**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

---

**TRẦN ĐOÀN TRUNG**

# NGHIÊN CỨU VÀ ĐÁNH GIÁ GIẢI PHÁP QUẢN LÝ TRUY CẬP ĐẶC QUYỀN CYBERARK

**Chuyên ngành: Kỹ thuật Viễn thông**

**Mã số: 8.52.02.08**

**TÓM TẮT ĐỀ ÁN TỐT NGHIỆP THẠC SĨ**

HÀ NỘI – NĂM 2023

Đề án tốt nghiệp được hoàn thành tại:

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

Người hướng dẫn khoa học: PGS. TS. Dương Thị Thanh Tú

Phản biện 1: ……

Phản biện 2: ……

Đề án tốt nghiệp sẽ được bảo vệ trước Hội đồng chấm đề án tốt nghiệp thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: ..... giờ ..... ngày ..... tháng ..... .. năm .....

Có thể tìm hiểu đề án tốt nghiệp tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông.

# MỞ ĐẦU

Công nghệ thông tin ngày nay đã và đang được ứng dụng rộng rãi trong mọi lĩnh vực, góp phần vào sự tăng trưởng, chuyển dịch cơ cấu kinh tế và làm thay đổi cơ bản cách quản lý, học tập, làm việc của con người. Rất nhiều nước đã coi sự phát triển công nghệ thông tin và truyền thông là hướng ưu tiên trong chiến lực phát triển kinh tế xã hội. Thế giới những tác động của công nghệ thông tin và truyền thông, đang đi vào nền kinh tế tri thức, trong đó công nghệ thông tin có một vai trò quyết định.

Ứng dụng công nghệ thông tin (CNTT) trong quản lý nhà nước là việc không thể thiếu trong quá trình hiện đại hoá công tác quản lý, góp phần thức đẩy tăng trưởng kinh tế, nâng cao năng xuất lao động, nâng cao lực cạnh tranh của nền kinh tế, thúc đẩy quá trình hội nhập, trong đó công tác quản lý nhà nước được nâng cao một cách hiệu quả rõ rệt nhờ CNTT hiện đại.

Hiện nay trong hạ tầng công nghệ thông tin của bất kỳ doanh nghiệp, tổ chức nào hầu hết đều có những thiết bị mạng, máy chủ dịch vụ phục vụ cho các công việc nội bộ cũng hoạt động kinh doanh mang lại lợi ích kinh tế cao. Để có thể giám sát tài nguyên của tất cả máy chủ hàng ngày, hàng giờ, theo dõi tỷ lệ chiếm dụng CPU, dung lượng còn lại của ổ cứng, tỷ lệ sử dụng bộ nhớ RAM…quản trị viên không thể kết nối vào từng thiết bị mạng, từng máy chủ để mà theo dõi hiệu năng của chúng, cũng như xem các ứng dụng có đang chạy hay không. Chính vì vậy việc đảm bảo hạ tầng công nghệ thông tin hoạt động ổn định là vô cùng quan trọng trong doanh nghiệp. Phần mềm giám sát chính là công cụ giúp người quản trị có thể thực hiện việc này một cách tối ưu nhất.

Phần mềm giám sát giúp cho việc quản lý theo dõi, giám sát tập trung hệ thống mạng, dịch vụ, thực hiện các tác vụ quản lý vận hành mạng. Ghi thông tin và hiển thị chi tiết theo giờ, tuần, tháng, năm việc sử dụng các thông số chính của từng thiết bị: lưu lượng qua các giao tiếp mạng, sử dụng CPU, HDD, RAM,… Ghi thông tin và hiển thị chi tiết theo giờ, ngày, tháng, năm các dịch vụ mạng, các máy chủ,…

- Quản lý giám sát chi tiết về lưu lượng, sử dụng băng thông sử dụng
- Giám sát các hoạt động của người dung, các tấn công và các hoạt động không bình thường, có thể gây hại cho hệ thống
- Giám sát và thống kê các lưu lượng, các giao thức, các dịch vụ được sử dụng trong hệ thống, sử dụng hết bao nhiêu

Trung tâm Dịch vụ số MobiFone là đơn vị trực thuộc Tổng Công ty Viễn thông Mobifone với chức năng phát triển và kinh doanh các dịch vụ giá trị gia tăng, đa phương

tiện, quảng cáo, thanh toán, tài chính trên mạng viễn thông MobiFone. Trên thực tế, cơ sở hạ tầng CNTT của Trung tâm Dịch vụ số Mobifone chưa có hệ thống giám sát cảnh báo tập chung cho tất cả hạ tầng CNTT, chỉ có giám sát của từng hệ thống riêng lẻ nên có rất nhiều hệ thống hạ tầng có nhiều nguy cơ ảnh hưởng như: không ổn định về hệ thống, không phát hiện và dự báo sớm về các yếu tố hạ tầng, …

Polestar EMS là một giải pháp giám sát hạ tầng mạng CNTT dựa trên các kỹ thuật quản trị mạng tiến tiến như kỹ thuật quản trị mạng dựa trên agent, kỹ thuật quản trị mạng dựa trên web, kỹ thuật quản trị mạng dựa trên trí tuệ nhân tao,… Các tính năng nổi bật của giải pháp giám sát Polestar có thể chỉ ra như: giám sát theo thời gian thực, xử lý và phân tích BIGDATA, dự báo ngăn ngừa lỗi bằng công nghệ AI, tối đa khả năng sử dụng với giao diện người dùng dễ sử dụng, trực quan với công nghệ duyệt web đáng tin cậy.

Chính vì vậy, việc chọn đề án "Nghiên cứu giải pháp giám sát Polestar và ứng dụng cho triển khai giám sát hạ tầng CNTT Mobifone" mang ý nghĩa cấp thiết cho việc đảm bảo hạ tầng CNTT hoạt động ổn định và giảm thiểu các rủi ro về an toàn thông tin trong doanh nghiệp nói chung và Trung tâm Dịch vụ số Mobifone nói riêng.

Đề án được chia làm 3 chương chính như sau:

**Chương 1:** Hạ tầng mạng Trung tâm Dịch vụ số MobiFone

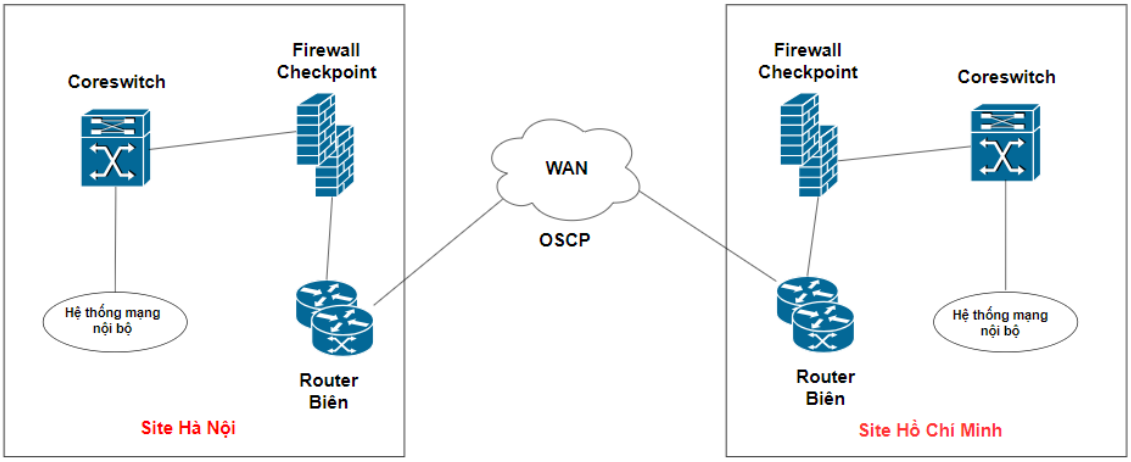
**Chương 2:** Nghiên cứu giải pháp Polestar

**Chương 3:** Xây dựng triển khai thử nghiệm giám sát Polestar cho hạ tầng mạng Trung tâm Dịch vụ số MobiFone

# CHƯƠNG 1: HẠ TẦNG MẠNG TRUNG TÂM DỊCH VỤ SỐ MOBIFONE

## 1.1. Khảo sát hiện trạng hạ tầng mạng Trung tâm Dịch vụ số Mobifone

Khảo sát hiện trạng hạ tầng mạng Trung tâm Dịch vụ số Mobifone là bước quan trọng để đảm bảo hệ thống vận hành ổn định, an toàn và hiệu quả. Dù giữ vai trò then chốt trong cung cấp dịch vụ viễn thông, hạ tầng hiện tại còn hạn chế trong giám sát tập trung và phát hiện sớm sự cố. Do đó, cần thực hiện khảo sát tổng thể theo mô hình mạng Tier 3 (gồm Border Router, Firewall, Core Switch, Switch access) để đánh giá, từ đó làm cơ sở tối ưu hóa hạ tầng mạng trong tương lai.




**Hình 1. 1: Sơ đồ mạng Trung tâm Dịch vụ số MobiFone**

### 1.1.1. Border Router

Border Router là thiết bị định tuyến kết nối mạng nội bộ với mạng bên ngoài như Internet hoặc WAN, đóng vai trò quan trọng trong mô hình phân lớp Tier 3. Thiết bị này đảm nhận định tuyến liên miền (BGP, OSPF), triển khai chính sách bảo mật, kiểm soát lưu lượng và đảm bảo chất lượng dịch vụ (QoS). Trong OSPF, Border Router có thể là ABR hoặc ASBR, cho phép tối ưu và phân phối bảng định tuyến hiệu quả.

### 1.1.2. Firewall

Firewall (tường lửa) là thiết bị bảo mật mạng quan trọng, hoạt động như lớp chắn giữa các vùng mạng có độ tin cậy khác nhau, thường nằm giữa mạng nội bộ và Internet. Thiết bị này kiểm soát lưu lượng vào ra theo các chính sách đã cấu hình nhằm đảm bảo an toàn cho hệ thống. Firewall có thể là thiết bị phần cứng, phần mềm hoặc tích hợp trong router, được triển khai chủ yếu tại lớp biên và phân phối trong mô hình mạng Tier 3.

### 1.1.3. Core Switch

Trong kiến trúc mạng phân tầng tiêu chuẩn (3-tier architecture) bao gồm các lớp Access – Distribution – Core, Core Switch (thiết bị chuyển mạch lõi) là thiết bị chuyển mạch trung tâm, nằm tại lớp lõi của hệ thống mạng, có nhiệm vụ chính là xử lý và định tuyến lưu lượng dữ liệu tốc độ cao giữa các khu vực mạng, đảm bảo độ trễ tối thiểu và băng thông tối đa. Core Switch thường đóng vai trò là xương sống (backbone) của hệ thống mạng doanh nghiệp hoặc trung tâm dữ liệu, nơi mà toàn bộ lưu lượng từ các access switch, server farm hoặc thiết bị biên hội tụ về.

### 1.1.4. Switch access

Core Switch là thiết bị chuyển mạch trung tâm trong kiến trúc mạng phân tầng (Access – Distribution – Core), đóng vai trò xương sống của hệ thống, đảm nhiệm việc xử lý và định tuyến lưu lượng dữ liệu tốc độ cao giữa các thành phần mạng. Khác với các switch tầng dưới, Core Switch yêu cầu hiệu năng cao, độ tin cậy lớn và khả năng dự phòng mạnh để đảm bảo mạng luôn hoạt động ổn định, thông suốt.

## 1.2. Giới thiệu về các hệ thống giám sát hiện tại của Trung tâm Dịch vụ số Mobifone

Trong bối cảnh hệ thống CNTT ngày càng mở rộng với độ phức tạp cao, nhu cầu giám sát tập trung và hiệu quả là một yêu cầu tất yếu. Hiện nay, Trung tâm Dịch vụ số MobiFone đang sử dụng kết hợp hai hệ thống giám sát phổ biến: Prometheus – một giải pháp mã nguồn mở, và SolarWinds – một giải pháp thương mại toàn diện. Việc áp dụng đồng thời hai công cụ này giúp Trung tâm bao phủ tốt cả hai khía cạnh: giám sát ứng dụng container hóa hiện đại và giám sát thiết bị truyền thống/hạ tầng vật lý.

### 1.2.1. Giải pháp giám sát cảnh báo Prometheus

Prometheus là nền tảng giám sát mã nguồn mở, chuyên thu thập và lưu trữ dữ liệu chuỗi thời gian, phù hợp với hệ thống phân tán, microservices và container như Kubernetes.

Công cụ này sử dụng cơ chế pull để lấy dữ liệu từ các exporter qua HTTP hoặc SNMP, lưu trữ vào cơ sở dữ liệu tích hợp. PromQL hỗ trợ truy vấn, phân tích và xây dựng cảnh báo linh hoạt. Alertmanager cho phép gửi cảnh báo qua email, Slack, Telegram… và hỗ trợ gom nhóm, lọc cảnh báo trùng.

Prometheus dễ tích hợp với Grafana để trực quan hóa dữ liệu, tương thích tốt với các hệ thống cloud-native.

Tại Trung tâm Dịch vụ số MobiFone, Prometheus được dùng để giám sát hệ thống container, máy chủ ứng dụng, tài nguyên phần cứng... giúp phát hiện sự cố sớm, tối ưu chi

phí. Nhược điểm là giao diện gốc chưa thân thiện, cần kết hợp với công cụ như Grafana để hiển thị hiệu quả hơn..

### 1.2.2. Giải pháp giám sát cảnh báo SolarWinds

SolarWinds là giải pháp giám sát mạng thương mại toàn diện, phù hợp với hệ thống quy mô lớn và đa tầng. Hệ thống cho phép theo dõi hiệu suất thiết bị mạng, máy chủ, ứng dụng trong cả môi trường vật lý và ảo hóa.

SolarWinds hỗ trợ giám sát router, switch, firewall, server, thiết bị lưu trữ... theo các chỉ số như băng thông, độ trễ, packet loss. Hệ thống cảnh báo linh hoạt, tích hợp với email, SMS, và các công cụ quản lý sự cố. Tính năng NCM cho phép sao lưu, khôi phục cấu hình thiết bị mạng nhanh chóng. Giao diện Web trực quan, dễ sử dụng, hỗ trợ báo cáo, biểu đồ, heatmap và dashboard tùy biến.

SolarWinds tương thích với nhiều giao thức và thiết bị đa hãng (Cisco, Juniper, Fortinet...), giúp giám sát tập trung hiệu quả.

Tại Trung tâm Dịch vụ số MobiFone, SolarWinds được dùng để giám sát thiết bị mạng lõi, router biên, switch, server, cơ sở dữ liệu và kênh truyền. Giải pháp này hỗ trợ phát hiện nhanh lỗi phần cứng, sự cố mạng, đồng thời giúp tiết kiệm thời gian cấu hình và đảm bảo hỗ trợ kỹ thuật từ nhà cung cấp..

## 1.3. Các vấn đề còn tồn tại

Trong Trung tâm Dịch vụ số của Mobifone, việc sử dụng cả Prometheus và SolarWinds là một nỗ lực để đảm bảo việc giám sát toàn diện và hiệu quả của hệ thống mạng và dịch vụ. Tuy nhiên, sự không đồng bộ giữa hai hệ thống này có thể dẫn đến các vấn đề như:

- **Thiếu tính nhất quán trong dữ liệu**: Prometheus và SolarWinds sử dụng các cơ chế thu thập và lưu trữ dữ liệu khác nhau, dẫn đến sự không nhất quán trong thông tin giám sát. Điều này có thể gây ra hiểu nhầm và ảnh hưởng đến quyết định quản lý.
- **Khó khăn trong cấu hình và quản lý**: Việc phải quản lý hai hệ thống riêng biệt đòi hỏi nhiều công sức và tài nguyên. Các nhân viên cần phải có kiến thức sâu về cả hai nền tảng để có thể cấu hình và quản lý hiệu quả.
- **Thiếu khả năng tích hợp**: Không có khả năng tích hợp hoặc tích hợp hạn chế giữa Prometheus và SolarWinds có thể gây ra rào cản trong việc chia sẻ dữ liệu giám sát và tổ chức các quy trình quản lý.

Vì vậy, để đạt được một hệ thống giám sát toàn diện và hiệu quả hơn, việc tìm kiếm một giải pháp giám sát thống nhất và tích hợp hơn là cần thiết. Một nền tảng giám sát đồng

nhất sẽ giúp Trung tâm Dịch vụ số Mobifone tăng cường khả năng quản lý và giám sát hệ thống mạng và dịch vụ của mình một cách hiệu quả và đáng tin cậy hơn.

## 1.4. Giải pháp

Để đảm bảo vận hành ổn định hệ thống mạng tại Trung tâm Dịch vụ số MobiFone, việc giám sát hoạt động toàn hệ thống là yếu tố then chốt. Các sự cố như thiết bị lỗi, tấn công mạng, hay tài nguyên quá tải cần được phát hiện và cảnh báo sớm để xử lý kịp thời. Trong môi trường mạng lớn có thiết kế dự phòng, nếu không phát hiện nhanh sự cố ở phần chính, nguy cơ mất ổn định sẽ tăng cao dù thành phần dự phòng vẫn hoạt động. Thiếu công cụ giám sát sẽ khiến quản trị viên bị động trước các tình huống bất ngờ.

Các lý do cần thực hiện sử dụng hệ thống giám sát mạng tập trung:

- Biết được những gì xảy ra trên hệ thống
- Lên kế hoạch cho việc sửa chữa và thay thế
- Chuẩn đoán nhanh chóng các lỗi phát sinh
- Xem xét và có báo cáo trực quan về các hoạt động của hệ thống
- Theo dõi hoạt động của các tài nguyên trong hệ thống
- Đảm bảo hệ thống hoạt động liên tục
- Tiết kiệm thời gian, chi phí **:** giảm thiểu tối đa thời gian nhân sự quản trị và chi phí điều tra sự cố.

## 1.5. Kết luận chương 1

Việc khảo sát và đánh giá hạ tầng mạng của Trung tâm Dịch vụ số Mobifone đã chỉ ra rằng, mặc dù hệ thống hiện tại có vai trò quan trọng trong việc hỗ trợ các dịch vụ giá trị gia tăng, nhưng vẫn tồn tại nhiều vấn đề cần được cải thiện. Các thách thức về giám sát hiệu suất, quản lý bảo mật, và khả năng dự phòng đã được nhận diện, từ đó đặt ra yêu cầu cấp thiết về việc nâng cấp hệ thống giám sát hạ tầng một cách tập trung và hiệu quả hơn. Hạ tầng mạng hiện tại còn thiếu sự tích hợp giữa các hệ thống giám sát riêng lẻ, dẫn đến sự thiếu đồng bộ trong việc phát hiện và xử lý sự cố. Việc triển khai một giải pháp giám sát toàn diện sẽ không chỉ giúp tối ưu hóa hiệu năng của hệ thống mà còn góp phần đảm bảo tính ổn định và an toàn cho hoạt động của Trung tâm Dịch vụ số Mobifone.

Những vấn đề này sẽ là nền tảng để nghiên cứu và đề xuất giải pháp giám sát phù hợp trong các chương tiếp theo, đặc biệt là giải pháp Polestar, nhằm nâng cao khả năng quản lý và tối ưu hóa hạ tầng mạng

# CHƯƠNG 2: NGHIÊN CỨU GIẢI PHÁP POLESTAR

## 2.1. Tổng quan về quản lý mạng

Trong thế giới ngày nay, hệ thống quản lý hạ tầng mạng (Network Infrastructure Management System) không chỉ đơn thuần là một công cụ giám sát, mà còn là trái tim của mọi hệ thống mạng hiện đại. Chương này sẽ mở đầu với mục tiêu là tìm hiểu sâu hơn về các thành phần cơ bản của hệ thống quản lý hạ tầng mạng và cách chúng hoạt động, đồng thời xem xét kiến trúc quản lý mạng dựa trên mô hình TMN.

### 2.1.1. Các thành phần cơ bản của hệ thống quản lý mạng hạ tầng

Hệ thống quản lý mạng hạ tầng là một tập hợp các công cụ và phần mềm được sử dụng để giám sát, quản lý và điều khiển mạng máy tính. Hệ thống quản lý mạng hạ tầng giúp quản trị viên mạng theo dõi hiệu suất của mạng, xác định và khắc phục sự cố, cũng như thực hiện các thay đổi cấu hình mạng.

- **Quản lý thiết bị (Element Management)**

Quản lý thiết bị là thành phần quan trọng trong hệ thống quản lý hạ tầng mạng, nhằm đảm bảo mỗi thiết bị vận hành ổn định và hiệu quả. Trước hết, hệ thống thực hiện kiểm kê tài sản, ghi nhận đầy đủ thông tin như nhà sản xuất, số serial, địa chỉ MAC/IP, vị trí triển khai…, giúp theo dõi và quản lý thiết bị chính xác.

- **Quản lý kết nối (Connection Management)**

Quản lý kết nối là yếu tố thiết yếu trong quản trị hạ tầng mạng, nhằm đảm bảo các kết nối giữa thiết bị luôn ổn định và đạt hiệu suất cao. Hệ thống giúp giám sát băng thông, điều chỉnh lưu lượng phù hợp để tránh nghẽn mạng và ưu tiên cho các ứng dụng quan trọng.

- **Quản lý bảo mật (Security Management)**

Quản lý bảo mật là thành phần thiết yếu trong hệ thống quản lý hạ tầng mạng, giúp bảo vệ thông tin và ngăn chặn các mối đe dọa từ bên trong lẫn bên ngoài. Một nhiệm vụ trọng tâm là quản lý tường lửa, bao gồm thiết lập và duy trì các chính sách kiểm soát truy cập để ngăn chặn kết nối trái phép và phòng chống tấn công.

### 2.1.2. Các chức năng quản lý

Các chức năng quản lý trong hệ thống quản lý hạ tầng mạng là những hoạt động quan trọng nhằm đảm bảo sự ổn định, hiệu quả, và an toàn của mạng. Các chức năng này không chỉ giúp quản trị viên theo dõi mạng một cách chi tiết mà còn cung cấp các công cụ để cấu hình và giải quyết vấn đề nhanh chóng. Dưới đây là các chức năng quản lý quan trọng:

- Giám Sát (Monitoring)

- Cấu hình (Configuration)
- Quản lý sự cố (Fault Management)
- Bảo mật (Security)
- Tích hợp và mở rộng (Integration and Scalability)

### 2.1.3. Kiến trúc quản lý mạng dựa trên TMN

Trong các mạng viễn thông hiện đại, dịch vụ và tài nguyên mạng được triển khai theo mô hình đa lớp, gắn liền với các hệ thống quản lý và điều hành (OAM&P) riêng biệt cho từng cặp dịch vụ – tài nguyên. Do các phần tử mạng có các thuộc tính OAM&P riêng biệt, hệ thống quản lý mạng cũng cần thiết lập các vùng quản lý riêng cho từng loại phần tử, và các vùng này thường ít liên quan trực tiếp với nhau.

Theo hướng tiếp cận mạng thông minh (TMN – Telecommunication Management Network), việc quản lý mạng được tổ chức dựa trên các giao diện chuẩn giữa các khối chức năng chính như: hệ thống điều hành, phần tử mạng và mạng thông tin số liệu. TMN cũng đưa ra nguyên tắc điều khiển phân mạng, cho phép mở rộng và phát triển mạng quản lý phù hợp với yêu cầu tương lai.

Từ góc độ chức năng, quản lý mạng được chia thành 5 nhóm chính:

- Quản lý hiệu năng;
- Quản lý sự cố;
- Quản lý cấu hình;
- Quản lý tài khoản;
- Quản lý bảo mật.

#### 2.1.3.1. Quản lý hiệu năng

Quản lý hiệu năng là quá trình giám sát và tối ưu hoạt động của hạ tầng mạng nhằm đảm bảo hệ thống vận hành ổn định, hiệu quả và đáp ứng yêu cầu của người dùng.

- Giám sát hoạt động

Điều khiển và quản lý hoạt động mạng là quy trình then chốt giúp duy trì hiệu suất, tối ưu tài nguyên và đảm bảo hệ thống hoạt động ổn định. Nội dung chính bao gồm điều khiển lưu lượng và quản lý lưu lượng.

- Phân tích hoạt động

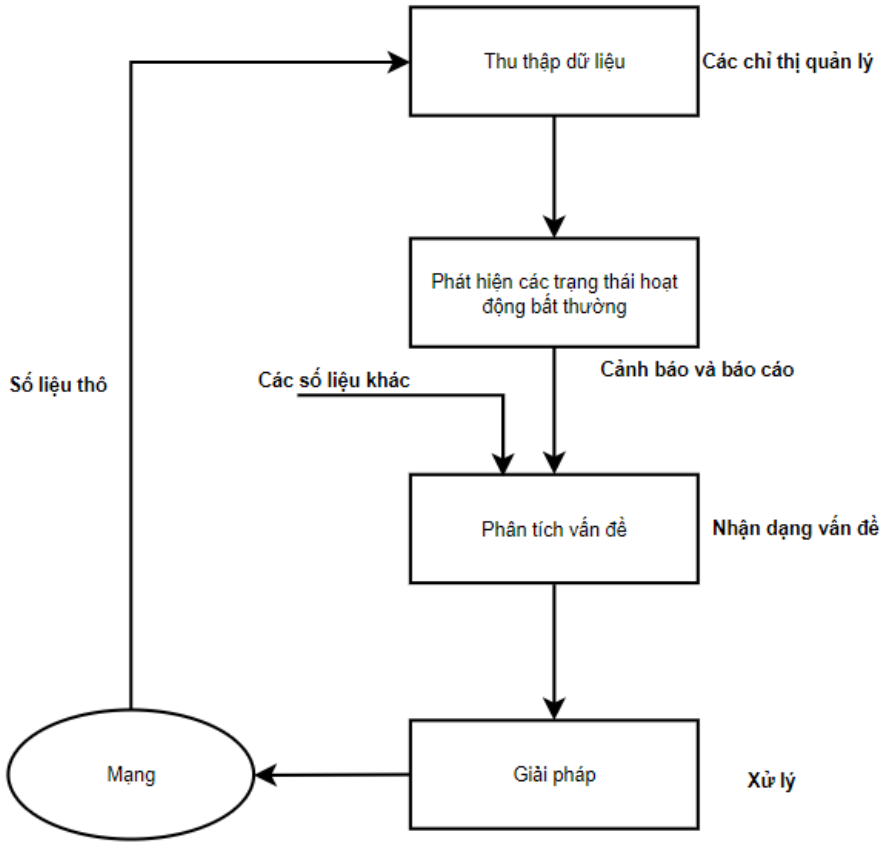
Phân tích hoạt động là khâu quan trọng trong quản lý hiệu năng, giúp người quản trị hiểu rõ tình trạng vận hành hệ thống, từ đó phát hiện và xử lý kịp thời các vấn đề có thể ảnh hưởng đến hiệu suất mạng.

– Đảm bảo chất lượng hoạt động

Đảm bảo chất lượng hoạt động là yếu tố then chốt giúp duy trì sự ổn định, tin cậy và hiệu quả của các dịch vụ CNTT. Việc này bao gồm đánh giá hiệu suất mạng định kỳ, đảm bảo các chỉ số như tốc độ, độ trễ, và khả năng đáp ứng luôn đạt yêu cầu, đặc biệt trong điều kiện tải cao.

### 2.1.3.2. Quản lý sự cố (Fault Management)

Quản lý sự cố trong mạng là một quá trình phức tạp nhằm đảm bảo rằng mạng luôn hoạt động ổn định và có khả năng phục hồi nhanh chóng sau khi gặp phải các vấn đề. Quá trình này được đưa ra theo mô hình tại *Hình 2.1* bao gồm ba chức năng chính: Giám sát cảnh báo, cô lập sự cố, sửa chữa và kiểm tra lỗi.




**Hình 2. 1: Sơ đồ quản lý sự số**

### 2.1.3.3. Quản lý cấu hình (Configuration Management)

Quản lý cấu hình là một phần quan trọng trong việc duy trì tính ổn định và an toàn của hạ tầng mạng. Nó bao gồm việc quản lý các thiết lập và cấu hình của các thiết bị mạng, ứng dụng và hệ thống để đảm bảo chúng hoạt động đúng cách và tuân thủ các yêu cầu bảo mật. Dưới đây là các khía cạnh cơ bản của quản lý cấu hình:

- Cung cấp cấu hình
- Trạng thái và điều khiển thiết bị
- Cài đặt thiết bị

#### 2.1.3.4. Quản lý tài khoản (Accounting Management)

Quản lý tài khoản là một phần quan trọng trong việc bảo đảm an toàn cho hệ thống. Điều này bao gồm việc tạo và quản lý tài khoản người dùng, giúp xác định quyền truy cập của họ. Để đảm bảo chỉ những người được ủy quyền mới có thể vào hệ thống, chúng ta cần sử dụng các phương pháp xác thực đáng tin cậy. Bên cạnh đó, việc quản lý quyền truy cập cho từng tài khoản giúp đảm bảo người dùng chỉ có thể truy cập vào các tài nguyên và chức năng cần thiết cho công việc của họ. Phần này sẽ khám phá các bước cần thiết trong việc quản lý tài khoản, từ việc tạo tài khoản đến xác thực và quản lý quyền truy cập.

- Tạo và quản lý quản lý tài khoản người dùng.
- Xác thực và xác minh.
- Quản lý quyền truy cập.
- Theo dõi và đánh giá.

#### 2.1.3.5. Quản lý bảo mật (Security Management)

Quản lý bảo mật là quá trình quản lý và bảo vệ các tài nguyên thông tin hệ và hệ thống của tố chức khỏi các mối đe dọa và rủi ro bảo mật.

Giúp quản lý và điều khiển quyền truy cập tới các thiết bị có trong hạ tầng mạng, quản lý bảo mật gồm các chức năng sau:

- Xác định quyền truy nhập.
- Điều khiển truy nhập.
- Mã hóa và kiểm soát khóa mã hóa.
- Ủy quyền truy nhập.
- Đăng ký bảo mật.

### 2.2. Một số giải pháp giám sát hiện nay

Trong thời đại số hiện nay, mạng thông tin đã trở thành một hệ thống phức tạp với quy mô ngày càng mở rộng, chịu áp lực lớn từ tốc độ phát triển công nghệ và sự phổ biến của các ứng dụng kỹ thuật số. Điều này đòi hỏi phải có những giải pháp giám sát và cảnh báo mạng hiệu quả nhằm đảm bảo hoạt động ổn định, an toàn cho toàn hệ thống.

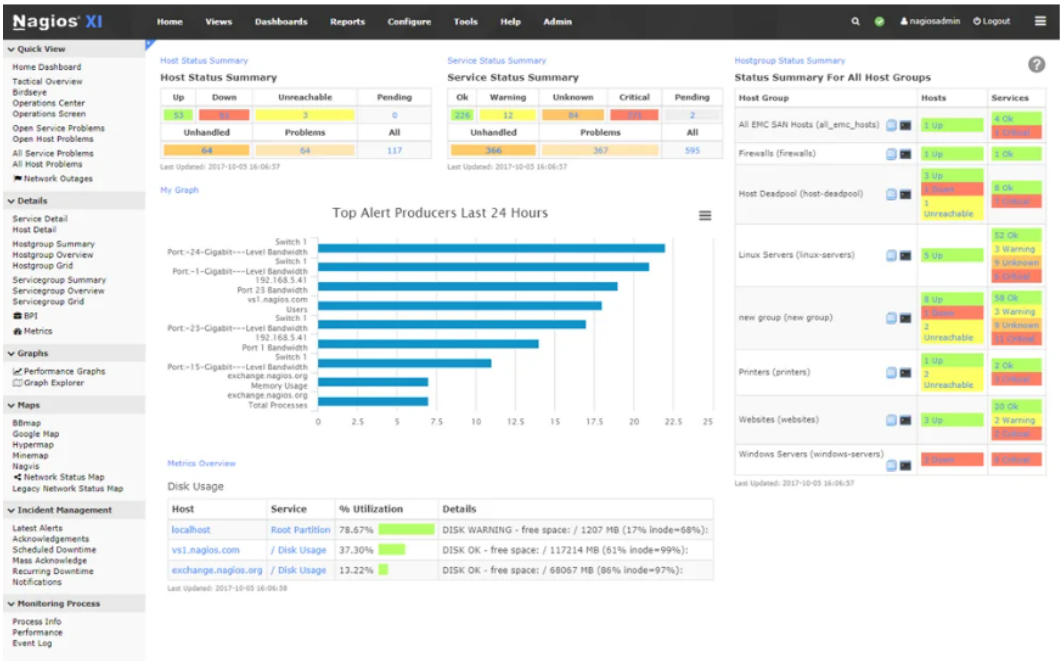
Sự gia tăng nhanh chóng về số lượng thiết bị và ứng dụng khiến công tác quản lý mạng trở nên khó khăn hơn. Doanh nghiệp không chỉ cần theo dõi hiệu suất của thiết bị mà còn

phải đối mặt với các nguy cơ về bảo mật, lỗi kỹ thuật và sự không ổn định trong vận hành dịch vụ..

### 2.2.1. Giải pháp giám sát cảnh báo Nagios:

Nagios được phát triển lần đầu tiên vào năm 1999 bởi Ethan Galstad với tên gọi ban đầu là NetSaint. Sau đó, nó được đổi tên thành Nagios và phát triển thành một dự án mã nguồn mở vào năm 2004. Nagios nhanh chóng trở thành một trong những phần mềm giám sát phổ biến nhất do tính linh hoạt, dễ sử dụng và khả năng mở rộng của nó.

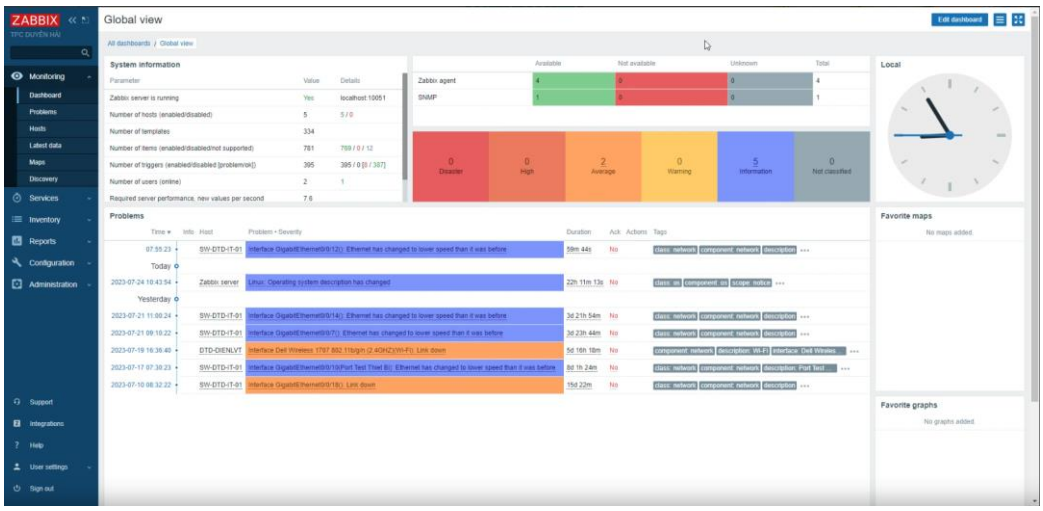
Nagios hoạt động dựa trên mô hình client-server. Máy chủ Nagios được cài đặt trên một máy tính trung tâm và các agent được cài đặt trên các máy chủ, thiết bị mạng và các hệ thống khác cần được giám sát. Agent sẽ thu thập dữ liệu về trạng thái và hiệu suất của hệ thống và gửi dữ liệu này về máy chủ Nagios. Máy chủ Nagios sẽ phân tích dữ liệu và đưa ra thông báo hoặc cảnh báo nếu có bất kỳ vấn đề nào xảy ra như màn hình thông báo tại *Hình 2.2*.




**Hình 2. 2: Giải pháp giám sát cảnh báo Nagios**

### 2.2.2. Giải pháp giám sát cảnh báo Zabbix:

Zabbix là phần mềm giám sát mã nguồn mở được phát triển từ năm 1998, chính thức ra mắt năm 2001. Hoạt động theo mô hình client-server, Zabbix cho phép giám sát hiệu suất và trạng thái của hệ thống thông qua các agent cài đặt trên máy chủ hoặc thiết bị mạng. Dữ liệu thu thập sẽ được gửi về máy chủ trung tâm để phân tích và đưa ra cảnh báo kịp thời khi có sự cố.




**Hình 2. 3: Giải pháp giám sát cảnh báo Zabbix**

### 2.2.3. Giải pháp giám sát cảnh báo PRTG Network Monitor

PRTG Network Monitor được phát triển bởi Paessler AG, một công ty Đức được thành lập vào năm 1997. Phiên bản đầu tiên của PRTG được phát hành vào năm 2000 và nhanh chóng trở thành một trong những phần mềm giám sát mạng phổ biến nhất trên thị trường. PRTG hiện có hơn 200.000 người dùng trên toàn thế giới và được dịch sang hơn 30 ngôn ngữ.

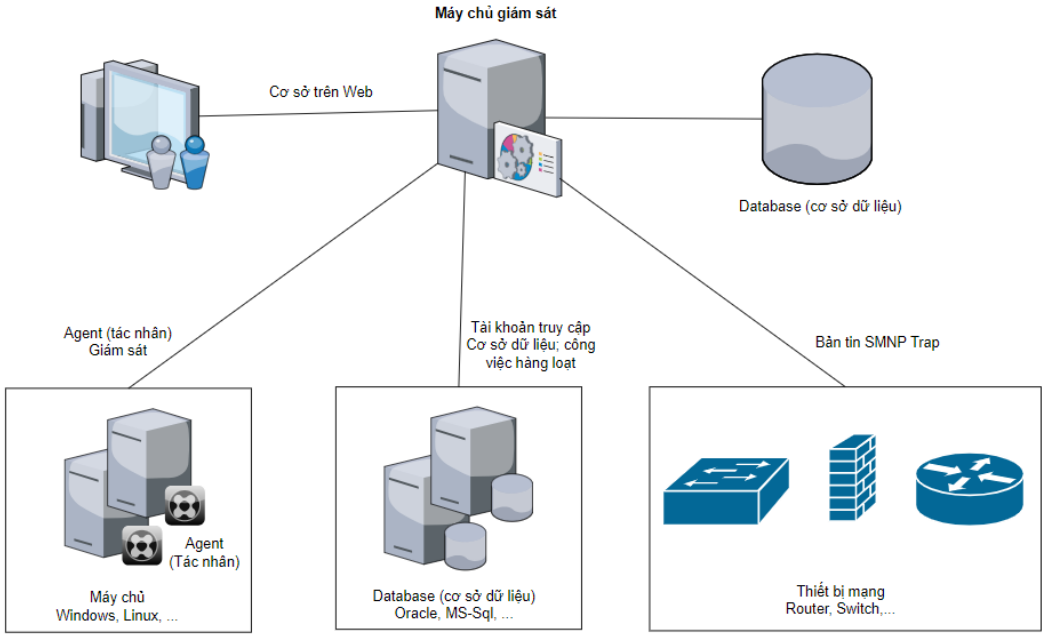
PRTG Network Monitor hoạt động dựa trên mô hình client-server. Máy chủ PRTG được cài đặt trên một máy tính trung tâm và các probe PRTG được cài đặt trên các máy chủ, thiết bị mạng và các hệ thống khác cần được giám sát. Probe PRTG sẽ thu thập dữ liệu về trạng thái và hiệu suất của hệ thống và gửi dữ liệu này về máy chủ PRTG. Máy chủ PRTG sẽ phân tích dữ liệu và đưa ra thông báo hoặc cảnh báo nếu có bất kỳ vấn đề nào xảy ra như màn hình thông báo tại *Hình 2.4*.


**Hình 2. 4: Giải pháp giám sát cảnh báo PRTG Network Monitor**

## 2.3. Giải pháp giám sát cảnh báo Polestar

### 2.3.1. Giới thiệu về hệ thống

Hệ thống giám sát Polestar (OMC) là hệ thống giám sát tập trung hoạt động của các hệ thống VAS về cơ bản dựa trên nguyên lý thu thập các thông tin từ các đối tượng cần được theo dõi, phân tích, xử lý và đưa ra cảnh báo cho người quản trị hệ thống qua các kênh khác nhau: SMS, Email, âm thanh, giao diện quản lý. Giải pháp theo dõi tập trung hoạt động của các hệ thống VAS đang được sử dụng để thu thập thông tin từ các đối tượng được theo dõi, cụ thể như sơ đồ tại *Hình 2.5* như sau:




**Hình 2. 5: Sơ đồ tổng quan kết nối hệ thống giám sát Polestar**

Hệ thống giám sát được cấu thành từ bốn thành phần chính gồm: Node, Manager, Viewer, Repository. Đóng vai trò then chốt trong việc đảm bảo hoạt động giám sát toàn diện và hiệu quả cho hạ tầng công nghệ thông tin.

Sự phối hợp chặt chẽ giữa các thành phần này tạo nên một hệ thống giám sát hoàn chỉnh, giúp nâng cao khả năng quản lý, kiểm soát và bảo vệ hạ tầng CNTT của tổ chức một cách hiệu quả và chủ động.

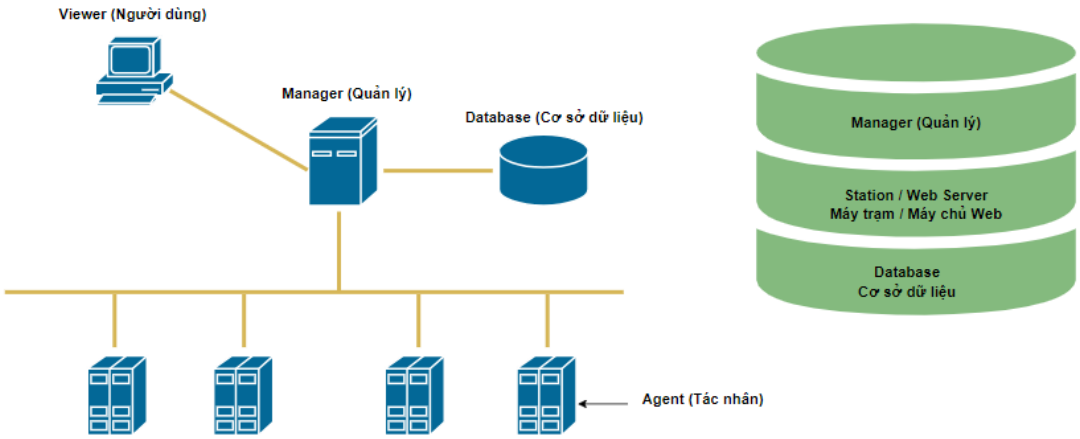
### 2.3.2. Các đối tượng giám sát

Hệ thống giám sát Polestar được thiết kế để cung cấp cái nhìn toàn diện và chi tiết về hạ tầng công nghệ thông tin thông qua việc theo dõi nhiều đối tượng quan trọng gồm có:

- Máy chủ.
- Thiết bị mạng.
- Cơ sở dữ liệu.

### 2.3.3. Kiến trúc hệ thống giám sát Polestar

Mô hình kết nối giữa các thành phần của hệ thống giám sát Polestar được xây dựng theo kiến trúc tập trung, đảm bảo khả năng thu thập, xử lý và hiển thị dữ liệu giám sát một cách hiệu quả và đồng bộ. Các thành phần chính trong mô hình tại Hình 2.8.




**Hình 2. 8: Mô hình hệ thống giám sát sử dụng Polestar**

### 2.3.4. Các chức năng giám sát chính

Giám sát hệ thống là một yếu tố cốt lõi giúp duy trì hiệu quả và ổn định cho hạ tầng mạng, đặc biệt trong các tổ chức lớn như Trung tâm Dịch vụ số Mobifone. Với sự phát triển nhanh chóng của công nghệ, nhu cầu theo dõi chi tiết từng thông số hoạt động và khả năng phản ứng kịp thời với các bất thường trở nên cấp thiết. Polestar mang đến một giải pháp toàn diện với nhiều tính năng giám sát mạnh mẽ, không chỉ cung cấp khả năng giám sát thời gian thực mà còn hỗ trợ phân tích và tối ưu hóa hiệu suất hệ thống. Trong phần này, chúng ta sẽ đi sâu vào các chức năng giám sát chính mà Polestar cung cấp, bao gồm theo dõi hiệu suất, bản đồ hình thái học, bảng điều khiển hệ thống, và nhiều công cụ hữu ích khác để quản trị viên có thể dễ dàng quản lý, giám sát và xử lý sự cố trong hệ thống.

– **Real-time Monitoring**

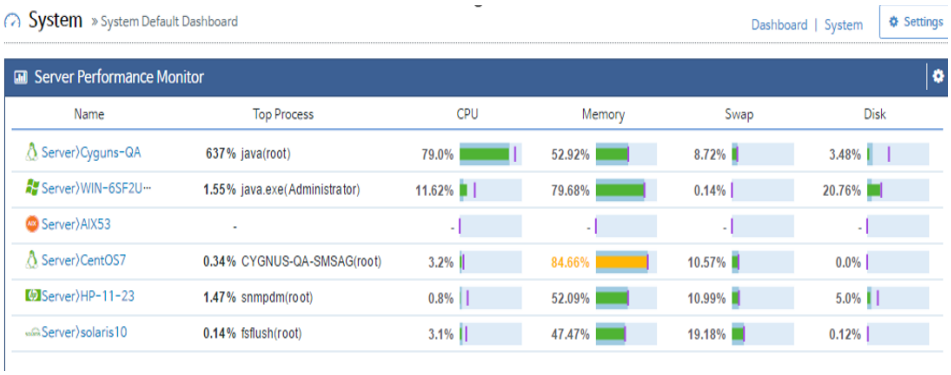
Polestar hỗ trợ bảng điều khiển giám sát thời gian thực để xem các chỉ số chính của tài nguyên được thu thập thời gian thực trên một màn hình duy nhất như *Hình 2.12*. Hiện tại, bảng điều khiển giám sát Real-time Monitoring chỉ hỗ trợ giám sát các thông số: CPU, Memory Utilization của máy chủ Servers.

– **Topology Map**

POLESTAR cung cấp chức năng bản đồ hình thái học (Topology Map) cho phép người dùng trực quan hóa các kết nối giữa các tài nguyên trong hệ thống. Mỗi tài khoản có thể tạo và chỉnh sửa số lượng bản đồ tùy ý, đồng thời thêm các tài nguyên và liên kết giữa các nút để hiển thị mối quan hệ kết nối.

– **System Dashboard**

POLESTAR cung cấp một bảng điều khiển dựa trên các thiết bị với các nhãn, bảng và biểu đồ hiển thị thông tin về trạng thái tài nguyên, danh sách cảnh báo, top 5 trạng thái, vv., trên một trang duy nhất.




**Hình 2. 14: Giao diện màn hình System Dashboard của hệ thống Polestar**

– **Xem trạng thái về hiệu năng**

Polestar cung cấp một giao diện quản lý nhiều chỉ số của tất cả các thiết bị trong hệ thống trên một màn hình tập trung. Danh sách các máy chủ được Polestar quản lý và hiển thị trên một màn hình tập trung cùng các thông tin cơ bản của chúng như trạng thái hoạt động, CPU, bộ nhớ, hệ thống file …

– **Chức năng View Event**

Chức năng View Event trong hệ thống giám sát Polestar cho phép quản trị viên theo dõi, phân tích và đánh giá chi tiết các sự kiện phát sinh trong hệ thống mạng. Giao diện Review Event cung cấp biểu đồ thống kê theo thời gian và theo tài nguyên, giúp hiển thị rõ ràng số lượng sự kiện được phân loại theo mức độ nghiêm trọng (Critical, Major, Minor, Warning).

– **Sử dụng chức năng kiểm soát lỗi Alarm Console**

Xem thông tin về lịch sử lỗi trong toàn hệ thống tại *Hình 2.19*.


**Hình 2. 19: Giao diện màn hình cảnh báo tập trung của hệ thống Polestar**

– **Thiết lập ngưỡng cảnh báo**

Để thiết lập các cảnh báo trợ giúp người dùng quản trị phòng ngừa các sự cố liên quan đến việc quá tải (CPU, Ram, …) Đầy dung lượng (File System, tablespace, …), Polestar cho phép người dùng tự thiết lập các cảnh báo với cấp độ mà cảnh báo được kích hoạt, được điều chỉnh một cách mềm dẻo thông qua chức năng Threshold Setting. Có 3 phương thức được sử dụng để thiết lập ngưỡng:

## 2.4. Đánh giá tổng quan về các giải pháp giám sát

Từ bảng so sánh tổng quan, có thể thấy mỗi giải pháp giám sát mạng đều có thế mạnh riêng phù hợp với từng nhu cầu sử dụng. Polestar nổi bật nhờ khả năng giám sát thông minh, tích hợp trí tuệ nhân tạo (AI) để phân tích và dự đoán, rất phù hợp với các hệ thống mạng lớn và phức tạp. Zabbix là lựa chọn tối ưu cho doanh nghiệp có đội ngũ kỹ thuật chuyên sâu, cần sự linh hoạt cao trong cấu hình và mở rộng.

Nagios phù hợp với tổ chức có ngân sách hạn chế và hệ thống nhỏ, tuy nhiên yêu cầu người triển khai phải có kiến thức kỹ thuật tốt để vận hành hiệu quả. Trong khi đó, PRTG lại được ưa chuộng trong các doanh nghiệp vừa và nhỏ nhờ giao diện thân thiện, dễ sử dụng và triển khai nhanh, dù còn hạn chế khi mở rộng quy mô giám sát.

## 2.5. Kết luận chương 2

Trong chương này, luận án đã trình bày một cách toàn diện về các thành phần cơ bản, chức năng quản lý và kiến trúc hệ thống giám sát hạ tầng mạng hiện đại, đặc biệt là trong bối cảnh của mô hình quản lý TMN. Qua việc phân tích sâu các chức năng như giám sát, cấu hình, quản lý sự cố, bảo mật và khả năng tích hợp – mở rộng, có thể khẳng định rằng một hệ thống giám sát hiệu quả cần có khả năng chủ động, toàn diện và linh hoạt để đáp ứng các yêu cầu ngày càng cao trong quản lý hạ tầng mạng.

Giải pháp Polestar đã được đánh giá và phân tích như một mô hình tiên tiến, có khả năng tích hợp cao và cung cấp chức năng giám sát mạnh mẽ thông qua nhiều giao thức khác nhau như SNMP, RMON và agent-based. Với các tính năng như giám sát theo thời gian thực, cảnh báo tức thời, khả năng dự đoán nhờ AI và giao diện trực quan, Polestar nổi bật so với các giải pháp truyền thống khác như Nagios, Zabbix hay PRTG. Những phân tích và đánh giá trong chương này đã làm rõ sự ưu việt và tính ứng dụng cao của Polestar trong việc nâng cao hiệu quả giám sát và vận hành hạ tầng mạng tại các doanh nghiệp lớn như Trung tâm Dịch vụ số Mobifone.

# CHƯƠNG 3: ỨNG DỤNG GIẢI PHÁP GIÁM SÁT POLESTAR CHO HẠ TẦNG MẠNG TRUNG TÂM DỊCH VỤ SỐ MOBIOFNE

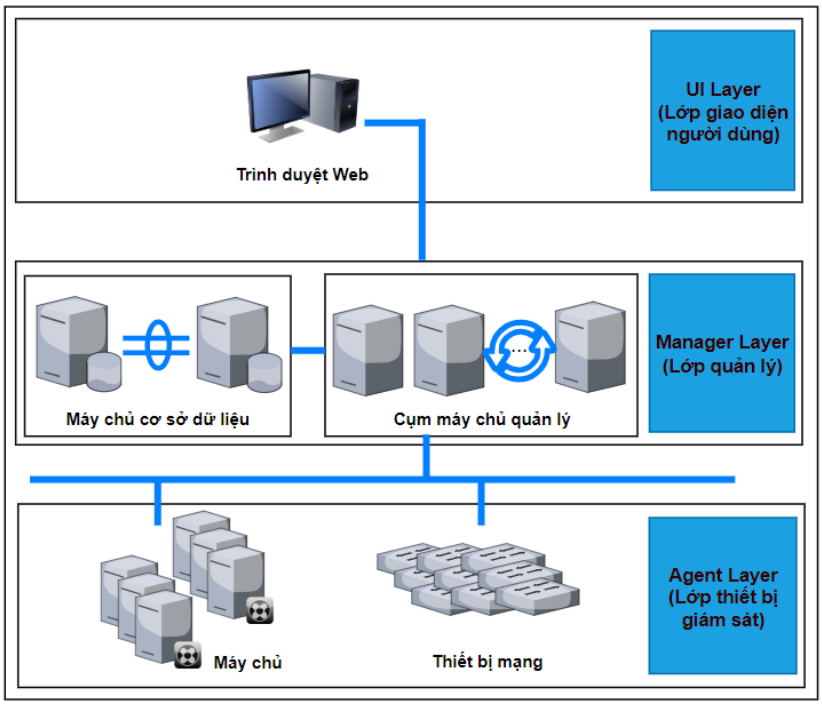
## 3.1. Đặt vấn đề

Trong bối cảnh hệ thống CNTT ngày càng phức tạp, việc giám sát mạng đóng vai trò quan trọng nhằm đảm bảo hiệu suất, an toàn và tính liên tục trong vận hành. Tại Trung tâm Dịch vụ số MobiFone, hệ thống mạng chứa nhiều dữ liệu quan trọng, đòi hỏi phải được giám sát chặt chẽ để phát hiện sớm sự cố và tối ưu tài nguyên.

Tuy đã có nhiều công cụ hỗ trợ, nhưng chi phí cao hoặc thiếu linh hoạt khiến việc lựa chọn giải pháp phù hợp gặp nhiều khó khăn. Do đó, việc xây dựng một hệ thống giám sát hiệu quả, phù hợp với hạ tầng hiện có là yêu cầu cấp thiết nhằm nâng cao hiệu quả quản lý và đảm bảo chất lượng dịch vụ.

## 3.2. Giải pháp giám sát cho hạ tầng mạng của Trung tâm Dịch vụ số Mobifone

### 3.2.1. Giới thiệu mô hình




**Hình 3. 1: Mô hình giải pháp giám sát hạ tầng mạng Trung tâm Dịch vụ số Mobifone**

Trong *Hình 3.1* này gồm có 3 lớp riêng biệt:

- UI Layer (Lớp giao diện người dùng)
- Manager Layer (Lớp quản lý)
- Agent Layer

### 3.2.2. Kịch bản giám sát hệ thống mạng

Xây dựng kịch bản giám sát thiết bị mạng (Server và Devices network) trong hệ thống mạng bao gồm: máy chủ chạy hệ điều hành Linux và thiết bị mạng Switch Cisco.

– Giám sát trạng thái trên các thiết bị mạng
– Giám sát việc sử dụng tài nguyên
– Giám sát lưu lượng mạng vào ra trên các thiết bị mạng
– Giám sát lưu lượng vào ra trên các interface của thiết bị mạng: tổng lưu lượng vào ra
– Thông tin, quản lý dữ liệu giám sát của các thiết bị mạng
– Cảnh báo

### 3.2.3. Tiến trình xây hệ thống giám sát

– Mở kết nối từ máy chủ cần tích hợp đến hệ thống giám sát hạ tầng mạng Polestar
– Thêm thiết bị trên giao diện người dùng
– Sau khi thêm thiết bị ta sẽ có thông tin thiết bị gồm các trường: Availability, CPU, Memory, Top 5 Disk IO, Top 5 Filesystem, Alarm, Information.

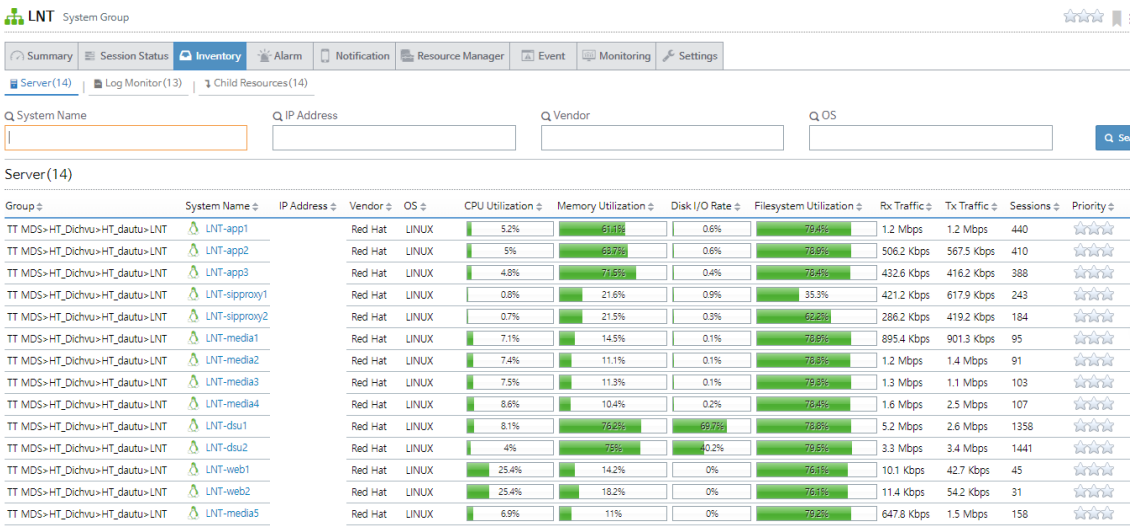
### 3.2.4. Thiết lập cảnh báo

– Tạo Role người dùng
– Tạo tài khoản
– Tiếp tục add role đã tạo “test canh bao” với user đã được tạo.

## 3.3.Đánh giá hoạt động của hệ thống

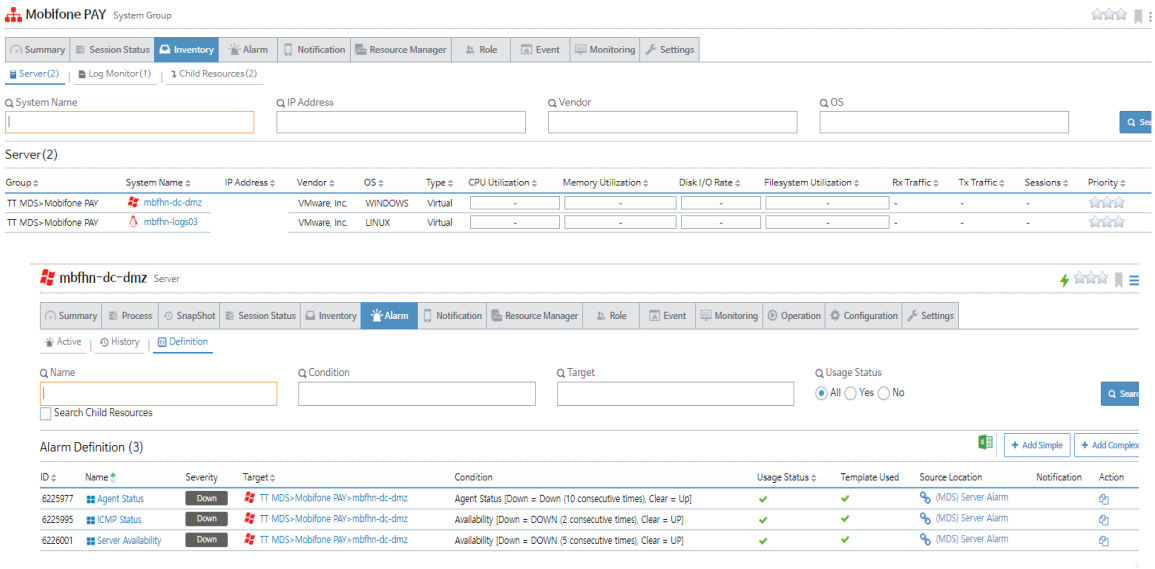
### 3.3.1. Giám sát các trạng thái của host

Theo dõi trạng thái của máy chủ đã được tích hợp ở tab Inventory trong System Group LNT.



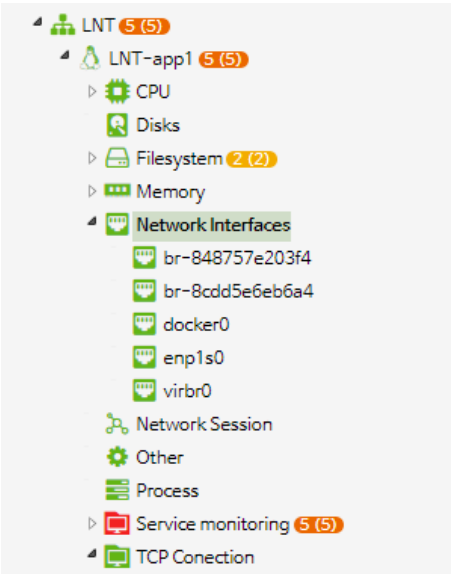

**Hình 3. 8: Giao diện chi tiết thiết bị đã được thêm của nhóm LNT trên hệ thống Polestar**

Trường hợp báo lỗi Polestar Agent như trong *Hình 29*: System Name mbf-dc-dmz và mbfhn-log3 của System Group TT MDS-Mobifone PAY đang báo đỏ (Down). Để kiểm tra lỗi rõ hơn ta Click 2 lần vào Host đang lỗi và vào tab Alarm như *Hình 3.9* sẽ thấy được hiện tại có 3 cảnh báo lỗi: Agent Status (Polestar Agent mất kết nối Port 31001-31003), ICMP Status (Kết nối ICMP đến Polestar đang mất kết nối), Server Availability (Trạng thái Server đang không hoạt động).



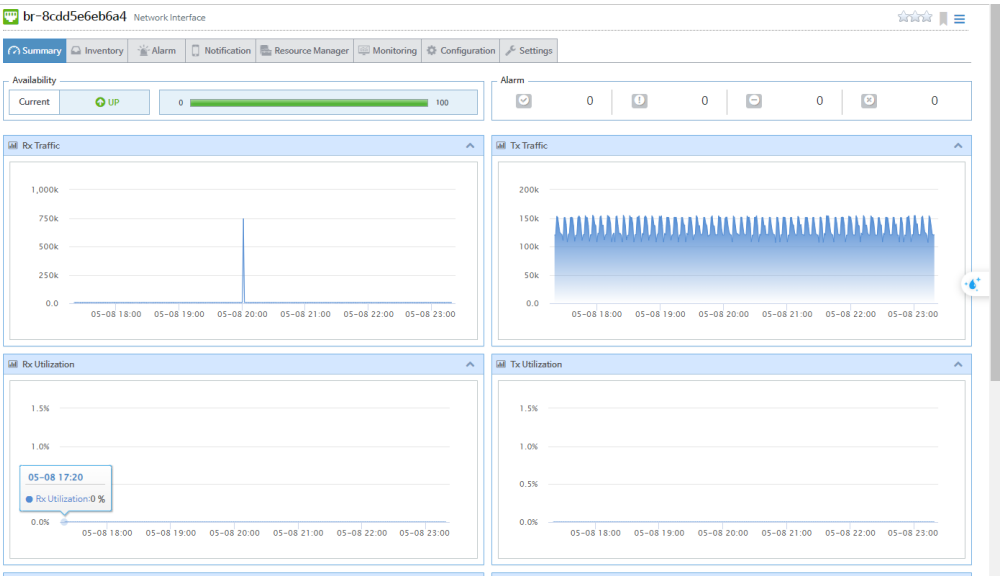

**Hình 3. 9: Giao diện kiểm tra lỗi tích hợp thiết bị trên hệ thống Polestar**

Để kiểm tra trạng thái của các Interfaces trên một host ta Vào Host LNT-app1 như *Hình 3.10* có thể thấy được các Interfaces đang được list trên host đó (Gồm 5 Interfaces)




**Hình 3. 10: Cột các hạng mục của hệ thống được tích hợp giám sát**

Để kiểm tra traffic của từng Interfaces ta chọn vào từng Interfaces cần kiểm tra và vào Tab Summary như *Hình 3.11* để thấy được các biểu đồ thông tin chi tiết trạng thái của Interfaces cần kiểm tra.




**Hình 3. 11: Bảng chi tiết các thông số kỹ thuật của Network interface**

Tính năng giám sát trạng thái host trong Polestar cho phép theo dõi toàn diện hoạt động của các máy chủ theo thời gian thực. Việc hiển thị rõ ràng trạng thái bằng màu sắc (xanh – hoạt động, đỏ – ngưng hoạt động) giúp người quản trị dễ dàng nhận diện các thiết bị gặp sự cố. Đồng thời, chức năng cảnh báo chi tiết như lỗi kết nối Agent, lỗi ICMP hay mất tín hiệu từ server cung cấp thông tin kịp thời và trực quan. Tuy nhiên, việc giám sát trạng thái có thể được nâng cao hơn nữa nếu tích hợp thêm khả năng tự động phân tích nguyên nhân sự cố (RCA) và đề xuất hướng xử lý bằng AI

### 3.3.2. Giám sát các tài nguyên của host

Trong Polestar (Web) việc hiển thị trạng thái tài nguyên host được thể hiện trong mục Group của từng Host (Trạng thái xanh là UP, đỏ là Down).

Về thông số các tài nguyên của Host ta có thể xem tổng quan tại tab Summary của Host như: CPU, Memory. Top 5 Process, Top 5 Disk, Top 5 Filesystem, Rx/Tx traffic, CPU Utilization, …

### 3.3.3. Giám sát trạng thái hoạt động của các Service trên các host

Tại tab Process của máy chủ LNT-app1 ta có 2 lựa chọn kiểu xem là Graph (dạng biểu đồ) như hình và Table (Thông tin bảng cột) thống kê chi tiết về tất cả các Process đang chạy trên các host với đầy đủ các thông tin: PID, PPID, Process Nam, CPU/Memory Utilazition, …

Thông qua tab Process, Polestar hỗ trợ cả hai chế độ hiển thị dạng biểu đồ và bảng dữ liệu, cho phép người quản trị theo dõi đầy đủ thông tin về các tiến trình đang chạy như PID, tên tiến trình, mức sử dụng CPU/RAM. Việc hỗ trợ truy xuất theo thời gian thực và truy vấn dữ liệu lịch sử tạo điều kiện thuận lợi trong phân tích hành vi hoạt động của dịch vụ. Tính năng này rất hữu ích trong việc đánh giá mức độ tiêu thụ tài nguyên và phát hiện tiến trình bất thường. Tuy nhiên, để tăng tính thông minh, có thể tích hợp cơ chế cảnh báo dựa trên hành vi (behavioral anomaly detection) bằng mô hình AI.

### 3.3.4. Giám sát lưu lượng mạng trên các host

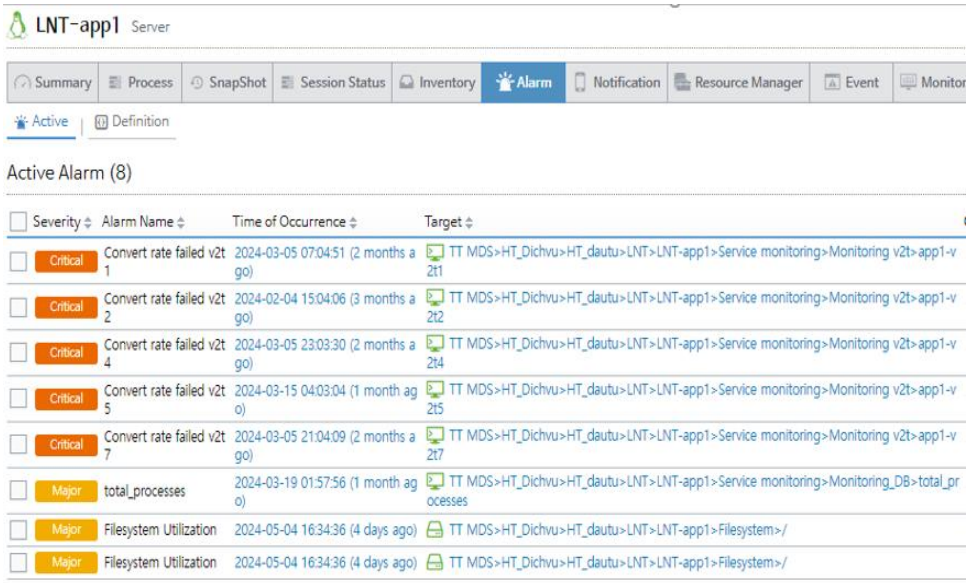
Vào lúc 19:45 ngày 01-05 thì có hiện tượng traffice Rxx tăng đột biến với biên độ cao: Min = 1.00ms và Max 53.00ms (Ta có thể thấy rõ trên biểu đồ).


**Hình 3. 17: Biểu đồ giám sát lưu lượng mạng của thiết bị**

Vào lúc 19:45 ngày 01-05 thì có hiện tượng traffice Rxx tăng đột biến với biên độ cao: Min = 1.00ms và Max 53.00ms (Ta có thể thấy rõ trên biểu đồ).

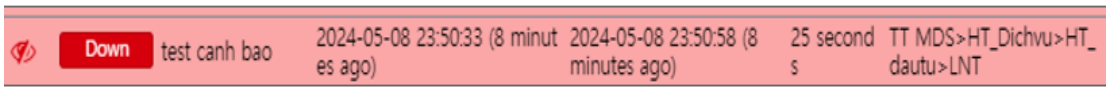
### 3.3.5. Cảnh báo sự cố

Tại tab Alarm của server LNT-app1 như *Hình 3.18* ta có thể thấy các cảnh báo của các lỗi được cấu hình.




**Hình 3. 18: Giao diện giám sát tập trung của thiết bị trên hệ thống Polestar**

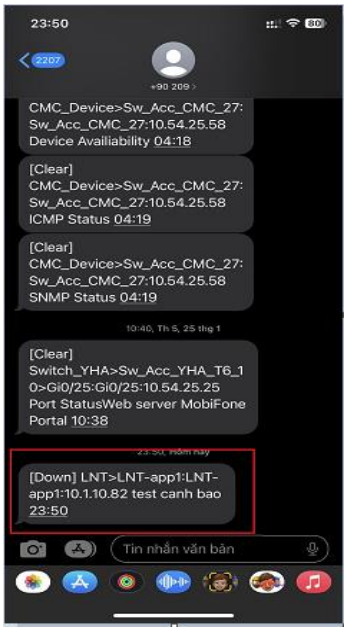
Trường hợp xảy ra sự cố như server bị down giống như *Hình 3.19* sẽ có cảnh báo xuất hiện trên Bảng Alarm console




**Hình 3. 19: Cảnh báo Down trên thiết bị**

Cảnh báo sẽ thực hiện gửi tin nhắn SMS và gửi mail về tới tài khoản chủ trì được thiết lập nhận cảnh báo như *Hình 3.20* với đầy đủ các thông tin như:

– Tin nhắn cảnh báo SMS gồm các thông tin: Trạng thái (Down), tên hệ thống, tên máy chủ, IP hệ thống, nội dung cảnh báo và thời gian lỗi.




**Hình 3. 20: Giao hiện tin nhắn cảnh báo Down trên thiết bị**

– Email cảnh báo gồm các thông tin: Trạng thái, tên System group, tên máy chủ, nội dung cảnh báo, thời gian, lỗi phát sinh, đường link tới hệ thống Polestar quản lý lỗi như *Hình 3. 21*.


[POLESTAR] - Canh bao [Down] LNT>LNT-app1:10.1.10.82 test canh bao

Severity : Down Ancestry : TT MDS>HT_Dichvu>HT_dautu>LNT>LNT-app1 Resource : LNT-app1 Type : Server [UP (= UP, 2 consecutive times)] Resource URL : http://10.1.10.97/management/resourcedetail/2338590
IMPORTANT NOTICE:
The information in this email is the property of MobiFone. This communication is confidential and intended solely for the addressee(s). Any unauthorized r notify the sender by replying to this transmission and delete the message without disclosing it. Thank you.
E-mail including attachments is susceptible to data corruption, interception, unauthorized amendment, tampering and viruses, and we only send and receive any consequences thereof.

THÔNG BÁO BẢO MẬT:

**Hình 3. 21: Giao hiện email cảnh báo Down trên thiết bị**

## 3.4. Kết luận chương 3

Chương này đã thực hiện triển khai thử nghiệm giải pháp Polestar vào thực tế tại Trung tâm Dịch vụ số Mobifone, từ đó kiểm chứng hiệu quả và khả năng ứng dụng của giải pháp trong điều kiện hạ tầng mạng cụ thể. Việc xây dựng mô hình giám sát, cấu hình hệ thống, thiết lập cảnh báo, và giám sát theo các kịch bản thực tiễn đã được thực hiện đầy đủ, cho phép theo dõi chi tiết các thành phần như trạng thái host, tài nguyên hệ thống, dịch vụ, lưu lượng mạng, và các sự cố xảy ra.

Kết quả thử nghiệm cho thấy Polestar không những đáp ứng tốt các yêu cầu về hiệu năng và độ ổn định, mà còn giúp giảm thiểu thời gian phản hồi trước các sự cố, hỗ trợ nâng cao tính sẵn sàng và khả năng quản trị hệ thống mạng. Thông qua các giao diện trực quan và công cụ cảnh báo đa dạng, người quản trị có thể chủ động giám sát, phát hiện và xử lý sự cố một cách hiệu quả. Thành công của việc triển khai thử nghiệm khẳng định tính khả thi và lợi ích thiết thực của việc áp dụng Polestar vào hệ thống giám sát hạ tầng mạng, mở ra hướng phát triển mạnh mẽ cho các mô hình giám sát tập trung tại Mobifone và các tổ chức có hạ tầng mạng tương tự

# KẾT LUẬN

Đề án "Nghiên cứu giải pháp Polestar và ứng dụng triển khai giám sát hạ tầng mạng Trung tâm Dịch vụ số Mobifone" đã hoàn thành các nội dung nghiên cứu trọng tâm, đáp ứng đúng định hướng ứng dụng thực tiễn. Trong bối cảnh yêu cầu ngày càng cao về độ ổn định, an toàn và hiệu quả của hạ tầng mạng trong các doanh nghiệp viễn thông, việc triển khai hệ thống giám sát tập trung như Polestar là vô cùng cần thiết và cấp bách.

Qua quá trình khảo sát, phân tích và thử nghiệm, đề án đã chỉ ra được các hạn chế trong mô hình giám sát hạ tầng hiện tại tại Trung tâm Dịch vụ số Mobifone, bao gồm thiếu sự đồng bộ giữa các hệ thống giám sát, khả năng cảnh báo chậm, và khó khăn trong việc phân tích, xử lý sự cố. Trên cơ sở đó, giải pháp Polestar đã được nghiên cứu và triển khai thử nghiệm, cho thấy hiệu quả rõ rệt trong việc nâng cao khả năng theo dõi hệ thống theo thời gian thực, phát hiện sớm sự cố, tối ưu tài nguyên và giảm thiểu chi phí vận hành.

Kết quả thực nghiệm cho thấy hệ thống Polestar có thể giám sát linh hoạt các thành phần trong hạ tầng mạng, cung cấp giao diện trực quan, khả năng cảnh báo tức thời qua SMS/email và tích hợp tốt với các hệ thống quản lý hiện hữu. Điều này minh chứng rằng Polestar hoàn toàn có khả năng đáp ứng yêu cầu quản lý hạ tầng mạng trong các tổ chức quy mô lớn như Mobifone. Đề án đã bám sát đề cương được phê duyệt với bố cục như sau:

**Chương 1:** Hạ tầng mạng Trung tâm Dich vụ số MobiFone

**Chương 2:** Nghiên cứu giải pháp Polestar

**Chương 3:** Xây dựng triển khai thử nghiệm giám sát Polestar cho hạ tầng mạng Trung tâm Dịch vụ số MobiFone

Từ kết quả nghiên cứu, đề án cũng đề xuất hướng phát triển mở rộng bao gồm: tích hợp AI trong việc phân tích dữ liệu giám sát, phát triển các dashboard tùy biến theo từng vai trò quản trị, và mở rộng quy mô triển khai trên toàn bộ hệ thống của Tổng công ty Viễn thông Mobifone.

# HƯỚNG PHÁT TRIỂN CỦA ĐỀ ÁN

Học viên sẽ tiếp tục nghiên cứu, tiềm hiểu các công nghệ về giám sát, quản lý hạ tầng mạng hiện có trên thế giới, nhằm bổ sung kiến thức và góp phần đề xuất tới các doanh nghiệp tổ chức có thể triển khai giải pháp đáp ứng được nhu cầu của đơn vi;

Trong tương lai, để nâng cao hơn nữa hiệu quả giám sát và quản trị hạ tầng mạng, đề án có thể được mở rộng theo một số hướng nghiên cứu và ứng dụng công nghệ tiên tiến như sau:

**Ứng dụng trí tuệ nhân tạo (AI) và học máy (Machine Learning – ML) trong phân tích và dự báo sự cố mạng:**

Mặc dù giải pháp Polestar hiện tại đã tích hợp các tính năng giám sát thời gian thực và cảnh báo sự cố, nhưng việc bổ sung các mô hình học máy sẽ giúp nâng cao khả năng phân tích dữ liệu lịch sử, phát hiện hành vi bất thường và dự đoán các sự cố tiềm ẩn trước khi chúng ảnh hưởng đến hệ thống. Các thuật toán như Random Forest, K-means Clustering hoặc LSTM (Long Short-Term Memory) có thể được huấn luyện trên tập dữ liệu giám sát để nhận diện xu hướng bất thường hoặc mô hình hóa rủi ro.

Điều này sẽ chuyển đổi hệ thống từ dạng giám sát phản ứng (reactive monitoring) sang giám sát chủ động (proactive/predictive monitoring), góp phần giảm thời gian gián đoạn và tăng độ tin cậy cho hệ thống mạng tại Trung tâm Dịch vụ số MobiFone.

**Phát triển hệ thống giám sát thông minh tích hợp đa nền tảng dựa trên AI:**

Một hướng phát triển tiềm năng khác là xây dựng nền tảng giám sát tập trung được hỗ trợ bởi các trợ lý ảo AI (AIOps), có khả năng tự động phân tích nguyên nhân gốc rễ (Root Cause Analysis – RCA), đề xuất phương án khắc phục (Recommendation Engine), và tối ưu hóa cấu hình hệ thống thông qua cơ chế học liên tục.

Nền tảng này có thể kết hợp dữ liệu từ nhiều nguồn (log server, SNMP, API, hệ thống firewall, IDS/IPS) và sử dụng các kỹ thuật NLP (Natural Language Processing) để phân tích nội dung cảnh báo, hỗ trợ người quản trị ra quyết định nhanh chóng hơn. Việc tích hợp giao diện AI tương tác (AI ChatOps) cũng là một xu hướng nổi bật, giúp người vận hành truy vấn trạng thái hệ thống và ra lệnh thông qua ngôn ngữ tự nhiên.

**Hướng tới kiến trúc giám sát phân tán sử dụng mô hình microservice và container hóa:**

Với xu hướng chuyển đổi hạ tầng sang kiến trúc microservices và container (như Kubernetes, Docker), hệ thống giám sát cũng cần thích ứng bằng cách phát triển các agent hoặc module riêng biệt, có khả năng tự triển khai, tự cập nhật và dễ dàng mở rộng. Điều này giúp đáp ứng nhu cầu giám sát linh hoạt trong môi trường đám mây lai (hybrid cloud) và đa đám mây (multi-cloud).