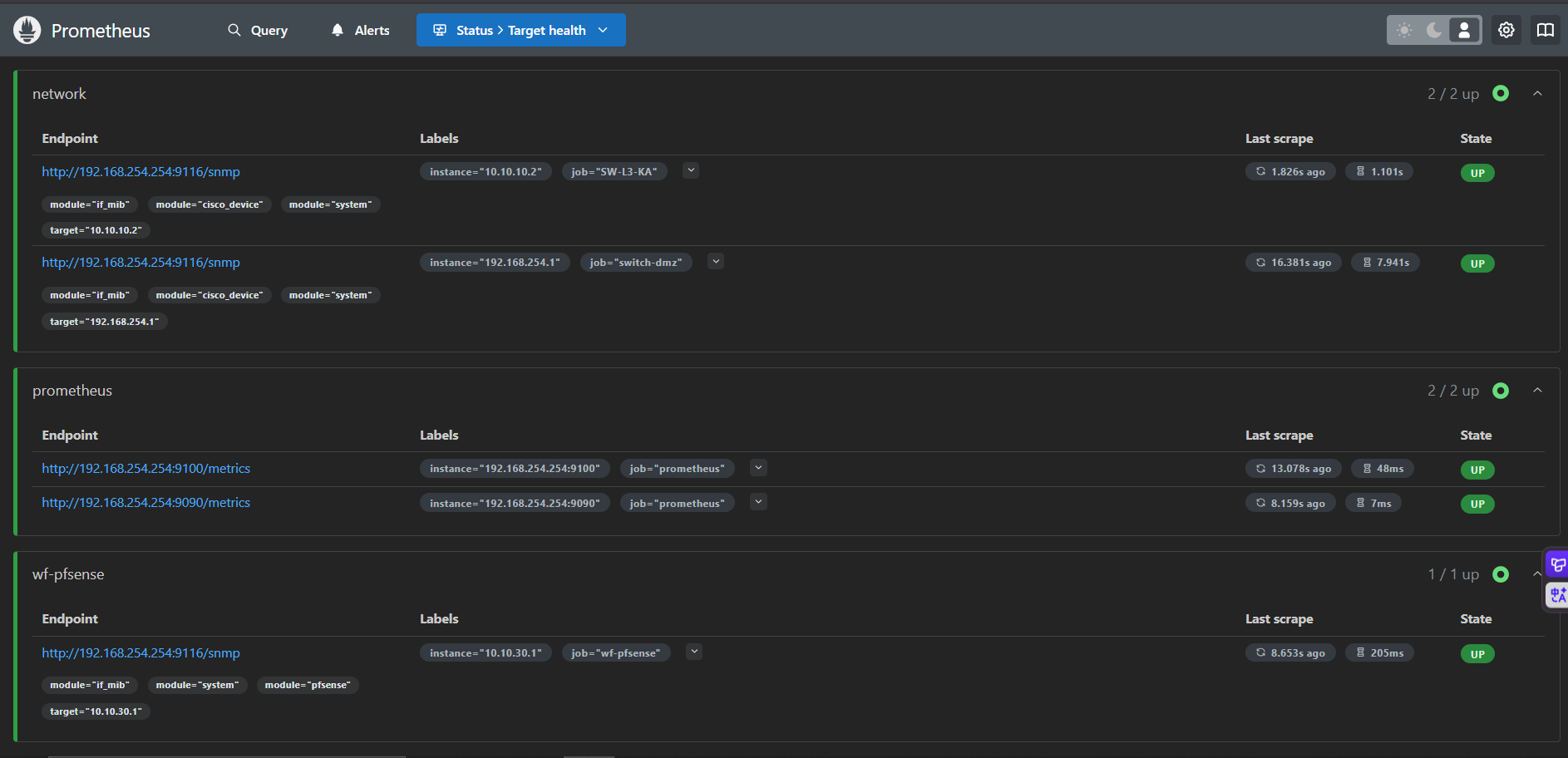
Quy định job name cho từng đối tượng

Đường dẫn đến file snmp và sử dụng các module nào



Hình .14. Cấu hình file Prometheus.yml

Sau khi đã cấu hình xong thì ta cần quay lại giao diện web Prometheus để kiểm tra trạng thái các node.



Hình .15. Kiểm tra trạng thái hoạt động của từng thiết bị

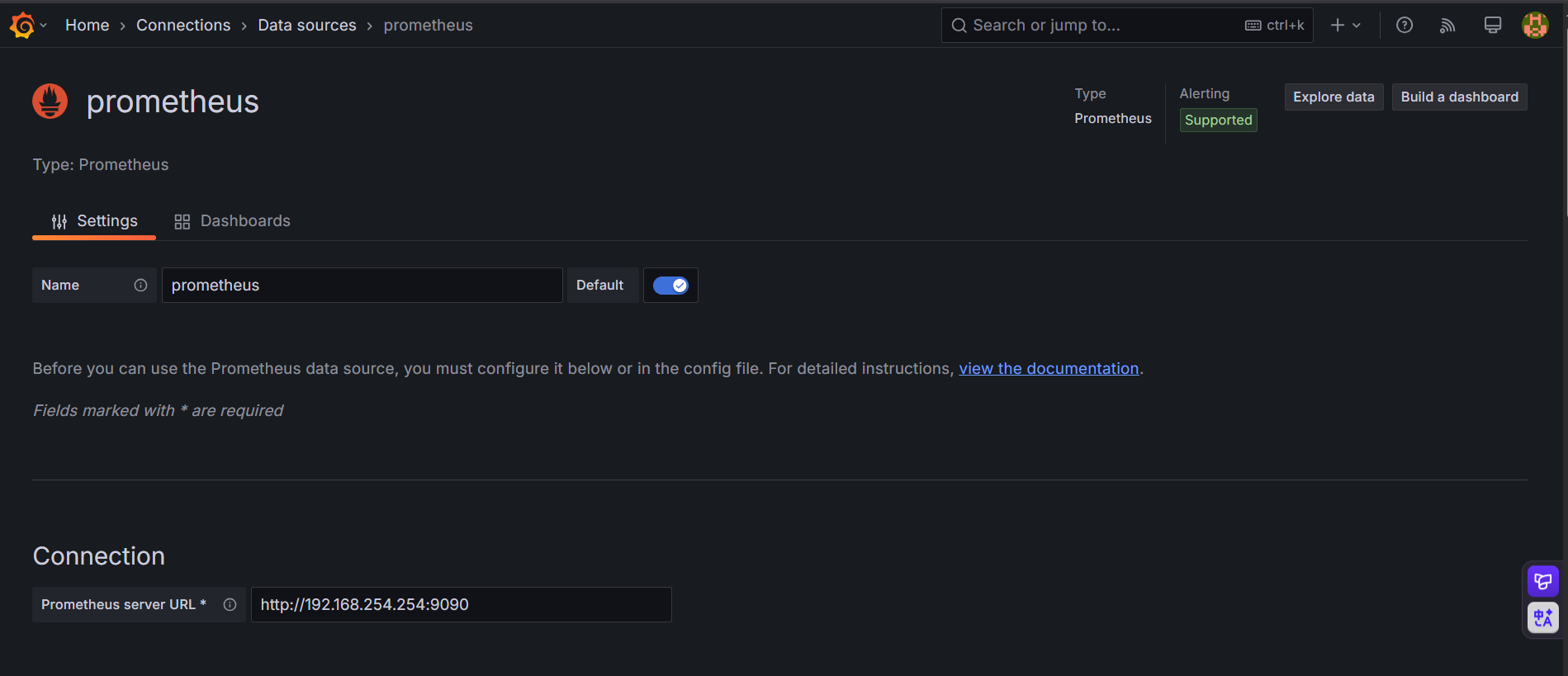
## Tích hợp hệ thống và tạo Dashboard

### ****Thêm Prometheus vào Grafana****

Vào **Configuration → Data Sources → Add Data Source**

Chọn **Prometheus →** nhập URL: http://192.168.254.254:9090

Save & Test.



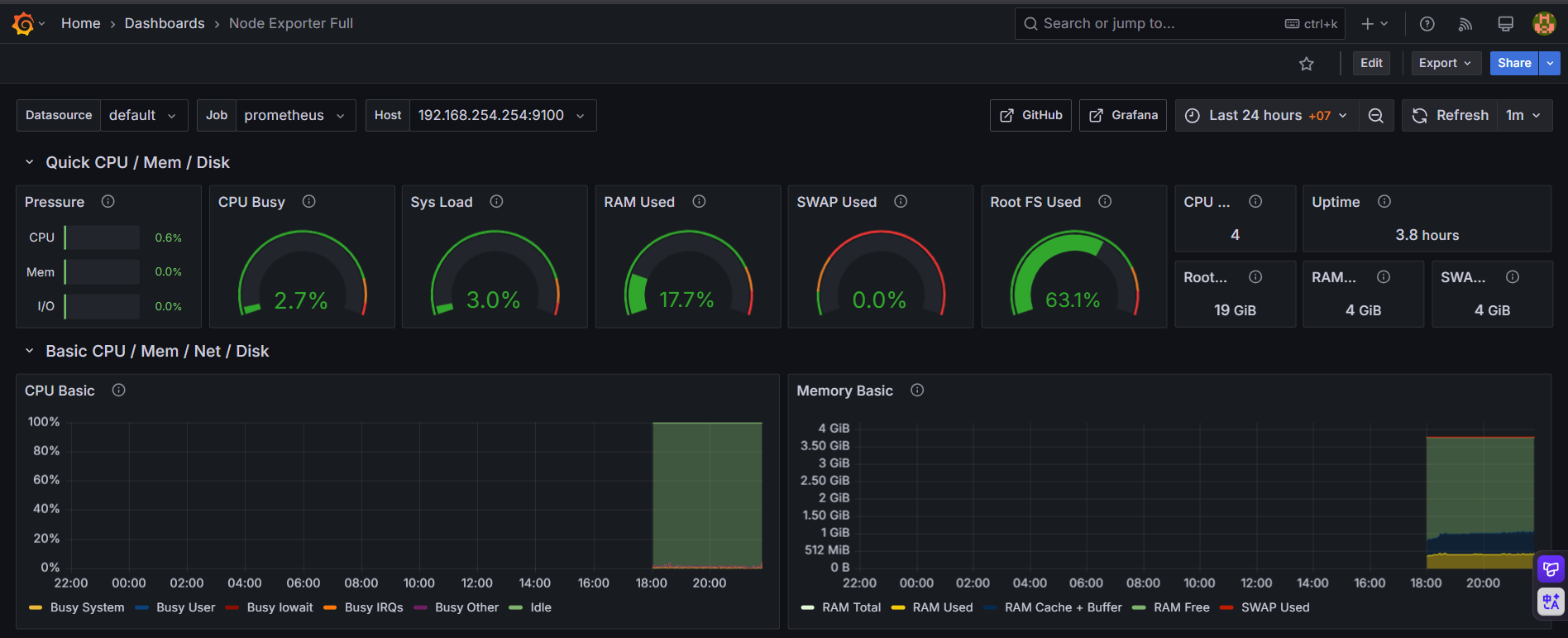
Hình .16. Tích hợp Prometheus vào Grafana

### ****Tạo Dashboard giám sát sử dung node\_exporter****

Import dashboard sẵn có từ **Grafana Labs (ID: 1860 – Node Exporter Full)**

Hoặc tự tạo panel hiển thị:

* **CPU Usage**
* **Memory Usage**
* **Disk I/O**
* **Network Traffic**

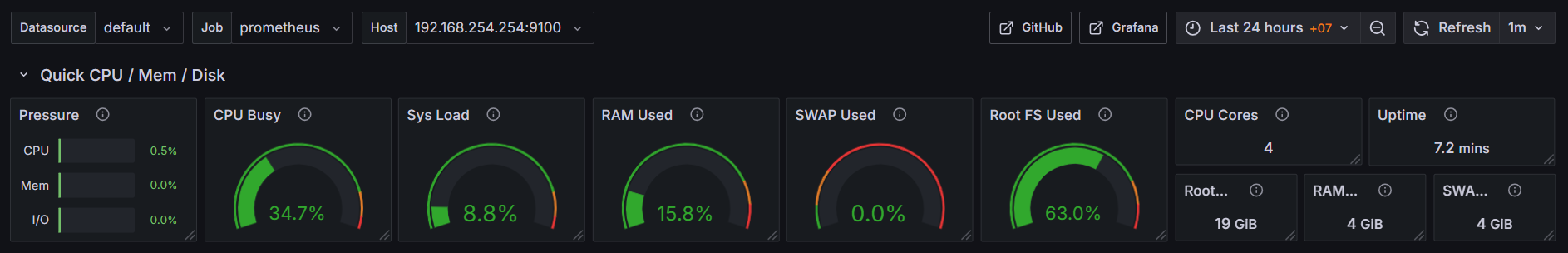


Hình .17. Import Dashboard có sẵn từ Grafana Lab

Qua dashboard trên ta thu thập được các thông tin như:

1. **Thông tin chung về hệ thống**

* Tên máy chủ, địa chỉ IP, uptime (thời gian hoạt động).
* Phiên bản kernel, phiên bản Node Exporter.
* Số CPU, tổng dung lượng RAM, dung lượng disk.



Hình .18. Thông tin chung về hệ thống

1. Hiệu suất CPU

* Tổng quan CPU usage (%): idle, user, system, iowait, steal…
* Tải trung bình (Load Average): 1 phút, 5 phút, 15 phút.
* Usage từng core CPU (nếu server đa nhân).



Hình .19. Hiệu suất

1. Bộ nhớ (Memory)

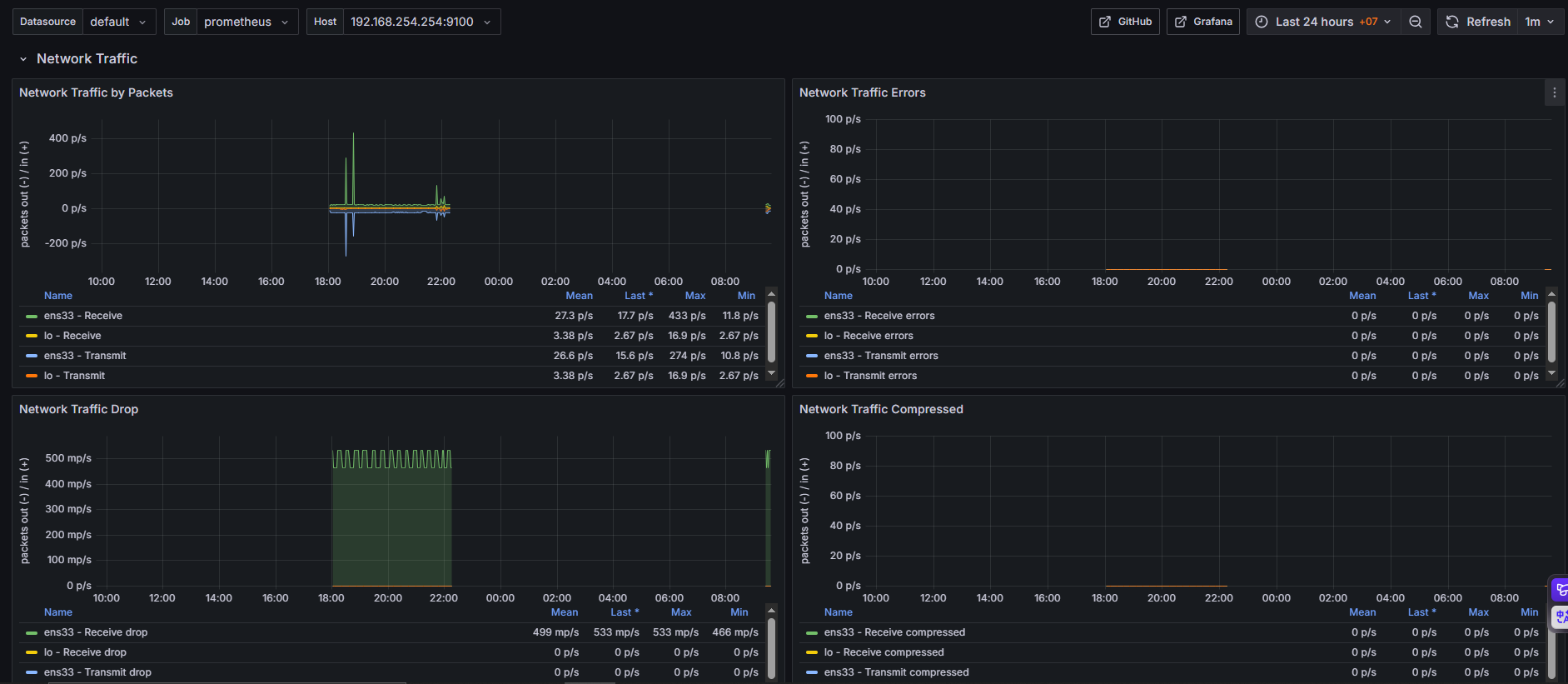
* RAM tổng, đã sử dụng, còn trống, buffers/cache.
* Swap memory: sử dụng bao nhiêu, còn trống bao nhiêu.
* Tỷ lệ phần trăm sử dụng RAM theo thời gian.

1. Disk (Ổ đĩa)

* Disk usage: dung lượng đã dùng / tổng dung lượng từng partition.
* Disk I/O: số lượng đọc/ghi, tốc độ đọc/ghi (MB/s), độ trễ.
* Inode usage: dung lượng inode còn trống / đã dùng.

1. Network (Mạng)

* Lưu lượng mạng In/Out theo interface (eth0, ens33, v.v…).
* Tốc độ (bytes per second hoặc Mbps).
* Tổng bytes đã truyền và nhận.
* Gói tin bị lỗi, dropped packets.



Hình .20. Network traffic trên từng cổng

1. File System & Mount Points

* Danh sách tất cả filesystem được mount.
* Tỷ lệ sử dụng từng phân vùng.

1. Process

* Số lượng tiến trình đang chạy, sleep, zombie.
* Tiến trình chiếm nhiều CPU/RAM nhất (có thể custom thêm).

1. Thông tin khác

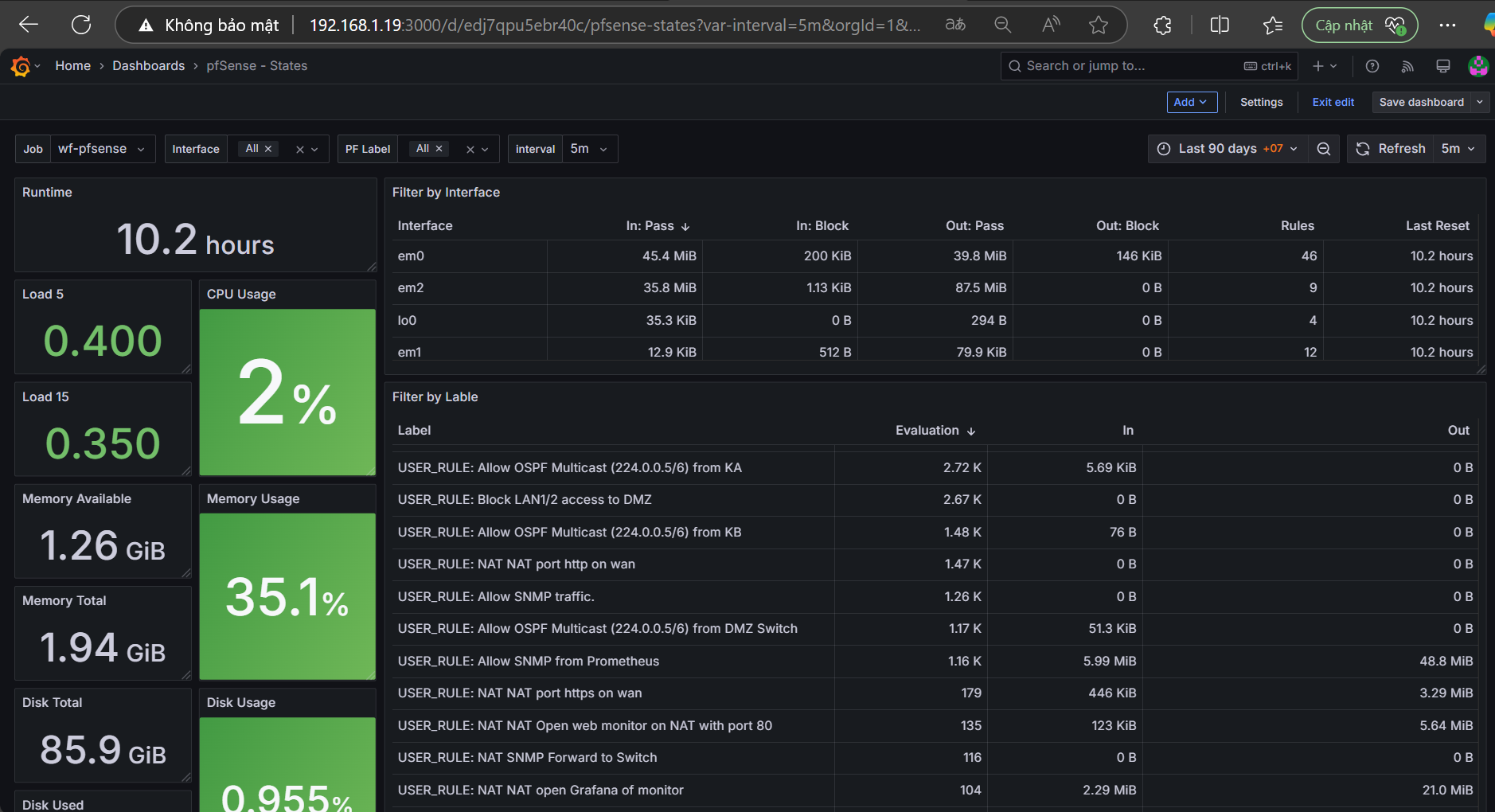
* Temperature (nếu server hỗ trợ sensor).
* Context switches, interrupts.
* Boot time (thời gian khởi động gần nhất).

### Tạo dashboard giám sát sử dụng SNMP walk

Kích hoạt dịch vụ SNMP để cho phép phần mềm giám sát thu thập dữ liệu trạng thái hệ thống.

SNMP Daemon hoạt động với community string là public.

Dữ liệu như CPU, RAM, traffic interface được thu thập qua SNMP Walk/Prometheus

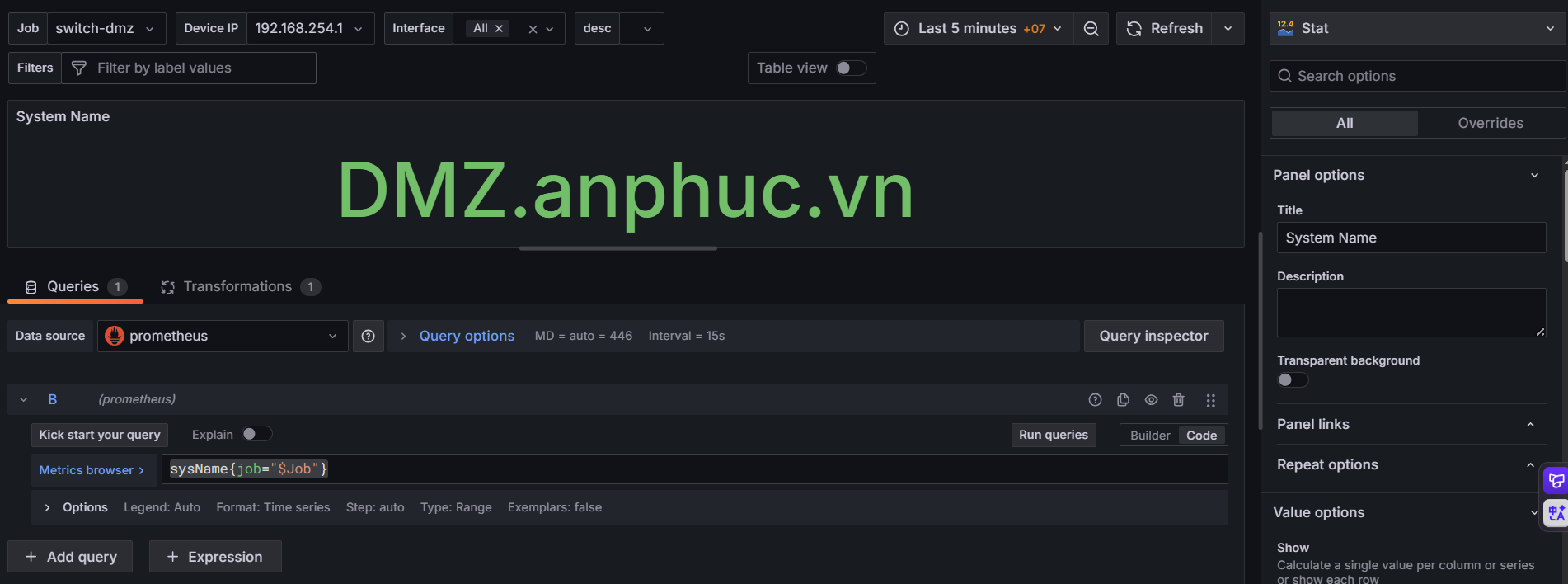


Hình .21: Xem giám sát thông qua Grafana

### Tự tạo dashboard để giám sát các thiết bị switch

1. Cấu hình tên thiết bị

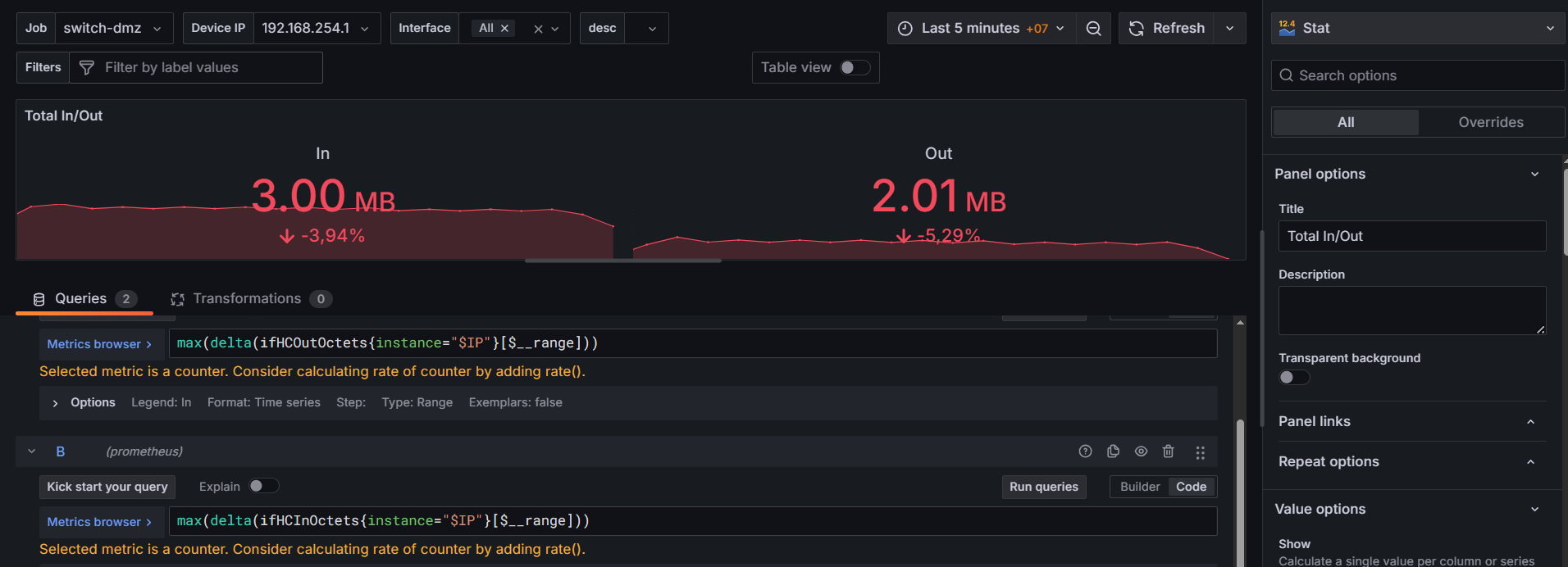
Vào new dashboard -> add visualization -> datasource: Prometheus



Hình .22. Giao diện tùy chỉnh

Vào Metric browsers: thêm queries “sysName{job="$Job"}” để lấy được hostname của thiết bị. Vào transformation thêm “Lables to fields” để chỉ hiển thị sysName, và sử dụng biểu đồ Stat để hiển thị

1. Cấu hình hiển thị tổng lưu lượng mạng In/Out



Hình .23. Tổng lưu lượng mạng In/Out

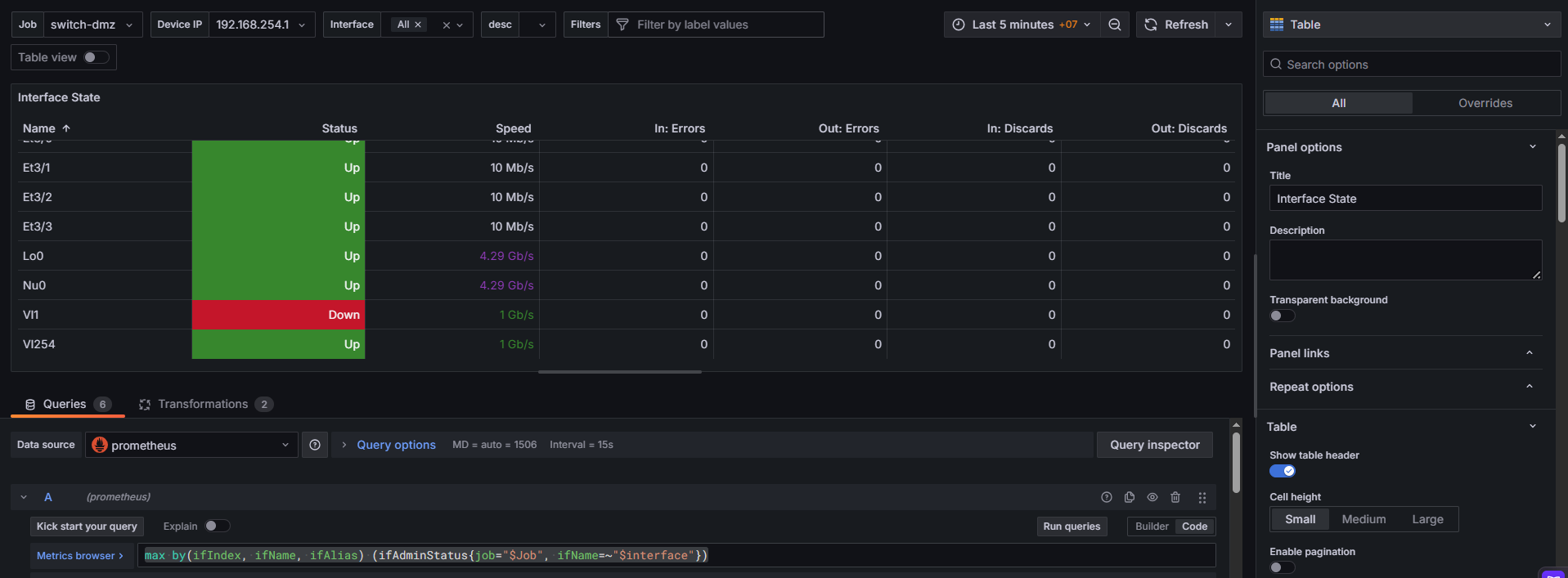
Sửu dụng các truy vấn

* ifHCInOctets và ifHCOutOctets là metric SNMP thể hiện tổng số byte nhận/gửi của interface.

Biểu đồ này cho biết lượng dữ liệu tổng cộng đã vào/ra thiết bị trong một khoảng thời gian nhất định.

* Dùng để kiểm tra nhanh tình trạng tải mạng của switch/router DMZ.
* Có thể dùng làm cơ sở đặt cảnh báo (ví dụ: In/Out vượt quá 100MB trong 5 phút → cảnh báo).

1. **Bảng trạng thái (Interface State):**

****

Hình .24. Bảng trạng thái từng cổng

Sử dụng query:

ifAdminStatus: Đây là metric thu thập từ SNMP Exporter, thể hiện trạng thái hành chính (administrative status) của các interface (cổng mạng) trên thiết bị (switch/router).

Giá trị thường là:

1: Up (được bật)

2: Down (được tắt)

3: Testing

max by(ifIndex, ifName, ifAlias)

* ifIndex: Chỉ số duy nhất cho mỗi interface.
* ifName: Tên interface (VD: Et3/0, Vi1).
* ifAlias: Mô tả/ghi chú interface nếu được cấu hình trong thiết bị.
* max by(...): Gom nhóm các metric theo các nhãn này và lấy giá trị cao nhất (thường là 1 hoặc 2).
* Mục đích: Hiển thị trạng thái hiện tại của từng interface.

Biến $Job và $interface

* $Job: Lọc theo tên job đã cấu hình trong Prometheus (ví dụ switch-dmz).
* $interface: Lọc theo tên interface cụ thể hoặc tất cả interface (All).

### Cấu hình tích hợp alertmanager gửi cảnh báo

Hệ thống Prometheus kết hợp Alertmanager được triển khai nhằm:

* Giám sát tình trạng mạng và tài nguyên hệ thống.
* Phát hiện sự cố tức thời (Interface Down/Backup Fail).
* Theo dõi xu hướng tăng tải (Traffic/Memory).
* Gửi cảnh báo đa kênh (Telegram + Email) giúp phản ứng nhanh.

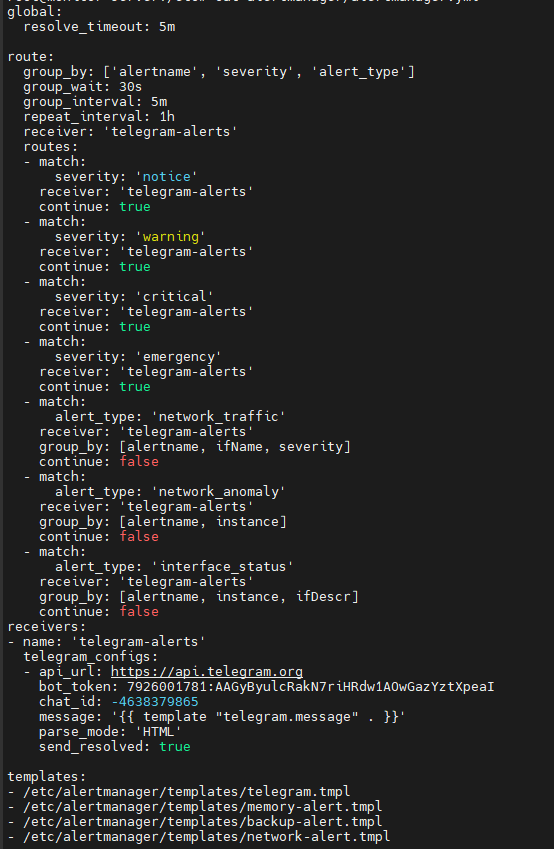


Hình .25. Hệ thống gửi cảnh báo Alertmanager

### Kết nối cấu hình cảnh báo đến telegram

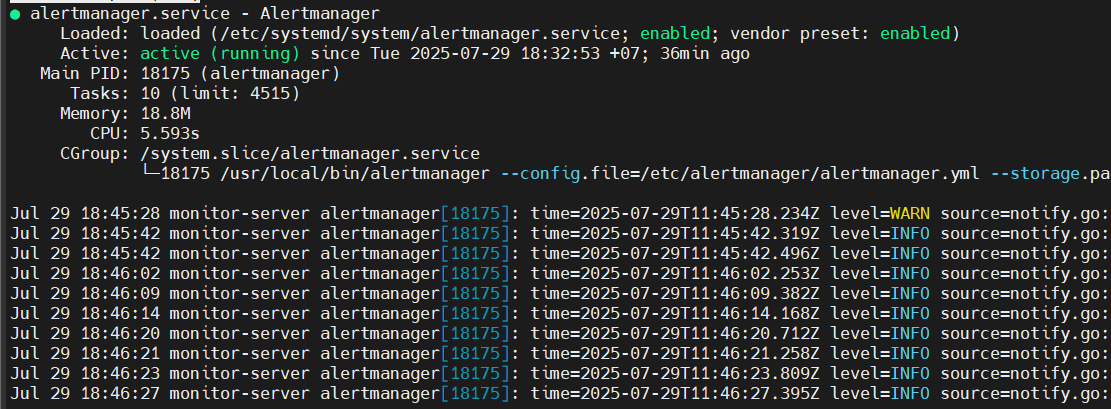
Thực hiện kết nối đến alertmanager bằng cách tạo file alertmanager.yml trong /etc/alertmanager/

Cấu hình token-id và chat-id để kết nối được đến với telegram



Hình .26. Cấu hình alertmanager.yml

Thực hiện restart và kiểm tra trạng thái hoạt động của alertmanager



Hình .27. Trạng thái dịch vụ Alertmanager

### Quy tắc cảnh báo (Alert Rules)

1. Cảnh báo trạng thái cổng mạng (Interface)

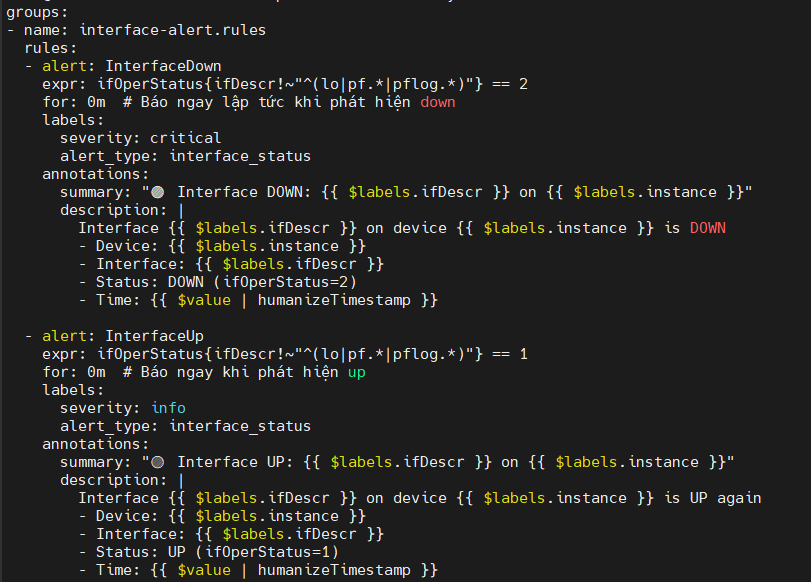
Mục tiêu: Phát hiện nhanh khi cổng mạng bị down hoặc up trở lại.

Rule:

* InterfaceDown: Nếu ifOperStatus == 2 → severity critical.
* InterfaceUp: Nếu ifOperStatus == 1 → severity info.

Tính năng:

* Bỏ qua loopback và interface ảo (lo, pf.\*, pflog.\*).
* Gửi ngay lập tức (for: 0m).

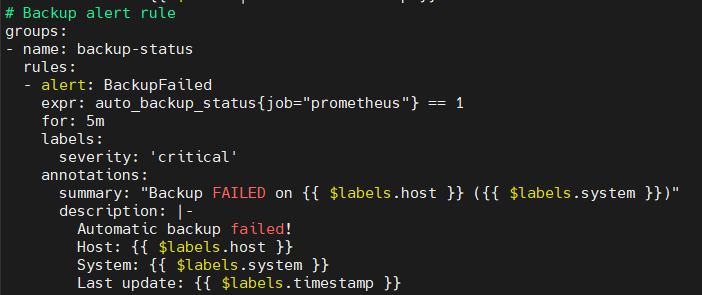


Hình .28. Rule cảnh báo trạng thái cổng mạng

1. Cảnh báo lỗi Backup

Mục tiêu: Đảm bảo sao lưu tự động không bị gián đoạn.

* Rule: auto\_backup\_status == 1 trong 5 phút → severity critical.
* Thông tin bổ sung: Hiển thị tên host, loại thiết bị, timestamp.



Hình .29. Rule cảnh báo trạng backup khi không backup thành công

1. Cảnh báo Traffic mạng

Mục tiêu: Giám sát lưu lượng In/Out bất thường hoặc vượt ngưỡng.

Rule:

* HighInboundTraffic > 100 Mbps (warning) hoặc > 150 Mbps (critical).
* HighOutboundTraffic > 50 Mbps (warning) hoặc > 75 Mbps (critical).
* NetworkTrafficAnomaly: Lưu lượng bất thường so với trung bình 7 ngày.
* Ý nghĩa: Hỗ trợ phát hiện tấn công DDoS hoặc lỗi cấu hình mạng.



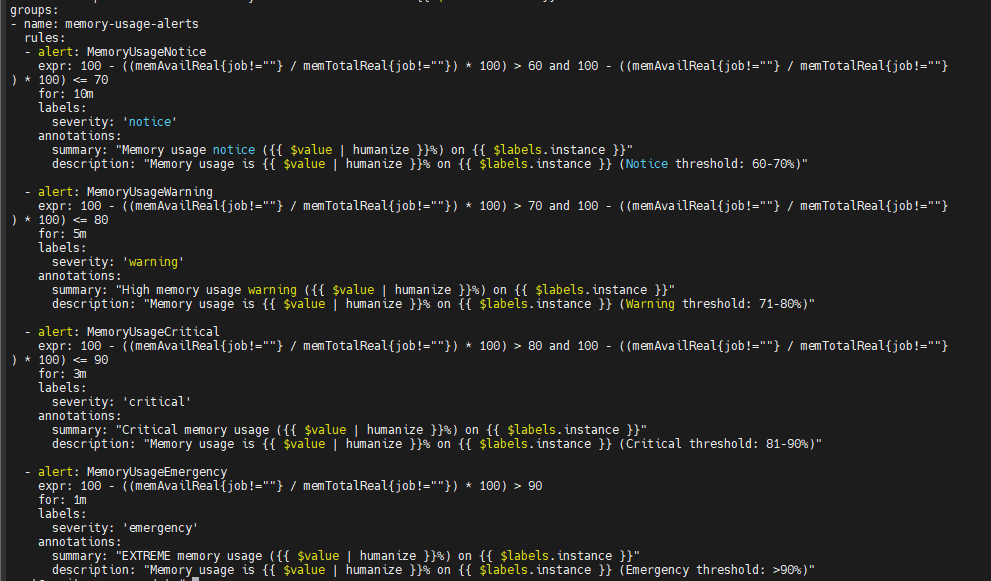
Hình .30. Rule cảnh báo khi có lưu lượng In/Out tăng cao

1. Cảnh báo sử dụng Memory

Mục tiêu: Giám sát mức sử dụng bộ nhớ và phân loại theo 4 mức:

* Notice: >60% đến 70%.
* Warning: >70% đến 80%.
* Critical: >80% đến 90%.
* Emergency: >90%.

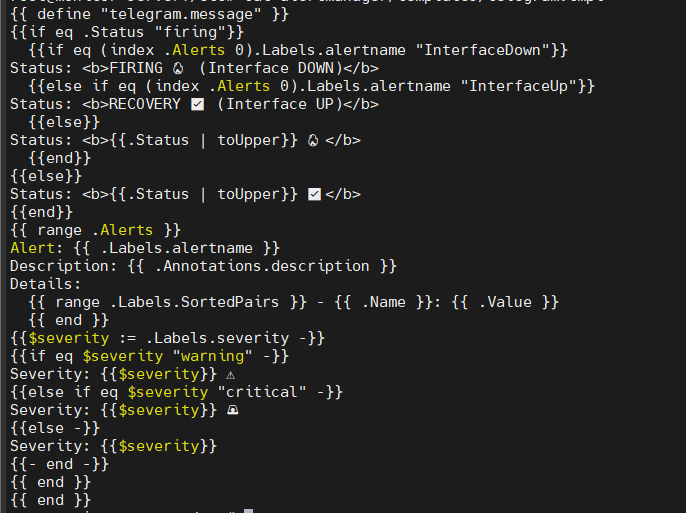
Rule: Sử dụng memAvailReal và memTotalReal để tính toán phần trăm bộ nhớ sử dụng.



Hình .31. Rule gửi cảnh báo theo tình trạng mức sử dụng bộ nhớ

### Cơ chế gửi cảnh báo

Ta tạo các template theo từng rule cụ thể để biết được chính xác các thông tin mà ta nhận được. Ta sử dụng 2 kênh chính là telegram và email để thực hiện nhận thông tin

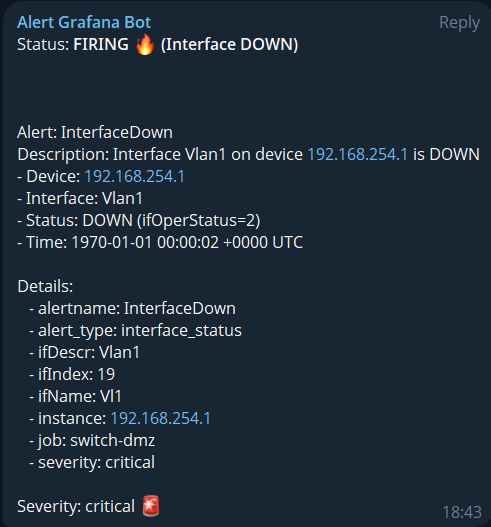


Hình .32. Ví dụ về template mẫu của cảnh báo Up/Down trên cổng mạng

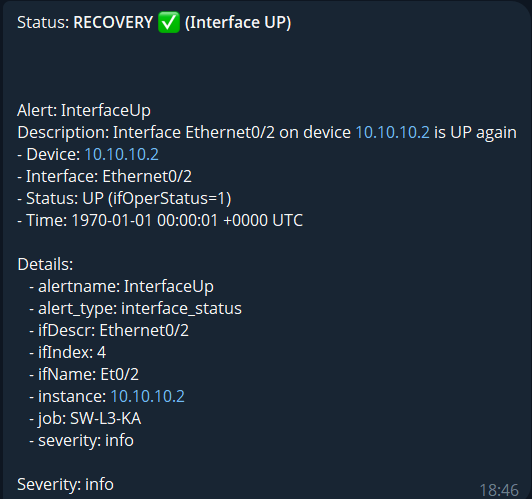
Kênh: Telegram và Email.

Định dạng thông báo (HTML):

* Kết quả trạng thái cổng mạng

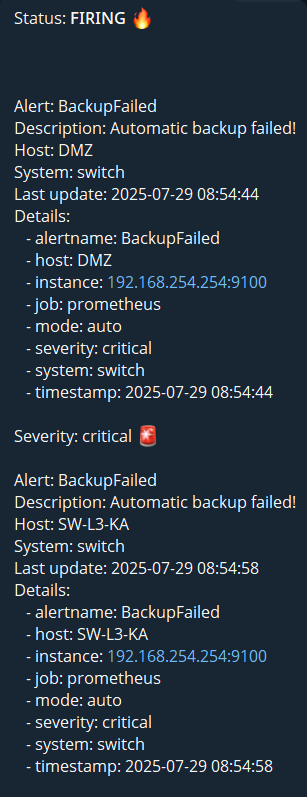


Hình .33. Cảnh báo khi trạng thái cổng down



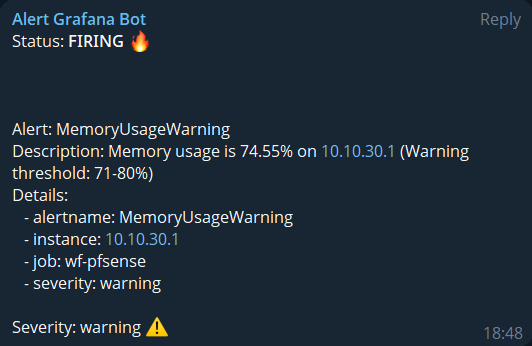
Hình .34. Cảnh báo khi trạng thái cổng được khôi phục trở lại

* Kết quả trạng thái khi backup failed



Hình .35. Cảnh báo khi backup failed

* Kết quả khi lượng memory sử dụng đạt đến ngưỡng cảnh báo



Hình .36. Cảnh báo khi lượng memory đạt 74.55%

## Kết luận chương

Trong chương này, em đã xây dựng và triển khai hoàn chỉnh hệ thống tự động hóa cấu hình, giám sát và cảnh báo mạng trong mô hình lab bằng cách kết hợp Ansible, Prometheus, Grafana và Alertmanager. Toàn bộ quá trình triển khai được thực hiện theo các bước rõ ràng và logic, bao gồm:

* **Tự động hóa với Ansible**: triển khai playbook để sao lưu cấu hình thiết bị (pfSense, Switch Cisco), tích hợp node vào Teleport Server, và tự động cài đặt dịch vụ Nginx. Các tác vụ này giúp loại bỏ thao tác thủ công, đảm bảo tính nhất quán và dễ dàng mở rộng.
* **Cấu hình Prometheus** để thu thập số liệu từ nhiều nguồn: trạng thái backup, dịch vụ Nginx, node\_exporter và SNMP Exporter. Điều này cho phép giám sát toàn diện từ hạ tầng phần cứng, dịch vụ đến thiết bị mạng.
* **Xây dựng dashboard trên Grafana** để trực quan hóa dữ liệu giám sát, bao gồm hiệu suất CPU, RAM, Disk, lưu lượng mạng, trạng thái switch và firewall. Dashboard giúp đội ngũ vận hành theo dõi hệ thống theo thời gian thực, dễ dàng phát hiện bất thường.
* **Thiết lập hệ thống cảnh báo với Alertmanager** cùng các bộ luật cảnh báo chi tiết:
  + Cảnh báo khi cổng mạng bị mất kết nối hoặc hoạt động trở lại.
  + Cảnh báo khi tiến trình backup thất bại.
  + Cảnh báo khi lưu lượng mạng vượt ngưỡng quy định.
  + Cảnh báo khi mức sử dụng bộ nhớ vượt các ngưỡng (Notice, Warning, Critical, Emergency).
* **Tích hợp cảnh báo đa kênh (Telegram, Email)** nhằm gửi thông tin tức thì đến quản trị viên với đầy đủ nội dung về thiết bị, sự cố và thời gian.

**Kết quả kiểm thử**

* Các cảnh báo được kích hoạt chính xác, kịp thời theo điều kiện đã cấu hình; ví dụ: khi một cổng mạng bị down, thông báo lập tức được gửi về Telegram.
* Tích hợp Telegram và Email hoạt động ổn định, bảo đảm truyền tải sự kiện đến nhiều kênh liên lạc.
* Dashboard Grafana trực quan, dễ sử dụng, hỗ trợ phân tích xu hướng và kiểm tra nhanh trạng thái hệ thống.
* Cơ chế cảnh báo phân cấp mức độ (Notice → Warning → Critical → Emergency) giúp tối ưu hóa quy trình phản ứng sự cố, giảm thiểu rủi ro.

**Đánh giá hệ thống**

* Hệ thống có chi phí thấp, sử dụng công cụ mã nguồn mở, dễ triển khai và tùy chỉnh.
* Khả năng mở rộng cao: có thể thêm exporter mới hoặc bổ sung luật cảnh báo phù hợp với nhu cầu thực tế.
* Cảnh báo đa kênh giúp giảm thiểu thời gian phản hồi, nâng cao độ tin cậy của hạ tầng mạng.
* Dashboard Grafana mang lại cái nhìn toàn diện và trực quan về toàn bộ hệ thống.

Tuy nhiên, hệ thống vẫn còn một số điểm cần tối ưu trong các bước tiếp theo, chẳng hạn như tinh chỉnh biểu thức cảnh báo phức tạp để hạn chế cảnh báo nhiễu (alert noise), và bổ sung cơ chế **tự động khắc phục sự cố (auto-remediation)** nhằm nâng cao hơn nữa khả năng tự chủ của hệ thống.

KẾT LUẬN

1. KẾT QUẢ ĐẠT ĐƯỢC

Trong quá trình thực tập tại VNNIC, tôi đã tiếp thu và nắm vững nhiều kiến thức chuyên môn quan trọng, mặc dù những kiến thức này là những kiến thức rất cơ bản như ip, lớp của ip, mô hình OSI, Quản Trị và Giám Sát Mạng,... đặc biệt là trong các lĩnh vực liên quan đến quản lý và vận hành hệ thống mạng. Cụ thể, tôi đã được ôn lại các kỹ thuật cấu hình mạng, bao gồm việc thiết lập và quản lý các thiết bị mạng như router và switch, đảm bảo hệ thống mạng hoạt động ổn định và hiệu quả.

Trong thời gian này, tôi đã được làm quen với thầy Bình, là thầy đã dạy và chia sẻ cho tôi những kiến thức và những câu chuyện trong công ty. Người đã giúp đỡ tôi rất nhiều từ việc làm đơn xin vào thực tập cho đến hết quá trình thực tập tại đó. Ngoài ra tôi còn được làm quen với nhiều anh chị năm cuối cũng đang thực tập thực tế tại đó, các anh chị ở đó rất cởi mở và hòa đồng, giúp tôi cải thiện rất nhiều về khả năng giao tiếp. Sau khi thực tập ở đó tôi đã cảm nhận được kỹ năng giao tiếp của tôi được cải thiện đi rất nhiều, tôi cũng thoải mái và tự tin hơn khi hỏi hay giải thích một thứ gì đó mà tôi biết một cách tự nhiên nhất.

Và cuối cùng là khả năng tự học. Khi ở trong một môi trường thực tế, tôi luôn có một áp lực ngầm sau lưng, ở đó tôi và các bạn trong nhóm thực tập doanh nghiệp không được giao cho các đồ án hay các bài tập lớn, nhưng khi thầy thông báo các buổi thầy chia sẻ, củng cố kiến thức và các bạn nên ôn trước một vài kiến thức như giao thức snmp chẳng hạn. Thì tôi đã trở nên chủ động hơn, ngoài việc tìm hiểu cái đó tôi còn tự giác tìm hiểu thêm về nhiều thứ khác bên lề như giám sát mạng, quản trị mạng,.. Khi thầy đưa ra lời đề nghị thì tôi xem như mình phải có trách nhiệm, nhiệm vụ trong lời đề nghị đó. Cảm giác nó không phải như ở trên trường lớp, ở trên trường lớp tôi có thể không làm, hay tôi có thể làm theo kiểu đối phó, nhưng trong môi trường thực tế tôi có cảm giác mình có trách nhiệm hơn. Và khả năng tự học tự tìm tòi của tôi được cải thiện hơn rất nhiều.

Thời gian Thực Tập rất ngắn, chỉ khoảng một tháng nhưng đối với tôi học tập và củng cố kiến thức không phải là thứ quan trọng nhất vì trên trường tôi cũng đã được các thầy cô dạy đầy đủ cả rồi, nhưng được tiếp xúc với môi trường làm việc thực tế, được làm quen với các anh chị thực tập thực tế, Thầy Bình dẫn dắt tôi trong thời gian thực tập, và Giảng Viên Hướng Dẫn môn học THS. Trần Thu Thủy là những gì quan trọng nhất mà tôi cảm nhận được. Bản thân tôi đã học hỏi được rất nhiều thứ từ những con người trên. Tôi đã cải thiện rất nhiều về khả năng giao tiếp, hòa đồng và cởi mở hơn từ các anh chị và bạn bè cũng đang thực tập ở đó. Tôi cũng đã thấy và học tập được đôi chút về phong thái làm việc, sự kỷ luật và tận tâm hướng dẫn sinh viên từ Thầy Bình và Cô Thủy.

1. NHẬN XÉT SAU THỜI GIAN THỰC TẬP TẠI CÔNG TY VNNIC

Nhận xét về Bản Thân Sau Thời Gian Thực Tập

* Học hỏi được rất nhiều điều mới mẻ từ kiến thức đến các kỹ năng ngoài lề
* Có cái nhìn sâu rộng hơn trong môi trường làm việc thực tế
* Cởi mở và hòa đồng hơn với nhiều người khác
* Có trách nghiệm hơn mặc dù những thứ rất đơn giản như ôn lại kiến thức
* Có cái nhìn tổng quát hơn về các công việc làm
* Chưa hoàn thành tốt nhiệm vụ thực tập mà giảng viên hướng dẫn đề ra
* Chưa chủ động hoàn toàn trong việc học

Nhận Xét về Công Ty và Cơ Sở Vật Chất

* Công Ty khi nhìn ở bên ngoài và khi vào trong có cảm giác rất hiện đại
* Bàn ghế rất mới mẻ
* Các nhân viên làm việc ở tầng dưới cùng nhìn rất phong thái, nghiêm túc
* Các bộ phận được chia theo từng phòng như phòng phần mềm, phòng họp,..
* Phòng học có cả điều hòa và máy chiếu
* Các thành viên trong công ty và thực tập rất vui vẻ và hòa đồng
* Thầy dạy chỗ công ty rất nhiệt huyết và tận tình

Thời gian thực tập tại công ty VNNIC đã mang lại cho tôi nhiều trải nghiệm quý báu và cơ hội để phát triển cả về mặt chuyên môn và cá nhân. Dưới đây là những nhận xét cá nhân về quá trình thực tập:

Khả Năng Học Hỏi và Tiếp Thu : Tôi đã học hỏi được rất nhiều điều mới mẻ, từ kiến thức chuyên môn như cấu hình mạng và mô hình OSI cho đến các kỹ năng mềm như giao tiếp và làm việc nhóm. Sự tiếp xúc với các tình huống thực tế đã giúp tôi hiểu sâu hơn về các vấn đề mà lý thuyết không thể giải quyết đầy đủ.

Cái Nhìn Sâu Rộng về Môi Trường Làm Việc : Thực tập tại VNNIC đã giúp tôi có cái nhìn tổng quan và rõ nét hơn về môi trường làm việc thực tế. Tôi đã thấy được cách thức các quy trình được vận hành và sự phối hợp giữa các bộ phận trong một tổ chức lớn, từ đó hiểu rõ hơn về yêu cầu và kỳ vọng trong công việc.

Tinh Thần Cởi Mở và Hòa Đồng : Tôi đã trở nên cởi mở và hòa đồng hơn khi giao tiếp và làm việc với các đồng nghiệp. Sự kết nối và hợp tác hiệu quả với các thành viên trong công ty đã giúp tôi nâng cao kỹ năng giao tiếp và xây dựng các mối quan hệ chuyên nghiệp.

Tinh Thần Trách Nhiệm : Tôi đã rèn luyện được tinh thần trách nhiệm qua việc ôn lại và thực hiện các nhiệm vụ, dù là những công việc đơn giản. Điều này đã giúp tôi nhận thức rõ hơn về sự quan trọng của từng nhiệm vụ trong quá trình làm việc.

Nhận Thức về Tự Chủ và Sáng Tạo : Mặc dù tôi đã học được rất nhiều, tôi nhận ra rằng mình vẫn chưa hoàn toàn chủ động trong việc tìm tòi và học hỏi. Sự chủ động và sáng tạo trong việc giải quyết vấn đề và tìm kiếm cơ hội học hỏi sẽ là những điểm tôi cần cải thiện trong tương lai.

Nhận Xét về Kỹ Năng và Hiệu Quả Làm Việc : Tôi nhận thấy mình cần cải thiện khả năng tổ chức và quản lý thời gian để hoàn thành nhiệm vụ một cách hiệu quả hơn. Việc chủ động hơn trong việc học hỏi và tìm kiếm thông tin sẽ giúp tôi đạt được kết quả tốt hơn trong các nhiệm vụ được giao.

TÀI LIỆU THAM KHẢO

[1] Giới thiệu về VNNIC: https://vnnic.vn/giới-thiệu-về-vnnic

[2] Các hoạt động của VNNIC: https://vnnic.vn/tintuc

[3] Hệ thống VNIX: <https://vnnic.vn/vnix/gioi-thieu>

**[4] Ansible Documentation** – Hướng dẫn chính thức cho việc tự động hóa cấu hình hệ thống mạng và tích hợp với giám sát: https://docs.ansible.com/

[5] Prometheus Documentation – Tài liệu chính thức của Prometheus, hướng dẫn cài đặt, cấu hình và viết rule cảnh báo - https://prometheus.io/docs/introduction/overview/

[6] Grafana Documentation – Hướng dẫn sử dụng Grafana để xây dựng dashboard và trực quan hóa dữ liệu giám sát mạng - https://grafana.com/docs/grafana/latest/

[7] Alertmanager Documentation – Tài liệu cấu hình Alertmanager để quản lý cảnh báo và tích hợp gửi thông báo qua các kênh (Telegram, Email) - https://prometheus.io/docs/alerting/latest/alertmanager/

[8] SNMP Exporter Documentation – Hướng dẫn triển khai SNMP Exporter để thu thập thông tin thiết bị mạng qua SNMP- https://github.com/prometheus/snmp\_exporter

[9] pfSense Documentation – Tài liệu cấu hình pfSense làm tường lửa và gateway, tích hợp SNMP để giám sát - https://docs.netgate.com/pfsense/en/latest/

[10] Telegram Bot API – Tài liệu về API của Telegram để gửi cảnh báo tự động từ Alertmanager - https://core.telegram.org/bots/api

[11] Node Exporter Documentation – Hướng dẫn triển khai Node Exporter để thu thập metric hệ thống (CPU, RAM, Disk) - https://prometheus.io/docs/guides/node-exporter/