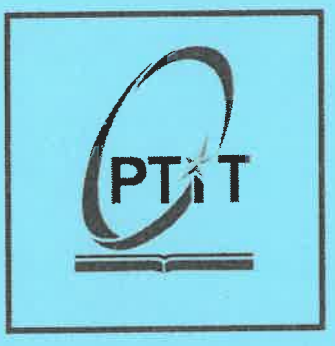
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



TRẦN ĐOÀN TRUNG

NGHIÊN CỨU GIẢI PHÁP POLESTAR VÀ ỨNG DỤNG TRIỂN KHAI GIÁM SÁT HẠ TẦNG MẠNG TRUNG TÂM DỊCH VỤ SỐ MOBIFONE

ĐỀ ÁN TỐT NGHIỆP THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

HÀ NỘI – 2025

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

TRẦN ĐOÀN TRUNG

NGHIÊN CỨU GIẢI PHÁP POLESTAR VÀ ỨNG DỤNG TRIỂN KHAI GIÁM SÁT HẠ TẦNG MẠNG TRUNG TÂM DỊCH VỤ SỐ MOBIFONE

CHUYÊN NGÀNH: KỸ THUẬT VIỄN THÔNG

MÃ SỐ: 8.52.02.08

ĐỀ ÁN TỐT NGHIỆP THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

NGƯỜI HƯỚNG DẪN KHOA HỌC: PGS TS DƯƠNG THỊ THANH TÚ

HÀ NỘI – 2025

LỜI CAM ĐOAN

Tôi xin cam đoan đề án tốt nghiệp "Nghiên cứu giải pháp Polestar và ứng dụng triển khai giám sát hạ tầng mạng Trung tâm Dịch vụ số" là công trình nghiên cứu khoa học của riêng tôi được thực hiện dưới sự hướng dẫn của giảng viên PGS.TS Dương Thị Thanh Tú. Các nội dung nghiên cứu và kết quả trong đề án này là trung thực và chưa từng được công bố bất cứ công trình nghiên cứu nào trước đây. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi trong phần tài liệu tham khảo.

Nếu phát hiện có bất kỳ gian lận nào tôi xin hoàn toàn chịu trách nhiệm trước Hội đồng cũng như kết quả luận văn của mình.

Tác giả đề án

(Ký và ghi rõ họ tên)

Trần Đoàn Trung

LỜI CẢM ƠN

Trong quá trình nghiên cứu và hoàn thành đề án tốt nghiệp thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông, bên cạnh sự nỗ lực của bản thân, học viên đã nhận được sự giảng dạy và hướng dẫn nhiệt tình của các thầy cô giáo. Học viên xin gửi lời cảm ơn chân thành nhất tới tất cả những thầy cô giáo đã giảng dạy và PGS.TS Dương Thị Thanh Tú – người đã tận tình, chu đáo hướng dẫn học viên trong suốt quá trình học tập, nghiên cứu để học viên có thể hoàn thành đề án "Nghiên cứu giải pháp Polestar và ứng dụng triển khai giám sát hạ tầng mạng Trung tâm Dịch vụ số MobiFone".

Do tính phức tạp của đề án nghiên cứu, cũng như khả năng và kiến thức của học viên còn nhiều hạn chế nên đề án không tránh khỏi những sai sót nhất định.

Học viên rất mong nhận những đóng góp ý kiến của các thầy cô và những nhà nghiên cứu khác để nội dung nghiên cứu được hoàn thiện hơn.

Học viên xin chân thành cảm ơn!

Tác giả đề án

(Ký và ghi rõ họ tên)

Trần Đoàn Trung

MỤC LỤC

LỜI CAM ĐOAN i
LỜI CẢM ƠN ii
BẢNG DANH MỤC TỪ VIẾT TẮT v
DANH MỤC HÌNH VẼ vi
DANH MỤC BẢNG BIỂU viii
MỞ ĐẦU 1
CHƯƠNG 1: HẠ TẦNG MẠNG TRUNG TÂM DỊCH VỤ SỐ MOBIFONE 3
1.1. Khảo sát hiện trạng hạ tầng mạng Trung tâm Dịch vụ số Mobifone 3
1.1.1. Border Router 4
1.1.2. Firewall 7
1.1.3. Core Switch 10
1.1.4. Switch access 13
1.2. Giới thiệu về các hệ thống giám sát hiện tại của Trung tâm Dịch vụ số Mobifone 16
1.2.1. Giải pháp giám sát cảnh báo Prometheus 16
1.2.2. Giải pháp giám sát cảnh báo SolarWinds 18
1.3. Các vấn đề còn tồn tại 19
1.4. Giải pháp 20
1.5. Kết luận chương 1 21
CHƯƠNG 2: NGHIÊN CỨU GIẢI PHÁP POLESTAR 22
2.1. Tổng quan về quản lý mạng 22
2.1.1. Các thành phần cơ bản của hệ thống quản lý mạng hạ tầng 22
2.1.2. Các chức năng quản lý 24
2.1.3. Kiến trúc quản lý mạng dựa trên TMN 27
2.1.3.1.Quản lý hiệu năng 27
2.1.3.2.Quản lý sự cố (Fault Management) 32
2.1.3.3.Quản lý cấu hình (Configuration Management) 34
2.1.3.4.Quản lý tài khoản (Accounting Management) 36
2.1.3.5.Quản lý bảo mật (Security Management) 36

2.2. Một số giải pháp giám sát hiện nay 37
2.2.1. Giải pháp giám sát cảnh báo Nagios: 37
2.2.2. Giải pháp giám sát cảnh báo Zabbix: 39
2.2.3. Giải pháp giám sát cảnh báo PRTG Network Monitor 41
2.3. Giải pháp giám sát cảnh báo Polestar 44
2.3.1. Giới thiệu về hệ thống 44
2.3.2. Các đối tượng giám sát 45
2.3.3. Kiến trúc hệ thống giám sát Polestar 50
2.3.4. Các chức năng giám sát chính 53
2.4. Đánh giá tổng quan về các giải pháp giám sát 60
2.5. Kết luận chương 2 63
CHƯƠNG 3: ỨNG DỤNG GIẢI PHÁP GIÁM SÁT POLESTAR CHO HẠ TẦNG MẠNG TRUNG TÂM DỊCH VỤ SỐ MOBIOFNE 65
3.1. Đặt vấn đề 65
3.2. Giải pháp giám sát cho hạ tầng mạng của Trung tâm Dịch vụ số Mobifone 66
3.2.1. Giới thiệu mô hình 67
3.2.2. Kịch bản giám sát hệ thống mạng 69
3.2.3. Tiến trình xây hệ thống giám sát 70
3.2.4. Thiết lập cảnh báo 73
3.3. Đánh giá hoạt động của hệ thống 75
3.3.1. Giám sát các trạng thái của host 75
3.3.2. Giám sát các tài nguyên của host 78
3.3.3. Giám sát trạng thái hoạt động của các Service trên các host 79
3.3.4. Giám sát lưu lượng mạng trên các host 81
3.3.5. Cảnh báo sự cố 82
3.4. Kết luận chương 3 85
KẾT LUẬN 86
HƯỚNG PHÁT TRIỂN CỦA ĐỀ ÁN 87
TÀI LIỆU THAM KHẢO 89

BẢNG DANH MỤC TỪ VIẾT TẮT

Thuật ngữ viết tắt	Tiếng Anh	Tiếng Việt
AI	Artificial Intelligence	Trí tuệ nhân tạo
AP	Access Point	Điểm truy cập
CLI	Command Line Interface	Giao diện dòng lệnh
CNTT		Công nghệ thông tin
CPU	Central Processing Unit	Bộ xử lý trung tâm
CSDL		Cơ sở dữ liệu
DB	Data Base	Cơ sở dữ liệu
EMS	Element Management System	Hệ thống quản lý phần tử mạng
GUI	Graphical User Interface	Giao diện đồ họa
HDD	Hard Disk Drive	Ổ đĩa cứng
IP	Internet Protocol	Giao thức Internet
LAN	Local Area Network	Mạng cục bộ
MDS	MobiFone Digital Service	Trung tâm Dịch vụ số Mobifone
NCM	Network Configuration Manager	Trình quản lý cấu hình mạng
NMS	Network Management System	Hệ thống quản lý mạng
OMC	Operation and Maintenance Center	Trung tâm Vận hành và Bảo trì
OSPF	Open Shortest Path First	Giao thức định tuyến trạng thái liên kết
PoE	Power over Ethernet	Cấp nguồn qua mạng Ethernet
PRTG	Paessler Router Traffic Grapher	Công cụ đồ họa lưu lượng Router của Paessler
QoS	Quality of Service	Chất lượng dịch vụ
RAM	Random Access Memory	Bộ nhớ truy cập ngẫu nhiên
REST	Representational State Transfer	Truyền trạng thái đại diện
SNMP	Simple Network Management Protocol	Giao thức quản lý mạng đơn giản
SQL	Structured Query Language	Ngôn ngữ truy vấn có cấu trúc
TMN	Telecommunication Management Network	Mạng quản lý viễn thông
VPN	Virtual Private Network	Mạng riêng ảo
VSS	Virtual Switching System	Hệ thống chuyển mạch ảo

DANH MỤC HÌNH VẼ

Hình 1. 1: Sơ đồ mạng Trung tâm Dịch vụ số MobiFone 3
Hình 2. 1: Sơ đồ quản lý sự số 32
Hình 2. 2: Giải pháp giám sát cảnh báo Nagios 38
Hình 2. 3: Giải pháp giám sát cảnh báo Zabbix 40
Hình 2. 4: Giải pháp giám sát cảnh báo PRTG Network Monitor 42
Hình 2. 5: Sơ đồ tổng quan kết nối hệ thống giám sát Polestar 44
Hình 2. 6: Giám sát máy chủ cài đặt Agent 47
Hình 2. 7: Giám sát qua giao thức SNMP 48
Hình 2. 8: Mô hình hệ thống giám sát sử dụng Polestar 50
Hình 2. 9: Cổng giao tiếp của Polestar 51
Hình 2. 10: Giao diện nhóm Server được giám sát cảnh báo Polestar 52
Hình 2. 11: Giao diện nhóm Network Device được giám sát cảnh báo Polestar 53
Hình 2. 12: Giao diện giám sát Real-time Monitoring của hệ thống Polestar 54
Hình 2. 13: Giao diện nhóm Topology map của hệ thống Polestar 55
Hình 2. 14: Giao diện màn hình System Dashboard của hệ thống Polestar 56
Hình 2. 15: Giao diện màn hình quản lý của hệ thống Polestar 57
Hình 2. 16: Giao diện thông số Performance của hệ thống được giám sát bởi Polestar 58
Hình 2. 17: Giao diện Dashboard của thiết bị được giám sát bởi Polestar 58
Hình 2. 18: Giao diện chức năng Review Event của hệ thống Polestar 59
Hình 2. 19: Giao diện màn hình cảnh báo tập trung của hệ thống Polestar 59
Hình 2. 20: Giao diện chi tiết cảnh bảo của hệ thống Polestar 60
Hình 3. 1: Mô hình giải pháp giám sát hạ tầng mạng Trung tâm Dịch vụ số Mobifone 68
Hình 3. 2: Giao diện tích hợp thiết bị cần giám sát trên hệ thống Polestar 72
Hình 3. 3: Giao diện thông tin chi tiết thiết bị cần giám sát hệ thống Polestar 72
Hình 3. 4: Giao diện Dashboard thiết bị được tích hợp trên hệ thống Polestar 73
Hình 3.5: Giao diện quyền người dùng trên hệ thống Polestar 74
Hình 3. 6: Giao diện thông tin chi tiết người dùng trên hệ thống Polestar 74
Hình 3. 7: Giao diện thêm phân quyền trên tài khoản người dùng 75

Hình 3. 8: Giao diện chi tiết thiết bị đã được thêm của nhóm LNT trên hệ thống Polestar 76
Hình 3. 9: Giao diện kiểm tra lỗi tích hợp thiết bị trên hệ thống Polestar 76
Hình 3. 10: Cột các hạng mục của hệ thống được tích hợp giám sát 77
Hình 3. 11: Bảng chi tiết các thông số kỹ thuật của Network interface 77
Hình 3. 12: Cột các hạng mục của hệ thống được tích hợp giám sát 78
Hình 3. 13: Giao diện Dashboard của hệ thống đã được tích hợp trên hệ thống Polestar 79
Hình 3. 14: Biểu đồ giám sát Process của thiết bị 80
Hình 3. 15: Thông số chi tiết giám sát Process của thiết bị 80
Hình 3. 16: Thông số chi tiết giám sát Process của thiết bị 81
Hình 3. 17: Biểu đồ giám sát lưu lượng mạng của thiết bị 82
Hình 3. 18: Giao diện giám sát tập trung của thiết bị trên hệ thống Polestar 83
Hình 3. 19: Cảnh báo Down trên thiết bị 83
Hình 3. 20: Giao hiện tin nhắn cảnh báo Down trên thiết bị 84
Hình 3. 21: Giao hiện email cảnh báo Down trên thiết bị 84

DANH MỤC BẢNG BIỂU

Bảng 2.1 So sánh tổng quan các giải pháp giám sát mạng 61
Bảng 3.1: Thông tin kết nối đến hệ thống giám sát hạ tầng mạng Polestar 70

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 [2].

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

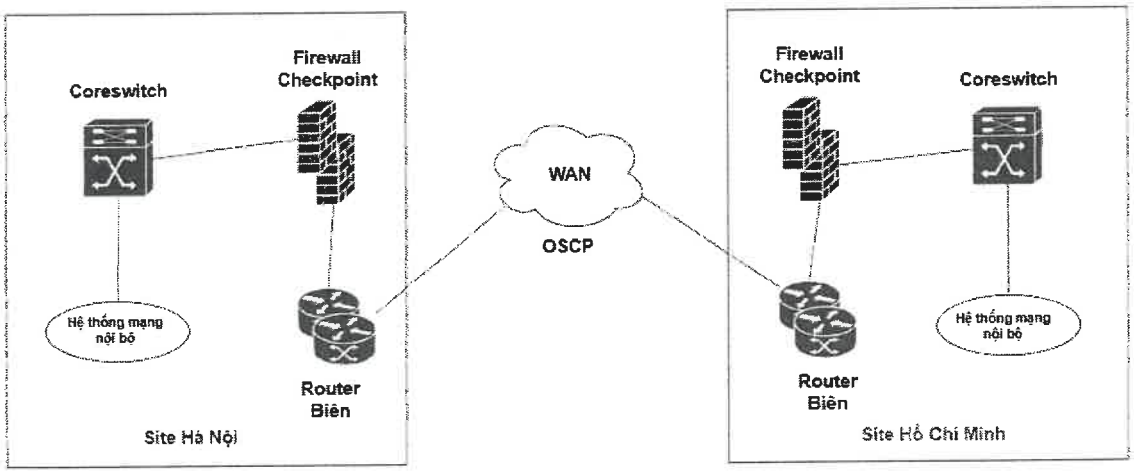
Chương 2: Nghiên cứu giải pháp Polestar

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

Việc khảo sát hiện trạng hạ tầng mạng của Trung tâm Dịch vụ số Mobifone là một bước quan trọng nhằm đảm bảo hệ thống vận hành ổn định, an toàn và hiệu quả. Trung tâm Dịch vụ số Mobifone đóng vai trò then chốt trong việc phát triển và cung cấp các dịch vụ giá trị gia tăng trên nền tảng viễn thông. Tuy nhiên, cơ sở hạ tầng mạng hiện tại vẫn đối mặt với nhiều thách thức, bao gồm khả năng phát hiện sớm các sự cố tiềm ẩn và việc giám sát tập trung còn hạn chế. Để hiểu rõ hơn về các vấn đề tồn tại và xác định các giải pháp khắc phục, cần tiến hành một cuộc khảo sát tổng thể nhằm đánh giá hiện trạng mạng hiện tại, đồng thời xem xét các hệ thống giám sát và công nghệ đang được sử dụng. Điều này sẽ tạo nền tảng cho các bước nâng cao và tối ưu hóa hạ tầng mạng trong tương lai.



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

Hạ tầng mạng Trung tâm Dịch vụ số MobiFone được thiết kế theo mô hình tại *Hình 1.1* Với thiết kế hạ tầng mạng theo mô hình tiêu chuẩn Tier 3 gồm các thành phần:

- Border Router;

- Firewall;
- Core Switch;
- Switch access.

1.1.1. Border Router

- Khái niệm của thiết bị Border Router:

Trong kiến trúc mạng hiện đại, đặc biệt là mạng quy mô lớn theo mô hình phân lớp như Tier 3, Border Router (Router biên) đóng vai trò là cổng kết nối quan trọng giữa hệ thống mạng nội bộ (Intranet) và các mạng bên ngoài như mạng WAN, mạng lõi nhà mạng hoặc Internet. Thiết bị này đảm nhận chức năng định tuyến biên, thiết lập các chính sách định tuyến xuyên miền (inter-domain routing), đồng thời triển khai các chính sách bảo mật và phân phối lưu lượng có kiểm soát giữa các miền mạng.

Trong mô hình định tuyến OSPF (Open Shortest Path First), Border Router thường đảm nhận vai trò của một Area Border Router (ABR) hoặc Autonomous System Border Router (ASBR), tức là thiết bị định tuyến giao tiếp giữa các area nội bộ hoặc giữa các hệ thống tự trị (AS - Autonomous System). Điều này cho phép Border Router không chỉ thực hiện định tuyến truyền thống, mà còn phân phối và tối ưu bảng định tuyến thông qua cơ chế tóm tắt tuyến (route summarization) và lọc tuyến (route filtering).

- Các chức năng chính của Border Router:

Border Router trong một hệ thống mạng lớp doanh nghiệp hoặc nhà cung cấp dịch vụ viễn thông lớn như MobiFone đảm nhận nhiều chức năng phức tạp và quan trọng, bao gồm:

+ Định tuyến liên miền (Inter-domain Routing): Thực hiện trao đổi bảng định tuyến với các hệ thống mạng bên ngoài thông qua các giao thức định tuyến động như BGP (Border Gateway Protocol) hoặc OSPF, kết hợp static route trong các trường hợp đặc biệt nhằm tối ưu hóa lưu lượng.

+ Phân tách miền định tuyến: Trong mô hình OSPF, Border Router đóng vai trò kết nối các khu vực (Area) khác nhau, giúp mở rộng quy mô hệ thống mà vẫn đảm bảo tính khả thi và hiệu năng xử lý định tuyến.
+ Triển khai chính sách bảo mật biên: Kết hợp với firewall hoặc Access Control List (ACL) để kiểm soát truy cập hai chiều, ngăn chặn các luồng lưu lượng trái phép, đồng thời hỗ trợ chống tấn công từ bên ngoài như DoS/DDoS.
+ Tối ưu hóa lưu lượng và đảm bảo chất lượng dịch vụ (QoS): Phân loại và ưu tiên lưu lượng theo lớp dịch vụ nhằm đảm bảo các dịch vụ thời gian thực (real-time services) như thoại, video được xử lý với độ trễ thấp và thông lượng ổn định.
+ Đảm bảo tính sẵn sàng cao: Hỗ trợ các giao thức dự phòng như HSRP/VRRP, cùng với cấu hình song song (redundant) đảm bảo hoạt động liên tục kể cả khi xảy ra sự cố phần cứng.

– Các dòng thiết bị Border Router phổ biến trên thị trường:
+ Cisco Systems:
  - Cisco ASR Series (ASR 9000, ASR 1000): Thiết bị định tuyến đa dịch vụ Aggregation Services Router, hỗ trợ khả năng mở rộng lớn, thích hợp cho mạng lõi của nhà mạng.
  - Cisco ISR (Integrated Services Router): Dùng cho doanh nghiệp quy mô trung bình, hỗ trợ tích hợp các dịch vụ bảo mật và định tuyến.
+ Juniper Networks – MX Series: Router hiệu năng cao, hỗ trợ BGP/MPLS, có tính năng bảo mật và tích hợp SDN.
+ Huawei NE Series (NE20E, NE40E): Router đa năng được sử dụng trong mạng metro hoặc mạng trục của nhà mạng, có khả năng xử lý lưu lượng lên đến hàng Tbit/s.

+ Arista, MikroTik, Fortinet: Các thiết bị định tuyến ở mức trung cấp và chuyên biệt hóa cho môi trường bảo mật, có tính linh hoạt cao và giá thành tối ưu.

– Thiết bị Border Router tại Trung tâm Dịch vụ số MobiFone

Tại Trung tâm Dịch vụ số MobiFone – đơn vị trực thuộc Tổng Công ty Viễn thông MobiFone chuyên về các dịch vụ số và giá trị gia tăng, hiện nay thiết bị Border Router chính được triển khai là Cisco ASR 9010 – một trong những sản phẩm cao cấp nhất của Cisco thuộc dòng Aggregation Services Router (ASR 9000 Series).

Việc lựa chọn Cisco ASR 9010 được đánh giá là chiến lược tối ưu về mặt kỹ thuật và vận hành, xuất phát từ các lý do sau:

+ Hiệu năng xử lý cực cao: ASR 9010 hỗ trợ kiến trúc modular với khả năng mở rộng lên tới nhiều Tbit/s thông qua các line card tốc độ cao. Đây là yêu cầu bắt buộc trong môi trường hạ tầng lớn có lưu lượng cao, nhiều site phân tán và truyền thông đa hướng.
+ Hỗ trợ đa giao thức định tuyến nâng cao: Thiết bị tích hợp đầy đủ các giao thức định tuyến như BGP, OSPF, MPLS, giúp Trung tâm triển khai kết nối linh hoạt với hệ thống mạng lõi MobiFone, WAN tin học quốc gia, và các hệ thống đối tác.
+ Khả năng tích hợp và tương thích cao: Thiết bị tương thích hoàn toàn với các thiết bị lõi và access layer của hệ sinh thái mạng MobiFone, giúp tối ưu chi phí tích hợp, giảm độ phức tạp trong vận hành.
+ Hỗ trợ chính sách bảo mật biên: ASR 9010 cho phép triển khai các ACL phức tạp và cơ chế kiểm soát truy cập theo lớp dịch vụ (CoS) ngay tại lớp biên, tăng cường khả năng phòng chống tấn công và ngăn chặn truy cập trái phép từ mạng ngoài.

Việc sử dụng Border Router ASR 9010 không chỉ giúp Trung tâm Dịch vụ số MobiFone đảm bảo vận hành ổn định, đáp ứng lưu lượng truyền tải ngày càng

tăng, mà còn tạo nền tảng kỹ thuật vững chắc để mở rộng hạ tầng mạng trong giai đoạn chuyển đổi số sâu rộng sắp tới.

1.1.2. Firewall

– Khái niệm của thiết bị Firewall

Firewall (tường lửa) là một thiết bị bảo mật mạng, hoạt động như một rào chắn giữa các miền mạng có độ tin cậy khác nhau – điển hình là giữa mạng nội bộ và Internet, hoặc giữa các phân vùng mạng nội bộ. Firewall được thiết kế nhằm kiểm soát lưu lượng mạng vào và ra theo các chính sách bảo mật được cấu hình trước. Các chính sách này giúp xác định xem một gói tin có được phép truyền qua firewall hay bị chặn lại.

Tường lửa có thể được triển khai dưới dạng thiết bị phần cứng (hardware appliance), phần mềm (software-based firewall) hoặc tích hợp trong các thiết bị mạng như router, tùy thuộc vào kiến trúc mạng và mức độ yêu cầu bảo mật của hệ thống. Trong kiến trúc mạng tiêu chuẩn Tier 3, firewall đóng vai trò quan trọng tại lớp phân phối và lớp biên, nơi các truy cập từ bên ngoài được kiểm soát nghiêm ngặt.

– Chức năng chính của thiết bị Firewall

Firewall hiện đại không chỉ đơn thuần lọc lưu lượng dựa trên địa chỉ IP và cổng mà còn tích hợp nhiều tính năng bảo mật nâng cao, hỗ trợ phát hiện và ngăn chặn tấn công theo thời gian thực. Các chức năng chính bao gồm:

+ Lọc gói (Packet Filtering): Phân tích tiêu đề của các gói tin để xác định xem chúng có được phép truyền qua hay không dựa trên các quy tắc IP, port, protocol.
+ Tường lửa trạng thái (Stateful Inspection): Theo dõi trạng thái của các kết nối mạng, chỉ cho phép các gói tin thuộc về phiên giao tiếp hợp lệ đi qua.
+ Phân đoạn mạng (Network Segmentation): Kiểm soát truy cập giữa các subnet hoặc VLAN trong hệ thống nội bộ, tăng cường khả năng cô lập sự cố và giảm nguy cơ lây lan.

+ Phát hiện và ngăn chặn xâm nhập (IPS/IDS): Tích hợp cơ chế phân tích hành vi và chữ ký để ngăn chặn các cuộc tấn công như port scanning, DDoS, SQL injection.
+ Kiểm soát ứng dụng (Application Control): Phân loại lưu lượng dựa trên ứng dụng chứ không chỉ dựa trên port, cho phép quản trị viên kiểm soát chi tiết các dịch vụ như web, mail, VPN, v.v.
+ VPN Gateway: Hỗ trợ kết nối an toàn giữa các site thông qua các giao thức VPN như IPsec, SSL-VPN.
+ Ghi nhật ký và phân tích lưu lượng: Ghi nhận toàn bộ hoạt động để phục vụ kiểm toán bảo mật và phân tích sự cố.

– Các dòng thiết bị Firewall phổ biến trên thị trường

Trên thị trường hiện nay, có nhiều dòng thiết bị firewall được sử dụng rộng rãi trong cả môi trường doanh nghiệp và nhà mạng. Một số thương hiệu tiêu biểu bao gồm:

– Thiết bị Firewall tại Trung tâm Dịch vụ số MobiFone
  + Fortinet (FortiGate Series): Nổi bật với khả năng xử lý hiệu năng cao, tích hợp nhiều chức năng bảo mật (UTM – Unified Threat Management), có giải pháp từ phân khúc SMB đến nhà mạng.
  + Palo Alto Networks: Dẫn đầu về tường lửa thế hệ mới (Next-Generation Firewall - NGFW), tích hợp AI, kiểm soát ứng dụng và sandboxing.
  + Cisco Firepower/ASA: Thiết bị firewall kết hợp giữa tính ổn định của Cisco với khả năng tích hợp IPS/IDS và kiểm soát lớp ứng dụng.
  + Check Point: Firewall tập trung vào khả năng phân tích lưu lượng và kiểm soát truy cập lớp ứng dụng, thường được sử dụng trong các hệ thống đòi hỏi tính tùy biến cao.
  + SonicWall, Juniper SRX, WatchGuard: Phù hợp cho doanh nghiệp vừa và nhỏ, với khả năng mở rộng linh hoạt và giá thành cạnh tranh.

– Thiết bị Firewall tại Trung tâm Dịch vụ số MobiFone

Trong kiến trúc bảo mật tại Trung tâm Dịch vụ số MobiFone, thiết bị Firewall Fortinet FortiGate 400F đang được triển khai làm thành phần bảo vệ lớp biên và lớp truy cập mạng quan trọng. Việc lựa chọn Fortinet 400F được đánh giá là phù hợp với đặc thù vận hành của một trung tâm dữ liệu quy mô lớn, vì các lý do sau:

+ Hiệu năng xử lý vượt trội: FortiGate 400F tích hợp vi xử lý bảo mật FortiASIC riêng biệt, cung cấp khả năng xử lý tường lửa lên tới hơn 100 Gbps và hàng triệu session đồng thời, đáp ứng tốt lưu lượng lớn trong các trung tâm dữ liệu như MobiFone.
+ Tích hợp tính năng bảo mật nâng cao: Thiết bị hỗ trợ đầy đủ IPS, Application Control, Web Filtering, Antivirus, SSL Inspection và bảo vệ chống DDoS – những yêu cầu bắt buộc trong môi trường mạng đa tầng, có kết nối Internet và WAN rộng khắp.
+ Khả năng phân đoạn và kiểm soát lớp ứng dụng mạnh: FortiGate 400F cho phép cấu hình phân đoạn mạng nội bộ theo mô hình Zero Trust, kiểm soát lưu lượng giữa các hệ thống dịch vụ số khác nhau, đồng thời đảm bảo tuân thủ các chính sách truy cập nghiêm ngặt.
+ Khả năng mở rộng và quản lý tập trung: Thiết bị hỗ trợ triển khai theo cụm (HA – High Availability), tích hợp với hệ thống quản lý FortiManager và FortiAnalyzer giúp Trung tâm quản lý bảo mật tập trung toàn hệ thống một cách linh hoạt và hiệu quả.
+ Chi phí sở hữu tối ưu và hỗ trợ tốt: Fortinet cung cấp chi phí phù hợp so với các thiết bị cùng phân khúc, trong khi vẫn đảm bảo hiệu năng và chính sách hỗ trợ kỹ thuật cao từ các đối tác trong nước, thuận lợi cho việc vận hành liên tục.

Nhờ những ưu điểm về hiệu năng, độ tin cậy và khả năng bảo vệ toàn diện, Firewall Fortinet 400F là lựa chọn phù hợp và chiến lược để đảm bảo an toàn

cho hạ tầng mạng quy mô lớn, đa site và vận hành 24/7 như tại Trung tâm Dịch vụ số MobiFone.

1.1.3. Core Switch

– Khái niệm của thiết bị 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.

Khác với các switch ở lớp truy cập (Access) hoặc lớp phân phối (Distribution), Core Switch yêu cầu hiệu năng cực cao, độ tin cậy tuyệt đối, khả năng dự phòng tốt và tốc độ truyền tải dữ liệu rất lớn, thường đạt tới hàng chục hoặc hàng trăm Gbps.

– Chức năng chính của thiết bị Core Switch

Core Switch đóng vai trò trung tâm điều phối luồng dữ liệu trong toàn bộ hạ tầng mạng. Các chức năng chính bao gồm:

+ Chuyển mạch và định tuyến tốc độ cao: Core Switch hỗ trợ switching Layer 2 và định tuyến Layer 3 ở tốc độ đường truyền cao (10G/40G/100G), đảm bảo hiệu năng cho các hệ thống thời gian thực như VoIP, Video Conference, các ứng dụng tài chính hoặc xử lý dữ liệu lớn.
+ Hội tụ và điều phối lưu lượng: Là điểm trung tâm kết nối toàn bộ các thiết bị mạng từ access switch, firewall, router và các server, đảm bảo quá trình truyền thông nội bộ và kết nối ra bên ngoài không bị tắc nghẽn.

+ Tối ưu hóa mạng với tính năng QoS (Quality of Service): Ưu tiên các loại lưu lượng quan trọng như thoại, video, giao dịch tài chính nhằm đảm bảo trải nghiệm người dùng và độ ổn định dịch vụ.
+ Hỗ trợ đa giao thức và tính năng mở rộng: Core Switch cần hỗ trợ các giao thức định tuyến động như OSPF, EIGRP, BGP; các giao thức kết nối dự phòng như VRRP, HSRP; và các tính năng nâng cao như MPLS, VLAN, STP, VSS, Multicast, v.v.
+ Tính sẵn sàng cao (High Availability): Core Switch thường có cấu trúc module với khả năng thay nóng (hot-swappable), tích hợp nguồn kép, quạt kép và tính năng nâng cấp phần mềm không gián đoạn (ISSU – In-Service Software Upgrade), đảm bảo hệ thống mạng hoạt động liên tục 24/7.

– Các dòng thiết bị Core Switch phổ biến trên thị trường

Trên thị trường hiện nay, nhiều hãng sản xuất thiết bị mạng cung cấp các dòng Core Switch chuyên dụng dành cho trung tâm dữ liệu và hệ thống doanh nghiệp lớn. Một số dòng tiêu biểu bao gồm:

+ Cisco Systems:
  - Cisco Catalyst 6500/6800 Series: Dòng switch module phổ biến, hỗ trợ Layer 2/3, có khả năng mở rộng linh hoạt và tính năng bảo mật tích hợp.
  - Cisco Nexus Series (Nexus 7000/9000): Dòng thiết bị chuyển mạch dành riêng cho trung tâm dữ liệu, hỗ trợ công nghệ SDN, VXLAN, và tích hợp ACI.
+ Juniper Networks: QFX Series, EX9200: Cung cấp hiệu năng cao, kiến trúc mở, hỗ trợ automation và tích hợp hệ điều hành Junos mạnh mẽ.
+ Huawei: CloudEngine 12800, 8800 Series: Switch lõi hiệu suất cao với khả năng xử lý hàng Tbps, phù hợp cho hệ thống mạng đa lớp và đám mây.

+ Arista Networks: 7500R, 7280 Series: Thiết kế cho trung tâm dữ liệu, nổi bật với latency thấp, throughput lớn và hệ điều hành EOS dễ lập trình.
+ HPE (Hewlett Packard Enterprise): Aruba CX Series: Tối ưu cho SDN và mạng campus hiện đại, tích hợp tính năng phân tích và bảo mật sâu.

– Thiết bị Core Switch tại Trung tâm Dịch vụ số MobiFone

Hiện tại, Trung tâm Dịch vụ số MobiFone đang triển khai thiết bị Cisco Catalyst 6509-E tại lớp lõi của hệ thống mạng. Việc lựa chọn dòng switch này là quyết định chiến lược nhằm đáp ứng yêu cầu vận hành của một hệ thống mạng có quy mô lớn, lưu lượng cao, nhiều lớp mạng phức tạp và yêu cầu độ tin cậy gần như tuyệt đối.

Lý do lựa chọn Cisco Catalyst 6509-E bao gồm:

+ Kiến trúc module linh hoạt: Catalyst 6509-E hỗ trợ tới 9 khe cắm (slots) cho line card và supervisor, cho phép cấu hình nhiều module như 10G Ethernet, Gigabit SFP, supervisor engine VSS – phục vụ tốt các cấu hình nâng cao và nhu cầu mở rộng hệ thống trong tương lai.
+ Khả năng xử lý lưu lượng lớn: Với khả năng chuyển mạch Layer 2/3 đạt hàng trăm Gbps, thiết bị hoàn toàn đáp ứng được yêu cầu truyền tải giữa các site dịch vụ số, server, hệ thống lưu trữ nội bộ và các phân mạng chuyên biệt.
+ Độ ổn định và sẵn sàng cao: Hỗ trợ đầy đủ cơ chế dự phòng nguồn (redundant power), quạt làm mát, supervisor engine kép và ISSU – giúp nâng cấp phần mềm không làm gián đoạn dịch vụ, đảm bảo mạng luôn hoạt động liên tục 24/7.
+ Tương thích cao với hệ sinh thái Cisco: Thiết bị dễ dàng tích hợp với các thành phần Cisco khác như router biên ASR 9010, firewall

FortiGate (qua chuẩn giao tiếp tiêu chuẩn), hệ thống quản trị trung tâm và các dịch vụ bảo mật nội bộ.

+ Khả năng bảo mật và quản lý nâng cao: Tích hợp tính năng ACL, NetFlow, DHCP Snooping, Port Security và khả năng giám sát SNMP, NetConf cho phép Trung tâm giám sát, phân tích và quản lý lưu lượng một cách chi tiết và chủ động.
+ Tối ưu chi phí đầu tư dài hạn: Với độ bền đã được chứng minh trong môi trường vận hành khắt khe và cộng đồng hỗ trợ lớn từ Cisco, thiết bị Catalyst 6509-E mang lại hiệu quả đầu tư cao, hạn chế rủi ro về lỗi thiết bị cũng như chi phí vận hành.

Việc triển khai Core Switch Cisco Catalyst 6509-E đã và đang góp phần quan trọng trong việc duy trì sự ổn định, hiệu quả và tính mở rộng cao cho hạ tầng mạng Trung tâm Dịch vụ số MobiFone – nơi vận hành hàng chục dịch vụ số, nền tảng dữ liệu, hệ thống thanh toán và các ứng dụng nội bộ phức tạp phục vụ hàng triệu người dùng.

1.1.4. Switch access

– Khái niệm của thiết bị Switch access

Switch access (thiết bị chuyển mạch lớp truy cập) là thành phần nằm ở lớp dưới cùng trong mô hình mạng phân cấp ba tầng (Three-tier Architecture: Core – Distribution – Access). Switch Access đảm nhiệm vai trò là điểm kết nối trực tiếp giữa các thiết bị đầu cuối như máy tính cá nhân, máy in, camera IP, điện thoại IP và các thiết bị IoT với mạng nội bộ (LAN).

Thiết bị switch lớp truy cập là nơi đầu tiên lưu lượng mạng đi vào hệ thống mạng doanh nghiệp. Vì vậy, ngoài chức năng chuyển mạch Layer 2 cơ bản, các switch này ngày nay thường được tích hợp thêm các tính năng về bảo mật, quản lý truy cập, cấp nguồn qua mạng (PoE), kiểm soát lớp dịch vụ (QoS), và hỗ trợ quản trị tập trung.

– Chức năng chính của thiết bị Switch access

Switch access đóng vai trò quan trọng trong việc triển khai các kết nối mạng đến người dùng cuối và thiết bị đầu cuối. Các chức năng chủ yếu của nó bao gồm:

+ Kết nối thiết bị đầu cuối: Cung cấp các cổng mạng tốc độ 1G/2.5G/10G để kết nối PC, IP phone, camera, thiết bị IoT với mạng nội bộ.
+ Chuyển mạch Layer 2: Chuyển tiếp các frame Ethernet dựa trên địa chỉ MAC, đảm bảo lưu lượng đi đúng đến thiết bị đích trong cùng VLAN.
+ Phân chia mạng với VLAN: Hỗ trợ tạo và gán VLAN cho từng port, giúp phân chia logic mạng theo phòng ban, chức năng hoặc mức độ bảo mật.
+ Kiểm soát truy cập (Port Security): Giới hạn số lượng thiết bị truy cập vào mỗi port, bảo vệ hệ thống khỏi truy cập trái phép.
+ Cấp nguồn PoE (Power over Ethernet): Hỗ trợ cấp nguồn cho các thiết bị như IP phone, camera giám sát hoặc access point mà không cần nguồn điện riêng.
+ Triển khai QoS: Gán mức ưu tiên khác nhau cho các loại lưu lượng (voice, video, data) đảm bảo chất lượng cho các ứng dụng thời gian thực.
+ Giám sát và quản trị từ xa: Hỗ trợ SNMP, Syslog, NetFlow và các giao thức quản lý mạng, giúp tích hợp với hệ thống giám sát trung tâm như Polestar hoặc SolarWinds.

– Các dòng thiết bị Switch access phổ biến trên thị trường

Hiện nay, trên thị trường có nhiều dòng thiết bị Switch Access được cung cấp bởi các hãng uy tín, đáp ứng đa dạng nhu cầu từ văn phòng nhỏ đến trung tâm dữ liệu lớn:

+ Cisco Systems: Cisco Catalyst 1000/2960/9200/9300 Series: Dòng switch truy cập phổ biến trong các doanh nghiệp và tổ chức lớn, hỗ

trợ đầy đủ VLAN, PoE+, QoS, khả năng bảo mật lớp truy cập và quản trị tập trung.

+ HPE Aruba Networks: Aruba 2530/2540/2930 Series: Hỗ trợ các tính năng truy cập doanh nghiệp, PoE, bảo mật nâng cao, và quản lý qua Aruba Central.
+ Huawei: S5700, S5720 Series: Hỗ trợ Layer 2/3, khả năng PoE+, bảo mật đầu cuối và quản trị từ xa qua eSight.
+ Juniper Networks: EX2300, EX3400 Series: Phù hợp với môi trường campus hoặc phân phối, hỗ trợ tính năng EVPN-VXLAN, PoE+, bảo mật động.
+ Dell, TP-Link, D-Link, MikroTik: Dành cho phân khúc SMB, với chi phí đầu tư hợp lý, cấu hình linh hoạt và dễ triển khai.

– Thiết bị Switch access tại Trung tâm Dịch vụ số MobiFone

Tại Trung tâm Dịch vụ số MobiFone, các thiết bị Cisco Catalyst 9200 và 9300 Series đang được triển khai rộng rãi tại lớp truy cập của hệ thống mạng. Việc lựa chọn hai dòng switch này là kết quả của quá trình đánh giá kỹ lưỡng về hiệu suất, độ tin cậy, khả năng mở rộng và khả năng tích hợp với hệ sinh thái mạng hiện có. Lý do cụ thể bao gồm:

+ Khả năng mở rộng linh hoạt và hiệu năng cao: Cả hai dòng Catalyst 9200 và 9300 hỗ trợ lên đến 48 cổng Gigabit, uplink 1G/10G, giúp đáp ứng tốt cho hệ thống có mật độ thiết bị đầu cuối lớn như tại Trung tâm Dịch vụ số.
+ Hỗ trợ PoE/PoE+: Với khả năng cấp nguồn qua Ethernet cho thiết bị như camera IP, điện thoại VoIP, access point – switch giúp đơn giản hóa triển khai, tiết kiệm hạ tầng điện và giảm chi phí vận hành.
+ Tính năng bảo mật lớp truy cập nâng cao: Tích hợp các cơ chế bảo vệ như 802.1x, DHCP Snooping, Dynamic ARP Inspection, giúp kiểm soát thiết bị truy cập và phòng chống tấn công giả mạo ngay tại lớp đầu vào.

+ Tích hợp với hệ sinh thái quản lý Cisco DNA Center: Cho phép triển khai và vận hành mạng dựa trên chính sách, tự động hóa cấu hình và giám sát thiết bị theo thời gian thực.
+ Độ tin cậy cao, hỗ trợ stack và nguồn dự phòng: Catalyst 9300 hỗ trợ stacking lên tới 8 thiết bị, đồng thời tích hợp nguồn dự phòng, giúp hệ thống mạng truy cập luôn sẵn sàng và ổn định.
+ Quản lý và giám sát dễ dàng: Các thiết bị này tương thích với các công cụ quản trị mạng trung tâm như SolarWinds, Polestar, giúp Trung tâm dễ dàng theo dõi trạng thái hoạt động và phát hiện sớm sự cố.

Việc sử dụng Cisco Catalyst 9200 và 9300 Series giúp Trung tâm Dịch vụ số MobiFone đảm bảo khả năng mở rộng mạng linh hoạt, bảo mật vững chắc, và vận hành mạng truy cập ổn định 24/7, phù hợp với yêu cầu vận hành của một hệ thống cung cấp dịch vụ số đa dạng và quy mô lớn trên toàn quốc.

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

– Khái niệm

Prometheus là một nền tảng giám sát mã nguồn mở chuyên dụng cho dữ liệu chuỗi thời gian (time-series), được phát triển bởi SoundCloud và sau đó trở thành dự án của Cloud Native Computing Foundation (CNCF). Prometheus

được thiết kế để phục vụ việc giám sát các hệ thống phân tán, đặc biệt phù hợp với kiến trúc microservices và nền tảng container như Kubernetes [1].

- Tính năng chính
  - + Cơ chế thu thập dữ liệu dạng "pull": Prometheus chủ động lấy dữ liệu từ các exporter được cài trên máy chủ hoặc thiết bị, thông qua giao thức HTTP hoặc SNMP, tạo điều kiện cho việc mở rộng giám sát dễ dàng mà không cần tác nhân (agent) phức tạp.
  - + CSDL chuỗi thời gian nội bộ: Tích hợp cơ sở dữ liệu time-series tối ưu hóa cao, cho phép lưu trữ lượng lớn dữ liệu giám sát, phục vụ mục đích truy vấn, phân tích và cảnh báo trong thời gian thực.
  - + Ngôn ngữ truy vấn PromQL mạnh mẽ: Hỗ trợ thực hiện các phép phân tích thống kê, tính toán trung bình, xu hướng, sai số, v.v. trên dữ liệu giám sát, giúp quản trị viên xây dựng dashboard và cảnh báo logic tùy biến.
  - + Hệ thống cảnh báo Alertmanager: Cho phép cấu hình các rule cảnh báo theo điều kiện cụ thể, gửi thông báo tới email, webhook, Slack, Telegram,... với khả năng gom nhóm cảnh báo và lọc sự kiện trùng lặp.
  - + Khả năng tích hợp và mở rộng cao: Prometheus dễ dàng tích hợp với Grafana để trực quan hóa dữ liệu, tương thích với hệ sinh thái cloud-native như Kubernetes, Docker, Istio.
- Ứng dụng tại Trung tâm Dịch vụ số MobiFone

  Prometheus được sử dụng chủ yếu để giám sát:
  - + Các dịch vụ nền tảng container (Kubernetes, Docker Swarm).
  - + Máy chủ ứng dụng (Java, NodeJS, .NET core) và hệ thống API gateway.
  - + Giám sát tài nguyên máy chủ (CPU, RAM, Disk, Network) thông qua node_exporter.

Hệ thống giúp Trung tâm phát hiện nhanh sự cố ở cấp độ ứng dụng, giám sát sát sao các thông số hiệu năng của dịch vụ, tối ưu hóa chi phí nhờ không phụ thuộc giấy phép phần mềm thương mại. Tuy nhiên, nhược điểm là giao diện trực quan chưa thân thiện, cần kết hợp với Grafana hoặc công cụ visualization khác để hoàn chỉnh trải nghiệm giám sát.

1.2.2. Giải pháp giám sát cảnh báo SolarWinds

– Khái niệm

SolarWinds là một hệ thống giám sát và quản lý mạng thương mại toàn diện, nổi bật với khả năng theo dõi hiệu suất thiết bị mạng, máy chủ, ứng dụng và dịch vụ CNTT trong cả môi trường vật lý lẫn ảo hóa. Đây là giải pháp phù hợp với hệ thống mạng quy mô lớn và yêu cầu giám sát đa tầng.

– Tính năng chính

+ Giám sát toàn diện thiết bị mạng: Bao gồm router, switch, firewall, server vật lý/ảo, thiết bị lưu trữ, access point,... theo các chỉ số hiệu năng, trạng thái hoạt động, băng thông sử dụng, độ trễ và packet loss.
+ Cảnh báo nâng cao: SolarWinds cho phép thiết lập rule cảnh báo dựa trên ngưỡng tự định nghĩa hoặc học từ dữ liệu lịch sử. Hệ thống có khả năng tự động gửi cảnh báo qua email, SMS hoặc công cụ ITSM như ServiceNow.
+ Tích hợp giám sát cấu hình: Tính năng Network Configuration Manager (NCM) hỗ trợ sao lưu, so sánh, khôi phục cấu hình thiết bị mạng – giúp kiểm soát thay đổi và phục hồi sau sự cố nhanh chóng.
+ Giao diện Web GUI mạnh mẽ: Dashboard dạng kéo-thả (drag & drop), biểu đồ dạng thời gian, heatmap và hệ thống báo cáo tùy biến giúp quản trị viên dễ dàng theo dõi tổng thể trạng thái hệ thống.

+ Khả năng tương thích cao: SolarWinds hỗ trợ SNMP, WMI, NetFlow, ICMP, syslog, API… cho phép giám sát thiết bị từ nhiều nhà cung cấp khác nhau như Cisco, Juniper, Fortinet, HP, Dell [14].

– Ứng dụng tại Trung tâm Dịch vụ số MobiFone

Tại Trung tâm Dịch vụ số MobiFone, SolarWinds được sử dụng để:

+ Giám sát thiết bị mạng lõi, các router biên, switch access/distribution.
+ Giám sát các server truyền thống (Windows, Linux) và các hệ thống cơ sở dữ liệu (SQL, Oracle) [14].
+ Theo dõi toàn bộ băng thông các kênh truyền, kiểm tra nghẽn cổ chai mạng hoặc bất thường.

SolarWinds giúp đảm bảo tính liên tục, giám sát tập trung và phát hiện nhanh lỗi phần cứng, lỗi kết nối trong hạ tầng mạng quy mô lớn. Việc sử dụng phần mềm thương mại này giúp tiết kiệm thời gian cấu hình, đảm bảo khả năng hỗ trợ kỹ thuật từ nhà cung cấp khi có sự cố.

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 trong quá trình vận hành khai thác hệ thống mạng của Trung tâm Dịch vụ số Mobifone, thì vấn đề giám sát hoạt động của toàn bộ hệ thống có vai trò rất quan trọng. Các bất thường liên quan đến thiết bị, dịch vụ, tấn công mạng, hay tài nguyên hệ thống,… cần được cảnh báo và phát hiện sớm các vấn đề để nhanh chóng có phương án giải quyết sửa chữa, thay thế và phản ứng kịp thời để hệ thống hoạt động ổn định, thông suốt.

Trong hệ thống mạng lớn như Trung tâm Dịch vụ số MobiFone hiện nay, các thiết bị ứng dụng đều được thiết kế mang tính dự phòng cao để sẵn sàng giải quyết khi có sự cố xảy ra. Nên việc phát hiện kịp thời các thiết bị, các kết nối hư hỏng để tiến hành sửa chữa thay thế lại càng quan trọng. Vì khi sự hư hỏng xảy ra một phần, thành phần dự phòng vẫn hoạt động. Nếu phần hư hỏng không được phát hiện, xử lý kịp thời sẽ nguy cơ cao cho việc vận hành hệ thống. Nếu không có công cụ hỗ trợ, người quản trị sẽ bị động trước các tình huống bất ngờ xảy ra.

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 một thành phần then chốt trong hệ thống quản lý hạ tầng mạng, đóng vai trò đảm bảo hoạt động ổn định, hiệu quả và liên tục của từng thiết bị mạng trong toàn bộ hệ thống. Một trong những nhiệm vụ quan trọng đầu tiên là kiểm kê tài sản, trong đó hệ thống sẽ ghi nhận và cập nhật đầy đủ các thông tin chi tiết về thiết bị như nhà sản xuất, số serial, địa chỉ MAC/IP, vị trí triển khai… giúp quản trị viên theo dõi và quản lý tài sản mạng một cách chính xác [1].

Tiếp theo, giám sát trạng thái là chức năng giúp theo dõi liên tục hoạt động của các thiết bị mạng như router, switch, firewall nhằm phát hiện sớm các bất thường hoặc lỗi, đảm bảo thiết bị luôn vận hành đúng cách. Bên cạnh đó, hệ thống còn hỗ trợ quản lý cấu hình, bao gồm việc lưu trữ, kiểm soát và cập nhật cấu hình thiết bị để đáp ứng các yêu cầu thay đổi của mạng, đồng thời đảm bảo tính nhất quán và an toàn trong quá trình vận hành.

Ngoài ra, việc bảo dưỡng định kỳ và hỗ trợ chia sẻ thông tin qua diễn đàn nội bộ cũng đóng vai trò quan trọng trong việc phòng ngừa sự cố, đồng thời tạo môi trường trao đổi giữa các quản trị viên để nhanh chóng giải quyết vấn đề khi phát sinh. Cuối cùng, quản lý vòng đời thiết bị là chức năng theo dõi toàn bộ quá trình sử dụng thiết bị từ khi triển khai đến khi ngừng sử dụng hoặc loại bỏ, đảm bảo việc tái sử dụng, thay thế hoặc hủy bỏ diễn ra đúng quy trình và phù hợp với chính sách của tổ chức[5].

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

Quản lý kết nối là một thành phần thiết yếu trong quản trị hạ tầng mạng, tập trung vào việc duy trì, giám sát và tối ưu hóa các kết nối giữa các thiết bị mạng nhằm đảm bảo sự ổn định và hiệu suất cao trong toàn hệ thống. Một trong những chức năng quan trọng là quản lý băng thông, cho phép giám sát và điều chỉnh lưu lượng mạng theo nhu cầu sử dụng, từ đó tránh tình trạng tắc nghẽn và đảm bảo hiệu suất tối ưu cho các ứng dụng quan trọng.

Bên cạnh đó, quản lý đường truyền đóng vai trò theo dõi trạng thái các tuyến kết nối, đánh giá mức độ ổn định, độ trễ và khả năng đáp ứng, giúp duy trì độ tin cậy của mạng trong quá trình vận hành. Khi xảy ra sự cố, hệ thống quản lý kết nối có khả năng xác định và xử lý nhanh các vấn đề liên quan đến kết nối, chẳng hạn như thiếu hụt băng thông, mất gói, hoặc độ trễ lớn, giúp khôi phục hoạt động bình thường một cách kịp thời.

Ngoài ra, quản lý kết nối còn bao gồm quản lý tài nguyên mạng, cụ thể là việc phân bổ, gán và thu hồi địa chỉ IP hoặc các tài nguyên mạng khác theo chính sách của tổ chức, nhằm đảm bảo hiệu quả sử dụng, tránh xung đột và tăng tính nhất quán trong quản trị hệ thống. Thực hiện tốt các chức năng này sẽ góp phần quan trọng vào việc nâng cao chất lượng dịch vụ, giảm thiểu thời gian gián đoạn và tối ưu hóa hạ tầng mạng tổng thể.

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

Quản lý bảo mật là một phần không thể thiếu trong hệ thống quản lý hạ tầng mạng, giữ vai trò then chốt trong việc bảo vệ an toàn thông tin và ngăn chặn các

mối đe dọa từ bên trong lẫn bên ngoài. Một trong những nhiệm vụ quan trọng hàng đầu là quản lý tường lửa, bao gồm việc thiết lập, cấu hình và duy trì các chính sách kiểm soát truy cập nhằm ngăn chặn các kết nối trái phép, đảm bảo mạng nội bộ luôn được bảo vệ trước các cuộc tấn công tiềm ẩn.

Bên cạnh đó, mã hóa dữ liệu cũng đóng vai trò quan trọng trong việc bảo vệ tính toàn vẹn và bí mật của thông tin truyền qua mạng. Việc áp dụng các phương pháp mã hóa mạnh sẽ giúp ngăn chặn nguy cơ rò rỉ dữ liệu hoặc bị đánh cắp trong quá trình truyền tải. Ngoài ra, hệ thống còn thực hiện xác thực người dùng và quản lý quyền truy cập, đảm bảo rằng chỉ những cá nhân được ủy quyền mới có thể tiếp cận tài nguyên hệ thống, từ đó giảm thiểu rủi ro do truy cập trái phép hoặc lạm quyền.

Tổng thể, quản lý bảo mật không chỉ giúp duy trì sự an toàn cho hệ thống mạng mà còn góp phần quan trọng trong việc tuân thủ các tiêu chuẩn và chính sách bảo mật của tổ chức, nâng cao độ tin cậy và khả năng phục hồi của hạ tầng CNTT trước các sự cố an ninh mạng.

Những thành phần cơ bản này là nền tảng để hệ thống quản lý hạ tầng mạng có thể hoạt động một cách hiệu quả, đáp ứng đúng nhu cầu của tổ chức trong việc duy trì một môi trường mạng an toàn và ổn định. Trong những chương tiếp theo, chúng ta sẽ chi tiết hóa mỗi thành phần này để hiểu rõ hơn về cách chúng tương tác và ảnh hưởng đến hiệu suất toàn bộ hệ thống.

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)

Giám sát (Monitoring) là một yếu tố then chốt trong quản lý hạ tầng mạng hiện đại, giúp đảm bảo hệ thống hoạt động ổn định, hiệu quả và phát hiện kịp thời các sự cố trước khi gây ảnh hưởng nghiêm trọng. Việc giám sát không chỉ dừng ở theo dõi trạng thái thiết bị, mà còn hỗ trợ tối ưu hóa tài nguyên và nâng cao hiệu suất toàn hệ thống [12].

Cụ thể, theo dõi hiệu suất giúp quản trị viên giám sát liên tục các chỉ số như băng thông, độ trễ, tải CPU để đánh giá tổng thể hoạt động mạng. Giám sát tình trạng cho phép phát hiện sớm sự cố thông qua việc kiểm tra trạng thái thiết bị và kết nối theo thời gian thực. Cuối cùng, thống kê và báo cáo cung cấp dữ liệu trực quan, hỗ trợ phân tích xu hướng và ra quyết định kịp thời nhằm cải thiện hiệu quả vận hành hệ thống.

Cấu hình (Configuration) là yếu tố then chốt trong quản lý hạ tầng mạng, ảnh hưởng trực tiếp đến sự ổn định, hiệu quả và an toàn của hệ thống. Việc cấu hình chính xác và đồng bộ giúp tối ưu hiệu suất và giảm thiểu rủi ro do lỗi thao tác hoặc không nhất quán.

Quản lý cấu hình không chỉ bao gồm việc chỉnh sửa và lưu trữ thông số thiết bị, mà còn cung cấp giao diện trực quan giúp quản trị viên dễ dàng theo dõi và kiểm soát các thay đổi. Trong môi trường hiện đại, tự động hóa cấu hình trở nên quan trọng, giúp triển khai nhanh chóng, giảm lỗi thủ công và đảm bảo tính nhất quán toàn hệ thống.

Phần này sẽ tập trung vào các khía cạnh chính của quản lý cấu hình, từ giao diện quản trị đến các công cụ tự động hóa, nhằm nâng cao độ tin cậy và khả năng mở rộng trong vận hành mạng.

Quản lý sự cố (Fault Management) là yếu tố quan trọng trong việc duy trì sự ổn định và liên tục của hệ thống mạng, nơi các sự cố như mất kết nối, giảm hiệu suất hay lỗi phần cứng có thể xảy ra bất kỳ lúc nào. Một hệ thống quản lý

sự cố hiệu quả cần có khả năng phát hiện tự động các vấn đề, từ đó gửi cảnh báo và báo cáo kịp thời giúp quản trị viên nhanh chóng nắm bắt tình hình.

Bên cạnh đó, hệ thống còn cần cung cấp các công cụ hỗ trợ xử lý sự cố, cho phép quản trị viên can thiệp nhanh chóng và chính xác. Việc tự động hóa toàn bộ quy trình từ phát hiện đến khắc phục giúp giảm thiểu thời gian gián đoạn và nâng cao hiệu quả vận hành mạng.

Bảo mật (Security) là yếu tố thiết yếu để đảm bảo an toàn cho dữ liệu và dịch vụ trong hệ thống mạng hiện đại. Quản lý bảo mật không chỉ dừng lại ở việc ngăn chặn các mối đe dọa bên ngoài mà còn bao gồm việc xây dựng chính sách bảo mật rõ ràng, giám sát liên tục các mối nguy và kiểm soát truy cập hệ thống[5].

Việc quản lý chính sách bảo mật giúp đảm bảo hệ thống tuân thủ các quy định an toàn, trong khi giám sát mối đe dọa hỗ trợ phát hiện và phản ứng kịp thời với các hành vi bất thường. Đồng thời, xác thực và quản lý quyền truy cập giúp giới hạn quyền thao tác, đảm bảo chỉ người có thẩm quyền mới được phép truy cập và cấu hình hệ thống.

Tích hợp và mở rộng (Integration and Scalability) là những yếu tố then chốt giúp hệ thống mạng duy trì hiệu quả hoạt động trong bối cảnh công nghệ thông tin liên tục phát triển. Việc tích hợp các hệ thống quản lý như quản lý dịch vụ, quản lý doanh nghiệp và các ứng dụng bên thứ ba không chỉ tạo nên một hệ sinh thái mạng đồng bộ mà còn góp phần tối ưu hóa quy trình vận hành, giúp giảm thiểu chi phí và thời gian quản trị.

Song song với đó, khả năng mở rộng linh hoạt cho phép hệ thống dễ dàng thích ứng với sự phát triển của tổ chức và đáp ứng tốt nhu cầu ngày càng tăng của người dùng. Một hệ thống mạng hiện đại cần được thiết kế để không chỉ đáp ứng yêu cầu hiện tại, mà còn sẵn sàng mở rộng cả về quy mô lẫn chức năng trong tương lai.

Nhìn chung, các chức năng quản lý này đóng vai trò quan trọng trong việc duy trì hệ thống mạng hoạt động hiệu quả, an toàn và linh hoạt. Trong các chương tiếp theo, chúng ta sẽ đi sâu phân tích cách từng chức năng tương tác và tác động đến hiệu suất tổng thể của hạ tầng mạng.

2.1.3. Kiến trúc quản lý mạng dựa trên TMN

Các mạng viễn thông ngày nay được đặc trưng bởi sự kết hợp chặt chẽ giữa các dịch vụ và tài nguyên mạng, được triển khai theo một chuỗi các đa lớp: các mạng OAM&P và các hệ thống điều hành cho mỗi một cặp dịch vụ và tài nguyên tương ứng. Hơn nữa, các phần tử được quản lý có các thuộc tính riêng biệt đối với các chức năng OAM&P. Do đó mạng quản lý cũng phải tạo ra các vùng quản lý riêng biệt cho các phần từ này và các vùng này ít liên quan với nhau.

Quan điểm mạng thông minh sẽ được áp dụng trong mạng quản lý viễn thông (TMN), nguyên tắc thông tin quản lý định nghĩa mối quan hệ cơ bản giữa các khối chức năng mạng cơ bản (hệ thống điều hành, mạng thông tin số liệu, phần tử mạng) băng các giao diện chuẩn. TMN còn giới thiệu nguyên tắc điều khiển phân mạng trong đó phân mạng đóng vai trò quan trọng trong việc phát triển mạng quản lý đáp ứng các yêu cầu tương lai. [12]

Từ quan điểm quản lý mạng, quản lý mạng được chia thành năm nhóm chức năng như sau:

- 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 một khía cạnh quan trọng trong việc duy trì và tối ưu hóa hoạt động của một hạ tầng mạng. Nó là quá trình giám sát, đánh giá, và điều chỉnh hiệu suất của hệ thống mạng để đảm bảo rằng nó hoạt động ổn định, hiệu quả, và đáp ứng được nhu cầu của người dùng và ứng dụng.

Quản lý hiệu năng bao gồm việc thu thập, phân tích, và báo cáo về các chỉ số quan trọng của mạng như băng thông, tải trọng, độ trễ, và sự sụp đổ. Bằng cách giám sát và đánh giá các chỉ số này, người quản trị mạng có thể nhận biết các vấn đề và tiềm ẩn, từ đó có thể thực hiện các biện pháp cải thiện và dự đoán các tình huống tiềm ẩn.

Trong quá trình quản lý hiệu năng, cảnh báo và báo động được sử dụng để thông báo về các sự cố hoặc vượt ngưỡng về hiệu suất. Các công cụ phân tích và đánh giá được sử dụng để xác định nguyên nhân của các vấn đề và đề xuất các biện pháp sửa chữa phù hợp.

Mục tiêu của quản lý hiệu năng là đảm bảo rằng mạng hoạt động một cách ổn định và hiệu quả, đồng thời đáp ứng được yêu cầu của người dùng và ứng dụng. Bằng cách tối ưu hóa hiệu suất của mạng, tổ chức và doanh nghiệp có thể tăng cường năng suất làm việc, cải thiện trải nghiệm người dùng, và đảm bảo tính liên tục của dịch vụ.[5]

– Giám sát hoạt động

Trong quản lý hiệu năng hệ thống, việc giám sát hoạt động của mạng là một bước không thể thiếu nhằm đảm bảo hệ thống vận hành ổn định, hiệu quả và đáp ứng tốt các yêu cầu về hiệu suất. Quá trình này bao gồm nhiều khía cạnh quan trọng, bắt đầu từ thu thập dữ liệu hiệu năng. Các công cụ giám sát sẽ tự động thu thập các chỉ số như băng thông, tải CPU, độ trễ truyền tải và số lượng gói tin qua mạng từ các thiết bị và hệ thống. Những dữ liệu này được xử lý để tạo thành các báo cáo và biểu đồ thống kê, giúp quản trị viên có cái nhìn toàn diện về tình trạng hệ thống.

Tiếp theo, việc theo dõi trạng thái hoạt động được thực hiện liên tục để đảm bảo mạng hoạt động ổn định, không xảy ra sự cố về hiệu suất. Các chỉ số hiệu năng quan trọng được hiển thị trực quan trên giao diện quản lý, giúp người quản trị mạng dễ dàng giám sát trạng thái hiện tại và phát hiện sớm các bất thường tiềm ẩn.

Khi các chỉ số vượt quá ngưỡng an toàn hoặc có sự cố xảy ra, hệ thống sẽ tự động kích hoạt cảnh báo và báo động, thông qua email, tin nhắn hoặc thông báo trên giao diện điều khiển. Điều này giúp người quản trị phản ứng kịp thời, ngăn chặn hoặc giảm thiểu tác động tiêu cực đến hoạt động chung của hệ thống.

Cuối cùng, quá trình giám sát cho phép tương tác và can thiệp trực tiếp. Khi phát hiện vấn đề, quản trị viên có thể chủ động thực hiện các hành động cần thiết như thay đổi cấu hình, khởi động lại dịch vụ hoặc điều hướng lưu lượng mạng. Các biện pháp này giúp khắc phục nhanh chóng các sự cố, duy trì hiệu suất mạng ổn định và đảm bảo chất lượng dịch vụ liên tục.

– Điều khiển quản lý hoạt động

Trong quản lý hiệu năng hệ thống, điều khiển và quản lý hoạt động mạng là một quy trình trọng yếu nhằm đảm bảo hạ tầng mạng hoạt động đúng theo mong đợi và đáp ứng đầy đủ nhu cầu của người dùng. Quá trình này không chỉ giúp duy trì hiệu suất ổn định mà còn hỗ trợ tối ưu tài nguyên, giảm thiểu rủi ro tắc nghẽn và tăng tính sẵn sàng của hệ thống. Điều khiển hoạt động thường được chia thành hai nội dung chính: điều khiển lưu lượng và chức năng quản lý lưu lượng.

Về phía điều khiển lưu lượng, đây là yếu tố quyết định trong việc duy trì và tối ưu hóa quá trình truyền dữ liệu trong mạng. Một trong những nội dung quan trọng là quản lý băng thông, trong đó người quản trị cần kiểm soát cách sử dụng tài nguyên mạng để đảm bảo sự phân phối hợp lý và hiệu quả. Điều này thường được thực hiện thông qua việc thiết lập giới hạn băng thông cho từng nhóm người dùng hoặc ứng dụng, đồng thời ưu tiên tài nguyên cho các dịch vụ quan trọng.

Tiếp theo là kiểm soát lưu lượng, cho phép thiết lập các quy tắc điều chỉnh việc truyền dữ liệu trong mạng. Bằng cách xác định rõ các chính sách ưu tiên, người quản trị có thể giảm thiểu hiện tượng tắc nghẽn, đảm bảo chất lượng dịch vụ (QoS) cho các ứng dụng thiết yếu như thoại, video, hay hệ thống giao dịch thời gian thực.

Về chức năng quản lý lưu lượng, đầu tiên là khả năng xác định và phân loại lưu lượng. Người quản trị cần nắm rõ luồng dữ liệu trong mạng đến từ đâu, thuộc loại nào (ứng dụng, dịch vụ, người dùng...) để áp dụng các chính sách phù hợp. Song song với đó là quá trình giám sát và phân tích lưu lượng, giúp hiểu rõ hành vi hoạt động của mạng và phát hiện sớm các bất thường tiềm ẩn, như lưu lượng đột biến, truy cập bất thường hoặc lạm dụng tài nguyên.

Cuối cùng, dựa trên các dữ liệu phân tích, người quản trị sẽ thực hiện các biện pháp kiểm soát phù hợp. Điều này có thể bao gồm thiết lập quy tắc chặn, giới hạn hoặc ưu tiên lưu lượng, áp dụng các chính sách phân loại nâng cao nhằm đảm bảo mạng luôn vận hành ổn định, hiệu quả và phù hợp với mục tiêu khai thác của tổ chức.

– Phân tích hoạt động

Phân tích hoạt động là một phần không thể thiếu trong quản lý hiệu năng mạng, đóng vai trò quan trọng trong việc giúp người quản trị hiểu rõ cách hệ thống vận hành, đồng thời phát hiện sớm các vấn đề tiềm ẩn có thể ảnh hưởng đến hiệu suất và độ ổn định của mạng. Quá trình này bắt đầu bằng giám sát và thu thập dữ liệu từ các thiết bị mạng và hệ thống. Các công cụ giám sát sẽ tự động ghi nhận các chỉ số như băng thông, mức sử dụng CPU, độ trễ và lưu lượng dữ liệu, làm nền tảng cho các bước phân tích tiếp theo.

Sau khi dữ liệu được thu thập, bước tiếp theo là xử lý và biến đổi dữ liệu. Thông qua việc áp dụng các kỹ thuật lọc, tổng hợp và chuyển đổi, dữ liệu thô được chuyển hóa thành thông tin có giá trị, dễ hiểu và phù hợp cho việc phân tích chuyên sâu. Các công cụ phân tích có thể tích hợp thêm các thuật toán học máy hoặc mô hình dự báo để nâng cao độ chính xác trong việc đánh giá hiệu năng hệ thống.

Một trong những mục tiêu chính của phân tích hoạt động là phát hiện sự cố và xu hướng bất thường trong mạng. Bằng cách so sánh các chỉ số hiện tại với ngưỡng định trước hoặc mô hình hành vi tiêu chuẩn, hệ thống có thể cảnh báo sớm về những bất thường, chẳng hạn như tắc nghẽn, rò rỉ tài nguyên hoặc sự tấn

công từ bên ngoài. Việc phát hiện sớm này cho phép người quản trị chủ động ứng phó và ngăn chặn các sự cố trước khi chúng ảnh hưởng đến toàn hệ thống.

Ngoài ra, phân tích hoạt động còn hỗ trợ tạo ra các báo cáo và biểu đồ thống kê, giúp minh họa trực quan kết quả phân tích và cung cấp cái nhìn tổng thể về hiệu suất mạng theo thời gian. Những thông tin này không chỉ hỗ trợ giám sát thời gian thực mà còn là cơ sở dữ liệu quan trọng phục vụ việc đánh giá định kỳ và tối ưu hóa hệ thống.

Cuối cùng, dựa trên kết quả phân tích, người quản trị mạng có thể đưa ra các quyết định và hành động cụ thể nhằm cải thiện hiệu suất vận hành. Các hành động này có thể là can thiệp tức thời để xử lý sự cố, hoặc xây dựng kế hoạch dài hạn nhằm nâng cấp, tối ưu hoặc thay đổi kiến trúc mạng theo hướng hiệu quả và bền vững hơn.

– Đảm bảo chất lượng hoạt động

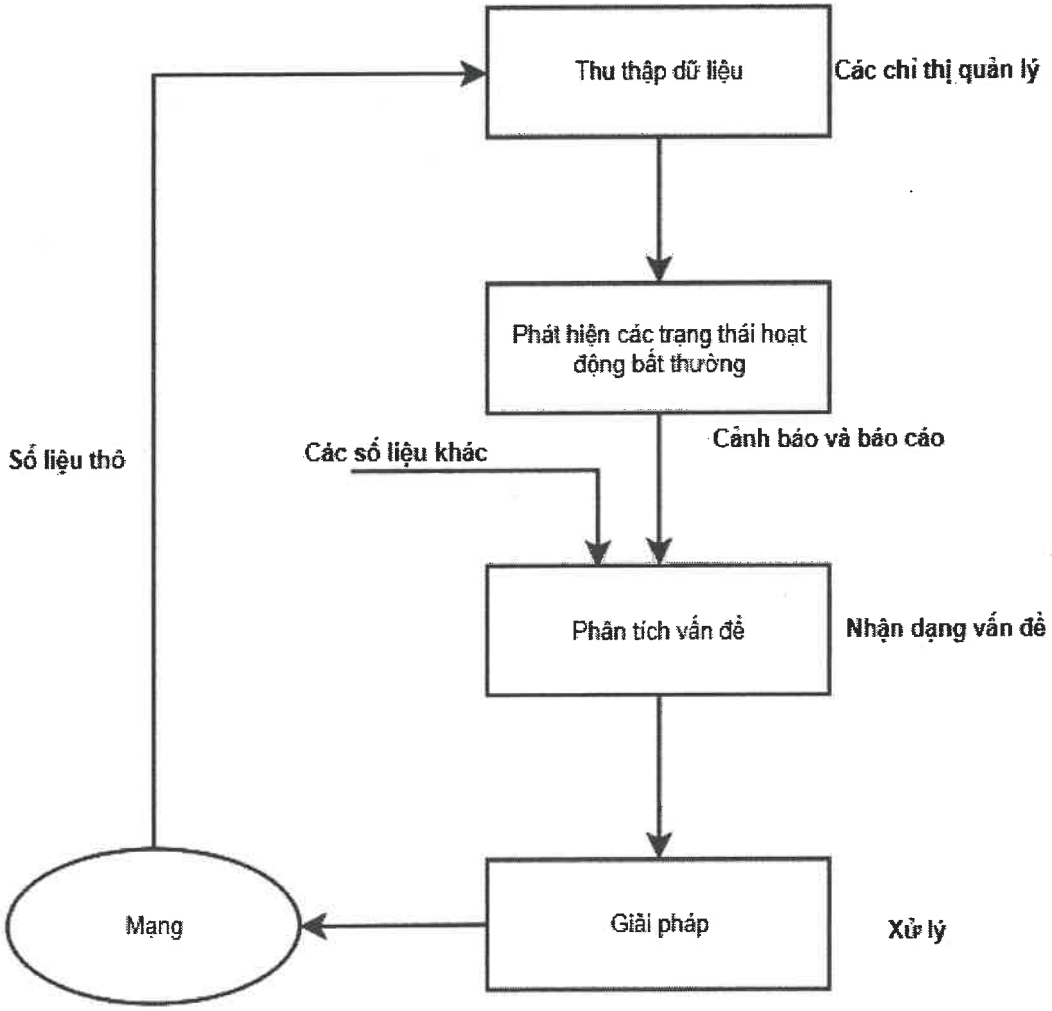
Đảm bảo chất lượng hoạt động là một yếu tố cốt lõi trong quản lý hạ tầng mạng, nhằm duy trì sự ổn định, tin cậy và hiệu quả của các dịch vụ CNTT cung cấp cho người dùng. Để đạt được điều này, hệ thống cần được đánh giá hiệu suất mạng định kỳ, đảm bảo các chỉ số vận hành luôn nằm trong ngưỡng cho phép và đáp ứng tốt các yêu cầu về tốc độ, độ trễ cũng như khả năng đáp ứng trong các tình huống tải cao.

Bên cạnh đó, việc theo dõi liên tục hoạt động của hệ thống giúp phát hiện sớm các sự cố hoặc vấn đề tiềm ẩn trước khi chúng ảnh hưởng đến trải nghiệm người dùng. Điều này đòi hỏi hệ thống giám sát phải luôn sẵn sàng, chính xác và có khả năng ghi nhận các thay đổi bất thường trong thời gian thực.

Ngoài ra, cấu hình hệ thống cũng cần được tối ưu hóa thường xuyên, đảm bảo phù hợp với sự phát triển của hạ tầng và nhu cầu sử dụng. Khi xảy ra sự cố, việc xử lý nhanh chóng và hiệu quả là yếu tố quyết định giúp giảm thiểu thời gian gián đoạn và giữ cho chất lượng dịch vụ luôn ở mức cao. Như vậy, việc đảm bảo chất lượng hoạt động không chỉ là công việc kỹ thuật mà còn là quá trình quản lý toàn diện, liên tục và chủ động.

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

Giám sát cảnh báo là một chức năng thiết yếu trong quản lý hạ tầng mạng, giúp đảm bảo hệ thống luôn được vận hành trong trạng thái ổn định và an toàn. Quá trình này bắt đầu bằng việc theo dõi hoạt động mạng thông qua các công cụ giám sát chuyên dụng. Những công cụ này thu thập và hiển thị dữ liệu thời

gian thực về các chỉ số quan trọng như băng thông, tải trọng CPU, lưu lượng dữ liệu và các thông số vận hành khác của hệ thống.

Một trong những mục tiêu quan trọng của giám sát cảnh báo là phát hiện sớm sự cố. Điều này được thực hiện bằng cách thiết lập các ngưỡng cảnh báo cụ thể cho từng chỉ số hiệu năng. Khi giá trị vượt quá ngưỡng cho phép – ví dụ như CPU quá tải hoặc lưu lượng bất thường – hệ thống sẽ ngay lập tức phát hiện và đánh dấu đây là dấu hiệu của sự cố tiềm ẩn.

Tiếp theo, hệ thống sẽ thực hiện chức năng cảnh báo và gửi thông báo đến các cá nhân hoặc nhóm hỗ trợ có liên quan, thông qua nhiều kênh như email, tin nhắn SMS hoặc thông báo trực tiếp trên giao diện quản lý. Nhờ đó, người quản trị có thể phản ứng nhanh chóng, tiến hành kiểm tra và xử lý sự cố kịp thời, giúp giảm thiểu tối đa thời gian gián đoạn và rủi ro cho toàn bộ hệ thống.

Cô lập sự cố là một bước quan trọng trong quy trình quản lý sự cố mạng, nhằm giảm thiểu tối đa tác động tiêu cực đến toàn bộ hệ thống. Quá trình này bắt đầu bằng việc phân loại và ưu tiên sự cố, trong đó các sự cố được đánh giá dựa trên mức độ nghiêm trọng, phạm vi ảnh hưởng và mức độ ảnh hưởng đến người dùng hoặc dịch vụ. Việc xác định mức độ ưu tiên giúp đội ngũ kỹ thuật đưa ra quyết định xử lý theo thứ tự hợp lý và hiệu quả nhất.

Sau khi xác định được mức độ nghiêm trọng, bước tiếp theo là phân tích nguyên nhân, tức là tìm ra gốc rễ của sự cố – liệu đó là do lỗi phần cứng, phần mềm, cấu hình hay do yếu tố bên ngoài như tấn công mạng. Quá trình này đòi hỏi các công cụ giám sát và kỹ thuật phân tích chính xác để làm rõ bản chất của vấn đề và phạm vi ảnh hưởng.

Cuối cùng, hệ thống sẽ tiến hành cô lập sự cố, tức là ngăn chặn sự cố lan rộng bằng cách khoanh vùng khu vực bị ảnh hưởng và tạm thời cách ly nó khỏi các thành phần khác của hệ thống mạng. Việc cô lập kịp thời không chỉ giúp hạn chế thiệt hại mà còn tạo điều kiện thuận lợi cho quá trình khắc phục, đồng thời đảm bảo các phần còn lại của hệ thống vẫn duy trì hoạt động ổn định.

Sau khi sự cố đã được cô lập, bước tiếp theo trong quy trình xử lý là thực hiện các biện pháp khắc phục nhằm sửa chữa lỗi và khôi phục hệ thống về trạng thái hoạt động bình thường. Các biện pháp này có thể bao gồm khởi động lại thiết bị, cập nhật cấu hình, thay thế phần cứng hoặc sửa lỗi phần mềm tùy theo nguyên nhân đã xác định.

Sau khi khắc phục, cần tiến hành kiểm tra và xác nhận để đảm bảo rằng sự cố đã được giải quyết triệt để và hệ thống hoạt động ổn định. Việc xác minh kỹ lưỡng sau khi xử lý giúp tránh tình trạng sự cố tái phát hoặc phát sinh vấn đề mới liên quan.

Cuối cùng, một bước không thể thiếu là ghi nhận và học hỏi từ sự cố. Toàn bộ quá trình xử lý cần được ghi chép lại đầy đủ, bao gồm nguyên nhân, giải pháp và kết quả sau can thiệp. Việc này không chỉ giúp cải thiện quy trình xử lý sự cố trong tương lai mà còn tạo ra cơ sở tri thức hữu ích để phòng ngừa các sự cố tương tự, nâng cao năng lực quản lý và vận hành hệ thống mạng một cách chủ động và hiệu quả hơn.

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

Cung cấp cấu hình là yếu tố then chốt đảm bảo hiệu suất và an toàn cho hệ thống mạng. Việc quản lý cấu hình cần được thực hiện theo quy trình chặt chẽ, gồm ba bước: thu thập, tổ chức và bảo mật thông tin cấu hình.

Trước tiên, quản trị viên cần thu thập dữ liệu cấu hình từ các thiết bị mạng và ứng dụng để hiểu rõ trạng thái hoạt động. Sau đó, tổ chức và lưu trữ thông tin một cách khoa học giúp dễ dàng tra cứu, so sánh và phục hồi khi cần. Cuối

cùng, bảo mật cấu hình là bước quan trọng nhằm bảo vệ dữ liệu nhạy cảm, thông qua mã hóa, phân quyền và kiểm soát truy cập.

Quản lý cấu hình hiệu quả không chỉ duy trì sự ổn định của hệ thống, mà còn giúp giảm rủi ro, nâng cao khả năng phục hồi và tối ưu công tác quản trị mạng..

– Trạng thái và điều khiển thiết bị

Trạng thái và điều khiển thiết bị là yếu tố quan trọng trong quản lý hạ tầng mạng hiện đại, giúp đảm bảo hệ thống vận hành ổn định và liên tục. Theo dõi trạng thái thiết bị theo thời gian thực cho phép quản trị viên phát hiện sớm các dấu hiệu bất thường như lỗi phần cứng, quá tải hoặc ngắt kết nối, từ đó can thiệp kịp thời.

Bên cạnh đó, điều khiển thiết bị từ xa giúp thực hiện các thao tác như khởi động lại, thay đổi cấu hình hoặc cập nhật phần mềm mà không cần trực tiếp đến hiện trường. Sự kết hợp giữa giám sát và điều khiển từ xa góp phần nâng cao hiệu quả quản lý, giảm chi phí vận hành và tăng tính linh hoạt cho hệ thống mạng.

– Cài đặt thiết bị

Việc cài đặt thiết bị trong hệ thống mạng là một khâu then chốt trong quá trình triển khai hạ tầng công nghệ thông tin, bởi nó ảnh hưởng trực tiếp đến hiệu suất hoạt động, độ ổn định và tính nhất quán của toàn bộ hệ thống. Trong đó, triển khai cấu hình mới không chỉ dừng lại ở việc thiết lập ban đầu cho các thiết bị mạng và ứng dụng, mà còn bao gồm việc cập nhật cấu hình định kỳ nhằm đáp ứng những thay đổi về kiến trúc hệ thống, nhu cầu sử dụng, hoặc yêu cầu mở rộng.

Bên cạnh đó, đồng bộ hóa cấu hình giữa các thiết bị là yếu tố cần thiết để đảm bảo tất cả thiết bị trong mạng hoạt động theo cùng một tiêu chuẩn, tuân thủ các chính sách quản trị và quy định kỹ thuật chung. Việc đồng bộ hóa không chỉ giúp duy trì sự nhất quán trong vận hành mà còn giảm thiểu rủi ro do cấu hình không đồng đều gây ra, như lỗi kết nối, xung đột truy cập hay lỗ hổng bảo mật.

Phần này sẽ trình bày chi tiết các bước triển khai cấu hình mới cũng như quy trình đồng bộ hóa cấu hình thiết bị, từ đó hỗ trợ người quản trị hệ thống đảm bảo môi trường mạng luôn được vận hành một cách ổn định, hiệu quả và linh hoạt trước các yêu cầu thay đổi trong thực tế.

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: Tạo và quản lý các tài khoản người dùng trên hệ thống để xác định quyền truy cập và phân quyền.
- Xác thực và xác minh: Sử dụng các phương tiện xác thực đáng tin cậy để xác định danh tính của người dùng và đảm bảo rằng chỉ những người được ủy quyền mới có thể truy cập.
- Quản lý quyền truy cập: Xác định và quản lý quyền truy cập của từng tài khoản người dùng để đảm bảo rằng họ chỉ có thể truy cập vào các tài nguyên và chức năng mà họ cần thiết.
- Theo dõi và đánh giá: Theo dõi hoạt động của tài khoản người dùng và đánh giá các hoạt động để phát hiện và ngăn chặn các hành vi không đáng tin cậy.

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 tổ 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

Mạng thông tin ngày nay đã trở thành hệ thống rộng lớn và phức tạp, chịu áp lực ngày càng tăng từ sự phát triển nhanh chóng của công nghệ và sự phổ biến của các ứng dụng kỹ thuật số. Để đảm bảo hoạt động ổn định và an toàn mạng, việc triển khai các giải pháp giám sát và cảnh báo hệ thống mạng trở nên hết sức quan trọng.

Cùng với sự phát triển của các hệ thống mạng, số lượng thiết bị và ứng dụng cũng gia tăng, đặt ra thách thức đối với việc quản lý và duy trì môi trường mạng. Các tổ chức ngày nay không chỉ cần quan tâm đến việc theo dõi hiệu suất của các thiết bị mạng mà còn phải đối mặt với những rủi ro về bảo mật, sự cố kỹ thuật và sự không ổn định của ứng dụng.

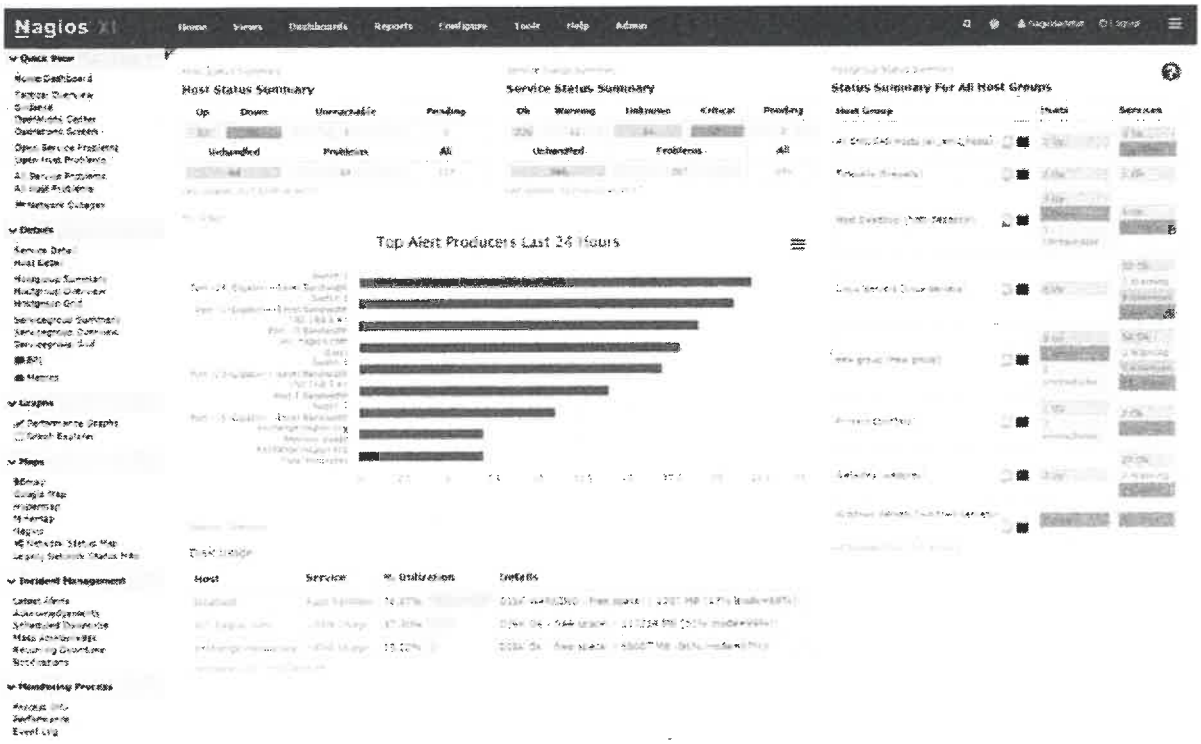
Trong bối cảnh này, các giải pháp giám sát và cảnh báo hệ thống mạng trở thành một phần quan trọng trong chiến lược quản lý mạng của doanh nghiệp. Những công cụ này không chỉ giúp đảm báo tính khả dụng và hiệu suất của mạng mà còn cung cấp thông tin chi tiết và cảnh báo kịp thời, hỗ trợ người quản trị trong việc phân tích, đánh giá và giải quyết sự cố một cách hiệu quả.

Dưới đây là một số giải pháp hàng đầu trong lĩnh vực này để hiểu rõ hơn về cách chúng đóng một vai trò quan trọng trong quản lý mạng hiện tại.

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 [6].

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

Nagios là một hệ thống giám sát cảnh báo nổi bật nhờ nhiều ưu điểm vượt trội, phù hợp với nhu cầu đa dạng của các tổ chức và doanh nghiệp. Trước hết, đây là một giải pháp mã nguồn mở và miễn phí, giúp tiết kiệm đáng kể chi phí triển khai và vận hành so với các phần mềm thương mại. Bên cạnh đó, Nagios có kiến trúc mô-đun cùng hệ thống plugin phong phú, cho phép người quản trị dễ dàng tùy chỉnh và mở rộng chức năng theo yêu cầu cụ thể, từ đó đáp ứng hiệu quả nhiều mô hình và quy mô giám sát khác nhau.

Hơn nữa, với thời gian tồn tại lâu dài và được ứng dụng rộng rãi, Nagios đã chứng minh được độ ổn định và tính đáng tin cậy trong thực tiễn. Hệ thống còn

được hỗ trợ bởi một cộng đồng người dùng và nhà phát triển rộng lớn, cung cấp tài liệu hướng dẫn, diễn đàn thảo luận và các khóa đào tạo chuyên sâu – tạo điều kiện thuận lợi cho việc học hỏi và chia sẻ kinh nghiệm. Ngoài ra, Nagios còn nổi bật với khả năng tích hợp mạnh mẽ thông qua API và các tiện ích mở rộng, cho phép liên kết với nhiều công cụ và ứng dụng khác, từ đó nâng cao năng lực giám sát toàn diện cho hệ thống.

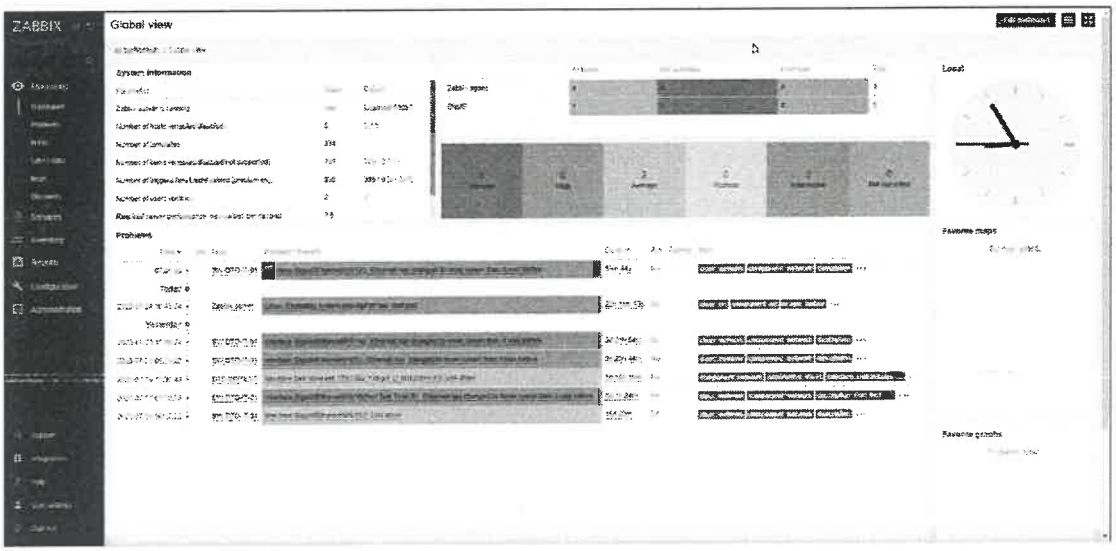
Bên cạnh những ưu điểm nổi bật, hệ thống giám sát cảnh báo Nagios cũng tồn tại một số nhược điểm cần được cân nhắc khi triển khai. Trước hết, do đặc tính tùy chỉnh cao, việc cấu hình và triển khai Nagios có thể trở nên phức tạp, đặc biệt đối với những người dùng mới. Việc làm quen và sử dụng hiệu quả hệ thống này đòi hỏi một khoảng thời gian học hỏi và thực hành đáng kể. Thêm vào đó, mặc dù giao diện web của Nagios được đánh giá là thân thiện, nhưng so với kỳ vọng ngày càng cao của người dùng hiện đại, nó vẫn cần được cải tiến. Khi phải xử lý và giám sát một lượng lớn dữ liệu, giao diện có thể trở nên rối rắm, gây khó khăn cho quá trình quản lý.

Ngoài ra, Nagios phụ thuộc nhiều vào hệ thống plugin và các tiện ích mở rộng (addon) để mở rộng chức năng. Mặc dù điều này mang lại tính linh hoạt, nhưng cũng đồng thời làm tăng độ phức tạp trong quá trình quản lý, cập nhật và bảo trì hệ thống. Cuối cùng, trong các môi trường mạng có quy mô lớn, thời gian phản hồi của Nagios có thể bị ảnh hưởng nếu cấu hình không được tối ưu hóa hợp lý, dẫn đến hiệu suất giám sát không đạt mức kỳ vọng. Những hạn chế này cho thấy Nagios tuy là một công cụ mạnh mẽ, nhưng cần được triển khai và vận hành một cách cẩn trọng để phát huy tối đa hiệu quả.

2.2.2. Giải pháp giám sát cảnh báo Zabbix:

Zabbix được ra mắt lần đầu tiên vào năm 1998 bởi Alexei Vexler với tên gọi ban đầu là "Soviet Linux Network Monitor". Sau đó, nó được đổi tên thành Zabbix và phát triển thành một dự án mã nguồn mở vào năm 2001. Zabbix 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 [7].

Zabbix hoạt động dựa trên mô hình client-server. Máy chủ Zabbix được cài đặt trên một máy tính trung tâm và các agent Zabbix được cài đặt trên các máy chủ, thiết bị mạng và các hệ thống khác cần được giám sát. Agent Zabbix sẽ thu thập dữ liệu về trạng thái và hiệu suất của hệ thống và gửi dữ liệu này về máy chủ Zabbix. Máy chủ Zabbix 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 2.3*.



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

Zabbix là một hệ thống giám sát toàn diện nổi bật nhờ thiết kế linh hoạt và khả năng mở rộng mạnh mẽ. Hệ thống này cho phép thu thập và giám sát dữ liệu từ nhiều nguồn khác nhau như hệ điều hành, ứng dụng và các thiết bị mạng thông qua các giao thức và kỹ thuật phổ biến như SNMP, JMX, SSH, v.v. Điều này giúp Zabbix dễ dàng tích hợp vào nhiều môi trường hạ tầng CNTT khác nhau, từ các doanh nghiệp nhỏ đến các hệ thống phức tạp, đa tầng.

Một điểm nổi bật khác của Zabbix là giao diện web trực quan, hiện đại và dễ sử dụng. Giao diện này được thiết kế theo hướng đối tượng hóa, giúp người quản trị dễ dàng tương tác, nắm bắt trạng thái hệ thống cũng như truy xuất thông tin một cách nhanh chóng và hiệu quả. Đồng thời, hệ thống cảnh báo của Zabbix cũng rất linh hoạt, cho phép người dùng thiết lập cảnh báo dựa trên các ngưỡng định sẵn, sự kiện cụ thể hoặc kịch bản tùy chỉnh, giúp nâng cao khả năng ứng phó và xử lý sự cố kịp thời.

Về mặt bảo mật, Zabbix đáp ứng tốt các yêu cầu hiện đại với các tính năng như mã hóa dữ liệu trong quá trình truyền, xác thực hai yếu tố (2FA) và cơ chế phân quyền chặt chẽ, đảm bảo an toàn cho toàn bộ quá trình giám sát. Cuối cùng, Zabbix còn sở hữu một cộng đồng người dùng đông đảo và năng động, sẵn sàng chia sẻ kinh nghiệm, tài liệu, plugin và hỗ trợ kỹ thuật thông qua diễn đàn, kho tài liệu và các nền tảng trực tuyến – góp phần giúp người dùng khai thác hiệu quả hơn các tính năng của hệ thống.

Bên cạnh những ưu điểm vượt trội, Zabbix cũng tồn tại một số nhược điểm cần được cân nhắc khi triển khai trong thực tế. Trước hết, mặc dù hệ thống cung cấp khả năng tùy chỉnh rất cao, chính điều này lại có thể trở thành rào cản đối với người mới. Việc cấu hình các tham số giám sát theo yêu cầu cụ thể đòi hỏi kiến thức chuyên sâu và sự am hiểu về hệ thống, gây khó khăn cho những người chưa có nhiều kinh nghiệm.

Ngoài ra, giao diện web của Zabbix, dù được đánh giá là đẹp và mạnh mẽ, nhưng trong các môi trường giám sát quy mô lớn, việc hiển thị và quản lý một khối lượng lớn thông tin có thể trở nên phức tạp, gây quá tải về mặt trực quan và thao tác. Hệ thống cũng có yêu cầu khá cao về tài nguyên phần cứng, đặc biệt khi triển khai trong các môi trường lớn hoặc có tần suất thu thập dữ liệu cao, điều này đòi hỏi một hạ tầng đủ mạnh để đảm bảo hiệu suất ổn định.

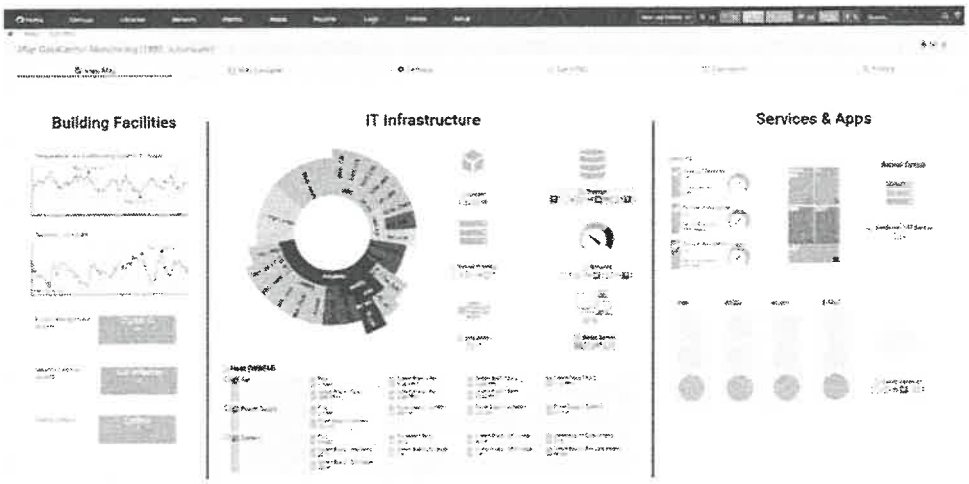
Cuối cùng, việc sử dụng hiệu quả Zabbix đòi hỏi một quá trình đào tạo bài bản. Người dùng cần có thời gian để tìm hiểu rõ về kiến trúc, các khái niệm cốt lõi, cũng như cách thức hoạt động và cấu hình hệ thống. Điều này có thể ảnh hưởng đến tiến độ triển khai nếu đội ngũ kỹ thuật chưa có đủ kỹ năng chuyên môn ngay từ đầu. Vì vậy, mặc dù Zabbix là một công cụ mạnh mẽ, nhưng để khai thác tối đa hiệu quả của nó, cần có sự đầu tư thích đáng về thời gian và nguồn lực.

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 [8].

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

PRTG là một giải pháp giám sát mạng được đánh giá cao nhờ sự tiện lợi và hiệu quả trong quá trình triển khai và vận hành. Một trong những ưu điểm nổi bật của PRTG là khả năng triển khai và cấu hình nhanh chóng. Với quy trình cài đặt đơn giản cùng giao diện người dùng trực quan, thân thiện, PRTG cho phép các quản trị viên thiết lập hệ thống giám sát mà không cần quá nhiều kiến thức kỹ thuật chuyên sâu, từ đó tiết kiệm đáng kể thời gian và công sức.

Hệ thống còn hỗ trợ nhiều giao thức phổ biến như SNMP, WMI, Packet Sniffing, cũng như các loại cảm biến chuyên biệt dành cho từng thiết bị và ứng dụng cụ thể. Điều này giúp PRTG có thể giám sát một cách toàn diện các thành

phần trong mạng, từ thiết bị phần cứng đến phần mềm và dịch vụ chạy trên đó. Giao diện web của PRTG được thiết kế hiện đại, không chỉ dễ sử dụng mà còn cho phép tùy chỉnh linh hoạt, giúp người quản trị theo dõi hiệu suất mạng một cách trực quan và hiệu quả.

Đặc biệt, PRTG cung cấp hệ thống báo cáo chi tiết và các biểu đồ thống kê trực quan, hỗ trợ quản trị viên phân tích hiệu suất mạng và phát hiện xu hướng theo thời gian. Nhờ đó, việc đưa ra các quyết định quản lý, tối ưu hóa hạ tầng mạng hoặc xử lý sự cố trở nên nhanh chóng và chính xác hơn. Với những tính năng này, PRTG trở thành một công cụ giám sát phù hợp với nhiều tổ chức, từ quy mô nhỏ đến doanh nghiệp lớn.

Mặc dù PRTG là một công cụ giám sát mạng mạnh mẽ và thân thiện với người dùng, nó vẫn tồn tại một số nhược điểm đáng lưu ý, đặc biệt khi được triển khai trong các môi trường có quy mô lớn hoặc yêu cầu đặc thù. Một trong những hạn chế đầu tiên là giới hạn số lượng cảm biến trong phiên bản miễn phí. Điều này có thể trở thành trở ngại đối với các tổ chức lớn có nhu cầu giám sát nhiều thiết bị, dịch vụ hoặc ứng dụng đa dạng, buộc họ phải đầu tư vào phiên bản thương mại nếu muốn mở rộng khả năng giám sát.

Bên cạnh đó, PRTG cũng đòi hỏi một lượng tài nguyên hệ thống tương đối lớn, đặc biệt khi được triển khai trong các môi trường mạng phức tạp hoặc có khối lượng dữ liệu giám sát cao. Việc xử lý đồng thời nhiều cảm biến và truy vấn liên tục có thể gây áp lực lên hệ thống máy chủ, ảnh hưởng đến hiệu suất tổng thể nếu không được tối ưu hóa đúng cách.

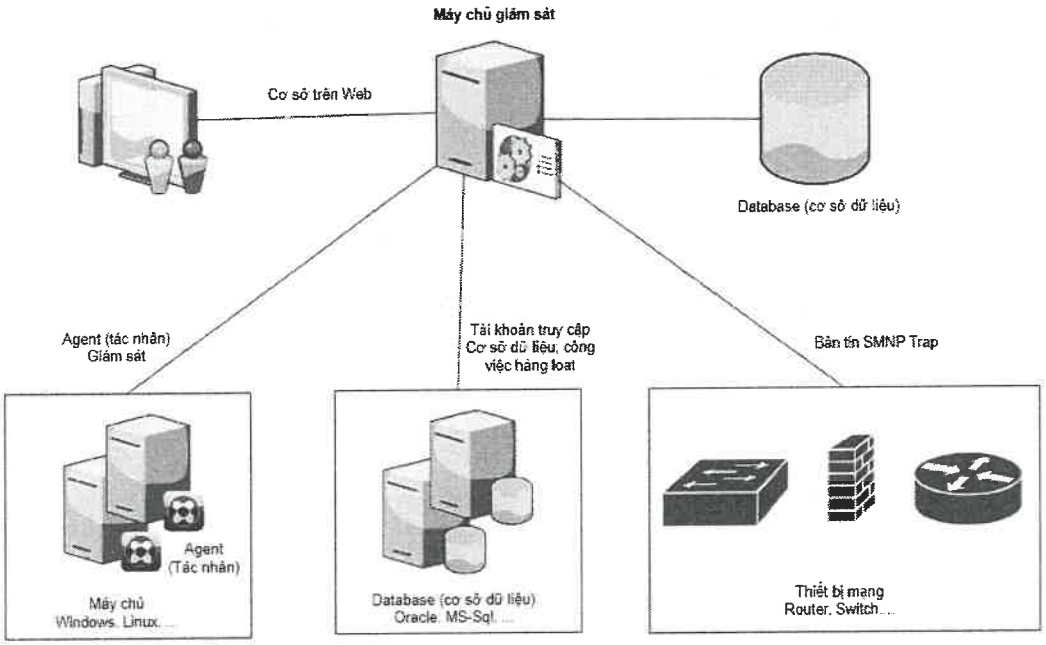
Một nhược điểm khác là khả năng mở rộng còn hạn chế so với một số giải pháp giám sát chuyên sâu khác. Khi hệ thống mạng phát triển với quy mô lớn và cấu trúc phức tạp, PRTG có thể gặp khó khăn trong việc mở rộng hoặc quản lý hiệu quả, dẫn đến nguy cơ giảm hiệu suất và tính ổn định. Ngoài ra, PRTG chủ yếu hỗ trợ mô hình giám sát truyền thống và có thể không thực sự phù hợp với các mô hình mạng hiện đại như hạ tầng đám mây, hybrid cloud hoặc các hệ

thống phân tán phức tạp. Trong những trường hợp này, người dùng có thể cần tìm đến các giải pháp giám sát chuyên biệt hơn để đáp ứng yêu cầu.

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, 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.

Thứ nhất là Node – đây là các đối tượng được hệ thống giám sát theo dõi và thu thập dữ liệu. Các node có thể bao gồm máy chủ (server), thiết bị mạng

(switch, router), ứng dụng, cơ sở dữ liệu, cũng như các tiến trình đang chạy trong hệ thống. Mỗi node cung cấp các chỉ số quan trọng về hiệu năng, trạng thái hoạt động và các sự kiện cần theo dõi.

Thành phần thứ hai là Manager (hay còn gọi là máy chủ giám sát) – đây được xem là thành phần trung tâm và quan trọng nhất trong kiến trúc hệ thống. Manager hoạt động như một framework tích hợp, thực hiện vai trò thu thập dữ liệu từ các node, sau đó xử lý, phân loại và lưu trữ thông tin. Ngoài ra, Manager còn cung cấp các chức năng tương tác với dữ liệu, như hiển thị, cảnh báo, thống kê hoặc kiểm soát truy cập người dùng. Hệ thống Manager được thiết kế với độ ổn định cao, hiệu suất mạnh mẽ và có thể triển khai trên nhiều nền tảng khác nhau, giúp đảm bảo tính linh hoạt và mở rộng của toàn bộ hệ thống.

Tiếp theo là Viewer (người dùng) – đây là những người sử dụng hệ thống giám sát ở các cấp độ khác nhau, từ người dùng phổ thông đến quản trị viên hệ thống. Mỗi người dùng được cấp tài khoản truy cập với giao diện web (web-based) và được phân quyền chi tiết theo vai trò, chức năng và thiết bị cụ thể mà họ có quyền giám sát hoặc thao tác.

Cuối cùng là Repository (cơ sở dữ liệu) – đây là nơi lưu trữ toàn bộ dữ liệu thu thập được từ hệ thống, từ thông tin cấu hình, trạng thái node đến lịch sử sự kiện và cảnh báo. Hệ thống giám sát hỗ trợ sử dụng cơ sở dữ liệu Oracle từ phiên bản 9i trở lên, đảm bảo khả năng lưu trữ dữ liệu ổn định, an toàn và dễ dàng truy xuất khi cần thiết cho phân tích hoặc lập báo cáo.

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.

Hệ thống giám sát tập trung Polestar có thể theo dõi hiệu suất và khả năng đáp ứng của môi trường hệ thống không đồng nhất bao gồm cả các máy chủ khác nhau. Giải pháp có thể theo dõi các chỉ số hiệu suất hệ thống, phân tích các xu hướng và tạo báo cáo, thiết lập các ngưỡng giám sát sự biến đổi hiệu suất (CPU, bộ nhớ, ổ đĩa, hệ thống file, trạng thái session, thông tin các tiến trình đang chạy trên máy chủ).

Các giải pháp sử dụng để giám sát máy chủ đóng vai trò quan trọng trong việc đảm bảo hệ thống vận hành ổn định, phát hiện sớm các sự cố và hỗ trợ xử lý kịp thời. Một trong những phương pháp phổ biến và hiệu quả nhất là giám sát sử dụng Agent.

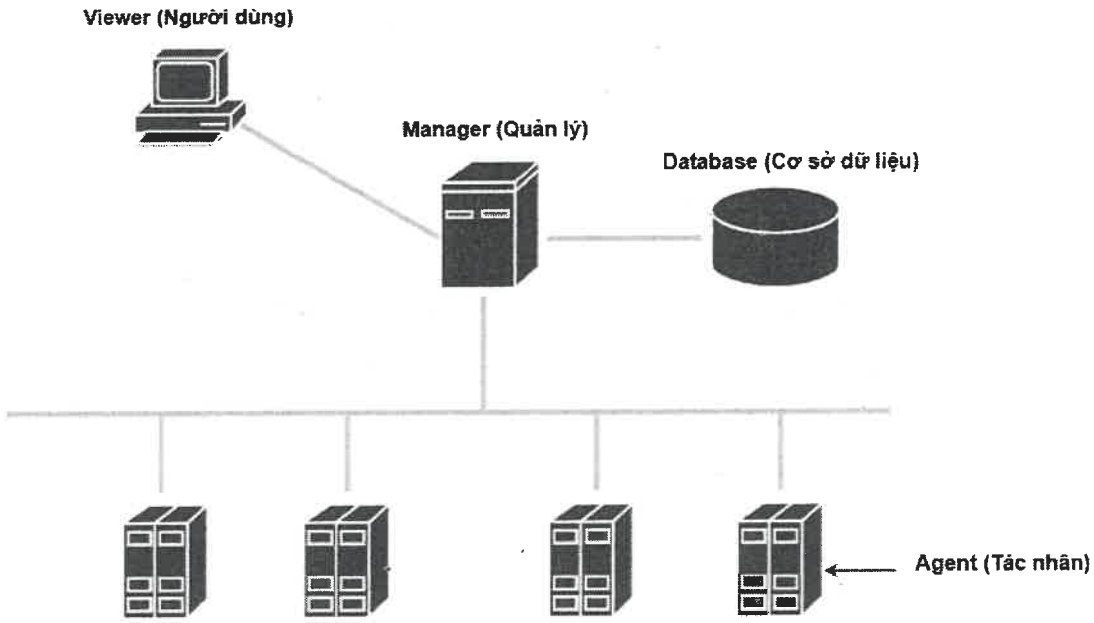
Trong giải pháp này, một Agent sẽ được cài đặt trực tiếp trên máy chủ cần giám sát. Agent đóng vai trò như một công cụ thu thập dữ liệu tại chỗ, liên tục theo dõi các chỉ số hoạt động quan trọng của hệ thống như: hiệu suất CPU, mức sử dụng bộ nhớ, dung lượng ổ đĩa, trạng thái hệ thống file, các phiên làm việc (session), thông tin tiến trình đang chạy, và cả danh sách các tiến trình tiêu tốn nhiều tài nguyên nhất (top process). Những thông tin này được cập nhật định kỳ và gửi về máy chủ giám sát tập trung OMC (Operations Management Console) để lưu trữ, phân tích và hiển thị theo thời gian thực hoặc thông qua báo cáo.

Ưu điểm nổi bật của phương pháp giám sát sử dụng Agent là khả năng thu thập dữ liệu chi tiết, chính xác và có độ sâu, nhờ vào việc Agent có thể truy cập trực tiếp vào tài nguyên hệ thống. Đồng thời, việc gửi dữ liệu về một server tập trung giúp dễ dàng quản lý và theo dõi từ xa nhiều máy chủ cùng lúc, đặc biệt hiệu quả trong các hệ thống lớn hoặc môi trường phức tạp như trung tâm dữ liệu.

Các nền tảng hỗ trợ của hệ thống giám sát bao gồm Sun SOLARIS, AIX, Windows và Linux, cho phép triển khai linh hoạt trên nhiều loại hệ điều hành khác nhau. Nhờ đó, hệ thống có thể giám sát hiệu quả cả môi trường máy chủ

truyền thống lẫn hiện đại, đáp ứng nhu cầu đa dạng của các tổ chức, doanh nghiệp.

Giải pháp này được minh họa cụ thể trong *Hình 2.6,* thể hiện rõ luồng dữ liệu từ Agent trên máy chủ gửi về hệ thống giám sát OMC trung tâm, từ đó cho phép nhà quản trị nhanh chóng phát hiện các bất thường và chủ động xử lý các vấn đề phát sinh.



Hình 2. 6: Giám sát máy chủ cài đặt Agent

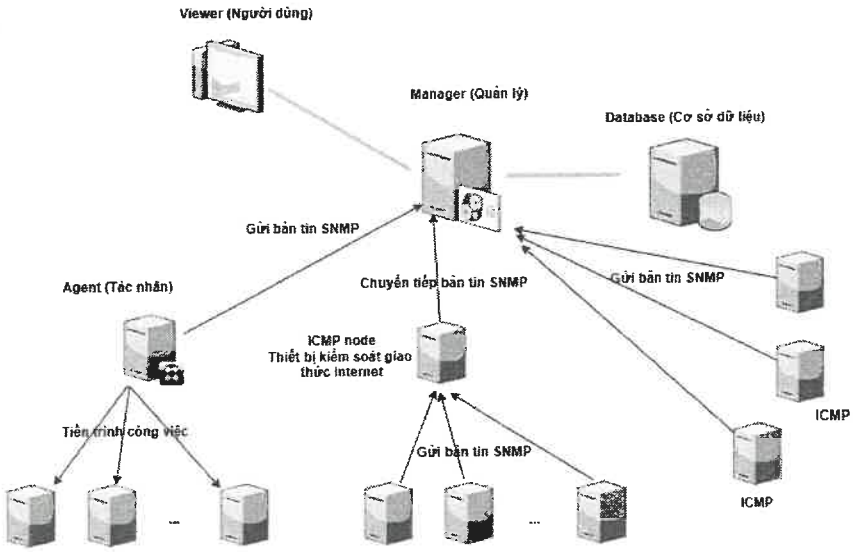
Giám sát máy chủ sử dụng giao thức chuẩn SNMP Trap là một phương pháp phổ biến khác trong hệ thống giám sát tập trung, cho phép thu thập thông tin một cách hiệu quả và gần như theo thời gian thực mà không cần cài đặt phần mềm Agent trên máy chủ giám sát.

Trong mô hình này, các máy chủ hoặc thiết bị cần giám sát sẽ được cấu hình để gửi các bản tin SNMP Trap đến máy chủ giám sát trung tâm. SNMP Trap là một dạng thông điệp thông báo sự kiện được thiết bị gửi đi một cách chủ động khi có thay đổi trạng thái hoặc khi xảy ra sự cố, chẳng hạn như CPU vượt ngưỡng, ổ đĩa đầy, tiến trình bị treo hoặc có thay đổi trong cấu hình hệ thống.

Không giống như phương pháp giám sát chủ động (Agent-based) phải thường xuyên truy vấn và thu thập dữ liệu, SNMP Trap hoạt động theo cơ chế bị động, chỉ gửi thông tin khi có sự kiện xảy ra, giúp giảm tải cho mạng và hệ thống giám sát, đồng thời tăng tốc độ phản hồi với các sự kiện bất thường.

Thông tin được gửi đến máy chủ giám sát trung tâm, nơi tiếp nhận, phân tích và xử lý các Trap này để hiển thị cảnh báo, ghi log hoặc kích hoạt các kịch bản xử lý tự động. Phương pháp này đặc biệt phù hợp trong các hệ thống lớn hoặc đa nền tảng, nơi không thể triển khai Agent cho tất cả thiết bị hoặc máy chủ.

Cấu trúc và luồng hoạt động của mô hình này được thể hiện rõ trong *Hình 2.7*, minh họa quá trình máy chủ gửi các bản tin SNMP Trap về hệ thống giám sát trung tâm để đảm bảo khả năng phản ứng nhanh chóng và hiệu quả với các sự cố xảy ra trong hệ thống.



Hình 2. 7: Giám sát qua giao thức SNMP

Trong quản lý hạ tầng công nghệ thông tin hiện đại, việc giám sát các thiết bị mạng đóng vai trò then chốt nhằm đảm bảo kết nối luôn ổn định, liên tục và an toàn. Các thiết bị như router, switch hay firewall là mắt xích quan trọng trong hệ thống mạng, do đó cần được theo dõi liên tục để kịp thời phát hiện và xử lý

sự cố. Giải pháp giám sát của Polestar được thiết kế để đáp ứng yêu cầu này một cách hiệu quả, thông qua việc sử dụng các giao thức tiêu chuẩn như SNMP, RMON1&2, ICMP Ping và SNMP Trap. Các giao thức này cho phép thu thập dữ liệu chi tiết từ thiết bị mạng, phục vụ cho việc phân tích hiệu suất và cảnh báo sự cố.

Những thông số được Polestar giám sát bao gồm băng thông cổng (Interface), mức sử dụng CPU, bộ nhớ (Memory), điện áp (Voltage), nhiệt độ (Temperature), tình trạng quạt làm mát (Fan) và nguồn điện (Power). Nhờ vậy, quản trị viên có thể nắm bắt toàn diện tình trạng hoạt động của hệ thống mạng, từ đó đưa ra các quyết định điều chỉnh, bảo trì hoặc xử lý kịp thời.

Ngoài ra, hệ thống còn hỗ trợ đa dạng các nền tảng thiết bị mạng phổ biến như Cisco, Juniper, cũng như các thiết bị khác có hỗ trợ giao thức SNMP và RMON, giúp đảm bảo khả năng tích hợp linh hoạt, mở rộng và giám sát toàn diện trong mọi môi trường mạng.

Trong hệ thống CNTT phức tạp, cơ sở dữ liệu (CSDL) đóng vai trò trung tâm trong việc lưu trữ và xử lý thông tin, hỗ trợ các ứng dụng và dịch vụ vận hành mượt mà. Tuy nhiên, các vấn đề về hiệu năng như nghẽn tài nguyên, phiên chờ lâu, hay lỗi kết nối có thể gây ảnh hưởng nghiêm trọng đến hoạt động của toàn hệ thống. Vì vậy, giám sát hiệu năng CSDL là yếu tố thiết yếu để đảm bảo dữ liệu được truy xuất nhanh chóng và hệ thống hoạt động ổn định. Polestar cung cấp các giải pháp giám sát toàn diện, từ thu thập thông tin thông qua tài khoản quản trị riêng cho đến thiết lập các tác vụ tự động trên máy chủ. Trong phần này, chúng ta sẽ tìm hiểu cách Polestar hỗ trợ giám sát hiệu quả các loại CSDL như Oracle và MS SQL, bao gồm các chỉ số quan trọng như Wait Session, Job Queue, và Tablespace, nhằm kịp thời phát hiện và xử lý các vấn đề tiềm ẩn.

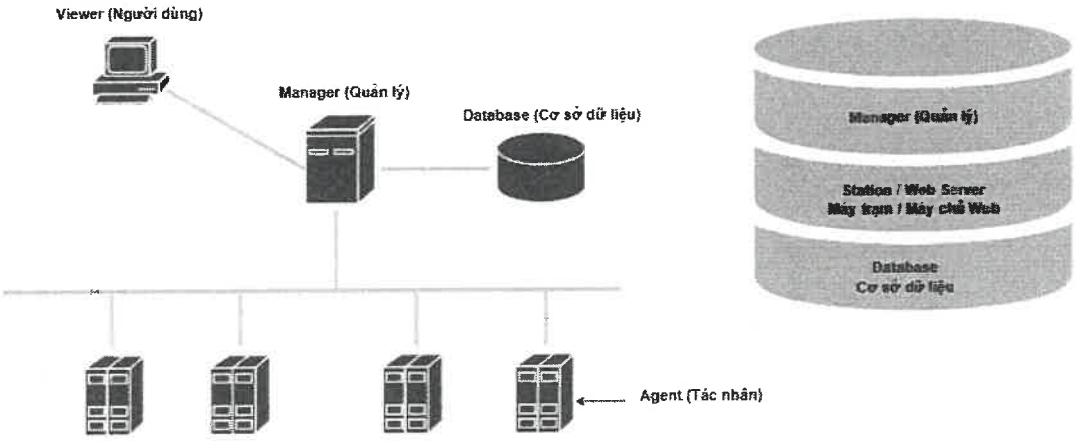
Hệ thống Polestar cung cấp khả năng giám sát cơ sở dữ liệu (CSDL) thông qua nhiều phương pháp linh hoạt, phù hợp với từng môi trường triển khai cụ thể. Một trong những cách phổ biến là sử dụng tài khoản truy vấn riêng biệt, cho phép hệ thống kết nối trực tiếp vào CSDL để thu thập thông tin cần thiết. Ngoài

ra, người quản trị cũng có thể thiết lập các Job chạy tự động từ máy chủ đã cài đặt Agent, nhằm giám sát các chỉ số quan trọng của hệ thống cơ sở dữ liệu theo lịch trình định sẵn.

Polestar hỗ trợ giám sát nhiều loại cơ sở dữ liệu phổ biến như Oracle, MS SQL và các hệ quản trị cơ sở dữ liệu khác, đảm bảo tính tương thích và khả năng mở rộng linh hoạt. Các thông tin được giám sát bao gồm: User process, Wait session, Server process, Job queue, Dispatchers, Tablespace và Redolog Buffer. Việc theo dõi các chỉ số này giúp quản trị viên nhanh chóng phát hiện những bất thường, xử lý kịp thời các vấn đề tiềm ẩn và tối ưu hiệu suất hoạt động của hệ thống 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*.

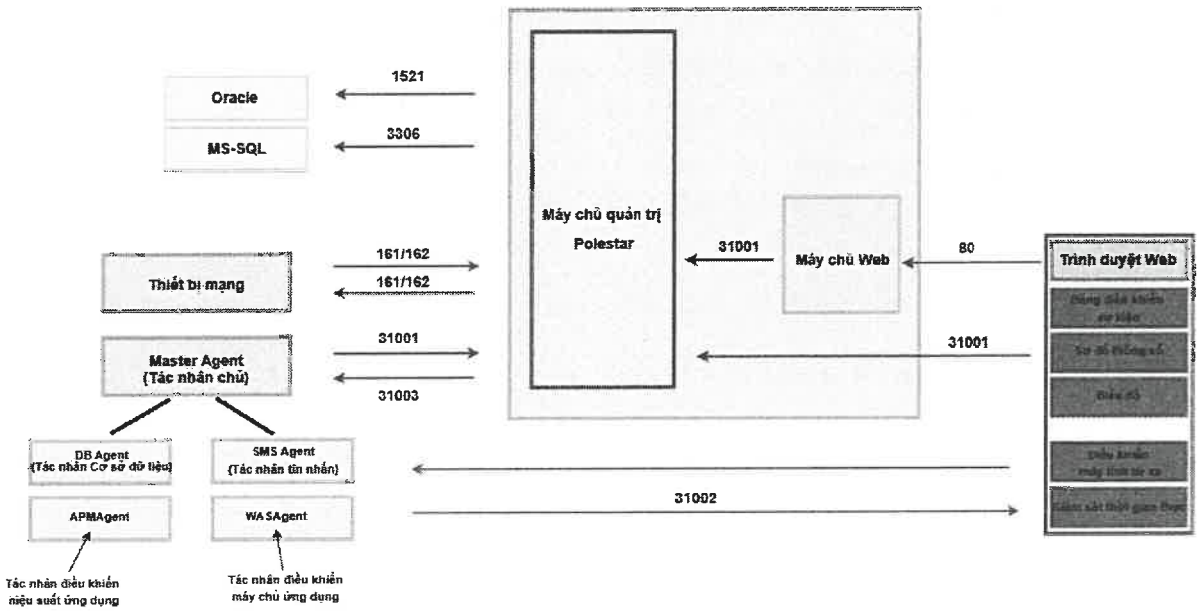


Hình 2. 8: Mô hình hệ thống giám sát sử dụng Polestar

Agent của Polestar được cài đặt trên đối tượng (Server, Database, thiết bị mạng) cần giám sát như *Hình 2.8*. Nó có nhiệm vụ thu thập dữ liệu thô, thực hiện chức năng tự động Recovery trong trường hợp có lỗi xảy ra trên đối tượng chịu giám sát.

- Cổng giao tiếp của Polestar

Polestar giao tiếp với các đối tượng giám sát thông qua các Ports, các Ports này được mô tả như *Hình 2.9* dưới đây:



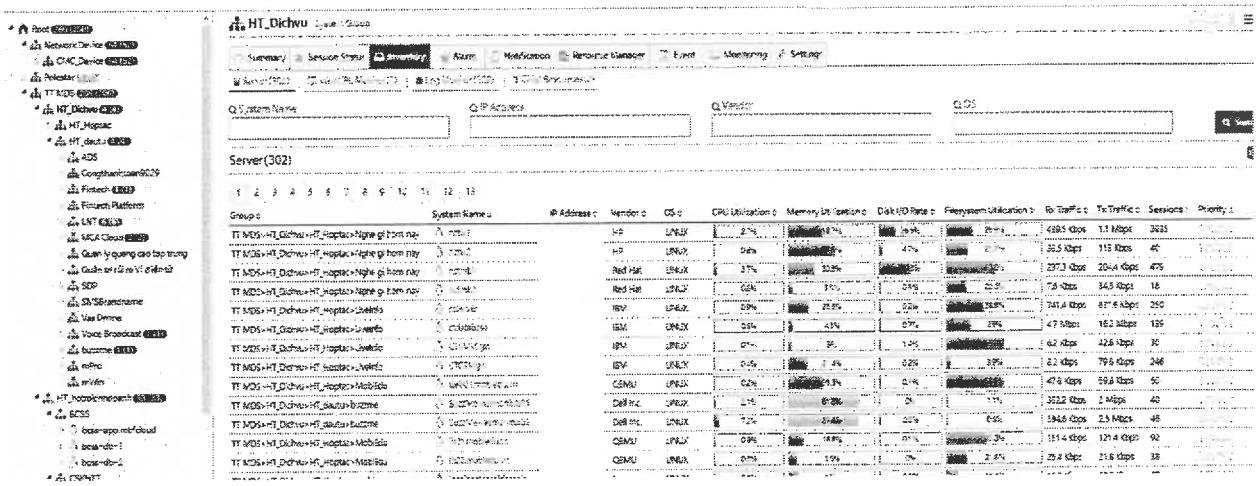
Hình 2. 9: Cổng giao tiếp của Polestar

– Đối tượng giám sát

Trong bất kỳ hệ thống quản lý mạng nào, việc xác định rõ các đối tượng cần giám sát là bước nền tảng để đảm bảo hiệu quả trong theo dõi và vận hành. Đối tượng giám sát không chỉ giới hạn ở các máy chủ, thiết bị mạng mà còn bao gồm cả cơ sở dữ liệu và các ứng dụng quan trọng. Mỗi loại đối tượng có các đặc điểm và yêu cầu giám sát riêng, đòi hỏi công cụ giám sát phải linh hoạt và đa năng. Với Polestar, việc theo dõi không chỉ tập trung vào hiệu năng của các thiết bị mà còn bao gồm thông tin trạng thái, kết nối, và các yếu tố vận hành khác. Phần này sẽ đi sâu vào cách Polestar phân loại và quản lý các đối tượng giám sát, từ máy chủ, thiết bị mạng đến các ứng dụng và dịch vụ, giúp đảm bảo toàn bộ hệ thống hoạt động ổn định và an toàn.

– Nhóm Server

Các Agent của Polestar được cài đặt trên các máy chủ Server nhằm theo dõi về hiệu năng, tình trạng hoạt động của chúng như *Hình 2.10*.



Hình 2. 10: Giao diện nhóm Server được giám sát cảnh báo Polestar

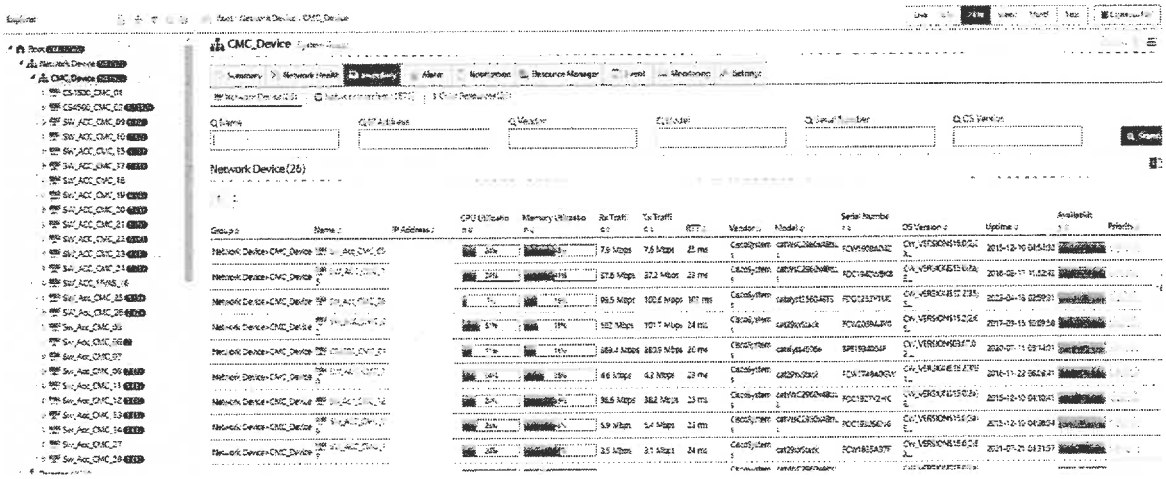
– Nhóm Network Device

Nhóm Network Device trong hệ thống giám sát Polestar bao gồm các thiết bị mạng như router, switch và các thiết bị tương tự, được giám sát thông qua giao thức chuẩn SNMP. Việc giám sát các thiết bị này đóng vai trò quan trọng trong việc đảm bảo tính ổn định, hiệu quả và bảo mật của hệ thống mạng.

Trên giải pháp Polestar, các thông tin được thu thập và giám sát bao gồm:

+ Hiệu suất hoạt động của CPU và bộ nhớ (Memory) của thiết bị, giúp đánh giá mức độ sử dụng tài nguyên và phát hiện sớm tình trạng quá tải.
+ Thông tin các cổng mạng (Network Interface) như trạng thái hoạt động (Up/Down), tốc độ truyền và nhận gói tin, tỉ lệ mất gói, từ đó hỗ trợ kiểm soát lưu lượng và chất lượng kết nối mạng.
+ Thông tin kết nối (Connection) giữa các thiết bị, phục vụ cho việc phân tích tuyến đường và xác định điểm nghẽn trong hệ thống.
+ Thông tin phần cứng của thiết bị như nhà sản xuất (Vendor), model, và số seri (Serial Number), giúp quản lý tài sản mạng và hỗ trợ bảo trì.

Việc giám sát đầy đủ và chi tiết các thông số này giúp quản trị viên nắm bắt kịp thời tình trạng thiết bị mạng, từ đó chủ động xử lý sự cố, tối ưu hiệu suất và nâng cao độ tin cậy của toàn bộ hệ thống mạng.



Hình 2. 11: Giao diện nhóm Network Device được giám sát cảnh báo Polestar

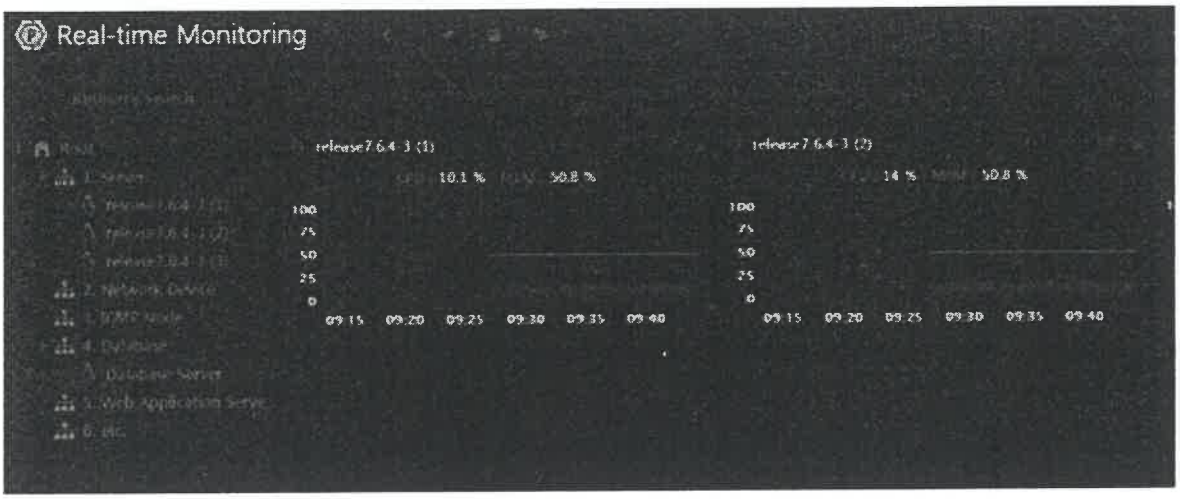
2.3.4. Các chức năng giám sát chính

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.



Hình 2. 12: Giao diện giám sát Real-time Monitoring của hệ thống Polestar

Cách chọn tài nguyên cần giám sát: Trong khu vực tìm kiếm tài nguyên bên trái của bảng điều khiển, kéo máy chủ mục tiêu hoặc nhóm hệ thống mà máy chủ thuộc về, vào khu vực bảng điều khiển, và tài nguyên máy chủ mục tiêu sẽ xuất hiện dưới dạng ô trên bảng điều khiển.

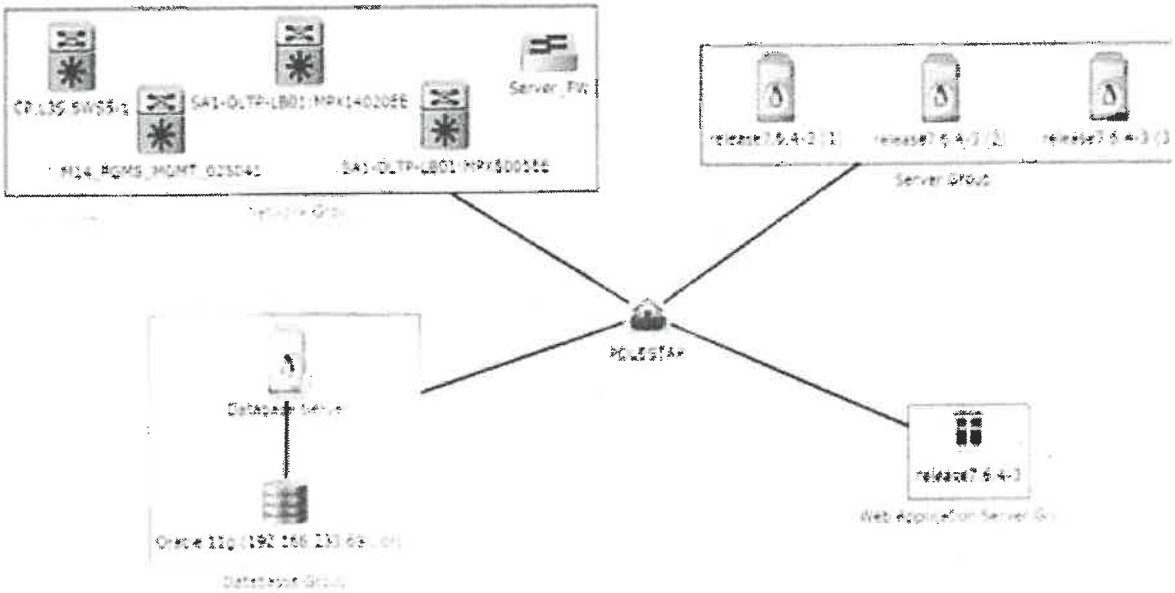
Thay đổi vị trí ô trên bảng điều khiển bằng cách nhấp vào biểu tượng ở góc trên bên phải của bảng điều khiển.

Các tài nguyên được tìm kiếm thường xuyên có thể được lưu bằng chức năng Lưu tài nguyên. Một danh sách các tài nguyên đã lưu có thể được tải lên bằng chức năng Nhập. Danh sách các tài nguyên và cài đặt bố cục có thể được lưu.

– **Topology Map**

POLESTAR cung cấp chức năng bản đồ hình thái học (Topology Map) từ đó người dùng có thể nhận thông tin về các kết nối của các tài nguyên đã tích hợp trong hệ thống. Người dùng có thể tạo ra bất kỳ số lượng bản đồ hình thái học nào mà họ mong muốn với mỗi tài khoản và chỉnh sửa các bản đồ hình thái học đã tạo ra. Sau khi tạo ra một bản đồ hình thái học như *Hình 2. 13* và thêm các tài nguyên, người dùng cũng có thể nhận thông tin về các kết nối giữa các

nút mới được tạo ra bằng cách thêm các liên kết nút cá nhân. POLESTAR cũng cung cấp một menu ngữ cảnh để tìm kiếm thông tin chi tiết về tài nguyên và thông tin Ping/Traceroute, thiết lập và tìm kiếm một bản đồ thấp hơn, truy cập HTTP/HTTPS, thêm các nút giả, kết nối thông tin về liên kết tài nguyên, và cung cấp một công cụ chỉnh sửa hình dạng liên kết. Các bản đồ hình thái học được tạo ra được quản lý theo từng người dùng và có thể được chia sẻ với người dùng khác.



Hình 2. 13: Giao diện nhóm Topology map của hệ thống Polestar

Để nhận thông tin về một bản đồ hình thái học, chọn menu Bản đồ Topology từ menu chính ở bên trái của cửa sổ. POLESTAR Topology Map cung cấp một Bản đồ Hệ thống có thể truy cập được cho tất cả người dùng, mà người dùng có thể thêm khi cần thiết. Tất cả người dùng có thể truy cập vào Bản đồ Hệ thống nhưng chỉ có người dùng quản trị có quyền được phép chỉnh sửa bản đồ. Đối với các tài khoản mới được thêm, Bản đồ Hệ thống mặc định sẽ được hiển thị trong cửa sổ bản đồ hình thái học. Nếu người dùng có nhiều bản đồ hình thái học, bản đồ hình thái học có ưu tiên cao nhất sẽ được hiển thị làm bản đồ mặc định. Bản đồ hình thái học được tìm kiếm gần đây nhất sẽ được hiển thị cho đến khi người dùng đăng xuất hoặc đóng trình duyệt. Bản đồ hình thái học có ưu

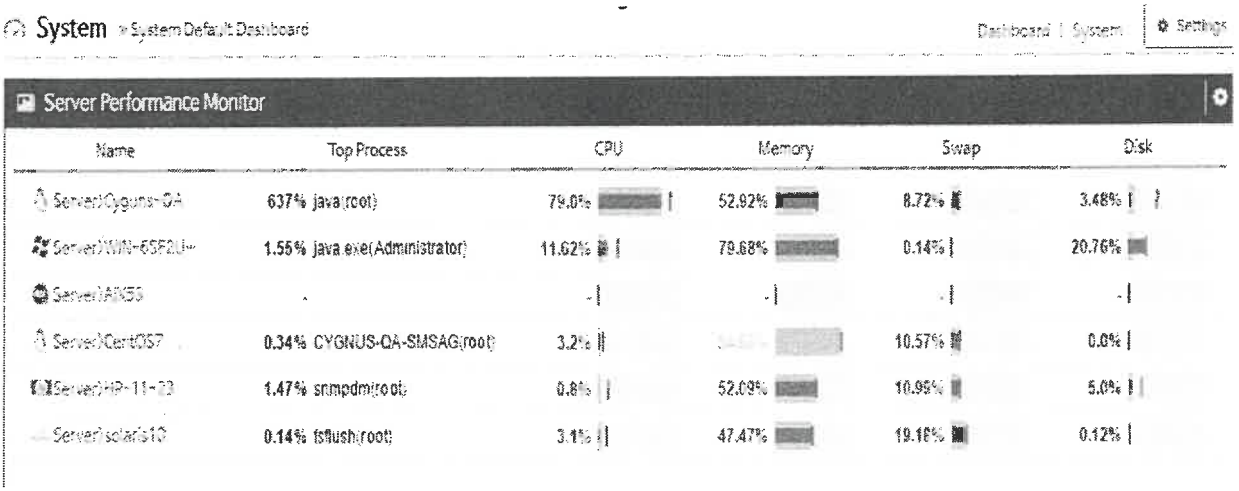
tiên cao nhất sẽ được hiển thị làm bản đồ mặc định trong cửa sổ Bản đồ Topology. Nếu có nhiều bản đồ có cùng ưu tiên cao, bản đồ đầu tiên trong số các liên kết đã đánh dấu sẽ trở thành bản đồ mặc định. Để thiết lập bản đồ hình thái học mặc định, hãy thiết lập bản đồ mặc định mong muốn có ưu tiên cao nhất

– **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.

Người dùng có thể tạo ra nhiều bảng điều khiển trên tài khoản của họ và chia sẻ các bảng điều khiển của họ với người dùng khác. Người dùng có thể quản lý các bảng điều khiển của mình bằng cách đặt thứ tự ưu tiên mong muốn và kiểm tra độ phổ biến của các bảng điều khiển được chia sẻ bằng tần suất chia sẻ của chúng như *Hình 2.14.*

Các thiết bị trên bảng điều khiển có thể được thêm, sửa đổi và/hoặc xóa một cách mạch lạc cũng như được sắp xếp theo ý thích của người dùng bằng cách di chuyển các thiết bị và thay đổi bố cục.

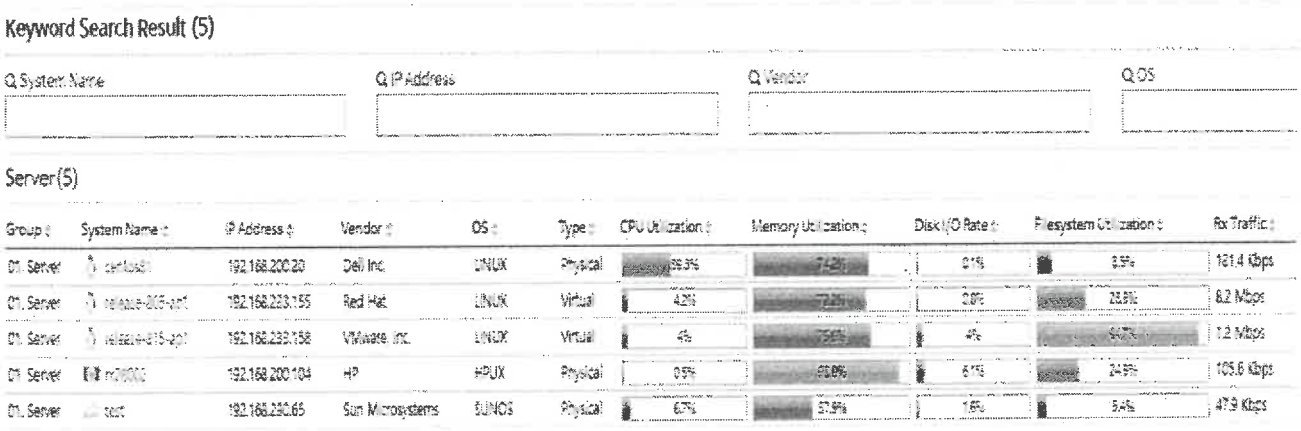


Hình 2. 14: Giao diện màn hình System Dashboard của hệ thống Polestar

– **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 … Qua đó người dùng có thể theo dõi và so sánh sự thực thi giữa các máy chủ trong hệ thống tại cùng một thời điểm như *Hình 2.15*.

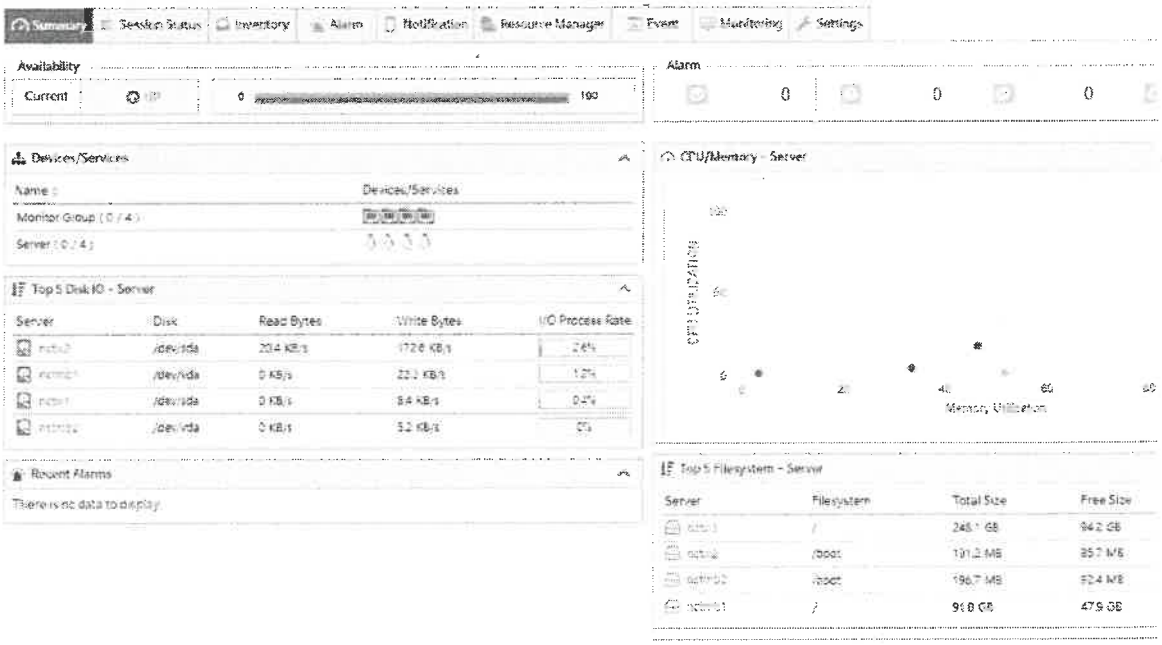


Hình 2. 15: Giao diện màn hình quản lý của hệ thống Polestar

+ Polestar cho phép tìm kiếm và hiển thị các thông tin về máy chủ theo các điều kiện như: hiển thị theo nhóm thiết bị "Group"; theo IP và hostname; theo loại thiết bị và có thể thiết lập thời gian quét theo ý muốn.
+ Danh sách các máy chủ và các thông tin chỉ số được hiển thị với các màu sắc khác nhau thể hiện tình trạng hoạt động, hoặc các cấp độ lỗi.
+ Các biểu đồ thể hiện phân loại các chỉ số như CPU, bộ nhớ, hệ thống file đĩa của từng máy chủ. Với hình ảnh trực quan dạng biểu đồ thể hiện trạng thái như thực thi giúp người quản trị dễ dàng so sánh các thông số với nhau của máy chỉ. Để xem thông tin chi tiết của từng chỉ số người dùng nhấn chuột vào biểu tượng kính lúp trên từng sơ đồ.

Hình 2. 16: Giao diện thông số Performance của hệ thống được giám sát bởi Polestar

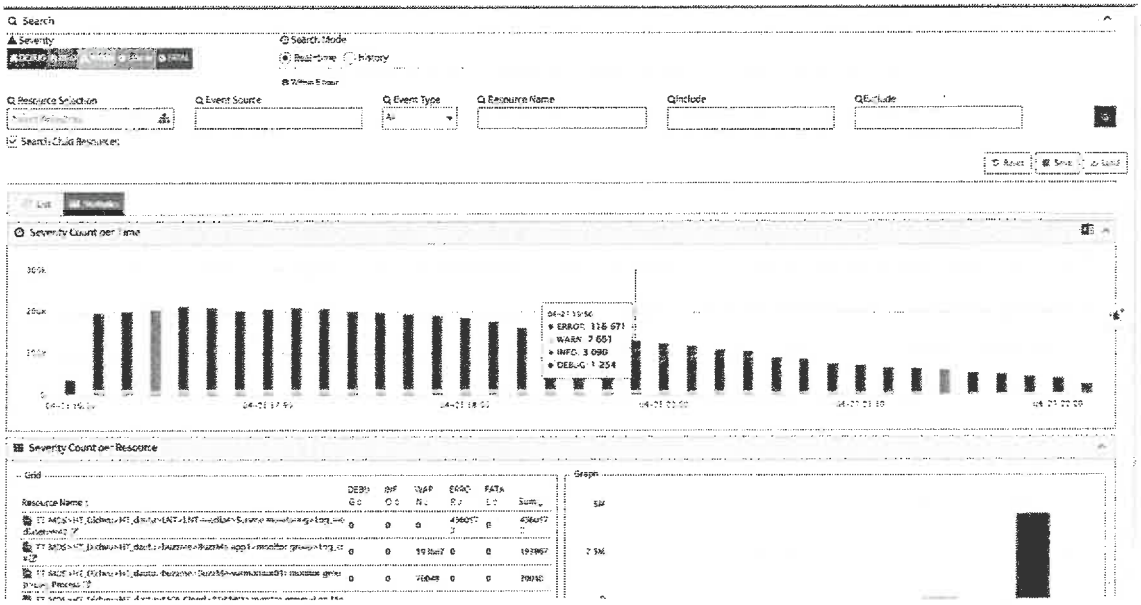
Summary: Những thông số cơ bản của từng máy chủ thể hiện trực quan qua các sơ đồ và thông tin con cấu thành như *Hình 2.17*.



Hình 2. 17: Giao diện Dashboard của thiết bị được giám sát bởi Polestar

– **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).



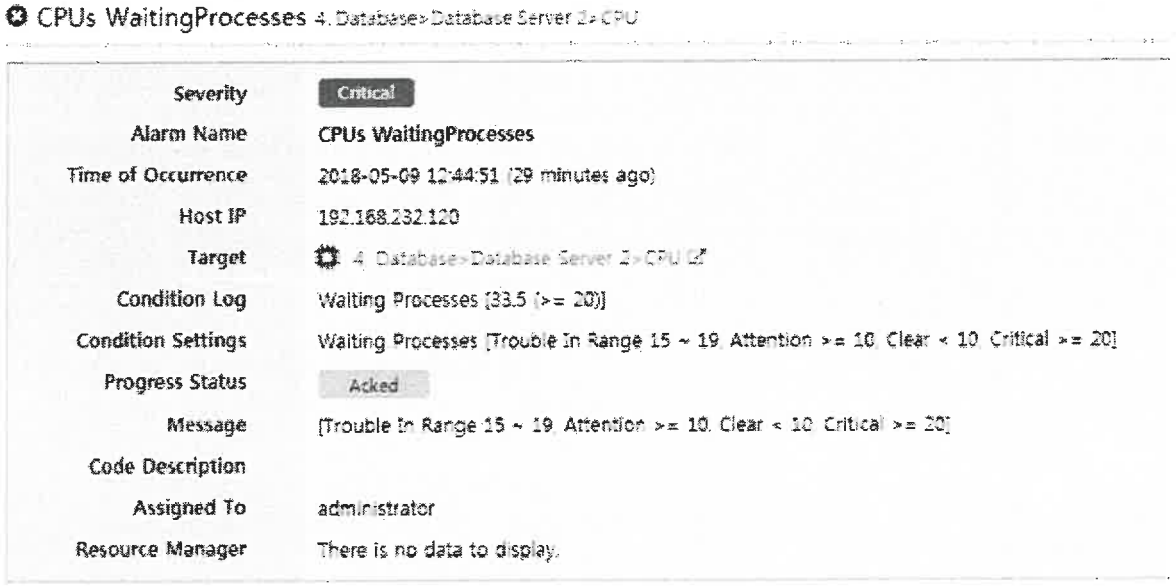
Hình 2. 18: Giao diện chức năng Review Event của hệ thống Polestar

– **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

Khi một cảnh báo được nhấp vào, chi tiết của cảnh báo sẽ được hiển thị. Các chi tiết này bao gồm xác nhận cá nhân, tùy chọn xóa cảnh báo, và hiển thị toàn bộ danh sách cảnh báo bên trái, để người dùng có thể xem các cảnh báo khác. Người dùng có thể kiểm tra thông tin cơ bản của cảnh báo với các tab như Condition Log, Alarm Notes, Notification Log, Trigger Action Log, Alarm History, Alarm Definition, Knowledge Database, Associated Resource, Custom Property trong cửa sổ chi tiết của cảnh báo như *Hình 2.20*.



Hình 2. 20: Giao diện chi tiết cảnh bảo 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

Để lựa chọn được giải pháp giám sát mạng phù hợp với đặc thù hệ thống và yêu cầu vận hành của tổ chức, cần có cái nhìn tổng quan về các công cụ phổ

biến hiện nay, từ góc độ kiến trúc, khả năng mở rộng, tính linh hoạt đến mức độ dễ sử dụng và hiệu quả cảnh báo. Trong phần này tôi đã tiến hành phân tích, so sánh các giải pháp giám sát mạng tiêu biểu như Nagios, Zabbix, PRTG Network Monitor và Polestar. Các tiêu chí được lựa chọn đánh giá đều xuất phát từ yêu cầu thực tiễn trong quá trình quản trị hệ thống mạng doanh nghiệp. *Bảng 2.1* trình bày tổng quan các tiêu chí kỹ thuật quan trọng và mức độ đáp ứng của từng giải pháp, làm cơ sở để phân tích ưu – nhược điểm và khả năng ứng dụng trong các mô hình hạ tầng khác nhau.

Bảng 2.1 So sánh tổng quan các giải pháp giám sát mạng

STT	Tiêu chí đánh giá	Nagios	Zabbix	PTRG Network Monitor	Polestar
1	**Loại phần mềm**	Mã nguồn mở	Mã nguồn mở	Thương mại (có bản miễn phí giới hạn)	Thương mại
2	**Khả năng mở rộng**	Trung bình (tùy thuộc cấu hình plugin)	Cao	Trung bình (giới hạn trong môi trường lớn)	Cao (hỗ trợ mạng quy mô lớn)
3	**Hỗ trợ giao thức giám sát**	SNMP, ICMP, HTTP, plugin	SNMP, JMX, IPMI, SSH, Telnet	SNMP, WMI, NetFlow, Packet Sniffing	SNMP, Agent, RMON, Trap
4	**Dễ sử dụng và cấu hình ban đầu**	Khó (yêu cầu kiến thức cấu hình)	Trung bình (đòi hỏi học tập ban đầu)	Dễ (giao diện thân thiện, hướng dẫn rõ ràng)	Trung bình (cần đào tạo ban đầu)
5	**Khả năng cảnh báo và gửi thông báo**	Tốt (email, SMS qua cấu hình plugin)	Rất tốt (linh hoạt theo kịch bản và ngưỡng)	Tốt (tùy chỉnh alert dễ dàng)	Xuất sắc (cảnh báo theo logic nghiệp vụ và AI)
6	**Phân quyền người dùng**	Cơ bản	Tốt (hỗ trợ theo nhóm)	Cơ bản	Rất tốt (chi tiết theo vai trò)
7	**Hiển thị trực quan và dashboard**	Đơn giản (ít đồ hoạ)	Tốt (có biểu đồ và báo cáo linh hoạt)	Xuất sắc (đồ họa đẹp, biểu đồ chi tiết)	Rất tốt (hỗ trợ Topology Map, System Map)

8	**Tính năng phân tích & dự đoán (AI/ML)**	Không hỗ trợ	Không hỗ trợ	Không hỗ trợ	Có (dự báo hiệu năng, xu hướng sự cố với AI)
9	**Khả năng tích hợp hệ thống khác**	Cao (nhiều plugin)	Rất cao (API mạnh mẽ, hỗ trợ DevOps)	Trung bình (có API riêng nhưng bị giới hạn)	Tốt (hỗ trợ API và tích hợp dữ liệu từ nhiều nguồn)
10	**Tính bảo mật và kiểm soát truy cập**	Cơ bản	Cao (2FA, phân quyền chi tiết)	Trung bình	Cao (xác thực nhiều lớp, nhật ký truy cập đầy đủ)
11	**Chi phí triển khai và vận hành**	Thấp (miễn phí)	Thấp (miễn phí, trừ chi phí hạ tầng)	Trung bình – cao (phiên bản trả phí theo số lượng sensor)	Cao (phù hợp doanh nghiệp lớn, cần đầu tư ban đầu)
12	**Phù hợp với quy mô tổ chức**	Nhỏ - Trung bình	Trung bình - Lớn	Nhỏ - Trung bình	Trung bình - Lớn (đặc biệt thích hợp doanh nghiệp viễn thông)
13	**Khả năng giám sát đa nền tảng**	Có (qua plugin)	Có (đa dạng agent và tích hợp cloud)	Có (nhưng giới hạn ở cloud phức tạp)	Có (đa hệ điều hành, cloud, hybrid và thiết bị mạng)

Từ bảng so sánh tổng quan các giải pháp giám sát mạng, có thể rút ra một số kết luận quan trọng nhằm định hướng lựa chọn phù hợp với từng mô hình và nhu cầu sử dụng. Trong đó, **Polestar** nổi bật với khả năng giám sát thông minh, tích hợp các tính năng phân tích và dự đoán nhờ ứng dụng trí tuệ nhân tạo (AI), đồng thời có thể triển khai hiệu quả trong các hệ thống mạng lớn và phức tạp. **Zabbix** là giải pháp phù hợp cho các doanh nghiệp có đội ngũ kỹ thuật chuyên sâu, với yêu cầu cao về khả năng tùy biến, linh hoạt trong cấu hình và mở rộng. Trong khi đó, **Nagios** là lựa chọn lý tưởng cho những tổ chức có ngân sách hạn chế, phù hợp với hệ thống quy mô nhỏ; tuy nhiên, việc triển khai và vận hành đòi hỏi người dùng phải có kiến thức kỹ thuật vững vàng. Cuối cùng, **PRTG**

đáp ứng tốt nhu cầu của các doanh nghiệp vừa và nhỏ nhờ khả năng triển khai nhanh, giao diện trực quan và dễ sử dụng, nhưng lại gặp hạn chế nhất định khi mở rộng quy mô giám sát lên mức cao hơn.

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.

Từ việc nghiên cứu sâu giải pháp Polestar và phân tích so sánh tổng quan với các công cụ giám sát phổ biến hiện nay như Nagios, Zabbix, PRTG Network Monitor, có thể thấy rằng Polestar nổi bật nhờ khả năng giám sát toàn diện, linh hoạt và thông minh hơn. Hệ thống được thiết kế với kiến trúc tập trung, hỗ trợ đa giao thức (SNMP, RMON, Trap, Agent), có thể giám sát đồng thời nhiều đối tượng hạ tầng như máy chủ, thiết bị mạng, cơ sở dữ liệu và dịch vụ ứng dụng.

Đặc biệt, Polestar tích hợp các tính năng hiện đại như giám sát theo thời gian thực, phân tích hiệu năng, cảnh báo theo ngưỡng linh hoạt, hiển thị dữ liệu trực quan trên Topology Map và Dashboard hệ thống. Việc ứng dụng công nghệ AI trong phân tích xu hướng sự cố và tối ưu vận hành là một điểm mạnh vượt trội, giúp dự báo và ngăn ngừa sự cố hiệu quả – điều mà các giải pháp giám sát truyền thống còn hạn chế. Đồng thời, hệ thống hỗ trợ phân quyền chi tiết theo vai trò và tích hợp dễ dàng với các hạ tầng CNTT hiện hữu[3].

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 công nghệ thông tin phát triển mạnh mẽ và hệ thống hạ tầng ngày càng trở nên phức tạp, việc giám sát mạng đóng vai trò then chốt trong bảo đảm tính ổn định, an toàn và hiệu quả vận hành của toàn bộ hệ thống. Giám sát mạng không chỉ giúp quản trị viên nắm bắt chính xác và kịp thời các hoạt động đang diễn ra trong hệ thống, mà còn là cơ sở để lập kế hoạch sửa chữa, thay thế thiết bị một cách chủ động, tránh tình trạng hỏng hóc đột ngột gây gián đoạn dịch vụ.

Một trong những lợi ích thiết thực của giám sát là khả năng chẩn đoán nhanh các sự cố phát sinh, từ đó rút ngắn thời gian khắc phục và giảm thiểu tác động đến người dùng cuối. Đồng thời, hệ thống giám sát còn cung cấp báo cáo trực quan, rõ ràng, hỗ trợ việc theo dõi hiệu suất hoạt động và lập kế hoạch nâng cấp, mở rộng tài nguyên phù hợp. Việc giám sát liên tục các tài nguyên trong hệ thống như CPU, băng thông, bộ nhớ hay thiết bị mạng cũng là yếu tố quan trọng giúp duy trì hiệu suất tối ưu.

Ngoài ra, giám sát hạ tầng mạng còn góp phần đảm bảo hệ thống vận hành liên tục và ổn định, giảm thiểu thời gian chết và nâng cao trải nghiệm người dùng. Về lâu dài, việc triển khai hệ thống giám sát hiệu quả sẽ giúp tiết kiệm thời gian, chi phí vận hành, đồng thời nâng cao hiệu quả quản lý và bảo trì hệ thống CNTT trong tổ chức.

Trung tâm Dịch vụ số Mobifone hoạt động trong lĩnh vực viễn thông – công nghệ thông tin. Do đó công ty có các máy chủ chứa nhiều thông tin quan trọng về khách hàng cũng như các số liệu tài chính. Cùng với sự đòi hỏi lớn hơn về băng thông mạng các thiết bị, máy chủ chứa các dữ liệu và tài nguyên này yêu cầu cần được giám sát tình trạng mạng sử dụng một cách chặt chẽ và cần thiết.

Ngoài sự hỗ trợ của hệ thống bảo vệ mạng như tường lửa thì vai trò của người quản trị viên cũng hết sức quan trọng. Tuy nhiên không phải lúc nào người quản trị cũng có thể nắm bắt được hết tình trạng của hệ thống, khi có hệ thống bị sự cố rồi thì quản trị viên mới bắt đầu dò tìm nguyên nhân và khắc phục sự cố. Hoặc khi cấp trên yêu cầu báo cáo tình trạng hệ thống hằng ngày, hằng tuần thì công việc đó cũng làm người quản trị mất rất nhiều công sức để thực hiện. Nhưng hiệu quả đem lại thực sự chưa cao, thông tin hệ thống đáp ứng chưa đủ. Hiện nay có rất nhiều phần mềm quản lý hệ thống tài nguyên mạng sử dụng các thiết bị phần cứng đắt tiền. Tuy nhiên một số phần mềm cũng đáp ứng một cách toàn diện với nhiều tính năng vượt trội.

Xuất phát từ những nhu cầu trên, vậy nên xây dựng một hệ thống giám sát mạng là điều hết sức cần thiết.

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

Trước thực trạng hệ thống giám sát tại Trung tâm Dịch vụ số MobiFone còn tồn tại nhiều bất cập như thiếu tính đồng bộ, khó tích hợp, giao diện phân tán và đòi hỏi vận hành độc lập giữa các nền tảng Prometheus và SolarWinds, nhu cầu cấp thiết đặt ra là phải xây dựng một giải pháp giám sát hợp nhất, thông minh và linh hoạt hơn. Việc lựa chọn giải pháp Polestar trong đề án này xuất phát từ khả năng đáp ứng toàn diện những yêu cầu kỹ thuật cũng như nhu cầu vận hành thực tế của Trung tâm.

Polestar mang lại nhiều lợi ích nổi bật. Trước hết, đây là một nền tảng giám sát toàn diện, cho phép hợp nhất việc theo dõi tất cả các thành phần trong hạ tầng CNTT – từ máy chủ, thiết bị mạng, cơ sở dữ liệu cho đến các ứng dụng và dịch vụ – trong một giao diện quản trị duy nhất. Điều này giúp loại bỏ tình trạng rời rạc giữa các công cụ giám sát hiện tại, tránh phân mảnh dữ liệu và giảm thiểu thời gian xử lý khi sự cố xảy ra. Việc giám sát tập trung cũng tạo điều kiện để quản trị viên nắm bắt toàn cảnh hệ thống một cách chủ động và kịp thời.

Bên cạnh đó, Polestar còn được tích hợp các công nghệ tiên tiến như trí tuệ nhân tạo (AI) và phân tích dữ liệu lớn (Big Data), giúp hệ thống không chỉ dừng lại ở việc phát hiện mà còn có khả năng dự báo sớm các rủi ro có thể xảy ra trong tương lai. Nhờ đó, đội ngũ vận hành có thể chủ động trong công tác bảo trì, phòng ngừa sự cố thay vì chỉ phản ứng bị động sau khi lỗi đã phát sinh như trước đây.

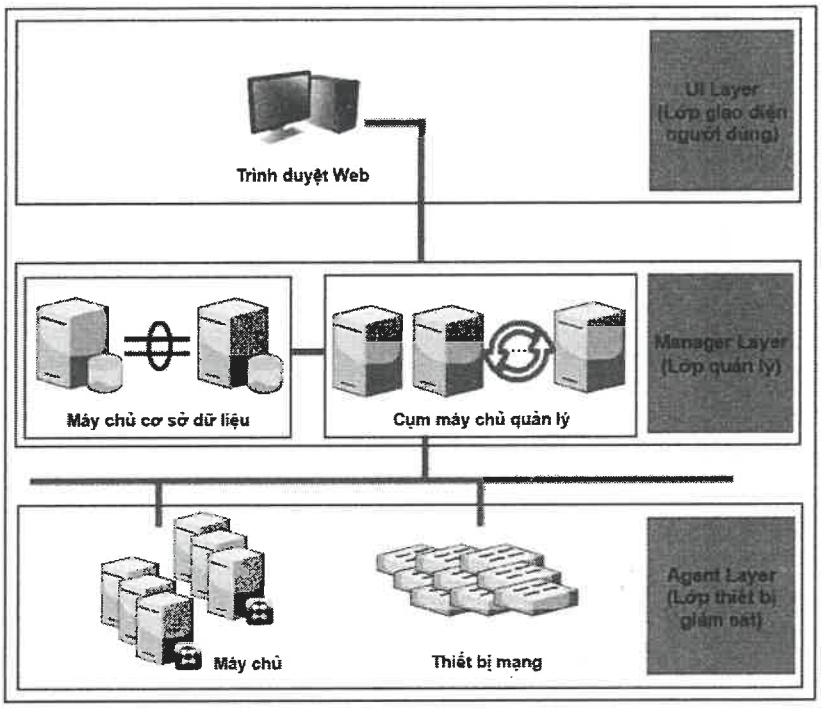
Về giao diện, Polestar sử dụng công nghệ HTML5 hiện đại, cung cấp hệ thống dashboard trực quan, bản đồ hình thái học (Topology Map), biểu đồ và bảng thông số dễ sử dụng, giúp quá trình giám sát trở nên trực quan, sinh động và dễ thao tác hơn với người dùng. Đây là điểm cộng lớn so với các hệ thống hiện tại còn phụ thuộc nhiều vào thao tác dòng lệnh hoặc giao diện phức tạp.

Ngoài ra, hệ thống Polestar hỗ trợ nhiều giao thức giám sát tiêu chuẩn như SNMP, RMON, ICMP, kết hợp cả giám sát qua agent và SNMP trap, nên có thể triển khai linh hoạt trên các loại thiết bị và hệ điều hành phổ biến như Linux, Windows, Solaris, AIX,... Đây là một yếu tố đảm bảo tính mở rộng, đáp ứng được sự phát triển dài hạn của Trung tâm Dịch vụ số trong tương lai [4].

Hơn thế nữa, Polestar còn cho phép thiết lập phân quyền truy cập theo vai trò người dùng một cách chi tiết, giúp kiểm soát quyền hạn một cách chặt chẽ, giảm thiểu rủi ro lạm quyền hoặc sai sót thao tác ngoài ý muốn. Đồng thời, việc triển khai một hệ thống giám sát duy nhất còn giúp tối ưu chi phí vận hành, tiết kiệm thời gian theo dõi thủ công, giảm áp lực cho đội ngũ kỹ thuật và hạn chế tổn thất do sự cố gián đoạn dịch vụ gây ra.

Tổng hợp lại, Polestar không chỉ giải quyết các vấn đề tồn tại của mô hình giám sát hiện tại mà còn mang đến một giải pháp đồng bộ, thông minh và bền vững. Việc triển khai giải pháp này là bước đi đúng đắn nhằm nâng cao hiệu quả quản trị hạ tầng CNTT, đồng thời phù hợp với định hướng chuyển đổi số toàn diện mà Trung tâm Dịch vụ số MobiFone đang hướng tới.

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

UI Layer (Lớp giao diện người dùng): Polestar cung cấp giao diện người dùng dựa trên web của công nghệ HTML5. Người dùng có thể sử dụng các chức năng của POLESTAR thông qua web mà không cần cài đặt ứng dụng riêng[3].

Manager Layer (Lớp quản lý) : Lớp quản lý bao gồm máy chủ DB và máy chủ AP trong đó POLESTAR được cài đặt để hoạt động. Máy chủ AP nhận yêu cầu của người dùng thông qua UI và mang thông tin từ kho lưu trữ dữ liệu và lớp tác nhân để cung cấp cho người dùng. Nó cũng thu thập thông tin từ lớp tác nhân theo chu kỳ thu thập xác định để xử lý thông tin về cấu hình và hiệu suất. Tải của máy chủ AP tăng tuyến tình với số lượng người dùng và thiết bị kiểm soát tăng lên. Việc kết hợp nhiều máy chủ AP trong các cụm cho phép xây dựng hệ thống có tính sẵn sàng cao cùng với sự phân tán tải. Ngoài ra, chế độ xem giống hệt nhau được hiển thị bất kể máy chủ AP nào người dùng truy cập.

Repository (DB): cơ sở dữ liệu chứa các thông tin giám sát để phục vụ phân tích, thống kê, báo cáo theo ý muốn. Đây cũng là nguồn dữ liệu quý giá hỗ trợ việc hoạch định đầu tư nâng cấp cơ sở hạ tầng sau này.

Agent layer : Là lớp thiết bị để giám sát, máy chủ phải được tải Agent POLESTAR và thiết bị mạng sẽ tiếp tục kích hoạt Agent SMNP. Các phiên bản SNMP được hỗ trợ Versionsarev1, v2c và v3 [4].

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
  - + Trạng thái hoạt động.
  - + Trạng thái hoạt động của các Interface.
- Giám sát việc sử dụng tài nguyên
  - + CPU: số lượng processes trong hàng đợi hay theo % sử dụng CPU của hệ thống.
  - + Ram: Cho biết dung lượng tổng, số lượng dung lượng sử dụng hay còn trống.
  - + Disk: Cho biết dung lượng tổng, còn trống và đã sử dụng.
- 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
  - + Lưu trữ các thông số trong 7 -> 30 ngày có thể xem lại và phục vụ cho công tác phân tích sau này.
  - + Biểu diễn theo danh sách hoặc biểu đồ trực quan các thông số về tình trạng tài nguyên của các thiết bị mạng.
- Cảnh báo

+ Cảnh báo trạng thái hoạt động: Ví dụ thiết bị mạng bị down hoặc sự cố bất thường.
+ Cảnh báo dịch vụ: Service bị tắt hay thay đổi trạng thái hoạt động.

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

Bảng 3.1: Thông tin kết nối đến hệ thống giám sát hạ tầng mạng Polestar

ĐỐI TƯỢNG	IP Nguồn (Polestar)	IP Đích	Mở Port và cung cấp thông tin
Server	10.10.1.97 10.10.1.98	Thiết bị cần giám sát	Port: 31001, 31002, 31003, TCP/UDP (2 chiều) Thực hiện login vào server để cài Agent
Network		Thiết bị cần giám sát	Port: 161/162 (TCP;UDP) Cung cấp snmp community string

Tích hợp máy Agent trên máy chủ Linux

– Kiểm tra thông tin OS và di chuyển tập cài đặt Agent cho máy chủ Linux vào thư mục cài đặt đã được tạo:

[root@Linux agent]# uname -a

Linux Linux 3.10.0-1127.10.1.el7.x86_64 #1 SMP Wed Jun 3 14:28:03 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux

– Giải nén tập bằng tar:

[root@Linux agent]#tar -zxvf NNPAgent_SMS_Linux64_3.4_7.6.18.tar

– Sẽ thấy tệp AgentInstall.sh và thư mục NNPAgent_SMS_Linux64_3.4_7.6.18.tar

[root@Linux agent]#ls

AgentInstall.sh NNPAgent

NNPAgent_SMS_Linux64_3.4_7.6.18.tar.

- Cài đặt Agent

[root@Linux agent]#./AgentInstall.sh -t 2

AGENT_ID = Linux_20200903100616

AGENT_PORT = 31003

agent conf file setup success!!

systemctl

auto start script add success.

[root@Linux agent]#

- Kiểm tra tiến trình SMS Agent

[root@PS-APES-HN01 agent]# ps -ef\|grep AGENT

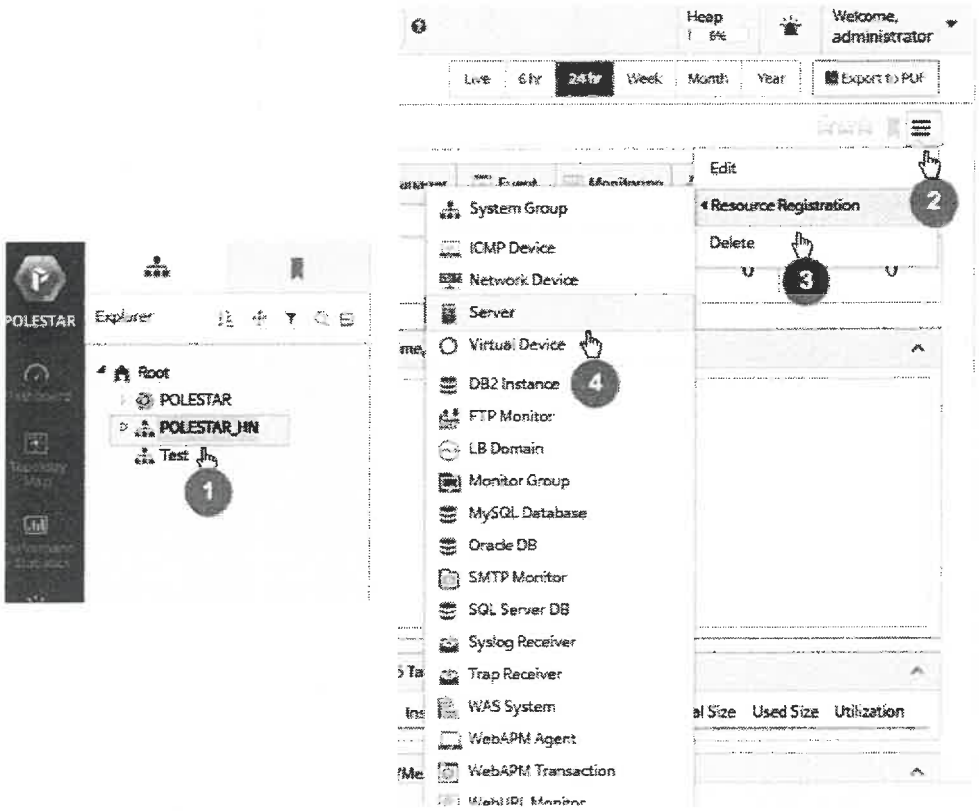
root 11836 9256 0 09:49 pts/2 00:00:00 grep --color=auto AGENT

root 24206 1 0 Sep02 ? 00:02:10 MAGENT7

root 24251 1 0 Sep02 ? 00:09:44 SMSAGENT7

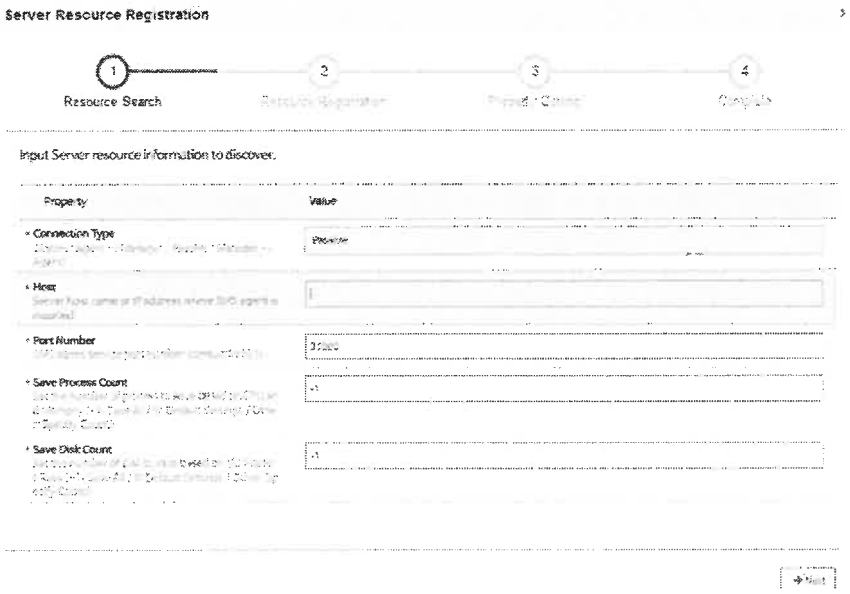
Thêm thiết bị trên giao diện người dùng

- Nhấp vào [Group_Name] và làm theo các bước như *Hình 3.2*



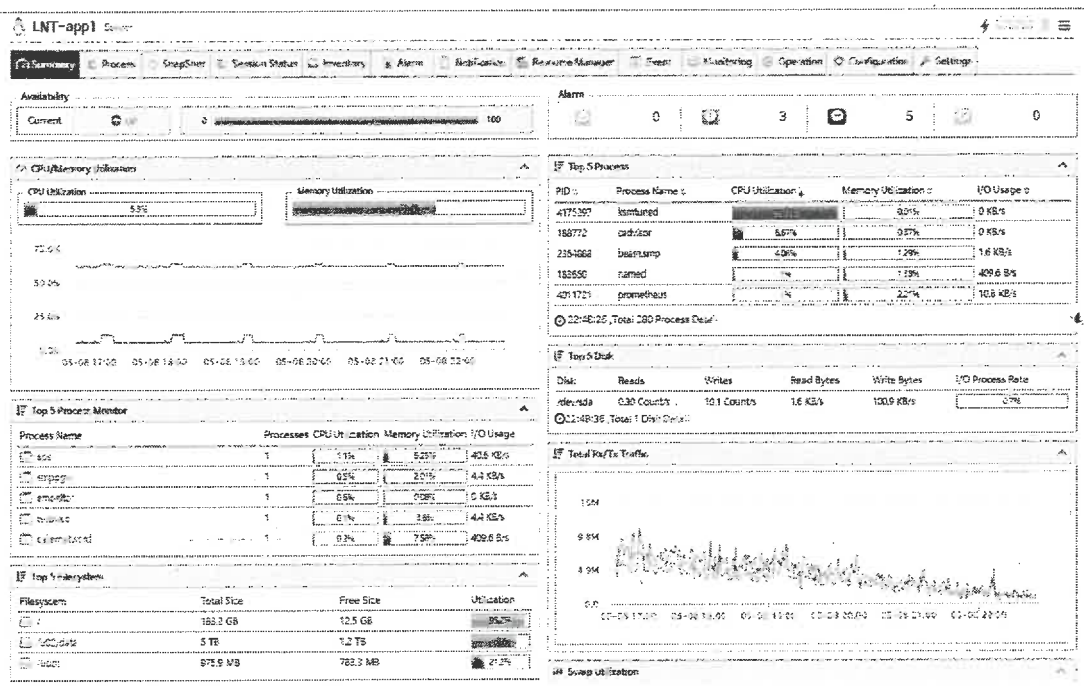
Hình 3. 2: Giao diện tích hợp thiết bị cần giám sát trên hệ thống Polestar

– Chuyển đến "*Host", điền thông tin IP máy chủ giám sát, sau đó nhấp vào "Next" khi hoàn tất như *Hình 3.3*.



Hình 3. 3: Giao diện thông tin chi tiết thiết bị cần giám sát hệ thống Polestar

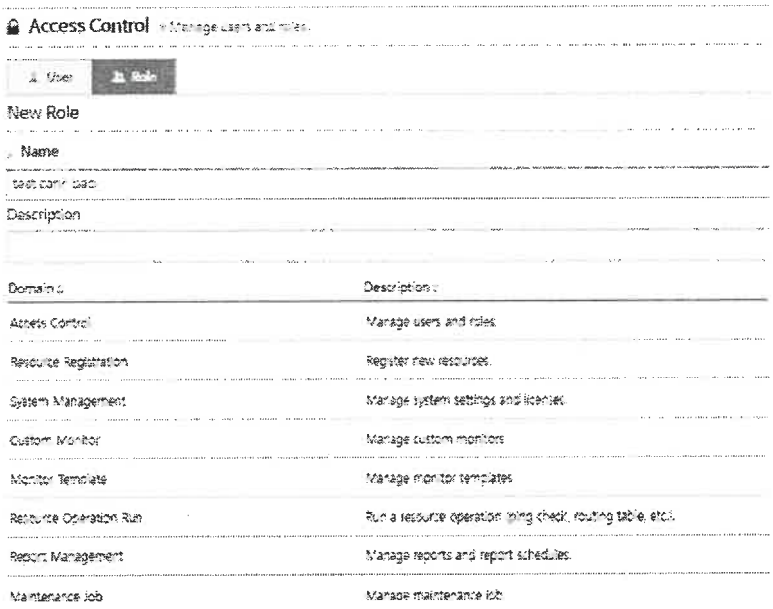
– Sau khi thêm thiết bị ta sẽ có thông tin thiết bị gồm các trường: Availability, CPU, Memory, Top 5 Disk IO, Top 5 Filesystem, Alarm, Information như *Hình 24*.



Hình 3. 4: Giao diện Dashboard thiết bị được tích hợp trên hệ thống Polestar

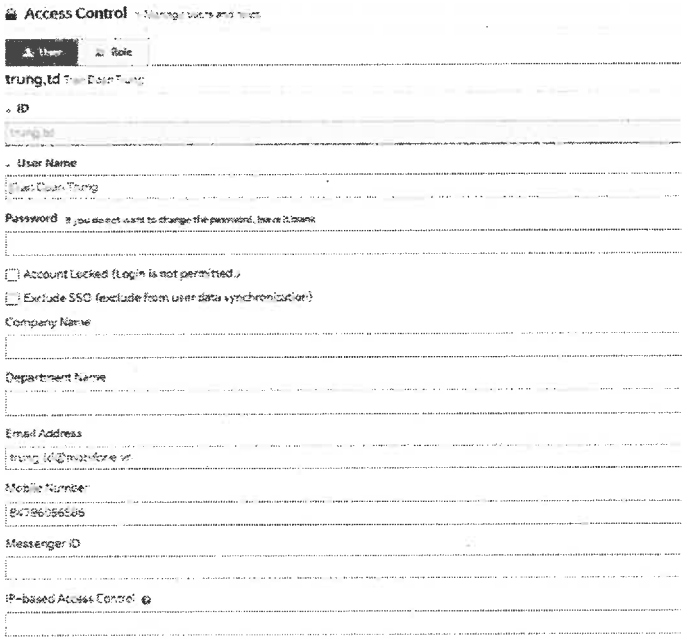
3.2.4. Thiết lập cảnh báo

Tạo Role người dùng, ở đây ta thực hiện tạo Role tại Tab Access Control – Mânge users and roles và điền các thông tin cần thiết như trong *Hình 3.5*.



Hình 3.5: Giao diện quyền người dùng trên hệ thống Polestar

Tạo tài khoản đầy đủ thông tin tại mục Access Control với đầy đủ các thông tin cơ bản (ID, Password, Company Name, Department Name, email address, Mobifone Number) như *Hình 3.6*.



Hình 3. 6: Giao diện thông tin chi tiết người dùng trên hệ thống Polestar

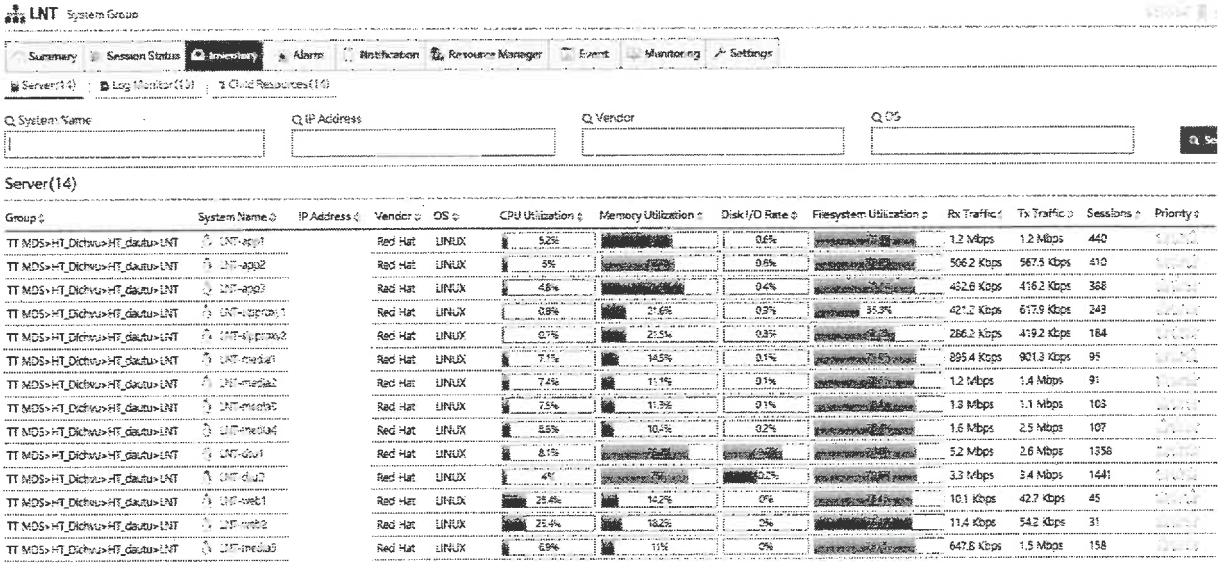
Tiếp tục add role đã tạo "test canh bao" với user đã được tạo ở trên như *Hình 3.7*. Trong giao diện này, người quản trị có thể lựa chọn các quyền (role) có sẵn từ danh sách bên trái "Available Role" và thêm vào danh sách quyền đã chọn "Selected Role" bằng cách sử dụng nút chuyển hướng. Việc thêm quyền như "test canh bao" giúp giới hạn và định nghĩa rõ phạm vi thao tác của người dùng trong hệ thống, đảm bảo tính bảo mật và kiểm soát truy cập chặt chẽ. Sau khi lựa chọn xong, nhấn Save để hoàn tất quá trình gán quyền cho tài khoản. Đây là bước quan trọng trong việc cấu hình phân quyền nhằm đảm bảo mỗi người dùng chỉ được thao tác trong phạm vi chức năng được cấp phép

Hình 3. 7: Giao diện thêm phân quyền trên tài khoản người dùng

3.3.Đánh giá hoạt động của hệ thống

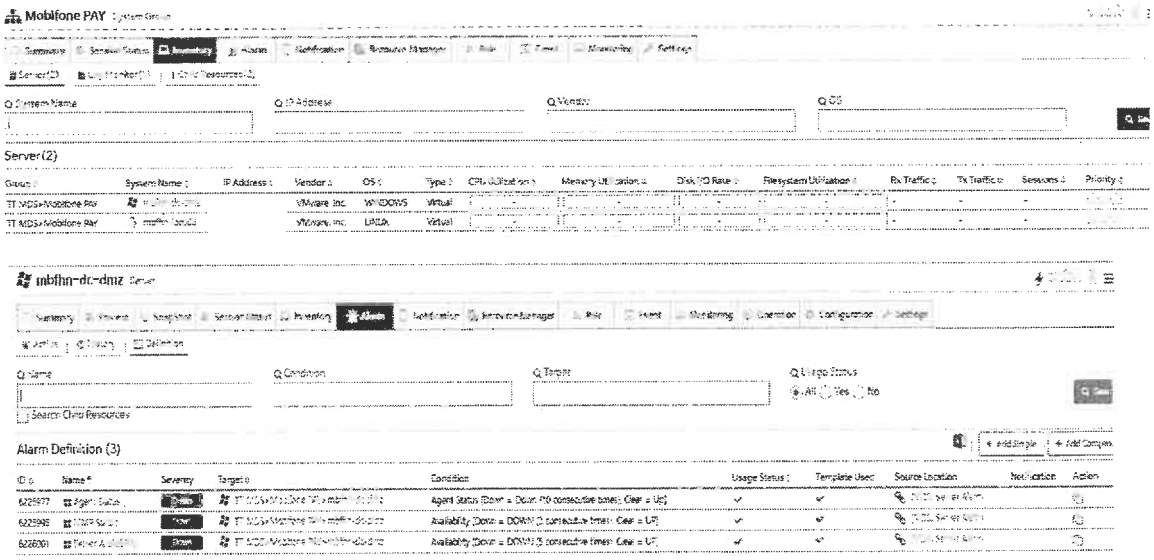
3.3.1. Giám sát các trạng thái của host

Theo dõi trạng thái của máy chủ đã được tích hợp ở tab Inventory trong System Group LNT như *Hình 3.8*. Tại Tab Server đang được tích hợp là 14 server như *Hình 3.8*. Màu xanh tại cột System Name báo hiện host đang hoạt động bình thường (UP). Trường hợp màu đỏ là host gặp sự cố kết nối hay bị down. Trong hình ảnh ta có thể thấy , việc giám sát được tôi sử dụng Polestar Agent (Port 31001-31003) có đầy đủ các thông tin như: CPU Utilization, Memory Utilization, Disk I/O Rate, Filesystem Utilization, Rx/Tx Traffic,….



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).

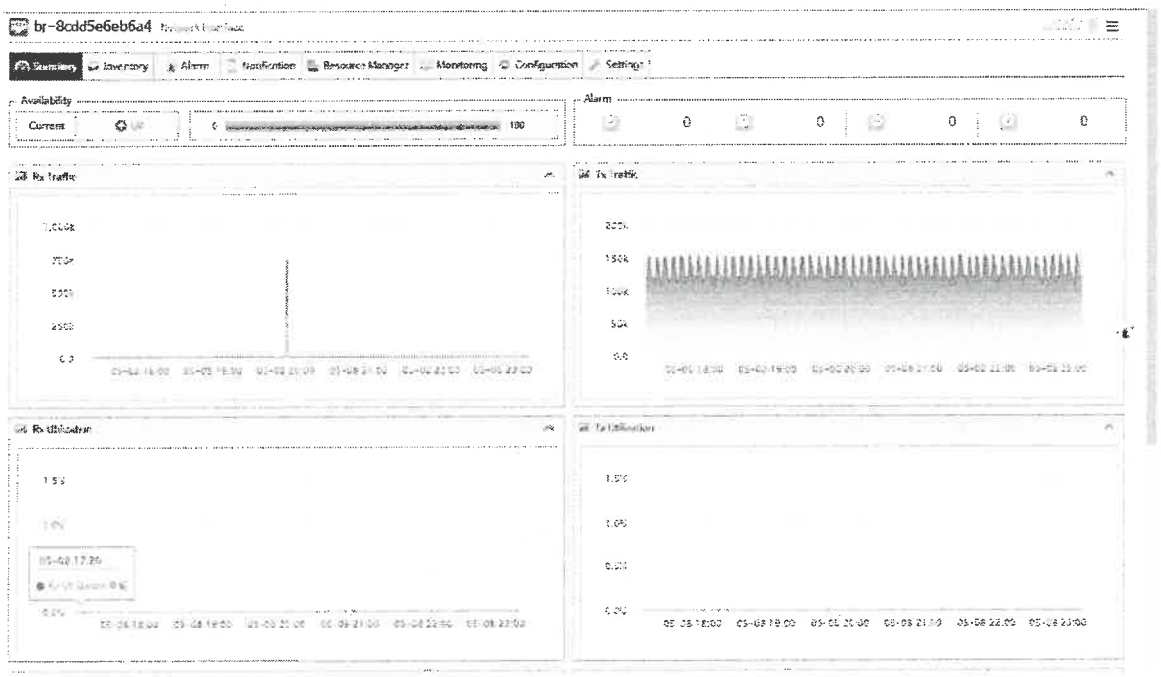


Hình 3. 9: Giao diện kiểm tra lỗi tích hợp thiết bị trên hệ thống Polestar

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.

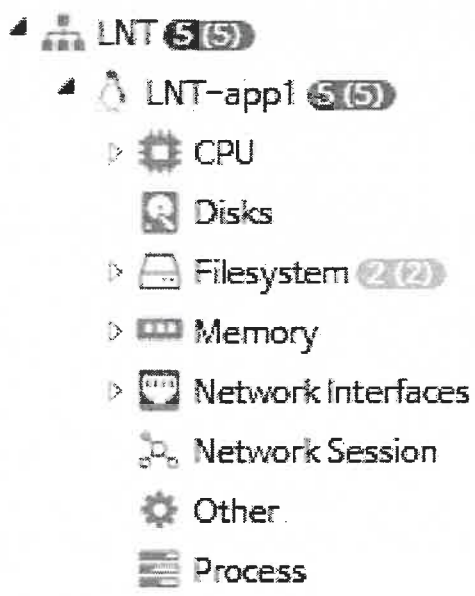


Hình 3. 11: Bảng chi tiết các thông số kỹ thuật của Network interface

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 như *Hình 3.12* (Trạng thái xanh là UP, đỏ là Down).



Hình 3. 12: Cột các hạng mục của hệ thống được tích hợp giám sát

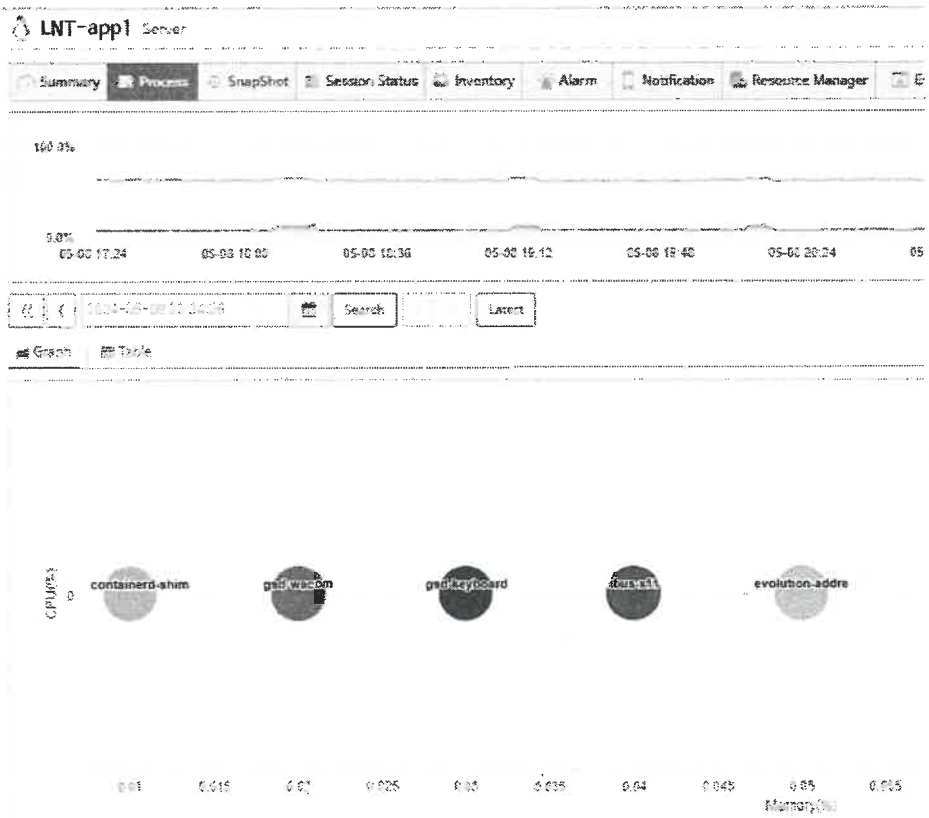
Về thông số các tài nguyên của Host ta có thể xem tổng quan tại tab Summary của Host đã được tích hợp như *Hình 3.13* Gồm đầy đủ các tài nguyên như: CPU, Memory. Top 5 Process, Top 5 Disk, Top 5 Filesystem, Rx/Tx traffic, CPU Utilization, …

Hình 3. 13: Giao diện Dashboard của hệ thống đã được tích hợp trên hệ thống Polestar

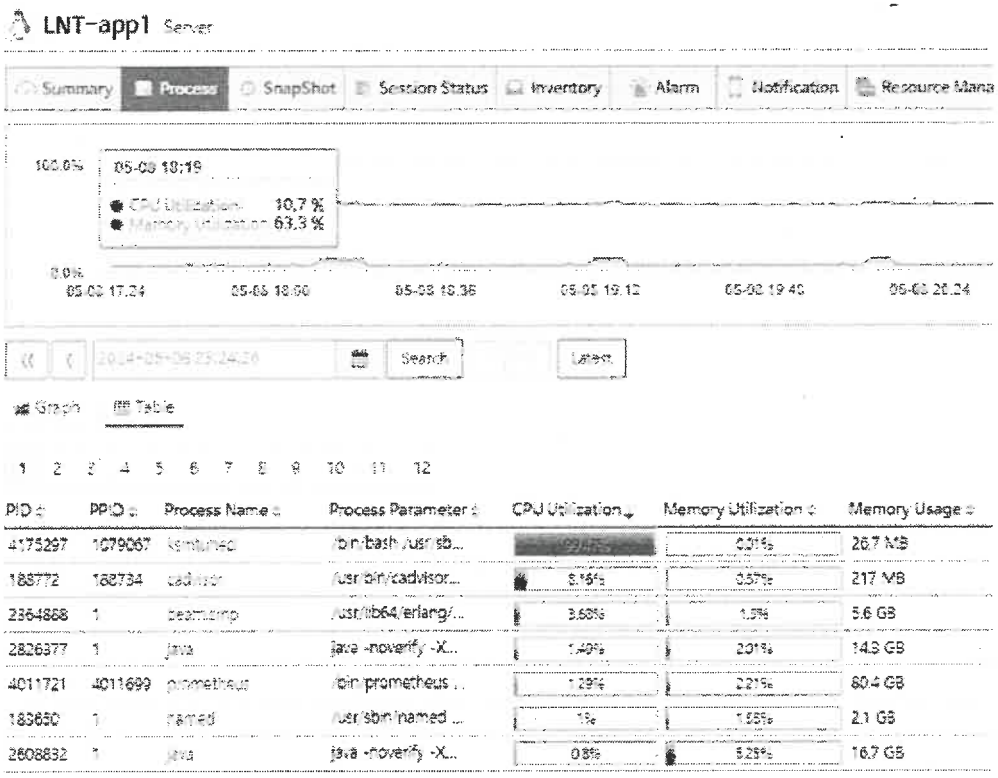
Giải pháp giám sát hạ tầng mạng Polestar cung cấp giao diện trực quan để giám sát tài nguyên hệ thống như CPU, bộ nhớ, hệ thống tệp, tiến trình và lưu lượng mạng. Các thông số này được tổng hợp tại tab Summary theo nhóm host, giúp người dùng có cái nhìn tổng thể và kịp thời đánh giá hiệu suất của từng máy chủ. Biểu đồ và bảng thống kê trực quan giúp dễ dàng phát hiện các tài nguyên sử dụng vượt ngưỡng. Tuy nhiên, việc giám sát tài nguyên hiện tại mang tính mô tả; khả năng phân tích xu hướng và dự đoán quá tải dựa trên học máy (ví dụ: LSTM cho dự báo CPU load) sẽ là hướng phát triển cần thiết.

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) như *Hình 3.14 và Hình 3.15* 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, …

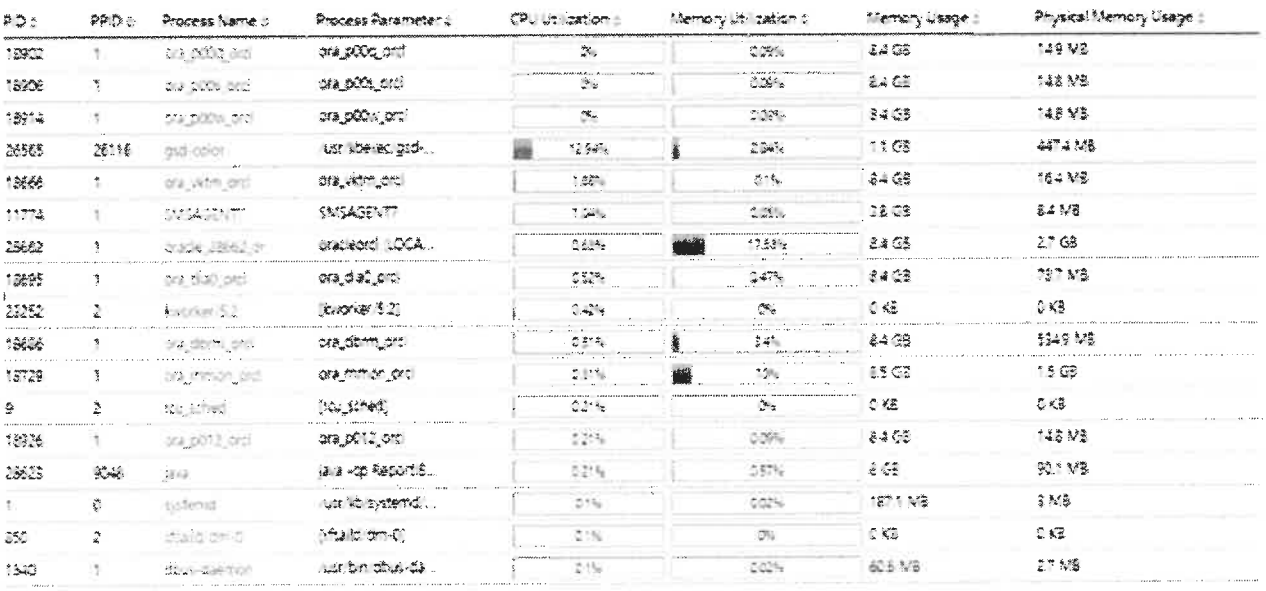


Hình 3. 14: Biểu đồ giám sát Process của thiết bị



Hình 3. 15: Thông số chi tiết giám sát Process của thiết bị

Ở đây ta có thể theo dõi theo thời gian thực hoặc lựa chọn thông tin thời gian để kiểm tra lại các Log hoạt động của các Process theo thời gian nhất định như *Hình 3.16*.

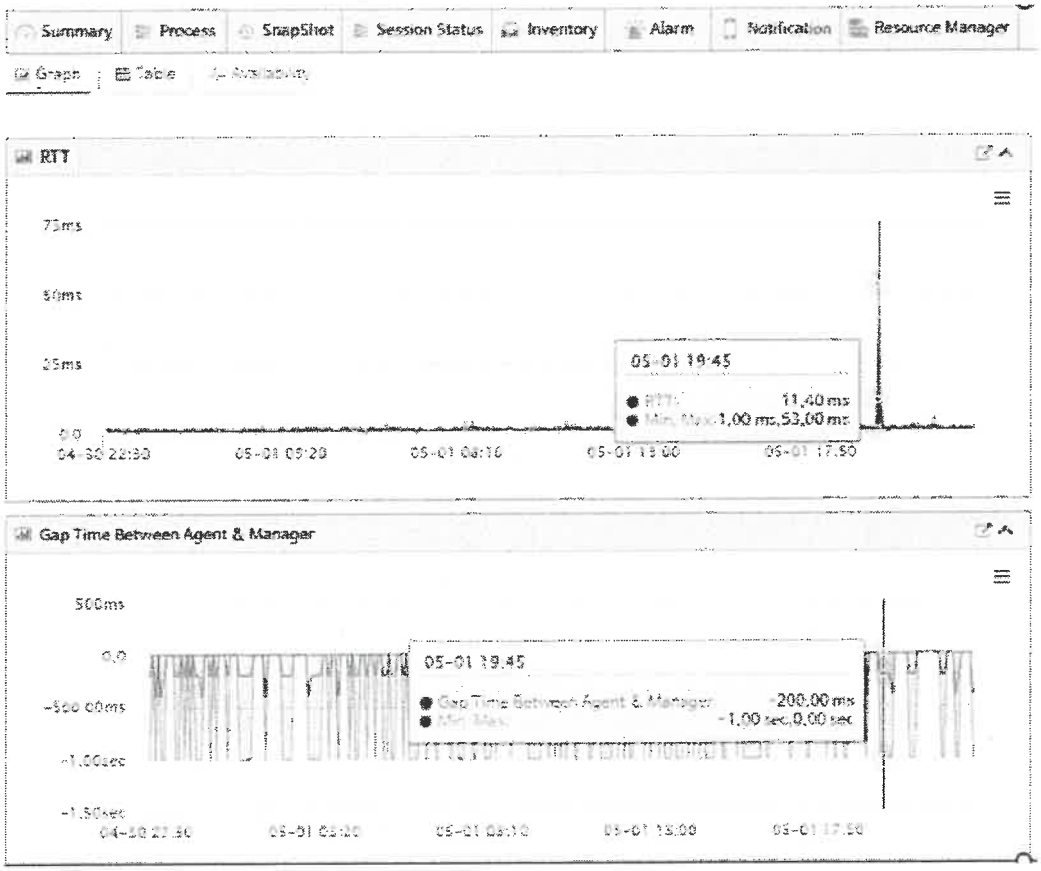


Hình 3. 16: Thông số chi tiết giám sát Process của thiết bị

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) tại *Hình 3.17*.



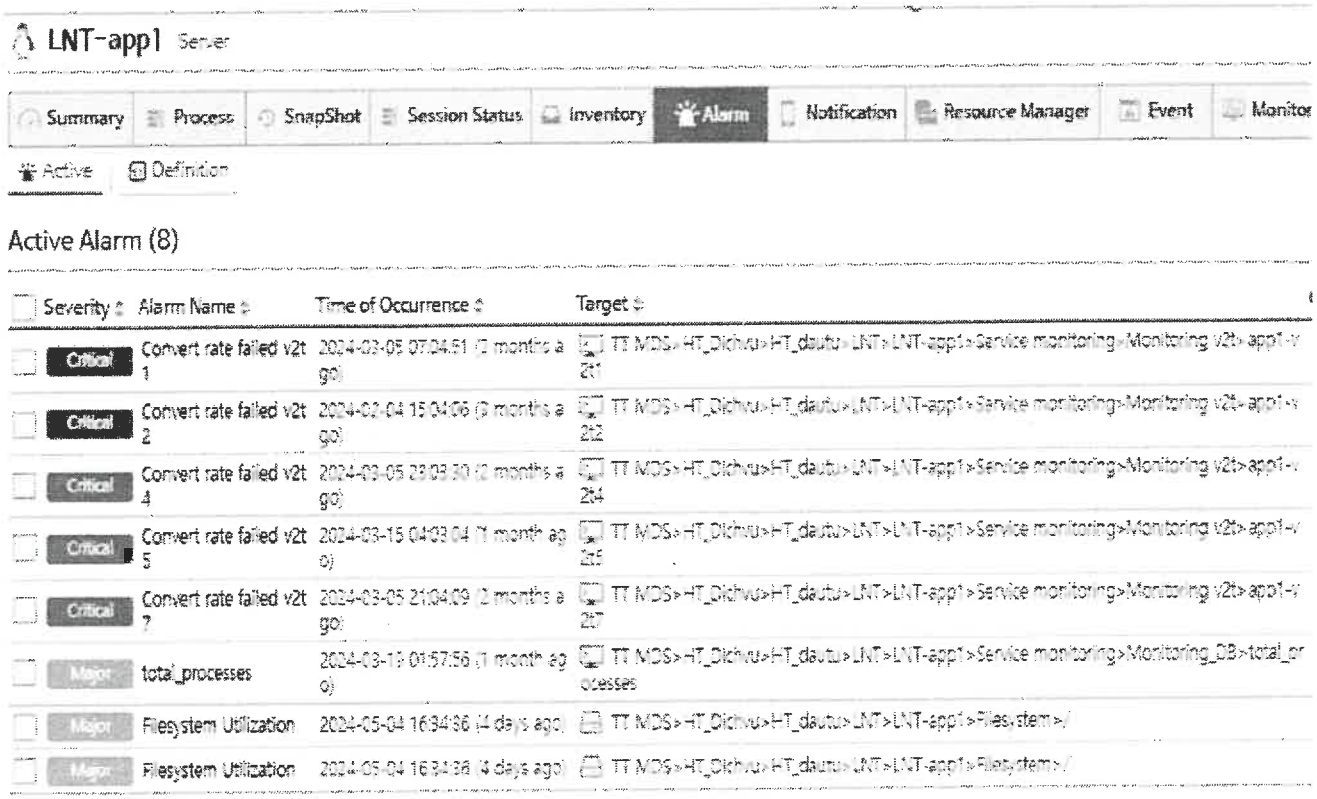
Hình 3. 17: Biểu đồ giám sát lưu lượng mạng của thiết bị

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) tại *Hình 3.17*.

Chức năng giám sát lưu lượng mạng cho phép theo dõi chi tiết traffic in/out trên từng interface mạng, hỗ trợ nhận diện nhanh các hiện tượng đột biến băng thông hoặc tắc nghẽn cục bộ. Các biểu đồ thời gian thực minh họa rõ ràng sự thay đổi lưu lượng theo thời gian giúp người vận hành chủ động điều phối tài nguyên mạng. Dù tính năng này đáp ứng tốt yêu cầu quan sát hiện trạng, nhưng để cải thiện hơn nữa, hệ thống có thể tích hợp các thuật toán phát hiện DDoS hoặc lưu lượng bất thường dựa trên mô hình clustering hoặc deep learning.

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.



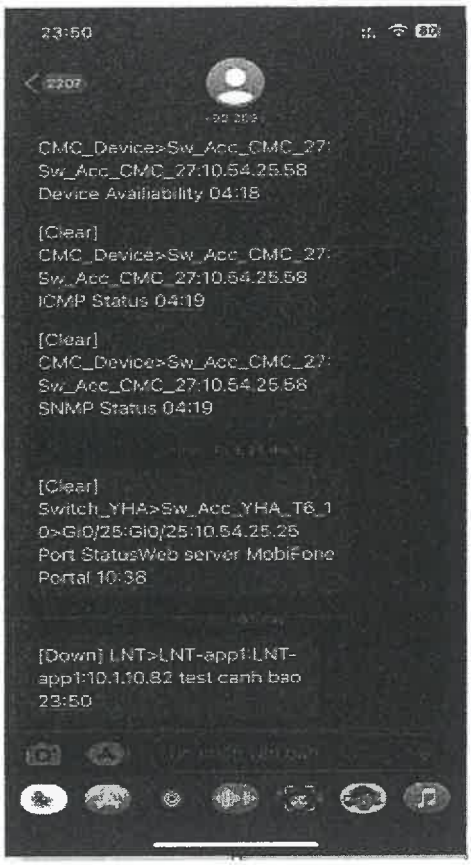
Hình 3. 18: Giao diện giám sát tập trung của thiết bị trên hệ thống Polestar

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

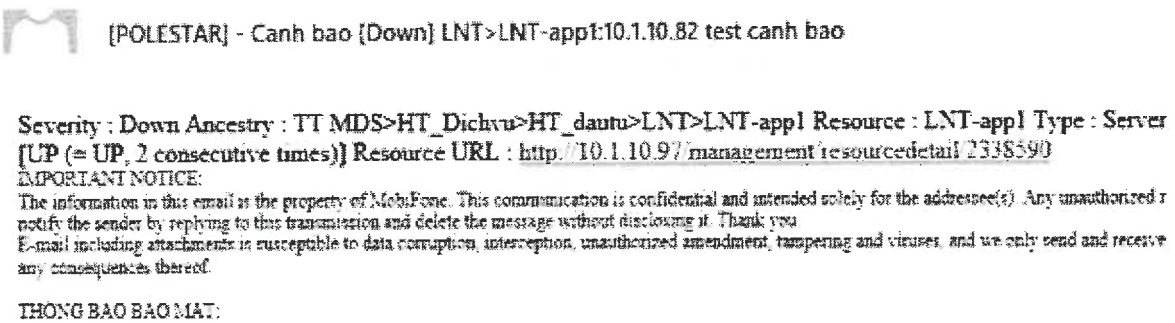
Cảnh báo sẽ thực hiện gửi tin nhắn SMS và gửi mail về tới tài khoản chủ trì được thiết lập nhận cảnh báo như *Hình 3.20* với đầy đủ các thông tin như:

– 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.

THONG BAO BAO MAT:

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

Hệ thống cảnh báo của Polestar hoạt động hiệu quả với khả năng gửi thông báo qua email và SMS khi xảy ra sự cố. Bảng điều khiển Alarm Console hiển thị tập trung các sự kiện lỗi cùng thông tin chi tiết như thời gian, trạng thái, địa

chỉ IP, nội dung lỗi. Điều này giúp rút ngắn thời gian phản ứng và nâng cao độ tin cậy trong vận hành. Tuy nhiên, hệ thống cảnh báo vẫn phụ thuộc vào ngưỡng định nghĩa thủ công. Việc ứng dụng học máy để tự động hiệu chỉnh ngưỡng cảnh báo hoặc xác định cảnh báo ảo (false positive) sẽ giúp nâng cao độ chính xác và giảm thiểu cảnh báo sai.

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).

TÀI LIỆU THAM KHẢO

[1] Josune Hernantes, Gorka Gallardo, Nicolás Serrano, "IT Infrastructure-Monitoring Tools", IEEE Software 32(4):88-93, July 2015.

[2] Thu Hương, "MobiFone cần xây dựng hạ tầng số Việt Nam hiện đại, bền vững, xanh và an toàn", Chuyên mục Viễn thông, trang thông tin Bộ thông tin và truyền thông, 14 tháng 4 năm 2023.

[3] "Polestar EMS v8.3.0", Administrator Manual, Total EMS Solution Polestar, NKIA Inc, 2021.

[4] "Polestar EMS v8.3.0", User Manual, Total EMS Solution Polestar, NKIA Inc, 2021.

[5] "Quản lý mạng Viễn thông", Học viên Công nghệ bưu chính Viễn thông, Chương trình đào tạo đại học từ xa, 2017.

[6] James Turnbull, Pro Nagios 2.0, Apress, 2006.

[7] Rihards Olups, Zabbix Network Monitoring – Second Edition, Packt Publishing, 2016.

[8] Dirk Paessler, PRTG Network Monitor - Manual, Paessler AG, 2020.

[9] Microsoft Corporation, SQL Server Monitoring and Tuning Guide, Microsoft Docs, 2021.

[10] Oracle, Oracle Database Performance Tuning Guide 19c, Oracle Documentation, 2021.

[11] Cisco Systems, Cisco Network Management Solutions, Cisco Press, 2020.

[12] William Stallings, Network Security Essentials: Applications and Standards, 6th Edition, Pearson, 2020.

[13] IBM, AIX Performance and Tuning Guide, IBM Redbooks, 2019.

[14] SolarWinds, Introduction to IT Infrastructure Monitoring, SolarWinds eBook, 2020.

[15] ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements.

[16] Wendell Odom, CCNA 200-301 Official Cert Guide, Volume 1 & 2, Cisco Press, 2020.

[17] Raymond Lacoste, Kevin Wallace, CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, Cisco Press, 2020.

[18] Cisco Networking Academy, Switching, Routing, and Wireless Essentials v7 (SRWE), Cisco Press, 2021.

[19] Sean Wilkins, Cisco Networking All-in-One For Dummies, Wiley Publishing, 2021.

BẢN CAM ĐOAN

Tôi xin cam đoan đã thực hiện việc kiểm tra mức độ tương đồng nội dung luận văn qua phần mềm DoIT một cách trung thực và đạt kết quả tương đồng 8% toàn bộ nội dung luận văn, Bản luận văn kiểm tra qua phần mềm là bản cứng luận văn đã nộp để bảo vệ trước hội đồng. Nếu sai tôi xin chịu các hình thức kỷ luật theo quy định hiện hành của Học viện.

Hà Nội, ngày tháng năm 2025

HỌC VIÊN CAO HỌC

(Ký và ghi rõ họ tên)

Trần Đoàn Trung

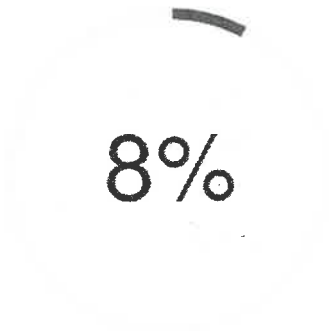
KiểmTraTàiLiệu

BÁO CÁO KIỂM TRA TRÙNG LẶP

Thông tin tài liệu

Tên tài liệu:	Đề án tốt nghiệp thạc sĩ Trần Đoàn Trung
Tác giả:	Trung Trần Đoàn
Điểm trùng lặp:	8
Thời gian tải lên:	14:43 01/08/2025
Thời gian sinh báo cáo:	14:46 01/08/2025
Các trang kiểm tra:	104/104 trang

Kết quả kiểm tra trùng lặp



Có 8% nội dung trùng lặp

Có 92% nội dung không trùng lặp

Có 0% nội dung người dùng loại trừ

Có 0% nội dung hệ thống bỏ qua

Nguồn trùng lặp tiêu biểu

123docz.net www.slideshare.net tailieu.vn

Trần Đoàn Trung

Nguyễn Thị Thanh Tú

BỘ KHOA HỌC VÀ CÔNG NGHỆ
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

BÁO CÁO GIẢI TRÌNH
SỬA CHỮA, HOÀN THIỆN ĐỀ ÁN TỐT NGHIỆP

Họ và tên học viên: Trần Đoàn Trung
Chuyên ngành: KTVT
Khóa: 2022 đợt 2

Tên đề tài: Nghiên cứu giải pháp Polestar và ứng dụng triển khai giám sát hạ tầng mạng Trung tâm Dịch vụ số MobiFone

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

Ngày bảo vệ: 19/07/2025

Các nội dung học viên đã sửa chữa, bổ sung trong đề án tốt nghiệp theo ý kiến đóng góp của Hội đồng chấm đề án tốt nghiệp:

TT	Ý kiến hội đồng	Sửa chữa của học viên
1	Rà soát lỗi chính tả, trích dẫn tài liệu tham khảo	Học viên đã rà soát, chỉnh sửa các lỗi soạn thảo, các lỗi ngữ pháp và thêm trích dẫn tài liệu tham khảo
2	Rà soát hiệu chỉnh theo ý kiến đóng góp của ủy viên phản biện và các thành viên hội đồng	Tiếp thu góp ý của Hội đồng, tác giả đã rà soát và hiệu chỉnh theo ý kiến đóng góp của ủy viên phản biện và các thành viên hội đồng
3	Phân tích thêm về sở cứ lựa chọn giải pháp, tính logic nội dung	Tiếp thu góp ý của Hội đồng, tác giả đã bổ sung thêm các nội dung sở cứ tại các mục sau: - Kết luận chương 2. - Chương 3 - Mục 3.2 Giải pháp giám sát cho hạ tầng mạng của Trung tâm Dịch vụ số MobiFone

Hà Nội, ngày tháng năm 2025

Ký xác nhận của

CHỦ TỊCH HỘI ĐỒNG CHẤM ĐỀ ÁN	THƯ KÝ HỘI ĐỒNG	NGƯỜI HƯỚNG DẪN KHOA HỌC	HỌC VIÊN
PGS.TS Lê Nhật Thăng	TS. Nguyễn Thị Thu Hiên	PGS.TS Dương Thị Thanh Tú	Trần Đoàn Trung

BỘ KHOA HỌC VÀ CÔNG NGHỆ
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

BIÊN BẢN
HỌP HỘI ĐỒNG CHẤM ĐỀ ÁN TỐT NGHIỆP THẠC SĨ

Căn cứ quyết định số Quyết định số 1098/QĐ-HV ngày 26 tháng 06 năm 2025 của Giám đốc Học viện Công nghệ Bưu chính Viễn thông về việc thành lập Hội đồng chấm đề án tốt nghiệp thạc sĩ. Hội đồng đã họp vào hồi..10..giờ..05..phút, ngày 19 tháng 07 năm 2025 tại Học viện Công nghệ Bưu chính Viễn thông để chấm đề án tốt nghiệp thạc sĩ cho:

Học viên: **Trần Đoàn Trung**

Tên đề án tốt nghiệp: **Nghiên cứu giải pháp Polestar và ứng dụng triển khai giám sát hạ tầng mạng Trung tâm Dịch vụ số Mobifone**

Chuyên ngành: **Kỹ thuật viễn thông** Mã số: **8520208**

Các thành viên của Hội đồng chấm đề án tốt nghiệp có mặt: ..05.../ 05

TT	HỌ VÀ TÊN	TRÁCH NHIỆM TRONG HĐ	GHI CHÚ
1	**PGS. TS. Lê Nhật Thăng**	Chủ tịch	
2	**TS. Nguyễn Thị Thu Hiên**	Thư ký	
3	**PGS.TS. Nguyễn Chiến Trinh**	Phản biện 1	
4	**TS. Lê Anh Ngọc**	Phản biện 2	
5	**TS. Nguyễn Hồng Thủy**	Uỷ viên	

Các nội dung thực hiện:

1. Chủ tịch Hội đồng điều khiển buổi họp. Công bố quyết định của Giám đốc Học viện Công nghệ Bưu chính Viễn thông về việc thành lập Hội đồng chấm đề án tốt nghiệp thạc sĩ.
2. Người hướng dẫn khoa học hoặc thư ký đọc lý lịch khoa học và các điều kiện bảo vệ đề án tốt nghiệp của học viên. (có bản lý lịch khoa học và kết quả các môn học cao học của học viên kèm theo).
3. Học viên trình bày tóm tắt đề án tốt nghiệp.
4. Phản biện 1 đọc nhận xét (có văn bản kèm theo)
5. Phản biện 2 đọc nhận xét (có văn bản kèm theo)
6. Các câu hỏi của thành viên Hội đồng:

1) Lý do chọn Polestar?
2) Yêu cầu mở rộng khi triển khai hạ tầng lớn?
3) Khả năng giám sát thông minh của Polestar?
4) Phân tích hạn chế & nêu giải pháp?

7. Trả lời của học viên:

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập – Tự do – Hạnh phúc

BẢN NHẬN XÉT ĐỀ ÁN TỐT NGHIỆP THẠC SĨ
(*Dùng cho người phản biện*)

Tên đề tài đề án tốt nghiệp: Nghiên cứu giải pháp Polestar và ứng dụng triển khai giám sát hạ tầng mạng Trung tâm Dịch vụ số MobiFone

Chuyên ngành: KỸ THUẬT VIỄN THÔNG

Mã chuyên ngành: 8.52.02.08

Họ và tên học viên: Trần Đoàn Trung

Họ và tên người nhận xét: Lê Anh Ngọc

Học hàm, học vị: Tiến sĩ

Chuyên ngành: Kỹ thuật thông tin và truyền thông

Cơ quan công tác: Đại học FPT

Số điện thoại: 0916880777 E-mail: anhngocle.vn@gmail.com

NỘI DUNG NHẬN XÉT

I/ Cơ sở khoa học và thực tiễn, tính cấp thiết của đề tài:

Đề tài "Nghiên cứu giải pháp Polestar và ứng dụng triển khai giám sát hạ tầng mạng Trung tâm Dịch vụ số MobiFone" có tính cấp thiết cao trong bối cảnh công nghệ thông tin ngày càng phát triển và được ứng dụng rộng rãi, yêu cầu đảm bảo sự ổn định của hạ tầng CNTT trong các doanh nghiệp. Luận văn đã chỉ ra rằng việc thiếu một hệ thống giám sát cảnh báo tập trung tại Trung tâm Dịch vụ số MobiFone đang tiềm ẩn nhiều rủi ro về hệ thống không ổn định và khó phát hiện, dự báo sớm các vấn đề hạ tầng. Việc lựa chọn giải pháp Polestar EMS, một hệ thống giám sát dựa trên các kỹ thuật quản trị mạng tiên tiến như agent-based, web-based, và AI-based, là một hướng đi phù hợp để giải quyết các vấn đề tồn đọng, đảm bảo hoạt động ổn định và giảm thiểu rủi ro an toàn thông tin cho MobiFone nói riêng và các doanh nghiệp tương tự nói chung.

II/ Nội dung của đề án tốt nghiệp, các kết quả đã đạt được:

Đề án được cấu trúc rõ ràng với ba chương chính:

- Chương 1: Hạ tầng mạng Trung tâm Dịch vụ số MobiFone : Khảo sát chi tiết hiện trạng hạ tầng mạng của Trung tâm Dịch vụ số MobiFone, bao gồm các thành phần như Border Router, Firewall, Core Switch và Access Switch theo mô hình Tier 3. Chương này cũng đánh giá các giải pháp giám sát hiện tại (Prometheus, SolarWinds) và chỉ ra

những vấn đề còn tồn tại như thiếu khả năng giám sát cảnh báo tập trung và tích hợp hạn chế.

- Chương 2: Nghiên cứu giải pháp Polestar : Trình bày tổng quan về quản lý mạng, các thành phần cơ bản, chức năng quản lý (hiệu năng, sự cố, cấu hình, tài khoản, bảo mật) và kiến trúc TMN. Luận văn đã so sánh Polestar với các giải pháp giám sát phổ biến khác như Nagios, Zabbix, PRTG Network Monitor. Điểm nổi bật là việc giới thiệu chi tiết giải pháp Polestar, bao gồm kiến trúc, các đối tượng và chức năng giám sát chính (Real-time Monitoring, Topology Map, System Dashboard, Xem trạng thái hiệu năng, Review Event, Centralized Alarm System). Chương này khẳng định tính ưu việt và khả năng ứng dụng cao của Polestar so với các giải pháp truyền thống.
- Chương 3: Ứng dụng giải pháp giám sát Polestar cho hạ tầng mạng Trung tâm Dịch vụ số MobiFone: Tập trung vào việc triển khai thử nghiệm giải pháp Polestar vào thực tế tại MobiFone. Các bước như xây dựng mô hình giám sát, cấu hình hệ thống, thiết lập cảnh báo và giám sát các kịch bản thực tiễn đã được thực hiện. Kết quả thử nghiệm cho thấy Polestar đáp ứng tốt các yêu cầu về hiệu năng, độ ổn định, giảm thời gian phản hồi sự cố, và nâng cao tính sẵn sàng cũng như khả năng quản trị hệ thống mạng.

Các kết quả đạt được của đề án là rất đáng ghi nhận, thể hiện sự nghiên cứu nghiêm túc và khả năng ứng dụng thực tiễn của giải pháp Polestar trong việc nâng cao hiệu quả giám sát và vận hành hạ tầng mạng tại Trung tâm Dịch vụ số MobiFone.

III/ Những vấn đề cần giải thích thêm:

Q1. Luận văn đã đánh giá tính ưu việt của Polestar. Học viên có thể phân tích thêm về lý do lựa chọn Polestar về mặt chi phí và lợi ích cụ thể mà giải pháp này mang lại so với các giải pháp giám sát khác đã được đề cập (Nagios, Zabbix, PRTG, Prometheus, SolarWinds) trong môi trường thực tiễn của MobiFone?

Q2. Với đặc thù hạ tầng mạng lớn và không ngừng phát triển của MobiFone, học viên có thể làm rõ hơn về khả năng mở rộng (scalability) của Polestar trong việc quản lý số lượng thiết bị và lưu lượng dữ liệu giám sát gia tăng theo thời gian? Giải pháp này có những cơ chế hay kiến trúc nào để đảm bảo hiệu năng ổn định khi quy mô giám sát ngày càng lớn?

IV/ Kết luận:

Đồng ý cho phép học viên bảo vệ đề án tốt nghiệp.

Ngày..18....tháng....7....năm 2025

NGƯỜI NHẬN XÉT

TS Lê Anh Ngọc

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

----------oOo----------

BẢN NHẬN XÉT ĐỀ ÁN TỐT NGHIỆP THẠC SĨ

(Dùng cho người phản biện)

Tên đề tài luận văn: Nghiên cứu giải pháp Polestar và ứng dụng triển khai giám sát hạ tầng mạng trung tâm dịch vụ số Mobifone.

Chuyên ngành: Kỹ thuật viễn thông.

Mã chuyên ngành: 60.52.02.08

Họ và tên học viên: Trần Đoàn Trung

Họ và tên người nhận xét: Nguyễn Chiến Trinh

Học hàm, học vị: Phó Giáo sư - Tiến sĩ.

Chuyên ngành: Điện tử - Viễn thông

Cơ quan công tác: Học viện Công nghệ Bưu chính Viễn thông.

Số điện thoại: 0915400946.....E-mail: trinhnc@ptit.edu.vn.

NỘI DUNG NHẬN XÉT

I/ Cơ sở khoa học và thực tiễn, tính cấp thiết của đề tài:

Hệ thống quản lí là một trong những thành phần không thể thiếu của hạ tầng mạng, công nghệ thông tin, nhằm đảm bảo vận hành và hoạt động của mạng cũng như các hệ thống cung cấp dịch vụ. Đề tài "Nghiên cứu giải pháp Polestar và ứng dụng triển khai giám sát hạ tầng mạng trung tâm dịch vụ số Mobifone" nghiên cứu giải pháp và công cụ/nền tảng giám sát hạ tầng mạng do vậy có ý nghĩa khoa học và thực tiễn. Kết quả của đề án có thể hỗ trợ cho quá trình triển khai, xây dựng hệ thống quản lí mạng cho các doanh nghiệp.

II/ Nội dung của luận văn, các kết quả đã đạt được:

Luận văn bao gồm 3 chương: giới thiệu hạ tầng mạng TT dịch vụ số Mobifone, các nền tảng giám sát hạ tầng mạng, hệ thống giám sát hạ tầng TT dịch vụ số Mobifone trên Polestar. Bố cục của đề án hợp lí, bám sát đề cương được duyệt. Tuy nhiên có một số nội dung cần lưu ý hoàn thiện:

- Chương 1 nên đưa ra yêu cầu kĩ thuật về hệ thống giám sát hạ tầng mạng TT dịch vụ số Mobifone.
- Chương 3 nội dung đề án có sự khác biệt với đề cương được duyệt: "ứng dụng giải pháp" – "triển khai thử nghiệm".

- Đánh giá hệ thống giám sát Polesatr triển khai còn chung chung và định tính, nên có một số dữ liệu đánh giá cụ thể hơn.
- Hình thức trình bày: hình vẽ còn mờ, trích dẫn tài liệu tham khảo đầy đủ.

III/ Những vấn đề cần giải trình thêm:

1) Các khả năng giám sát thông minh của Polestar? Đã triển khai thử nghiệm các chức năng này và kết quả?
2) Phân tích lựa chọn giải pháp Polestar cho hạ tầng mạng TT dịch vụ Mobifone?

IV/ Kết luận:

Đề án đạt yêu cầu của đề án hướng ứng dụng tốt nghiệp Thạc sĩ.

Đồng ý cho phép học viên bảo vệ trước hội đồng.

Hà Nội, ngày tháng năm 2025

NGƯỜI NHẬN XÉT

PGS.TS Nguyễn Chiến Trinh