



Viettel Endpoint Detection & Protection (VCS-aJiant phiên bản EDP)

Phiên bản tài liệu: 4.133 – Ngày cập nhật: 03/12/2025

Tài liệu Hướng dẫn sử dụng



Lịch sử cập nhật

STT	Ngày cập nhật	Phiên bản	Lý do thay đổi	Ghi chú
1	...	3.3.0		
2	30/06/2022	3.3.20	Bổ sung/ cập nhật hướng dẫn: 3.4.8 IRFlow Response - 73 3.6 Response - 119 3.7.5 Update management - 174	
3	10/10/2022	3.3.31	Bổ sung/ cập nhật hướng dẫn: 3.11 Anti – Malware – 247	
4	16/12/2022	3.3.38	Bổ sung/ cập nhật hướng dẫn: 3.5.4 Investigation_Deploy tool - 116	
5	28/12/2022	3.3.43	Bổ sung/ cập nhật hướng dẫn 3.6.1 Response_Live response - 154	
6	21/03/2023	4.5.1	Bổ sung hướng dẫn bật 2FA	
7	20/04/2023	4.14.0	Cập nhật Agent Gui mới	
8	15/05/2023	4.18.0	Bổ sung hướng dẫn Device Control	
9	12/09/2023	4.48	- Bổ sung hướng dẫn Tính năng chống mã hóa mã độc tống tiền (Ransomware) - Update giao diện	
10	27/09/2023	4.52	Cập nhật chức năng 3.10.2 Endpoint Firewall	

STT	Ngày cập nhật	Phiên bản	Lý do thay đổi	Ghi chú
11	15/7/2024	4.52	Bổ sung làm rõ các rule BLS	
13	13/11/2024	4.100	Hướng dẫn sử dụng config Auto scan trong Policy	
14	17/12/2024	4.106	Hướng dẫn sử dụng tính năng Threat Hunting	
15	6/10/2025	4.110	Bổ sung cách tính license sản phẩm VCS-aJiant mục 3.7.1	
16	10/7/2025	4.115.0	Hướng dẫn sử dụng command line interface cho tính năng scan mã độc. Mục 3.17	
17	18/09/2025	4.128.0	Bổ sung mô tả luật kiểm tra vi phạm BLS Mục 3.5.2.3.1	
18	04/11/2025	4.130.0	Bổ sung mục 3.5.2 – Hướng dẫn sử dụng Isolate Devices Cập nhật mục 3.3.4 – Không hiển thị tính năng IR flow Cập nhật mục 3.4.2 – Không hiển thị tính năng Mark Artifacts	
19	04/11/2025	4.131.0	Bổ sung mô tả chức năng cách ly mã độc. Mục 3.14	
20	24/11/2025	4.132.0	Cập nhật giao diện màn Agent Management mục 3.6.1	
21	28/11/2025	4.133.0	Cập nhật mục 3.6.2 Policy Setting, thêm phần Performance control linux	

Mục lục

1. GIỚI THIỆU	10
1.1 Thực trạng hiện nay	10
1.2 Sự phát triển của công nghệ	10
1.3 VCS-aJiant	10
1.4 Các thông tin nâng cấp.....	11
2. TỔNG QUAN	11
2.1 Công nghệ	11
2.2 Kiến trúc hạ tầng	12
2.3 Làm việc với giao diện quản trị.....	13
3. HƯỚNG DẪN SỬ DỤNG	14
3.1 Đăng nhập	14
3.2 Dashboard VCS-aJiant.....	14
3.2.1 Thao tác với dữ liệu	16
Xuất dữ liệu.....	16
Tìm kiếm theo ngày	16
Làm mới dữ liệu.....	17
3.2.2 Thống kê Overview	17
3.2.3 Theo dõi Security Operation.....	23
3.2.4 Theo dõi Agent Monitoring	24
3.2.5 Theo dõi Risk Detection	26
3.3 Quản lý Alert.....	28
3.3.1 Tìm kiếm Alert	30

Tìm kiếm theo thời gian	30
Tìm kiếm nhanh	30
Tìm kiếm theo câu query	31
3.3.2 Danh sách Alert	33
3.3.3 Gom nhóm Alert	36
3.3.4 Xem chi tiết Alert	37
3.3.5 Biểu đồ điều tra (Enhance Alert)	40
Khu vực hiển thị biểu đồ và các thao tác trên biểu đồ	40
Khu vực hiển thị thông tin chi tiết	48
3.3.6 Cập nhật trạng thái không nguy hiểm hoặc đóng cảnh báo cho 01/nhiều Alert hoặc nhóm Alert	50
3.4 Nhóm chức năng Investigation	51
3.4.1 Process Analysis	52
3.4.2 Event Search	57
Tìm kiếm Event	57
Highlight	58
Need help	59
Wrap text	60
Export Data	61
3.4.3 Note	62
3.4.4 Deploy Tools	63
Tool Management	63
Deploy tool	64
Task management	78
3.5 Nhóm chức năng Response	102

3.5.1	Live Response.....	102
3.5.2	Isolate Devices	121
	Tạo lệnh Isolate devices (cô lập)	122
	Tạo lệnh Release isolation (bỏ cô lập)	124
	Kiểm tra thông tin cô lập/ bỏ cô lập thiết bị.....	125
	Xem danh sách lịch sử tác động theo thiết bị.....	126
3.6	Nhóm chức năng Setting.....	126
3.6.1	Agent Management	126
3.6.2	Policy Setting.....	137
3.6.3	Group Management	148
3.6.4	Account Management	157
	Permission management	158
	Role Management.....	159
	User management	165
3.6.5	Update management.....	172
	Update groups	172
	Update packages	176
3.7	Chức năng Baseline Policy (BLS)	181
3.7.1	Thống kê vi phạm (Violation statistic).....	181
	Màn hình Thống kê vi phạm	182
	Tab Loại vi phạm	185
	Tab Đơn vị	187
3.7.2	Thống kê phần mềm (Software statistic).....	188
3.8	Threat Hunting.....	191

3.8.1	Bật/tắt policy	191
3.8.2	Tìm kiếm theo agents/ nhóm	192
3.8.3	Tìm kiếm IOCs.....	193
	Các loại IOCs hỗ trợ	193
	Chi tiết kết quả tìm kiếm	195
3.8.4	Xem lịch sử truy vấn (View History)	199
	Xem danh sách truy vấn	199
	Xem chi tiết lịch sử truy vấn.....	200
3.9	Rules Correlation	201
3.9.1	Danh sách hiển thị.....	201
3.9.2	Thêm mới Rules Correlation	206
3.9.3	Sửa Rules Correlation.....	213
3.9.4	Xóa Rules Correlation	214
3.10	Protect & Prevention.....	215
3.10.1	Application Control	215
	Hiển thị danh sách các ứng dụng/tiến trình bị chặn	216
	Tìm kiếm ứng dụng/tiến trình bị chặn	216
	Thêm mới ứng dụng/tiến trình bị chặn	216
	Thêm mới ứng dụng/tiến trình từ tập tin có sẵn	217
	Xóa ứng dụng/tiến trình bị chặn trong danh sách.....	217
	Luồng cập nhật số lượng các máy agent đã cập nhật danh sách mới thành công	217
3.10.2	Endpoint Firewall.....	218
	Hiển thị danh sách các kết nối bị chặn	218
	Tìm kiếm các kết nối bị chặn	219

Thêm mới các kết nối bị chặn	219
Tạo bản sao chép từ điều kiện đã có	220
Thêm mới kết nối bị chặn từ tập tin có sẵn	221
Xóa kết nối bị chặn trong danh sách	221
Xuất dữ liệu các điều kiện.....	222
3.11 Anti – Malware	222
3.11.1 Scan Schedule	222
Tìm kiếm Scan Schedule task	222
Thêm mới Scan Schedule task.....	223
Nhân bản Schedule task.....	230
Xem chi tiết	231
Xóa Schedule task	232
Xem báo cáo	234
3.11.2 Device control.....	236
Tìm kiếm Group	237
Danh sách Device của từng group	239
Màn Exception	239
Màn Add Exception.....	241
3.12 Giao diện phía Agent GUI - Main	249
3.13 Giao diện phía Agent GUI - Protection.....	251
3.14 Giao diện phía Agent GUI - Report	255
3.15 Giao diện phía Agent GUI - Setting.....	258
3.16 Giao diện dòng lệnh của tính năng On-demand Scan	262
3.16.1 Sub-command scan	263

3.16.2	Sub-command report.....	264
3.16.3	Sub-command backup	266
3.16.4	Sub-command show.....	266

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:	

Thuật ngữ	Diễn giải	Ghi chú
	- Response Scenario - LiveResponse	
Timeline	Đường thời gian thể hiện các hoạt động trong: - Tạo/đóng phiên Process Analysis - Tạo/đóng phiên Live Response	

1. GIỚI THIỆU

1.1 Thực trạng hiện nay

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

1.2 Sự phát triển của công nghệ

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

1.3 VCS-aJiant

VCS-aJiant có khả năng cung cấp thông tin chi tiết về việc lây nhiễm phần mềm độc hại và các hành vi mở rộng phạm vi tấn công (lateral movement) của những kẻ

tấn công khi chúng thực hiện việc dò quét hoặc sử dụng thông tin bị đánh cắp trong mạng nội bộ đối với các hệ thống và ứng dụng.

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

1.4 Các thông tin nâng cấp

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

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

2. TỔNG QUAN

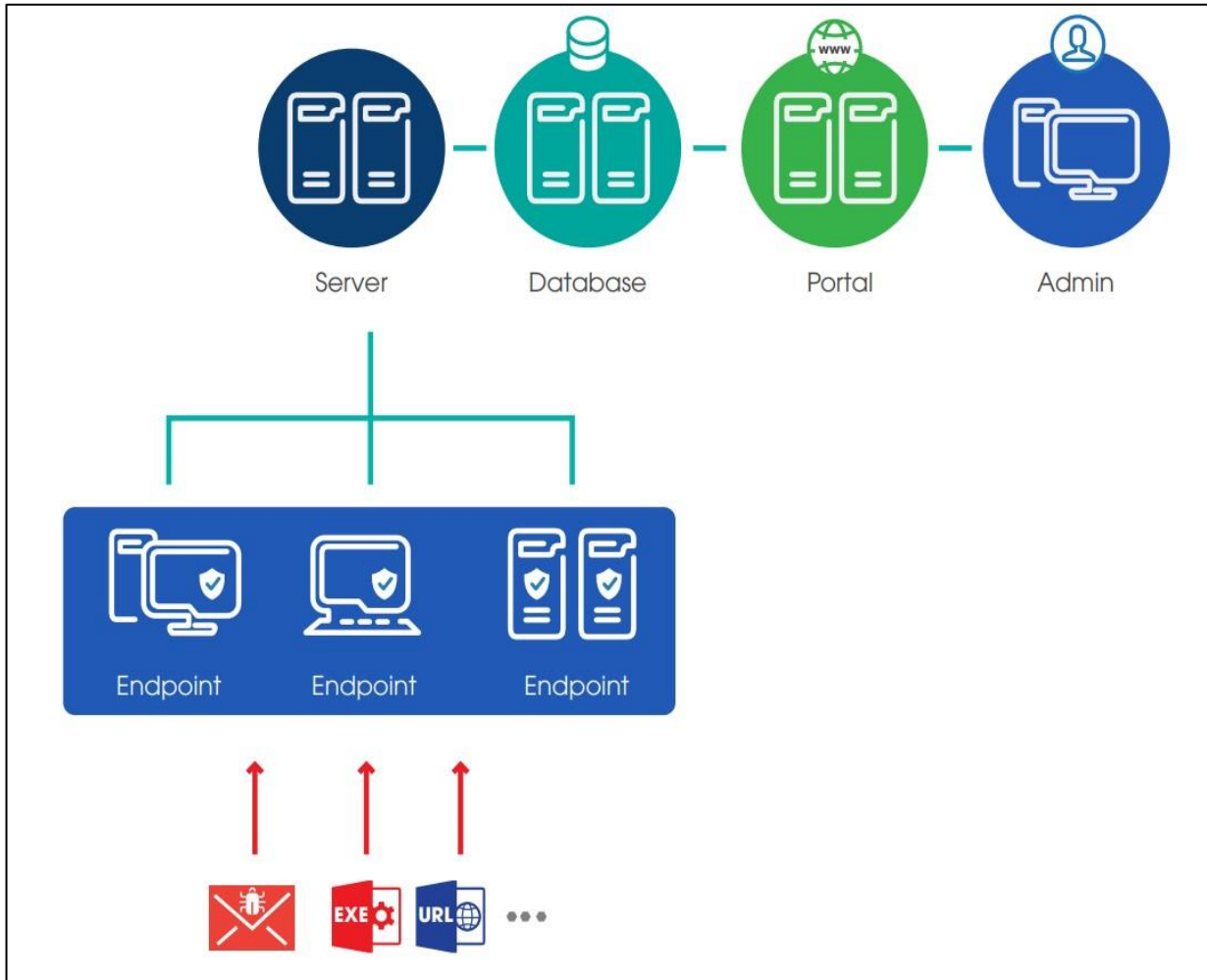
2.1 Công nghệ

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

Luồng nghiệp vụ điều tra tấn công được thiết kế khép kín theo kịch bản incident response, hỗ trợ phát hiện và phân tích các dấu 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;

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

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

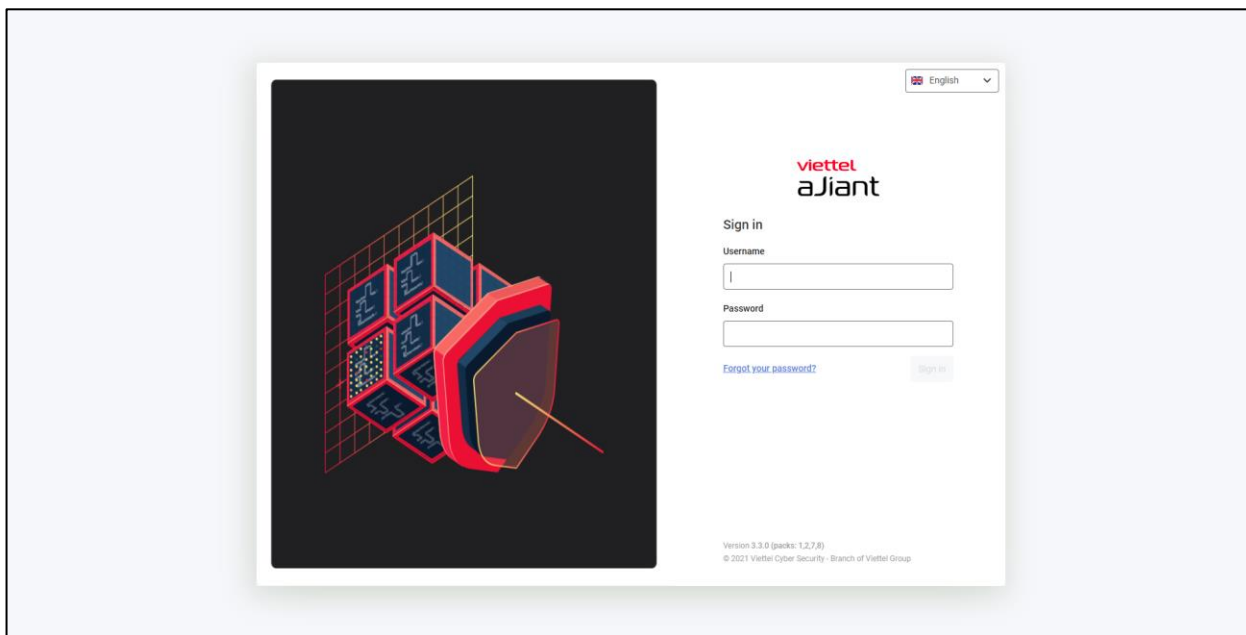
Protect & Prevention: danh sách các tính năng phòng chống và bảo vệ máy trạm (Application control và Endpoint firewall);

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

3. HƯỚNG DẪN SỬ DỤNG

3.1 Đăng nhập

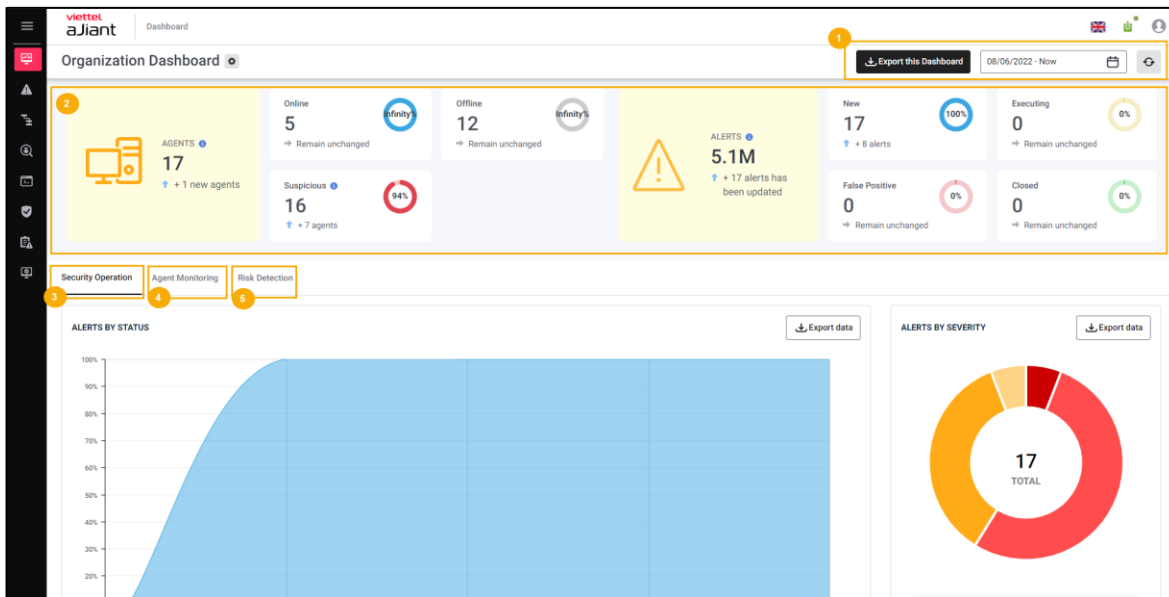
Bước 1: Truy cập vào hệ thống tại địa chỉ được cung cấp;



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

3.2 Dashboard VCS-aJiant

Các tính năng chính gồm có:



1 – Các thao tác với dữ liệu trên Dashboard:

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

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

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

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

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

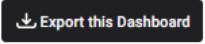
Phân quyền dữ liệu tại tính năng như sau:

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

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

3.2.1 Thao tác với dữ liệu

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;

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 	Last 90 days
Apply time range	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.

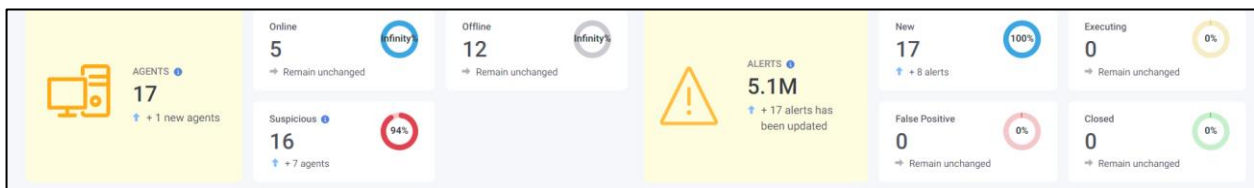
+ Sau khi chọn khoảng thời gian muốn theo dõi, chọn **Apply time range** để tải lại dữ liệu tương ứng.

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.

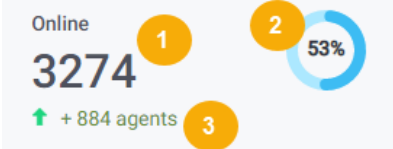
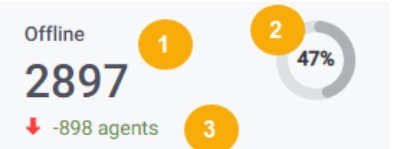
3.2.2 Thống kê Overview

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;



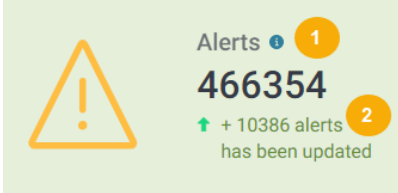
+ Thống kê liên quan đến agents:

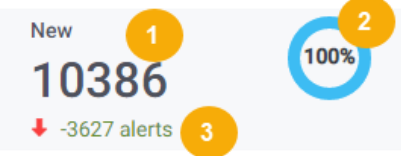
Số thống kê	Ý nghĩa
 AGENTS 17 + 1 new agents	Bao gồm 02 chỉ số: 1 – Tổng số máy đã cài đặt agent trên hệ thống (không phụ thuộc khoảng thời gian tìm kiếm); 2 – Số máy mới cài đặt agent;

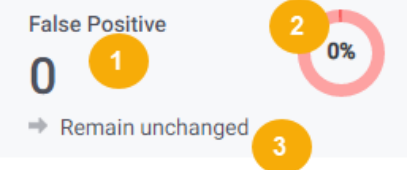
	2 – Tổng số máy mới cài đặt agent trong khoảng thời gian tìm kiếm; (+: Máy mới cài đặt, Remain unchanged: Không có máy mới cài đặt trong khoảng thời gian tìm kiếm)
	Bao gồm 03 chỉ số: 1 – Trung bình số máy Online trong khoảng thời gian tìm kiếm (chỉ tính thời gian làm việc trong giờ hành chính 08:00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

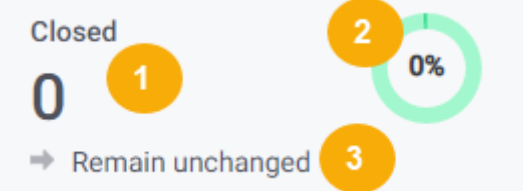
	(+: Số lượng máy Offline trung bình tăng so với giai đoạn trước, Remain unchanged: Không có chênh lệch)
	Bao gồm 03 chỉ số: 1 – Tổng số máy đã cài đặt agent trên hệ thống (không phụ thuộc khoảng thời gian tìm kiếm) có phát sinh Alert chưa được xử lý; 2 – Tỷ lệ máy có phát sinh Alert so với số lượng máy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

+ Thống kê liên quan đến Alerts:

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

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

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

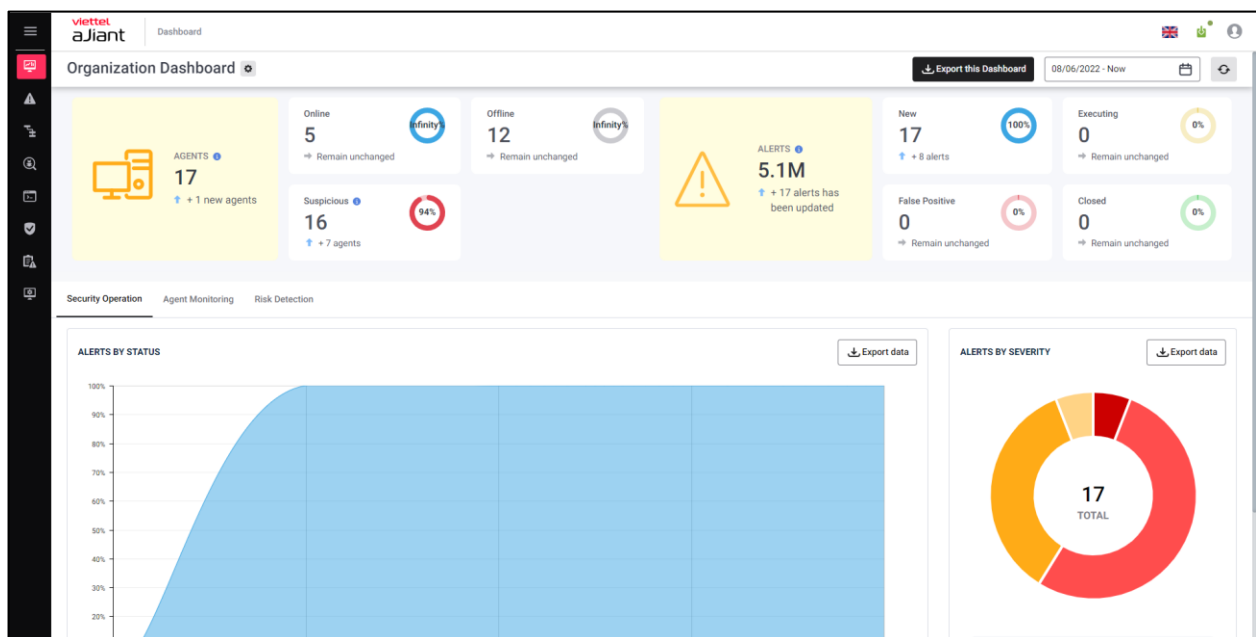
	phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm; 3 – Tổng số Alert mới phát sinh hoặc được cập nhật trong khoảng thời gian tìm kiếm và đang ở trạng thái = CLOSED chênh lệch so với chu kỳ trước. (+: Tổng số Alert tăng so với giai đoạn trước, Remain unchanged: Tổng số Alert không thay đổi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

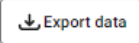
	(+: Tổng số Alert tăng so với giai đoạn trước, Remain unchanged: Tổng số Alert không thay đổi so với giai đoạn trước)
--	--

3.2.3 Theo dõi Security Operation

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

- + Thống kê tình trạng xử lý Alert theo trạng thái;
- + Thống kê Alert theo mức độ nguy hại;
- + Trích xuất dữ liệu tương ứng trong các biểu đồ;



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



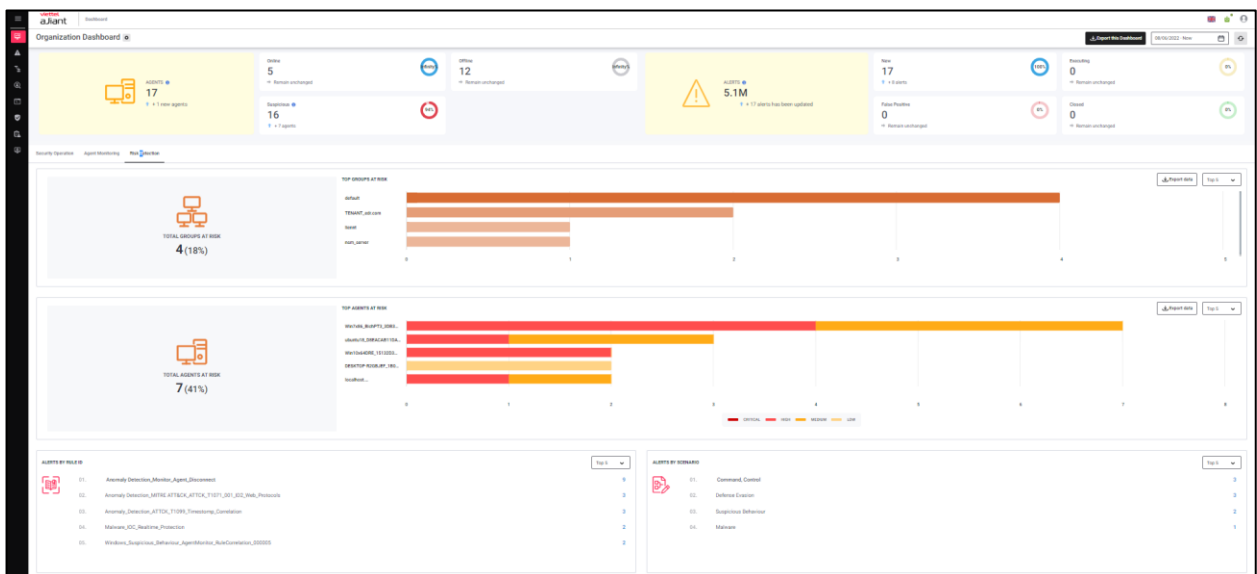
<i>Biểu đồ/thống kê</i>	<i>Ý nghĩa</i>
Agent by status	Biểu đồ miền- Theo dõi tình hình ghi nhận máy theo trạng thái (Online/Offline) trong chu kỳ báo cáo tính đến thời điểm hiện tại, bao gồm: Trục y: Tỷ lệ máy phân chia theo 02 nhóm status (Online, Offline); Trục x: thời gian thống kê; Hiển thị số lượng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

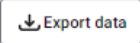
	Cho phép chọn Export data để tải về danh sách máy sắp xếp theo thông tin hệ điều hành.
Agent by OS version	Thống kê top phiên bản hệ điều hành cài đặt trên máy nhiều nhất; Cho phép thay đổi khoảng thống kê: Top 5, Top 10, Top 20, Top 50. Mặc định chọn Top 5.

3.2.5 Theo dõi Risk Detection

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

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



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

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

3.3 Quản lý Alert

Các tính năng chính gồm có:

SEVERITY	Critical	High	Medium	Low	No impact	STATUS	New	In progress	False positive	Closed
	0	176	19.5k	5.4k	0		25k	1	2	1

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

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

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

- + Tìm kiếm dữ liệu theo thời gian.

2 – Tìm kiếm nhanh;

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

- + Xem danh sách Alert;
- + Gom nhóm Alert;
- + Xem tóm tắt Alert;
- + Xem chi tiết 01 Alert;
- + Xem biểu đồ điều tra (Investigation Graph);
- + Đánh dấu không nguy hiểm (Set False Positive) cho 01/nhiều Alert;

Phân quyền dữ liệu tại tính năng như sau:

- + User đăng nhập thuộc group root: Hiện 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;

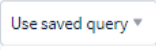
Tìm kiếm theo câu query



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

2 – Nhập câu query để tìm kiếm;

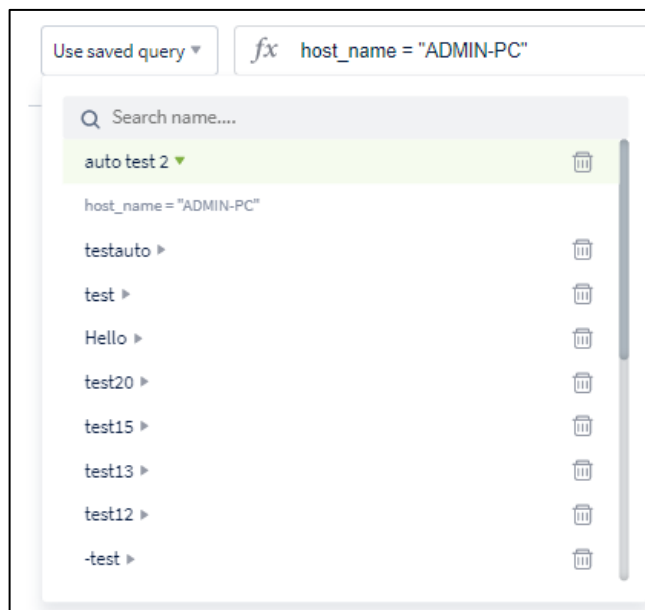
(*) Sử dụng câu query đã lưu trước đó để tìm kiếm

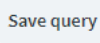
Bước 1: Chọn query đã lưu trước đó tại combobox  ;

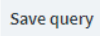
Bước 2: Xem lại nội dung câu query trước khi chọn bằng cách chọn  ;

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
- 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 gọi 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

Host name	Severity	Alert id	Status	Ajant event id	Agent id	Timestamp create	Target commandline	Hash sha1	Description	Action
ubuntu18	HIGH	20220609_173832_553078267_618098...	New	500	D8EACAB11DA9DA3F0F65575E9E9C313DC61A83B	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 loc	

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

Selected

☒ Target commandline
☒ Alert id
☒ Agent id
☒ Severity
☒ Description

☒ Hash sha1
☒ Host name
☒ Timestamp create
☒ Status
☒ Ajiant event id

Others

☐ File hash sha1
☐ Malware type
☐ Classify
☐ Ir flow name

☐ Scan result
☐ Malware name
☐ Assignee
☐ 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										
☐	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	D8EACAB11DA9F0A3F0F6557SE9EC313DC61A83B	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 !\[\]\(d84e7ea36f695d92cb39ec32c307ac93_img.jpg\) 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

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

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	D8EACAB11DA9FA3F0F65575E9EC313DC61A83B	New	500	20220609_173832_553078267_618098	09/06/2022 17:38:31	N/A	N/A	Computer ubun	
localhost.localdo main	HIGH	31F6FA372944D72C2DC85AE155A63170CE9686AD	New	500	20220609_113824_267803584_564214	09/06/2022 11:38:23	N/A	N/A	Computer loca	

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

Update status to:

False Positive

Comment

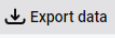
Write something...

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;

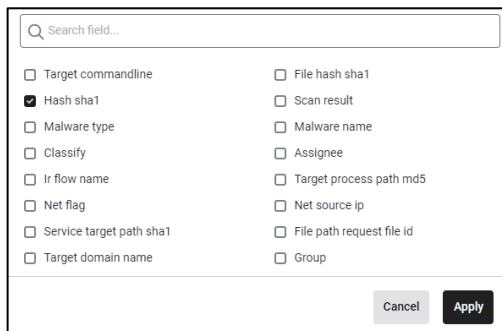
Lưu ý: Thao tác này chỉ áp dụng khi toàn bộ Alert được chọn đều ở trạng thái = “NEW”, nếu có ít nhất một Alert đang ở trạng thái khác “NEW”, thao tác sẽ bị ẩn đi . Chi tiết xem trong trường hợp đánh dấu không nguy hiểm 01 Alert trong [3.3.5 Đánh dấu không nguy hiểm cho 01/nhiều Alert hoặc nhóm Alert](#)

+ 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  để lựa chọn các tiêu chí muốn sử dụng làm tiêu chí gom nhóm Alert;



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

Bước 2: Chọn  để áp dụng.

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

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 ajsant_event_id: N/A	189	
target_commandline: N/A ajsant_event_id: 3	7	
target_commandline: N/A ajsant_event_id: 11	155	
target_commandline: N/A ajsant_event_id: 13	2	
target_commandline: N/A ajsant_event_id: 23	1	
target_commandline: N/A ajsant_event_id: 400	1	
target_commandline: N/A ajsant_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”;

Selected

☐ Target commandline
 ☐ Ajiant 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

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;

NEW

HIGH

20220609_173832_553078267_618098

2

Add to IRFlow

Related events

Enhance Alert

Update status

×

GROUP

default

HOST NAME

ubuntu18

1

Detail

Raw data

Description

Computer ubuntu18 was disconnected at least 30 days

Rule ID

Anomaly_Detection_Monitor_Agent_Disconnect

Source event logs

This section defines source event list of this alert, which creates and contains more context information for this alert.

1 result(s)

SystemTimeStamp	Event ID	Description
09/06/2022 17:38:30	500	Agent was disconnected

Show columns

Advanced

Host

This information is about suspicious host.

Client id

D8EACAB11DA9F0A3F0F65575E9E9C313DC61A83B

Hostname

ubuntu18

Network Connection

This information is about suspicious network connection.

MAC

00:0c:29:fb:19:eb

Others

These other information provides more context about this alert collected by VCS-aJiant.

Create time

09/06/2022 17:38:30

Log provider name

AdvanceCollector

Source log

mixed

Sub category

Monitor

Description

Computer ubuntu18 was disconnected at least 30 days

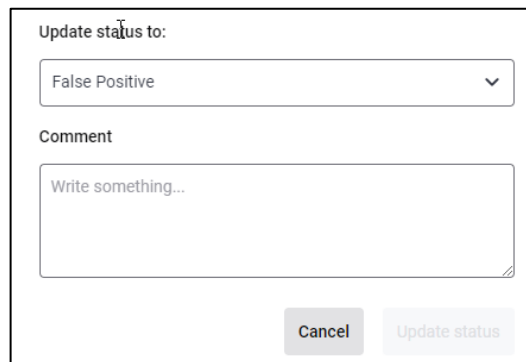
1 – Nhóm thông tin chung của Alert, trong đó:

2 –

- + Status: Hiển thị trạng thái của Alert (New, In Progress, False Positive, Closed);
- + Severity: Phân loại Alert theo mức độ nguy hại (Critical, High, Medium, Low);
- + Alert_id: Hiển thị thông tin id của Alert;
- + First seen: Thời gian Alert được tạo;
- + Last seen: Thời gian gần nhất Alert được cập nhật;

3 – Nhóm các thao tác với Alert

- + [Chọn](#)  để cập nhật trạng thái của Alert:



The dialog box titled "Update status to:" contains a dropdown menu with "False Positive" selected. Below it is a "Comment" section with a text area containing the placeholder "Write something...". At the bottom right are two buttons: "Cancel" and "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

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

● In progress

khaib 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

4 – Tab các thông tin liên quan đến Alert:

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

Detail

Raw data

Description

Detect attack technique T1562.004: Disable or Modify System Firewall on ANM-PHUCVD2. Process with path = C:\program files\del\supportassistent\bin\supportassistent.exe (PID = 7656, commandline = "C:\Program Files\Del\SupportAssistAgent\bin\SupportAssistAgent.exe") is creating child process with path = C:\windows\system32\netsh.exe (commandline = "netsh.exe" http delete sslcert ipport=0.0.0.0:5700, PID = 9732) to the disable firewall.

Rule ID [Anomaly_Detection_ATTCK_T1562_004_Disa...](#)

Source event logs

No tracked events!

Advanced

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\del\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\Del\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\del\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,2a:6b:ad:71:14:2b,00:50:56:c0:00:01,00:50:56:c0:00:08,48:4d:7e:ba:be:53

Others

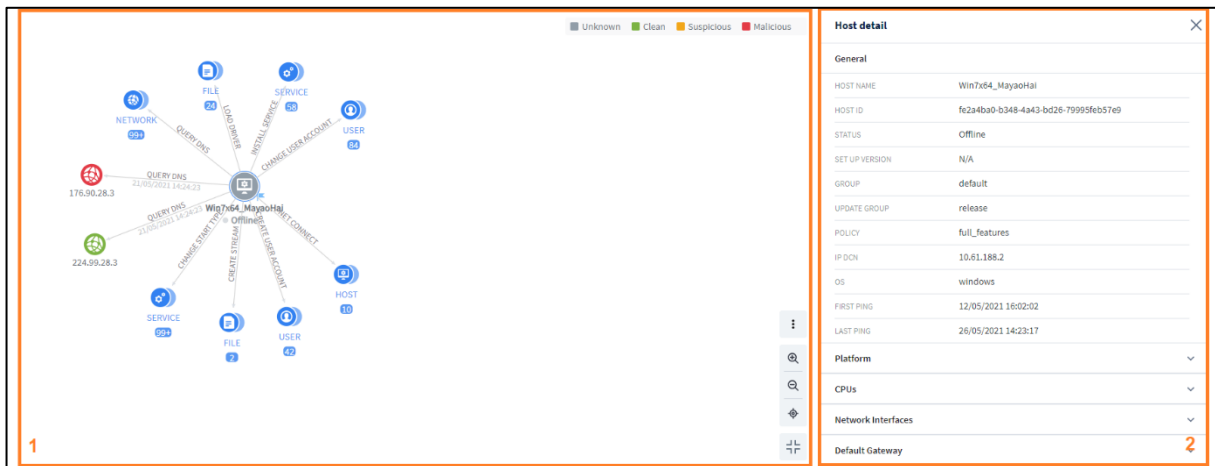
These other information provides more context about this alert collected by VCS-aJiant.

- Khung thông tin (1) Description: Cho phép hiển thị thông tin mô tả chi tiết Alert và RuleID;
- Khung thông tin (2):
 - Source event logs: Ghi lại Source event logs liên quan đến Alert (nếu có);

- Advance: Thông tin nâng cao liên quan đến Alert bao gồm: File, Process, Host, Others, ...

3.3.5 Biểu đồ điều tra (Enhance Alert)

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

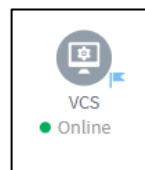


- 1 – Khu vực hiển thị biểu đồ và các thao tác trên biểu đồ
- 2 – Khu vực hiển thị thông tin chi tiết các đối tượng trên biểu đồ

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

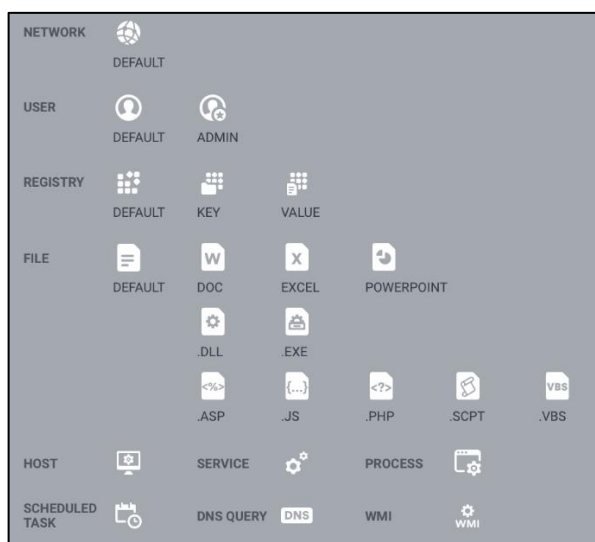
Cho phép hiển thị trực quan các đối tượng trong Alert phục vụ xem thông tin và điều tra;

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 cấm 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

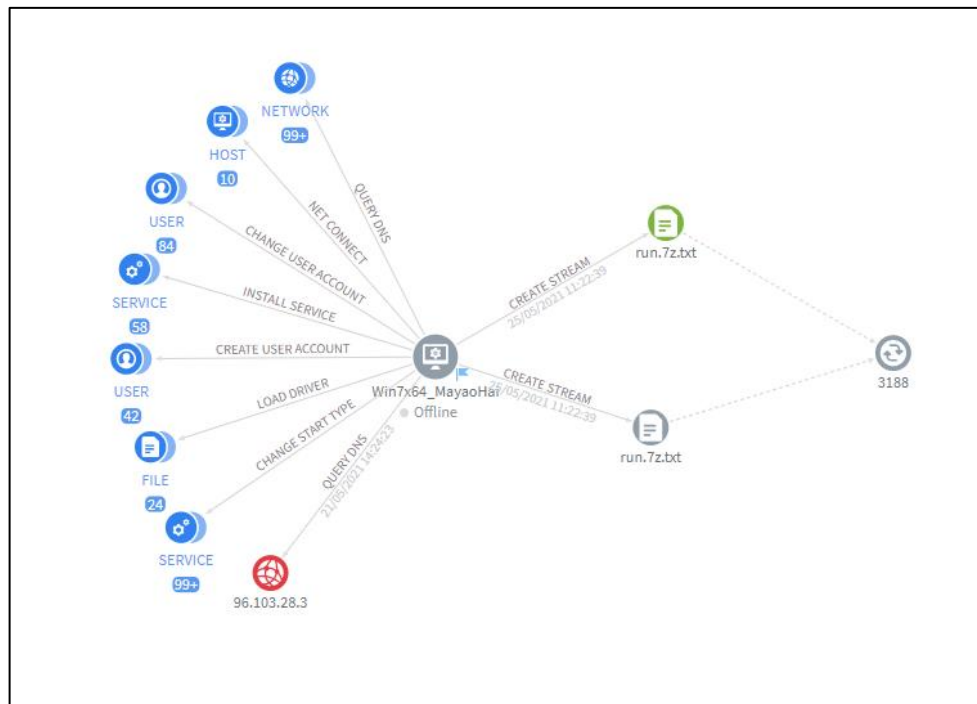
mũi tên nối liền 02 đối tượng)



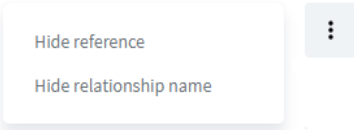
+ Reference: Mối quan hệ tham chiếu, là các đối tượng khác ghi nhận được trong sự kiện chính phát sinh ra đối tượng (được thể hiện bởi nét đứt và không có tên quan hệ cụ thể)



Ví dụ:

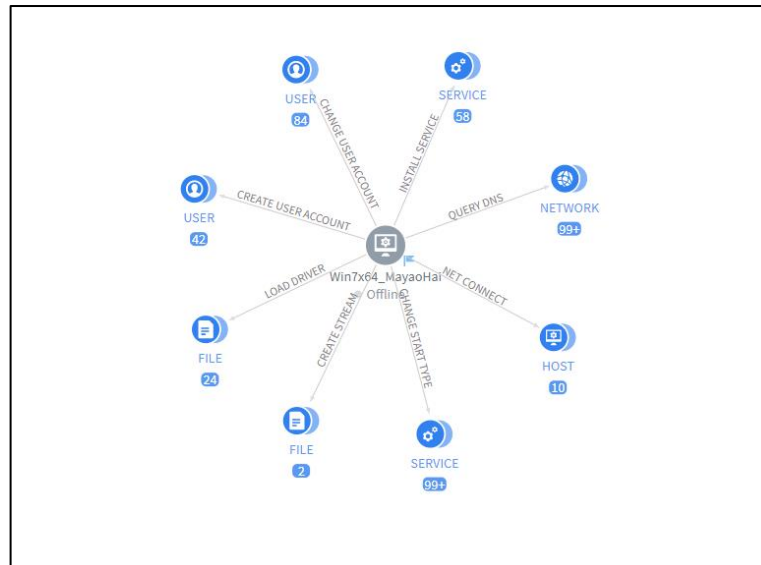


Các thao tác hỗ trợ hiển thị biểu đồ bao gồm:

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

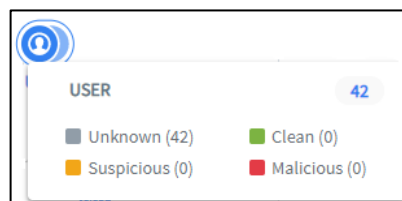
	Cho phép quay lại vị trí trung tâm của biểu đồ (máy gốc)
	Cho phép mở rộng màn hình tối đa để xem biểu đồ và thao tác trên biểu đồ

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) View column

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

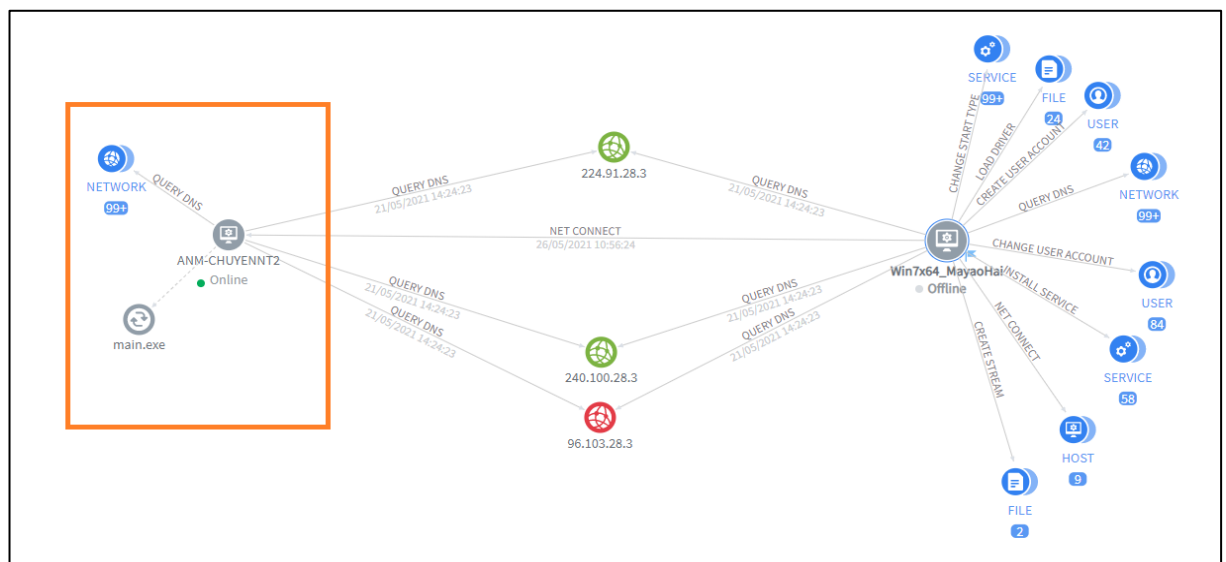
	STATUS	DOMAIN ADDRESS	IP	LOCAL PORT	PROCESS NAME	ACTION
☒	Clean	ocsp.verisign.com	240.100.28.3	N/A	SYSTEM	
☐	Clean	crf4.digicert.com	80.105.28.3	N/A	SYSTEM	
☐	Clean	crf4.microsoft.com	16.87.28.3	N/A	SYSTEM	
☐	Malicious	www.microsoft.com	96.103.28.3	N/A	SYSTEM	
☐	Clean	ocsp.digicert.com	240.94.28.3	N/A	SYSTEM	
☐	Clean	crf4.verisign.com	224.91.28.3	N/A	SYSTEM	
☐	Malicious	www.msftncsi.com	0.96.28.3	N/A	SYSTEM	
☐	Clean	csc3-2010-crf4.verisign.com	112.89.28.3	N/A	SYSTEM	
☐	Clean	ocsp.globalsign.com	48.88.28.3	N/A	SYSTEM	
☐	Clean	crf4.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;

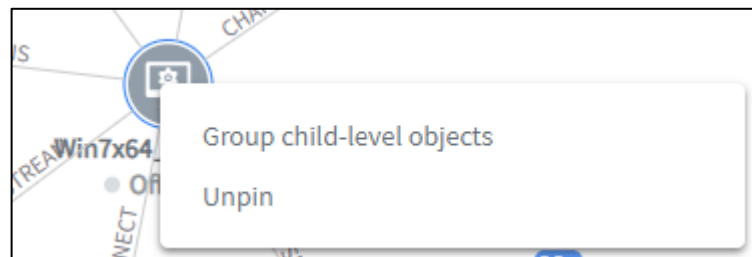
+ Khi đã chọn được đối tượng phù hợp, chọn để hiển thị 01 đối tượng lên biểu đồ hoặc chọn Show on graph để chọn tối đa 20 đối tượng lên biểu đồ;

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

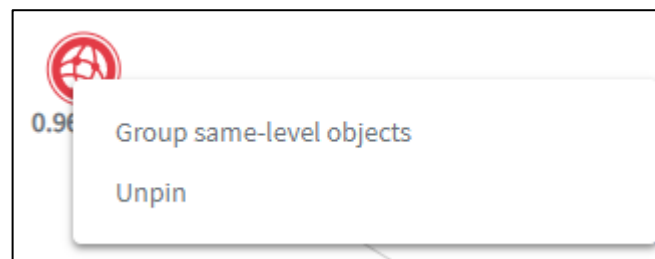


Bước 2: Sau khi đã hiển thị các đối tượng cần điều tra trên biểu đồ, các thao tác hỗ trợ mở rộng/thu gọn bao gồm:

+ 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”;

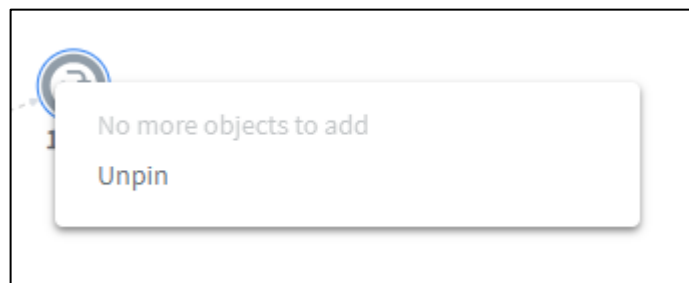


+ Tại các đối tượng khác: Hỗ trợ thu gọn bằng cách nhóm lại theo loại đối tượng và loại quan hệ với các đối tượng cùng cấp bằng cách chọn chuột phải tại đối tượng, sau đó chọn “Group same-level objects”;

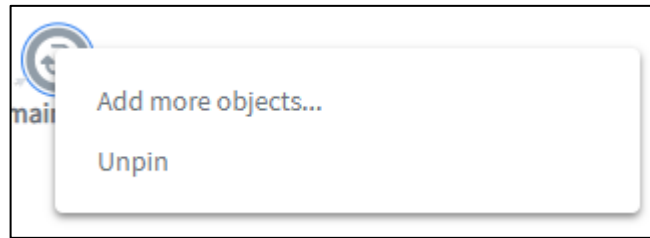


+ Tại đối tượng là tiến trình (process) cho phép mở rộng để điều tra loang bằng cách chọn chuột phải tại đối tượng,

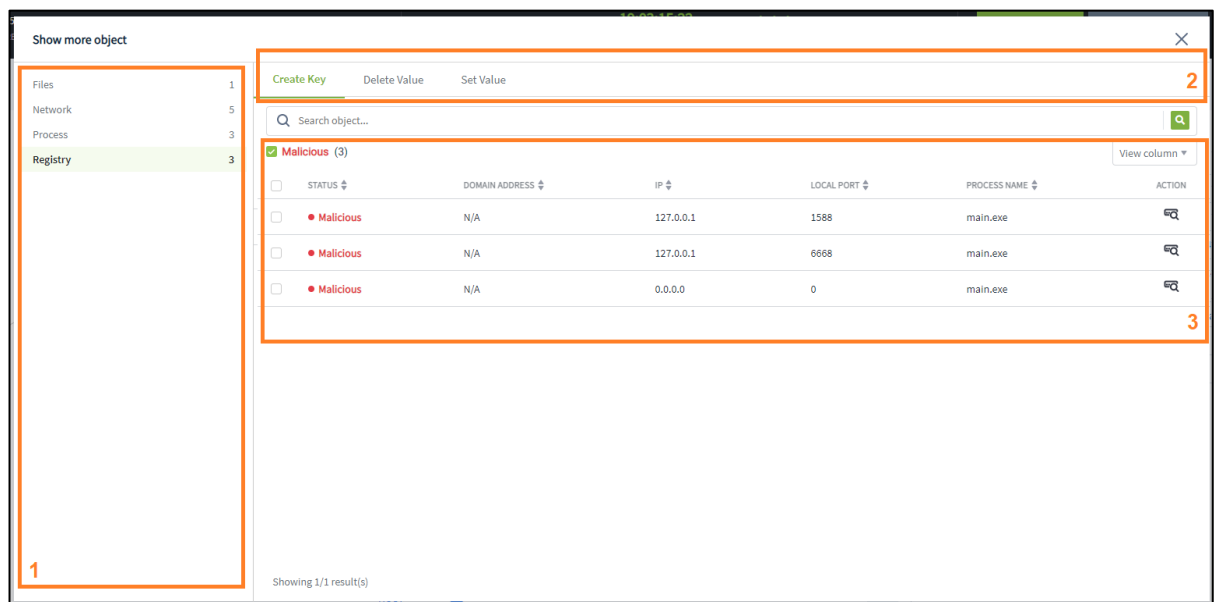
+ Trường hợp không thể tiếp tục loang, hiển thị:



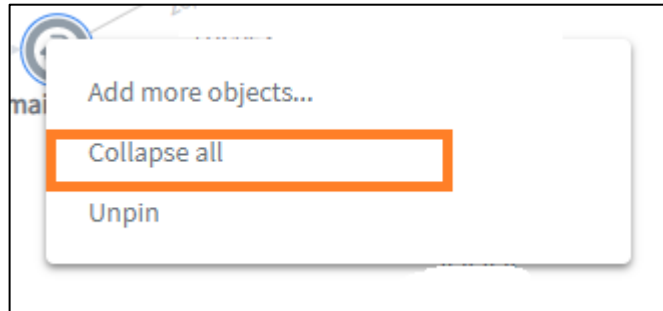
+ Trường hợp có thể loang, chọn “Add more objects...”



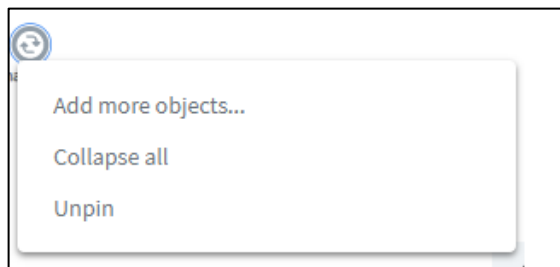
Hiện thị giao diện cho phép chọn đối tượng muốn loang đến



- 1 – Chọn loại đối tượng;
- 2 – Chọn loại quan hệ từ tiến trình tới đối tượng;
- 3 – Chọn trực tiếp đối tượng muốn hiển thị. Hỗ trợ tìm kiếm theo trạng thái độc/sạch của đối tượng hoặc tìm kiếm theo nội dung có tại các trường thông tin của đối tượng.
 - + Chọn View column để lựa chọn các trường thông tin hiển thị hoặc dùng tính năng ↑ để sắp xếp thông tin trong danh sách
 - + Khi đã chọn được đối tượng phù hợp, chọn 🔍 để hiển thị 01 đối tượng lên biểu đồ hoặc chọn Show on graph để chọn tối đa 20 đối tượng lên biểu đồ;
 - + Tại đối tượng là tiến trình (process), khi có các đối tượng đang được mở rộng cho phép thu gọn lại bằng cách chọn chuột phải tại đối tượng;



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



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	

1

Platform

CPUs

Network Interfaces

Default Gateway

2

- 1 – Nhóm thông tin chung: Bao gồm các thông tin chung/thông tin định danh của đối tượng, mặc định luôn hiển thị khi vừa truy cập;
 - 2 – Nhóm thông tin chi tiết: Bao gồm các thông tin chi tiết của đối tượng, được phân thành các nhóm thông tin khác nhau, mặc định các nhóm thông tin này sẽ được đóng lại, chọn  để mở rộng và hiển thị nhóm thông tin.
- + Thao tác  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	
SHA26	1941d3f261033344b22c5e9cf246e5683c17d450ac87d0af6f3ed7a52f431bb6	
PROCESS PATH	C:\users\admin\desktop\taodataloang\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:

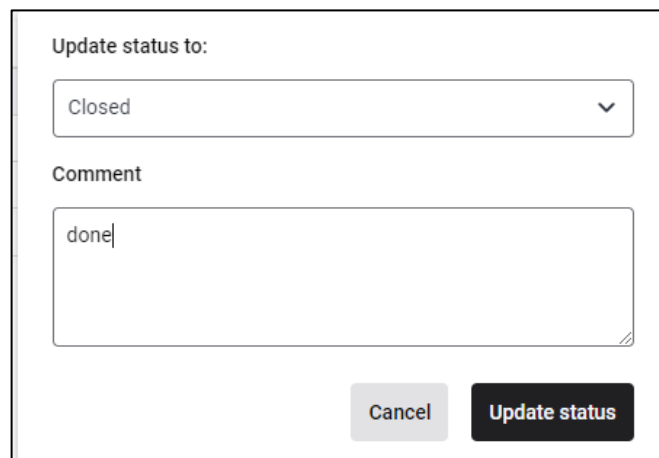
- Chọn “ Update status” để xác nhận đánh dấu không nguy hiểm cho Alert;

- 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:

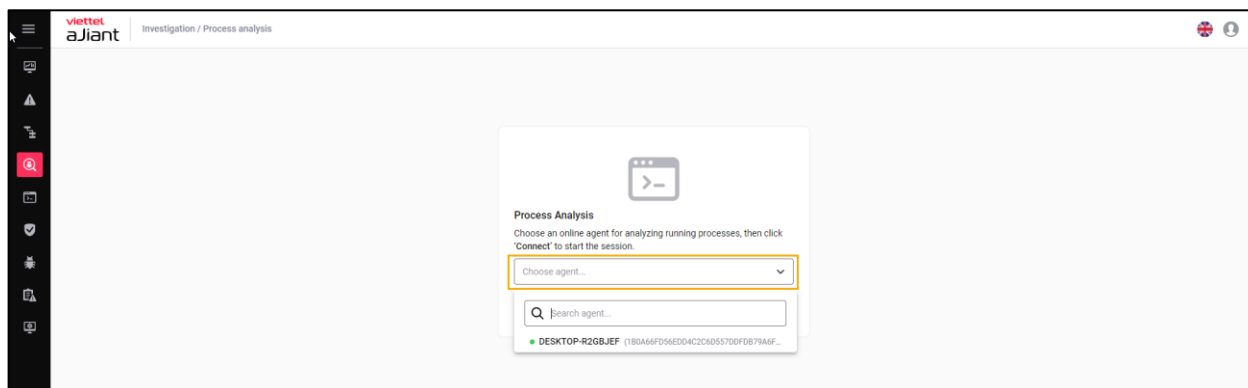
- Chọn “ Update status” để xác nhận đóng Alert;
- Chọn “Cancel” để xác nhận hủy thao tác đóng Alert;

3.4 Nhóm chức năng Investigation

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

3.4.1 Process Analysis

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



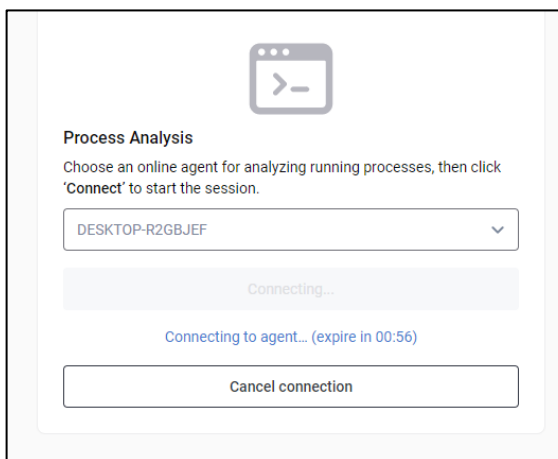
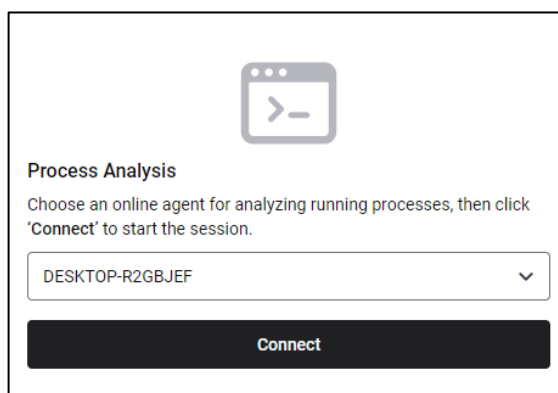
Danh sách máy người dùng:

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

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

Investigation / Process analysis

HOST NAME: DESKTOP-R20BJEF (180A66FD56EDD4C2C0855700F0B79A6F5046FCC0) | CONNECTED TIME: 21/06/2022 11:45:40 | DURATION: 00:00:18 | STATUS: Running | Change agent | Stop connect

Search: Type to search... | Refresh

118 result(s) | Last updated: 21/06/2022 11:45:57

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	
vm3dservice.exe	5520	C:\Windows\System32\vm3dservice.exe	test	"C:\Windows\System32\vm3dservice.exe" -u	VMware, Inc.	
vmtoolsd.exe	5956	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	test	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vm- 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=go-pro...	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-url=...	Microsoft Corporation	
Code.exe	5008	C:\Program Files\Microsoft VS Code\Code.exe	test	"C:\Program Files\Microsoft VS Code\Code.exe" -no-lazy-insp...	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"	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	

Show verified signature ☐ | View all artifacts (0) | Filter by signature | Show columns

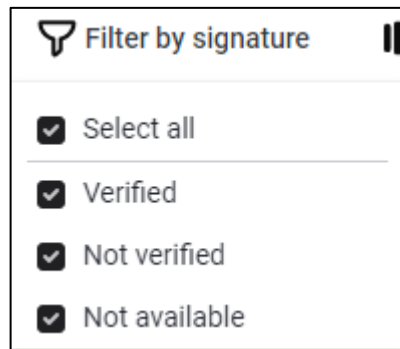
Trong đó giao diện chia làm các nhóm thông tin:

- 1 – Nhóm thông tin liên quan đến kết nối, bao gồm: Máy đang kết nối, thời gian tạo kết nối, thời lượng kết nối tính đến hiện tại, trạng thái kết nối
- 2 – Nhóm thông tin hỗ trợ tìm kiếm/làm mới và lọc dữ liệu tại danh sách, bao gồm các thao tác:

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

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

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



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

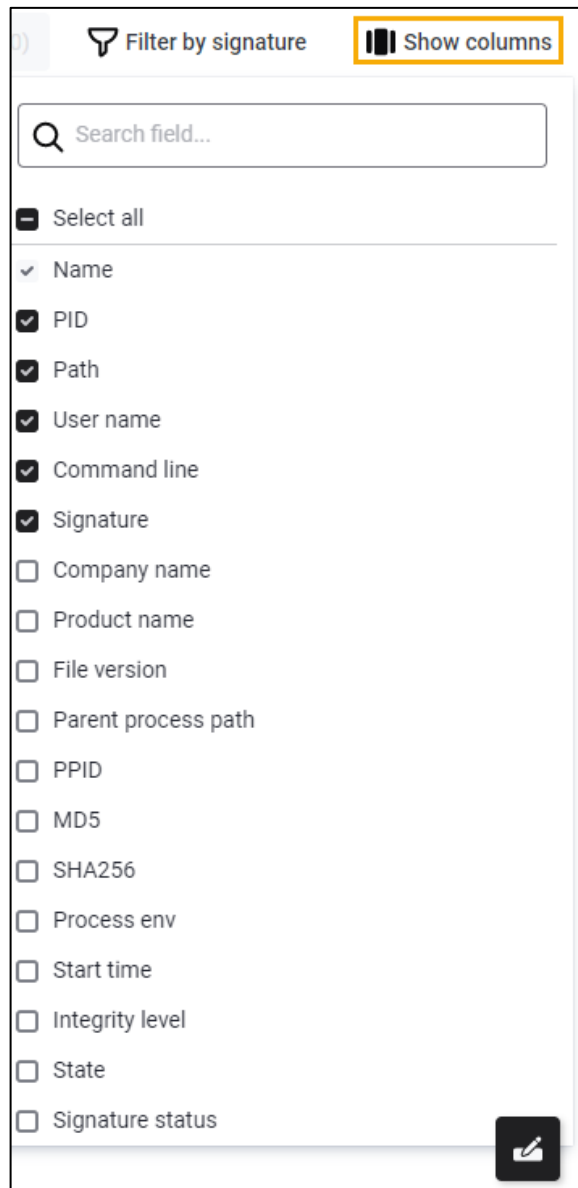
Type to search...							
116 result(s) Last updated: 21/06/2022 11:50:01							
Name	PID	Path	User name	Command line	Signature	Action	
svchost.exe	3360	C:\Windows\System32\svchost.exe	test	C:\Windows\system32\svchost.exe -k UnistackSvcGroup	Microsoft Windows Publisher		
svchost.exe	3680	C:\Windows\System32\svchost.exe	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		
▼ VESSvc.exe	14380	C:\Program Files\Ajan\VESSvc.exe	SYSTEM	"C:\Program Files\Ajan\VESSvc.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\autoscanner\VESAutoScan.exe	SYSTEM	"C:\Program Files\Ajan\autoscanner\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;

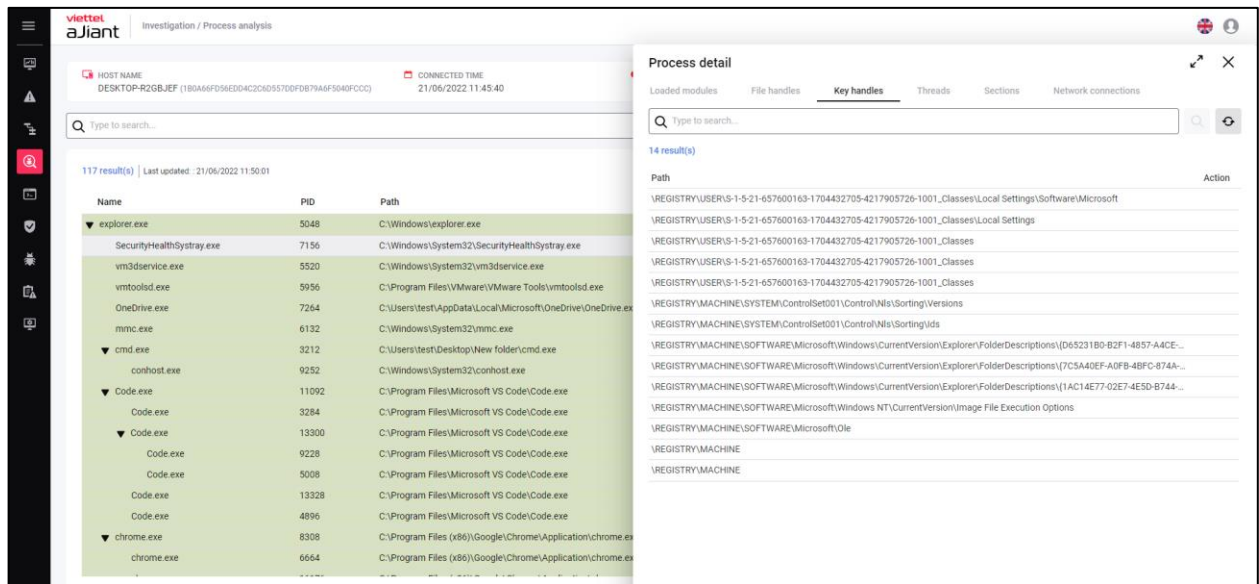
Show columns ▼

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

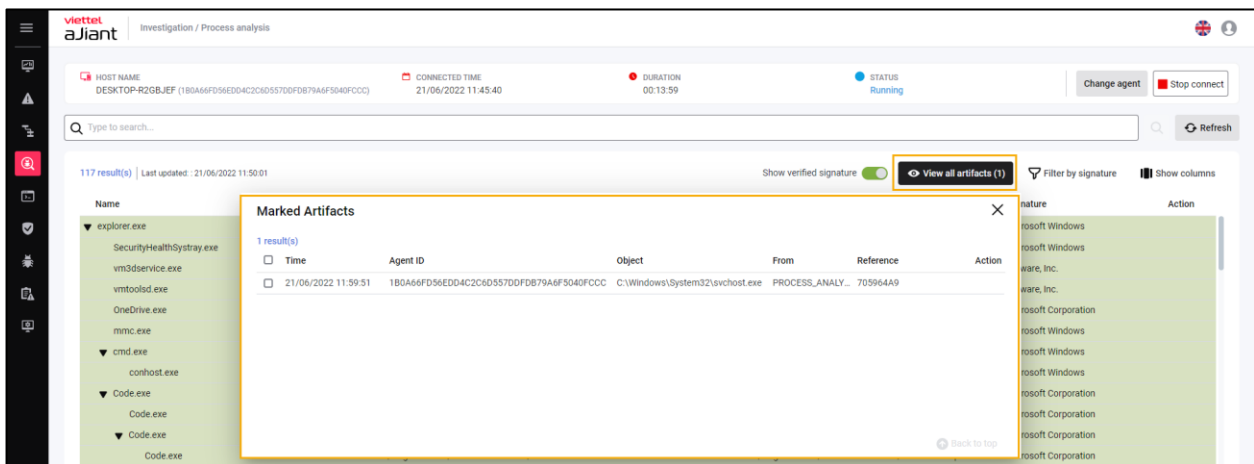
Trên danh sách ngoài trường "Name" luôn hiển thị cố định, các trường còn lại đều có thể tùy chọn hiển thị hoặc không hiển thị.



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



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



3.4.2 Event Search

Tìm kiếm Event

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

The screenshot shows the Splunk Enterprise interface. At the top, there is a navigation bar with icons for Search, Settings, Data, and Tools. Below this is a search bar with the query 'SELECT * FROM ...'. The main content area displays a table of search results. The table has columns for EventID, Computer, Location, EventType, and TimeStamp. The results are filtered by the query 'SELECT * FROM ...' and show a list of events with their corresponding timestamps and computer names.

EventID	Computer	Location	EventType	TimeStamp
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 14:22:34	27/06/2022 14:22:34
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 14:18:36	27/06/2022 14:18:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 14:13:36	27/06/2022 14:13:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 14:08:36	27/06/2022 14:08:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 14:03:36	27/06/2022 14:03:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 13:58:36	27/06/2022 13:58:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 13:53:36	27/06/2022 13:53:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 13:48:36	27/06/2022 13:48:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 13:43:36	27/06/2022 13:43:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 13:38:36	27/06/2022 13:38:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 13:33:36	27/06/2022 13:33:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 13:28:36	27/06/2022 13:28:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 13:23:36	27/06/2022 13:23:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 13:18:36	27/06/2022 13:18:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 13:13:36	27/06/2022 13:13:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 13:08:36	27/06/2022 13:08:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 13:03:36	27/06/2022 13:03:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 12:58:36	27/06/2022 12:58:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 12:53:36	27/06/2022 12:53:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 12:48:36	27/06/2022 12:48:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 12:43:36	27/06/2022 12:43:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 12:38:36	27/06/2022 12:38:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 12:33:36	27/06/2022 12:33:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 12:28:36	27/06/2022 12:28:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 12:23:36	27/06/2022 12:23:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 12:18:36	27/06/2022 12:18:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 12:13:36	27/06/2022 12:13:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 12:08:36	27/06/2022 12:08:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 12:03:36	27/06/2022 12:03:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 11:58:36	27/06/2022 11:58:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 11:53:36	27/06/2022 11:53:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 11:48:36	27/06/2022 11:48:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 11:43:36	27/06/2022 11:43:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 11:38:36	27/06/2022 11:38:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 11:33:36	27/06/2022 11:33:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 11:28:36	27/06/2022 11:28:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 11:23:36	27/06/2022 11:23:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 11:18:36	27/06/2022 11:18:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 11:13:36	27/06/2022 11:13:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 11:08:36	27/06/2022 11:08:36
130.031	DESKTOP-HQKJLBY	EventLog	27/06/2022 11:03:36	27/06/2022 11:03:36
130.031	DESKTOP-HQKJLBY	EventLog</		

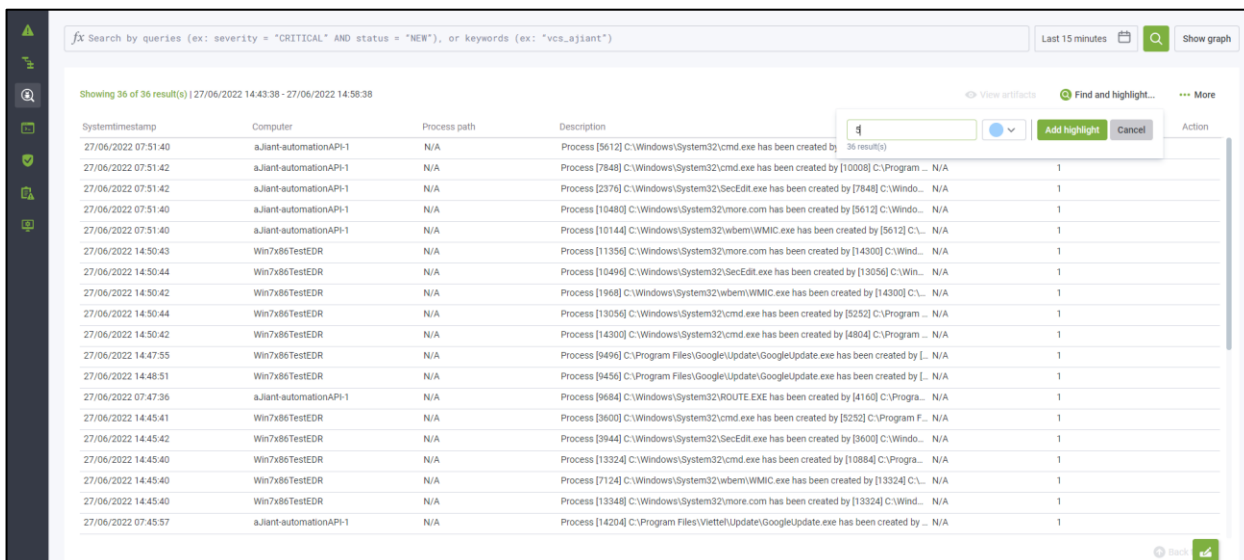
Mục đích: Cho phép thêm 01 hoặc nhiều highlight để rà soát đồng thời tại một thời điểm (không giới hạn số lượng tối đa), khi thực hiện search hoặc sort thì mọi highlight đã tạo sẽ bị clear;

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

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

Viettel Cyber Security

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



Need help

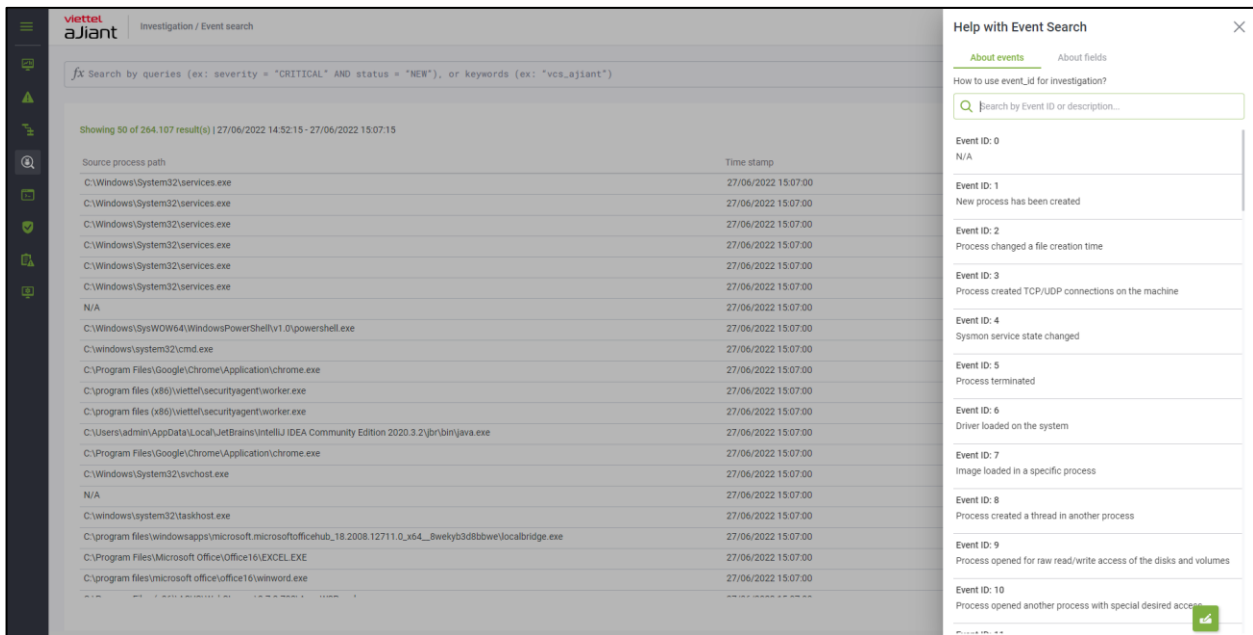
- Mục đích: tra thông tin event, ý nghĩa trường;
- Các bước thực hiện:

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.



Wrap text

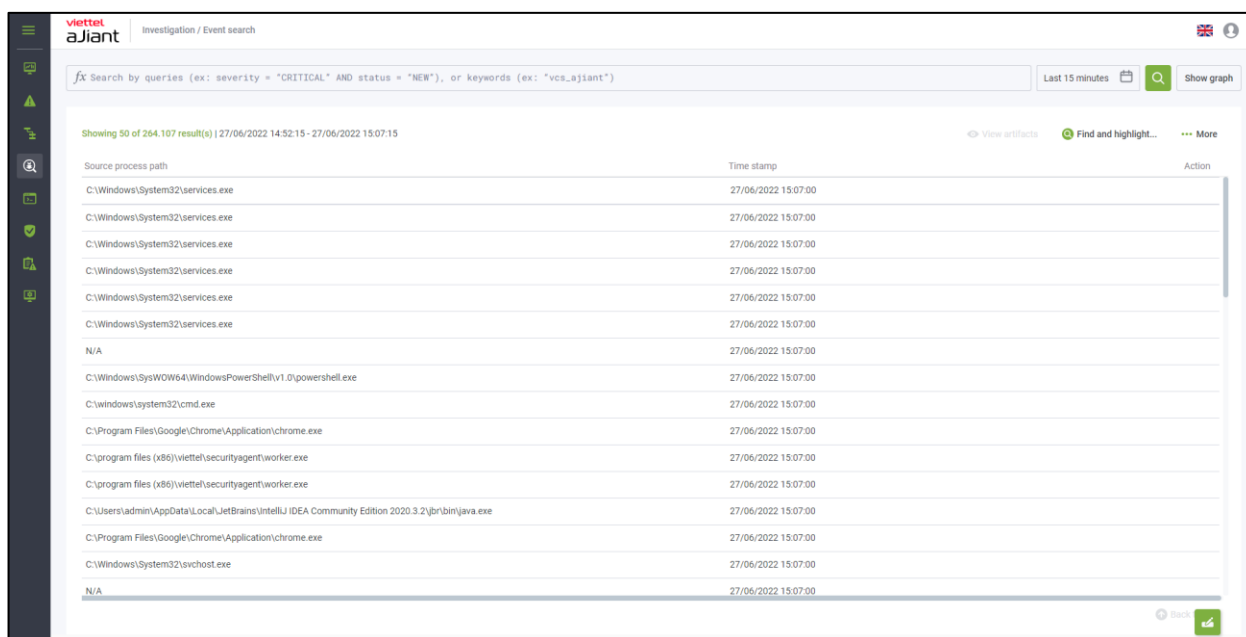
Mục đích: Có thể hiển thị toàn bộ dữ liệu hoặc thu gọn lại dữ liệu khi click vào nút “wrap text”;

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, Wrap text, Export, Need help, Chọn “Wrap 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”;



Export Data

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

Các bước thực hiện:

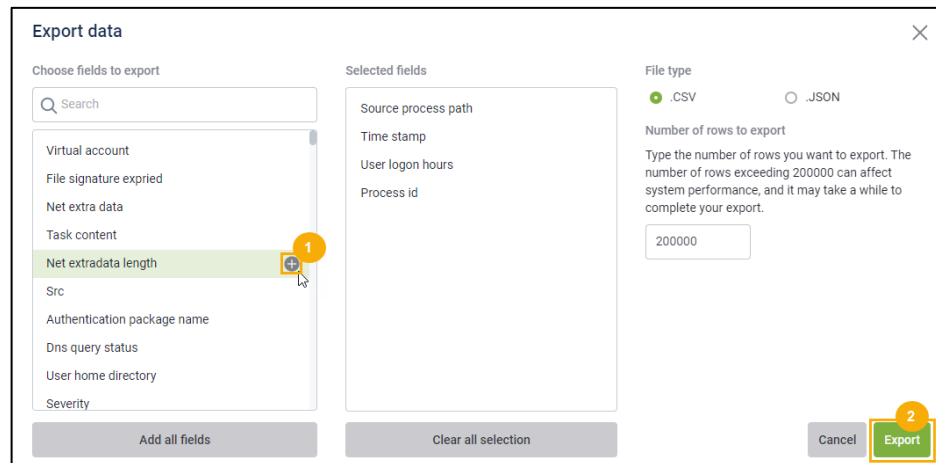
Bước 1: Tại màn hình Event Search, chọn “More”;

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;



Export data

Choose fields to export

Search

- Virtual account
- File signature expired
- Net extra data
- Task content
- Net extradata length** (1)
- Src
- Authentication package name
- Dns query status
- User home directory
- Severity

Add all fields

Selected fields

- Source process path
- Time stamp
- User logon hours
- Process id

Clear all selection

File type

☒ .CSV ☐ .JSON

Number of rows to export

Type the number of rows you want to export. The number of rows exceeding 200000 can affect system performance, and it may take a while to complete your export.

200000

Cancel **Export** (2)

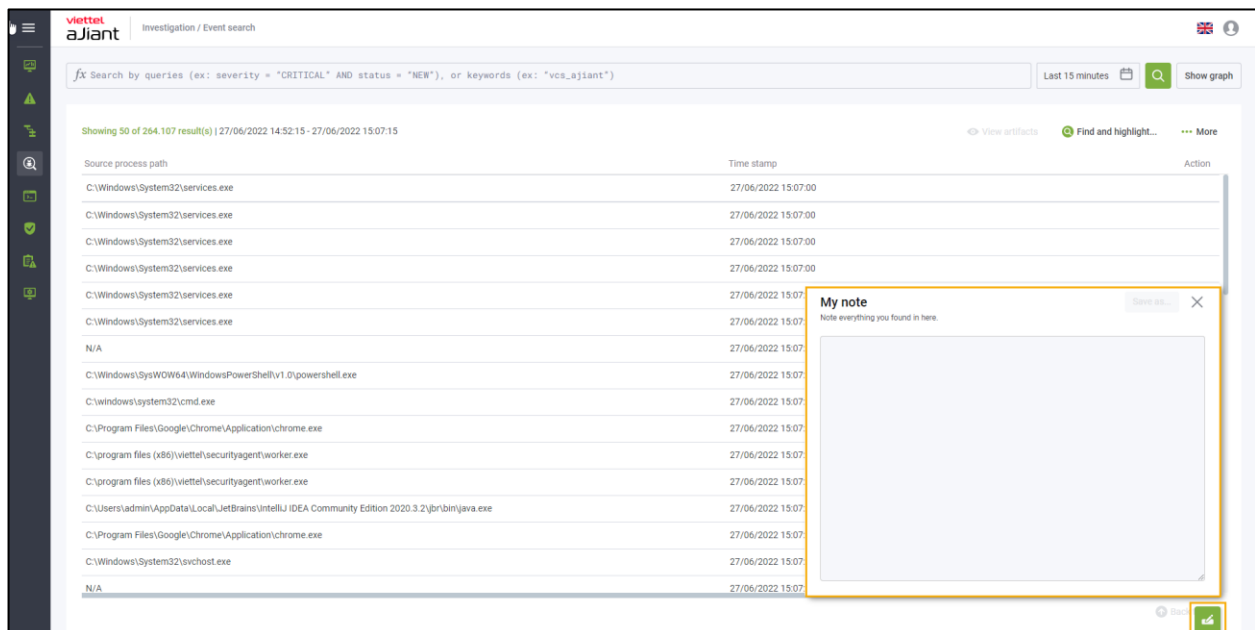
3.4.3 Note

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

Các bước thực hiện:

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

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



Investigation / Event search

Search by queries (ex: severity = "CRITICAL" AND status = "NEW"), or keywords (ex: "vcs_ajiant")

Last 15 minutes

Show graph

Showing 50 of 264,107 result(s) | 27/06/2022 14:52:15 - 27/06/2022 15:07:15

Source process path	Time stamp	Action
C:\Windows\System32\services.exe	27/06/2022 15:07:00	
C:\Windows\System32\services.exe	27/06/2022 15:07:00	
C:\Windows\System32\services.exe	27/06/2022 15:07:00	
C:\Windows\System32\services.exe	27/06/2022 15:07:00	
C:\Windows\System32\services.exe	27/06/2022 15:07:00	
C:\Windows\System32\services.exe	27/06/2022 15:07:00	
N/A	27/06/2022 15:07:00	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	27/06/2022 15:07:00	
C:\windows\system32\cmd.exe	27/06/2022 15:07:00	
C:\Program Files\Google\Chrome\Application\chrome.exe	27/06/2022 15:07:00	
C:\program files (x86)\viettel\securityagent\worker.exe	27/06/2022 15:07:00	
C:\program files (x86)\viettel\securityagent\worker.exe	27/06/2022 15:07:00	
C:\Users\admin\AppData\Local\JetBrains\IntelliJ IDEA Community Edition 2020.3.2\bin\java.exe	27/06/2022 15:07:00	
C:\Program Files\Google\Chrome\Application\chrome.exe	27/06/2022 15:07:00	
C:\Windows\System32\svchost.exe	27/06/2022 15:07:00	
N/A	27/06/2022 15:07:00	

My note

Note everything you found in here.

Save as...

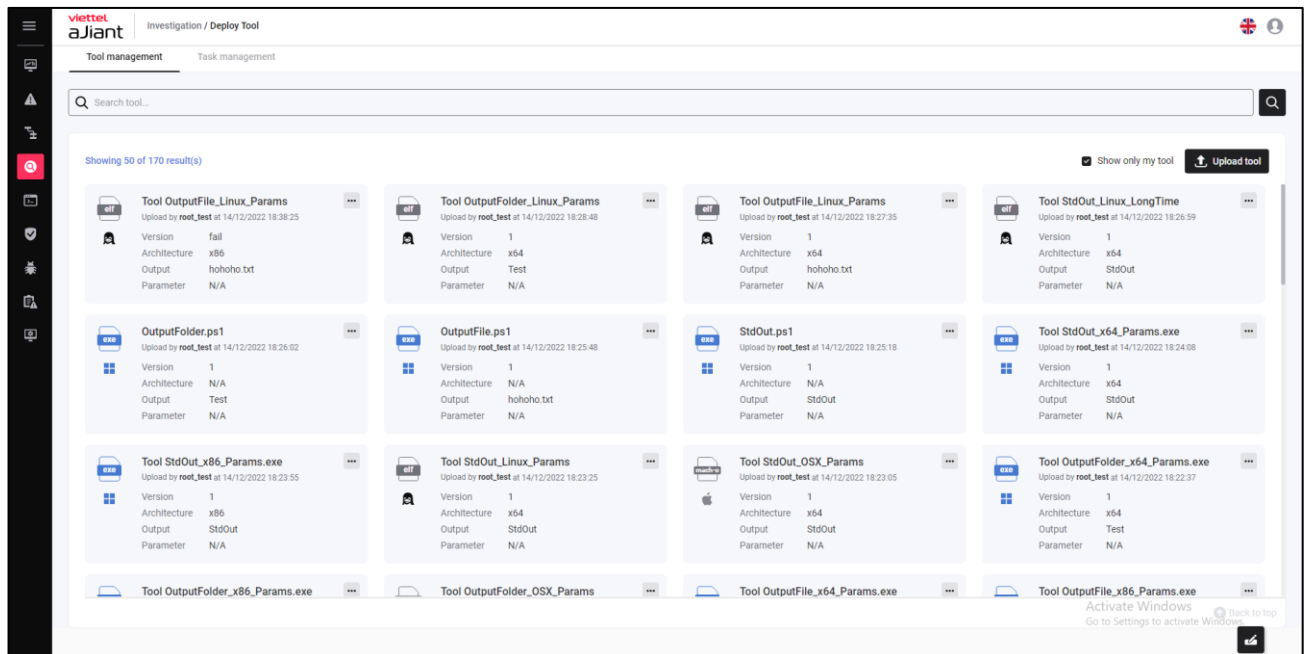
3.4.4 Deploy Tools

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

Tool Management

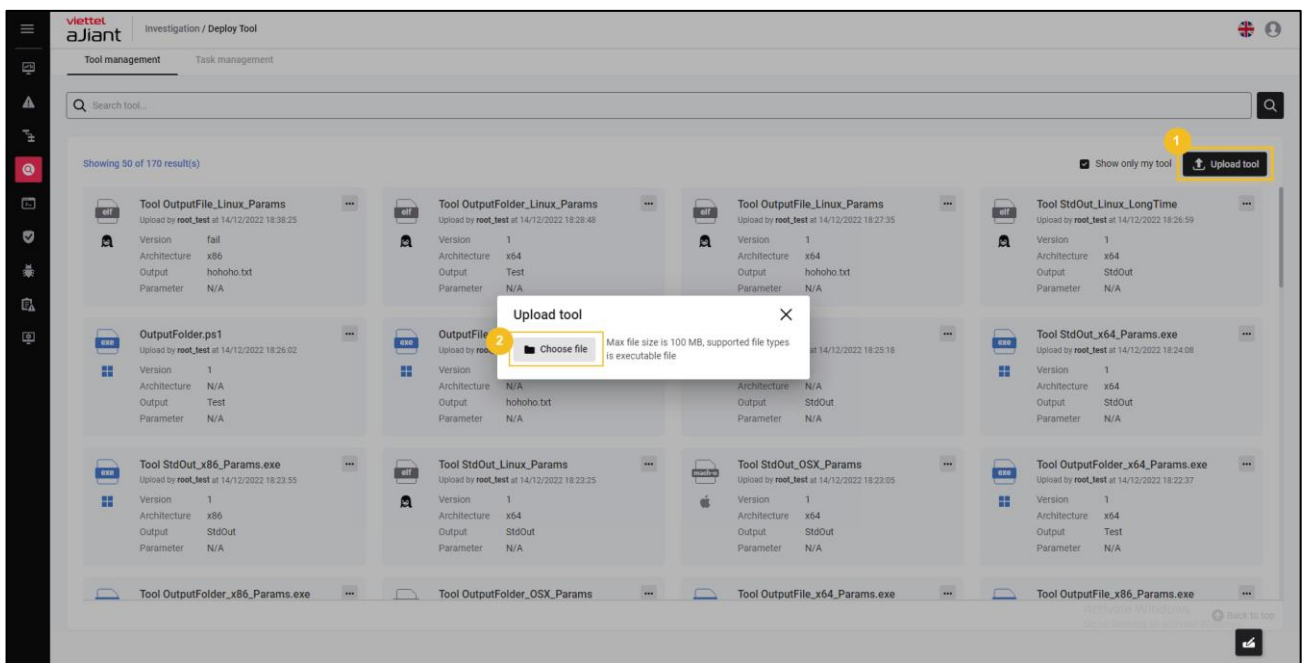
Mục đích: quản lý toàn bộ tool của hệ thống, người sử dụng có thể thêm/ xóa tool ở màn hình này. Các tính năng ở màn hình này gồm có:

- + 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;

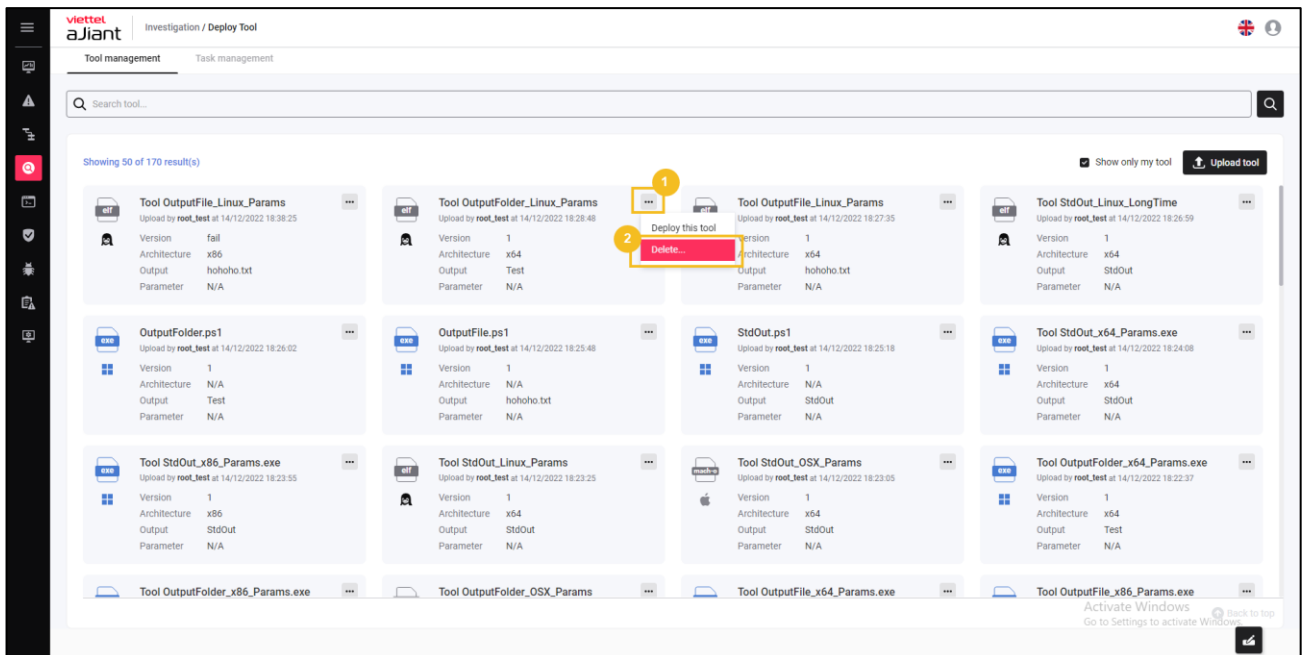


Với tính năng Upload tool thao tác theo các bước sau:

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**



Deploy tool

Mục đích: Cấu hình thông tin deploy tool dưới agent

Điều kiện:

Viettel Cyber Security

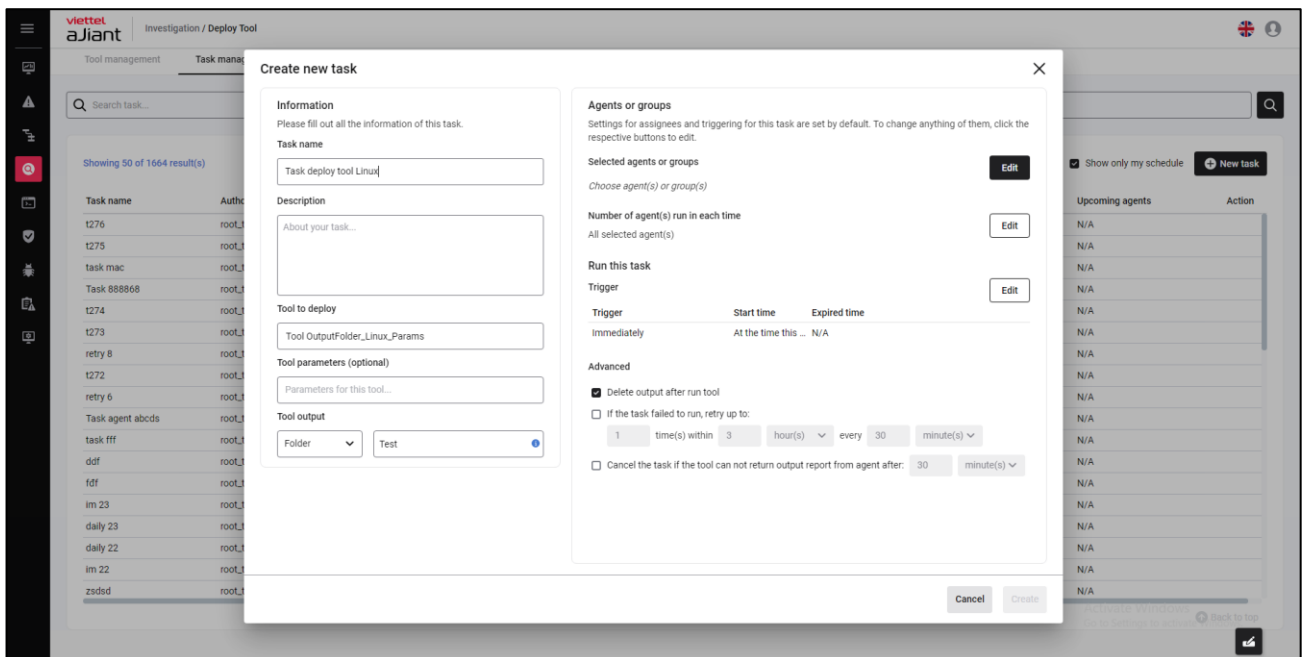
Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi

T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

- + 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;

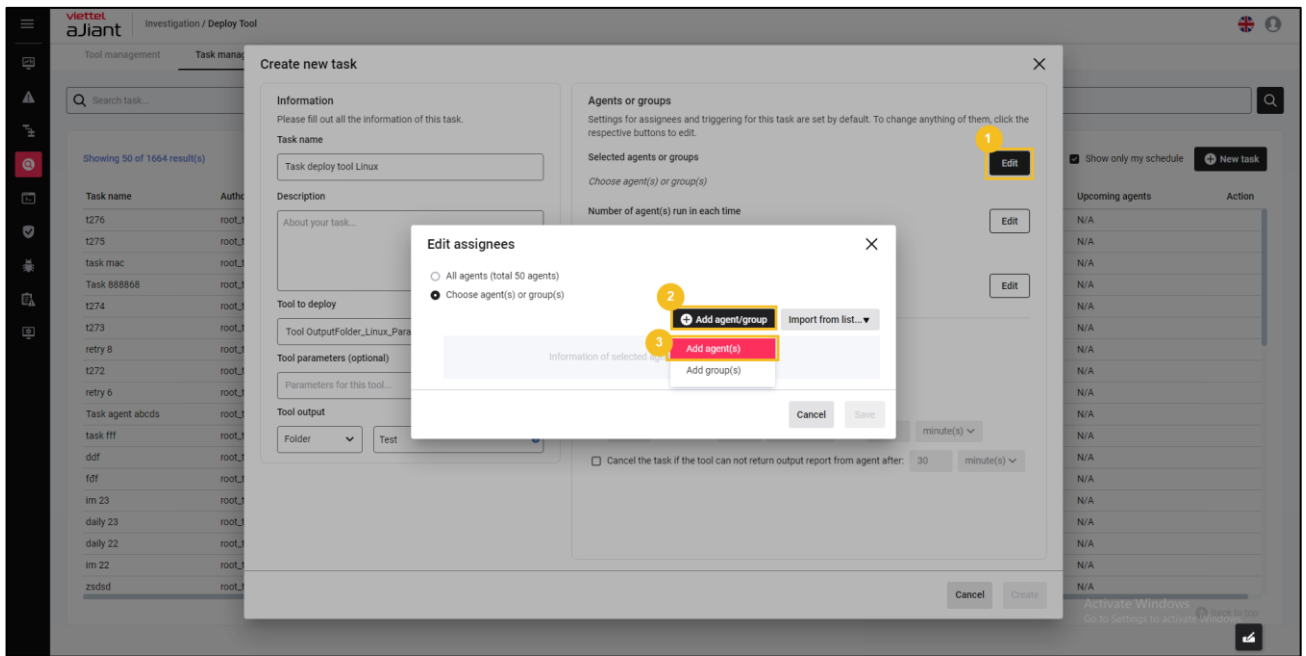
Bước 3: Lựa chọn thông tin nhóm (group), máy trạm (agent) để thực hiện deploy:

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;

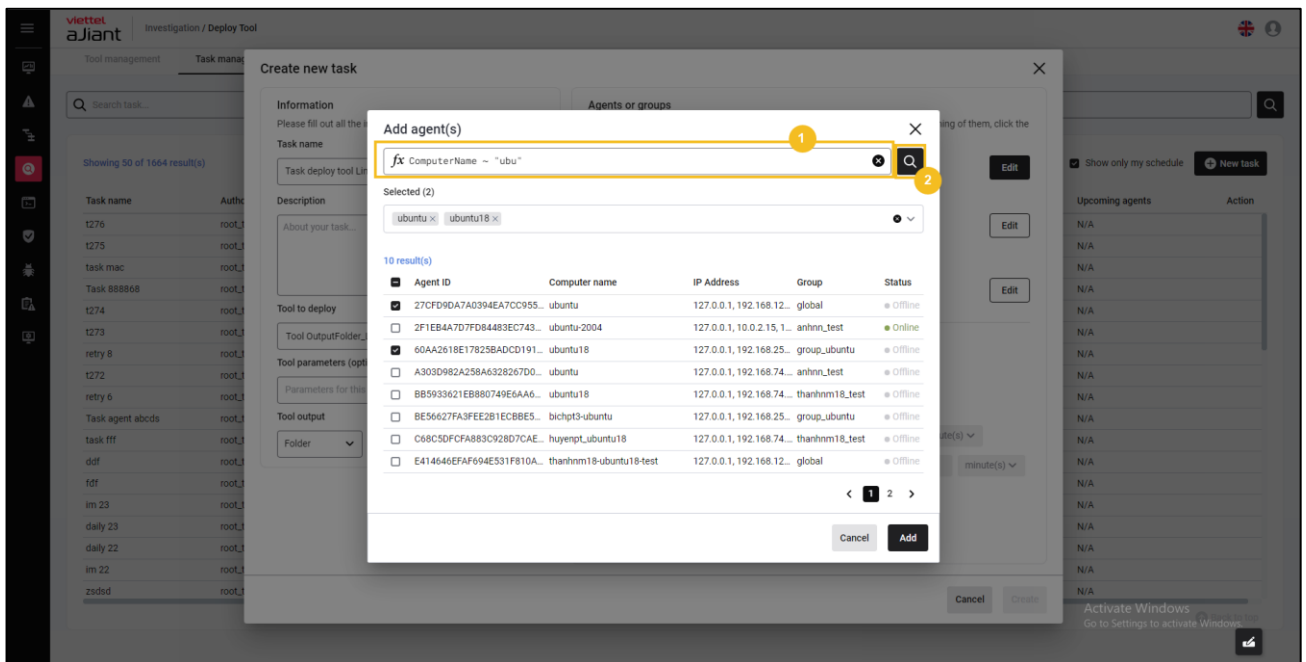
Lựa chọn agents or groups thực hiện deploy – **Choose agent(s) or group(s)**:

The screenshot shows the 'Create new task' window. On the left, there are sections for 'Information' (Task name: 'Task deploy tool Linux', Description: 'About your task...'), 'Tool to deploy' (Tool OutputFolder_Linux_Para), 'Tool parameters (optional)' (Parameters for this tool...), and 'Tool output' (Folder, Test). On the right, the 'Agents or groups' section has a description, 'Selected agents or groups' (Choose agent(s) or group(s)), and 'Number of agent(s) run in each time'. An 'Edit' button in this section is highlighted with a yellow box and a circled '1'. An 'Edit assignees' modal is open in the center, showing two radio buttons: 'All agents (total 50 agents)' and 'Choose agent(s) or group(s)'. The second option is selected. A '+ Add agent/group' button is highlighted with a yellow box and a circled '2'. Below this button is a text box that says 'Information of selected agent(s) will be showing here.' and buttons for 'Cancel' and 'Save'. At the bottom right of the modal are 'Cancel' and 'Save' buttons. At the bottom right of the main window are 'Cancel' and 'Create' buttons.

+ Chọn Add agent(s):

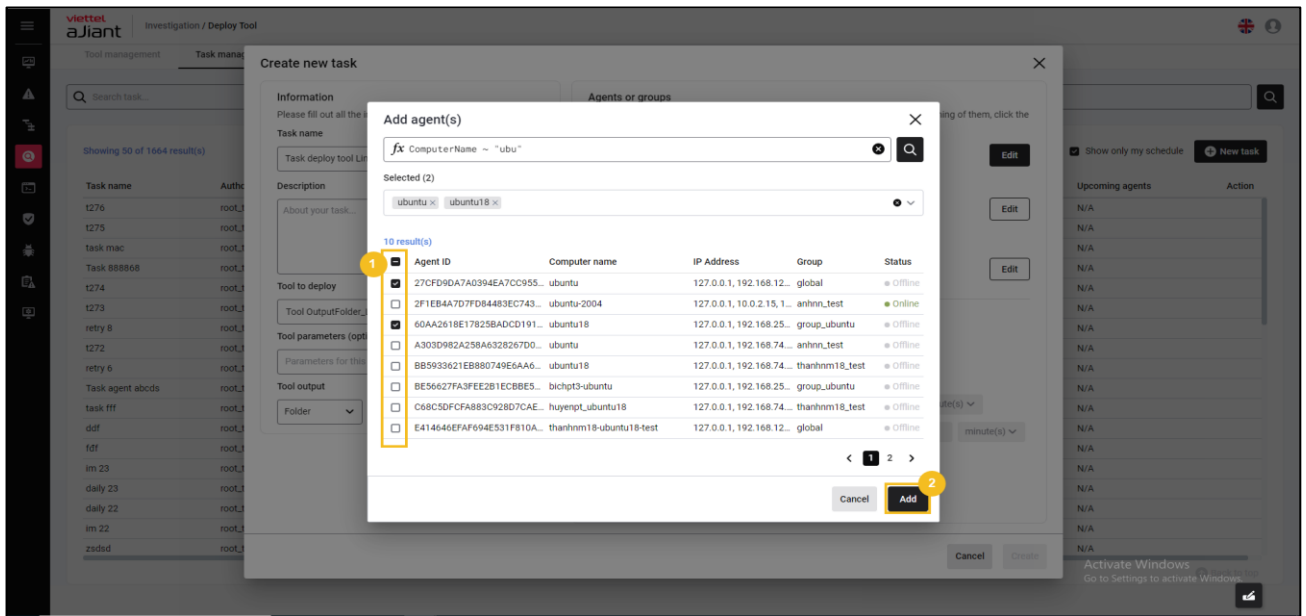


- Tìm kiếm Agent: Cho phép tạo câu lệnh truy vấn, sử dụng câu lệnh truy vấn để tìm kiếm Agent

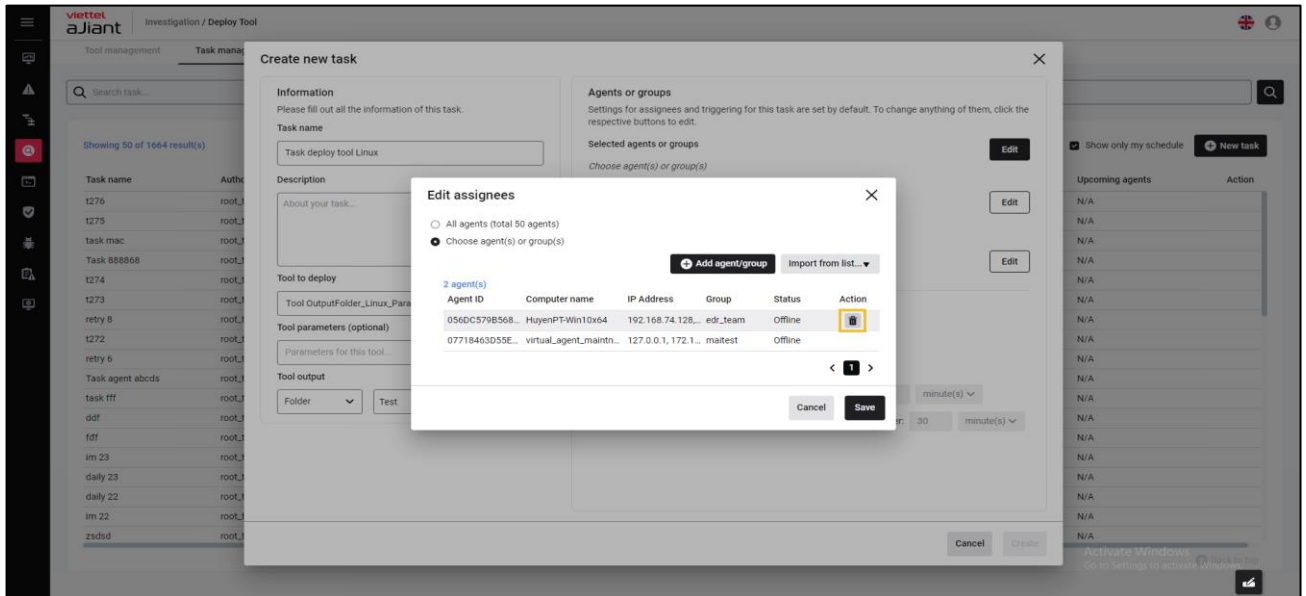


- Chọn Agent(s) để deploy bằng cách tích chọn vào một hoặc nhiều Agent(s) > Thông tin Agent(s) đã được chọn hiển thị ở khung **Selected** > chọn

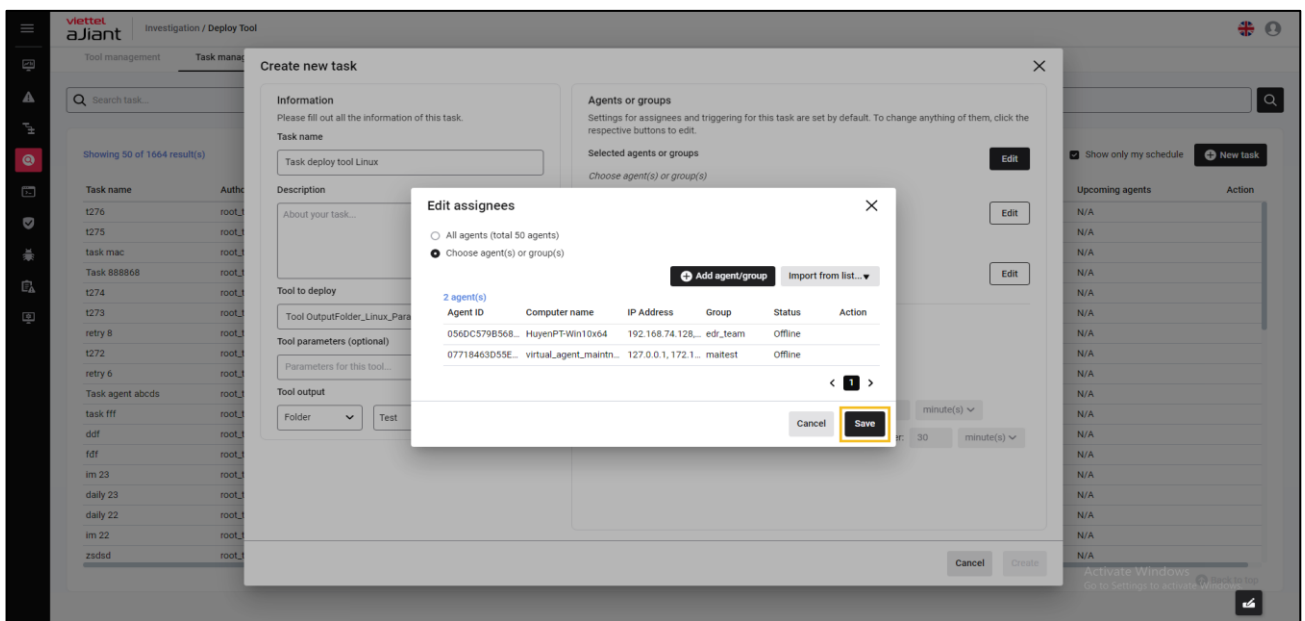
Cancel để hủy thao tác thêm Agent để deploy hoặc chọn nút **Add** để xác nhận danh sách Agent(s):



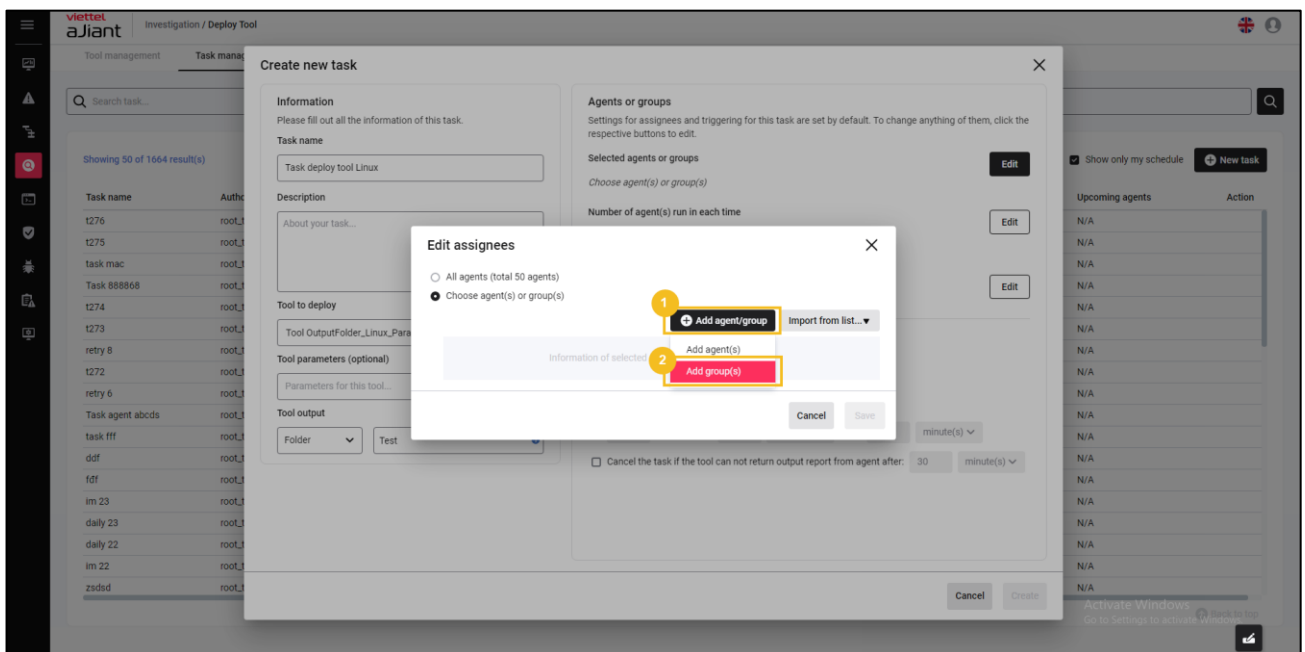
- Hover vào các Agent(s) đã chọn > Chọn icon  để thực hiện loại bỏ Agent(s) khỏi danh sách đã chọn



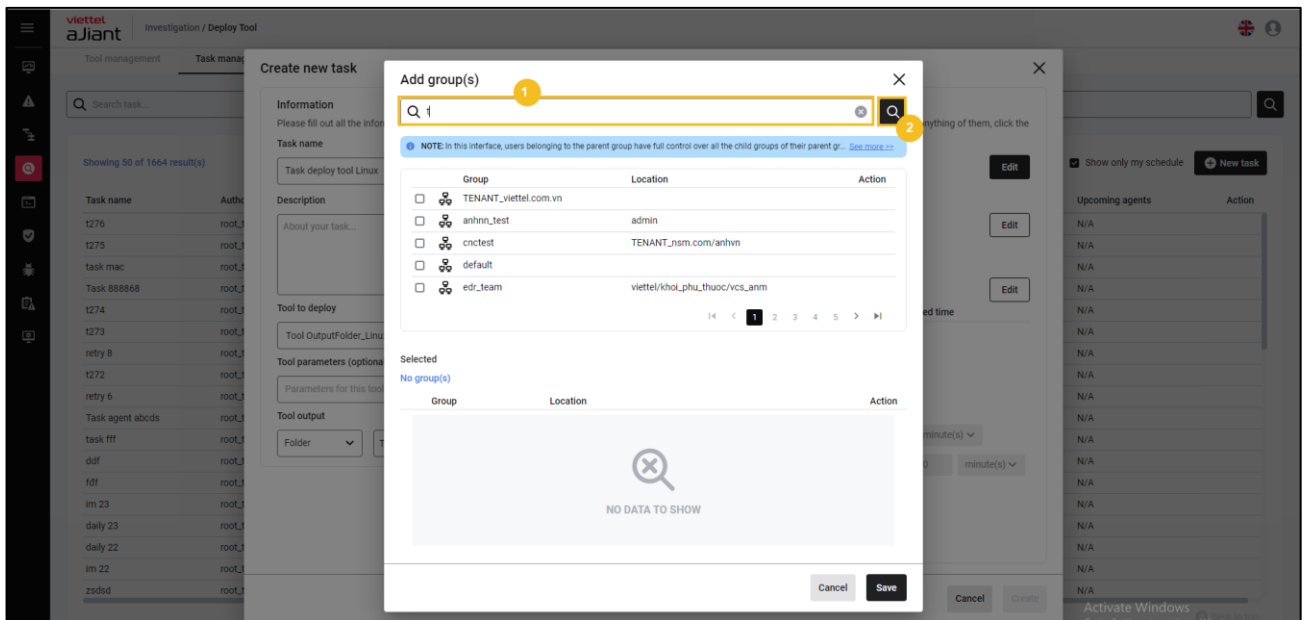
- Chọn **Cancel** để hủy hoặc chọn **Save** để lưu thông tin các Agent(s) đã chọn để deploy:



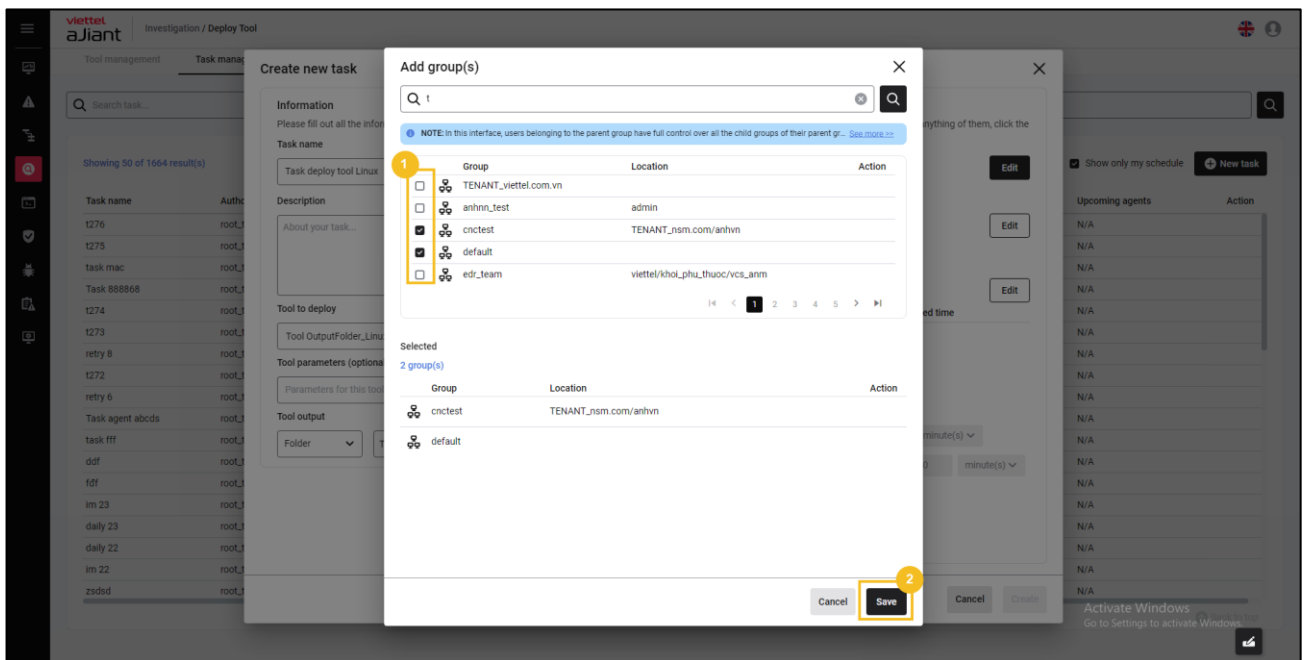
+ Chọn Add group(s):



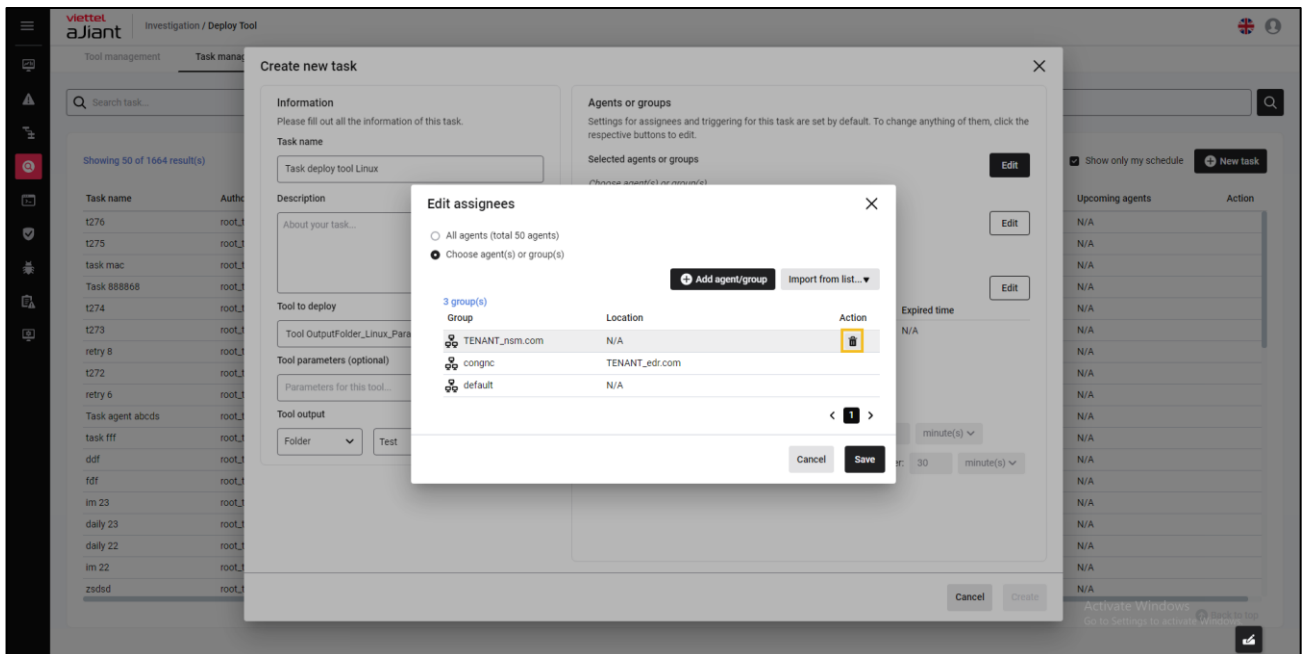
- Tìm kiếm group(s) theo tên, cho phép nhập từ khóa tìm kiếm group theo tên group:



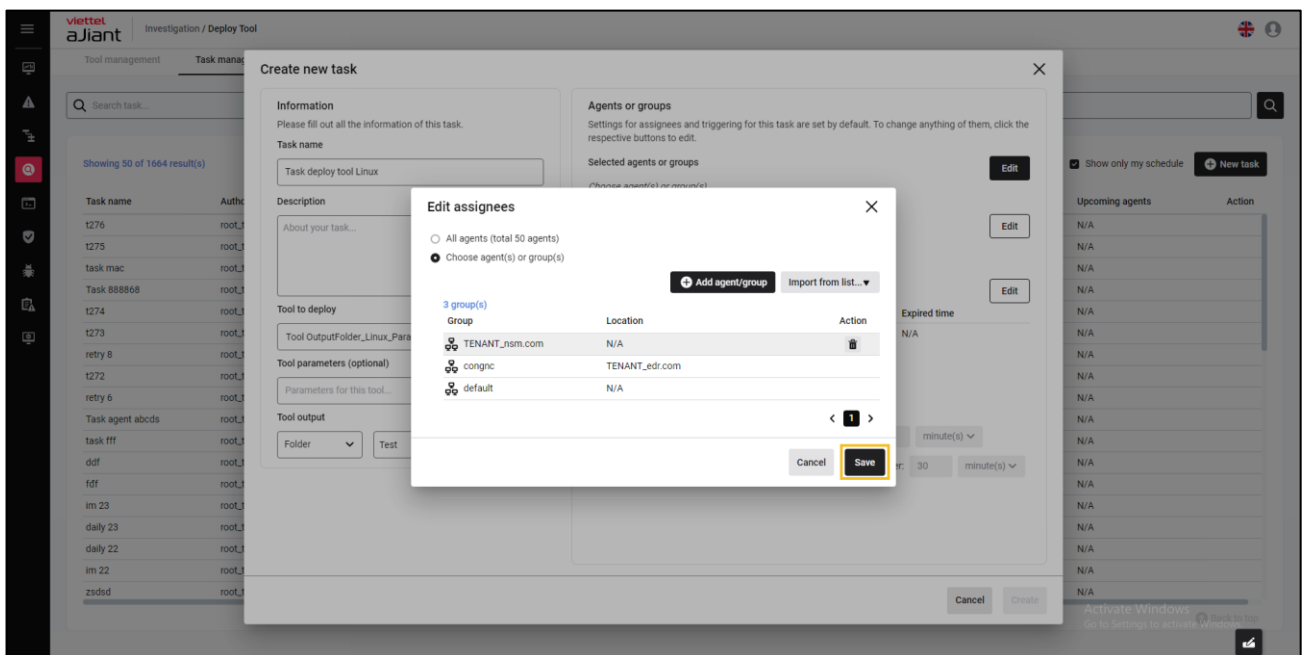
- Chọn group(s) để deploy bằng cách tích chọn vào một hoặc nhiều group(s) > Thông tin group(s) đã được chọn hiển thị ở khung **Selected** > chọn **Cancel** để hủy thao tác thêm group(s) để deploy hoặc chọn nút **Save** để xác nhận danh sách group(s):



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

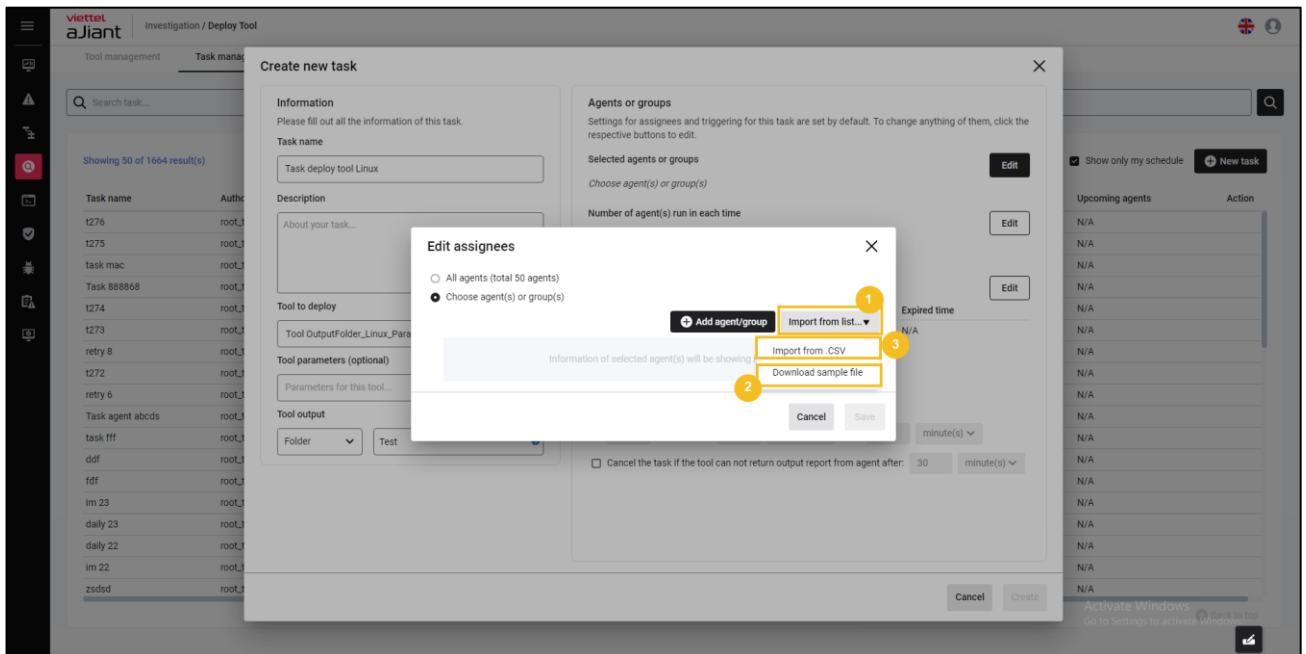


- Chọn **Cancel** để hủy hoặc Chọn **Save** các group(s) đã chọn để deploy:



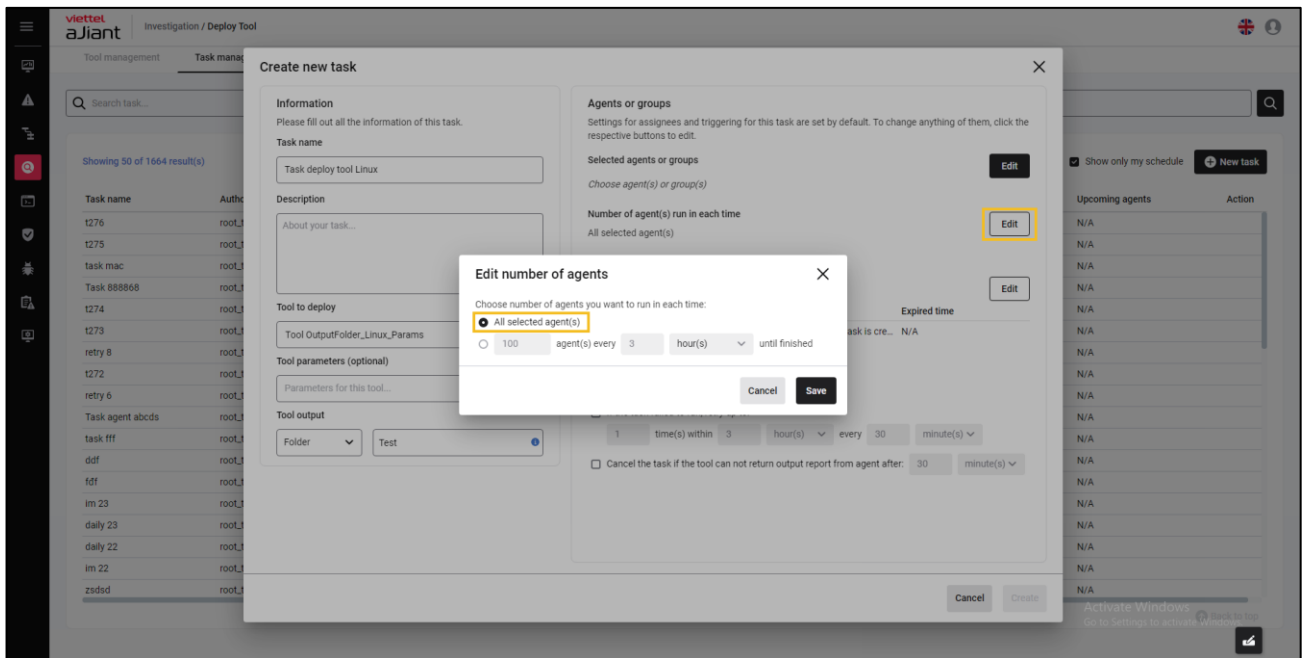
+ Import from list: Cho phép upload danh sách agent(s) từ file .csv > Chọn **Import from list**

- 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)

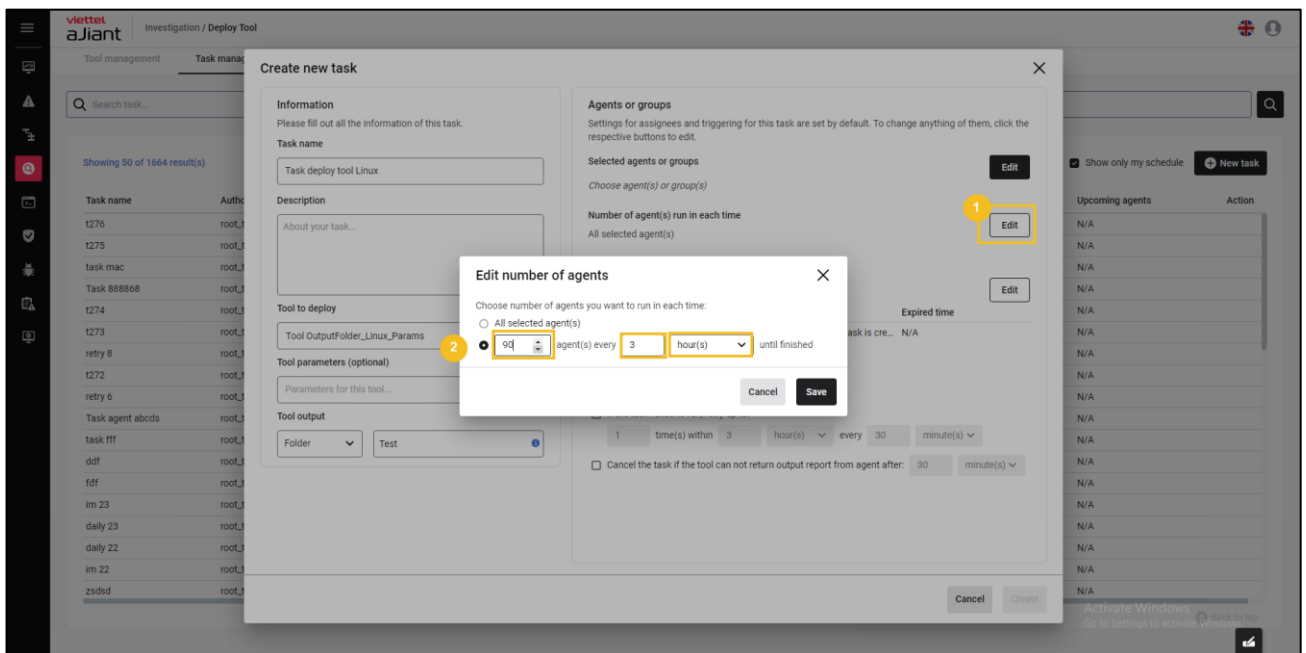


Bước 4: Cấu hình số lượng agent deploy tool mỗi lần:

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

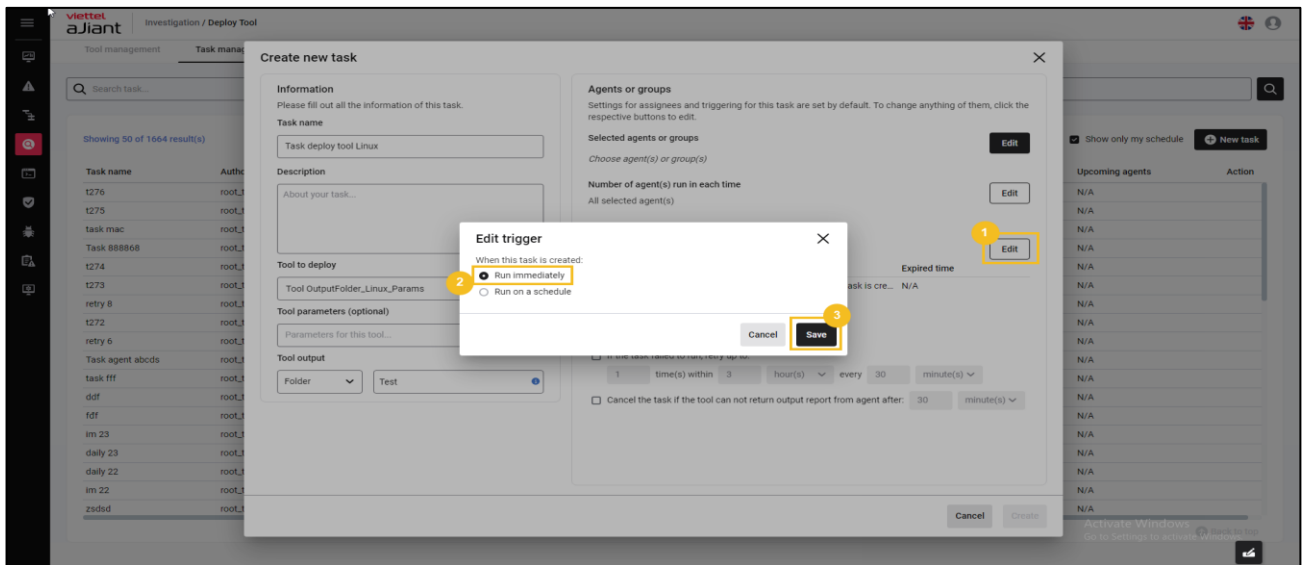


+ Cấu hình số lượng agent mỗi lần deploy:



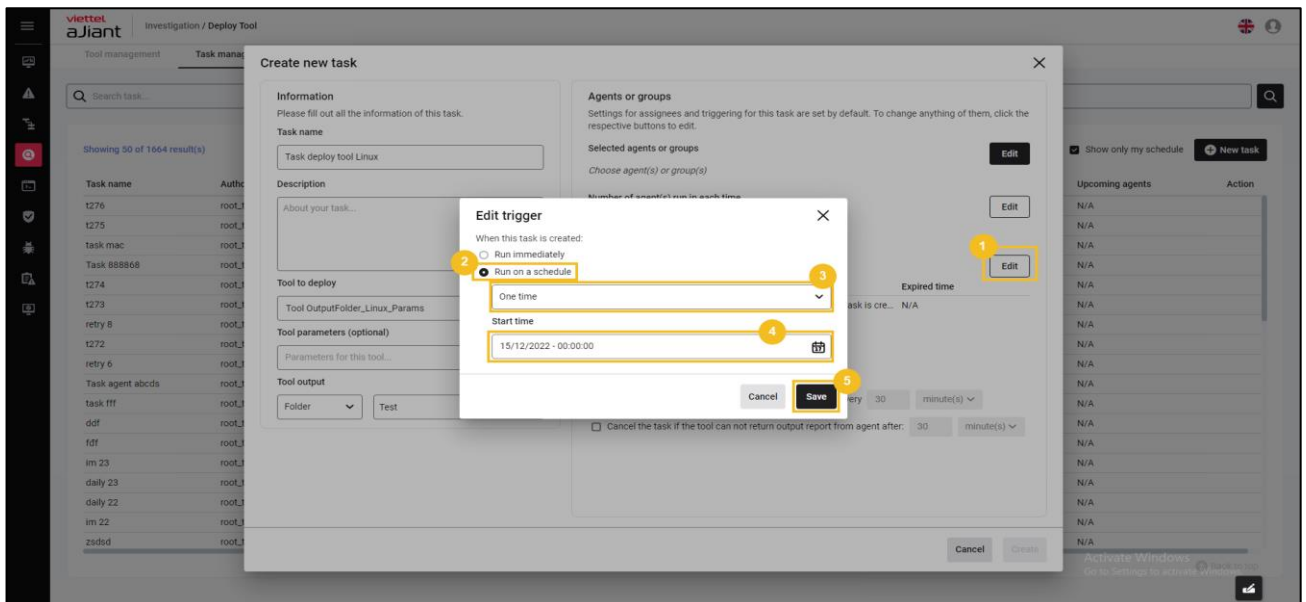
Bước 5: Cấu hình thông tin thời gian (lập lịch) thực hiện deploy tool:

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



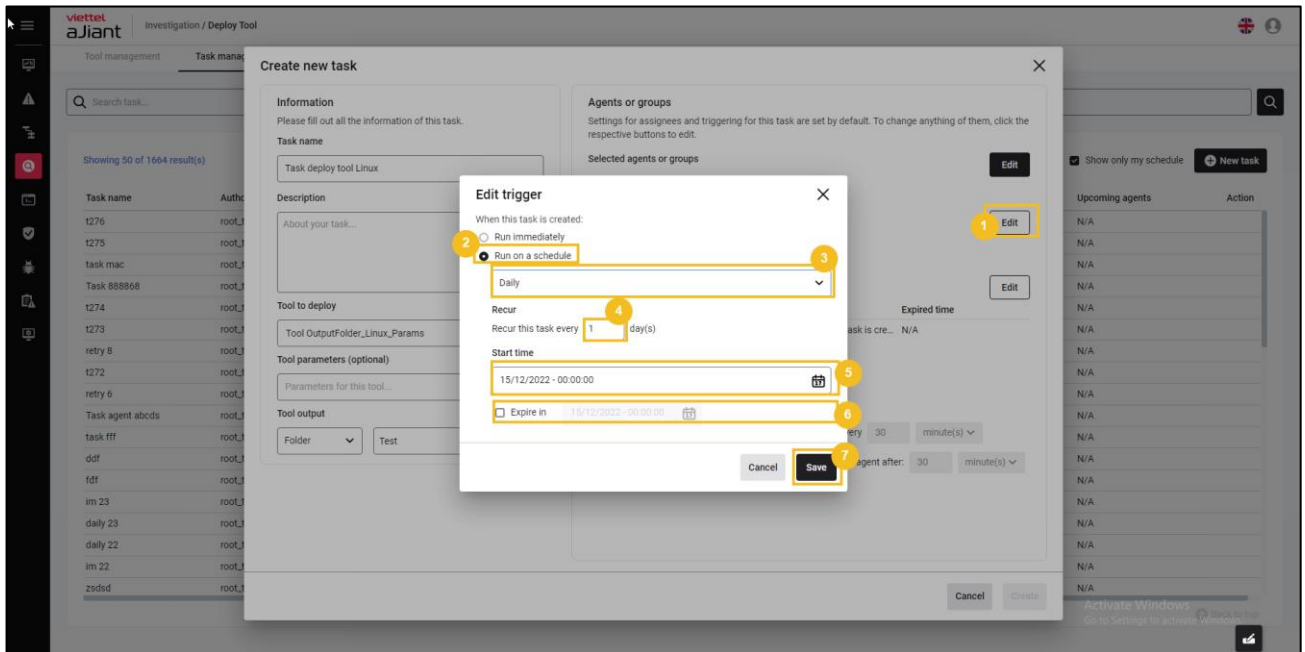
+ Chọn **Run on schedule** để thực hiện cấu hình thời gian deploy tool theo lịch:

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

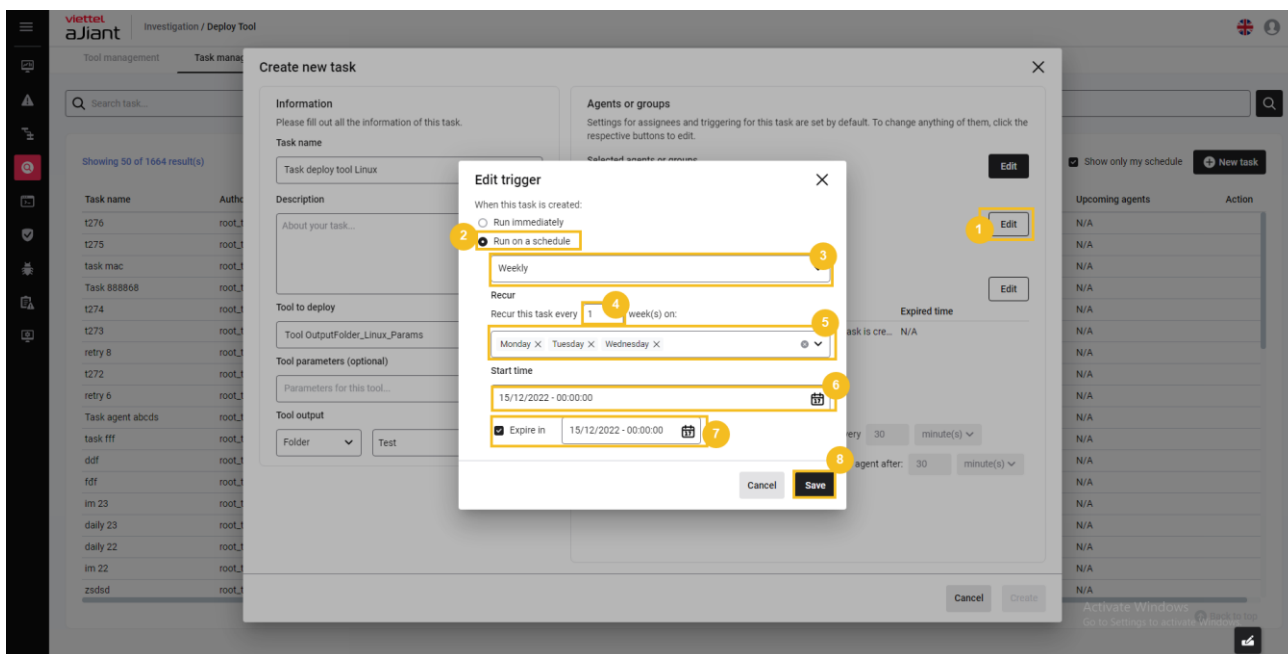


- Chọn schedule **Daily**:
 - Cho phép lập lịch deploy tool hàng ngày;

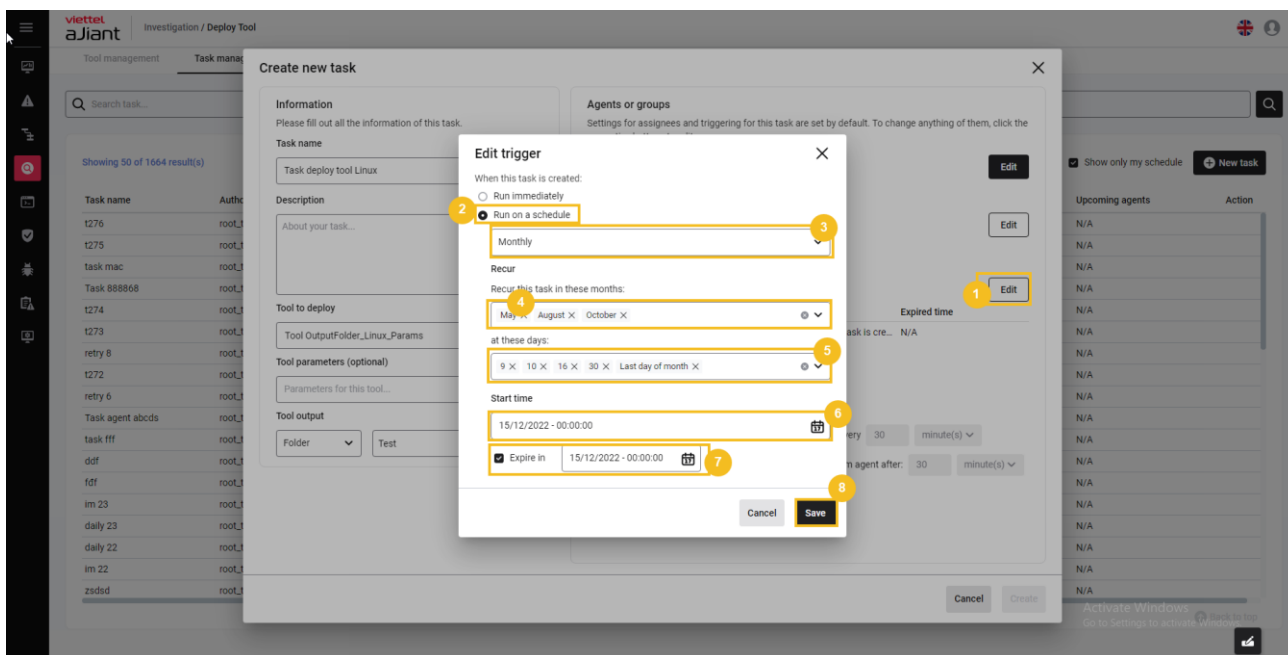
- Thời gian lặp lại;
- Cấu hình thời gian bắt đầu và kết thúc:



- 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)

Create new task

Information
Please fill out all the information of this task.

Task name
Task deploy tool Linux

Description
About your task...

Tool to deploy
Tool OutputFolder_Linux_Params

Tool parameters (optional)
Parameters for this tool...

Tool output
Folder Test

Agents or groups
Settings for assignees and triggering for this task are set by default. To change anything of them, click the respective buttons to edit.

Selected agents or groups
All agents (total 50 agents) Edit

Number of agent(s) run in each time
All selected agent(s) Edit

Run this task

Trigger
Trigger Start time Expired time
On day(s) 9, 10, 16, 30 and last day of May.. 15/12/2022 15:00:00 23/12/2022 00:00:00 Edit

Advanced

☒ Delete output after run tool

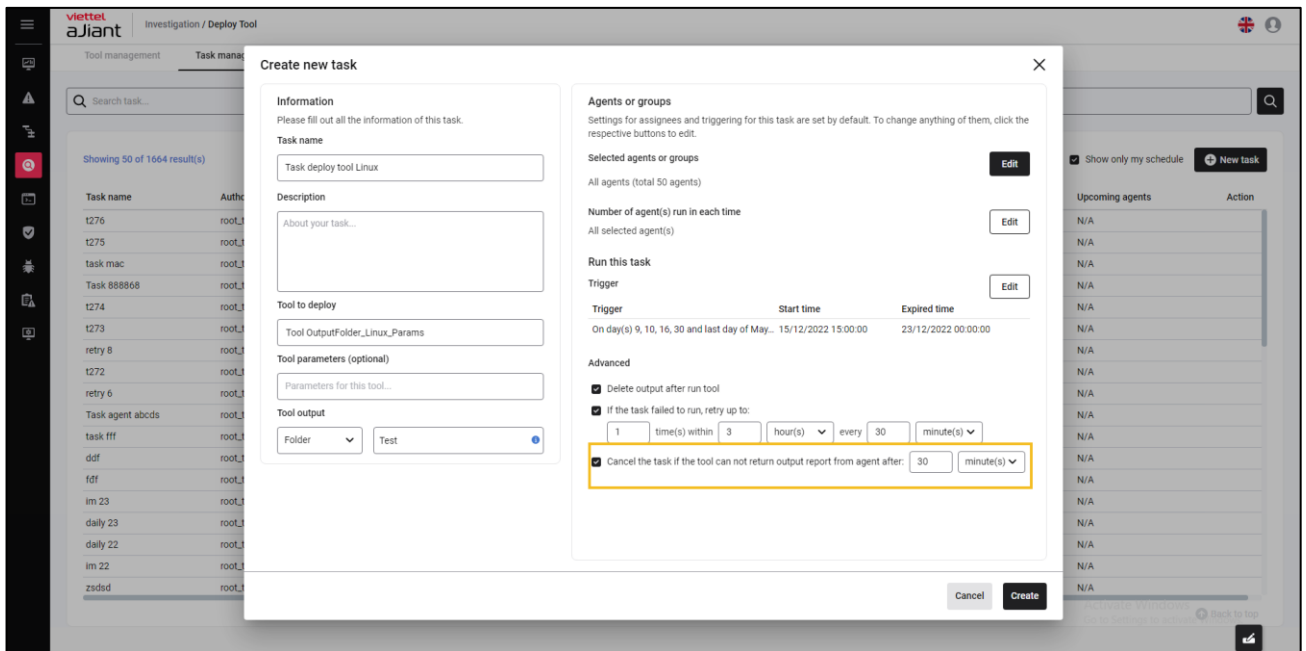
☒ If the task failed to run, retry up to:

1 time(s) within 3 hour(s) every 30 minute(s)

☒ Cancel the task if the tool can not return output report from agent after: 30 minute(s)

Cancel Create

- + **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:



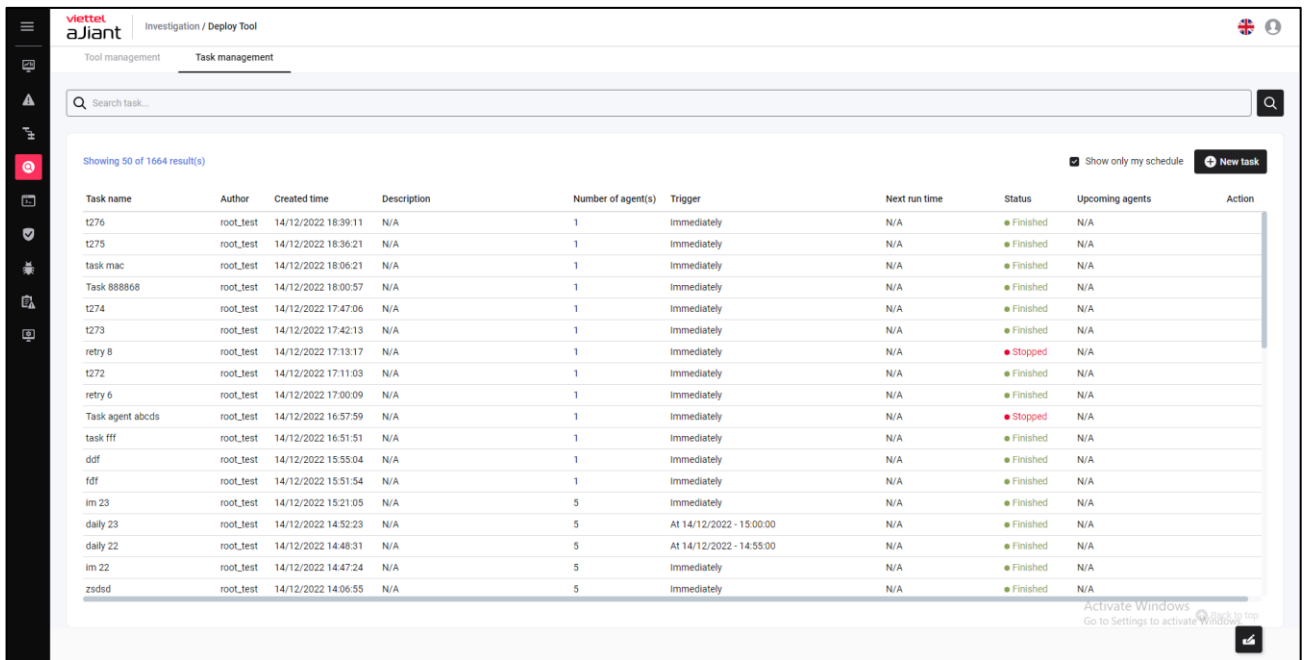
Bước 7: Chọn **Create** để tạo mới task/ cấu hình thông tin deploy tool dưới agent hoặc chọn **Cancel** để hủy task/ hủy cấu hình thông tin deploy tool dưới agent

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



Investigation / Deploy Tool

Tool management Task management

Search task...

Showing 50 of 1664 result(s) ☒ Show only my schedule [New task](#)

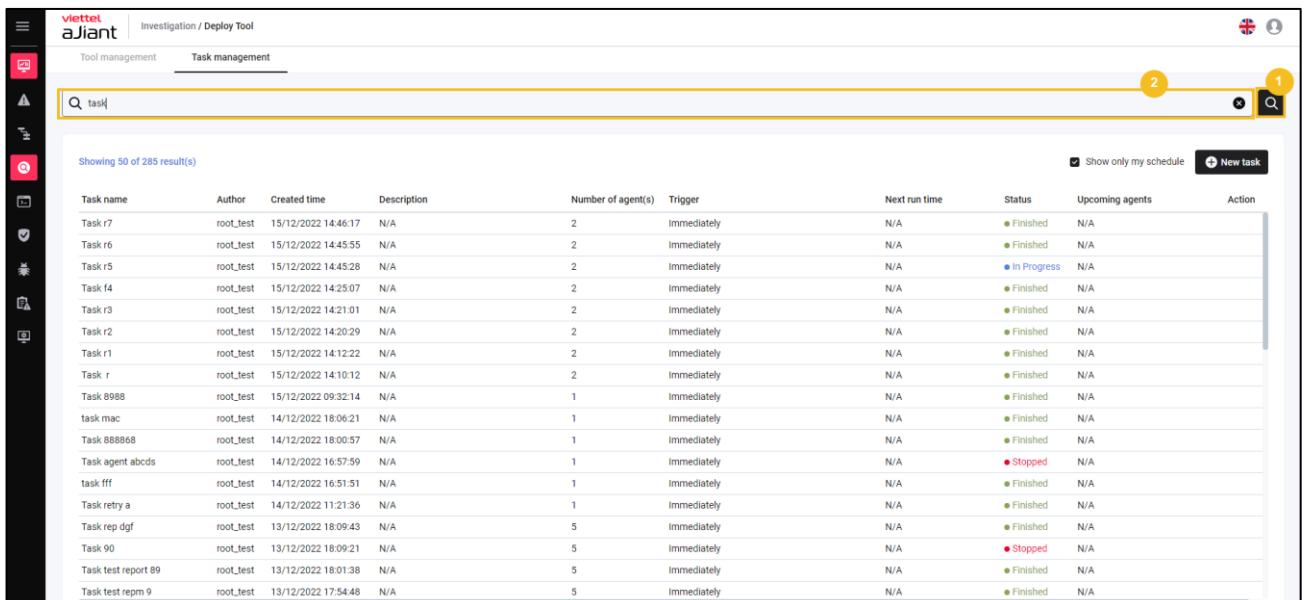
Task name	Author	Created time	Description	Number of agent(s)	Trigger	Next run time	Status	Upcoming agents	Action
1276	root_test	14/12/2022 18:39:11	N/A	1	Immediately	N/A	Finished	N/A	
1275	root_test	14/12/2022 18:36:21	N/A	1	Immediately	N/A	Finished	N/A	
task mac	root_test	14/12/2022 18:06:21	N/A	1	Immediately	N/A	Finished	N/A	
Task 888868	root_test	14/12/2022 18:00:57	N/A	1	Immediately	N/A	Finished	N/A	
1274	root_test	14/12/2022 17:47:06	N/A	1	Immediately	N/A	Finished	N/A	
1273	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	
1272	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	
zsdssd	root_test	14/12/2022 14:06:55	N/A	5	Immediately	N/A	Finished	N/A	

Activate Windows Go to Settings to activate Windows

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:



Investigation / Deploy Tool

Tool management Task management

Search task...

Showing 50 of 285 result(s) ☒ Show only my schedule [New 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	
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	

c. Tạo task

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

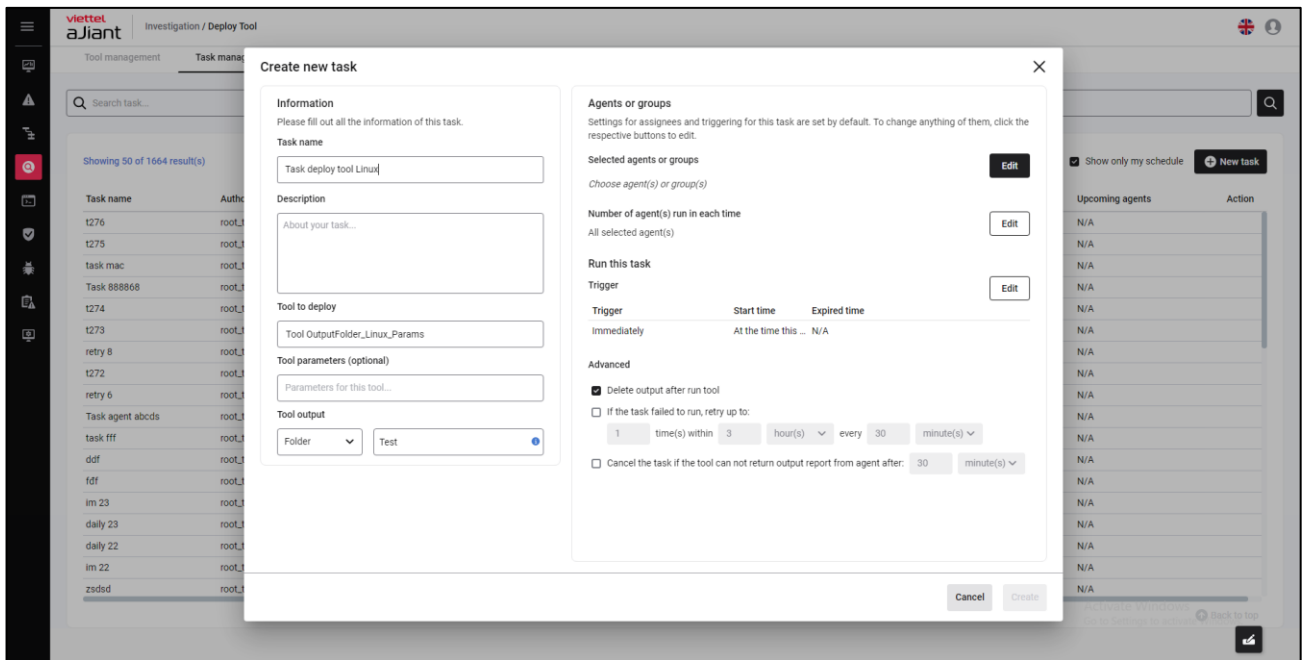
Mục đích: Cấu hình thông tin deploy tool dưới agent

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;

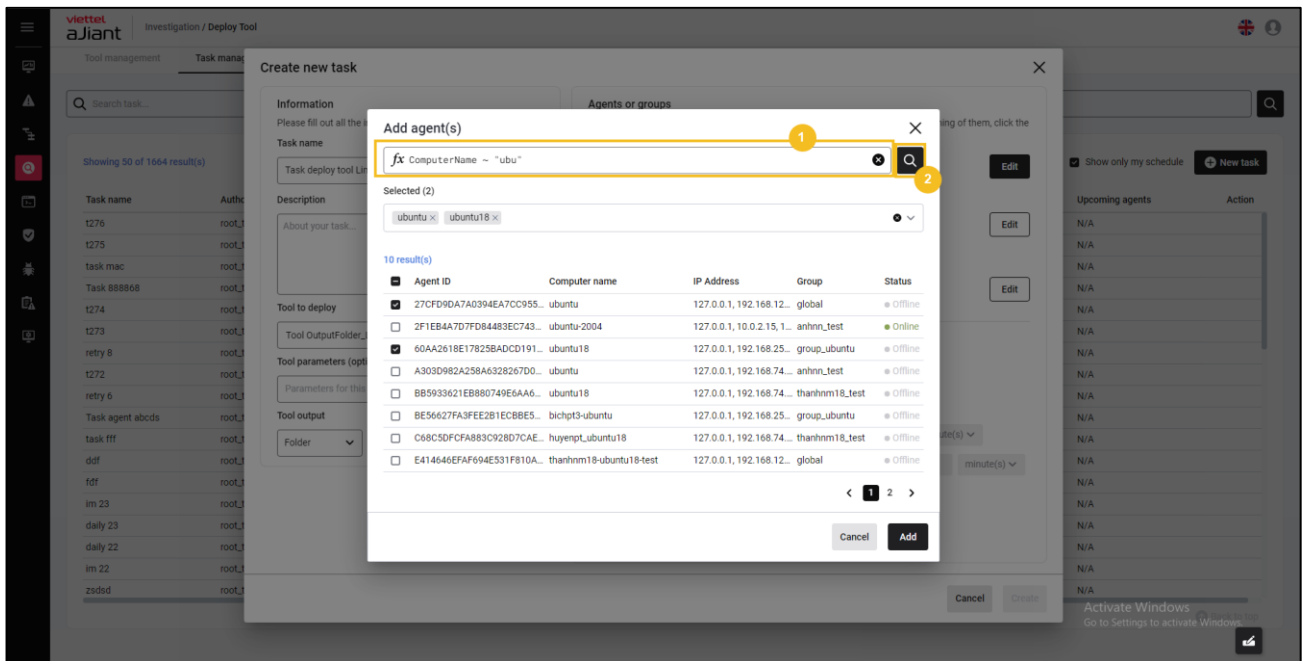
Bước 3: Lựa chọn thông tin nhóm (group), máy trạm (agent) để thực hiện deploy:

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;

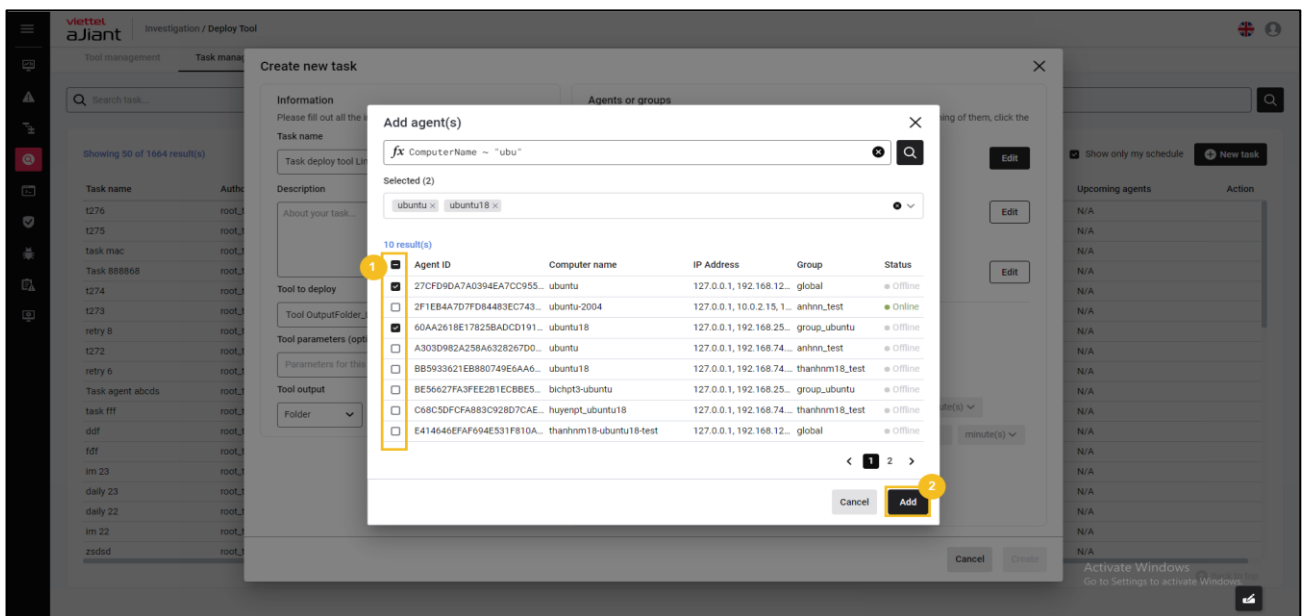
Lựa chọn agents or groups thực hiện deploy – **Choose agent(s) or group(s)**:

+ Chọn Add agent(s):

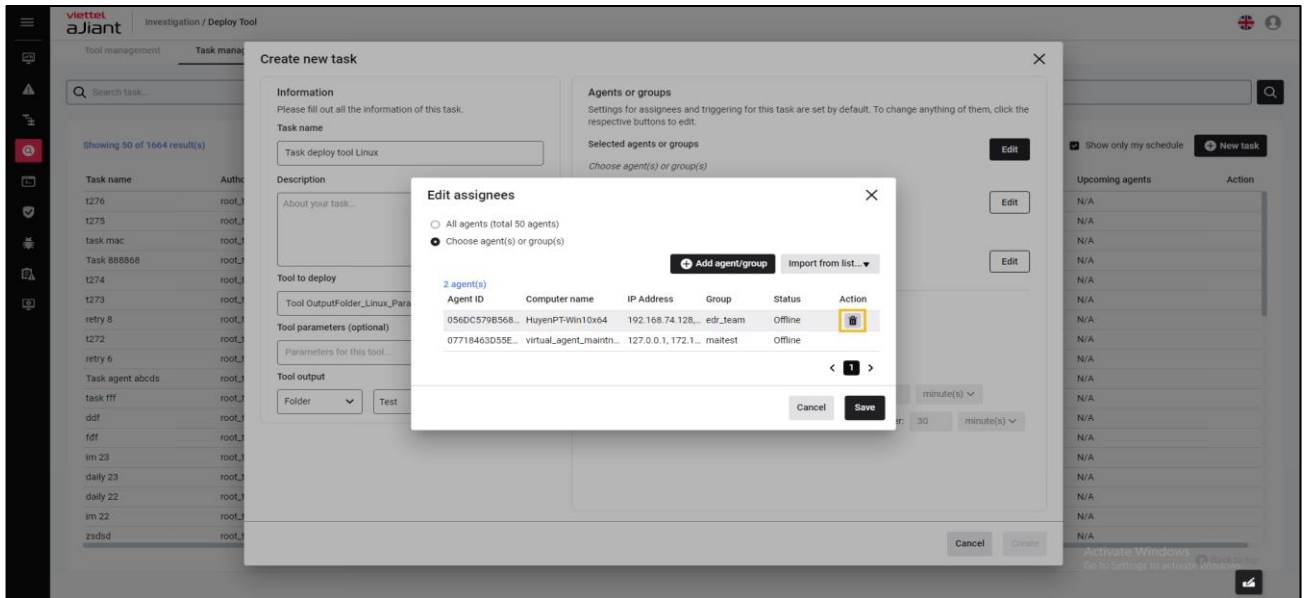
- **Tìm kiếm Agent:** Cho phép tạo câu lệnh truy vấn, sử dụng câu lệnh truy vấn để tìm kiếm Agent



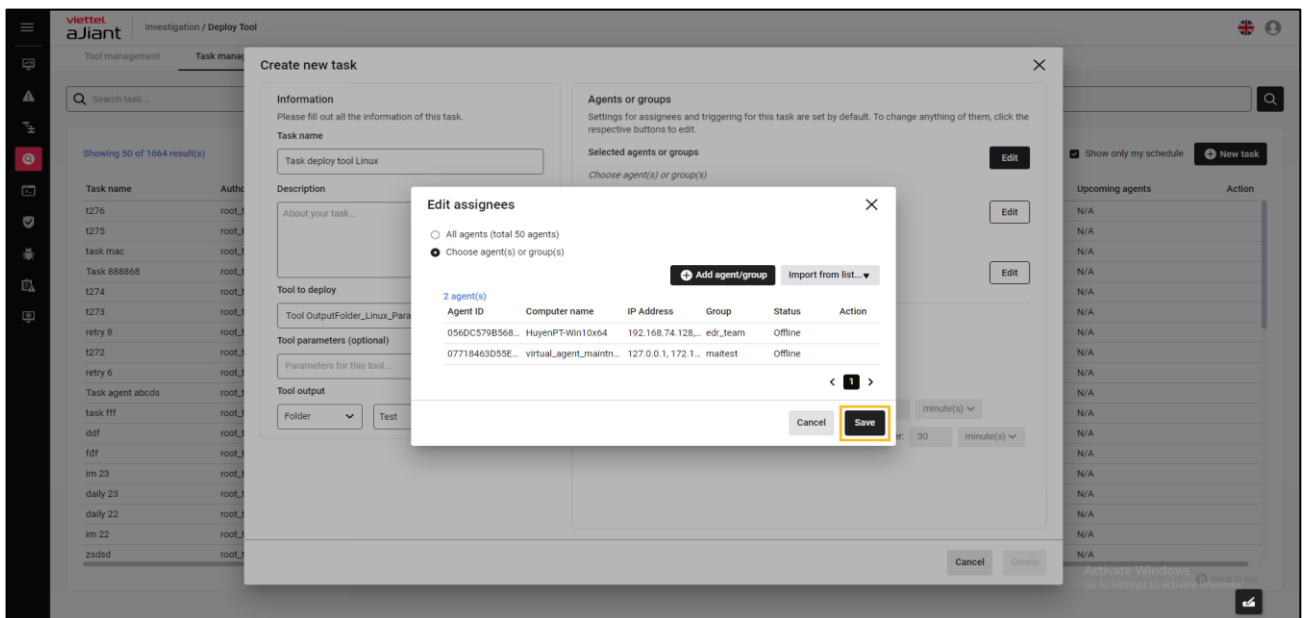
- Chọn Agent(s) để deploy bằng cách tích chọn vào một hoặc nhiều Agent(s) > Thông tin Agent(s) đã được chọn hiển thị ở khung **Selected** > chọn **Cancel** để hủy thao tác thêm Agent để deploy hoặc chọn nút **Add** để xác nhận danh sách Agent(s):



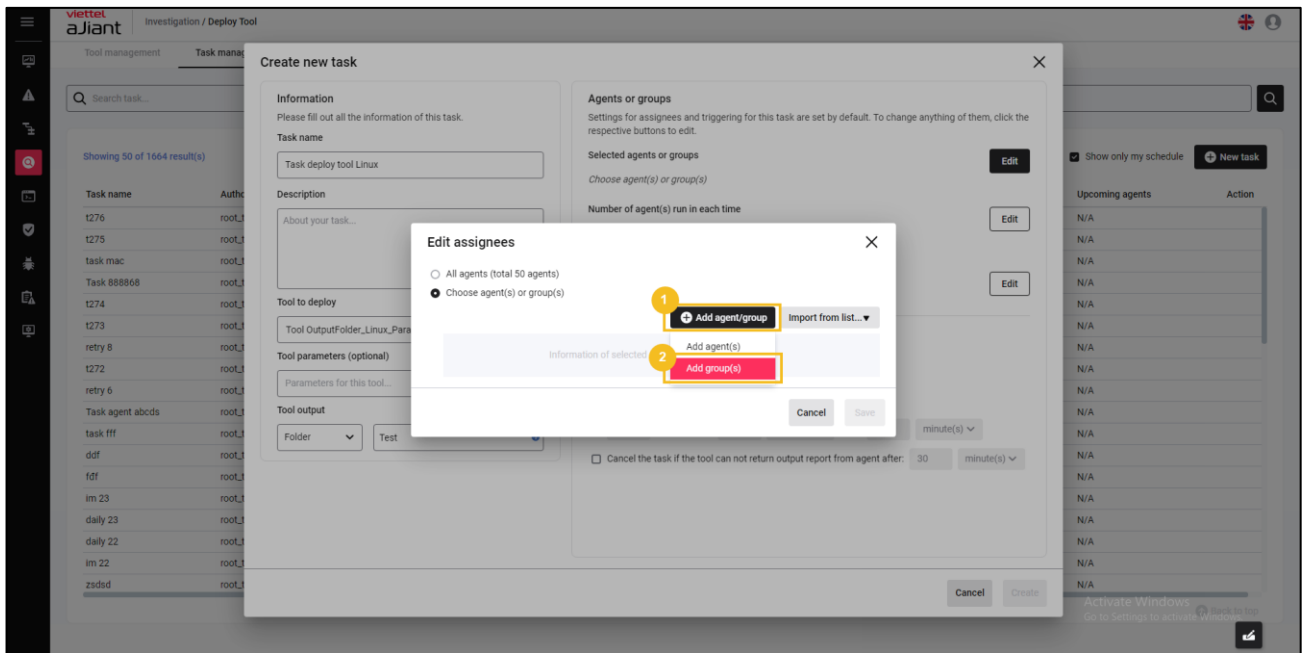
- Hover vào các Agent(s) đã chọn > Chọn icon  để thực hiện loại bỏ Agent(s) khỏi danh sách đã chọn:



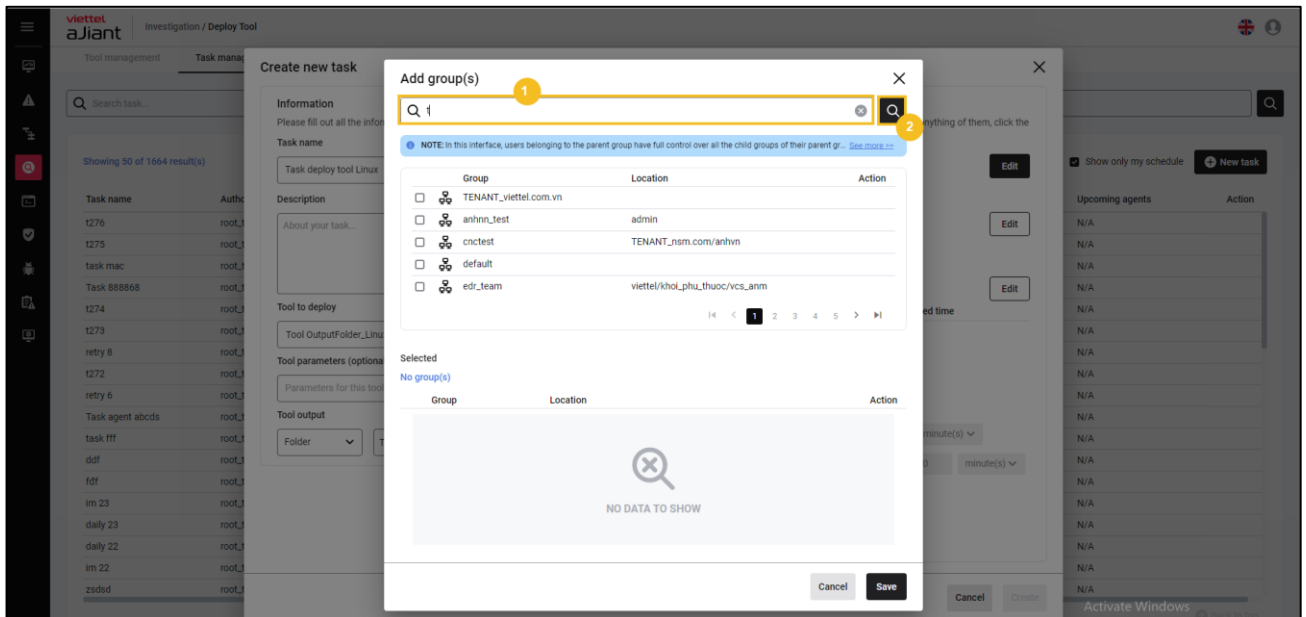
- Chọn **Cancel** để hủy hoặc chọn **Save** để lưu thông tin các Agent(s) đã chọn để deploy:



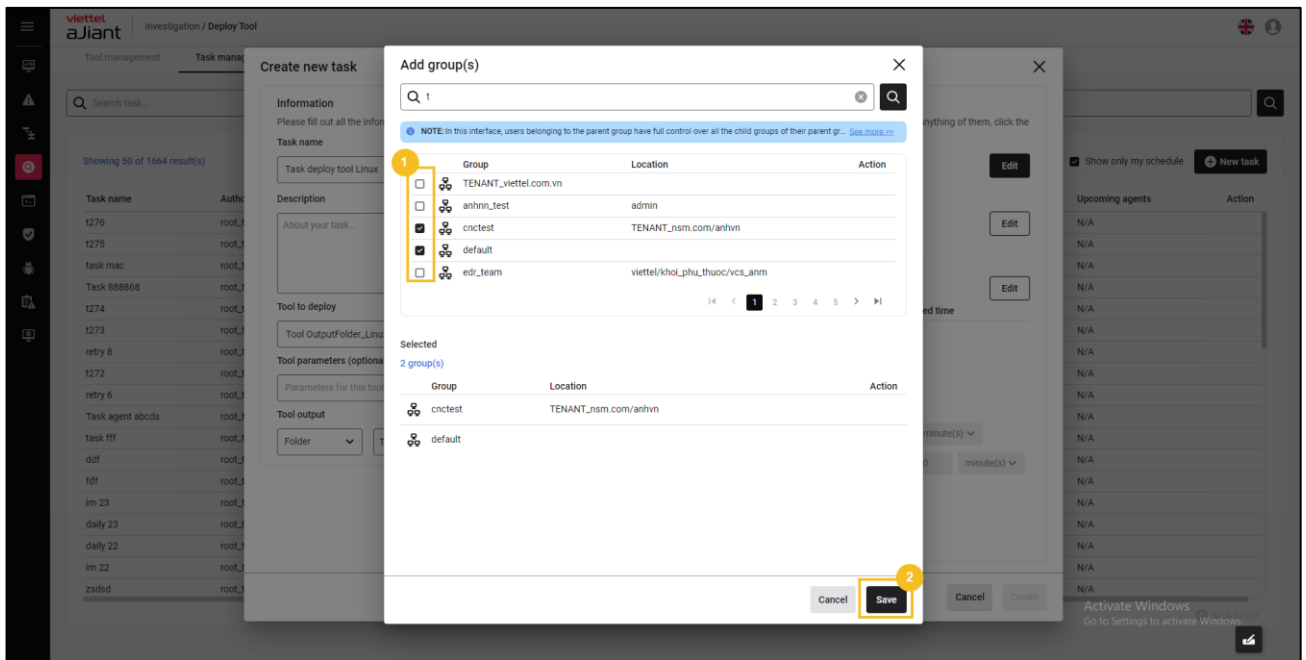
+ Chọn Add group(s):



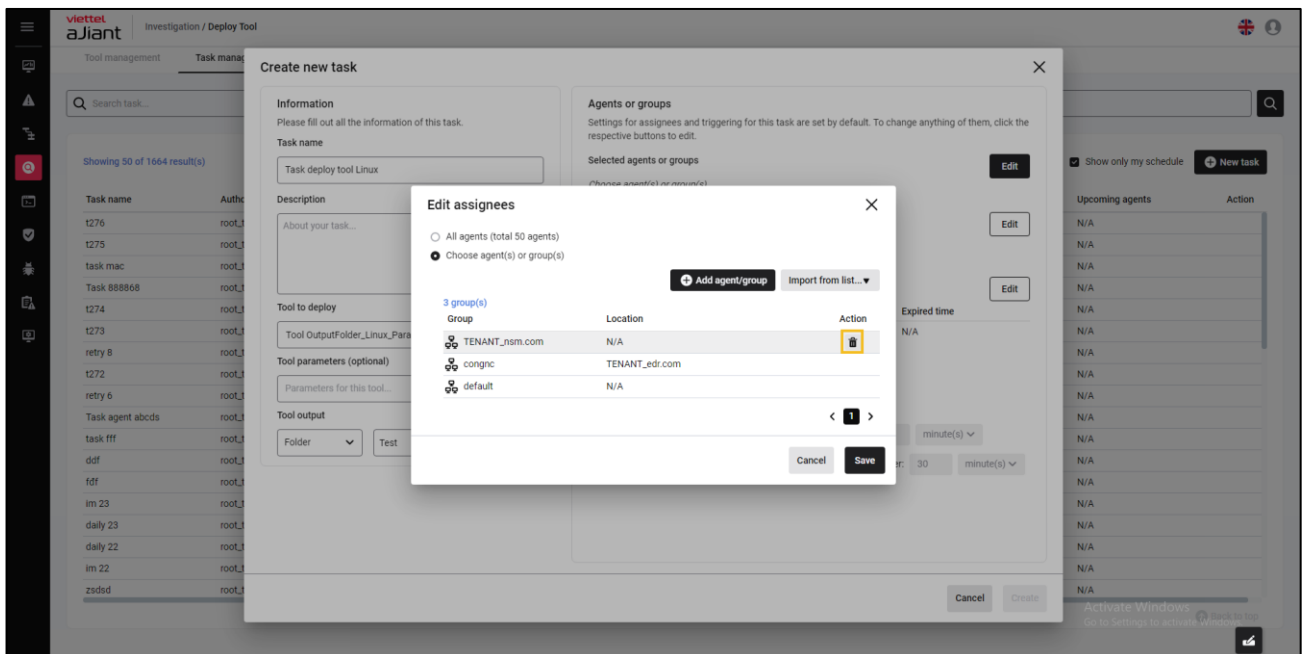
- Tìm kiếm group(s) theo tên, cho phép nhập từ khóa tìm kiếm group theo tên group:



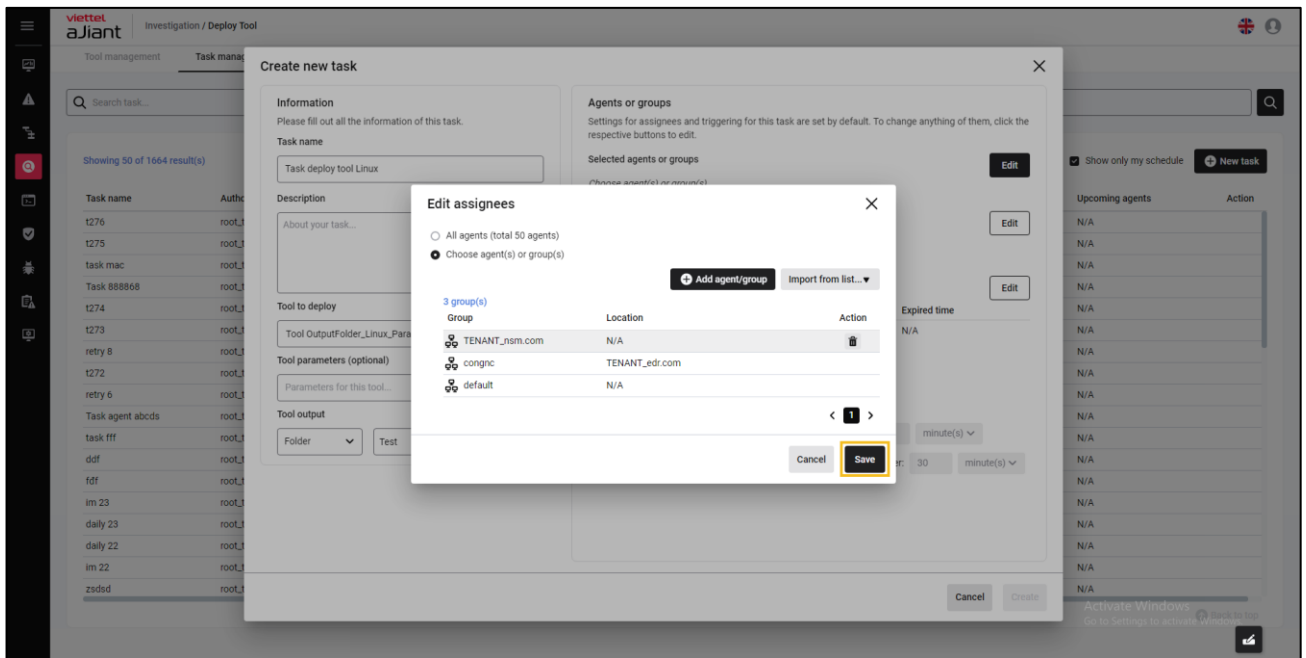
- Chọn group(s) để deploy bằng cách tích chọn vào một hoặc nhiều group(s) > Thông tin group(s) đã được chọn hiển thị ở khung **Selected** > chọn **Cancel** để hủy thao tác thêm group(s) để deploy hoặc chọn nút **Save** để xác nhận danh sách group(s):



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

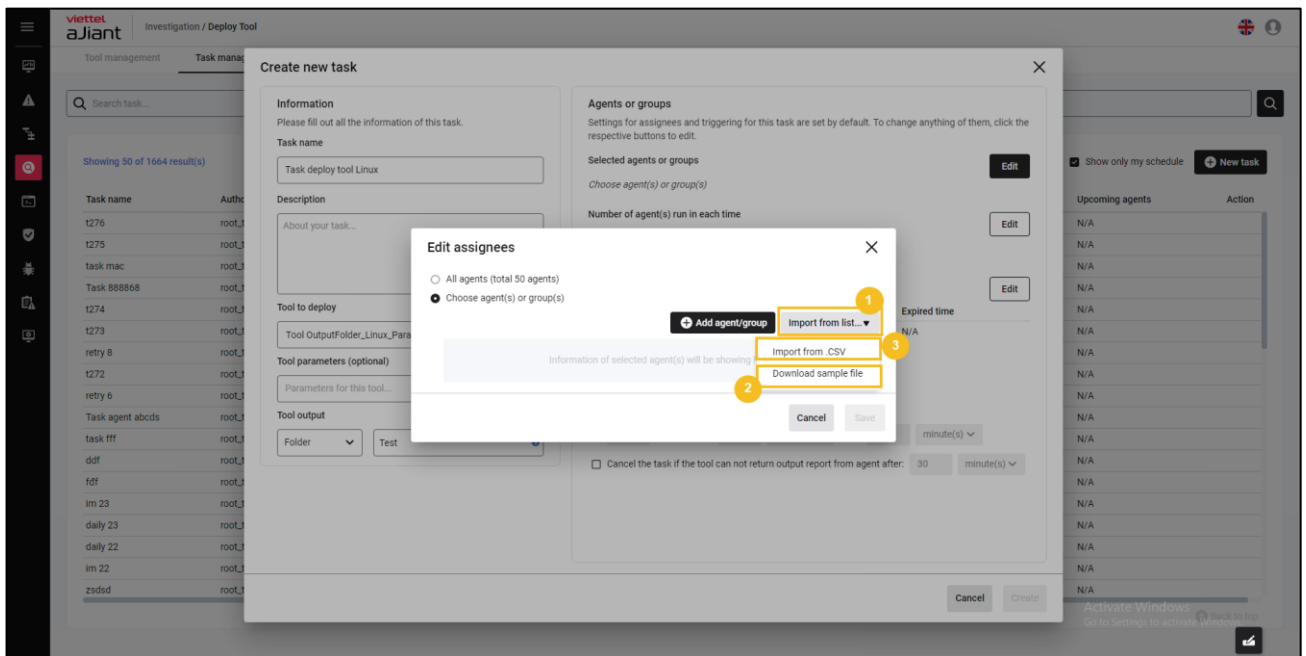


- Chọn **Cancel** để hủy hoặc Chọn **Save** các group(s) đã chọn để deploy:



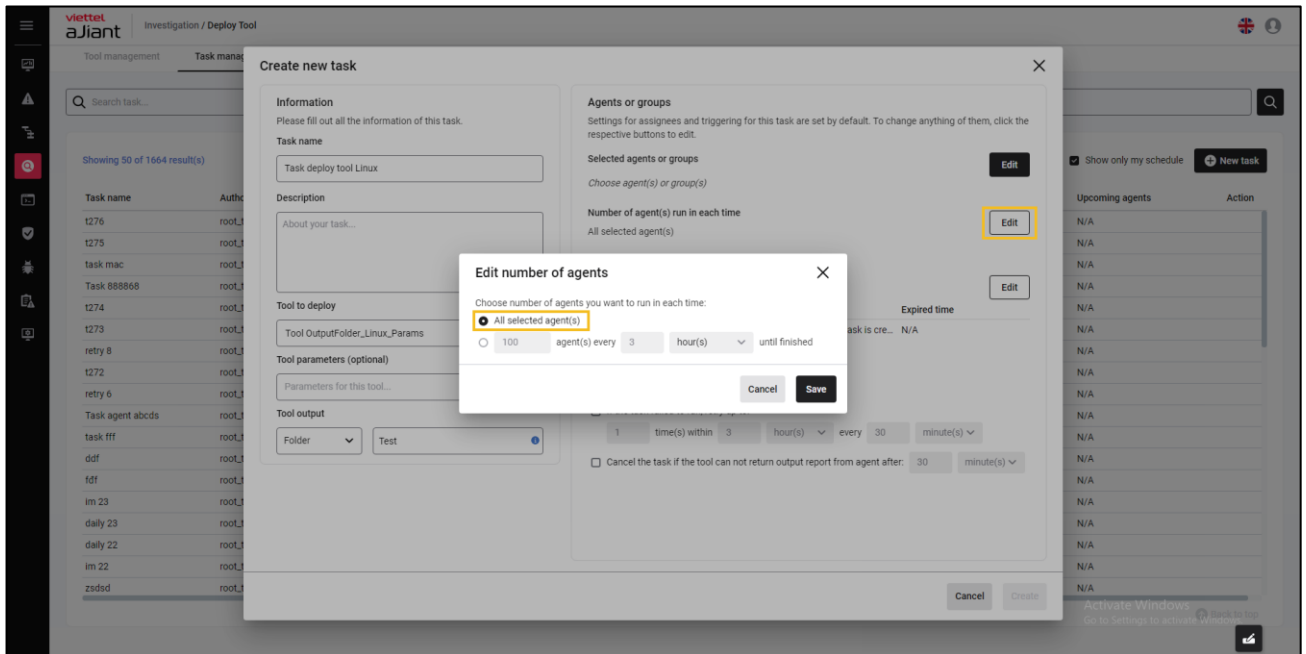
+ Import from list: Cho phép upload danh sách agent(s) từ file .csv > Chọn **Import from list**

- 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)

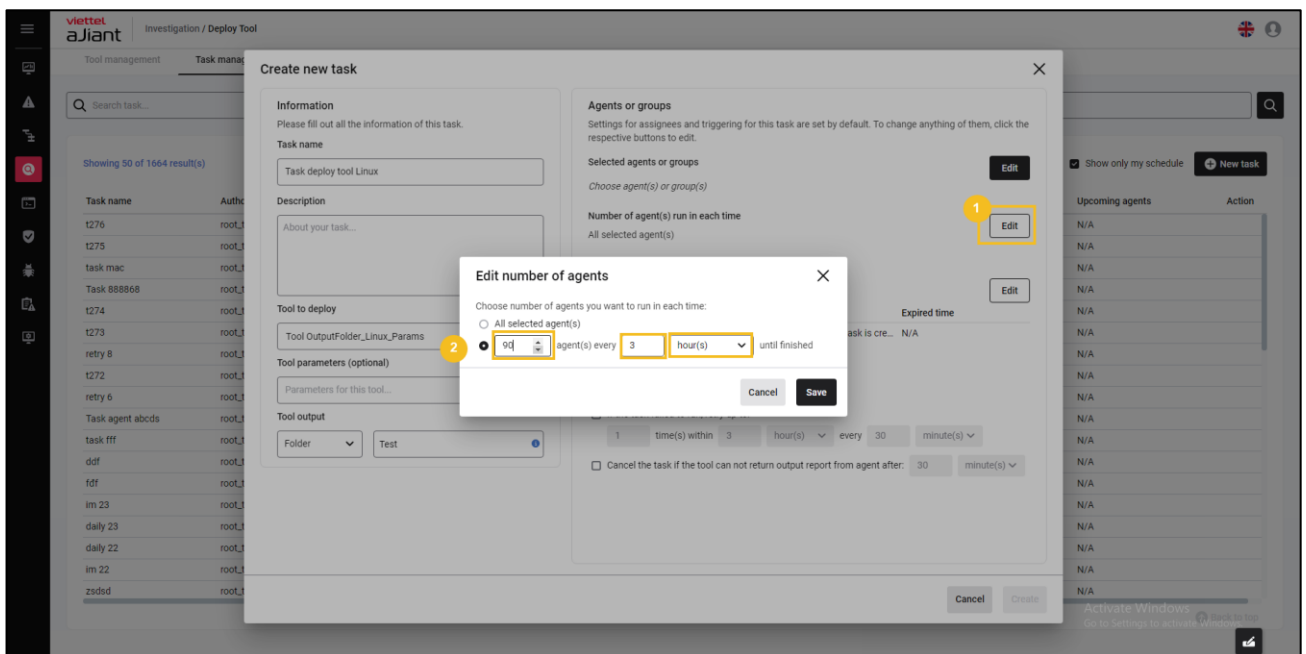


Bước 4: Cấu hình số lượng agent deploy tool mỗi lần:

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

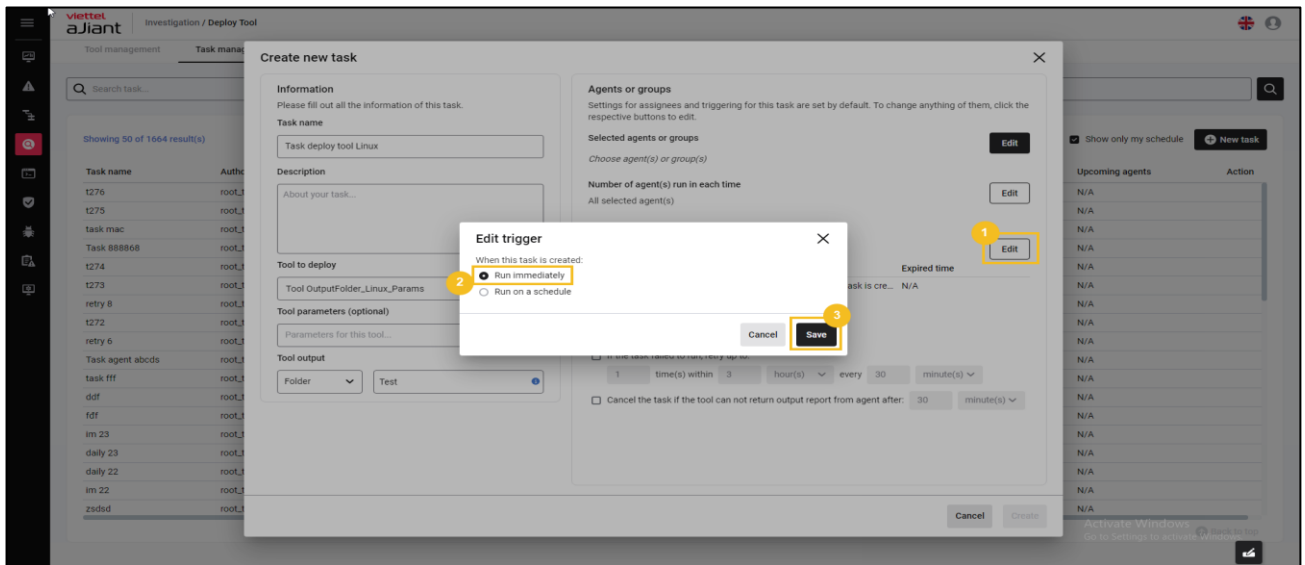


+ Cấu hình số lượng agent mỗi lần deploy:



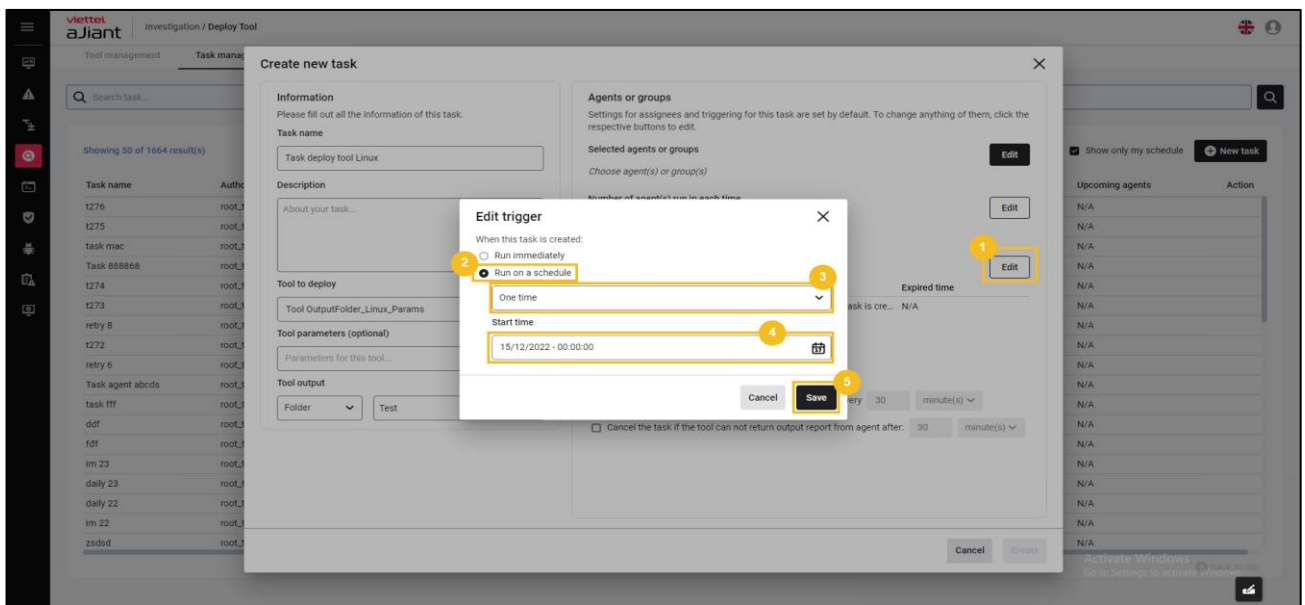
Bước 5: Cấu hình thông tin thời gian (lập lịch) thực hiện deploy tool:

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

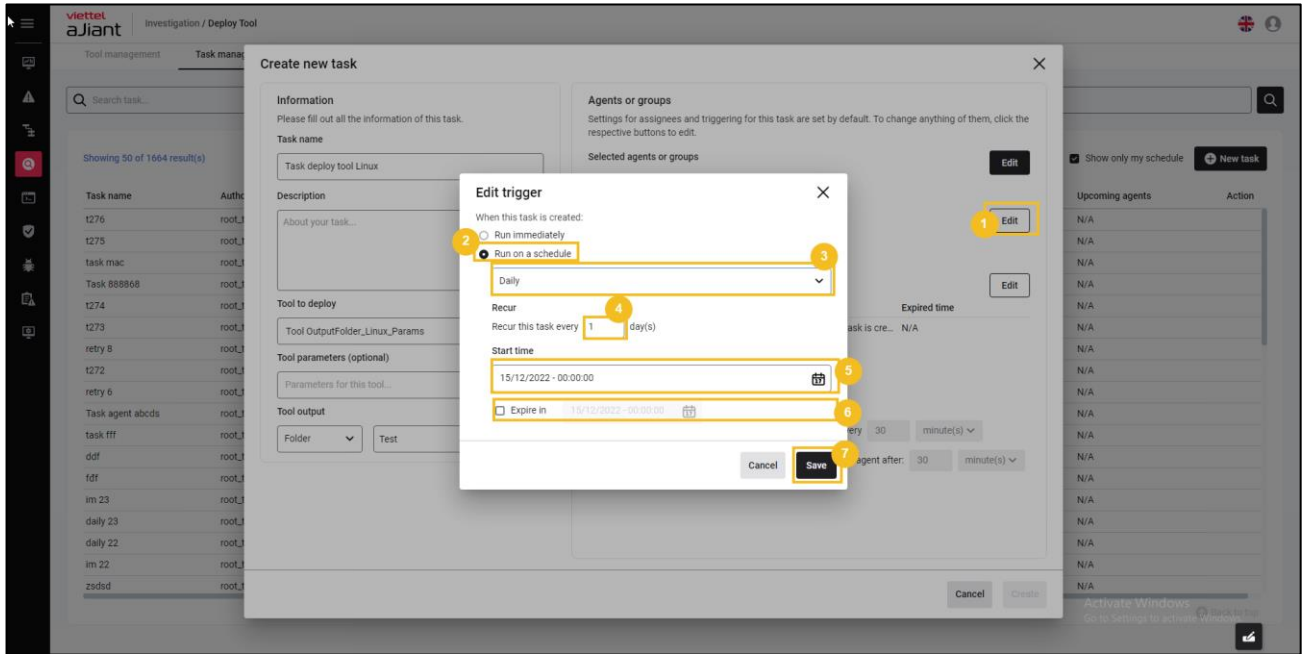


+ Chọn **Run on schedule** để thực hiện cấu hình thời gian deploy tool theo **lập lịch**:

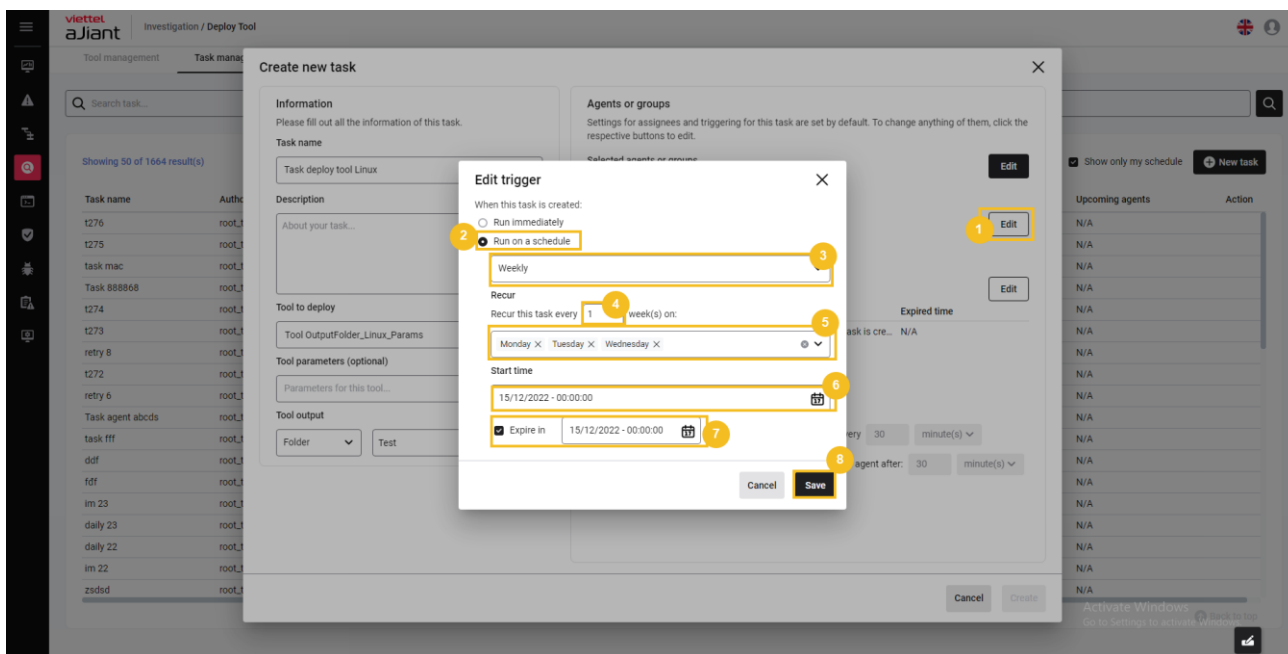
- Chọn schedule **One time**:
 - Cho phép lập lịch deploy tool một lần;
 - Cấu hình thời gian bắt đầu:



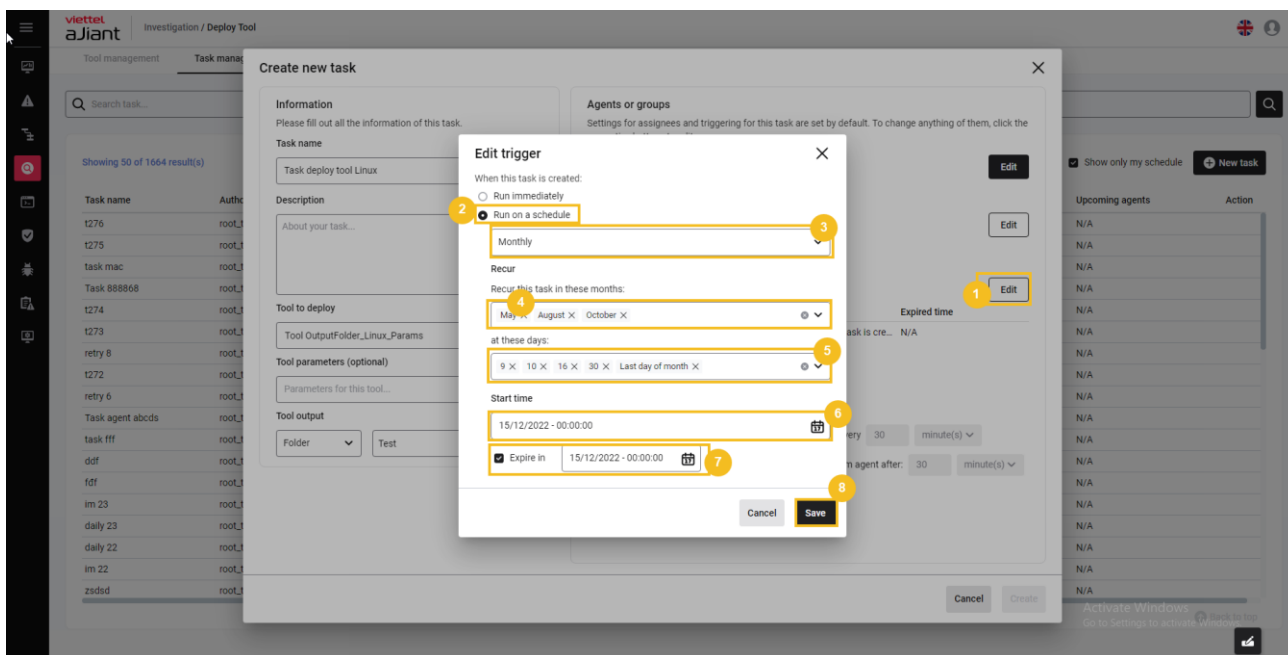
- Chọn schedule **Daily**:
 - Cho phép lập lịch deploy tool hàng ngày;
 - Thời gian lặp lại;
 - Cấu hình thời gian bắt đầu và kết thúc:



- 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:



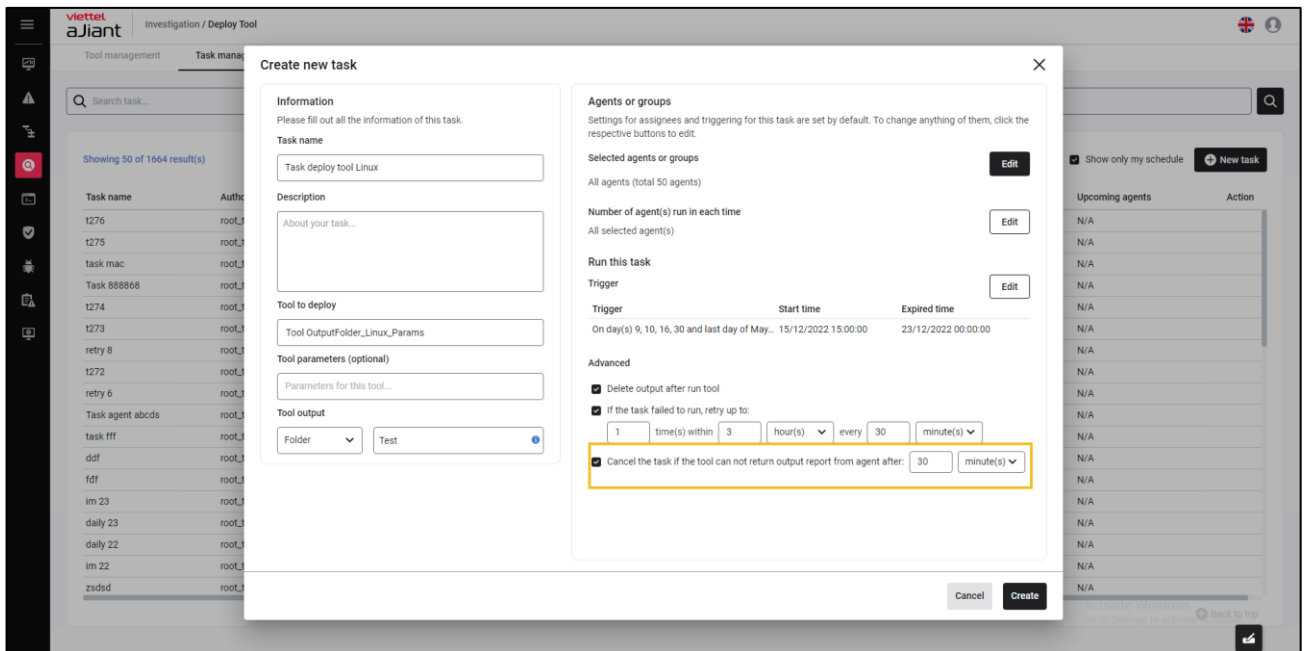
Bước 6: Cấu hình thông tin nâng cao cho task

- + **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)

The screenshot shows the 'Create new task' dialog in the Viettel aJiant interface. The 'Advanced' section is highlighted, showing the following configuration:

- ☒ Delete output after run tool
- ☒ If the task failed to run, retry up to: 1 time(s) within 3 hour(s) every 30 minute(s)
- ☒ Cancel the task if the tool can not return output report from agent after: 30 minute(s)

- + **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:



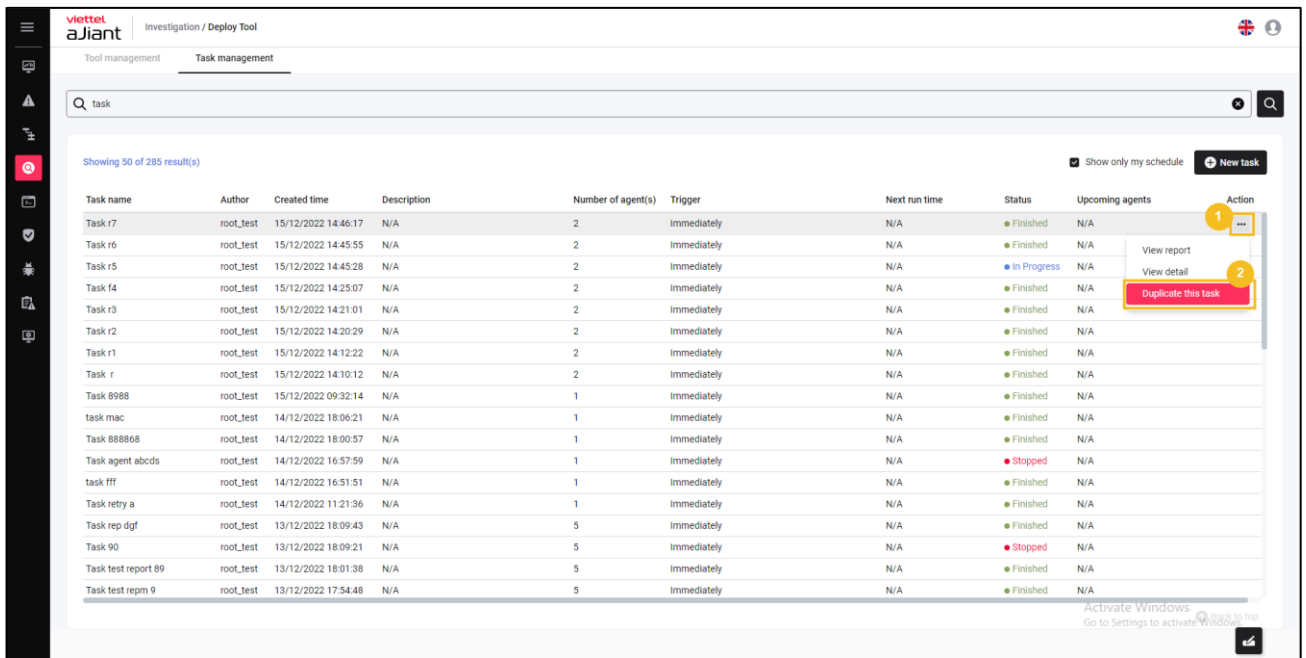
Chọn **Create** để tạo mới task/ cấu hình thông tin deploy tool dưới agent hoặc chọn **Cancel** để hủy task/ hủy cấu hình thông tin deploy tool dưới agent

d. Nhân bản task (Duplicate task)

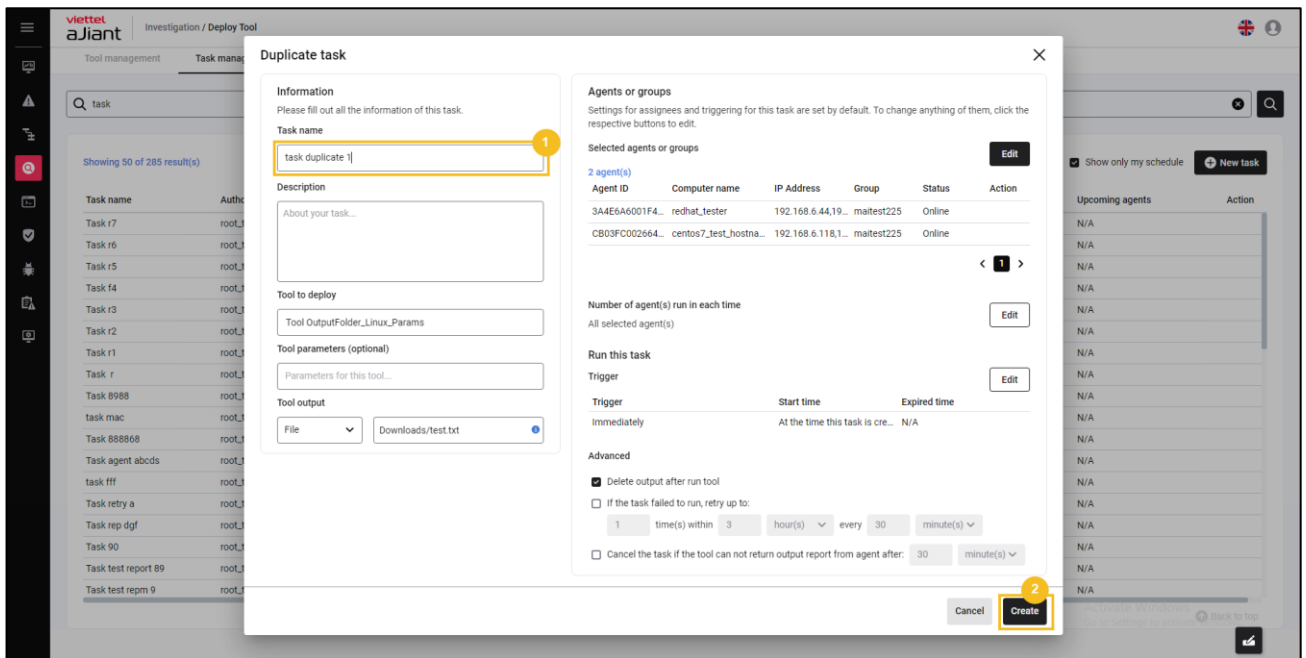
Mục đích: Cho phép nhân bản task (sao chép task), tự động điền các giá trị như task gốc ngoại trừ trường Task name (Yêu cầu người dùng nhập/ sửa lại tên tasks);

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

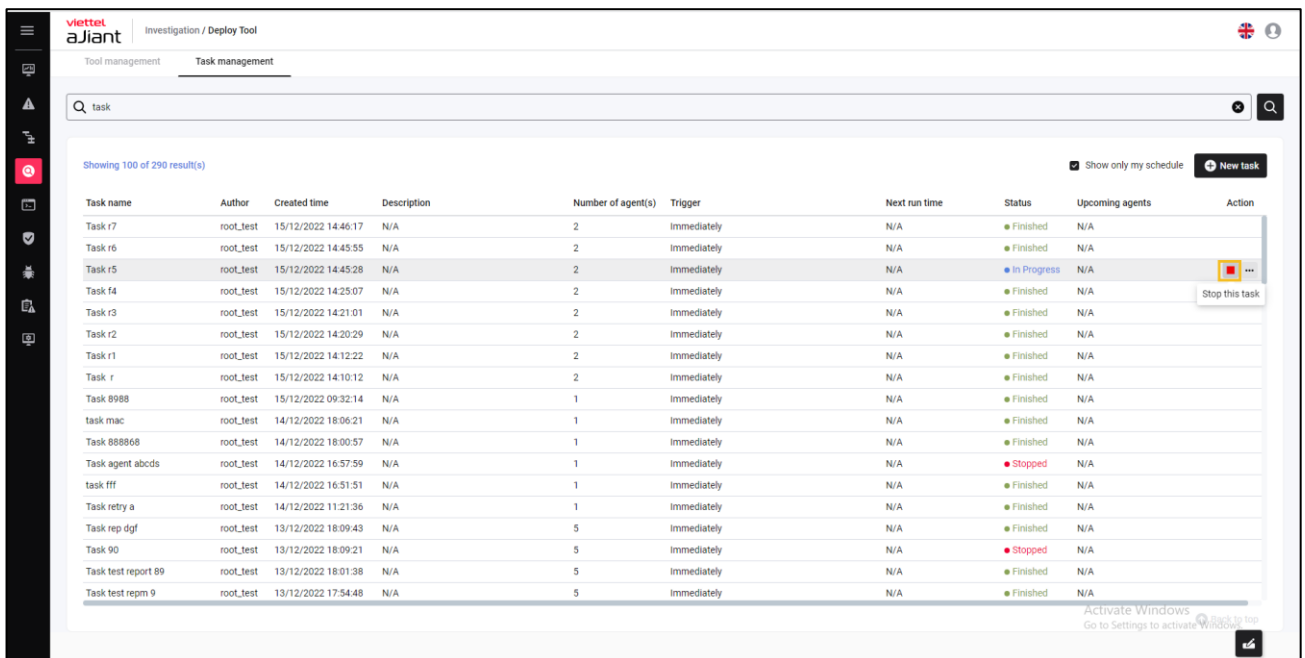
Mục đích: Cho phép hiển thị danh sách Agents sắp được deploy tool;

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	 ... Stop this task
Task r4	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 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:

Investigation / Deploy Tool

Task management

Showing 100 of 290 result(s)

Show only my schedule New task

Task name	Author	Created time	Description	Number of agent(s)	Trigger	Next run time	Status	Upcoming agents	Action
Task immediately 989	root_test	07/12/2022 14:49:13	N/A	1	Immediately	N/A	Stopped	N/A	
Task 8955455	root_test	07/12/2022 13:55:58	N/A	1	Immediately	N/A	Finished	N/A	
Task Monthly MacOS	root_test	06/12/2022 18:25:02	N/A	1	On day(s) 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 of Nov...	07/11/2023 09:00:00	In Progress	N/A	
Task weekly MacOS	root_test	06/12/2022 18:23:59	N/A	1	On Mondays, Tuesdays, Wednesdays, Thursdays, ...	16/12/2022 09:00:00	In Progress	N/A	
Task MacOS daily 1	root_test	06/12/2022 18:23:17	N/A	1	Every 1 day(s) at 09:00:00	16/12/2022 09:00:00	In Progress	N/A	
Task 7647657465	root_test	06/12/2022 17:57:36	N/A	1	Immediately	N/A	Finished	N/A	
new task 8	root_test	06/12/2022 17:56:16	N/A	1	Immediately	N/A	Finished	N/A	
new task 6	root_test	06/12/2022 17:50:15	N/A	1	Immediately	N/A	Finished	N/A	
new task 4	root_test	06/12/2022 17:43:13	N/A	1	Immediately	N/A	Finished	N/A	
Task macosvb 1	root_test	06/12/2022 16:41:35	N/A	1	Immediately	N/A	Stopped	N/A	
Task monthly dai	root_test	06/12/2022 15:18:38	N/A	1	On day(s) 7, 8, 9, 10, 11, 12 of December at 09:00:00	N/A	Stopped	N/A	
Task abfbvrvf	root_test	06/12/2022 13:58:21	N/A	1	Immediately	N/A	Finished	N/A	Run this task
New task 2	root_test	06/12/2022 11:14:48	Description	52	On Mondays, Wednesday every 1 week(s) at 12:00:00	19/12/2022 12:00:00	In Progress	N/A	
Task 787878f	root_test	06/12/2022 11:11:58	N/A	1	Immediately	N/A	Finished	N/A	
New task 1	root_test	06/12/2022 11:11:42	Description	48	Immediately	N/A	Finished	N/A	
Task test retry 132	root_test	06/12/2022 10:49:15	N/A	1	Immediately	N/A	Finished	N/A	
Task abfbvrvf	root_test	06/12/2022 13:58:21	N/A	1	Immediately	N/A	Finished	N/A	
New task 2	root_test	06/12/2022 11:14:48	Description	52	On Mondays, Wednesday every 1 week(s) at 12:00:00	19/12/2022 12:00:00	In Progress	N/A	

Activate Windows Go to Settings to activate Windows. Back to top

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**:

Investigation / Deploy Tool

Task management

Showing 100 of 290 result(s)

View task detail

General

Name Task immediately 989

Description N/A

Tool to deploy Bichpt3_Hello.exe

Parameters N/A

Output type none

Output path N/A

Agents & groups

Assignees

1 agent(s)

Agent ID	Computer name	IP Address	Group	Status
97617AC1A609458E...	Maingocwinx64	192.168.74.128	mailest225	Online

Number of agent(s) run in each time

All choosing agent(s)

Run this task

Trigger

Trigger	Start time	Expired time
Immediately	At the time this task is created.	N/A

Advance

Retry None

Timeout None

Activate Windows Go to Settings to activate Windows.

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 Cyber Security aJiant interface. On the left, the 'Task management' section shows a list of tasks with columns for Task name, Author, Created time, and Description. A task named 'New task 2' is highlighted. On the right, the 'View report - New task 2' window is open, showing a summary of the task's status (Total agents: 51, Success: 1) and a detailed table of results. The table includes columns for Agent ID, Computer name, IP Address, Tool exit code, Status, Message, and Action. The results show various agents with different statuses, including 'Failed', 'Success', and '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
8E03ADB705FF8...	virtualAgent_mai...	172.17.0.2	N/A	Failed	Platform invalid (Tool wind.)	
A6ED648CC1C17...	virtualAgent_mai...	172.17.0.5	N/A	Failed	Platform invalid (Tool wind.)	
AA657D644FF8C...	virtualAgent_mai...	172.17.0.11	N/A	Failed	Platform invalid (Tool wind.)	
210352BC56C0B...	macOS-Mais-Mac...	192.168.74.1...	N/A	Failed	Platform invalid (Tool wind.)	
71BC4C742BB32...	virtualAgent_mai...	172.17.0.4	N/A	Failed	Platform invalid (Tool wind.)	
E450A71C08FD...	virtualAgent_mai...	172.17.0.3	N/A	Failed	Platform invalid (Tool wind.)	
3CAD1ACA8489...	virtualAgent_mai...	172.17.0.7	N/A	Failed	Platform invalid (Tool wind.)	
07718463D55E5...	virtualAgent_mai...	172.17.0.10	N/A	Failed	Platform invalid (Tool wind.)	
6C648D7431177...	virtualAgent_mai...	172.17.0.9	N/A	Failed	Platform invalid (Tool wind.)	
556075243054B...	virtualAgent_mai...	172.17.0.8	N/A	Failed	Platform invalid (Tool wind.)	
60BE442B80298...	virtualAgent_mai...	172.17.0.6	N/A	Failed	Platform invalid (Tool wind.)	
97617AC1A6094...	Maingocwinx64	192.168.74.1...	0	Success	N/A	

Activate Windows
Go to Settings to activate Windows

The tool results is going to be deleted automatically after 2 months for saving resources

+ 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 290 result(s)

Task name	Author	Created time	Description
Task weekly MacOS	root_test	06/12/2022 18:23:59	N/A
Task MacOS daily 1	root_test	06/12/2022 18:23:17	N/A
Task 7647657465	root_test	06/12/2022 17:57:36	N/A
new task 8	root_test	06/12/2022 17:56:16	N/A
new task 6	root_test	06/12/2022 17:50:15	N/A
new task 4	root_test	06/12/2022 17:43:13	N/A
Task macosvb 1	root_test	06/12/2022 16:41:35	N/A
Task monthly dai	root_test	06/12/2022 15:18:38	N/A
Task abfbvrf	root_test	06/12/2022 13:58:21	N/A
New task 2	root_test	06/12/2022 11:14:48	Description
Task 787878f	root_test	06/12/2022 11:11:58	N/A
New task 1	root_test	06/12/2022 11:11:42	Description
Task test retry 132	root_test	06/12/2022 10:49:15	N/A
Task abfbvrf	root_test	06/12/2022 13:58:21	N/A
New task 2	root_test	06/12/2022 11:14:48	Description
Task 787878f	root_test	06/12/2022 11:11:58	N/A
New task 1	root_test	06/12/2022 11:11:42	Description
Task test retry 132	root_test	06/12/2022 10:49:15	N/A

Showing 12 of 12 results

Agent ID	Computer name	IP Address	Tool exit code	Status	Message	Action
8E03ADB705FF8...	virtualAgent_mai...	172.17.0.2	N/A	Failed	Platform invalid (Tool wind.)	
A6ED648CC1C17...	virtualAgent_mai...	172.17.0.5	N/A	Failed	Platform invalid (Tool wind.)	
AA657D644FF8C...	virtualAgent_mai...	172.17.0.11	N/A	Failed	Platform invalid (Tool wind.)	
210352BC56C0B...	macOS-Mais-Mac...	192.168.74.1...	N/A	Failed	Platform invalid (Tool wind.)	
71BC4C742BB32...	virtualAgent_mai...	172.17.0.4	N/A	Failed	Platform invalid (Tool wind.)	
E450A71C08FD...	virtualAgent_mai...	172.17.0.3	N/A	Failed	Platform invalid (Tool wind.)	
3CAD1ACA8489...	virtualAgent_mai...	172.17.0.7	N/A	Failed	Platform invalid (Tool wind.)	
07718463D55E5...	virtualAgent_mai...	172.17.0.10	N/A	Failed	Platform invalid (Tool wind.)	
6C648D7431177...	virtualAgent_mai...	172.17.0.9	N/A	Failed	Platform invalid (Tool wind.)	
556075243054B...	virtualAgent_mai...	172.17.0.8	N/A	Failed	Platform invalid (Tool wind.)	
60BE442B80298...	virtualAgent_mai...	172.17.0.6	N/A	Failed	Platform invalid (Tool wind.)	
97617AC1A6094...	Maingocwinx64	192.168.74.1...	0	Success	N/A	

Activate Windows
Go to Settings to activate Windows

The tool results is going to be deleted automatically after 2 months for saving resources

+ 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**:

The screenshot displays the Viettel Cyber Security aJiant interface. On the left, there's a sidebar with navigation icons. The main area is divided into two sections: 'Task management' and 'View report - New task 2'. The 'Task management' section shows a list of tasks with columns for Task name, Author, Created time, and Description. The 'View report - New task 2' section shows a detailed report for a specific task, including a table of agents and their deployment status. The 'Get report' button is highlighted in the top right corner of the report window.

+ 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**

The screenshot displays the Viettel aJiant security management interface. On the left, the 'Task management' tab is active, showing a list of tasks with columns for Task name, Author, Created time, and Description. The main panel on the right shows the 'View report - New task 2' for the date 14/12/2022 - 12:00:00. It includes a summary of agents (Total agents: 51, Success: 1) and a detailed table of results. A red box highlights the 'Download outputs' button, and a yellow box highlights the 'Get report' button. The table lists various computer names, IP addresses, tool exit codes, and statuses (Failed or Success).

Computer name	IP Address	Tool exit code	Status	Message	Action
8E03AD8705FF8...	virtualAgent_mai...	172.17.0.2	N/A	Failed	Platform invalided (Tool: wind.
A6ED648CC1C17...	virtualAgent_mai...	172.17.0.5	N/A	Failed	Platform invalided (Tool: wind.
AA657D644FFBC...	virtualAgent_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.
71BC4C742BB32...	virtualAgent_mai...	172.17.0.4	N/A	Failed	Platform invalided (Tool: wind.
E450A71CC08FD...	virtualAgent_mai...	172.17.0.3	N/A	Failed	Platform invalided (Tool: wind.
3CAD1ACA8489...	virtualAgent_mai...	172.17.0.7	N/A	Failed	Platform invalided (Tool: wind.
07718463D55E5...	virtualAgent_mai...	172.17.0.10	N/A	Failed	Platform invalided (Tool: wind.
6C648D7431177...	virtualAgent_mai...	172.17.0.9	N/A	Failed	Platform invalided (Tool: wind.
556075243054B...	virtualAgent_mai...	172.17.0.8	N/A	Failed	Platform invalided (Tool: wind.
60BE442B0298...	virtualAgent_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 thống kê báo cáo kết quả deploy tool tại từng lần lập lịch (định dạng .csv)
- Các bước thực hiện: Tại màn hình View report, chọn icon bản ghi lập lịch mà người dùng muốn download báo cáo > Chọn **Get report**

View report - New task 2

14/12/2022 - 12:00:00

Total agents: 51
Success: 1

Download outputs

Get report

Agent ID	Computer name	IP Address	Tool exit code	Status	Message	Action
8E03AD8705FF8...	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.	
71BC4C742BB32...	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.	
60BE442B80298...	virtual_agent_mai...	172.17.0.6	N/A	Failed	Platform invalided (Tool: wind.	
97617AC1A6094...	Maingocwinx64	192.168.74.1...	0	Success	N/A	

Activate Windows
Go to Settings to activate Windows.

The tool results is going to be deleted automatically after 2 months for saving resources

+ 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**

View report - New task 2

14/12/2022 - 12:00:00

Total agents: 51
Success: 1

Download outputs

Get report

Agent ID	Computer name	IP Address	Tool exit code	Status	Message	Action
8E03AD8705FF8...	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.	
71BC4C742BB32...	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.	
60BE442B80298...	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 output

Activate Windows
Go to Settings to activate Windows.

The tool results is going to be deleted automatically after 2 months for saving resources

+ 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**

cần xem báo cáo (có trạng thái Success) > chọn icon > Chọn **Download output**

The screenshot displays the Viettel aJiant interface. On the left, the 'Task management' tab is active, showing a list of tasks with columns for Task name, Author, Created time, and Description. On the right, the 'View report - New task 2' window is open, showing a table of agent results. The table has columns for Agent ID, Computer name, IP Address, Tool exit code, Status, Message, and Action. A specific agent is highlighted, and a dropdown menu is visible with the option 'Download output' selected.

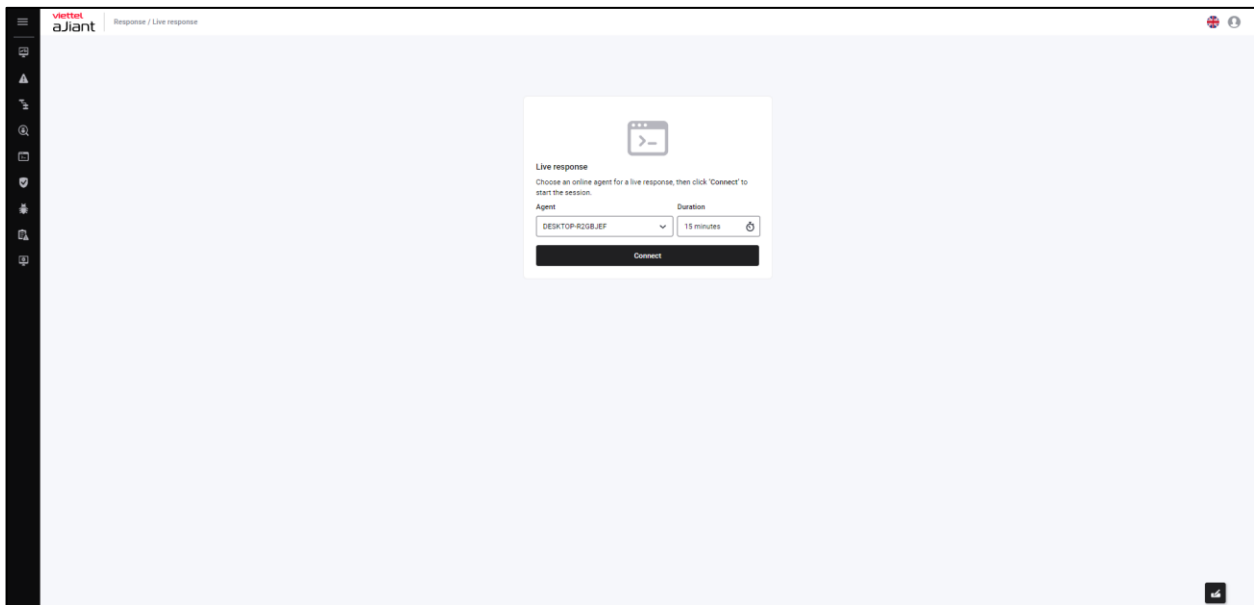
3.5 Nhóm chức năng Response

3.5.1 Live Response

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

Các bước thực hiện chức năng Live Response:

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



Bước 2: Thực hiện tạo mới 1 phiên live response

Chọn Agent: Hiển thị danh sách các agent:

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

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



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

Duration

15 minutes 

5 minutes

✓ 15 minutes

1 hour

3 hours

+ Click nút “Connect”:



Live response
Choose an online agent for a live response, then click 'Connect' to start the session.

Agent Duration 2

1 DESKTOP-R2GBJEF 15 minutes 

Connect 3

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

Connect to agent
Choose an online agent for a live response, then click 'Connect' to start the session.

Agent Duration

DESKTOP-R2GBJEF 5 minutes 

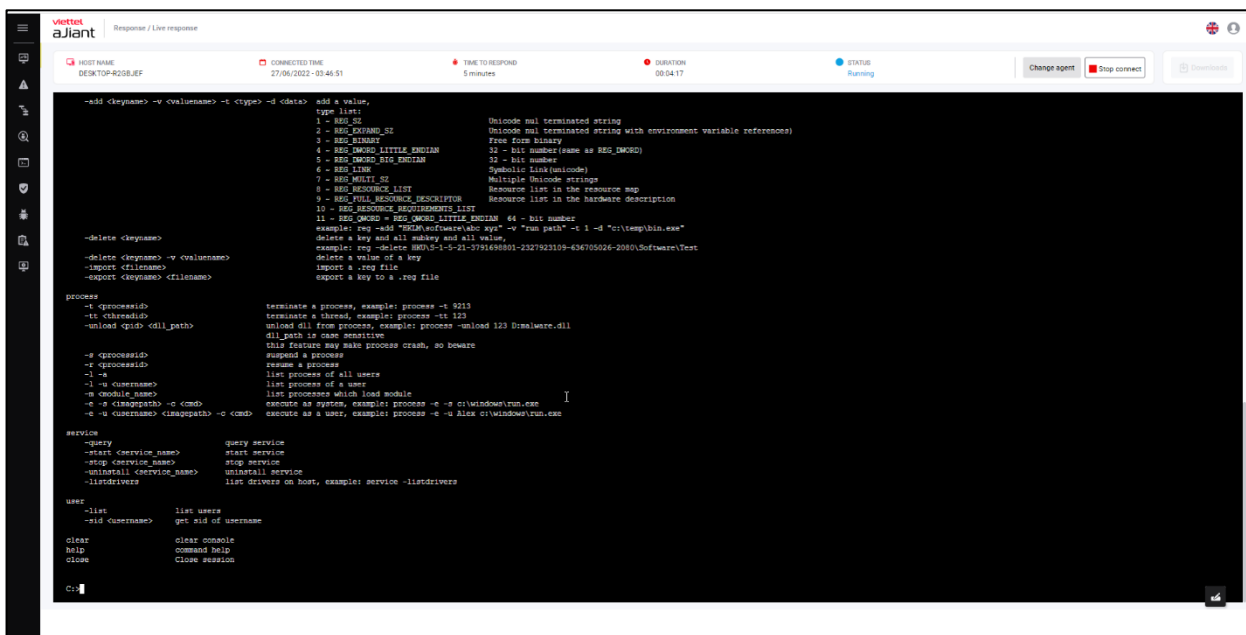
Connecting...

Connecting to agent... (expire in 00:58)

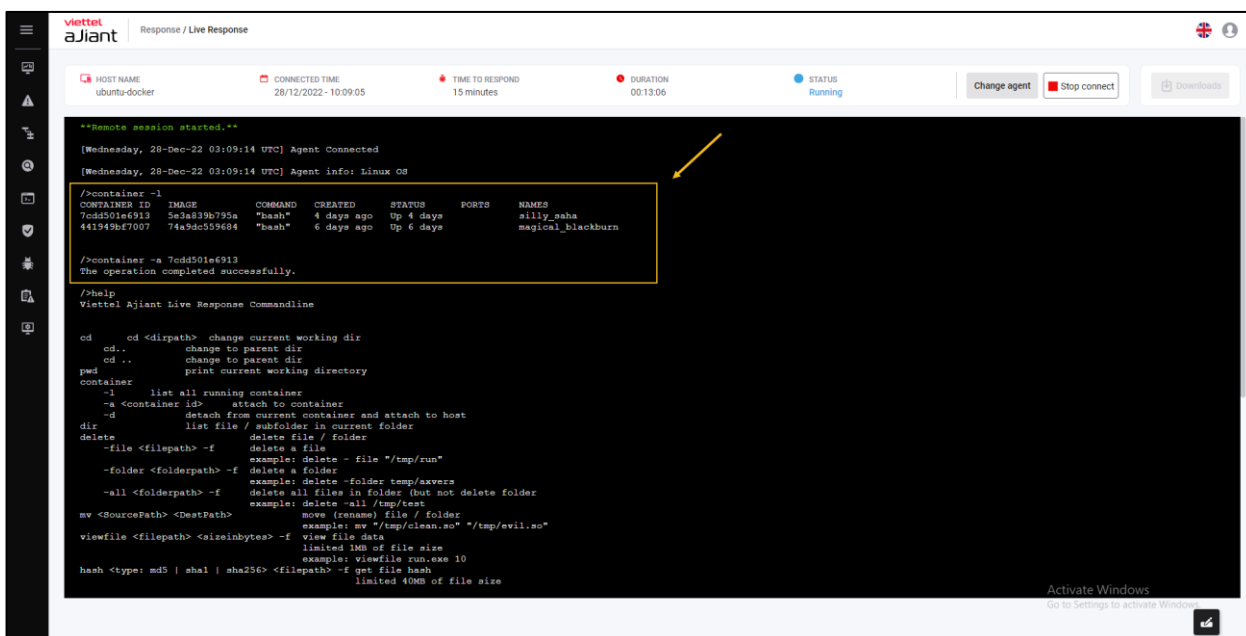
Cancel connection

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	

<i>STT</i>	<i>Các lệnh</i>	<i>Tham số</i>	<i>Mô tả</i>
		/O:[-]sortorder List by files in sorted order. sortorder 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	

STT	Các lệnh	Tham số	Mô tả
		/R Display alternate data streams of the file. Ví dụ: dir /R	
		/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	Cho phép di chuyển file/ folder

STT	Các lệnh	Tham số	Mô tả
		Ví dụ: example: mv "c:\temp\clean.exe" "c:\temp\evil.exe"	
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

STT	Các lệnh	Tham số	Mô tả
		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

STT	Các lệnh	Tham số	Mô tả
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

STT	Các lệnh	Tham số	Mô tả
		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

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

STT	Các lệnh	Tham số	Mô tả
		-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: example: hash md5 c:\test\run.exe	Cho phép mã hóa file tối đa 1MB Option -f để buộc mở tệp khi tệp đang được mở bởi một quy trình khác
8	get	<filepath>	Upload 1 file từ host lên server
9	put	<url><folderpath>	Download 1 file tới máy host
10	mkdir	<dir name>	Tạo 1 thư mục
11	process		Các lệnh liên quan đến process
		-t <processid>	Tắt 1 tiến trình đang chạy theo ID tiến trình
		-s <processid>	Tạm dừng 1 tiến trình

STT	Các lệnh	Tham số	Mô tả
		-r <processid>	Hồi phục lại 1 tiến trình đã bị tạm dừng trước đó
		-l -a	Liệt kê toàn bộ các process của tất cả các user
		-l -u <username>	Liệt kê các process của 1 user
		-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

STT	Các lệnh	Tham số	Mô tả
		-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

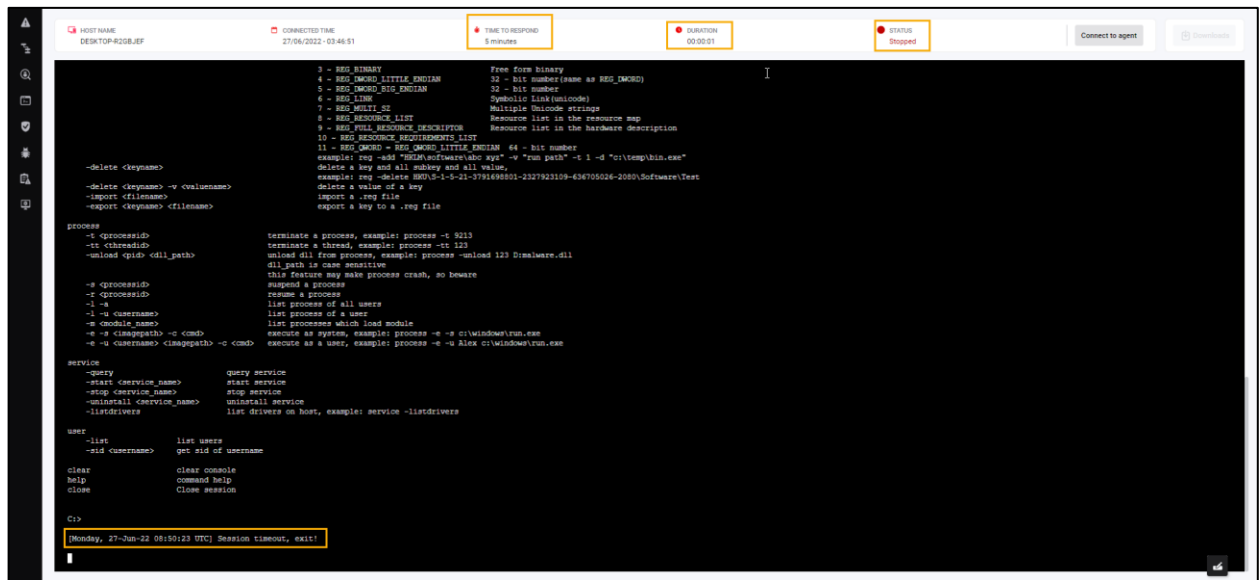
Một số lưu ý khi làm việc với các lệnh trên màn hình console:

+ 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”;

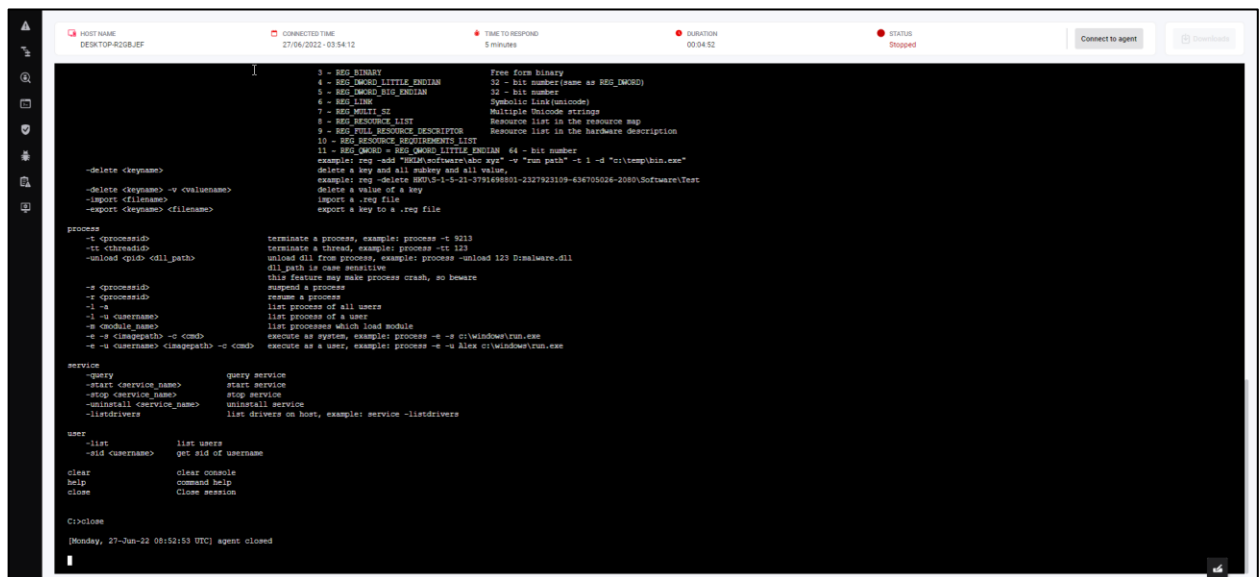
+ Lệnh get <filepath>: ví dụ: get procexp.exe trong màn hình console thì kết quả lấy file về được hiển thị ở màn hình Attachment Log ở phía dưới góc bên phải của màn hình. Người dùng được phép tải file về trình duyệt hoặc xóa file đã lấy về server.

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.

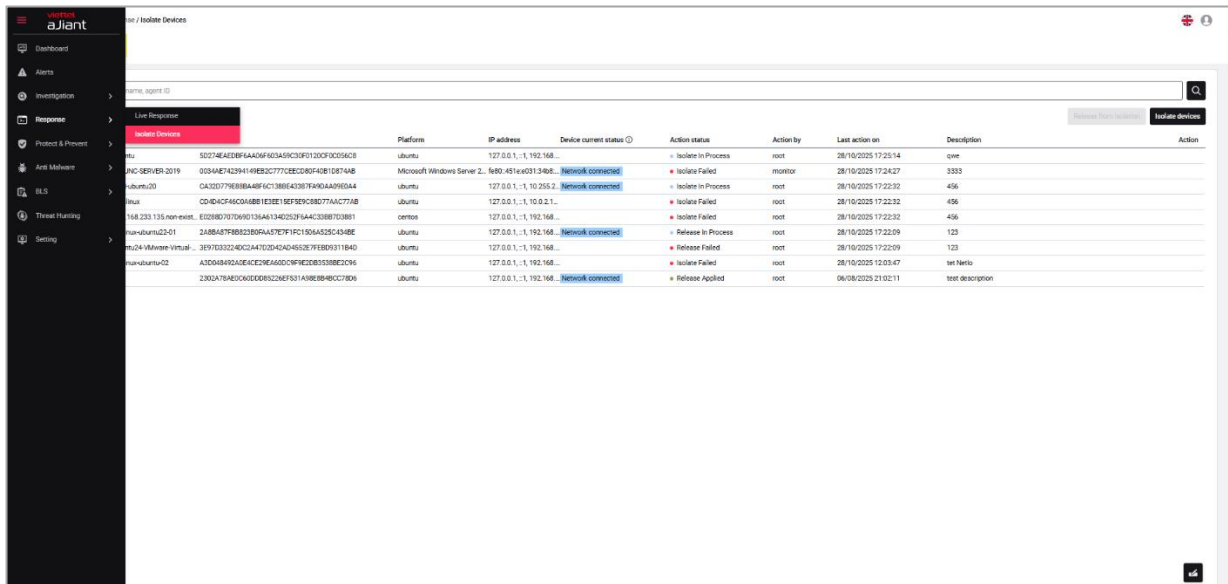


3.5.2 Isolate Devices

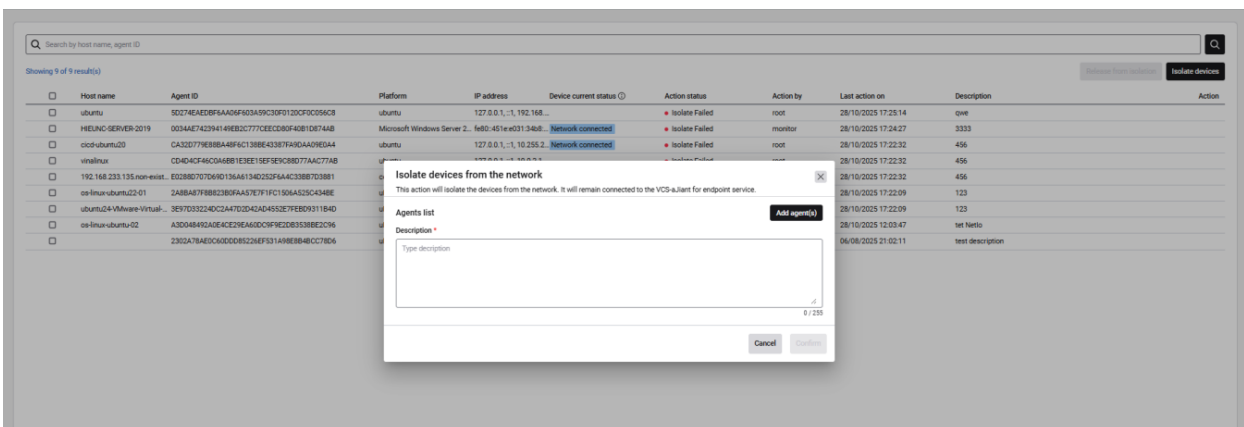
Mục đích: Cho phép SOC cô lập một thiết bị nghi ngờ bị xâm nhập khỏi mạng. Mục tiêu chính là ngăn chặn sự lây lan của mã độc, hạn chế giao tiếp nguy hiểm, đồng thời duy trì kết nối giữa thiết bị và hệ thống VCS-aJiant để tiếp tục điều tra, thu thập bằng chứng và khôi phục thiết bị.

Tạo lệnh Isolate devices (cô lập)

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



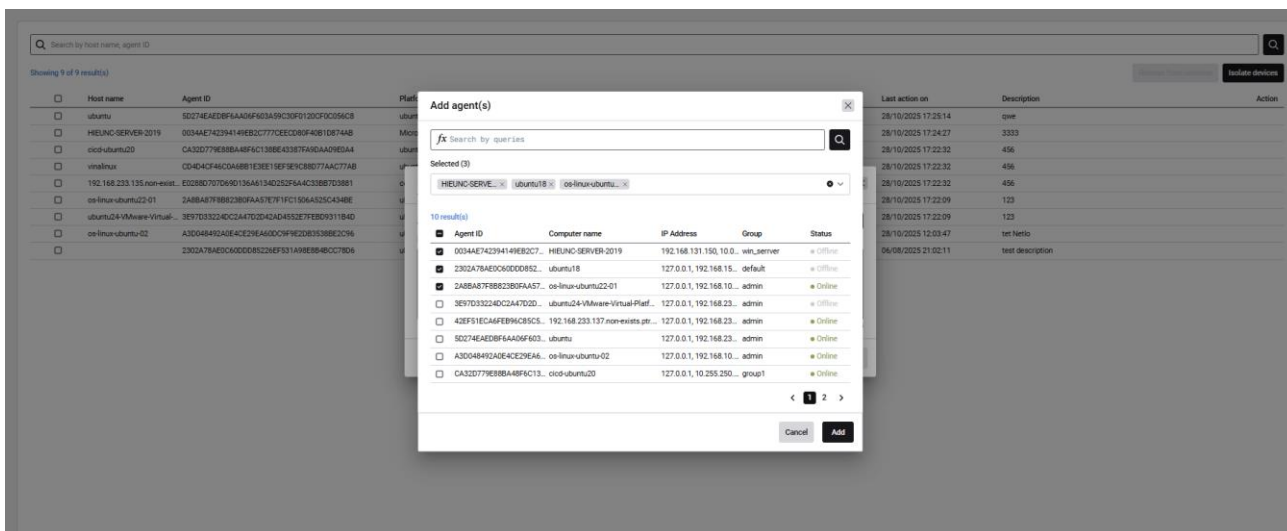
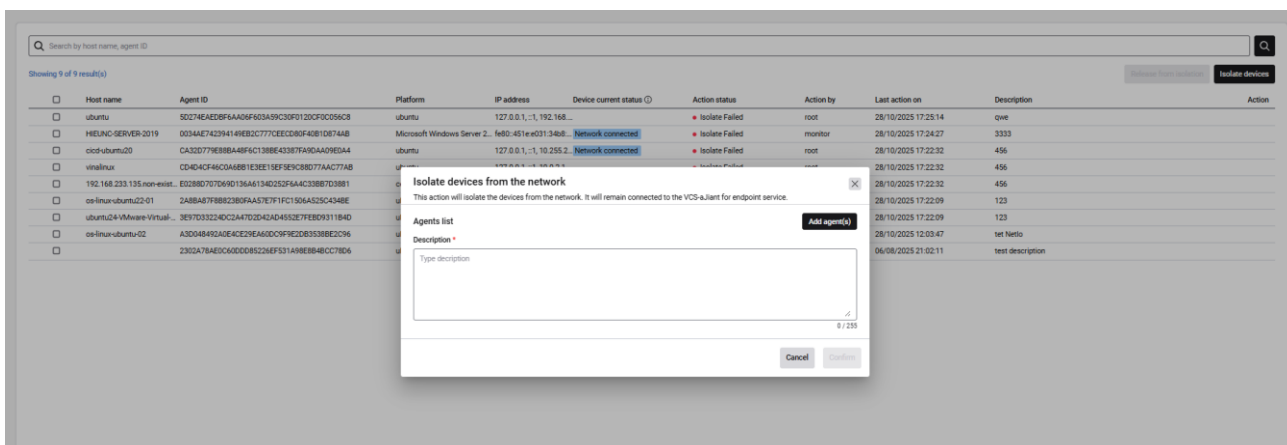
Bước 2: Chọn button Isolate devices



Bước 3: Nhập các thông tin cần thiết bao gồm

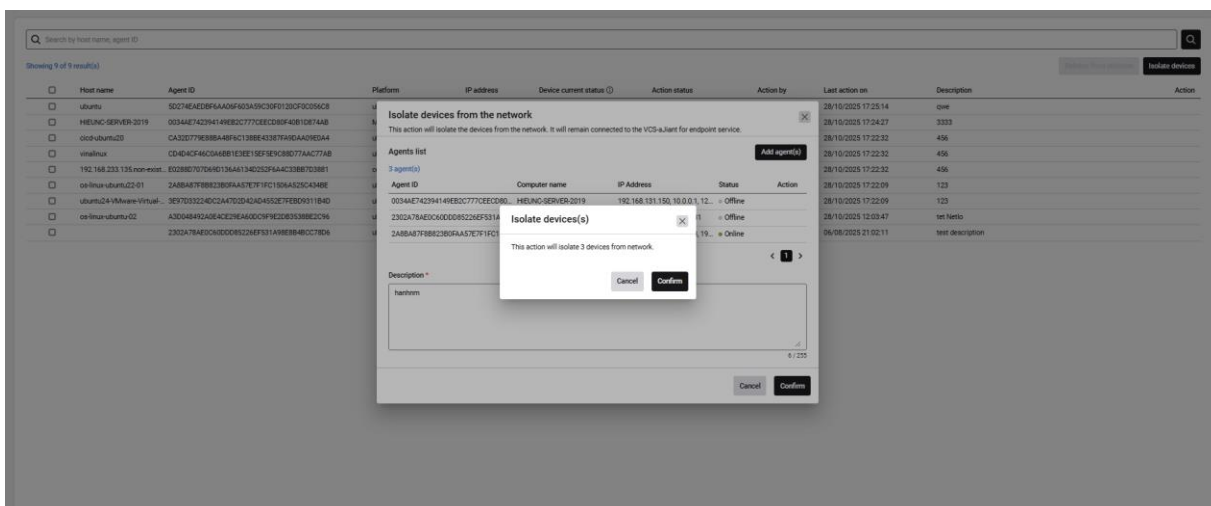
- Mô tả (bắt buộc)
- Chọn Agent(s)

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



Bước 4: Xác nhận cô lập thiết bị

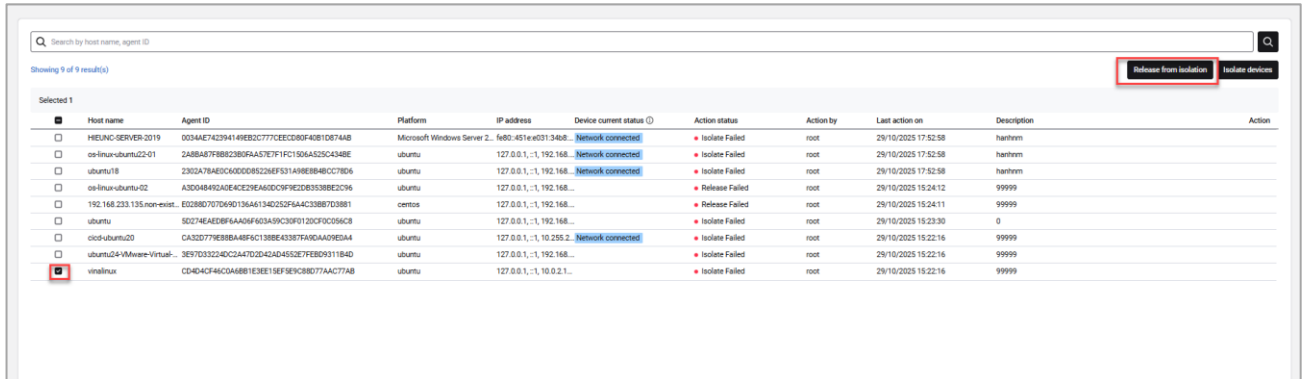
Người dùng nhấn Confirm để xác nhận thực hiện cô lập thiết bị.



Tạo lệnh Release isolation (bỏ cô lập)

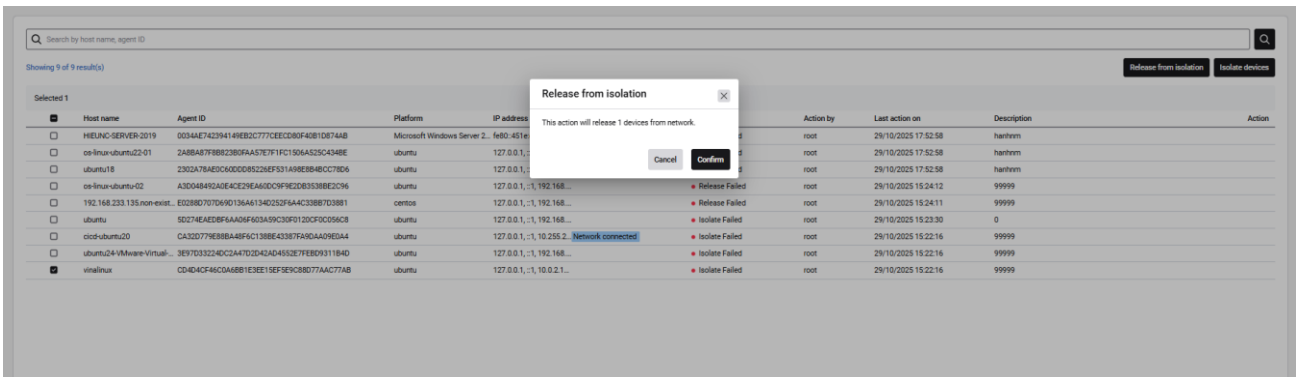
Người dùng có thể bỏ cô lập thiết bị như sau:

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

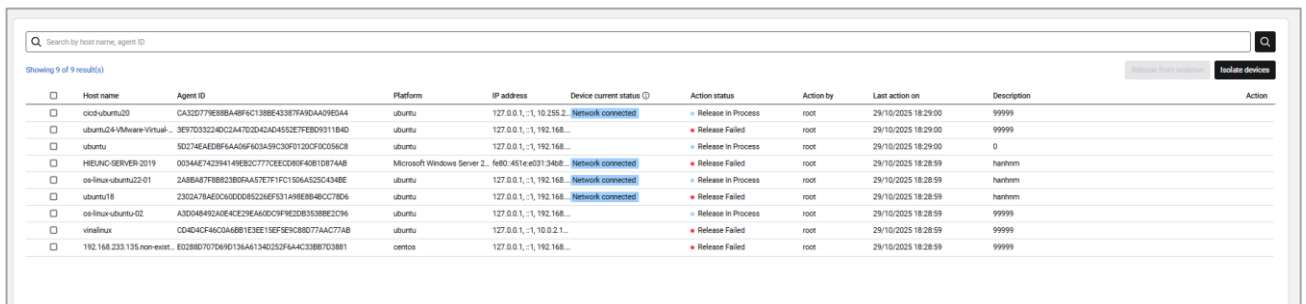


Bước 2: Chọn button Release from isolation-> thực hiện Xác nhận

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



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



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

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

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

Search by host name, agent ID

Showing 9 of 9 result(s)

☐	Host name	Agent ID	Platform	IP address	Device current status	Action status	Action by	Last action on	Description	Action
☐	HELUNG-SERVER-2019	0034AE74294149E8C277CEC8D6F40E1D87448	Microsoft Windows Server 2...	1601-481e4031-3468...	Network connected	Isolate Failed	root	29/10/2025 17:52:58	harthom	
☐	os-linux-ubuntu22-01	24AB4E7F98B23865A457C7F1C1506A325C4348E	ubuntu	127.0.0.1, 192.168...	Network connected	Isolate Failed	root	29/10/2025 17:52:58	harthom	
☐	ubuntu18	2302A78AED3C94EDC8D325F531A9B8B94BC78D6	ubuntu	127.0.0.1, 192.168...	Network connected	Isolate Failed	root	29/10/2025 17:52:58	harthom	
☐	os-linux-ubuntu02	A3D0A8492A0E4CE29E46D0F9E2D3338B2C206	ubuntu	127.0.0.1, 192.168...	Network connected	Release Failed	root	29/10/2025 15:24:12	99999	
☐	192.168.233.135 non-exist...	E028B707D69D136A6134D25F8A4C3BB7D3881	centos	127.0.0.1, 192.168...	Network connected	Release Failed	root	29/10/2025 15:24:11	99999	
☐	ubuntu	5D274EAE0BFAA0A6F603A9C30F0120C7C056C8	ubuntu	127.0.0.1, 192.168...	Network connected	Isolate Failed	root	29/10/2025 15:23:30	0	
☐	cicd-ubuntu20	CA32D779E88BA8F5C138BE43367A9DAA9ED64	ubuntu	127.0.0.1, 10.255.2...	Network connected	Isolate Failed	root	29/10/2025 15:22:16	99999	
☐	ubuntu24-VMware-Virtual...	3E9703324DCC447D2D4240433E7FEB0931184D	ubuntu	127.0.0.1, 192.168...	Network connected	Isolate Failed	root	29/10/2025 15:22:16	99999	
☐	virtualinux	CD4D4CF46C0A88B1E3EE19F9E9C8B077AAC77AB	ubuntu	127.0.0.1, 10.0.2.1...	Network connected	Isolate Failed	root	29/10/2025 15:22:16	99999	

Xem danh sách lịch sử tác động theo thiết bị

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

viettel
ajant

Response / Isolate Devices

Enter your license to access the full features

Search by host name, agent ID

Showing 9 of 9 result(s)

☐	Host name	Agent ID	Platform	IP address	Device current status
☐	cicd-ubuntu20	CA32D779E88BA8F5C138BE43367A9DAA9ED64	ubuntu	127.0.0.1, 10.255.2...	Network connected
☐	ubuntu24-VMware-Virtual...	3E9703324DCC447D2D4240433E7FEB0931184D	ubuntu	127.0.0.1, 192.168...	Network connected
☐	ubuntu	5D274EAE0BFAA0A6F603A9C30F0120C7C056C8	ubuntu	127.0.0.1, 192.168...	Network connected
☐	HELUNG-SERVER-2019	0034AE74294149E8C277CEC8D6F40E1D87448	Microsoft Windows Server 2...	1601-481e4031-3468...	Network connected
☐	os-linux-ubuntu22-01	24AB4E7F98B23865A457C7F1C1506A325C4348E	ubuntu	127.0.0.1, 192.168...	Network connected
☐	ubuntu18	2302A78AED3C94EDC8D325F531A9B8B94BC78D6	ubuntu	127.0.0.1, 192.168...	Network connected
☐	os-linux-ubuntu02	A3D0A8492A0E4CE29E46D0F9E2D3338B2C206	ubuntu	127.0.0.1, 192.168...	Network connected
☐	virtualinux	CD4D4CF46C0A88B1E3EE19F9E9C8B077AAC77AB	ubuntu	127.0.0.1, 10.0.2.1...	Network connected
☐	192.168.233.135 non-exist...	E028B707D69D136A6134D25F8A4C3BB7D3881	centos	127.0.0.1, 192.168...	Network connected

View detail - cicd-ubuntu20

Showing 6 of 6 result(s)

Host name	Agent ID	Platform	IP address	Action	Action by	Last action on	Description
cicd-ubuntu20	CA32D779E88BA8F5C138BE43367A9DAA9ED64	ubuntu	127.0.0.1, 10.255.2...	Release from isolation	root	29/10/2025 18:29...	99999
cicd-ubuntu20	CA32D779E88BA8F5C138BE43367A9DAA9ED64	ubuntu	127.0.0.1, 10.255.2...	Isolate device	root	29/10/2025 15:22...	99999
cicd-ubuntu20	CA32D779E88BA8F5C138BE43367A9DAA9ED64	ubuntu	127.0.0.1, 10.255.2...	Isolate device	root	29/10/2025 15:21...	33221
cicd-ubuntu20	CA32D779E88BA8F5C138BE43367A9DAA9ED64	ubuntu	127.0.0.1, 10.255.2...	Isolate device	root	29/10/2025 15:20...	12345
cicd-ubuntu20	CA32D779E88BA8F5C138BE43367A9DAA9ED64	ubuntu	127.0.0.1, 10.255.2...	Release from isolation	root	29/10/2025 15:20...	456
cicd-ubuntu20	CA32D779E88BA8F5C138BE43367A9DAA9ED64	ubuntu	127.0.0.1, 10.255.2...	Isolate device	root	29/10/2025 17:22...	456

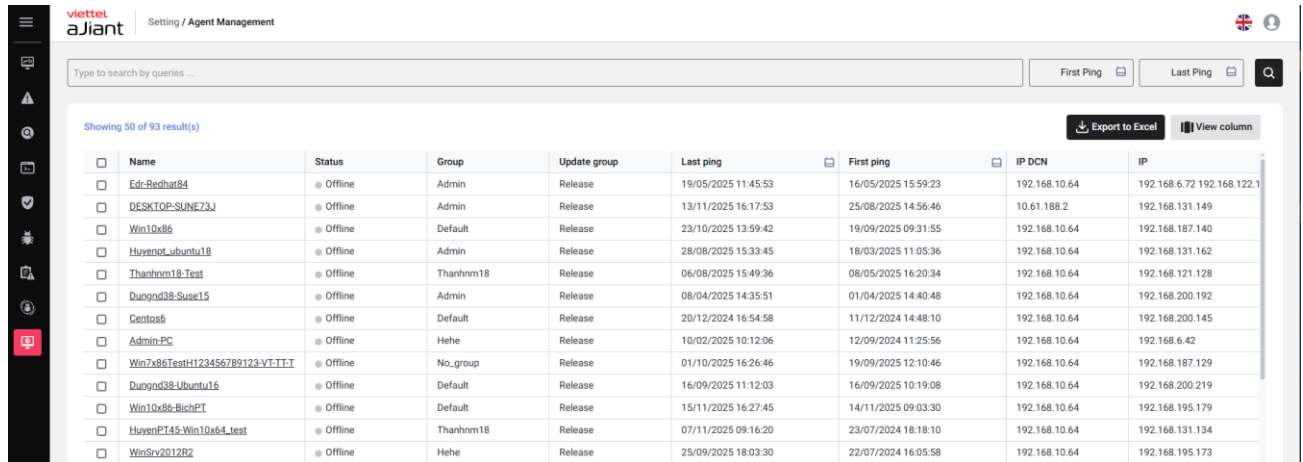
3.6 Nhóm chức năng Setting

3.6.1 Agent Management

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

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

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



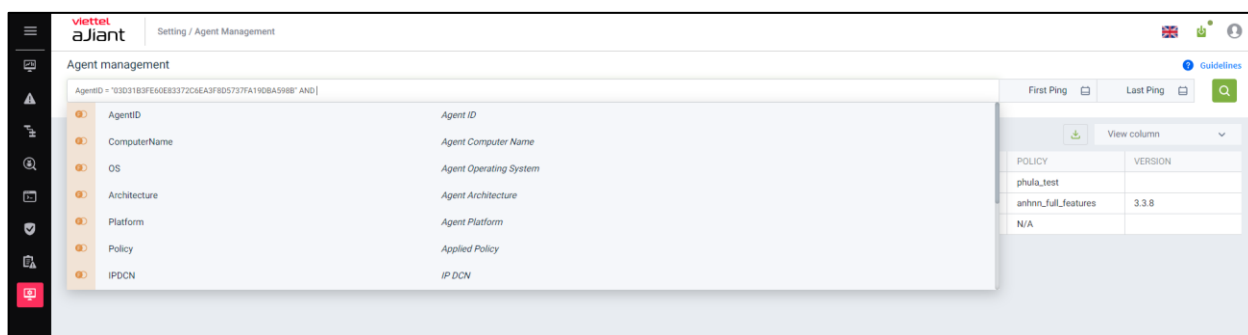
The screenshot shows the 'Setting / Agent Management' page in the Viettel aJiant interface. It displays a table with 10 columns: Name, Status, Group, Update group, Last ping, First ping, IP DCN, and IP. The table lists 20 agents, all with a status of 'Offline'. The agents are grouped into 'Admin', 'Default', 'Thanhnm18', and 'Hehe'. The table is filtered to show 50 of 93 results.

Name	Status	Group	Update group	Last ping	First ping	IP DCN	IP
Edi-Redhat84	Offline	Admin	Release	19/05/2025 11:45:53	16/05/2025 15:59:23	192.168.10.64	192.168.6.72 192.168.122.1
DESKTOP-SUNE73J	Offline	Admin	Release	13/11/2025 16:17:53	25/08/2025 14:56:46	10.61.188.2	192.168.131.149
Win10x86	Offline	Default	Release	23/10/2025 13:59:42	19/09/2025 09:31:55	192.168.10.64	192.168.187.140
Huyenot-ubuntu18	Offline	Admin	Release	28/08/2025 15:33:45	18/03/2025 11:05:36	192.168.10.64	192.168.131.162
Thanhnm18-Test	Offline	Thanhnm18	Release	06/08/2025 15:49:36	08/05/2025 16:20:34	192.168.10.64	192.168.121.128
Duongnd38-Suse15	Offline	Admin	Release	08/04/2025 14:35:51	01/04/2025 14:40:48	192.168.10.64	192.168.200.192
Centos6	Offline	Default	Release	20/12/2024 16:54:58	11/12/2024 14:48:10	192.168.10.64	192.168.200.145
Admin-PC	Offline	Hehe	Release	10/02/2025 10:12:06	12/09/2024 11:25:56	192.168.10.64	192.168.6.42
Win7x86TestH123456789123-YET-ET	Offline	No_group	Release	01/10/2025 16:26:46	19/09/2025 12:10:46	192.168.10.64	192.168.187.129
Duongnd38-Ubuntu16	Offline	Default	Release	16/09/2025 11:12:03	16/09/2025 10:19:08	192.168.10.64	192.168.200.219
Win10x86-BichPT	Offline	Default	Release	15/11/2025 16:27:45	14/11/2025 09:03:30	192.168.10.64	192.168.195.179
HuyenPT45-Win10x64-test	Offline	Thanhnm18	Release	07/11/2025 09:16:20	23/07/2024 18:18:10	192.168.10.64	192.168.131.134
WinSrv2012R2	Offline	Hehe	Release	25/09/2025 18:03:30	22/07/2024 16:05:58	192.168.10.64	192.168.195.173

Hệ thống hỗ trợ thực hiện các tính năng:

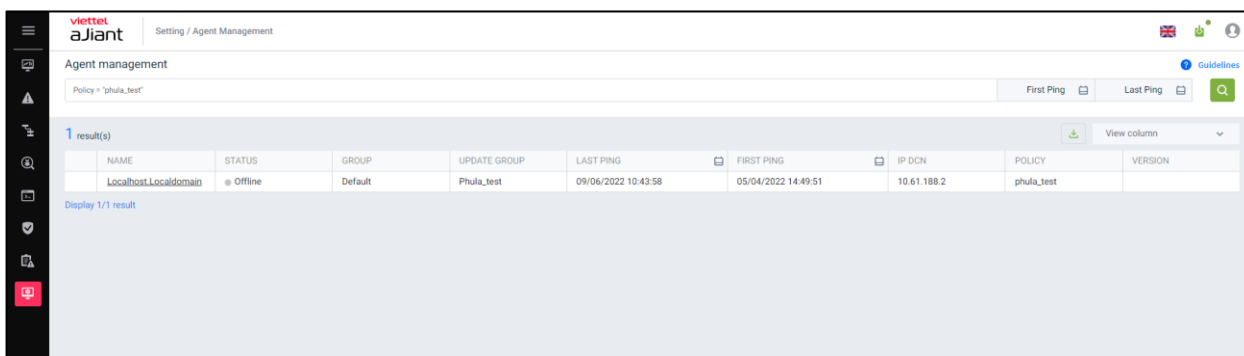
- 1 – Xem danh sách các agent đã được cài đặt trên hệ thống:
 - + User đăng nhập thuộc group root: Hiển thị tất cả Agent trong hệ thống active < 30 ngày;
 - + User đăng nhập thuộc group default: Hiển thị tất cả Agent thuộc group default;
 - + User đăng nhập thuộc group cha: Hiển thị tất cả Agent thuộc group của user đang login và group con tương ứng;
 - + User đăng nhập thuộc group một hoặc nhiều con: Hiển thị tất cả Agent thuộc group của user đang login;
 - + Mỗi agent được hiển thị các thông tin chung gồm: Name, Status, Group, Update Group, Last Ping, First Ping, DNS, Policy, AgentID, PlatForm, PlatForm Version, Architecture, DNS, Version, IP, License.

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

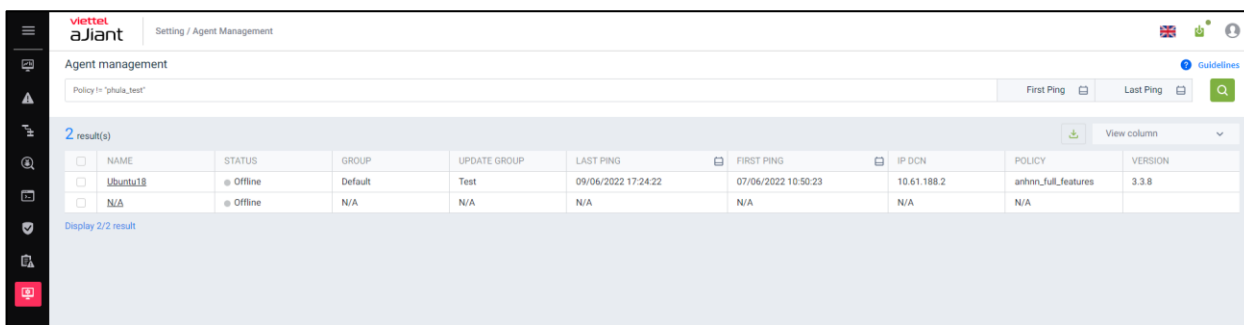


Ví dụ về các câu tìm kiếm:

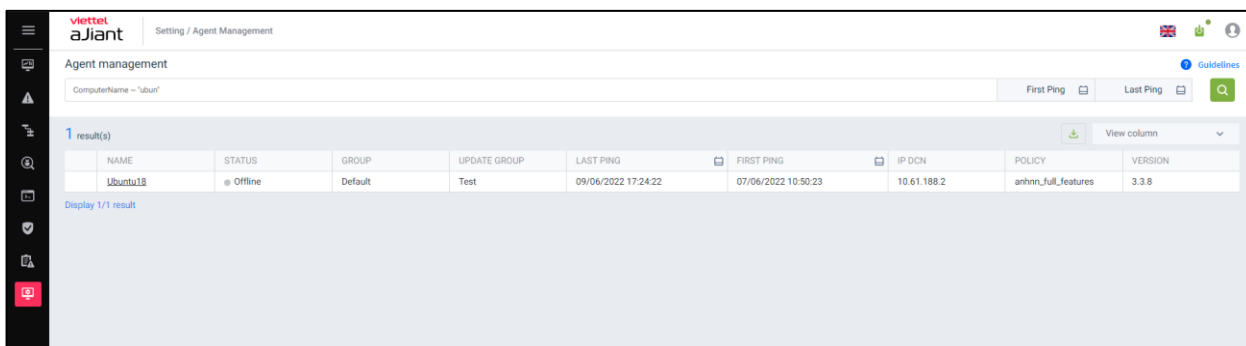
+ Tìm kiếm với điều kiện “=”:



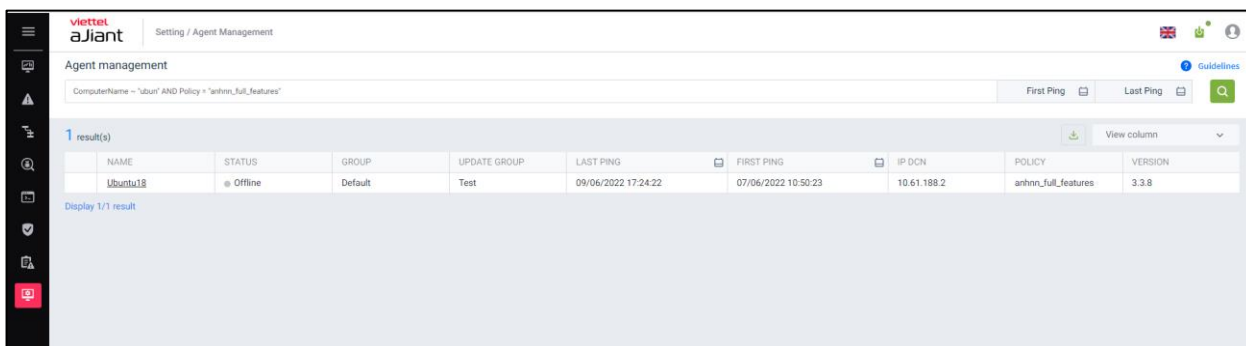
+ Tìm kiếm với điều kiện “!=”:



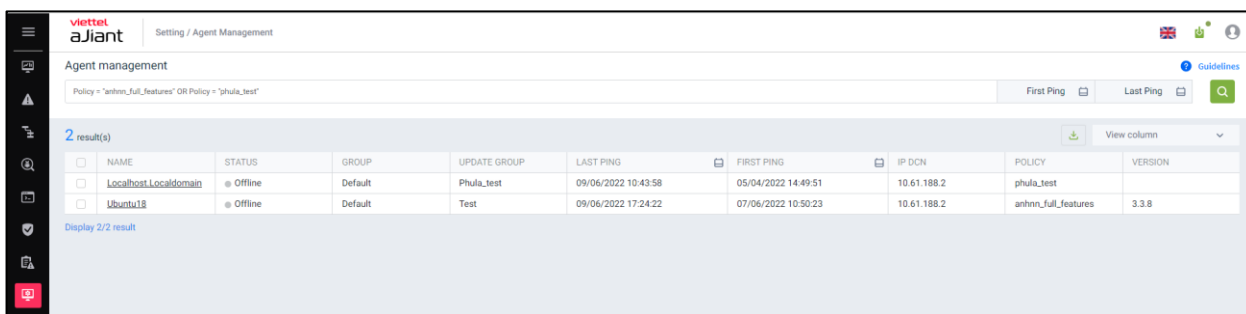
+ Tìm kiếm với điều kiện “~”:



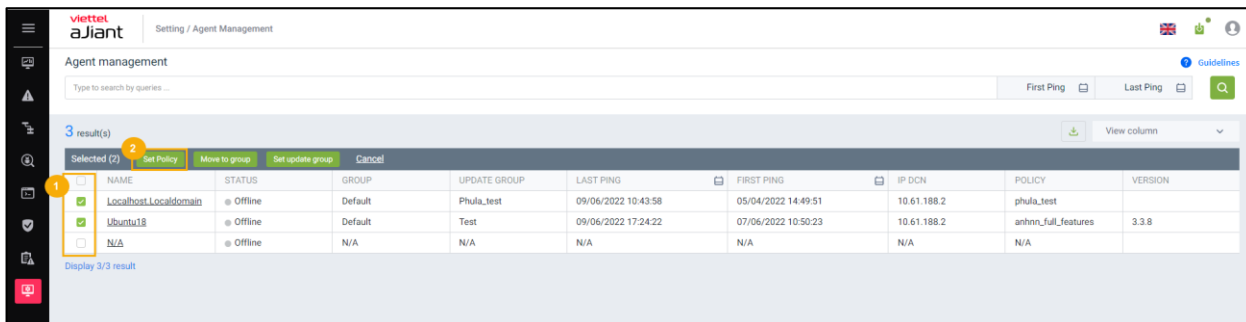
+ Tìm kiếm theo tiêu chí kết hợp AND:



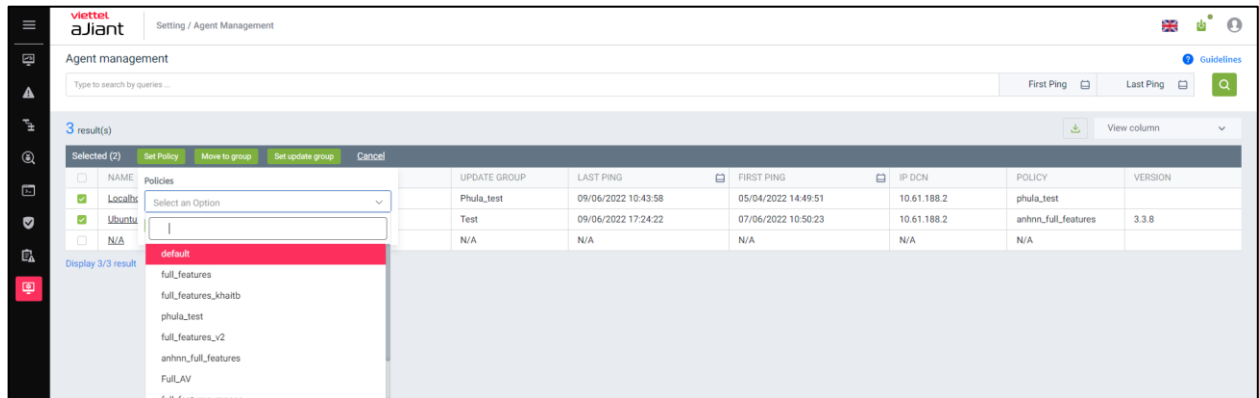
+ Tìm kiếm theo tiêu chí kết hợp OR:



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

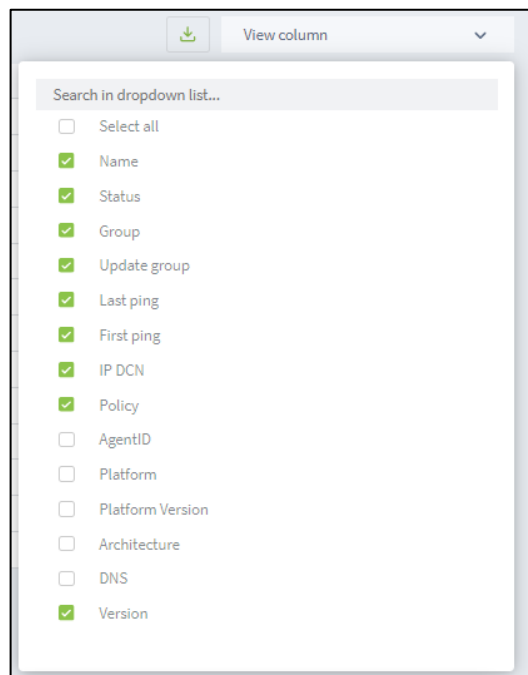


- + Tích chọn 1 agent/ nhiều agent để vào phiên Multiselected;
- + Thực hiện Set Policy:
 - Chọn Policy:



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

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



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

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

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

Tab General info

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

Agent management

Type to search by queries...

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

Display 3/3 result

Agent localhost.localdomain

Agent ID 31F6FA3794407C2DC854E155A3170C79686AD

First ping: 05/04/2022 14:49:51 | Last ping: 05/06/2022 10:43:58

Agent properties

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

About this agent

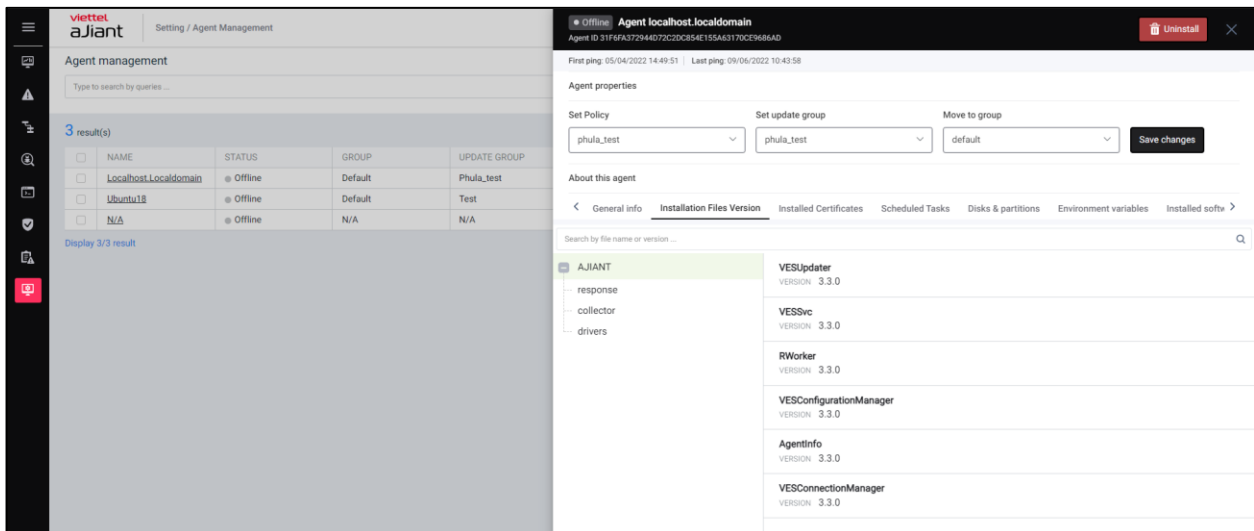
General info | Installation Files Version | Installed Certificates | Scheduled Tasks | Disks & partitions | Environment variables | Installed soft

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::437e:dc7a:2765:34ad
Platform Family	rhel	MAC	00:0c:29:e8:c3:48
Architecture	amd64	Name	ens160
Physical Memory	1,843,832		
		Default Gateway	192.168.121.2
CPUs		DNS Server	192.168.121.2
Cores	1		
mhz	1992.001000		
Model Name	Intel(R) Core(TM) i7-10700T CPU @ 2.00GHz		
Vendor ID	GenuineIntel		

Installation Files Version

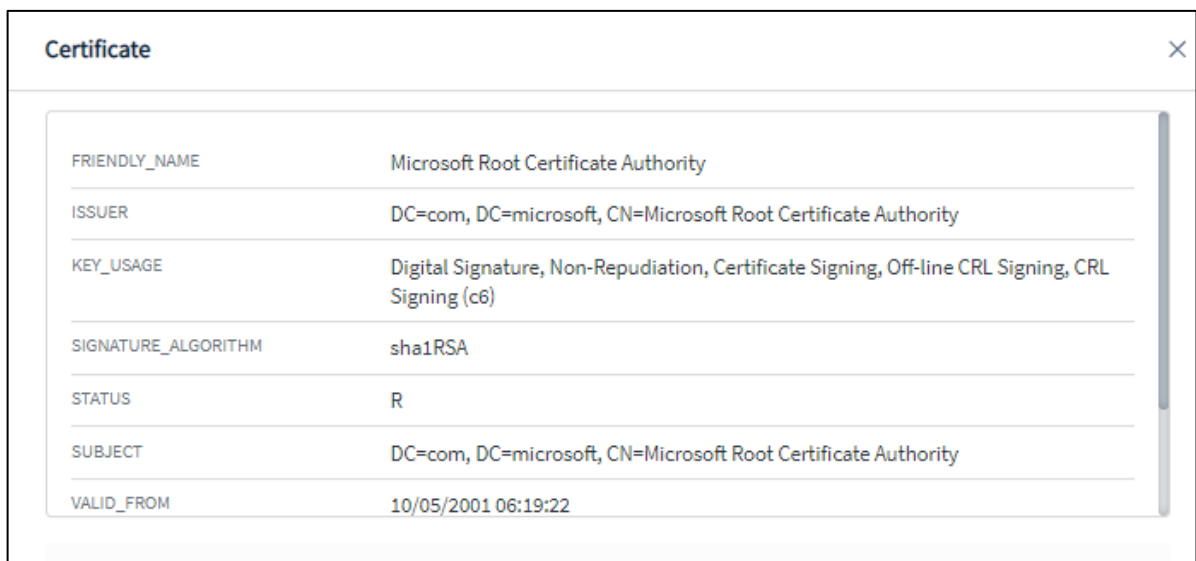
- + Thống kê tất cả các file cài agent, bao gồm các thông tin: Tên folder chứa file cài, File name, Version;
- + Hỗ trợ search nhanh theo File name, Version vào text box search



Installed Certificates

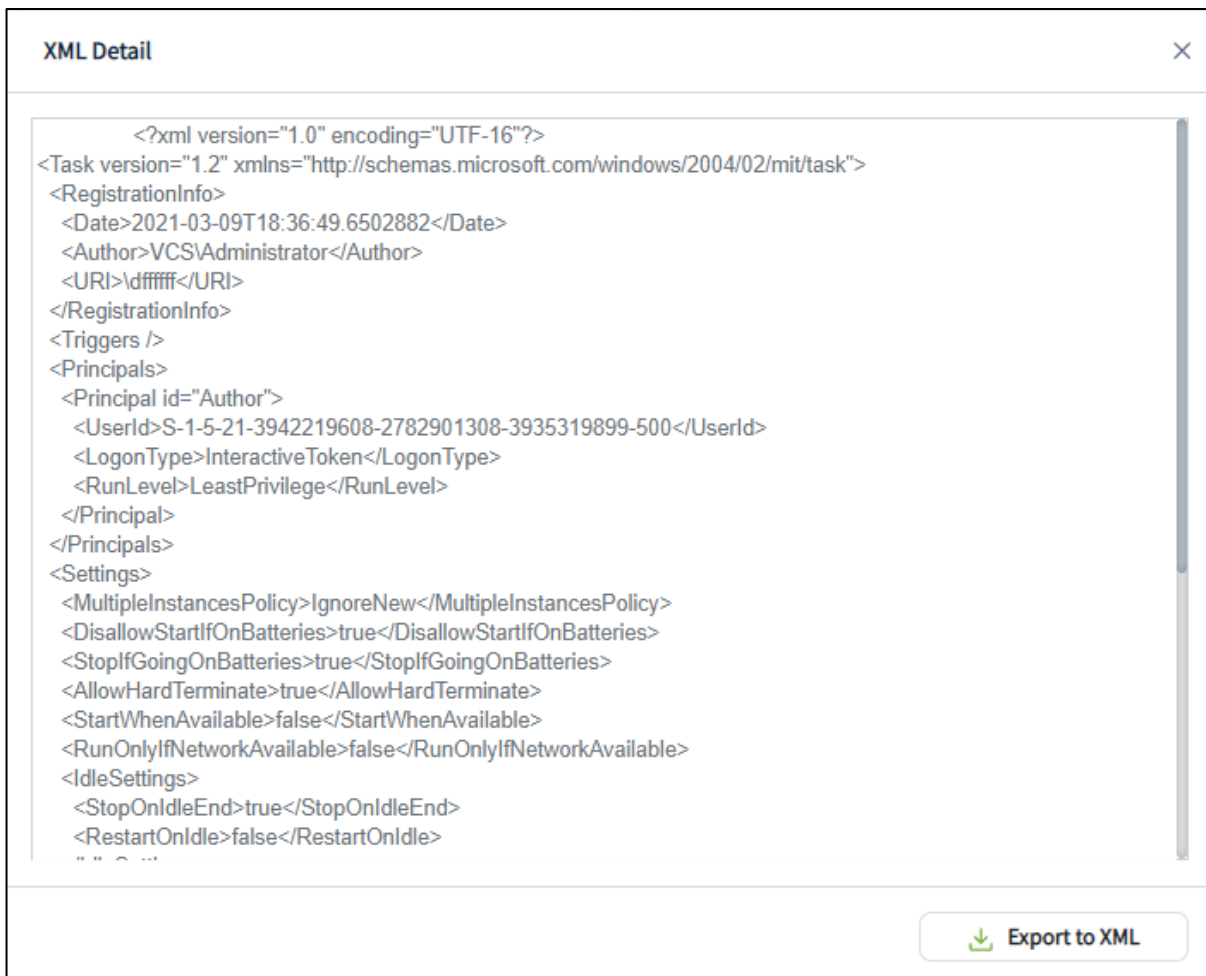
+ Thống kê tất cả các certificate trên máy cài agent, bao gồm các thông tin: Danh sách certificates trên máy, Issued by, Issued to, Expiration date, Status;

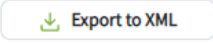
+ Trường hợp muốn xem chi tiết với nhiều thông tin hơn, chọn , hiển thị màn hình như sau:



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

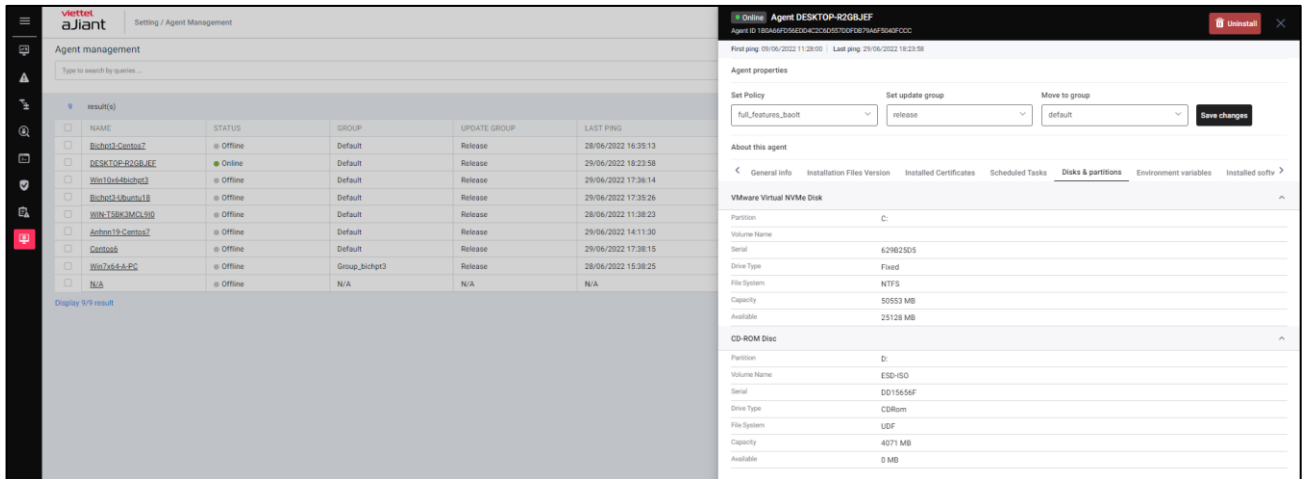


- + Chọn  để tải về thông tin scheduled task, hỗ trợ định dạng .xml

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.



The screenshot shows the Viettel Ajiant Agent Management interface. On the left, there's a sidebar with navigation icons. The main area is divided into two panels. The left panel shows a list of agents with columns: NAME, STATUS, GROUP, UPDATE GROUP, and LAST PING. The right panel shows the details of a selected agent, 'Agent DESKTOP-R2GBJEF'. It includes a 'Set Policy' dropdown, a 'Set update group' dropdown, and a 'Move to group' dropdown. Below these, there's a 'Disks & partitions' tab. The 'Disks & partitions' tab shows details for two disks: 'VMware Virtual NVMe Disk' and 'CD-ROM Disk'. Each disk has fields for Partition, Volume Name, Serial, Drive Type, File System, Capacity, and Available.

NAME	STATUS	GROUP	UPDATE GROUP	LAST PING
Desktop-Centos7	Offline	Default	Release	28/06/2022 16:35:13
DESKTOP-R2GBJEF	Online	Default	Release	29/06/2022 18:23:58
Win10-48484848	Offline	Default	Release	29/06/2022 17:36:14
Win10-48484848	Offline	Default	Release	29/06/2022 17:35:26
Win10-48484848	Offline	Default	Release	28/06/2022 11:38:23
Centos7	Offline	Default	Release	29/06/2022 14:11:36
Centos7	Offline	Default	Release	29/06/2022 17:36:15
Win7-48484848	Offline	Group_bichpt3	Release	28/06/2022 15:36:25
N/A	Offline	N/A	N/A	N/A

Agent properties for Agent DESKTOP-R2GBJEF:

- Set Policy: Full, Features, boot
- Set update group: release
- Move to group: default

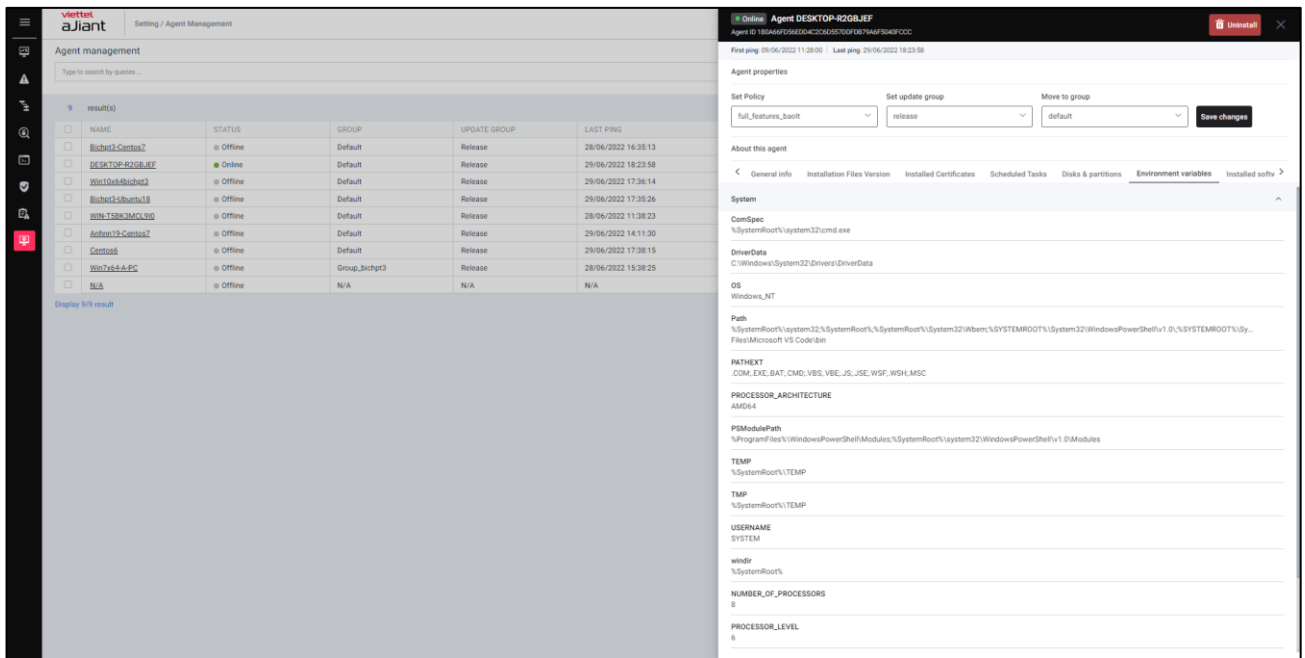
Disks & partitions:

Partition	Volume Name	Serial	Drive Type	File System	Capacity	Available
C:	62962505	62962505	Fixed	NTFS	50553 MB	25128 MB
D:	ESD-ISO	0015655F	CDROM	UDF	4071 MB	0 MB

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

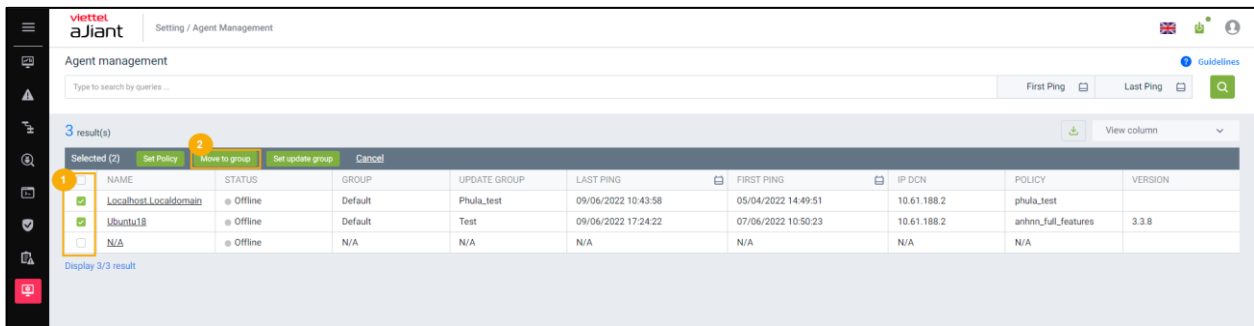
- + Thống kê tất cả phần mềm bắt buộc đã cài hoặc chưa cài trong agent bao gồm thông tin: Tên phần mềm, version cài, trạng thái cài;
- + Hỗ trợ search nhanh phần mềm bắt buộc chưa cài đặt trên máy hoặc nhập tên phần mềm vào text box search.

Tab User list

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

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

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



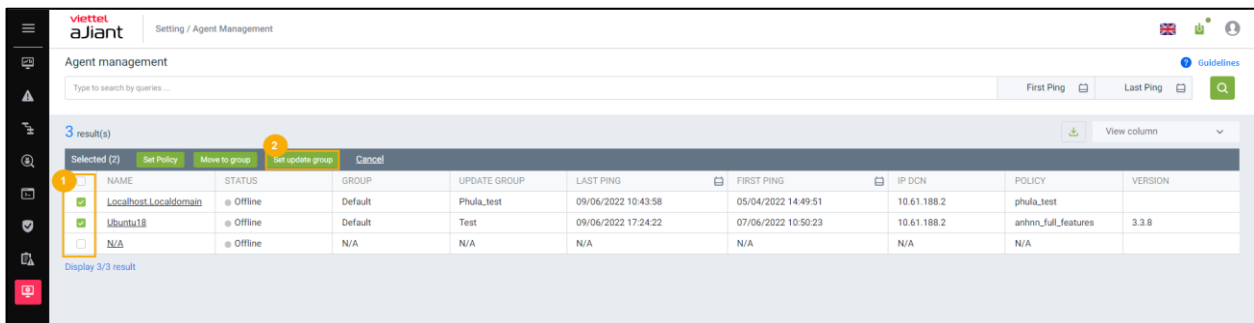
+ Thực hiện Move to group:

Danh sách Group trong combobox Move to group:

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

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

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



- Thực hiện Set update group;

Lưu ý:

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

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

Cách tính license VCS-ajiant:

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

+ Hệ thống sẽ tính license cho agent theo thời gian agent kết nối tới hệ thống VCS-ajiant (thời gian first ping, agent kết nối trước sẽ được gán license trước)
Trong trường hợp:

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

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

3.6.2 Policy Setting

Mục đích: Hỗ trợ người dùng quản lý danh sách các chính sách thiết lập cho các Agent;

Màn hình giao diện khi người dùng truy nhập vào Setting >> Policy Setting:

POLICY NAME	NUMBER OF AGENTS	CREATED TIME	UPDATED TIME	APPLIED TIME	STATUS
default	0	28/01/2019 14:11:52	03/12/2020 11:42:43	03/12/2020 11:42:50	Applied
full_features	0	09/12/2021 10:20:00	26/05/2022 14:14:25	08/06/2022 13:54:08	Applied
full_features_khaib	0	13/01/2022 13:49:13	13/01/2022 14:15:50	13/01/2022 14:15:53	Applied
phula_test	1	14/01/2022 13:17:12	31/03/2022 13:07:30	31/03/2022 13:07:35	Applied
full_features_v2	0	17/01/2022 14:29:12	08/06/2022 16:02:34	08/06/2022 16:02:37	Applied
anhn_full_features	1	08/02/2022 15:51:36	08/06/2022 16:19:12	08/06/2022 16:19:14	Applied
Full_AV	0	01/03/2022 14:36:25	20/05/2022 15:02:30	20/05/2022 15:02:34	Applied
full_features_macos	0	11/03/2022 18:22:01	18/03/2022 11:29:29	18/03/2022 11:29:32	Applied
full_features_anhn	0	15/03/2022 15:14:32	25/05/2022 17:50:28	25/05/2022 17:50:31	Applied
full_features_baot	0	17/03/2022 15:12:01	09/06/2022 15:32:37	09/06/2022 15:32:40	Applied

1 – 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);

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

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

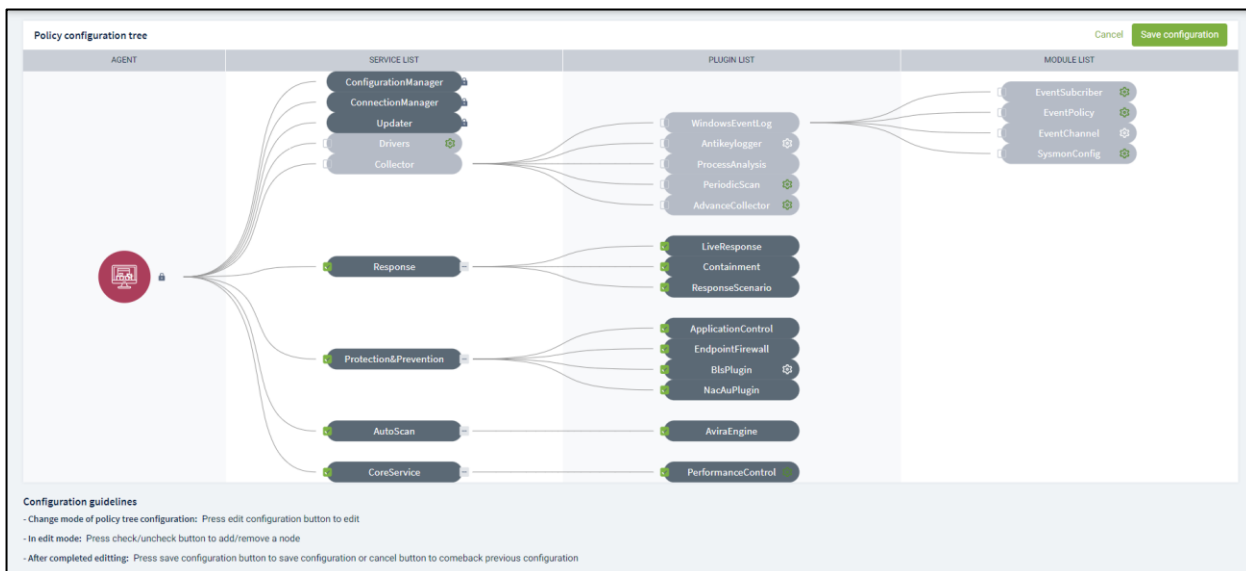
Sau khi tạo mới policy thành công hệ thống sẽ hiển thị màn hình chi tiết của 1 policy:



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

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

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



Bước 3: Sau khi hoàn thành chế độ edit:

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

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

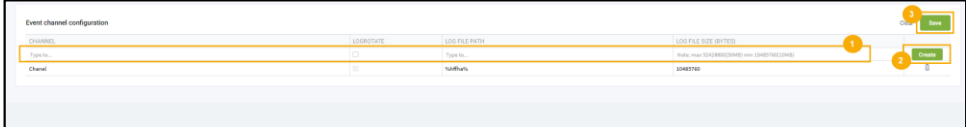
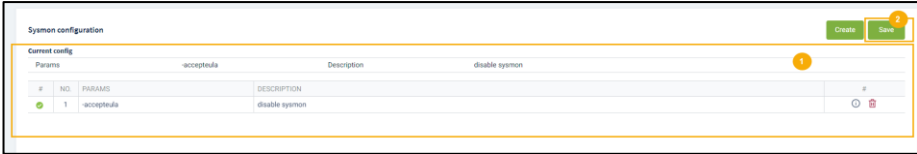
- + Trường **providers** các string con cách nhau dấu chấm phẩy (;);
- + Các trường bắt buộc phải điền: **subs_type, channel;**
- + Channel: nguồn log;
- + sub_type:
 - PUSH: khi có event mới → gọi hàm của VCS-aJiant để xử lý;
 - POLLING: VCS-aJiant sau 1 khoảng thời gian chủ động lấy log;
 - PULL: VCS-aJiant chủ động lấy log sau 1 khoảng thời gian;

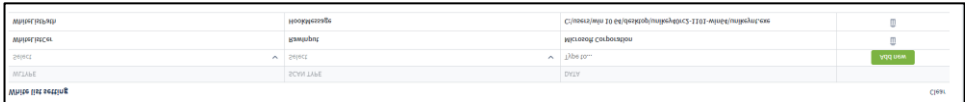
Sau khi cấu hình xong cần Save lại:

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

- Yêu cầu: có ít nhất 1 trường được chọn

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

	- Retention: có lưu log xoay vòng hay không (Nếu chọn Rentention thì khi file log đầy có log mới sẽ ghi đè lên log cũ nhất); - Log file path: đường dẫn file log; - Log file size: kích thước file log; - Yêu cầu: tất cả dữ liệu đều phải điền;  + SysmonConfig: enable/disable sysmon tool trên Agent để lấy log sysmon: Microsoft-Windows-Sysmon/Operational; 
Antikeylogger	Cấu hình Antikeylogger: là một SelfRun Plugin của VCS-aJiant, có nhiệm vụ định kỳ quét toàn bộ máy để tìm ra KeyLogger đang chạy trên máy nếu có; - Scan setting: cấu hình các loại KeyLogger cần quét; - Yêu cầu: - Scan cycle: min là 1 phút, max là 180 phút; - Chọn ít nhất 1 loại Keylogger; + Whitelist setting: cấu hình whitelist 1 số phần mềm theo đường dẫn của file trên ổ đĩa hoặc theo chữ ký số (cert) của file chạy key logger - Yêu cầu: điền đầy đủ các trường;

	Sau khi nhập xong cần “Save” lại cấu hình: 
Self defend	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

Version

disable autoscan

Description

disable autoscan

Data configuration for Windows

```

1 {
2   "auto_scan": {
3     "enable_auto_scan": false
4   }
5 }

```

Cancel

Create

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

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

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

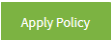
Các trường hỗ trợ config cho luồng quét thủ công như sau

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

	<table><tr><td>rescan_disinfected</td><td>integer</td><td>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</td></tr></table>	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_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														
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: <table><tr><td>Config</td><td>Type</td><td>Mô tả</td></tr><tr><td>silent</td><td>bool</td><td>bật tắt chế độ hoạt động silent</td></tr><tr><td>protect_ext</td><td>string list</td><td>danh sách đuôi file được bảo vệ</td></tr><tr><td>protect_whitelist</td><td>string list</td><td>danh sách folder được white list không bảo vệ</td></tr><tr><td>actor_whitelist</td><td>string list</td><td>danh sách file, folder chứa process được phép thực hiện hành vi</td></tr></table>	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
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														
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	bật tắt chế độ hoạt động silent
Config	Type	Mô tả					
silent	bool	bật tắt chế độ hoạt động silent					
Performance control linux	+ Performance control là module thực hiện chức năng monitor, giới hạn các tài nguyên mà từng service của EDR được sử dụng trên máy người dùng. Các thông số giới hạn về lượng tài nguyên được cấu hình trên portal: - Config ngưỡng cho CPU: Cho phép người dùng cấu hình mức giới hạn CPU cho từng agent. Agent sẽ hoạt động trong phạm vi cấu hình, không vượt ngưỡng CPU đã đặt - Config ngưỡng cho MEM: Cho phép người dùng cấu hình mức giới hạn bộ nhớ (Memory limit) cho process. Khi mức sử dụng bộ nhớ vượt ngưỡng cấu hình, process sẽ tự động bị restart để giải phóng tài nguyên. - Config cho giá trị FD: Cho phép người dùng cấu hình mức giới hạn file được mở bởi process. Khi mức sử dụng bộ nhớ vượt ngưỡng cấu hình, process sẽ tự động bị restart để giải phóng tài nguyên. - Config giá trị DiskIO: Cho phép người dùng giới hạn tốc độ truy xuất đĩa (đọc/ghi) của process. Process sẽ giảm tốc độ (throttling) dưới giá trị config - Config giá trị Network: Giới hạn tốc độ mạng mà process có thể xử lý trong mỗi giây. Process sẽ giảm tốc độ (throttling) dưới giá trị config - Yêu cầu: Chọn CoreService-> chọn PerformanceControl Các trường hỗ trợ config như sau: <table><tr><th>STT</th><th>Cấu hình</th><th>Kiểu giá trị</th><th>Ý nghĩa</th></tr></table>	STT	Cấu hình	Kiểu giá trị	Ý nghĩa		
STT	Cấu hình	Kiểu giá trị	Ý nghĩa				

		1	Process name	String	Tên process được quản lý
		2	Cpu peak	Int	Ngưỡng cpu
		3	Cpu Avr	Int	Ngưỡng cpu trung bình
		4	Memory peak	int	Ngưỡng memory
		5	Memory Avr	Int	Ngưỡng memory trung bình
		6	Disk IO peak	Int	Ngưỡng io peak
		7	Disk IO Avr	int	Ngưỡng io trung bình
		8	Network Peak	Int	Ngưỡng network
		9	Network Avr	Int	Ngưỡng network trung bình
		10	deltatime_cpu	Int	Time đo cpu
		11	deltatime_memory	Int	Time đo mem
		12	deltatime_disk_io	Int	Time đo io
		13	deltatime_network	Int	Time đo net

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.

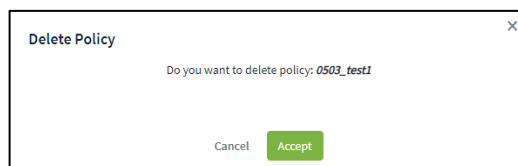
Clone from policy:
test_sample

NAME OF POLICY

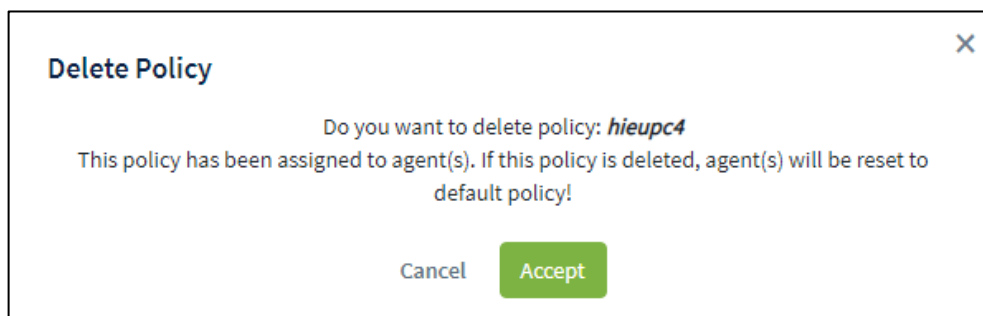
Cannot edit name of policy after create policy



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



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



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

3.6.3 Group Management

Cấu hình luật để tự động chuyển policy và chuyển nhóm cho các agent nếu thỏa mãn luật trên Portal, giảm thời gian chuyển policy và chuyển nhóm cho từng agent và đồng bộ policy cho các agent thỏa mãn luật đã cấu hình.

Các tính năng chính trên màn hình này bao gồm:

- + Quản lý nhóm theo cây;
- + Tìm kiếm nhóm;
- + Thêm mới nhóm:
 - Tạo luật tự động chuyển nhóm cho agent;
 - Tùy chọn cách thức chuyển nhóm (All existing agents, New agents only, All existing and new agents) và gán policy (gán ngay, không gán);
- + Theo dõi các agent thuộc nhóm, tổng số agent thuộc nhóm;
- + Chỉnh sửa nhóm;
- + Xóa nhóm, xóa agent thuộc nhóm;

1 – Quản lý nhóm theo cây:

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

Danh sách nhóm hiển thị theo dạng cây bao gồm các nhóm gốc và mỗi nhóm gốc gồm các nhóm con cấp 1, cấp 2...

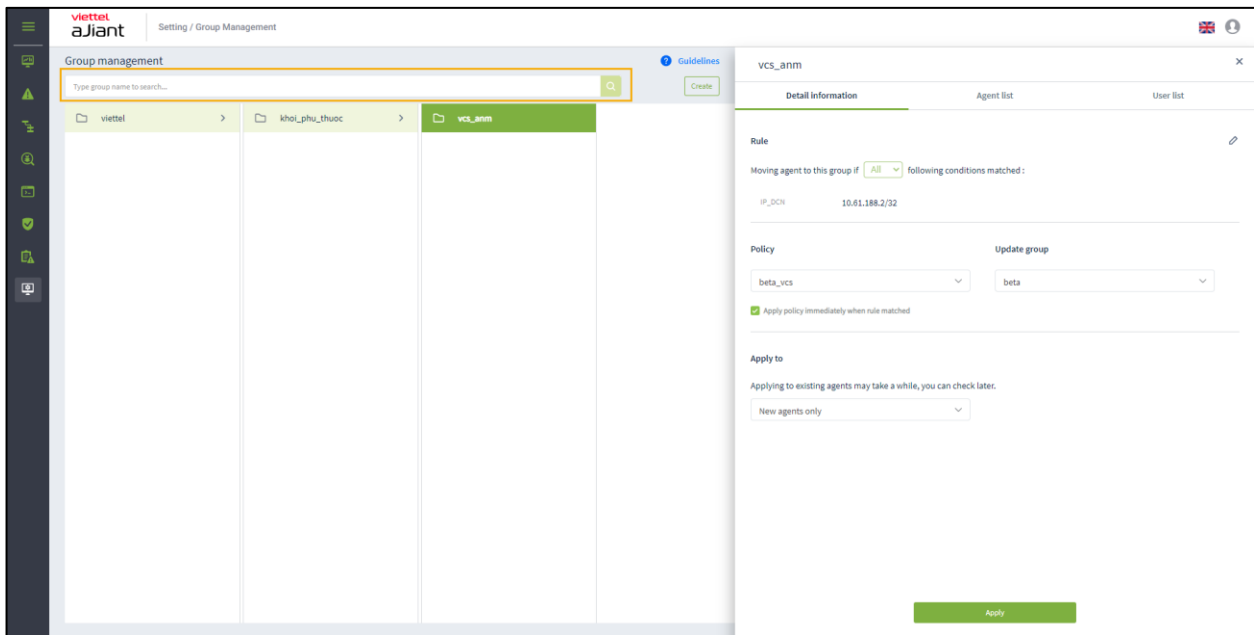
Mỗi nhóm gồm tên nhóm, thông tin cấu hình của nhóm (rule, policy, apply to), và danh sách agent thuộc nhóm.

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

Khi user thuộc group con, chọn group cha sẽ không nhìn thấy popup group detail

2 – Tìm kiếm nhóm

- + Cách 1: Click vào textbox Search > hiện danh sách các nhóm của tương ứng với user đang login có thể scroll được > Chọn nhóm trong danh sách hiện ra;
- + Cách 2: Click vào textbox Search > nhập ký tự tìm kiếm vào textbox > hệ thống tự động tìm kiếm các bản ghi chứa ký tự nhập vào > Chọn 1 bản ghi phù hợp trong danh sách gợi ý hoặc click Search hoặc Enter sẽ hiện danh sách các bản ghi thỏa mãn;



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

- + Tab thông tin chi tiết hiển thị là Detail, dữ liệu của group đó là Rule, Policy, Apply to;
- + Khi chọn tab Agent list thì dữ liệu thông tin các agent match với group đó.
- + Khi chuột phải vào 1 bản ghi thì sẽ hiển thị 2 option: Go to group và Delete group.
- + Nếu chọn Go to group thì đưa user đến vị trí của group đó trên cây;
- + Nếu chọn Delete group thì hiển thị popup confirm xóa group.

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

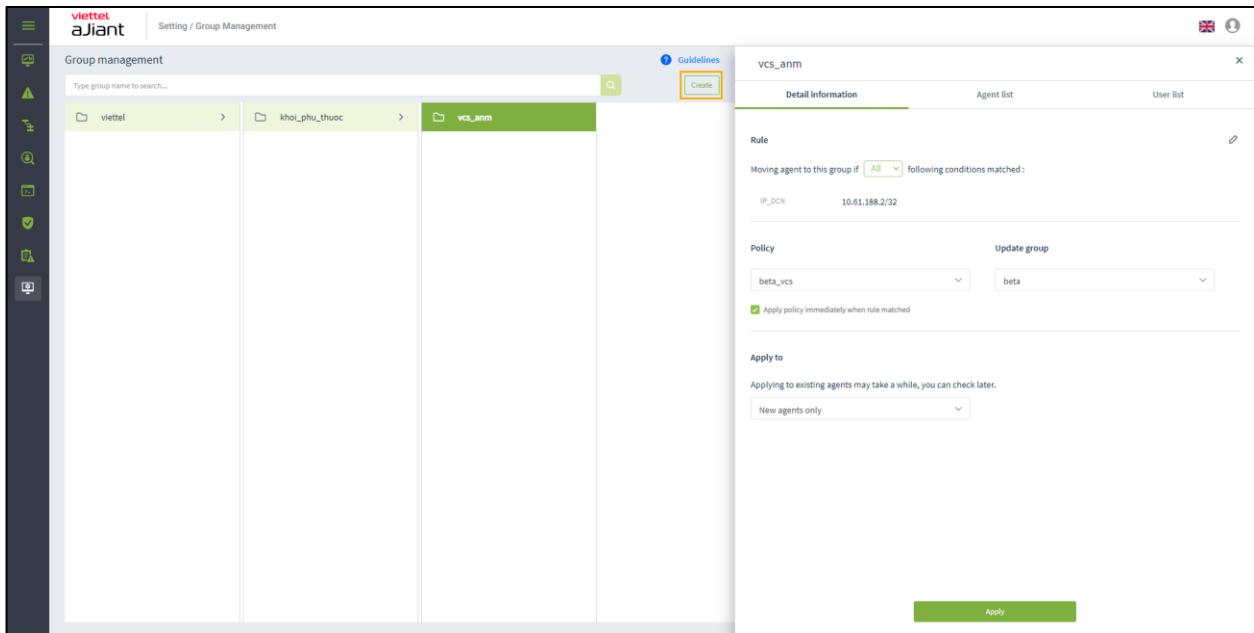
3 – Thêm mới nhóm:

- + 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 ;

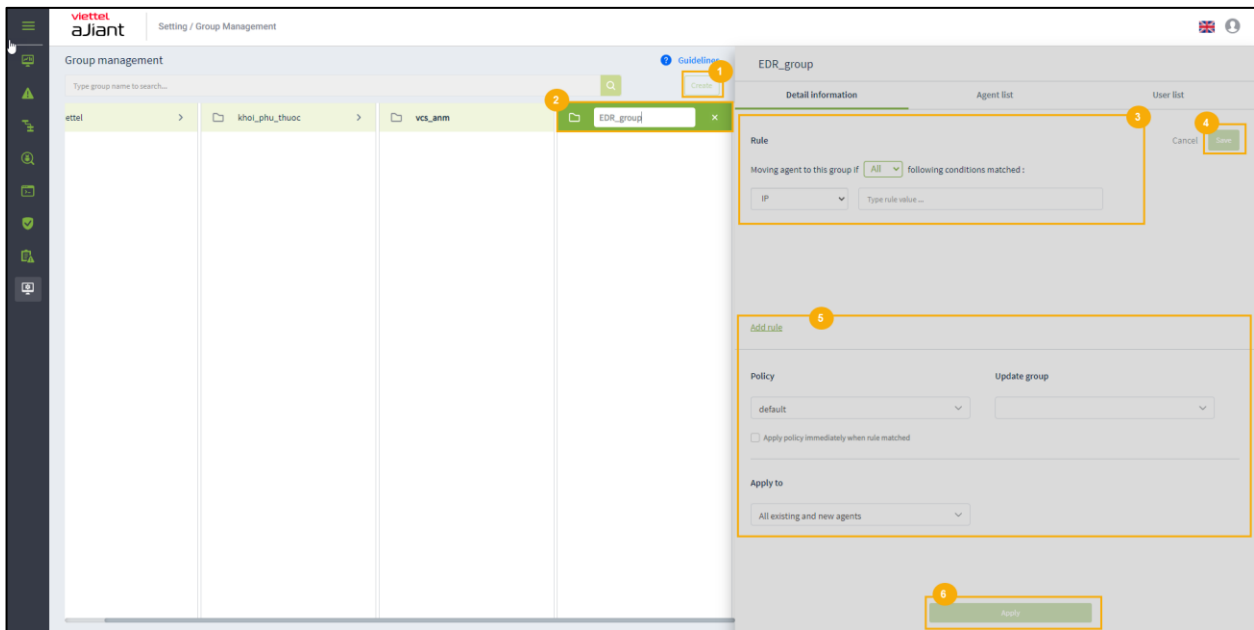


+ Nếu tạo mới nhóm là nhóm con trong một nhóm gốc hoặc nhóm cấp 1, cấp 2... thì click vào nhóm cha sau đó click “Create” trên màn hình hoặc hover vào cuối danh sách nhóm cùng cấp và click “Create”;

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.

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

- + User đăng nhập thuộc group root: Có thể sửa tất cả group trong hệ thống;
- + User đăng nhập thuộc group default: Không được sửa group default;
- + User đăng nhập thuộc group cha: Có thể sửa tất cả group thuộc đang login và group con có role cũng thuộc group role con của role user đang login;
- + User đăng nhập thuộc group một hoặc nhiều con: Có thể sửa tất cả group thuộc user đang login;
- + Để sửa Rule (luật) của nhóm, click vào icon Edit > Chỉnh sửa luật của nhóm sau đó click Save > Sau đó có thể chỉnh sửa ở mục “Policy” và “Apply to” rồi click Apply;

The screenshot displays the 'vcs_anm' configuration window. It has three tabs: 'Detail information' (selected), 'Agent list', and 'User list'. Under 'Detail information', there are three sections: 'Rule', 'Policy', and 'Apply to'. The 'Rule' section includes an 'Edit' icon and a condition: 'Moving agent to this group if [All] following conditions matched: IP_DCN 10.61.188.2/32'. The 'Policy' section has a 'Policy' dropdown set to 'beta_vcs', an 'Update group' dropdown set to 'beta', and a checked checkbox 'Apply policy immediately when rule matched'. The 'Apply to' section has a dropdown set to 'New agents only' with a note: 'Applying to existing agents may take a while, you can check later.' At the bottom is a green 'Apply' button.

Lưu ý:

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

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

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

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

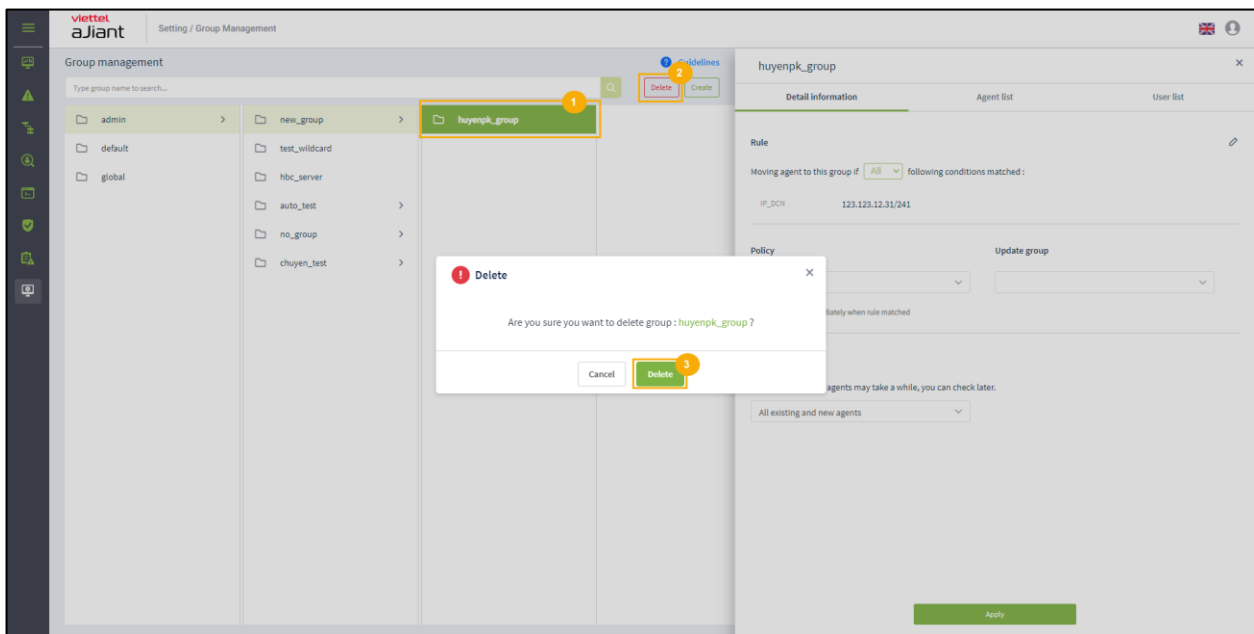
phần “Apply to” thì thực hiện quét thông tin toàn bộ agent trong hệ thống và chuyển nhóm cho agent, sau đó cập nhật Agent list.

Đối với Agent mới xử lý tương tự như trên.

5 – Xóa nhóm hoặc xóa agent khỏi nhóm:

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

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



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

vcs_anm

Detail information

Agent list

User list

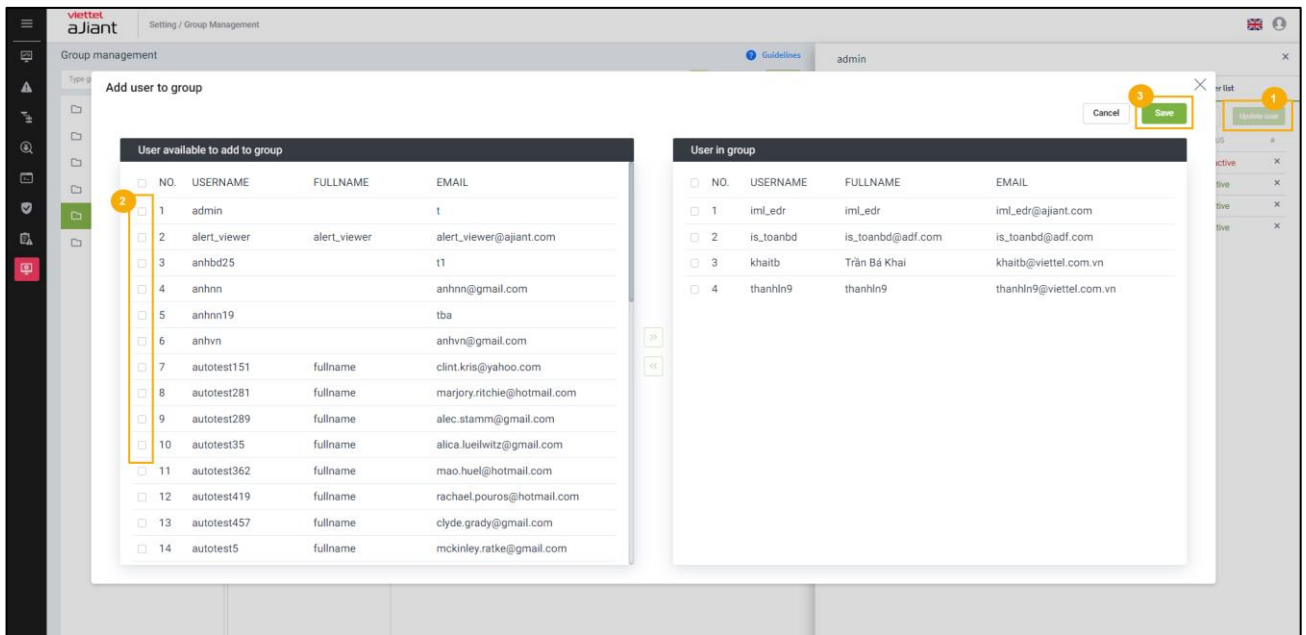
50/279 agent(s)

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:

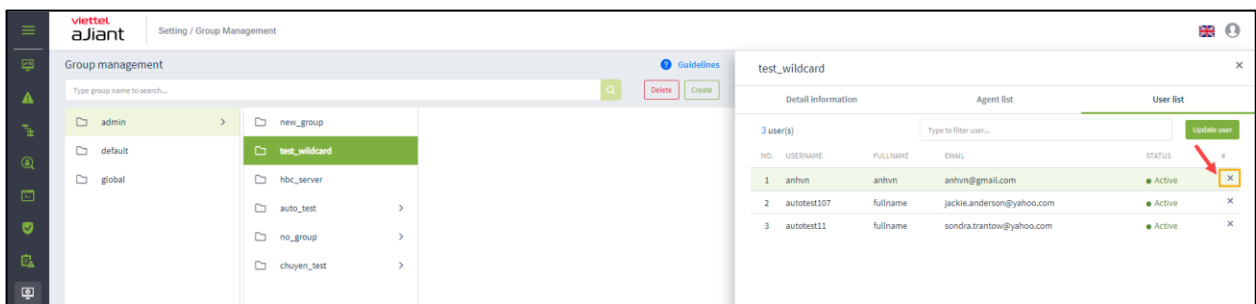
- + Xóa tất cả nhóm con;
 - + Chuyển tất cả agent của nhóm cha và các nhóm con về nhóm mặc định: “default”;
 - + Giữ nguyên policy của các agent trong nhóm cha và con;
- 6 – Thêm mới user vào group



Danh sách user:

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

7 – Xóa user



3.6.4 Account Management

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

Permission management

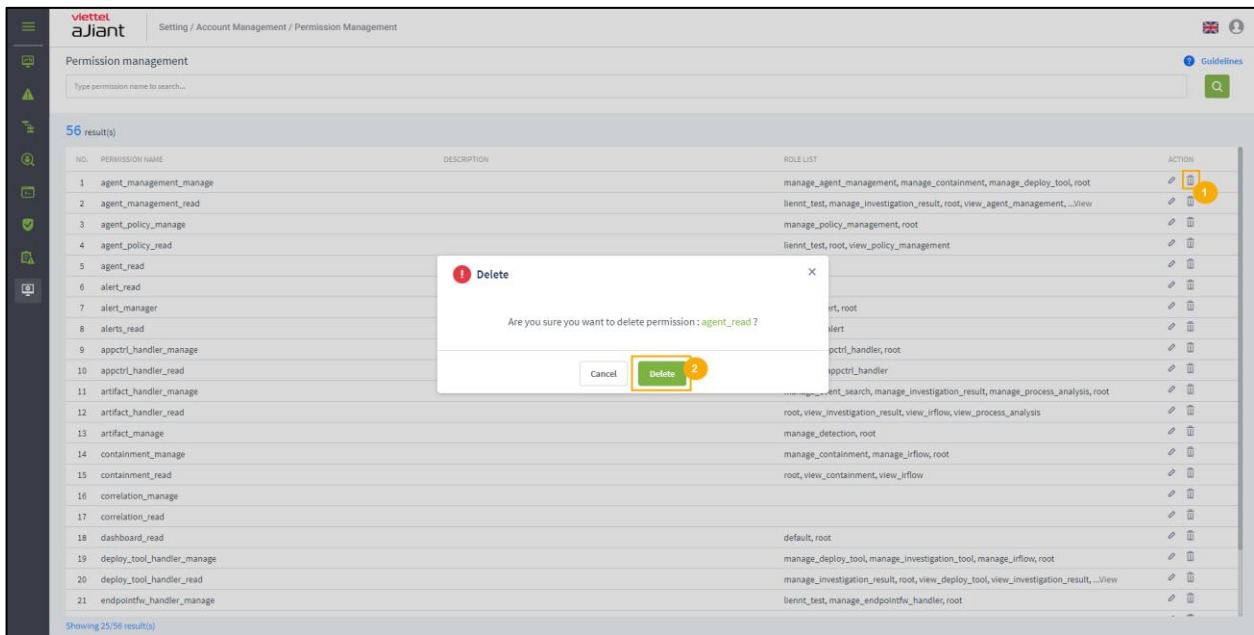
Quản lý các quyền truy cập vào tài nguyên (API) của hệ thống. 1 permission là quyền truy cập vào 1 tài nguyên xác định (API) của hệ thống;

Các chức năng chính trên màn hình này:

- + Quản lý các permission;
 - + Tìm kiếm permission;
 - + Xóa permission;
- 1 – Quản lý các permission: hiển thị toàn bộ các permission của hệ thống. Trong trường hợp xóa permission trên màn hình này, khi thực hiện các chức năng trên portal mà bị thiếu permission thì sẽ tự động thêm permission đã xóa trên màn hình quản lý Permission
 - 2 – Tìm kiếm permission: nhập ký tự tìm kiếm vào 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	

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



Role Management

Quản lý các role (nhóm quyền hay nhóm permission) của hệ thống;

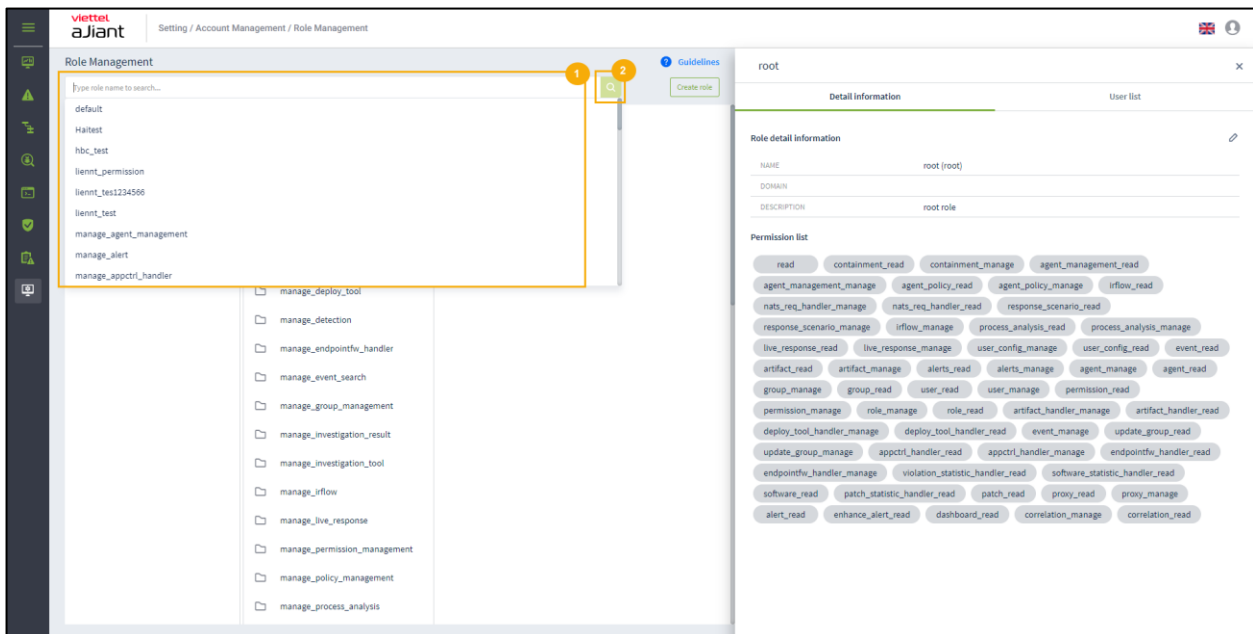
Các chức năng trên màn hình này bao gồm:

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

- + Role “default”: User có quyền “default” chỉ có quyền truy cập vào Portal, không có quyền xem dữ liệu hoặc thao tác chức năng;
- + Role “root”: bao gồm toàn bộ các role của hệ thống, User có role “root” có toàn bộ quyền sử dụng tất cả chức năng trên Portal;
- + Click vào 1 role sẽ hiển thị thông tin chi tiết của role. Một role sẽ bao gồm các thông tin: tên role, danh sách các permission, danh sách User (tài khoản) chứa role, role cha hoặc danh sách role con (nếu có)

2 – Tìm kiếm role

- + Cách 1: Click vào textbox Search > hiển thị danh sách các role trong hệ thống và có thể scroll được danh sách role > Lựa chọn role trong danh sách hiện ra
- + Cách 2: Click vào textbox Search > Nhập ký tự tìm kiếm vào textbox > Hệ thống lọc ra các role chứa ký tự tìm kiếm > chọn role trong danh sách đã lọc hoặc click Enter hoặc click nút “Search”



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

- Khi chọn tab User list là danh sách User chứa role;
 - + Khi chuột phải vào 1 bản ghi thì sẽ hiển thị Go to role. Click vào “Go to role” đưa về danh sách role dạng cây ban đầu;
 - + Khi click vào menu góc phải mỗi bản ghi cũng hiển thị option: Go to role;
- 3 – Thêm mới role:
- + User đăng nhập thuộc group root: Có thể 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.

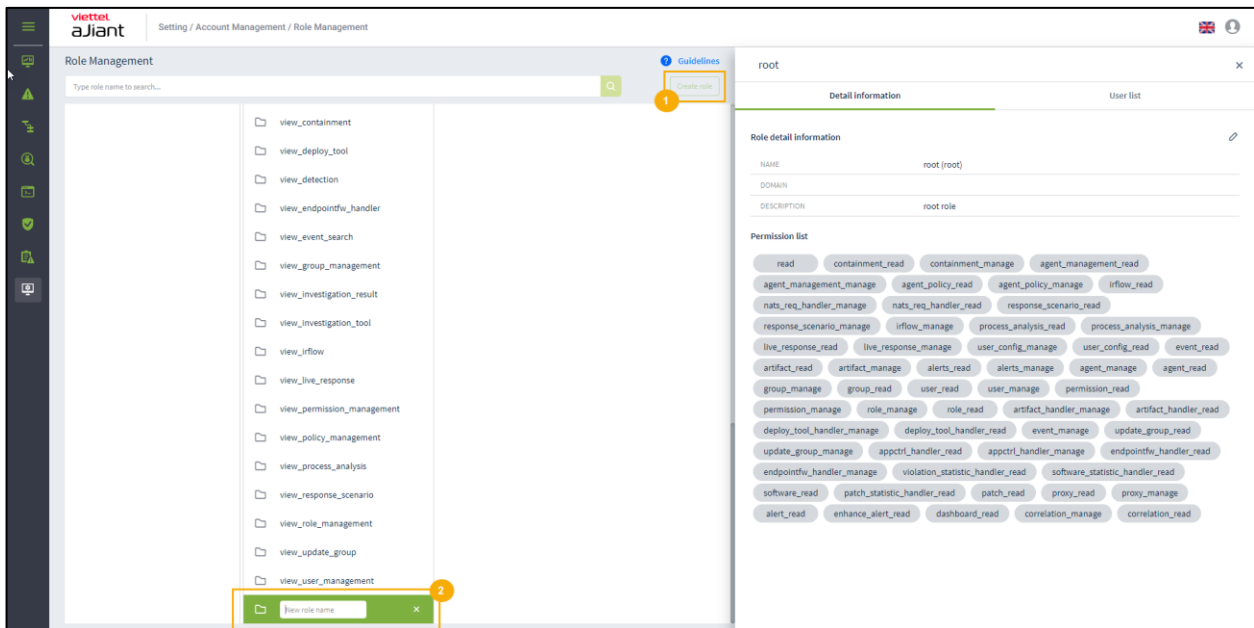
Bước 1: Có các cách tạo mới role như sau:

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.

view_irflow ×

Detail information User list

Role detail information ✎ 1

NAME	view_irflow (view_irflow)
DOMAIN	
DESCRIPTION	view_irflow

Permission list

irflow_read
containment_read
process_analysis_read
live_response_read
artifact_handler_read
response_scenario_read
deploy_tool_handler_read
event_read

view_live_response ×

Detail information User list

Role detail information Cancel Save 3

Name	view_live_response
Domain	
Description	view_live_response

Permission list 2

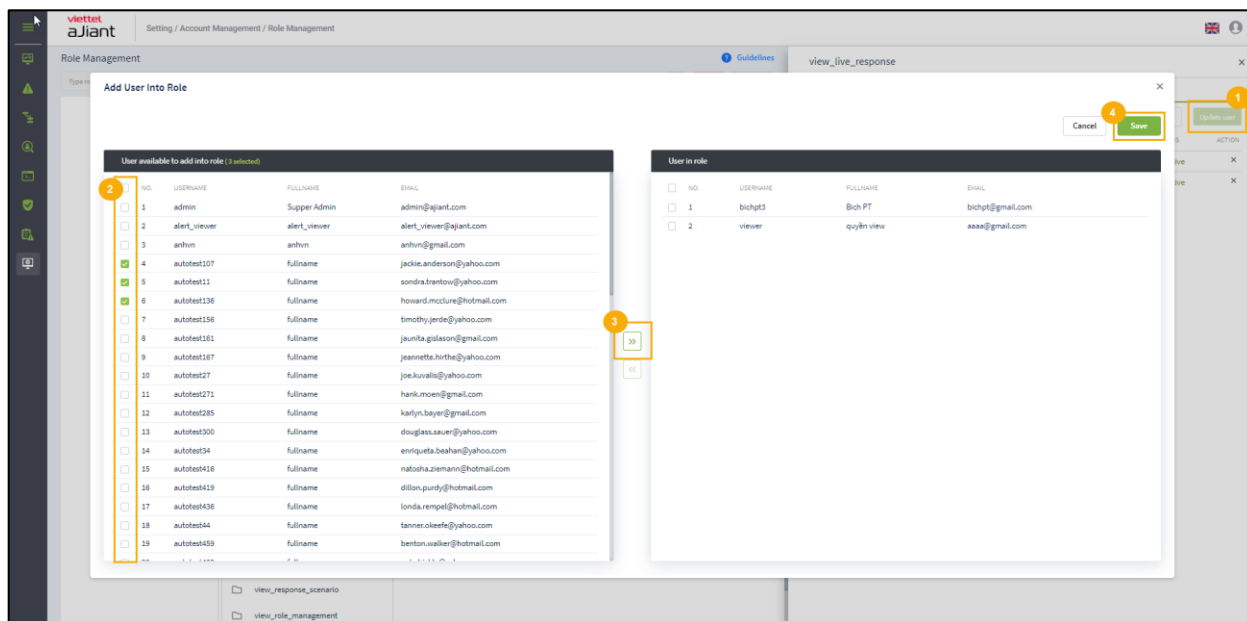
live_response_read ✕

read
containment_read
containment_manage
agent_management_read
agent_management_manage
agent_policy_read

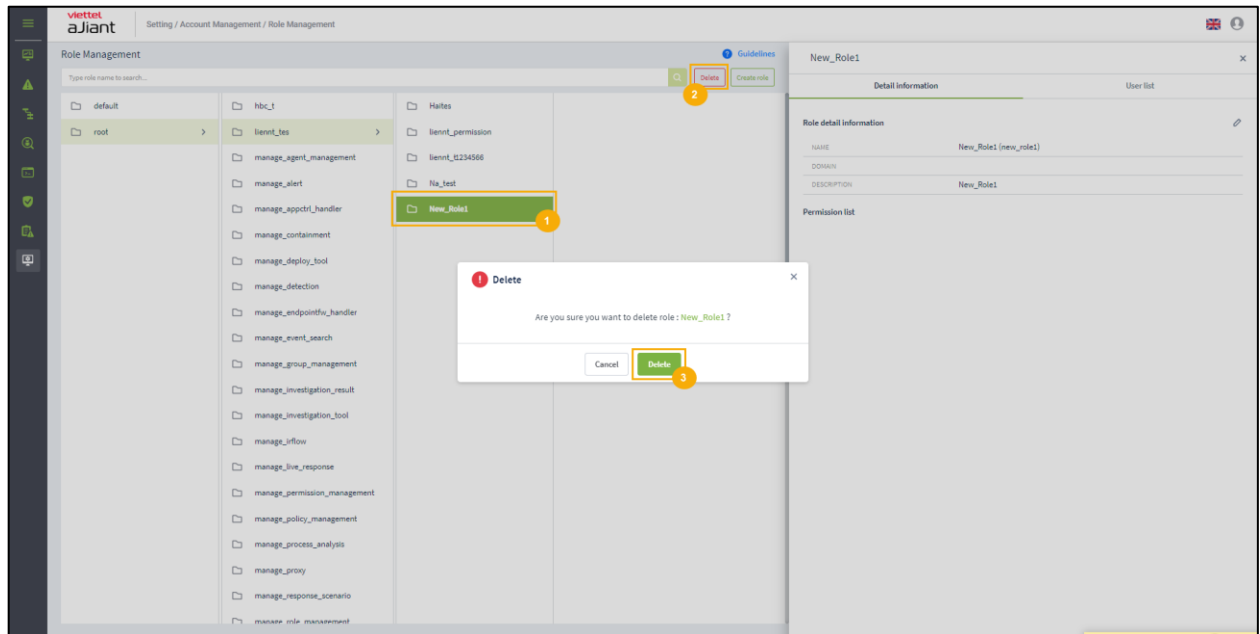
Bước 3: Chuyển sang tab User list để thêm role vào danh sách role của User

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

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



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



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

User management

Quản lý các tài khoản đăng nhập vào hệ thống Portal VCS-aJiant.
Các chức năng chính trên màn hình này gồm có:

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

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.ritchie@hotmail.com	N/A	Active	
9	autotest289	fullname	alec.stamm@gmail.com	N/A	Active	
10	autotest35	fullname	alica.lueitwitz@gmail.com	N/A	Active	
11	autotest362	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	Supper Admin	admin@ajiant.com	N/A	Active	
2	alert_viewer	alert_viewer	alert_viewer@ajiant.com	N/A	Active	
3	anhvn				Active	
4	autotest107				Active	
5	autotest11				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	autotest34				Active	
15	autotest416	fullname	natasha.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.hickle@yahoo.com	N/A	Active	
21	autotest49	fullname	gerald.ledner@gmail.com	N/A	Active	
22	autotest493	fullname	stefany.kill@yahoo.com	N/A	Active	

Showing 25/66 result(s)

Create

User information

Role

Group

Username

Fullname

Email

Password

Status

Active

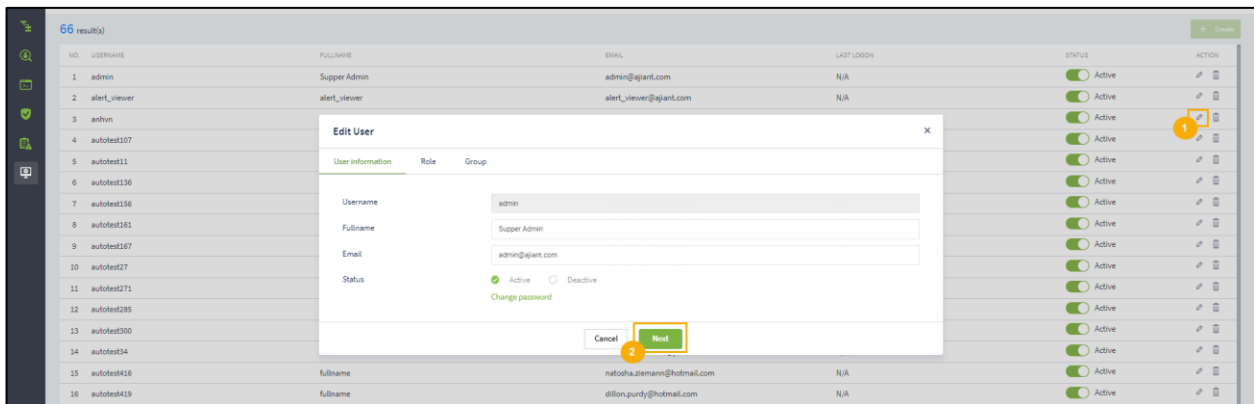
Deactive

Cancel

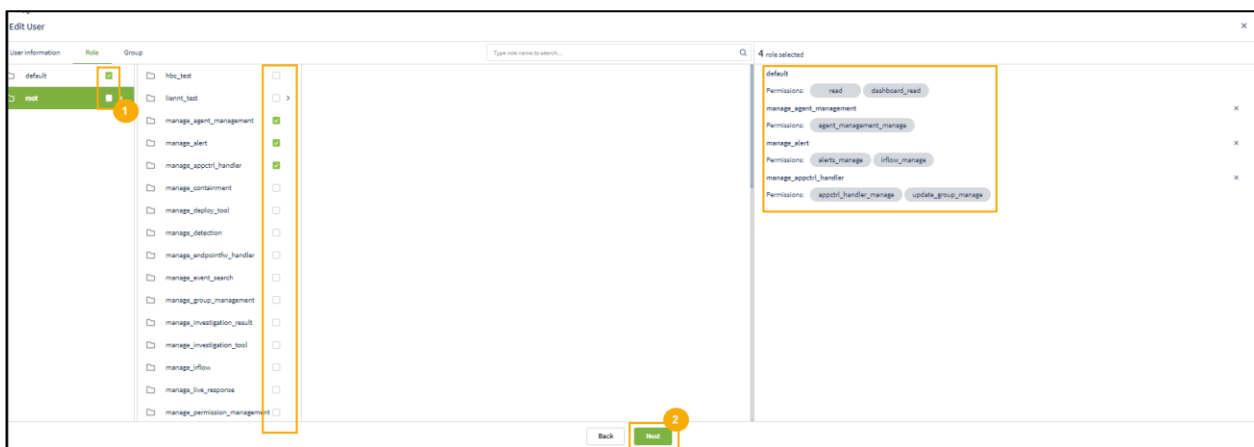
Next

- + 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: Hiển thị tất cả Role thuộc Role của user đang login;

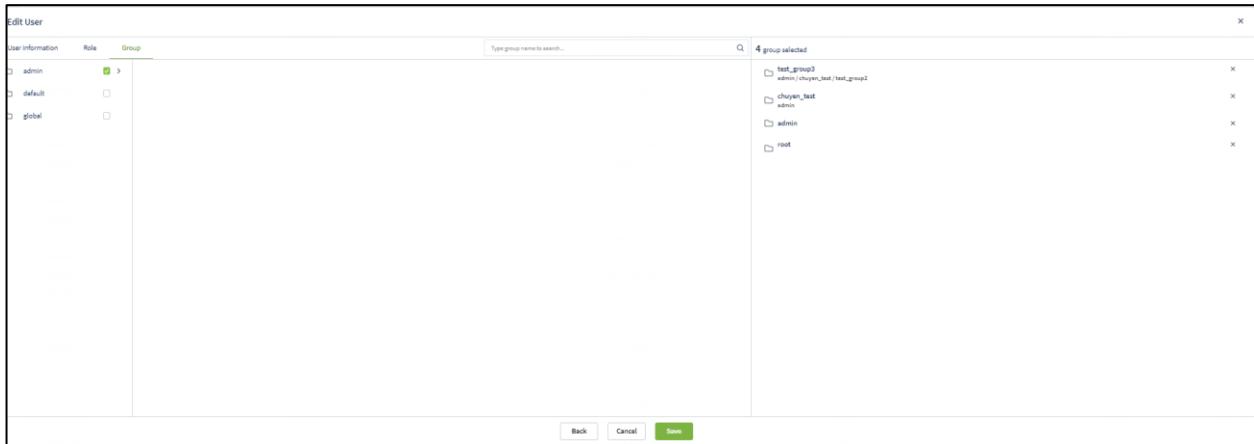


Trên màn hình add role cho User, có thể tìm kiếm các role tương tự phần tìm kiếm tài khoản, sau khi nhập các ký tự tìm kiếm vào textbox “Search” > click icon Search hoặc Enter hiện màn hình các role thỏa mãn điều kiện tìm kiếm;



- + Click chọn checkbox tương ứng với role cần thêm, sau đó click “Go to role” để về màn hình danh sách role ban đầu, sau đó click “Create” để tạo tài khoản;
- + Lưu ý: Tài khoản đang đăng nhập tạo 1 tài khoản mới chỉ tạo được các tài khoản chứa các role con thuộc danh sách role mà tài khoản đang đăng nhập được cấp;
- + Lựa chọn group sẽ gán cho tài khoản, sau đó click “Create”;
- + Khi click vào check box từng role sẽ hiện thị các permission (quyền) tương ứng với role đó;

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



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

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

Kiểm tra hiển thị icon xóa:

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

ID	USERNAME	FULLNAME	EMAIL	LAST_LOGIN	STATUS	ACTION
1	admin	SuperAdmin	admin@ajant.com	N/A	Active	
2	aler_viewer	aler_viewer	aler_viewer@ajant.com	N/A	Active	
3	arhyn	arhyn	arhyn@gmail.com	28/04/2022 10:44:40	Active	
4	autotest027	Fullname	jackie.anderson@yahoo.com	N/A	Active	
5	autotest011	Fullname	sandra.tanoto@yahoo.com	N/A	Active	
6	autotest036	Fullname	howard.mcdure@hotmail.com	N/A	Active	
7	autotest036	Fullname	timothy.jerde@yahoo.com	N/A	Active	
8	autotest081	Fullname	jaunita.gilason@gmail.com	N/A	Active	
9	autotest087	Fullname		N/A	Active	
10	autotest027	Fullname		N/A	Active	
11	autotest071	Fullname		N/A	Active	
12	autotest085	Fullname		N/A	Active	
13	autotest000	Fullname		N/A	Active	
14	autotest04	Fullname		N/A	Active	
15	autotest408	Fullname	natascha.ziemann@hotmail.com	N/A	Active	
16	autotest029	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

kYXRlcGlja2VyljoiRmlyc3QgUGluZylsImtleV90aW1lIjoiaWiaW50ZXJ2YWxfGltZSI6MCwidH...

First Ping

Export

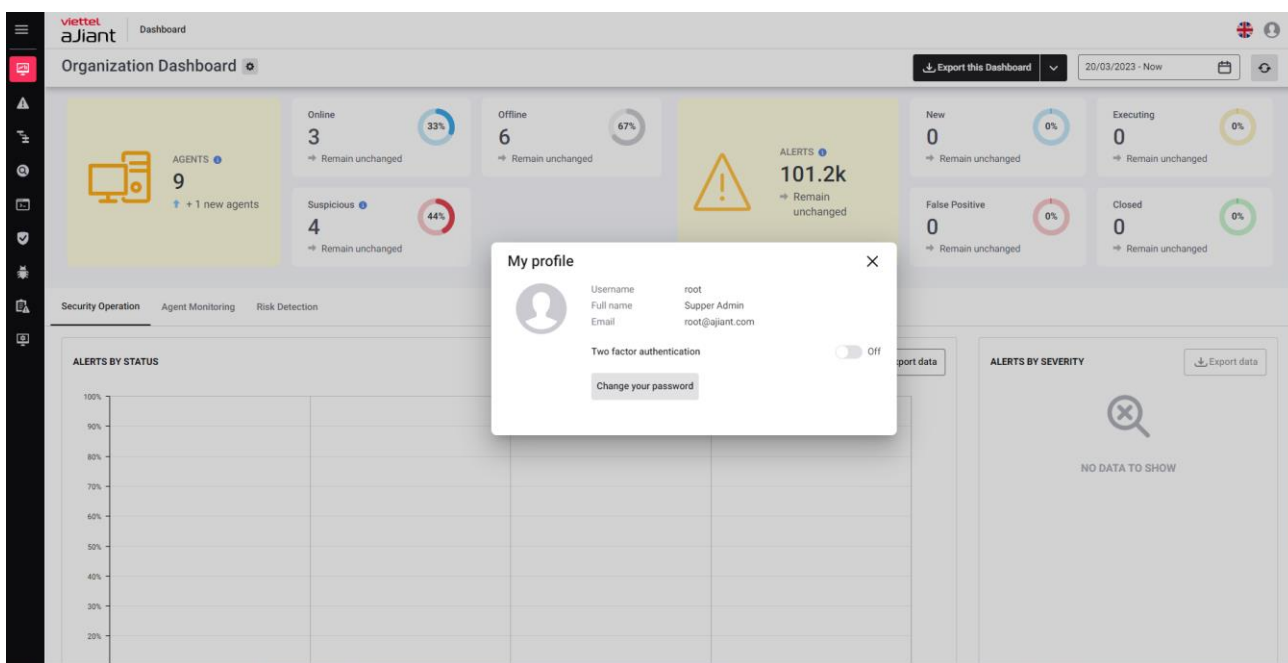
My profile

About VCS-aJiant

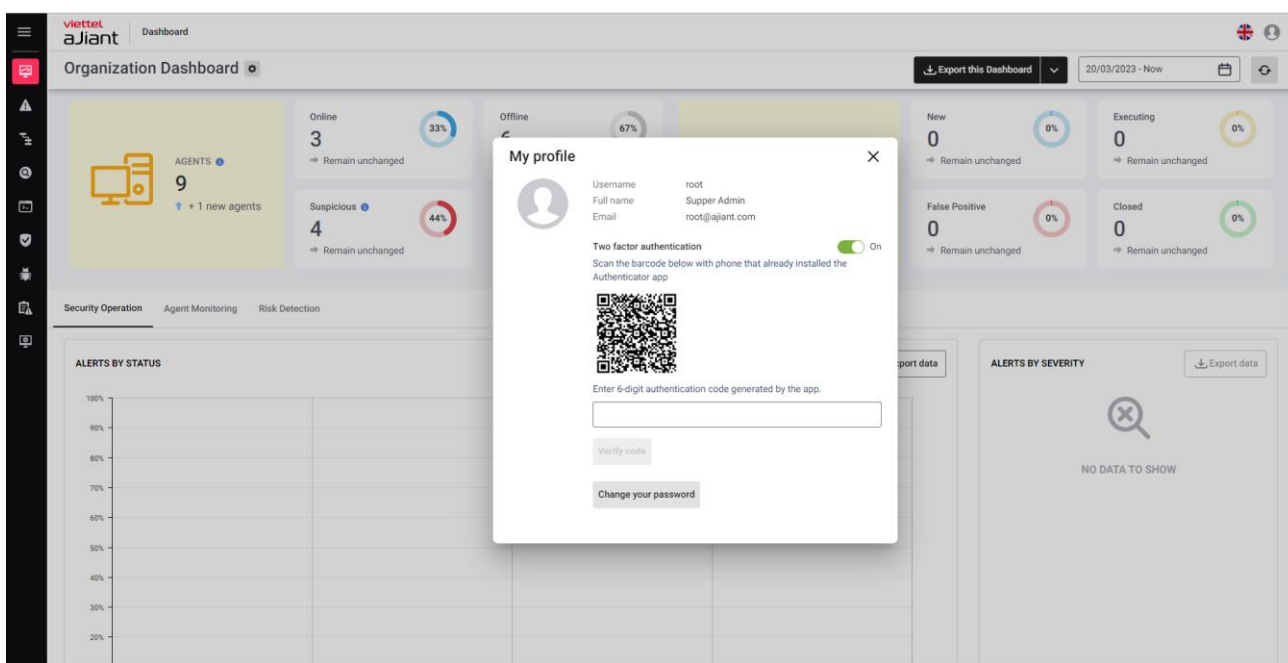
Sign out

First ping	IP DCN	Policy	
15/11/2021 07:14:51	10.207.26.203	full_features_3.3.0	3.3.37
13/11/2022 08:24:49	10.61.74.206	full_features_3.3.0	3.3.37
10/07/2020 17:24:36	10.230.65.69	full_features_3.3.0_linux	3.3.36
2/01/2023 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
15/09/2022 20:33:15	192.168.81.44	full_features_3.3.0	3.3.37

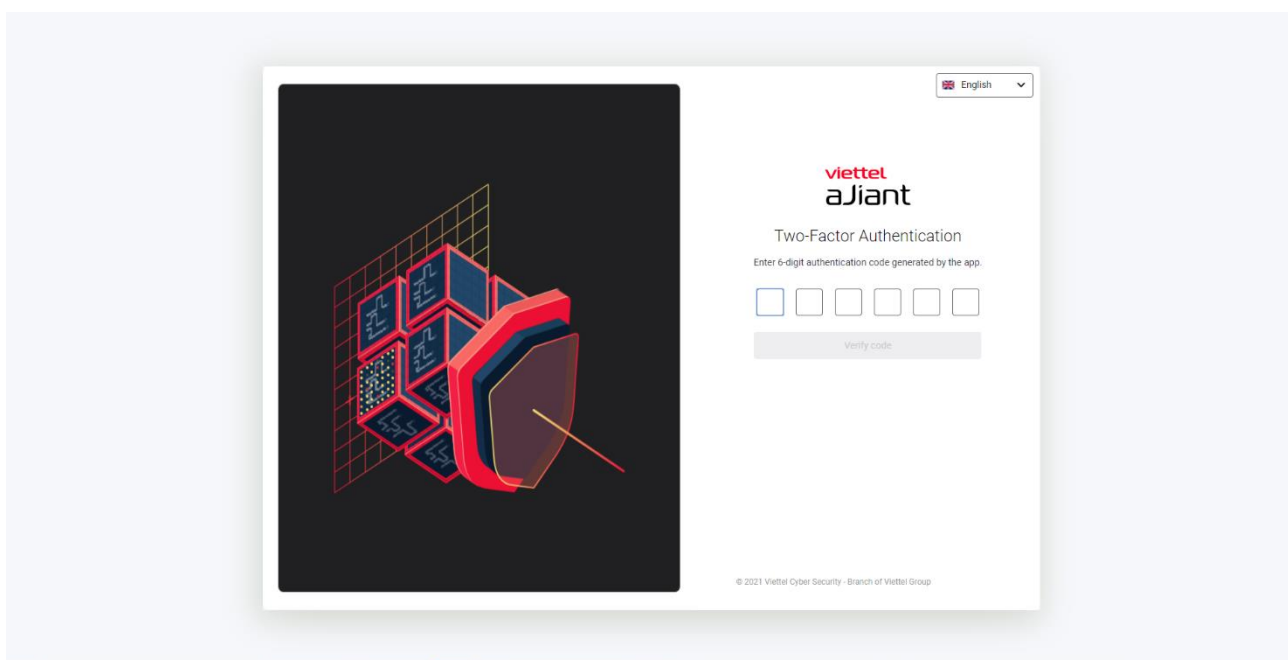
Bước 2: Click để bật Two Factor authentication



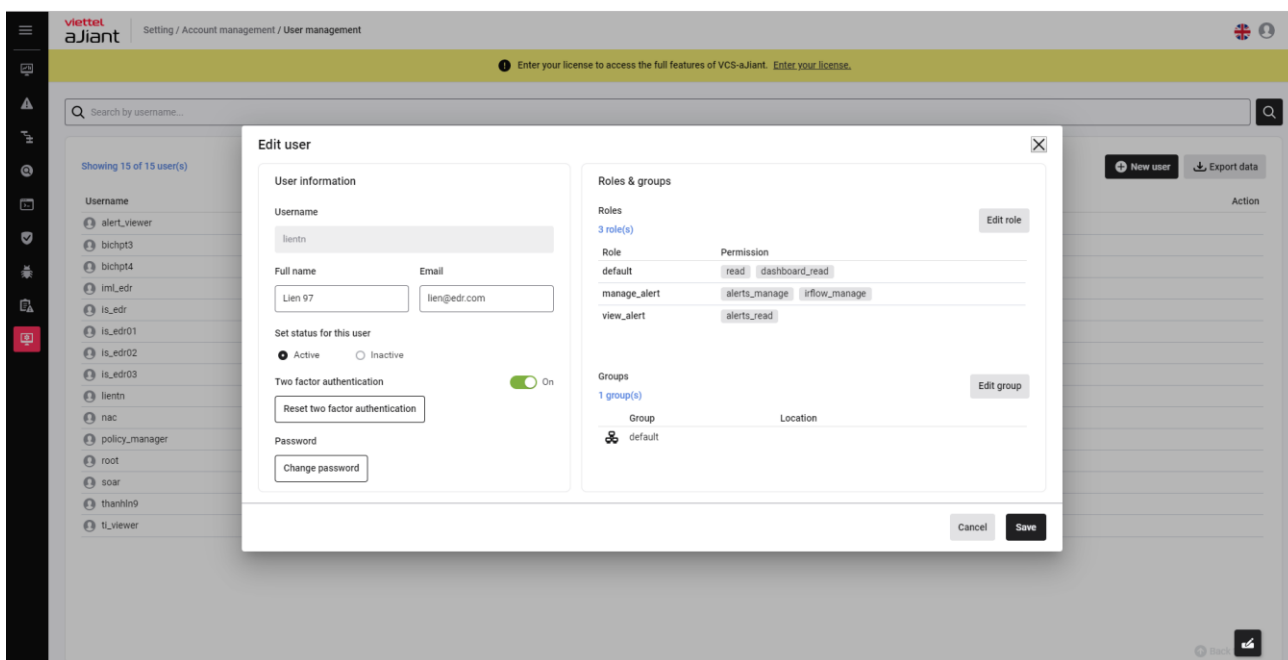
Bước 3: Dùng 2FA app để quét mã QR, sau đó nhập OTP để hoàn thành quá trình bật 2FA



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

3.6.5 Update management

Update groups

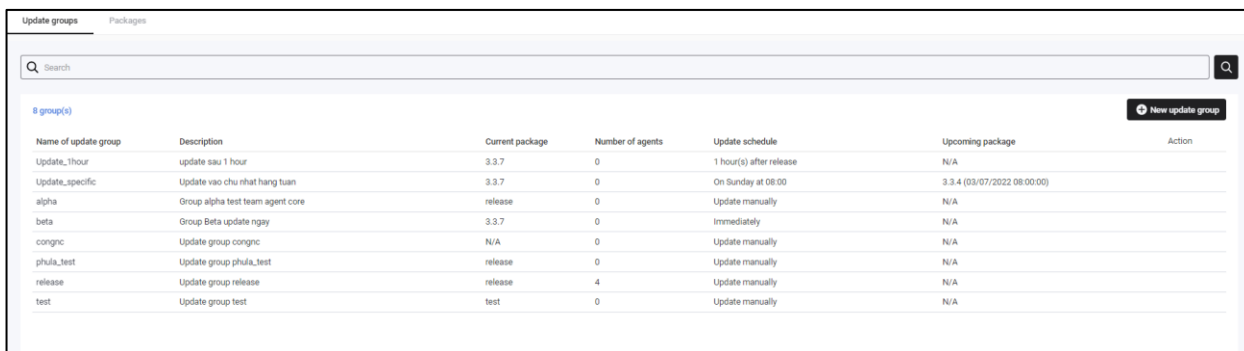
Mục đích: là tính năng cho phép quản lý, tạo mới và cập nhật các Update Group (Chia các Agent thành các nhóm cập nhật, giúp dễ dàng phân chia, quản lý)

1 – Tìm kiếm:

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

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

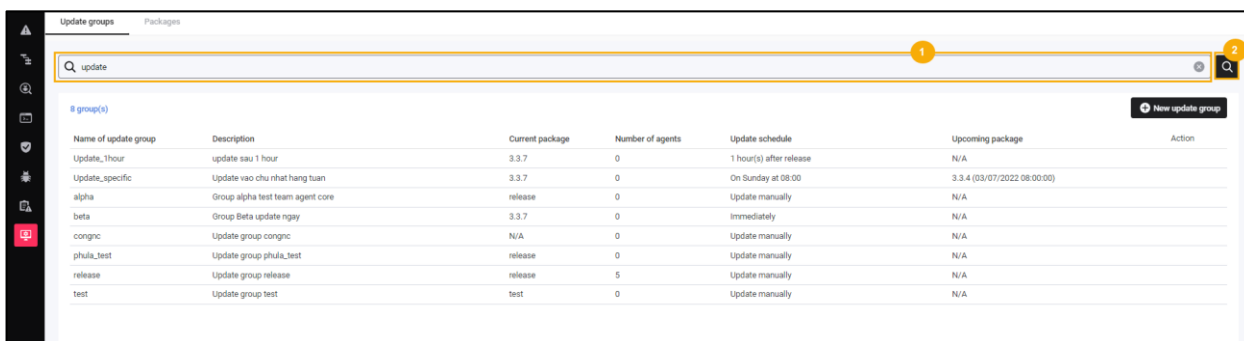
Bước 3: Chọn Update Management, hệ thống hiển thị Danh sách Update Group;



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”



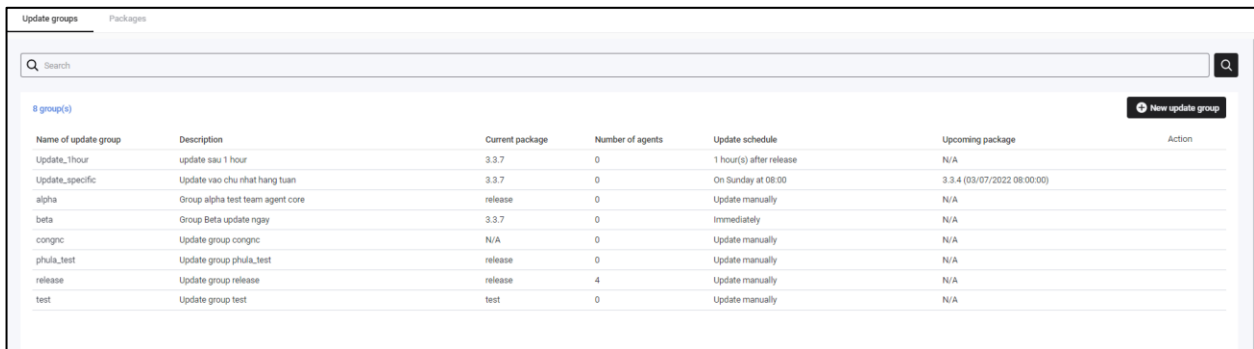
Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
Update_1hour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	
Update_specific	Update vào chủ nhật hàng tuần	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	
alpha	Group alpha test team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

2 – Thêm mới Update groups:

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

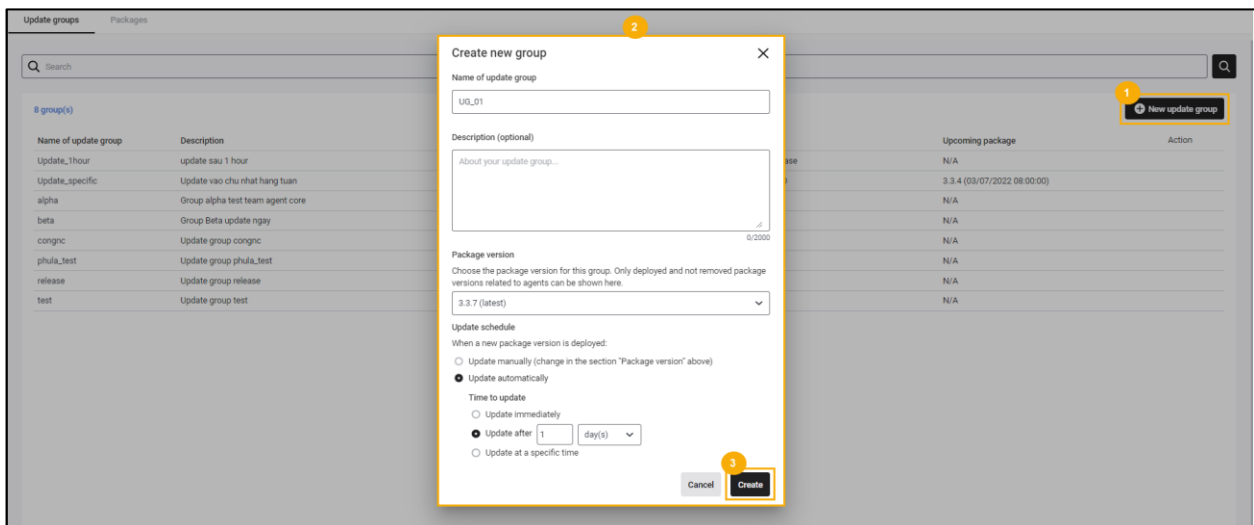
Bước 2: Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;

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



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



Create new group

Name of update group:

Description (optional):

Package version:

Update schedule: ☒ Update automatically

Time to update: ☒ Update after 1 day(s)

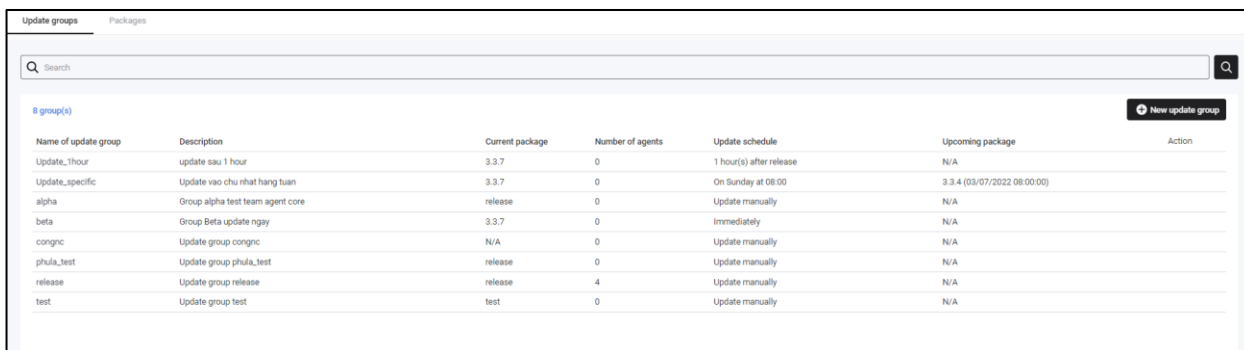
Bước 5: Nhập thông tin thêm mới Update Group và chọn nút “Create”. Hệ thống ghi nhận và quay về màn hình danh sách Update Group.

3 – Cập nhật Update groups:

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

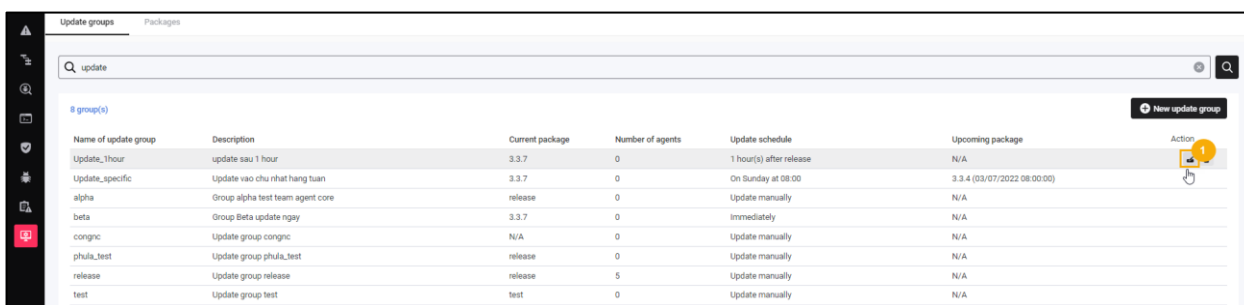
Bước 2: Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;

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



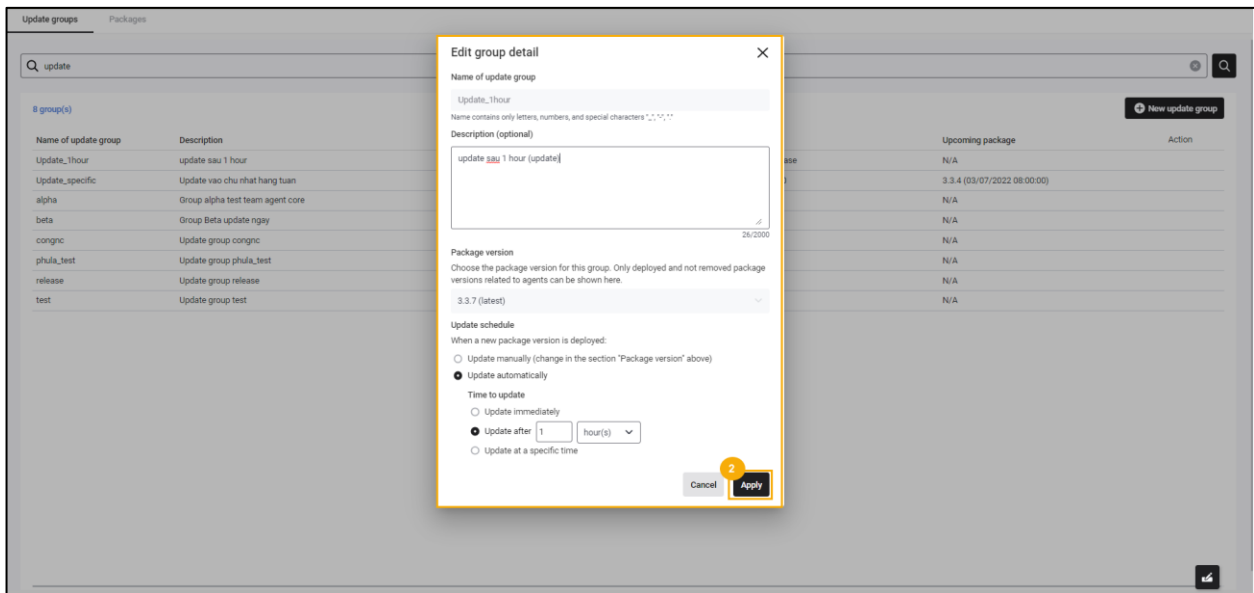
Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
Update_1hour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	New update group
Update_specific	Update vào chủ nhật hàng tuần	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	
alpha	Group 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”:



4 – Xóa Update groups:

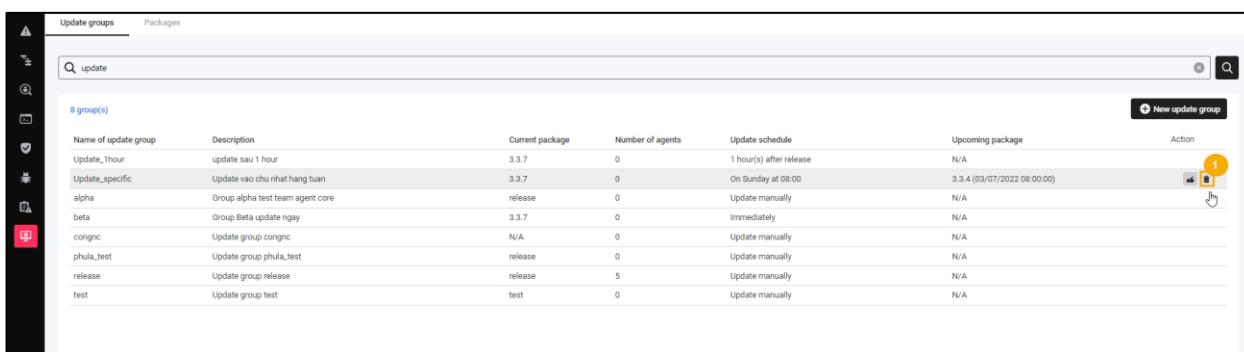
Bước 1: Login vào Portal bằng tài khoản đã được cung cấp;

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

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

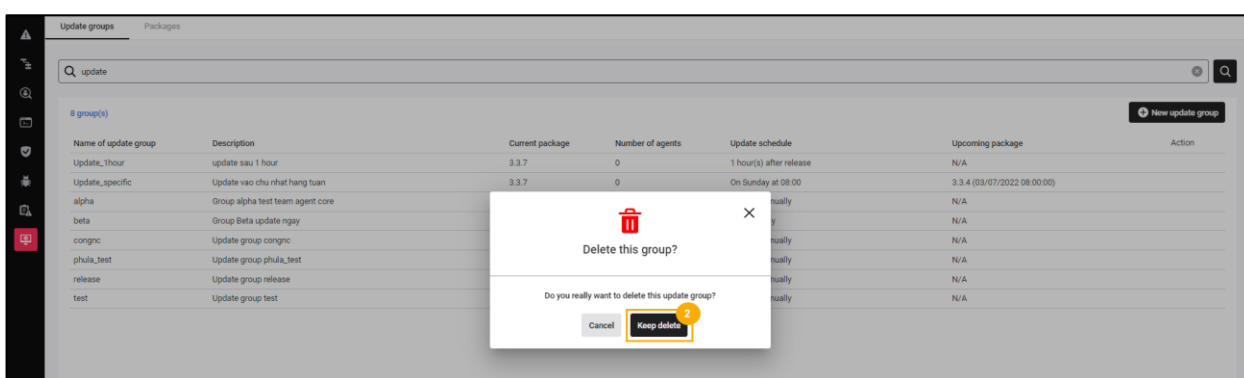
Name of update group	Description	Current package	Number of agents	Update schedule	Upcoming package	Action
Update_1hour	update sau 1 hour	3.3.7	0	1 hour(s) after release	N/A	
Update_specific	Update vào chủ nhật hàng tuần	3.3.7	0	On Sunday at 08:00	3.3.4 (03/07/2022 08:00:00)	
alpha	Group alpha test team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



Update packages

1 – Tìm kiếm packages:

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

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

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

Bước 4: Chọn tab “Package”, hệ thống hiển thị Danh sách 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	

2 – Auto Update

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

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

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

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

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

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

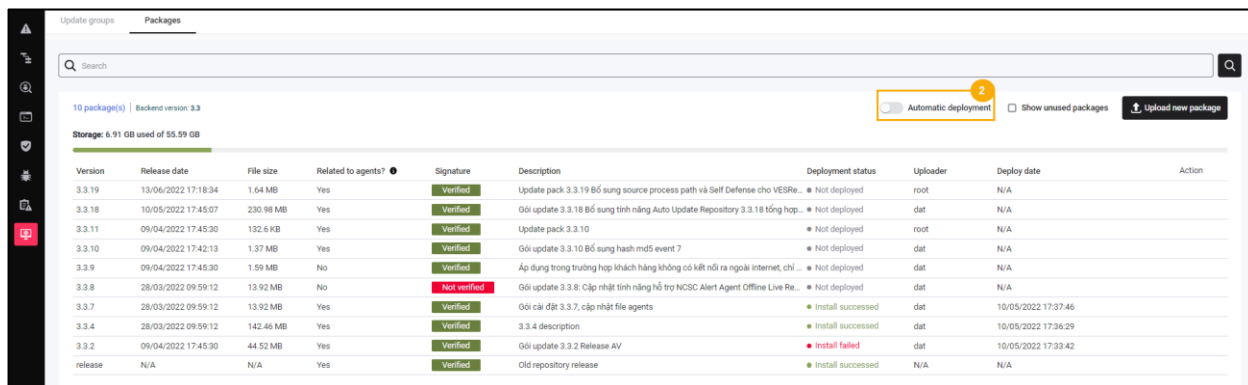
Bước 5: Chọn nút “Update new package”, hệ thống hiển thị Popup “Upload package”;

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;

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



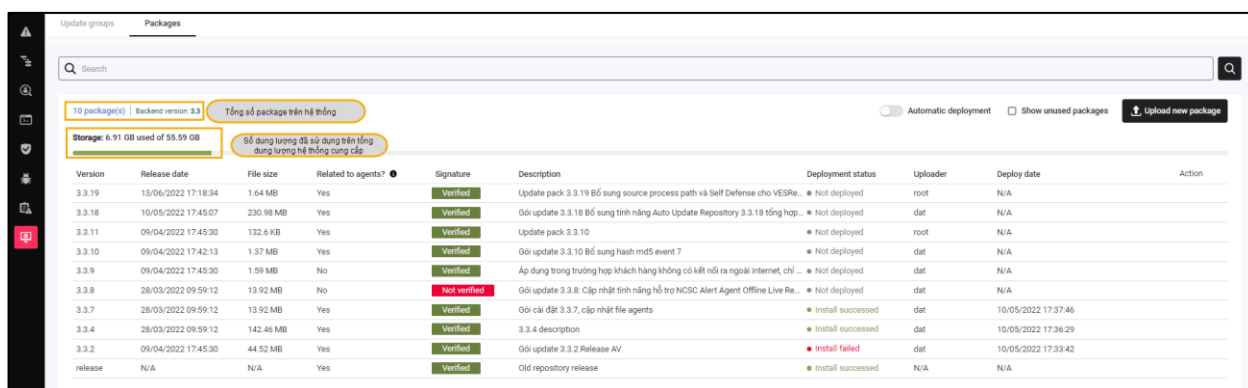
3 – Deploy package

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

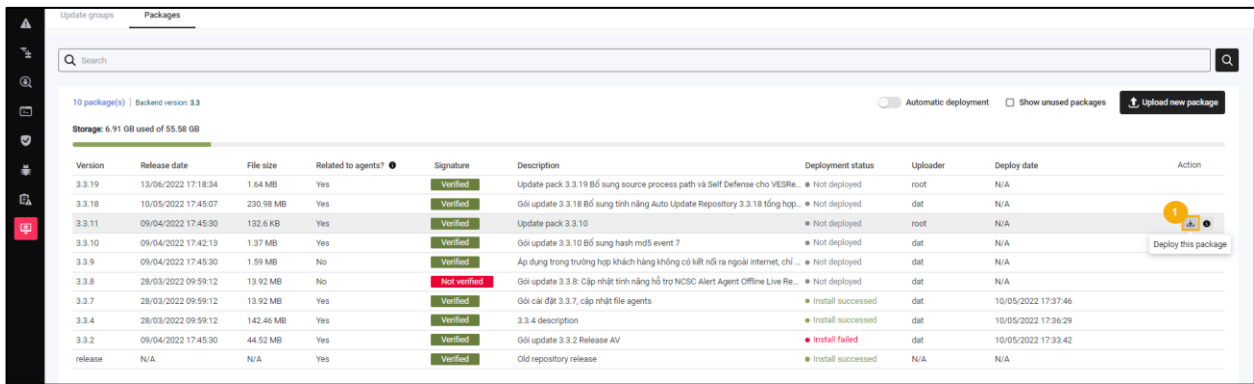
Bước 2: Chọn Setting, hệ thống hiển thị các sub-menu: Policy Setting, Agent Management, Group Management, Update Management, Rules Correlation, Account Management;

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

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

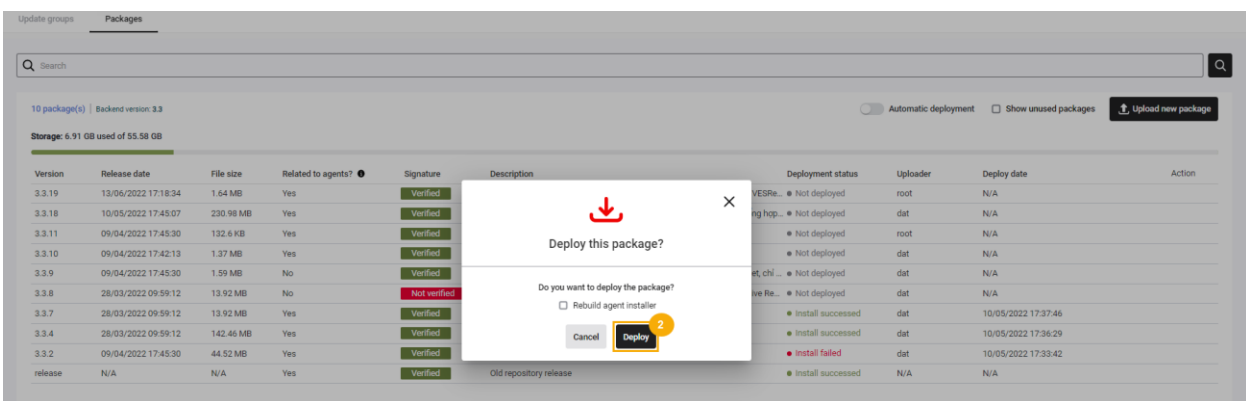


Bước 5: Chọn icon “Deploy this package” tại bản ghi package đó, hệ thống hiển thị Popup Xác nhận Deploy package



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	
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	Deploy this package
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 nút “Deploy” để xác nhận Deploy package trên thiết bị hoặc chọn nút “Cancel” để hủy thao tác Deploy package.



4 – Chi tiết Package

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

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

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

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

3.7 Chức năng Baseline Policy (BLS)

3.7.1 Thống kê vi phạm (Violation statistic)

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

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

+ Xem danh sách các đơn vị vi phạm và danh sách vi phạm trong từng đơn vị;

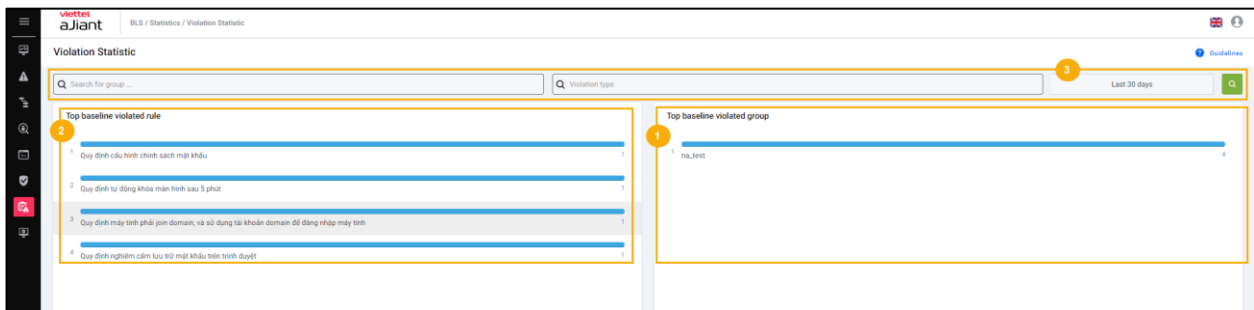
+ Xem chi tiết của Agent;

+ Export vi phạm;

+ Report vi phạm;

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

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;

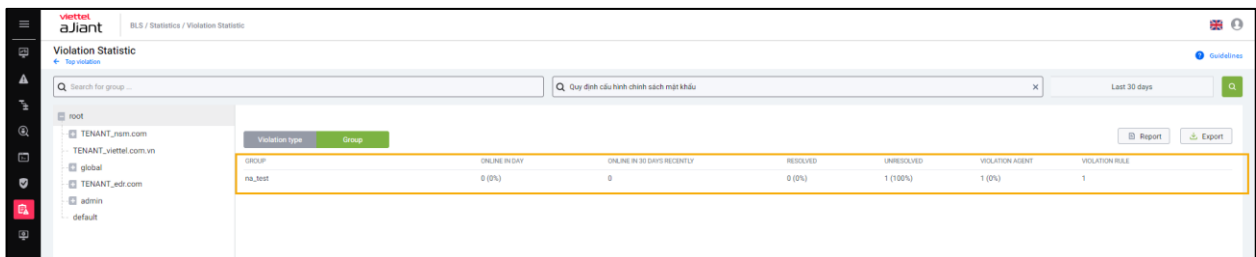
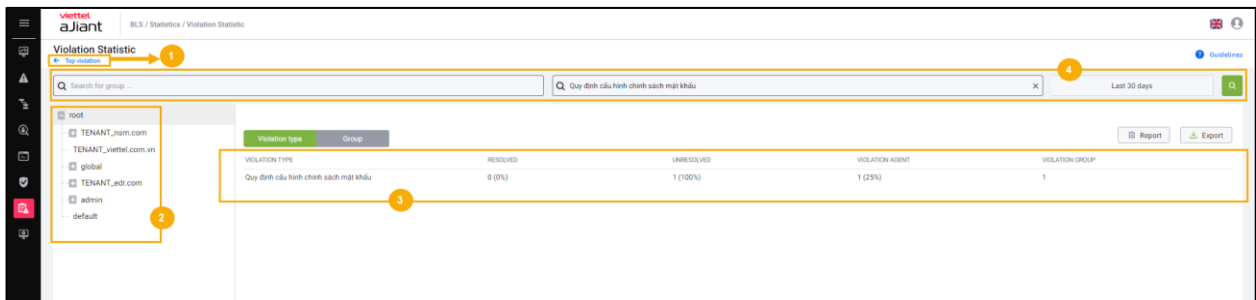
Mô tả các rule trong BLS

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
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 bật chế độ cập nhật bản vá hệ điều hành tự động
Quy định cài đặt và sử dụng phần mềm	Máy trạm vi phạm rule này khi cài đặt hoặc không cài đặt các phần mềm được cấu hình
Quy định bắt buộc cài đặt và sử dụng phần mềm diệt virus	Yêu cầu máy trạm phải cài đặt phần mềm antivirus: luôn bật chức năng realime protection và thiết lập cấu hình update.
Quy định bắt buộc sử dụng phần mềm vượt tường lửa	Yêu cầu máy trạm phải bật firewall trên hệ điều hành hoặc trên phần mềm antivirus
Quy định cài đặt và sử dụng phần mềm diệt virus Kaspersky	Yêu cầu máy trạm bắt buộc phải cài phần mềm AV Kaspersky
Quy định máy tính phải join domain, và sử dụng tài khoản domain để đăng nhập máy tính	Quy định máy tính phải join domain, và sử dụng tài khoản domain để đăng nhập máy tính
Quy định thu hồi tài khoản local	Tự động thu hồi (remove) tài khoản local khi vi phạm

Quy định nghiêm cấm lưu trữ mật khẩu trên trình duyệt	Nghiêm cấm lưu trữ mật khẩu trên trình duyệt
Quy định cấu hình chính sách mật khẩu	Quy định bao gồm các rule sau: + Đáp ứng đủ số kí tự + Thay đổi mật khẩu sau một khoảng thời gian được config + Tài khoản bị khóa sau khi nhập sai nhiều lần

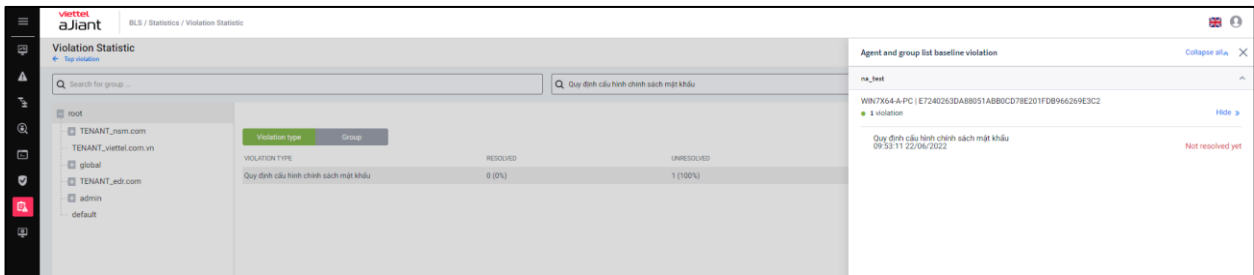
Tab Loại vi phạm



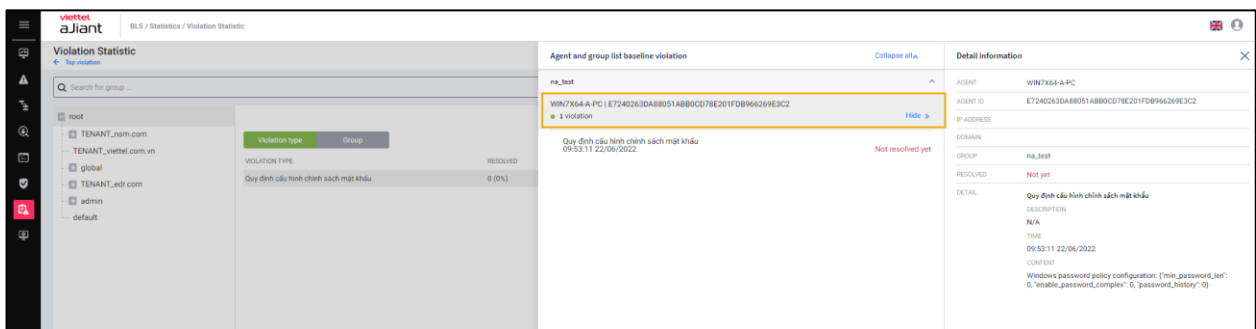
Hệ thống hỗ trợ thực hiện các tính năng:

- + Chọn link Top vi phạm: Di chuyển về màn hình Dashboard, danh sách top vi phạm và top đơn vị vi phạm
- + Cây dữ liệu đơn vị của hệ thống

- 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

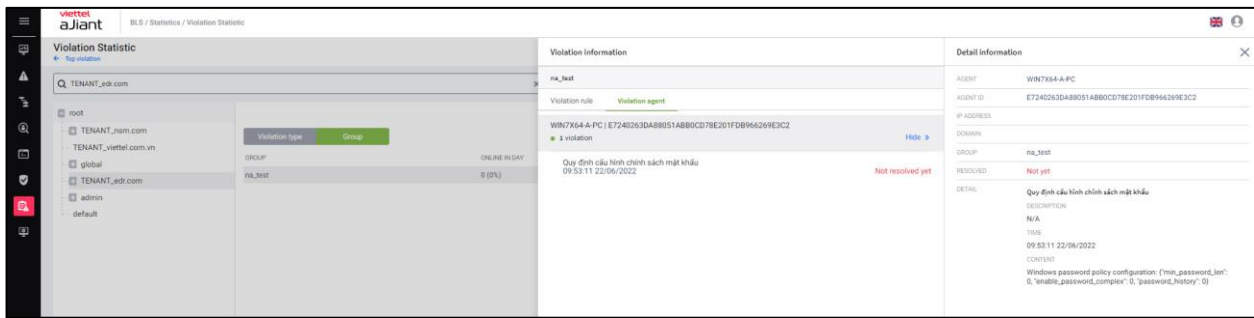
- Loại vi phạm: Hiển thị vi phạm đã chọn
 - Thời gian bị vi phạm
- + Tìm kiếm kết hợp: Khi nhập 2 hoặc nhiều điều kiện tìm kiếm thì sẽ thực hiện tìm kiếm theo điều kiện AND

Tab Đơn vị

Violation type	Group	ONLINE IN DAY	ONLINE IN 30 DAYS RECENT	RESOLVED	UNRESOLVED	VIOLATION AGENT	VIOLATION RULE
na_test		0 (0%)	0	0 (0%)	1 (100%)	1 (0%)	1

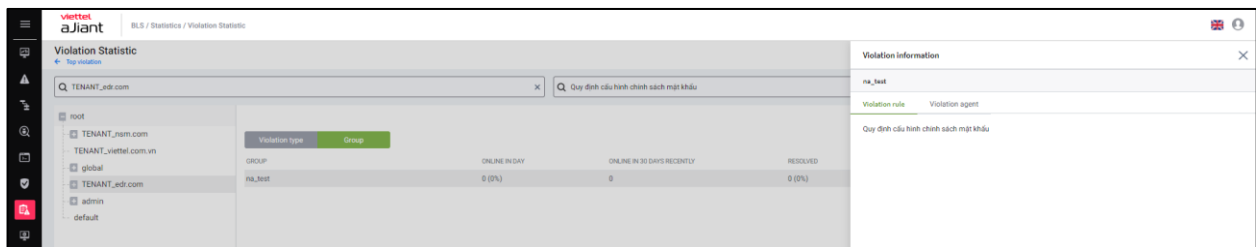
Hệ thống hỗ trợ thực hiện các tính năng:

- + Chọn link Top đơn vị: Di chuyển về màn hình Dashboard, danh sách top vi phạm và top đơn vị vi phạm;
- + Cây dữ liệu đơn vị của hệ thống;
 - Hiển thị toàn bộ đơn vị của hệ thống được phân cấp cha-con;
 - Có thể chọn đơn vị trên cây dữ liệu đơn vị để thực hiện lọc đơn vị cha – con;
- + Tab Đơn vị;
 - Mỗi Loại vi phạm được hiển thị các thông tin chung gồm: Unit, Online in day, Online in 30 days recent, Resolved, Unresolved, Violation computer, Violation rule;
 - Chọn icon detail của cột violation computer trên danh sách: Hiển thị danh sách máy tính trong từng đơn vị vi phạm bao gồm Tên đơn vị, Tên máy tính|Agent ID, danh sách vi phạm của từng máy, thời gian vi phạm, trạng thái vi phạm (đã fix hay chưa fix vi phạm);



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

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



Tìm kiếm

+ Tìm kiếm riêng lẻ:

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

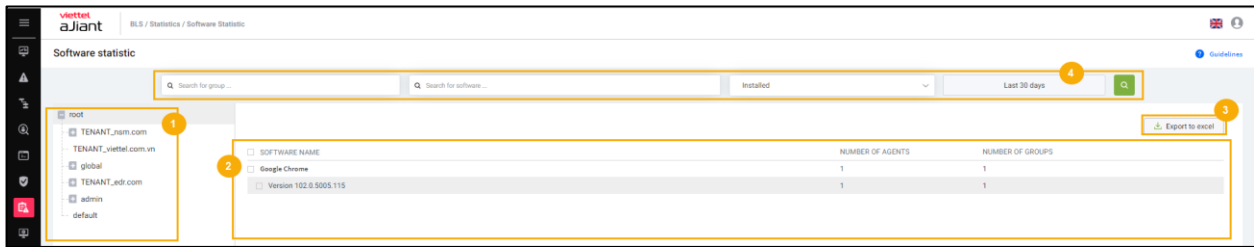
+ Tìm kiếm kết hợp: Khi nhập 2 hoặc nhiều điều kiện tìm kiếm thì sẽ thực hiện tìm kiếm theo điều kiện AND;

3.7.2 Thống kê phần mềm (Software statistic)

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

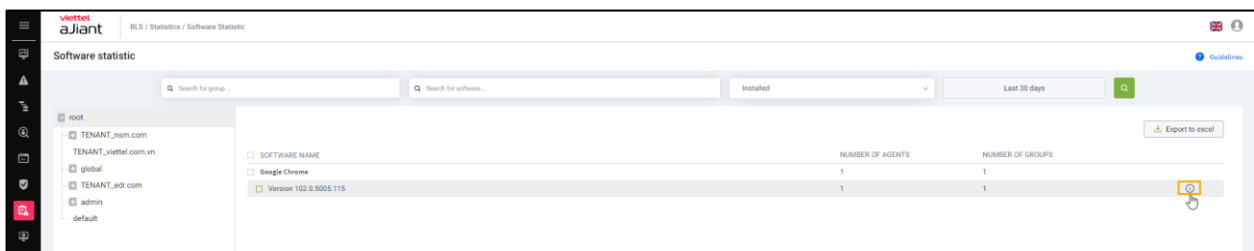
- + Xem danh sách các phần mềm đã cài trong 1 đơn vị được chọn;

- + Xem chi tiết của Agent;
- + Export phần mềm;

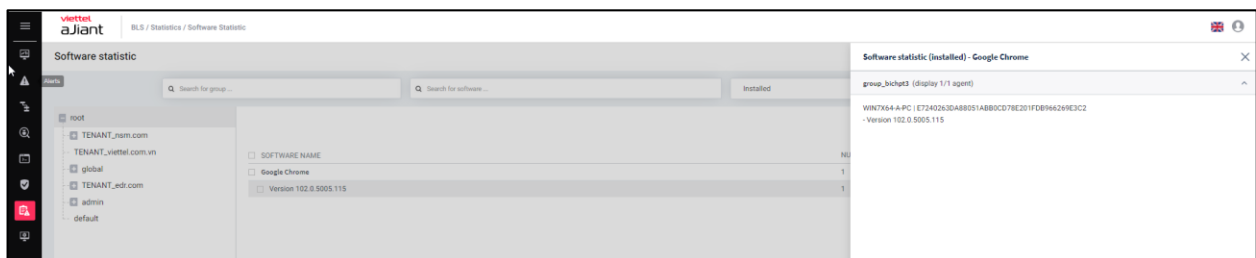


Hệ thống hỗ trợ thực hiện các tính năng:

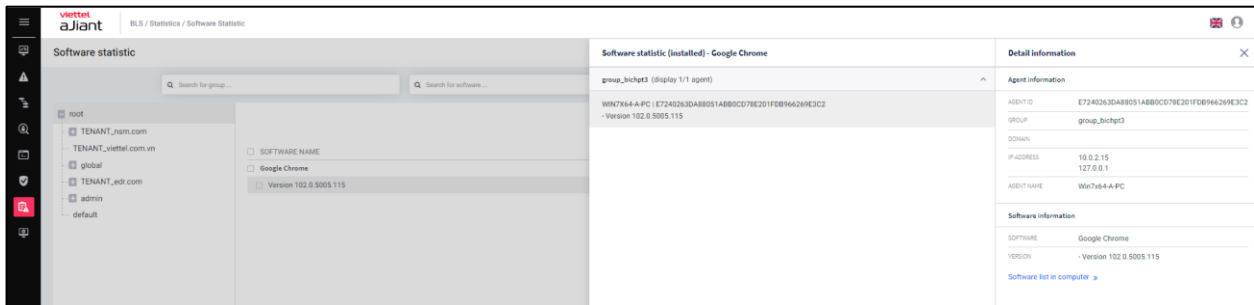
- + Cây dữ liệu đơn vị của hệ thống
- + Hiển thị toàn bộ đơn vị của hệ thống được phân cấp cha-con
- + Có thể chọn đơn vị trên cây dữ liệu đơn vị để thực hiện lọc phần mềm
- + Danh sách phần mềm
 - Mỗi phần mềm được hiển thị các thông tin chung gồm: Software name, number of computer, number of unit;



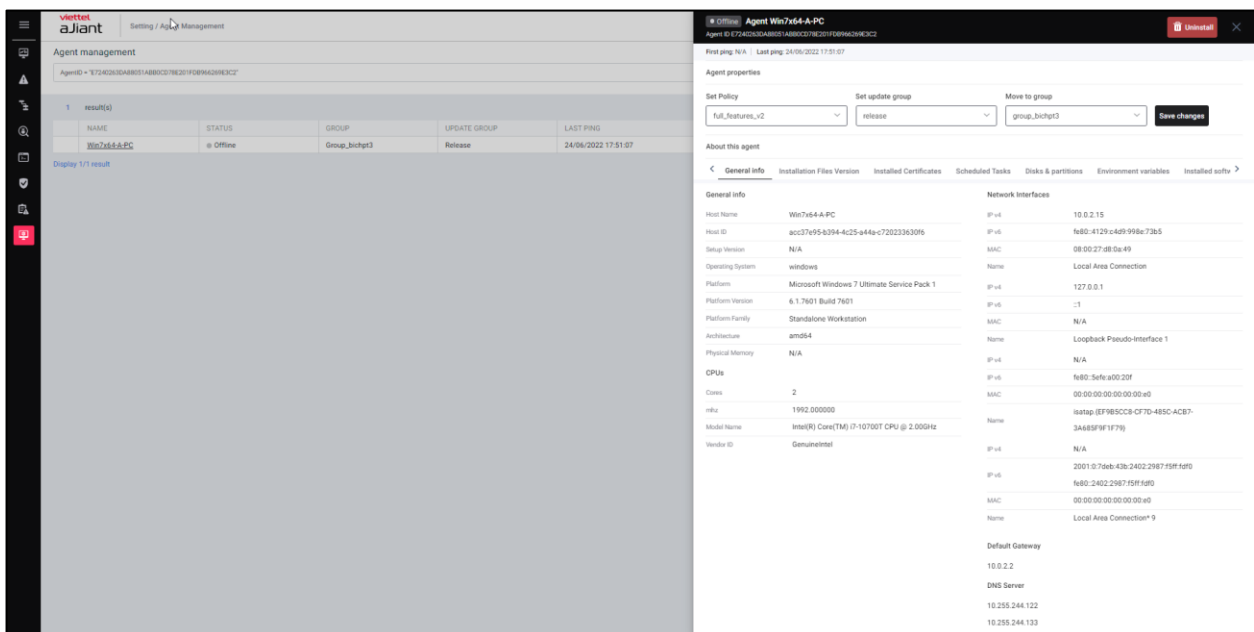
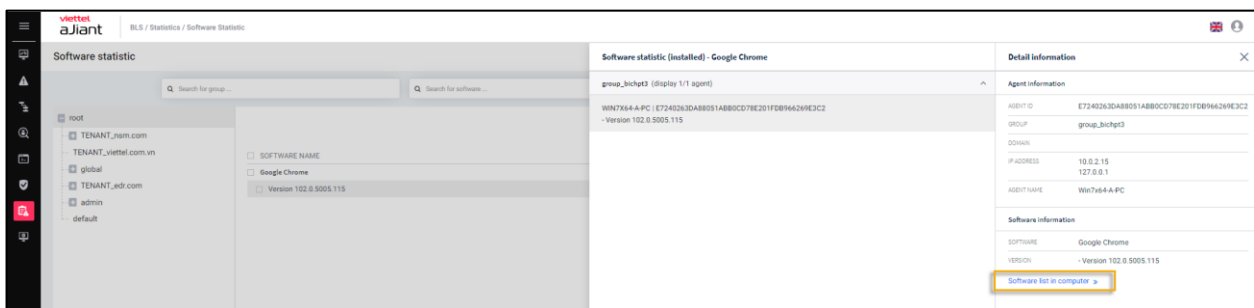
- Chọn icon detail của cột violation computer trên danh sách: Hiển thị danh sách máy tính trong từng đơn vị bao gồm Tên đơn vị, Tên máy tính|Agent ID, Version;



- 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

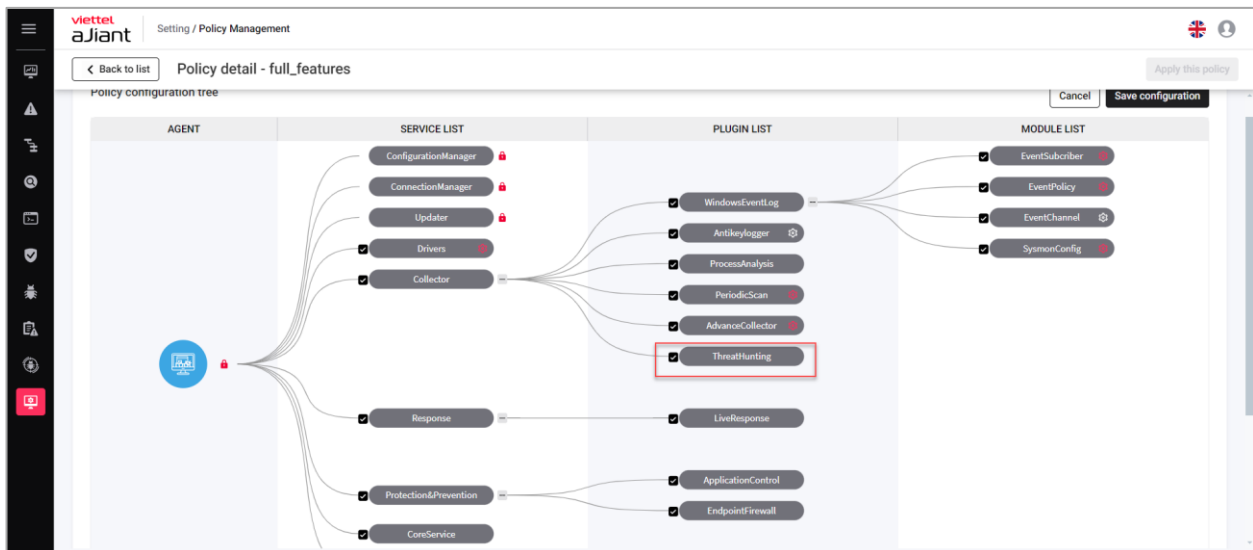
Export: Chọn Export: Hệ thống sẽ download file Export có dữ liệu giống với dữ liệu đang hiển thị trên màn hình

3.8 Threat Hunting

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

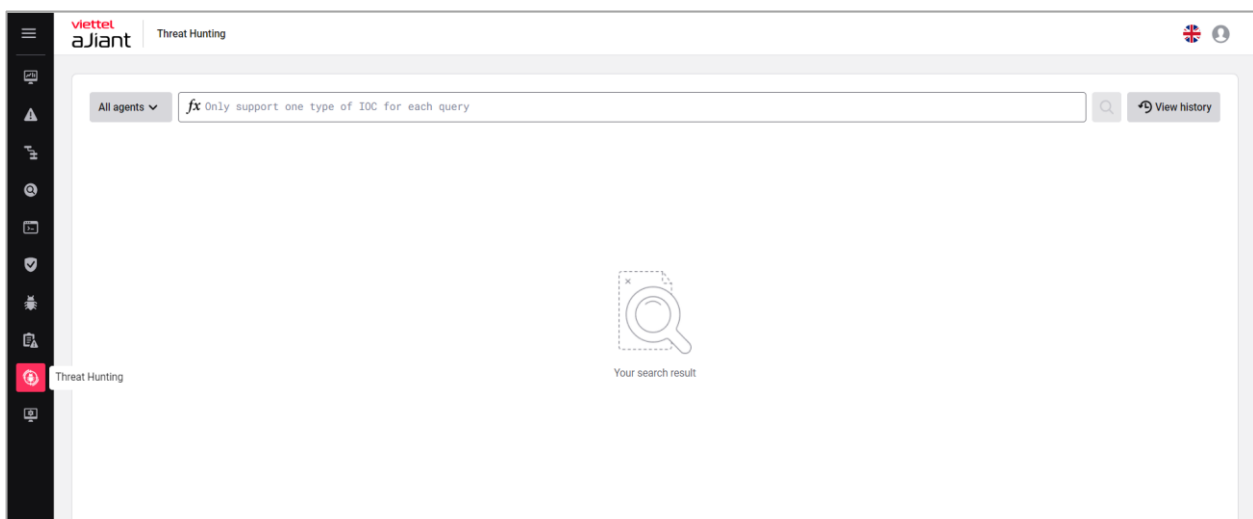
3.8.1 *Bật/tắt policy*

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

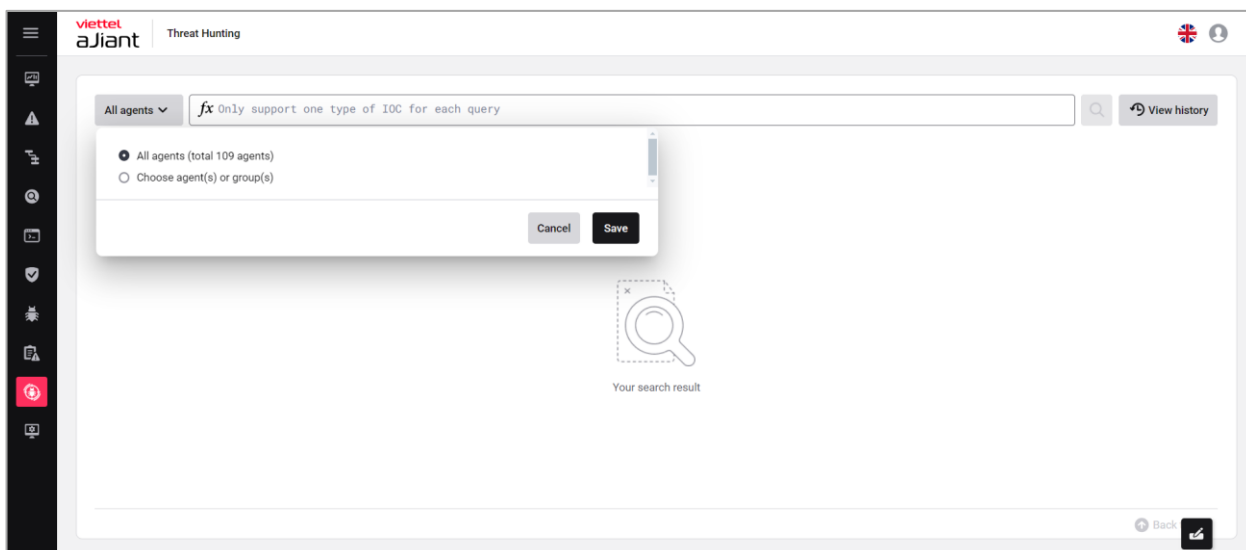


3.8.2 Tìm kiếm theo agents/ nhóm

- Trên Menu chọn Threat Hunting



- Cho phép admin tìm kiếm iocs theo agents/ groups
 - 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



3.8.3 Tìm kiếm IOCs

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	registry_data_string	~	

Registry data				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
-----	-----	----------	------	--------------------------------------

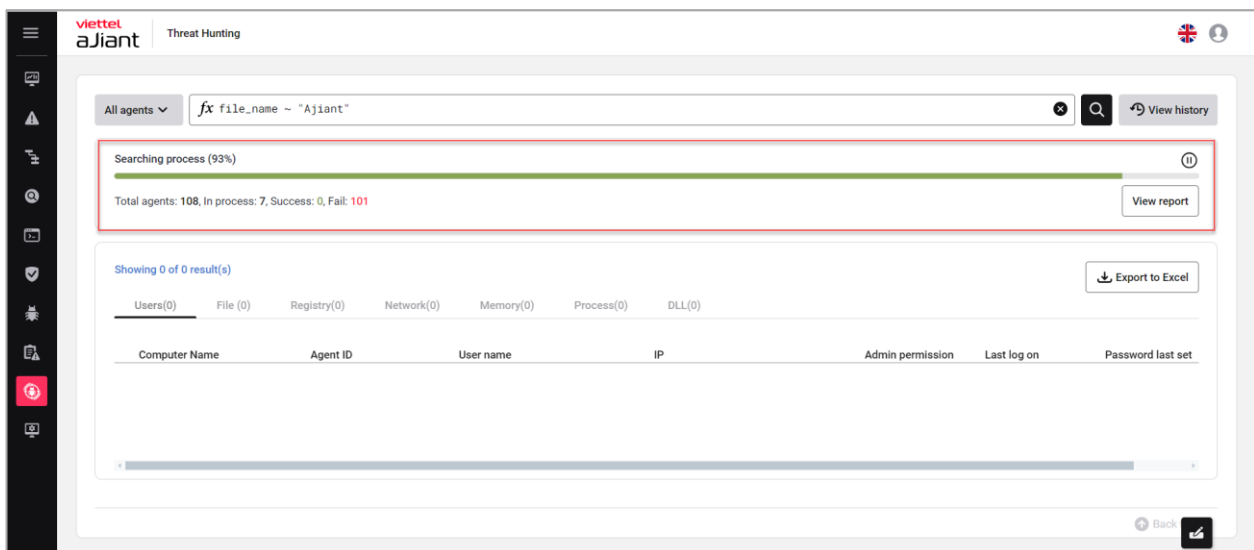
Lưu ý:

- 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.

Chi tiết kết quả tìm kiếm

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



Chi tiết kết quả tìm kiếm

- Cho phép người dùng xem chi tiết kết quả tìm kiếm theo từng tab

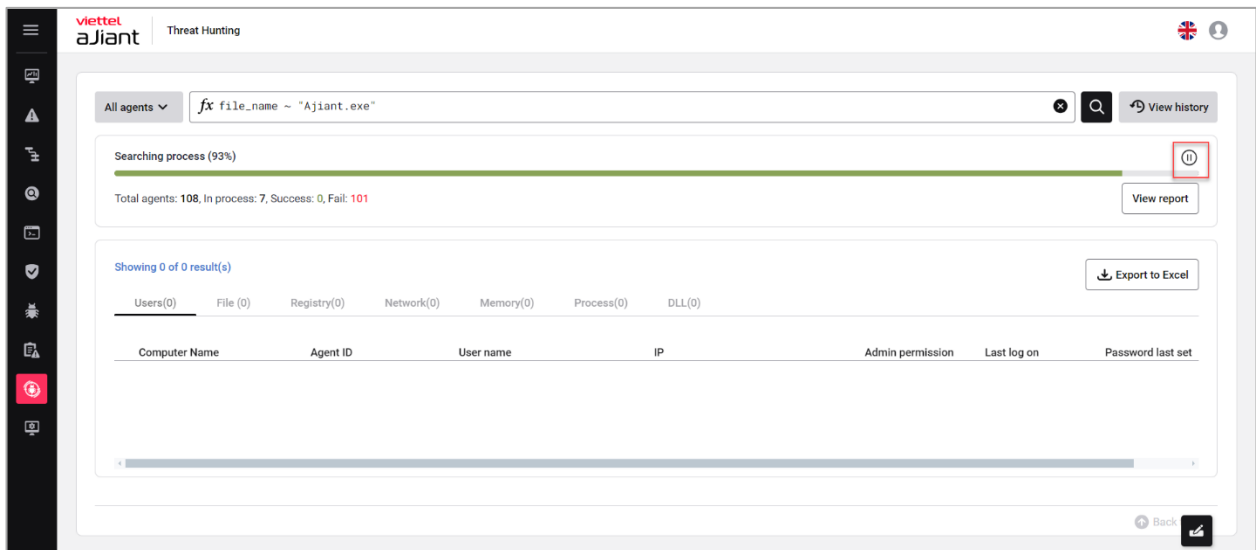
- Users
 - File
 - Registry
 - Network
 - Memory
 - Process
 - DLL
- Kết quả được hiển thị đúng theo từng tab theo đúng câu truy vấn của người dùng

The screenshot shows the Viettel Ajiant Threat Hunting dashboard. The search bar contains the query 'file_name ~ "Ajiant"'. The search is completed (100%). The results show 7 files found. The table below lists the details of these files.

Computer Name	Agent ID	IP	File Name	File path	File hash SHA256	File created time	Last modified time	IOC details
Win10x86_bichpt31	676181C52CA...	192.168.195.179	ajiant.log	C:\ProgramData\ajiant.log	9E18963E445C6DC1A...	04/09/2024 14:37:56	21/11/2024 09:49:06	17/12/2
11-Windowsptbich	853DCA6465B...	192.168.195.135	ajiant.db	C:\Program Files\Ajiant\ajiant.db	5BAFD36A0FF0DEC1...	12/12/2024 14:58:57	12/12/2024 14:58:57	17/12/2
Admin-PC	466167E9E8D0...	192.168.6.42	ajiant.db	C:\Program Files\Ajiant\ajiant.db	CCD1D6A3DF84F962...	15/11/2024 15:33:17	15/11/2024 15:33:17	17/12/2
EDR_Test03	2903CE7FDBF2...	192.168.255.1,192.16...	ajiant.db	C:\Program Files\Ajiant\ajiant.db	2005C2DFD5CF120D...	06/08/2024 02:38:53	16/12/2024 19:00:22	17/12/2

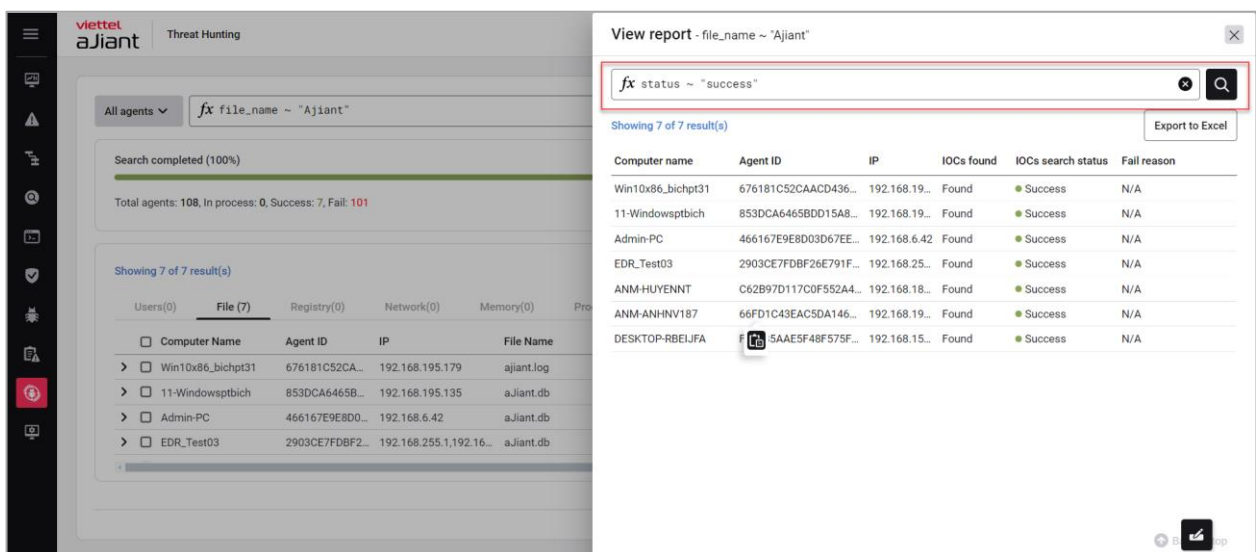
Dừng tìm kiếm

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



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

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



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

- Fail reason: Chi tiết lí do tìm kiếm thất bại

The screenshot displays the Viettel aJiant Threat Hunting dashboard. On the left, a sidebar contains navigation icons. The main panel shows a search query 'fx file_name ~ "Ajiang"' with a progress bar indicating 'Search completed (100%)'. Below this, a table lists search results for various agents. On the right, a 'View report' window is open, showing a detailed table of search results for the same query. The table includes columns for Computer name, Agent ID, IP, IOCs found, IOCs search status, and Fail reason. The 'Export to Excel' button is visible in the top right of the report window.

Computer name	Agent ID	IP	IOCs found	IOCs search status	Fail reason
Win10x86_bichpt31	676181C52CAACD436...	192.168.19...	Found	Success	N/A
11-Windowsptbich	853DCA6465BDD15A8...	192.168.19...	Found	Success	N/A
Admin-PC	466167E9E8D03D67EE...	192.168.6.42	Found	Success	N/A
EDR_Test03	2903CE7FDBF26E791F...	192.168.25...	Found	Success	N/A
ANM-HUYENNT	C62B97D117C0F552A4...	192.168.18...	Found	Success	N/A
ANM-ANHNV187	66FD1C43EAC5DA146...	192.168.19...	Found	Success	N/A
DESKTOP-RBELJFA	F92185AAEF48F575F...	192.168.15...	Found	Success	N/A
WinSrv2016	C877C486C743B797B9...	192.168.18...	N/A	Failed	The policy has been ..
Win10x64	88C5118E6AE9CAF4F5...	192.168.13...	N/A	Failed	The policy has been ..
Win10x64_edr03	91E1D567010025848D...	192.168.25...	N/A	Failed	The policy has been ..
DESKTOP-6KRVVQ2	1E6AF8040B8A1AF54C...	192.168.6.6...	N/A	Failed	The policy has been ..
vtt_huyenmy01	CD9F6C4984FA99F2ED...	192.168.19...	N/A	Failed	The policy has been ..
Win10x64	78AE3983BC1D6F98F...	192.168.25...	N/A	Failed	The policy has been ..

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

The screenshot shows the Viettel aJiant Threat Hunting interface. On the left, a sidebar contains navigation icons. The main panel displays search results for the query 'fx file_name ~ "Ajiang"'. A progress bar indicates 'Search completed (100%)' and 'Total agents: 108, In process: 0, Success: 7, Fail: 101'. Below this, a table shows 7 results. On the right, a 'View report' window is open, displaying a detailed table of search results with columns: Computer name, Agent ID, IP, IOCs found, IOCs search status, and Fail reason. An 'Export to Excel' button is highlighted in the top right corner of the report window.

Computer name	Agent ID	IP	IOCs found	IOCs search status	Fail reason
Win10x86_bichpt31	676181C52CA...	192.168.19...	Found	Success	N/A
11-Windowsptbich	853DCA6465B...	192.168.19...	Found	Success	N/A
Admin-PC	466167E9E8D...	192.168.6.42	Found	Success	N/A
EDR_Test03	2903CE7FDBF2...	192.168.25...	Found	Success	N/A
ANM-HUYENNT	C62B97D117C...	192.168.18...	Found	Success	N/A
ANM-ANHNV187	66FD1C43EAC...	192.168.19...	Found	Success	N/A
DESKTOP-RBELJFA	F92185AAE5F4...	192.168.15...	Found	Success	N/A

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

This screenshot shows the same Viettel aJiant Threat Hunting interface, but with a more detailed view of the search results. The 'View report' window is open, showing a table with columns: Computer Name, Agent ID, IP, File Name, File path, File hash SHA256, File created time, Last modified time, and IOC detected time. An 'Export to Excel' button is highlighted in the top right corner of the report window.

Computer Name	Agent ID	IP	File Name	File path	File hash SHA256	File created time	Last modified time	IOC detected time
Win10x86_bichpt31	676181C52CA...	192.168.195.179	ajiang.log	C:\ProgramData\ajiang.log	9E18963E445C6DC1A...	04/09/2024 14:37:56	21/11/2024 09:49:06	17/12/2024 10:42:57
11-Windowsptbich	853DCA6465B...	192.168.195.135	ajiang.db	C:\Program Files\Ajiang\ajiang.db	5BAFD36A0FF0DEC1...	12/12/2024 14:58:57	12/12/2024 14:58:57	17/12/2024 10:42:54
Admin-PC	466167E9E8D...	192.168.6.42	ajiang.db	C:\Program Files\Ajiang\ajiang.db	CCD1D6A3DF84F962...	15/11/2024 15:33:17	15/11/2024 15:33:17	17/12/2024 10:44:01
EDR_Test03	2903CE7FDBF2...	192.168.255.1,192.16...	ajiang.db	C:\Program Files\Ajiang\ajiang.db	2005C2DFD5CF120D...	06/08/2024 02:38:53	16/12/2024 19:00:22	17/12/2024 10:45:20
ANM-HUYENNT	C62B97D117C...	192.168.187.128	ajiang.db	C:\Program Files\Ajiang\ajiang.db	FCD24FF69664D1E6F...	17/09/2024 15:58:52	19/11/2024 15:31:07	17/12/2024 10:44:22
ANM-ANHNV187	66FD1C43EAC...	192.168.190.1,192.16...	ajiang.db	C:\Program Files\Ajiang\ajiang.db	CCD1D6A3DF84F962...	06/12/2024 15:26:22	06/12/2024 15:26:22	17/12/2024 10:45:22

3.8.4 Xem lịch sử truy vấn (View History)

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

Search

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	

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

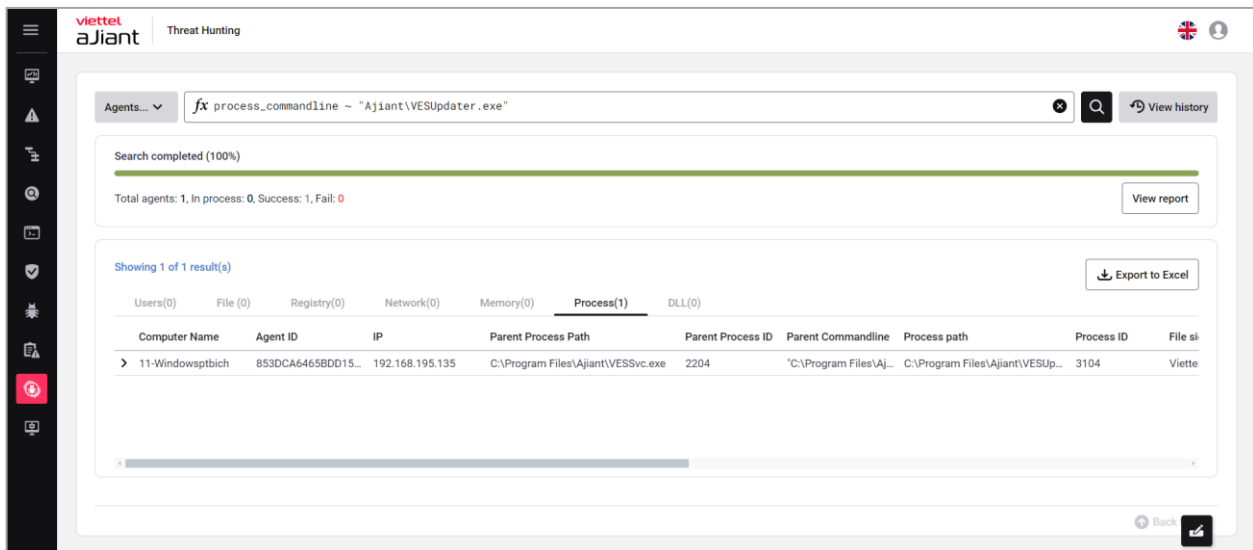
View history

Search

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:

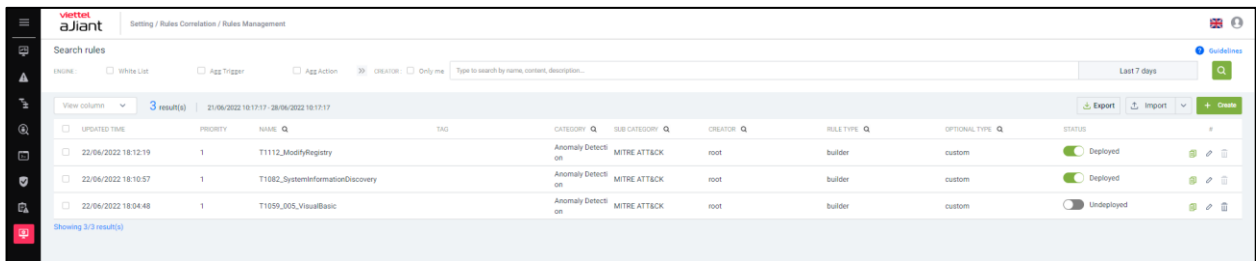


3.9 Rules Correlation

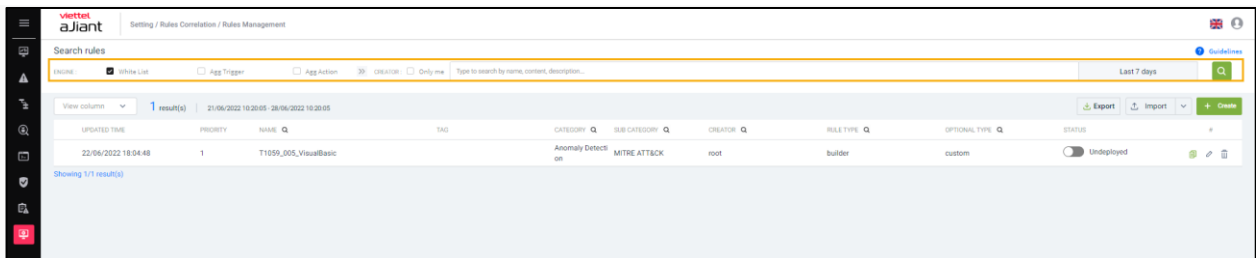
3.9.1 Danh sách hiển thị

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

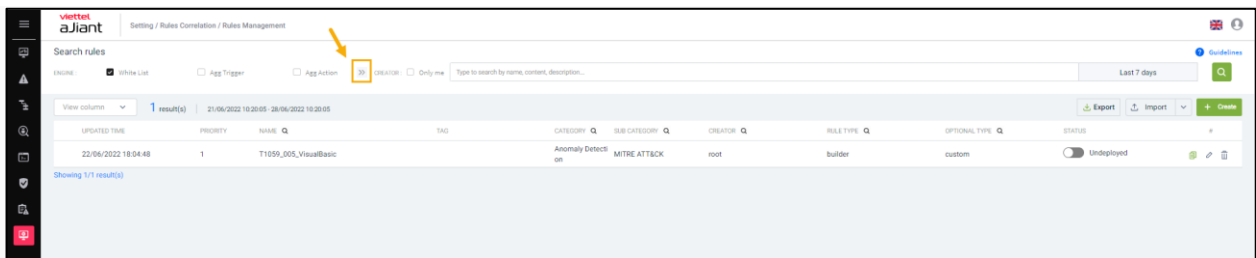
- + Bộ lọc FITTER;
- + Bộ lọc FITTER bao gồm:
 - 6 Engine: Whitelist, Agg Trigger, Agg Action, Filter, Indicator, False-Positive;
 - Text box search theo các trường: Name, content, description;
 - Thời gian cập nhật;
 - Tạo bởi tôi;
 - Lọc theo **Engine**;



Bước 1: Chọn 1 hoặc nhiều Engine mặc định;

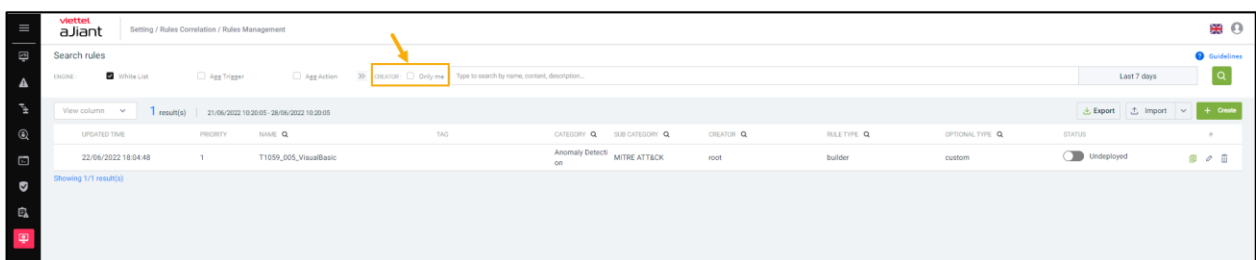


Bước 2: Chọn Mở rộng để thêm các Engine cần lọc;

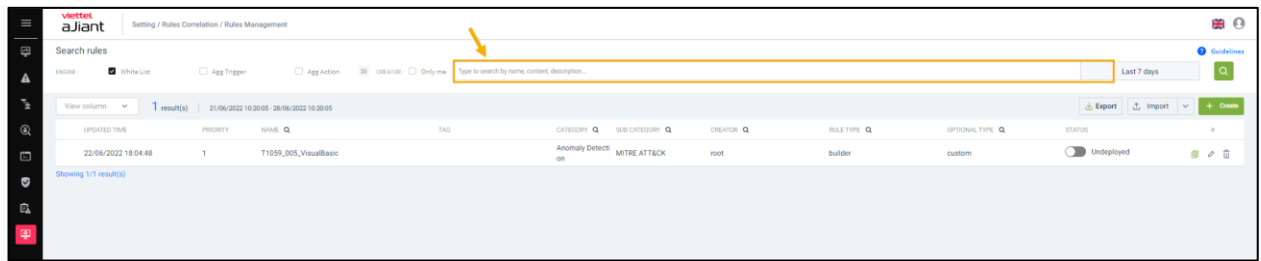


Khi chọn 2 hoặc nhiều Engine, màn hình trả về kết quả được lọc theo phép toán AND;

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



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



Bước 5: Nhập thông tin cần tìm kiếm;

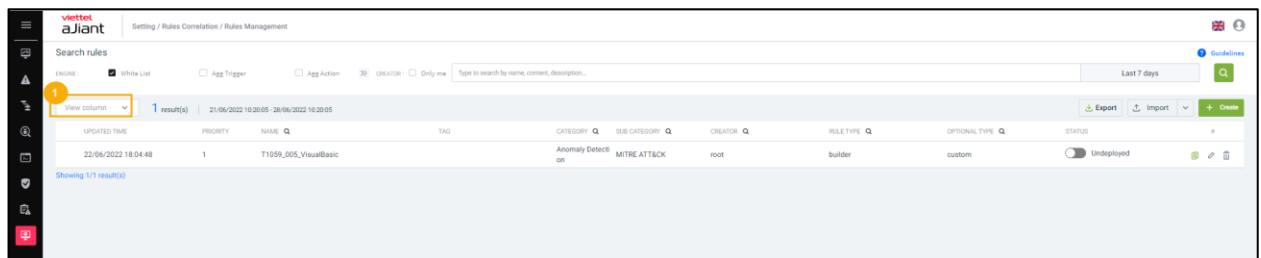
Bước 6: Nhấn Search để hiển thị kết quả tìm kiếm.

Chọn cột

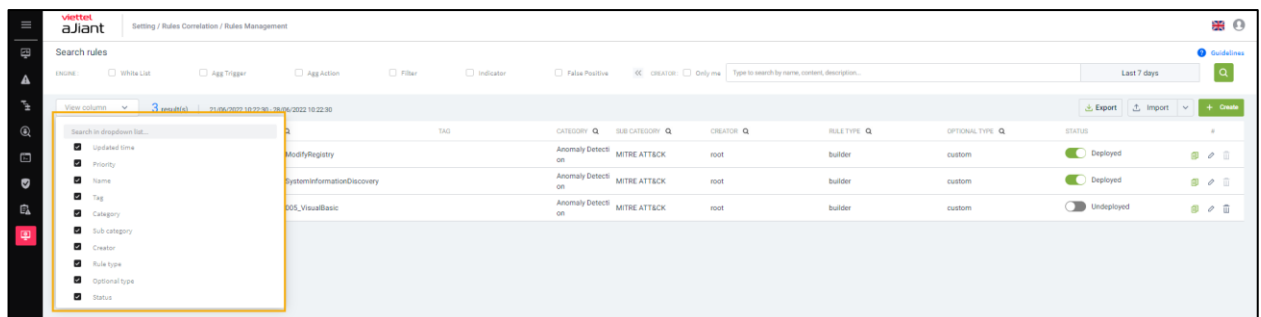
Cho phép người dùng lựa chọn các cột hiển thị trên màn hình correlation.

Các bước thực hiện:

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



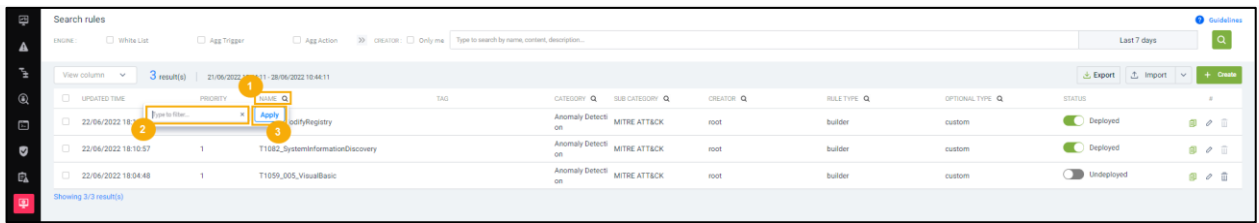
Bước 2: Chọn vào những tên cột muốn hiển thị;



1 – Hỗ trợ tìm kiếm nhanh

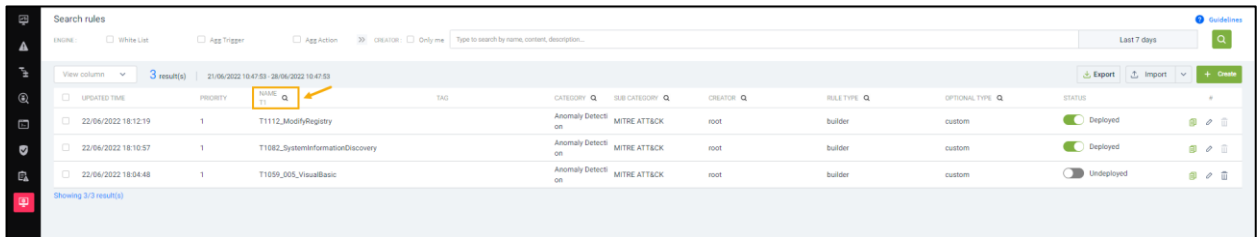
- Tìm kiếm theo tên rule

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



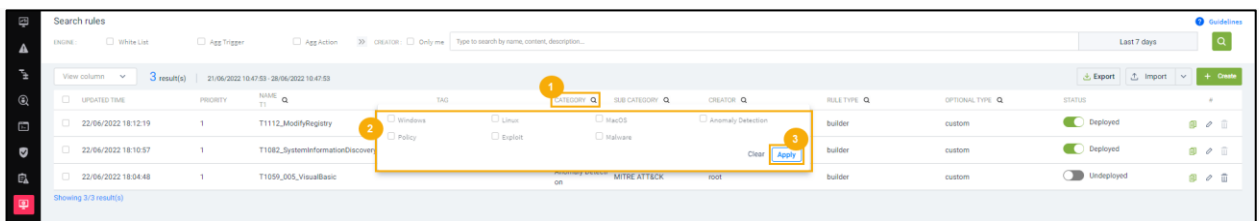
Bước 2: Nhập tên rules muốn tìm kiếm;

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



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

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



Bước 5: Chọn category muốn 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”;

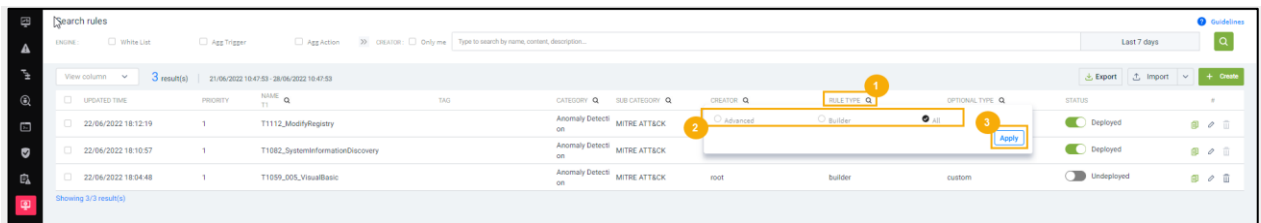
Tìm kiếm Creator

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.

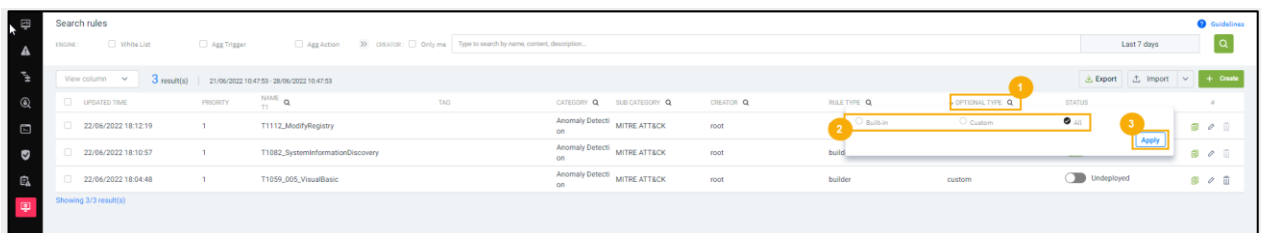


Bước 1: Click icon  để hiển thị danh sách Rule type;

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.

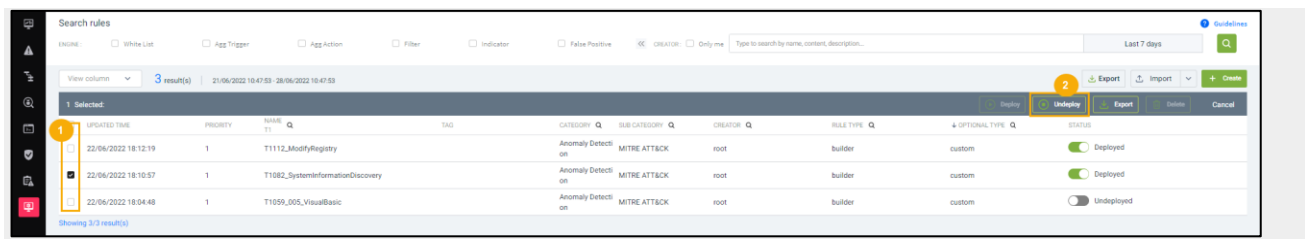


Bước 1: Click icon  để hiển thị danh sách Optional type;

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

Bước 3: Click “Apply”;

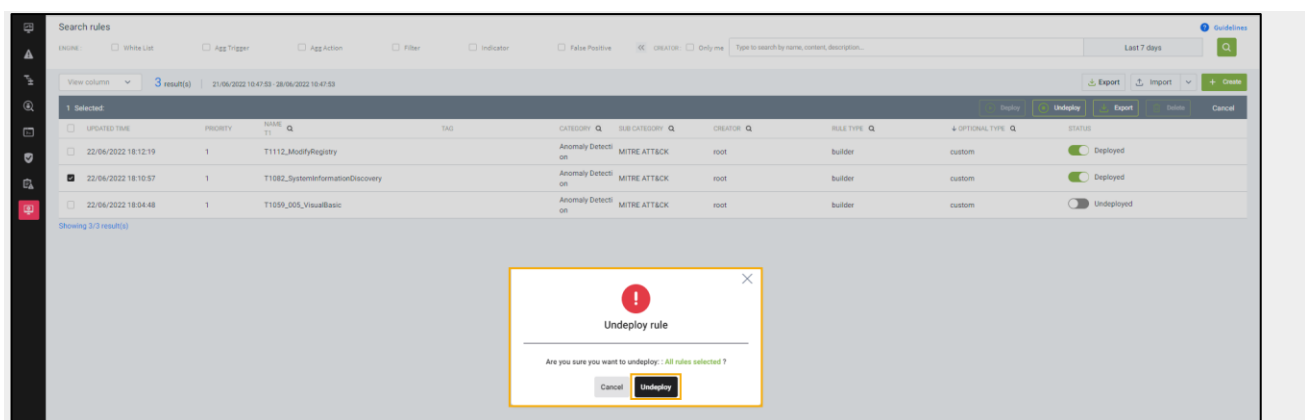
Hỗ trợ Deploy/Undeploy cho nhiều Rules



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;



3.9.2 Thêm mới Rules Correlation

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

Tổng quan

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

- Whitelist là một Stateless Engine thực hiện loại bỏ nhanh các event mà hệ thống không cần xử lý. Các event khớp với rule whitelist sẽ bị drop khỏi luồng xử lý;
- Agg_trigger và Agg_action là một Stateful Engine thực hiện gom nhóm các event tương tự nhau. Mỗi rule aggregate chứa các thông tin về điều kiện gom nhóm (định nghĩa event tương tự nhau), khoảng thời gian gom nhóm (ví dụ 30s, 1

phút, 2 phút, ...). Các event khớp điều kiện gom nhóm được lưu lại và chỉ trả về một event có kèm theo số lượng sau một khoảng thời gian. Các event không khớp điều kiện gom nhóm được trả ra ngay lập tức với số lượng là 1;

- Filter là một Stateless Engine thực hiện lọc các điều kiện để đẩy vào indicator;

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

- FalsePositive engine là một Stateless Engine thực hiện loại bỏ các trường hợp Alert bị Alert sai. Mỗi Alert khi khớp với rule Falsepositive sẽ bị drop;

- + Debug/ Not Debug là hai trạng thái của engine. Khi thực hiện thao tác debug, log được đẩy về 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

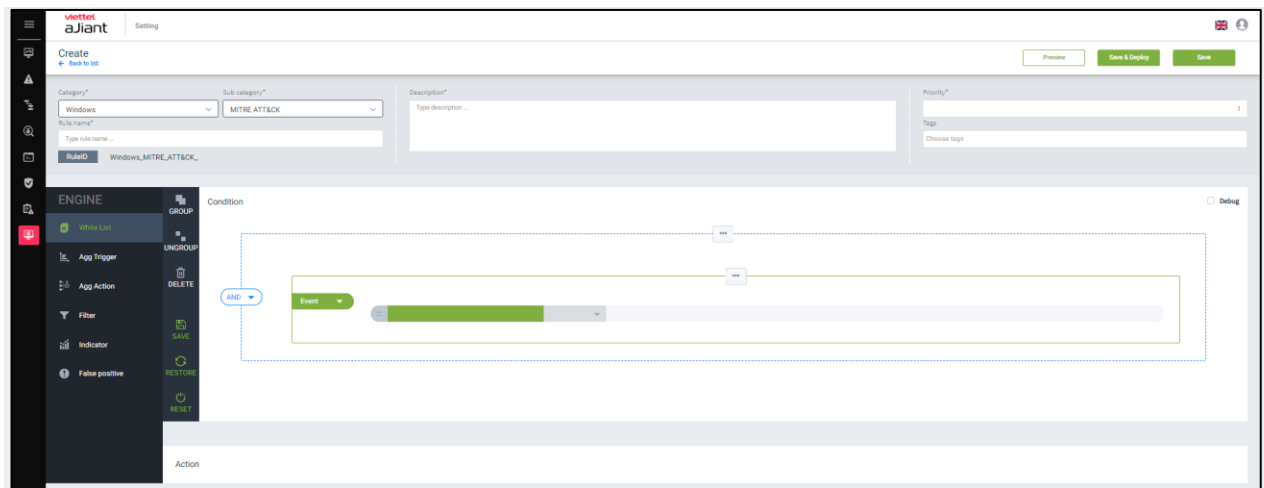
+ **Restore:** Tự động reset lại đến ngay sau khi nhấn “Save” gần nhất;

+ **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;

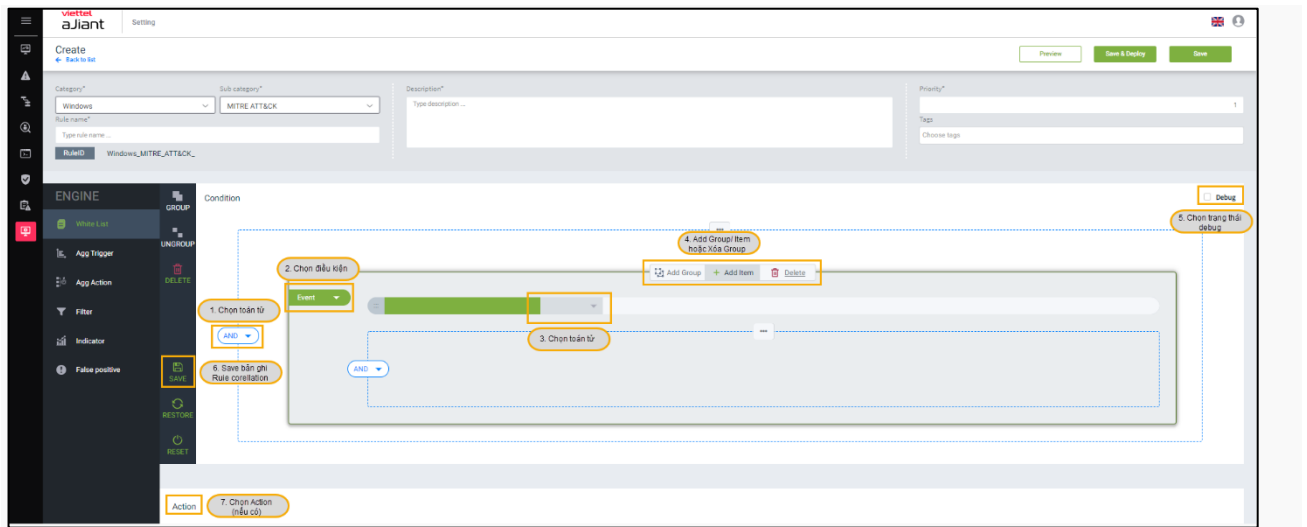


Bước 2: Nhập thông tin của rule;



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.

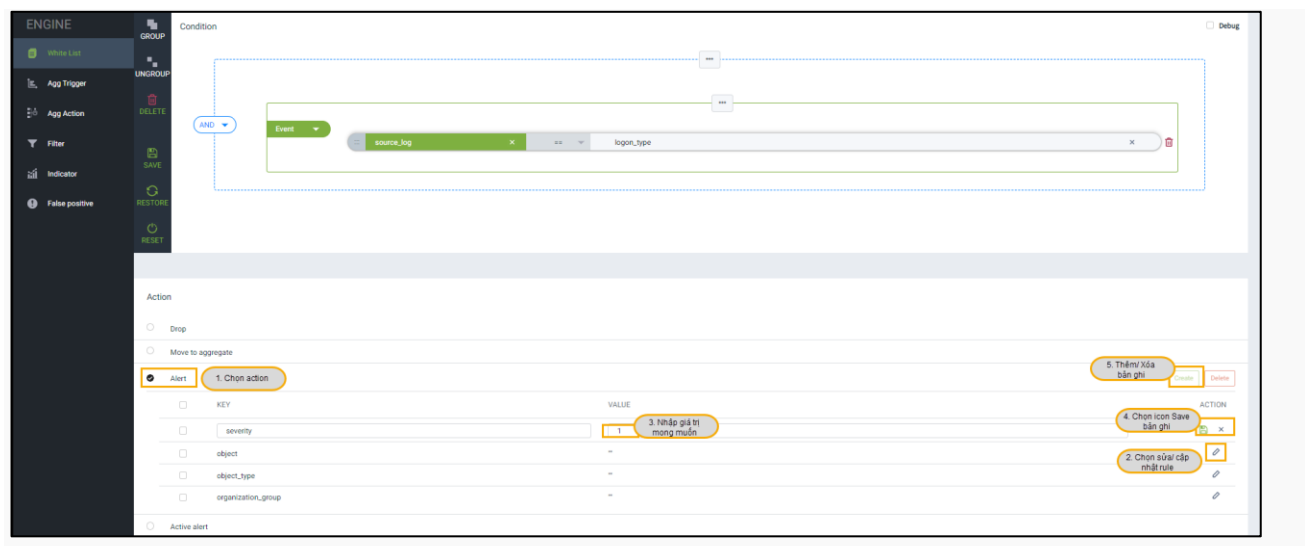
Whitelist: Gồm 4 hành động dưới dạng check box : Drop, Chuyển sang aggregate, Alert và Danh sách Active, người dùng bắt buộc phải chọn 1 trong 4 hành động này. Khi các log đầy vào thỏa mãn điều kiện sẽ thực hiện 1 trong 4 hành động mà người dùng đã tích chọn. Chi tiết chức năng của 4 hành động:

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

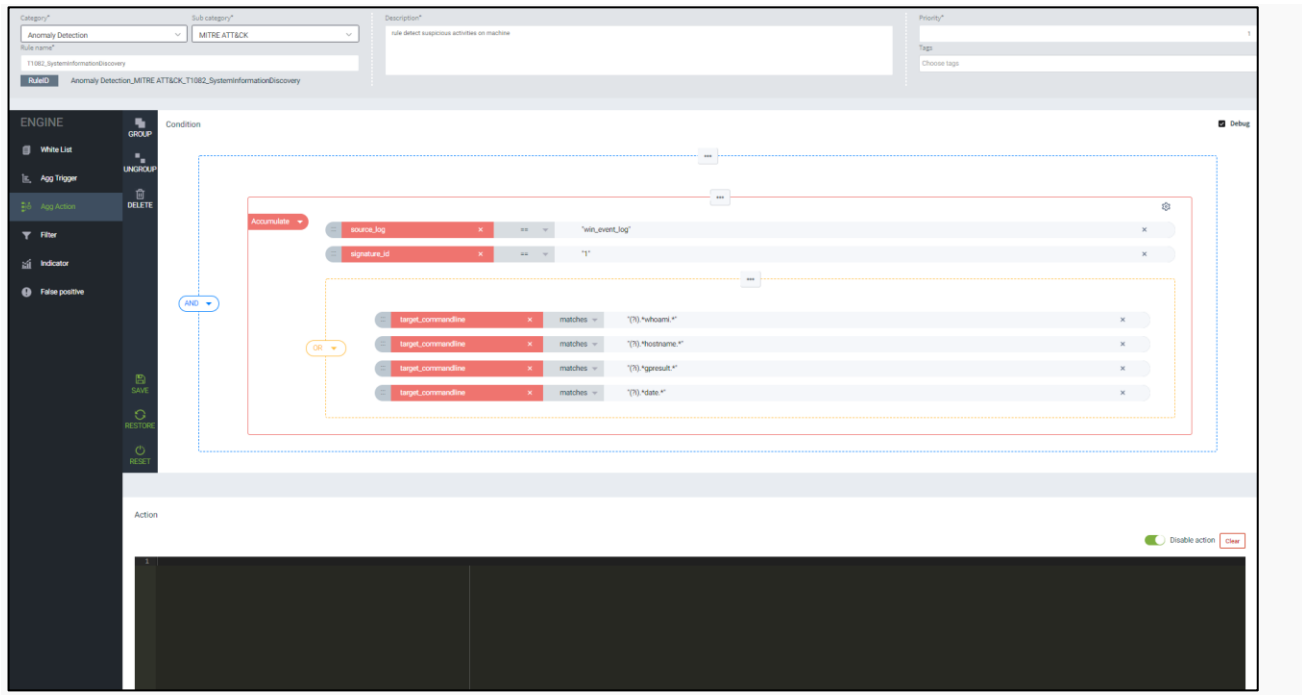
Lưu ý: Có thể tạo nhiều hành động với các trường khác nhau tùy theo mục đích người sử dụng.

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”.

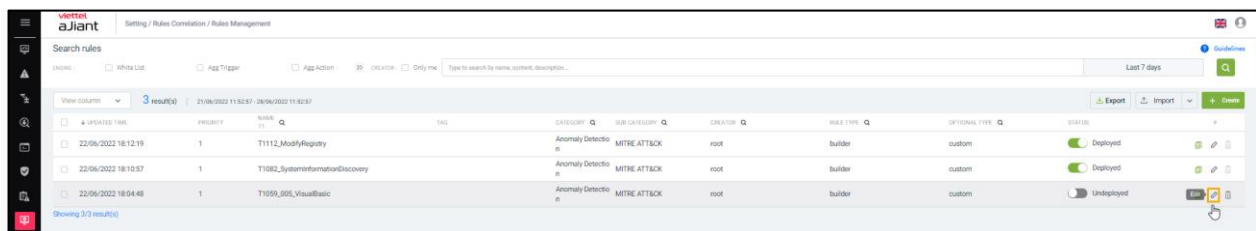
Lưu ý: Khi có lỗi, người dùng có thể nhấn nút “Preview” để xem lỗi.

3.9.3 Sửa Rules Correlation

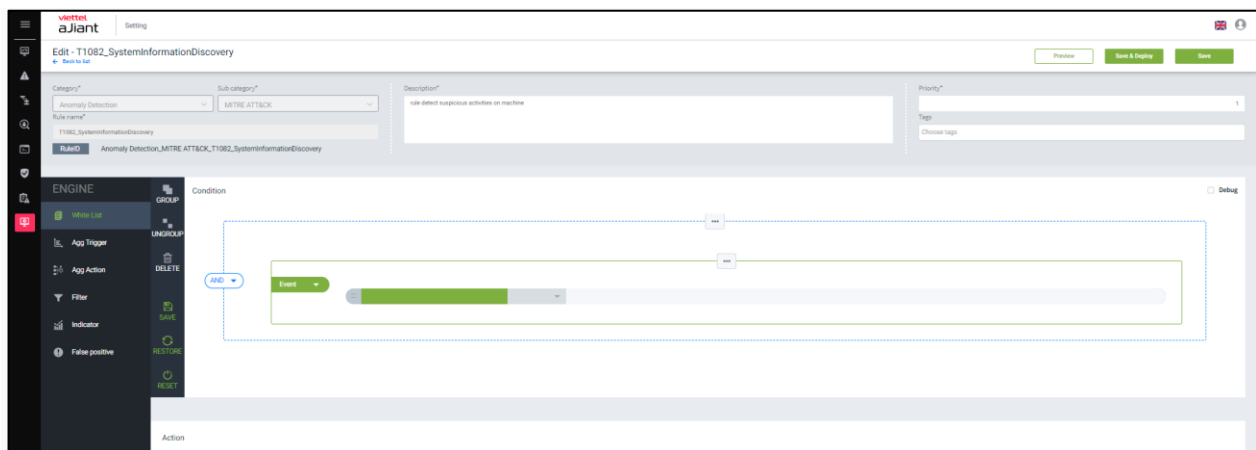
Cho phép người dùng chỉnh sửa các rule đã tạo.

Các bước thực hiện:

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



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



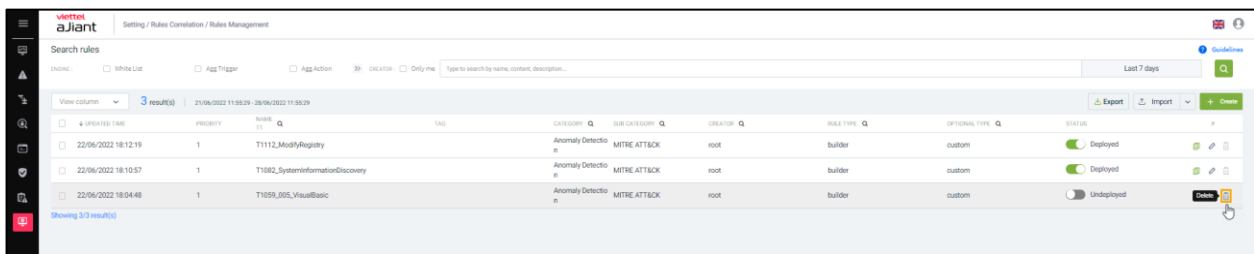
Lưu ý: Các trường tên rule, category, subcategory là những trường không chỉnh sửa được.

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

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

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

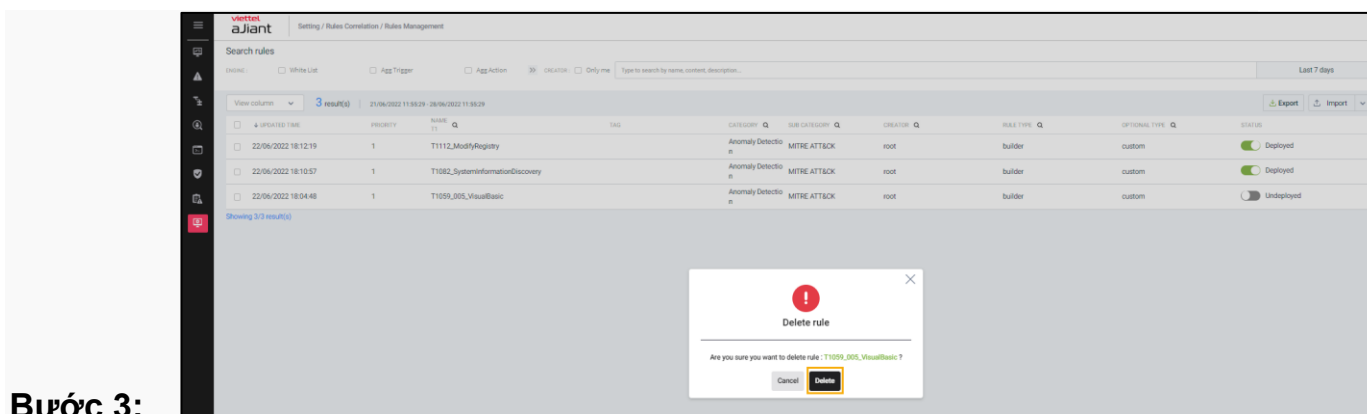
3.9.4 Xóa Rules Correlation



Các bước thực hiện xóa 01 rule:

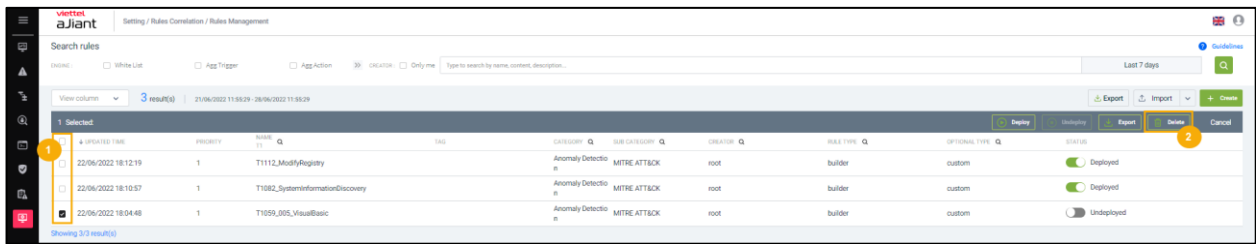
Bước 1: Click icon “Xoá” tại rule muốn xoá;

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



Bước 3:

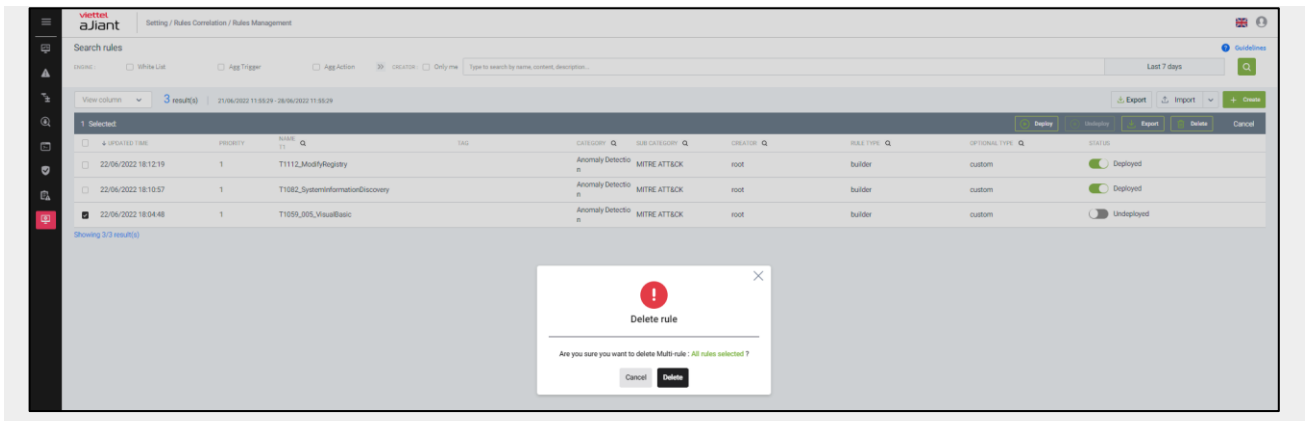
+ Nếu chọn “Delete”, rule được chọn xoá sẽ biến mất khỏi màn hình hiển thị;



Các bước thực hiện xóa nhiều rule:

Bước 1: Click chọn những rule muốn 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.

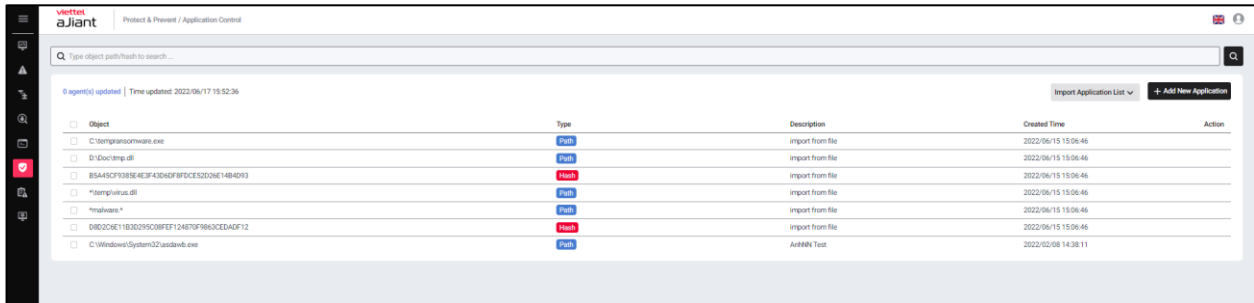
3.10 Protect & Prevention

3.10.1 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.

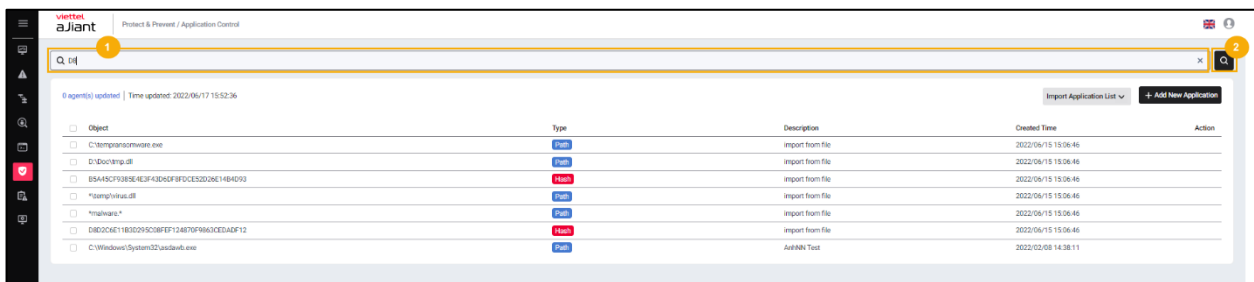
Hiển thị danh sách các ứng dụng/tiến trình bị chặn

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.



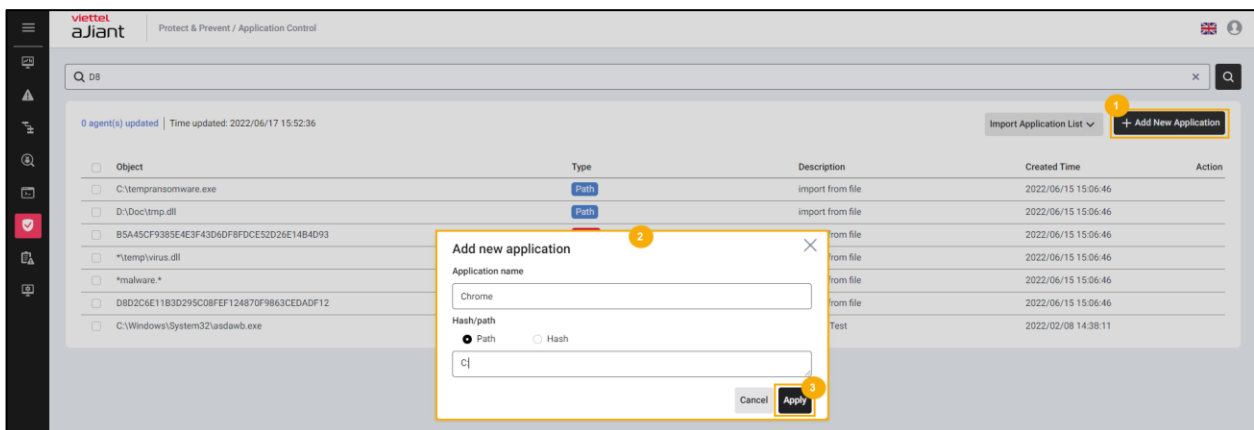
Tìm kiếm ứng dụng/tiến trình bị chặn

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



Thêm mới ứng dụng/tiến trình bị chặn

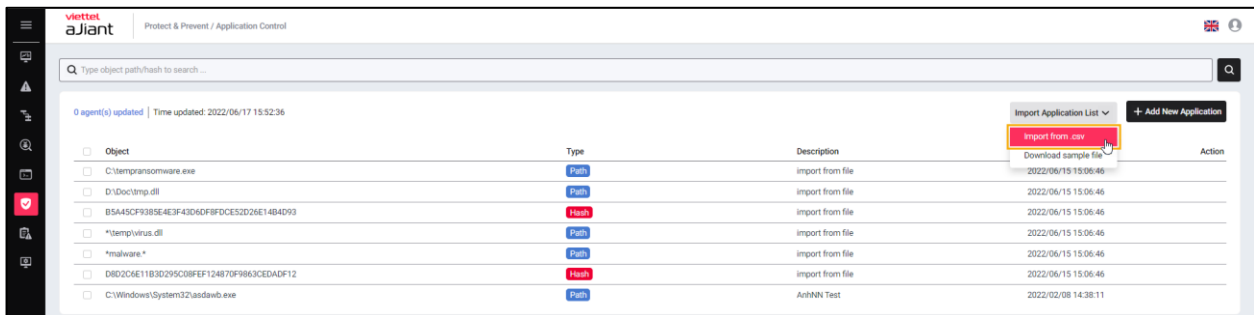
Click vào “Add new” để thêm mới ứng dụng/tiến trình bị chặn, người dùng có thể chọn chặn theo Path hoặc mã Hash (MD5, SHA1, SHA256)



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;

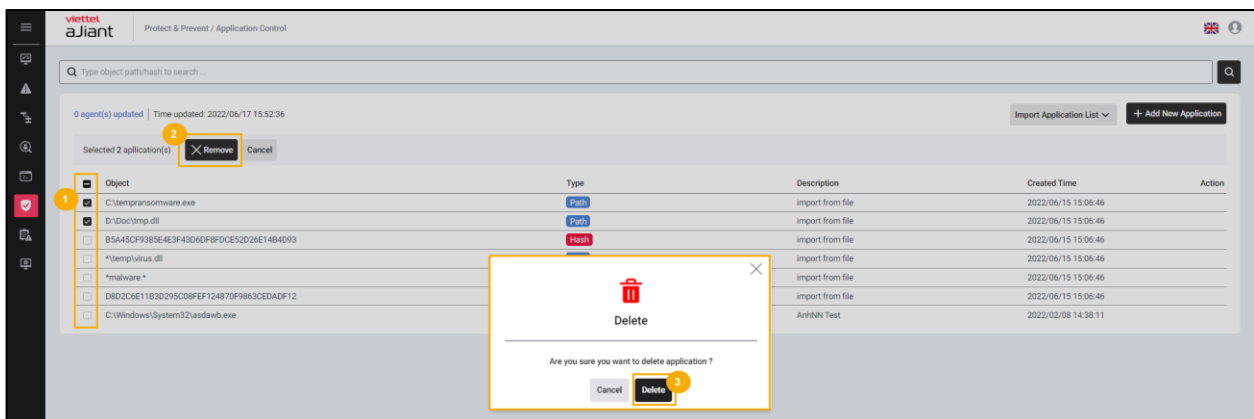
Click “Import”, chọn đường dẫn đến file cần tải lên và click “Open”, hệ thống sẽ tự động thêm danh sách các ứng dụng cần chặn lên hệ thống.



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”



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.

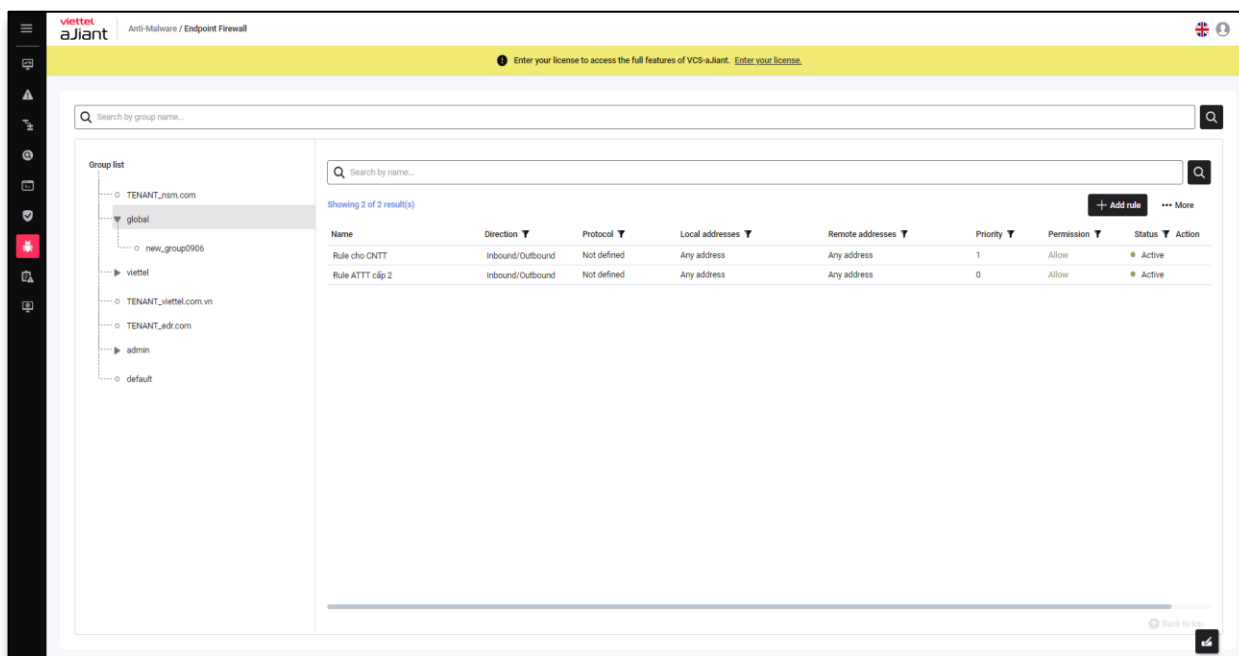


3.10.2 Endpoint Firewall

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.

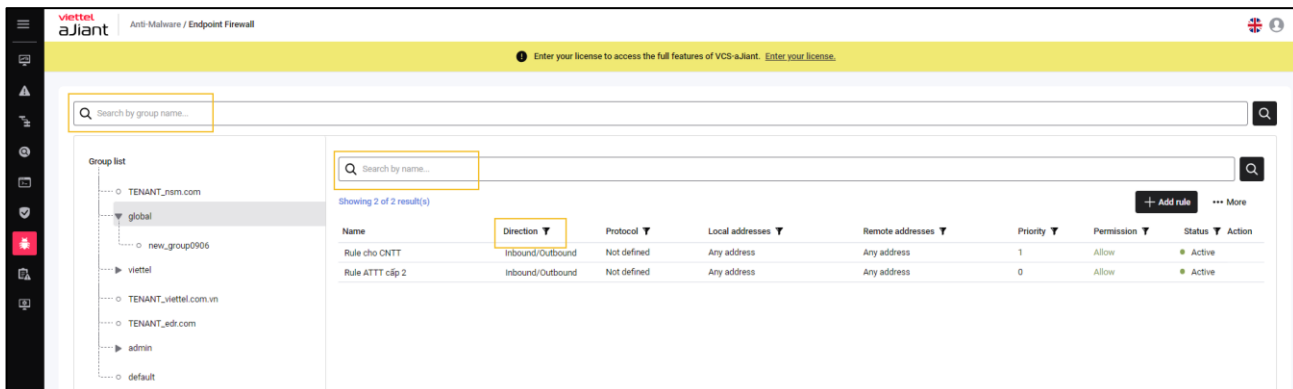
Hiển thị danh sách các kết nối bị chặn

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



Tìm kiếm các kết nối bị chặn

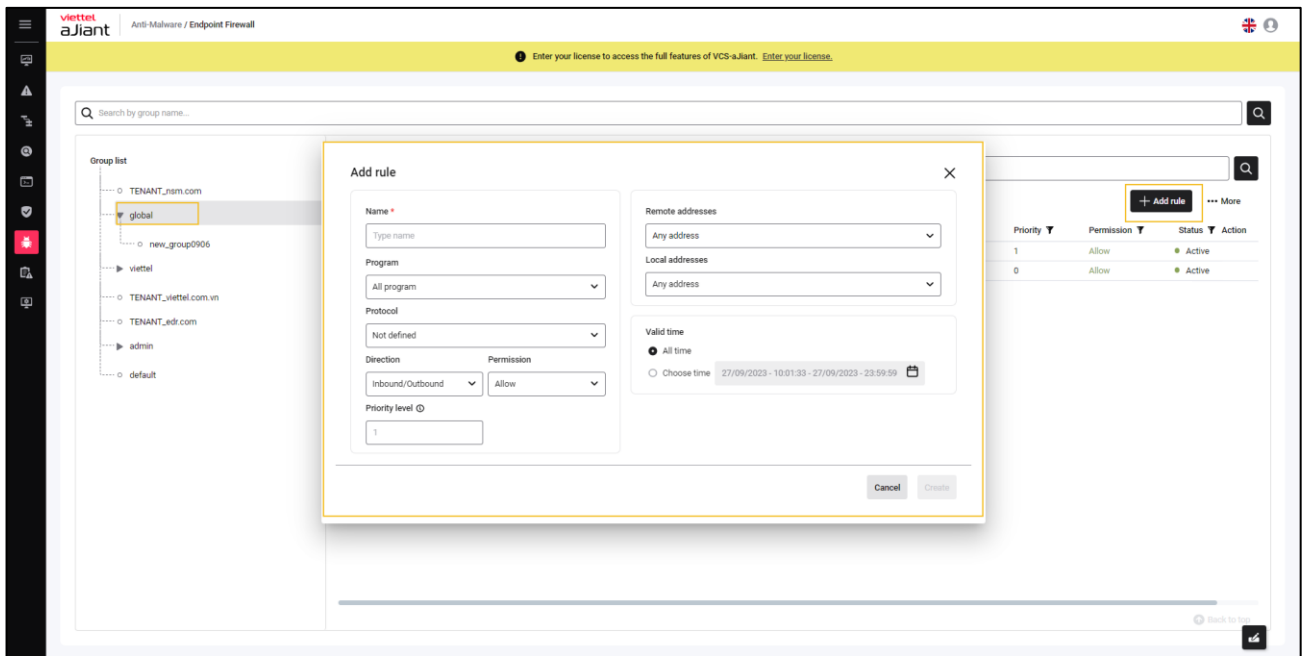
Người dùng có thể tìm kiếm theo nhóm người dùng, theo tên quy tắc firewall hoặc filter theo giá trị của từng điều kiện (Tên, kiểu connect inbound/outbound, ip...) trên màn danh sách firewall:



Thêm mới các kết nối bị chặn

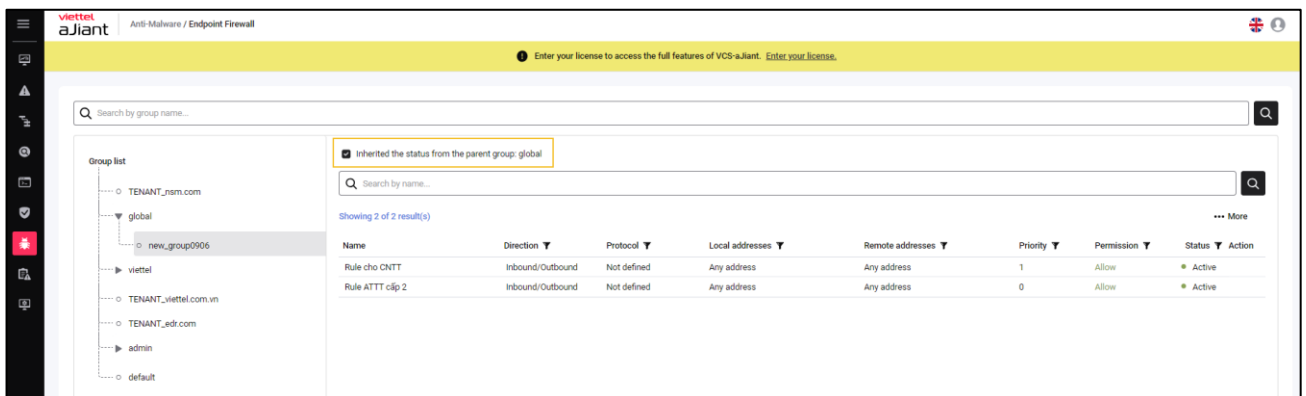
Chọn nhóm người, sau đó Click nút “Add new”, nhập thông tin trên popup thêm mới kết nối bị chặn

- + 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



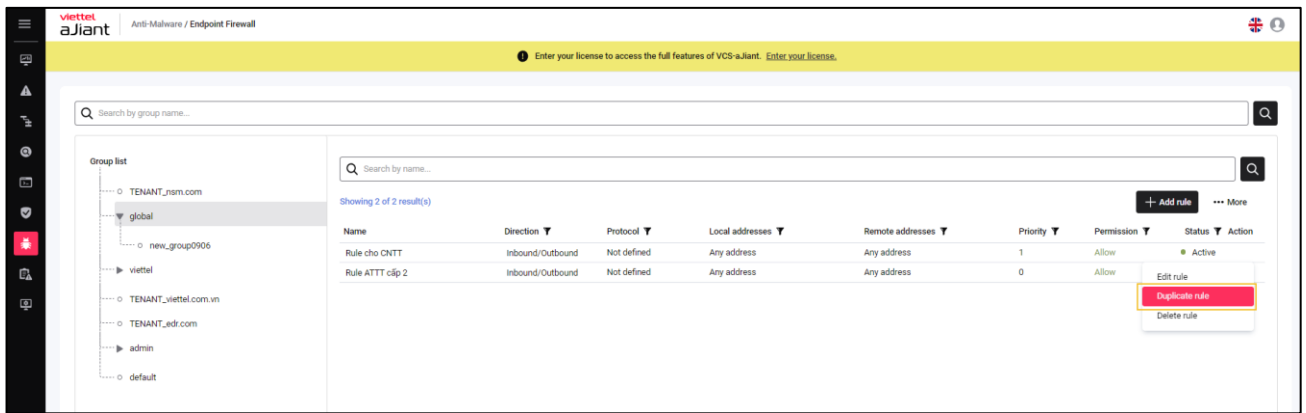
Lưu ý: quy tắc kế thừa từ nhóm cha

- + 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



Tạo bản sao chép từ điều kiện đã có

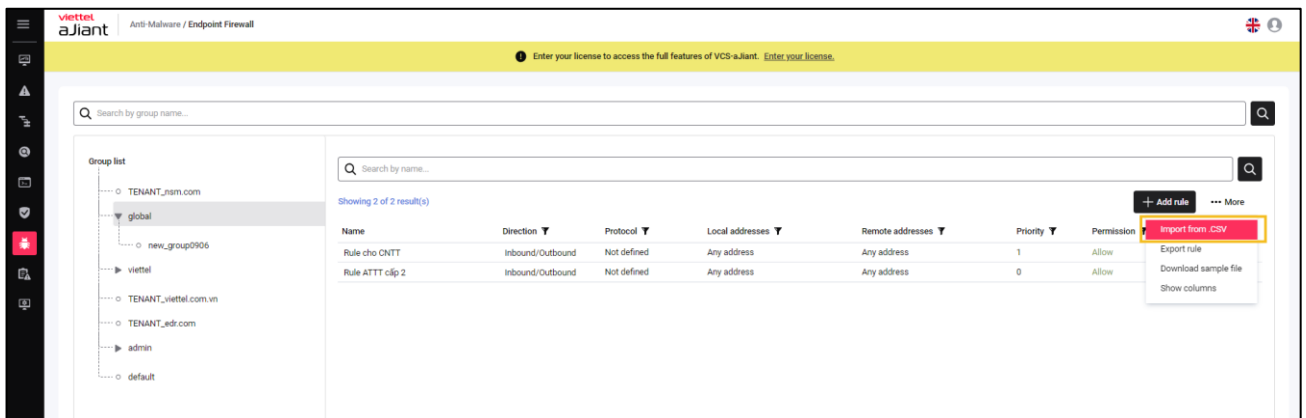
Chọn điều kiện muốn tạo bản sao chép, thực hiện Action, chọn *Duplicate rule*



Thêm mới kết nối bị chặn từ tập tin có sẵn

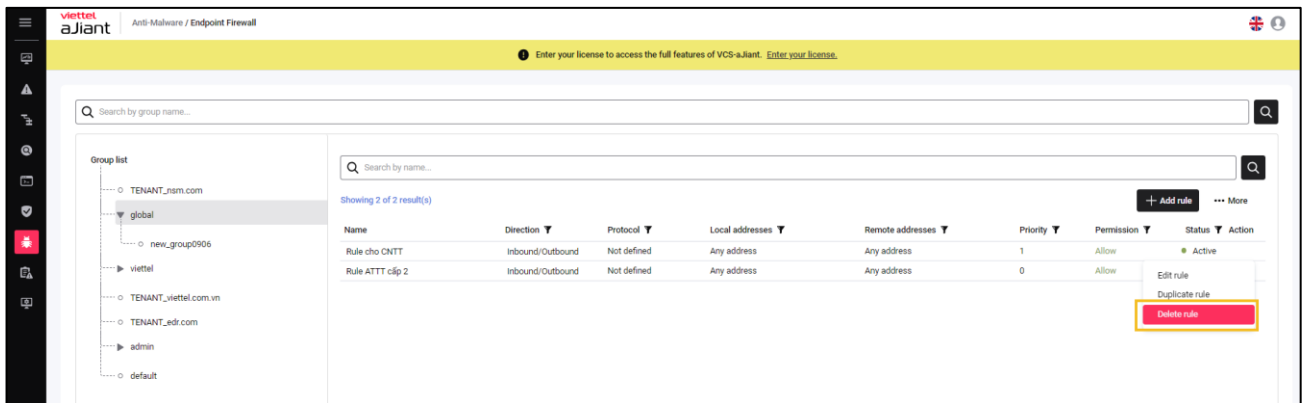
Người dùng có thể thêm mới các ứng dụng/tiến trình bị chặn từ tập tin .csv theo mẫu có sẵn lên danh sách ứng dụng hiện tại;

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;



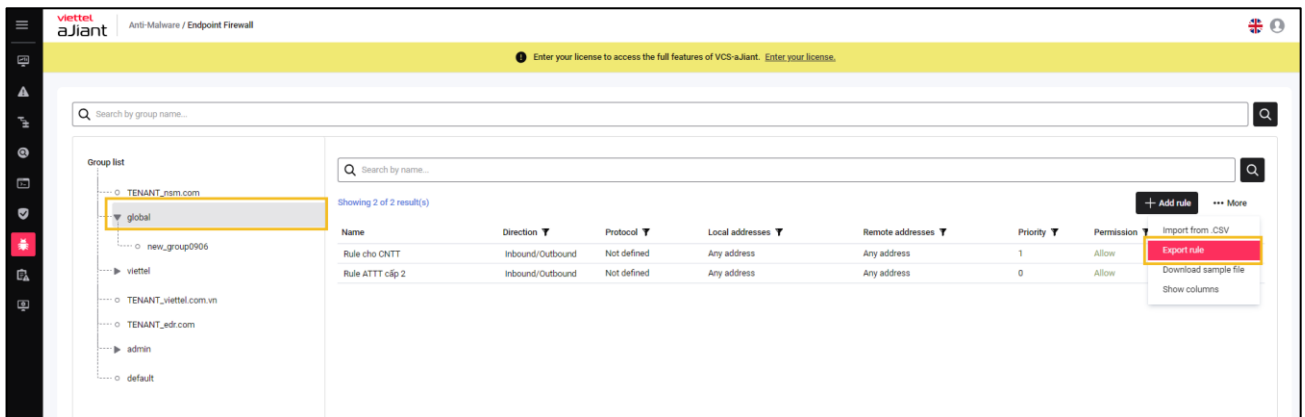
Xóa kết nối bị chặn trong danh sách

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



Xuất dữ liệu các điều kiện

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



3.11 Anti – Malware

3.11.1 Scan Schedule

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

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	
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 top

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.

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**

Anti-Malware / Scan Scheduler

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	
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 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 top

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

Anti-Malware / Scan Scheduler

Showing 11 of 11 result(s)

Show only my schedule

New task

Create new task

Task name: new task 1

Scan type: Quick scan

Priority: Low

Trigger: ☒ When this task is created ☐ Run on a schedule

Assignee(s): ☒ All agents (total 38 agents) ☐ Choose group(s) and agent(s)

0 assignee(s)

Information of selected agent(s) will be showing here.

Cancel Create

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

Task name: Người dùng nhập vào tên lập lịch quét;

Scan type: Người dùng lựa chọn một trong 3 loại scan. Cho phép:

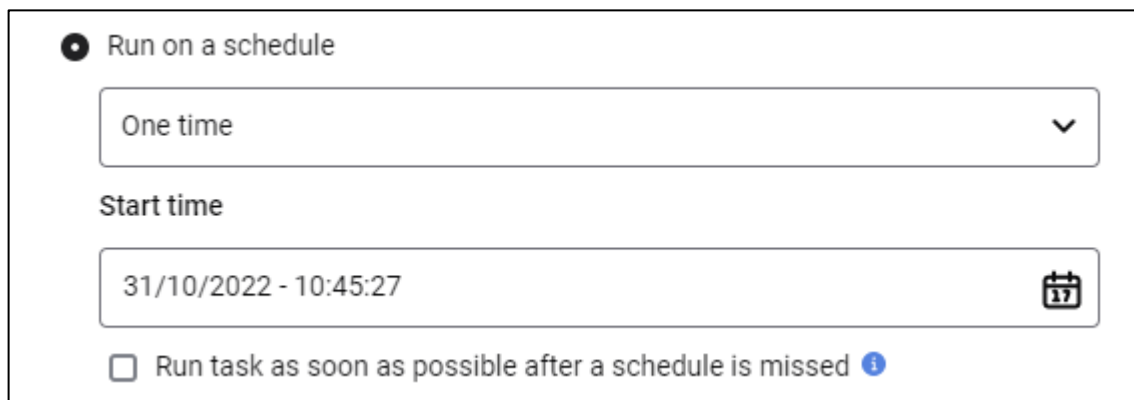
- + Quét nhanh: Kiểm tra nhanh các tệp và thư mục đáng ngờ tiềm ẩn;
- + Quét toàn bộ: Kiểm tra toàn bộ các tệp và thư mục trong máy tính. Quá trình này có thể mất vài giờ để hoàn thành;
- + Quét tùy chỉnh: Cho phép người dùng một tệp / thư mục cụ thể trong máy tính của bạn để quét.

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

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

Run immediately: Cho phép người dùng lập lịch quét ngay lập tức dưới các máy trạm khi task vừa được tạo thành công;

Run on Schedule: Cho phép người dùng lập lịch quét theo cấu hình của người dùng:



☒ Run on a schedule

One time

Start time

31/10/2022 - 10:45:27

☐ Run task as soon as possible after a schedule is missed

+ Schedule:

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

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

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

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

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

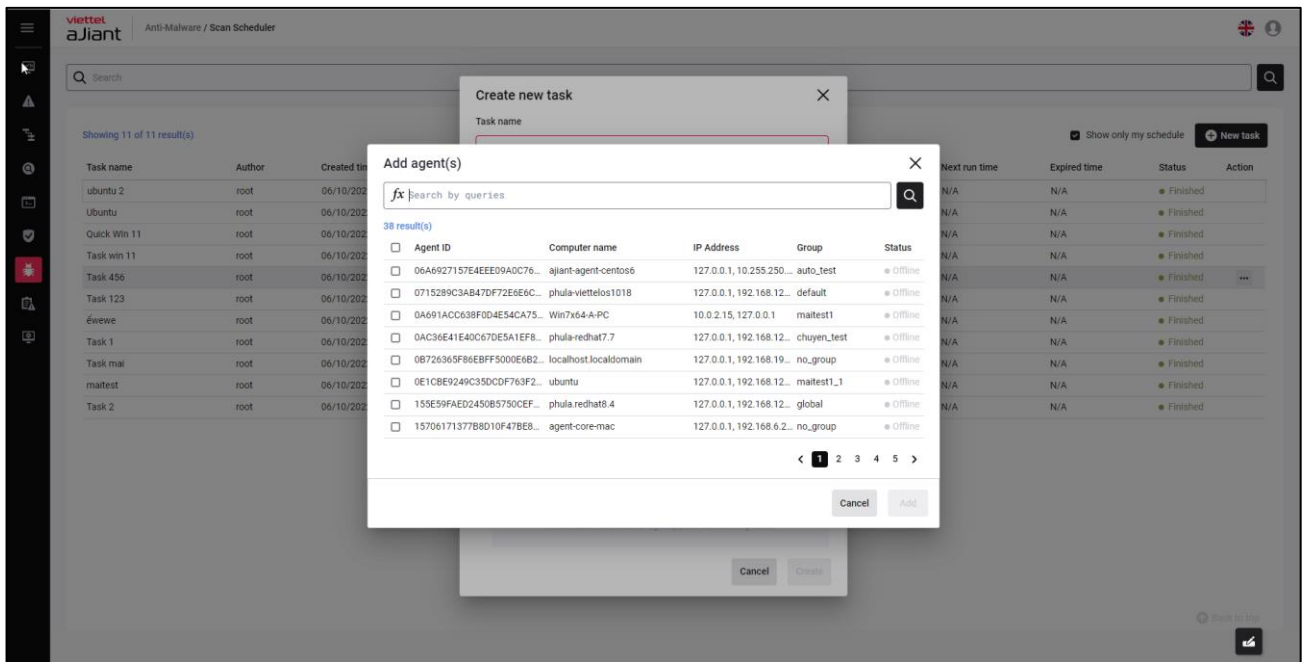
All Agent(s): Lập lịch với tất cả các máy trạm thuộc quyền quản lý của người dùng đang đăng nhập;

Choose Agent(s) or Group(s):

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

+ Các bước thực hiện: Add Agents or Group

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



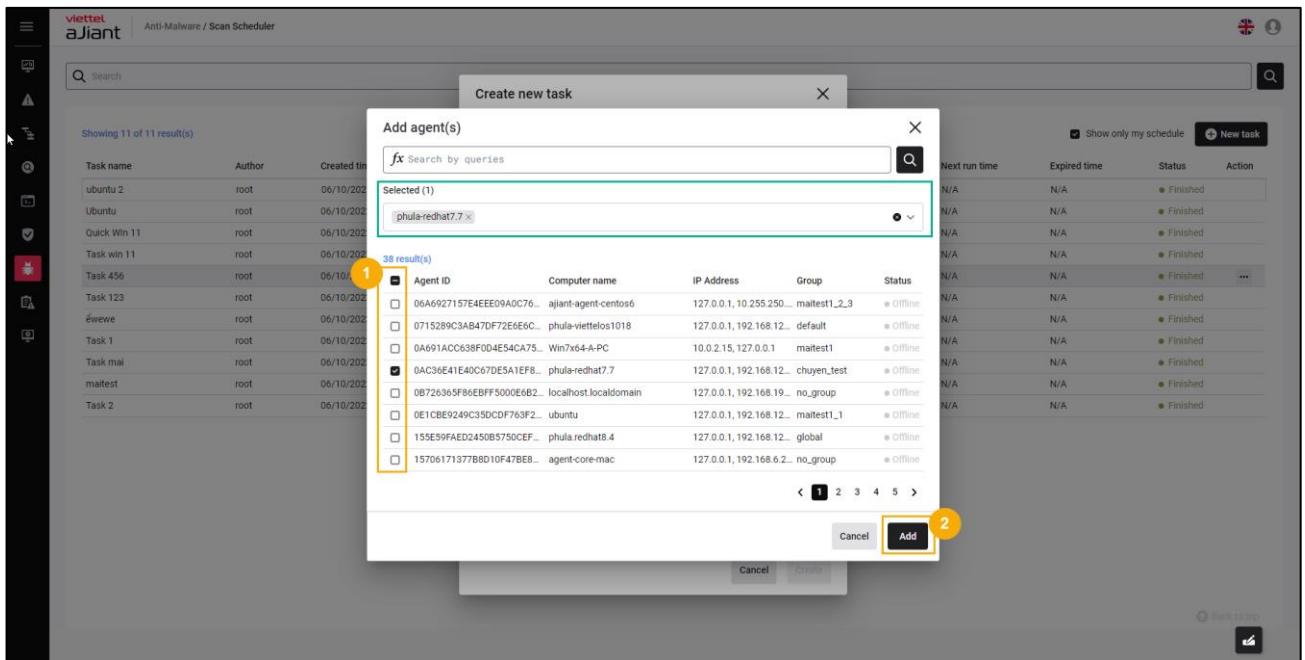
○ Tìm kiếm máy trạm:

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

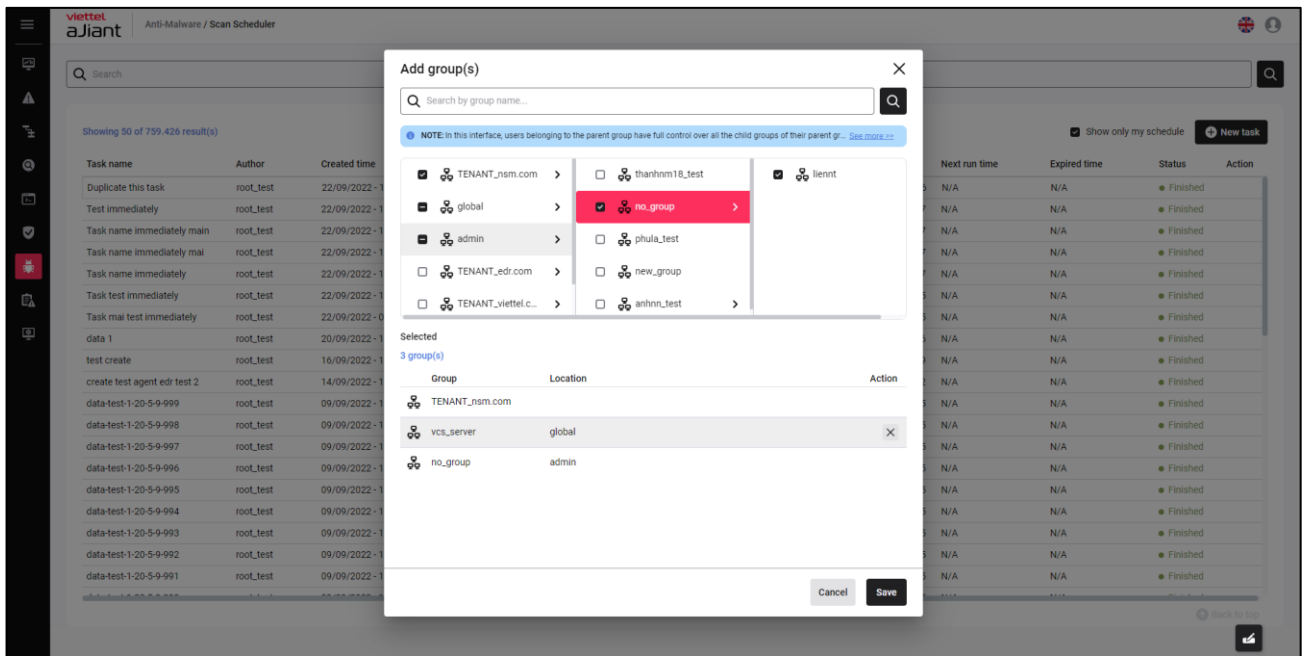
➔ Danh sách các máy trạm được lựa chọn sẽ được tự động thêm vào khung thông tin máy trạm đã được chọn.

- 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**

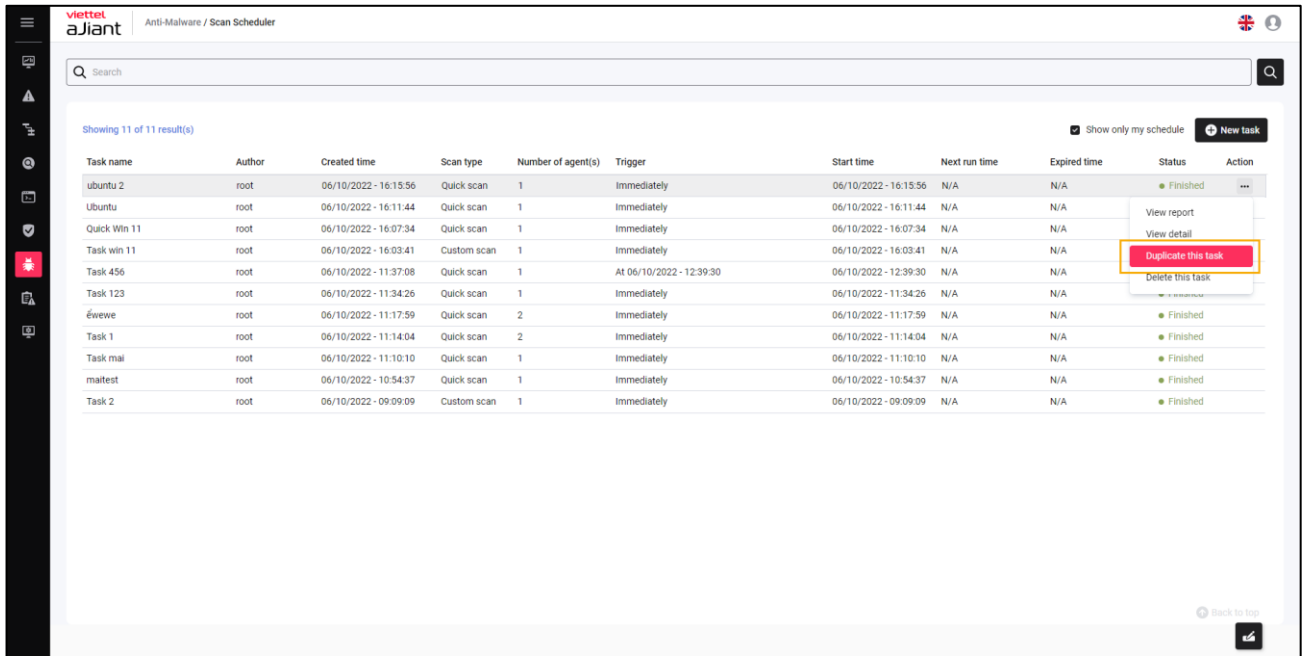
Bước 3: Người dùng chọn nút **Create** để hoàn thiện thao tác thêm mới lập lịch quét. Hoặc, chọn nút **Cancel** để hủy thao tác thêm mới lập lịch quét

Nhân bản Schedule task

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

Các bước thực hiện:

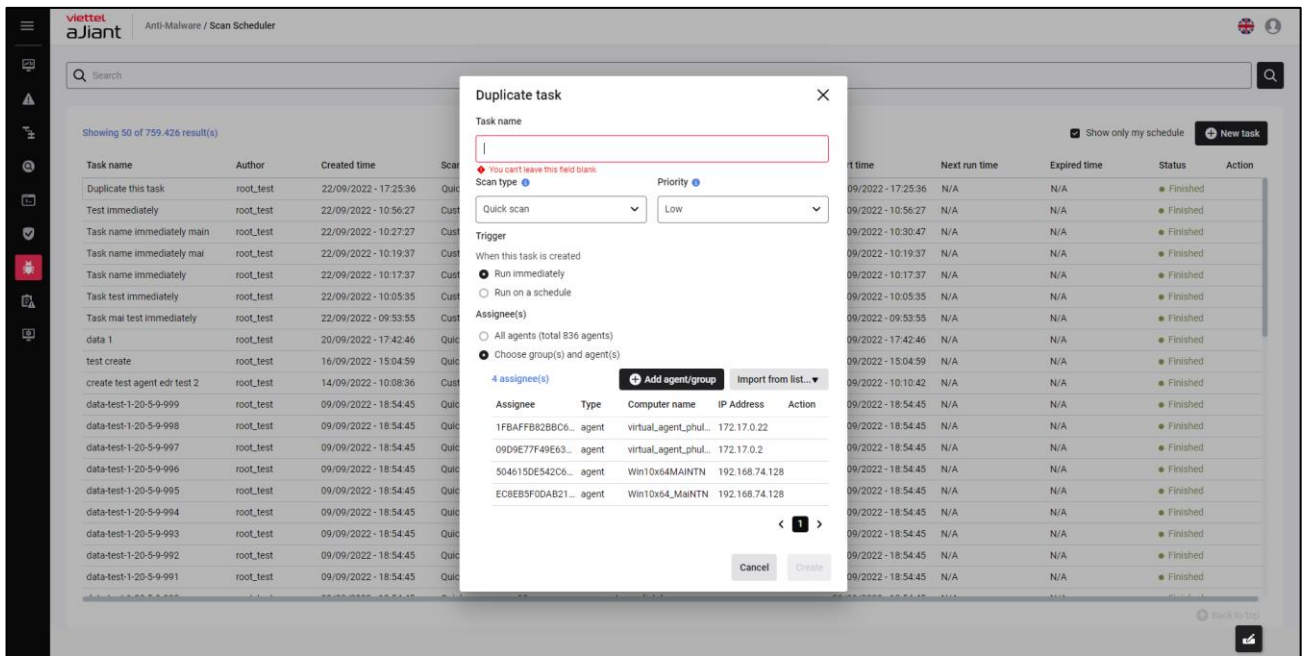
Bước 1: Tại màn hình danh sách task, người dùng chọn **Duplicate** bản ghi task cần nhân bản:



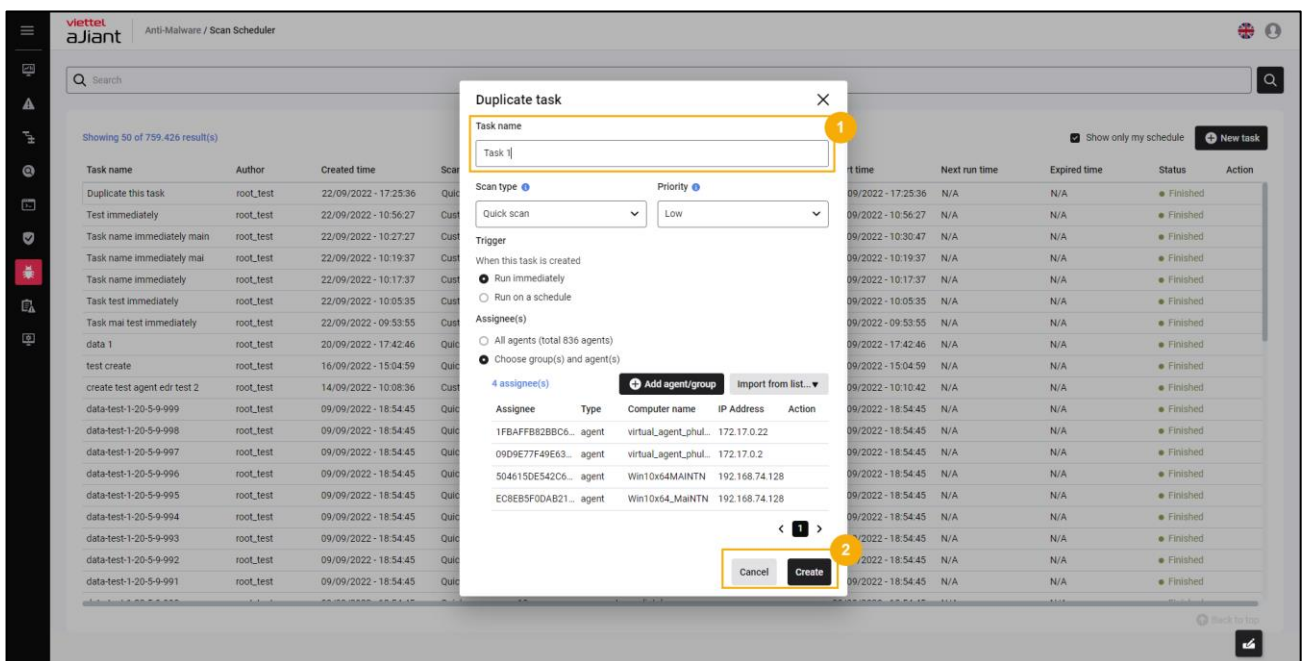
The screenshot shows the 'Anti-Malware / Scan Scheduler' interface. It displays a table with 11 results. The 'Task 456' row is highlighted, and a context menu is open over it, showing options: 'View report', 'View detail', 'Duplicate this task' (highlighted with a red box), and 'Delete this task'.

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	...
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	...
éviewe	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	...
maifest	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 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.

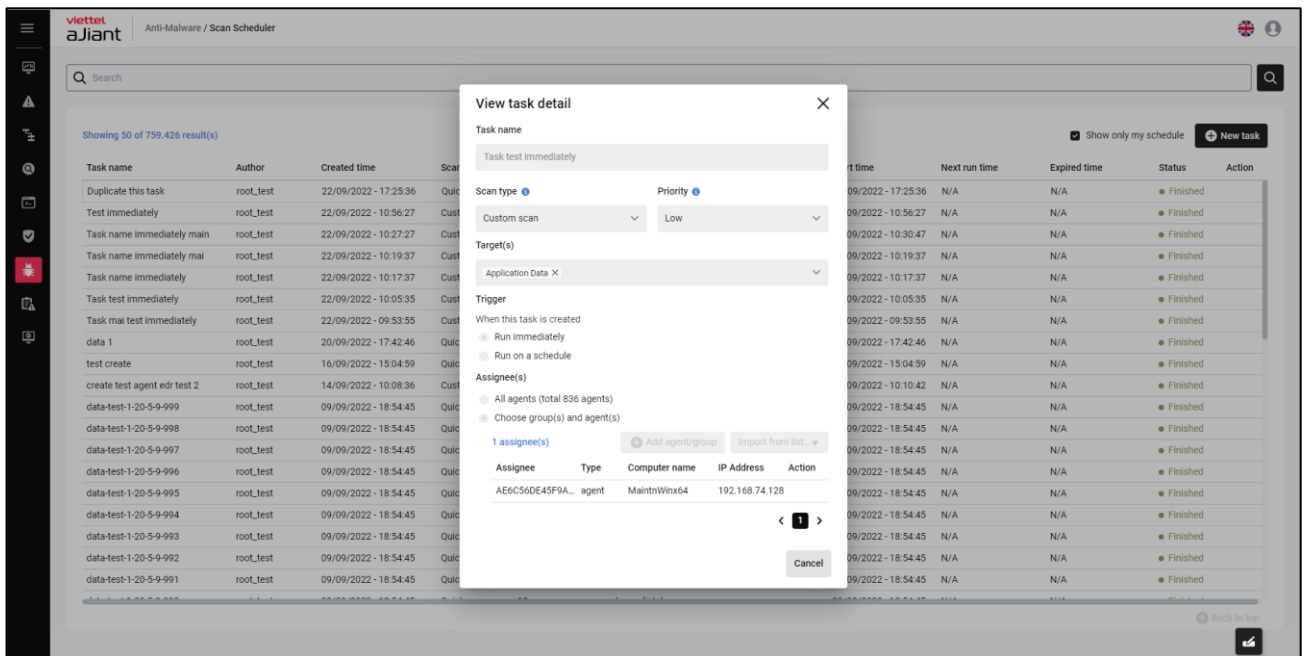


Xem chi tiết

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

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;

Anti-Malware / Scan Scheduler

Showing 50 of 759,426 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
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	View report View detail Duplicate this task Delete this task
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	

Back to top

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

Anti-Malware / Scan Scheduler

Showing 50 of 759,426 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
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 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	

Back to top

Xem báo cáo

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

Các bước thực hiện:

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

The screenshot shows the Viettel aJiant Anti-Malware / Scan Scheduler interface. It displays a table of tasks with columns: Task name, Author, Created time, Scan type, Number of agent(s), Trigger, Start time, Next run time, Expired time, Status, and Action. A red box highlights the 'View report' button in the Action column for the task 'Task mai test immediately'.

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	View report View detail Duplicate this task Delete this task
data 1	root_test	20/09/2022 - 17:42:46	Quick scan	1	Immediately	20/09/2022 - 17:42:46	N/A	N/A		
test create	root_test	16/09/2022 - 15:04:59	Quick scan	0	Immediately	16/09/2022 - 15:04:59	N/A	N/A		
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		
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		
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		
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 **View report**:

1 – Tìm kiếm:

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

Các bước thực hiện:

View task report

Task nameTask per

Created time14/09/2022 14:32:24

Authorroot_test

Scan typeCustom scan

2

1

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.

2 – 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 nameTask per

Created time14/09/2022 14:32:24

Authorroot_test

Scan typeCustom scan

2

1

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.

3 – View on dashboard

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

The screenshot shows the 'View task report' window. At the top, it displays task details: Task name, Task per, Author (root_test), Created time (14/09/2022 14:32:24), and Scan type (Custom scan). Below this is a search bar with 'fx' and a magnifying glass icon. To the right are two buttons: 'Export to Excel' and 'View on Dashboard' (highlighted with a yellow border). Below the buttons, it says '5 result(s)'. A table follows with columns: Agent ID, Computer name, IP Address, Platform, Group, Status, and Result. The table contains three rows of scan data. At the bottom right, there is a 'Back to top' link.

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	Blichpt3_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;

3.11.2 Device control

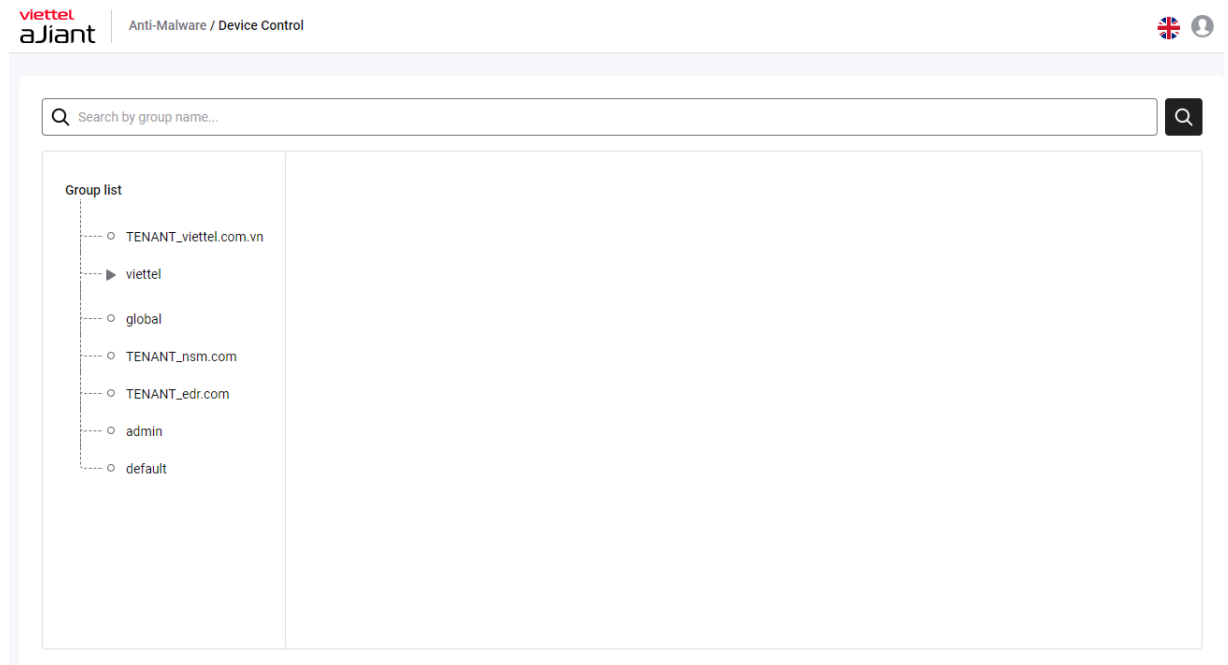
Chức năng: Cho phép kiểm soát, bảo vệ dữ liệu quan trọng thông qua thiết bị ngoại vi, như ổ USB, thiết bị Bluetooth và đĩa CD và DVD ghi được.

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

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



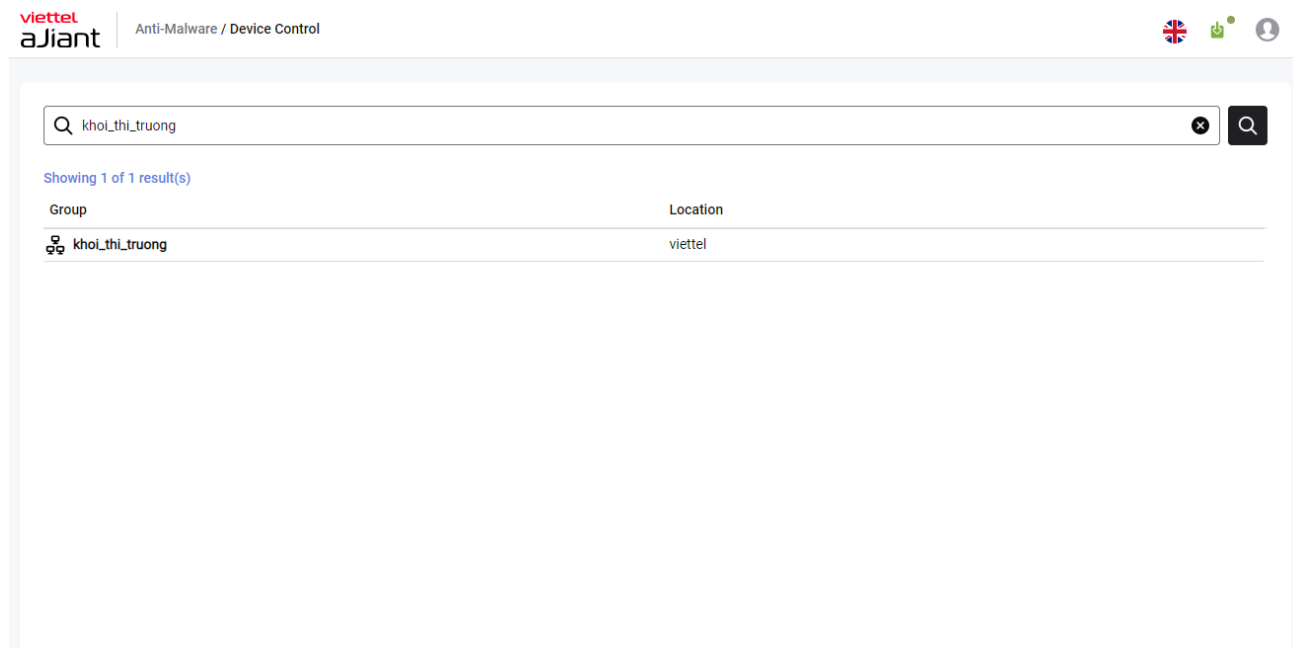
Bước 1: Người dùng nhập vào từ khóa tìm kiếm ở Search by group name (Có từ từ khóa gợi ý theo text)



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.

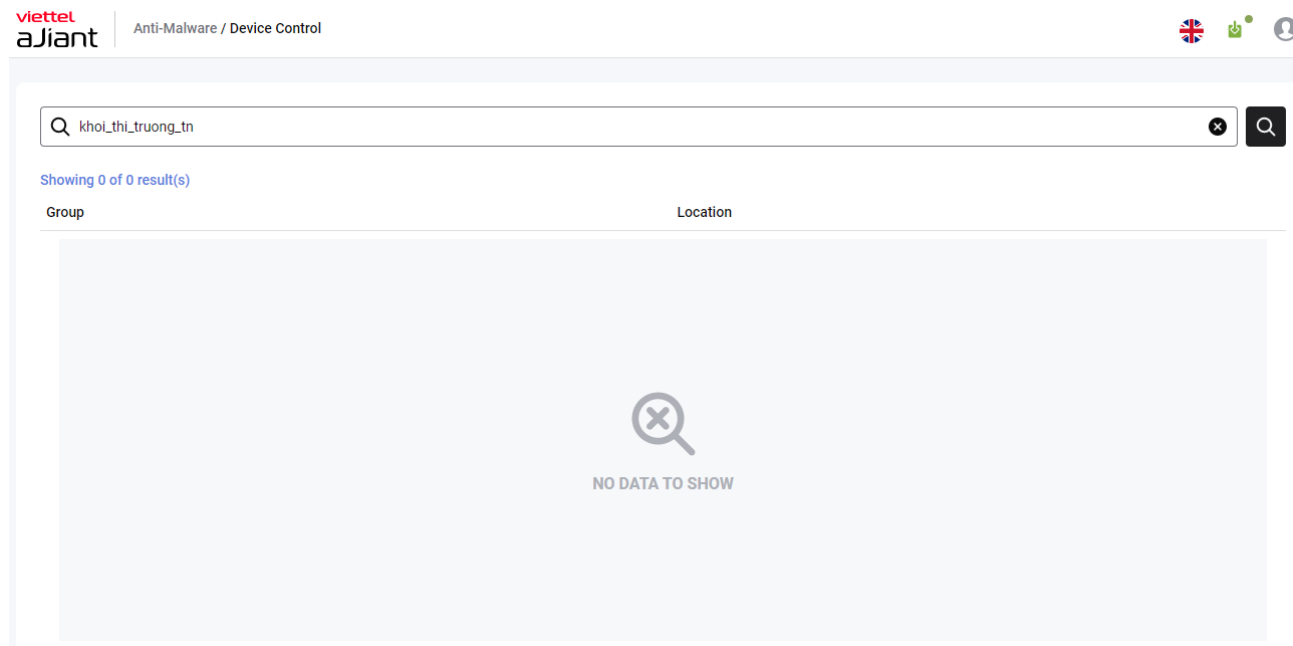
Nếu có kết quả sẽ trả về



The screenshot shows the Viettel aJiant interface with the search bar containing 'khoi_thi_truong'. Below the search bar, it says 'Showing 1 of 1 result(s)'. A table displays the search results:

Group	Location
 khoi_thi_truong	viettel

Còn tìm kiếm không có kết quả



The screenshot shows the Viettel aJiant interface with the search bar containing 'khoi_thi_truong_tn'. Below the search bar, it says 'Showing 0 of 0 result(s)'. The table area is empty, and a message 'NO DATA TO SHOW' is displayed with a magnifying glass icon.

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)

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	
teasdass	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:

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

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

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

6. Action:

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

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

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

Tối đa 20 bản ghi trên bảng danh sách exception

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

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

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

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 *

Permission

Rule 01

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). Ký tự theo alphabet, số 1,2,3..0, không phân biệt chữ hoa, chữ thường, dưới 500 ký 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 hiển thị dd/mm/yyyy hh:mm:ss - dd/mm/yyyy hh:mm:ss (mặc định là thời điểm hiện tại đến tương lai, thời gian để chênh 5 phút để người dùng k bị gặp lỗi khi đang Add exception (thời gian thao tác lâu)

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

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

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

6. Action:

- Button Add: tạo mới được các Exception

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

Khi chưa có device: Chỉ hiển thị Button Add device

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

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

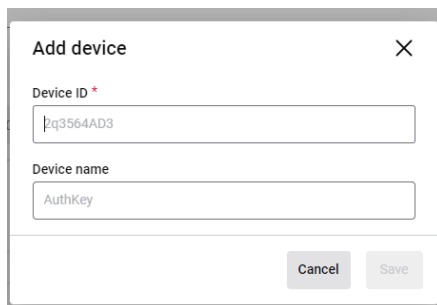
Device list (1)

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
☐	15B2BBFFEBBC988C8080297...	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 hiển thị các trường thông tin như cột: Agent ID, Computer name, IP address, Group, Status
 - + Nếu không có dữ liệu thỏa mãn, thông báo: No data;
 - + Nếu có dữ liệu thỏa mãn: Hiển thị danh sách tương ứng;
- Checkbox: Cho phép check chọn 1 hoặc nhiều Agents, Mặc định không check;
- Agent ID: Hiển thị thông tin Agent ID

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

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

Sau khi Add xong Agent quay về màn Add Exception:
Sẽ hiện thị các trường : Agent ID Computer name IP Address Group Status
Màn này 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)
X

Q Search by group name...

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
X NO DATA TO SHOW		

Cancel Save

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: Hiện 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)

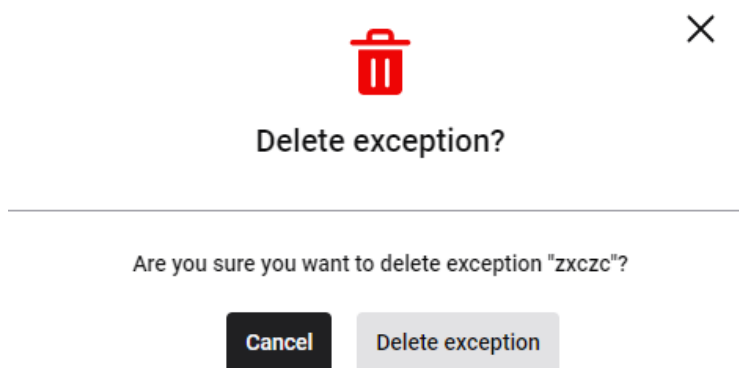
☐ Choose agent(s) (0)

☐ 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



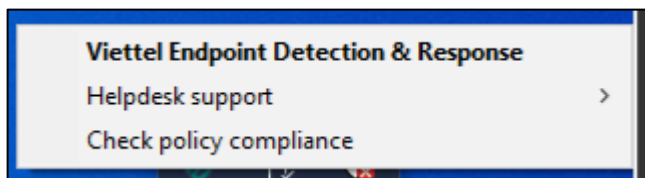
Nếu chọn Button **Delete exception** người dùng đồng ý Exception này. Lúc này Portal sẽ hiện thị 1 thông báo, Bạn đã xóa exception thành công

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

3.12 Giao diện phía Agent GUI - Main

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

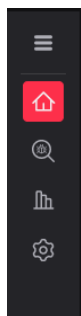
Trên thanh taskbar tìm icon  click chuột phải và chọn “Viettel Endpoint Detection & Response”:



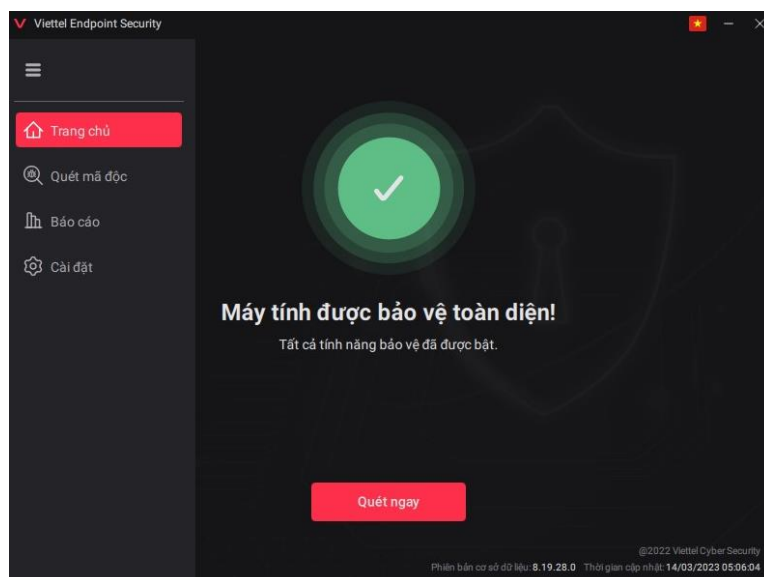
Hệ thống hiển thị các thông tin:

- + Được hiển thị 2 ngôn ngữ: Anh-Việt.

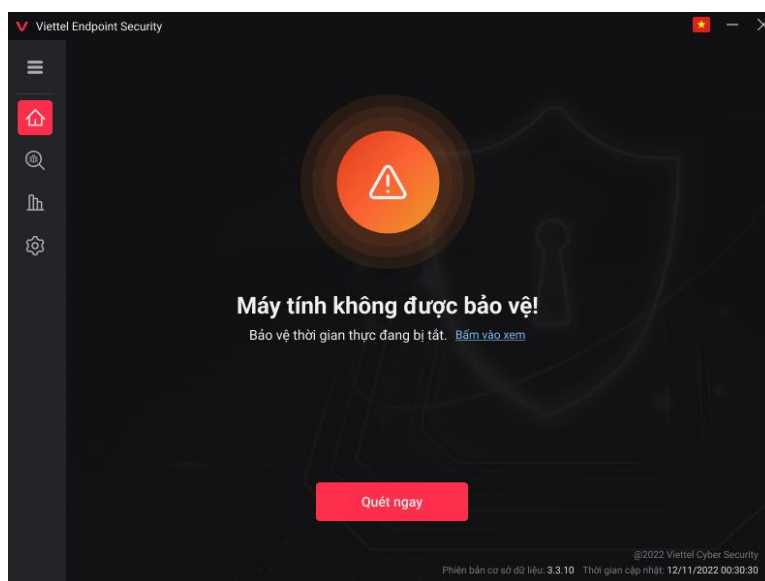
+ Trên Siderbar hiện icon cho các tính năng lớn: Trang chủ, Quét mã độc, Báo cáo, Cài đặt. Có thể đóng hoặc mở rộng sidebar.



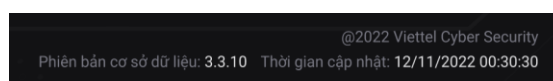
+ Trường hợp máy không có mã độc nào, đã được bật Real-time Protection hoặc toàn bộ mã độc đã được xử lý:



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



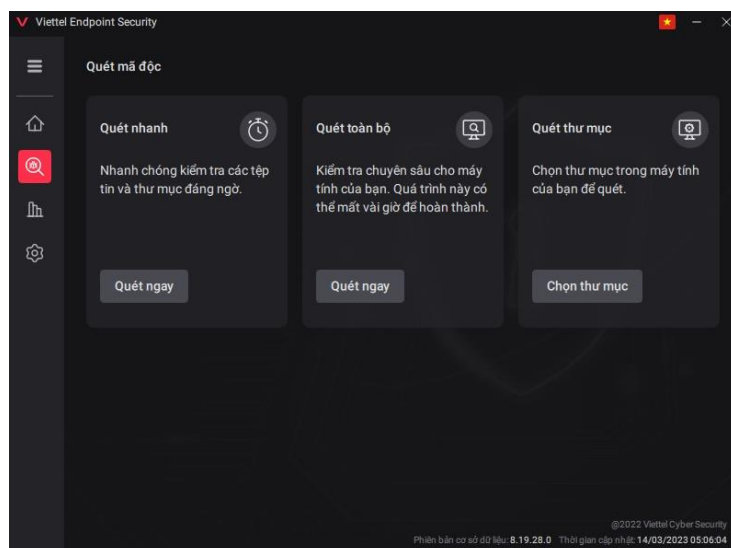
Thông tin về version: thông tin về phiên bản Agent cài trên máy người dùng, thời gian update và thông tin hỗ trợ sản phẩm, được thể hiện ở góc màn hình.



3.13 Giao diện phía Agent GUI - Protection

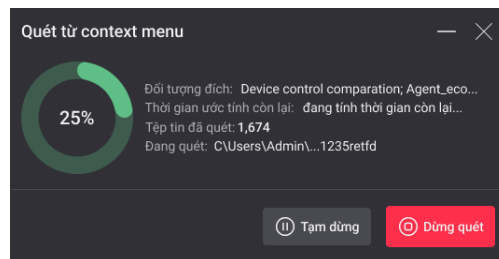
Mục đích: cho phép người dùng chủ động sử dụng hệ thống để quét và xử lý mã độc trên máy

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

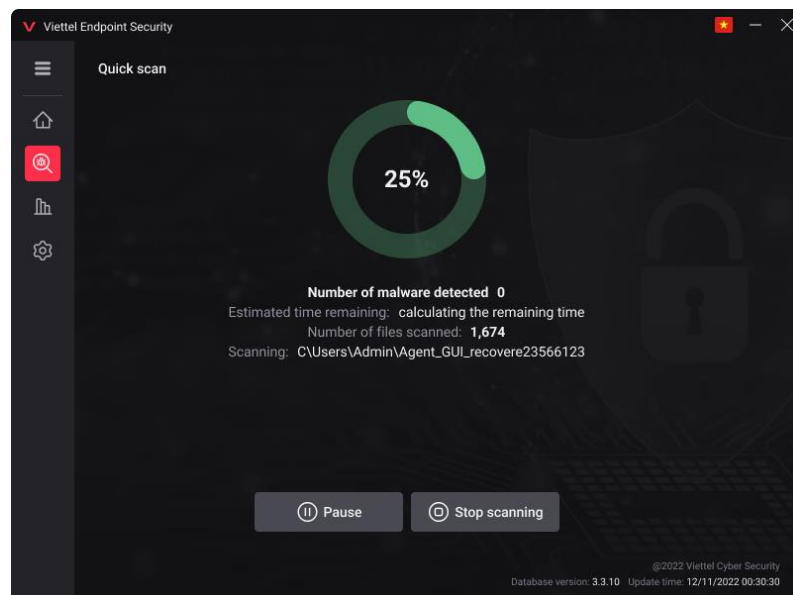


Các phương thức quét được hỗ trợ bao gồm

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

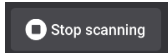


Sau khi chọn phương thức phù hợp, hệ thống thực hiện quét và xử lý mã độc:

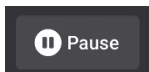


- + Hiển thị % tổng quá trình scan
- + Hiển thị thông tin số lượng mã độc đã được phát hiện
- + Hiển thị thời gian ước lượng còn lại để kết thúc scan
- + Hiển thị số lượng file đã được scan
- + Hiển thị đường dẫn file Đang scan

Hỗ trợ các thao tác trong lúc quét như sau:



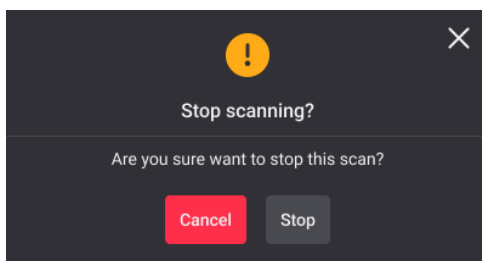
: Cho phép kết thúc quá trình quét;



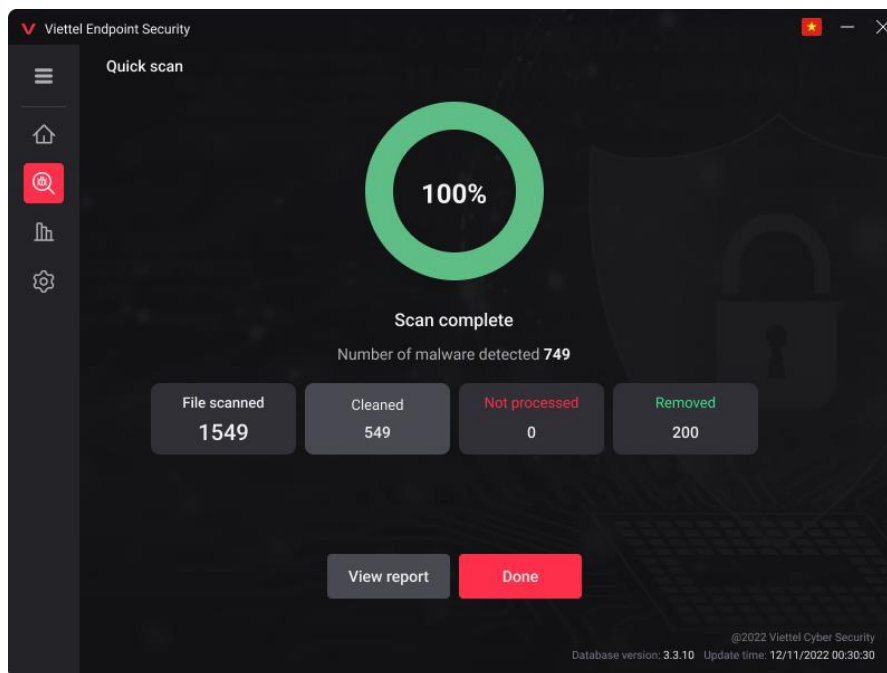
: Cho phép tạm dừng quá trình quét;



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



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



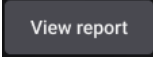
+ File scanned: Hiển thị số lượng file đã được scan

+ Cleaned: Hiển thị tổng số file đã được diệt

+ Not processed: Hiện thị tổng số file chưa xử lý

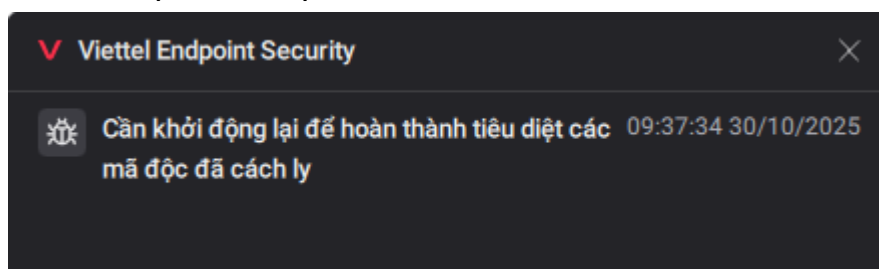
+ Removed: Hiện thị tổng số file đã được xóa

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

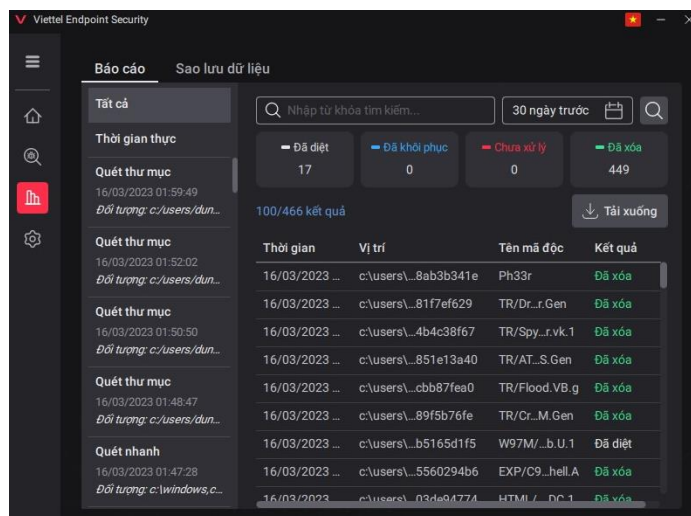
Sau quá trình quét, nếu agent phát hiện mã độc dạng dll đang được load mà không thể xóa trực tiếp được, agent sẽ hiển thị popup yêu cầu restart máy để hoàn tất quá trình quét



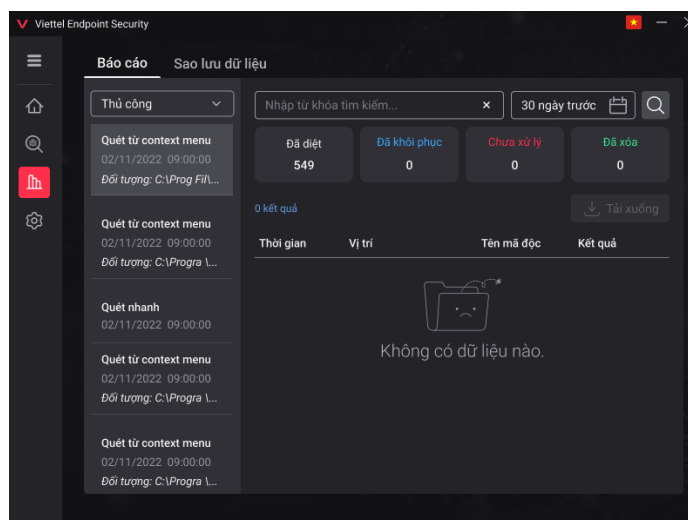
3.14 Giao diện phía Agent GUI - Report

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

a. Tab report (Báo cáo)



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



- Nếu người dùng chọn All:

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

- Nếu người dùng chọn *Manual scan*:

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

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

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

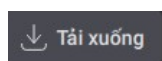
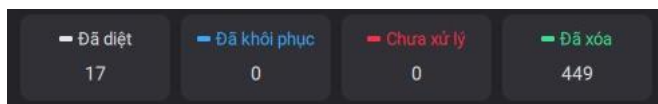
- Nếu người dùng chọn *Real-time*:

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

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



- *Tìm kiếm theo kết quả mã độc*

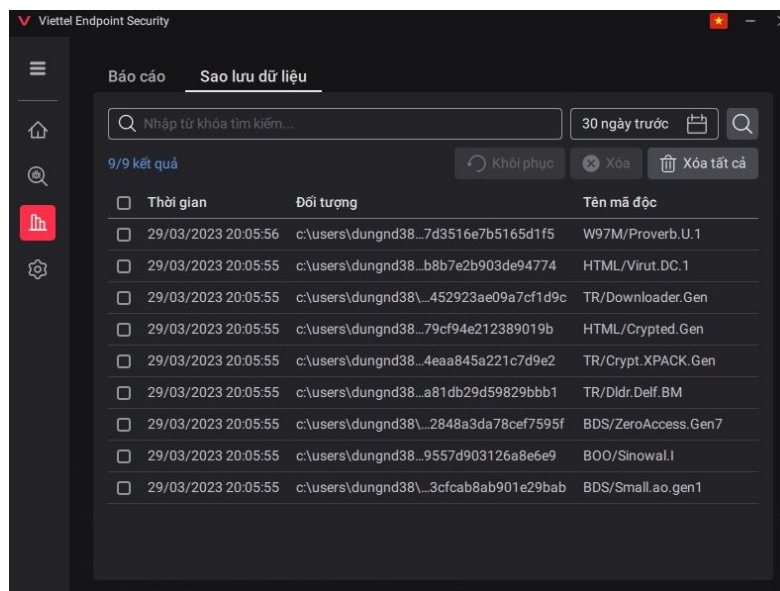


Trong mục report người dùng có thể tải toàn bộ báo cáo về máy (theo các mục đã chọn)

b. Tab Backup

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

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



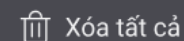
Các file chứa mã độc trước khi được xử lý đều được lưu trữ bản gốc trong thư mục Backup, để dọn thư mục Backup hoặc phục hồi file, sản phẩm cung cấp các tính năng sau:



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

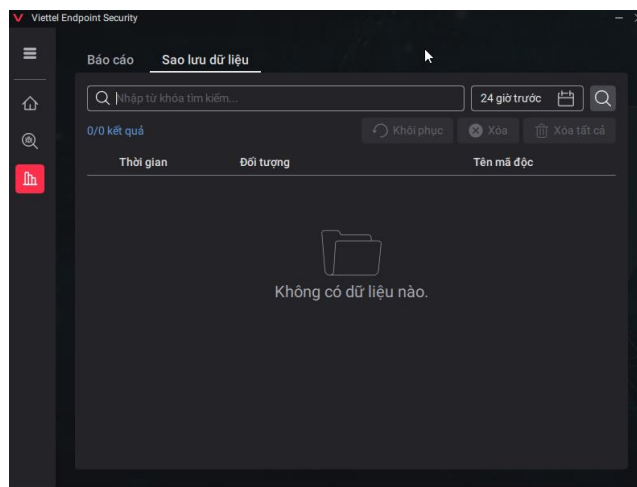


: Cho phép lựa chọn 01 hoặc nhiều file để xóa khỏi thư mục Backup;



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

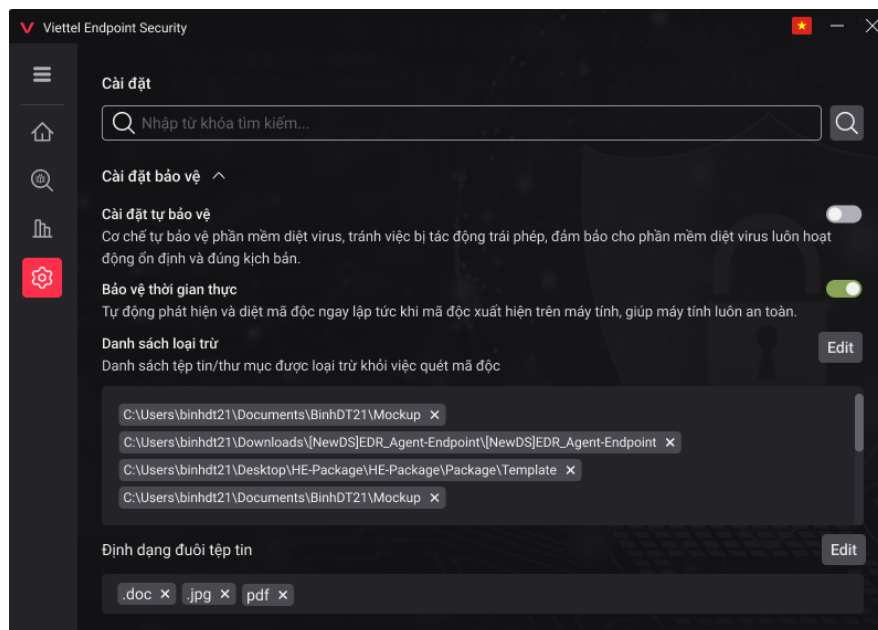
- Trong trường hợp không có kết quả phù hợp với yêu cầu tìm kiếm thì hiển thị trạng thái **Không tìm thấy kết quả phù hợp**



3.15 Giao diện phía Agent GUI - Setting

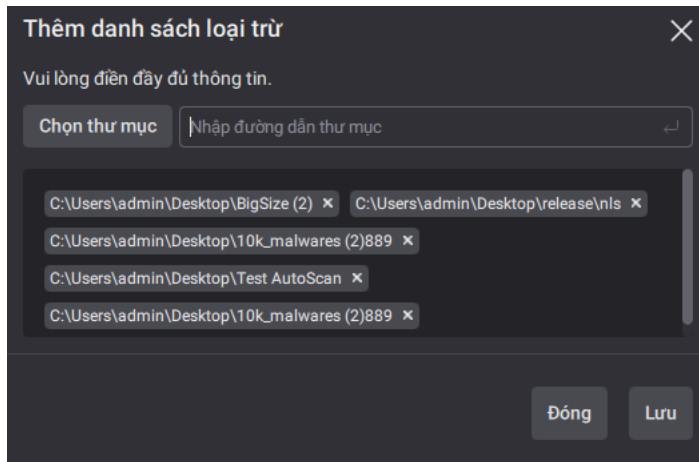
Mục đích: Cấu hình cài đặt trên từng máy agent

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

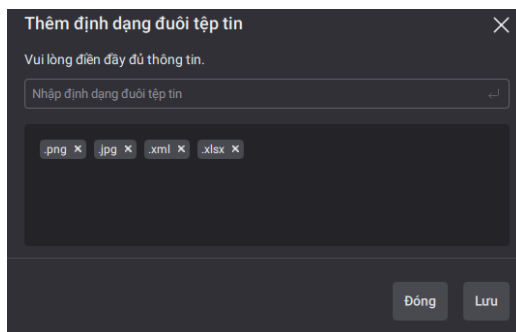


- a. **Protection setting (Cài đặt bảo vệ):** Vì có 2 vị trí cấu hình Policy (Self defense và Real-time protection) trên Portal và dưới từng Agent.

- Self defense: Cho phép bật tắt Self defense. → Bảo vệ các tài nguyên của agent, tránh việc bị tác động trái phép từ các tác nhân bên ngoài - *Chưa update hoàn thiện*
- Real-time protection: Bảo vệ toàn diện cho máy tính, tự động phát hiện và diệt mã độc ngay khi chúng xuất hiện trên máy tính (Bật/Tắt thiết bị)
- Exclusion list: Cho phép lựa chọn folder được loại trừ (không bị quét bởi Real-time Protection); *Thêm mới/ Chỉnh sửa folder được loại trừ*

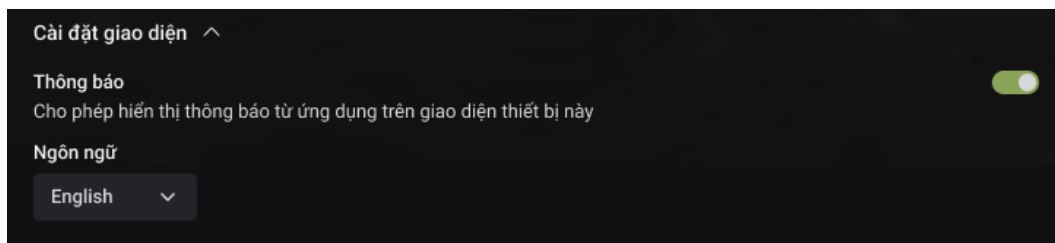


- Extension: Cho phép thêm mới/ chỉnh sửa vào Extension (Loại đuôi tài liệu) được loại trừ (không bị quét bởi Real-time Protection);



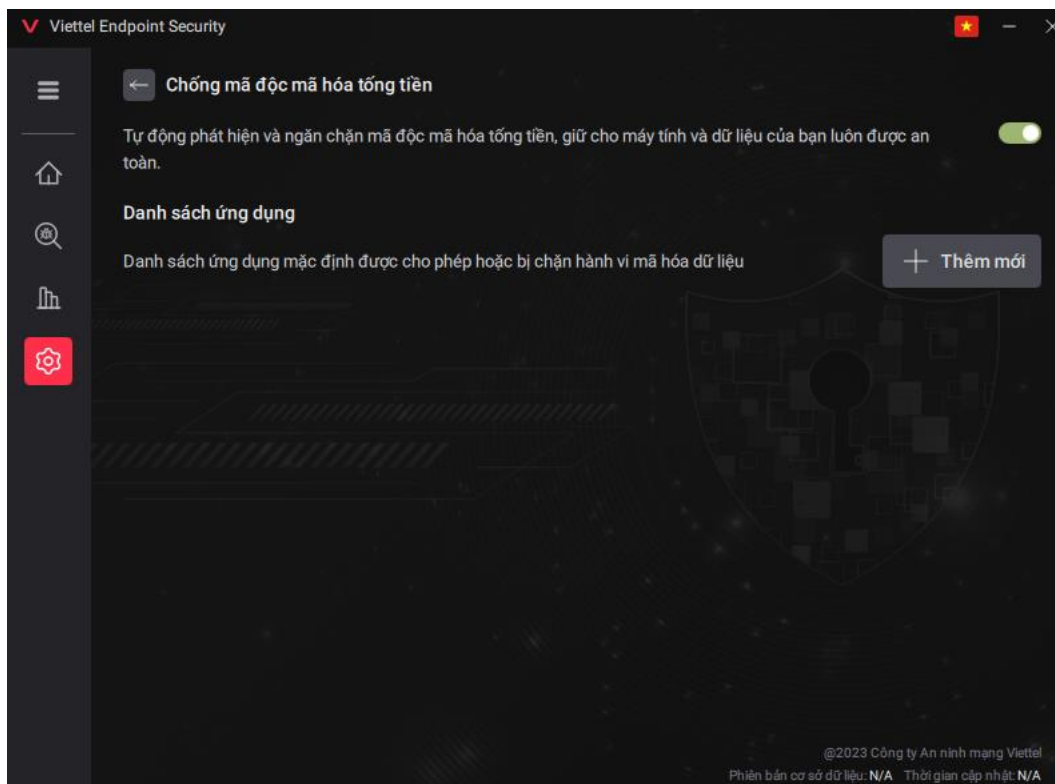
b. Interface setting (Cài đặt giao diện)

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

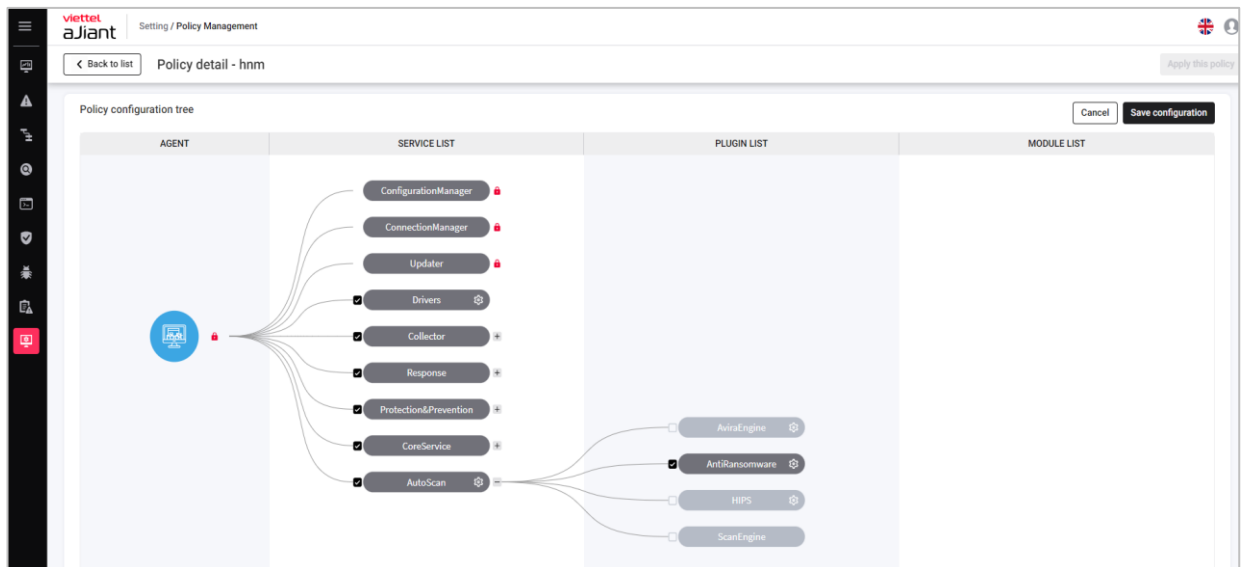


c. Anti-Ransomware (Chống mã độc mã hóa tổng tiền)

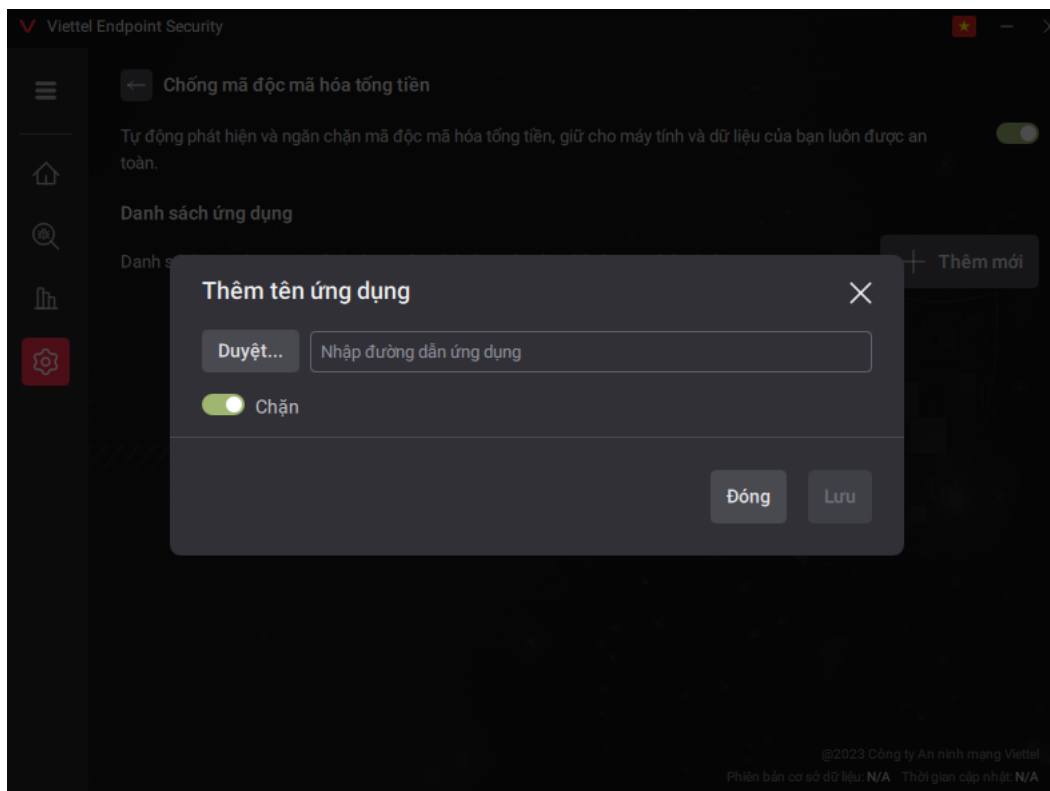
- Cho phép người dùng bật/tắt chế độ bảo vệ mã độc mã hóa tổng tiền. Hệ thống sẽ tự động phát hiện và ngăn chặn mã độc mã hóa tổng tiền cho máy tính.



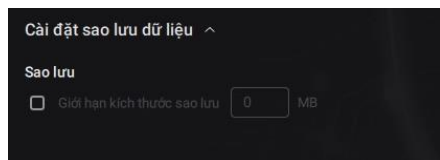
Lưu ý: Để sử dụng tính năng cần bật Policy AntiRansomware trên Portal



- 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



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



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

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

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

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

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

Chạy command liệt kê các tính năng hỗ trợ

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

Manage scan & protection service

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

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

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

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

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

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

3.16.1 Sub-command scan

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

a. Bắt đầu 1 scan session

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

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

b. Dừng 1 scan session

Người dùng chỉ định scan session cần dừng quét

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

c. Hiển thị trạng thái của 1 scan session

Người dùng chỉ định scan session cần hiển thị thông tin

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

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

Hiển thị các scan session đang quét và vị trí quét

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

3.16.2 Sub-command report

a. Liệt kê lịch sử quét và thông tin

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

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

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

```
$ VESAutoScan report list all
```

+-----+						
Realtime Scan Report						
+-----+						
REPORT ID	MALWARE DETECTED					
+-----+						
realtime	2					
+-----+						
+-----+						
Manual Scan Report						
+-----+						
REPORT ID	TIMESTAMP	LOCATION	FILE	FILE SCANNED	MALWARE DETECTED	STATUS
+-----+						
1	2025-07-10T17:46:32+07:00	/usr,/home	30231	312837	0	Stopped
2	2025-07-10T17:53:01+07:00	/usr,/home	56013	312838	0	Scanning
+-----+						

b. Hiển thị thông tin chi tiết về 1 báo cáo

Người dùng chỉ định id của báo cáo cần hiển thị, có thể chỉ định “realtime” để hiển thị báo cáo chi tiết cho tính năng quét mã độc theo thời gian thực

```
$ VESAutoScan report show realtime
```

+-----+		
FILE PATH	MALWARE NAME	STATUS
+-----+		
/adware+virus	ADWARE/Patched.Ren.Gen	Deleted
+-----+		
TOTAL		1
+-----+		

```
$ VESAutoScan report show 3
```

+-----+						
REPORT ID	TIMESTAMP	LOCATION	FILE	FILE SCANNED	MALWARE DETECTED	STATUS
+-----+						
3	2025-07-10T18:13:19+07:00	/home	496	153052	1	Scanning
+-----+						
+-----+						
FILE PATH	MALWARE NAME	STATUS				
+-----+						
/home/adware+virus	ADWARE/Patched.Ren.Gen	Deleted				
+-----+						
TOTAL		1				
+-----+						

c. Tìm kiếm file hoặc mã độc đã từng phát hiện

Người dùng có thể chỉ định 1 phần đường dẫn đến file cần tìm

```
$ VESAutoScan report search home
```

+-----+		
REPORT ID: 3		
+-----+		
FILE PATH	MALWARE NAME	STATUS
+-----+		
/home/adware+virus	ADWARE/Patched.Ren.Gen	Deleted
+-----+		
TOTAL		1
+-----+		

3.16.3 Sub-command backup

- a. Liệt kê các file đã phát hiện và có thể khôi phục

```
$ VESAutoScan backup list
+-----+-----+
| FILE ID | FILE PATH |
+-----+-----+
|      1  | /adware+virus |
|      2  | /home/adware+virus |
+-----+-----+
|   TOTAL | 2         |
+-----+-----+
```

- b. Tìm kiếm file đã phát hiện và có thể khôi phục

Người dùng chỉ định 1 phần đường dẫn đến file cần tìm

```
$ VESAutoScan backup search home
+-----+-----+
| FILE ID | FILE PATH |
+-----+-----+
|      2  | /home/adware+virus |
+-----+-----+
|   TOTAL | 1         |
+-----+-----+
```

- c. Khôi phục 1 file

Người dùng chỉ định id của file được sao lưu và tên file sau khi khôi phục, có thể chỉ định tên file là đường dẫn tuyệt đối hoặc tương đối

File sau khi khôi phục được nén dạng zip và đặt mật khẩu là “infected”

```
$ VESAutoScan backup restore 2 /home/linux/malware
restoring adware+virus to /home/linux/malware.zip
restore success to /home/linux/malware.zip with password: infected
```

3.16.4 Sub-command show

- a. Hiển thị phiên bản của service quản lý quét mã độc

```
$ VESAutoScan show version
Version: 3.3.0.545.e8d14fe
Build: 2025-06-09T10:30:04+0000
```

- b. Hiển thị phiên bản database

```
$ VESAutoScan show database-version
DatabaseVersion: 8.20.57.224
UpdateDate: 10/07/2025 17:55:30
```