



Viettel Endpoint Detection & Protection (VCS-aJiant)

Phiên bản 4.106 – Ngày cập nhật: 24/12/2024

Tài liệu Hướng dẫn sử dụng



Mục lục

1. GIỚI THIỆU	9
1.1 Thực trạng hiện nay	9
1.2 Sự phát triển của công nghệ	9
1.3 VCS-aJiant	9
1.4 Các thông tin nâng cấp	10
2. TỔNG QUAN.....	10
2.1 Công nghệ	10
2.2 Kiến trúc hạ tầng	11
2.3 Làm việc với giao diện quản trị	12
3. HƯỚNG DẪN SỬ DỤNG.....	12
A. Giao diện web Portal	12
3.1 Đăng nhập	12
3.2 Dashboard VCS-aJiant.....	13
3.2.1 Thao tác với dữ liệu	14
3.2.1.1 Xuất dữ liệu	14
3.2.1.2 Tìm kiếm theo ngày	14
3.2.1.3 Làm mới dữ liệu.....	15
3.2.2 Thống kê Overview	16
3.2.3 Theo dõi Security Operation.....	21
3.2.4 Theo dõi Agent Monitoring	23
3.2.5 Theo dõi Risk Detection	25
3.3 Quản lý Alert.....	27
3.3.1 Tìm kiếm Alert	29
3.3.2 Danh sách Alert.....	32
3.3.3 Gom nhóm Alert	35

3.3.4	Xem chi tiết Alert	36
3.3.5	Biểu đồ điều tra (Enhance Alert)	39
3.3.5.1	Khu vực hiển thị biểu đồ và các thao tác trên biểu đồ.....	40
3.3.5.2	Khu vực hiển thị thông tin chi tiết.....	47
3.3.6	Cập nhật trạng thái không nguy hiểm hoặc đóng cảnh báo cho 01/nhiều Alert hoặc nhóm Alert.....	49
3.3.7	Tạo IR flow từ 01/nhiều Alert hoặc nhóm Alert	50
3.3.8	Thêm 01/nhiều Alert hoặc nhóm Alert vào IR fLow đã có.....	52
3.4	Màn hình IRFLow	52
3.4.1	Danh sách hiển thị.....	52
3.4.2	Tìm kiếm IRFLow	53
3.4.3	Cách tạo IRFlow	55
3.4.4	Các bước thực hiện trong IRFlow	56
3.4.5	IRFLow – Detection.....	57
3.4.6	IRFlow – Containment.....	57
3.4.7	IRFLow – Investigation.....	59
3.4.7.1	Process Analysis	59
3.4.7.2	Event Search	65
3.4.8	IRFlow – Response	73
3.4.8.1	Live Response	73
3.4.8.2	Response Scenario	92
3.4.9	Close IRFLow	95
3.5	Màn hình Investigation	97
3.5.1	Investigation_Process Analysis.....	97
3.5.2	Investigation_Event Search.....	106
3.5.2.1	Tìm kiếm Event.....	106

3.5.2.2	Highlight.....	107
3.5.2.3	Need help	108
3.5.2.4	Wrap text	109
3.5.2.5	Export Data	110
3.5.3	Note	111
3.5.3.1	Xử lý Event	111
3.5.4	Investigation_Deploy Tools	114
3.5.4.1	Tool Management.....	114
3.5.4.2	Deploy tool.....	116
3.5.4.3	Task management	129
3.6	Màn hình Response	152
3.6.1	Response_Live Response	152
3.7	Màn hình Setting	171
3.7.1	Agent Management.....	171
3.7.2	Policy Setting.....	181
3.7.3	Group Management	191
3.7.4	Account Management	201
3.7.4.1	Permission management.....	202
3.7.4.2	Role Management	203
3.7.4.3	User management	209
3.7.5	Update management.....	216
3.7.5.1	Update groups	216
3.7.5.2	Update packages.....	220
3.8	Màn hình BLS.....	226
3.8.1	Thống kê vi phạm (Violation statistic).....	226
3.8.1.1	Màn hình Thống kê vi phạm	226

3.8.1.2	Tab Loại vi phạm	229
3.8.1.3	Tab Đơn vị	231
3.8.2	Thống kê phần mềm (Software statistic).....	232
3.9	Threat Hunting.....	235
3.9.1	Bật/tắt policy	235
3.9.2	Tìm kiếm theo agents/ nhóm.....	236
3.9.3	Tìm kiếm IOCs	236
3.9.3.1	Các loại IOCs hỗ trợ	236
3.9.4	Chi tiết kết quả tìm kiếm.....	238
3.9.4.1	Theo dõi trạng thái tìm kiếm	238
3.9.4.2	Chi tiết kết quả tìm kiếm	239
3.9.4.3	Dừng tìm kiếm	240
3.9.4.4	Xem chi tiết báo cáo tìm kiếm iocs dưới agents (View report) .	240
3.9.4.5	Export to Excel.....	241
3.9.4.6	Tải xuống kết quả tìm kiếm.....	242
3.9.5	Xem lịch sử truy vấn (View History)	242
3.9.5.1	Xem danh sách truy vấn	242
3.9.5.2	Xem chi tiết lịch sử truy vấn.....	243
3.10	Rules Correlation.....	244
3.10.1	Danh sách hiển thị.....	244
3.10.2	Thêm mới Rules Correlation	249
3.10.2.1	Sửa Rules Correlation	256
3.10.3	Xóa Rules Correlation	257
3.11	Protect & Prevention	258
3.11.1	Application Control	258
3.11.1.1	Hiển thị danh sách các ứng dụng/tiến trình bị chặn	258

3.11.1.2	Tìm kiếm ứng dụng/tiến trình bị chặn	259
3.11.1.3	Thêm mới ứng dụng/tiến trình bị chặn	259
3.11.1.4	Thêm mới ứng dụng/tiến trình từ tập tin có sẵn	259
3.11.1.5	Xóa ứng dụng/tiến trình bị chặn trong danh sách	260
3.11.1.6	Luồng cập nhật số lượng các máy agent đã cập nhật danh sách mới thành công	260
3.11.2	Endpoint Firewall	261
3.11.2.1	Hiển thị danh sách các kết nối bị chặn	261
3.11.2.2	Tìm kiếm các kết nối bị chặn	261
3.11.2.3	Thêm mới các kết nối bị chặn	262
3.11.2.4	Tạo bản sao chép từ điều kiện đã có	263
3.11.2.5	Thêm mới kết nối bị chặn từ tập tin có sẵn	264
3.11.2.6	Xóa kết nối bị chặn trong danh sách	264
3.11.2.7	Xuất dữ liệu các điều kiện	265
3.12	Anti – Malware	265
3.12.1	Scan Schedule	265
3.12.1.1	Tìm kiếm Scan Schedule task	265
3.12.1.2	Thêm mới Scan Schedule task	266
3.12.1.3	Nhập bản Schedule task	273
3.12.1.4	Xem chi tiết	274
3.12.1.5	Xóa Schedule task	275
3.12.1.6	Xem báo cáo	276
3.12.2	Device control	279
3.12.2.1	Tìm kiếm Group	280
3.12.2.2	Danh sách Device của từng group	282
3.12.2.3	Màn Exception	282

3.12.2.4	Màn Add Exception.....	284
B.	Giao diện Agent.....	293
3.13	Main.....	293
3.14	Protection	295
3.15	Report.....	298
3.16	Setting	301

Thuật ngữ

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

1. GIỚI THIỆU

1.1 Thực trạng hiện nay

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

1.2 Sự phát triển của công nghệ

Công nghệ của Giải pháp VCS-aJiant giúp bù đắp các thiếu sót của các công nghệ dựa trên chữ ký mà các tổ chức đang sử dụng như antivirus hay IPS/IDS để cung cấp khả năng phát hiện bất thường dựa trên hành vi và cho cái nhìn sâu hơn về các thông tin cụ thể có liên quan trên endpoint để phát hiện và giảm thiểu các mối đe dọa nâng cao.

1.3 VCS-aJiant

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

Ngoài ra, VCS-aJiant cũng bổ sung cho các công nghệ bảo mật hiện có như giải pháp quản lý sự kiện và thông tin bảo mật (SIEM), các công cụ giám định mạng (Network Forensics) và các thiết bị phòng chống mối đe dọa tiên tiến (Advanced

Threat Detection), đồng nghĩa là bổ sung vào danh mục các giải pháp phản ứng sự cố an toàn thông tin của tổ chức.

1.4 Các thông tin nâng cấp

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

Cải tiến tính năng Login, Process Analysis theo thiết kế giao diện mới, cải thiện trải nghiệm người dùng và bổ sung các thông tin process cần thiết hỗ trợ người dùng trong quá trình điều tra;

Cải thiện các vấn đề trong phiên bản cũ nhằm đảm bảo tính ổn định.

2. TỔNG QUAN

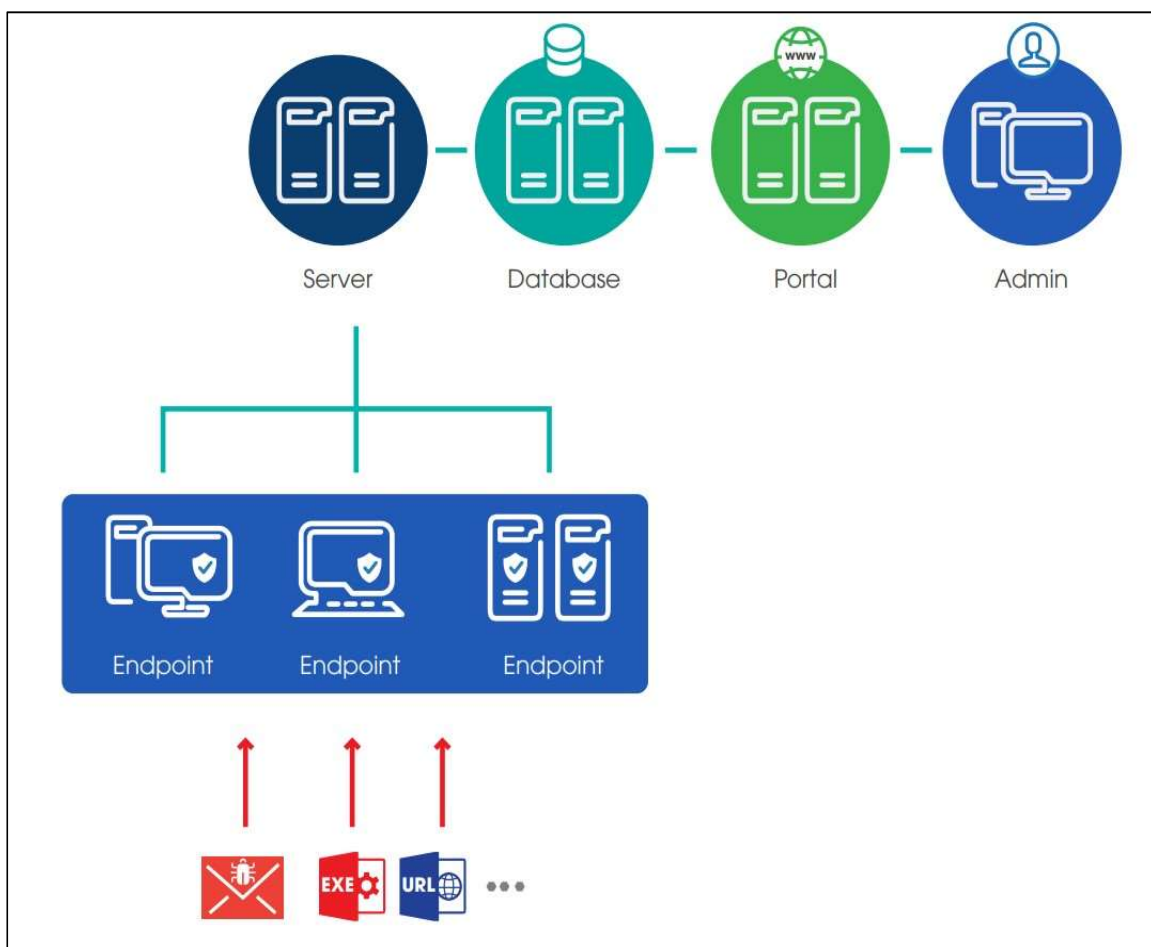
2.1 Công nghệ

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

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

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

2.2 Kiến trúc hạ tầng



Có 3 thành phần chính:

Agent: Là thành phần được cài đặt trên từng máy trạm, máy chủ, có nhiệm vụ giám sát các dấu hiệu bất thường trên các máy trạm, máy chủ, gửi log về máy chủ quản trị tập trung;

Cụm máy chủ quản trị, xử lý tập trung và lưu trữ: Là thành phần xử lý dữ liệu được gửi về từ các agent, đóng vai trò chính trong việc phân tích và xử lý dữ liệu theo thời gian thực;

Giao diện Web-Portal: Là thành phần mà người quản trị sẽ sử dụng để theo dõi, giám sát và phân tích các thông tin của hệ thống.

2.3 Làm việc với giao diện quản trị

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

Dashboard: thống kê, biểu đồ trực quan về tình hình an toàn thông tin của tổ chức;

Alert management: danh sách các alert về các dấu hiệu xuất hiện mã độc trên máy người dùng;

IR flow management: danh sách các IR flow được tạo bởi người quản trị trong quá trình điều tra. Luồng xử lý bao gồm: Detection, Containment, Investigation, Response;

Investigation: danh sách các công cụ phục vụ điều tra (Process Analysis, Event search và Deploy tools);

Response: danh sách các công cụ phục vụ phản ứng, xử lý sự cố (Live response);

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

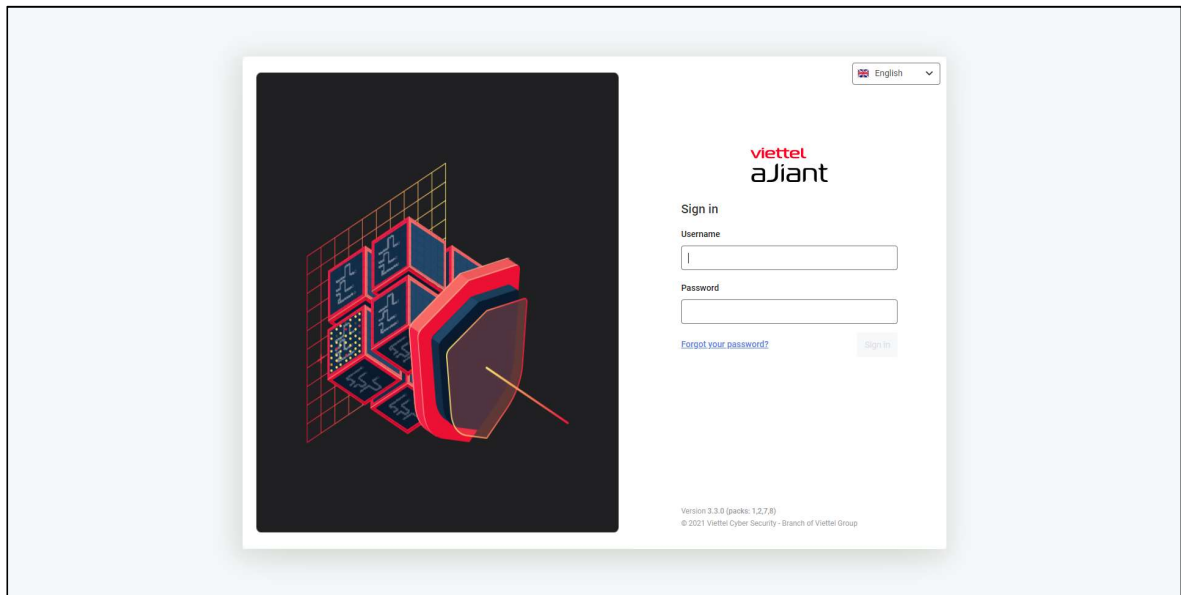
Setting: danh sách các chức năng cài đặt hệ thống (Policy management, Agent management, Group management, Rule correlation và Account management: User, Role, Permission management);

3. HƯỚNG DẪN SỬ DỤNG

A. Giao diện web Portal

3.1 Đăng nhập

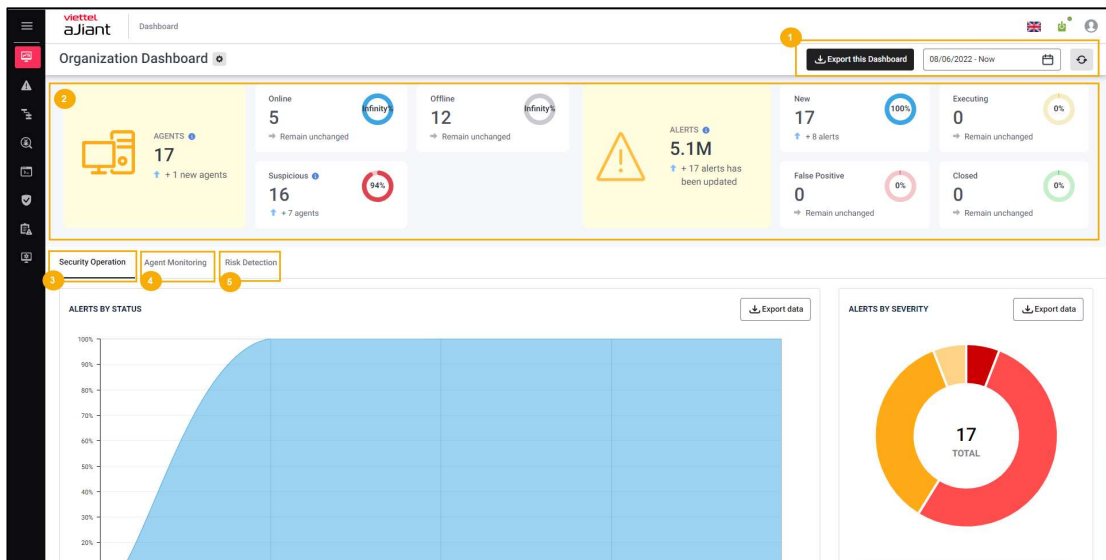
Bước 1: Truy cập vào hệ thống tại địa chỉ được cung cấp;



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

3.2 Dashboard VCS-aJiant

Các tính năng chính gồm có:



– Các thao tác với dữ liệu trên Dashboard:

- + Trích xuất dữ liệu trên dashboard;
- + Tìm kiếm dữ liệu tối đa 90 ngày gần đây;

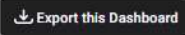
- + Làm mới dữ liệu.
 - Overview: Thống kê tổng quan tình hình an toàn thông tin tổ chức (thông qua trạng thái agents và Alerts);
 - Security Operation: Theo dõi tình hình vận hành an toàn thông tin (thông qua việc theo dõi vận hành Alert);
 - Agent Monitoring: Theo dõi tình hình cài đặt và trạng thái agents;
 - 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:

Absolute time range	Relative time range
From 08/06/2022  Apply time range	Last 90 days Last 60 days Last 30 days Last day

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

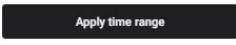
VD: Hiện tại là 03 giờ sáng ngày 07/06/2021, lựa chọn ngày bắt đầu = “06/06/2021”.

→ 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.

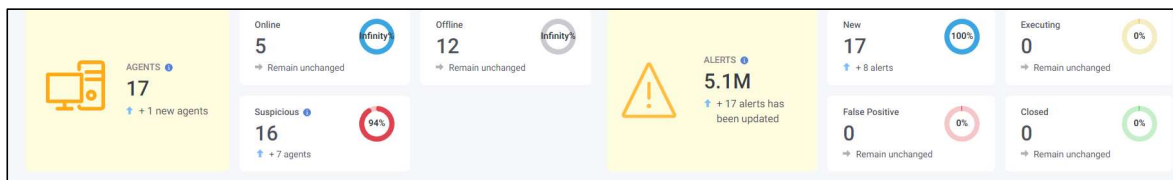
- + Sau khi chọn khoảng thời gian muốn theo dõi, chọn  để tải lại dữ liệu tương ứng.

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;

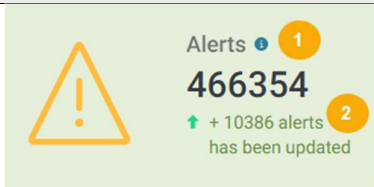
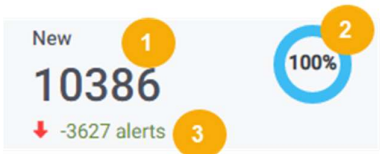


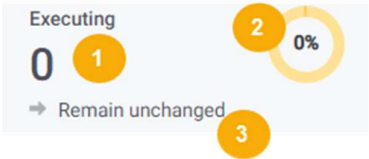
+ Thống kê liên quan đến agents:

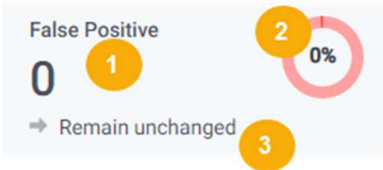
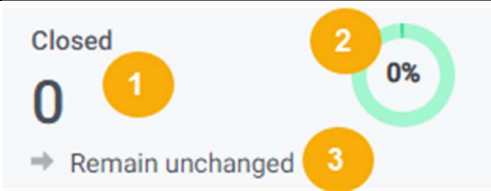
Số thống kê	Ý nghĩa
The card shows 17 agents with 1 new agent added. A yellow circle with the number 2 is next to the '+ 1 new agents' text.	Bao gồm 02 chỉ số: - Tổng số máy đã cài đặt agent trên hệ thống (không phụ thuộc khoảng thời gian tìm kiếm); - Tổng số máy mới cài đặt agent trong khoảng thời gian tìm kiếm; (+: Máy mới cài đặt, Remain unchanged: Không có máy mới cài đặt trong khoảng thời gian tìm kiếm)
The card shows 3274 online agents with 884 new agents added. A yellow circle with the number 1 is next to the 'Online' text, a yellow circle with the number 2 is next to the '3274' text, and a yellow circle with the number 3 is next to the '+ 884 agents' text. A blue circle with 53% is also present.	Bao gồm 03 chỉ số: - 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); - Tỷ lệ máy Online trung bình so với toàn hệ thống; - 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 – 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); – Tỷ lệ máy Offline trung bình so với toàn hệ thống; – 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: – 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; – Tỷ lệ máy có phát sinh Alert so với số lượng máy trên toàn hệ thống (không phụ thuộc thời gian tìm kiếm); – 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)

– Thông kê liên quan đến Alerts:

Số thống kê	Ý nghĩa
	Bao gồm 02 chỉ số: - Tổng số Alert trên toàn bộ hệ thống (không phụ thuộc khoảng thời gian tìm kiếm); - 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: - Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = NEW; - 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; - 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.

Số thống kê	Ý nghĩa
	(+: 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: – Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái $\diamond$ (NEW, FALSE POSITIVE, CLOSED); – Tỷ lệ Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái $\diamond$ (NEW, FALSE POSITIVE, CLOSED) so với toàn bộ Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm; – Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái $\diamond$ (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)

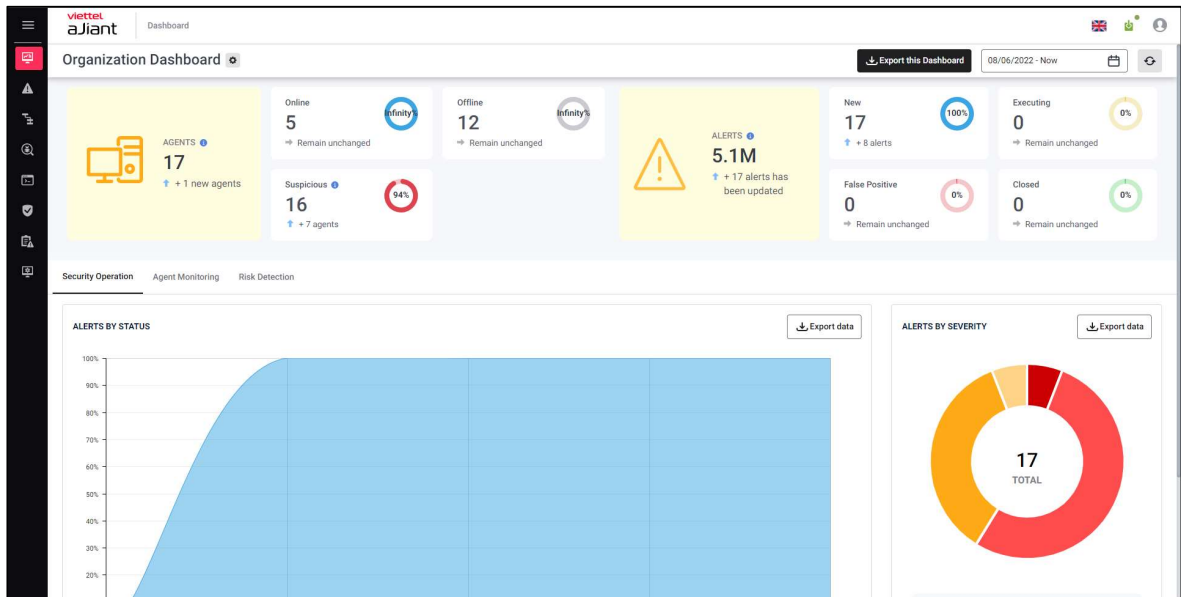
Số thống kê	Ý nghĩa
 False Positive 0 → Remain unchanged 2 0% 3	Bao gồm 03 chỉ số: - Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = CLOSED; - Tỷ lệ Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = CLOSED so với toàn bộ Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm; - 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)
 Closed 0 → Remain unchanged 2 0% 3	Bao gồm 03 chỉ số: - Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = FALSE POSITIVE; - Tỷ lệ Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = FALSE POSITIVE;

Số thống kê	Ý nghĩa
	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; 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;

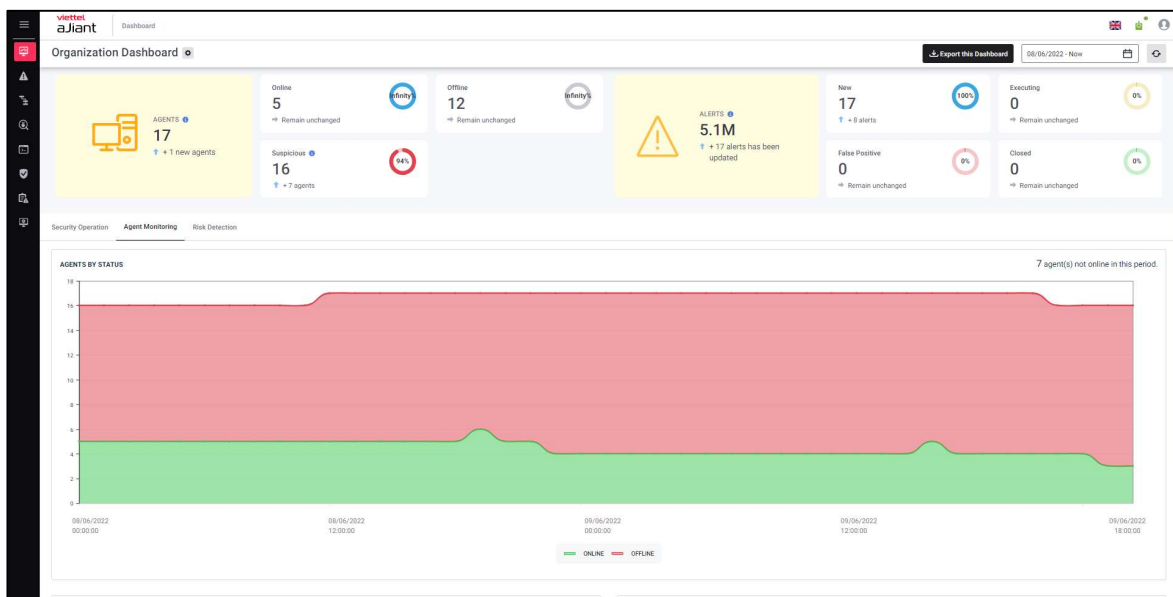


<i>Biểu đồ/thống kê</i>	<i>Ý nghĩa</i>
Alert by status	Biểu đồ miền - Theo dõi tình hình ghi nhận các Alert mới ghi nhận hoặc có cập nhật trong khoảng thời gian tìm kiếm, bao gồm: Trục x: thời gian; Trục y: Tỷ lệ Alert phân chia theo 04 nhóm trạng thái = (New, Executing, Closed, False Positive); Cho phép chọn  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  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 tuyến);
- Thống kê agent theo hệ điều hành, phiên bản hệ điều hành;
- Trích xuất dữ liệu thông tin agent;



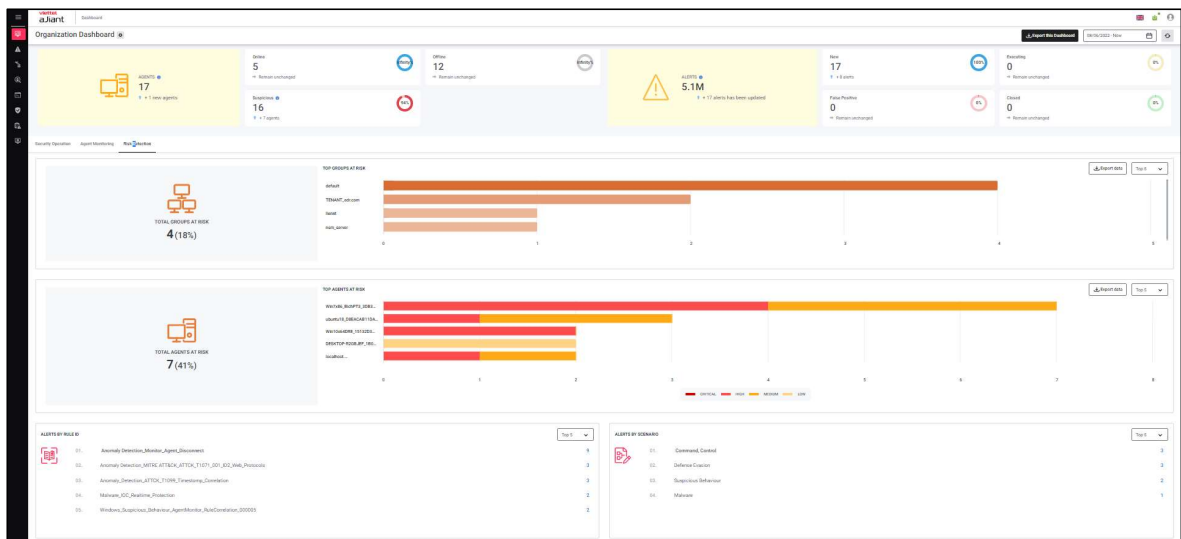
<i>Biểu đồ/thống kê</i>	<i>Ý nghĩa</i>
Agent by status	Biểu đồ miền- Theo dõi tình hình ghi nhận máy theo trạng thái (Online/Offline) trong chu kỳ báo cáo tính đến thời điểm hiện tại, bao gồm: Trục y: Tỷ lệ máy phân chia theo 02 nhóm status (Online, Offline); Trục x: thời gian thống kê; Hiển thị số lượng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

<i>Biểu đồ/thống kê</i>	<i>Ý nghĩa</i>
	Cho phép chọn  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 báo nhất;
- Trích xuất dữ liệu thông tin theo đối tượng nguy hại;

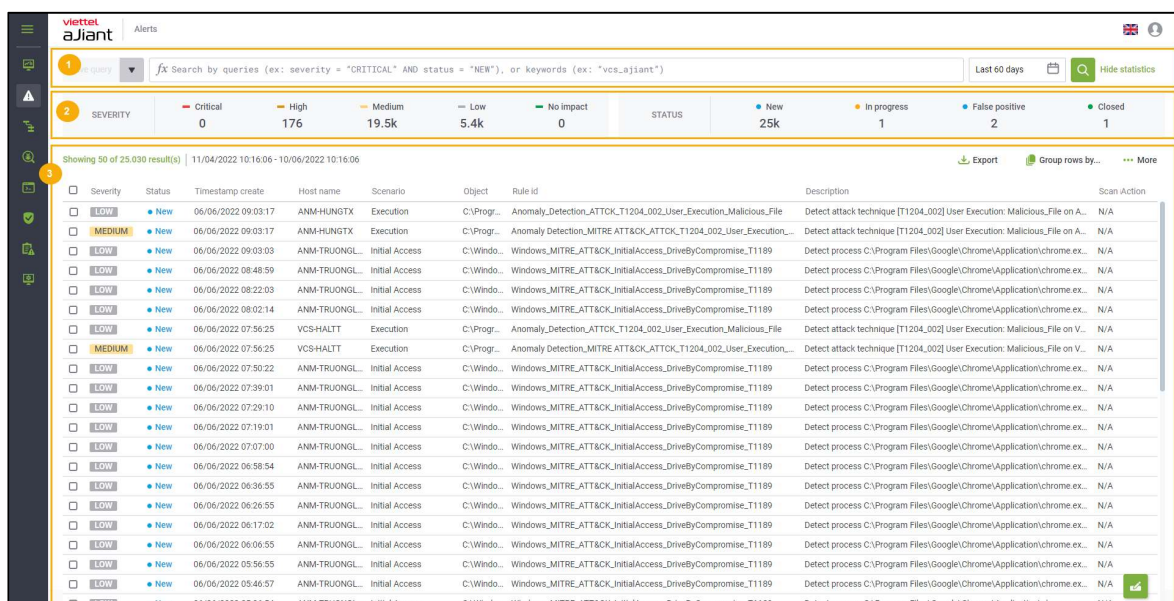


<i>Biểu đồ/thống kê</i>	<i>Ý nghĩa</i>
Total groups at risk	Tổng số nhóm có chứa máy tính phát sinh Alert mới ghi nhận hoặc có cập nhật (không kể Alert false positive và closed, không kể nhóm đã bị xóa) trong thời gian tìm kiếm; Tỷ lệ nhóm khả nghi so với toàn bộ nhóm trên hệ thống (không kể nhóm đã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

<i>Biểu đồ/thống kê</i>	<i>Ý nghĩa</i>
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:



Severity	Status	Timestamp create	Host name	Scenario	Object	Rule id	Description	Scan Action
LOW	New	06/06/2022 09:03:17	ANM-HUNGTX	Execution	C:\Progr...	Anomaly_Detection.ATTCK.T1204.002_User_Execution_Malicious_File	Detect attack technique [T1204.002] User Execution: Malicious_File on A...	N/A
MEDIUM	New	06/06/2022 09:03:17	ANM-HUNGTX	Execution	C:\Progr...	Anomaly_Detection.MITRE.ATT&CK.ATTCK.T1204.002_User_Execution...	Detect attack technique [T1204.002] User Execution: Malicious_File on A...	N/A
LOW	New	06/06/2022 09:03:03	ANM-TRUONGL...	Initial Access	C:\Windo...	Windows.MITRE.ATT&CK.InitialAccess_DriveByCompromise.T1189	Detect process C:\Program Files\Google\Chrome\Application\chrome.ex...	N/A
LOW	New	06/06/2022 08:48:59	ANM-TRUONGL...	Initial Access	C:\Windo...	Windows.MITRE.ATT&CK.InitialAccess_DriveByCompromise.T1189	Detect process C:\Program Files\Google\Chrome\Application\chrome.ex...	N/A
LOW	New	06/06/2022 08:22:03	ANM-TRUONGL...	Initial Access	C:\Windo...	Windows.MITRE.ATT&CK.InitialAccess_DriveByCompromise.T1189	Detect process C:\Program Files\Google\Chrome\Application\chrome.ex...	N/A
LOW	New	06/06/2022 08:02:14	ANM-TRUONGL...	Initial Access	C:\Windo...	Windows.MITRE.ATT&CK.InitialAccess_DriveByCompromise.T1189	Detect process C:\Program Files\Google\Chrome\Application\chrome.ex...	N/A
LOW	New	06/06/2022 07:56:25	VCS-HALTT	Execution	C:\Progr...	Anomaly_Detection.ATTCK.T1204.002_User_Execution_Malicious_File	Detect attack technique [T1204.002] User Execution: Malicious_File on V...	N/A
MEDIUM	New	06/06/2022 07:56:25	VCS-HALTT	Execution	C:\Progr...	Anomaly_Detection.MITRE.ATT&CK.ATTCK.T1204.002_User_Execution...	Detect attack technique [T1204.002] User Execution: Malicious_File on V...	N/A
LOW	New	06/06/2022 07:50:22	ANM-TRUONGL...	Initial Access	C:\Windo...	Windows.MITRE.ATT&CK.InitialAccess_DriveByCompromise.T1189	Detect process C:\Program Files\Google\Chrome\Application\chrome.ex...	N/A
LOW	New	06/06/2022 07:39:01	ANM-TRUONGL...	Initial Access	C:\Windo...	Windows.MITRE.ATT&CK.InitialAccess_DriveByCompromise.T1189	Detect process C:\Program Files\Google\Chrome\Application\chrome.ex...	N/A
LOW	New	06/06/2022 07:29:10	ANM-TRUONGL...	Initial Access	C:\Windo...	Windows.MITRE.ATT&CK.InitialAccess_DriveByCompromise.T1189	Detect process C:\Program Files\Google\Chrome\Application\chrome.ex...	N/A
LOW	New	06/06/2022 07:19:01	ANM-TRUONGL...	Initial Access	C:\Windo...	Windows.MITRE.ATT&CK.InitialAccess_DriveByCompromise.T1189	Detect process C:\Program Files\Google\Chrome\Application\chrome.ex...	N/A
LOW	New	06/06/2022 07:07:00	ANM-TRUONGL...	Initial Access	C:\Windo...	Windows.MITRE.ATT&CK.InitialAccess_DriveByCompromise.T1189	Detect process C:\Program Files\Google\Chrome\Application\chrome.ex...	N/A
LOW	New	06/06/2022 06:58:54	ANM-TRUONGL...	Initial Access	C:\Windo...	Windows.MITRE.ATT&CK.InitialAccess_DriveByCompromise.T1189	Detect process C:\Program Files\Google\Chrome\Application\chrome.ex...	N/A
LOW	New	06/06/2022 06:36:55	ANM-TRUONGL...	Initial Access	C:\Windo...	Windows.MITRE.ATT&CK.InitialAccess_DriveByCompromise.T1189	Detect process C:\Program Files\Google\Chrome\Application\chrome.ex...	N/A
LOW	New	06/06/2022 06:26:55	ANM-TRUONGL...	Initial Access	C:\Windo...	Windows.MITRE.ATT&CK.InitialAccess_DriveByCompromise.T1189	Detect process C:\Program Files\Google\Chrome\Application\chrome.ex...	N/A
LOW	New	06/06/2022 06:17:02	ANM-TRUONGL...	Initial Access	C:\Windo...	Windows.MITRE.ATT&CK.InitialAccess_DriveByCompromise.T1189	Detect process C:\Program Files\Google\Chrome\Application\chrome.ex...	N/A
LOW	New	06/06/2022 06:06:55	ANM-TRUONGL...	Initial Access	C:\Windo...	Windows.MITRE.ATT&CK.InitialAccess_DriveByCompromise.T1189	Detect process C:\Program Files\Google\Chrome\Application\chrome.ex...	N/A
LOW	New	06/06/2022 05:56:55	ANM-TRUONGL...	Initial Access	C:\Windo...	Windows.MITRE.ATT&CK.InitialAccess_DriveByCompromise.T1189	Detect process C:\Program Files\Google\Chrome\Application\chrome.ex...	N/A
LOW	New	06/06/2022 05:46:57	ANM-TRUONGL...	Initial Access	C:\Windo...	Windows.MITRE.ATT&CK.InitialAccess_DriveByCompromise.T1189	Detect process C:\Program Files\Google\Chrome\Application\chrome.ex...	N/A

- 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.
 - Tìm kiếm nhanh;
 - 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;
- + Tạo IR flow từ 01/nhiều Alert;
- + Thêm 01/nhiều Alert vào IR flow;

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.

– 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.

– 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;

– **Tìm kiếm theo câu query**



- + Sử dụng câu query đã lưu trước đó để tìm kiếm;
- + Nhập câu query để tìm kiếm;

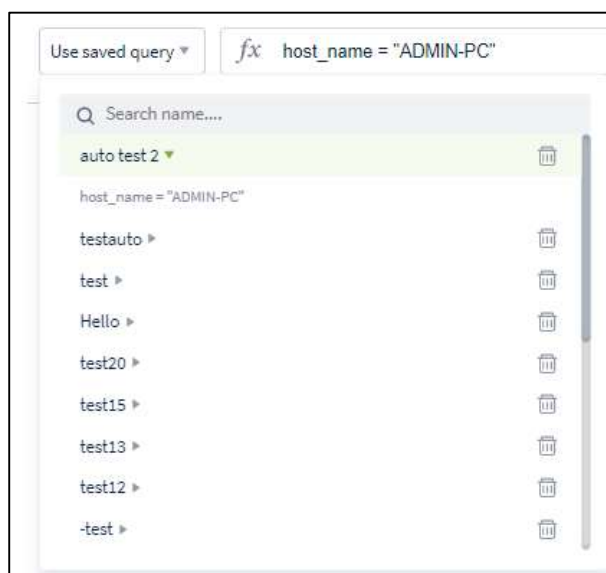
(*) Sử dụng câu query đã lưu trước đó để tìm kiếm

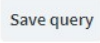
Bước 1: Chọn query đã lưu trước đó tại combobox Use saved query ▾;

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  để lưu lại.

Lưu ý: nút  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
- ir_flow_name: tên IR flow mà Alert thuộc IR flow đó
- 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

Save query

fx alert_id ~ "20220609"

Last 24 hours

Hide statistics

SEVERITY

Critical0

High2

Medium0

Low0

No impact0

STATUS

New2

In progress0

False positive0

Closed0

Showing 2 of 2 result(s) | 09/06/2022 09:06:27 - 10/06/2022 09:06:27

Export

Group rows by...

More

☐	Host name	Severity	Alert id	Status	Agent id	Timestamp create	Target commandline	Hash sha1	Description	Action
☐	ubuntu18	HIGH	20220609_173832_553078267_618098...	New	500	09/06/2022 17:38:31	N/A	N/A	Computer ubu	
☐	localhost.localdo...	HIGH	20220609_113824_267803984_564214...	New	500	09/06/2022 11:38:23	N/A	N/A	Computer loci	

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

Selected

☒ Target commandline
 ☒ Hash sha1

☒ Alert id
 ☒ Host name

☒ Agent id
 ☒ Timestamp create

☒ Severity
 ☒ Status

☒ Description
 ☒ Ajiant event id

Others

☐ File hash sha1
 ☐ Scan result

☐ Malware type
 ☐ Malware name

☐ Classify
 ☐ Assignee

☐ Ir flow name
 ☐ Target process path md5

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:

SEVERITY

Critical

0

High

2

Medium

0

Low

0

No impact

0

STATUS

New

2

In progress

0

False positive

0

Closed

0

Showing 2 of 2 result(s) | 09/06/2022 09:06:27 - 10/06/2022 09:06:27

Export

Group rows by...

More

☐	Host name	Severity	Alert id	Status	Ajiant event id	Agent id	Timestamp create	Target commandline	Hash sha1	Description	Action
☐	ubuntu18	HIGH	20220609_173832_553078267_618098...	New	500	D8EACAB11DA9FA3F0F65575E9EC313DC61A89B	09/06/2022 17:38:31	N/A	N/A	Computer ubu	
☐	localhost.localdo...	HIGH	20220609_113824_267803584_564214...	New	500	31F6FA372944D72C2DC854E155A63170CE9686AD	09/06/2022 11:38:23	N/A	N/A	Computer loci	

1. Chọn cột (trường thông tin muốn thay đổi vị trí)

2. Kéo thả tới 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  và chọn “Add to IR Flow” để đưa Alert vào IR flow, xem trường hợp đưa 01 Alert vào IR flow đã tồn tại trong [3.3.8 Thêm 01/nhiều Alert hoặc nhóm Alert vào IR fLow đã có](#) hoặc vào IR flow mới trong [3.3.6 Tạo IR flow từ 01/nhiều Alert hoặc nhóm Alert](#)
- + 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:

SEVERITY					STATUS				
Critical	High	Medium	Low	No impact	New	In progress	False positive	Closed	
0	2	0	0	0	2	0	0	0	

Showing 2 of 2 result(s) | 09/06/2022 09:06:27 - 10/06/2022 09:06:27

Selected 2 alert(s)  Update status  Add to IRFlow  Export data  Clear selection

Host name	Severity	Agent id	Status	Ajant event id	Alert id	Timestamp create	Target commandline	Hash sha1	Description	Action
☒ ubuntu18	HIGH	D8EACAB11DA9F0A3F0F65575E9E9C313DC61A83B	New	500	20220609_173832_553078267_61809	09/06/2022 17:38:31	N/A	N/A	Computer ubu	
☒ localhost.localdo main	HIGH	31F6FA372944D72C2DC854E155A63170CE9686AD	New	500	20220609_113824_267803584_56421	09/06/2022 11:38:23	N/A	N/A	Computer loca	

Bước 2: Chọn  Add to IRFlow để thêm Alert vừa chọn vào IR flow để xử lý.

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”, Hệ thống ẩn đi các thao tác  Update status  Add to IRFlow  Export data  Clear selection . Chi tiết xem trong trường hợp đưa 01 Alert vào IR flow mới trong [3.3.6 Tạo IR flow từ 01/nhiều Alert hoặc nhóm Alert](#) hoặc thêm vào IR flow đã tồn tại trong [3.3.7 Thêm 01/nhiều Alert hoặc nhóm Alert vào IR fLow đã có](#)

- + Chọn  Update status để cập nhật trạng thái của Alert:



Update status to:

False Positive

Comment

Write something...

Cancel Update status

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

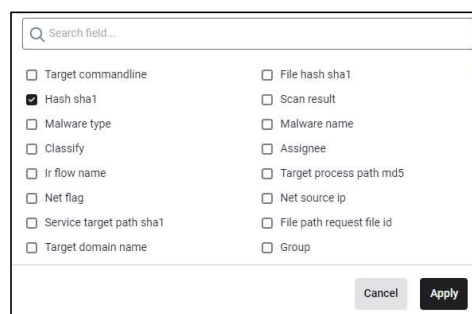
Lưu ý: Thao tác này chỉ áp dụng khi toàn bộ Alert được chọn đều ở trạng thái = “NEW”, nếu có ít nhất một Alert đang ở trạng thái khác “NEW”, thao tác sẽ bị ẩn đi. Chi tiết xem trong trường hợp đánh dấu không nguy hiểm 01 Alert trong [3.3.5 Đánh dấu không nguy hiểm cho 01/nhiều Alert hoặc nhóm Alert](#)

+ Chọn  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;



Search field...

☐ Target commandline	☐ File hash sha1
☒ Hash sha1	☐ Scan result
☐ Malware type	☐ Malware name
☐ Classify	☐ Assignee
☐ Ir flow name	☐ Target process path md5
☐ Net flag	☐ Net source ip
☐ Service target path sha1	☐ File path request file id
☐ Target domain name	☐ Group

Cancel Apply

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

Bước 2: Chọn **Apply** để áp dụng.

Những Alert có cùng các tiêu chí đã chọn và có cùng trạng thái và đang ở cùng IR flow (nếu có) sẽ được gom lại 1 dòng trong danh sách kết quả.

Showing 7 group(s) of 390 result(s) | 11/05/2022 09:53:31 - 10/06/2022 09:53:31

Change fields for grouping... Ungroup *** More

Fields	Number of alerts	Action
target_commandline: N/A ajant_event_id: N/A	189	
target_commandline: N/A ajant_event_id: 3	7	
target_commandline: N/A ajant_event_id: 11	155	
target_commandline: N/A ajant_event_id: 13	2	
target_commandline: N/A ajant_event_id: 23	1	
target_commandline: N/A ajant_event_id: 400	1	
target_commandline: N/A ajant_event_id: 500	35	

Trong đó:

- + Các trường được sử dụng làm tiêu chí gom nhóm sẽ được bôi đậm;
- + Hiện 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”;

Search field...

Selected

☐ Target commandline ☐ Ajant event id

Others

☐ File hash sha1 ☐ Hash sha1

☐ Scan result ☐ Malware type

☐ Malware name ☐ Classify

☐ Assignee ☐ Ir flow name

☐ Target process path md5 ☐ Net flag

☐ Net source ip ☐ Service target path sha1

Cancel 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;

– Nhóm thông tin chung của Alert, trong đó:

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

– Nhóm các thao tác với Alert

- + Chọn  để đưa Alert vào IR flow, xem trường hợp đưa 01 Alert vào IR flow đã tồn tại trong [3.3.7 Thêm 01/nhiều Alert hoặc nhóm Alert vào IR fLow đã có](#) hoặc vào IR flow mới trong [3.3.6 Tạo IR flow từ 01/nhiều Alert hoặc nhóm Alert](#)
- + Chọn  để cập nhật trạng thái của Alert:

Update status to:

False Positive

Comment

Write something...

Cancel

Update status

- 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;

Closed

 khaitb update status into **Closed**
22/04/2022 18:07:01

In progress

 khaitb added the alert into the IR Flow **IRF_Demo**
22/04/2022 17:48:52

New

 VCS-aJiant created the alert.
22/04/2022 17:35:48

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

The screenshot displays the 'Detail' view of an alert in the Viettel Cyber Security system. It is divided into two main sections: 'Description' (labeled 1) and 'Source event logs' (labeled 2).

Description (1): This section provides a detailed account of the detected attack technique, T1562.004: Disable or Modify System Firewall on ANM-PHUCVD2. It specifies the process path as C:\program files\delld\supportassistent\bin\supportassistent.exe (PID = 7656) and the commandline as 'C:\Program Files\Delld\SupportAssistAgent\bin\SupportAssistAgent.exe'. It notes that this process is creating a child process with path C:\windows\system32\netsh.exe (commandline = 'netsh.exe' http delete sslcert ipport=0.0.0.0:5700, PID = 9732) to disable the firewall. The Rule ID is identified as Anomaly_Detection_ATTCK_T1562_004_Disg...

Source event logs (2): This section provides additional context about the alert, categorized into File, Process, Host, and Others.

- File:** This file is impacted (created/modified/deleted/executed) suspiciously. Target process path: Signed C:\windows\system32\netsh.exe. Source process path: Unknown C:\program files\delld\supportassistent\bin\supportassistent.exe.
- Process:** This source/target process has suspicious behaviours. Target process path: Signed C:\windows\system32\netsh.exe. Source commandline: Unknown 'C:\Program Files\Delld\SupportAssistAgent\bin\SupportAssistAgent.exe'. Target commandline: Unknown 'netsh.exe' http delete sslcert ipport=0.0.0.0:5700. Source process path: Unknown C:\program files\delld\supportassistent\bin\supportassistent.exe.
- Host:** This information is about suspicious host. Client id: 9C4C8D5F62C98BE5918732E0D8D91DCD01121CD2. Ip dcn: 10.61.188.2. MAC Address: a8:6b:ad:71:14:2b, 1a:6b:ad:71:14:2b, 00:50:56:c0:00:01, 00:50:56:c0:00:08, 48:4d:7e:ba:be:53.
- Others:** These other information provides more context about this alert collected by VCS-aJant.

- 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.

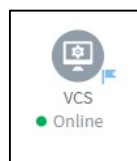


- Khu vực hiển thị biểu đồ và các thao tác trên biểu đồ
- Khu vực hiển thị thông tin chi tiết các đối tượng trên biểu đồ

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:



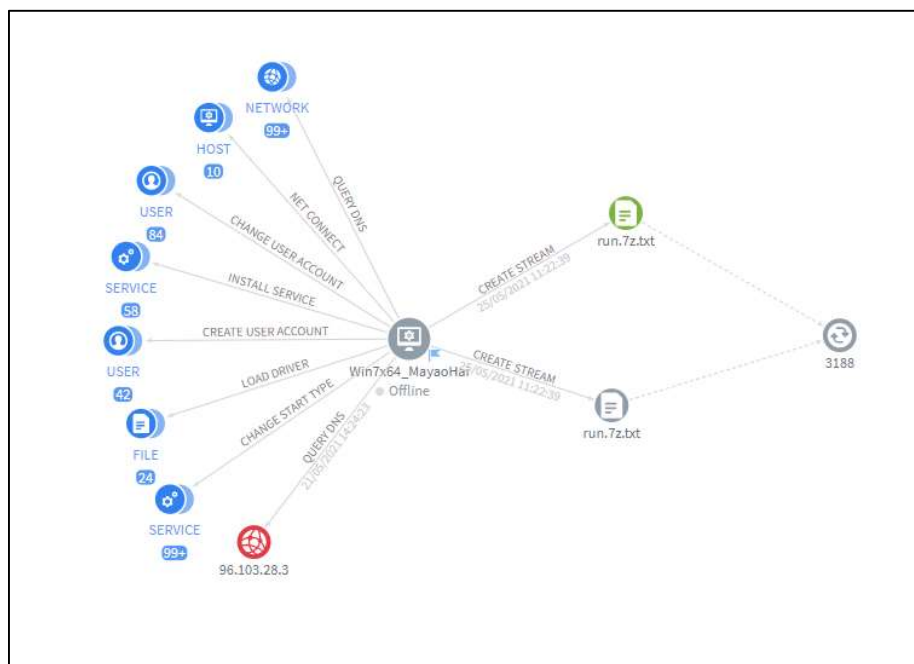
Mỗi đối tượng bao gồm các trạng thái như sau:

Unknown Clean Suspicious Malicious

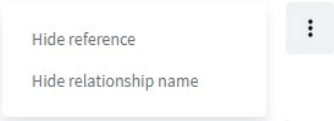
Giữa các đối tượng, hiển thị mối quan hệ bao gồm:

- + 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 liền 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:

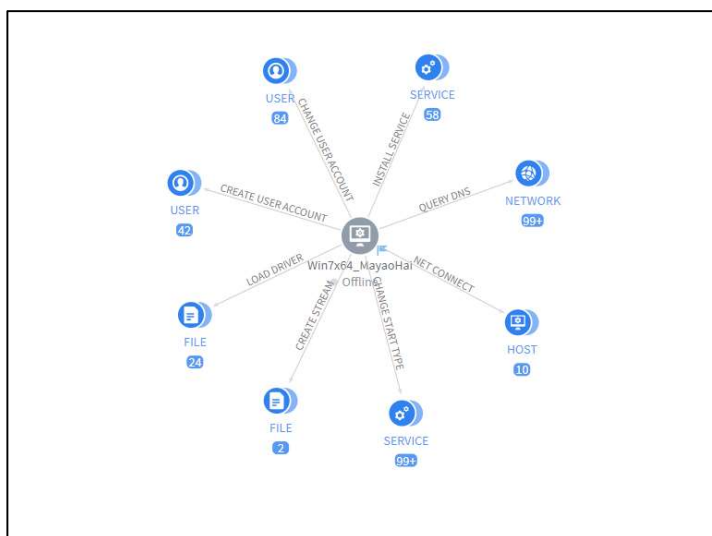


Các thao tác hỗ trợ hiển thị biểu đồ bao gồm:

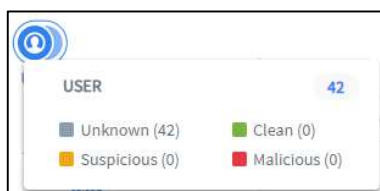
Thao tác hỗ trợ hiển thị	Ý nghĩa
	Cho phép ẩn/hiện các thông tin trên biểu đồ: + Reference: Khi chọn, cho phép ẩn/hiện thông tin tham chiếu bao gồm mũi tên nét đứt và đối tượng tham chiếu tại tất cả các đối tượng hiện có trên biểu đồ; + Relationship name: Khi chọn, cho phép ẩn/hiện thông tin tên mối 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

Thao tác hỗ trợ hiển thị	Ý nghĩa
	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:

Objects in this group network

Search object...

Unknown (48) Clean (125) Malicious (87)

Selected 1/20 node(s) Show on graph Clear selection

STATUS	DOMAIN ADDRESS	IP	LOCAL PORT	PROCESS NAME	ACTION
Clean	ocsp.verisign.com	240.100.28.3	N/A	SYSTEM	
Clean	cr14.digicert.com	80.105.28.3	N/A	SYSTEM	
Clean	cr14.microsoft.com	16.87.28.3	N/A	SYSTEM	
Malicious	www.microsoft.com	96.103.28.3	N/A	SYSTEM	
Clean	ocsp.digicert.com	240.94.28.3	N/A	SYSTEM	
Clean	cr14.verisign.com	224.91.28.3	N/A	SYSTEM	
Malicious	www.msftncsl.com	0.96.28.3	N/A	SYSTEM	
Clean	csc3-2010-cr14.verisign.com	112.89.28.3	N/A	SYSTEM	
Clean	ocsp.globalsign.com	48.88.28.3	N/A	SYSTEM	
Clean	cr14.digicert.com	80.105.28.3	N/A	SYSTEM	

Showing 20/260 result(s)

- + Cho phép lọc các đối tượng trong nhóm theo trạng thái Unknown Clean Suspicious Malicious hoặc tìm kiếm nhanh bằng cách 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 Show on graph 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:

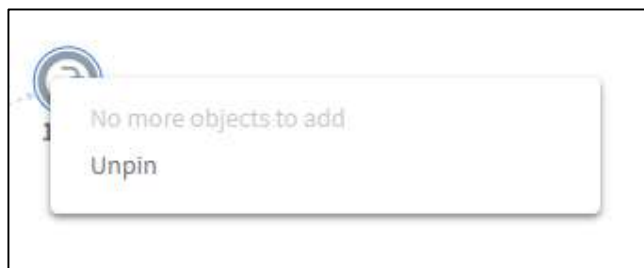
- + Tại máy gốc/máy tính thường: Hỗ trợ thu gọn các đối tượng về trạng thái mặc định khi hiển thị máy (Chỉ bao gồm các đối tượng có quan hệ trực tiếp với máy, mỗi loại đối tượng nếu nhiều hơn 01 đối tượng, hiển thị dạng nhóm) bằng cách chọn chuột phải tại đối tượng, sau đó chọn “Group child-level objects”;



- + 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”;



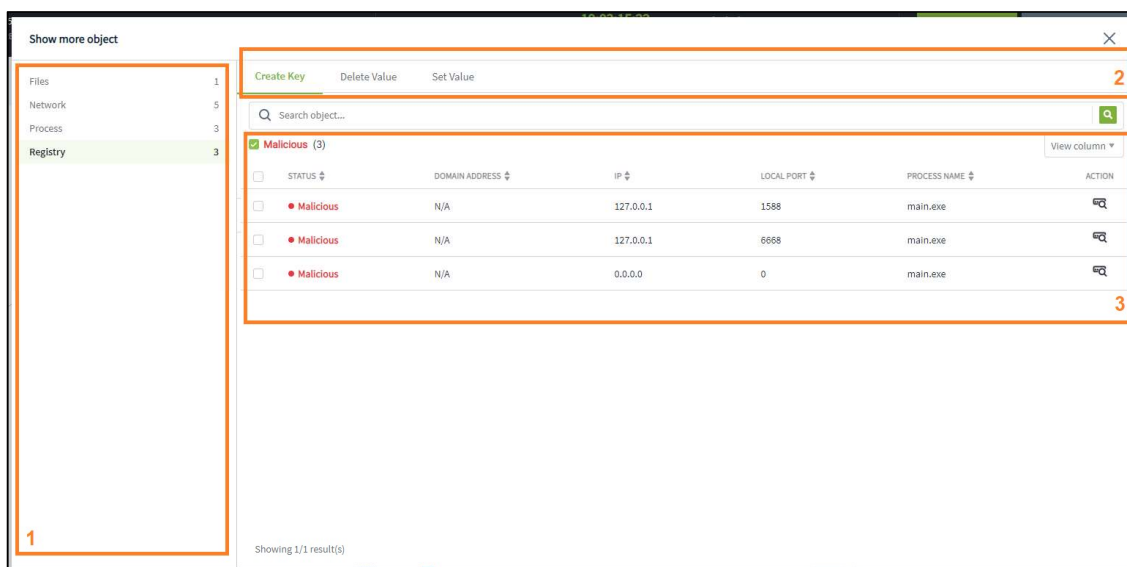
- + Tại đối tượng là tiến trình (process) cho phép mở rộng để điều tra loang bằng cách chọn chuột phải tại đối tượng,
- + Trường hợp không thể tiếp tục loang, hiển thị:



- + Trường hợp có thể loang, chọn “Add more objects...”



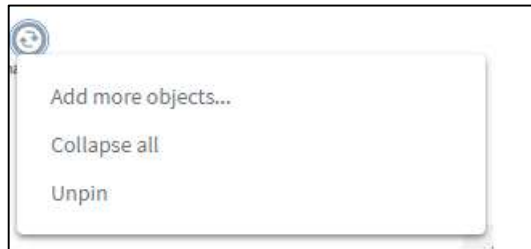
Hiện thị giao diện cho phép chọn đối tượng muốn loang đến



- Chọn loại đối tượng;
- Chọn loại quan hệ từ tiến trình tới đối tượng;
- 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 Show on graph 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);

Host detail

General

HOST NAME	Win7x64_MayaoHai	3 Copy
HOST ID	fe2a4ba0-b348-4a43-bd26-79995feb57e9	
STATUS	Offline	
SET UP VERSION	N/A	
GROUP	default	
UPDATE GROUP	release	
POLICY	full_features	
IP DCN	10.61.188.2	
OS	windows	
FIRST PING	12/05/2021 16:02:02	
LAST PING	26/05/2021 14:23:17	

Platform

CPUs

Network Interfaces

Default Gateway

- 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;
- 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.

Process detail		✕
General		
PROCESS ID	1432	
PROCESS NAME	main.exe	
MD5	1e092a44d44c29ef8d6bfc3a74f34b73	
SHA256	1941d3f261033344b22c5e9cf246e5683c17d450ac87d0af6f3ed7a52f431bb6	
PROCESS PATH	C:\users\admin\desktop\taodataoang\main.exe	
FILE COMPANY	N/A	
FILE DESCRIPTION	N/A	
FILE VERSION	N/A	
FILE PRODUCT	N/A	
USER NAME	admin	
COMMANDLINE	.\main.exe	
INTEGRITY LEVEL	HIGH	

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  **Update status** để cập nhật trạng thái của Alert:

Update status to:

False Positive

Comment

Add to False Positive

Cancel

Update status

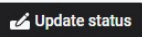
Bước 3: Chọn Update Status to “False Positive”;

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  Update status để cập nhật trạng thái của Alert:

Update status to:

Closed

Comment

done

Cancel

Update status

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;

3.3.7 Tạo IR flow từ 01/nhiều Alert hoặc nhóm Alert

Bước 1: Lựa chọn 01/nhiều Alert để tạo IRFlow và chọn “Add to IR Flow”;

Showing 4 of 4 result(s) | 09/06/2022 11:50:00 - 10/06/2022 11:50:00

Selected 2 alert(s)  Update status  Add to IRFlow  Export data  Clear selection

Severity	Status	Timestamp create	Host name	Scenario	Object	Rule id	Description	Action
 LOW	New	10/06/2022 07:34:15	DESKTOP-R2GBJE...	Suspicious Behavio...	C:\Windo...	Windows_Suspicious_Behaviour_AgentMonitor_RuleCorrelation_000005	Detect process [C:\Windows\System32\svchost.exe] (PID: [1094]) i	
 LOW	New	09/06/2022 18:09:26	DESKTOP-R2GBJE...	Suspicious Behavio...	C:\Windo...	Windows_Suspicious_Behaviour_AgentMonitor_RuleCorrelation_000005	Detect process [C:\Windows\System32\svchost.exe] (PID: [1094]) i	
 HIGH	New	09/06/2022 17:38:31	ubuntu18	N/A	N/A	Anomaly Detection_Monitor_Agent_Disconnect	Computer ubuntu18 was disconnected at least 30 days	
 LOW	New	09/06/2022 15:05:02	DESKTOP-R2GBJE...	Suspicious Behavio...	C:\Windo...	Windows_Suspicious_Behaviour_AgentMonitor_RuleCorrelation_000005	Detect process [C:\Windows\System32\svchost.exe] (PID: [1094]) i	

Bước 2: Nhập các thông tin và tạo IRFlow:

New IR Flow

IR Flow name

new_critical_IRFlow

Assignee(s)

root

×

+

▼

Note (optional)

Write something...

List of alerts

Alert ID	Host name	Action
20220606_18134_278220796_546256		
20220606_18153_440049062_394732		

Cancel

Add to IR Flow

Dữ liệu hiển thị trong Combobox Assigned to bao gồm:

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

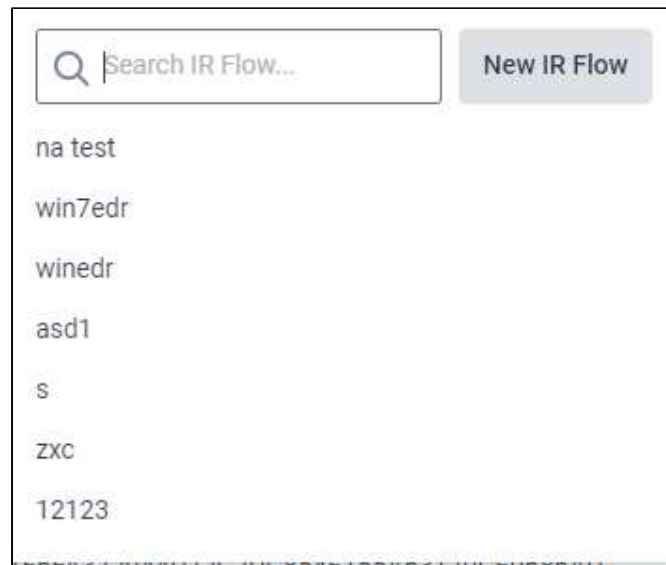
Bước 3: Sau khi thêm 1 hoặc nhiều Alert vào luồng xử lý IR flow, có thể hoàn tác trong 10s:

- + Để hoàn tác: chọn “Cancel” trong 10 s;

- + Để tạo ngay IR flow và chuyển sang màn hình IR flow chọn tên IR flow vừa tạo: chọn “Add to IR Flow”;

3.3.8 Thêm 01/nhiều Alert hoặc nhóm Alert vào IR fLow đã có

Tương tự như 3.3.5 nhưng không chọn “Add new IRFlow” mà chọn IR flow đã có từ danh sách chọn;



Hệ thống hiển thị popup Xác nhận thao tác thêm 1 hoặc nhiều Alerts vào luồng xử lý IRFlow có sẵn trong hệ thống:



3.4 Màn hình IRFlow

3.4.1 Danh sách hiển thị

Mục đích: Cho phép hiển thị danh sách IRFlow trong hệ thống theo phân quyền người dùng:

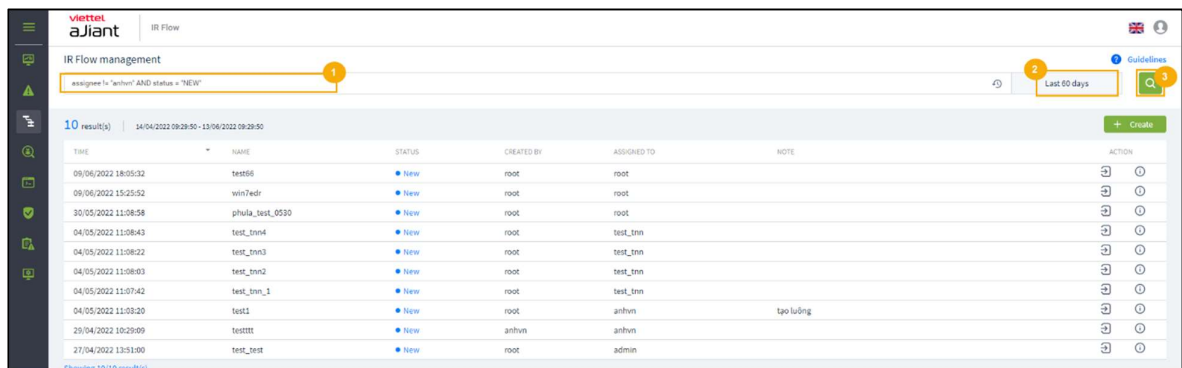
- + User đăng nhập thuộc group root: Hiển thị tất cả IRFlow trong hệ thống;

- + User đăng nhập thuộc group default: Hiển thị tất cả IRFlow được assign cho user đang login;
- + User đăng nhập thuộc group cha: Hiển thị tất cả IRFlow được assign cho user đang login và các user thuộc group con tương ứng;
- + User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tất cả IRFlow được assign cho user đang login;

3.4.2 Tìm kiếm IRFlow

Mục đích: Cho phép tìm kiếm được những bản ghi IRFlow theo phân quyền người dùng đăng nhập;

Tương tự chức năng tìm kiếm ở màn hình Alert, màn hình IRFlow hỗ trợ tìm kiếm theo query như sau:



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:
 - assignee: người được phân công xử lý Alert;
 - created_by: tài khoản tạo IRFlow;

- name: Tên của IRFlow;
- notation: lưu ý của IRFlow;
- status: trạng thái của IRFlow;

+ <toán_tử> là các giá trị sau:

- = : 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: Chọn khoảng thời gian tìm kiếm bằng cách click vào nút “Date & Time” và chọn khoảng thời gian tùy ý. Nếu không chọn mặc định là Last 7 days;

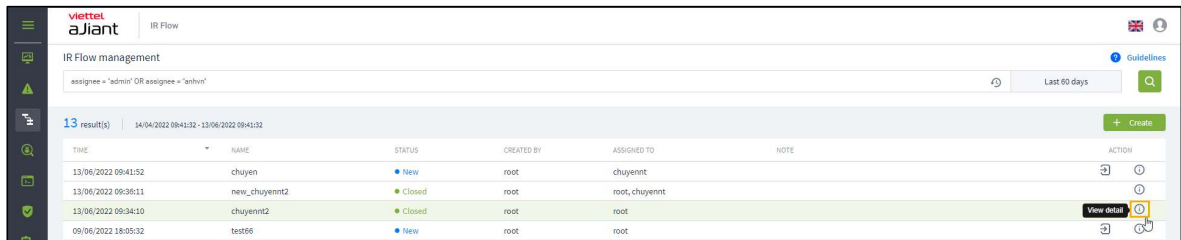
Bước 3: Click on “Search”

Ngoài ra hỗ trợ tìm kiếm theo lịch sử tìm kiếm

The screenshot shows the 'IR Flow management' section of the Viettel aJiant interface. A search bar is at the top with a dropdown menu showing three search queries. Below the search bar is a table with columns for time, name, status, and actions. The table displays 12 results. On the right side, there is a 'Guidelines' button and a 'Last 60 days' filter.

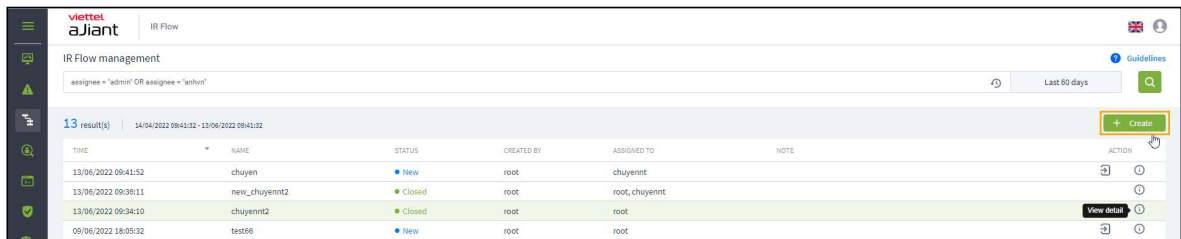
Time	Name	Status	Actions
09/06/2022 18:05:52	test06	New	root
09/06/2022 15:25:52	winTedr	New	root
30/05/2022 11:08:58	phula_test_0530	New	root
04/05/2022 11:08:43	test_tnn4	New	test_tnn
04/05/2022 11:08:22	test_tnn3	New	test_tnn
04/05/2022 11:08:03	test_tnn2	New	test_tnn
04/05/2022 11:07:42	test_tnn_1	New	test_tnn
04/05/2022 11:03:20	test1	New	anhvn
29/04/2022 10:28:09	testttt	New	anhvn
27/04/2022 13:51:00	test_test	New	admin

Để vào xem thông tin chi tiết 1 IRFlow và thực hiện các hành động điều tra, xử lý người dùng chọn “IRFlow Detail”:



3.4.3 Cách tạo IRFlow

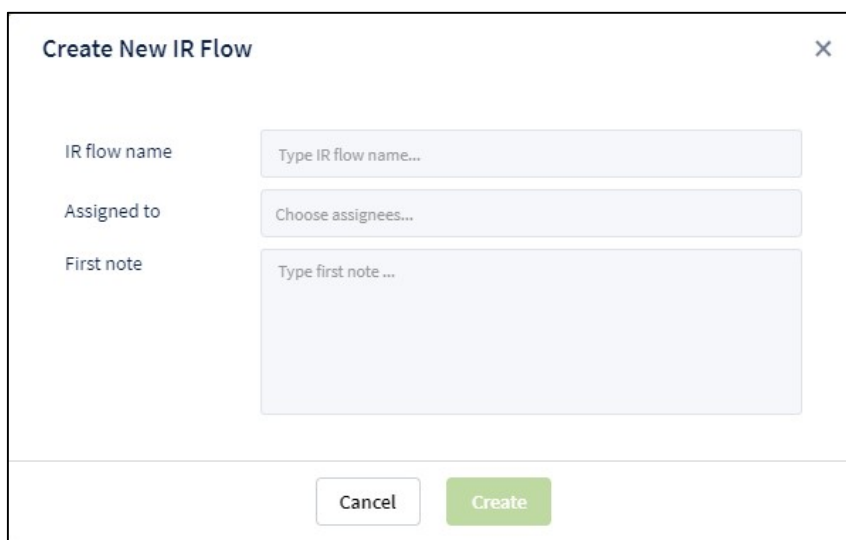
Bước 1: Click vào “Create”;



Bước 2: Hệ thống hiển thị Popup form Create New IRFlow, nhập thông tin hợp lệ;

Dữ liệu hiển thị trong Combobox Assigned to:

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



Create New IR Flow [X]

IR flow name:

Assigned to:

First note:

Bước 3:

- + Người dùng chọn nút “Create”, Hệ thống ghi nhận IRFlow vừa tạo và hiển thị trên màn hình danh sách IRFlow;
- + Người dùng chọn nút “Cancel”, Hệ thống hủy thao tác thêm mới IRFlow vừa tạo và quay về màn hình danh sách IRFlow;

3.4.4 Các bước thực hiện trong IRFlow

Sau khi tạo IRFlow từ các Alert hoặc đưa các Alert vào IRFlow, người vận hành sẽ vào trang IRFlow để thực hiện các hành động sau:

- + Xem các thông tin để điều tra: danh sách Alert, máy tính có Alert, các đối tượng liên quan (file/registry/process);
- + Cô lập các máy phát sinh Alert: cô lập mạng, cô lập tiến trình;
- + Điều tra và phát hiện các đối tượng liên quan đến Alert (artifacts);
- + Phản ứng: xử lý các kết quả đã điều tra. Ví dụ: kill tiến trình mã độc, xóa file mã độc, xóa các registry do mã độc sinh ra ...
- + Kết thúc điều tra: đóng IRFlow, dừng cô lập máy, đóng các phiên ProcessAnalysis và LiveResponse;

3.4.5 IRFlow – Detection

Mục đích: Tab Detection cho phép hiển thị các đối tượng liên quan đến Alert như:

- + Danh sách máy tính có Alert;
- + Danh sách Alert;
- + Danh sách artifacts được phát hiện trong quá trình điều tra (investigation);

Detection				
Original detection				
Agent				
DESKTOP-HHN2B1Q				
Alert				
TIME	GROUP	HOSTNAME	SCENARIO	SEVERITY
07:00:00 14/01/2019	no_group	DESKTOP-HHN2B1Q	Execution	High
07:00:00 14/01/2019	no_group	DESKTOP-HHN2B1Q	Execution	High
07:00:00 14/01/2019	no_group	DESKTOP-HHN2B1Q	Initial Access	High
Additional detection				
Artifacts				
TIME	AGENT ID	OBJECT	FROM	REFERENCE
07:25:05 14/01/2019	9D76E75C81645C6B88E18B46961C5D75C8154752	c:\Users\Test\Desktop\demo.exe	WIN_EVENT_LOG	plq3SWg8Ty9idpUvVJ-d
07:25:05 14/01/2019	9D76E75C81645C6B88E18B46961C5D75C8154752	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\demo	WIN_EVENT_LOG	plq3SWg8Ty9idpUvVJ-d

Các đối tượng thuộc phần “Original Detection”: là các Alert (Alert) và máy tính (Agent) ban đầu khi IRFlow được tạo;

Còn các đối tượng thuộc phần “Additional Detection”: là các Alert, máy tính, artifacts được thêm vào ở bước điều tra (Investigation);

Ý nghĩa một số trường trên màn hình detection:

- + Time: thời gian thêm agent/artifact vào màn hình detection;
- + Object: đường dẫn file/registry của artifact;
- + From: nguồn phát sinh artifact (Event log hoặc Process Analysis);
- + Reference: ID của event log hoặc ID của phiên kết nối Process Analysis;

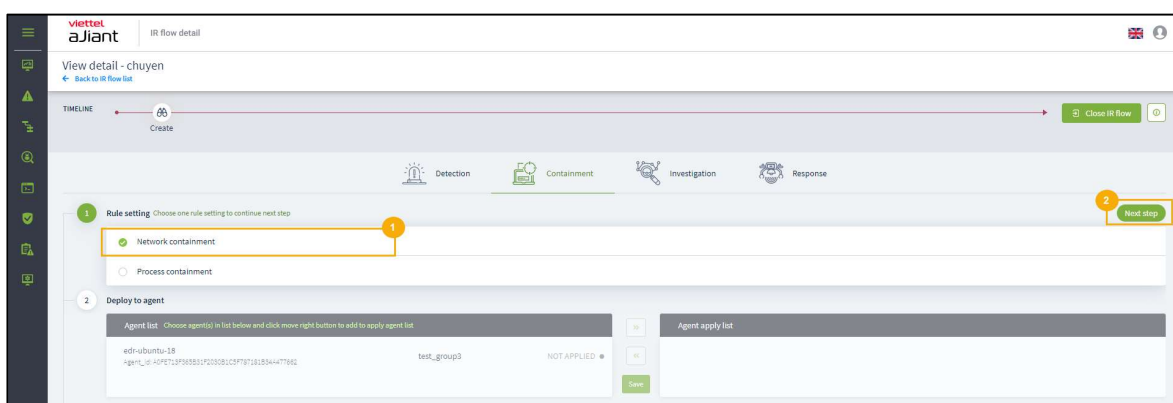
3.4.6 IRFlow – Containment

Mục đích: Tab Containment cho phép thực hiện cô lập 1 hay nhiều máy tính có trong tab Detection hoặc Suspend tiến trình thuộc Alert nằm trong IRFlow;

Các trạng thái của Containment:

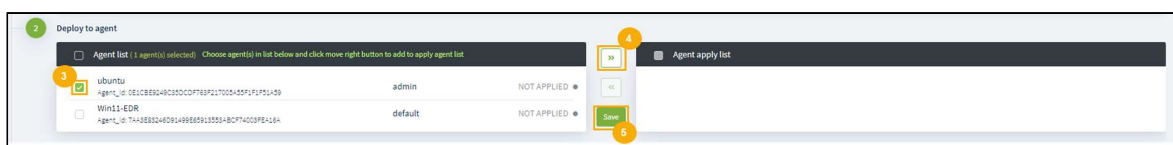
- + NOT APPLIED: chưa gửi lệnh xuống Agent;
- + APPLYING: đang gửi lệnh xuống agent;
- + APPLIED: đã gửi lệnh cô lập thành công;
- + STOPPING: đang gửi lệnh dừng cô lập;
- + STOPPED: đã gửi lệnh dừng cô lập thành công;

Bước 1: lựa chọn hình thức điều tra: cô lập mạng hoặc suspend tiến trình sau đó chọn “Next Step”;

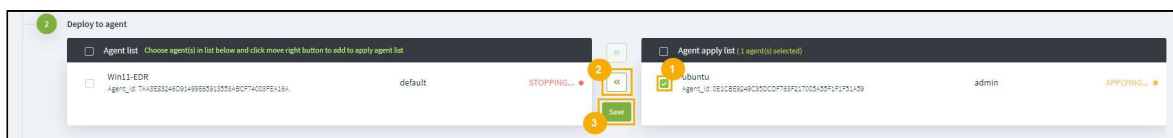


Lưu ý: sau khi nhập Path/PID thì phải ấn Enter để lưu lại cấu hình. Có thể suspend cùng lúc nhiều tiến trình.

Bước 1: chọn danh sách Agent cần cô lập và chọn “Start” để bắt đầu cô lập:



Bước 2: Để dừng việc cô lập click “Stop” hoặc chọn agent ở “Agent apply list” và chuyển về danh sách “Agent list”;



Trong trường hợp người quản trị không chủ động dừng việc cô lập trên Portal thì sau thời gian mặc định (24h) thì Agent cũng tự động gỡ cô lập dưới Agent.

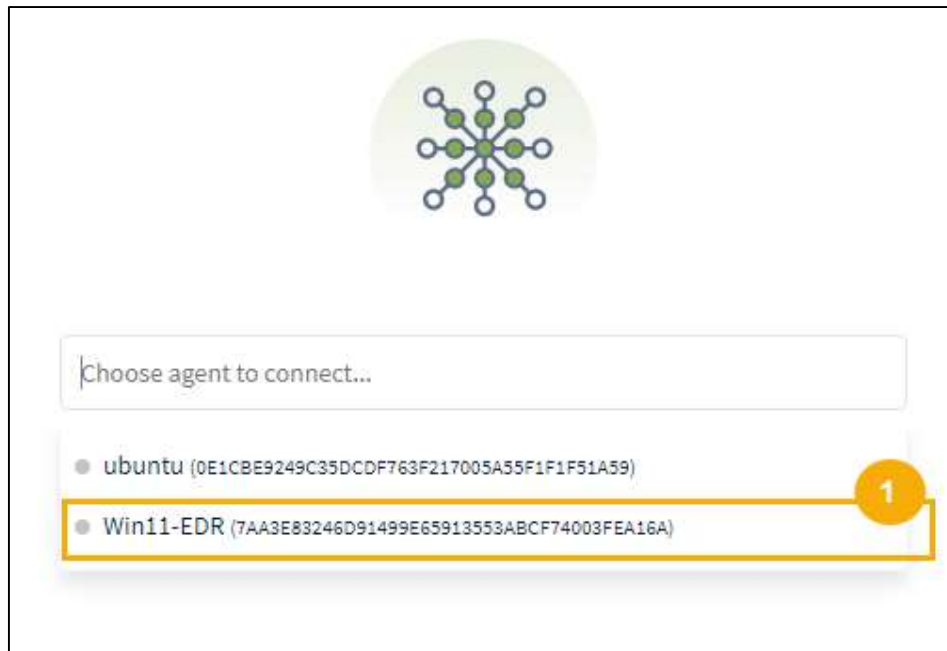
3.4.7 IRFLow – Investigation

3.4.7.1 Process Analysis

a. Xem thông tin process

Mục đích: là quá trình phân tích các tiến trình trên máy người dung có trong tab Detection theo thời gian thực nhằm tìm kiếm các dấu hiệu bất thường;

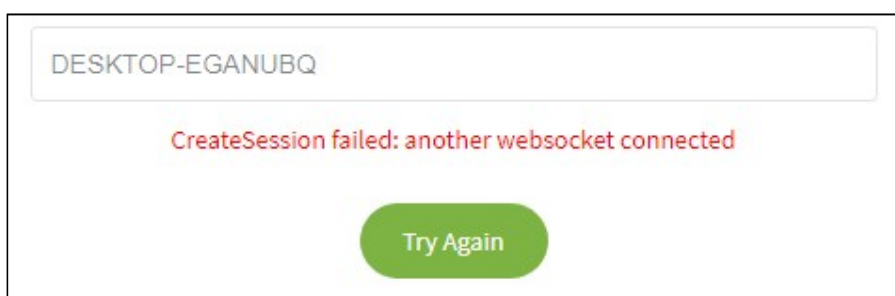
Bước 3: Chọn agent để kết nối, sau đó click “Start”. Danh sách Agent là các Agent trong IRFLow;





Lưu ý:

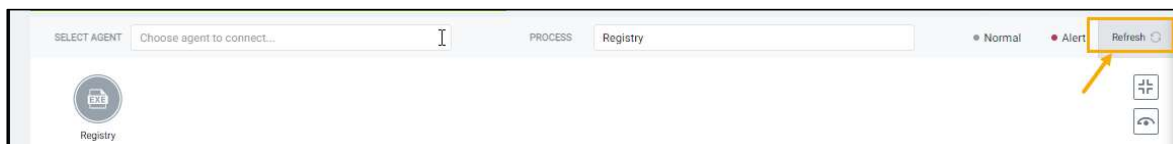
- + Thời gian timeout tạo kết nối là 60s. Hết 60s không kết nối được Agent thì cần kết nối lại;
- + Tại 1 thời điểm trong 1 IRFLow chỉ có thể tạo 1 kết nối tới Agent. Trong trường hợp có tài khoản khác đang kết nối với Agent trong cùng IRFLow thì sẽ thông báo lỗi:



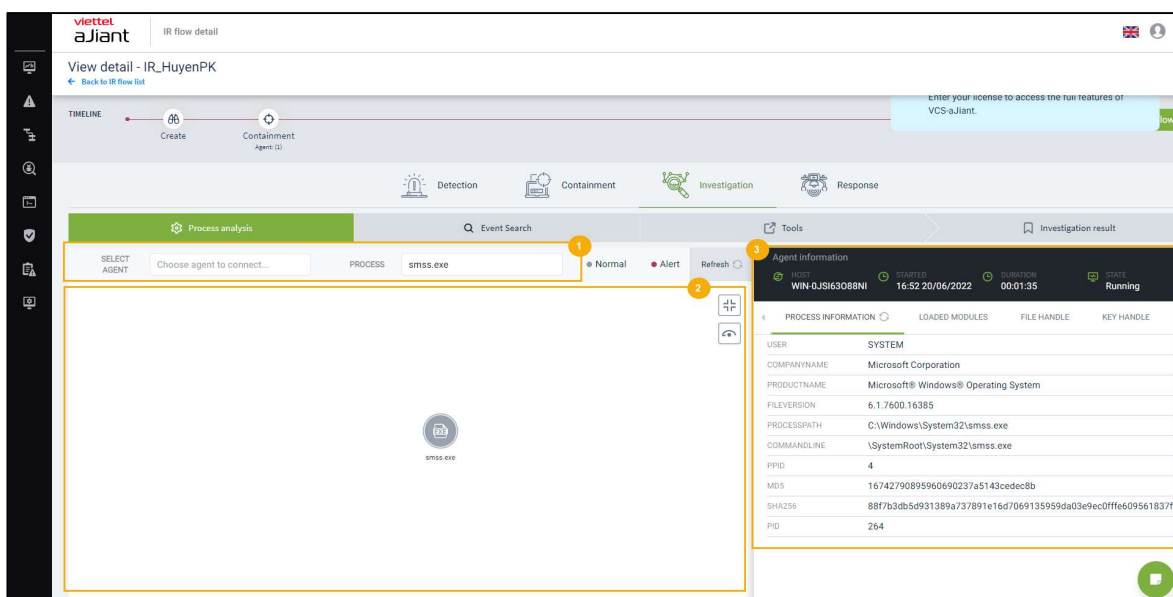
- + Tại thời điểm kết nối, nếu Agent offline. Hệ thống sẽ hiển thị popup thông báo Agent đang ở trạng thái Offline:



Bước 4: Click “Refresh” để lấy danh sách process mới nhất dưới Agent:



Bước 5: Lựa chọn process trong list process để xem thông tin chi tiết:



- Chọn agent và chọn process;
- Hiển thị thông tin cây process, mặc định hiển thị 1 cấp cha và 1 cấp con. Cho phép mở thêm/thu nhỏ các cấp khi click vào process trong cây. Process được focus trong cây sẽ hiển thị icon khác so với process không được focus;
- Hiển thị thông tin process được focus trong cây bao gồm thông tin trên các tab: Process info, Modules (loaded dll), File handles, Key handles, Thread List, Section handles, Network Connection;

Bước 6: Để lấy thông tin mới nhất của process, click icon Refresh trên mỗi tab

Agent information	
HOST WIN-0JSI63O88NI	STARTED 16:52 20/06/2022
DURATION 00:01:35	STATE Running
PROCESS INFORMATION	LOADED MODULES
FILE HANDLE	KEY HANDLE
USER SYSTEM	
COMPANYNAME Microsoft Corporation	
PRODUCTNAME Microsoft® Windows® Operating System	
FILEVERSION 6.1.7600.16385	
PROCESSPATH C:\Windows\System32\smss.exe	
COMMANDLINE \SystemRoot\System32\smss.exe	
PPID 4	
MD5 16742790895960690237a5143cedec8b	
SHA256 88f7b3db5d931389a737891e16d7069135959da03e9ec0ffe609561837fa7	
PID 264	

Lưu ý:

- + Khi chuyển tab con trong Investigation như Event Search, Tools, Investigation Result thì phiên kết nối với Agent được giữ và không cần kết nối lại;
- + Khi chuyển tab khác như Detection, Containment, Response hay Alert, Setting.... Hoặc F5, Logout... thì cần phải tạo lại kết nối với Agent;
- + Phiên kết nối Process Analysis trong IRFLow chỉ đóng khi quản trị đóng IRFLow. Tức là nếu chưa đóng IRFLow thì mỗi lần vào IRFLow và kết nối với Agent thì ID của phiên kết nối ko thay đổi;

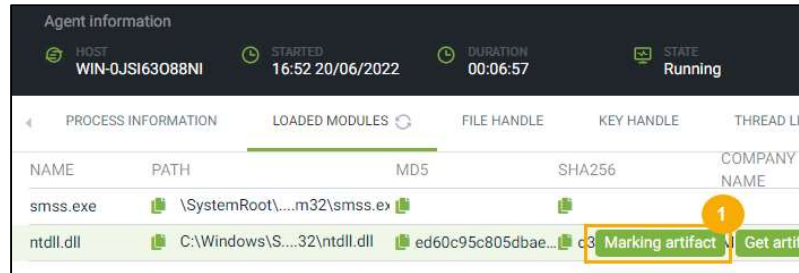
b. Marking/Get artifact

Chức năng Marking artifact cho phép đánh dấu các artifact cần theo dõi. Có thể marking các dữ liệu sau:

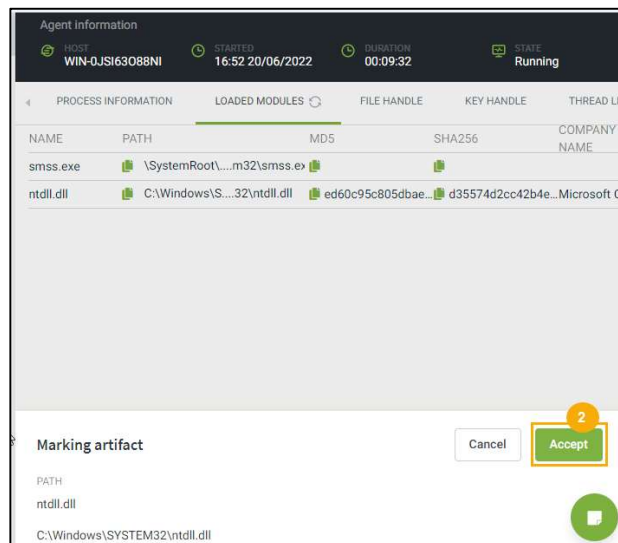
- + Process Info: ProcessPath;
- + Loaded module: Path;
- + File Handle: Path;
- + Key Handle: Key path, Value;

Đánh dấu thông tin trong Process:

Bước 1: Chọn 1 bản ghi bất kỳ và hover vào bản ghi đó. Thực hiện click vào nút “Marking artifact”;

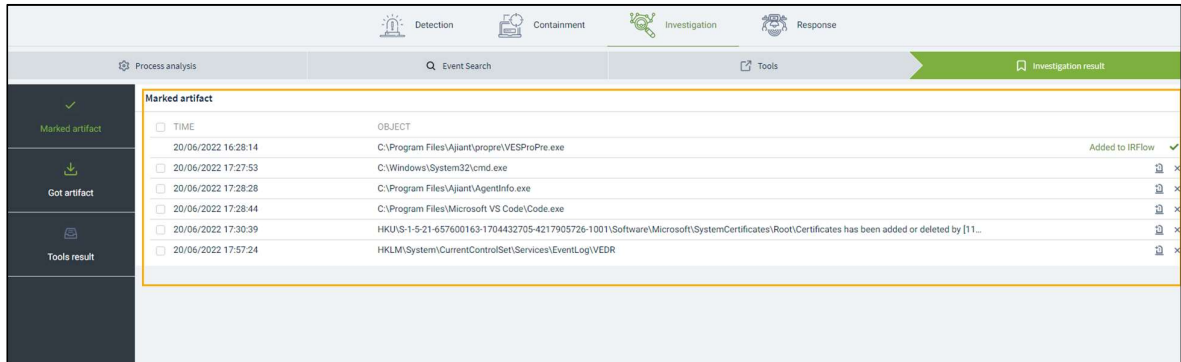
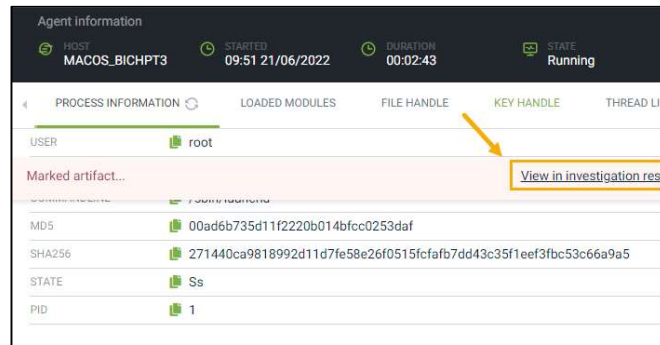


Bước 2: Click vào nút “Accept”, có thể chỉnh sửa đường dẫn file khi click vào icon “edit”:



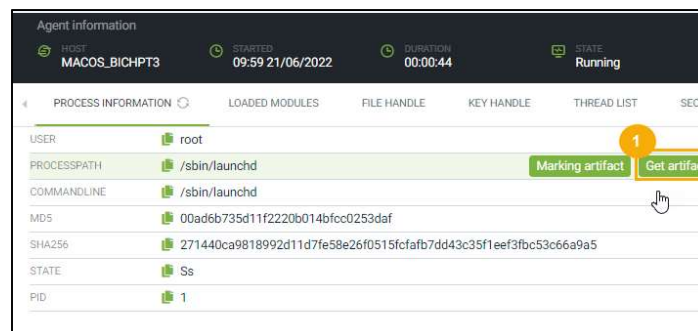
- + Trường hợp chọn bản ghi có Agent chưa tồn tại trong Detection sẽ có thêm check box Add Agent to IRFlow. Khi thực hiện Accept thì Agent tương ứng sẽ được add vào Detection.

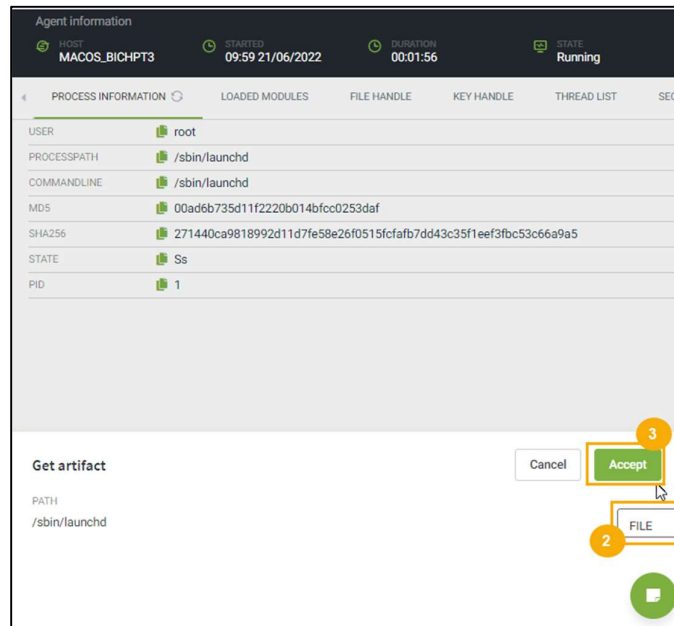
Sau khi marking thành công, hiển thị thông báo. Click vào nút “View all artifacts in Investigation Result” để chuyển đến màn hình Investigation Result. Artifact được marking sẽ hiển thị trên màn hình này:



Chức năng Get Artifact cho phép lấy thông tin file/registry dưới Agent phục vụ cho việc điều tra;

Chọn 1 bản ghi và hover vào bản ghi đó. Click nút “Get artifact” > Lựa chọn loại artifact (File/Registry) > Click “Accept”. Sau đó kiểm tra kết quả thực hiện Get artifact trên màn hình Investigation Result;

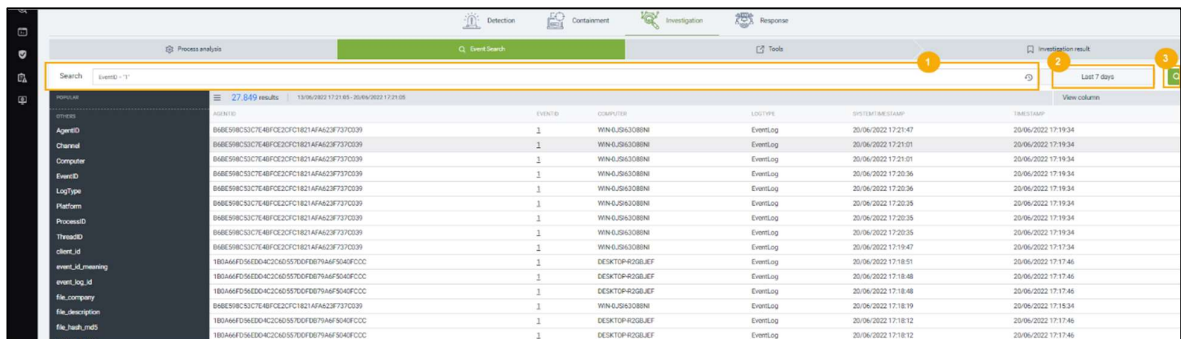




3.4.7.2 Event Search

Đây là quá trình tìm kiếm các đối tượng dựa vào event logs. Khác với các tab khác trong IRFlow chỉ hiển thị thông tin các Agent được add vào IRFlow thì ở tab này hiển thị toàn bộ event của tất cả Agent trong hệ thống.

a. Tìm kiếm Event



Bước 3: 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:
 - AgentID: ID của agent;
 - EventID: ID của event;
 - Computer: Tên của computer;
 - LogType: Loại log;
 - Channel: Channel của event;

- + <toán_tử> là các giá trị sau:
 - = : 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 4: Chọn khoảng thời gian tìm kiếm bằng cách click vào nút “Date & Time” và chọn thời gian tùy ý. Nếu không chọn thời gian thì hệ thống chọn mặc định là Last 7 days;

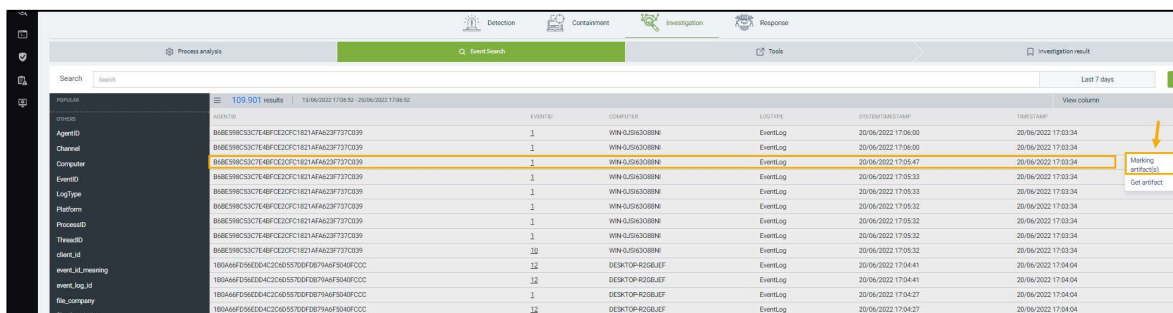
Bước 5: Click on Search:

- + 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 với 5 cột hiển thị mặc định bao gồm: AgentID, EventID, Computer, LogType, Channel;

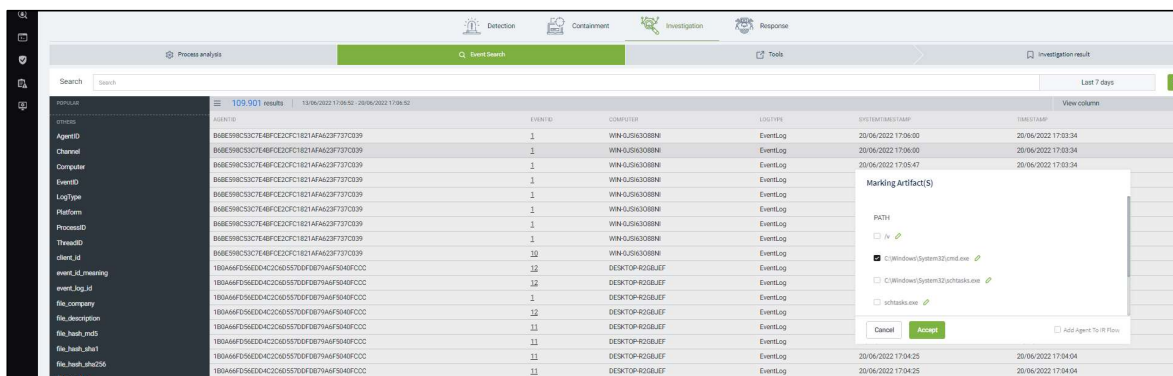
b. Xử lý Event

Mục đích: Hỗ trợ người dùng thao tác và xử lý các Event;

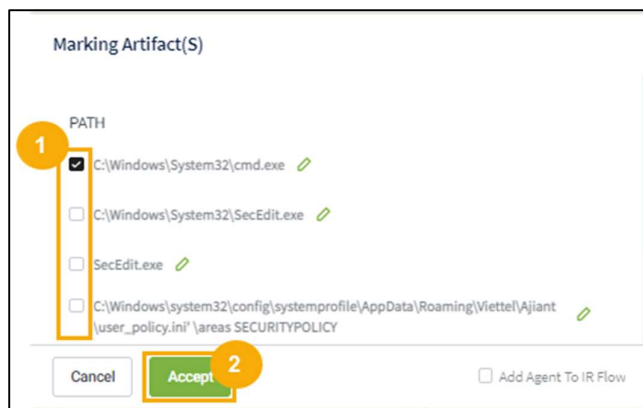
Marking artifact: Đánh dấu artifact



Bước 1: Chọn 1 bản ghi bất kỳ và hover vào bản ghi đó. Thực hiện click vào nút “Marking artifact”. Trên màn hình sẽ hiển thị popup như sau:



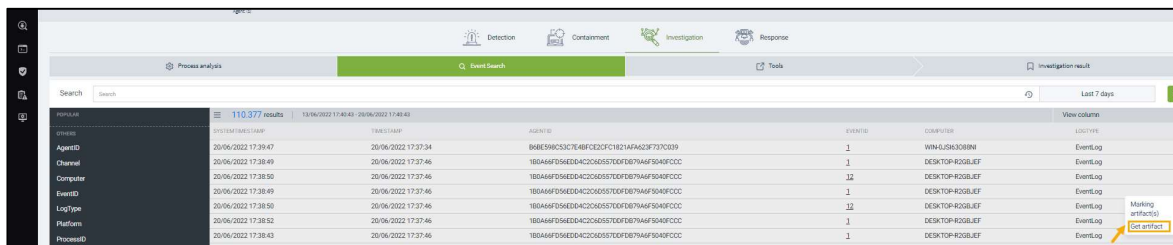
Bước 2: Chọn 1 hoặc nhiều path thực hiện đánh dấu Artifact:



- + Chọn nút “Accept” để xác nhận yêu cầu đánh dấu Artifact;
- + Chọn nút “Cancel” để xác nhận hủy bỏ yêu cầu đánh dấu Artifact;

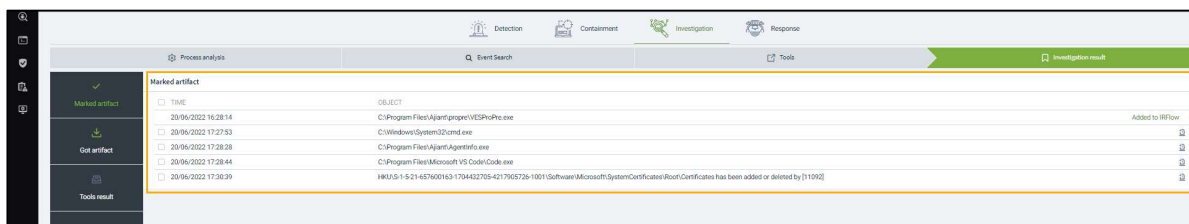
Get artifact: thực hiện get file/registry dưới Agent lên server để phục vụ cho quá trình điều tra;

Bước 1: Chọn 1 bản ghi bất kỳ và hover vào bản ghi đó. Thực hiện click vào nút “Get artifact” Trên màn hình sẽ hiển thị popup như sau:



Bước 2: Chọn artifact sau đó chọn loại artifact (File/Registry) và click “Accept”

Khi marking artifact thành công màn hình sẽ hiển thị thông báo. Click vào “View in investigation result” để chuyển đến màn hình Investigation Result. Kết quả của việc Get artifact sẽ hiển thị trên tab này:



c. Deploy Tools

Mục đích: là quá trình đẩy tool xuống dưới Agent lấy thông tin để điều tra. Thông tin một số tool có sẵn trên hệ thống:

+ Với agent Windows:

- Listdlls: lấy thông tin các processs và dll đang được load lên;
- Autorunsc: lấy thông tin các tiến trình, dịch vụ khởi động cùng hệ thống;

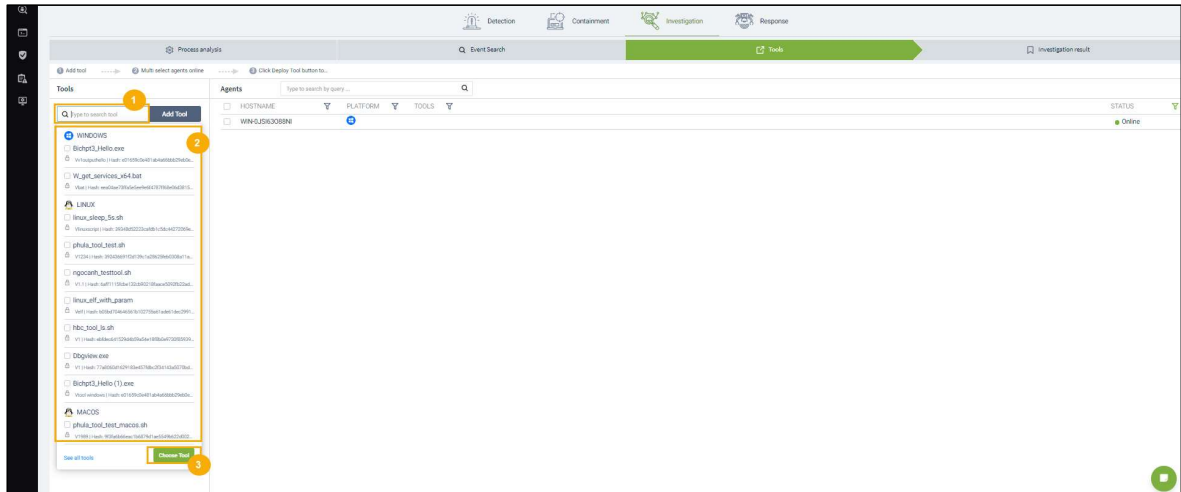
+ Với agent Linux:

- ListService: lấy danh sách service dưới máy agent;

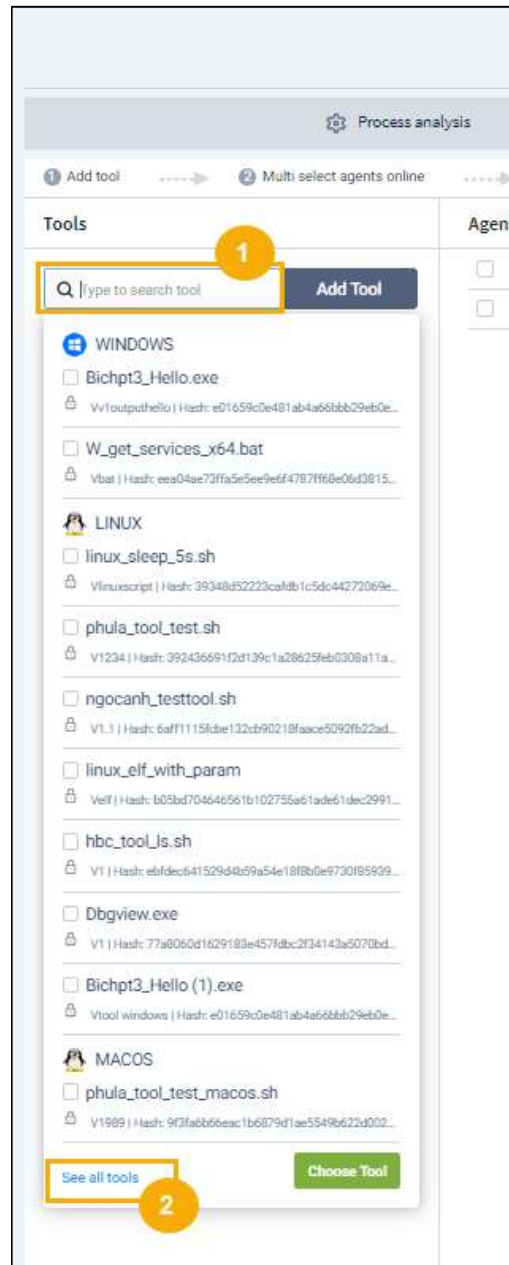
+ Luồng thực hiện chức năng này như sau: Thực hiện lựa chọn tool > Chọn agent > click “Deploy tools”;

Để lựa chọn tool thích hợp có 2 cách sau:

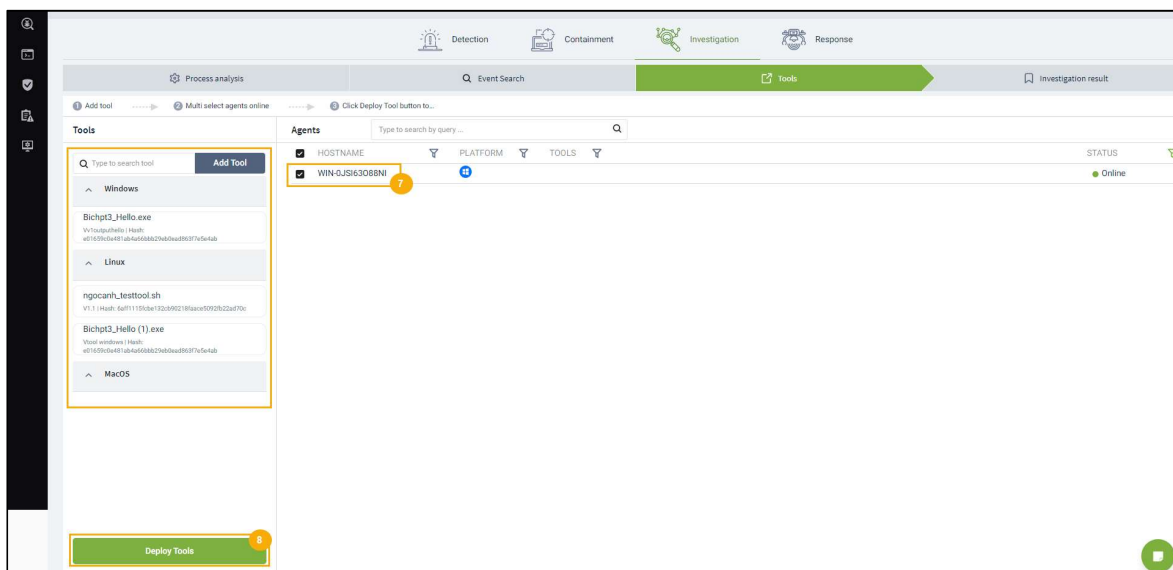
- + Cách 1: Click vào textbox search tool > click tool cần deploy > click “Choose tool”:



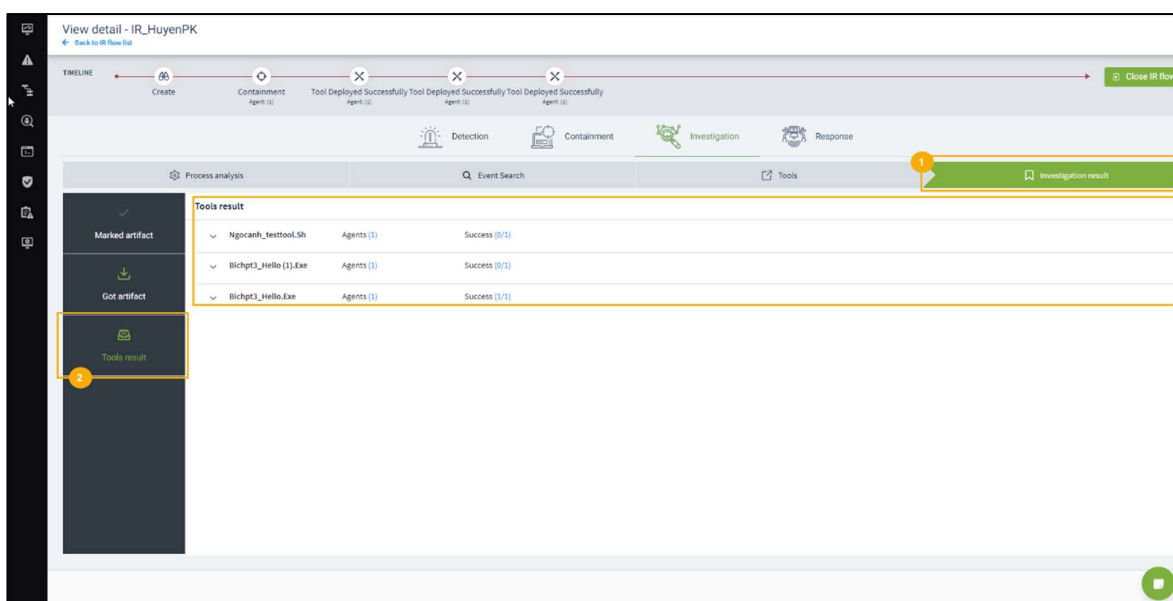
- + Cách 2: Click vào textbox search tool > click “See all tools” => hiện ra màn hình danh sách tool đầy đủ > Tìm kiếm và lựa chọn tool cần deploy > click “Add tool”;



+ Sau bước tìm kiếm tool thực hiện chọn agent và click “Deploy tools”



+ Sau khi deploy tool thì xem kết quả ở tab Investigation Result, tab Tools Result



d. Investigation result

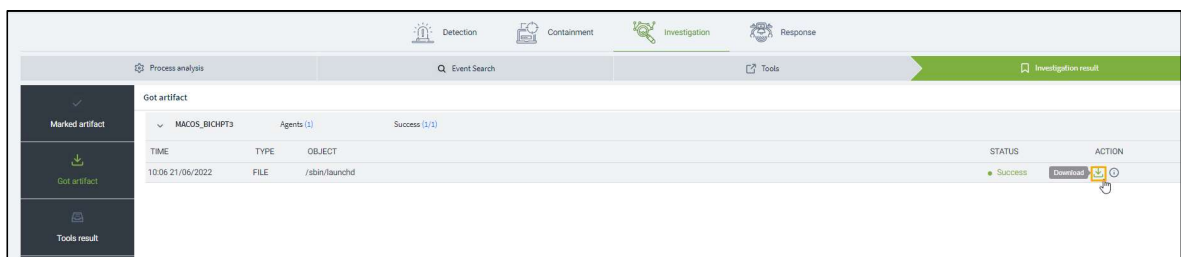
Đây là màn hình hiển thị thông tin kết quả Deploy tool, Marking/Get Artifact ở 3 tab: Process Analysis, Event search, Tools:

- + Tab “Got Artifact”: kết quả thực hiện lệnh Get Artifact;
- + Tab “Tool Results”: kết quả thực hiện lệnh Deploy tools;

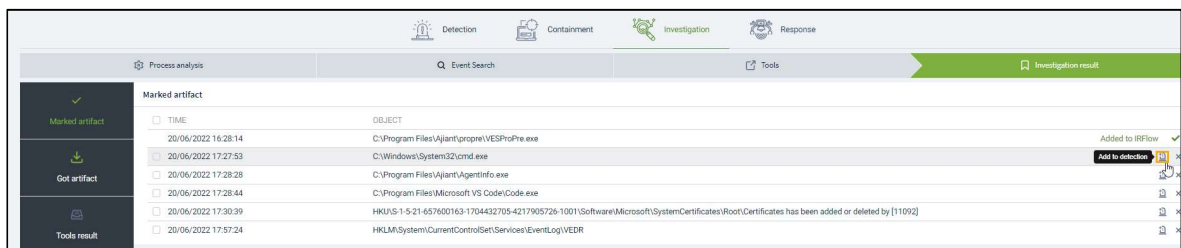
- + Tab “Marked Artifact”: các artifact đã marking;

Trong tab “Got Artifact” và “Tool Results”, có thể thực hiện các hành động sau:

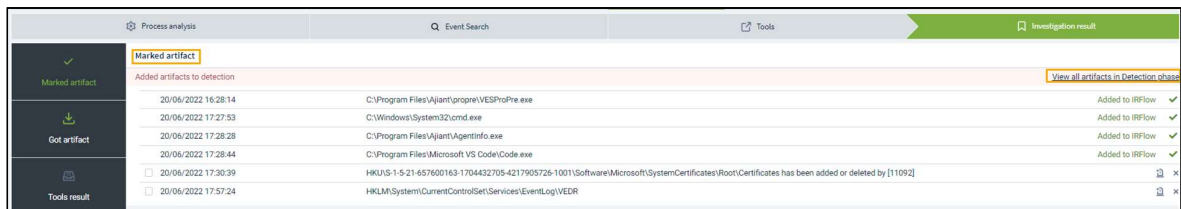
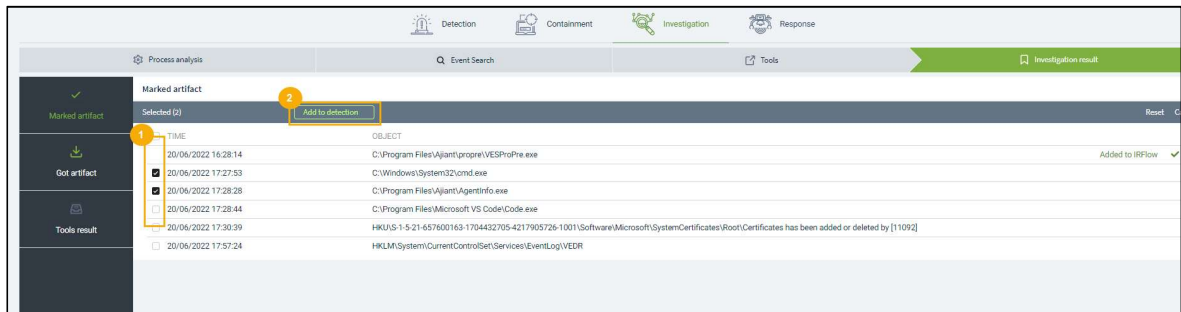
- + Xem nội dung chi tiết của artifact đã lấy hoặc kết quả chạy tool dưới agent. Nếu dữ liệu là text thì có thể xem trực tiếp trên giao diện, nếu dữ liệu là file thực thi (.exe) thì cần download về máy local để kiểm tra;
- + Download artifact hoặc kết quả chạy tool. Có 2 cách Download: click icon “Download” trên giao diện hoặc click icon “Detail” > click icon “Download” trên màn hình này;



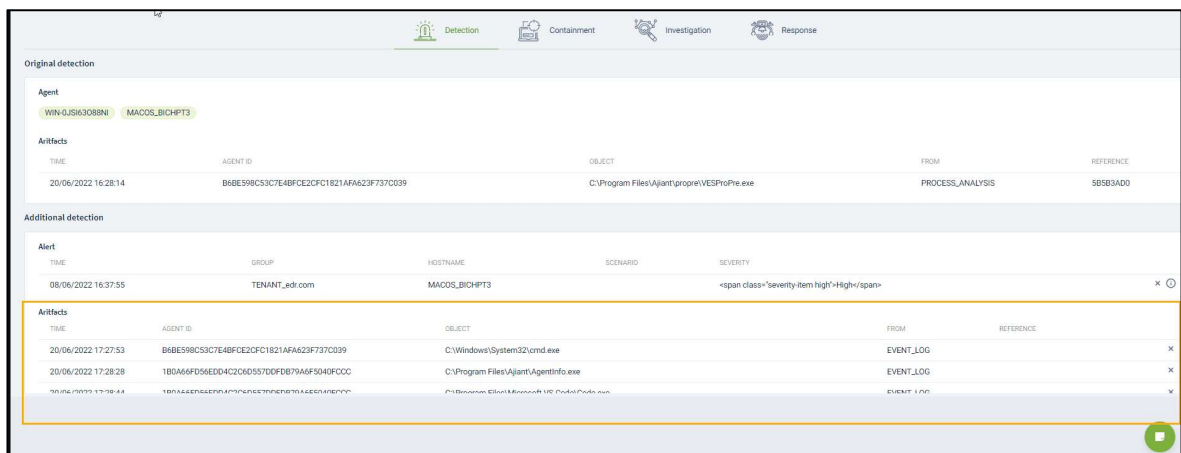
Trong Tab Marked artifact, lựa chọn artifact để thêm vào màn hình Detection, Chọn 1 artifact và click “Add to detection”:



Chọn nhiều artifact và click “Add to detection”:



Sau khi add thành công sẽ hiện thông báo thành công, click vào “View all artifacts in Detection phase” chuyển đến màn hình Detection. Các artifact được thêm vào mục Additional detection trên màn hình Detection:



3.4.8 IRFlow – Response

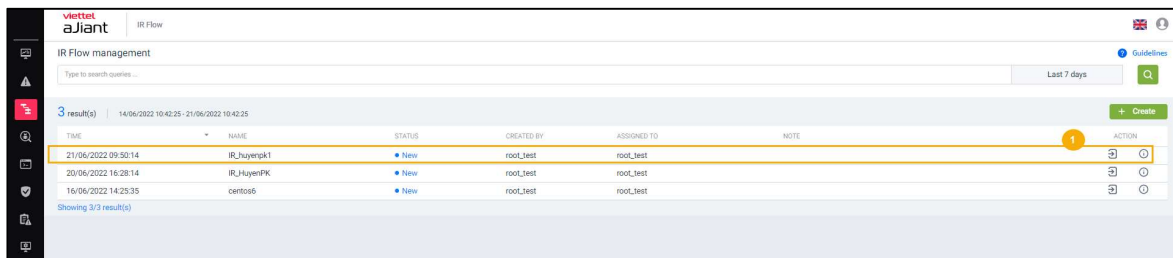
3.4.8.1 Live Response

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;

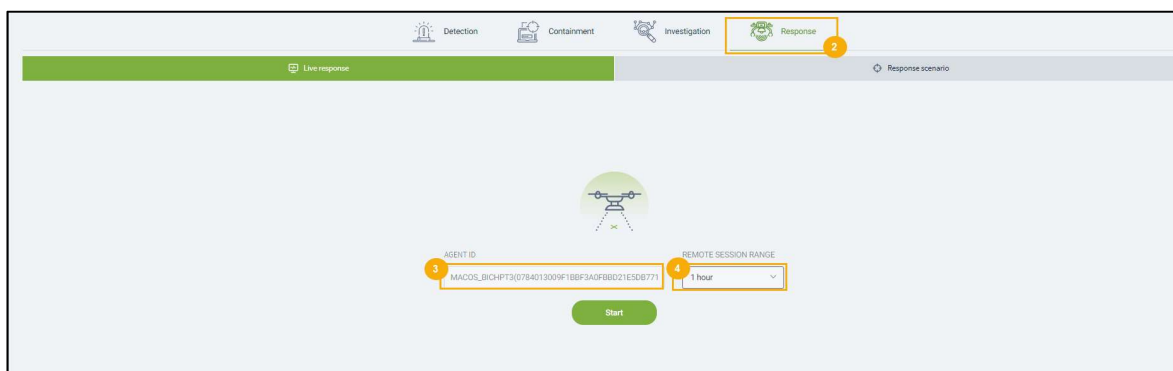
Các bước thực hiện chức năng Live Response trong IRFlow:

Bước 1: Click tab “IRFlow”;

Bước 2: Click đúp vào 1 bản ghi trong danh sách các bản ghi (lưu ý: Chọn đúng bản ghi IRFlow mà có chứa Agent cần thực hiện Live Response);



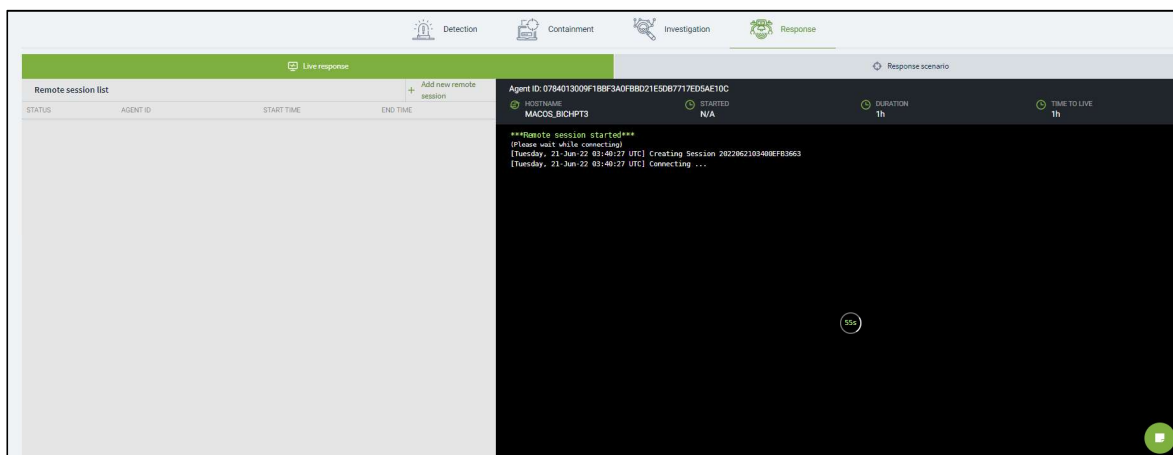
Bước 3: Click tab con Response:



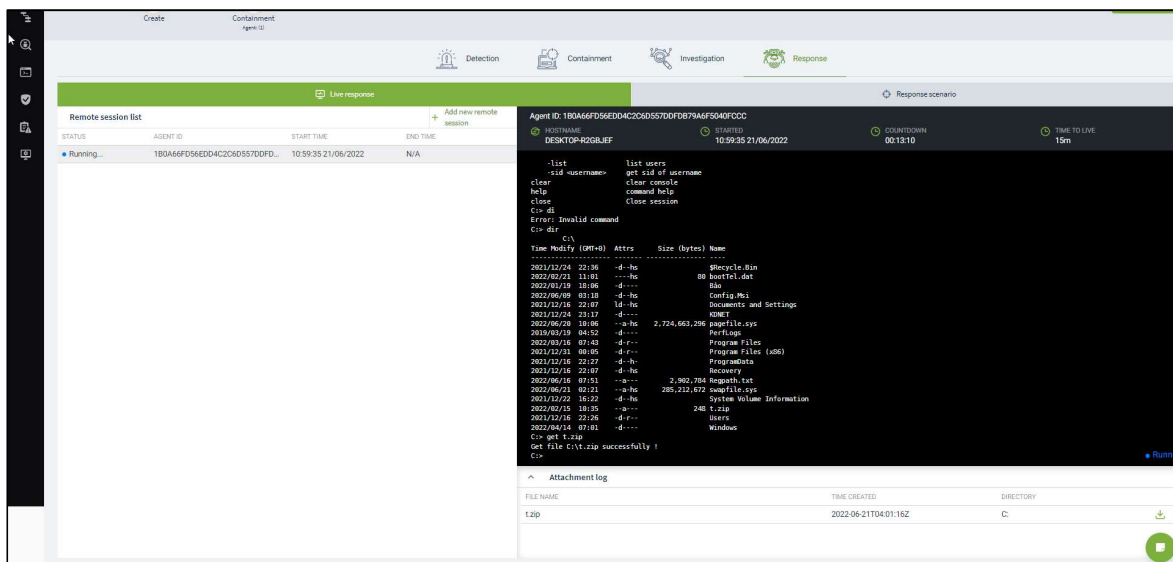
Bước 4: Chọn Agent và khoảng thời gian cần thực hiện (5 phút/ 15 phút/ 1 giờ/ 3 giờ) Live Response và bấm nút “Start Live Response”;

Danh sách Agent hiển thị trong combobox là tất cả các Agent hiển thị trong tab Detection;

Sau đó, người dùng cần chờ 1 phút để hệ thống thực hiện kết nối tới agent, trạng thái hệ thống là “connecting”;



Bước 5: Khi kết nối thành công, hệ thống hiển thị 1 bản ghi bên Remote session list và màn hình console có thông tin của kết nối và hiển thị trạng thái “running”.



(Remote Session List: hiển thị danh sách các phiên live response đã được thực hiện của IRFlow)

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

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

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
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	

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
		N By name (alphabetic) 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	

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
		/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/ thư 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

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
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	Dump process bởi Process name

STT	Các lệnh	Tham số	Mô tả
		Ví dụ: dump -process -name Evil.exe -f "C:\Users\Evil_dumped.dmp"	
		-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:	Truy vấn tất cả các subkey và value và data

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
		reg-query "HKLM\Software\abc xyz" -s	
		add <keyname> ví dụ: reg-add "HKLM\software\abc xyz"	Thêm 1 key
		add <keyname> -v <valuenam> -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 <valuenam>	Xóa 1 giá trị của key
		import <filename>	Import 1 file .reg
		export <keyname> <filename>	Export 1 file .reg

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
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
		-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

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
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
18	help		Lệnh help
19	Clear		Làm sạch console
20	Close		Đóng session

+ Ubuntu: Thực hiện các câu lệnh sau:

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
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>	Xóa 1 thư mục

STT	Các lệnh	Tham số	Mô tả
		ví dụ: delete -folder temp\axvers	
		delete –all <folderpath> ví dụ: delete –all c:\temp	Xóa tất cả các file/ thư 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

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
		-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	
		-d <processid> -o <imagepath> generate core file of running program, ví dụ: process -d 231 -o /tmp/core_file	

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
12	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
13	user	-list	Liệt kê các user trên máy
		-sid<username>	Lấy sid của username
14	help		Lệnh help
15	Clear		Làm sạch console

+ MACOS:

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
1	cd	cd <dirpath>	Thay đổi thư mục làm việc hiện tại
		cd.. hoặc cd ..	Chuyển về thư mục cha

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
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
		delete –all <folderpath> ví dụ: delete –all c:\temp	Xóa tất cả các file/ thư 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)

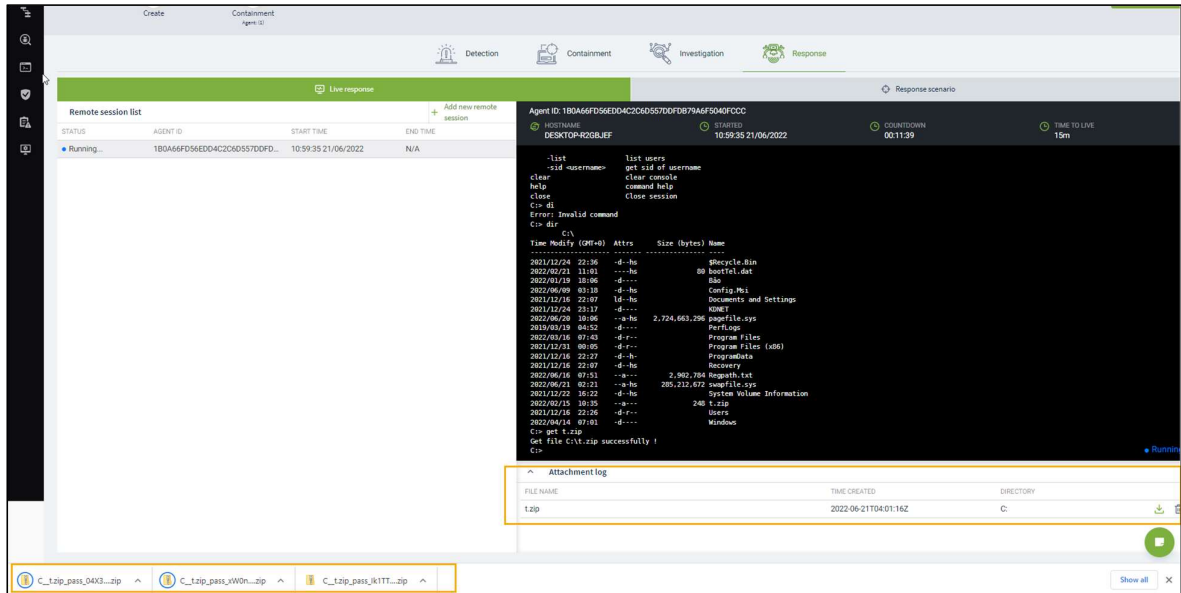
<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
7	Hash	hash <type: md5 sha1 sha256> <filepath> -f get file hash ví dụ: hash md5 example: c:\test\run.exe	Cho phép mã hóa file tối đa 1MB Option -f để buộc mở tệp khi tệp đang được mở bởi một quy trình khác
8	get	<filepath>	Upload 1 file từ host lên 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
		-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	

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
		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
		-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:

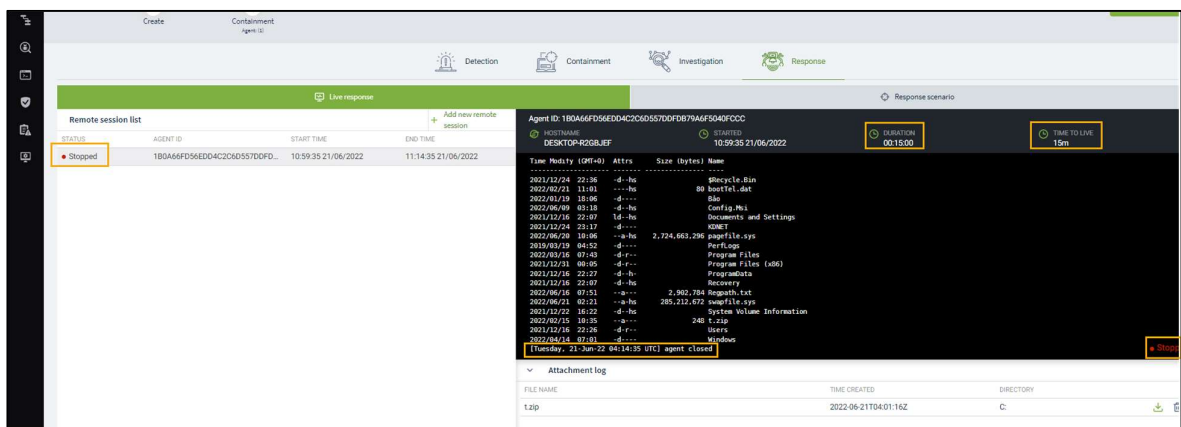
Lệnh get <filepath>:

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.

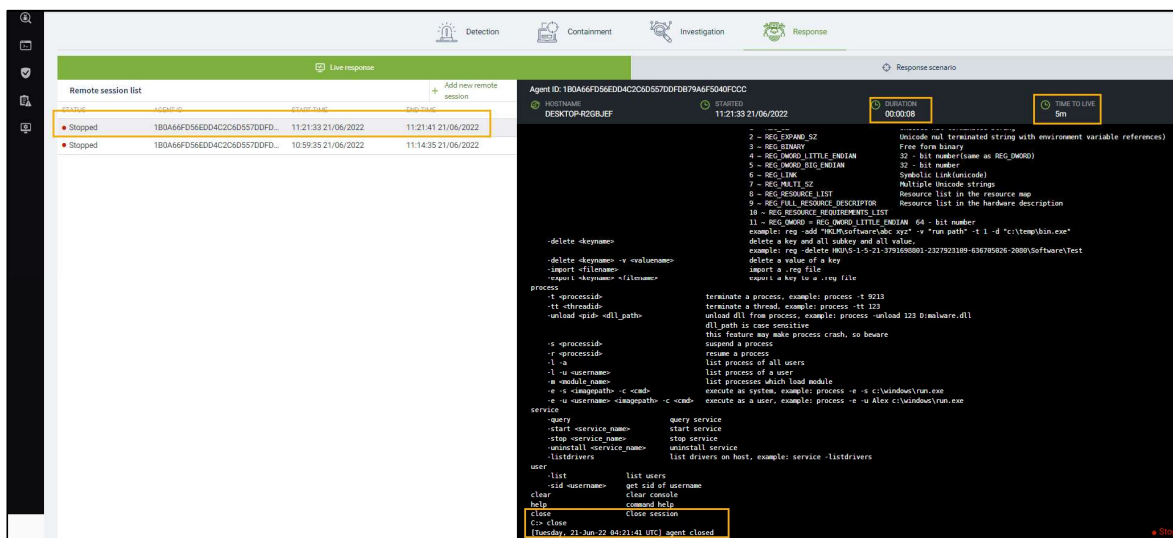


Bước 6: Phiên làm việc của Live Response kết thúc khi:

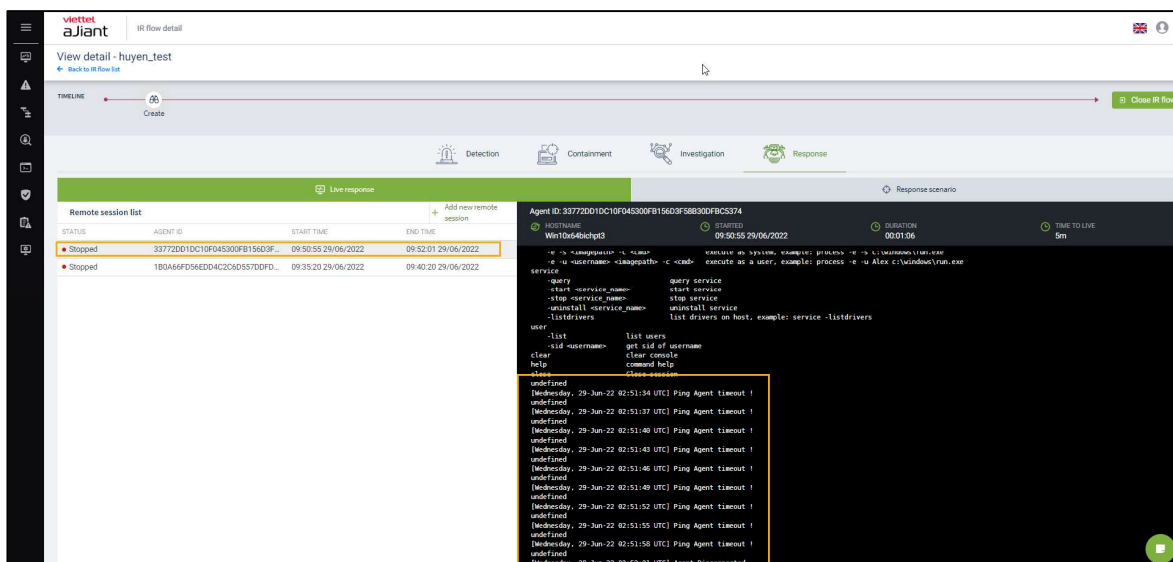
Thời gian của phiên hết hiệu lực: Khi trường “Duration” bằng thời gian với trường “Time To Live”;



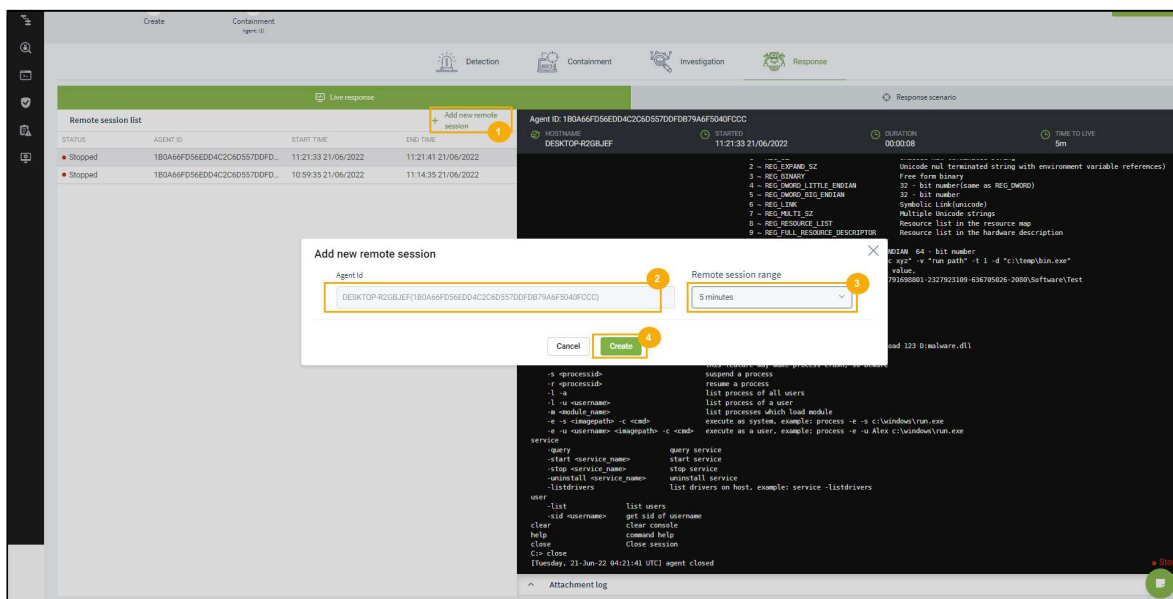
Người dùng chủ động yêu cầu đóng kết nối bằng lệnh “close”;



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



Ngoài ra, người dùng có thể click nút “+ Add New Remote” để tạo 1 phiên live response mới:

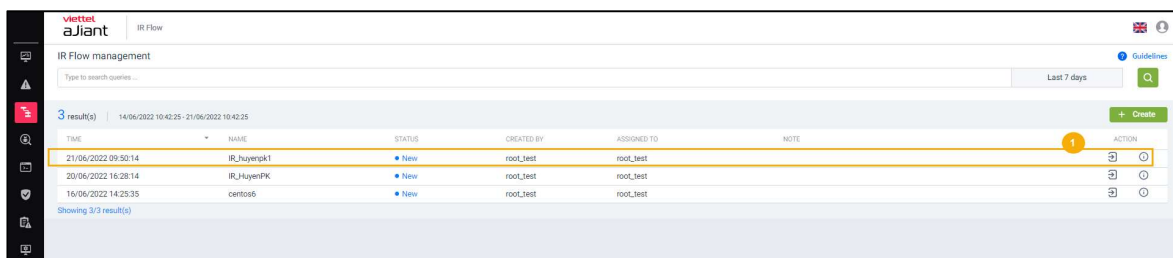


3.4.8.2 Response Scenario

Chức năng Response scenario cung cấp khả năng cài đặt một kịch bản Response và thực hiện phản ứng trên một hoặc nhiều Agent;

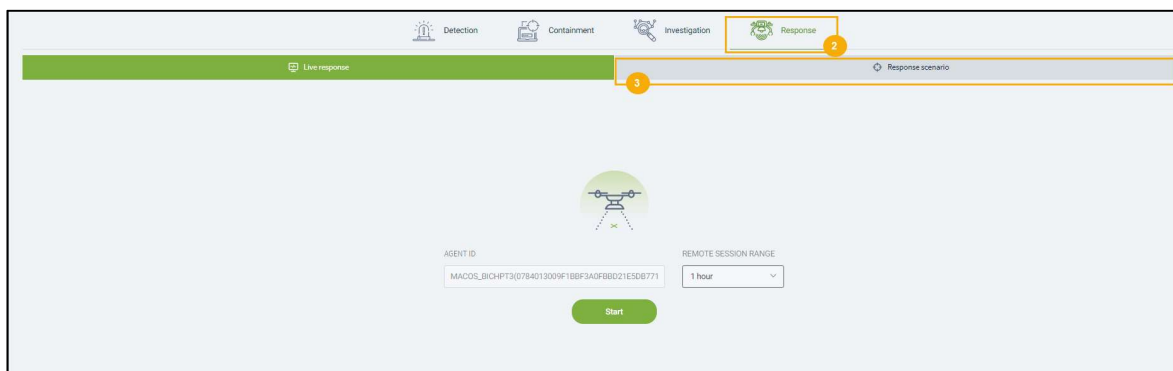
Các bước thực hiện chức năng Response Scenario trong IRFlow:

Bước 1: Click tab IRFlow:

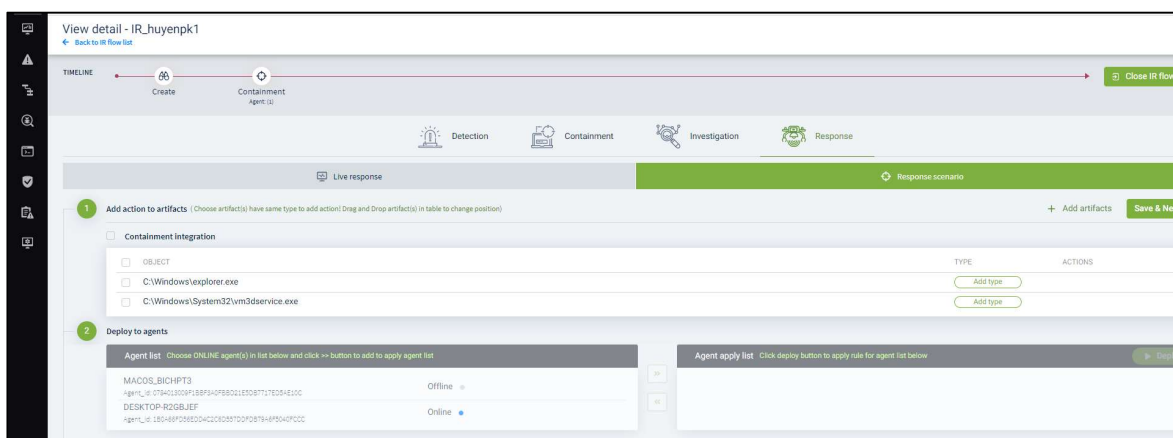


Bước 2: Click duplicate vào 1 bản ghi trong danh sách các bản ghi (lưu ý: Chọn đúng bản ghi IRFlow mà có chứa Agent cần thực hiện Response Scenario);

Lưu ý: Để thực hiện được các kịch bản phản ứng thì người quản trị phải add sẵn các Artifact ở phần Detection như hình dưới:



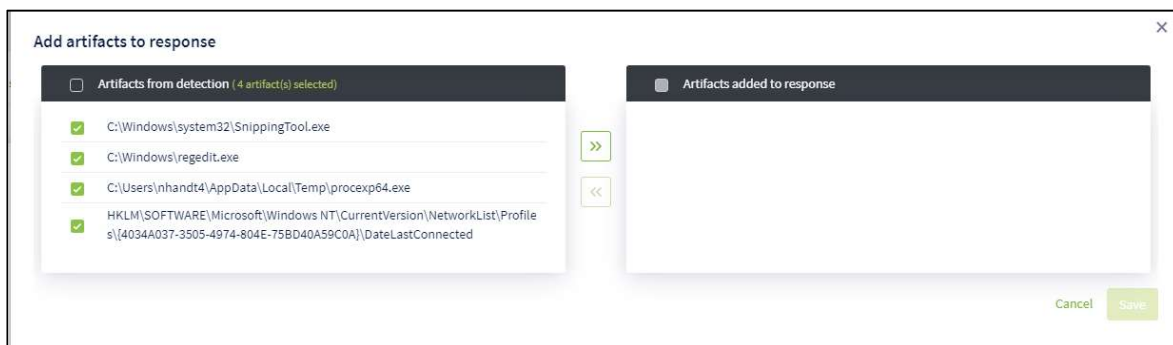
Bước 3: Click Response Tab >> Response Scenario:



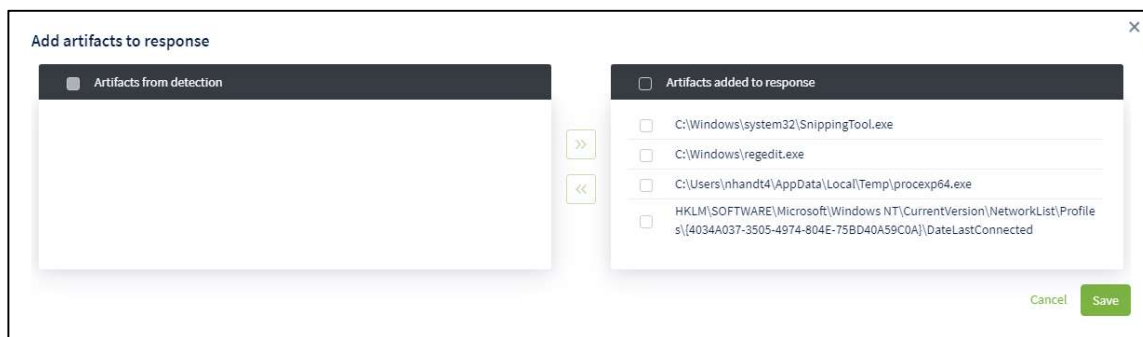
Bước 4: Thực hiện các cấu hình chi tiết: Add action to Artifact

Click nút **Add artifacts from detection phase** để bắt đầu thêm artifacts vào kịch bản phản ứng;

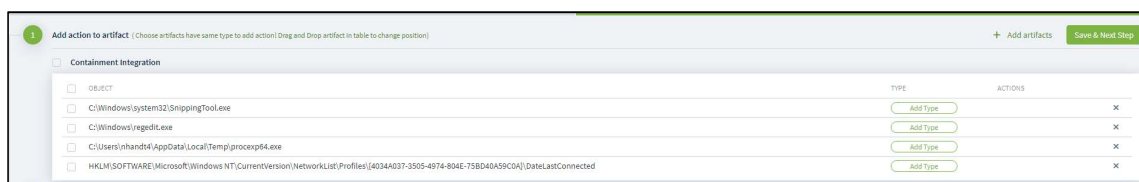
Danh sách Artifact hiển thị từ tab Detection:



Click nút **>>** để chuyển sang phần các artifact trong kịch bản phản ứng:



Click “Save” để lưu lại danh sách Artifact đã chọn hoặc “Cancel” để hủy bỏ thao tác chọn trên:



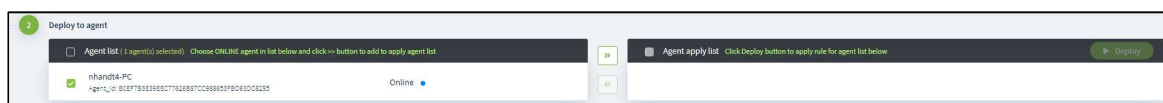
Lựa chọn Type cho các Artifact. Hệ thống hỗ trợ gán từng type và action cho từng Artifact hoặc 1 type/action cho nhiều Artifact. Có 3 type: File, Process, Registry. Mỗi Type lại có 1 action riêng;



Sau khi hoàn tất phần gán Type và Action, Click **Save & Next Step** để lưu và chuyển sang bước tiếp hoặc Click **+ Add artifacts** để tiếp tục thêm Artifact;

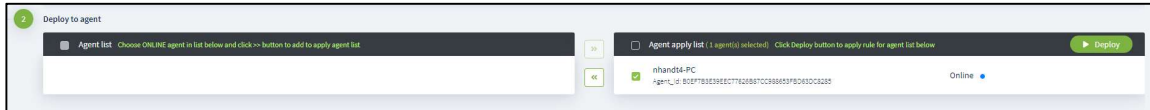
Deploy to Agent: Danh sách Agent được lấy từ tab Detection;

Tích chọn Agent đang online trong List Agent của IRFlow để thực hiện chuyển sang List các agent thực hiện kịch bản phản ứng;



Click **>>** để chuyển sang List các agent có thể deploy;

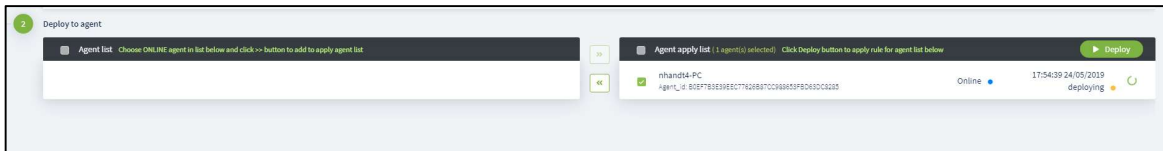
Tích chọn Agent để Deploy;



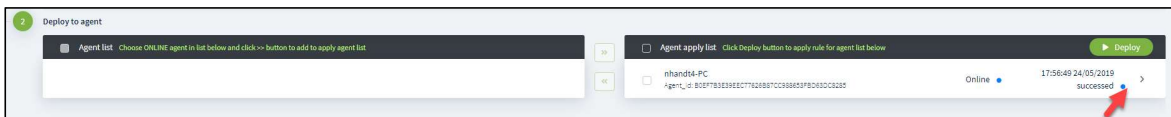
Bấm nút Deploy

Sau khi bấm nút Deploy, có các trạng thái:

Deploying:



Succeeded



Click vào chi tiết để xem kết quả triển khai kịch bản

Deploy result			
Object	Type	Action	Result
C:\Windows\system32\SnippingTool.exe	PROCESS	Terminate	succeeded
C:\Windows\regedit.exe	PROCESS	Suspend	Error: Incorrect function.
C:\Users\nhandt4\AppData\Local\Temp\procepx64.exe	FILE	Delete	Error: The request is not supported.
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{4034A037-350...	REGISTRY	Delete	succeeded

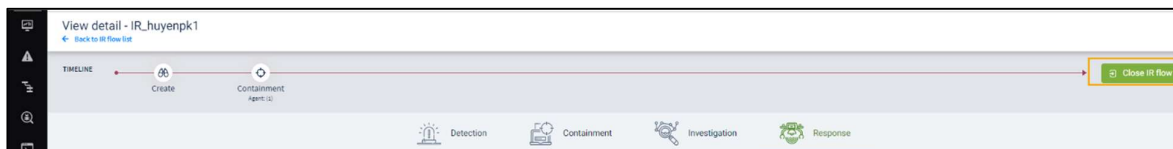
3.4.9 Close IRFlow

Đóng IRFlow sau khi đã điều tra và xử lý xong;

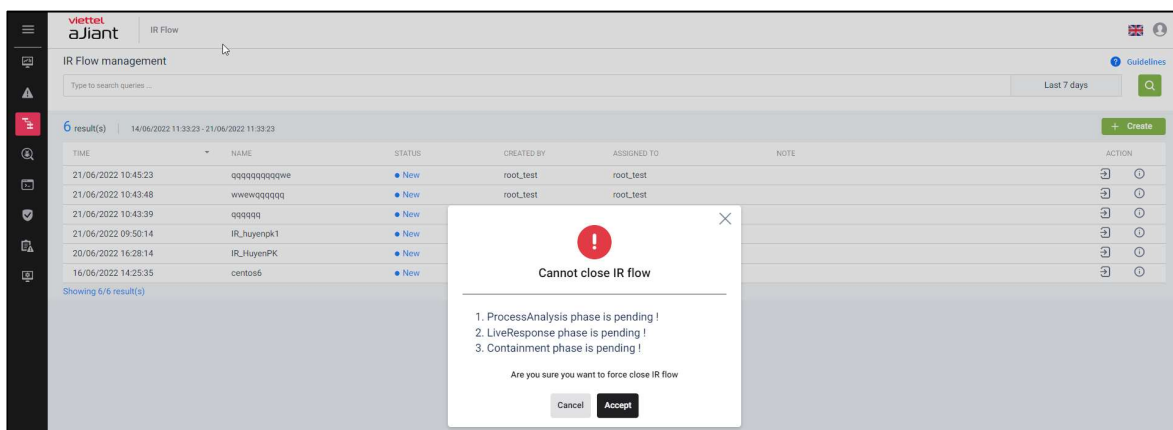
Để thực hiện close IRFlow click “Close IRFlow” trên màn hình danh sách IRFlow;

viettel aJiant IR Flow						
IR Flow management						
Type to search queries...						
14/06/2022 11:33:23 - 21/06/2022 11:33:23						
TIME	NAME	STATUS	CREATED BY	ASSIGNED TO	NOTE	ACTION
21/06/2022 10:45:23	qqqqqqqqqqqq	New	root_test	root_test		Close IR flow
21/06/2022 10:43:48	wwwqqqqqqq	New	root_test	root_test		
21/06/2022 10:43:39	qqqqqqq	New	root_test	root_test		
21/06/2022 09:50:14	IR_huyengk1	New	root_test	root_test		
20/06/2022 16:28:14	IR_HuyenPK	New	root_test	root_test		
16/06/2022 14:25:35	centos6	New	root_test	root_test		

Hoặc click “Close IRFlow” trên timeline ở bất cứ pha nào trong IRFlow: Detection, Containment, Investigation, Response;

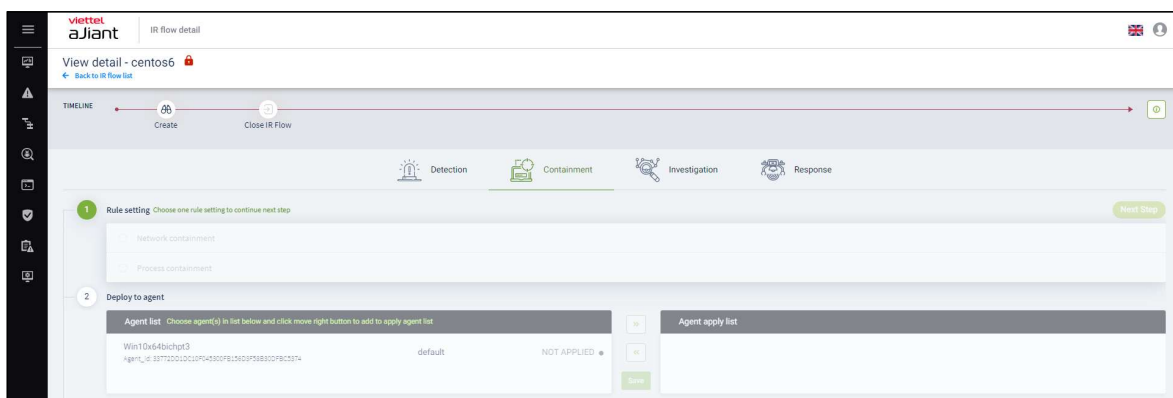


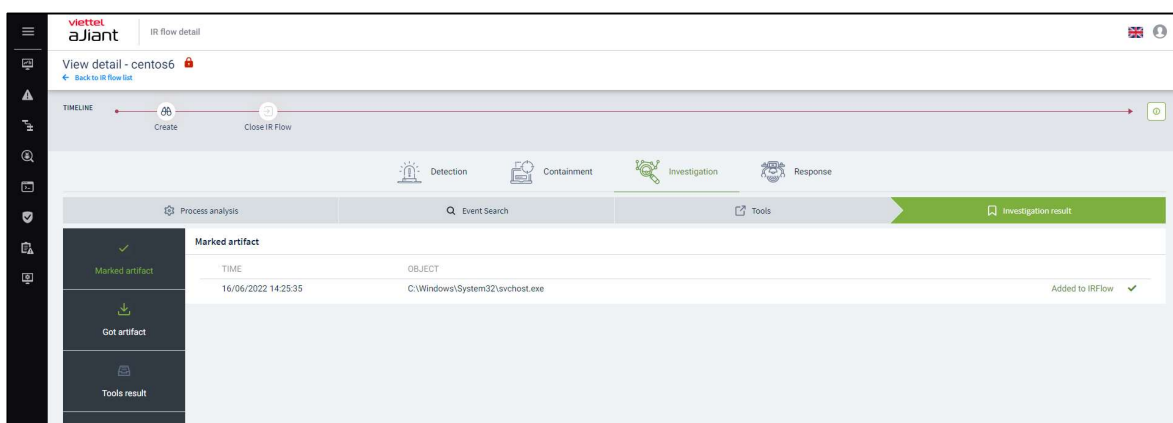
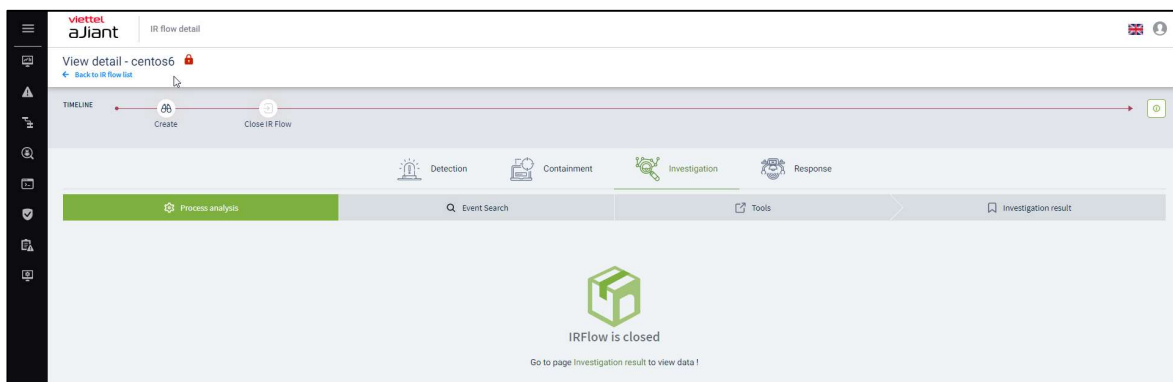
Nếu khi chọn close IRFlow mà có các tác vụ chưa thực hiện xong như: Containment, Live Response, Response Scenario, Deploy tool... thì sẽ hiện thông báo hỏi người dùng;



Khi người dùng chọn Ok thì sẽ đóng tất cả các kết nối tới Agent trong Irflow;

Khi vào IRFlow đã closed chỉ xem được thông tin ở 2 tab Detection và Investigation Result, các tab khác chức năng sẽ bị disable hoặc không hiển thị dữ liệu;



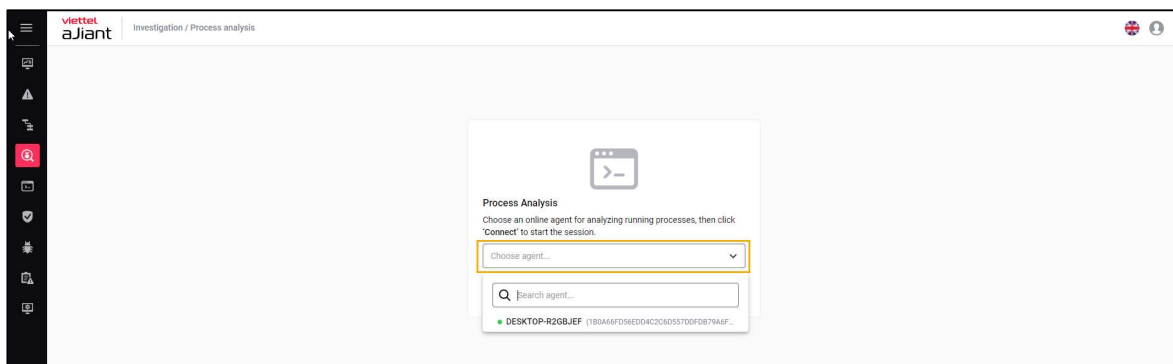


3.5 Màn hình Investigation

Màn hình Investigation gồm một số tab nhỏ là Process Analysis, Event Search, Deploy Tools. Về mặt hoạt động thì 2 chức năng này không khác nhiều so với trong IRFlow. Có 1 số điểm khác sẽ được trình bày cụ thể dưới đây

3.5.1 Investigation_Process Analysis

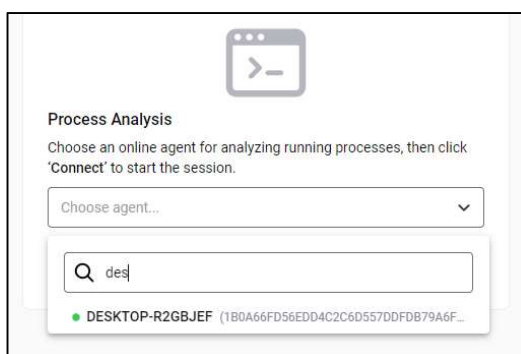
- Mục đích: Chức năng cho phép người dùng tạo kết nối và kiểm tra hiện trạng process dưới máy người dùng. Trong đó:



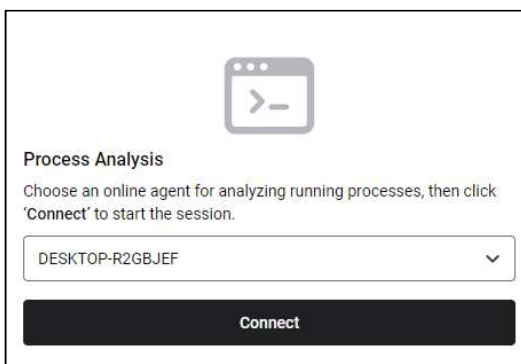
Danh sách máy người dùng:

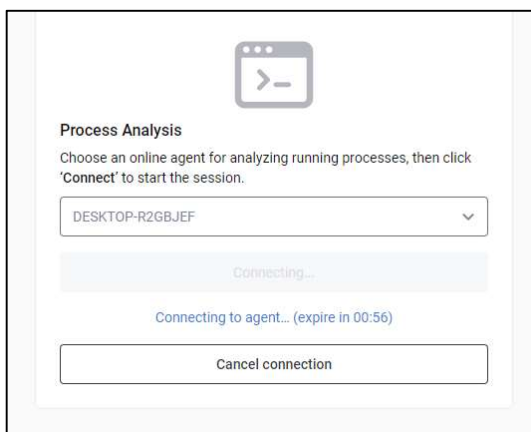
- + User đăng nhập thuộc group root: Hiện thị tất cả Agent trong hệ thống active < 30 ngày;
- + User đăng nhập thuộc group default: Hiện thị tất cả Agent thuộc group default;
- + User đăng nhập thuộc group cha: Hiện thị tất cả Agent thuộc group của user đang login và group con tương ứng;
- + User đăng nhập thuộc group một hoặc nhiều con: Hiện thị tất cả Agent thuộc group của user đang login;

Bước 1: Tìm kiếm và chọn Agent kết nối (Lưu ý để đảm bảo 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

Name	PID	Path	User name	Command line	Signature	Action
explorer.exe	5048	C:\Windows\explorer.exe	test	C:\Windows\Explorer.EXE	Microsoft Windows	
SecurityHealthSystray.exe	7156	C:\Windows\System32\SecurityHealthSystray.exe	test	"C:\Windows\System32\SecurityHealthSystray.exe"	N/A	
vmtoolsd.exe	5956	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	test	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vm- VMware, Inc.	VMware, Inc.	
OneDrive.exe	7264	C:\Users\test\AppData\Local\Microsoft\OneDrive\OneDrive.exe	test	"C:\Users\test\AppData\Local\Microsoft\OneDrive\OneDrive.exe"	Microsoft Corporation	
mmc.exe	6132	C:\Windows\System32\mmc.exe	test	"C:\Windows\system32\mmc.exe" "C:\Windows\system32\per..."	N/A	
cmd.exe	3212	C:\Users\test\Desktop\New folder\cmd.exe	test	"C:\Users\test\Desktop\New folder\cmd.exe"	N/A	
conhost.exe	9252	C:\Windows\System32\conhost.exe	test	"C:\Windows\system32\conhost.exe" 0x4	N/A	
Code.exe	11092	C:\Program Files\Microsoft VS Code\Code.exe	test	"C:\Program Files\Microsoft VS Code\Code.exe"	Microsoft Corporation	
Code.exe	3284	C:\Program Files\Microsoft VS Code\Code.exe	test	"C:\Program Files\Microsoft VS Code\Code.exe" --type=gui...	Microsoft Corporation	
Code.exe	13300	C:\Program Files\Microsoft VS Code\Code.exe	test	"C:\Program Files\Microsoft VS Code\Code.exe" --type=render...	Microsoft Corporation	
Code.exe	9228	C:\Program Files\Microsoft VS Code\Code.exe	test	"C:\Program Files\Microsoft VS Code\Code.exe" --reporter=ur...	Microsoft Corporation	
Code.exe	5008	C:\Program Files\Microsoft VS Code\Code.exe	test	"C:\Program Files\Microsoft VS Code\Code.exe" --no-lazy-asp...	Microsoft Corporation	
Code.exe	13328	C:\Program Files\Microsoft VS Code\Code.exe	test	"C:\Program Files\Microsoft VS Code\Code.exe" --type=utility...	Microsoft Corporation	
Code.exe	4896	C:\Program Files\Microsoft VS Code\Code.exe	test	"C:\Program Files\Microsoft VS Code\Code.exe" --type=render...	Microsoft Corporation	
chrome.exe	8308	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	test	"C:\Program Files (x86)\Google\Chrome\Application\chrome.e...	Google LLC	
chrome.exe	6664	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	test	"C:\Program Files (x86)\Google\Chrome\Application\chrome.e...	Google LLC	

Trong đó giao diện chia làm các nhóm thông tin:

- 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 thái kết nối
- 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

116 result(s) Last updated: 21/06/2022 11:50:51						
Name	PID	Path	User name	Command line	Signature	Action
svchost.exe	3360	C:\Windows\System32\svchost.exe	test	C:\Windows\system32\svchost.exe -k UnistackSvcGroup	Microsoft Windows Publisher	
svchost.exe	3680	C:\Windows\System32\svchost.exe	test	C:\Windows\system32\svchost.exe -k ClipboardSvcGroup-p	Microsoft Windows Publisher	
SecurityHealthService.exe	6076	C:\Windows\System32\SecurityHealthService.exe	SYSTEM	"C:\Windows\System32\SecurityHealthSystray.exe"	Microsoft Windows Publisher	
svchost.exe	8084	C:\Windows\System32\svchost.exe	SYSTEM	C:\Windows\System32\svchost.exe -k netsvcs-p	Microsoft Windows Publisher	
▼ VESvc.exe	14380	C:\Program Files\Ajan\VESvc.exe	SYSTEM	"C:\Program Files\Ajan\VESvc.exe"	N/A	
VESConfigurationManager.exe	3500	C:\Program Files\Ajan\VESConfigurationManager.exe	SYSTEM	"C:\Program Files\Ajan\VESConfigurationManager.exe"	N/A	
VESConnectionManager.exe	8628	C:\Program Files\Ajan\VESConnectionManager.exe	SYSTEM	"C:\Program Files\Ajan\VESConnectionManager.exe"	N/A	
VESUpdater.exe	11864	C:\Program Files\Ajan\VESUpdater.exe	SYSTEM	"C:\Program Files\Ajan\VESUpdater.exe"	N/A	
VESResponse.exe	18852	C:\Program Files\Ajan\response\VESResponse.exe	SYSTEM	"C:\Program Files\Ajan\response\VESResponse.exe"	Viettel Group	
▼ VESProPre.exe	16604	C:\Program Files\Ajan\propre\VESProPre.exe	SYSTEM	"C:\Program Files\Ajan\propre\VESProPre.exe"	N/A	
SecurityNotify.exe	7640	C:\Program Files\Ajan\propre\BLS\SecurityNotify.exe	test	"C:\Program Files\Ajan\propre\BLS\SecurityNotify.exe" -ppid ...	Viettel Group	
VESAutoScan.exe	16592	C:\Program Files\Ajan\autoscan\VESAutoScan.exe	SYSTEM	"C:\Program Files\Ajan\autoscan\VESAutoScan.exe"	Viettel Group	
VESCollector.exe	18304	C:\Program Files\Ajan\collector\VESCollector.exe	SYSTEM	"C:\Program Files\Ajan\collector\VESCollector.exe"	N/A	
svchost.exe	2656	C:\Windows\System32\svchost.exe	SYSTEM	"C:\Windows\regedit.exe"	Microsoft Windows Publisher	
TrustedInstaller.exe	3908	C:\Windows\System32\wermgr.exe	SYSTEM	C:\Windows\system32\wermgr.exe -upload	Microsoft Windows	
lsass.exe	800	C:\Windows\System32\lsass.exe	SYSTEM	C:\Windows\system32\lsass.exe	Microsoft Windows Publisher	
fontdrvhost.exe	940	C:\Windows\System32\fontdrvhost.exe	UMFD-0	"fontdrvhost.exe"	Microsoft Windows	

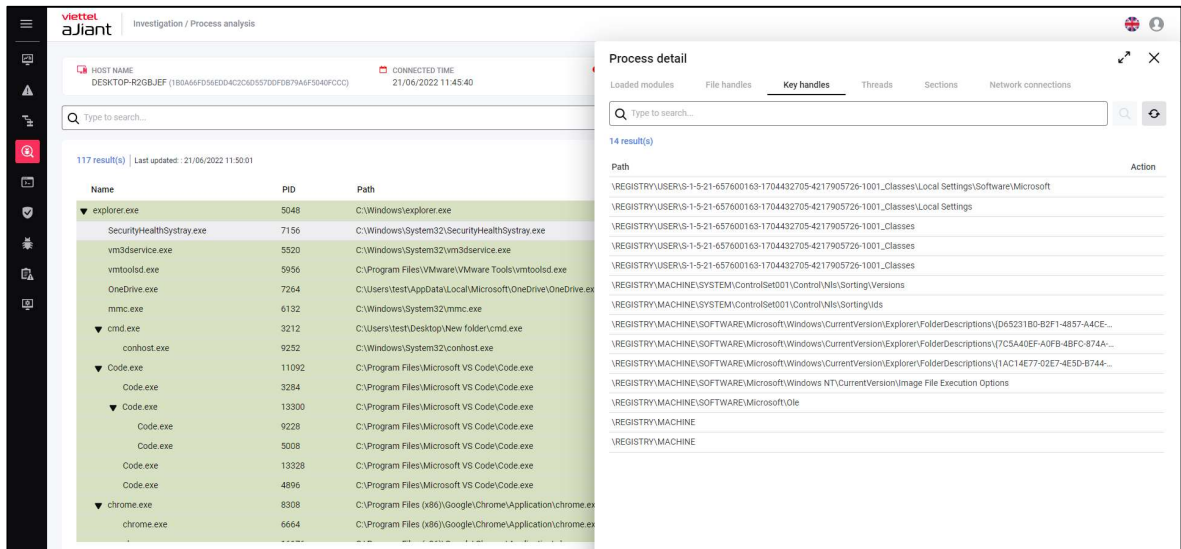
- Verified: Xanh – có chữ ký số và còn hạn;
- Not verified: Đỏ - không có chữ ký số hoặc chữ ký hết hạn;
- N/A: Trắng – không tìm thấy thông tin chữ ký số;

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.

-

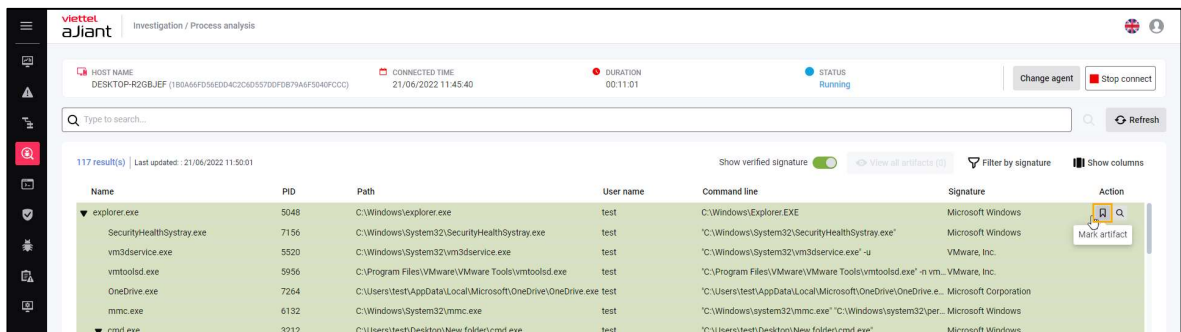


Chi tiết tiến trình được chia thành các tabs, với mỗi tab, danh sách thông tin tương ứng được hiển thị.

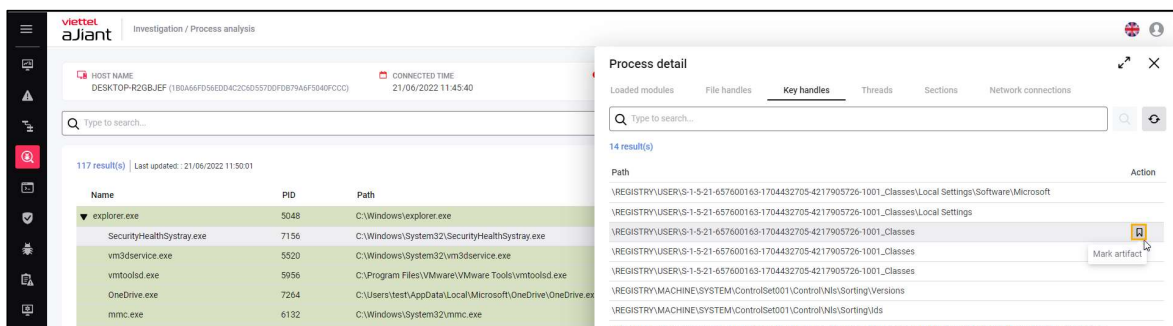
Bước 3: Marking artifact

Tương tự như chức năng Process Analysis trong IRFlow ở màn hình này cũng cung cấp việc đánh dấu các artifact để phục vụ cho việc điều tra;

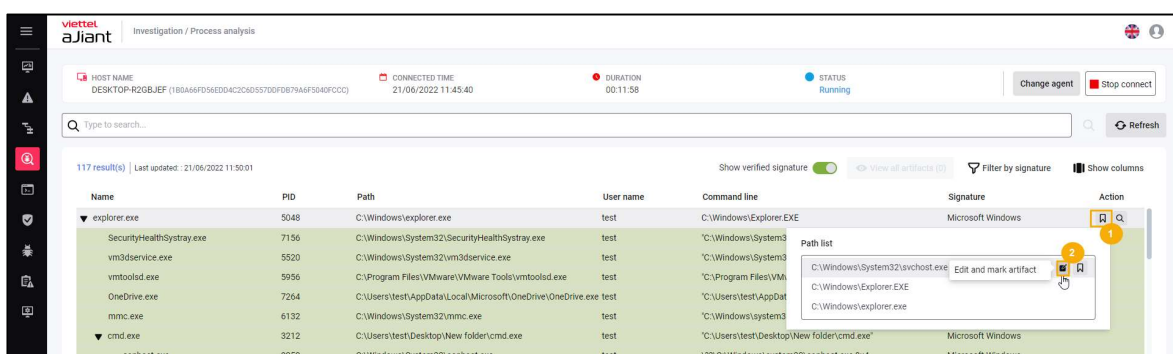
Người dùng có thể chọn tiến trình từ ngoài danh sách để mark:



Hoặc mark các đối tượng khả nghi trong chi tiết tiến trình:

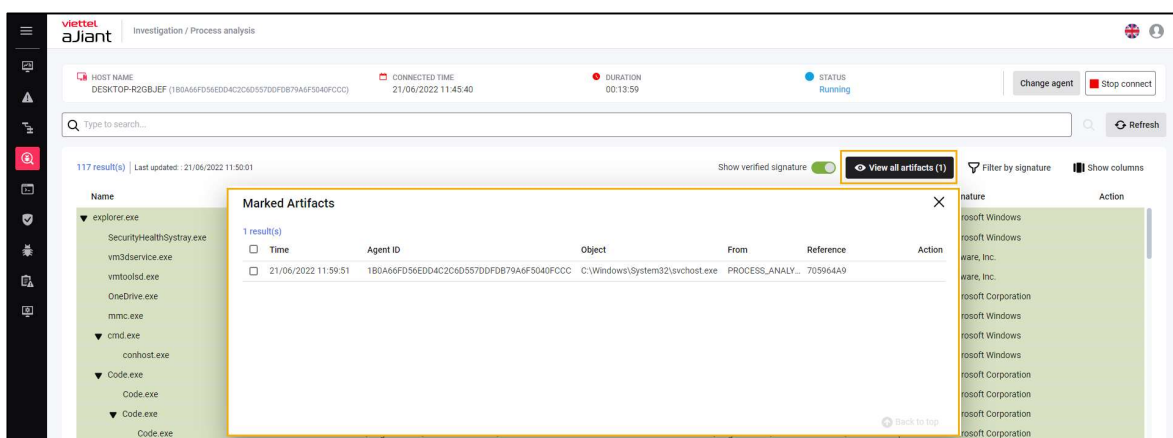


Với mỗi đối tượng được chọn, lựa chọn “Mark with edit” – đánh dấu trực tiếp nội dung hiện tại. Hoặc người dùng có thể chỉnh sửa nội dung đối tượng trước khi đánh dấu



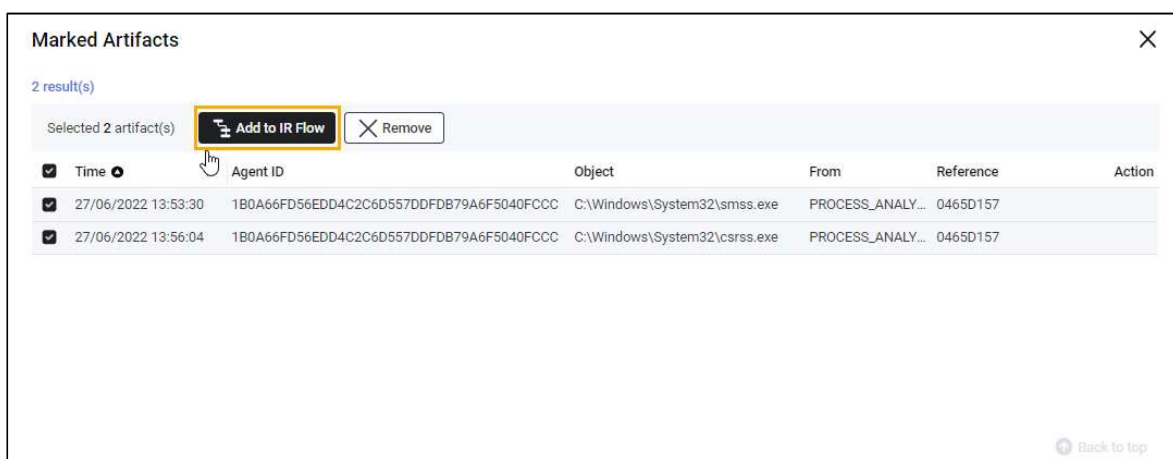
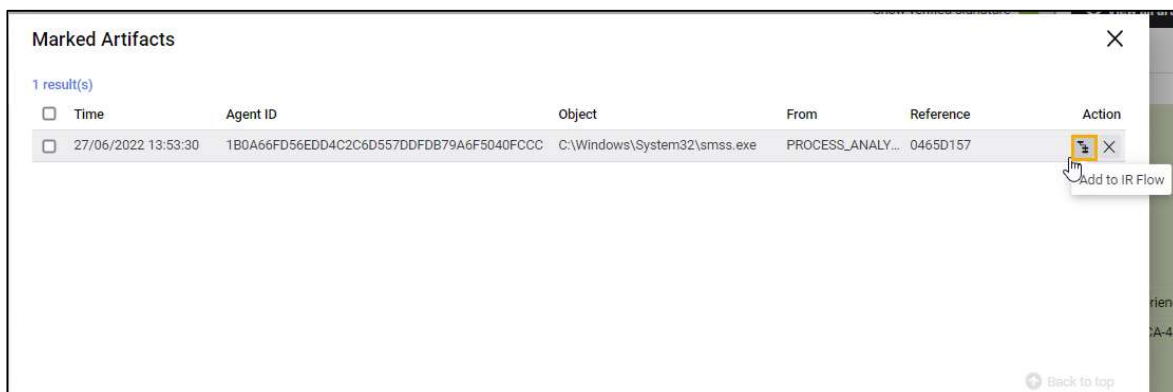
Sau khi đánh dấu, có thể xem lại danh sách bằng cách click **View all artifacts (1)**

Lưu ý: Nút này chỉ hiển thị khi có ít nhất 01 artifact được đánh dấu.

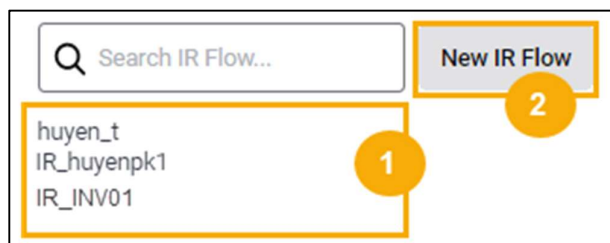


Bước 4: Thêm artifact vào IRFlow:

Trên tab Marked artifact, click “Add to IRFlow” trên 1 bản ghi hoặc chọn nhiều artifact ở chế độ multi select và click “Add to IRFlow”:



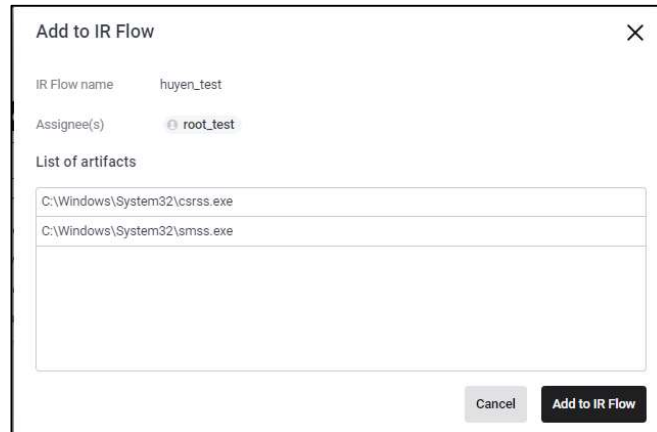
Lựa chọn IRFlow đã tạo sẵn hoặc tạo mới IRFlow:



– Danh sách IRFlow đã tạo sẵn:

- + User đăng nhập thuộc group root: Hiển thị tất cả IRFlow trong hệ thống;
- + User đăng nhập thuộc group default: Hiển thị tất cả IRFlow được assign cho user đang login;

- + User đăng nhập thuộc group cha: Hiển thị tất cả IRFlow được assign cho user đang login và các user thuộc group con tương ứng;
- + User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tất cả IRFlow được assign cho user đang login;



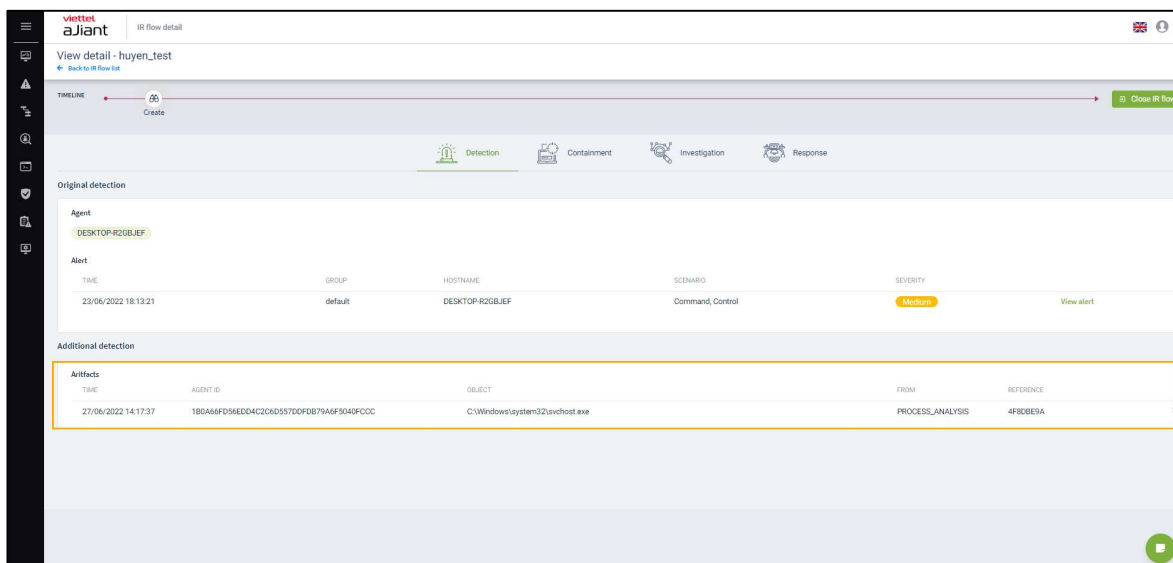
List of artifacts	
C:\Windows\System32\csrss.exe	
C:\Windows\System32\smss.exe	

Danh sách assigned to khi tạo mới 1 IRFlow:

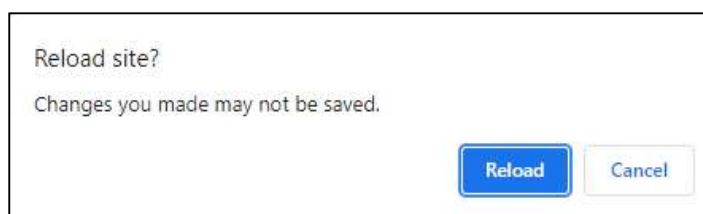
- + User đăng nhập thuộc group root: Hiển thị tất cả tên User trong hệ thống;
- + User đăng nhập thuộc group default: Hiển thị tên User đang login;
- + User đăng nhập thuộc group cha: Hiển thị tất cả tên User thuộc group con của user đang login và user đang login;
- + User đăng nhập thuộc group một hoặc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

Nếu chọn để add vào 1 IRFlow đã tồn tại thì khi chuyển đến màn hình Detection artifact đó sẽ được thêm vào phần Additional detection;

Nếu chọn để add vào 1 IRFlow mới thì khi chuyển đến màn hình Detection artifact đó sẽ được thêm vào phần Original detection;



Lưu ý: Dữ liệu artifacts sẽ không bị mất đi nếu chuyển kết nối đến các máy khác nhau hoặc khi máy hiện tại mất kết nối, trường hợp người dùng tải lại trang hoặc điều hướng đến trang khác, hệ thống yêu cầu xác nhận:



3.5.2 Investigation_Event Search

3.5.2.1 Tìm kiếm Event

Chức năng này tương tự trong Event Search của IRFlow:

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

[illegible]

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

[illegible]

3.5.2.2 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 thực hiện:

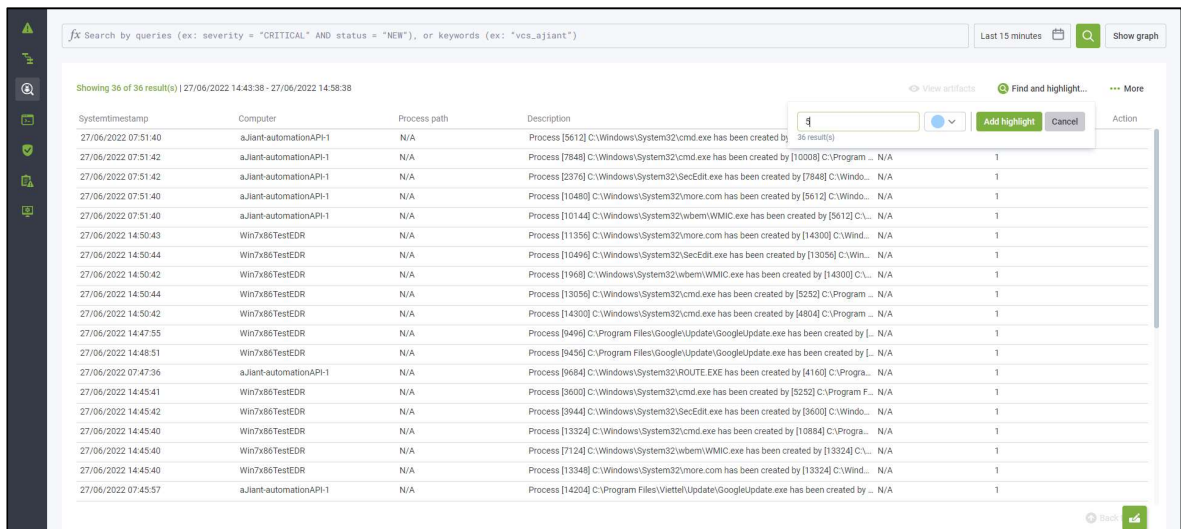
Bước 1: ND chọn Investigation >> Chọn tab Event search;

Bước 2: Màn hình hiển thị danh sách event, Chọn nút “Find and highlight”, HT hiển thị popup 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;



3.5.2.3 Need help

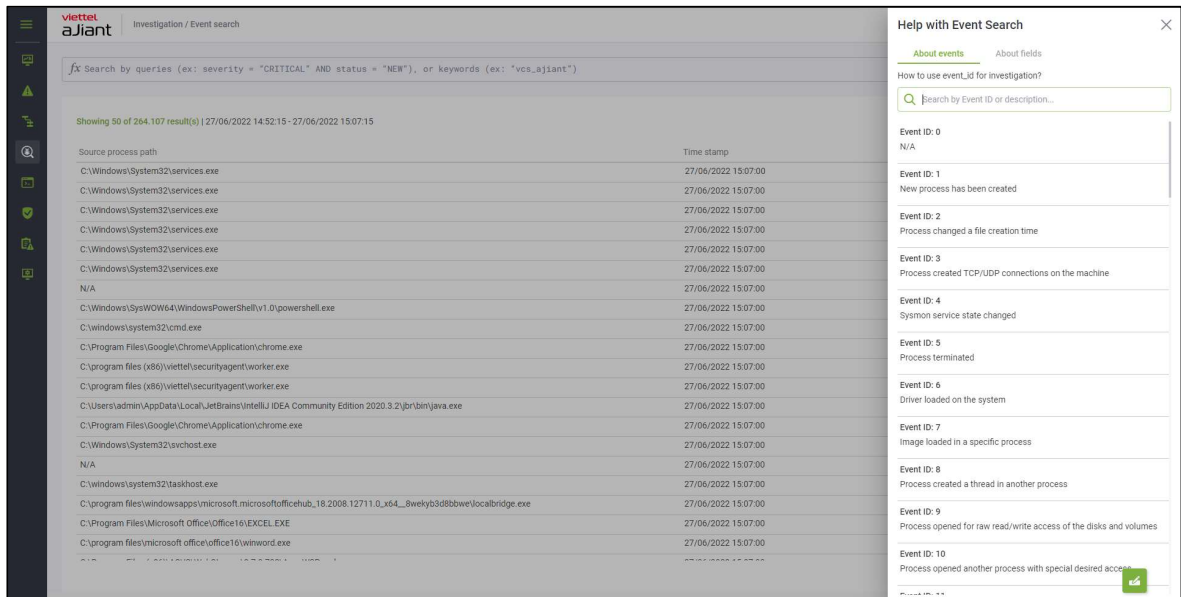
- Mục đích: tra thông tin event, ý nghĩa trường;
- Các bước thực hiện:

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.



3.5.2.4 Wrapt text

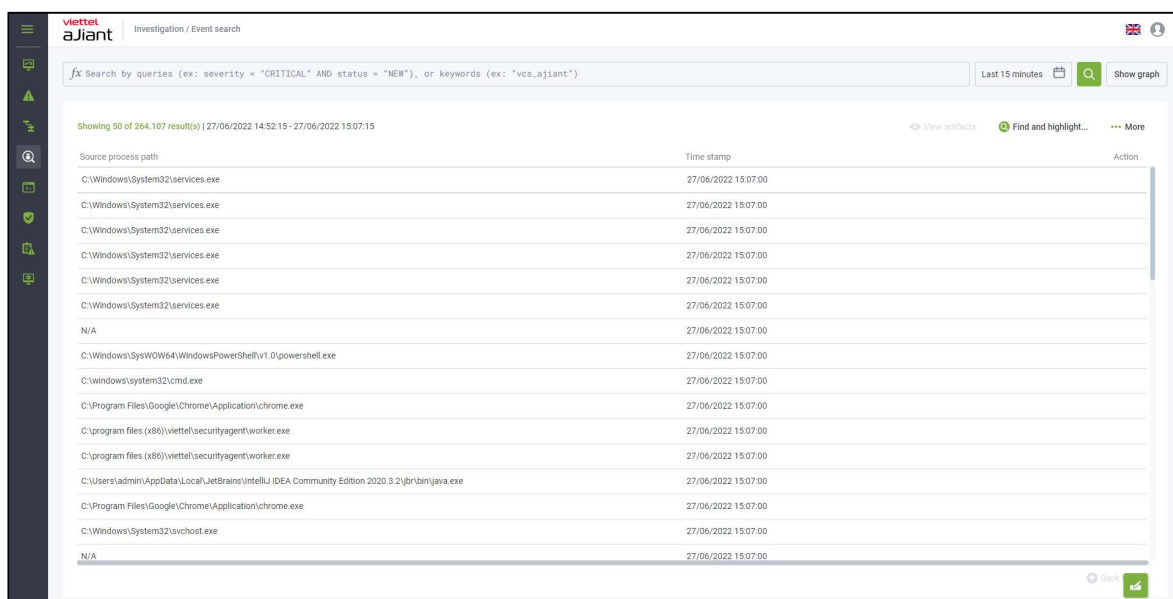
Mục đích: Có thể hiển thị toàn bộ dữ liệu hoặc thu gọn lại dữ liệu khi click vào nút “wrap text”;

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”;



3.5.2.5 Export Data

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

Các bước thực hiện:

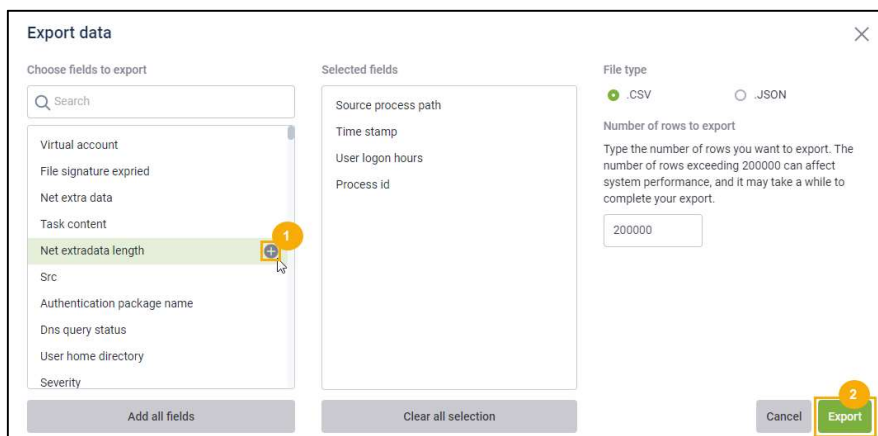
Bước 1: Tại màn hình Event Search, chọn “More”;

Bước 2: HT hiển thị danh sách các thao tác: Show columns, Wrap 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;



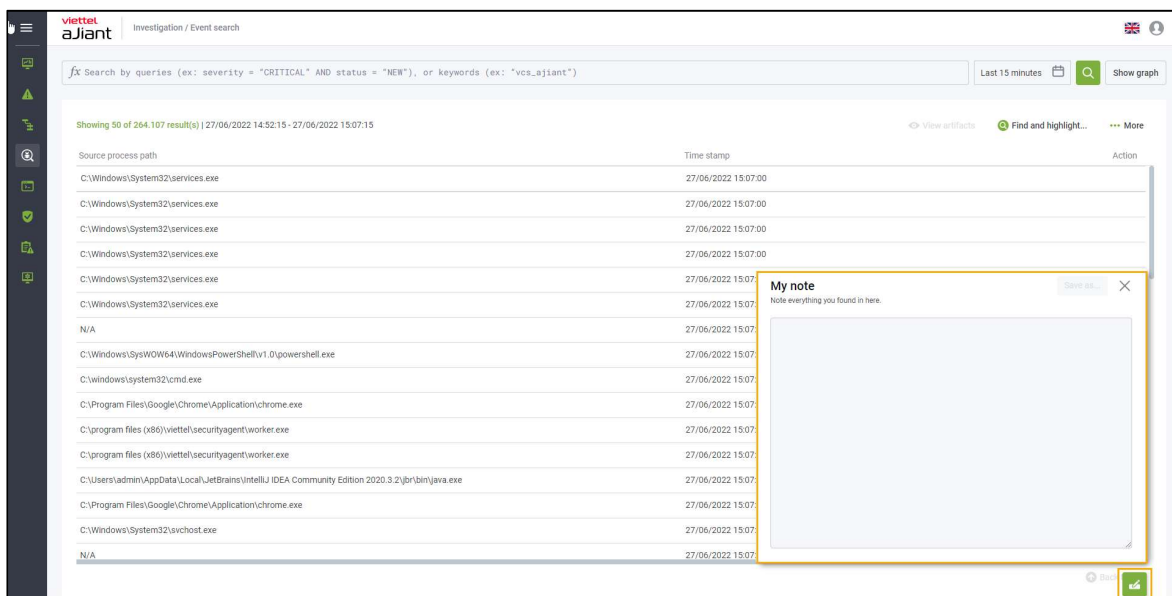
3.5.3 Note

Mục đích: Hiện 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 hiện 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”.



3.5.3.1 Xử lý Event

Marking artifact: Đánh dấu artifact;

Showing 50 of 120 result(s) | 17/06/2022 10:14:38 - 17/06/2022 10:29:38

Event id	Time stamp	File path	Target process path	File signature	Source process path	File signed	Hash md5	Action
1	17/06/2022 10:28:31	N/A	C:\Windows\servicing\TrustedInstaller.exe	Microsoft Windows	C:\Windows\System32\services.exe	true	N/A	1 Mark artifact
1	17/06/2022 10:28:31	N/A	C:\Windows\System32\more.com	Microsoft Windows	C:\Windows\System32\cmd.exe	true	N/A	
10	17/06/2022 10:28:31	N/A	C:\Windows\system32\lsass.exe	Sysinternals	C:\Users\admin\AppData\Local\Temp\procexp - Copy64.exe	true	N/A	
1	17/06/2022 10:28:31	N/A	C:\Windows\System32\SecEdit.exe	Microsoft Windows	C:\Windows\System32\cmd.exe	true	N/A	
1	17/06/2022 10:28:31	N/A	C:\Windows\System32\cmd.exe	Microsoft Windows	C:\Program Files\Ajan\proprietary\BLS\BLSutils.exe	true	N/A	
3	17/06/2022 10:28:31	N/A	N/A	N/A	C:\Windows\system32\svchost.exe	N/A	N/A	

Bước 1: Chọn 1 bản ghi bất kỳ và hover vào bản ghi đó. Thực hiện click vào nút icon “Marking artifact”. Trên màn hình sẽ hiển thị popup như sau:



+ ND có thể thực hiện chỉnh sửa và đánh dấu bằng cách:

- Chọn icon Edit and mark artifact;
- Edit đường dẫn (thông tin cần đánh dấu);
- Chọn icon Complete and Mark để kết thúc thao tác Edit and mark artifact;

Showing 50 of 120 result(s) | 17/06/2022 10:14:38 - 17/06/2022 10:29:38

Event id	Time stamp	File path	Target process path	File signature	Source process path	File signed	Hash md5	Action
1	17/06/2022 10:28:31	N/A	C:\Windows\servicing\TrustedInstaller.exe	Microsoft Windows	C:\Windows\System32\services.exe	true	N/A	1
1	17/06/2022 10:28:31	N/A	C:\Windows\System32\more.com	Microsoft Windows	C:\Windows\System32\cmd.exe			2
10	17/06/2022 10:28:31	N/A	C:\Windows\system32\lsass.exe	Sysinternals	C:\Users\admin\AppData\Local\Temp\procexp - Copy64.exe			3

Showing 50 of 120 result(s) | 17/06/2022 10:14:38 - 17/06/2022 10:29:38

Event id	Time stamp	File path	Target process path	File signature	Source process path	File signed	Hash md5	Action
1	17/06/2022 10:28:31	N/A	C:\Windows\servicing\TrustedInstaller.exe	Microsoft Windows	C:\Windows\System32\services.exe	true	N/A	4
1	17/06/2022 10:28:31	N/A	C:\Windows\System32\more.com	Microsoft Windows	C:\Windows\System32\cmd.exe			5
10	17/06/2022 10:28:31	N/A	C:\Windows\system32\lsass.exe	Sysinternals	C:\Users\admin\AppData\Local\Temp\procexp - Copy64.exe			6
1	17/06/2022 10:28:31	N/A	C:\Windows\System32\SecEdit.exe	Microsoft Windows	C:\Windows\System32\cmd.exe	true	N/A	7

+ ND chỉ đánh dấu Mark Artifact:

Showing 50 of 120 result(s) | 17/06/2022 10:14:38 - 17/06/2022 10:29:38

Event id	Time stamp	File path	Target process path	File signature	Source process path	File signed	Hash md5	Action
4624	17/06/2022 10:28:49	N/A	N/A	N/A	C:\Windows\System32\services.exe	N/A	N/A	
10	17/06/2022 10:28:31	N/A	C:\Windows\system32\lsass.exe	Sysinternals	C:\Users\admin\AppData\Local\Temp\groceip - Copy64.exe	true	N/A	
1	17/06/2022 10:28:31	N/A	C:\Windows\servicing\TrustedInstaller.exe	Microsoft Windows	C:\Windows\System32\services.exe	true	N/A	
1	17/06/2022 10:28:31	N/A	C:\Windows\System32\more.com	Microsoft Windows	C:\Windows\System32\cmd.exe			
10	17/06/2022 10:28:31	N/A	C:\Windows\system32\lsass.exe	Sysinternals	C:\Users\admin\AppData\Local\Temp\groceip - Copy64.exe			

1: Click on the artifact row.
2: Click on the 'Mark without edit' icon.

Hoặc chọn icon Cancel để bỏ đánh dấu marking artifact:

3	20/06/2022 11:32:03	N/A	N/A	N/A	C:\program files (x86)\google\chrome\application\chrome.exe	N/A	N/A	
1	20/06/2022 11:32:03	N/A	C:\Windows\System32\wbem\wmic.exe	Microsoft Windows	C:\Windows\System32\cmd.exe	true	N/A	
10	20/06/2022 11:32:03	N/A	C:\Windows\system32\lsass.exe	Microsoft Corporation	C:\Users\test\Desktop\SysinternalsSuite\lsass.exe			
1	20/06/2022 11:32:03	N/A	C:\Windows\System32\cmd.exe	Microsoft Windows	C:\Program Files\Ajan\propre\BLS\BLSUtil.exe			
1	20/06/2022 11:32:03	N/A	C:\Program Files\Ajan\propre\BLS\BLSUtil.exe	Viettel Group	C:\Program Files\Ajan\propre\BLS\BLSUtil.exe			
1	20/06/2022 11:32:03	N/A	C:\Windows\servicing\TrustedInstaller.exe	Microsoft Windows	C:\Windows\System32\services.exe			
13	20/06/2022 11:32:03	N/A	N/A	N/A	C:\Windows\System32\wbem\wmic.exe			
3	20/06/2022 11:32:03	N/A	N/A	N/A	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe			
11	20/06/2022 11:32:03	C:\Users\test\AppData\Local\Microsoft\Windows\CurrentControlSet\Services\EventLog\VEDR	N/A	N/A	C:\Windows\System32\cmd.exe			

Unmark artifact

Bước 2: Khi marking artifact thành công màn hình sẽ hiển thị thông báo:

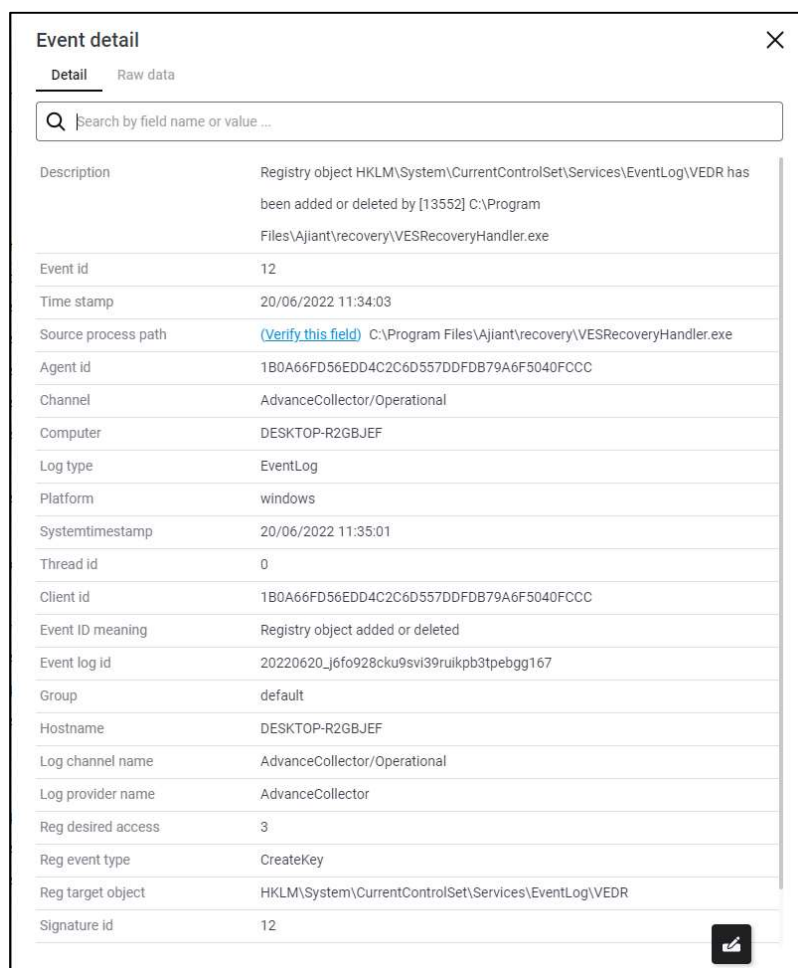


ND chọn nút “View artifacts” để chuyển đến màn hình danh sách Artifacts:

Time	Agent ID	Object	From	Action
☐ 20/06/2022 11:36:59	1B0A66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	C:\Program Files\Ajan\recovery\VESRecoveryHandler.exe	EVENT_LOG	
☐ 20/06/2022 11:38:23	1B0A66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	C:\program files (x86)\google\chrome\application\chrome.exe	EVENT_LOG	
☐ 20/06/2022 11:39:09	1B0A66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	C:\Windows\System32\cmd.exe	EVENT_LOG	
☐ 20/06/2022 11:39:14	1B0A66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	C:\Windows\system32\wbem\wmic.exe	EVENT_LOG	
☐ 20/06/2022 11:45:08	1B0A66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	C:\Windows\System32\wbem\en-US\csv	EVENT_LOG	
☐ 20/06/2022 11:48:10	1B0A66FD56EDD4C2C6D557DDFDB79A6F5040FCCC	HKLM\System\CurrentControlSet\Services\EventLog\VEDR	EVENT_LOG	

6 result(s) Back to top

Xem thông tin chi tiết event: ND chọn 1 bản ghi bất kỳ và hover vào bản ghi đó, click vào icon “Xem chi tiết” :



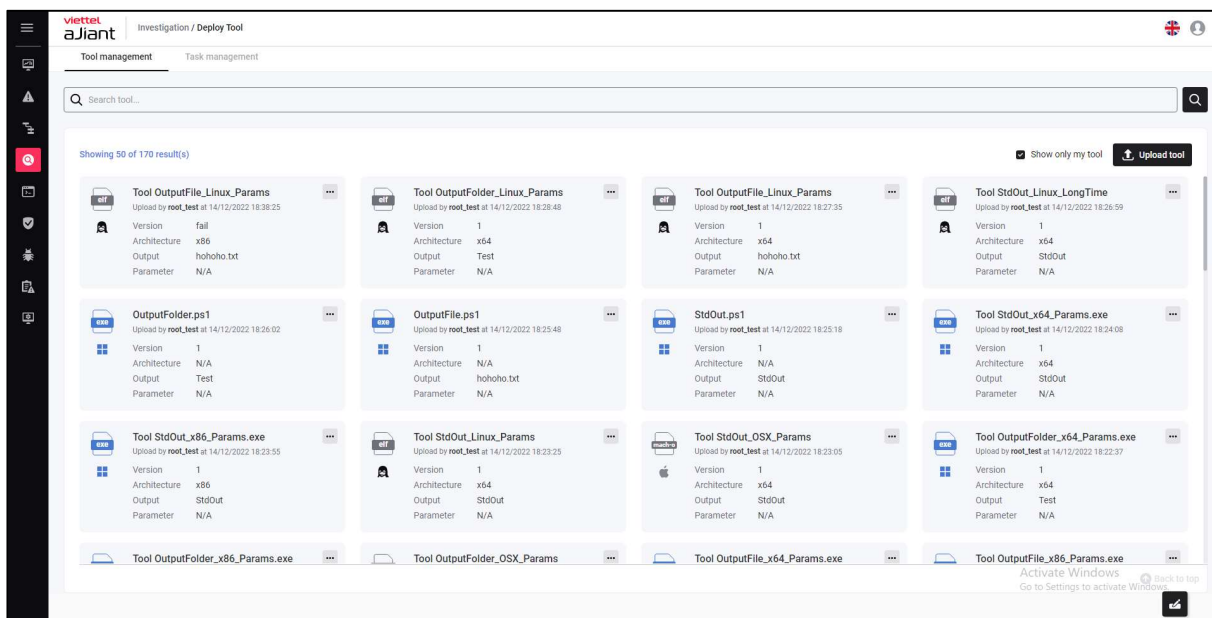
3.5.4 Investigation_Deploy Tools

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.

3.5.4.1 Tool Management

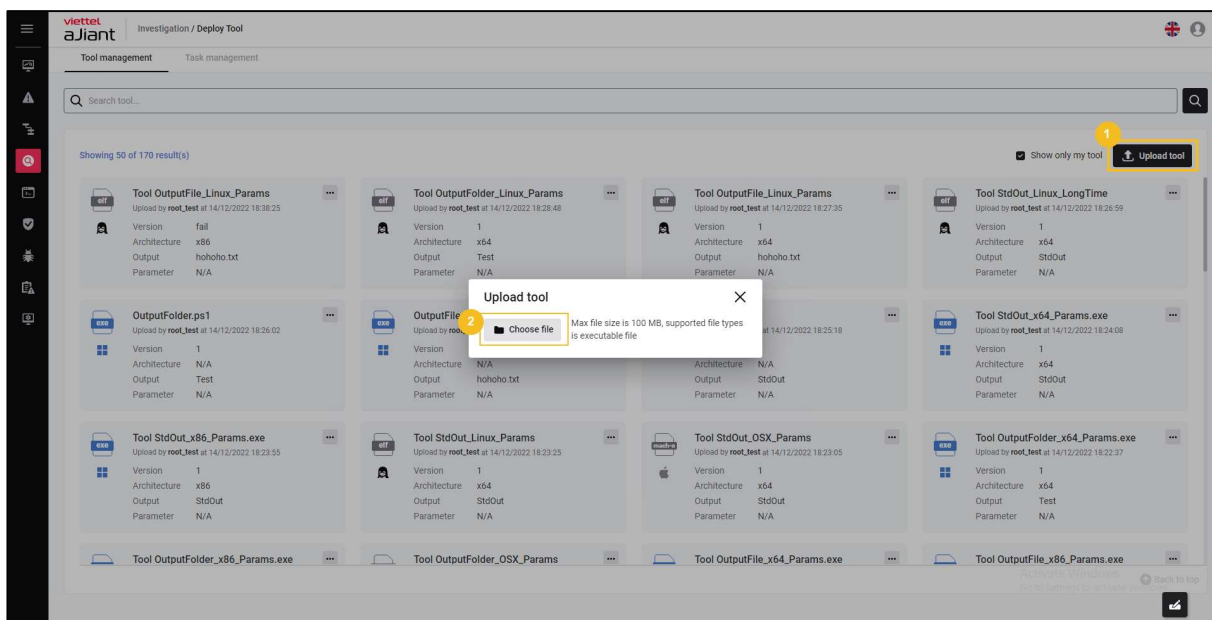
Mục đích: quản lý toàn bộ tool của hệ thống, người sử dụng có thể thêm/ xóa tool ở màn hình này. Các tính năng ở màn hình này gồm có:

- + 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;

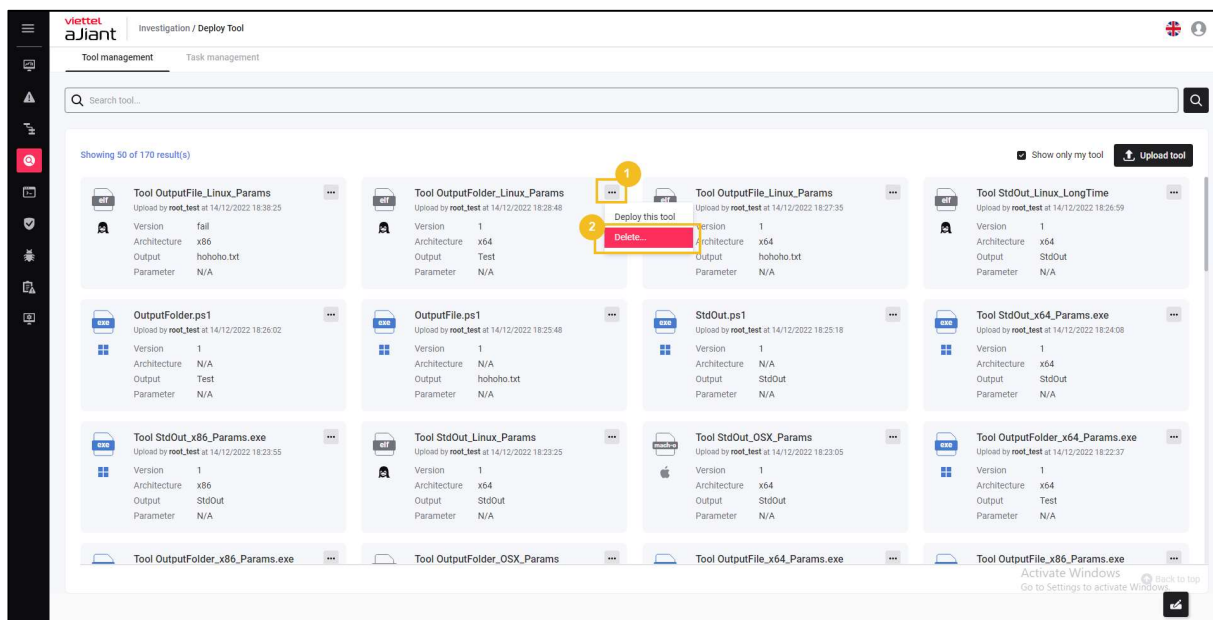


Với tính năng Upload tool thao tác theo các bước sau:

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**



3.5.4.2 Deploy tool

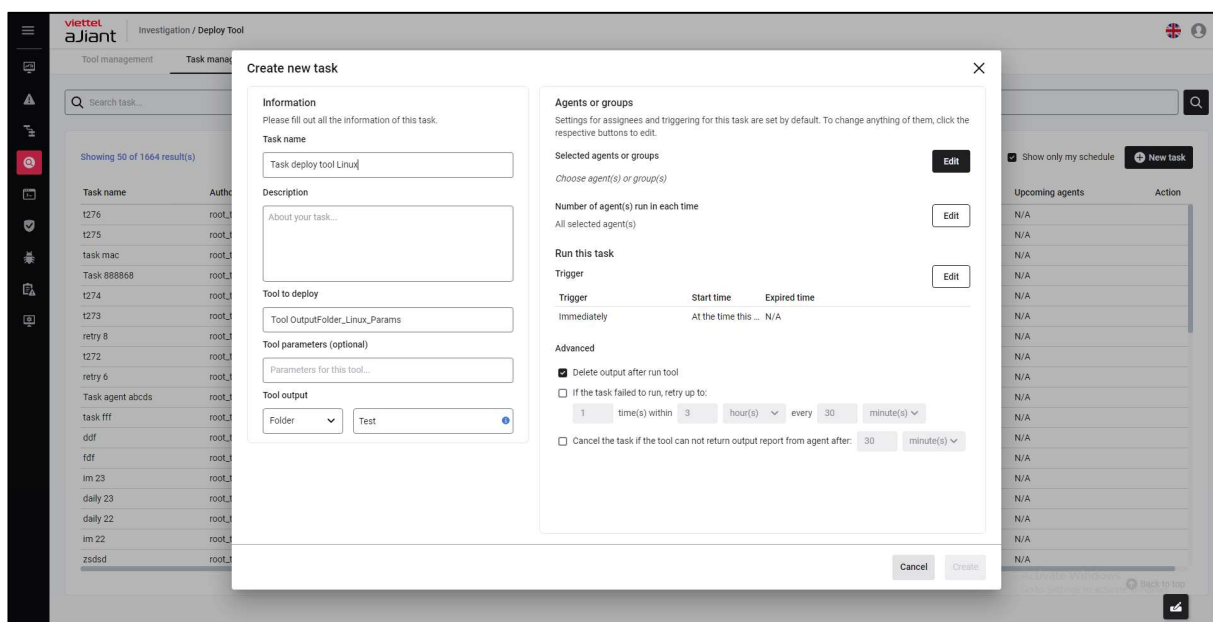
Mục đích: Cấu hình thông tin deploy tool dưới agent

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 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:

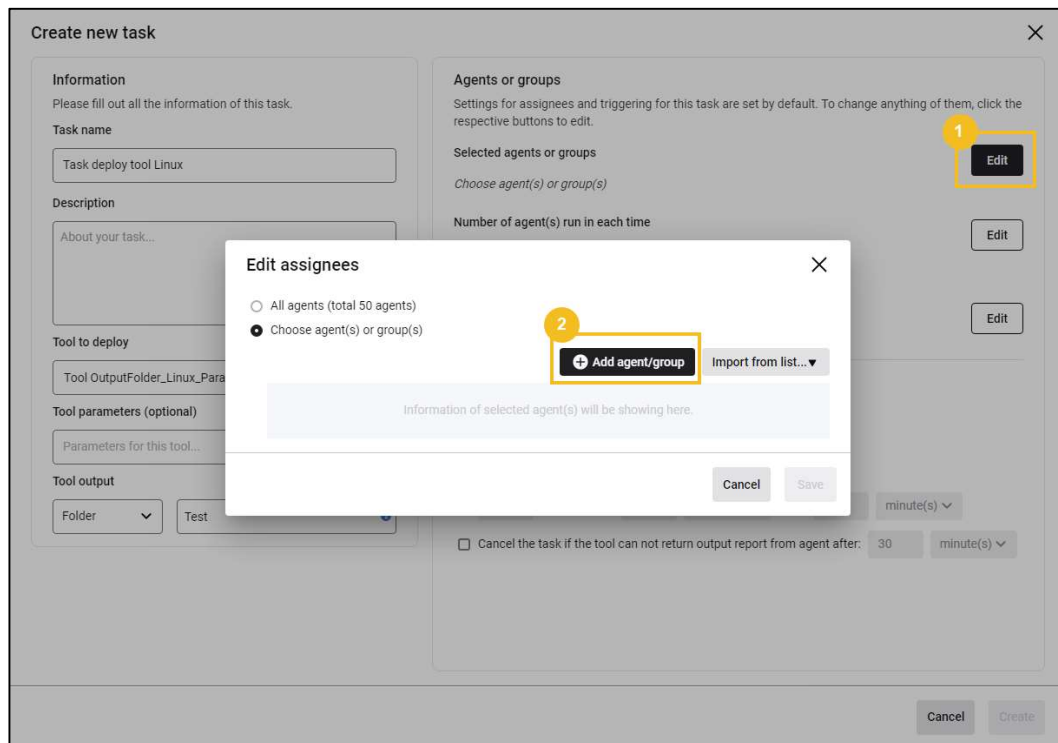


Bước 2: Thực hiện nhập các thông tin task để deploy tool: Task name, Description, Tool parameters, Tool output;

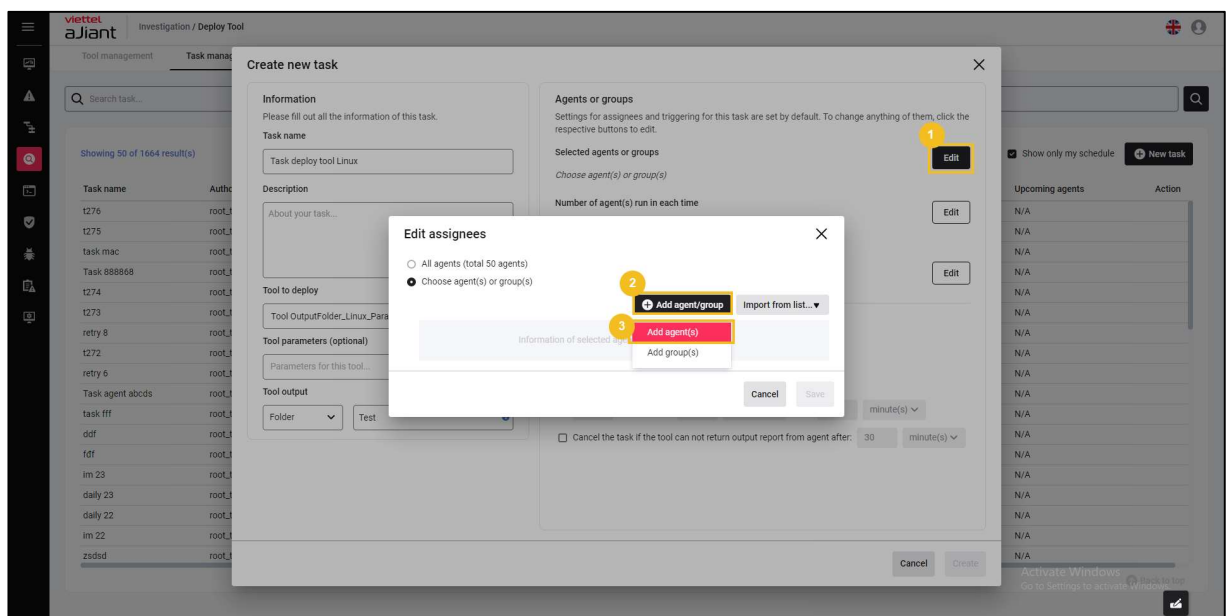
Bước 3: Lựa chọn thông tin nhóm (group), máy trạm (agent) để thực hiện deploy:

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;

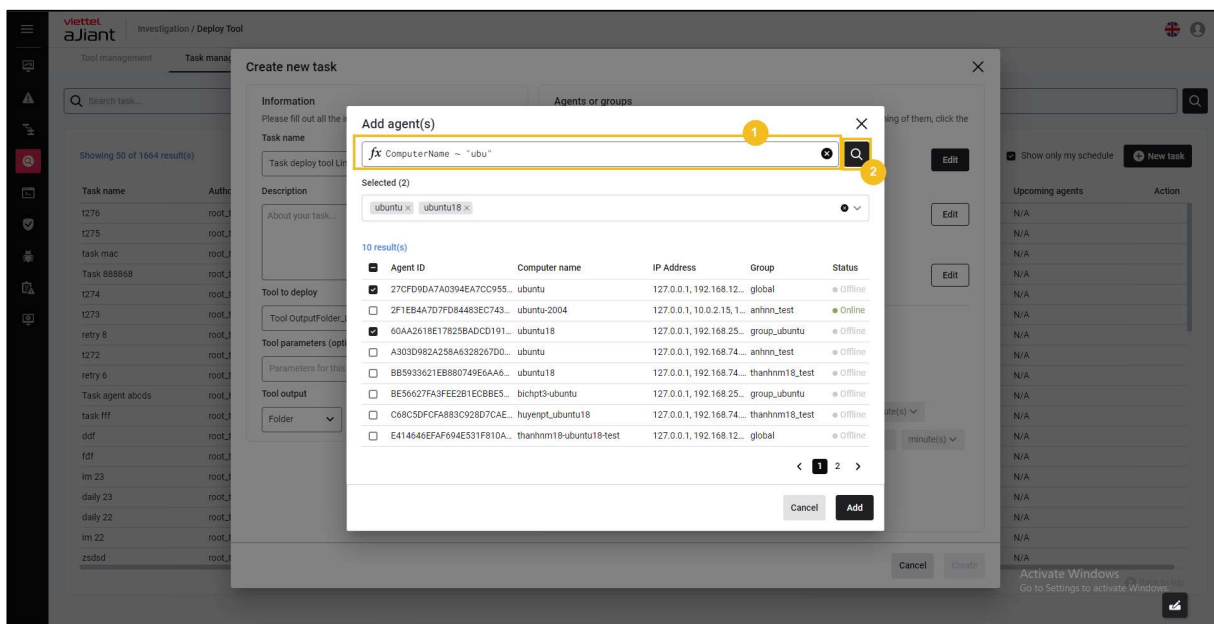
Lựa chọn agents or groups thực hiện deploy – **Choose agent(s) or group(s)**:



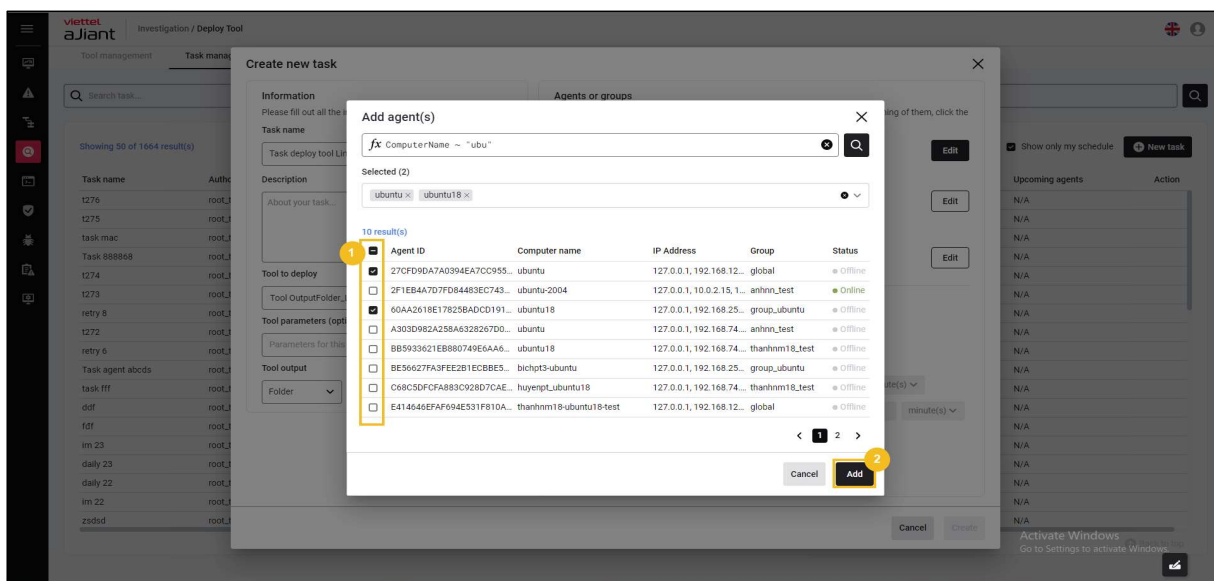
+ Chọn Add agent(s):



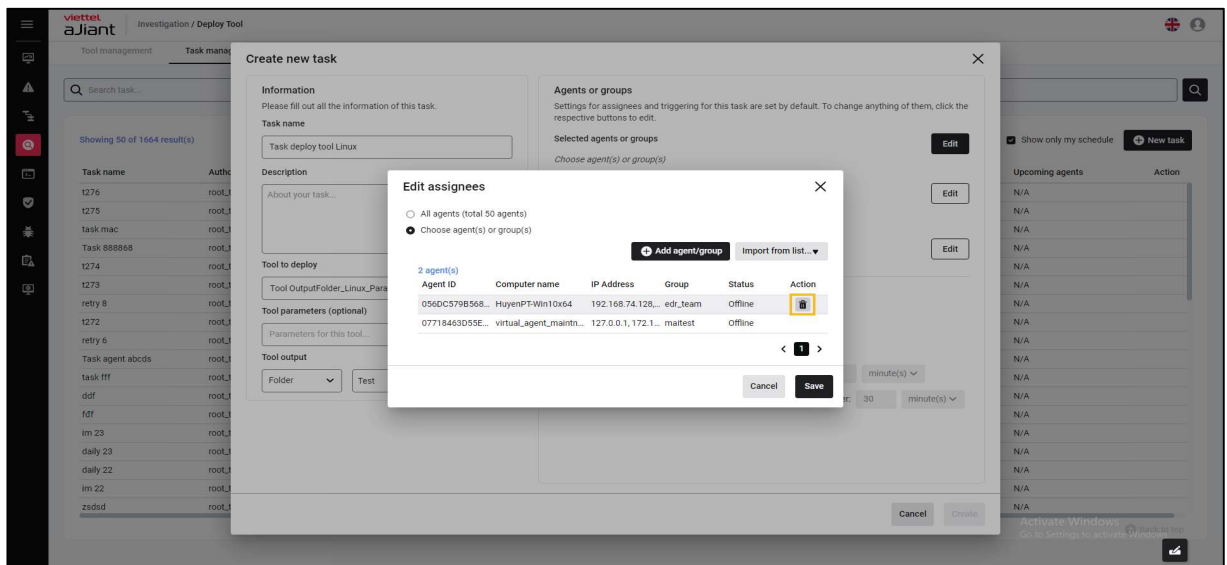
- **Tìm kiếm Agent:** Cho phép tạo câu lệnh truy vấn, sử dụng câu lệnh truy vấn để tìm kiếm Agent



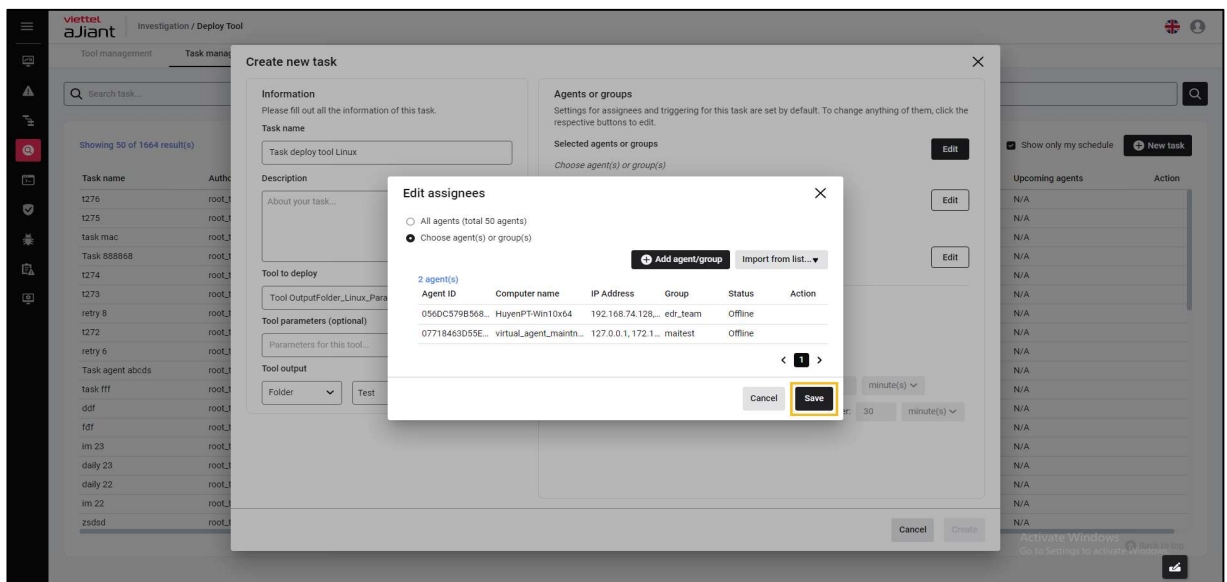
- Chọn Agent(s) để deploy bằng cách tích chọn vào một hoặc nhiều Agent(s) > Thông tin Agent(s) đã được chọn hiển thị ở khung **Selected** > chọn **Cancel** để hủy thao tác thêm Agent để deploy hoặc chọn nút **Add** để xác nhận danh sách Agent(s):



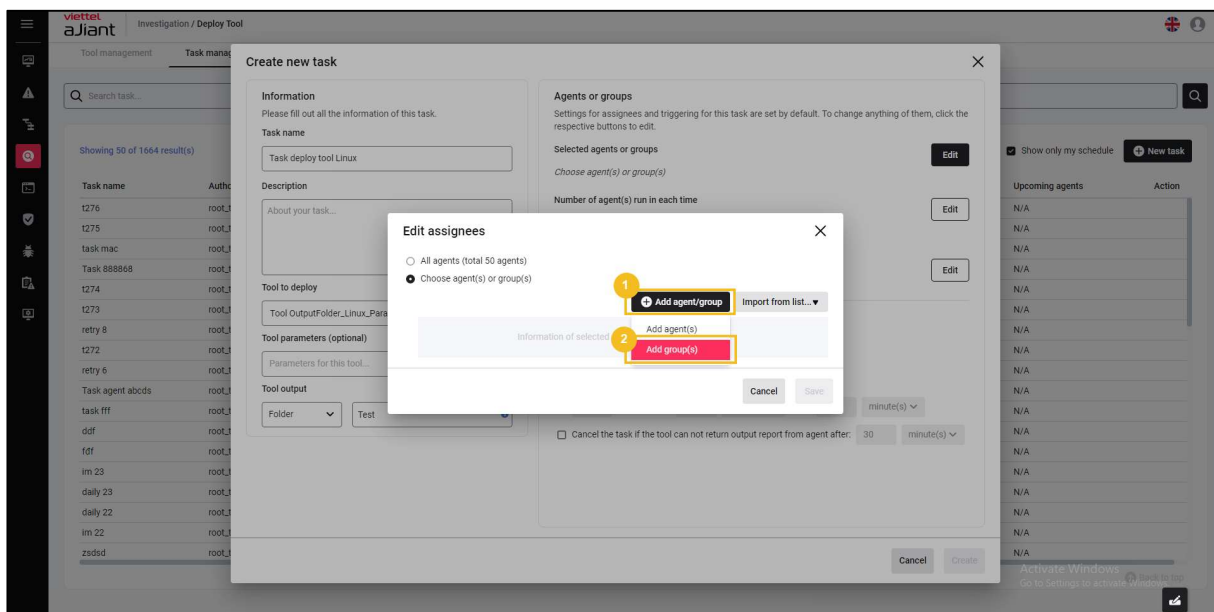
- Hover vào các Agent(s) đã chọn > Chọn icon  để thực hiện loại bỏ Agent(s) khỏi danh sách đã chọn



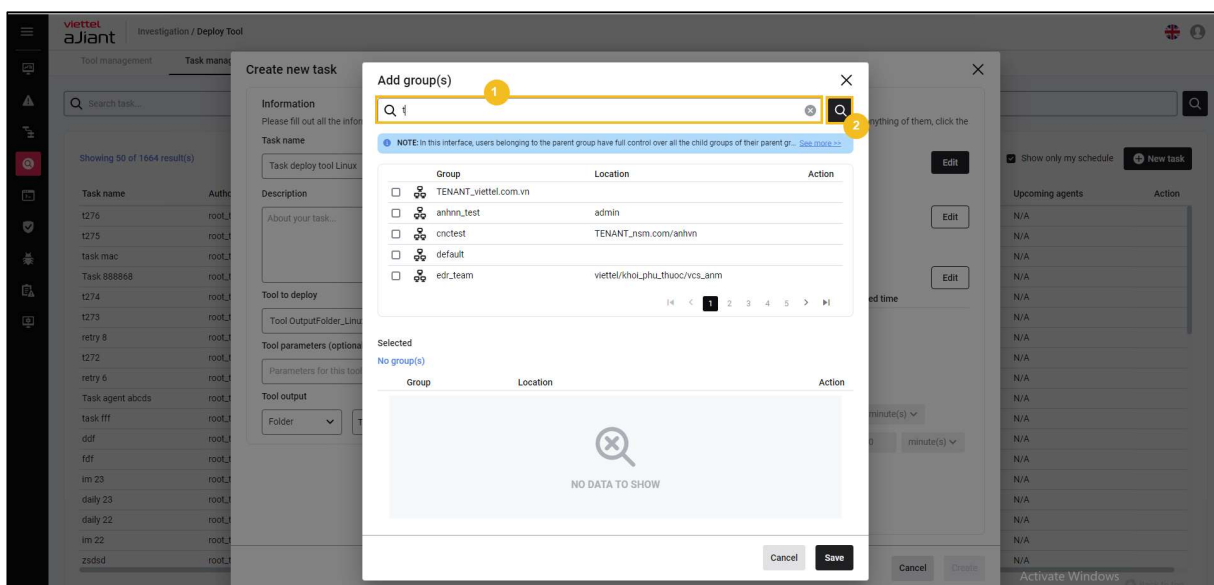
- Chọn **Cancel** để hủy hoặc chọn **Save** để lưu thông tin các Agent(s) đã chọn để deploy:



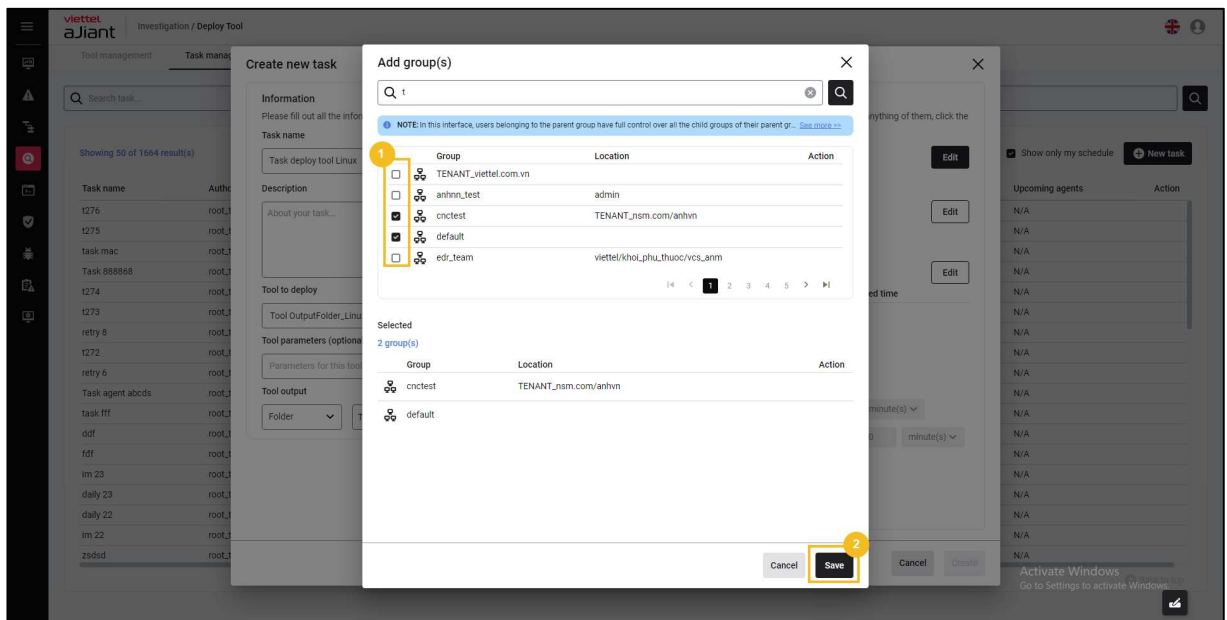
- + Chọn **Add group(s)**:



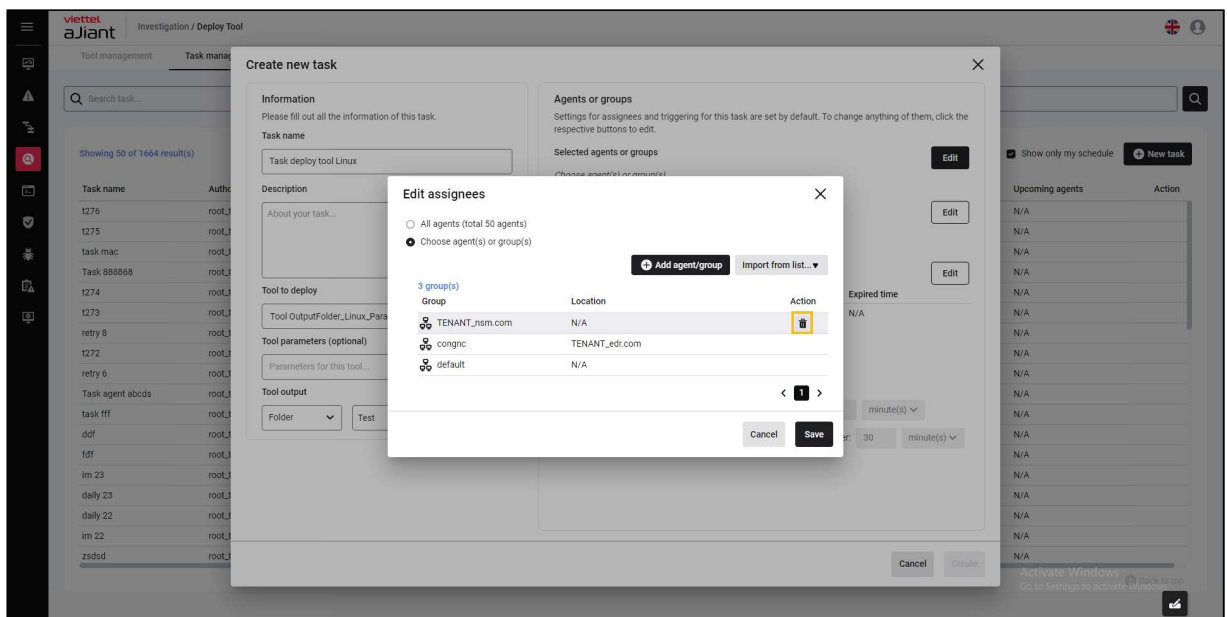
- Tìm kiếm group(s) theo tên, cho phép nhập từ khóa tìm kiếm group theo tên group:



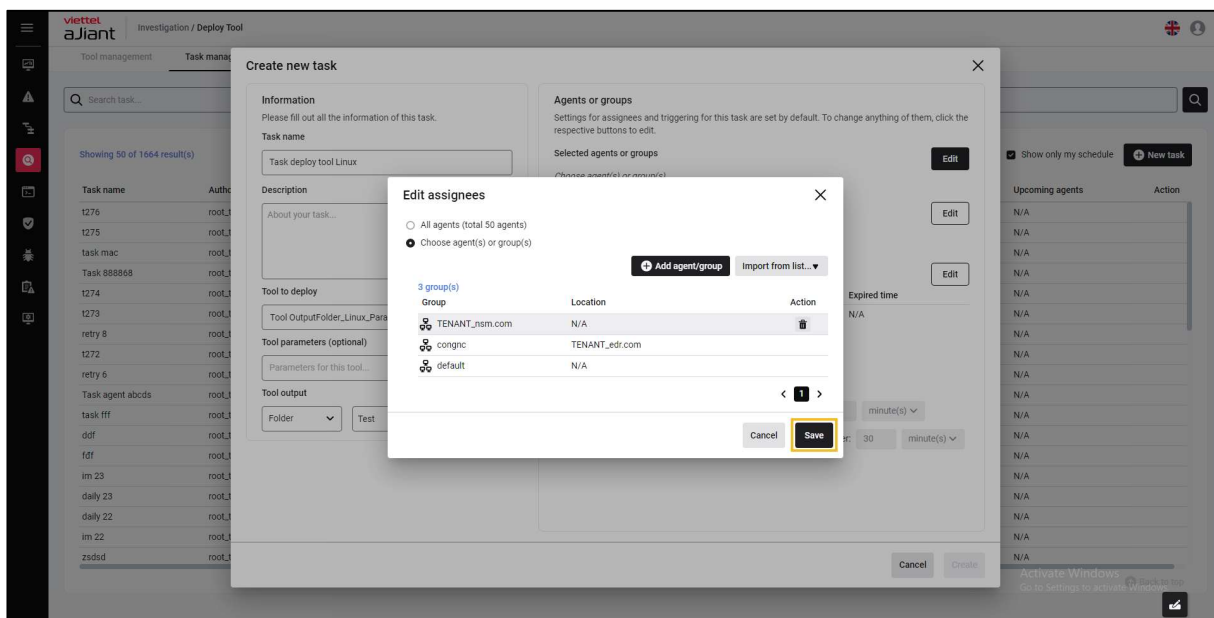
- Chọn group(s) để deploy bằng cách tích chọn vào một hoặc nhiều group(s) > Thông tin group(s) đã được chọn hiển thị ở khung **Selected** > chọn **Cancel** để hủy thao tác thêm group(s) để deploy hoặc chọn nút **Save** để xác nhận danh sách group(s):



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

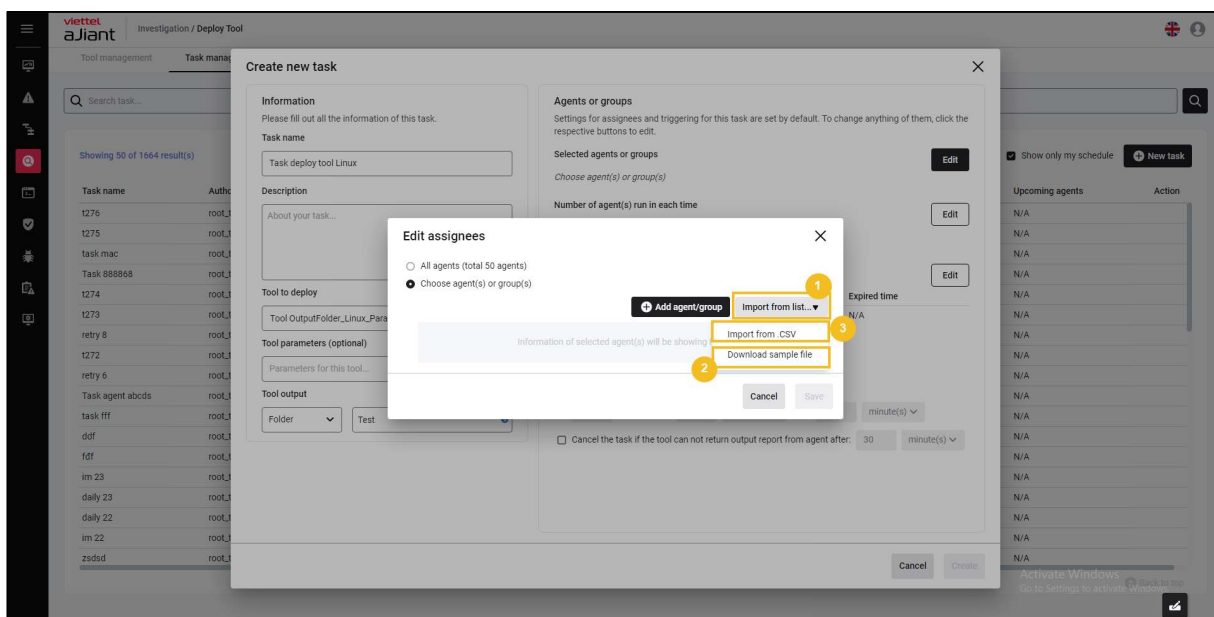


- Chọn **Cancel** để hủy hoặc Chọn **Save** các group(s) đã chọn để deploy:



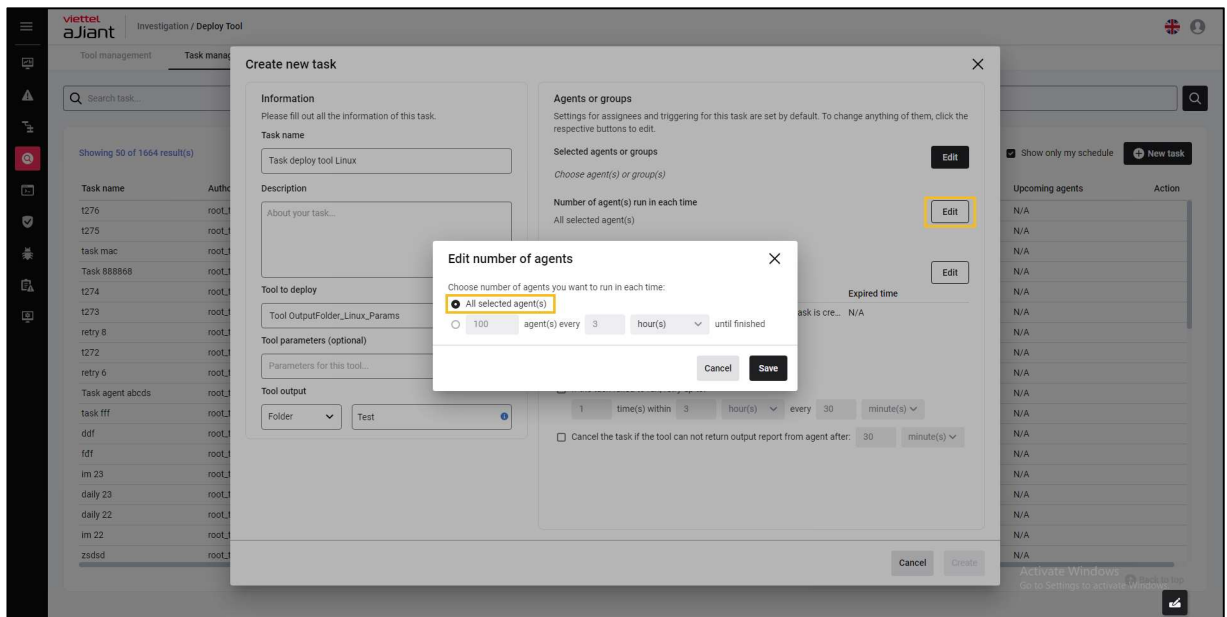
+ Import from list: Cho phép upload danh sách agent(s) từ file .csv > Chọn **Import from list**

- 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)

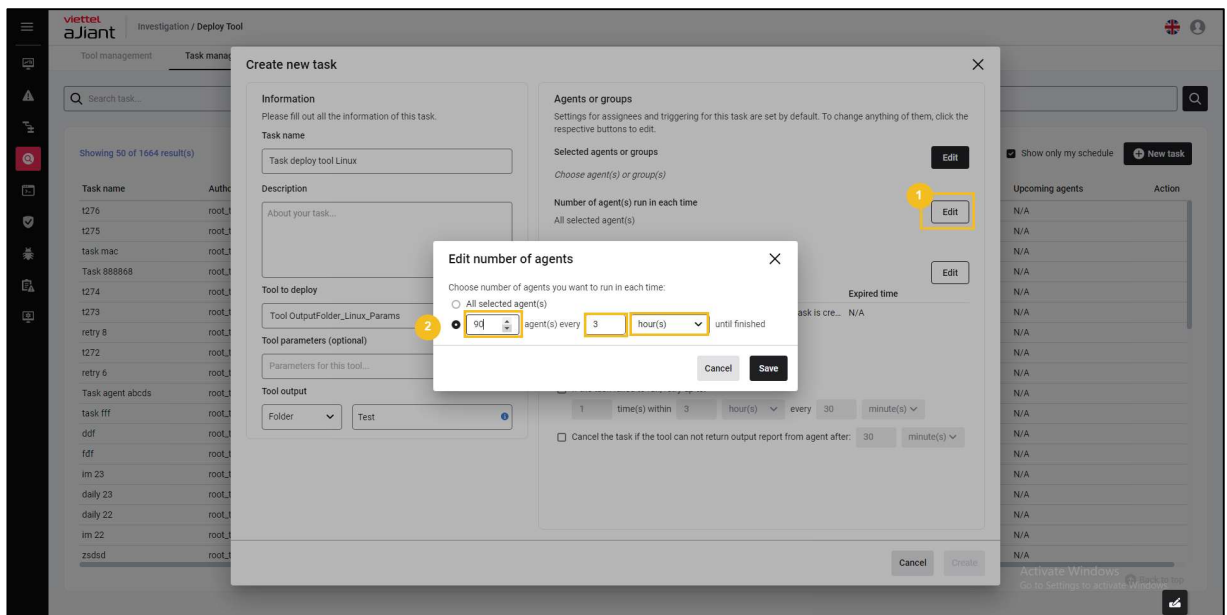


Bước 4: Cấu hình số lượng agent deploy tool mỗi lần:

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

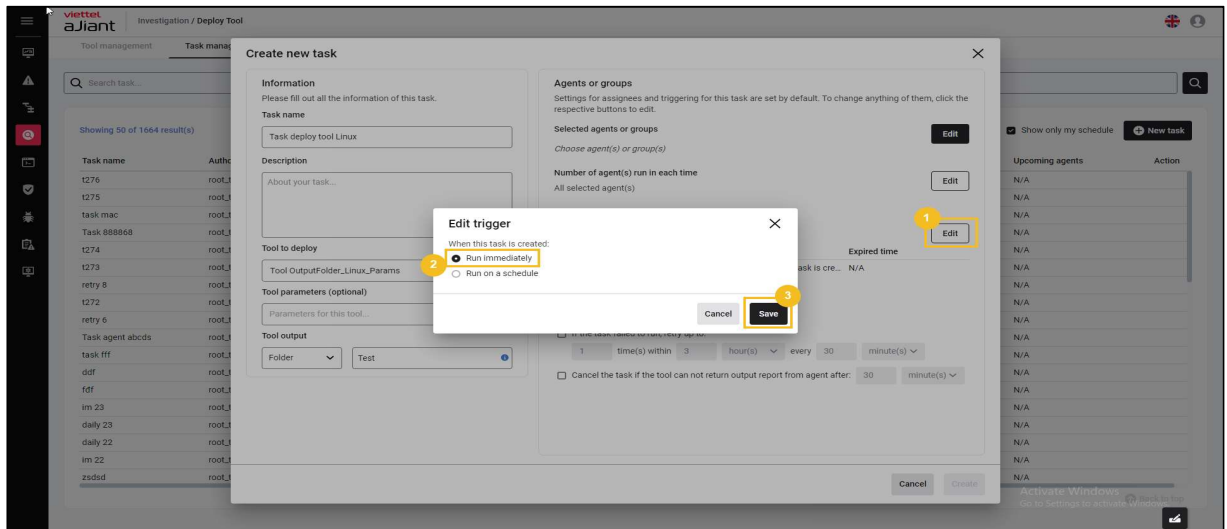


- + Cấu hình số lượng agent mỗi lần deploy:



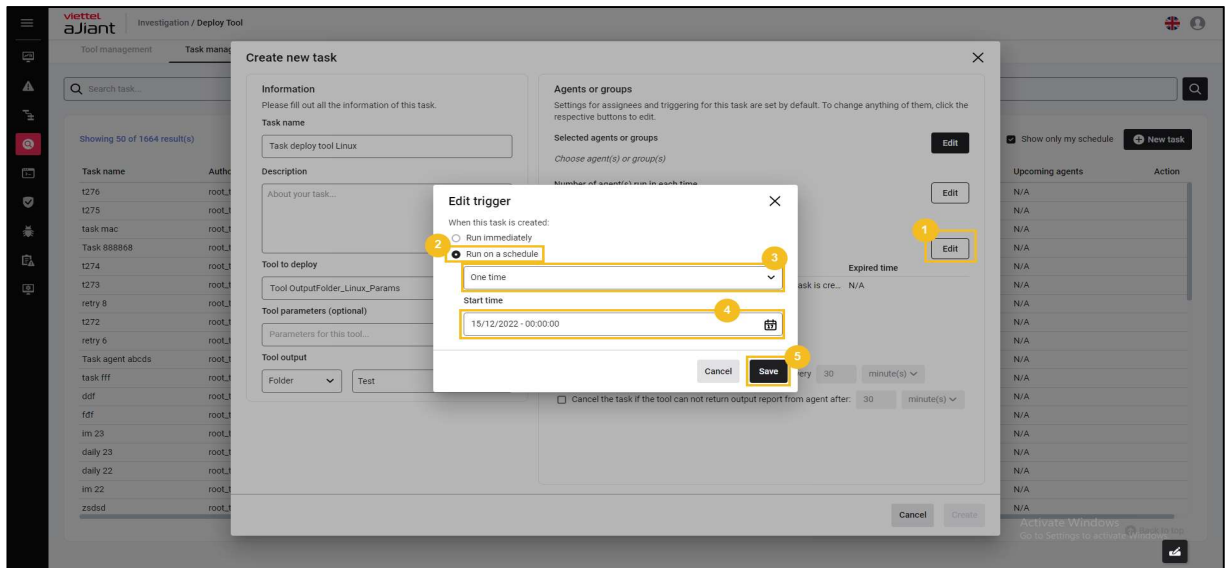
Bước 5: Cấu hình thông tin thời gian (lập lịch) thực hiện deploy tool:

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



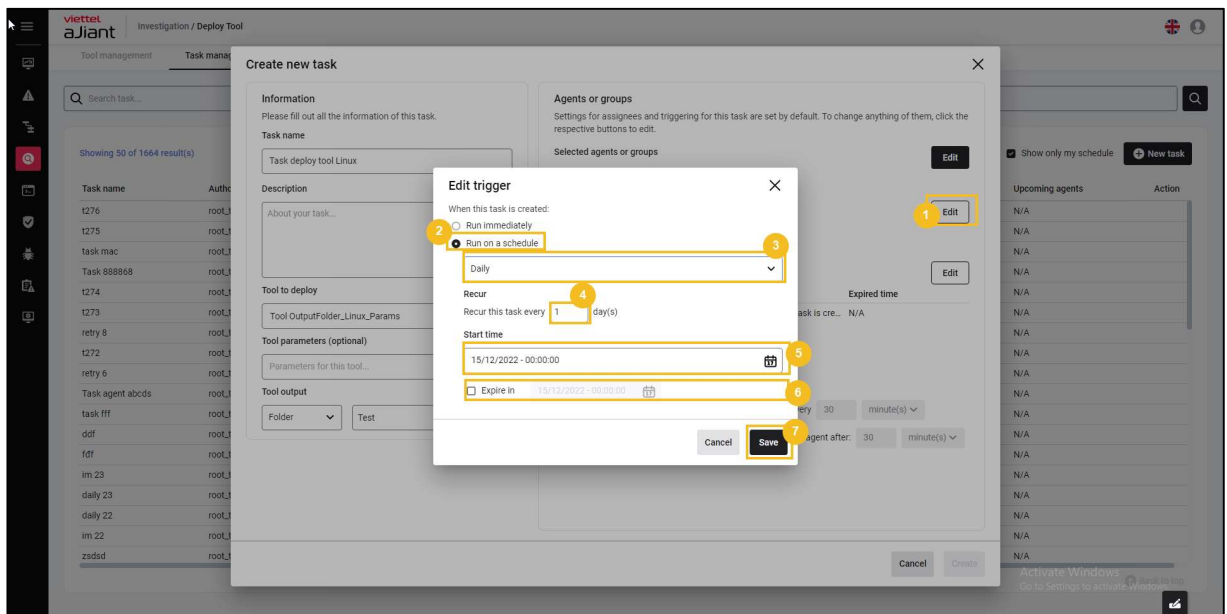
+ Chọn **Run on schedule** để thực hiện cấu hình thời gian deploy tool theo lập lịch:

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

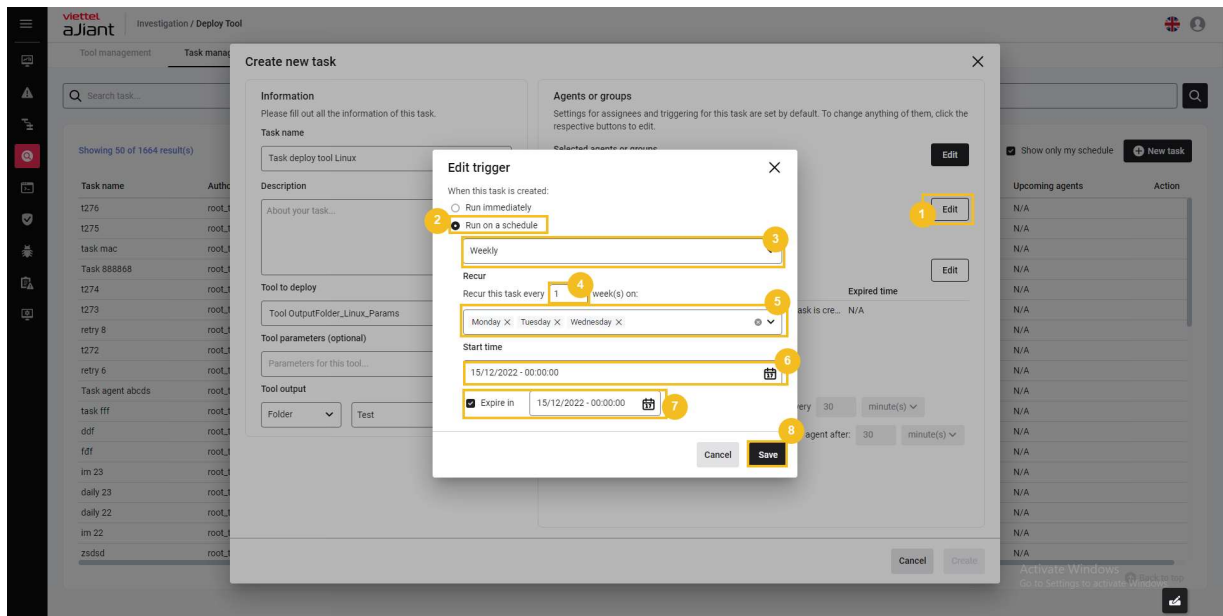


- Chọn schedule **Daily**:
 - Cho phép lập lịch deploy tool hàng ngày;

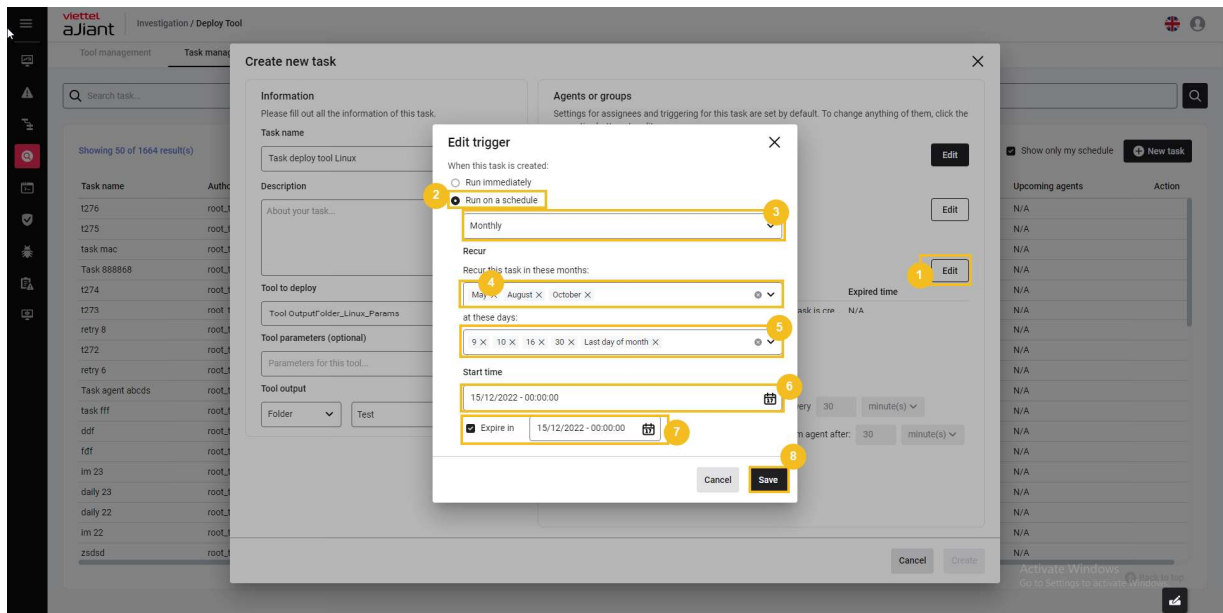
- Thời gian lặp lại;
- Cấu hình thời gian bắt đầu và kết thúc:



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

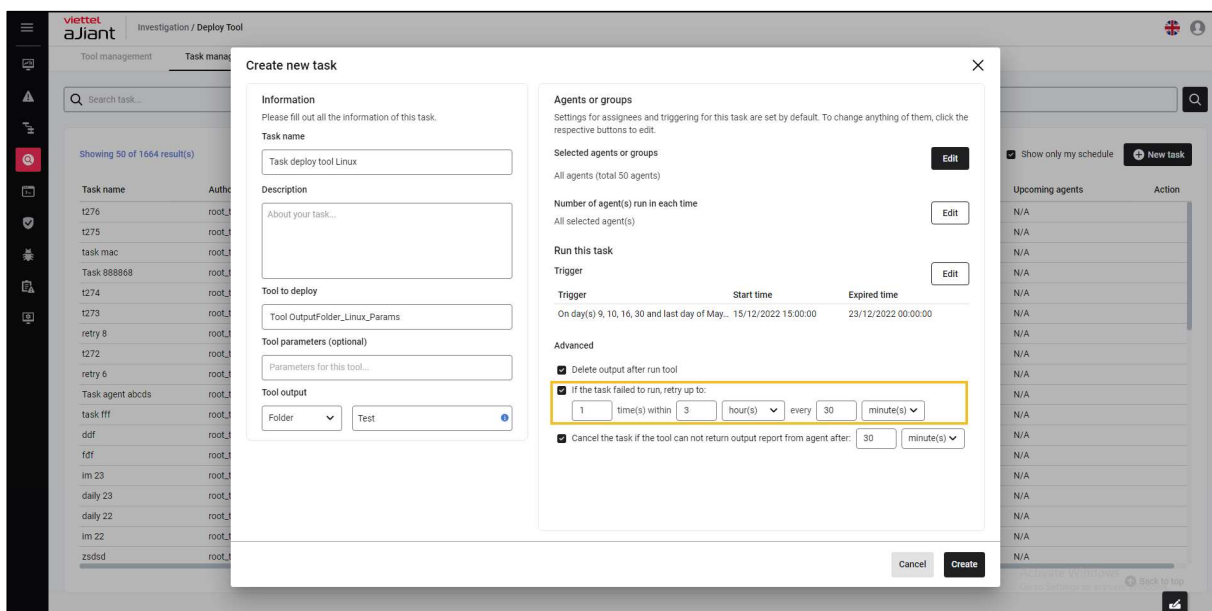


- Chọn schedule **Monthly**:
 - Cho phép lập lịch deploy tool hàng tháng;
 - Thời gian lặp lại;
 - Cấu hình thời gian bắt đầu và kết thúc:

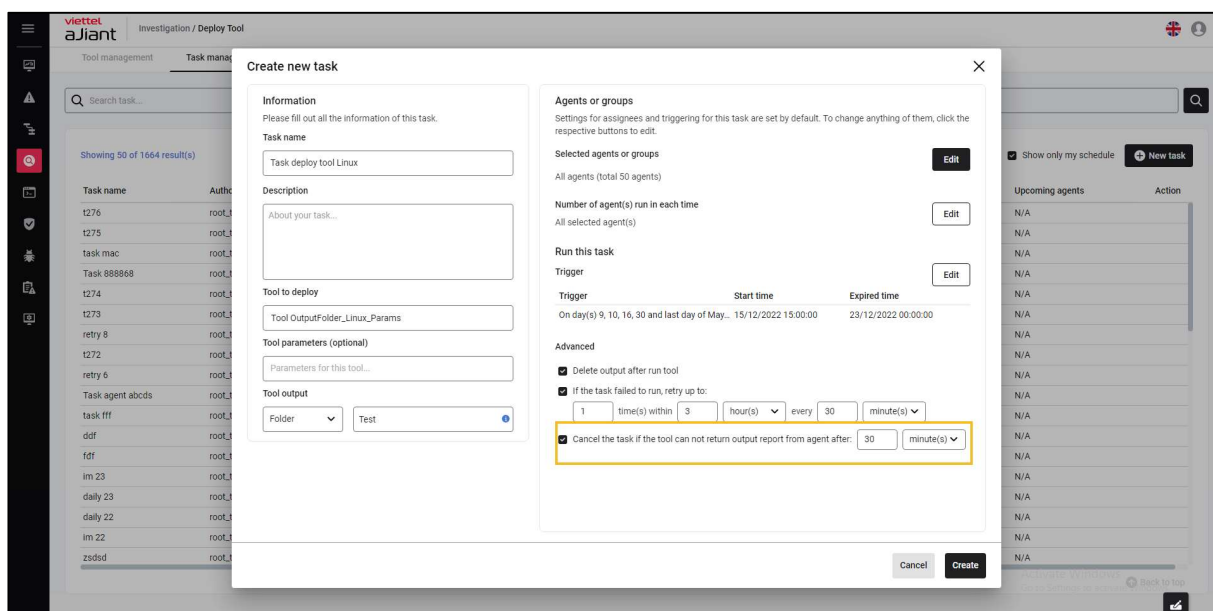


Bước 6: Cấu hình thông tin nâng cao cho task

- + **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:



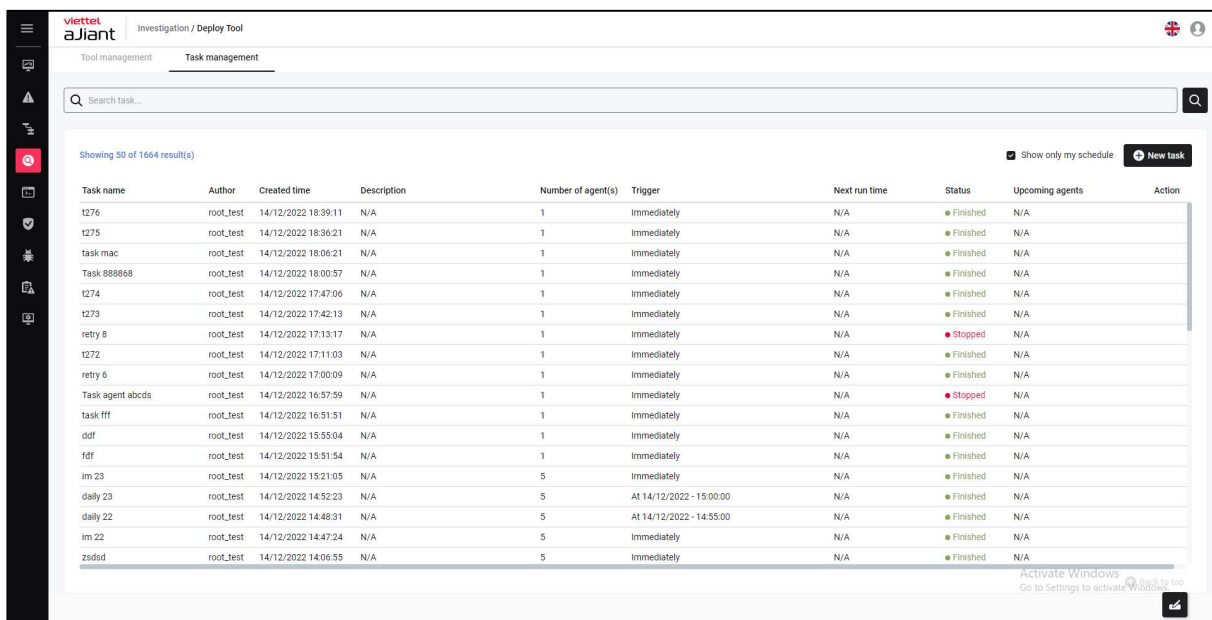
Bước 7: Chọn **Create** để tạo mới task/ cấu hình thông tin deploy tool dưới agent hoặc chọn **Cancel** để hủy task/ hủy cấu hình thông tin deploy tool dưới agent

3.5.4.3 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



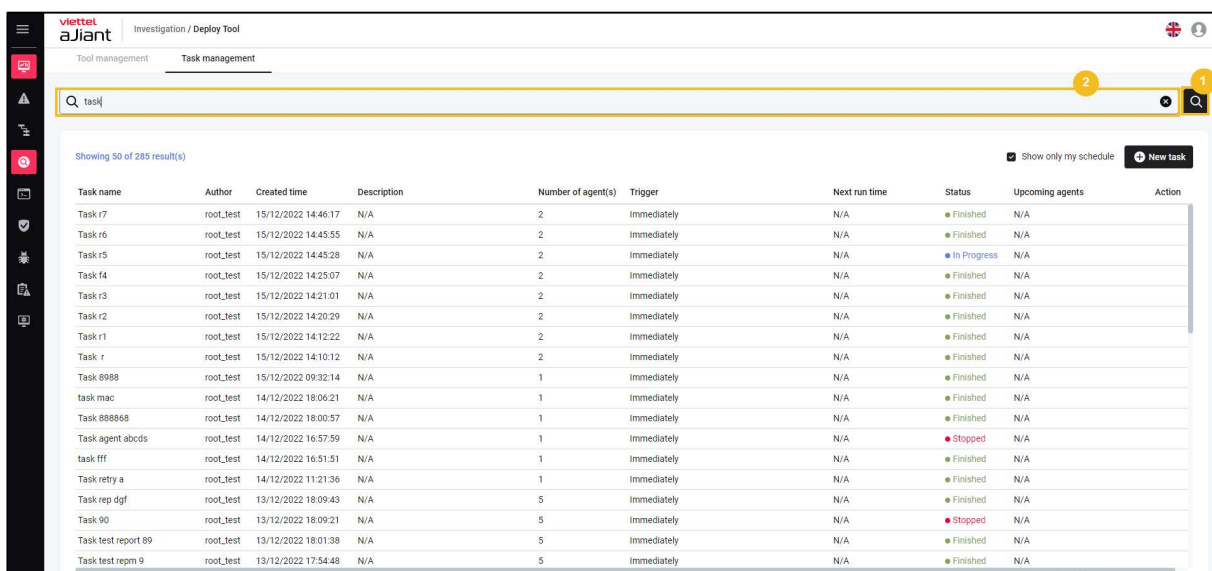
The screenshot shows the 'Task management' section of the Viettel aJiant interface. A search bar at the top contains the text 'Search task...'. Below it, a table lists 50 tasks (out of 1664 results). The table columns are: Task name, Author, Created time, Description, Number of agent(s), Trigger, Next run time, Status, Upcoming agents, and Action. The tasks listed include 't276', 't275', 'task mac', 'Task 888868', 't274', 't273', 'retry 8', 't272', 'retry 6', 'Task agent abcds', 'task fff', 'ddf', 'fdf', 'im 23', 'daily 23', 'daily 22', 'im 22', and 'zedds'.

Task name	Author	Created time	Description	Number of agent(s)	Trigger	Next run time	Status	Upcoming agents	Action
t276	root_test	14/12/2022 18:39:11	N/A	1	Immediately	N/A	Finished	N/A	
t275	root_test	14/12/2022 18:36:21	N/A	1	Immediately	N/A	Finished	N/A	
task mac	root_test	14/12/2022 18:06:21	N/A	1	Immediately	N/A	Finished	N/A	
Task 888868	root_test	14/12/2022 18:00:57	N/A	1	Immediately	N/A	Finished	N/A	
t274	root_test	14/12/2022 17:47:06	N/A	1	Immediately	N/A	Finished	N/A	
t273	root_test	14/12/2022 17:42:13	N/A	1	Immediately	N/A	Finished	N/A	
retry 8	root_test	14/12/2022 17:13:17	N/A	1	Immediately	N/A	Stopped	N/A	
t272	root_test	14/12/2022 17:11:03	N/A	1	Immediately	N/A	Finished	N/A	
retry 6	root_test	14/12/2022 17:00:09	N/A	1	Immediately	N/A	Finished	N/A	
Task agent abcds	root_test	14/12/2022 16:57:59	N/A	1	Immediately	N/A	Stopped	N/A	
task fff	root_test	14/12/2022 16:51:51	N/A	1	Immediately	N/A	Finished	N/A	
ddf	root_test	14/12/2022 15:55:04	N/A	1	Immediately	N/A	Finished	N/A	
fdf	root_test	14/12/2022 15:51:54	N/A	1	Immediately	N/A	Finished	N/A	
im 23	root_test	14/12/2022 15:21:05	N/A	5	Immediately	N/A	Finished	N/A	
daily 23	root_test	14/12/2022 14:52:23	N/A	5	At 14/12/2022 - 15:00:00	N/A	Finished	N/A	
daily 22	root_test	14/12/2022 14:48:31	N/A	5	At 14/12/2022 - 14:55:00	N/A	Finished	N/A	
im 22	root_test	14/12/2022 14:47:24	N/A	5	Immediately	N/A	Finished	N/A	
zedds	root_test	14/12/2022 14:06:55	N/A	5	Immediately	N/A	Finished	N/A	

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 tin Agent liên quan đến từ khóa tìm kiếm có trong hệ thống:



The screenshot shows the 'Task management' section of the Viettel aJiant interface with a search bar containing 'task'. The results show 50 tasks (out of 285 results). The table columns are: Task name, Author, Created time, Description, Number of agent(s), Trigger, Next run time, Status, Upcoming agents, and Action. The tasks listed include 'Task r7', 'Task r6', 'Task r5', 'Task f4', 'Task r3', 'Task r2', 'Task r1', 'Task r', 'Task 8088', 'task mac', 'Task 888868', 'Task agent abcds', 'task fff', 'Task retry a', 'Task rep dgf', 'Task 90', 'Task test report 89', and 'Task test repm 9'.

Task name	Author	Created time	Description	Number of agent(s)	Trigger	Next run time	Status	Upcoming agents	Action
Task r7	root_test	15/12/2022 14:46:17	N/A	2	Immediately	N/A	Finished	N/A	
Task r6	root_test	15/12/2022 14:45:55	N/A	2	Immediately	N/A	Finished	N/A	
Task r5	root_test	15/12/2022 14:45:28	N/A	2	Immediately	N/A	In Progress	N/A	
Task f4	root_test	15/12/2022 14:25:07	N/A	2	Immediately	N/A	Finished	N/A	
Task r3	root_test	15/12/2022 14:21:01	N/A	2	Immediately	N/A	Finished	N/A	
Task r2	root_test	15/12/2022 14:20:29	N/A	2	Immediately	N/A	Finished	N/A	
Task r1	root_test	15/12/2022 14:12:22	N/A	2	Immediately	N/A	Finished	N/A	
Task r	root_test	15/12/2022 14:10:12	N/A	2	Immediately	N/A	Finished	N/A	
Task 8088	root_test	15/12/2022 09:32:14	N/A	1	Immediately	N/A	Finished	N/A	
task mac	root_test	14/12/2022 18:06:21	N/A	1	Immediately	N/A	Finished	N/A	
Task 888868	root_test	14/12/2022 18:00:57	N/A	1	Immediately	N/A	Finished	N/A	
Task agent abcds	root_test	14/12/2022 16:57:59	N/A	1	Immediately	N/A	Stopped	N/A	
task fff	root_test	14/12/2022 16:51:51	N/A	1	Immediately	N/A	Finished	N/A	
Task retry a	root_test	14/12/2022 11:21:36	N/A	1	Immediately	N/A	Finished	N/A	
Task rep dgf	root_test	13/12/2022 18:09:43	N/A	5	Immediately	N/A	Finished	N/A	
Task 90	root_test	13/12/2022 18:09:21	N/A	5	Immediately	N/A	Stopped	N/A	
Task test report 89	root_test	13/12/2022 18:01:38	N/A	5	Immediately	N/A	Finished	N/A	
Task test repm 9	root_test	13/12/2022 17:54:48	N/A	5	Immediately	N/A	Finished	N/A	

c. Tạo task

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

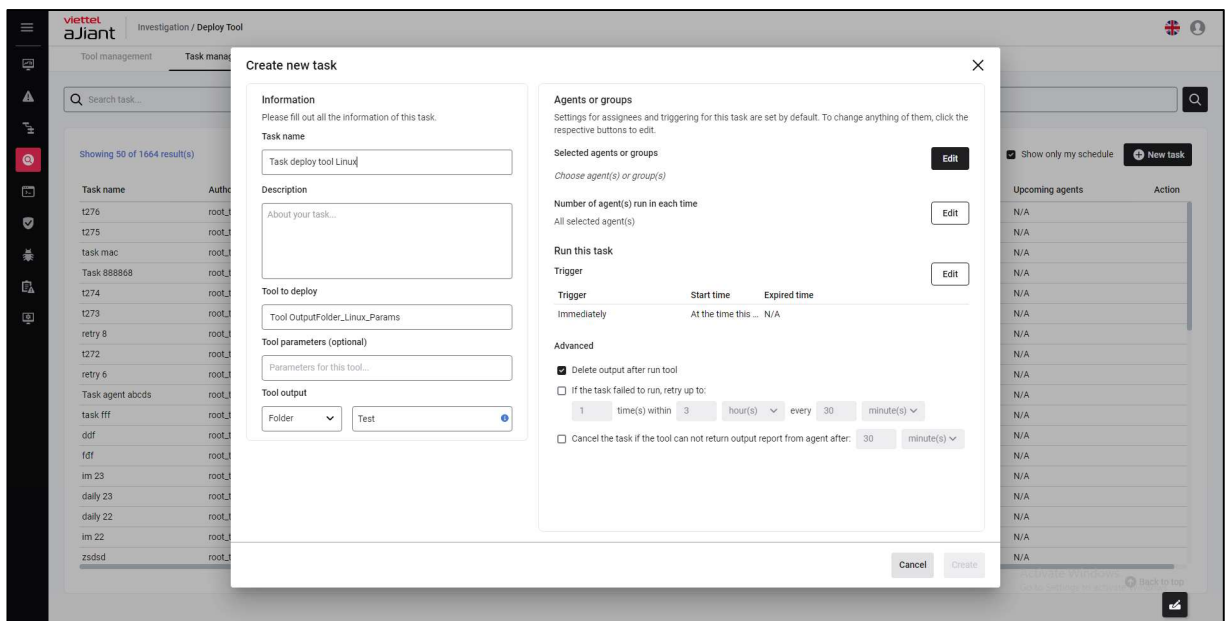
Mục đích: Cấu hình thông tin deploy tool dưới agent

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:

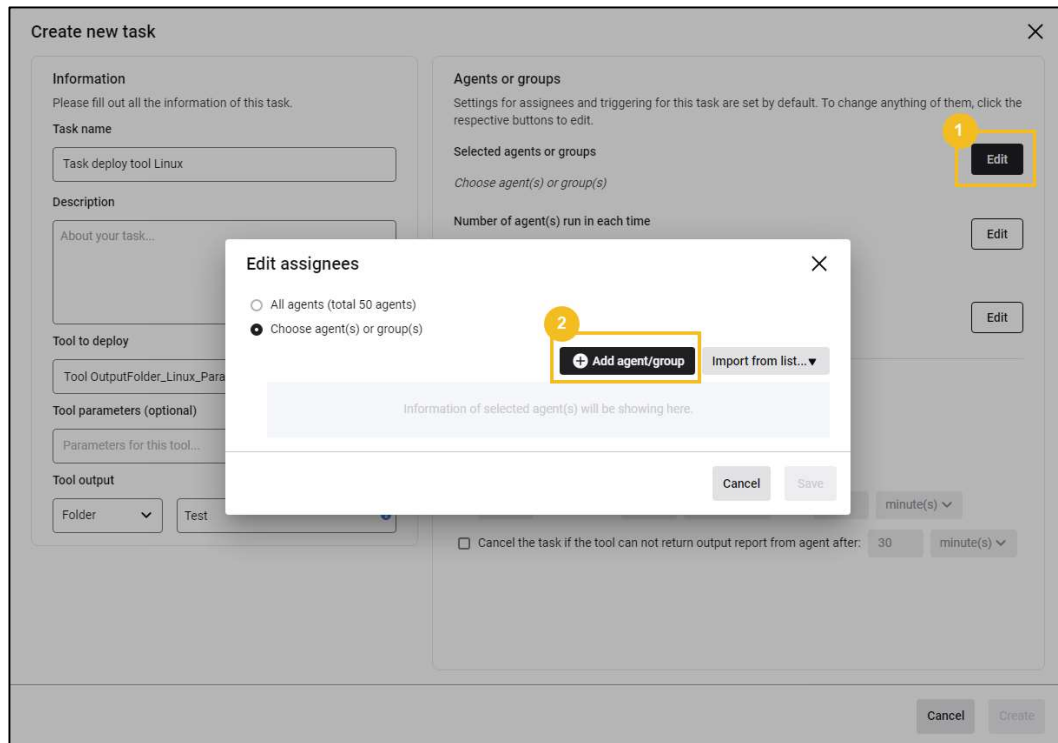


Bước 2: Thực hiện nhập các thông tin task để deploy tool: Task name, Tool to deploy, Description, Tool parameters, Tool output;

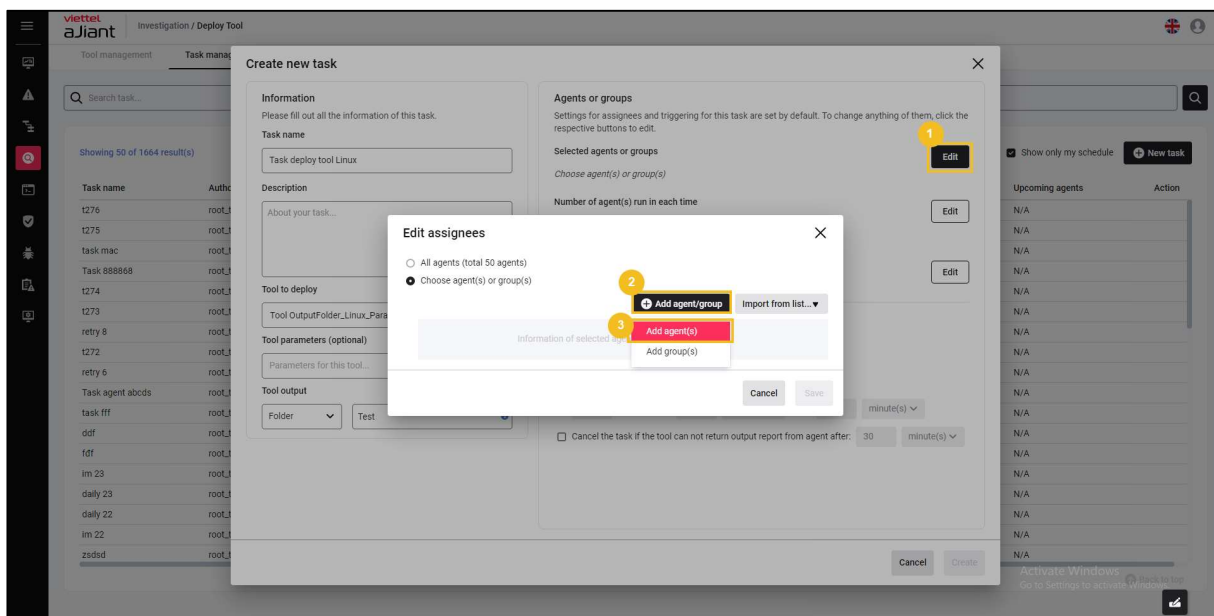
Bước 3: Lựa chọn thông tin nhóm (group), máy trạm (agent) để thực hiện deploy:

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;

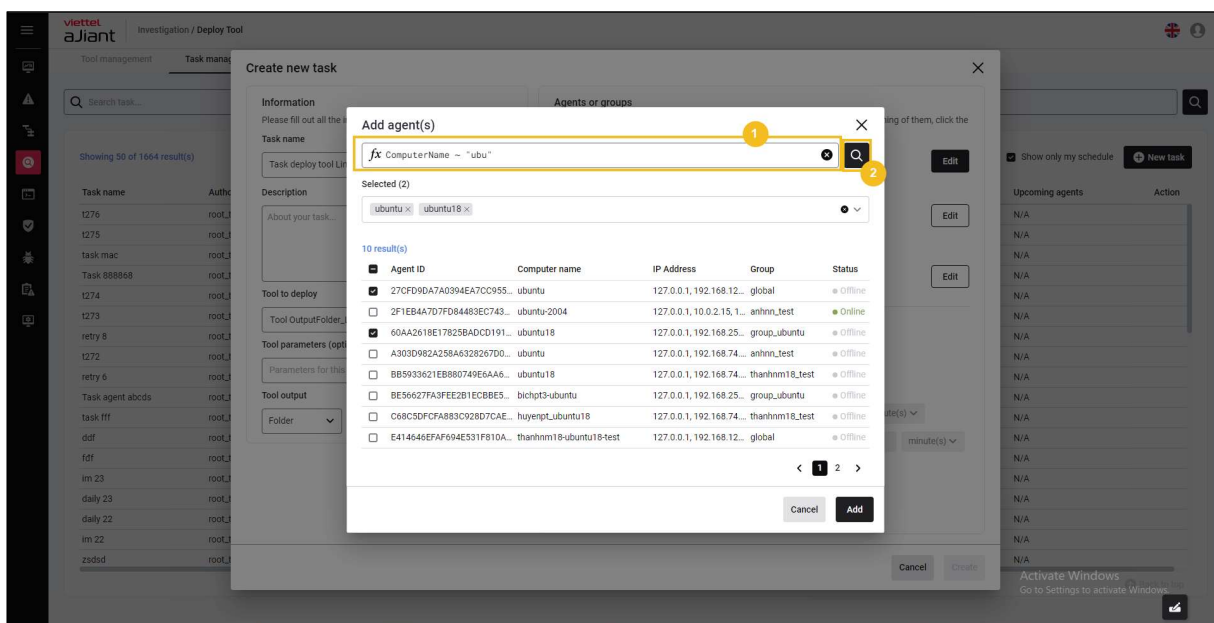
Lựa chọn agents or groups thực hiện deploy – **Choose agent(s) or group(s)**:



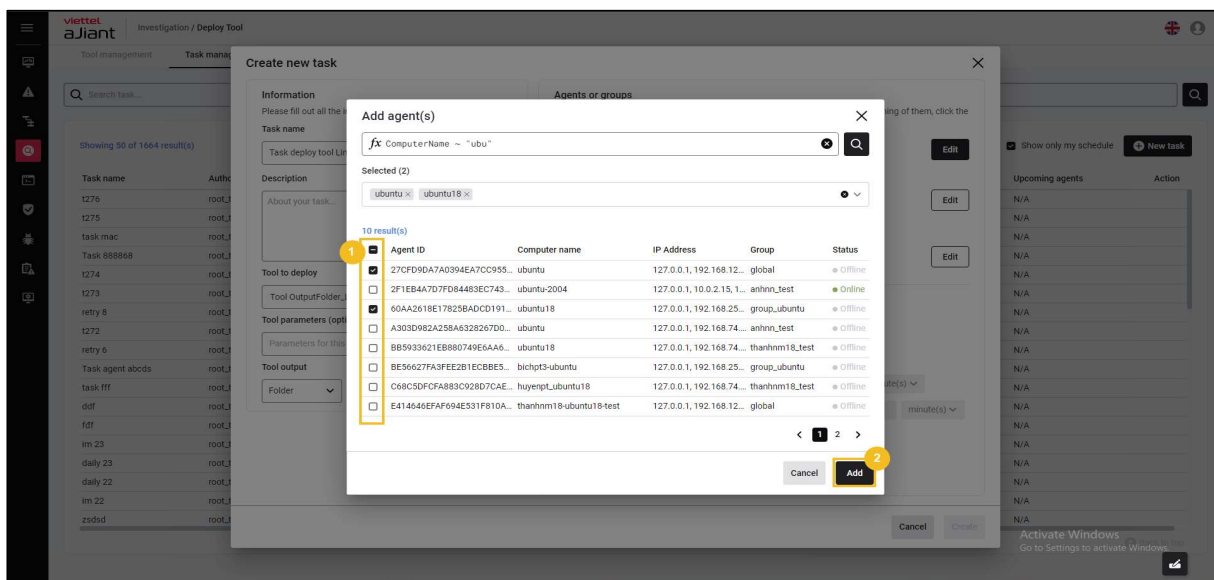
+ Chọn Add agent(s):



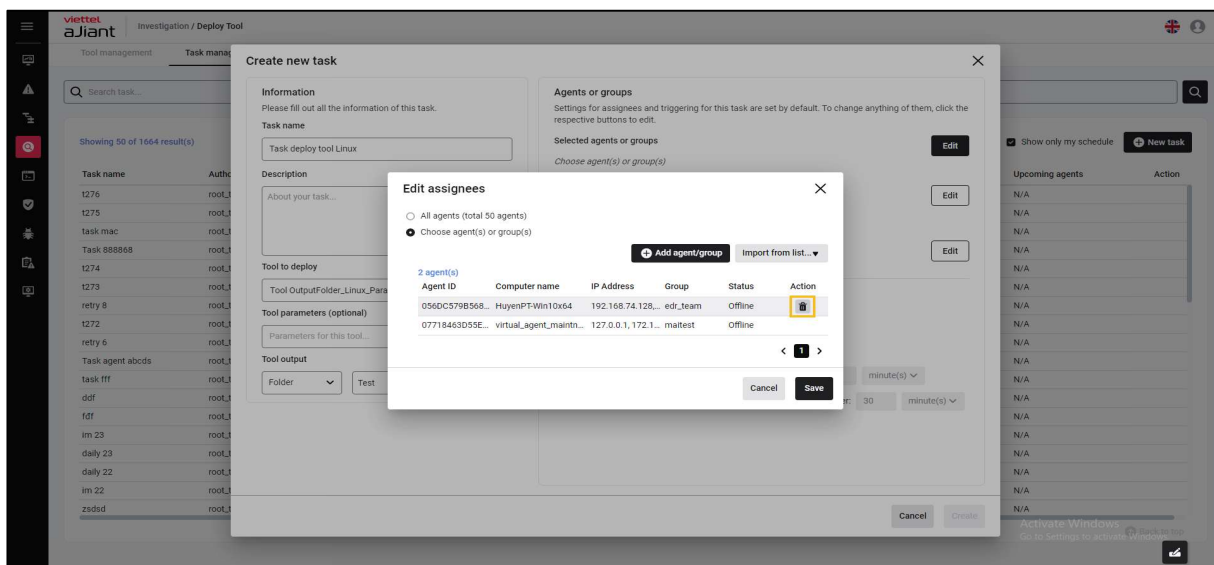
- Tìm kiếm Agent: Cho phép tạo câu lệnh truy vấn, sử dụng câu lệnh truy vấn để tìm kiếm Agent



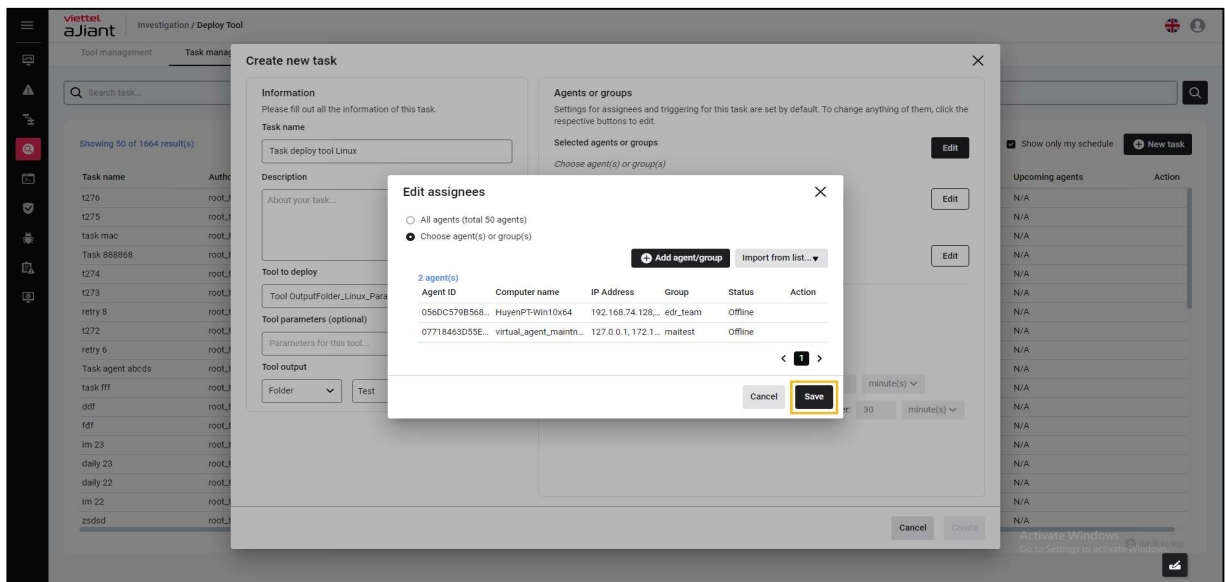
- Chọn Agent(s) để deploy bằng cách tích chọn vào một hoặc nhiều Agent(s) > Thông tin Agent(s) đã được chọn hiển thị ở khung **Selected** > chọn **Cancel** để hủy thao tác thêm Agent để deploy hoặc chọn nút **Add** để xác nhận danh sách Agent(s):



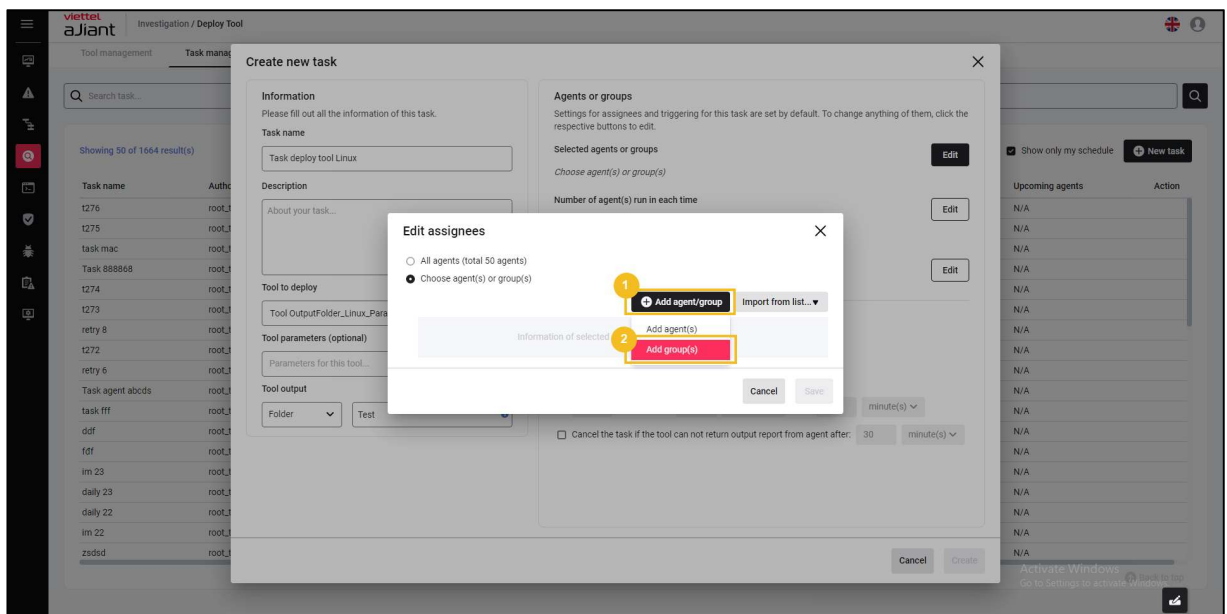
- Hover vào các Agent(s) đã chọn > Chọn icon  để thực hiện loại bỏ Agent(s) khỏi danh sách đã chọn:



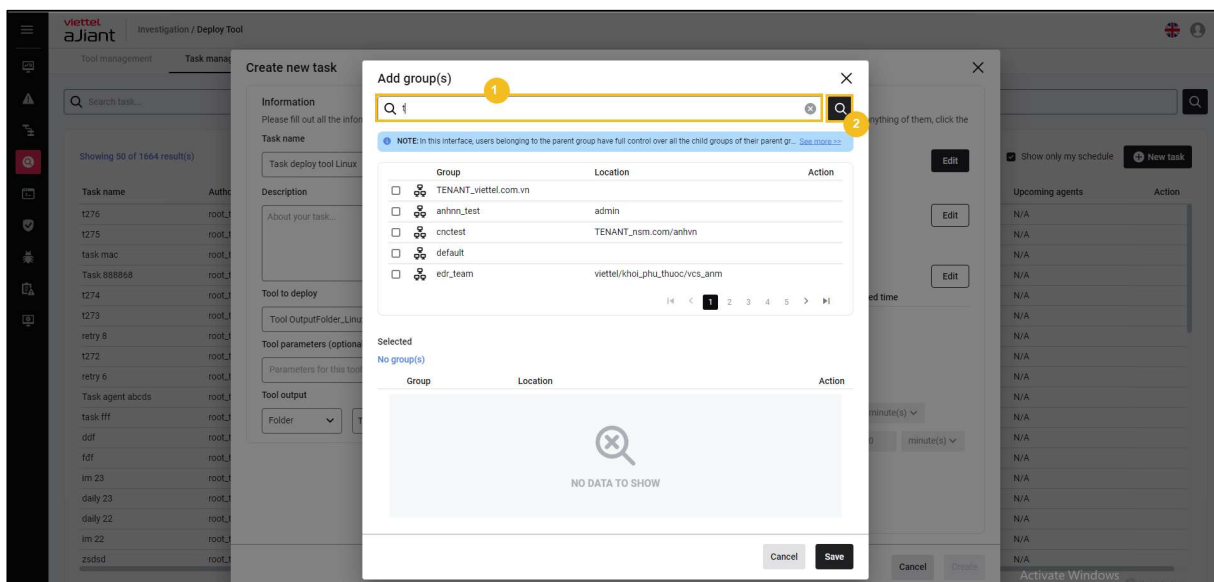
- Chọn **Cancel** để hủy hoặc chọn **Save** để lưu thông tin các Agent(s) đã chọn để deploy:



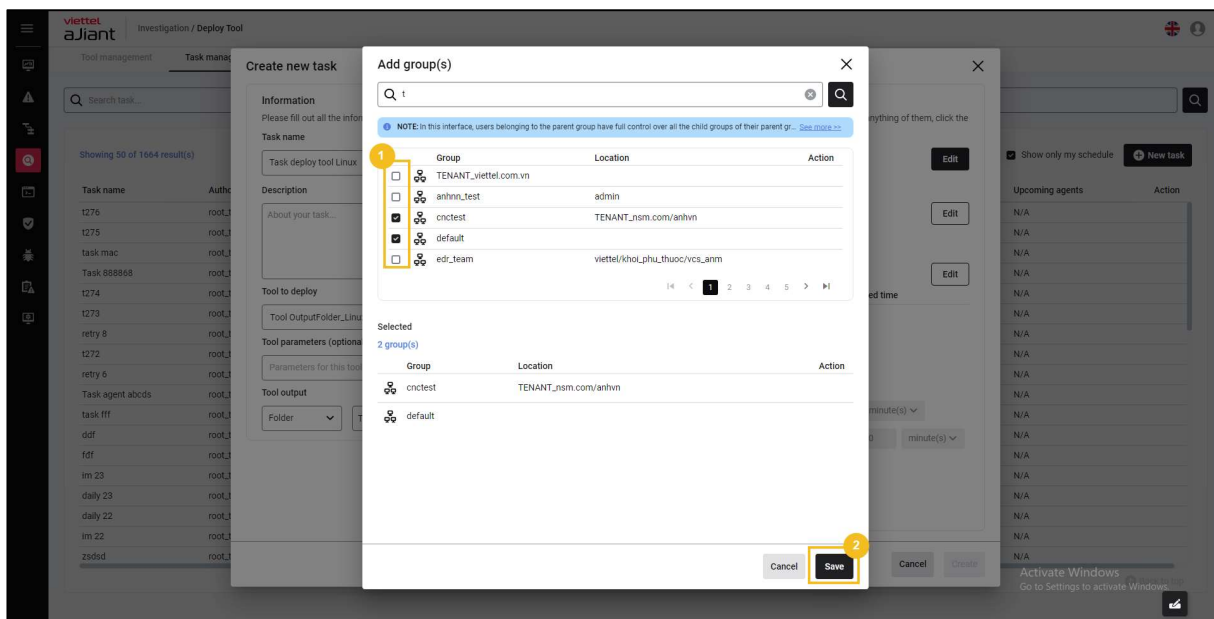
+ Chọn Add group(s):



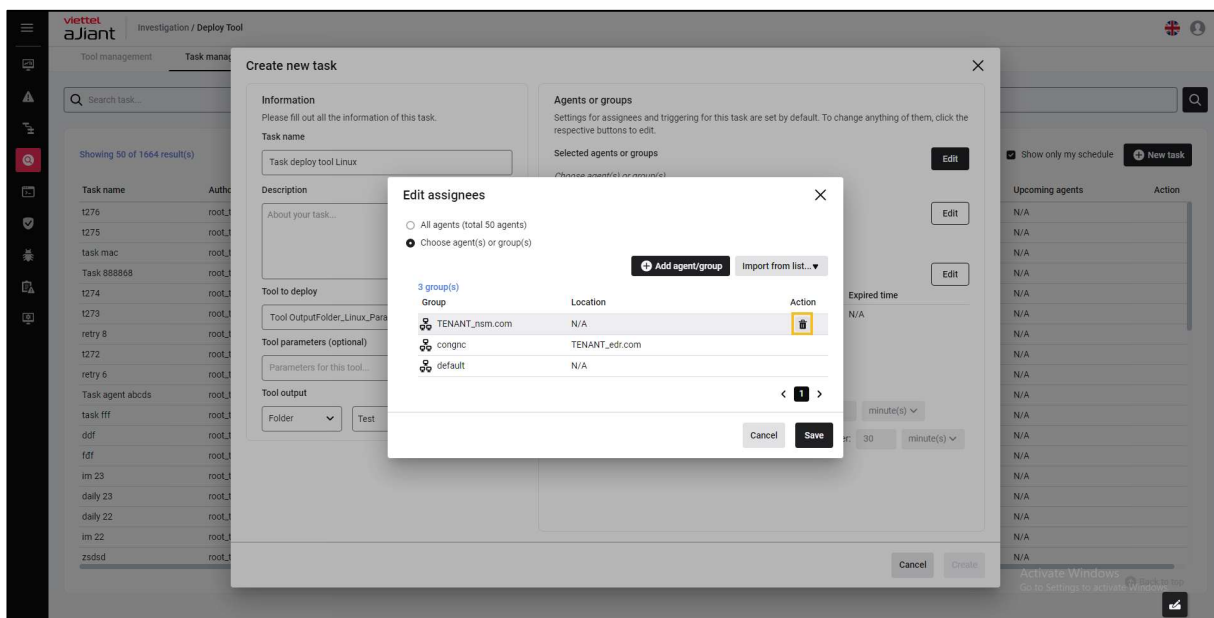
- Tìm kiếm group(s) theo tên, cho phép nhập từ khóa tìm kiếm group theo tên group:



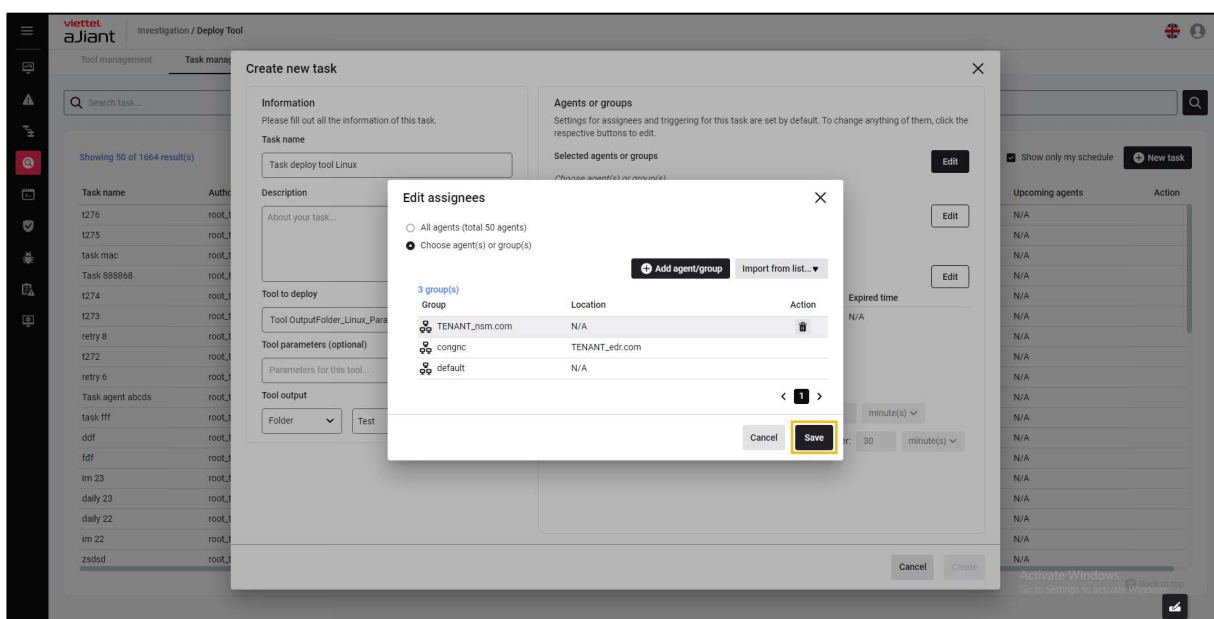
- Chọn group(s) để deploy bằng cách tích chọn vào một hoặc nhiều group(s) > Thông tin group(s) đã được chọn hiển thị ở khung **Selected** > chọn **Cancel** để hủy thao tác thêm group(s) để deploy hoặc chọn nút **Save** để xác nhận danh sách group(s):



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

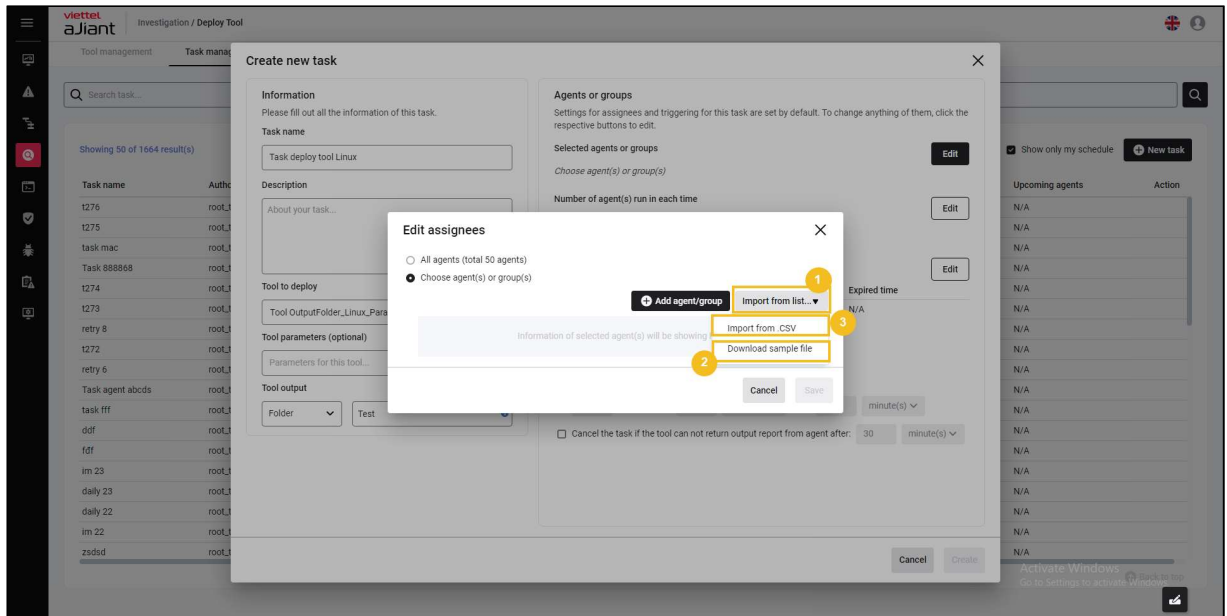


- Chọn **Cancel** để hủy hoặc Chọn **Save** các group(s) đã chọn để deploy:



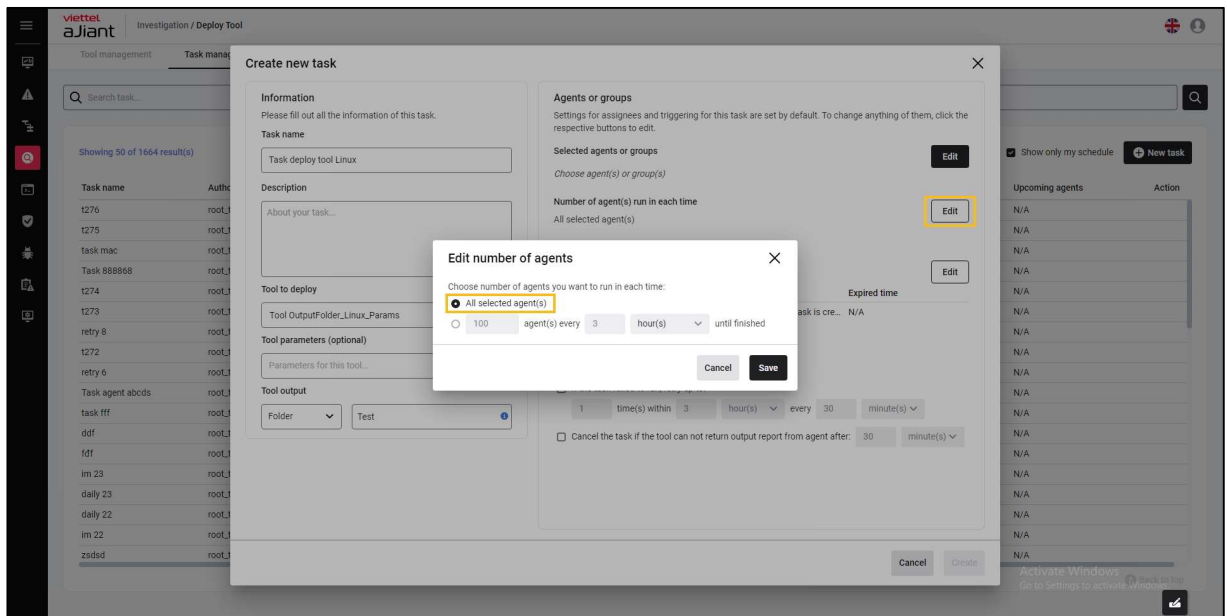
- + Import from list: Cho phép upload danh sách agent(s) từ file .csv > Chọn **Import from list**
 - Chọn **Download sample file** để lấy form danh sách file agent(s) mẫu;

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

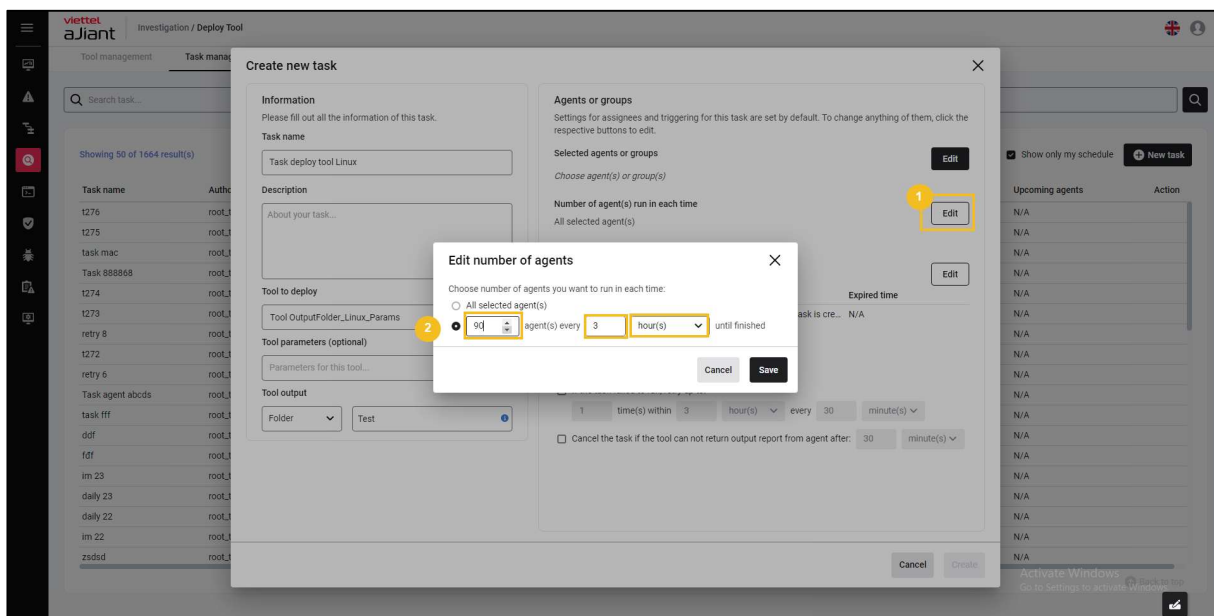


Bước 4: Cấu hình số lượng agent deploy tool mỗi lần:

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

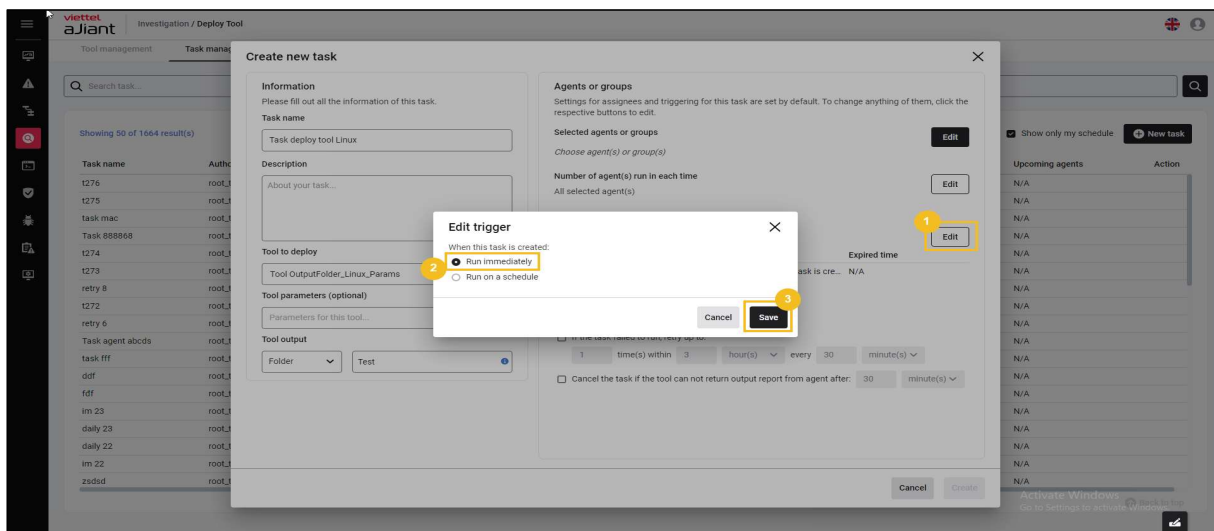


- + Cấu hình số lượng agent mỗi lần deploy:



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

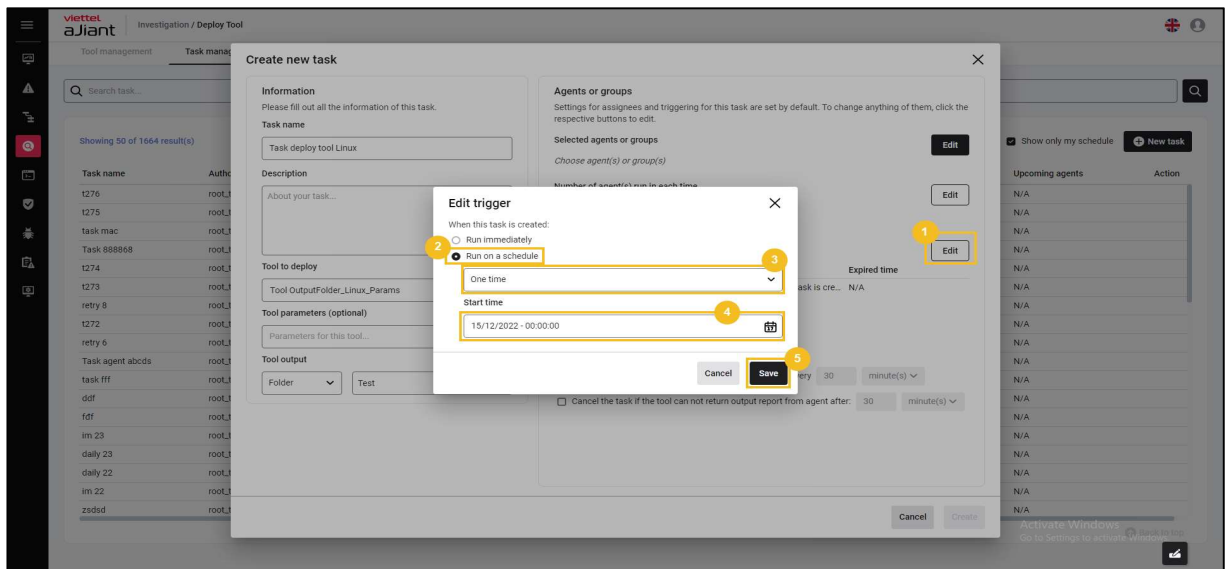
- + Chọn **Run immediately** để thực hiện cấu hình thời gian deploy tool **ngay lập tức** (sau khi tạo task thành công)



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

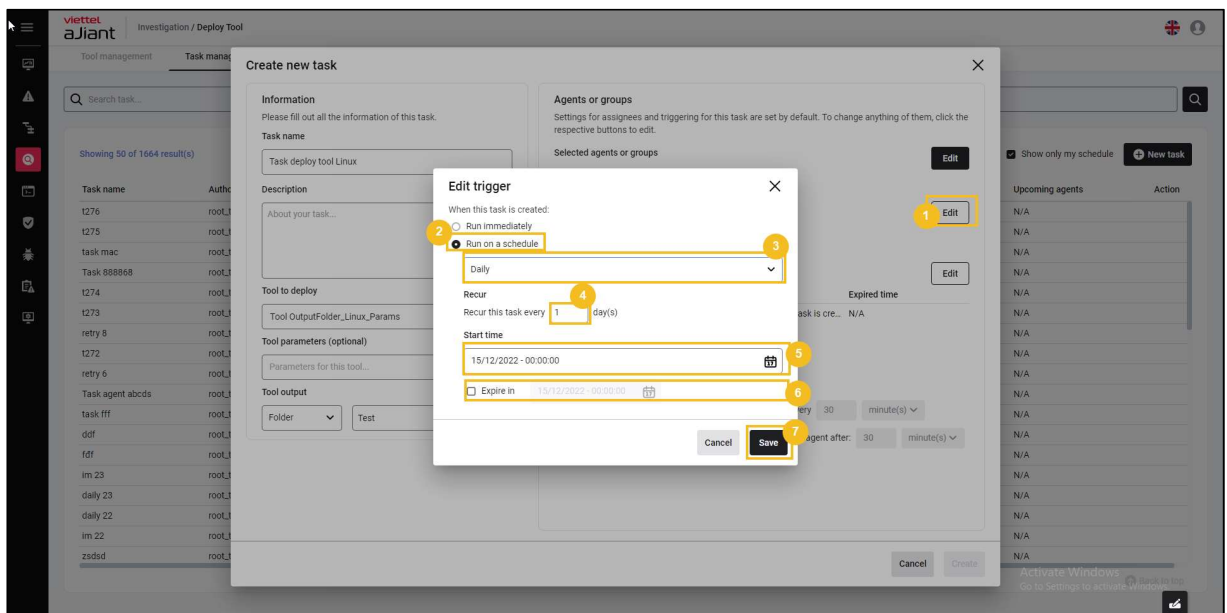
- Chọn schedule **One time**:
 - Cho phép lập lịch deploy tool một lần;

○ Cấu hình thời gian bắt đầu:



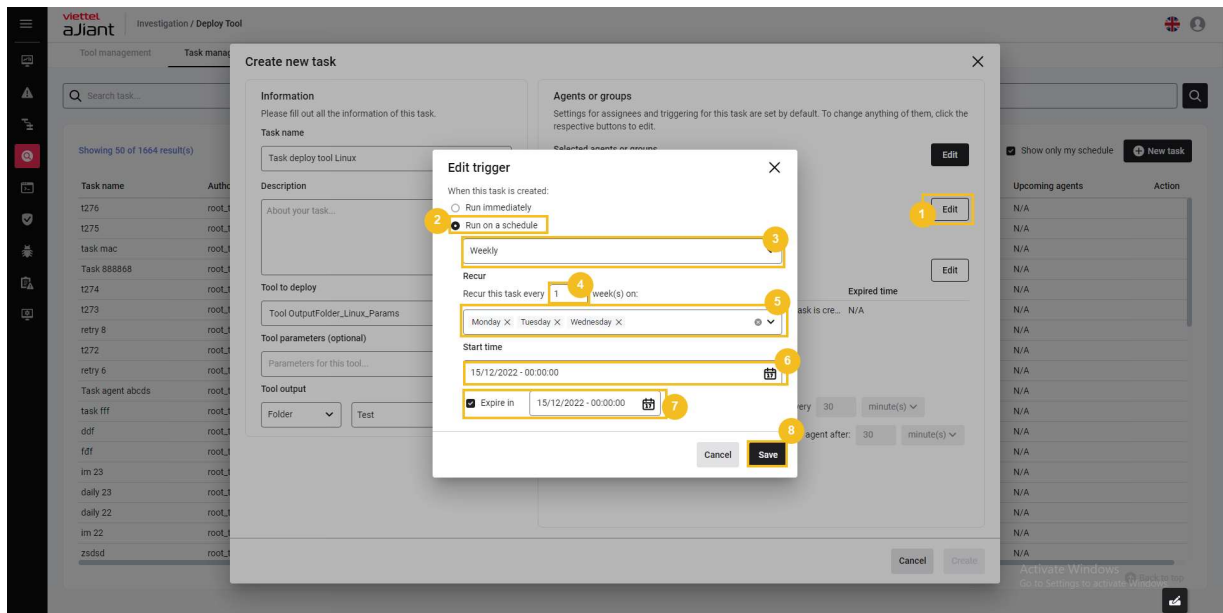
● Chọn schedule **Daily**:

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

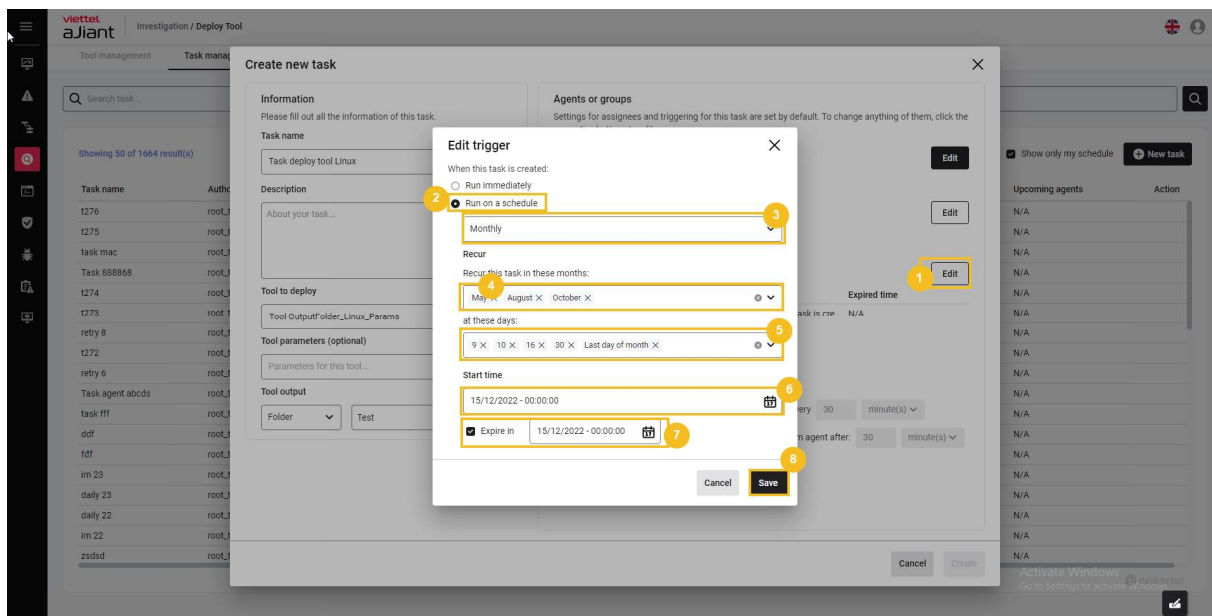


● Chọn schedule **Weekly**:

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

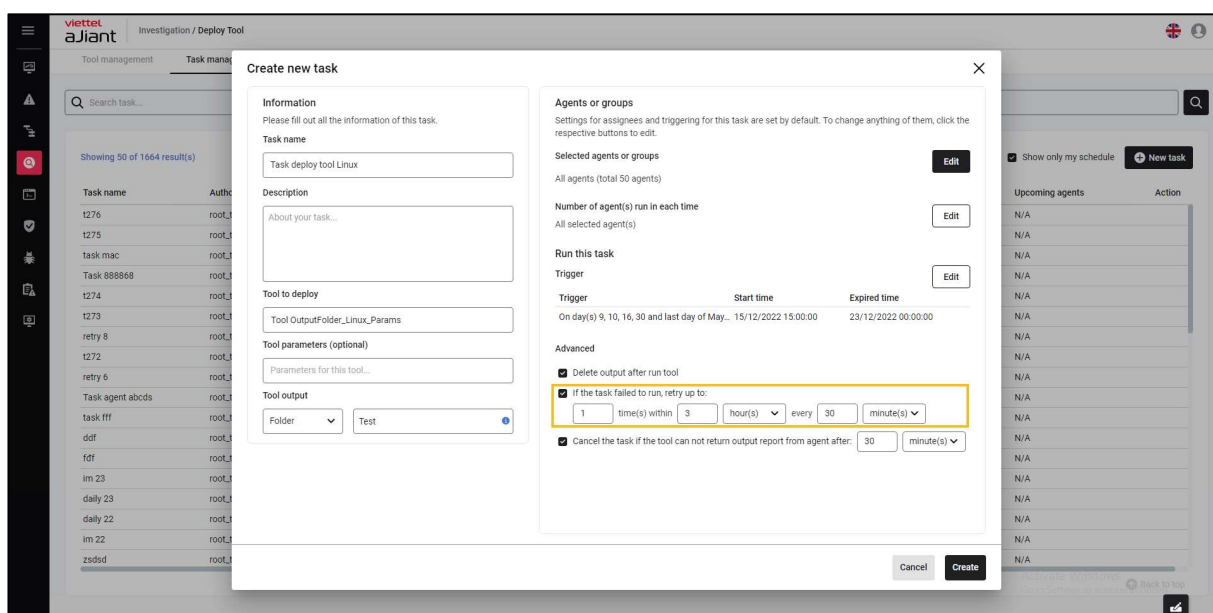


- Chọn schedule **Monthly**:
 - Cho phép lập lịch deploy tool hàng tháng;
 - Thời gian lặp lại;
 - Cấu hình thời gian bắt đầu và kết thúc:

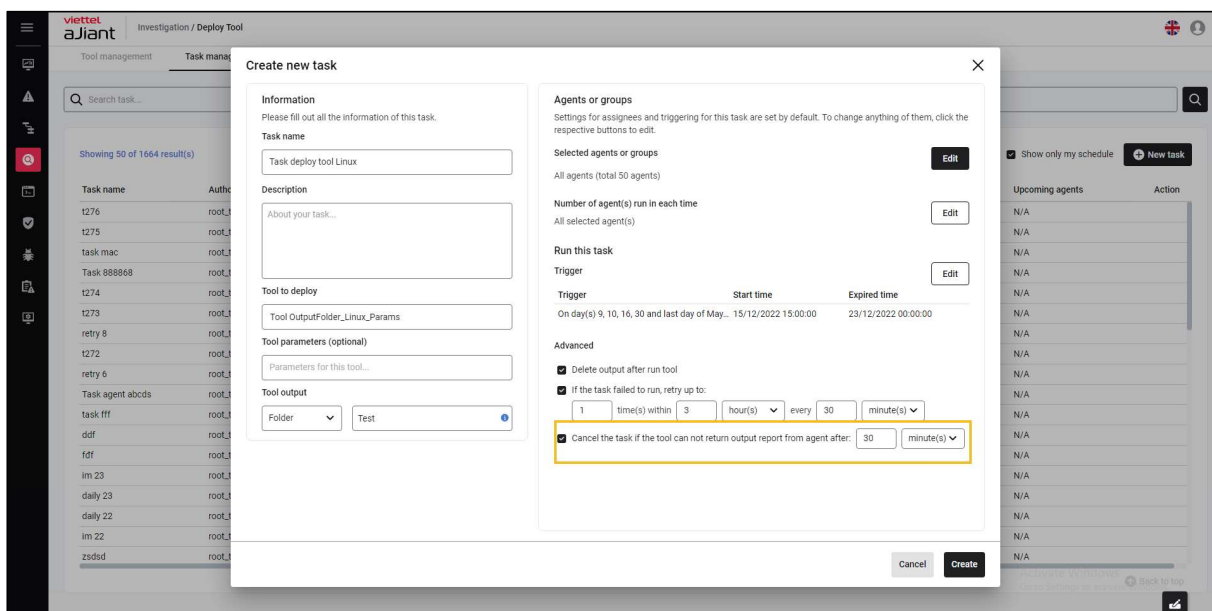


Bước 6: Cấu hình thông tin nâng cao cho task

- + **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

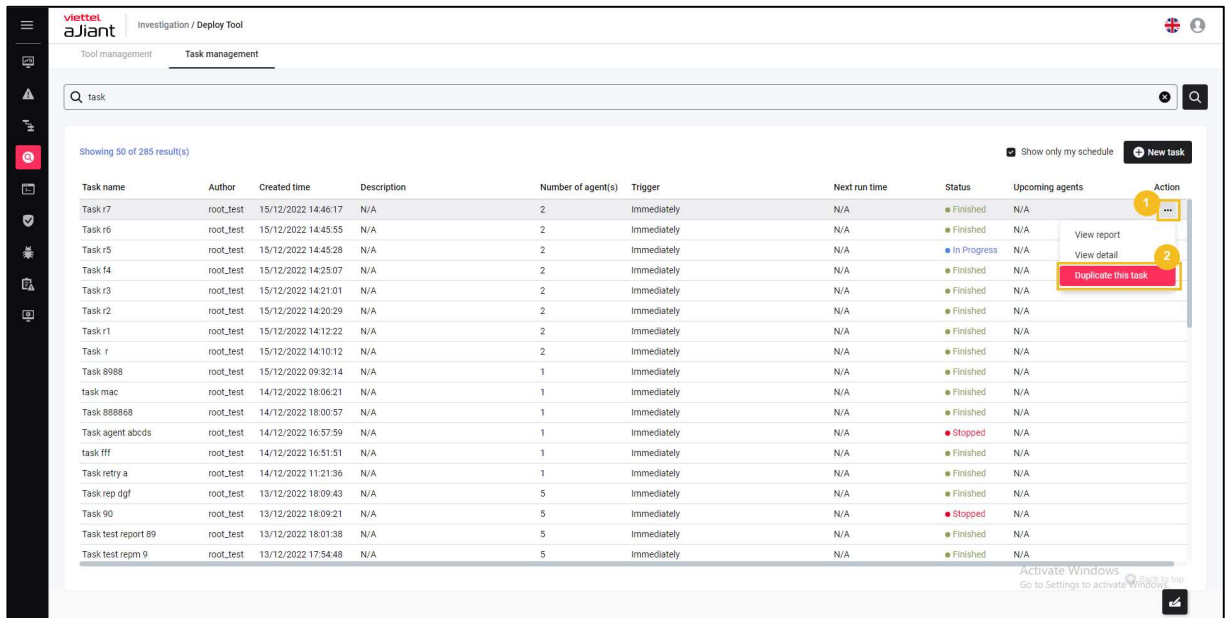
d. Nhân bản task (Duplicate task)

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);

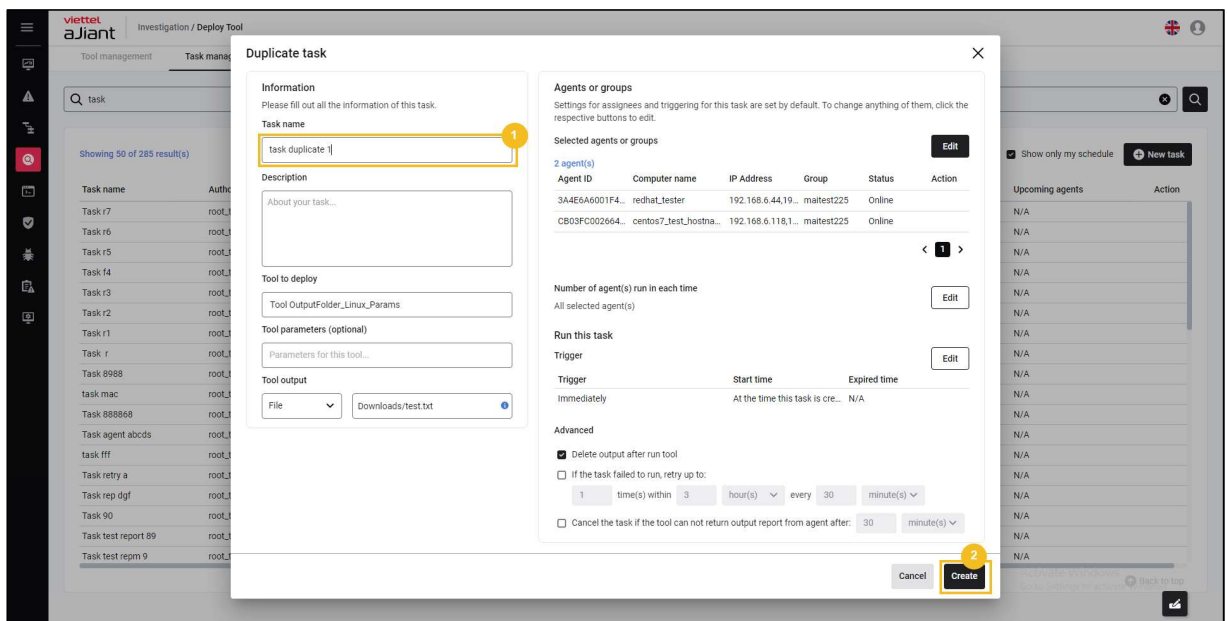
Các bước thực hiện:

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

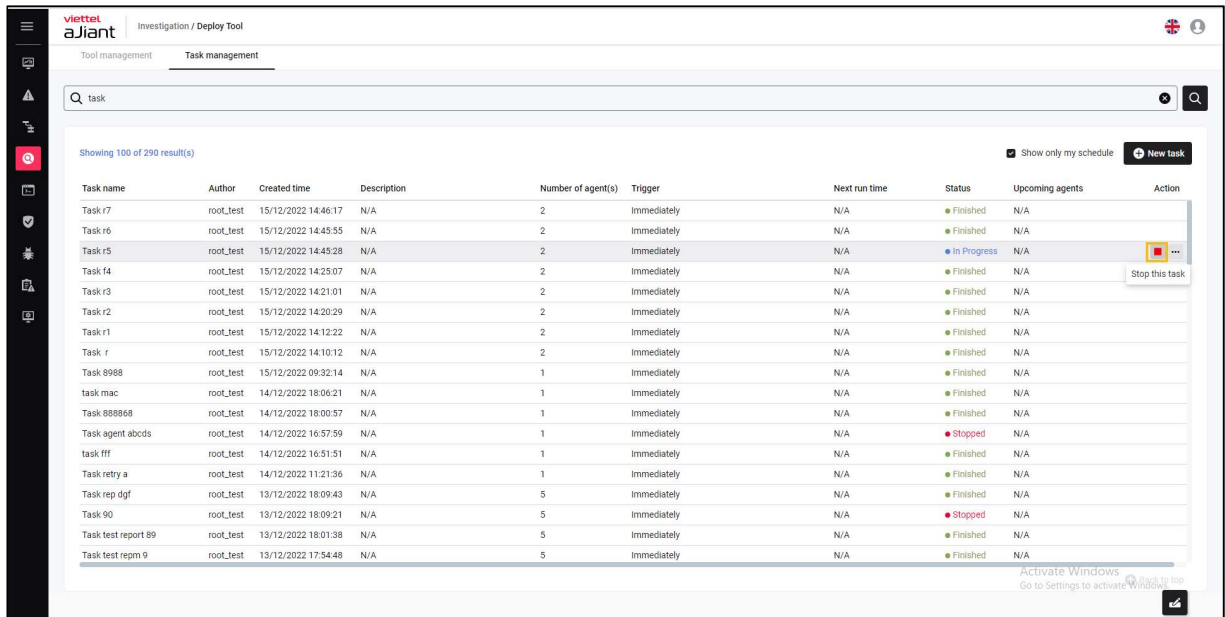
Mục đích: Cho phép hiển thị danh sách Agents sắp được deploy tool;

Các bước thực hiện: Tại màn hình danh sách task > Chọn Danh sách Upcoming agents.

f. Stop/ Start task

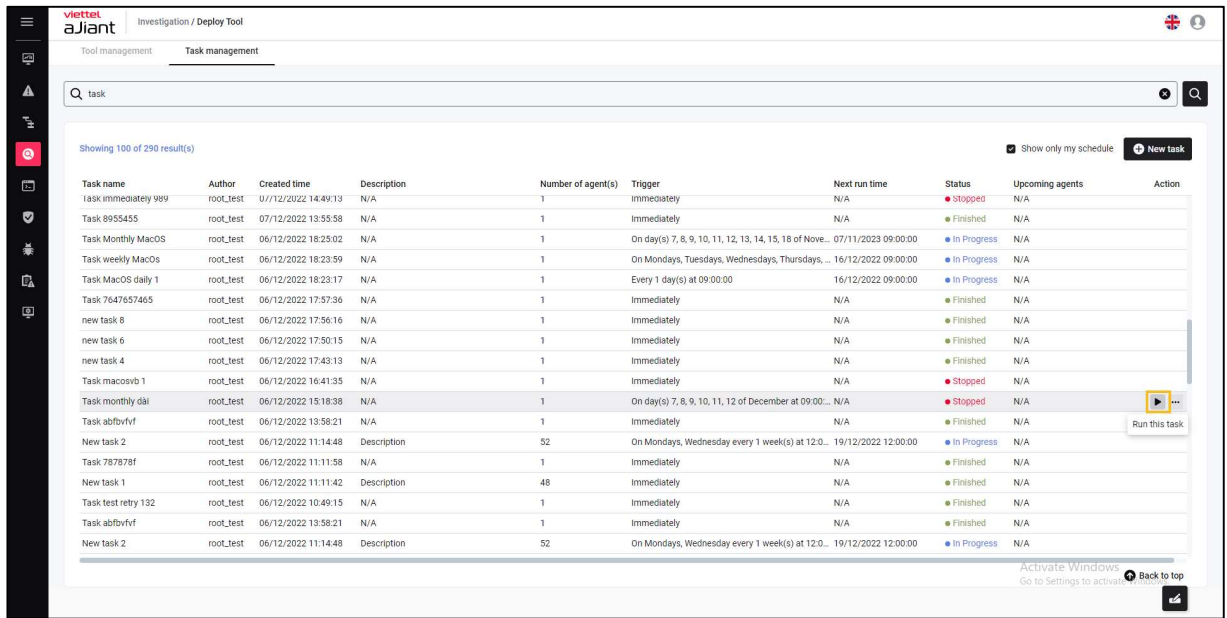
Mục đích: Cho phép Stop/ Restart task (Dừng deploy task hoặc deploy lại task đã tạm dừng).

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:



Task name	Author	Created time	Description	Number of agent(s)	Trigger	Next run time	Status	Upcoming agents	Action
Task r7	root_test	15/12/2022 14:46:17	N/A	2	Immediately	N/A	Finished	N/A	
Task r6	root_test	15/12/2022 14:45:55	N/A	2	Immediately	N/A	Finished	N/A	
Task r5	root_test	15/12/2022 14:45:28	N/A	2	Immediately	N/A	In Progress	N/A	 ...
Task f4	root_test	15/12/2022 14:25:07	N/A	2	Immediately	N/A	Finished	N/A	Stop this task
Task r3	root_test	15/12/2022 14:21:01	N/A	2	Immediately	N/A	Finished	N/A	
Task r2	root_test	15/12/2022 14:20:29	N/A	2	Immediately	N/A	Finished	N/A	
Task r1	root_test	15/12/2022 14:12:22	N/A	2	Immediately	N/A	Finished	N/A	
Task r	root_test	15/12/2022 14:10:12	N/A	2	Immediately	N/A	Finished	N/A	
Task 8988	root_test	15/12/2022 09:32:14	N/A	1	Immediately	N/A	Finished	N/A	
task mac	root_test	14/12/2022 18:06:21	N/A	1	Immediately	N/A	Finished	N/A	
Task 888868	root_test	14/12/2022 18:00:57	N/A	1	Immediately	N/A	Finished	N/A	
Task agent abcds	root_test	14/12/2022 16:57:59	N/A	1	Immediately	N/A	Stopped	N/A	
task fff	root_test	14/12/2022 16:51:51	N/A	1	Immediately	N/A	Finished	N/A	
Task retry a	root_test	14/12/2022 11:21:36	N/A	1	Immediately	N/A	Finished	N/A	
Task rep dgf	root_test	13/12/2022 18:09:43	N/A	5	Immediately	N/A	Finished	N/A	
Task 90	root_test	13/12/2022 18:09:21	N/A	5	Immediately	N/A	Stopped	N/A	
Task test report 89	root_test	13/12/2022 18:01:38	N/A	5	Immediately	N/A	Finished	N/A	
Task test repm 9	root_test	13/12/2022 17:54:48	N/A	5	Immediately	N/A	Finished	N/A	

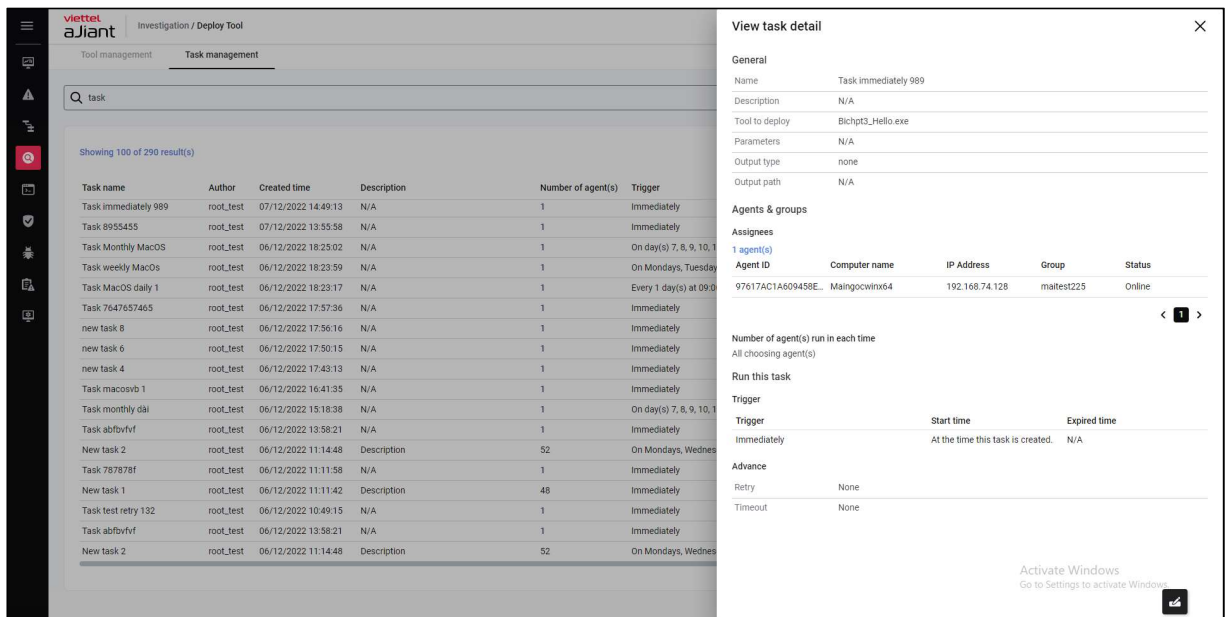
Các bước thực hiện deploy lại task (đã tạm dừng – Stopped): Tại màn hình danh sách task, hover vào task cần deploy lại > Chọn icon  để deploy lại task:



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**:

The screenshot displays the Viettel aJiant Task management interface. On the left, a sidebar contains navigation icons. The main area is divided into two panels. The left panel, titled 'Task management', shows a list of tasks with columns for Task name, Author, Created time, and Description. The right panel, titled 'View report - New task 2', displays a detailed report for a specific task. This report includes a search bar, a table of results with columns for Agent ID, Computer name, IP Address, Tool exit code, Status, Message, and Action, and a summary section at the bottom.

Agent ID	Computer name	IP Address	Tool exit code	Status	Message	Action
97EB9873A6807...	Win7x86-A-PC	10.0.2.15	N/A	Failed	Architecture invalid (Tool: ...)	
A23B7D0C7455D...	thanhnm18-test	192.168.121...	0	Failed	Failed to get output(tool outp...	
97617AC1A6094...	Maingocwinx64	192.168.74.1...	0	Success	N/A	
A86963E7A5830...	Win10x64-A-PC	10.0.2.15	0	Failed	Failed to get output(tool outp...	
50EF37015E7D1...	D5Test-PC	192.168.56.1...	N/A	Failed	Unknown error	
524B30C4C568F...	EDR-TEST02	192.168.133...	N/A	Failed	Unknown error	
056DC579B5681...	HuyenPT-Win10x...	192.168.74.1...	N/A	Failed	Unknown error	
12B680FA5B449...	Win7x86	192.168.74.1...	N/A	Failed	Unknown error	
AE36AD62DEA59...	BichPT3	192.168.255...	N/A	Expired	Task time expired	
1B0A66FD56EDD...	DESKTOP-R20BJ...	192.168.198...	N/A	Expired	Task time expired	
C81D5366CED36...	HuyenPT-Win7x86	192.168.74.1...	N/A	Expired	Task time expired	
1B2D5EC3C7611...	HuyenPT-Win7x64	192.168.74.1...	N/A	Expired	Task time expired	
97EA4D29AA9AF...	BichPT3_7x86	192.168.255...	N/A	Expired	Task time expired	
AB5555ED3C77...	thanhnm18-w10x...	192.168.121...	N/A	Expired	Task time expired	
5DF667D8A4E3F...	HuyenPT-Win10x...	192.168.74.1...	N/A	Expired	Task time expired	
F2AA317BE8769...	BichPT3_Win10T...	192.168.255...	N/A	Expired	Task time expired	
3C7764CA3BD8...	bao-PC	10.0.2.15	N/A	Expired	Task time expired	
EA4B8A29CC45...	x64_ptbich	192.168.255...	N/A	Expired	Task time expired	
AC736D6DD5A3...	Win10x86	192.168.74.1...	N/A	Expired	Task time expired	
E1A2D22E765E5...	thanhnm18-test-7...	192.168.121...	N/A	Expired	Task time expired	
EF0C1A62F117F...	thanhnm18-w7x64	192.168.121...	N/A	Expired	Task time expired	

+ 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

View report - New task 2

14/12/2022 - 12:00:00
Total agents: 51
Success: 1

12/12/2022 - 12:00:00
Total agents: 49
Success: 2

07/12/2022 - 12:00:00
Total agents: 49
Success: 0

Showing 12 of 12 results

Agent ID	Computer name	IP Address	Tool exit code	Status	Message	Action
8E03AD8705FF8...	virtual_agent_mai...	172.17.0.2	N/A	Failed	Platform invalidated (Tool wind.	
A6ED648CC1C17...	virtual_agent_mai...	172.17.0.5	N/A	Failed	Platform invalidated (Tool wind.	
AA657D644FF8C...	virtual_agent_mai...	172.17.0.11	N/A	Failed	Platform invalidated (Tool wind.	
210352BC56C0B...	macOS-Mais-Mac...	192.168.74.1...	N/A	Failed	Platform invalidated (Tool wind.	
718C4C742BB32...	virtual_agent_mai...	172.17.0.4	N/A	Failed	Platform invalidated (Tool wind.	
E450A71CC08FD...	virtual_agent_mai...	172.17.0.3	N/A	Failed	Platform invalidated (Tool wind.	
3CAD1ACA8489...	virtual_agent_mai...	172.17.0.7	N/A	Failed	Platform invalidated (Tool wind.	
07718463D55E5...	virtual_agent_mai...	172.17.0.10	N/A	Failed	Platform invalidated (Tool wind.	
6C648D7431177...	virtual_agent_mai...	172.17.0.9	N/A	Failed	Platform invalidated (Tool wind.	
556075243054B...	virtual_agent_mai...	2.17.0.8	N/A	Failed	Platform invalidated (Tool wind.	
6D8E442BB0298...	virtual_agent_mai...	172.17.0.6	N/A	Failed	Platform invalidated (Tool wind.	
97617AC1A6094...	Maingocwinx64	192.168.74.1...	0	Success	N/A	

+ 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**

View report - New task 2

14/12/2022 - 12:00:00
Total agents: 51
Success: 1

12/12/2022 - 12:00:00
Total agents: 49
Success: 2

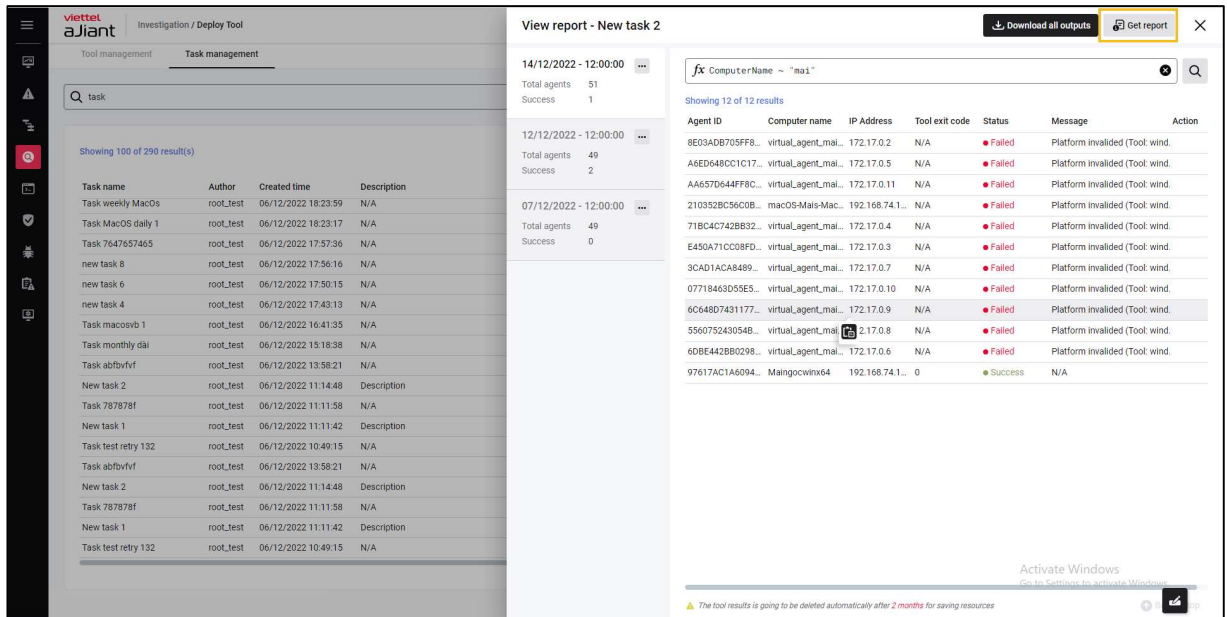
07/12/2022 - 12:00:00
Total agents: 49
Success: 0

Showing 12 of 12 results

Agent ID	Computer name	IP Address	Tool exit code	Status	Message	Action
8E03AD8705FF8...	virtual_agent_mai...	172.17.0.2	N/A	Failed	Platform invalidated (Tool wind.	
A6ED648CC1C17...	virtual_agent_mai...	172.17.0.5	N/A	Failed	Platform invalidated (Tool wind.	
AA657D644FF8C...	virtual_agent_mai...	172.17.0.11	N/A	Failed	Platform invalidated (Tool wind.	
210352BC56C0B...	macOS-Mais-Mac...	192.168.74.1...	N/A	Failed	Platform invalidated (Tool wind.	
718C4C742BB32...	virtual_agent_mai...	172.17.0.4	N/A	Failed	Platform invalidated (Tool wind.	
E450A71CC08FD...	virtual_agent_mai...	172.17.0.3	N/A	Failed	Platform invalidated (Tool wind.	
3CAD1ACA8489...	virtual_agent_mai...	172.17.0.7	N/A	Failed	Platform invalidated (Tool wind.	
07718463D55E5...	virtual_agent_mai...	172.17.0.10	N/A	Failed	Platform invalidated (Tool wind.	
6C648D7431177...	virtual_agent_mai...	172.17.0.9	N/A	Failed	Platform invalidated (Tool wind.	
556075243054B...	virtual_agent_mai...	2.17.0.8	N/A	Failed	Platform invalidated (Tool wind.	
6D8E442BB0298...	virtual_agent_mai...	172.17.0.6	N/A	Failed	Platform invalidated (Tool wind.	
97617AC1A6094...	Maingocwinx64	192.168.74.1...	0	Success	N/A	

+ 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**

View report - New task 2

14/12/2022 - 12:00:00

Total agents: 51
Success: 1

Download outputs

Get report

Computer name	IP Address	Tool exit code	Status	Message	Action
8E03ADB705FF8...	virtual_agent_mai...	172.17.0.2	N/A	Failed	Platform invalided (Tool wind.
A6ED648CC1C17...	virtual_agent_mai...	172.17.0.5	N/A	Failed	Platform invalided (Tool wind.
AA657D644FF8C...	virtual_agent_mai...	172.17.0.11	N/A	Failed	Platform invalided (Tool wind.
210352BC56C0B...	macOS-Mais-Mac...	192.168.74.1...	N/A	Failed	Platform invalided (Tool wind.
718C4C742BB32...	virtual_agent_mai...	172.17.0.4	N/A	Failed	Platform invalided (Tool wind.
E450A71CC08FD...	virtual_agent_mai...	172.17.0.3	N/A	Failed	Platform invalided (Tool wind.
3CAD1ACA8489...	virtual_agent_mai...	172.17.0.7	N/A	Failed	Platform invalided (Tool wind.
07718463D55E5...	virtual_agent_mai...	172.17.0.10	N/A	Failed	Platform invalided (Tool wind.
6C648D7431177...	virtual_agent_mai...	172.17.0.9	N/A	Failed	Platform invalided (Tool wind.
556075243054B...	virtual_agent_mai...	172.17.0.8	N/A	Failed	Platform invalided (Tool wind.
6D6E442BB0298...	virtual_agent_mai...	172.17.0.6	N/A	Failed	Platform invalided (Tool wind.
97617AC1A6094...	Maingocwinx64	192.168.74.1...	0	Success	N/A

+ Download báo cáo của từng lần lập lịch:

- Mục đích: Cho phép download tất cả danh sách thông 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 report - New task 2

14/12/2022 - 12:00:00

Total agents: 51
Success: 1

Download outputs

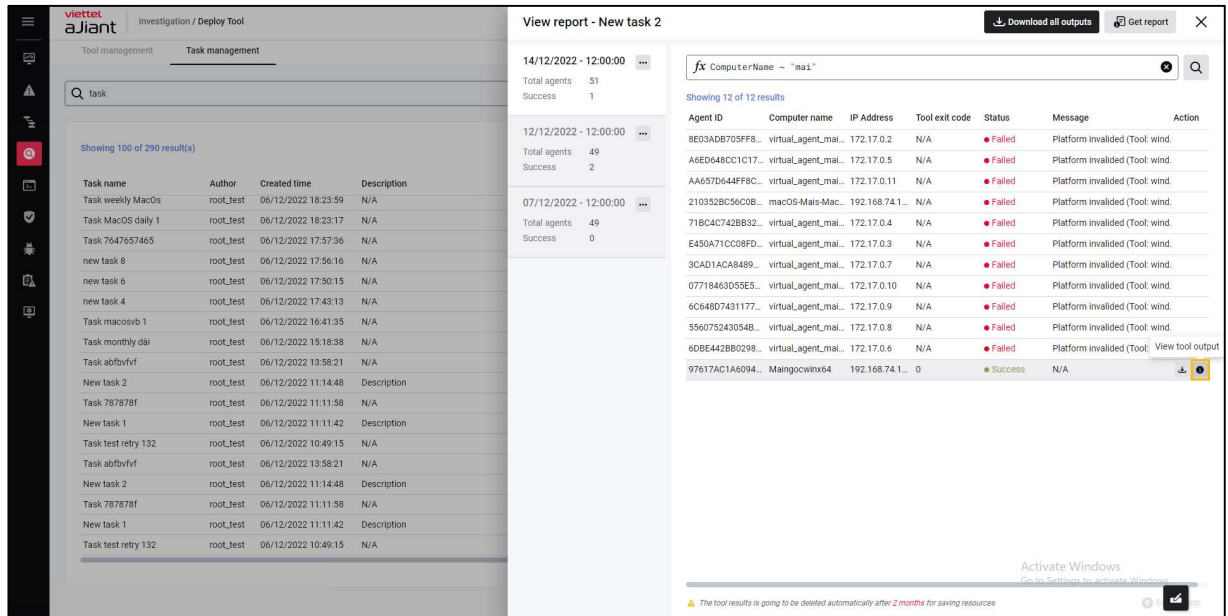
Get report

Computer name	IP Address	Tool exit code	Status	Message	Action
8E03ADB705FF8...	virtual_agent_mai...	172.17.0.2	N/A	Failed	Platform invalided (Tool wind.
A6ED648CC1C17...	virtual_agent_mai...	172.17.0.5	N/A	Failed	Platform invalided (Tool wind.
AA657D644FF8C...	virtual_agent_mai...	172.17.0.11	N/A	Failed	Platform invalided (Tool wind.
210352BC56C0B...	macOS-Mais-Mac...	192.168.74.1...	N/A	Failed	Platform invalided (Tool wind.
718C4C742BB32...	virtual_agent_mai...	172.17.0.4	N/A	Failed	Platform invalided (Tool wind.
E450A71CC08FD...	virtual_agent_mai...	172.17.0.3	N/A	Failed	Platform invalided (Tool wind.
3CAD1ACA8489...	virtual_agent_mai...	172.17.0.7	N/A	Failed	Platform invalided (Tool wind.
07718463D55E5...	virtual_agent_mai...	172.17.0.10	N/A	Failed	Platform invalided (Tool wind.
6C648D7431177...	virtual_agent_mai...	172.17.0.9	N/A	Failed	Platform invalided (Tool wind.
556075243054B...	virtual_agent_mai...	172.17.0.8	N/A	Failed	Platform invalided (Tool wind.
6D6E442BB0298...	virtual_agent_mai...	172.17.0.6	N/A	Failed	Platform invalided (Tool wind.
97617AC1A6094...	Maingocwinx64	192.168.74.1...	0	Success	N/A

+ 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**

The screenshot displays the Viettel aJiant web interface. On the left, the 'Task management' section shows a list of tasks with columns for Task name, Author, Created time, and Description. The main area on the right is titled 'View report - New task 2' and shows a summary of results for the date 14/12/2022. Below the summary, a table lists 51 results with columns for Agent ID, Computer name, IP Address, Tool exit code, Status, Message, and Action. The status column shows various outcomes like 'Failed', 'Success', and 'Expired'. At the bottom, a warning message states: 'The tool results is going to be deleted automatically after 2 months for saving resources'.

3.6 Màn hình Response

3.6.1 Response_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”;

The screenshot shows the 'Response / Live response' section of the Viettel aJiant interface. It features a central configuration box for initiating a live response session. The box includes a 'Live response' title, a brief instruction to choose an online agent and click 'Connect', and a form with an 'Agent' dropdown menu (currently showing 'DESKTOP-R20B.JEF') and a 'Duration' field (set to '15 minutes'). A 'Connect' button is located at the bottom of the configuration box.

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;

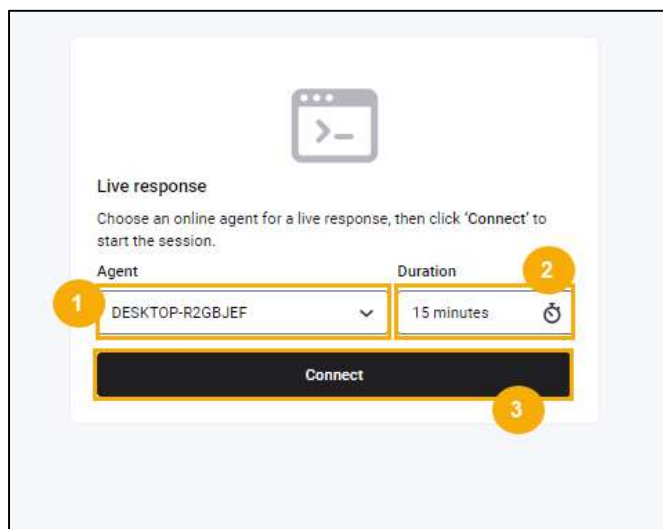
Người dùng chỉ thực hiện được Live Response với những agent đang có trạng thái online:



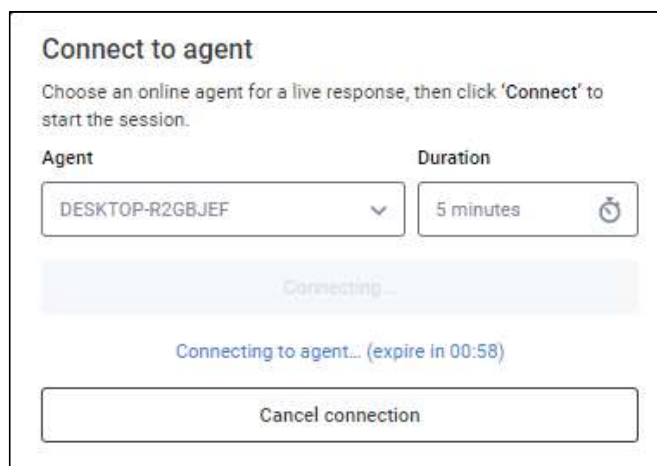
- + Chọn Duration: có các khoảng thời gian 5 phút, 15 phút, 1 giờ, 3 giờ;



- + Click nút “Connect”:

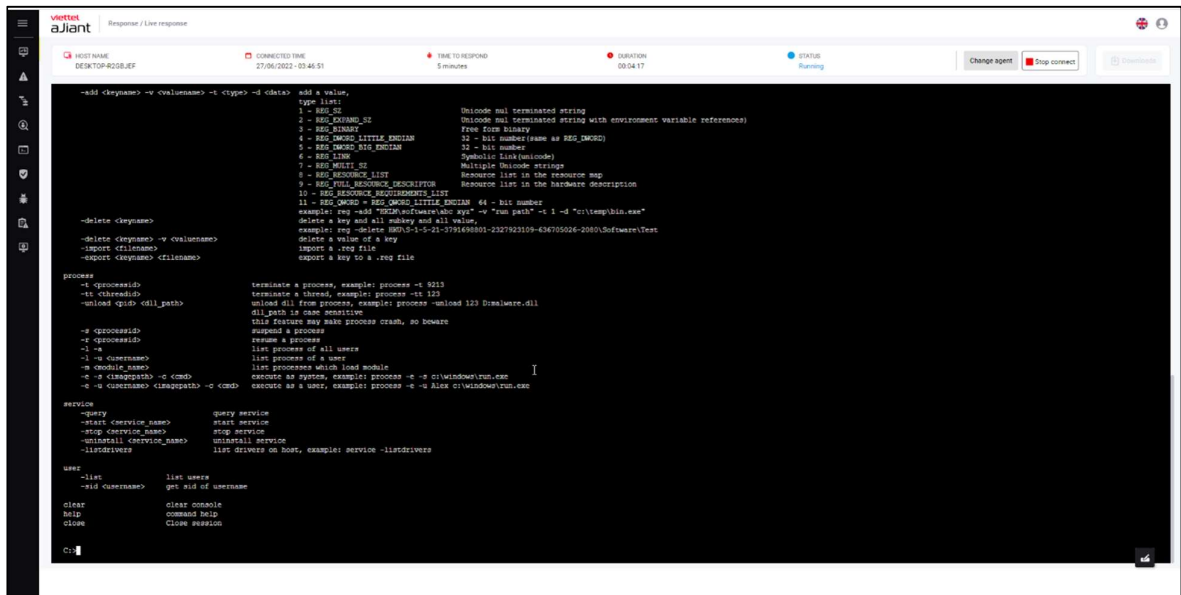


Bước 3: Chờ 1 phút để hệ thống thực hiện kết nối tới agent, trạng thái hệ thống là “connecting”:

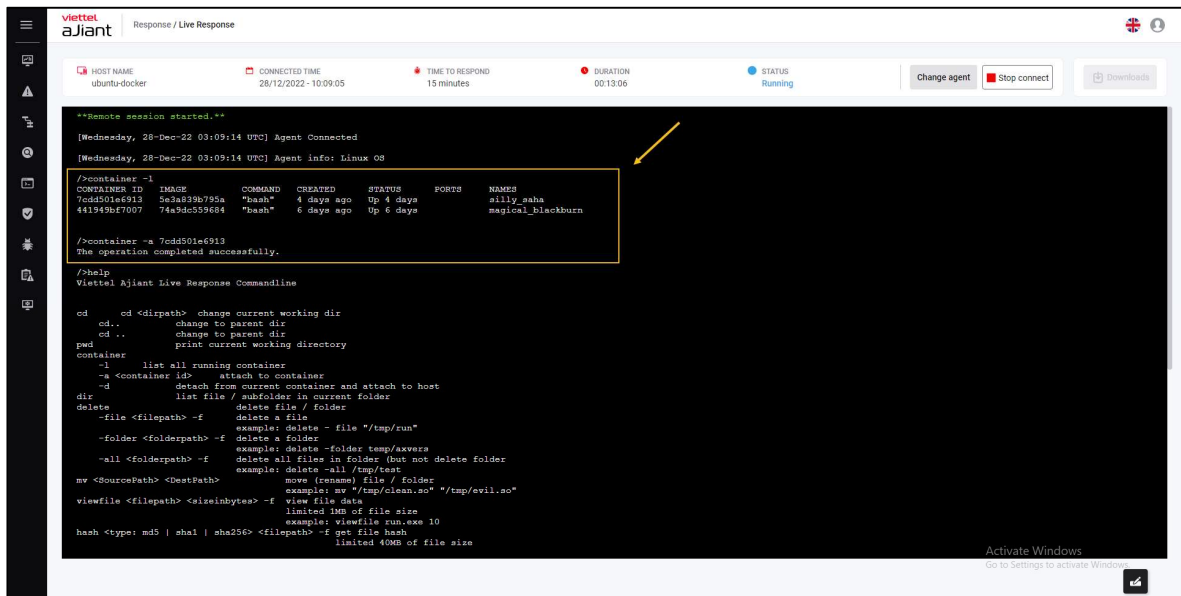


Bước 4: Khi kết nối thành công, người dùng được phép thực hiện các lệnh ở màn hình console và trạng thái của phiên Live response “running”;

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:

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
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	

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
		N By name (alphabetic) 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	

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
		/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/ thư 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

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
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	Dump process bởi Process name

STT	Các lệnh	Tham số	Mô tả
		Ví dụ: dump -process -name Evil.exe -f "C:\Users\Evil_dumped.dmp"	
		-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:	Truy vấn tất cả các subkey và value và data

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
		reg-query "HKLM\Software\abc xyz" -s	
		add <keyname> ví dụ: reg-add "HKLM\software\abc xyz"	Thêm 1 key
		add <keyname> -v <valuenam> -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 <valuenam>	Xóa 1 giá trị của key
		import <filename>	Import 1 file .reg
		export <keyname> <filename>	Export 1 file .reg

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
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
		-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

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
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
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:

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
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>	Xóa 1 file

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
		ví dụ: delete -file "c:\temp\run path.exe"	
		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/ thư 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

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
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	

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
		-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
		-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

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
		-d	Thoát kết nối container

+ MACOS:

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
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
		delete -all <folderpath> ví dụ: delete -all c:\temp	Xóa tất cả các file/ thư mục con trong thư mục (nhưng không xóa thư mục)

STT	Các lệnh	Tham số	Mô tả
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: hash md5 example: 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
		-s <processid>	Tạm dừng 1 tiến trình

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
		-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
		-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

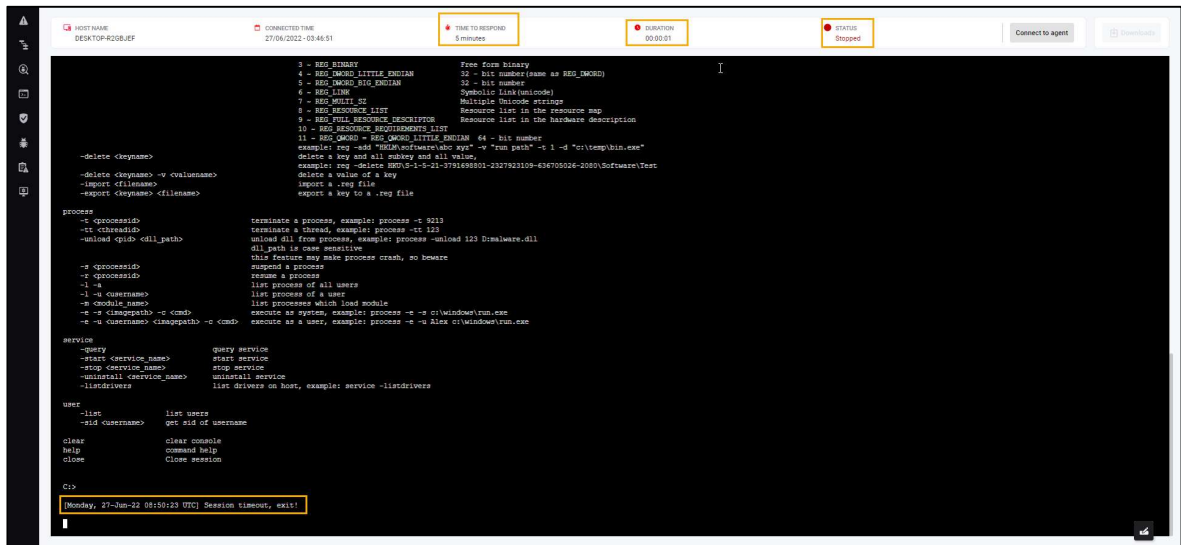
<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
		-listdrivers list drivers on host, example: service -listdrivers	List danh sách drivers trên host
13	user	-list	Liệt kê các user trên máy
		-sid<username>	Lấy sid của username
14	help		Lệnh help
15	Clear		Làm sạch console

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

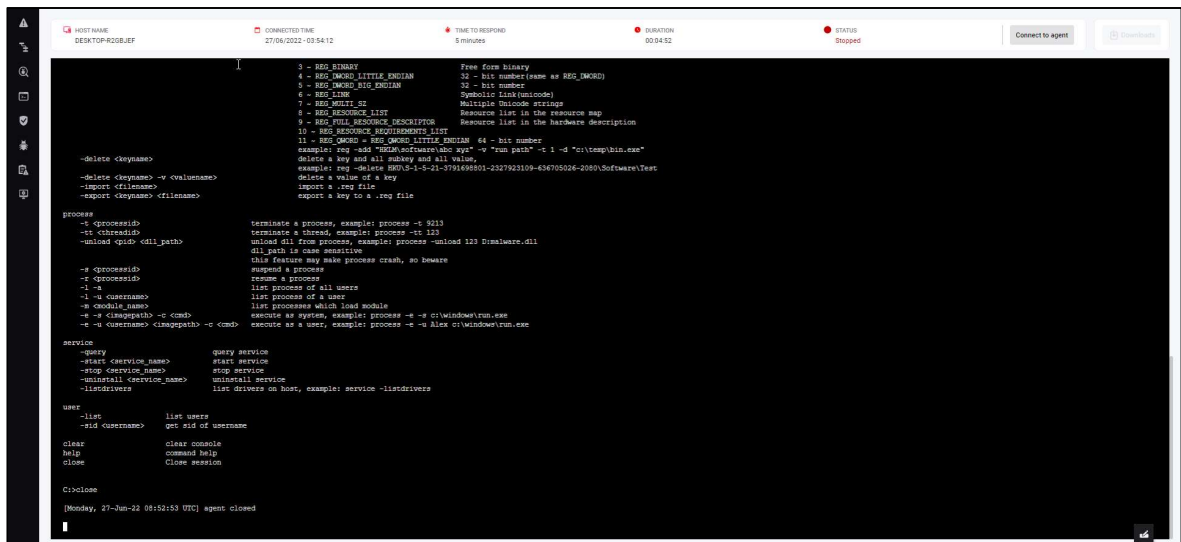
- + Lệnh Clear: Sau khi thực hiện lệnh clear thì hệ thống sẽ hỗ trợ người dùng download toàn bộ log đã thực hiện trên màn hình console trước đây, bằng thao tác click vào link “here”;
- + Lệnh get <filepath>: ví dụ: get procexp.exe trong màn hình console thì kết quả lấy file về được hiển thị ở màn hình 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.



3.7 Màn hình Setting

3.7.1 Agent Management

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

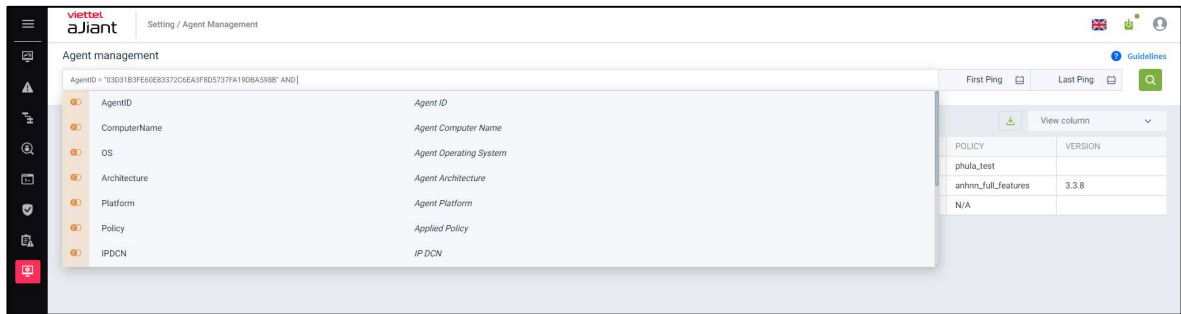
- + Xem danh sách các agent và các thông tin chung;
- + Xem chi tiết của Agent;

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

	NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	IP DCN	POLICY	VERSION
☐	Localhost\Localdomain	Offline	Default	Phula_test	09/06/2022 10:43:58	05/04/2022 14:49:51	10.61.188.2	phula_test	
☐	Ubuntu18	Offline	Default	Test	09/06/2022 17:24:22	07/06/2022 10:50:23	10.61.188.2	anhn_full_features	3.3.8
☐	N/A	Offline	N/A	N/A	N/A	N/A	N/A	N/A	

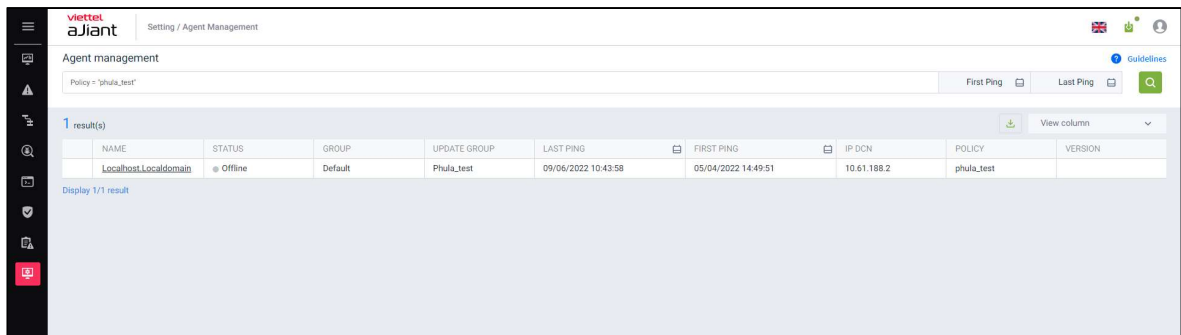
Hệ thống hỗ trợ thực hiện các tính năng:

- 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.
 - 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 "=", "!=", "~";

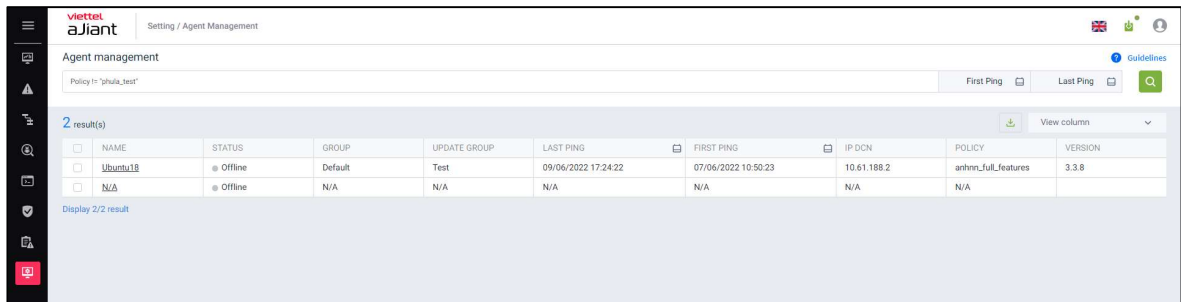


Ví dụ về các câu tìm kiếm:

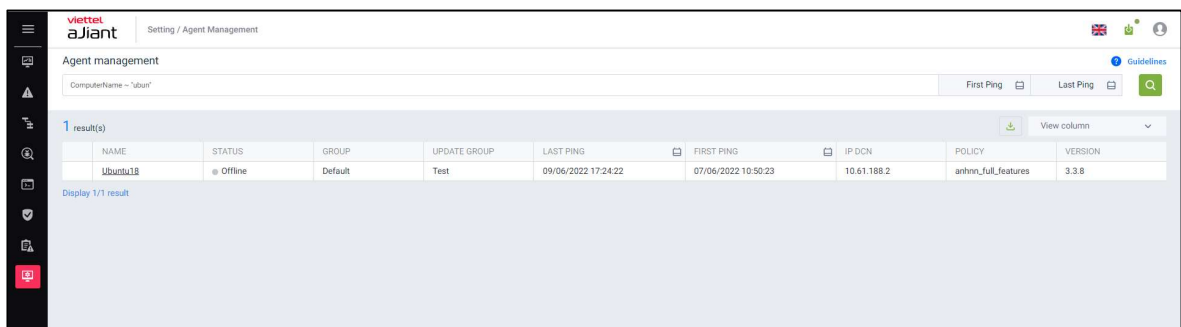
+ Tìm kiếm với điều kiện “=”:



+ Tìm kiếm với điều kiện “!=”:



+ Tìm kiếm với điều kiện “~”:



+ Tìm kiếm theo tiêu chí kết hợp AND:

Agent management

ComputerName = "ubuntu" AND Policy = "anhnm_full_features"

First Ping Last Ping

1 result(s)

NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	IP DCN	POLICY	VERSION
Ubuntu18	Offline	Default	Test	09/06/2022 17:24:22	07/06/2022 10:50:23	10.61.188.2	anhnm_full_features	3.3.8

Display 1/1 result

+ Tìm kiếm theo tiêu chí kết hợp OR:

Agent management

Policy = "anhnm_full_features" OR Policy = "phula_test"

First Ping Last Ping

2 result(s)

NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	IP DCN	POLICY	VERSION
Localhost_Localdomain	Offline	Default	Phula_test	09/06/2022 10:43:58	05/04/2022 14:49:51	10.61.188.2	phula_test	
Ubuntu18	Offline	Default	Test	09/06/2022 17:24:22	07/06/2022 10:50:23	10.61.188.2	anhnm_full_features	3.3.8

Display 2/2 result

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

Agent management

Type to search by queries ...

First Ping Last Ping

3 result(s)

Selected (2) Set Policy Move to group Set update group Cancel

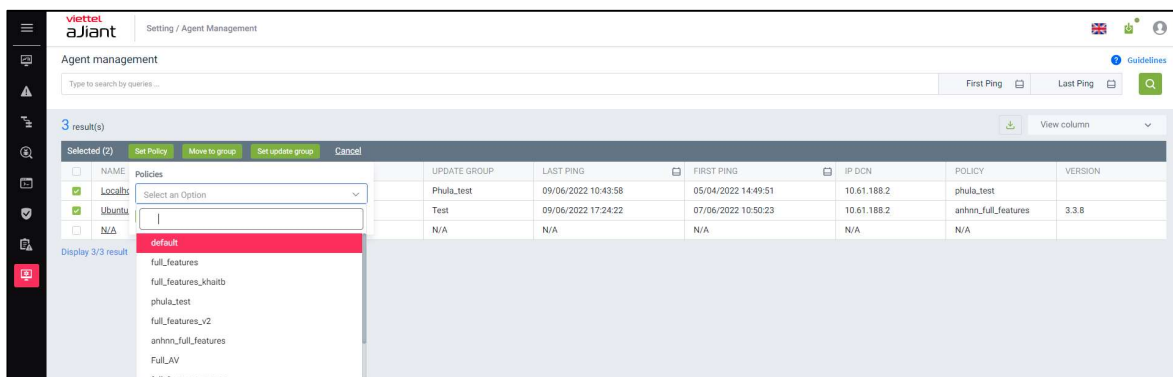
NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	IP DCN	POLICY	VERSION
Localhost_Localdomain	Offline	Default	Phula_test	09/06/2022 10:43:58	05/04/2022 14:49:51	10.61.188.2	phula_test	
Ubuntu18	Offline	Default	Test	09/06/2022 17:24:22	07/06/2022 10:50:23	10.61.188.2	anhnm_full_features	3.3.8
N/A	Offline	N/A	N/A	N/A	N/A	N/A	N/A	

Display 3/3 result

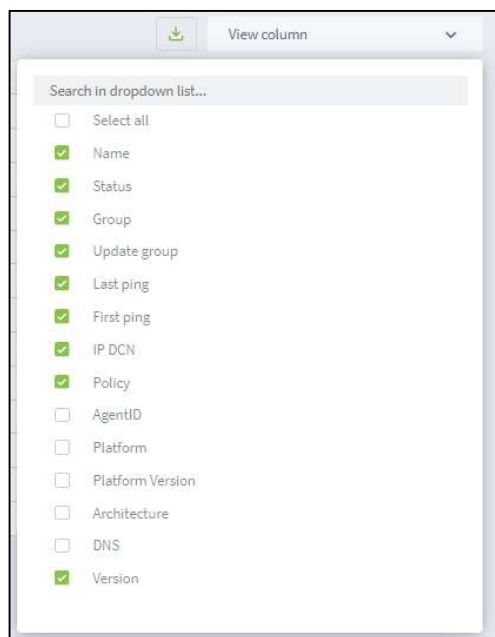
+ Tích chọn 1 agent/ nhiều agent để vào phiên Multiselected;

+ 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”.
- View Column: Cấu hình hiển thị các cột theo mong muốn.



– 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;

The screenshot displays the Viettel Ajiant Agent Management interface. On the left, the 'Agent management' section shows a table with 3 results. The main panel on the right shows the 'General info' tab for the agent 'localhost.localdomain'.

NAME	STATUS	GROUP	UPDATE GROUP
localhost.localdomain	Offline	Default	Phula_test
Ubuntu18	Offline	Default	Test
N/A	Offline	N/A	N/A

Agent properties

Set Policy: phula_test | Set update group: phula_test | Move to group: default | **Save changes**

About this agent

General info

Host Name	localhost.localdomain	IP v4	127.0.0.1
Host ID	015a4d56-e545-241a-e66b-14410ce8c348	IP v6	::1
Setup Version	N/A	MAC	N/A
Operating System	linux	Name	lo
Platform	redhat	IP v4	192.168.121.132
Platform Version	8.2	IP v6	fe80::437edc7a276534ad
Platform Family	rhel	MAC	00:0c:29:e8:c3:48
Architecture	amd64	Name	ens160
Physical Memory	1,843,832		

CPUs

Cores	1
mhz	1992.001000
Model Name	Intel(R) Core(TM) i7-10700T CPU @ 2.00GHz
Vendor ID	GenuineIntel

Default Gateway

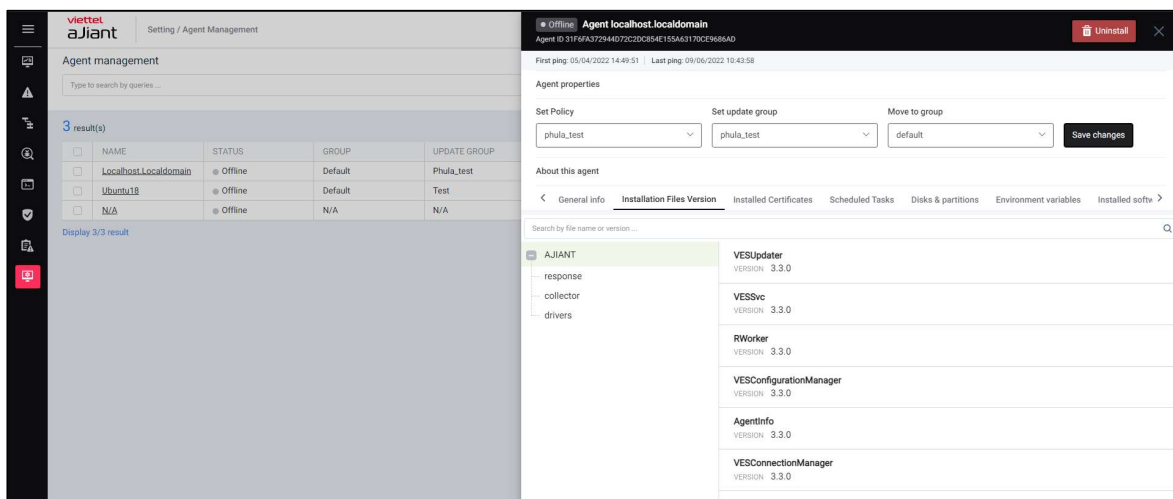
192.168.121.2

DNS Server

192.168.121.2

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

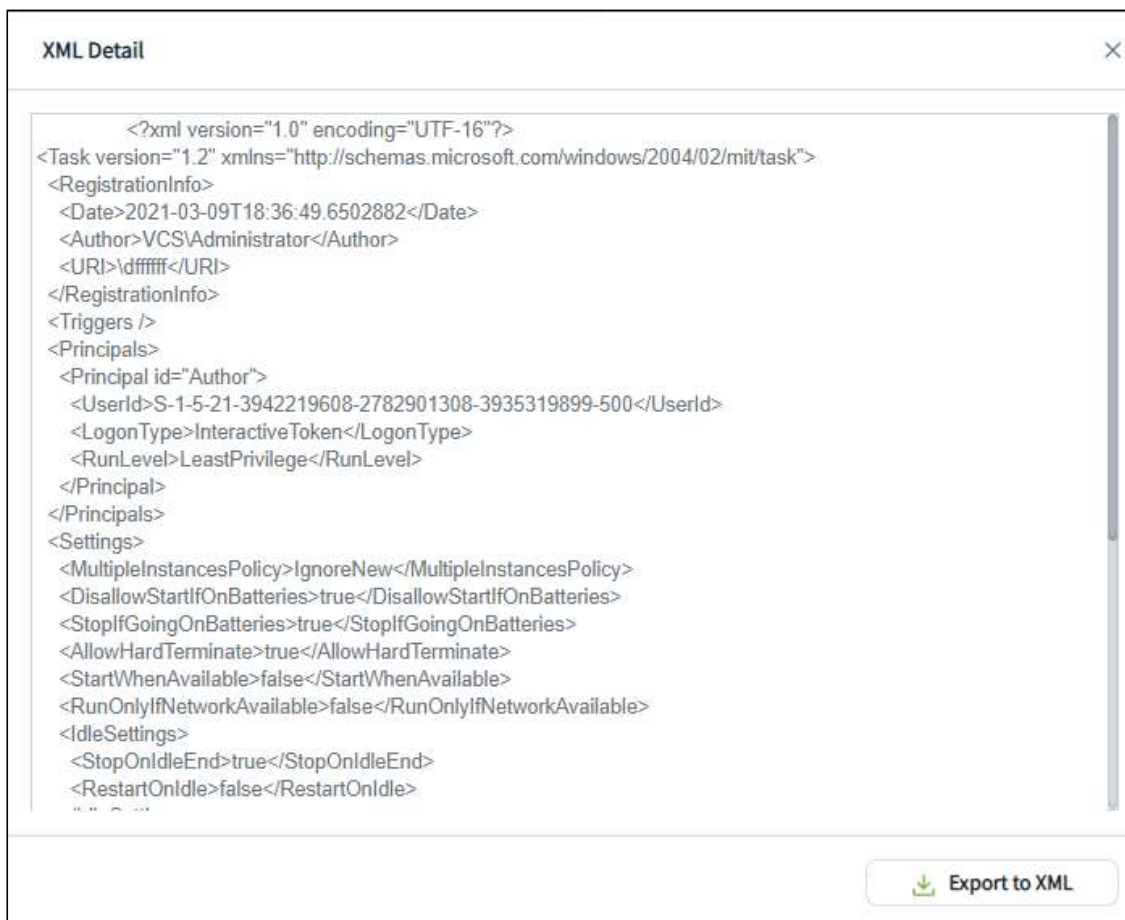
- + Thống kê tất cả các certificate trên máy cài agent, bao gồm các thông tin: Danh sách certificates trên máy, Issued by, Issued to, Expiration date, Status;
- + Trường hợp muốn xem chi tiết với nhiều thông tin hơn, chọn , hiển thị màn hình như sau:



Scheduled Tasks

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

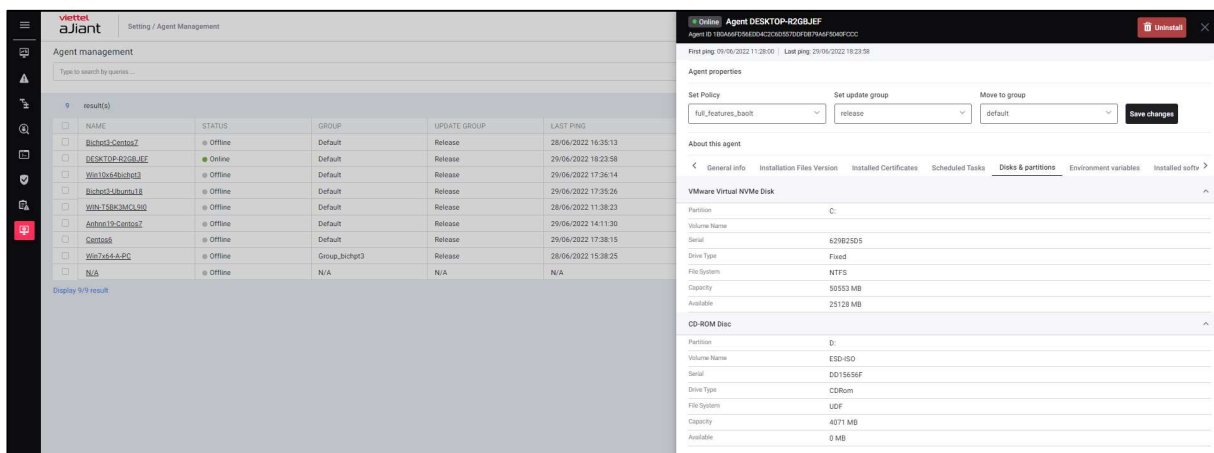
- + Chọn [Show »](#) hoặc [Hide »](#) để tùy chỉnh việc hiển thị thông tin bổ sung cho từng task;
- + Hover vào task và chọn  để xem thông tin đầy đủ của task dưới dạng xml



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

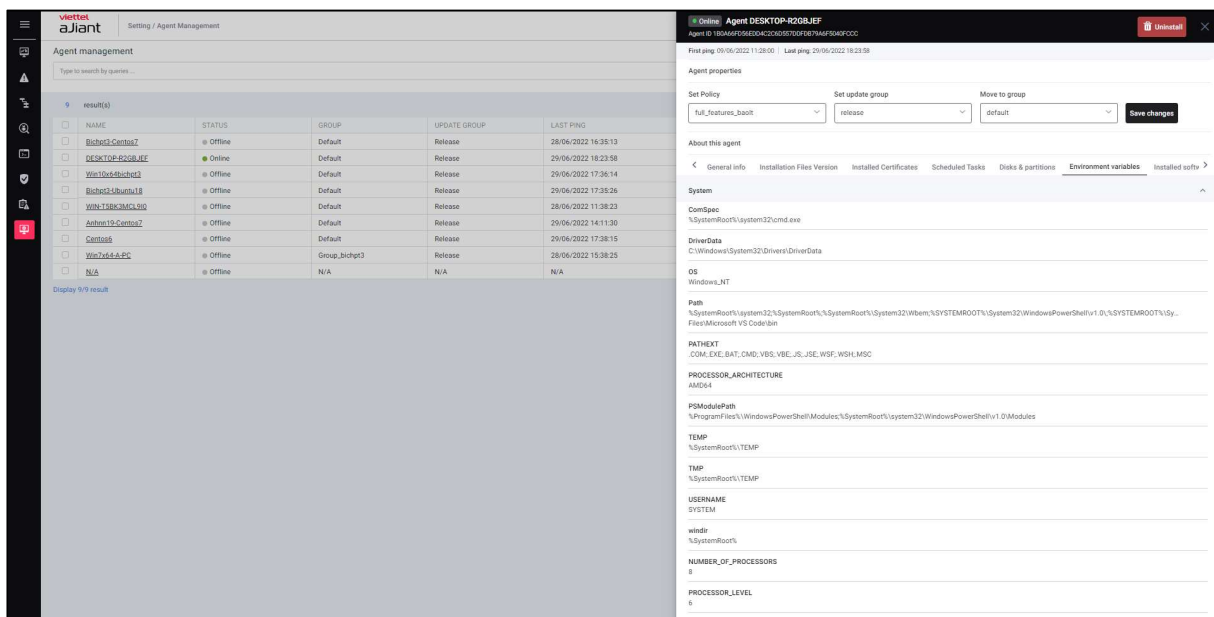
Disks & partitions

- + Thống kê tất cả disks & partitions trên máy cài agent, bao gồm các thông tin: Danh sách Disks, Partition, Volume name, Serial, Drive type, File system, Capacity, Available
- + Chọn  hoặc  để tùy chỉnh việc hiển thị thông tin bổ sung cho từng disk.



Environment variables

- + Thống kê tất cả environment variables trên máy cài agent, bao gồm các thông tin: Danh sách system và users, tên biến, giá trị trực thuộc system hoặc user;
- + Chọn  hoặc  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
 - Chọn nhanh 1 agent/ 1 nhóm các agent để thiết lập Move to group
- + Tích chọn 1 agent/ nhiều agent để vào phiên Multiselected;

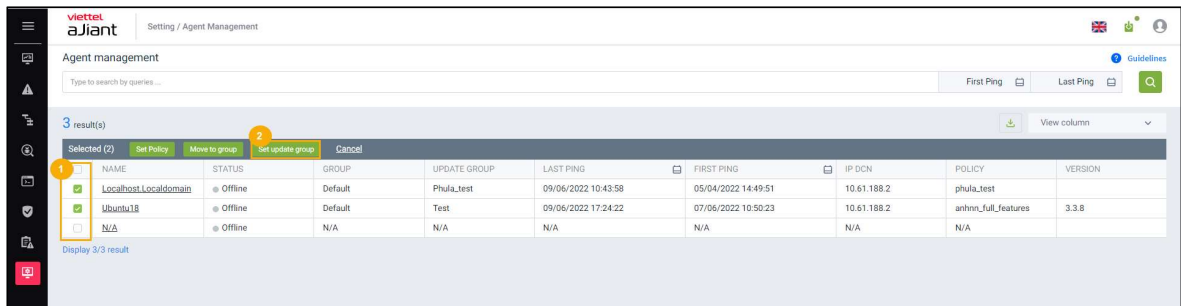
NAME	STATUS	GROUP	UPDATE GROUP	LAST PING	FIRST PING	IP	DCN	POLICY	VERSION
Localhost Localdomain	Offline	Default	PhuLa_test	09/06/2022 10:43:58	05/04/2022 14:49:51	10.61.188.2		phuLa_test	
Ubuntu18	Offline	Default	Test	09/06/2022 17:24:22	07/06/2022 10:50:23	10.61.188.2		anhnm_full_features	3.3.8
N/A	Offline	N/A	N/A	N/A	N/A	N/A		N/A	

- + Thực hiện Move to group:

Danh sách Group trong combobox Move to group:

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

- + Chọn nhanh 1 agent/ 1 nhóm các agent để thiết lập Set update group:
 - Tích chọn 1 agent/ nhiều agent để vào phiên Multiselected;



- Thực hiện Set update group;

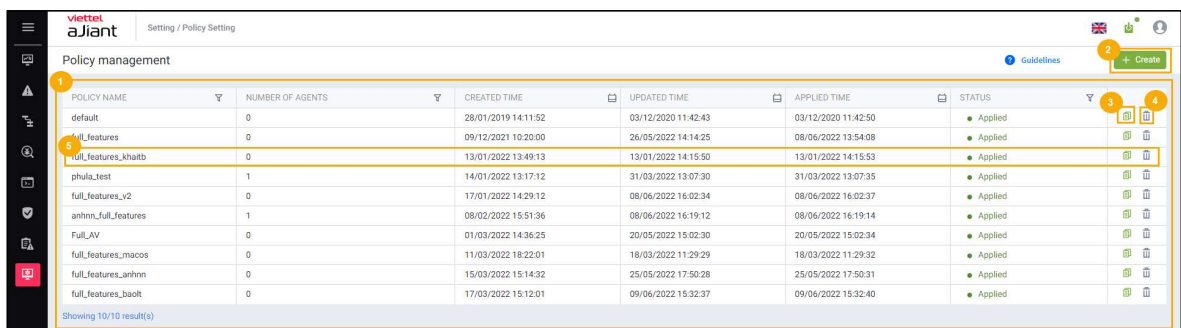
Lưu ý:

- + Move to group: Chuyển agent vào các group có trong màn hình Group management;
- + Update group: chuyển agent vào các group lưu trữ các file chạy dưới Agent, mỗi group có các file chạy khác nhau được định nghĩa trong server.

3.7.2 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:



- Hiện 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

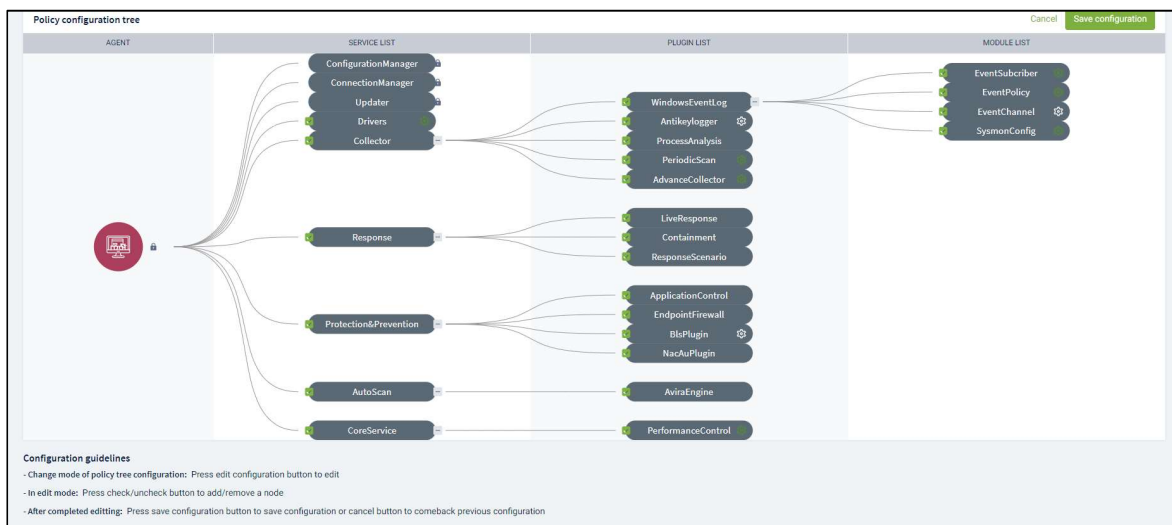
gian cập nhật, Thời gian áp chính sách, trạng thái (có 2 trạng thái: Applied và Not Applied);

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

The screenshot shows a 'Create Policy' popup. At the top right is a green '+ Create' button (callout 1). Below it is a text input field for 'POLICY NAME' containing 'full_features_huyenpk' (callout 2). At the bottom left is a green 'Create' button (callout 3). A note below the field states 'Cannot edit policy name after created'.

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

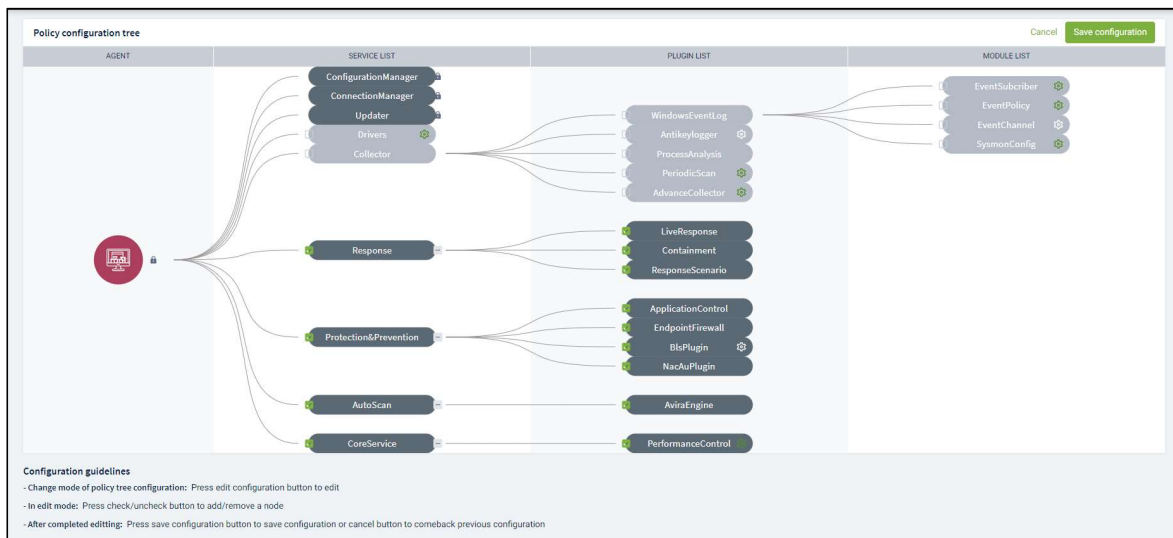
Sau khi tạo mới policy thành công hệ thống sẽ hiển thị màn hình chi tiết của 1 policy:



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:

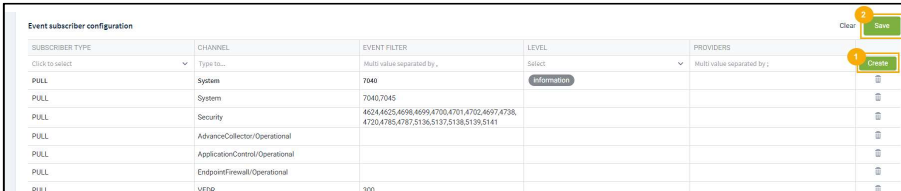
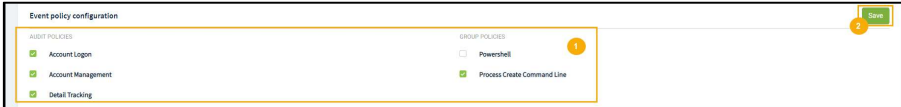


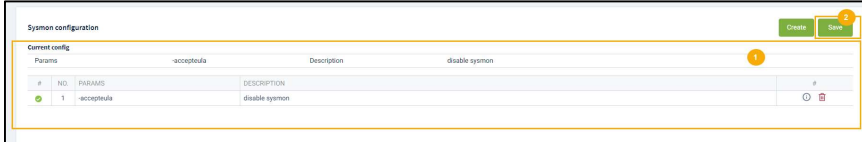
Bước 3: Sau khi hoàn thành chế độ edit:

- 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 đây.

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

Module/plugin	Mô tả
WindowsEventLog	- Cấu hình WindowsEventLog: Lầu hình các nguồn log lấy dưới Agent + EventSubscriber: 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

Module/plugin	Mô tả
	“-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:

Module/plugin	Mô tả
	- Retention: có lưu log xoay vòng hay không (Nếu chọn Retention 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: - Scan cycle: min là 1 phút, max là 180 phút; - Chọn ít nhất 1 loại Keylogger; + Whitelist setting: cấu hình whitelist 1 số phần mềm theo đường dẫn của file trên ổ đĩa hoặc theo chữ ký số (cert) của file chạy key logger

Module/plugin	Mô tả
	- 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

Module/plugin	Mô tả																		
	Version disable autoscanner Description disable autoscanner Data configuration for Windows <pre>1 { 2 "auto_scan": { 3 "enable_auto_scan": false 4 } 5 }</pre> Cancel Create Các trường hỗ trợ config trong luồng auto scan như sau: <table><tr><th>Config</th><th>Type</th><th>Mô tả</th></tr><tr><td>enable_auto_scan</td><td>bool</td><td>bật/tắt auto scan</td></tr><tr><td>max_queue_length</td><td>integer</td><td>số lượng phần tử tối đa của scan queue và disinfect queue</td></tr><tr><td>scan_sleep_time</td><td>mili-second</td><td>thời gian sleep giữa 2 lần scan file, tránh xử lý liên tục gây cao tải hệ thống</td></tr><tr><td>scan_timeout</td><td>mili-second</td><td>thời gian tối đa cho phép av engine scan một file</td></tr><tr><td>scan_max_filesize</td><td>byte</td><td>kích thước file được scan tối đa, file lớn hơn kích thước này sẽ bỏ qua ko scan</td></tr></table>	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
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																	

Module/plugin	Mô tả																	
	rescan_removal_faile d	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 disinfect 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 <table><tr><th>Config</th><th>Type</th><th>Mô tả</th></tr><tr><td>max_manual_scan</td><td>integer</td><td>số lượng manual scan tối đa đồng thời</td></tr><tr><td>max_queue_lengt h</td><td>integer</td><td>độ dài tối đa của manual scan queue</td></tr><tr><td>scan_sleep_time</td><td>mili-second</td><td>thời gian sleep trước khi scan file tiếp theo, tránh xử lý liên tục gây cao tải hệ thống</td></tr><tr><td>scan_timeout</td><td>mili-second</td><td>thời gian tối đa cho phép av engine scan một file</td></tr></table>				Config	Type	Mô tả	max_manual_scan	integer	số lượng manual scan tối đa đồng thời	max_queue_lengt h	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
Config	Type	Mô tả																
max_manual_scan	integer	số lượng manual scan tối đa đồng thời																
max_queue_lengt h	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																

Module/plugin	Mô tả		
	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
AntiRansomware	AntiRansomware: cho phép thay đổi các config khi diệt mã độc mã hóa tổng tiền		
	- Yêu cầu: Chọn Auto Scan -> chọn Anti Ransomware		
	Các trường hỗ trợ config như sau:		
	Config	Type	Mô tả
	silent	bool	bật tắt chế độ hoạt động silent
	protect_ext	string list	danh sách đuôi file được bảo vệ
	protect_whitelist	string list	danh sách folder được white list không bảo vệ
	actor_whitelist	string list	danh sách file, folder chứa process được phép thực hiện hành vi

Module/plugin	Mô tả					
HIPS	HIPS: cho phép thay đổi config khi diệt mã độc dựa trên hành vi					
	- Yêu cầu: 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>	Config	Type	Mô tả	silent	bool
Config	Type	Mô tả				
silent	bool	bật tắt chế độ hoạt động silent				

Bước 5: Click nút  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.

Clone from policy:
test_sample

NAME OF POLICY

Cannot edit name of policy after create policy



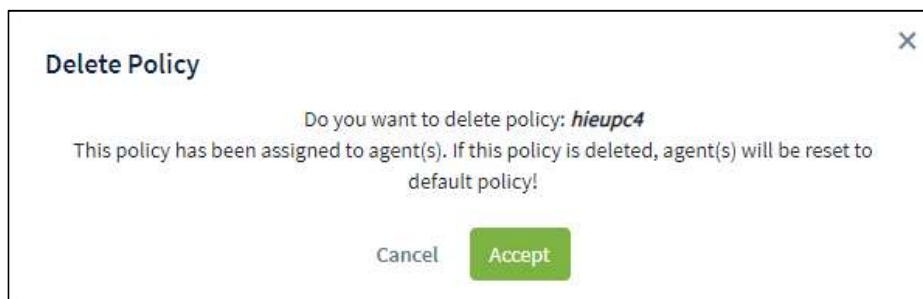
- + Xóa chính sách: Click vào nút  hệ thống hiển thị pop up để người dùng đưa ra quyết định xóa hay không?

Delete Policy

Do you want to delete policy: **0503_test1**

Cancel 

- + 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.

3.7.3 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;
 - 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...

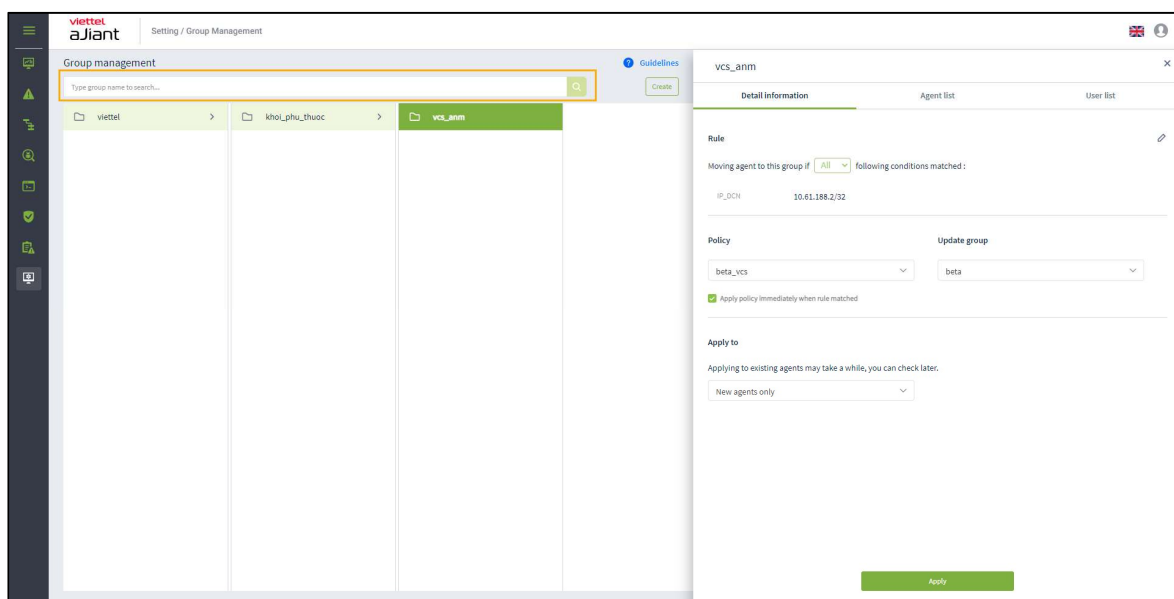
Mỗi nhóm gồm tên nhóm, thông tin cấu hình của nhóm (rule, policy, apply to), và danh sách agent thuộc nhóm.

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

– 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.

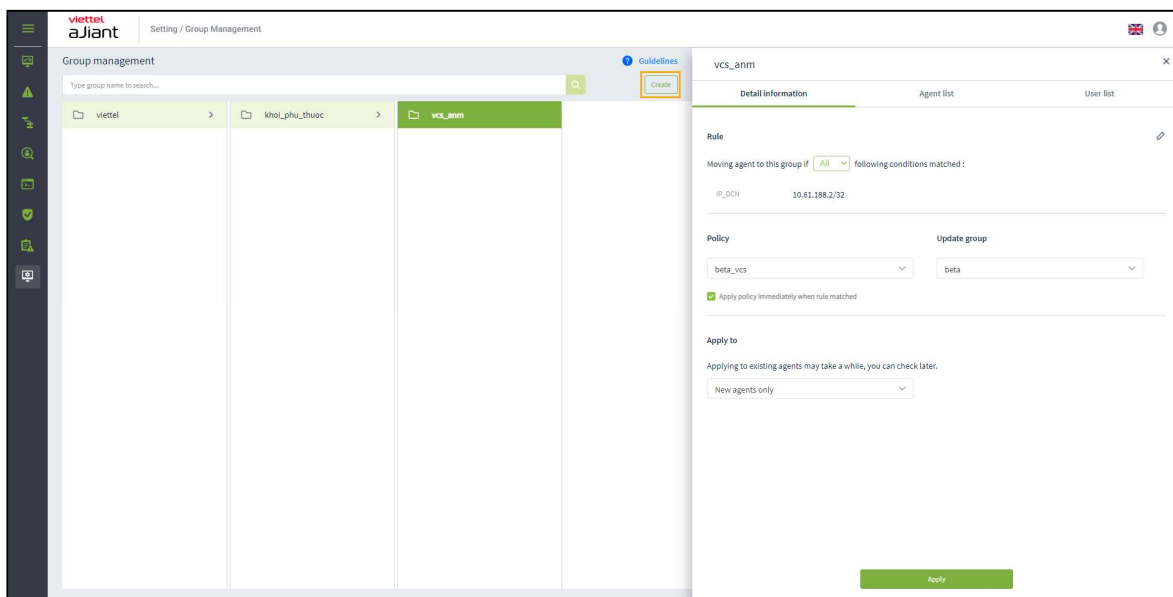
Khi click vào menu góc phải mỗi bản ghi cũng hiển thị 2 option: Go to group và Delete group.

– Thêm mới nhóm:

- + User đăng nhập thuộc group root: Có thể thêm 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 thêm 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 ;

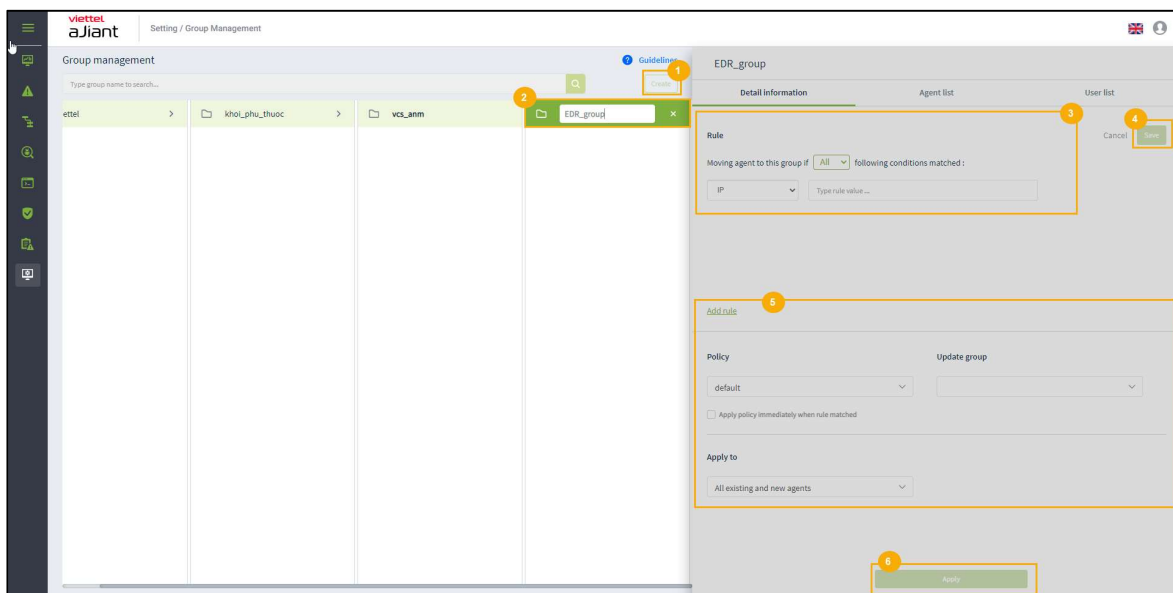


- + Nếu tạo mới nhóm là nhóm con trong một nhóm gốc hoặc nhóm cấp 1, cấp 2... thì click vào nhóm cha sau đó click “Create” trên màn hình hoặc hover vào cuối danh sách nhóm cùng cấp và click “Create”;

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.
 - 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;

vcs_anm

Detail information Agent list User list

Rule Edit

Moving agent to this group if **All** following conditions matched:

IP_DCN 10.61.188.2/32

Policy **Update group**

beta_vcs beta

☒ Apply policy immediately when rule matched

Apply to

Applying to existing agents may take a while, you can check later.

New agents only

Apply

vcs_anm

Detail information Agent list User list

Rule Cancel Save

Moving agent to this group if **All** following conditions matched:

IP_DCN 10.61.188.2/32

[Add rule](#)

Policy **Update group**

beta_vcs beta

☒ Apply policy immediately when rule matched

Apply to

New agents only

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.

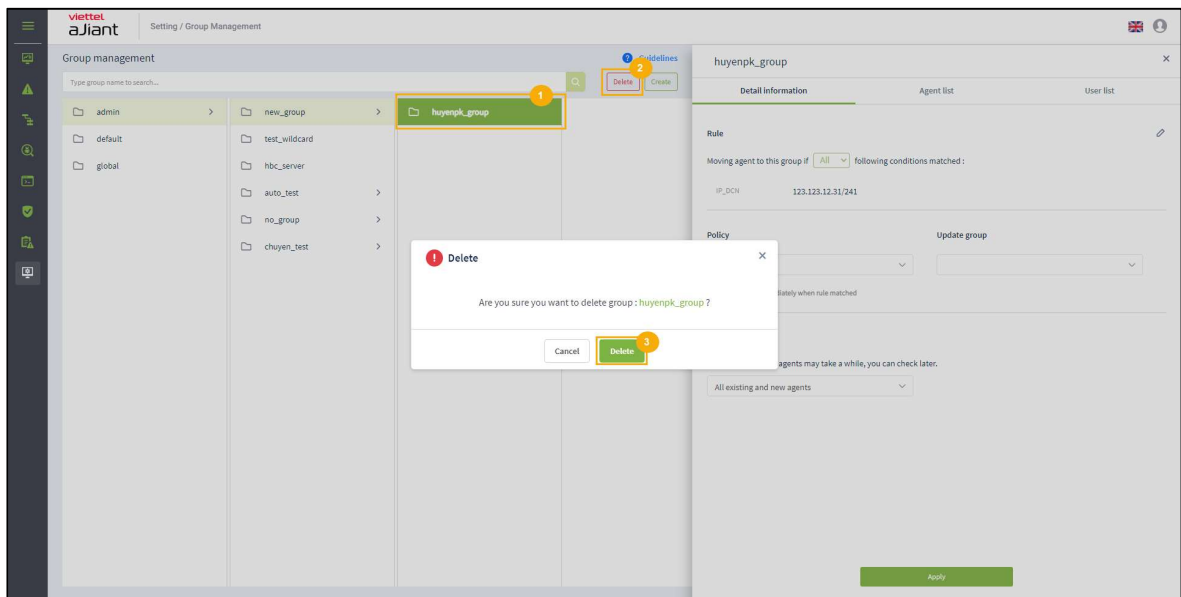
- + Trường hợp sửa xong các thành phần của nhóm rồi click Apply thì nội dung chỉnh sửa được lưu lại, đồng thời nếu có lựa chọn “All existing agents” trong phần “Apply to” thì thực hiện quét thông tin toàn bộ agent trong hệ thống và chuyển nhóm cho agent, sau đó cập nhật Agent list.

Đối với Agent mới xử lý tương tự như trên.

– 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

vcs_anm

Detail information

Agent list

User list

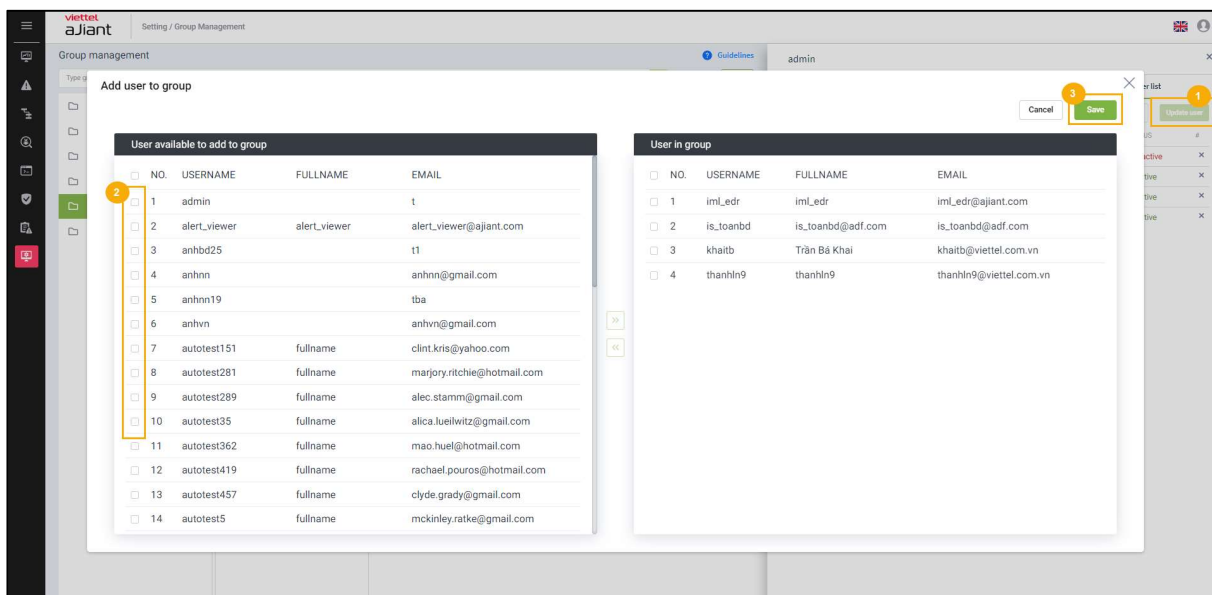
50/279 agent(s)

Search agent...

AGENT ID	HOSTNAME	GROUP	STATUS	POLICY	#
4AE8D11BFB5037899FD20F5CEDF	ANM-HOANGND31	vcs_anm	● Offline	full_features_with_autoscan_selfdefense	✕
1B37DBD39D0F632D9F7BEFBE421	ANM-SANGLV11	vcs_anm	● Offline	full_features_with_autoscan_selfdefense	✕
75E895D48390F5C642FC57AD62C	ANM-THONGND7	vcs_anm	● Offline	full_features_with_autoscan_selfdefense	✕
1F8AF3B15A9A343F992D3596EBA3	ANM-HOABT21	vcs_anm	● Offline	full_features_with_autoscan_selfdefense	✕
2FA6F1E3E016C748600CAF0C1A7	ubunbu-18	vcs_anm	● Offline	full_features_3.3.0	✕
5CA1E94EC4C99ACE5EDB202FD7E	ANM-ANHNN19	vcs_anm	● Offline	full_features_with_autoscan_selfdefense	✕
9ACE6C4888F8E1F04428BC8BDD1	IS-LANNT	vcs_anm	● Offline	beta_vcs	✕
143E35A30D5CC8EFC65AC7A83EB1	ANM-THANGNM14	vcs_anm	● Offline	full_features_with_autoscan	✕
A04CF97FF6250F800308CE68352	ANM-DUCDH8	vcs_anm	● Offline	full_features_with_autoscan_selfdefense	✕

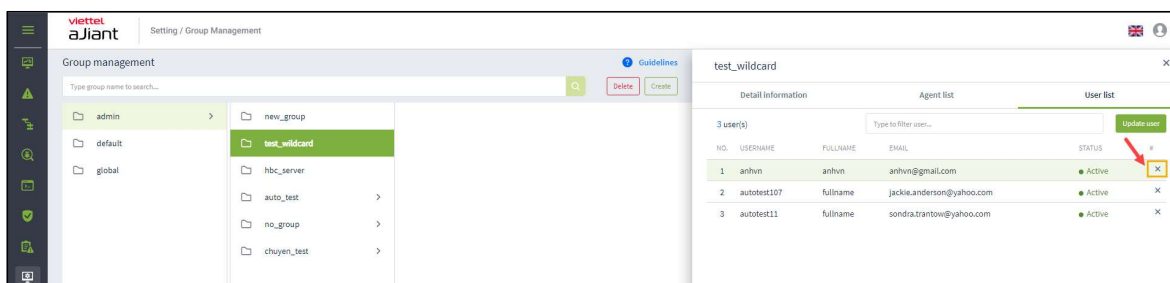
Lưu ý: trường hợp xóa một nhóm cha:

- + 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;
 - Thêm mới user vào group



Danh sách user:

- + User đăng nhập thuộc group root: Hiện thị tất cả User trong hệ thống;
- + User đăng nhập thuộc group default: Hiện thị user chỉ thuộc default;
- + User đăng nhập thuộc group cha: Hiện 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: Hiện thị user đang login:
- Xóa user



3.7.4 Account Management

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

3.7.4.1 Permission management

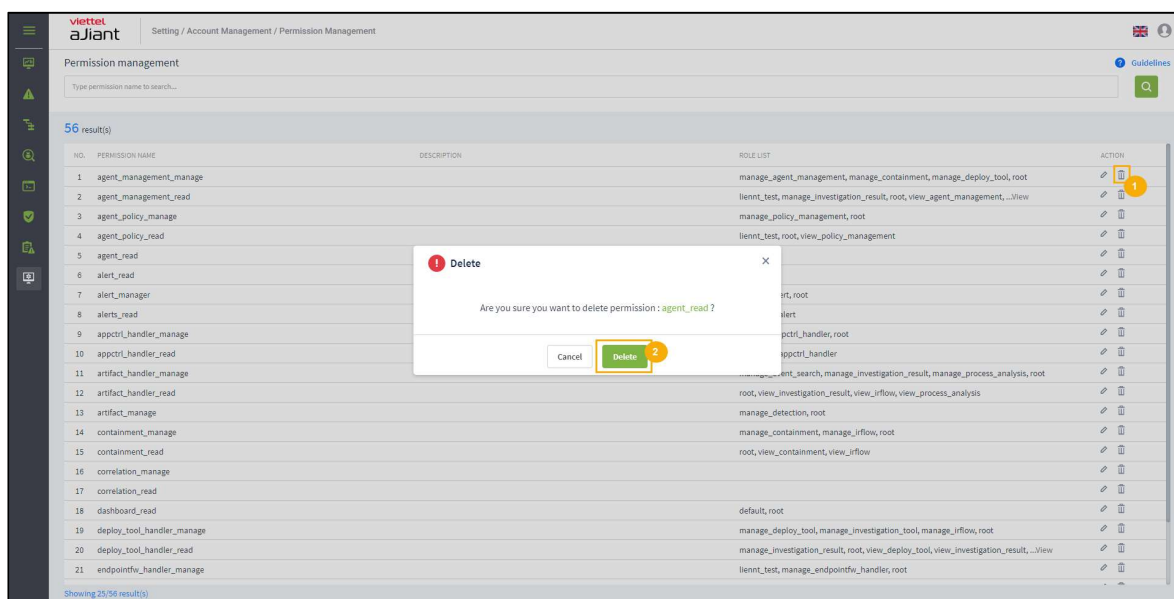
Quản lý các quyền truy cập vào tài nguyên (API) của hệ thống. 1 permission là quyền truy cập vào 1 tài nguyên xác định (API) của hệ thống;

Các chức năng chính trên màn hình này:

- + Quản lý các permission;
- + Tìm kiếm permission;
- + Xóa permission;
 - 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
 - Tìm kiếm permission: nhập ký tự tìm kiếm vào textbox Search > click Enter hoặc nút “Search” => hiển thị danh sách permission thỏa mãn

NO.	PERMISSION NAME	DESCRIPTION	ROLE LIST	ACTION
1	agent_management_manage		manage_agent_management, manage_containment, manage_deploy_tool, root	
2	agent_management_read		liennt_test, manage_investigation_result, root, view_agent_management, ...View	
3	agent_policy_manage		manage_policy_management, root	
4	agent_policy_read		liennt_test, root, view_policy_management	
5	agent_read			
6	alert_read			
7	alert_manager		manage_alert, root	
8	alerts_read		root, view_alert	
9	appctrl_handler_manage		manage_appctrl_handler, root	
10	appctrl_handler_read		root, view_appctrl_handler	
11	artifact_handler_manage		manage_event_search, manage_investigation_result, manage_process_analysis, root	
12	artifact_handler_read		root, view_investigation_result, view_inflow, view_process_analysis	
13	artifact_manage		manage_detection, root	
14	containment_manage		manage_containment, manage_inflow, root	
15	containment_read		root, view_containment, view_inflow	
16	correlation_manage			
17	correlation_read			
18	dashboard_read		default, root	
19	deploy_tool_handler_manage		manage_deploy_tool, manage_investigation_tool, manage_inflow, root	
20	deploy_tool_handler_read		manage_investigation_result, root, view_deploy_tool, view_investigation_result, ...View	
21	endpointfw_handler_manage		liennt_test, manage_endpointfw_handler, root	

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

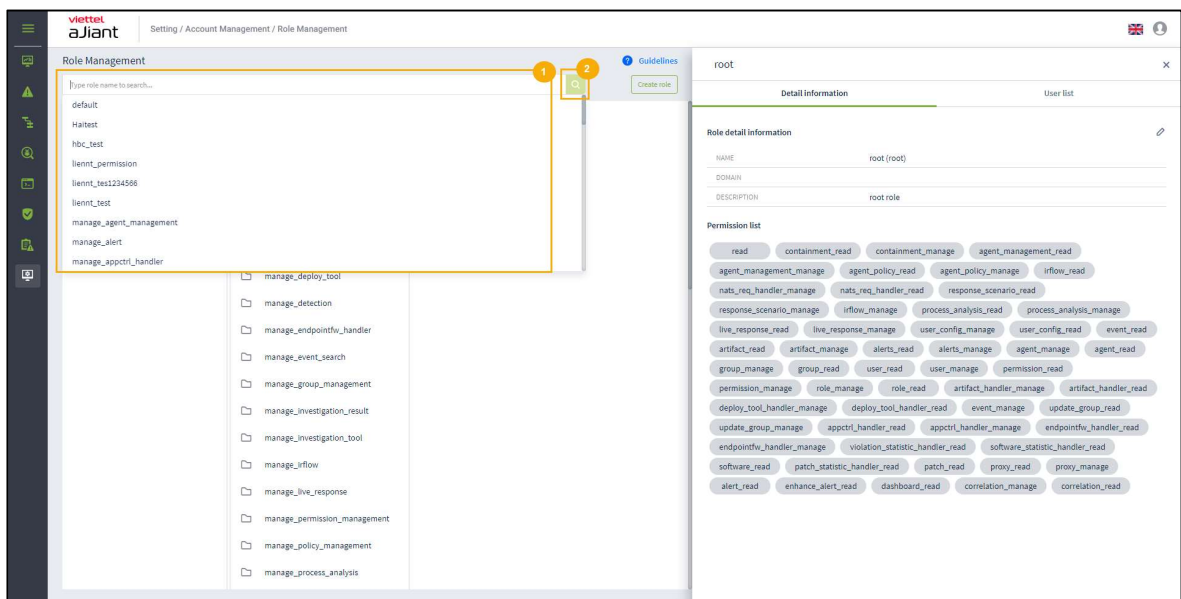


3.7.4.2 Role Management

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: Hiện thị tất cả Role trong hệ thống;
 - User đăng nhập thuộc Role default: Hiện thị Role default;
 - User đăng nhập thuộc Role cha: Hiện thị tất cả Role thuộc của user đang login và group con tương ứng;
 - User đăng nhập thuộc Role có một hoặc nhiều con: Hiện thị tất cả Role thuộc Role của user đang login;
 - + Tìm kiếm role;
 - + Thêm mới role;
 - + Xóa role.
- 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)
 - 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;
 - Thêm mới role:
- + User đăng nhập thuộc group root: Có thể thêm 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 thêm mới role cùng cấp;
- + User đăng nhập thuộc group một hoặc nhiều con: có thể thêm mới group con tương ứng của group thuộc user đang login.

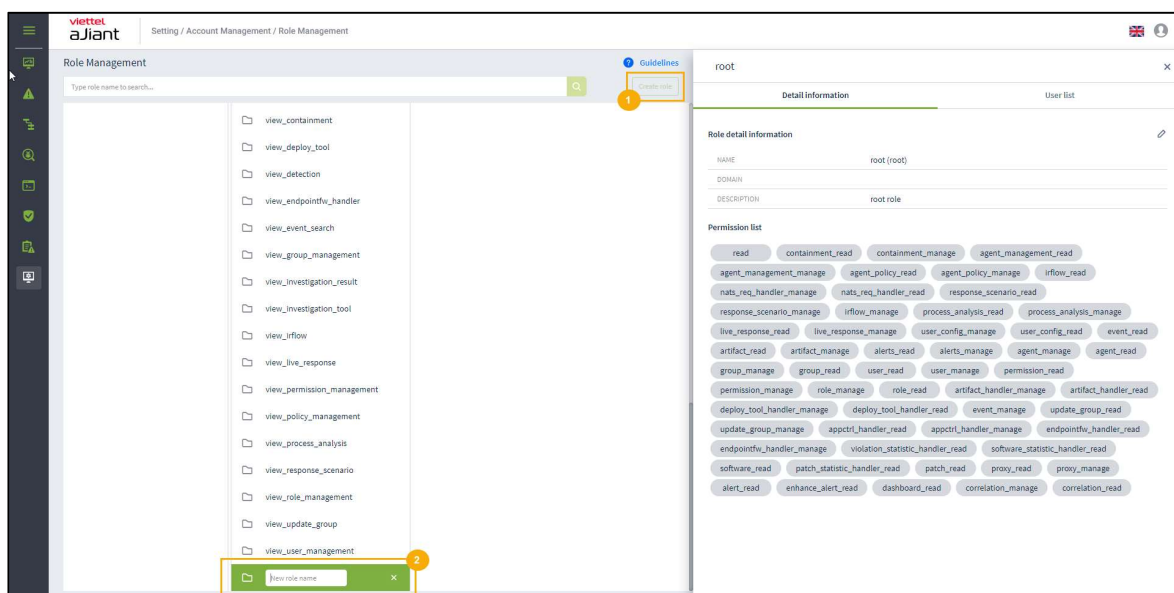
Bước 1: Có các cách tạo mới role như sau:

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:

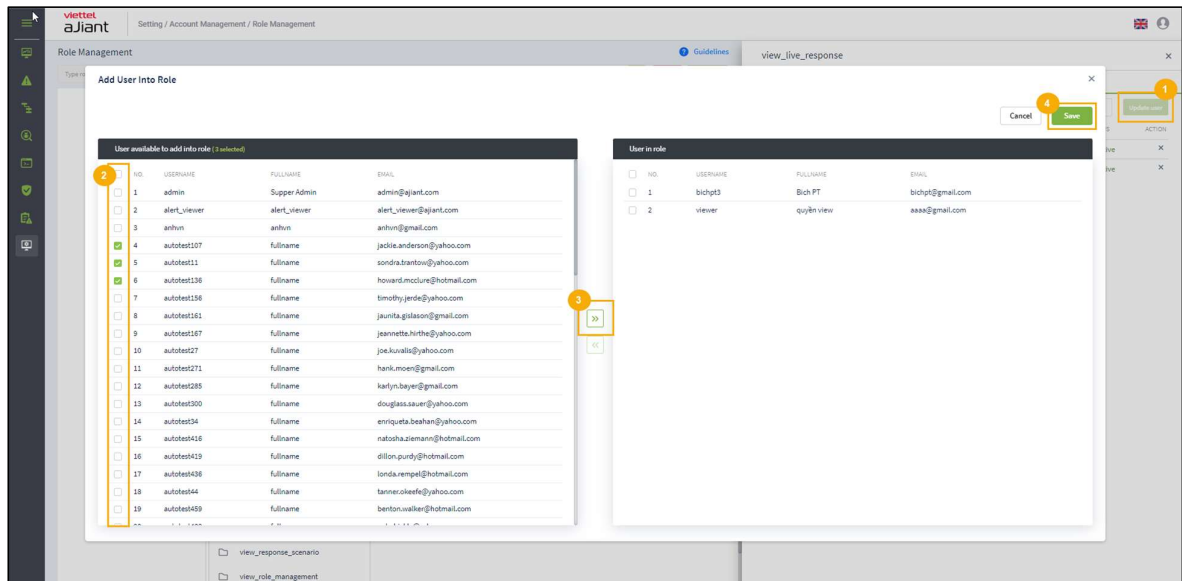
- + User đăng nhập thuộc group root: Có thể sửa tất cả role trong hệ thống;
- + User đăng nhập thuộc group default: Không được sửa role default;
- + User đăng nhập thuộc group cha: Có thể sửa tất cả role thuộc đang login và role con role ;
- + User đăng nhập thuộc group một hoặc nhiều con: Có thể sửa 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.

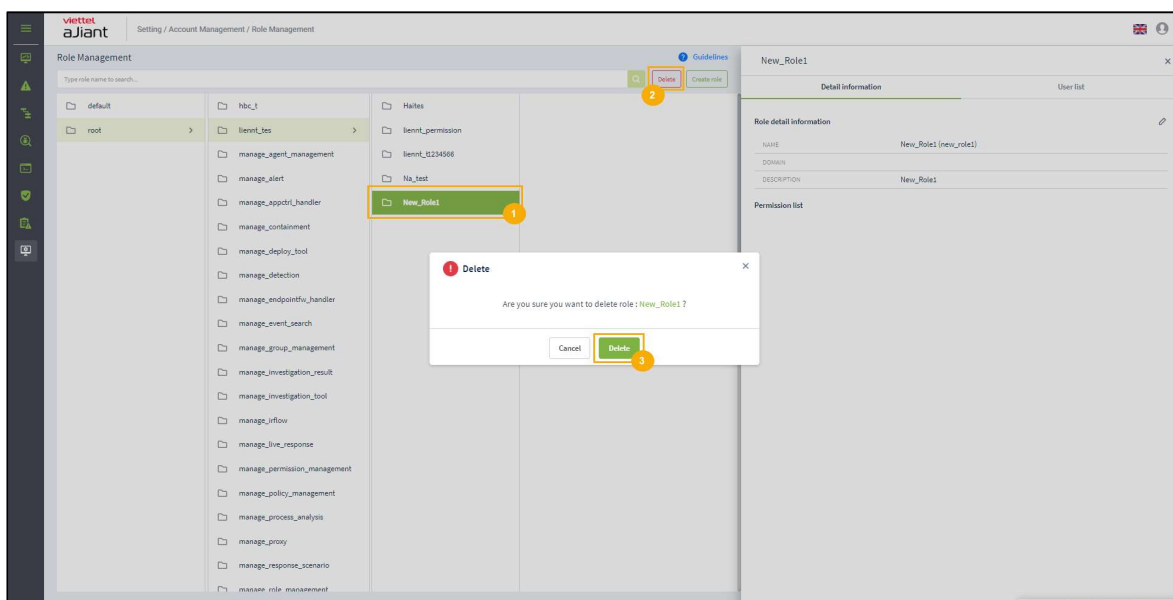
Bước 3: Chuyển sang tab User list để thêm role vào danh sách role của User

- + 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;



- 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.

3.7.4.3 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;
- 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

User management

Type username to search...

44 result(s)

NO.	USERNAME	FULLNAME	EMAIL	LAST LOGIN	STATUS	ACTION
1	admin		t	N/A	Active	
2	alert_viewer	alert_viewer	alert_viewer@ajiant.com	N/A	Active	
3	anhbd25		t1	N/A	Active	
4	anhnn		anhnn@gmail.com	N/A	Active	
5	anhnn19		tba	N/A	Active	
6	anhvn		anhvn@gmail.com	N/A	Active	
7	autotest151	fullname	clint.kris@yahoo.com	N/A	Active	
8	autotest281	fullname	marjory.richie@hotmail.com	N/A	Active	
9	autotest289	fullname	alec.stamm@gmail.com	N/A	Active	
10	autotest335	fullname	alica.loellwitz@gmail.com	N/A	Active	
11	autotest382	fullname	mao.huel@hotmail.com	N/A	Active	

+ Create

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

viettel
ajiant

Setting / Account Management / User Management

User management

Type username to search...

66 result(s)

NO.	USERNAME	FULLNAME	EMAIL	LAST LOGIN	STATUS	ACTION
1	admin	Super Admin	admin@ajiant.com	N/A	Active	
2	alert_viewer		alert_viewer@ajiant.com	N/A	Active	
3	anhvn				Active	
4	autotest107				Active	
5	autotest111				Active	
6	autotest136				Active	
7	autotest156				Active	
8	autotest161				Active	
9	autotest167				Active	
10	autotest27				Active	
11	autotest271				Active	
12	autotest285				Active	
13	autotest300				Active	
14	autotest314				Active	
15	autotest416	fullname	natosha.ziemann@hotmail.com	N/A	Active	
16	autotest419	fullname	dillon.purdy@hotmail.com	N/A	Active	
17	autotest436	fullname	londa.rempel@hotmail.com	N/A	Active	
18	autotest444	fullname	tanner.okeefe@yahoo.com	N/A	Active	
19	autotest459	fullname	benton.walker@hotmail.com	N/A	Active	
20	autotest483	fullname	pete.hickie@yahoo.com	N/A	Active	
21	autotest489	fullname	gerald.ledner@gmail.com	N/A	Active	
22	autotest493	fullname	stefany.hill@yahoo.com	N/A	Active	

Showing 25/66 result(s)

Create

User information Role Group

Username

Fullname

Email

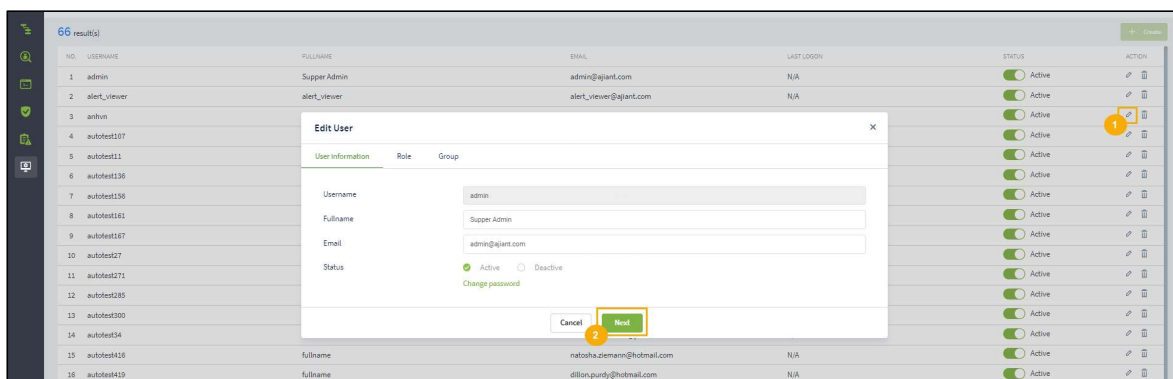
Password

Status ☒ Active ☐ Deactive

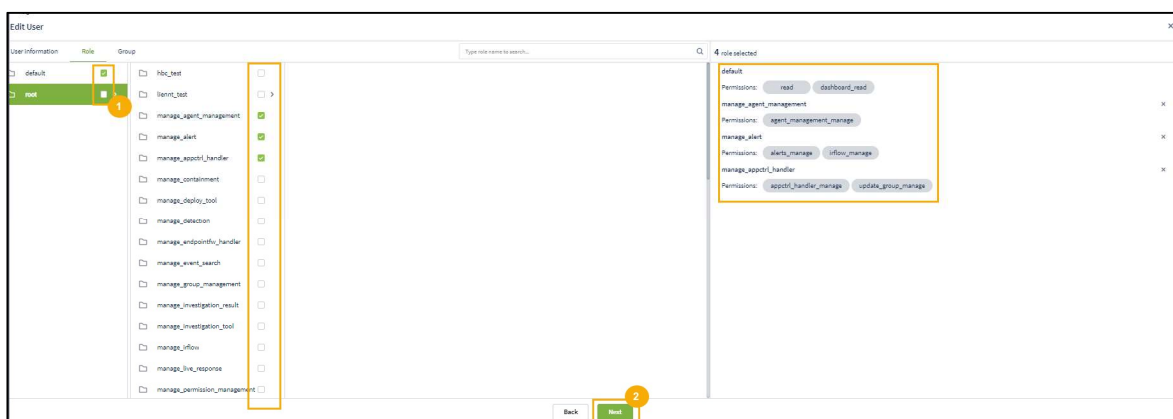
Cancel Next

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

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

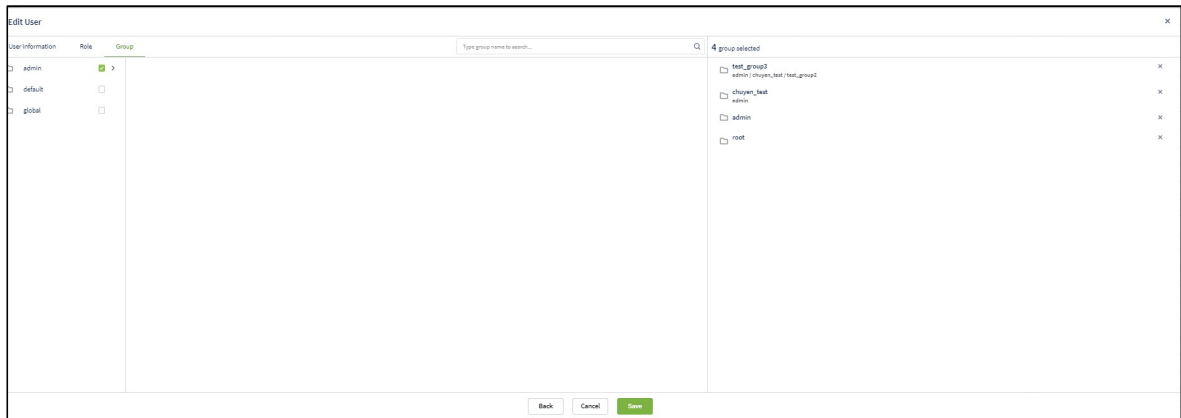


Trên màn hình add role cho User, có thể tìm kiếm các role tương tự phần tìm kiếm tài khoản, sau khi nhập các ký tự tìm kiếm vào textbox “Search” > click icon Search hoặc Enter hiện màn hình các role thỏa mãn điều kiện tìm kiếm;



- + 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;

ID	USERNAME	FULLNAME	EMAIL	LAST LOGON	STATUS	ACTION
1	admin	Super Admin	admin@ajant.com	N/A	Active	
2	aler_viewer	aler_viewer	aler_viewer@ajant.com	N/A	Active	
3	arthur	arthur	arthur@gmail.com	28/04/2022 10:44:40	Active	
4	autotest07	fullname	jackie.anderson@yahoo.com	N/A	Active	
5	autotest11	fullname	sondra.trantov@yahoo.com	N/A	Active	
6	autotest136	fullname	howard.mclure@hotmail.com	N/A	Active	
7	autotest156	fullname	timothy.jerde@yahoo.com	N/A	Active	
8	autotest161	fullname	jaunita.glaum@gmail.com	N/A	Active	
9	autotest167	fullname	N/A	N/A	Active	
10	autotest27	fullname	N/A	N/A	Active	
11	autotest272	fullname	N/A	N/A	Active	
12	autotest285	fullname	N/A	N/A	Active	
13	autotest300	fullname	N/A	N/A	Active	
14	autotest34	fullname	N/A	N/A	Active	
15	autotest416	fullname	natasha.siemann@hotmail.com	N/A	Active	
16	autotest419	fullname	dillon.purdy@hotmail.com	N/A	Active	

Bật tính năng xác thực 2 bước cho tài khoản:

Bước 1: Vào giao diện My profile như ảnh dưới

kYXRicGlja2VyljoiRmlyc3QgUGluZylsImtleV90aW11IjoilwiawW50ZXJ2YWxfGltZSI6MCwidH...

First Ping

Export

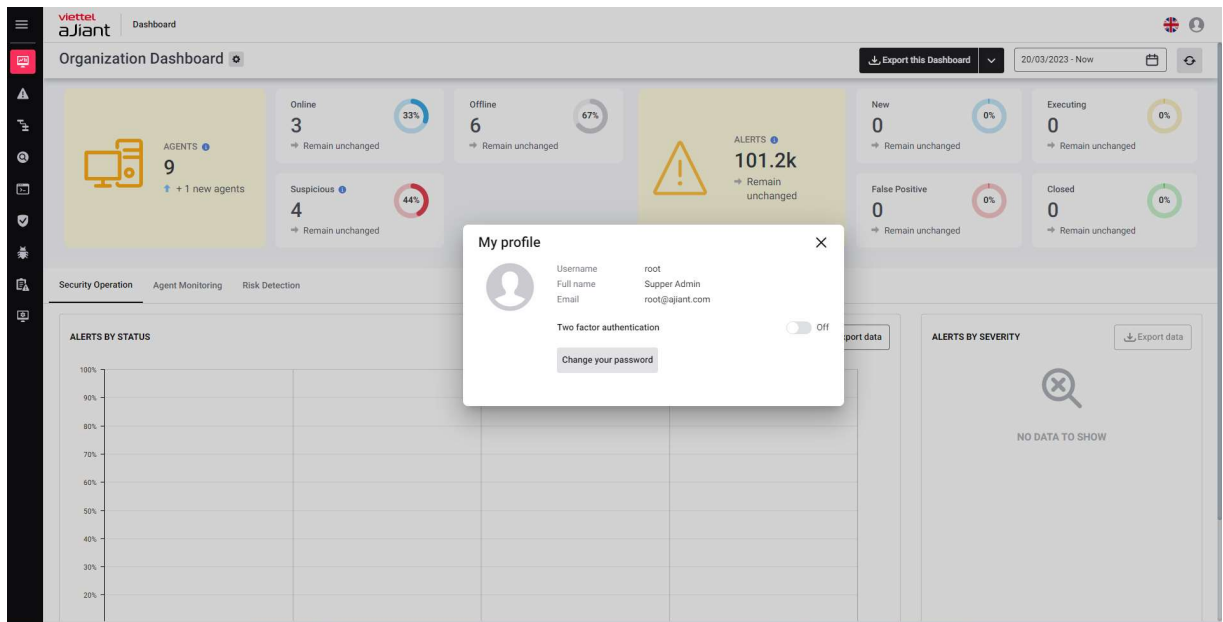
My profile

About VCS-aJiant

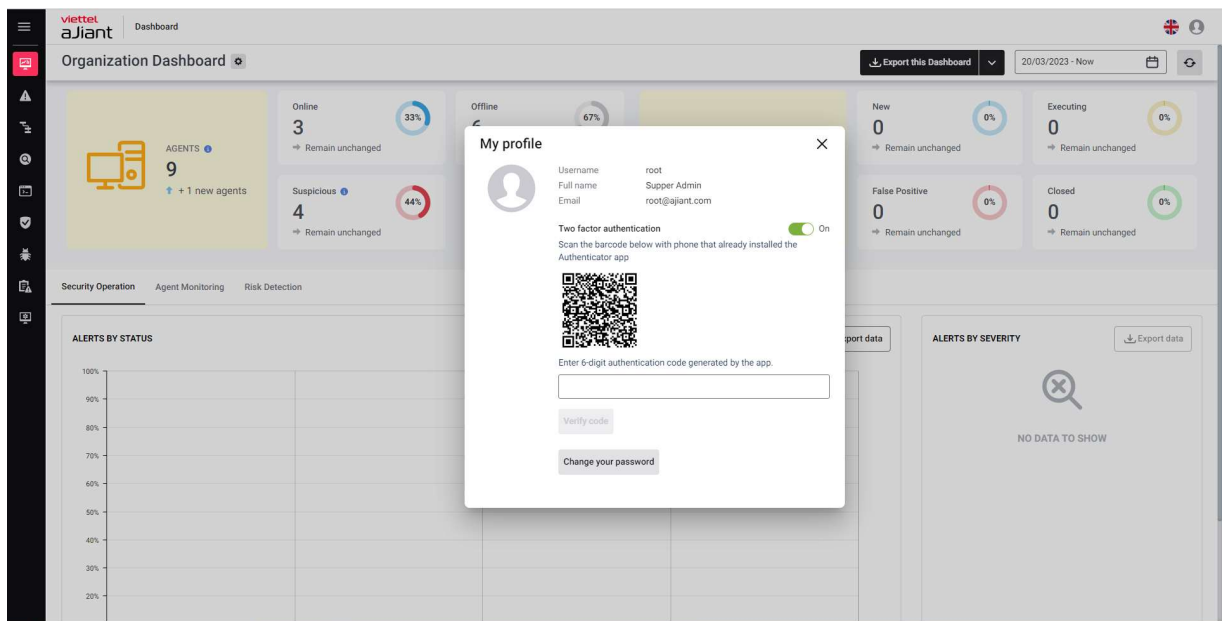
Sign out

First ping	IP DCN	Policy	
25/11/2021 07:14:51	10.207.26.203	full_features_3.3.0	3.3.37
23/11/2022 08:24:49	10.61.74.206	full_features_3.3.0	3.3.37
20/07/2020 17:24:36	10.230.65.69	full_features_3.3.0_linux	3.3.36
22/01/2023 11:31:19	10.61.1.141	nac_plugin_only	3.3.37
13/08/2020 12:05:38	10.230.246.204	full_features_3.3.0_linux	3.3.36
25/09/2022 20:33:15	192.168.81.44	full_features_3.3.0	3.3.37

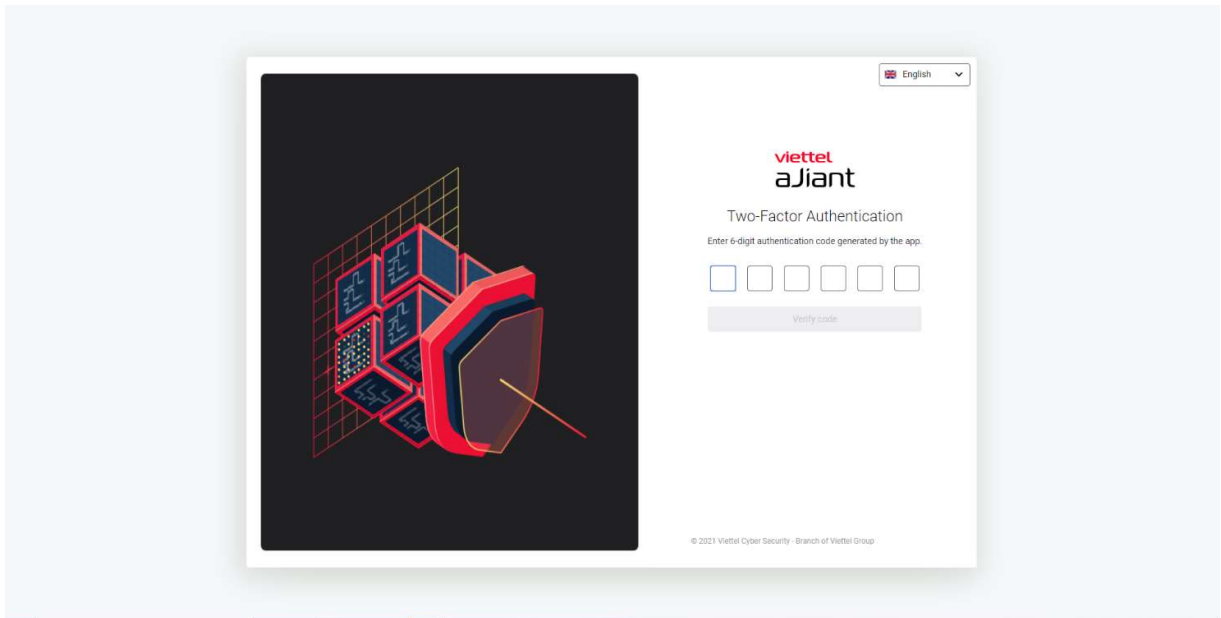
Bước 2: Click để bật Two Factor authentication



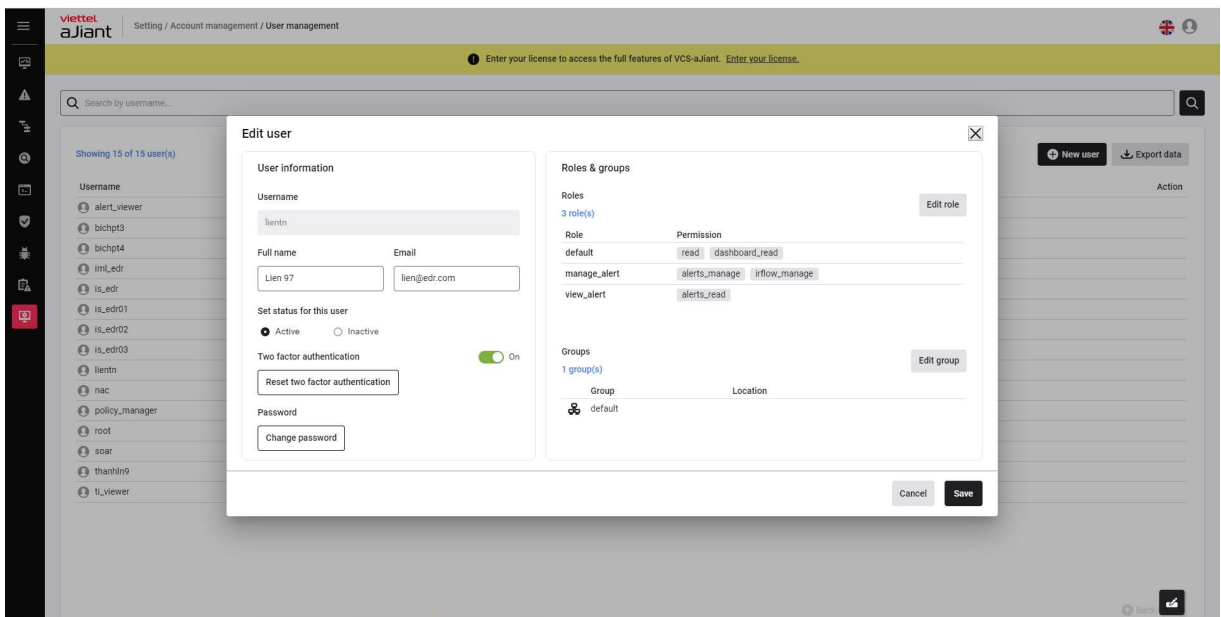
Bước 3: Dùng 2FA app để quét mã QR, sau đó nhập OTP để hoàn thành quá trình bật 2FA



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

3.7.5 Update management

3.7.5.1 Update groups

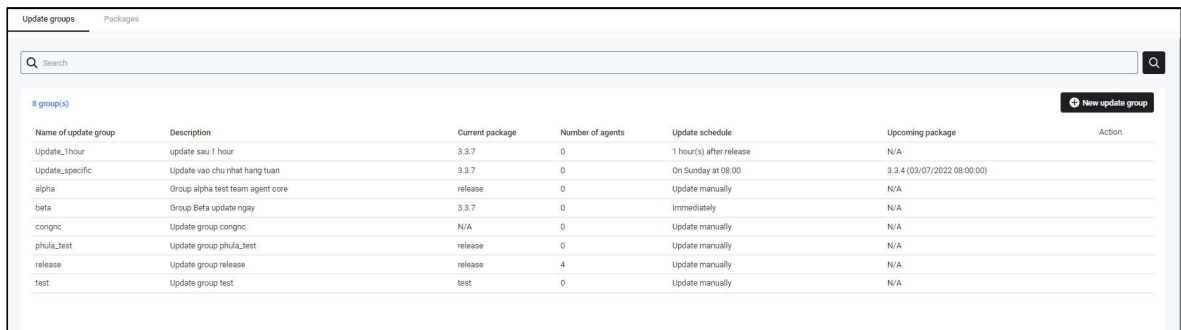
Mục đích: là tính năng cho phép quản lý, tạo mới và cập nhật các Update Group (Chia các Agent thành các nhóm cập nhật, giúp dễ dàng phân chia, quản lý)

– 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;

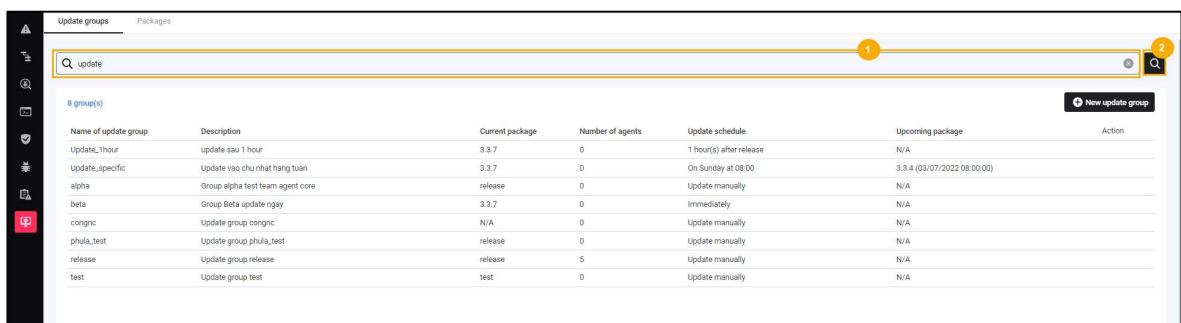
Bước 3: Chọn Update Management, hệ thống hiển thị Danh sách Update Group;



Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
Update_1hour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	
Update_specific	Update vào chủ nhật hàng tuần	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	
alpha	Group alpha test team agent core	release	0	Update manually	N/A	
beta	Group Beta update ngay	3.3.7	0	Immediately	N/A	
congnic	Update group congnic	N/A	0	Update manually	N/A	
phula_test	Update group phula_test	release	0	Update manually	N/A	
release	Update group release	release	4	Update manually	N/A	
test	Update group test	test	0	Update manually	N/A	

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”



Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
Update_1hour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	
Update_specific	Update vào chủ nhật hàng tuần	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	
alpha	Group alpha test team agent core	release	0	Update manually	N/A	
beta	Group Beta update ngay	3.3.7	0	Immediately	N/A	
congnic	Update group congnic	N/A	0	Update manually	N/A	
phula_test	Update group phula_test	release	0	Update manually	N/A	
release	Update group release	release	5	Update manually	N/A	
test	Update group test	test	0	Update manually	N/A	

- 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;

Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
Update_Thour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	
Update_specific	Update vào chủ nhật hàng tuần	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	
alpha	Group alpha test team agent core	release	0	Update manually	N/A	
beta	Group Beta update ngay	3.3.7	0	Immediately	N/A	
congnic	Update group congnic	N/A	0	Update manually	N/A	
phula_test	Update group phula_test	release	0	Update manually	N/A	
release	Update group release	release	4	Update manually	N/A	
test	Update group test	test	0	Update manually	N/A	

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

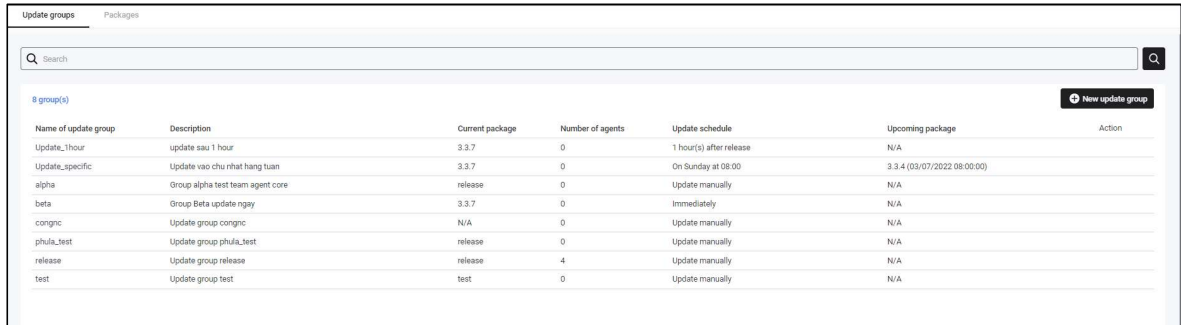
Bước 5: Nhập thông tin thêm mới Update Group và chọn nút “Create”. Hệ thống ghi nhận và quay về màn hình danh sách Update Group.

- Cập nhật Update groups:

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

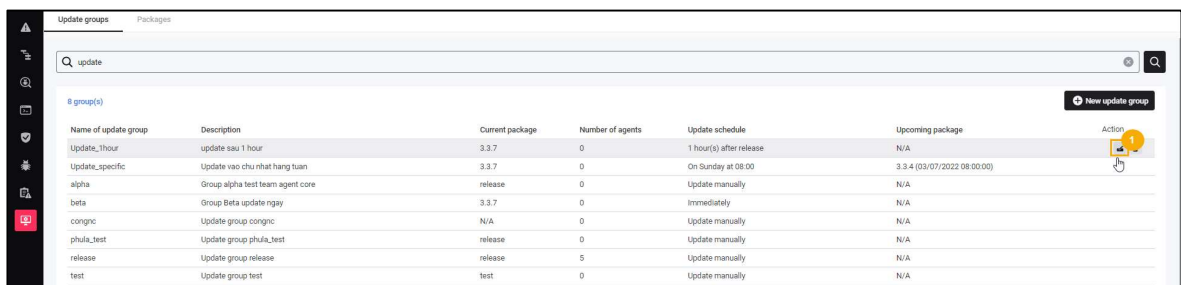
Bước 2: Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;

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



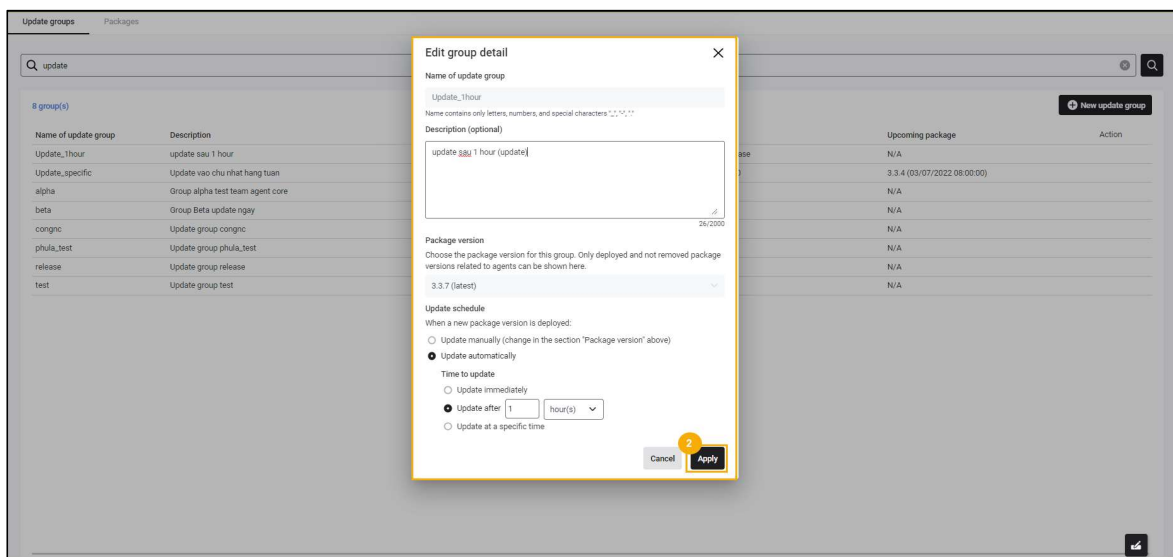
Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
Update_1hour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	
Update_specific	Update vào chủ nhật hàng tuần	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	
alpha	Group alpha test team agent core	release	0	Update manually	N/A	
beta	Group Beta update ngay	3.3.7	0	Immediately	N/A	
congnic	Update group congnic	N/A	0	Update manually	N/A	
phula_test	Update group phula_test	release	0	Update manually	N/A	
release	Update group release	release	4	Update manually	N/A	
test	Update group test	test	0	Update manually	N/A	

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



Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
Update_1hour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	
Update_specific	Update vào chủ nhật hàng tuần	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	
alpha	Group alpha test team agent core	release	0	Update manually	N/A	
beta	Group Beta update ngay	3.3.7	0	Immediately	N/A	
congnic	Update group congnic	N/A	0	Update manually	N/A	
phula_test	Update group phula_test	release	0	Update manually	N/A	
release	Update group release	release	5	Update manually	N/A	
test	Update group test	test	0	Update manually	N/A	

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”:



– Xóa Update groups:

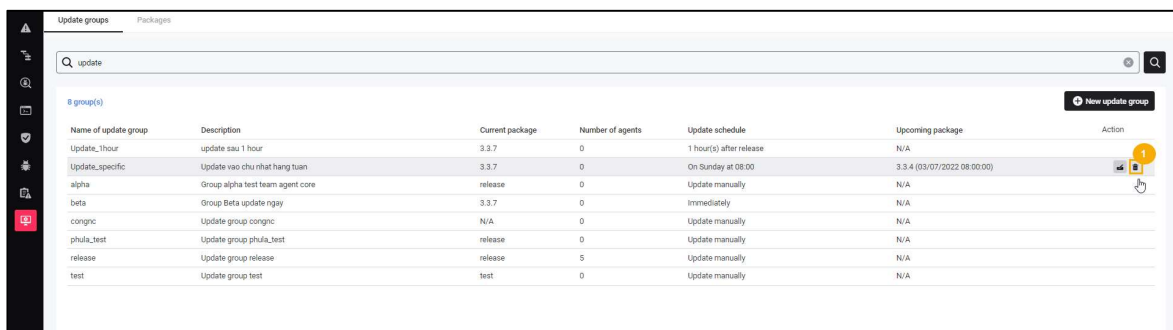
Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;

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;

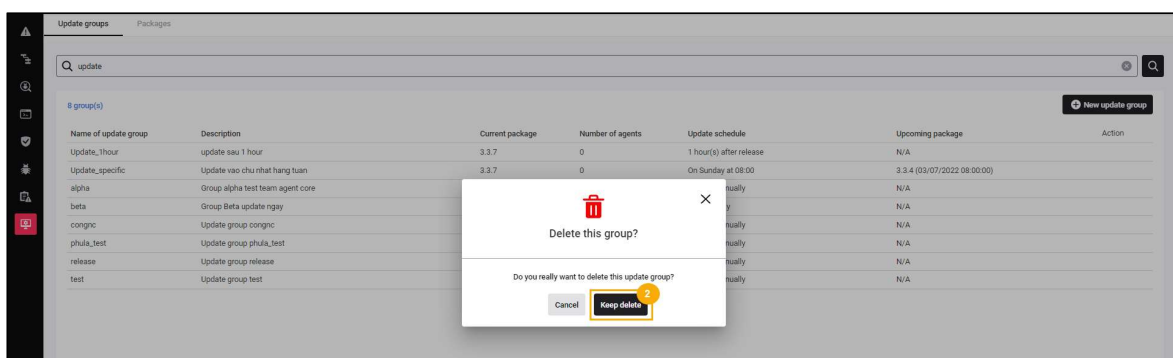
Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
Update_1hour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	
Update_specific	Update vào chủ nhật hàng tuần	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	
alpha	Group alpha test team agent core	release	0	Update manually	N/A	
beta	Group Beta update ngay	3.3.7	0	Immediately	N/A	
congnic	Update group congnic	N/A	0	Update manually	N/A	
phula_test	Update group phula_test	release	0	Update manually	N/A	
release	Update group release	release	4	Update manually	N/A	
test	Update group test	test	0	Update manually	N/A	

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



Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
Update_1hour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	
Update_specific	Update vào chủ nhật hàng tuần	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	
alpha	Group alpha test team agent core	release	0	Update manually	N/A	
beta	Group Beta update ngay	3.3.7	0	Immediately	N/A	
congruc	Update group congruc	N/A	0	Update manually	N/A	
phula_test	Update group phula_test	release	0	Update manually	N/A	
release	Update group release	release	5	Update manually	N/A	
test	Update group test	test	0	Update manually	N/A	

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.



3.7.5.2 Update packages

– 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 Package trong hệ thống;

Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Action
3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe...	Not deployed	root	N/A	
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp...	Not deployed	dat	N/A	
3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	Not deployed	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 Bổ sung hash md5 event 7	Not deployed	dat	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chỉ ...	Not deployed	dat	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re...	Not deployed	dat	N/A	
3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7, cập nhật file agents	Install succeeded	dat	10/05/2022 17:37:46	
3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	Install succeeded	dat	10/05/2022 17:36:29	
3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	Install failed	dat	10/05/2022 17:33:42	
release	N/A	N/A	Yes	Verified	Old repository release	Install succeeded	N/A	N/A	

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

Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Action
3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe...	Not deployed	root	N/A	
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp...	Not deployed	dat	N/A	
3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	Not deployed	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 Bổ sung hash md5 event 7	Not deployed	dat	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chỉ ...	Not deployed	dat	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re...	Not deployed	dat	N/A	
3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7, cập nhật file agents	Install succeeded	dat	10/05/2022 17:37:46	
3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	Install succeeded	dat	10/05/2022 17:36:29	
3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	Install failed	dat	10/05/2022 17:33:42	
release	N/A	N/A	Yes	Verified	Old repository release	Install succeeded	N/A	N/A	

– 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;

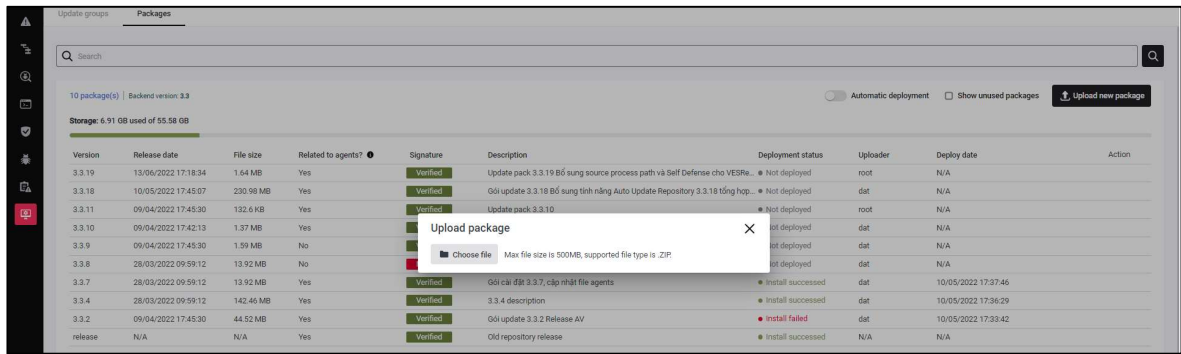
Bước 4: Chọn Tab “Package”, hệ thống hiển thị Danh sách Package trong hệ thống;

Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Action
3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe...	Not deployed	root	N/A	
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp...	Not deployed	dat	N/A	
3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	Not deployed	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 Bổ sung hash md5 event 7	Not deployed	dat	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Ứng dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chỉ...	Not deployed	dat	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re...	Not deployed	dat	N/A	
3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7: cập nhật file agents	Install succeeded	dat	10/05/2022 17:37:46	
3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	Install succeeded	dat	10/05/2022 17:36:29	
3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	Install failed	dat	10/05/2022 17:33:42	
release	N/A	N/A	Yes	Verified	Old repository release	Install succeeded	N/A	N/A	

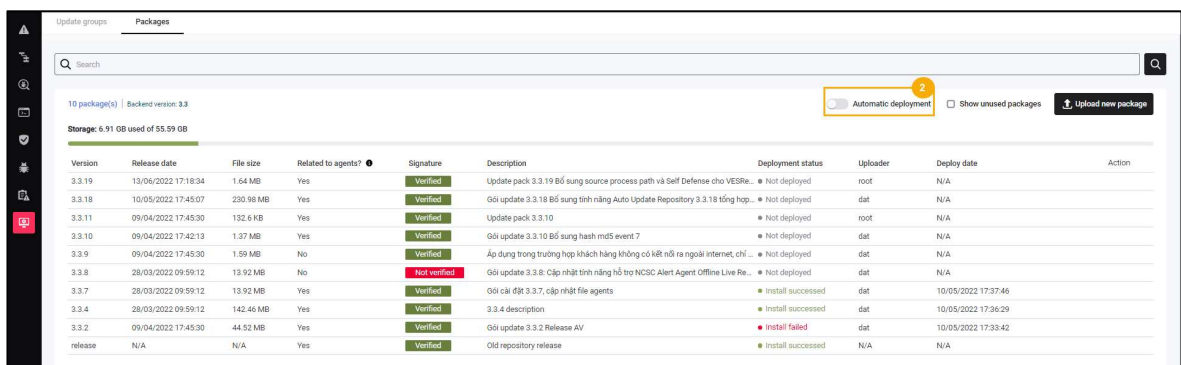
Bước 5: Chọn nút “Update new package”, hệ thống hiển thị Popup “Upload package”;

Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Action
3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe...	Not deployed	root	N/A	
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp...	Not deployed	dat	N/A	
3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	Not deployed	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 Bổ sung hash md5 event 7	Not deployed	dat	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Ứng dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chỉ...	Not deployed	dat	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re...	Not deployed	dat	N/A	
3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7: cập nhật file agents	Install succeeded	dat	10/05/2022 17:37:46	
3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	Install succeeded	dat	10/05/2022 17:36:29	
3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	Install failed	dat	10/05/2022 17:33:42	
release	N/A	N/A	Yes	Verified	Old repository release	Install succeeded	N/A	N/A	

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.



– 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 Package trong hệ thống;

Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Action
3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 bổ sung source process path và Self Defense cho VESRe...	Not deployed	root	N/A	Deploy this package
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp...	Not deployed	dat	N/A	
3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	Not deployed	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 bổ sung hash md5 event 7	Not deployed	dat	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chỉ...	Not deployed	dat	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re...	Not deployed	dat	N/A	
3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7: cập nhật file agents	Install succeeded	dat	10/05/2022 17:37:46	
3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	Install succeeded	dat	10/05/2022 17:36:29	
3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	Install failed	dat	10/05/2022 17:33:42	
release	N/A	N/A	Yes	Verified	Old repository release	Install succeeded	N/A	N/A	

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

Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Action
3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 bổ sung source process path và Self Defense cho VESRe...	Not deployed	root	N/A	Deploy this package
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp...	Not deployed	dat	N/A	
3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	Not deployed	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 bổ sung hash md5 event 7	Not deployed	dat	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chỉ...	Not deployed	dat	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re...	Not deployed	dat	N/A	
3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7: cập nhật file agents	Install succeeded	dat	10/05/2022 17:37:46	
3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	Install succeeded	dat	10/05/2022 17:36:29	
3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	Install failed	dat	10/05/2022 17:33:42	
release	N/A	N/A	Yes	Verified	Old repository release	Install succeeded	N/A	N/A	

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

Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Action
3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 bổ sung source process path và Self Defense cho VESRe...	Not deployed	root	N/A	Deploy
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp...	Not deployed	dat	N/A	
3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	Not deployed	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 bổ sung hash md5 event 7	Not deployed	dat	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chỉ...	Not deployed	dat	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re...	Not deployed	dat	N/A	
3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7: cập nhật file agents	Install succeeded	dat	10/05/2022 17:37:46	
3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	Install succeeded	dat	10/05/2022 17:36:29	
3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	Install failed	dat	10/05/2022 17:33:42	
release	N/A	N/A	Yes	Verified	Old repository release	Install succeeded	N/A	N/A	

– 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 Package trong hệ thống;

Version	Release date	File size	Related to agents?	Signature	Description	Deployment status	Uploader	Deploy date	Action
3.3.19	13/06/2022 17:18:34	1.64 MB	Yes	Verified	Update pack 3.3.19 Bổ sung source process path và Self Defense cho VESRe...	Not deployed	root	N/A	
3.3.18	10/05/2022 17:45:07	230.98 MB	Yes	Verified	Gói update 3.3.18 Bổ sung tính năng Auto Update Repository 3.3.18 tổng hợp...	Not deployed	dat	N/A	
3.3.11	09/04/2022 17:45:30	132.6 KB	Yes	Verified	Update pack 3.3.10	Not deployed	root	N/A	
3.3.10	09/04/2022 17:42:13	1.37 MB	Yes	Verified	Gói update 3.3.10 Bổ sung hash md5 event ?	Not deployed	dat	N/A	
3.3.9	09/04/2022 17:45:30	1.59 MB	No	Verified	Áp dụng trong trường hợp khách hàng không có kết nối ra ngoài internet, chỉ...	Not deployed	dat	N/A	
3.3.8	28/03/2022 09:59:12	13.92 MB	No	Not verified	Gói update 3.3.8: Cập nhật tính năng hỗ trợ NCSC Alert Agent Offline Live Re...	Not deployed	dat	N/A	
3.3.7	28/03/2022 09:59:12	13.92 MB	Yes	Verified	Gói cài đặt 3.3.7; cập nhật file agents	Install succeeded	dat	10/05/2022 17:37:46	
3.3.4	28/03/2022 09:59:12	142.46 MB	Yes	Verified	3.3.4 description	Install succeeded	dat	10/05/2022 17:36:29	
3.3.2	09/04/2022 17:45:30	44.52 MB	Yes	Verified	Gói update 3.3.2 Release AV	Install failed	dat	10/05/2022 17:33:42	
release	N/A	N/A	Yes	Verified	Old repository release	Install succeeded	N/A	N/A	

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

Package detail

Deployment

Status

Not deployed

Information

Backend version

N/A

Package version

3.3.8

File size

13.92 MB

SHA256

46bac489a084ed4115de3ef71f30e89ceed60fa15b4d23f93edb929bc39c3d83

Signature

Not verified

Release date

28/03/2022 09:59:12

Upload date

10/05/2022 17:33:05

Uploader

dat

Description

Gói update 3.3.8:

Cập nhật tính năng hỗ trợ NCSC

Alert Agent Offline

Live Response v2

Fix lỗi Dashboard, checkmarx

3.8 Màn hình BLS

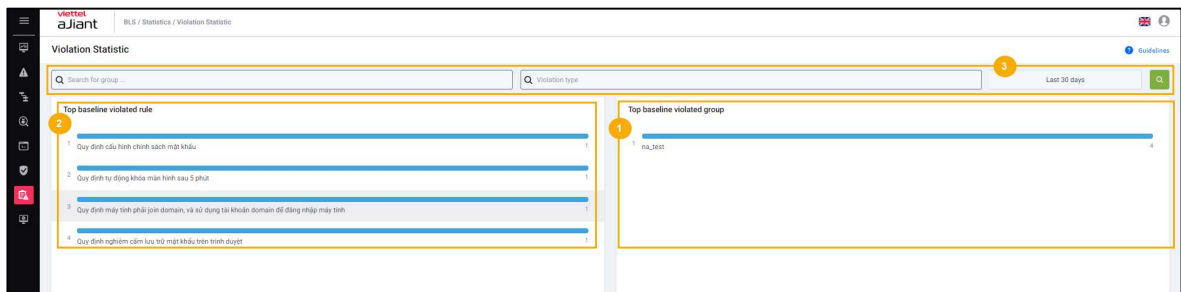
3.8.1 Thống kê vi phạm (Violation statistic)

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;

3.8.1.1 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 đơn 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

Rule	Mô tả chi tiết
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 trạm 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 cài đặt OS version hợp lệ (ánh xạ từ OS version của windows)
Quy định cài đặt và sử dụng phần mềm	Máy trạm vi phạm rule này khi cài đặt/ không cài đặt các phần mềm được config
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

Rule	Mô tả chi tiết
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

3.8.1.2 Tab Loại vi phạm

Violation Statistic

Search for group: [] Q Quy định cấu hình chính sách mật khẩu X Last 30 days []

Violation type Group

VIOLATION TYPE	RESOLVED	UNRESOLVED	VIOLATION AGENT	VIOLATION GROUP
Quy định cấu hình chính sách mật khẩu	0 (0%)	1 (100%)	1 (25%)	1

Violation rule

Search for group: [] Q Quy định cấu hình chính sách mật khẩu X Last 30 days []

Violation type Group

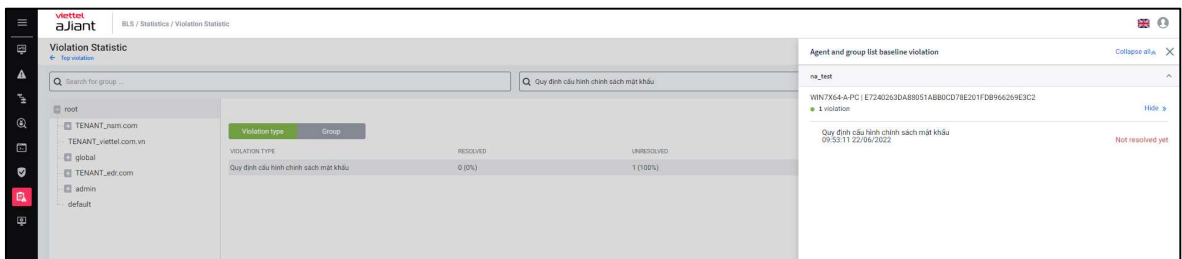
GROUP	ONLINE IN DAY	ONLINE IN 30 DAYS RECENTLY	RESOLVED	UNRESOLVED	VIOLATION AGENT	VIOLATION RULE
ha_test	0 (0%)	0	0 (0%)	1 (100%)	1 (0%)	1

Hệ thống hỗ trợ thực hiện các tính năng:

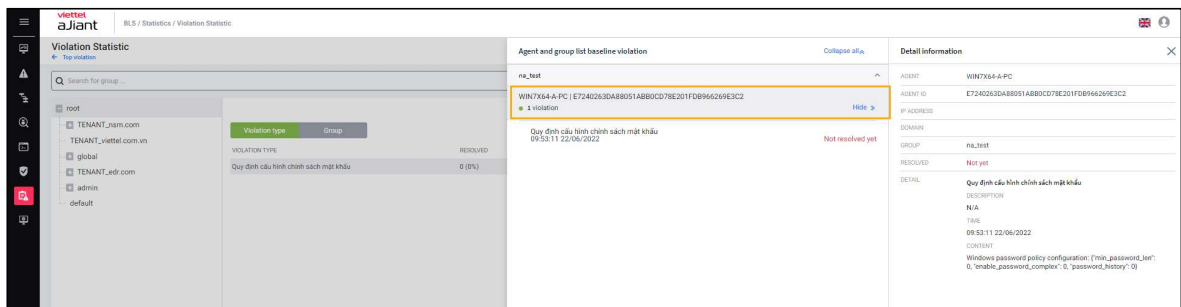
- + Chọn link Top vi phạm: Di chuyển về màn hình Dashboard, danh sách top vi phạm và top đơn vị vi phạm
- + Cây dữ liệu đơn vị của hệ thống
 - Hiện thị toàn bộ đơn vị của hệ thống được phân cấp cha-con;
 - Có thể chọn đơn vị trên cây dữ liệu đơn vị để thực hiện lọc vi phạm;

+ 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

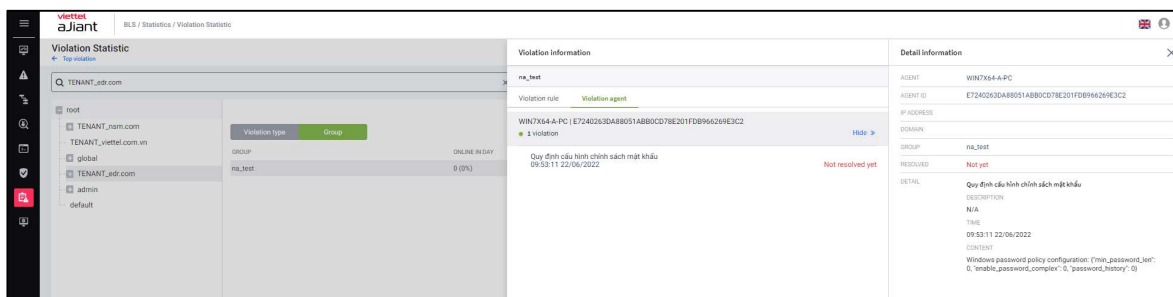
- + Tìm kiếm kết hợp: Khi nhập 2 hoặc nhiều điều kiện tìm kiếm thì sẽ thực hiện tìm kiếm theo điều kiện AND

3.8.1.3 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;
 - Hiện 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: Hiện 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;

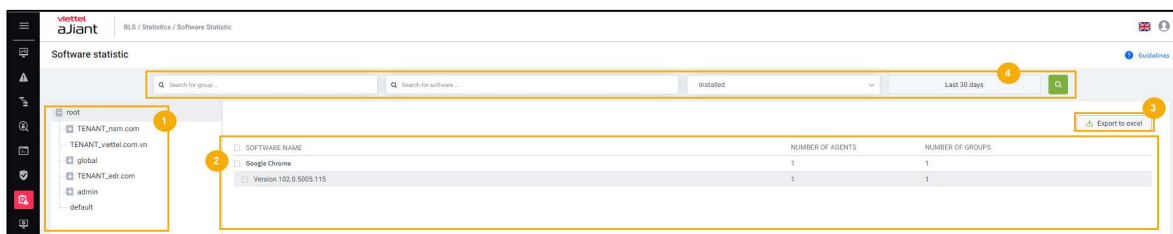
+ Tìm kiếm kết hợp: Khi nhập 2 hoặc nhiều điều kiện tìm kiếm thì sẽ thực hiện tìm kiếm theo điều kiện AND;

3.8.2 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:

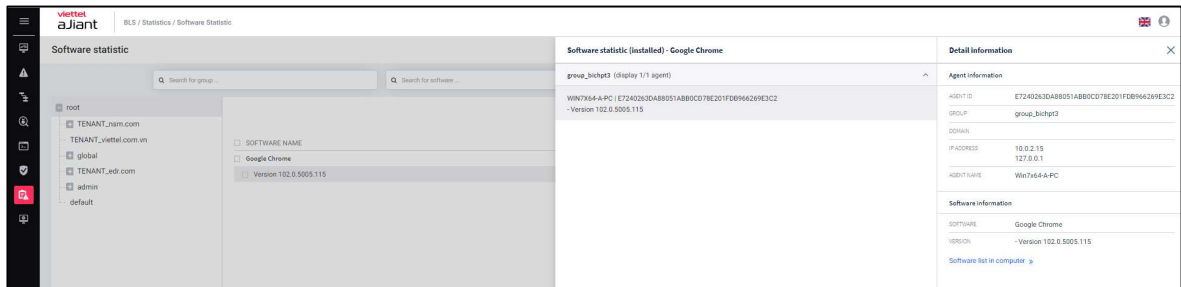
- + Cây dữ liệu đơn vị của hệ thống
- + Hiển thị toàn bộ đơn vị của hệ thống được phân cấp cha-con
- + Có thể chọn đơn vị trên cây dữ liệu đơn vị để thực hiện lọc phần mềm
- + Danh sách phần mềm
 - Mỗi phần mềm được hiển thị các thông tin chung gồm: Software name, number of computer, number of unit;



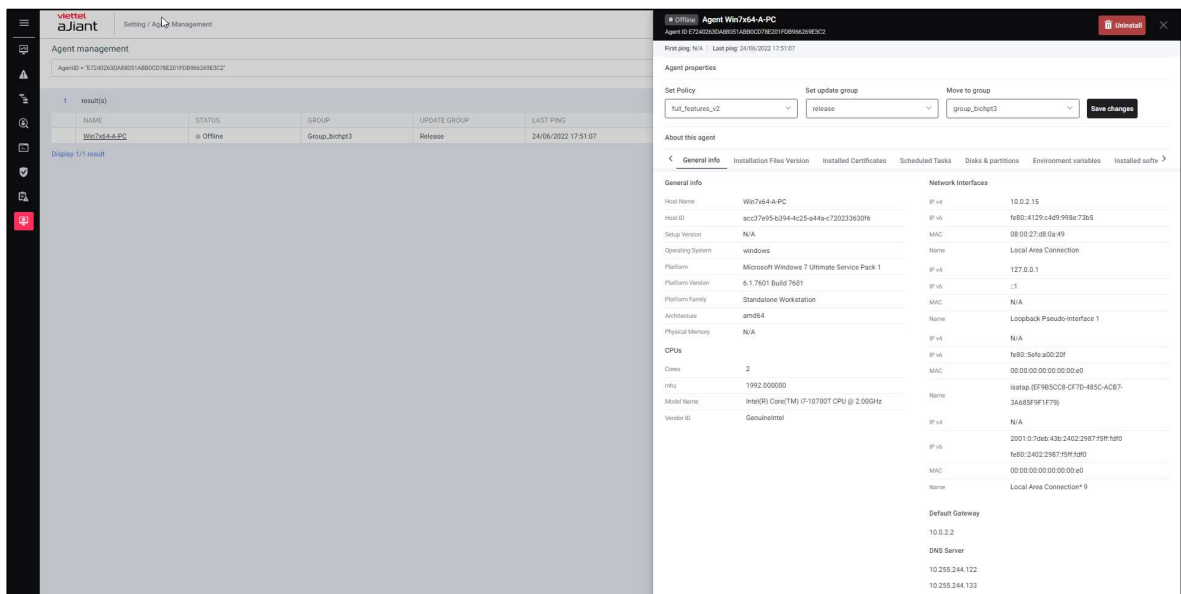
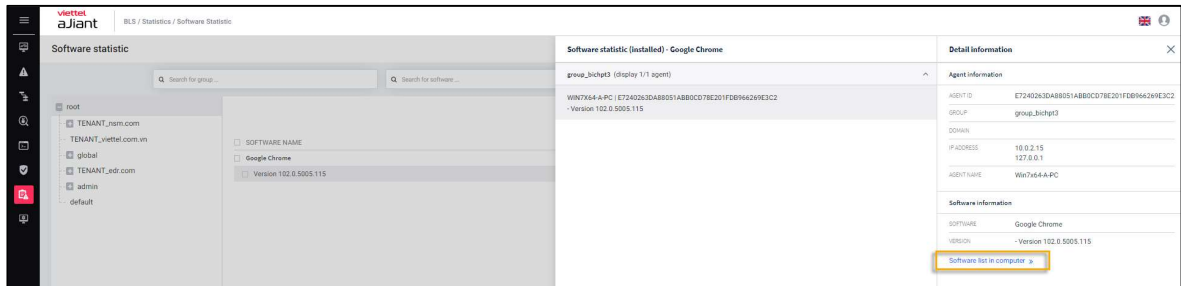
- Chọn icon detail của cột violation computer trên danh sách: Hiển thị danh sách máy tính trong từng đơn vị bao gồm Tên đơn vị, Tên máy tính|Agent ID, Version;



- 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

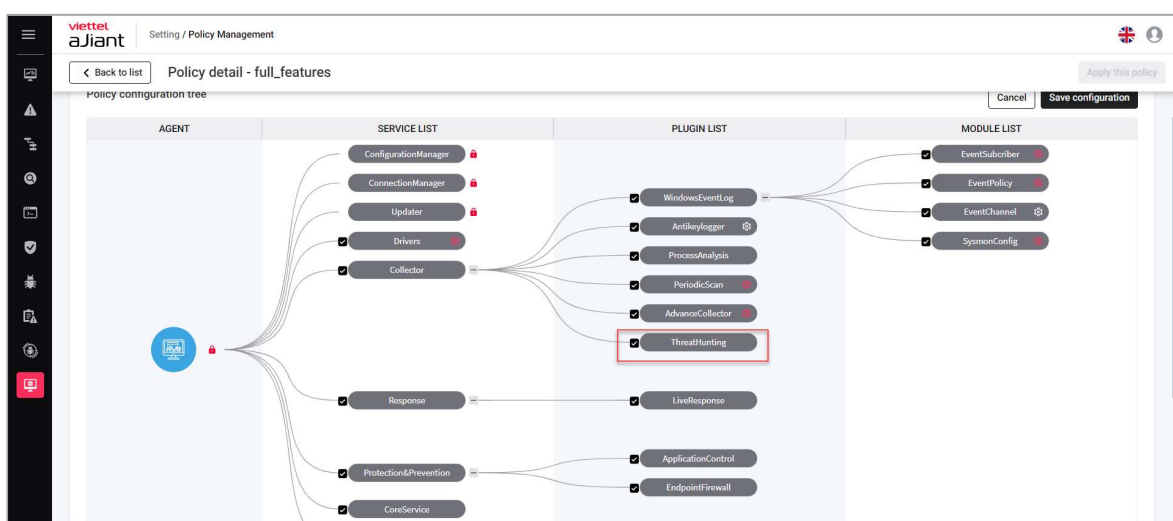
Export: Chọn Export: Hệ thống sẽ download file Export có dữ liệu giống với dữ liệu đang hiển thị trên màn hình

3.9 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.

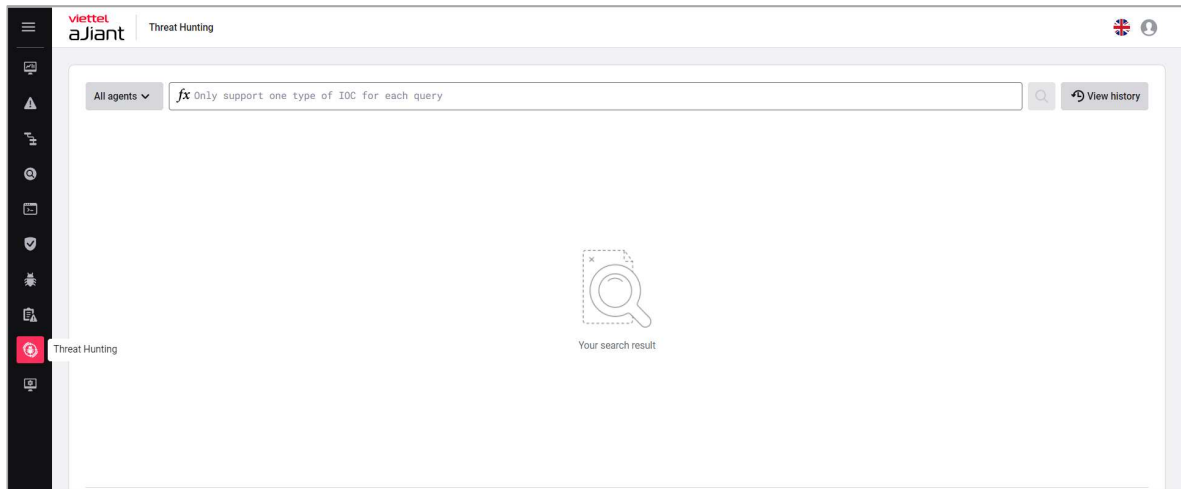
3.9.1 Bật/tắt policy

- 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

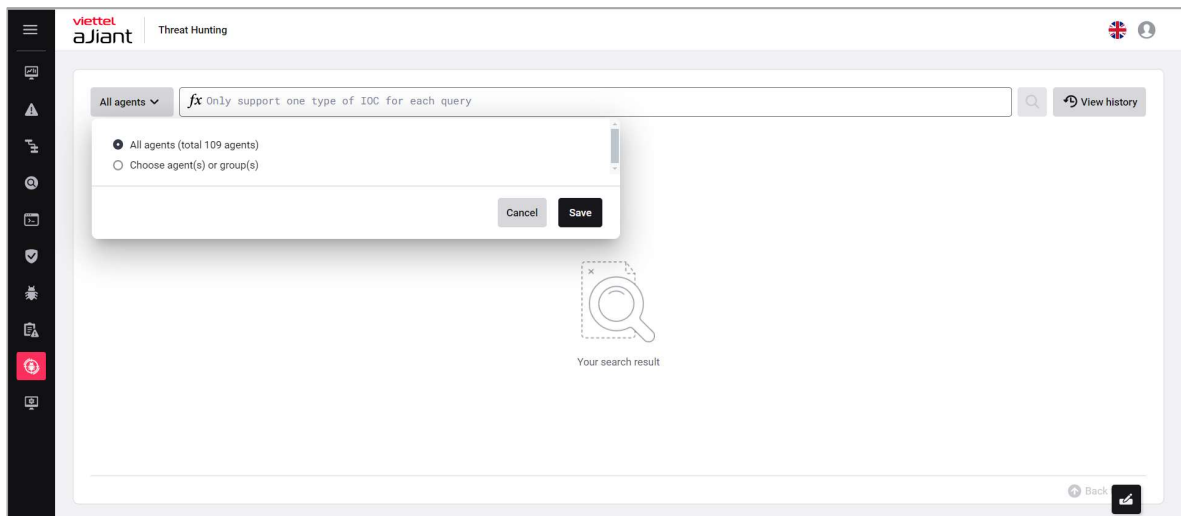


3.9.2 Tìm kiếm theo agents/ nhóm

- Trên Menu chọn Threat Hunting



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



3.9.3 Tìm kiếm IOCs

3.9.3.1 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

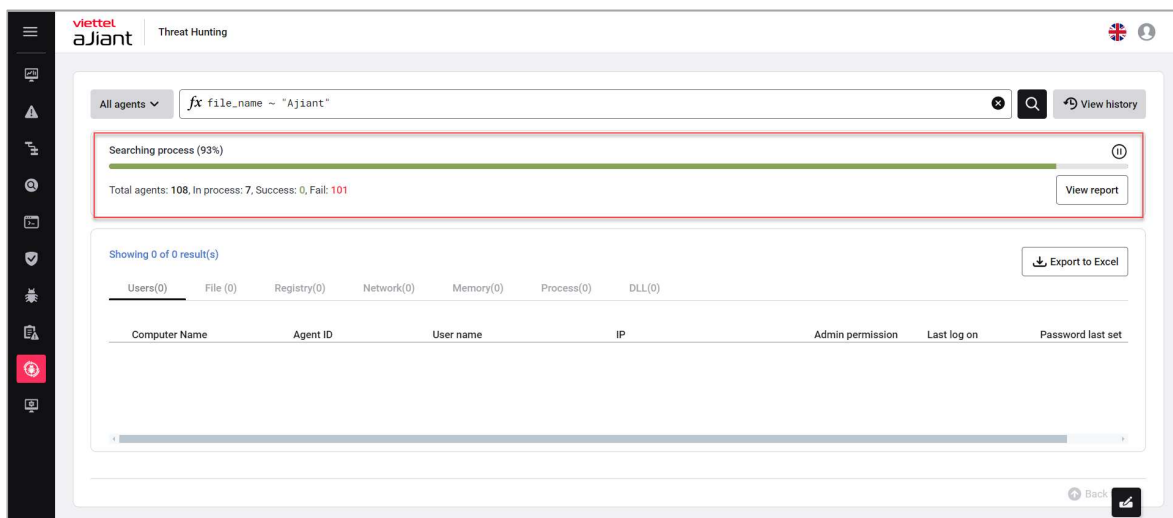
Lưu ý:

- 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.

3.9.4 Chi tiết kết quả tìm kiếm

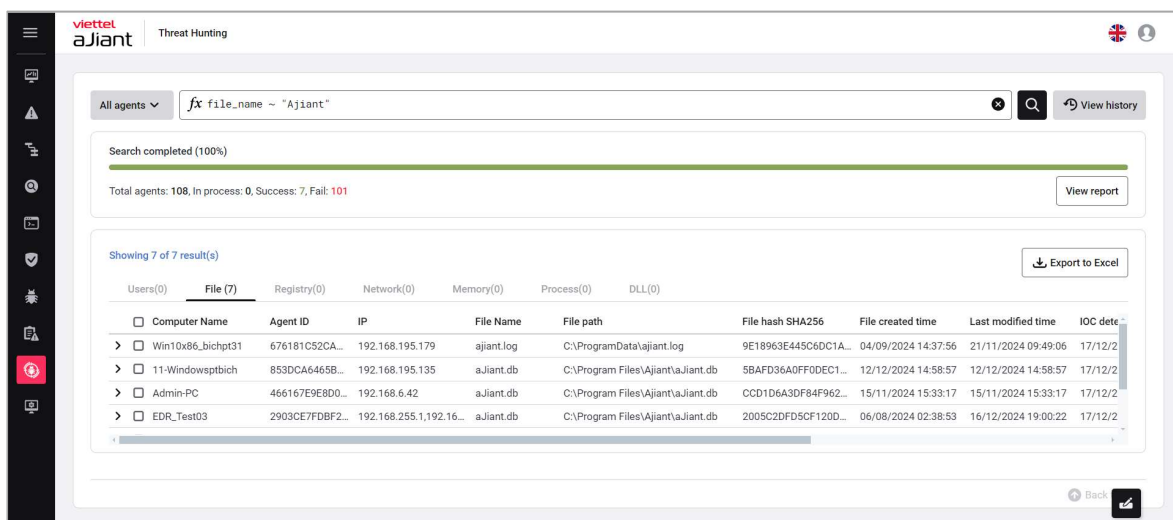
3.9.4.1 Theo dõi trạng thái tìm kiếm

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



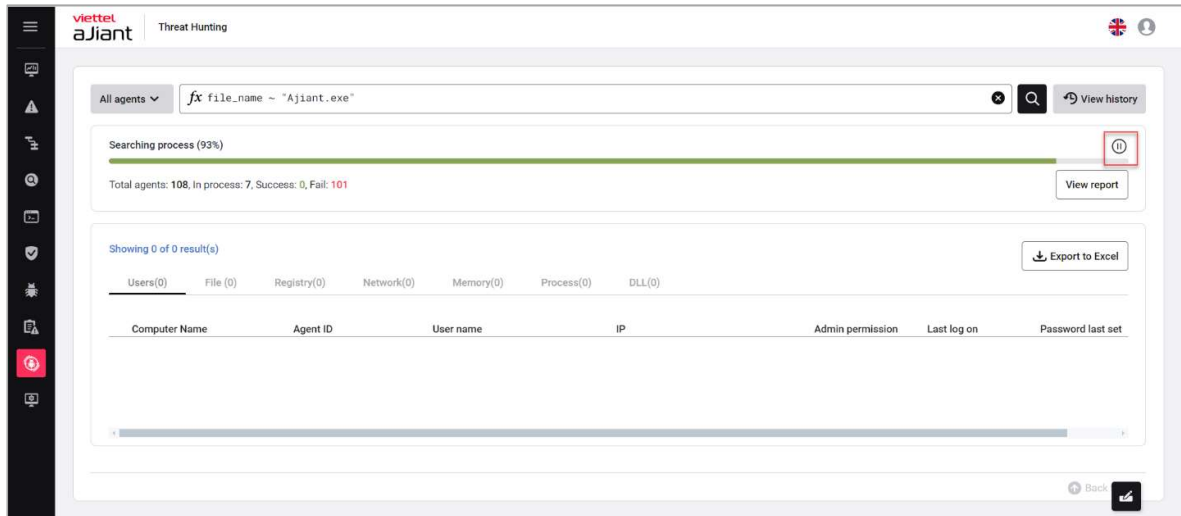
3.9.4.2 Chi tiết kết quả tìm kiếm

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



3.9.4.3 Dừng tìm kiếm

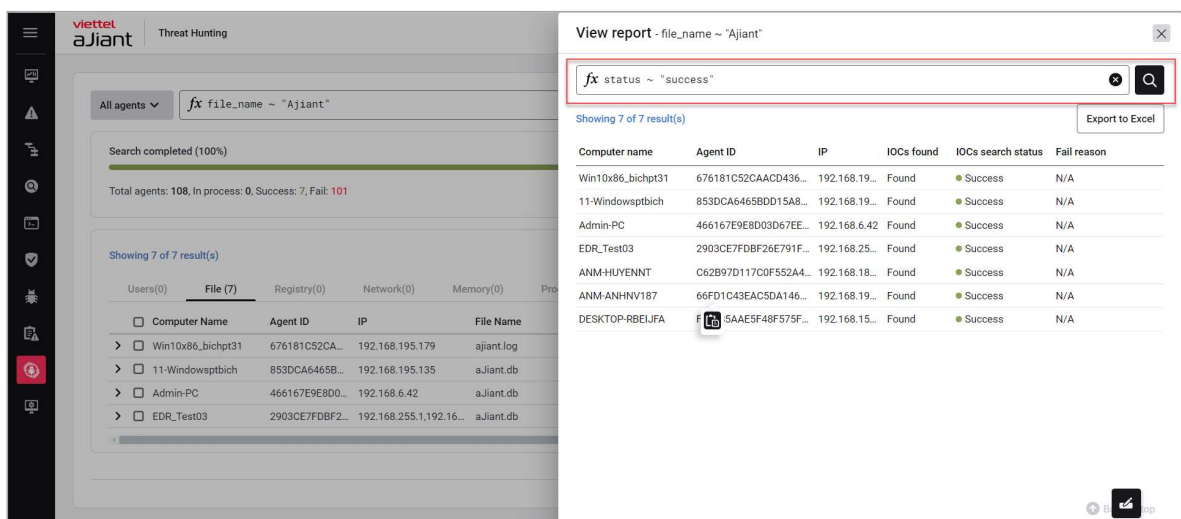
- Cho phép người dùng dừng việc tìm kiếm: Trên Searching Process bar -> chọn button Pause
- Sau khi Dừng tìm kiếm:
 - o Hệ thống sẽ dừng việc tìm kiếm
 - o Không hỗ trợ thực hiện tiếp tục tìm kiếm câu truy vấn



3.9.4.4 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

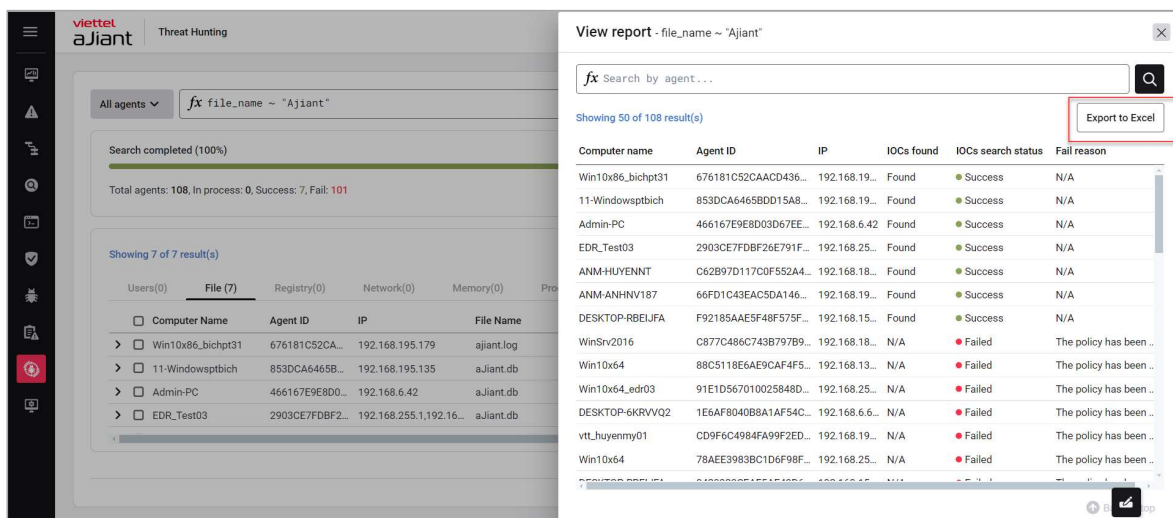


- Báo cáo này sẽ cung cấp cho người dùng chi tiết về trạng thái tìm kiếm iocs trên từng agent. Các thông tin trên báo cáo gồm có:
 - Computer name
 - Agent ID
 - IP
 - IOCs found: Có tìm thấy dấu hiệu IOCs dựa trên câu truy vấn của người dùng hay không
 - IOCs search status: Trạng thái tìm kiếm iocs trên agent
 - Fail reason: Chi tiết lí do tìm kiếm thất bại

The screenshot displays the Viettel Ajiant Threat Hunting dashboard. On the left, a sidebar shows navigation icons. The main panel is titled 'View report - file_name ~ "Ajiant"'. It features a search bar with the query 'fx file_name ~ "Ajiant"', a search button, and an 'Export to Excel' button. Below the search bar, it indicates 'Showing 50 of 108 result(s)'. A table lists search results with columns: Computer name, Agent ID, IP, IOCs found, IOCs search status, and Fail reason. The table shows various agents like Win10x86_bichpt31, 11-Windowsptbich, Admin-PC, EDR_Test03, ANM-HUYENNT, ANM-AMHNV187, DESKTOP-RBEUJFA, WinSrv2016, Win10x64, Win10x64_edr03, DESKTOP-6KRVVQ2, vtt_huyenmy01, and Win10x64. The 'IOCs found' column shows 'Found' or 'N/A', and the 'IOCs search status' column shows 'Success' or 'Failed'. The 'Fail reason' column provides details for failed searches, such as 'The policy has been ..'.

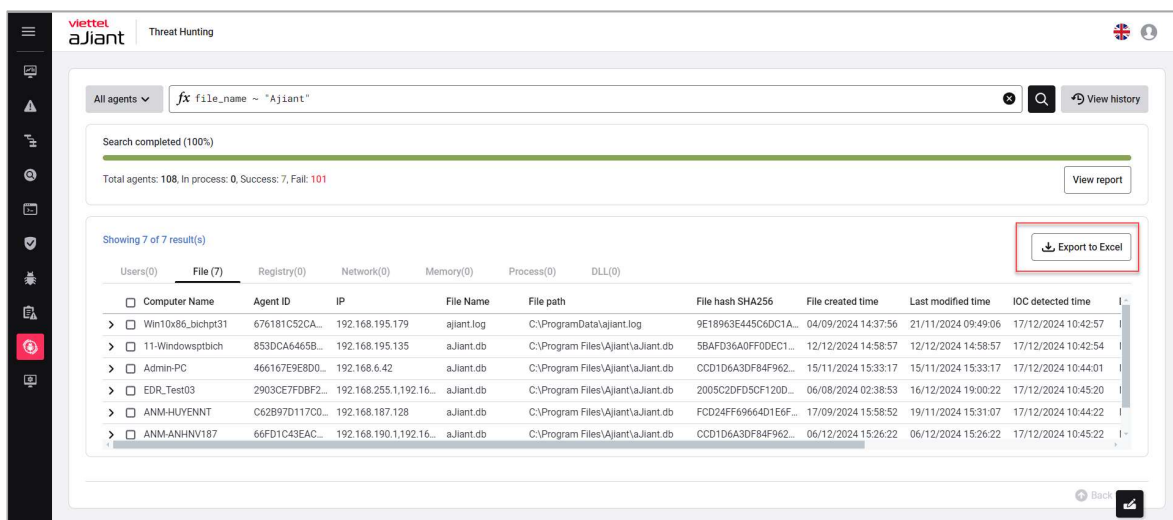
3.9.4.5 Export to Excel

- 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



3.9.4.6 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



3.9.5 Xem lịch sử truy vấn (View History)

3.9.5.1 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

- Success: Tìm kiếm thành công trên máy endpoint
- In-process: Đang trong quá trình tìm kiếm trên máy endpoint
- Fail: Tìm kiếm thất bại

View history

Showing 50 of 287 result(s)

Query start time	Query end time	Query	Total agents	Success	In-process	Fail	Action
13/12/2024 10:54:25	13/12/2024 10:54:34	process_commandline ~ "...	1	1	0	0	
13/12/2024 10:53:56	13/12/2024 10:54:02	process_path ~ "C:\Progr...	1	1	0	0	
13/12/2024 10:53:39	13/12/2024 10:53:46	process_path ~ "C:\Progr...	1	1	0	0	
13/12/2024 10:53:26	13/12/2024 10:53:30	process_path ~ "C:\Progr...	1	1	0	0	
13/12/2024 10:51:55	13/12/2024 10:52:02	process_path ~ "C:\Progr...	1	1	0	0	
13/12/2024 10:51:19	13/12/2024 10:51:26	process_path ~ "chrome"	1	1	0	0	
12/12/2024 17:25:35	12/12/2024 17:25:53	file_path ~ "threat hunting"	4	3	0	1	
12/12/2024 17:13:34	12/12/2024 17:18:38	file_path ~ "abc"	20001	602	0	19399	
12/12/2024 16:53:48	N/A	file_path ~ "abc"	20001	0	20001	0	
12/12/2024 16:38:49	12/12/2024 16:53:32	file_path ~ "abc"	20001	138	0	19863	
12/12/2024 15:37:42	12/12/2024 15:57:58	file_path ~ "abc"	1	0	0	1	
12/12/2024 15:28:30	12/12/2024 15:43:31	user_name ~ "ad"	1	0	0	1	
12/12/2024 15:26:09	12/12/2024 15:41:31	user_name ~ "adm"	107	1	0	106	
12/12/2024 15:21:30	12/12/2024 15:36:31	user_name ~ "admin"	107	1	0	106	

3.9.5.2 Xem chi tiết lịch sử truy vấn

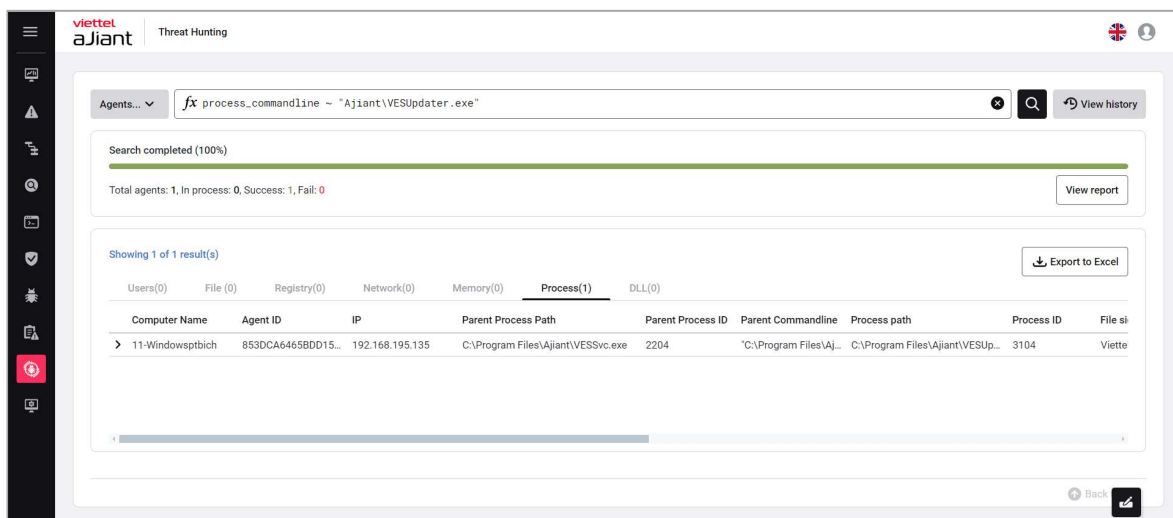
- Cho phép người dùng xem chi tiết lại kết quả của từng lần truy vấn: Action - > chọn View

View history

Showing 50 of 287 result(s)

Query start time	Query end time	Query	Total agents	Success	In-process	Fail	Action
13/12/2024 10:54:25	13/12/2024 10:54:34	process_commandline ~ "...	1	1	0	0	View
13/12/2024 10:53:56	13/12/2024 10:54:02	process_path ~ "C:\Progr...	1	1	0	0	
13/12/2024 10:53:39	13/12/2024 10:53:46	process_path ~ "C:\Progr...	1	1	0	0	
13/12/2024 10:53:26	13/12/2024 10:53:30	process_path ~ "C:\Progr...	1	1	0	0	
13/12/2024 10:51:55	13/12/2024 10:52:02	process_path ~ "C:\Progr...	1	1	0	0	
13/12/2024 10:51:19	13/12/2024 10:51:26	process_path ~ "chrome"	1	1	0	0	
12/12/2024 17:25:35	12/12/2024 17:25:53	file_path ~ "threat hunting"	4	3	0	1	
12/12/2024 17:13:34	12/12/2024 17:18:38	file_path ~ "abc"	20001	602	0	19399	
12/12/2024 16:53:48	N/A	file_path ~ "abc"	20001	0	20001	0	
12/12/2024 16:38:49	12/12/2024 16:53:32	file_path ~ "abc"	20001	138	0	19863	
12/12/2024 15:37:42	12/12/2024 15:57:58	file_path ~ "abc"	1	0	0	1	
12/12/2024 15:28:30	12/12/2024 15:43:31	user_name ~ "ad"	1	0	0	1	
12/12/2024 15:26:09	12/12/2024 15:41:31	user_name ~ "adm"	107	1	0	106	
12/12/2024 15:21:30	12/12/2024 15:36:31	user_name ~ "admin"	107	1	0	106	

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



3.10 Rules Correlation

3.10.1 Danh sách hiển thị

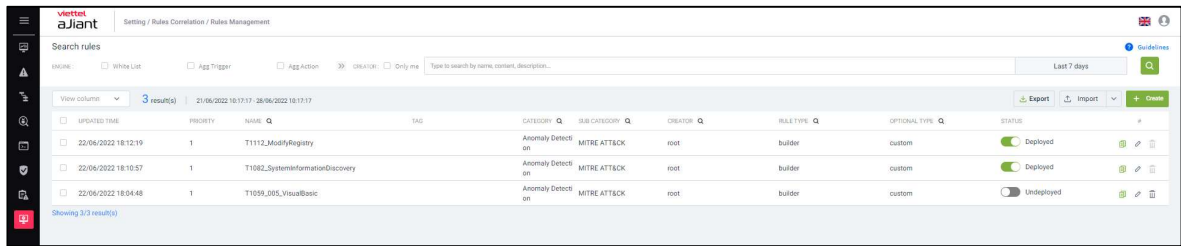
Mục đích: Chức năng cho phép người dùng xem danh sách rules correlation trong hệ thống. Nhập hoặc chọn điều kiện tìm kiếm để thực hiện tìm kiếm rule đang có trên hệ thống, thao tác deploy/undeploy/xóa nhanh với các rule.

+ Bộ lọc FITTER;

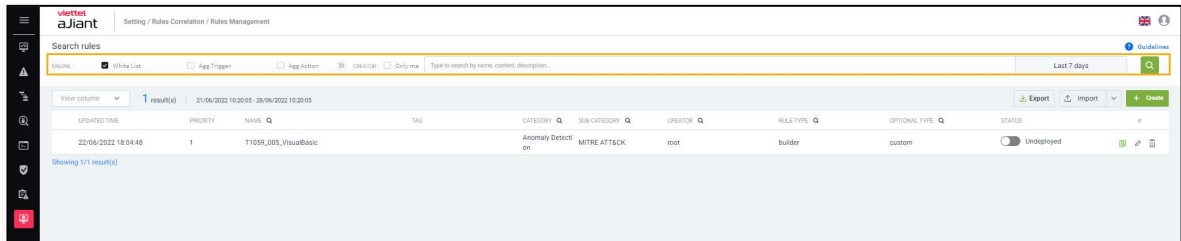
+ Bộ lọc FITTER bao gồm:

- 6 Engine: Whitelist, Agg Trigger, Agg Action, Filter, Indicator, False-Positive;

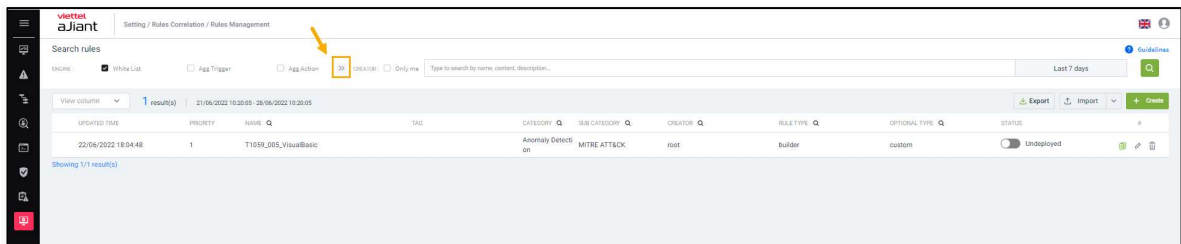
- Text box search theo các trường: Name, content, description;
- Thời gian cập nhật;
- Tạo bởi tôi;
- Lọc theo **Engine**;



Bước 1: Chọn 1 hoặc nhiều Engine mặc định;

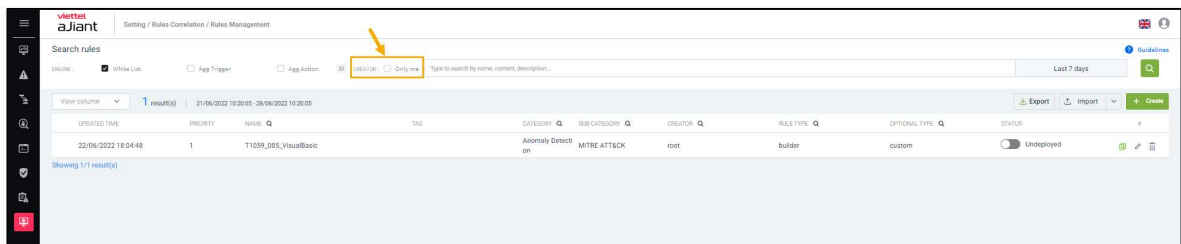


Bước 2: Chọn Mở rộng để thêm các Engine cần lọc;

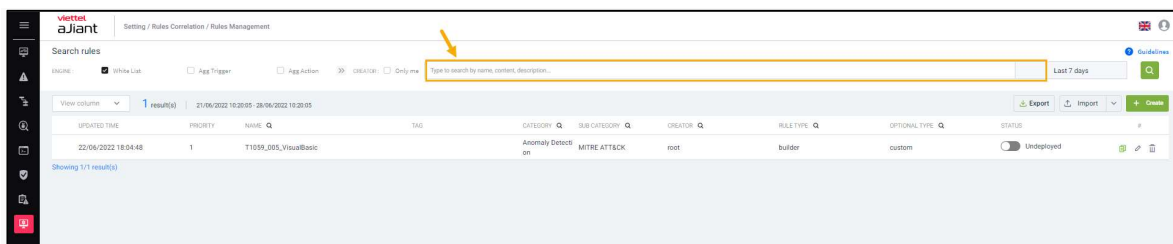


Khi chọn 2 hoặc nhiều Engine, màn hình trả về kết quả được lọc theo phép toán AND;

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

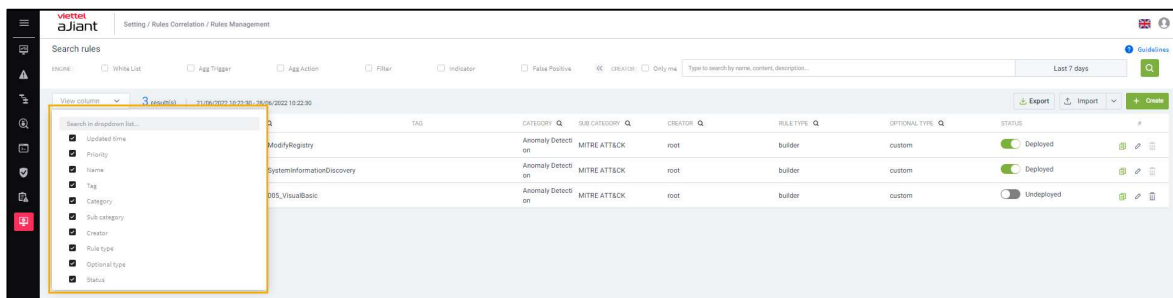
Cho phép người dùng lựa chọn các cột hiển thị trên màn hình correlation.

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;



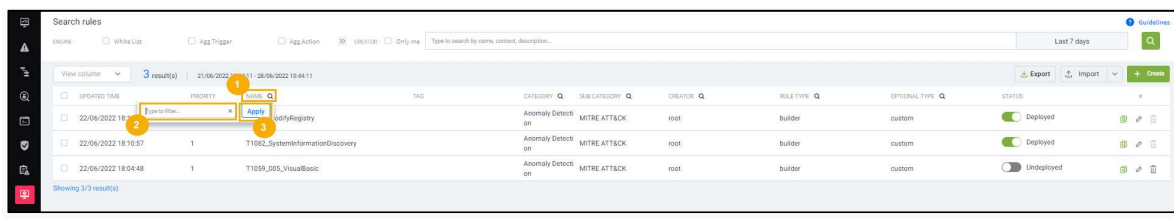
Bước 2: Chọn vào những tên cột muốn hiển thị;



– Hỗ trợ tìm kiếm nhanh

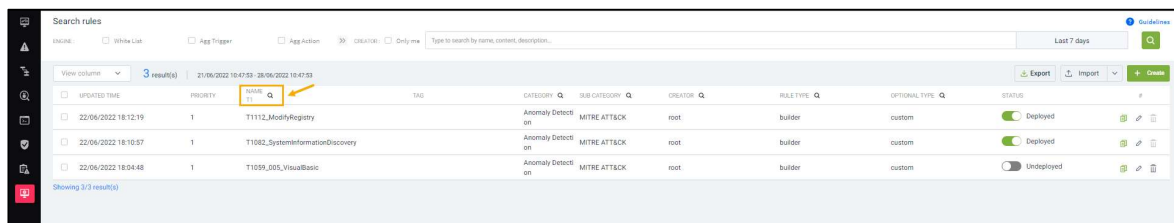
- Tìm kiếm theo tên rule

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



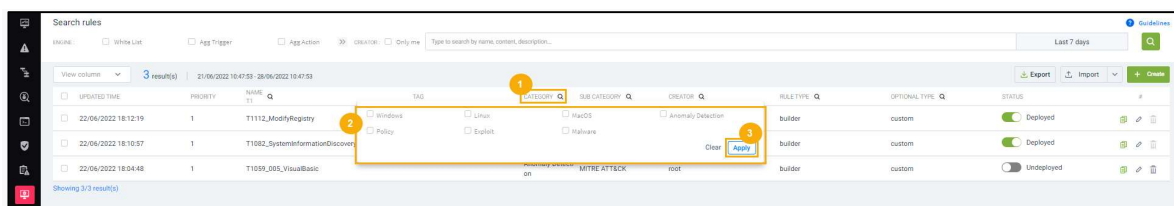
Bước 2: Nhập tên rules muốn tìm kiếm;

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 tìm 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 tìm kiếm;

Bước 3: Click “Apply”;

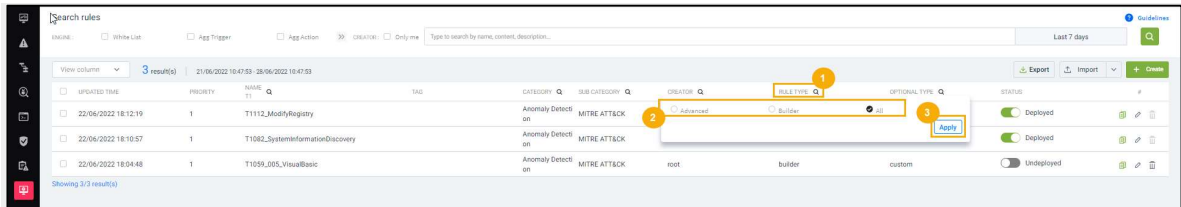
Tìm kiếm Creator

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

Bước 2: Nhập tên người tạo muốn tìm kiếm;

Bước 3: Click “Apply”;

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

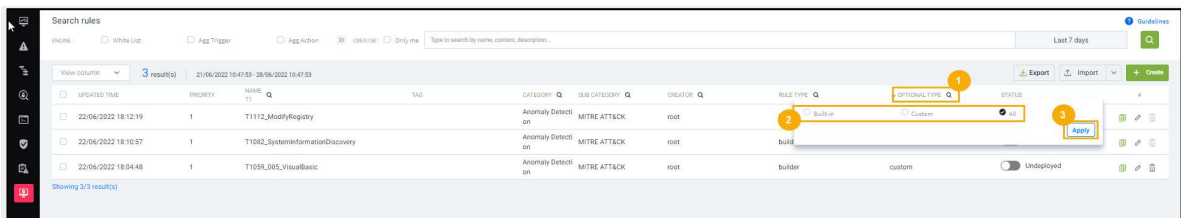


Bước 1: Click icon 🔍 để hiển thị danh sách Rule type;

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.

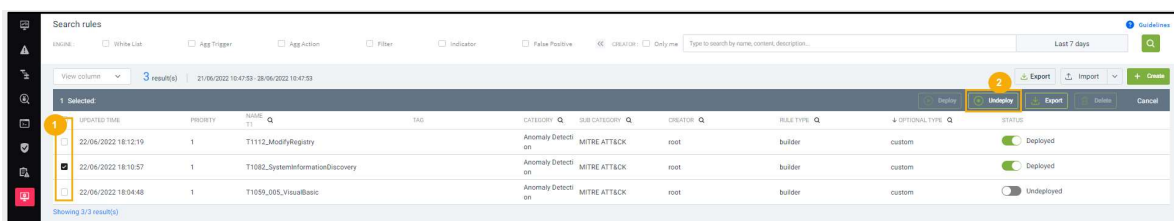


Bước 1: Click icon 🔍 để hiển thị danh sách Optional type;

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

Bước 3: Click “Apply”;

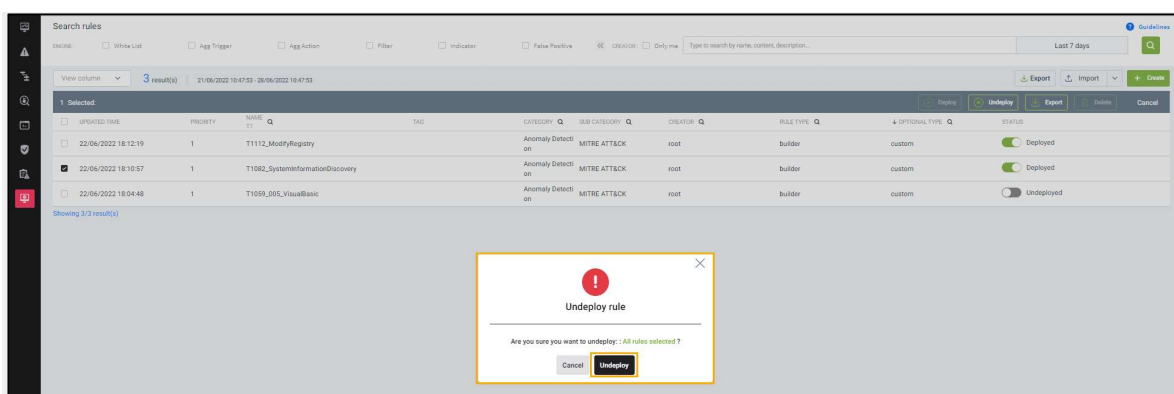
Hỗ trợ Deploy/Undeploy cho nhiều Rules



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;



3.10.2 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 thỏa 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 thỏa mãn số lượng từ đó sinh ra Alert;

- Function: Là các hàm. Lưu ý: Với các 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

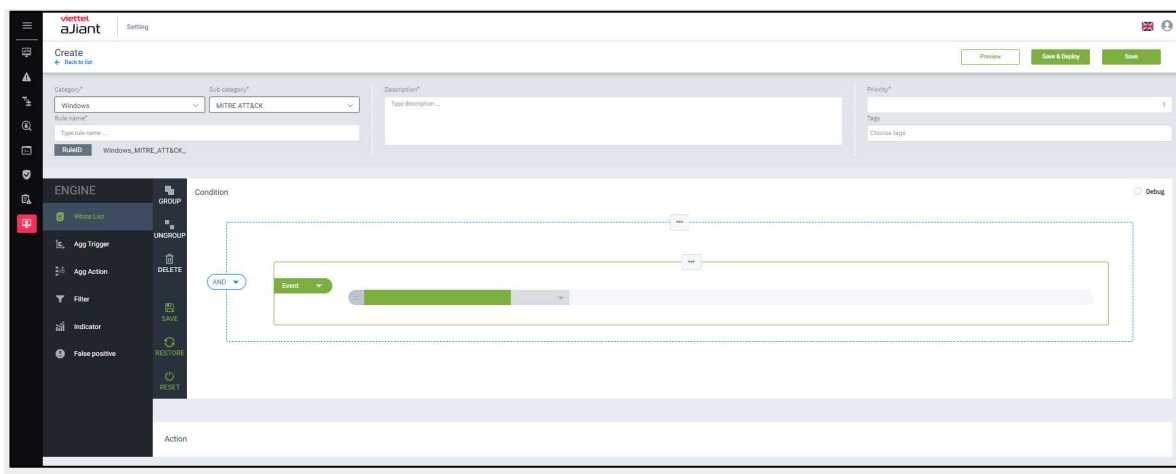
+ **Restore:** Tự động reset lại đến ngay sau khi nhấn “Save” gần nhất;

+ **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;

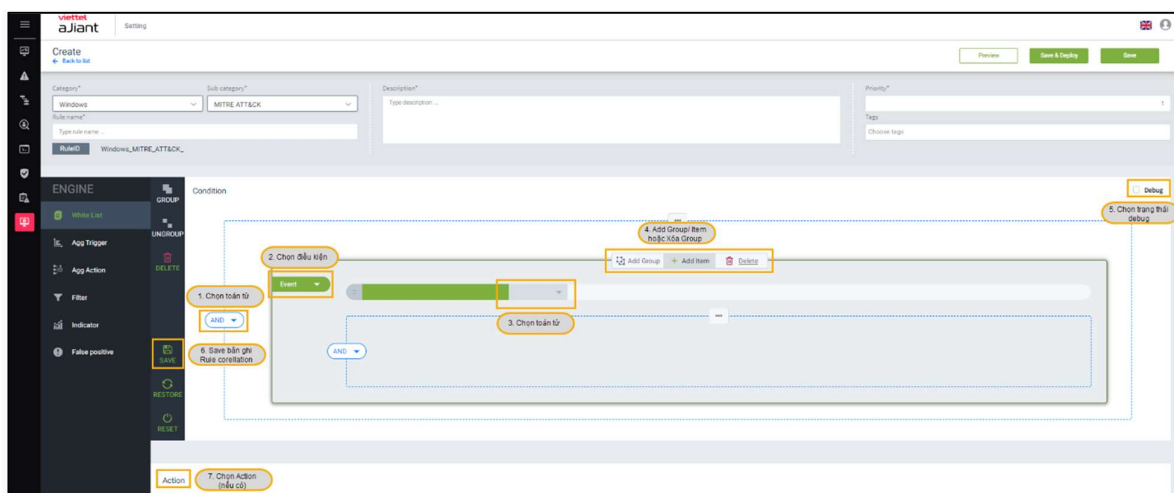


Bước 2: Nhập thông tin của rule;



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.

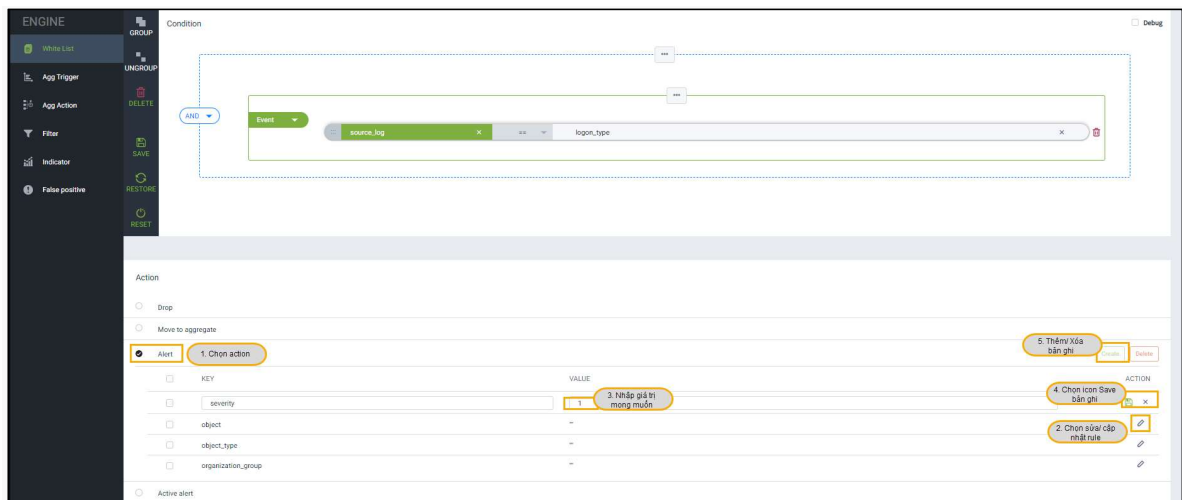
Các bước thực hiện thêm hành động tương ứng với từng engine: Khi người dùng thực hiện xong các bước tạo điều kiện và nhấn lưu, màn hình sẽ hiển thị các hành động cho từng engine. Mỗi engine sẽ bao gồm các hành động tương ứng. Engine Agg_trigger sẽ không có hành động.

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 đầy vào thỏa 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 thỏa mãn điều kiện sẽ được loại bỏ khỏi luồng xử lý;
- Chuyển sang aggregate: Log đẩy vào thỏa 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 thỏa 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 thêm;
- 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 xóa hành động vừa tạo, click icon “Delete”;
- + Để chỉnh sửa hành động, Click icon “edit”;

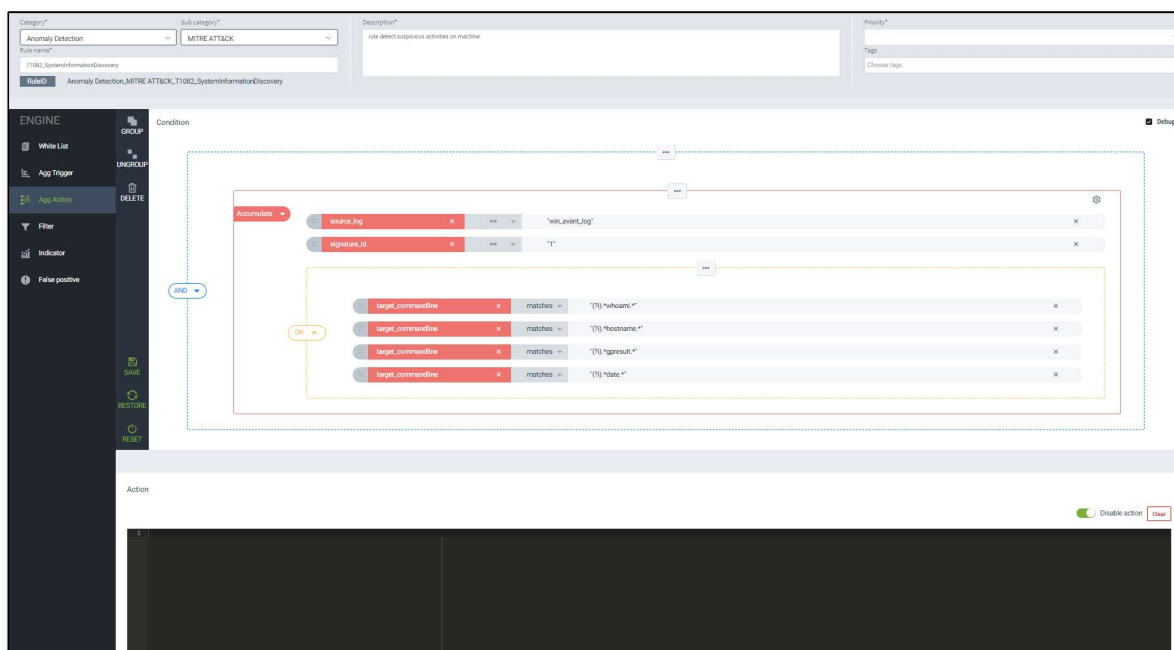
Lưu ý: Có thể tạo nhiều hành động với các trường khác nhau tùy theo mục đích người sử dụng.

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, xóa 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, xóa 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 xóa 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 engine thì nhấn “Save & Deploy”.

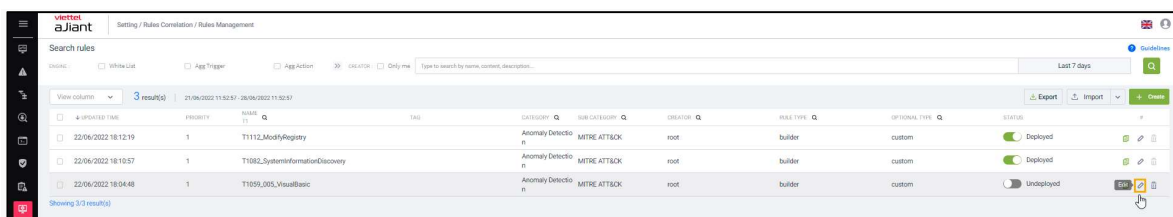
Lưu ý: Khi có lỗi, người dùng có thể nhấn nút “Preview” để xem lỗi.

3.10.2.1 Sửa Rules Correlation

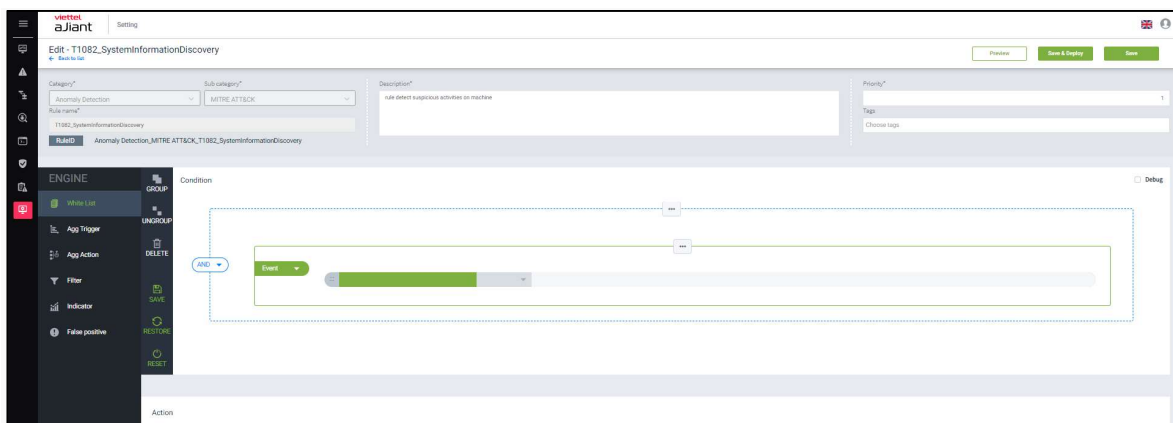
Cho phép người dùng chỉnh sửa các rule đã tạo.

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;



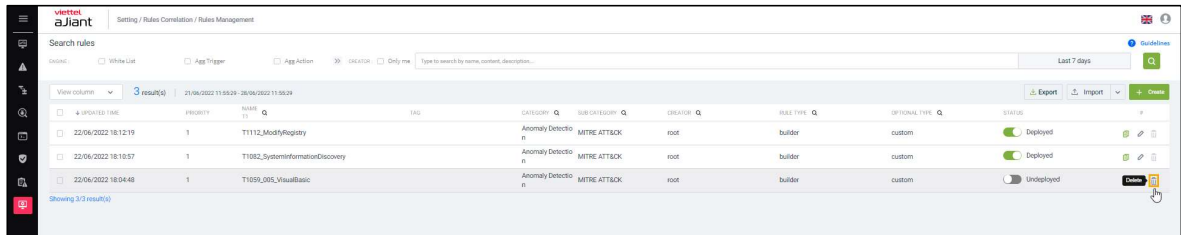
Lưu ý: Các trường tên rule, category, subcategory là những trường không chỉnh sửa được.

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.

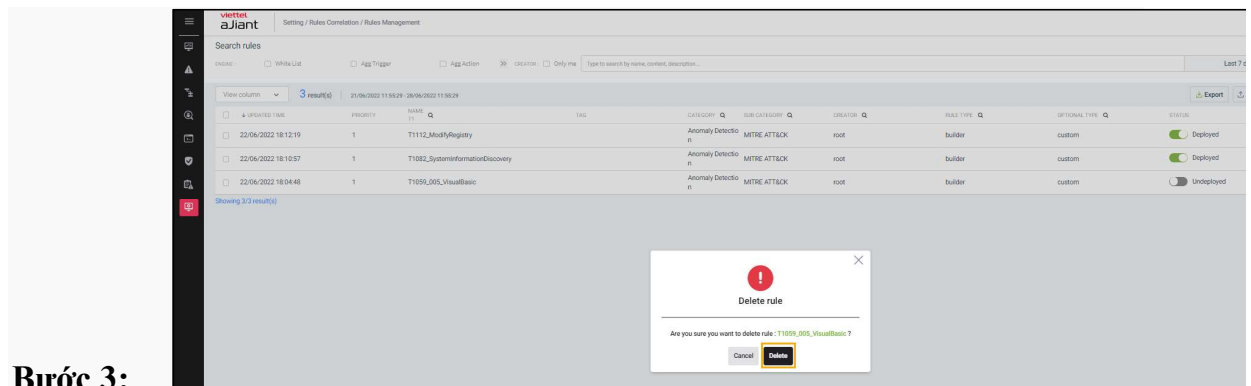
3.10.3 Xóa Rules Correlation



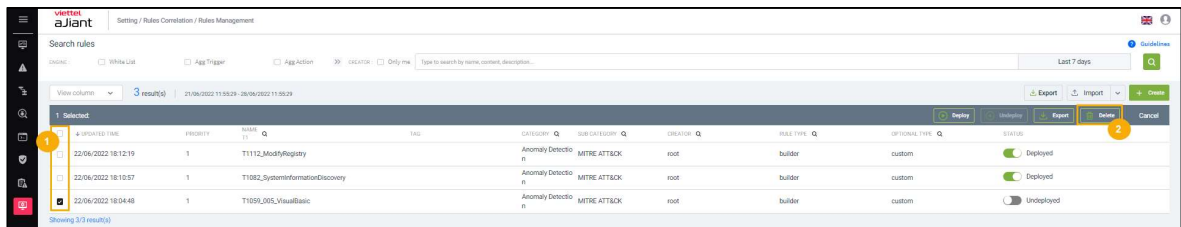
Các bước thực hiện xóa 01 rule:

Bước 1: Click icon “Xóa” tại rule muốn xóa;

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



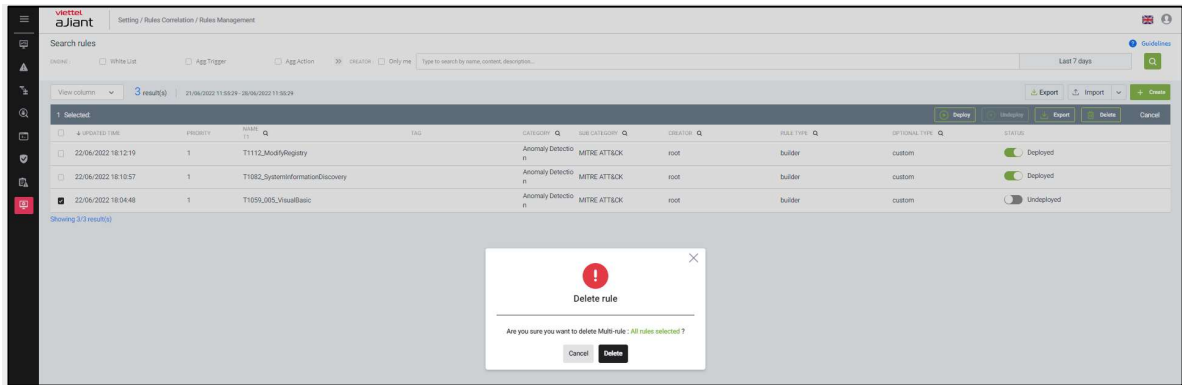
+ Nếu chọn “Delete”, rule được chọn xóa sẽ biến mất khỏi màn hình hiển thị;



Các bước thực hiện xóa nhiều rule:

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

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



Bước 3: Chọn “Delete”, tất cả rule sẽ được xóa khỏi màn hình hiển thị. Chọn “Cancel”, thao tác vừa chọn sẽ được hủy bỏ.

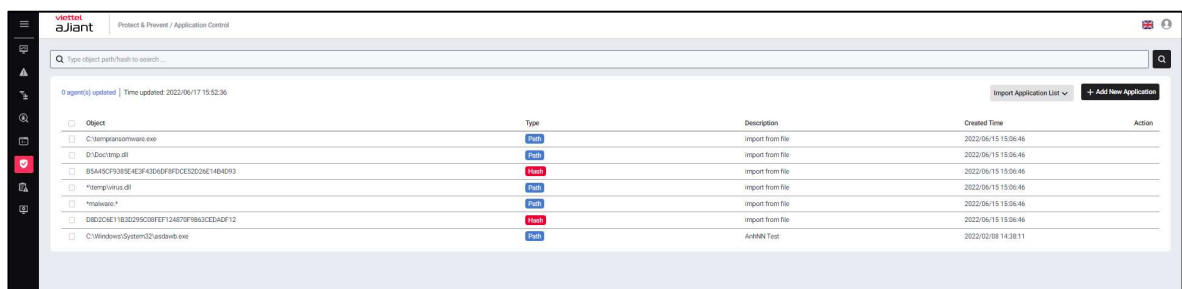
3.11 Protect & Prevention

3.11.1 Application Control

Mục đích: Chức năng Application Control cho phép cấu hình các ứng dụng/tiến trình (process) sẽ chặn dưới máy người dùng không cho phép chạy (execute). Ứng dụng/tiến trình được nhận dạng dựa vào mã băm (MD5, SHA1, SHA256) hoặc đường dẫn.

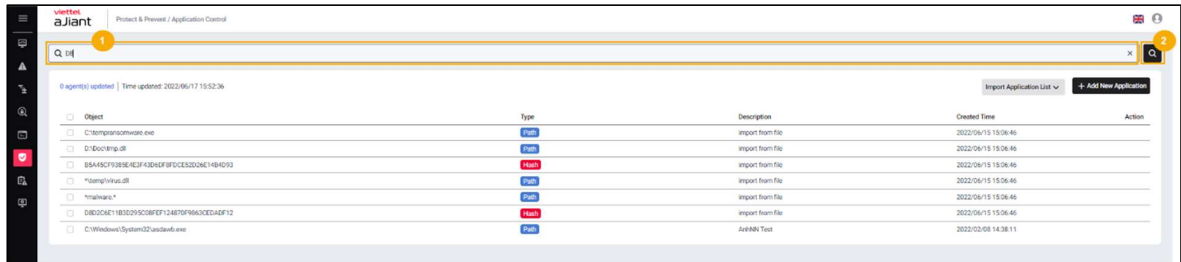
3.11.1.1 Hiển thị danh sách các ứng dụng/tiến trình bị chặn

Click vào tab Protect & Prevention > chọn Application control sẽ hiển thị toàn bộ các ứng dụng/tiến trình dưới máy người dùng không cho sử dụng.



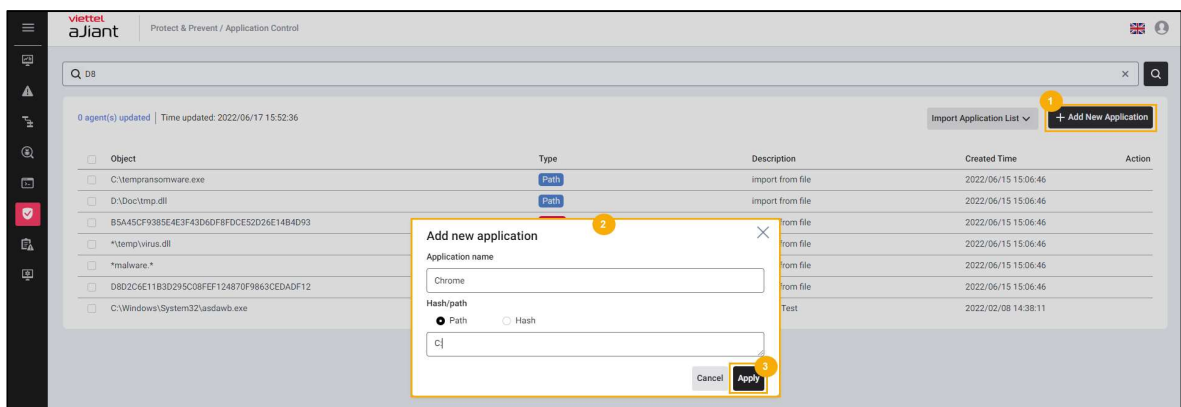
3.11.1.2 Tìm kiếm ứng dụng/tiến trình bị chặn

Người dùng có thể tìm kiếm theo mã băm hoặc đường dẫn của ứng dụng bị chặn



3.11.1.3 Thêm mới ứng dụng/tiến trình bị chặn

Click vào “Add new” để thêm mới ứng dụng/tiến trình bị chặn, người dùng có thể chọn chặn theo Path hoặc mã Hash (MD5, SHA1, SHA256)



3.11.1.4 Thêm mới ứng dụng/tiến trình 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;

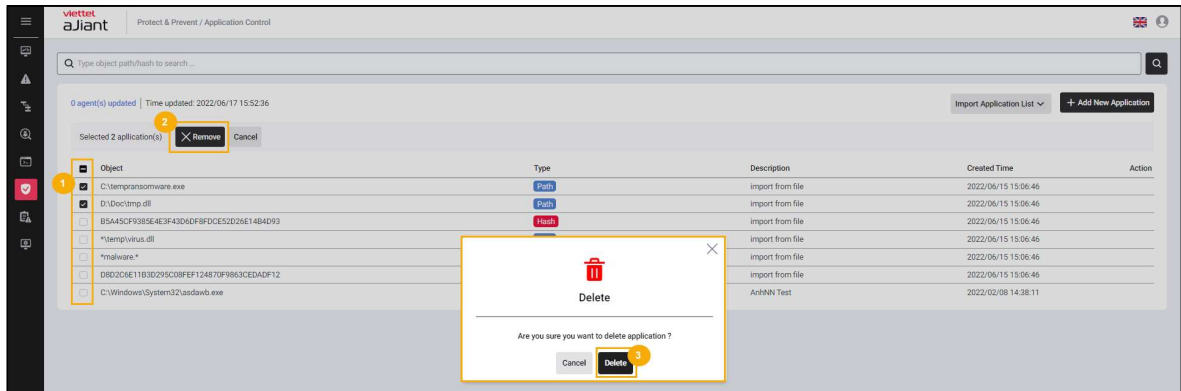
Click “Import”, chọn đường dẫn đến file cần tải lên và click “Open”, hệ thống sẽ tự động thêm danh sách các ứng dụng cần chặn lên hệ thống.



3.11.1.5 Xóa ứng dụng/tiến trình bị chặn trong danh sách

Hệ thống hỗ trợ xóa 1 hoặc nhiều ứng dụng bị chặn;

Click vào từng ứng dụng cần xóa và click icon “Delete”, hoặc click vào checkbox đầu mỗi ứng dụng và click nút “Delete”



3.11.1.6 Luồng cập nhật số lượng các máy agent đã cập nhật danh sách mới thành công

Sau khi người dùng thêm/sửa/xóa danh sách các tiến trình trên giao diện, hệ thống sẽ cập nhật danh sách này xuống dưới các agent theo luồng update file agent (chu kỳ 3 phút/lần). Agent nhận được cấu hình mới, phát sinh log với eventID =101 và đẩy lên server, hiển thị trên màn hình Event search. Sau đó hệ thống sẽ tự động cập nhật số lượng agent đã cập nhật danh sách cấu hình mới trên màn Application control.

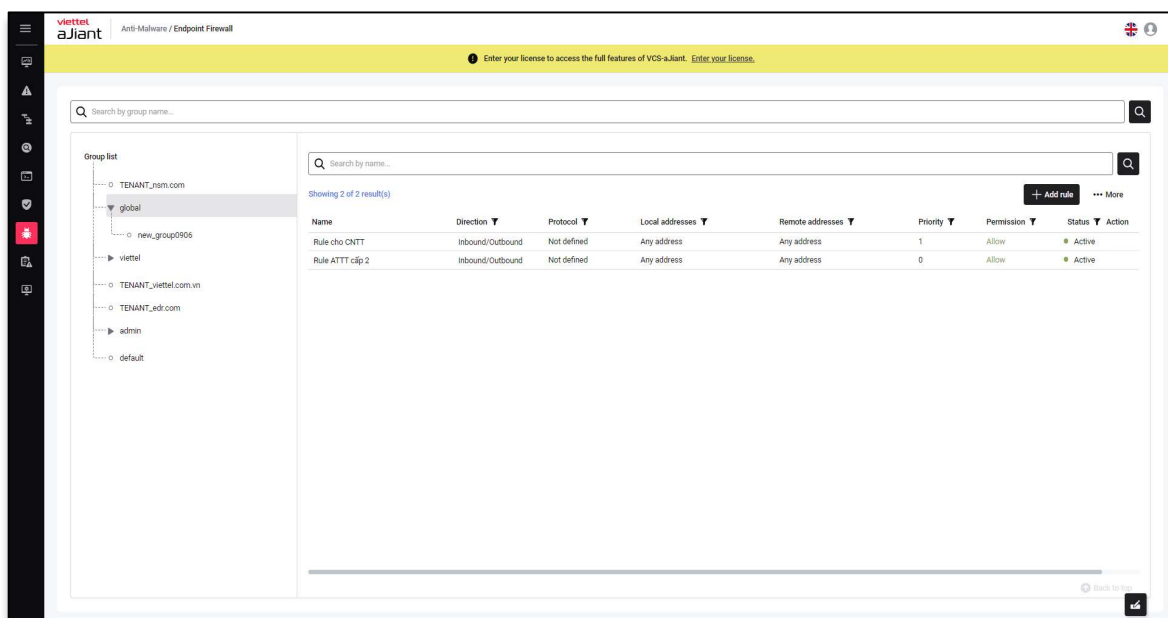


3.11.2 Endpoint Firewall

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.

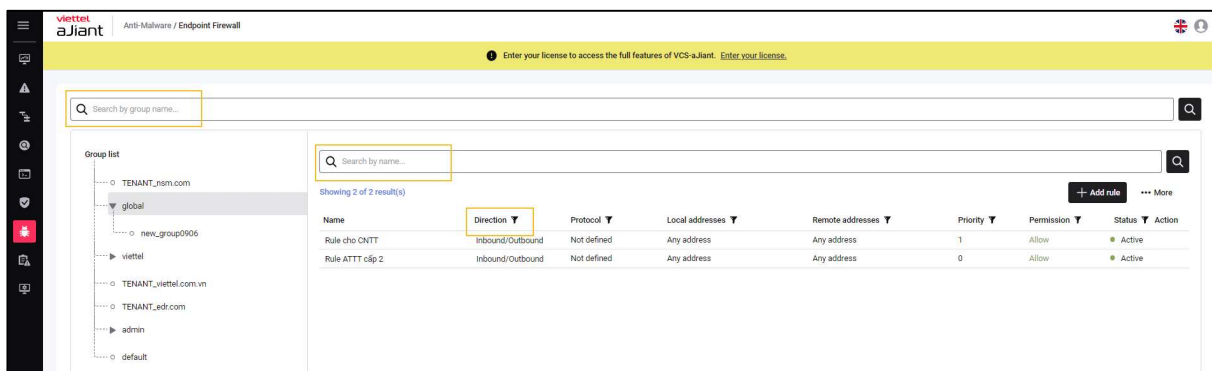
3.11.2.1 Hiện thị danh sách các kết nối bị chặn

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



3.11.2.2 Tìm kiếm các kết nối bị chặn

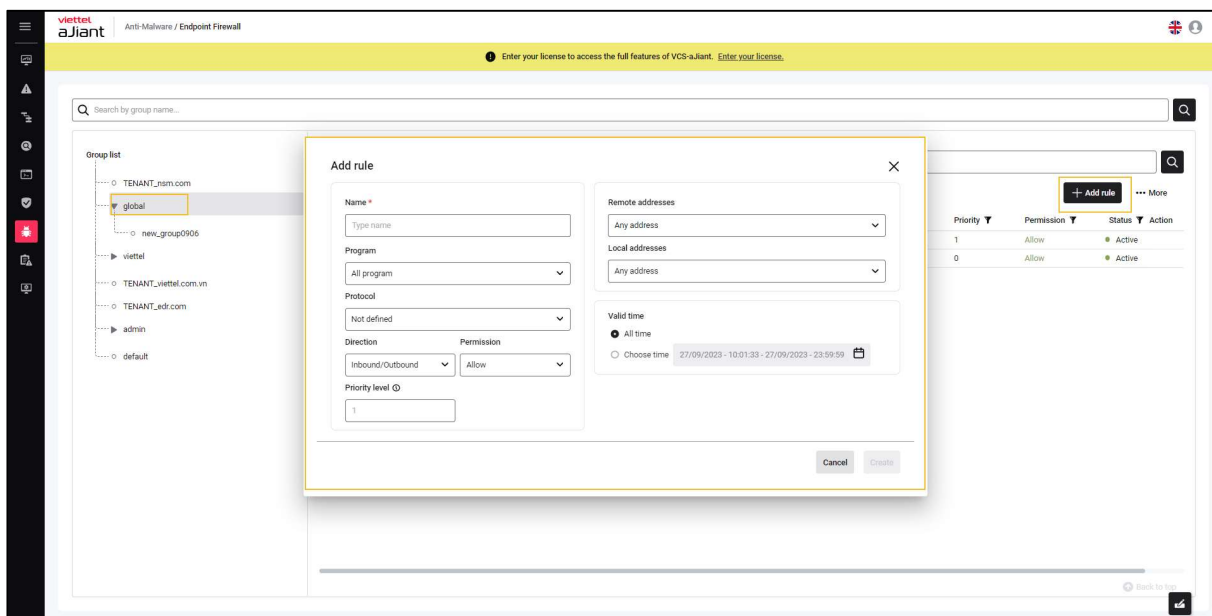
Người dùng có thể tìm kiếm theo nhóm người dùng, theo tên quy tắc firewall hoặc filter theo giá trị của từng điều kiện (Tên, kiểu connect inbound/outbound, ip...) trên màn danh sách firewall:



3.11.2.3 Thêm mới các kết nối bị chặn

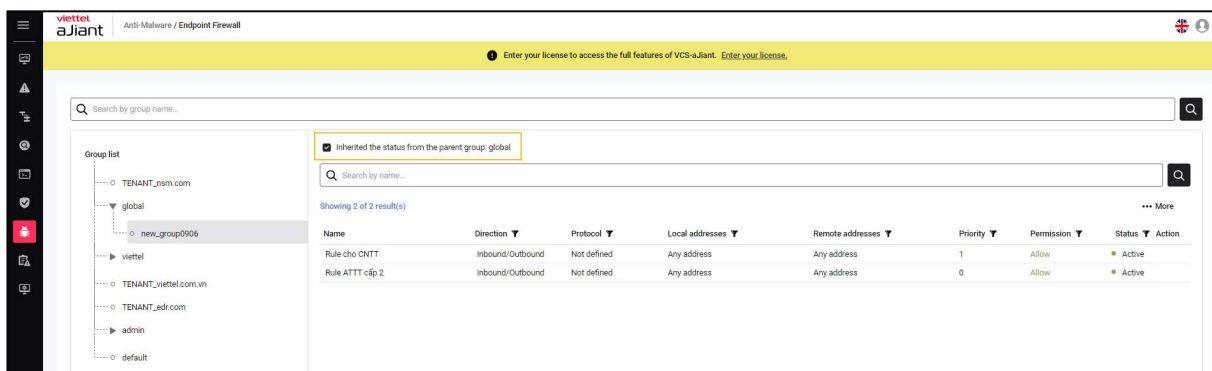
Chọn nhóm người, sau đó Click nút “Add new”, nhập thông tin trên popup thêm mới kết nối bị chặn

- + 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



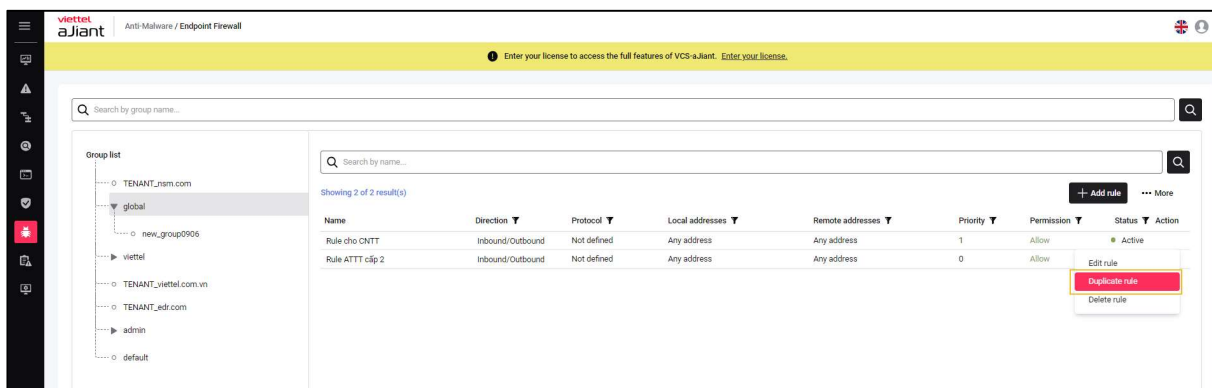
Lưu ý: quy tắc kế thừa từ nhóm cha

- + 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



3.11.2.4 Tạo bản sao chép từ điều kiện đã có

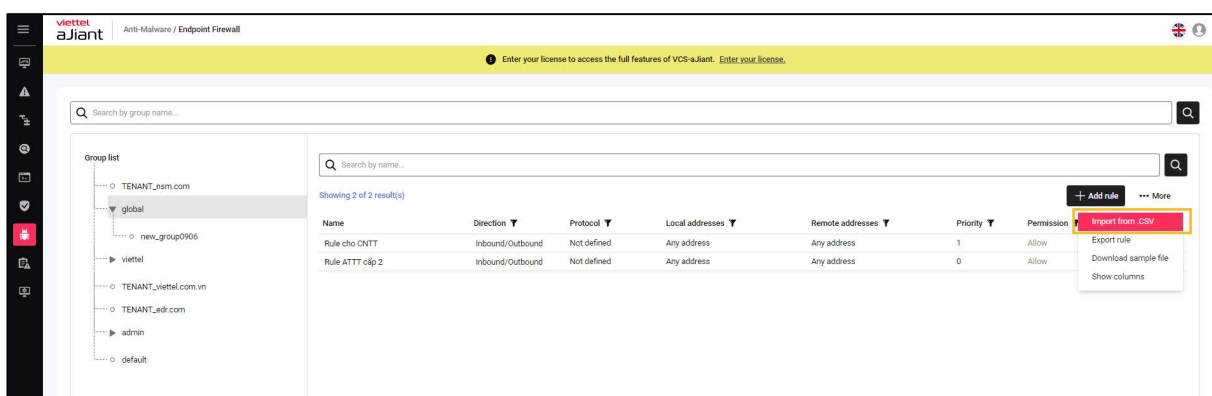
Chọn điều kiện muốn tạo bản sao chép, thực hiện Action, chọn *Duplicate rule*



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

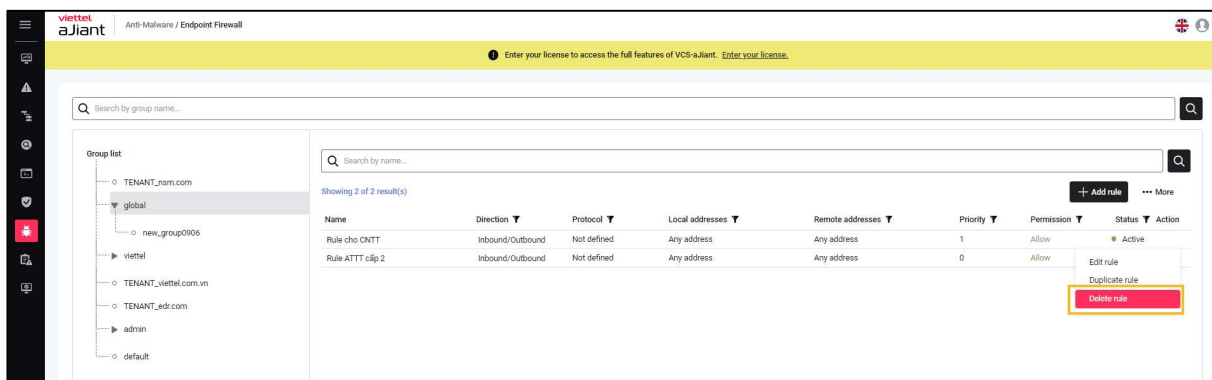
Người dùng có thể thêm mới các ứng dụng/tiến trình bị chặn từ tập tin .csv theo mẫu có sẵn lên danh sách ứng dụng hiện tại;

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;



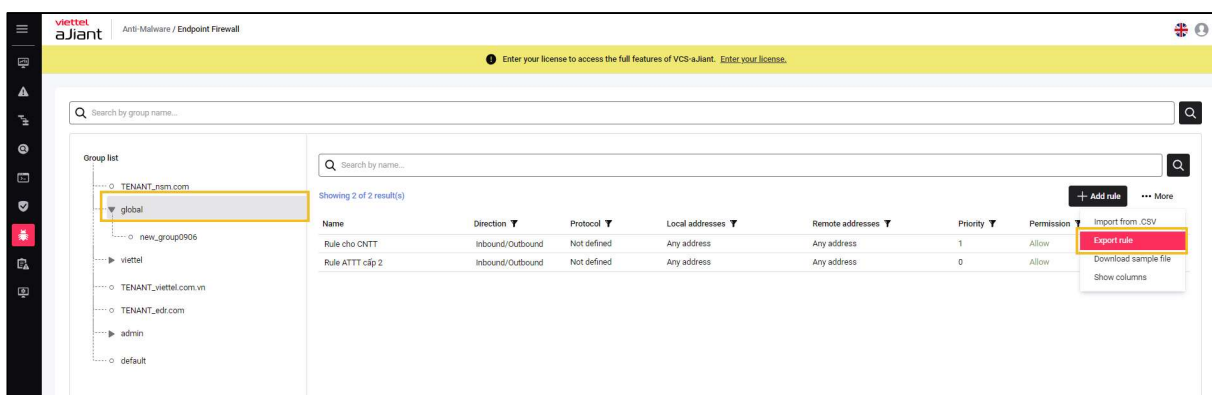
3.11.2.6 Xóa kết nối bị chặn trong danh sách

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



3.11.2.7 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



3.12 Anti – Malware

3.12.1 Scan Schedule

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

3.12.1.1 Tìm kiếm Scan Schedule task

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

Các bước thực hiện:

Showing 11 of 11 result(s)

Task name	Author	Created time	Scan type	Number of agent(s)	Trigger	Start time	Next run time	Expired time	Status	Action
ubuntu 2	root	06/10/2022 - 16:15:56	Quick scan	1	Immediately	06/10/2022 - 16:15:56	N/A	N/A	Finished	
Ubuntu	root	06/10/2022 - 16:11:44	Quick scan	1	Immediately	06/10/2022 - 16:11:44	N/A	N/A	Finished	
Quick Win 11	root	06/10/2022 - 16:07:34	Quick scan	1	Immediately	06/10/2022 - 16:07:34	N/A	N/A	Finished	
Task win 11	root	06/10/2022 - 16:03:41	Custom scan	1	Immediately	06/10/2022 - 16:03:41	N/A	N/A	Finished	
Task 456	root	06/10/2022 - 11:37:08	Quick scan	1	At 06/10/2022 - 12:39:30	06/10/2022 - 12:39:30	N/A	N/A	Finished	
Task 123	root	06/10/2022 - 11:34:26	Quick scan	1	Immediately	06/10/2022 - 11:34:26	N/A	N/A	Finished	
éwewe	root	06/10/2022 - 11:17:59	Quick scan	2	Immediately	06/10/2022 - 11:17:59	N/A	N/A	Finished	
Task 1	root	06/10/2022 - 11:14:04	Quick scan	2	Immediately	06/10/2022 - 11:14:04	N/A	N/A	Finished	
Task mal	root	06/10/2022 - 11:10:10	Quick scan	1	Immediately	06/10/2022 - 11:10:10	N/A	N/A	Finished	
maltest	root	06/10/2022 - 10:54:37	Quick scan	1	Immediately	06/10/2022 - 10:54:37	N/A	N/A	Finished	
Task 2	root	06/10/2022 - 09:09:09	Custom scan	1	Immediately	06/10/2022 - 09:09:09	N/A	N/A	Finished	

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.

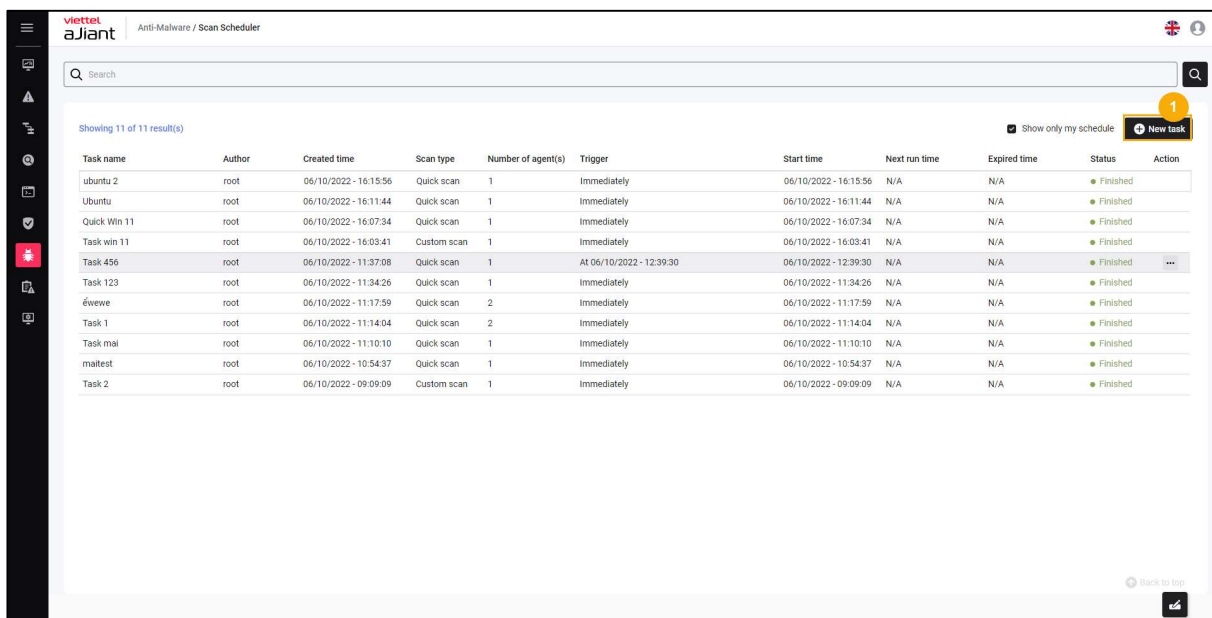
Bước 3: Hệ thống sẽ hiển thị danh sách lập lịch quét theo từ khóa tìm kiếm.

3.12.1.2 Thêm mới Scan Schedule task

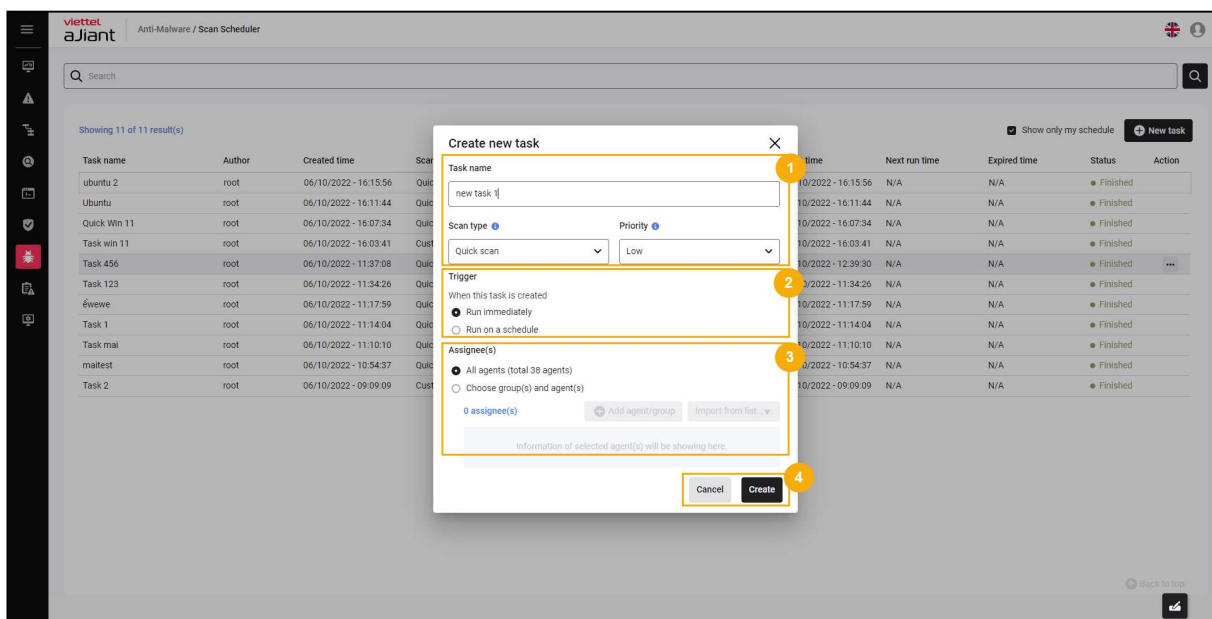
Mục đích: Cho phép người dùng thêm mới một lập lịch quét, cấu hình thời gian và thông tin máy trạm.

Các bước thực hiện:

Bước 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:



– 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;

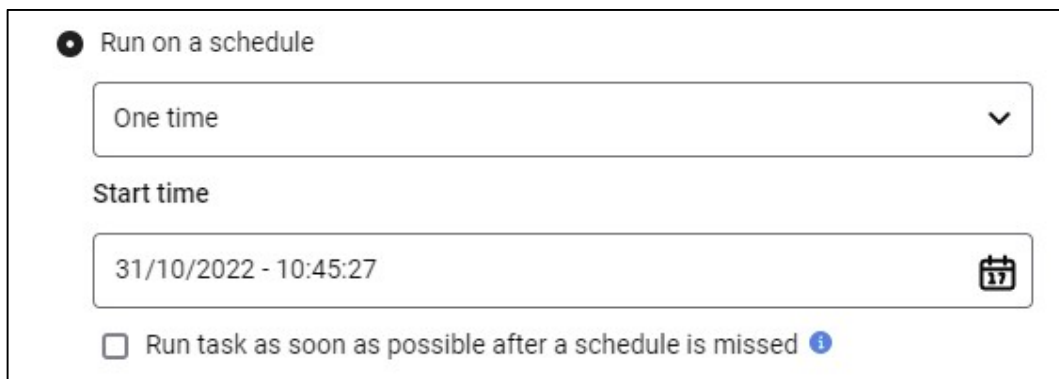
- + Quét toàn bộ: Kiểm tra toàn bộ các tệp và thư mục trong máy tính. Quá trình này có thể mất vài giờ để hoàn thành;
- + Quét tùy chỉnh: Cho phép người dùng một tệp / thư mục cụ thể trong máy tính của bạn để quét.

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.

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

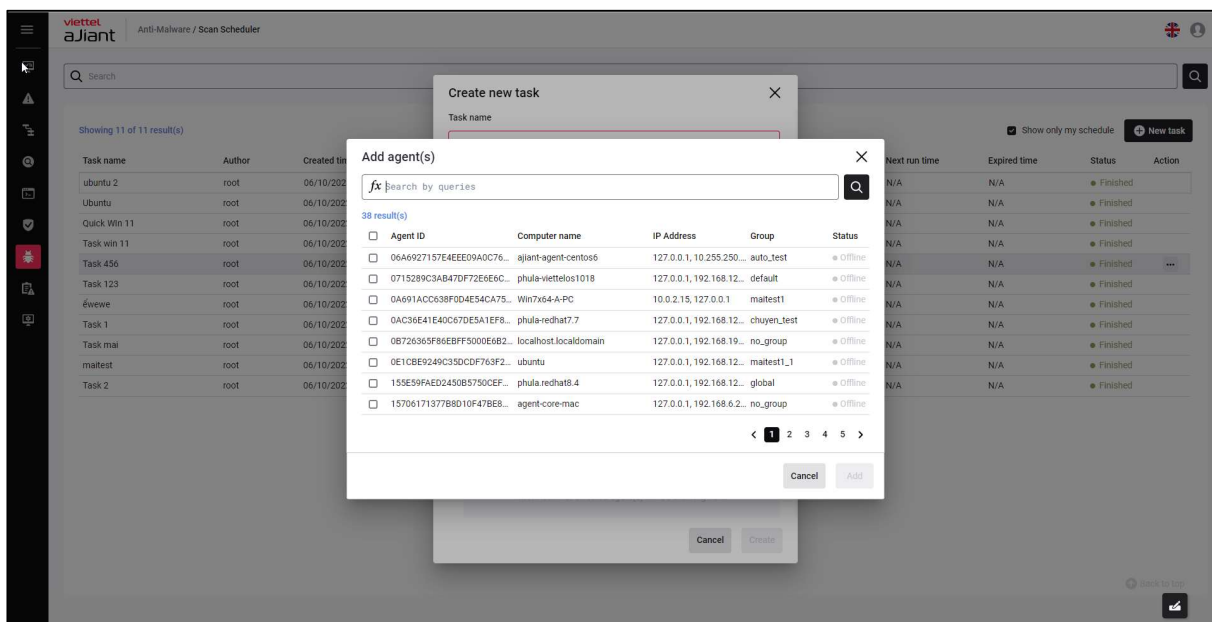
All Agent(s): Lập lịch với tất cả các máy trạm thuộc quyền quản lý của người dùng đang đăng nhập;

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:



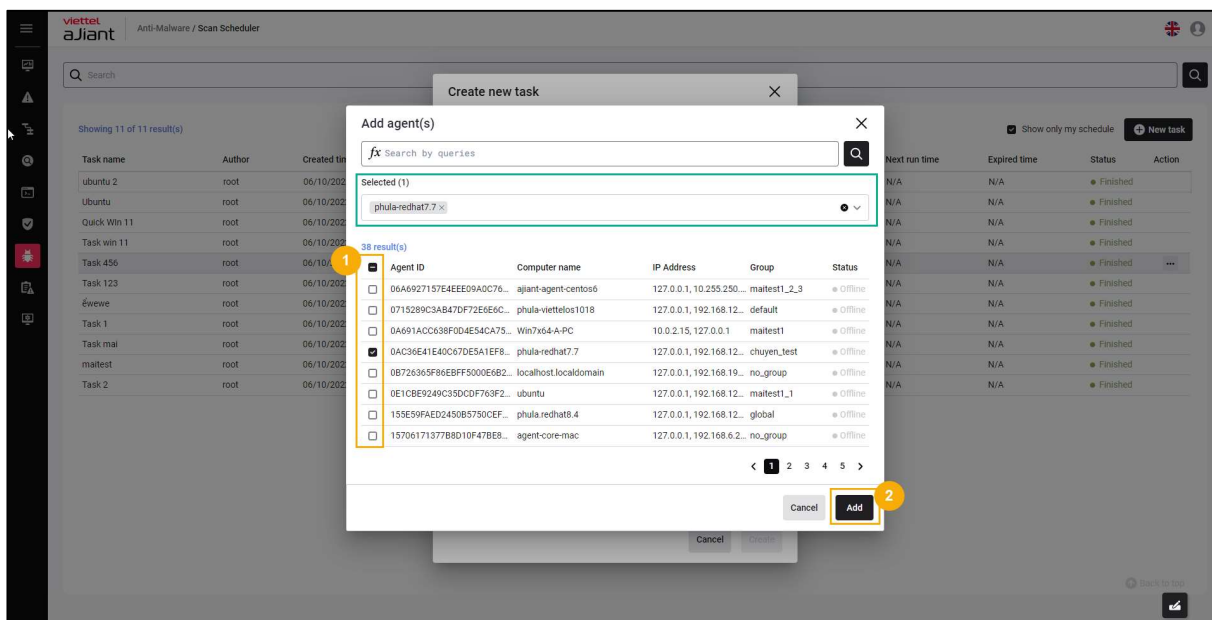
○ Tìm kiếm máy trạm:

▪ Tại popup Add agent(s), người dùng có thể tìm kiếm máy trạm theo truy vấn các trường thông tin: AgentID, Computer name, IP Address, 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;

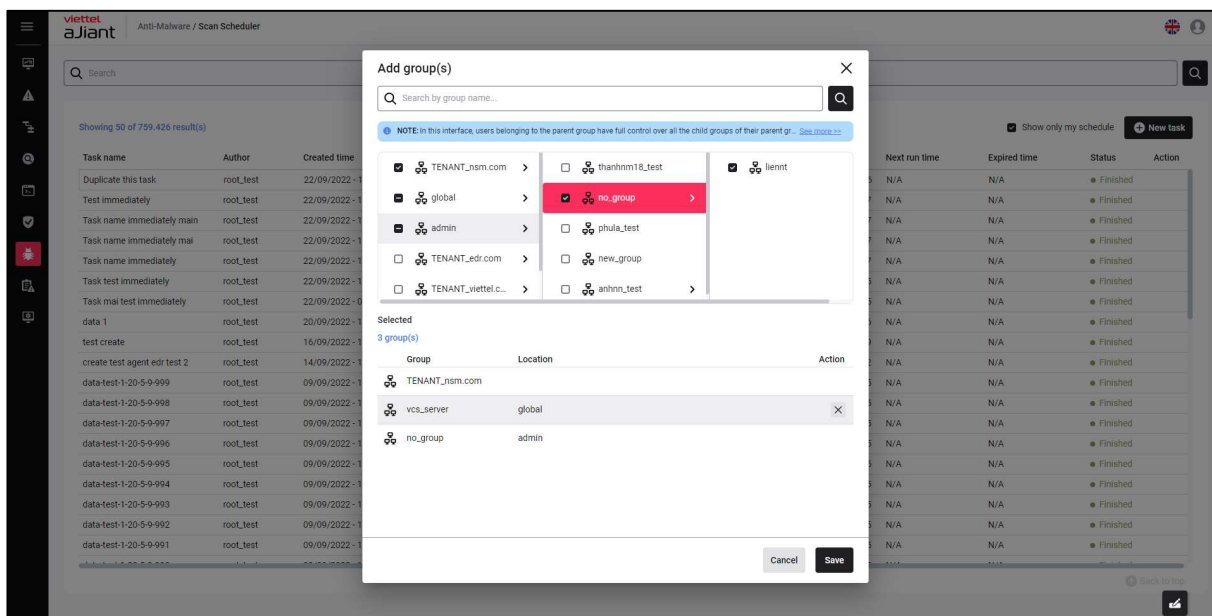
➔ Danh sách các máy trạm được lựa chọn sẽ được tự động thêm vào khung thông tin máy trạm đã được chọn.

- 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**

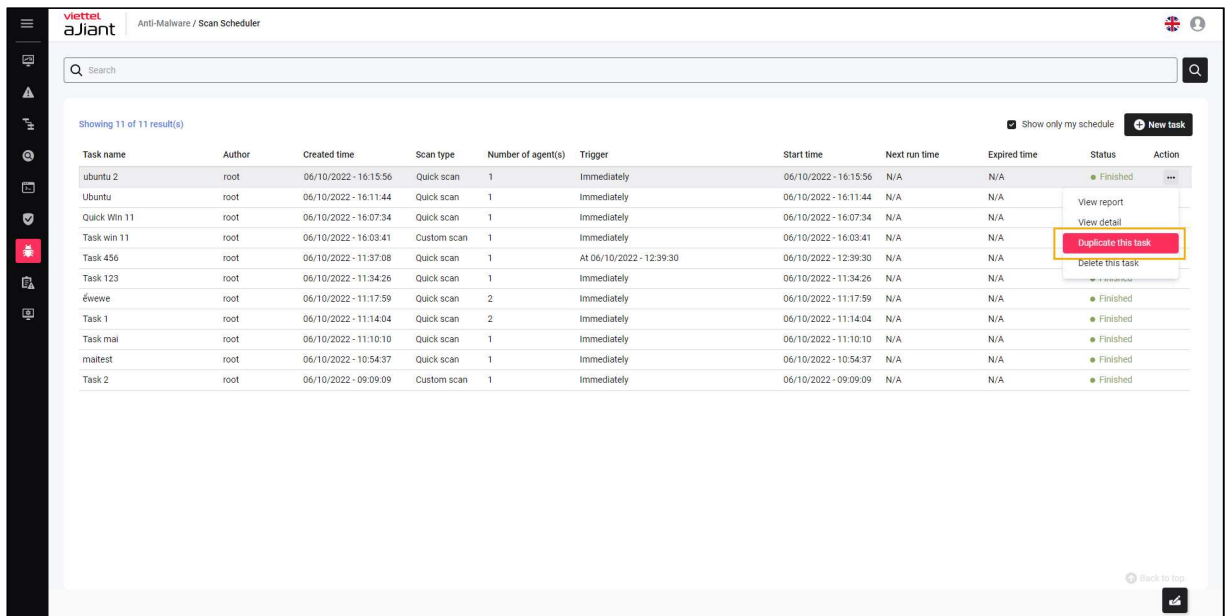
Bước 3: Người dùng chọn nút **Create** để hoàn thiện thao tác thêm mới lập lịch quét. Hoặc, chọn nút **Cancel** để hủy thao tác thêm mới lập lịch quét

3.12.1.3 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:

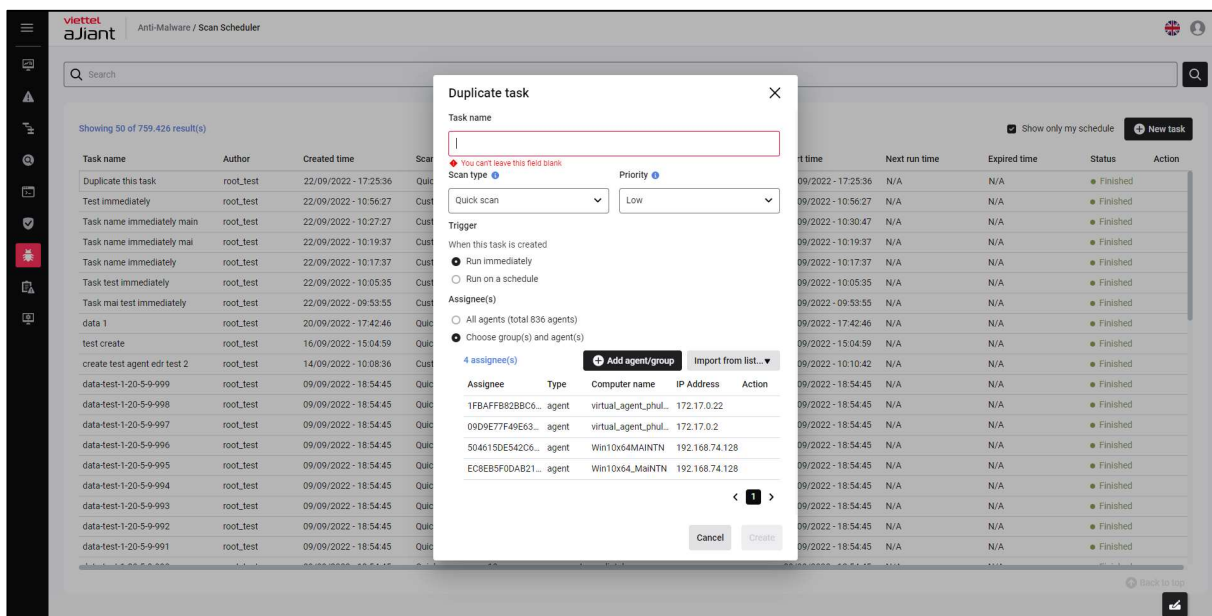


Showing 11 of 11 result(s) Show only my schedule New task

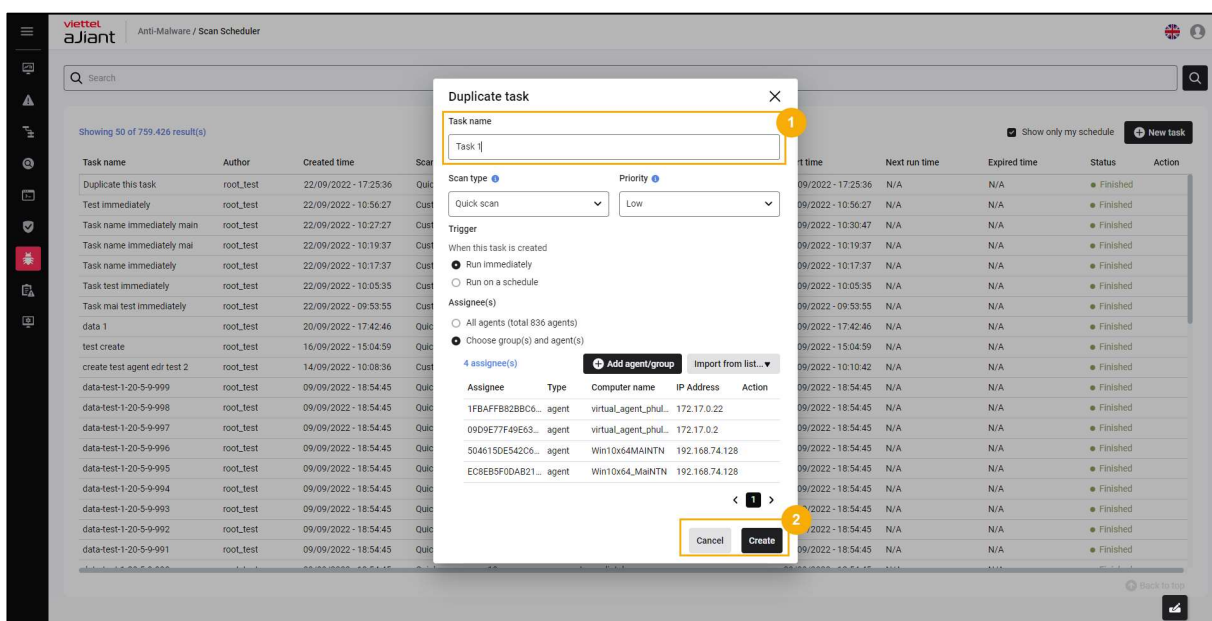
Task name	Author	Created time	Scan type	Number of agent(s)	Trigger	Start time	Next run time	Expired time	Status	Action
ubuntu 2	root	06/10/2022 - 16:15:56	Quick scan	1	Immediately	06/10/2022 - 16:15:56	N/A	N/A	Finished	...
Ubuntu	root	06/10/2022 - 16:11:44	Quick scan	1	Immediately	06/10/2022 - 16:11:44	N/A	N/A	Finished	View report
Quick Win 11	root	06/10/2022 - 16:07:34	Quick scan	1	Immediately	06/10/2022 - 16:07:34	N/A	N/A	Finished	View detail
Task win 11	root	06/10/2022 - 16:03:41	Custom scan	1	Immediately	06/10/2022 - 16:03:41	N/A	N/A	Finished	Duplicate this task
Task 456	root	06/10/2022 - 11:37:08	Quick scan	1	At 06/10/2022 - 12:39:30	06/10/2022 - 12:39:30	N/A	N/A	Finished	Delete this task
Task 123	root	06/10/2022 - 11:34:26	Quick scan	1	Immediately	06/10/2022 - 11:34:26	N/A	N/A	Finished	
ewewe	root	06/10/2022 - 11:17:59	Quick scan	2	Immediately	06/10/2022 - 11:17:59	N/A	N/A	Finished	
Task 1	root	06/10/2022 - 11:14:04	Quick scan	2	Immediately	06/10/2022 - 11:14:04	N/A	N/A	Finished	
Task mai	root	06/10/2022 - 11:10:10	Quick scan	1	Immediately	06/10/2022 - 11:10:10	N/A	N/A	Finished	
maitest	root	06/10/2022 - 10:54:37	Quick scan	1	Immediately	06/10/2022 - 10:54:37	N/A	N/A	Finished	
Task 2	root	06/10/2022 - 09:09:09	Custom scan	1	Immediately	06/10/2022 - 09:09:09	N/A	N/A	Finished	

Back to list

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.

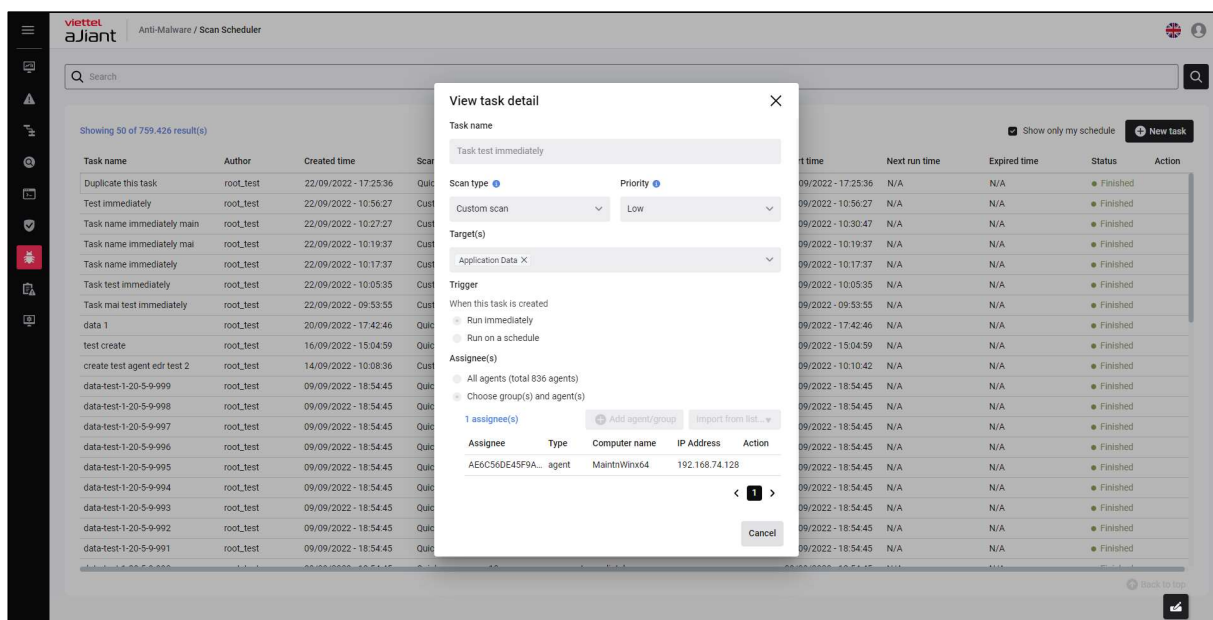


3.12.1.4 Xem chi tiết

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

3.12.1.5 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;

Task name	Author	Created time	Scan type	Number of agent(s)	Trigger	Start time	Next run time	Expired time	Status	Action
Duplicate this task	root_test	22/09/2022 - 17:25:36	Quick scan	5	Immediately	22/09/2022 - 17:25:36	N/A	N/A	Finished	
Test immediately	root_test	22/09/2022 - 10:56:27	Custom scan	1	Immediately	22/09/2022 - 10:56:27	N/A	N/A	Finished	
Task name immediately main	root_test	22/09/2022 - 10:27:27	Custom scan	1	At 22/09/2022 - 10:30:47	22/09/2022 - 10:30:47	N/A	N/A	Finished	
Task name immediately mai	root_test	22/09/2022 - 10:19:37	Custom scan	1	Immediately	22/09/2022 - 10:19:37	N/A	N/A	Finished	View report View detail Duplicate this task Delete this task
Task name immediately	root_test	22/09/2022 - 10:17:37	Custom scan	1	Immediately	22/09/2022 - 10:17:37	N/A	N/A	Finished	
Task test immediately	root_test	22/09/2022 - 10:05:35	Custom scan	1	Immediately	22/09/2022 - 10:05:35	N/A	N/A	Finished	
Task mai test immediately	root_test	22/09/2022 - 09:53:55	Custom scan	1	Immediately	22/09/2022 - 09:53:55	N/A	N/A	Finished	
data 1	root_test	20/09/2022 - 17:42:46	Quick scan	1	Immediately	20/09/2022 - 17:42:46	N/A	N/A	Finished	
test create	root_test	16/09/2022 - 15:04:59	Quick scan	0	Immediately	16/09/2022 - 15:04:59	N/A	N/A	Finished	
create test agent edr test 2	root_test	14/09/2022 - 10:08:36	Custom scan	1	At 29/09/2022 - 10:10:42	29/09/2022 - 10:10:42	N/A	N/A	Finished	
data-test-1-20-5-9-999	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-998	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-997	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-996	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-995	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-994	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-993	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-992	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-991	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	

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

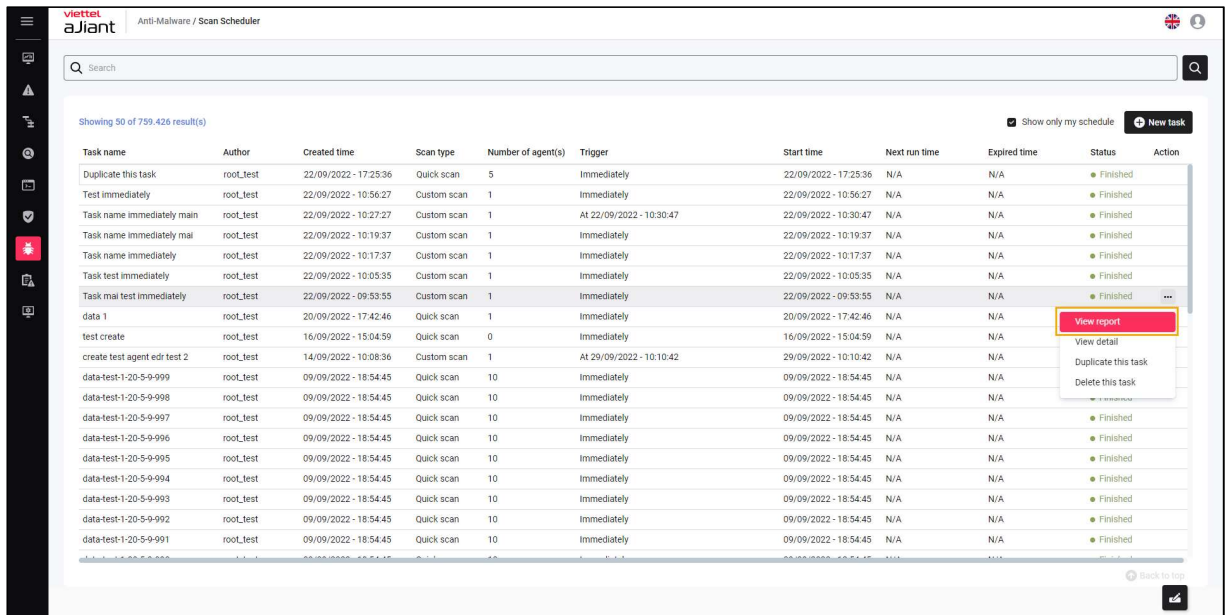
Task name	Author	Created time	Scan type	Number of agent(s)	Trigger	Start time	Next run time	Expired time	Status	Action
Duplicate this task	root_test	22/09/2022 - 17:25:36	Quick scan	5	Immediately	22/09/2022 - 17:25:36	N/A	N/A	Finished	
Test immediately	root_test	22/09/2022 - 10:56:27	Custom scan	1	Immediately	22/09/2022 - 10:56:27	N/A	N/A	Finished	
Task name immediately main	root_test	22/09/2022 - 10:27:27	Custom scan	1	At 22/09/2022 - 10:30:47	22/09/2022 - 10:30:47	N/A	N/A	Finished	
Task name immediately mai	root_test	22/09/2022 - 10:19:37	Custom scan	1	Immediately	22/09/2022 - 10:19:37	N/A	N/A	Finished	
Task name immediately	root_test	22/09/2022 - 10:17:37	Custom scan	1	Immediately	22/09/2022 - 10:17:37	N/A	N/A	Finished	
Task test immediately	root_test	22/09/2022 - 10:05:35	Custom scan	1	Immediately	22/09/2022 - 10:05:35	N/A	N/A	Finished	
Task mai test immediately	root_test	22/09/2022 - 09:53:55	Custom scan	1	Immediately	22/09/2022 - 09:53:55	N/A	N/A	Finished	
data 1	root_test	20/09/2022 - 17:42:46	Quick scan	1	Immediately	20/09/2022 - 17:42:46	N/A	N/A	Finished	
test create	root_test	16/09/2022 - 15:04:59	Quick scan	0	Immediately	16/09/2022 - 15:04:59	N/A	N/A	Finished	
create test agent edr test 2	root_test	14/09/2022 - 10:08:36	Custom scan	1	At 29/09/2022 - 10:10:42	29/09/2022 - 10:10:42	N/A	N/A	Finished	
data-test-1-20-5-9-999	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-998	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-997	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-996	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-995	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-994	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-993	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-992	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	
data-test-1-20-5-9-991	root_test	09/09/2022 - 18:54:45	Quick scan	10	Immediately	09/09/2022 - 18:54:45	N/A	N/A	Finished	

3.12.1.6 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** bên ghi task cần xem báo cáo;



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

– 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:

View task report

Task name

Task per

Created time

14/09/2022 14:32:24

Author

root_test

Scan type

Custom scan

1

2

Q

Export to Excel

View on Dashboard

5 result(s)

Agent ID	Computer name	IP Address	Platform	Group	Status	Result
FC97D9289BFA70F681BB4B8FED595CDEA2CA9AD1	bich3_win7x86	192.168.255.136	Microsoft Windows 7 Ultimate Service Pack 1	group_windows	Scan skip	Start time: 15/09/2022 14:34:52 End time: 15/09/2022 14:34:52 Agent missed this schedule
524B30C4C568F59292D6076E25F4C83AF5C33B5C	EDR-TEST02	192.168.133.1, 192.168.255.1, 192.168.6.40	Microsoft Windows 10 Enterprise	group_1	Scan completed	Start time: 14/09/2022 14:36:18 End time: 14/09/2022 14:36:59 Total file scan: 96 Total malware found: 0
F2AA317BE87690E505BF7D25CA6A7DC68D1FC37D	Bichpt3_Win10Test	192.168.255.138	Microsoft Windows 10 Pro	group_windows	Scan completed	Start time: 14/09/2022 14:36:18 End time: 14/09/2022 14:36:52 Total file scan: 28 Total malware found: 0

Back to top

+ 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.

– Export to Excel

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

View task report

Task name

Task per

Created time

14/09/2022 14:32:24

Author

root_test

Scan type

Custom scan

Q

Export to Excel

View on Dashboard

5 result(s)

Agent ID	Computer name	IP Address	Platform	Group	Status	Result
FC97D9289BFA70F681BB4B8FED595CDEA2CA9AD1	bich3_win7x86	192.168.255.136	Microsoft Windows 7 Ultimate Service Pack 1	group_windows	Scan skip	Start time: 15/09/2022 14:34:52 End time: 15/09/2022 14:34:52 Agent missed this schedule
524B30C4C568F59292D6076E25F4C83AF5C33B5C	EDR-TEST02	192.168.133.1, 192.168.255.1, 192.168.6.40	Microsoft Windows 10 Enterprise	group_1	Scan completed	Start time: 14/09/2022 14:36:18 End time: 14/09/2022 14:36:59 Total file scan: 96 Total malware found: 0
F2AA317BE87690E505BF7D25CA6A7DC68D1FC37D	Bichpt3_Win10Test	192.168.255.138	Microsoft Windows 10 Pro	group_windows	Scan completed	Start time: 14/09/2022 14:36:18 End time: 14/09/2022 14:36:52 Total file scan: 28 Total malware found: 0

Back to top

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.

– View on dashboard

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

Agent ID	Computer name	IP Address	Platform	Group	Status	Result
FC97D9289BFA70F681BB4B8FED595CDEA2CA9AD1	bich3_win7x86	192.168.255.136	Microsoft Windows 7 Ultimate Service Pack 1	group_windows	Scan skip	Start time: 15/09/2022 14:34:52 End time: 15/09/2022 14:34:52 Agent missed this schedule
524B30C4C568F59292D6076E25F4C83AF5C33B5C	EDR-TEST02	192.168.133.1, 192.168.255.1, 192.168.6.40	Microsoft Windows 10 Enterprise	group_1	Scan completed	Start time: 14/09/2022 14:36:18 End time: 14/09/2022 14:36:59 Total file scan: 96 Total malware found: 0
F2A317BE87690E5058F7D25CA6A7DC68D1FC37D	Bichpt3_Win10Test	192.168.255.138	Microsoft Windows 10 Pro	group_windows	Scan completed	Start time: 14/09/2022 14:36:18 End time: 14/09/2022 14:36:52 Total file scan: 28 Total malware found: 0

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;

3.12.2 Device control

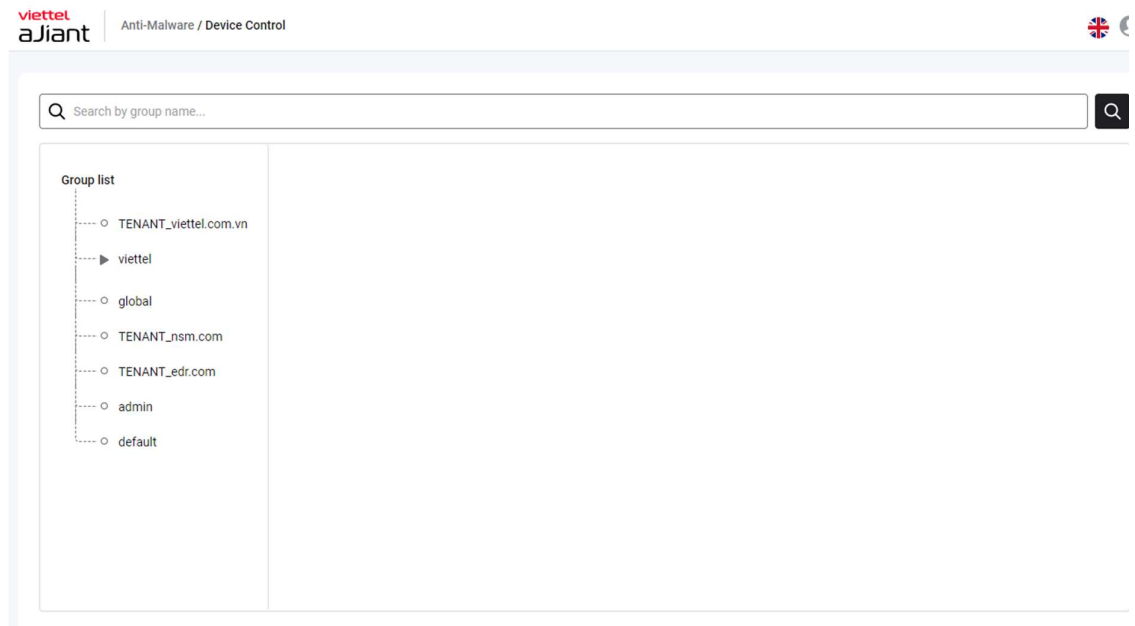
Chức năng: Cho phép kiểm soát, bảo vệ dữ liệu quan trọng thông qua thiết bị ngoại vi, như ổ USB, thiết bị Bluetooth và đĩa CD và DVD ghi được.

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

3.12.2.1 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



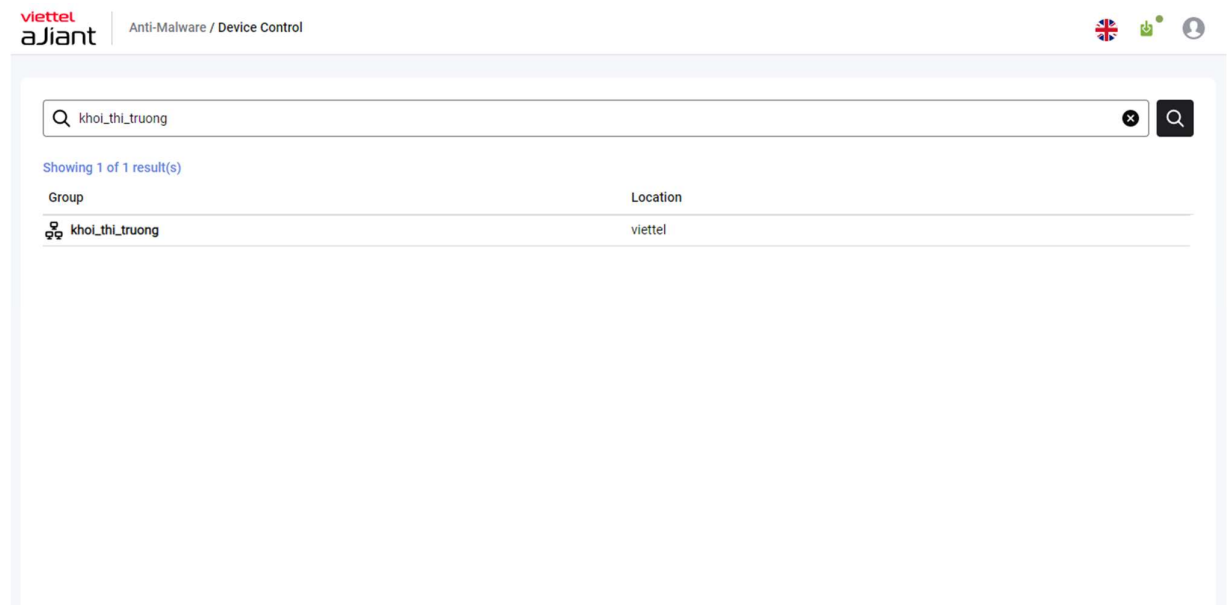
Bước 1: Người dùng nhập vào từ khóa tìm kiếm ở Search by group name (Có từ từ khóa gợi ý theo text)



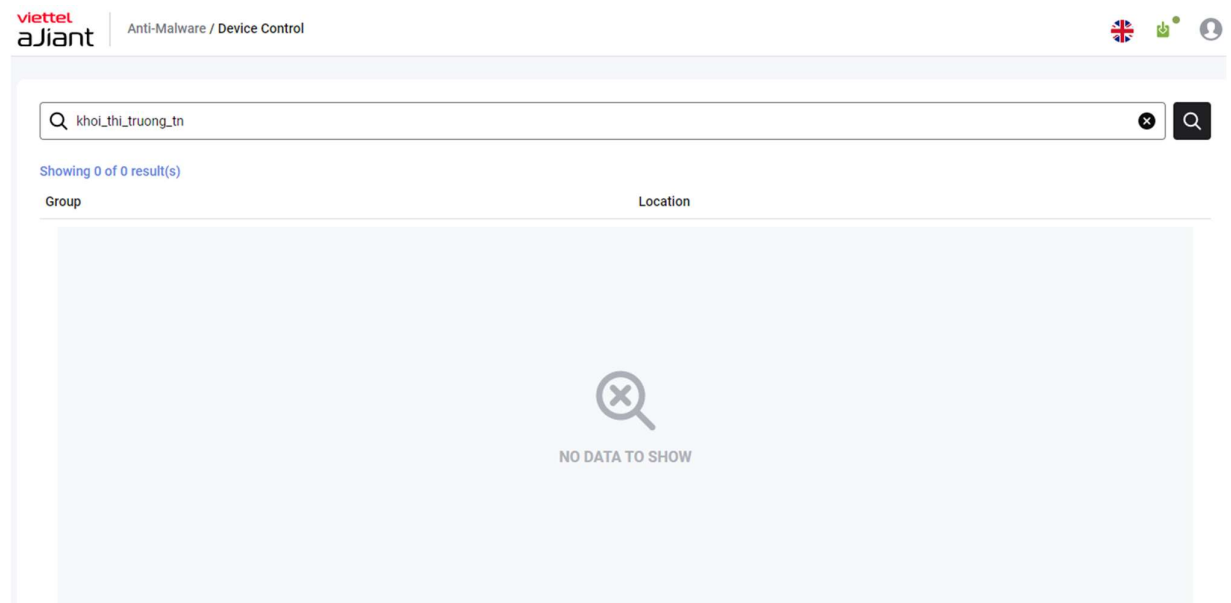
Bước 2: Chọn nút  hoặc nhấn **Enter** để xác nhận thao tác tìm kiếm với từ khóa vừa nhập.

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



3.12.2.2 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

☐ Inherited the status from the father group: liennt

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:

☐ Inherited the status from the father group: liennt

Device type	Status	Numbers of exception rules	Action
Removable drives	☐ Block	0	
Portable devices (MTP, PTP)	☐ Block	0	
Network devices	☐ Block	0	
Camera and scanners	☐ Block	0	
Smart card devices	☐ Block	0	
Other USB devices	☒ Allow	0	

+ **Device type:** hiển thị tên thiết bị fix cứng

+ **Status:** *Allow/Block* hiển thị trạng thái phân quyền truy cập từng loại thiết bị 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)

3.12.2.3 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

Detail - Removable drives



Exception list



Showing 10 of 10 result(s)

Add

Exception name	Description	Duration	Status	Action
zxczc	N/A	Forever	● Active	
teasd	vdvdv	Forever	● Active	
acca	N/A	18/05/2023 05:00:00 - 20/05/2023 14:30:00	● Active	
tasdasd	N/A	Forever	● Active	
tesda	N/A	Forever	● Active	
teasd	N/A	Forever	● Active	
yrdfds	N/A	Forever	● Active	
USB storage block forever	block forever	Forever	● Active	
test forever 2 USB storage	block USB Stor...	Forever	● Active	
test forever	N/A	Forever	● Active	

- TH Numbers of exception rules = 0

>> Hiện thị msg "NO DATA TO SHOW"

- TH Numbers of exception rules !=0

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

Tìm kiếm không có kết quả

>>Hiện 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:

- **Exception name** - hiển thị tên ngoại lệ
- **Description** - Mô tả thông tin được áp dụng ngoại lệ
- **Device(s)** - hiển thị tên device
- **Duration** - hiển thị thời hạn của exception
- **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)

3.12.2.4 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)

Add exception

Exception name *

Rule 01

Permission

Allow

Description

Text description

0/100

Valid time

Forever

Choose time

09:00:00 23/05/2023 - 09:00:00 24/05/2023

Devices list (0)

Add device

Assignees

All agent(s)

Choose group(s) (0)

Choose agent(s) (0)

Cancel

Save

- **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** - Hiện 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 hiện 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 chèn 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:

- **Exception name** - hiển thị tên ngoại lệ
 - **Description** - Mô tả thông tin được áp dụng ngoại lệ
 - **Device(s)** - hiển thị tên device
 - **Duration** - hiển thị thời hạn của exception
 - **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

Device list (1)		Add device
Device ID	Device name	Action
Device USB 123	Thiết bị USB	 

< 1 >

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 available.

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

Quay trở lại màn **Add exception**

Assign 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 hiển thị thêm button **Add agent**.

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

Add agent(s)
✕

fx AgentID
✕
🔍

36 result(s)

☐	Agent ID	Computer name	IP Address	Group	Status
☐	077278CE6797BB6B6395AB...	edr02_win10	192.168.40.129, 127...	vcs_anm	● Online
☐	0EB4F0A2D2FE6432C50AFA...	ubuntu20	127.0.0.1, 10.0.2.15, 1...	vcs_anm	● Online
☐	12CFB4DA48D28053302D14...	DESKTOP-7G2IBRE	192.168.56.1, 192.16...	vcs_anm	● Offline
☐	15B2BBFFBEC988C8080297...	JungJungJung	192.168.195.133, 127...	no_group	● Offline
☐	1A2AA14691E192A4E1AF4A...	Win7x86	192.168.74.132, 127...	khoi_doc_lap	● Offline
☐	1B0A66FD56EDD4C2C6D557...	DESKTOP-R2GBJEF	192.168.198.138, 127...	vcs_anm	● Offline
☐	35BB40573301CD6ECD7194...	HuyenPT-Win7x86	192.168.131.129, 127...	vcs_anm	● Offline
☐	44FF36ED36F0B20030539F5...	JUNGJU_JiuJiu	192.168.195.133, 127...	no_group	● Online

<
1
2
3
4
5
>

Cancel
Add

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: Hiện 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 available 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 hiện thị thêm cột Action (Icon Xóa), 5 bản ghi tối đa nhiều thì phân trang.

Exception name *

Rule 1

You can't leave this field blank.

Permission

Block

Description

Description of this rule

0/100

Valid time

☒ Forever
☐ Choose time

16/05/2023 - 17:13:19 - 17/05/2023 - 17:03:19

Device list (0)

Add device

Assignees

☐ All agent(s)
☐ Choose agent(s) (2)
☒ Choose group(s) (4)

Add group

Group	Location	Action
TENANT_viettel.com.vn		
viettel		
global		
TENANT_nsm.com		

< 1 >

Cancel

Save

- 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;

Add group(s)
✕

NOTE: In this interface, users belonging to the parent group have full control over all the child groups of their parent gr... [See more >>](#)

☐ TENANT_viettel.c...
☐ viettel >
☐ global
☐ TENANT_nsm.com
☐ TENANT_edr.com

Selected (0)

Group	Location	Action
NO DATA TO SHOW		

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

Exception name *

qwr

Permission

Block

Description

wrqw

Valid time

☒ Forever

☐ Choose time

Device list (0)

Assignees

☒ All agent(s)

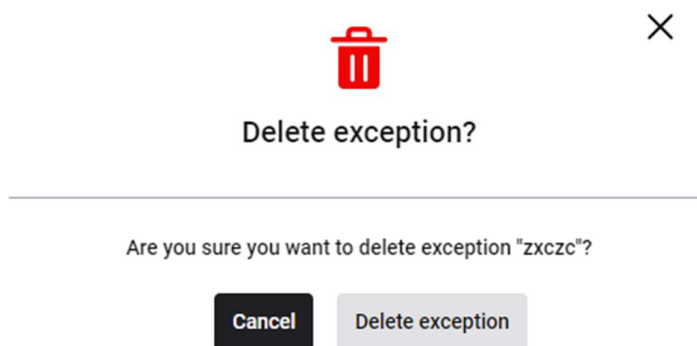
☐ Choose agent(s) (0)

☐ Choose group(s) (0)

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

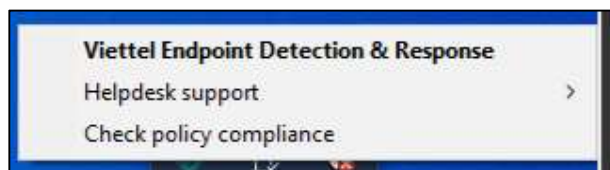
Chọn **Cancel** thì quay lại màn **Device list**.

B. Giao diện Agent

3.13 Main

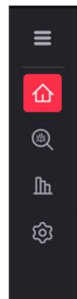
Chức năng cho phép người dùng xem nhanh trạng thái an toàn thông tin tại máy đang cài agent;

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

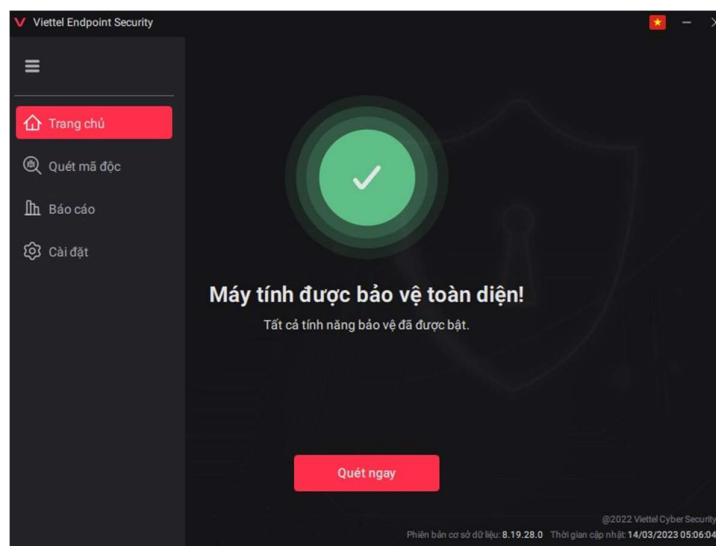


Hệ thống hiển thị các thông tin:

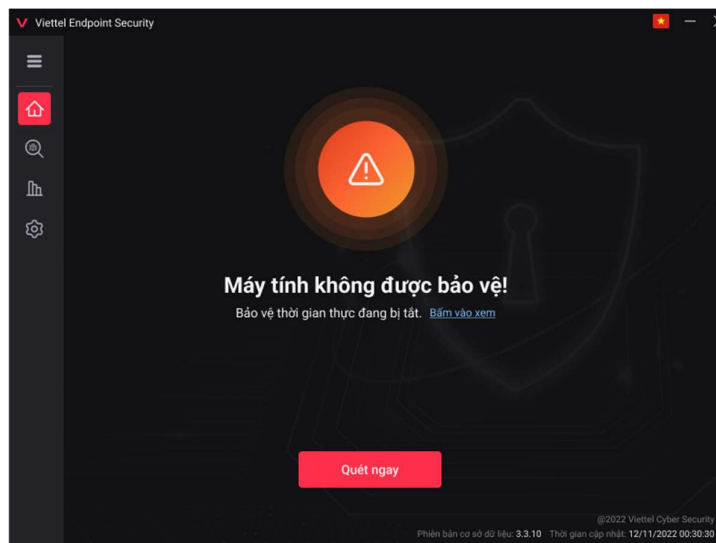
- + Được hiển thị 2 ngôn ngữ: Anh-Việt.
- + Trên Siderbar hiện icon cho các tính năng lớn: Trang chủ, Quét mã độc, Báo cáo, Cài đặt. Có thể đóng hoặc mở rộng sidebar.



- + 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



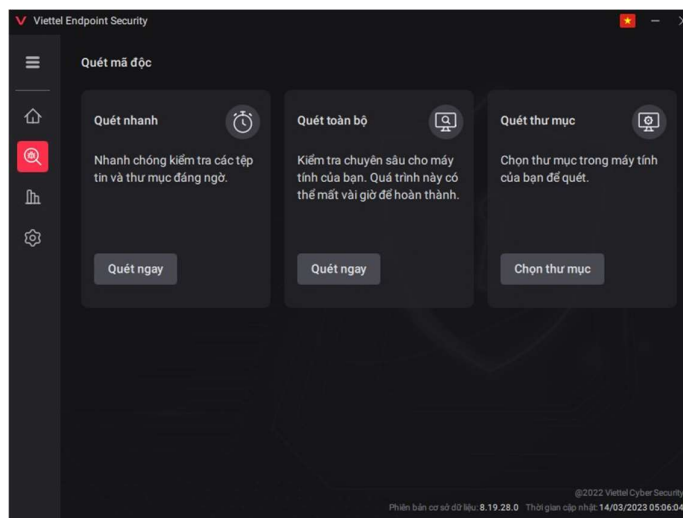
Thông tin về version: thông tin về phiên bản Agent cài trên máy người dùng, thời gian update và thông tin hỗ trợ sản phẩm, được thể hiện ở góc màn hình.

@2022 Viettel Cyber Security
Phiên bản cơ sở dữ liệu: 3.3.10 Thời gian cập nhật: 12/11/2022 00:30:30

3.14 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)

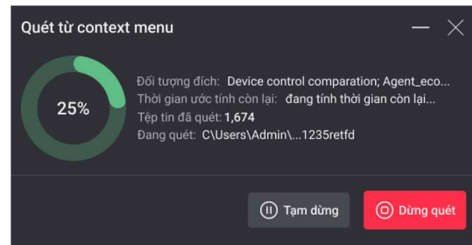


Các phương thức quét được hỗ trợ bao gồm

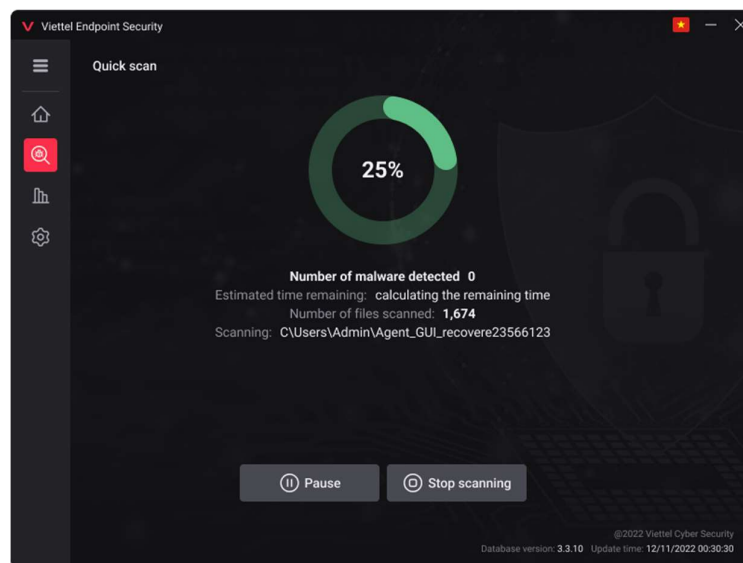
+ Lựa chọn các hình thức quét từ giao diện phía agent;

- **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**);

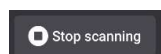


Sau khi chọn phương thức phù hợp, hệ thống thực hiện quét và xử lý mã độc:

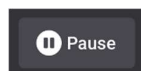


- + Hiển thị % tổng quá trình scan
- + Hiển thị thông tin số lượng mã độc đã được phát hiện
- + Hiển thị thời gian ước lượng còn lại để kết thúc scan
- + Hiển thị số lượng file đã được scan
- + Hiển thị đường dẫn file Đang scan

Hỗ trợ các thao tác trong lúc quét như sau:



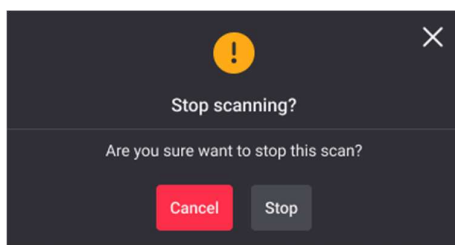
: Cho phép kết thúc quá trình quét;



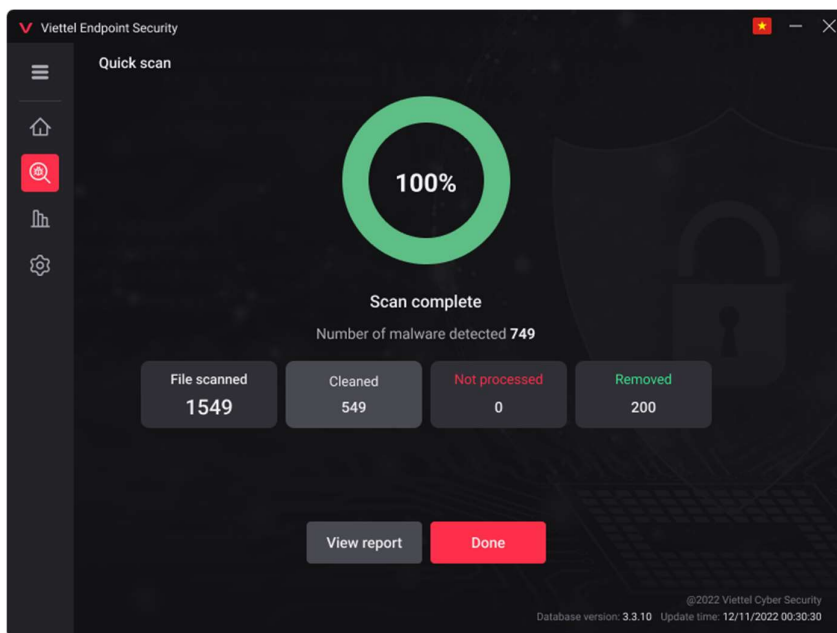
: Cho phép tạm dừng quá trình quét;



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, hiển thị kết quả quét



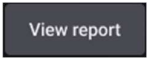
+ File scanned: Hiển thị số lượng file đã được scan

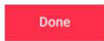
+ Cleaned: Hiển thị tổng số file đã được diệt

+ 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.

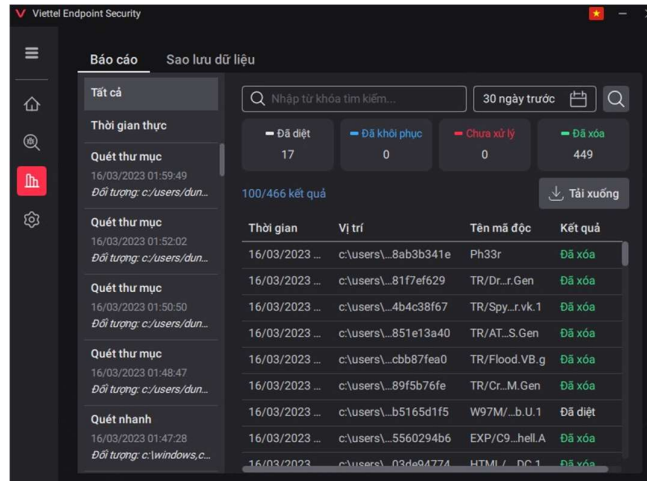
Hoặc có thể click vào button  để xem tổng thể báo cáo của kết quả vừa quét.

Click done  để quay về màn chính của Protection

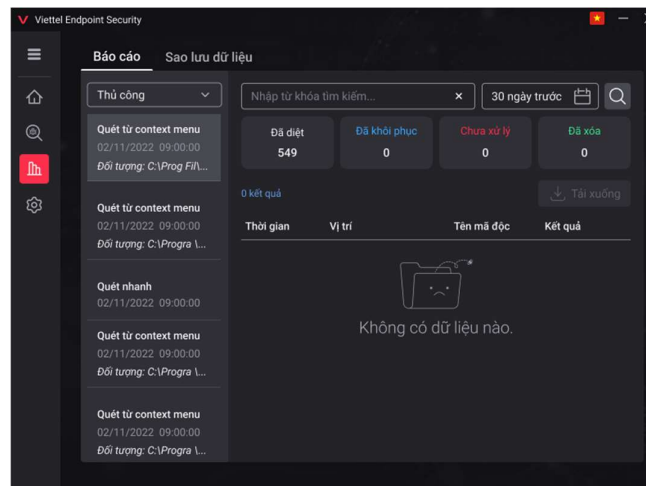
3.15 Report

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

- 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*:

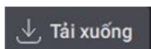
+ Danh sách mã độc: Hiển thị tất cả các mã độc được phát hiện realtime

- *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

— Đã diệt	— Đã khôi phục	— Chưa xử lý	— Đã xóa
17	0	0	449

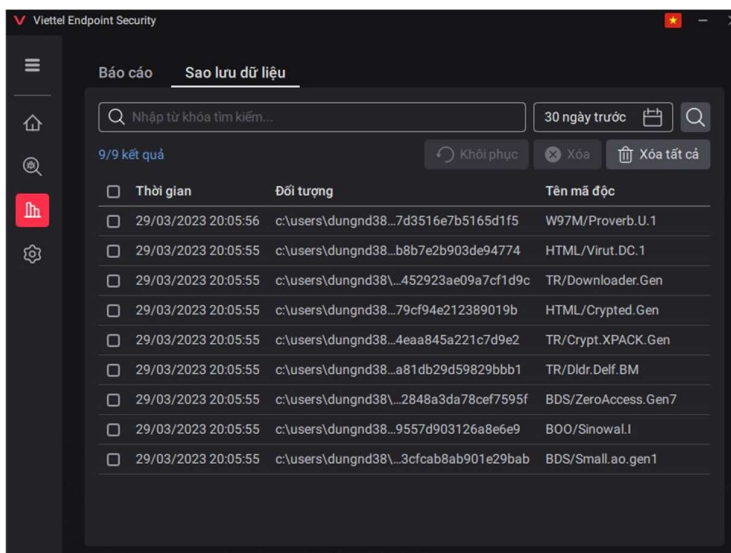


Trong mục report người dùng có thể tải toàn bộ báo cáo về máy (theo các mục đã chọn)

- **Tab Backup**

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

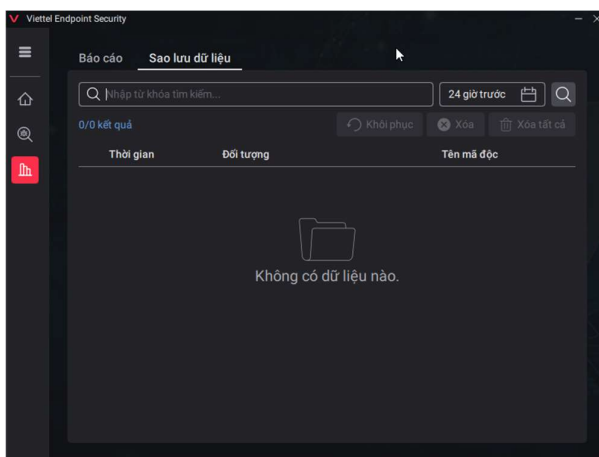
Người dùng có thể tìm kiếm, lựa chọn thời gian rồi click tìm kiếm danh sách sẽ hiển thị theo tham số tìm kiếm.



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;

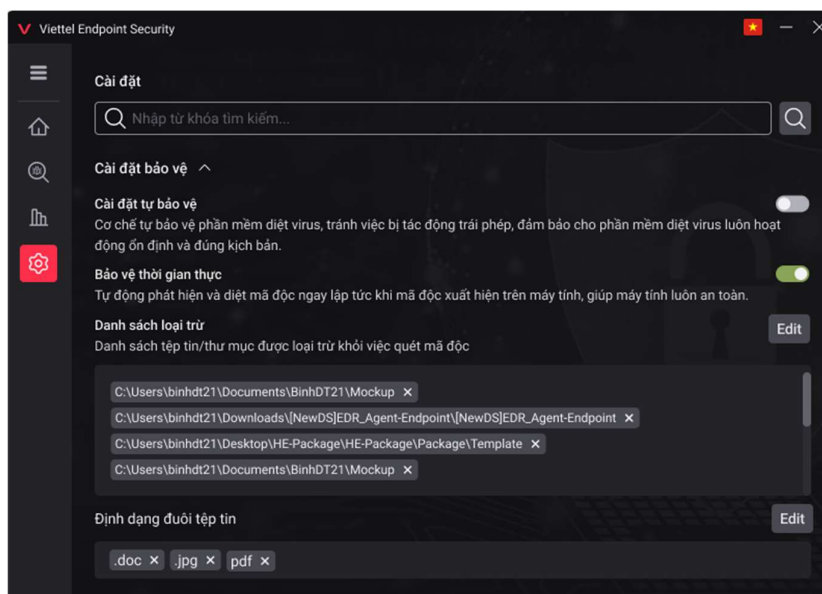
- Trong trường hợp không có kết quả phù hợp với yêu cầu tìm kiếm thì hiển thị trạng thái **Không tìm thấy kết quả phù hợp**



3.16 Setting

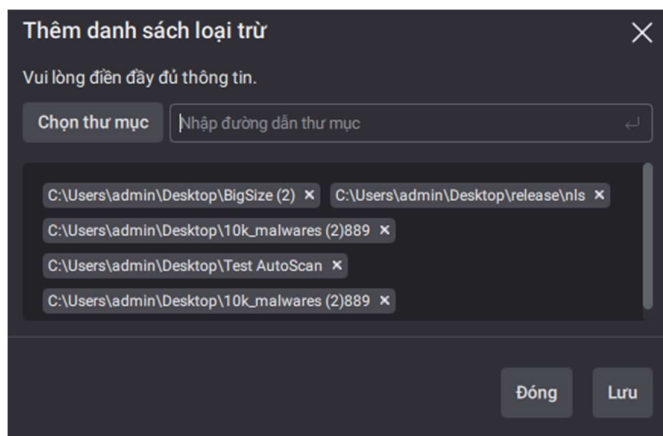
Mục đích: Cấu hình cài đặt trên từng máy agent

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

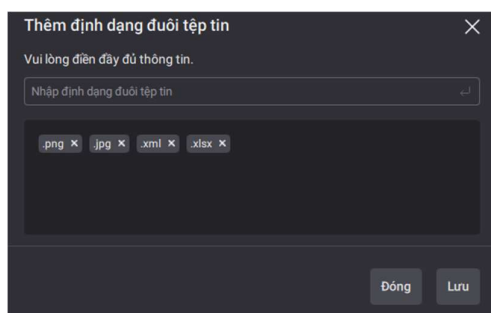


+ **Protection setting** (Cài đặt bảo vệ): Vì có 2 vị trí cấu hình Policy (Self defense và Real-time protection) trên Portal và dưới từng Agent.

- 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*

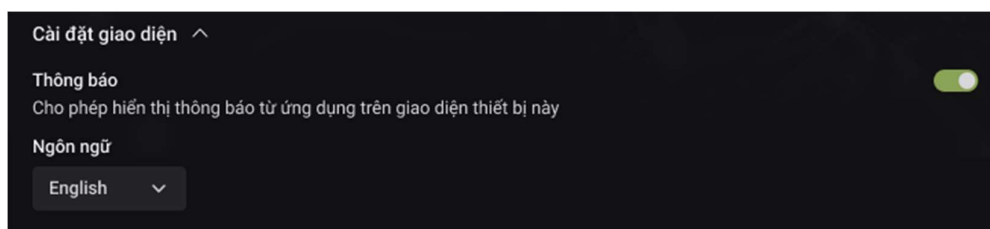


- Extension: Cho phép thêm mới/ chỉnh sửa vào Extension (Loại đuôi tài liệu) được loại trừ (không bị quét bởi Real-time Protection);



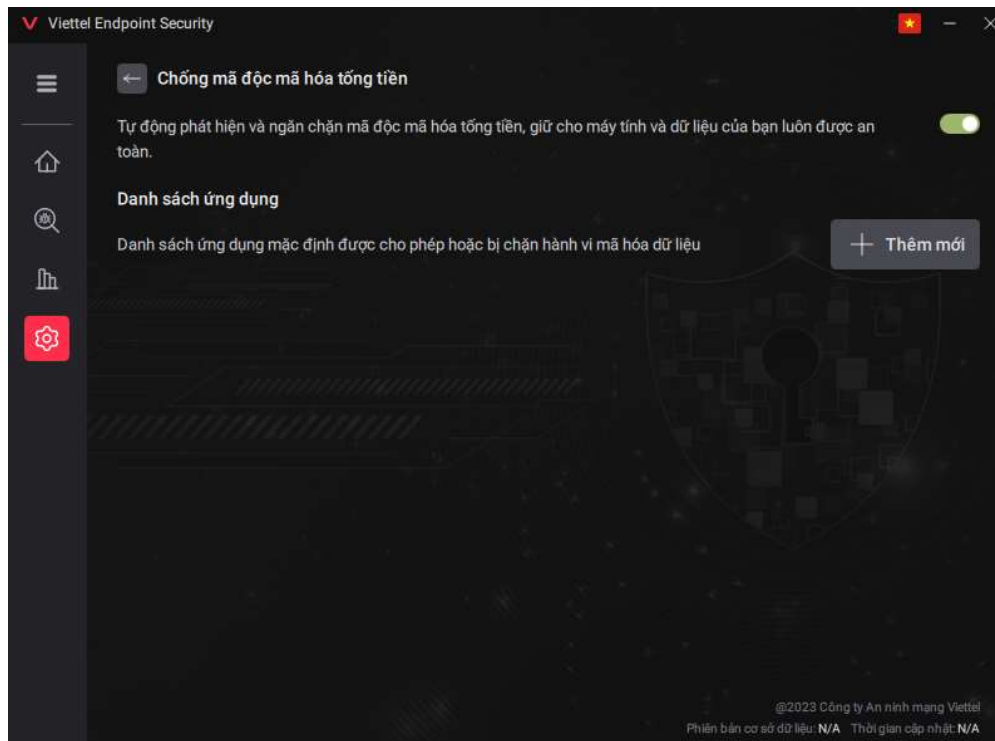
+ Interface setting (Cài đặt giao diện)

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

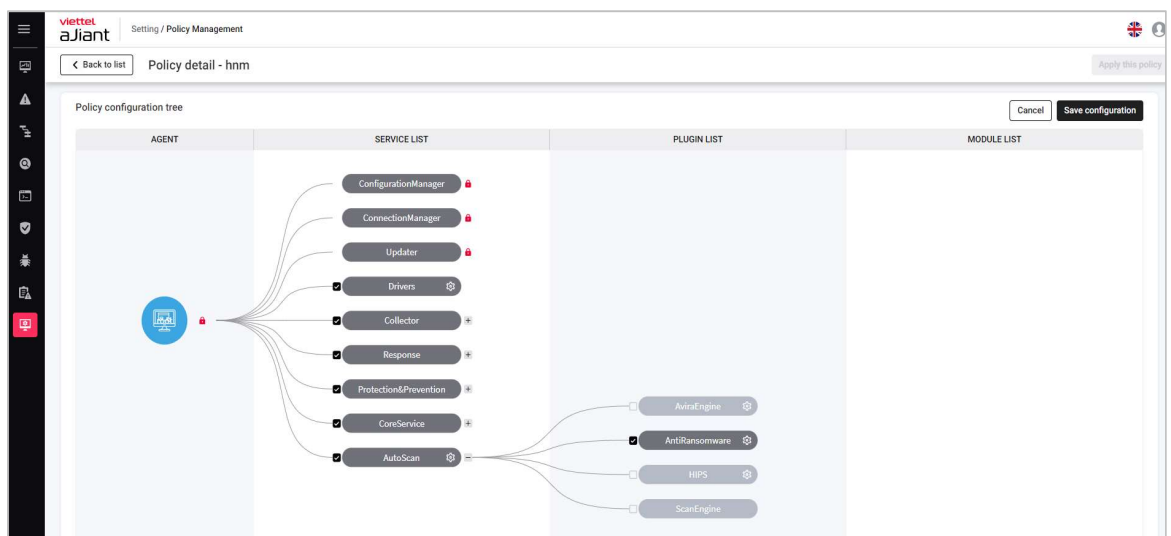


+ Anti-Ransomware (Chống mã độc mã hóa tổng tiền)

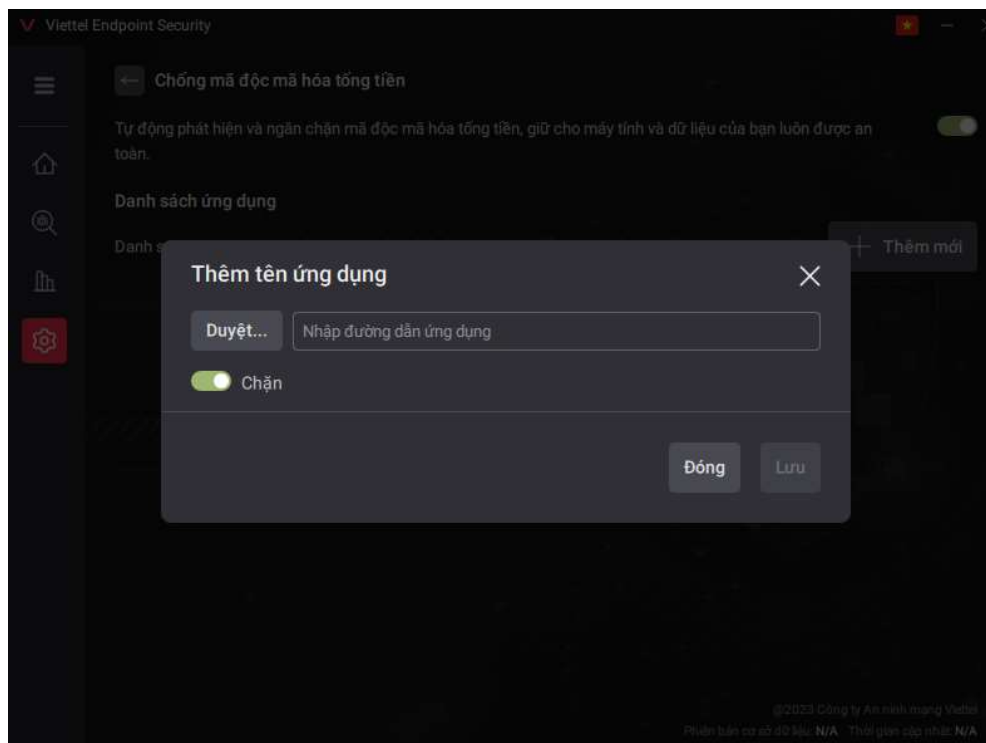
- Cho phép người dùng bật/tắt chế độ bảo vệ mã độc mã hóa tổng tiền. Hệ thống sẽ tự động phát hiện và ngăn chặn mã độc mã hóa tổng tiền cho máy tính.



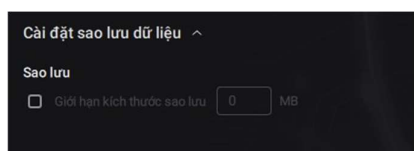
Lưu ý: Để sử dụng tính năng cần bật Policy AntiRansomware trên Portal



- 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



+ **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)./.