viettel security

Viettel Endpoint Detection & Protection

(VCS-aJiant phiên bản EDP)

Phiên bản tài liệu: 4.138 – Ngày cập nhật: 22/01/2026

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:* *3.4.8 IRFlow Response - 73* *3.6 Response - 119* *3.7.5 Update management - 174*	
3	10/10/2022	3.3.31	*Bổ sung/ cập nhật hướng dẫn:* *3.11 Anti – Malware – 247*	
4	16/12/2022	3.3.38	*Bổ sung/ cập nhật hướng dẫn:* *3.5.4 Investigation_Deploy tool - 116*	
5	28/12/2022	3.3.43	*Bổ sung/ cập nhật hướng dẫn* *3.6.1 Response_Live resonse - 154*	
6	21/03/2023	4.5.1	*Bổ sung hướng dẫn bật 2FA*	
7	20/04/2023	4.14.0	*Cập nhật Agent Gui mới*	
8	15/05/2023	4.18.0	*Bổ sung hướng dẫn Device Control*	
9	12/09/2023	4.48	*- Bổ sung hướng dẫn Tính năng chống mã hóa mã độc tống tiền (Ransomware)* *- Update giao diện*	
10	27/09/2023	4.52	*Cập nhật chức năng 3.10.2 Endpoint Firewall*	
11	15/7/2024	4.52	*Bổ sung làm rõ các rule BLS*	
13	13/11/2024	4.100	*Hướng dẫn sử dụng config Auto scan trong Policy*	

STT	Ngày cập nhật	Phiên bản	Lý do thay đổi	Ghi chú
14	17/12/2024	4.106	*Hướng dẫn sử dụng tính năng Threat Hunting*	
15	6/10/2025	4.110	*Bổ sung cách tính license sản phẩm VCS-aJiant mục 3.7.1*	
16	10/7/2025	4.115.0	*Hướng dẫn sử dụng command line interface cho tính năng scan mã độc. Mục 3.17*	
17	18/09/2025	4.128.0	*Bổ sung mô tả luật kiểm tra vi phạm BLS Mục 3.5.2.3.1*	
18	04/11/2025	4.130.0	*Bổ sung mục 3.5.2 – Hướng dẫn sử dụng Isolate Devices* *Cập nhật mục 3.3.4 – Không hiển thị tính năng IR flow* *Cập nhật mục 3.4.2 – Không hiển thị tính năng Mark Artifacts*	
19	04/11/2025	4.131.0	*Bổ sung mô tả chức năng cách ly mã độc. Mục 3.14*	
20	24/11/2025	4.132.0	*Cập nhật giao diện màn Agent Management mục 3.6.1*	
21	28/11/2025	4.133.0	*Cập nhật mục 3.6.2 Policy Setting, thêm phần Performance control linux*	
22	24/12/2025	4.135.0	*Thêm mới mục 3.4.5 Event Search V2*	
23	24/12/2025	4.136.0	*Cập nhật mục 3.6.2 Policy Setting, thêm phần Prevention Known Threat*	

STT	Ngày cập nhật	Phiên bản	Lý do thay đổi	Ghi chú
24	24/12/2025	4.137.0	*Thêm mục mục 3.10.1 IOC Management*	
25	22/01/2026	4.138.0	*Cập nhật mục 3.6.2 Policy Setting, thêm phần Fileless*	

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:	

Thuật ngữ	Diễn giải	Ghi chú
	- Process Analysis - Tìm kiếm event logs Dùng tool điều tra: autoruns, listdlls	
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: - Tạo/đóng phiên Process Analysis - Tạo/đóng phiên Live Response	

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

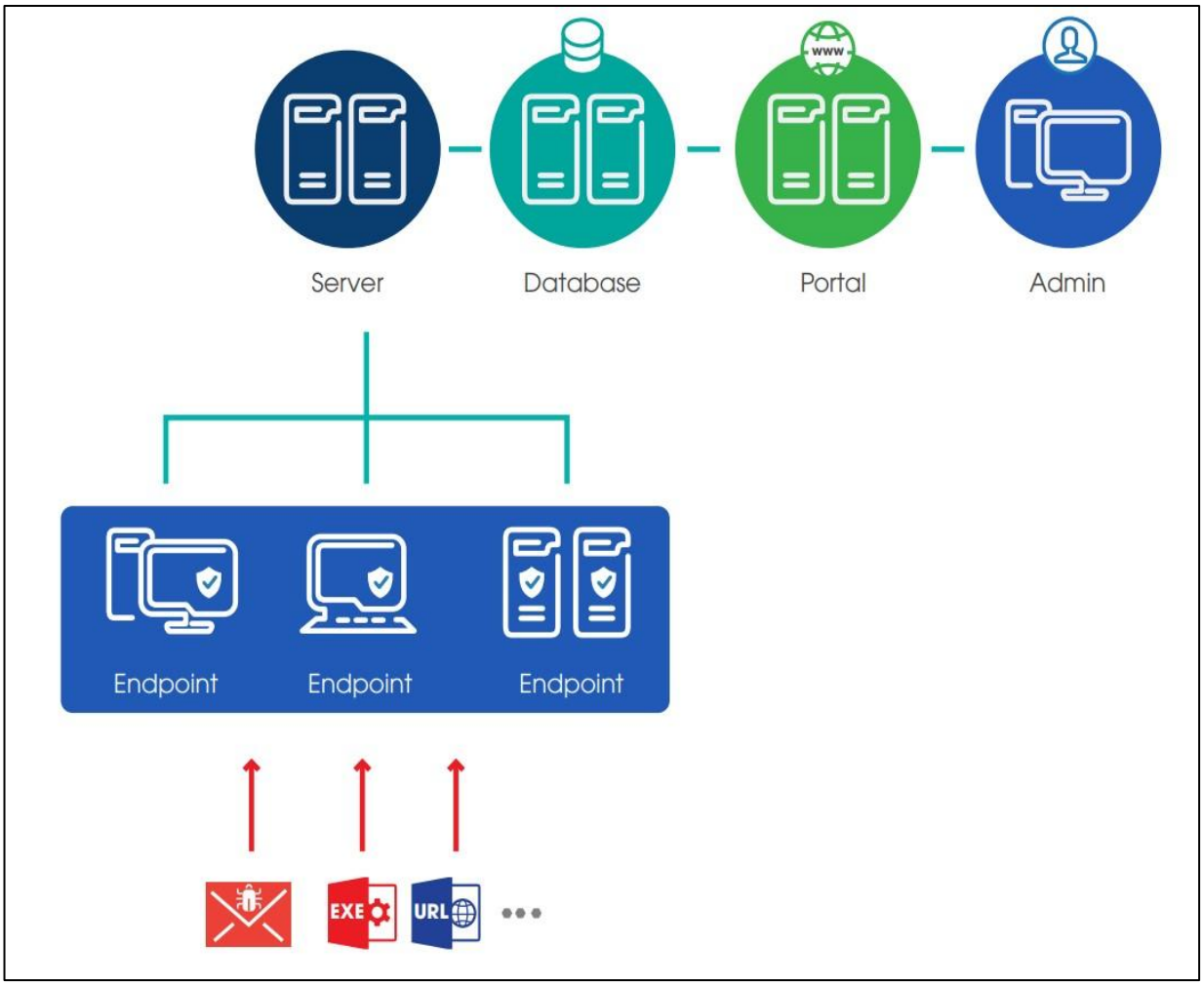
VCS-aJiant sử dụng cộng nghệ Filter Driver (cho phép chạy và theo dõi ở mức Kernelbased) thu thập các thông tin bao gồm File, Process, Registry, Network trên máy tính người dùng và server. Các dấu hiệu về file bao gồm (modified, delete, changed attribute), về registry (delete key/value, set value, rename 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, 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;

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);

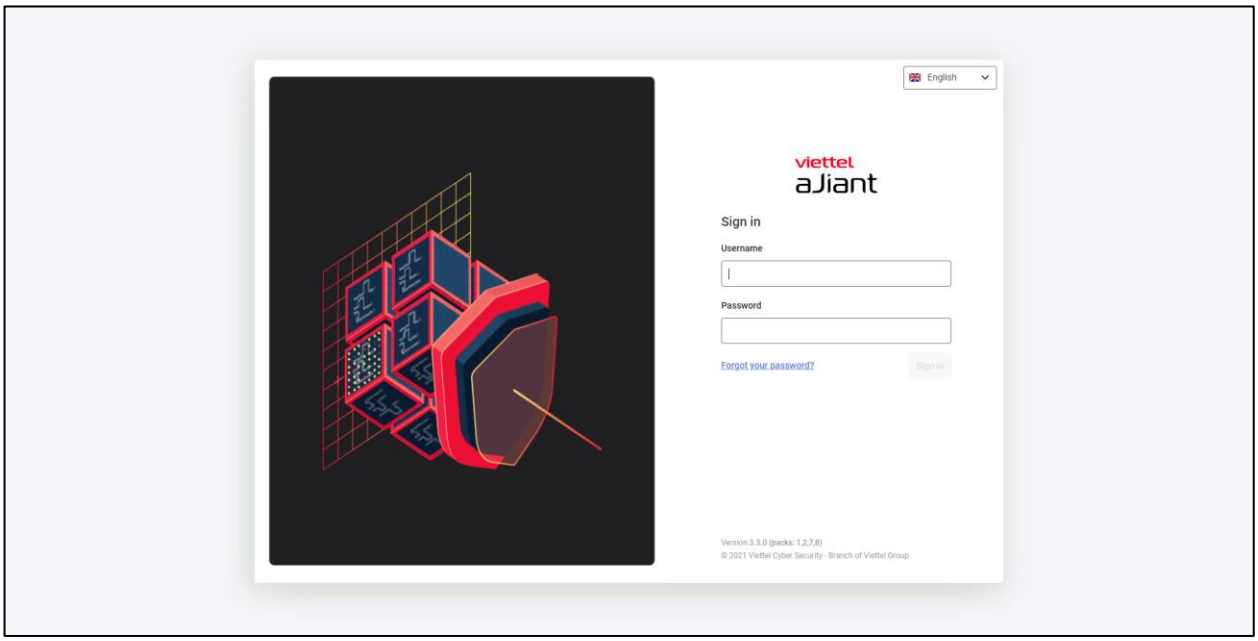
Protect & Prevention: danh sách các tính năng phòng chống và bảo vệ máy trạm (Application control và Endpoint firewall);

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

3.1 Đăng nhập

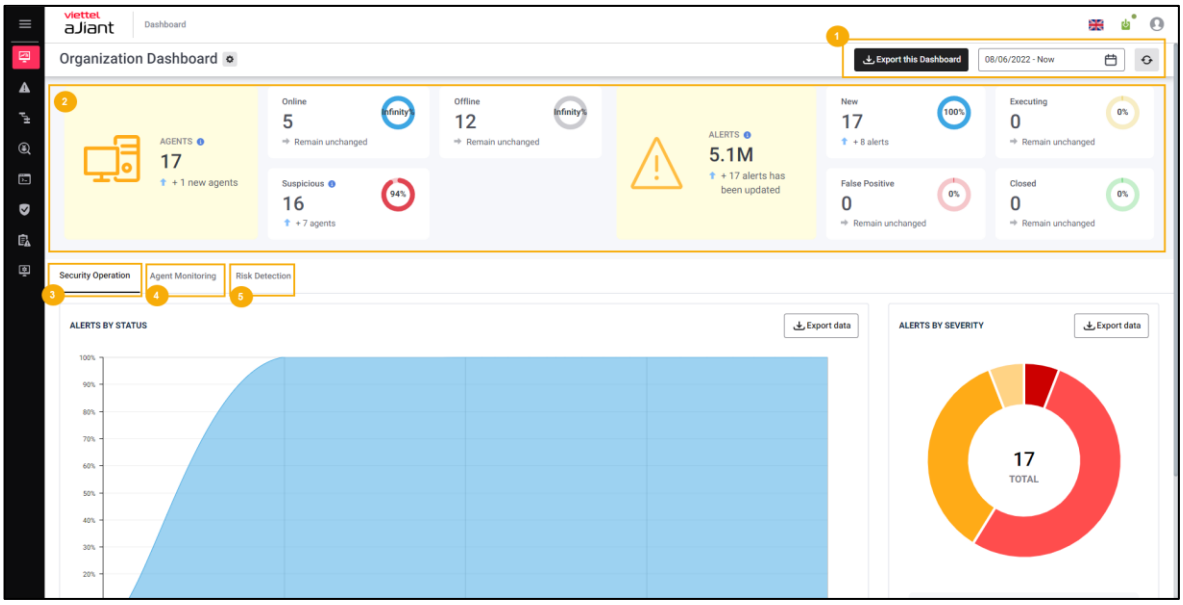
Bước 1: Truy cập vào hệ thống tại địa chỉ được cung cấp;



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:

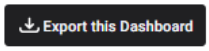
+ User đăng nhập thuộc group root: Hiển thị dữ liệu toàn bộ hệ thống;

+ 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;

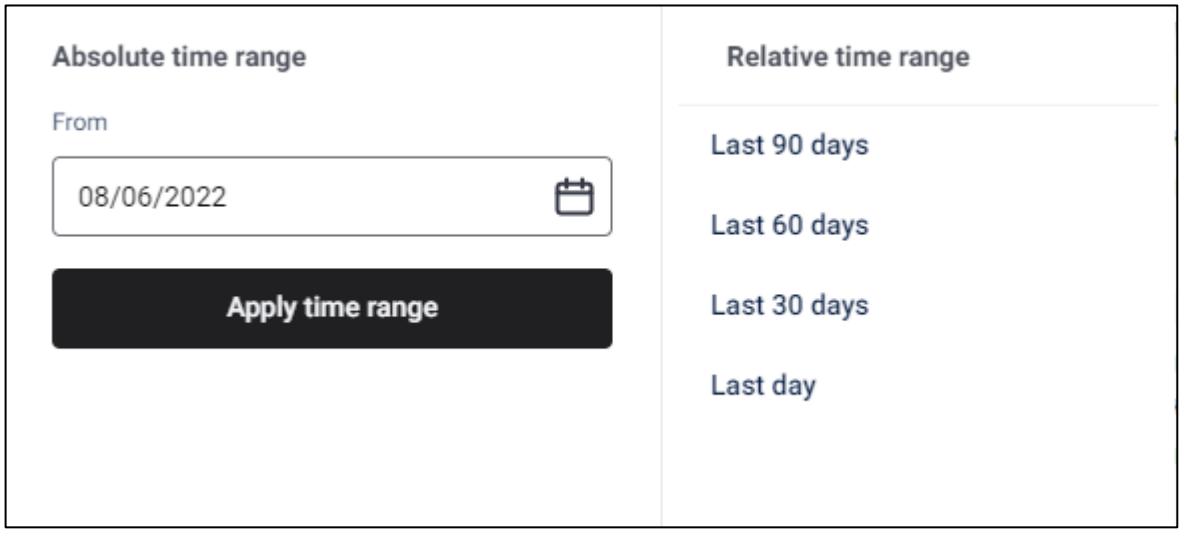
+ Trường hợp lỗi kết nối hoặc không có dữ liệu trên toàn bộ các thành phần của Dashboard, không hỗ trợ trích xuất, thao tác sẽ bị ẩn đi;

+ 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;

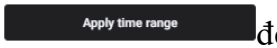
VD: Hiện tại là 03 giờ sáng ngày 07/06/2021, lựa chọn ngày bắt đầu = “06/06/2021”.

→ 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.

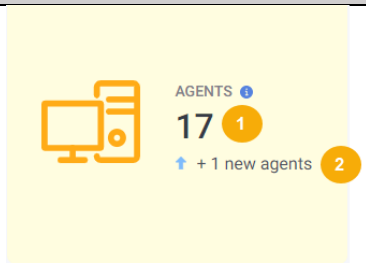
3.2.1.3 Làm mới dữ liệu

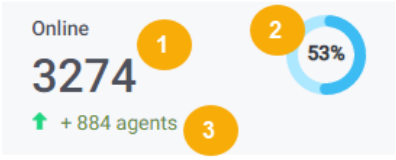
Mục đích: Cho phép làm mới dữ liệu thủ công, chọn  để cập nhật dữ liệu mới nhất tính đến thời điểm hiện tại.

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;

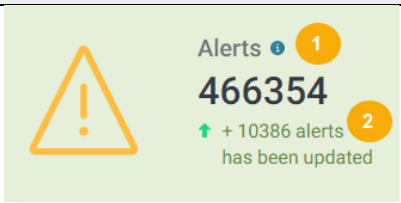
+ Thống kê liên quan đến agents:

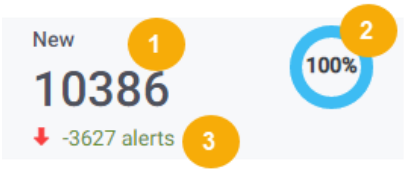
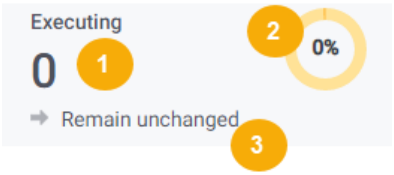
Số thống kê	*Ý nghĩa*
	Bao gồm 02 chỉ số: 1 – Tổng số máy đã cài đặt agent trên hệ thống (không phụ thuộc khoảng thời gian tìm kiếm); 2 – Tổng số máy mới cài đặt agent trong khoảng thời gian tìm kiếm;

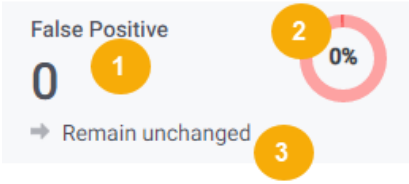
	(+: Máy mới cài đặt, Remain unchanged: Không có máy mới cài đặt trong khoảng thời gian tìm kiếm)
	Bao gồm 03 chỉ số: 1 – Trung bình số máy Online trong khoảng thời gian tìm kiếm (chỉ tính thời gian làm việc trong giờ hành chính 08:00 – 18:00); 2 – Tỷ lệ máy Online trung bình so với toàn hệ thống; 3 – 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:

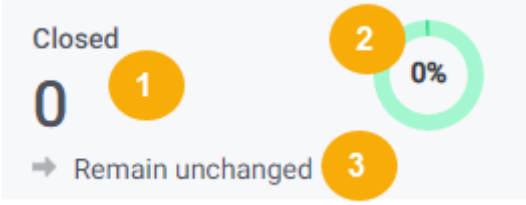
	1 – Tổng số máy đã cài đặt agent trên hệ thống (không phụ thuộc khoảng thời gian tìm kiếm) có phát sinh Alert chưa được xử lý; 2 – Tỷ lệ máy có phát sinh Alert so với số lượng máy trên toàn hệ thống (không phụ thuộc thời gian tìm kiếm); 3 – Tổng số máy có phát sinh Alert trong khoảng thời gian tìm kiếm. (+: 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)

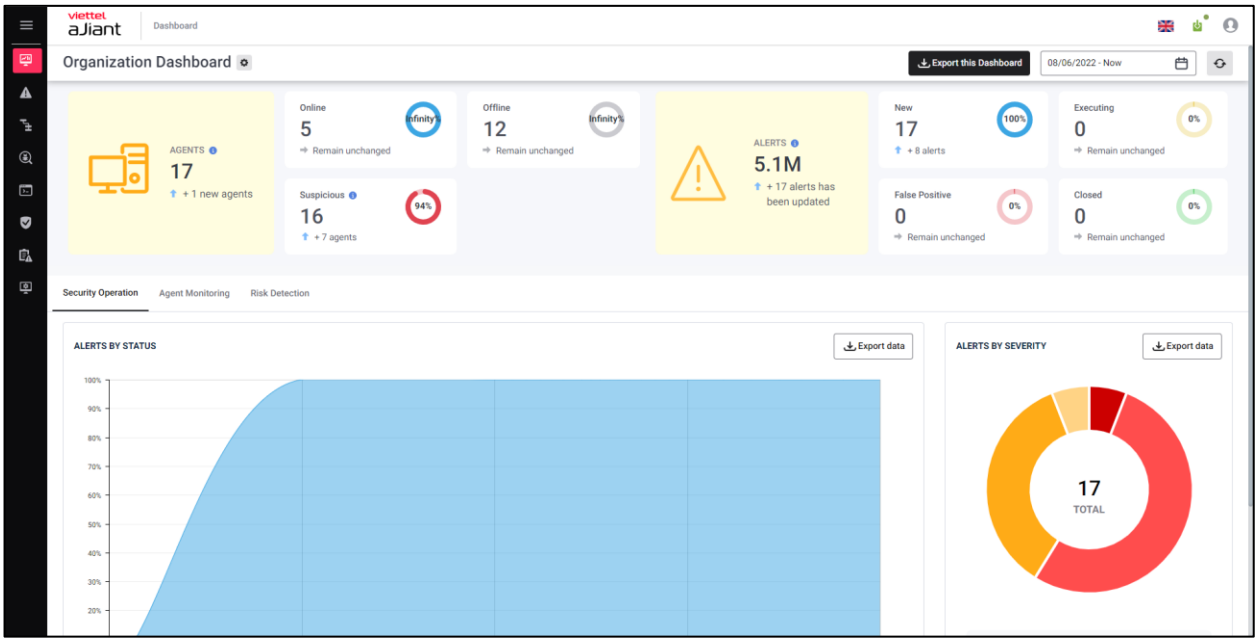
	Bao gồm 03 chỉ số: 1 – Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = FALSE POSITIVE; 2 – Tỷ lệ Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = FALSE POSITIVE so với toàn bộ Alert mới phát sinh hoặc được 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;

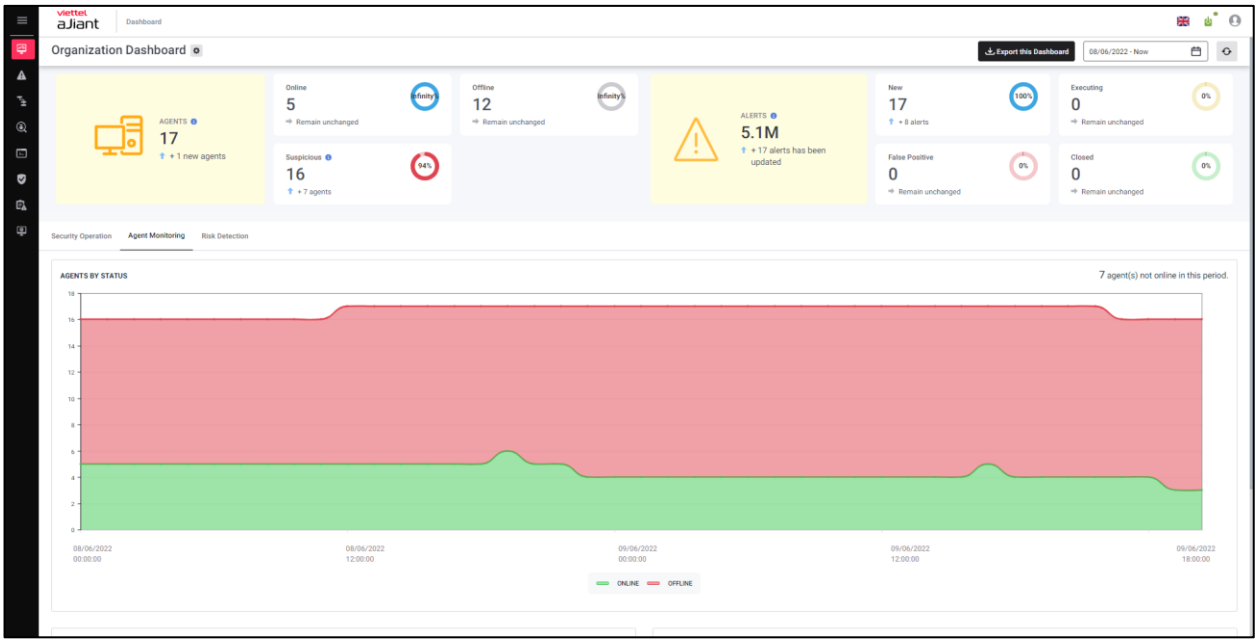


Biểu đồ/thống kê	*Ý nghĩa*
Alert by status	Biểu đồ miền - Theo dõi tình hình ghi nhận các Alert mới ghi nhận hoặc có cập nhật trong khoảng thời gian tìm kiếm, bao gồm: Trục x: thời gian; Trục y: Tỷ lệ Alert phân chia theo 04 nhóm trạng thái = (New, Executing, Closed, False Positive); Cho phép chọn Export 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;



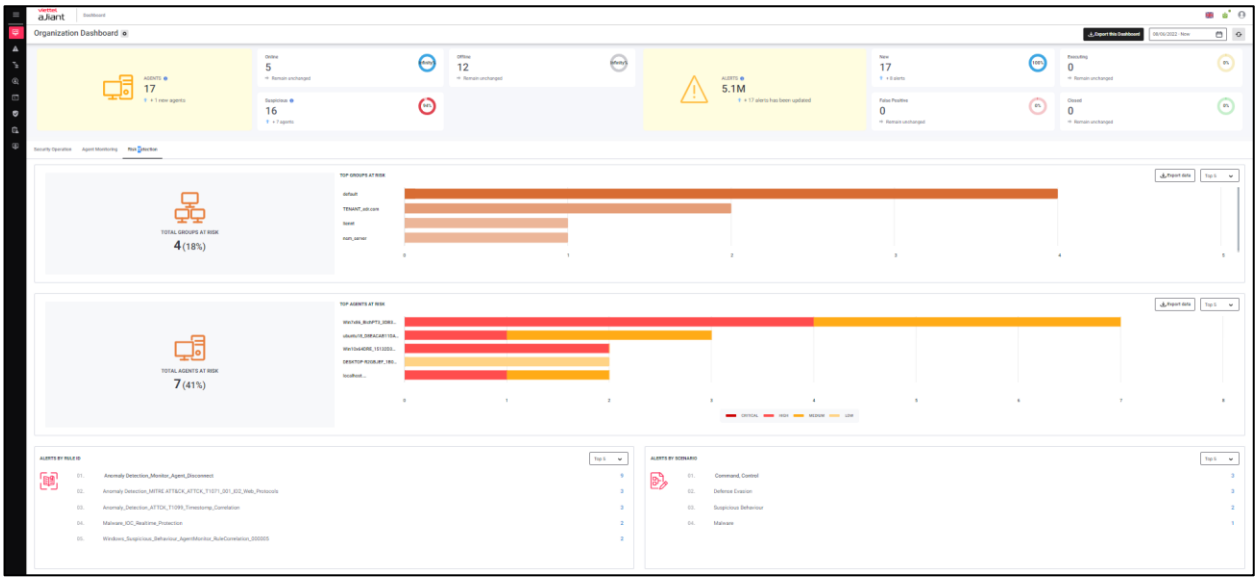
Biểu đồ/thống kê	*Ý nghĩa*
Agent by status	Biểu đồ miền- Theo dõi tình hình ghi nhận máy theo trạng thái (Online/Offline) trong chu kỳ báo cáo tính đến thời điểm hiện tại, bao gồm: Trục y: Tỷ lệ máy phân chia theo 02 nhóm status (Online, Offline); Trục x: thời gian thống kê; Hiển thị số lượng máy không 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;

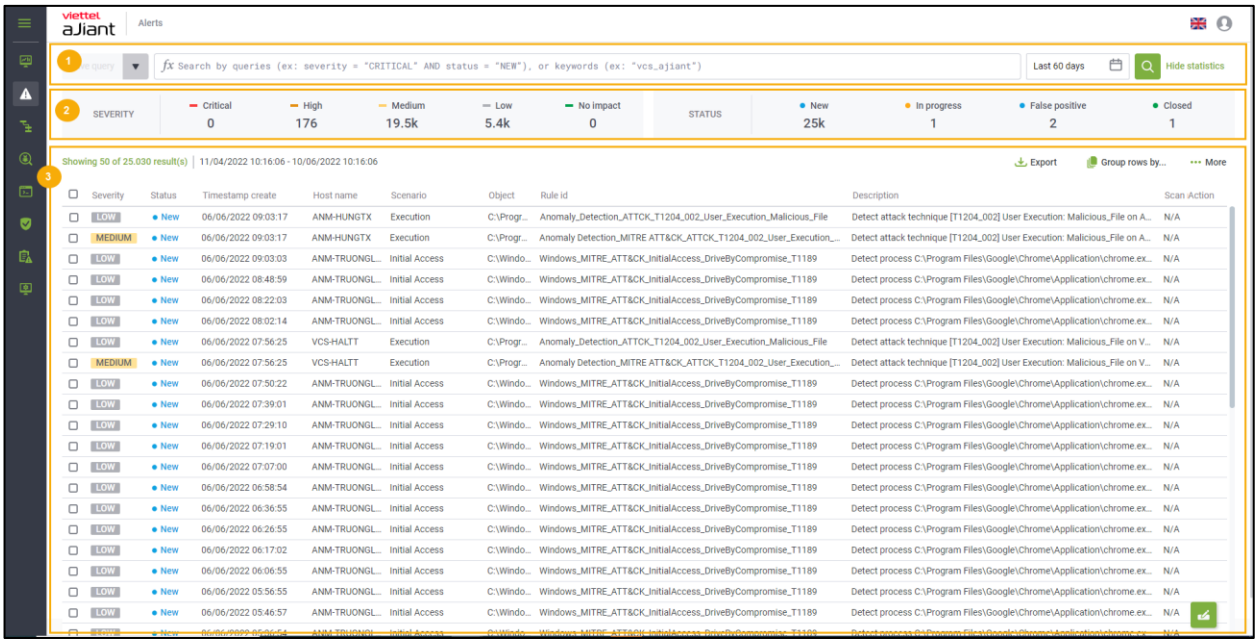


Biểu đồ/thống kê	*Ý nghĩa*
Total groups at risk	Tổng số nhóm có chứa máy tính phát sinh Alert mới ghi nhận hoặc có cập nhật (không kể Alert false positive và closed, không kể nhóm đã bị xóa) trong thời gian tìm kiếm; Tỷ lệ nhóm khả nghi so với toàn bộ nhóm trên hệ thống (không kể nhóm đã bị xóa).
Top 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 Quản lý Alert

Các tính năng chính gồm có:



1 – Tìm kiếm dữ liệu theo truy vấn và thời gian:

+ Tìm kiếm dữ liệu theo câu lệnh truy vấn và sử dụng các câu lệnh truy vấn đã lưu;

+ Tìm kiếm dữ liệu theo thời gian.

2 – Tìm kiếm nhanh;

3 – Danh sách Alert và các thao tác với Alert:

+ Xem danh sách Alert;

+ Gom nhóm Alert;

+ Xem tóm tắt Alert;

+ Xem chi tiết 01 Alert;

+ Xem biểu đồ điều tra (Investigation Graph);

+ Đánh dấu không nguy hiểm (Set False Positive) cho 01/nhiều Alert;

Phân quyền dữ liệu tại tính năng như sau:

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

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

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

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

3.3.1 Tìm kiếm Alert

Mục đích: Cho phép tạo câu lệnh truy vấn, sử dụng câu lệnh truy vấn đã lưu hoặc tìm kiếm nhanh để tìm kiếm Alert theo thời gian phát sinh Alert.

3.3.1.1 Tìm kiếm theo thời gian

Mặc định khi vừa truy cập vào hệ thống, tìm kiếm Alert theo 7 ngày gần đây;
Mục đích: Cho phép thay đổi giá trị thời gian bằng cách chọn thời gian tuyệt đối hoặc thời gian tương đối:

+ Thời gian tuyệt đối: Là giá trị thời gian bắt đầu – thời gian kết thúc cụ thể, cho phép nhập hoặc chọn từ lịch, hỗ trợ định dạng ngày/tháng/năm giờ:phút:giây;

+ Thời gian tương đối: Là khoảng thời gian tương đối giữa thời gian bắt đầu và thời gian 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 03:00 giờ của ngày đó.

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

3.3.1.2 Tìm kiếm nhanh

Mục đích: Hỗ trợ tìm kiếm Alert nhanh theo các trường:

+ Time: thời gian phát sinh Alert;

+ Status: trạng thái của Alert;

+ Severity: mức độ nguy hại của Alert;

+ Scenario: kịch bản sinh ra Alert;

+ Assigned to: người được phân công xử lý Alert;

3.3.1.3 Tìm kiếm theo câu query

1 – Sử dụng câu query đã lưu trước đó để tìm kiếm;

2 – Nhập câu query để tìm kiếm;

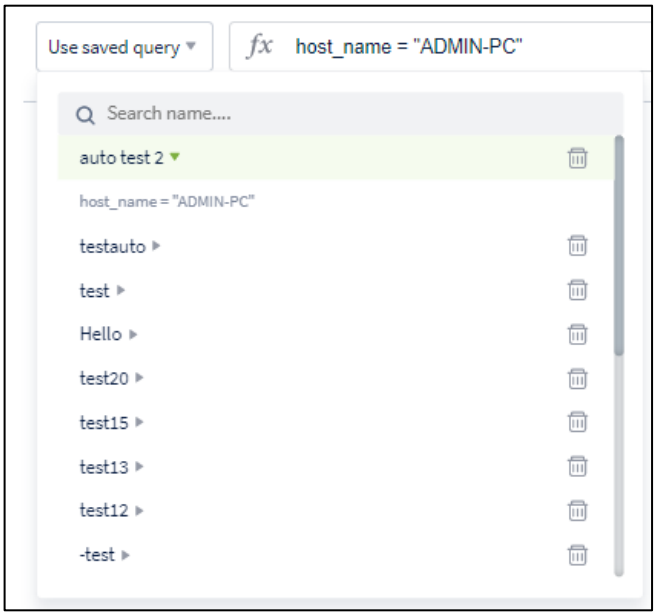
(*) Sử dụng câu query đã lưu trước đó để tìm kiếm

Bước 1: Chọn query đã lưu trước đó tại combobox Use saved query ;

Bước 2: Xem lại nội dung câu query trước khi chọn bằng cách chọn ▼;

Bước 3: Trường hợp muốn xóa câu query cũ, di chuột qua bản ghi muốn xóa và chọn 🗑;

Bước 4: Click vào bản ghi muốn sử dụng để truy vấn, nội dung query cũ được hiển thị tại ô nhập query;



➔ Trường hợp muốn thêm mới/chỉnh sửa nội dung câu query, có thể cập nhật ngay tại ô nhập query và chọn Save query để lưu lại.

Lưu ý: nút Save query chỉ hiển thị khi câu lệnh query đúng cấu trúc.

(*) Nhập câu query để tìm kiếm:

Bước 1: Nhập vào textbox Search câu query với format như sau:

<tên_trường> <toán tử> “<value>” AND/OR <tên_trường> <toán tử> “<value>”…..

Trong đó:

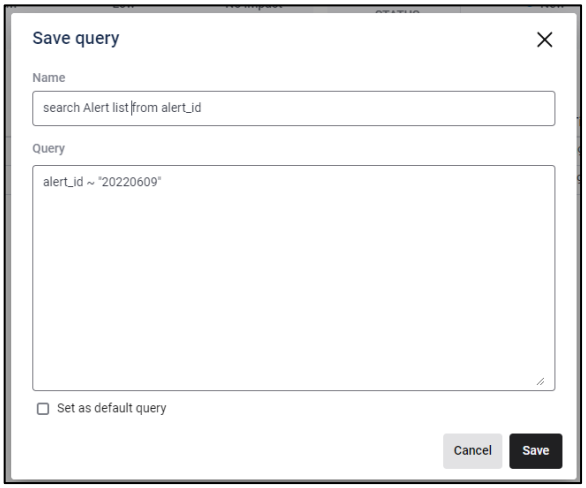
+ <tên_ trường> là các giá trị sau:
  - severity: độ nghiêm trọng của Alert
  - Alert_id: mã Alert
  - status: trạng thái của Alert
  - group: nhóm của sự kiện sinh Alert
  - hostname: Tên của máy trạm
  - scenario: kịch bản sinh ra Alert dựa theo MITRE ATT&CK
  - assignee: người được phân công xử lý Alert
  - signature_id: mã sự kiện phát sinh Alert
  - rule_id: mã bộ luật phát sinh Alert
  - description: mô tả thông tin ngữ cảnh phát sinh Alert
+ <toán tử> là các giá trị:
  - = : tìm chính xác giá trị là value
  - != : tìm giá trị khác với value
  - ~: tìm giá trị like với value
  - AND/OR: toán tử kết hợp để kết hợp 2 câu query.

Bước 2: Click nút “Search”.

+ Trường hợp không có kết quả phù hợp, hệ thống sẽ hiển thị thông báo: No data;

+ Trường hợp có kết quả phù hợp, hệ thống hiển thị mặc định 50 bản ghi theo thứ tự giảm dần theo thời gian. Để xem nhiều bản ghi hơn thực hiện scroll dữ liệu xuống cuối trang, hệ thống sẽ load 50 bản ghi tiếp theo;

+ Trường hợp câu query đúng cấu trúc và muốn lưu lại để sử dụng cho các lần tiếp theo, chọn Save query và nhập tên gợi nhớ cho query:



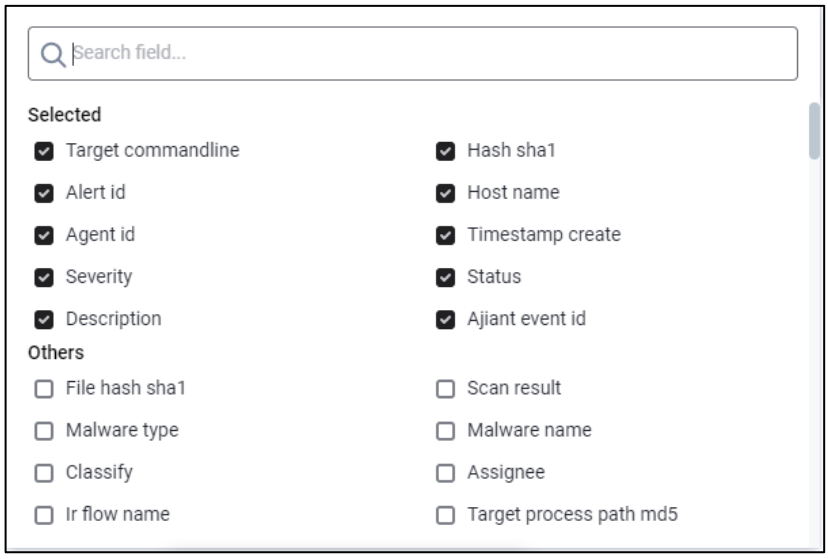
Lưu ý: nút Save query chỉ hiển thị khi câu lệnh query đúng cấu trúc.

3.3.2 Danh sách Alert

Mục đích: Hiển thị danh sách Alert trong hệ thống;

Cho phép xem danh sách các Alert đáp ứng điều kiện tìm kiếm

Bước 1: Chọn View column để lựa chọn các trường muốn hiển thị trên danh sách Alert:



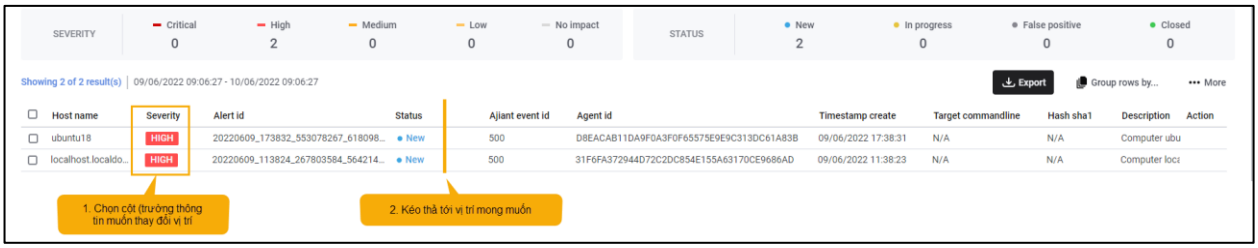
Tại đây có thể tìm kiếm trường thông tin theo tên trường, hỗ trợ chọn/bỏ chọn tất cả các trường;

Bước 2: Trên danh sách hỗ trợ các thao tác như sau:

+ Sắp xếp theo dữ liệu tại từng cột:

VD: Để sắp xếp dữ liệu theo trường thời gian tạo, click lần thứ nhất tại tên trường để sắp xếp theo thời gian tạo tăng dần Timestamp create, click lần thứ hai để sắp xếp theo thời gian tạo giảm dần Timestamp create, click lần thứ ba để bỏ sắp xếp, quay lại trạng thái ban đầu Timestamp create;

+ Kéo thả trường thông tin đến vị trí mong muốn:

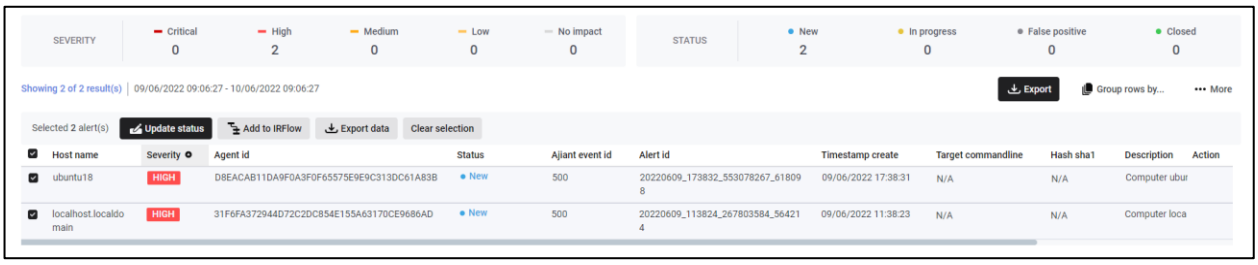


+ Click 01 lần để xem thông tin chi tiết hoặc chọn ... và chọn "View detail", chi tiết xem trong [3.3.4 Xem chi tiết Alert]

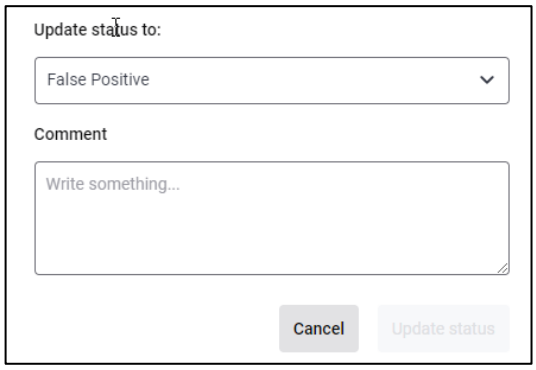
+ Chọn ... và chọn "Update status" để cập nhật trạng thái cho Alert (Update status to "False Positive" hoặc Update status to "Close", xem trường hợp đánh dấu 01 Alert trong

+ Chọn để xem lý do đánh dấu không nguy hiểm tại các Alert đang ở trạng thái "FALSE POSITIVE"..

Bước 1: Sau khi đã thao tác trên các bản ghi xong, cho phép chọn 01 hoặc nhiều bản ghi bằng cách click chọn tại đầu mỗi Alert để tiếp tục thao tác, hỗ trợ các thao tác sau:



Bước 2: Chọn Update status để cập nhật trạng thái của Alert:



- Chọn Update Status to "False Positive" để đánh dấu không nguy hiểm cho Alert;
- Chọn Update Status to "Close" để đóng Alert;

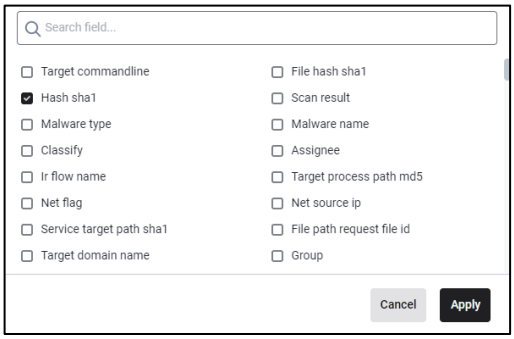
Lưu ý: Thao tác này chỉ áp dụng khi toàn bộ Alert được chọn đều ở trạng thái = "NEW", nếu có ít nhất một Alert đang ở trạng thái khác "NEW", thao tác sẽ bị ẩn đi . Chi tiết xem trong trường hợp đánh dấu không nguy hiểm 01 Alert trong 3.3.5 Đánh dấu không nguy hiểm cho 01/nhiều Alert hoặc nhóm Alert

+ Chọn Export data để trích xuất các Alert đang được chọn.

3.3.3 Gom nhóm Alert

Mục đích: Cho phép gom nhóm các Alert theo 01 hoặc nhiều tiêu chí: hostname, scenario, group, ruleid;

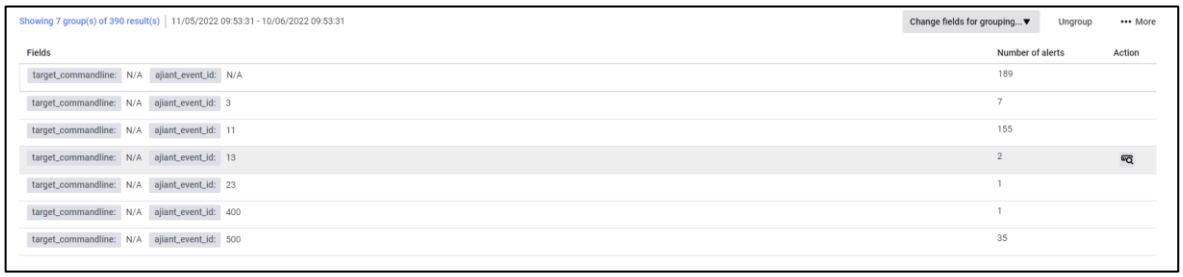
Bước 1: Sau khi tìm kiếm có thể gom nhóm Alert lại, chọn Group rows by... để lựa chọn các tiêu chí muốn sử dụng làm tiêu chí gom nhóm Alert;



Hỗ trợ tìm kiếm theo tên tiêu chí và lựa chọn 01 hoặc nhiều tiêu chí đê gom nhóm.

Bước 2: Chọn Apply để áp dụng.

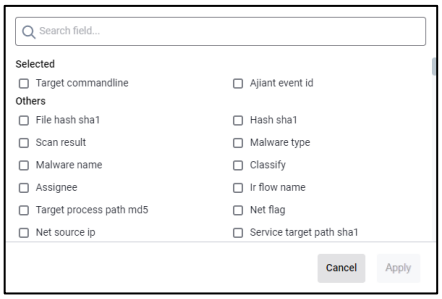
Những Alert có cùng các tiêu chí đã chọn và có cùng trạng thái sẽ được gom lại 1 dòng trong danh sách kết quả.



Trong đó:

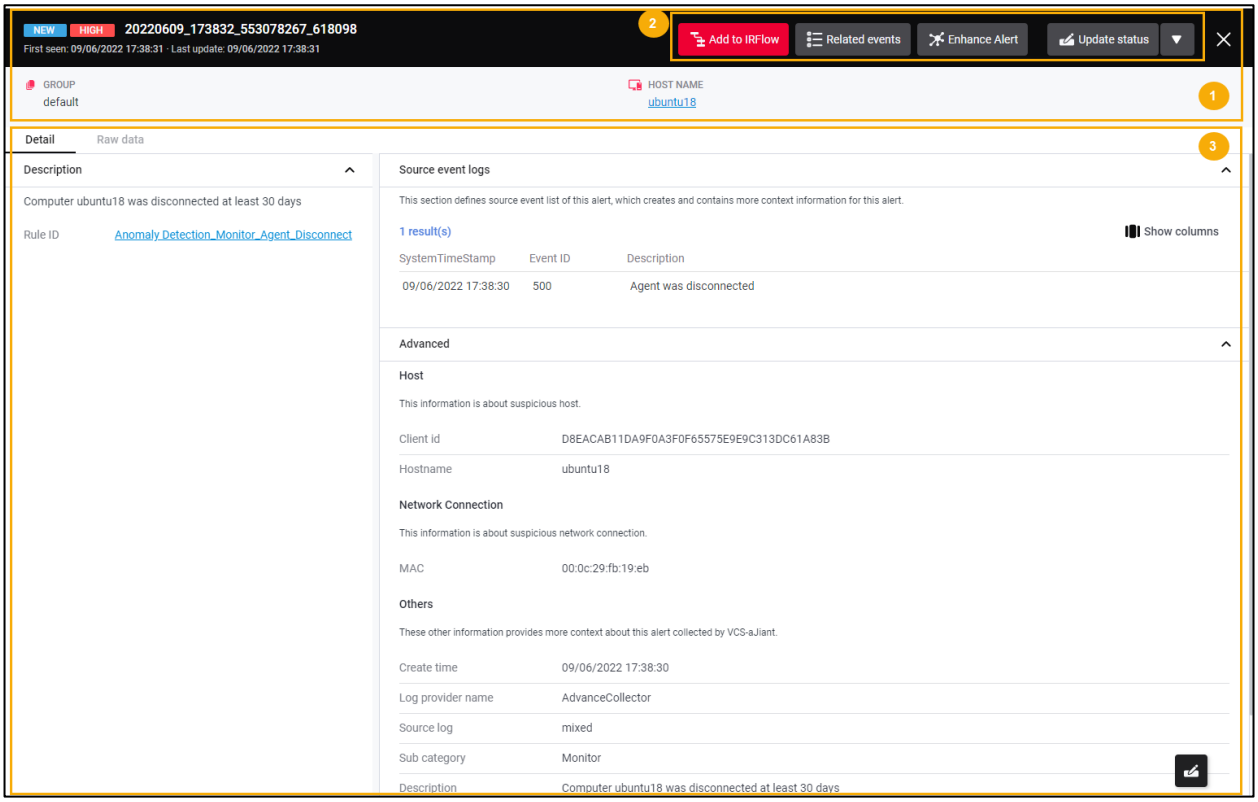
+ Các trường được sử dụng làm tiêu chí gom nhóm sẽ được bôi đậm;
+ Hiển thị số lượng các Alert được gom nhóm tại tiêu chí đã chọn.

Bước 3: Để bỏ gom nhóm, thực hiện tương tự nhưng không chọn tiêu chí nào và chọn "Apply";



3.3.4 Xem chi tiết Alert

Mục đích: Cho phép xem thông tin chi tiết Alert, hỗ trợ tự động làm đa dạng thông tin bằng cách tự động thu thập thông tin các sự kiện liên quan đến Alert vừa phát sinh, cung cấp biểu đồ trực quan để xem nhanh mối quan hệ giữa các đối tượng có trong Alert;



1 – Nhóm thông tin chung của Alert, trong đó:

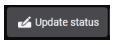
2 –

+ Status: Hiển thị trạng thái của Alert (New, In Progress, False Positive, Closed);

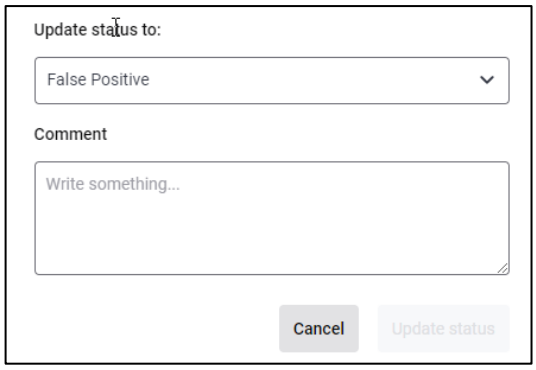
+ Severity: Phân loại Alert theo mức độ nguy hại (Critical, High, Medium, Low);

+ Alert_id: Hiển thị thông tin id của Alert;
+ First seen: Thời gian Alert được tạo;
+ Last seen: Thời gian gần nhất Alert được cập nhật;

3 – Nhóm các thao tác với Alert

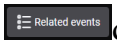
+ Chọn 

để cập nhật trạng thái của Alert:



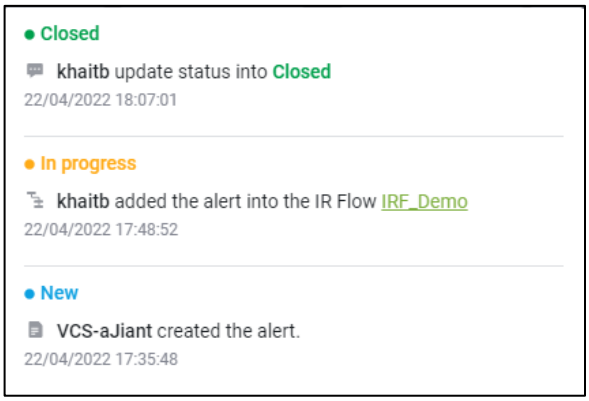
- Chọn Update Status to "False Positive" để đánh dấu không nguy hiểm cho Alert;
- Chọn Update Status to "Close" để đóng Alert;

Lưu ý: Thao tác này chỉ áp dụng khi Alert được chọn ở trạng thái = "NEW", thao tác sẽ bị ẩn đi. Chi tiết xem trong trường hợp đánh dấu không nguy hiểm 01 Alert trong 3.3.5 Đánh dấu không nguy hiểm cho 01/nhiều Alert hoặc nhóm Alert;

+ Chọn 

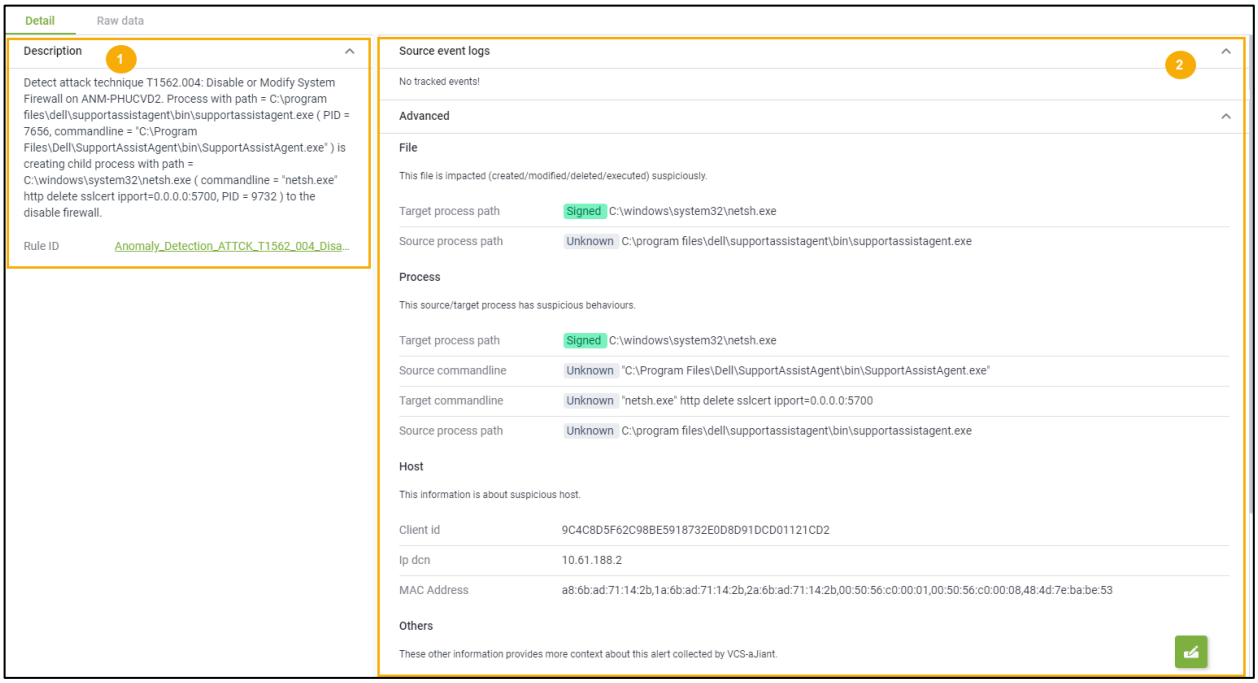
để chuyển đến tính năng Event Search với thời gian mặc định là 04 tiếng trước và sau thời gian phát sinh Alert;

+ Chọn  để xem logs hoạt động liên quan đến Alert;



4 – Tab các thông tin liên quan đến Alert:

+ Tab Detail: Cho phép hiển thị toàn bộ thông tin chi tiết liên quan tới Alert;

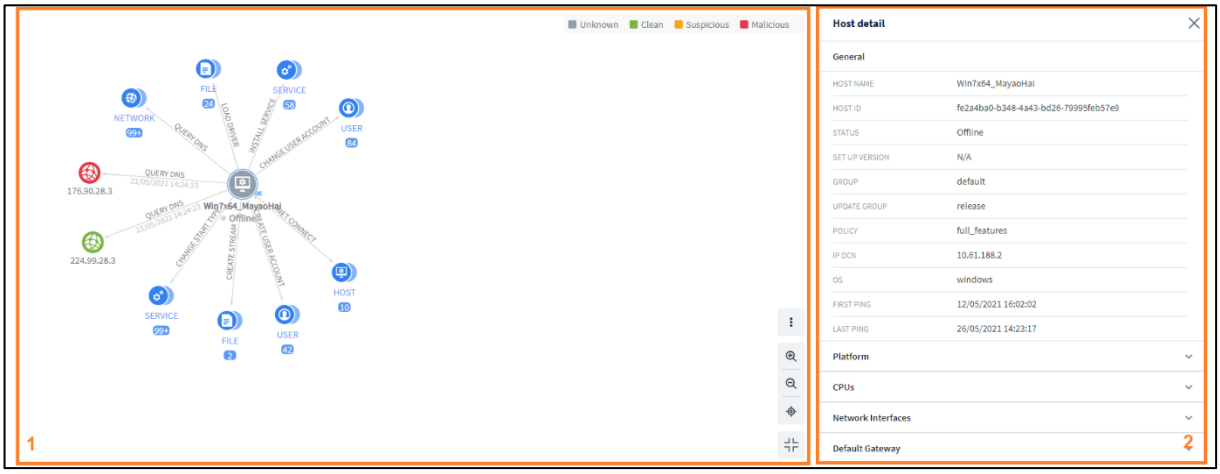


- Khung thông tin (1) Description: Cho phép hiển thị thông tin mô tả chi tiết Alert và RuleID;

- Khung thông tin (2):
  - Source event logs: Ghi lại Source event logs liên quan đến Alert (nếu có);
  - Advance: Thông tin nâng cao liên quan đến Alert bao gồm: File, Process, Host, Others, ...

3.3.5 Biểu đồ điều tra (Enhance Alert)

Mục đích: Cho phép hiển thị mối quan hệ của các đối tượng trong Alert, xem chi tiết các đối tượng và hỗ trợ điều tra loang dựa trên tập các sự kiện thu thập được trong hệ thống.

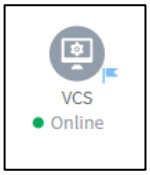


1 – Khu vực hiển thị biểu đồ và các thao tác trên biểu đồ

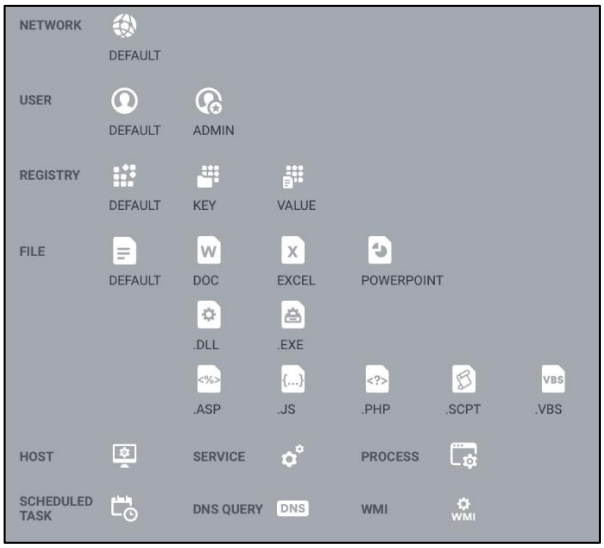
2 – Khu vực hiển thị thông tin chi tiết các đối đượng trên biểu đồ

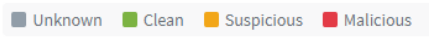
3.3.5.1 **Khu vực hiển thị biểu đồ và các thao tác trên biểu đồ**

Cho phép hiển thị trực quan các đối tượng trong Alert phục vụ xem thông tin và điều tra; Mặc định khi vừa truy cập, biểu đồ hiển thị thông tin liên quan đến máy gốc phát sinh Alert, cụ thể như sau:



Trong biểu đồ luôn có 01 máy được cắm cờ để đánh dấu máy gốc phát sinh Alert, mặc định tại mỗi máy luôn đi kèm các đối tượng có quan hệ trực tiếp máy gốc trong vòng 01 ngày kể từ thời điểm phát sinh Alert, danh sách các đối tượng bao gồm:



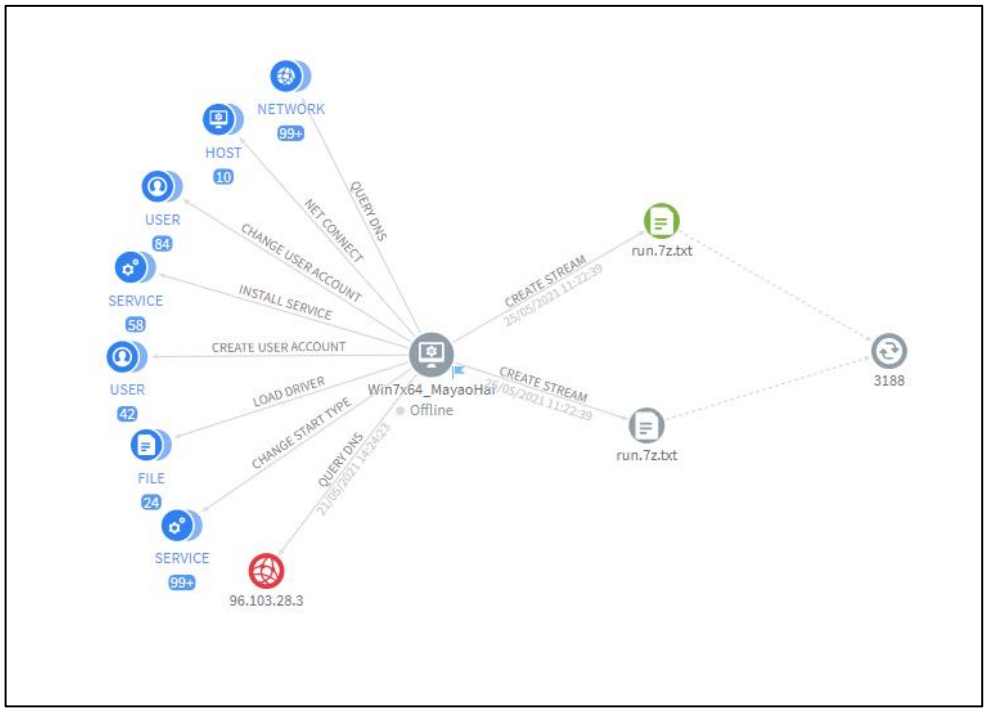
Mỗi đối tượng bao gồm các trạng thái như sau: 

Giữa các đối tượng, hiển thị mối quan hệ bao gồm:

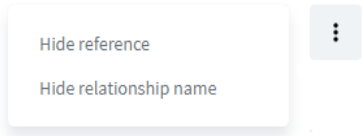
+ Relationship: Mối quan hệ định nghĩa theo các sự kiện phát sinh trong vòng 01 ngày từ thời điểm phát sinh Alert (trong đó tên mối quan hệ nằm phía trên mũi tên nối liên 02 đối tượng) 

+ Reference: Mối quan hệ tham chiếu, là các đối tượng khác ghi nhận được trong sự kiện chính phát sinh ra đối tượng (được thể hiện bởi nét đứt và không có tên quan hệ cụ thể) 

Ví dụ:

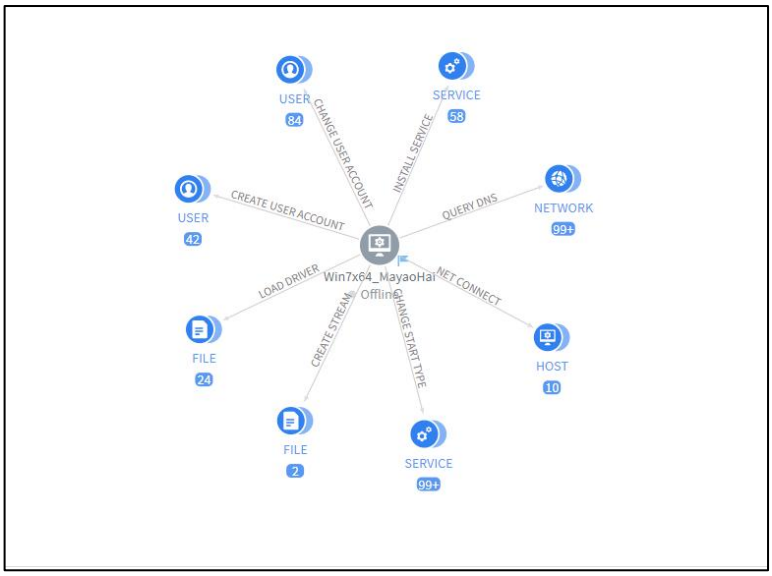


Các thao tác hỗ trợ hiển thị biểu đồ bao gồm:

Thao tác hỗ trợ hiển thị	***Ý nghĩa***
	Cho phép ẩn/hiện các thông tin trên biểu đồ: + Reference: Khi chọn, cho phép ẩn/hiện thông tin tham chiếu bao gồm mũi tên nét đứt và đối tượng tham chiếu tại tất cả các đối tượng hiện có trên biểu đồ; + Relationship name: Khi chọn, cho phép ẩn/hiện thông tin tên mối quan hệ phía trên tất cả các mũi tên nét liền hiện có trên biểu đồ
	Cho phép zoom in/zoom out biểu đồ tương ứng tại vị trí đang trỏ chuột Ngoài ra có thể lăn chuột tại vị trí muốn zoom in/out để thao tác nhanh

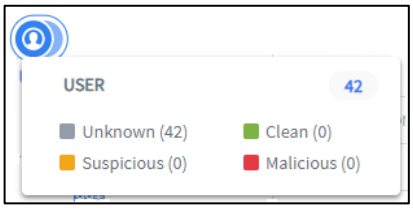
	Cho phép quay lại vị trí trung tâm của biểu đồ (máy gốc)
	Cho phép mở rộng màn hình tối đa để xem biểu đồ và thao tác trên biểu đồ

Ví dụ một biểu đồ mặc định như sau:



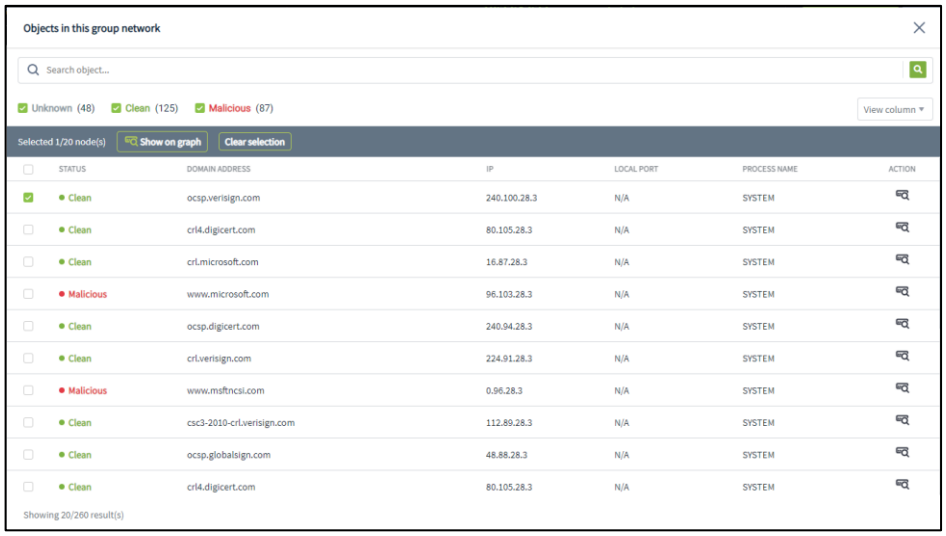
+ Trường hợp tại mỗi loại đối tượng có nhiều hơn 01 đối tượng trực thuộc, các đối tượng sẽ được tự động nhóm lại.

+ Hover để xem thống kê nhanh tại từng nhóm đối tượng như sau:



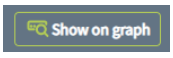
➔ Từ đây, muốn điều tra loang tiếp các đối tượng thực hiện các bước như sau:

Bước 1: Click chọn nhóm đối tượng muốn xem, hiển thị giao diện như sau:



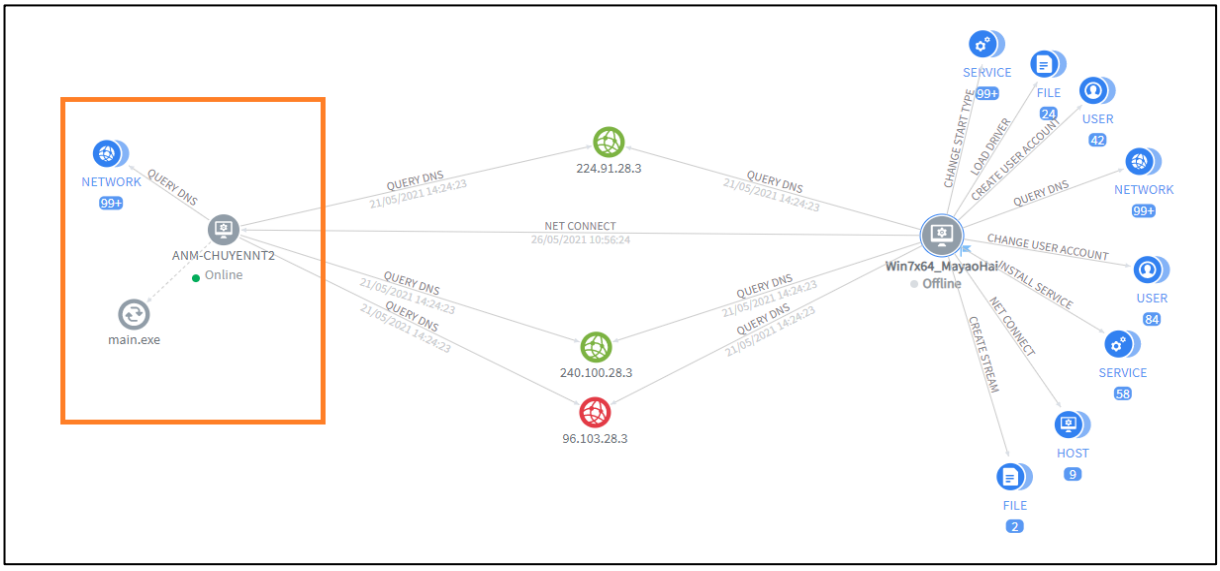
+ Cho phép lọc các đối tượng trong nhóm theo trạng thái

hoặc tìm kiếm nhanh bằng cách nhập nhập dữ liệu muốn tìm kiếm trong tất cả các trường;

+ Khi đã chọn được đối tượng phù hợp, chọn  để hiển thị 01 đối tượng lên biểu đồ hoặc chọn 

để chọn tối đa 20 đối tượng lên biểu đồ;

Lưu ý: Nếu đối tượng được mở rộng là một máy tính, mặc định khi hiển thị đối tượng, cũng tự động hiển thị các đối tượng các quan hệ trực tiếp đến máy tính trong vòng 01 ngày kể từ thời điểm phát sinh Alert



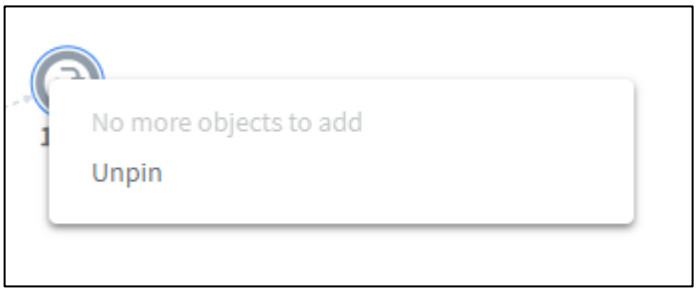
Bước 2: Sau khi đã hiển thị các đối tượng cần điều tra trên biểu đồ, các thao tác hỗ trợ mở rộng/thu gọn bao gồm:

+ Tại máy gốc/máy tính thường: Hỗ trợ thu gọn các đối tượng về trạng thái mặc định khi hiển thị máy (Chỉ bao gồm các đối tượng có quan hệ trực tiếp với máy, mỗi loại đối tượng nếu nhiều hơn 01 đối tượng, hiển thị dạng nhóm) bằng cách chọn chuột phải tại đối tượng, sau đó chọn "Group child-level objects";

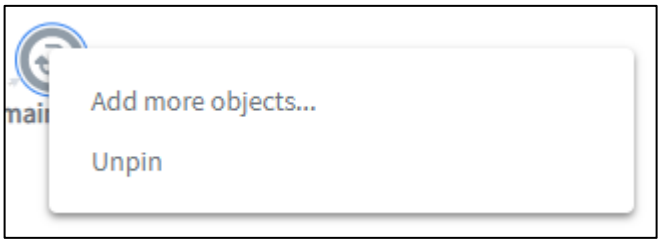
+ Tại các đối tượng khác: Hỗ trợ thu gọn bằng cách nhóm lại theo loại đối tượng và loại quan hệ với các đối tượng cùng cấp bằng cách chọn chuột phải tại đối tượng, sau đó chọn "Group same-level objects";

+ Tại đối tượng là tiến trình (process) cho phép mở rộng để điều tra loang bằng cách chọn chuột phải tại đối tượng,

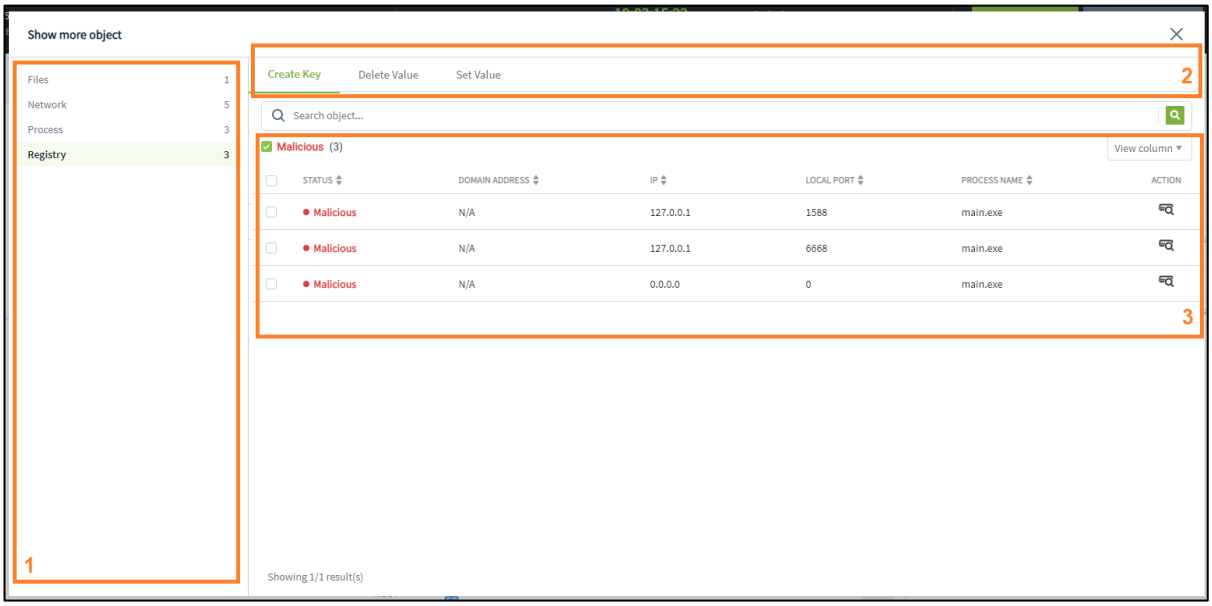
+ Trường hợp không thể tiếp tục loang, hiển thị:



+ Trường hợp có thể loang, chọn "Add more objects…"



Hiển thị giao diện cho phép chọn đối tượng muốn loang đến



1 – Chọn loại đối tượng;

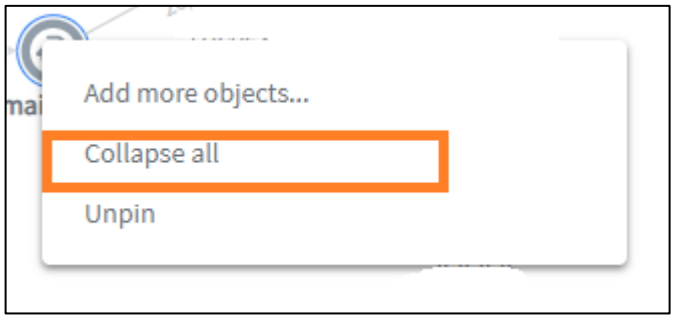
2 – Chọn loại quan hệ từ tiến trình tới đối tượng;

3 – Chọn trực tiếp đối tượng muốn hiển thị. Hỗ trợ tìm kiếm theo trạng thái độc/sạch của đối tượng hoặc tìm kiếm theo nội dung có tại các trường thông tin của đối tượng.

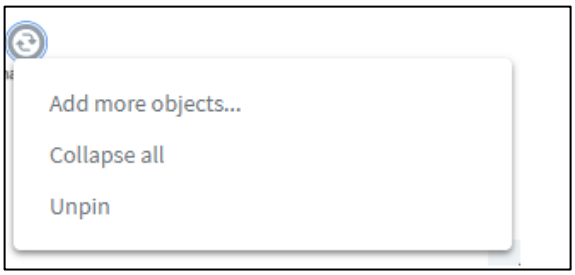
+ Chọn View column để lựa chọn các trường thông tin hiển thị hoặc dùng tính năng để sắp xếp thông tin trong danh sách

+ Khi đã chọn được đối tượng phù hợp, chọn để hiển thị 01 đối tượng lên biểu đồ hoặc chọn Show on graph để chọn tối đa 20 đối tượng lên biểu đồ;

+ Tại đối tượng là tiến trình (process), khi có các đối tượng đang được mở rộng cho phép thu gọn lại bằng cách chọn chuột phải tại đối tượng;

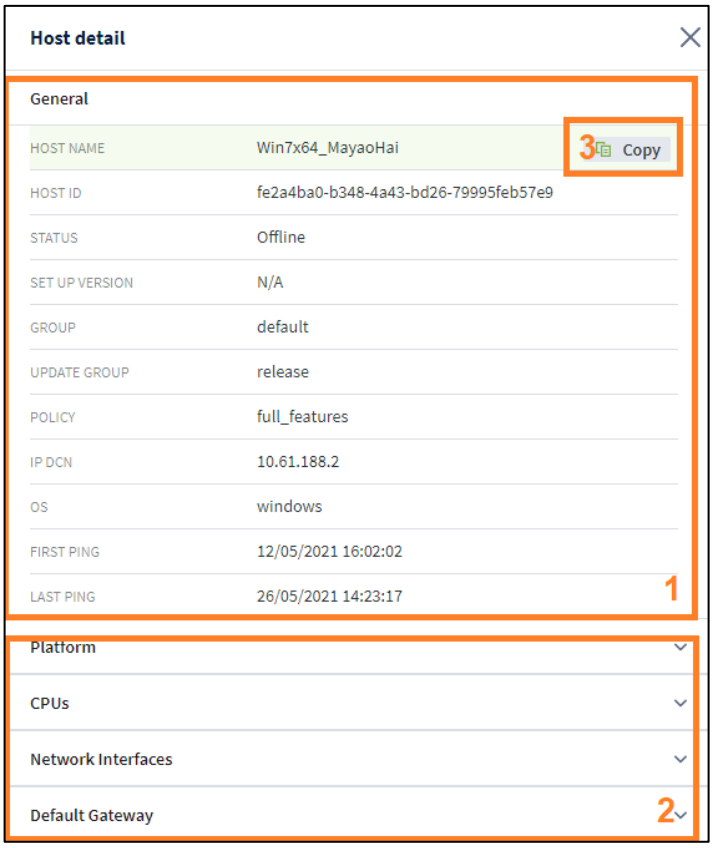


+ Mặc định tại biểu đồ, các đối tượng tự động chạy và giữ khoảng cách với nhau khi bị di chuyển. Trường hợp dùng chuột chọn và kéo thả các đối tượng, sau khi bỏ chuột đối tượng tự động được Pin vào vị trí mới. Để hủy thao tác Pin, chọn Unpin



3.3.5.2 Khu vực hiển thị thông tin chi tiết

Là tính năng bổ sung của biểu đồ, cho phép hiển thị thông tin chi tiết của các thành phần trong biểu đồ (bao gồm các đối tượng và mối quan hệ trong biểu đồ);

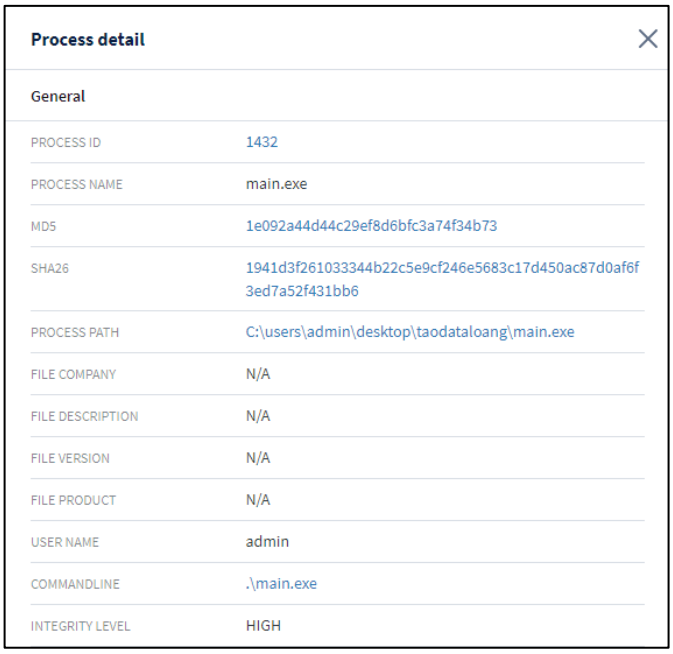


1 – Nhóm thông tin chung: Bao gồm các thông tin chung/thông tin định danh của đối tượng, mặc định luôn hiển thị khi vừa truy cập;

2 – Nhóm thông tin chi tiết: Bao gồm các thông tin chi tiết của đối tượng, được phân thành các nhóm thông tin khác nhau, mặc định các nhóm thông tin này sẽ được đóng lại, chọn ˅ để mở rộng và hiển thị nhóm thông tin.

+ Thao tác Copy hỗ trợ sao chép nội dung trường thông tin

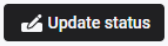
Lưu ý: Một số trường thông tin định danh đối tượng cho phép link nhanh để tra cứu trong Event Search hoặc Agent Management.



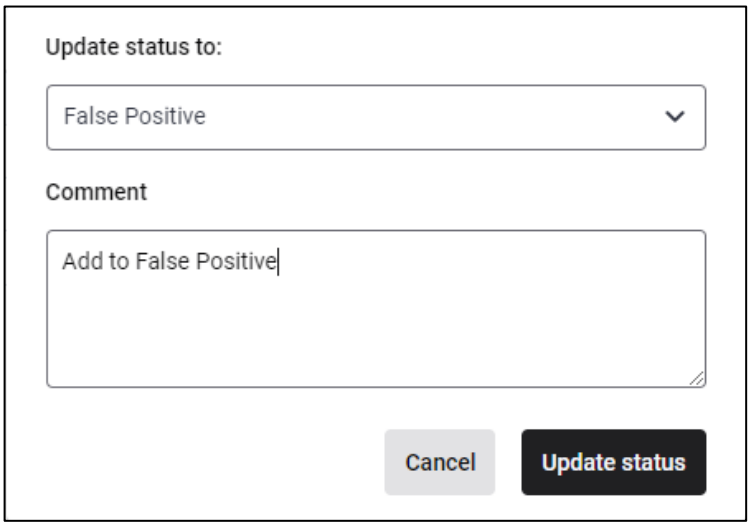
3.3.6 Cập nhật trạng thái không nguy hiểm hoặc đóng cảnh báo cho 01/nhiều Alert hoặc nhóm Alert

Mục đích: Cho phép đánh dấu Alert là không nguy hiểm;

Bước 1: Chọn 01/nhiều Alert muốn đánh dấu không nguy hiểm;

Bước 2: Chọn 

để cập nhật trạng thái của Alert:



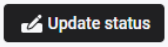
Bước 3: Chọn Update Status to “False Positive”;

Bước 4: Nhập lý do đánh dấu không nguy hiểm và:

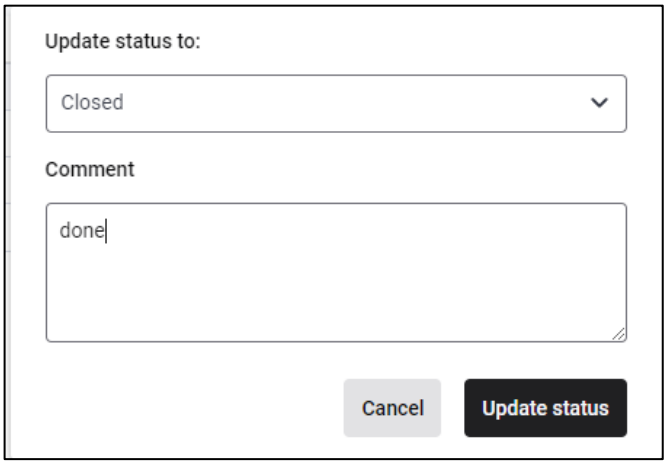
- Chọn “ Update status” để xác nhận đánh dấu không nguy hiểm cho Alert;
- Chọn “Cancel” để xác nhận hủy thao tác đánh dấu không nguy hiểm cho Alert;

Chọn Update Status to “Close” để đóng Alert;

Bước 1: Chọn 01/nhiều Alert muốn đóng (Closed);

Bước 2: Chọn 

để cập nhật trạng thái của Alert:



Bước 3: Chọn Update Status to “Closed”;

Bước 4: Nhập lý do đóng Alert và:

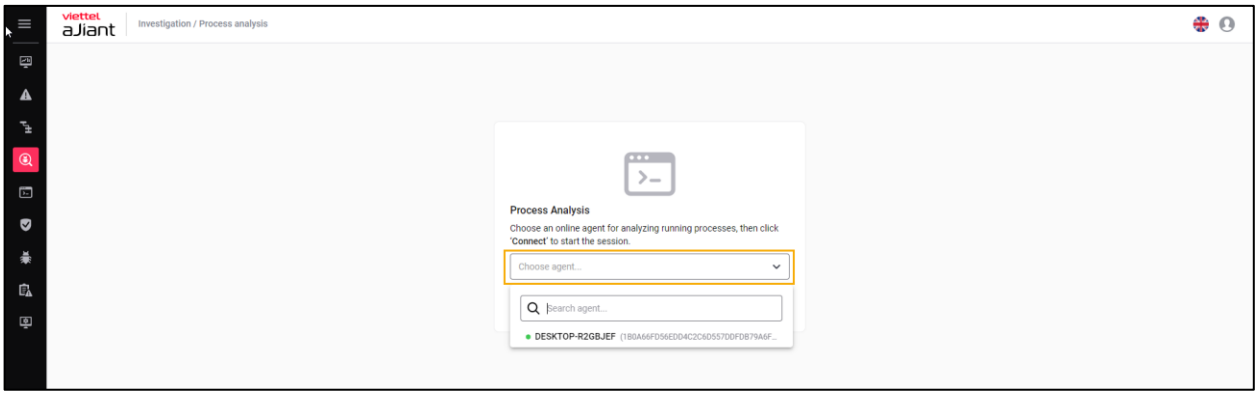
- Chọn “ Update status” để xác nhận đóng Alert;
- Chọn “Cancel” để xác nhận hủy thao tác đóng Alert;

3.4 Nhóm chức năng Investigation

Màn hình Investigation gồm một số tab nhỏ là Process Analysis, Event Search, Deploy Tools.

3.4.1 Process Analysis

- Mục đích: Chức năng cho phép người dùng tạo kết nối và kiểm tra hiện trạng process dưới máy người dùng. Trong đó:



Danh sách máy người dùng:

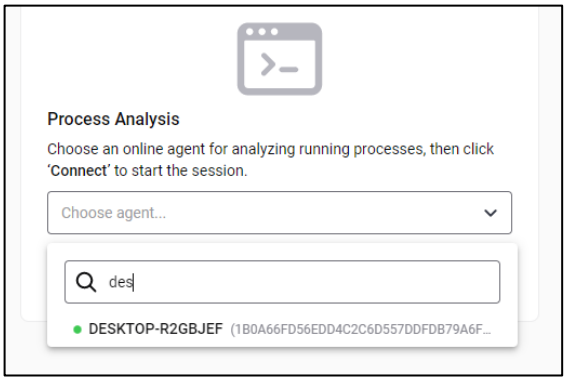
+ User đăng nhập thuộc group root: Hiển thị tất cả Agent trong hệ thống active < 30 ngày;

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

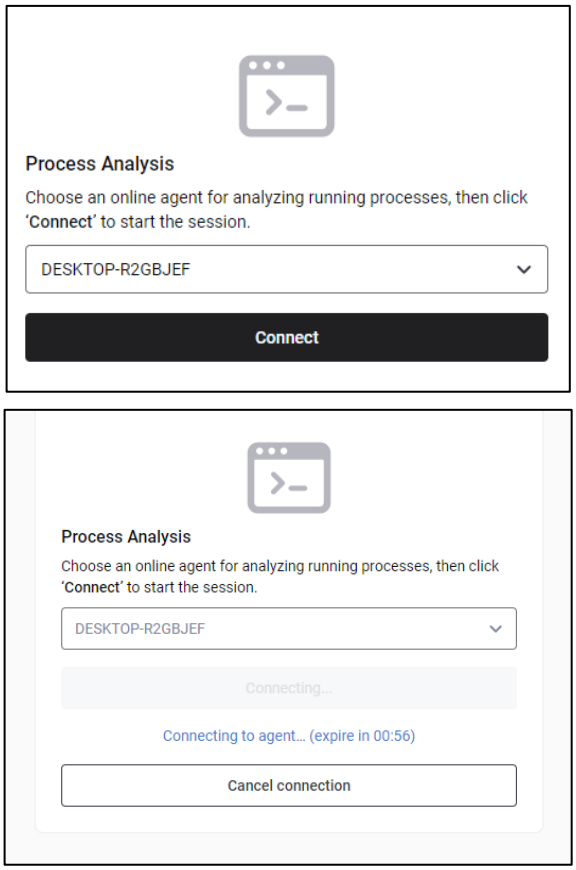
+ User đăng nhập thuộc group cha: Hiển thị tất cả Agent thuộc group của user đang login và group con tương ứng;

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

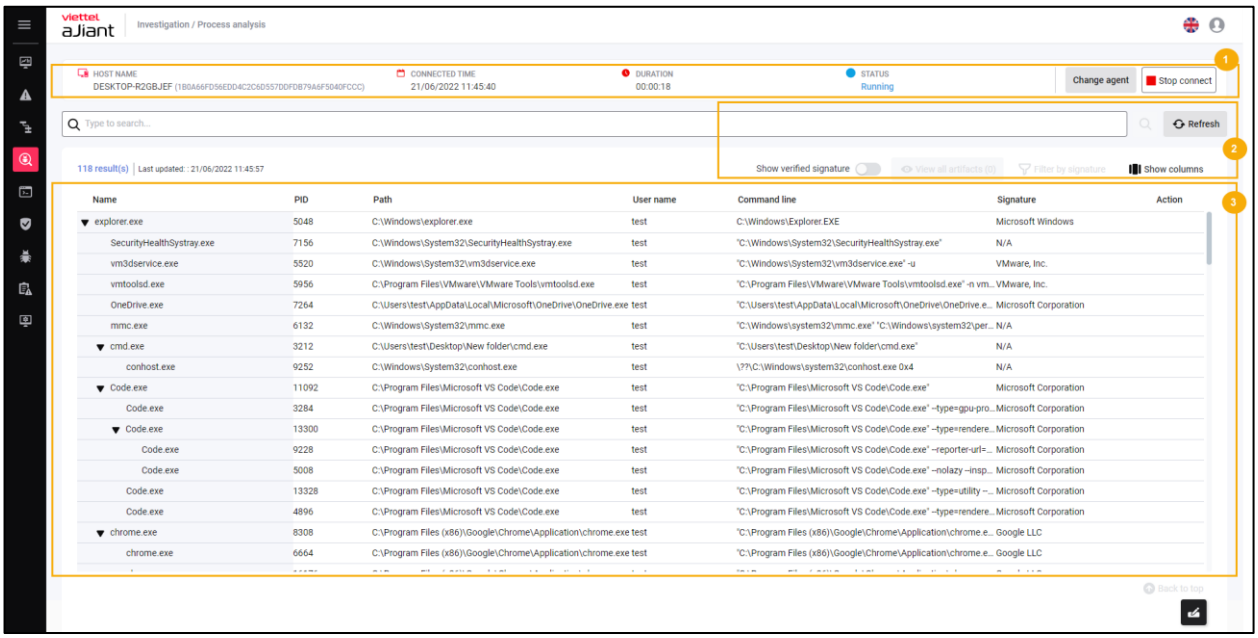
Bước 1: Tìm kiếm và chọn Agent kết nối (Lưu ý để đảm bao có thể kết nối, danh sách chỉ hiển thị các máy đang Online);



Chọn 01 máy và click nút "Connect" để thực hiện kết nối (kết nối có thể mất tối đa 60 giây)



Bước 2: Xem danh sách tiến trình đang hoạt động tại máy người dùng



Trong đó giao diện chia làm các nhóm thông tin:

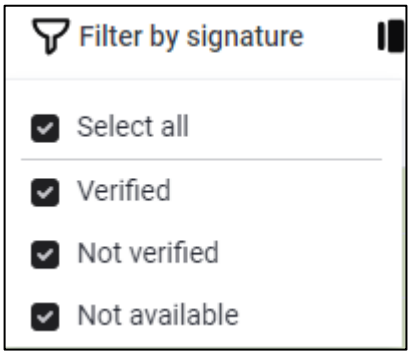
1 – Nhóm thông tin liên quan đến kết nối, bao gồm: Máy đang kết nối, thời gian tạo kết nối, thời lượng kết nối tính đến hiện tại, trạng thá kết nối

2 – Nhóm thông tin hỗ trợ tìm kiếm/làm mới và lọc dữ liệu tại danh sách, bao gồm các thao tác:

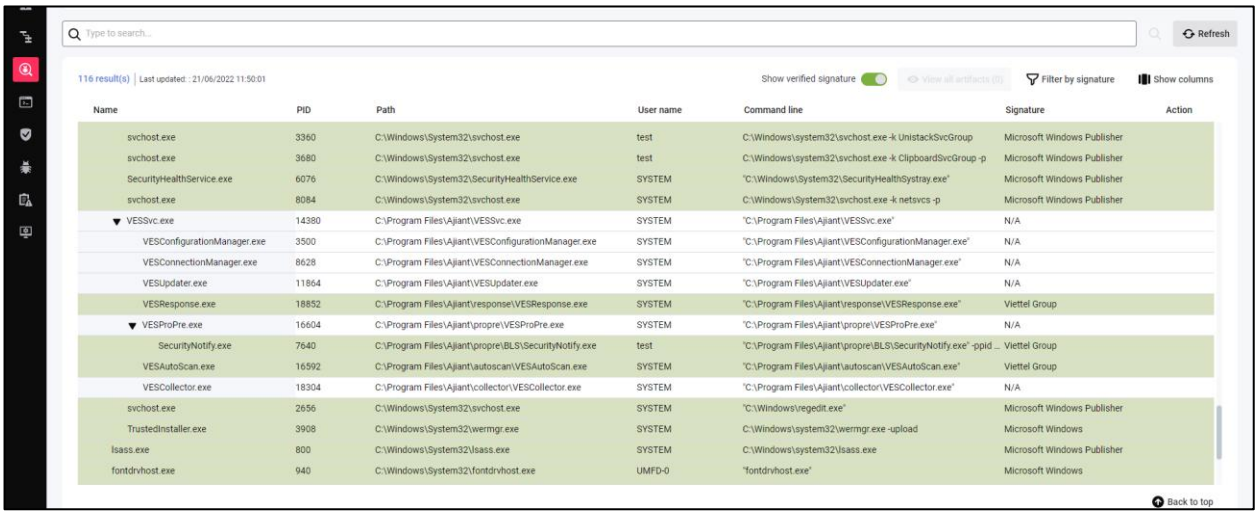
: Cho phép tìm kiếm theo từ khóa của dữ liệu đang hiển thị trong tất cả các trường trên danh sách;

Refresh : Cho phép làm mới dữ liệu (vẫn giữ lại các điều kiện tìm kiếm và điều kiện lọc đang sử dụng, chỉ lấy dữ liệu mới nhất từ máy người dùng để hiển thị);

Show verified signature : Cho phép bật/tắt việc lấy thông tin chữ ký số cho các tiến trình. Trong trường hợp bật cấu hình này, cho phép lọc dữ liệu tiến trình theo chữ ký số:



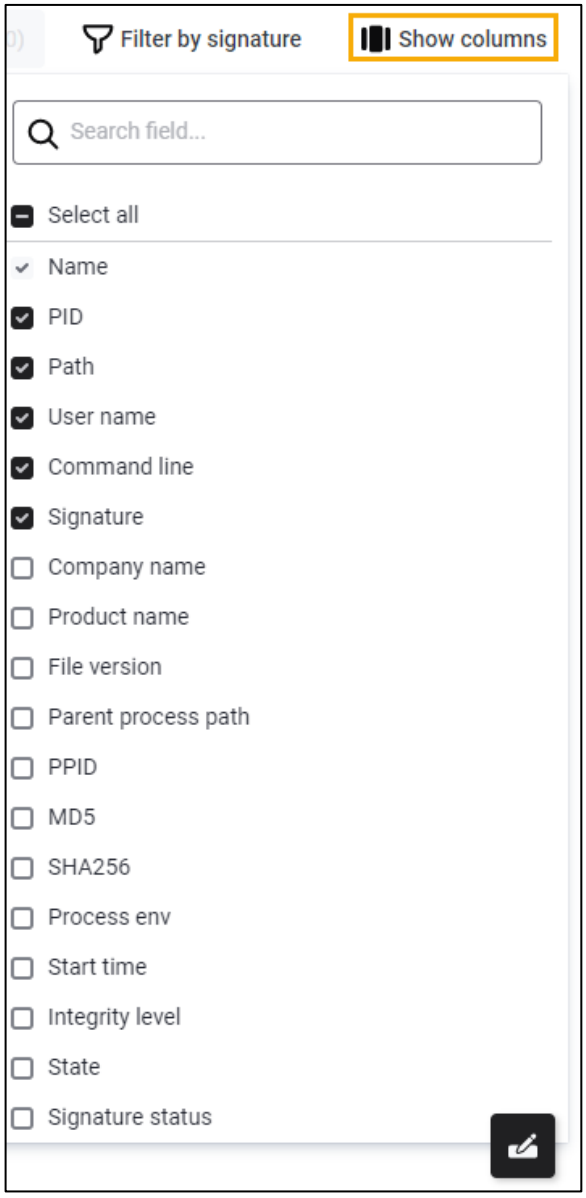
Các trạng thái chữ ký số sẽ quy định màu của bản ghi tương ứng



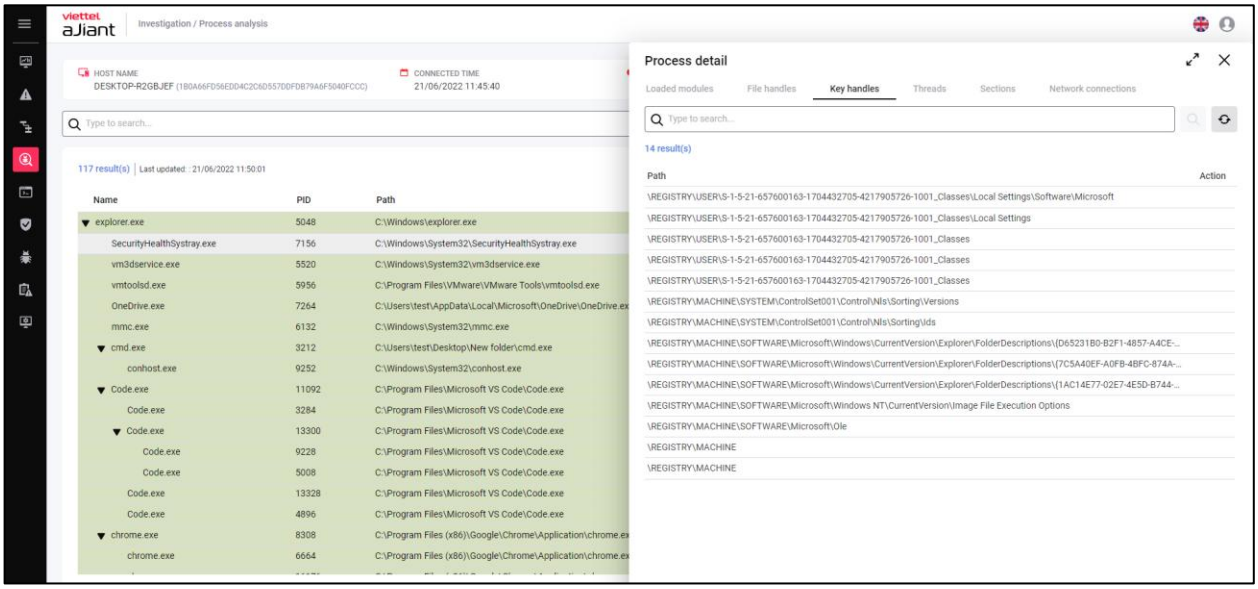
- Verified: Xanh – có chữ ký số và còn hạn;
- Not verified: Đỏ - không có chữ ký số hoặc chữ ký hết hạn;
- N/A: Trắng – không tìm thấy thông tin chữ ký số;

Show columns ▼: Cho phép điều chỉnh trường hiển thị trên danh sách tiến trình.

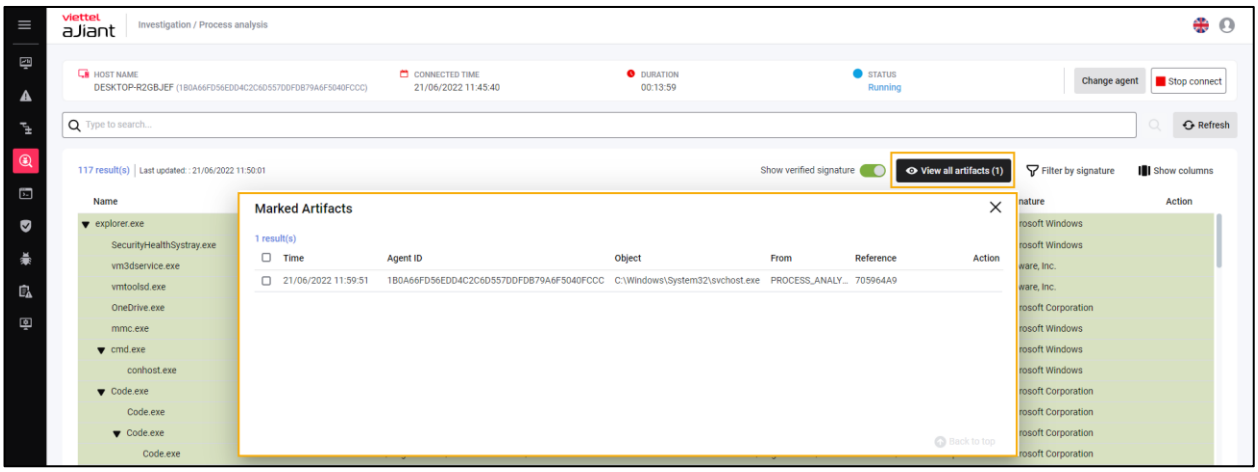
Trên danh sách ngoài trường "Name" luôn hiển thị cố định, các trường còn lại đều có thể tùy chọn hiển thị hoặc không hiển thị.



3 – Danh sách tiến trình, hiển thị dữ liệu tiến trình hiện tại trên máy người dùng với các trường thông tin đã chọn trong phần Show column.Tại mỗi bản ghi, click đúp để xem chi tiết tiến trình;



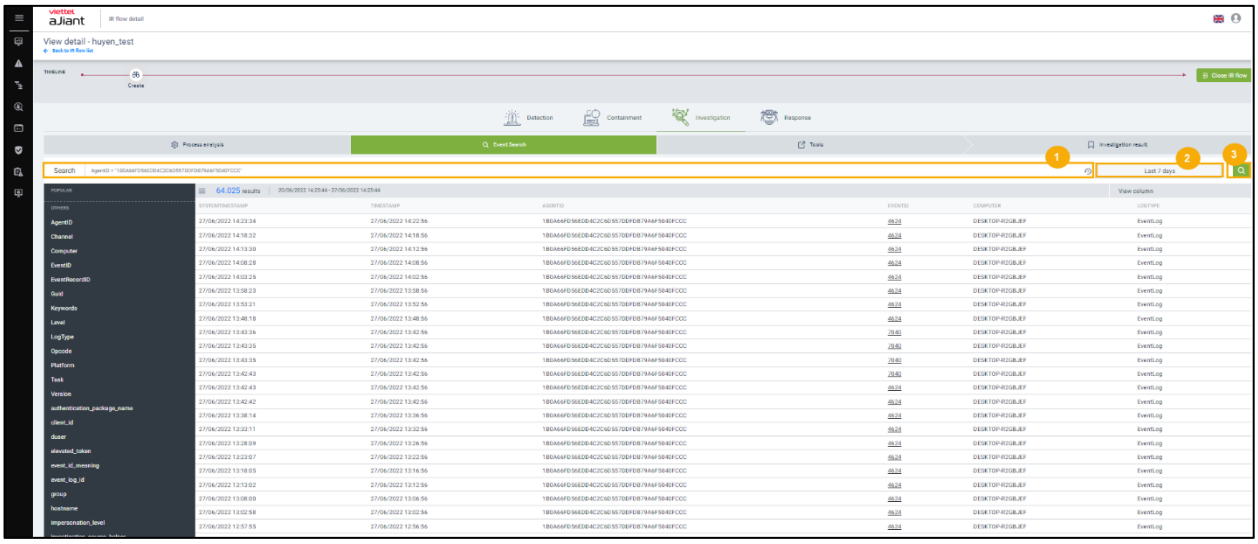
Chi tiết tiến trình được chia thành các tabs, với mỗi tab, danh sách thông tin tương ứng được hiển thị.



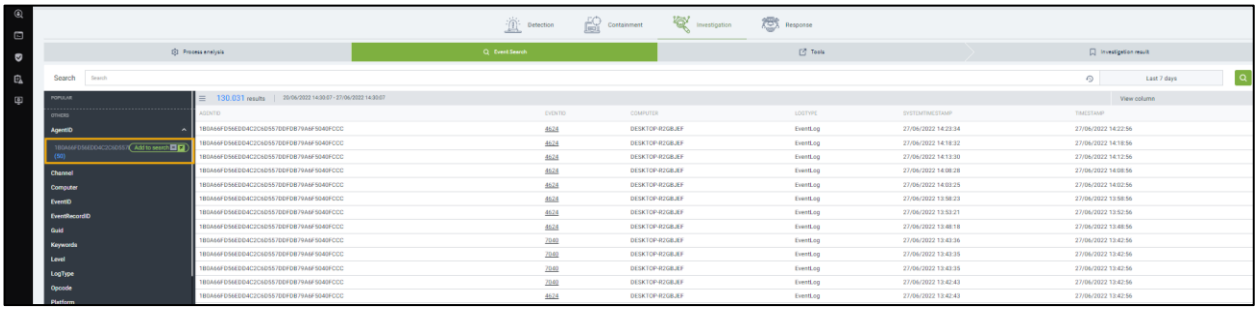
3.4.2 Event Search

3.4.2.1 Tìm kiếm Event

Bước 1: Nhập câu query >Chọn khoảng thời gian > Click nút “Search”:



Bước 2: Thêm các trường tìm kiếm vào câu query với trường Popular và Others bằng cách chọn queries "=" hoặc "#" tại Add to search:



3.4.2.2 Highlight

Mục đích: Cho phép thêm 01 hoặc nhiều highlight để rà soát đồng thời tại một thời điểm (không giới hạn số lượng tối đa), khi thực hiện search hoặc sort thì mọi highlight đã tạo sẽ bị clear;

Các bước thự hiện:

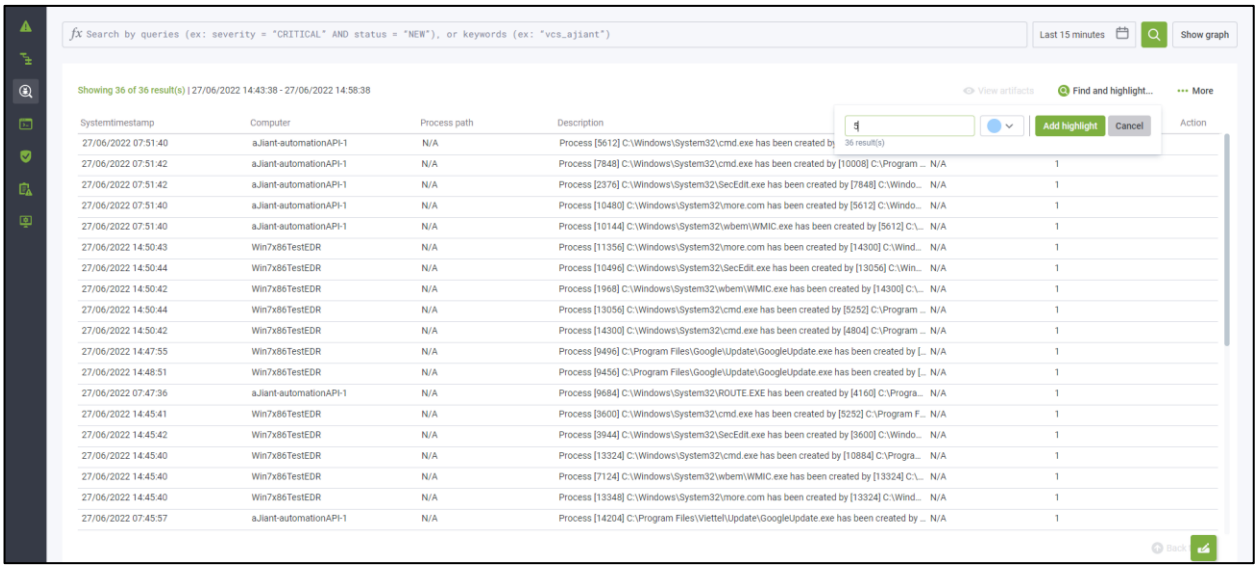
Bước 1: ND chọn Investigation >> Chọn tab Event search;

Bước 2: Màn hình hiển thị danh sách event, Chọn nút "Find and highlight", HT hiển thị poup Find in table;

Bước 3: Nhập vào từ khóa đánh dấu, lựa chọn màu đánh dấu và xác nhận thao tác:

Chọn nút "Add highlight", để xác nhận từ khóa đánh dấu;

Chọn nút "Cancel", để hủy thao tác đánh dấu từ khóa tìm kiếm;



3.4.2.3 Need help

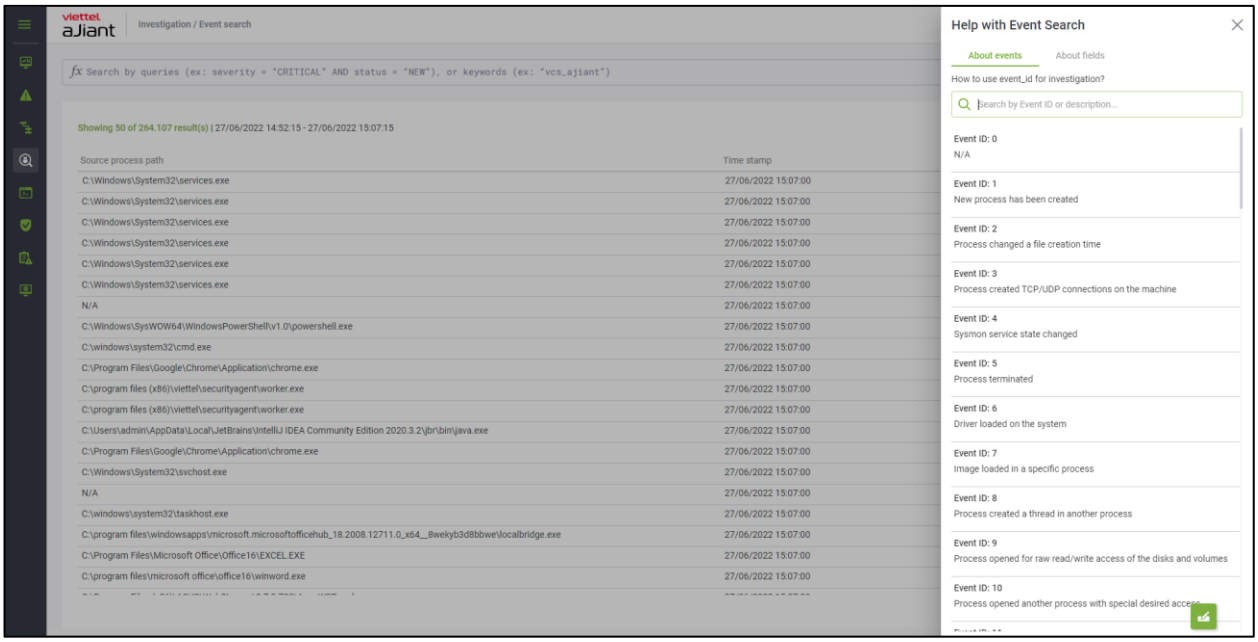
- Mục đích: tra thông tin event, ý nghĩa trường;
- Các bước thực hiện:

Bước 1: ND chọn Investigation >> Chọn tab Event search;

Bước 2: Tại màn hình Event Search, chọn "More";

Bước 3: HT hiển thị danh sách các thao tác: Show columns, Wrapt text, Export, Need help, Chọn "Need help?";

Bước 4: HT hiển thị popup Help with Event Search, cho phép tra cứu thông tin, ý nghĩa các trường trong Event Search.



3.4.2.4 **Wrapt text**

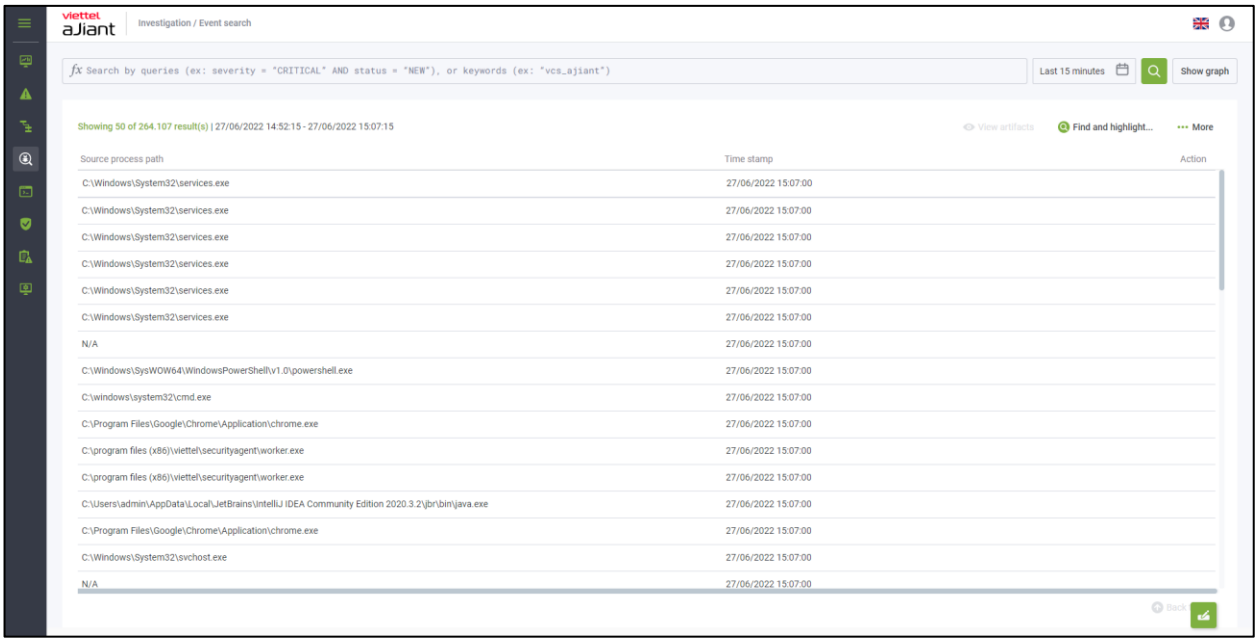
Mục đích: Có thể hiển thị toàn bộ dữ liệu hoặc thu gọn lại dữ liệu khi click vào nút "wrap text";

Các bước thực hiện:

Bước 1: Tại màn hình Event Search, chọn "More";

Bước 2: HT hiển thị danh sách các thao tác: Show columns, Wrapt text, Export, Need help, Chọn "Wrapt text?";

Bước 3: HT thay đổi thông tin hiển thị toàn bộ dữ liệu hoặc thu gọn lại dữ liệu khi click vào nút "Wrap text";



3.4.2.5 Export Data

Mục đích: Cho phép tải xuống dữ liệu liên quan đến Event trong hệ thống

Các bước thực hiện:

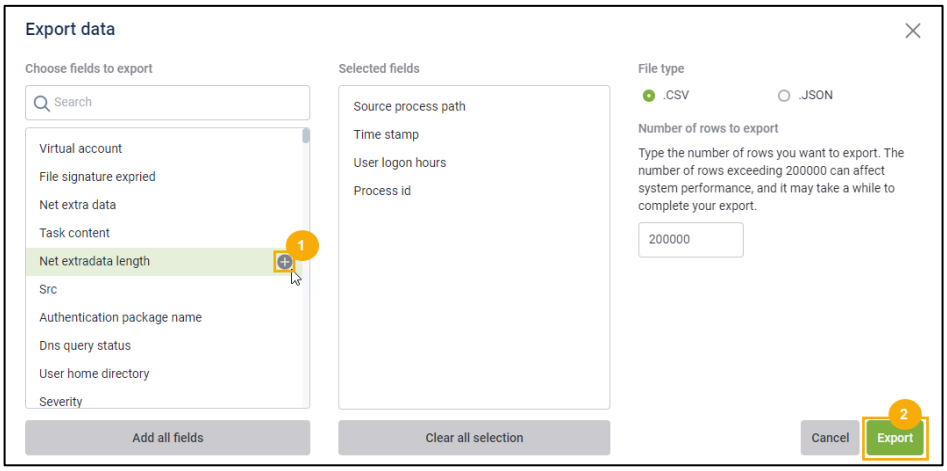
Bước 1: Tại màn hình Event Search, chọn “More”;

Bước 2: HT hiển thị danh sách các thao tác: Show columns, Wrapt text, Export, Need help, Chọn “Export”

Bước 3: HT hiển thị Popup lọc thông tin Data Event, Chọn các tham số lọc theo điều kiện có sẵn trong hệ thống: Chọn các trường thông tin, Định dạng file export, Số dòng và xác nhận thao tác;

Chọn nút “Export”, để xác nhận thao tác tải Data Event;

Chọn nút “Cancel”, để hủy thao tác;



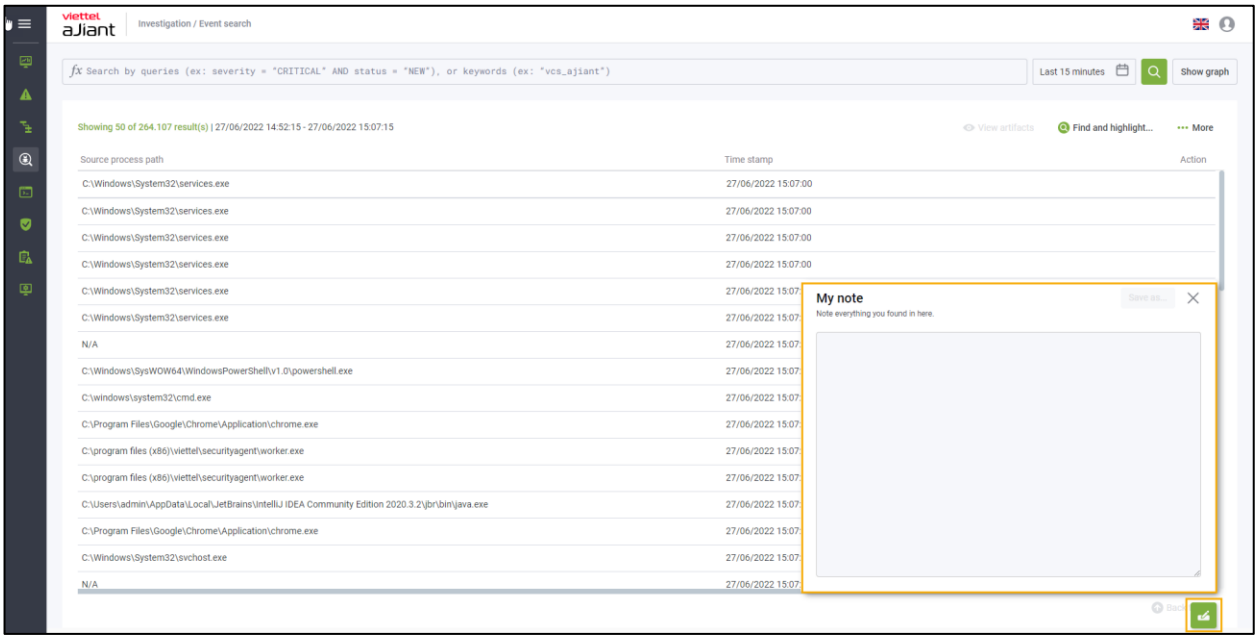
3.4.3 Note

Mục đích: Hiển thị ở tất cả các màn hình, khi di chuyển đến các màn hình thì nội dung không thay đổi, có thể di chuyển được nút "Note";

Các bước thực hiện:

Bước 1: Tại màn hình Event Search, chọn icon ;

Bước 2: HT hiển thị note ở tất cả các màn hình, khi di chuyển đến các màn hình thì nội dung không thay đổi, có thể di chuyển được nút "Note".



3.4.4 Deploy Tools

Mục đích: chức năng cho phép deploy (triển khai) các tools (công cụ) phục vụ điều tra, xử lý sự cố an toàn thông tin từ Portal xuống các Agents.

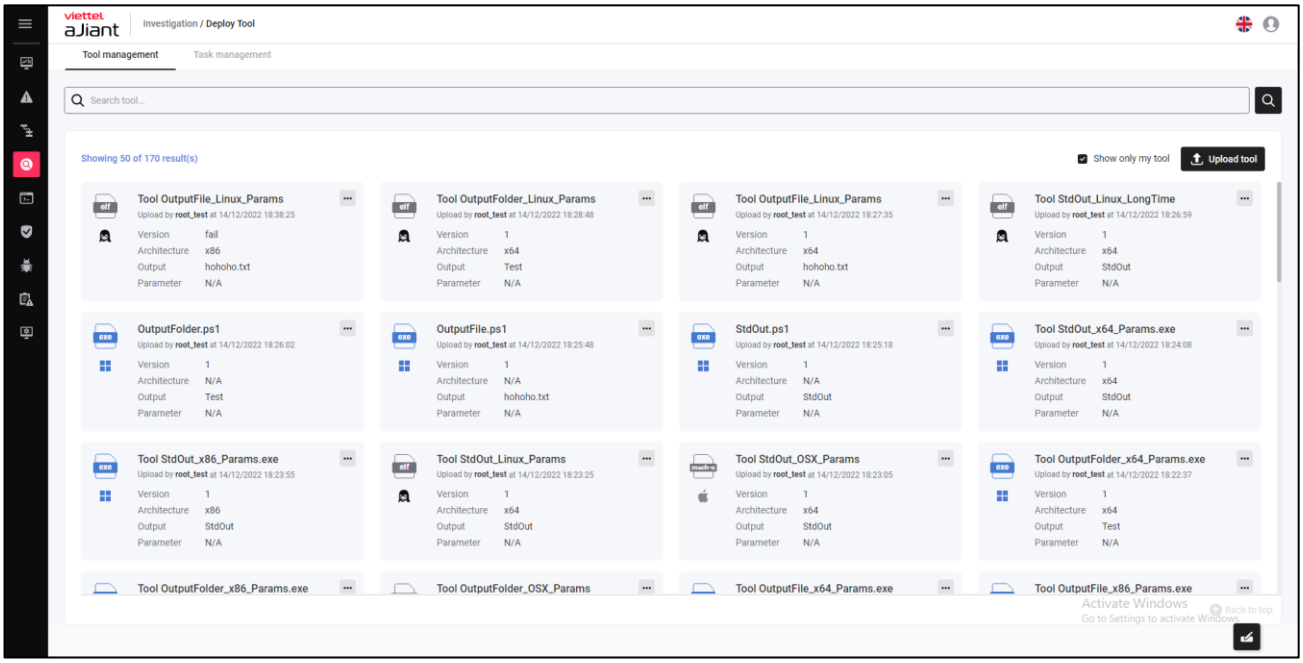
3.4.4.1 Tool Management

Mục đích: quản lý toàn bộ tool của hệ thống, người sử dụng có thể thêm/ xóa tool ở màn hình này. Các tính năng ở màn hình này gồm có:

+ Hiển thị danh sách tool cùng các thông tin chi tiết của tool: Tên, Parameter, Version, Architecture, Upload User, Platform, Output, Thời gian upload;

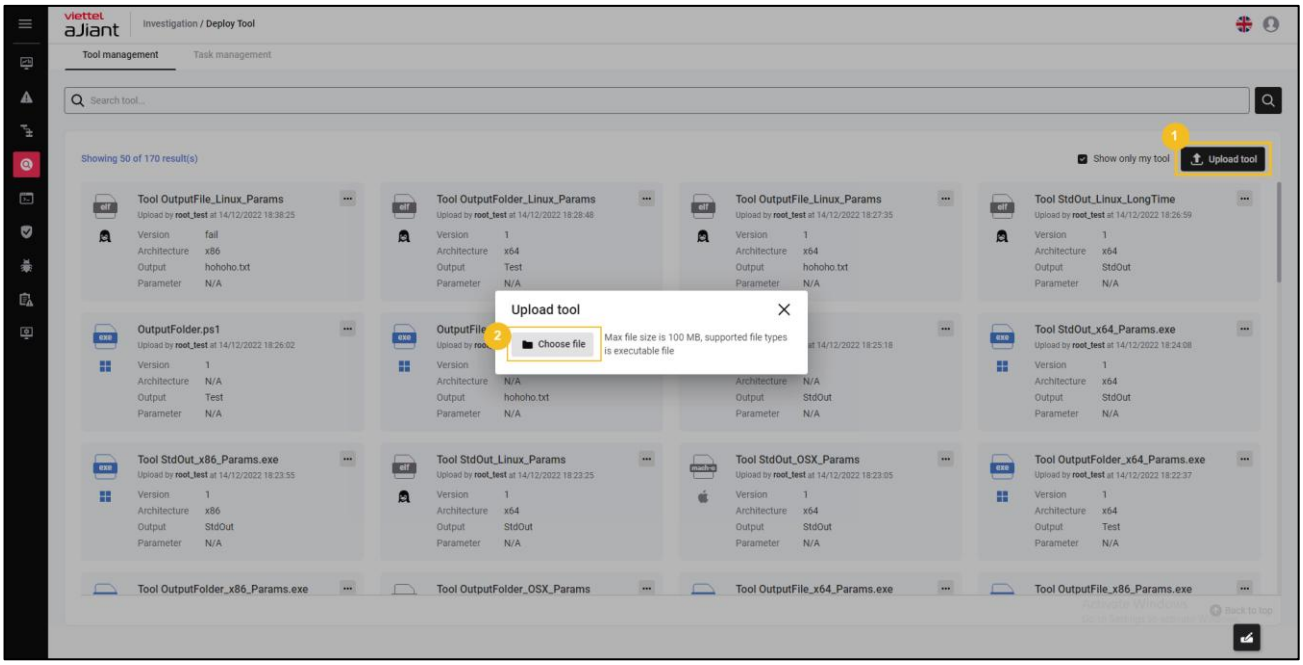
+ Tìm kiếm tool: Tìm kiếm theo tên tool

+ Upload tool: upload tool chạy trên agent Windows, MacOS và Linux có dung lượng tối đa 100MB;

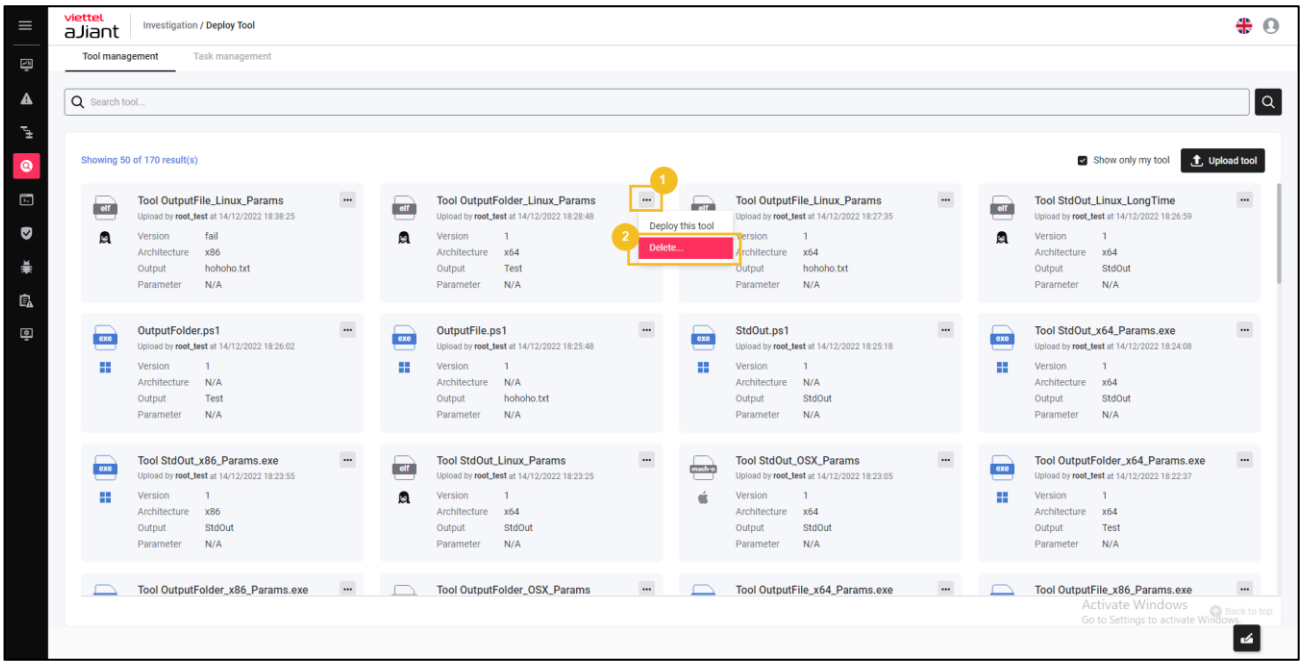


Với tính năng Upload tool thao tác theo các bước sau:

Click vào “Upload tool” > Chọn đường dẫn đến tool cần upload hoặc kéo thả tool vào giao diện > Nhập thông tin vào popup Tool info > click **Upload tool**:



Với tính năng xóa tool, chọn icon ··· tại tool cần xóa > chọn **Delete**



3.4.4.2 **Deploy tool**

Mục đích: Cấu hình thông tin deploy tool dưới agent

Điều kiện:

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

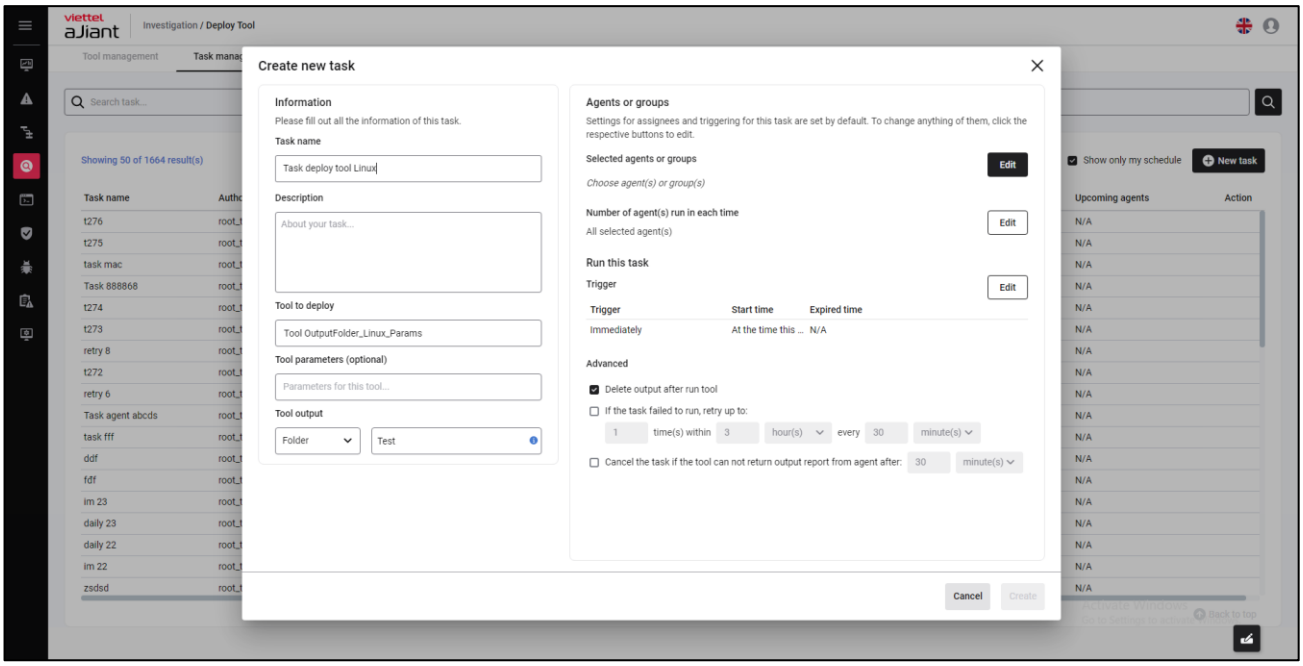
+ User đăng nhập thuộc group default: Hiển thị tất cả Agent thuộc group default;

+ 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;

Các bước thực hiện Deploy tool tại màn hình Tab Tool management:

Bước 1: Sau khi lựa chọn tool, chọn icon [...] tại bản ghi tool cần deploy > chọn **Deploy this tool**, màn hình Create new task hiển thị:

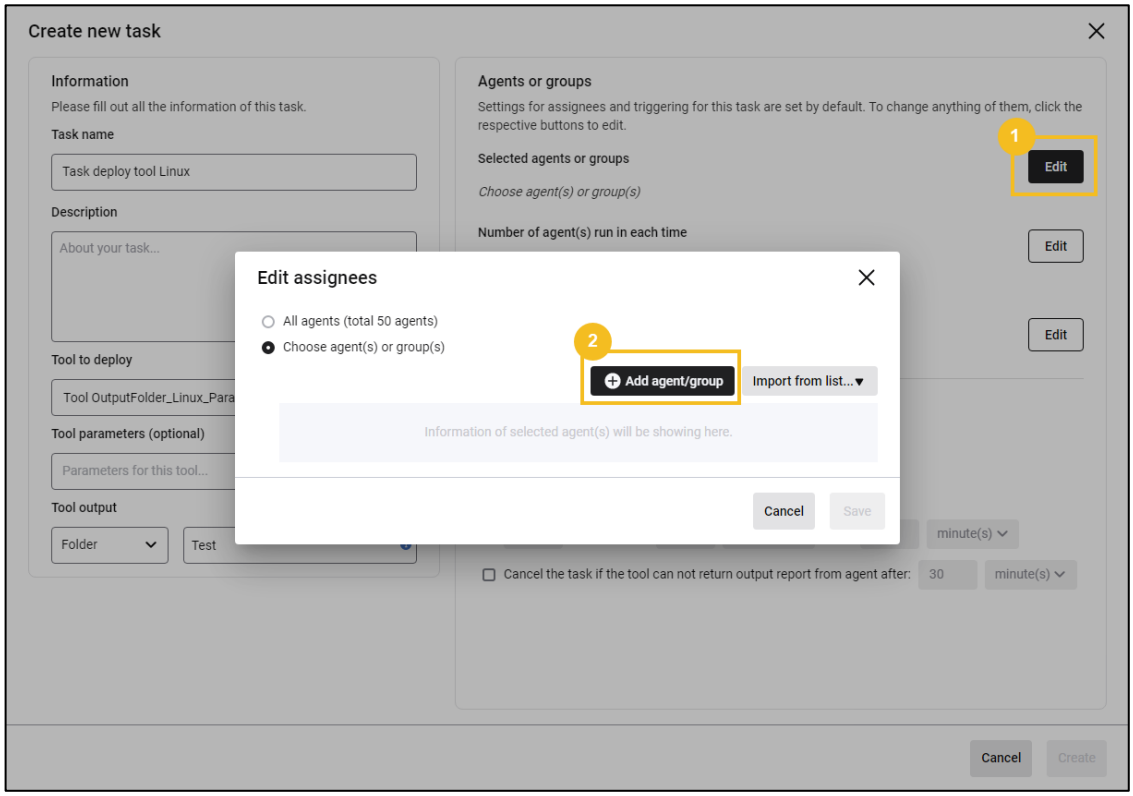


Bước 2: Thực hiện nhập các thông tin task để deploy tool: Task name, Description, Tool parameters, Tool output;

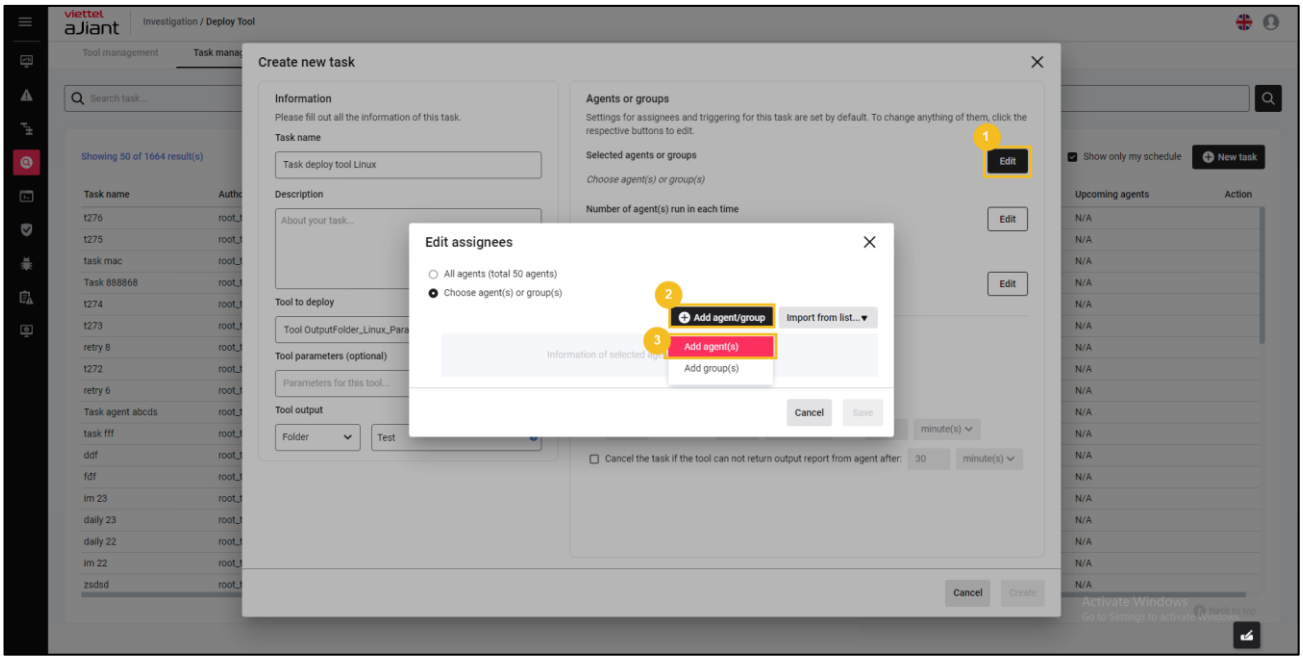
Bước 3: Lựa chọn thông tin nhóm (group), máy trạm (agent) để thực hiện deploy:

Lựa chọn **All agent(s)**: chọn tất cả các agent(s) trong phạm vi quản lý của user đang đăng nhập để thực hiện deploy;

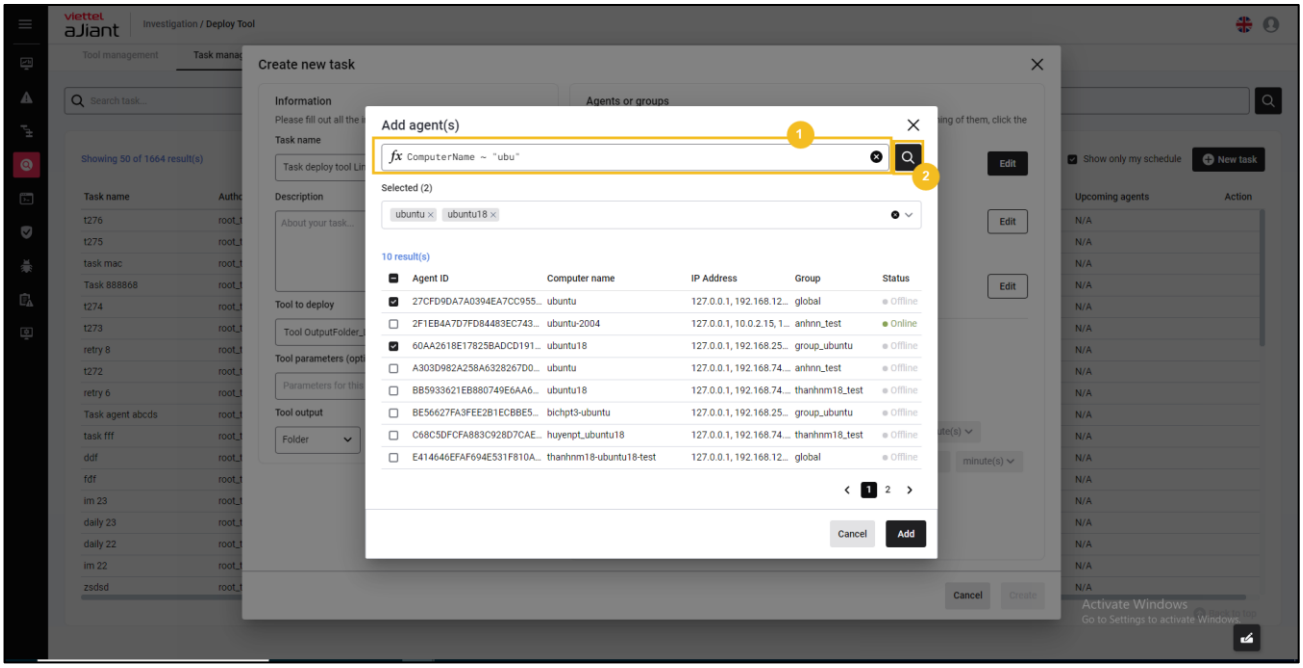
Lựa chọn agents or groups thực hiện deploy – **Choose agent(s) or group(s)**:



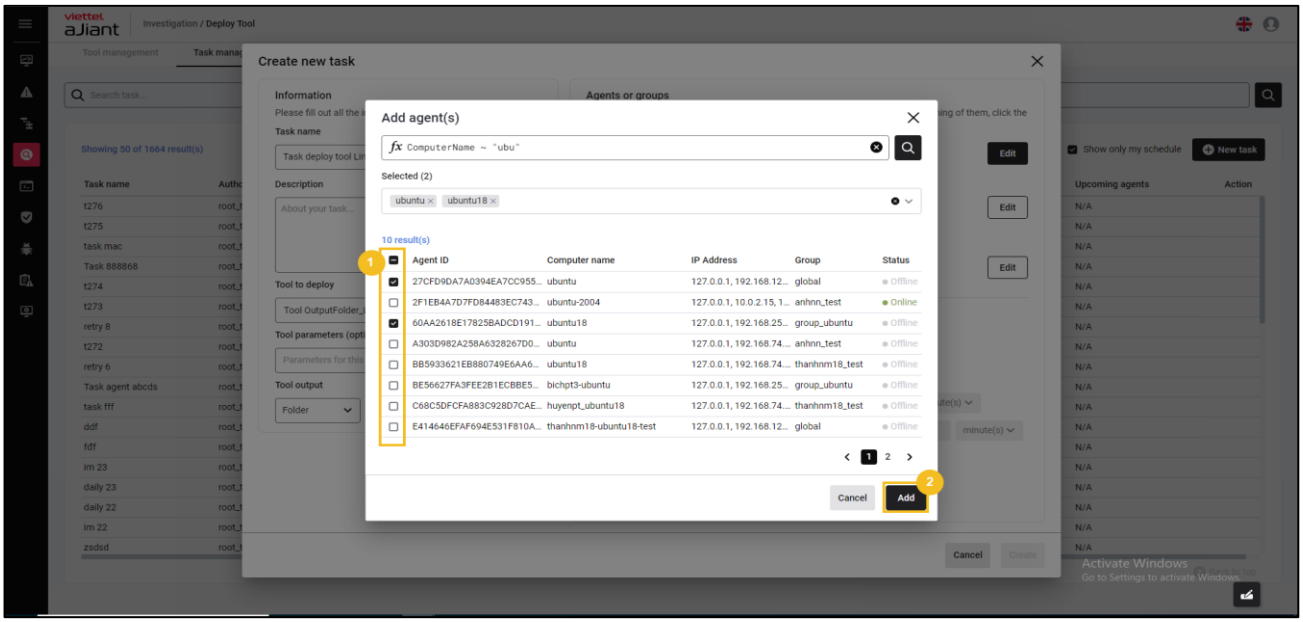
+ Chọn Add agent(s):



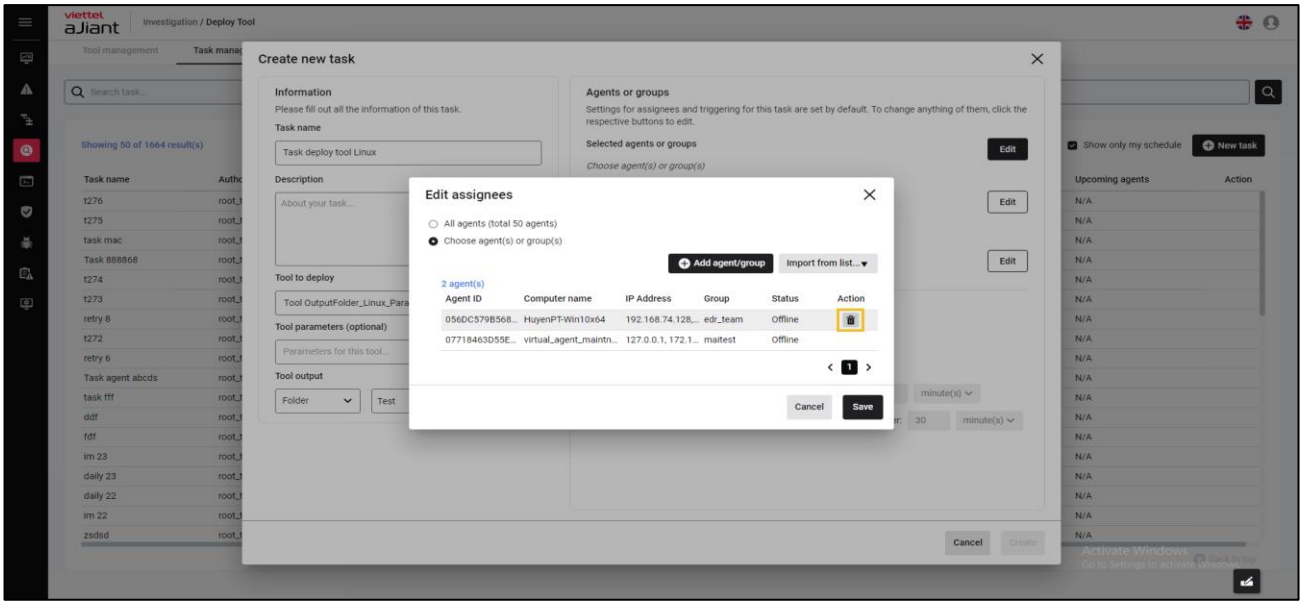
- Tìm kiếm Agent: Cho phép tạo câu lệnh truy vấn, sử dụng câu lệnh truy vấn để tìm kiếm Agent



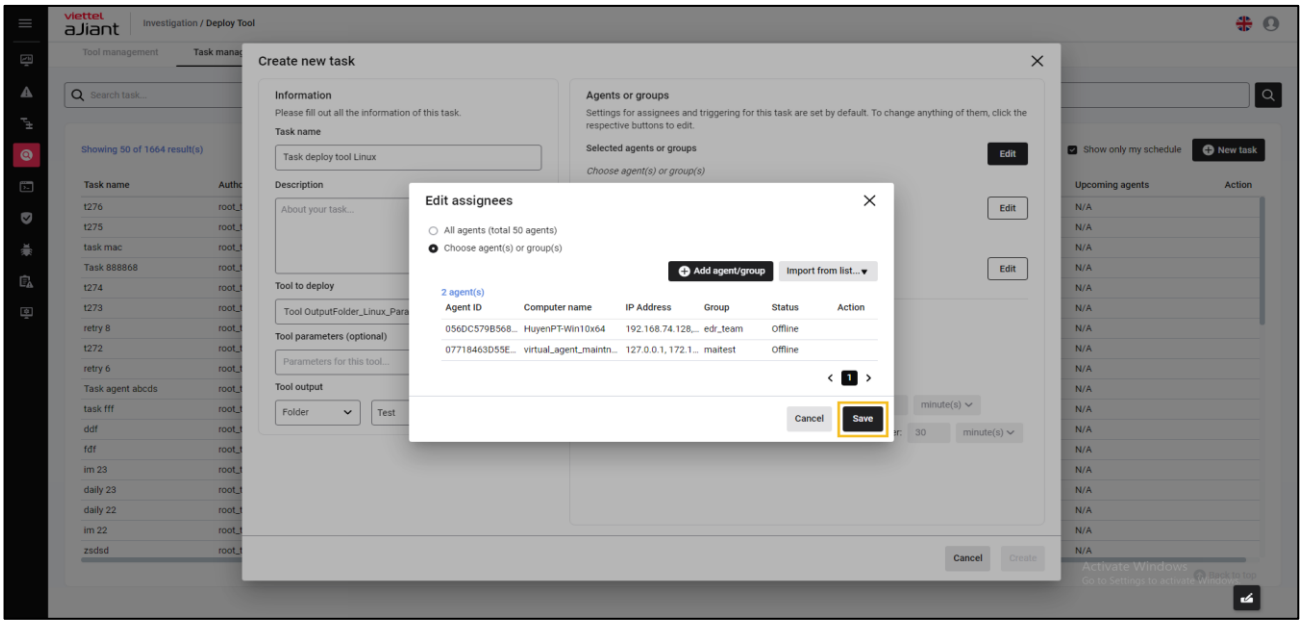
- Chọn Agent(s) để deploy bằng cách tích chọn vào một hoặc nhiều Agent(s) > Thông tin Agent(s) đã được chọn hiển thị ở khung **Selected** > chọn **Cancel** để hủy thao tác thêm Agent để deploy hoặc chọn nút **Add** để xác nhận danh sách Agent(s):



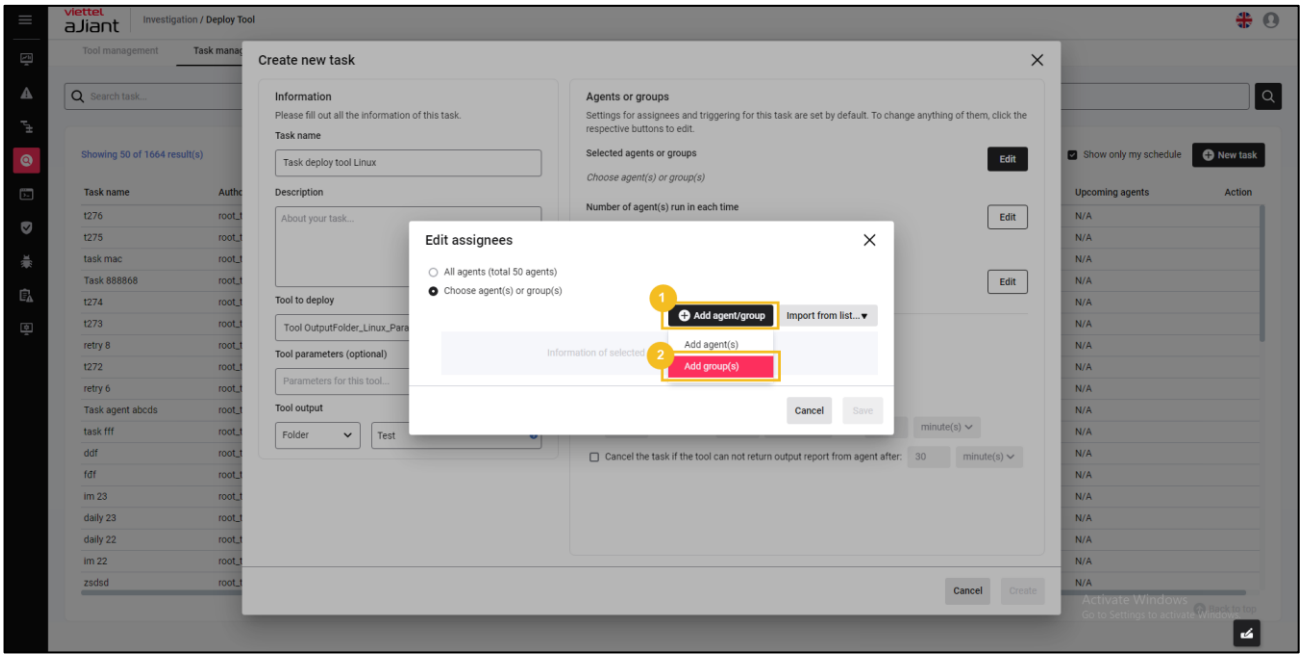
- Hover vào các Agent(s) đã chọn > Chọn icon  để thực hiện loại bỏ Agent(s) khỏi danh sách đã chọn



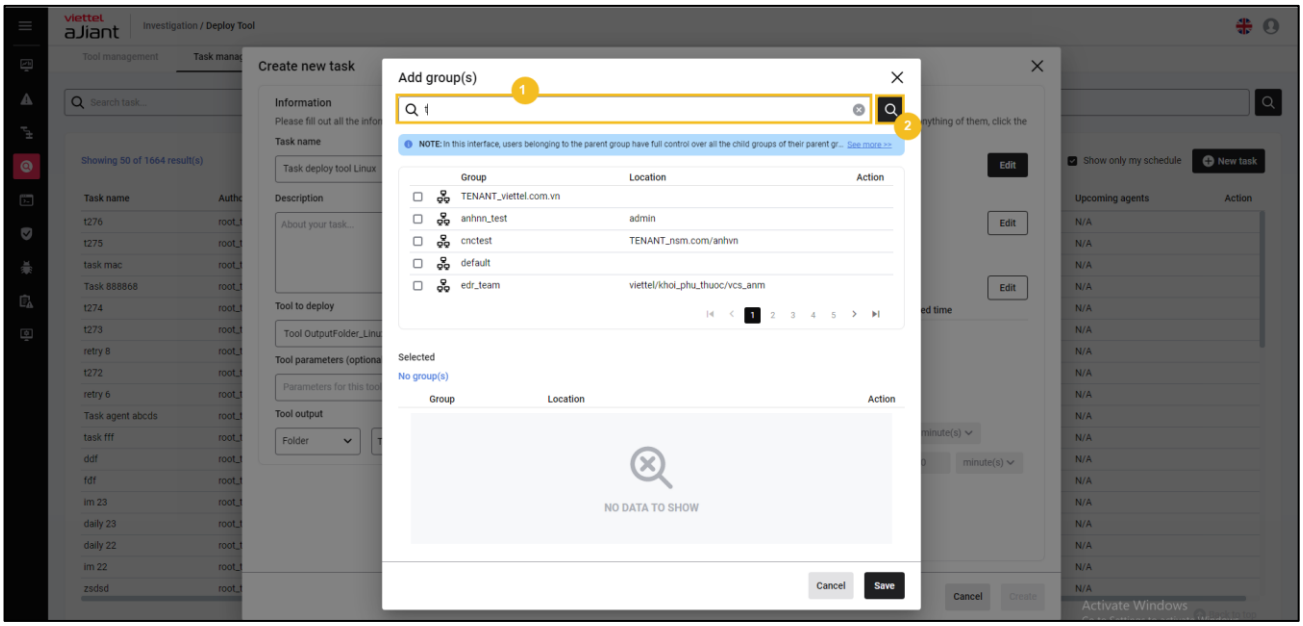
- Chọn **Cancel** để hủy hoặc chọn **Save** để lưu thông tin các Agent(s) đã chọn để deploy:



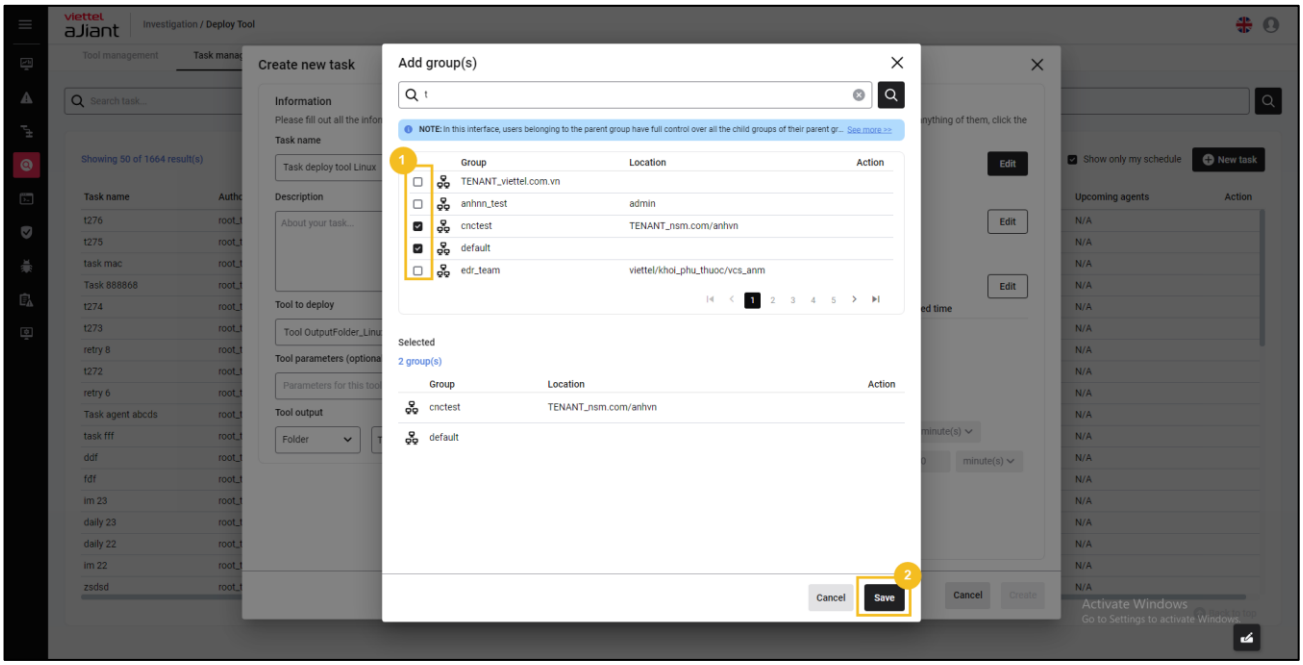
+ Chọn Add group(s):



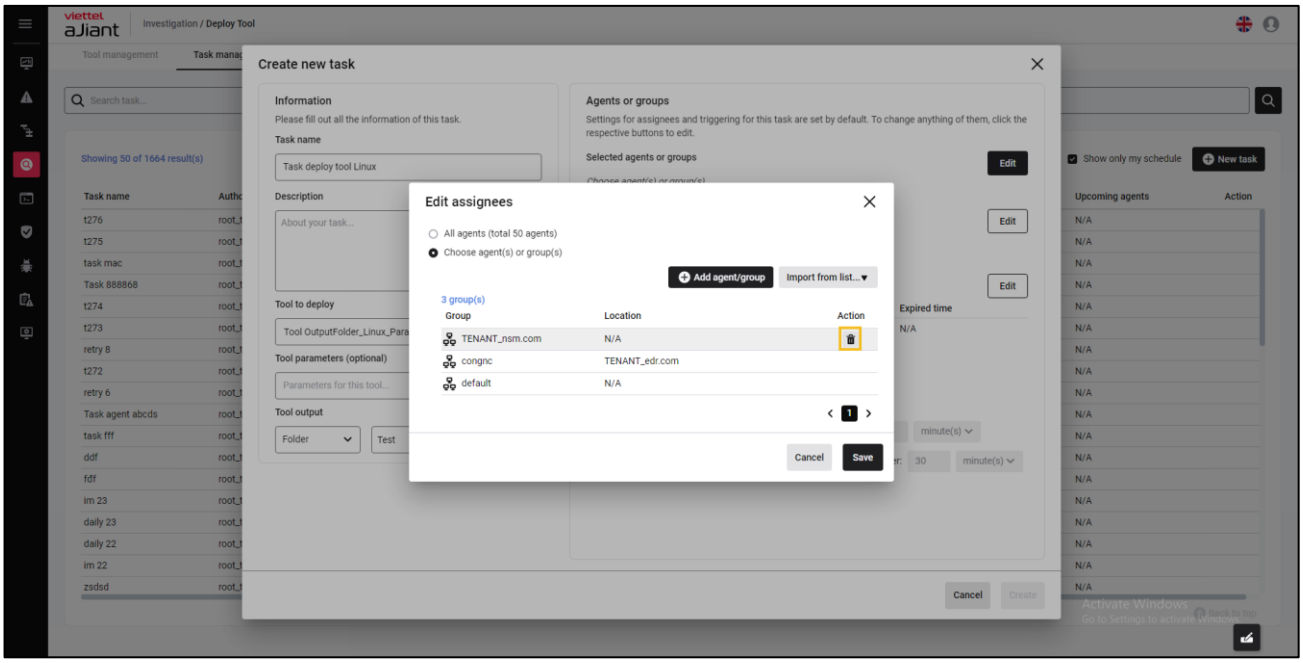
- Tìm kiếm group(s) theo tên, cho phép nhập từ khóa tìm kiếm group theo tên group:



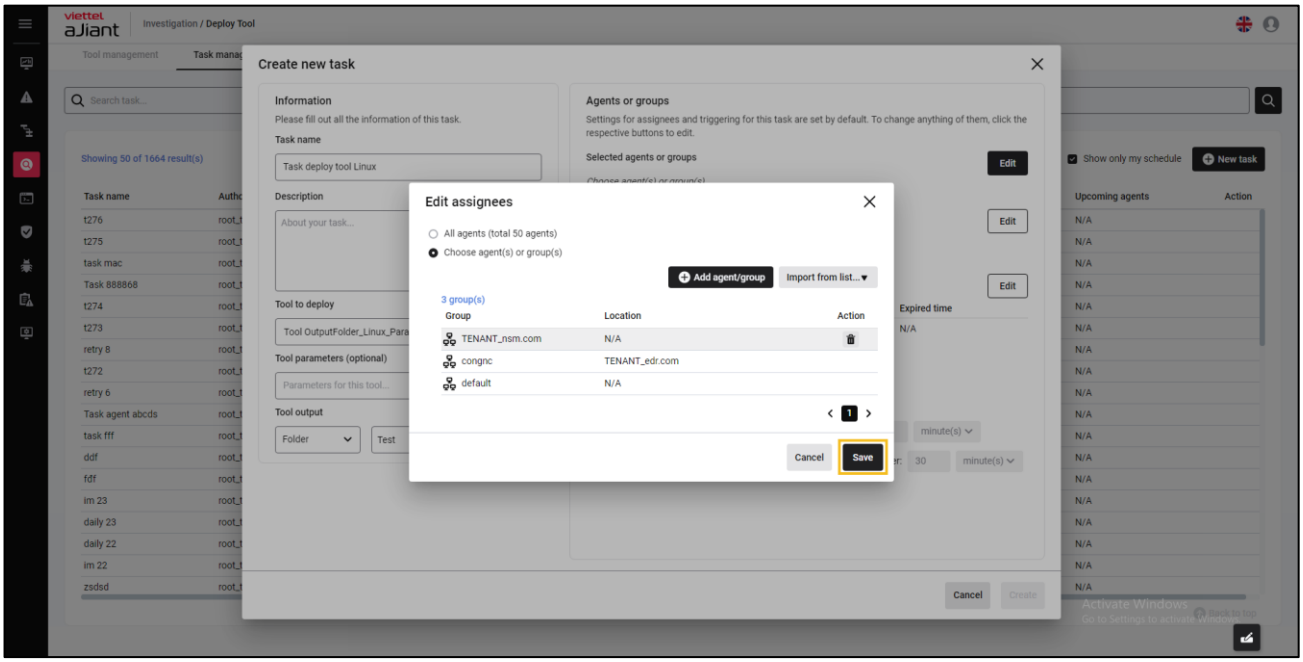
- Chọn group(s) để deploy bằng cách tích chọn vào một hoặc nhiều group(s) > Thông tin group(s) đã được chọn hiển thị ở khung **Selected** > chọn **Cancel** để hủy thao tác thêm group(s) để deploy hoặc chọn nút **Save** để xác nhận danh sách group(s):



  - Hover vào các group(s) đã chọn > Chọn icon  để thực hiện loại bỏ group(s) khỏi danh sách đã chọn



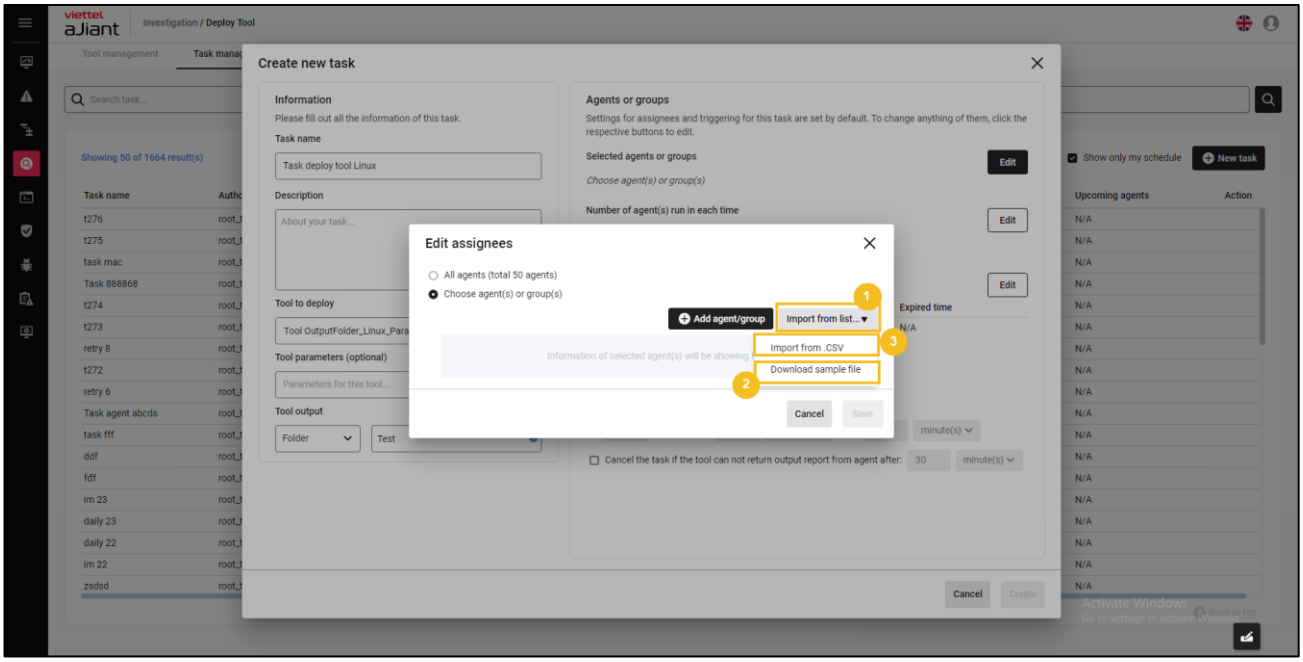
- Chọn **Cancel** để hủy hoặc Chọn **Save** các group(s) đã chọn để deploy:



+ Import from list: Cho phép upload danh sách agent(s) từ file .csv > Chọn **Import from list**

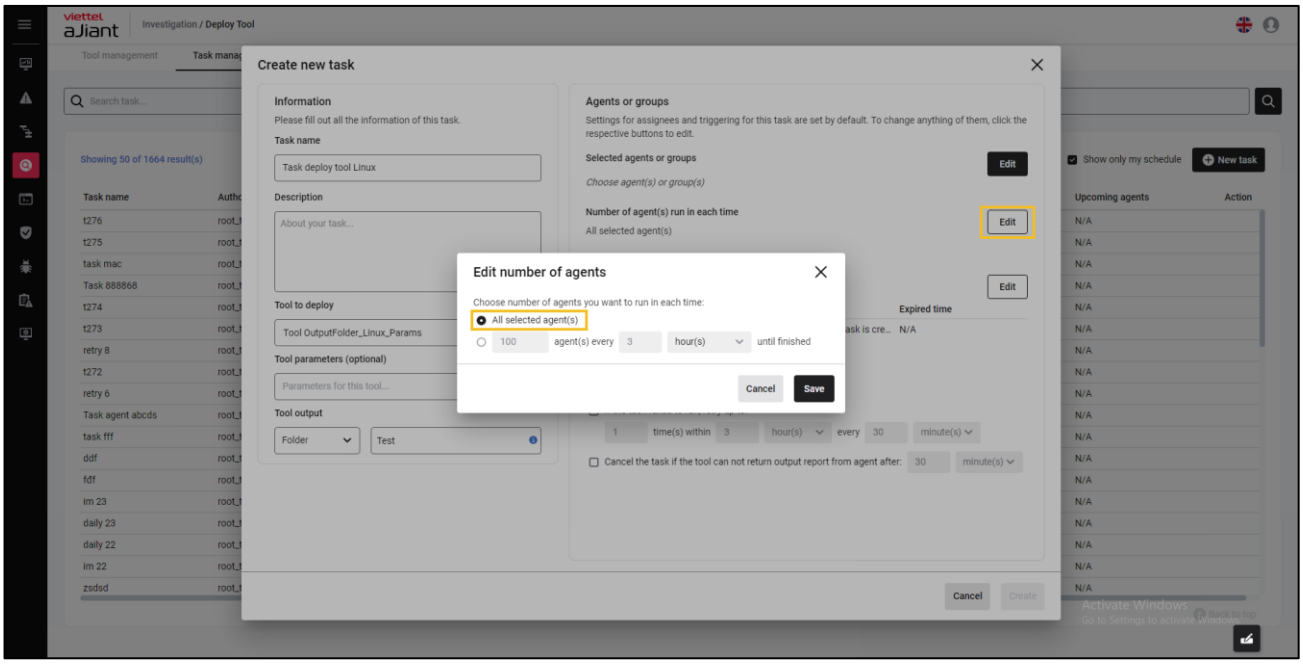
- Chọn **Download sample file** để lấy form danh sách file agent(s) mẫu;

- Nhập thông tin agent(s) > chọn **Import from .CSV** để thực hiện tải lên danh sách agent(s)

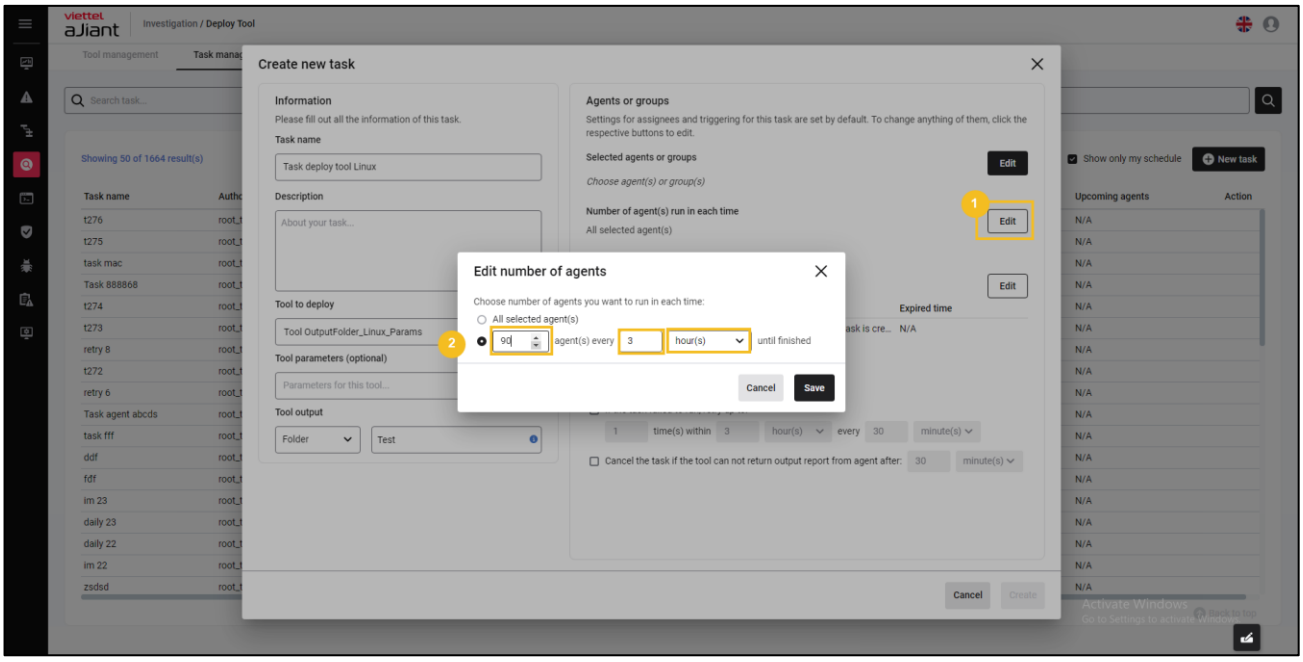


Bước 4: Cấu hình số lượng agent deploy tool mỗi lần:

+ All Agent: Cho phép deploy toàn bộ agent(s) người dùng đã chọn

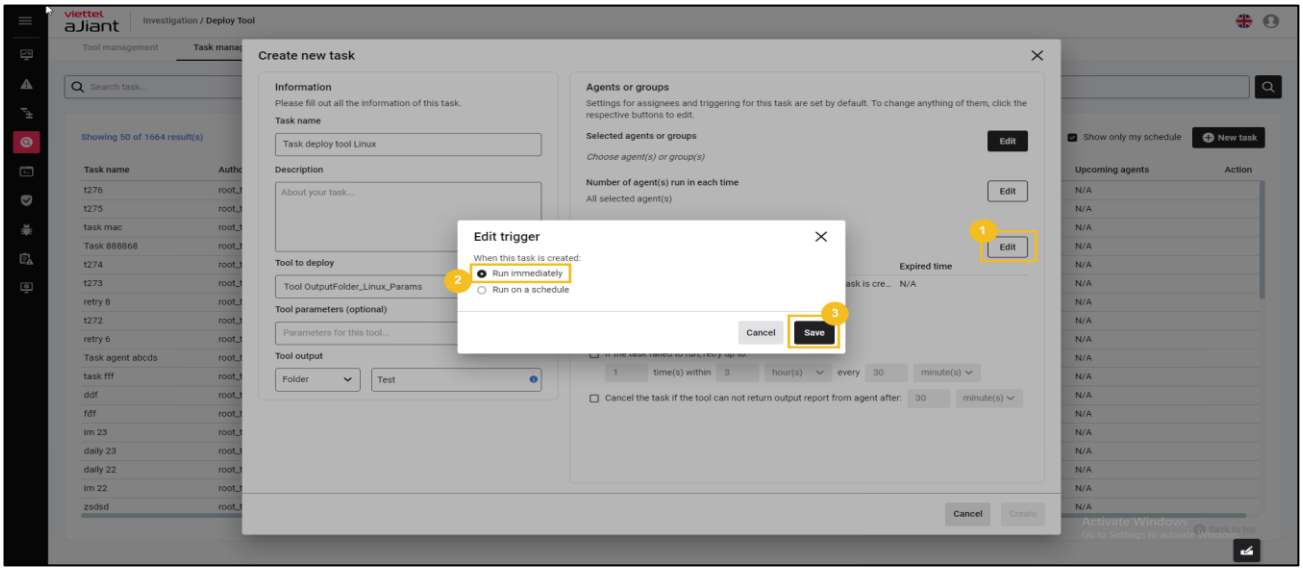


+ Cấu hình số lượng agent mỗi lần deploy:



Bước 5: Cấu hình thông tin thời gian (lập lịch) thực hiện deploy tool:

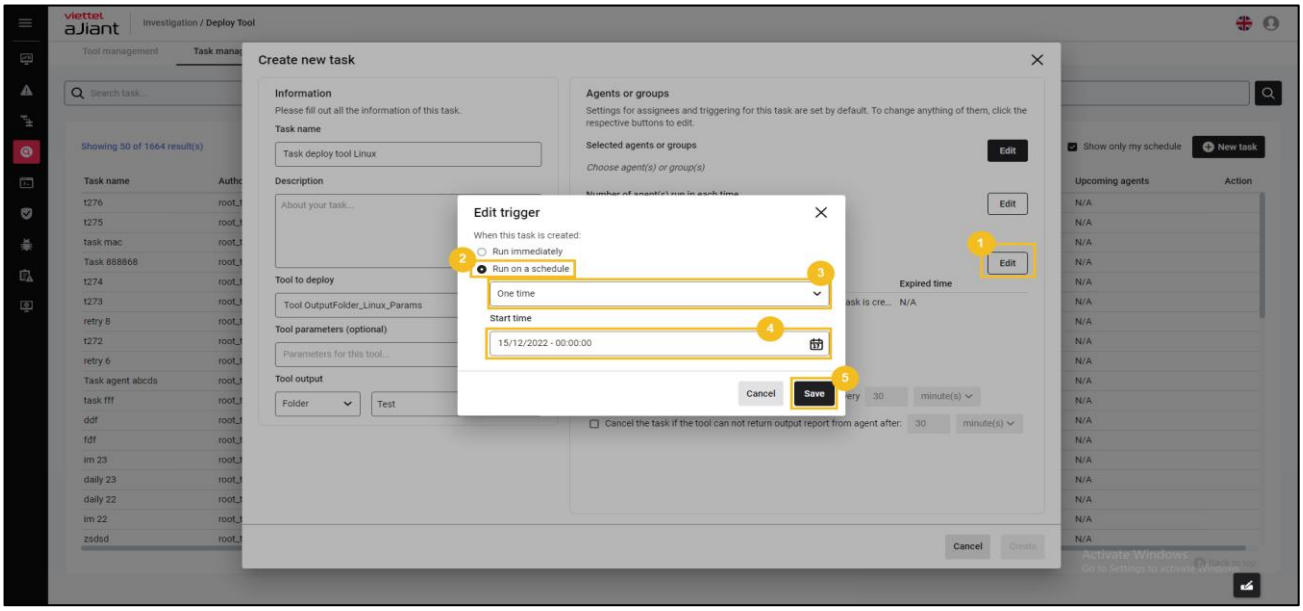
+ Chọn **Run immediately** để thực hiện cấu hình thời gian deploy tool **ngay lập tức** (sau khi tạo task thành công)



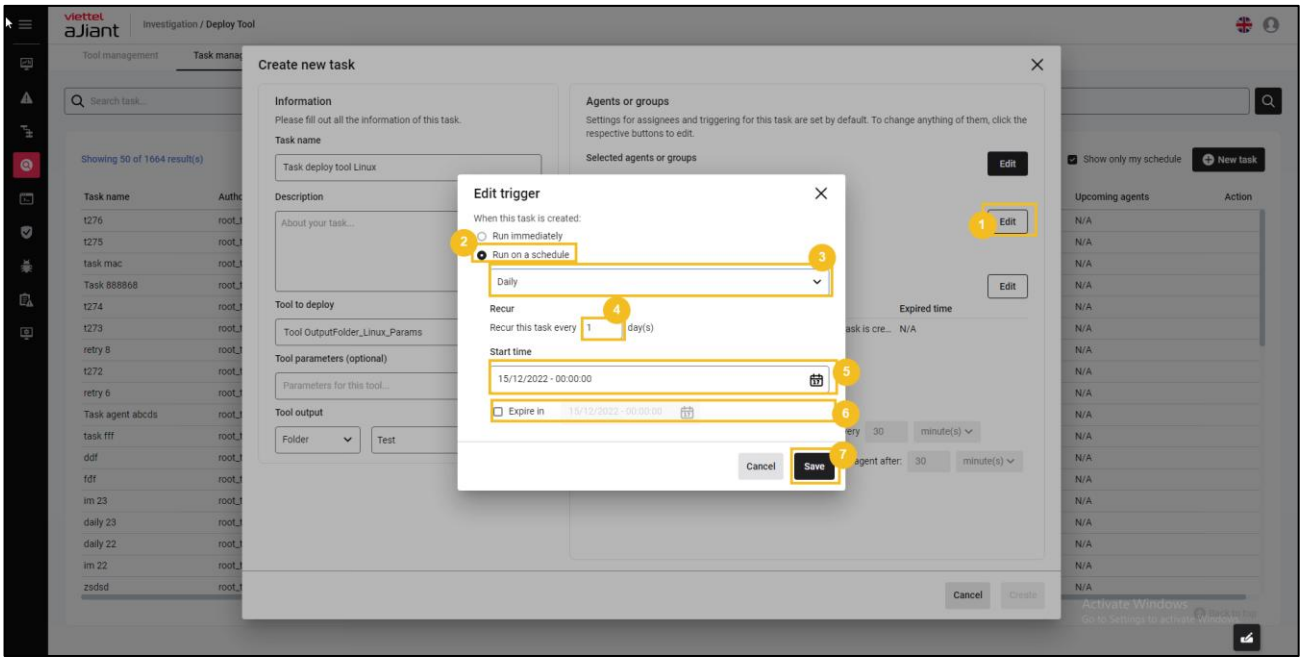
+ Chọn **Run on schedule** để thực hiện cấu hình thời gian deploy tool theo lập lịch:

  - Chọn schedule **One time**:

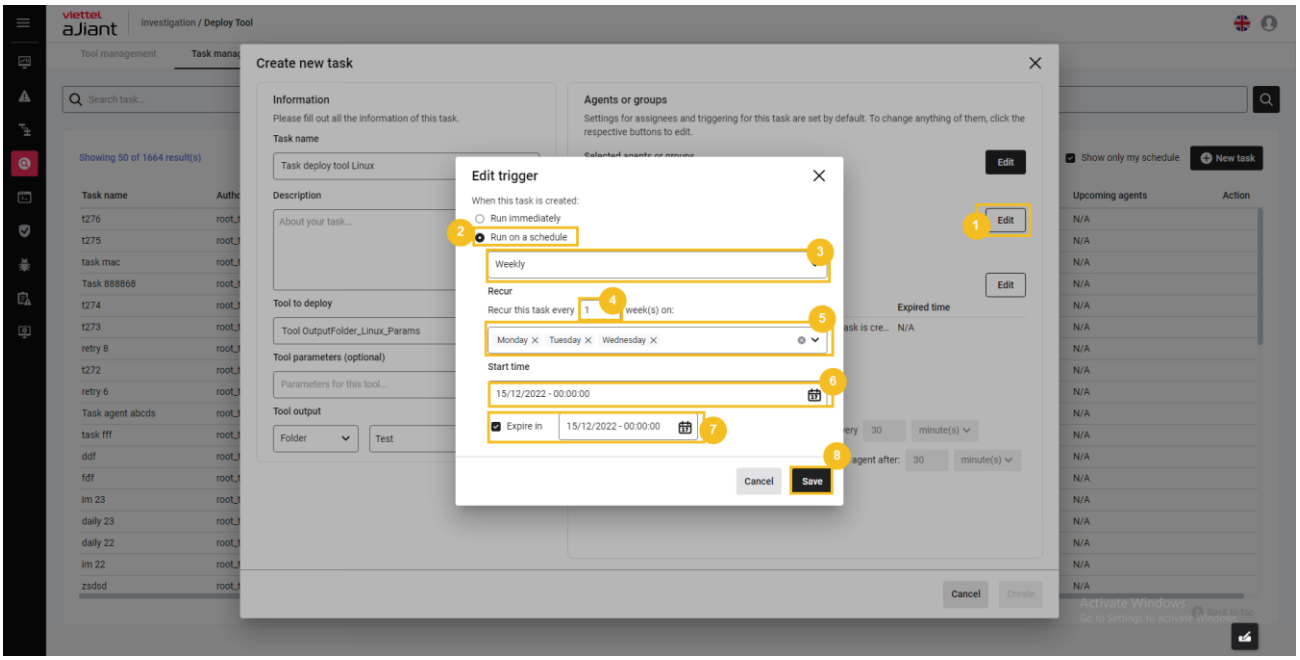
- Cho phép lập lịch deploy tool một lần;
- Cấu hình thời gian bắt đầu:



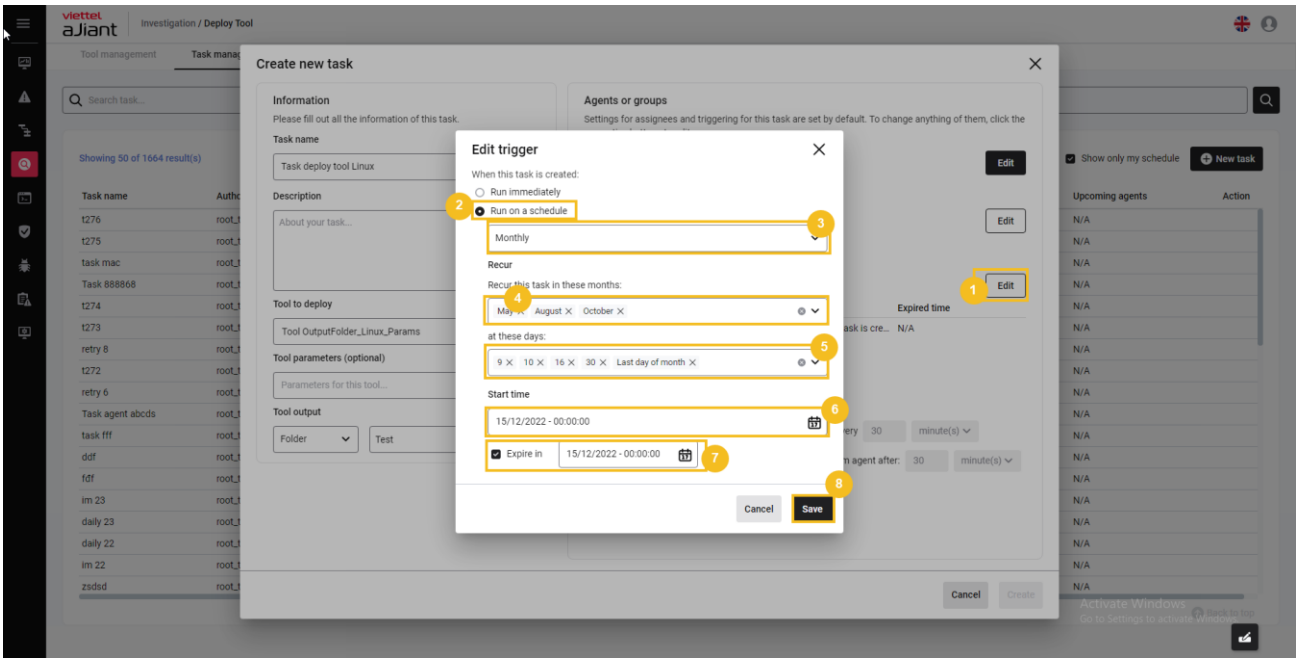
- Chọn schedule **Daily**:
  - Cho phép lập lịch deploy tool hàng ngày;
  - Thời gian lặp lại;
  - Cấu hình thời gian bắt đầu và kết thúc:



- Chọn schedule **Weekly**:
  - Cho phép lập lịch deploy tool hàng tuần;
  - Thời gian lặp lại;
  - Cấu hình thời gian bắt đầu và kết thúc:



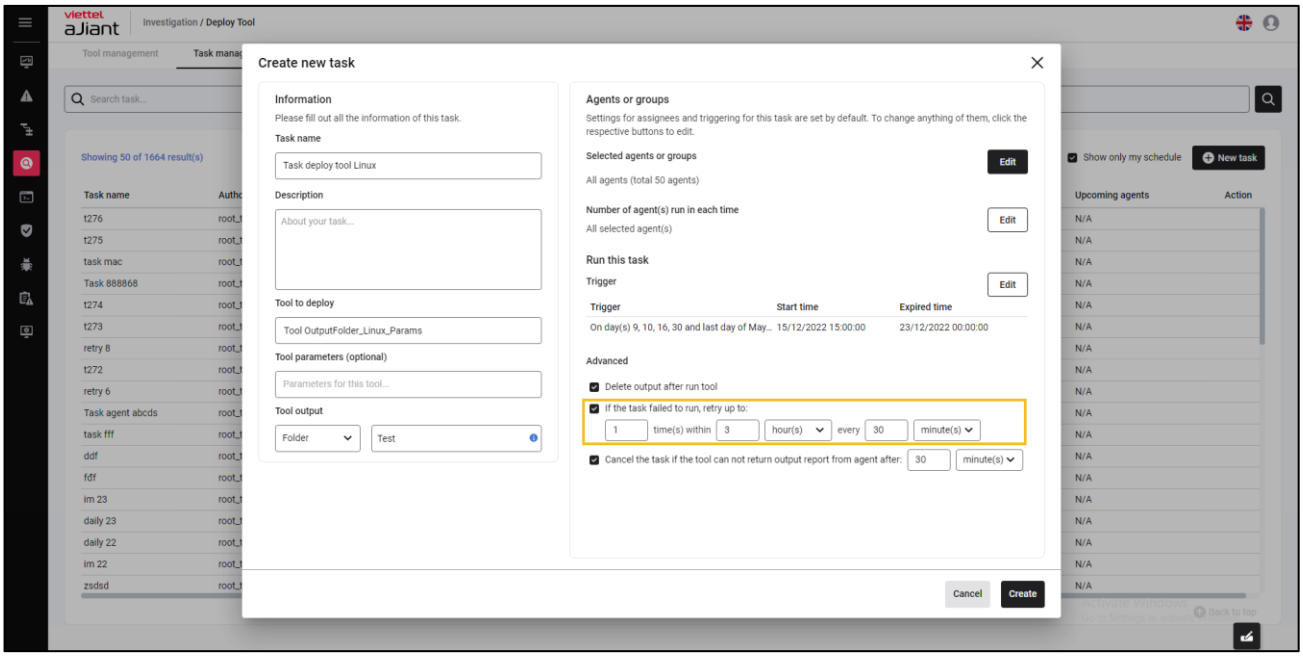
- Chọn schedule **Monthly**:
  - Cho phép lập lịch deploy tool hàng tháng;
  - Thời gian lặp lại;
  - Cấu hình thời gian bắt đầu và kết thúc:



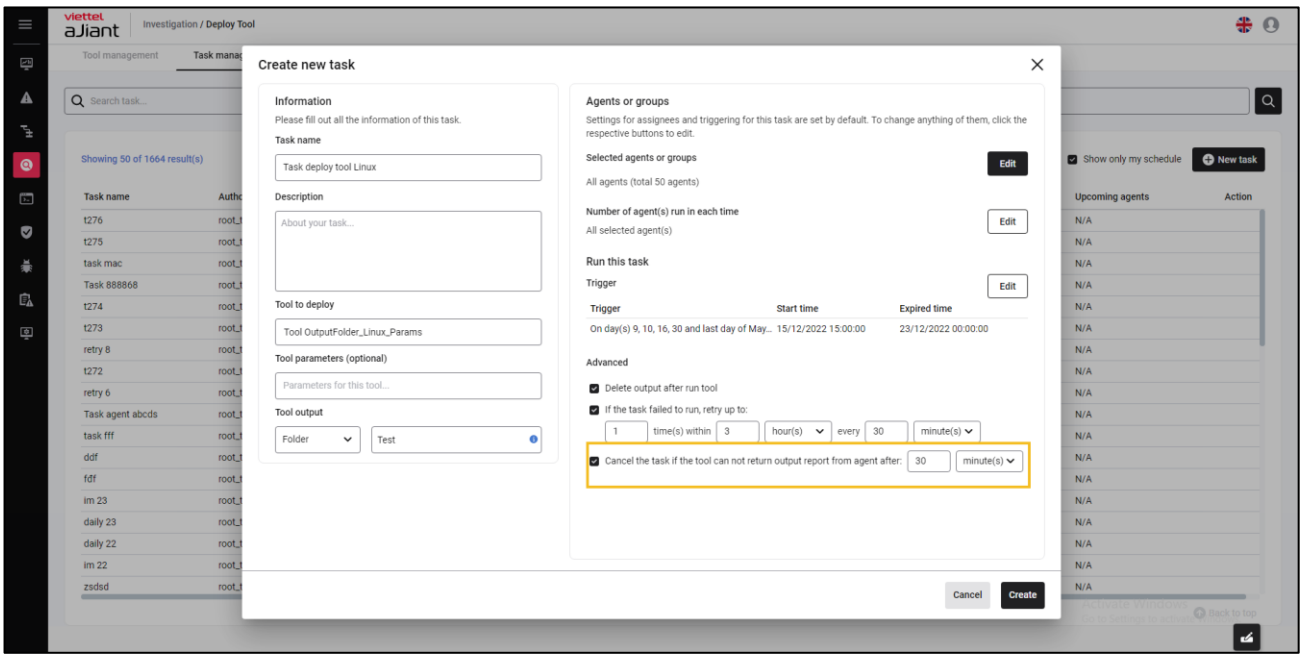
Bước 6: Cấu hình thông tin nâng cao cho task

+ **Delete tool after run tool** cho phép xóa tool output sau khi run tool và trả kết quả về BE thành công;

+ **If the task failed to run, retry upto** khi task deploy thất bại,cho phép cấu hình thông tin retry task (deploy lại task)



+ **Cancel the task if the tool can not return output report from agent after** cho phép hủy task nếu task không thể chạy sau thời gian cấu hình của người dùng:



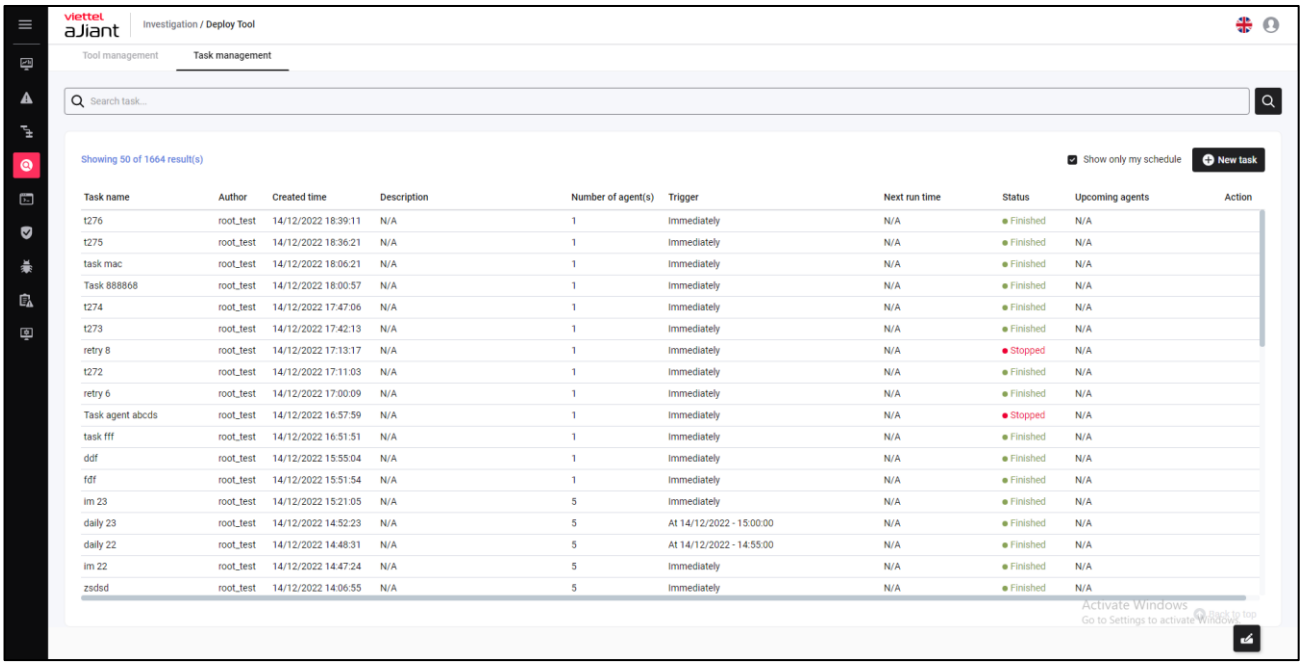
Bước 7: Chọn **Create** để tạo mới task/ cấu hình thông tin deploy tool dưới agent hoặc chọn **Cancel** để hủy task/ hủy cấu hình thông tin deploy tool dưới agent

3.4.4.3 Task management

a. Danh sách task

Mục đích: Hiển thị danh sách task lập lịch deploy tool;

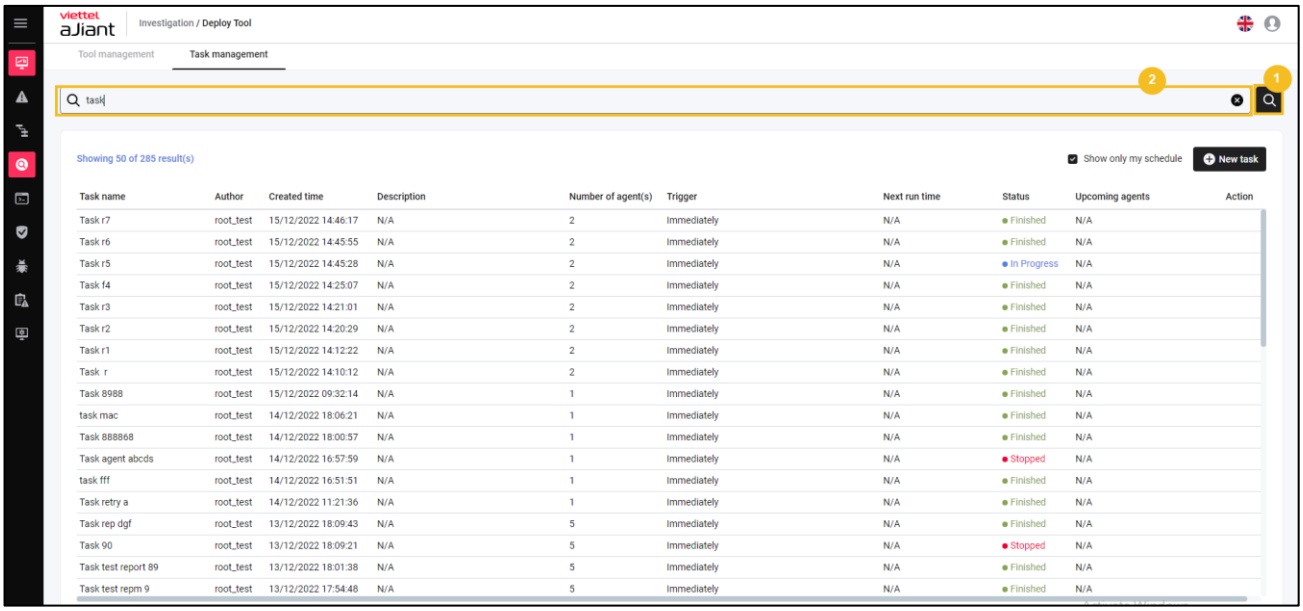
Các trường thông tin hiển thị: Task name, Author, Created time, Description, Number of agent(s), Trigger, Next run time, Status, Upcoming agents



b. Tìm kiếm task

Mục đích: Cho phép tìm kiếm task theo tên task;

Các bước thực hiện: Nhập vào từ khóa tìm kiếm > chọn nút **Search** hoặc kết thúc nhập từ khóa > nhấn enter. HT thực hiện tìm kiếm thông in Agent liên quan đến từ khóa tìm kiếm có trong hệ thống:



c. Tạo task

(Chức năng tương tự như mục 3.5.4.2. Deploy tool)

Mục đích: Cấu hình thông tin deploy tool dưới agent

Điều kiện:

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

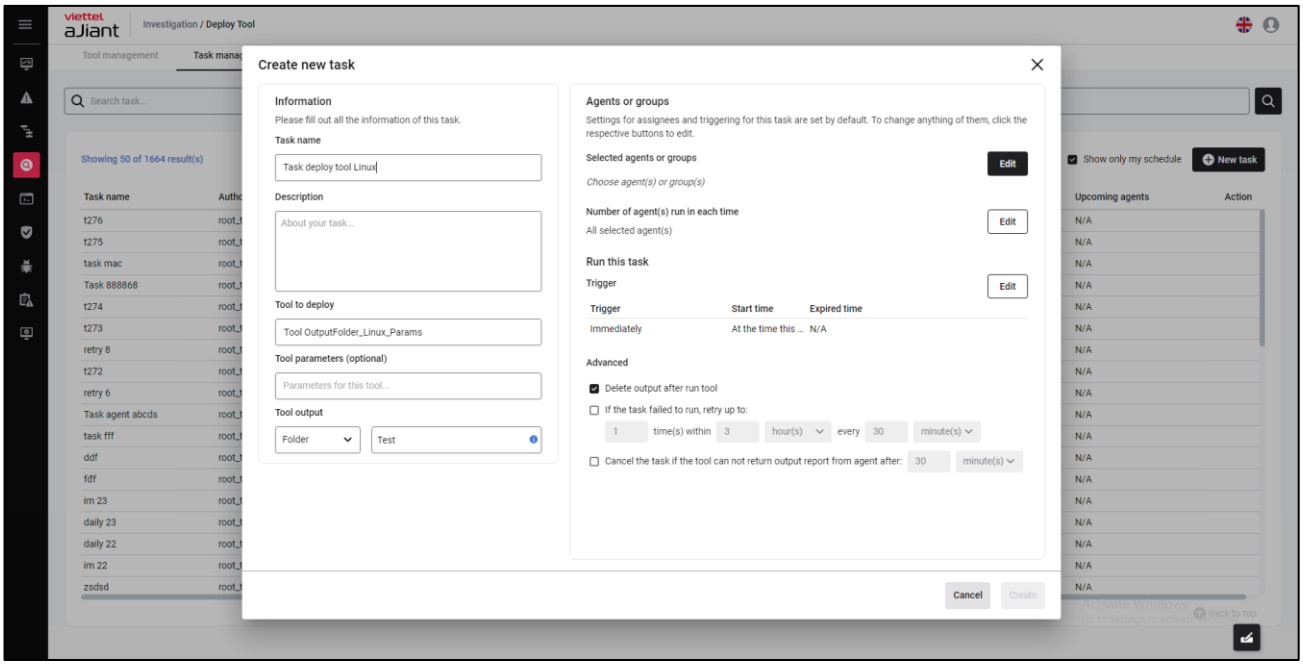
+ User đăng nhập thuộc group default: Hiển thị tất cả Agent thuộc group default;

+ 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;

Các bước thực hiện deploy tool tại tab Task management:

Bước 1: Sau khi lựa chọn tool, chọn icon [...] tại bản ghi tool cần deploy > chọn **Deploy this tool**, màn hình Create new task hiển thị:

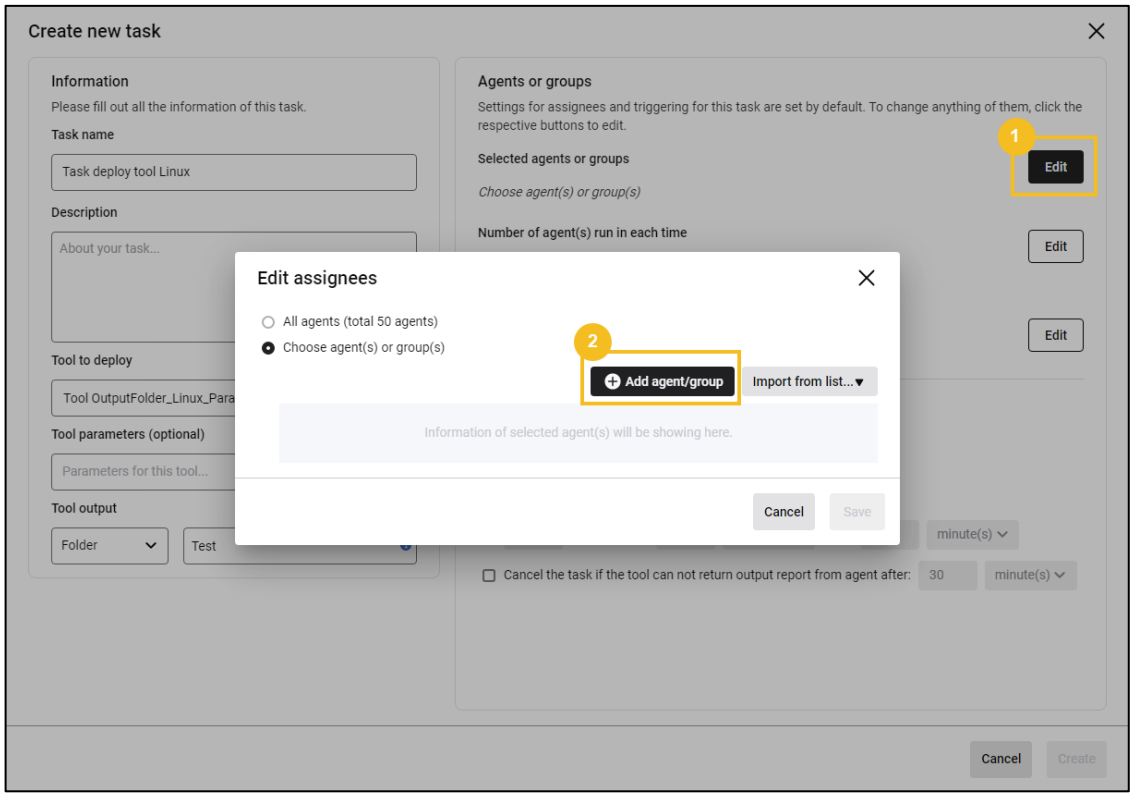


Bước 2: Thực hiện nhập các thông tin task để deploy tool: Task name, Tool to deploy, Description, Tool parameters, Tool output;

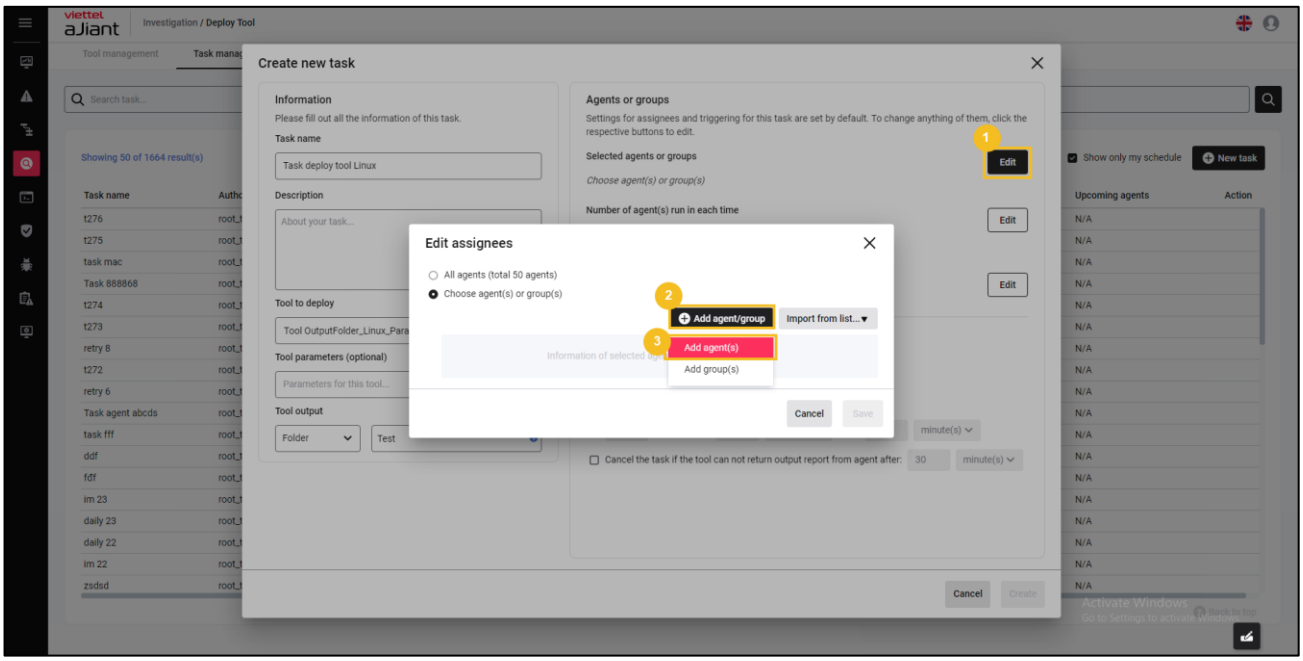
Bước 3: Lựa chọn thông tin nhóm (group), máy trạm (agent) để thực hiện deploy:

Lựa chọn **All agent(s)**: chọn tất cả các agent(s) trong phạm vi quản lý của user đang đăng nhập để thực hiện deploy;

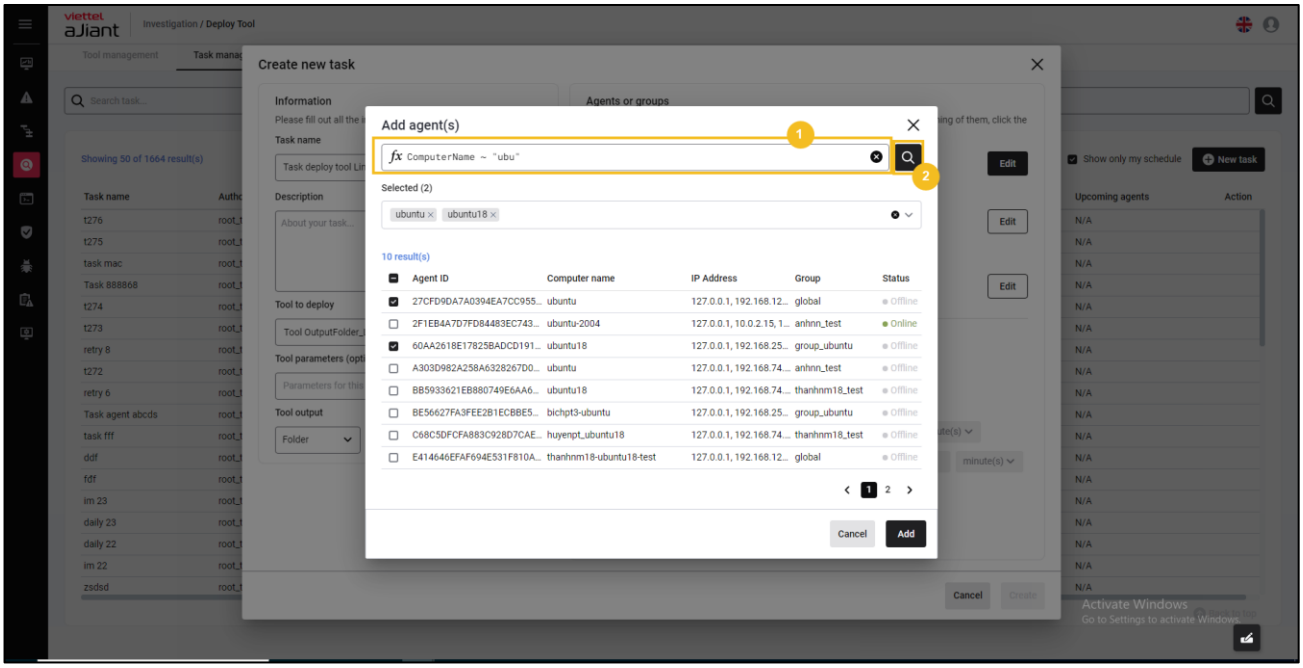
Lựa chọn agents or groups thực hiện deploy – **Choose agent(s) or group(s)**:



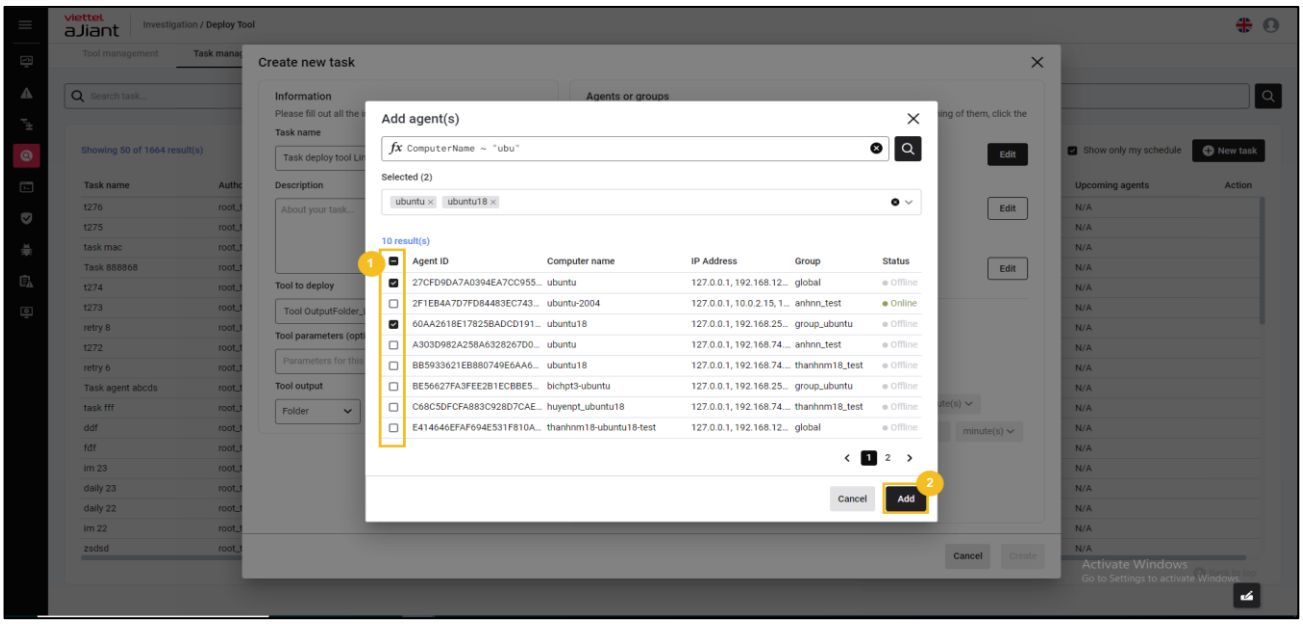
+ Chọn Add agent(s):



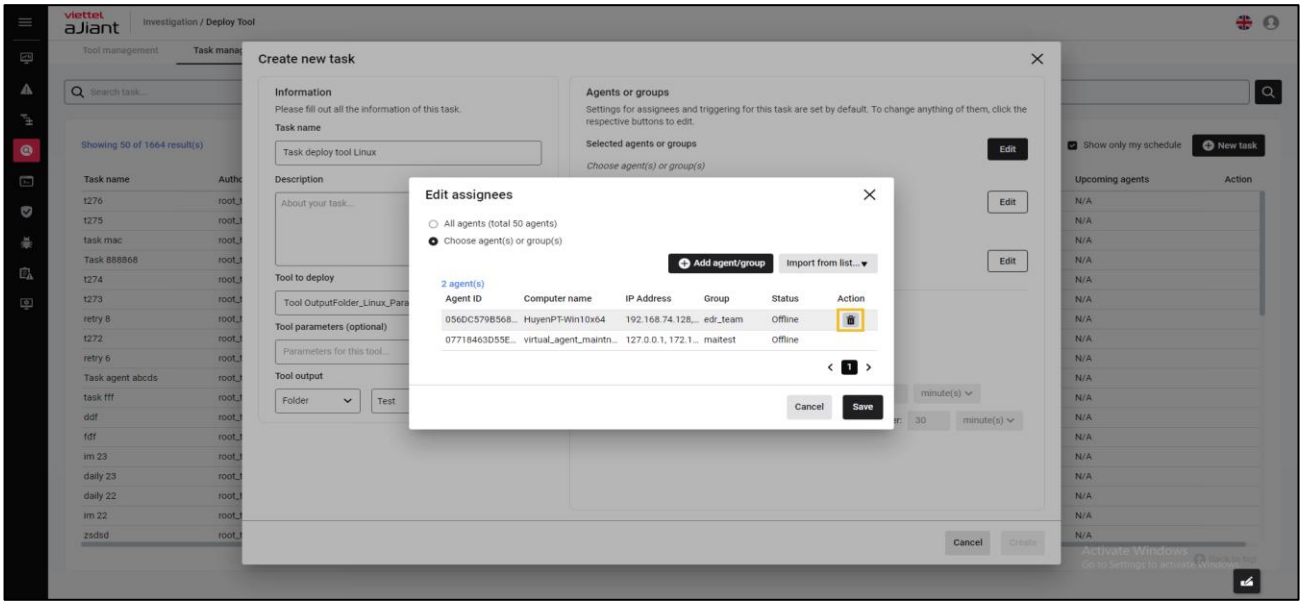
- Tìm kiếm Agent: Cho phép tạo câu lệnh truy vấn, sử dụng câu lệnh truy vấn để tìm kiếm Agent



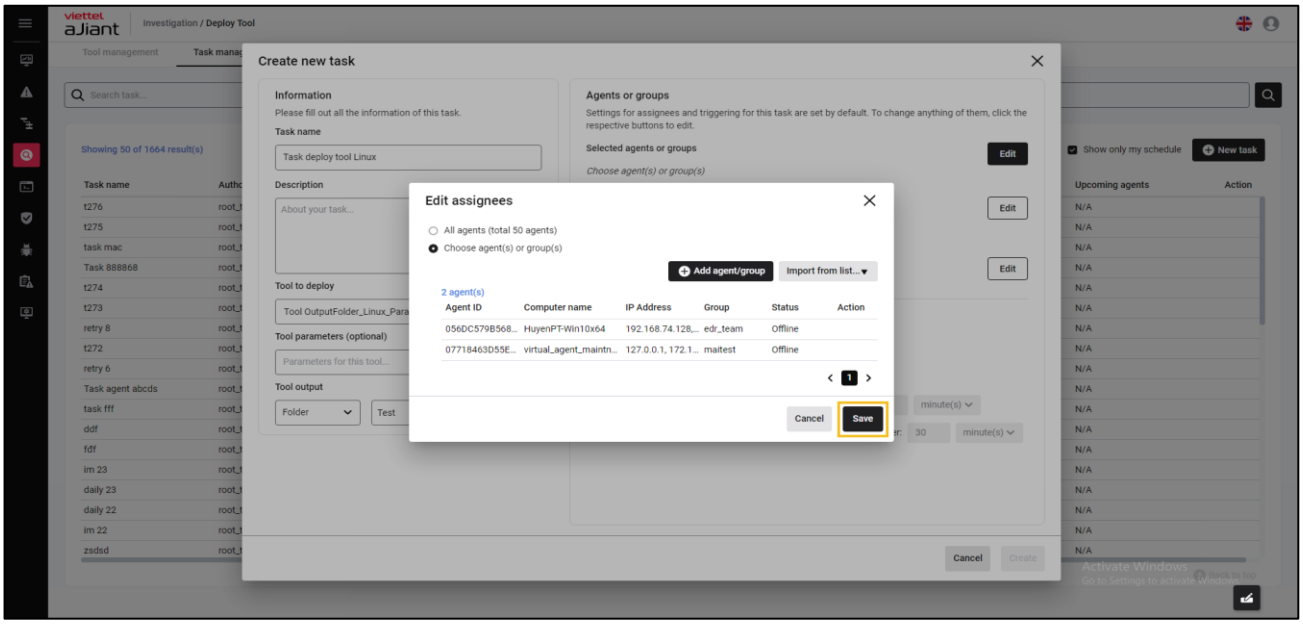
- Chọn Agent(s) để deploy bằng cách tích chọn vào một hoặc nhiều Agent(s) > Thông tin Agent(s) đã được chọn hiển thị ở khung **Selected** > chọn **Cancel** để hủy thao tác thêm Agent để deploy hoặc chọn nút **Add** để xác nhận danh sách Agent(s):



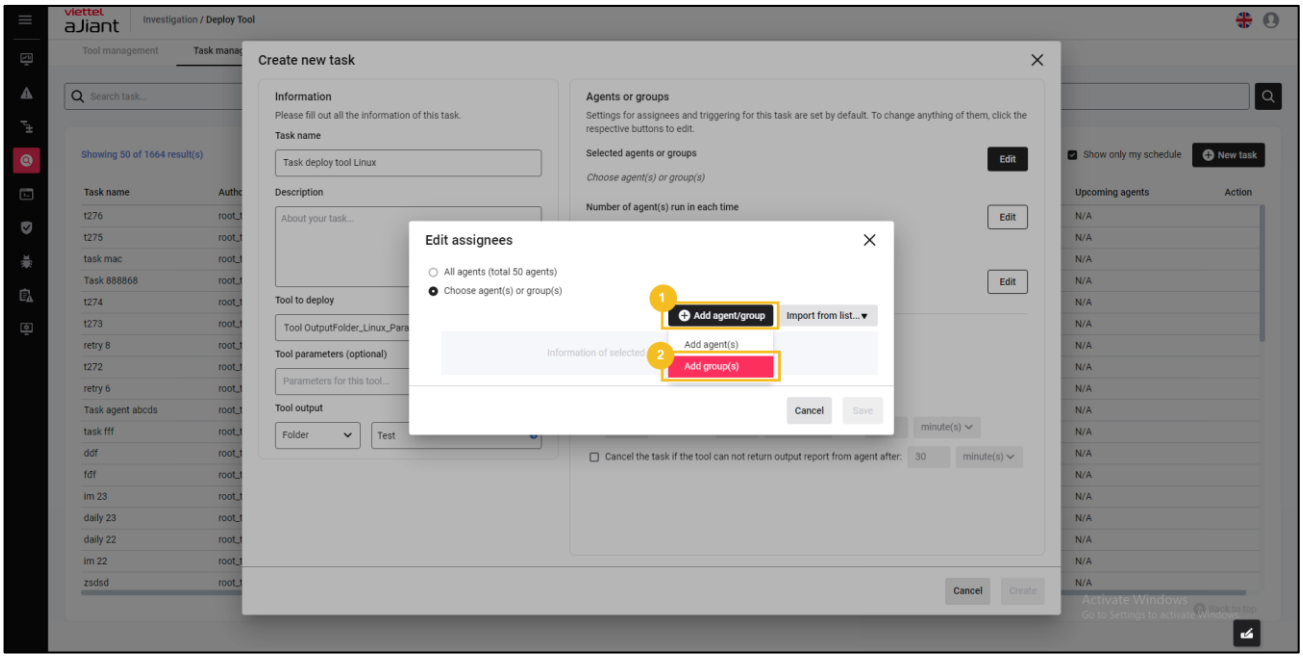
- Hover vào các Agent(s) đã chọn > Chọn icon  để thực hiện loại bỏ Agent(s) khỏi danh sách đã chọn:



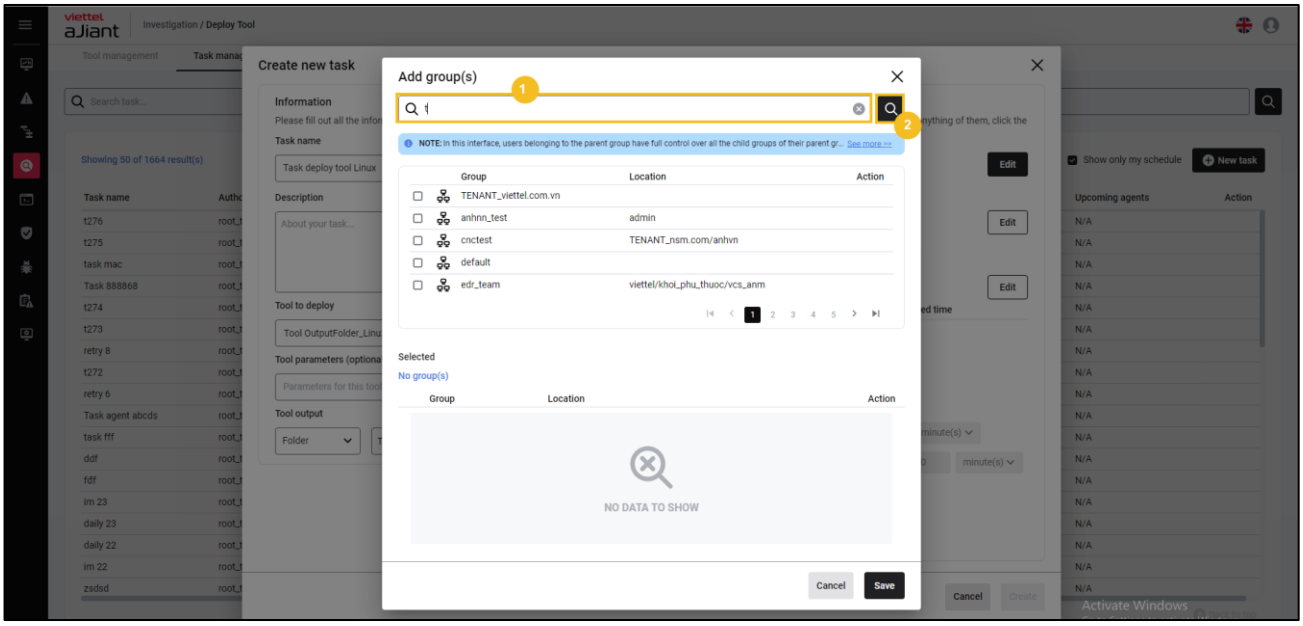
- Chọn **Cancel** để hủy hoặc chọn **Save** để lưu thông tin các Agent(s) đã chọn để deploy:



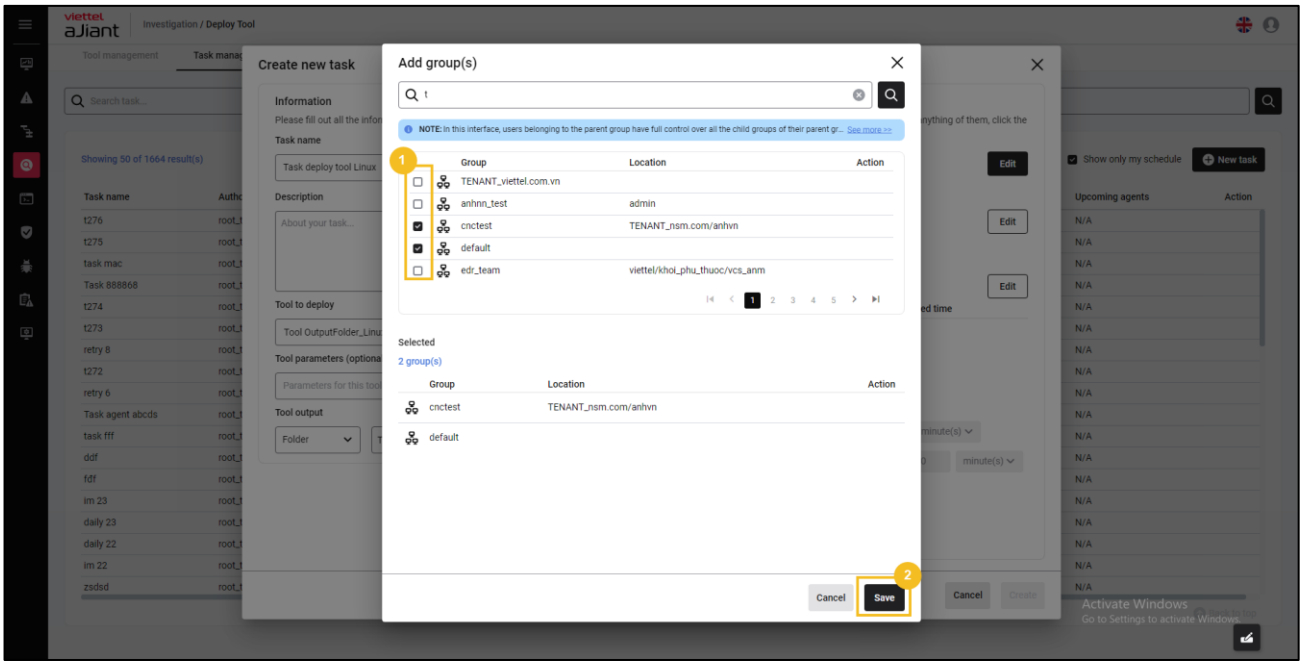
+ Chọn Add group(s):



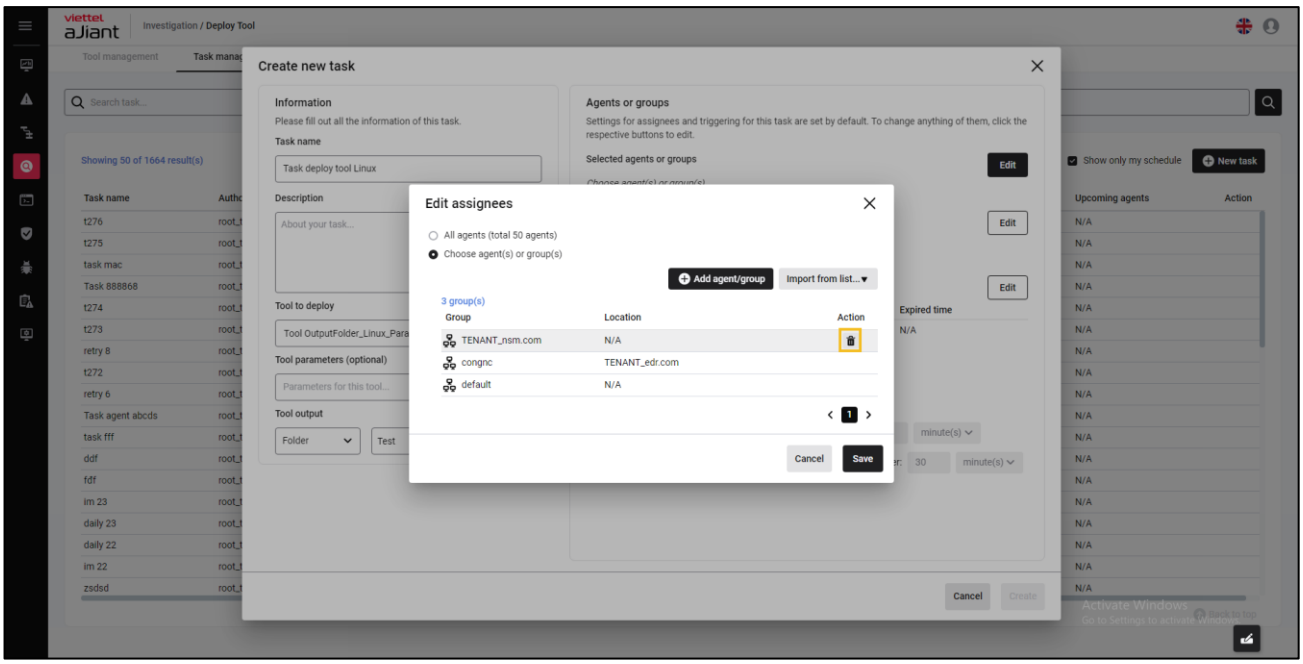
- Tìm kiếm group(s) theo tên, cho phép nhập từ khóa tìm kiếm group theo tên group:



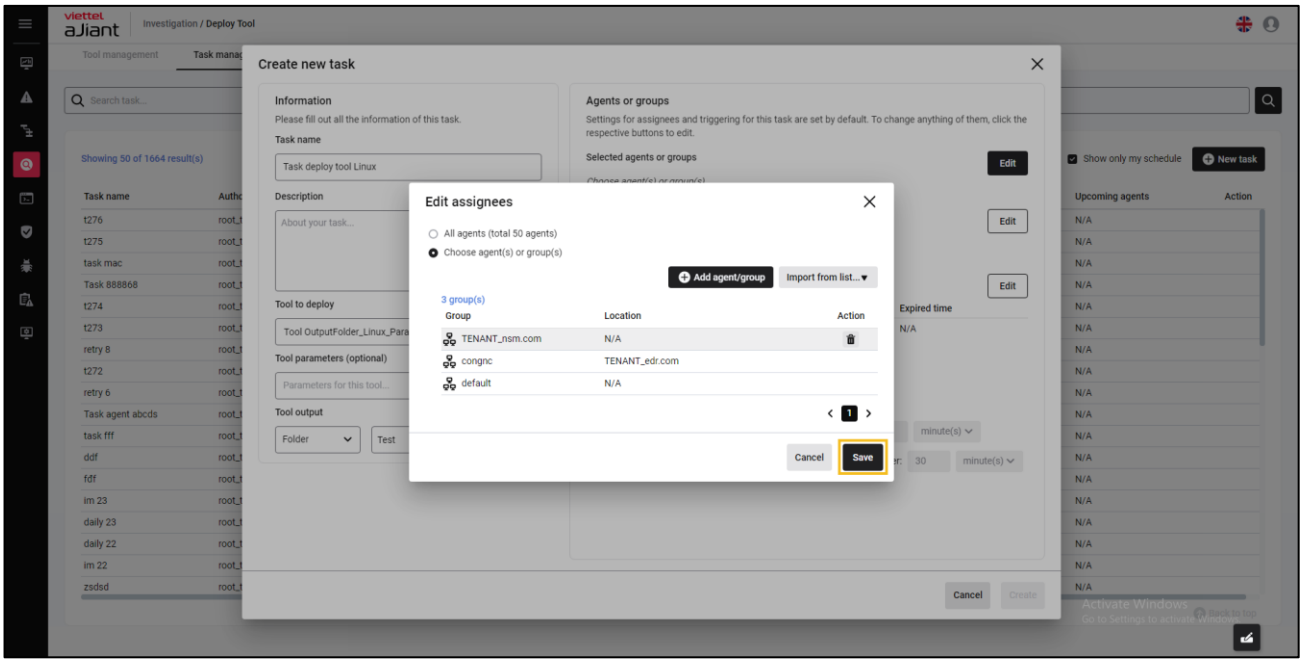
- Chọn group(s) để deploy bằng cách tích chọn vào một hoặc nhiều group(s) > Thông tin group(s) đã được chọn hiển thị ở khung **Selected** > chọn **Cancel** để hủy thao tác thêm group(s) để deploy hoặc chọn nút **Save** để xác nhận danh sách group(s):



- Hover vào các group(s) đã chọn > Chọn icon  để thực hiện loại bỏ group(s) khỏi danh sách đã chọn

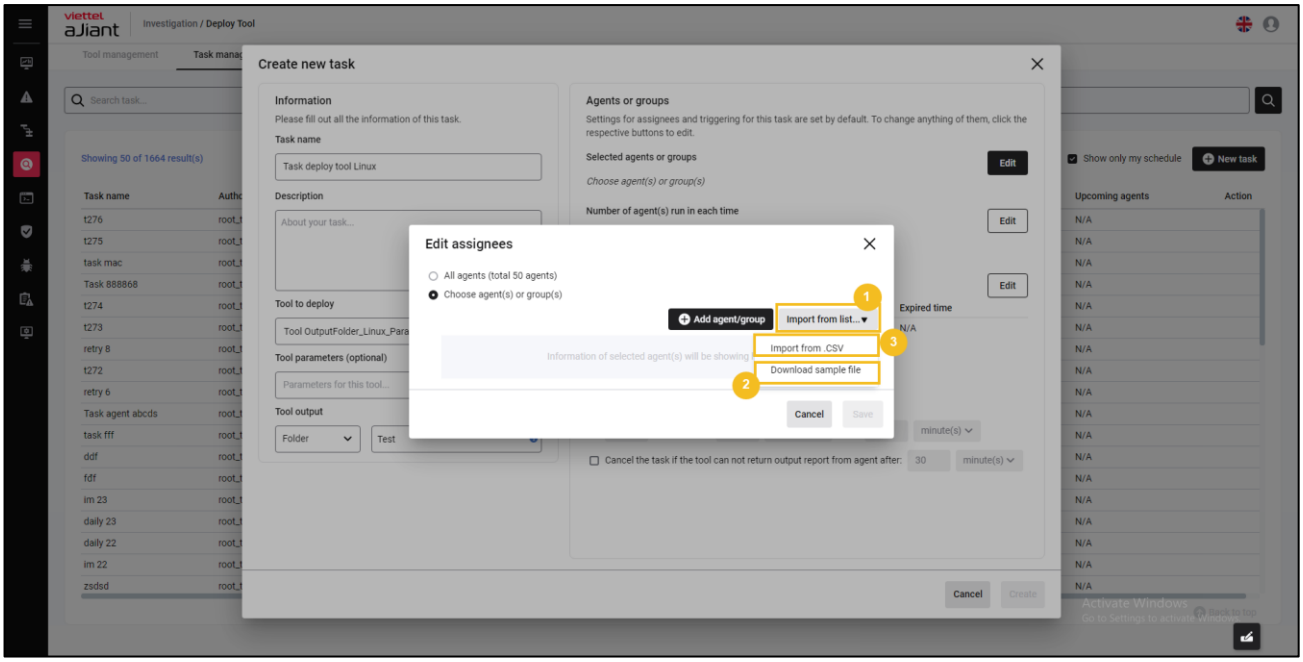


- Chọn **Cancel** để hủy hoặc Chọn **Save** các group(s) đã chọn để deploy:



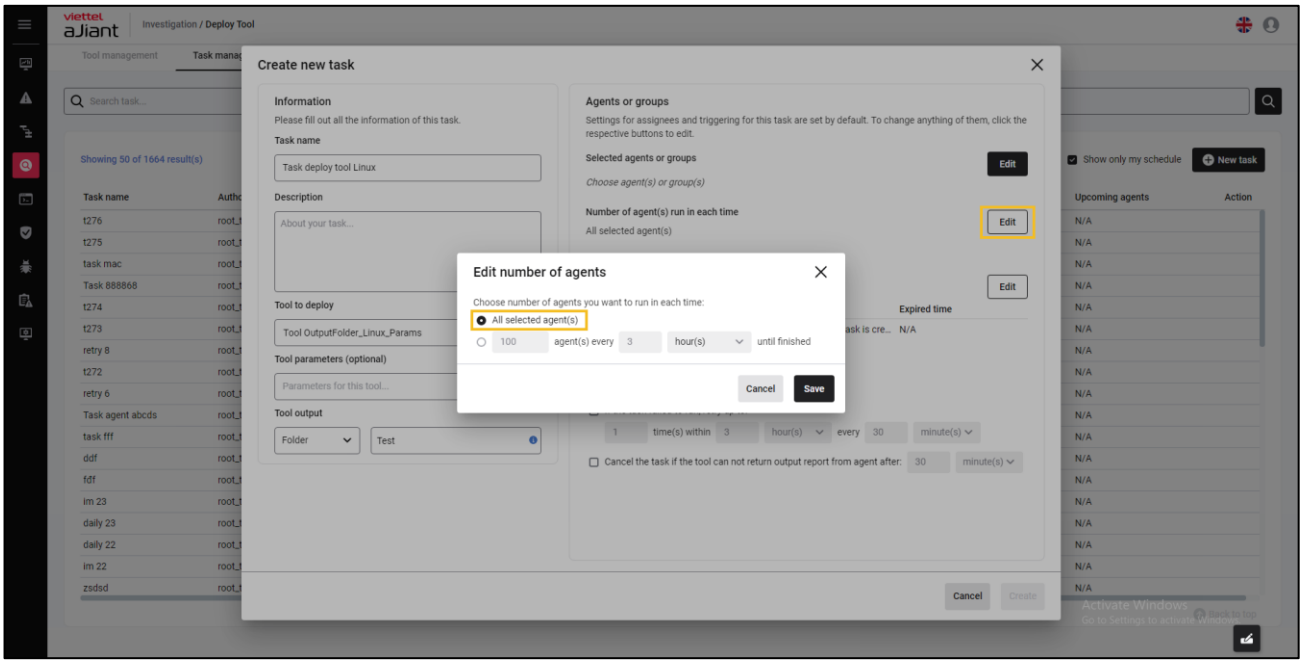
+ Import from list: Cho phép upload danh sách agent(s) từ file .csv > Chọn **Import from list**

- Chọn **Download sample file** để lấy form danh sách file agent(s) mẫu;
- Nhập thông tin agent(s) > chọn **Import from .CSV** để thực hiện tải lên danh sách agent(s)

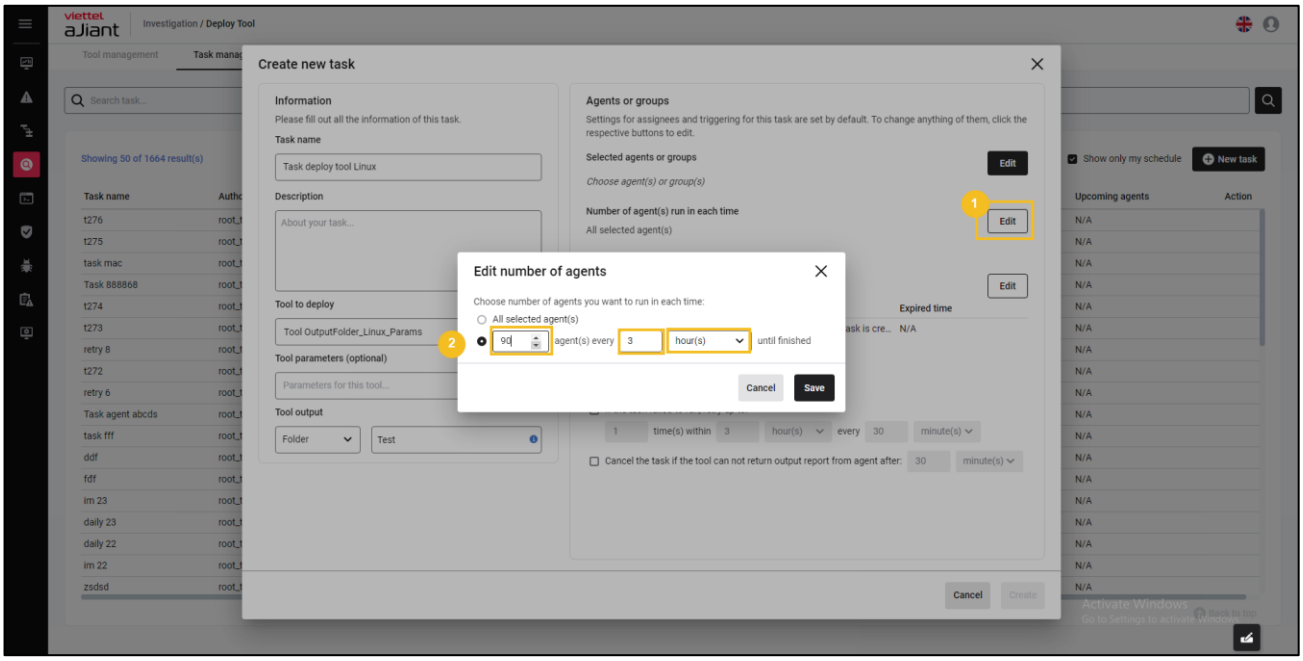


Bước 4: Cấu hình số lượng agent deploy tool mỗi lần:

+ All Agent: Cho phép deploy toàn bộ agent(s) người dùng đã chọn

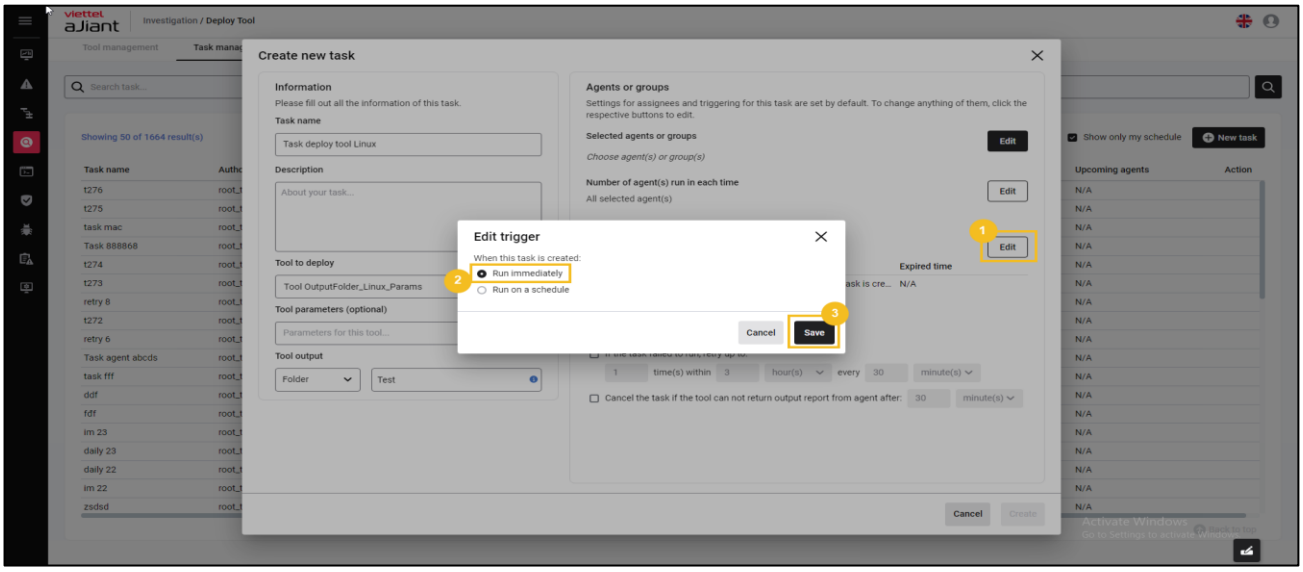


+ Cấu hình số lượng agent mỗi lần deploy:



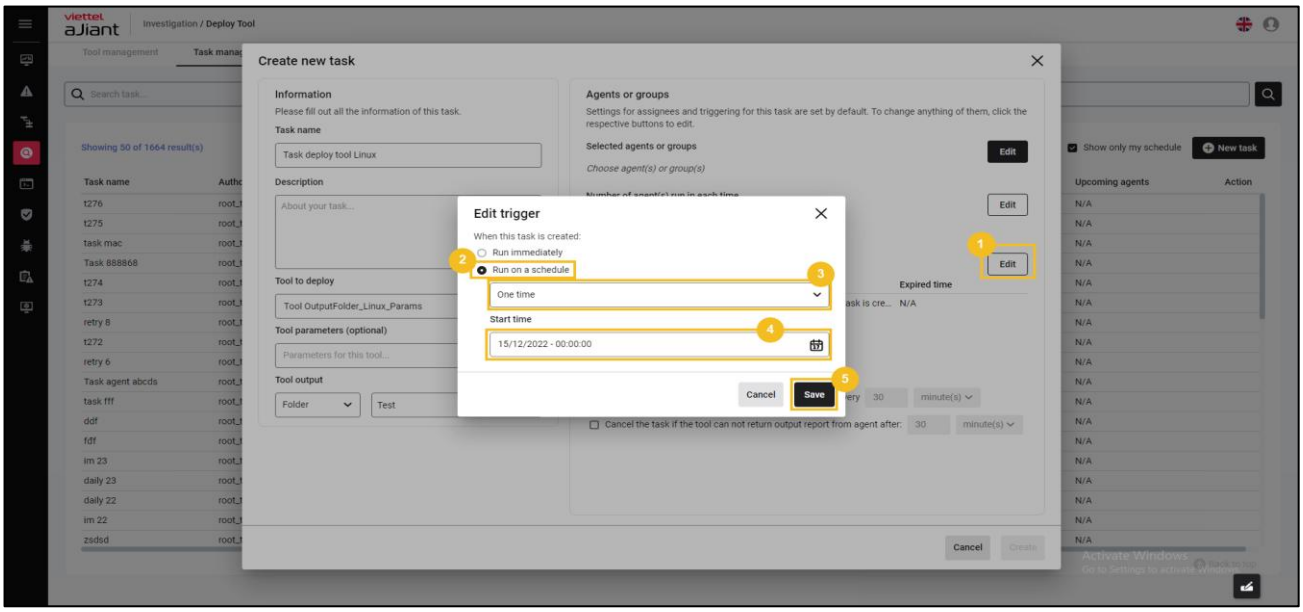
Bước 5: Cấu hình thông tin thời gian (lập lịch) thực hiện deploy tool:

+ Chọn **Run immediately** để thực hiện cấu hình thời gian deploy tool **ngay lập tức** (sau khi tạo task thành công)

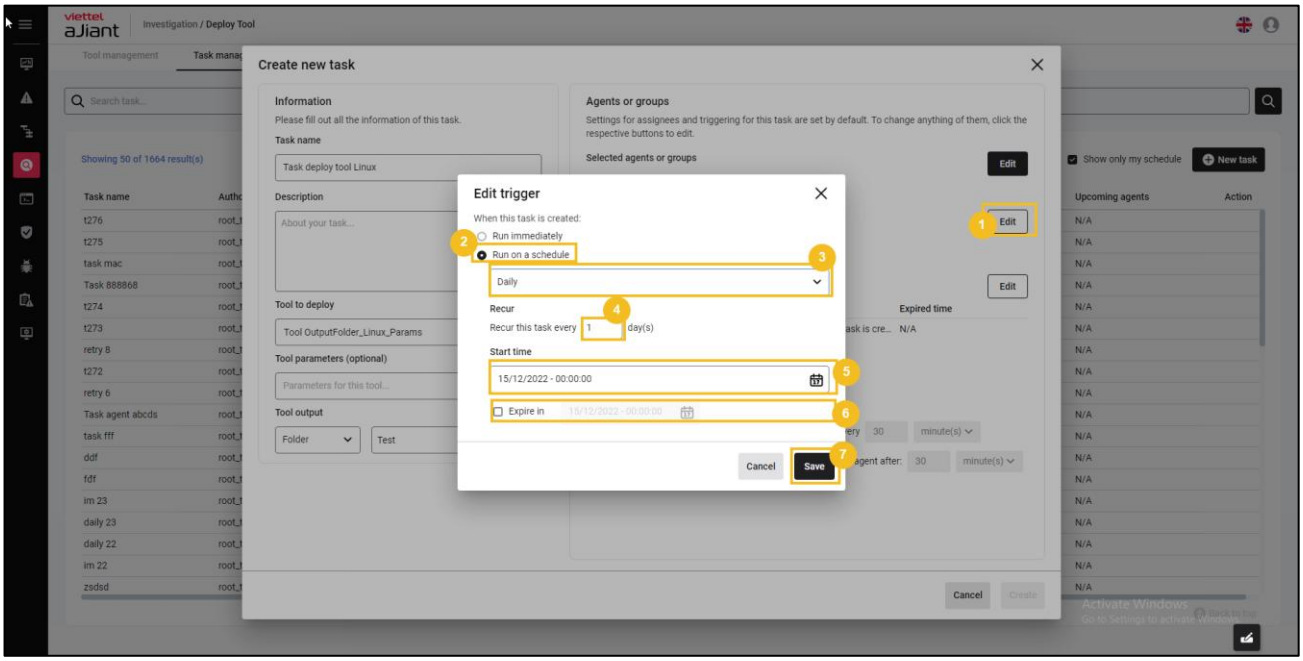


+ Chọn **Run on schedule** để thực hiện cấu hình thời gian deploy tool theo lập lịch:

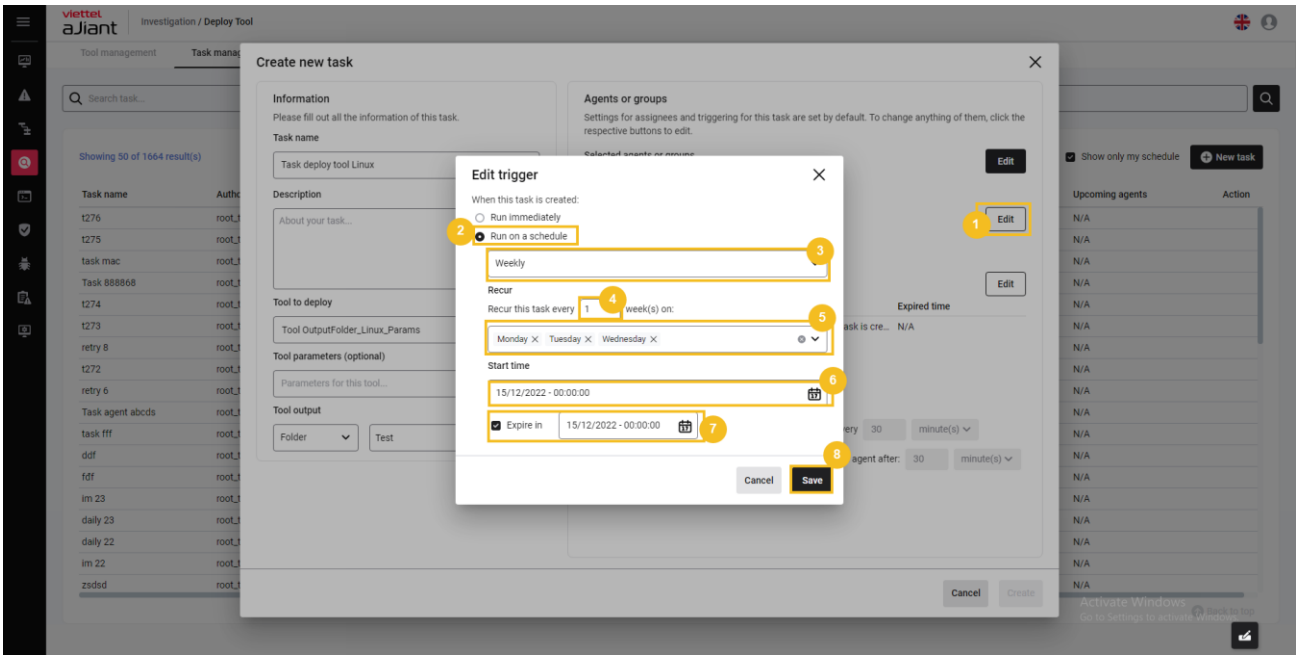
- Chọn schedule **One time**:
  - Cho phép lập lịch deploy tool một lần;
  - Cấu hình thời gian bắt đầu:



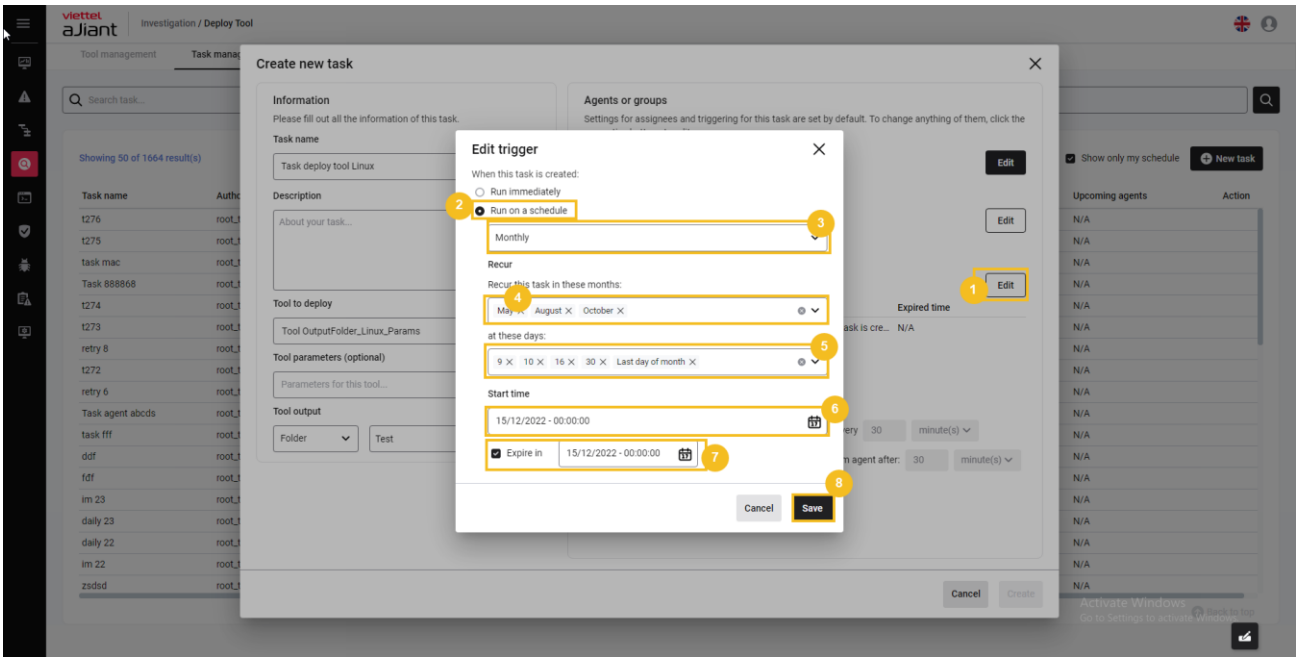
- Chọn schedule **Daily**:
  - Cho phép lập lịch deploy tool hàng ngày;
  - Thời gian lặp lại;
  - Cấu hình thời gian bắt đầu và kết thúc:



- Chọn schedule **Weekly**:
  - Cho phép lập lịch deploy tool hàng tuần;
  - Thời gian lặp lại;
  - Cấu hình thời gian bắt đầu và kết thúc:



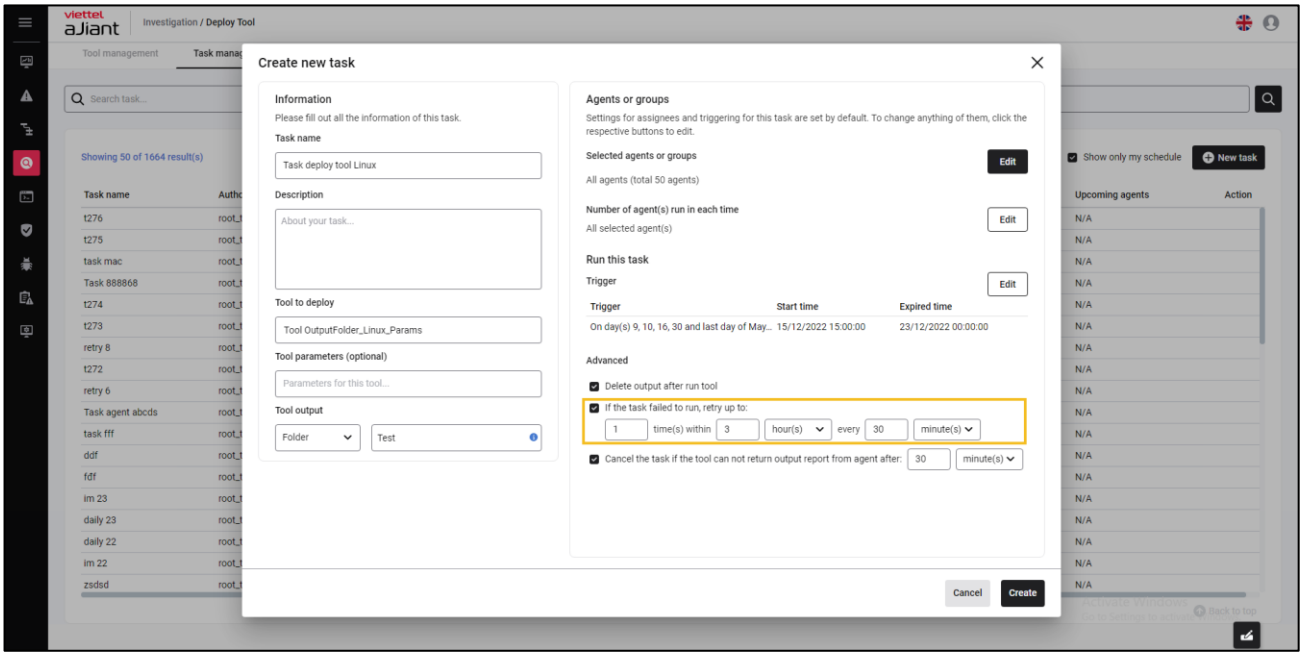
- Chọn schedule **Monthly**:
  - Cho phép lập lịch deploy tool hàng tháng;
  - Thời gian lặp lại;
  - Cấu hình thời gian bắt đầu và kết thúc:



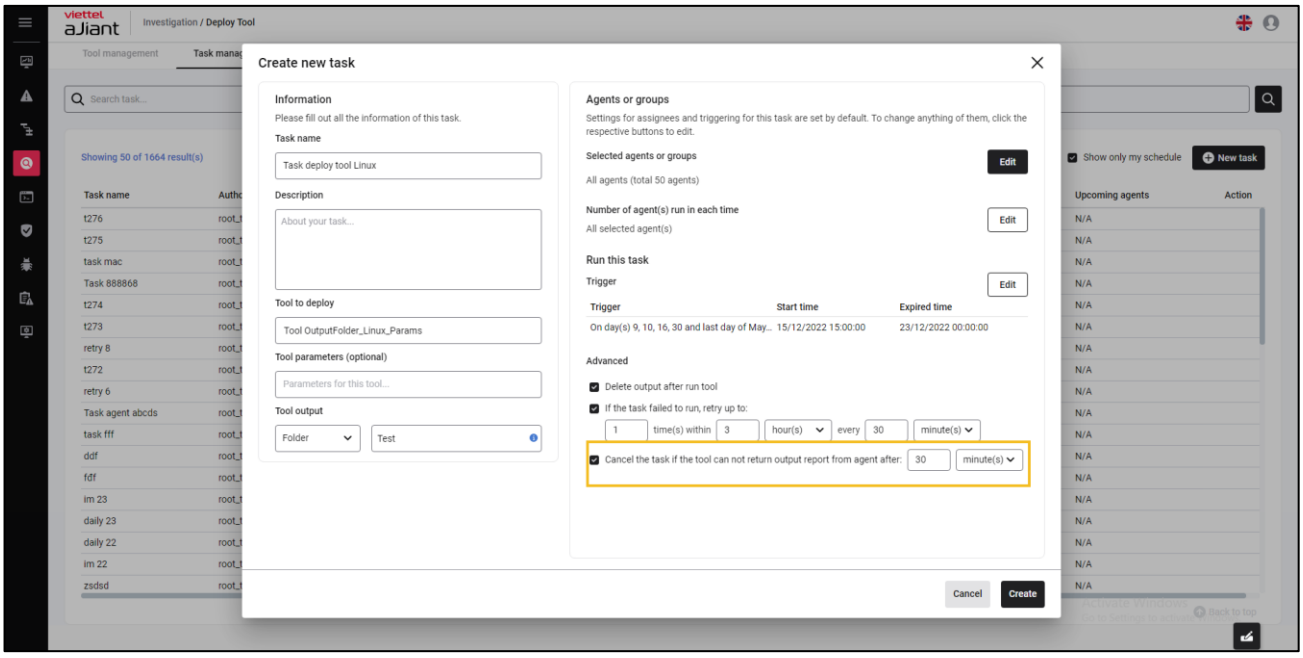
Bước 6: Cấu hình thông tin nâng cao cho task

+ **Delete tool after run tool** cho phép xóa tool output sau khi run tool và trả kết quả về BE thành công;

+ **If the task failed to run, retry upto** khi task deploy thất bại,cho phép cấu hình thông tin retry task (deploy lại task)



+ **Cancel the task if the tool can not return output report from agent after** cho phép hủy task nếu task không thể chạy sau thời gian cấu hình của người dùng:



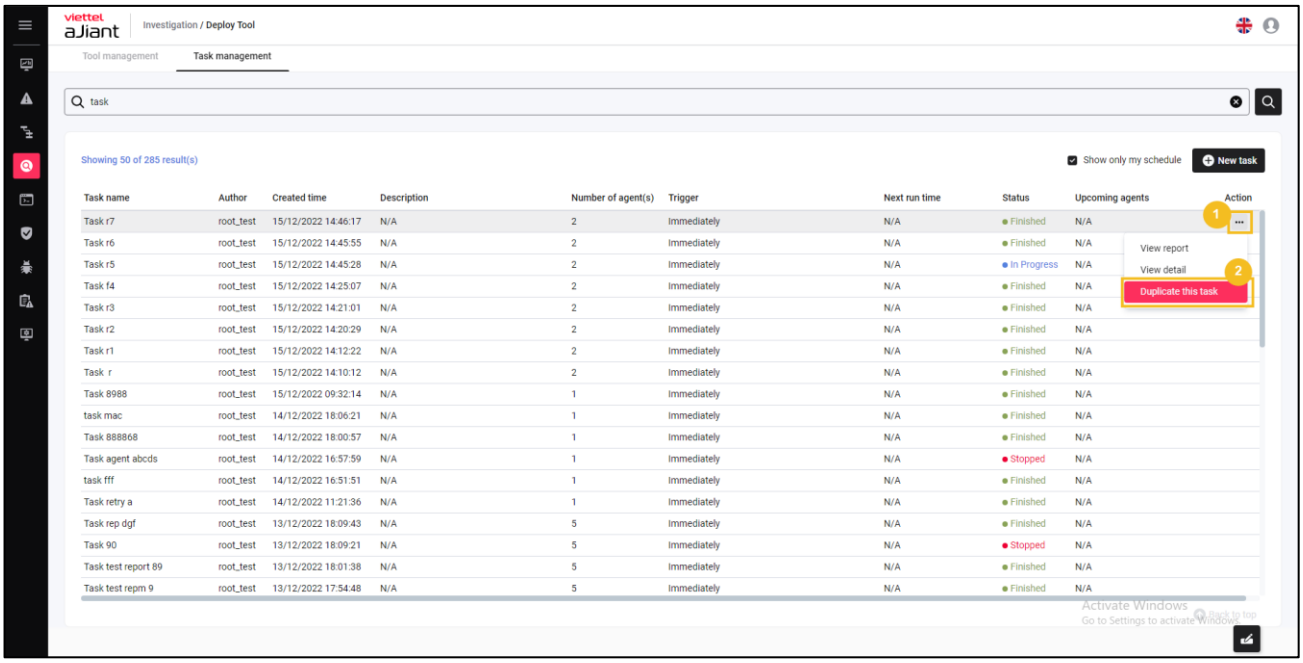
Chọn **Create** để tạo mới task/ cấu hình thông tin deploy tool dưới agent hoặc chọn **Cancel** để hủy task/ hủy cấu hình thông tin deploy tool dưới agent

d. Nhân bản task (Duplicate task)

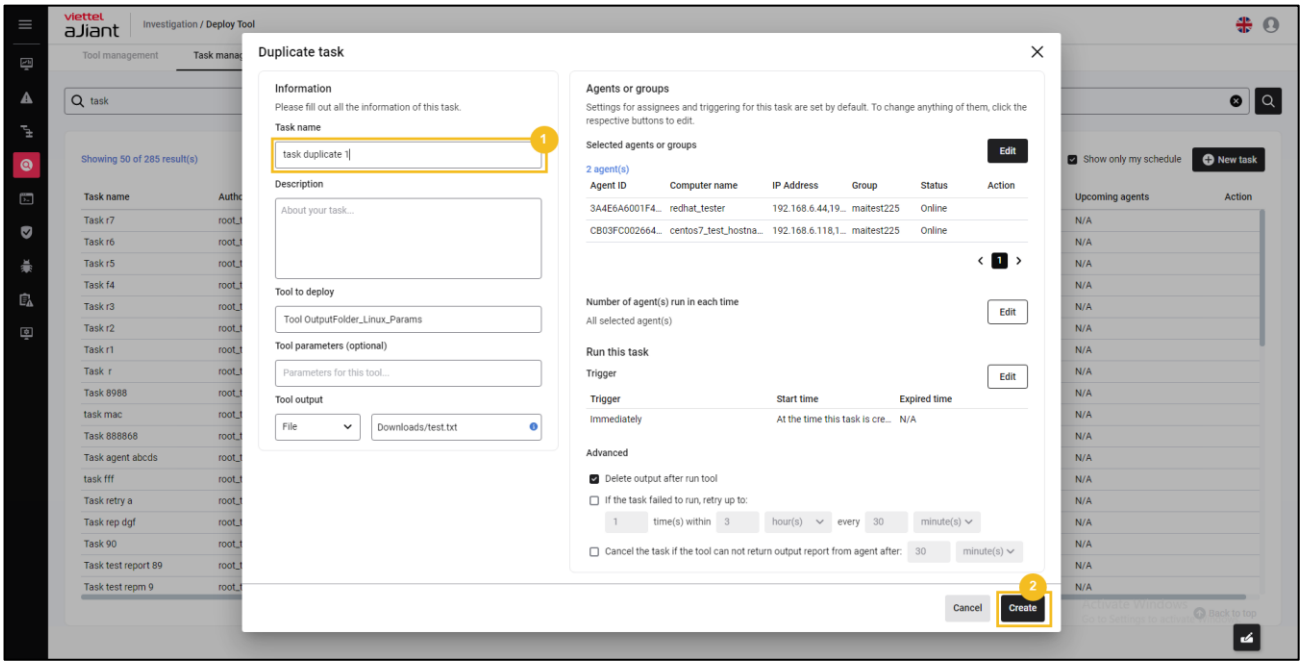
Mục đích: Cho phép nhân bản task (sao chép task), tự động điền các giá trị như task gốc ngoại trừ trường Task name (Yêu cầu người dùng nhập/ sửa lại tên tasks);

Các bước thực hiện:

Bước 1: Tại màn hình danh sách tool, hover vào tool cần nhân bản (duplicate) > chọn ··· > chọn duplicate this task



Bước 2: Nhập thông tin Task name và kiểm tra/ cập nhật thông tin task > Chọn **Create** để hoàn thiện cấu hình hoặc chọn **Cancel** để hủy thao tác nhân bản task

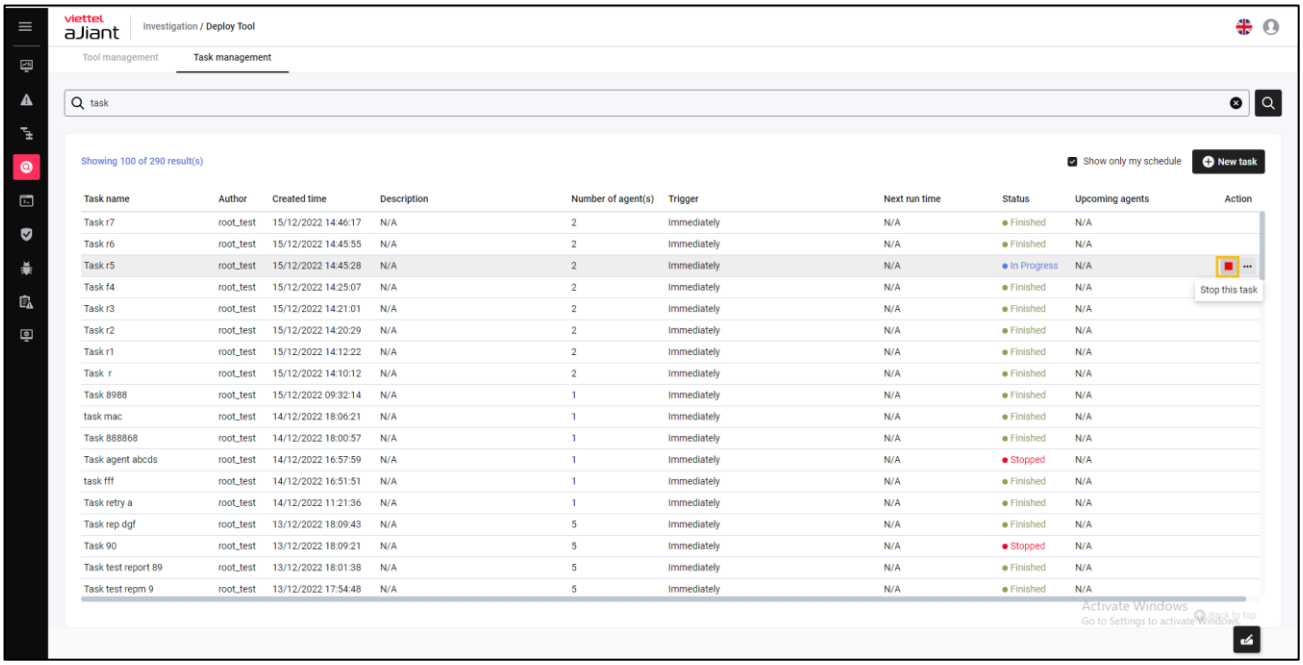


e. Danh sách Upcoming Agents

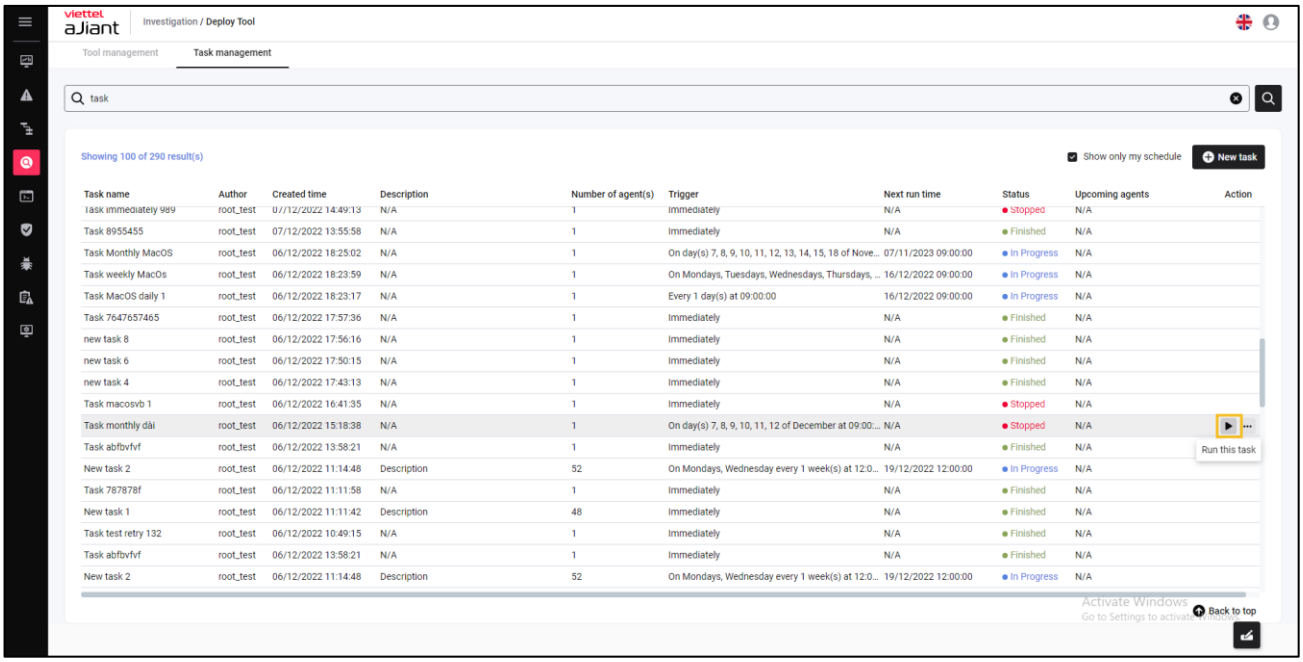
Mục đích: Cho phép hiển thị danh sách Agents sắp được deploy tool;
Các bước thực hiện: Tại màn hình danh sách task > Chọn Danh sách Upcoming agents.

f. Stop/ Start task

Mục đích: Cho phép Stop/ Restart task (Dừng deploy task hoặc deploy lại task đã tạm dừng).
Các bước thực hiện tạm dừng task: Tại màn hình danh sách task, hover vào task cần tạm dừng > Chọn icon  để tạm dừng task:



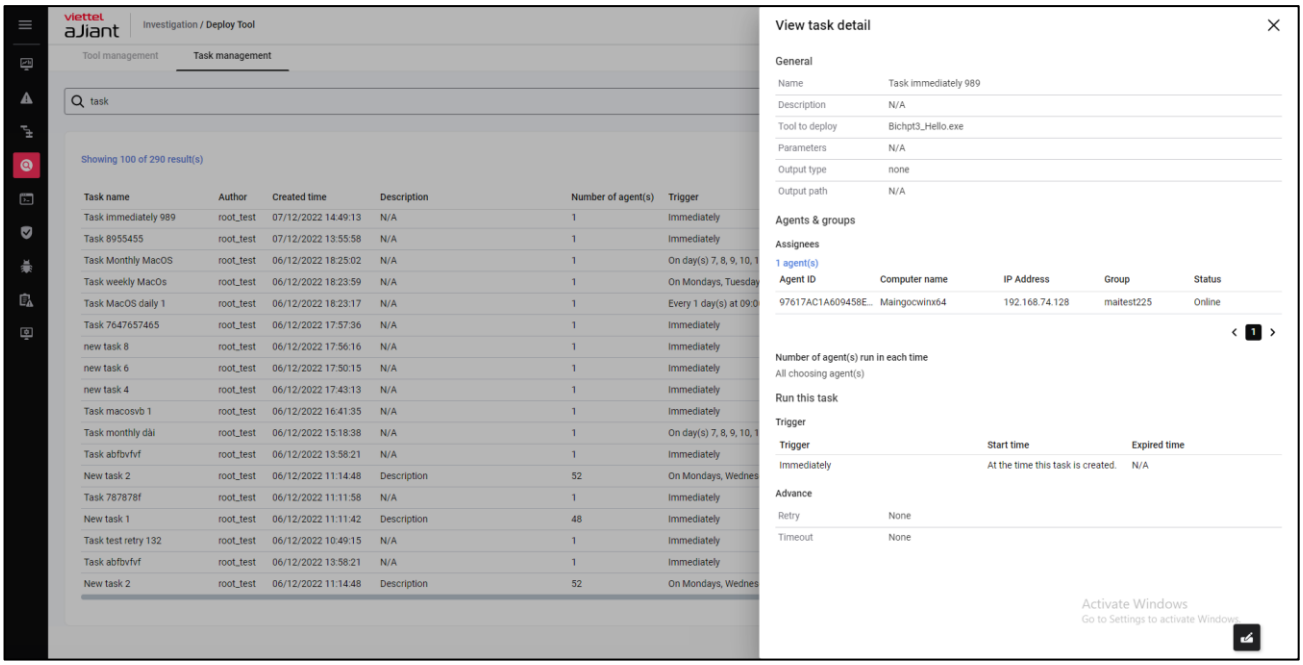
Các bước thực hiện deploy lại task (đã tạm dừng – Stopped): Tại màn hình danh sách task, hover vào task cần deploy lại > Chọn icon  để deploy lại task:



g. Chi tiết task (Detail task)

Mục đích: Cho phép xem thông tin chi tiết task;

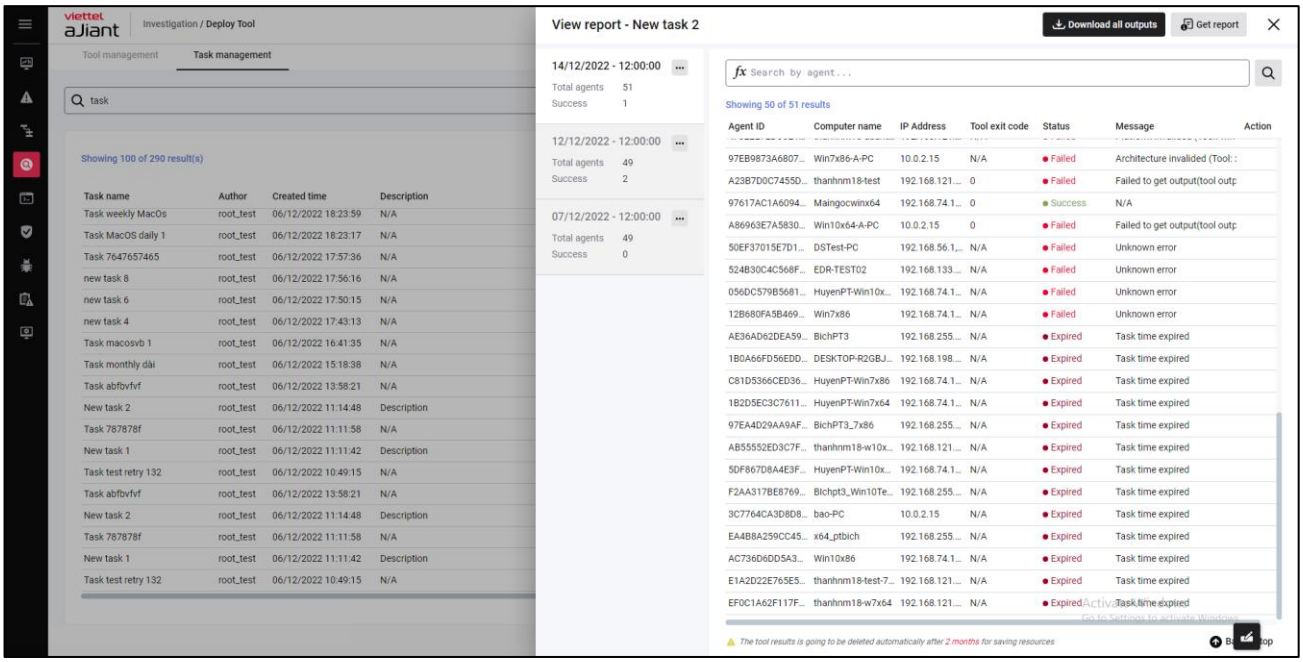
Các bước thực hiện: Tại màn hình danh sách task, hover vào task cần xem chi tiết > Chọn **View detail**:



h. Xem báo cáo (View tool result)

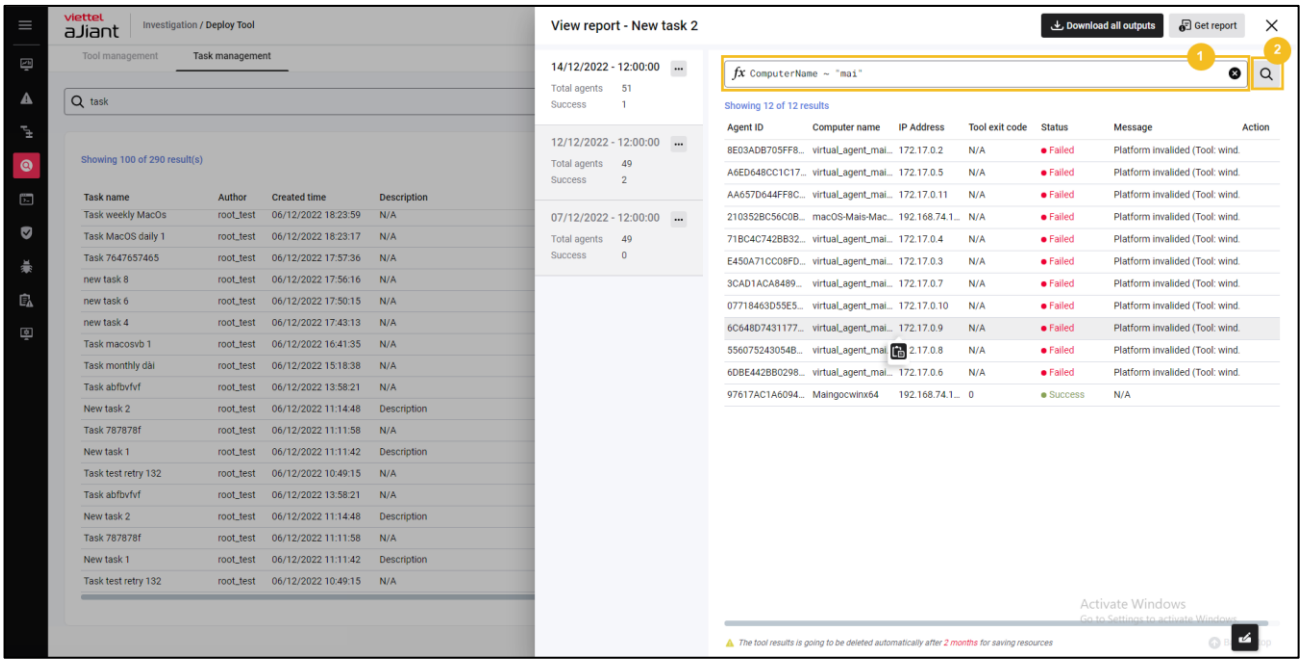
Mục đích: Xem kết quả báo cáo deploy tool;

Các bước thực hiện: Tại màn hình danh sách task, hover vào task cần xem chi tiết > Chọn **View report**:



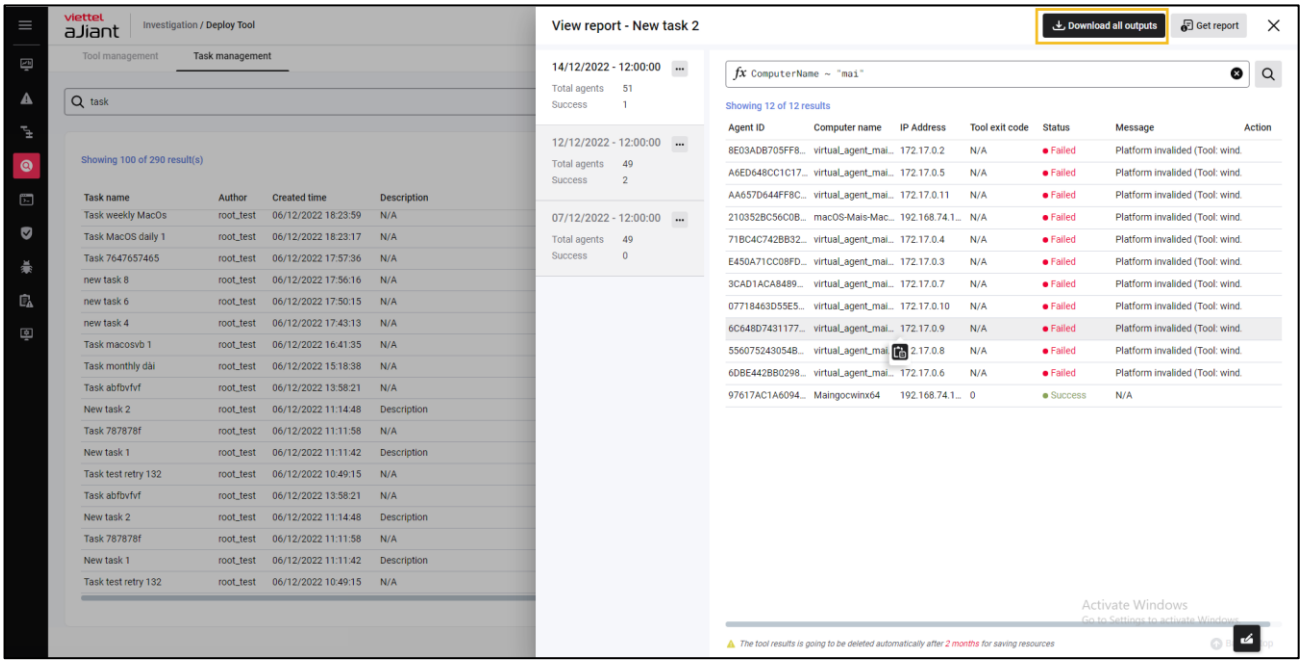
+ Tìm kiếm kết quả deploy tool theo các câu lệnh truy vấn:

  - Mục đích: Cho phép tìm kiếm kết quả deploy tool theo câu lệnh truy vấn;
  - Các bước thực hiện: Nhập vào câu lệnh truy vấn tìm kiếm > tích chọn nút Search hoặc kết thúc nhập từ khóa > nhấn enter. HT thực hiện tìm kiếm thông tin kết quả liên quan đến từ khóa tìm kiếm có trong hệ thống



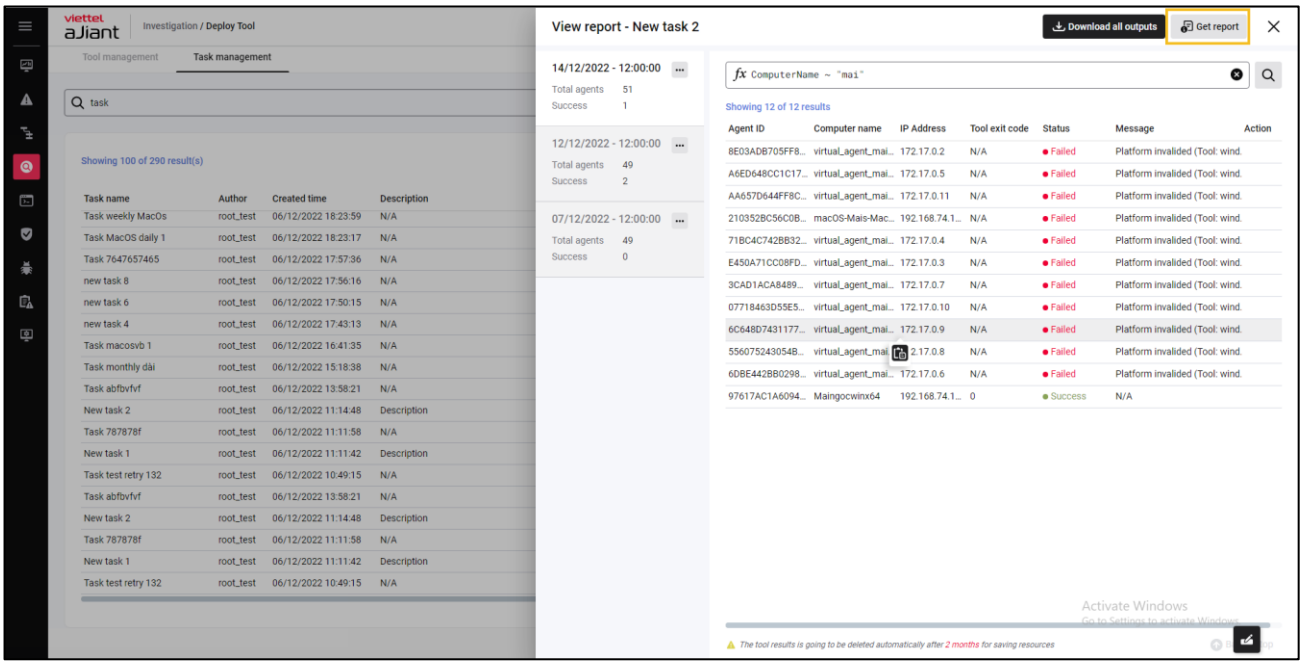
+ Tải xuống toàn bộ kết quả deploy tool (theo lập lịch task):

  - Mục đích: Cho phép tải xuống toàn bộ kết quả deploy tool (theo lập lịch task);
  - Các bước thực hiện: Tại màn hình View report, chọn nút **Download all output**



+ Get all report:

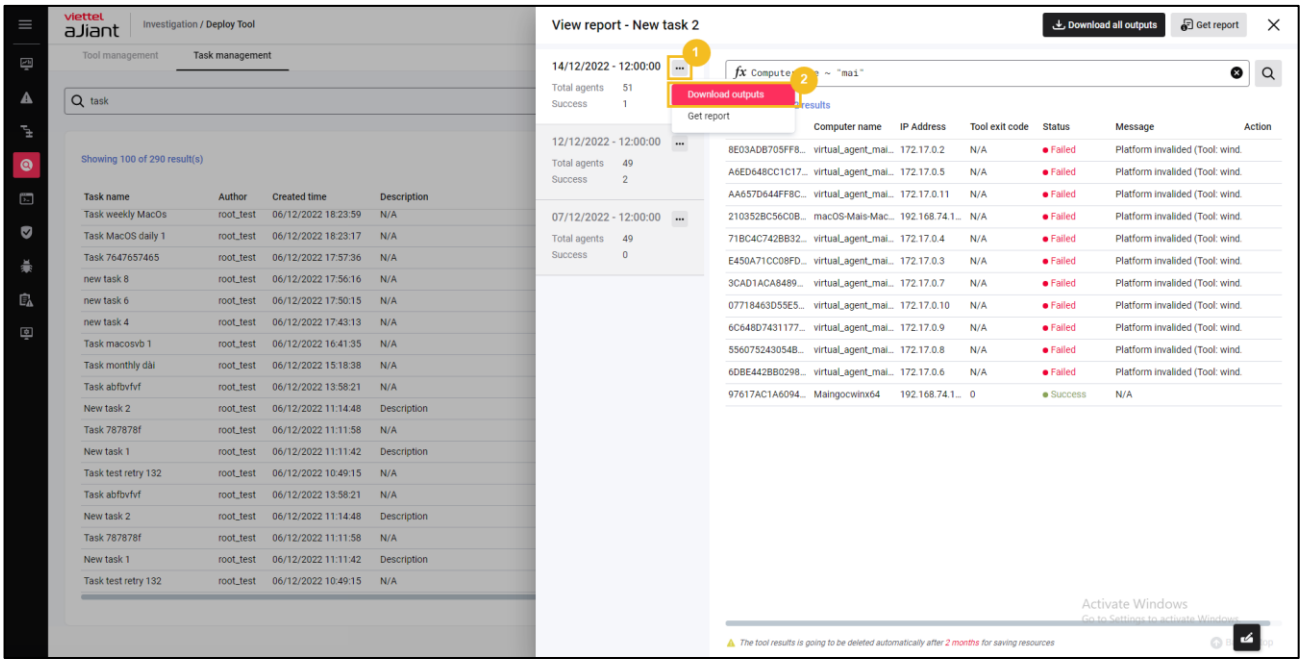
- Mục đích: Cho phép download tất cả danh sách báo cáo kết quả deploy tool.
- Các bước thực hiện: Tại màn hình View report, chọn nút **Get report**:



+ Download output của từng lần lập lịch:

- Mục đích: Cho phép download tất cả danh sách báo cáo kết quả deploy tool tại từng lần lập lịch;

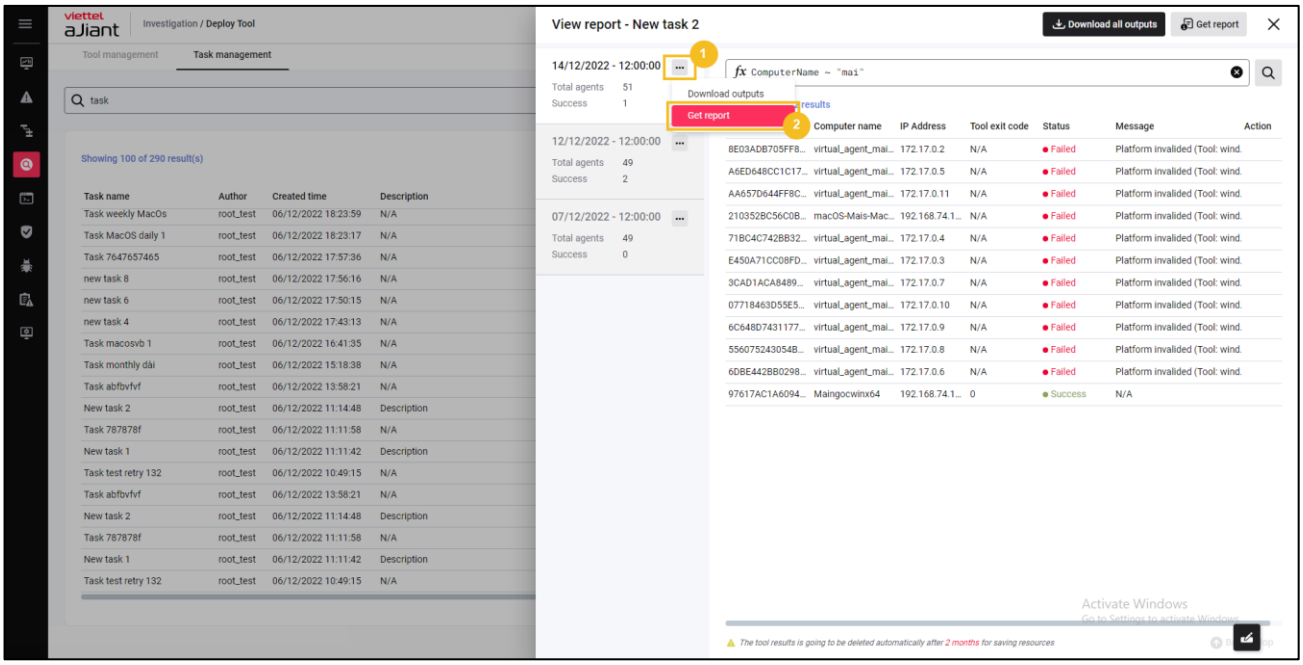
- Các bước thực hiện: Tại màn hình View report, chọn icon ••• bản ghi lập lịch mà người dùng muốn download outputs > Chọn **Download outputs**



+ Download báo cáo của từng lần lập lịch:

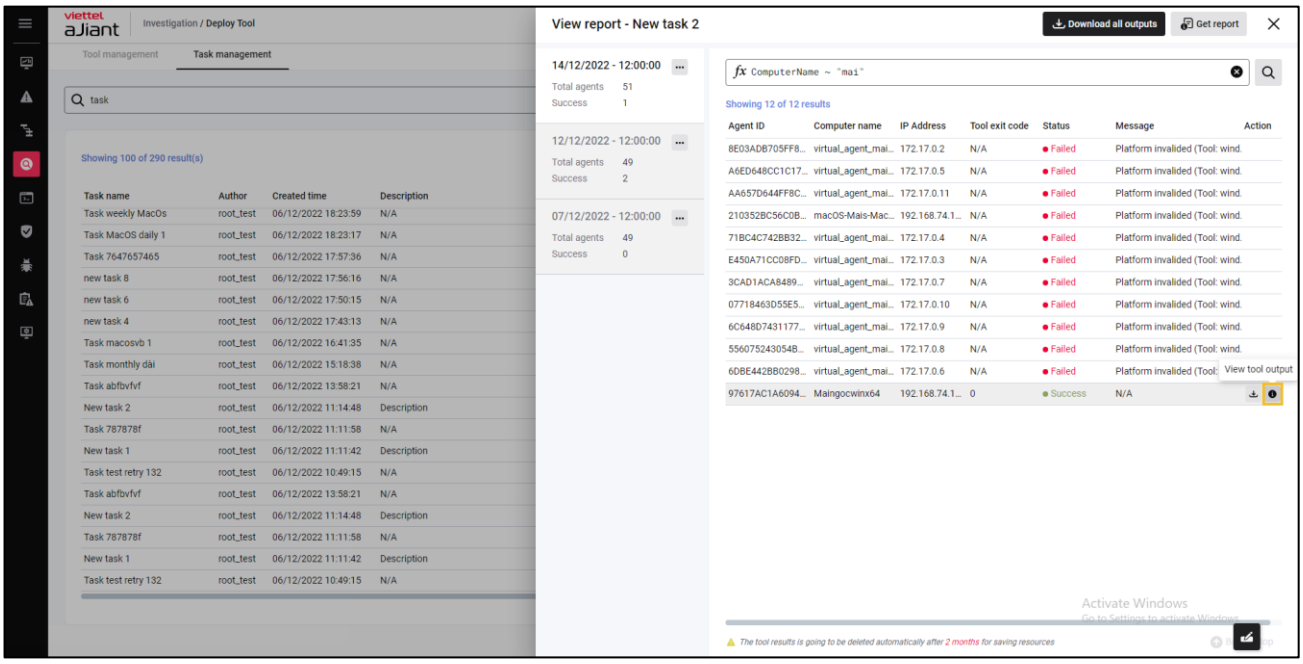
- Mục đích: Cho phép download tất cả danh sách thống kê báo cáo kết quả deploy tool tại từng lần lập lịch (định dạng .csv)

- Các bước thực hiện: Tại màn hình View report, chọn icon ••• bản ghi lập lịch mà người dùng muốn download báo cáo > Chọn **Get report**



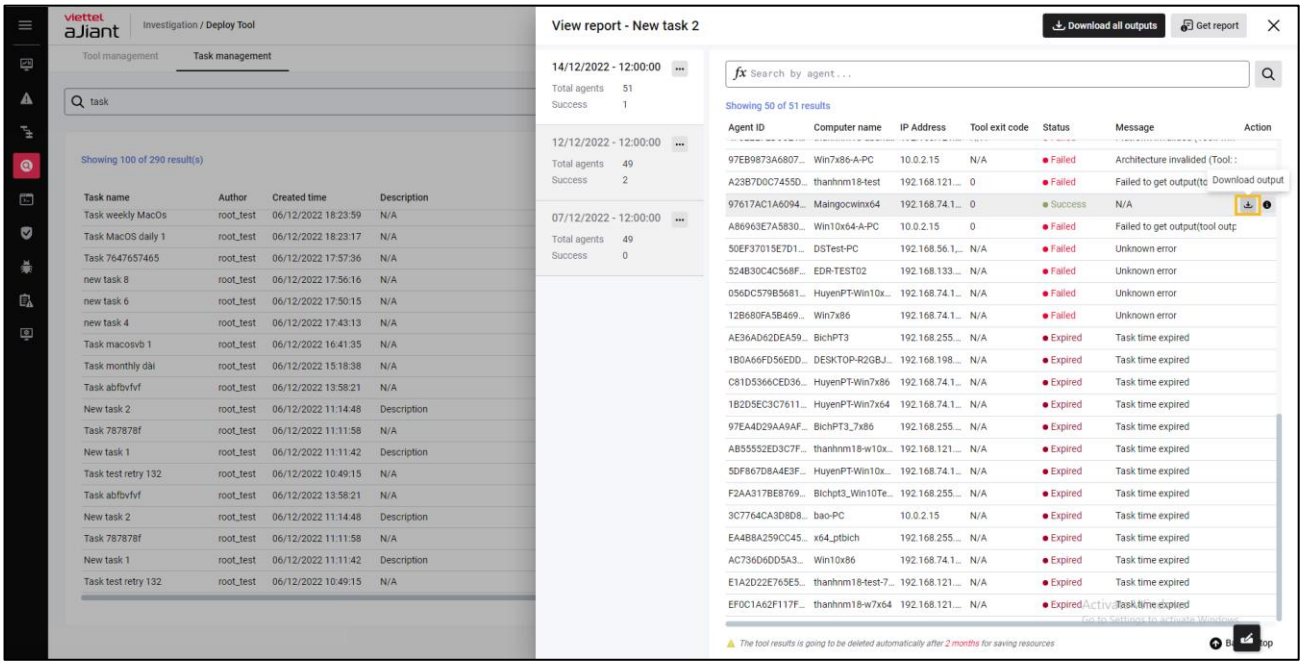
+ View tool outputs của từng agent:

  - Mục đích: Cho phép người dùng xem tool outputs của từng agent
  - Các bước thực hiện: Tại màn hình View report, hover vào bản ghi cần xem báo cáo (có trạng thái Success) > chọn icon ••• > Chọn **View tool output**



+ Download báo cáo kết quả deploy tool từng agent:

  - Mục đích: Cho phép download báo cáo kết quả deploy tool từng agent;
  - Các bước thực hiện: Tại màn hình view report, hover vào bản ghi agent cần xem báo cáo (có trạng thái Success) > chọn icon ••• > Chọn **Download output**



3.4.5 Event Search V2

Tính năng này cho phép người dùng tìm kiếm dữ liệu event được lưu trữ tối thiểu 30 ngày (sử dụng công nghệ lưu trữ bằng ClickHouse).

Các khác biệt so với Event Search:

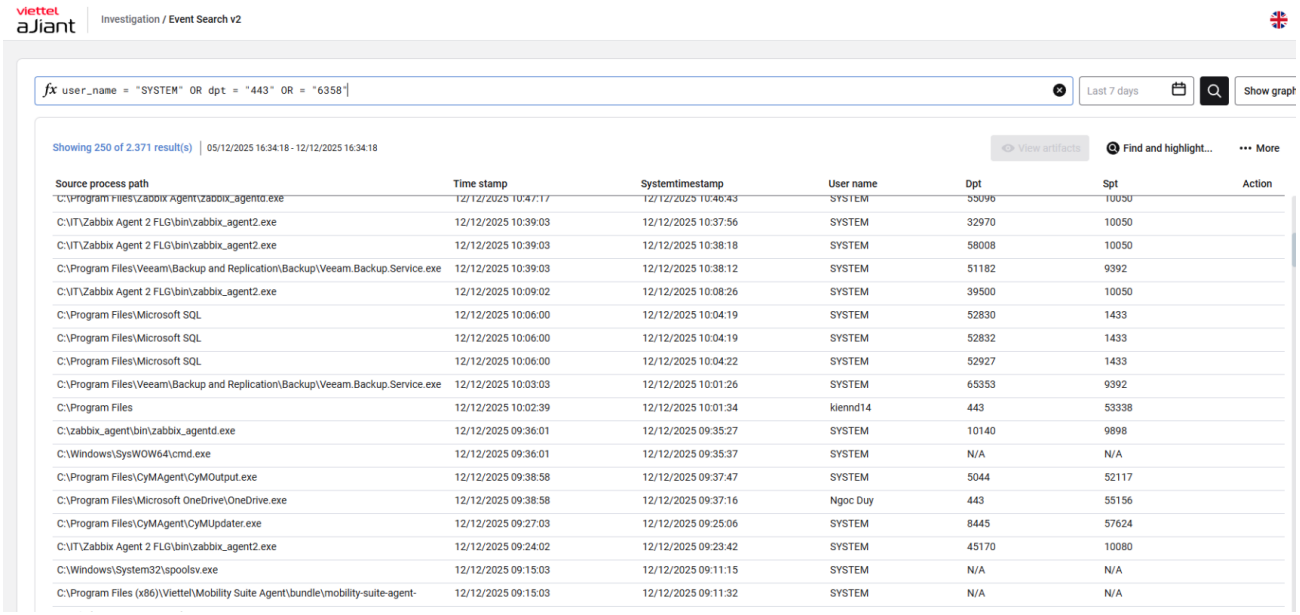
- Lưu trữ log tối thiểu 30 ngày và cho phép người dùng có thể truy vấn tìm kiếm các log tương ứng (Event Search log chỉ lưu được trong 7 ngày)
- Ngoài ra, các cột dữ liệu search khác với Event Search V1 và ẩn bớt một số tính năng phụ
- Chi tiết xem hướng dẫn bên dưới

  Mục đích chính của Event Search V2 là để người dùng có thể search được các log lưu trữ tối thiểu 30 ngày.

3.4.5.1 Tìm kiếm Event

Bước 3: Nhập câu query >Chọn khoảng thời gian > Click nút "Search":

- Nhập câu query với định dạng field name – điều kiện toán tử - "value"
- Có thể sử dụng AND/ OR để nối các điều kiện
- Lưu ý: Không hỗ trợ search theo keyword



Source process path	Time stamp	Systemtimestamp	User name	Dpt	Spt	Action
C:\Program Files\Zabbix Agent\zabbix_agentd.exe	12/12/2025 10:47:17	12/12/2025 10:46:43	SYSTEM	55096	10050	
C:\IT\Zabbix Agent 2 FLG\bin\zabbix_agent2.exe	12/12/2025 10:39:03	12/12/2025 10:37:56	SYSTEM	32970	10050	
C:\IT\Zabbix Agent 2 FLG\bin\zabbix_agent2.exe	12/12/2025 10:39:03	12/12/2025 10:38:18	SYSTEM	58008	10050	
C:\Program Files\Veeam\Backup and Replication\Backup\Veeam.Backup.Service.exe	12/12/2025 10:39:03	12/12/2025 10:38:12	SYSTEM	51182	9392	
C:\IT\Zabbix Agent 2 FLG\bin\zabbix_agent2.exe	12/12/2025 10:09:02	12/12/2025 10:08:26	SYSTEM	39500	10050	
C:\Program Files\Microsoft SQL	12/12/2025 10:06:00	12/12/2025 10:04:19	SYSTEM	52830	1433	
C:\Program Files\Microsoft SQL	12/12/2025 10:06:00	12/12/2025 10:04:19	SYSTEM	52832	1433	
C:\Program Files\Microsoft SQL	12/12/2025 10:06:00	12/12/2025 10:04:22	SYSTEM	52927	1433	
C:\Program Files\Veeam\Backup and Replication\Backup\Veeam.Backup.Service.exe	12/12/2025 10:03:03	12/12/2025 10:01:26	SYSTEM	65353	9392	
C:\Program Files	12/12/2025 10:02:39	12/12/2025 10:01:34	kiennd14	443	53338	
C:\zabbix_agent\bin\zabbix_agentd.exe	12/12/2025 09:36:01	12/12/2025 09:35:27	SYSTEM	10140	9898	
C:\Windows\SysWOW64\cmd.exe	12/12/2025 09:36:01	12/12/2025 09:35:37	SYSTEM	N/A	N/A	
C:\Program Files\CyMAgent\CyMOutput.exe	12/12/2025 09:38:58	12/12/2025 09:37:47	SYSTEM	5044	52117	
C:\Program Files\Microsoft OneDrive\OneDrive.exe	12/12/2025 09:38:58	12/12/2025 09:37:16	Ngoc Duy	443	55156	
C:\Program Files\CyMAgent\CyMUpdater.exe	12/12/2025 09:27:03	12/12/2025 09:25:06	SYSTEM	8445	57624	
C:\IT\Zabbix Agent 2 FLG\bin\zabbix_agent2.exe	12/12/2025 09:24:02	12/12/2025 09:23:42	SYSTEM	45170	10080	
C:\Windows\System32\spoolsv.exe	12/12/2025 09:15:03	12/12/2025 09:11:15	SYSTEM	N/A	N/A	
C:\Program Files (x86)\Viettel\Mobility Suite Agent\bundle\mobility-suite-agent-	12/12/2025 09:15:03	12/12/2025 09:11:32	SYSTEM	N/A	N/A	

3.4.5.2 Highlight

Mục đích: Cho phép thêm 01 hoặc nhiều highlight để rà soát đồng thời tại một thời điểm (không giới hạn số lượng tối đa), khi thực hiện search hoặc sort thì mọi highlight đã tạo sẽ bị clear;

Các bước thự hiện:

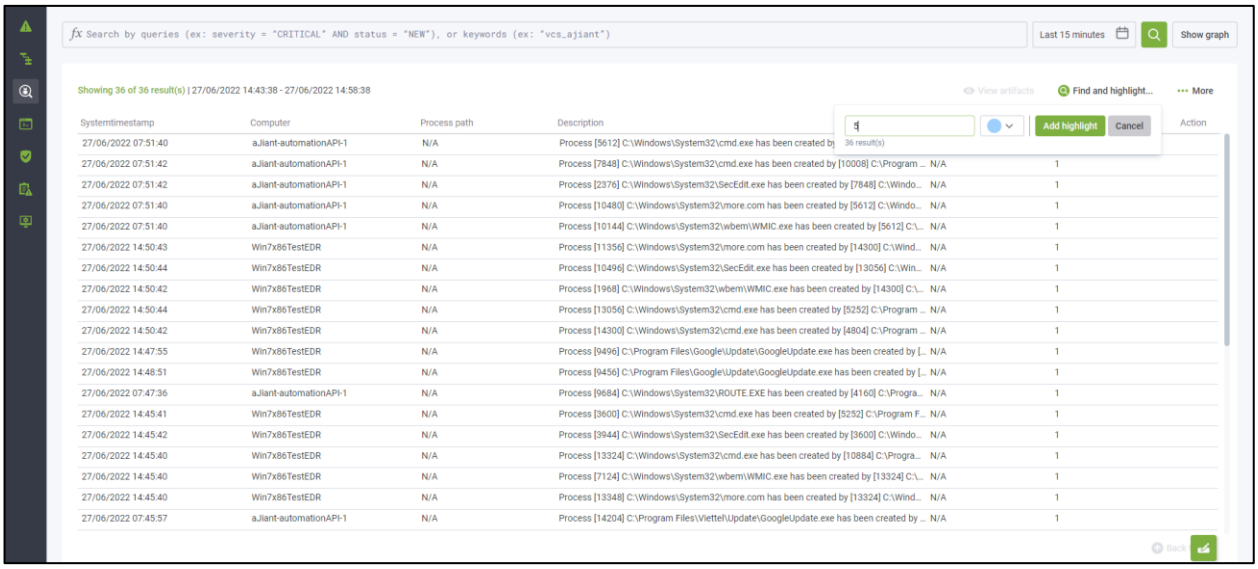
Bước 4: ND chọn Investigation >> Chọn tab Event search V2;

Bước 5: Màn hình hiển thị danh sách event, Chọn nút "Find and highlight", HT hiển thị poup Find in table;

Bước 6: Nhập vào từ khóa đánh dấu, lựa chọn màu đánh dấu và xác nhận thao tác:

Chọn nút "Add highlight", để xác nhận từ khóa đánh dấu;

Chọn nút "Cancel", để hủy thao tác đánh dấu từ khóa tìm kiếm;



3.4.5.3 Need help

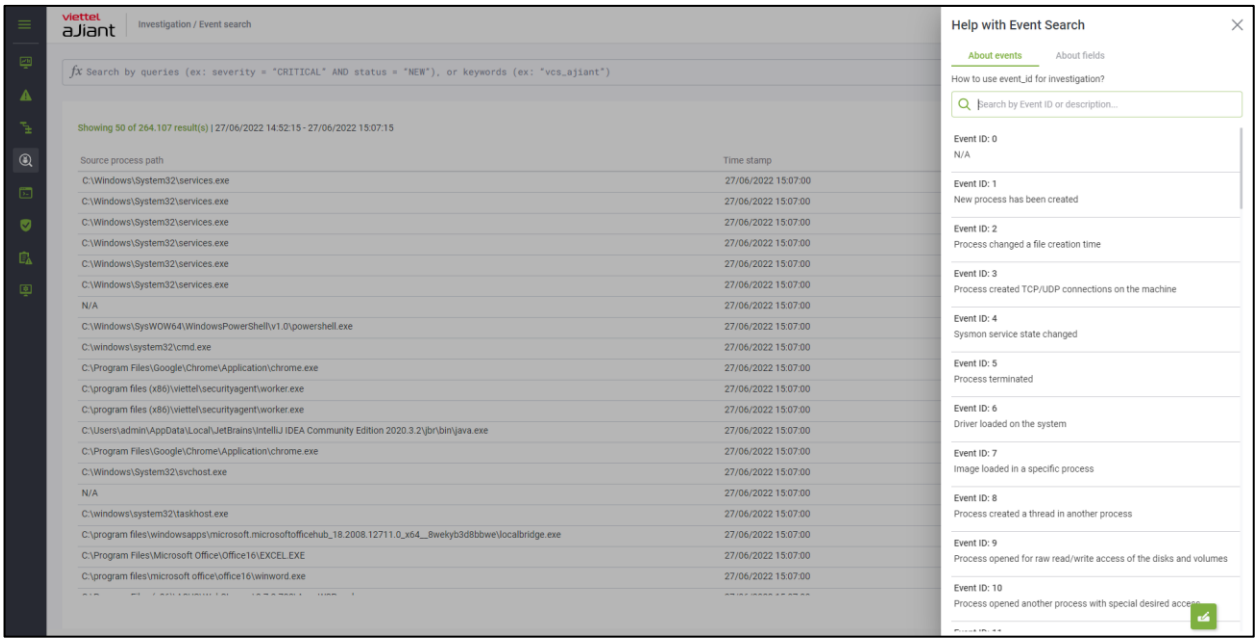
- Mục đích: tra thông tin event, ý nghĩa trường;
- Các bước thực hiện:

Bước 7: ND chọn Investigation >> Chọn tab Event search V2;

Bước 8: Tại màn hình Event Search V2, chọn "More";

Bước 9: HT hiển thị danh sách các thao tác: Show columns, Wrapt text, Need help, Chọn "Need help?";

Bước 10: HT hiển thị popup Help with Event Search, cho phép tra cứu thông tin, ý nghĩa các trường trong Event Search.



3.4.5.4 Wrapt text

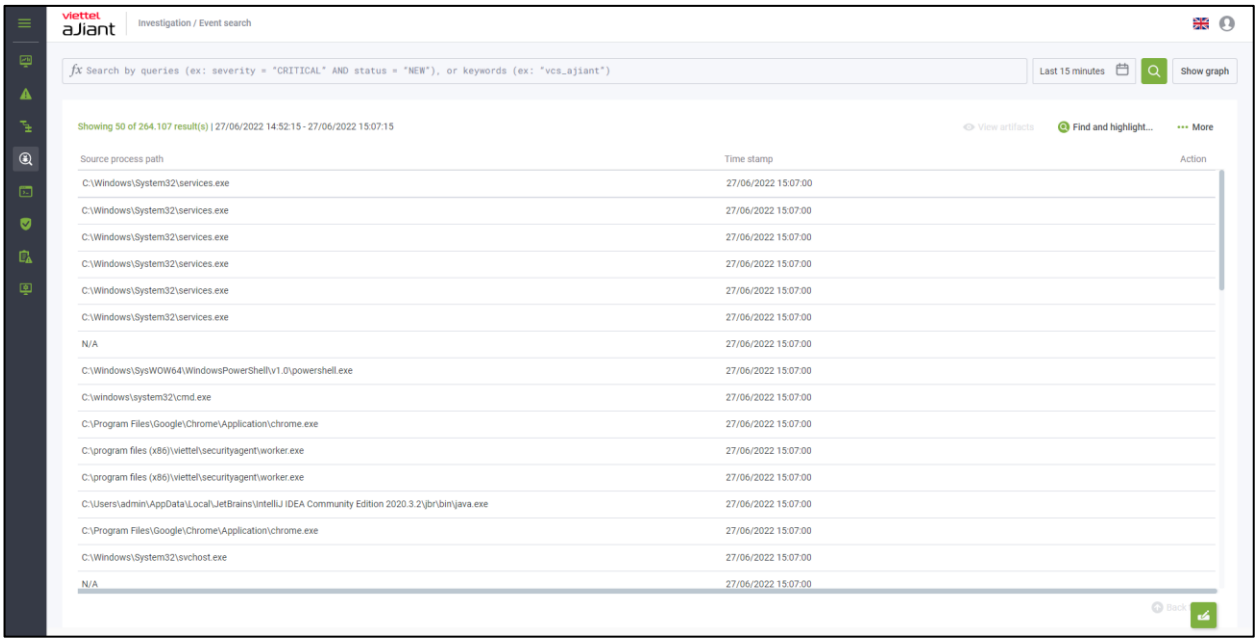
Mục đích: Có thể hiển thị toàn bộ dữ liệu hoặc thu gọn lại dữ liệu khi click vào nút "wrap text";

Các bước thực hiện:

Bước 11: Tại màn hình Event Search V2, chọn "More";

Bước 12: HT hiển thị danh sách các thao tác: Show columns, Wrapt text, Need help, Chọn "Wrapt text?";

Bước 13: HT thay đổi thông tin hiển thị toàn bộ dữ liệu hoặc thu gọn lại dữ liệu khi click vào nút "Wrap text";



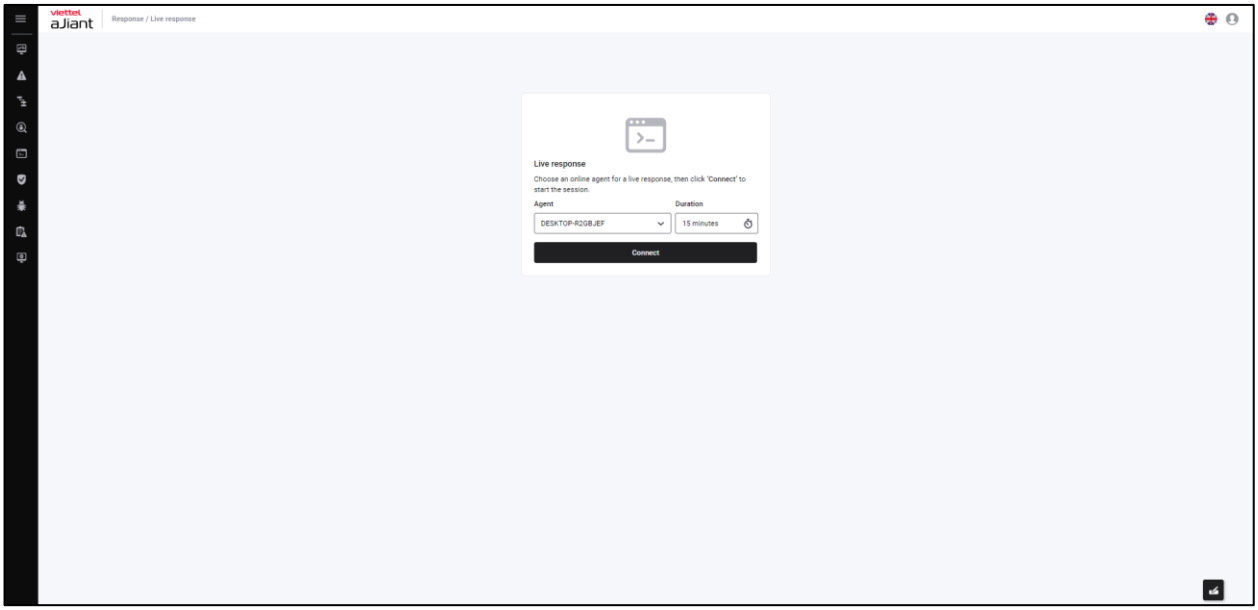
3.5 Nhóm chức năng Response

3.5.1 Live Response

Mục đích: Chức năng Live response cung cấp khả năng xử lý một tập các command từ xa theo phiên làm việc nhằm cho biết các thông tin hoặc xử lý yêu cầu trên host;

Các bước thực hiện chức năng Live Response:

Bước 1: Click tab “Response” và chọn “Live Response”;



Bước 2: Thực hiện tạo mới 1 phiên live response

Chọn Agent: Hiển thị danh sách các agent:

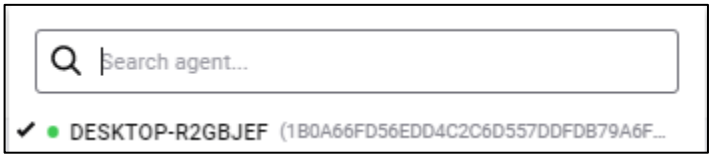
+ User đăng nhập thuộc group root: Hiển thị tất cả Agent trong hệ thống active < 30 ngày;

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

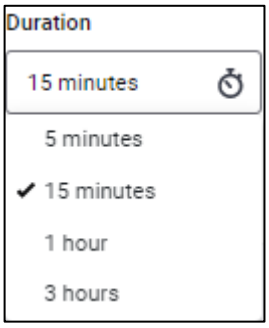
+ User đăng nhập thuộc group cha: Hiển thị tất cả Agent thuộc group của user đang login và group con tương ứng;

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

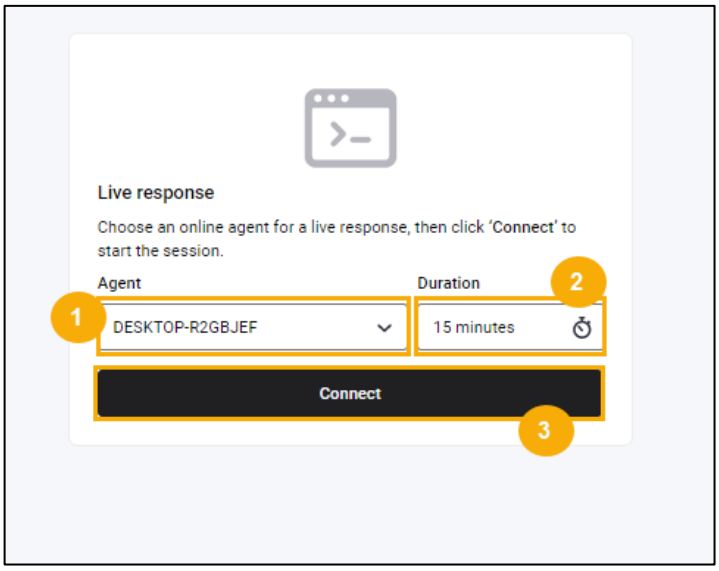
Người dùng chỉ thực hiện được Live Response với những agent đang có trạng thái online:



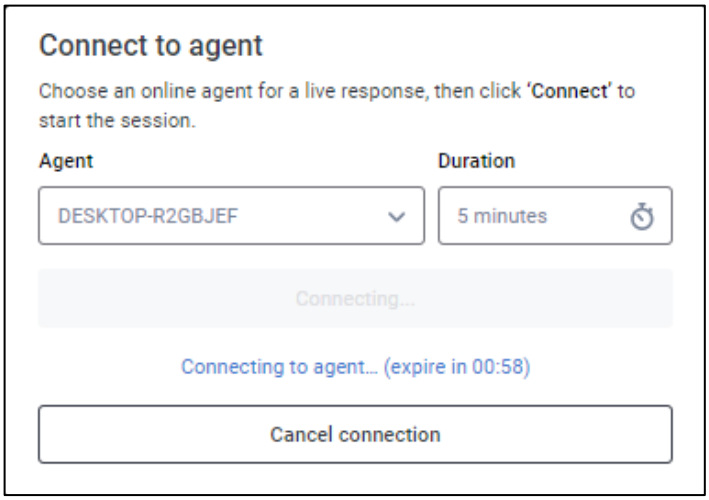
+ Chọn Duration: có các khoảng thời gian 5 phút, 15 phút, 1 giờ, 3 giờ;



+ Click nút “Connect”:

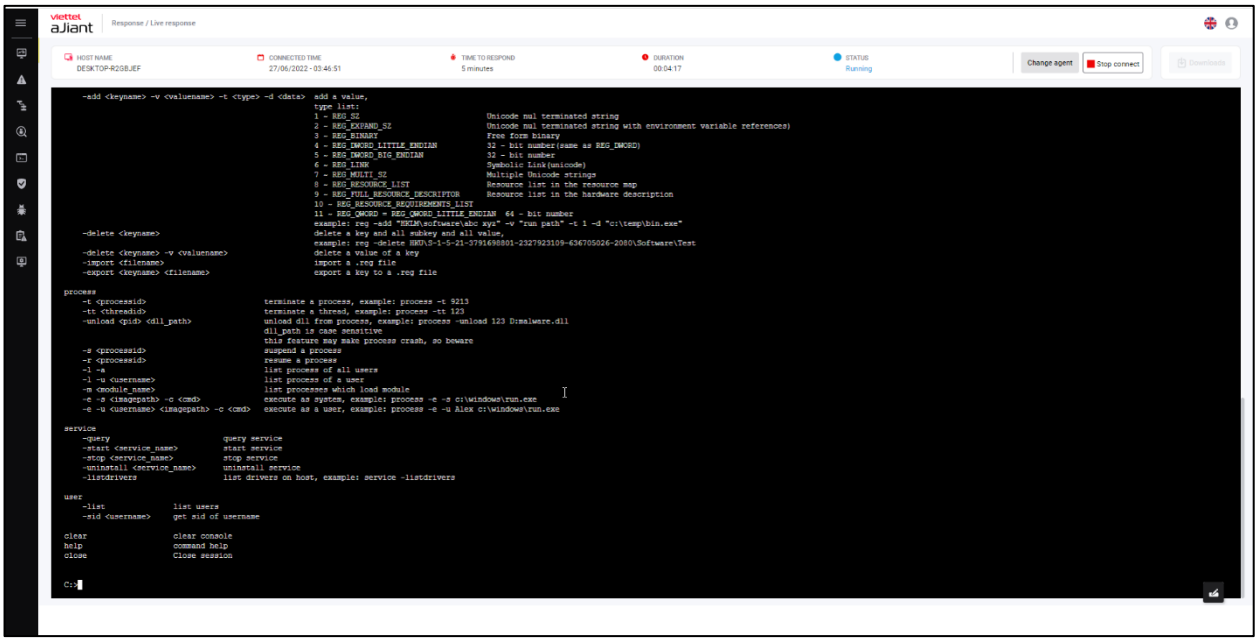


Bước 3: Chờ 1 phút để hệ thống thực hiện kết nối tới agent, trạng thái hệ thống là "connecting":

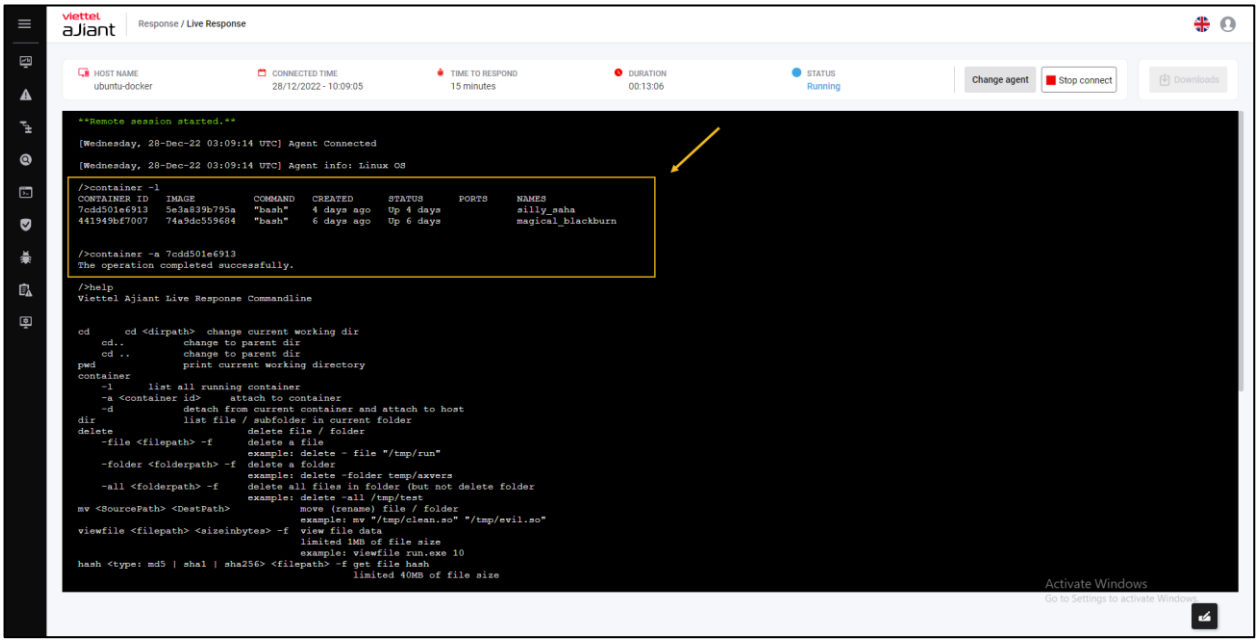


Bước 4: Khi kết nối thành công, người dùng được phép thực hiện các lệnh ở màn hình console và trạng thái của phiên Live response "running";

Lưu ý: Mỗi agent tại một thời điểm chỉ có 1 phiên Live response làm việc.



Lưu ý: Người dùng có thể thực hiện câu lệnh kết nối tới container bằng cách thực hiện các lệnh màn hình console container



Người dùng có thể thực hiện các lệnh tại màn hình console như sau:

+ Window: thực hiện các câu lệnh sau:

STT	*Các lệnh*	*Tham số*	*Mô tả*
1	cd	cd <dirpath>	Thay đổi thư mục làm việc hiện tại
		cd.. hoặc cd ..	Chuyển về thư mục cha
2	pwd		In thư mục hiện thời đang làm việc
3	dir	dir [drive:][path][filename] [/A[[:]attributes]] [/O[[:]sortorder]] [/T[[:]timefield]] [/L] [/Q] [/R] [/S] [/X]	Liệt kê các file/ các thư mục con trong thư mục hiện thời
		/A:[-] attributes Displays files with specified attributes. Attributes: D Directories R Read-only files H Hidden files A Files ready for archiving S System files L Reparse Points	
		/L Lower-case filename	
		/O:[-]sortorder List by files in sorted order. sortorder N By name (alphabetic)	

STT	*Các lệnh*	*Tham số*	*Mô tả*
		S By size (smallest first) E By extension (alphabetic) D By date/time (oldest first) G Group directories first - Prefix to reverse order Ex: dir /O:N;	
		/T:timefield Choose which time field displayed timefield C Creation M MFT Creation A Last Access W Last Written Ví dụ: dir /T:A - Prefix to exclude attribute Ví dụ: dir /A:D-AH	
		/Q Display the owner of the file. Ví dụ: dir /Q	
		/R Display alternate data streams of the file. Ví dụ: dir /R	

STT	*Các lệnh*	*Tham số*	*Mô tả*
		/S Displays files in specified directory and all subdirectories. Ví dụ: dir /S	
		/X This displays the short names generated for non-8dot3 file names. Ví dụ: dir /X	
4	delete	delete –file <path> ví dụ: delete -file "c:\temp\run path.exe"	Xóa 1 file
		delete -folder <folderpath> ví dụ: delete -folder temp\axvers	Xóa 1 thư mục
		delete –all <folderpath> ví dụ: delete –all c:\temp	Xóa tất cả các file/ thự mục con trong thư mục (nhưng không xóa thư mục)
5	mv	<SourcePath> <DestPath> move (rename) file / folder Ví dụ: example: mv "c:\temp\clean.exe" "c:\temp\evil.exe"	Cho phép di chuyển file/ folder

STT	*Các lệnh*	*Tham số*	*Mô tả*
6	viewfile	<filepath><sizeinbytes>	Hiển thị dữ liệu trong file (giới hạn kích thước file)
7	Hash	hash <type: md5 | sha1 | sha256> <filepath> -f get file hash ví dụ: example: hash md5 c:\test\run.exe	Cho phép mã hóa file tối đa 1MB Option -f để buộc mở tệp khi tệp đang được mở bởi một quy trình khác
8	dump		Cho phép dump tiến trình. Nếu bạn bỏ qua đường dẫn tệp kết xuất, nó sẽ mặc định là <processname> _ <datetime> .dmp
		-process -pid <ProcessID> [-f <DestPath>] dump process by process id Ví dụ: dump -process -pid 452 -f "C:\Users\Evil_dumped.dmp"	Dump process bởi Process id
		-process -name <ProcessName> [-f <DestPath>] dump process by process name Ví dụ: dump -process -name Evil.exe -f "C:\Users\Evil_dumped.dmp"	Dump process bởi Process name

STT	*Các lệnh*	*Tham số*	*Mô tả*
		-process -path <ProcessPath> [-f <DestPath>] dump process by process path Ví dụ: dump -process -path "C:\Users\Evil.exe" -f "C:\Users\Evil_dumped.dmp"	Dump process bởi Process Path
9	get	<filepath>	Upload 1 file từ host lên server
10	put	<url><folderpath>	Download 1 file tới máy host
11	mkdir	<dir name>	Tạo 1 thư mục
12	reg		Các lệnh liên quan đến Registry
		query <keyname> -v <valuename> ví dụ: reg-query "HKLM\Software\abc xyz" -v "run path"	Truy vấn dữ liệu value của 1 key
		query <keyname> -s ví dụ: reg-query "HKLM\Software\abc xyz" -s	Truy vấn tất cả các subkey và value và data
		add <keyname> ví dụ:	Thêm 1 key

STT	*Các lệnh*	*Tham số*	*Mô tả*
		reg-add "HKLM\software\abc xyz"	
		add <keyname> -v <valuename> -t <type> -d <data> ví dụ: reg-add "HKLM\software\abc xyz" -v "run path" -t REG_SZ -d "c:\temp\bin.exe"	Thêm 1 value
		delete <keyname> ví dụ: reg -delete HKU\S-1-5-21-3791698801-2327923109-636705026-2080\Software\Test	Xóa 1 key và tất cả các subkey và value
		delete <keyname> -v <valuename>	Xóa 1 giá trị của key
		import <filename>	Import 1 file .reg
		export <keyname> <filename>	Export 1 file .reg
13	process		Các lệnh liên quan đến process
		-t <processid>	Tắt 1 tiến trình đang chạy theo ID tiến trình
		-s <processid>	Tạm dừng 1 tiến trình

STT	*Các lệnh*	*Tham số*	*Mô tả*
		-r <processid>	Hồi phục lại 1 tiến trình đã bị tạm dừng trước đó
		-l -a	Liệt kê toàn bộ các process của tất cả các user
		-l -u <username>	Liệt kê các process của 1 user
14	service		Các lệnh liên quan đến service
		-query	Liệt kê các service đang chạy trên máy host
		-start <servicename>	Start 1 service
		-stop <servicename>	Stop 1 service
		-uninstall <service_name> uninstall service	Gỡ cài đặt service
		-listdrivers list drivers on host, example: service -listdrivers	List danh sách drivers trên host
15	user	-list	Liệt kê các user trên máy
		-sid<username>	Lấy sid của username
16	grep	grep -t <text> <param> <command>	Hỗ trợ tìm kiếm theo từ hoặc chuỗi từ kết quả đầu ra được theo lệnh command truyền vào
17	cls		Xóa màn hình console

STT	Các lệnh	Tham số	Mô tả
18	help		Lệnh help
19	Clear		Làm sạch console
20	Close		Đóng session
21	container	- l	Liệt kê danh sách container
		-a <container id>	Kết nối tới từng container
		-d	Thoát kết nối container

+ Ubuntu: Thực hiện các câu lệnh sau:

STT	Các lệnh	Tham số	Mô tả
1	cd	cd <dirpath>	Thay đổi thư mục làm việc hiện tại
		cd.. hoặc cd ..	Chuyển về thư mục cha
2	pwd		In thư mục hiện thời đang làm việc
3	dir	dir list file / subfolder in current folder	Liệt kê các file/ các thư mục con trong thư mục hiện thời
4	delete	delete –file <path> ví dụ: delete -file "c:\temp\run path.exe"	Xóa 1 file
		delete -folder <folderpath> ví dụ: delete -folder temp\axvers	Xóa 1 thư mục

STT	Các lệnh	Tham số	Mô tả
		delete –all <folderpath> ví dụ: delete –all c:\temp	Xóa tất cả các file/ thự mục con trong thư mục (nhưng không xóa thư mục)
5	mv	<SourcePath> <DestPath> move (rename) file / folder Ví dụ: example: mv "c:\temp\clean.exe" "c:\temp\evil.exe"	Cho phép di chuyển file/ folder
6	viewfile	<filepath><sizeinbytes>	Hiển thị dữ liệu trong file (giới hạn kích thước file)
7	Hash	hash <type: md5 | sha1 | sha256> <filepath> -f get file hash ví dụ: example: hash md5 c:\test\run.exe	Cho phép mã hóa file tối đa 1MB Option -f để buộc mở tệp khi tệp đang được mở bởi một quy trình khác
8	get	<filepath>	Upload 1 file từ host lên server
9	put	<url><folderpath>	Download 1 file tới máy host
10	mkdir	<dir name>	Tạo 1 thư mục
11	process		Các lệnh liên quan đến process
		-t <processid>	Tắt 1 tiến trình đang chạy theo ID tiến trình

STT	*Các lệnh*	*Tham số*	*Mô tả*
		-s <processid>	Tạm dừng 1 tiến trình
		-r <processid>	Hồi phục lại 1 tiến trình đã bị tạm dừng trước đó
		-l -a	Liệt kê toàn bộ các process của tất cả các user
		-l -u <username>	Liệt kê các process của 1 user
		-e -s <imagepath> -c <cmd> execute a non GUI process as system Ví dụ: process -e -s /tmp/run	
		-e-u<username> <imagepath> -c <cmd> execute a non GUI process as a user Ví dụ: process -e -u Alex /tmp/run	
		-d <processid> -o <imagepath> generate core file of running program, ví dụ: process -d 231 -o /tmp/core_file	
12	service		Các lệnh liên quan đến service
		-query	Liệt kê các service đang chạy trên máy host
		-start <servicename>	Start 1 service

STT	Các lệnh	Tham số	Mô tả
		-stop <servicename>	Stop 1 service
		-uninstall <service_name> uninstall service	Gỡ cài đặt service
		-listdrivers list drivers on host, example: service -listdrivers	List danh sách drivers trên host
13	user	-list	Liệt kê các user trên máy
		-sid<username>	Lấy sid của username
14	help		Lệnh help
15	Clear		Làm sạch console
21	container	- l	Liệt kê danh sách container
		-a <container id>	Kết nối tới từng container
		-d	Thoát kết nối container

+ MACOS:

STT	Các lệnh	Tham số	Mô tả
1	cd	cd <dirpath>	Thay đổi thư mục làm việc hiện tại
		cd.. hoặc cd ..	Chuyển về thư mục cha
2	pwd		In thư mục hiện thời đang làm việc
3	dir	dir list file / subfolder in current folder	Liệt kê các file/ các thư mục con trong thư mục hiện thời

STT	Các lệnh	Tham số	Mô tả
4	delete	delete –file <path> ví dụ: delete -file "c:\temp\runpath.exe"	Xóa 1 file
		delete -folder <folderpath> ví dụ: delete -folder temp\axvers	Xóa 1 thư mục
		delete –all <folderpath> ví dụ: delete –all c:\temp	Xóa tất cả các file/ thự mục con trong thư mục (nhưng không xóa thư mục)
5	mv	<SourcePath> <DestPath> move (rename) file / folder Ví dụ: example: mv "c:\temp\clean.exe" "c:\temp\evil.exe"	Cho phép di chuyển file/ folder
6	viewfile	<filepath><sizeinbytes>	Hiển thị dữ liệu trong file (giới hạn kích thước file)
7	Hash	hash <type: md5 | sha1 | sha256> <filepath> -f get file hash ví dụ: example: hash md5 c:\test\run.exe	Cho phép mã hóa file tối đa 1MB Option -f để buộc mở tệp khi tệp đang được mở bởi một quy trình khác
8	get	<filepath>	Upload 1 file từ host lên server

STT	*Các lệnh*	*Tham số*	*Mô tả*
9	put	<url><folderpath>	Download 1 file tới máy host
10	mkdir	<dir name>	Tạo 1 thư mục
11	process		Các lệnh liên quan đến process
		-t <processid>	Tắt 1 tiến trình đang chạy theo ID tiến trình
		-s <processid>	Tạm dừng 1 tiến trình
		-r <processid>	Hồi phục lại 1 tiến trình đã bị tạm dừng trước đó
		-l -a	Liệt kê toàn bộ các process của tất cả các user
		-l -u <username>	Liệt kê các process của 1 user
		-e -s <imagepath> -c <cmd> execute a non GUI process as system Ví dụ: process -e -s /tmp/run	
		-e-u<username> <imagepath> -c <cmd> execute a non GUI process as a user Ví dụ: process -e -u Alex /tmp/run	
12	service		Các lệnh liên quan đến service

STT	*Các lệnh*	*Tham số*	*Mô tả*
		-query	Liệt kê các service đang chạy trên máy host
		-start <servicename>	Start 1 service
		-stop <servicename>	Stop 1 service
		-uninstall <service_name> uninstall service	Gỡ cài đặt service
		-listdrivers list drivers on host, example: service -listdrivers	List danh sách drivers trên host
13	user	-list	Liệt kê các user trên máy
		-sid<username>	Lấy sid của username
14	help		Lệnh help
15	Clear		Làm sạch console

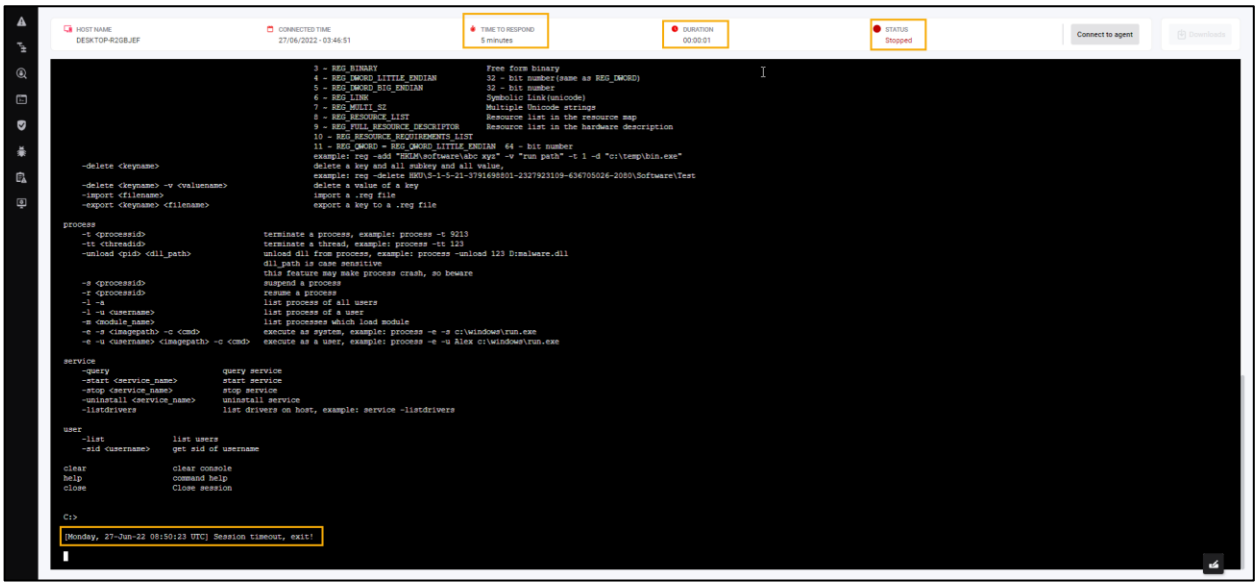
Một số lưu ý khi làm việc với các lệnh trên màn hình console:

+ Lệnh Clear: Sau khi thực hiện lệnh clear thì hệ thống sẽ hỗ trợ người dùng download toàn bộ log đã thực hiện trên màn hình console trước đấy, bằng thao tác click vào link “here”;

+ Lệnh get <filepath>: ví dụ: get procexp.exe trong màn hình console thì kết quả lấy file về được hiển thị ở màn hình Attachment Log ở phía dưới góc bên phải của màn hình. Người dùng được phép tải file về trình duyệt hoặc xóa file đã lấy về server.

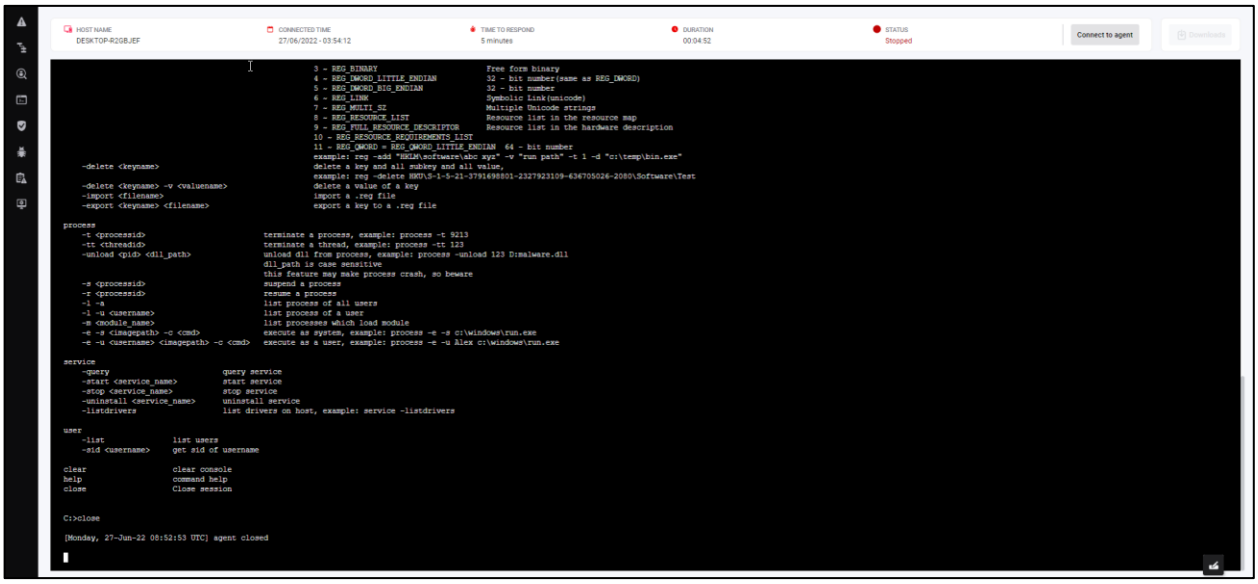
Bước 5: Phiên làm việc của Live Response kết thúc khi:

+ Thời gian của phiên hết hiệu lực: Khi trường "Duration" bằng thời gian với trường "Time To Live";



+ Người dùng chủ động yêu cầu đóng kết nối bằng lệnh "close";

+ Khi mất kết nối với agent, server thực hiện ping/pong failed trên 3 lần.

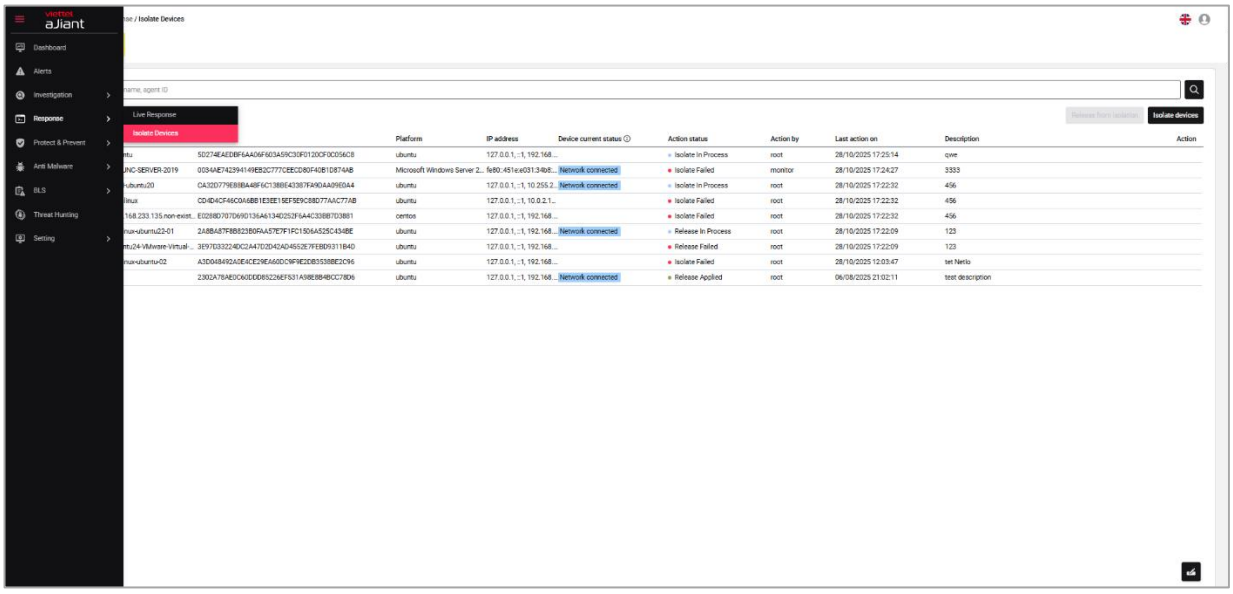


3.5.2 Isolate Devices

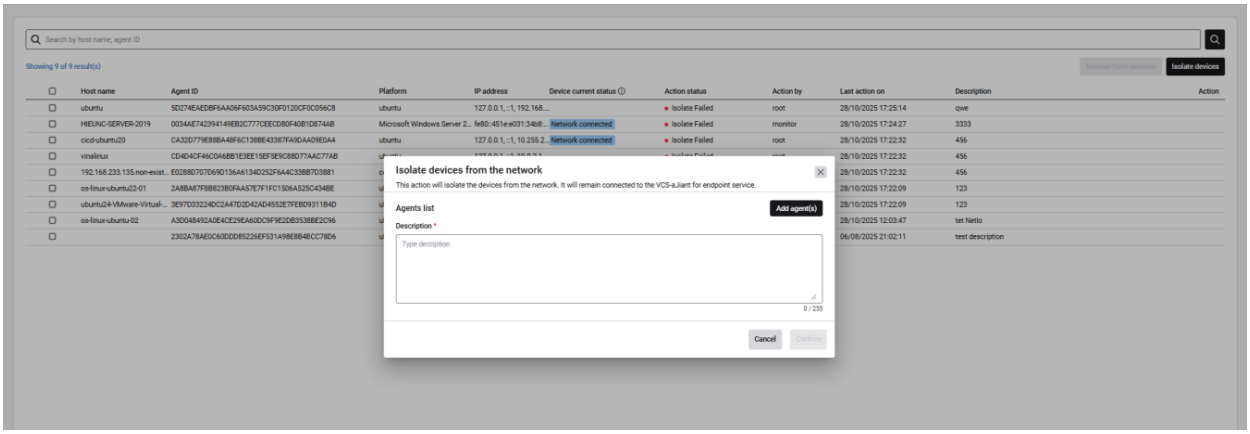
Mục đích: Cho phép SOC cô lập một thiết bị nghi ngờ bị xâm nhập khỏi mạng. Mục tiêu chính là ngăn chặn sự lây lan của mã độc, hạn chế giao tiếp nguy hiểm, đồng thời duy trì kết nối giữa thiết bị và hệ thống VCS-aJiant để tiếp tục điều tra, thu thập bằng chứng và khôi phục thiết bị.

3.5.2.1 **Tạo lệnh Isolate devices (cô lập)**

Bước 1: Truy cập vào menu Response -> chọn menu Isolate Devices



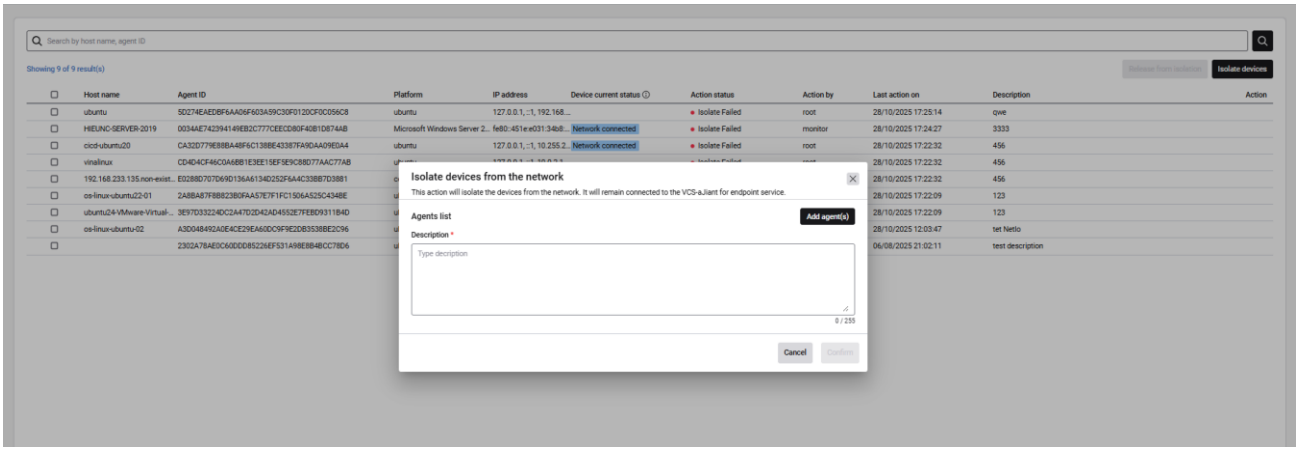
Bước 2: Chọn button Isolate devices

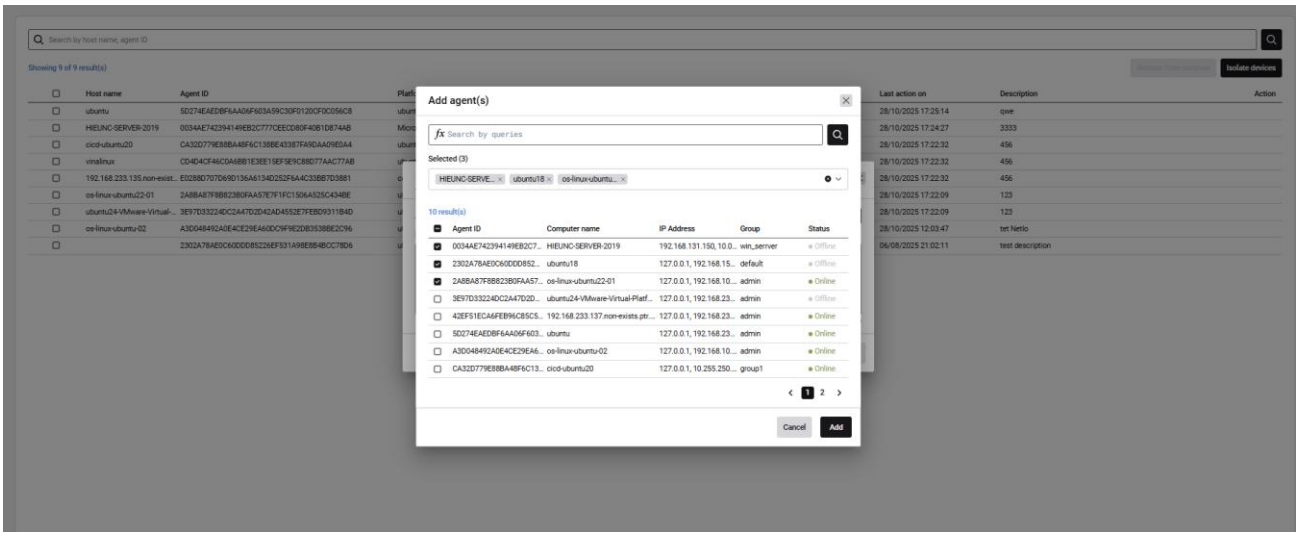


Bước 3: Nhập các thông tin cần thiết bao gồm

- Mô tả (bắt buộc)
- Chọn Agent(s)

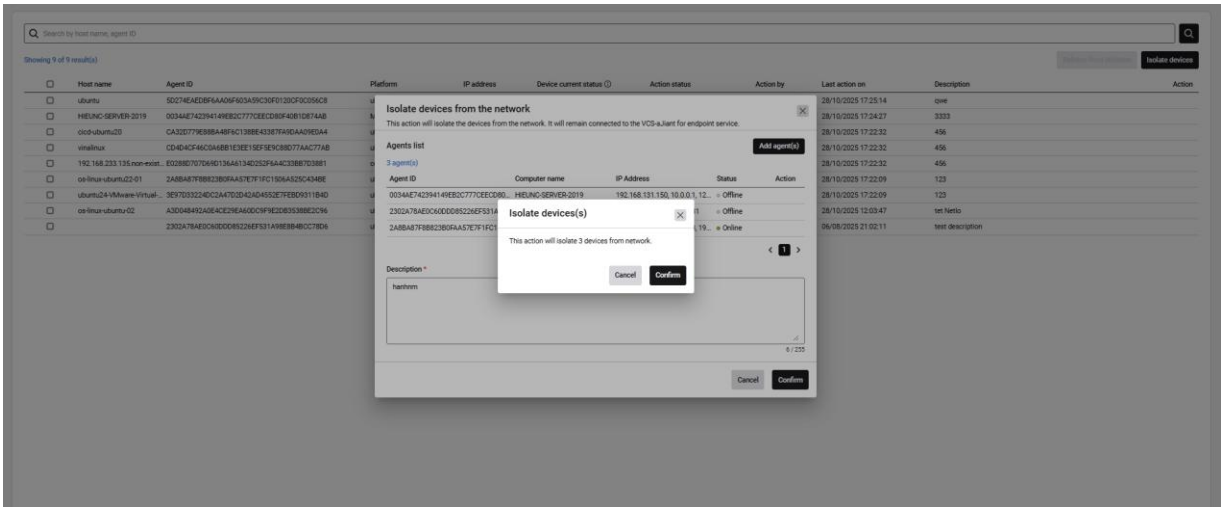
Lưu ý: User chỉ được phép thao tác với các agent được phân quyền





Bước 4: Xác nhận cô lập thiết bị

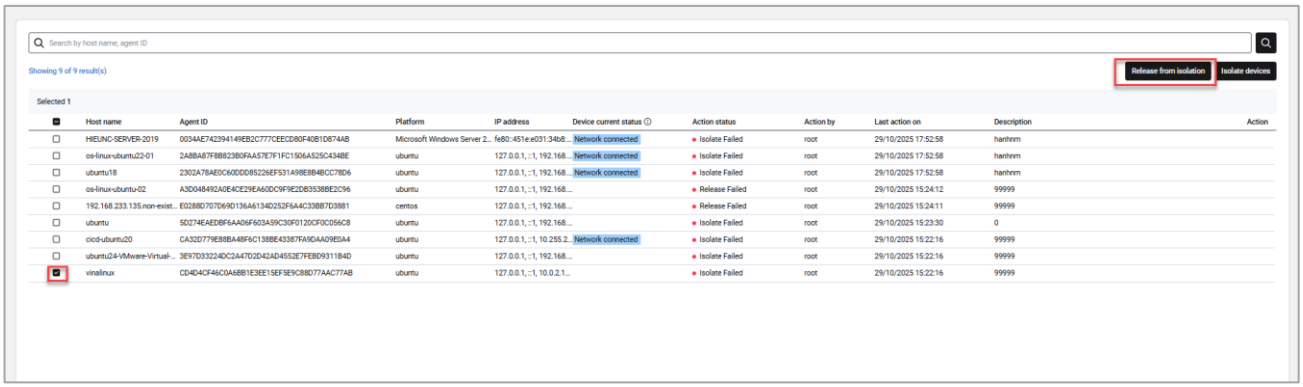
Người dùng nhấn Confirm để xác nhận thực hiện cô lập thiết bị.



3.5.2.2 Tạo lệnh Release isolation (bỏ cô lập)

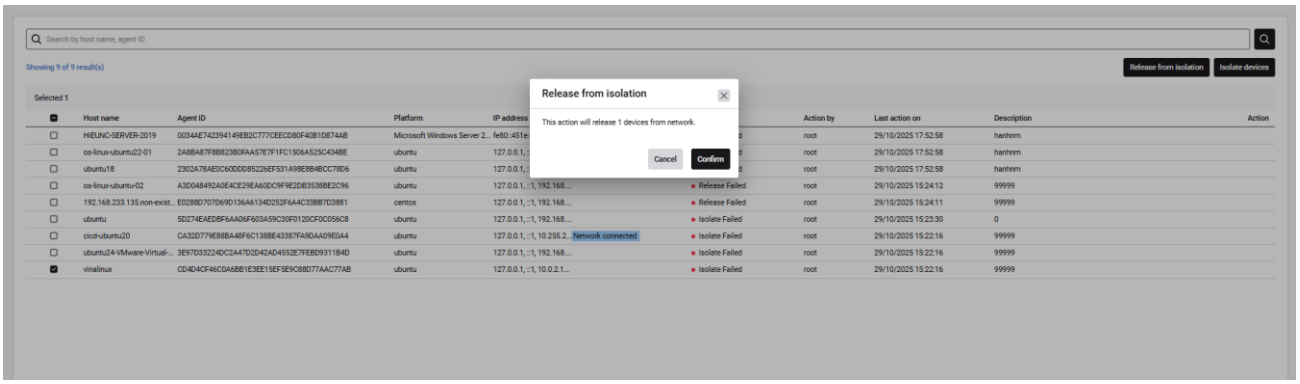
Người dùng có thể bỏ cô lập thiết bị như sau:

Bước 1: Trên danh sách, người dùng chọn một/ nhiều thiết bị muốn bỏ cô lập

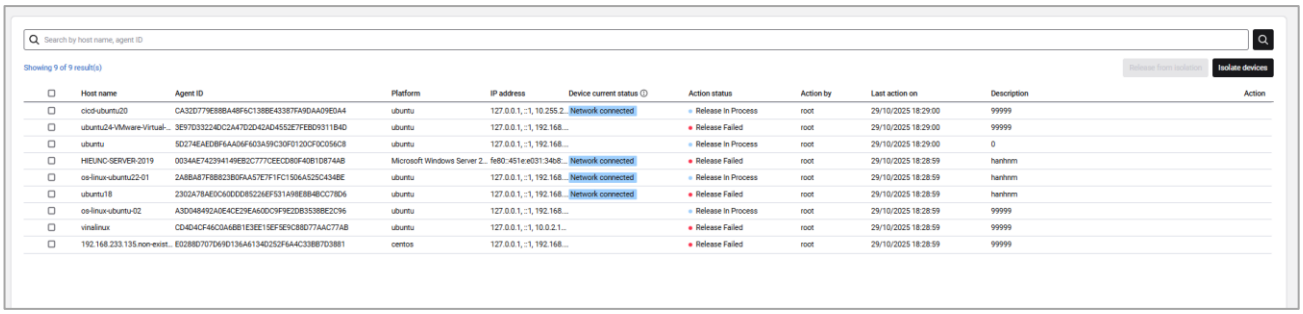


Bước 2: Chọn button Release from isolation-> thực hiện Xác nhận

Sau khi Xác nhận bỏ cô lập, hệ thống tiến hành bỏ cô lập thiết bị.



Người dùng có thể theo dõi trạng thái bỏ cô lập trên màn danh sách (như ảnh ví dụ phía dưới hệ thống đang thực thi lệnh bỏ cô lập)

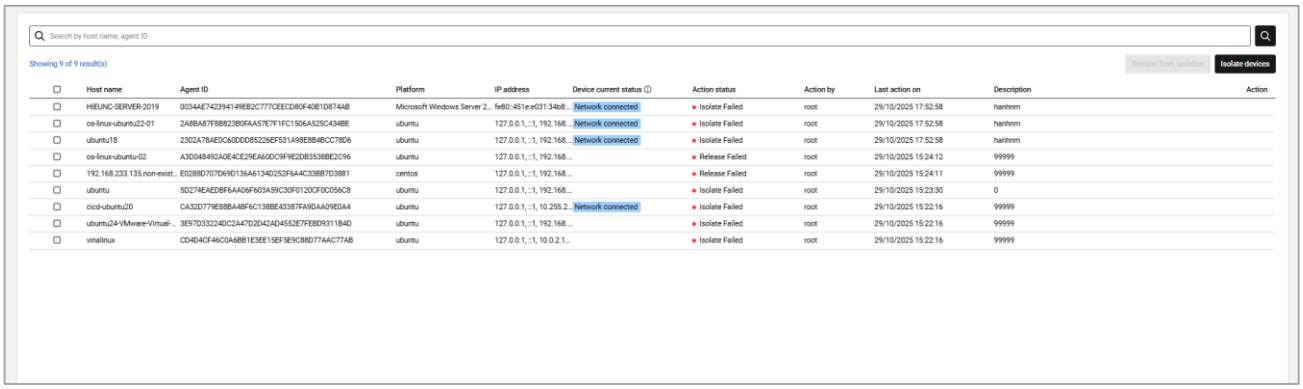


3.5.2.3 Kiểm tra thông tin cô lập/ bỏ cô lập thiết bị

Sau khi người dùng thực thi Isolate devices, thông tin thiết bị sẽ hiển thị trên danh sách, người dùng có thể kiểm tra các thông tin như sau:

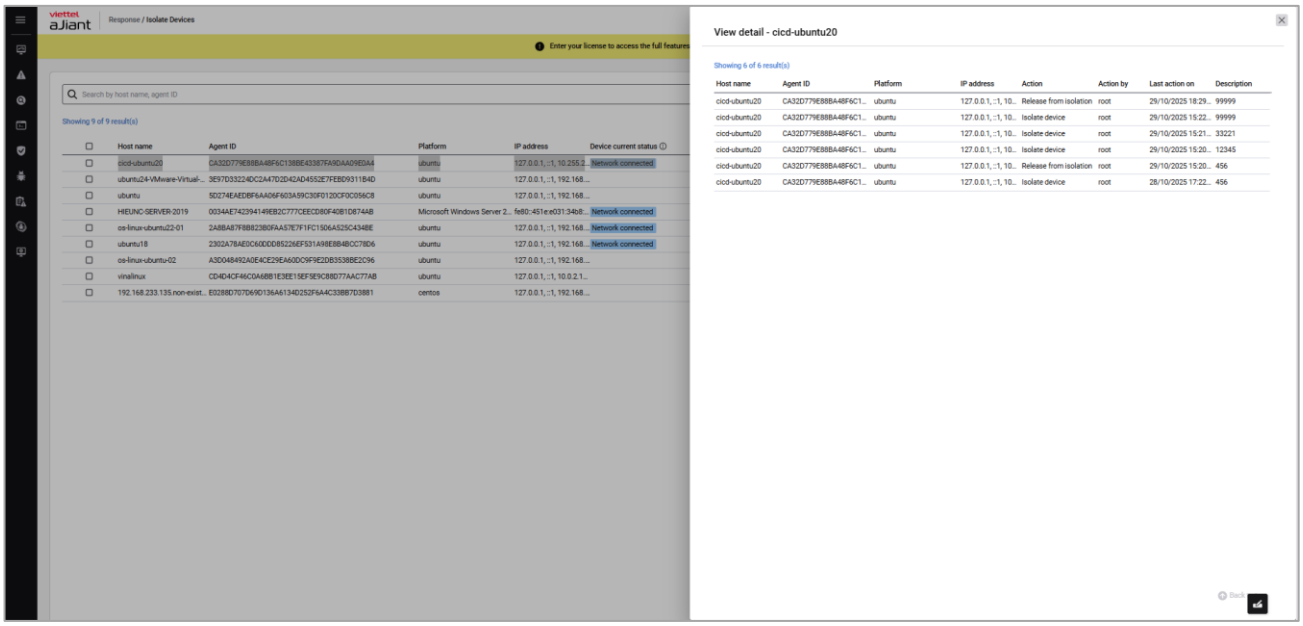
- **Host name**: thông tin tên máy bị tác động (cô lập/ bỏ cô lập)

- **Agent ID**: là ID máy bị tác động
- **Platform**: thông tin OS platform của thiết bị bị tác động
- **IP address**: thông tin IP thiết bị bị tác động
- **Device current status**: là trạng thái network thực tế của thiết bị có 2 trạng thái
    - Network connected: trạng thái kết nối mạng bình thường
    - Network isolated: thiết bị đã bị cô lập, đã ngắt kết nối mạng, chỉ có connect tới hệ thống VCS-aJiant
- **Action status**: là thể hiện trạng thái thực tế theo thao tác người dùng bao gồm các trạng thái sau
    - In process: là trạng thái thể hiện hệ thống đang thực thi yêu cầu người dùng (Isolate devices/ Release from isolation)
    - Applied: là trạng thái thể hiện hệ thống đã thực hiện thành công (Isolate devices/ Release from isolation) của người dùng
    - Fail: hệ thống thực hiện không thành công yêu cầu Isolate devices/ Release from isolation) của người dùng
- **Action by**: thông tin user thực thi
- **Last action on**: thời gian update cuối cùng của một bản ghi
- **Description**: mô tả



3.5.2.4 Xem danh sách lịch sử tác động theo thiết bị

Người dùng chọn Action View trên từng bản ghi-> xem danh sách lịch sử tác động theo thời gian (Isolate devices/ Release from isolation)

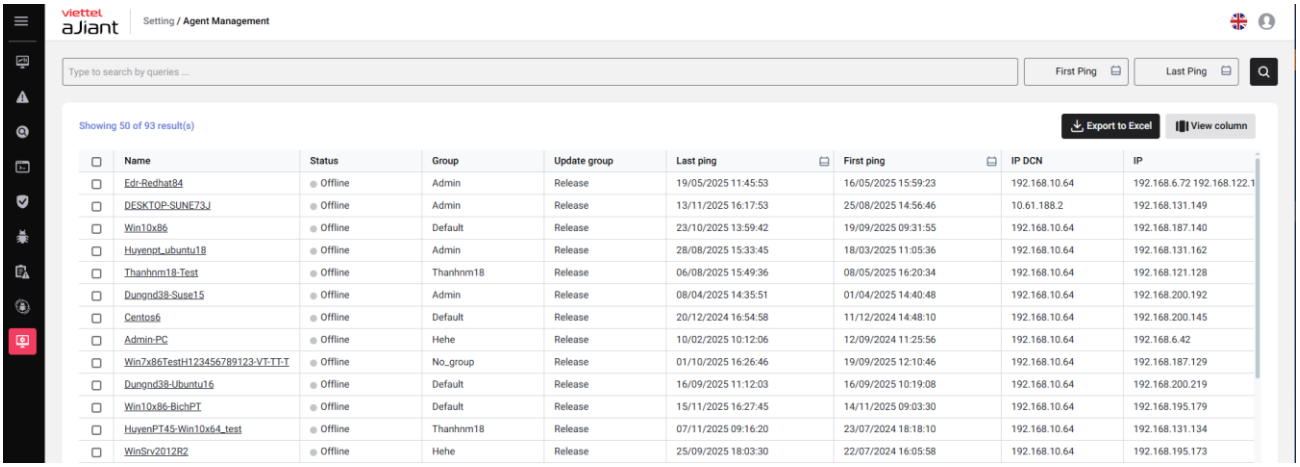


3.6 Nhóm chức năng Setting

3.6.1 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;

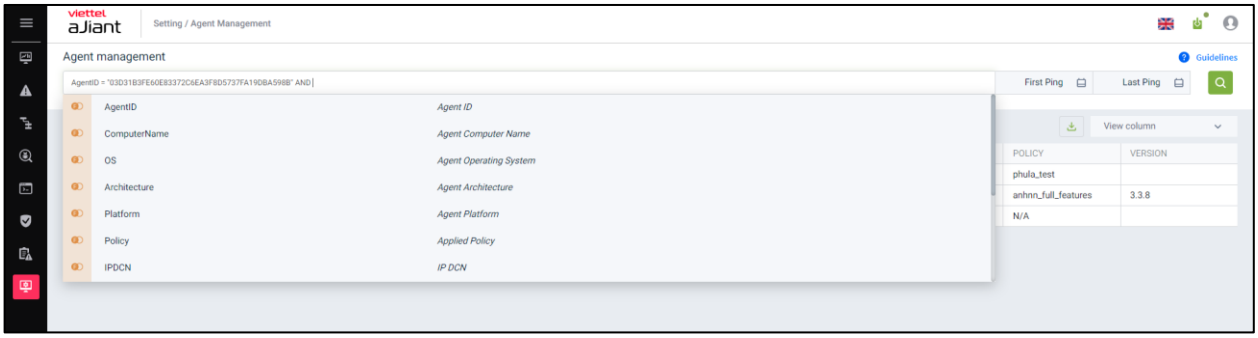
+ User đăng nhập thuộc group default: Hiển thị tất cả Agent thuộc group default;

+ 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;

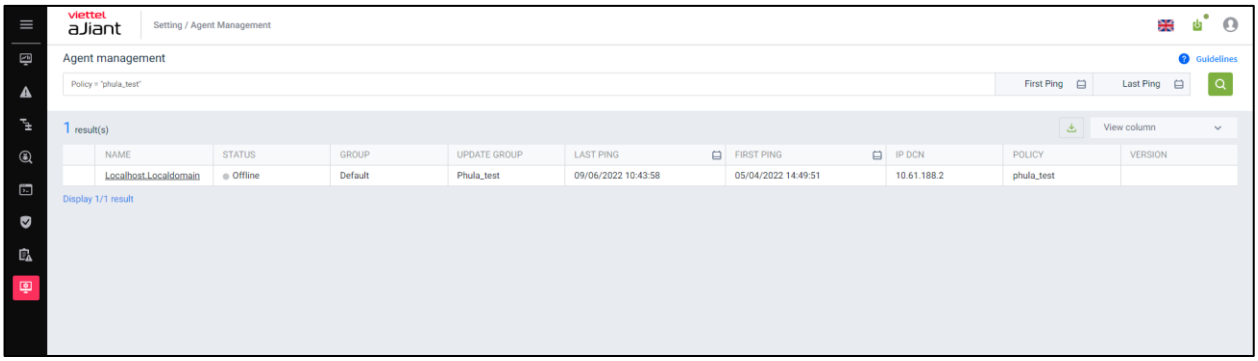
+ Mỗi agent được hiển thị các thông tin chung gồm: Name, Status, Group, Update Group, Last Ping, First Ping, DNS, Policy, AgentID, PlatForm, PlatForm Version, Architecture, DNS, Version, IP, License.

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 “=”, “!=”, “~”;

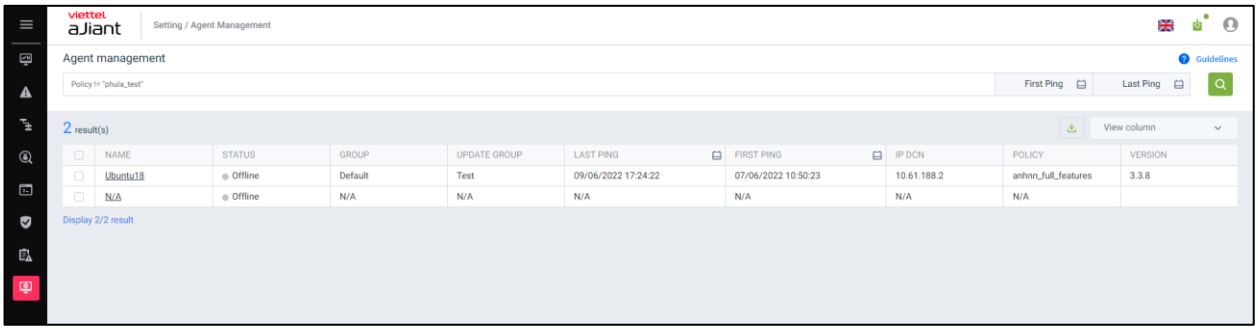


Ví dụ về các câu tìm kiếm:

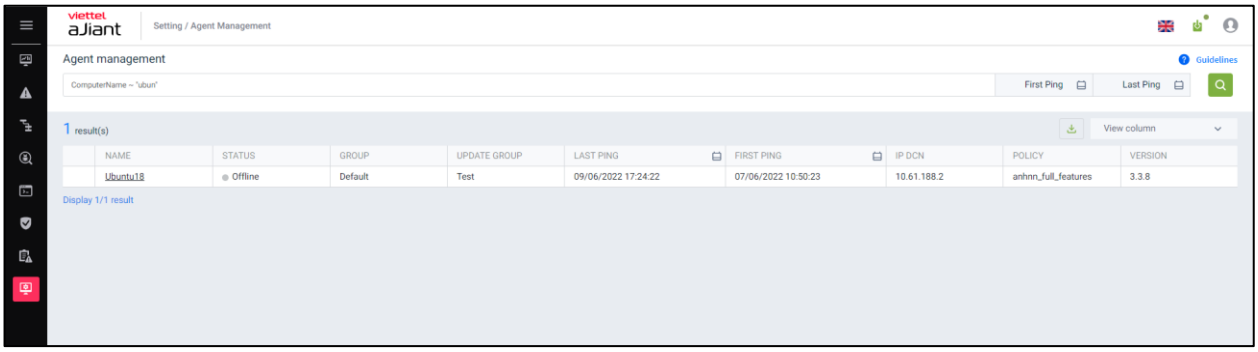
+ Tìm kiếm với điều kiện “=”:



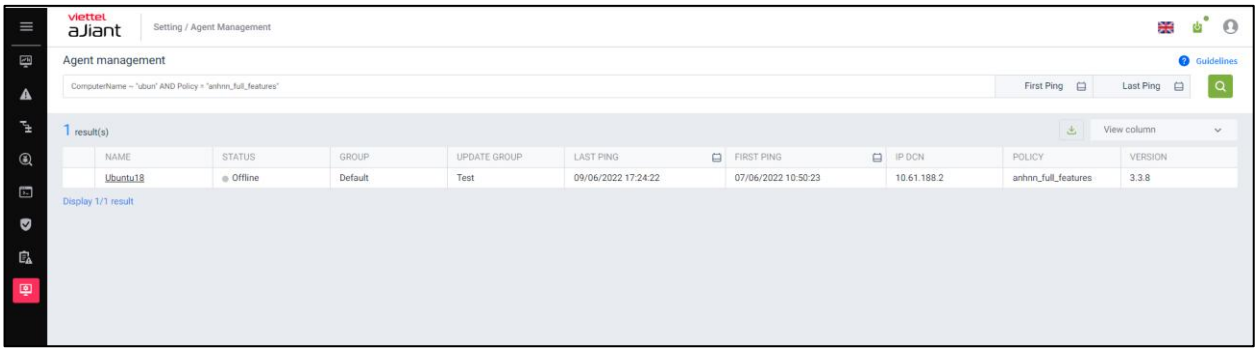
+ Tìm kiếm với điều kiện "!=":



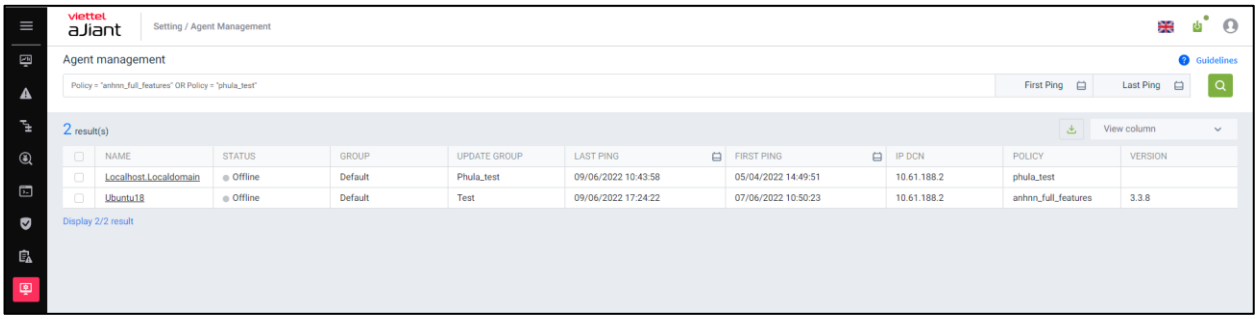
+ Tìm kiếm với điều kiện "~":



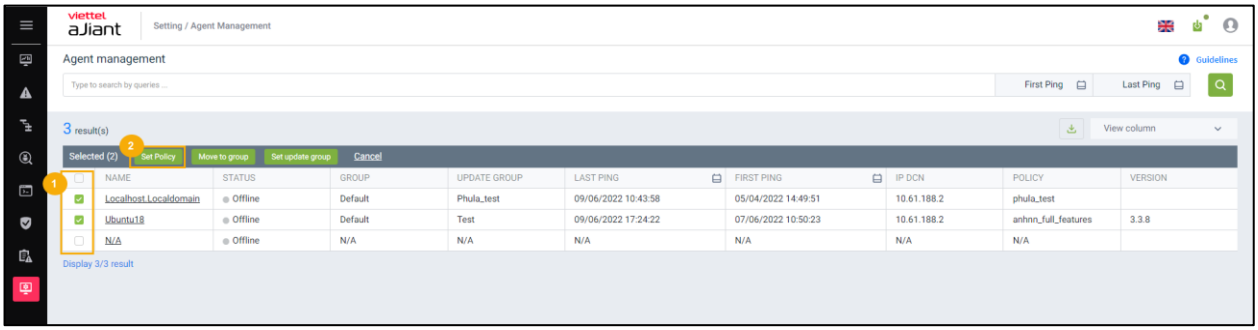
+ Tìm kiếm theo tiêu chí kết hợp AND:



+ Tìm kiếm theo tiêu chí kết hợp OR:



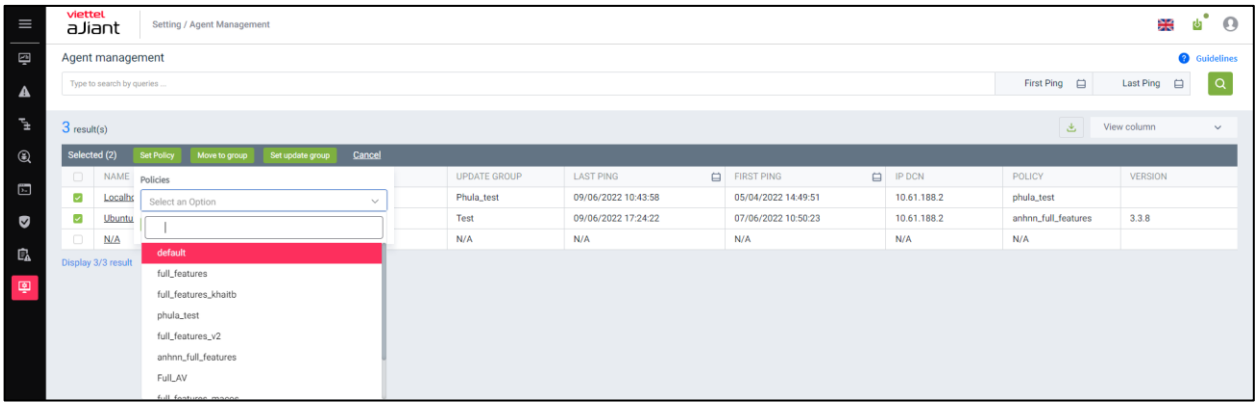
3 – Chọn nhanh 1 agent/ 1 nhóm các agent để thiết lập Policy



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

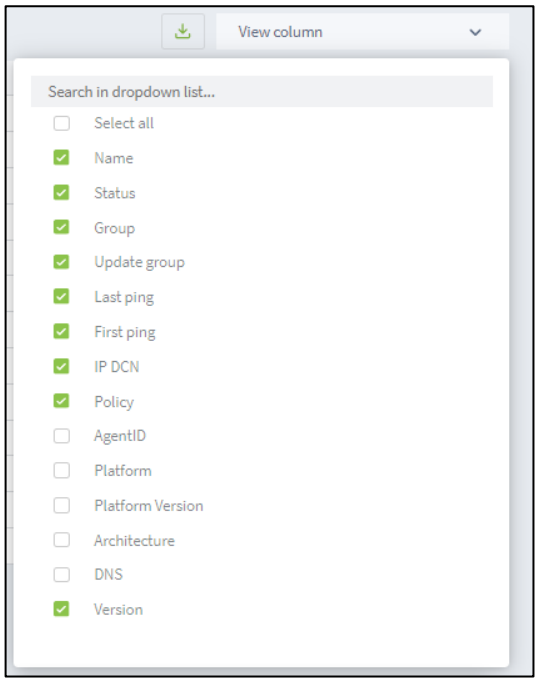
+ Thực hiện Set Policy:

  - 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.

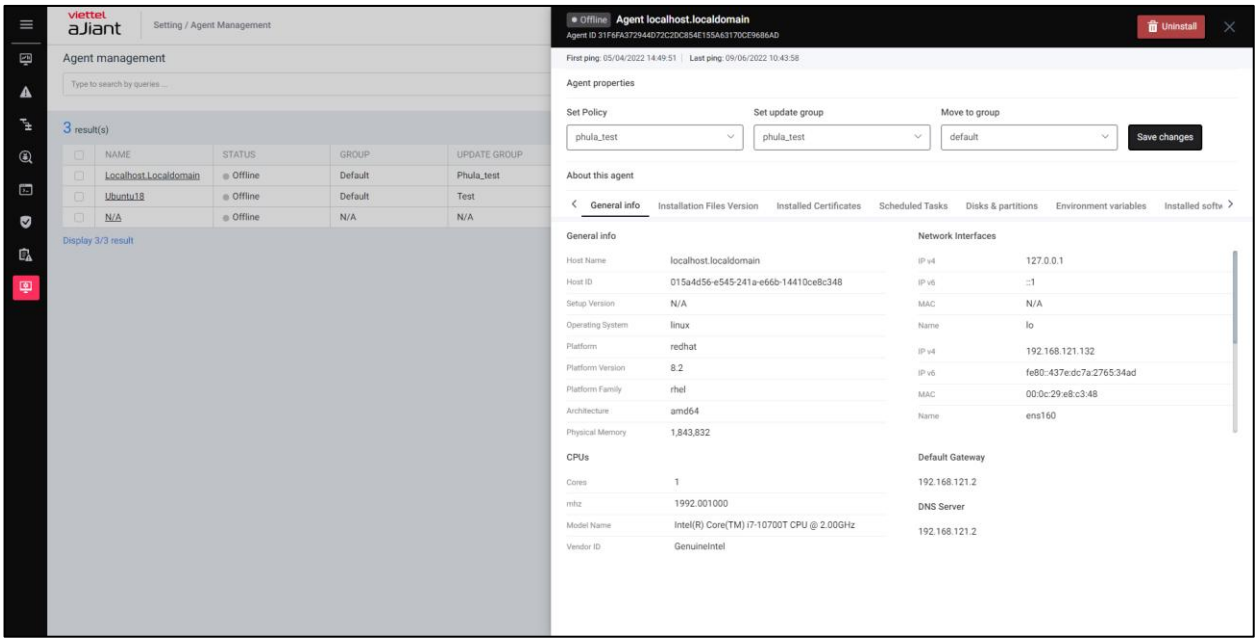
+ User đăng nhập thuộc group root: Hiển thị tất cả Group trong hệ thống;
+ User đăng nhập thuộc group default: Hiển thị Group default;

+ 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

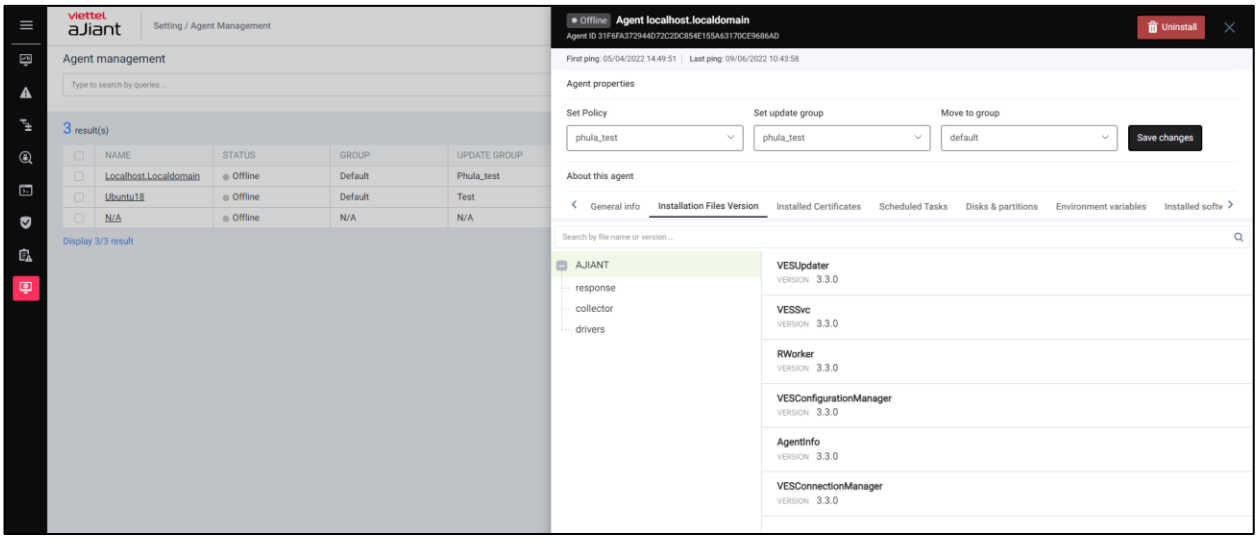
+ Hệ thống hiển thị các thông tin chung về agent gồm: Các thông tin chung, CPUs, Network Interfaces, Default Gateway, DNS Server;



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;

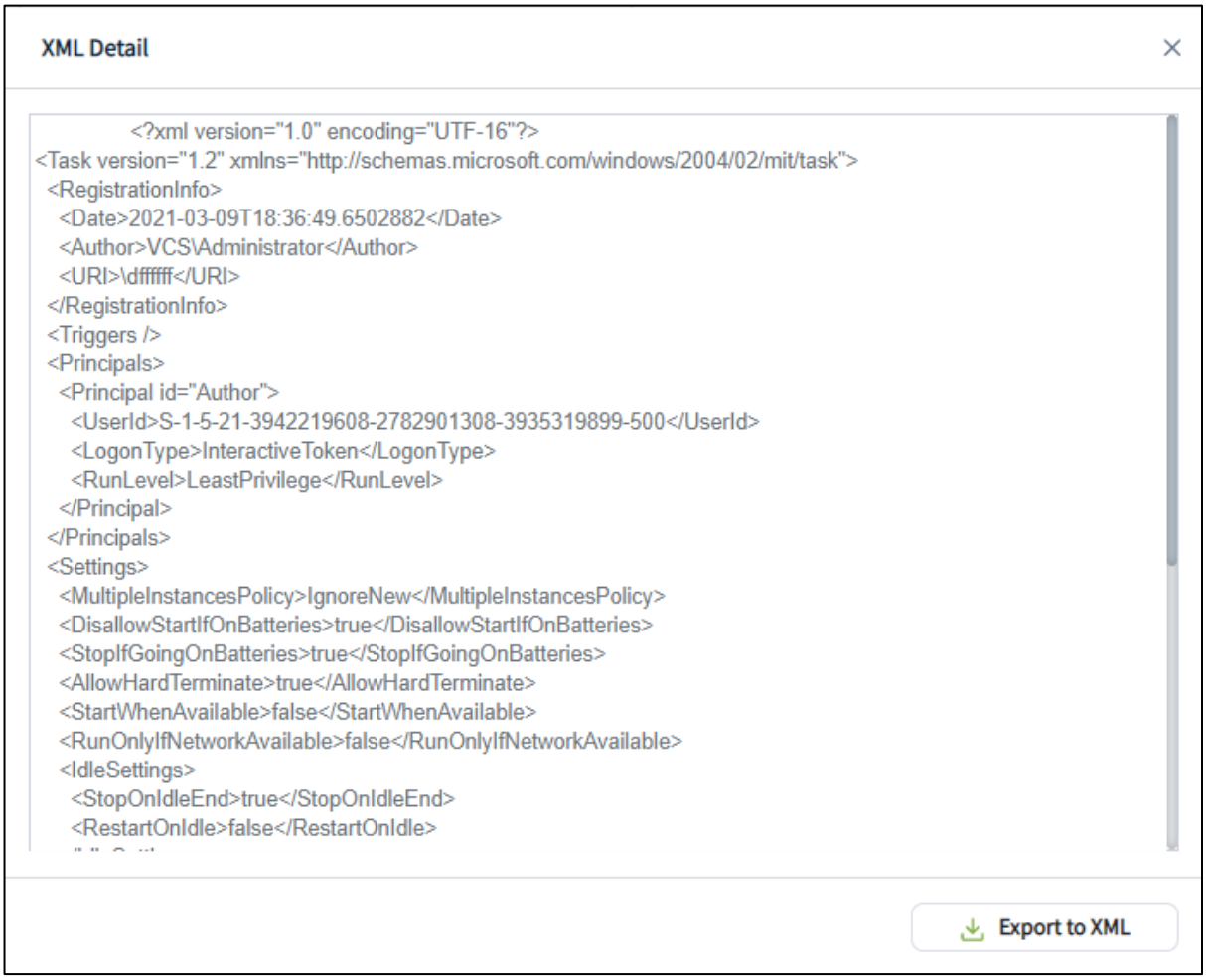
+ Trường hợp muốn xem chi tiết với nhiều thông tin hơn, chọn , hiển thị màn hình như sau:

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

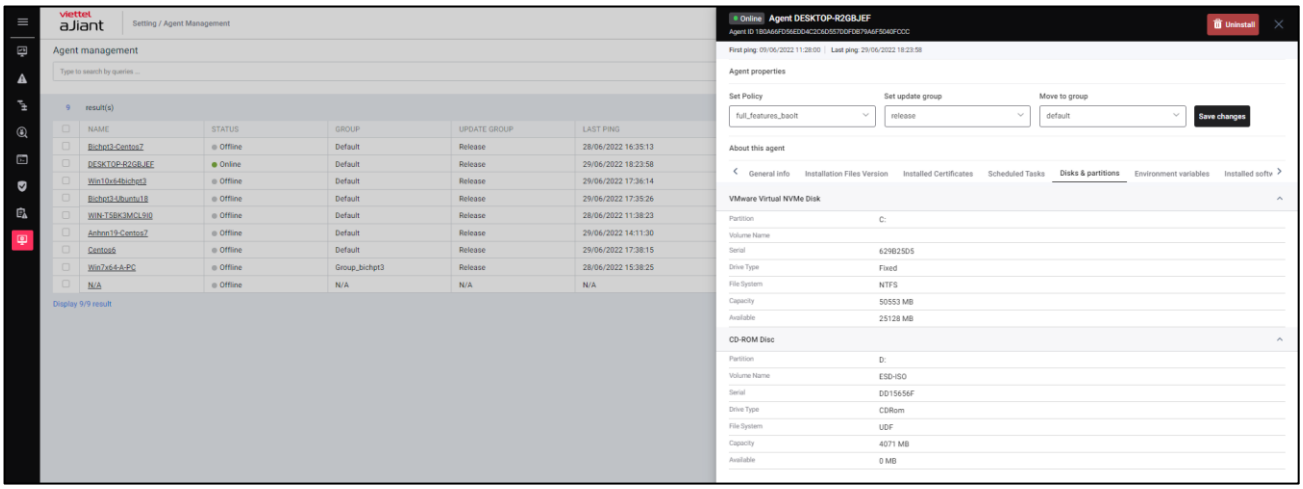


+ Chọn Export to XML để tải về thông tin scheduled task, hỗ trợ định dạng .xml

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

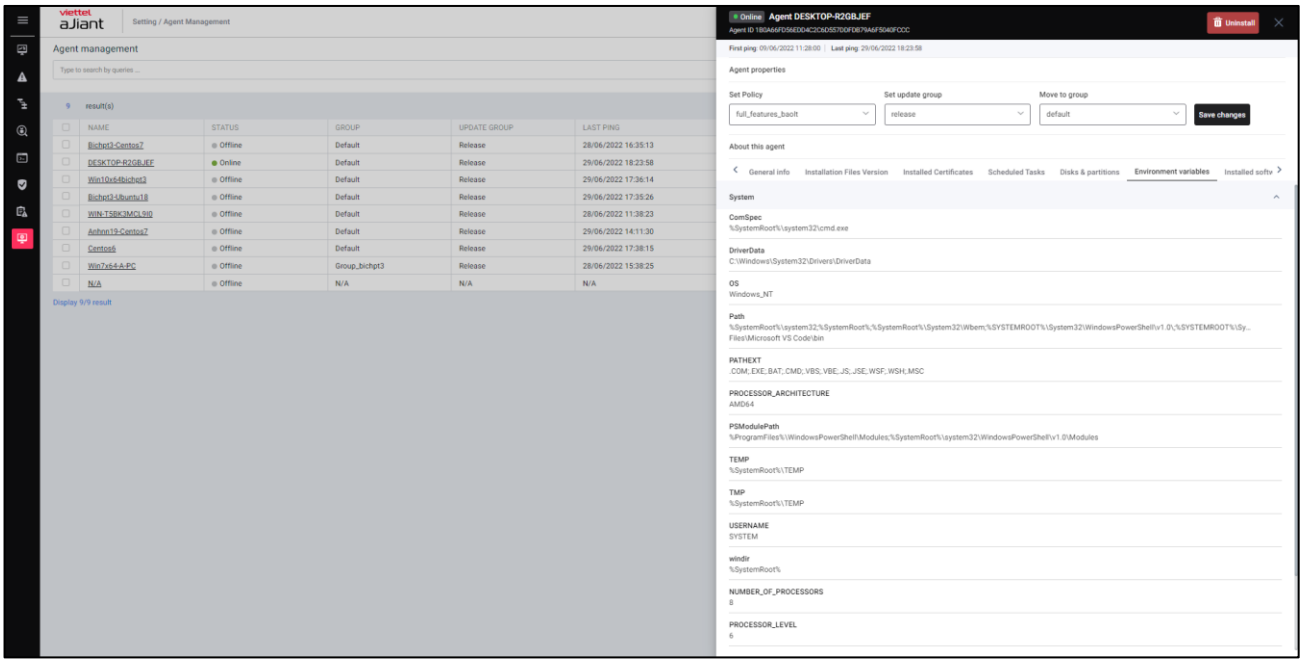
+ Chọn ^ hoặc v để tùy chỉnh việc hiển thị thông tin bổ sung cho từng disk.



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;

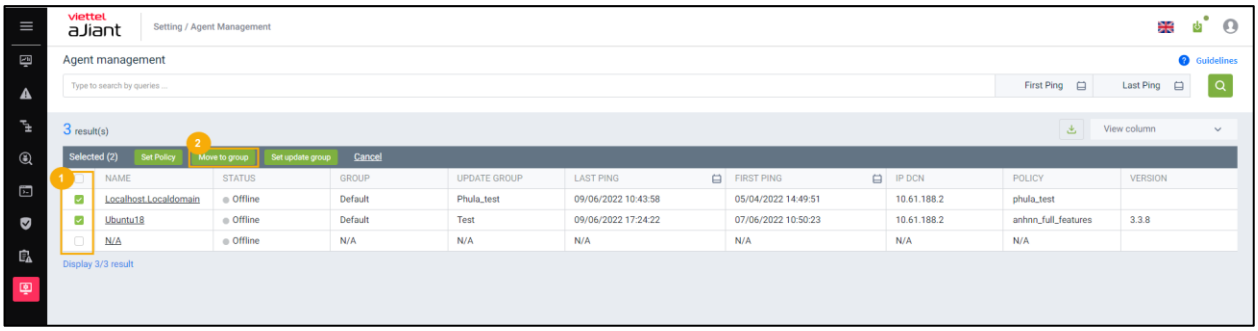
+ Hỗ trợ search nhanh phần mềm bắt buộc chưa cài đặt trên máy hoặc nhập tên phần mềm vào text box search.

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:

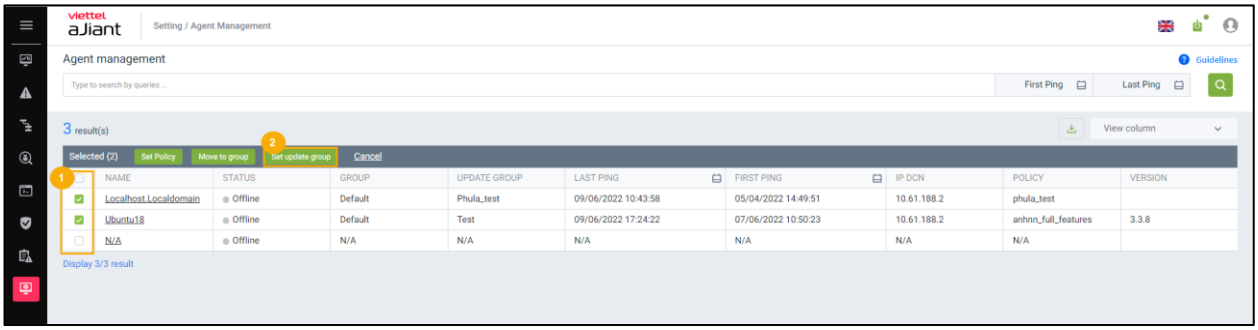
- User đăng nhập thuộc group root: Hiển thị tất cả Group trong hệ thống;
- User đăng nhập thuộc group default: Hiển thị Group default;

- 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.

Cách tính license VCS-ajiant:

+ License sẽ được tính theo số lượng endpoint (ví dụ khách mua license 10 endpoint, khách hàng sẽ được cài agent trên 10 thiết bị)

+ Hệ thống sẽ tính license cho agent theo thời gian agent kết nối tới hệ thống VCS-aJiant (thời gian first ping, agent kết nối trước sẽ được gán license trước

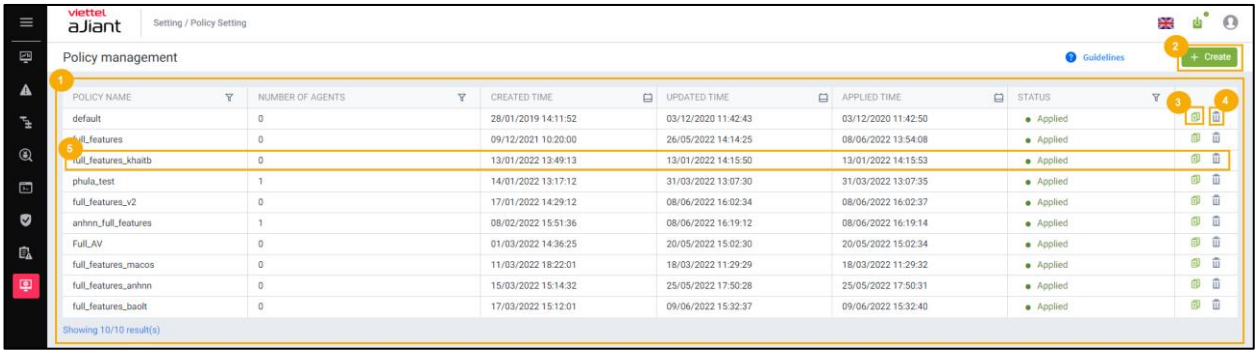
Trong trường hợp:

+ 1. Nếu khách hàng cài quá số lượng license: các tính năng detection, prevention, response... sẽ không hoạt động trên các thiết bị này

+ 2. Nếu license hết hạn: hệ thống tự động tắt toàn bộ tính năng trên toàn bộ thiết bị cho tới khi license được gia hạn, khách hàng nhìn thấy agent online trên portal.

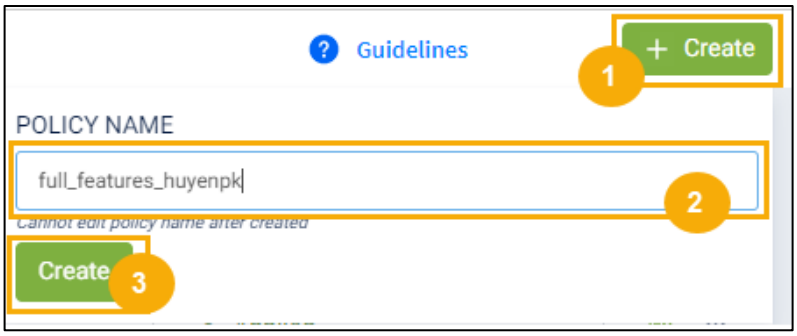
3.6.2 Policy Setting

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:



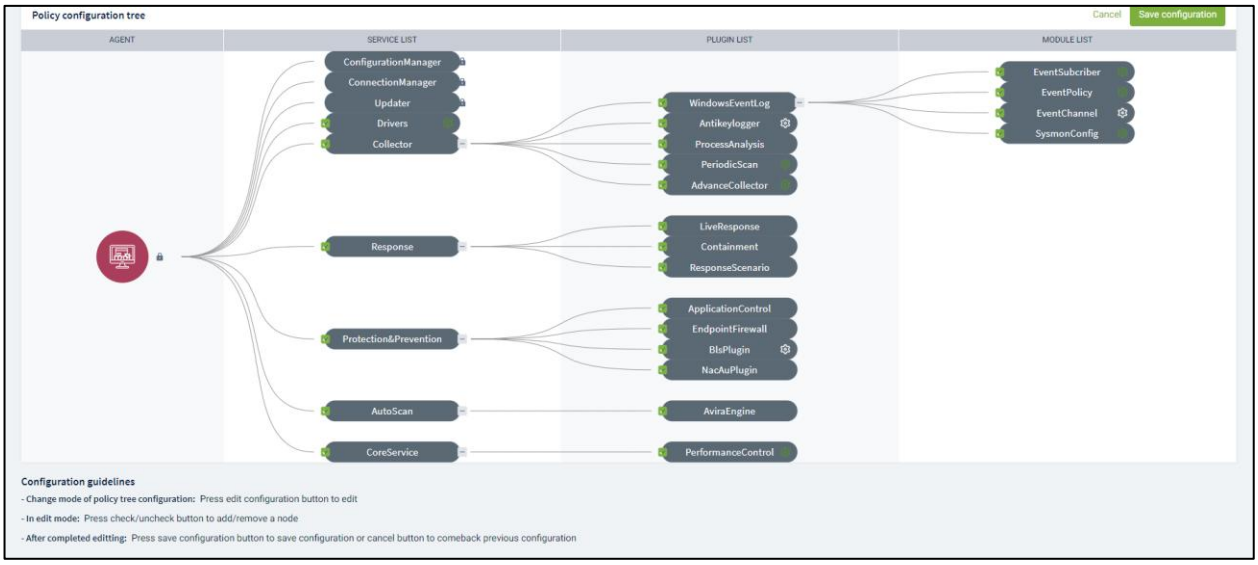
1 – Hiển thị danh sách các Policy đã được tạo trên hệ thống. Mỗi 1 policy gồm các thông tin: Tên, số lượng Agent được áp chính sách, Thời gian tạo, thời gian cập nhật, Thời gian áp chính sách, trạng thái (có 2 trạng thái: Applied và Not Applied);

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.

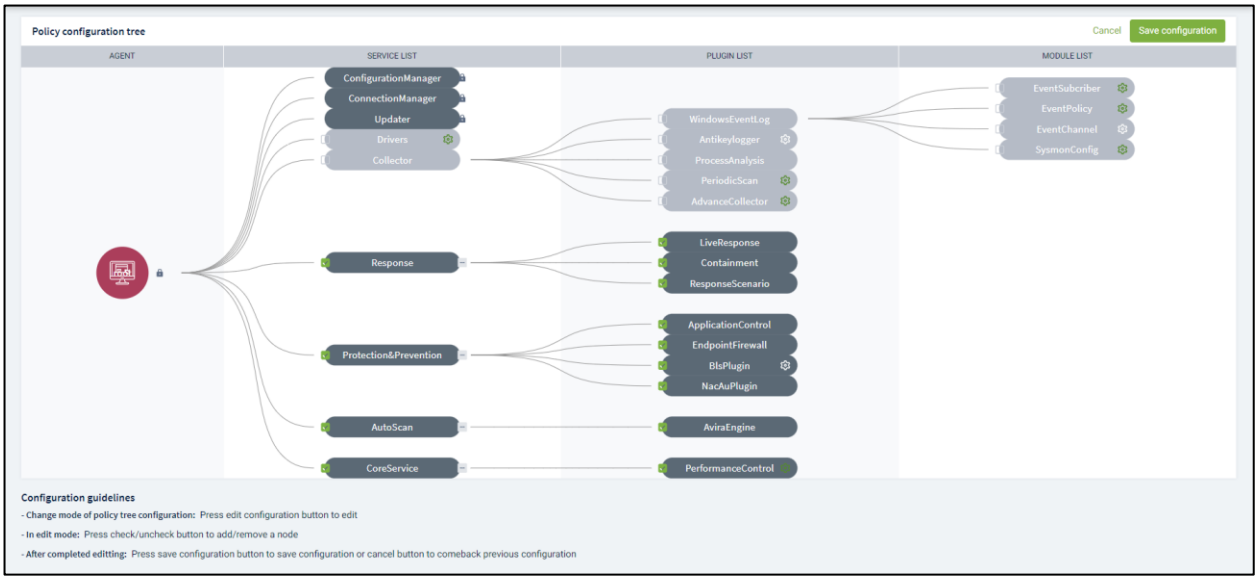
Sau khi tạo mới policy thành công hệ thống sẽ hiển thị màn hình chi tiết của 1 policy:



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:



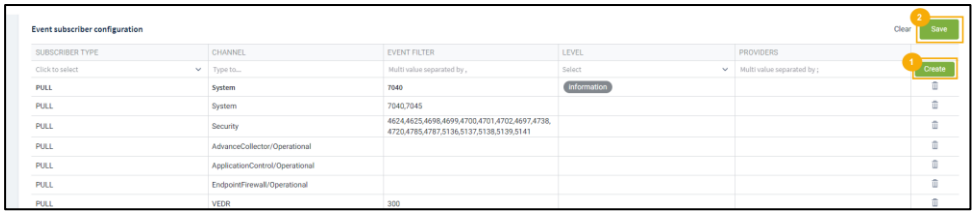
Bước 3: Sau khi hoàn thành chế độ edit:

- 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.

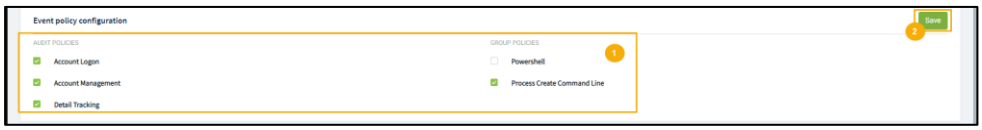
Module/plugin	**Mô tả**
WindowsEvent Log	- **Cấu hình WindowsEventLog**: Lấu hình các nguồn log lấy dưới Agent + EventSubcriber: chỉ định các kênh lấy log Yêu cầu dữ liệu: + Trường **event_filter** (lọc theo Event ID): các string con cách nhau dấu phẩy (,); VD: "4": lọc các event có eventID = 4 "-689": 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;

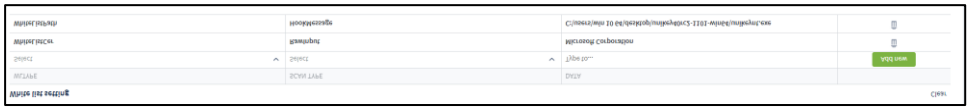
- Yêu cầu: có ít nhất 1 trường được chọn



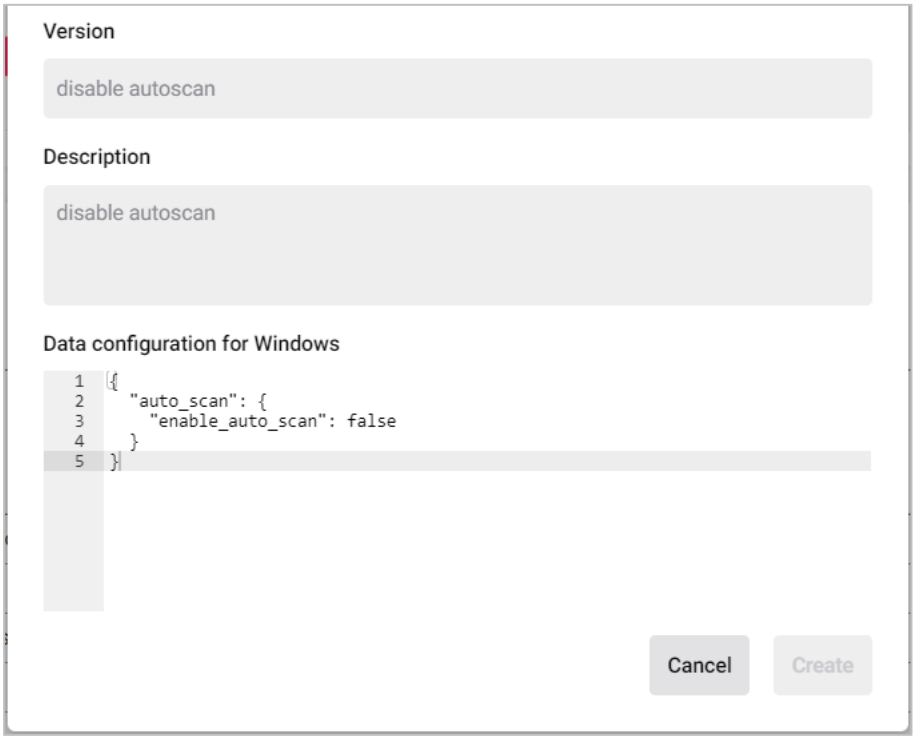
+ EventChannel: cấu hình chi tiết 1 số nguồn log:

- 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	**Cấu hình 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: o Scan cycle: min là 1 phút, max là 180 phút; o 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	**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;
Autoscan	**Cấu hình Autoscan:** cho phép người dùng bổ sung thêm các config khi quét mã độc -Yêu cầu: Lựa chọn Autoscan -> Add new configuration. Các thông tin cần thêm mới bao gồm + Version + Description + Data config for Windows sẽ có format ví dụ như sau

Lưu ý: Với các config của luồng quét mã độc tự động hoặc manual cần nằm trong key “auto_scan” / “manual_scan” tương ứng



Các trường hỗ trợ config trong luồng auto scan như sau:

Config	Type	Mô tả
enable_auto_scan	bool	bật/tắt auto scan
max_queue_length	integer	số lượng phần tử tối đa của scan queue và disinfect queue
scan_sleep_time	mili-second	thời gian sleep giữa 2 lần scan file, tránh xử lý liên tục gây cao tải hệ thống
scan_timeout	mili-second	thời gian tối đa cho phép av engine scan một file
scan_max_filesize	byte	kích thước file được scan tối đa, file lớn hơn kích thước này sẽ bỏ qua ko scan

rescan_removal_failed	integer	số lần tối đa lặp lại việc scan & disinfect file có trạng thái RemovalFailed, nhằm cố gắng thử lại việc xóa file mã độc
rescan_disinfected	integer	số lần tối đa lặp lại việc scan & disinfect file có trạng thái Disinfected, tránh việc disinfected lỗi dẫn tới scan & disinfect một file vô hạn lần
rescan_not_processed	second	thời gian scan lại file ở trạng thái not processed
disinfect_sleep_time	mili-second	thời gian sleep giữa 2 lần disinfect file, tránh xử lý liên tục gây cao tải hệ thống
disinfect_timeout	mili-second	thời gian tối đa cho phép av engine disinfect một file

Các trường hỗ trợ config cho luồng quét thủ công như sau

Config	Type	Mô tả
max_manual_scan	integer	số lượng manual scan tối đa đồng thời
max_queue_length	integer	độ dài tối đa của manual scan queue
scan_sleep_time	mili-second	thời gian sleep trước khi scan file tiếp theo, tránh xử lý liên tục gây cao tải hệ thống
scan_timeout	mili-second	thời gian tối đa cho phép av engine scan một file

<table>
<tr><td></td><td>
<table>
<tr><td>rescan_disinfected</td><td>integer</td><td>số lần tối đa lặp lại việc scan & disinfect file có trạng thái Disinfected, tránh việc disinfected lỗi dẫn tới scan & disinfect một file vô hạn lần</td></tr>
</table>
</td></tr>
<tr><td>AntiRansomware</td><td>
AntiRansomwaer: cho phép thay đổi các config khi diệt mã độc mã hóa tống tiền
- Yêu cầu: Chọn Auto Scan -> chọn Anti Ransomware
Các trường hỗ trợ config như sau:
<table>
<tr><th>Config</th><th>Type</th><th>Mô tả</th></tr>
<tr><td>silent</td><td>bool</td><td>bật tắt chế độ hoạt động silent</td></tr>
<tr><td>protect_ext</td><td>string list</td><td>danh sách đuôi file được bảo vệ</td></tr>
<tr><td>protect_whitelist</td><td>string list</td><td>danh sách folder được white list không bảo vệ</td></tr>
<tr><td>actor_whitelist</td><td>string list</td><td>danh sách file, folder chứa process được phép thực hiện hành vi</td></tr>
</table>
</td></tr>
<tr><td>HIPS</td><td>HIPS: cho phép thay đổi config khi diệt mã độc dựa trên hành vi</td></tr>
</table>

<table>
<tr><td></td><td>
- Yêu càu: Chọn Auto Scan -> chọn HIPS

Các trường hỗ trợ config như sau:

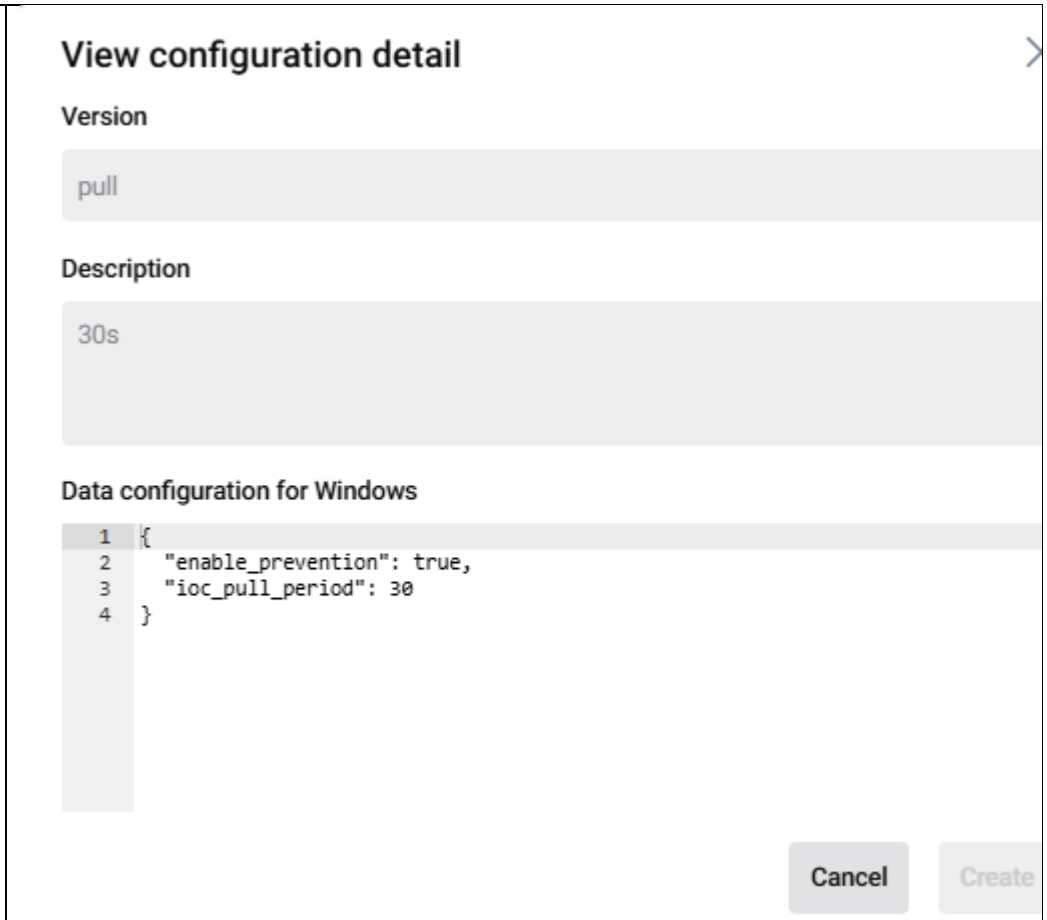
<table>
<tr><th>Config</th><th>Type</th><th>Mô tả</th></tr>
<tr><td>silent</td><td>bool</td><td>bật tắt chế độ hoạt động silent</td></tr>
</table>
</td></tr>
<tr><td>Performance control linux</td><td>
+ Performance control là module thực hiện chức năng monitor, giới hạn các tài nguyên mà từng service của EDR được sử dụng trên máy người dùng. Các thông số giới hạn về lượng tài nguyên được cấu hình trên portal:

- Config ngưỡng cho CPU: Cho phép người dùng cấu hình mức giới hạn CPU cho từng agent. Agent sẽ hoạt động trong phạm vi cấu hình, không vượt ngưỡng CPU đã đặt
- Config ngưỡng cho MEM: Cho phép người dùng cấu hình mức giới hạn bộ nhớ (Memory limit) cho process. Khi mức sử dụng bộ nhớ vượt ngưỡng cấu hình, process sẽ tự động bị restart để giải phóng tài nguyên.
- Config cho giá trị FD: Cho phép người dùng cấu hình mức giới hạn file được mở bởi process. Khi mức sử dụng bộ nhớ vượt ngưỡng cấu hình, process sẽ tự động bị restart để giải phóng tài nguyên.
- Config giá trị DiskIO: Cho phép người dùng giới hạn tốc độ truy xuất đĩa (đọc/ghi) của process. Process sẽ giảm tốc độ (throttling) dưới giá trị config
- Config giá trị Network: Giới hạn tốc độ mạng mà process có thể xử lý trong mỗi giây. Process sẽ giảm tốc độ (throttling) dưới giá trị config
- Yêu cầu: Chọn CoreService-> chọn PerformanceControl

Các trường hỗ trợ config như sau:

<table>
<tr><th>STT</th><th>Cấu hình</th><th>Kiểu giá trị</th><th>Ý nghĩa</th></tr>
</table>
</td></tr>
</table>

		1	Process name	String	Tên process được quản lý
		2	Cpu peak	Int	Ngưỡng cpu
		3	Cpu Avr	Int	Ngưỡng cpu trung bình
		4	Memory peak	int	Ngưỡng memory
		5	Memory Avr	Int	Ngưỡng memory trung bình
		6	Disk IO peak	Int	Ngưỡng io peak
		7	Disk IO Avr	int	Ngưỡng io trung bình
		8	Network Peak	Int	Ngưỡng network
		9	Network Avr	Int	Ngưỡng network trung bình
		10	deltatime_cpu	Int	Time đo cpu
		11	deltatime_memory	Int	Time đo mem
		12	deltatime_disk_io	Int	Time đo io
		13	deltatime_network	Int	Time đo net
Prevention Known Threat	+ **Prevention Known Threat** là tính năng hỗ trợ phát hiện các hành vi tấn công hoặc mã độc đã được công bố/ghi nhận trên thế giới thể hiện qua IOC dạng hash - Yêu cầu: Lựa chọn Autoscan -> chọn IocEngine. - Trường hợp không có config thì sẽ IocEngine sẽ sử dụng config mặc định - Trường hợp thêm config, chọn IocEngine -> Add new configuration. Các thông tin cần thêm mới bao gồm + Version + Description + Data config for Windows sẽ có format ví dụ như sau				



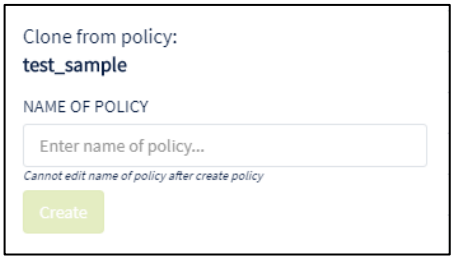
Các trường hỗ trợ config trong luồng IocEngine như sau:

Config	Type	Mô tả	Mặc định
enable_prevention	bool	bật tắt chế độ chặn IOC độc	false
revoke_ttl	integer	thời gian tối đa mà revoke list có hiệu lực	7*24 (7 days)
max_file_size	integer	kích thước file được scan tối đa, file lớn hơn kích thước này sẽ bỏ qua không scan IOC	10MB
whitelist_ioc	string array	danh sách các hash được whitelist	Empty list
max_hash_speed	integer	tốc độ đọc file tính hash tối đa	512 KB/s
max_queue_length	integer	số lượng phần tử tối đa của IOC scan queue	10.000
delay_scan_time	integer	thời gian delay trước khi retry scan IOC với file bị quét lỗi	10 second

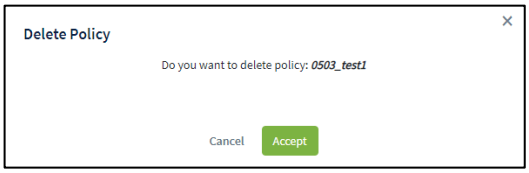
	max_cache_size	integer	số lượng phần tử tối đa của IOC scan cache	100000
	ioc_pull_period	integer	chu kỳ pull IOC DB từ backend	600(10 minutes)
	disinfect_timeout_ms	integer	thời gian cố gắng xóa IOC	3000 milisecond
	rescan_timeout_min	integer	thời gian không quét lại một file khi đã quét xong	5 minute
	disinfect_retry_interval_hour	integer	thời gian không thử lại khi xóa thất bại một IOC độc	24 hour
	scan_sleep_time_ms	integer	thời gian delay giữa mỗi lần quét	50 milisecond
Fileless	+ **Phát hiện kỹ thuật fileless** là tính năng giúp phát hiện các hành vi mã độc ẩn mình, vượt qua antivirus và chiếm quyền thực thi - Yêu cầu: Lựa chọn VESCollector -> chọn MemmoryScanner.			

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

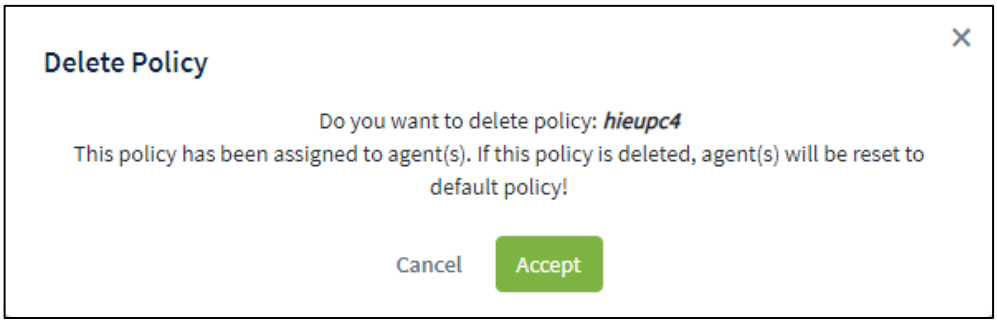
+ Clone chính sách mới: Click vào nút hệ thống sao chép toàn bộ chi tiết của policy được clone ngoại trừ tên policy.



+ 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.

3.6.3 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.

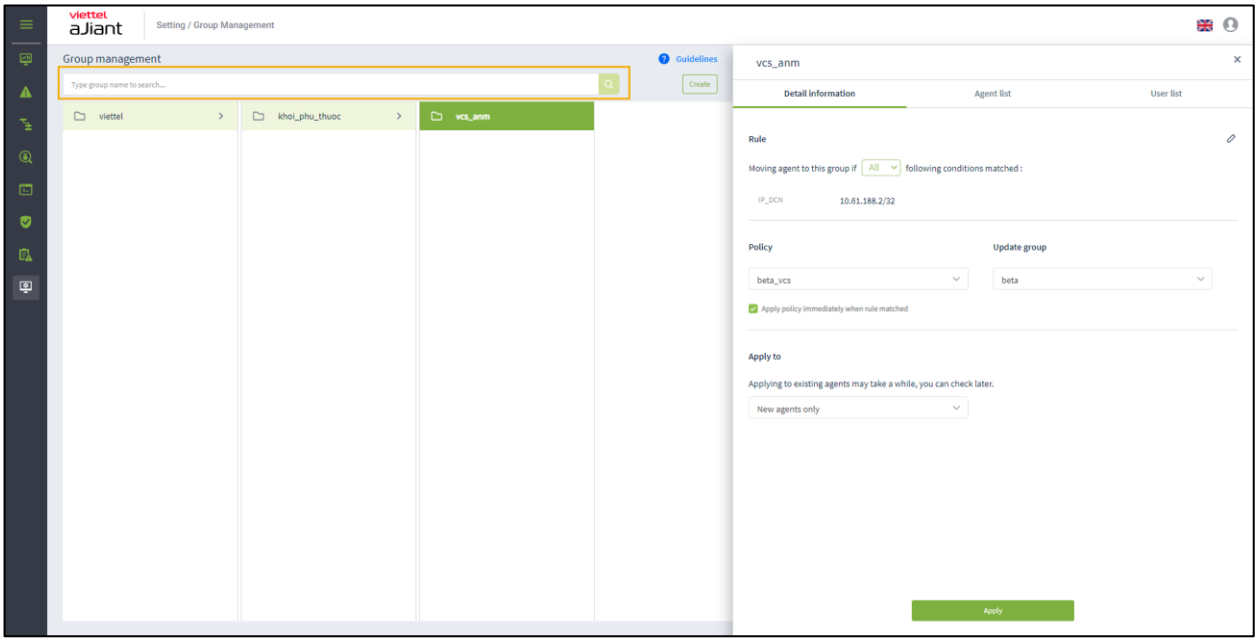
Các rule của nhóm là độc lập giữa các nhóm (không có kế thừa cha con). Việc quản lý nhóm theo cây để quản lý dễ dàng hơn khi số lượng agent lớn và có sự phân cấp về quản lý agent theo công ty, phòng, ban…

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;

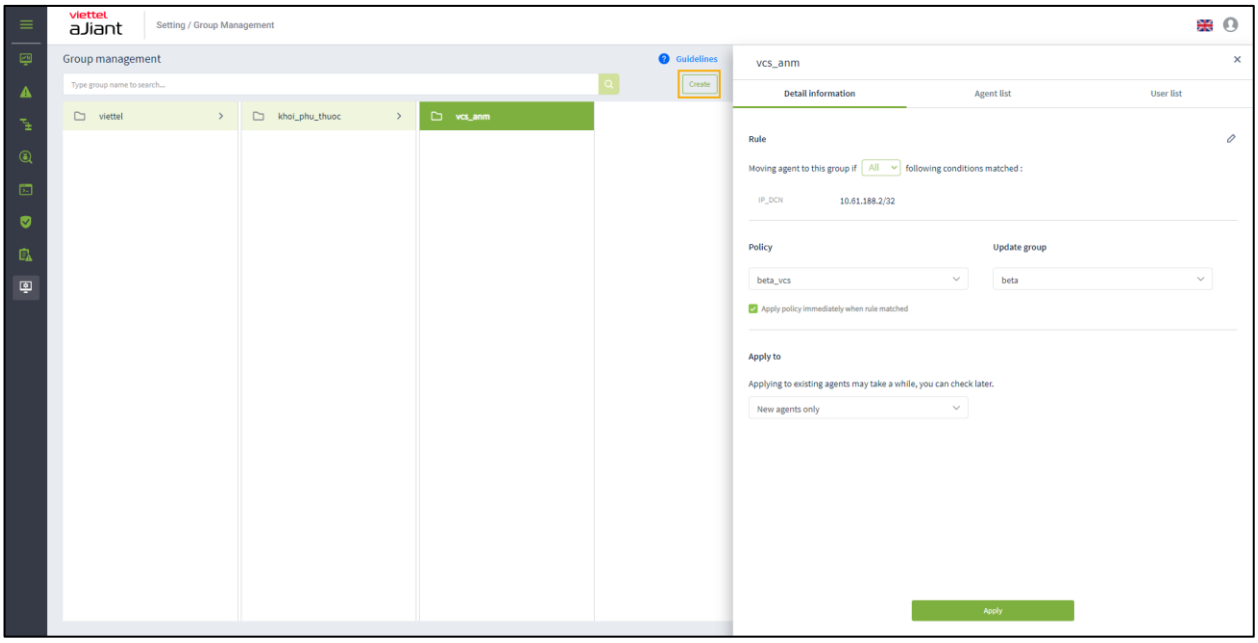
+ User đăng nhập thuộc group default: Không thể thêm mới;

+ 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 ;



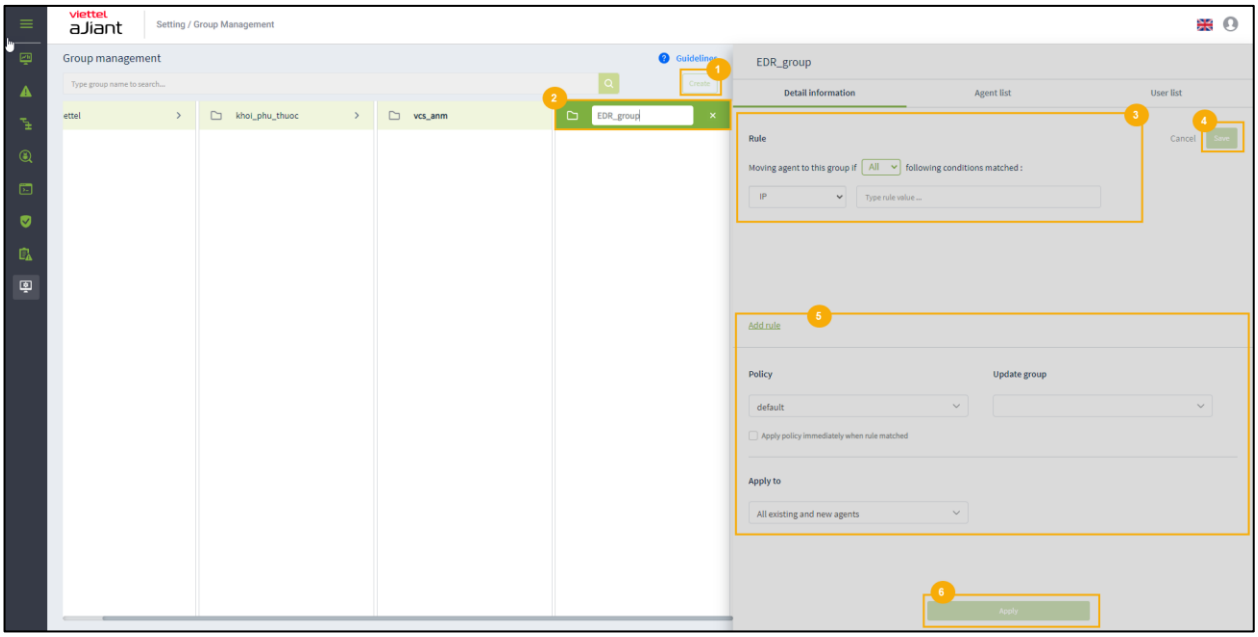
+ Nếu tạo mới nhóm là nhóm con trong một nhóm gốc hoặc nhóm cấp 1, cấp 2… thì click vào nhóm cha sau đó click “Create” trên màn hình hoặc hover vào cuối danh sách nhóm cùng cấp và click “Create”;

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

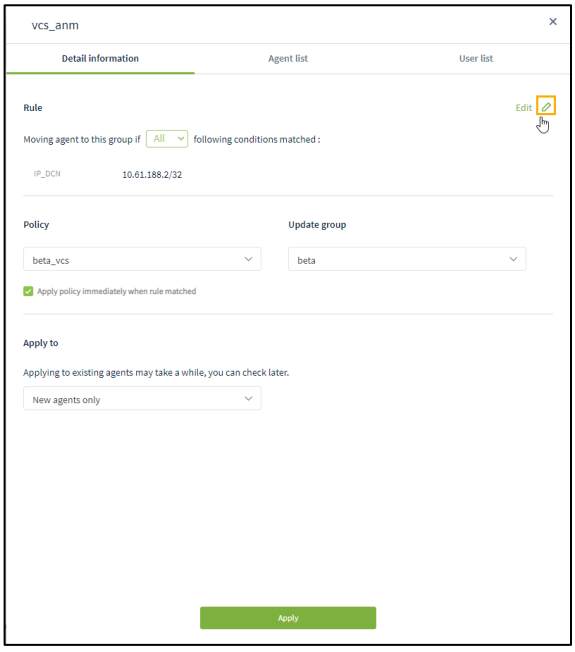
+ User đăng nhập thuộc group root: Có thể sửa tất cả group trong hệ thống;

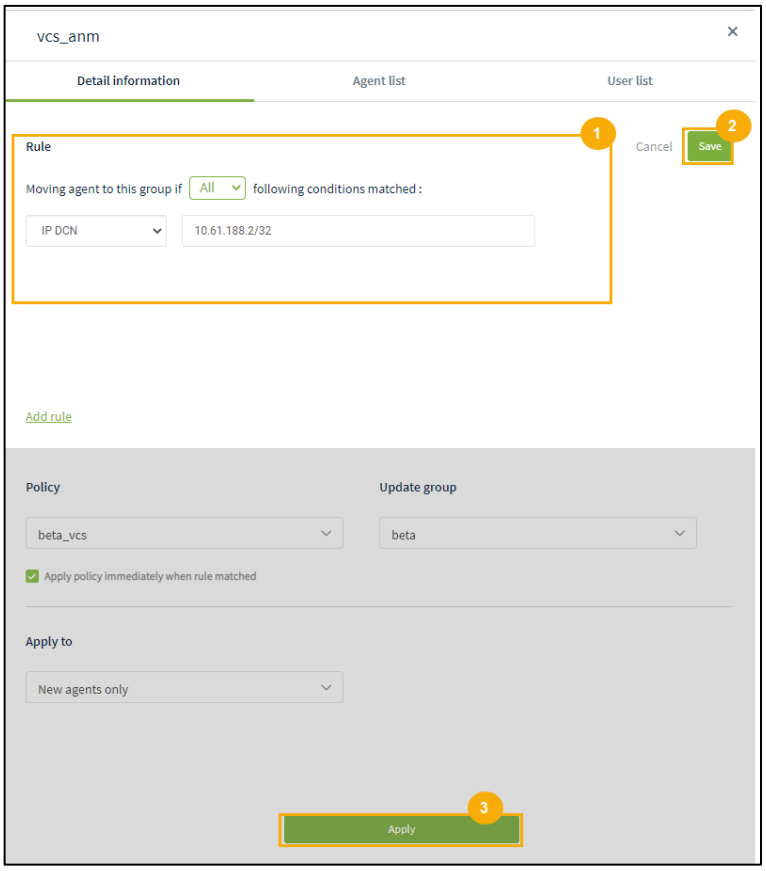
+ User đăng nhập thuộc group default: Không được sửa group default;

+ 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:

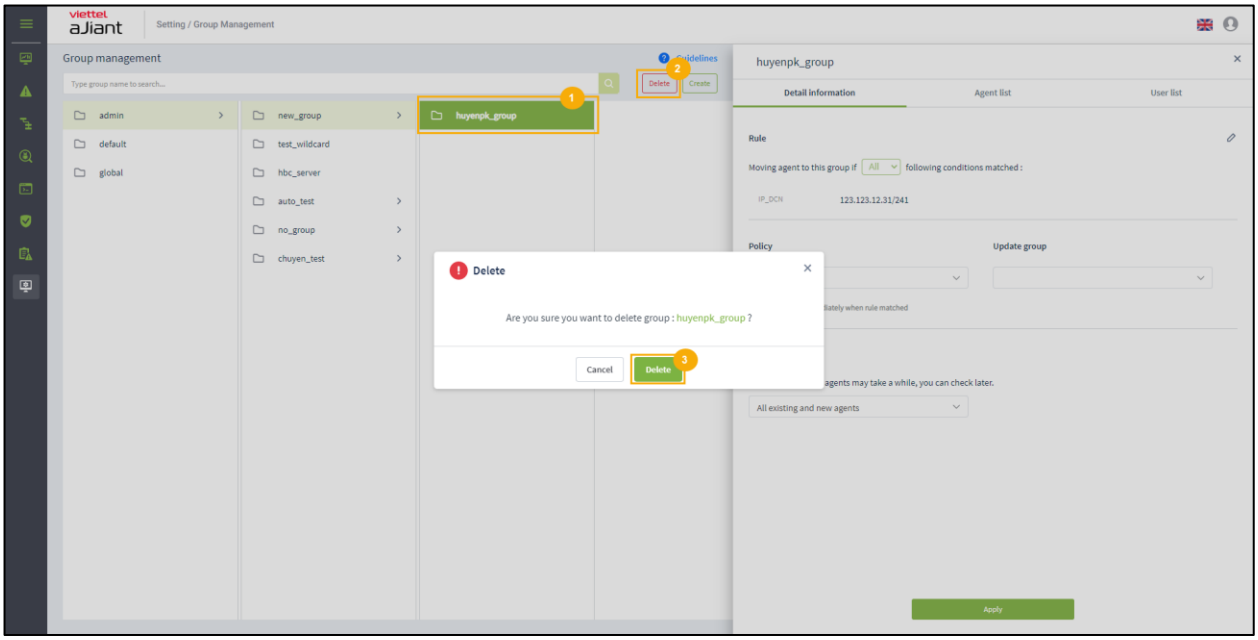
+ User đăng nhập thuộc group root: Có thể xóa tất cả group trong hệ thống;

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

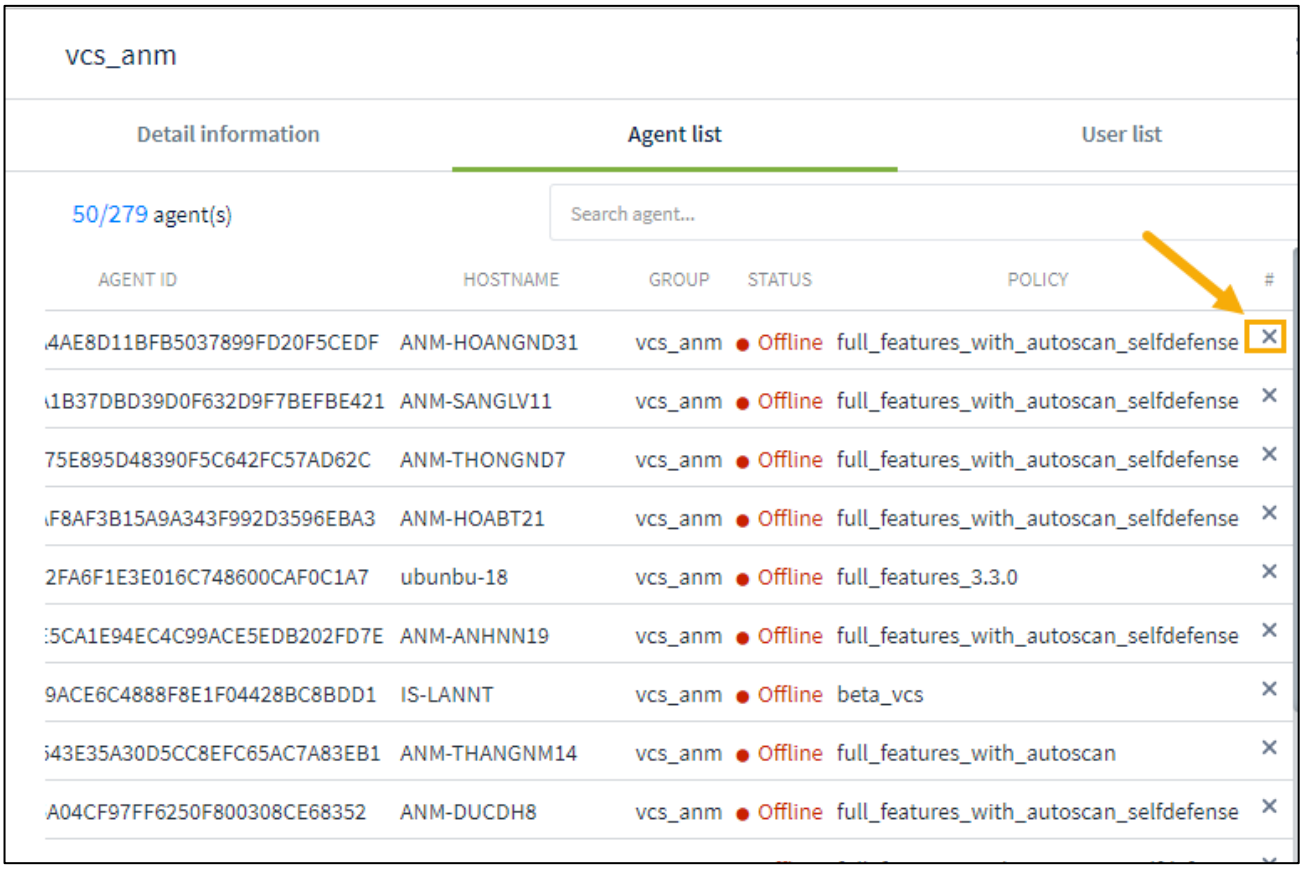
+ User đăng nhập thuộc group cha: Có thể xóa tất cả group thuộc đang login và group con có role cũng thuộc group role con của role user đang login;

+ 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;



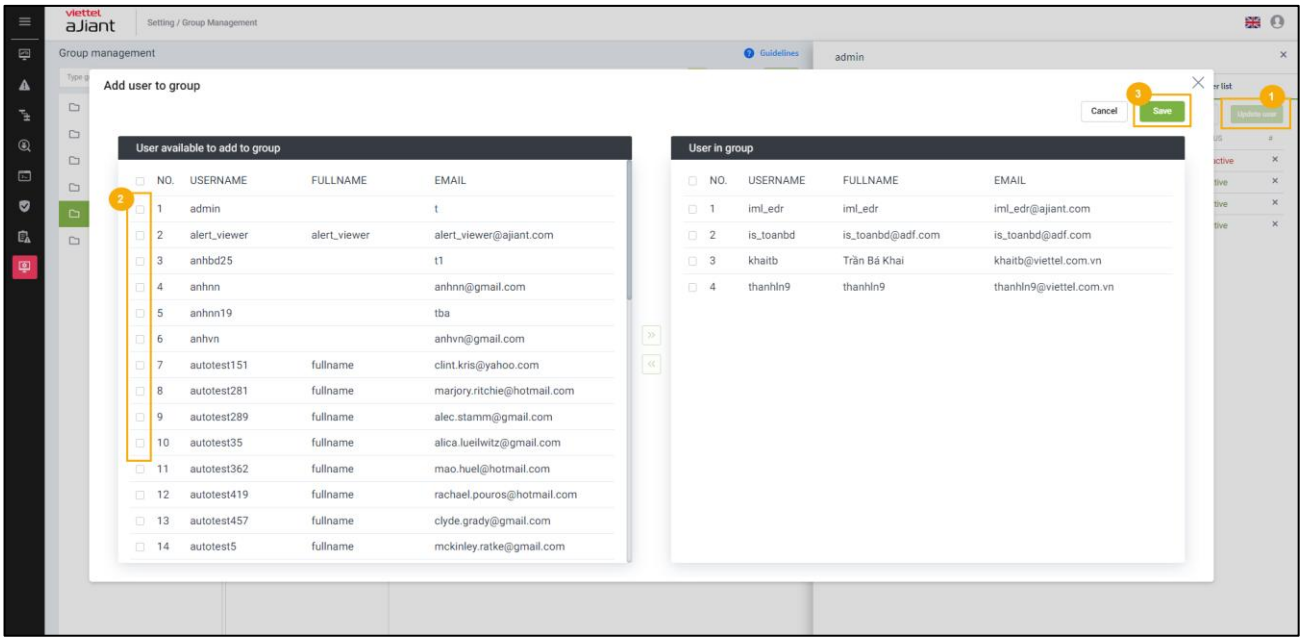
Để xóa Agent khỏi nhóm thì click vào tab Agent list, click icon "x" để xóa agent khỏi nhóm. Sau khi xóa agent khỏi nhóm thì agent được chuyển về nhóm mặc định: "default", policy giữ nguyên



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:

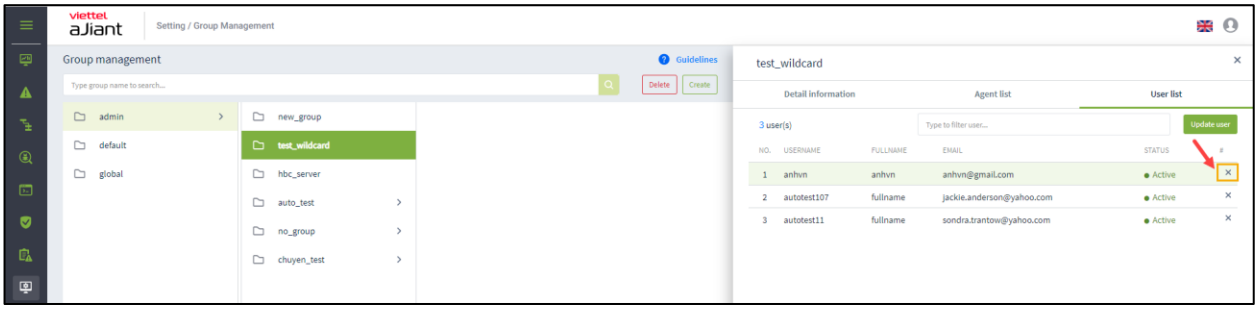
+ User đăng nhập thuộc group root: Hiển thị tất cả User trong hệ thống;

+ 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



3.6.4 Account Management

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

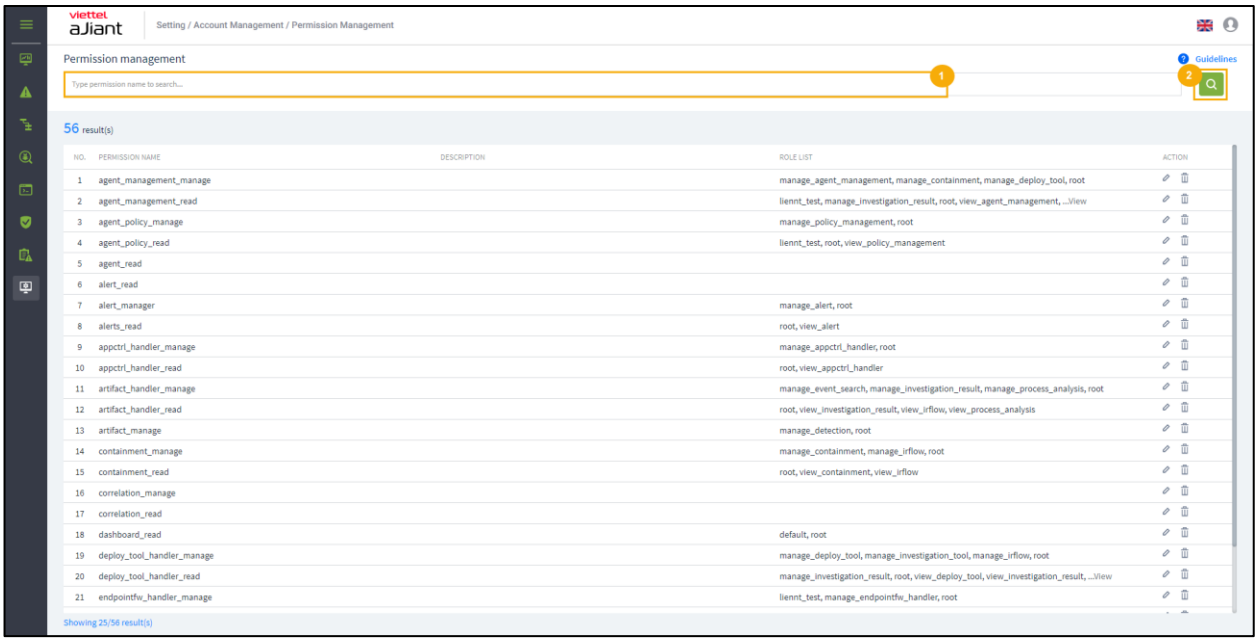
3.6.4.1 Permission management

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:

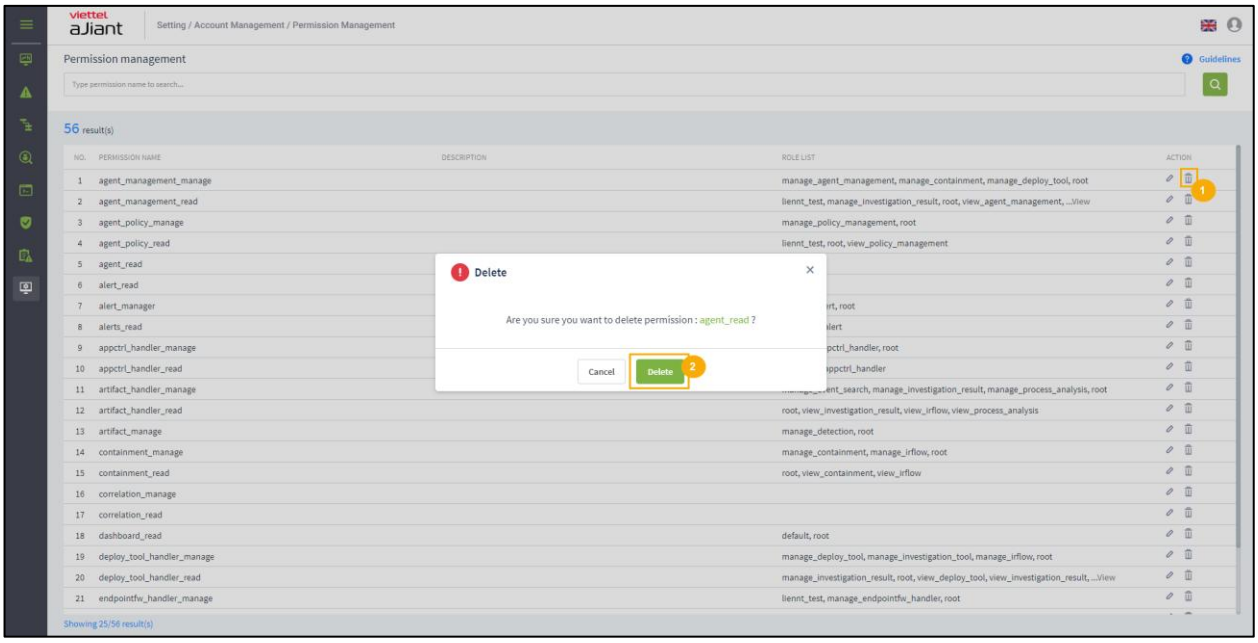
+ Quản lý các permission;
+ Tìm kiếm permission;
+ Xóa permission;

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:



3.6.4.2 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;

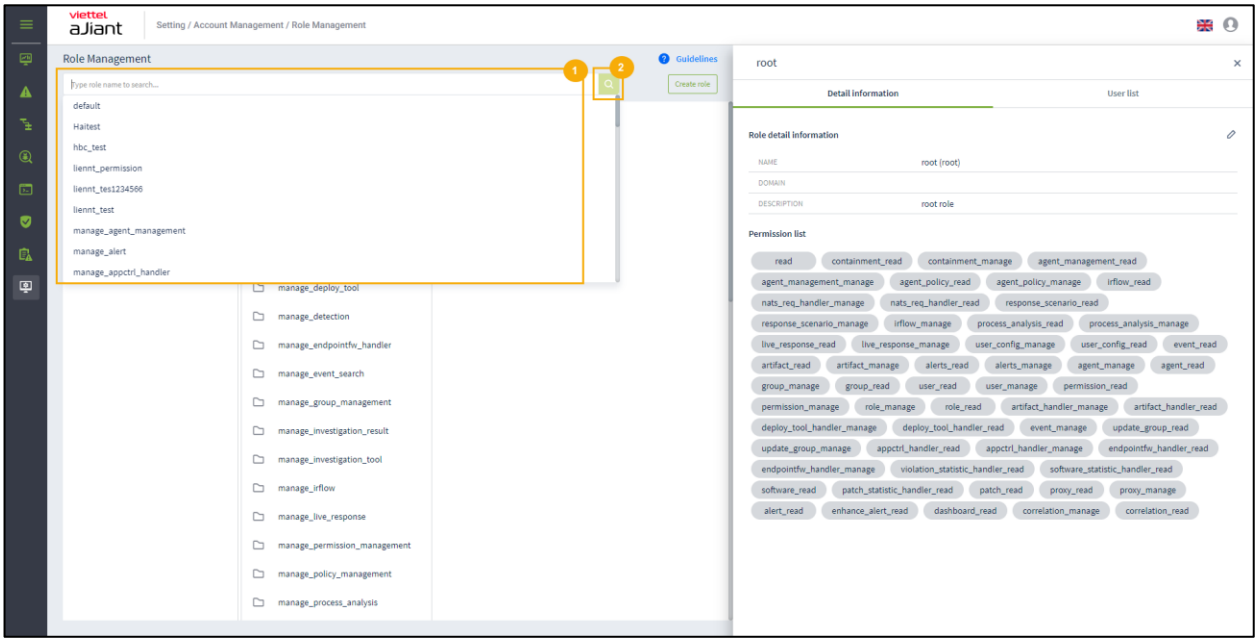
+ Role “root”: bao gồm toàn bộ các role của hệ thống, User có role “root” có toàn bộ quyền sử dụng tất cả chức năng trên Portal;

+ 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.

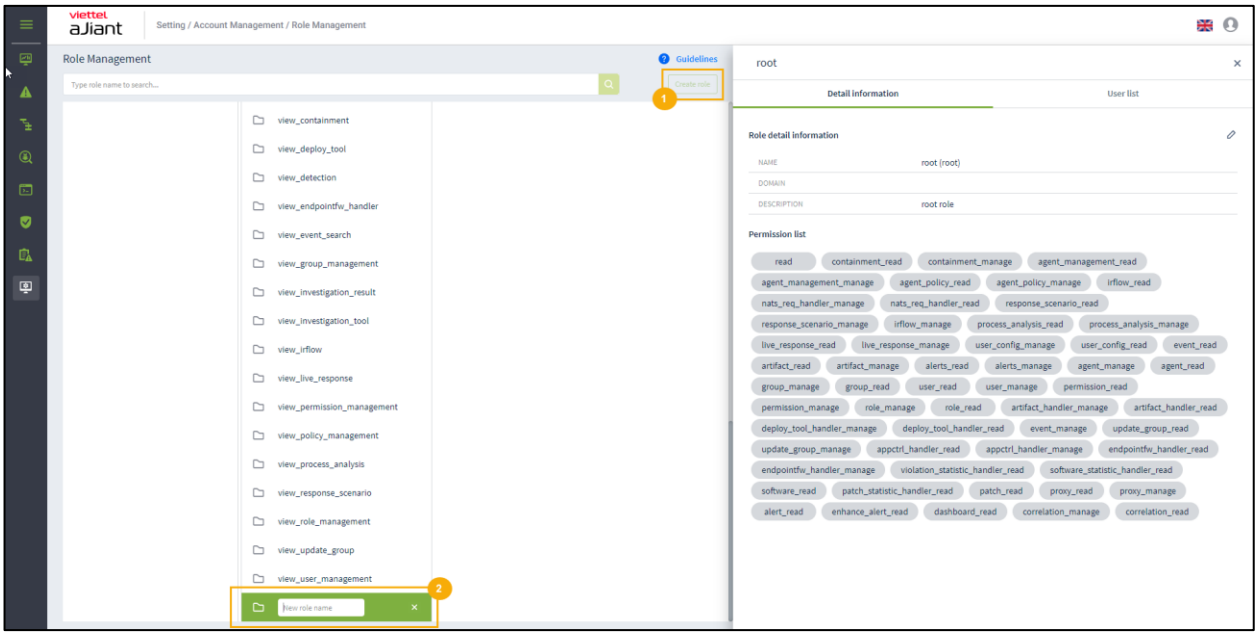
Bước 1: Có các cách tạo mới role như sau:

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:

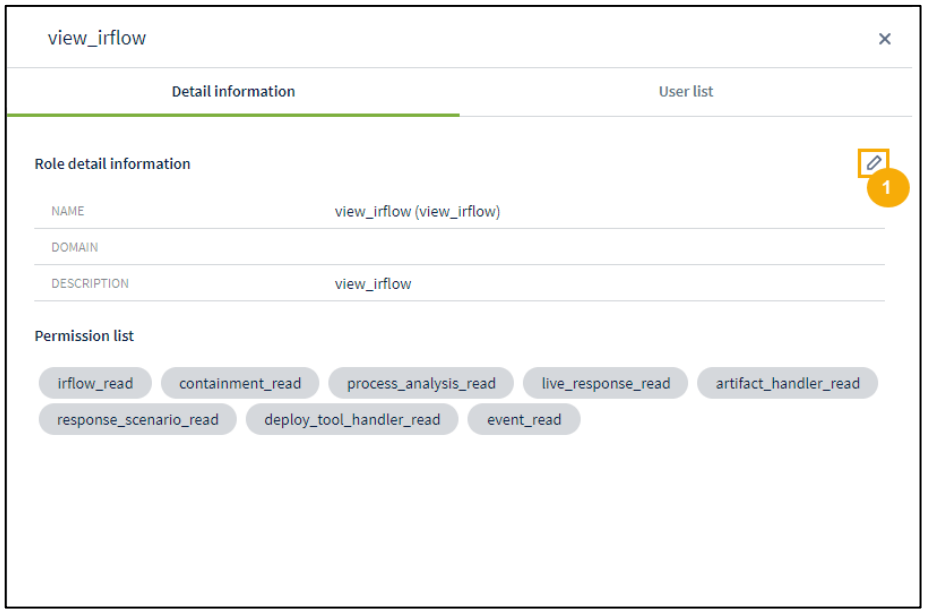
+ User đăng nhập thuộc group root: Có thể sửa tất cả role trong hệ thống;

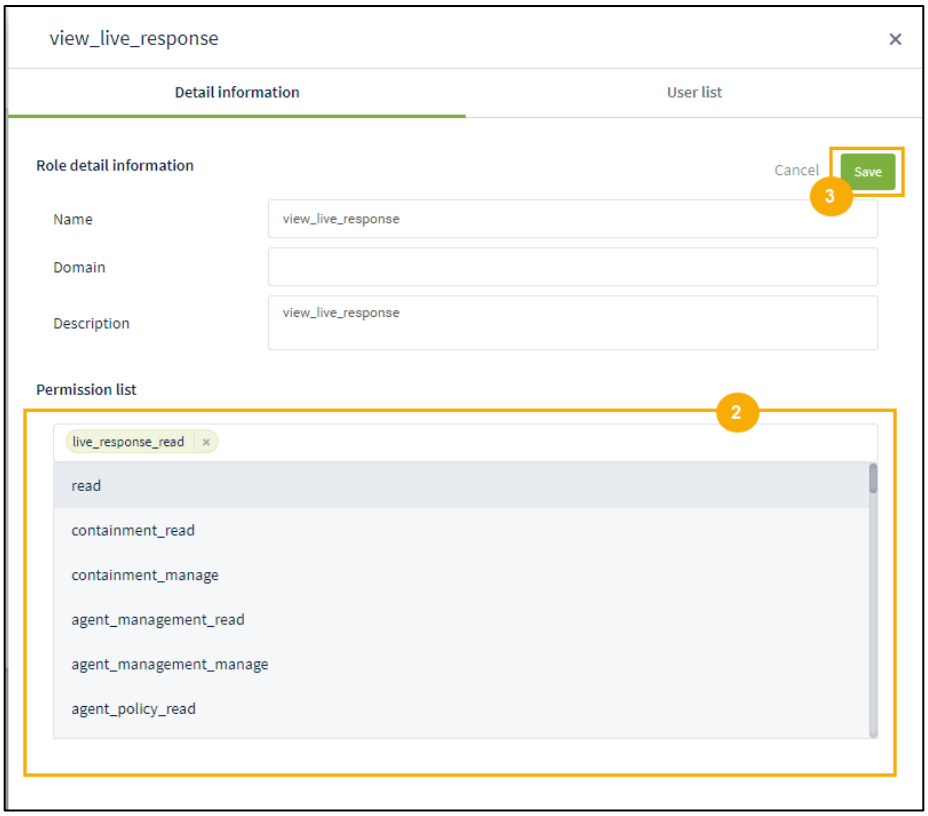
+ User đăng nhập thuộc group default: Không được sửa role default;

+ 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.



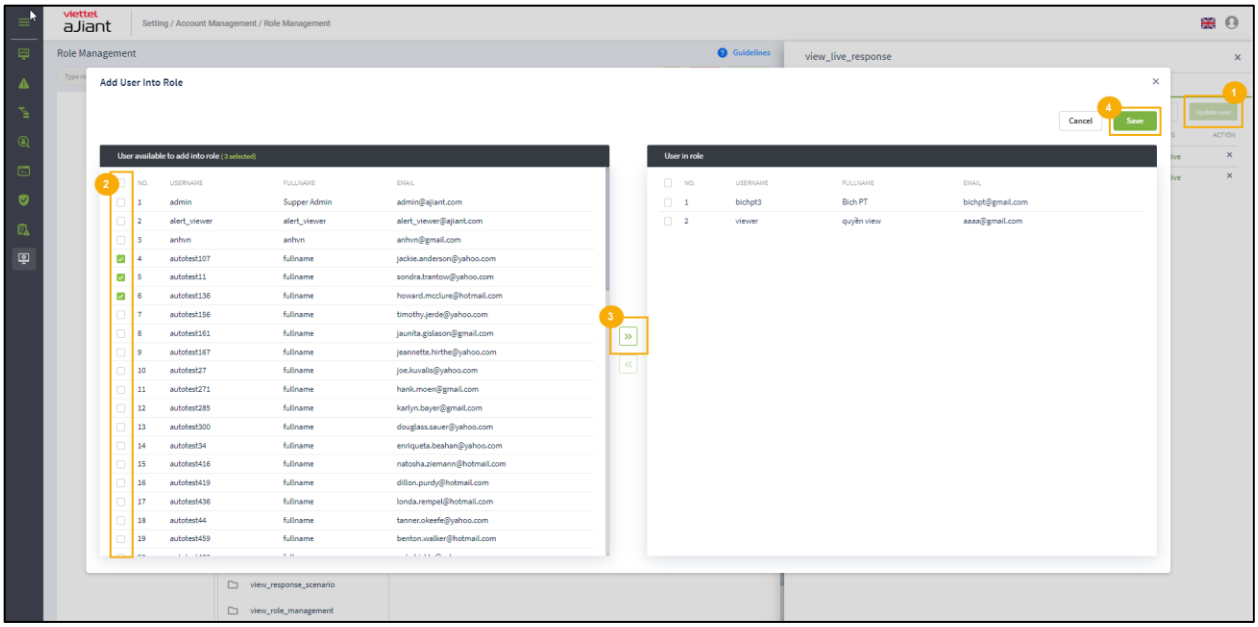


Bước 3: Chuyển sang tab User list để thêm role vào danh sách role của User

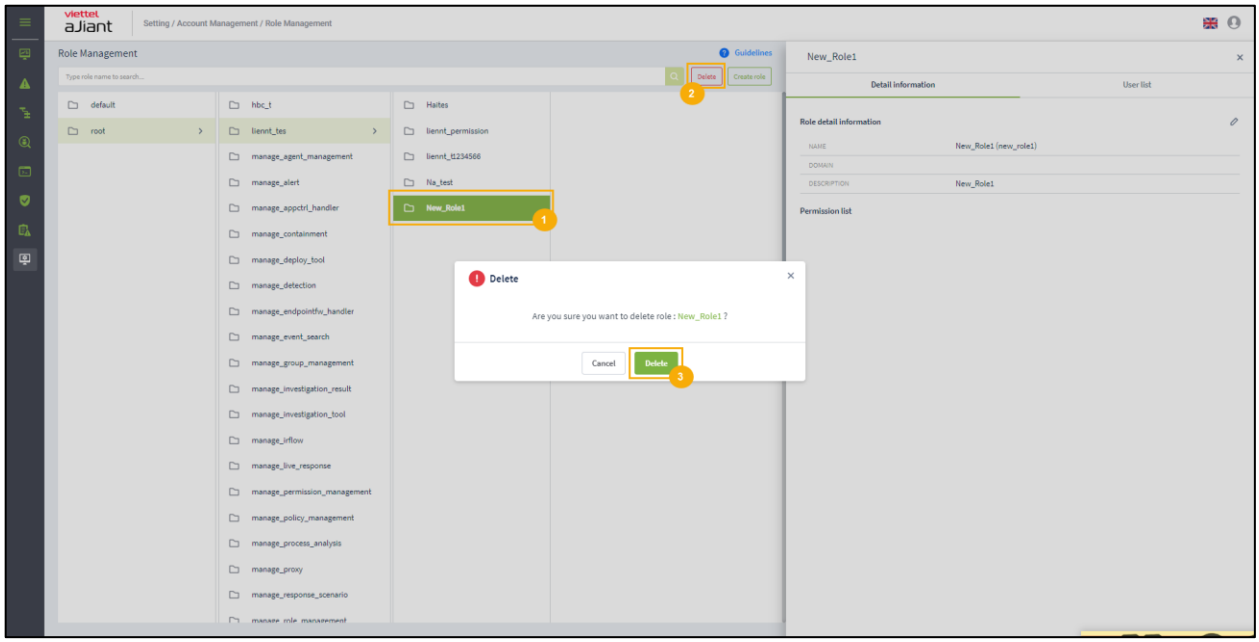
+ User đăng nhập thuộc group root: Hiển thị tất cả User trong hệ thống;
+ User đăng nhập thuộc group default: Hiển thị user chỉ thuộc default;

+ 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.

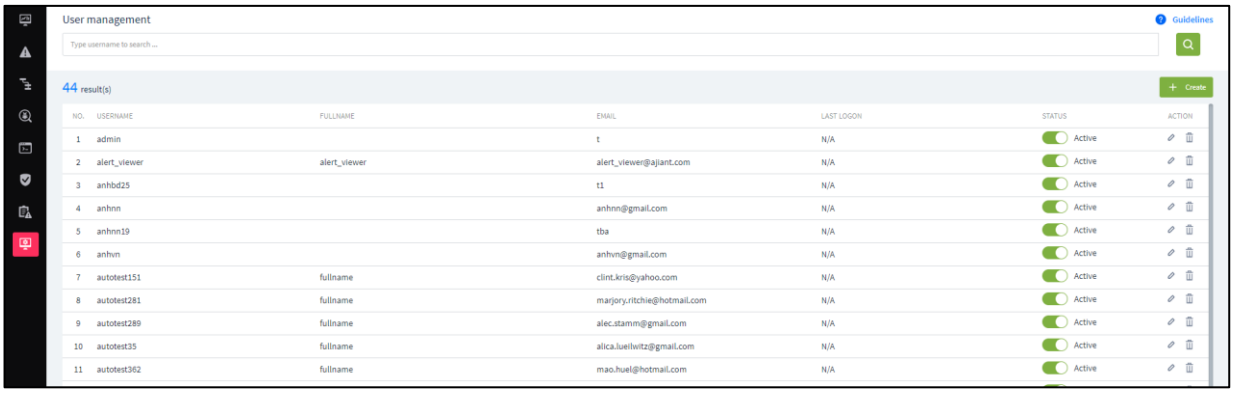
3.6.4.3 User management

Quản lý các tài khoản đăng nhập vào hệ thống Portal VCS-aJiant.

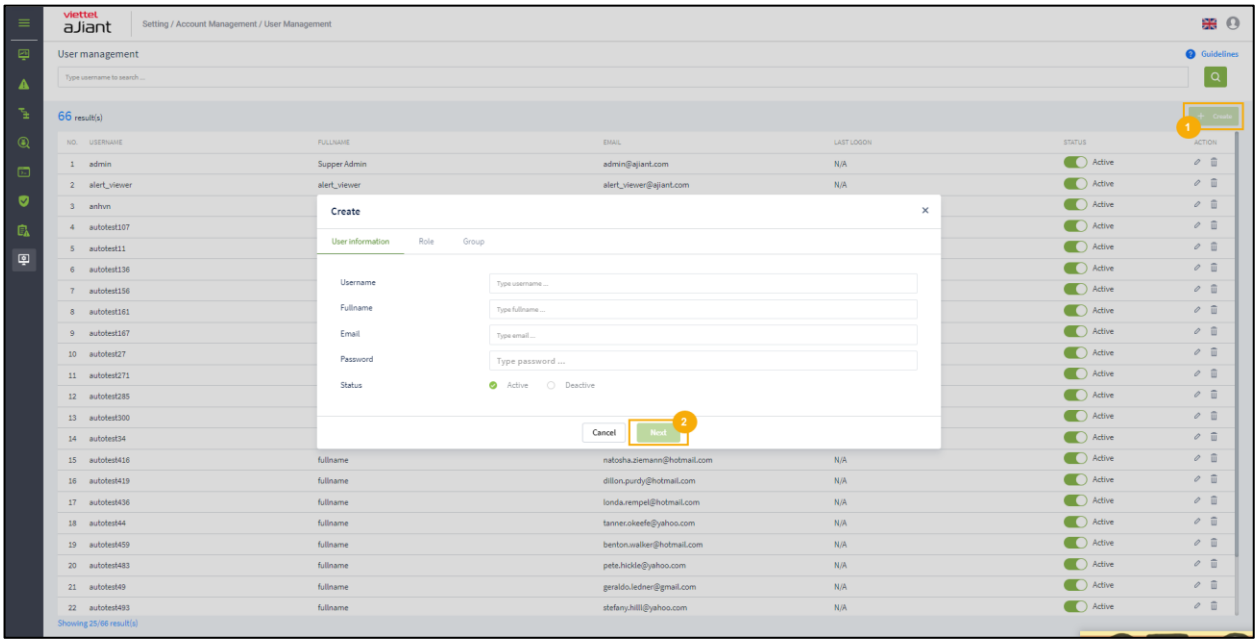
Các chức năng chính trên màn hình này gồm có:

+ 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”

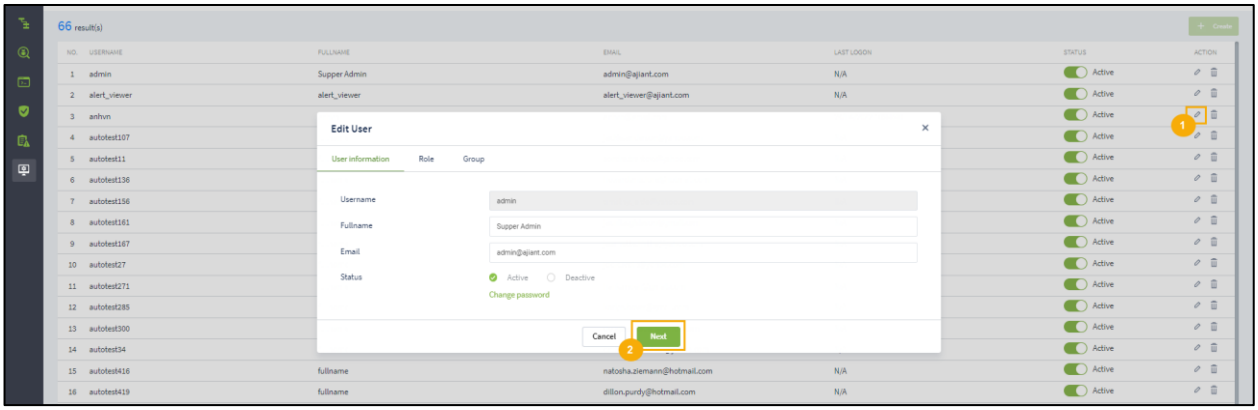


+ Lựa chọn role (nhóm quyền) sẽ gán cho tài khoản, sau đó click “next”;

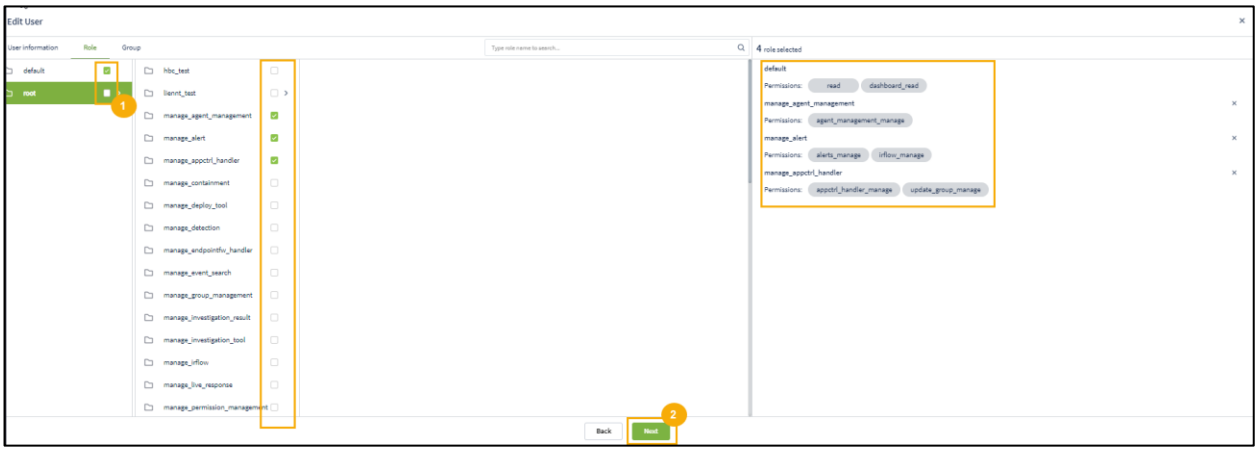
+ Khi click vào check box từng role sẽ hiện thị các permission (quyền) tương ứng với role đó:

- 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;



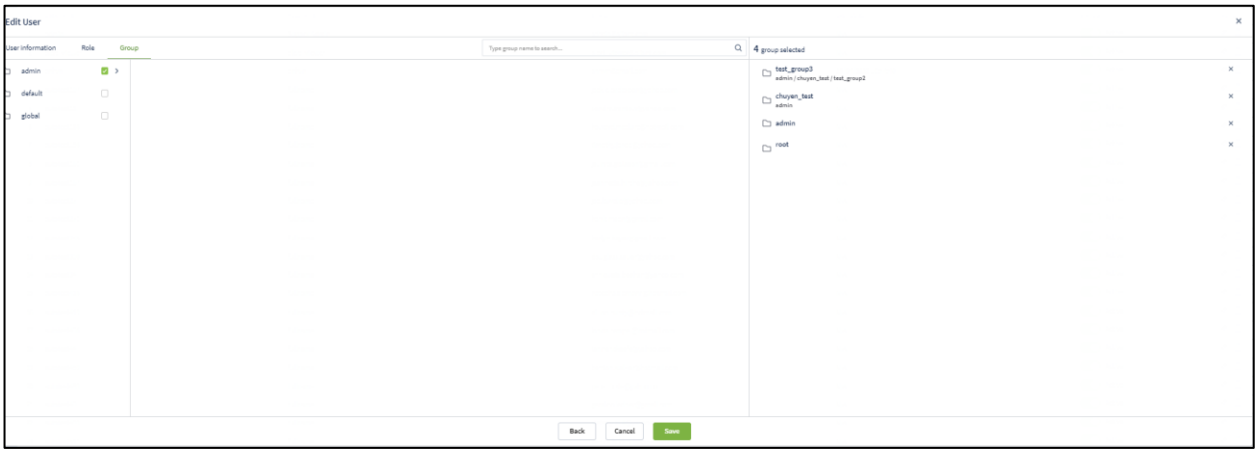
+ Click chọn checkbox tương ứng với role cần thêm, sau đó click "Go to role" để về màn hình danh sách role ban đầu, sau đó click "Create" để tạo tài khoản;

+ 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;

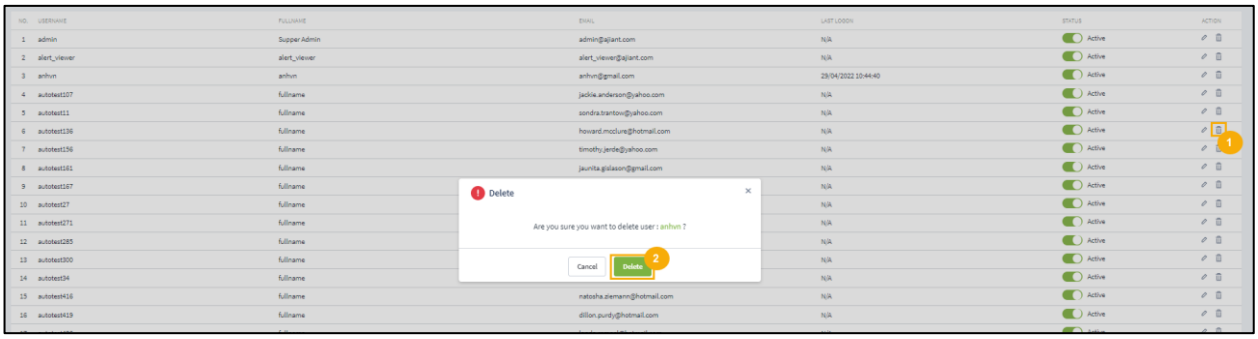


+ Click chọn checkbox tương ứng với group cần thêm, sau đó click "Go to role" để về màn hình danh sách group ban đầu, sau đó click "Create" để tạo tài khoản.

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

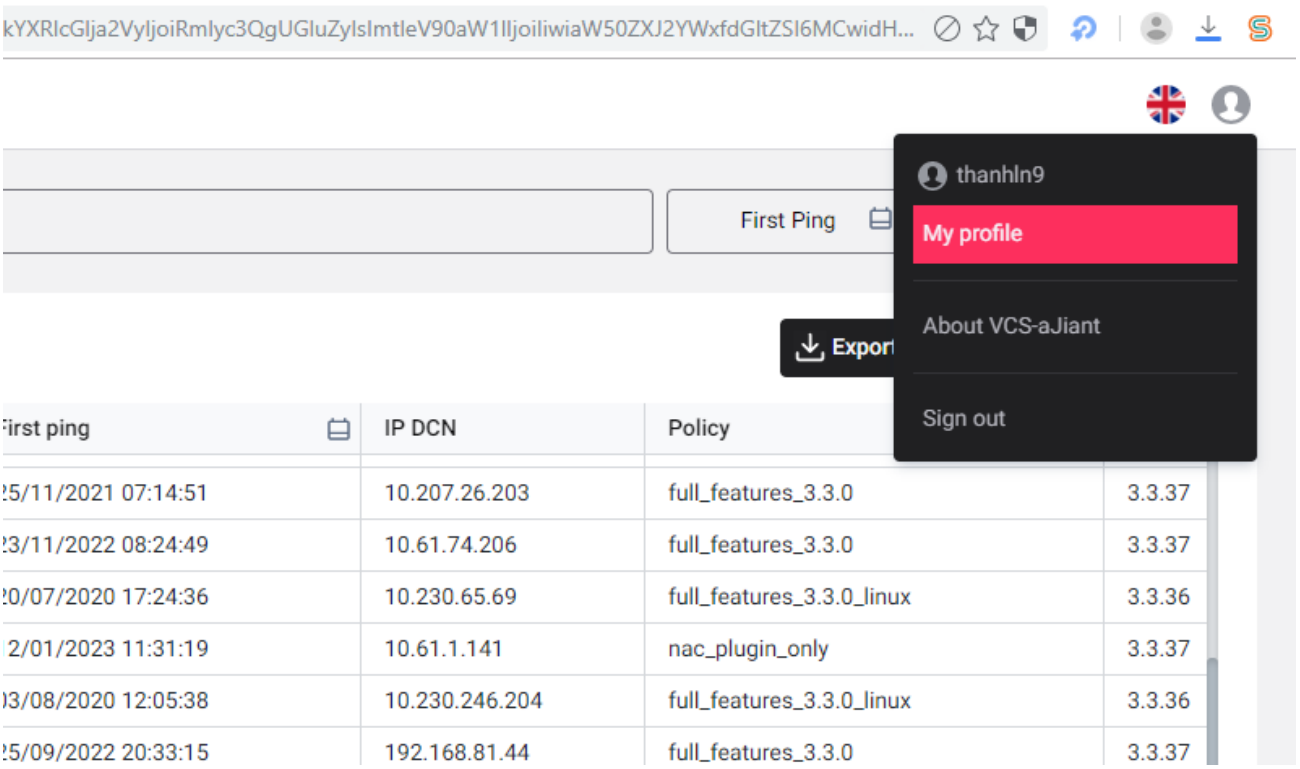
Kiểm tra hiển thị icon xóa:

+ 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;

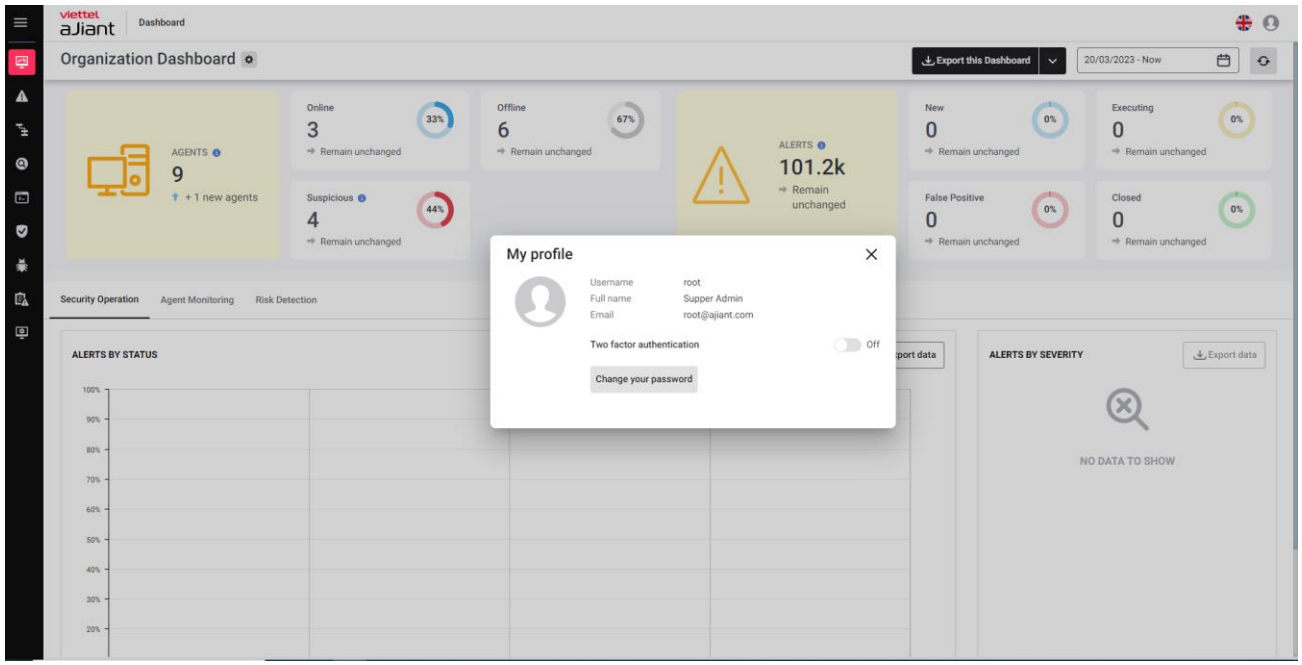


<u>Bật tính năng xác thực 2 bước cho tài khoản:</u>

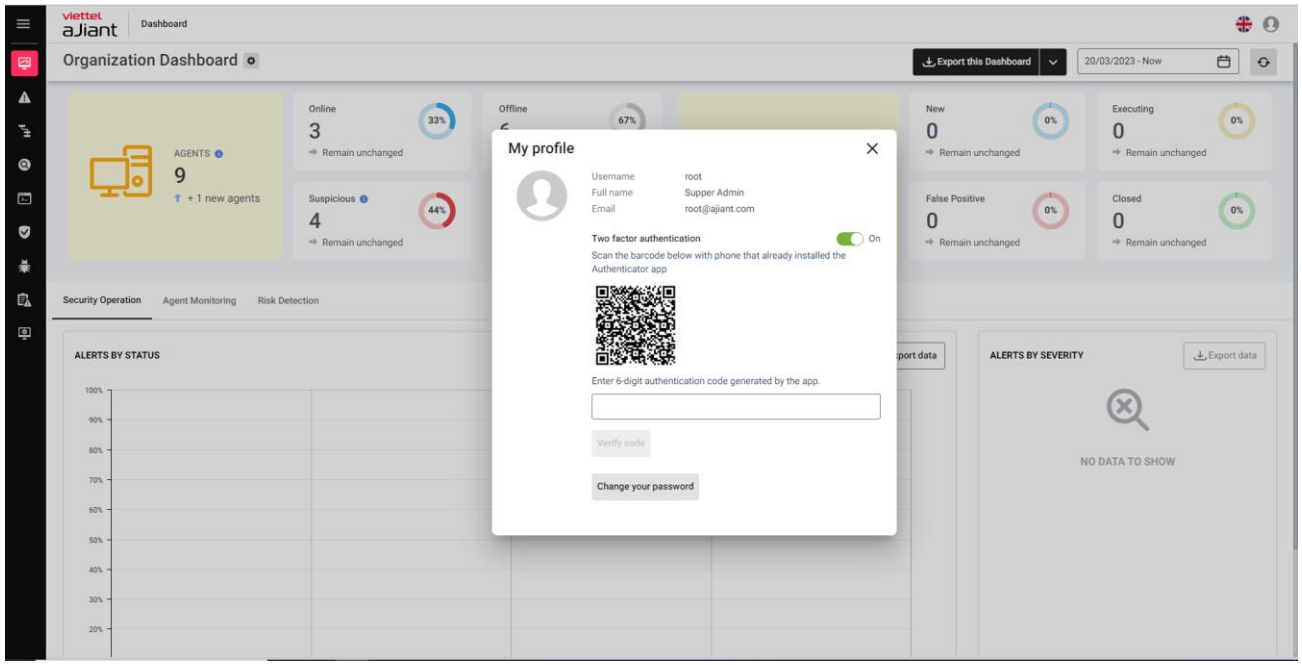
Bước 1: Vào giao diện My profile như ảnh dưới



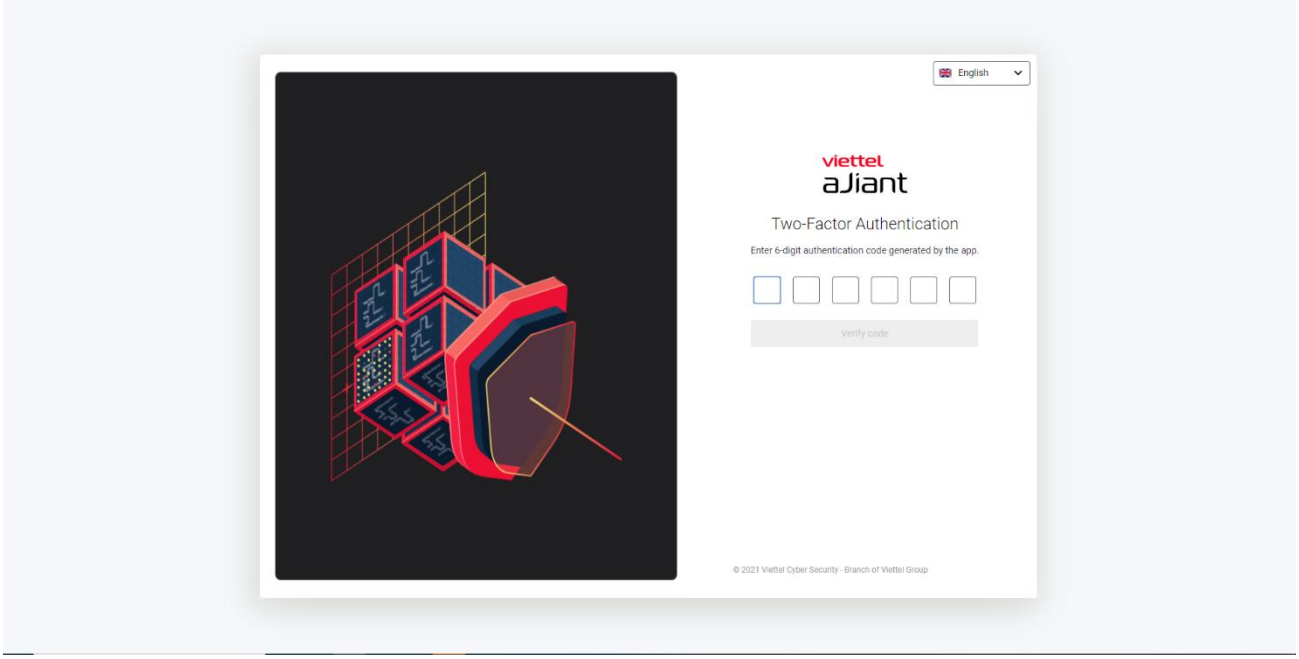
Bước 2: Click để bật Two Factor authentication



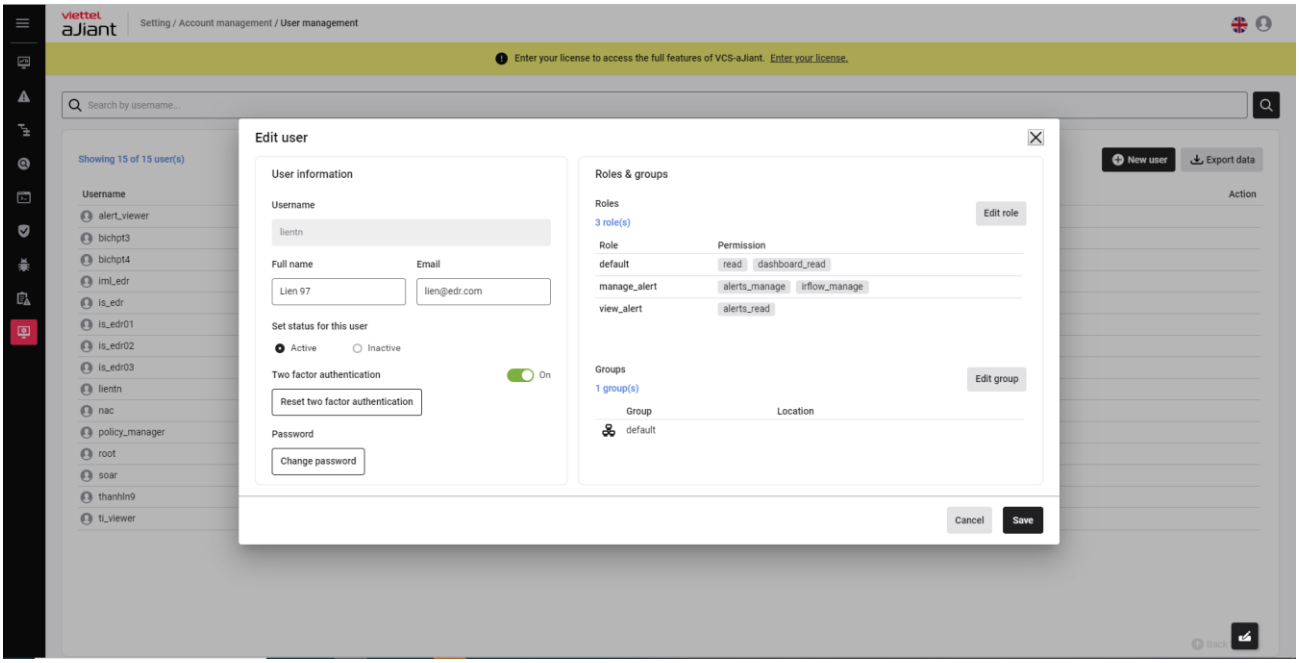
Bước 3: Dùng 2FA app để quét mã QR, sau đó nhập OTP để hoàn thành quá trình bật 2FA



Sau khi bật 2FA, khi login, người dùng sẽ được yêu cầu nhập OTP như ảnh dưới



Có thể bật 2FA cho các users khác như ảnh dưới



Giải pháp cũng hỗ trợ force enable 2FA cho toàn bộ tài khoản

3.6.5 Update management

3.6.5.1 Update groups

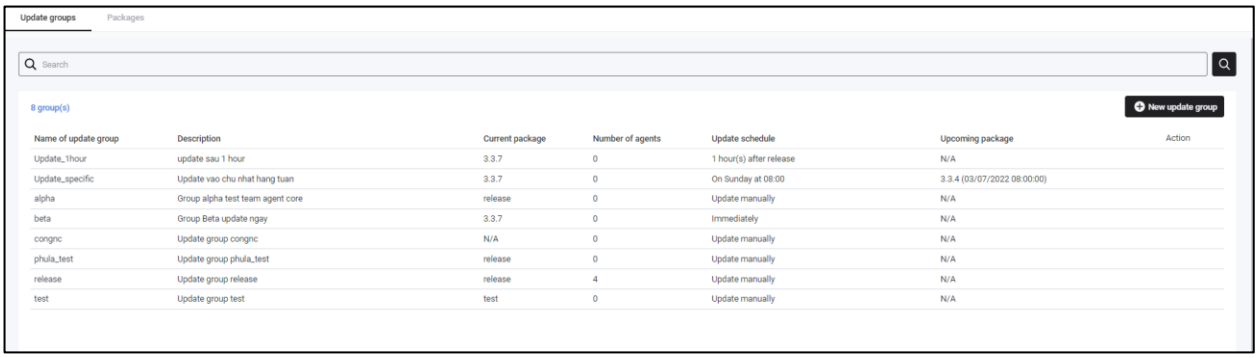
Mục đích: là tính năng cho phép quản lý, tạo mới và cập nhật các Update Group (Chia các Agent thành các nhóm cập nhật, giúp dễ dàng phân chia, quản lý)

1 – Tìm kiếm:

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

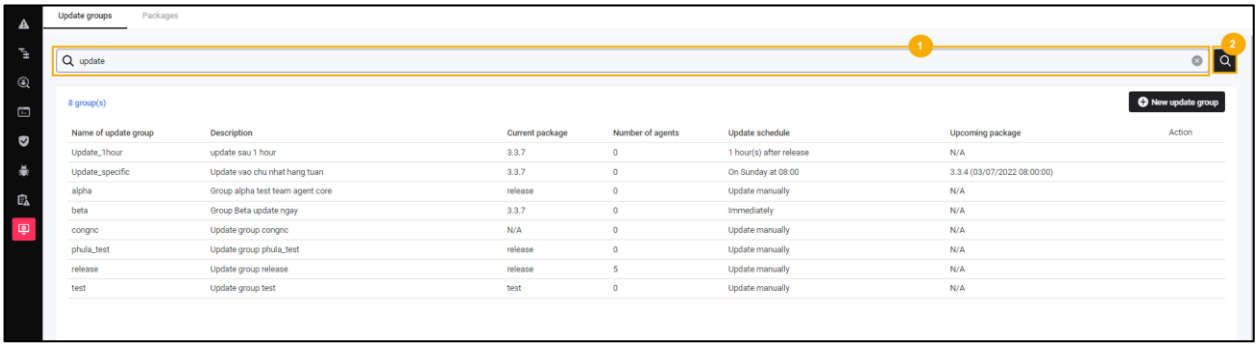
Bước 2: Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;

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"

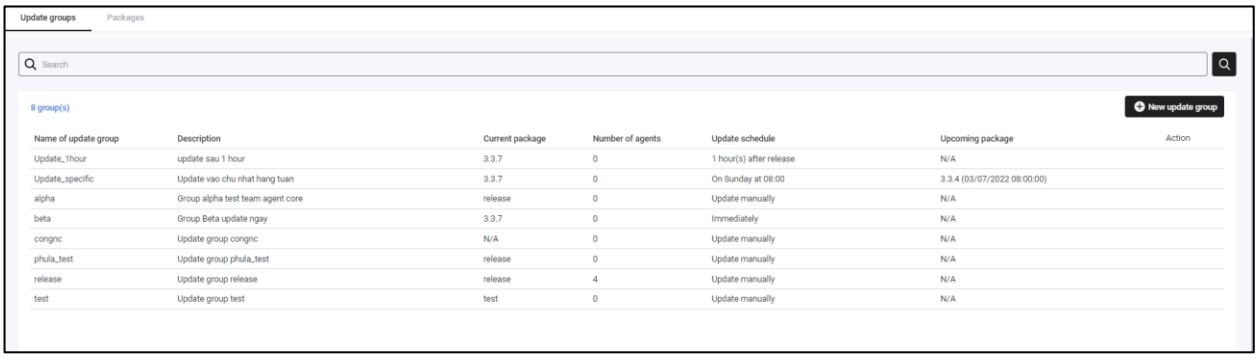


2 – Thêm mới Update groups:

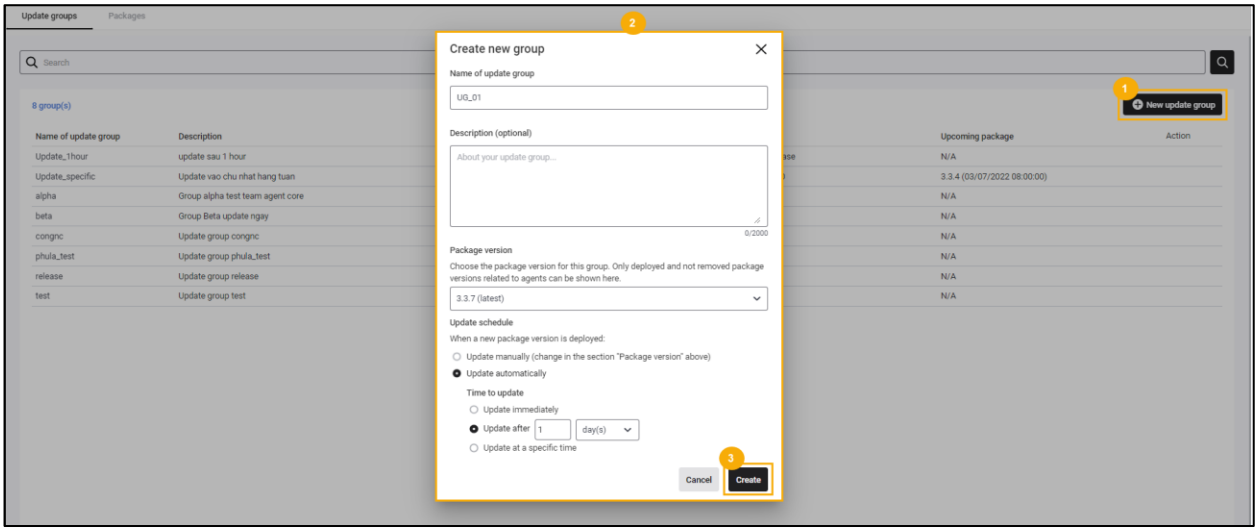
Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;

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;



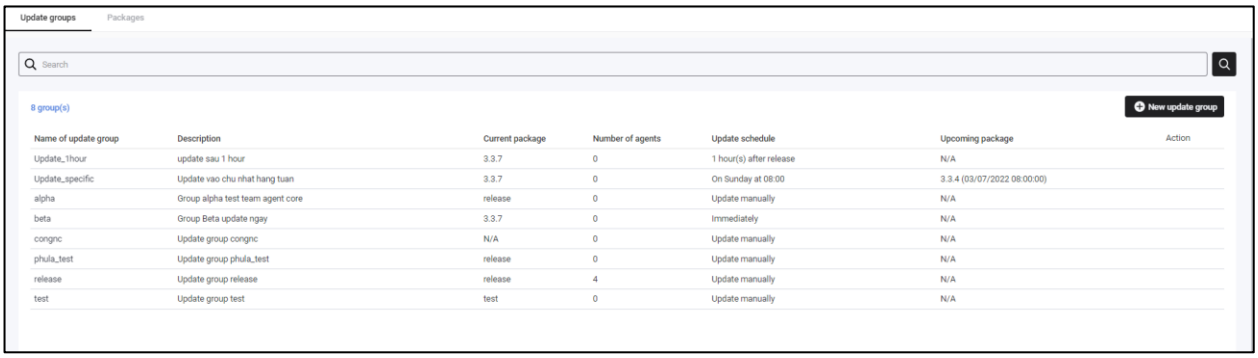
Bước 5: Nhập thông tin thêm mới Update Group và chọn nút "Create". Hệ thống ghi nhận và quay về màn hình danh sách Update Group.

3 – Cập nhật Update groups:

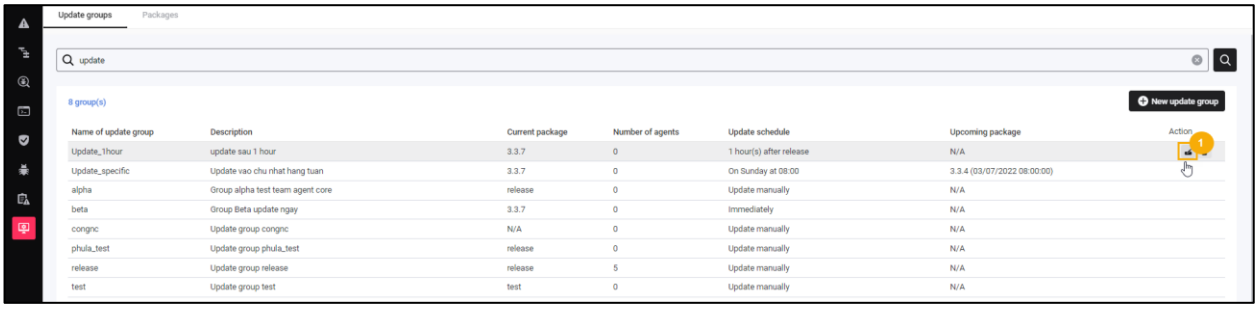
Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;

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

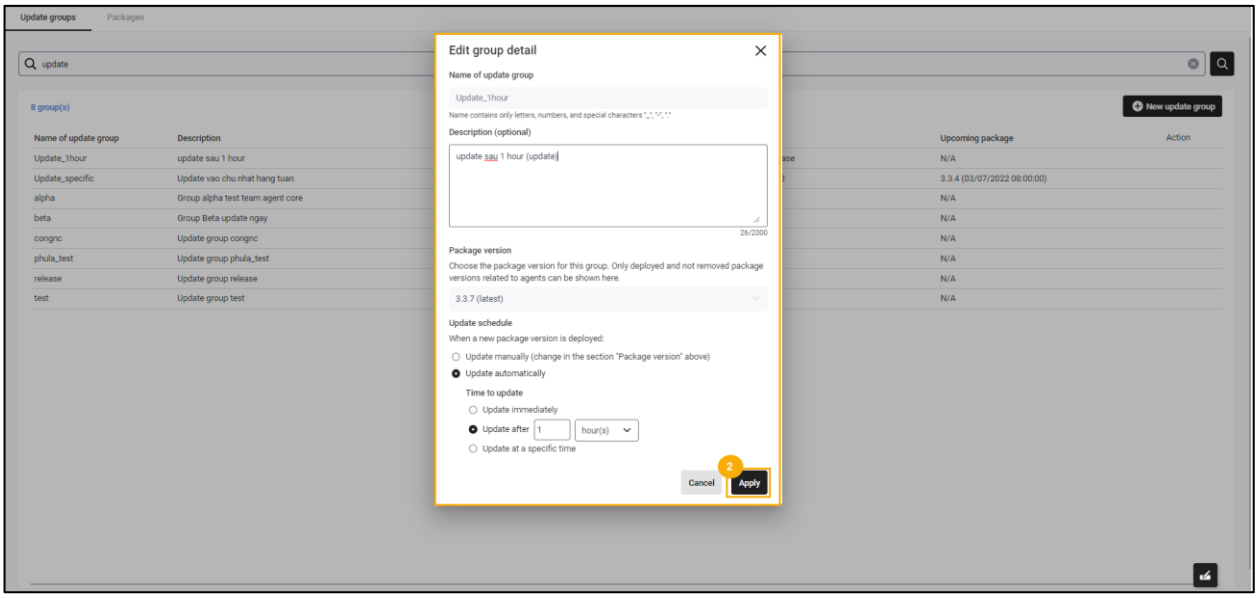
Bước 3: Chọn Update Management, hệ thống hiển thị Danh sách Update Group;



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":

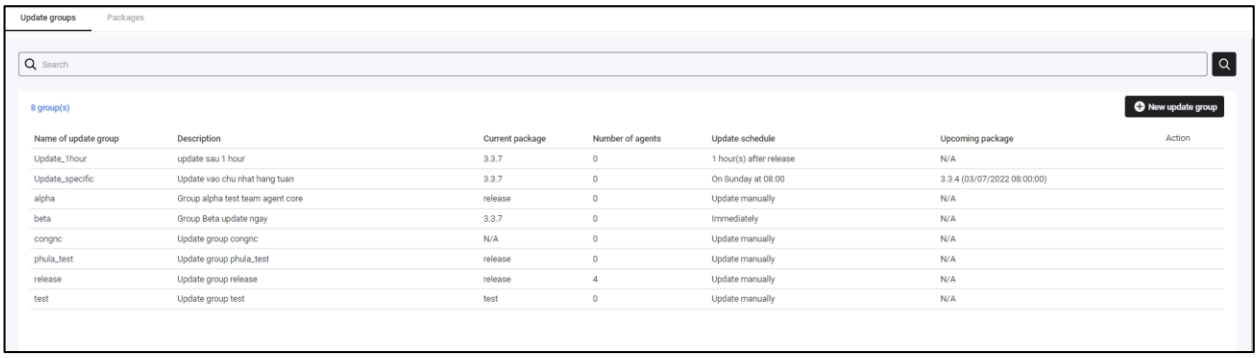


4 – Xóa Update groups:

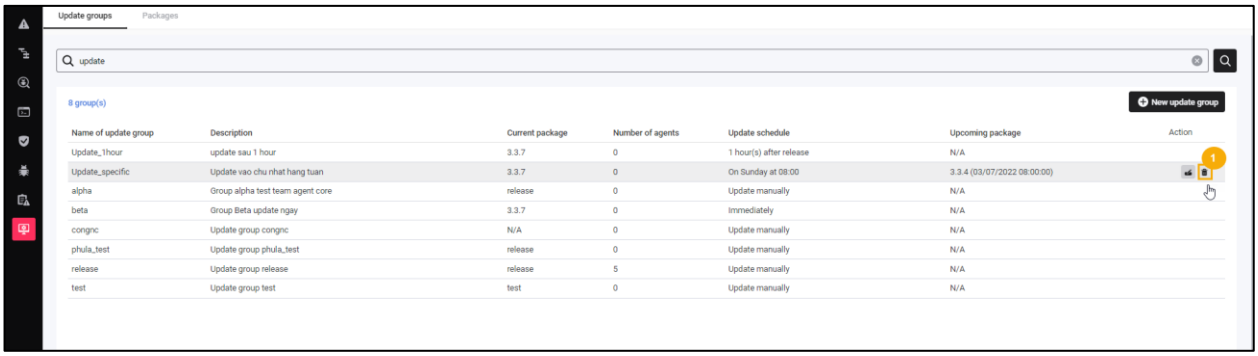
Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;

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

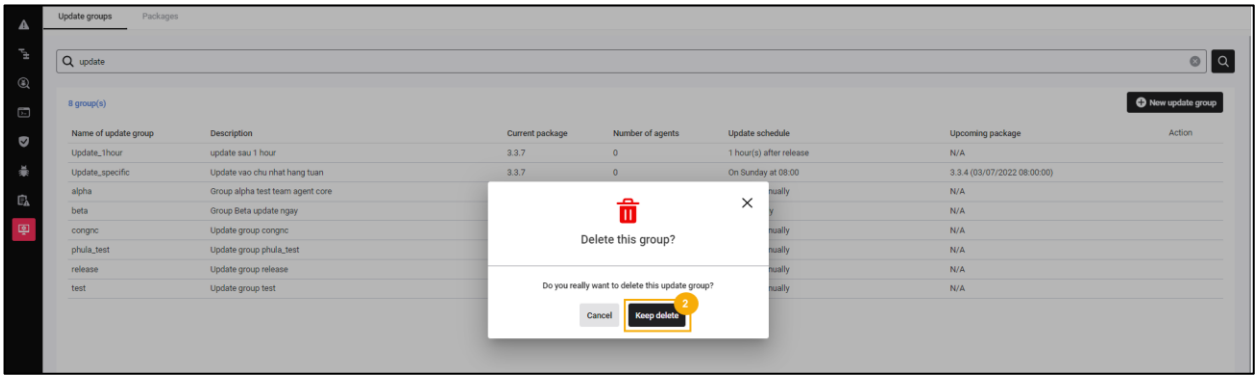
Bước 3: Chọn Update Management, hệ thống hiển thị Danh sách Update Group;



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.



3.6.5.2 Update packages

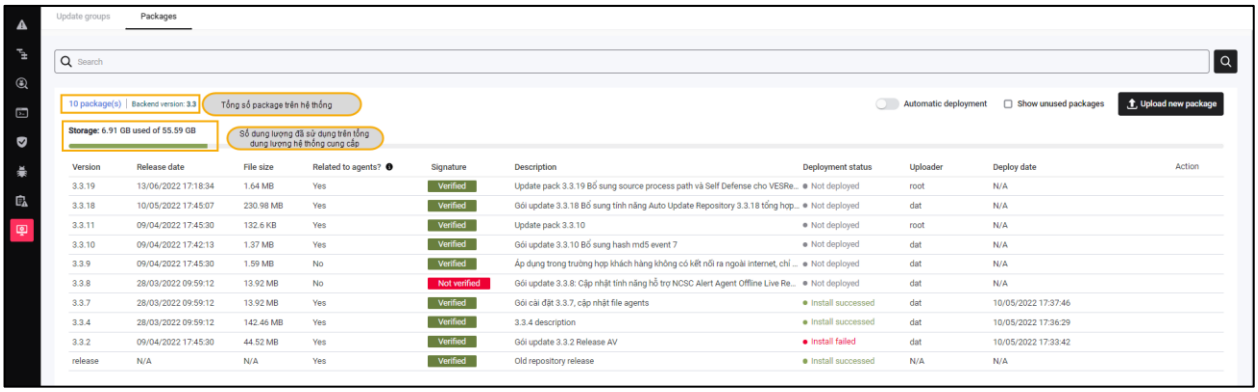
1 – Tìm kiếm packages:

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

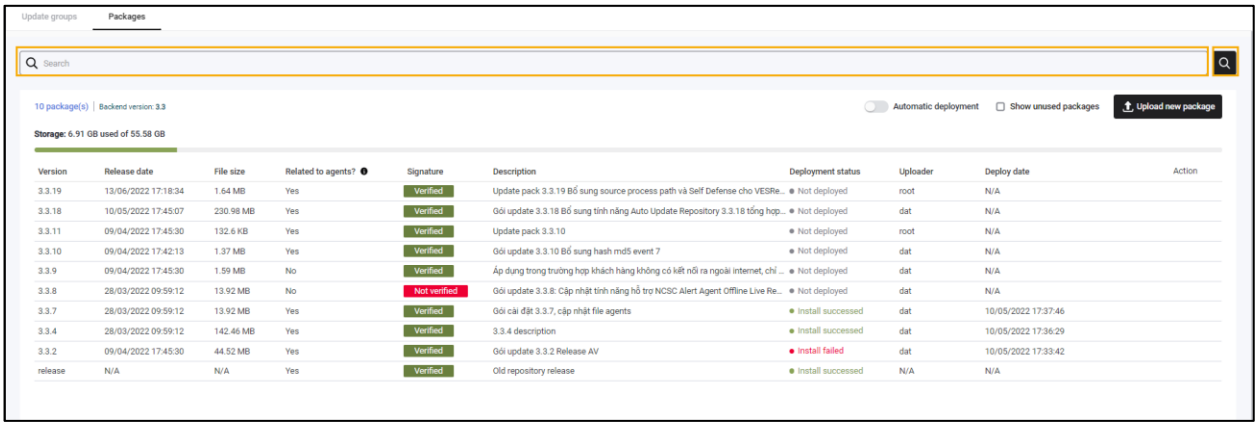
Bước 2: Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;

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;

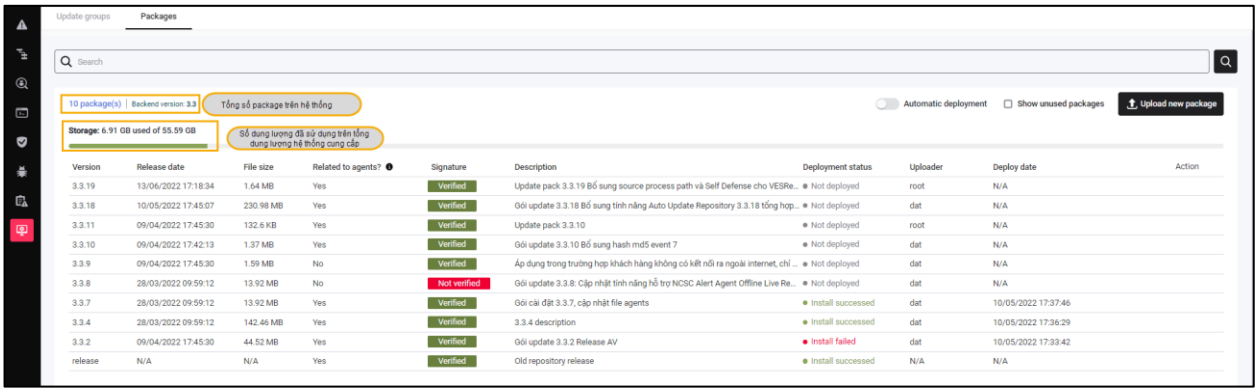
Lưu ý: Đội triển khai gửi lại các thông tin trên cho đội dự án Ajiant để cập nhật vào hệ thống để cho phép triển khai gói tự động tại khách hàng. Về sau, khi cần triển khai gói update mới, đội triển khai hoặc phía khách hàng chỉ cần lấy gói update được cung cấp và upload lên portal ajiant và chọn triển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

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

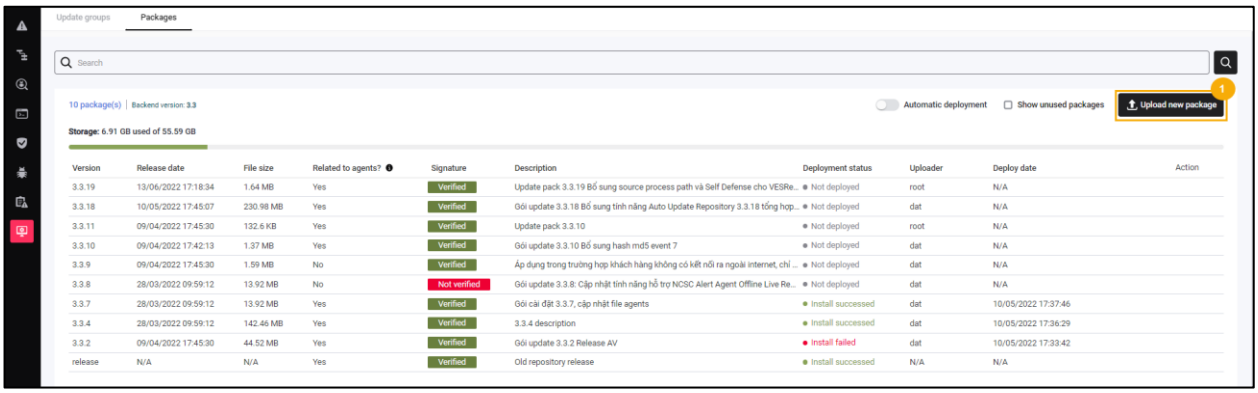
Bước 2: Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;

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

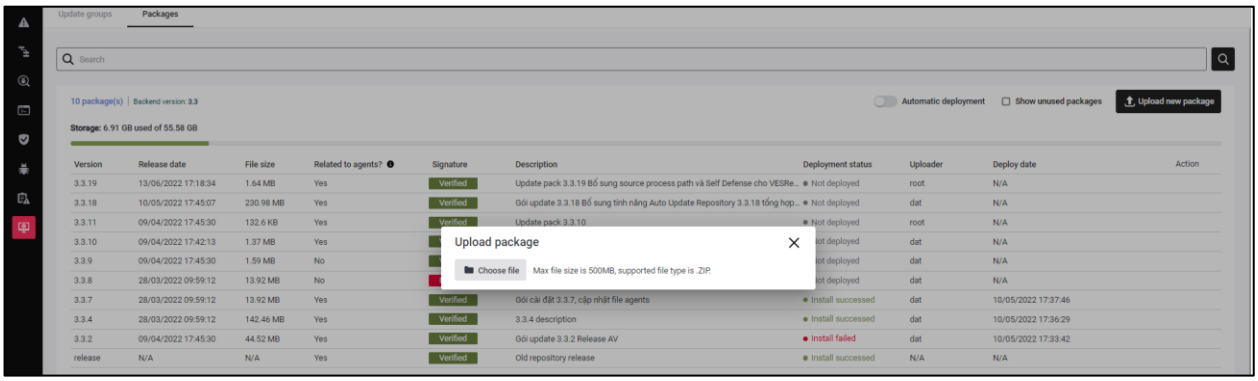
Bước 4: Chọn Tab "Package", hệ thống hiển thị Danh sách Pakage trong hệ thống;



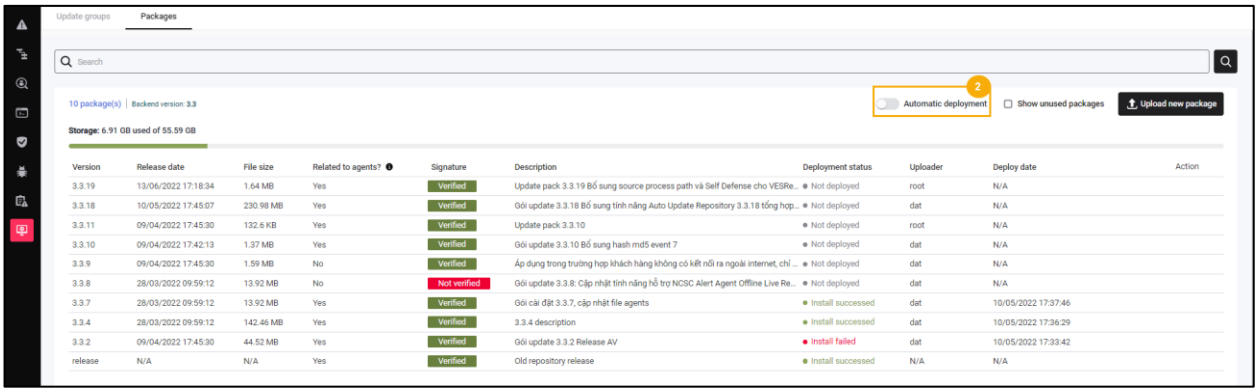
Bước 5: Chọn nút "Update new package", hệ thống hiển thị Popup "Upload package";



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.



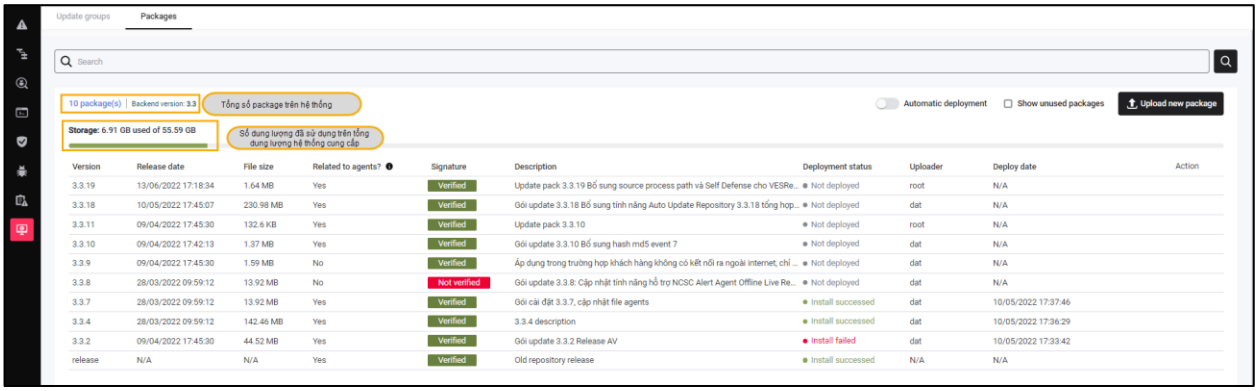
3 – Deploy package

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

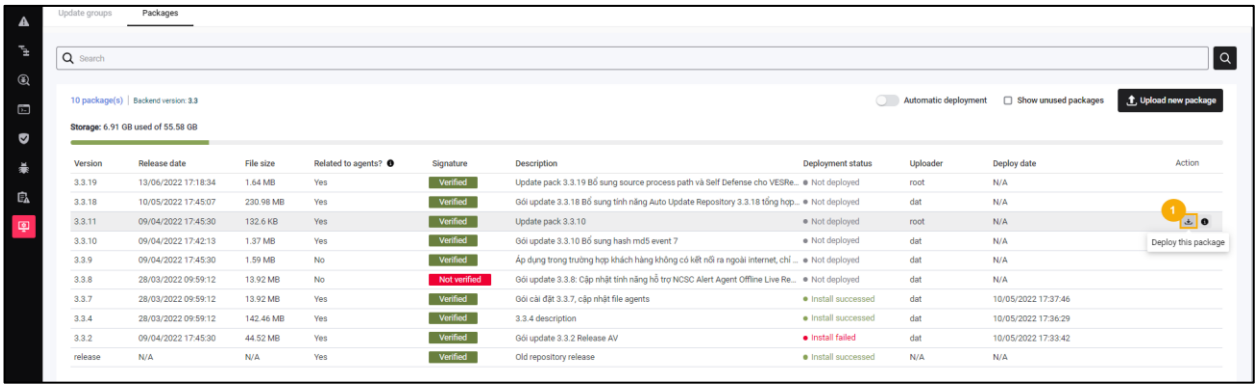
Bước 2: Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;

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

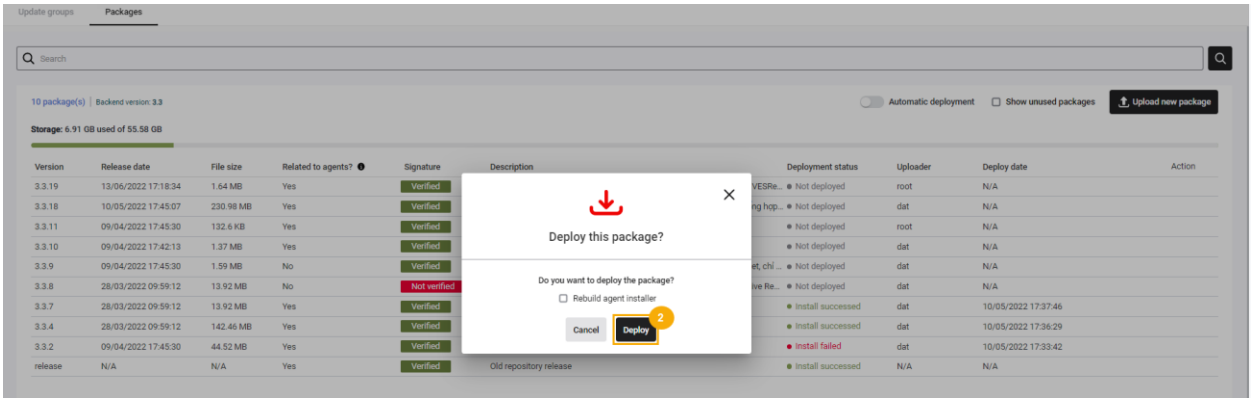
Bước 4: Chọn Tab "Package", hệ thống hiển thị Danh sách Pakage trong hệ thống;



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.



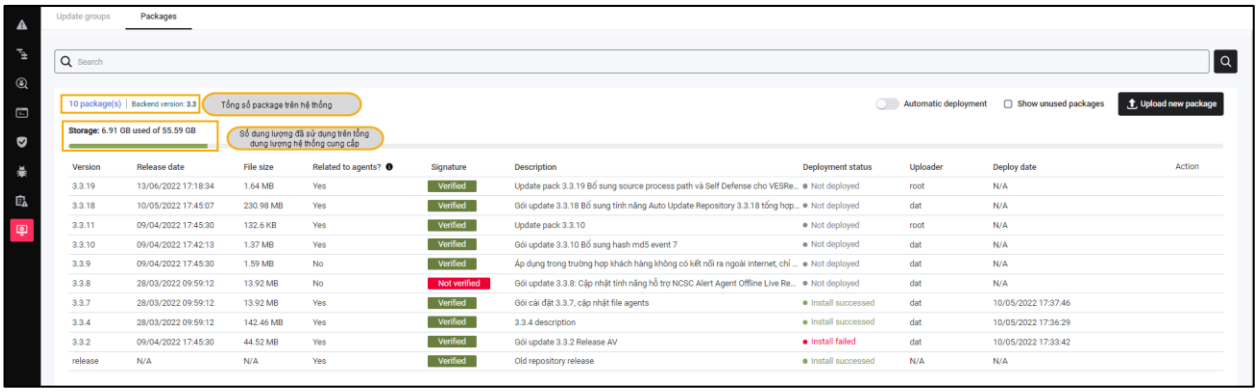
4 – Chi tiết Package

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

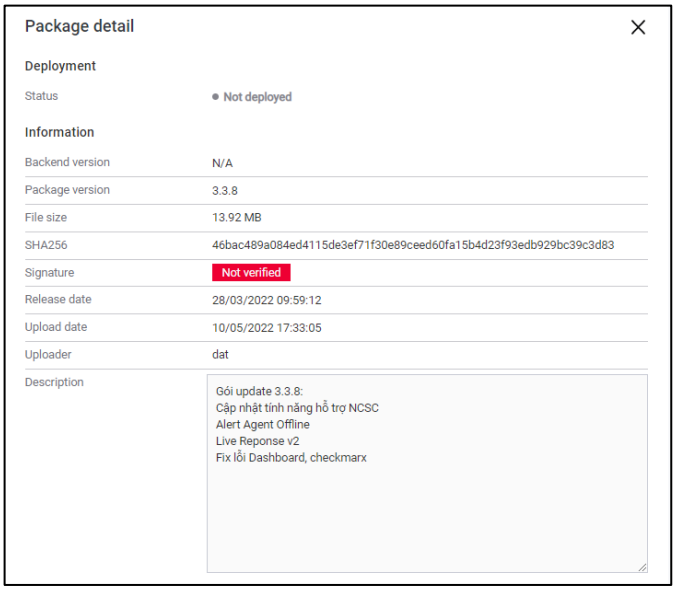
Bước 2: Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;

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:



3.7 Chức năng Baseline Policy (BLS)

3.7.1 Thống kê vi phạm (Violation statistic)

Mục đích: Chức năng Thống kê vi phạm hỗ trợ người quản trị thống kê các vi phạm của agent đã cài đặt bao gồm:

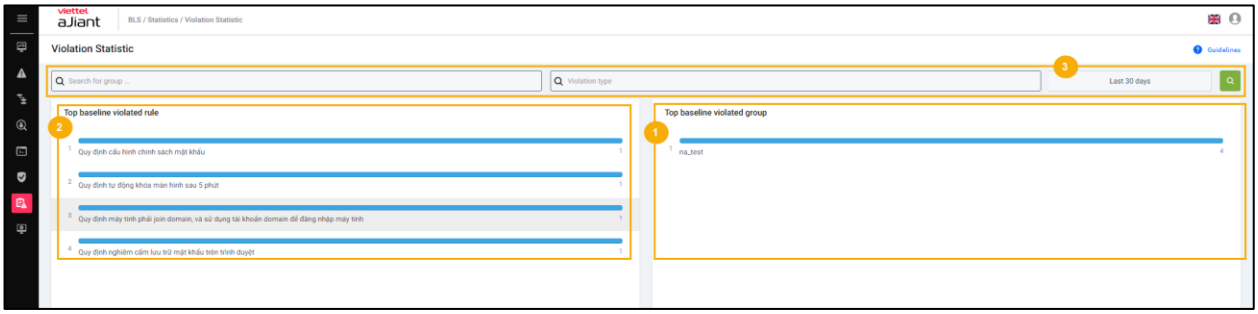
+ Top các vi phạm base line, top đơn vị vi phạm baseline;
+ Xem danh sách các vi phạm và danh sách agent vi phạm trong từng đơn vị;
+ Xem danh sách các đơn vị vi phạm và danh sách vi phạm trong từng đơn vị;
+ Xem chi tiết của Agent;

+ Export vi phạm;

+ Report vi phạm;

Click vào tab “BLS” >> Thống kê vi phạm;

3.7.1.1 Màn hình Thống kê vi phạm



Hệ thống hỗ trợ thực hiện các tính năng:

+ Thống kê Top 10 vi phạm base line nhiều nhất sắp xếp theo thứ tự giảm dần

- Mỗi bản ghi được hiển thị các thông tin gồm: Nội dung vi phạm, số lượng máy vi phạm;

- Chọn bản ghi bất kì trong Top vi phạm baseline, hệ thống sẽ di chuyển đến màn hình chi tiết tương ứng với vi phạm đã được chọn;

+ Thống kê Top 10 đơn vị vi phạm base line nhiều nhất sắp xếp theo thứ tự giảm dần:

- Mỗi bản ghi được hiển thị các thông tin gồm: Tên đơn vị vi phạm, số lượng máy vi phạm;

- Chọn bản ghi bất kì trong Top đơn vị vi phạm baseline, hệ thống sẽ di chuyển đến màn hình chi tiết tương ứng với đơn vị đã được chọn;

+ Tìm kiếm

- Tìm kiếm riêng lẻ:

- Tìm kiếm theo Đơn vị

  - Top đơn vị vi phạm hiển thị đơn vị đã nhập và danh sách đơn vị con tương ứng (nếu có);

- Top vi phạm: Hiển thị các vi phạm của đơn vị và đon vị con (nếu có) tương ứng;

- Loại vi phạm
  - Top đơn vị vi phạm: hiển thị danh sách đơn vị vi phạm Loại vi phạm đã chọn;
  - Top vi phạm: Hiển thị vi phạm đã chọn;
  - Thời gian bị vi phạm;

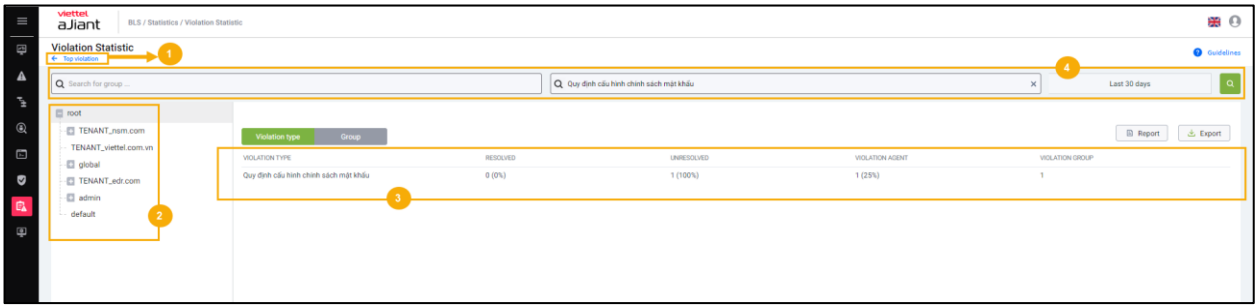
- Tìm kiếm kết hợp: Khi nhập 2 hoặc nhiều điều kiện tìm kiếm thì sẽ thực hiện tìm kiếm theo điều kiện AND;

Mô tả các rule trong BLS

Rule	Mô tả chi tiết
Quy định hiển thị đuôi mở rộng của file	Trên máy endpoint quy định phải hiển thị đuôi mở rộng của file
Quy định tắt cấu hình Remote Desktop	Tắt không cho phép Remote Desktop
Quy định tự động khóa màn hình sau 5 phút	Vi phạm không khóa màn hình sau 5 phút
Quy định tắt chức năng Autorun của USB, ổ CD	Cho phép bật/ tắt tính năng Autorun của USB, CD
Quy định làm việc không quá 19h	Máy tạm không làm việc quá 19h
Máy tính vi phạm quy định sử dụng USB 3G	Máy trạm không được sử dụng thiết bị MTP (smart phone…), USB (lưu trữ, 3g…)
Quy định nghiêm cấm kết nối trực tiếp mạng Internet	Người dùng có thể sử dụng trình duyệt để truy cập mạng hoặc thông qua system proxy

Quy định cấu hình cập nhật Hệ điều hành	Yêu cầu máy trạm bật chế độ cập nhật bản vá hệ điều hành tự động
Quy định cài đặt và sử dụng phần mềm	Máy trạm vi phạm rule này khi cài đặt hoặc không cài đặt các phần mềm được cấu hình
Quy định bắt buộc cài đặt và sử dụng phần mềm diệt virus	Yêu cầu máy trạm phải cài đặt phần mềm antivirus: luôn bật chức năng realime protection và thiết lập cấu hình update.
Quy định bắt buộc sử dụng phần mềm vượt tường lửa	Yêu cầu máy trạm phải bật firewall trên hệ điều hành hoặc trên phần mềm antivirus
Quy định cài đặt và sử dụng phần mềm diệt virus Kaspersky	Yêu cầu máy trạm bắt buộc phải cài phần mềm AV Kaspersky
Quy định máy tính phải join domain, và sử dụng tài khoản domain để đăng nhập máy tính	Quy định máy tính phải join domain, và sử dụng tài khoản domain để đăng nhập máy tính
Quy định thu hồi tài khoản local	Tự động thu hồi (remove) tài khoản local khi vi phạm
Quy định nghiêm cấm lưu trữ mật khẩu trên trình duyệt	Nghiêm cấm lưu trữ mật khẩu trên trình duyệt
Quy định cấu hình chính sách mật khẩu	Quy định bao gồm các rule sau: + Đáp ứng đủ số kí tự +Thay đổi mật khẩu sau một khoảng thời gian được config + Tài khoản bị khóa sau khi nhập sai nhiều lần

3.7.1.2 Tab Loại vi phạm



Hệ thống hỗ trợ thực hiện các tính năng:

+ Chọn link Top vi phạm: Di chuyển về màn hình Dashboard, danh sách top vi phạm và top đơn vị vi phạm

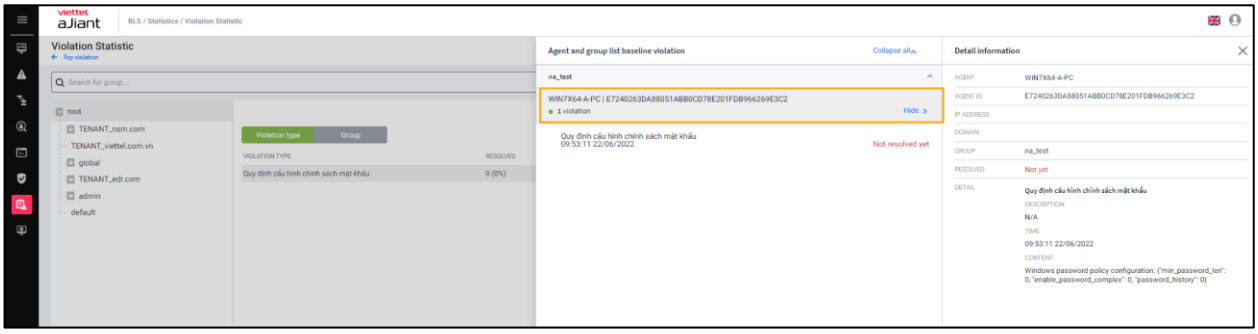
+ Cây dữ liệu đơn vị của hệ thống

- Hiển thị toàn bộ đơn vị của hệ thống được phân cấp cha-con;
- Có thể chọn đơn vị trên cây dữ liệu đơn vị để thực hiện lọc vi phạm;

+ Tab Loại vi phạm:

- Mỗi Loại vi phạm được hiển thị các thông tin chung gồm: Violation type, Resolved, Unresolved, Violation Computer, Violation unit;
- Chọn bản ghi Loại vi phạm trên danh sách: Hiển thị danh sách máy tính trong từng đơn vị vi phạm;
- Chọn máy tính: Hiển thị thông tin chi tiết máy tính và danh sách vi phạm tương ứng của máy tính;

Chọn máy tính trên popup danh sách máy tính: hiển thị popup thông tin chi tiết máy tính bao gồm Computer, AgentID, IP Address, Domain, Group, Resolved, Detail (tất cả loại vi phạm của máy)



Tìm kiếm

+ Tìm kiếm riêng lẻ:

- Tìm kiếm theo Đơn vị: Hiển thị đơn vị đã nhập và danh sách đơn vị con tương ứng
- Loại vi phạm: Hiển thị vi phạm đã chọn
- Thời gian bị vi phạm

+ Tìm kiếm kết hợp: Khi nhập 2 hoặc nhiều điều kiện tìm kiếm thì sẽ thực hiện tìm kiếm theo điều kiện AND

3.7.1.3 Tab Đơn vị

Hệ thống hỗ trợ thực hiện các tính năng:

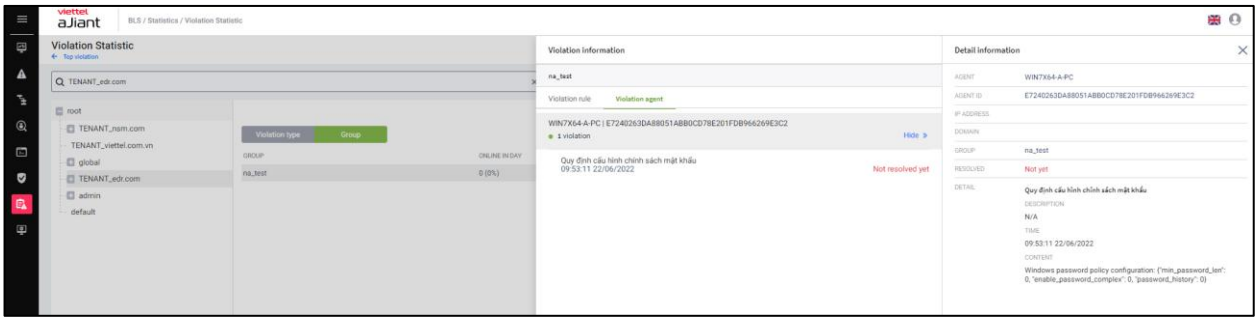
+ Chọn link Top đơn vị: Di chuyển về màn hình Dashboard, danh sách top vi phạm và top đơn vị vi phạm;

+ Cây dữ liệu đơn vị của hệ thống;

- Hiển thị toàn bộ đơn vị của hệ thống được phân cấp cha-con;
- Có thể chọn đơn vị trên cây dữ liệu đơn vị để thực hiện lọc đơn vị cha – con;

+ Tab Đơn vị;

- Mỗi Loại vi phạm được hiển thị các thông tin chung gồm: Unit, Online in day, Online in 30 days recent, Resolved, Unresolved, Violation computer, Violation rule;
- Chọn icon detail của cột violation computer trên danh sách: Hiển thị danh sách máy tính trong từng đơn vị vi phạm bao gồm Tên đơn vị, Tên máy tính|Agent ID, danh sách vi phạm của từng máy, thời gian vi phạm, trạng thái vi phạm (đã fix hay chưa fix vi phạm);



Chọn máy tính trên popup danh sách máy tính: hiển thị popup thông tin chi tiết máy tính bao gồm Computer, AgentID, IP Address, Domain, Group, Resolved, Detail (tất cả loại vi phạm của máy);

Chọn icon detail của cột violation rule trên danh sách: Hiển thị danh sách vi phạm của đơn vị;

Tìm kiếm

+ Tìm kiếm riêng lẻ:

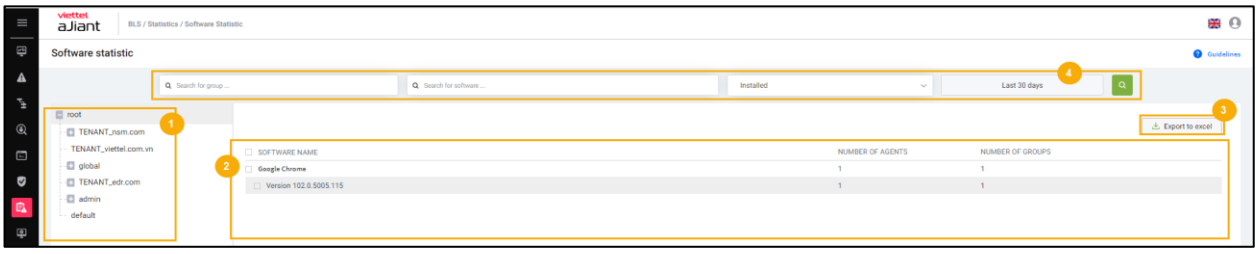
- Tìm kiếm theo Đơn vị: Hiển thị đơn vị đã nhập và danh sách đơn vị con tương ứng;
- Loại vi phạm: Hiển thị vi phạm đã chọn;
- Thời gian bị vi phạm;

+ Tìm kiếm kết hợp: Khi nhập 2 hoặc nhiều điều kiện tìm kiếm thì sẽ thực hiện tìm kiếm theo điều kiện AND;

3.7.2 Thống kê phần mềm (Software statistic)

Mục đích: Chức năng Thống kê phần mềm hỗ trợ người quản trị thống kê các phần mềm đã cài đặt trong một đơn vị bao gồm:

+ Xem danh sách các phần mềm đã cài trong 1 đơn vị được chọn;
+ Xem chi tiết của Agent;
+ Export phần mềm;



Hệ thống hỗ trợ thực hiện các tính năng:

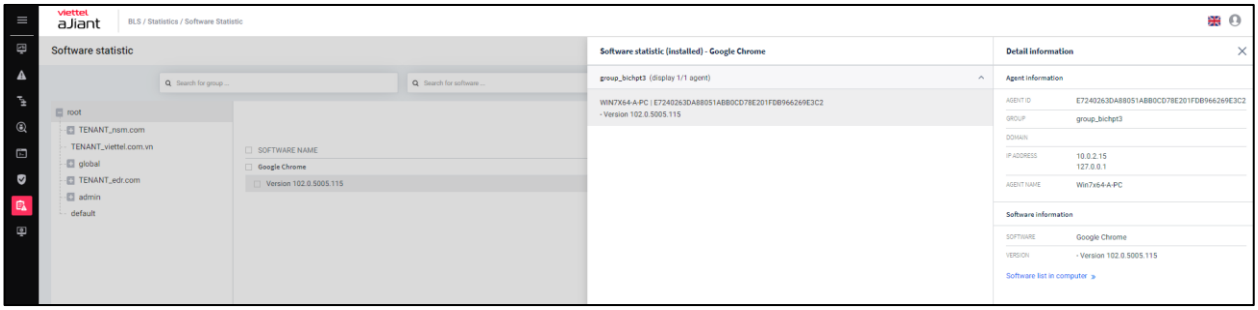
+ Cây dữ liệu đơn vị của hệ thống

+ Hiển thị toàn bộ đơn vị của hệ thống được phân cấp cha-con
+ Có thể chọn đơn vị trên cây dữ liệu đơn vị để thực hiện lọc phần mềm
+ Danh sách phần mềm

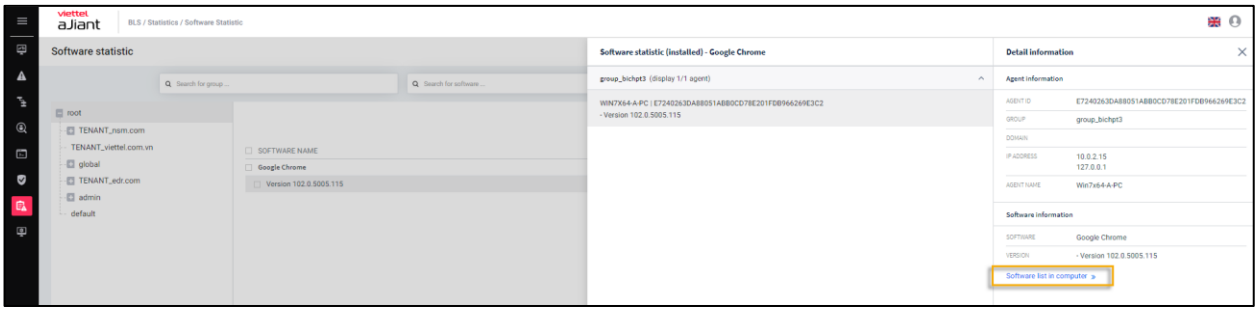
- Mỗi phần mềm được hiển thị các thông tin chung gồm: Software name, munber of computer, munber of unit;

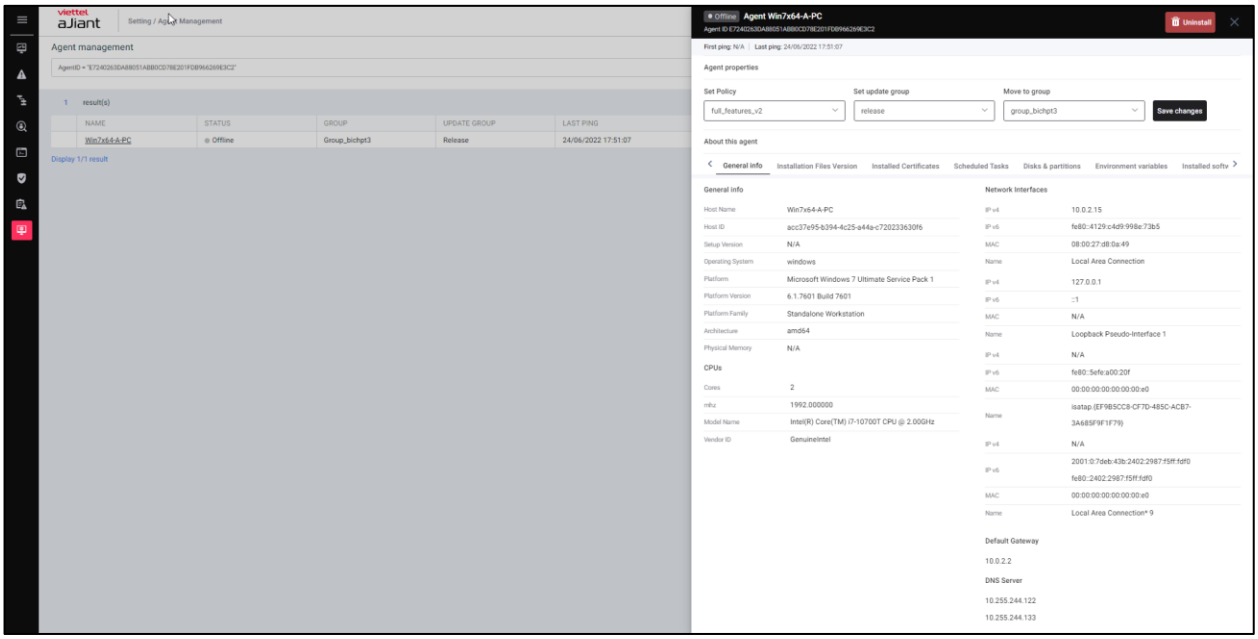
- Chọn icon detail của cột violation computer trên danh sách: Hiển thị danh sách máy tính trong từng đơn vị bao gồm Tên đơn vị, Tên máy tính|Agent ID, Version;

- Chọn máy tính trên popup danh sách máy tính: hiển thị popup thông tin chi tiết máy tính bao gồm Computer, AgentID, IP Address, Domain, Group, Software information (software name, version);



- Chọn link [List softwares in computer]: Hệ thống đi chuyển đến màn hình Agent management và popup chi tiết máy tính tương ứng đã chọn hiển thị;





Tìm kiếm

+ Tìm kiếm riêng lẻ:

- Tìm kiếm theo Đơn vị: Hiển thị các phần mềm đã cài trong đơn vị
- Tên phần mềm: hiển thị danh sách phần mềm đã nhập
- Tìm kiếm theo trạng thái: Installed, uninstalled
- Thời gian cài

+ Tìm kiếm kết hợp: Khi nhập 2 hoặc nhiều điều kiện tìm kiếm thì sẽ thực hiện tìm kiếm theo điều kiện AND

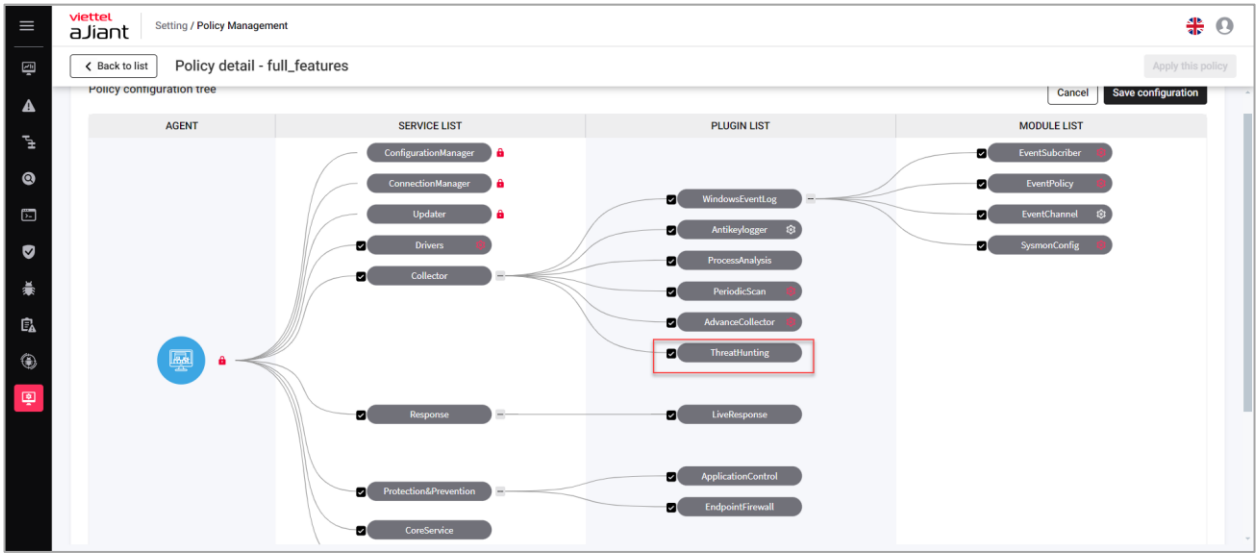
Export: Chọn Export: Hệ thống sẽ download file Export có dữ liệu giống với dữ liệu đang hiển thị trên màn hình

3.8 Threat Hunting

Tính năng Threat Hunting cho phép người dùng tìm kiếm các dấu hiệu nghi ngờ tấn công, IOCs của các máy trạm trong tổ chức, từ đó sẽ có các phương án ứng phó và xử lý sớm. Tính năng sẽ hỗ trợ trong việc

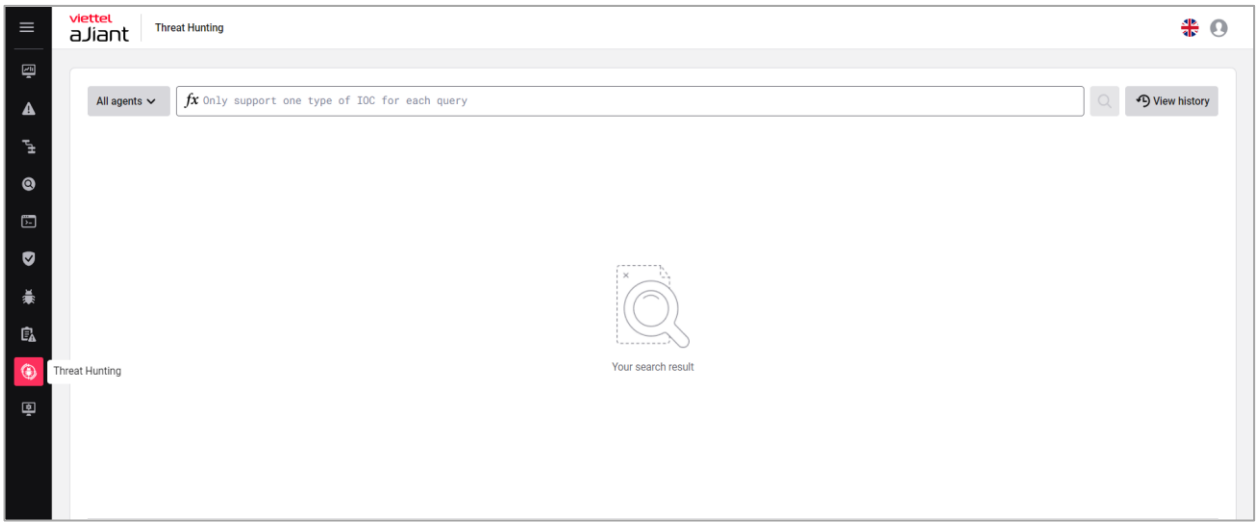
3.8.1 Bật/tắt policy

- Để có thể sử dụng tính năng Threat Hunting, cần bật policy trong Policy Management -> Chọn service Collector -> Chọn plugin ThreatHunting
- Lưu ý: Agent cần được apply policy bật ThreatHunting mới có thể thực hiện tìm kiếm iocs

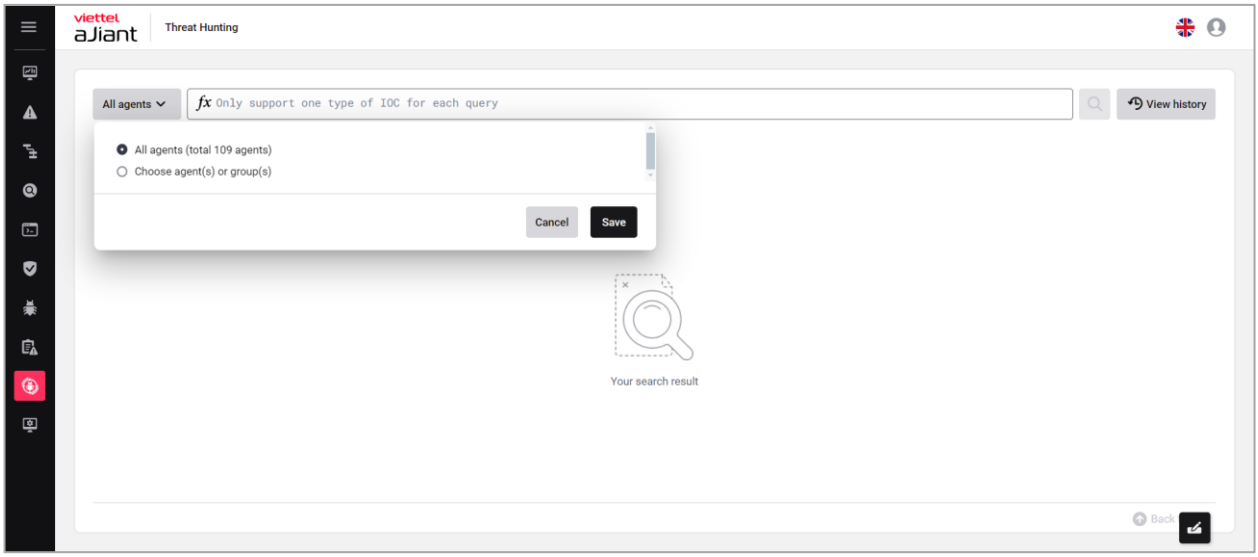


3.8.2 Tìm kiếm theo agents/ nhóm

- Trên Menu chọn Threat Hunting



- Cho phép admin tìm kiếm iocs theo agents/ groups
    - Cho phép tìm kiếm trên toàn bộ agents (All agents)
    - Cho phép tìm kiếm theo từng agent cụ thể hoặc chọn theo nhóm



3.8.3 Tìm kiếm IOCs

3.8.3.1 **Các loại IOCs hỗ trợ**

- Người dùng có thể tìm kiếm theo các loại iocs dưới bảng sau:

IOCs	Tab	Query field	Toán tử hỗ trợ	Note

File path	File	file_path	=, ~	Tìm kiếm theo đường dẫn file
File name	File	file_name	=,~	Tìm kiếm theo tên file
File hash SHA256	File	file_sha256	=	Tìm kiếm file hash SHA256
Registry path	Registry	registry_path	=,~	Tìm kiếm theo đường dẫn Registry
Registry key	Registry	registry_key	=,~	Tìm kiếm theo Registry key
Registry data	Registry	registry_data_string	~	Tìm kiếm theo Registry data kiểu string, dword, binary
		registry_data_dword	=	
		registry_data_binary	=,~	
Strings Memory	Memory	strings_memory	~	Cho phép tìm kiếm theo string memory
Hex Memory	Memory	Hex_memory	~	Cho phép tìm kiếm theo dạng hex
User Name	User	User_name	=,~	Cho phép tìm kiếm theo user trên máy endpoint
Domain	Network	Domain	=,~	Cho phép tìm kiếm theo domain mà các máy endpoint đã từng truy cập

IP	Network	Domain	=,~	Cho phép tìm kiếm theo ip mà các máy endpoint đã từng truy cập
Process Path	Process	Process_path	=,~	Cho phép tìm kiếm theo đường dẫn của process
Process Command Line	Process	Process_commandline	=, ~	Cho phép tìm kiếm theo process commandline
DLL	DLL	Dll_path	=, ~	Cho phép tìm kiếm theo đường dẫn dll

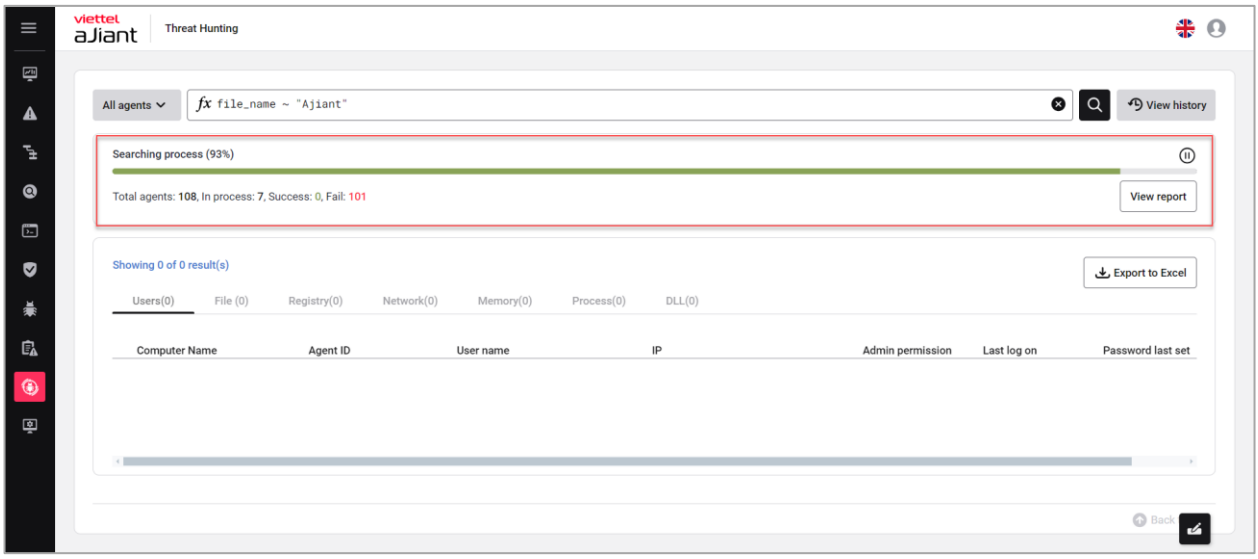
Lưu ý:

- Người dùng chỉ được phép tìm kiếm theo một loại IOCs trên cùng một câu query
- Cho phép tìm kiếm theo các điều kiện AND, OR
- Giá trị tìm kiếm không phân biệt chữ hoa, chữ thường
- Sau khi người dùng thực hiện tìm kiếm, hệ thống thực hiện quét trên máy endpoint theo đúng yêu cầu truy vấn và gửi kết quả về portal.
- Thời gian tìm kiếm phụ thuộc vào độ phức tạp của câu truy vấn và số lượng máy agent thực hiện tìm kiếm.

3.8.3.2 Chi tiết kết quả tìm kiếm

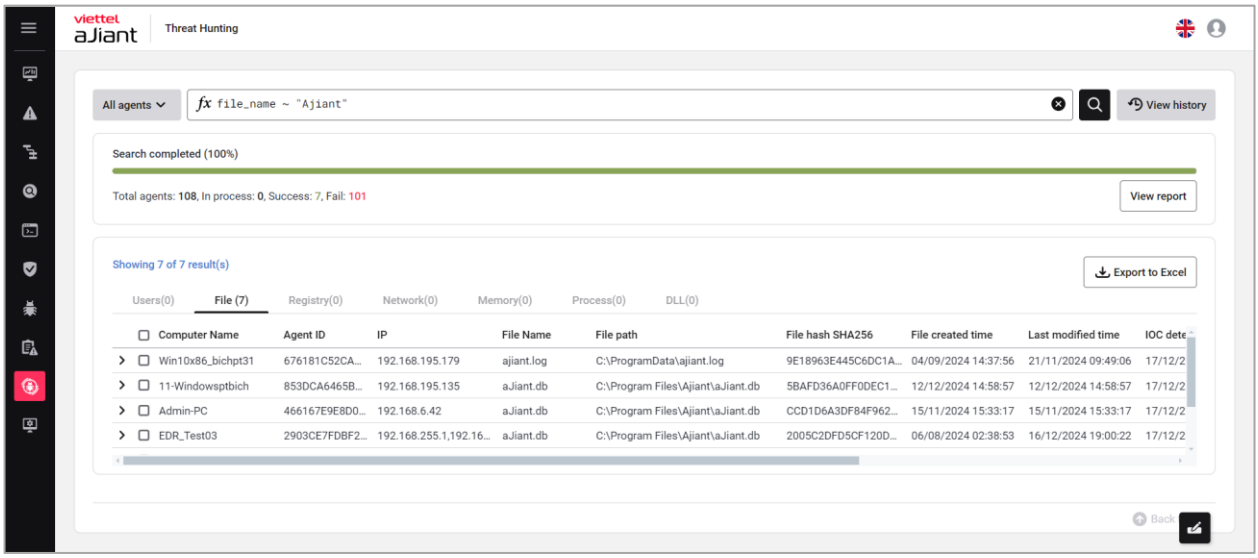
Theo dõi trạng thái tìm kiếm

- Cho phép người dùng theo dõi tiến trình tìm kiếm
    - Total agent: Tổng số agent thực hiện tìm kiếm
    - In-process: Đang thực hiện tìm kiếm
    - Success: Tìm kiếm thành công
    - Fail: Tìm kiếm thất bại



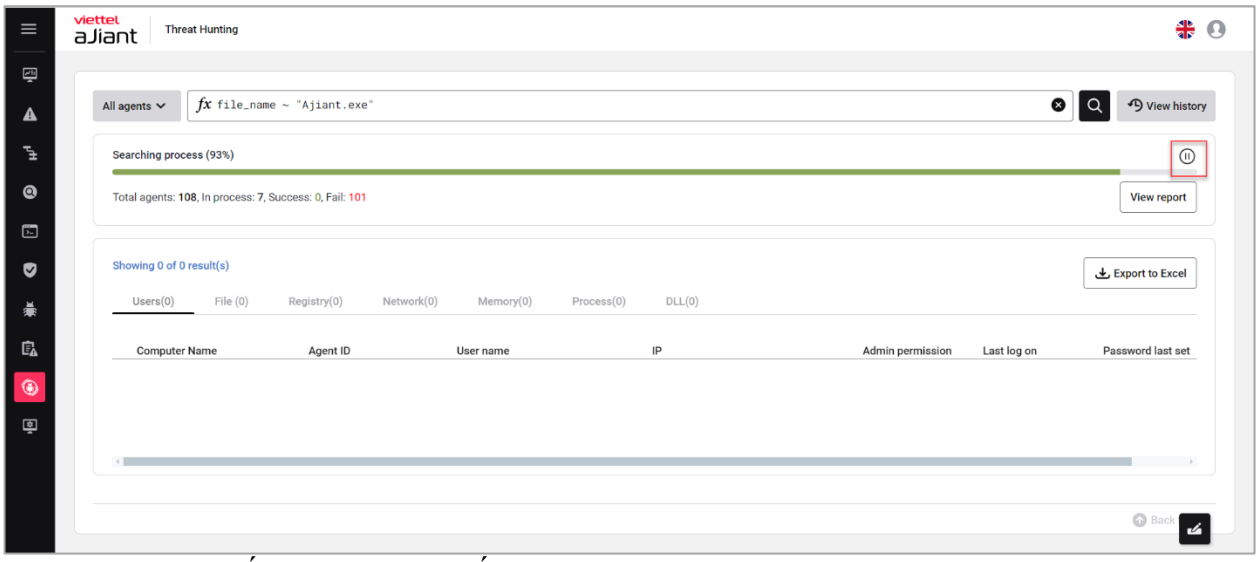
Chi tiết kết quả tìm kiếm

- Cho phép người dùng xem chi tiết kết quả tìm kiếm theo từng tab
    - Users
    - File
    - Registry
    - Network
    - Memory
    - Process
    - DLL
- Kết quả được hiển thị đúng theo từng tab theo đúng câu truy vấn của người dùng



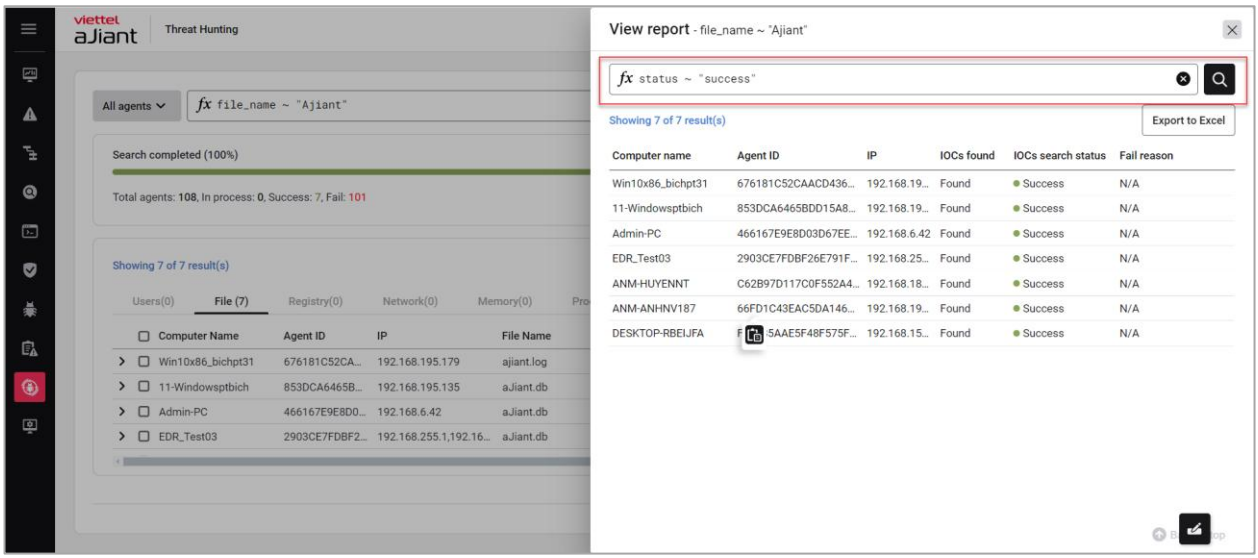
Dừng tìm kiếm

- Cho phép người dùng dừng việc tìm kiếm: Trên Searching Process bar -> chọn button Pause
- Sau khi Dừng tìm kiếm:
    - Hệ thống sẽ dừng việc tìm kiếm
    - Không hỗ trợ thực hiện tiếp tục tìm kiếm câu truy vấn



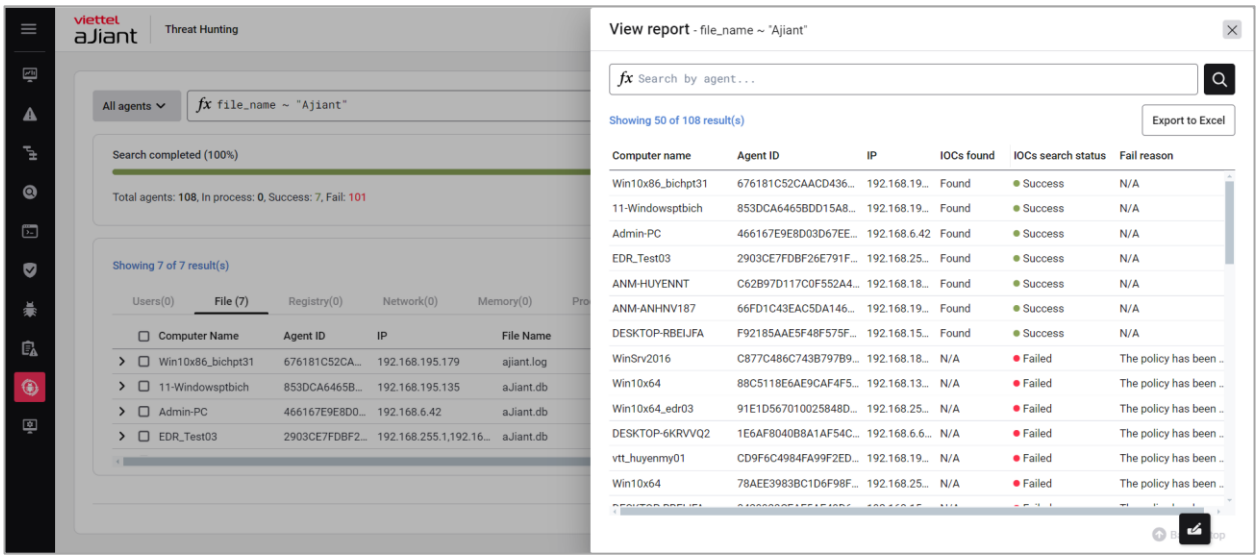
Xem chi tiết báo cáo tìm kiếm iocs dưới agents (View report)

- Cho phép người dùng tìm kiếm theo thông tin Computer name, AgentID, IP, IOCs Search Status



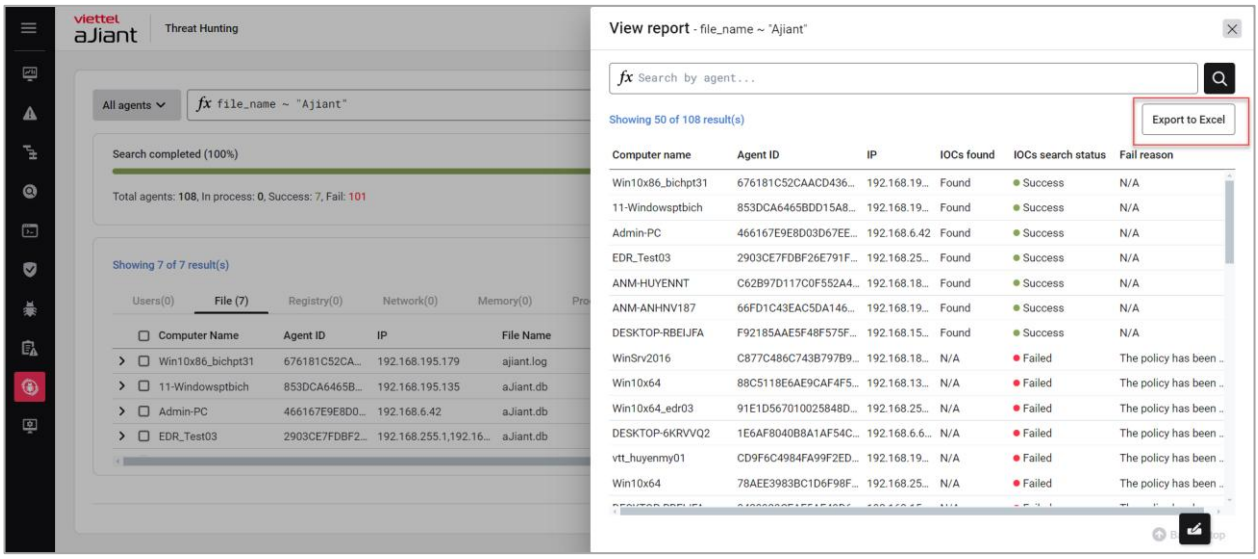
- Báo cáo này sẽ cung cấp cho người dùng chi tiết về trạng thái tìm kiếm iocs trên từng agent. Các thông tin trên báo cáo gồm có:
    - Computer name

- Agent ID
- IP
- IOCs found: Có tìm thấy dấu hiệu IOCs dựa trên câu truy vấn của người dùng hay không
- IOCs search status: Trạng thái tìm kiếm iocs trên agent
- Fail reason: Chi tiết lí do tìm kiếm thất bại



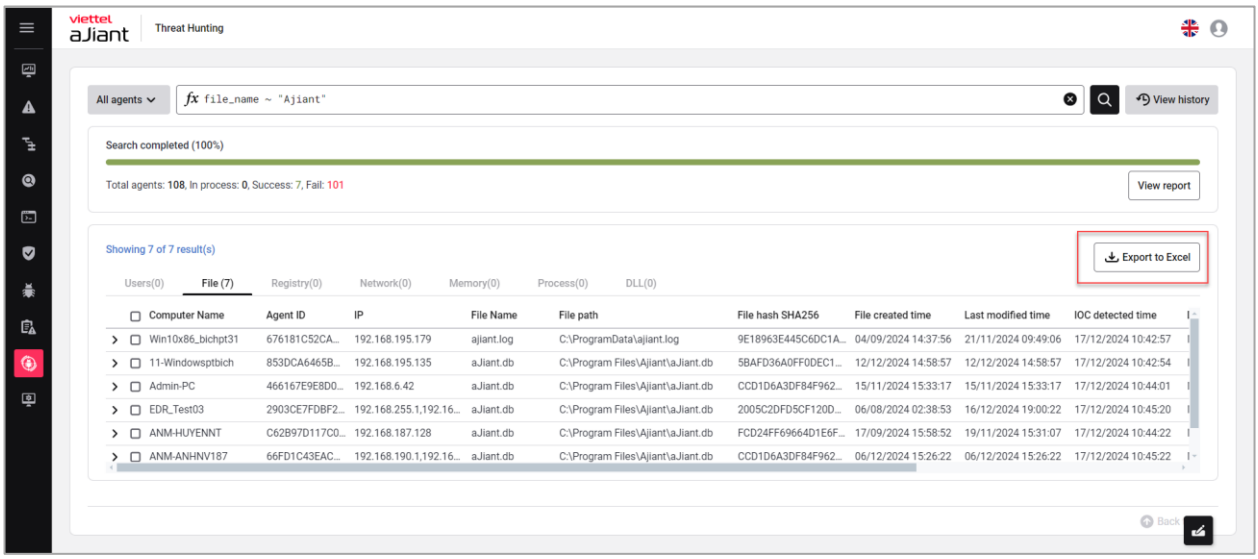
Export to Excel

- Cho phép người dùng tải xuống file excel tổng hợp kết quả tìm kiếm dưới agent
- Các thông tin trên file bao gồm
  - Computer name
  - Agent ID
  - IP
  - IOCs found: Có tìm thấy dấu hiệu IOCs dựa trên câu truy vấn của người dùng hay không
  - IOCs search status: Trạng thái tìm kiếm iocs trên agent
  - Fail reason: Chi tiết lí do tìm kiếm thất bại



Tải xuống kết quả tìm kiếm

- Cho phép người dùng tải xuống kết quả tìm kiếm iocs trên máy agent
- Hỗ trợ tải xuống file excel

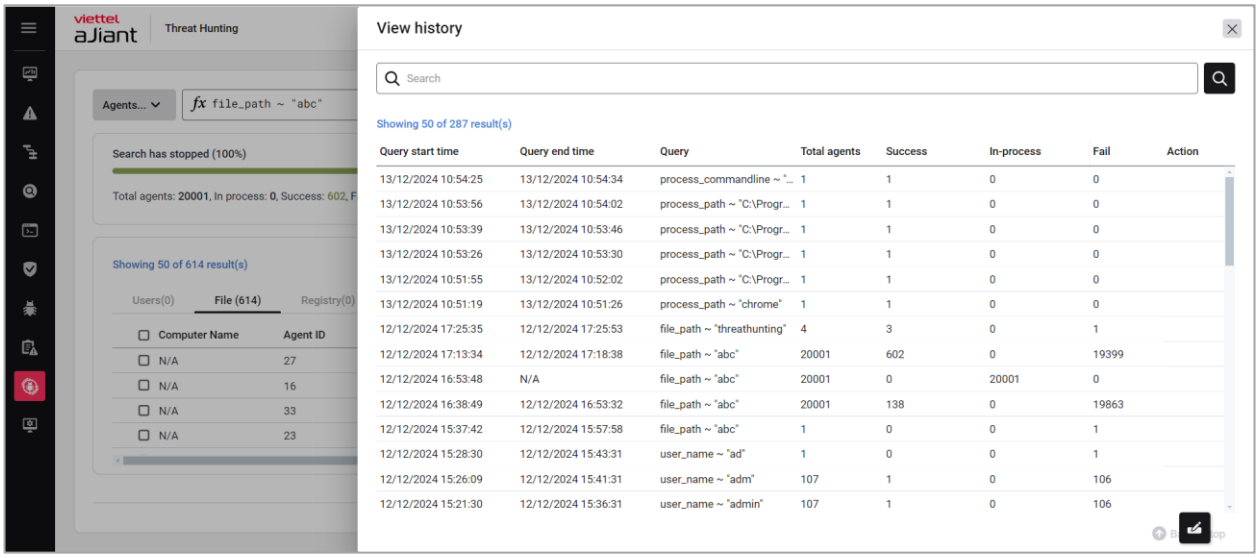


3.8.4 Xem lịch sử truy vấn (View History)

3.8.4.1 Xem danh sách truy vấn

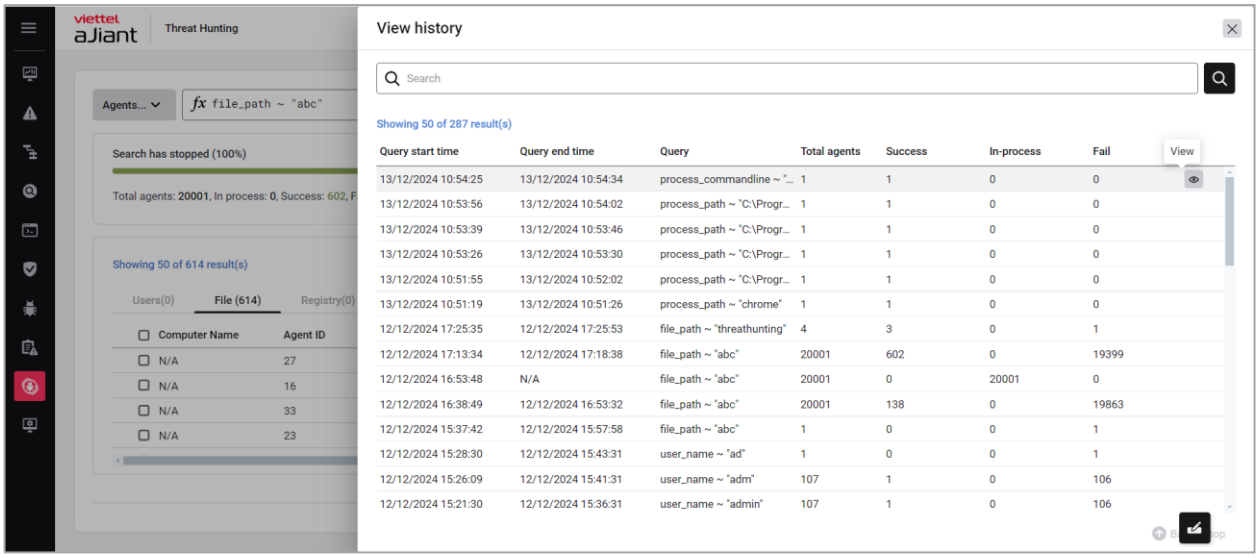
- Cho phép người dùng xem lại lịch sử truy vấn. Thông tin lịch sử truy vấn gồm có các thông tin sau:
    - Query start time: Thời gian bắt đầu thực hiện query
    - Query end time: Thời gian tìm kiếm xong

- Query: câu truy vấn của người dùng
- Total agents: Tổng số agent đã tìm kiếm
- Susccess: Tìm kiếm thành công trên máy endpoint
- In-process: Đang trong quá trình tìm kiếm trên máy endpoint
- Fail: Tìm kiếm thất bại

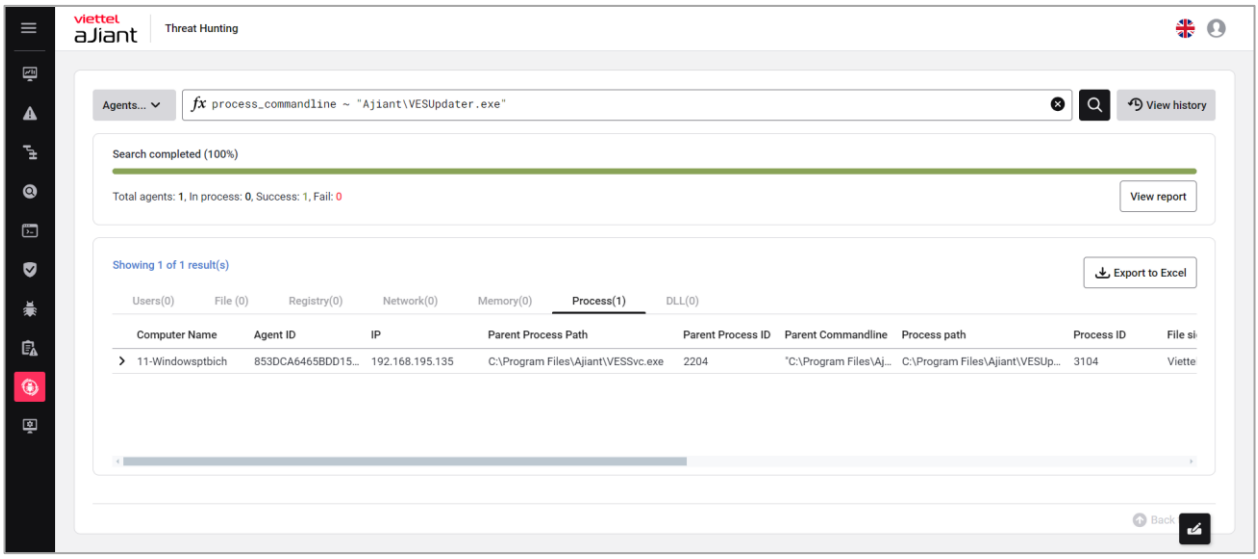


3.8.4.2 Xem chi tiết lịch sử truy vấn

- Cho phép người dùng xem chi tiết lại kết quả của từng lần truy vấn: Action -> chọn View



- Cho phép xem chi tiết kết quả của lần truy vấn trong lịch sử:



3.9 Rules Correlation

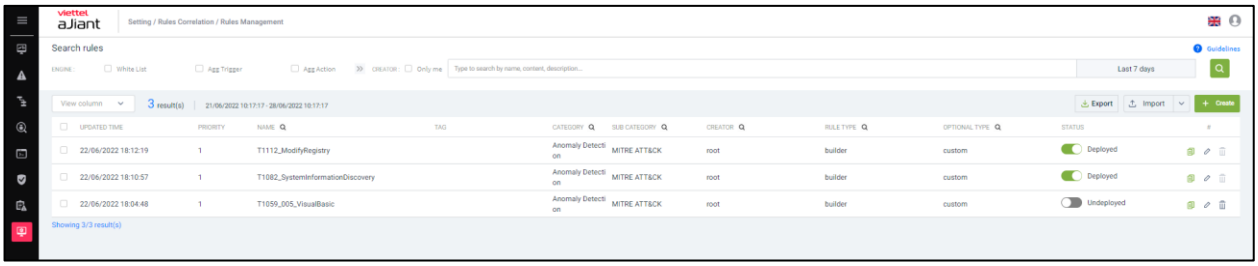
3.9.1 Danh sách hiển thị

Mục đích: Chức năng cho phép người dùng xem danh sách rules correlation trong hệ thống. Nhập hoặc chọn điều kiện tìm kiếm để thực hiện tìm kiếm rule đang có trên hệ thống, thao tác deploy/undeploy/xóa nhanh với các rule.

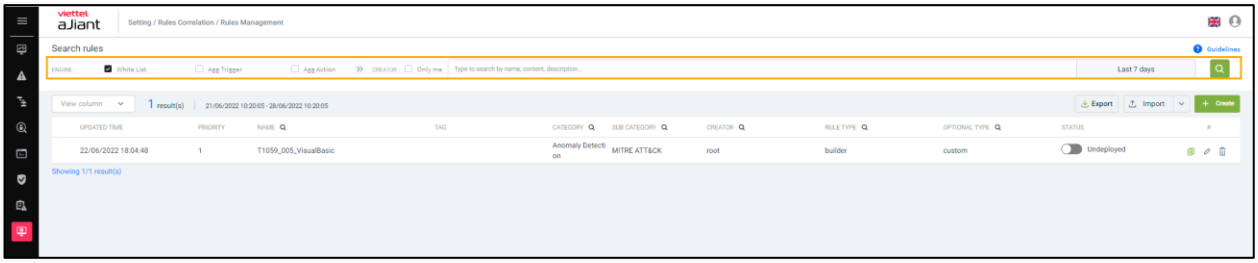
+ Bộ lọc FITTER;

+ Bộ lọc FITTER bao gồm:

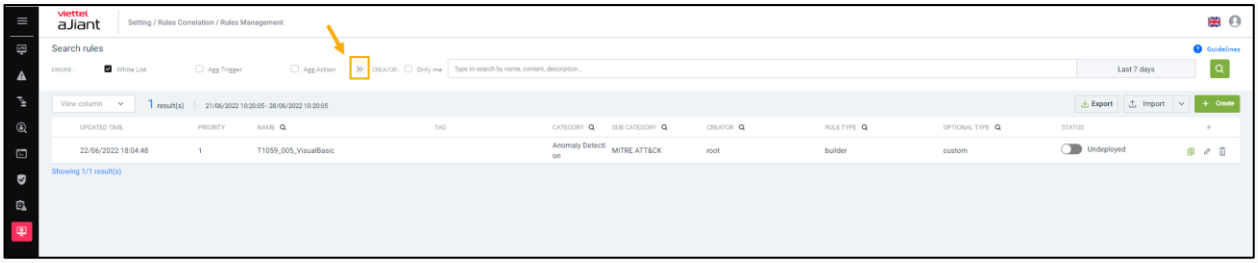
- 6 Engine: Whitelist, Agg Trigger, Agg Action, Filter, Indicator, False-Positive;
- Text box search theo các trường: Name, content, description;
- Thời gian cập nhật;
- Tạo bởi tôi;
- Lọc theo **Engine;**



Bước 1: Chọn 1 hoặc nhiều Engine mặc định;

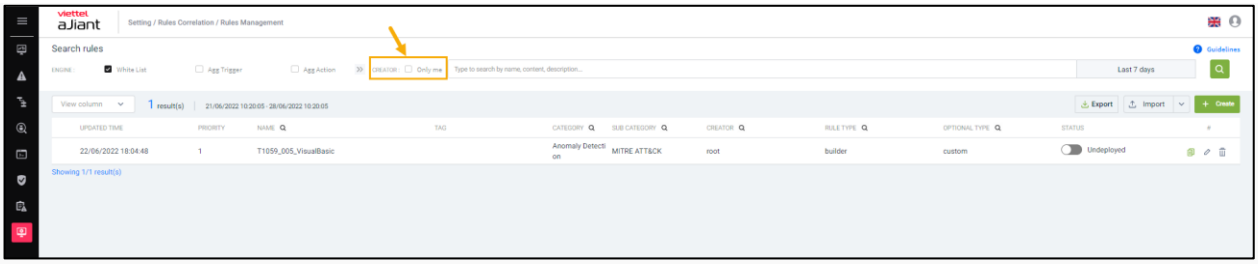


Bước 2: Chọn Mở rộng để thêm các Engine cần lọc;

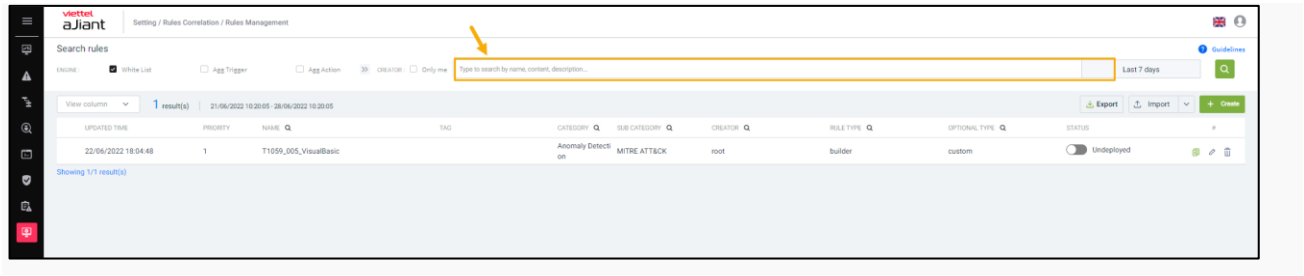


Khi chọn 2 hoặc nhiều Engine, màn hình trả về kết quả được lọc theo phép toán AND;

Bước 3: Tích chọn người tạo Rules là user đang login vào hệ thống;



Bước 4: Nhập Name, content, description muốn search vào text box;



Bước 5: Nhập thông tin cần tìm kiếm;

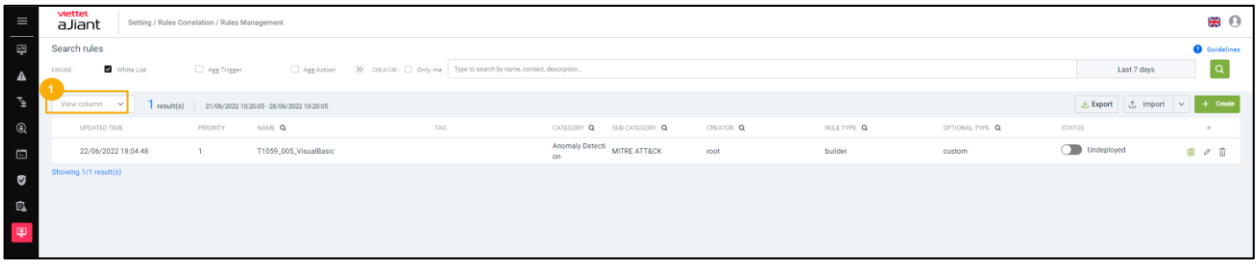
Bước 6: Nhấn Search để hiển thị kết quả tìm kiếm.

Chọn cột

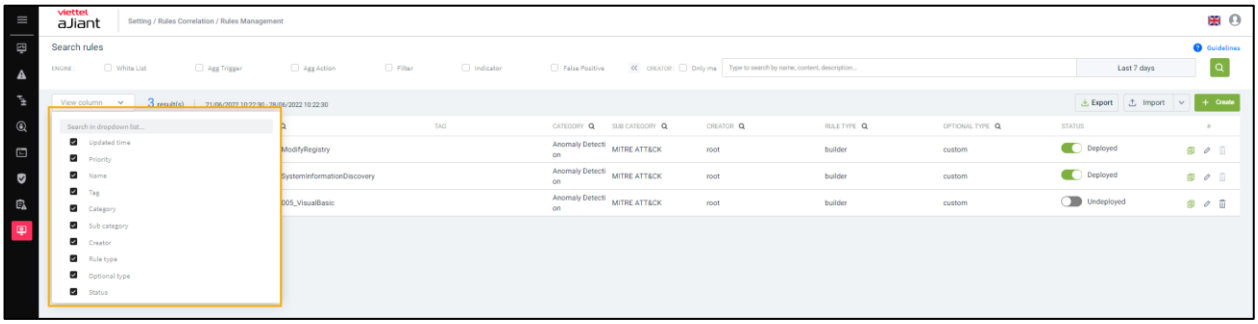
Cho phép người dùng lựa chọn các cột hiển thị trên màn hình correlation.

Các bước thực hiện:

Bước 1: Click vào combo box View column. Màn hình hiển thị danh sách lựa chọn các cột ở dạng check box;



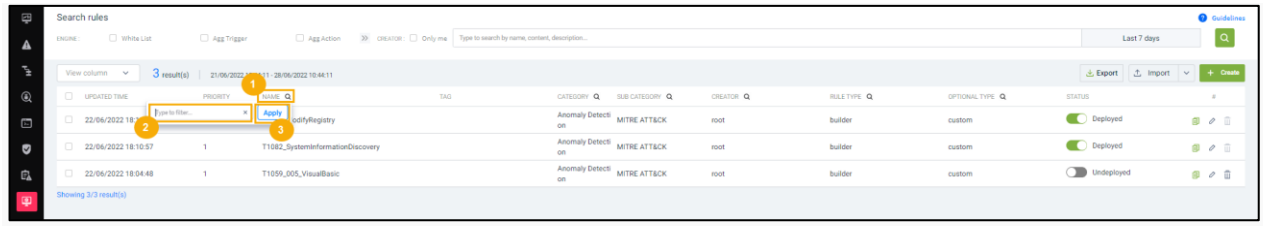
Bước 2: Chọn vào những tên cột muốn hiển thị;



1 – Hỗ trợ tìm kiếm nhanh

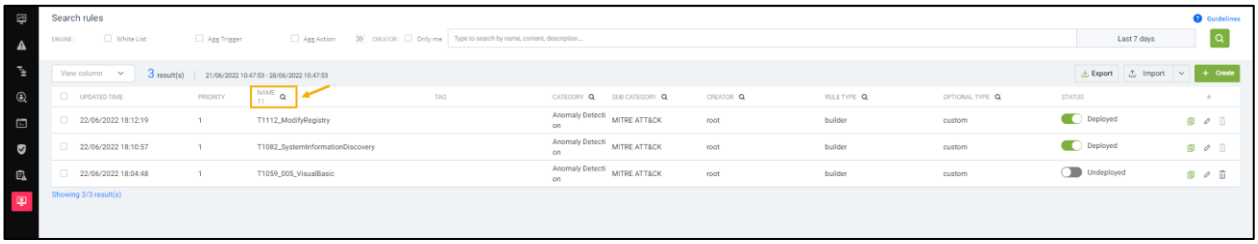
- Tìm kiếm theo tên rule

Bước 1: Click icon  để hiển thị thanh tìm kiếm;



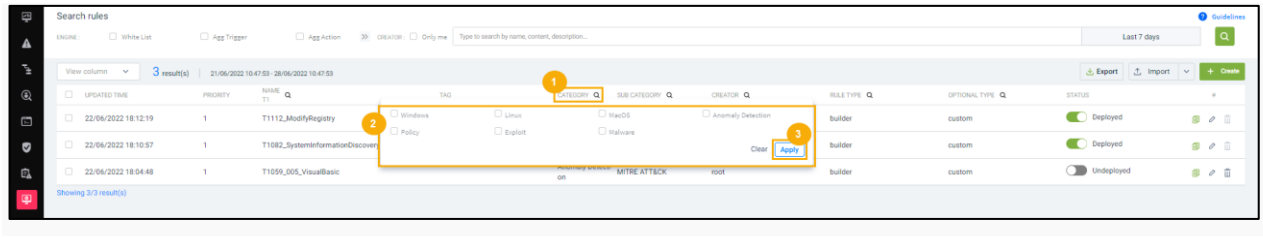
Bước 2: Nhập tên rules muốn tìm kiếm;

Bước 3: Nhấn Enter để hiển thị kết quả tìm kiếm.



Tìm kiếm theo Category: Hỗ trợ tìm kiếm nhanh gồm 3 loại mặc định là: Windows, Linux, MacOS.

Bước 4: Click icon để hiển thị danh sách loại Category;



Bước 5: Chọn category muốn tìn kiếm;

Bước 6: Click “Apply”;

Tìm kiếm Sub Category: Hỗ trợ tìm kiếm nhanh theo loại triển khai, gồm 3 loại mặc định là: Metre ATT&CK, Malware, Suspicious Behaviour:

Bước 1: Click icon để hiển thị thanh tìm kiếm;

Bước 2: Chọn sub category muốn tìn kiếm;

Bước 3: Click “Apply”;

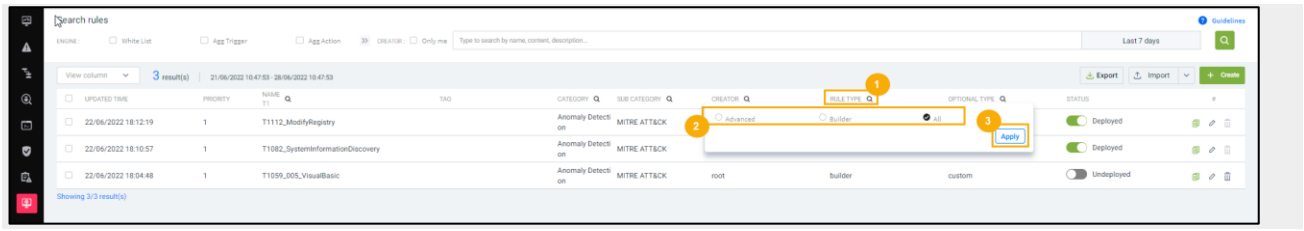
Tìm kiếm Creator

Bước 1: Click icon  để hiển thị thanh tìm kiếm;

Bước 2: Nhập tên người tạo muốn tìn kiếm;

Bước 3: Click “Apply”;

Tìm kiếm Rule type: Hỗ trợ tìm kiếm nhanh gồm 3 loại mặc định là: Advanced, Builder, All.

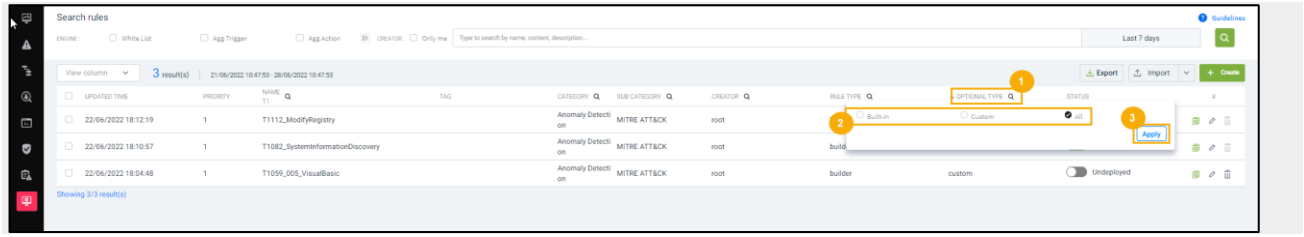


Bước 1: Click icon  để hiển thị danh sách Rule type;

Bước 2: Click vào “Rule type” muốn tìm kiếm;

Bước 3: Click “Apply”;

Tìm kiếm Optional type: Hỗ trợ tìm kiếm nhanh gồm 3 loại mặc định là: Built-in, Custom, All.

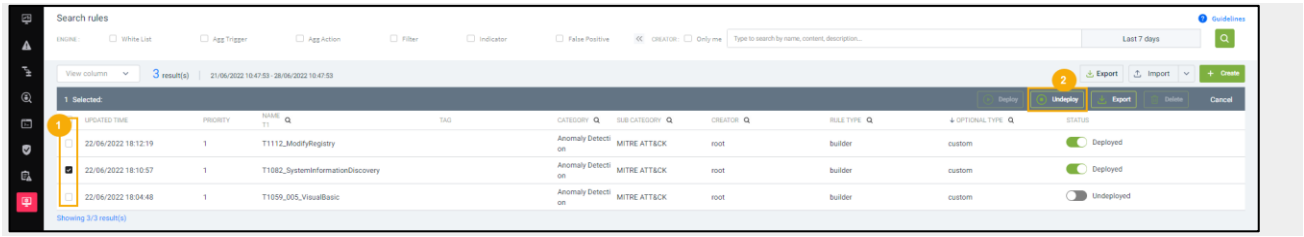


Bước 1: Click icon  để hiển thị danh sách Optional type;

Bước 2: Click “Optional” type muốn tìn kiếm;

Bước 3: Click “Apply”;

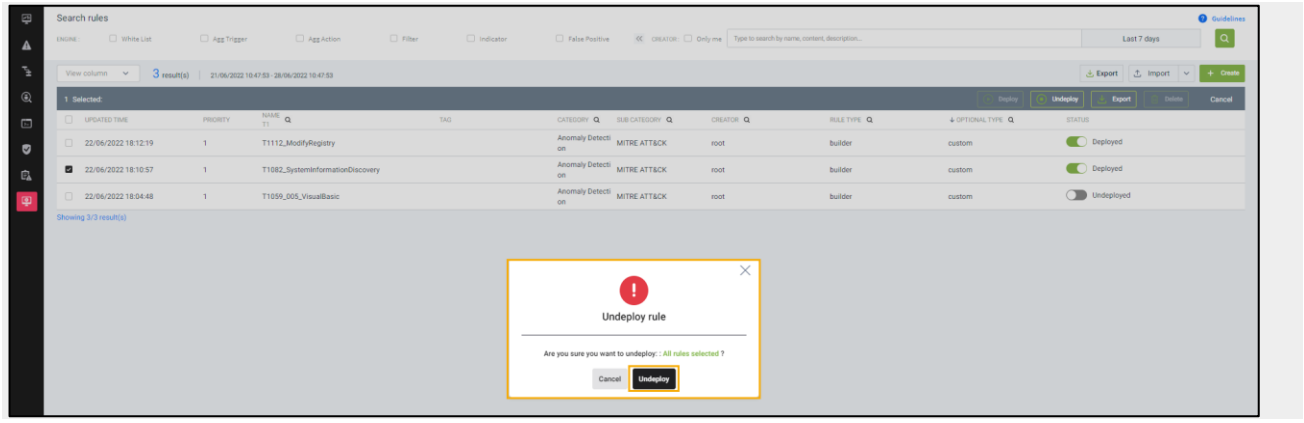
Hỗ trợ Deploy/Undeploy cho nhiều Rules



Bước 1: Click vào nhiều check box có cùng trạng thái là Deploy hoặc Undeploy;

Bước 2: Click vào nút "Deploy/Undeploy";

Bước 3: Chọn "Deploy/Undeploy" trên popup hiển thị để thực hiện Deploy/Undeploy;



3.9.2 Thêm mới Rules Correlation

Mục đích: Chức năng cho phép người dùng cấu hình một rule correlation mới hoàn chỉnh.

Tổng quan

+ Engine: Gồm tất cả 6 engine với thông tin chi tiết lần lượt là:

- Whitelist là một Stateless Engine thực hiện loại bỏ nhanh các event mà hệ thống không cần xử lý. Các event khớp với rule whitelist sẽ bị drop khỏi luồng xử lý;

- Agg_trigger và Agg_action là một Stateful Engine thực hiện gom nhóm các event tương tự nhau. Mỗi rule aggregate chứa các thông tin về điều kiện gom nhóm (định nghĩa event tương tự nhau), khoảng thời gian gom nhóm (ví dụ 30s, 1 phút, 2 phút, …). Các event khớp điều kiện gom nhóm được lưu lại và chỉ trả về một event có kèm theo số lượng sau một khoảng thời gian. Các event không khớp điều kiện gom nhóm được trả ra ngay lập tức với số lượng là 1;

- Filter là một Stateless Engine thực hiện lọc các điều kiện để đẩy vào indicator;
- Indicator là một Stateful Engine thực hiện kiểm tra, thống kê trên các event thỏa mãn Filter. Đầu vào của Indicator là các event thỏa mãn Filter, đầu ra là các Indicator Event hoặc Alert Event. Indicator hỗ trợ các phép thống kê số lượng (count) trong một đơn vị thời gian (time-windows) của cùng một đối tượng, không Alert lặp lại đối với cùng một đối tượng trong khoảng thời gian quy định trước. Mỗi rule indicator chỉ thực hiện xét các điều kiện cùng loại, trên cùng một hệ thống;
- FalsePositive engine là một Stateless Engine thực hiện loại bỏ các trường hợp Alert bị Alert sai. Mỗi Alert khi khớp với rule Falsepositive sẽ bị drop;

+ Debug/ Not Debug là hai trạng thái của engine. Khi thực hiện thao tác debug, log được đẩy về thoả mãn điều kiện của engine sẽ hiển thị trên màn hình Gỡ rối Correlation;

+ Điều kiện: Mỗi engine sẽ hỗ trợ các điều kiện về Event, not Event, Alert Event, not Alert Event, Accumulate, Function, not Function khác nhau . Chi tiết về các điều kiện và cách sử dụng:

- Event: Được sử dụng cho các trường event;
- Not Event: Chỉ được tạo ra khi có event;
- Alert: Được sử dụng cho các trường Alert;
- Not Alert: Xét xem không có Alert event trong bao lâu;
- Accumulate: Thực hiện gom nhóm điều kiện event thoả mãn số lượng từ đó sinh ra Alert;
- Function: Là các hàm. Lưu ý: Vớicác hàm boolean, giá trị trả về là true hoặc false;
- Not Function: Với not function, các hàm được sử dụng giống với function. Tuy nhiên giá trị trả về sẽ có kết quả true/false ngược lại.

+ Toán tử :

- Các toán tử cơ bản gồm: =, !=, >, <, >=, <= .
- In: Kiểm tra giá trị của một trường có nằm trong danh sách không.

- Bên trái toán tử: Tên trường cần kiểm tra.
- Bên phải toán tử: Danh sách giá trị để kiểm tra được phân cách bởi dấu “,”.

- Contains: kiểm tra giá trị của một trường có chứa giá trị mà cần kiểm tra.
  - Bên trái toán tử: Tên trường cần kiểm tra (trường này cần có giá trị là mảng hoặc string);
  - Bên phải toán tử: Giá trị để kiểm tra.
- Assign: để gán giá trị của một trường vào một biến.
  - Bên trái toán tử: Tên trường cần gán;
  - Bên phải toán tử: Tên biến cần gán.
- Matches: kiểm tra giá trị của một trường có thoả mãn một chuỗi regex.
  - Bên trái toán tử: Tên trường cần kiểm tra;
  - Bên phải toán tử: Chuỗi regex.
- Cấu hình thời gian: Kiểm tra điều kiện trong một khoảng thời gian , chỉ có ở các engine Agg_trigger ,Agg_action và Indicator.
- Count: Kiểm tra số event đếm được trong một khoảng thời gian có thoả mãn điều kiện không.

+ Nhóm/ Bỏ nhóm : Cho phép người dùng gộp hoặc tách nhanh các điều kiện trong một toán tử AND hoặc OR. Các bước thực hiện gộp nhóm/ tách nhóm:

- Gộp nhóm

Bước 1: Click vào vào trường cần gộp nhóm;

Bước 2: Chọn NHÓM Màn hình chi tiết các bước thực hiện gộp nhóm;

- Tách nhóm:

Bước 1: Click vào các item cần tách nhóm;

Bước 2: Chọn BỎ NHÓM Màn hình chi tiết các bước thực hiện tách nhóm

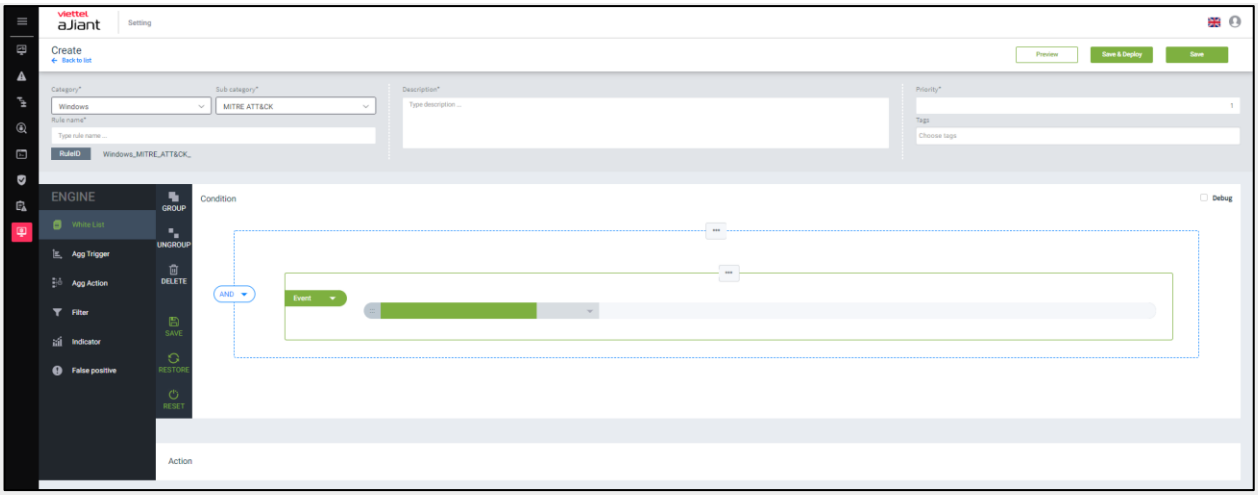
+ **Restore:** Tự động reset lại đến ngay sau khi nhấn “Save” gần nhất;

+ **Reset:** Thực hiện reset condition (về trạng thái ban đầu);

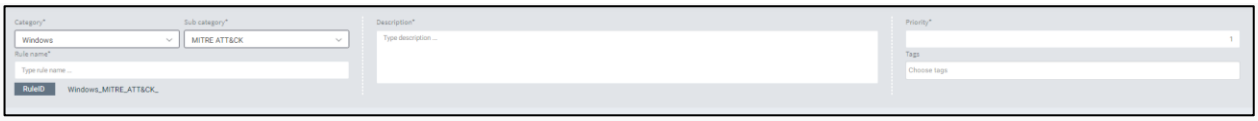
+ **Delete:** Xóa Condition đang được focus;

Các bước thêm mới rule correlation:

Bước 1: Tại màn hình Correlation, Chọn nút "Create" > Hệ thống hiển thị màn hình tạo mới rule;

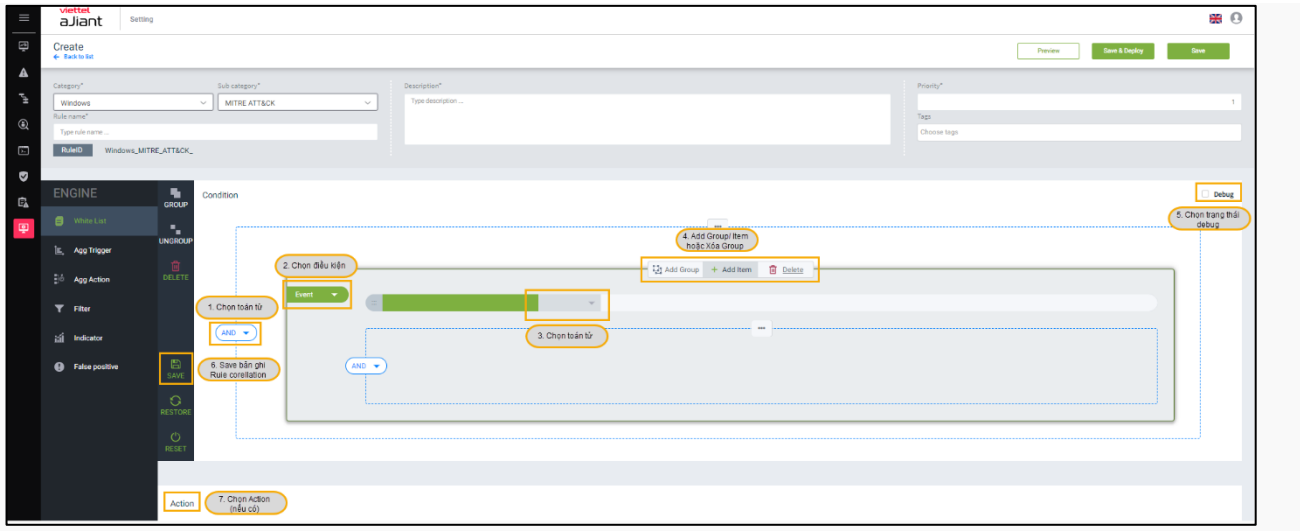


Bước 2: Nhập thông tin của rule;



Lưu ý: Các trường có dấu (*) là các trường bắt buộc nhập.

Bước 3: Chọn Engine, nhập điều kiện cho các Event, not Event, Alert, not Alert, Accumulate, Function tương ứng;



Bước 4: Nhấn "Save" để lưu lại điều kiện hoặc nhấn "Restore" để trở lại ngay sau bước mới lưu;

Bước 5: Tại Hành động , chọn hành động cần thực hiện đối với engine đó.

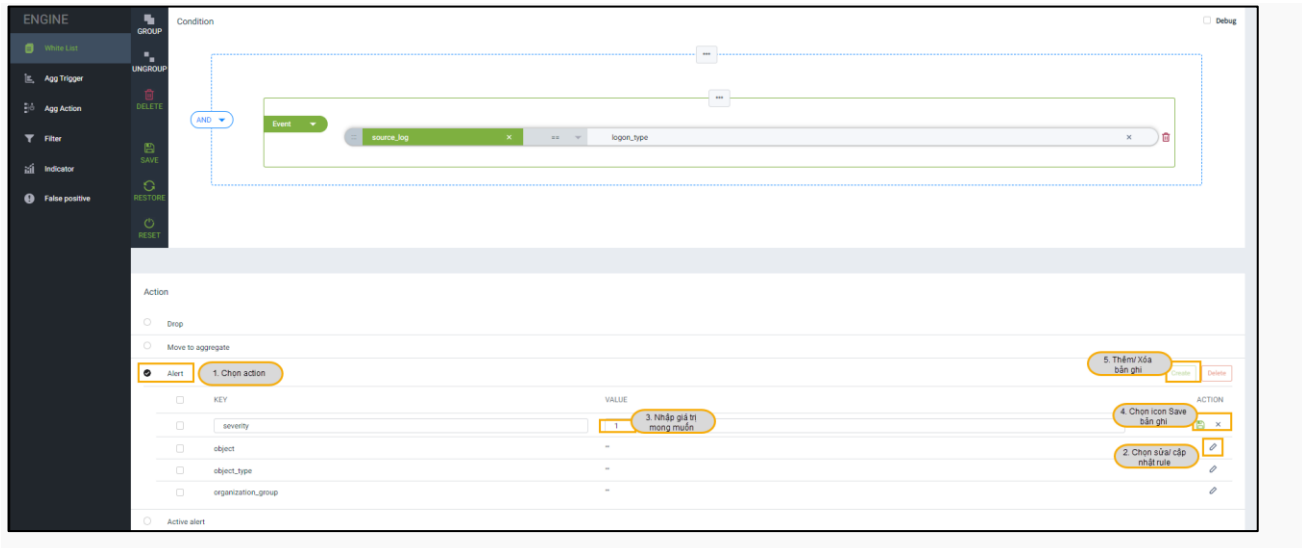
Các bước thực hiện thêm hành động tương ứng với từng engine: Khi người dùng thực hiện xong các bước tạo điều kiện và nhấn lưu, màn hình sẽ hiển thị các hành động cho từng engine. Mỗi engine sẽ bao gồm các hành động tương ứng. Engine Agg_trigger sẽ không có hành động.

Whitelist: Gồm 4 hành động dưới dạng check box : Drop, Chuyển sang aggregate, Alert và Danh sách Active, người dùng bắt buộc phải chọn 1 trong 4 hành động này. Khi các log đẩy vào thoả mãn điều kiện sẽ thực hiện 1 trong 4 hành động mà người dùng đã tích chọn. Chi tiết chức năng của 4 hành động:

- Drop: Các log được đẩy vào thoả mãn điều kiện sẽ được loại bỏ khỏi luồng xử lý;
- Chuyển sang aggregate: Log đẩy vào thoả mãn điều kiện sẽ được chuyển sang engine aggregate để tiếp tục xử lý;
- Alert: Khi thêm các trường key và value cho Alert, các log đẩy vào thoả mãn điều kiện sẽ hiển thị Alert tại màn hình quản lý Alert;
- Danh sách Active: Các value của active list sẽ được thêm vào danh sách hiển thị trên màn hình Active List;

Các bước thêm trường cho hành động Alert/ Danh sách active:

- Bước 5.1: Click chọn hành động muốn them;
- Bước 5.2: Click nút “edit” để nhập giá trị cho trường;
- Bước 5.3: Nhập giá trị cho trường;
- Bước 5.4: Click nút “Save”;
- Bước 5.5: Click nút “Add” để thêm mới một trường vào Alert.



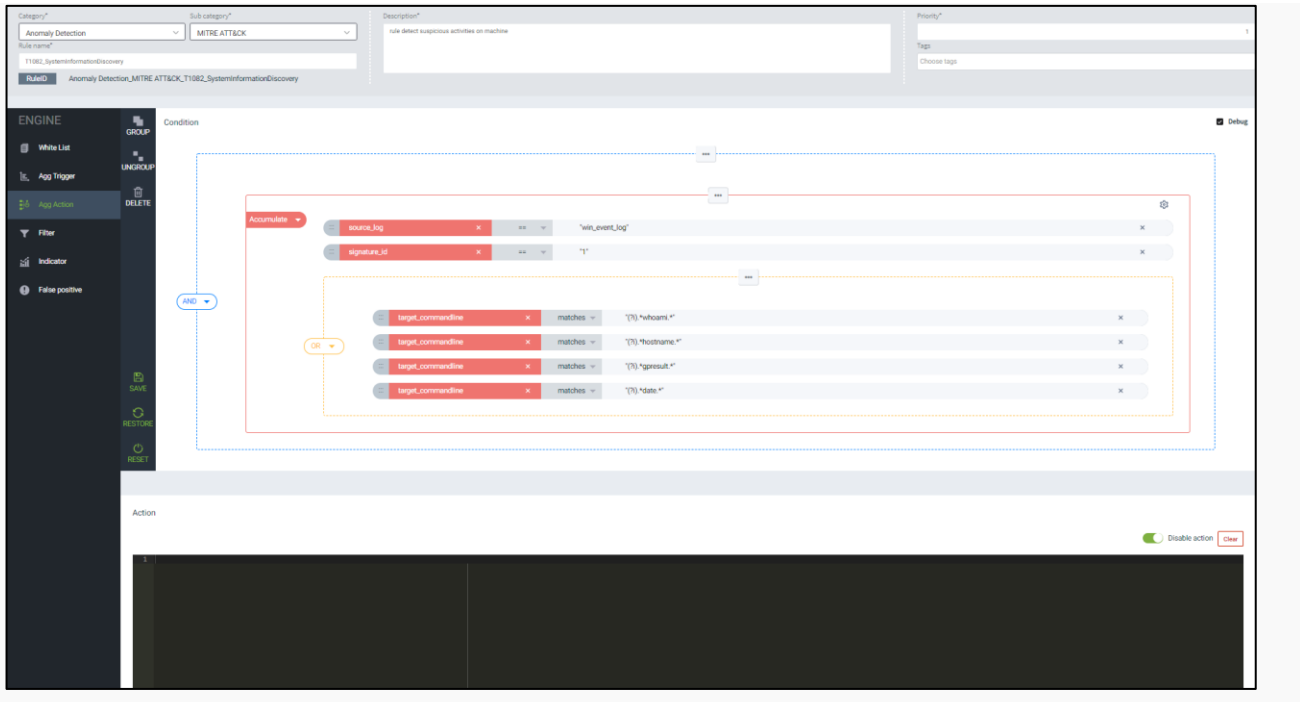
+ Để xoá hành động vừa tạo, click icon “Delete”;
+ Để chỉnh sửa hành động, Click icon “edit”;

Lưu ý: Có thể tạo nhiều hành động với các trường khác nhau tuỳ theo mục đích người sử dụng.

Agg_action: Tại engine này, người dùng có thể thực hiện hành động thêm code.

Các bước thêm trường cho hành động thêm code

- Bước 5.1: Nhập đầy đủ điều kiện và toán tử. Click vào “Save”;
- Bước 5.2: Tại mục Action, click vào icon “Enable action”;
- Bước 5.3: Nhập nội dung của code;
- Bước 5.4: Chọn nút “clear” => Nội dung nhập của code sẽ bị xóa toàn bộ;



Filter : Gồm 3 hành động: Alert, Enrichment và Danh sách Active. Người dùng có thể 1 hoặc nhiều hành động trong cùng engine. Chi tiết chức năng của 3 hành động:

- Enrichment: Thêm trường vào Alert;
- Alert và Danh sách Active (như engine Whitelist).

Các thao tác thêm mới, sửa, xoá cho các hành động của engine filter tương tự với khi thêm mới các trường cho engine whitelist.

Indicator : Hành động Alert. Các thao tác thêm mới, sửa, xoá cho các hành động của engine Indicator tương tự với khi thêm mới các trường cho engine whitelist .

FalsePositive: Hành động Enrichment. Các thao tác thêm mới, sửa xoá cho các hành động của engine FalsePositive tương tự với khi thêm mới các trường cho engine whitelist .

Bước 6: Nhấn "Save" để lưu rule vào hệ thống. Khi người dùng muốn lưu lại vào hệ thống , đồng thời deploy xuống correl enginee thì nhấn "Save & Deploy".

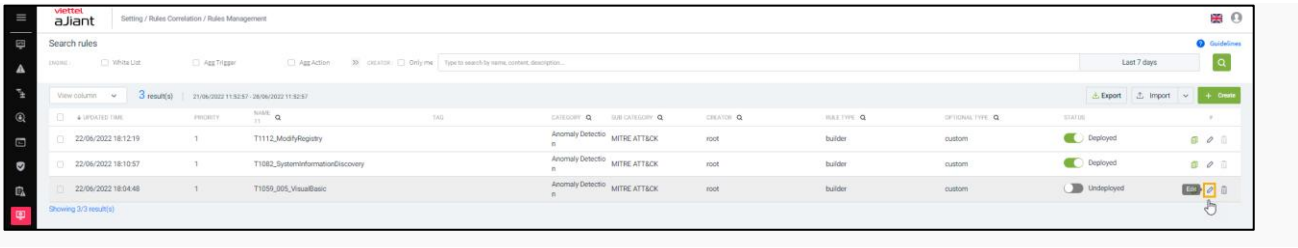
Lưu ý: Khi có lỗi, người dùng có thể nhấn nút "Preview" để xem lỗi.

3.9.3 Sửa Rules Correlation

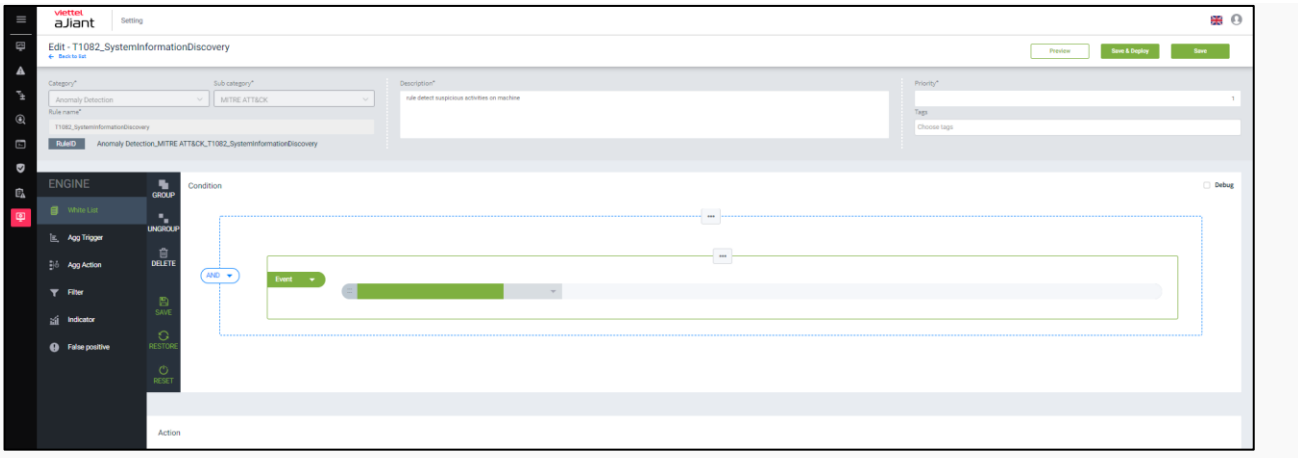
Cho phép người dùng chỉnh sửa các rule đã tạo.

Các bước thực hiện:

Bước 1: Tại màn hình quản lý rule, click icon Chỉnh sửa của rule muốn chỉnh sửa;



Bước 2: Tại màn hình chỉnh sửa , nhập thông tin cần chỉnh sửa;



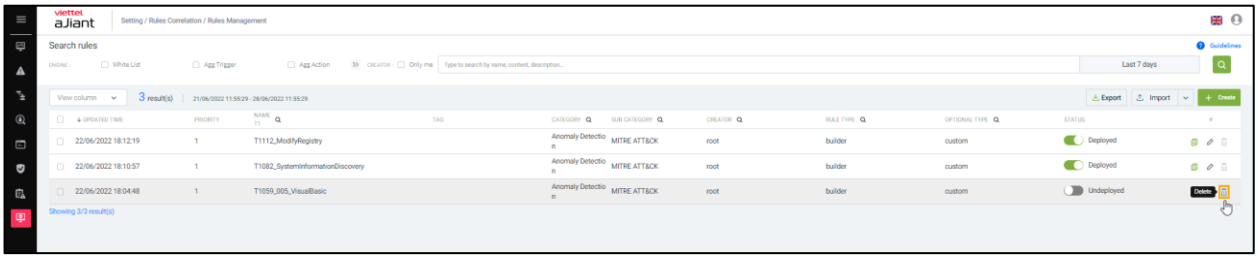
Lưu ý: Các trường tên rule, category, subcategory là những trường không chỉnh sửa được.

Bước 3: Nhấn nút "Save" để lưu rule lại vào hệ thống. Khi người dùng muốn lưu lại vào hệ thống , đồng thời deploy xuống correlation engine thì nhấn "Save & Deploy".

Với những rule chỉnh sửa nhưng chỉ Lưu, người dùng phải click Redeploy tại màn hình quản lý rule thì rule mới có tác dụng đối với hệ thống.

Lưu ý: Khi có lỗi, người dùng có thể nhấn Preview để xem lỗi

3.9.4 Xóa Rules Correlation

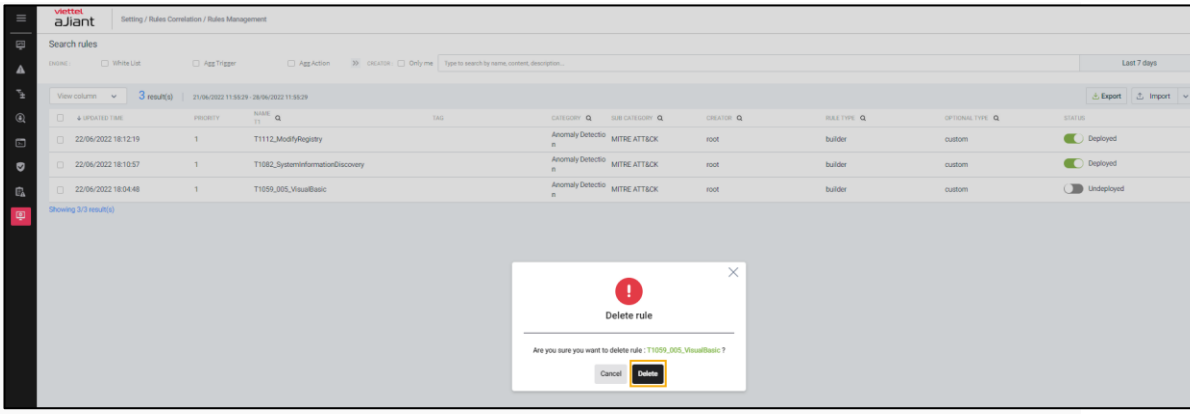


Các bước thực hiện xóa 01 rule:

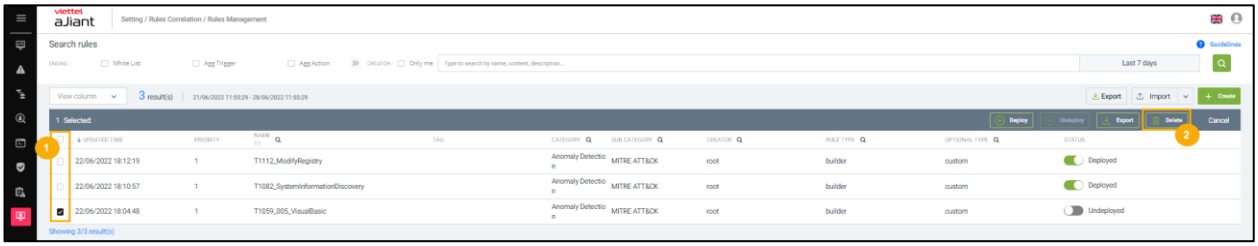
Bước 1: Click icon “Xoá” tại rule muốn xoá;

Bước 2: Màn hình hiển thị thông báo xác nhận xoá , chọn “Cancel” hoặc “Delete”;

Bước 3:



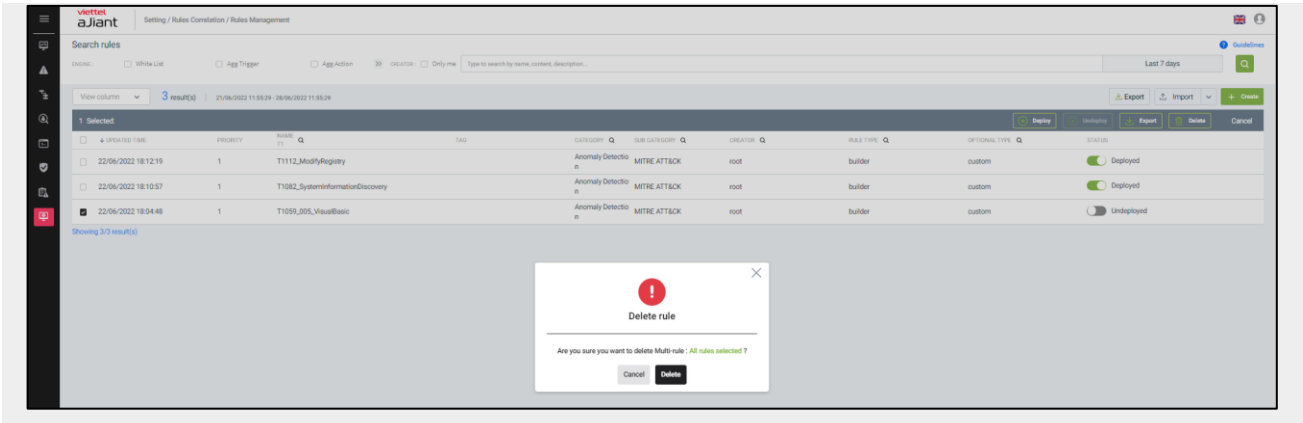
+ Nếu chọn “Delete”, rule được chọn xoá sẽ biến mất khỏi màn hình hiển thị;



Các bước thực hiện xóa nhiều rule:

Bước 1: Click chọn những rule muốn xoá (Có thể xoá tất cả bằng cách Click Chọn tất cả rule);

Bước 2: Màn hình hiển thị thông báo xác nhận xoá, chọn “Cancel” hoặc “Delete”;



Bước 3: Chọn "Delete", tất cả rule sẽ được xoá khỏi màn hình hiển thị. Chọn "Cancel", thao tác vừa chọn sẽ được huỷ bỏ.

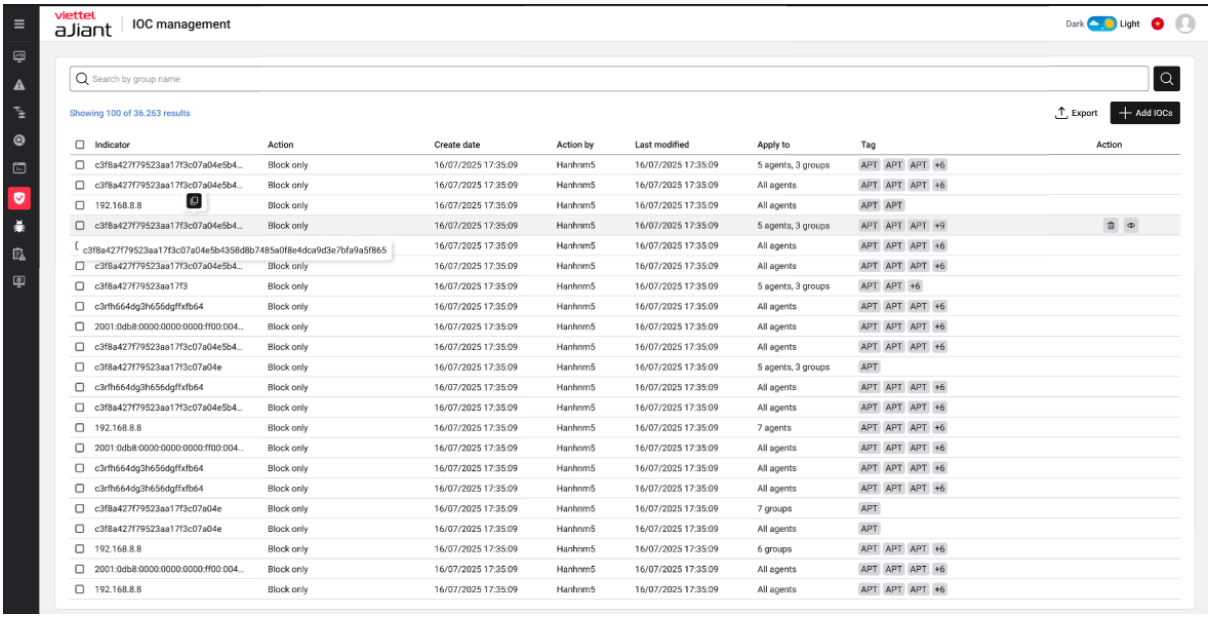
3.10 Protect & Prevention

3.10.1 IOC Management

Mục đích: Chức năng Quản lý IOC đóng vai trò là "lá chắn chủ động" giúp quản trị viên kiểm soát và bảo vệ hệ thống thông qua ba mục tiêu chính:

- **Kiểm soát Thực thi Ứng dụng**: Ngăn chặn triệt để việc khởi chạy các phần mềm lạ, ứng dụng không an toàn hoặc nằm trong danh sách đen ngay tại máy trạm của người dùng.
- **Giám sát và Chặn kết nối Độc hại**: Theo dõi các luồng truy cập Internet, tự động phát hiện và ngắt kết nối tới các địa chỉ (IP/Domain) nghi ngờ để ngăn chặn hành vi xâm nhập trái phép hoặc đánh cắp dữ liệu.
- **Phòng ngừa Mã độc Chủ động**: Bảo vệ an toàn cho dữ liệu và các ứng dụng trọng yếu bằng cách nhận diện sớm các dấu hiệu tấn công (IOC), từ đó cô lập mối đe dọa trước khi mã độc có thể gây hại cho hệ thống.

3.10.1.1 Xem danh sách rule block

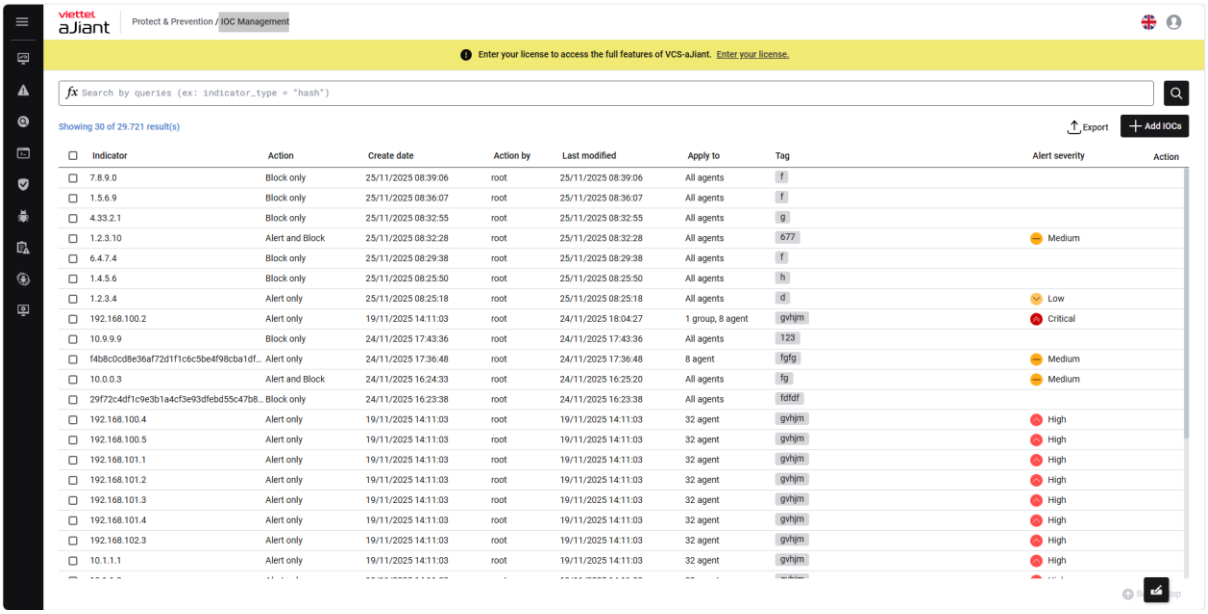


Bước 1 : Khách hàng đăng nhập vào hệ thống bằng tài khoản có quyền iocmanagement_manage và iocmanagement_read

Bước 2: Tại menu -> Click vào tab Protect&Prevent -> Click vào tab IOC Management

Màn hình bảng dữ liệu hiển thị các thông tin bao gồm:

- Indicator : Tên của hash/ IP
- Action: Hiển thị hành động đối với Hash/ IP bao gồm : Block only
- Create date: Thời gian tạo rule
- Action by: User thực hiện hành động cuối cùng đối với hash/IP
- Last modified: Thời gian sửa đổi rule gần nhất
- Apply to: Hiển thị agent được gán với rule
- Tag: Hiển thị Tag gán với Hash/ IP đó
- Action: Hiển thị icon Delete và icon View

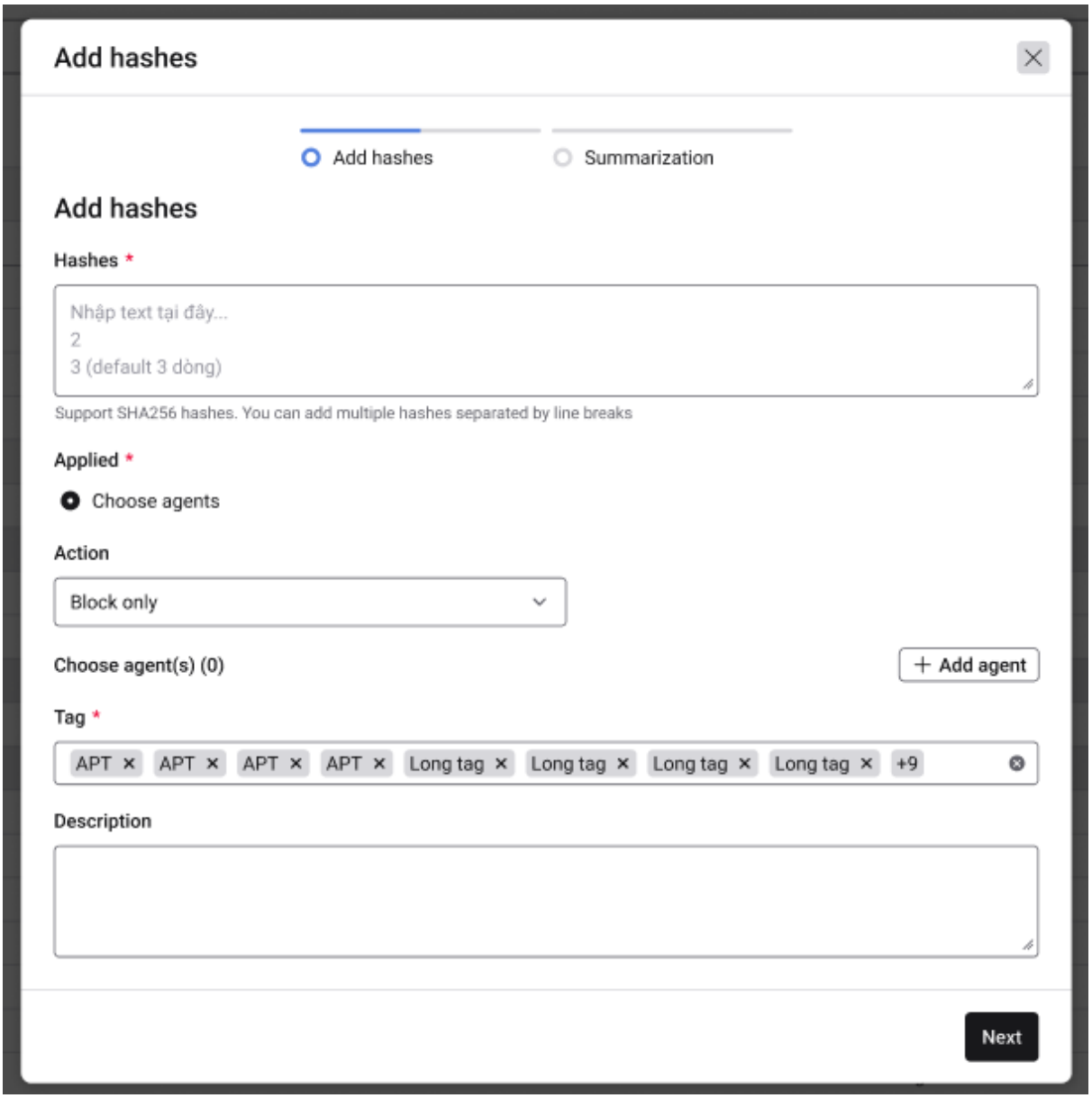


3.10.1.2 Thêm mới hashes/IP

1. *Thêm mới hashes*

Bước 1: Khách hàng đăng nhập vào hệ thống bằng tài khoản có quyền iocmanagement_manage và iocmanagement_read

Bước 2: Tại màn hình màn hình IOC Management -> Click button [Add IOCs] -> Click [Add hashes] để mở popup Add hashes

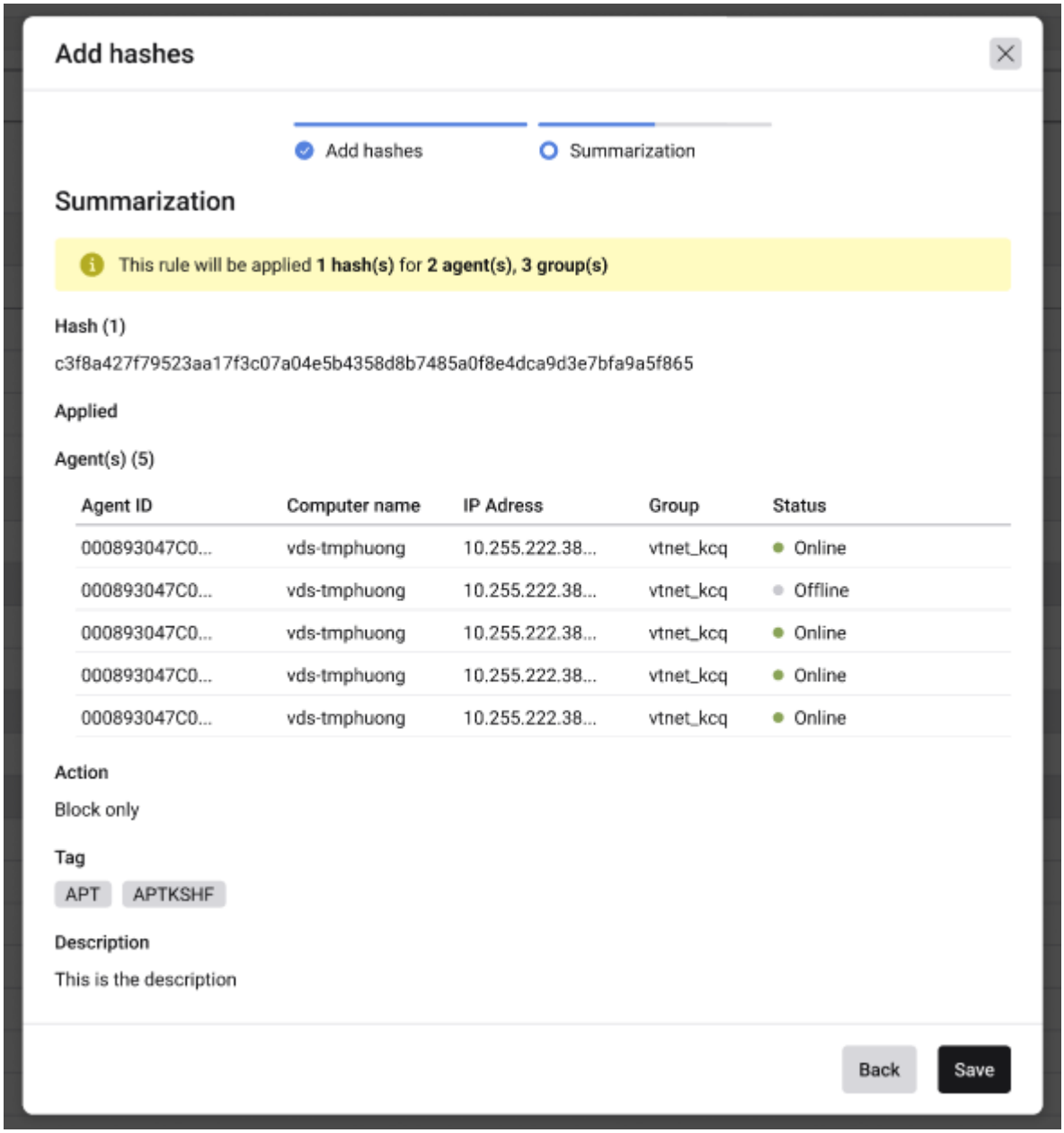


Bước 3: Nhập đầy đủ các trường thông tin bắt buộc

- Trường "Hashes" (bắt buộc) : nhập 1 hoặc nhiều mã sha256, phân tách nhau bằng dấu xuống dòng (tối đa 50 mã)
- Trường " Applied" (bắt buộc) : Mặc định chọn Choose agents
- Trường "Action" (bắt buộc) : Mặc định chọn Block only
- Trường "Tags" (bắt buộc) : Nhập các ký tự -> Ấn Enter để hoàn thành nhập tag

- Trường "Description" (bắt buộc): Nhập tối đa 255 ký tự

Bước 4: Click button [Next] để chuyển sang tab "Summarization"



Bước 5: Click button [Apply] tại tab "Summarization"

Bước 6:

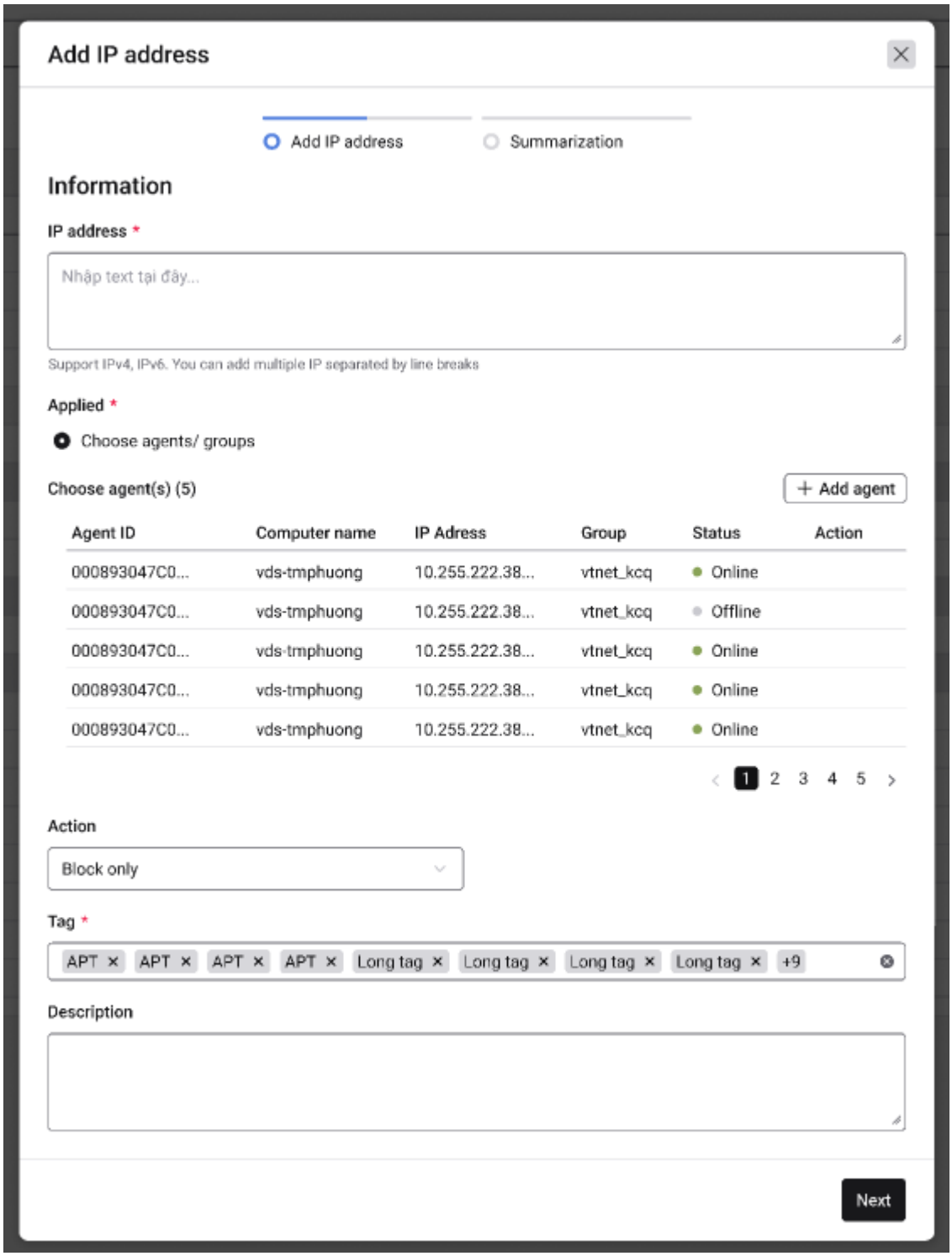
- Hiển thị message thông báo "Add IOC successfully"

- Tạo mới hash thành công
- Màn hình được back về màn danh sách IOC
- Hash mới tạo được hiển thị trên cùng tại màn danh sách

2. Thêm mới IP

Bước 1: Khách hàng đăng nhập vào hệ thống bằng tài khoản có quyền iocmanagement_manage và iocmanagement_read

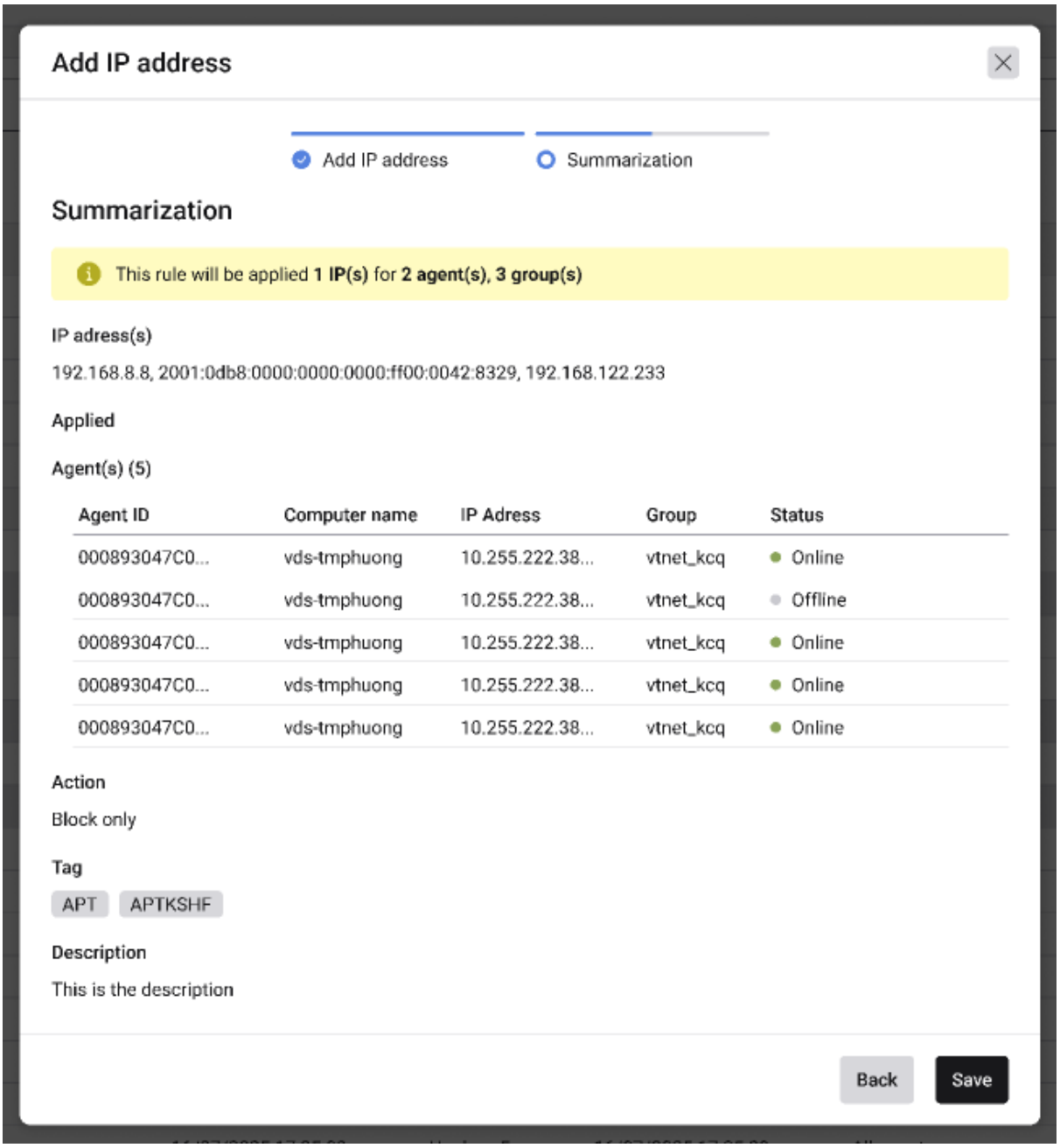
Bước 2: Tại màn hình màn hình IOC Management -> Click button [Add IOCs] -> Click [Add IP] để mở popup Add IP



Bước 3: Nhập đầy đủ các trường thông tin bắt buộc

- Trường "IP" (bắt buộc) : nhập 1 hoặc nhiều IPV4 / IPV6, phân tách nhau bằng dấu xuống dòng (tối đa 50 mã)
- Trường " Applied" (bắt buộc) : Mặc định chọn Choose agents
- Trường "Action" (bắt buộc) : Mặc định chọn Block only
- Trường "Tags" (bắt buộc) : Nhập các ký tự -> Ấn Enter để hoàn thành nhập tag
- Trường "Description" (bắt buộc): Nhập tối đa 255 ký tự

Bước 4: Click button [Next] để chuyển sang tab "Summarization"



Bước 5: Click button [Apply] tại tab "Summarization"

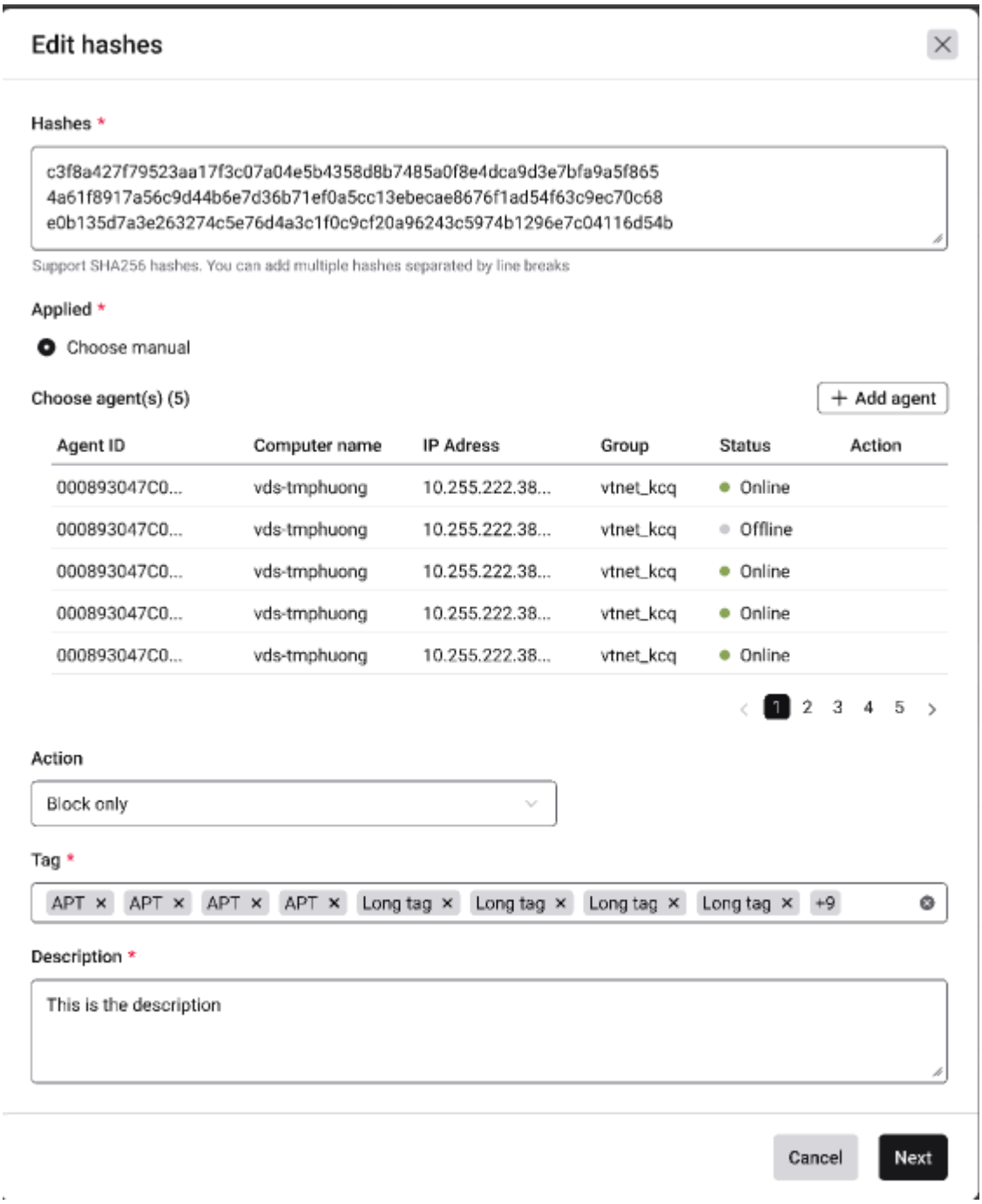
Bước 6:

- Hiển thị message thông báo "Add IOC successfully"
- Tạo mới IP thành công
- Màn hình được back về màn danh sách IOC
- Hash mới tạo được hiển thị trên cùng tại màn danh sách

3.10.1.3 Cập nhật rule block

Bước 1: Khách hàng đăng nhập vào hệ thống bằng tài khoản có quyền iocmanagement_manage và iocmanagement_read

Bước 2: Tại màn hình màn hình IOC Management -> Click vào icon view của 1 bản ghi bất kì để mở popup Edit

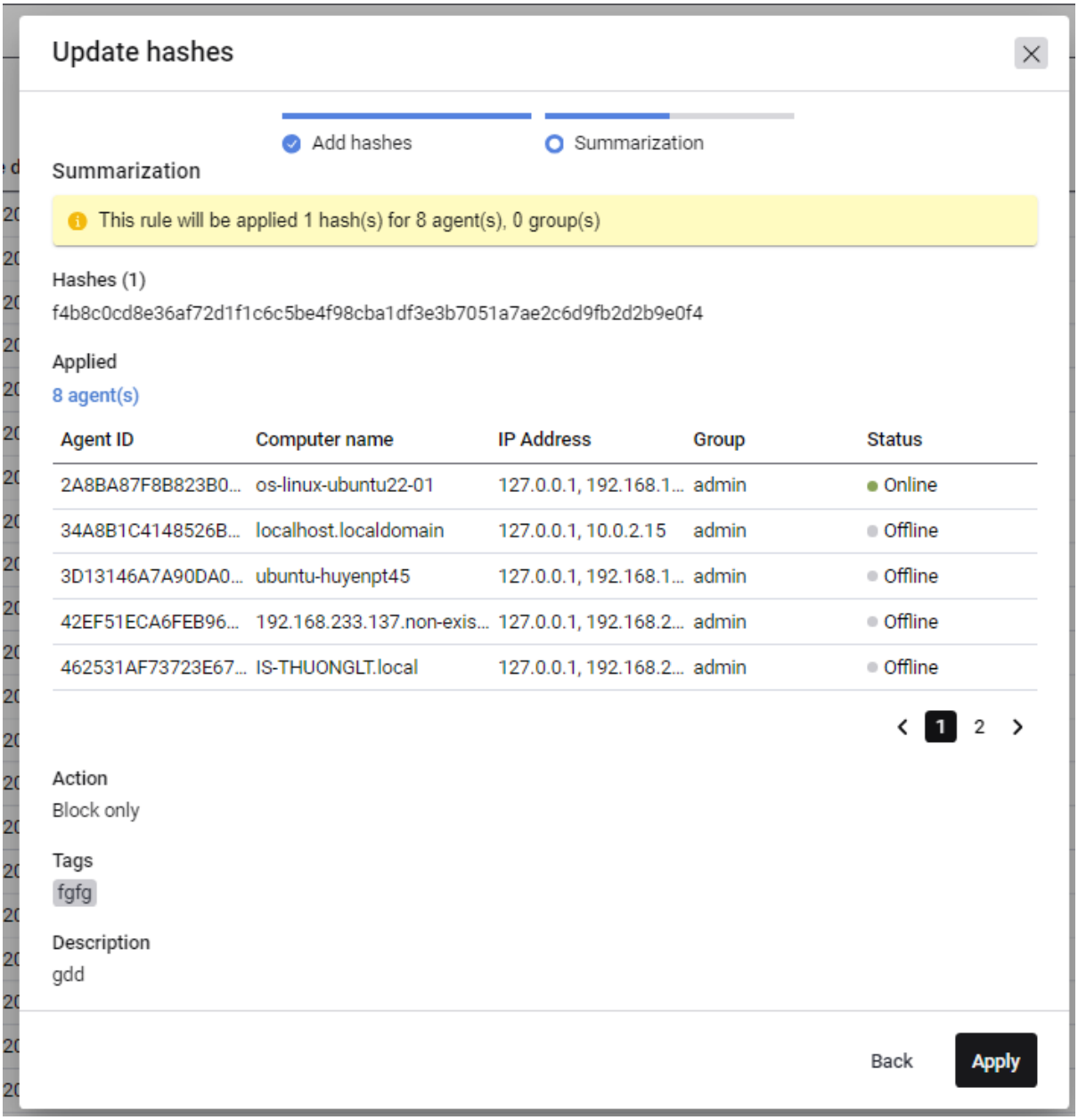


Bước 3: Thực hiện thay đổi các trường theo mong muốn:

- Trường " Applied" (bắt buộc) : Mặc định chọn Choose agents
- Trường "Action" (bắt buộc) : Mặc định chọn Block only

- Trường "Tags" (bắt buộc) : Nhập các ký tự -> Ấn Enter để hoàn thành nhập tag
- Trường "Description" (bắt buộc): Nhập tối đa 255 ký tự

Bước 4: Click button [Next] để chuyển sang tab "Summarization"



Bước 5 : Click button [Apply] tại tab "Summarization" để update hash/ IP

Bước 6:

- Hiển thị message thông báo "Update IOC successfully"

- Update rule thành công
- Màn hình được back về màn danh sách IOC
- Rule mới update được hiển thị trên cùng tại màn danh sách

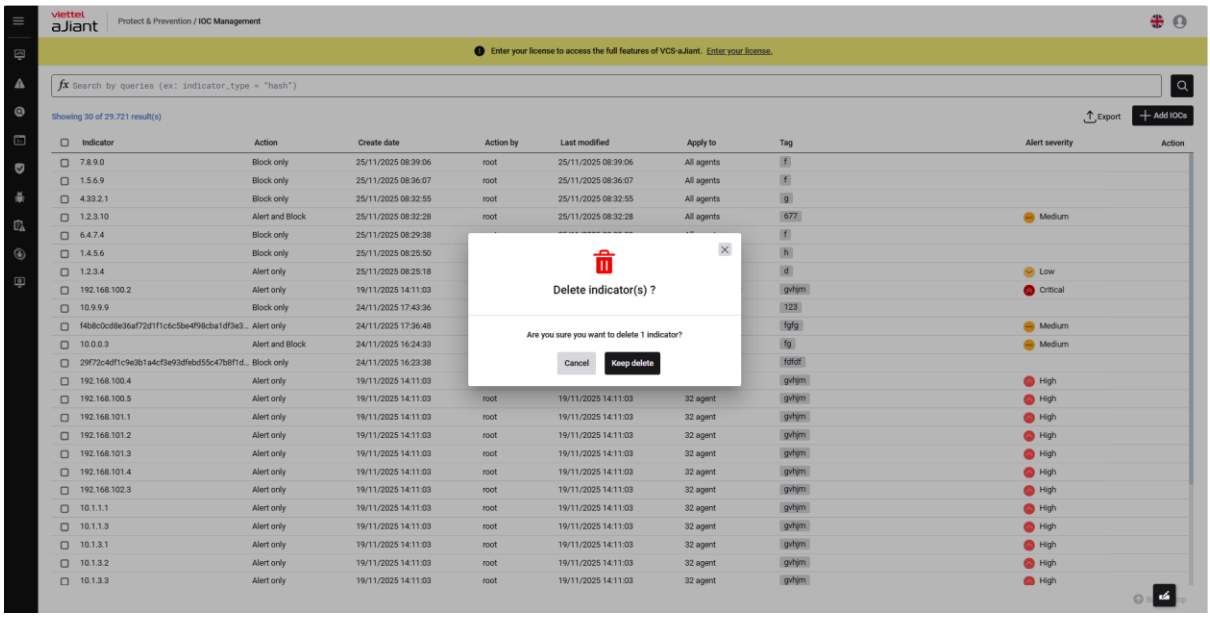
3.10.1.4 Xóa rule block

Bước 1: Khách hàng đăng nhập vào hệ thống bằng tài khoản có quyền iocmanagement_manage và iocmanagement_read

Bước 2: Tại màn hình màn hình IOC Management

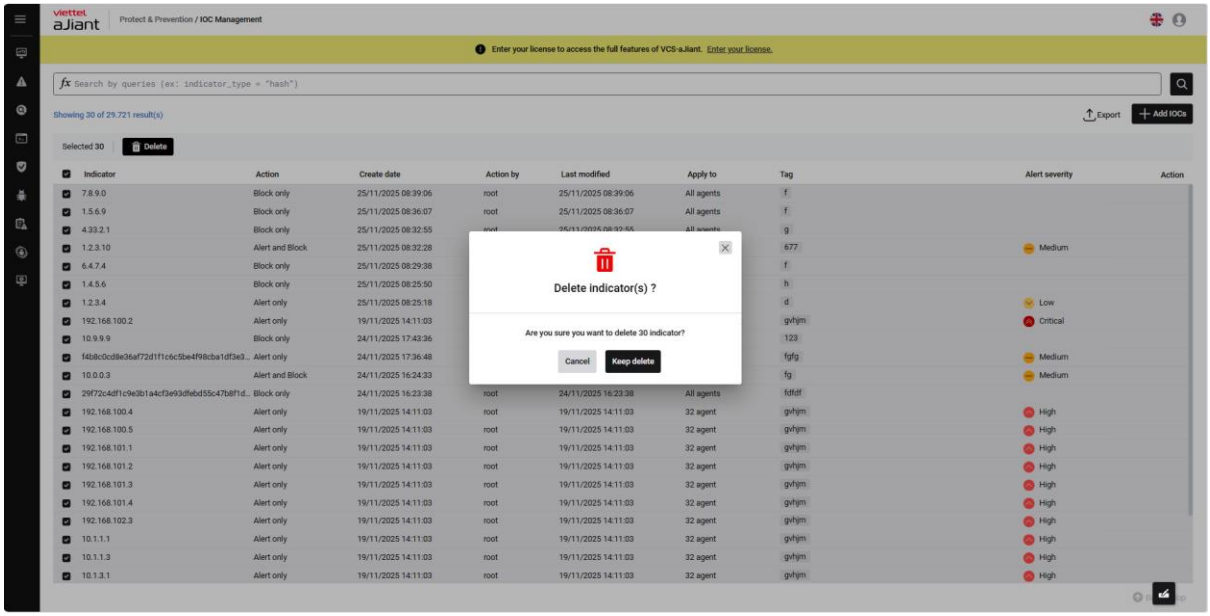
- Trường hợp xóa 1 rule

  Hover chuột vào cột Action -> Click vào icon [Delete] tại 1 rule bất kỳ muốn xóa



- Trường hợp xóa nhiều rule

  Check chọn các rule muốn xóa -> Click vào button [Keep delete]



Bước 3: Click vào button [Keep delete] để xác nhận xóa rule

Bước 4:

- Hiển thị message thông báo "Deleted successfully"
- Màn hình được back về màn danh sách IOC
- Bản ghi vừa xóa sẽ mất khỏi danh sách và database

3.10.1.5 Export rule block

Bước 1: Khách hàng đăng nhập vào hệ thống bằng tài khoản có quyền iocmanagement_manage và iocmanagement_read

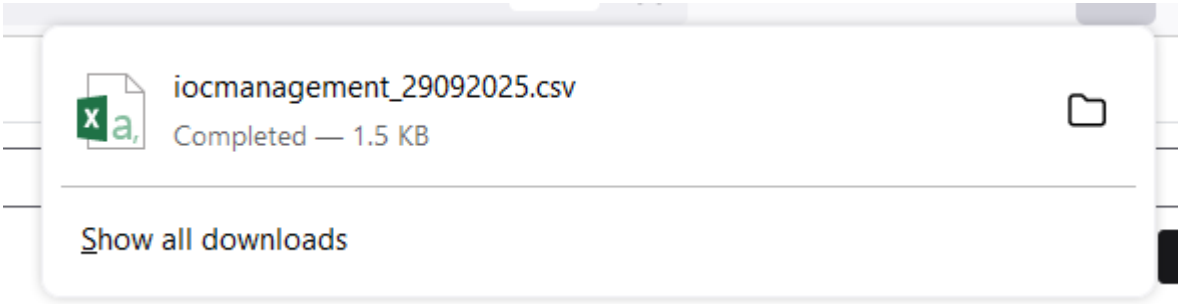
Bước 2: Tại màn hình màn hình IOC Management -> Click button [Export]

Bước 3: File export được tải về thành công trên máy

- File export đầy đủ các trường và dữ liệu tương ứng trên portal:
  - Indicator : Tên của hash/ IP
  - Action: Hiển thị hành động đối với Hash/ IP
  - Create date: Thời gian tạo rule
  - Action by: User thực hiện hành động cuối cùng đối với hash/IP
  - Last modified: Thời gian sửa đổi rule gần nhất

- Apply to: Hiển thị agent được gán với rule
- Tag: Hiển thị Tag gán với Hash/ IP đó

- File tải xuống có định dạng csv với tên file là: iocmanagement_ddmmyy (ddmmyy là thời gian tải xuống)



3.10.1.6 Tìm kiếm rule block

Bước 1: Khách hàng đăng nhập vào hệ thống bằng tài khoản có quyền iocmanagement_manage và iocmanagement_read

Bước 2: Tại màn hình màn hình IOC Management -> Click thanh tìm kiếm

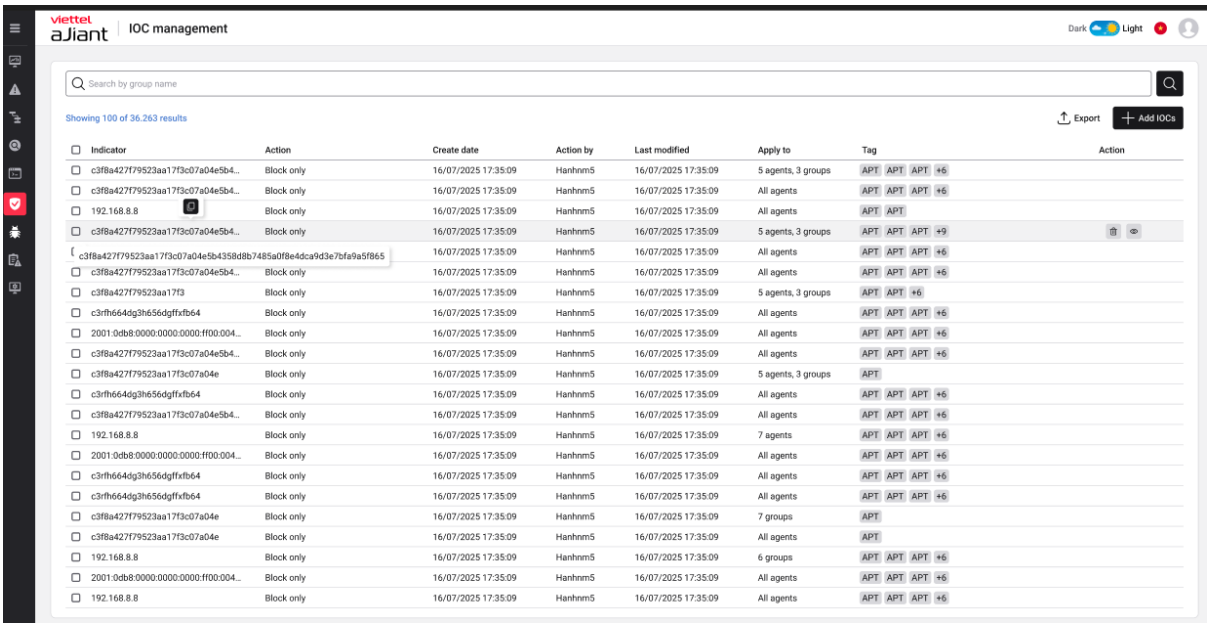
Bước 3: Thực hiện Tìm kiếm theo dạng query

VD: Tìm kiếm theo indicator

indicator = " 2.2.2.2"

Bước 3: Click button [Search] để thực hiện tìm kiếm

Bước 4: Hiển thị kết quả tìm kiếm thỏa mãn điều kiện tìm kiếm



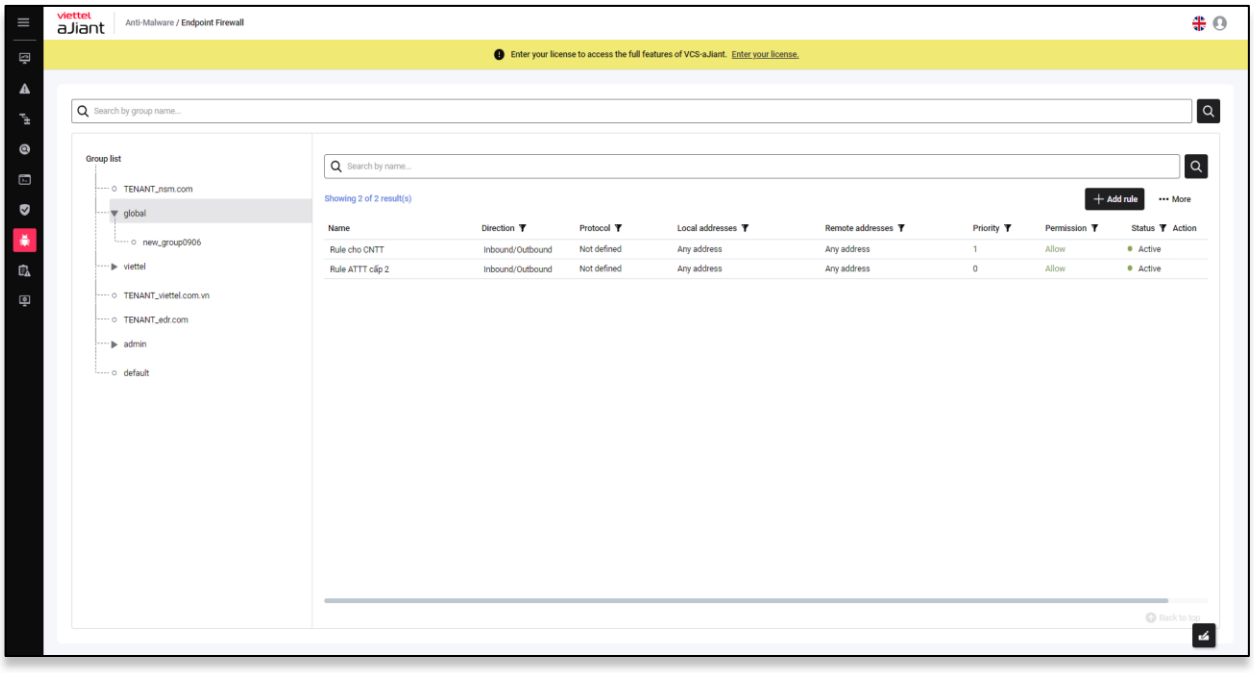
3.11 Anti – Malware

3.11.1 Endpoint Firewall

Mục đích: Chức năng Endpoint Firewall cho phép cấu hình các kết nối sẽ chặn/ cho phép dưới máy người dùng, bao gồm chặn theo ứng dụng, ip, port, hoặc cả ip và port, hỗ trợ các protocol TCP, UDP, ICMP, ICMPv6, IGMP, hỗ trợ Ipv4 và Ipv6, hỗ trợ inbound và outbound connection.

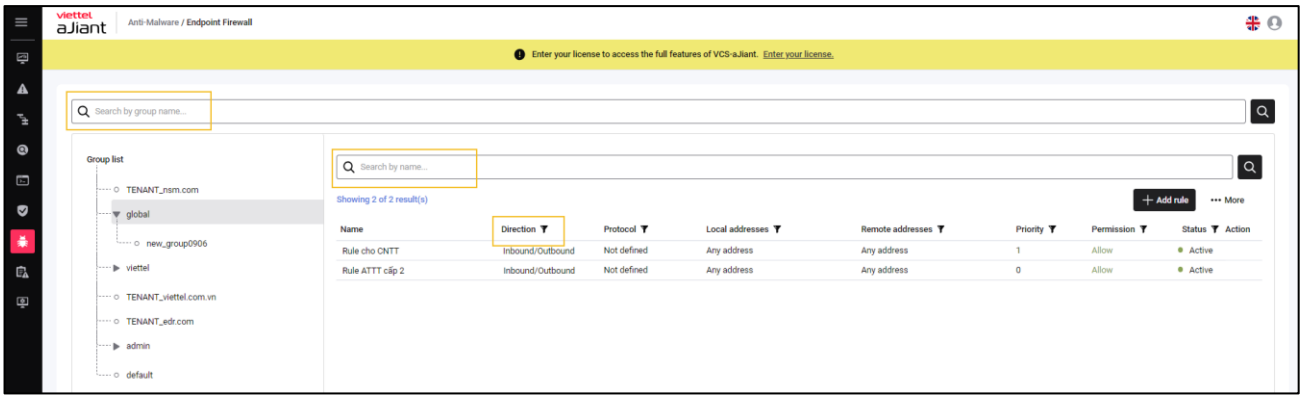
3.11.1.1 Hiển thị danh sách các kết nối bị chặn

Click vào tab Alti-Malware > chọn Endpoint Firewall sẽ hiển thị toàn bộ danh sách các kết nối bị chặn theo từng nhóm người dùng.



3.11.1.2 Tìm kiếm các kết nối bị chặn

Người dùng có thể tìm kiếm theo nhóm người dùng, theo tên quy tắc firewall hoặc filter theo giá trị của từng điều kiện (Tên, kiểu connect inbound/outbound, ip…) trên màn danh sách firewall:



3.11.1.3 Thêm mới các kết nối bị chặn

Chọn nhóm người, sau đó Click nút “Add new”, nhập thông tin trên popup thêm mới kết nối bị chặn

+ Name: tên điều kiện bạn muốn tạo;

+ Program: các chương trình cần chặn/ cho phép dưới máy người dùng. Ví dụ *"%ProgramFiles% (x86) \Tên_ứng_dụng.exe"*

+ Protocol: Not defined, ICMP, TCP, UDP, ICMPV6, IGMP

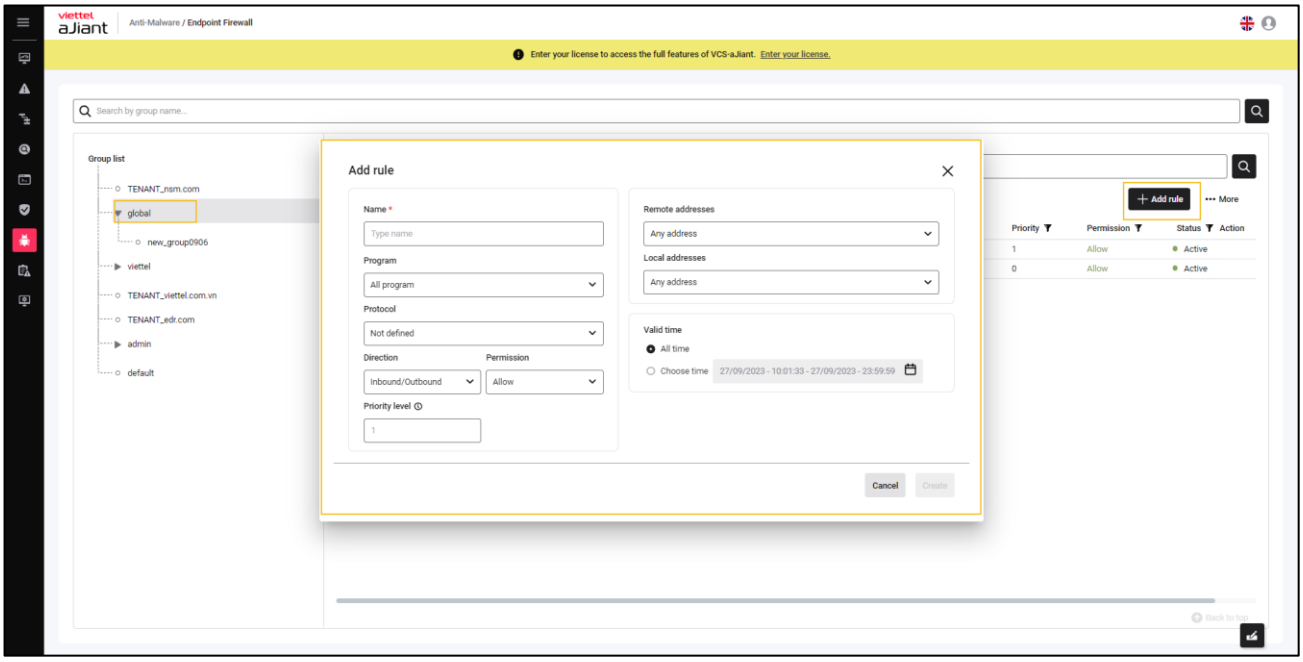
+ Port: port cần chặn, nếu chặn tất cả port thì nhập 0;

+ Direction: inbound, outbound, inbound/outbound

+ Permission: Allow (cho phép) /Block (chặn)

+ Remote address/ Local address: hỗ trợ ip v4, v6, dải IP.

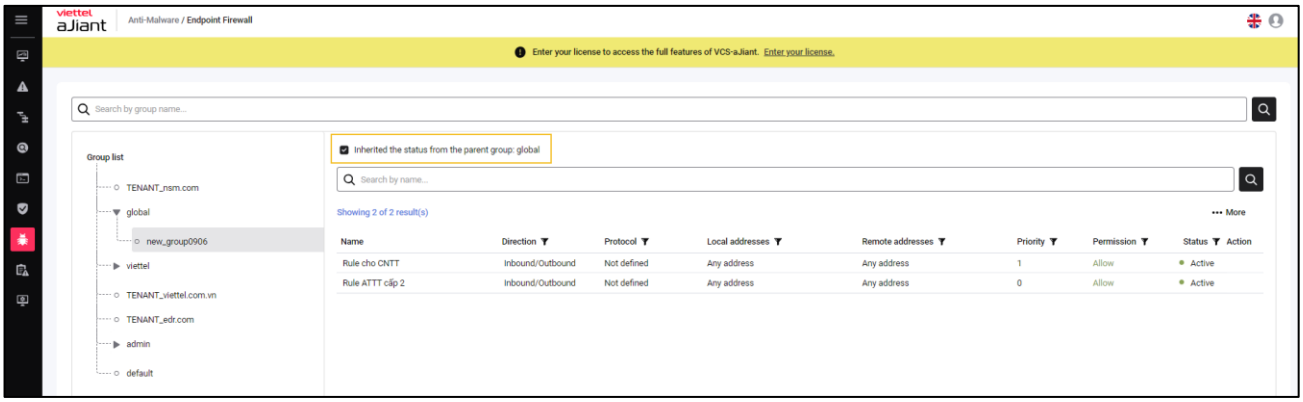
+ Valid time: thời gian điều kiện có hiệu lực



Lưu ý: quy tắc kế thừa từ nhóm cha

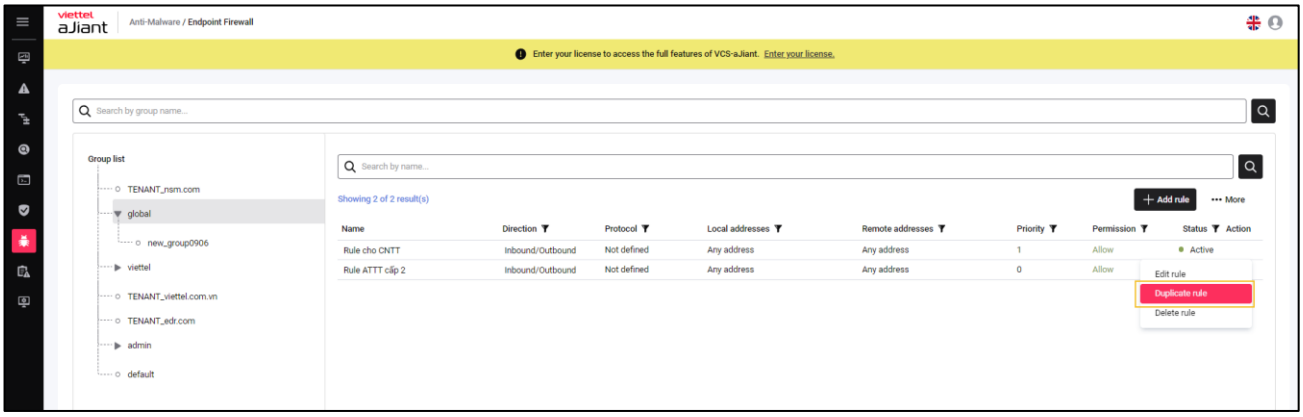
+ Nếu tích chọn *Inherit the status from the parent group* : nhóm con sẽ kế thừa toàn bộ điều kiện từ nhóm cha, và không được thêm mới hoặc sửa các điều kiện kế thừa

+ Nếu không tích chọn *Inherit the status from the parent group*: nhóm con sẽ không kế thừa từ nhóm cha, và được thêm mới, xóa các điều kiện



3.11.1.4 Tạo bản sao chép từ điều kiện đã có

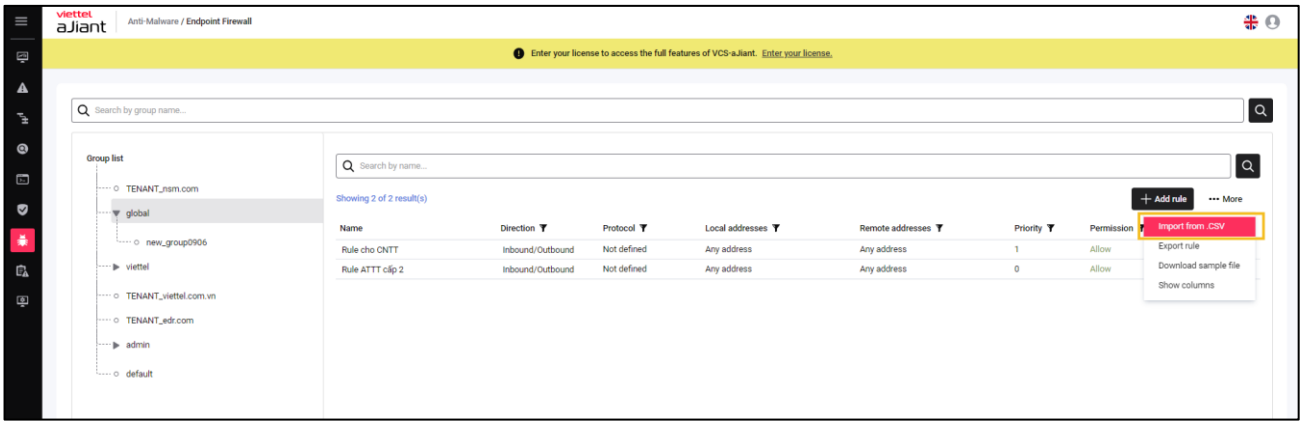
Chọn điều kiện muốn tạo bản sao chép, thực hiện Action, chọn *Duplicate rule*



3.11.1.5 Thêm mới kết nối bị chặn từ tập tin có sẵn

Người dùng có thể thêm mới các ứng dụng/tiến trình bị chặn từ tập tin .csv theo mẫu có sẵn lên danh sách ứng dụng hiện tại;

Click nút “Import from .CSV”, chọn đường dẫn đến file cần tải lên và click nút “Open”, hệ thống sẽ tự động thêm danh sách các ứng dụng cần chặn lên hệ thống;

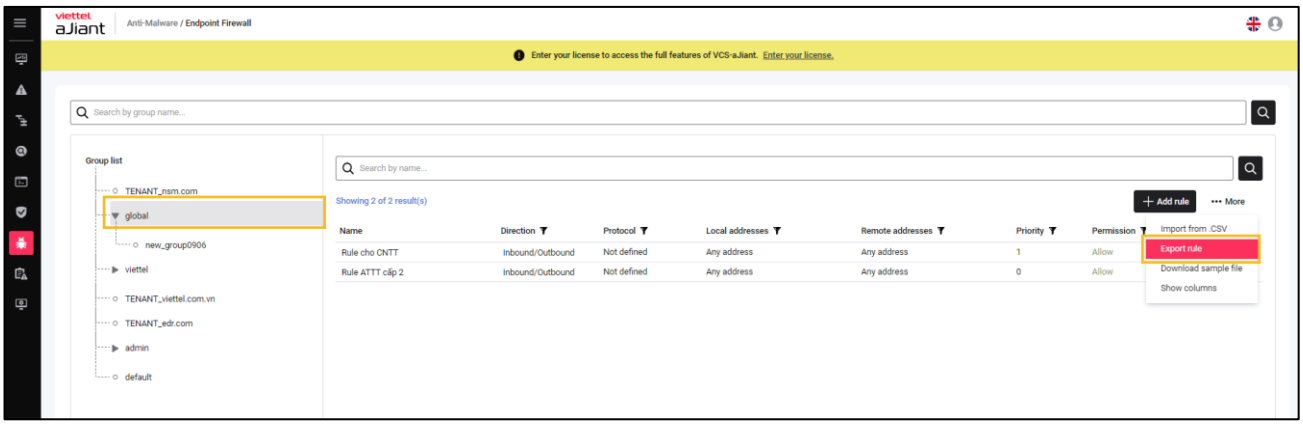


3.11.1.6 Xóa kết nối bị chặn trong danh sách

Click vào từng kết nối cần xóa và click icon “Delete”

3.11.1.7 Xuất dữ liệu các điều kiện

Chọn nhóm người dùng, chọn More, chọn Export Rule để export file csv chứa toàn bộ thông tin các điều kiện của nhóm đã chọn



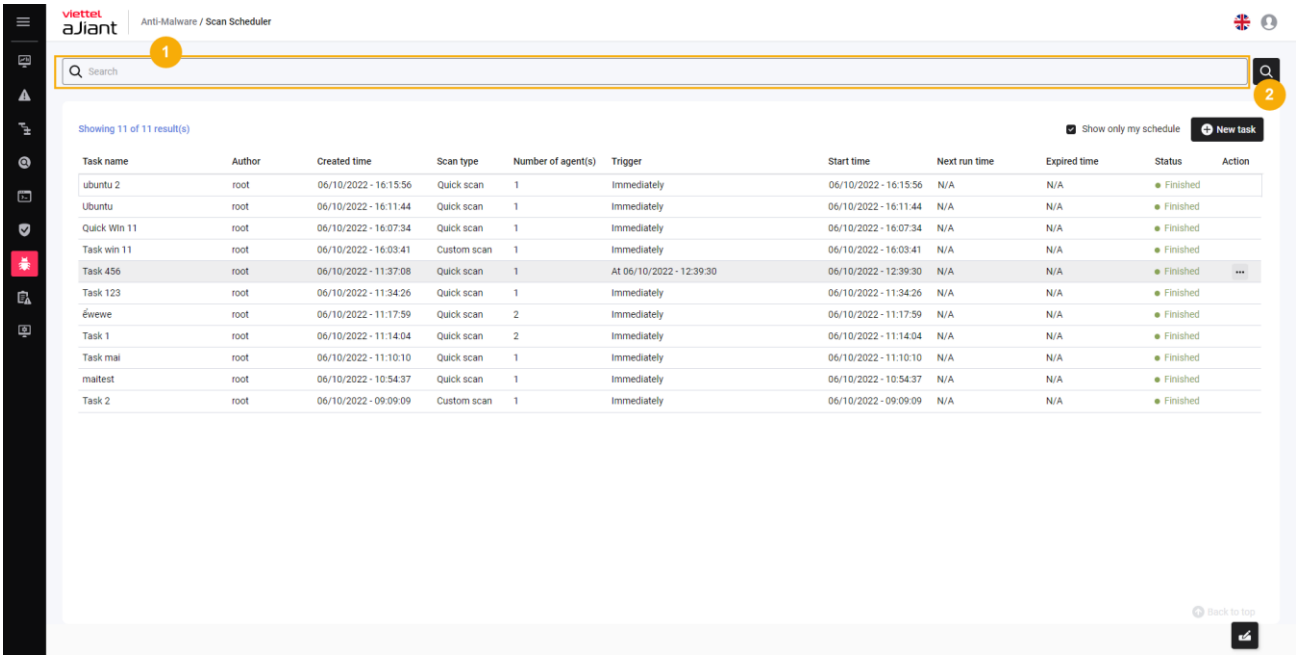
3.11.2 Scan Schedule

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

3.11.2.1 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.

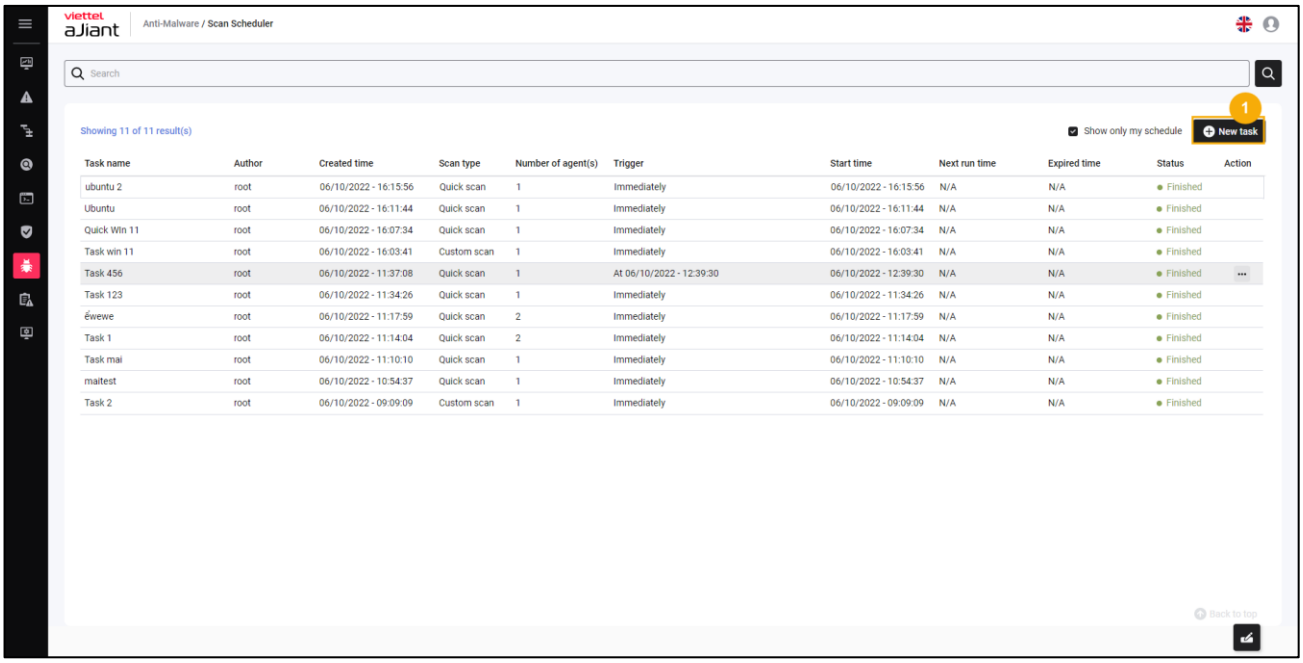
Bước 3: Hệ thống sẽ hiển thị danh sách lập lịch quét theo từ khóa tìm kiếm.

3.11.2.2 Thêm mới Scan Schedule task

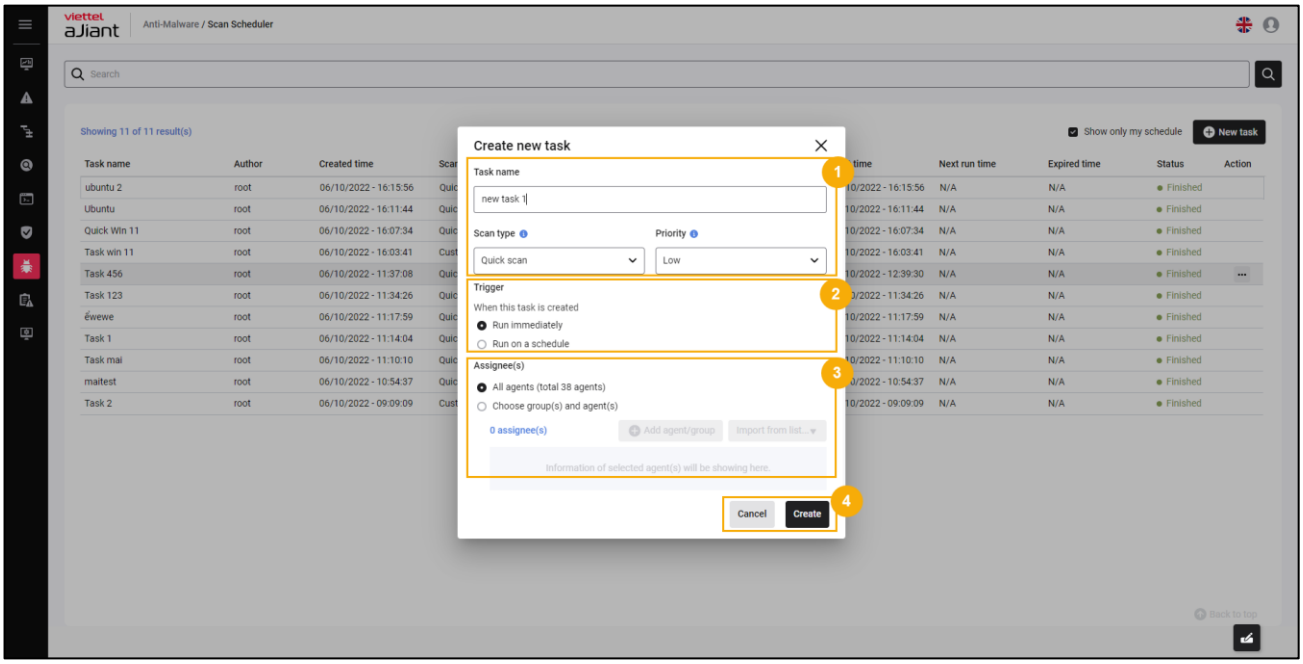
Mục đích: Cho phép người dùng thêm mới một lập lịch quét, cấu hình thời gian và thông tin máy trạm.

Các bước thực hiện:

Bước 1: Tại màn hình danh sách lập lịch quét, người dùng chọn nút **New task**



Bước 2: Hệ thống hiển thị màn hình thêm mới một lập lịch quét, người dùng nhập vào các thông tin:



1 – 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;

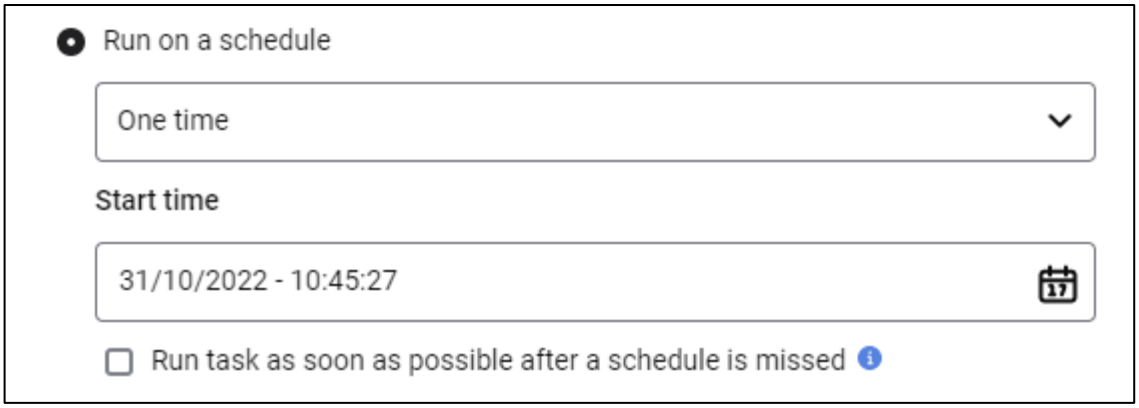
+ Quét toàn bộ: Kiểm tra toàn bộ các tệp và thư mục trong máy tính. Quá trình này có thể mất vài giờ để hoàn thành;

+ 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.

2 – 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

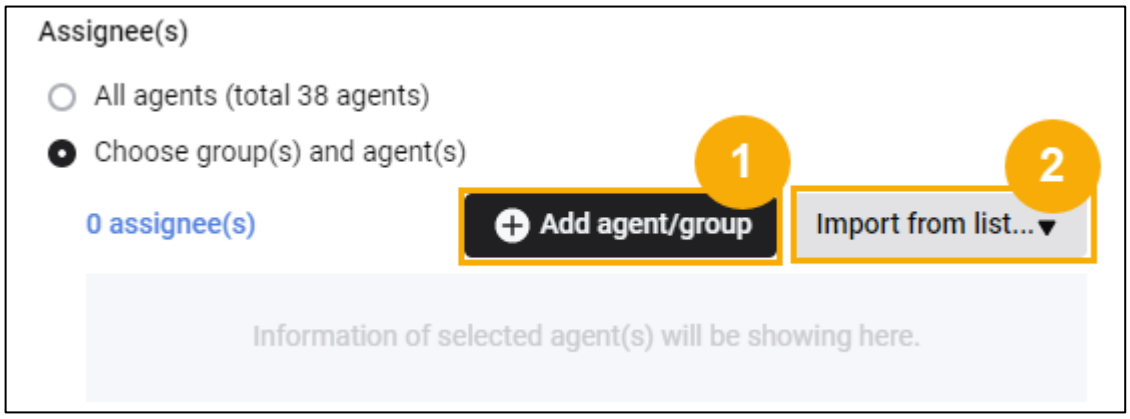
+ Ví dụ: Schedule: Daily, Start time: 15/08/2022 – 03:00:00. Được hiểu là cấu hình lập lịch quét hàng ngày lúc 03:00:00;

+ 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.

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

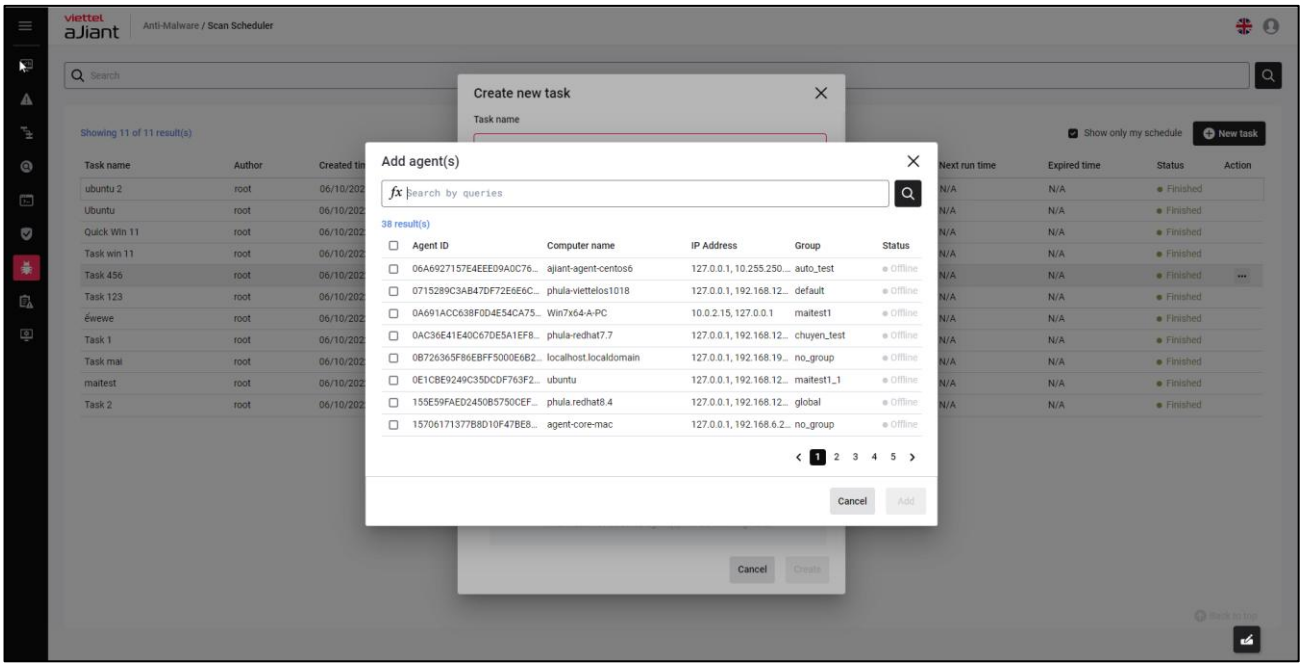
All Agent(s): Lập lịch với tất cả các máy trạm thuộc quyền quản lý của người dùng đang đăng nhập;
Choose Agent(s) or Group(s):

+ 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:



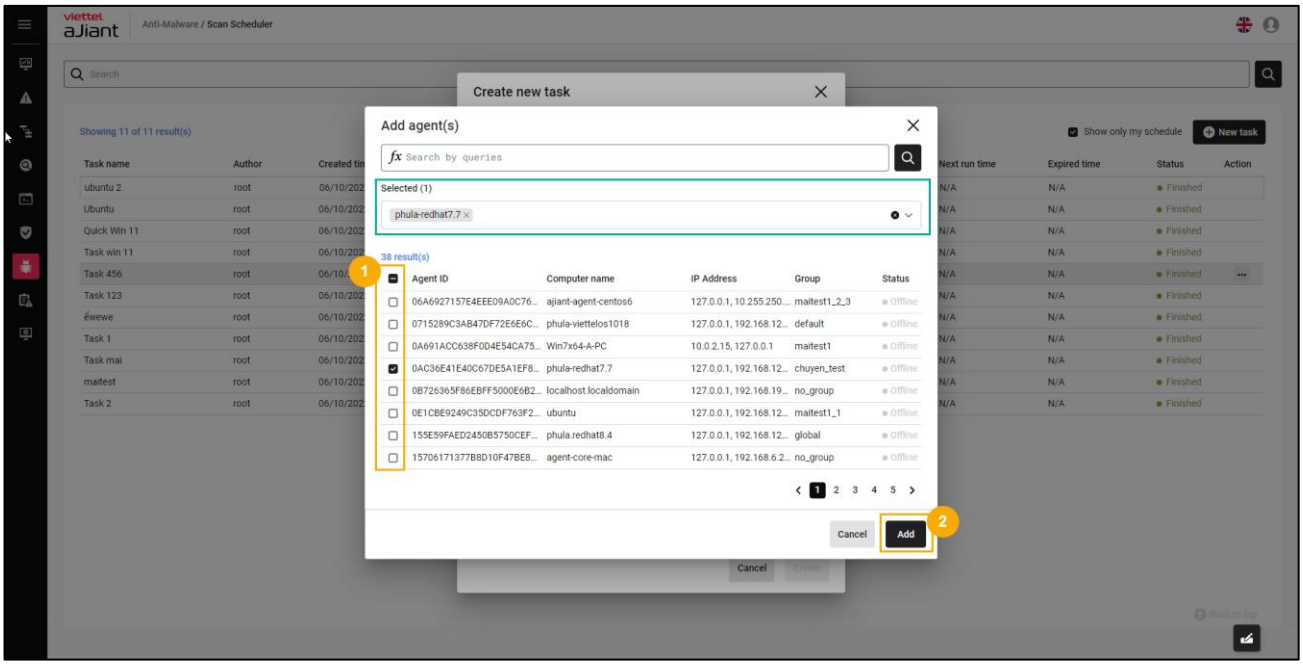
- Tìm kiếm máy trạm:

  - 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:



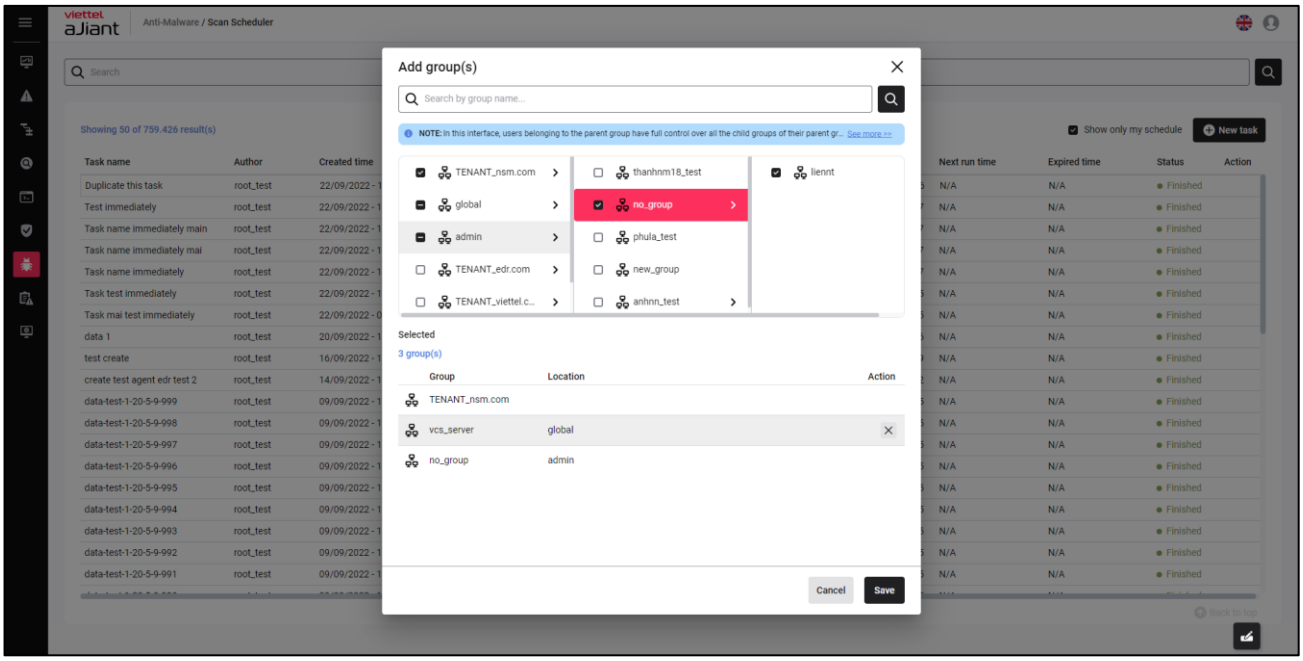
- Chọn nút **Add** để thực hiện thêm thông tin Agent/ Group → HT quay lại danh sách Agent/ Group;
- Hoặc chọn nút **Cancel** để thực hiện hủy thao tác thêm thông tin Agent/ Group;

➔ 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**

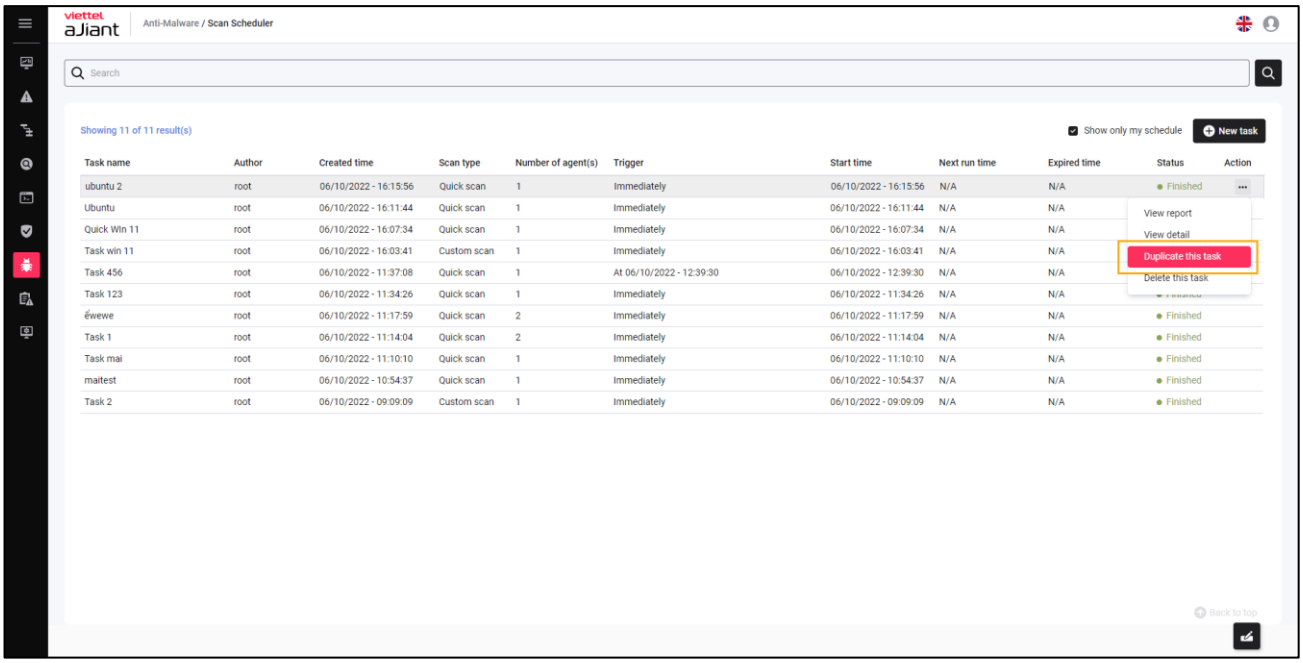
Bước 3: Người dùng chọn nút **Create** để hoàn thiện thao tác thêm mới lập lịch quét. Hoặc, chọn nút **Cancel** để hủy thao tác thêm mới lập lịch quét

3.11.2.3 Nhân bản Schedule task

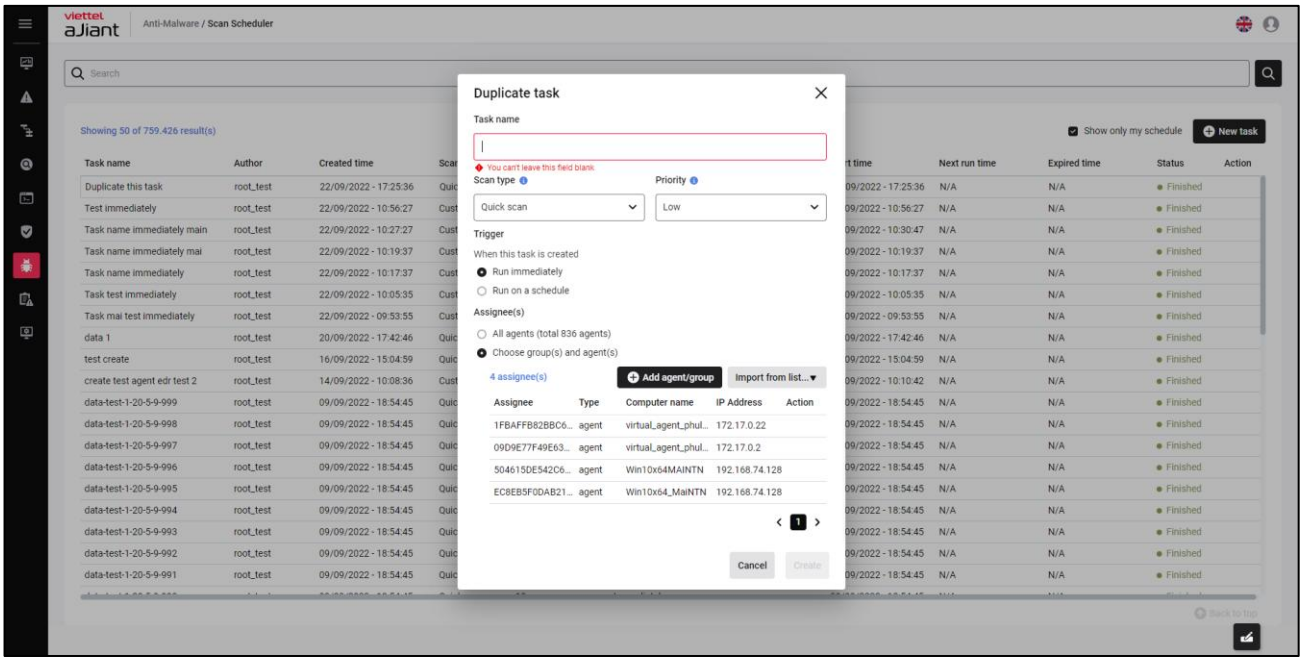
Mục đích: Cho phép người dùng nhân bản lập lịch quét.

Các bước thực hiện:

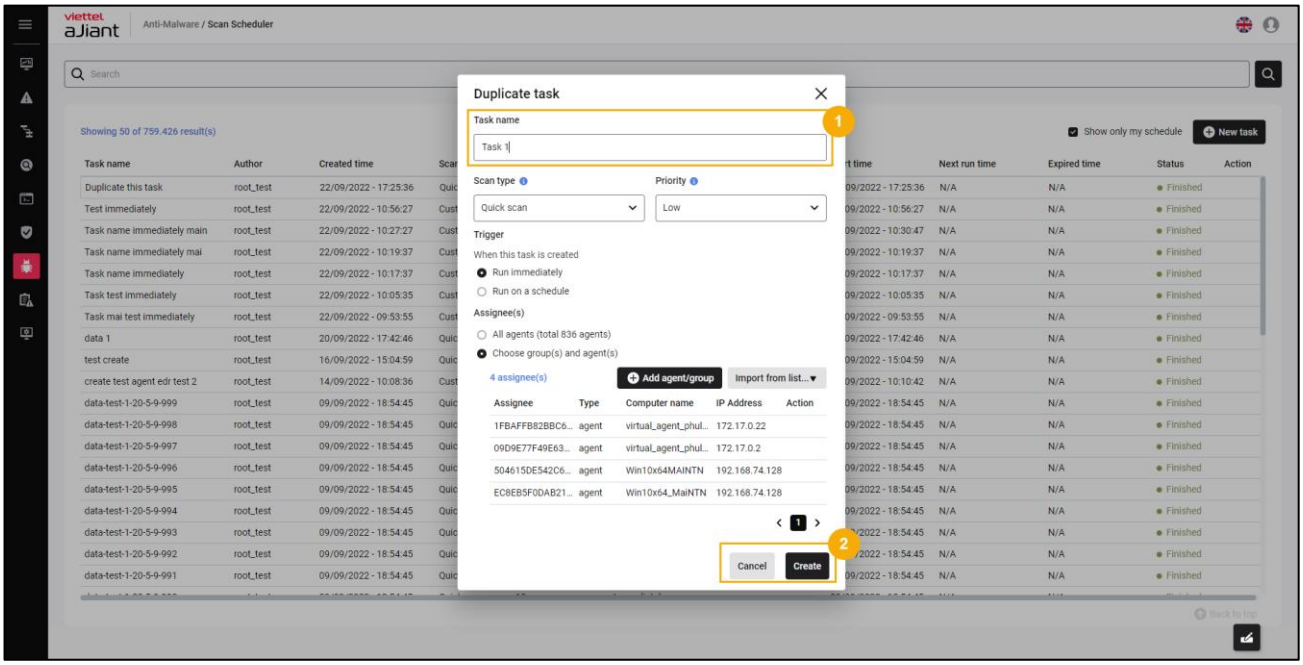
Bước 1: Tại màn hình danh sách task, người dùng chọn **Duplicate** bản ghi task cần nhân bản:



Bước 2: 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 3: 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.



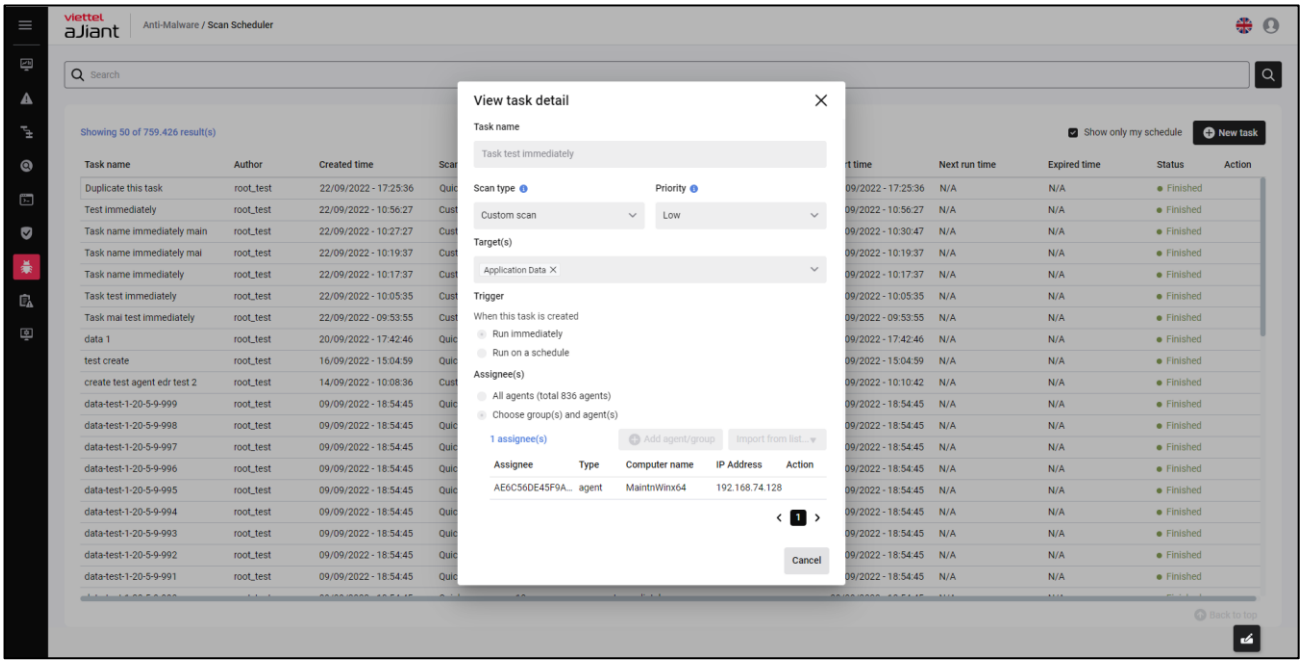
3.11.2.4 **Xem** chi tiết

Mục đích: Cho phép người dùng xem thông tin chi tiết lập lịch quét

Các bước thực hiện:

Bước 1: 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



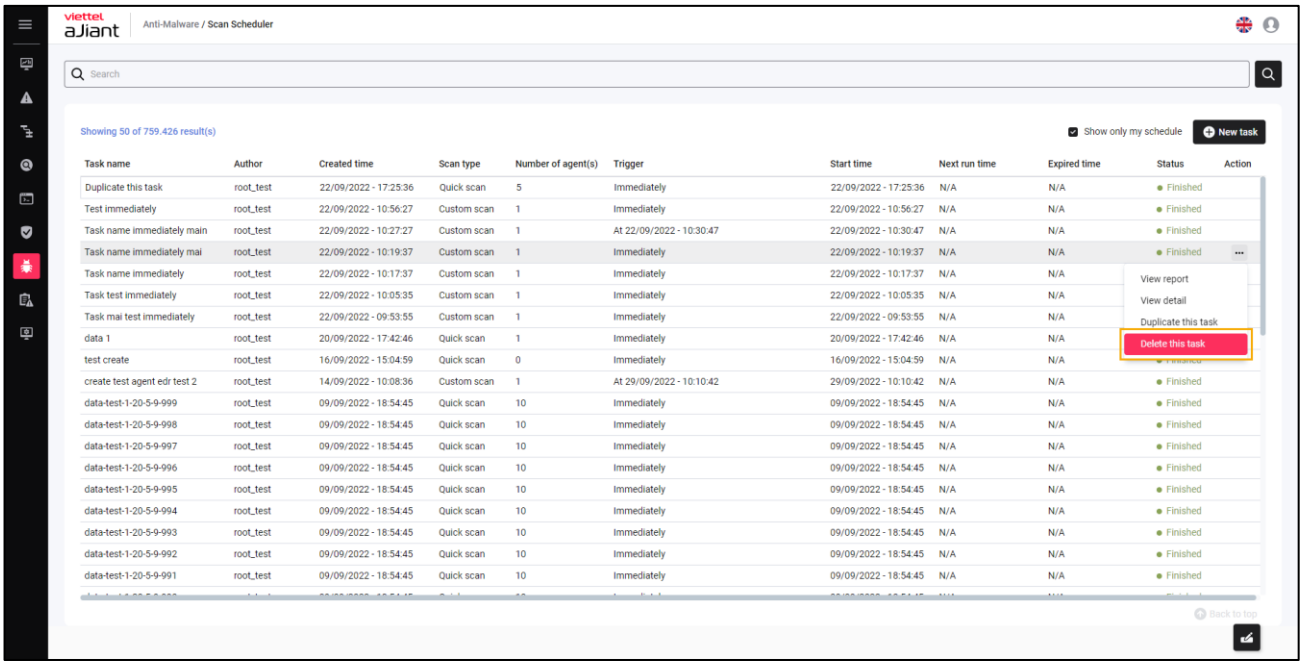
Bước 2: Người dùng chọn nút **Cancel** hoặc icon **Close** để hủy thao tác xem chi tiết lập lịch quét

3.11.2.5 Xóa Schedule task

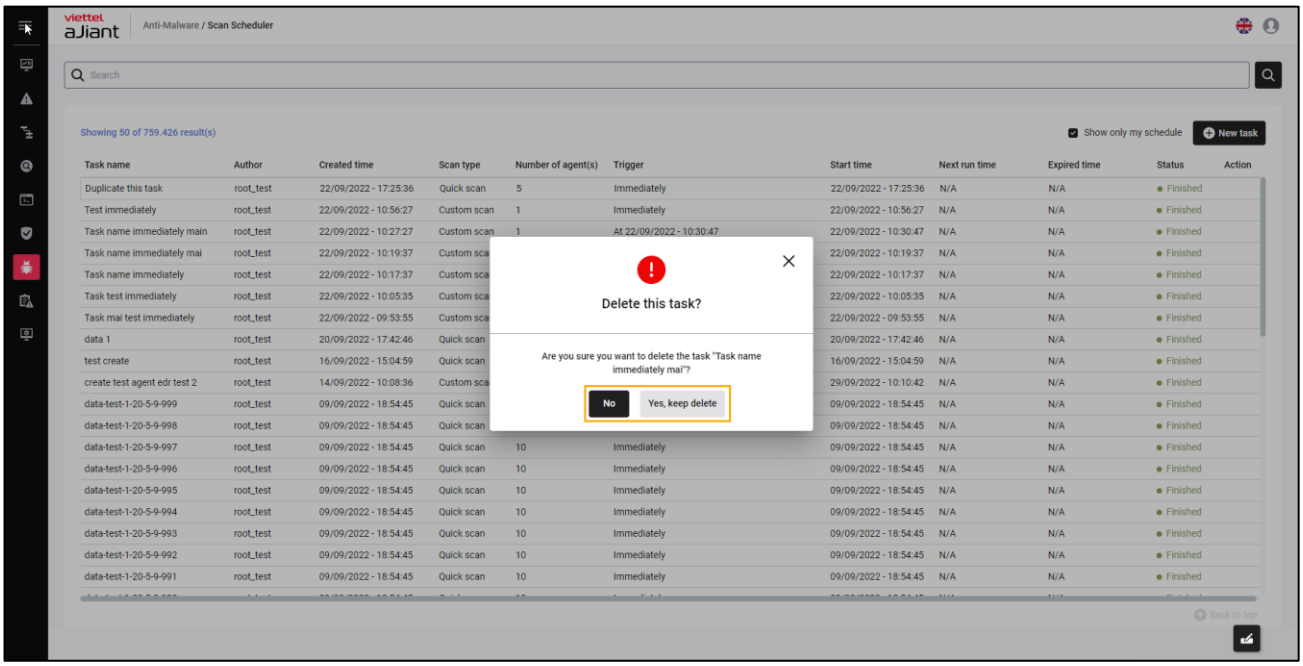
Mục đích: Cho phép xóa lập lịch quét trong danh sách task;

Các bước thực hiện:

Bước 1: Tại màn hình danh sách task, người dùng chọn **Delete this task** bản ghi task cần xóa;



Bước 2: 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

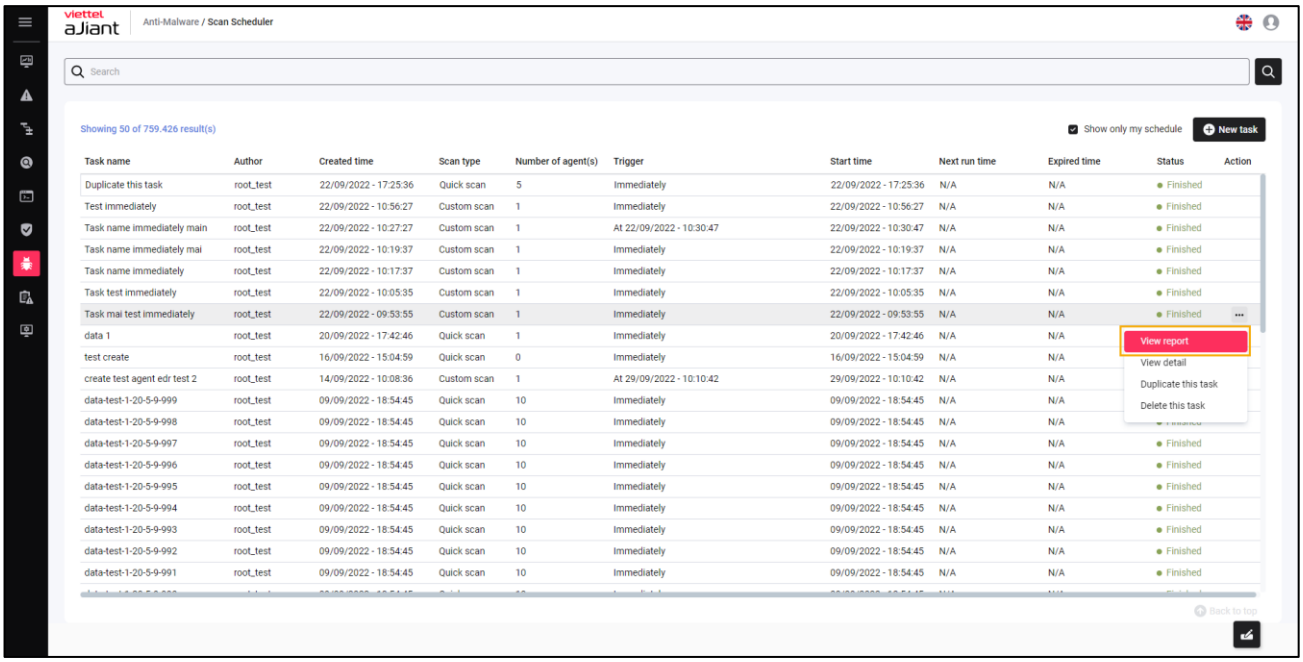


3.11.2.6 Xem báo cáo

Mục đích: Cho phép người dùng xem báo cáo lập lịch quét;

Các bước thực hiện:

Bước 1: Tại màn hình danh sách task, người dùng chọn **View report** bản ghi task cần xem báo cáo;

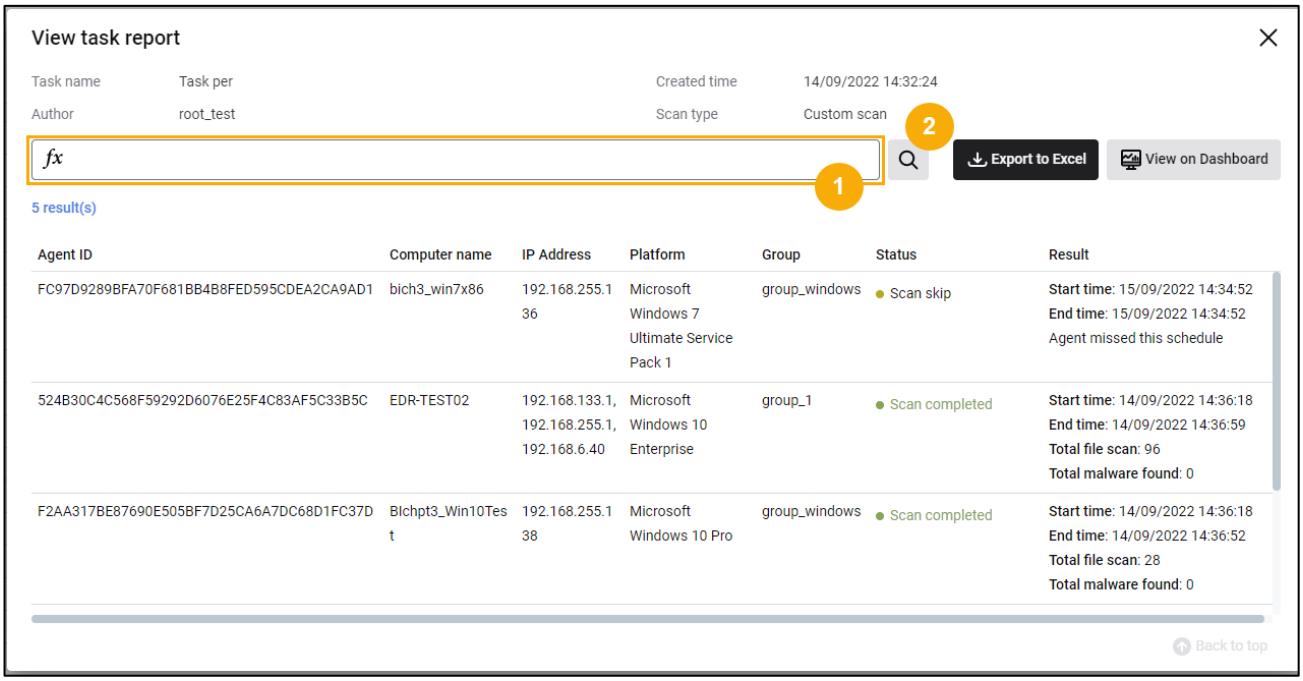


Bước 2: Hệ thống hiển thị màn hình **View report**:

1 – 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:

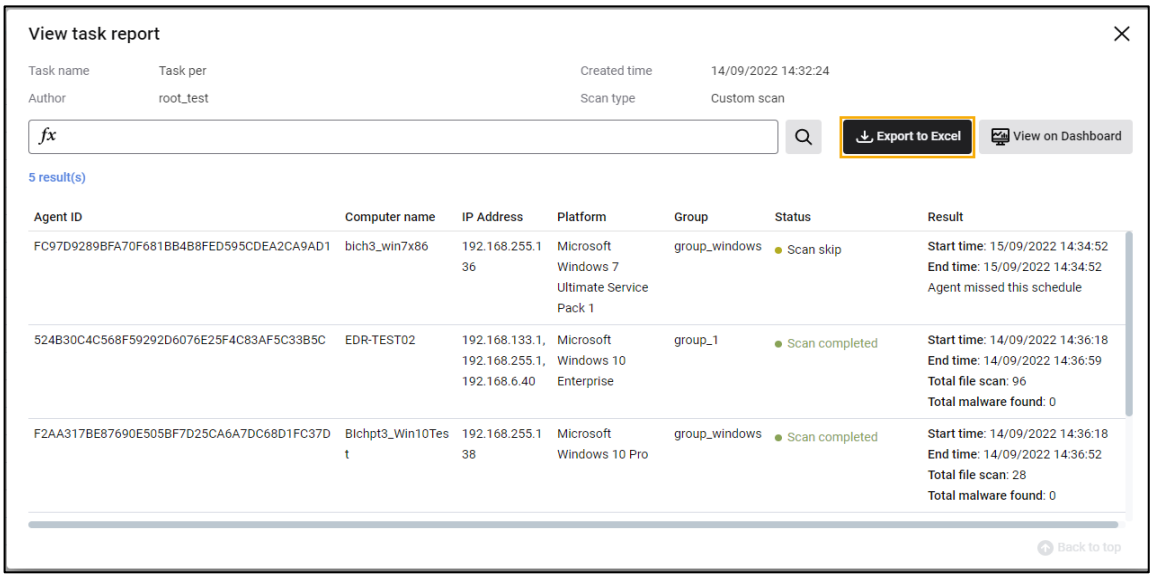


+ Người dùng nhập vào thông tin truy vấn và chọn icon hoặc nhấn nút **Enter** để xác nhận truy vấn;

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

2 – Export to Excel

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

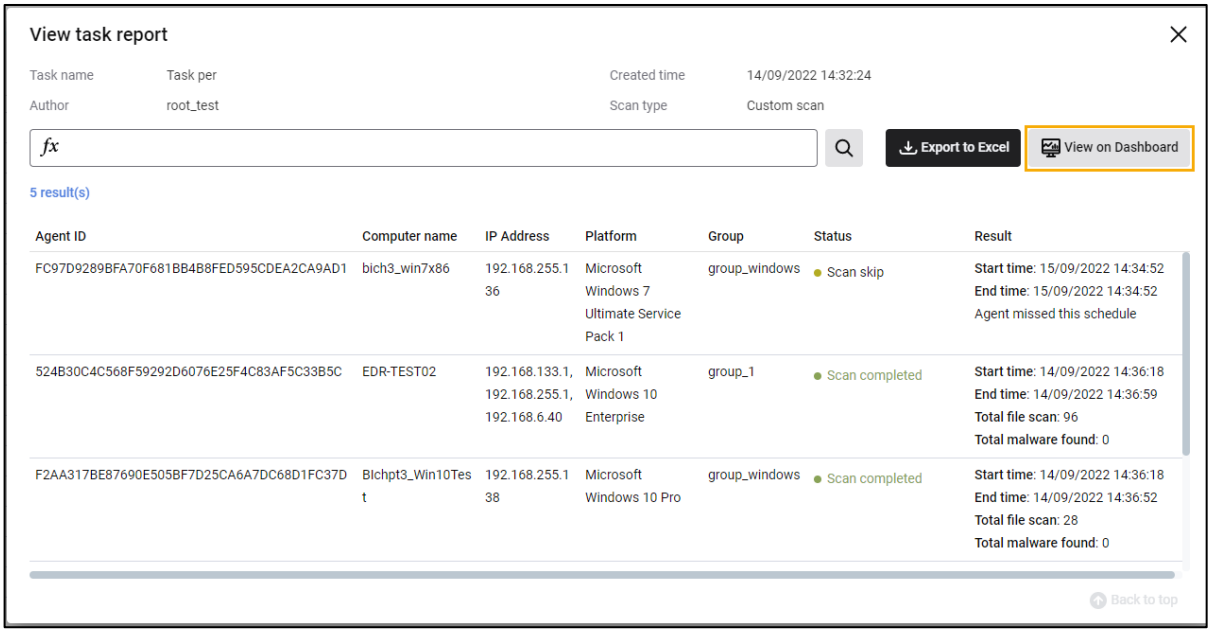


Các bước thực hiện: Tại màn hình View task report, người dùng chọn nút **Export to Excel**

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

3 – 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;

3.11.3 Device control

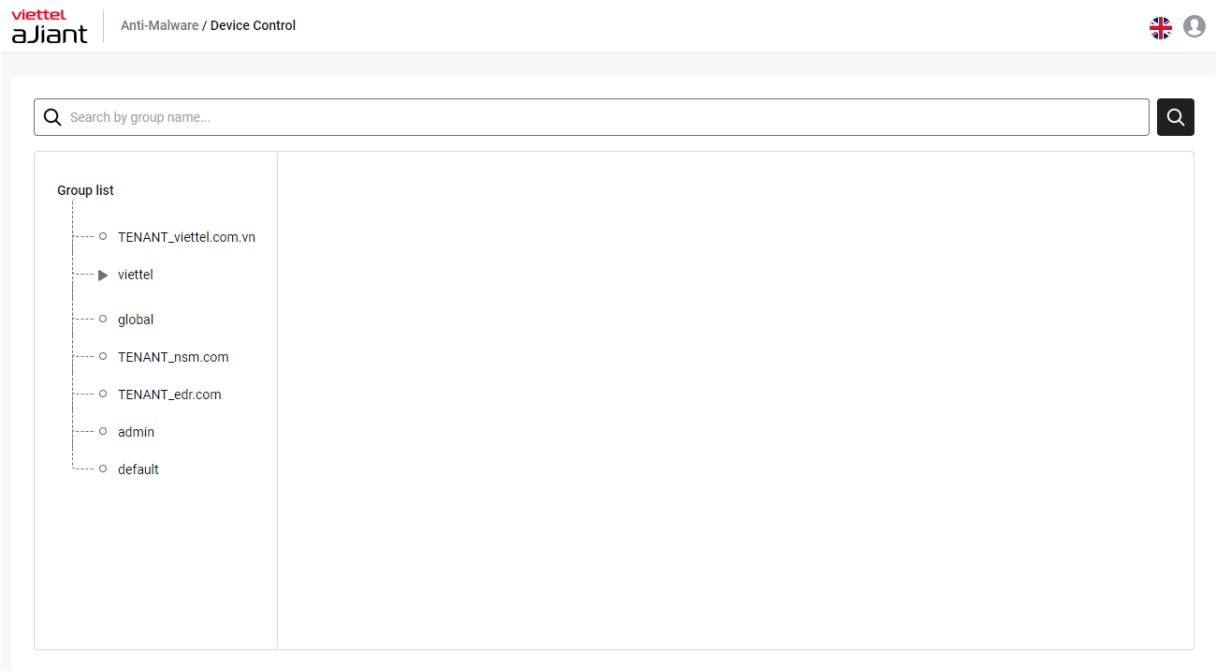
Chức năng: Cho phép kiểm soát, bảo vệ dữ liệu quan trọng thông qua thiết bị ngoại vi, như ổ USB, thiết bị Bluetooth và đĩa CD và DVD ghi được.

Mục đích: *Thiết bị USB, CD, DVD và các thiết bị ngoại vi khác, tuy rất hữu dụng nhưng cũng mang lại những mối đe dọa thực sự cho tổ chức. Do vậy, cần quản lý thông tin và kiểm soát các thiết bị ngoại vi thực hiện thao tác truy cập tới các máy tính của end users*

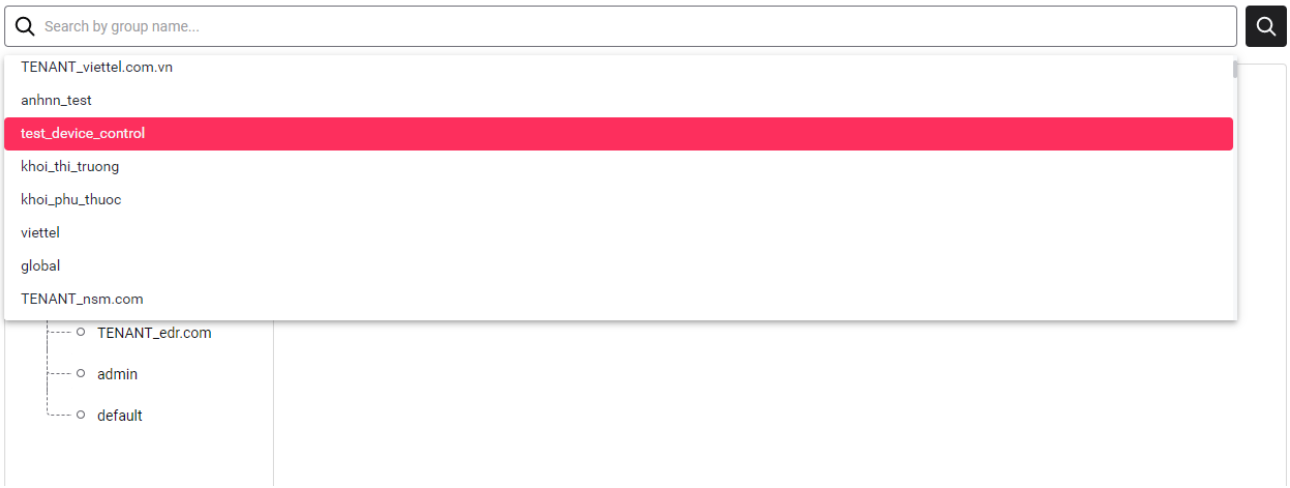
3.11.3.1 Tìm kiếm Group

Mục đích: Chức năng tìm kiếm Group cho phép người dùng hiển thị danh sách group list theo cấu trúc tree

Màn hình giao diện khi vào tính năng Device control: Anti-malware/Device-control



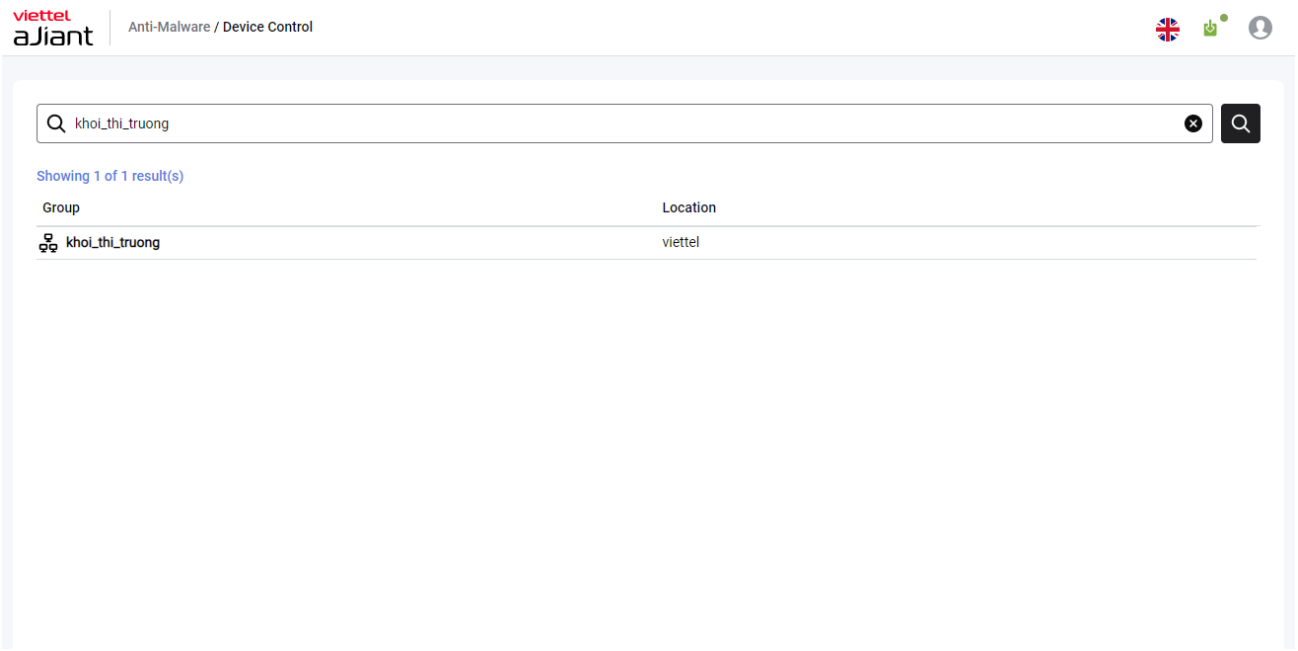
Bước 1: Người dùng nhập vào từ khóa tìm kiếm ở Search by group name (Có từ từ khóa gợi ý theo text)



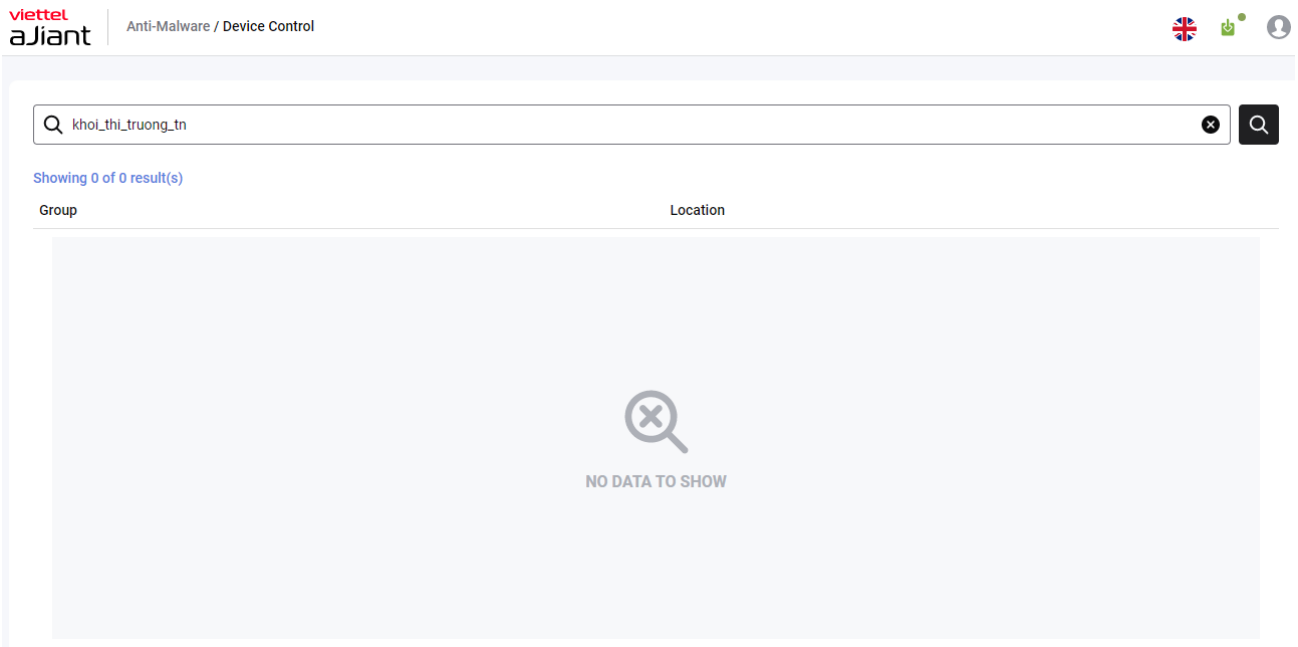
Bước 2: Chọn nút hoặc nhấn **Enter** để xác nhận thao tác tìm kiếm với từ khóa vừa nhập.

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

Nếu có kết quả sẽ trả về



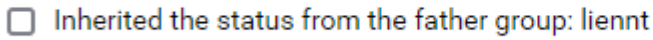
Còn tìm kiếm không có kết quả



3.11.3.2 Danh sách Device của từng group

Sau khi chọn hiện thị group mong muốn, màn hình sẽ hiện thị bảng Device Type

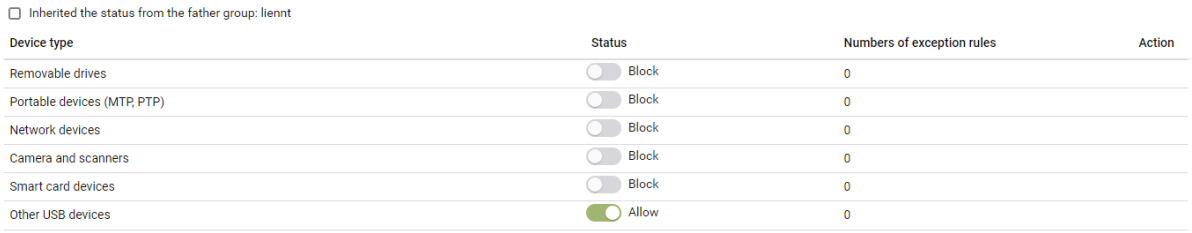
Có ô tích chọn



Group cấp dưới thì khi check chọn inherit thì nó sẽ kế thừa status và exception của group cha gần nhất>> Không có quyền chỉnh sửa, chỉ có quyền View

Còn uncheck thì ngược lại chị nhé nó tự thêm sửa xóa được

Về phần **Bảng danh sách thiết bị** bao gồm các trường thông tin sau:



+ Device type: hiển thị tên thiết bị fix cứng

+ Status*: Allow/Block* hiển thị trạng thái phân quyền truy cập từng loại thiết cho từng group.

+ **Numbers of exception rules**: hiển thị số lượng ngoại lệ (Exception rule) từng loại thiết bị cho từng group

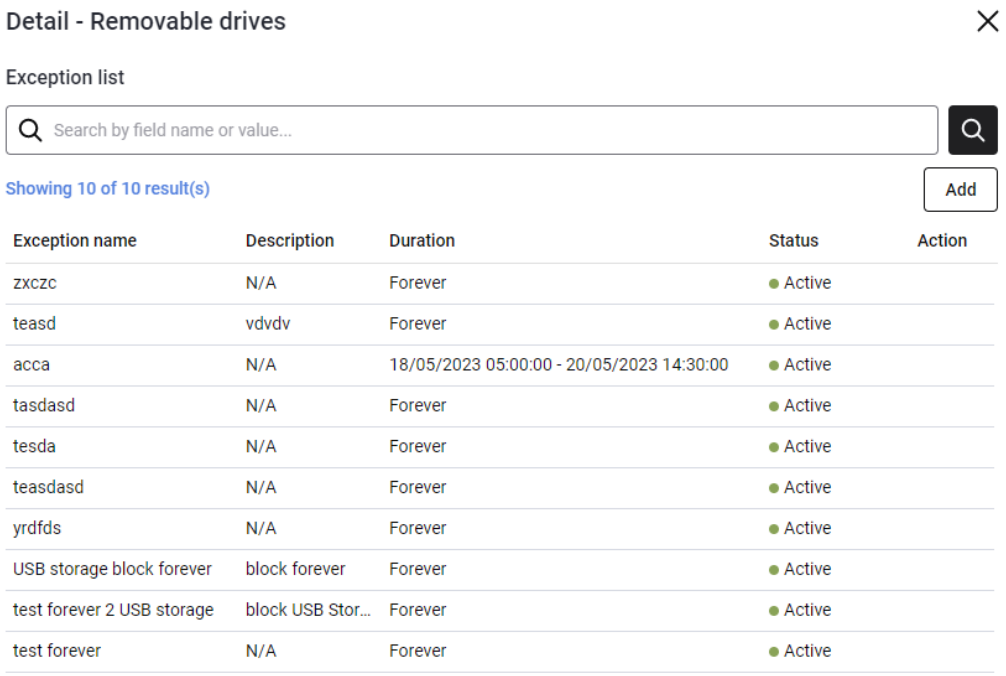
+ **Action:** Hiển thị icon Edit Exception tại column Action trên mỗi bản ghi khi hover vào bản ghi (Click icon edit=> Hiển thị tab Exception list)

3.11.3.3 Màn Exception

Mục đích:

Cho phép người dùng có thể xem được danh sách exception của loại thiết bị theo group.

Danh sách Exception list



- TH Numbers of exception rules = 0

>> Hiển thị msg "NO DATA TO SHOW"

- TH Numbers of exception rules !=0

>> Hiển thị danh sách exception tương ứng với thiết bị

Tìm kiếm không có kết quả

>>Hiển thị msg "NO DATA TO SHOW"

Tìm kiếm có kết quả

>>KT nhập chuỗi khớp 1 hoặc toàn phần trường name, không phân biệt chữ hoa hay thường. Khi bắt đầu nhập text, góc input sẽ có icon xóa => Click button **search** hoặc **enter**

Luôn hiển thị bảng danh sách exception bao gồm các trường thông tin sau:

1. Exception name - hiển thị tên ngoại lệ

2. Description - Mô tả thông tin được áp dụng ngoại lệ

3. Device(s) - hiển thị tên device

4. Duration - hiển thị thời hạn của exception

5. Status - hiển thị trạng thái của exception. Bao gồm Expired và Active

Nếu exception đã quá duration cho phép so với thời gian hiện tại thì hiển thị Status = "**Expired**"

+ Nếu exception đảm bảo duration cho phép so với thời gian hiện tại thì hiển thị Status = "**Active**"

6. Action:

Button **Add**: tạo mới được các Exception

Hiển thị số kết quả "Showing x of n results"

- x: đếm **số lượng** bản ghi **đang hiển thị** trên bảng danh sách
- y: đếm **tổng số lượng** tất cả các bản ghi đã ghi nhận

Tối đa 20 bản ghi trên bảng danh sách exception

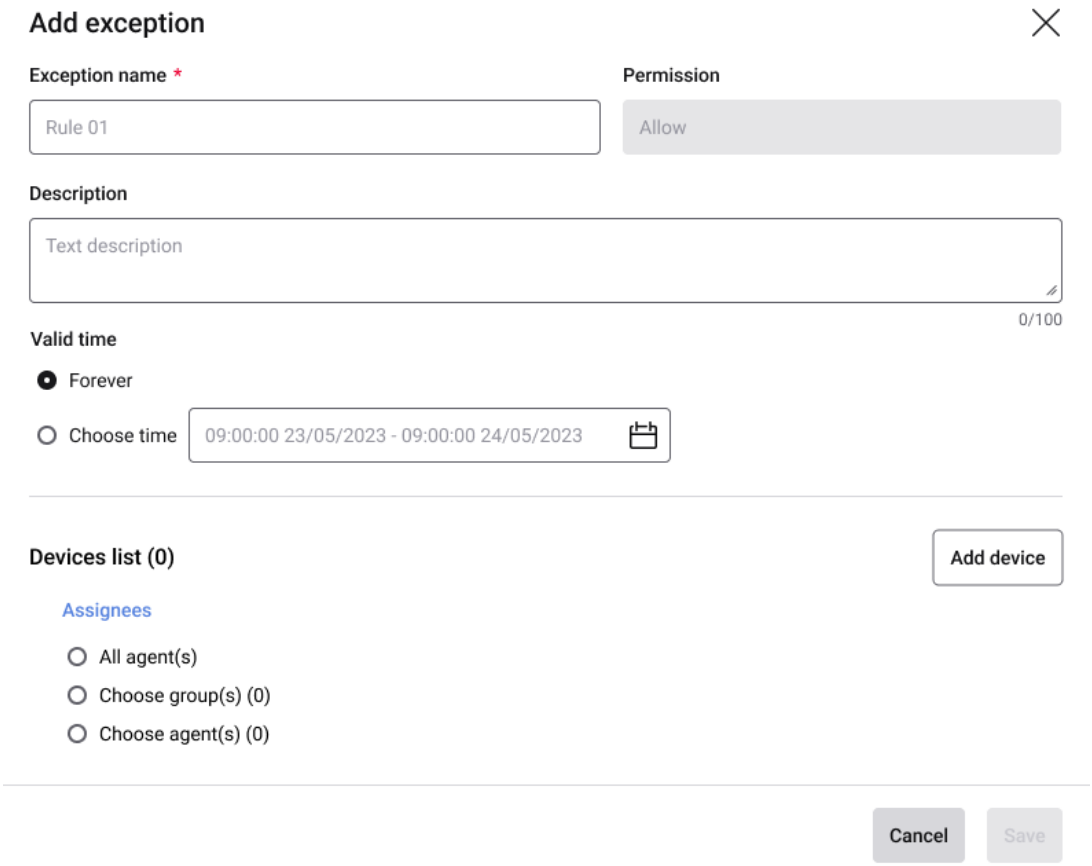
→ **Phân trang** bảng dữ liệu nếu > 20 bản ghi, người dùng chọn trang nào hiển thị bảng dữ liệu tương ứng với trang đó.

→ Mặc định hiển thị **trang đầu tiên**

→ Thứ tự bản ghi được hiển thị theo thời gian tạo mới/ chỉnh sửa (**gần nhất lên đầu** và đẩy dần các bản ghi cũ xuống dưới)

3.11.3.4 Màn Add Exception

Mục đích: tạo mới được các ngoại lệ, để mỗi đơn vị có thể ngoại lệ một số người dùng cuối được phép truy cập thiết bị (phục vụ mục đích nghiệp vụ cá nhân)



- **Exception name:** Cho phép nhập tên của exception(Bắt buộc, không được trùng tên). Kí tự theo anphabet, số 1,2.3..0, không phân biệt chữ hoa, chữ thường, dưới 500 kí tự
- **Permission** - Hiển thị phân quyền truy cập của exception (để dạng Disable),

Nếu loại thiết bị được phân quyền truy cập là **Allow**, tương ứng phân quyền truy cập của exception là **Block**

+ Nếu loại thiết bị được phân quyền truy cập là **Block**, tương ứng phân quyền truy cập của exception là **Allow**

- **Description:** mô tả thông tin việc tạo exception
- **Valid time** - Cho phép lựa chọn thời hạn hợp lệ của exception

  Để radio button và có 2 lựa chọn cho người dùng:

  - **Forever :** Cho phép/ Chặn mãi mãi

- **Absolute time range** → Định dạng hiển thị dd/mm/yyyy hh:mm:ss - dd/mm/yyyy hh:mm:ss (mặc định là thời điểm hiện tại đến tương lai, thời gian để chênh 5 phút để người dùng k bị gặp lỗi khi đang Add exception (thời gian thao tác lâu)

Nếu tồn tại ít nhất một bản ghi exception thì hiển thị Bảng danh sách exception bao gồm các trường thông tin sau:

1. **Exception name** - hiển thị tên ngoại lệ
2. **Description** - Mô tả thông tin được áp dụng ngoại lệ
3. **Device(s)** - hiển thị tên device
4. **Duration** - hiển thị thời hạn của exception
5. **Status** - hiển thị trạng thái của exception. Bao gồm Expired và Active

Nếu exception đã quá duration cho phép so với thời gian hiện tại thì hiển thị Status = "**Expired**"

+ Nếu exception đảm bảo duration cho phép so với thời gian hiện tại thì hiển thị Status = "**Active**"

6. Action:

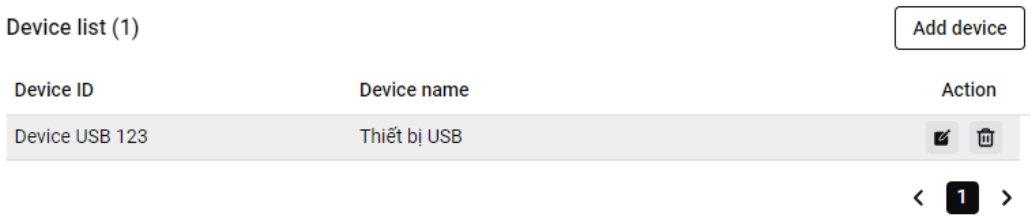
- Button Add: tạo mới được các Exception

Device list (mặc định ít nhất 1 bản ghi device)

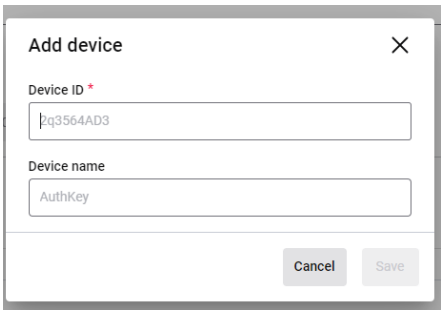
Khi chưa có device: Chỉ hiển thị Button Add device

Khi có device: Hiển thị Button Add device và hiển thị table gồm các column: Device control ID, Action (Hiển thị icon edit, xóa khi move chuột vào)

- Nếu người dùng chỉ có quyền view thì chỉ có quyền xem mà k dc Add, edit, xóa



Click vào button **Add device** ra popup để người dùng nhập thông tin tạo thiết bị ngoại lệ



Thông tin gồm:

- **Device ID**: chứa ký tự alphabet, số, ký tự đặc biệt, ID của thiết bị ngoại vi, trường bắt buộc
- **Device name**: hiển thị tên của thiết bị, có thể để trống

Khi chưa nhập Device ID thì nút **Save** sẽ disable.

Khi đã nhập đủ thông tin, nút **Save** sẽ avialbe.

Nhất **Cancel** hoặc click icon đóng sẽ thoát khỏi màn popup

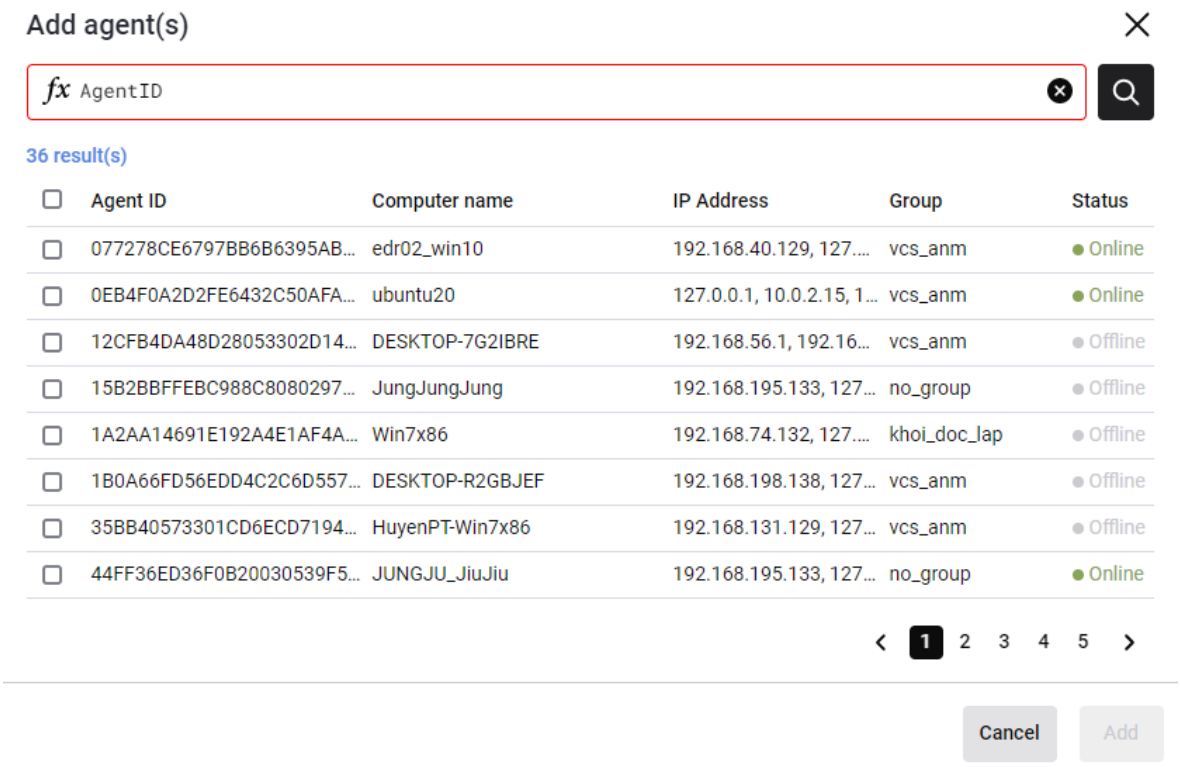
Quay trở lại màn **Add exception**

Assigness có 3 option cho người dùng chọn (chọn được 1 option)

- Nếu chọn **All agent(s),** chọn tất cả agent cho phép/chặn thiết bị Exception này.
- Nếu chọn **Choose agent(s) (0),** người dùng có thể chọn 1 hoặc nhiều agent cho phép/ chặn thiết bị Exception này.

Lúc này sẽ hiện thị thêm button **Add agent.**

Click vào button sẽ ra 1 popup tương ứng (Chỉ có các agent thuộc group đó mới hiện thị ở phần Add agent(s).)



Search:

Cho phép người dùng nhập vào key tìm kiếm thông tin Query gợi ý có trong hệ thống theo AgentID, Computer name, IP address

Mặc định trống, không bắt buộc nhập, cho phép nhập ký tự đặc biệt;

>> Khi click kiểm tra nội dung query đã đúng format query chưa:

Thực hiện tìm kiếm dữ liệu, kiểm tra có dữ liệu thỏa mãn: KT nhập chuỗi khớp 1 hoặc toàn phần trường name, không phân biệt chữ hoa hay thường. Khi bắt đầu nhập text, góc input sẽ có icon xóa

=> ***Click button search hoặc enter***

- Luôn hiện thị các trường thông tin như cột: Agent ID, *Computer name, IP address, Group, Status*

+ Nếu không có dữ liệu thỏa mãn, thông báo: No data;

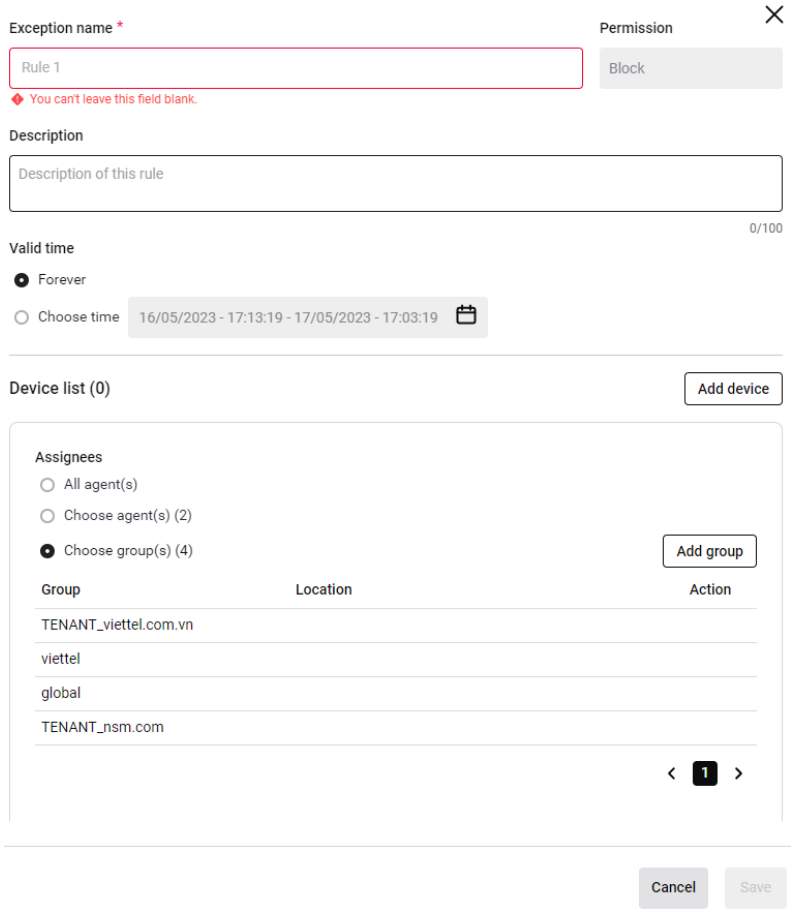
+ Nếu có dữ liệu thỏa mãn: Hiển thị danh sách tương ứng;

- Checkbox: Cho phép check chọn 1 hoặc nhiều Agents, Mặc định không check;
- Agent ID: Hiển thị thông tin Agent ID
- *Computer name*: Hiển thị thông tin thiết bị (máy tính)

- *IP address:* Hiển thị thông tin địa chỉ IP của thiết bị (máy trạm)
- *Group:* Hiển thị thông tin Group của Agent
- *Status:* Hiển thị thông tin trạng thái hoạt động của Agent: Online/ Offline
- Có phân trang, tối thiểu 8 bản ghi

Sau khi tích chọn agent nào thấy phù hợp, button ***Add*** sẽ dc aviable lên
Click vào nút **Add** là người dùng đã chọn thành công 1 hoặc nhiều agent vào phần Add Exception

Sau khi Add xong Agent quay về màn Add Exception:
Sẽ hiện thị các trường : Agent ID Computer name IP Address Group Status
Màn này hiển thị thêm cột Action (Icon Xóa), 5 bản ghi tối đa nhiều thì phân trang



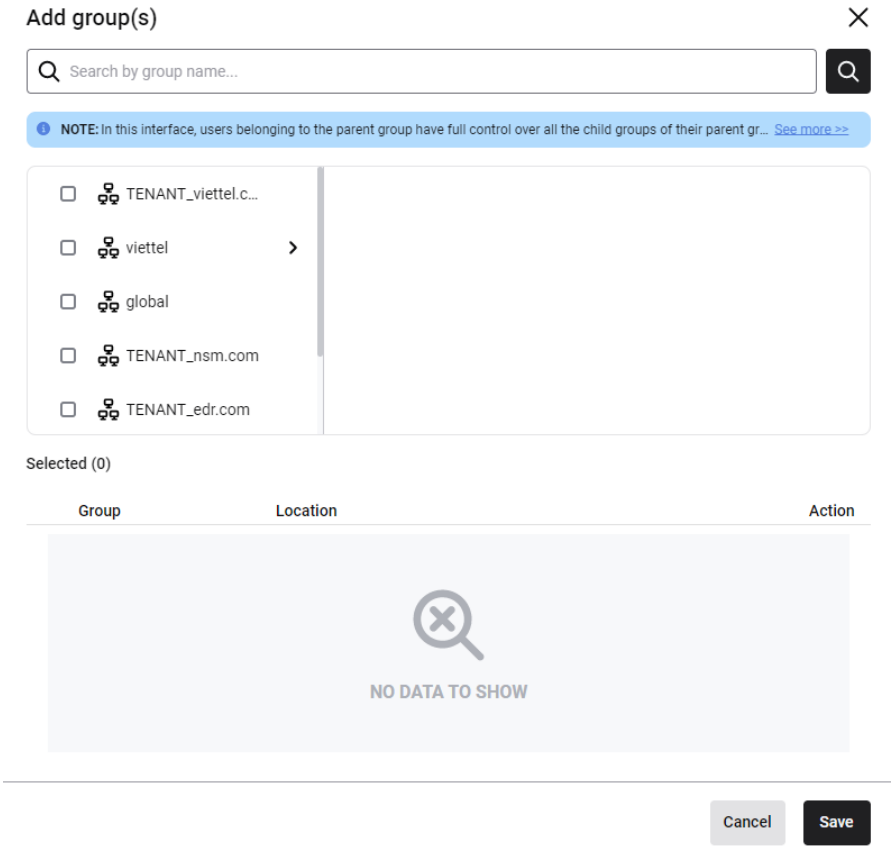
- Nếu chọn ***Choose group(s) (0),*** người dùng có thể chọn 1 hoặc nhiều group cho phép chặn thiết bị này. Mặc định hiển thị danh sách Group (theo user đăng nhập quản lý).

Danh sách Group yêu cầu hiển thị dạng cây, yêu cầu check trùng trong chính danh sách Group

Search box: Cho phép người dùng nhập vào key tìm kiếm thông tin Group có trong hệ thống theo Group name
Mặc định trống, không bắt buộc nhập, Trim khoảng trắng đầu cuối, cho phép nhập ký tự đặc biệt;

Click vào Button ***Search***, thực hiện tìm kiếm thông tin Group liên quan đến key tìm kiếm có trong hệ thống

***Checkbox Item*:** Cho phép check chọn 1 hoặc nhiều Group, mặc định không check;



Check trùng Group(s);

Mặc định không hiển thị kết quả nếu người dùng không lựa chọn bản ghi nào;

Nếu tồn tại ít nhất 1 bản ghi thì hiển thị phân trang và số lượng Agent(s) đã được chọn;

Checkbox: Tích chọn 1 hoặc nhiều group mà Agent đó có trong các group liên quan. Mặc định là không chọn(uncheck)

Các thuộc tính cột bao gồm: *Group, Location, Action.* Chọn cái nào sẽ có **Seleted(0)** tương ứng

Group: Hiển thị thông tin Group của Agent

Location: Hiển thị vị trí cây quan hệ của Group;

VD: root/ TT GPSP/EDR

Action: (xóa) nếu không muốn chọn group đó

Nếu không chọn 1 group nào >> Trả về No data

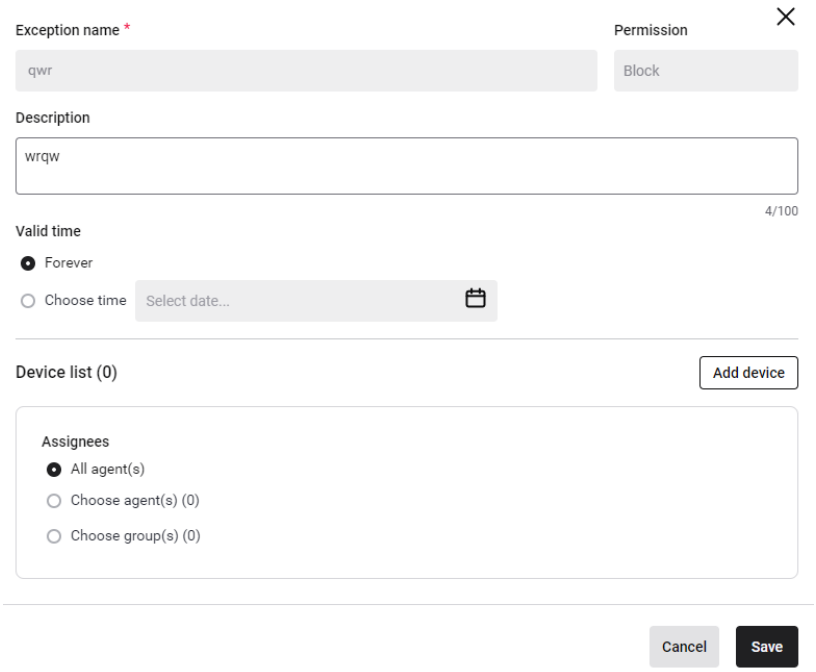
Sau khi đã chọn group hợp lý, người dùng chọn button **Save** thành công, quay về màn **Add Exception** . Lúc này Portal sẽ hiện thị 1 thông báo, Bạn đã thêm exception thành công

Nếu không muốn chọn group bạn click **Cancel** để quay về màn **Add Exception**

Khi đã đủ thông tin cần thiết cho **Add Exception**, người dùng chọn **Save** để lưu toàn bộ thông tin của Exception này. >> **quay lại màn Exception list của group đó**

Ở màn Exception list, Lúc này ở phần Action, có icon **Edit** và **Delete**

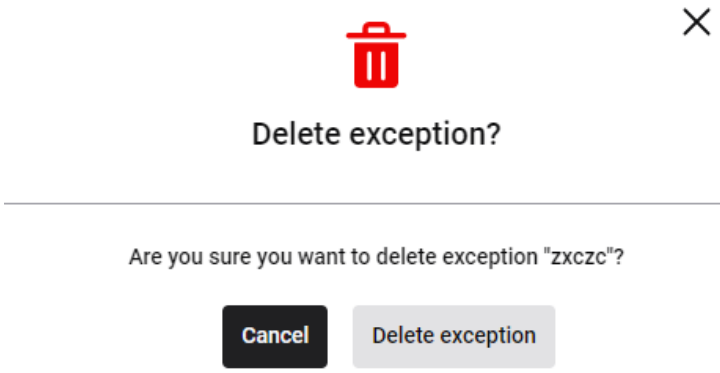
Nếu chọn icon Edit sẽ ra màn tương tự



Chỉ có Exception name, Permission là bị khóa, không thay đổi được. Còn lại người dùng có thể tự ý thay đổi.

Sau khi chỉnh sửa click Save để lưu lại thông tin. Lúc này Portal sẽ hiện thị 1 thông báo, Bạn đã edit exception thành công

Với trường hợp Icon xóa, hiện thị popup



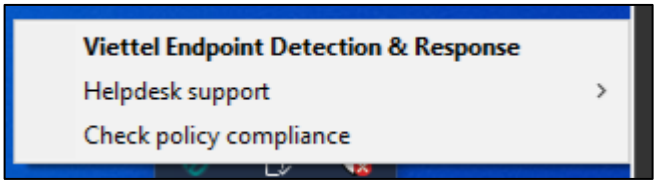
Nếu chọn Button **Delete exception** người dùng đồng ý Exception này. Lúc này Portal sẽ hiện thị 1 thông báo, Bạn đã xóa exception thành công

Chọn **Cancel** thì quay lại màn **Device list.**

3.12 Giao diện phía Agent GUI - Main

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

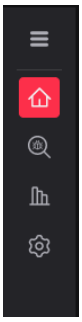
Trên thanh taskbar tìm icon  click chuột phải và chọn “Viettel Endpoint Detection & Response”:



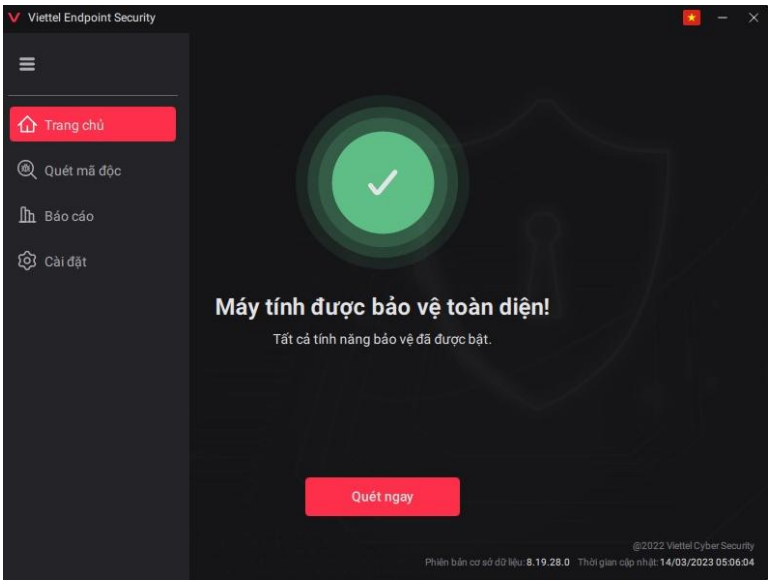
Hệ thống hiển thị các thông tin:

+ Được hiện thị 2 ngôn ngữ: Anh-Việt.

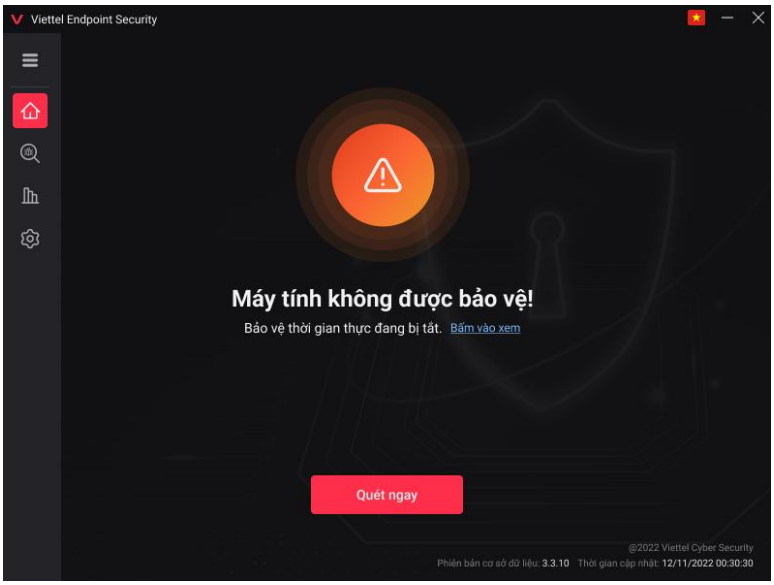
+ Trên Siderbar hiện icon cho các tính năng lớn: Trang chủ, Quét mã độc, Báo cáo, Cài đặt. Có thể đóng hoặc mở rộng siderbar.



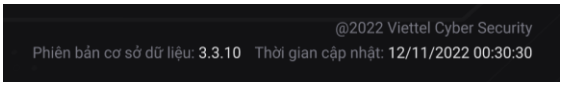
+ Trường hợp máy không có mã độc nào, đã được bật Real-time Protection hoặc toàn bộ mã độc đã được xử lý:



+ Trường hợp máy có ít nhất 01 mã độc vì không bật Real-time protection



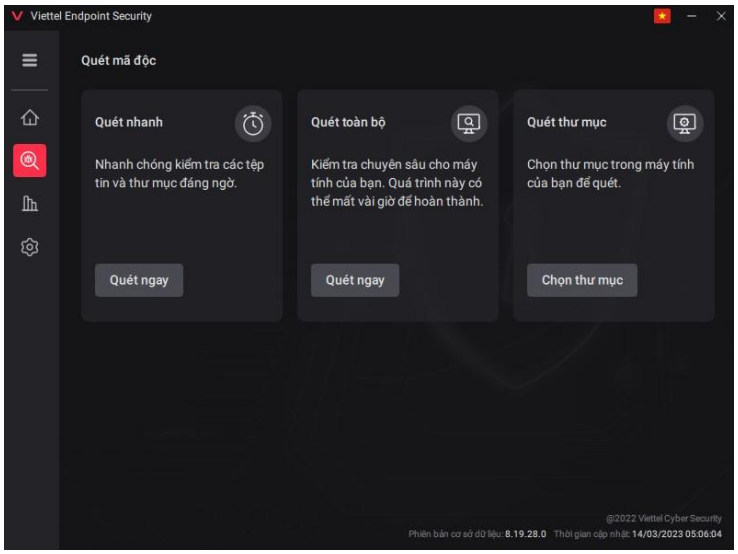
Thông tin về version: thông tin về phiên bản Agent cài trên máy người dùng, thời gian update và thông tin hỗ trợ sản phẩm, được thể hiện ở góc màn hình.



3.13 Giao diện phía Agent GUI - Protection

Mục đích: cho phép người dùng chủ động sử dụng hệ thống để quét và xử lý mã độc trên máy

Chỉ cho phép thực hiện 1 loại scan: Quick scan, Full scan, Custom scan(quét nhanh, quét toàn bộ, Quét thư mục)

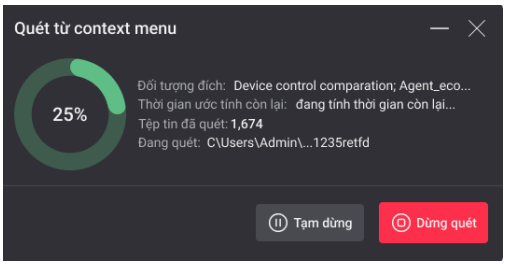


Các phương thức quét được hỗ trợ bao gồm

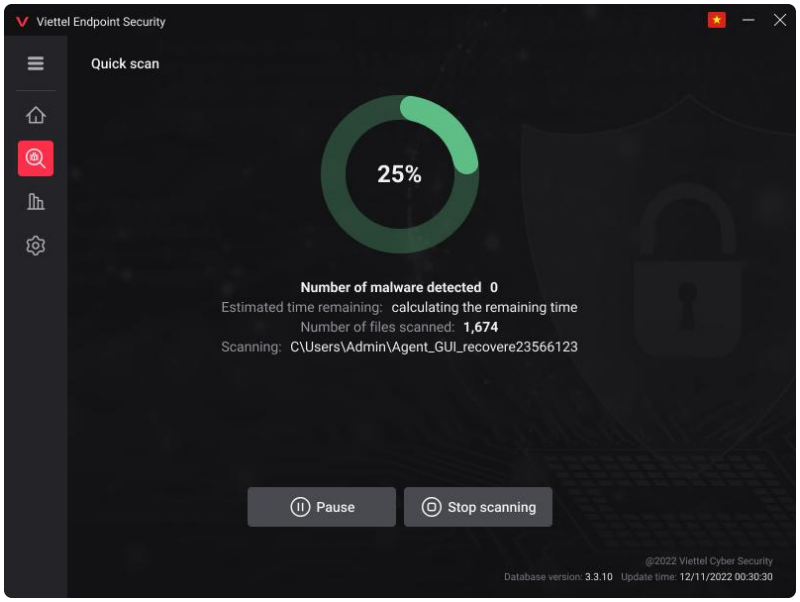
+ Lựa chọn các hình thức quét từ giao diện phía agent;

- **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.

+ Lựa chọn trực tiếp từ file explorer, cho phép chọn nhiều tệp tin và thư mục, chuột phải chọn quét (**Context scan**);



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



+ Hiển thị % tổng quá trình scan

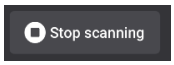
+ Hiển thị thông tin số lượng mã độc đã được phát hiện

+ Hiển thị thời gian ước lượng còn lại để kết thúc scan

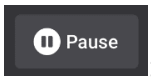
+ Hiển thị số lượng file đã được scan

+ Hiển thị đường dẫn file Đang scan

Hỗ trợ các thao tác trong lúc quét như sau:

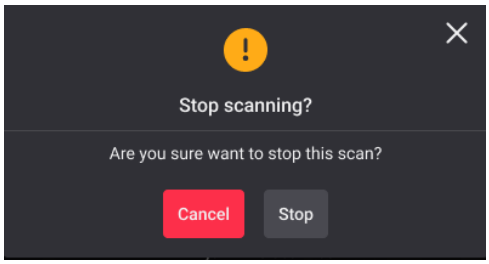


: Cho phép kết thúc quá trình quét;

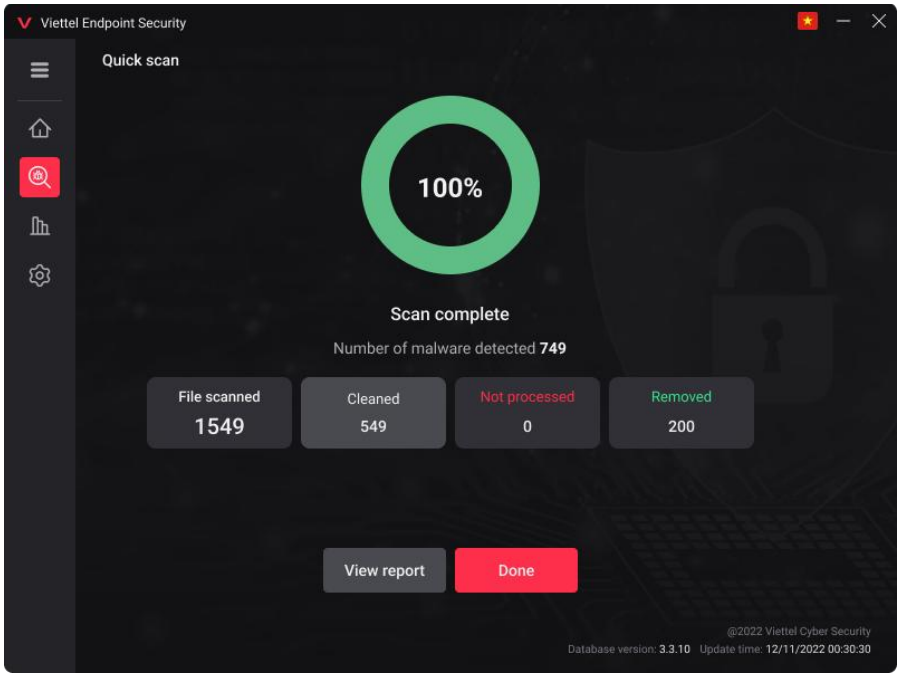


: Cho phép tạm dừng quá trình quét;

Khi click vào Pause, đồng thời button chuyển thành Resume lúc này cho phép chọn để tiếp tục quét



Sau khi thực hiện xong quá trình quét, hiện thị kết quả quét



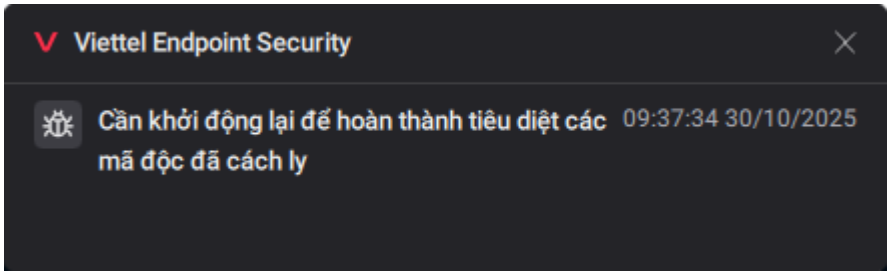
+ File scaned: Hiển thị số lượng file đã được scan
+ Cleaned: Hiển thị tổng số file đã được diệt
+ Not processed: Hiện thị tổng số file chưa xử lý
+ Removed: Hiện thị tổng số file đã được xóa

Các Button này có thể link trực tiếp sang phần báo cáo liên quan.

Hoặc có thể click vào button View report để xem tổng thể báo cáo của kết quả vừa quét.

Click done Done để quay về màn chính của Protection

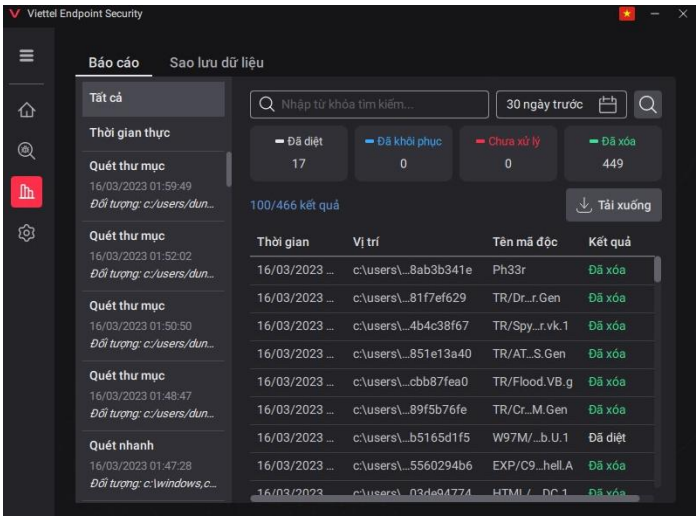
Sau quá trình quét, nếu agent phát hiện mã độc dạng dll đang được load mà không thể xóa trực tiếp được, agent sẽ hiển thị popup yêu cầu restart máy để hoàn tất quá trình quét



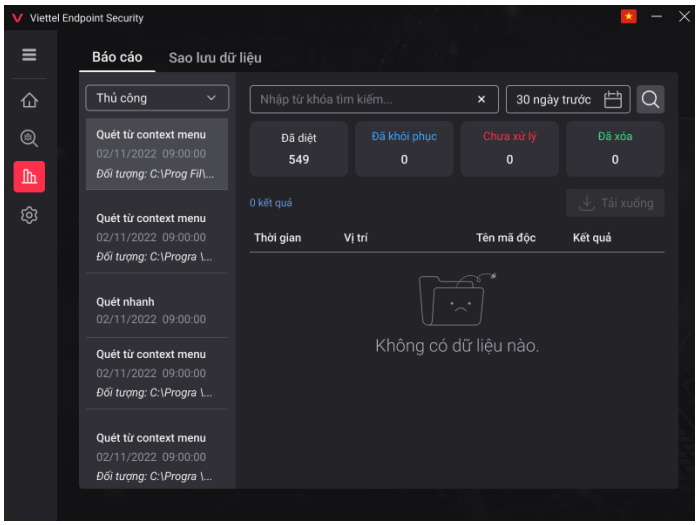
3.14 Giao diện phía Agent GUI - Report

Mục đích: Thống kê báo cáo phát hiện mã độc của thiết bị, hiện thị được tổng số mã độc được liệt kê trong danh sách

a. Tab report (Báo cáo)



- Trong trường hợp **không có kết quả phù hợp** với yêu cầu tìm kiếm thì hiển thị trạng thái **Không có dữ liệu nào**



- Nếu người dùng chọn All:

+ Danh sách mã độc: Hiển thị tất cả các mã độc đã được phát hiện;

- Nếu người dùng chọn Manual scan:

+ Danh sách số lần scan: Hiển thị danh sách lịch sử scan trong 30 ngày gần nhất;

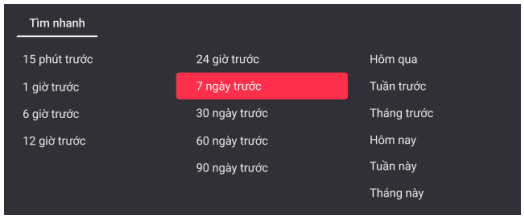
+ Mặc định: Chọn lần scan gần nhất để hiển thị danh sách mã độc tương ứng cho người dùng;

+ Danh sách mã độc: Hiển thị tất cả các mã độc được phát hiện với lần scan người dùng lựa chọn;

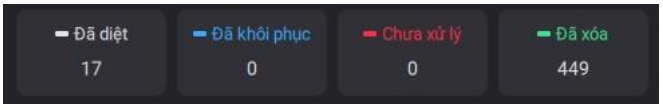
- Nếu người dùng chọn Real-time:

+ Danh sách mã độc: Hiển thị tất cả các mã độc được phát hiện realtime

- *Tìm kiếm theo thời gian:* 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



- Tìm kiếm theo kết quả mã độc

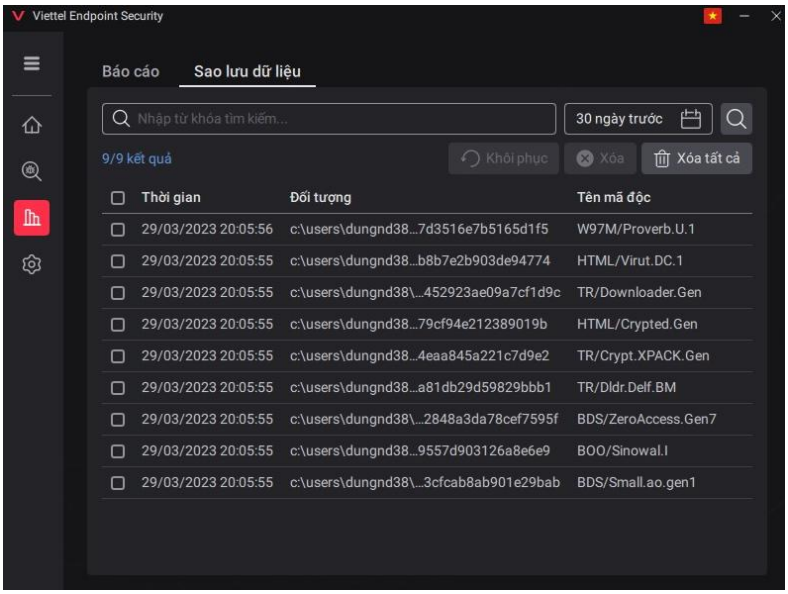


Trong mục report người dùng có thể tải toàn bộ báo cáo về máy (theo các mục đã chọn)

b. Tab Backup

Mục đích: thông tin danh sách các file mã độc đang được backup

Người dùng có thể tìm kiếm, lựa chọn thời gian rồi click tìm kiếm danh sách sẽ hiện thị theo tham số tìm kiếm.



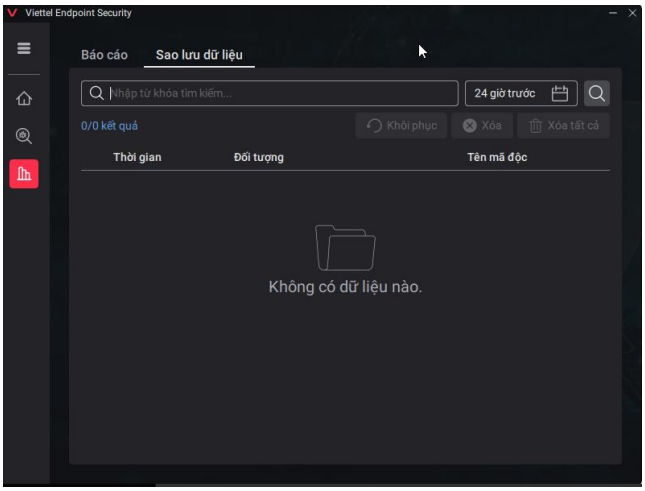
Các file chứa mã độc trước khi được xử lý đều được lưu trữ bản gốc trong thư mục Backup, để dọn thư mục Backup hoặc phục hồi file, sản phẩm cung cấp các tính năng sau:

Khôi phục: Cho phép lựa chọn 01 hoặc nhiều file để phục hồi;

Xóa: Cho phép lựa chọn 01 hoặc nhiều file để xóa khỏi thư mục Backup;

Xóa tất cả: Cho phép dọn nhanh toàn bộ file hiện có trong thư mục Backup;

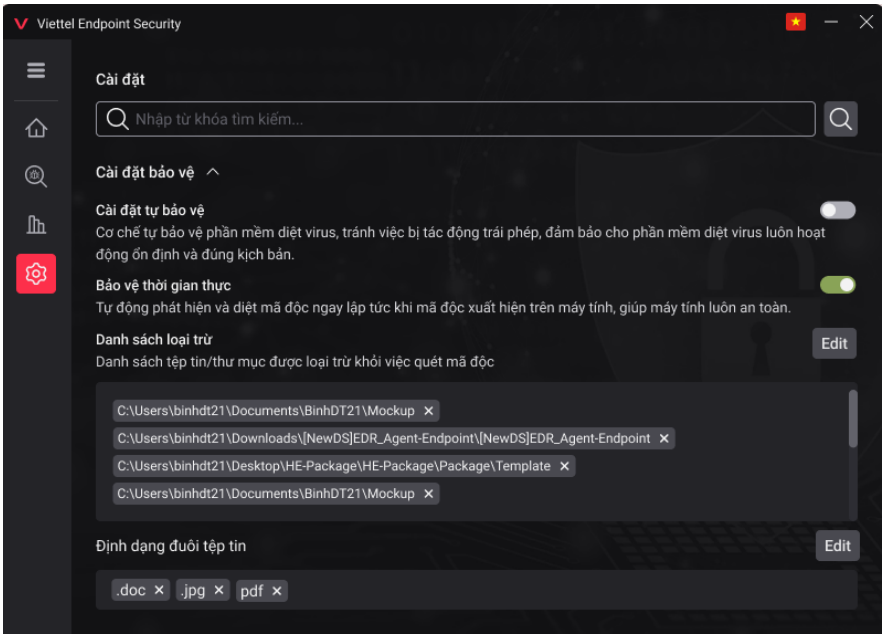
- Trong trường hợp không có kết quả phù hợp với yêu cầu tìm kiếm thì hiển thị trạng thái **Không tìm thấy kết quả phù hợp**



3.15 Giao diện phía Agent GUI - Setting

Mục đích: Cấu hình cài đặt trên từng máy agent

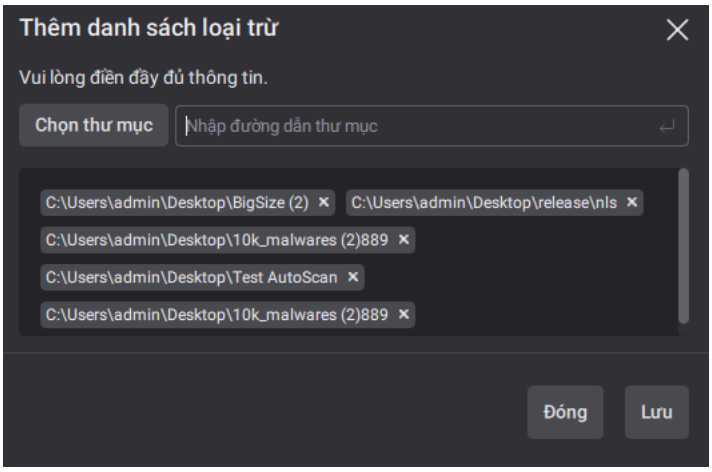
Cho phép tìm kiếm tất cả nội dung có trong trang setting theo từ khóa tìm kiếm



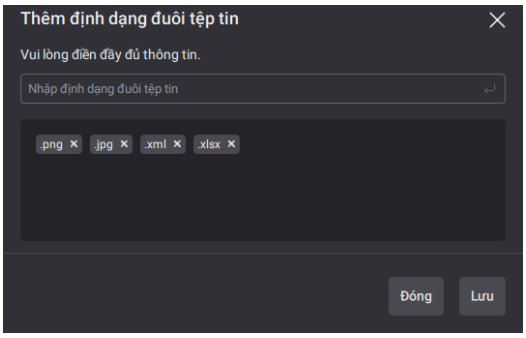
a. **Protection setting** (Cài đặt bảo vệ): Vì có 2 vị trí cấu hình Policy (Self defense và Real-time protection) trên Portal và dưới từng Agent.

- Self defense: Cho phép bật tắt Self defense. → Bảo vệ các tài nguyên của agent, tránh việc bị tác động trái phép từ các tác nhân bên ngoài -*Chưa update hoàn thiện*

- Real-time protection: Bảo vệ toàn diện cho máy tính, tự động phát hiện và diệt mã độc ngay khi chúng xuất hiện trên máy tính (Bật/Tắt thiết bị)
- Exclusion list: Cho phép lựa chọn folder được loại trừ (không bị quét bởi Real-time Protection); *Thêm mới/ Chỉnh sửa folder được loại trừ*

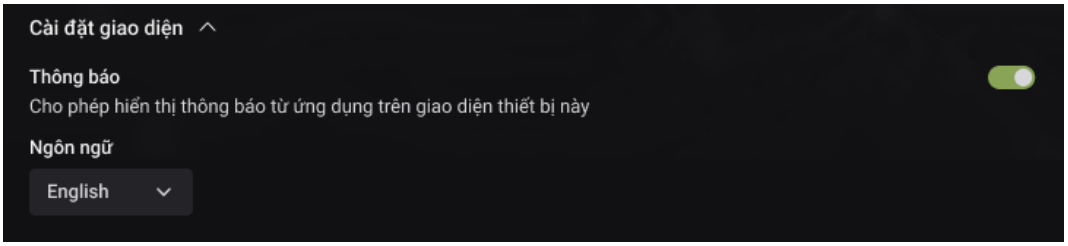


- Extension: Cho phép thêm mới/ chỉnh sửa vào Extension (Loại đuôi tài liệu) được loại trừ (không bị quét bởi Real-time Protection);



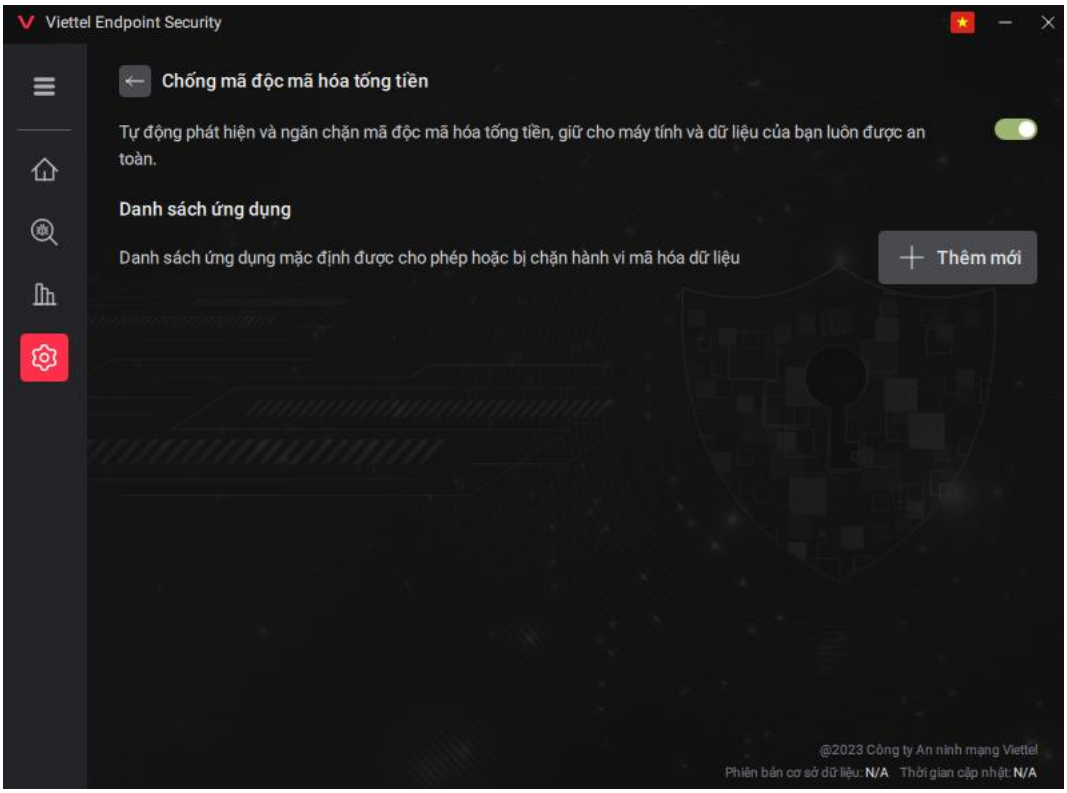
b. Interface setting (Cài đặt giao diện)

- Cho phép bật tắt Notification → Hiển thị thông báo trên màn hình thiết bị khi có lệnh scan từ hệ thống, khi phát hiện mã độc
- Langugage: Cho phép lựa chọn ngôn ngữ Tiếng anh/ Tiếng việt

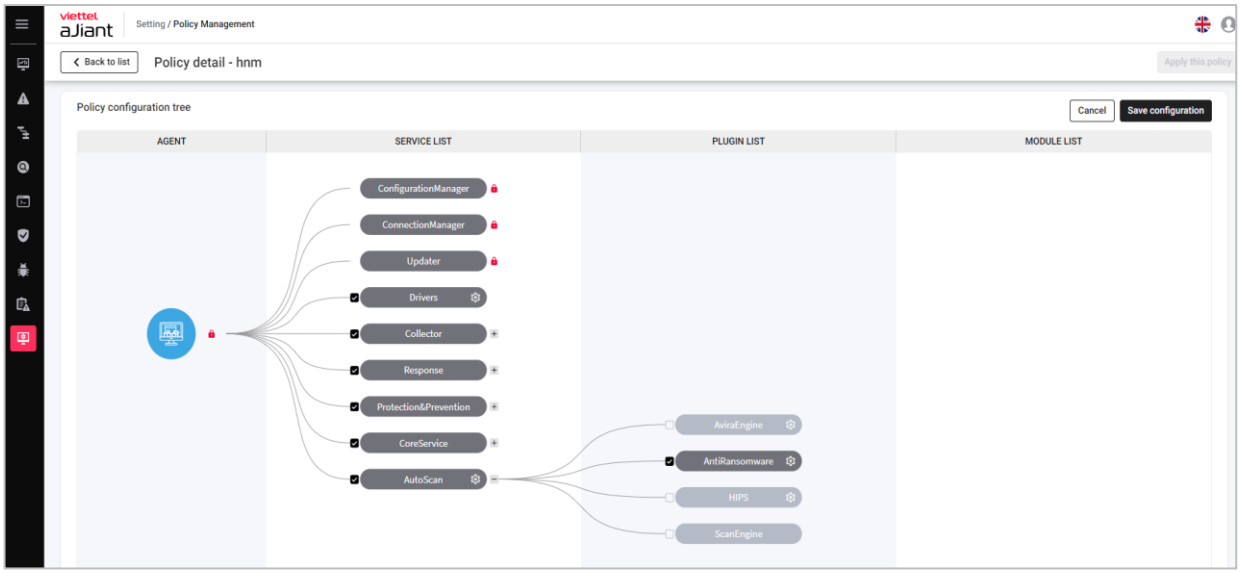


c. Anti-Ransomware (Chống mã độc mã hóa tống tiền)

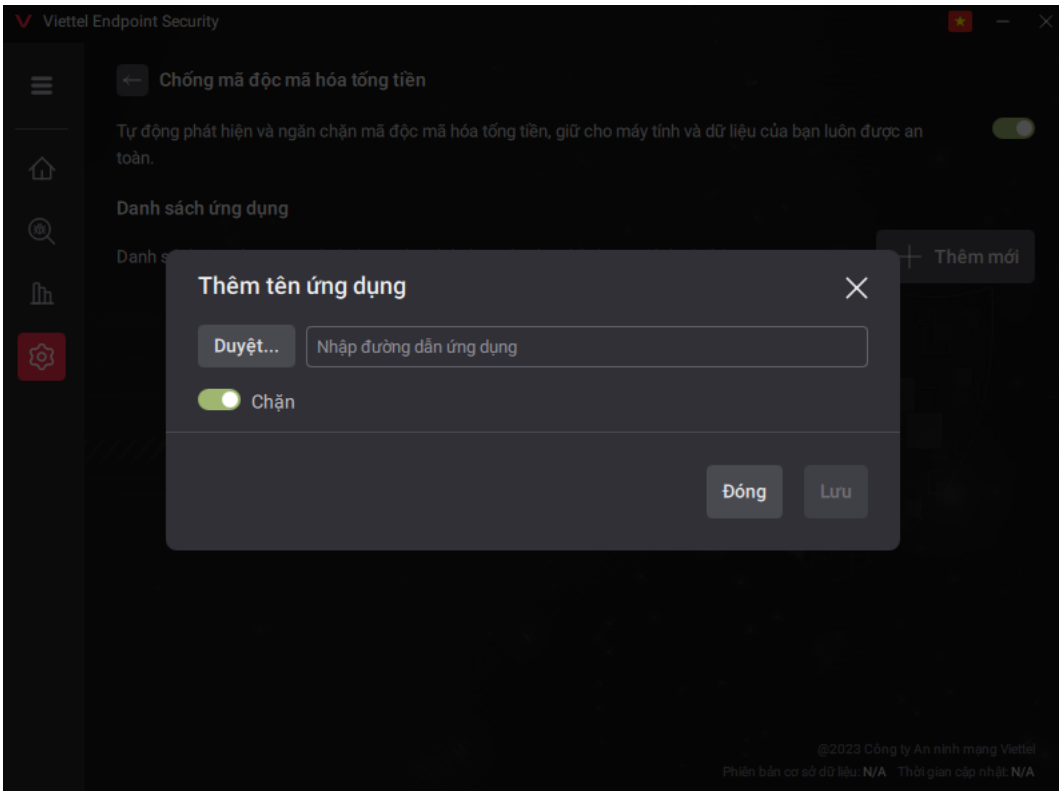
- Cho phép người dùng bật/tắt chế độ bảo vệ mã độc mã hóa tống tiền. Hệ thống sẽ tự động phát hiện và ngăn chặn mã độc mã hóa tống tiền cho máy tính.



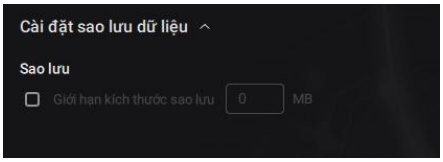
Lưu ý: Để sử dụng tính năng cần bật Policy AntiRansomware trên Portal



- Danh sách ứng dụng: Cho phép người dùng chọn ứng dụng mà các ứng dụng này có thể thực hiện các hành vi nghi ngờ là mã độc mã hóa dữ liệu



d. Backup setting (Cài đặt sao lưu): Hỗ trợ người dùng cấu hình thông tin lưu trữ file backups.



- Tích chọn hiện thị giới hạn kích thước sao lưu, đồng thời Cho phép nhập vào giới hạn size lưu trữ file backup

  (Cho phép cấu hình max 5120 MB→ Thông báo khi đạt ngưỡng 5G: The size of backup file have reached the limit! The system is going to delete the oldest files from Backup

  Để tránh vượt quá kích thước lưu trữ tối đa, sẽ tự động xóa các tập tin **cũ nhất** trong phần lưu trữ khi đạt đến kích thước lưu trữ tối đa)

3.16 Giao diện dòng lệnh của tính năng On-demand Scan

Command cho phép quản lý việc quét mã độc, xem báo cáo và các bản sao lưu mã độc đã phát hiện

Chạy command liệt kê các tính năng hỗ trợ.

Lưu ý: chuyển đến thư mục cài đặt agent */usr/local/bin/ajiant/autoscan* để sử dụng các lệnh của chương trình VESAutoScan

```
$ VESAutoScan -h
Usage: VESAutoScan <command>

Manage scan & protection service

Commands:
  scan                 Manage scan sessions
  |- start             Start a scan session
  |  |- <files> ...     File paths to scan
  |- stop              Stop a scan session
  |  |- <id>           Scan session id to stop
  |- show              Show a scan session details
  |  |- <id>           Scan session id to query
  |- list              List all running scan sessions

  report               Manage scan reports
  |- list              List all scan reports
  |  |- <type>          Type of report, available type are realtime, manual,
                       all
  |- show              Show a scan report details
  |  |- <id>           Report ID to show, id can be 'realtime' or report id
                       number
  |- search            Search for file in scan reports
  |  |- <str>          String to search, in file path

  backup               Manage backup files
  |- restore           Restore a backup file
  |  |- <id>           Id of file to restore
  |  |- <output-path>    Output path restore file
  |- list              List all backup files
  |- search            Search backup files
  |  |- <str>          String to search in file names

  show                 Show scan service information
  |- version           Show version
  |- database-version    Show database version

Flags:
  -h, --help    Show context-sensitive help.

Run "VESAutoScan <command> --help" for more information on a command.
```

3.16.1 Sub-command scan

Quản lý các scan session, cho phép người dùng tạo scan session thủ công, quản lý các scan session được tạo theo cách này

a. Bắt đầu 1 scan session

Người dùng chỉ định các vị trí cần quét mã độc, có thể chỉ định nhiều hơn 1 vị trí.

```
$ VESAutoScan scan start /home/ /usr/
path: /home
path: /usr
start scan success, id: 1
use command `VESAutoScan scan show 1` to show scan details.
```

b. Dừng 1 scan session

Người dùng chỉ định scan session cần dừng quét

```
$ VESAutoScan scan stop 1
stop success
```

c. Hiển thị trạng thái của 1 scan session

Người dùng chỉ định scan session cần hiển thị thông tin

```
$ VESAutoScan scan show 1
+----+---------+----------+--------------+------------------+-----------------+
| ID | STATUS  | PROGRESS | FILE SCANNED | MALWARE DETECTED | MALWARE CLEANED |
+----+---------+----------+--------------+------------------+-----------------+
|  1 | Stopped | 9.00%    |        30231 |                0 |               0 |
+----+---------+----------+--------------+------------------+-----------------+
```

d. Liệt kê các scan session đang chạy được tạo theo cách sử dụng dòng lệnh

Hiển thị các scan session đang quét và vị trí quét

```
$ VESAutoScan scan list
+---------+------------+
| SCAN ID | LOCATION   |
+---------+------------+
|       1 | /usr,/home |
+---------+------------+
```

3.16.2 Sub-command report

a. Liệt kê lịch sử quét và thông tin

Người dùng chỉ định loại báo cáo, có thể chỉ định “realtime” cho báo cáo về quét mã độc theo thời gian thực, “manual” cho báo cáo về các lần quét chủ động, hoặc “all” để hiển thị tất cả

```
$ VESAutoScan report list realtime
+-----------------------------+
| Realtime Scan Report        |
+-----------+-----------------+
| REPORT ID | MALWARE DETECTED |
+-----------+-----------------+
| realtime  |               2 |
+-----------+-----------------+
```

```
$ VESAutoScan report list manual
```

```
+-----------------------------------------------------------------------------------------------+
| Manual Scan Report                                                                            |
+-----------+--------------------------+-----------+-------+-------------+-----------------+----------+
| REPORT ID | TIMESTAMP                | LOCATION  | FILE | FILE SCANNED | MALWARE DETECTED | STATUS   |
+-----------+--------------------------+-----------+-------+-------------+-----------------+----------+
|         1 | 2025-07-10T17:46:32+07:00 | /usr,/home | 30231 | 312837      |               0 | Stopped  |
|         2 | 2025-07-10T17:53:01+07:00 | /usr,/home | 31795 | 312838      |               0 | Scanning |
+-----------+--------------------------+-----------+-------+-------------+-----------------+----------+
```

```
$ VESAutoScan report list all
+-----------------------------+
| Realtime Scan Report        |
+-----------+-----------------+
| REPORT ID | MALWARE DETECTED |
+-----------+-----------------+
| realtime  |               2 |
+-----------+-----------------+

+-----------------------------------------------------------------------------------------------+
| Manual Scan Report                                                                            |
+-----------+--------------------------+-----------+-------+-------------+-----------------+----------+
| REPORT ID | TIMESTAMP                | LOCATION  | FILE | FILE SCANNED | MALWARE DETECTED | STATUS   |
+-----------+--------------------------+-----------+-------+-------------+-----------------+----------+
|         1 | 2025-07-10T17:46:32+07:00 | /usr,/home | 30231 | 312837      |               0 | Stopped  |
|         2 | 2025-07-10T17:53:01+07:00 | /usr,/home | 56013 | 312838      |               0 | Scanning |
+-----------+--------------------------+-----------+-------+-------------+-----------------+----------+
```

b. Hiển thị thông tin chi tiết về 1 báo cáo

Người dùng chỉ định id của báo cáo cần hiển thị, có thể chỉ định “realtime” để hiển thị báo cáo chi tiết cho tính năng quét mã độc theo thời gian thực

```
$ VESAutoScan report show realtime
+---------------+------------------------+-------------+
| FILE PATH     | MALWARE NAME           | STATUS      |
+---------------+------------------------+-------------+
| /adware+virus | ADWARE/Patched.Ren.Gen | Deleted     |
+---------------+------------------------+-------------+
|               | TOTAL                  | 1           |
+---------------+------------------------+-------------+
```

```
$ VESAutoScan report show 3
+-----------+--------------------------+----------+------+-------------+-----------------+----------+
| REPORT ID | TIMESTAMP                | LOCATION | FILE | FILE SCANNED | MALWARE DETECTED | STATUS   |
+-----------+--------------------------+----------+------+-------------+-----------------+----------+
|         3 | 2025-07-10T18:13:19+07:00 | /home    | 496 | 153052      |               1 | Scanning |
+-----------+--------------------------+----------+------+-------------+-----------------+----------+
+--------------------+------------------------+-------------+
| FILE PATH          | MALWARE NAME           | STATUS      |
+--------------------+------------------------+-------------+
| /home/adware+virus | ADWARE/Patched.Ren.Gen | Deleted     |
+--------------------+------------------------+-------------+
|                    | TOTAL                  | 1           |
+--------------------+------------------------+-------------+
```

c. Tìm kiếm file hoặc mã độc đã từng phát hiện

Người dùng có thể chỉ định 1 phần đường dẫn đến file cần tìm

```
$ VESAutoScan report search home
+-------------------------------------------------------------+
| REPORT ID: 3                                                |
+--------------------+------------------------+-------------+
```

```
| FILE PATH         | MALWARE NAME          | STATUS     |
+-------------------+-----------------------+------------+
| /home/adware+virus | ADWARE/Patched.Ren.Gen | Deleted    |
+-------------------+-----------------------+------------+
|                   | TOTAL                 | 1          |
+-------------------+-----------------------+------------+
```

3.16.3 Sub-command backup

a. Liệt kê các file đã phát hiện và có thể khôi phục

```
$ VESAutoScan backup list
+---------+--------------------+
| FILE ID | FILE PATH          |
+---------+--------------------+
|       1 | /adware+virus      |
|       2 | /home/adware+virus |
+---------+--------------------+
|   TOTAL | 2                  |
+---------+--------------------+
```

b. Tìm kiếm file đã phát hiện và có thể khôi phục

Người dùng chỉ định 1 phần đường dẫn đến file cần tìm

```
$ VESAutoScan backup search home
+---------+--------------------+
| FILE ID | FILE PATH          |
+---------+--------------------+
|       2 | /home/adware+virus |
+---------+--------------------+
|   TOTAL | 1                  |
+---------+--------------------+
```

c. Khôi phục 1 file

Người dùng chỉ định id của file được sao lưu và tên file sau khi khôi phục, có thể chỉ định tên file là đường dẫn tuyệt đối hoặc tương đối

File sau khi khôi phục được nén dạng zip và đặt mật khẩu là “infected”

```
$ VESAutoScan backup restore 2 /home/linux/malware
restoring adware+virus to /home/linux/malware.zip
restore success to /home/linux/malware.zip with password: infected
```

3.16.4 Sub-command show

a. Hiển thị phiên bản của service quản lý quét mã độc

```
$ VESAutoScan show version
Version: 3.3.0.545.e8d14fe
Build: 2025-06-09T10:30:04+0000
```

b. Hiển thị phiên bản database

```
$ VESAutoScan show database-version
DatabaseVersion: 8.20.57.224
UpdateDate: 10/07/2025 17:55:30
```