viettel security

Viettel Endpoint Detection & Response (VCS-aJiant)

Phiên bản 3.3.31 – Ngày cập nhật: 10/10/2022

Tài liệu Hướng dẫn sử dụng

Lịch sử cập nhật

STT	Ngày cập nhật	Phiên bản	Lý do thay đổi	Ghi chú
1	…	3.3.0		
2	30/06/2022	3.3.20	*Bổ sung/ cập nhật hướng dẫn:* *3.7.5 Update management - 174*	
3	10/10/2022	3.3.31	*Bổ sung/ cập nhật hướng dẫn:* *3.5 Anti – Malware – 79*	

Mục lục

Thuật ngữ

Thuật ngữ	Diễn giải	Ghi chú
VCS-aJiant	Tên thương mại của sản phẩm	
IR Flow	Incident Response Flow: luồng vận hành xử lý các Alert, điều tra và phản ứng.	
Artifact	Các đối tượng điều tra liên quan đến Alert như: đường dẫn file/registry/process	
Detection	Phát hiện các đối tượng liên quan đến Alert	
Containment	Quá trình cô lập máy tính: cô lập mạng, suspend tiến trình	
Investigation	Quá trình điều tra: dựa trên các log sự kiện (event logs) hoặc điều tra chủ động bằng công cụ trên máy người dùng. Có các cách điều tra được hỗ trợ sau: - Process Analysis - Tìm kiếm event logs Dùng tool điều tra: autoruns, listdlls	

Thuật ngữ	Diễn giải	Ghi chú
Response	Quá trình phản ứng: từ kết quả điều tra, người vận hành xử lý các kết quả điều tra được bằng các cách: - Response Scenario - LiveResponse	
Timeline	Đường thời gian thể hiện các hoạt động trong IRFlow: - Tạo IR Flow - Tạo/đóng phiên Process Analysis - Tạo/đóng phiên Live Response Đóng IR Flow	

1. GIỚI THIỆU

1.1 Thực trạng hiện nay

Ngày nay, các tổ chức, doanh nghiệp tiếp tục gặp rất nhiều khó khăn với việc phát hiện, xác định, điều tra và giảm thiểu các dạng phần mềm độc hại tiên tiến trong hệ thống. Các công nghệ phòng chống mã độc truyền thống như antivirus dựa trên chữ ký đang bị vượt qua một cách cố ý bởi những kẻ tấn công chuyên nghiệp có trình độ cao với các bộ công cụ tấn công, phần mềm độc hại được tùy chỉnh và hướng mục tiêu cụ thể. Nhiều tổ chức đã thừa nhận rằng các phương pháp phòng thủ chống phần mềm độc hại truyền thống của họ đã thất bại và một chiến lược mới phải được tạo ra để xác định những vi phạm này tại endpoint. Một số lượng đáng kể các vi phạm dữ liệu gần đây từ các dạng phần mềm độc hại nâng cao đã làm tăng sự quan tâm của khách hàng đối với các Giải pháp phát hiện và phản ứng cho lớp endpoint (EDR) mà VCS-aJiant là một trong số đó.

1.2 Sự phát triển của công nghệ

Công nghệ của Giải pháp VCS-aJiant giúp bù đắp các thiếu sót của các công nghệ dựa trên chữ ký mà các tổ chức đang sử dụng như antivirus hay IPS/IDS để cung cấp khả năng phát hiện bất thường dựa trên hành vi và cho cái nhìn sâu hơn về các

thông tin cụ thể có liên quan trên endpoint để phát hiện và giảm thiểu các mối đe dọa nâng cao.

1.3 VCS-aJiant

VCS-aJiant có khả năng cung cấp thông tin chi tiết về việc lây nhiễm phần mềm độc hại và các hành vi mở rộng phạm vi tấn công (lateral movement) của những kẻ tấn công khi chúng thực hiện việc dò quét hoặc sử dụng thông tin bị đánh cắp trong mạng nội bộ đối với các hệ thống và ứng dụng.

Ngoài ra, VCS-aJiant cũng bổ sung cho các công nghệ bảo mật hiện có như giải pháp quản lý sự kiện và thông tin bảo mật (SIEM), các công cụ giám định mạng (Network Forensics) và các thiết bị phòng chống mối đe dọa tiên tiến (Advanced Threat Detection), đồng nghĩa là bổ sung vào danh mục các giải pháp phản ứng sự cố an toàn thông tin của tổ chức.

1.4 Các thông tin nâng cấp

Phiên bản 3.3.0 mang đến các tính năng mới như sau:

- Cải tiến tính năng Login, Process Analysis theo thiết kế giao diện mới, cải thiện trải nghiệm người dùng và bổ sung các thông tin process cần thiết hỗ trợ người dùng trong quá trình điều tra;
- Cải thiện các vấn đề trong phiên bản cũ nhằm đảm bảo tính ổn định.

2. TỔNG QUAN

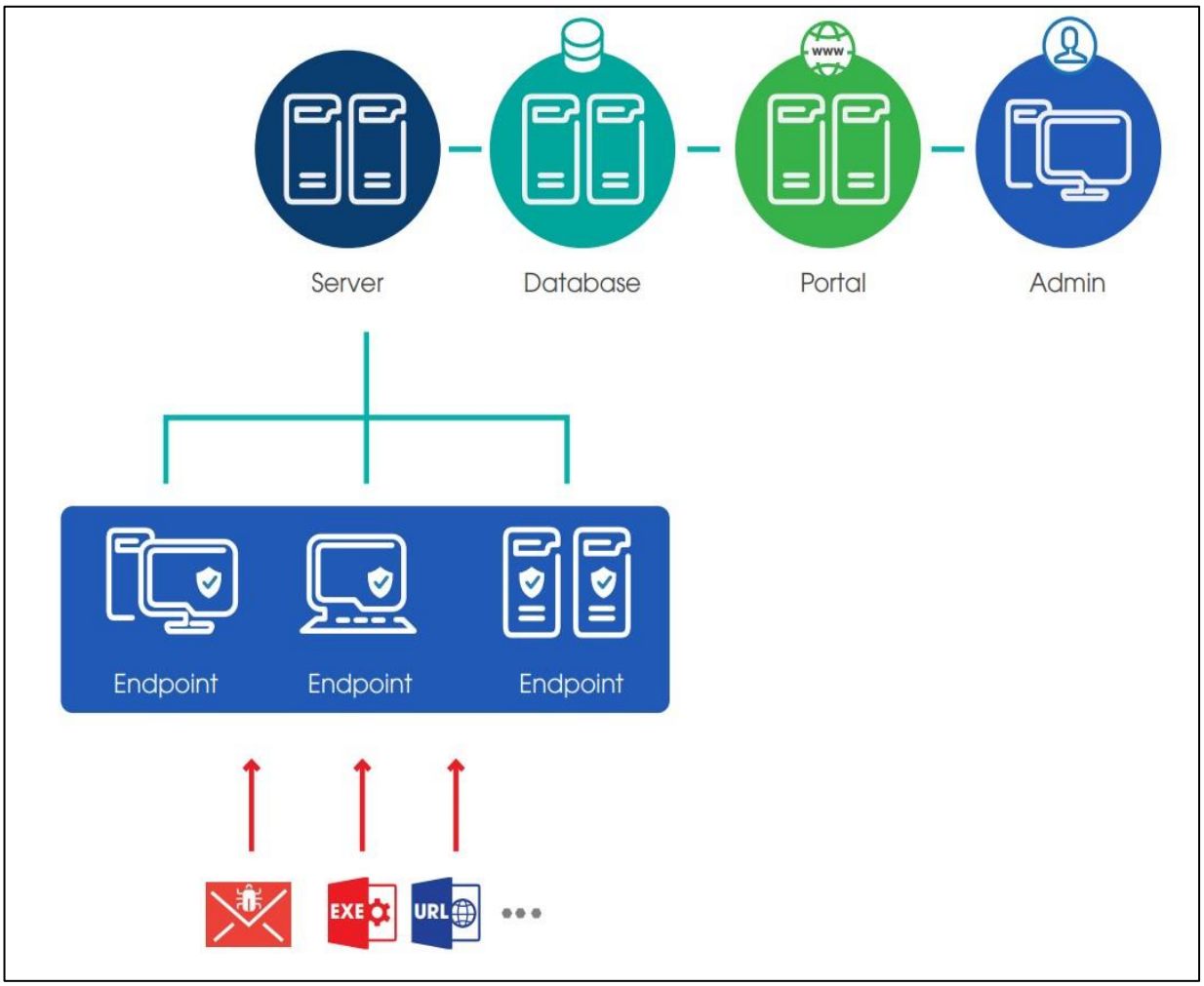
2.1 Công nghệ

VCS-aJiant sử dụng cộng nghệ Filter Driver (cho phép chạy và theo dõi ở mức Kernelbased) thu thập các thông tin bao gồm File, Process, Registry, Network trên máy tính người dùng và server. Các dấu hiệu về file bao gồm (modified, delete, changed attribute), về registry (delete key/value, set value, rename key/value, create key với access nghi ngờ. Các dấu hiệu nghi ngờ về Memory được định kì quét rà soát liên tục. Các hành vi được xác định là nghi ngờ được đẩy về hệ thống Back-end phân tích tập trung;

Luồng nghiệp vụ điều tra tấn công được thiết kế khép kín theo kịch bản incident response (IR Flow), hỗ trợ phát hiện và phân tích các dấu hiện bất thường ngay trên một giao diện duy nhất. Cung cấp các chức năng điều tra (Forensic) sâu trên Endpoint. Hỗ trợ lấy file nghi ngờ (Get Artifact), đẩy công cụ rà quét (Tool Deployment), cho phép thực hiện điều tra, cung cấp bằng chứng theo thời gian thực (Process Analysis, Live Response), cho phép thực hiện phản ứng khi phát hiện mối đe dọa;

Ngay khi xác minh được bất thường, Endpoint cung cấp các công cụ gỡ bỏ mã độc trên diện rộng (Response Scenario) bao gồm: cô lập mạng máy bị nhiễm (network containment), kill process, delete file/registry.

2.2 Kiến trúc hạ tầng



Có 3 thành phần chính:

- **Agent**: Là thành phần được cài đặt trên từng máy trạm, máy chủ, có nhiệm vụ giám sát các dấu hiệu bất thường trên các máy trạm, máy chủ, gửi log về máy chủ quản trị tập trung;
- **Cụm máy chủ quản trị, xử lý tập trung và lưu trữ**: Là thành phần xử lý dữ liệu được gửi về từ các agent, đóng vai trò chính trong việc phân tích và xử lý dữ liệu theo thời gian thực;
- **Giao diện Web-Portal:** Là thành phần mà người quản trị sẽ sử dụng để theo dõi, giám sát và phân tích các thông tin của hệ thống.

2.3 Làm việc với giao diện quản trị

Giao diện Web-portal bao gồm các giao diện chức năng và các luồng xử lý như sau:

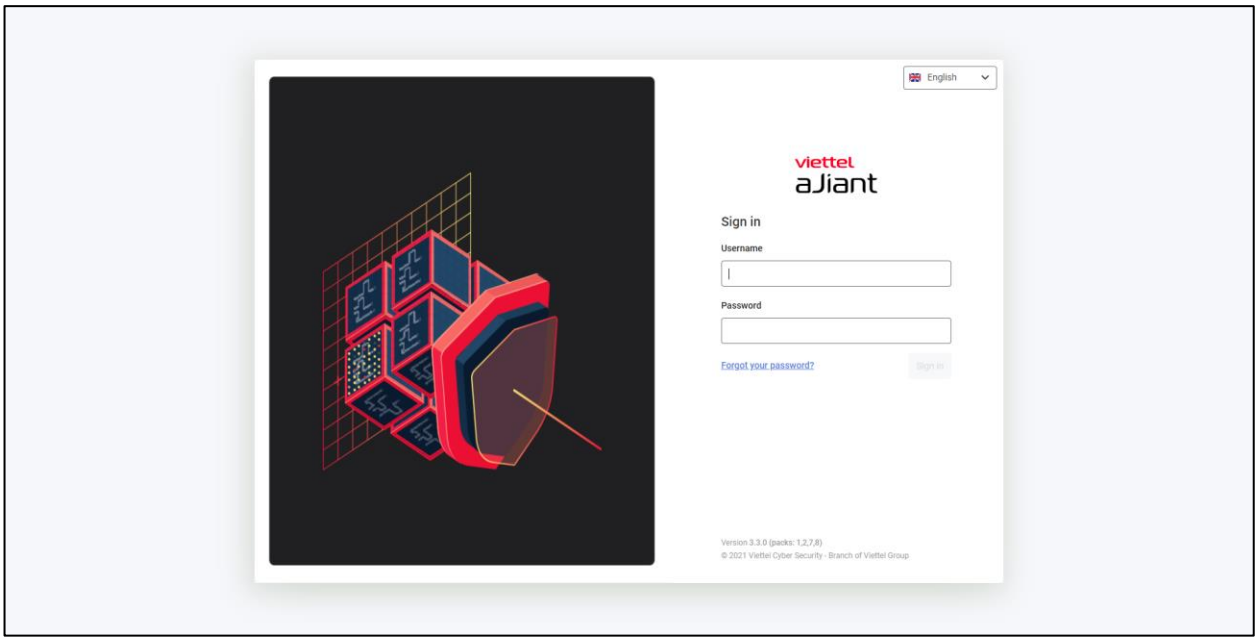
- Dashboard: thống kê, biểu đồ trực quan về tình hình an toàn thông tin của tổ chức;
- Alert management: danh sách các alert về các dấu hiệu xuất hiện mã độc trên máy người dùng;
- IR flow management: danh sách các IR flow được tạo bởi người quản trị trong quá trình điều tra. Luồng xử lý bao gồm: Detection, Containment, Investigation, Response;
- Investigation: danh sách các công cụ phục vụ điều tra (Process Analysis, Event search và Deploy tools);
- Response: danh sách các công cụ phục vụ phản ứng, xử lý sự cố (Live response);
- Protect & Prevention: danh sách các tính năng phòng chống và bảo vệ máy trạm (Application control và Endpoint firewall);
- Setting: danh sách các chức năng cài đặt hệ thống (Policy management, Agent management, Group management, Rule correlation và Account management: User, Role, Permission management);

3. HƯỚNG DẪN SỬ DỤNG

A. Giao diện web Portal

3.1 Đăng nhập

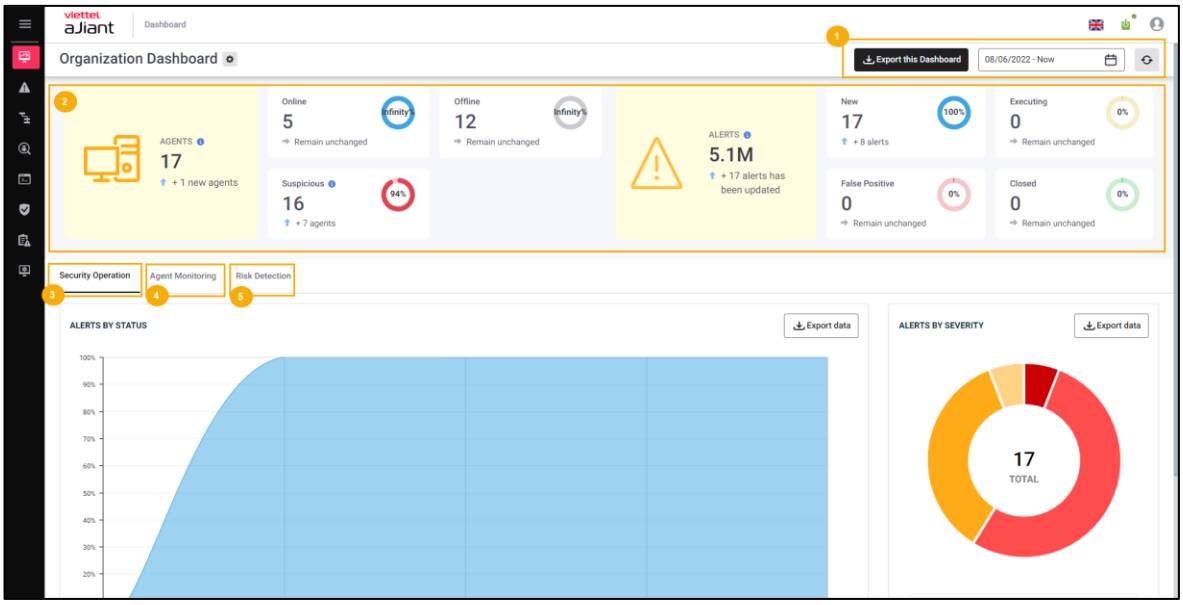
Bước 1: Truy cập vào hệ thống tại địa chỉ được cung cấp;



Bước 2: Đăng nhập với user/pass được cấp;

3.2 Dashboard VCS-aJiant

Các tính năng chính gồm có:



1 – Các thao tác với dữ liệu trên Dashboard:

+ Trích xuất dữ liệu trên dashboard;

+ Tìm kiếm dữ liệu tối đa 90 ngày gần đây;

+ Làm mới dữ liệu.

2 – Overview: Thống kê tổng quan tình hình an toàn thông tin tổ chức (thông qua trạng thái agents và Alerts);

3 – Security Operation: Theo dõi tình hình vận hành an toàn thông tin (thông qua việc theo dõi vận hành Alert);

4 – Agent Monitoring: Theo dõi tình hình cài đặt và trạng thái agents;

5 – Risk Detection: Theo dõi các mối nguy hại đến tổ chức (thông qua việc thống kê các đối tượng phát sinh nhiều Alert chưa xử lý nhất hệ thống);

- Phân quyền dữ liệu tại tính năng như sau:

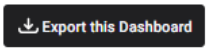
+ User đăng nhập thuộc group root: Hiển thị dữ liệu toàn bộ hệ thống;

+ User đăng nhập thuộc group cấp 1: Hiển thị dữ liệu tại toàn bộ group cấp 1 và các group con trực thuộc;

+ User đăng nhập thuộc group cấp 2 trở đi : Hiển thị dữ liệu tại toàn bộ group cấp 1 chứa group của user đang đăng nhập và các group con trực thuộc group cấp 1 tương ứng.

3.2.1 Thao tác với dữ liệu

3.2.1.1 *Xuất dữ liệu*

- Mục đích: Cho phép trích xuất dữ liệu hiện có trên giao diện dashboard bằng cách chọn 

, ngoài ra bổ sung các sheet dữ liệu chi tiết hỗ trợ báo cáo;

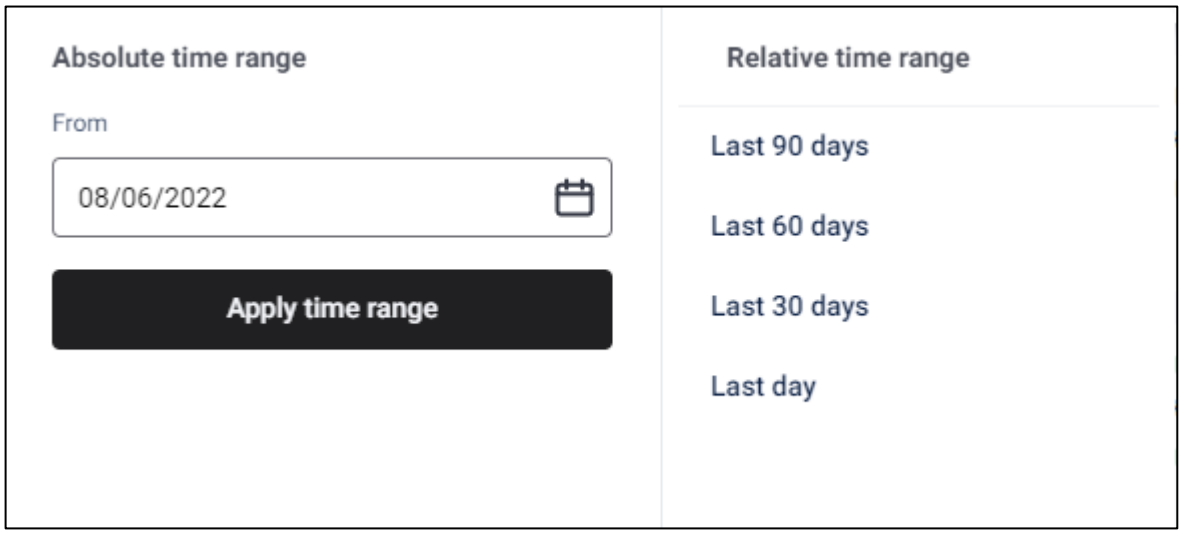
+ Trường hợp lỗi kết nối hoặc không có dữ liệu trên toàn bộ các thành phần của Dashboard, không hỗ trợ trích xuất, thao tác sẽ bị ẩn đi;

+ Trường hợp có dữ liệu, hỗ trợ xuất file định dạng .xlsx;

3.2.1.2 *Tìm kiếm theo ngày*

- Cho phép điều chỉnh khoảng thời gian cần theo dõi tình hình an toàn thông tin tính đến thời điểm hiện tại, mặc định tính từ ngày trước đó (Last day);

+ Để chọn thời điểm bắt đầu của khoảng thời gian cần theo dõi, có thể chọn thời gian tuyệt đối hoặc tương đối:



- Thời gian tuyệt đối: Là giá trị ngày bắt đầu cụ thể, hỗ trợ tối đa 90 ngày kể từ hiện tại;

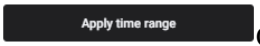
VD: Hiện tại là 03 giờ sáng ngày 07/06/2021, lựa chọn ngày bắt đầu = “06/06/2021”.

→ Khoảng thời gian theo dõi: 00:00 06/06/2021 đến 03:00 06/07/2021.

- Thời gian tương đối: Là khoảng thời gian tương đối giữa ngày bắt đầu và hiện tại.

VD: Hiện tại là 03 giờ sáng ngày 07/06/2021, lựa chọn ngày bắt đầu = “Last 30 days”. Hệ thống tự động tìm ngược lại 30 ngày trước và bắt đầu tính từ 00:00 của ngày đó.

→ Khoảng thời gian theo dõi: 00:00 08/05/2021 đến 03:00 07/06/2021.

+ Sau khi chọn khoảng thời gian muốn theo dõi, chọn 

để tải lại dữ liệu tương ứng.

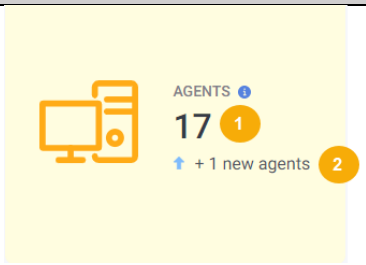
3.2.1.3 *Làm mới dữ liệu*

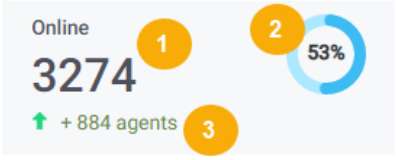
- Mục đích: Cho phép làm mới dữ liệu thủ công, chọn  để cập nhật dữ liệu mới nhất tính đến thời điểm hiện tại.

3.2.2 Thống kê Overview

- Mục đích: Cho phép thống kê nhanh về tình hình an toàn thông tin trên tổ chức theo khoảng thời gian đã chọn trong phần tìm kiếm;

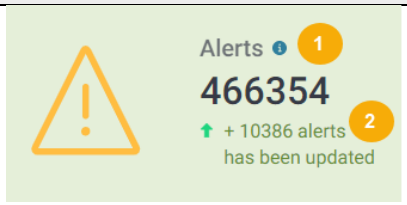
+ Thống kê liên quan đến agents:

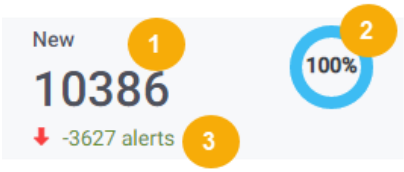
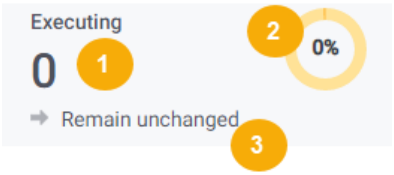
Số thống kê	***Ý nghĩa***
	Bao gồm 02 chỉ số: 1 – Tổng số máy đã cài đặt agent trên hệ thống (không phụ thuộc khoảng thời gian tìm kiếm);

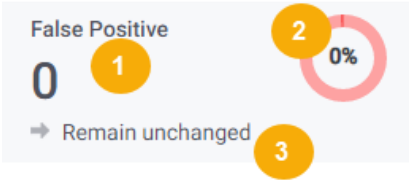
	2 – Tổng số máy mới cài đặt agent trong khoảng thời gian tìm kiếm; (+: Máy mới cài đặt, Remain unchanged: Không có máy mới cài đặt trong khoảng thời gian tìm kiếm)
	Bao gồm 03 chỉ số: 1 – Trung bình số máy Online trong khoảng thời gian tìm kiếm (chỉ tính thời gian làm việc trong giờ hành chính 08:00 – 18:00); 2 – Tỷ lệ máy Online trung bình so với toàn hệ thống; 3 – Số lượng máy Online trung bình chênh lệch so với chu kỳ trước. (+: Số lượng máy Online trung bình tăng so với giai đoạn trước, Remain unchanged: Không có chênh lệch)
	Bao gồm 03 chỉ số 1 – Trung bình số máy Offline trong khoảng thời gian tìm kiếm (chỉ tính thời gian làm việc trong giờ hành chính 08:00 – 18:00); 2 – Tỷ lệ máy Offline trung bình so với toàn hệ thống; 3 – Số lượng máy Offline trung bình chênh lệch so với chu kỳ trước.

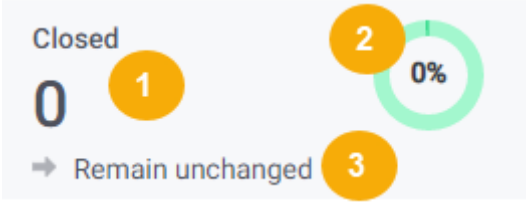
	(+: Số lượng máy Offline trung bình tăng so với giai đoạn trước, Remain unchanged: Không có chênh lệch)
	Bao gồm 03 chỉ số: 1 – Tổng số máy đã cài đặt agent trên hệ thống (không phụ thuộc khoảng thời gian tìm kiếm) có phát sinh Alert chưa được xử lý; 2 – Tỷ lệ máy có phát sinh Alert so với số lượng máy trên toàn hệ thống (không phụ thuộc thời gian tìm kiếm); 3 – Tổng số máy có phát sinh Alert trong khoảng thời gian tìm kiếm. (+: Máy mới phát sinh Alert, Remain unchanged: Không có máy mới phát sinh Alert trong khoảng thời gian tìm kiếm)

+ Thống kê liên quan đến Alerts:

Số thống kê	Ý nghĩa
	Bao gồm 02 chỉ số: 1 – Tổng số Alert trên toàn bộ hệ thống (không phụ thuộc khoảng thời gian tìm kiếm); 2 – Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm;

	(+: Alert mới phát sinh, Remain unchanged: Không có Alert mới phát sinh trong khoảng thời gian tìm kiếm)
	Bao gồm 03 chỉ số: 1 – Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = NEW; 2 – Tỷ lệ Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = NEW so với toàn bộ Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm; 3 – Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = NEW chênh lệch so với chu kỳ trước. (+: Tổng số Alert mới tăng so với giai đoạn trước, Remain unchanged: Tổng số Alert mới không thay đổi so với giai đoạn trước)
	Bao gồm 03 chỉ số: 1 – Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái <>

	(NEW, FALSE POSITIVE, CLOSED); 2 – Tỷ lệ Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái <> (NEW, FALSE POSITIVE, CLOSED) so với toàn bộ Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm; 3 – Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái <> (NEW, FALSE POSITIVE, CLOSED) chênh lệch so với chu kỳ trước. (+: Tổng số Alert tăng so với giai đoạn trước, Remain unchanged: Tổng số Alert không thay đổi so với giai đoạn trước)
	Bao gồm 03 chỉ số: 1 – Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = CLOSED; 2 – Tỷ lệ Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = CLOSED so với toàn bộ Alert mới

	phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm; 3 – Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = CLOSED chênh lệch so với chu kỳ trước. (+: Tổng số Alert tăng so với giai đoạn trước, Remain unchanged: Tổng số Alert không thay đổi so với giai đoạn trước)
	Bao gồm 03 chỉ số: 1 – Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = FALSE POSITIVE; 2 – Tỷ lệ Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = FALSE POSITIVE so với toàn bộ Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm; 3 – Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = FALSE POSITIVE chênh lệch so với chu kỳ trước.

	(+: Tổng số Alert tăng so với giai đoạn trước, Remain unchanged: Tổng số Alert không thay đổi so với giai đoạn trước)

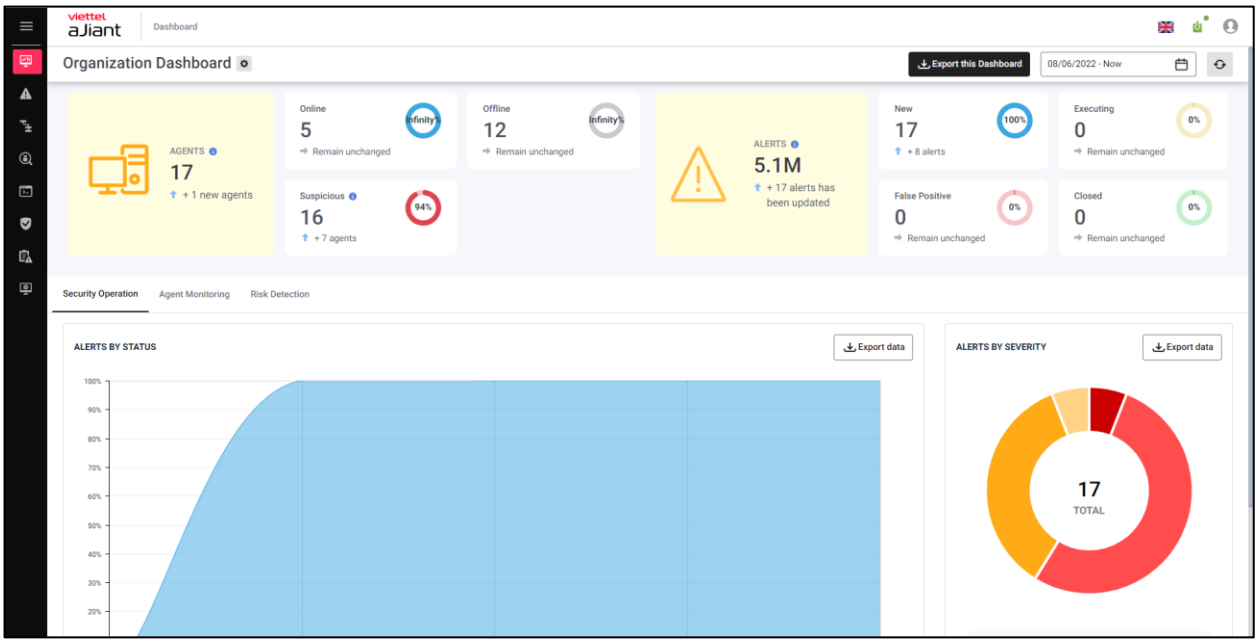
3.2.3 Theo dõi Security Operation

- Mục đích: Cho phép theo dõi tình hình vận hành an toàn thông tin (thông qua việc theo dõi vận hành Alert) theo khoảng thời gian đã chọn trong phần tìm kiếm:

+ Thống kê tình trạng xử lý Alert theo trạng thái;

+ Thống kê Alert theo mức độ nguy hại;

+ Trích xuất dữ liệu tương ứng trong các biểu đồ;

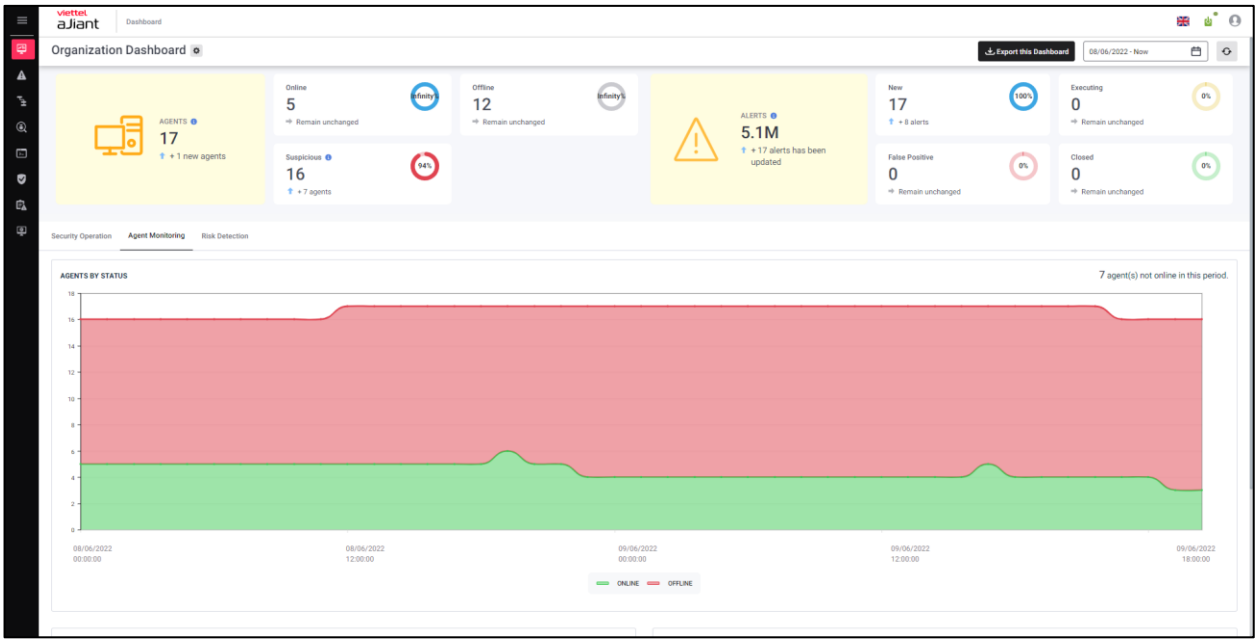


Biểu đồ/thống kê	*Ý nghĩa*
Alert by status	Biểu đồ miền - Theo dõi tình hình ghi nhận các Alert mới ghi nhận hoặc có cập nhật trong khoảng thời gian tìm kiếm, bao gồm: - Trục x: thời gian; - Trục y: Tỷ lệ Alert phân chia theo 04 nhóm trạng thái = (New, Executing, Closed, False Positive); - Cho phép chọn Export data để tải về danh sách Alert sắp xếp theo trạng thái.
Alert by severity	- Biểu đồ tròn - Theo dõi tình hình ghi nhận Alert mới ghi nhận hoặc có cập nhật theo mức độ nguy hiểm trong khoảng thời gian tìm kiếm, bao gồm: - Tỷ lệ: tỷ lệ Alert tại từng mức độ nguy hiểm; - Tại giữa biểu đồ hiển thị tổng số Alert mới hoặc có cập nhật trong khoảng thời gian; - Cho phép chọn Export data để tải về danh sách Alert sắp xếp theo mức độ nguy hiểm.

3.2.4 Theo dõi Agent Monitoring

- Mục đích: Cho phép thống kê agents theo trạng thái và thông tin hệ điều hành theo khoảng thời gian đã chọn trong phần tìm kiếm:

+ Thống kê trạng thái agent (Trực tuyến, ngoại truyến);
+ Thống kê agent theo hệ điều hành, phiên bản hệ điều hành;
+ Trích xuất dữ liệu thông tin agent;



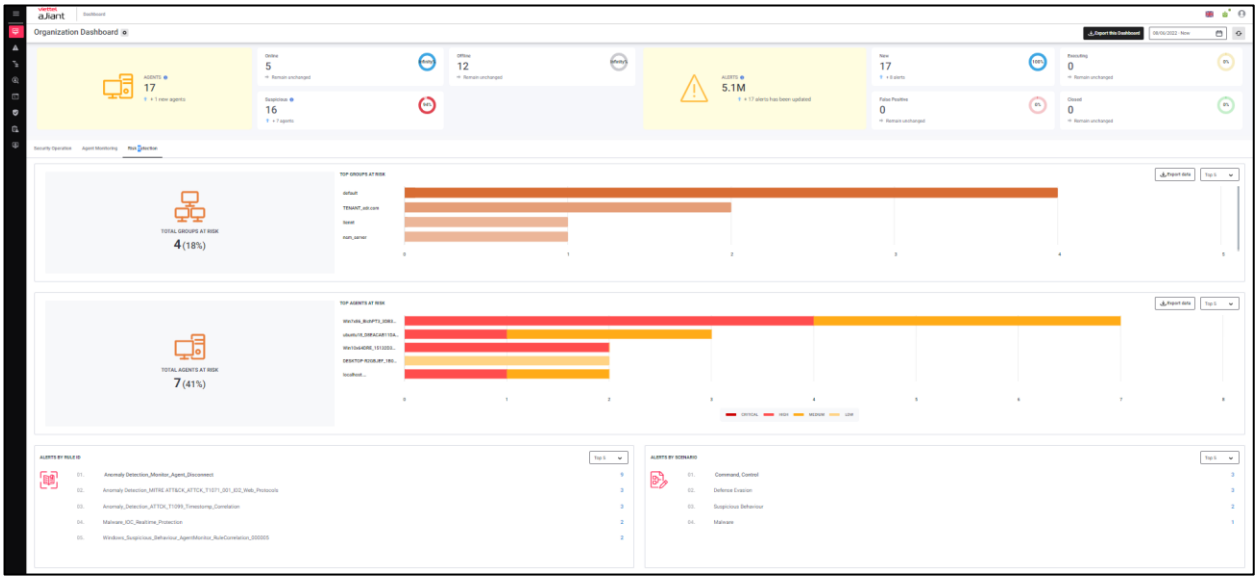
Biểu đồ/thống kê	***Ý nghĩa***
Agent by status	- Biểu đồ miền- Theo dõi tình hình ghi nhận máy theo trạng thái (Online/Offline) trong chu kỳ báo cáo tính đến thời điểm hiện tại, bao gồm: - Trục y: Tỷ lệ máy phân chia theo 02 nhóm status (Online, Offline); - Trục x: thời gian thống kê; - Hiển thị số lượng máy không online lần nào (trong trường hợp máy quá 30 ngày không online, tự động không ghi nhận máy).
Agent by operation system	Biểu đồ tròn - Theo dõi tình hình ghi nhận máy theo OS, bao gồm: - Tỷ lệ: tỷ lệ máy tại từng OS; - Phần ghi chú liệt kê danh sách các hệ điều hành: Windows, MacOS, Linux, các hệ điều hành khác;

	- Cho phép chọn Export data để tải về danh sách máy sắp xếp theo thông tin hệ điều hành.
Agent by OS version	Thống kê top phiên bản hệ điều hành cài đặt trên máy nhiều nhất; - Cho phép thay đổi khoảng thống kê: Top 5, Top 10, Top 20, Top 50. Mặc định chọn Top 5.

3.2.5 Theo dõi Risk Detection

- Cho phép theo dõi các mối nguy hại đến tổ chức (thông qua việc thống kê các đối tượng phát sinh nhiều Alert chưa xử lý nhất hệ thống):

+ Thống kê top các nhóm phát sinh nhiều Alert nhất;
+ Thống kê top agent phát sinh nhiều Alert nhất;
+ Thống kê top các ruleid và scenario phát sinh nhiều cảnh bsao nhất;
+ Trích xuất dữ liệu thông tin theo đối tượng nguy hại;



Biểu đồ/thống kê	*Ý nghĩa*
Total groups at risk	Tổng số nhóm có chứa máy tính phát sinh Alert mới ghi nhận hoặc có cập nhật (không kể Alert false positive và closed, không kể nhóm đã bị xóa) trong thời gian tìm kiếm; Tỷ lệ nhóm khả nghi so với toàn bộ nhóm trên hệ thống (không kể nhóm đã bị xóa).
Top groups at risk	Biểu đồ cột – thống kê top nhóm có chứa nhiều máy tính phát sinh nhiều Alert mới ghi nhận hoặc có cập nhật nhất (không kể Alert false positive và closed, không kể nhóm đã bị xóa) trong thời gian tìm kiếm; - Trục x: số lượng máy phát sinh nhiều Alert tại từng nhóm; - Trục y: tên nhóm tương ứng; - Cho phép thay đổi khoảng thống kê: Top 5, Top 10, Top 20, Top 50. Mặc định chọn Top 5; - Cho phép chọn  để tải về danh sách nhóm máy tính phát sinh Alert.
Total agents at risk	Tổng số máy tính phát sinh Alert mới ghi nhận hoặc có cập nhật (không kể Alert false positive và closed, không kể máy tính đã không hoạt động quá 30 ngày gần đây) trong thời gian tìm kiếm; Tỷ lệ máy khả nghi so với toàn bộ máy trên hệ thống (không kể máy tính đã không hoạt động quá 30 ngày gần đây).
Top agents at risk	Biểu đồ cột – thống kê top máy tính phát sinh nhiều Alert mới ghi nhận hoặc có cập nhật nhất (không kể

	Alert false positive và closed) trong thời gian tìm kiếm; - Trục x: số lượng Alert tại từng host, phân chia rõ tỷ lệ theo severity = (Critical, High, Medium, Low) - Trục y: tên máy tương ứng; - Cho phép thay đổi khoảng thống kê: Top 5, Top 10, Top 20, Top 50. Mặc định chọn Top 5; - Cho phép chọn  để tải về danh sách máy tính phát sinh Alert.
Alerts by RuleID	Thống kê top rule Id phát sinh nhiều Alert mới ghi nhận hoặc có cập nhật nhất trong thời gian tìm kiếm; - Cho phép thay đổi khoảng thống kê: Top 5, Top 10, Top 15, Top 20. Mặc định chọn Top 5.
Alerts by scenarios	Thống kê top Scenario phát sinh nhiều Alert mới ghi nhận hoặc có cập nhật nhất trong chu kỳ báo cáo tính đến thời điểm hiện tại: Cho phép thay đổi khoảng thống kê: Top 5, Top 10, Top 15, Top 20. Mặc định chọn Top 5

3.3 Dashboard Anti-malware

- Chức năng cung cấp các biểu đồ trực quan phục vụ theo dõi tình hình an toàn thông tin của tổ chức thông qua số liệu liên quan đến việc tiêu diệt mã độc;

- Các tính năng chính gồm có:

4 – Các thao tác với dữ liệu trên Dashboard:

+ Trích xuất dữ liệu trên dashboard;

+ Tìm kiếm dữ liệu tối đa 90 ngày gần đây.

Làm mới dữ liệu;

5 – Overview: Thống kê tổng quan tình hình an toàn thông tin tổ chức (thông qua trạng thái devices và threats);

6 – Risk Detection: Theo dõi các mối nguy hại đến tổ chức (thông qua việc thống kê các đối tượng phát sinh nhiều mã độc nhất hệ thống).

- Phân quyền dữ liệu tại tính năng như sau: Cho phép hiển thị toàn bộ dữ liệu, không phân theo đơn vị.

3.3.1 *Thao tác với dữ liệu*

3.3.1.1 *Xuất dữ liệu*

- Cho phép trích xuất dữ liệu hiện có trên giao diện dashboard bằng cách chọn 

, ngoài ra bổ sung các sheet dữ liệu chi tiết hỗ trợ báo cáo:

+ Trường hợp lỗi kết nối hoặc không có dữ liệu trên toàn bộ các thành phần của Dashboard, không hỗ trợ trích xuất, thao tác sẽ bị ẩn đi;

+ Trường hợp có dữ liệu, hỗ trợ xuất file định dạng .xlsx

3.3.1.2 *Tìm kiếm theo ngày*

- Cho phép điều chỉnh khoảng thời gian cần theo dõi tình hình an toàn thông tin tính đến thời điểm hiện tại, mặc định tính từ ngày trước đó (Last day):

+ Để chọn thời điểm bắt đầu của khoảng thời gian cần theo dõi, có thể chọn thời gian tuyệt đối hoặc tương đối:

- Thời gian tuyệt đối: Là giá trị ngày bắt đầu cụ thể, hỗ trợ tối đa 90 ngày kể từ hiện tại.

VD: Hiện tại là 03 giờ sáng ngày 07/06/2021, lựa chọn ngày bắt đầu = “06/06/2021”

→ Khoảng thời gian theo dõi: 00:00 06/06/2021 đến 03:00 06/07/2021.

- Thời gian tương đối: Là khoảng thời gian tương đối giữa ngày bắt đầu và hiện tại.

VD: Hiện tại là 03 giờ sáng ngày 07/06/2021, lựa chọn ngày bắt đầu = “Last 30 days”. Hệ thống tự động tìm ngược lại 30 ngày trước và bắt đầu tính từ 00:00 của ngày đó.

→ Khoảng thời gian theo dõi: 00:00 08/05/2021 đến 03:00 07/06/2021.

+ Sau khi chọn khoảng thời gian muốn theo dõi, chọn 

để tải lại dữ liệu tương ứng.

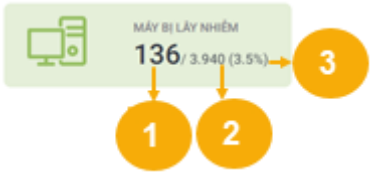
3.3.1.3 *Làm mới dữ liệu*

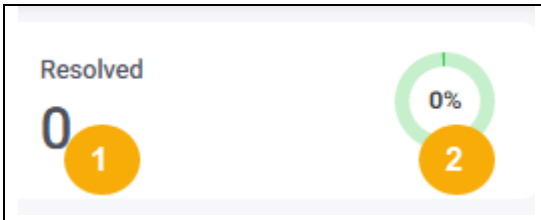
- Cho phép làm mới dữ liệu thủ công, chọn  để cập nhật dữ liệu mới nhất tính đến thời điểm hiện tại.

3.3.2 Thống kê Overview

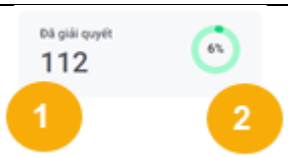
- Cho phép thống kê nhanh về tình hình an toàn thông tin trên tổ chức theo khoảng thời gian đã chọn trong phần tìm kiếm

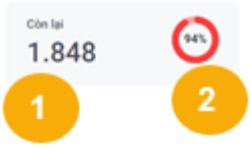
+ Thống kê liên quan đến agents:

Số thống kê	*Ý nghĩa*
	Bao gồm 03 chỉ số 1 – Tổng số máy bị lây nhiễm trên hệ thống trong khoảng thời gian tìm kiếm 2 – Tổng số máy cài đặt agent trong hệ thống (***không kể thời gian tìm kiếm***) 3 – Tỷ lệ máy bị lây nhiễm so với toàn bộ máy cài đặt agent trong hệ thống

	Bao gồm 02 chỉ số: 1 – Tổng số máy bị lây nhiễm trên hệ thống đã được xử lý thành công 2 – Tỷ lệ máy bị lây nhiễm được xử lý thành công so với toàn bộ máy bị lây nhiễm trên hệ thống.
	Bao gồm 02 chỉ số: 1 – Tổng số máy bị lây nhiễm trên hệ thống chưa được xử lý thành công 2 – Tỷ lệ máy bị lây nhiễm chưa được xử lý thành công so với toàn bộ máy bị lây nhiễm trên hệ thống

+ Thống kê liên quan đến alerts

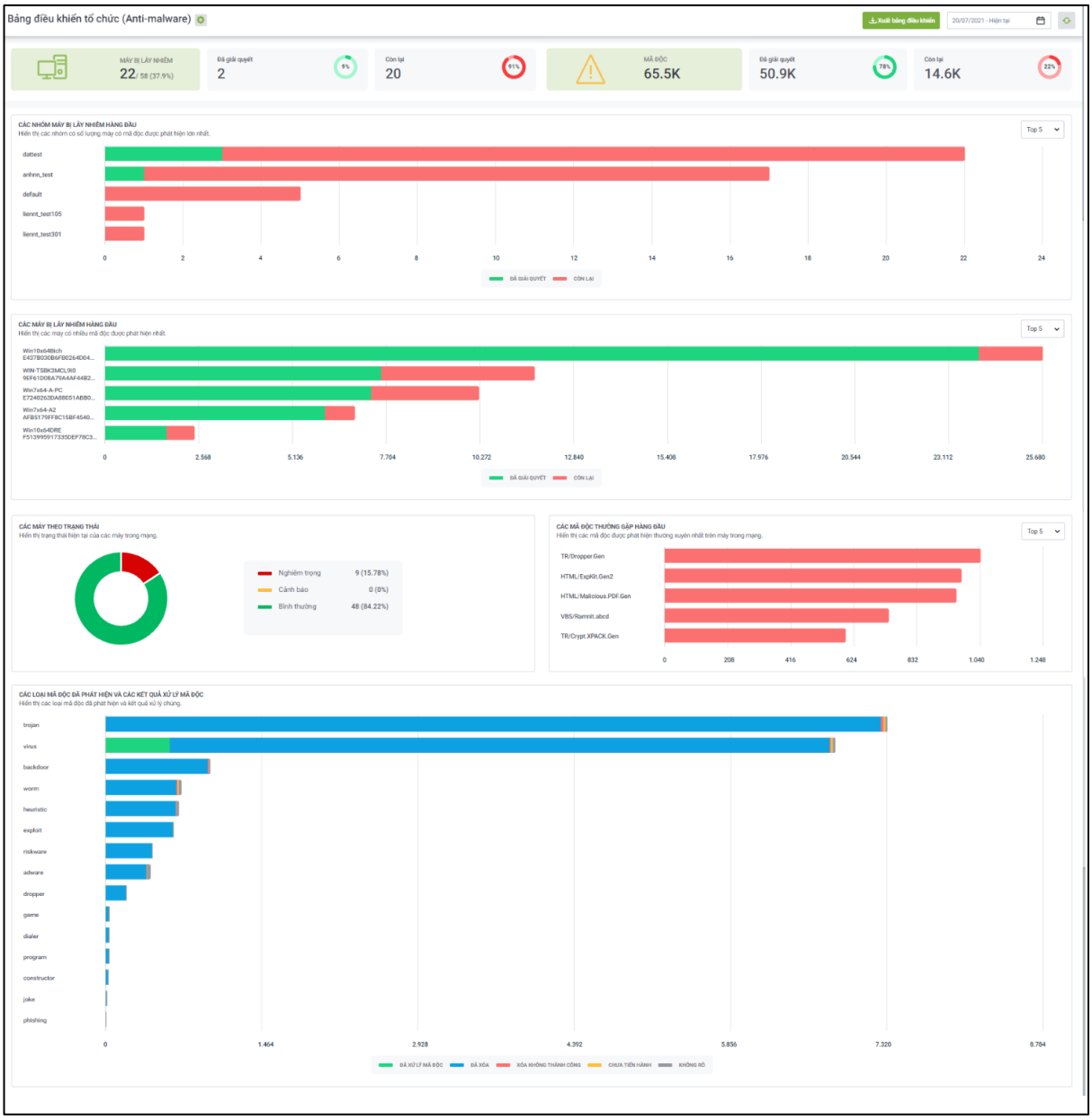
Số thống kê	***Ý nghĩa***
	Bao gồm 01 chỉ số: 1 – Tổng số mã độc ghi nhận trên toàn bộ hệ thống
	Bao gồm 02 chỉ số: 1 – Tổng số mã độc trên hệ thống đã được xử lý thành công; 2 – Tỷ lệ mã độc đã được xử lý thành công so với toàn bộ mã độc ghi nhận trên hệ thống.

	Bao gồm 02 chỉ số: 1 – Tổng số mã độc trên hệ thống chưa được xử lý thành công; 2 – Tỷ lệ mã độc trên hệ thống chưa được xử lý thành công so với toàn bộ mã độc ghi nhận trên hệ thống;

3.3.3 Theo dõi Risk Detection

- Cho phép theo dõi các mối nguy hại đến tổ chức (thông qua việc thống kê các đối tượng nhiễm mã độc nhiều nhất hệ thống):

+ Thống kê top các nhóm bị lây nhiễm;
+ Thống kê top các máy bị lây nhiễm;
+ Thống kê máy theo trạng thái;
+ Thống kê các mã độc thường gặp;
+ Thống kê tình trạng xử lý virus;



Biểu đồ/thống kê	***Ý nghĩa***
Top infected device groups	- Biểu đồ cột liệt kê nhóm máy có nhiều máy lây nhiễm mã độc nhất trong thời gian tìm kiếm tính đến thời điểm hiện tại: - Trục x: số lượng máy lây nhiễm mã độc tại từng nhóm theo trạng thái xử lý (Resolved - máy có

	toàn bộ mã độc đã xử lý và Remain - máy có ít nhất 01 mã độc chưa xử lý xong); - Trục y: Tên nhóm máy tương ứng; - Cho phép thay đổi khoảng thống kê: Top 5, Top 10, Top 20, Top 50. Mặc định chọn Top 5
Top infected devices	Biểu đồ cột liệt kê máy bị lây nhiễm mã độc nhiều nhất trong thời gian tìm kiếm tính đến thời điểm hiện tại: - Trục x: số lượng mã độc lây nhiễm theo trạng thái xử lý (Resolved và Remain); - Trục y: Tên máy tương ứng; - Cho phép thay đổi khoảng thống kê: Top 5, Top 10, Top 20, Top 50. Mặc định chọn Top 5.
Devices by status	Biểu đồ tròn - Theo dõi tình hình máy trong hệ thống theo trạng thái tại thời điểm hiện tại, bao gồm: - Tỷ lệ: Tỷ lệ máy tại từng trạng thái so với tổng số toàn bộ máy.
Top frequent threats	Biểu đồ cột liệt kê mã độc lây nhiễm nhiều nhất trong thời gian tìm kiếm tính đến thời điểm hiện tại: - Trục x: số lượng mã độc phát sinh; - Trục y: Tên loại mã độc; - Cho phép thay đổi khoảng thống kê: Top 5, Top 10, Top 20, Top 50. Mặc định chọn Top 5.
Types of detected viruses and disinfected results	Biểu đồ cột liệt kê virus xuất hiện trong thời gian tìm kiếm tính đến thời điểm hiện tại (sắp xếp theo số lượng virus giảm dần): - Trục x: số lượng virus phát sinh theo trạng thái xử lý;

	- Trục y: Tên virus

3.4 Màn hình Setting

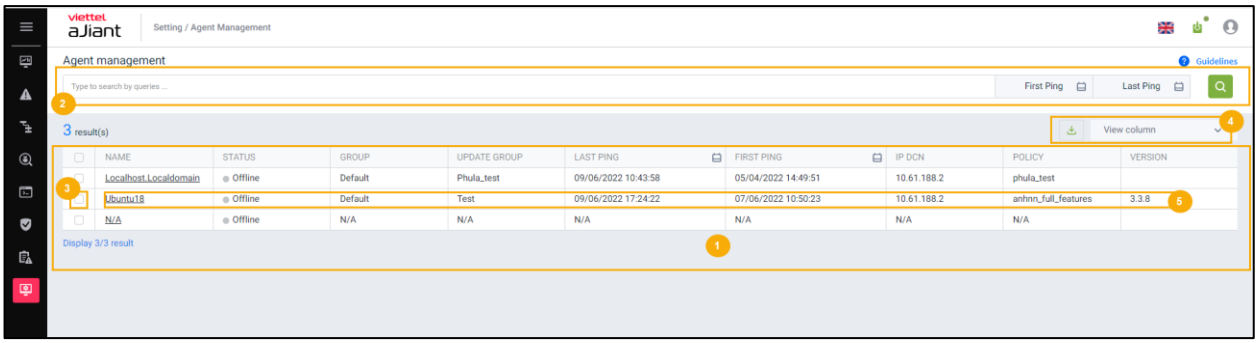
3.4.1 Agent Management

- Mục đích: Chức năng Agent Management hỗ trợ người quản trị quản lý các agent đã cài đặt bao gồm:

+ Xem danh sách các agent và các thông tin chung;

+ Xem chi tiết của Agent;

+ Chọn nhanh các agent và thiết lập một số cài đặt (policy, update group);



- Hệ thống hỗ trợ thực hiện các tính năng:

1 – Xem danh sách các agent đã được cài đặt trên hệ thống:

+ User đăng nhập thuộc group root: Hiển thị tất cả Agent trong hệ thống active < 30 ngày;

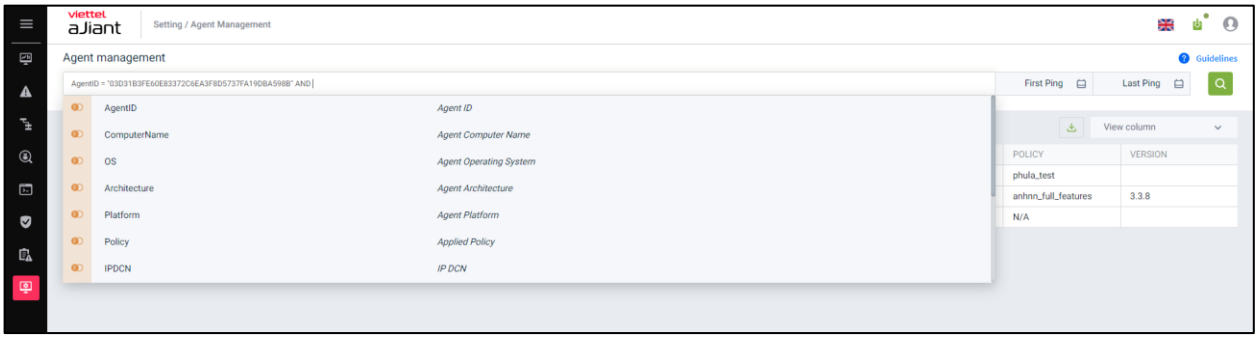
+ User đăng nhập thuộc group default: Hiển thị tất cả Agent thuộc group default;

+ User đăng nhập thuộc group cha: Hiển thị tất cả Agent thuộc group của user đang login và group con tương ứng;

+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tất cả Agent thuộc group của user đang login;

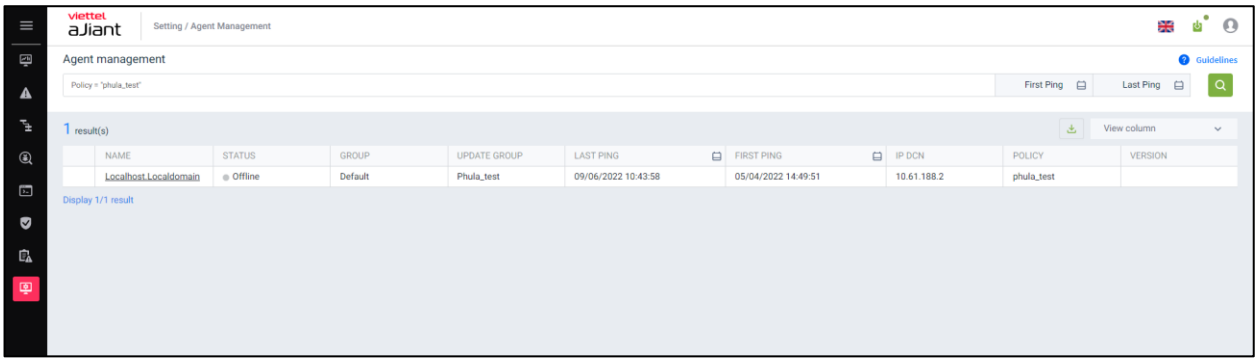
+ Mỗi agent được hiển thị các thông tin chung gồm: Name, Status, Group, Update Group, Last Ping, First Ping, DNS, Policy, AgentID, PlatForm, PlatForm Version, Architecture, DNS, Version.

2 – Hỗ trợ chức năng tìm kiếm Agent theo AgentID, ComputerName, OS, Architecture, Platform, Policy, IPDCN, Online, Update Group, Group ID, IP, Mac, Version. Với mỗi tiêu chí tìm kiếm thì hỗ trợ các toán tử tìm kiếm “=”, “!=”, “~”;

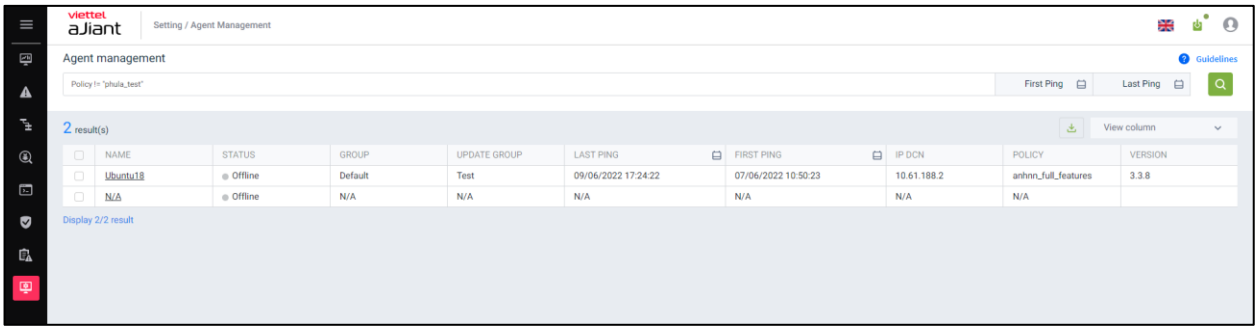


- Ví dụ về các câu tìm kiếm:

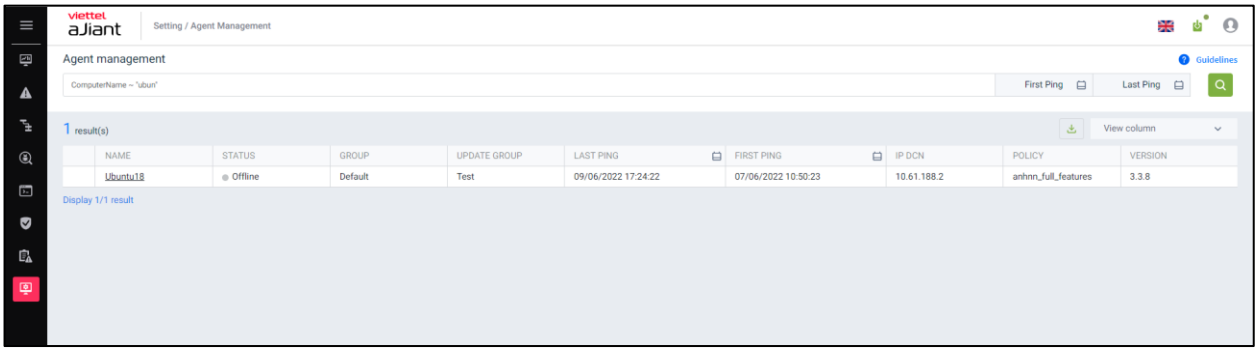
+ Tìm kiếm với điều kiện “=”:



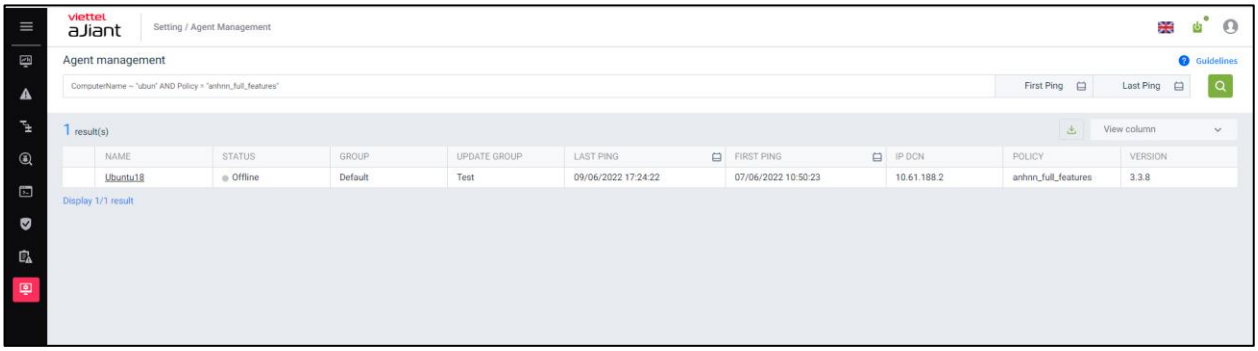
+ Tìm kiếm với điều kiện “!=”:



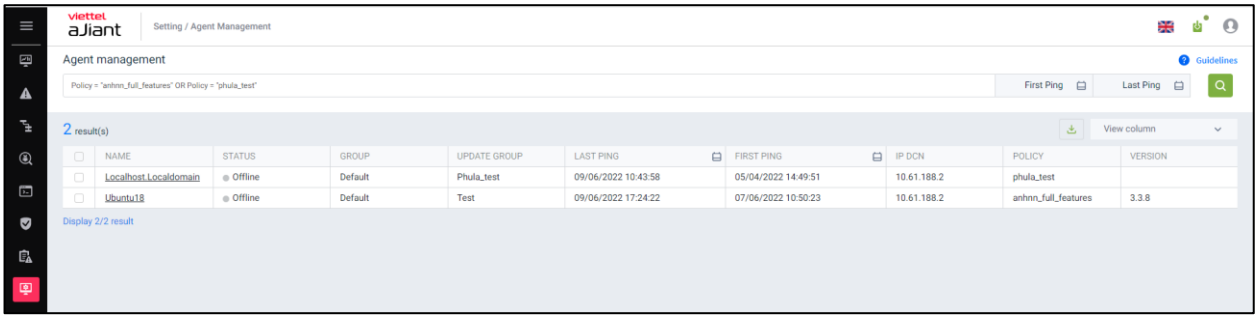
+ Tìm kiếm với điều kiện “~”:



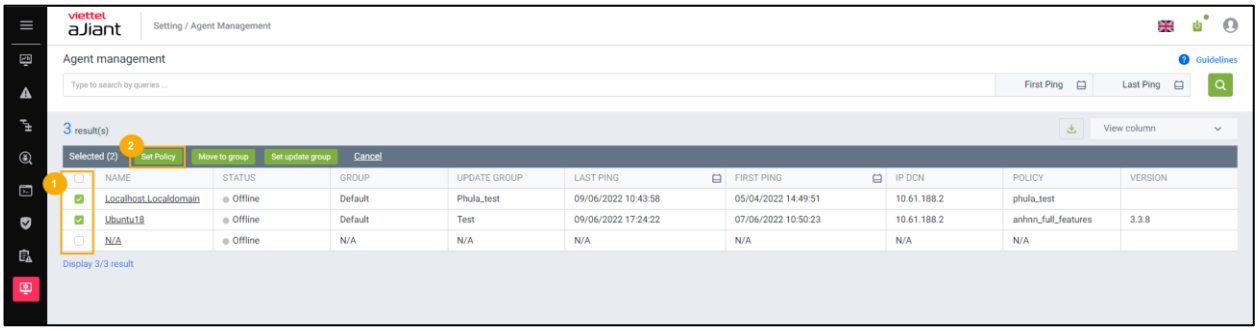
+ Tìm kiếm theo tiêu chí kết hợp AND:



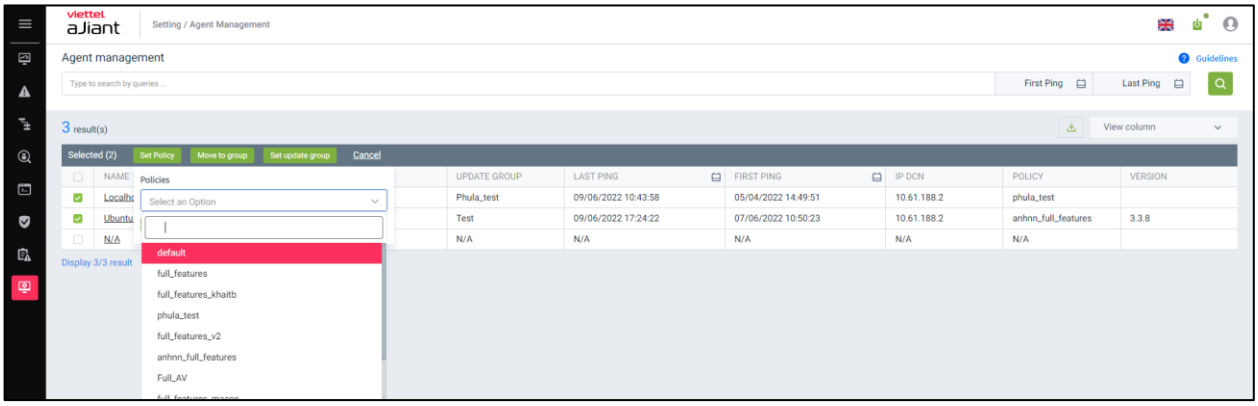
+ Tìm kiếm theo tiêu chí kết hợp OR:



3 – Chọn nhanh 1 agent/ 1 nhóm các agent để thiết lập Policy

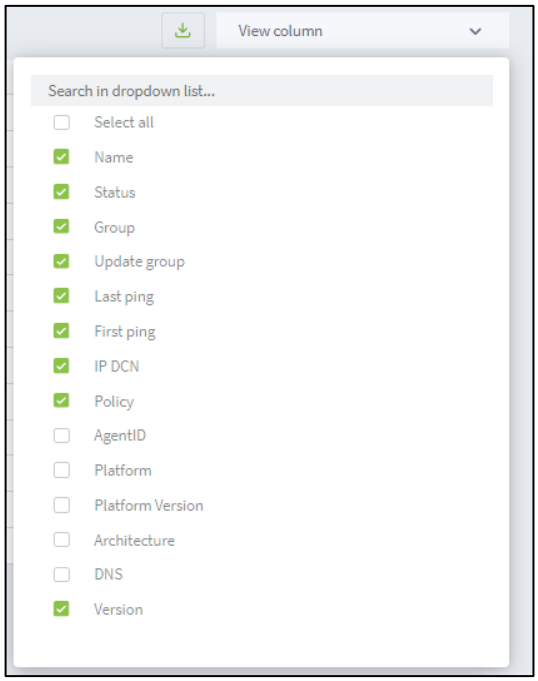


+ Tích chọn 1 agent/ nhiều agent để vào phiên Multiselected;
+ Thực hiện Set Policy:
  - Chọn Policy:



  - Xác nhận thao tác bằng cách chọn nút “Set policy”;
  - Xác nhận hủy thao tác bằng cách chọn nút “Cancel”.

4 – View Column: Cấu hình hiển thị các cột theo mong muốn.



5 – Xem chi tiết 1 agent bằng việc click duplicate chuột vào 1 row bất kỳ

Hệ thống hỗ trợ người dùng thiết lập Policy, Update Group và Move to group cho Agent 1 cách nhanh chóng.

+ User đăng nhập thuộc group root: Hiển thị tất cả Group trong hệ thống;

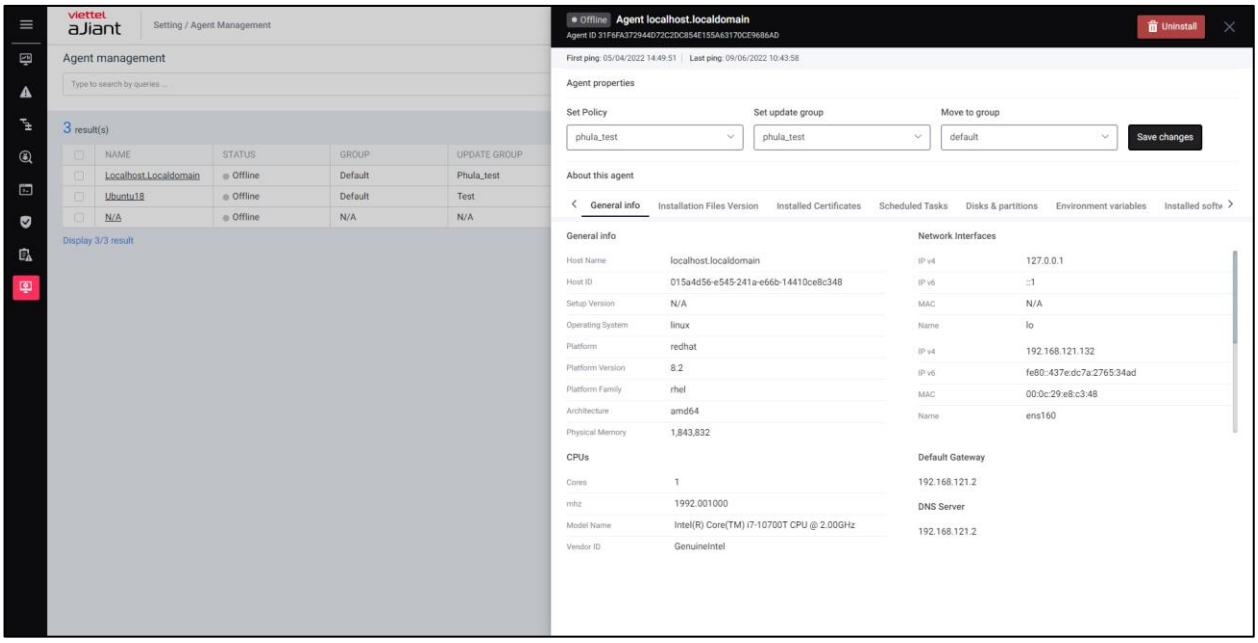
+ User đăng nhập thuộc group default: Hiển thị Group default;

+ User đăng nhập thuộc group cha: Hiển thị tất cả Group thuộc user đang login và các user thuộc group con tương ứng;

+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tất cả Group thuộc user đang login;

- Tab General info

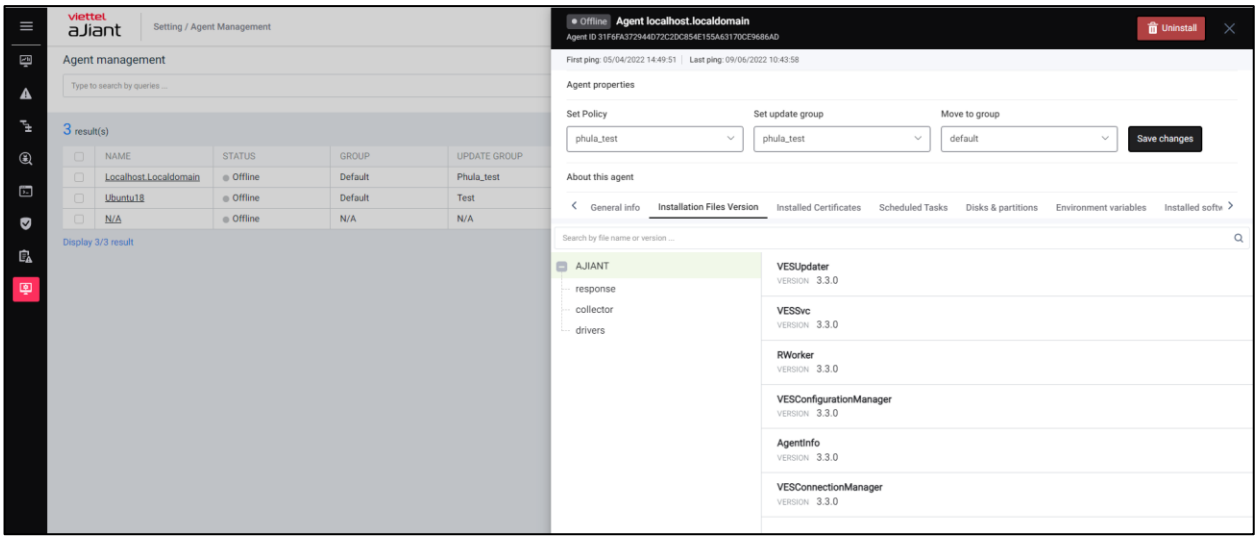
+ Hệ thống hiển thị các thông tin chung về agent gồm: Các thông tin chung, CPUs, Network Interfaces, Default Gateway, DNS Server;



- Installation Files Version

+ Thống kê tất cả các file cài agent, bao gồm các thông tin: Tên folder chứa file cài, File name, Version;

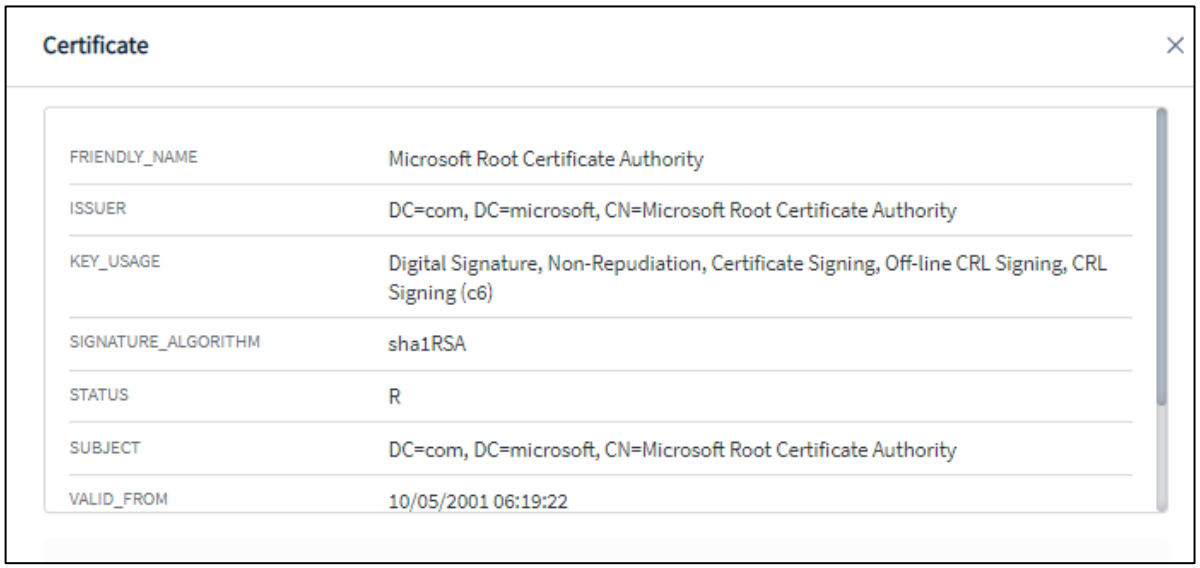
+ Hỗ trợ search nhanh theo File name, Version vào text box search



- Installed Certificates

+ Thống kê tất cả các certificate trên máy cài agent, bao gồm các thông tin: Danh sách certificates trên máy, Issused by, Issused to, Expiration date, Status;

+ Trường hợp muốn xem chi tiết với nhiều thông tin hơn, chọn , hiển thị màn hình như sau:

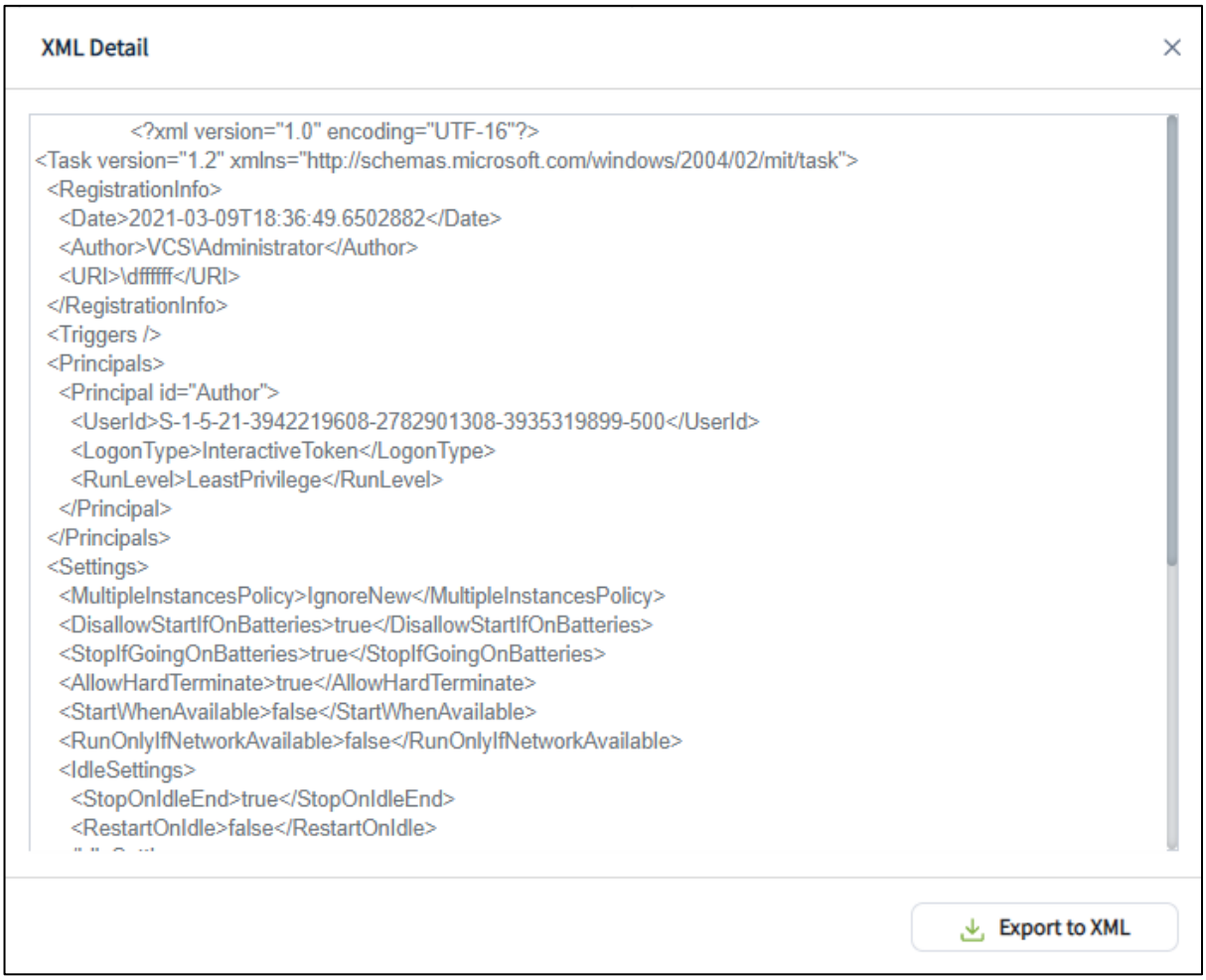


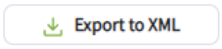
- Scheduled Tasks

+ Thống kê tất cả scheduled tasks trên máy cài agent, bao gồm các thông tin: Danh sách các scheduled tasks, Name, Status, Trigger, Next time run, Last time run, Author, Created;

+ Chọn Show » hoặc Hide » để tùy chỉnh việc hiển thị thông tin bổ sung cho từng task;

+ Hover vào task và chọn để xem thông tin đầy đủ của task dưới dạng xml



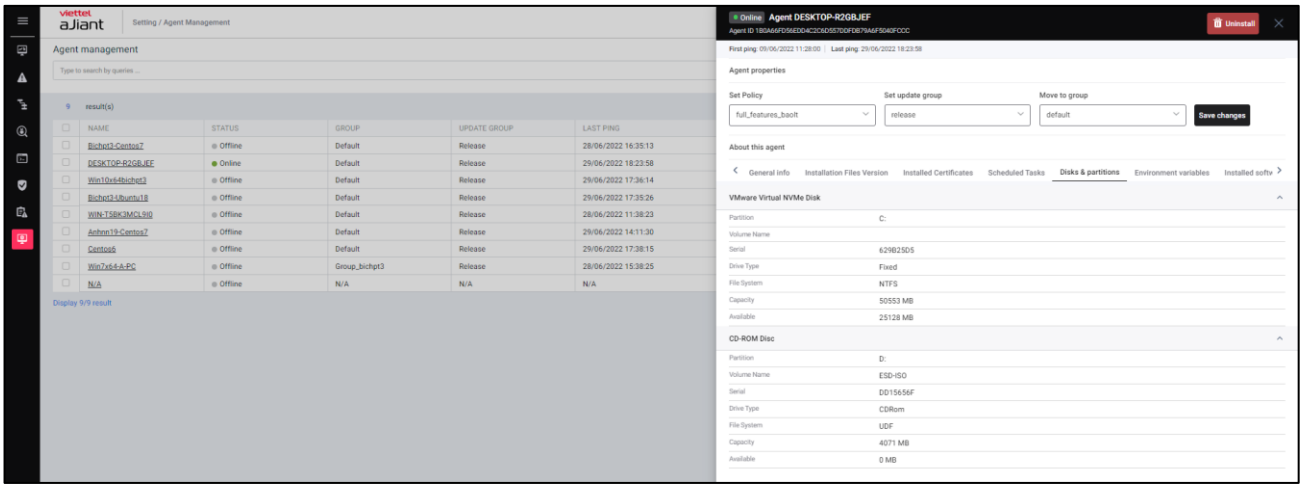
+ Chọn 

để tải về thông tin scheduled task, hỗ trợ định dạng .xml

- Disks & partitions

+ Thống kê tất cả disks & partitions trên máy cài agent, bao gồm các thông tin: Danh sách Disks, Partition, Volume name, Serial, Drive type, File system, Capacity, Available

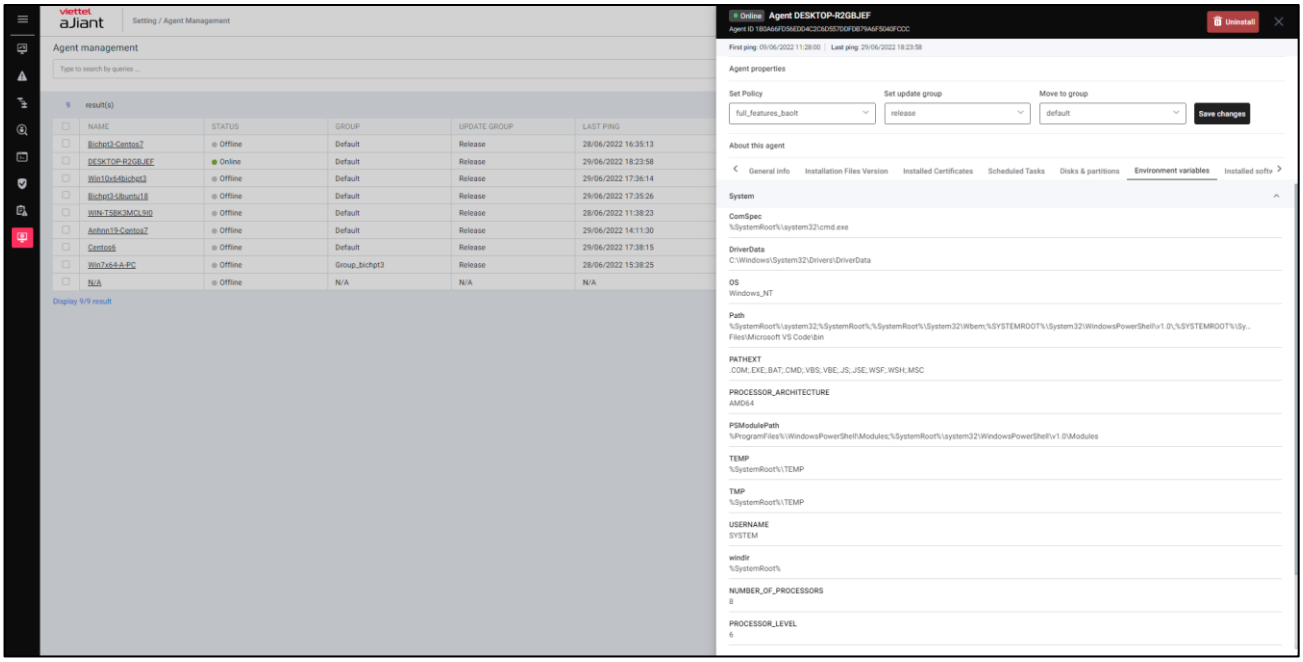
+ Chọn  hoặc để tùy chỉnh việc hiển thị thông tin bổ sung cho từng disk.



- Environment variables

+ Thống kê tất cả environment variables trên máy cài agent, bao gồm các thông tin: Danh sách system và users, tên biến, giá trị trực thuộc system hoặc user;

+ Chọn ^ hoặc v để tùy chỉnh việc hiển thị thông tin bổ sung cho từng disk.



- Tab Installed Software

+ Thống kê tất cả phần mềm đã cài trong agent bao gồm thông tin: Tên phần mềm, version cài, ngày cài;

+ Hỗ trợ search nhanh phần mềm Antivirus đã cài hoặc nhập tên phần mềm vào text box search;

- Tab Required Software

+ Thống kê tất cả phần mềm bắt buộc đã cài hoặc chưa cài trong agent bao gồm thông tin: Tên phần mềm, version cài, trạng thái cài;

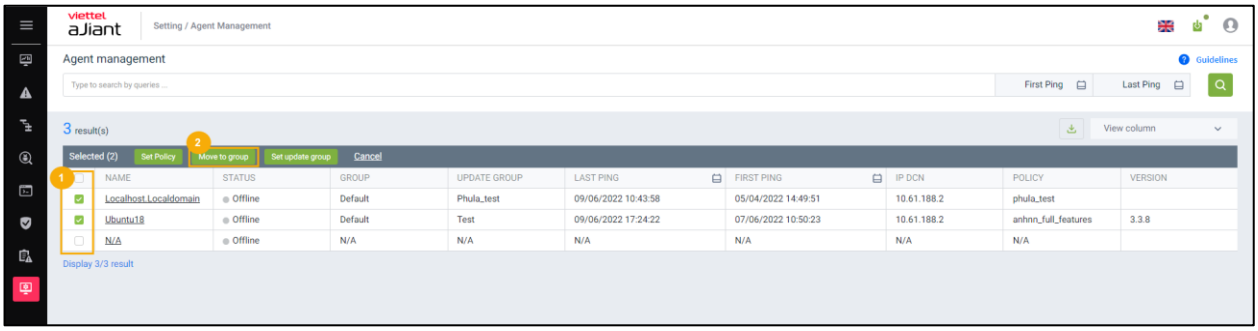
+ Hỗ trợ search nhanh phần mềm bắt buộc chưa cài đặt trên máy hoặc nhập tên phần mềm vào text box search.

- Tab User list

+ Thống kê tất cả User đăng nhập trong agent bao gồm thông tin: Tên user, active, administrator

6 – Chọn nhanh 1 agent/ 1 nhóm các agent để thiết lập Move to group

+ Tích chọn 1 agent/ nhiều agent để vào phiên Multiselected;



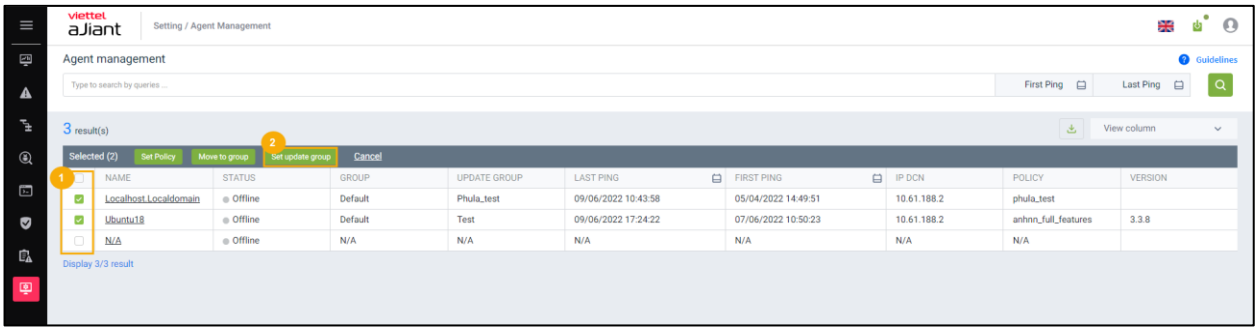
+ Thực hiện Move to group:

Danh sách Group trong combobox Move to group:

- User đăng nhập thuộc group root: Hiển thị tất cả Group trong hệ thống;
- User đăng nhập thuộc group default: Hiển thị Group default;
- User đăng nhập thuộc group cha: Hiển thị tất cả Group thuộc user đang login và các user thuộc group con tương ứng;
- User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tất cả Group thuộc user đang login;

+ Chọn nhanh 1 agent/ 1 nhóm các agent để thiết lập Set update group:

- Tích chọn 1 agent/ nhiều agent để vào phiên Multiselected;



- Thực hiện Set update group;

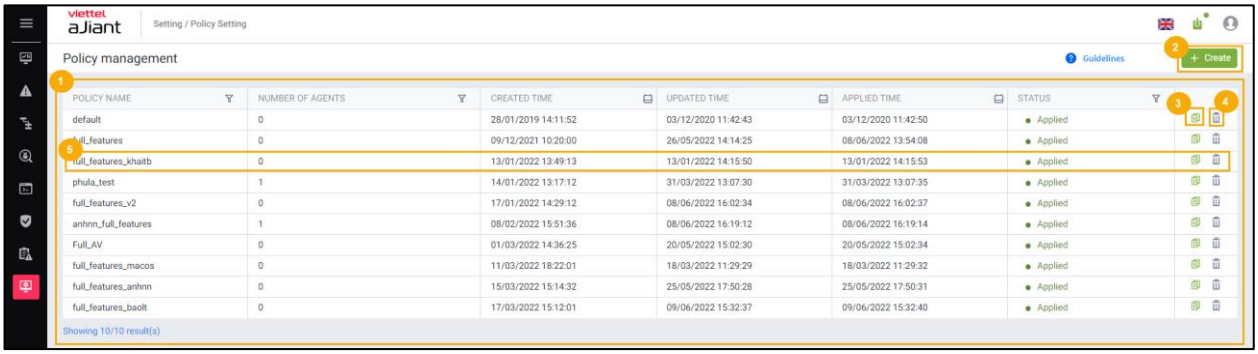
Lưu ý:

+ Move to group: Chuyển agent vào các group có trong màn hình Group management;

+ Update group: chuyển agent vào các group lưu trữ các file chạy dưới Agent, mỗi group có các file chạy khác nhau được định nghĩa trong server.

3.4.2 Policy Setting

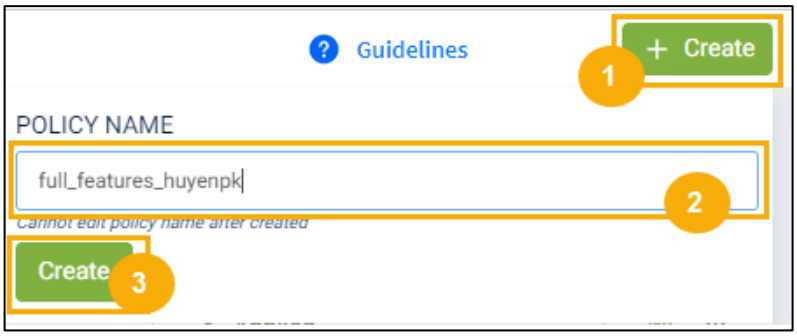
- Mục đích: Hỗ trợ người dùng quản lý danh sách các chính sách thiết lập cho các Agent;
- Màn hình giao diện khi người dùng truy nhập vào Setting >> Policy Setting:



1 – Hiển thị danh sách các Policy đã được tạo trên hệ thống. Mỗi 1 policy gồm các thông tin: Tên, số lượng Agent được áp chính sách, Thời gian tạo,

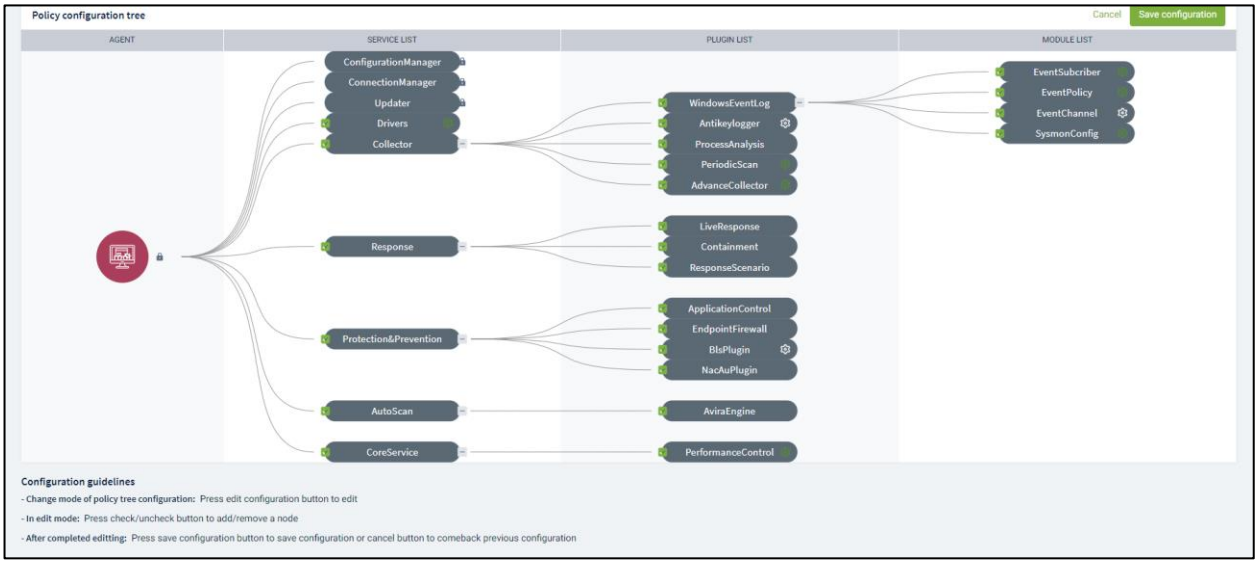
thời gian cập nhật, Thời gian áp chính sách, trạng thái (có 2 trạng thái: Applied và Not Applied);

2 – Tạo mới một chính sách: Click vào nút “Create” hệ thống hiển thị Popup tạo mới chính sách như sau:



Lưu ý: khi tạo mới: Tên Policy không được trùng với các Policy đã tạo trước đó.

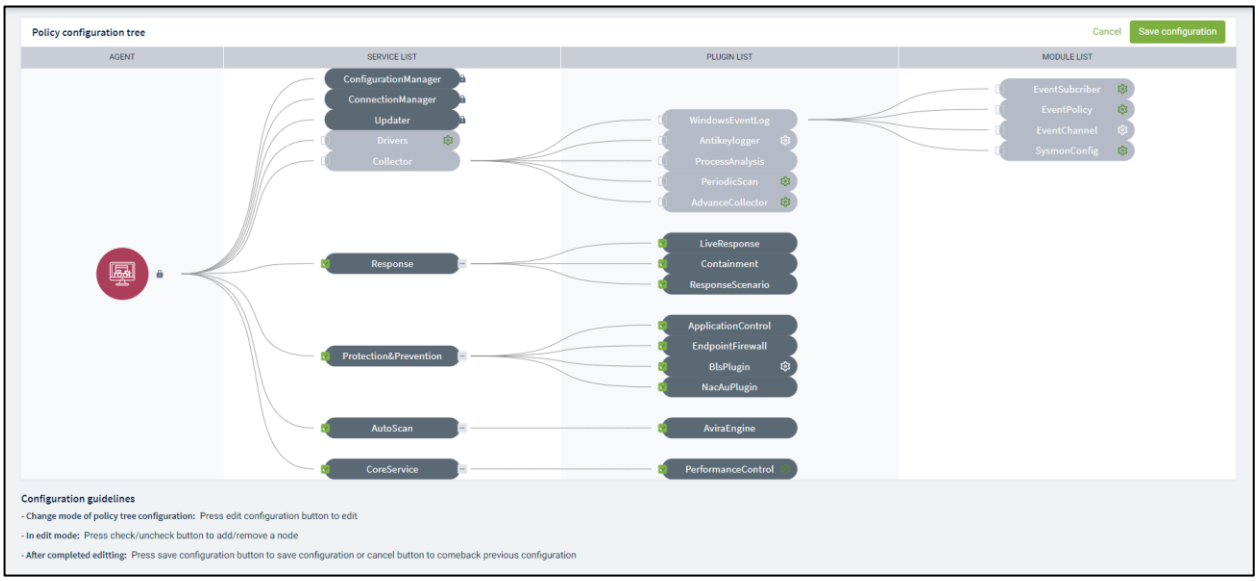
- Sau khi tạo mới policy thành công hệ thống sẽ hiển thị màn hình chi tiết của 1 policy:



- Mỗi 1 policy tạo xong thường có 3 core service mặc định: ConfigurationManager, ConnectionManager, Updater. Lưu ý 3 service này không được phép xóa khỏi hệ thống. Các bước để cấu hình cho 1 policy:

Bước 1: Click nút Edit Config để thay đổi cây Policy

Bước 2: Khi ở trong chế độ Edit, người dùng được phép Check/Uncheck để Add/Remote các service khác:



Bước 3: Sau khi hoàn thành chế độ edit:

- Người dùng nhấn nút “Save config” để lưu các thay đổi;
- Người dùng nhấn nút “Cancel” để hủy thao tác cập nhật Policy và hệ thống quay lại cấu hình trước đấy.

Bước 4: Click icon để thực hiện cấu hình chi tiết cho từng module/Plugin của các Service.

- WindowsEventLog: cấu hình các nguồn log lấy dưới Agent:
- EventSubcriber: chỉ định các kênh lấy log
- Yêu cầu dữ liệu:

+ Trường **event_filter** (lọc theo Event ID): các string con cách nhau dấu phẩy (,);

VD: “4”: lọc các event có eventID = 4

“-689”: lọc các event có eventID # 689

+ Trường **providers** các string con cách nhau dấu chấm phẩy (;);

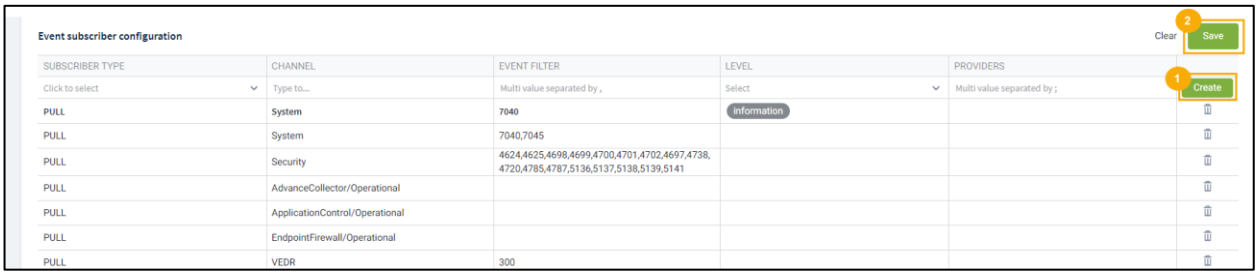
+ Các trường bắt buộc phải điền: **subs_type, channel;**

+ Channel: nguồn log;

+ sub_type:

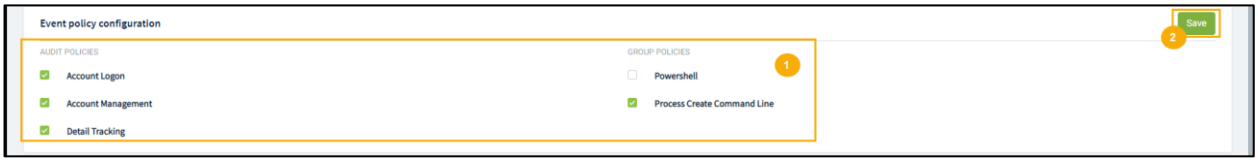
- PUSH: khi có event mới → gọi hàm của VCS-aJiant để xử lý;
- POLLING: VCS-aJiant sau 1 khoảng thời gian chủ động lấy log;
- PULL: VCS-aJiant chủ động lấy log sau 1 khoảng thời gian;

- Sau khi cấu hình xong cần Save lại:



+ EventPolicy: Thiết lập policy để enable/disable 1 số loại log mà hệ thống mặc định chưa có;

- Yêu cầu: có ít nhất 1 trường được chọn



+ EventChannel: cấu hình chi tiết 1 số nguồn log:

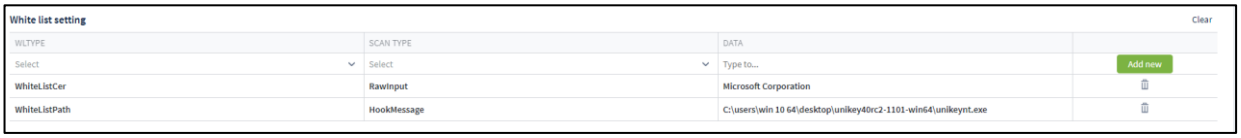
- Retention: có lưu log xoay vòng hay không (Nếu chọn Rentention thì khi file log đầy có log mới sẽ ghi đè lên log cũ nhất);
- Log file path: đường dẫn file log;
- Log file size: kích thước file log;
- Yêu cầu: tất cả dữ liệu đều phải điền;

+ SysmonConfig: enable/disable sysmon tool trên Agent để lấy log sysmon: Microsoft-Windows-Sysmon/Operational;

- Antikeylogger: là một SelfRun Plugin của VCS-aJiant, có nhiệm vụ định kỳ quét toàn bộ máy để tìm ra KeyLogger đang chạy trên máy nếu có;
- Scan setting: cấu hình các loại KeyLogger cần quét;
- Yêu cầu:
  - Scan cycle: min là 1 phút, max là 180 phút;
  - Chọn ít nhất 1 loại Keylogger;

+ Whitelist setting: cấu hình whitelist 1 số phần mềm theo đường dẫn của file trên ổ đĩa hoặc theo chữ ký số (cert) của file chạy key logger

- Yêu cầu: điền đầy đủ các trường;
- Sau khi nhập xong cần "Save" lại cấu hình:

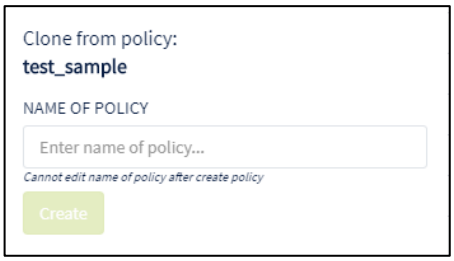


+ Self defend: Bổ sung cơ chế chống unintall cho Self Defense;

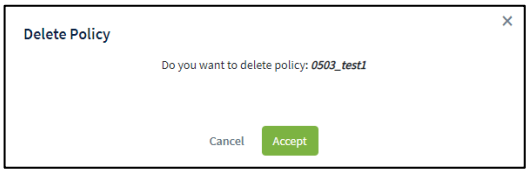
- Yêu cầu: Lựa chọn Chọn Drivers > Tích chọn Self Defense để bật tính năng Self Defense hoặc bỏ chọn để tắt > chọn Save > chọn Apply Policy;
- Sau khi cập nhật thay đổi xong cần "Save" lại cấu hình:

Bước 5: Click nút Apply Policy để thiết lập Policy vừa được cấu hình cho Agent:

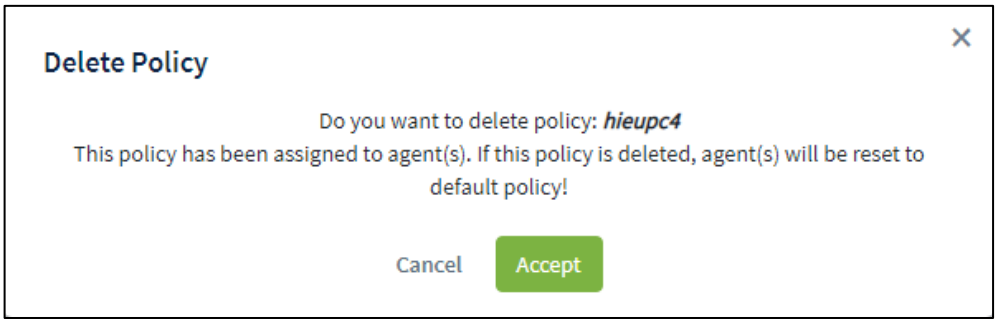
+ Clone chính sách mới: Click vào nút hệ thống sao chép toàn bộ chi tiết của policy được clone ngoại trừ tên policy.



+ Xóa chính sách: Click vào nút hệ thống hiển thị pop up để người dùng đưa ra quyết định xóa hay không?



+ Trường hợp Policy đã có agent được áp, sau khi xóa hệ thống tự động gán “default policy” cho các agent đó;



+ Khi click đúp vào từng bản ghi hệ thống sẽ chuyển tiếp tới trang chi tiết của 1 policy để người dùng xem/ thay đổi cấu hình cho Policy.

3.4.3 Group Management

- Cấu hình luật để tự động chuyển policy và chuyển nhóm cho các agent nếu thỏa mãn luật trên Portal, giảm thời gian chuyển policy và chuyển nhóm cho từng agent và đồng bộ policy cho các agent thỏa mãn luật đã cấu hình.
- Các tính năng chính trên màn hình này bao gồm:

+ Quản lý nhóm theo cây;

+ Tìm kiếm nhóm;

+ Thêm mới nhóm:

- Tạo luật tự động chuyển nhóm cho agent;
- Tùy chọn cách thức chuyển nhóm (All existing agents, New agents only, All existing and new agents) và gán policy (gán ngay, không gán);

+ Theo dõi các agent thuộc nhóm, tổng số agent thuộc nhóm;

+ Chỉnh sửa nhóm;

+ Xóa nhóm, xóa agent thuộc nhóm;

1 – Quản lý nhóm theo cây:

+ User đăng nhập thuộc group root: Hiển thị tất cả Group trong hệ thống;

+ User đăng nhập thuộc group default: Hiển thị group default;

+ User đăng nhập thuộc group cha: Hiển thị Group thuộc group của user đang login và group con tương ứng;

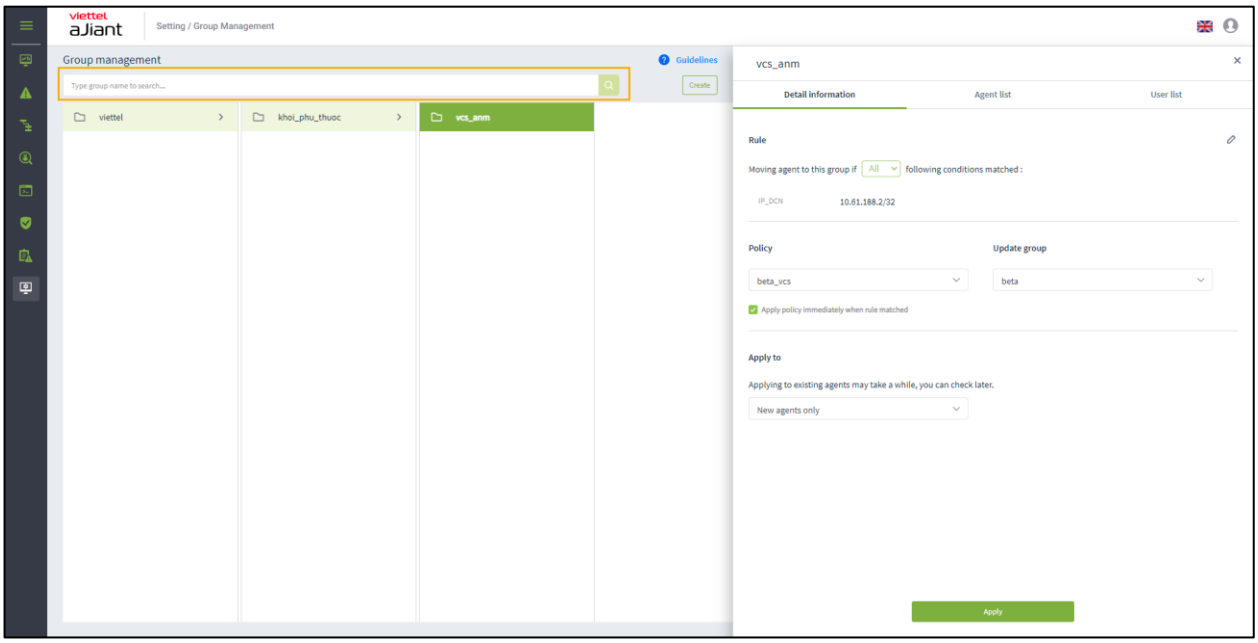
+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tất cả Group thuộc group của user đang login;

- Danh sách nhóm hiển thị theo dạng cây bao gồm các nhóm gốc và mỗi nhóm gốc gồm các nhóm con cấp 1, cấp 2…
- Mỗi nhóm gồm tên nhóm, thông tin cấu hình của nhóm (rule, policy, apply to), và danh sách agent thuộc nhóm.
- Các rule của nhóm là độc lập giữa các nhóm (không có kế thừa cha con). Việc quản lý nhóm theo cây để quản lý dễ dàng hơn khi số lượng agent lớn và có sự phân cấp về quản lý agent theo công ty, phòng, ban…
- Khi user thuộc group con, chọn group cha sẽ không nhìn thấy popup group detail

2 – Tìm kiếm nhóm

+ Cách 1: Click vào textbox Search > hiện danh sách các nhóm của tương ứng với user đang login có thể scroll được > Chọn nhóm trong danh sách hiện ra;

+ Cách 2: Click vào textbox Search > nhập ký tự tìm kiếm vào textbox > hệ thống tự động tìm kiếm các bản ghi chứa ký tự nhập vào > Chọn 1 bản ghi phù hợp trong danh sách gợi ý hoặc click Search hoặc Enter sẽ hiện danh sách các bản ghi thỏa mãn;



- Khi click đúp vào 1 bản ghi sẽ hiển thị thông tin chi tiết của bản ghi đó.

+ Tab thông tin chi tiết hiển thị là Detail, dữ liệu của group đó là Rule, Policy, Apply to;

+ Khi chọn tab Agent list thì dữ liệu thông tin các agent match với group đó.

+ Khi chuột phải vào 1 bản ghi thì sẽ hiển thị 2 option: Go to group và Delete group.

+ Nếu chọn Go to group thì đưa user đến vị trí của group đó trên cây;

+ Nếu chọn Delete group thì hiển thị popup confirm xóa group.

- Khi click vào menu góc phải mỗi ản ghi cũng hiển thị 2 option: Go to group và Delete group.

3 – Thêm mới nhóm:

+ User đăng nhập thuộc group root: Có thể them mới tất cả Group trong;

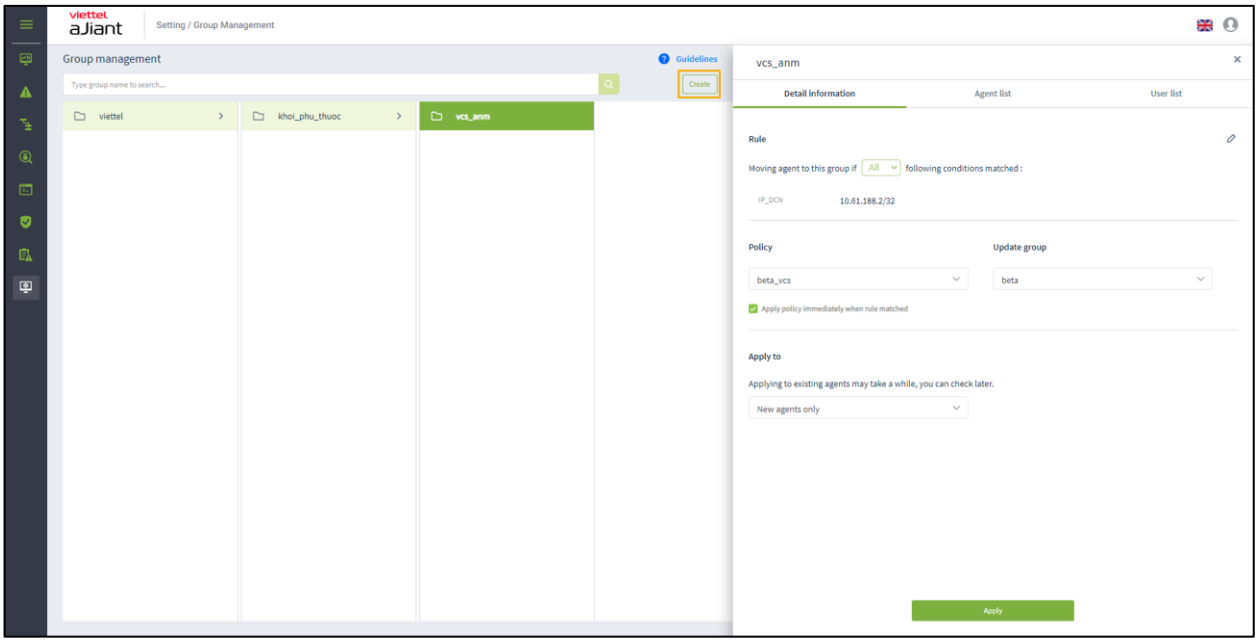
+ User đăng nhập thuộc group default: Không thể thêm mới;

+ User đăng nhập thuộc group cha: có thể thêm mới group con tương ứng của group thuộc user đang login;

+ User đăng nhập thuộc group một hoặc nhiều con: có thể them mới group con tương ứng của group thuộc user đang login;

Bước 1: Lựa chọn vị trí nhóm sẽ tạo

+ Nếu tạo mới nhóm ở danh sách nhóm gốc, click nút “Add new” góc phải màn hình hoặc hover vào cuối danh sách nhóm gốc trên màn hình, click Add new ;



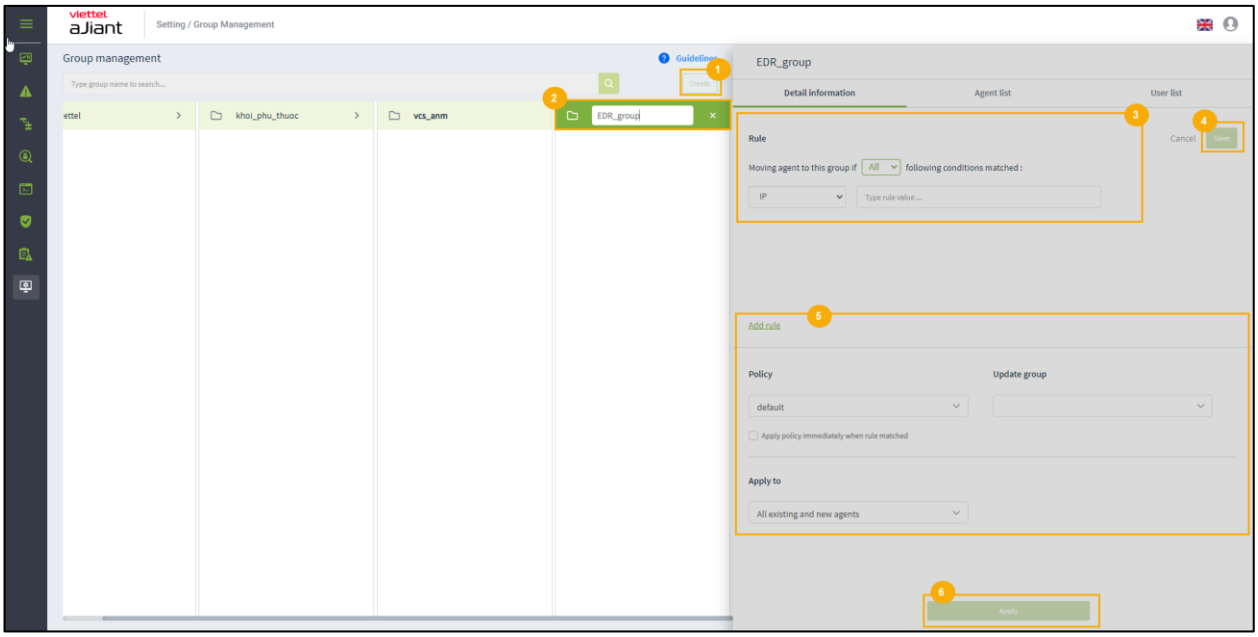
+ Nếu tạo mới nhóm là nhóm con trong một nhóm gốc hoặc nhóm cấp 1, cấp 2… thì click vào nhóm cha sau đó click “Create” trên màn hình hoặc hover vào cuối danh sách nhóm cùng cấp và click “Create”;

Bước 2: Nhập tên nhóm và cấu hình luật;

Lưu ý: tên và luật cấu hình không được trùng với tên và luật đã có.

+ Nếu chọn toán tử “All”: luật thỏa mãn khi cả 2 trường được thỏa mãn;

+ Nếu chọn toán tử “Any”: luật thỏa mãn khi 1 trong 2 hoặc cả 2 trường thỏa mãn;



Bước 3: Lựa chọn policy và loại agent sẽ apply policy nếu thỏa mãn rule:

- Sau khi click Apply kiểm tra agent được chuyển nhóm trong tab Agent list: danh sách agent thỏa mãn luật và được chuyển nhóm sang nhóm vừa thêm. Tùy thuộc vào lựa chọn ở phần "Apply to" để chuyển nhóm cho các agent trong hệ thống:

+ All existing agents: chuyển nhóm cho tất cả agent đang tồn tại trong hệ thống, các agent cài mới sau khi apply nếu có khớp luật cũng KHÔNG chuyển nhóm;

+ New agents only: chỉ chuyển nhóm cho các agent cài mới sau khi Apply, các agent đang tồn tại trên hệ thống nếu khớp luật cũng KHÔNG chuyển nhóm;

+ All existing and new agents: chuyển nhóm cho tất cả agent đang tồn tại trong hệ thống và agent cài mới sau khi apply nếu khớp luật;

Lưu ý:

+ Nếu chọn checkbox "Apply policy now when rule matched", sau đó click "Apply" thì với các agent được lựa chọn Apply sẽ kiểm tra các giá trị nếu khớp với luật đã cấu hình sẽ chuyển policy cho agent sang policy đã chọn ở mục "Policy", đồng thời chuyển nhóm;

Trong trường hợp ko chọn checkbox trên thì sau khi Apply, các agent được chọn Apply chuyển nhóm nhưng không chuyển policy, tức là agent giữ nguyên policy trong

khi chuyển sang nhóm có policy khác; với các agent cài mới nếu khớp luật thì chuyển nhóm và được áp policy "**default**" do không chọn checkbox > áp policy mặc định;

+ Nếu agent mới khớp luật của nhiều nhóm sẽ ưu tiên chuyển vào nhóm được tạo mới nhất, không tính thời gian sửa nhóm.

4 – Sửa nhóm: có thể lựa chọn sửa 1 hoặc 2 hoặc cả 3 thành phần trong một nhóm: Rule, Policy, Apply to

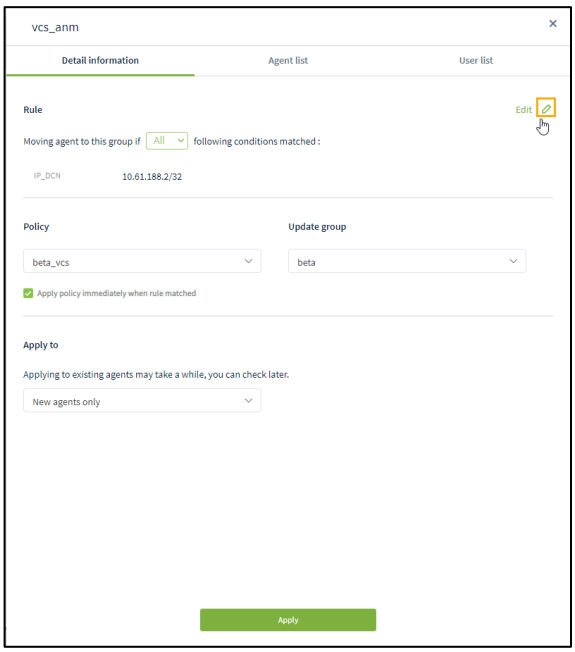
+ User đăng nhập thuộc group root: Có thể sửa tất cả group trong hệ thống;

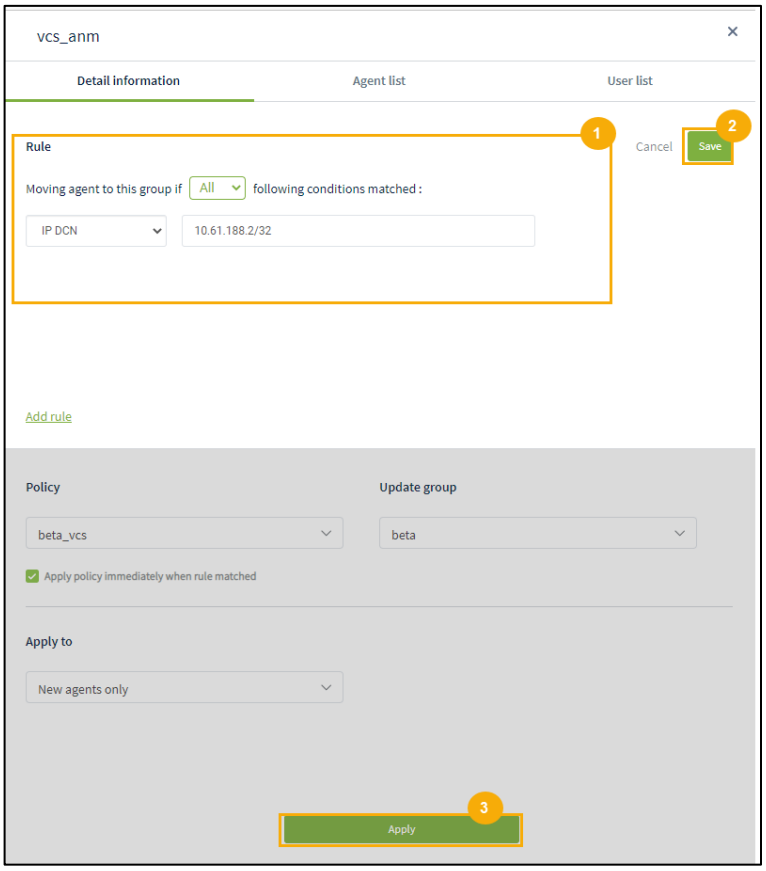
+ User đăng nhập thuộc group default: Không được sửa group default;

+ User đăng nhập thuộc group cha: Có thể sửa tất cả group thuộc đang login và group con có role cũng thuộc group role con của role user đang login;

+ User đăng nhập thuộc group một hoặc nhiều con: Có thể sửa tất cả group thuộc user đang login;

+ Để sửa Rule (luật) của nhóm, click vào icon Edit > Chỉnh sửa luật của nhóm sau đó click Save > Sau đó có thể chỉnh sửa ở mục "Policy" và "Apply to" rồi click Apply;





Lưu ý:

+ Trường hợp sửa các thành phần của nhóm (Rule, Policy hoặc Apply to) sau đó ko click Apply thì nội dung chỉnh sửa đã được lưu lại, nhưng không cập nhật Agent list. Với các Agent cài mới thì xử lý như sau:

- Chuyển nhóm: phụ thuộc Agent mới có được chọn ở mục “Apply to” hay không, nếu được chọn sẽ kiểm tra phía Agent, khớp luật của nhóm sẽ được chuyển vào nhóm;

- Apply policy: policy của agent phụ thuộc việc chọn checkbox “Apply policy now when rule matched”, nếu checkbox được chọn thì sẽ apply policy của nhóm, nếu không được chọn sẽ áp policy “default” do không chọn checkbox sẽ áp policy mặc định.

+ Trường hợp sửa xong các thành phần của nhóm rồi click Apply thì nội dung chỉnh sửa được lưu lại, đồng thời nếu có lựa chọn “All existing agents” trong

phần “Apply to” thì thực hiện quét thông tin toàn bộ agent trong hệ thống và chuyển nhóm cho agent, sau đó cập nhật Agent list.

- Đối với Agent mới xử lý tương tự như trên.

5 – Xóa nhóm hoặc xóa agent khỏi nhóm:

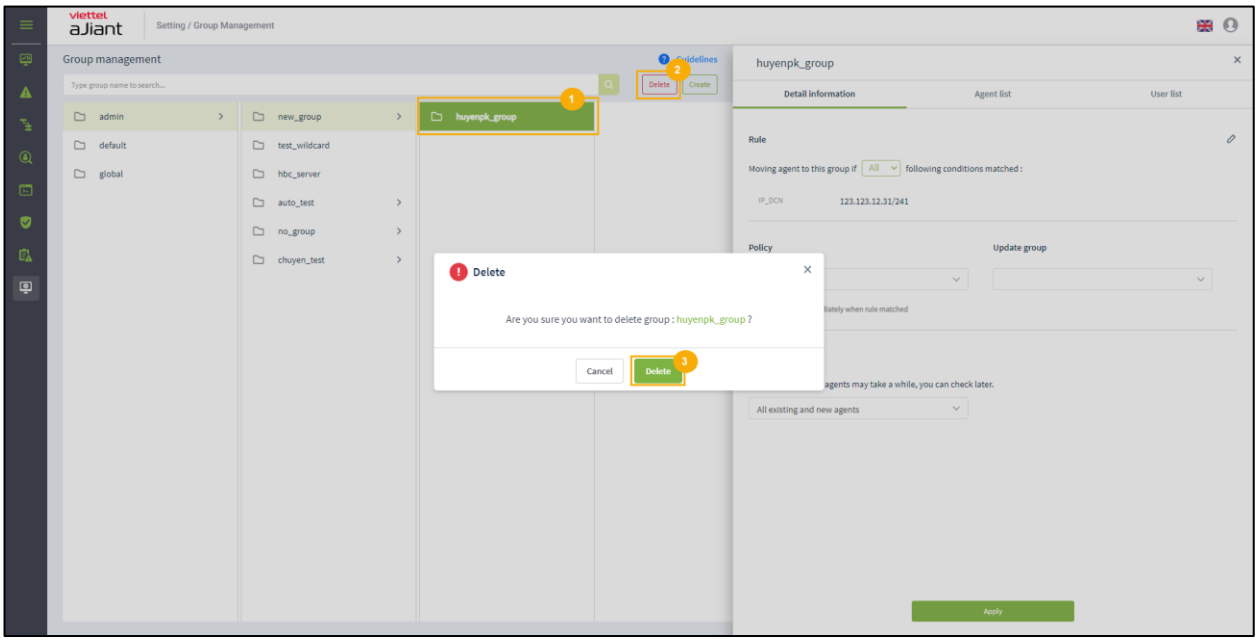
+ User đăng nhập thuộc group root: Có thể xóa tất cả group trong hệ thống;

+ User đăng nhập thuộc group default: Không được xóa group default;

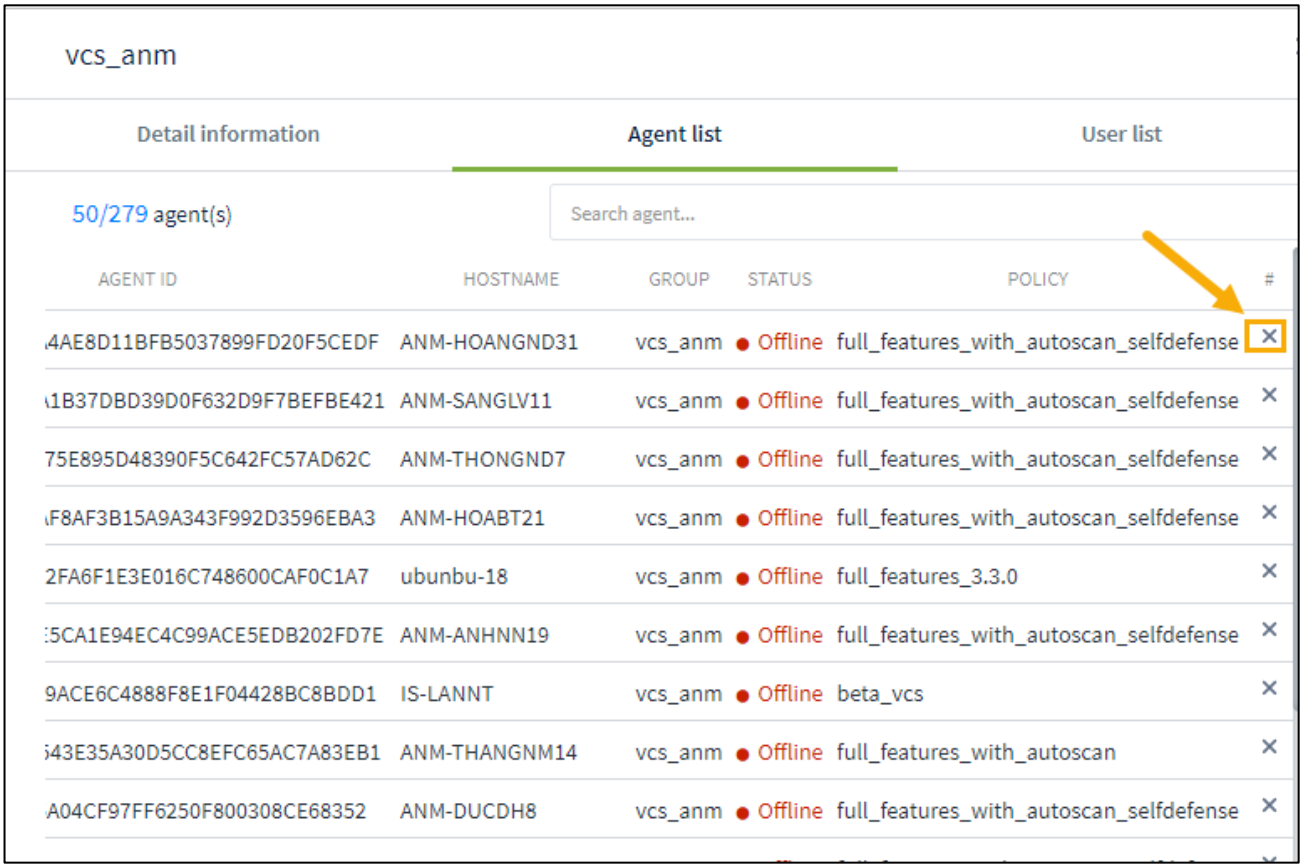
+ User đăng nhập thuộc group cha: Có thể xóa tất cả group thuộc đang login và group con có role cũng thuộc group role con của role user đang login;

+ User đăng nhập thuộc group một hoặc nhiều con: Có thể xóa tất cả group thuộc user đang login;

- Để xóa nhóm click vào nhóm cần xóa, click “Delete” sau đó click “OK” trên màn hình confirm. Sau khi xóa 1 nhóm thì các agent thuộc nhóm sẽ chuyển về nhóm mặc định, nhóm “default”, policy giữ nguyên;



- Để xóa Agent khỏi nhóm thì click vào tab Agent list, click icon “x” để xóa agent khỏi nhóm. Sau khi xóa agent khỏi nhóm thì agent được chuyển về nhóm mặc định: “default”, policy giữ nguyên



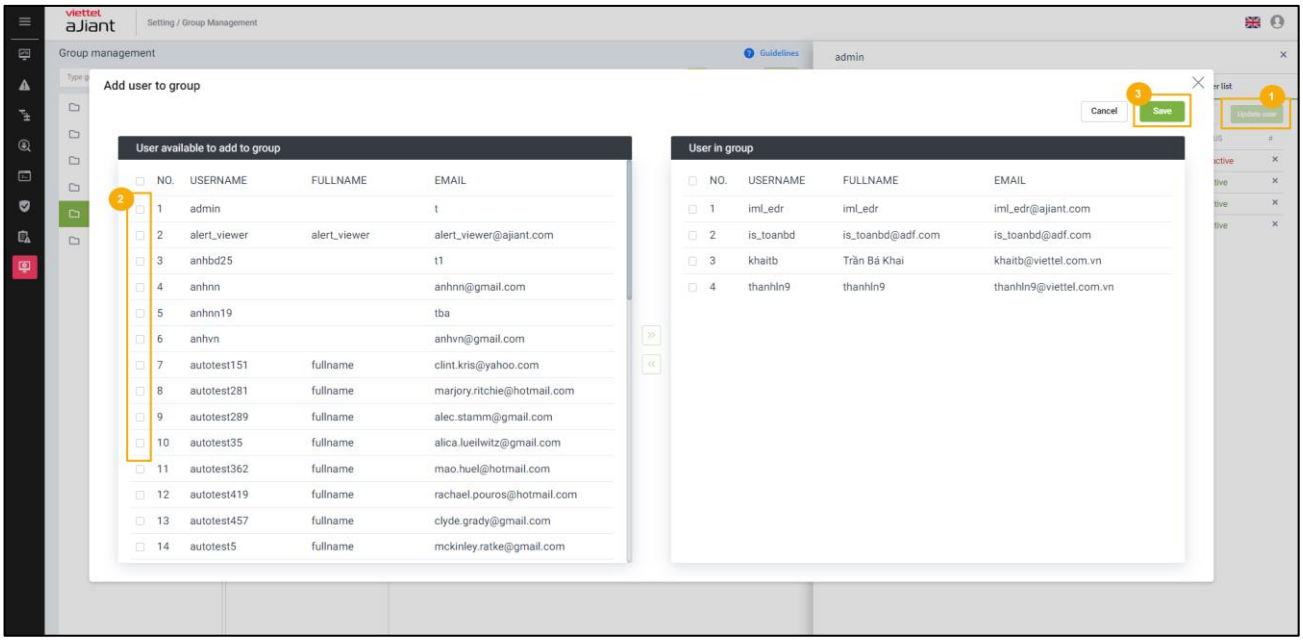
Lưu ý: trường hợp xóa một nhóm cha:

+ Xóa tất cả nhóm con;

+ Chuyển tất cả agent của nhóm cha và các nhóm con về nhóm mặc định: “default”;

+ Giữ nguyên policy của các agent trong nhóm cha và con;

6 – Thêm mới user vào group



- Danh sách user:

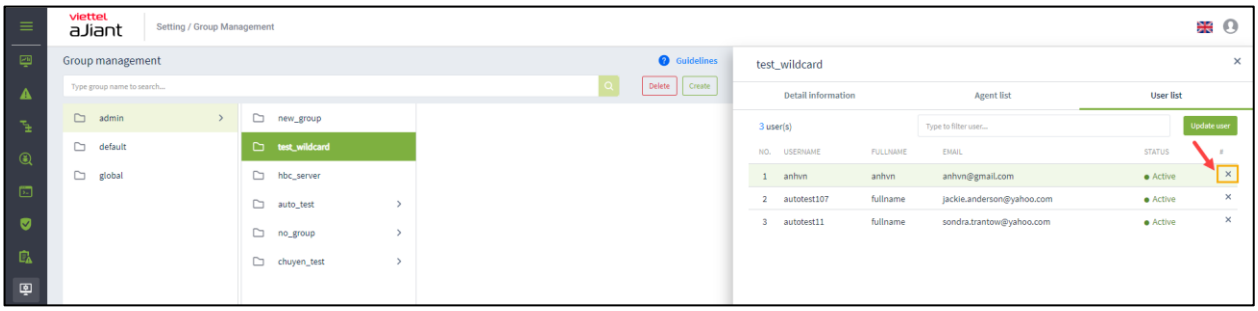
+ User đăng nhập thuộc group root: Hiển thị tất cả User trong hệ thống;

+ User đăng nhập thuộc group default: Hiển thị user chỉ thuộc default;

+ User đăng nhập thuộc group cha: Hiển thị User đang login và user thuộc group con có role cũng thuộc group role con của role user đang login;

+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị user đang login:

7 – Xóa user



3.4.4 Account Management

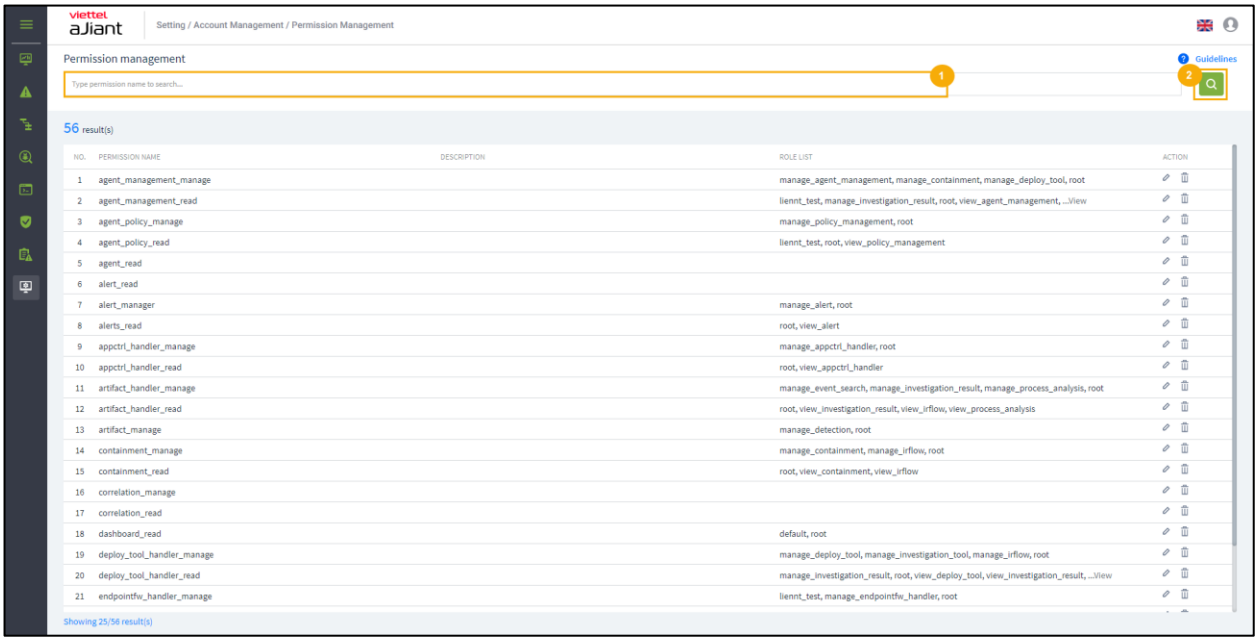
- Quản lý các tài khoản, quyền, nhóm quyền của hệ thống Portal

3.4.4.1 *Permission management*

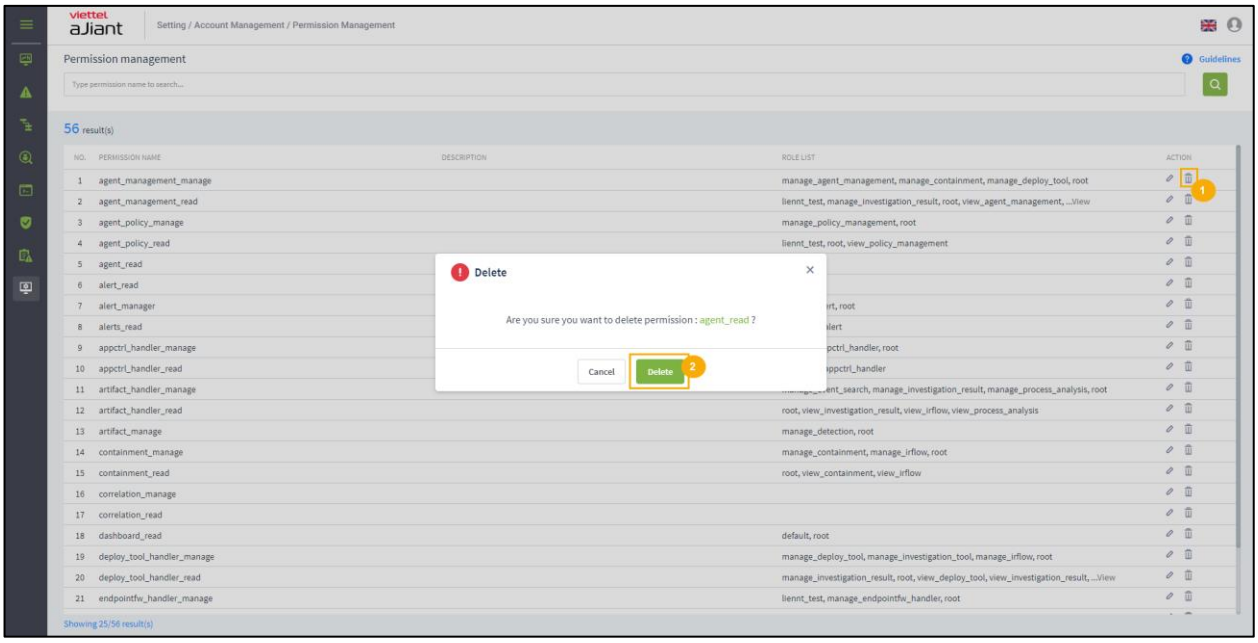
- Quản lý các quyền truy cập vào tài nguyên (API) của hệ thống. 1 permission là quyền truy cập vào 1 tài nguyên xác định (API) của hệ thống;
- Các chức năng chính trên màn hình này:
  + Quản lý các permission;
  + Tìm kiếm permission;
  + Xóa permission;

1 – Quản lý các permission: hiển thị toàn bộ các permission của hệ thống. Trong trường hợp xóa permission trên màn hình này, khi thực hiện các chức năng trên portal mà bị thiếu permission thì sẽ tự động thêm permission đã xóa trên màn hình quản lý Permission

2 – Tìm kiếm permission: nhập ký tự tìm kiếm vào texbox Search > click Enter hoặc nút “Search” => hiển thị danh sách permission thỏa mãn



3 – Xóa permission: click icon “Delete” > click “OK” trên màn hình confirm là xóa thành công:



3.4.4.2 *Role Management*

- Quản lý các role (nhóm quyền hay nhóm permission) của hệ thống;
- Các chức năng trên màn hình này bao gồm:
  + Quản lý danh sách role:
    - User đăng nhập thuộc Role root: Hiển thị tất cả Role trong hệ thống;
    - User đăng nhập thuộc Role default: Hiển thị Role default;
    - User đăng nhập thuộc Role cha: Hiển thị tất cả Role thuộc của user đang login và group con tương ứng;
    - User đăng nhập thuộc Role có một hoặc nhiều con: Hiển thị tất cả Role thuộc Role của user đang login;
  + Tìm kiếm role;
  + Thêm mới role;
  + Xóa role.

1 – Quản lý danh sách role: quản lý danh sách role theo dạng cây. Có 2 role ở gốc mặc định đã tạo sẵn: role “default” và “root”

+ Role “default”: User có quyền “default” chỉ có quyền truy cập vào Portal, không có quyền xem dữ liệu hoặc thao tác chức năng;

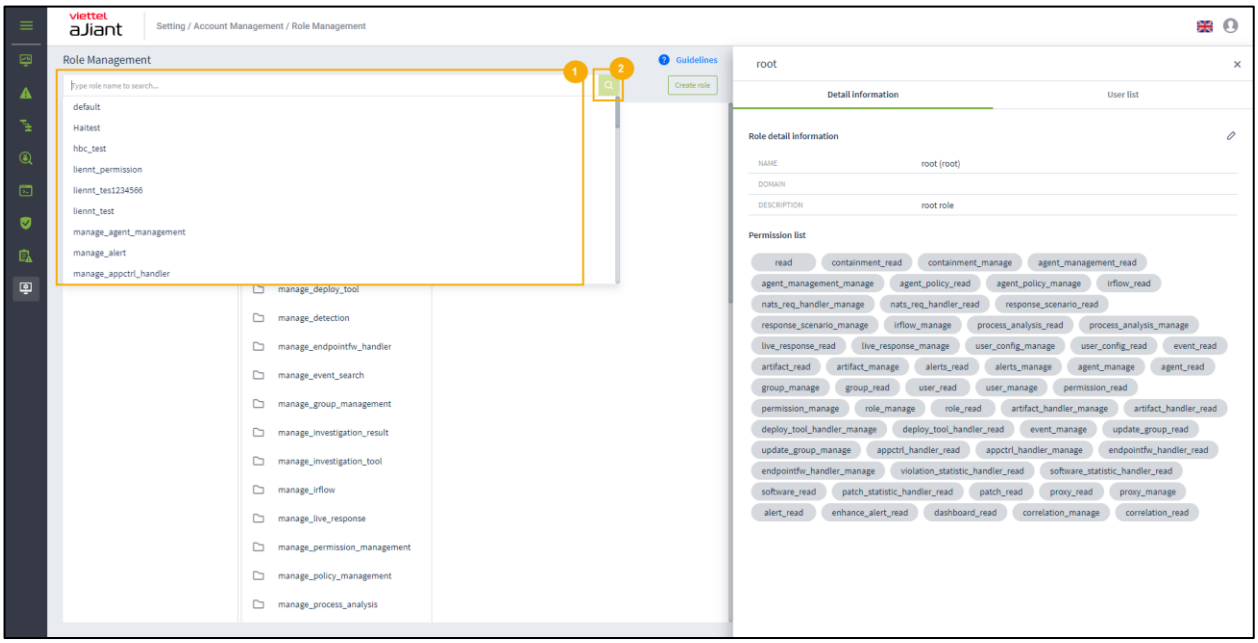
+ Role “root”: bao gồm toàn bộ các role của hệ thống, User có role “root” có toàn bộ quyền sử dụng tất cả chức năng trên Portal;

+ Click vào 1 role sẽ hiển thị thông tin chi tiết của role. Một role sẽ bao gồm các thông tin: tên role, danh sách các permission, danh sách User (tài khoản) chứa role, role cha hoặc danh sách role con (nếu có)

2 – Tìm kiếm role

+ Cách 1: Click vào textbox Search > hiển thị danh sách các role trong hệ thống và có thể scroll được danh sách role > Lựa chọn role trong danh sách hiện ra

+ Cách 2: Click vào textbox Search > Nhập ký tự tìm kiếm vào textbox > Hệ thống lọc ra các role chứa ký tự tìm kiếm > chọn role trong danh sách đã lọc hoặc click Enter hoặc click nút “Search”



- Khi click đúp vào 1 bản ghi sẽ hiển thị thông tin chi tiết của bản ghi đó.
  - Tab thông tin chi tiết hiển thị là Detail, dữ liệu của role bao gồm thông tin role và các permission của role đó;

- Khi chọn tab User list là danh sách User chứa role;

+ Khi chuột phải vào 1 bản ghi thì sẽ hiển thị Go to role. Click vào “Go to role” đưa về danh sách role dạng cây ban đầu;

+ Khi click vào menu góc phải mỗi bản ghi cũng hiển thị option: Go to role;

3 – Thêm mới role:

+ User đăng nhập thuộc group root: Có thể them mới tất cả role trong các cây dữ liệu;

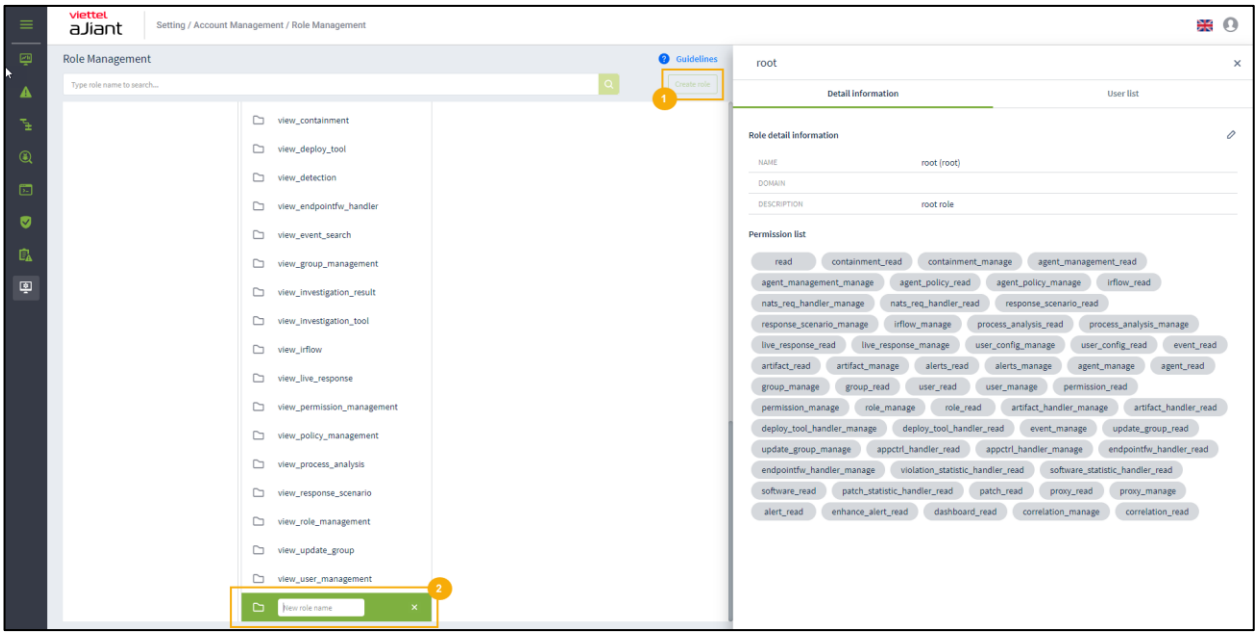
+ User đăng nhập thuộc group default: Không thể thêm mới;

+ User đăng nhập thuộc group cha: Có thể thêm mới role con tương ứng của group thuộc user đang login, không thể them mới role cùng cấp;

+ User đăng nhập thuộc group một hoặc nhiều con: có thể them mới group con tương ứng của group thuộc user đang login.

Bước 1: Có các cách tạo mới role như sau:

- Click vào 1 role sau đó hover vào cuối danh sách role chọn “Add new” để tạo role cùng cấp với role đã chọn
- Click “Add new” trên màn hình để tạo role con của role đã chọn
- Chuột phải vào 1 cột trong cây chọn “Add new role”
- Sau đó nhập tên role không trùng với tên role đã tồn tại trong hệ thống.



Bước 2: Click icon Edit để thêm thông tin permission cho role > Lựa chọn permission để thêm vào role > click Save:

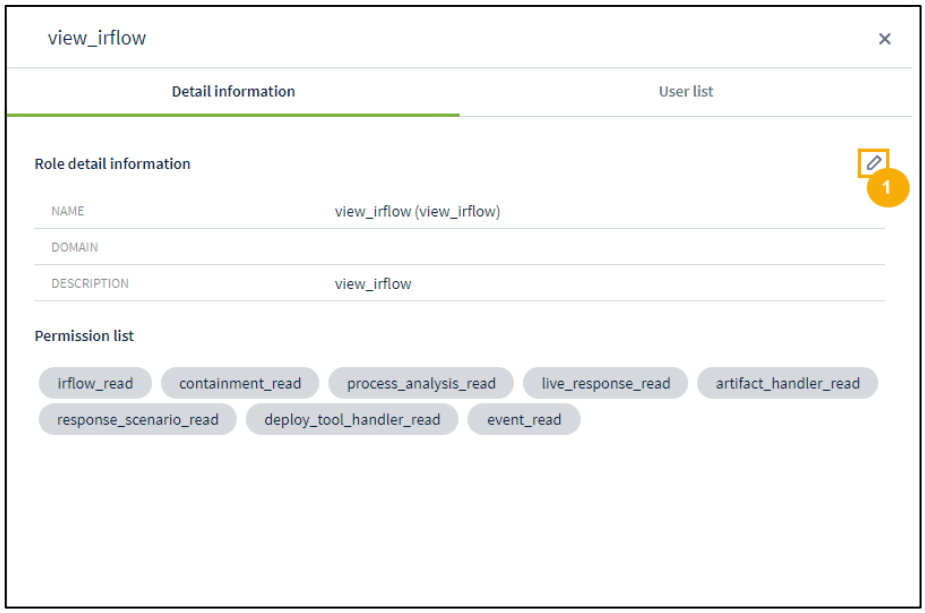
+ User đăng nhập thuộc group root: Có thể sửa tất cả role trong hệ thống;

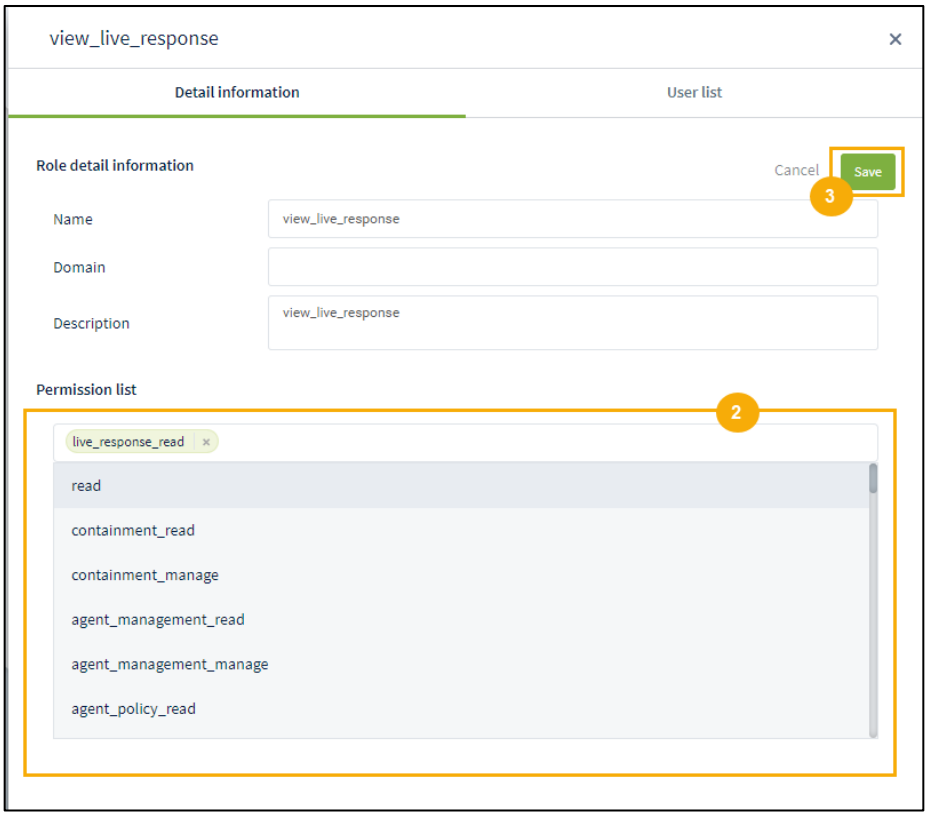
+ User đăng nhập thuộc group default: Không được sửa role default;

+ User đăng nhập thuộc group cha: Có thể sửa tất cả role thuộc đang login và role con role ;

+ User đăng nhập thuộc group một hoặc nhiều con: Có thể sửa tất cả role thuộc user đang login;

Lưu ý: danh sách permission của role con là tập con của role cha. Tức là khi muốn lựa chọn permission gán cho role con thì role đó phải thuộc danh sách permission của role cha.



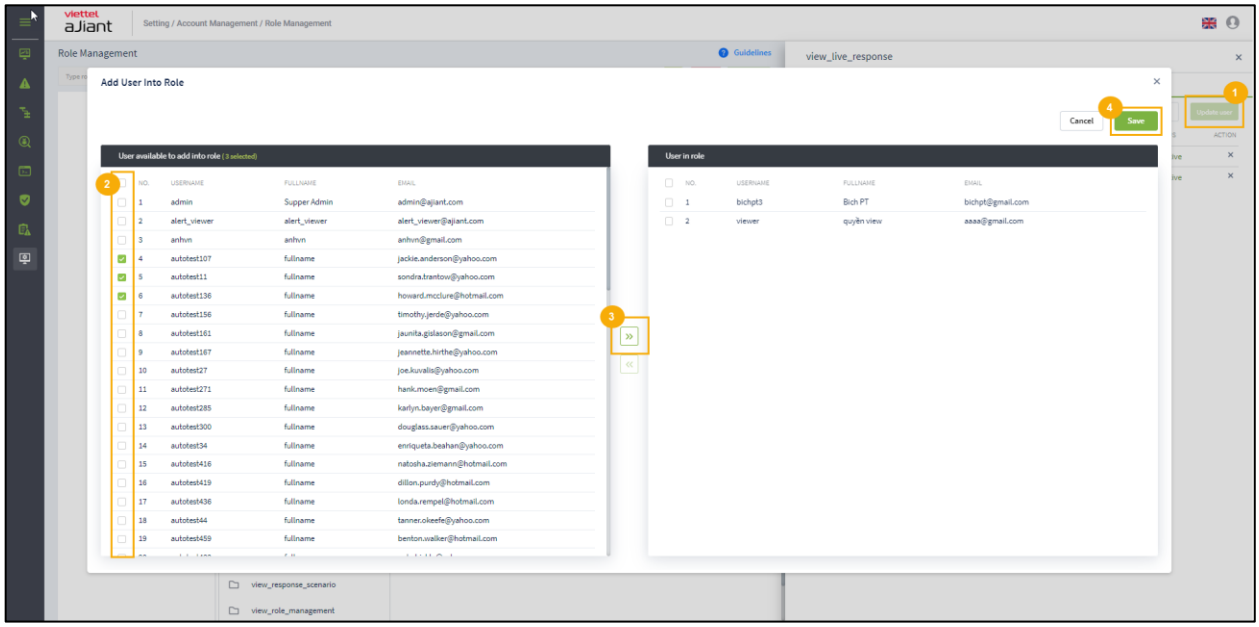


Bước 3: Chuyển sang tab User list để thêm role vào danh sách role của User

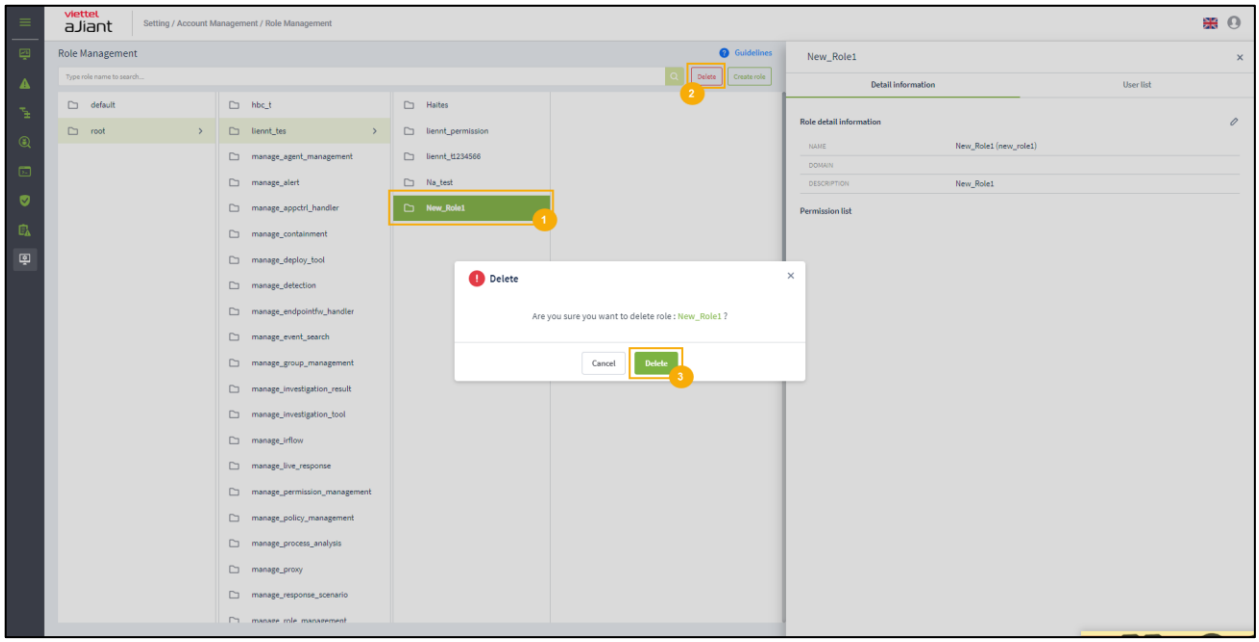
+ User đăng nhập thuộc group root: Hiển thị tất cả User trong hệ thống;
+ User đăng nhập thuộc group default: Hiển thị user chỉ thuộc default;

+ User đăng nhập thuộc group cha: Hiển thị User đang login và user thuộc group con có role cũng thuộc group role con của role user đang login;

+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị user đang login;



4 – Xóa role: click vào role cần xóa, chọn “Delete” > click OK trên màn hình confirm

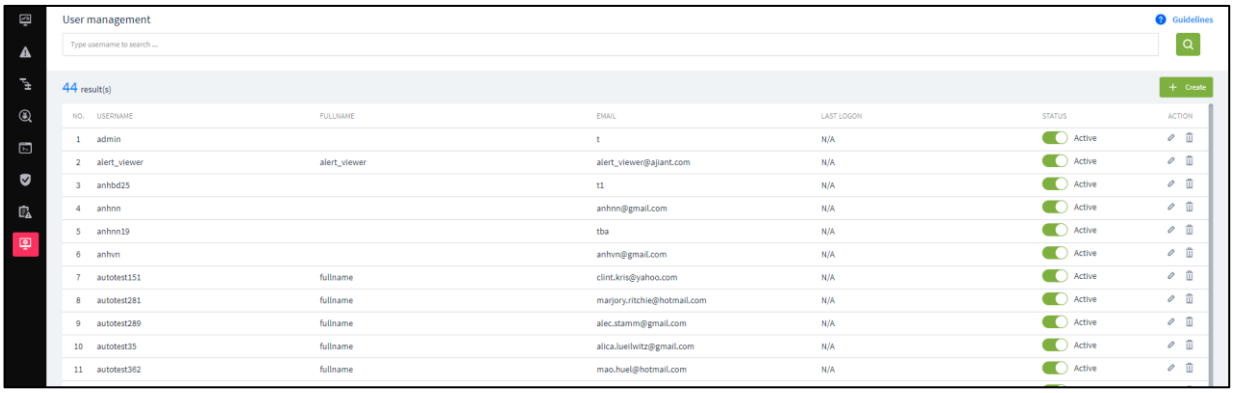


Lưu ý: Sau khi xóa 1 role, tất cả các user sử dụng role này được thay đổi: Nếu user X nằm trong role bị xóa và user X chỉ có 1 role thì chuyển user X về role mặc định, ngược lại, nếu user X có nhiều role thì chỉ loại bỏ role bị xóa ra khỏi danh sách role của user X.

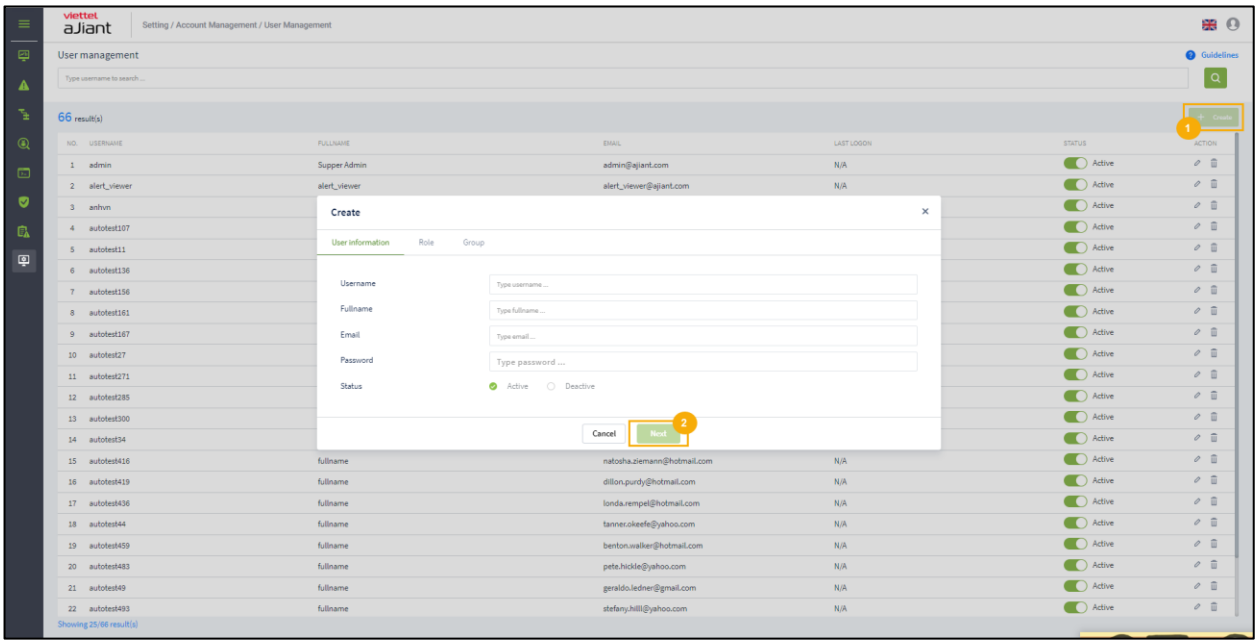
3.4.4.3 *User management*

- Quản lý các tài khoản đăng nhập vào hệ thống Portal VCS-aJiant.
- Các chức năng chính trên màn hình này gồm có:
  - + Tìm kiếm tài khoản;
  - + Thêm mới tài khoản;
  - + Chỉnh sửa tài khoản;
  - + Xóa tài khoản;

1 – Tìm kiếm tài khoản: click vào textbox Search > hiện danh sách các tài khoản trong hệ thống > Lựa chọn tài khoản cần tìm kiếm trong danh sách hoặc nhập ký tự <text> vào textbox để lọc bớt các tài khoản> Click “Search” hoặc chọn tài khoản cần tìm trong danh sách các tài khoản đã được lọc



- Thêm mới tài khoản: click “Create” > Nhập thông tin vào form hiện lên > click “Next”

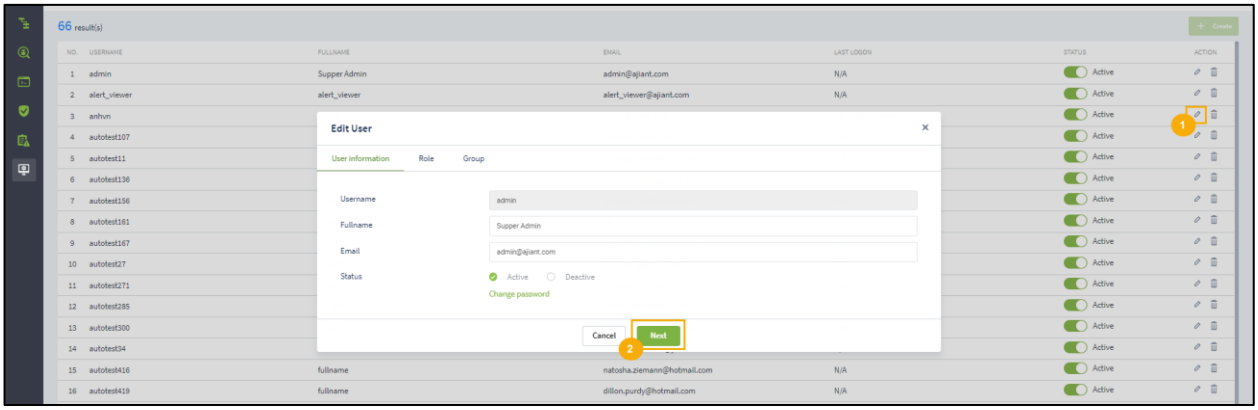


+ Lựa chọn role (nhóm quyền) sẽ gán cho tài khoản, sau đó click “next”;

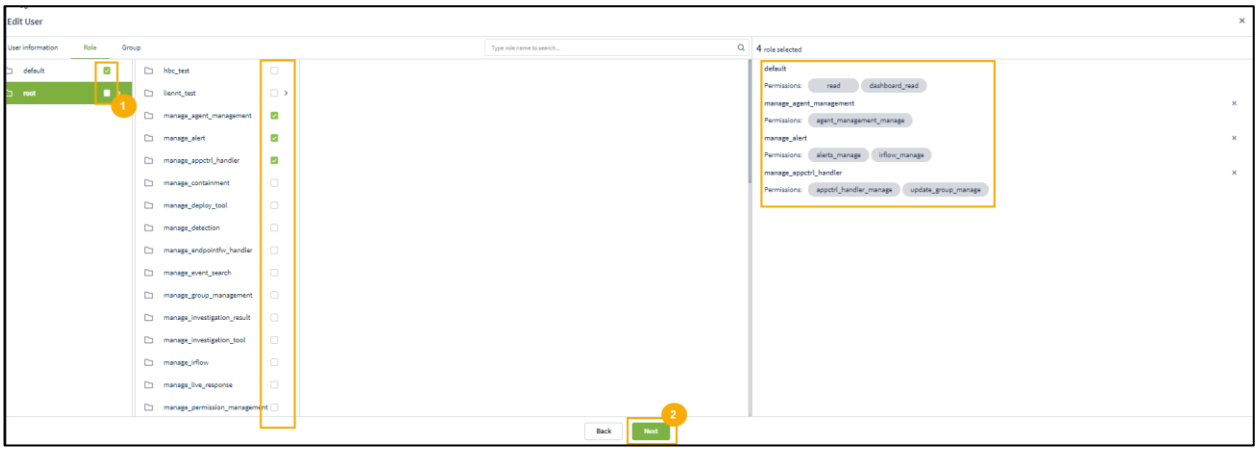
+ Khi click vào check box từng role sẽ hiện thị các permission (quyền) tương ứng với role đó:

- User đăng nhập thuộc Role root: Hiển thị tất cả Role trong hệ thống;
- User đăng nhập thuộc Role default: Hiển thị Role default;
- User đăng nhập thuộc Role cha: Hiển thị tất cả Role thuộc của user đang login và group con tương ứng;

- User đăng nhập thuộc Role có một hoặc nhiều con: Hiển thị tất cả Role thuộc Role của user đang login;



- Trên màn hình add role cho User, có thể tìm kiếm các role tương tự phần tìm kiếm tài khoản, sau khi nhập các ký tự tìm kiếm vào textbox “Search” > click icon Search hoặc Enter hiện màn hình các role thỏa mãn điều kiện tìm kiếm;



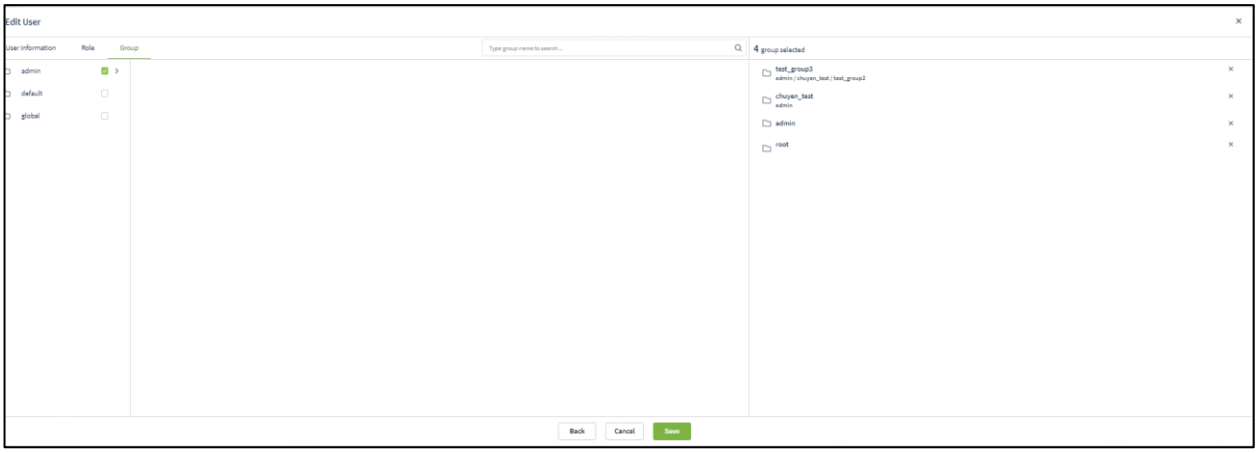
+ Click chọn checkbox tương ứng với role cần thêm, sau đó click “Go to role” để về màn hình danh sách role ban đầu, sau đó click “Create” để tạo tài khoản;

+ Lưu ý: Tài khoản đang đăng nhập tạo 1 tài khoản mới chỉ tạo được các tài khoản chứa các role con thuộc danh sách role mà tài khoản đang đăng nhập được cấp;

+ Lựa chọn group sẽ gán cho tài khoản, sau đó click “Create”;

+ Khi click vào check box từng role sẽ hiện thị các permission (quyền) tương ứng với role đó;

- User đăng nhập thuộc group root: Hiển thị tất cả Group trong hệ thống;
- User đăng nhập thuộc group default: Hiển thị group default;
- User đăng nhập thuộc group cha: Hiển thị Group thuộc group của user đang login và group con tương ứng;
- User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tất cả Group thuộc group của user đang login;



+ Click chọn checkbox tương ứng với group cần thêm, sau đó click “Go to role” để về màn hình danh sách group ban đầu, sau đó click “Create” để tạo tài khoản.

- Xóa tài khoản: click vào icon Xóa sau đó click OK trên màn hình confirm

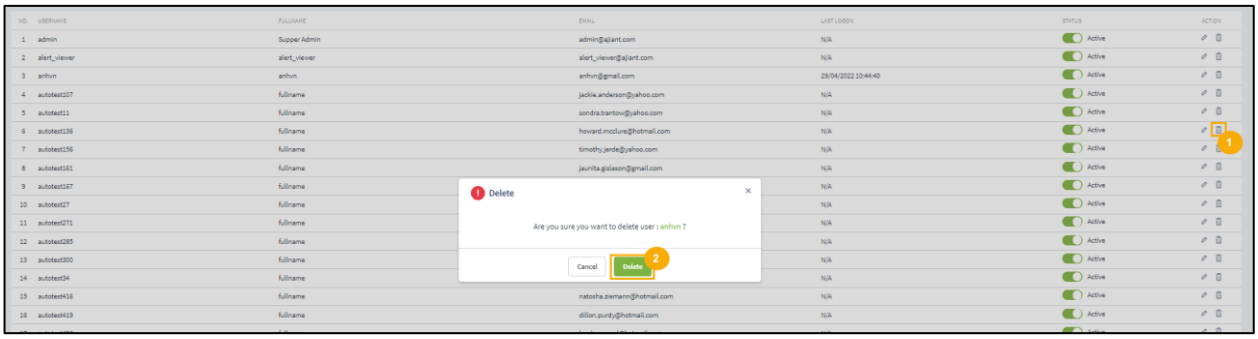
Kiểm tra hiển thị icon xóa:

+ User đăng nhập thuộc group root: Hiển thị tất cả User trong hệ thống;

+ User đăng nhập thuộc group default: Hiển thị user chỉ thuộc default;

+ User đăng nhập thuộc group cha: Hiển thị User đang login và user thuộc group con có role cũng thuộc group role con của role user đang login;

+ User đăng nhập thuộc group một hoặc nhiều con: Hiển thị user đang login;



3.4.5 Update management

3.4.5.1 *Update groups*

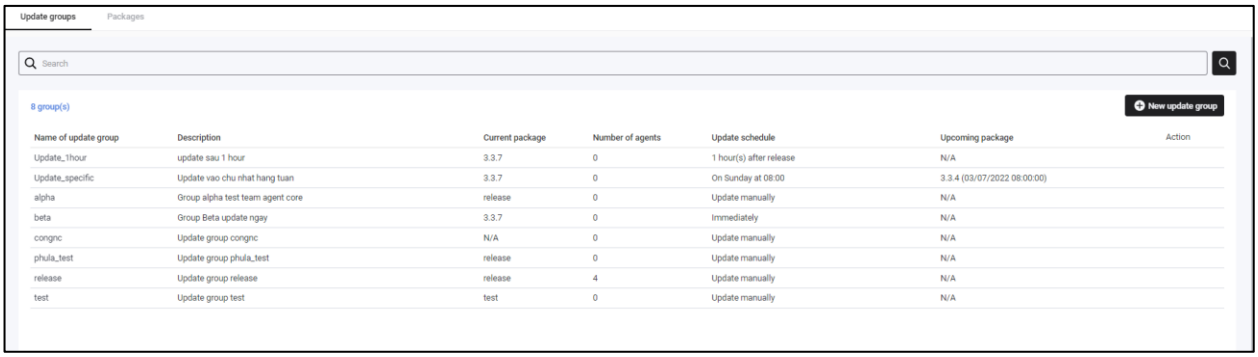
- Mục đích: là tính năng cho phép quản lý, tạo mới và cập nhật các Update Group (Chia các Agent thành các nhóm cập nhật, giúp dễ dàng phân chia, quản lý)

1 – Tìm kiếm:

Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;

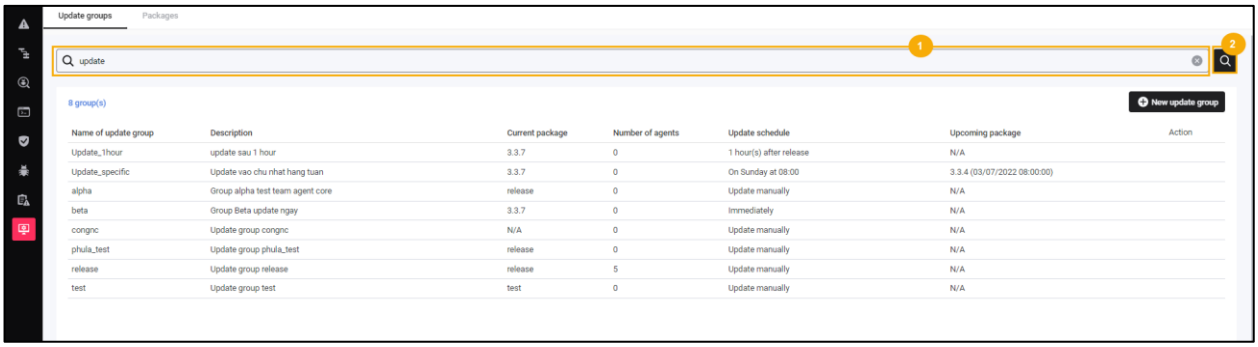
Bước 2: Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;

Bước 3: Chọn Update Management, hệ thống hiển thị Danh sách Update Group;



Bước 4: Chọn Update Management, hệ thống hiển thị Danh sách Update Group;

Bước 5: Nhập từ khóa tìm kiếm vào ô textbox và chọn nút “Search”

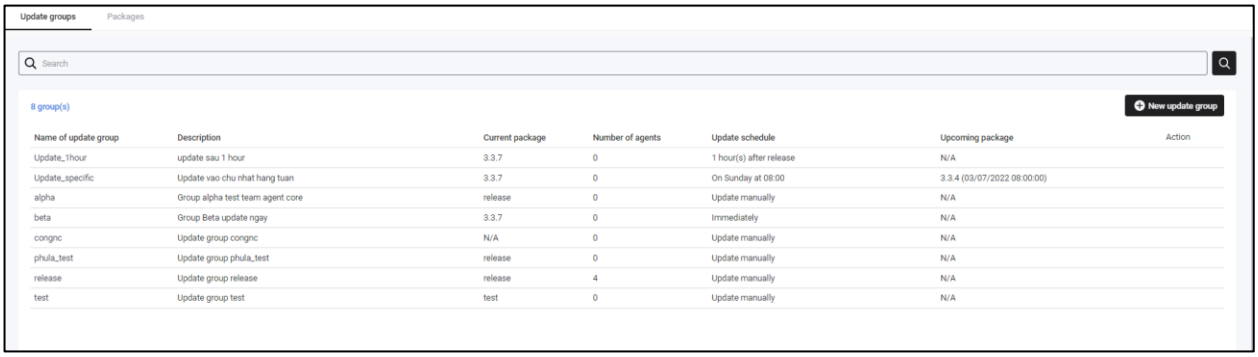


2 – Thêm mới Update groups:

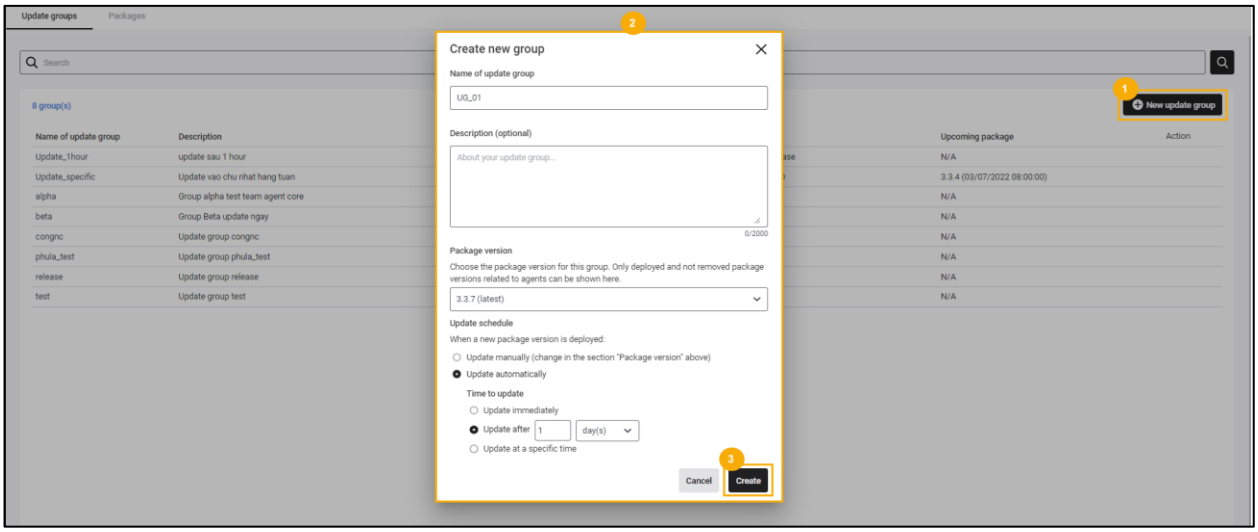
Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;

Bước 2: Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;

Bước 3: Chọn Update Management, hệ thống hiển thị Danh sách Update Group;



Bước 4: Chọn nút “New update group”, hệ thống hiển thị màn hình thêm mới Update Group;



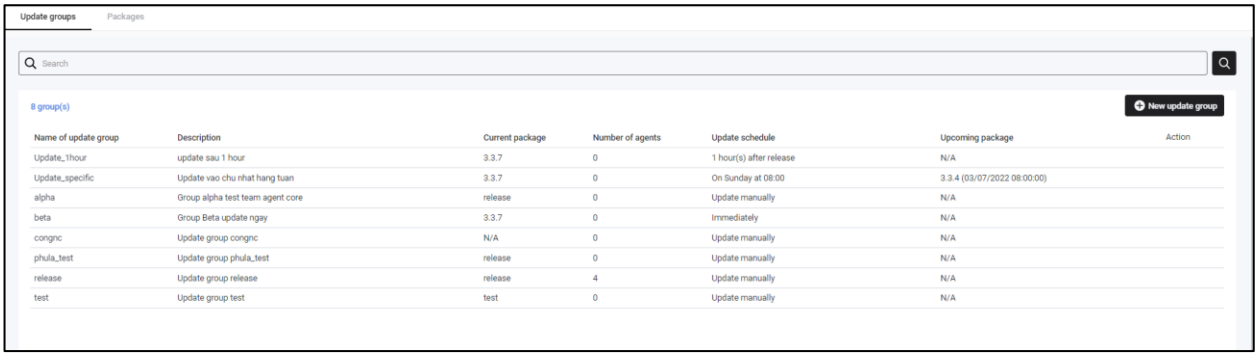
Bước 5: Nhập thông tin thêm mới Update Group và chọn nút “Create”. Hệ thống ghi nhận và quay về màn hình danh sách Update Group.

3 – Cập nhật Update groups:

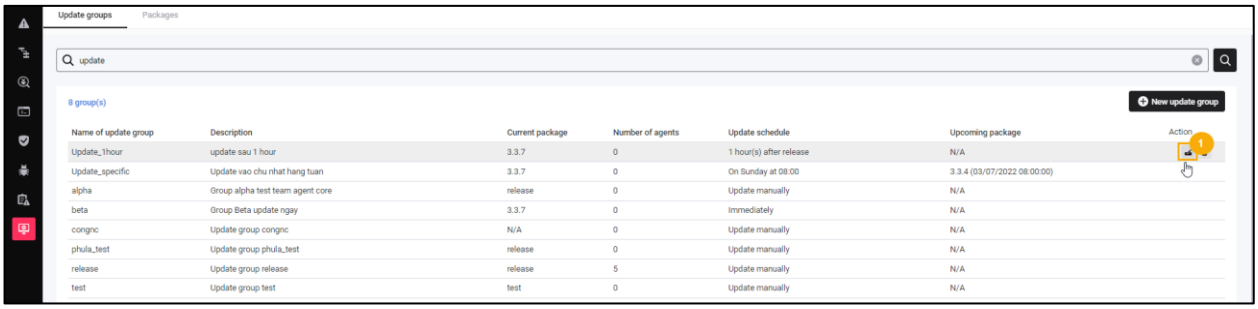
Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;

Bước 2: Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;

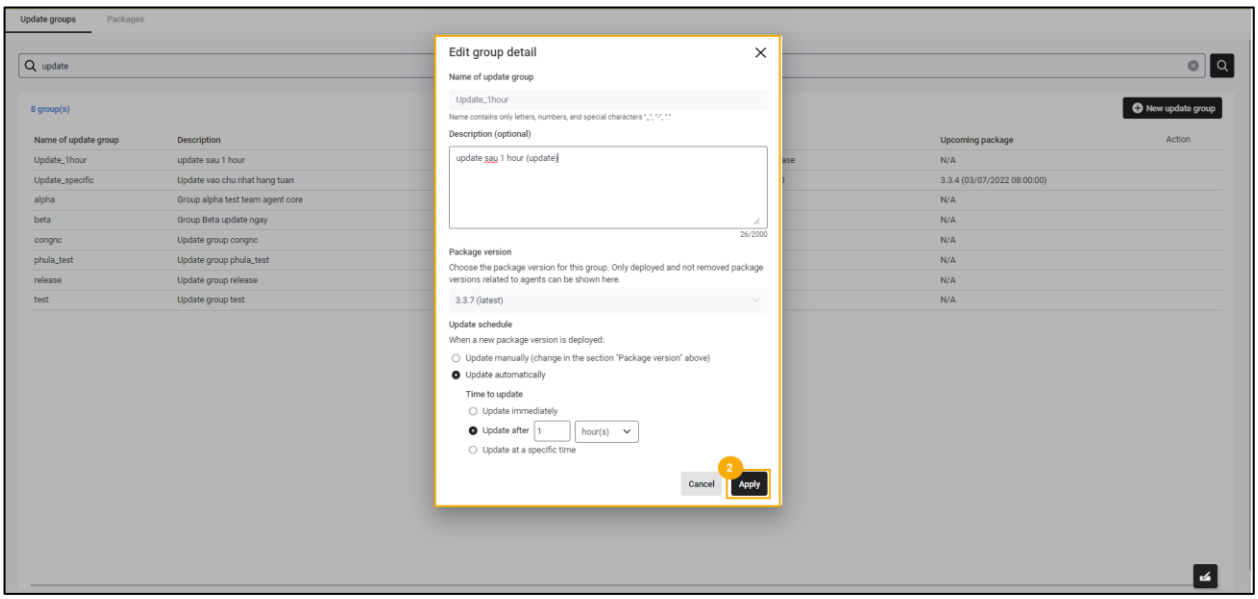
Bước 3: Chọn Update Management, hệ thống hiển thị Danh sách Update Group;



Bước 4: Tại bản ghi cần cập nhật/ chỉnh sửa thông tin, chọn icon “Cập nhật” thông tin Update Group:



Bước 5: Hệ thống hiển thị màn hình thông tin chi tiết Update Group, cho phép cập nhật/ chỉnh sửa thông tin và lưu lại bằng cách chọn nút “Apply”:

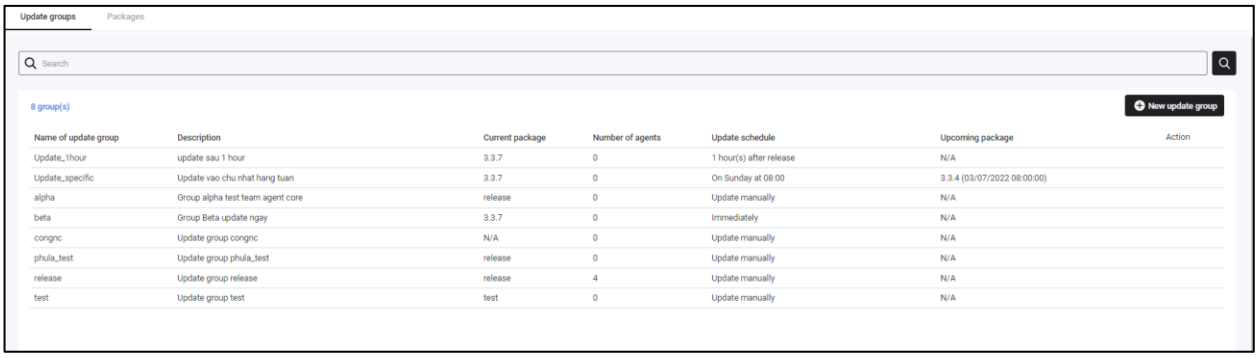


4 – Xóa Update groups:

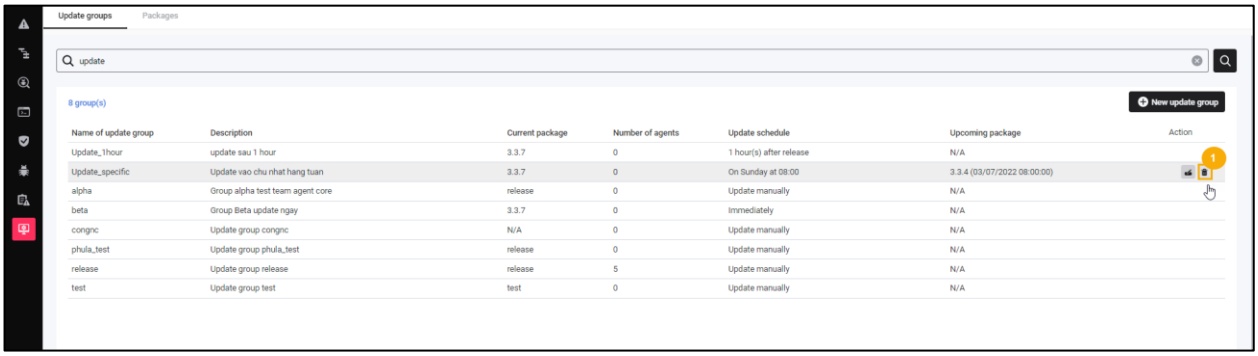
Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;

Bước 2: Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;

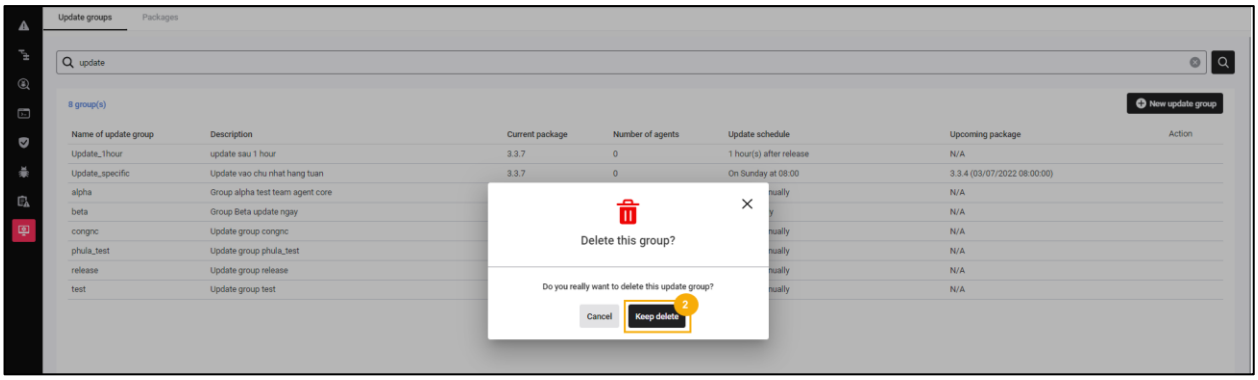
Bước 3: Chọn Update Management, hệ thống hiển thị Danh sách Update Group;



Bước 4: Tại bản ghi cần xóa, chọn icon “Xóa” Update Group:



Bước 5: Hệ thống hiển thị Popup Xác nhận xóa Update Group, Người dùng chọn nút “Delete” để xác nhận yêu cầu Xóa Update Group và chọn nút “Cancel” để hủy yêu cầu Xóa Update Group.



3.4.5.2 *Update packages*

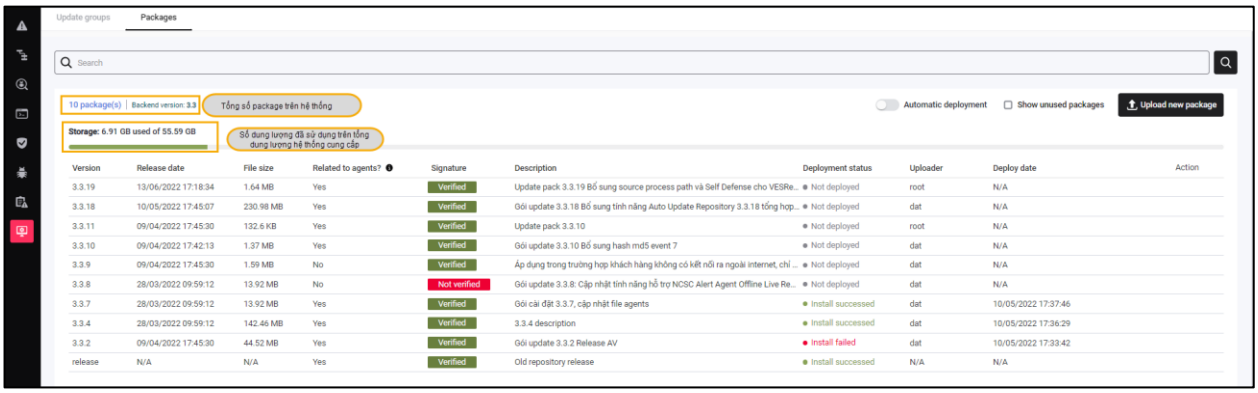
1 – Tìm kiếm packages:

Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;

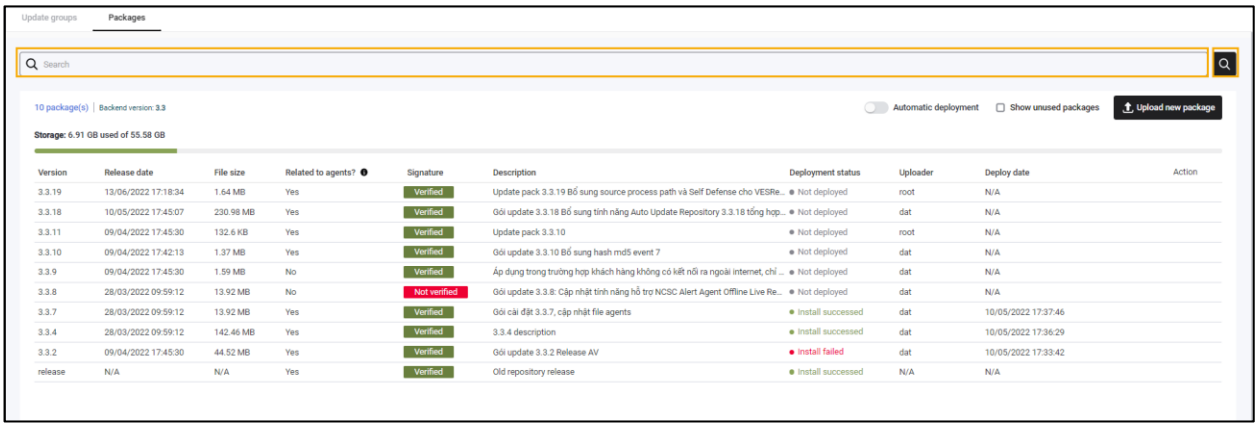
Bước 2: Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;

Bước 3: Chọn Update Management, hệ thống hiển thị Danh sách Update Group;

Bước 4: Chọn tab "Package", hệ thống hiển thị Danh sách Pakage trong hệ thống;



Bước 5: Nhập từ khóa tìm kiếm vào ô textbox và chọn nút "Search"



2 – Auto Update

- Mục đích: là tính năng cho phép tự động triển khai các bản update tới khách hàng một cách nhanh chóng và hiệu quả. Auto Update cho phép upload các gói qua giao diện portal hoặc tự động lấy các bản update qua trang hub.viettelcybersecurity.com;

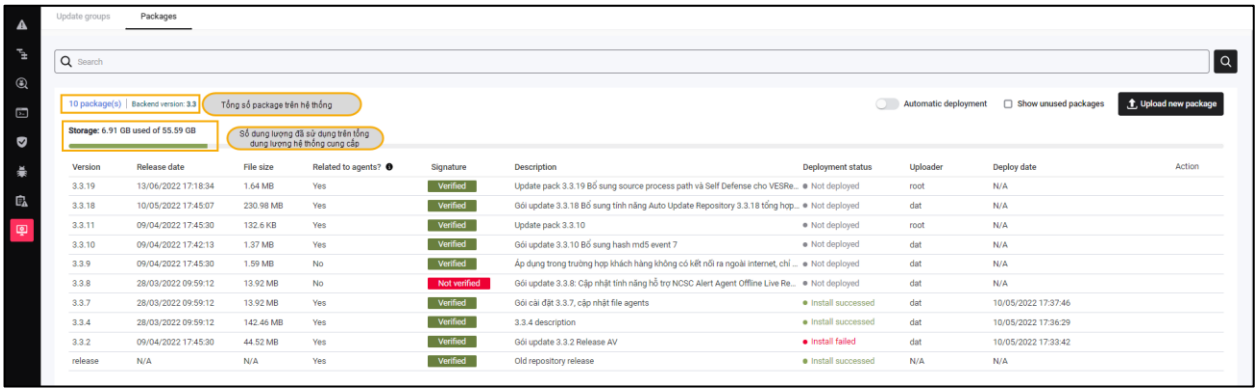
Lưu ý: Đội triển khai gửi lại các thông tin trên cho đội dự án Ajiant để cập nhật vào hệ thống để cho phép triển khai gói tự động tại khách hàng. Về sau, khi cần triển khai gói update mới, đội triển khai hoặc phía khách hàng chỉ cần lấy gói update được cung cấp và upload lên portal ajiant và chọn triển khai gói.

Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;

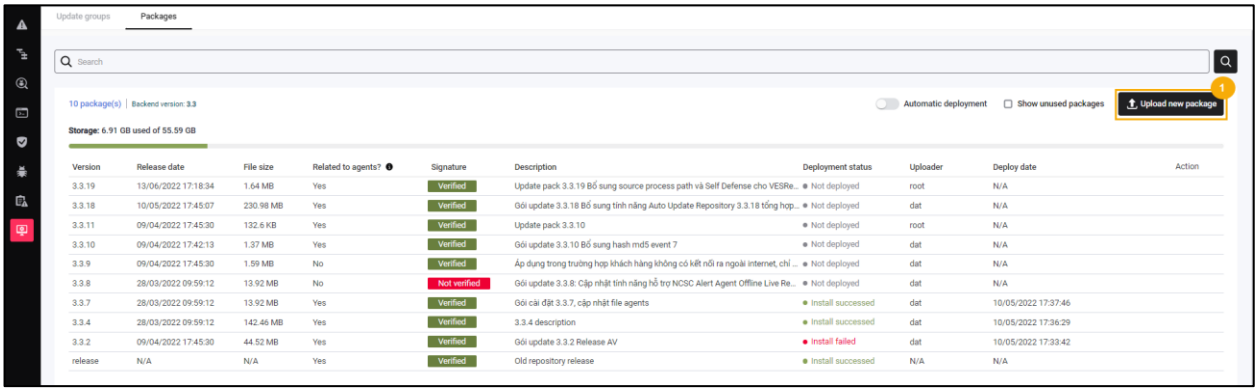
Bước 2: Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;

Bước 3: Chọn Update Management, hệ thống hiển thị Danh sách Update Group;

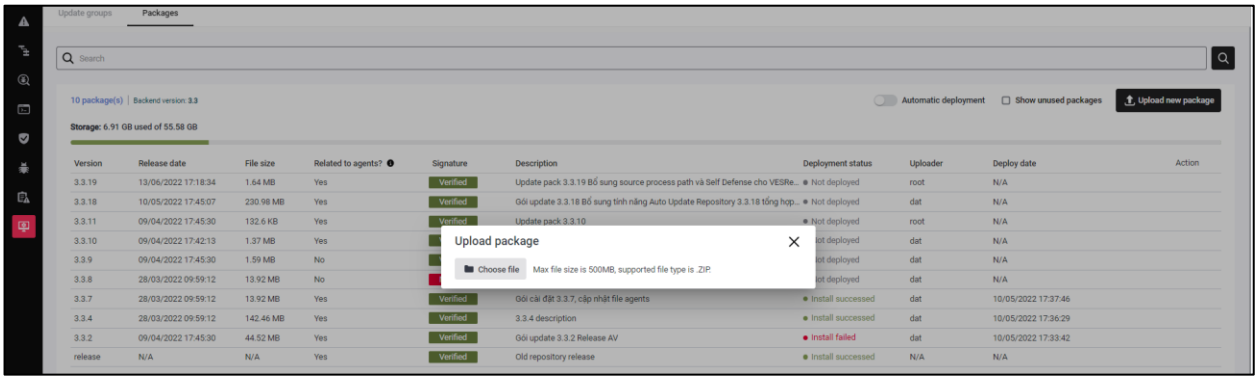
Bước 4: Chọn Tab “Package”, hệ thống hiển thị Danh sách Pakage trong hệ thống;



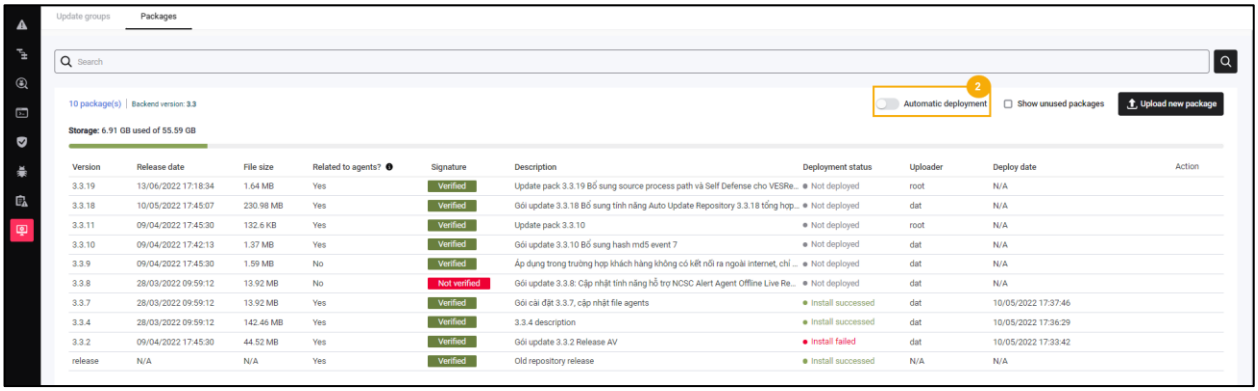
Bước 5: Chọn nút “Update new package”, hệ thống hiển thị Popup “Upload package”;



Bước 6: Chọn tải lên package;



Bước 7: Bật/ Tắt Action "Automatic Development" để tự động triển khai các bản cập nhật package tới khách hàng.



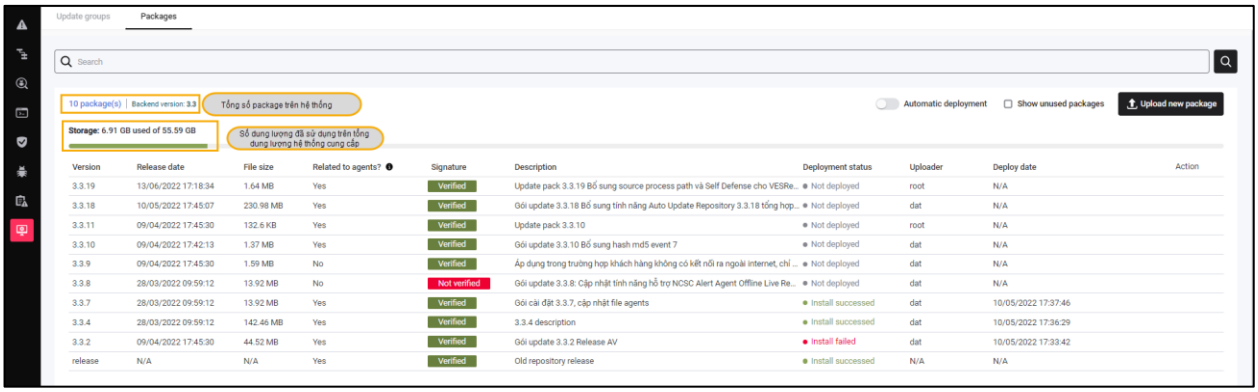
3 – Deploy package

Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;

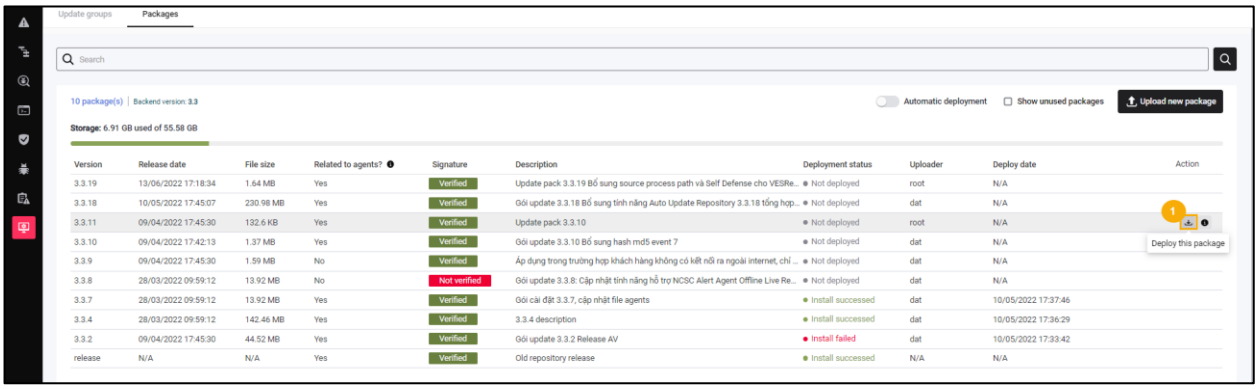
Bước 2: Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;

Bước 3: Chọn Update Management, hệ thống hiển thị Danh sách Update Group;

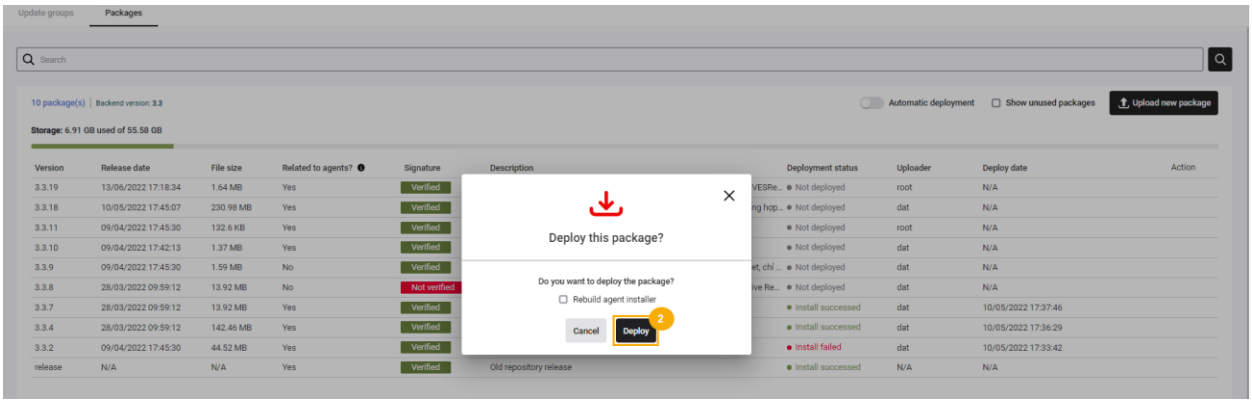
Bước 4: Chọn Tab "Package", hệ thống hiển thị Danh sách Pakage trong hệ thống;



Bước 5: Chọn icon “Deploy this package” tại bản ghi package đó, hệ thống hiển thị Popup Xác nhận Deploy package



Bước 6: Chọn nút “Deploy” để xác nhận Deploy package trên thiết bị hoặc chọn nút “Cancel” để hủy thao tác Deploy package.



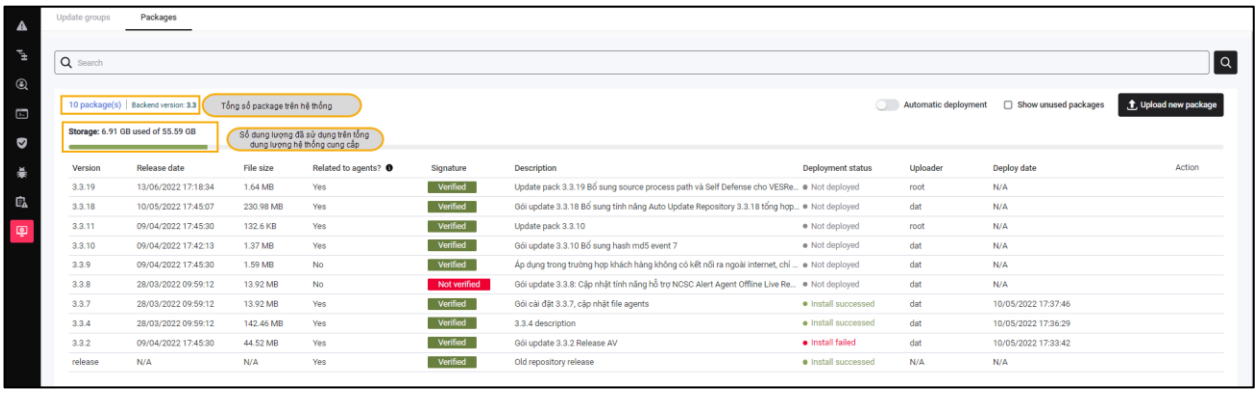
4 – Chi tiết Package

Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;

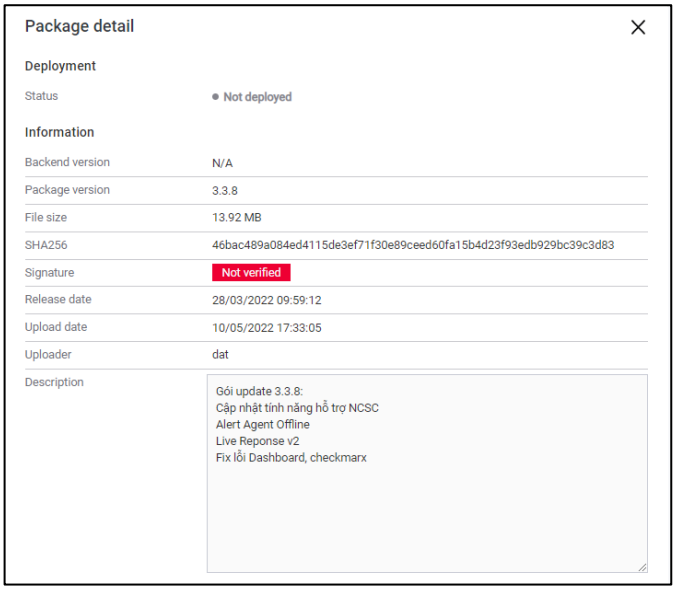
Bước 2: Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;

Bước 3: Chọn Update Management, hệ thống hiển thị Danh sách Update Group;

Bước 4: Chọn Tab "Package", hệ thống hiển thị Danh sách Pakage trong hệ thống;



Bước 5: Chọn icon "View Detail" tại bản ghi package đó, hệ thống hiển thị Popup thông tin chi tiết của Package vừa chọn:



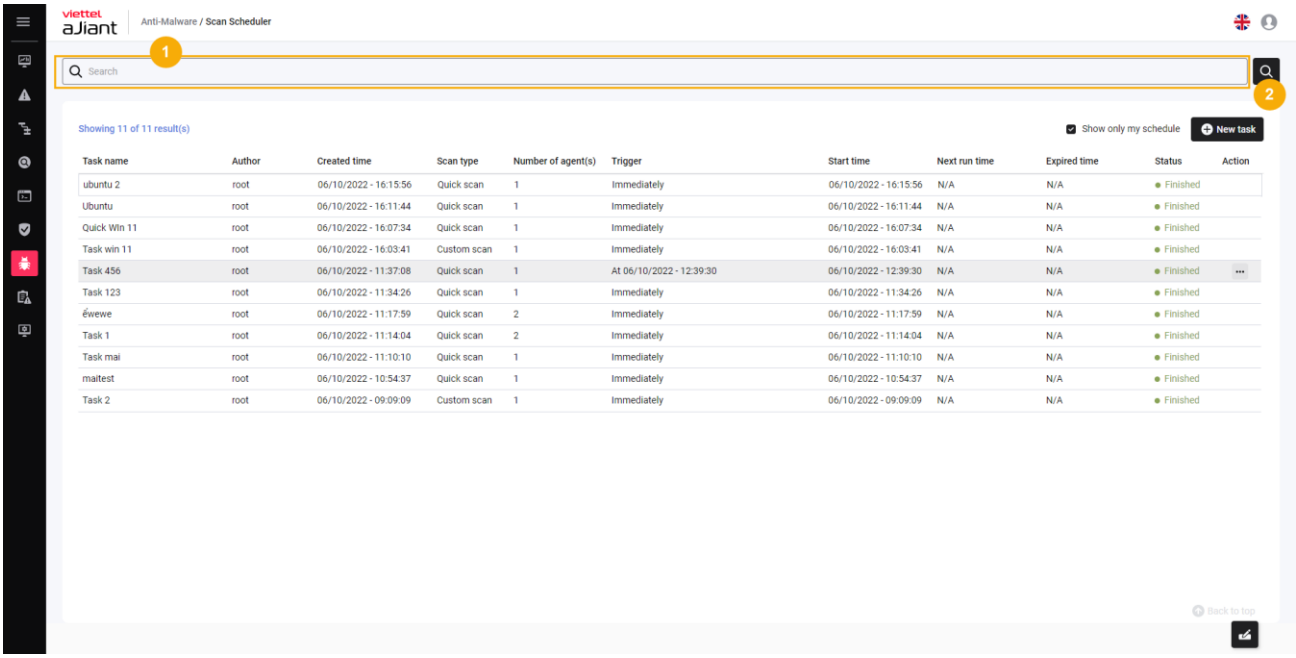
3.5 Anti – Malware

3.5.1 Scan Schedule

- Mục đích: Chức năng Scan Schedule cho phép người dùng lập lịch quét virus dưới các máy trạm từ xa.

3.5.1.1 *Tìm kiếm Scan Schedule task*

- Mục đích: Chức năng tìm kiếm Scan Schedule task cho phép người dùng tìm kiếm các lập lịch quét dưới các máy trạm theo Task name.
- Các bước thực hiện:



Bước 1: Người dùng nhập vào từ khóa tìm kiếm;

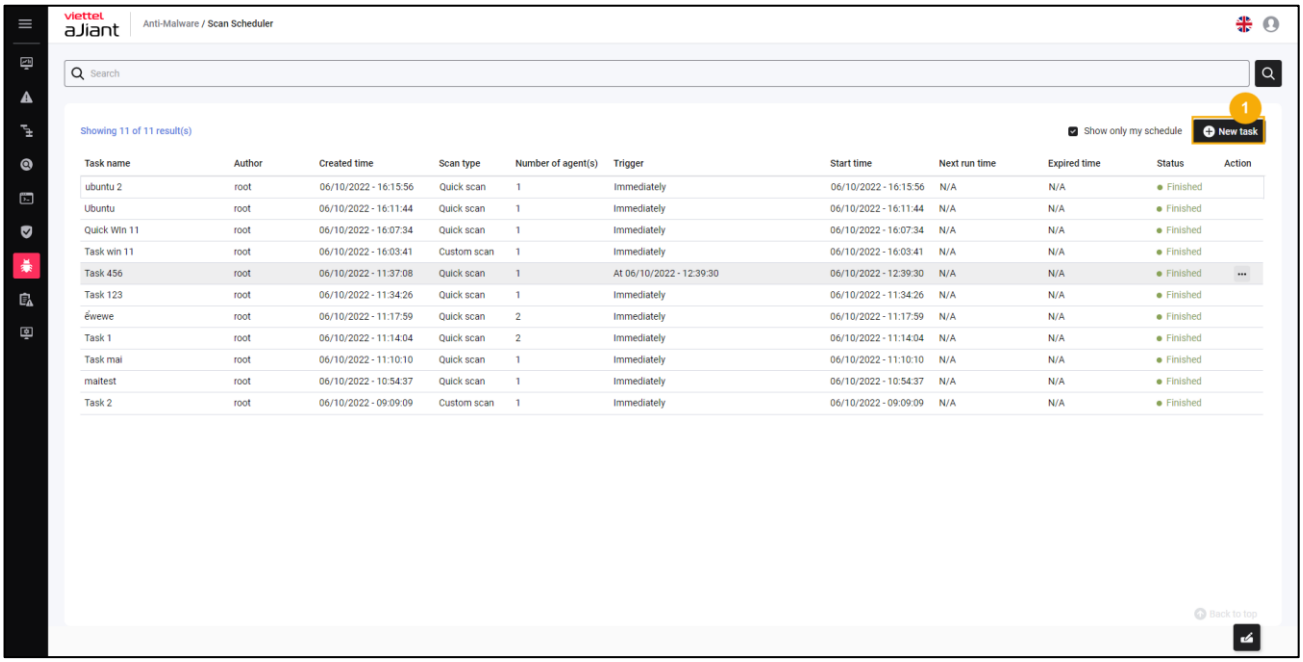
Bước 2: Chọn nút 🔍 hoặc nhấn **Enter** để xác nhận thao tác tìm kiếm với từ khóa vừa nhập.

Bước 3: Hệ thống sẽ hiển thị danh sách lập lịch quét theo từ khóa tìm kiếm.

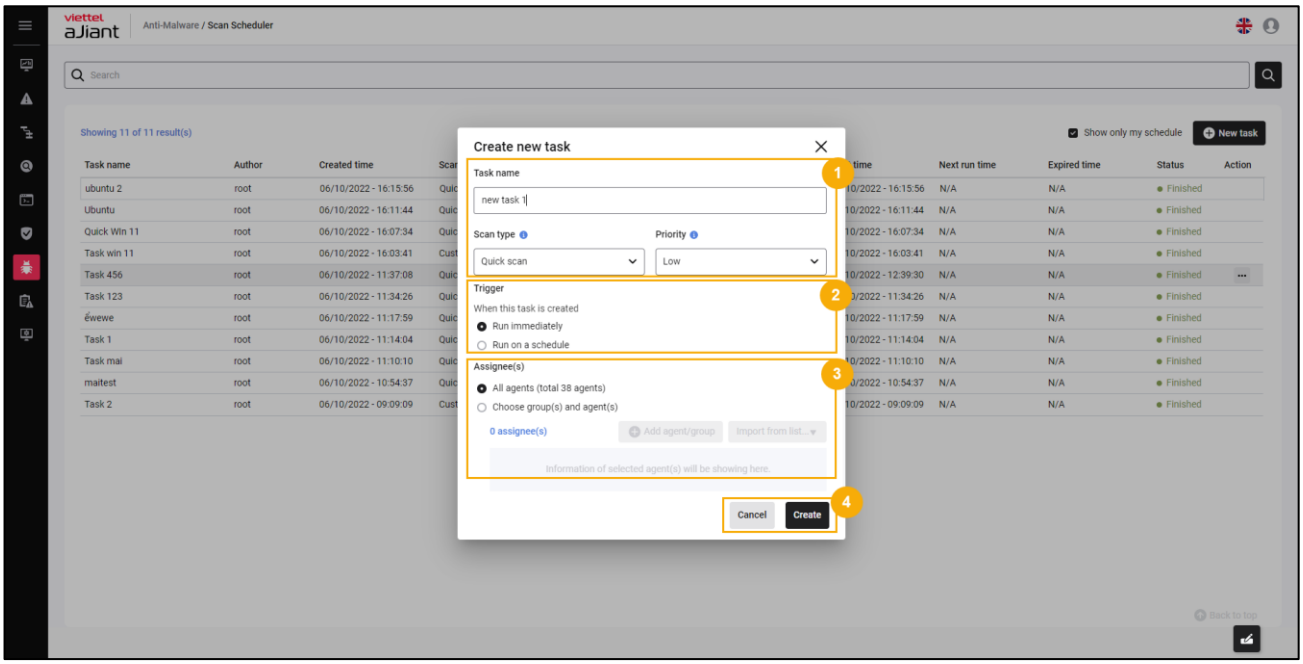
3.5.1.2 *Thêm mới Scan Schedule task*

- Mục đích: Cho phép người dùng thêm mới một lập lịch quét, cấu hình thời gian và thông tin máy trạm.
- Các bước thực hiện:

Bước 4: Tại màn hình danh sách lập lịch quét, người dùng chọn nút **New task**



Bước 5: Hệ thống hiển thị màn hình thêm mới một lập lịch quét, người dùng nhập vào các thông tin:



5 – Thông tin lập lịch quét bao gồm: Task name, Scan type, Priority

- Task name: Người dùng nhập vào tên lập lịch quét;
- Scan type: Người dùng lựa chọn một trong 3 loại scan. Cho phép:

+ Quét nhanh: Kiểm tra nhanh các tệp và thư mục đáng ngờ tiềm ẩn;

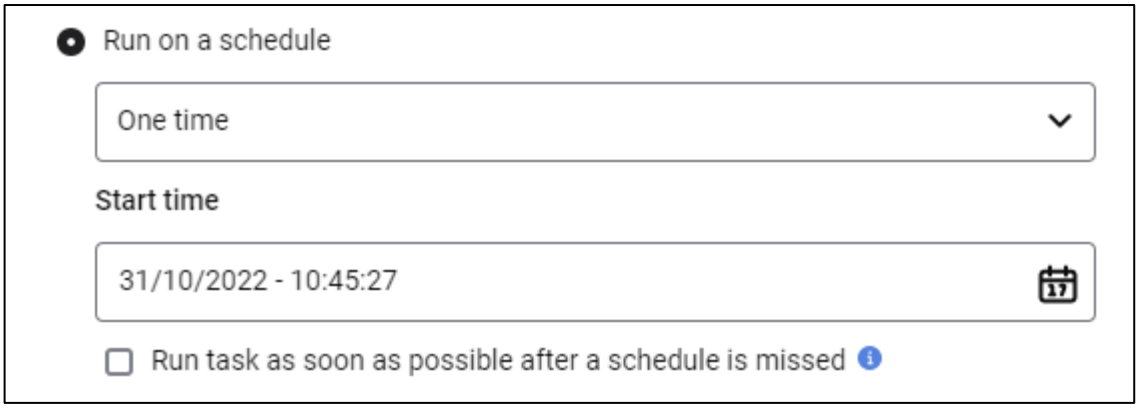
+ Quét toàn bộ: Kiểm tra toàn bộ các tệp và thư mục trong máy tính. Quá trình này có thể mất vài giờ để hoàn thành;

+ Quét tùy chỉnh: Cho phép người dùng một tệp / thư mục cụ thể trong máy tính của bạn để quét.

- Priority: Cho phép người dùng lựa chọn tốc độ quét và thay đổi mức độ chiếm dụng tài nguyên của máy. Khi đặt mức ưu tiên cao, hệ thống sẽ quét nhanh chóng, tuy nhiên sẽ tiêu tốn nhiều tài nguyên của CPU. Tương tự, nếu chọn mức độ ưu tiên thấp, hệ thống sẽ quét chậm hơn và tiết kiệm tài nguyên CPU.

6 – Thông tin Trigger cho phép người dùng lựa chọn loại lập lịch quét:

- Run immediately: Cho phép người dùng lập lịch quét ngay lập tức dưới các máy trạm khi task vừa được tạo thành công;
- Run on Schedule: Cho phép người dùng lập lịch quét theo cấu hình của người dùng:



+ Schedule:

- One time: Lập lịch quét một lần;
- Daily: Lập lịch quét hàng ngày;
- Weekly: Lập lịch quét hàng tuần;

- Monthly: Lập lịch quét hàng tháng;

+ Start time: Cho phép người dùng nhập vào thời gian bắt đầu lập lịch quét

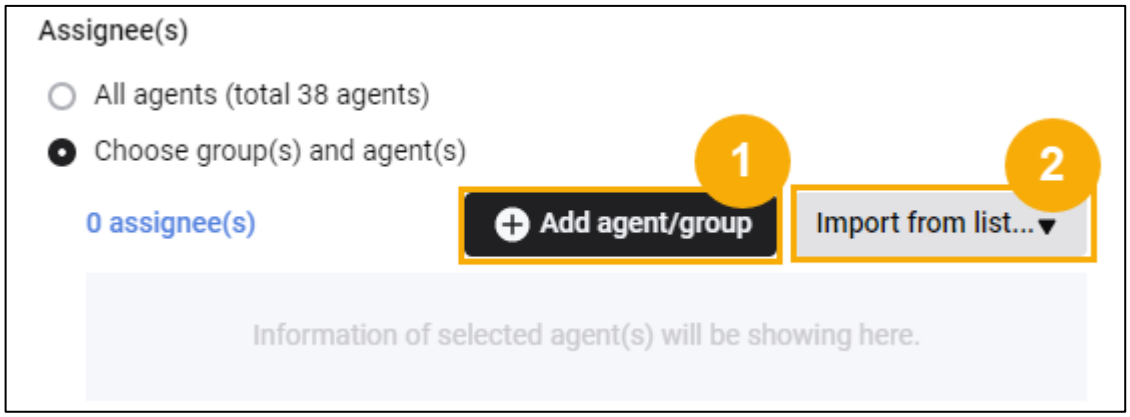
+ Ví dụ: Schedule: Daily, Start time: 15/08/2022 – 03:00:00. Được hiểu là cấu hình lập lịch quét hàng ngày lúc 03:00:00;

+ Run task as soon as possible after schedule is missed: Cho phép người dùng cấu hình lập lịch quét lại ngay khi lập lịch trước bị bỏ lỡ.

7 – Thông tin Assignee: Cho phép người dùng cấu hình thông tin các máy trạm nhận lập lịch

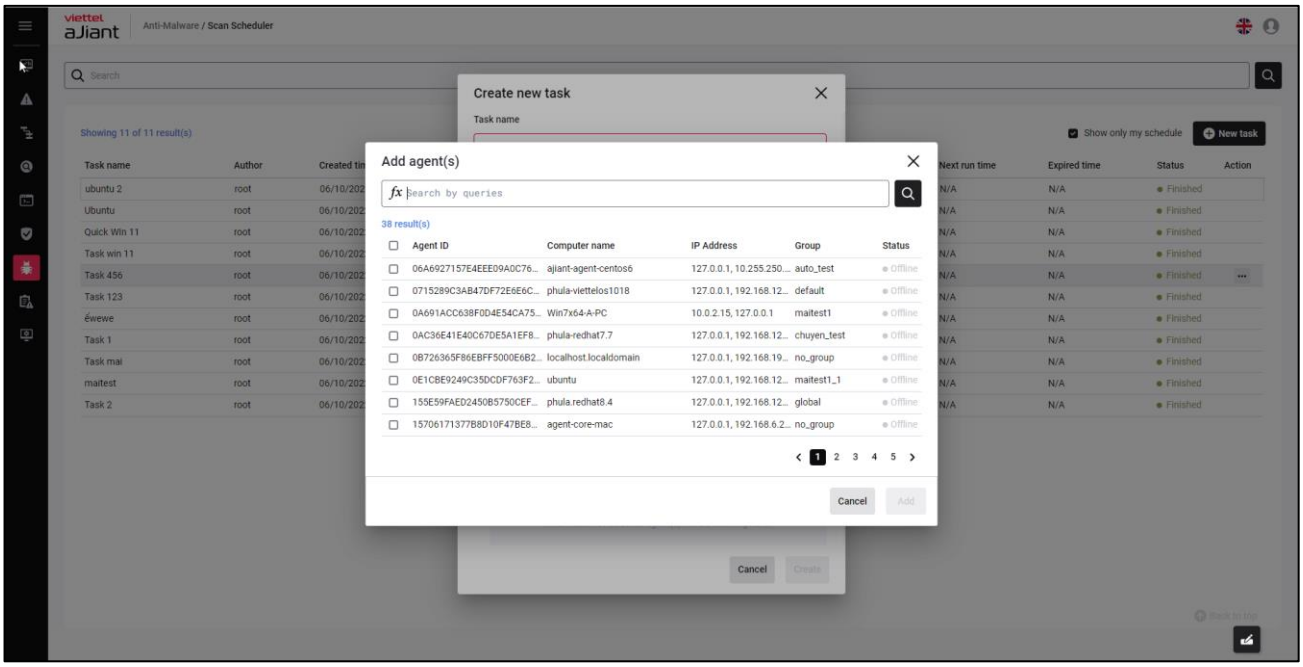
- All Agent(s): Lập lịch với tất cả các máy trạm thuộc quyền quản lý của người dùng đang đăng nhập;
- Choose Agent(s) or Group(s):

+ Mục đích: Cho phép cấu hình, lựa chọn các máy trạm hoặc các nhóm máy trạm:

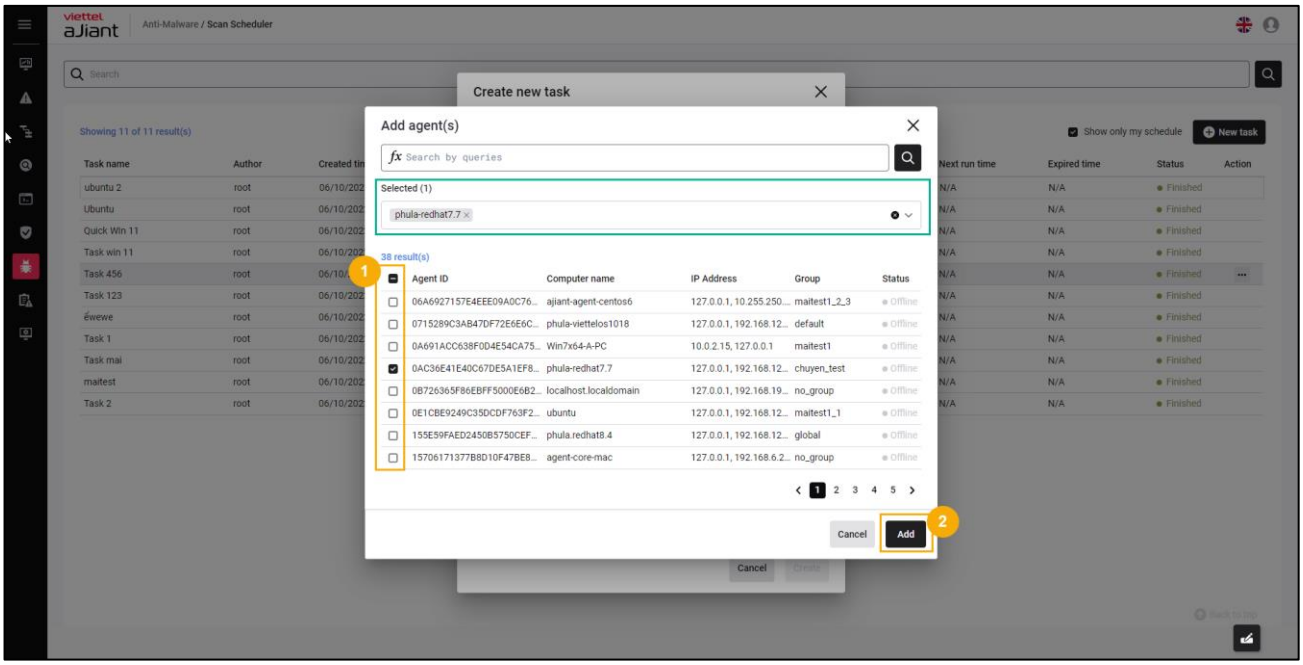


+ Các bước thực hiện: Add Agents or Group

- Add Agents or Group - Người dùng chọn **Add Agent**. Hệ thống hiển thị popup lựa chọn máy trạm:



- Tìm kiếm máy trạm:
  - Tại popup Add agent(s), người dùng có thể tìm kiếm máy trạm theo truy vấn các trường thông tin: AgentID, Computer name, IP Adress, Group, Status, …
  - Người dùng chọn icon 🔍 hoặc nhấn nút **Enter** để xác nhận tìm kiếm;
  - Hệ thống sẽ hiển thị danh sách máy trạm theo truy vấn.
- Tích chọn một hoặc nhiều các máy trạm để thực thi lập lịch quét:



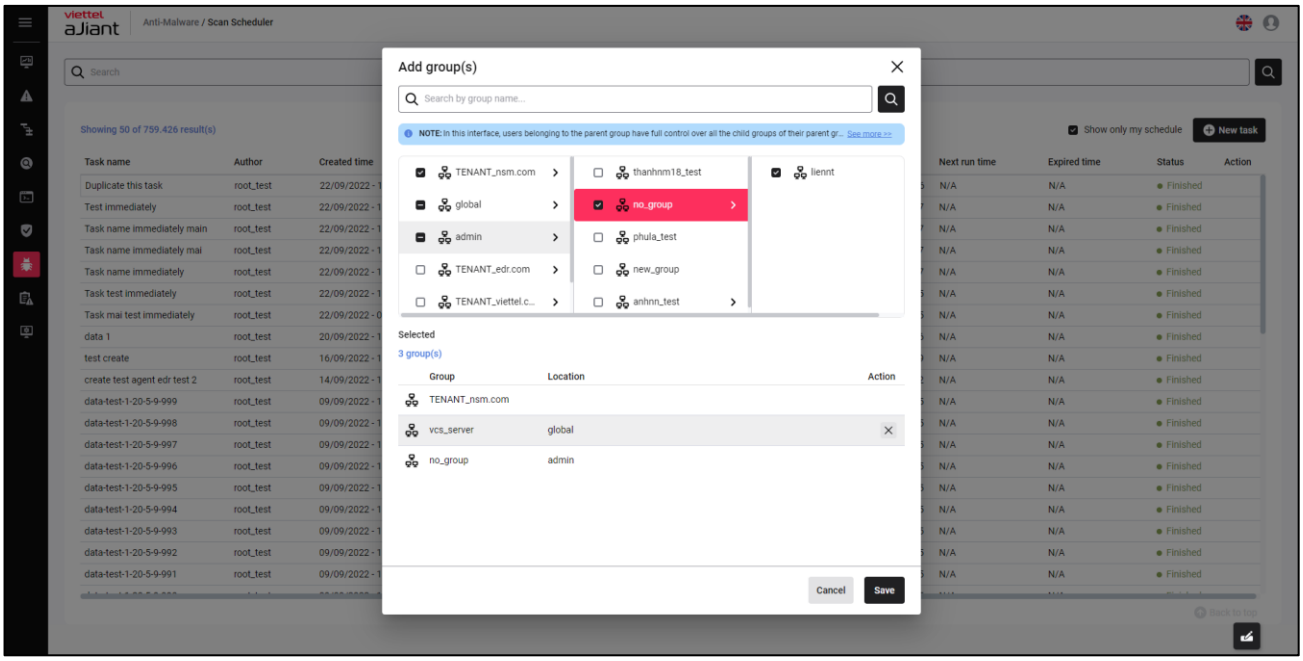
- Chọn nút **Add** để thực hiện thêm thông tin Agent/ Group → HT quay lại danh sách Agent/ Group;
- Hoặc chọn nút **Cancel** để thực hiện hủy thao tác thêm thông tin Agent/ Group;

➔ Danh sách các máy trạm được lựa chọn sẽ được tự động thêm vào khung thông tin máy trạm đã được chọn.

- Add Agents or Group - Người dùng chọn **Add Group**. Hệ thống hiển thị popup lựa chọn group:
  - Tìm kiếm group:
    - Tại popup Add group(s), người dùng có thể tìm kiếm máy trạm theo truy vấn các trường thông tin: Group name
    - Người dùng chọn icon hoặc nhấn nút Enter để xác nhận tìm kiếm;

➔ Hệ thống sẽ hiển thị danh sách group

  - Tích chọn một hoặc nhiều group để thực thi lập lịch quét:



- Chọn nút **Add** để thực hiện thêm thông tin Agent/ Group → HT quay lại danh sách Agent/ Group;
- Hoặc chọn nút **Cancel** để thực hiện hủy thao tác thêm thông tin Agent/ Group;

➔ Danh sách các máy trạm được lựa chọn sẽ được tự động thêm vào khung thông tin group đã được chọn.

+ Import from .CSV: Cho phép người dùng tải lên danh sách máy trạm bằng cách:

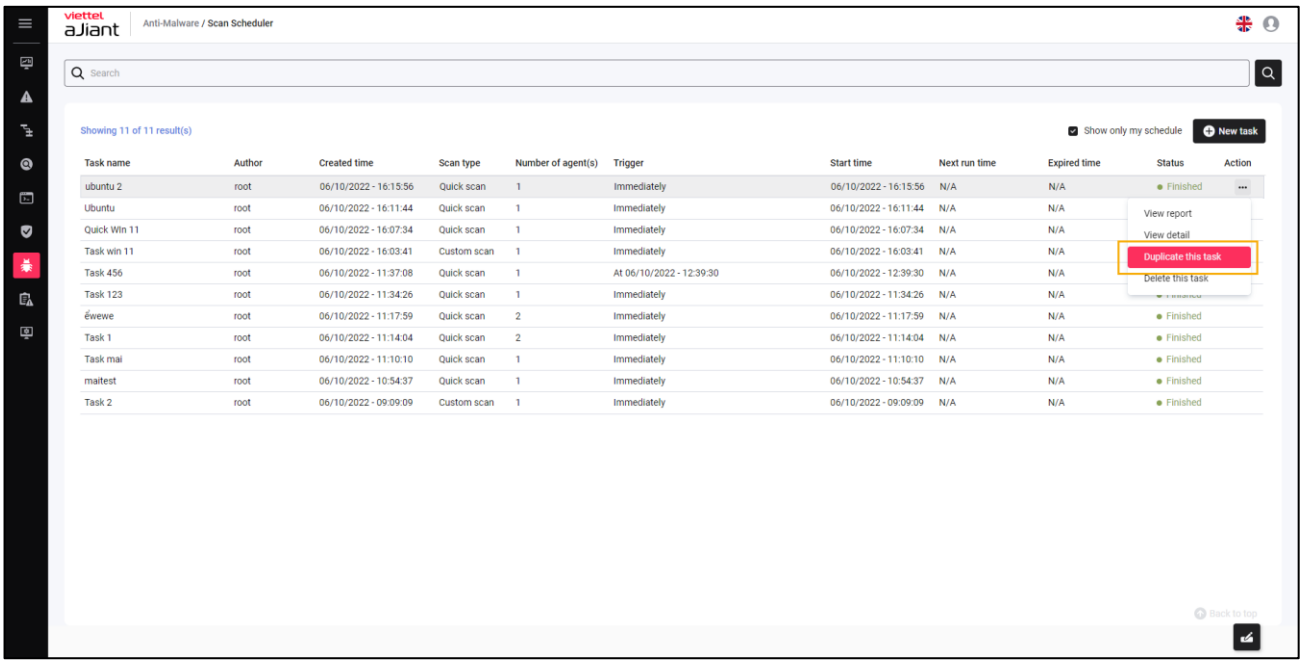
- Lựa chọn vào nút **Import from list;**
- Lựa chọn **Download sample file**, cho phép tải xuống file mẫu danh sách máy trạm;
- Người dùng nhập thông tin máy trạm và tải lên file danh sách máy trạm bằng cách chọn nút **Import from .CSV**

Bước 6: Người dùng chọn nút **Create** để hoàn thiện thao tác thêm mới lập lịch quét. Hoặc, chọn nút **Cancel** để hủy thao tác thêm mới lập lịch quét

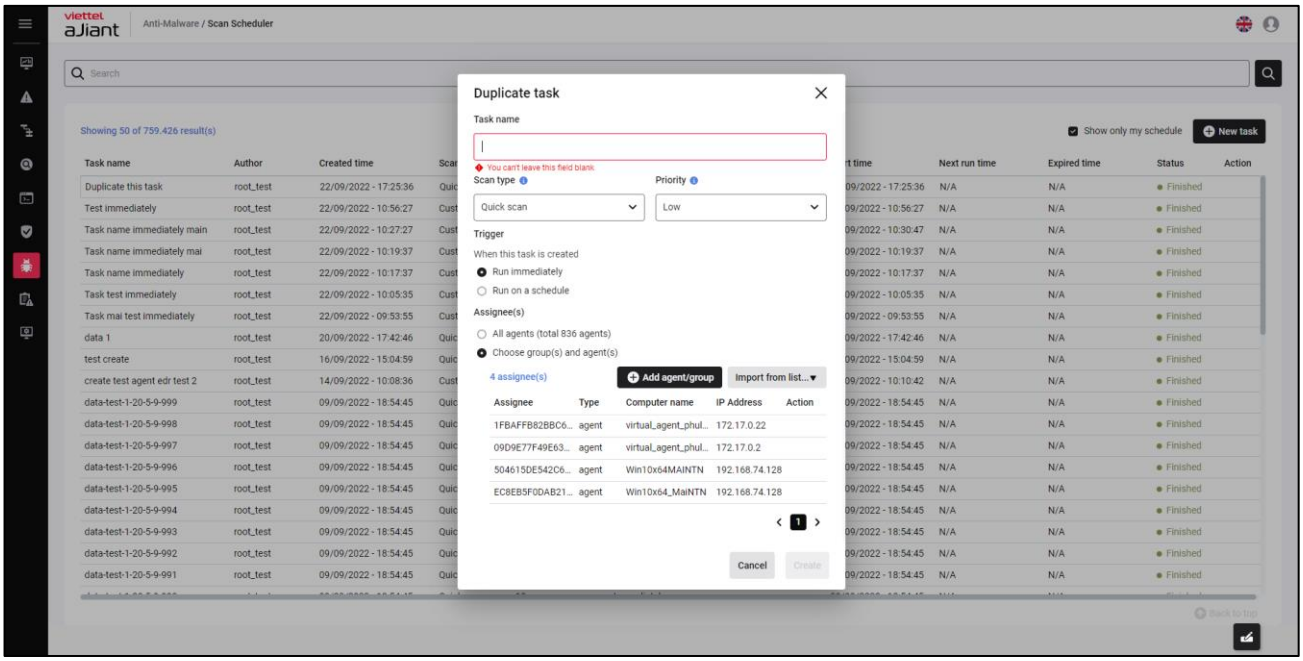
3.5.1.3 *Nhân bản Schedule task*

- Mục đích: Cho phép người dùng nhân bản lập lịch quét.
- Các bước thực hiện:

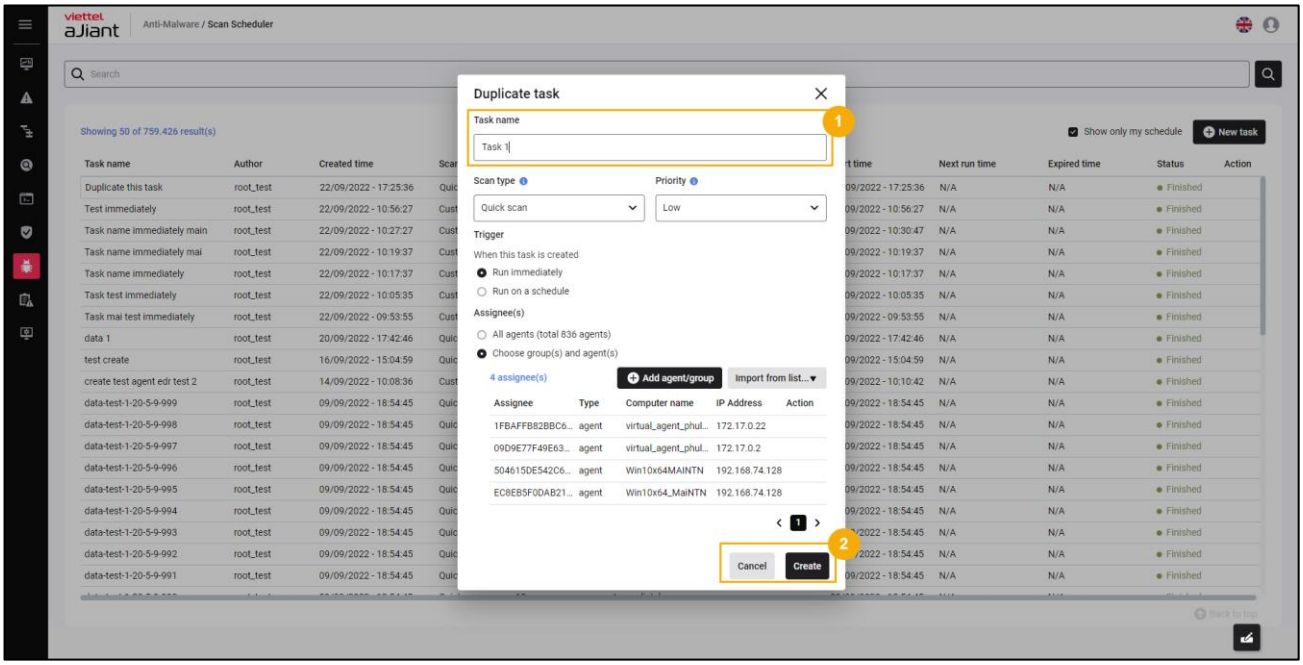
Bước 7: Tại màn hình danh sách task, người dùng chọn **Duplicate** bản ghi task cần nhân bản:



Bước 8: Hệ thống hiển thị màn hình Duplicate task, người dùng nhập lại task name và kiểm tra lại toàn bộ thông tin trước khi nhân bản



Bước 9: Người dùng chọn nút **Create** để hoàn thiện thao tác nhân bản lập lịch quét. Hoặc, chọn nút **Cancel** để hủy thao tác nhân bản lập lịch quét.

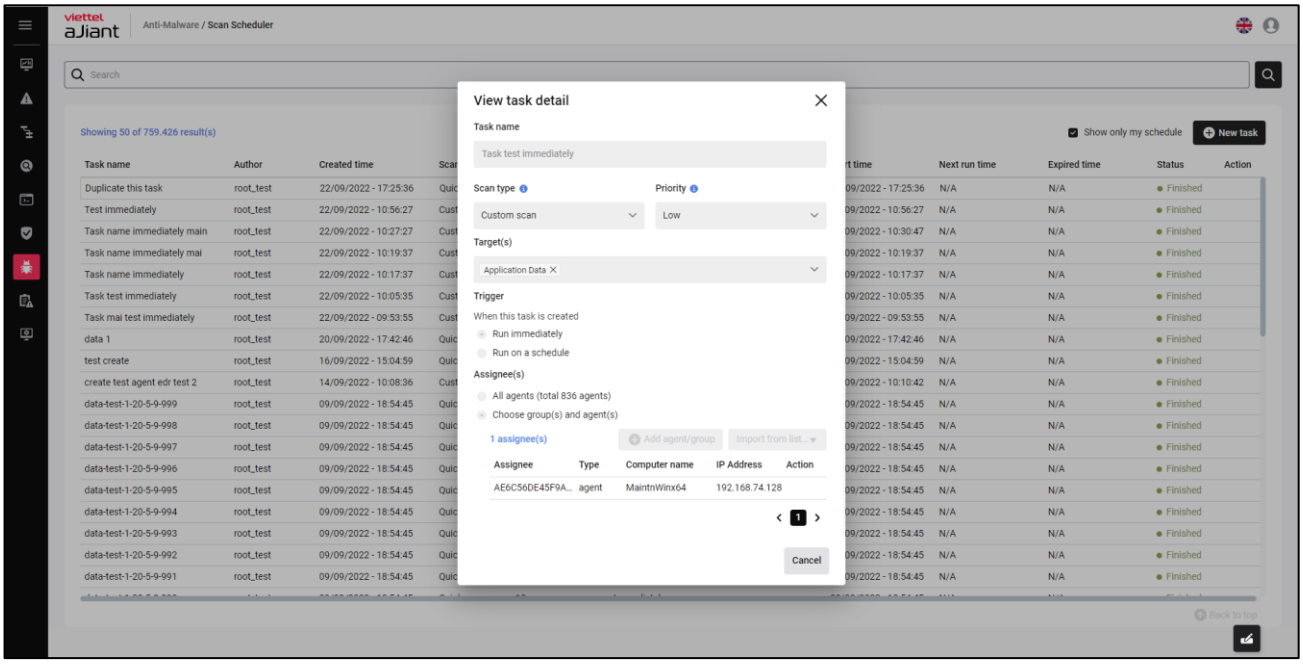


3.5.1.4 ***Xem*** chi ti***ết***

- Mục đích: Cho phép người dùng xem thông tin chi tiết lập lịch quét
- Các bước thực hiện:

Bước 10: Tại màn hình danh sách task, người dùng chọn **View Detail** bản ghi task cần xem chi tiết;

➔ Hệ thống hiển thị màn hình chi tiết lập lịch quét

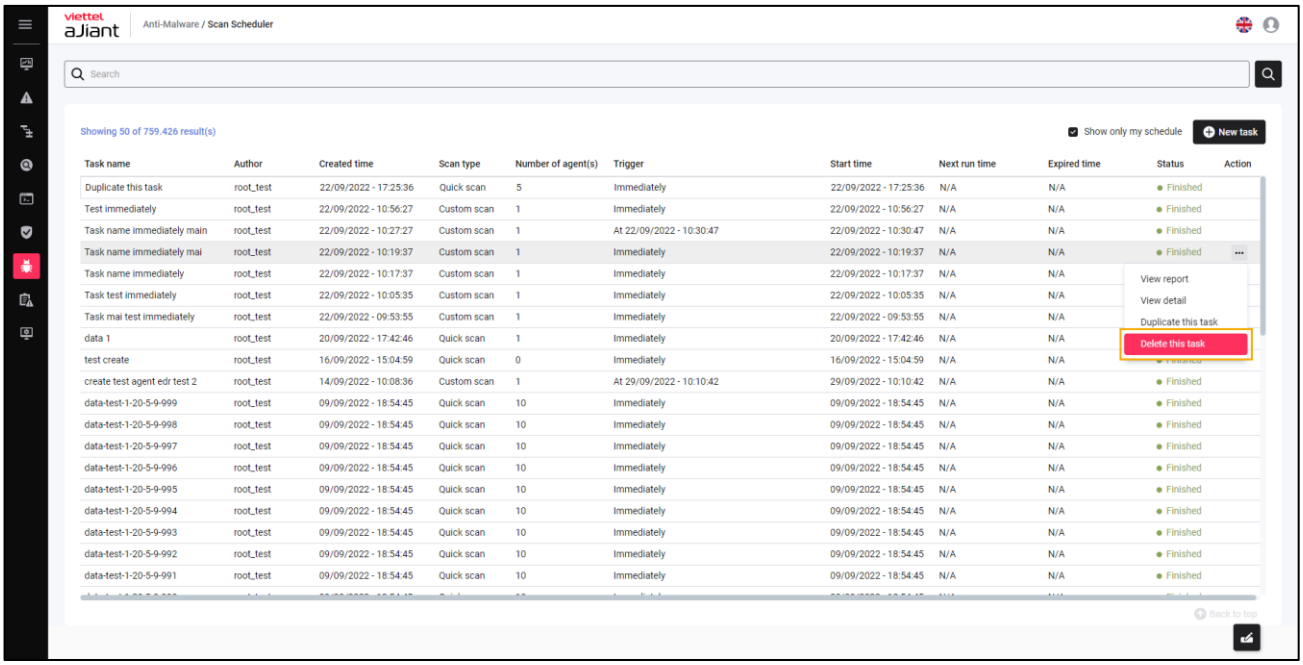


Bước 11: Người dùng chọn nút **Cancel** hoặc icon **Close** để hủy thao tác xem chi tiết lập lịch quét

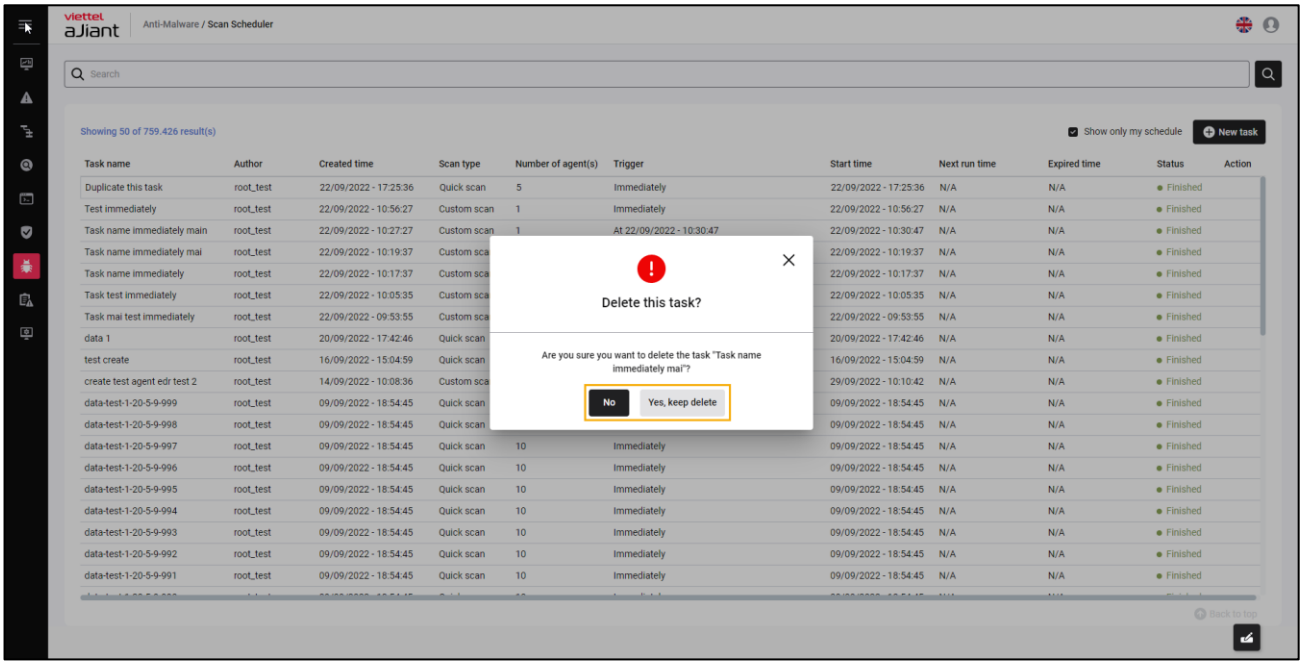
3.5.1.5 *Xóa Schedule task*

- Mục đích: Cho phép xóa lập lịch quét trong danh sách task;
- Các bước thực hiện:

Bước 12: Tại màn hình danh sách task, người dùng chọn **Delete this task** bản ghi task cần xóa;



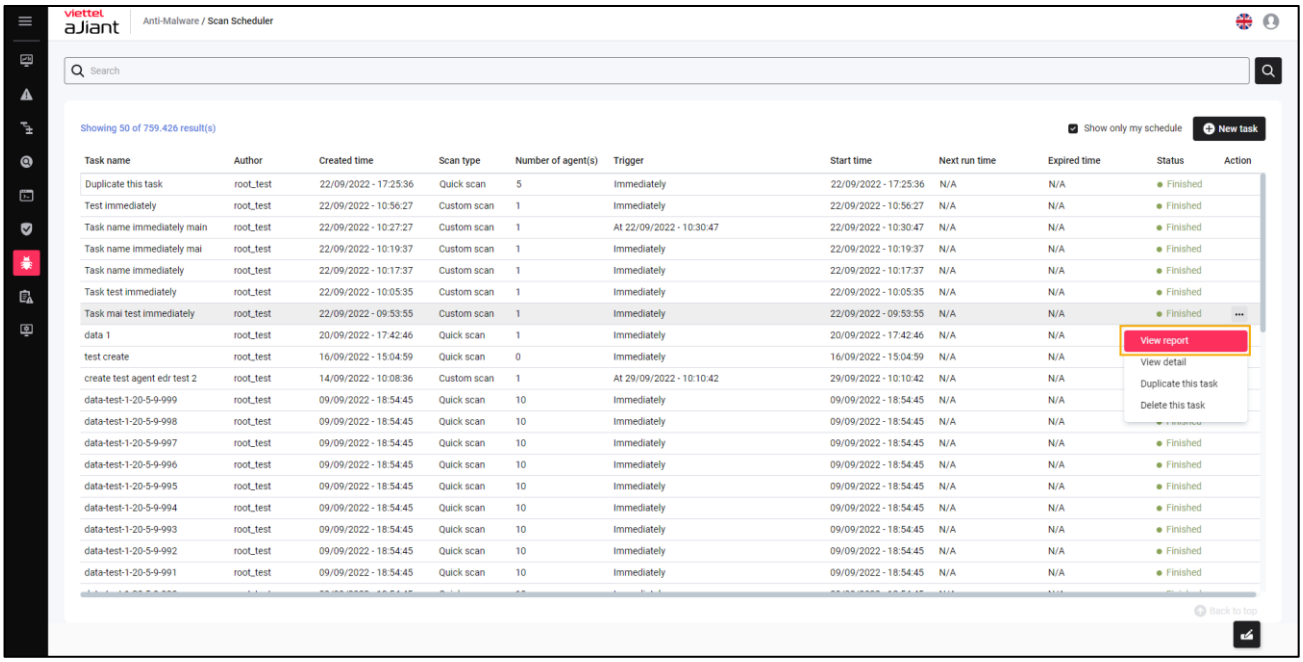
Bước 13: Hệ thống hiển thị màn hình popup Xác nhận xóa. Người dùng chọn **No** để hủy thao tác xóa lập lịch quét hoặc chọn **Yes, keep delete** để tiếp tục thao tác xóa



3.5.1.6 *Xem báo cáo*

- Mục đích: Cho phép người dùng xem báo cáo lập lịch quét;
- Các bước thực hiện:

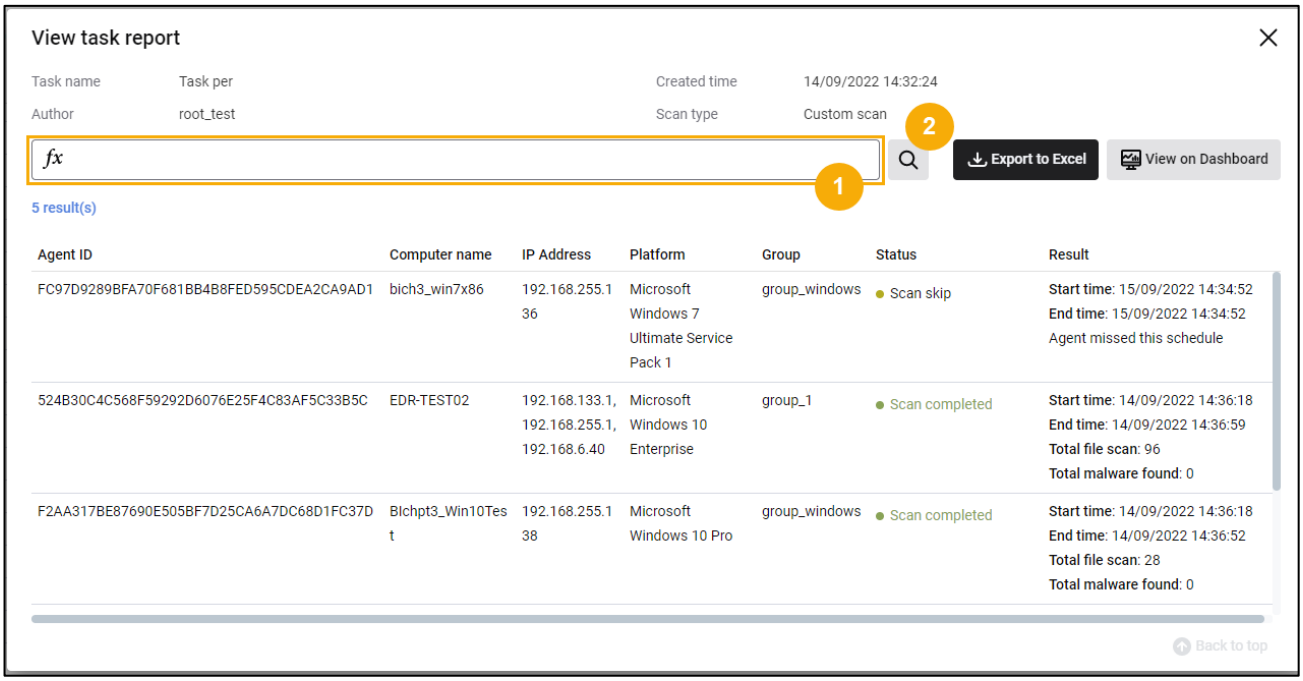
Bước 14: Tại màn hình danh sách task, người dùng chọn **View report** bản ghi task cần xem báo cáo;



Bước 15: Hệ thống hiển thị màn hình **View report**:

8 – Tìm kiếm:

- Mục đích: Cho phép tìm kiếm truy vấn các thông tin trong báo cáo như: AgentID, Computer name, IP Address, Platform, Group, Status, Result
- Các bước thực hiện:

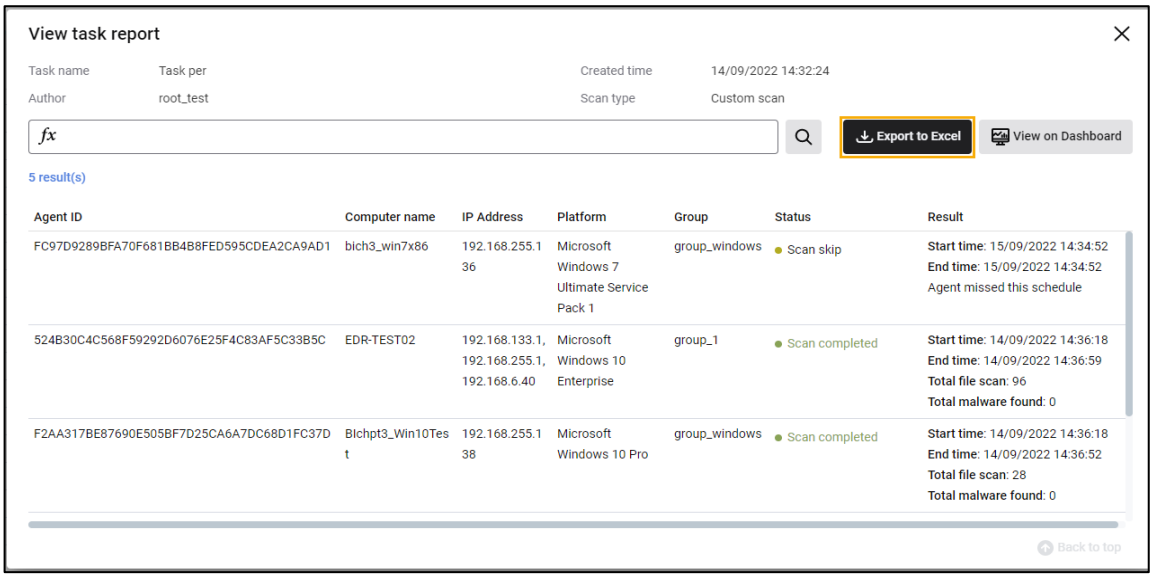


+ Người dùng nhập vào thông tin truy vấn và chọn icon hoặc nhấn nút **Enter** để xác nhận truy vấn;

➔ Hệ thống hiển thị danh sách kết quả báo cáo lập lịch quét sau khi truy vấn.

9 – Export to Excel

- Mục đích: Cho phép người dùng tải xuống báo cáo kết quả lập lịch quét theo định dạng file Excel;

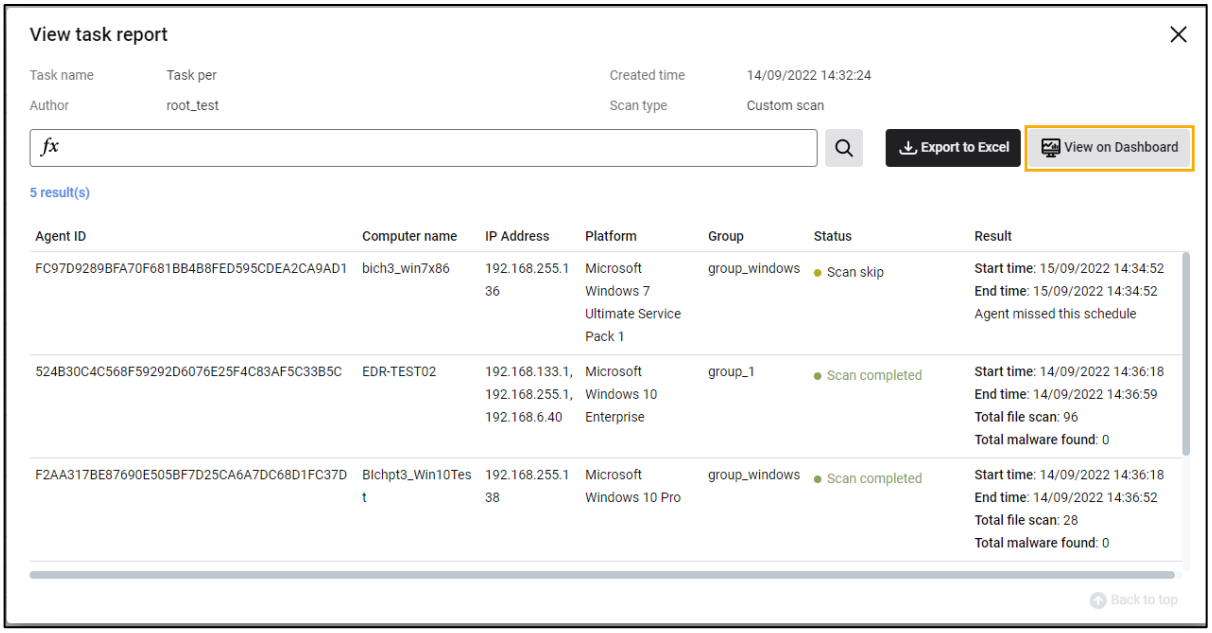


- Các bước thực hiện: Tại màn hình View task report, người dùng chọn nút **Export to Excel**

➔ Hệ thống cho phép tải xuống file kết quả báo cáo lập lịch quét.

10 – View on dashboard

- Mục đích: Cho phép xem báo cáo thống kê Anti-malware của hệ thống



- Các bước thực hiện: Tại màn hình View task report, người dùng chọn nút **View on dashboard**

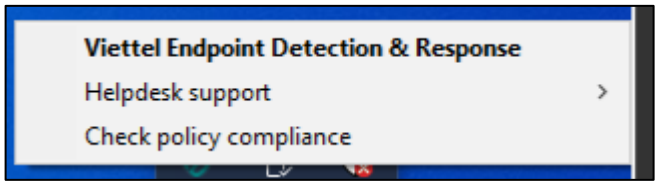
➔ Hệ thống điều hướng sang trang báo cáo thống kê Anti-malware của hệ thống;

B. Giao diện Agent

3.6 Main

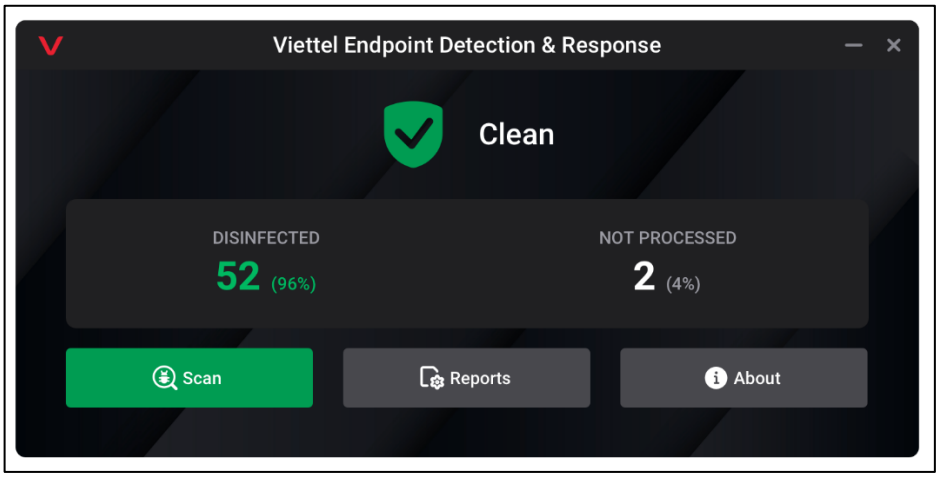
- Chức năng cho phép người dùng xem nhanh trạng thái an toàn thông tin tại máy đang cài agent;

- Trên thanh taskbar tìm icon  click chuột phải và chọn “Viettel Endpoint Detection & Response”:

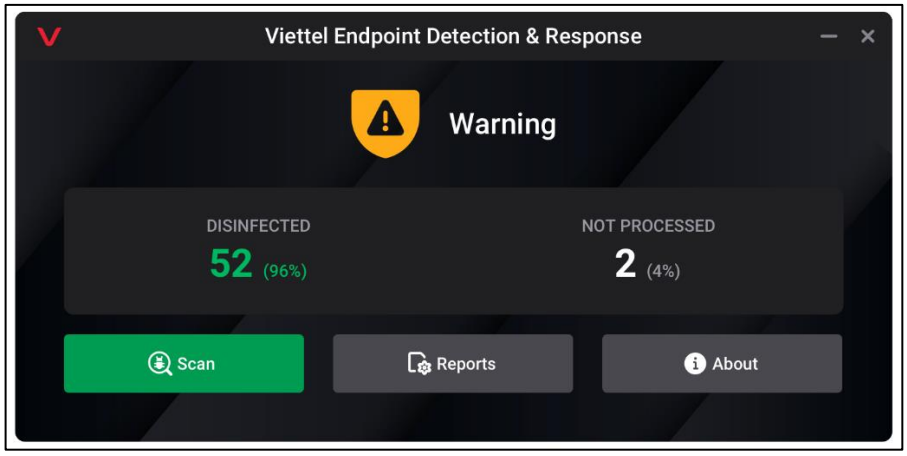


- Hệ thống hiển thị các thông tin:

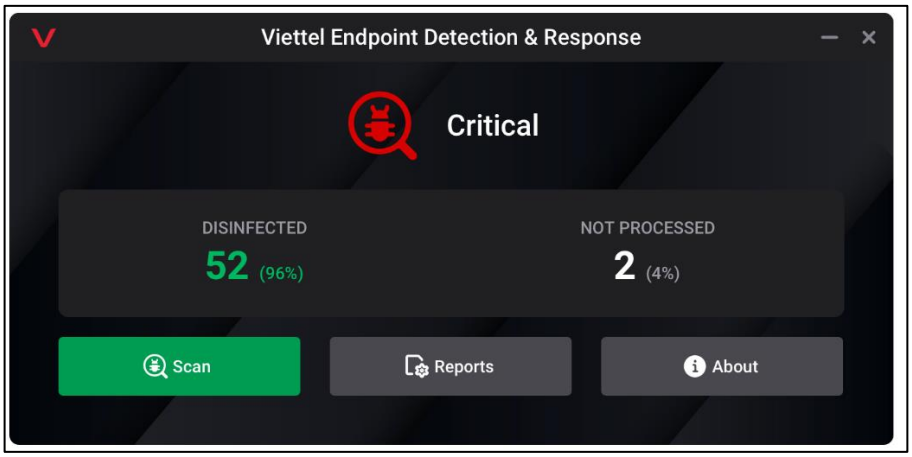
+ Trường hợp máy không có mã độc nào hoặc toàn bộ mã độc đã được xử lý:



+ Trường hợp máy có ít nhất 01 mã độc và không có mã độc nào có độ nguy hiểm cao;



+ Trường hợp máy có ít nhất 01 mã độc có độ nguy hiểm cao;



+ Ngoài ra hệ thống hiển thị con số thống kê liên quan đến tổng số mã độc đã được phát hiện;

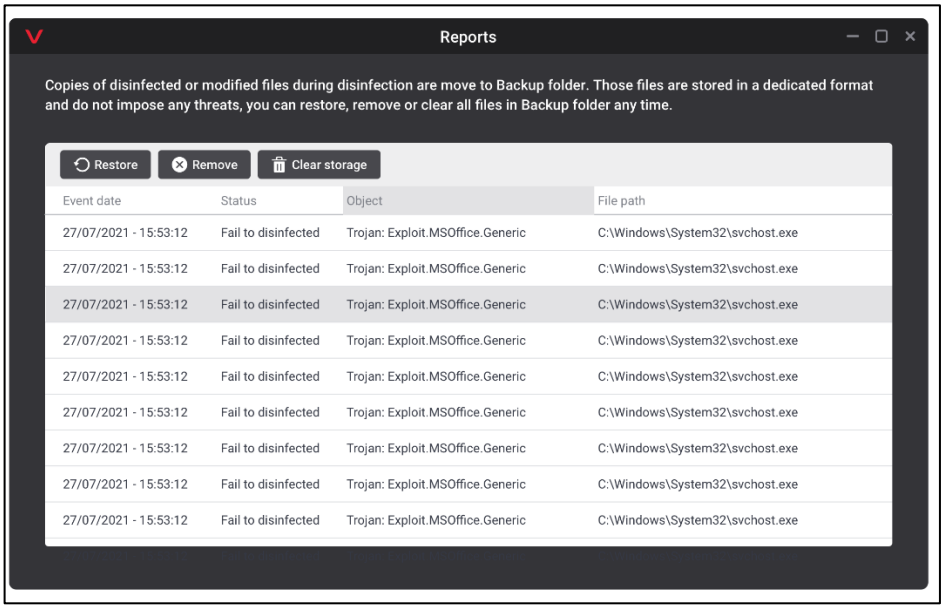
- Disinfected: Tổng số và tỷ lệ mã độc đã phát hiện và được xử lý;
- Not processed: Tổng số và tỷ lệ mã độc đã phát hiện nhưng chưa được xử lý.

3.7 About

- Chức năng cung cấp thông tin về phiên bản Agent cài trên máy người dùng và thông tin hỗ trợ sản phẩm:

3.8 Reports

- Chức năng tổng hợp danh sách các mã độc đã được phát hiện trên hệ thống và tình trạng xử lý tính đến thời điểm hiện tại;



- Các file chứa mã độc trước khi được xử lý đều được lưu trữ bản gốc trong thư mục Backup, để dọn thư mục Backup hoặc phục hồi file, sản phẩm cung cấp các tính năng sau:

Restore: Cho phép lựa chọn 01 file để phục hồi;

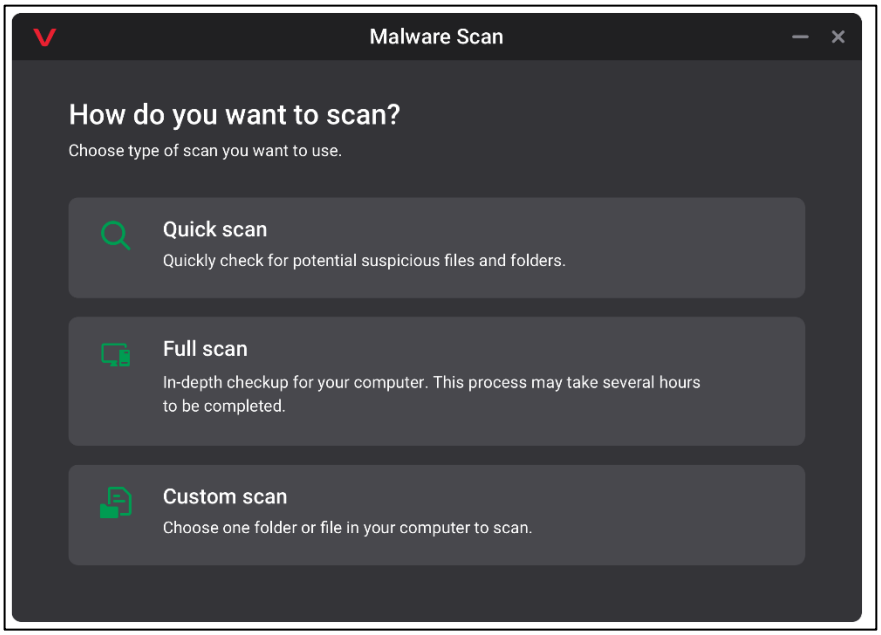
Remove: Cho phép lựa chọn 01 file để xóa khỏi thư mục Backup;

Clear storage: Cho phép dọn nhanh toàn bộ file hiện có trong thư mục Backup;

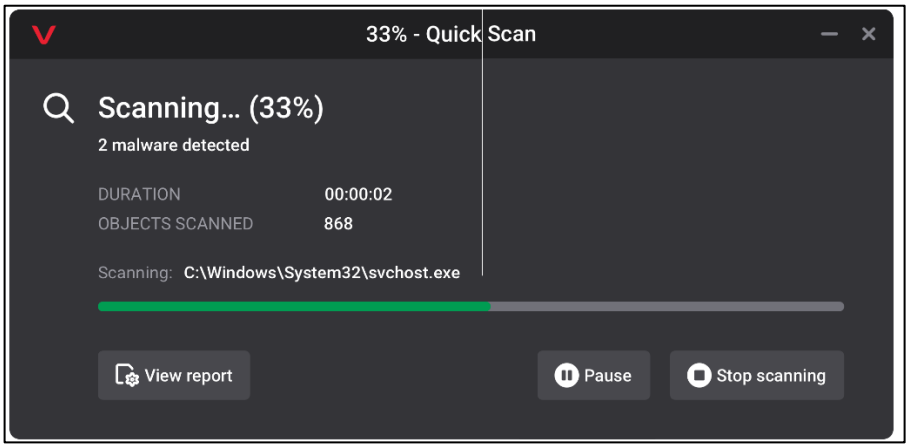
3.9 Scan

- Chức năng cho phép người dùng chủ động sử dụng hệ thống để quét và xử lý mã độc trên máy;
- Các phương thức quét được hỗ trợ bao gồm
  + Lựa chọn trực tiếp từ file explorer, cho phép chọn nhiều tệp tin và thư mục, chuột phải chọn quét (Context scan);
  + Lựa chọn các hình thức quét từ giao diện phía agent;

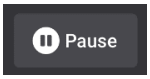
- Quick scan: Quét trên một tập các thư mục được định nghĩa trước, đây là các thư mục thường xuyên phát sinh mã độc, khi chọn quét toàn bộ các tệp tin và thư mục trực thuộc các thư mục đã chọn;
- Full scan: Quét toàn bộ các tệp tin và thư mục có trong máy người dùng;
- Custom scan: Tương tự context scan, khi chọn hình thức này agent hiển thị file explorer cho phép người dùng lựa chọn 01 tệp tin hoặc thư mục để quét



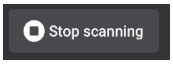
- Sau khi chọn phương thức phù hợp, hệ thống thực hiện quét và xử lý mã độc:



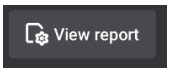
- Hỗ trợ các thao tác trong lúc quét như sau:



: Cho phép tạm dừng quá trình quét;

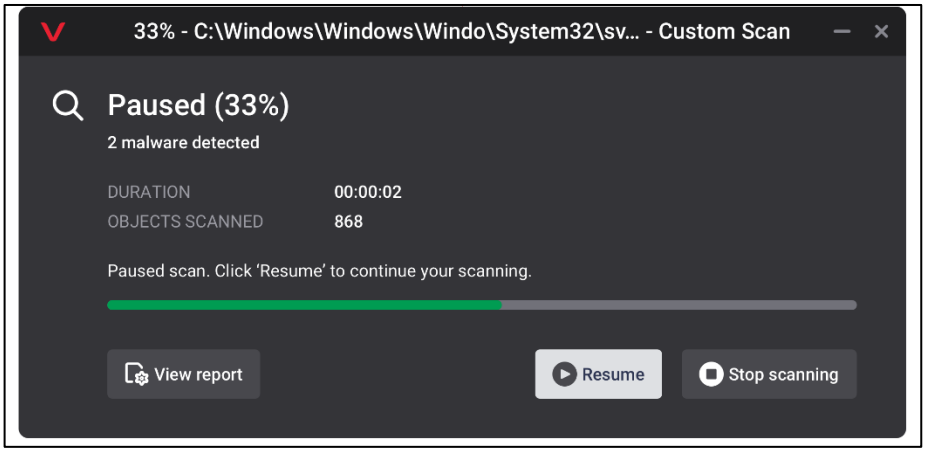


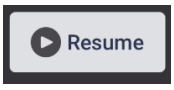
: Cho phép kết thúc quá trình quét;

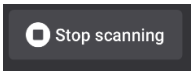


: Trường hợp phát hiện được ít nhất một mã độc, cho phép xem nhanh trạng thái xử lý tại 3.14 Reports;

Màn hình khi người dùng chọn tạm dừng quá trình quét





: Cho phép chọn để tiếp tục quét hoặc 

để hoàn thành quá trình quét.

- Khi hoàn thành quét, hiển thị kết quả như sau: