

AUTOPATCH

KIẾN TRÚC VÁ LỖI TỰ ĐỘNG DỰA TRÊN
CI/CD CHO HỆ THỐNG NGÂN HÀNG
NHÓM 173

TỔNG QUAN VỀ

AUTOPATCH

AutoPatch là giải pháp CI/CD pipeline tự động hóa vá lỗi bảo mật Windows Server dựa trên báo cáo CVE, được thiết kế riêng cho môi trường ngân hàng và doanh nghiệp có yêu cầu bảo mật cao.

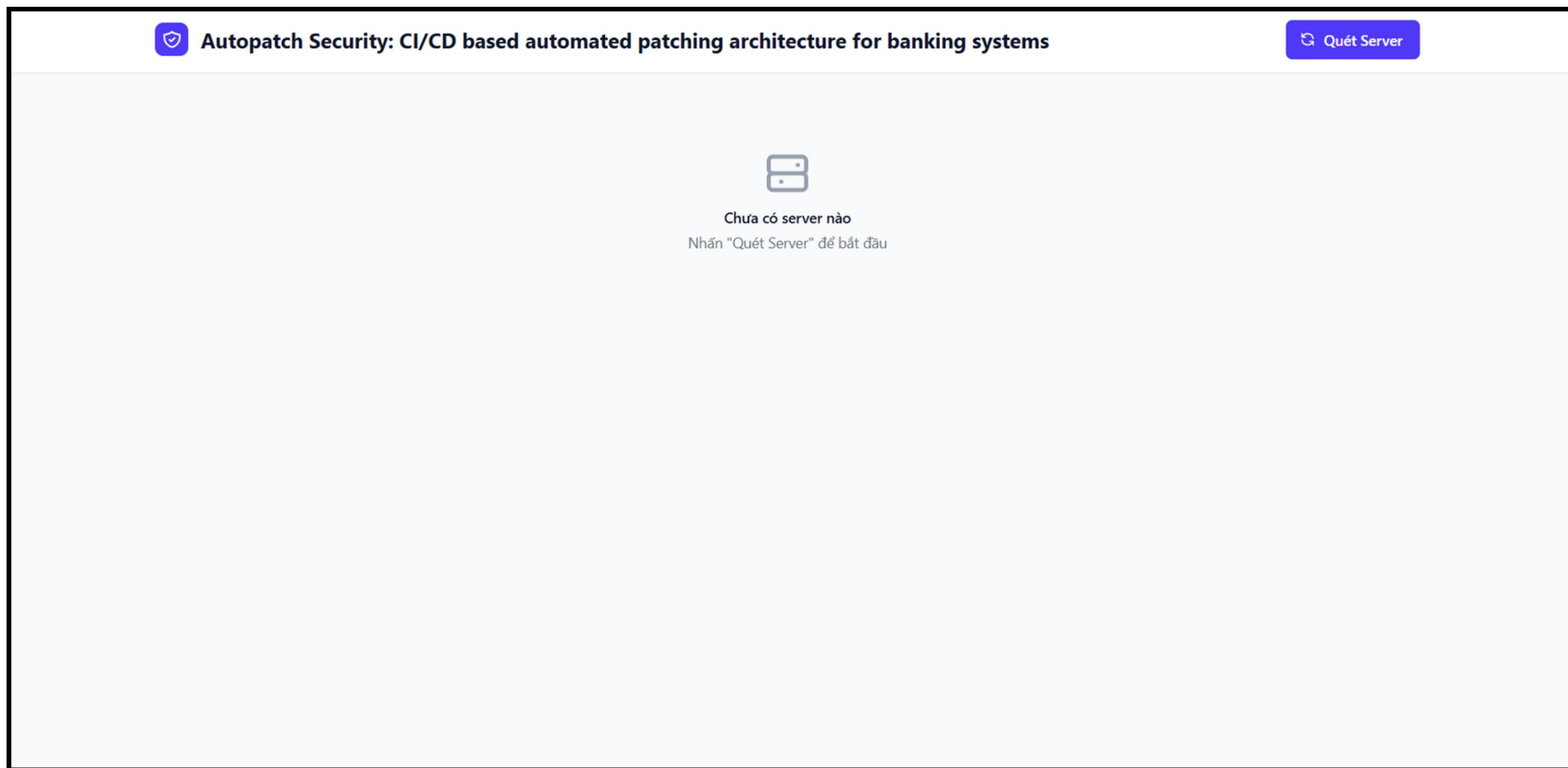
- Mục tiêu AutoPatch - xây dựng pipeline tự động:
 - Quét OS version của các máy chủ
 - Cào dữ liệu CVE mới nhất từ trang web: [MSRC](#)
 - Phân tích CVE, mapping KB phù hợp từng version OS
 - Triển khai patch tự động qua PowerShell (SSM Run Command)
 - Ghi log & báo cáo kết quả (Dashboard và Email - SNS), đảm bảo audit trail
 - Cho phép kiểm tra các KB sẽ được patch trước khi chạy script
 - Hỗ trợ Retry Patch các KB bị Failed khi chạy luồng chính
 - Hỗ trợ reboot thủ công

CÁC DỊCH VỤ AWS ĐƯỢC SỬ DỤNG

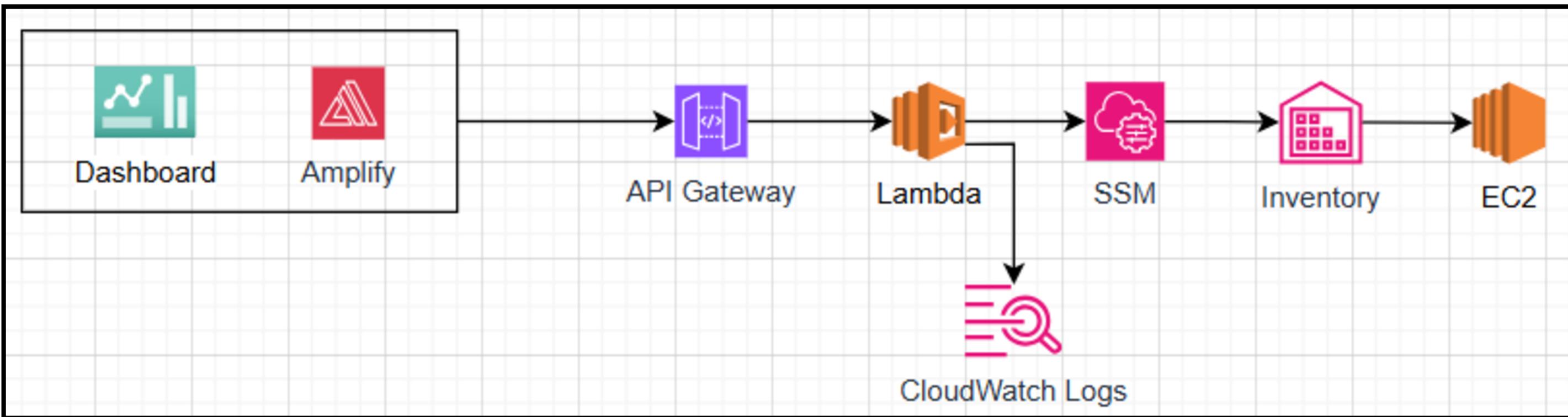
Tên dịch vụ	Nhiệm vụ
Lambda	Xử lý logic chính và các tác vụ backend
Step Functions	Điều phối quy trình vá lỗi tự động
DynamoDB	Lưu trữ trạng thái vá lỗi và ánh xạ CVE-KB
SSM (RunCommand)	Thực thi script vá lỗi
SNS	Gửi thông báo tổng hợp vá lỗi (ví dụ: qua email)
CloudWatch	Ghi log và giám sát để phục vụ việc debug
API Gateway	Cung cấp các endpoint backend cho frontend sử dụng
Amplify	Lưu trữ giao diện frontend và kết nối với các API backend

GIAO DIỆN CHÍNH

Khi bắt đầu vào Auto Patch, ta sẽ thấy giao diện như sau. Để bắt đầu sử dụng Auto Patch, ta nhấn nút **Quét Server**



LUÔNG DỮ LIỆU - QUÉT SERVER



Công việc chính của hàm Lambda:

1. Gọi SSM describe_instance_information()
2. Lặp qua từng instance EC2: lấy các thông tin cơ bản của server
3. Ghi log và trả kết quả

Hàm này cũng cho biết một server có đang hoạt động (running) hay không ?

GIAO DIỆN CHÍNH

Sau một khoảng thời gian, giao diện sẽ xuất hiện các thông tin như: tổng số server, danh sách server,...

Autopatch Security: CI/CD based automated patching architecture for banking systems

Tổng Server 1

Đã Chọn 0

CVE Found 0

Danh sách Server
Thông tin chi tiết về các server trong hệ thống 0 / 1 đã chọn [Chọn tất cả](#)

<input type="checkbox"/>	SERVER	OPERATING SYSTEM	IP ADDRESS	AMI	LAST UPDATED
<input type="checkbox"/>	i-076e21d791777f0e4 Active	Windows Server 2019 10.0.17763	172.31.28.187	Windows_Server-2019-English-Full-Base-2025.06.11	23:24:53 16/7/2025

[|– Cập nhật CVE mới nhất \(0 server\)](#) [⟳ Phân tích CVE \(0 server\)](#) [Run Patch KB \(0\)](#)

GIAO DIỆN CHÍNH

Tiếp theo, ta có thể lựa chọn một hoặc nhiều server để thực hiện:

- **Cập nhật CVE mới nhất** đối với các server được lựa chọn
- Tiến hành **phân tích các CVE** mà các server được lựa chọn đang mắc phải
- Tiến hành **vá các server** được lựa chọn

bằng cách nhấn nút thích hợp.

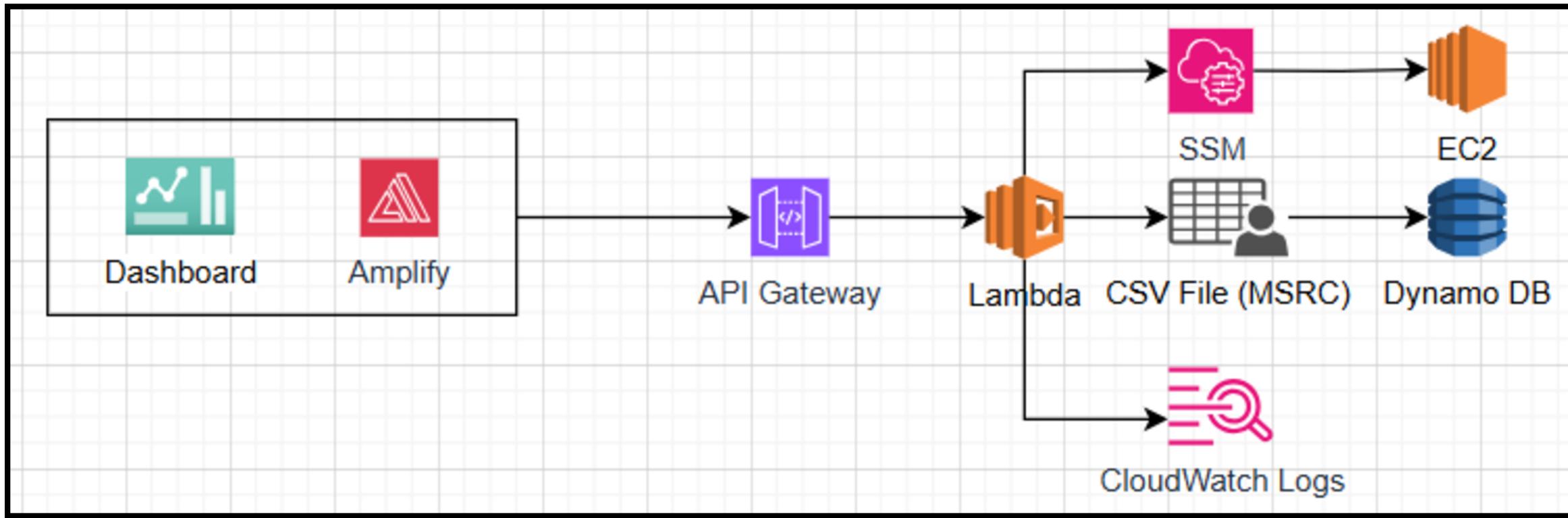
Danh sách Server
Thông tin chi tiết về các server trong hệ thống

1 / 1 đã chọn [Bỏ chọn tất cả](#)

<input checked="" type="checkbox"/> SERVER	OPERATING SYSTEM	IP ADDRESS	AMI	LAST UPDATED
<input checked="" type="checkbox"/>  i-076e21d791777f0e4 Active	Windows Server 2019 10.0.17763	172.31.28.187	Windows_Server-2019-English-Full-Base-2025.06.11	23:24:53 16/7/2025

[← Cập nhật CVE mới nhất \(1 server\)](#) [↻ Phân tích CVE \(1 server\)](#) [Run Patch KB \(1\)](#)

LUÔNG DỮ LIỆU - CẬP NHẬT CVE MỚI NHẤT



Công việc chính của hàm Lambda:

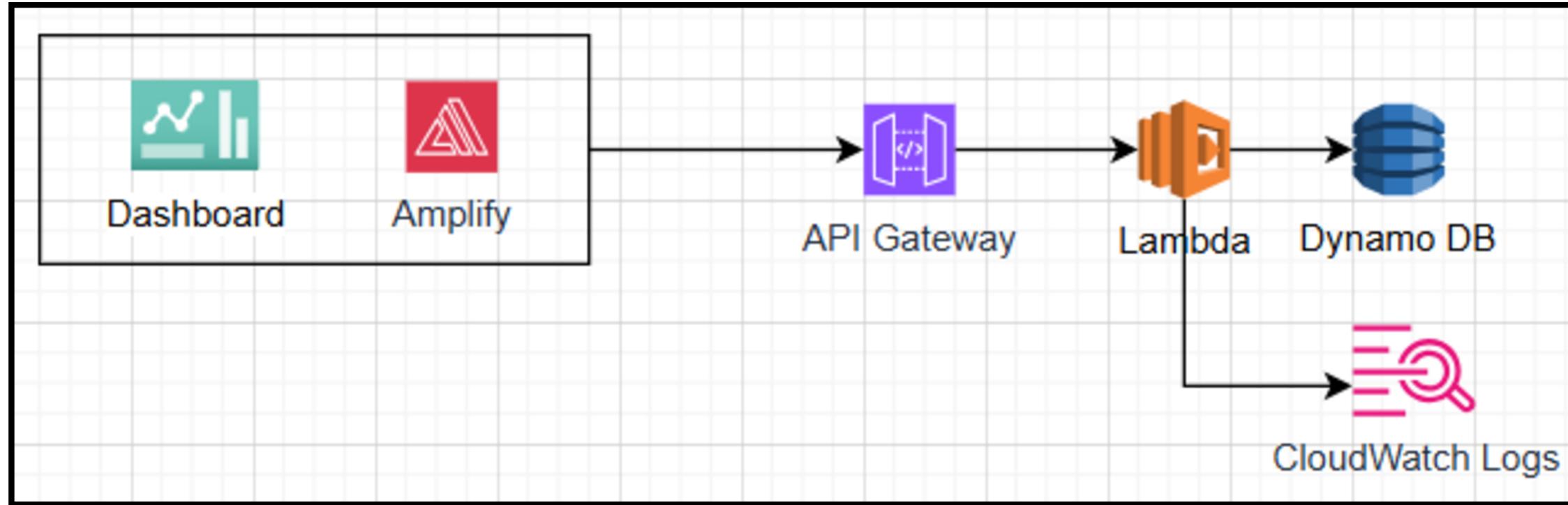
1. Dò tìm hệ điều hành từ tag OS của mỗi EC2
2. Cào dữ liệu liên quan đến CVE từ MSRC theo khoảng thời gian (từ ngày đầu tháng đến ngày hiện tại)
3. Lọc dữ liệu theo hệ điều hành và mức độ nghiêm trọng (Important/Critical)
4. Lưu dữ liệu CVE và KB xuống Dynamo DB
5. Ghi log và trả kết quả

GIAO DIỆN CHÍNH

Kết quả khi ta thực hiện cập nhật CVE mới nhất đối với các server được lựa chọn

LUÔNG DỮ LIỆU - PHÂN TÍCH CVE

Phân tích CVE (1 server)



Công việc chính của hàm Lambda:

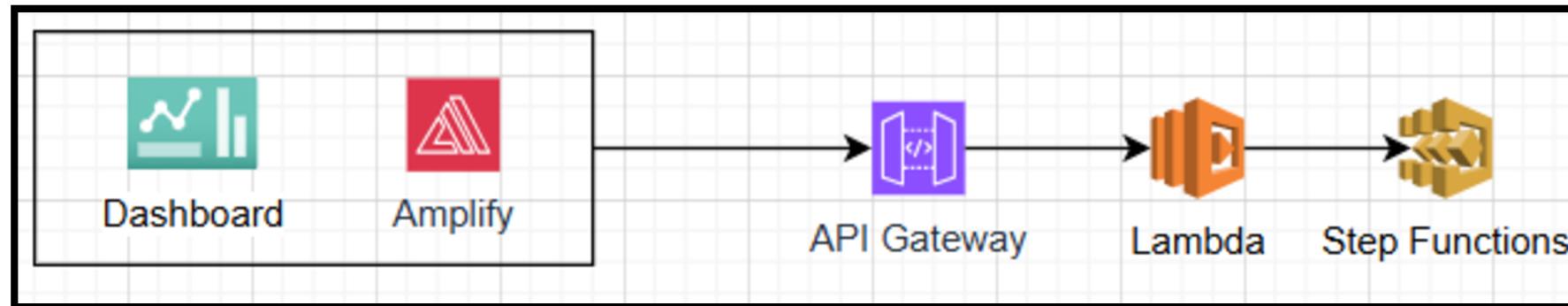
1. Nhận danh sách các phiên bản hệ điều hành (OS versions)
2. Truy vấn DynamoDB theo từng OS để lấy các bản ghi CVE tương ứng
3. Trả về kết quả gồm: mã CVE, mức độ nghiêm trọng, bài viết KB, ngày phát hành, yêu cầu reboot,...

GIAO DIỆN CHÍNH

Kết quả khi ta tiến hành phân tích các CVE mà các server được lựa chọn đang mắc phải

Kết quả phân tích CVE						
OS versions: Windows Server 2019						
Mức độ:	Tất cả	▼	OS:	Tất cả	▼	Hiển thị 88 / 88 CVE
CVE NUMBER	SEVERITY	BASE SCORE	IMPACT	OS	KB ARTICLE	RELEASE DATE
CVE-2025-36350	Critical	5.6	Information Disclosure	Windows Server 2019	5062557	8/7/2025
CVE-2025-36357	Critical	5.6	Information Disclosure	Windows Server 2019	5062557	8/7/2025
CVE-2025-47159	Important	7.8	Elevation of Privilege	Windows Server 2019	5062557	8/7/2025
CVE-2025-47971	Important	7.8	Elevation of Privilege	Windows Server 2019	5062557	8/7/2025
CVE-2025-47972	Important	8.0	Elevation of Privilege	Windows Server 2019	5062557	8/7/2025
CVE-2025-47973	Important	7.8	Elevation of Privilege	Windows Server 2019	5062557	8/7/2025
CVE-2025-47975	Important	7.0	Elevation of Privilege	Windows Server 2019	5062557	8/7/2025
CVE-2025-47976	Important	7.8	Elevation of Privilege	Windows Server 2019	5062557	8/7/2025
CVE-2025-47980	Critical	6.2	Information Disclosure	Windows Server 2019	5062557	8/7/2025

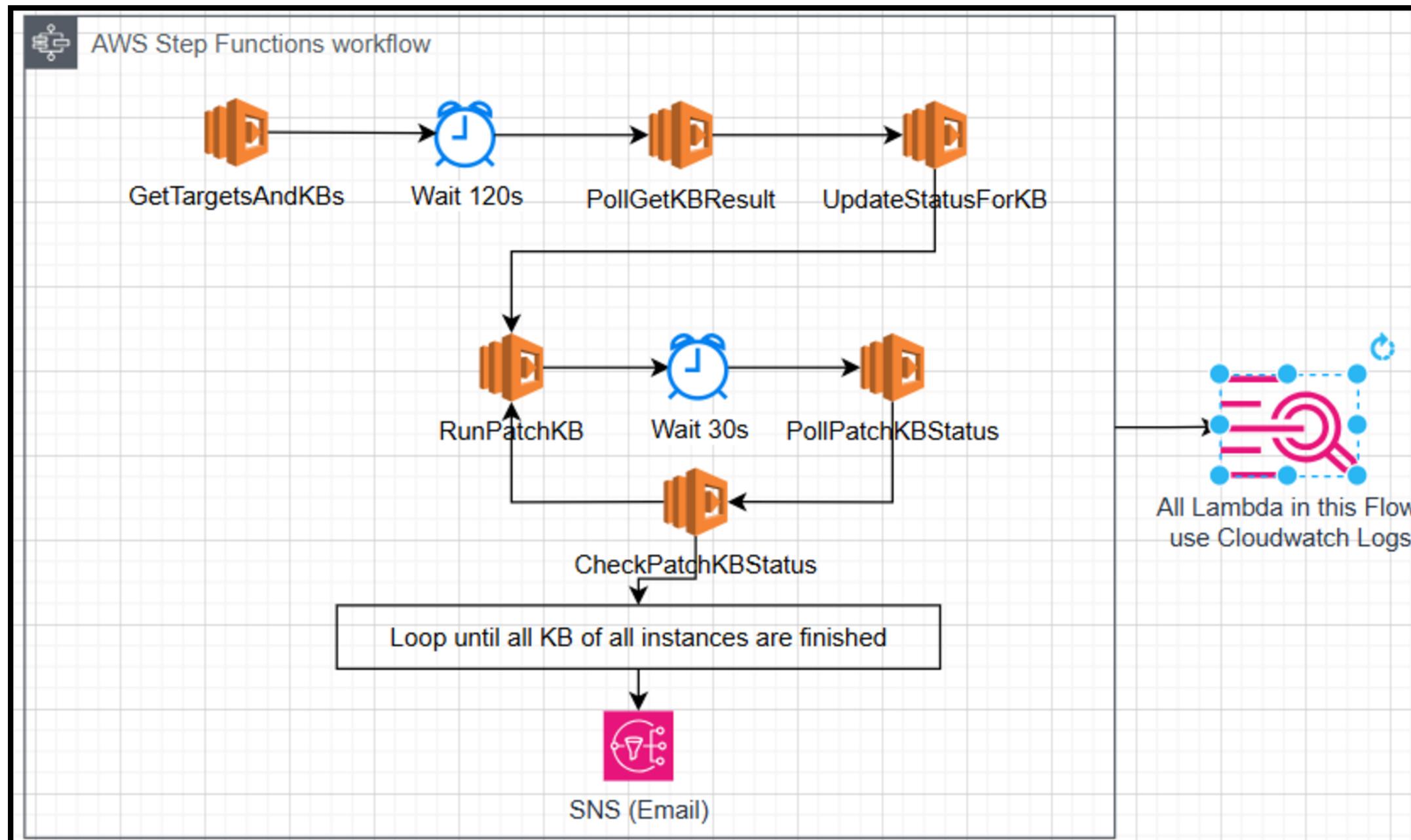
LUÔNG DỮ LIỆU - RUN PATCH (KB)



Run Patch KB (1)

Công việc chính của hàm Lambda:

1. Kích hoạt Step Functions cập nhật KB cho EC2



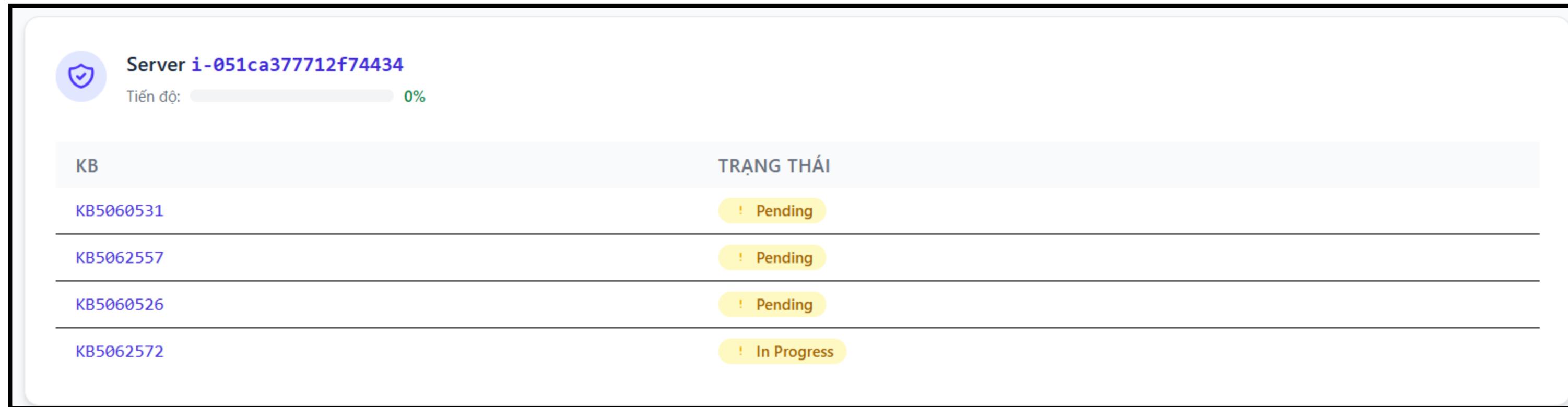
LUÔNG DỮ LIỆU - RUN PATCH (KB)

Các bước chính trong Step Functions:

1. Lấy danh sách KBs → từ các instance EC2 (qua Lambda)
2. Chờ & kiểm tra kết quả → đảm bảo dữ liệu đã sẵn sàng
3. Với từng máy chủ:
 - Đánh dấu các bản vá:
 - Đã cài → Already Installed
 - Bỏ qua → Skipped
 - Chưa cài → Pending
 - Với từng bản vá Pending:
 - Đánh dấu InProgress
 - Gọi Lambda để cài đặt
 - Kiểm tra trạng thái (Success, Failed, hoặc tiếp tục đợi)
 - Ghi kết quả
4. Gửi email tổng hợp (có thể bỏ qua nếu luồng Step Functions xảy ra lỗi)

GIAO DIỆN CHÍNH

Khi ta bắt đầu thực hiện vá, các bản vá KB sẽ được thực hiện lần lượt. Bản vá đang được thực hiện sẽ được đánh dấu là **In Progress**, các bản vá đang chờ được đánh dấu là **Pending**.



GIAO DIỆN CHÍNH

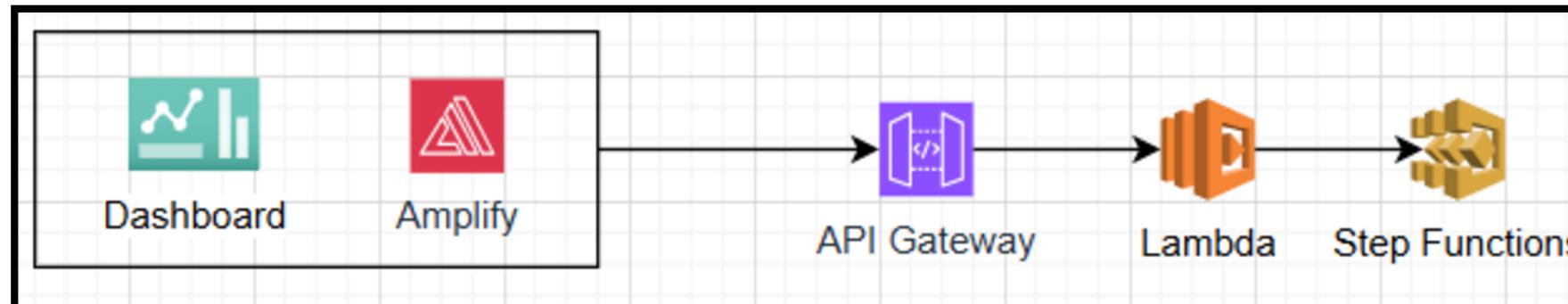
Sau một khoảng thời gian, quá trình patch đã hoàn thành. Các bản vá có thể có trạng thái như sau:

- Already Installed: Bản vá này đã được cập nhật từ trước
- Success: Bản vá đã được cập nhật thành công
- Failed: Bản vá đã thất bại. Bạn có thể nhấn nút bên cạnh để thử vá lại
- Not Available: Bản vá hiện không khả dụng

The screenshot shows a software interface for managing patches. At the top, it displays "Server i-051ca377712f74434" and a progress bar at 100%. Below this, there is a table with two columns: "KB" and "TRẠNG THÁI". The table lists five patches with their corresponding statuses:

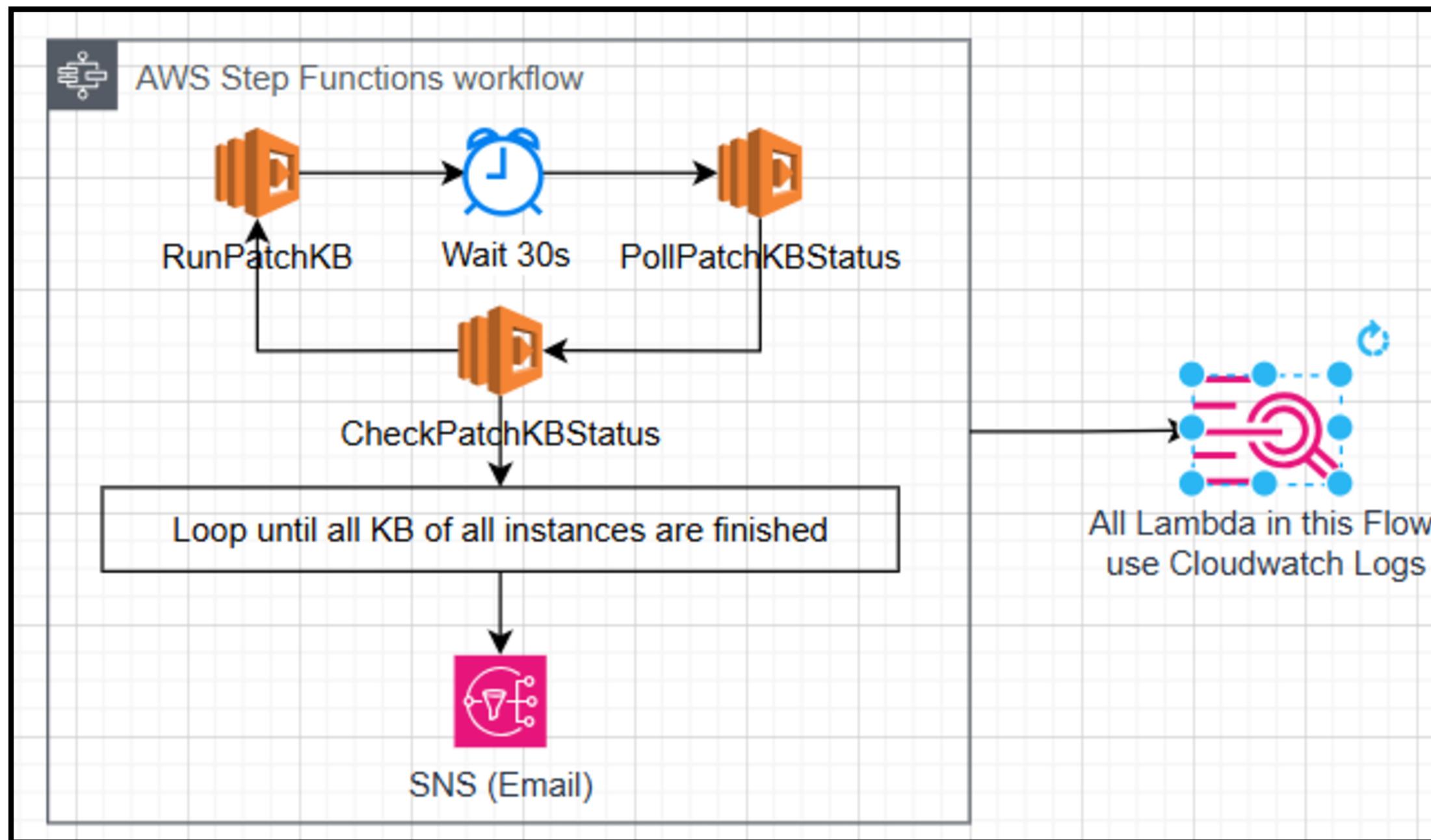
KB	TRẠNG THÁI
KB5060526	✓ Already Installed
KB5060531	✓ Success
KB5062557	✗ Failed Retry Run Patch KB
KB5062572	! Not Available

LUÔNG DỮ LIỆU - RETRY RUN PATCH (KB)



Công việc chính của hàm Lambda:

1. Kích hoạt Step Functions cập nhật single KB cho EC2



GIAO DIỆN CHÍNH

Sẽ có một số KB yêu cầu reboot sau khi patch thành công:

- Admin có thể chọn reboot thủ công bằng cách bấm nút reboot

Server i-0b60544ba4e6e70af
Tiến độ: 100%

KB	TRẠNG THÁI
KB5062572	Success Reboot

Danh sách Server

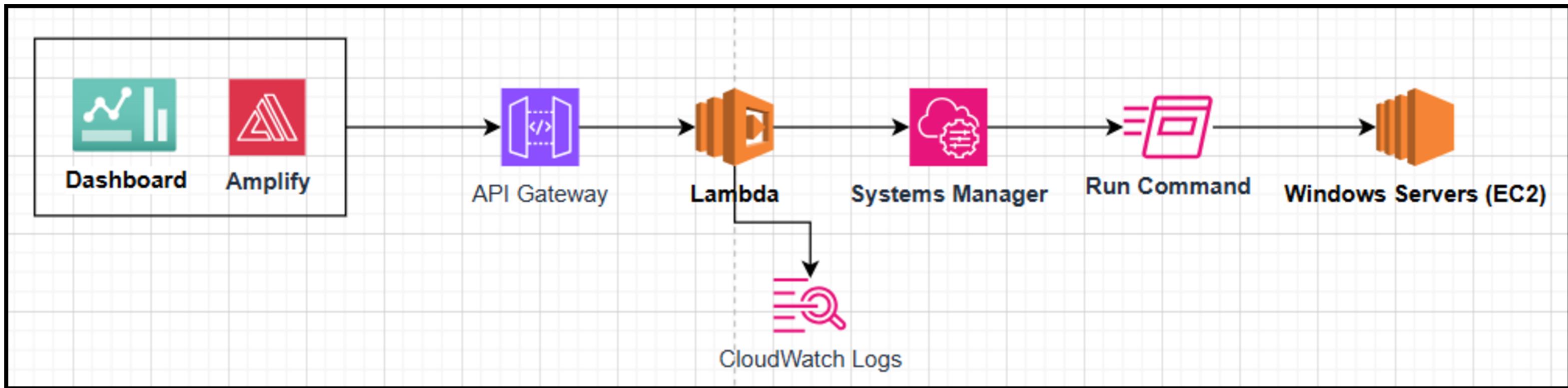
Thông tin chi tiết về các server trong hệ thống

1 / 2 đã chọn [Chọn tất cả](#)

<input type="checkbox"/>	SERVER	OPERATING SYSTEM	IP ADDRESS	AMI	LAST UPDATED
<input type="checkbox"/>	i-0a5ffd86b8a0c781 Active	Windows Server 2019 10.0.17763	172.31.20.230	Windows_Server-2019-English-Full-Base-2025.07.09	04:09:09 18/7/2025
<input checked="" type="checkbox"/>	i-0b60544ba4e6e70af Active	Windows Server 2022 10.0.20348	172.31.16.239	Windows_Server-2022-English-Full-Base-2025.07.09	04:09:09 18/7/2025

[← Cập nhật CVE mới nhất \(1 server\)](#) [↻ Phân tích CVE \(1 server\)](#) [Run Patch KB \(1\)](#) [← Reboot 1 server](#)

LUÔNG DỮ LIỆU - REBOOT SERVER



Công việc chính của hàm Lambda:

1. Kích hoạt SSM (Run Command) reboot EC2
2. Ghi log và trả về kết quả

SUMMARY REPORT

Sau khi hoàn thành việc update KB trên toàn bộ server được chọn, hệ thống sẽ tự động gửi mail cho admin.

Patch Report Summary Thùng rác ×

AWS Notifications <no-reply@sns.amazonaws.com>
đến tôi ▾

17:57 Th 4, 16 thg 7 (2 ngày trước) ⋮

Dịch sang Tiếng Việt X

🔧 Patch Report Summary
⌚ Timestamp: 2025-07-16T10:57:35.306594

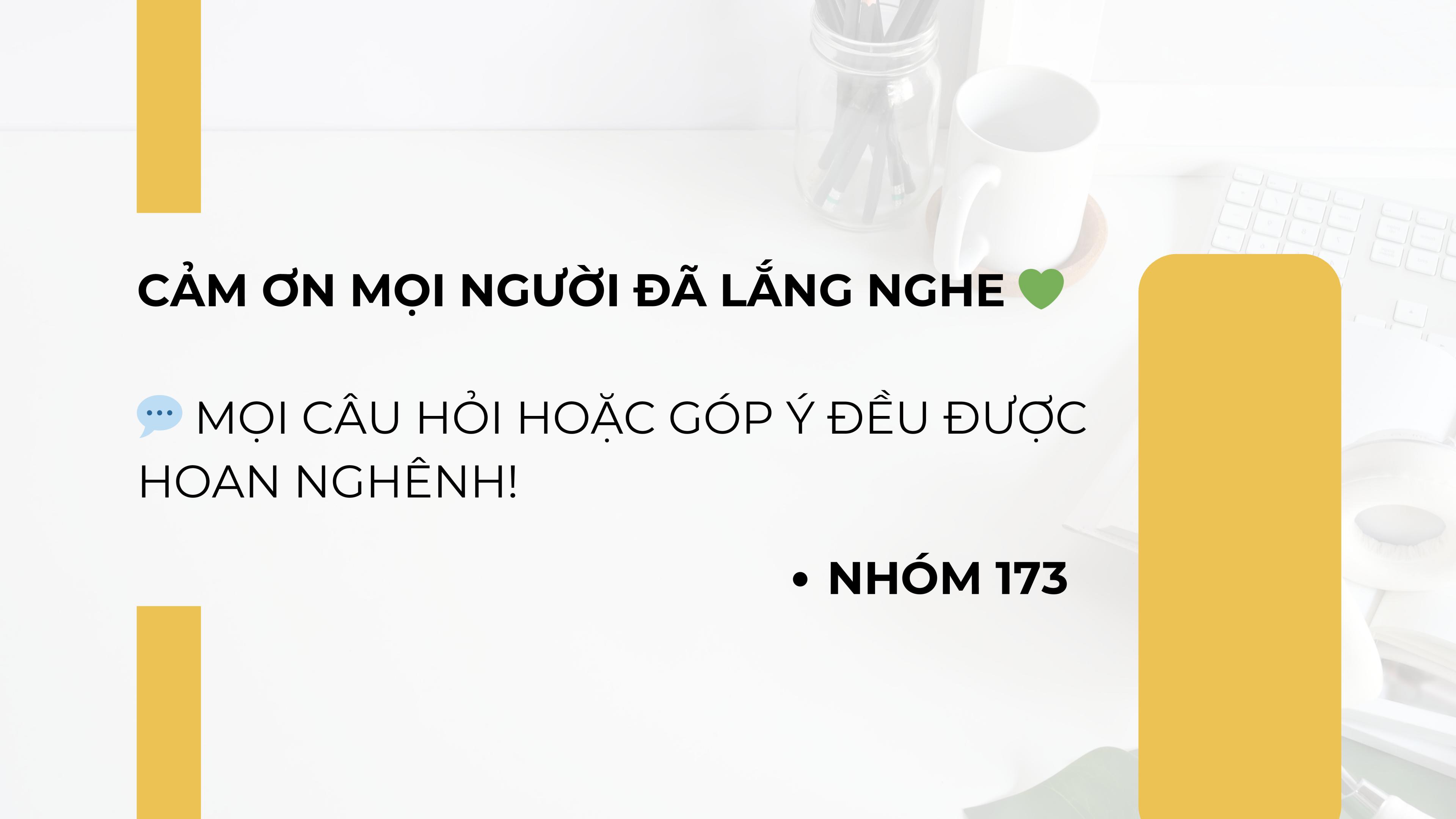
📍 Instance: i-076e21d791777f0e4
1 2 Total Patches: 1
✓ Successful: 1
✗ Failed: 0
🔧 KB Details:
• KB5062557 - Success

🤖 This is an automated patching report.

--

If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
<https://sns.us-east-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-east-1:982035845258:PatchFlowSummary:6cd02e82-17dc-4912-8d51-0f076c0287e8&Endpoint=sontr1023@gmail.com>

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at <https://aws.amazon.com/support>



CẢM ƠN MỌI NGƯỜI ĐÃ LẮNG NGHE ❤

💬 MỌI CÂU HỎI HOẶC GÓP Ý ĐỀU ĐƯỢC
HOAN NGHÊNH!

- NHÓM 173