viettel
security

Viettel Endpoint Detection & Protection

(VCS-aJiant バージョン EDP)

ドキュメントバージョン: 4.133 – 更新日: 2025年12月15日

ユーザーマニュアル

更新履歴

番号	更新日	バージョン	変更理由	注記
1	…	3.3.0		
2	2022年6月30日	3.3.20	補足／更新ガイドライン： 3.4.8 IRFlowレスポンス - 73 3.6 レスポンス - 119 3.7.5 更新管理 - 174	
3	2022年10月10日	3.3.31	補足／更新ガイドライン： 3.11 アンチマルウェア – 247	
4	2022年12月16日	3.3.38	補足／更新ガイド： 3.5.4 調査_ツール展開 - 116	
5	2022年12月28日	3.3.43	補足／更新ガイド 3.6.1 Response_Live response - 154	

番号	更新日	バージョン	変更理由	注記
6	2023年3月21日	4.5.1	2段階認証（2FA）の有効化手順を追加してください。	
7	2023年4月20日	4.14.0	新しいエージェントGUIの更新	
8	2023年5月15日	4.18.0	デバイス制御の指示を追加する	
9	2023年12月9日	4.48	- ランサムウェア対策機能の使用方法を追加 - インターフェースを更新	
１０	2023年9月27日	4.52	3.10.2　エンドポイントファイアウォール機能の更新	
１１	2024年7月15日	4.52	BLSのルールを補足して明確にする。	
１３	2024年11月13日	4.100	ポリシーにおける自動スキャン設定の使用方法	
14	2024年12月17日	4.106	脅威ハンティング機能の使用方法ガイド	
15	2025年6月10日	4.110	VCS-aJiant製品のライセンス計算方法を3.7.1項に追加する	

番号	更新日	バージョン	変更理由	注記
16	2025年10月7日	4.115.0	マルウェアスキャン機能のコマンドライン インターフェース使用ガイド 第3.17節	
17	2025年9月18日	4.128.0	BLS規則違反検査の説明を補足する セクション3.5.2.3.1	
1 8	2025年11月4日	4.130.0	3.5.2項の追加 – アイソレートデバイスの使用方法の案内 3.3.4項の更新 – IRフロー機能の非表示 3.4.2項の更新 – マークアーティファクト機能の非表示	
19	2025年11月4日	4.131.0	マルウェア隔離機能の説明を追加してください。セクション3.14	
20	2025年11月24日	4.132.0	エージェント管理画面のインターフェースをバージョン3.6.1に更新する	

索引

専門用語

用語	解説	注記
VCS-aJiant	製品の商標名	

用語	解説	注記
IRフロー	インシデント対応フロー：アラートの処理、調査および対応の運用フロー。	
アーティファクト	アラートに関連する調査対象：ファイルパス／レジストリ／プロセス	
検出	アラートに関連する対象の検出	
封じ込め	コンピュータの隔離プロセス：ネットワークの隔離、プロセスの一時停止	
調査	調査プロセス：イベントログに基づく調査またはユーザーの端末上のツールを用いた積極的な調査があります。 サポートされている調査方法は以下の通りです。 プロセス分析 イベントログの検索 調査ツールの使用：autoruns、listdlls - -	

用語	解説	注記
応答	反応の過程：調査結果から、オペレーターは調査結果を以下の方法で処理します： レスポンスシナリオ ライブレスポンス - -	
タイムライン	タイムラインは以下の活動を示します： プロセス分析セッションの作成／終了 ライブレスポンスセッションの作成／終了 - -	

1. 紹介

1.1 現在の状況

今日、多くの組織や企業は、システム内の高度なマルウェアの検出、特定、調査、および軽減において多くの困難に直面しています。従来の署名ベースのアンチウイルスなどのマルウェア対策技術は、高度なスキルを持つプロの攻撃者によって、攻撃ツールキットやカスタマイズされた標的型マルウェアを用いて意図的に突破されています。多くの組織は、従来のマルウェア防御手法が失敗していることを認めており、エンドポイントでの侵害を特定するための新たな戦略を構築する必要があります。最近の高度なマルウェアによる多数のデータ侵害は、エンドポイント検出および

対応（EDR）ソリューションに対する顧客の関心を高めており、その中にVCS-aJiantも含まれています。

1.2 技術の発展

VCS-aJiantソリューションの技術は、アンチウイルスやIPS/IDSなどの署名ベース技術の欠点を補完し、行動に基づく異常検知能力を提供するとともに、エンドポイント上の関連する具体的な情報に関するより深い洞察を可能にし、高度な脅威の検出と軽減を実現します。

1.3 VCS-aJiant

VCS-aJiantは、攻撃者が内部ネットワーク内のシステムやアプリケーションに対してスキャンを行ったり、盗まれた情報を利用したりする際のマルウェア感染や横展開（ラテラルムーブメント）に関する詳細な情報を提供する能力を有しています。

さらに、VCS-aJiantは既存のセキュリティ技術であるセキュリティ情報およびイベント管理（SIEM）、ネットワークフォレンジックツール、および高度な脅威検出装置（Advanced Threat Detection）を補完し、組織の情報セキュリティインシデント対応ソリューションのポートフォリオを拡充します。

1.4 アップグレード情報

バージョン3.3.0では、以下の新機能が追加されました。

ログイン機能およびプロセス分析機能を新しいインターフェース設計に基づいて改良し、ユーザー体験を向上させるとともに、調査過程でユーザーを支援するために必要なプロセス情報を追加する。

旧バージョンの問題を改善し、安定性を確保しました。

2. 概要

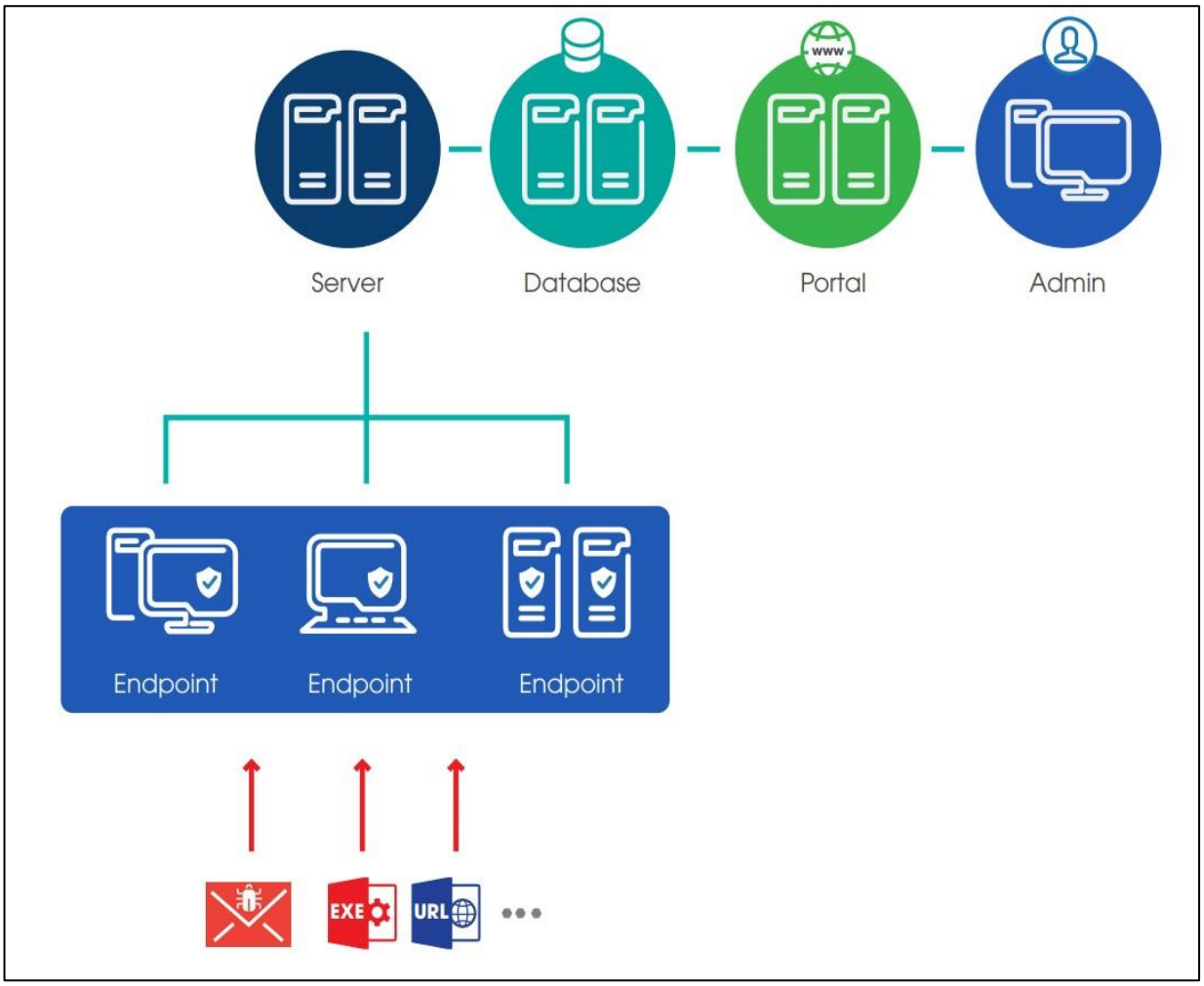
2.1 技術

VCS-aJiantは、Filter Driver技術（カーネルレベルでの実行および監視を可能にする）を使用して、ユーザーのコンピュータおよびサーバー上のファイル、プロセス、レジストリ、ネットワークに関する情報を収集します。ファイルに関する兆候には、変更、削除、属性の変更が含まれます。レジストリに関しては、キーや値の削除、値の設定、キーや値の名前変更、疑わしいアクセスを伴うキーの作成などがあります。メモリに関する疑わしい兆候は定期的にスキャンおよび監視されます。疑わしい行動はすべて集中分析のためにバックエンドシステムに送信されます。

攻撃調査の業務フローは、インシデントレスポンスのシナリオに基づき一貫して設計されており、単一のインターフェース上で異常の兆候を検出・分析することを支援します。エンドポイント上での高度なフォレンジック調査機能を提供し、疑わしいファイルの取得（Get Artifact）、スキャンツールの展開（Tool Deployment）をサポートします。また、調査の実施やリアルタイムでの証拠提供（プロセス分析、ライブレスポンス）を可能にし、脅威検出時の迅速な対応を実現します。

異常が確認され次第、エンドポイントは広範囲にわたるマルウェア除去ツール（レスポンスシナリオ）を提供します。これには、感染した端末のネットワーク隔離（ネットワークコンテインメント）、プロセスの強制終了、ファイルおよびレジストリの削除が含まれます。

2.2 インフラストラクチャーアーキテクチャ



主な成分は3つあります。

エージェント：各ワークステーションおよびサーバーにインストールされるコンポーネントであり、ワークステーションやサーバー上の異常兆候を監視し、ログを集中管理サーバーに送信する役割を担います。

管理、集中処理および保存サーバークラスター：エージェントから送信されたデータを処理するコンポーネントであり、リアルタイムでのデータ分析および処理において主要な役割を果たします。

ウェブポータルインターフェース：管理者がシステムの情報を監視、監督、分析するために使用するコンポーネントです。

2.3 管理インターフェースで作業する

Webポータルのインターフェースは、以下の機能インターフェースおよび処理フローで構成されています。

ダッシュボード：組織の情報セキュリティ状況に関する統計および視覚的なグラフ。

アラート管理：ユーザーの端末でマルウェアの兆候が現れたアラートの一覧。

調査：調査に使用されるツールの一覧（プロセス分析、イベント検索、および展開ツール）；

回答：ライブレスポンス（リアルタイム対応・インシデント対応）に使用されるツールの一覧；

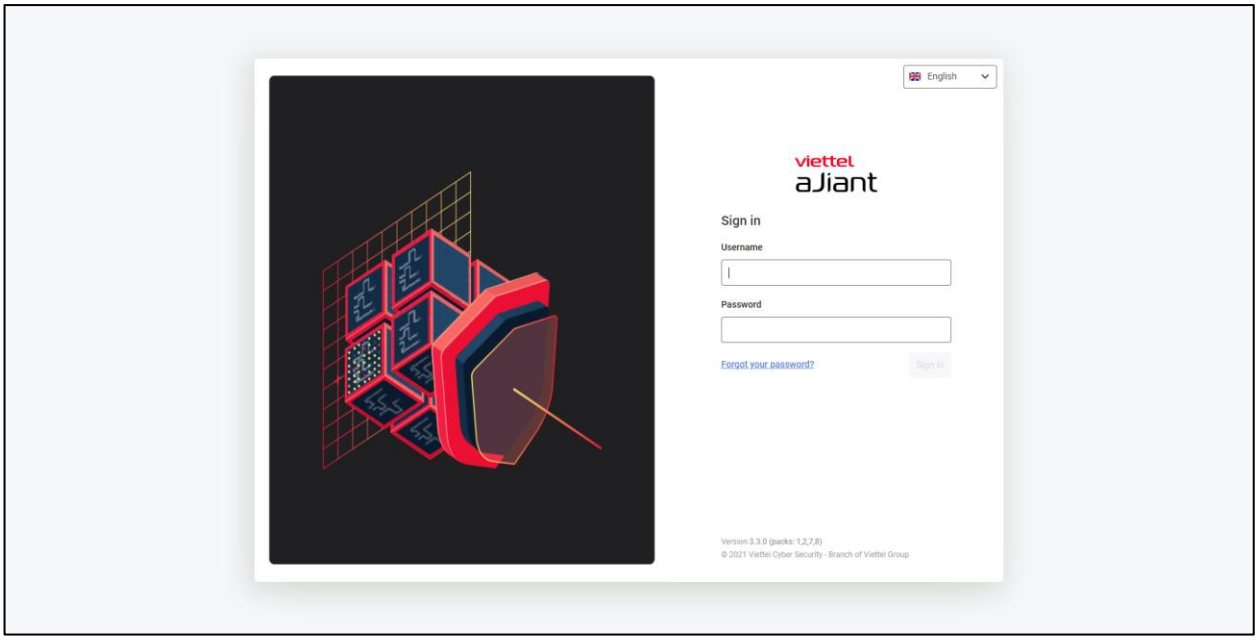
保護と予防：ワークステーションの防御および保護機能の一覧（アプリケーション制御およびエンドポイントファイアウォール）；

設定：システム設定機能一覧（ポリシー管理、エージェント管理、グループ管理、ルール相関、アカウント管理：ユーザー管理、ロール管理、権限管理）

3. 使用説明書

3.1 ログイン

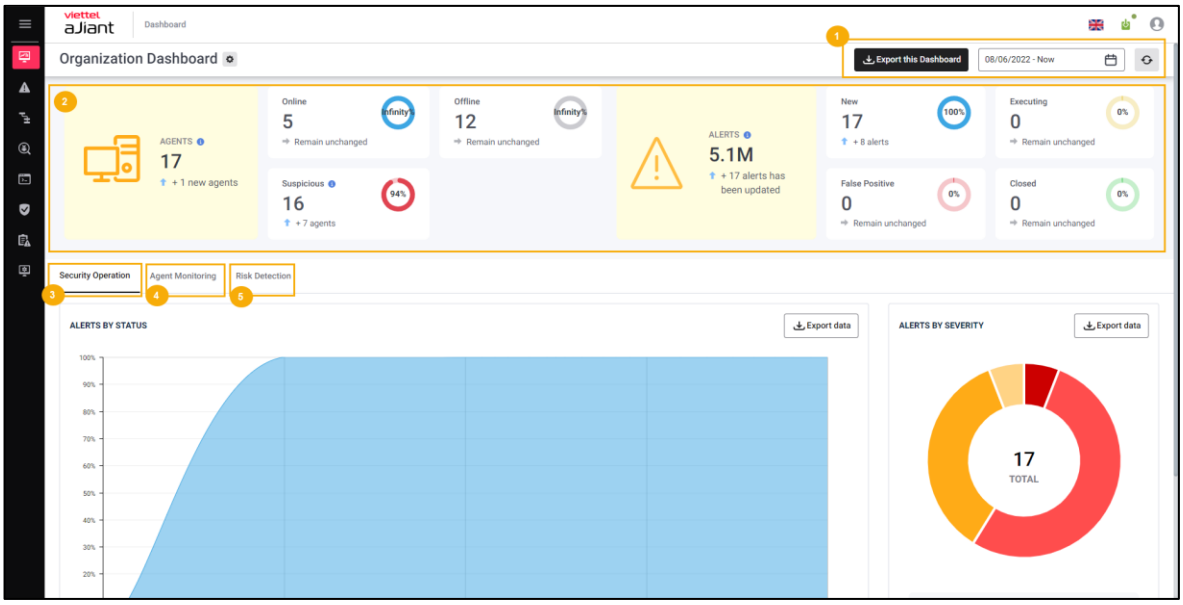
- 提供されたアドレスからシステムにアクセスしてください。



- 付与されたユーザー名とパスワードでログインしてください。

3.2 VCS-aJiant ダッシュボード

主な機能は以下の通りです：



1 – ダッシュボード上でのデータ操作：

+ ダッシュボードからデータを抽出する。

+ 過去最大90日間のデータを検索する。

+ データを更新する。

2 – 概要：組織の情報セキュリティ状況の総合統計（エージェントの状態およびアラートを通じて）。

3 – セキュリティ運用：アラートの運用監視を通じて情報セキュリティの運用状況を監視すること。

4 – エージェント監視：エージェントのインストール状況および状態の監視；

5 – リスク検出：組織に対する脅威を監視する（システム内で未処理のアラートが最も多く発生している対象を統計的に把握することによって）。

機能におけるデータの権限分配は以下の通りです：

+ ユーザーがrootグループに属している場合：システム全体のデータを表示する。

+ ユーザーがレベル1グループに所属している場合：レベル1グループおよびその配下のすべてのサブグループのデータを表示する。

+ ユーザーがグループレベル2以上に所属している場合：ログイン中のユーザーが所属するグループを含むレベル1の全グループおよび該当するレベル1グループに属するすべての子グループのデータを表示します。

3.2.1 *データの操作*

データのエクスポート

目的：ダッシュボードの画面上で既存のデータを選択して抽出できるようにし、さらに報告を支援する詳細データシートを追加すること。

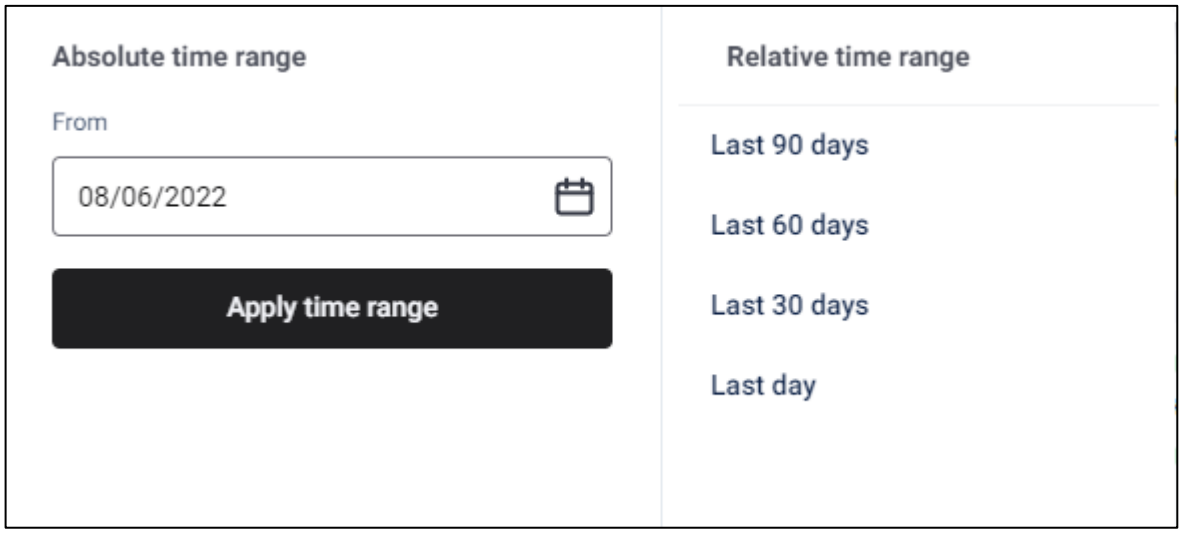
+ ダッシュボードのすべてのコンポーネントで接続エラーまたはデータがない場合、抽出や操作はサポートされず、操作は非表示になります。

+ データがある場合、.xlsx形式のファイル出力をサポートします。

日付で検索する

現在までの情報セキュリティ状況を監視する期間を調整できるようにし、デフォルトでは前日からの期間を設定します。

+ 監視する期間の開始時点を選択するには、絶対時間または相対時間を選択できます。



- 絶対時間：特定の開始日を示す値であり、現在から最大90日間までサポートします。

例：現在は2021年6月7日午前3時で、開始日を「2021年6月6日」に設定しています。

監視期間：2021年6月6日00:00から2021年7月6日03:00まで。

- 相対時間：開始日と現在の間の相対的な時間のことです。

例：現在は2021年6月7日午前3時で、開始日を「過去30日間」に設定しています。システムは自動的に30日前の日付を遡り、その日の00:00から計算を開始します。

監視期間：2021年5月8日00:00から2021年6月7日03:00まで。

+ 監視したい期間を選択した後、対応するデータを再読み込みしてください。

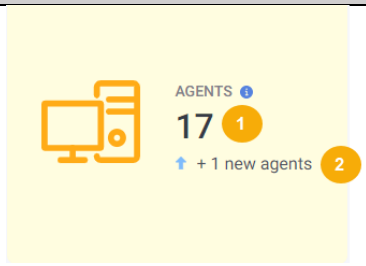
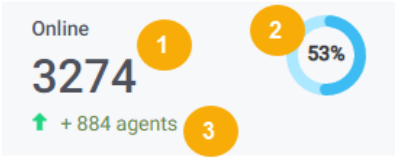
データを更新する

目的：手動でデータを更新できるようにし、現在時点までの最新データに更新するために選択します。

3.2.2 統計概要

目的：検索部分で選択した期間における組織の情報セキュリティ状況を迅速に集計できるようにすること。

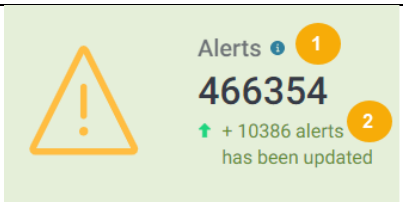
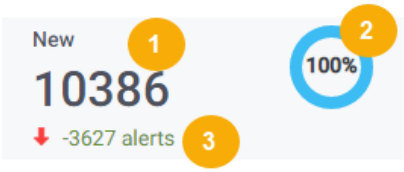
+ エージェントに関する統計：

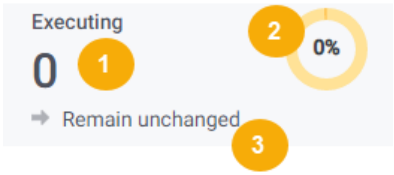
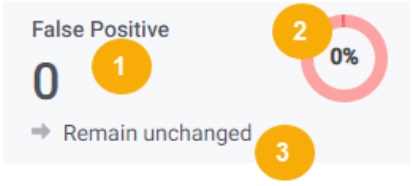
統計数	意味
	以下の2つの指標を含みます： ・システム上にエージェントがインストールされている総台数（検索期間に関係なく）； ・検索期間内に新たにエージェントがインストールされた台数； （+: 新規インストールされた端末、Remain unchanged: 検索期間内に新規インストールはなし）
	以下の3つの指標を含みます： 検索期間中の平均オンライン台数（営業時間の08:00～18:00のみを対象とします）； システム全体に対する平均オンライン率； 前周期と比較した平均オンライン台数の差異。

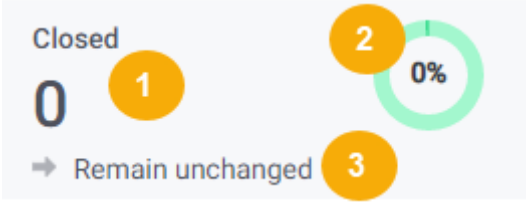
	（+: 前期間と比較して平均オンライン台数が増加、Remain unchanged: 差異なし）
	以下の3つの指標を含みます。 1. 検索期間中の平均オフライン台数（営業時間の08:00～18:00のみを対象とする）； 2. システム全体に対する平均オフライン率； 3. 前回サイクルと比較した平均オフライン台数の差異。 （+: 前期間と比べて平均オフライン台数が増加、Remain unchanged: 差異なし）
	以下の3つの指標を含みます： システム上にエージェントがインストールされている総台数（検索期間に関係なく）、未処理のアラートが発生しているかどうか； システム全体の台数に対するアラート発生台数の割合（検索期間に関係なく）； 検索期間内にアラートが発生した総台数。 （+: 新たにアラートが発生した機器、Remain unchanged: 検索期間内に新たなアラートが発生していない機器）

+ アラートに関する統計：

統計数	意味

	以下の2つの指標を含みます： システム全体のアラート総数（検索期間に依存しません）； 検索期間内に新たに発生または更新されたアラートの総数； （+: 新たに発生したアラート、Remain unchanged: 検索期間内に新たなアラートは発生していません）
	以下の3つの指標を含みます： 検索期間内に新たに発生または更新され、状態が「NEW」であるアラートの総数； 検索期間内に新たに発生または更新され、状態が「NEW」であるアラートの割合（検索期間内に新たに発生または更新された全アラートに対する比率）； 検索期間内に新たに発生または更新され、状態が「NEW」であるアラートの総数の前期間との増減差。 （+: 前期間と比較して新規アラート数が増加、Remain unchanged: 前期間と比較して新規アラート数に変化なし）

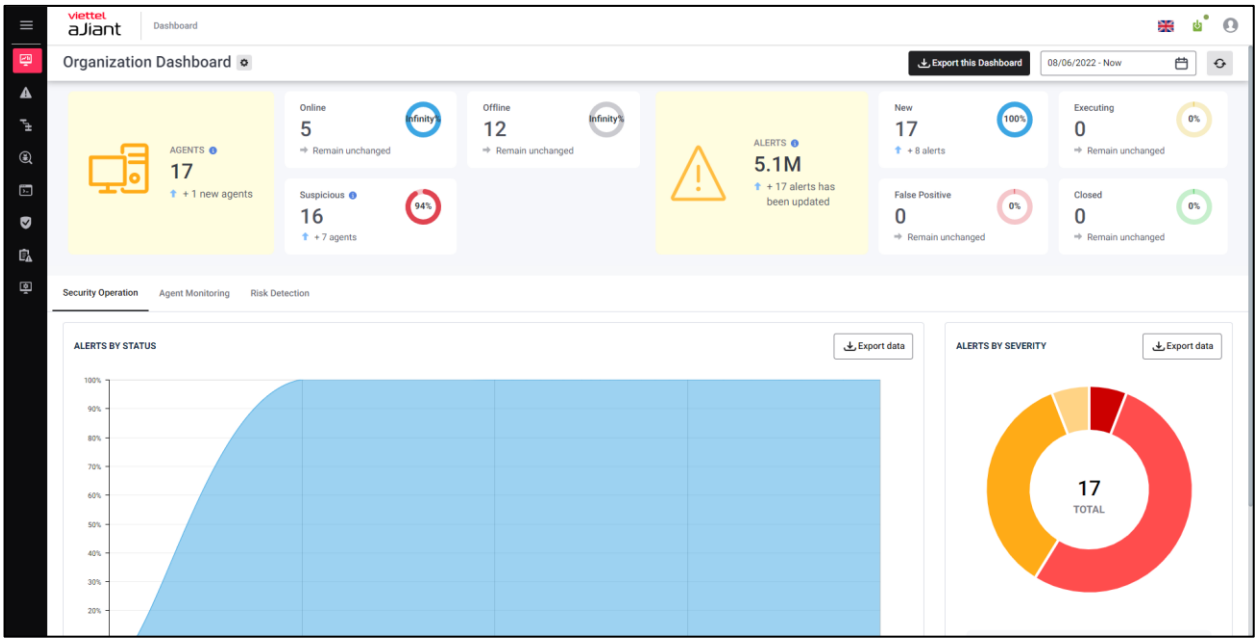
	以下の3つの指標を含みます： 検索期間内に新たに発生または更新され、かつ状態が<>（NEW、FALSE　POSITIVE、CLOSED）であるアラートの総数； 検索期間内に新たに発生または更新され、かつ状態が<>（NEW、FALSE　POSITIVE、CLOSED）であるアラートの割合（検索期間内に新たに発生または更新された全アラートに対する比率）； 検索期間内に新たに発生または更新され、かつ状態が<>（NEW、FALSE　POSITIVE、CLOSED）であるアラートの総数の前周期との差異。 （+:　　総アラート数が前期間より増加、Remain unchanged: 総アラート数が前期間と変わらない）
	以下の3つの指標を含みます： 検索期間内に新たに発生または更新され、状態が「CLOSED」であるアラートの総数； 検索期間内に新たに発生または更新され、状態が「CLOSED」であるアラートの割合（検索期間内に新たに発生または更新された全アラートに対する比率）； 検索期間内に新たに発生または更新され、状態が「CLOSED」であるアラートの総数の前周期との差異。

	（+: 総アラート数が前期間より増加、Remain unchanged: 総アラート数が前期間と変わらない）
	以下の3つの指標を含みます： 検索期間内に新たに発生または更新され、状態が「FALSE POSITIVE」であるアラートの総数； 検索期間内に新たに発生または更新され、状態が「FALSE POSITIVE」であるアラートの割合（全新規または更新アラートに対する比率）； 検索期間内に新たに発生または更新され、状態が「FALSE POSITIVE」であるアラートの総数の前期間との差異。 （+: 総アラート数が前期間より増加、Remain unchanged: 総アラート数が前期間と変わらない）

3.2.3 セキュリティオペレーションの監視

目的：選択した検索期間に基づいて、アラートの運用状況を監視することで、情報セキュリティの運用状況を追跡できるようにすること。

+ アラートの処理状況をステータス別に集計する。
+ 危険度別アラート統計；
+ グラフに対応するデータを抽出する。


viettel
aJiant
Dashboard
Organization Dashboard
Export this Dashboard
08/06/2022 - Now
AGENTS
17
+ 1 new agents
Online
5
Remain unchanged
Offline
12
Remain unchanged
Suspicious
16
+ 7 agents
94%
ALERTS
5.1M
+ 17 alerts has been updated
New
17
+ 8 alerts
100%
Executing
0
Remain unchanged
0%
False Positive
0
Remain unchanged
Closed
0
Remain unchanged
Security Operation
Agent Monitoring
Risk Detection
ALERTS BY STATUS
Export data
100%
90%
80%
70%
60%
50%
40%
30%
20%
ALERTS BY SEVERITY
Export data
17
TOTAL

グラフ／統計	意味
ステータスによるアラート	エリアチャート - 検索期間内に新たに記録された、または更新されたアラートの状況を追跡します。内容は以下の通りです： X軸：時間； Y軸：4つの状態グループ（新規、実行中、クローズ済み、誤検知）に分類されたアラートの割合； 状態別に並べ替えたアラート一覧のダウンロードが可能です。
重大度別アラート	円グラフ - 検索期間内に新たに記録された、または更新されたアラートの危険度別状況を追跡します。内容は以下の通りです： ・割合：各危険度レベルにおけるアラートの割合； ・グラフ中央には、期間内の新規または更新されたアラートの総数を表示； ・危険度順に並べ替えたアラート一覧のダウンロードが可能。

3.2.4 エージェントモニタリングの監視

目的：検索部分で選択した期間内におけるエージェントの状態およびオペレーティングシステム情報の統計を可能にすること。

+ エージェントの状態統計（オンライン、オフライン）；

+ エージェントの統計をOS別およびOSバージョン別に表示する。

+ エージェント情報のデータ抽出;

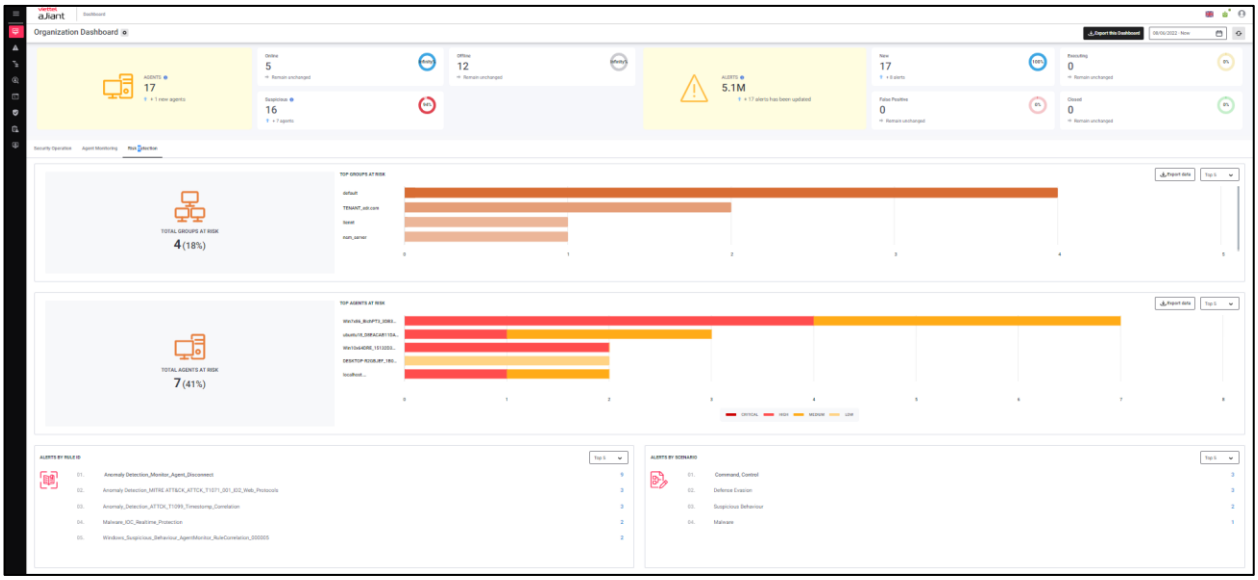
グラフ／統計	意味
ステータス別エージェント	エリアチャート - 現時点までの報告期間における機器の状態（オンライン／オフライン）別の記録状況を追跡します。内容は以下の通りです： 縦軸：状態別（オンライン、オフライン）に分類された機器の割合； 横軸：集計時間；

	オンラインになっていない機器の数を表示（機器が30日以上オンラインになっていない場合は、自動的に記録から除外されます）。
オペレーティングシステムによるエージェント	円グラフ - OS別の機器記録状況の追跡、内容は以下の通りです： 割合：各OSごとの機器の割合； 注釈欄には以下のOSリストを記載：Windows、MacOS、Linux、その他のOS； OS情報に基づいて並べ替えた機器リストのダウンロードが可能。
OSバージョン別エージェント	インストールされているオペレーティングシステムのバージョン別トップ統計を表示します。 統計範囲の変更を許可します：トップ5、トップ10、トップ20、トップ50。デフォルトはトップ5に設定されています。

3.2.5 リスク検出の監視

組織に対するリスクの監視を可能にする（システム内で未処理のアラートが最も多く発生している対象を統計的に把握することを通じて）：

+ アラート発生数が最も多いグループのトップ統計。
+ 最も多くのアラートを発生させたトップエージェントの統計;
+ 最も多くのbsaoシーンを発生させた上位のruleidとシナリオの統計。
+ 有害対象別の情報データ抽出；


Organization Dashboard
Export this Dashboard
AGENTS
17
Online
5
Offline
12
Suspicious
16
ALERTS
5.1M
New
17
Executing
0
False Positive
0
Closed
0
Security Operation
Agent Monitoring
Risk Detection
TOTAL GROUPS AT RISK
4 (18%)
TOP GROUPS AT RISK
default
TENANT_edr.com
tiavat
num_server
Export data
TOTAL AGENTS AT RISK
7 (41%)
TOP AGENTS AT RISK
CRITICAL
HIGH
MEDIUM
LOW
ALERTS BY RULE ID
01. Anomaly Detection_Monitor_Agent_Disconnect 9
02. Anomaly Detection_MITRE ATT&CK_ATTCK_T1071_001_IDS_Web_Protocols 3
03. Anomaly_Detection_ATTCK_T1099_Timestomp_Correlation 3
04. Malware_IOC_RealTime_Protection 2
05. Windows_Suspicious_Behaviour_AgentMonitor_RuleCorrelation_000005 2
ALERTS BY SCENARIO
01. Command_Control 3
02. Defense Evasion 3
03. Suspicious Behaviour 2
04. Malware 1

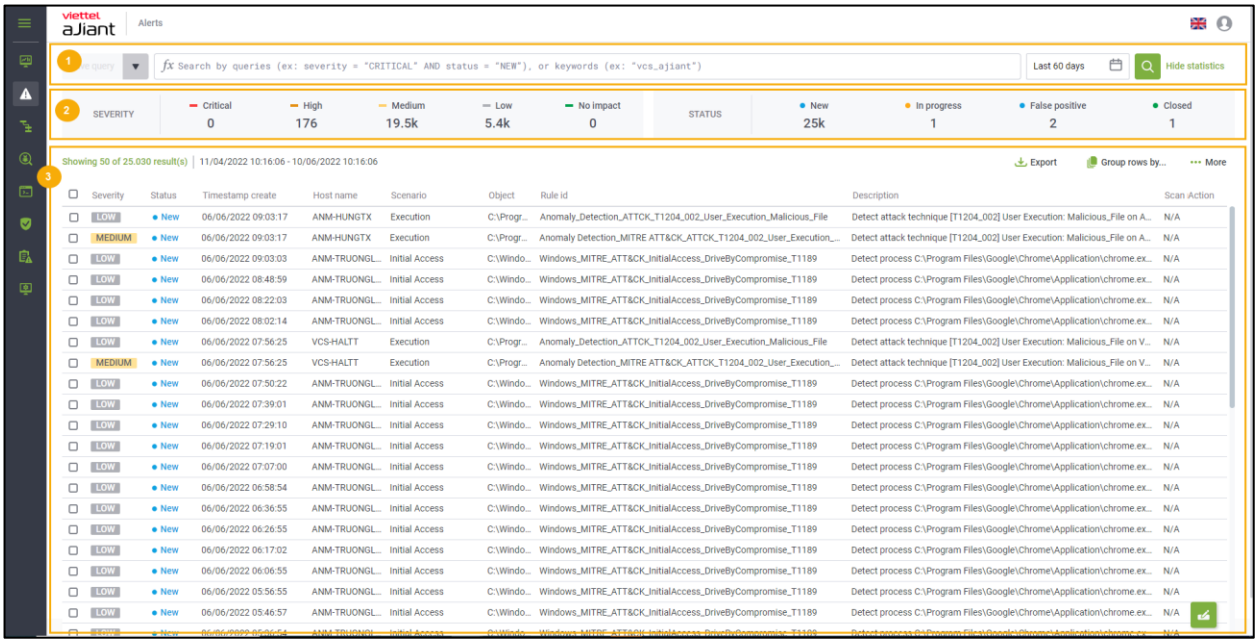
グラフ／統計	意味
リスクのある総グループ数	検索期間中に新たに記録された、または更新されたコンピュータを含むグループの総数（誤検知およびクローズ済みのアラート、削除されたグループは除く）； システム上の全グループに対する疑わしいグループの割合（削除されたグループは除く）。
リスクが高い主要グループ	**棒グラフ – 新たに記録された、または更新されたアラートが最も多く発生したコンピューターを含む上位グループの統計（誤検知およびクローズ済みのアラート、削除されたグループは除く）を検索期間内に表示；** **X軸：各グループでアラートが多く発生したコンピューターの数；** **Y軸：対応するグループ名；** **統計範囲の変更を許可：トップ5、トップ10、トップ20、トップ50。デフォルトはトップ5を選択；** **アラートが発生したコンピューターグループのリストをダウンロード可能。**
リスクにさらされている総エージェント数	検索期間中に新たに記録された、または更新されたアラートを発生させたコンピュータの総数（誤検知およびクローズ済みのアラート、直近30日間以上稼働していないコンピュータ

	を除く）； システム全体のコンピュータ数に対する疑わしいコンピュータの割合（直近30日間以上稼働していないコンピュータを除く）。
リスクにさらされているトップエージェント	棒グラフ – 新規または更新されたアラートが最も多く発生した上位コンピュータの統計（誤検知およびクローズ済みアラートは除く）を検索期間内で表示； X軸：各ホストごとのアラート数を、重大度（Critical、High、Medium、Low）別に割合を明確に分けて表示 Y軸：対応するコンピュータ名； 統計範囲の変更を許可：Top 5、Top 10、Top 20、Top 50。デフォルトはTop 5を選択； アラート発生コンピュータのリストをダウンロード可能にする。
ルールIDによるアラート	検索期間内に新たに記録された、または更新されたアラートが最も多く発生した上位のルールIDを集計します。 集計範囲は変更可能で、Top 5、Top 10、Top 15、Top 20から選択できます。デフォルトはTop 5です。
シナリオ別アラート	報告期間内で新たに発生または更新されたアラートが最も多いシナリオの上位統計：統計範囲の変更を許可（上

	位5件、上位10件、上位15件、上位20件）。デフォルトは上位5件に設定。

3.3 アラート管理

主な機能は以下の通りです：



1 – クエリと時間によるデータ検索：

+ クエリ文によるデータ検索および保存されたクエリ文の使用；

+ 時間によるデータ検索。

1 – クイック検索

2 – アラートの一覧とアラートに対する操作：

+ アラート一覧を見る;

+ アラートをグループ化する;

+ アラートの概要を見る;

+ アラート詳細を表示する 01;

+ 調査グラフを見る;

+ 1つまたは複数のアラートに対して誤検知としてマークする（False Positiveを設定する）。

機能におけるデータの権限分割は以下の通りです：

+ ユーザーがrootグループに属している場合：システム内のすべてのアラートを表示する。

+ ユーザーがデフォルトグループにログインしている場合：デフォルトグループに属するすべてのアラートを表示する。

+ ユーザーが親グループにログインしている場合：ログイン中のユーザーのグループおよび対応する子グループに属するすべてのアラートを表示する。

+ ユーザーが一つまたは複数のグループに所属している場合：ログインしているユーザーのグループに属するすべてのアラートを表示する。

3.3.1 アラート検索

目的：アラート発生時間に基づいてアラートを検索するために、クエリ文の作成、保存されたクエリ文の使用、またはクイック検索を可能にする。

時間で検索する

システムにアクセスした際、デフォルトで過去7日間のアラートを検索します。

目的：絶対時間または相対時間を選択して時間の値を変更できるようにすること。

+ 絶対時間：開始時間と終了時間の具体的な値であり、入力またはカレンダーからの選択が可能で、日/月/年 時:分:秒の形式をサポートします。

+ 相対時間：開始時間と現在時間の間の相対的な時間のこと。

例：現在は2021年6月7日午前3時で、開始日を「過去30日間」に設定しています。システムは自動的に30日前の日付を遡り、その日の午前3時から計算を開始します。

監視期間：2021年5月8日03:00から2021年6月7日03:00まで。

クイック検索

目的：以下の項目によるアラートの迅速な検索を支援すること。

+ 時間：アラート発生時刻；

+ ステータス：アラートの状態；

+ 重大度：アラートの危険度;

+ シナリオ：アラートを生成するシナリオ；

+ 担当者：アラート処理を割り当てられた者；

クエリによる検索

1 – 以前に保存したクエリを使用して検索します。

2 – 検索クエリを入力してください。

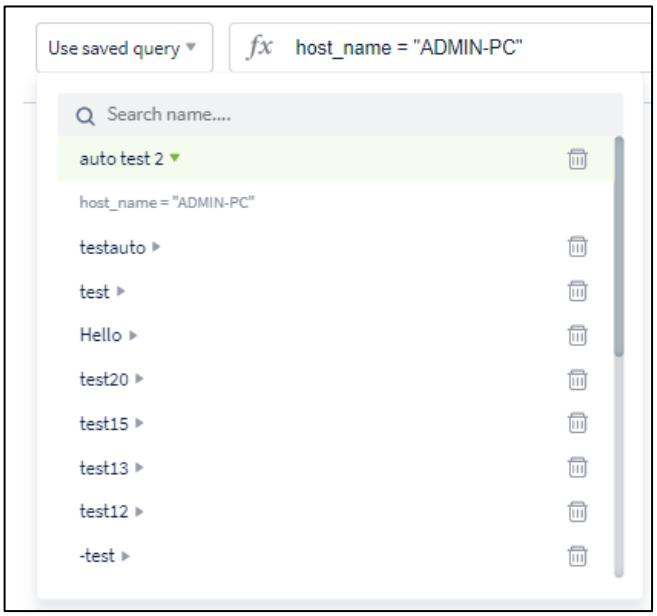
(*) 以前に保存したクエリを使用して検索する

- コンボボックスで以前に保存したクエリを選択してください。

- セミコロン（；）を選択して、クエリの内容を確認してください。

- 古いクエリを削除したい場合は、削除したいレコードにカーソルを合わせて選択してください。

- クエリに使用したいレコードをクリックすると、古いクエリ内容がクエリ入力欄に表示されます。



➔ クエリの内容を新規追加または編集したい場合は、クエリ入力欄で直接更新し、保存を選択してください。

注意：ボタンはクエリ文が正しい構造の場合にのみ表示されます。

(*) 検索クエリを入力してください：

- 検索ボックスに以下の形式でクエリを入力してください：

＜フィールド名＞ ＜演算子＞ “＜値＞” AND/OR ＜フィールド名＞ ＜演算子＞ “＜値＞”…..

その中で：

+ ＜学校名＞は以下の値です：

  - severity: アラートの重大度
  - Alert_id: アラートコード
  - ステータス：アラートの状態
  - グループ：アラート発生イベントのグループ
  - ホスト名：ワークステーションの名前
  - シナリオ：MITRE ATT&CKに基づくアラート生成のシナリオ
  - 担当者：アラートの処理を割り当てられた者
  - signature_id: アラート発生イベントコード
  - rule_id: アラート発生の法典コード
  - 説明：アラート発生の状況情報の説明

+ <演算子> は次の値です：

  - = ：正確な値を value として検索する
  - != ：valueと異なる値を探すこと

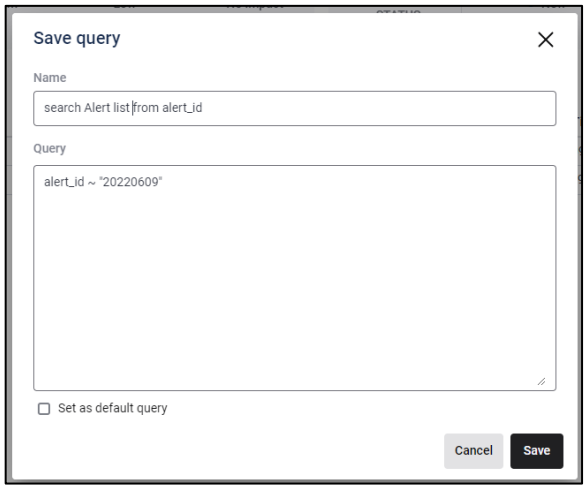
- ~: valueとlikeの値を検索する
- AND/OR：2つのクエリ文を組み合わせるための結合演算子。

- 「検索」ボタンをクリックしてください。

+ 適切な結果がない場合、システムは「データなし」というメッセージを表示します。

+ 適合する結果がある場合、システムはデフォルトで時間の降順に50件のレコードを表示します。より多くのレコードを表示するには、ページの下部までスクロールすると、システムが次の50件のレコードを読み込みます。

+ クエリが正しい構造で、今後も使用するために保存したい場合は、クエリの識別名を選択して入力してください。

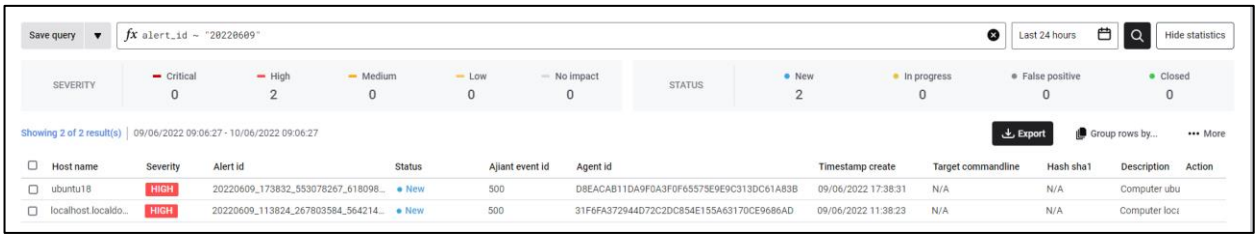


注意：ボタンはクエリ文が正しい構造の場合にのみ表示されます。

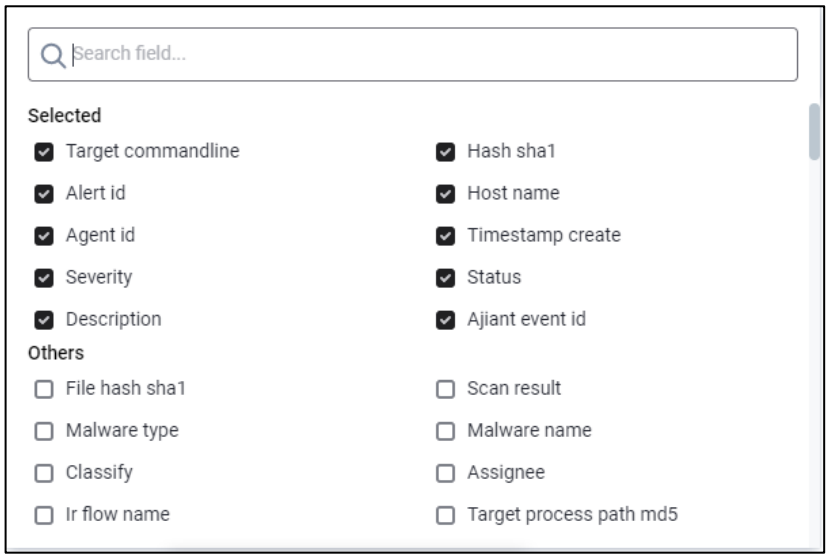
3.3.2 アラート一覧

目的：システム内のアラート一覧を表示すること。

検索条件に合致するアラートの一覧表示を許可する



- アラート一覧に表示する項目を選択してください：



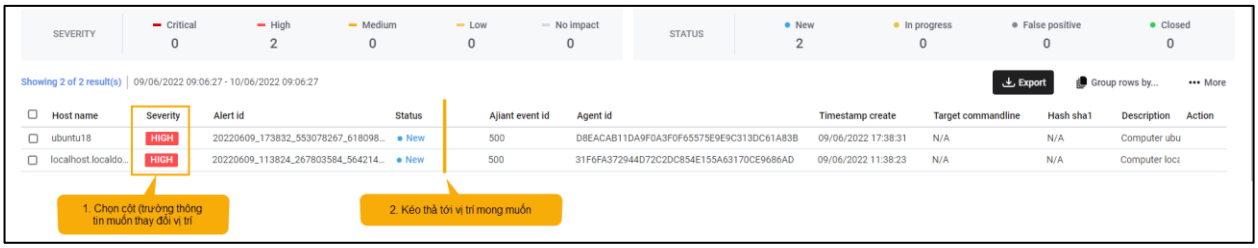
ここでは、フィールド名で情報フィールドを検索でき、すべてのフィールドを選択または選択解除することができます。

- サポートされている操作は以下の通りです：

  + 各列のデータに基づいて並べ替え：

例：作成日時のフィールドでデータを並べ替えるには、フィールド名を一度クリックすると作成日時の昇順で並べ替えられ、二度クリックすると作成日時の降順で並べ替えられ、三度クリックすると並べ替えが解除され、元の状態に戻ります。

  + 情報フィールドを希望の位置にドラッグ＆ドロップしてください。

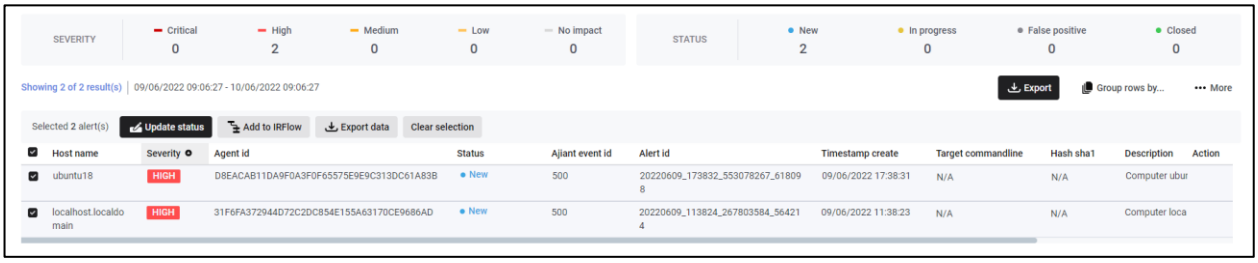


+ 詳細情報を見るには1回クリックするか、を選択して「View detail」を選んでください。詳細は3.3.4アラートの詳細表示をご参照ください。

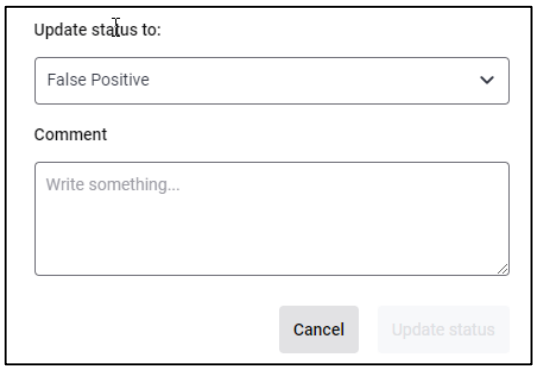
+ アラートのステータスを更新するには、「Update status」を選択し、「False Positive」または「Close」にステータスを更新します。アラートを1件選択した場合を参照してください。

+ 「FALSE POSITIVE」状態にあるアラートで危険なしとマークされた理由を見るには、を選択してください。

- レコードの操作が完了した後、各アラートの先頭をクリックして1つまたは複数のレコードを選択し、以下の操作を続行できます。



- アラートの状態を更新するには、 を選択してください。



- アラートが危険でないことを示すために、「ステータスを誤検知に更新」を選択してください。

- アラートを閉じるには、ステータスを「クローズ」に更新してください。

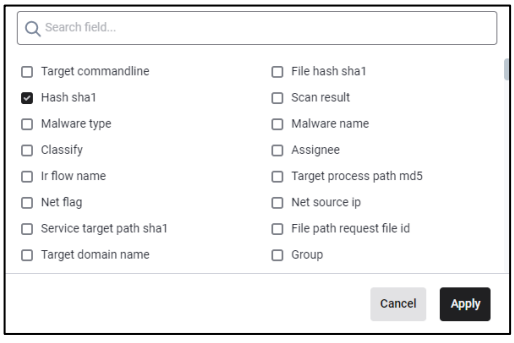
注意：この操作は、選択されたすべてのアラートが「NEW」状態の場合にのみ適用されます。もし少なくとも1つのアラートが「NEW」以外の状態であれば、操作は非表示になります。詳細は、3.3.5節「1つまたは複数のアラートまたはアラートグループの危険なしマーク」の「1つのアラートを危険なしにマークする場合」をご参照ください。

+ 選択されているアラートを抽出するには、を選択してください。

3.3.3 アラートのグループ化

目的：ホスト名、シナリオ、グループ、ルールIDのいずれかまたは複数の基準でアラートをグループ化できるようにすること。

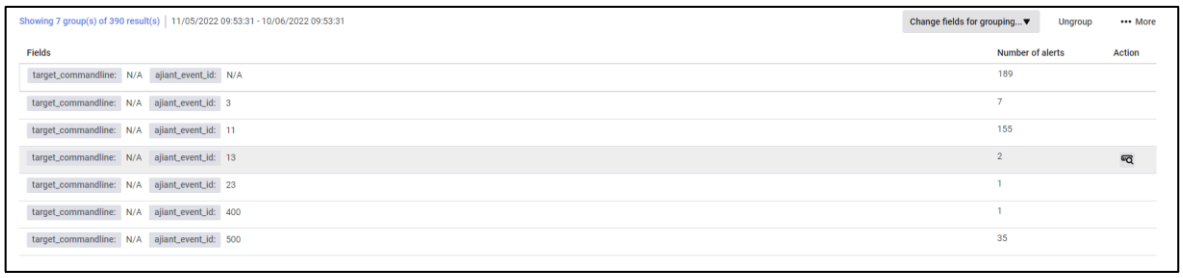
- **検索後、アラートをグループ化でき、グループ化に使用する基準を選択して指定します。**



基準名による検索サポートおよび1つまたは複数の基準を選択してグループ化する機能。

- **適用するには選択してください。**

選択された同じ基準および同じ状態を持つアラートは、結果リストで1行にまとめられます。

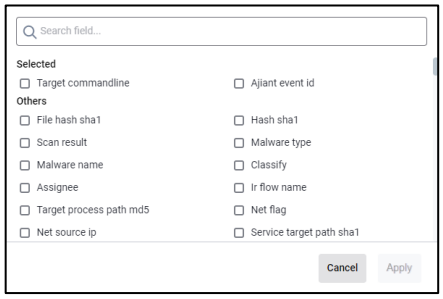


その中で：

+ グループ化の基準として使用されるフィールドは太字で表示されます。

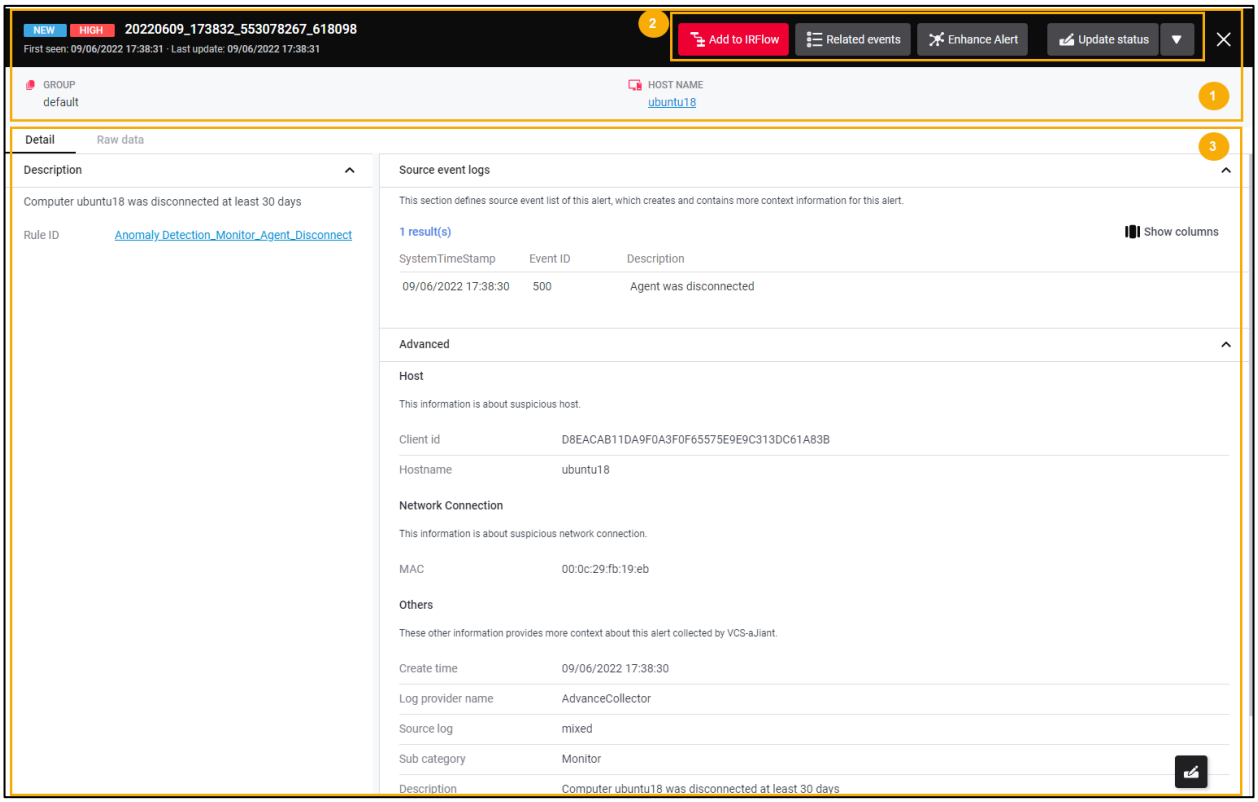
+ 選択した基準でグループ化されたアラートの数を表示します。

- グループ化を解除するには、同様に操作しますが、基準を選択せずに「適用」を選んでください。



3.3.4 アラートの詳細を見る

目的：アラートの詳細情報の閲覧を可能にし、発生したアラートに関連するイベント情報を自動収集することで情報の多様化を支援し、アラート内の対象間の関係を迅速に把握できる視覚的なグラフを提供すること。



1 – アラートの一般情報グループ、内訳は以下の通りです：

2 –

+ ステータス：アラートの状態を表示（新規、進行中、誤検知、クローズド）

+ 重大度：アラートを危険度（クリティカル、高、中、低）に分類すること；

+ Alert_id: アラートのID情報を表示する;

+ 初回確認日時：アラートが作成された時間;

+ 最終確認日時：アラートが最後に更新された時間；

3 – アラート操作グループ

+ アラートの状態を更新するには、を選択してください。

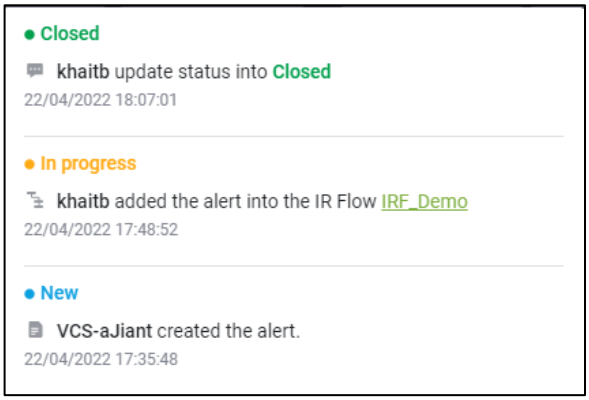
- アラートが危険でないことを示すために、ステータスを「誤検知（False Positive）」に更新してください。

- アラートを閉じるには、「ステータスを更新」から「クローズ」を選択してください。

注意：この操作はアラートが「NEW」状態に選択されている場合にのみ適用されます。操作は非表示になります。詳細は3.3.5「1つまたは複数のアラートまたはアラートグループの危険なしマーク」の「1つのアラートを危険なしとマークする場合」を参照してください。

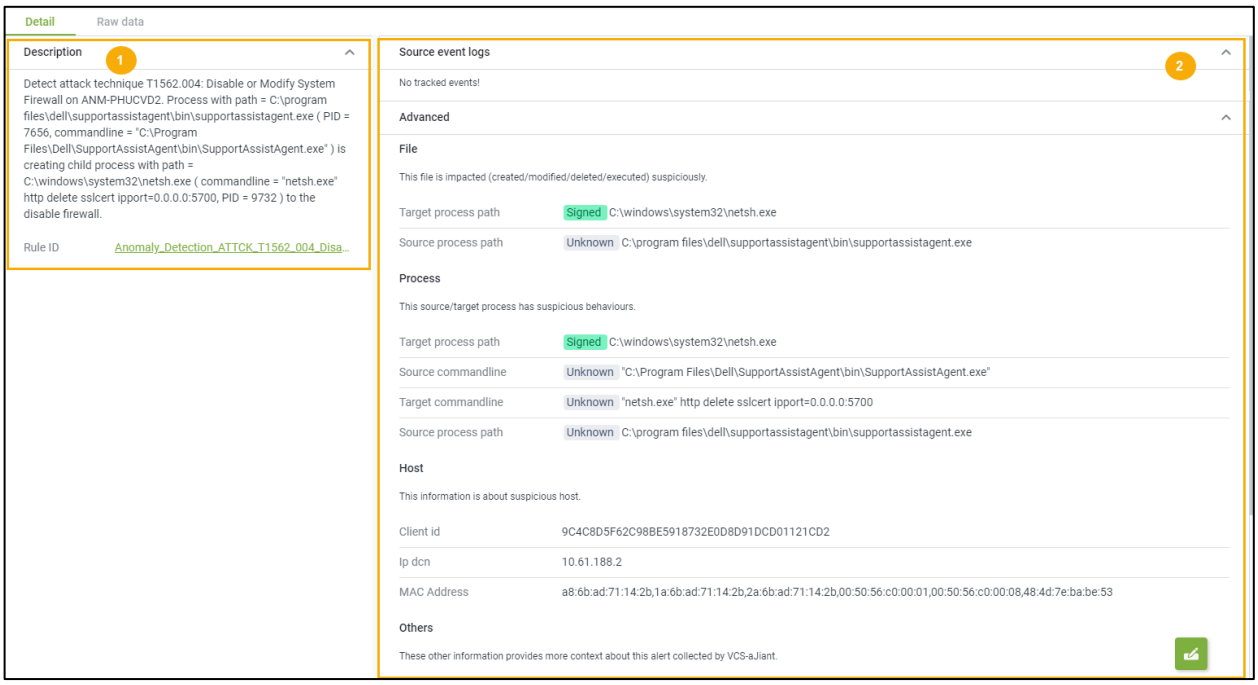
+ アラート発生時刻の前後4時間をデフォルト時間として、イベント検索機能に移動するために選択してください。

+ アラートに関連するログを表示するには、を選択してください。



4 – アラートに関連する情報のタブ：

+ タブ詳細：アラートに関連するすべての詳細情報の表示を許可する。

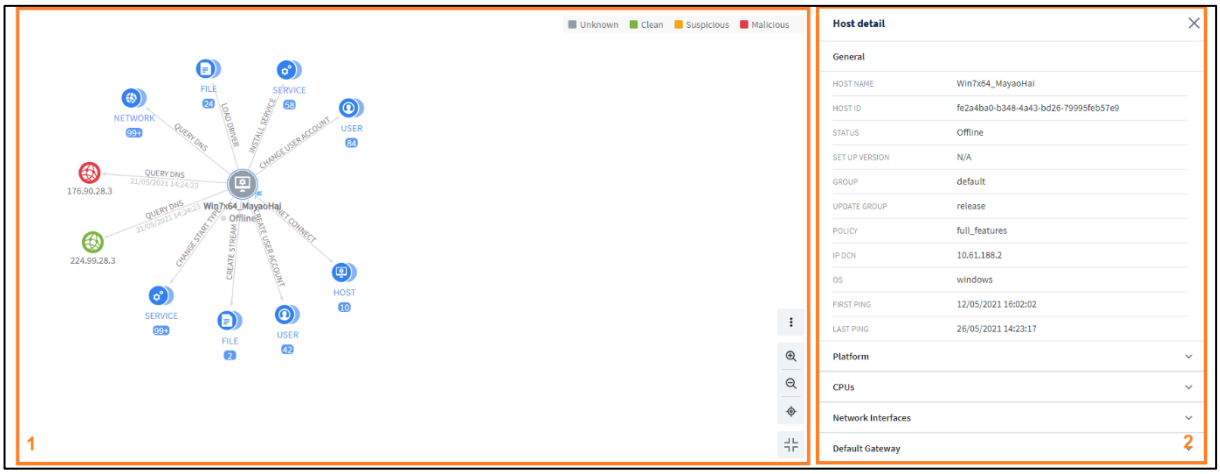


- 情報枠（1）説明：AlertおよびRuleIDの詳細説明情報の表示を可能にします。

- 情報枠（2）：
  - ソースイベントログ：アラートに関連するソースイベントログを記録する（ある場合）。
  - 詳細情報：アラートに関連する詳細情報には、ファイル、プロセス、ホスト、その他があります。

3.3.5 調査図（エンハンスアラート）

目的：アラート内のオブジェクト間の関係を表示し、各オブジェクトの詳細を確認できるようにし、システム内で収集されたイベント群に基づく拡散調査を支援すること。



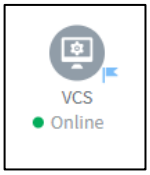
1 – グラフ表示エリアとグラフ操作

2 – グラフ上の各対象の詳細情報を表示するエリア

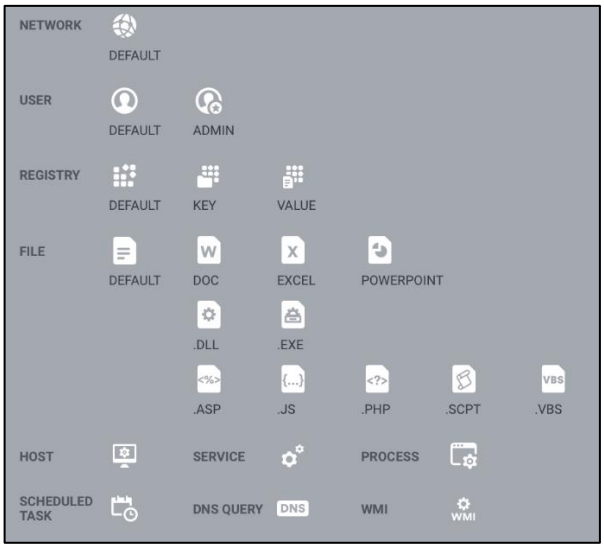
グラフ表示エリアおよびグラフ操作

アラート内のオブジェクトを視覚的に表示し、情報の確認および調査を可能にする。

デフォルトでは、アクセス直後にアラートを発生させた元の機器に関連する情報がグラフに表示されます。具体的には以下の通りです。



図表には常に1台の機器がフラグでマークされており、これはアラートを発生させた元の機器を示しています。各機器には、アラート発生時点から1日以内に元の機器と直接関係のある対象が常に付随しており、対象のリストは以下の通りです。



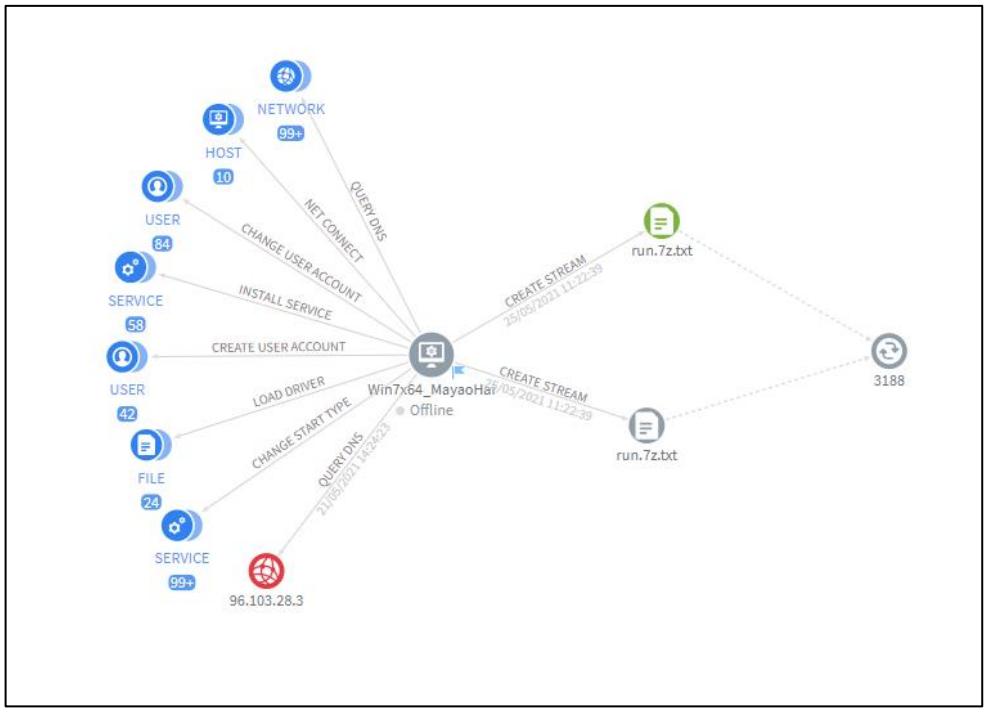
各オブジェクトは以下の状態を含みます：

オブジェクト間の関係を表示するには、以下を含みます：

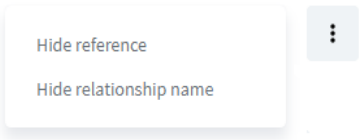
+ 関係：関係とは、アラート発生時点から1日以内に発生したイベントに基づいて定義されるものであり、その関係名は2つの対象を結ぶ矢印の上に表示されます。

+ 参照関係とは、主となるオブジェクトが発生するイベント内で他のオブジェクトが認識される関係を指し（破線で表され、特定の関係名は付されない）、示されます。

例：

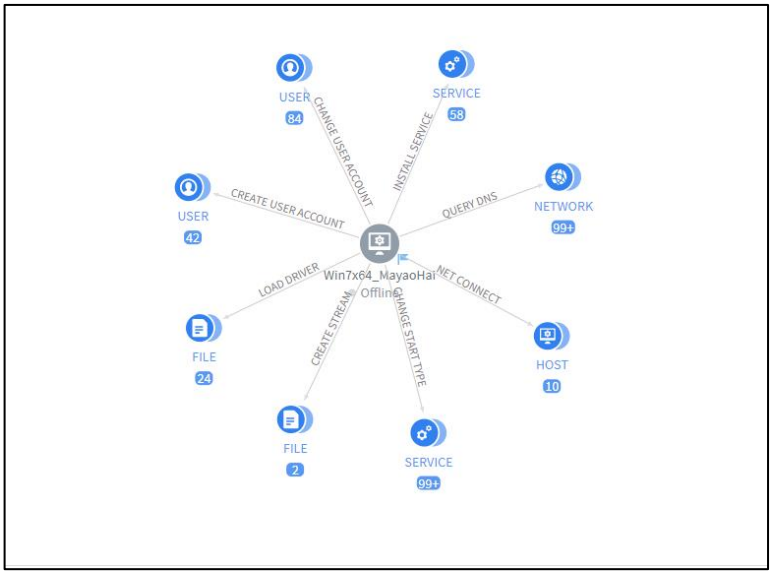


グラフ表示をサポートする操作には以下が含まれます：

表示サポート操作	意味
	グラフ上の情報の表示/非表示を許可する： 参照：選択すると、破線の矢印およびグラフ上のすべてのオブジェクトに存在する参照対象を含む参照情報の表示/非表示を許可します； 関係名：選択すると、グラフ上のすべての実線矢印の上に表示される関係名情報の表示/非表示を許可します。 + +

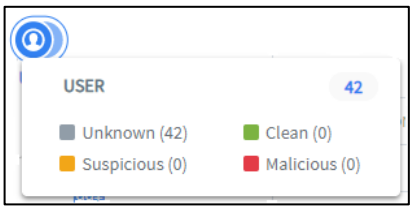
	カーソルが指している位置で対応するグラフのズームイン／ズームアウトを許可してください。また、ズームイン／ズームアウトしたい位置でマウスホイールを回転させて、迅速に操作できるようにしてください。
	チャートの中心位置（原点）に戻ることを許可する。
	チャートの表示と操作のために画面を最大限に拡張できるように許可する。

以下はデフォルトのグラフの例です。



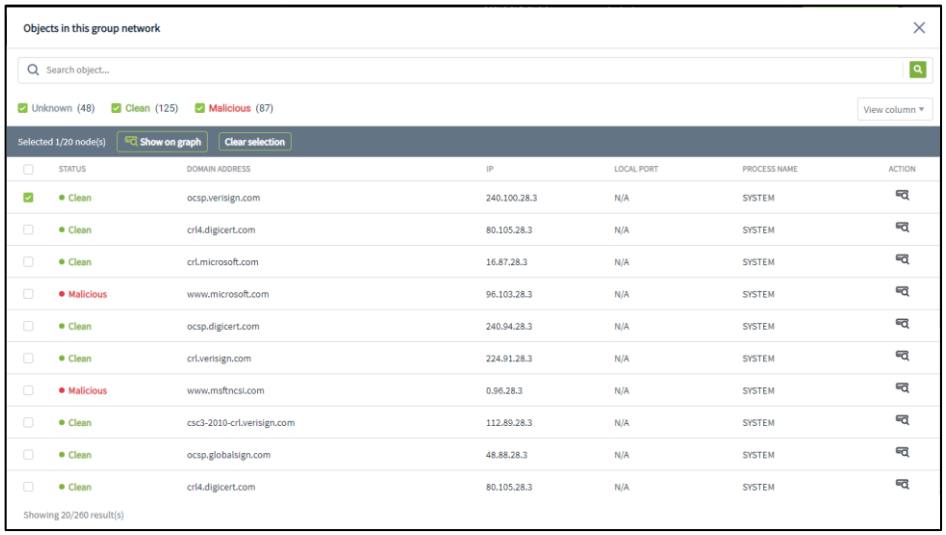
+ 各種類の対象に複数の従属対象がある場合、対象は自動的にグループ化されます。

+ 各対象グループの簡単な統計を見るには、ホバーしてください。



➔ ここから、対象者の調査をさらに進めるために、以下の手順を実施します。

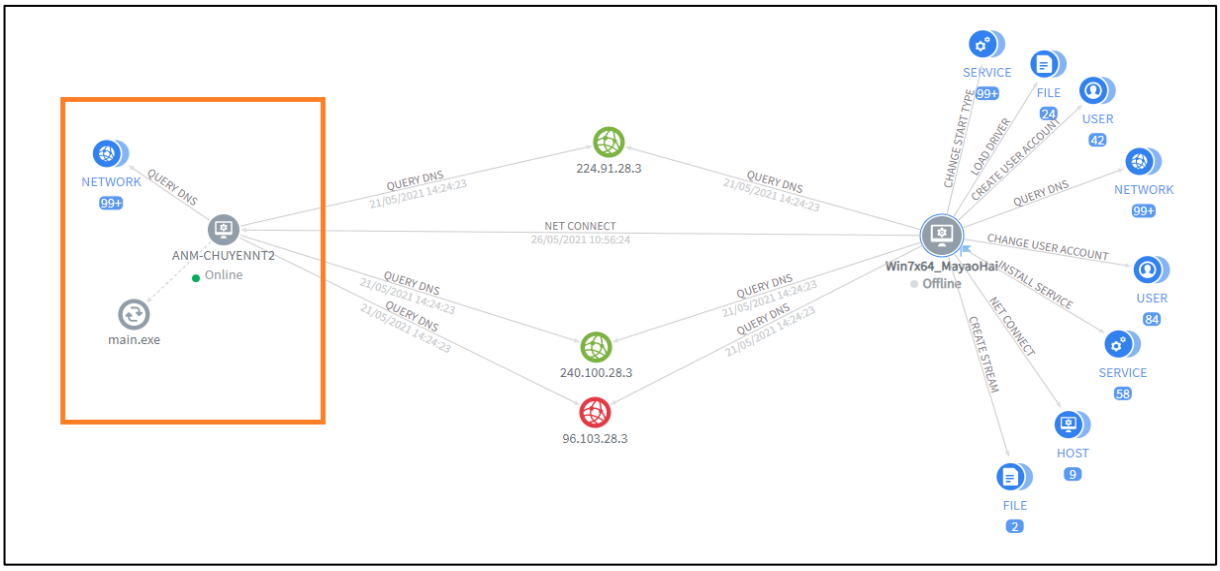
- 表示したい対象グループをクリックして選択すると、以下の画面が表示されます。



+ グループ内のオブジェクトを状態でフィルタリングしたり、すべてのフィールドに検索したいデータを入力して高速検索を行うことを許可します。

+ 適切な対象を選択したら、「01対象を表示」を選んで1つの対象をグラフに表示するか、「最大20対象を選択」を選んで最大20の対象をグラフに表示します。

注意：拡張対象がコンピュータの場合、対象を表示するとデフォルトで、アラート発生時点から1日以内にコンピュータに直接関連するオブジェクトも自動的に表示されます。



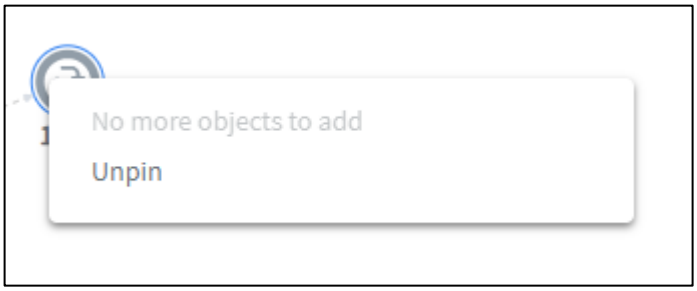
- 調査対象のオブジェクトをグラフに表示した後、拡大・縮小をサポートする操作には以下が含まれます：

+ 元の機械／通常のコンピュータにて：機械表示時にオブジェクトをデフォルト状態に折りたたむことをサポートします（機械と直接関係するオブジェクトのみを含み、同種のオブジェクトが複数ある場合はグループ表示）。対象のオブジェクトを右クリックし、「子レベルオブジェクトをグループ化」を選択してください。

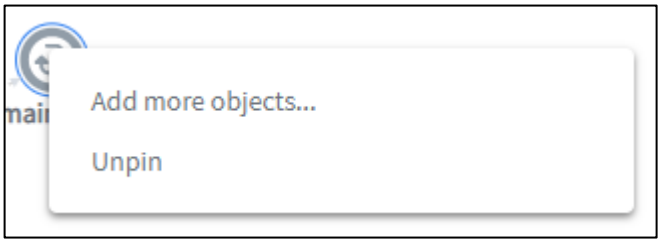
+ 他のオブジェクトの場合：オブジェクトを右クリックし、「同レベルのオブジェクトをグループ化」を選択することで、オブジェクトの種類および同じ階層のオブジェクトとの関係の種類ごとにまとめて折りたたむことができます。

+ 対象がプロセスの場合、対象を右クリックして拡張し、拡散調査を行うことができます。

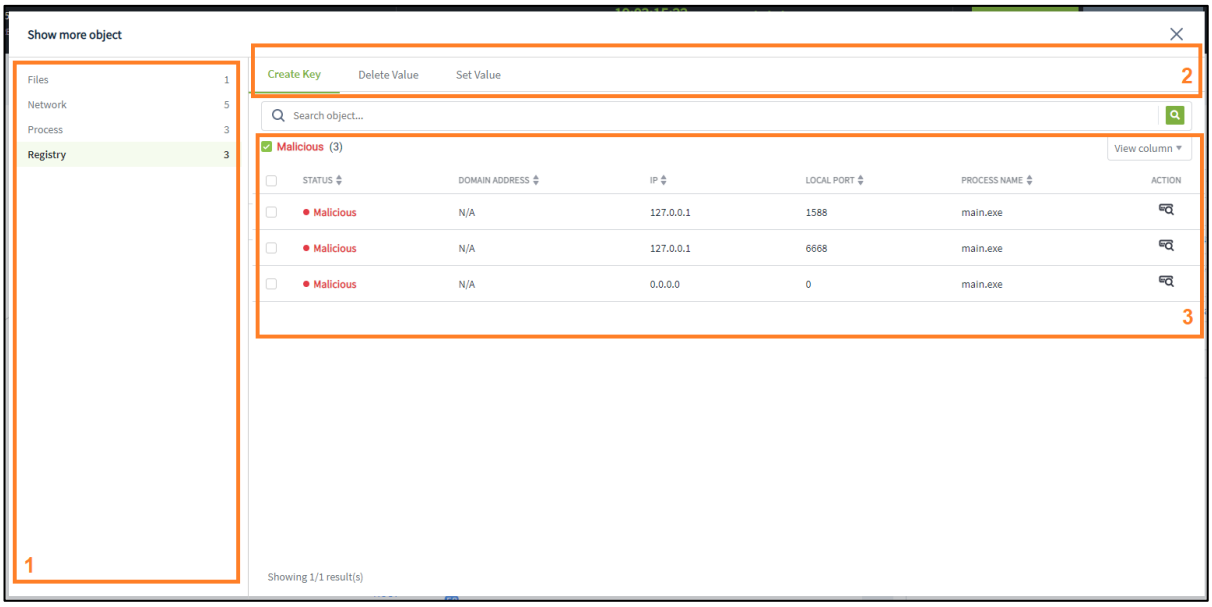
+ 拡散を続けられない場合は、以下を表示してください：



+ にじみが発生する場合は、「オブジェクトを追加…」を選択してください。



対象を選択してブラーを適用するインターフェースを表示する



1 – オブジェクトの種類を選択してください。

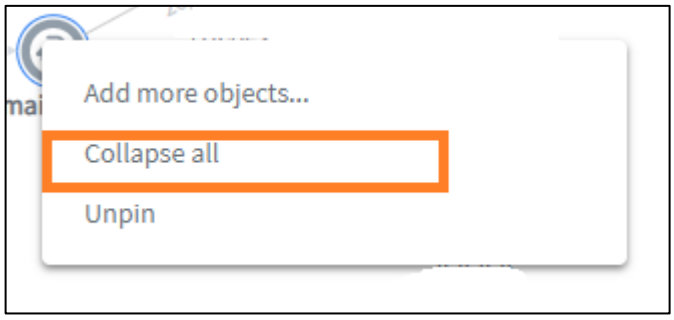
2 – プロセスから対象への関係の種類を選択してください。

3 – 表示したい対象を直接選択します。対象の状態（汚染/清浄）による検索や、対象の情報フィールドに含まれる内容による検索をサポートします。

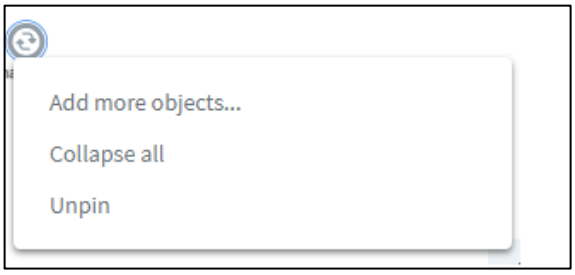
+ 表示する情報フィールドを選択するか、機能を使ってリスト内の情報を並べ替えてください。

+ 適切な対象を選択したら、グラフに1つの対象を表示するには「選択」を、最大20の対象をグラフに表示するには「複数選択」を選んでください。

+ 対象がプロセスの場合、展開されているオブジェクトを右クリックして折りたたむことができます。

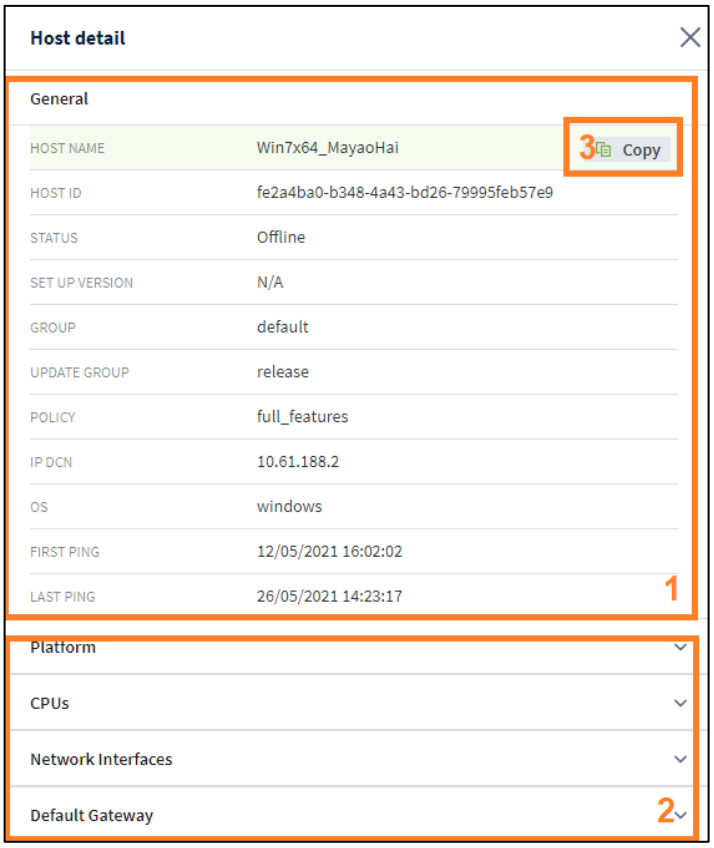


+ デフォルトでは、図表上のオブジェクトは自動的に移動し、互いに距離を保ちます。マウスでオブジェクトを選択してドラッグした場合、マウスを離すとオブジェクトは自動的に新しい位置に固定されます。固定を解除するには、を選択してください。



詳細情報表示エリア

これはチャートの追加機能であり、チャート内の要素（オブジェクトおよびチャート内の関係を含む）の詳細情報を表示することを可能にします。

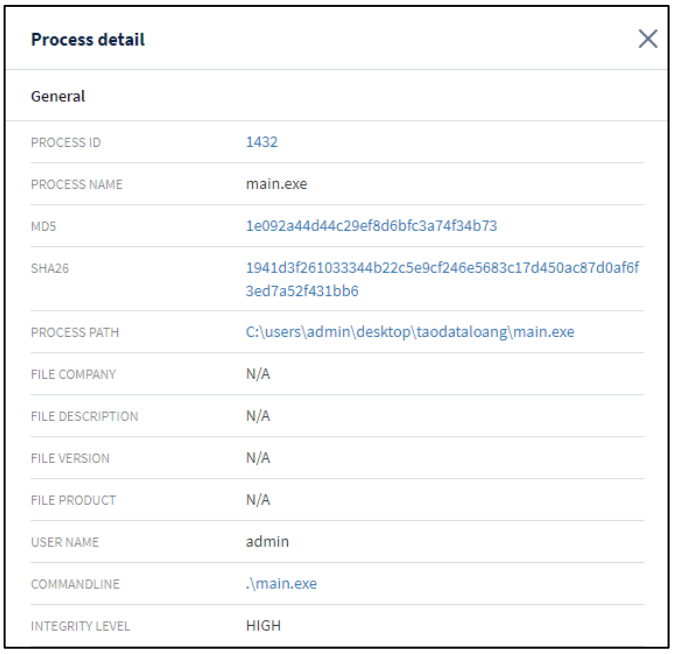


1 – 一般情報グループ：対象の一般情報／識別情報を含み、アクセス時に常に表示されます。

2 – 詳細情報グループ：対象の詳細情報を含み、異なる情報グループに分類されています。これらの情報グループはデフォルトで折りたたまれており、 を選択すると情報グループが展開され表示されます。

+ フィールド情報の内容コピー支援操作

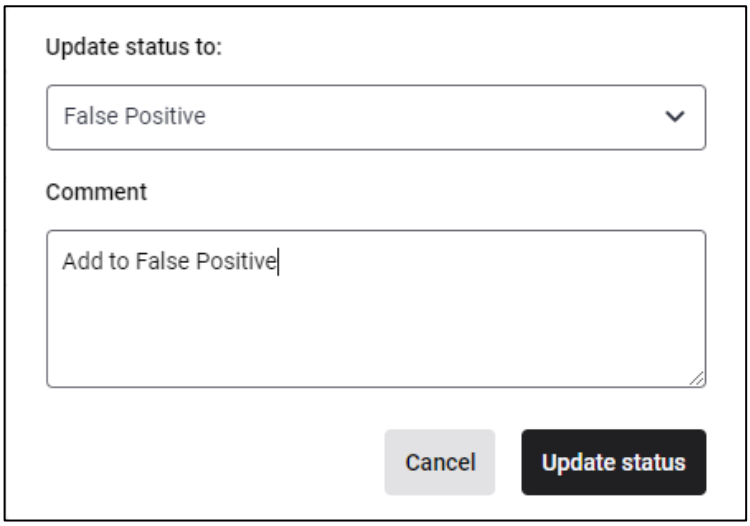
注意：一部の対象識別情報フィールドでは、イベント検索またはエージェント管理での迅速な参照のためのリンクが利用可能です。



3.3.6 1つまたは複数のアラート、またはアラートグループの状態を「危険なし」に更新するか、警告を閉じる。

目的：アラートを危険ではないとマークできるようにすること。

- 1つまたは複数のアラートを非危険としてマークする。
- アラートの状態を更新するには、を選択してください。

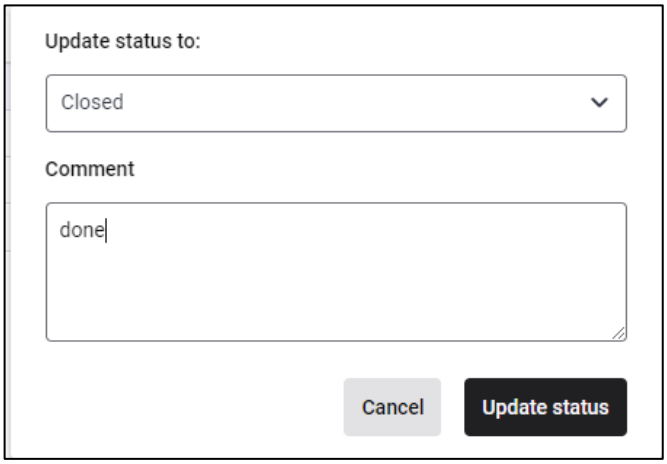


- ステータスを「誤検知」に更新してください。
- 危険なしとマークする理由を入力してください：
    - 「Update status」を選択して、アラートの危険なしを確認してください。
    - 「キャンセル」を選択して、アラートの「安全」とマークする操作を取り消してください

。

アラートを閉じるには、ステータスを「クローズ」に更新してください。

- 閉じたいアラートを1つまたは複数選択してください。
- アラートの状態を更新するには、を選択してください。



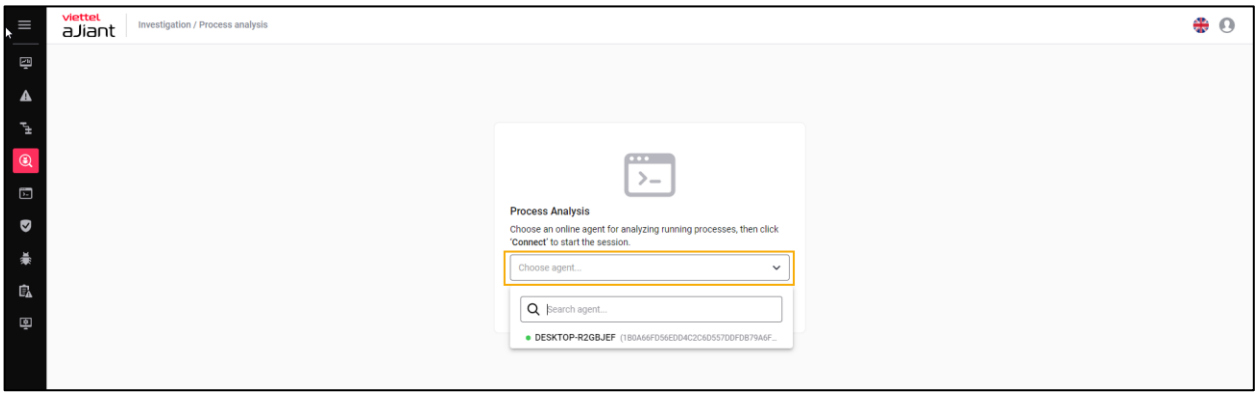
- ステータスを「クローズド」に更新してください。
- アラートを閉じる理由を入力してください：
    - 「ステータスを更新」を選択してアラートの終了を確認してください。
    - 「キャンセル」を選択して、アラートの閉じる操作を取り消してください。

3.4 調査画面

調査画面は、プロセス分析、イベント検索、ツール展開のいくつかの小さなタブで構成されています。

3.4.1 調査プロセス分析

- 目的：この機能は、ユーザーが自分の端末上のプロセスの接続を作成し、状態を確認できるようにするものです。具体的には：



ユーザーのデバイス一覧：

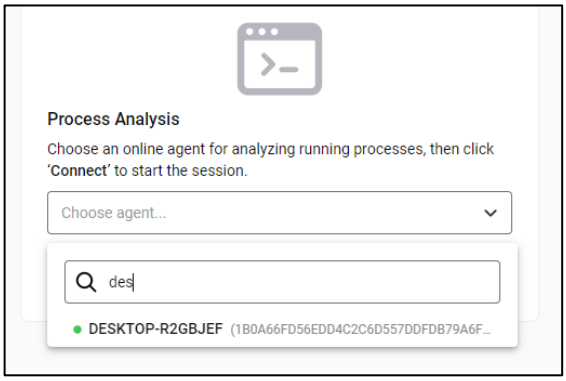
+ ユーザーがrootグループに属してログインした場合：システム内のアクティブなエージェントを30日未満で全て表示する。

+ ユーザーがデフォルトグループにログインしている場合：デフォルトグループに属するすべてのエージェントを表示する。

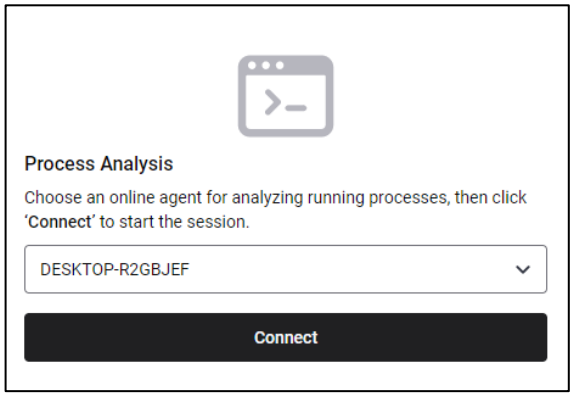
+ ユーザーが親グループにログインした場合：ログインしているユーザーのグループおよび対応する子グループに属するすべてのエージェントを表示する。

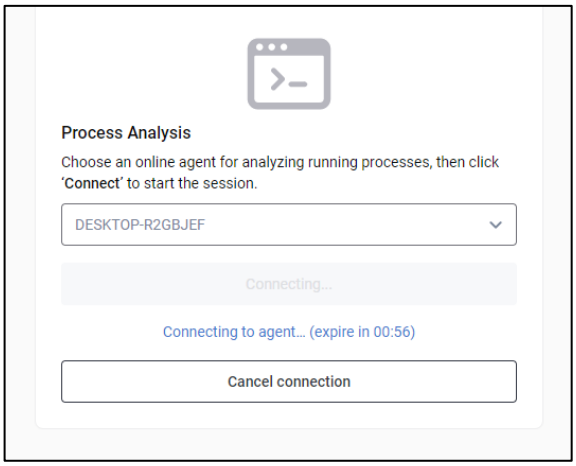
+ ユーザーが一つまたは複数のグループに所属している場合：ログインしているユーザーのグループに属するすべてのエージェントを表示する。

- エージェントを検索して選択する（接続を確実にするために、リストにはオンラインの端末のみが表示されます）。

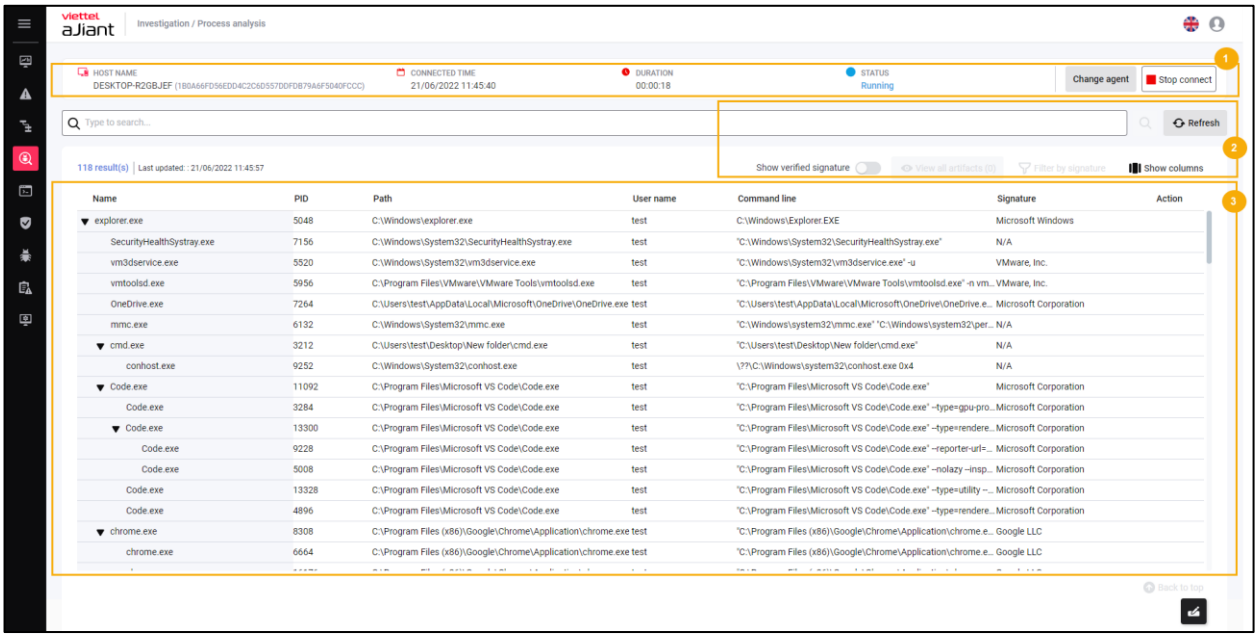


1台の機器を選択し、「接続」ボタンをクリックして接続を開始してください（接続には最大60秒かかる場合があります）。





- ユーザーのコンピュータで実行中のプロセス一覧を表示する



その中で、インターフェースは情報のグループに分かれています。

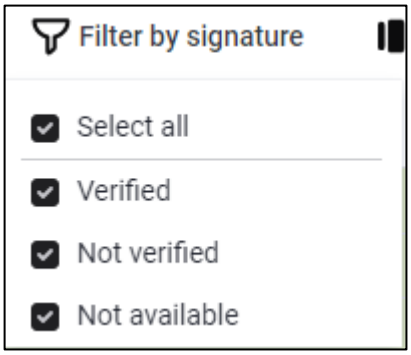
1 – 接続に関連する情報のグループには、接続中の機器、接続開始時間、現在までの接続時間、接続状態が含まれます。

2 – 検索・更新およびリスト内のデータフィルタリングを支援する情報グループには、以下の操作が含まれます：

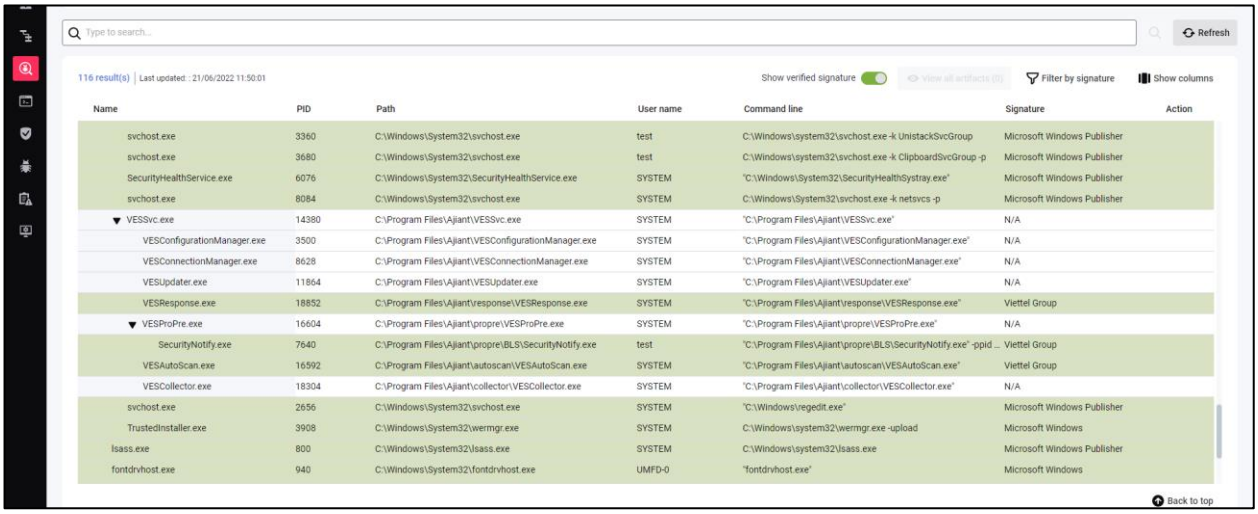
表示されているデータのすべてのフィールドに対してキーワード検索を許可する。

データの更新を許可する（現在使用中の検索条件およびフィルター条件は保持し、ユーザー端末から最新のデータのみを取得して表示する）。

: プロセスのデジタル署名情報の取得を有効または無効にすることができます。この設定を有効にした場合、デジタル署名に基づいてプロセスデータをフィルタリングすることが可能です。



電子署名の状態は、対応するレコードの色を規定します。

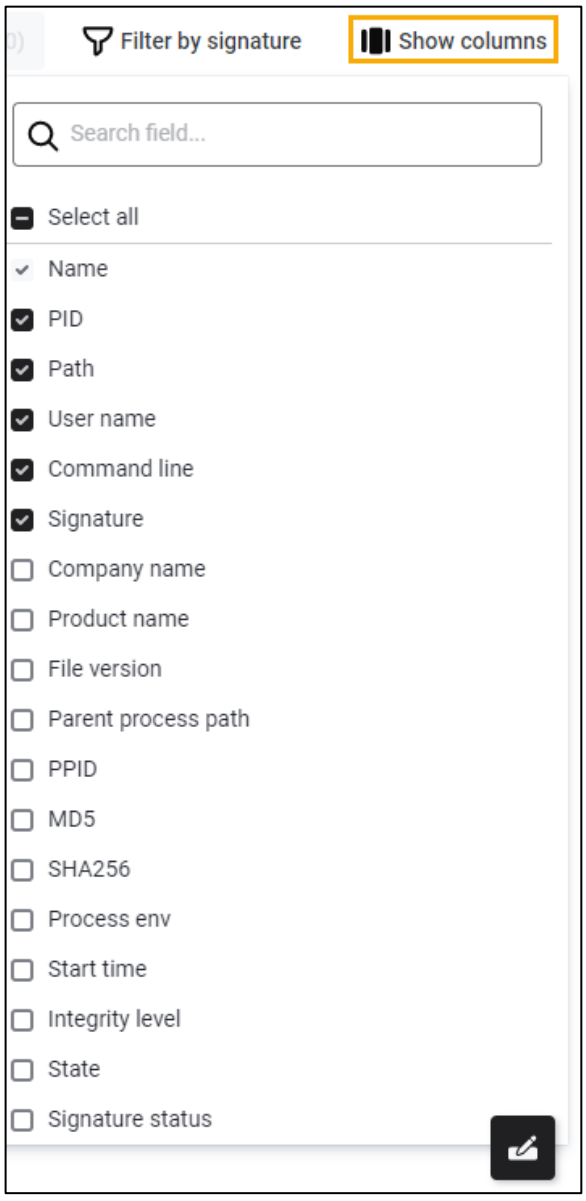


- 確認済み：青色 – 電子署名があり、有効期限内。
- 未確認：赤色 - 電子署名がないか、署名が期限切れです。

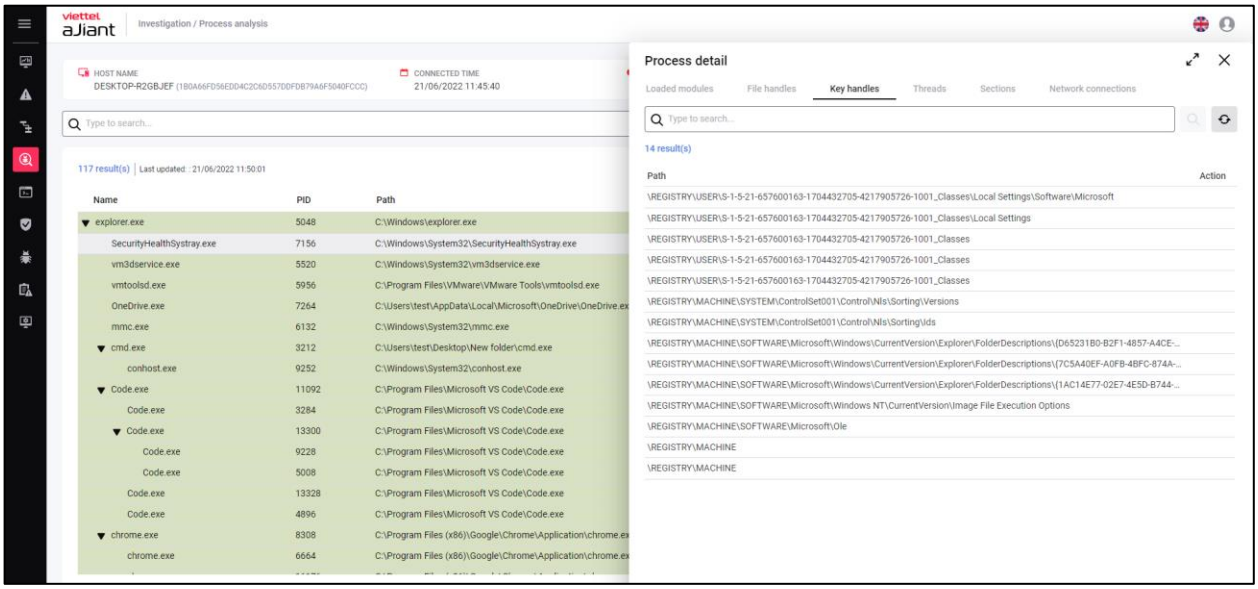
- 該当なし：白色 – 電子署名情報が見つかりません。

プロセス一覧の表示フィールドを調整できるようにします。

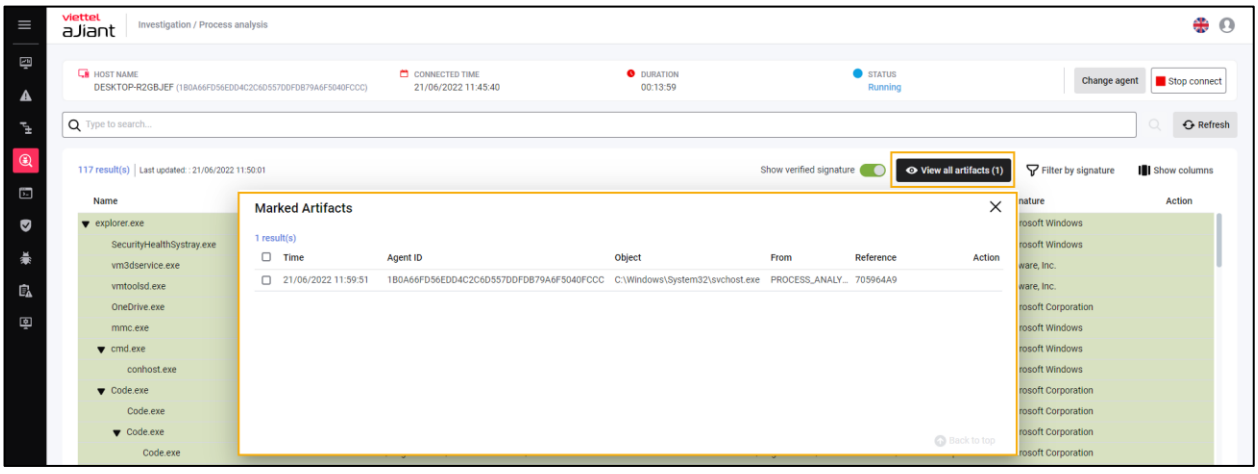
リストでは、「Name」フィールドが常に固定表示され、それ以外のフィールドは表示・非表示を選択できます。



3 – プロセス一覧は、ユーザーのコンピュータ上で現在のプロセスデータを表示し、「表示する列」セクションで選択された情報フィールドを含みます。各レコードをダブルクリックすると、プロセスの詳細を確認できます。



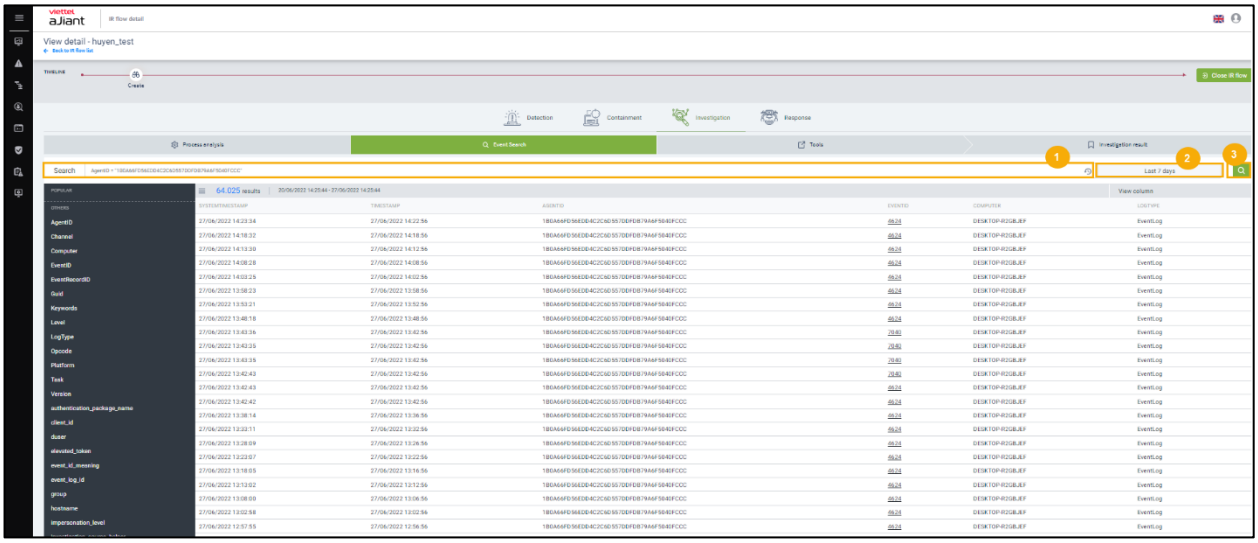
進捗の詳細はタブに分かれており、各タブには対応する情報の一覧が表示されます。



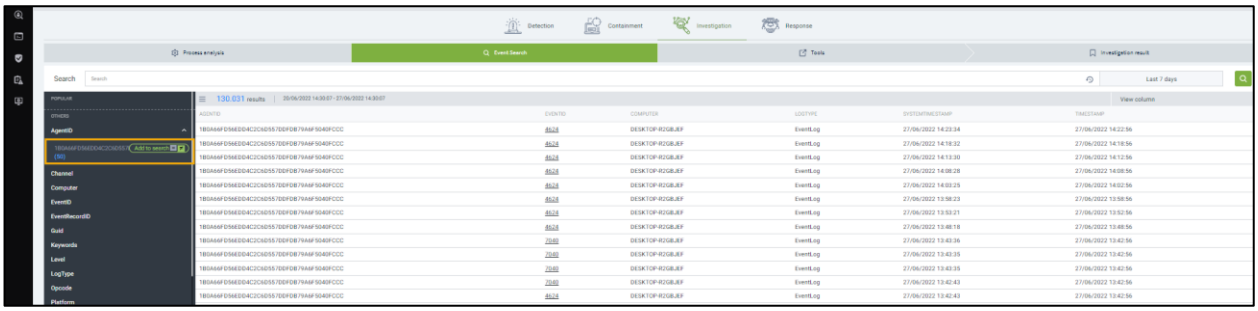
3.4.2 *調査イベント検索*

イベントを検索する

- クエリを入力 > 期間を選択 >「検索」ボタンをクリック：



- 「Add to search」で「Popular」と「Others」のフィールドを検索クエリに追加し、「=」または「#」のクエリを選択してください。



ハイライト

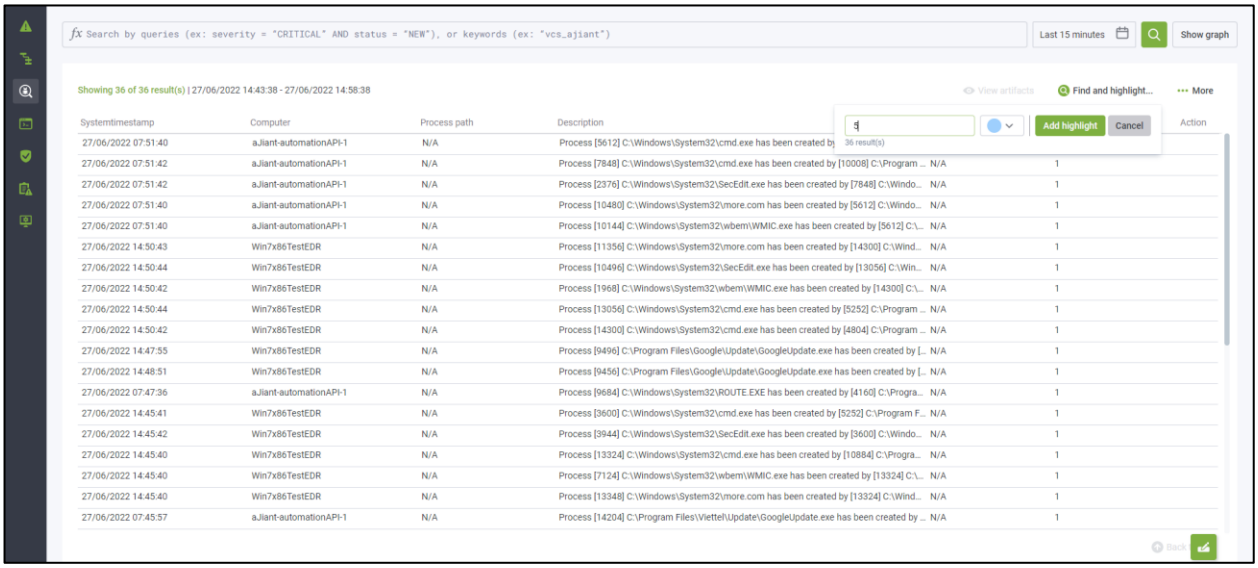
目的：同時に1つまたは複数のハイライトを追加して確認できるようにする（最大数の制限なし）。検索や並べ替えを実行すると、作成されたすべてのハイライトはクリアされる。

実施手順：

- NDは「Investigation」を選択し、「Event search」タブを選択します。
- 画面にイベント一覧を表示し、「検索して強調表示」ボタンを選択すると、システムは「テーブル内検索」ポップアップを表示します。
- マーカーキーワードを入力し、マーカーの色を選択して操作を確認してください。

「ハイライトを追加」ボタンを選択して、マークするキーワードを確認してください。

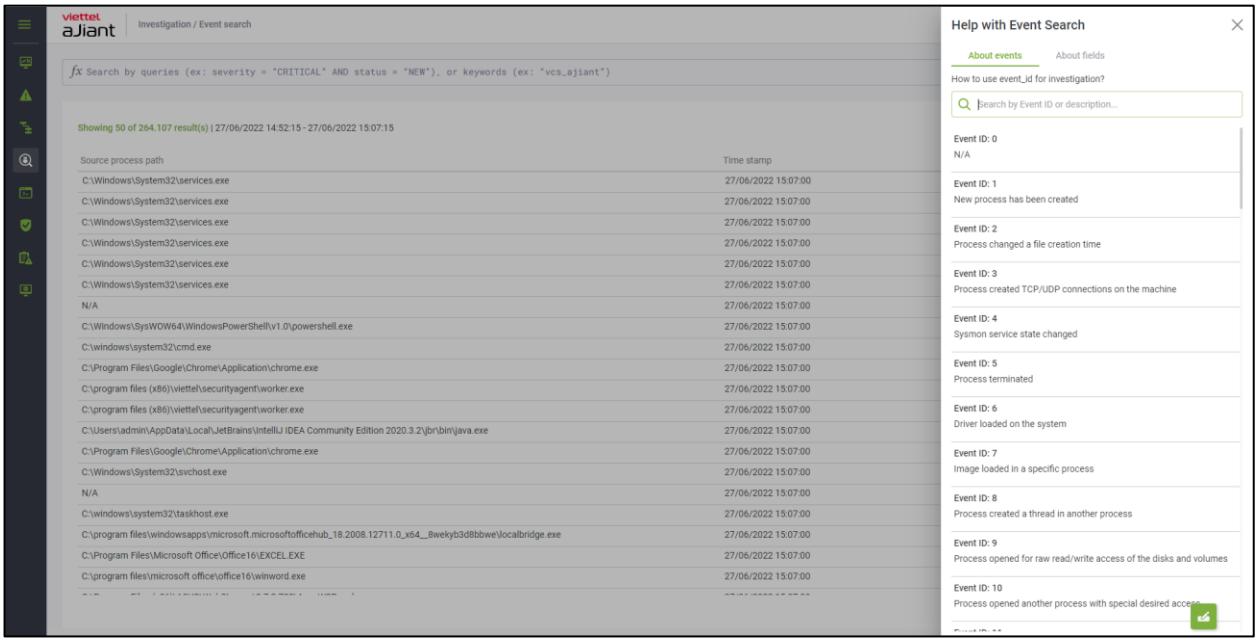
「キャンセル」ボタンを選択して、検索キーワードのマーク操作をキャンセルしてください。



3.5.2.3 助けが必要です。

- 目的：イベント情報の確認、学校の意義；
- 実施手順：
- NDは「Investigation」を選択し、「Event search」タブを選択します。
- イベント検索画面で「もっと見る」を選択してください。

- HTは操作リストを表示します：列の表示、テキストの折り返し、エクスポート、ヘルプが必要、「ヘルプが必要？」を選択してください。
- HTは「Event Searchのヘルプ」ポップアップを表示し、Event Search内の各フィールドの情報や意味を参照できるようにします。

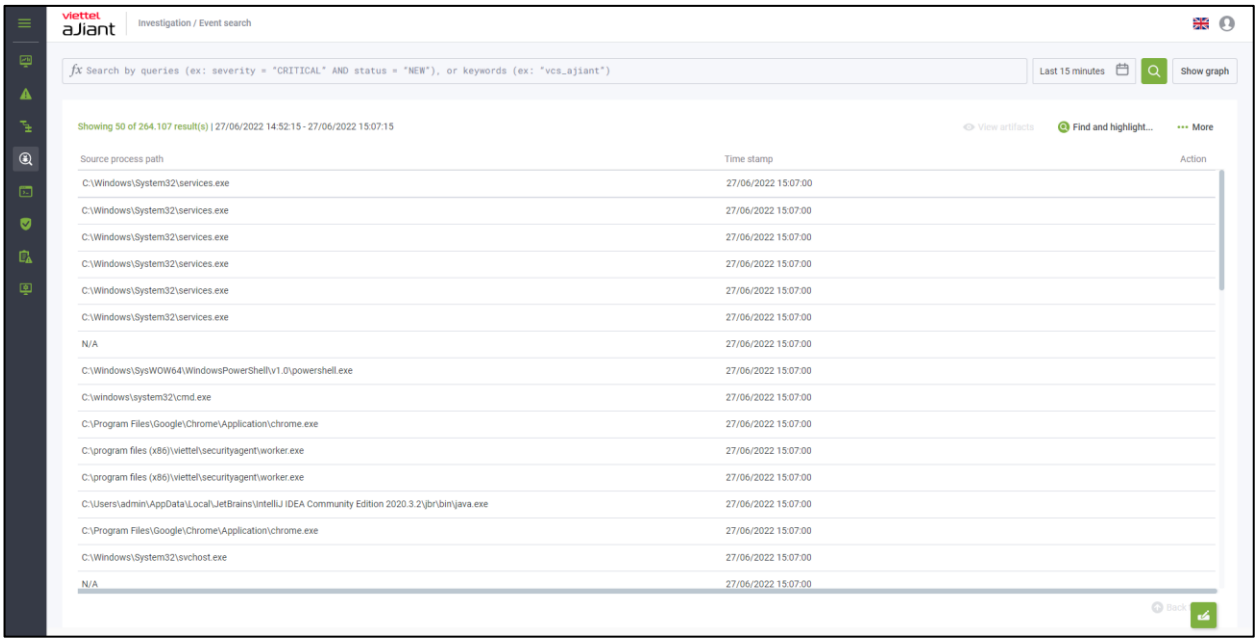


ラップトテキスト

目的：「折り返して全体を表示」ボタンをクリックすると、データ全体を表示するか、データを折りたたむことができます。

実施手順：

- イベント検索画面で「もっと見る」を選択してください。
- HTは以下の操作リストを表示します：列の表示、テキストの折り返し、エクスポート、ヘルプが必要、「テキストの折り返し」を選択してください。
- 「Wrap text」ボタンをクリックすると、表示されるデータが全て展開されたり、折りたたまれたりします。



データをエクスポートする

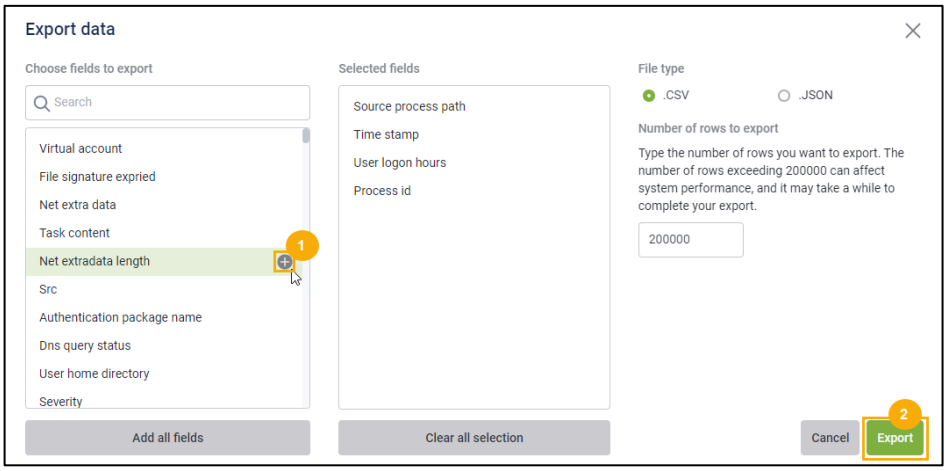
目的：システム内のイベントに関連するデータのダウンロードを許可すること。

実施手順：

- イベント検索画面で「もっと見る」を選択してください。
- HTは操作リストを表示します：列の表示、テキストの折り返し、エクスポート、ヘルプが必要、「エクスポート」を選択してください。
- HTはデータイベント情報のフィルターポップアップを表示し、システムに用意された条件に基づいてフィルターするパラメータを選択します：情報項目の選択、エクスポートファイルの形式、行数の指定、および操作の確認。

「エクスポート」ボタンを選択して、データイベントのダウンロード操作を確認してください。

「キャンセル」ボタンを選択して、操作を中止してください。

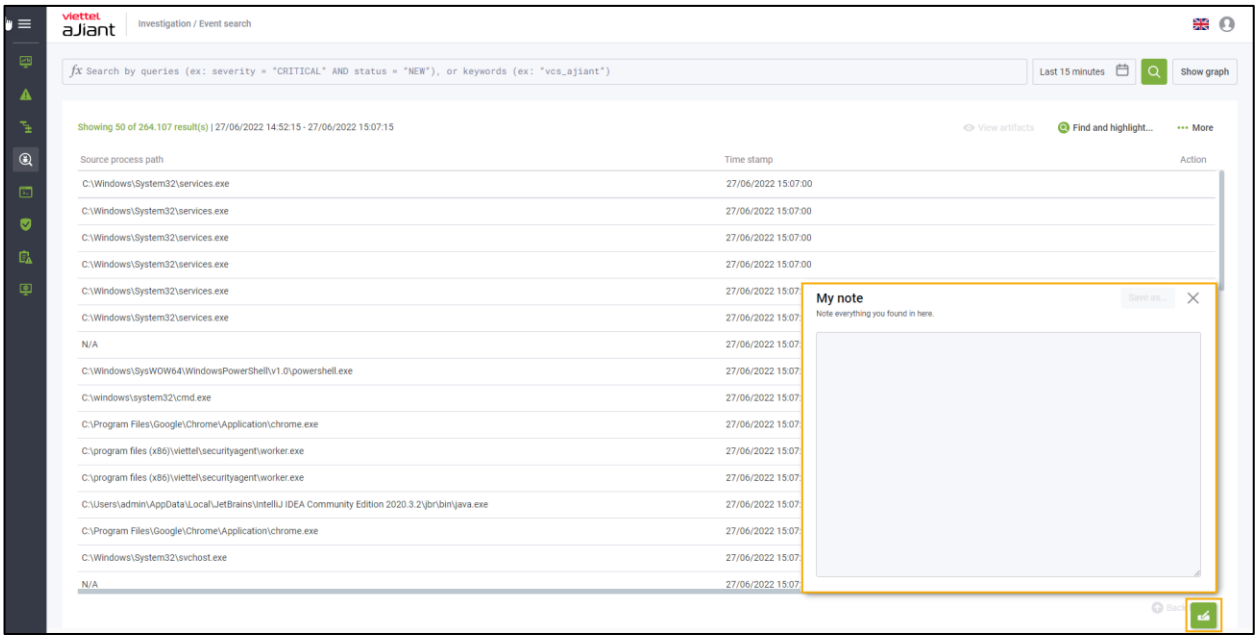


3.4.3 ノート

目的：すべての画面に表示し、画面を移動しても内容が変わらず、「Note」ボタンを移動可能にすること。

実施手順：

- イベント検索画面で、アイコンを選択してください。
- HTはすべての画面にノートを表示し、画面を移動しても内容は変わらず、「ノート」ボタンを移動させることができます。



3.4.4 調査_ ツール展開

目的：ポータルからエージェントへ、情報セキュリティの調査およびトラブルシューティングに使用するツールを展開（デプロイ）する機能。

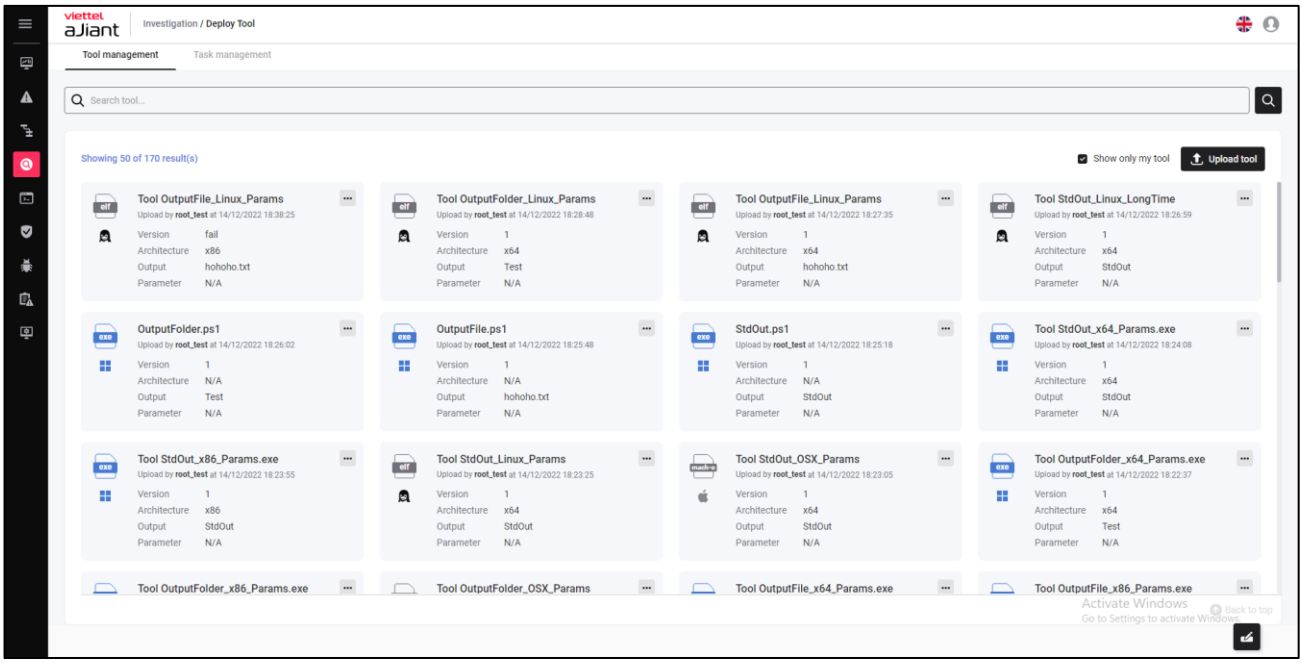
工具管理

目的：システムの全ツールを管理すること。利用者はこの画面でツールの追加・削除が可能です。この画面の機能は以下の通りです。

+ ツールの一覧と各ツールの詳細情報を表示します：名前、パラメータ、バージョン、アーキテクチャ、アップロードユーザー、プラットフォーム、出力、アップロード時間。

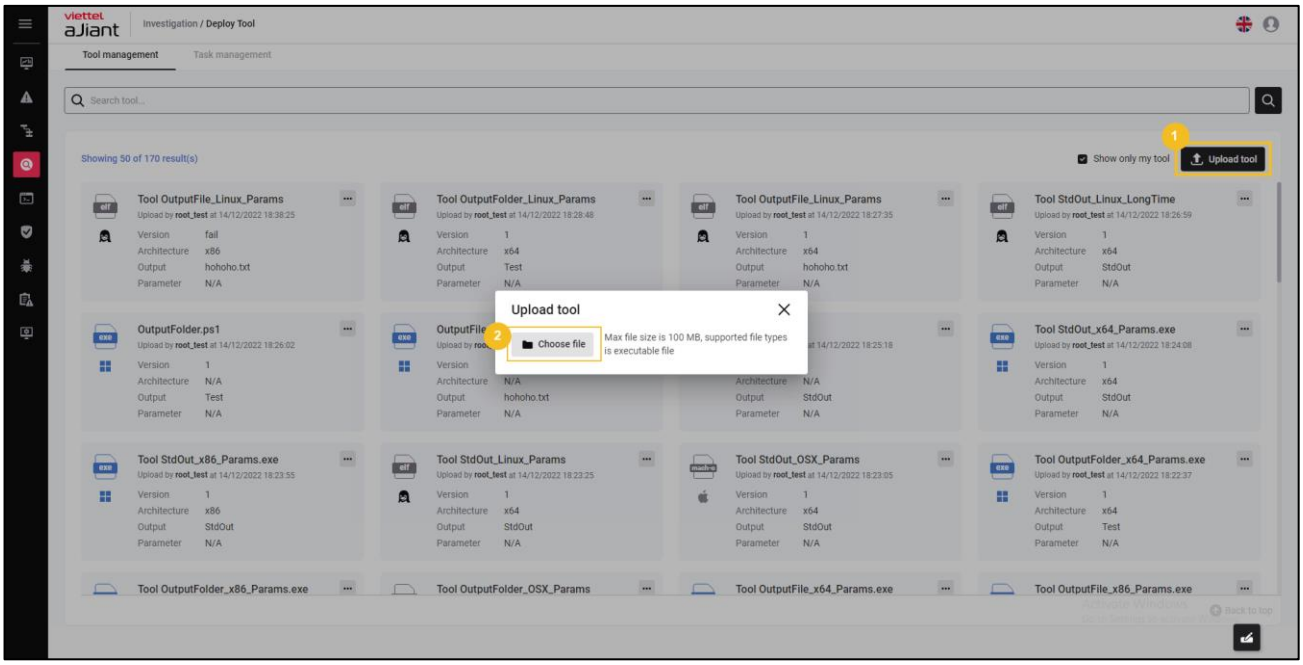
+ ツール検索：ツール名で検索する

+ アップロードツール：アップロードツールはWindows、MacOS、Linuxのエージェント上で動作し、最大容量は100MBです。

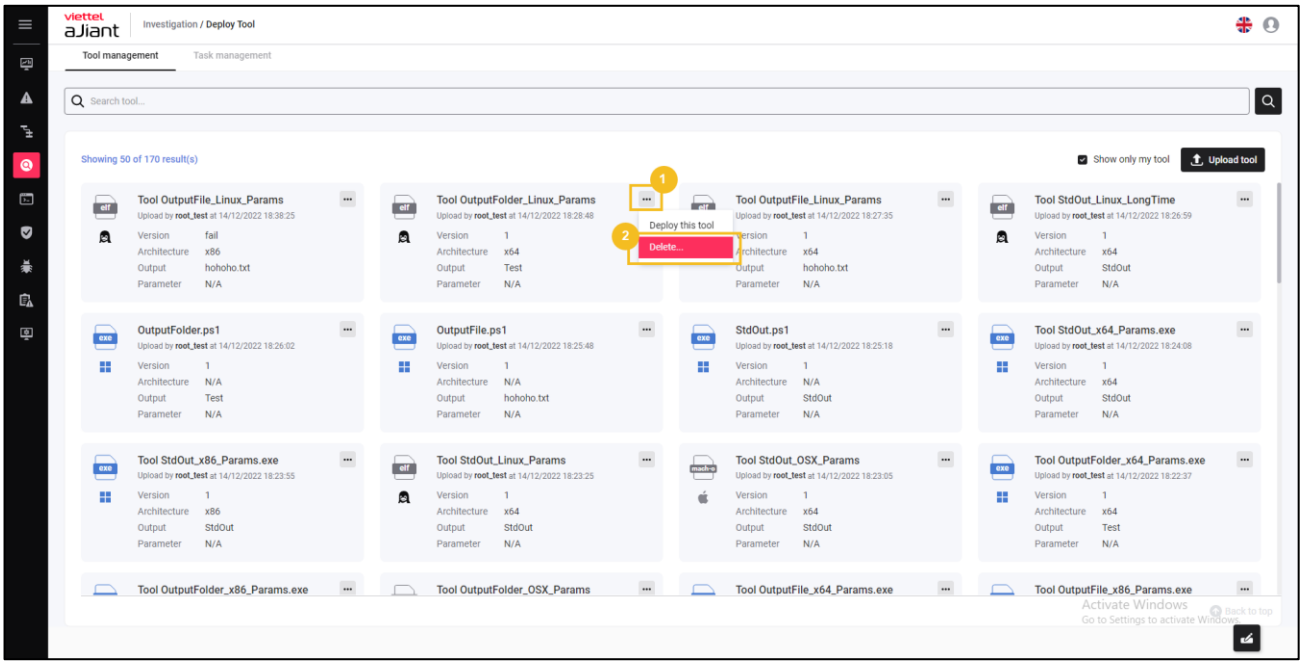


アップロードツールの機能は、以下の手順で操作します：

「アップロードツール」をクリック > アップロードするツールのパスを選択するか、ツールをインターフェースにドラッグ＆ドロップ > ポップアップの「ツール情報」に情報を入力 >「アップロードツール」をクリックしてください。



ツールを削除する機能では、削除したいツールのアイコンを選択し、「削除」を選んでください。



ツールを展開する

目的：エージェント下でのデプロイツール情報の設定

条件：

+ ユーザーがrootグループに属してログインした場合：アクティブ期間が30日未満のすべてのエージェントを表示する。

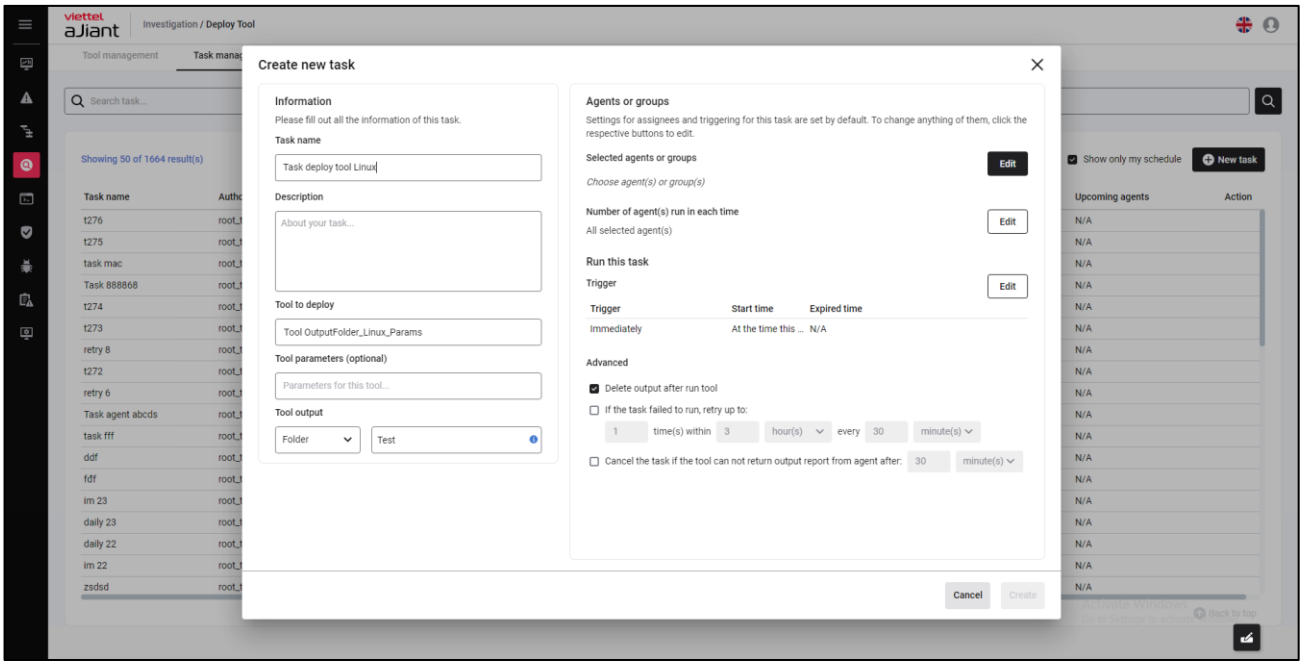
+ ユーザーがデフォルトグループにログインしている場合：デフォルトグループに属するすべてのエージェントを表示する。

+ ユーザーが親グループにログインした場合：ログインしているユーザーのグループおよび対応する子グループに属するすべてのエージェントを表示する。

+ ユーザーが属するグループまたは複数のサブグループに基づいてログイン：ログイン中のユーザーのグループに属するすべてのエージェントを表示する。

ツール管理タブ画面でのツールデプロイ手順：

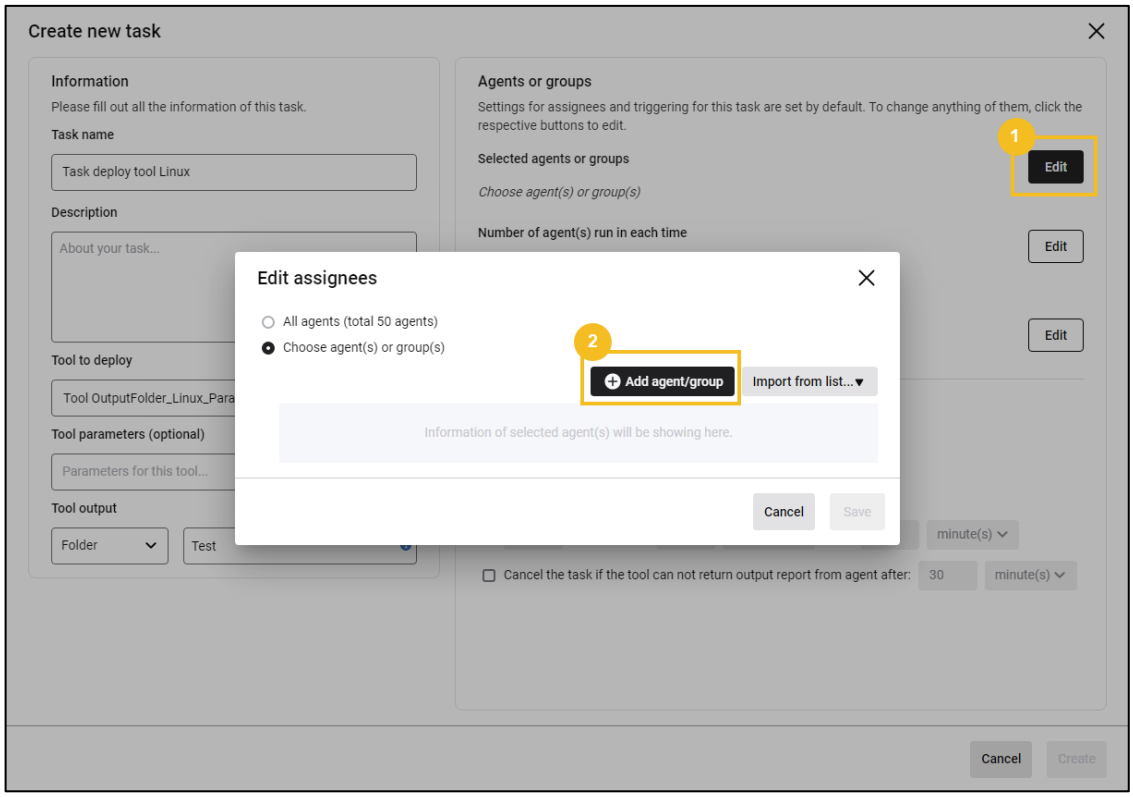
- ツールを選択した後、デプロイするツールのレコードでアイコンを選択し、「このツールをデプロイ」を選択すると、「新しいタスクの作成」画面が表示されます。



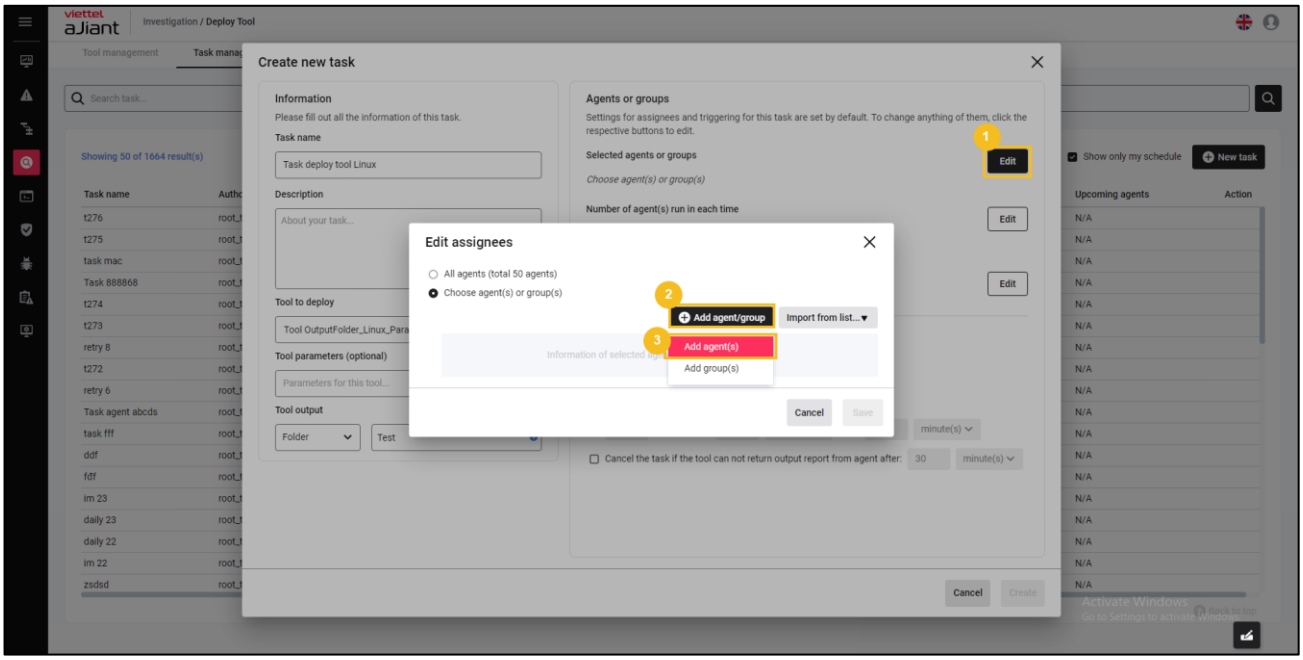
- ツールをデプロイするためのタスク情報を入力してください：タスク名、説明、ツールパラメータ、ツール出力。
- デプロイを実行するためのグループおよびエージェントの選択：

「All agent(s)を選択する」：ログイン中のユーザーの管理範囲内にあるすべてのエージェントを選択してデプロイを実行します。

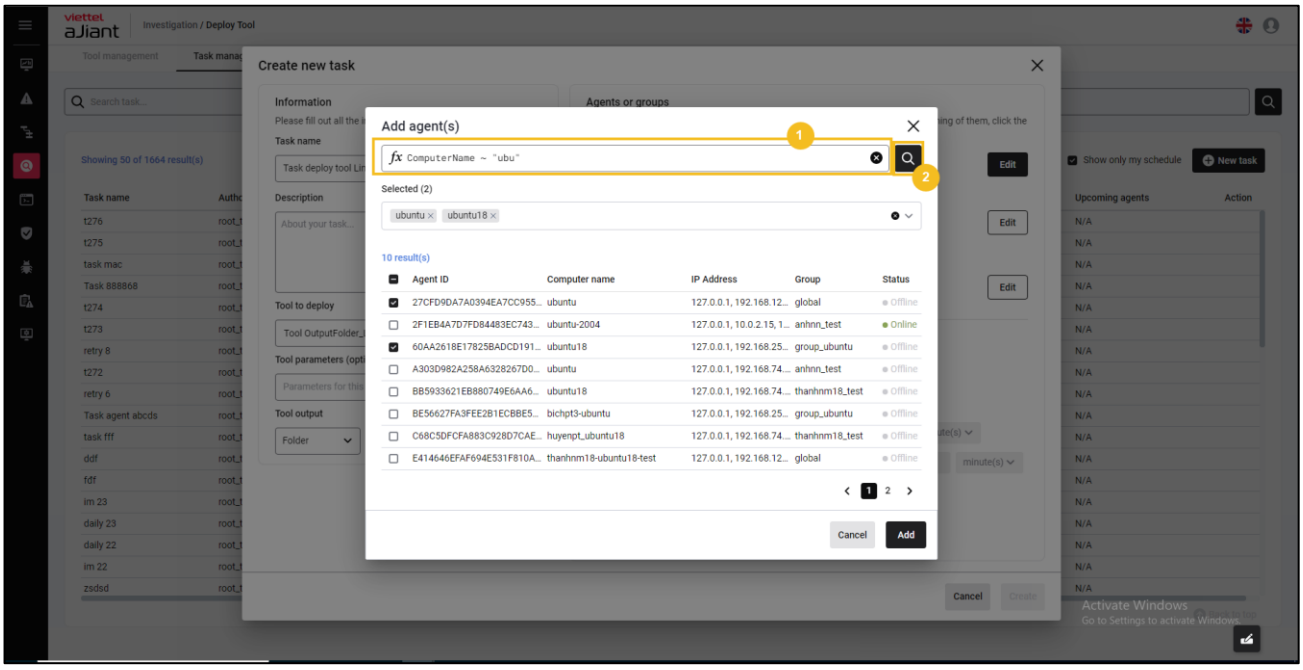
デプロイを実行するエージェントまたはグループを選択してください – エージェントまたはグループを選択:



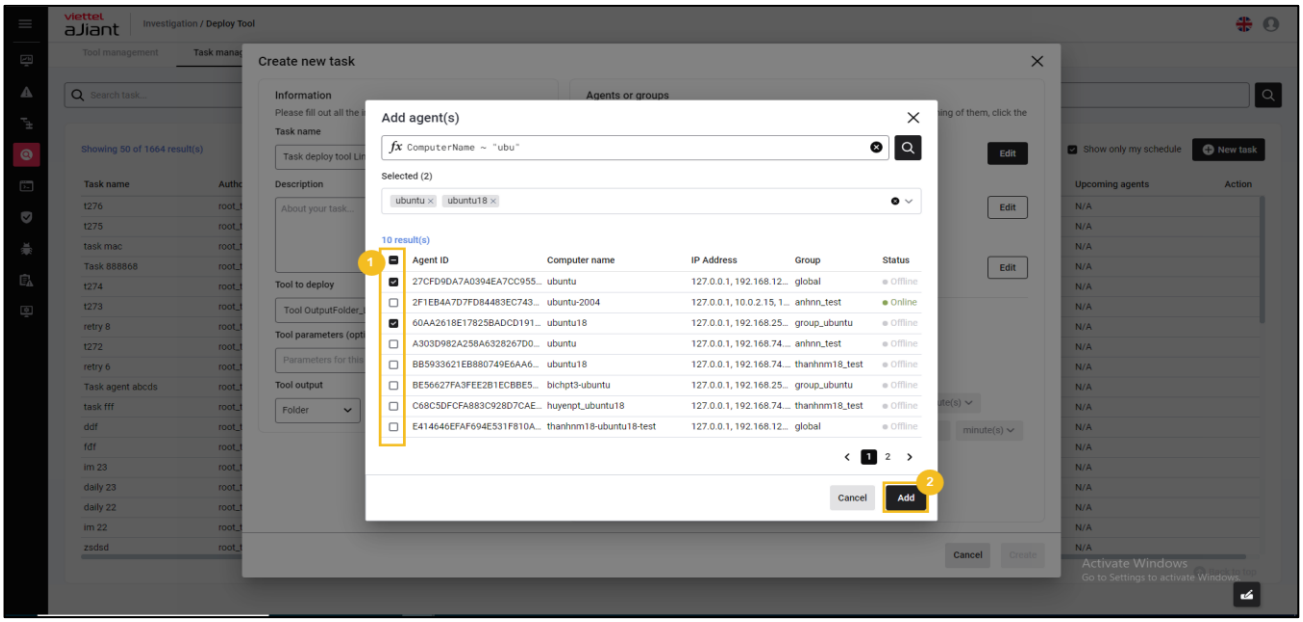
+ エージェントを追加を選択してください。



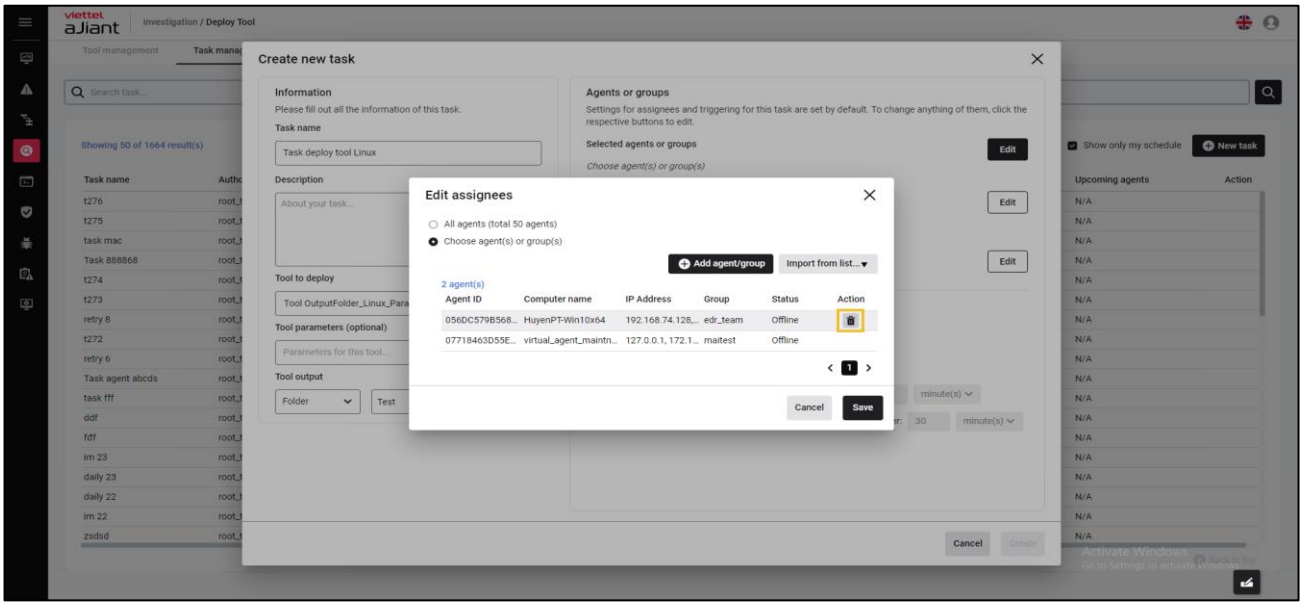
- エージェント検索：クエリ文を作成し、そのクエリ文を使用してエージェントを検索することができます。



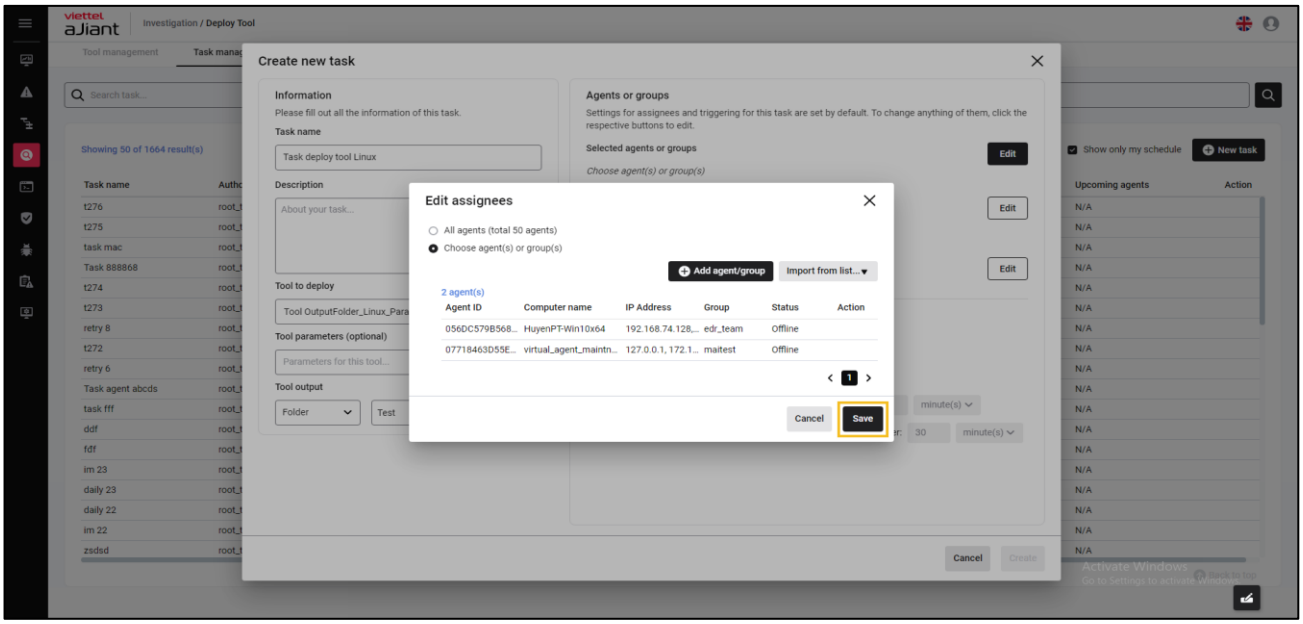
- デプロイするエージェントを1つ以上選択するには、エージェントのチェックボックスをオンにします > 選択したエージェントの情報は「Selected」枠に表示されます > エージェントの追加操作をキャンセルする場合は「Cancel」を選択し、エージェントリストを確定する場合は「Add」ボタンを押します。



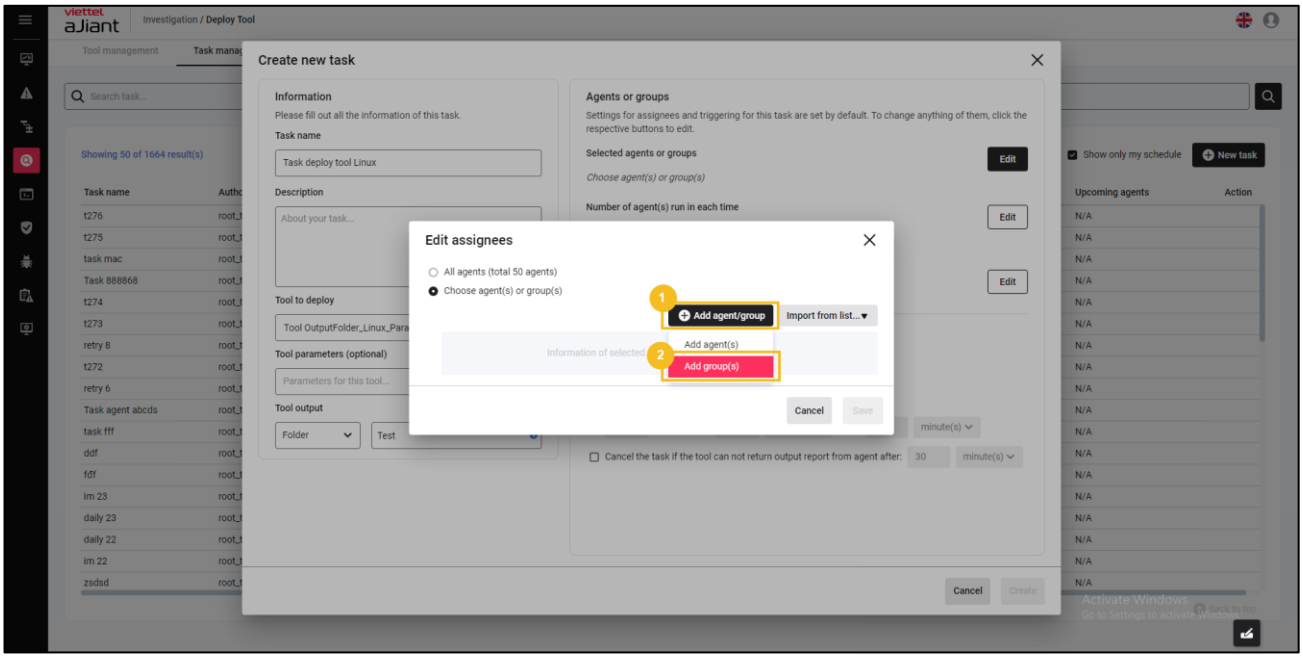
- 選択したエージェントにカーソルを合わせ、アイコンを選択して選択リストからエージェントを削除します。



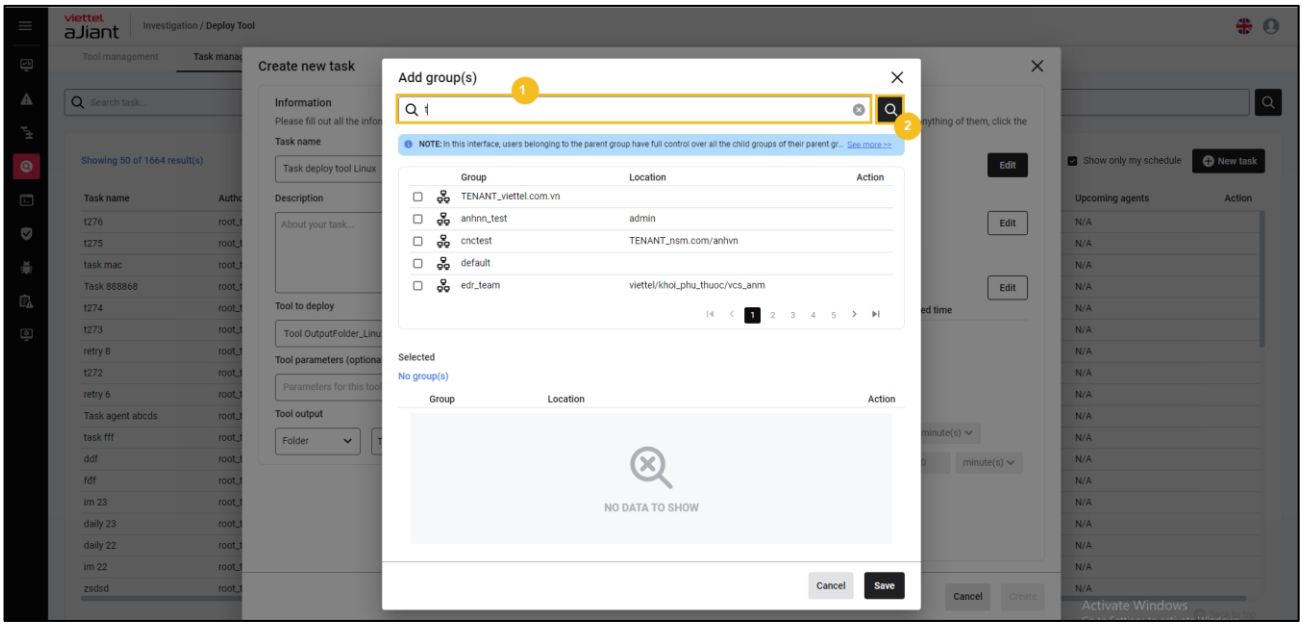
- キャンセルを選択して中止するか、保存を選択して選択したエージェントの情報を保存してください。



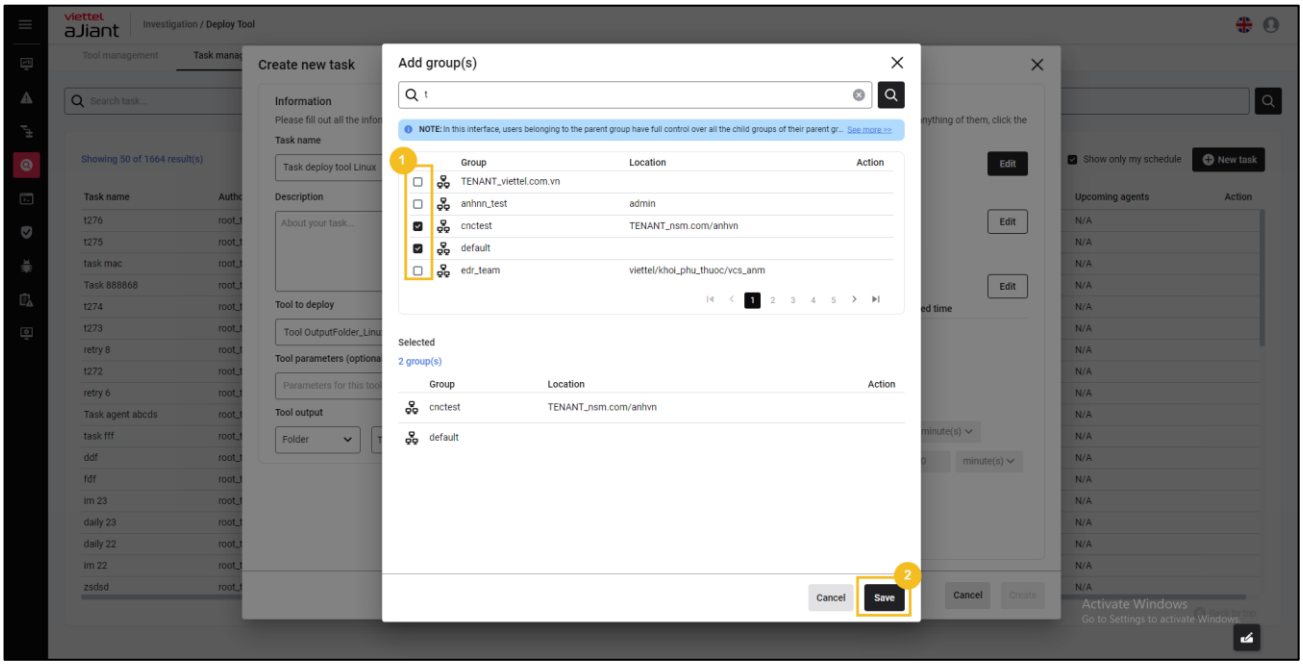
+ グループを追加するを選択してください。



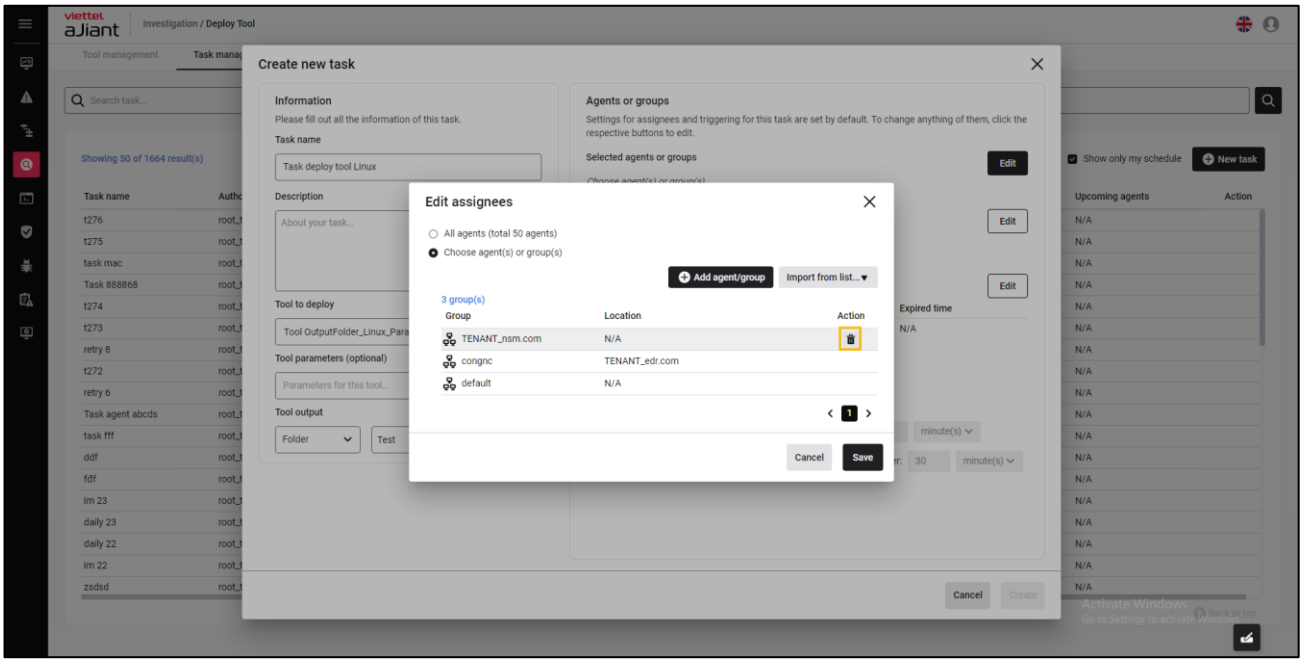
- グループ名でグループを検索し、グループ名のキーワードを入力できるようにする：



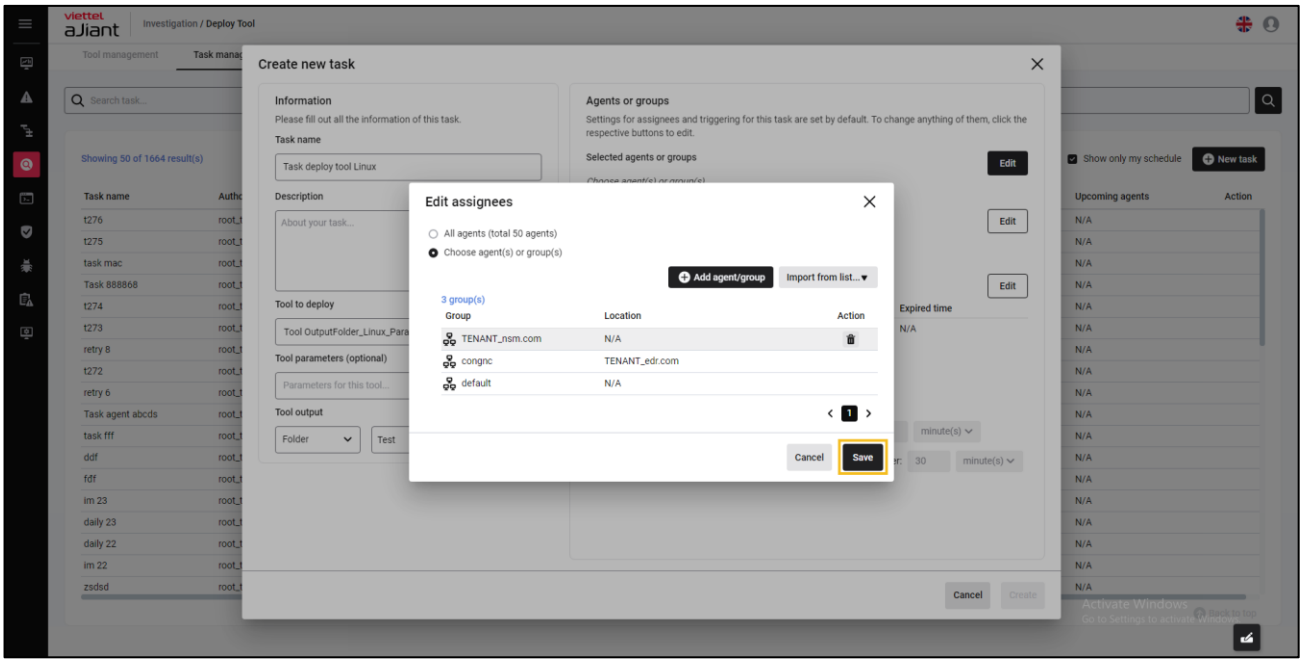
- デプロイするグループを1つまたは複数選択します > 選択されたグループの情報は「Selected」欄に表示されます > グループの追加をキャンセルする場合は「Cancel」を選択し、グループリストを確定する場合は「Save」ボタンを押してください。



- 選択したグループにカーソルを合わせ > アイコンを選択して、選択リストからグループを削除します。



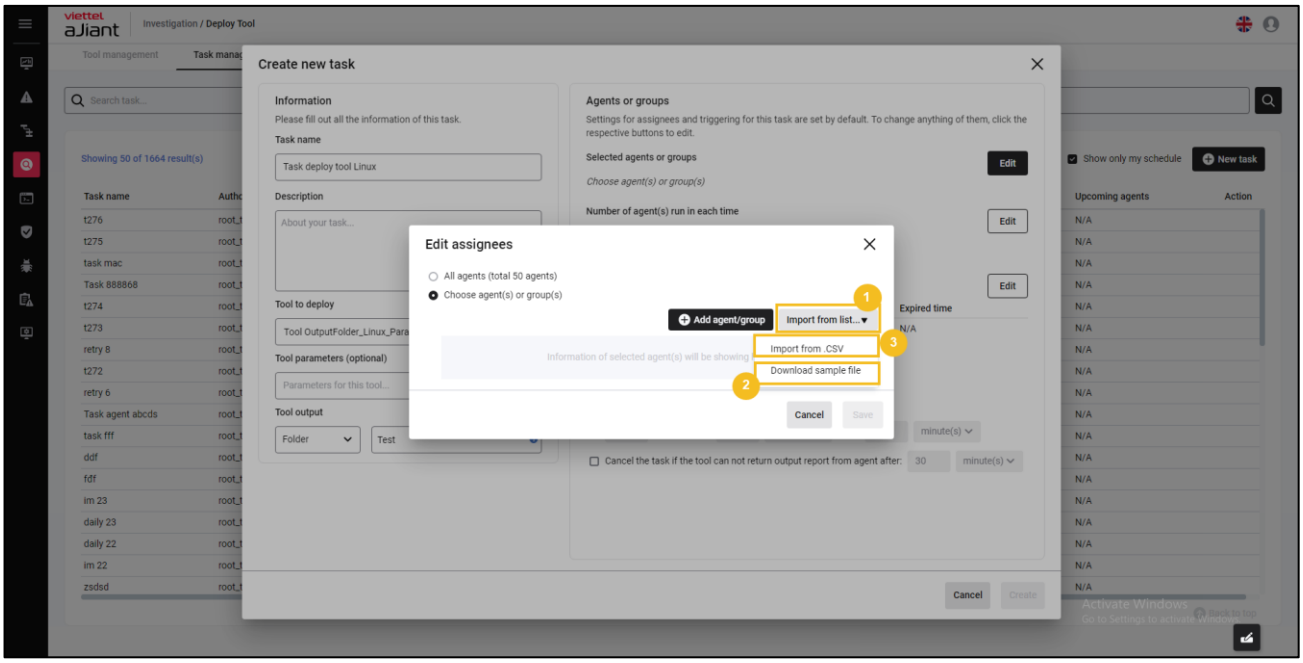
- キャンセルを選択して中止するか、選択したグループを保存してデプロイしてください。



+ リストからインポート：.csvファイルからエージェントのリストをアップロード可能 >「リストからインポート」を選択してください。

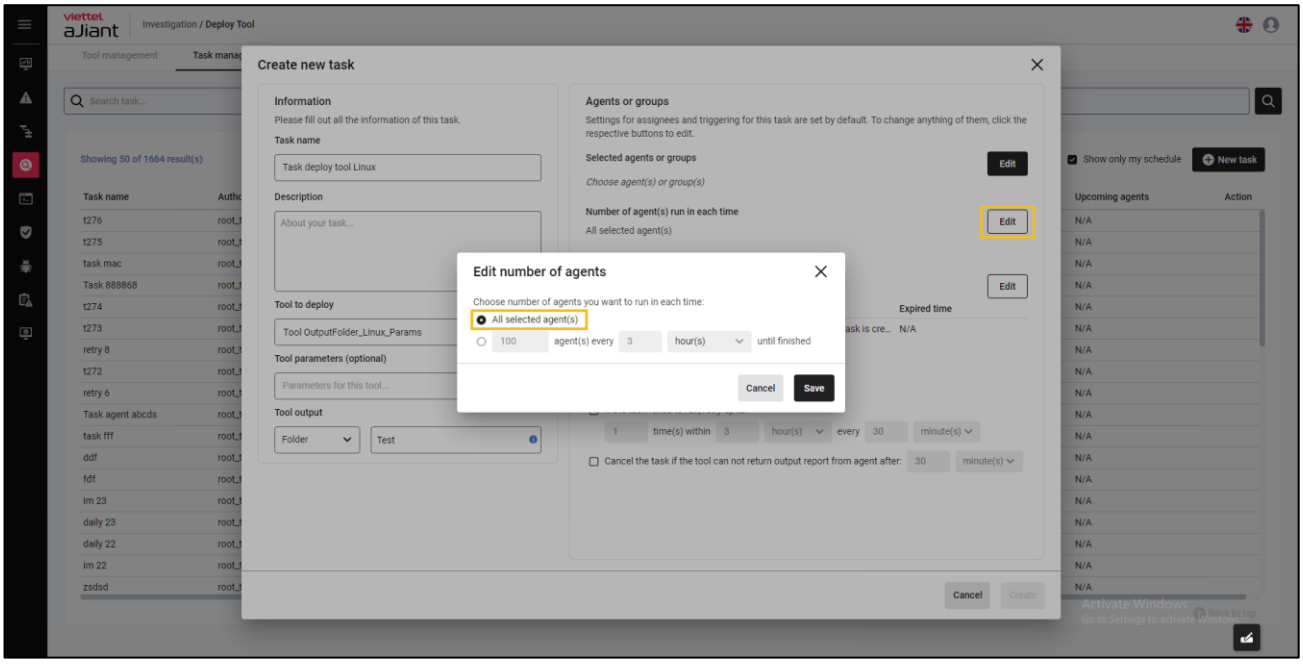
- サンプルファイルをダウンロードして、エージェントファイルのリストフォームを取得してください。

- エージェント情報を入力し、「.CSVからインポート」を選択してエージェントリストをアップロードしてください。

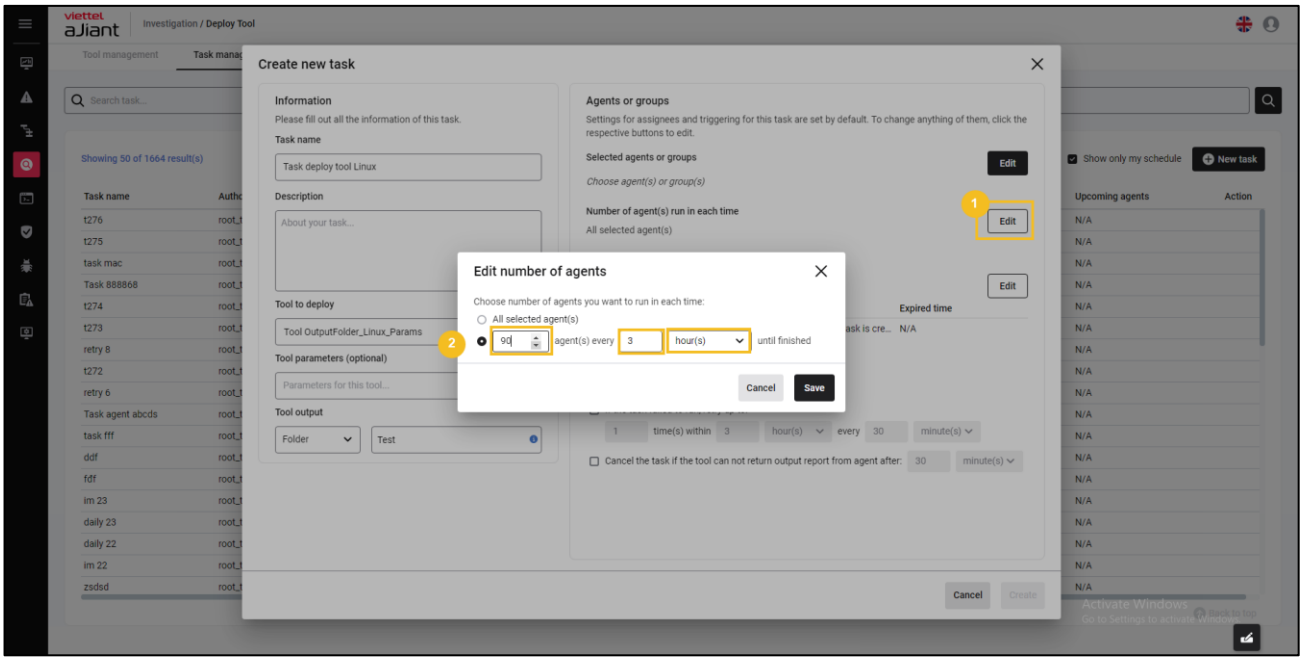


- ツールを一度にデプロイするエージェントの数の設定：

  + 全エージェント：選択したすべてのユーザーエージェントのデプロイを許可する

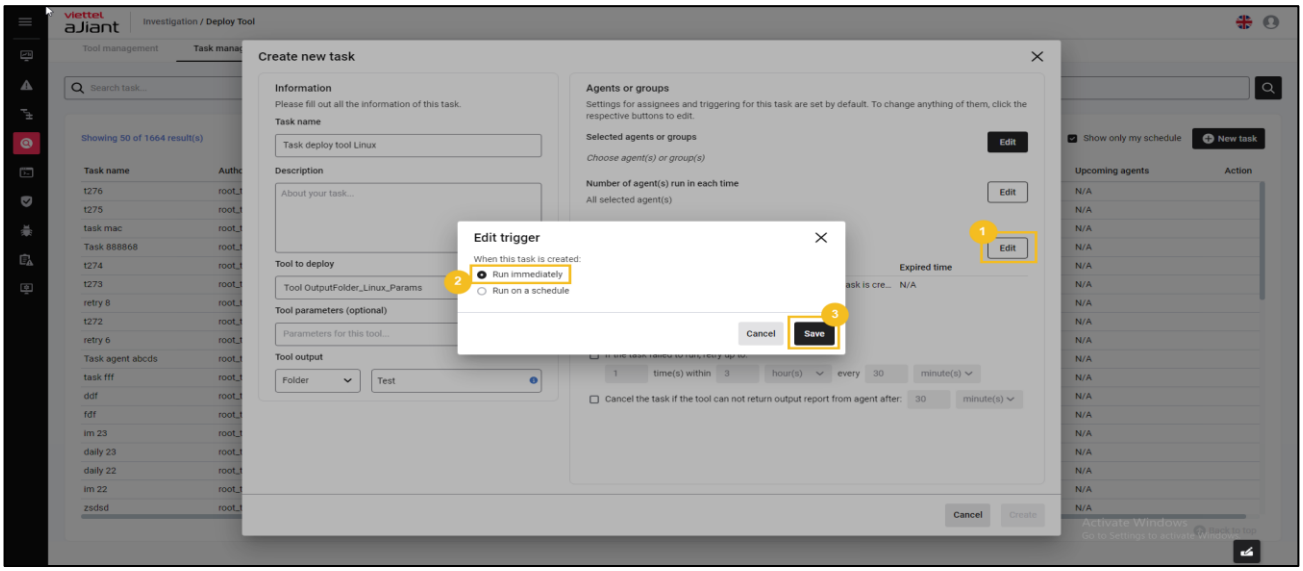


  + デプロイごとのエージェント数の設定：



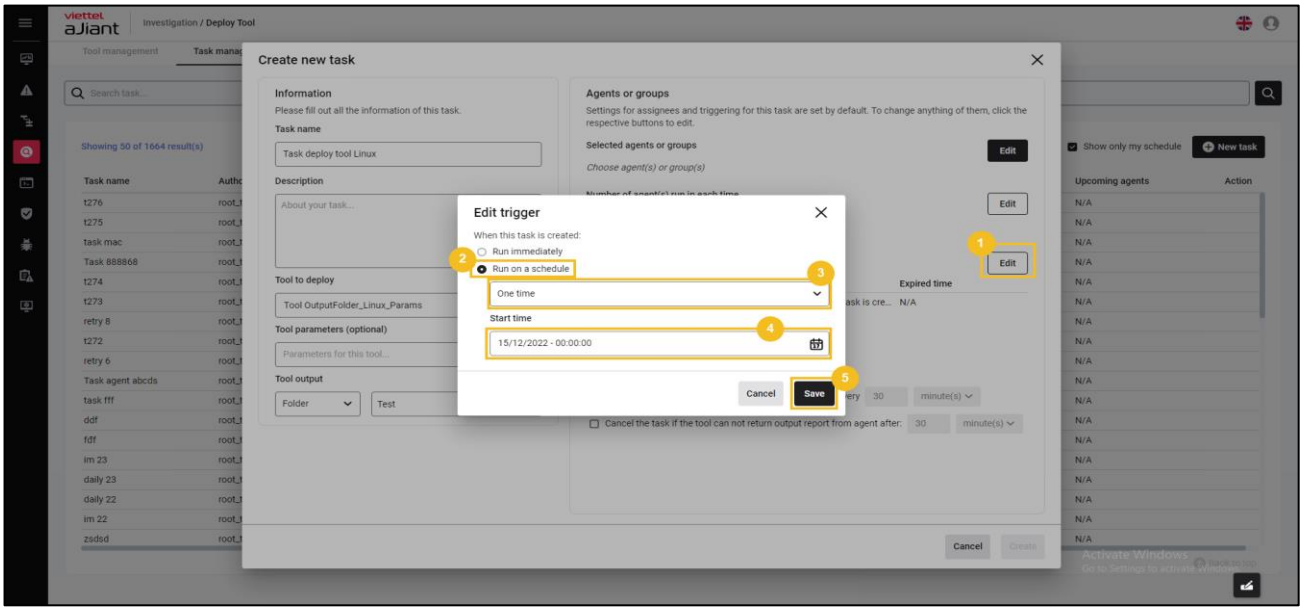
- デプロイツール実行の時間情報設定（スケジューリング）：

+ 「Run immediately」を選択すると、タスク作成後すぐにデプロイツールのスケジュール設定が実行されます。

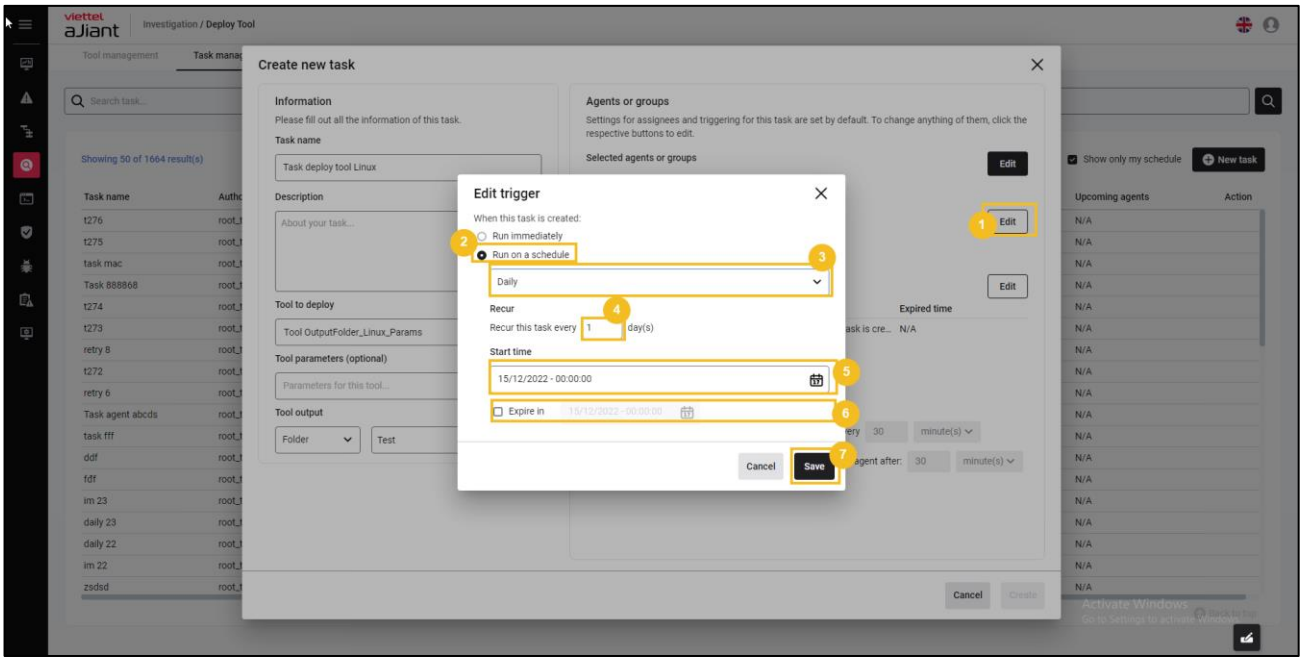


+ スケジュールに従って実行するには、「Run on schedule」を選択して、デプロイツールの時間設定を行います。

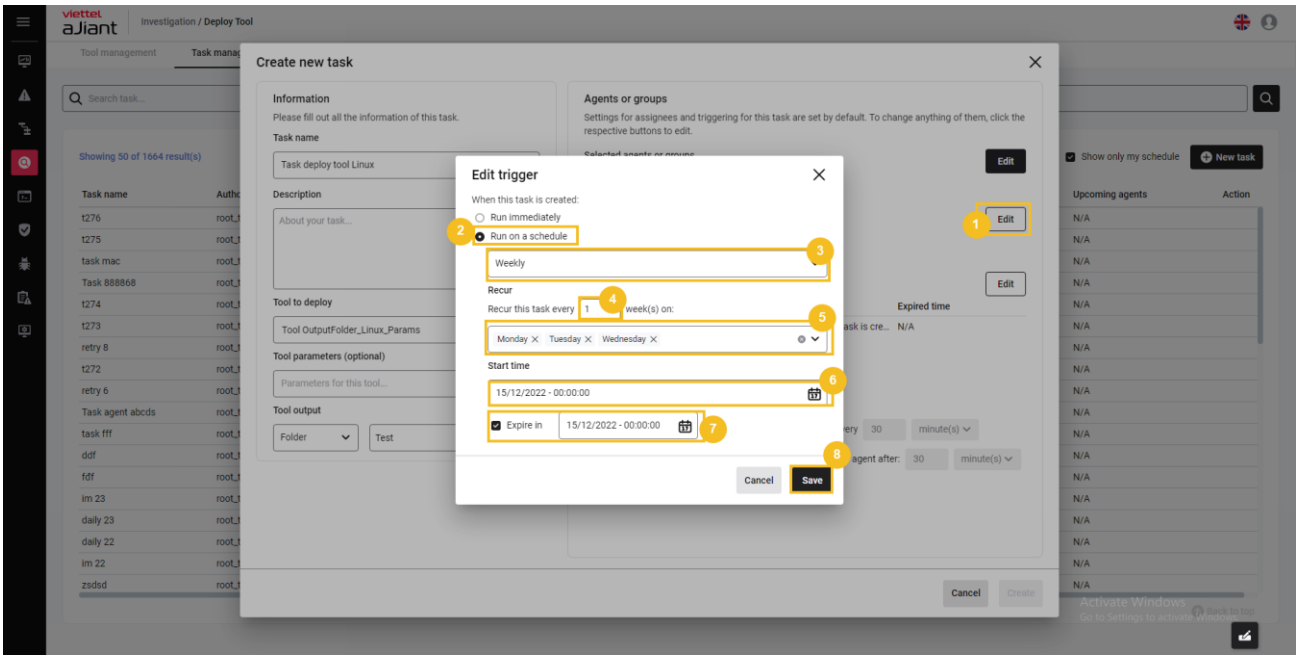
- スケジュールを「一回限り」に選択してください。
  - ツールのデプロイスケジュールを一度だけ設定できるようにする。
  - 開始時間の設定：



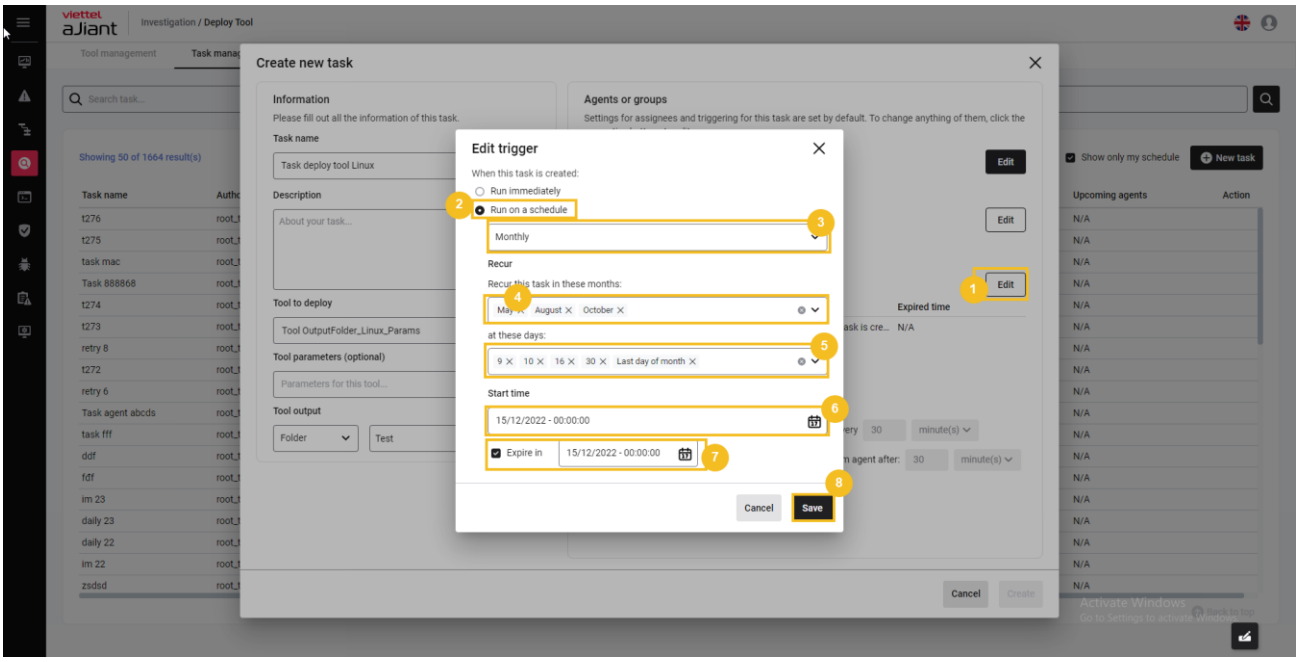
- スケジュールを「Daily（日次）」に選択してください。
  - ツールの毎日のデプロイスケジュールを許可する。
  - 繰り返し時間;
  - 開始時間と終了時間の設定：



- スケジュールを「週次」に選択してください。
  - 週次デプロイツールのスケジュール設定を許可する。
  - 繰り返し時間;
  - 開始時間と終了時間の設定：



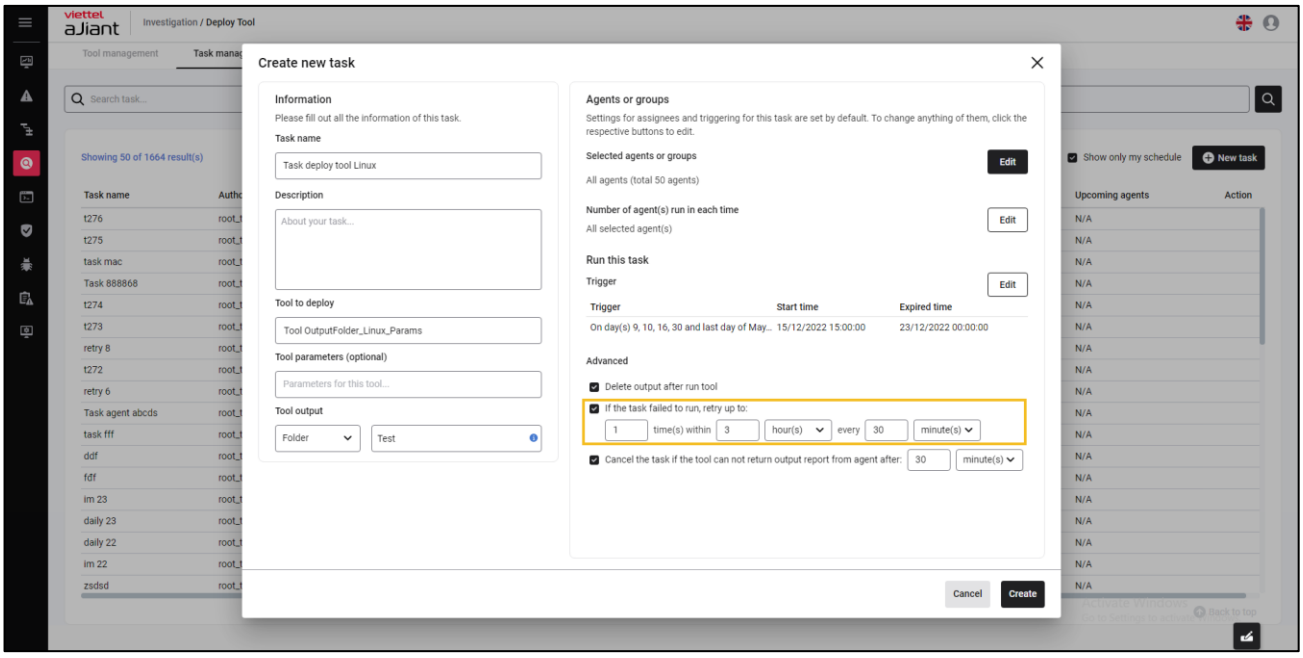
- スケジュールを「毎月」に選択してください。
  - 毎月のデプロイツールのスケジュール設定を許可する。
  - 繰り返し時間;
  - 開始時間と終了時間の設定：



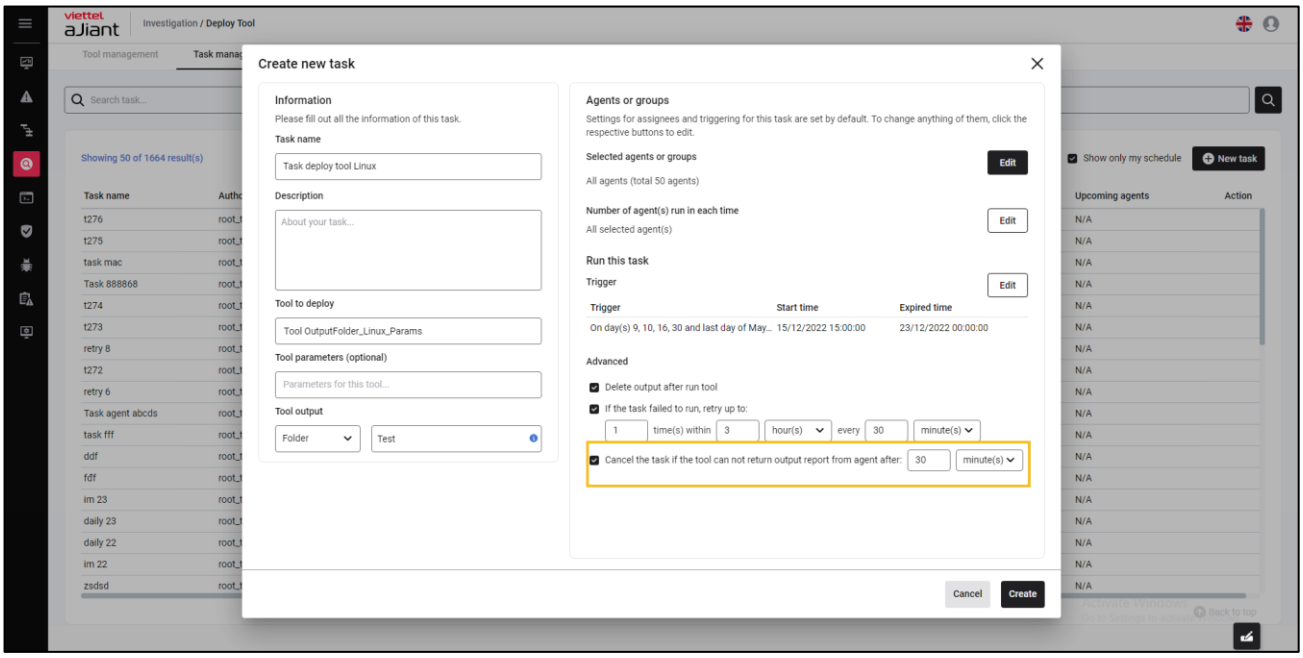
- タスクの詳細設定情報

+ 「Delete tool after run tool」は、ツール実行後にツールの出力を削除し、正常にバックエンドへ結果を返すことを可能にします。

+ タスクの実行に失敗した場合、タスクのデプロイが失敗するまで最大で再試行を行い、再試行タスク（タスクの再デプロイ）の情報を設定できるようにします。



+ ユーザーが設定した時間内にエージェントから出力レポートが返されない場合は、タスクをキャンセルしてください。



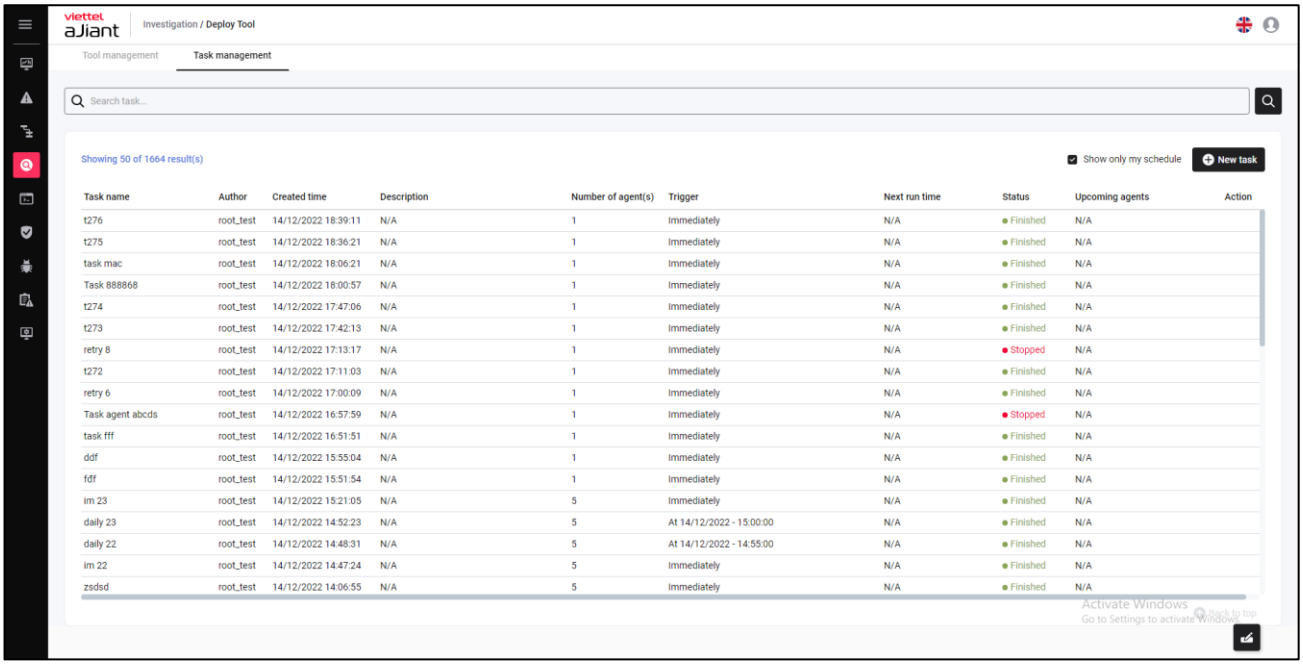
- 「Create」を選択して、新しいタスクを作成するか、エージェント下のデプロイツール情報を設定します。キャンセルする場合は「Cancel」を選択して、タスクのキャンセルまたはエージェント下のデプロイツール情報の設定を中止してください。

タスク管理

a. タスクリスト

目的：デプロイツールのスケジュールタスク一覧を表示すること。

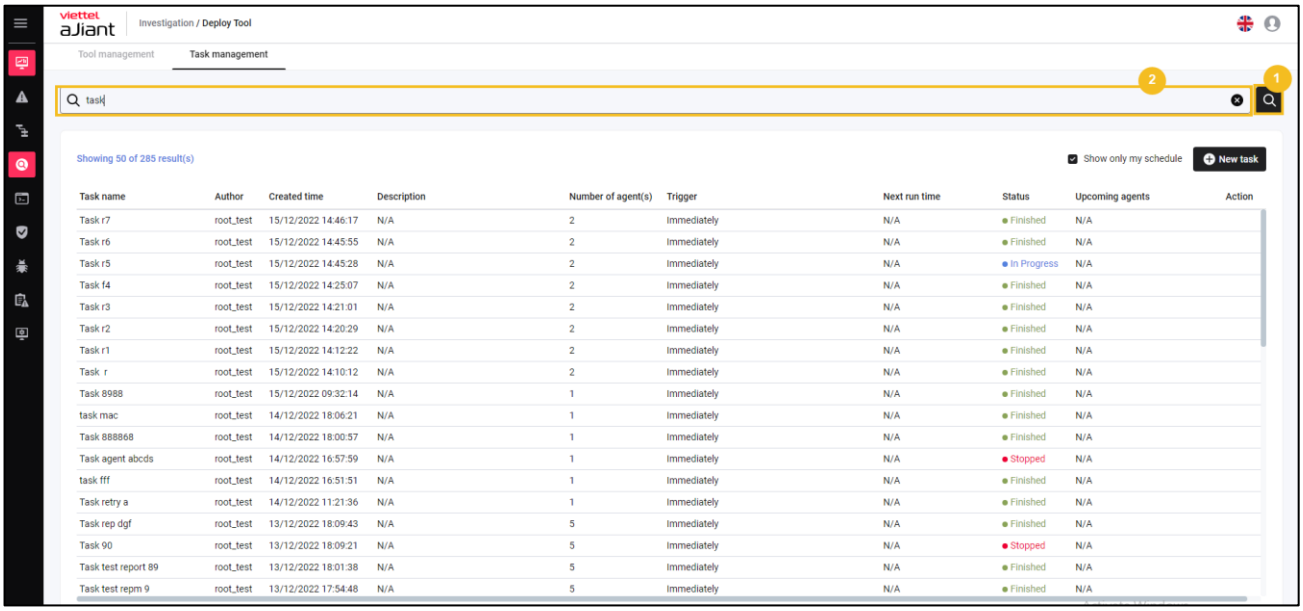
表示される情報フィールド：タスク名、作成者、作成日時、説明、エージェント数、トリガー、次回実行日時、ステータス、今後のエージェント



b. タスクを検索する

目的：タスク名によるタスク検索を可能にすること。

実行手順：検索キーワードを入力 > 「Search」ボタンを選択するか、キーワードの入力を終了 > Enterキーを押す。システムは、システム内にある検索キーワードに関連するエージェント情報の検索を実行します。



c. タスクを作成する

（3.5.4.2項「デプロイツール」と同様の機能）

目的：エージェント下でデプロイツールの情報を設定すること

条件：

+ ユーザーがrootグループに属している場合：アクティブ期間が30日未満のすべてのエージェントを表示する。

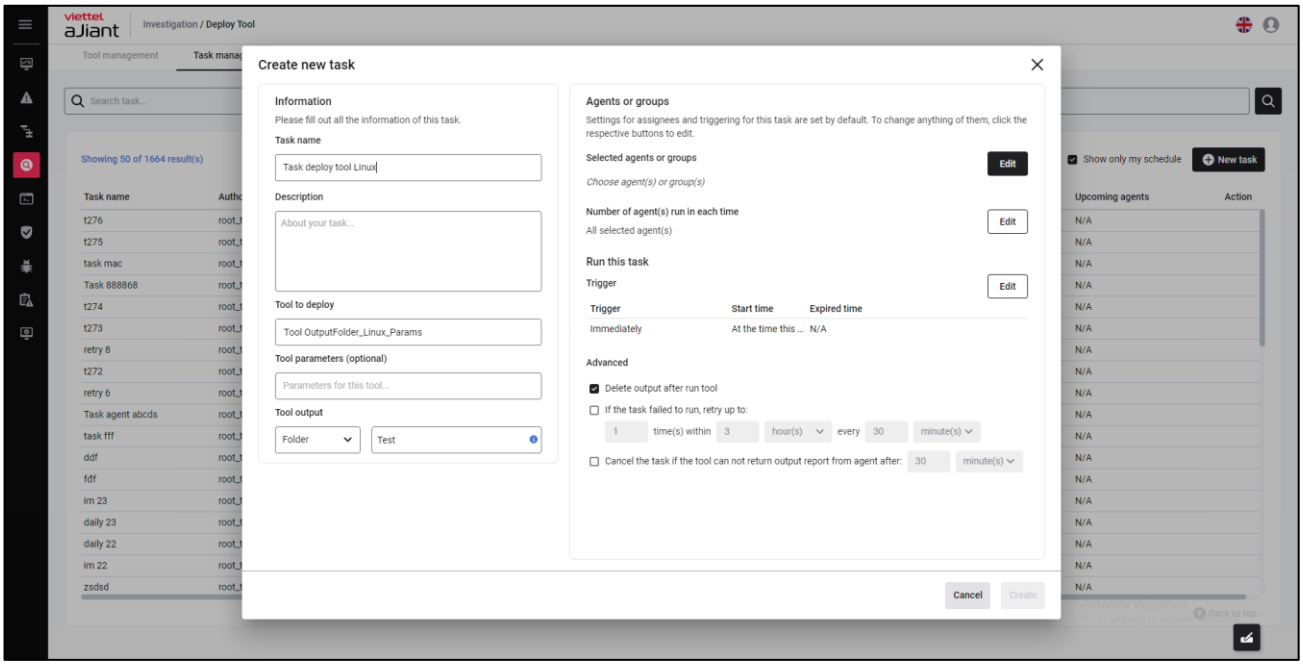
+ ユーザーがデフォルトグループにログインしている場合：デフォルトグループに属するすべてのエージェントを表示する。

+ ユーザーが親グループにログインした場合：ログインしているユーザーのグループおよび対応する子グループに属するすべてのエージェントを表示する。

+ ユーザーが一つまたは複数のグループに所属している場合：ログインしているユーザーのグループに属するすべてのエージェントを表示する。

タスク管理タブでツールをデプロイする手順：

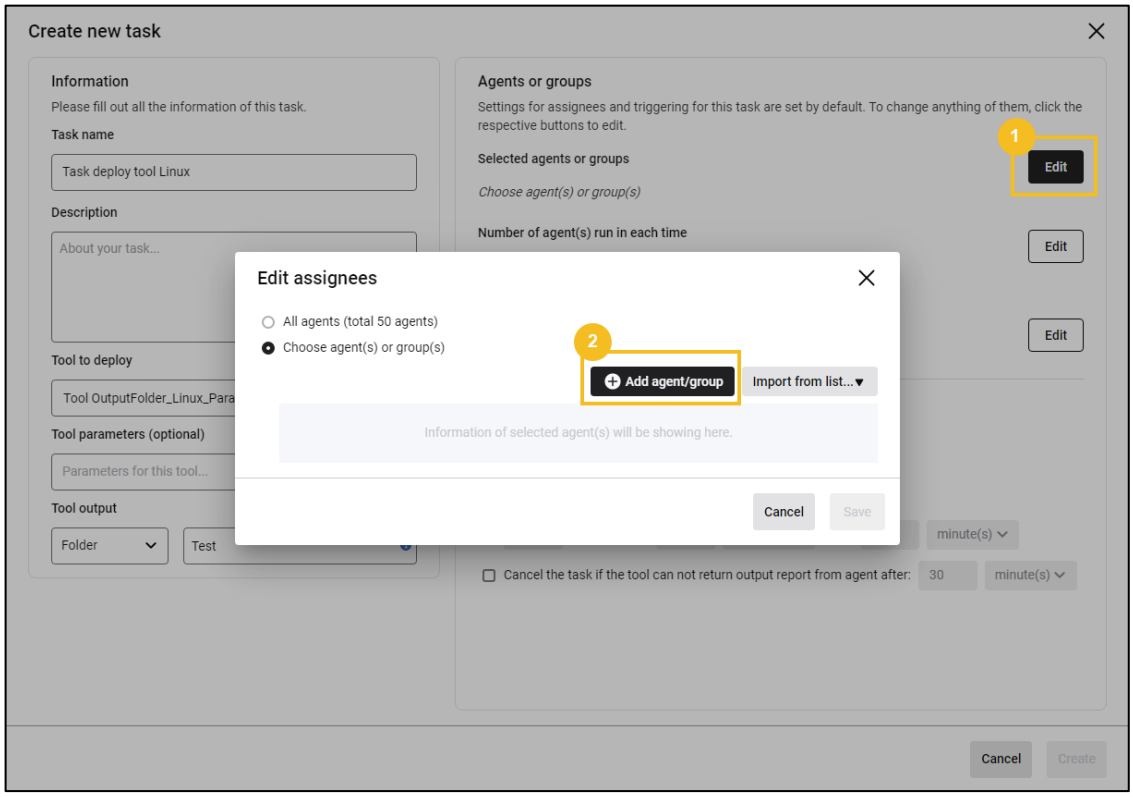
- ツールを選択した後、デプロイするツールのレコードでアイコンを選択し、「Deploy this tool」を選択すると、「Create new task」画面が表示されます。



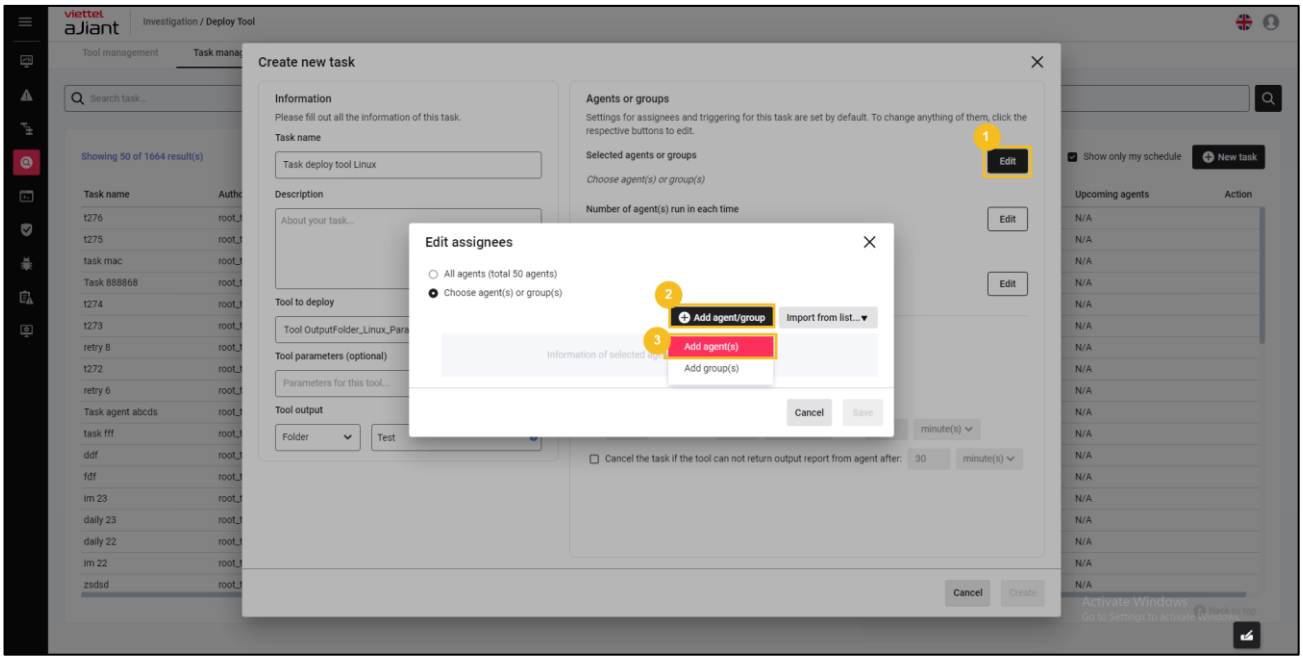
- ツールをデプロイするためのタスク情報を入力してください：タスク名、デプロイするツール、説明、ツールのパラメータ、ツールの出力。
- デプロイを実行するためのグループおよびエージェントの選択：

「All agent(s) を選択する：ログイン中のユーザーの管理範囲内にあるすべてのエージェントを選択してデプロイを実行します。」

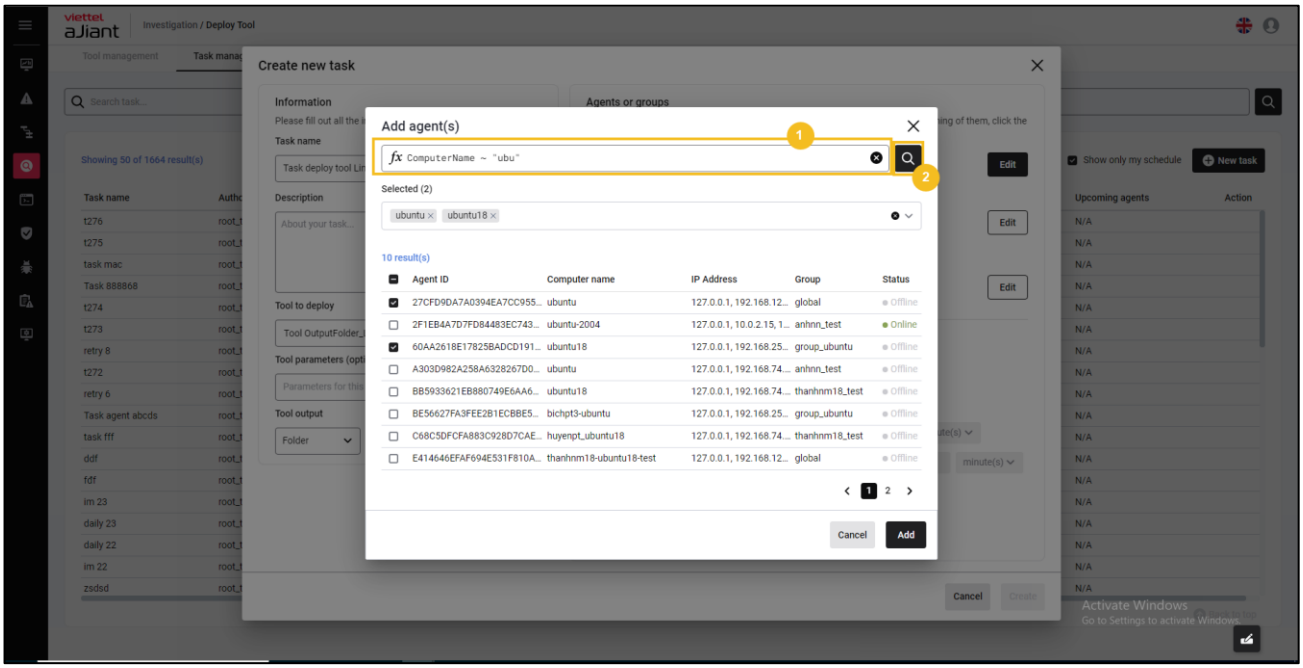
デプロイを実行するエージェントまたはグループを選択してください – エージェントまたはグループを選択:



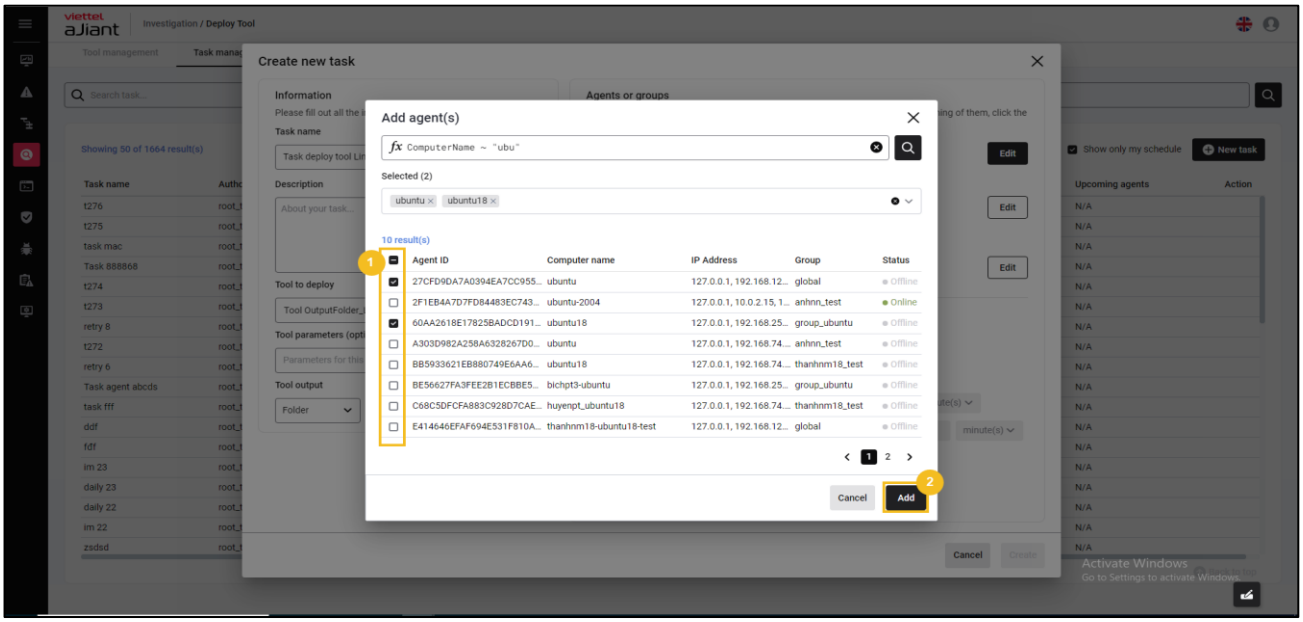
+ エージェントを追加を選択してください。



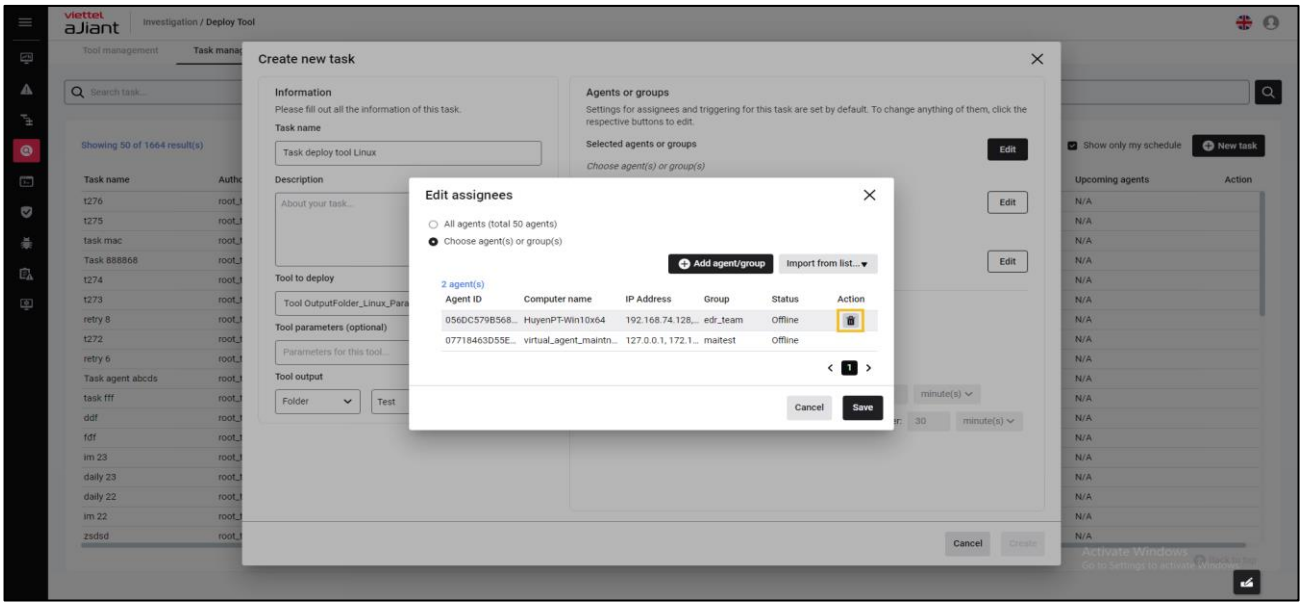
- エージェント検索：クエリ文を作成し、そのクエリ文を使用してエージェントを検索することができます。



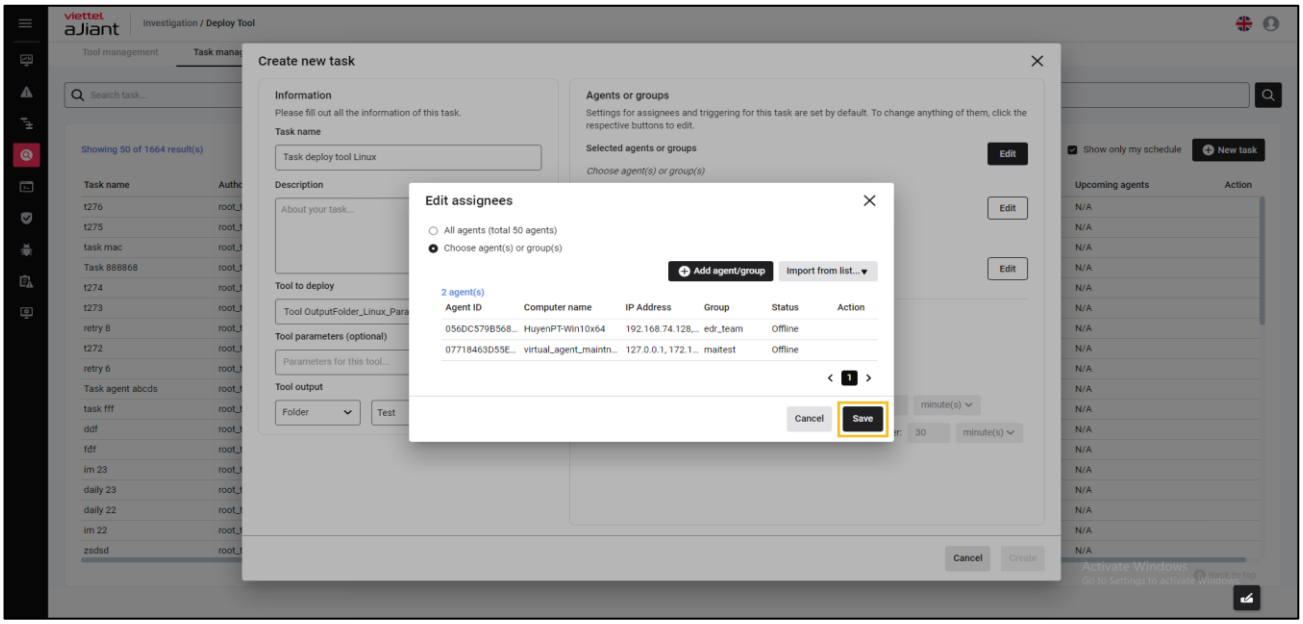
- デプロイするエージェントを1つまたは複数選択してください > 選択したエージェントの情報が「Selected」欄に表示されます > エージェントの追加をキャンセルする場合は「Cancel」を選択し、エージェントリストを確定する場合は「Add」ボタンを押してください。



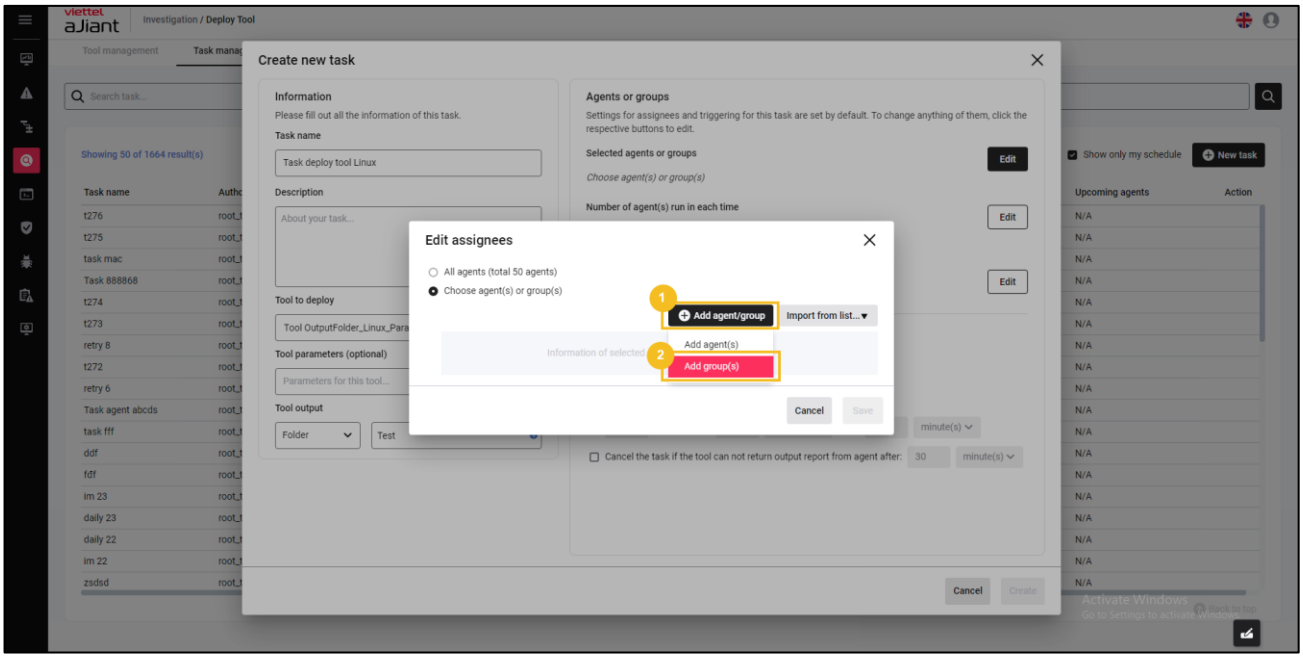
  - 選択したエージェントにカーソルを合わせ > アイコンを選択して、選択リストからエージェントを削除します。



- キャンセルを選択してキャンセルするか、保存を選択してデプロイするために選択したエージェントの情報を保存してください。

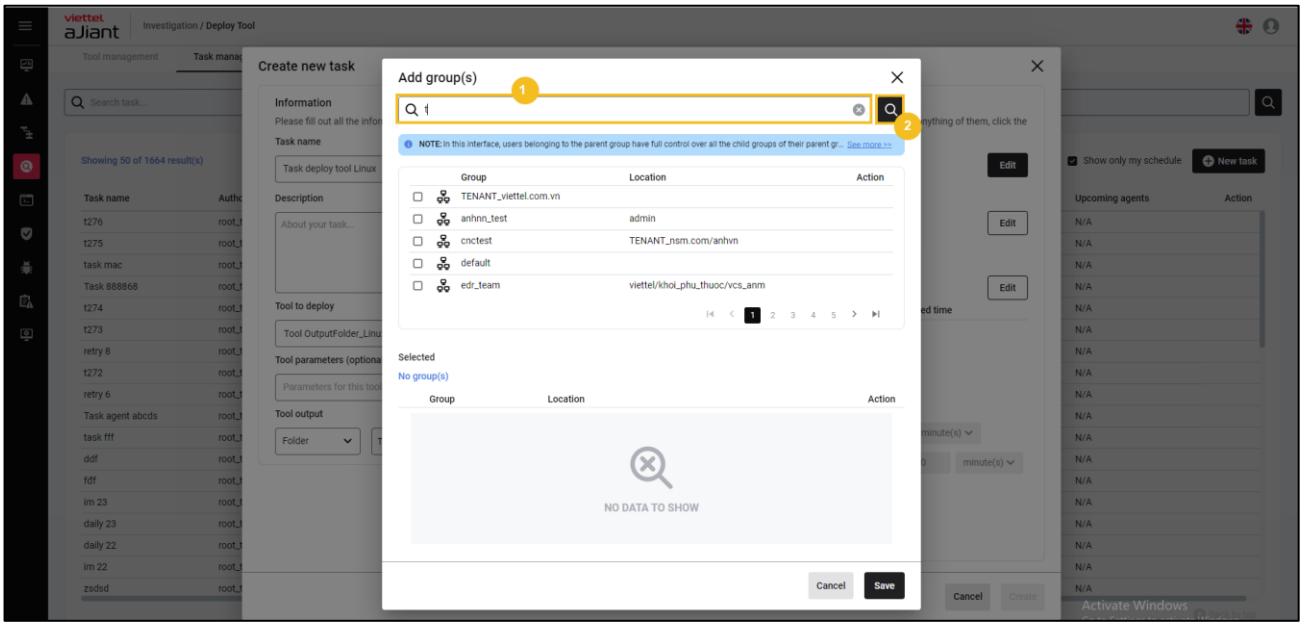


+ グループを追加するを選択してください。

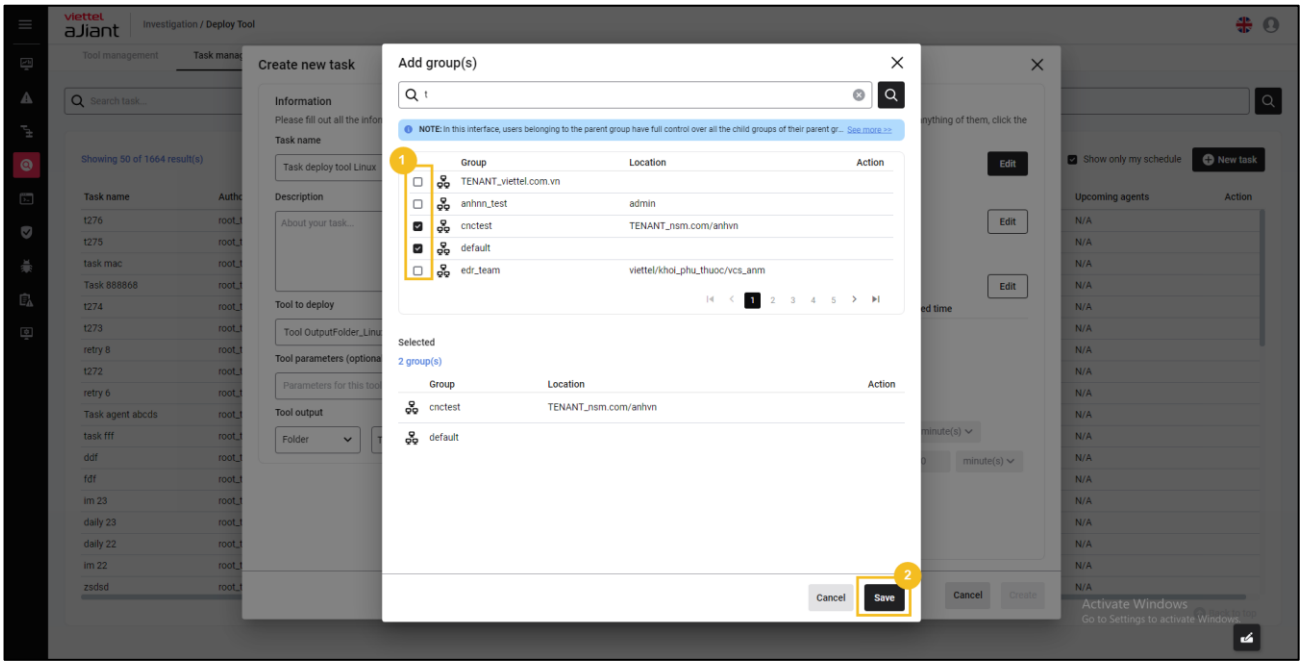


- グループ名でグループを検索し、グループ名のキーワードを入力して検索を許可する

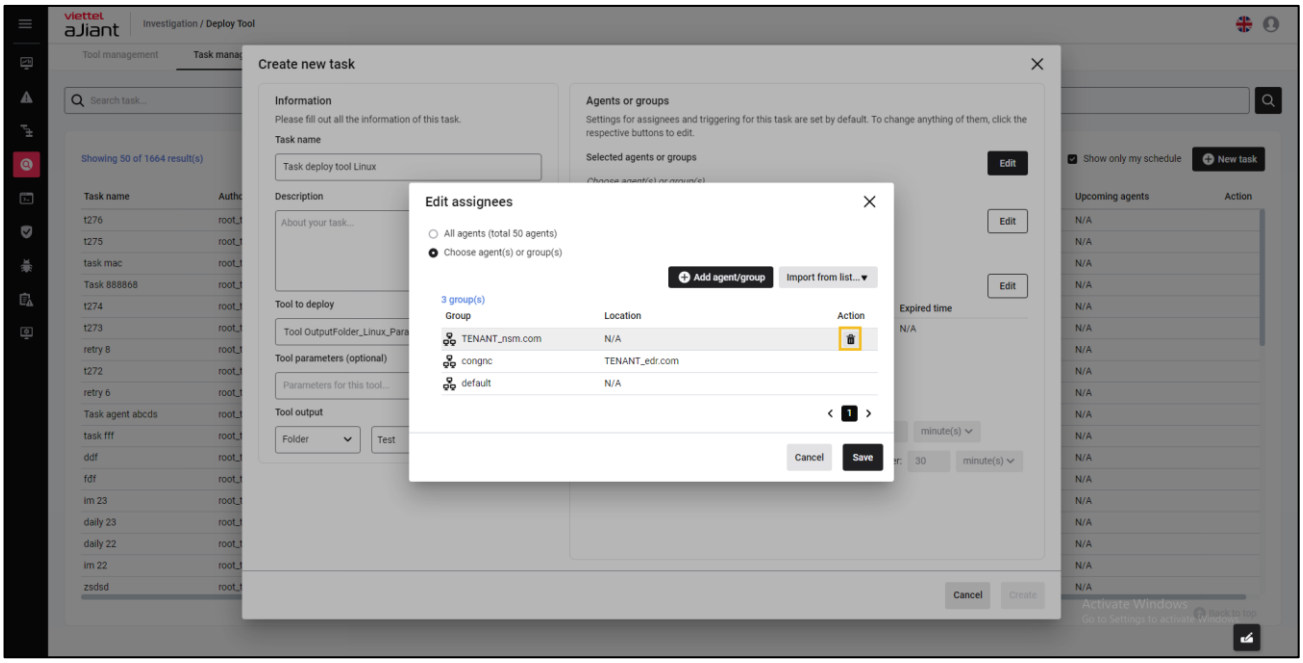
:



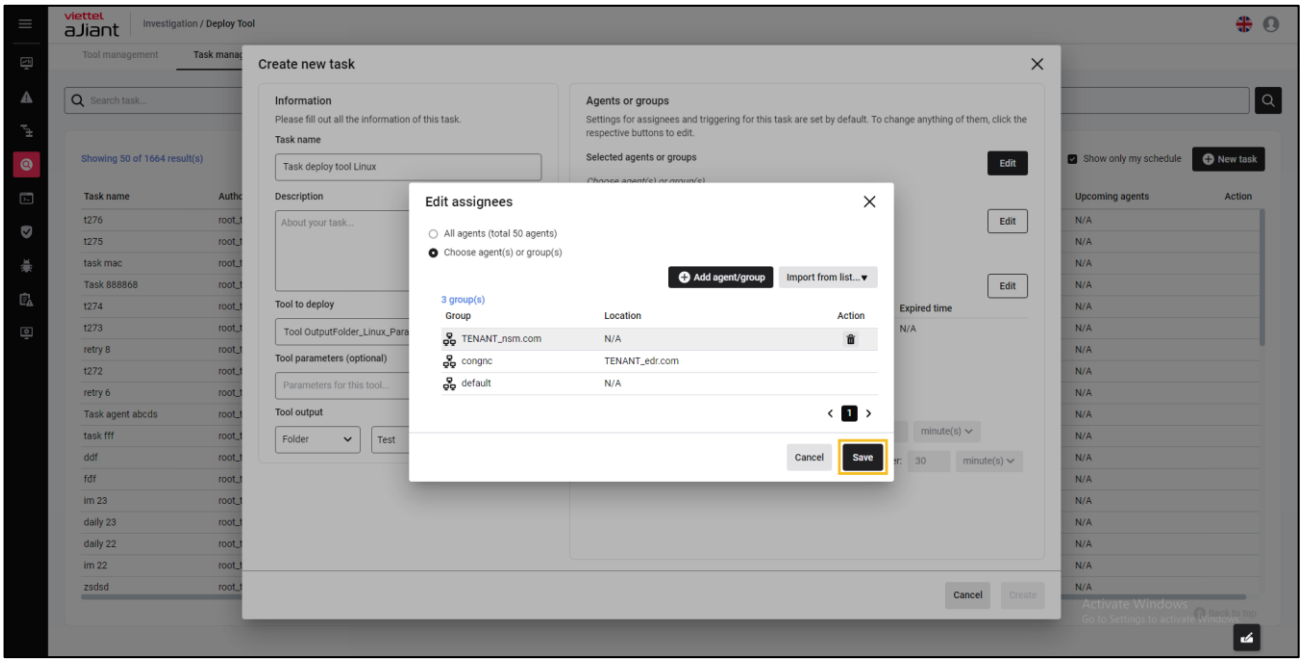
- デプロイするグループを1つまたは複数選択してください > 選択したグループの情報は「Selected」欄に表示されます > グループの追加をキャンセルする場合は「Cancel」を選択し、グループリストを確定する場合は「Save」ボタンを押してください。



  - 選択したグループにカーソルを合わせ > アイコンを選択して、選択リストからグループを削除します。



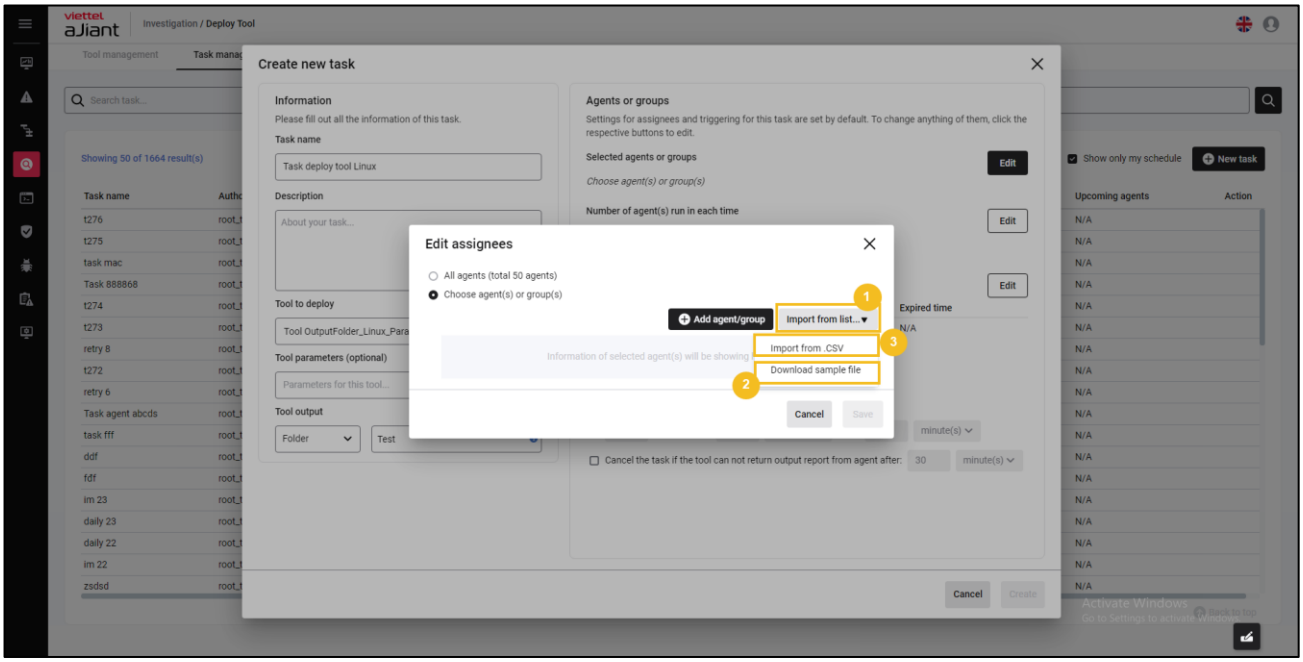
- キャンセルを選択して中止するか、選択したグループを保存してデプロイしてください。



+ リストからインポート：.csvファイルからエージェントのリストをアップロード可能 >「リストからインポート」を選択してください。

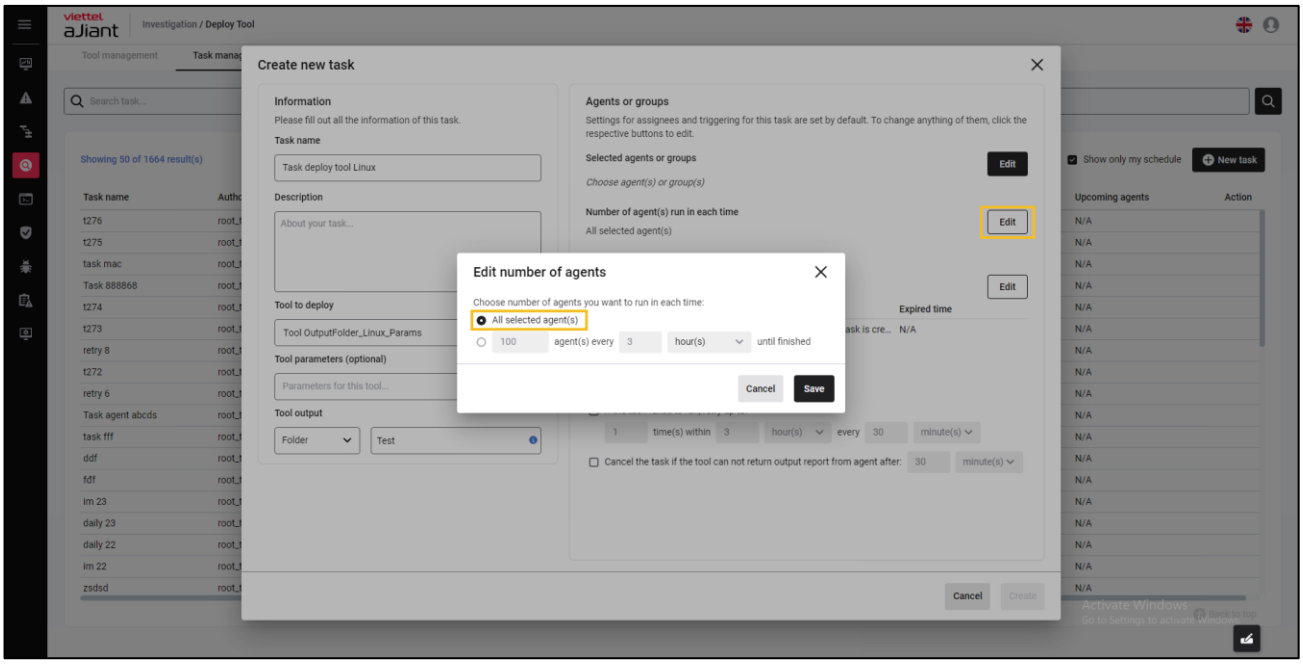
- サンプルファイルをダウンロードして、エージェントファイルのリストフォームを取得してください。

- エージェント情報を入力し、「.CSVからインポート」を選択してエージェントリストをアップロードしてください。

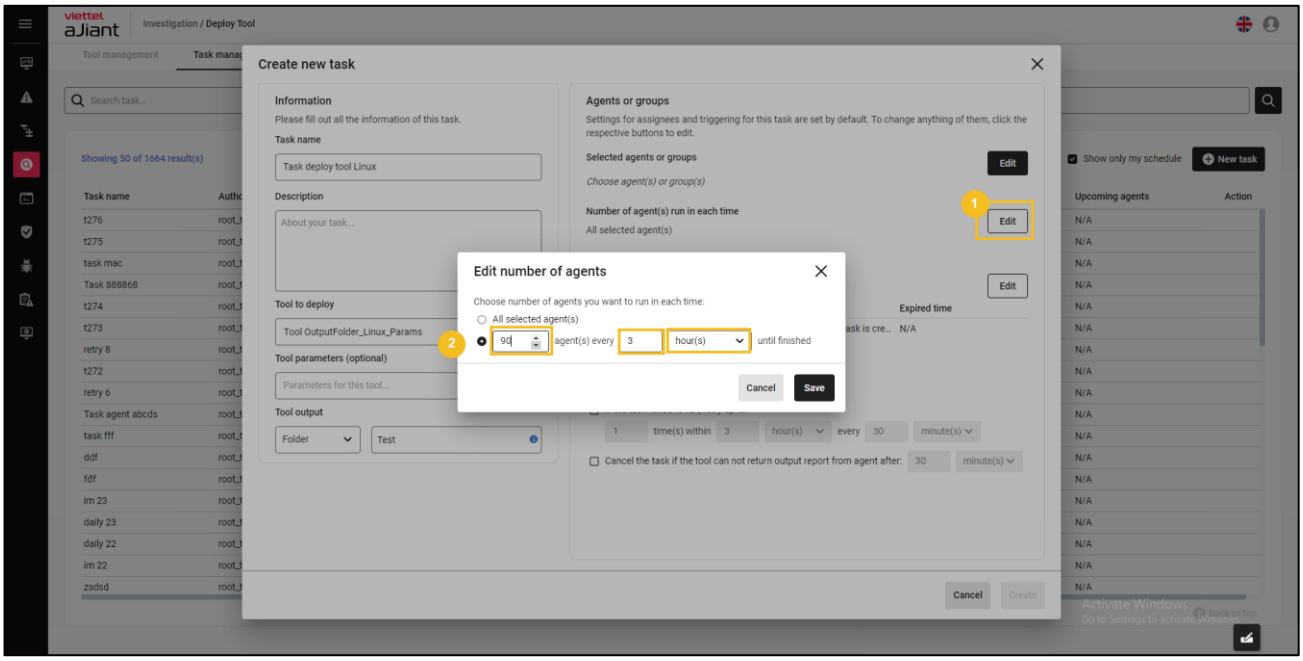


- ツールを一度にデプロイするエージェントの数の設定：

+ 全エージェント：選択したすべてのユーザーエージェントのデプロイを許可する

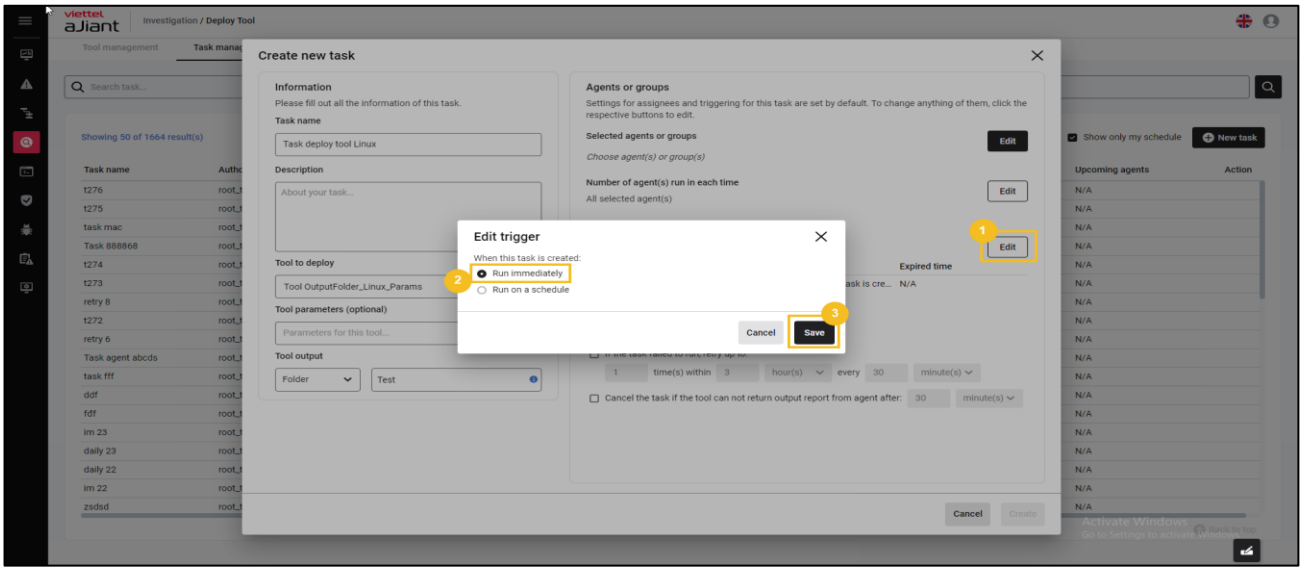


+ デプロイごとのエージェント数の設定：



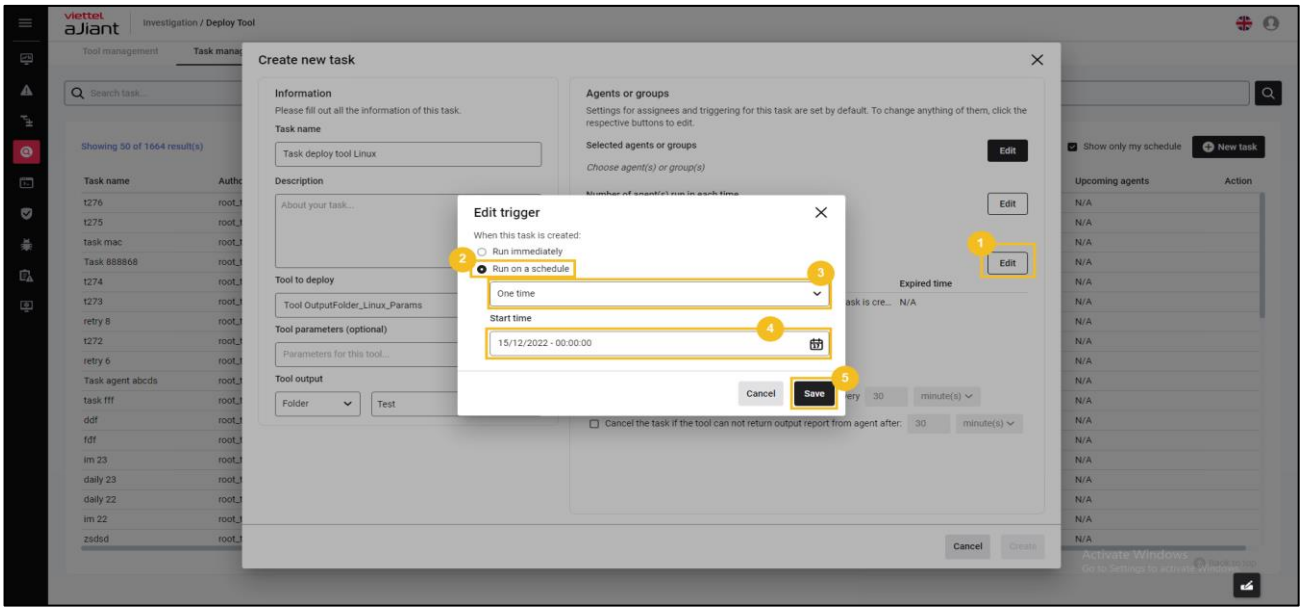
- デプロイツールの実行スケジュール設定：

+ 「Run immediately」を選択すると、タスク作成後すぐにデプロイツールのスケジュール設定が実行されます。

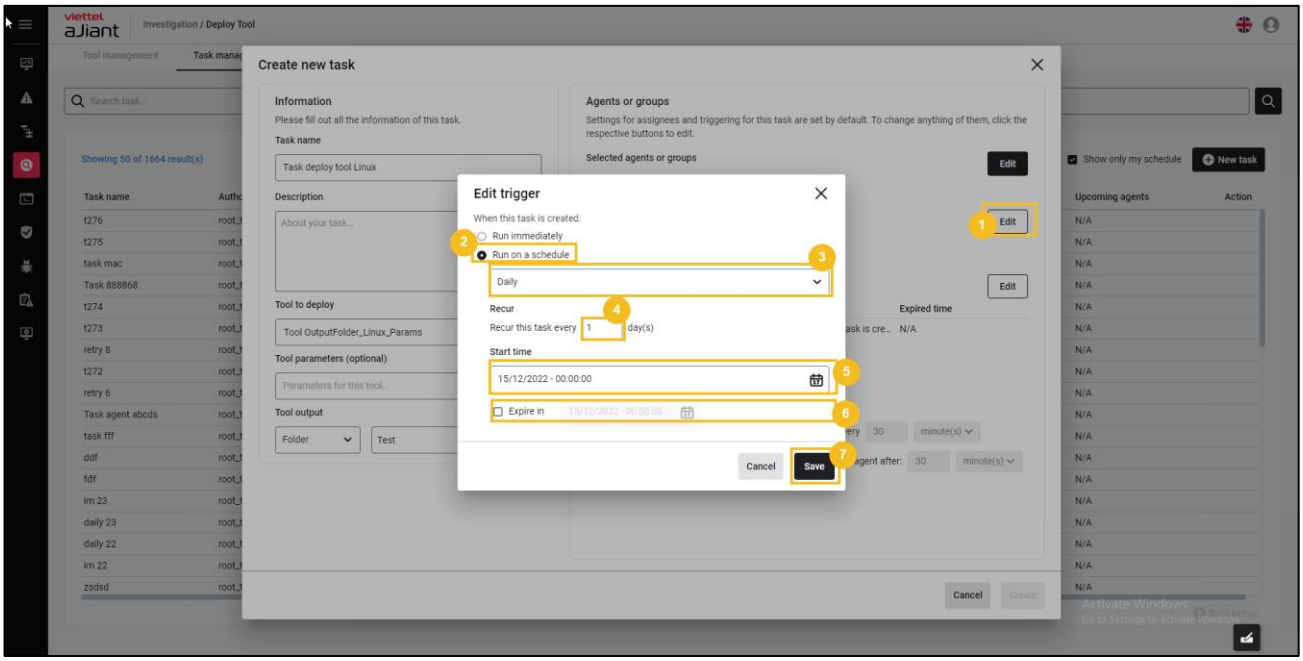


+ 「Run on schedule」を選択して、ツールのデプロイ時間のスケジュール設定を行います。

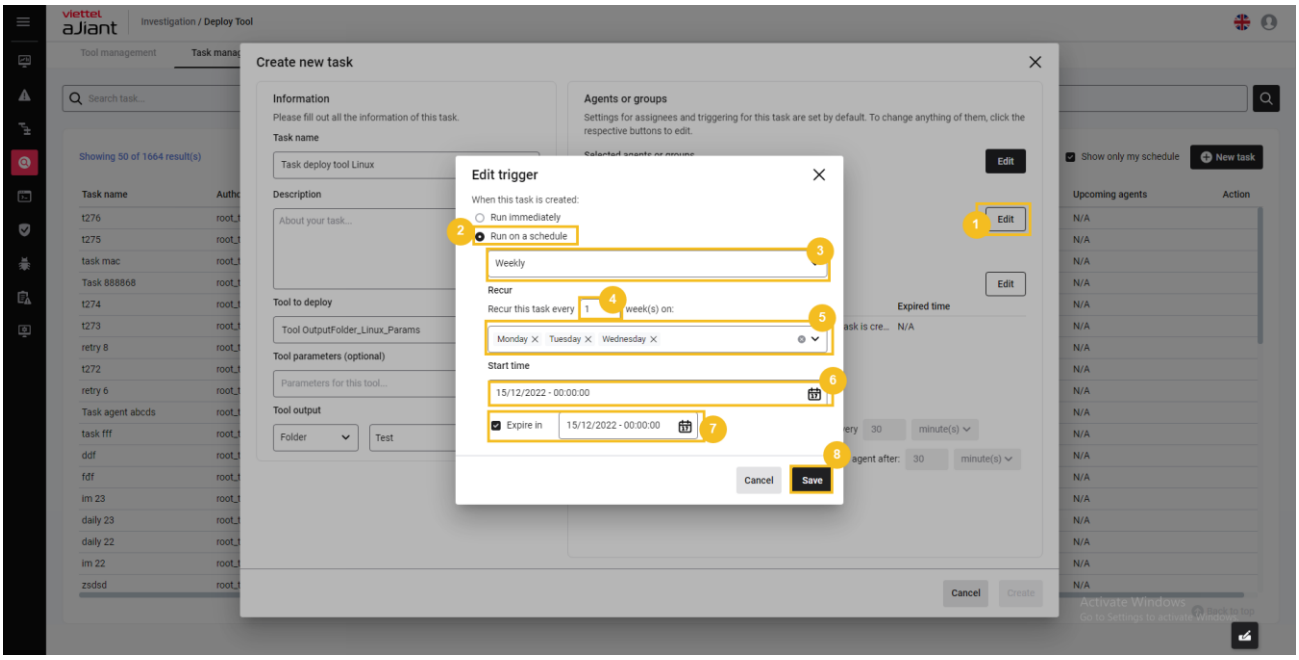
- スケジュールを「一回限り」に選択してください。
  - ツールのデプロイスケジュールを一度だけ設定できるようにする。
  - 開始時間の設定：



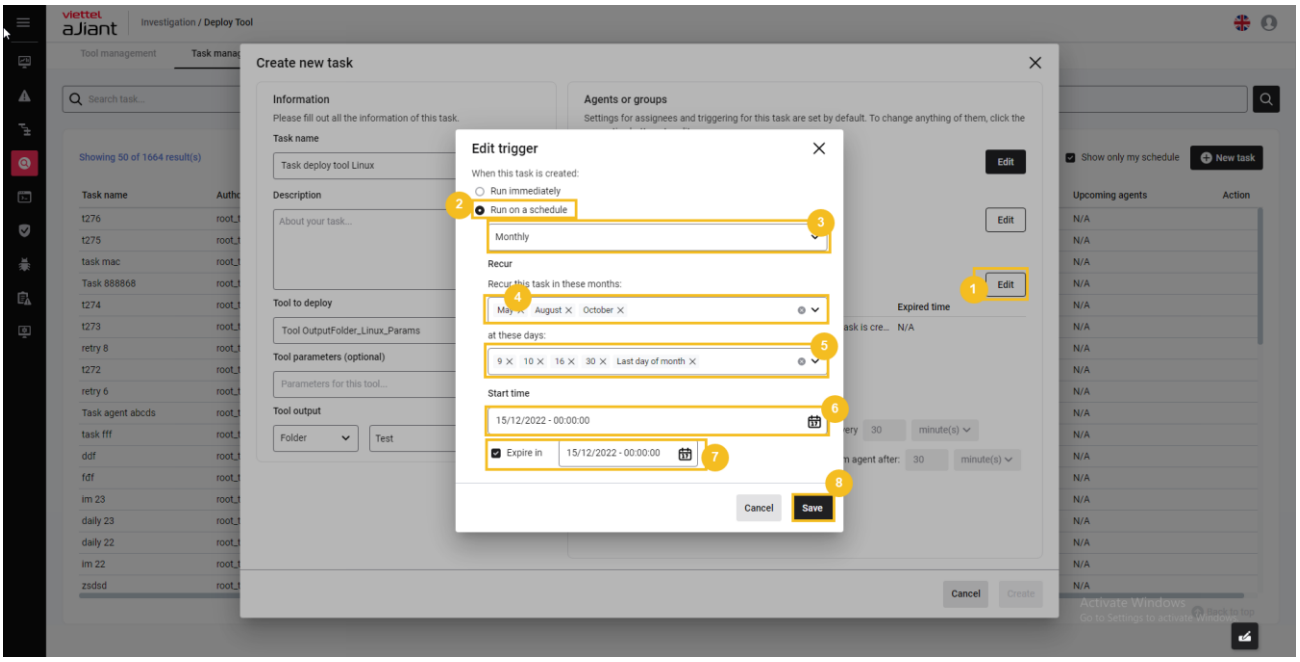
- スケジュールを「毎日」に設定してください。
  - ツールの毎日のデプロイスケジュールを許可する。
  - 繰り返し時間;
  - 開始時間と終了時間の設定：



- スケジュールを「週次」に選択してください。
  - 週次でのデプロイツールのスケジューリングを許可する。
  - 繰り返し時間;
  - 開始時間と終了時間の設定：



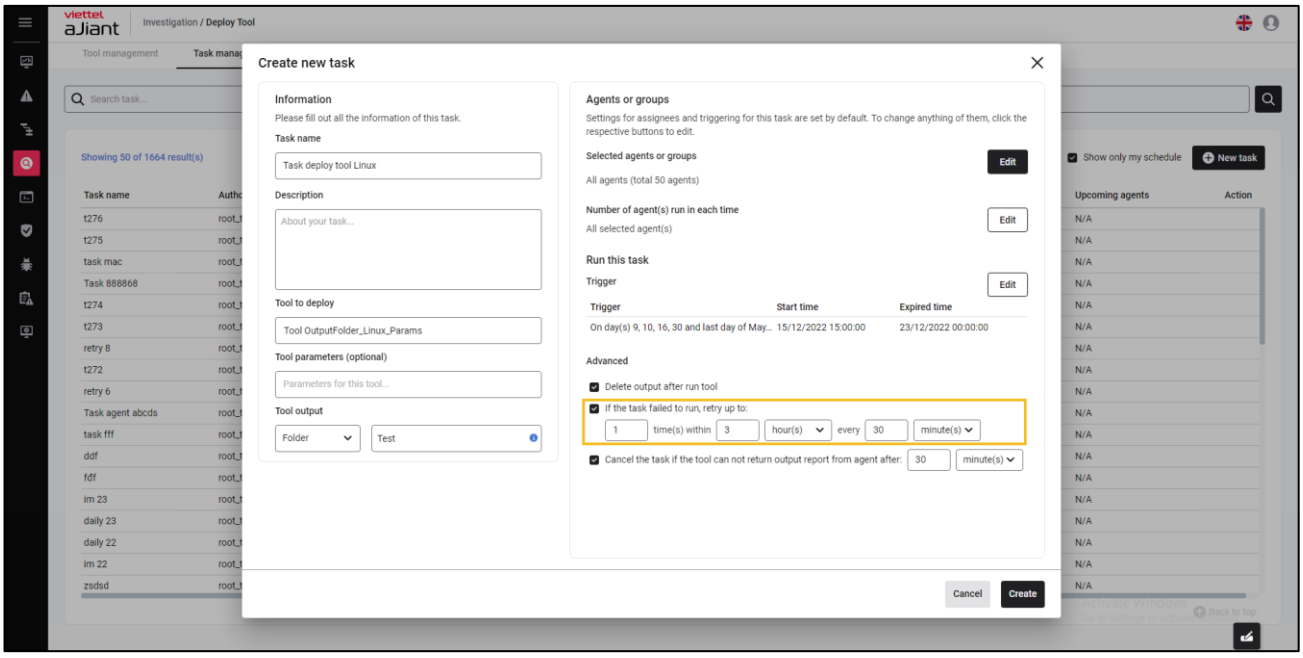
- スケジュールを「毎月」に選択してください。
  - 毎月のデプロイツールのスケジュール設定を許可する。
  - 繰り返し時間;
  - 開始時間と終了時間の設定：



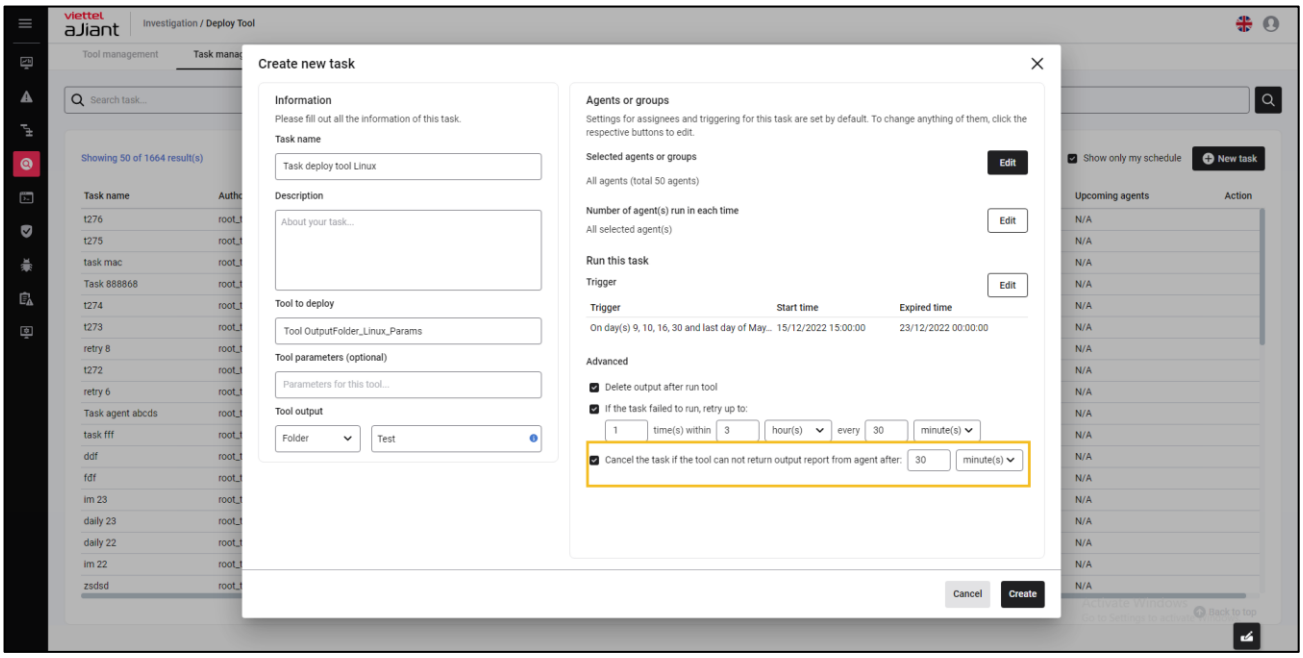
- **タスクの詳細設定の構成**

+ 「Delete tool after run tool」は、ツール実行後にツールの出力を削除し、正常にバックエンドへ結果を返すことを許可します。

+ タスクの実行に失敗した場合、タスクのデプロイが失敗するまで最大で再試行を行い、タスクの再デプロイに関する再試行情報の設定を許可する。



+ ツールがエージェントから出力レポートを返せない場合は、ユーザーが設定した時間内にタスクが実行できない場合にタスクのキャンセルを許可してください。



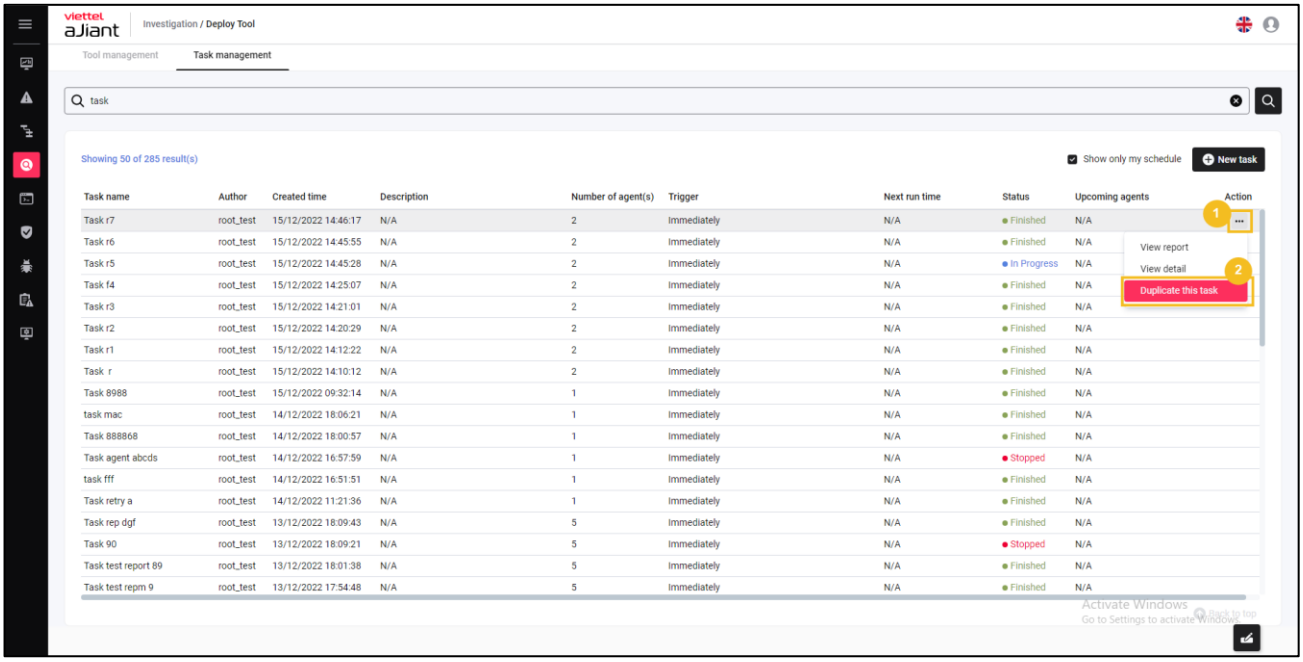
「Create」を選択して新しいタスクを作成するか、エージェント下のデプロイツール情報を設定します。キャンセルする場合は「Cancel」を選択してタスクの作成やエージェント下のデプロイツール情報の設定を中止してください。

d. タスクの複製

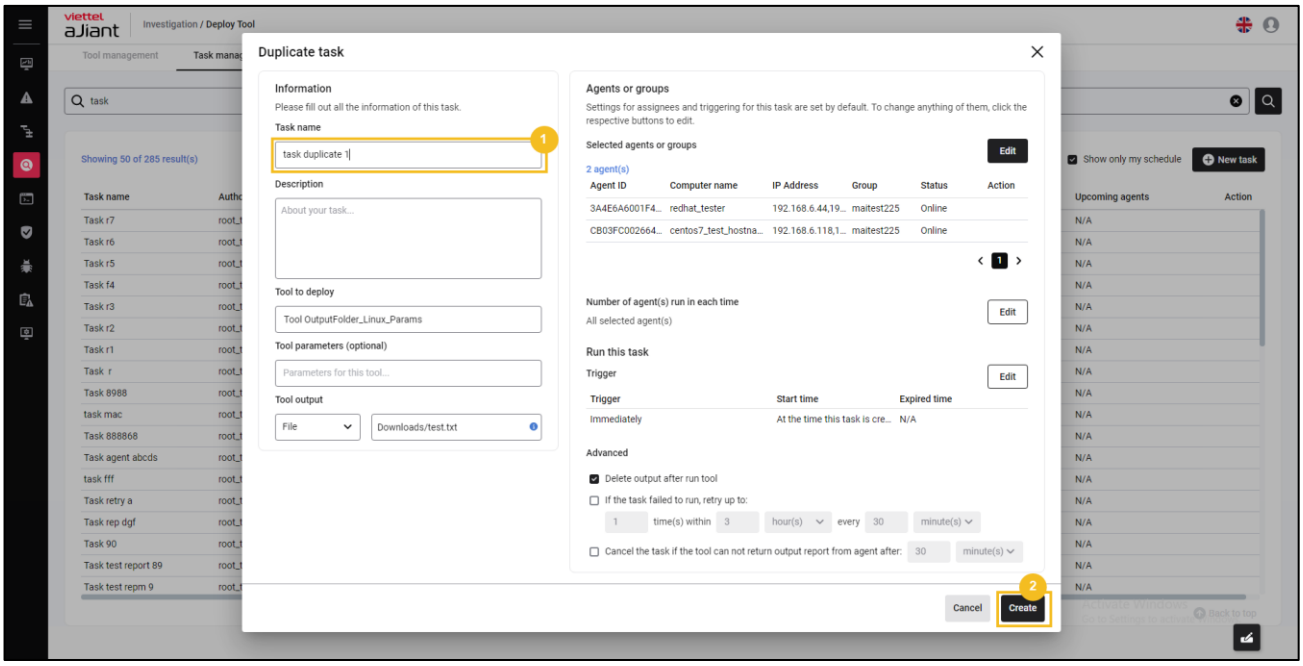
目的：タスクの複製を可能にし、元のタスクの値を自動的に入力しますが、タスク名の欄は除きます（ユーザーにタスク名の入力または修正を求めます）。

実施手順：

- ツール一覧画面で、複製したいツールにカーソルを合わせ > 選択 > 「このタスクを複製」を選択してください。



- タスク名を入力し、タスク情報を確認・更新してください。設定を完了するには「作成」を選択し、タスクの複製操作をキャンセルするには「キャンセル」を選択してください。



e. 今後のエージェント一覧

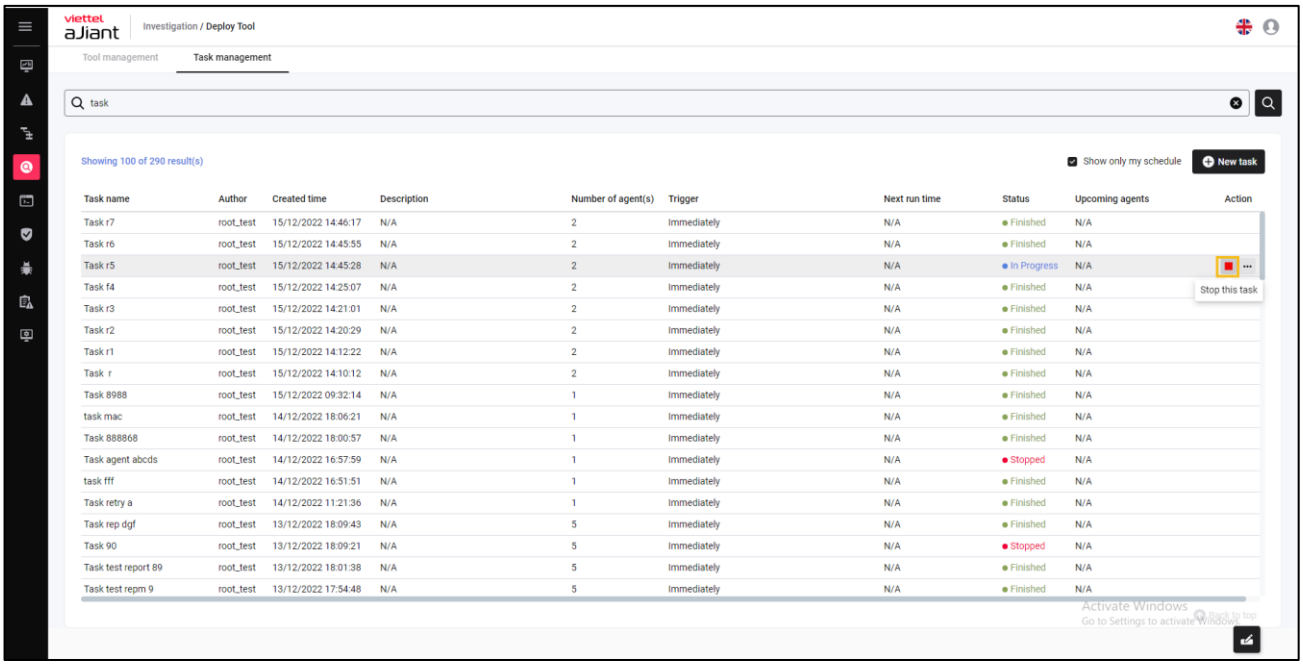
目的：ツールがまもなくデプロイされるエージェントの一覧を表示できるようにすること。

実施手順：タスクリスト画面で「今後のエージェント一覧」を選択します。

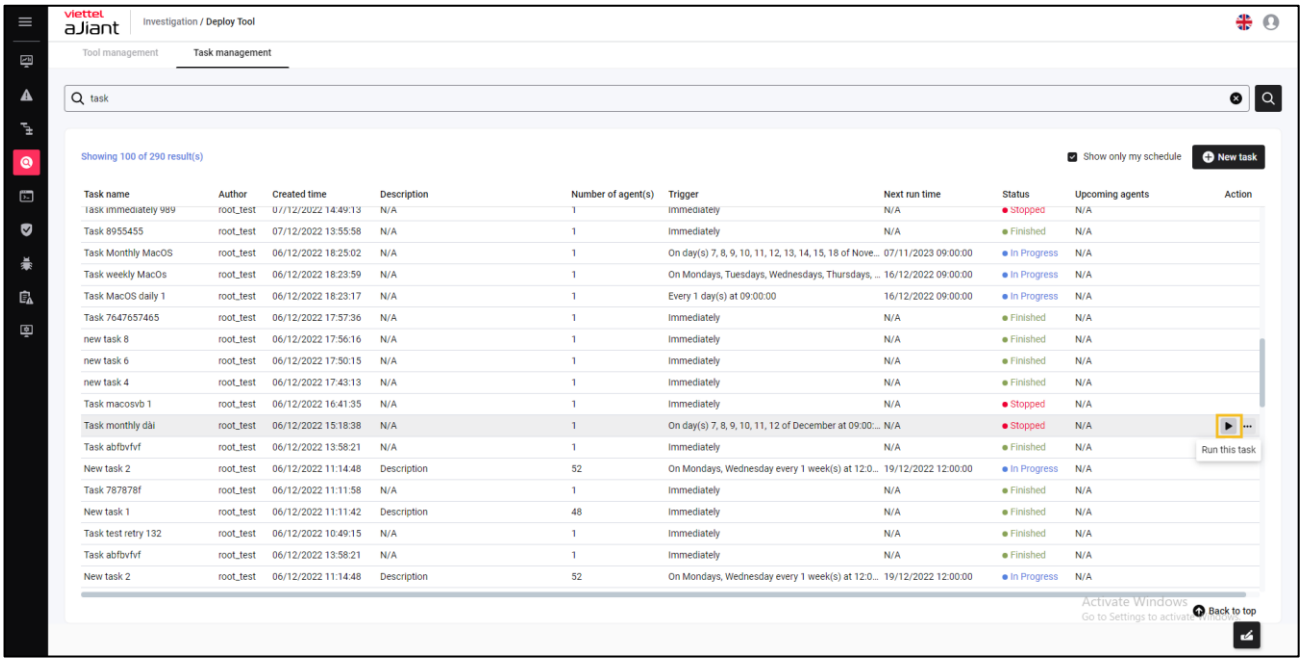
f. タスクの停止／開始

目的：タスクの停止および再起動を可能にする（デプロイタスクの停止または一時停止したタスクの再デプロイ）。

タスク一時停止の手順：タスクリスト画面で、一時停止したいタスクにカーソルを合わせる > タスクを一時停止するためのアイコンを選択する：



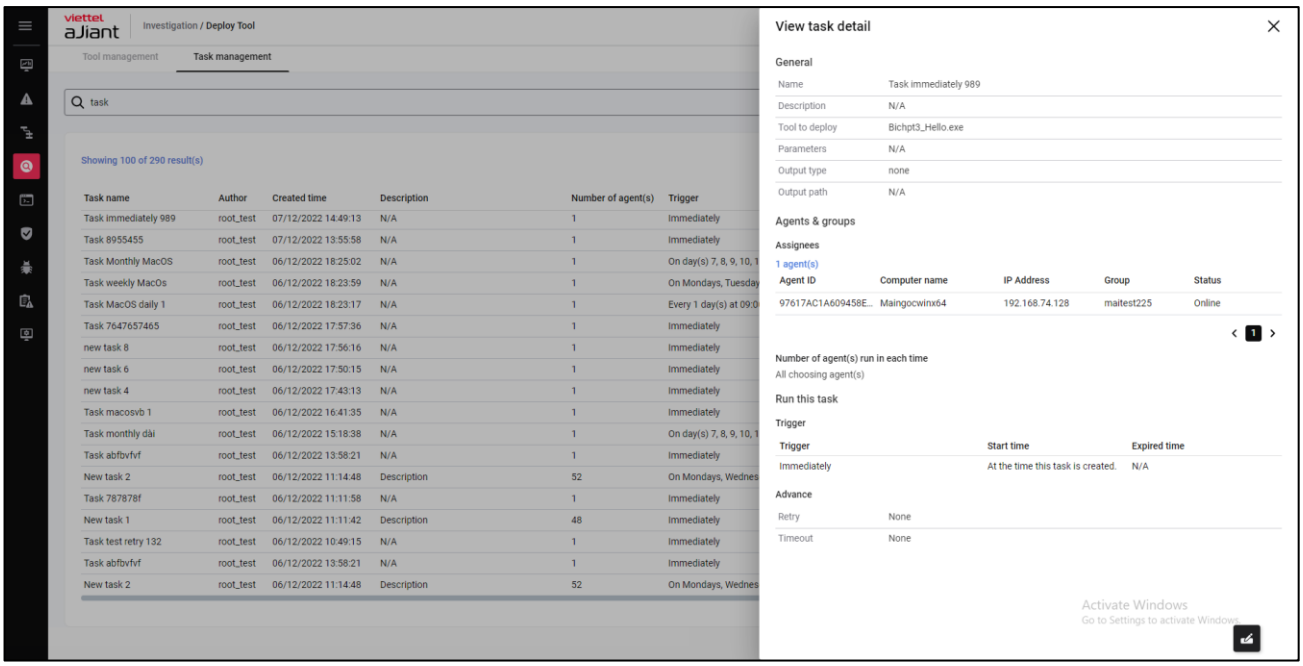
タスクを再デプロイする手順（停止中のタスクの場合）：タスクリスト画面で、再デプロイしたいタスクにカーソルを合わせ、再デプロイアイコンを選択してください。



g. タスクの詳細

目的：タスクの詳細情報を閲覧できるようにすること。

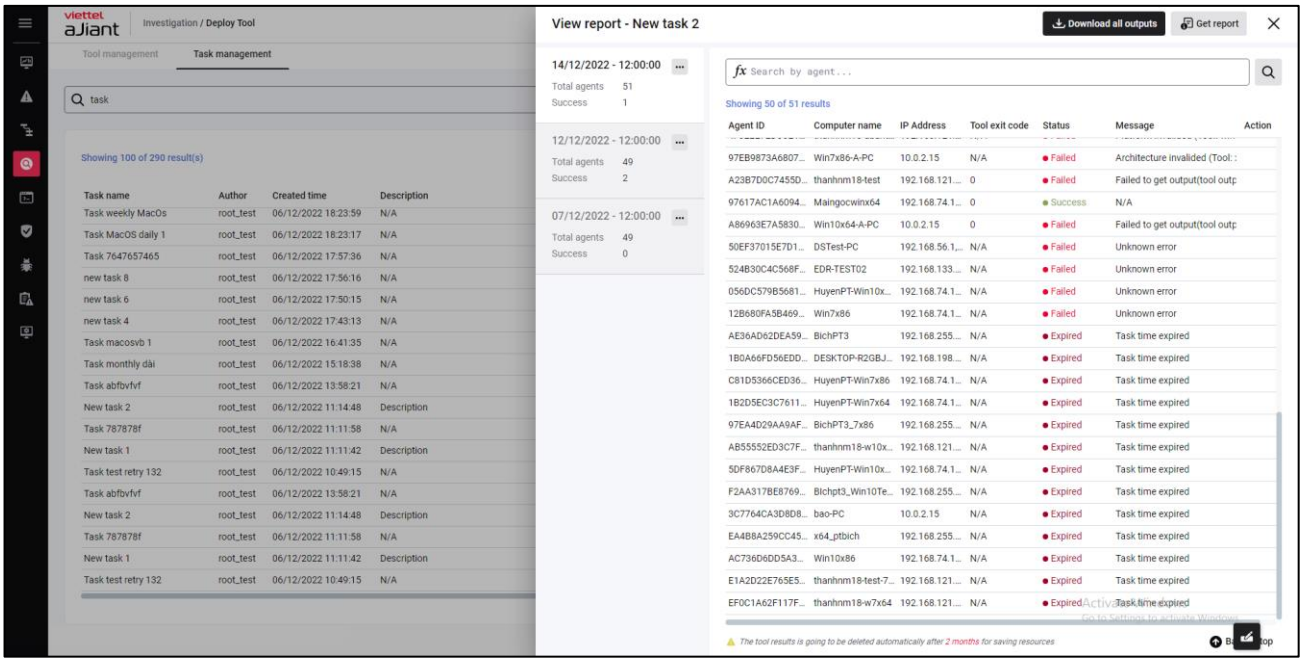
実施手順：タスクリスト画面で、詳細を確認したいタスクにカーソルを合わせる ＞「詳細を見る」を選択してください。



h. レポートを見る（ツール結果を表示）

目的：デプロイツールの報告結果を確認すること。

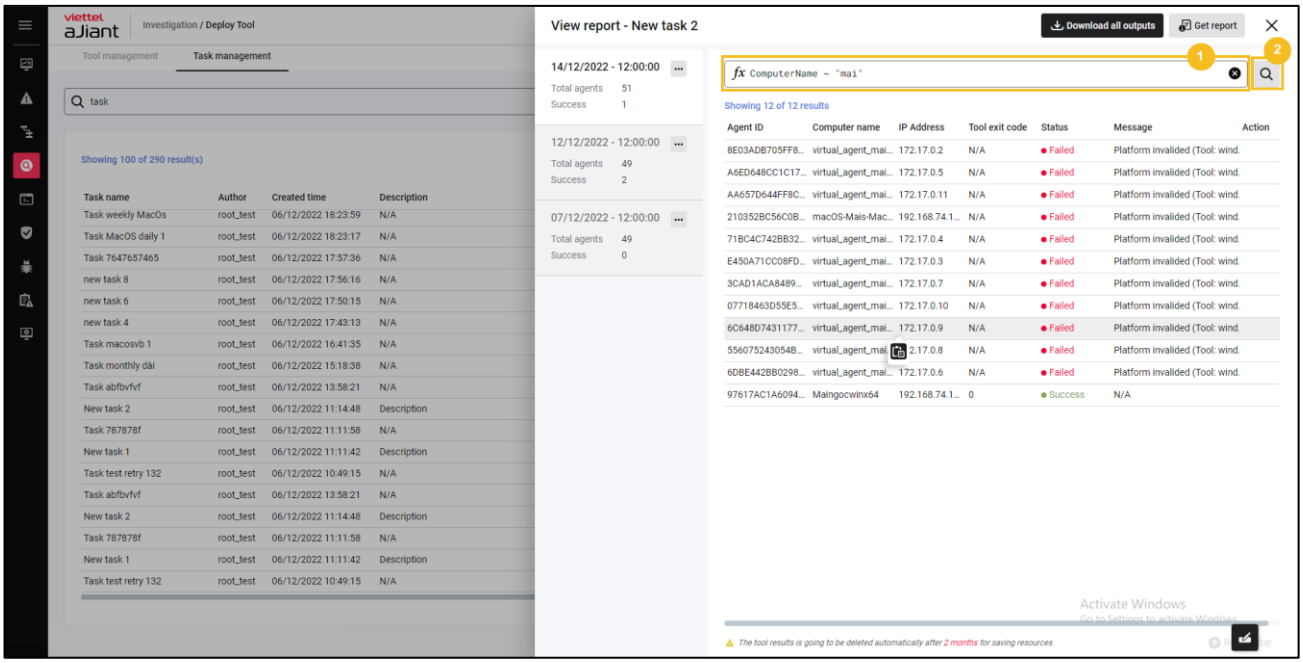
実施手順：タスクリスト画面で、詳細を確認したいタスクにカーソルを合わせ ＞「レポートを見る」を選択してください。



+ デプロイツールの結果を以下のクエリコマンドで検索してください：

  - 目的：クエリ文に基づいてデプロイツールの結果を検索できるようにすること。

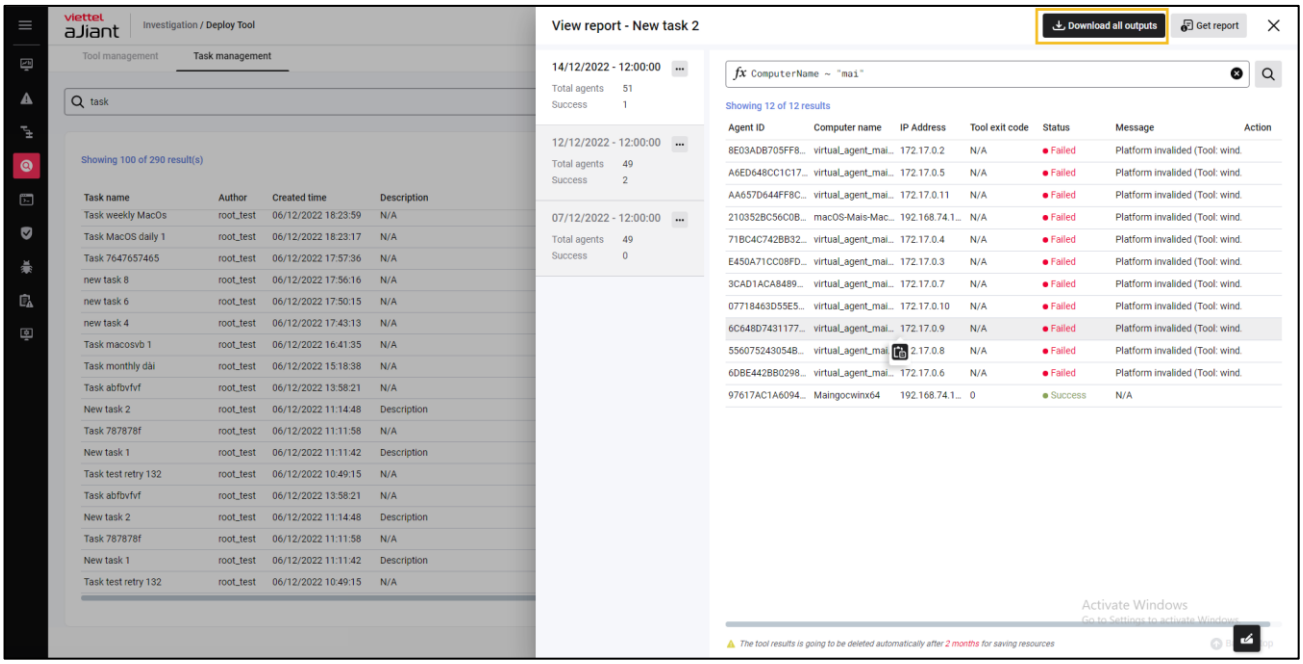
  - 実行手順：検索クエリを入力し、検索ボタンを選択するか、キーワードの入力を終了してEnterキーを押します。システムは、検索キーワードに関連する情報をシステム内で検索します。



+ スケジュールされたタスクに基づくデプロイツールの全結果をダウンロードしてください：

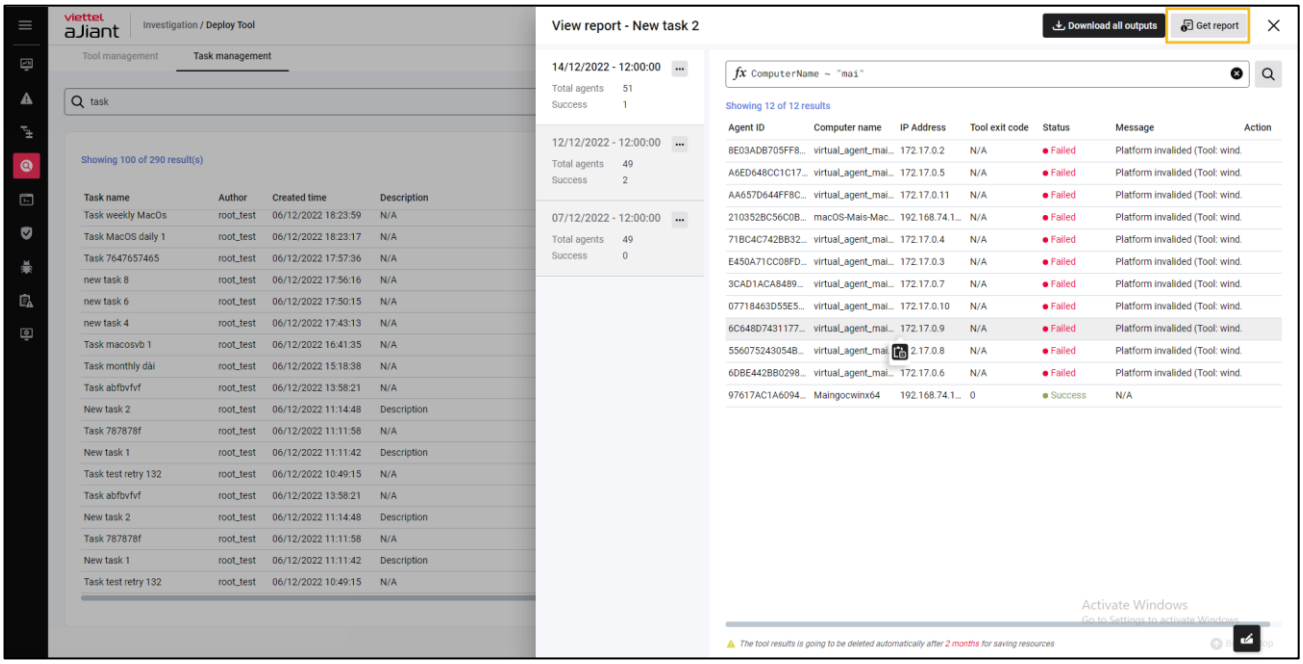
- 目的：スケジュールされたタスクに基づいて、デプロイツールの全結果をダウンロード可能にすること。

- 実行手順：レポート表示画面で、「すべての出力をダウンロード」ボタンを選択します。



+ すべてのレポートを取得してください。

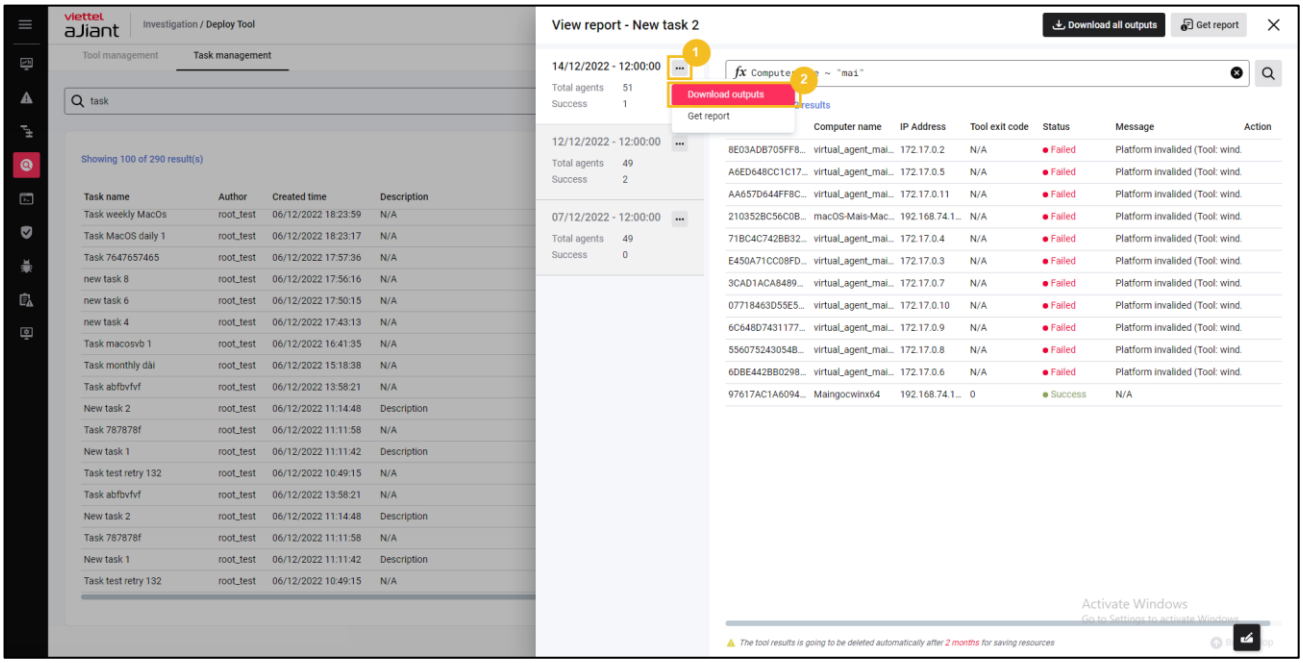
  - 目的：デプロイツールの結果報告リストをすべてダウンロードできるようにすること。
  - 実行手順：レポート表示画面で、「レポート取得」ボタンを選択します。



+ 各スケジューリングの出力をダウンロードする：

- 目的：各スケジュールごとにデプロイツールの結果報告一覧をすべてダウンロードできるようにすること。

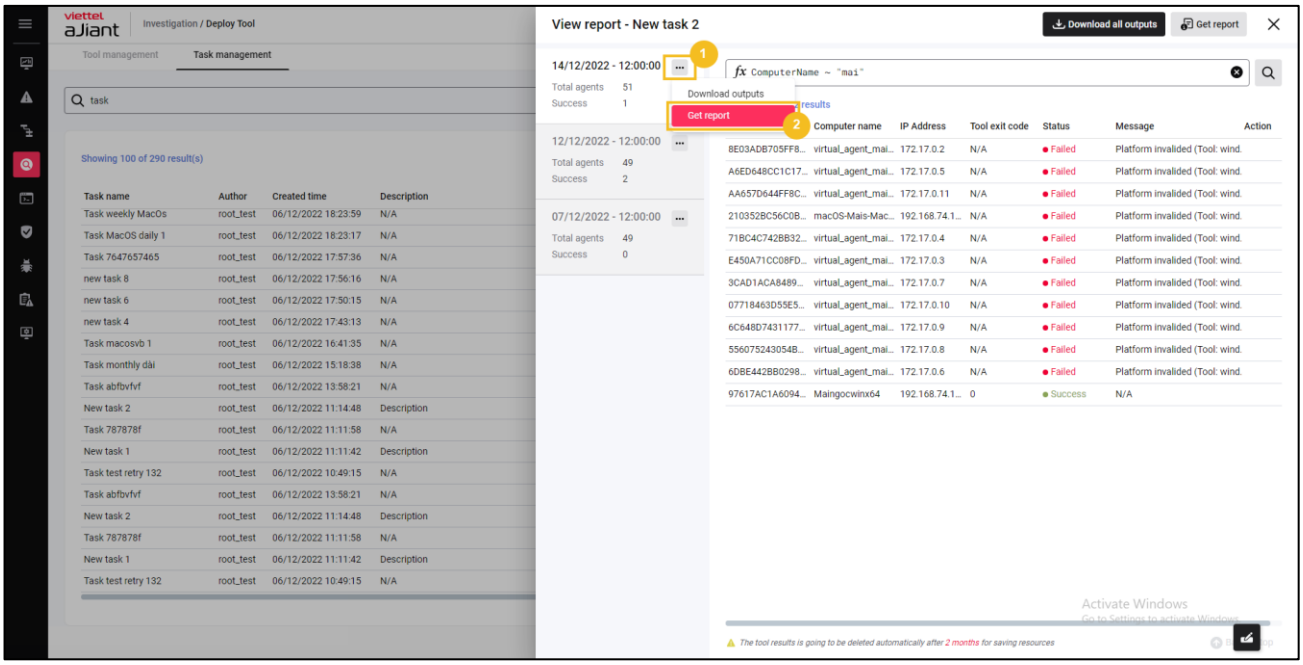
- 実行手順：レポート表示画面で、出力をダウンロードしたいスケジュールレコードのアイコンを選択し、次に「出力をダウンロード」を選択します。



+ 各スケジューリングのレポートをダウンロードする:

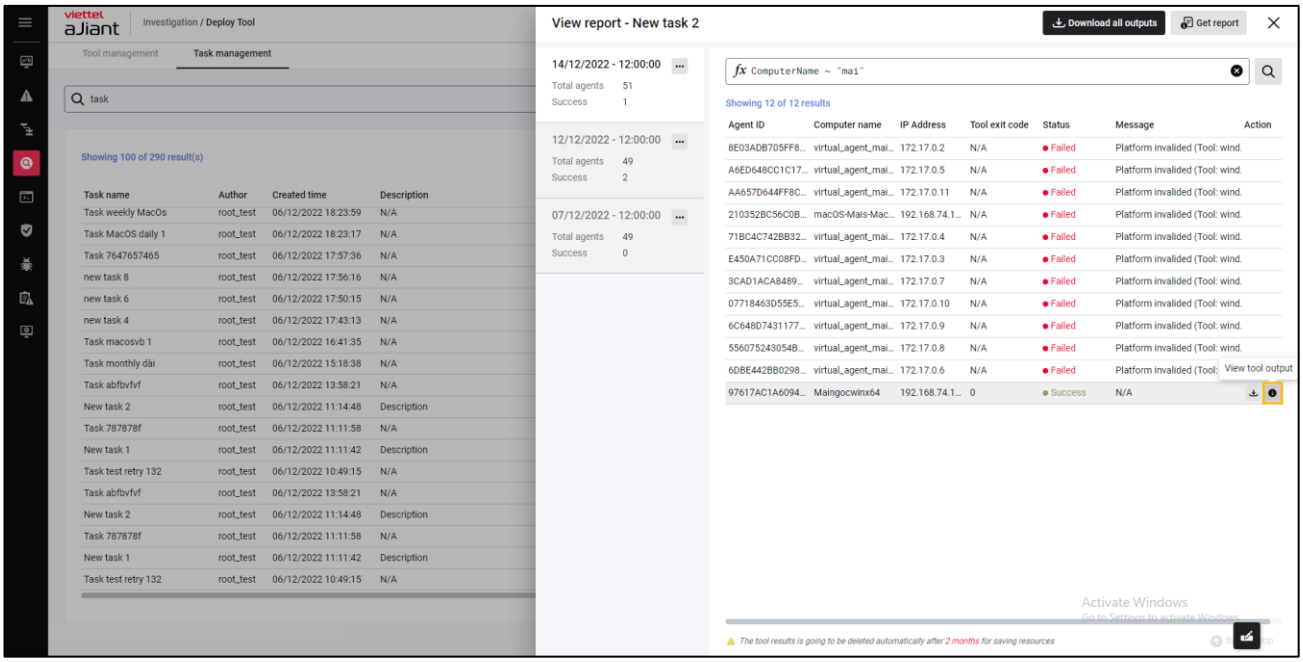
- 目的：各スケジュールごとにデプロイツールの結果報告の統計リストをすべてダウンロードできるようにすること（形式は.csv）。

- 実行手順：レポート表示画面で、レポートをダウンロードしたいスケジュール記録のアイコンを選択し、「レポート取得」を選びます。



+ 各エージェントのツール出力を表示：

  - 目的：ユーザーが各エージェントのツール出力を確認できるようにすること。
  - 実行手順：レポート表示画面で、レポートを確認したい（ステータスが「Success」の）レコードにカーソルを合わせる > アイコンを選択 > 「View tool output」を選択する。

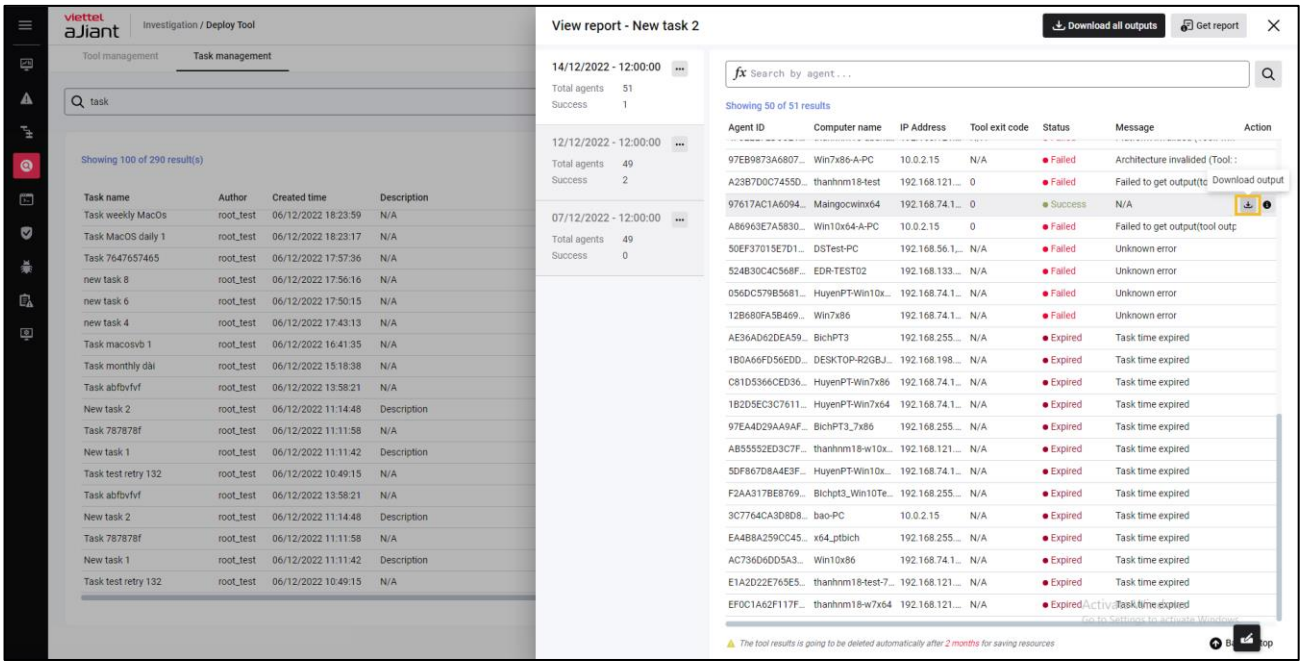


+ 各エージェントのツール展開結果レポートをダウンロードしてください。

  - 目的：各エージェントのデプロイツール結果レポートのダウンロードを可能にすること

。

  - 実行手順：レポート表示画面で、レポートを確認したい（ステータスが「Success」の）エージェントのレコードにカーソルを合わせる > アイコンを選択 >「出力をダウンロード」を選択する



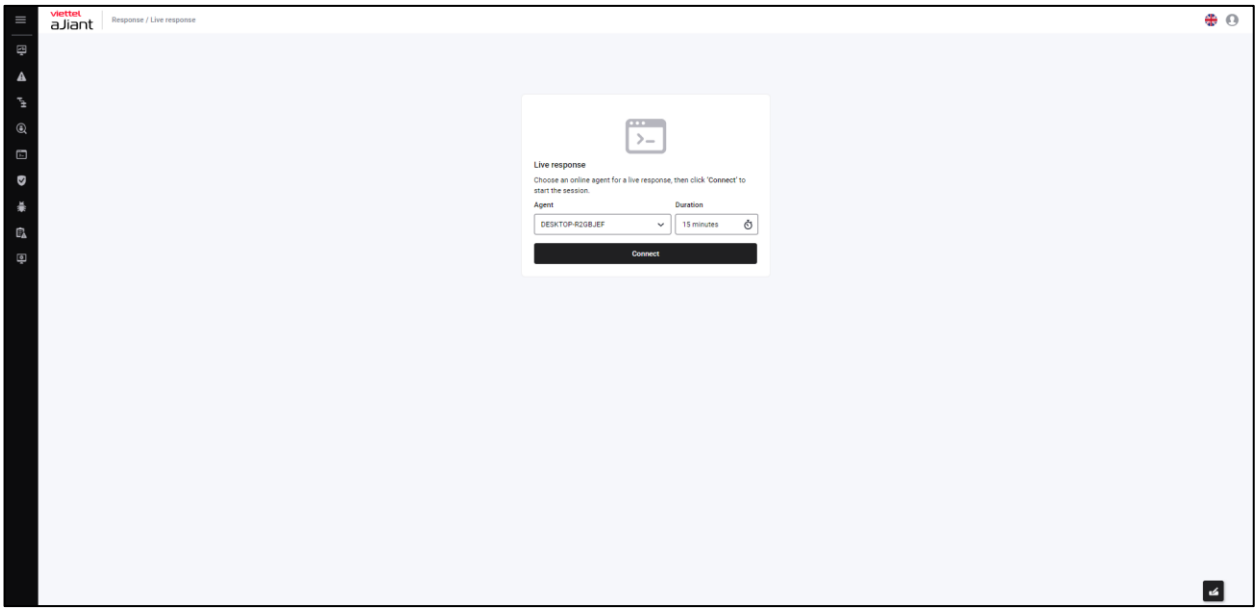
3.5 レスポンス画面

3.5.1 ライブレスポンス

目的：ライブレスポンス機能は、ホスト上の情報取得や要求処理のために、セッション単位でリモートから一連のコマンドを実行する能力を提供します。

ライブレスポンス機能の実行手順：

- 「Response」タブをクリックし、「Live Response」を選択してください。



- 新しいライブレスポンスセッションを作成する。

エージェントを選択：エージェントの一覧を表示する：

+ ユーザーがrootグループに属している場合：システム内の30日未満にアクティブなすべてのエージェントを表示する。

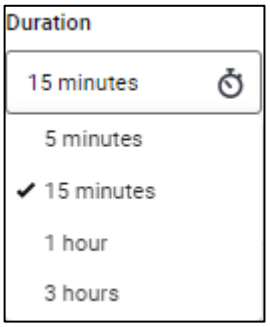
+ ユーザーがデフォルトグループにログインしている場合：デフォルトグループに属するすべてのエージェントを表示する。

+ ユーザーが親グループにログインした場合：ログインしているユーザーのグループおよび対応する子グループに属するすべてのエージェントを表示する。

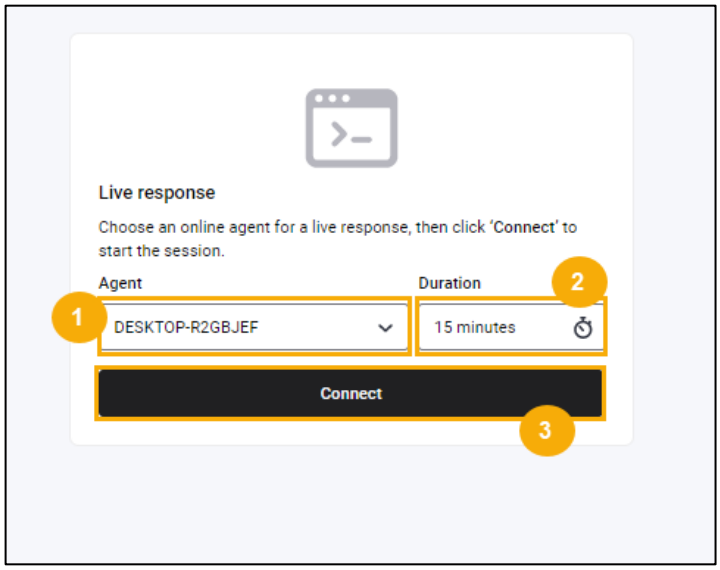
+ ユーザーが属するグループまたは複数のサブグループに対して：ログインしているユーザーのグループに属するすべてのエージェントを表示する。

ユーザーは、オンライン状態のエージェントに対してのみライブレスポンスを実行できます。

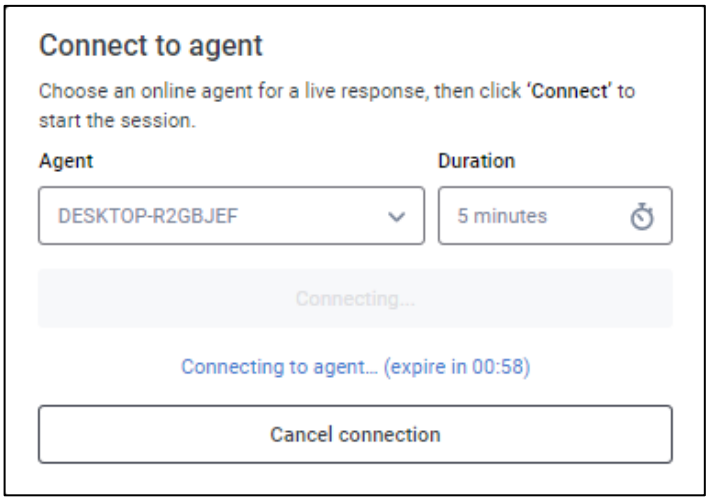
+ Durationを選択してください：5分、15分、1時間、3時間の時間帯があります。



+ 「接続」ボタンをクリックしてください。

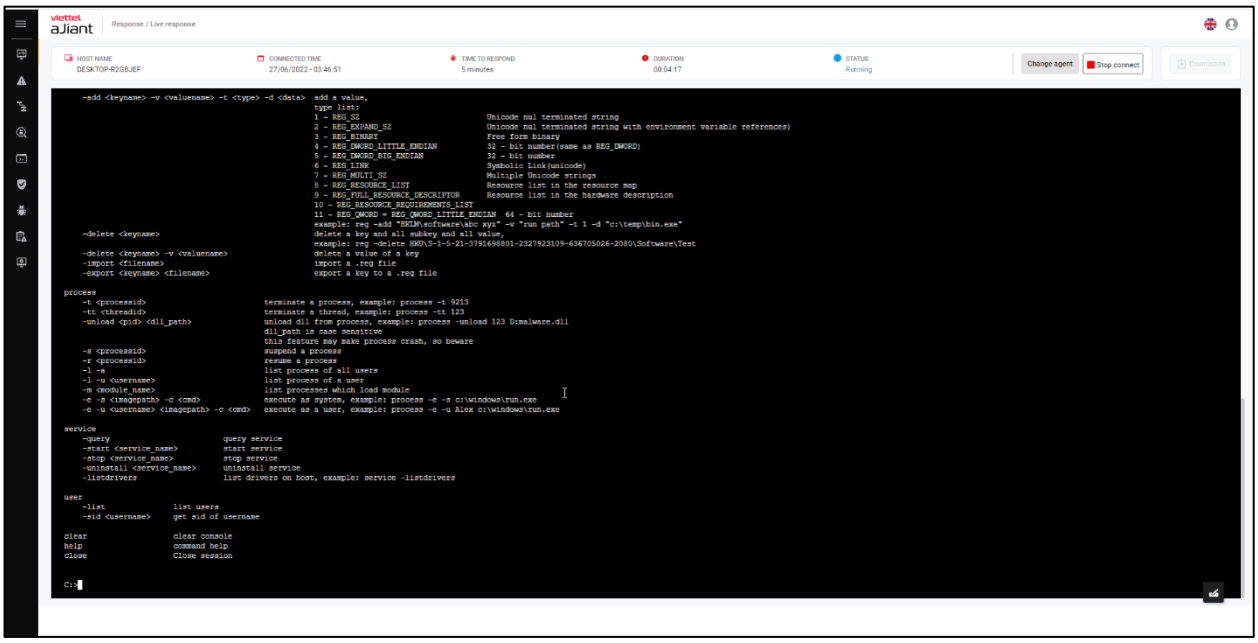


- エージェントへの接続をシステムが行っているため、1分間お待ちください。システムの状態は「接続中」です。

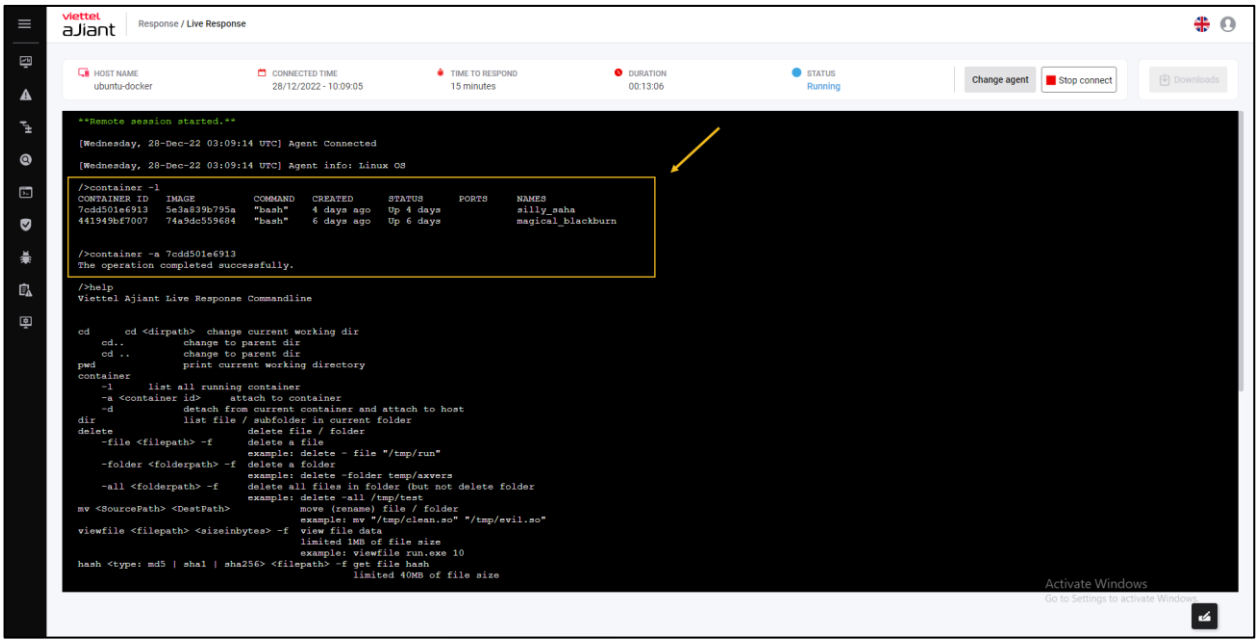


- 接続が成功すると、ユーザーはコンソール画面でコマンドを実行でき、Live Responseセッションの状態は「実行中」となります。

注意：各エージェントは同時に1つのライブレスポンスセッションのみを実行できます。



注意：ユーザーはコンテナのコンソール画面でコマンドを実行することで、コンテナへの接続を行うことができます。



ユーザーはコンソール画面で以下のコマンドを実行できます。

+ ウィンドウ：次のコマンドを実行してください。

番号	コマンド	パラメータ	説明
1	cd	cd <ディレクトリパス>	現在の作業ディレクトリを変更する
		cd.. または cd ..	親フォルダに移動する
2	pwd		現在作業中のフォルダに印刷する
3	ディレクトリー覧	dir [ドライブ:][パス][ファイル名] [/A[[:]属性]] [/O[[:]並べ替え順	現在のフォルダ内のファイルおよびサブフォルダを一覧表示する。

番号	コマンド	パラメータ	説明
		序]] [/T[[:]時間フィールド]] [/L] [/Q] [/R] [/S] [/X]	
		/ A: [-] 属性 指定された属性を持つファイルを表示します。 属性: D ディレクトリ R 読み取り専用ファイル H 隠しファイル A アーカイブ準備済みファイル S システムファイル L 再解析ポイント	
		/L 小文字のファイル名	
		/ O ：[-]sortorder ファイルをソート順で一覧表示します。 sortorder N 名前順（アルファベット順） S サイズ順（小さいものから） E 拡張子順（アルファベット順） D 日時順（古いものから） G ディレクトリを先にグループ化	

番号	コマンド	パラメータ	説明
		- 逆順にするための接頭辞 例：dir /O:N;	
		/ T:timefield 表示する時間フィールドを選択してください timefield C 作成日時 M MFT作成日時 A 最終アクセス日時 W 最終更新日時 例：dir /T:A - 属性を除外する接頭辞 例：dir /A:D-AH	
		/Q ファイルの所有者を表示します。 例：dir /Q	

番号	コマンド	パラメータ	説明
		/R ファイルの代替データストリームを表示します。 例：dir /R	
		/S 指定したディレクトリおよびすべてのサブディレクトリ内のファイルを表示します。 例：dir /S	
		/ X これは8.3形式でないファイル名に対して生成された短縮名を表示します。 例：dir /X	
4	削除する	delete –file <パス> 例： delete -file "c:\temp\runpath.exe"	ファイルを1つ削除する

番号	コマンド	パラメータ	説明
		delete -folder <フォルダパス> 例： delete -folder temp\axvers	フォルダを削除する
		delete –all <フォルダパス> 例： delete –all c:\temp	フォルダ内のすべてのファイルおよびサブフォルダを削除する（フォルダ自体は削除しない）
5	移動する	<SourcePath> <DestPath> ファイルまたはフォルダを移動（名前変更）する 例： 例：mv "c:\temp\clean.exe" "c:\temp\evil.exe"	ファイル/フォルダーの移動を許可する
6	ファイルを表示する	<ファイルパス><サイズ（バイト）>	ファイル内のデータを表示する（ファイルサイズの制限あり）
7	ハッシュ	ハッシュ <タイプ: md5 | sha1 | sha256> <ファイルパス> -f ファイルのハッシュを取得する 例: hash md5 c:\test\run.exe	最大1MBのファイルの暗号化を許可します。 -fオプションは、ファイルが他のプロセス

番号	コマンド	パラメータ	説明
			によって開かれている場合でも強制的にファイルを開きます。
8	ダンプ		プロセスのダンプを許可します。ダンプファイルのパスを省略した場合、デフォルトで <processname>_<datetime>.dmp となります。
		-process -pid <プロセスID> [-f <保存先パス>] プロセスIDでプロセスをダンプする 例: dump -process -pid 452 -f "C:\Users\Evil_dumped.dmp"	プロセスIDによるダンプ処理
		-process -name <プロセス名> [-f <保存先パス>] プロセス名でプロセスをダンプする 例: dump -process -name Evil.exe -f "C:\Users\Evil_dumped.dmp"	プロセス名によるダンプ処理

番号	コマンド	パラメータ	説明
		-process -path <プロセスパス> [-f <保存先パス>] プロセスパスによるプロセスのダンプ 例：dump -process -path "C:\Users\Evil.exe" -f "C:\Users\Evil_dumped.dmp"	プロセスパスによるダンプ処理
9	取得する	申し訳ありませんが、ファイルの内容を直接処理することはできません。翻訳したいテキストをこちらにご提供いただけますか？	ホストからサーバーへ1つのファイルをアップロードする
10	置く	<url><folderpath>	ホストマシンに1つのファイルをダウンロードする
11	ディレクトリを作成する	<ディレクトリ名>	フォルダを作成する
	登録		レジストリに関連するコマンド

番号	コマンド	パラメータ	説明
1 2		クエリ <keyname> -v <valuename> 例: reg-query "HKLM\Software\abc xyz" -v "run path"	1つのキーの値データをクエリする
		クエリ <keyname> -s 例: reg-query "HKLM\Software\abc xyz" -s	すべてのサブキー、値、およびデータをクエリする。
		<keyname>を追加する 例： reg-add "HKLM\software\abc xyz"	キーを1つ追加してください。
		<keyname> -v <valuename> -t <type> -d <data> を追加します 例： reg-add "HKLM\software\abc xyz" -v "run path" -t REG_SZ -d "c:\temp\bin.exe"	値を1つ追加してください。

番号	コマンド	パラメータ	説明
		<keyname> を削除する 例: reg -delete HKU\S-1-5-21-3791698801-2327923109-636705026-2080\Software\Test	1つのキーとそのすべてのサブキーおよび値を削除する。
		<keyname> -v <valuename> を削除する	キーの値を1つ削除する
		<ファイル名>をインポートする	.regファイルを1つインポートする
		export <キー名> <ファイル名>	1つの.regファイルをエクスポートする
13	プロセス		プロセスに関連するコマンド
		-t <プロセスID>	実行中のプロセスをプロセスIDで終了する
		-s <プロセスID>	プロセスを一時停止する
		-r <プロセスID>	以前に一時停止されたプロセスを復元する。

番号	コマンド	パラメータ	説明
		-l -a	すべてのユーザーのすべてのプロセスを一覧表示してください。
		-l -u <ユーザー名>	あるユーザーのプロセスを一覧表示する。
14	サービス		サービスに関連するコマンド
		クエリ	ホストマシンで実行中のサービスを一覧表示してください。
		-<servicename>を開始する	サービスを1つ開始する
		-<servicename> を停止する	サービス1を停止する
		-uninstall <service_name> サービスをアンインストールする	サービスのアンインストール
		-listdrivers ホスト上のドライバーを一覧表示します。例：service -listdrivers	ホスト上のドライバー一覧を表示する

番号	コマンド	パラメータ	説明
15	ユーザー	-リスト	コンピュータ上のユーザーを一覧表示してください。
		-sid<ユーザー名>	ユーザー名のSIDを取得する
16	グレップ	grep -t <テキスト> <パラメータ> <コマンド>	コマンドで指定された語句またはフレーズに基づく検索機能のサポート
17	クリアスクリーン		コンソール画面をクリアする
18	助けてください。		ヘルプコマンド
19	クリア		コンソールをクリアする
20	閉じる		セッションを終了する
21	コンテナ	- l	コンテナの一覧を作成してください。
		-a <コンテナID>	各コンテナへの接続

番号	コマンド	パラメータ	説明
		申し訳ありませんが、翻訳するためのテキストを提供してください。	コンテナの接続を切断する

+ Ubuntu：次のコマンドを実行してください。

番号	コマンド	パラメータ	説明
1	cd	cd <ディレクトリパス>	現在の作業ディレクトリを変更する
		cd.. または cd ..	親フォルダに移動する
2	pwd		現在作業中のフォルダに印刷する
3	ディレクトリ一覧	現在のフォルダー内のファイルおよびサブフォルダーの一覧を表示する	現在のフォルダ内のファイルおよびサブフォルダを一覧表示してください。
4	削除する	delete –file <パス> 例： delete -file "c:\temp\runpath.exe"	ファイルを1つ削除する
		delete -folder <フォルダパス> 例： delete -folder temp\axvers	フォルダを削除する

番号	コマンド	パラメータ	説明
		delete –all <フォルダパス> 例： delete –all c:\temp	フォルダ内のすべてのファイルおよびサブフォルダを削除する（フォルダ自体は削除しない）
5	移動する	<SourcePath> <DestPath> ファイルまたはフォルダを移動（名前変更）する 例： 例：mv "c:\temp\clean.exe" "c:\temp\evil.exe"	ファイル/フォルダの移動を許可する
6	ファイルを表示する	<ファイルパス><バイト数>	ファイル内のデータを表示する（ファイルサイズの制限あり）
7	ハッシュ	ハッシュ <タイプ: md5 | sha1 | sha256> <ファイルパス> -f ファイルのハッシュを取得する 例: hash md5 c:\test\run.exe	最大1MBのファイルの暗号化を許可します。 -fオプションは、ファイルが他のプロセスによって開かれている場合でも強制的に開くためのものです。

番号	コマンド	パラメータ	説明
8	取得する	申し訳ありませんが、ファイルの内容を直接処理することはできません。テキストをここに貼り付けていただければ、翻訳いたします。	ホストからサーバーへ1つのファイルをアップロードする
9	置く	<url><folderpath>	ホストマシンに1つのファイルをダウンロードする
１０	ディレクトリを作成する	<ディレクトリ名>	フォルダを作成する
11	process		プロセスに関連するコマンド
		-t <プロセスID>	実行中のプロセスをプロセスIDで終了する
		-s <プロセスID>	プロセスを一時停止する
		-r <プロセスID>	以前に一時停止されたプロセスを再開する。
		-l -a	
		-l -u <username>	

番号	コマンド	パラメータ	説明
		-e -s <imagepath> -c <cmd> execute a non GUI process as system Ví dụ: process -e -s /tmp/run	
		-e-u<username> <imagepath> -c <cmd> execute a non GUI process as a user Ví dụ: process -e -u Alex /tmp/run	
		-d <processid> -o <imagepath> generate core file of running program, ví dụ: process -d 231 -o /tmp/core_file	
1 2	サービス		
		-query	ホストマシンで実行中のサービスを一覧表示してください。
		-<servicename>を開始する	サービスを1つ開始する
		-stop <サービス名>	サービス1を停止する
		-uninstall <service_name> サービスをアンインストールする	サービスのアンインストール

番号	コマンド	パラメータ	説明
		-listdrivers ホスト上のドライバーを一覧表示します。例: service -listdrivers	ホスト上のドライバー一覧を表示する
13	ユーザー	-リスト	コンピュータ上のユーザーを一覧表示してください。
		-sid<ユーザー名>	ユーザー名のSIDを取得する
1 4	助けてください。		ヘルプコマンド
15	クリア		コンソールをクリアする
21	コンテナ	- l	コンテナの一覧を作成してください。
		-a <コンテナID>	各コンテナへの接続
		申し訳ありませんが、翻訳するためのテキストを提供してください。	コンテナの接続を切断する

+ MACOS：

番号	コマンド	パラメータ	説明
1	cd	cd <ディレクトリパス>	現在の作業ディレクトリを変更する
		cd.. または cd ..	親フォルダに移動する
2	pwd		現在作業中のフォルダに印刷する
3	ディレクトリ	現在のフォルダー内のファイルおよびサブフォルダーの一覧を表示する	現在のフォルダ内のファイルおよびサブフォルダを一覧表示する。
4	削除する	delete –file <パス> 例： delete -file "c:\temp\runpath.exe"	ファイルを1つ削除する
		delete -folder <フォルダパス> 例： delete -folder temp\axvers	フォルダを削除する
		delete –all <フォルダパス> 例： delete –all c:\temp	フォルダ内のすべてのファイルおよびサブフォルダを削除する（フォルダ自体は削除しない）

番号	コマンド	パラメータ	説明
5	移動する	<SourcePath> <DestPath> ファイルまたはフォルダの移動（名前変更） 例： 例：mv "c:\temp\clean.exe" "c:\temp\evil.exe"	ファイル/フォルダの移動を許可する
6	ファイルを表示する	<ファイルパス><バイト数>	ファイル内のデータを表示する（ファイルサイズの制限あり）
7	ハッシュ	hash <タイプ: md5 | sha1 | sha256> <ファイルパス> -f ファイルのハッシュを取得する 例: hash md5 c:\test\run.exe	ファイルの最大暗号化サイズは1MBまで許可します。 -fオプションは、ファイルが他のプロセスによって開かれている場合でも強制的に開くためのものです。
8	取得する	申し訳ありませんが、ファイルの内容を直接翻訳することはできません。翻訳したいテキストをこちらにご提供いただけますか？	ホストからサーバーへ1つのファイルをアップロードする

番号	コマンド	パラメータ	説明
9	置く	<url><folderpath>	ホストマシンに1つのファイルをダウンロードする
10	ディレクトリを作成する	<dir name>	フォルダを作成する
11	プロセス		プロセスに関連するコマンド
		-t <プロセスID>	実行中のプロセスをプロセスIDで終了する
		-s <プロセスID>	プロセスを一時停止する
		-r <プロセスID>	以前に一時停止されたプロセスを復元する。
		-l -a	すべてのユーザーのすべてのプロセスを一覧表示してください。
		-l -u <ユーザー名>	あるユーザーのプロセスを一覧表示する。

番号	コマンド	パラメータ	説明
		-e -s <イメージパス> -c <コマンド> システムとしてGUIなしのプロセスを実行する 例：process -e -s /tmp/run	
		-e-u<ユーザー名> <画像パス> -c <コマンド> ユーザーとしてGUIを使わないプロセスを実行する 例：process -e -u Alex /tmp/run	
1 2	サービス		サービスに関するコマンド
		クエリ	ホストマシンで実行中のサービスを一覧表示してください。
		-<servicename>を開始する	サービスを1つ開始する
		-<servicename>を停止する	サービス1を停止する
		-uninstall <service_name> サービスをアンインストールする	サービスのアンインストール

番号	コマンド	パラメータ	説明
		-listdrivers ホスト上のドライバーを一覧表示します。例：service -listdrivers	ホスト上のドライバー一覧を表示する
13	ユーザー	リスト	コンピュータ上のユーザーを一覧表示してください。
		-sid<ユーザー名>	ユーザー名のSIDを取得する
14	助けてください。		ヘルプコマンド
15	クリア		コンソールをクリアする

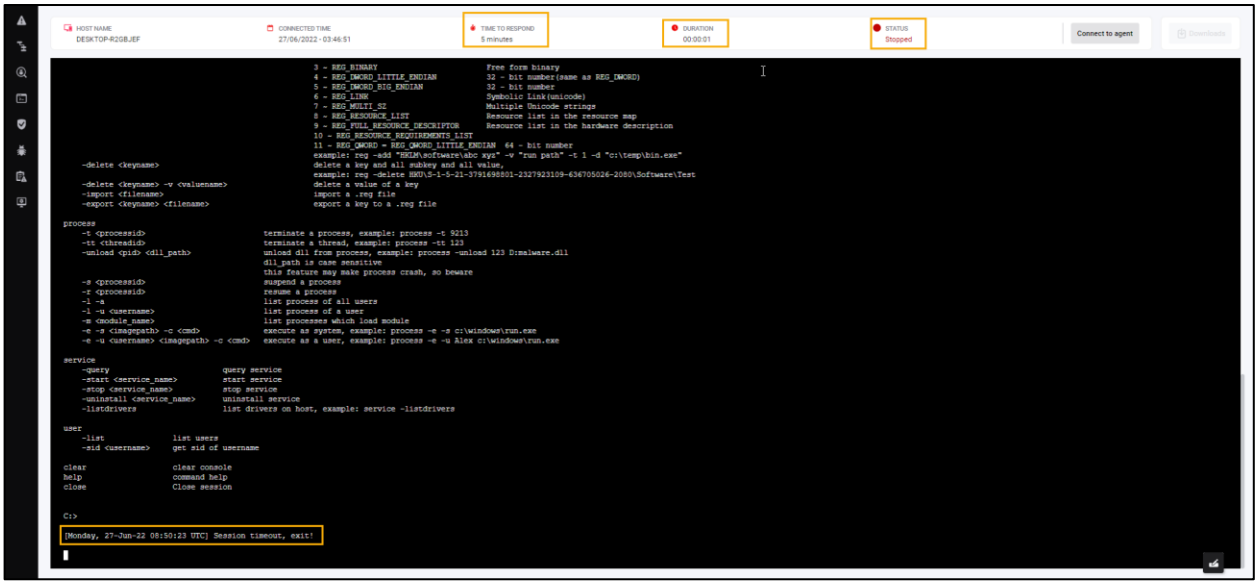
コンソール画面上のコマンドを操作する際の注意点：

+ クリアコマンド：クリアコマンドを実行すると、システムはユーザーがコンソール画面上でこれまでに行ったすべてのログを「here」というリンクをクリックすることでダウンロードできるようサポートします。

+ get <filepath> コマンド：例として、コンソール画面で get procexp.exe を実行すると、取得したファイルは画面右下の「Attachment Log」欄に表示されます。ユーザーはファイルをブラウザにダウンロードするか、サーバーから取得済みのファイルを削除することができます。

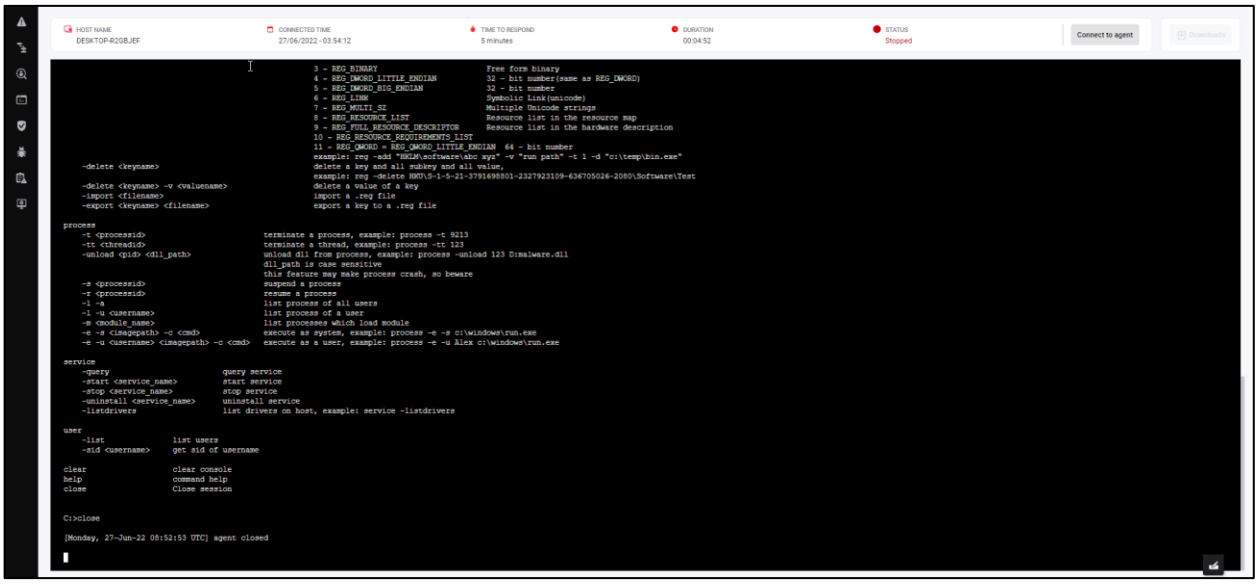
- **ライブレスポンスのセッションは以下の場合に終了します**：

+ **セッション**の有効期限時間：「Duration」フィールドの時間が「Time To Live」フィールドの時間と等しい場合。



+ ユーザーは「close」というコマンドで接続の切断を能動的に要求します。

+ エージェントとの接続が切断された場合、サーバーは3回連続でping/pongの失敗を検出します。

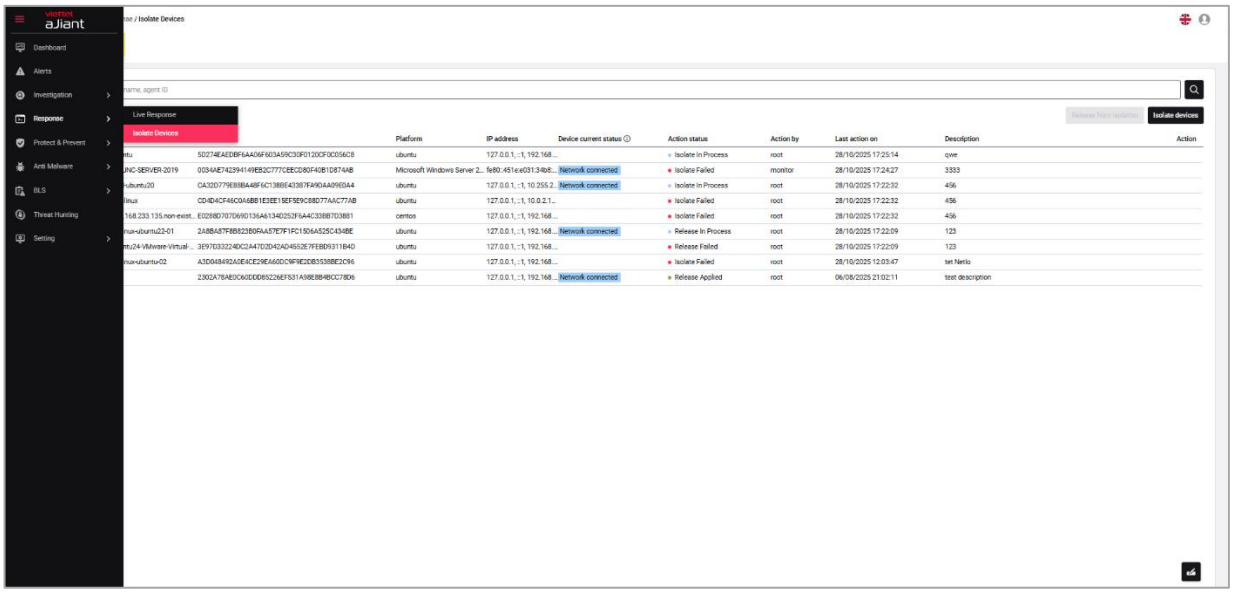


3.5.2 応答 - デバイスの隔離

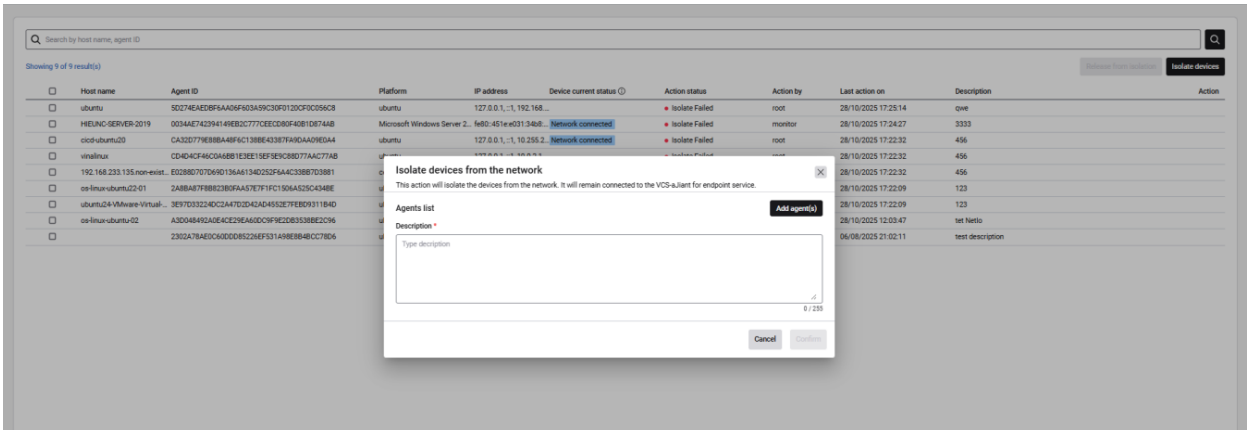
目的：SOCが侵害の疑いがあるデバイスをネットワークから隔離できるようにすること。主な目標は、マルウェアの拡散を防ぎ、危険な通信を制限するとともに、デバイスとVCS-aJiantシステム間の接続を維持し、調査の継続、証拠の収集、およびデバイスの復旧を可能にすることである。

デバイスのアイソレート（隔離）コマンドを作成する

ステップ1：メニューの「Response」にアクセスし、「Isolate Devices」メニューを選択します。



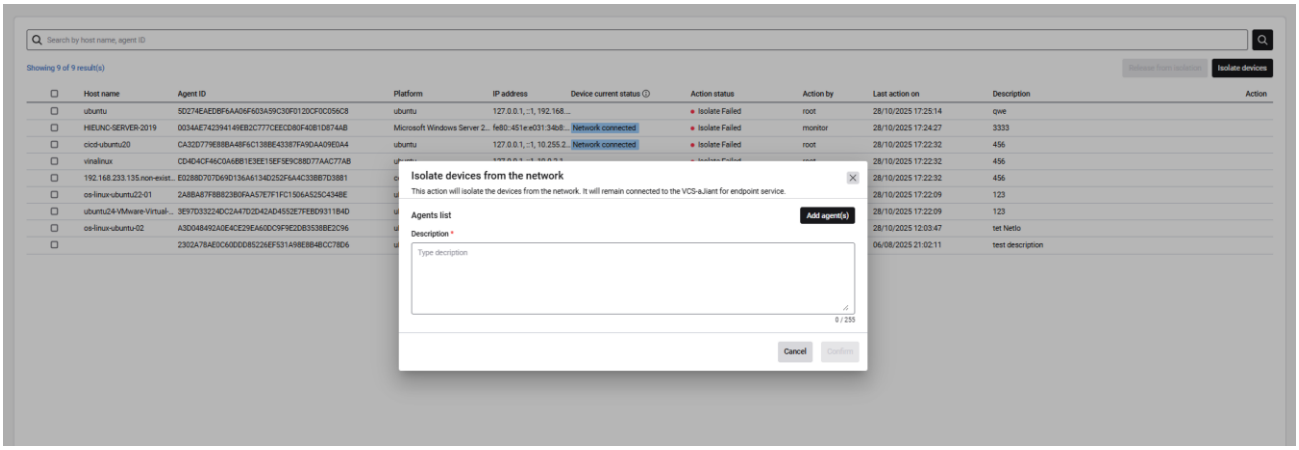
ステップ2：デバイスを分離するボタンを選択してください

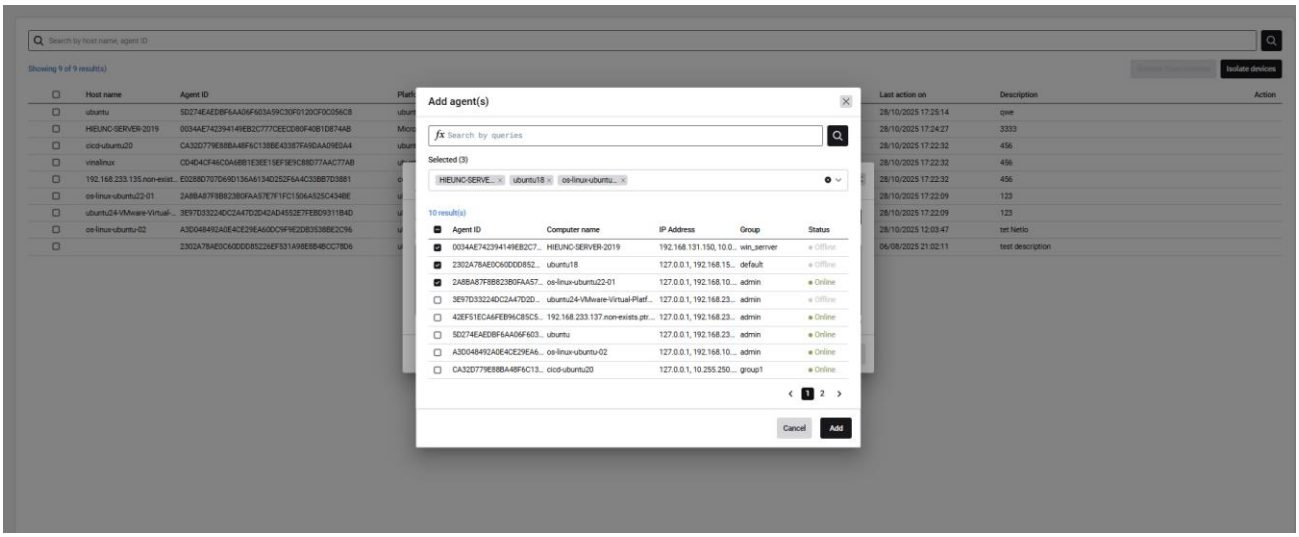


ステップ3：必要な情報を入力してください。

- 説明（必須）
- エージェントを選択してください

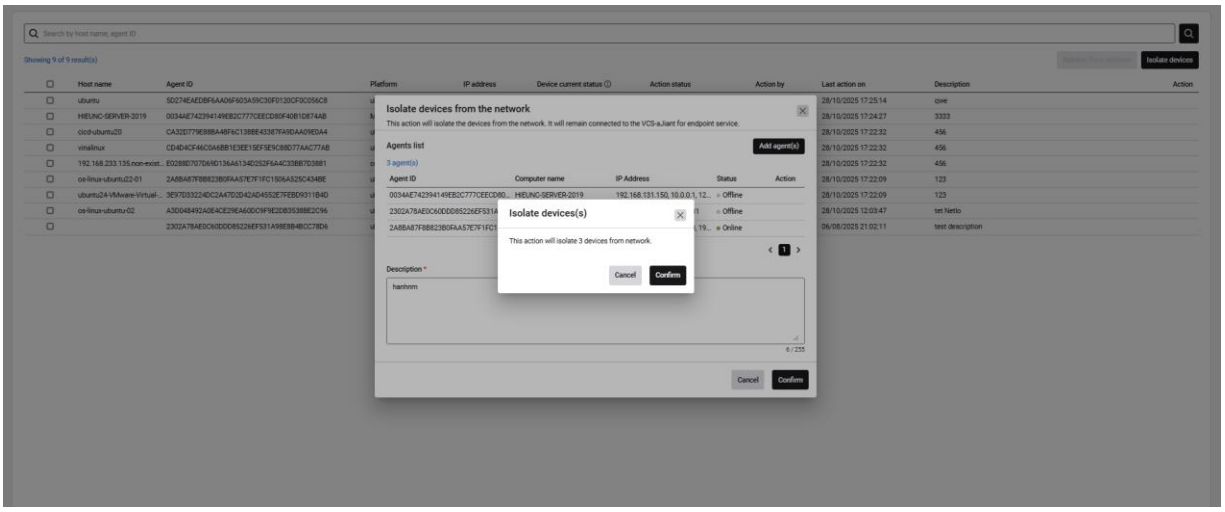
注意：ユーザーは権限が付与されたエージェントにのみ操作を行うことができます。





ステップ4：機器の隔離を確認する

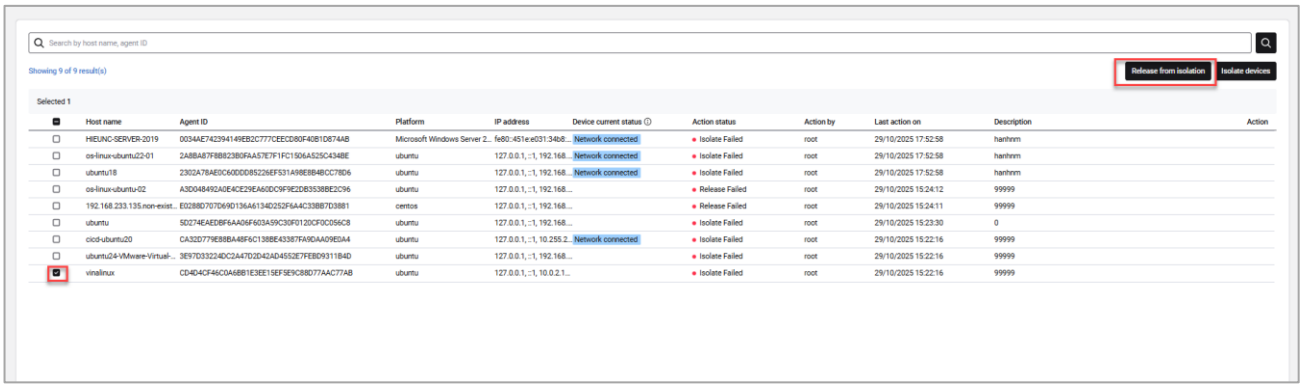
ユーザーは「確認」を押して、デバイスの隔離を実行することを確認します。



リリースアイソレーション（隔離解除）コマンドを作成する

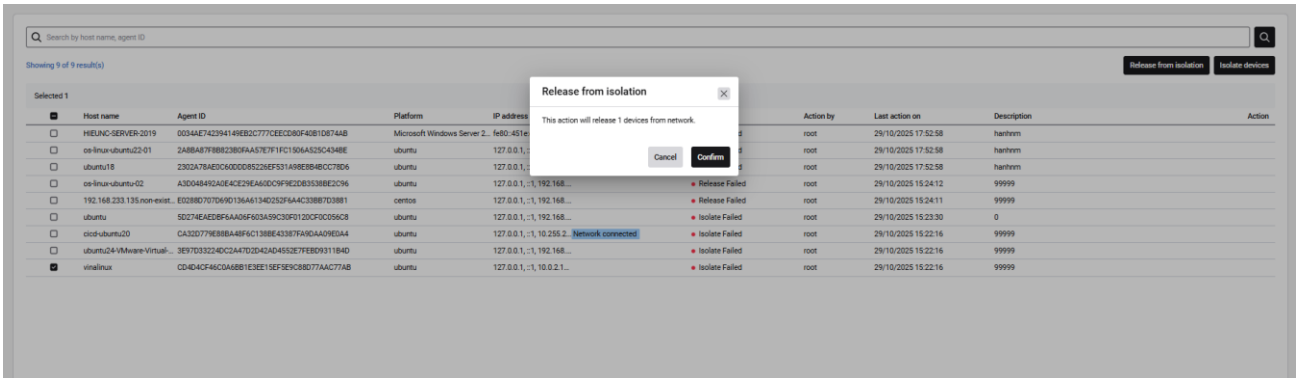
ユーザーは次の方法でデバイスの隔離を解除できます：

ステップ1：リストから、ユーザーは隔離を解除したいデバイスを1台または複数選択します。

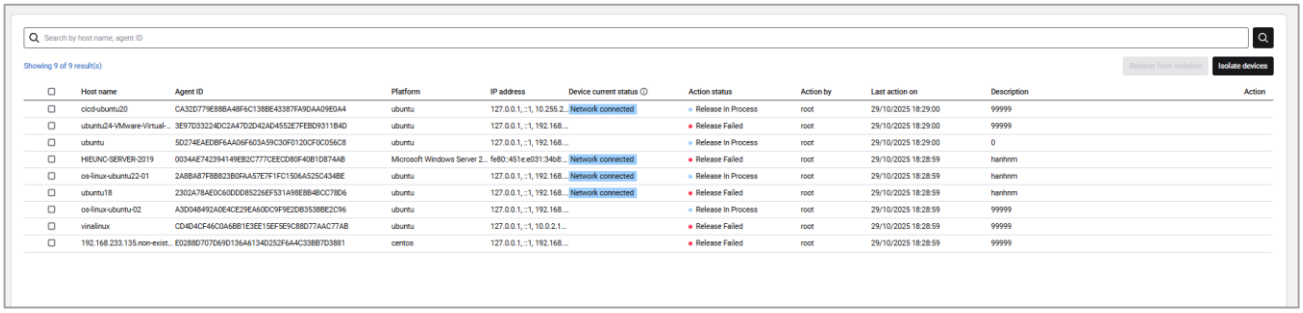


ステップ2：［隔離解除］ボタンを選択し、確認を実行します。

隔離解除を確認した後、システムはデバイスの隔離解除を実行します。



ユーザーはリスト画面で隔離解除の状態を確認できます（下の例の画像のように、システムが隔離解除のコマンドを実行中です）。



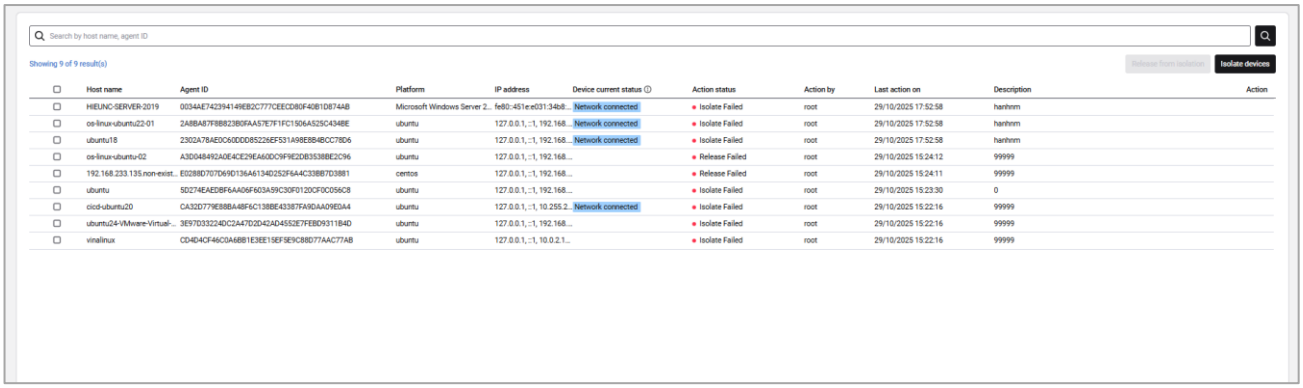
機器の隔離状況の確認／隔離解除

ユーザーがデバイスの分離を実行した後、デバイス情報がリストに表示され、ユーザーは以下の情報を確認できます。

- ホスト名：影響を受けた機器名（隔離／隔離解除）
- エージェントID：影響を受けた機器のIDです。
- プラットフォーム：影響を受けたデバイスのOSプラットフォーム情報
- IPアドレス：影響を受けたデバイスのIP情報
- デバイスの現在の状態：デバイスの実際のネットワーク状態で、2つの状態があります。

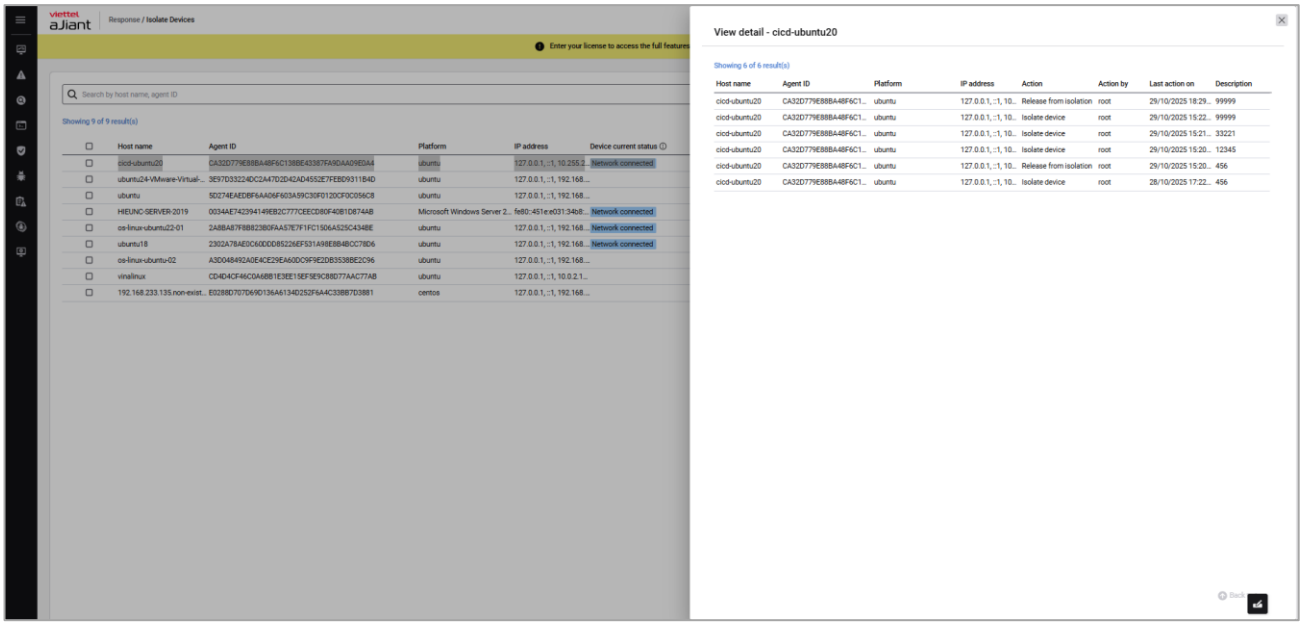
- ネットワーク接続済み：ネットワーク接続状態は正常です。
- ネットワーク隔離：デバイスは隔離され、ネットワーク接続が切断されており、VCS-aJiantシステムへの接続のみ可能です。

- アクションステータス：ユーザーの操作に基づく実際の状態を示し、以下の状態を含みます。
  - 処理中：システムがユーザーの要求（デバイスの隔離／隔離解除）を実行している状態を示します。
  - 適用済み：ユーザーによる（デバイスの隔離/隔離解除）がシステムで正常に実行された状態を示します。
  - 失敗：システムがユーザーの「デバイスの隔離」または「隔離解除」要求を正常に実行できませんでした。
- 実行者：操作を行ったユーザー情報
- 最終更新日時: レコードの最終更新時間
- 説明



デバイス別の影響履歴リストを表示する

ユーザーは各レコードで「アクションビュー」を選択し、時間順に影響履歴（デバイスの隔離／隔離解除）の一覧を確認します。



3.6 設定画面

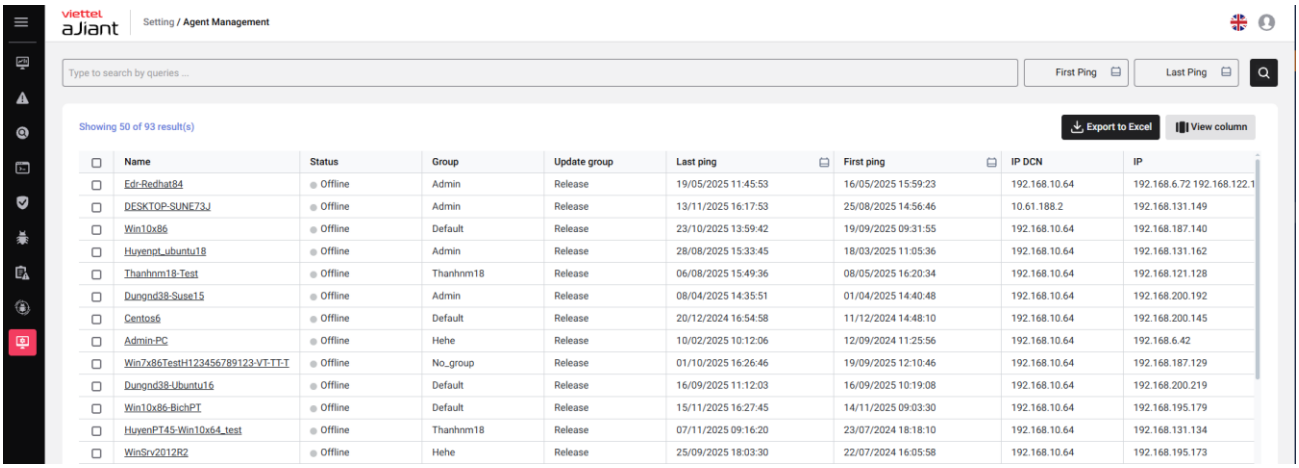
3.6.1 エージェント管理

目的：エージェント管理機能は、管理者がインストール済みのエージェントを管理することを支援します。内容は以下の通りです。

+ エージェントの一覧および一般情報を表示する。
+ エージェントの詳細を見る;

+ エージェントを素早く選択し、いくつかの設定（ポリシー、アップデートグループ）を行う

。



システムは以下の機能をサポートしています：

1 – システムにインストールされているエージェントの一覧を表示する：

+ ユーザーがrootグループに属している場合：システム内のアクティブなエージェントを30日未満で全て表示する。

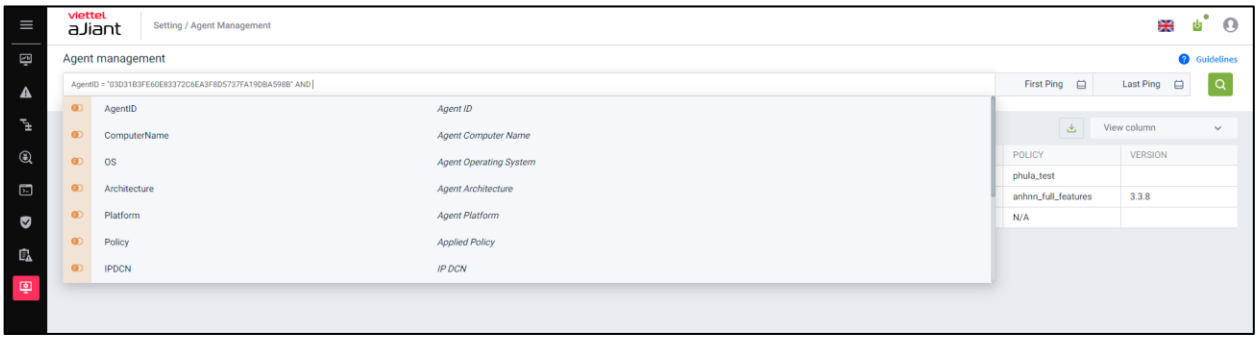
+ ユーザーがデフォルトグループにログインしている場合：デフォルトグループに属するすべてのエージェントを表示する。

+ ユーザーが親グループにログインした場合：ログインしているユーザーのグループおよび対応する子グループに属するすべてのエージェントを表示する。

+ ユーザーが一つまたは複数のグループに所属している場合：ログインしているユーザーのグループに属するすべてのエージェントを表示する。

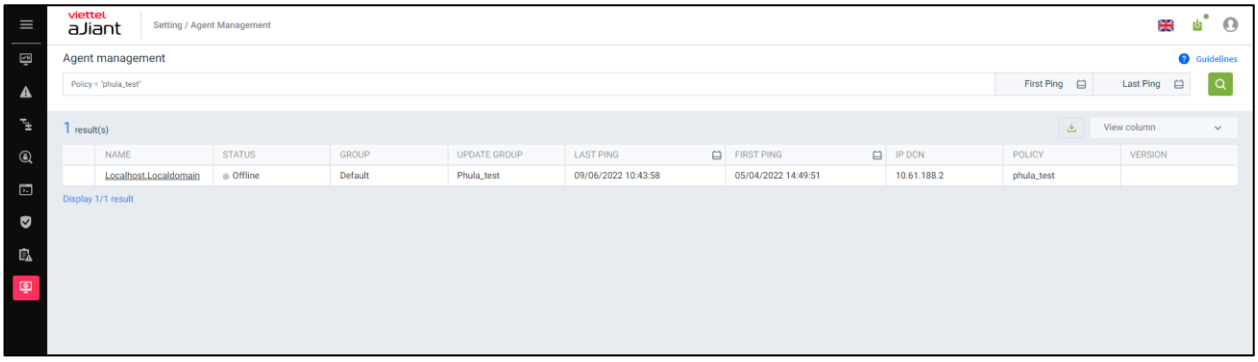
+ 各エージェントには、以下の共通情報が表示されます：名前、ステータス、グループ、グループ更新、最終ピング、初回ピング、DNS、ポリシー、エージェントID、プラットフォーム、プラットフォームバージョン、アーキテクチャ、DNS、バージョン、IP、ライセンス。

2 – AgentID、ComputerName、OS、Architecture、Platform、Policy、IPDCN、Online、Update Group、Group ID、IP、Mac、VersionによるAgent検索機能をサポートします。各検索条件に対して、「=」、「!=」、「~」の検索演算子をサポートしています。

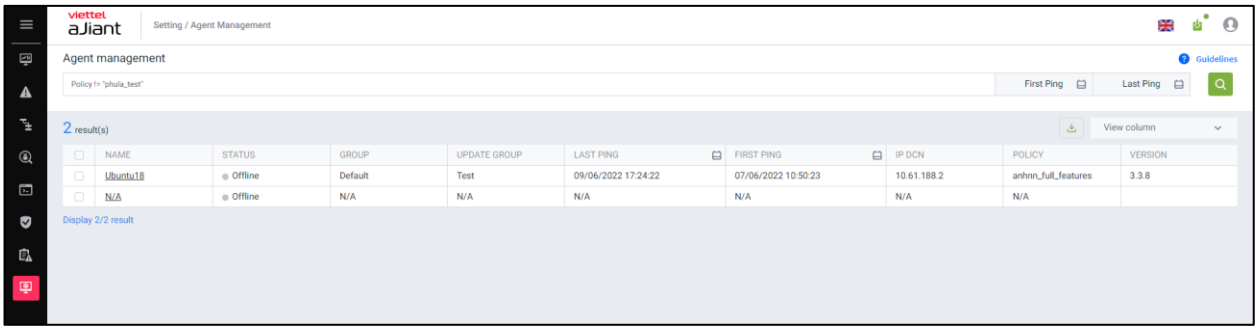


検索例：

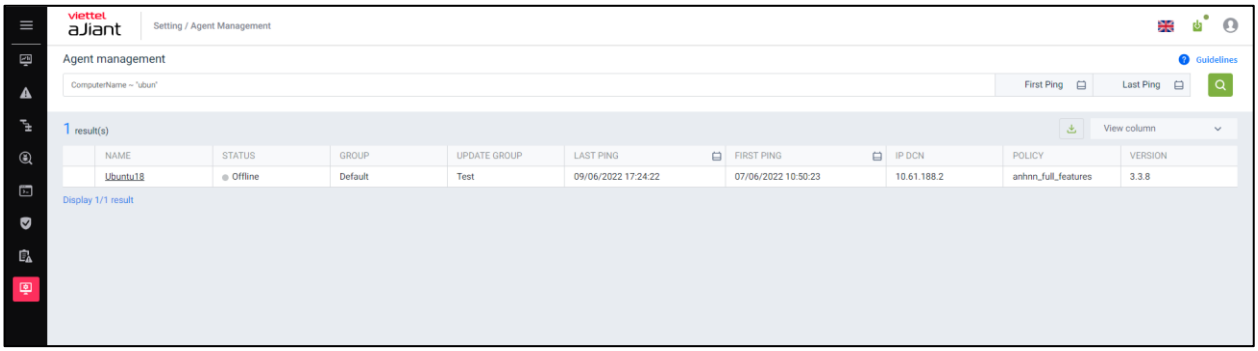
+ 「=」の条件で検索する：



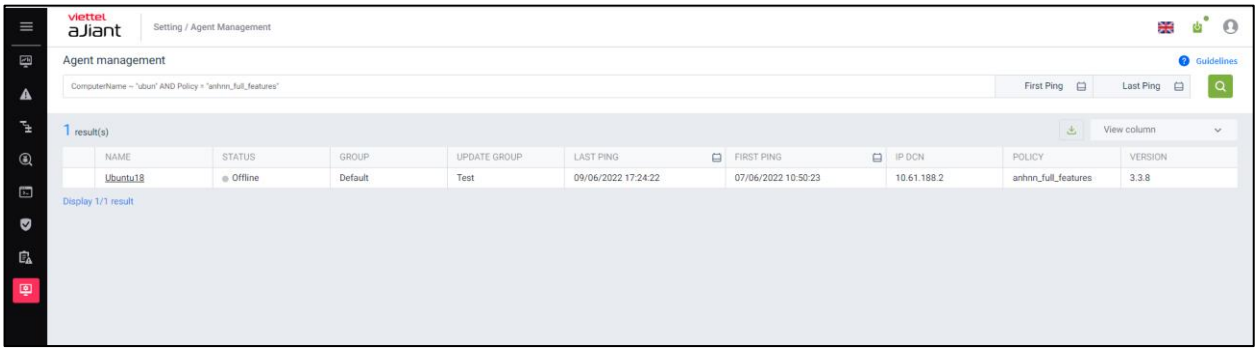
+ 「!=」の条件で検索する：



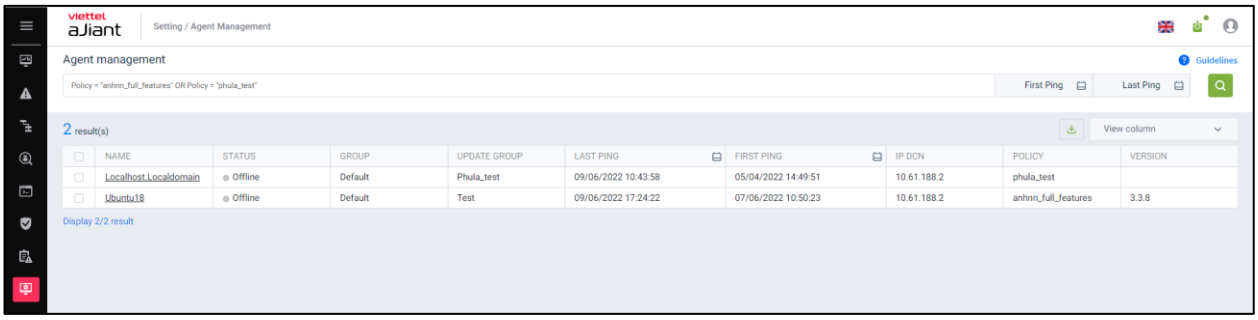
+ 「~」の条件で検索する：



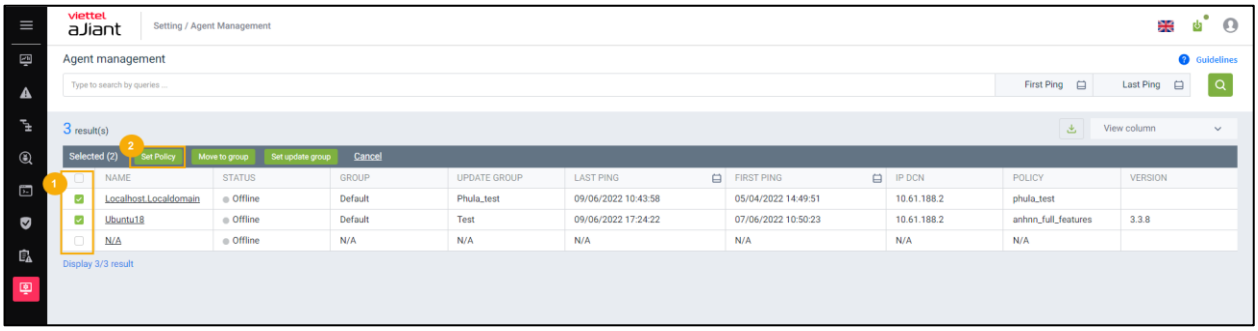
+ AND条件による検索：



+ OR条件による検索：



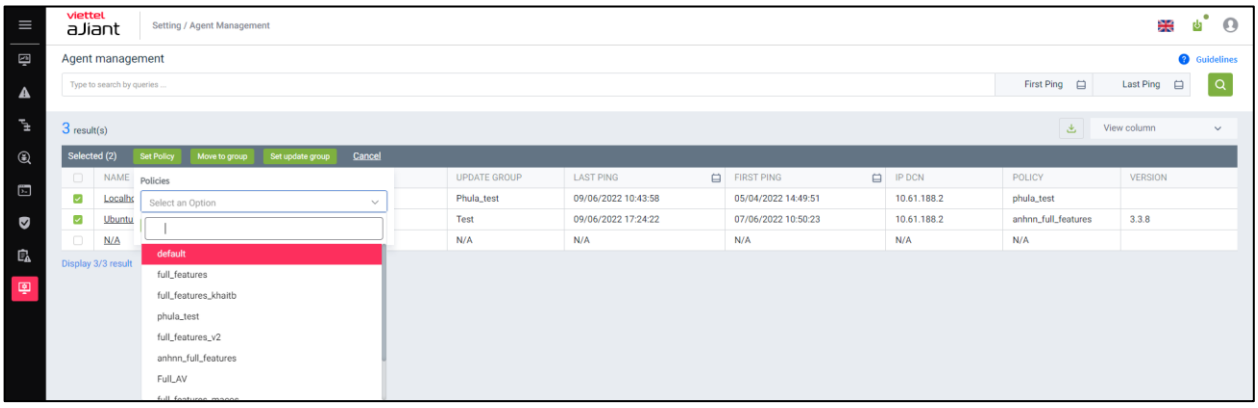
3 – ポリシーを設定するために、1つのエージェントまたは1つのエージェントグループを迅速に選択してください。



+ 1つまたは複数のエージェントを選択して、マルチセレクトセッションに参加させる。

+ ポリシーの設定を実行する:

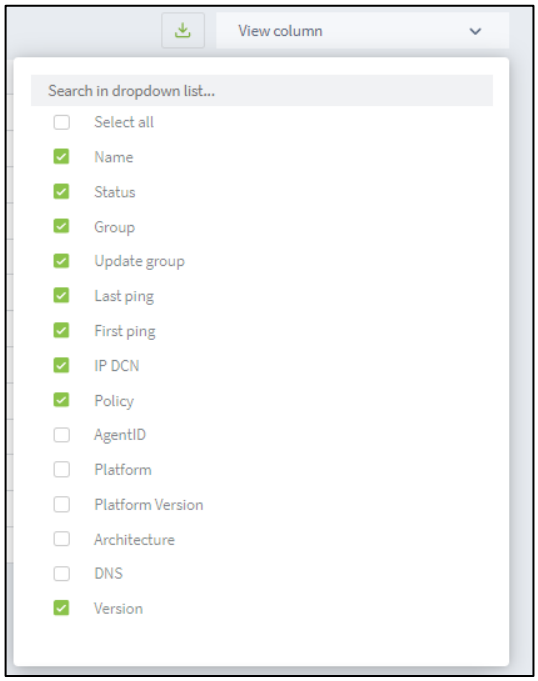
  - ポリシーを選択してください：



  - 「Set policy」ボタンを選択して操作を確認してください。

- 「キャンセル」ボタンを選択して操作の取り消しを確認してください。

4 – 列の表示設定：希望に応じて列の表示を構成します。



5 – 任意の行をダブルクリックして、エージェントの詳細を表示します。

システムはユーザーがエージェントのポリシー設定、グループの更新、およびグループへの移動を迅速に行えるようサポートします。

+ ユーザーがrootグループに属している場合：システム内のすべてのグループを表示する。

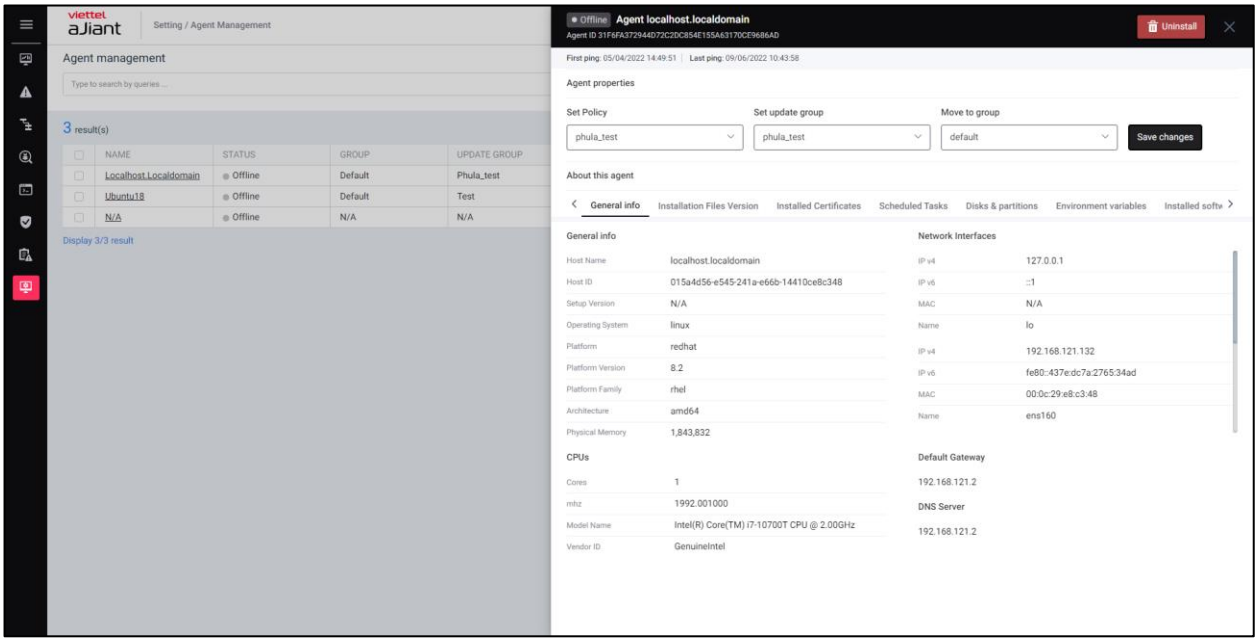
+ ユーザーがデフォルトグループにログイン：デフォルトグループを表示する；

+ ログインしているユーザーの親グループに属する場合：ログイン中のユーザーが所属するすべてのグループと、それに対応する子グループのユーザーを表示する。

+ ユーザーが属するグループまたは複数のサブグループ：ログイン中のユーザーに属するすべてのグループを表示する。

一般情報タブ

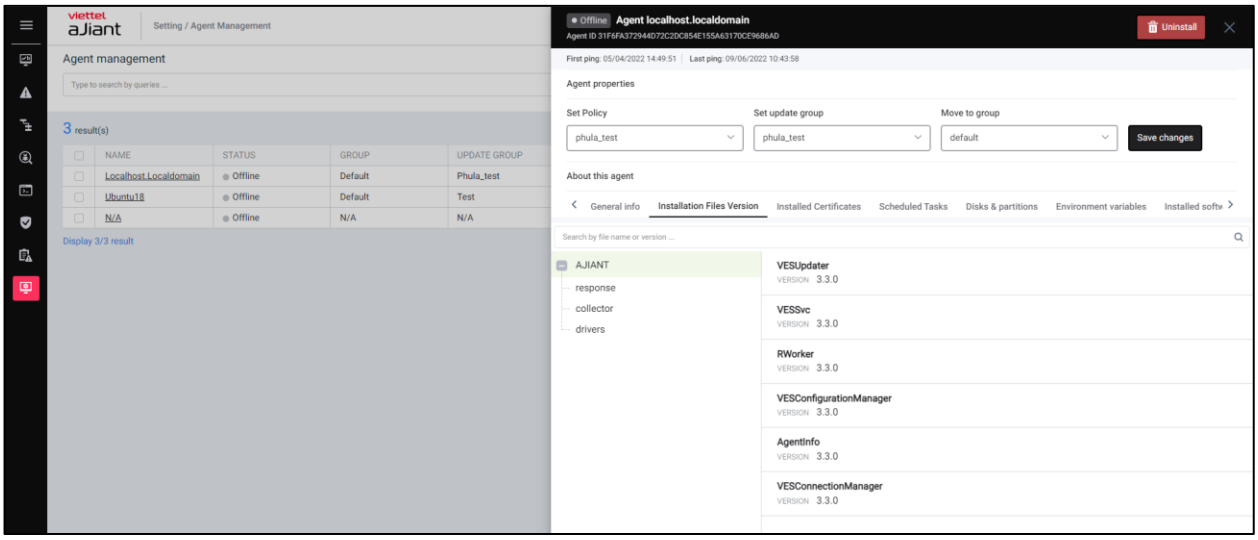
+ システムは、エージェントに関する以下の一般情報を表示します：一般情報、CPU、ネットワークインターフェース、デフォルトゲートウェイ、DNSサーバー。



インストールファイルのバージョン

+ エージェントインストールファイルのすべてを統計し、以下の情報を含めてください：ファイルを含むフォルダ名、ファイル名、バージョン。

+ ファイル名やバージョンでの高速検索を検索ボックスでサポートする。



インストール済み証明書

+ エージェントがインストールされているマシン上のすべての証明書を統計し、以下の情報を含めてください：マシン上の証明書一覧、発行者、発行先、有効期限、ステータス。

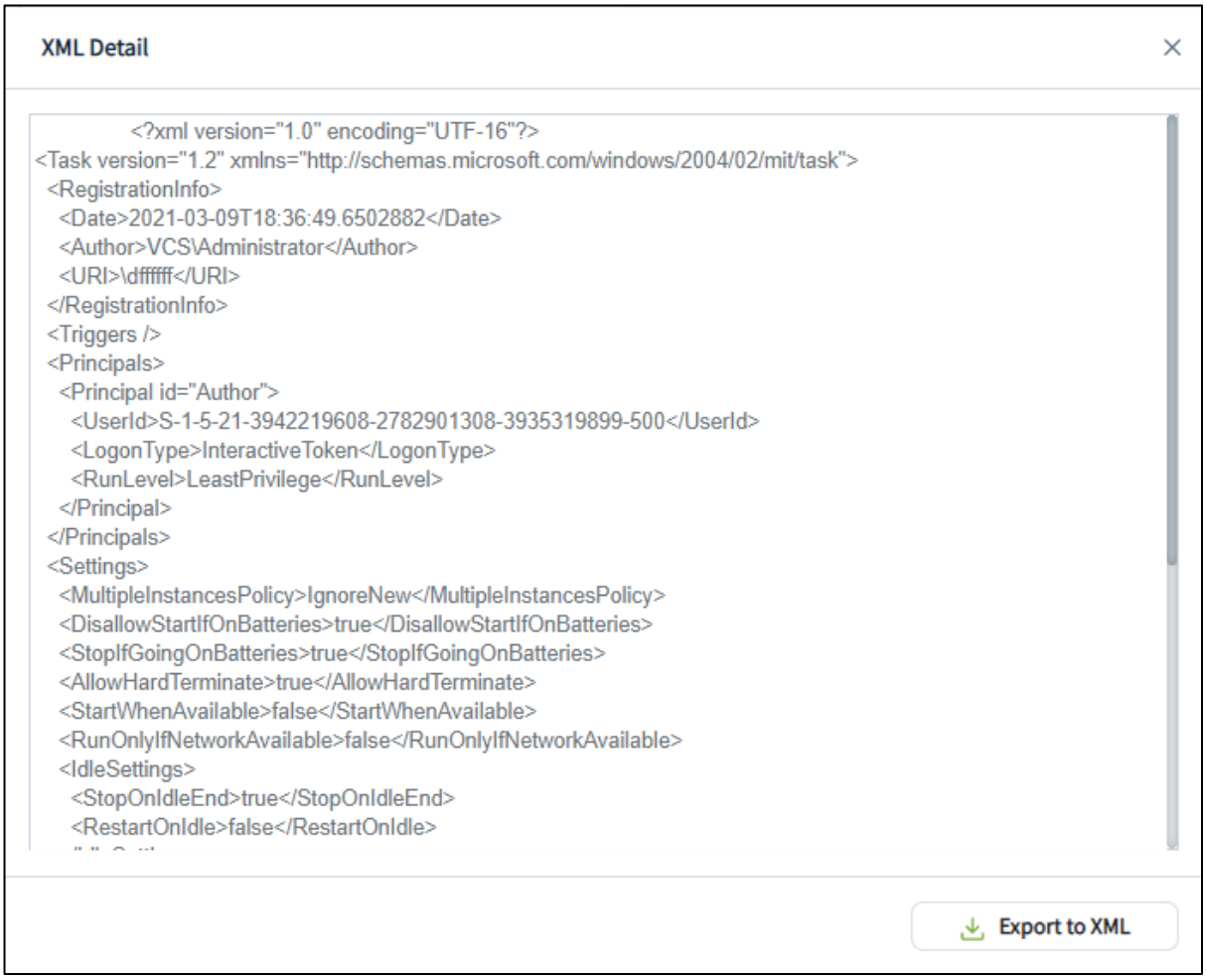
+ 詳細な情報を確認したい場合は、を選択すると、以下の画面が表示されます。

スケジュールされたタスク

+ エージェントがインストールされているマシン上のすべてのスケジュールタスクを統計し、以下の情報を含みます：スケジュールタスクの一覧、名前、状態、トリガー、次回実行時間、最終実行時間、作成者、作成日時。

+ 各タスクの追加情報の表示を選択またはカスタマイズしてください。

+ タスクにカーソルを合わせて、アイコンを選択すると、タスクの情報をXML形式で完全に表示できます。

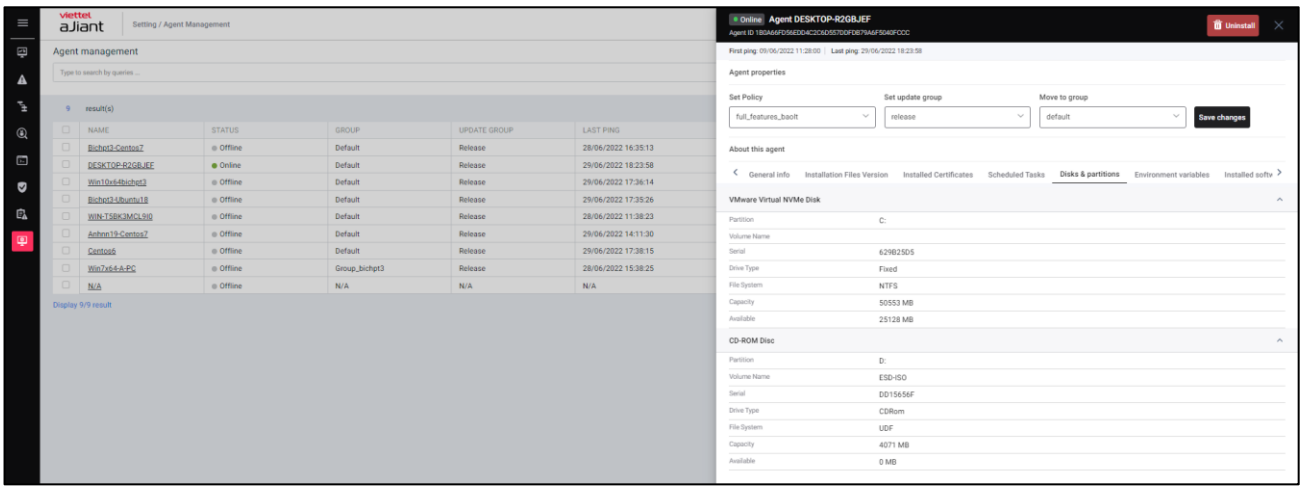


+ スケジュールされたタスクの情報をダウンロードするには選択してください。対応形式は.xmlです。

ディスクとパーティション

+ エージェントがインストールされているマシン上のすべてのディスクおよびパーティションの統計情報を取得してください。情報には以下を含みます：ディスク一覧、パーティション、ボリューム名、シリアル番号、ドライブタイプ、ファイルシステム、容量、空き容量。

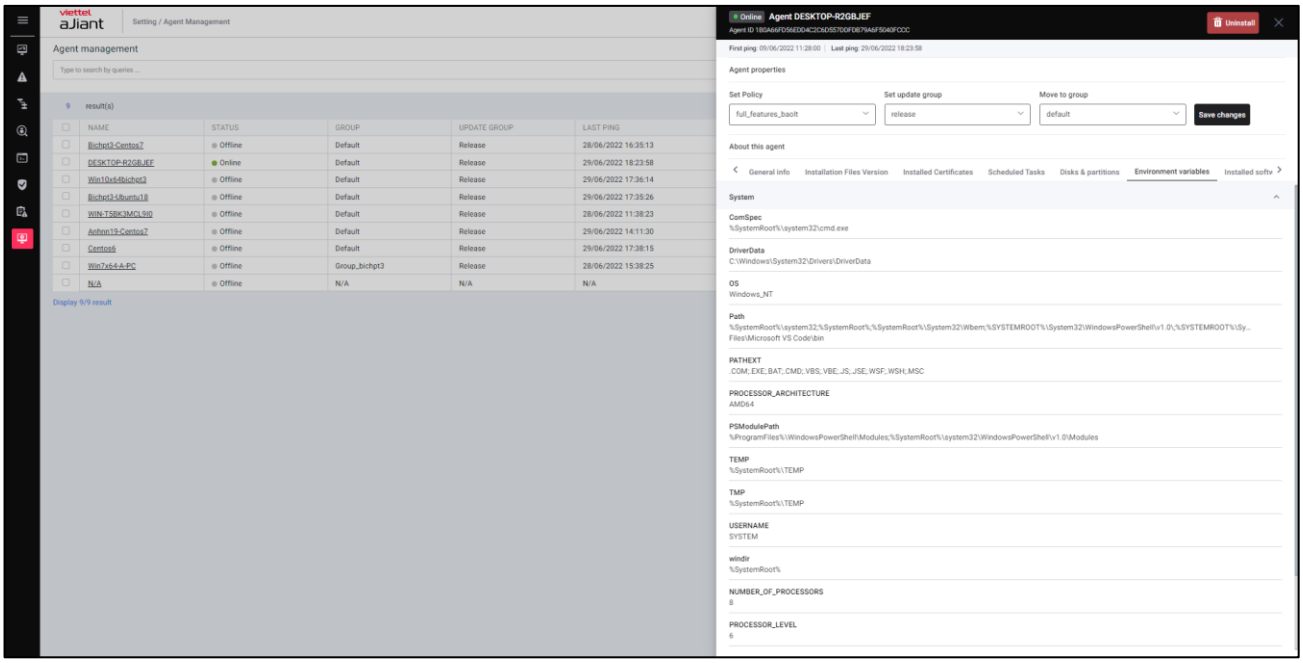
+ 各ディスクの追加情報の表示を選択またはカスタマイズしてください。



環境変数

+ エージェントがインストールされているマシン上のすべての環境変数を統計し、以下の情報を含めます：システムおよびユーザーの一覧、変数名、システムまたはユーザーに属する値。

+ 各ディスクの追加情報の表示を選択またはカスタマイズしてください。



インストール済みソフトウェアタブ

+ エージェントにインストールされているすべてのソフトウェアの統計情報を、ソフトウェア名、インストールバージョン、インストール日を含めて取得する。

+ インストール済みのアンチウイルスソフトウェアを迅速に検索するか、検索ボックスにソフトウェア名を入力してサポートします。

必要なソフトウェア

+ エージェントに必須のすべてのソフトウェアのインストール状況を統計し、以下の情報を含めること：ソフトウェア名、インストールバージョン、インストール状態。

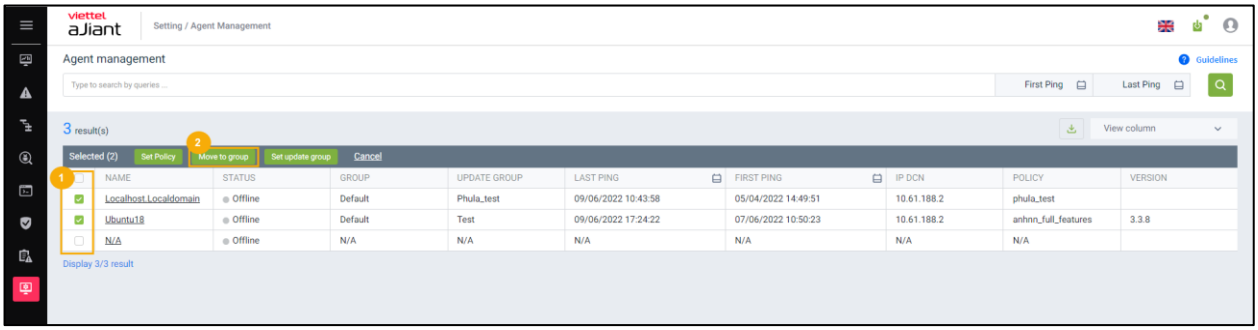
+ 必須ソフトウェアがまだインストールされていない場合に迅速に検索をサポートするか、検索テキストボックスにソフトウェア名を入力してください。

タブユーザーリスト

＋　エージェントにログインしたすべてのユーザーの統計情報（ユーザー名、アクティブ状態、管理者権限を含む）

6 –　移動先グループを設定するために、エージェントまたはエージェントグループを1つ素早く選択してください。

＋　マルチセレクトセッションに参加するために、1つまたは複数のエージェントを選択してください。



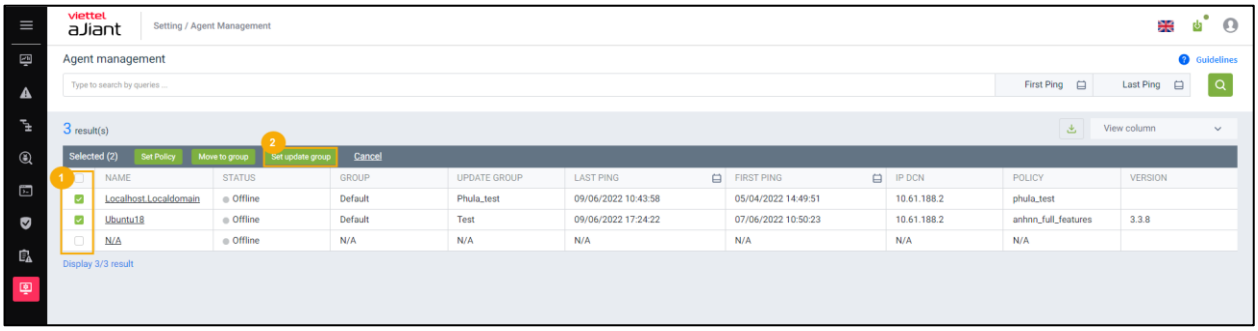
＋　グループに移動を実行する:

「グループに移動」コンボボックス内のグループ一覧：

- ユーザーがrootグループに属している場合：システム内のすべてのグループを表示する。
- ユーザーがデフォルトグループにログイン：デフォルトグループを表示する；
- ユーザーが親グループにログインする場合：ログイン中のユーザーが所属するすべてのグループと、それに対応する子グループに所属するユーザーを表示する。
- ユーザーが属するグループまたはその子グループ：ログイン中のユーザーに属するすべてのグループを表示する。

+ セットアップデートグループを設定するために、1つのエージェントまたは1つのエージェントグループを素早く選択してください。

- 1つまたは複数のエージェントを選択して、マルチセレクトセッションに参加させる。



- セットアップデートグループを実行する。

注意：

+ グループに移動：エージェントをグループ管理画面に表示されているグループに移動する。

+ グループの更新：エージェントをエージェント下で実行されるファイルを保存する各グループに移動します。各グループにはサーバーで定義された異なる実行ファイルがあります。

VCS-ajiantのライセンス計算方法：

+ ライセンスはエンドポイントの数に基づいて計算されます（例えば、顧客が10エンドポイントのライセンスを購入した場合、10台のデバイスにエージェントをインストールすることができます）。

+ システムは、エージェントがVCS-aJiantシステムに接続した時間に基づいてライセンスを計算します（最初のping時間）。先に接続したエージェントから順にライセンスが割り当てられます。

の場合：

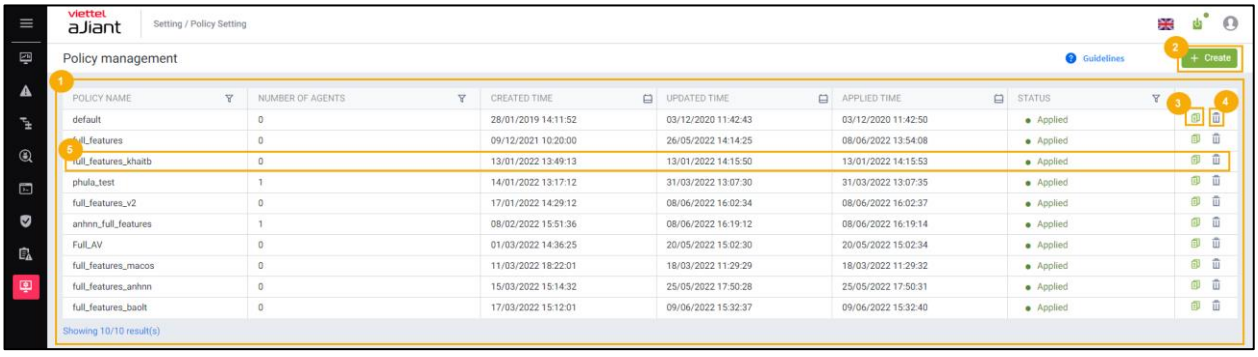
+ 1. お客様がライセンス数を超えてインストールした場合、これらのデバイスでは検出、予防、対応などの機能が動作しません。

+ 2. ライセンスが期限切れの場合：ライセンスが更新されるまで、システムは全デバイスのすべての機能を自動的に停止します。お客様はポータル上でエージェントがオンラインであることを確認できます。

3.6.2 ポリシー設定

目的：ユーザーがエージェントの設定ポリシーリストを管理するのを支援すること。

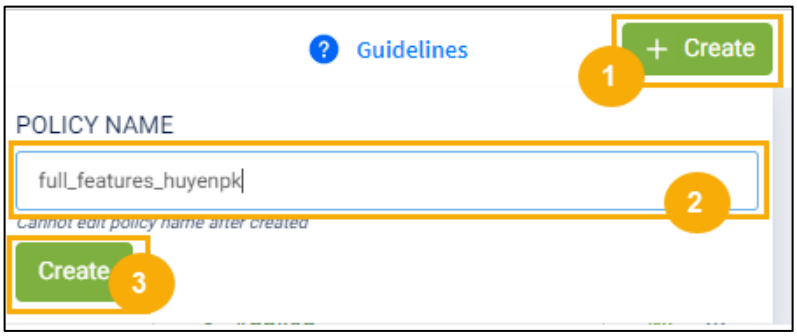
ユーザーが「設定」>>「ポリシー設定」にアクセスした際の画面インターフェース：



1 – システム上で作成されたポリシーの一覧を表示します。各ポリシーには以下の情報が含まれます：名前、ポリシーが適用されているエージェントの数、作成日時、更新日

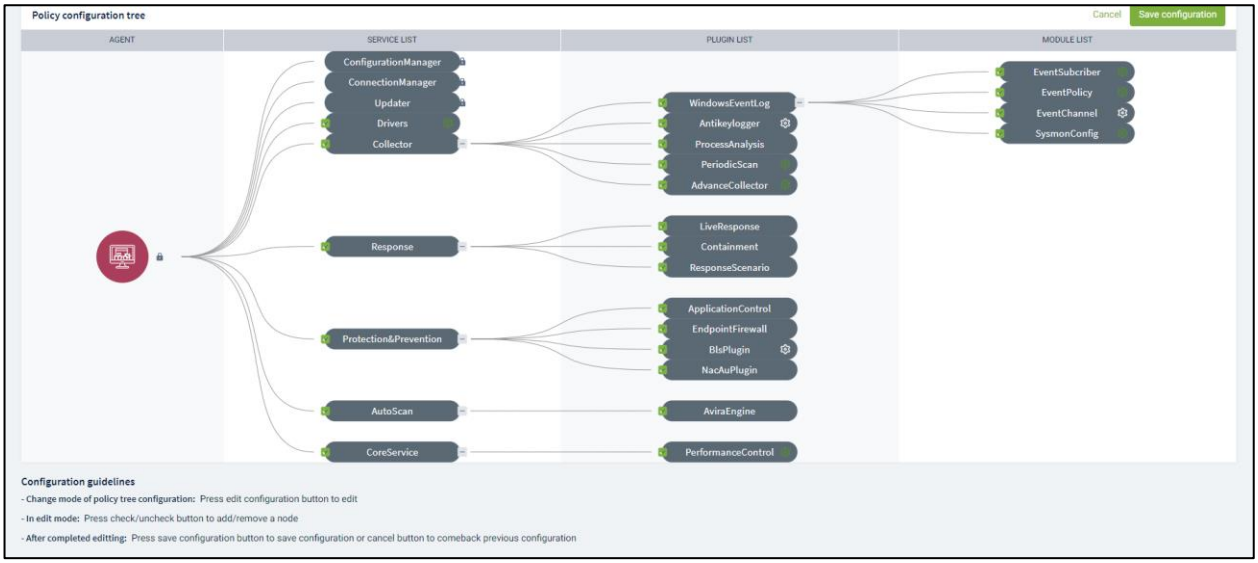
時、ポリシー適用期間、ステータス（2つのステータスがあります：適用済みと未適用）。

2 – 新しいポリシーを作成する：「Create」ボタンをクリックすると、システムは以下の新規ポリシー作成用のポップアップを表示します。



注意：新規作成時には、ポリシー名が既に作成されているポリシー名と重複しないようにしてください。

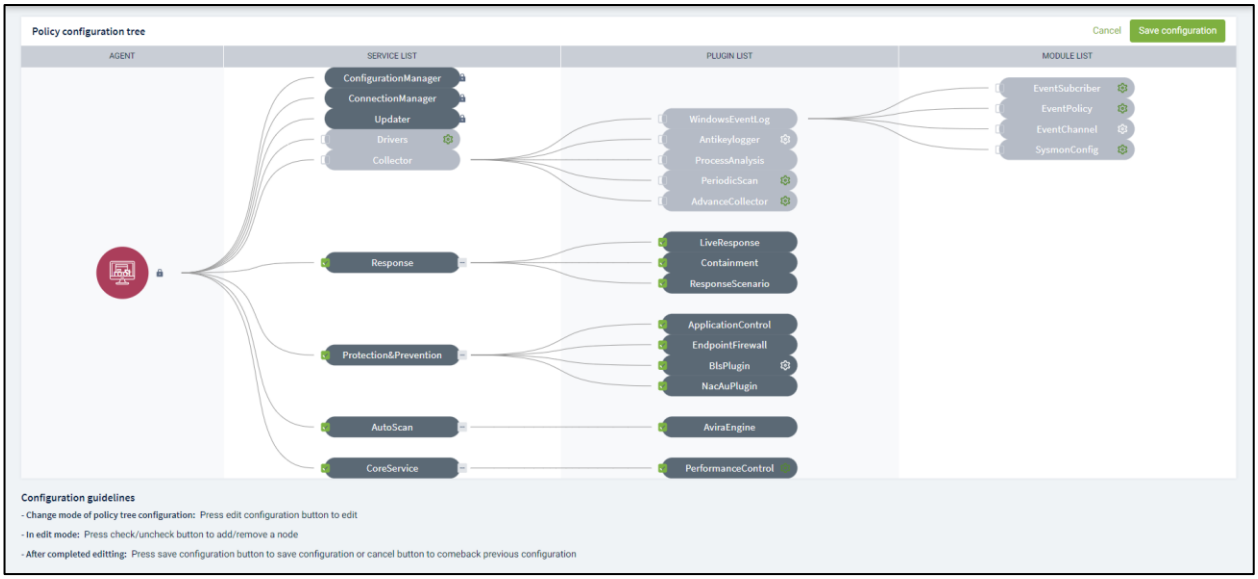
ポリシーの新規作成が成功すると、システムはポリシーの詳細画面を表示します。



各ポリシー作成後、通常は3つのコアサービスがデフォルトで含まれます：

ConfigurationManager、ConnectionManager、Updater。これら3つのサービスはシステムから削除してはいけません。ポリシーを設定する手順は以下の通りです：

- ポリシーツリーを変更するにはボタンをクリックしてください。
- 編集モードでは、ユーザーは他のサービスを追加または削除するためにチェック/チェック解除を行うことができます。



- 編集モードを完了した後：
    - ユーザーは「設定を保存」ボタンを押して変更を保存します。
    - ユーザーは「キャンセル」ボタンを押してポリシーの更新操作を中止し、システムは前の設定に戻ります。
- アイコンをクリックして、各サービスのモジュール／プラグインごとの詳細設定を行ってください。

モジュール／プラグイン	説明

Windowsイベントログ	- WindowsEventLogの設定：Agentから取得するログソースの設定 + EventSubscriber：ログを取得するチャネルを指定 データ要件： event_filterフィールド（Event IDでフィルタリング）：カンマ（,）で区切られた文字列 例：「4」：eventIDが4のイベントをフィルタリング 「-689」：eventIDが689以外のイベントをフィルタリング providersフィールド：セミコロン（;）で区切られた文字列 必須入力フィールド：subs_type、channel channel：ログソース subs_type： PUSH：新しいイベント発生時にVCS-aJiantの関数を呼び出して処理 POLLING：一定時間ごとにVCS-aJiantが能動的にログを取得 PULL：一定時間経過後にVCS-aJiantが能動的にログを取得 設定完了後は必ず保存してください EventPolicy：システムのデフォルトにない特定のログ種別を有効化/無効化するポリシー設定 要件：少なくとも1つのフィールドを選択すること EventChannel：特定のログソースの詳細設定 Retention：ログのローテーション保存の有無（

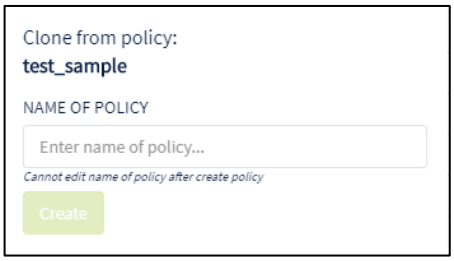
	Retentionを選択すると、ログファイルが満杯になった際に新しいログが最も古いログに上書きされます） ログファイルパス：ログファイルのパス ログファイルサイズ：ログファイルのサイズ 要件：すべてのデータを必ず入力すること SysmonConfig：Agent上のSysmonツール（Microsoft-Windows-Sysmon/Operationalログ取得）の有効化/無効化
アンチキーロガー	アンチキーロガーの設定：VCS-aJiantのSelfRunプラグインであり、定期的にシステム全体をスキャンして、実行中のキーロガーを検出する役割を持ちます。 スキャン設定：スキャン対象のキーロガーの種類を設定します。 要件： スキャン周期：最小1分、最大180分。 少なくとも1種類のキーロガーを選択してください。 ホワイトリスト設定：キーロガーを実行するファイルのパスまたはデジタル署名（証明書）に基づいて、一部のソフトウェアをホワイトリストに登録します。 要件：すべての項目を正確に入力してください。 入力が完了したら、設定を「保存」してください。

自己防衛	セルフディフェンドの設定：セルフディフェンスのアンインストール防止機能を追加； 手順：ドライバーを選択 > セルフディフェンスにチェックを入れて機能を有効化、またはチェックを外して無効化 > 保存を選択 > ポリシーを適用を選択；
オートスキャン	Autoscanの設定：ユーザーがマルウェアスキャン時に追加の設定を補足できる機能 - 要求事項：Autoscanを選択し、「新しい設定を追加」をクリックします。追加が必要な情報は以下の通りです。 + バージョン + 説明 + Windows用のデータ設定は以下のようなフォーマットになります。 注意：自動スキャンまたは手動スキャンの設定は、それぞれ「auto_scan」キーまたは「manual_scan」キー内に配置する必要があります。 自動スキャンフローでサポートされる設定項目は以下の通りです：
アンチランサムウェア	AntiRansomware：ランサムウェア駆除時に設定を変更可能 手順：Auto Scanを選択 → Anti Ransomwareを選択 設定可能な項目は以下の通りです：

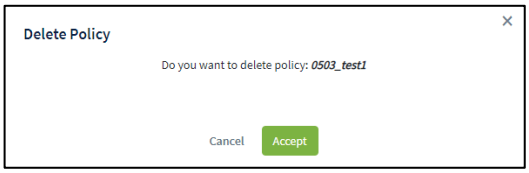
HIPS（高衝撃性ポリスチレン）	HIPS：マルウェア駆除時に動作に基づいて設定を変更可能 手順：Auto Scanを選択し、次にHIPSを選択 設定可能な項目は以下の通りです：

- ボタンをクリックして、エージェントに設定したポリシーを適用してください。

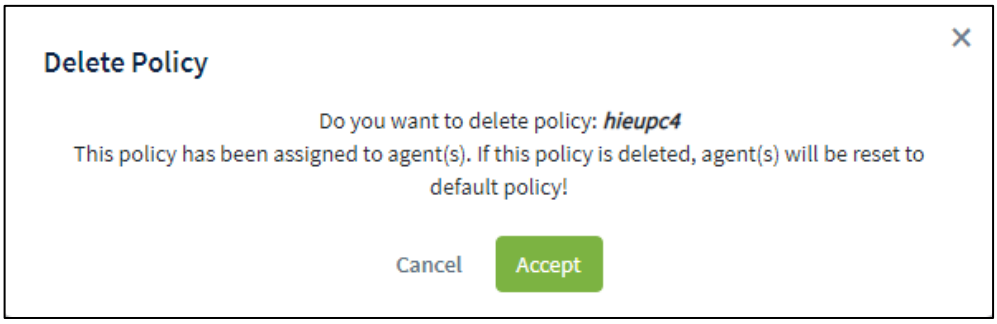
+ 新しいポリシーを複製する：ボタンをクリックすると、ポリシー名を除くすべてのポリシーの詳細がシステムによってコピーされます。



+ ポリシーの削除：システムのボタンをクリックすると、ユーザーに削除の可否を決定させるポップアップが表示されます。



+ ポリシーにすでにエージェントが適用されている場合、削除後にシステムが自動的にそれらのエージェントに「デフォルトポリシー」を割り当てます。



+ 各レコードをダブルクリックすると、システムはポリシーの詳細ページに遷移し、ユーザーがポリシーの設定を閲覧および変更できるようになります。

3.6.3 グループ管理

ポータル上でルールを設定し、条件を満たすエージェントに対して自動的にポリシーの変更およびグループの移動を行うことで、各エージェントのポリシー変更およびグループ移動の時間を短縮し、設定されたルールを満たすエージェントのポリシーを同期します。

この画面の主な機能は以下の通りです：

+ ツリー構造によるグループ管理;
+ グループを検索する;
+ 新しいグループを追加する：
  - エージェントのグループ自動移動ルールを作成する。
  - グループ移行方法の選択（既存の全エージェント、新規エージェントのみ、既存および新規の全エージェント）とポリシーの割り当て（即時割り当て、割り当てなし）。
+ グループに属するエージェントの監視およびグループに属するエージェントの総数。
+ グループを編集する;

+ グループの削除、グループに属するエージェントの削除；

1 – ツリー構造によるグループ管理：

+ ユーザーがrootグループに属している場合：システム内のすべてのグループを表示する。

+ ユーザーがデフォルトグループにログインした場合：デフォルトグループを表示する。

+ ユーザーが親グループにログインした場合：ログインしているユーザーの所属グループおよび対応する子グループを表示する。

+ ユーザーが属するグループまたは複数のサブグループ：ログイン中のユーザーが所属するすべてのグループを表示する。

グループ一覧はツリー形式で表示され、各ルートグループには第1階層、第2階層のサブグループが含まれます。

各グループには、グループ名、グループの構成情報（ルール、ポリシー、適用対象）、およびグループに属するエージェントのリストが含まれます。

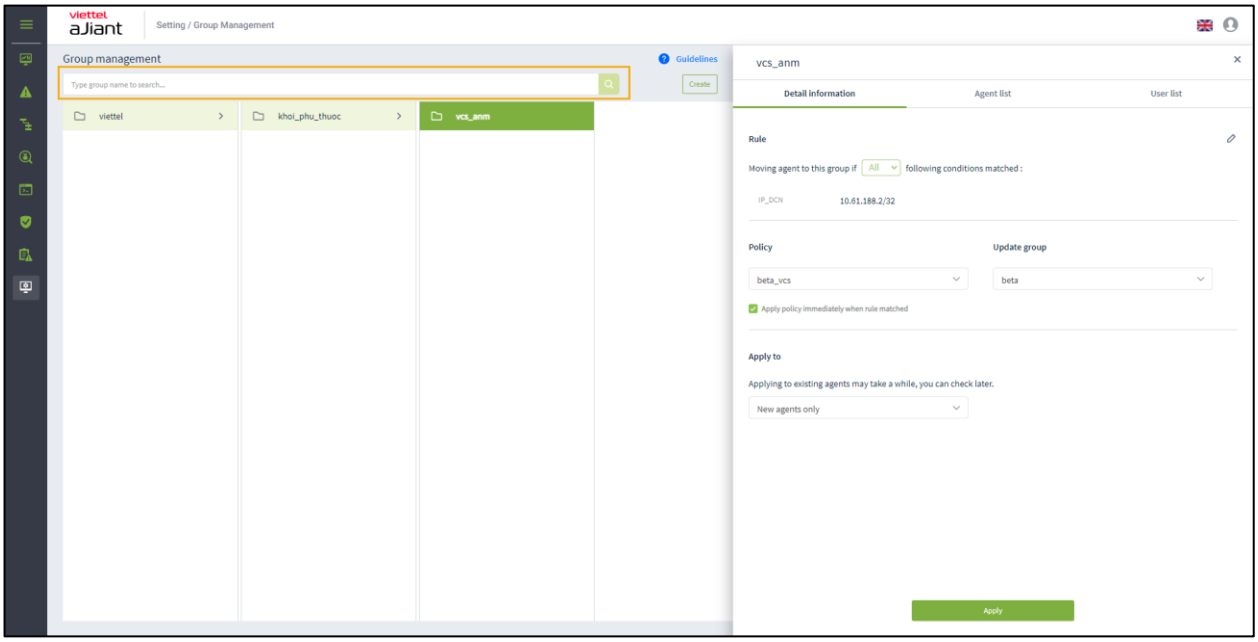
グループのルールは各グループ間で独立しており（親子継承はありません）、エージェントの数が多く、会社や部署などによるエージェント管理の階層化がある場合に、管理を容易にするためにグループをツリー構造で管理します。

ユーザーが子グループに所属している場合、親グループを選択してもグループ詳細のポップアップは表示されません。

2 – グループを検索する

＋　方法1：検索ボックスをクリックすると、ログイン中のユーザーに対応するグループのリストが表示され、スクロール可能です。表示されたリストからグループを選択します。

＋　方法2：検索ボックスをクリックし、検索文字を入力すると、システムが自動的に入力文字を含むレコードを検索します。候補リストから適切なレコードを選択するか、検索ボタンをクリックするか、Enterキーを押すと、条件に合致するレコードの一覧が表示されます。



レコードをダブルクリックすると、そのレコードの詳細情報が表示されます。

＋　表示される詳細情報は「Detail」で、そのグループのデータは「Rule」、「Policy」、「Apply to」です。

＋　「エージェントリスト」タブを選択すると、そのグループに一致するエージェントの情報データが表示されます。

+ レコードを右クリックすると、「グループへ移動」と「グループを削除」の2つのオプションが表示されます。

+ 「Go to group」を選択すると、ユーザーをそのグループのツリー上の位置に移動させます。

+ グループを削除するを選択すると、グループ削除の確認ポップアップが表示されます。

各レコードの右上メニューをクリックすると、「グループに移動」と「グループを削除」の2つのオプションが表示されます。

3 – 新しいグループを追加:

+ ユーザーがrootグループに属している場合：すべてのグループを新規追加できます。

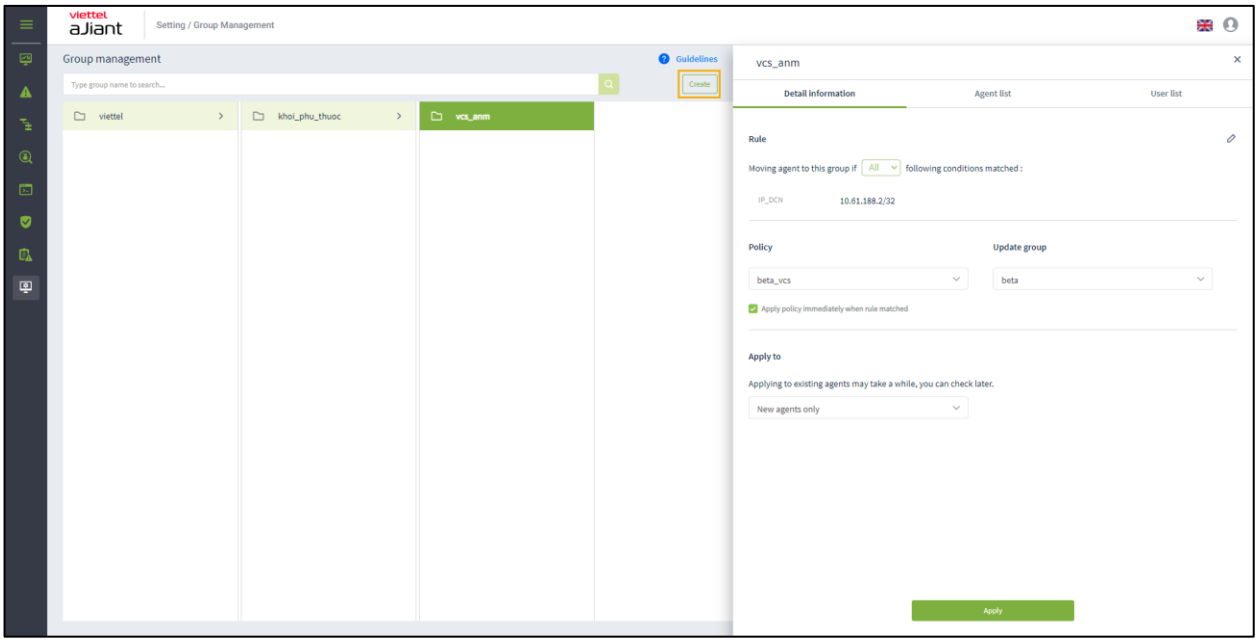
+ ユーザーがデフォルトグループに属している場合：新規追加できません。

+ ログインしているユーザーの親グループに属する場合、そのユーザーが所属するグループに対応する子グループを新規追加できます。

+ ユーザーが属するグループが一つまたは複数の子グループの場合、ログイン中のユーザーの属するグループに対応する新しい子グループを追加することができます。

- 作成するグループの位置を選択してください。

+ 元のグループリストで新しいグループを作成する場合は、画面右上の「Add new」ボタンをクリックするか、画面上の元のグループリストの末尾にカーソルを合わせて「Add new」をクリックしてください。



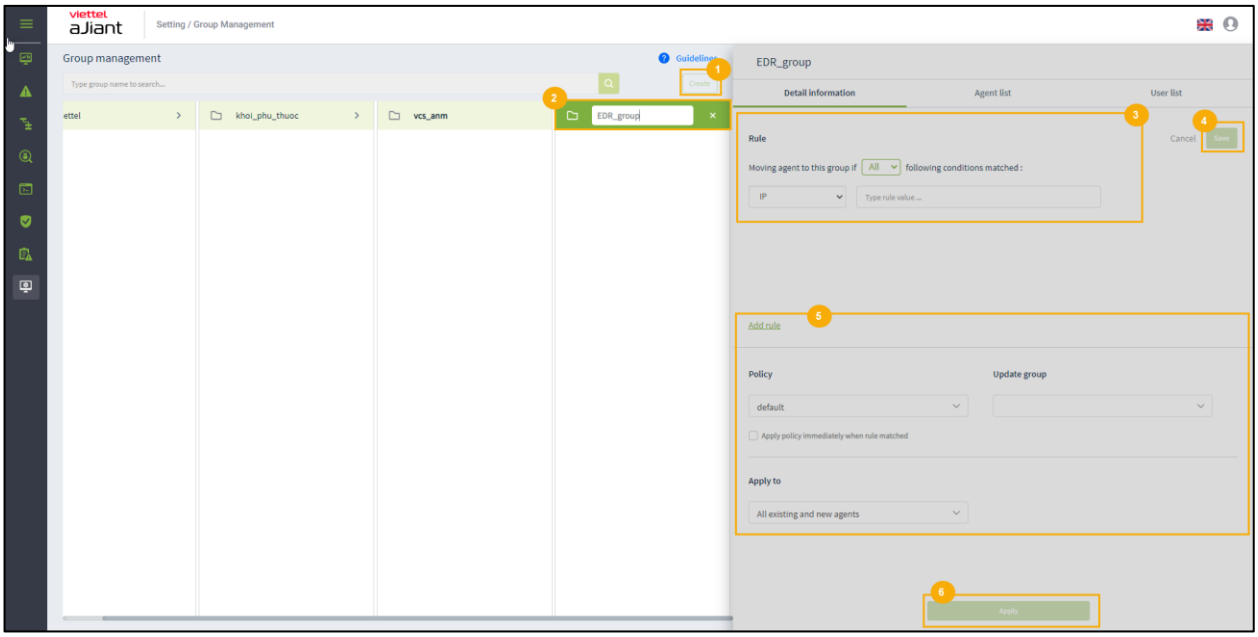
+ 新しいグループを親グループまたはレベル1、レベル2のグループのサブグループとして作成する場合は、親グループをクリックし、画面上の「作成」をクリックするか、同じレベルのグループリストの末尾にカーソルを合わせて「作成」をクリックしてください。

- **グループ名とルール設定を入力してください。**

注意：名前および設定ルールは、既存の名前およびルールと重複してはいけません。

+ 「すべて」オペレーターを選択した場合：両方の条件が満たされたときにルールが適用されます。

+ 「Any」演算子を選択した場合：いずれか一方または両方の条件が満たされていればルールが適用されます。



- ポリシーの選択およびルールを満たす場合にポリシーを適用するエージェントの種類：

「適用」をクリックした後、エージェントが「エージェントリスト」タブでグループに移動されていることを確認します。ルールを満たしたエージェントがリストに表示され、追加したグループに移動されます。「適用先」の選択に応じて、システム内のエージェントのグループ移動が行われます。

+ 既存のすべてのエージェント：システム内に存在するすべてのエージェントのグループを変更しますが、新たにインストールされたエージェントは、ルールに一致していてもグループは変更されません。

+ 新規エージェントのみ：適用後に新たにインストールされたエージェントに対してのみグループを変更し、既存のエージェントはルールに該当してもグループを変更しません。

+ 既存および新規のすべてのエージェント：ルールに一致する場合、適用後にシステム内のすべての既存エージェントおよび新規インストールされたエージェントをグループ移動する。

注意：

+ 「ルールに一致した場合にポリシーを即時適用する」チェックボックスを選択し、「適用」ボタンをクリックすると、選択されたエージェントは設定されたルールと値を照合し、一致した場合は「ポリシー」項目で選択されたポリシーにエージェントのポリシーを変更し、同時にグループも変更します。

上記のチェックボックスを選択しない場合、[適用]をクリックすると、選択されたエージェントはグループが変更されますが、ポリシーは変更されません。つまり、エージェントは異なるポリシーを持つグループに移動しても元のポリシーを保持します。一方、新規インストールされたエージェントはルールに一致すると、グループが変更され、「デフォルト」ポリシーが適用されます（チェックボックスを選択しないため、デフォルトポリシーが適用されます）。

+ もし新しいエージェントが複数のグループのルールに一致する場合、グループの修正時間は考慮せず、最も新しく作成されたグループに優先的に割り当てられます。

4 – グループの編集：1つまたは2つ、または3つすべての構成要素（ルール、ポリシー、適用先）を選択して編集できます。

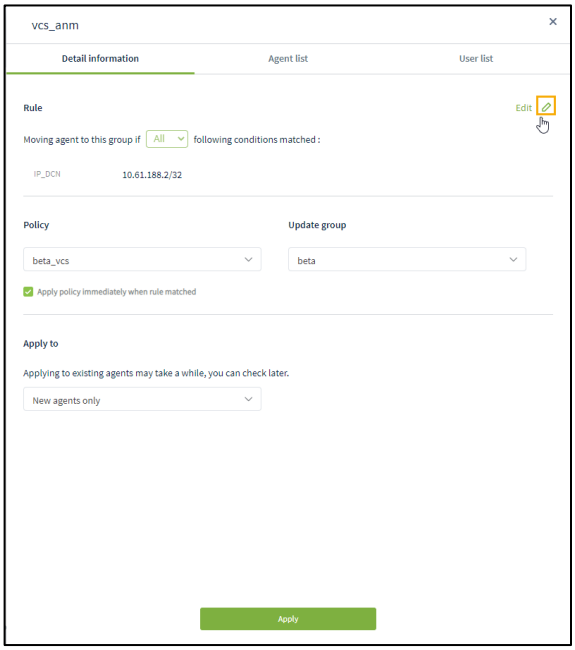
+ ユーザーがrootグループに属している場合：システム内のすべてのグループを変更できます。

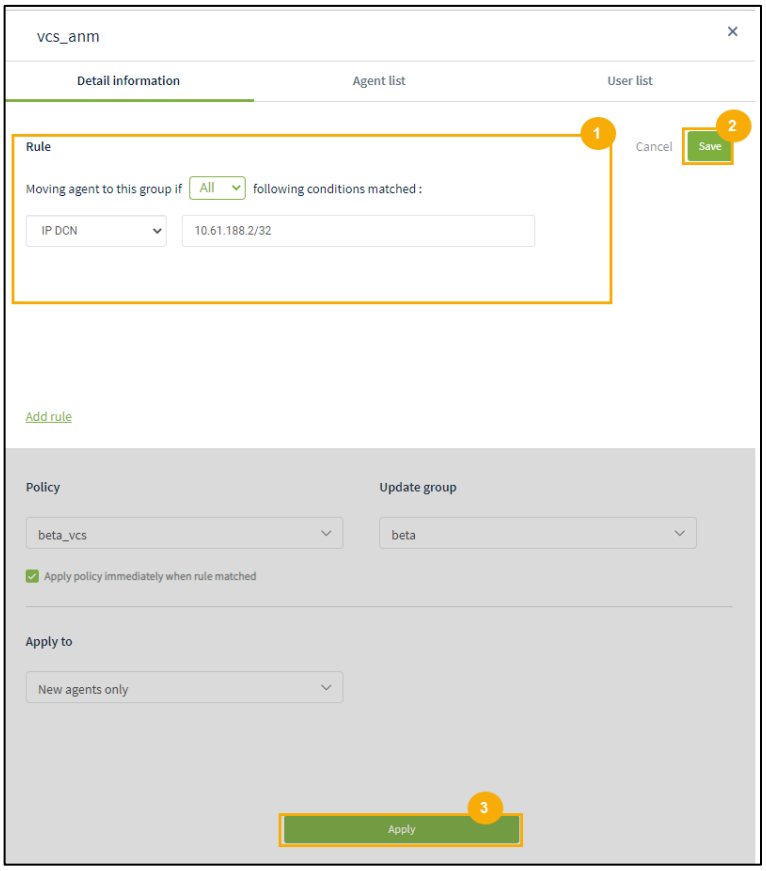
+ ユーザーがデフォルトグループにログインしています：デフォルトグループは変更できません。

＋　ユーザーが親グループにログインしている場合：ログイン中のユーザーのロールが属する子グループのロールも含め、すべての所属グループを編集可能です。

＋　ユーザーが一つまたは複数のグループに属している場合：ログインしているユーザーが所属するすべてのグループを編集できます。

＋　グループのルールを編集するには、編集アイコンをクリックし＞グループのルールを修正してから保存をクリックします＞その後、「ポリシー」と「適用先」の項目を編集し、適用をクリックしてください。





注意：

+ グループの構成要素（ルール、ポリシー、または適用先）を修正した後に「適用」をクリックしなかった場合、編集内容は保存されますが、エージェントリストは更新されません。新規にインストールされたエージェントについては、以下のように処理します。

- グループの変更：新しいエージェントが「適用先」項目で選択されているかどうかに依存し、選択されている場合はエージェント側で確認し、グループのルールが一致すればそのグループに変更されます。

- ポリシーの適用：エージェントのポリシーは「ルールに一致した場合に今すぐポリシーを適用する」チェックボックスの選択に依存します。チェックボックスが選択されている場合はグループのポリシーが適用され、選択されていない場合はデフォルトのポリシーが適用されます。

+ グループの各コンポーネントを修正して「適用」をクリックすると、編集内容が保存されます。同時に、「適用先」部分で「すべての既存エージェント」が選択されている場合は、システム内のすべてのエージェント情報をスキャンし、エージェントのグループを変更した後、エージェントリストを更新します。

新しいエージェントについても、上記と同様に処理してください。

5 – グループの削除またはエージェントのグループからの削除：

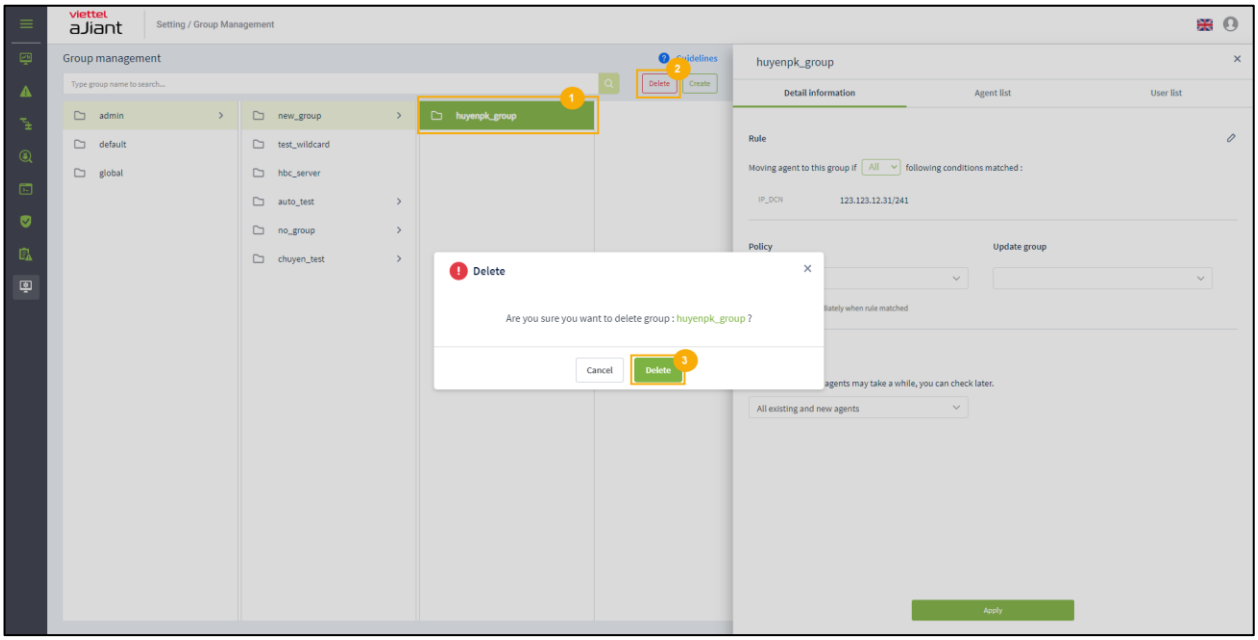
+ ユーザーがrootグループに属している場合：システム内のすべてのグループを削除できます。

+ ユーザーがデフォルトグループに所属している場合：デフォルトグループを削除してはいけません。

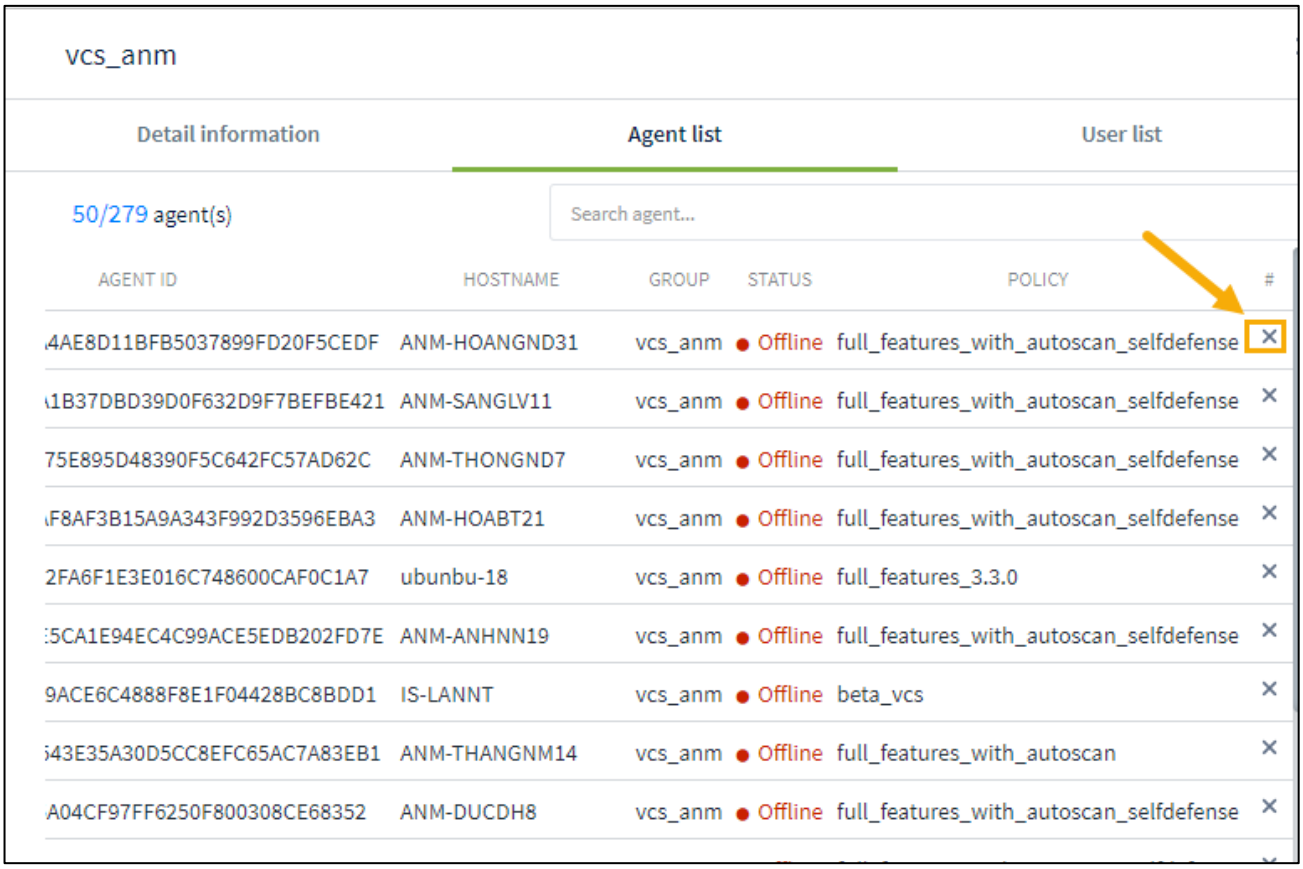
+ ログインしているユーザーが親グループに属している場合：ログイン中のユーザーのロールの子ロールに属する子グループおよびログイン中のグループをすべて削除できます。

+ ユーザーが一つまたは複数の子グループに属している場合：ログイン中のユーザーに属するすべてのグループを削除できます。

グループを削除するには、削除したいグループをクリックし、「Delete」をクリックした後、確認画面で「OK」をクリックしてください。グループを削除すると、そのグループに所属していたエージェントはデフォルトグループ「default」に移動し、ポリシーは変更されません。



エージェントをグループから削除するには、エージェントリストのタブをクリックし、「×」アイコンをクリックしてエージェントをグループから削除します。エージェントをグループから削除すると、エージェントはデフォルトグループ「default」に移動し、ポリシーはそのまま維持されます。



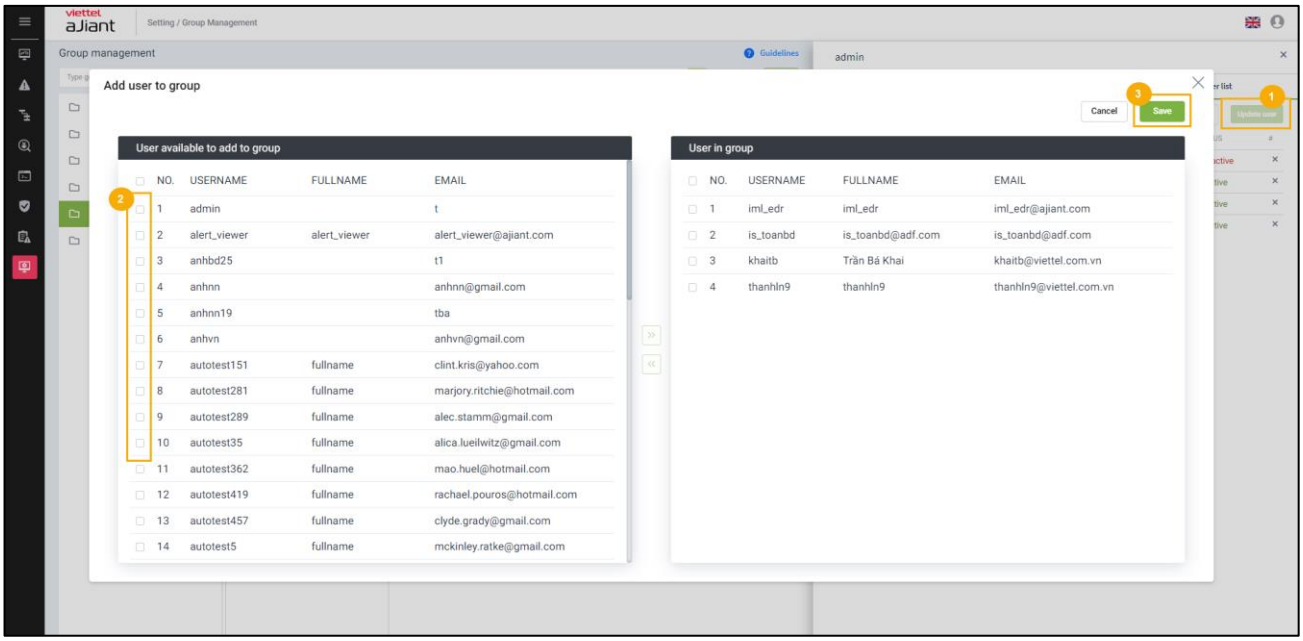
注意：親グループを削除する場合：

+ すべてのサブグループを削除する。

+ 親グループおよび子グループのすべてのエージェントをデフォルトグループ「default」に移動する。

+ 親グループと子グループのエージェントのポリシーを維持する。

6 – ユーザーをグループに追加する



ユーザーリスト：

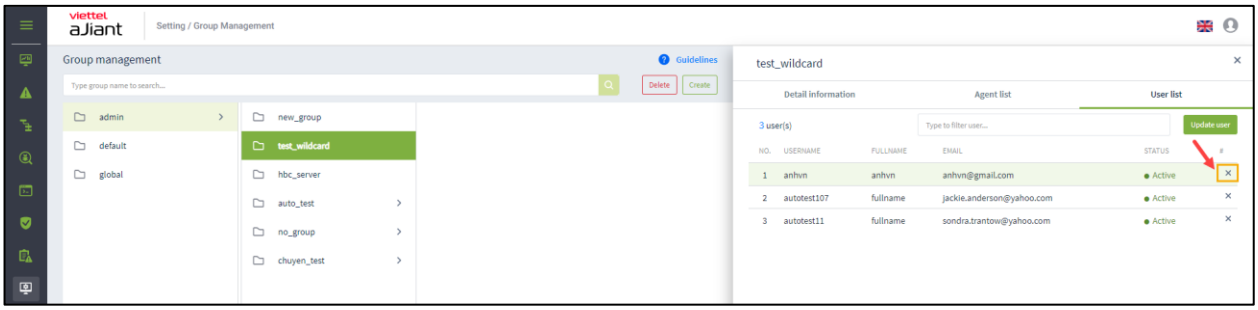
+ rootグループに属するユーザーがログイン：システム内のすべてのユーザーを表示する；

+ ユーザーがデフォルトグループに所属している場合：デフォルトにのみ所属するユーザーを表示する。

+ 親グループに属するユーザーのログイン：現在ログインしているユーザーと、そのユーザーが属する子グループのユーザーで、かつその子グループのロールがログイン中のユーザーのロールの子ロールに該当するユーザーを表示する。

+ ユーザーが一つ以上のグループに所属している場合：ログイン中のユーザーを表示する：

7 – ユーザーを削除する



3.6.4 アカウント管理

ポータルシステムのアカウント、権限、権限グループの管理

権限管理

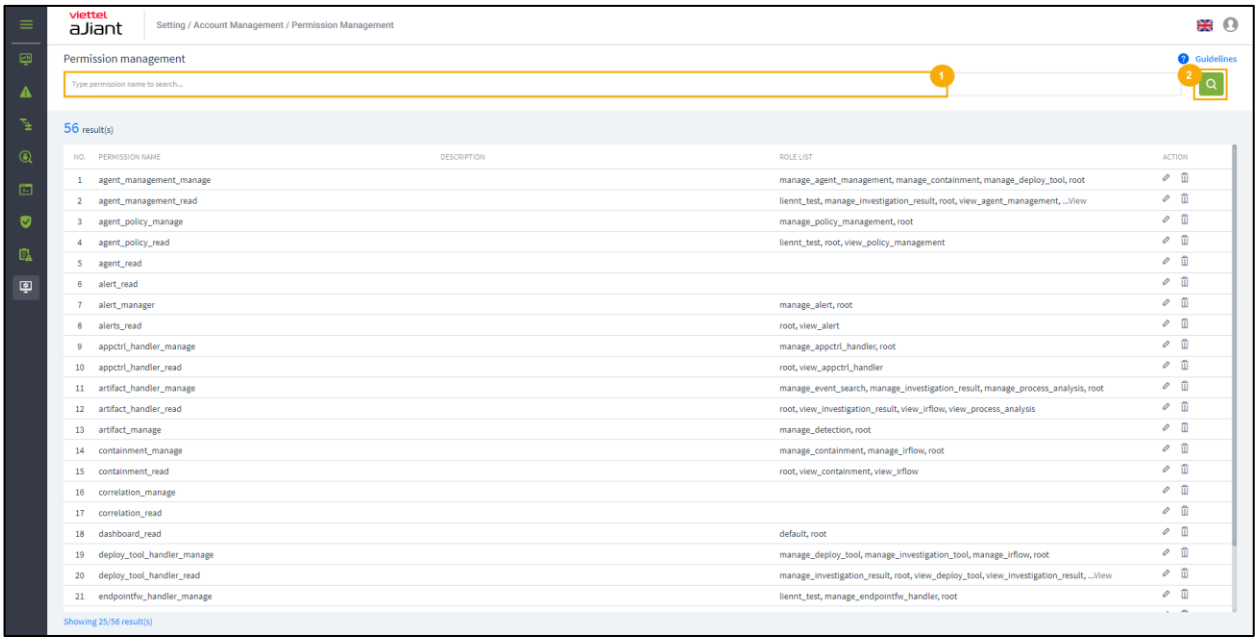
システムのリソース（API）へのアクセス権を管理します。1つのパーミッションは、システムの特定のリソース（API）へのアクセス権を指します。

この画面の主な機能：

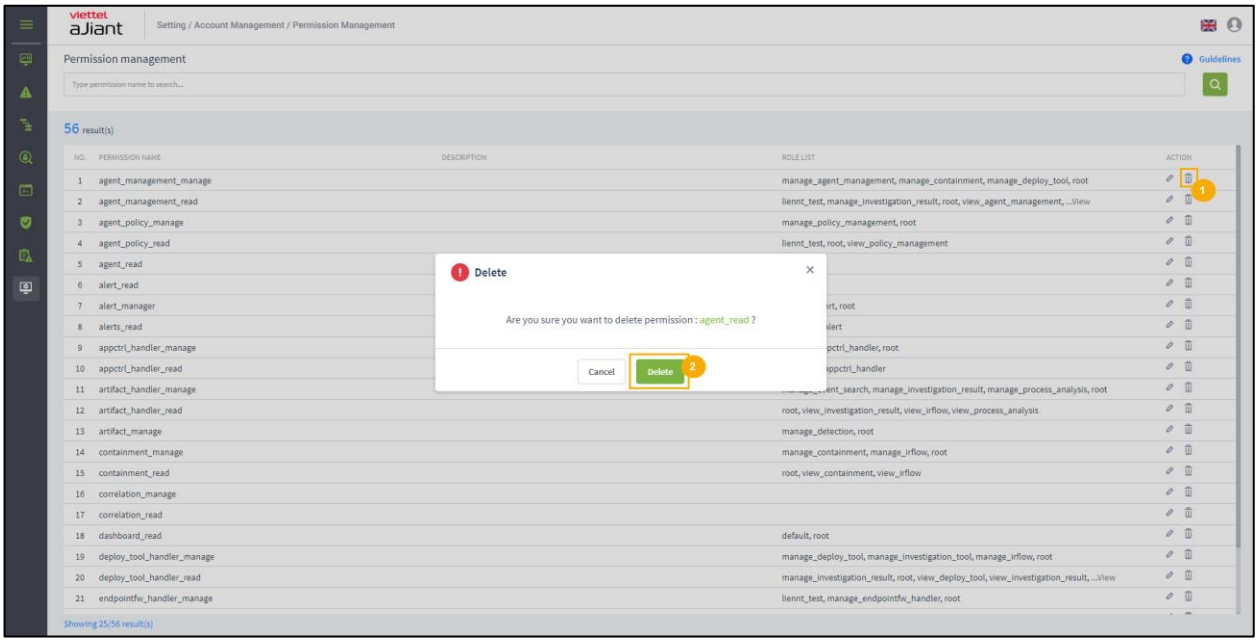
+ 権限の管理;
+ パーミッションを検索する;
+ 権限を削除する;

1 – 権限の管理：システムのすべての権限を表示します。この画面で権限を削除した場合、ポータル上で機能を実行する際に権限が不足していると、自動的に管理画面で削除した権限が追加されます。

2 – パーミッションの検索：検索ボックスに検索文字を入力し、Enterキーまたは「検索」ボタンをクリックすると、条件に合ったパーミッションの一覧が表示されます。



3 – 権限を削除するには、「削除」アイコンをクリックし、確認画面で「OK」をクリックすると、削除が完了します。



役割管理

システムのロール（権限グループまたはパーミッショングループ）の管理。

この画面の機能には以下が含まれます：

+ ロールリストの管理：

- ユーザーがrootロールでログインしている場合：システム内のすべてのロールを表示する。

- ユーザーがデフォルトのロールでログインした場合：デフォルトのロールを表示する。

- ユーザーが親ロールにログインした場合：ログイン中のユーザーに属するすべてのロールと対応する子グループを表示する。

- ユーザーがログインしているロールに一つ以上の子ロールがある場合：ログインしているユーザーのロールに属するすべてのロールを表示する。

+ 役割を検索する;

+ 新しい役割を追加する;

+ ロールを削除する。

1 – ロール一覧の管理：ツリー形式でロール一覧を管理します。デフォルトで作成されているルートに2つのロールがあります：「default」と「root」です。

+ ロール「default」：ユーザーは「default」権限を持ち、ポータルへのアクセスのみ許可されており、データの閲覧や機能の操作はできません。

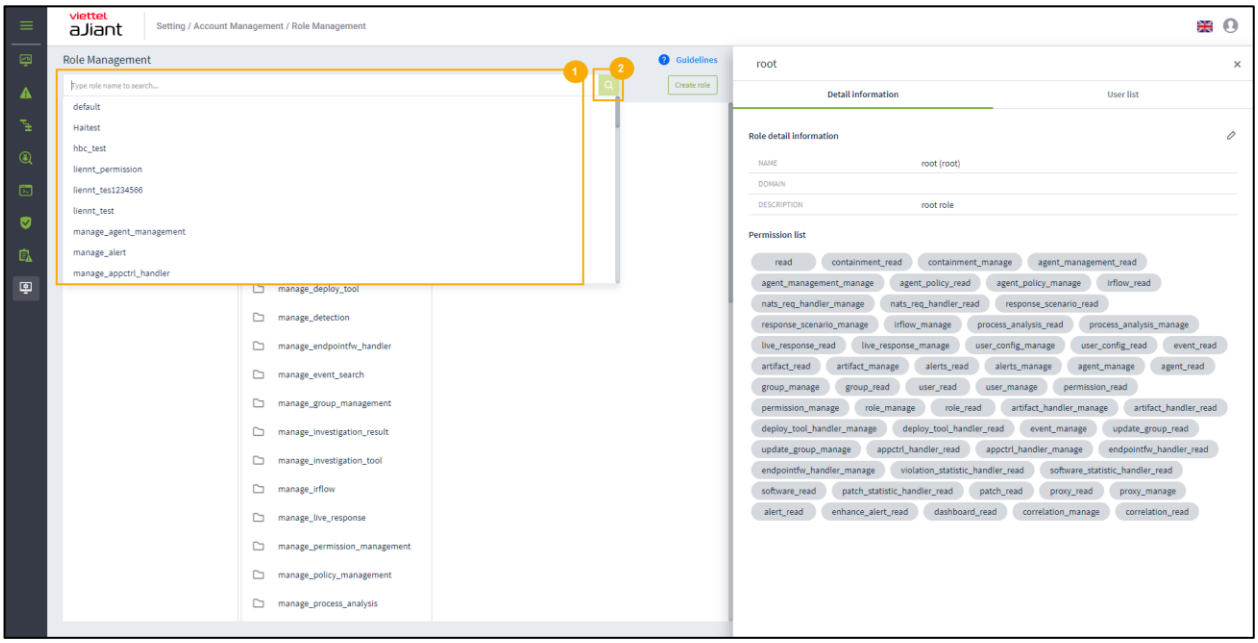
+ ロール「root」：システムのすべてのロールを含み、「root」ロールを持つユーザーは、ポータル上のすべての機能を使用する完全な権限を持ちます。

+ ロールをクリックすると、そのロールの詳細情報が表示されます。ロールには以下の情報が含まれます：ロール名、権限の一覧、ロールを持つユーザー（アカウント）の一覧、親ロールまたは子ロールの一覧（該当する場合）。

2 – ロールを検索する

+ 方法1：検索ボックスをクリックすると、システム内のロール一覧が表示され、スクロールしてロールを選択できます。

+ 方法2：検索ボックスをクリック > 検索文字を入力 > システムが検索文字を含むロールをフィルタリング > フィルタリングされたリストからロールを選択、またはEnterキーを押すか、「検索」ボタンをクリックしてください。



- レコードをダブルクリックすると、そのレコードの詳細情報が表示されます。

- 表示される詳細情報タブは「Detail」であり、ロールのデータにはロール情報とそのロールの権限が含まれます。
- 「User list」タブを選択すると、ロールを含むユーザーの一覧が表示されます。

+ レコードを右クリックすると「ロールへ移動」が表示されます。「ロールへ移動」をクリックすると、元のツリー形式のロール一覧に戻ります。

+ 各レコードの右上メニューをクリックすると、「役割へ移動」オプションも表示されます。

3 – 新しい役割を追加する:

+ ユーザーがrootグループに属している場合：すべてのデータツリー内のすべてのロールを新規追加できます。

+ ユーザーがデフォルトグループに属しているため、新規追加できません。

+ ユーザーが親グループに属している場合：ログインしているユーザーのグループに対応する子ロールを新規追加できますが、同階層のロールを新規追加することはできません。

+ ユーザーが属するグループが一つまたは複数の子グループの場合、ログインしているユーザーのグループに対応する新しい子グループを追加することができます。

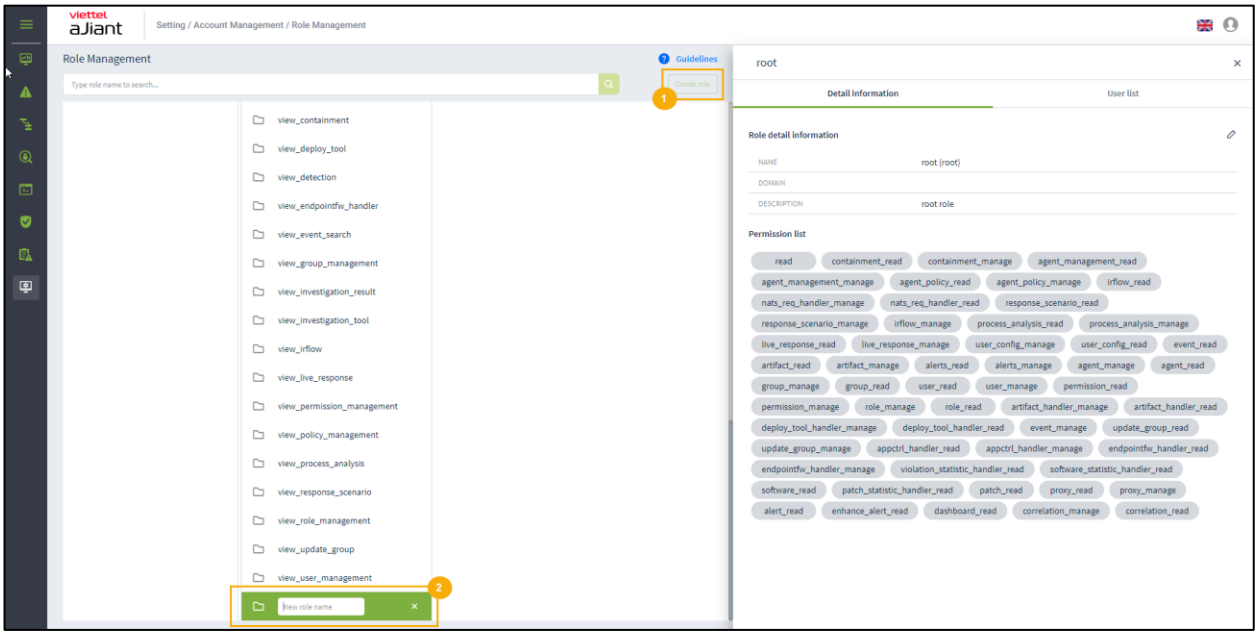
- **ロールを新規作成する方法は以下の通りです。**

1つのロールをクリックし、その後ロール一覧の最後にカーソルを合わせて「新規追加」を選択すると、選択したロールと同じ階層のロールを作成できます。

画面の「新規追加」をクリックして、選択したロールの子ロールを作成してください。

列の上で右クリックし、「新しい役割を追加」を選択してください。

その後、システム内に既に存在するロール名と重複しないロール名を入力してください。



- アイコンの「編集」をクリックしてロールの権限情報を追加します > 追加する権限を選択します > 「保存」をクリックします。

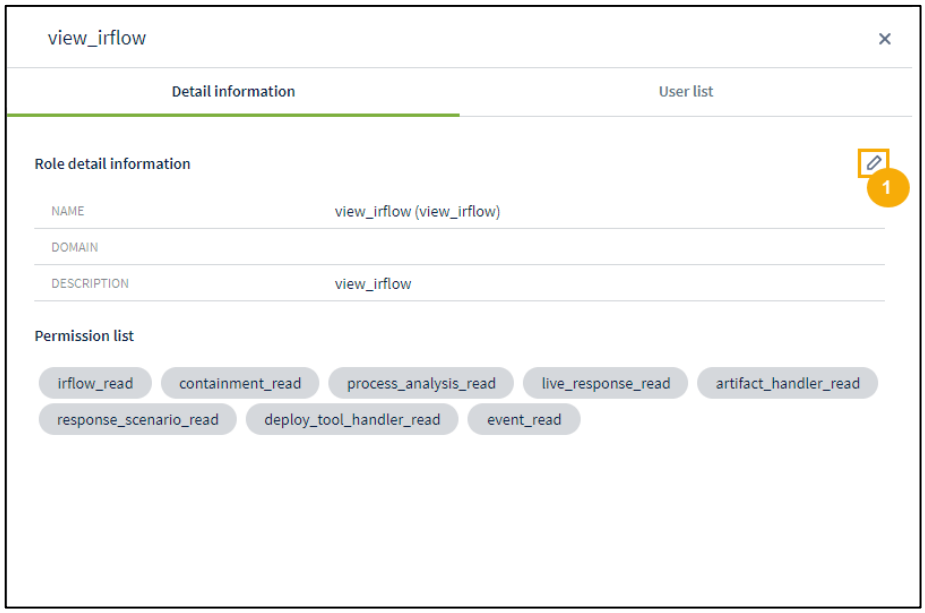
+ ユーザーがrootグループに属している場合：システム内のすべてのロールを編集できます。

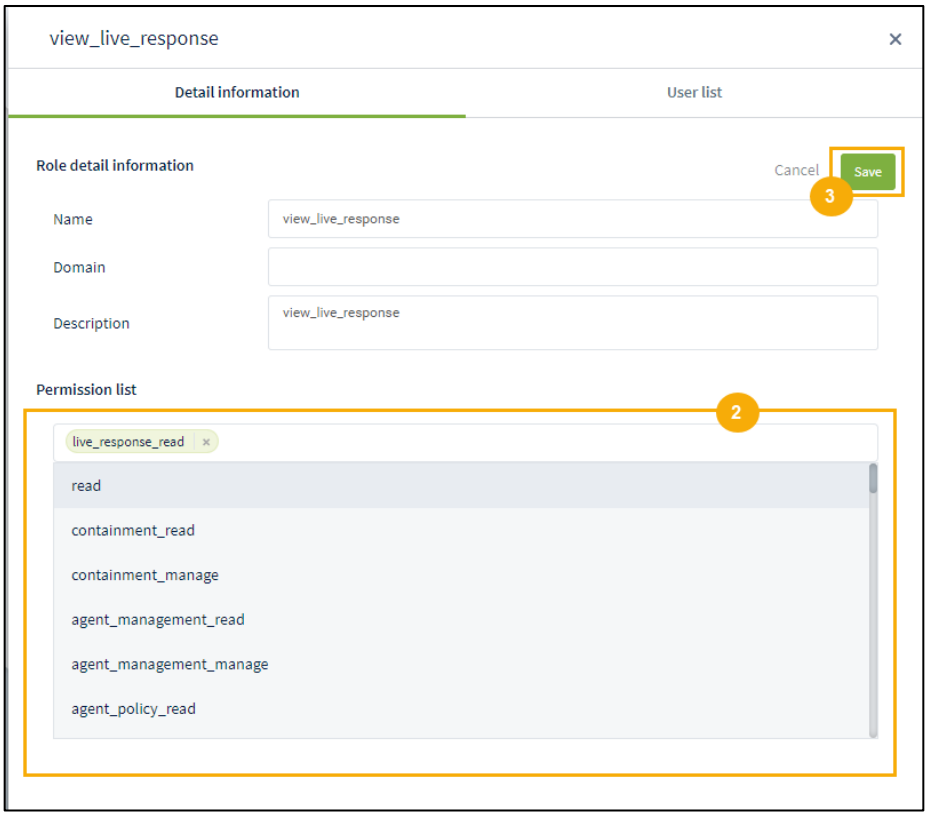
+ ユーザーがデフォルトグループに属している場合：デフォルトの役割は変更できません。

+ ユーザーが親グループにログインしている場合：ログイン中のすべてのロールおよび子ロールのロールを編集できます。

+ ユーザーが一つまたは複数のグループに所属している場合：ログイン中のユーザーに属するすべてのロールを編集できます。

注意：子ロールの権限リストは親ロールの権限リストの部分集合です。つまり、子ロールに割り当てる権限を選択する場合、その権限は親ロールの権限リストに含まれていなければなりません。





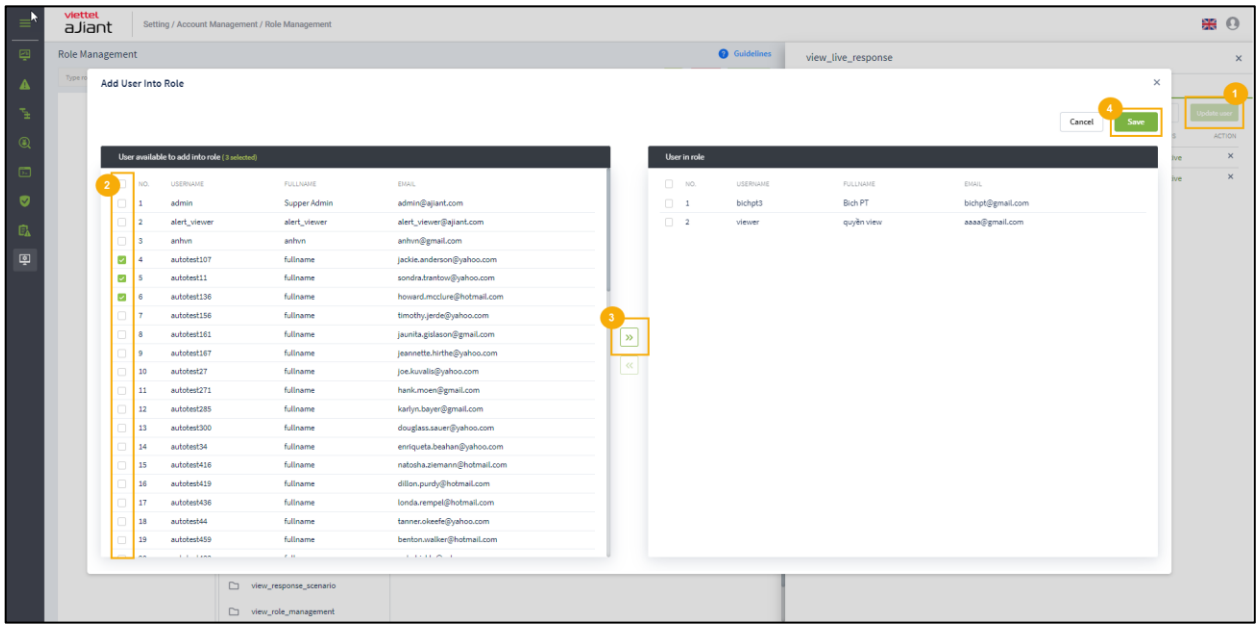
- ユーザーリストのタブに切り替えて、ユーザーのロールリストにロールを追加してください。

＋ ルートグループに属するユーザーがログインした場合：システム内のすべてのユーザーを表示する。

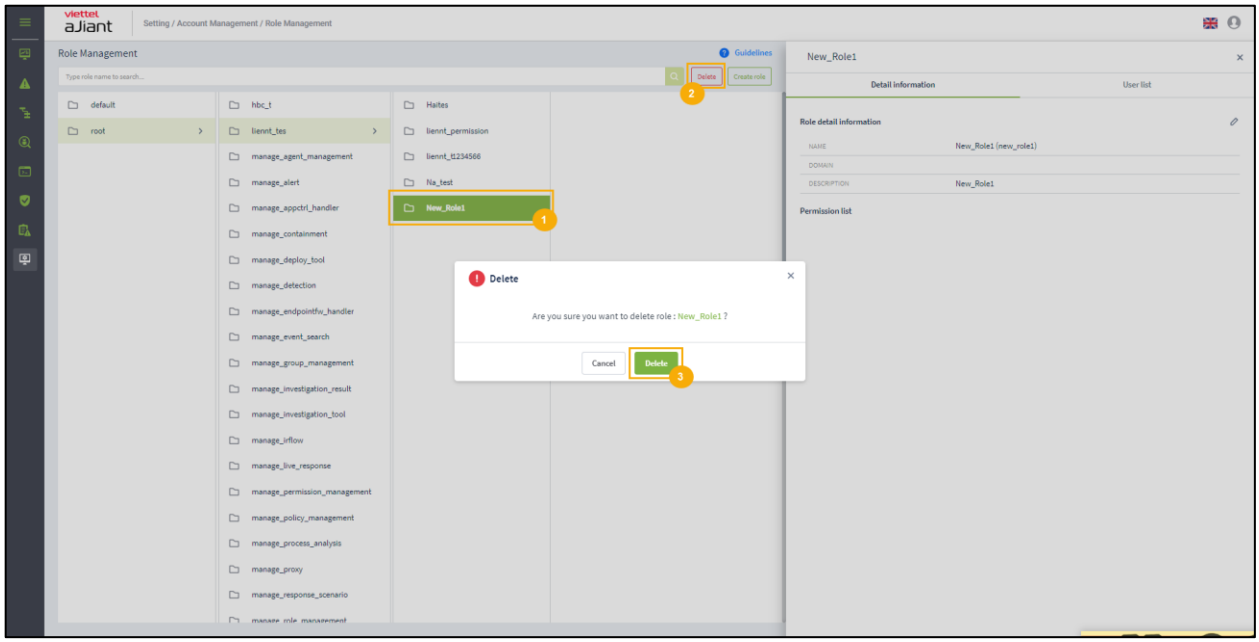
＋ ユーザーがデフォルトグループに所属している場合：デフォルトグループにのみ所属するユーザーを表示する。

＋ 親グループに属するユーザーのログイン：現在ログインしているユーザーと、そのユーザーが属する子グループのユーザーで、かつそのロールがログインユーザーのロールの子グループに属するものを表示する。

＋ ユーザーが一つまたは複数のグループに所属している場合：ログイン中のユーザーを表示する；



4 – ロールを削除するには、削除したいロールをクリックし、「Delete」を選択して、確認画面で「OK」をクリックしてください。



注意：ロールを1つ削除した後、そのロールを使用しているすべてのユーザーは次のように変更されます。ユーザーXが削除されたロールに属しており、かつユーザーXがそのロールのみを持っている場合は、ユーザーXをデフォルトロールに移行します。逆に、ユーザーXが複数のロールを持っている場合は、削除されたロールのみをユーザーXのロールリストから除外します。

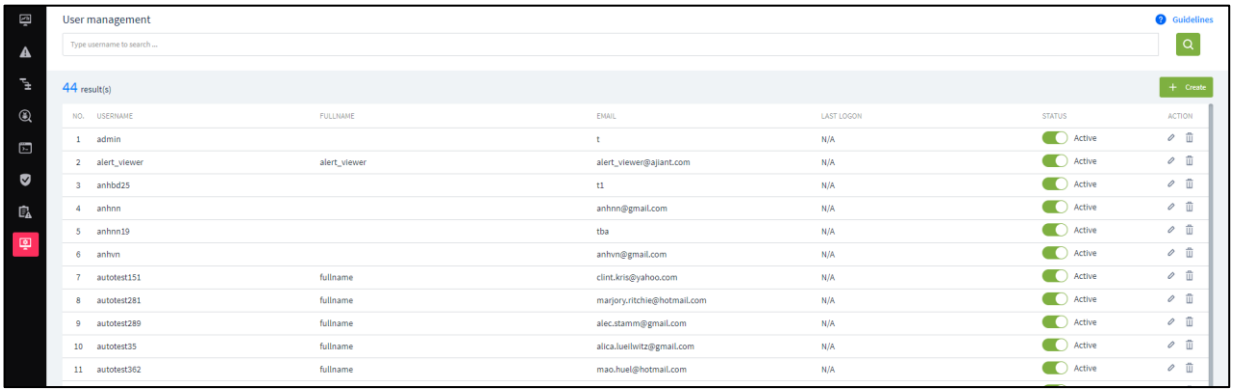
ユーザー管理

VCS-aJiantポータルシステムへのログインアカウントを管理する。

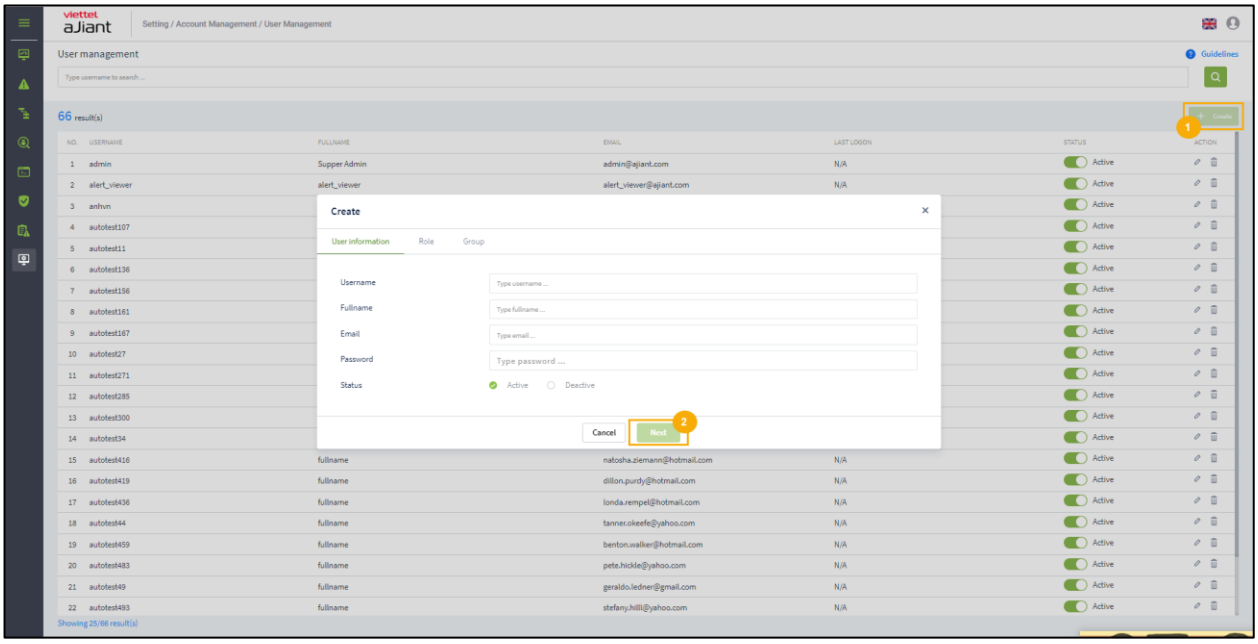
この画面の主な機能は以下の通りです：

+ アカウントを検索する;
+ 新しいアカウントを追加する;
+ アカウントの編集;
+ アカウントを削除する

1 – アカウント検索：検索ボックスをクリック > システム内のアカウント一覧が表示される > 一覧から検索したいアカウントを選択するか、検索ボックスに文字列<text>を入力してアカウントを絞り込む > 「検索」ボタンをクリックするか、絞り込まれたアカウント一覧から目的のアカウントを選択する。



新しいアカウントの追加：「作成」をクリック > 表示されたフォームに情報を入力 >「次へ」をクリック



+ アカウントに割り当てるロール（権限グループ）を選択し、「次へ」をクリックします。

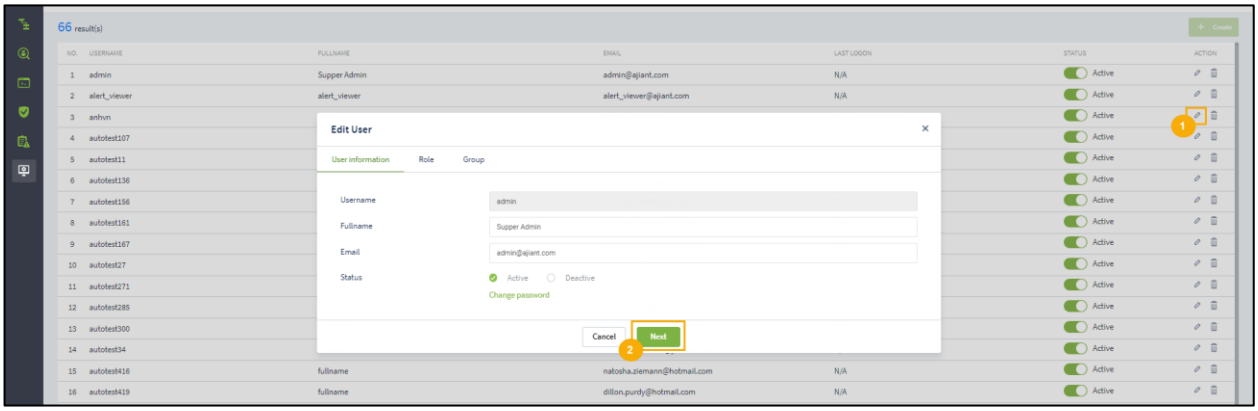
+ チェックボックスをクリックすると、それぞれのロールに対応する権限が表示されます。

- ユーザーがrootロールでログインしている場合：システム内のすべてのロールを表示する。

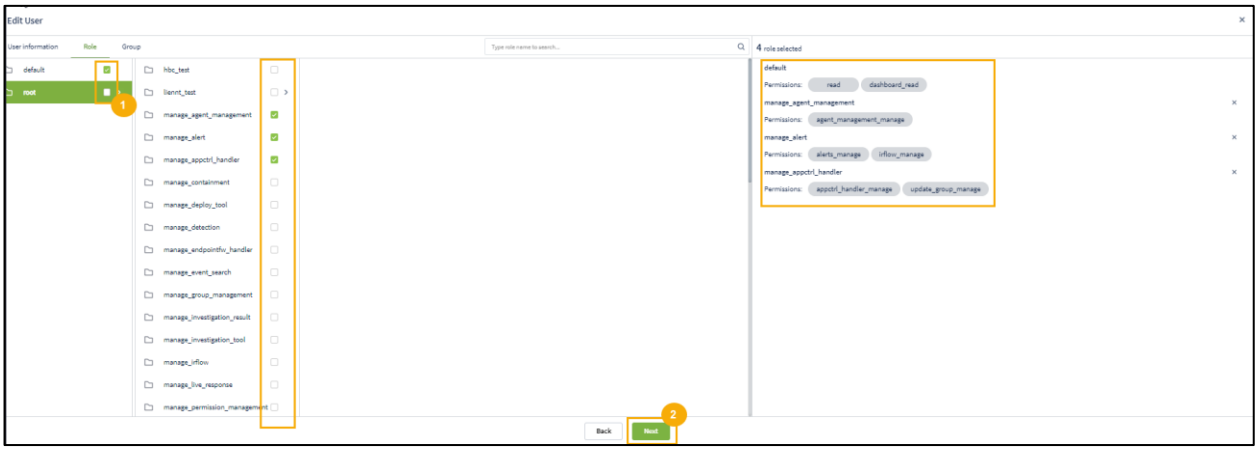
- ユーザーがデフォルトのロールでログインした場合：デフォルトのロールを表示する。

- ユーザーが親ロールにログインした場合：ログイン中のユーザーに属するすべてのロールと対応する子グループを表示する。

- ユーザーがログインしているロールに一つ以上の子ロールがある場合：ログインしているユーザーのロールに属するすべてのロールを表示する。



ユーザーに役割を追加する画面では、アカウント検索と同様に役割を検索できます。検索ボックス「Search」に文字を入力し、検索アイコンをクリックするかEnterキーを押すと、検索条件に合致する役割の一覧が表示されます。



+ 追加するロールに対応するチェックボックスをクリックし、その後「Go to role」をクリックして元のロール一覧画面に戻り、「Create」をクリックしてアカウントを作成してください。

+ 注意：現在ログインしているアカウントが新しいアカウントを作成する場合、作成できるのはログイン中のアカウントに付与されているロールのリストに含まれる子ロールのみです。

+ アカウントに割り当てるグループを選択し、「作成」をクリックします。

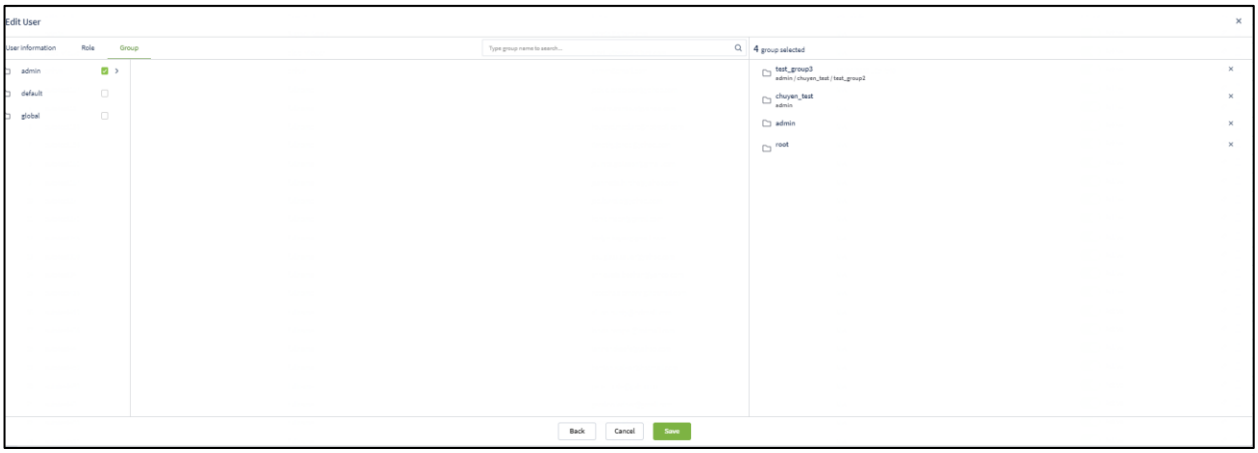
+ チェックボックスをクリックすると、それぞれのロールに対応する権限が表示されます。

- ユーザーがrootグループに属している場合：システム内のすべてのグループを表示する。

- ユーザーがデフォルトグループにログインした場合：デフォルトグループを表示する。

- ユーザーが親グループにログインした場合：ログイン中のユーザーの所属グループおよび対応する子グループを表示する。

- ユーザーが属するグループまたはその子グループに対して：ログインしているユーザーのグループに属するすべてのグループを表示する。



＋　追加するグループに対応するチェックボックスをクリックし、その後「Go to role」をクリックして元のグループ一覧画面に戻ります。次に「Create」をクリックしてアカウントを作成します。

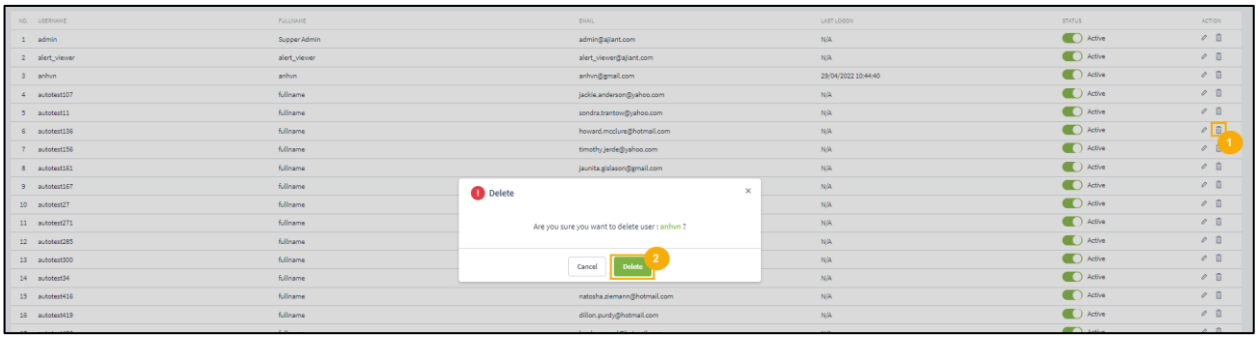
アカウント削除：削除アイコンをクリックし、その後確認画面で「OK」をクリックしてください。削除アイコンの表示を確認してください。

＋　rootグループに属するユーザーのログイン：システム内のすべてのユーザーを表示する；

＋　ユーザーがデフォルトグループに所属している場合：デフォルトにのみ所属するユーザーを表示する。

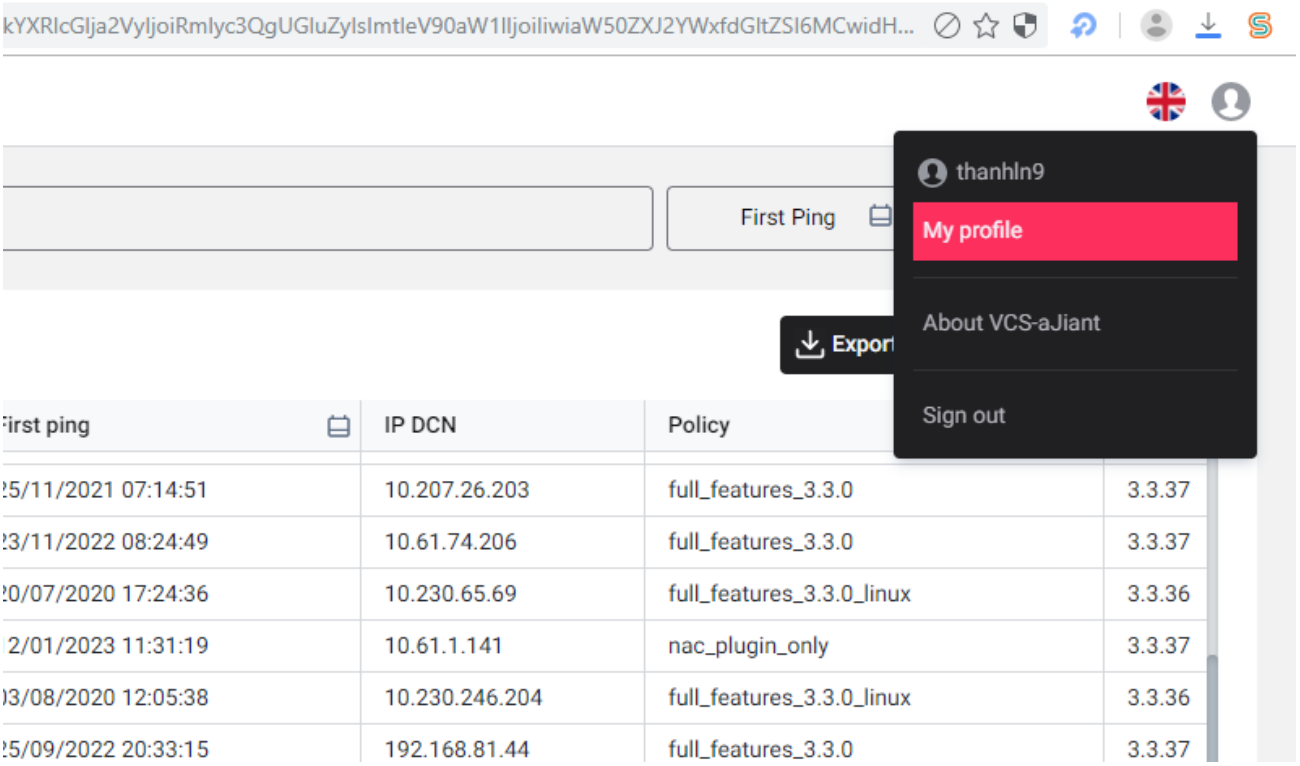
＋　親グループに属するユーザーのログイン：現在ログインしているユーザーと、そのユーザーが属する子グループのユーザーで、かつその子グループのロールがログイン中のユーザーのロールの子ロールに該当するユーザーを表示する。

＋　ユーザーが一つ以上のグループに所属している場合：ログイン中のユーザーを表示する；

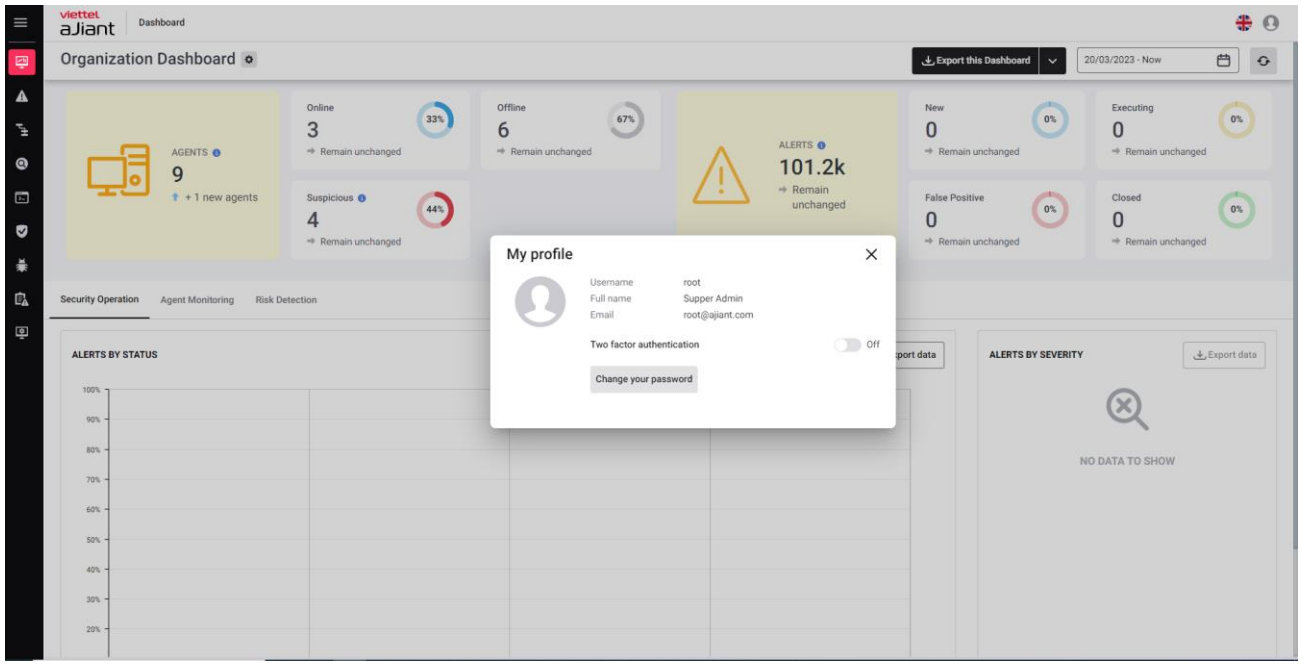


アカウントの二段階認証を有効にする：

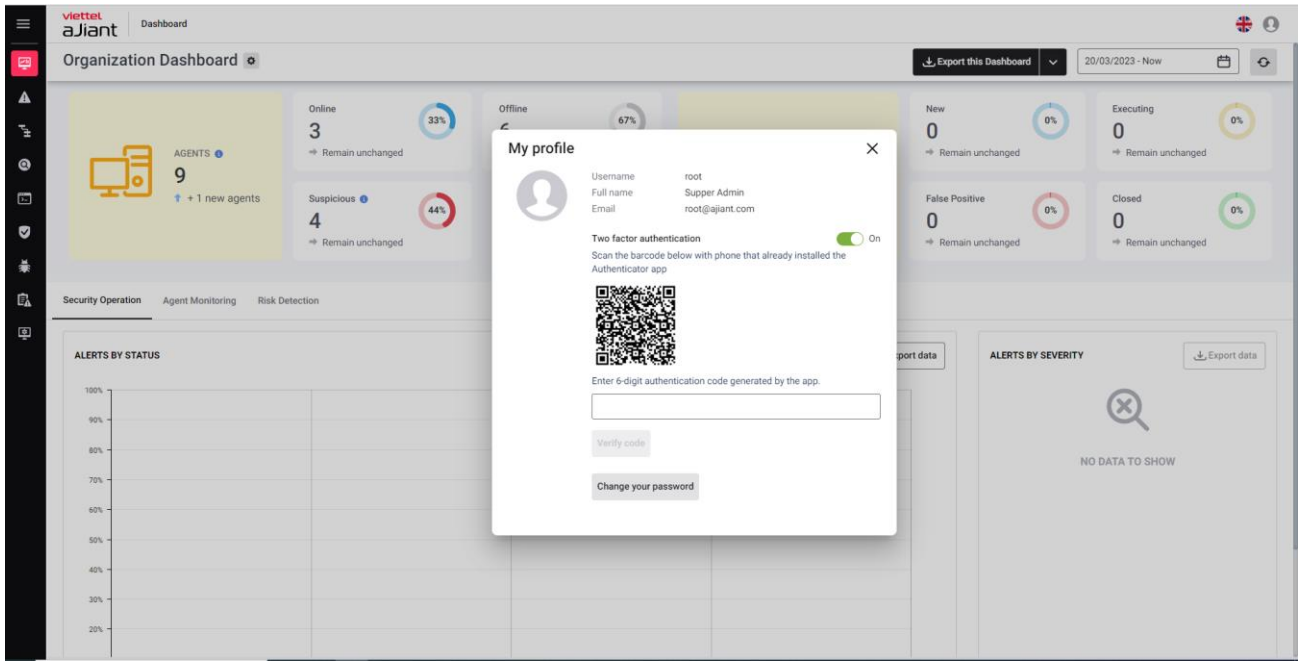
ステップ1：下の画像のように「マイプロフィール」画面にアクセスします。



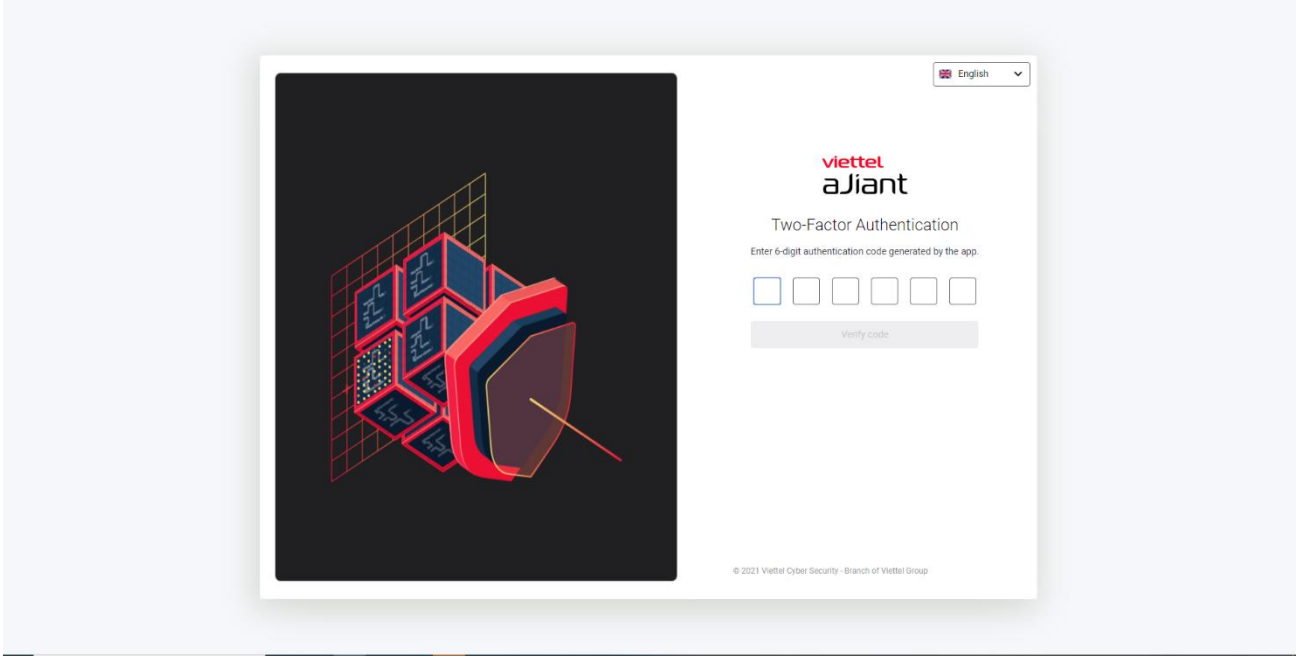
ステップ2：クリックして二要素認証を有効にする



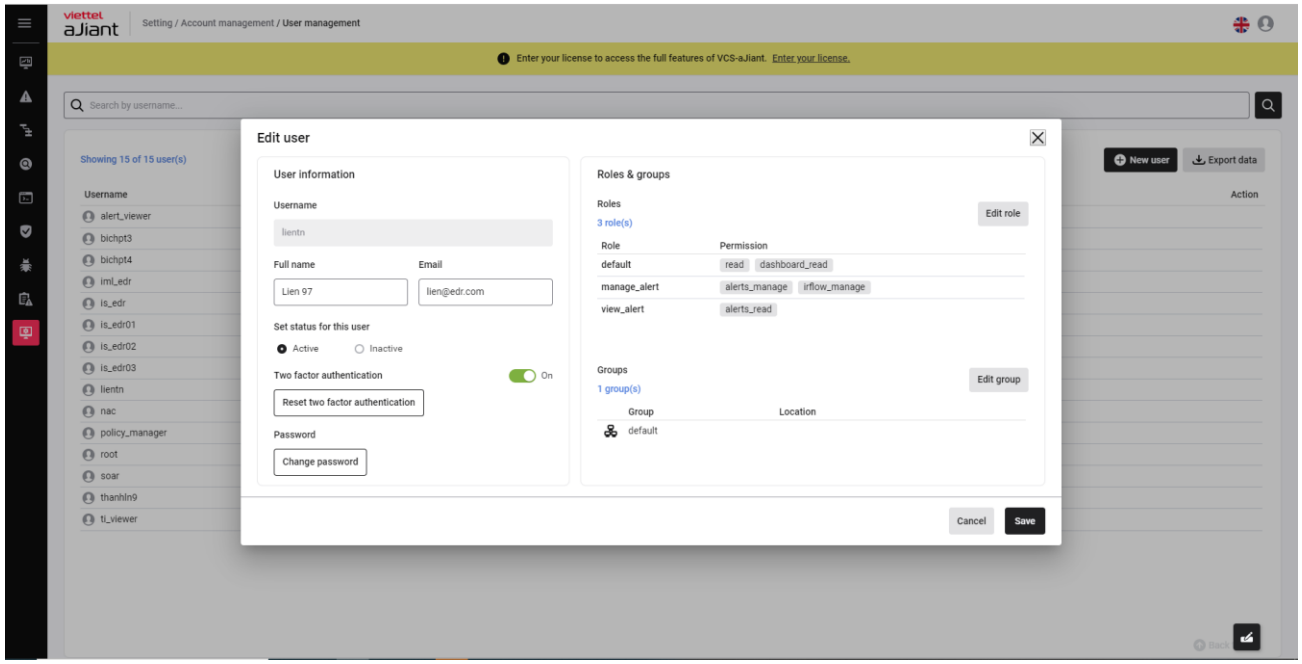
ステップ3：2FAアプリでQRコードをスキャンし、その後OTPを入力して2FAの設定を完了してください。



2段階認証（2FA）を有効にした後、ログイン時にユーザーは以下の画像のようにOTPの入力を求められます。



以下の画像のように、他のユーザーに対して2段階認証を有効にすることができます。



このソリューションは、すべてのアカウントに対して2段階認証を強制的に有効化することもサポートしています。

3.6.5 更新管理

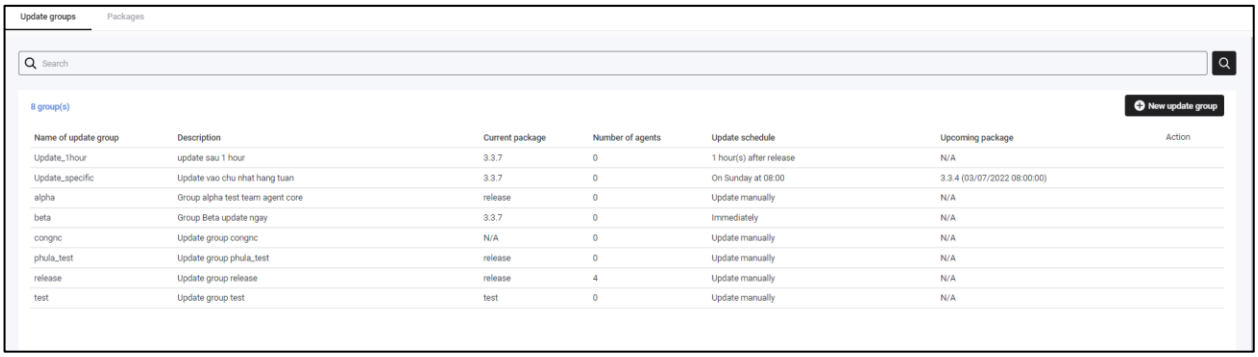
グループを更新する

目的：エージェントを更新グループに分けて管理しやすくするために、更新グループの管理、新規作成、および更新を可能にする機能。

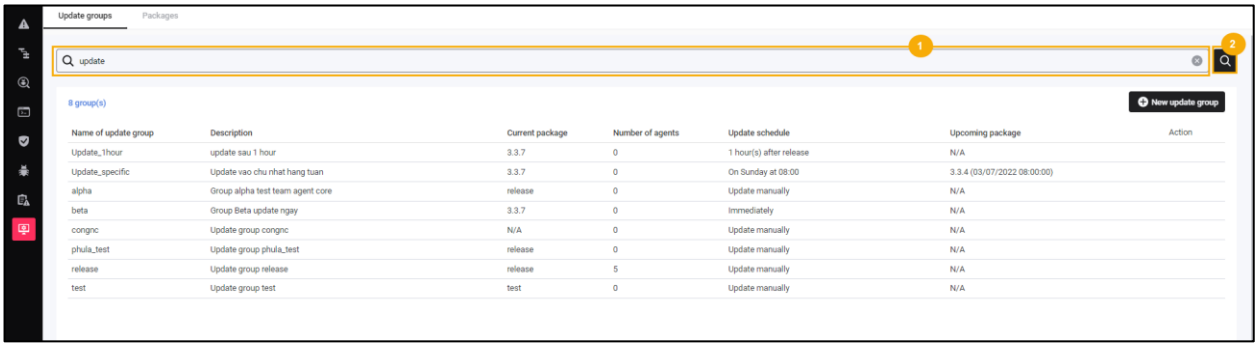
1 – 検索:

- 提供されたアカウントでポータルにログインしてください。
- 「設定」を選択すると、システムは以下のサブメニューを表示します：ポリシー設定、エージェント管理、グループ管理、アップデート管理、ルール相関、アカウント管理。

- 「Update Management」を選択すると、システムにUpdate Groupの一覧が表示されます。

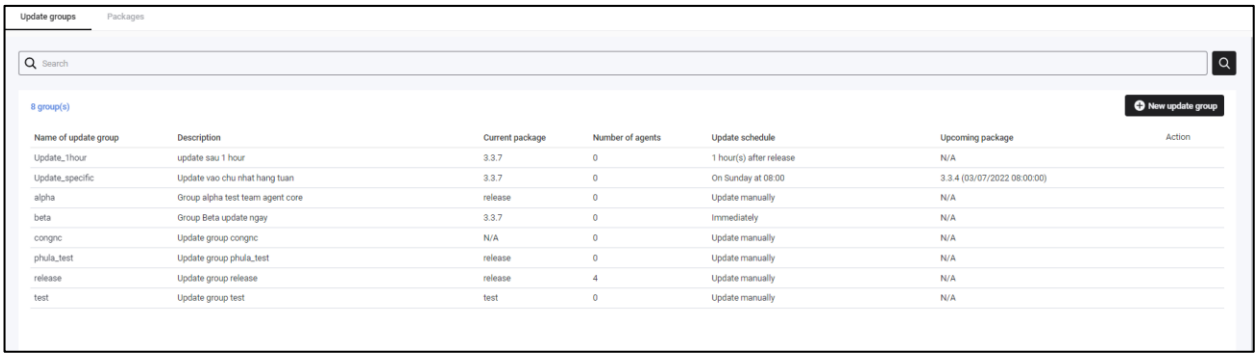


- 「Update Management」を選択すると、システムはUpdate Groupの一覧を表示します。
- 検索キーワードをテキストボックスに入力し、「検索」ボタンを選択してください。

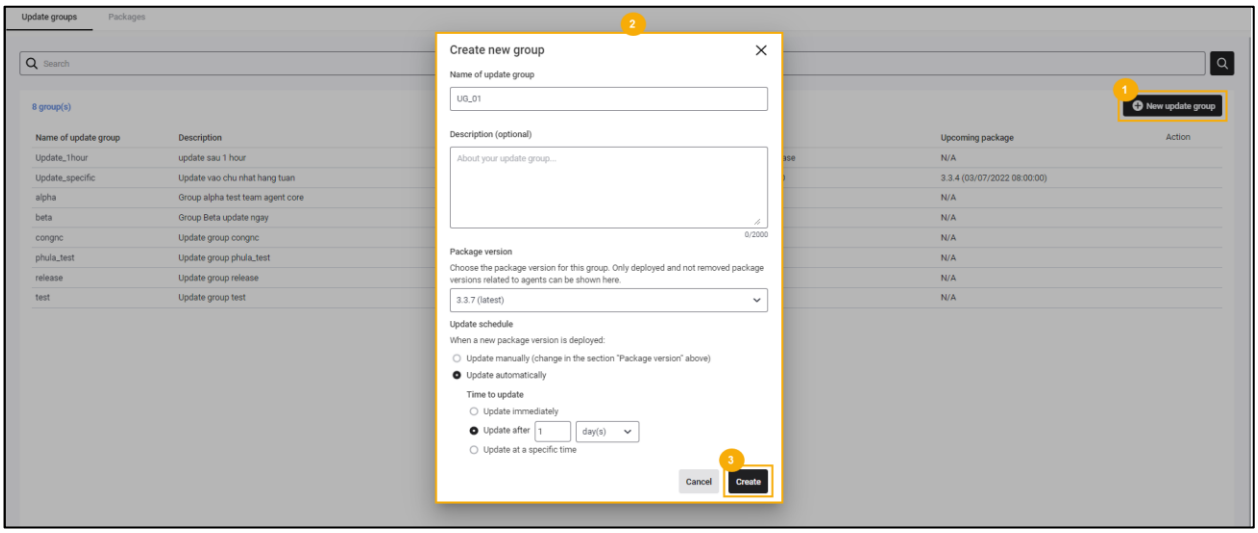


2 – グループの新規追加：

- 提供されたアカウントでポータルにログインしてください。
- 「設定」を選択すると、システムは以下のサブメニューを表示します：ポリシー設定、エージェント管理、グループ管理、アップデート管理、ルール相関、アカウント管理。
- 「Update Management」を選択すると、システムにUpdate Groupの一覧が表示されます。



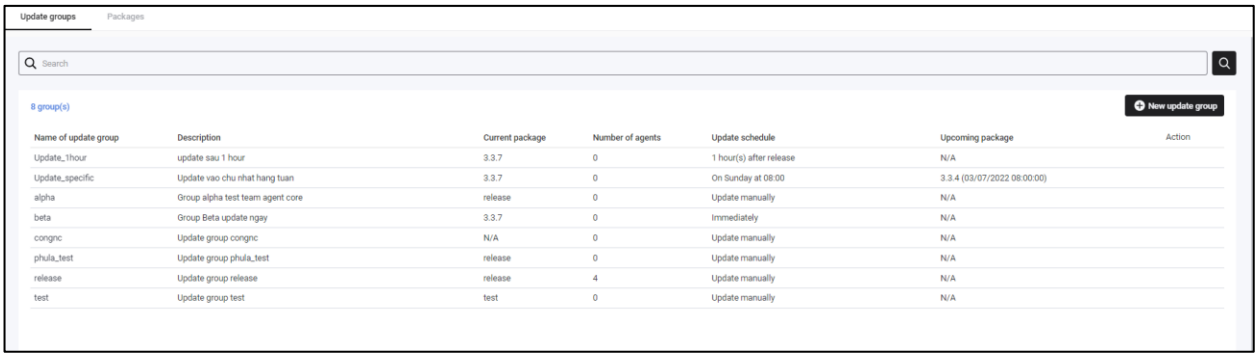
- 「New update group」ボタンを選択すると、システムは新しいアップデートグループ追加画面を表示します。



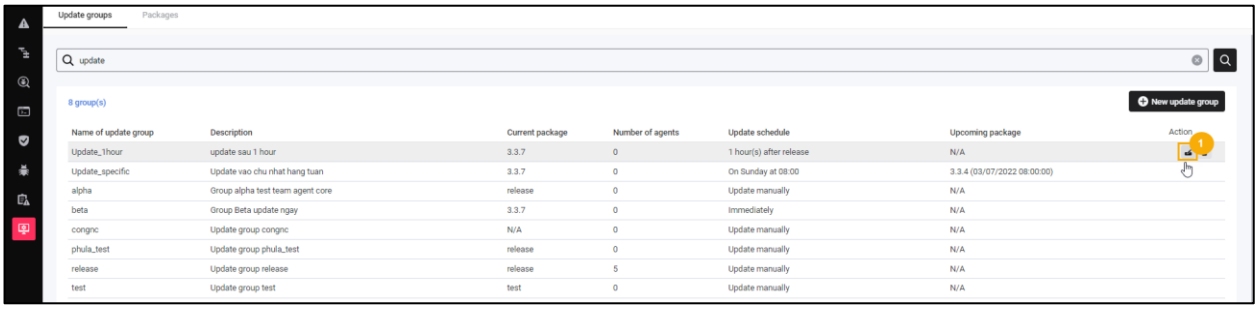
- 新しいアップデートグループの情報を入力し、「作成」ボタンを選択します。システムは情報を記録し、アップデートグループの一覧画面に戻ります。

3 – グループの更新:

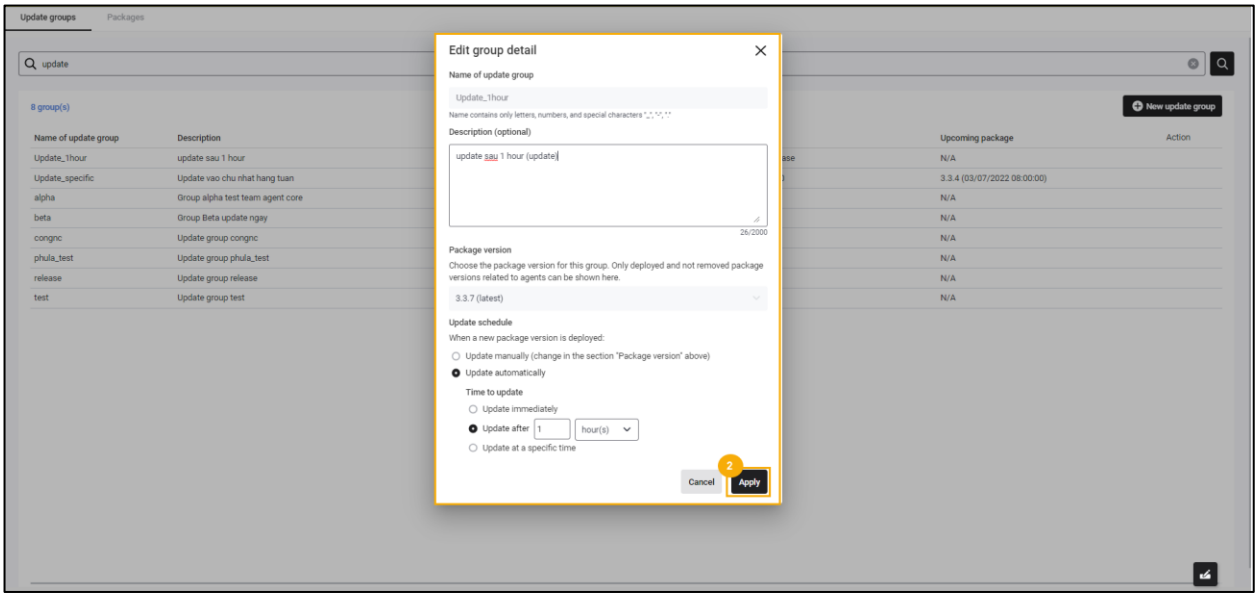
- 提供されたアカウントでポータルにログインしてください。
- 「設定」を選択すると、システムは以下のサブメニューを表示します：ポリシー設定、エージェント管理、グループ管理、アップデート管理、ルール相関、アカウント管理。
- 「Update Management」を選択すると、システムはUpdate Groupの一覧を表示します。



- 更新・編集が必要なレコードで、「更新」アイコンを選択し、情報を更新してください。

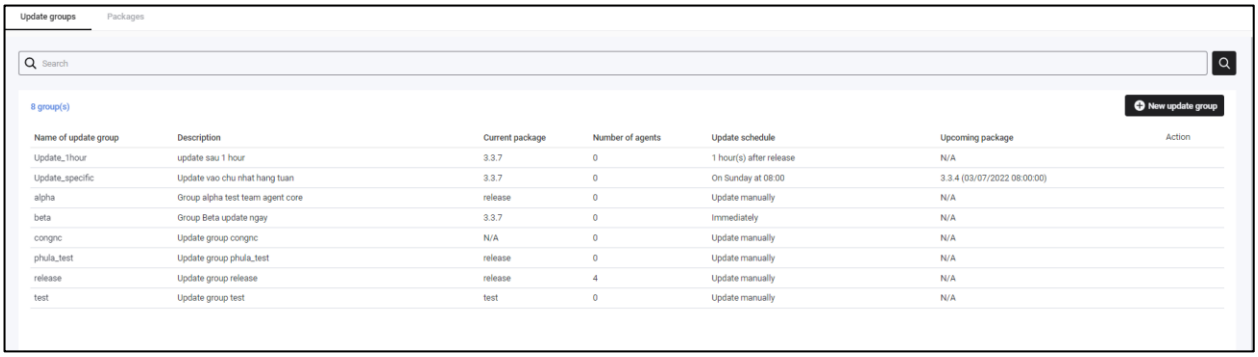


- システムは「Update Group」の詳細情報画面を表示し、情報の更新・編集を可能にし、「適用」ボタンを選択して保存します。

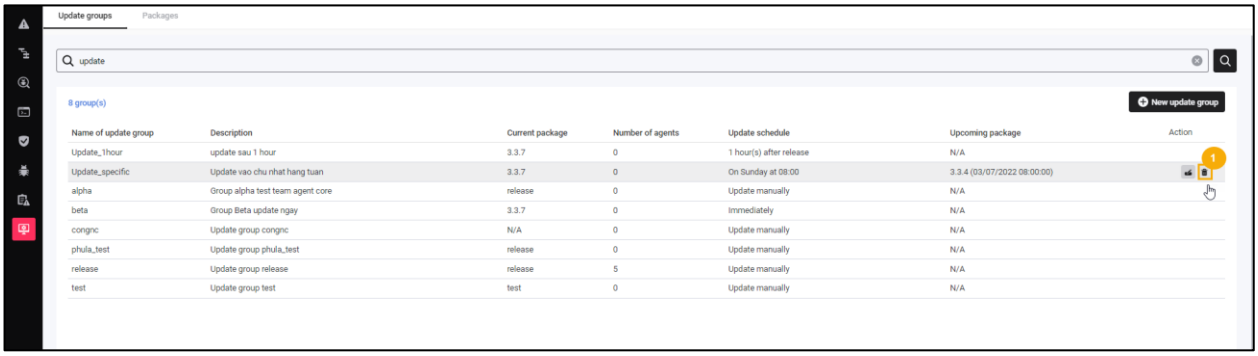


4 – アップデートグループを削除する：

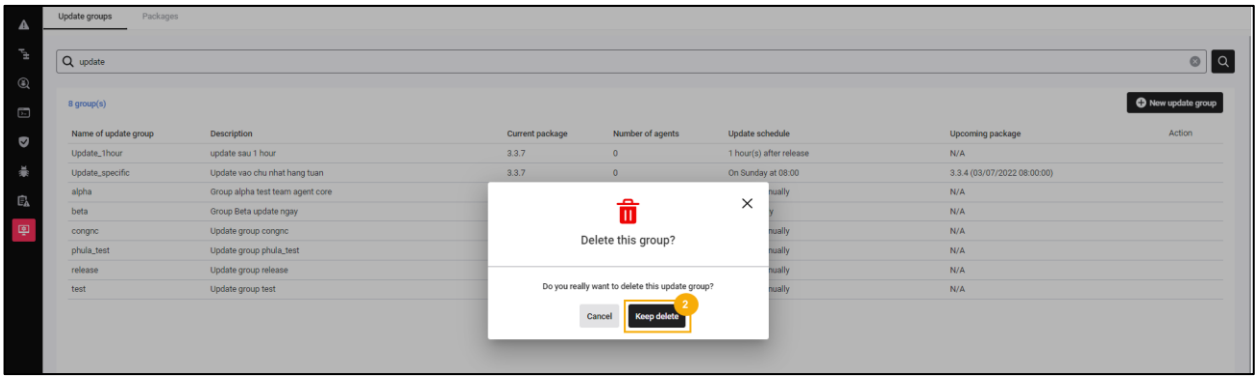
- 提供されたアカウントでポータルにログインしてください。
- 「設定」を選択すると、システムは以下のサブメニューを表示します：ポリシー設定、エージェント管理、グループ管理、アップデート管理、ルール相関、アカウント管理。
- 「Update Management」を選択すると、システムはUpdate Groupの一覧を表示します。



- 削除するレコードで、「削除」アイコンを選択し、グループを更新してください。



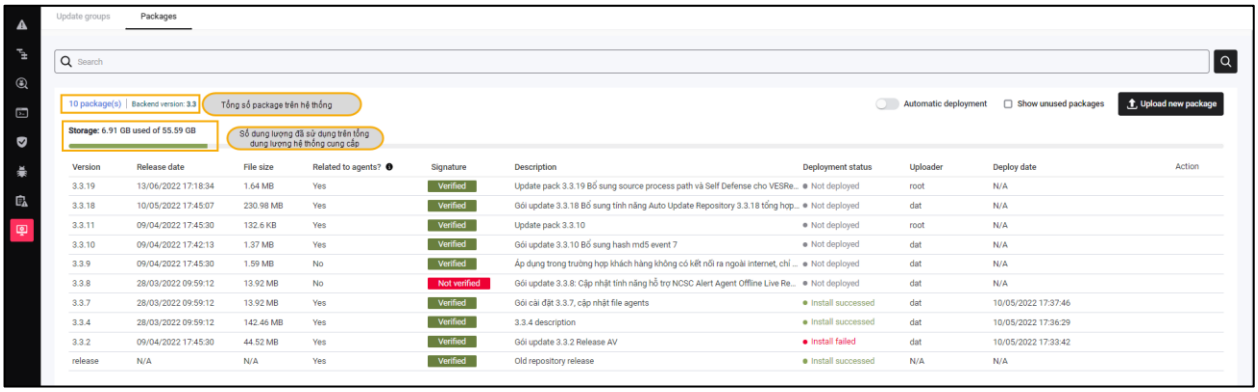
- システムは「Update Groupの削除確認」ポップアップを表示します。ユーザーは「削除」ボタンを選択してUpdate Groupの削除を確定し、「キャンセル」ボタンを選択して削除要求を取り消すことができます。



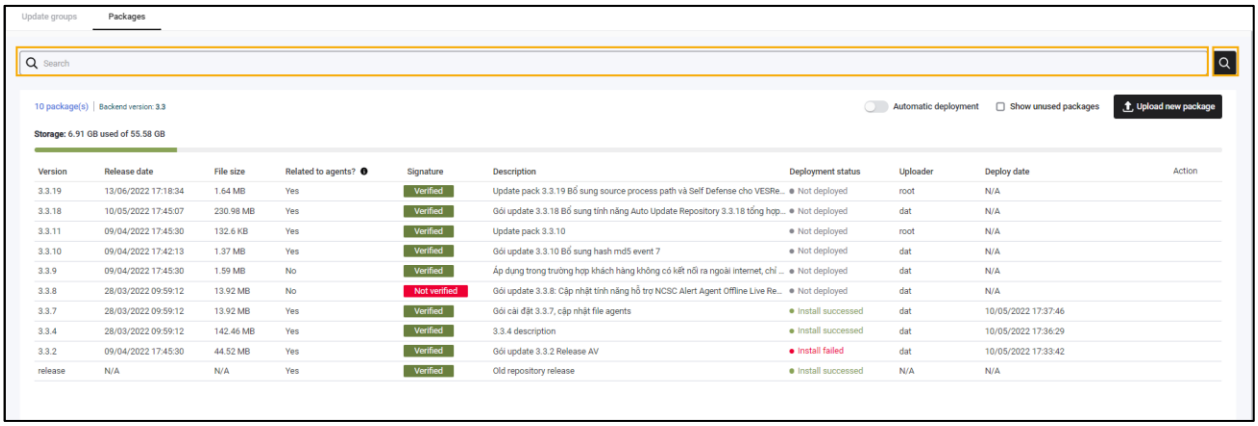
パッケージを更新する

1 – パッケージの検索：

- 提供されたアカウントでポータルにログインしてください。
- 「設定」を選択すると、システムは以下のサブメニューを表示します：ポリシー設定、エージェント管理、グループ管理、アップデート管理、ルール相関、アカウント管理。
- 「Update Management」を選択すると、システムはUpdate Groupの一覧を表示します。
- 「パッケージ」タブを選択すると、システムに登録されているパッケージの一覧が表示されます。



- 検索キーワードをテキストボックスに入力し、「検索」ボタンを選択してください。



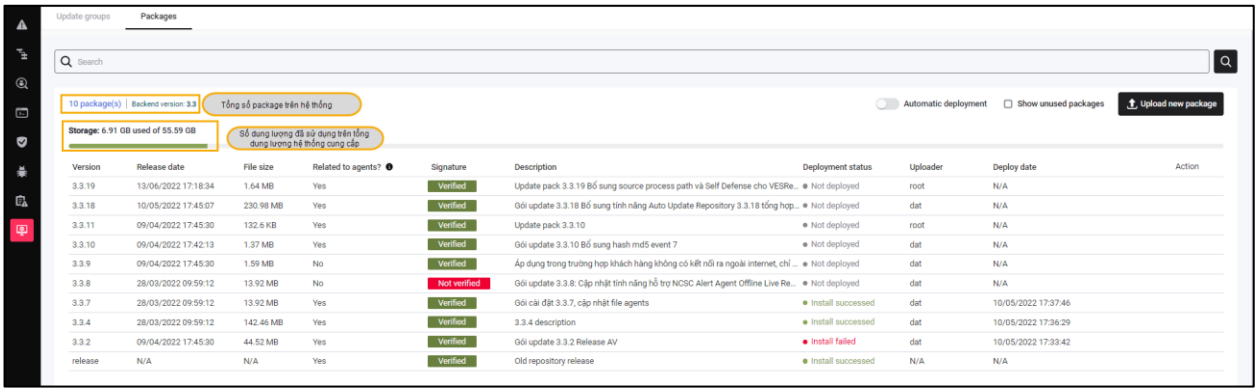
2 – 自動更新

目的：これは、アップデートを顧客に迅速かつ効率的に自動展開する機能です。Auto Updateは、ポータルのインターフェースを通じてパッケージをアップロードするか、またはhub.viettelcybersecurity.comのサイトから自動的にアップデートを取得することを可能にします。

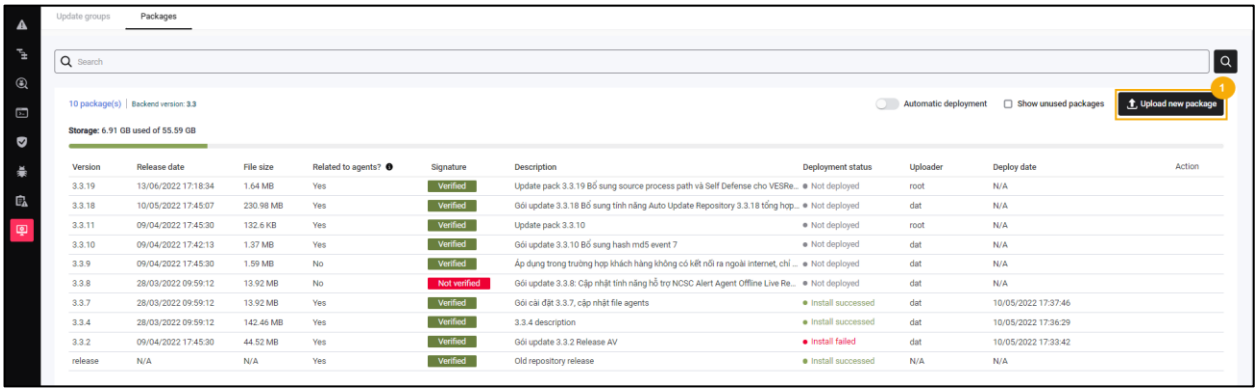
注意：展開チームは上記の情報をプロジェクトチームAjiantに再送し、システムに更新してもらい、顧客での自動パッケージ展開を許可してください。今後、新しいアップデートパッケージを展開する際は、展開チームまたは顧客側が提供されたアップデートパッケージを取得し、Ajiantポータルにアップロードしてパッケージを展開するだけで済みます。

- 提供されたアカウントでポータルにログインしてください。
- 「設定」を選択すると、システムは以下のサブメニューを表示します：ポリシー設定、エージェント管理、グループ管理、更新管理、ルール相関、アカウント管理。
- 「Update Management」を選択すると、システムにUpdate Groupの一覧が表示されます。

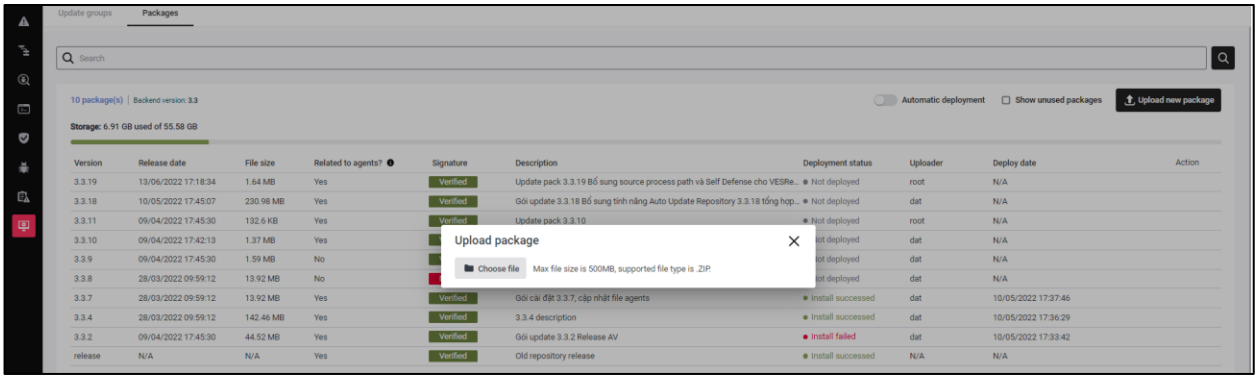
- 「パッケージ」タブを選択すると、システム内のパッケージ一覧が表示されます。



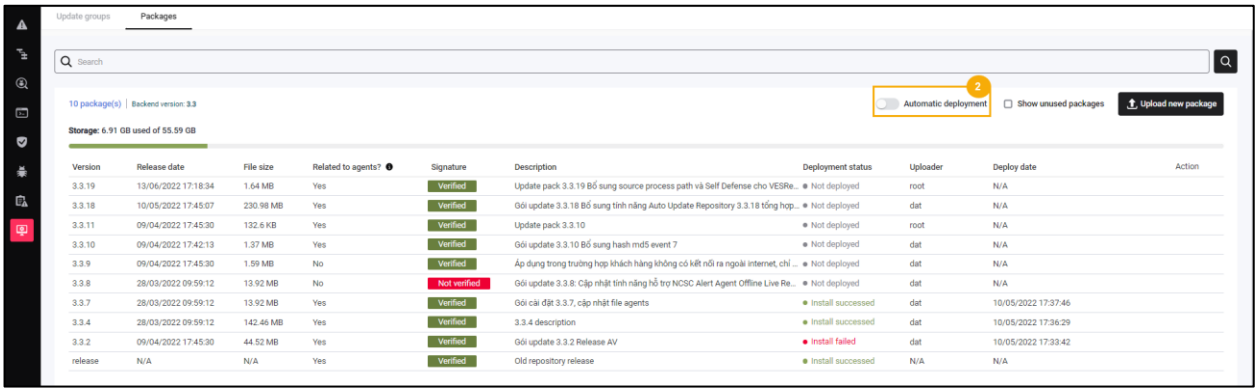
- 「新しいパッケージを更新」ボタンを選択すると、システムは「パッケージのアップロード」ポップアップを表示します。



- パッケージをアップロードしてください。

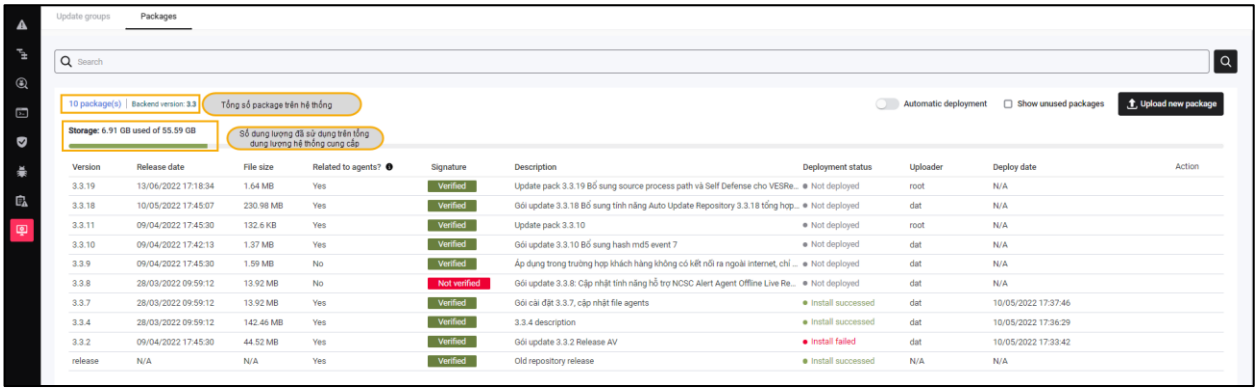


- 「自動開発」アクションのオン/オフを切り替えて、パッケージの更新を自動的に顧客に展開します。

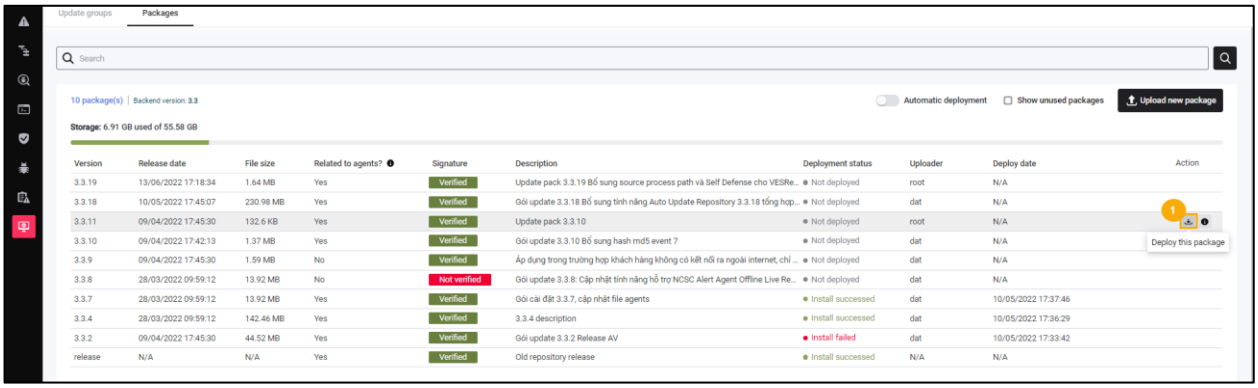


3 – パッケージを展開する

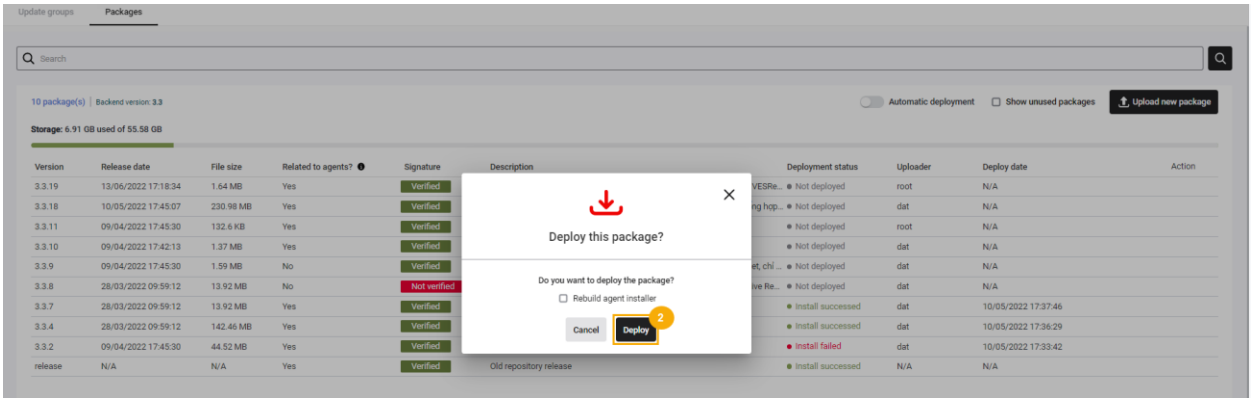
- 提供されたアカウントでポータルにログインしてください。
- 「設定」を選択すると、システムは以下のサブメニューを表示します：ポリシー設定、エージェント管理、グループ管理、アップデート管理、ルール相関、アカウント管理。
- 「Update Management」を選択すると、システムにUpdate Groupの一覧が表示されます。
- 「パッケージ」タブを選択すると、システム内のパッケージ一覧が表示されます。



- 該当のパッケージレコードで「このパッケージをデプロイ」アイコンを選択すると、システムはデプロイ確認のポップアップを表示します。



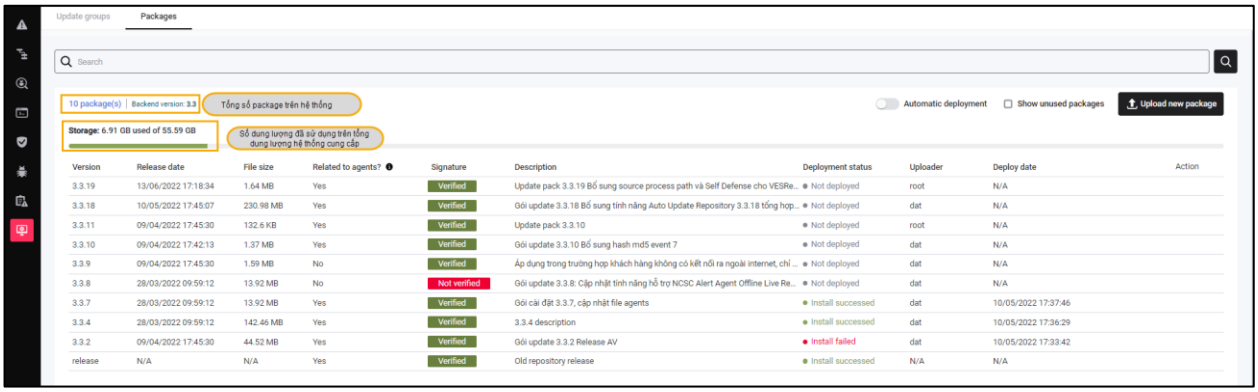
- 「Deploy」ボタンを選択してデバイスへのパッケージ展開を確認するか、「Cancel」ボタンを選択してパッケージ展開操作をキャンセルしてください。



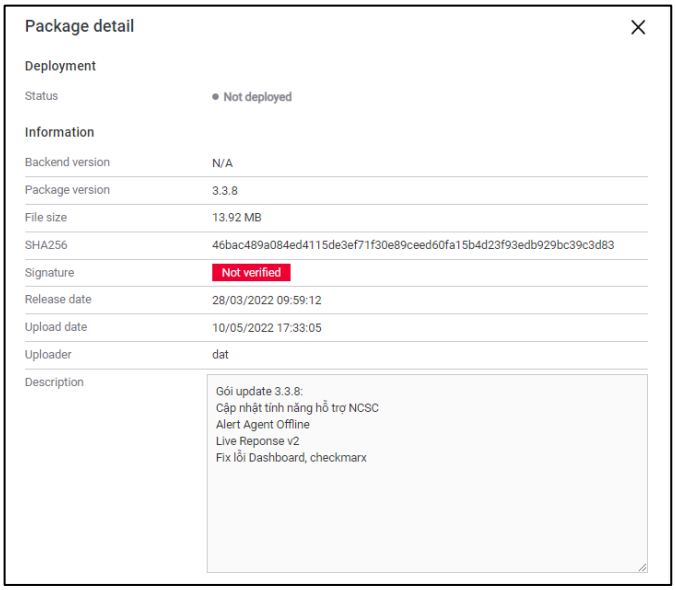
4 – パッケージの詳細

- 提供されたアカウントでポータルにログインしてください。
- 設定を選択すると、システムは以下のサブメニューを表示します：ポリシー設定、エージェント管理、グループ管理、アップデート管理、ルール相関、アカウント管理。
- 「Update Management」を選択すると、システムにUpdate Groupの一覧が表示されます。

- 「パッケージ」タブを選択すると、システムに登録されているパッケージの一覧が表示されます。



- 該当のパッケージレコードで「詳細表示」アイコンを選択すると、システムは選択したパッケージの詳細情報のポップアップを表示します。



3.7 BLSディスプレイ

3.7.1 違反統計

目的：違反統計機能は、管理者が設定されたエージェントの違反を統計することを支援します。内容は以下の通りです：

+ ベースライン違反のトップ項目およびベースライン違反のトップ組織；

+ 各部門ごとの違反リストおよび違反エージェントリストを確認する。

+ 各部門の違反リストおよび各部門内の違反内容リストを確認する。

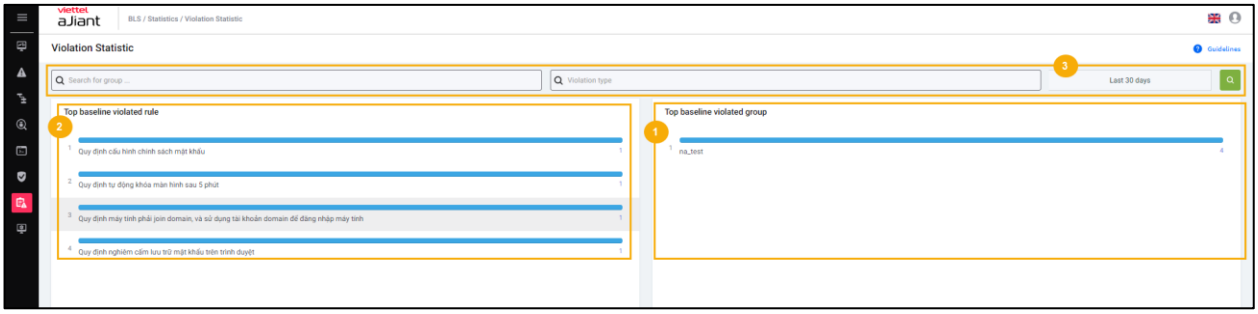
+ エージェントの詳細を見る;

+ 違反の輸出;

+ 違反報告;

「BLS」タブをクリック >> 違反統計;

違反統計画面



システムは以下の機能をサポートします：

+ ベースライン違反トップ10を違反件数の多い順に並べた統計データ

  - 各記録には、違反内容と違反した機器の台数が表示されます。

  - ベースライン違反トップの任意のレコードを選択すると、システムは選択された違反に対応する詳細画面に移動します。

+ ベースライン違反件数が多い上位10社の統計（降順で並べ替え）：

- 各記録には、違反事業所名と違反機器の台数が表示されます。
- ベースライン違反上位の任意のレコードを選択すると、システムは選択された単位の詳細画面に移動します。

+ 検索

- 個別検索：
- 単位別検索
  - 違反上位単位は、入力された単位と対応する子単位のリスト（ある場合）を表示します。
  - 主な違反事項：該当する場合、当該組織および子組織の違反事項を表示する。
- 違反の種類
  - 違反上位機関：選択された違反種類の違反機関リストを表示する。
  - 主な違反：選択された違反を表示する；
  - 違反期間;
- 複合検索: 2つ以上の検索条件を入力した場合、AND条件で検索が実行されます。

BLSのルールの説明

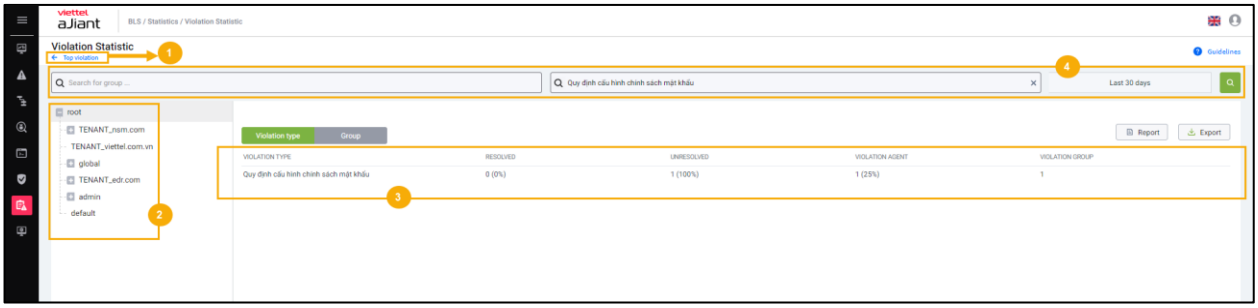
規則	詳細な説明

ファイル拡張子の表示設定	エンドポイント端末では、ファイルの拡張子を表示することが規定されています。
リモートデスクトップ設定の無効化規定	リモートデスクトップを許可しないように無効にする
5分後に自動で画面をロックする設定	5分以内に画面をロックしない違反
USBおよびCDドライブのAutorun機能を無効にする規定	USBやCDの自動再生機能のオン/オフを許可する。
19時を超えての勤務は禁止されています。	機械は19時間を超えて稼働しないこと。
コンピューターがUSB　3Gの使用規則に違反しました。	ワークステーションではMTP対応機器（スマートフォンなど）やUSB機器（ストレージ、3Gなど）の使用を禁止します。
インターネットへの直接接続の厳禁規定	ユーザーはブラウザを使用してネットワークにアクセスするか、システムプロキシを経由してアクセスすることができます。
オペレーティングシステムの更新構成規定	ワークステーションに自動OSパッチ更新モードを有効にするよう要求してください。

ソフトウェアのインストールおよび使用に関する規定	ワークステーションは、設定されたソフトウェアをインストールするかしないかのいずれかで、このルールに違反しています。
ウイルス対策ソフトのインストールおよび使用に関する必須規定	ワークステーションにはアンチウイルスソフトウェアをインストールし、リアルタイム保護機能を常に有効にし、更新設定を適切に構成することが求められます。
ファイアウォール回避ソフトウェアの使用義務規定	ワークステーションは、オペレーティングシステムまたはアンチウイルスソフトウェアでファイアウォールを有効にする必要があります。
カスペルスキーウイルス対策ソフトのインストールおよび使用規定	ワークステーションには必ずKasperskyのアンチウイルスソフトをインストールすること。
コンピュータはドメインに参加し、ドメインアカウントを使用してログインすることが規定されています。	コンピュータはドメインに参加し、ドメインアカウントを使用してログインすることが規定されています。
ローカルアカウントの回収規定	違反時にローカルアカウントを自動的に削除する

ブラウザにパスワードを保存することを厳禁とする規定	ブラウザにパスワードを保存することを厳禁します。
パスワードポリシー設定規定	規定には以下のルールが含まれます： + 必要な文字数を満たすこと + 設定された期間後にパスワードを変更すること + 複数回の誤入力によりアカウントがロックされること

違反の種類タブ



システムは以下の機能をサポートします：

+ トップ違反リンクを選択：ダッシュボード画面に移動し、トップ違反リストおよびトップ違反組織リストを表示する。

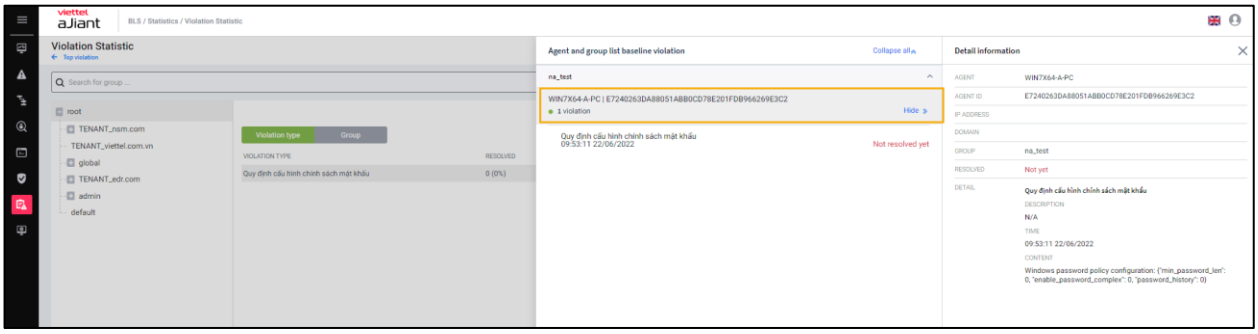
+ システムの単位データツリー

- システム内のすべての単位を親子階層で表示する。
- 違反フィルタリングを実行するために、データツリー上の単位を選択できます。

+ 違反種類タブ：

- 各違反種類には、以下の共通情報が表示されます：違反種類、解決済み、未解決、違反コンピュータ、違反ユニット。
- 違反種類のレコードをリストから選択してください：各違反単位ごとのコンピュータリストを表示します。
- コンピュータの選択：コンピュータの詳細情報と該当する違反リストを表示する。

ポップアップのコンピューター一覧からコンピューターを選択すると、Computer、AgentID、IPアドレス、ドメイン、グループ、解決状況、詳細（そのコンピューターのすべての違反種類を含む）を表示する詳細情報のポップアップが表示されます。



検索

+ 個別検索：

  - 単位別検索：入力された単位と対応する子単位の一覧を表示する
  - 違反の種類：選択された違反を表示する
  - 違反期間

+ 複合検索：2つ以上の検索条件を入力した場合、AND条件で検索が実行されます。

単位タブ

システムは以下の機能をサポートします：

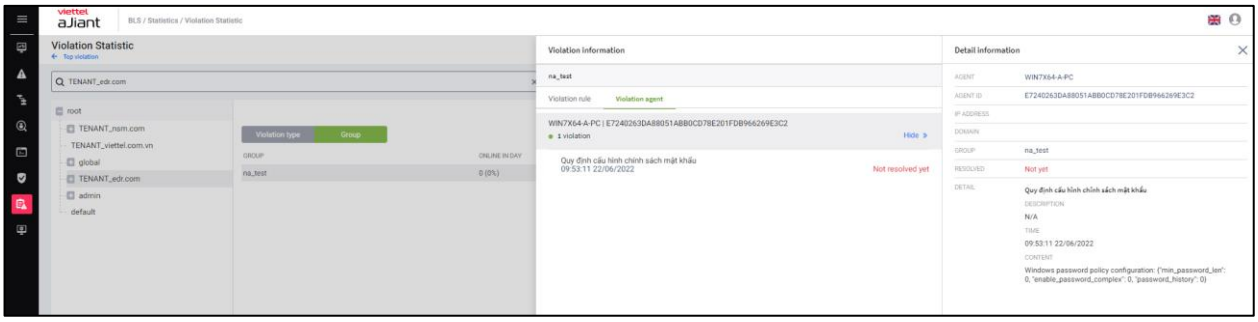
+ トップユニットリンクを選択：ダッシュボード画面に移動し、違反トップリストおよび違反トップユニットの一覧を表示します。

+ システムの単位データツリー;

  - システム内のすべての単位を親子階層で表示する。
  - データツリー上の単位を選択して、親子単位のフィルタリングを実行できます。

+ 単位タブ;

  - 各違反種類には、以下の共通情報が表示されます：ユニット、当日のオンライン数、直近30日間のオンライン数、解決済み、未解決、違反コンピュータ、違反ルール。
  - 違反コンピュータ列の詳細アイコンを選択すると、各違反ユニット内のコンピュータ一覧が表示されます。表示内容は、ユニット名、コンピュータ名｜エージェントID、各コンピュータの違反リスト、違反日時、違反状態（修正済みか未修正か）です。



ポップアップのコンピューター一覧からコンピューターを選択すると、Computer、AgentID、IPアドレス、ドメイン、グループ、解決状況、詳細（そのコンピューターのすべての違反種類を含む）を表示する詳細情報のポップアップが表示されます。

リストの違反ルール列の詳細アイコンを選択してください：該当ユニットの違反リストを表示します。

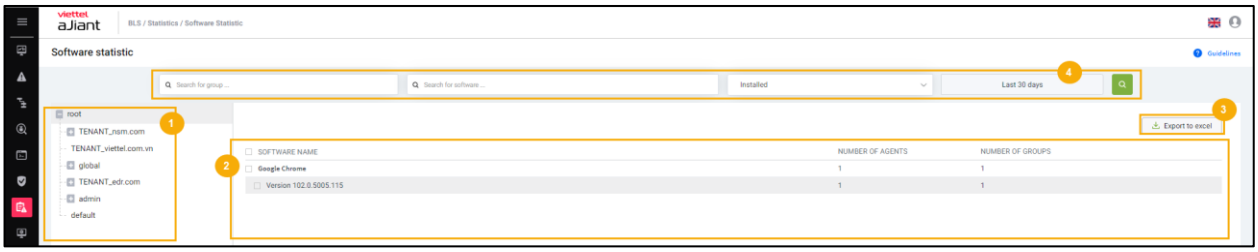
検索

+ 個別検索：
  - 単位別検索：入力された単位と対応する子単位の一覧を表示する；
  - 違反の種類：選択された違反を表示する；
  - 違反期間;
+ 複合検索：2つ以上の検索条件を入力した場合、AND条件で検索が実行されます。

3.7.2 *ソフトウェア統計*

目的：ソフトウェア統計機能は、管理者が組織内にインストールされたソフトウェアを統計的に把握することを支援します。内容は以下の通りです：

+ 選択した単位にインストールされているソフトウェアの一覧を表示する。
+ エージェントの詳細を見る;
+ ソフトウェアのエクスポート;

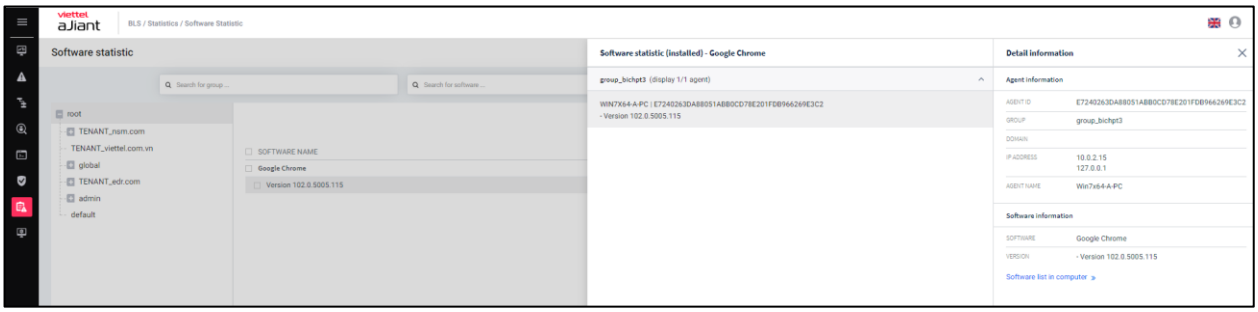


システムは以下の機能をサポートします：

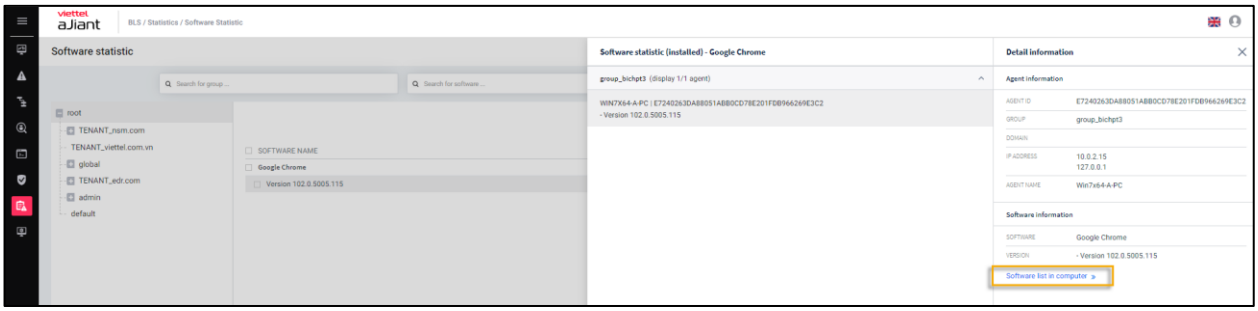
+ システムの単位データツリー
+ システム内のすべてのユニットを親子階層で表示する
+ データツリー上の単位を選択して、ソフトウェアのフィルタリングを実行できます。
+ ソフトウェア一覧
    - 各ソフトウェアには、以下の共通情報が表示されます：ソフトウェア名、コンピュータの台数、ユニット数。

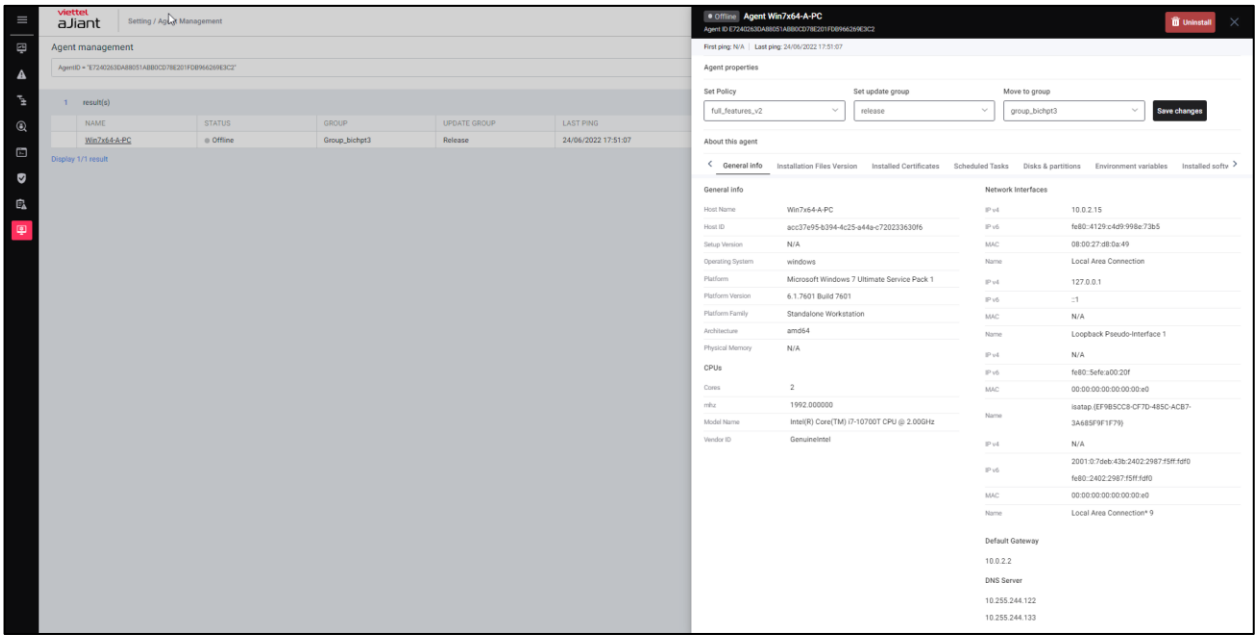
- 違反コンピューター列の詳細アイコンを選択します：各部門のコンピューター一覧を表示し、部門名、コンピューター名｜エージェントID、バージョンを含みます。

- ポップアップのコンピューター一覧からコンピューターを選択すると、Computer、AgentID、IPアドレス、ドメイン、グループ、ソフトウェア情報（ソフトウェア名、バージョン）を含む詳細情報のポップアップが表示されます。



- [コンピュータのソフトウェア一覧]リンクを選択すると、システムはエージェント管理画面に移動し、選択したコンピュータの詳細ポップアップが表示されます。





検索

+ 個別検索：

- 単位別検索：単位内にインストールされているソフトウェアを表示する
- ソフトウェア名：入力されたソフトウェアの一覧を表示する
- 状態で検索：インストール済み、未インストール
- インストール時間

+ 複合検索：2つ以上の検索条件を入力した場合、AND条件で検索を実行します

。

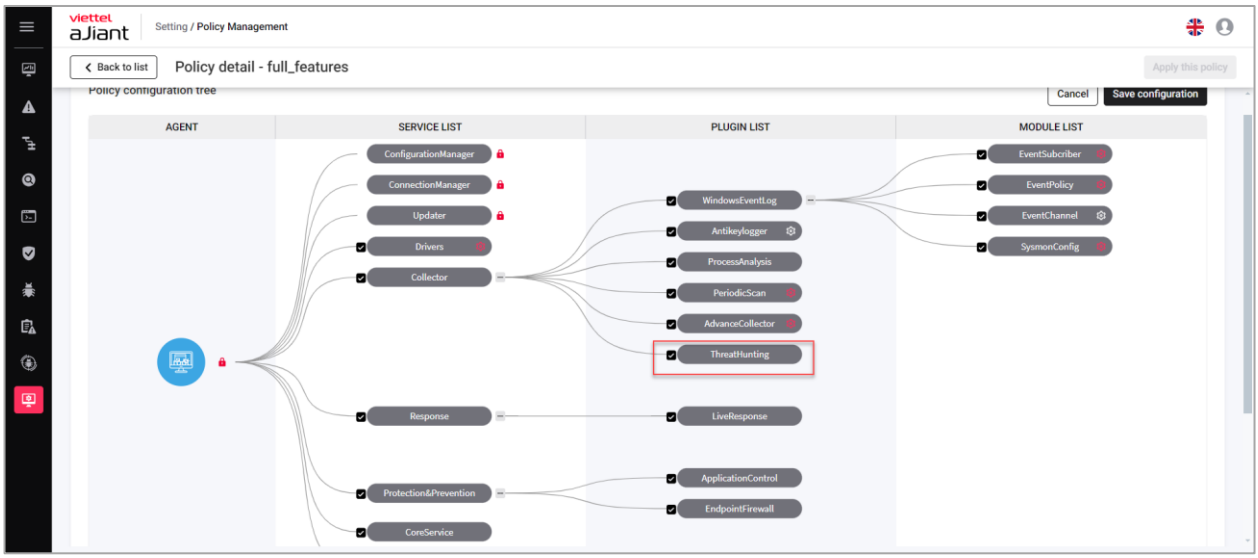
エクスポートを選択してください。システムは画面に表示されているデータと同じ内容のエクスポートファイルをダウンロードします。

3.8 脅威ハンティング

Threat Hunting機能は、ユーザーが組織内の各端末における攻撃の疑わしい兆候やIOC（侵害の痕跡）を検索できるようにし、早期の対応および処理策を講じることを可能にします。この機能は、以下の支援を行います。

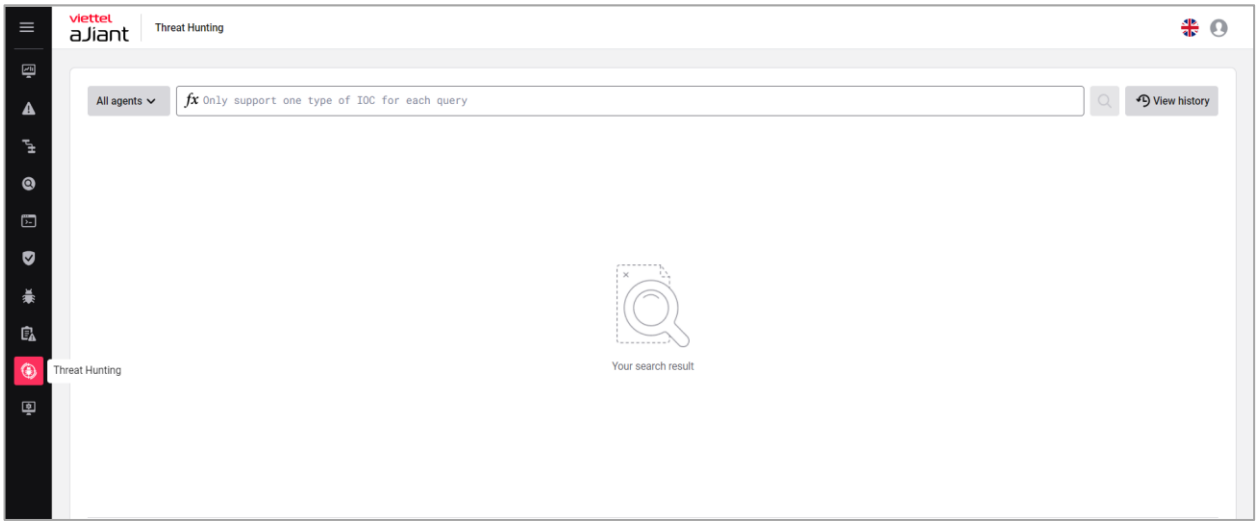
3.8.1 ポリシーのオン/オフ切り替え

- Threat Hunting機能を使用するには、Policy Managementでポリシーを有効にし、サービスコレクターを選択し、ThreatHuntingプラグインを選択する必要があります。
- 注意：エージェントはThreatHuntingを有効にするポリシーを適用する必要があり、そうしないとIOCの検索を実行できません。

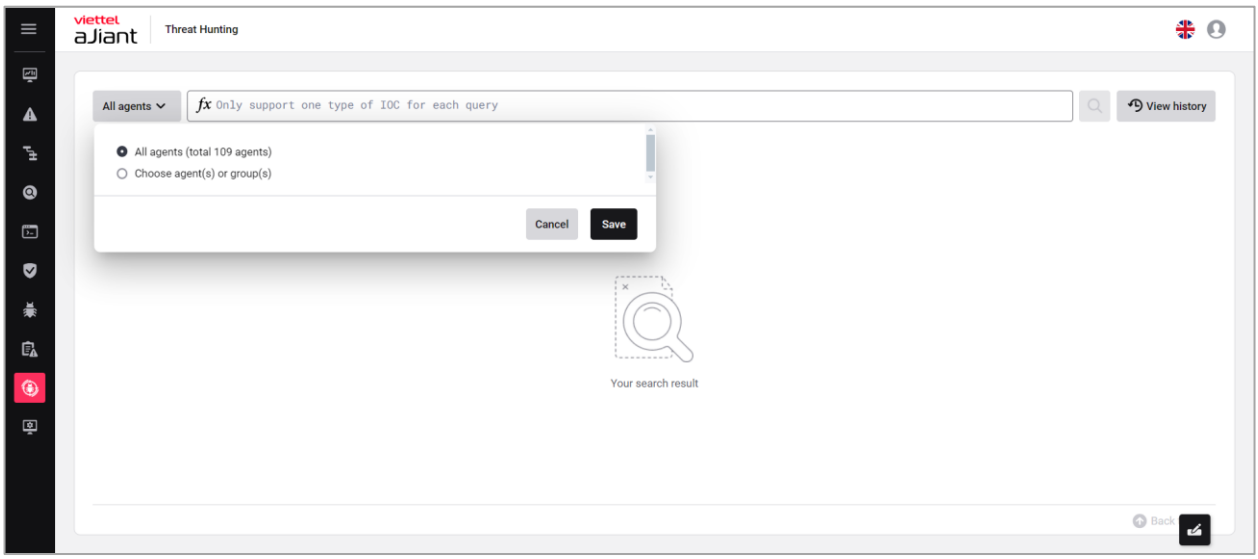


3.8.2 エージェント／グループ別検索

- メニューから「スレットハンティング」を選択してください。



- 管理者がエージェントやグループ別にIOCを検索できるようにする。
  - すべてのエージェント（All agents）での検索を許可する
  - 特定のエージェントごとに検索するか、グループ単位で選択することを許可する。



3.8.3 IOCの検索

サポートされているIOCの種類

- ユーザーは以下の表に示された各種IOCに基づいて検索することができます。

IOC（インジケーター・オブ・コンプロマイズ）	タブ	検索フィールド	サポート演算子	ノート
ファイルパス	ファイル	ファイルパス	＝、～	ファイルパスによる検索
ファイル名	ファイル	ファイル名	=,~	ファイル名で検索する
ファイルハッシュSHA256	ファイル	ファイルSHA256	=	SHA256ハッシュファイルの検索
レジストリパス	レジストリ	レジストリパス	=,~	レジストリパスによる検索
レジストリキー	レジストリ	レジストリキー	=、～	レジストリキーによる検索
レジストリデータ	レジストリ	レジストリデータ文字列	～	レジストリデータの文字列型、DWORD型、バイナリ型で検索する
		レジストリデータ_DWORD	=	

		レジストリデータバイナリ	=,~	
文字列メモリ	メモリ	文字列メモリ	～	文字列メモリによる検索を許可する
ヘックスメモリ	メモリ	ヘックスメモリ	～	16進数形式での検索を許可する
ユーザー名	ユーザー	ユーザー名	=,~	エンドポイント端末でユーザーによる検索を許可する。
ドメイン	ネットワーク	ドメイン	=,~	エンドポイントがこれまでにアクセスしたドメインでの検索を許可する。
IP（アイピー）	ネットワーク	ドメイン	=,~	エンドポイントがこれまでにアクセスしたIPアドレスによる検索を許可する。
プロセスパス	プロセス	プロセスパス	=,~	プロセスのパスによる検索を許可する

コマンドラインを処理する	プロセス	コマンドラインを処理する	=、～	プロセスのコマンドラインによる検索を許可する
DLL（ダイナミックリンクライブラリ）	DLL（ダイナミックリンクライブラリ）	Dll_path（ディーエルエルパス）	=、～	DLLのパスによる検索を許可する

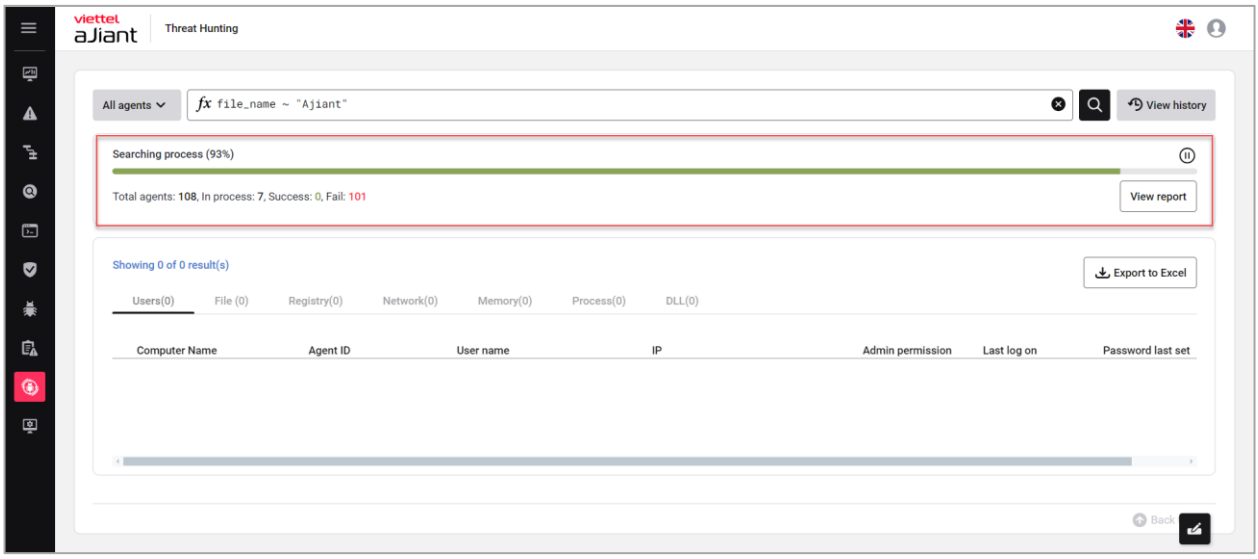
注意：

- ユーザーは同じクエリ内で一種類のIOCのみ検索することが許可されています。
- AND、OR条件による検索を許可する
- 検索値は大文字と小文字を区別しません。
- ユーザーが検索を実行した後、システムはクエリの要件に従ってエンドポイント上でスキャンを行い、結果をポータルに送信します。
- 検索時間は、クエリの複雑さと検索を実行するエージェントの数に依存します。

検索結果の詳細

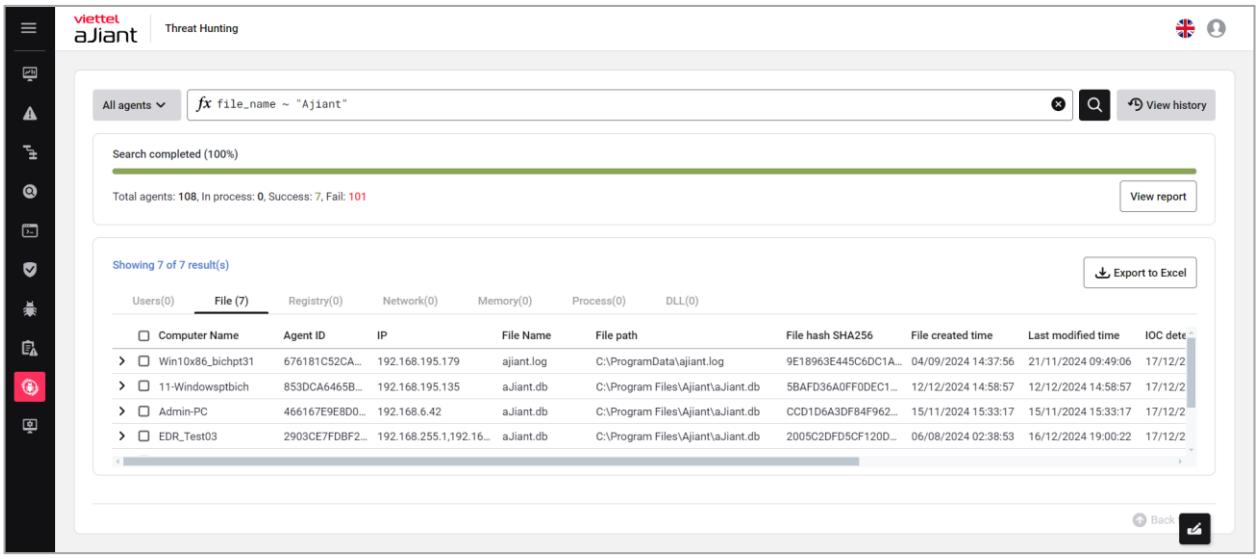
検索状況の追跡

- ユーザーが検索の進行状況を追跡できるようにする。
    - 総エージェント数：検索を実行したエージェントの総数
    - 処理中：検索を実行中です
    - 成功：検索に成功しました
    - 失敗：検索に失敗しました



検索結果の詳細

- ユーザーが各タブごとに検索結果の詳細を閲覧できるようにする。
    - ユーザー
    - ファイル
    - レジストリ
    - ネットワーク
    - メモリ
    - プロセス
    - DLL（ダイナミックリンクライブラリ）
- 結果は、ユーザーのクエリに従って各タブごとに正しく表示されます。

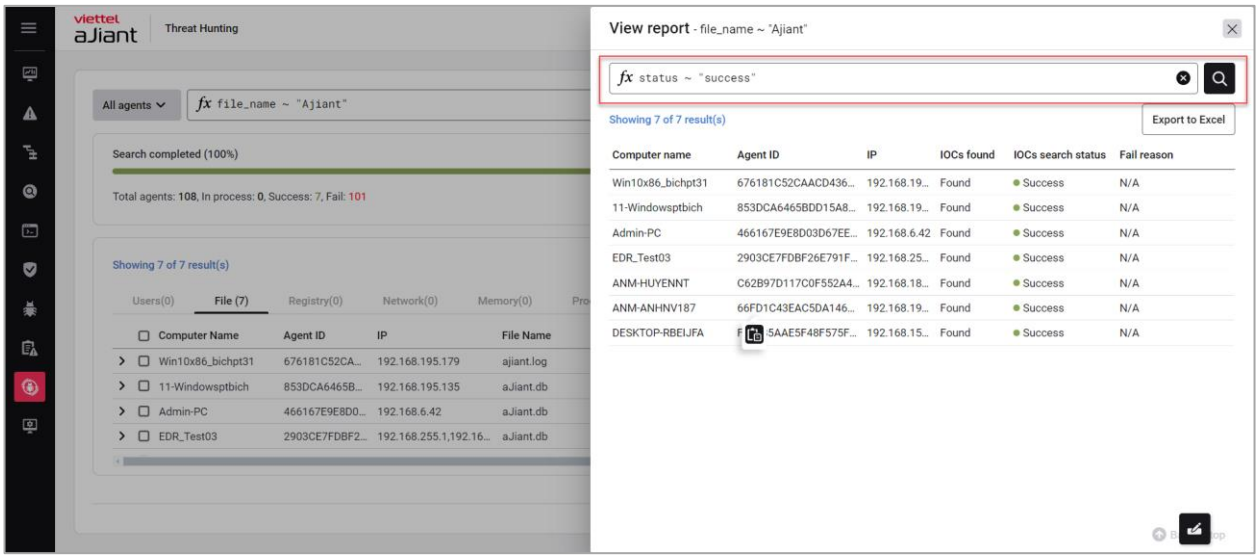


検索を停止する

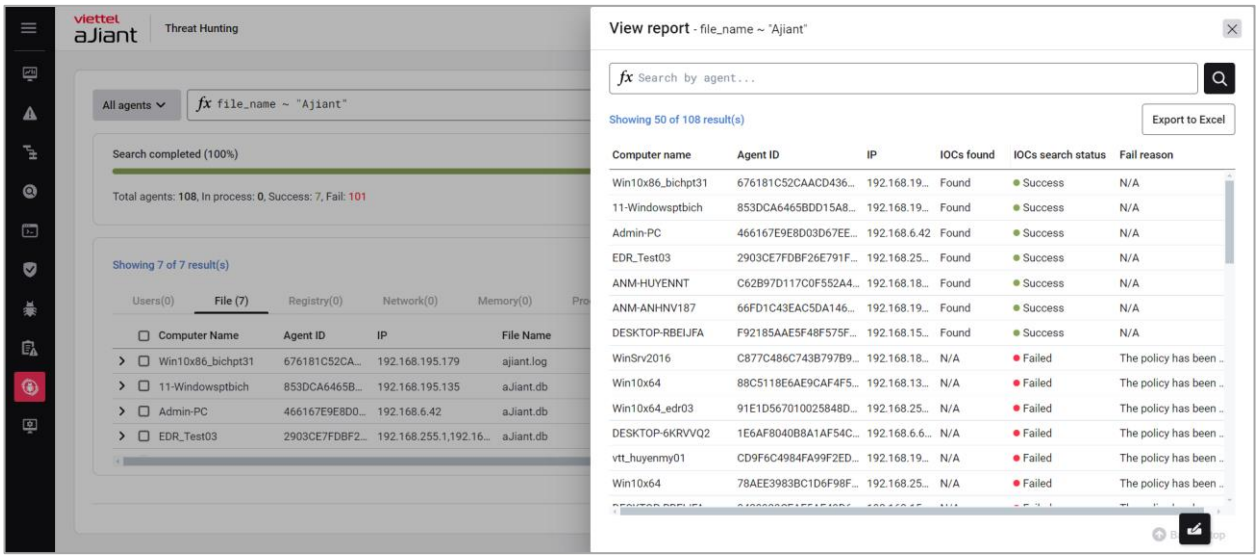
- ユーザーが検索を停止できるようにする：検索プロセスバーで「一時停止」ボタンを選択してください。
- 検索を停止した後：
    - システムは検索を停止します。
    - クエリの継続検索はサポートされていません。

エージェント下でのIOC検索レポートの詳細を見る（レポートを見る）

- ユーザーがコンピュータ名、エージェントID、IPアドレス、IOC検索ステータスで検索できるようにする。

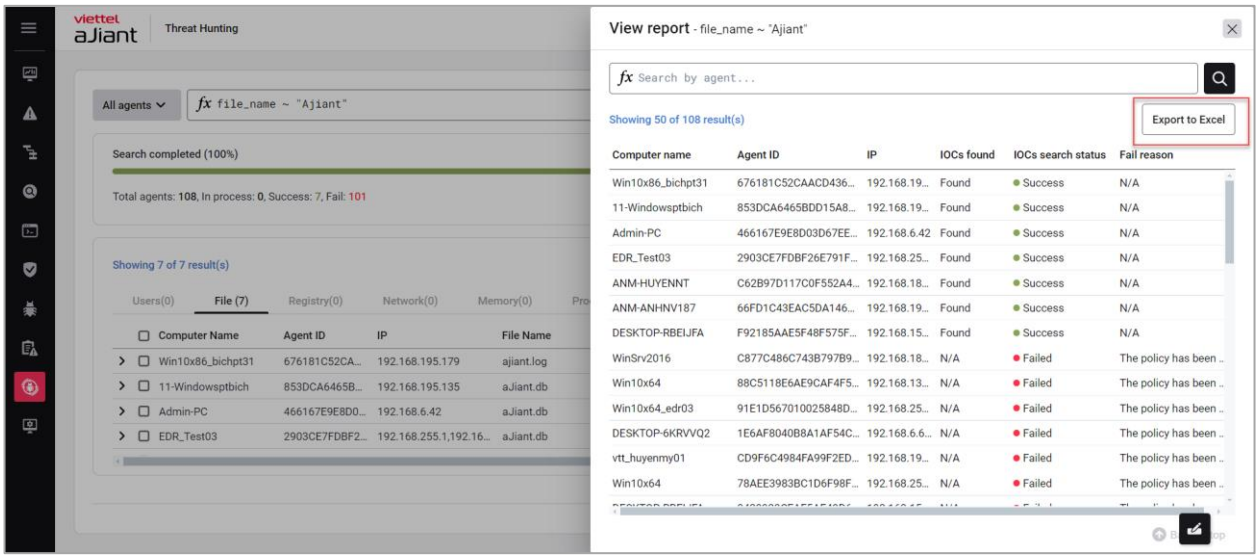


- このレポートは、各エージェントにおけるIOC検索の状況をユーザーに詳細に提供します。レポートに含まれる情報は以下の通りです。
    - コンピューター名
    - エージェントID
    - IP（アイピー）
    - 発見されたIOC：ユーザーのクエリに基づいてIOCの兆候が見つかったかどうか
    - IOCs検索状況：エージェント上のIOCs検索状態
    - 失敗理由：検索失敗の詳細理由



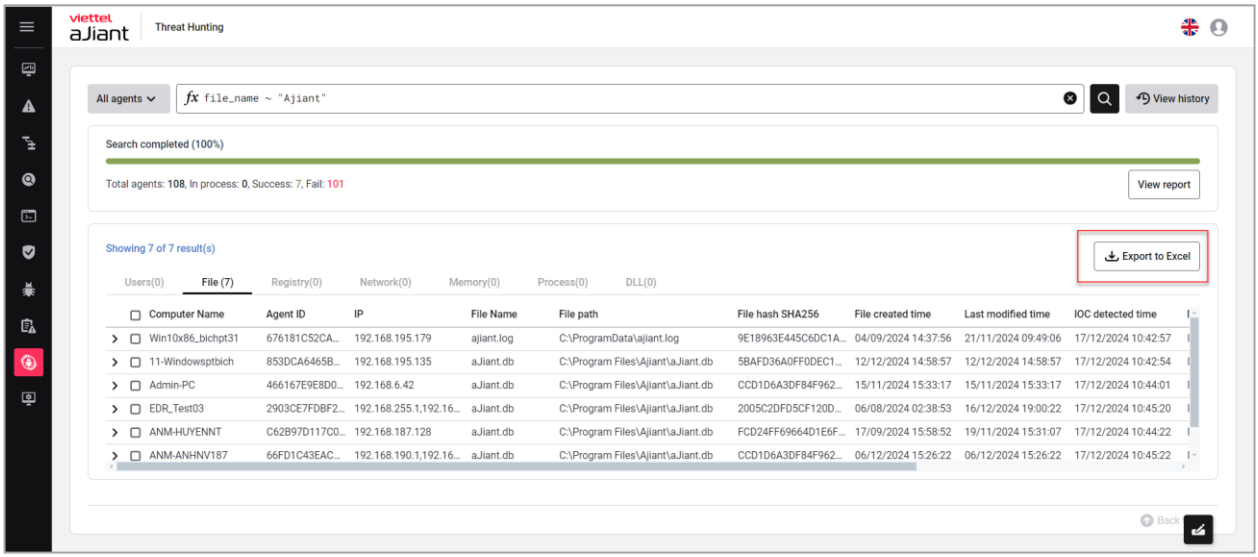
エクセルにエクスポートする

- ユーザーがエージェント配下の検索結果をまとめたExcelファイルをダウンロードできるようにする。
- ファイルに含まれる情報は以下の通りです。
    - コンピューター名
    - エージェントID
    - IP（アイピー）
    - 検出されたIOC: ユーザーのクエリに基づいてIOCの兆候が見つかったかどうか
    - IOCs検索状況：エージェント上のIOCs検索状態
    - 失敗理由：検索失敗の詳細理由



検索結果をダウンロードする

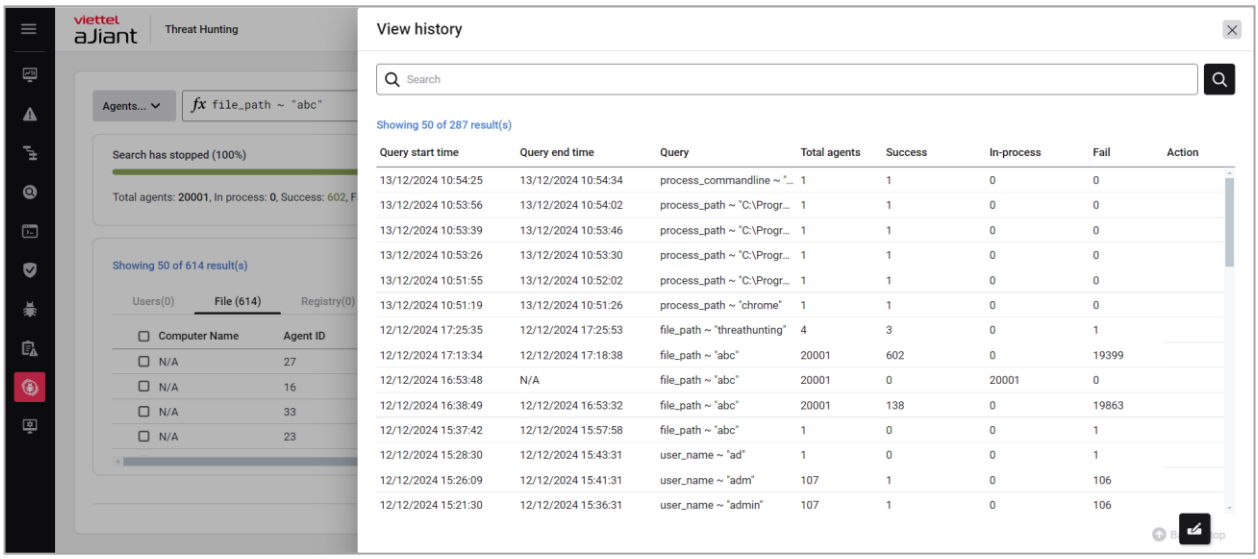
- ユーザーがエージェント端末上で検索結果のIOCをダウンロードできるようにする。
- エクセルファイルのダウンロードをサポートします。



3.8.4 クエリ履歴を見る

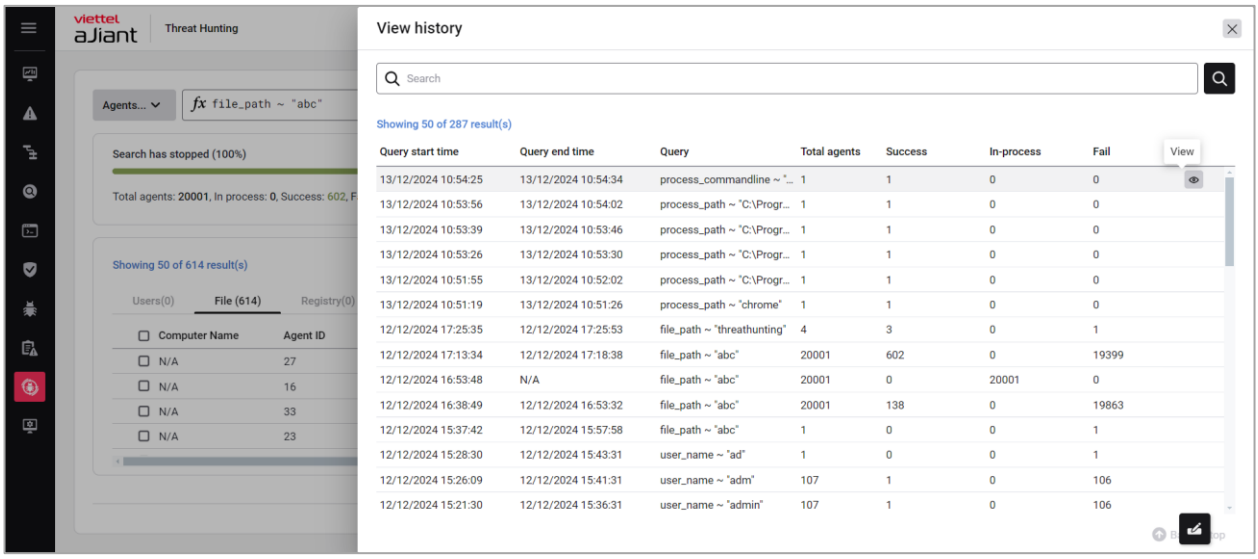
クエリ一覧を見る

- ユーザーがクエリ履歴を閲覧できるようにします。クエリ履歴の情報には以下の内容が含まれます：
    - クエリ開始時間：クエリ実行開始時刻
    - 検索終了時間
    - クエリ：ユーザーの問い合わせ内容
    - エージェント総数：検索されたエージェントの総数
    - 成功：エンドポイントでの検索に成功しました
    - 処理中：エンドポイント上で検索中です。
    - 失敗：検索に失敗しました

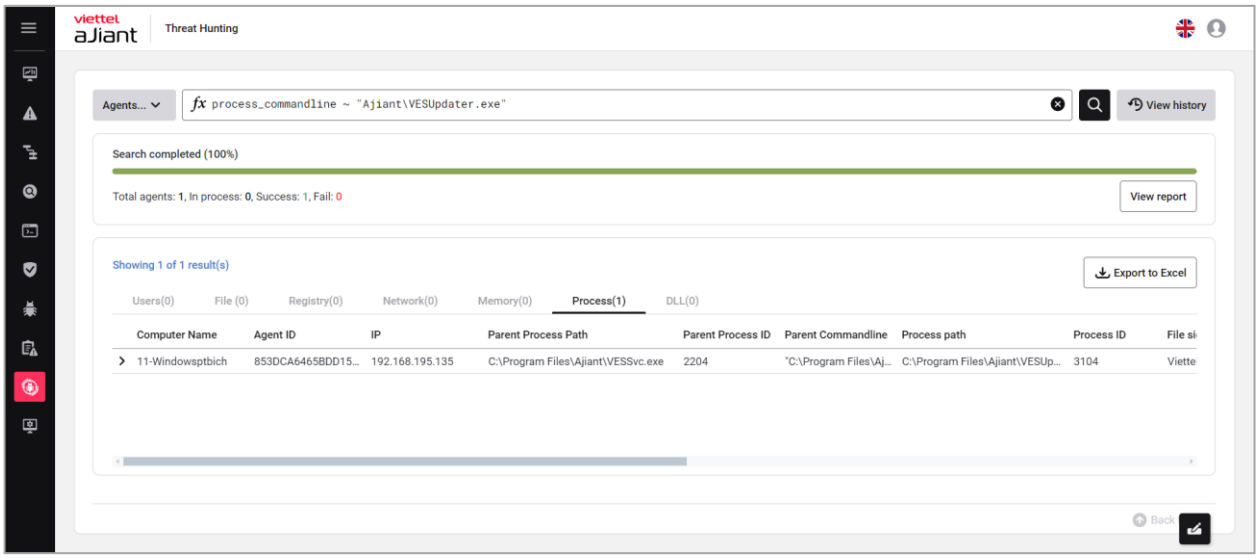


クエリ履歴の詳細を見る

- ユーザーが各クエリの結果を詳細に確認できるようにする：アクション -> 「表示」を選択してください。



- 履歴内のクエリ結果の詳細を表示することを許可する：



3.9 規則の相関関係

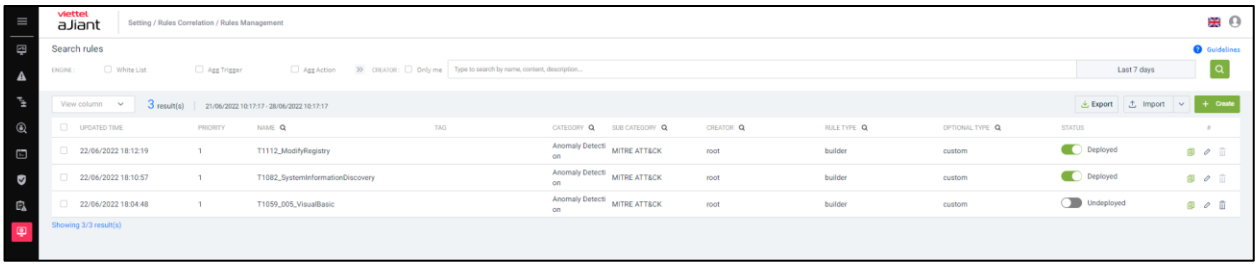
3.9.1 表示リスト

目的：この機能は、ユーザーがシステム内のルール相関リストを閲覧できるようにします。検索条件を入力または選択して、システム内のルールを検索し、ルールに対して迅速にデプロイ、アンデプロイ、削除の操作を行うことができます。

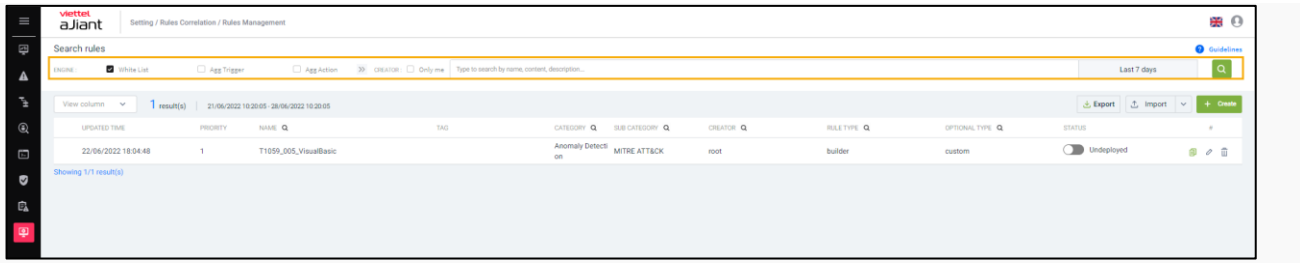
+ ;フィルターセット

+ フィルター（FITTER）には以下が含まれます：

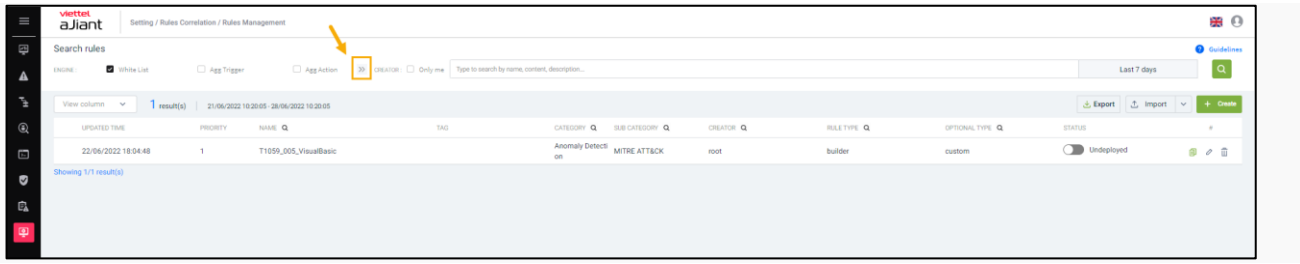
- 6 エンジン：ホワイトリスト、アグレッシブトリガー、アグレッシブアクション、フィルター、インジケーター、誤検知
- テキストボックス検索は、以下の項目で行います：名前、内容、説明。
- 更新時間；
- 私によって作成されました。
- ;エンジンでフィルタリングする;



- 1つまたは複数のデフォルトエンジンを選択してください。

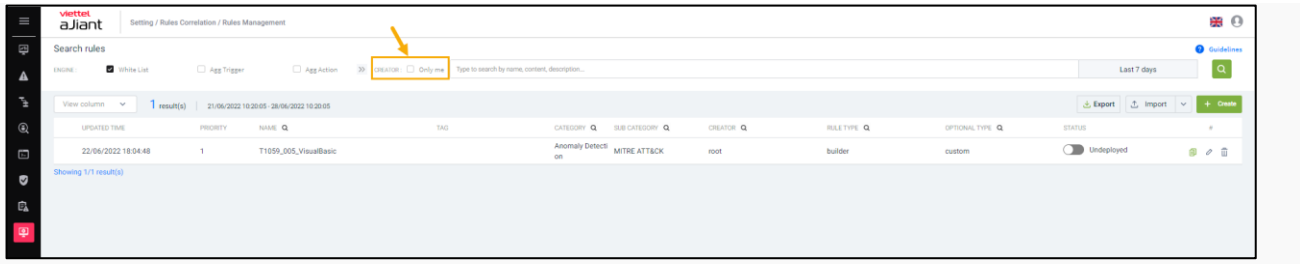


- フィルタリングするエンジンを追加するには、「拡張」を選択してください。

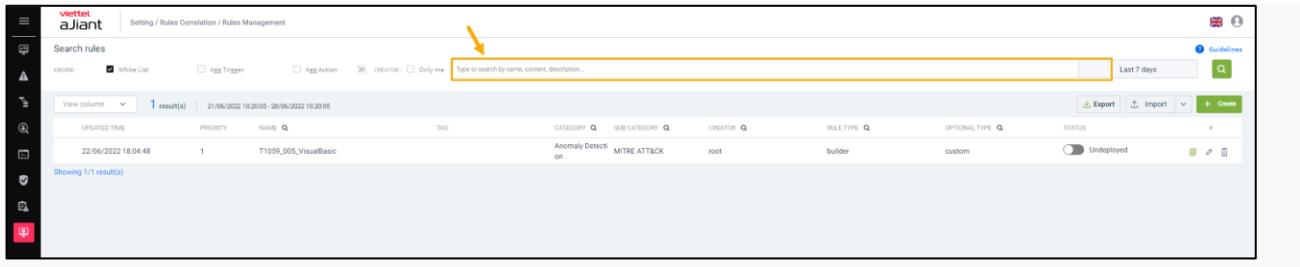


2つ以上のエンジンを選択した場合、画面はAND条件でフィルタリングされた結果を返します。

- ルール作成者として現在システムにログインしているユーザーを選択する。



- 検索したい名前、内容、説明をテキストボックスに入力してください。



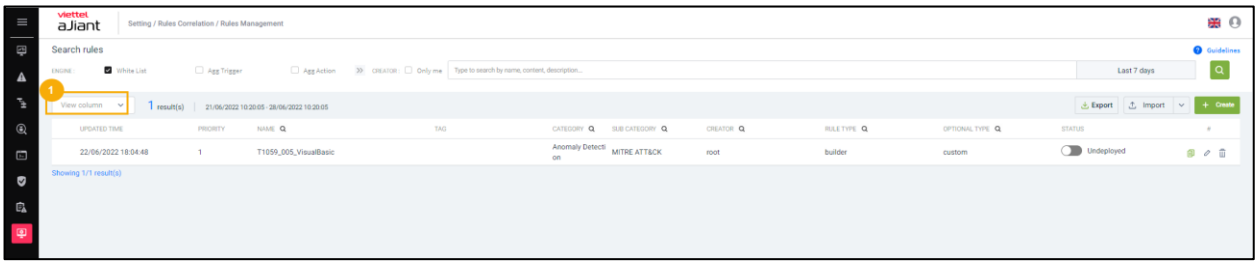
- 検索する情報を入力してください。
- 検索ボタンを押して、検索結果を表示してください。

列を選択してください

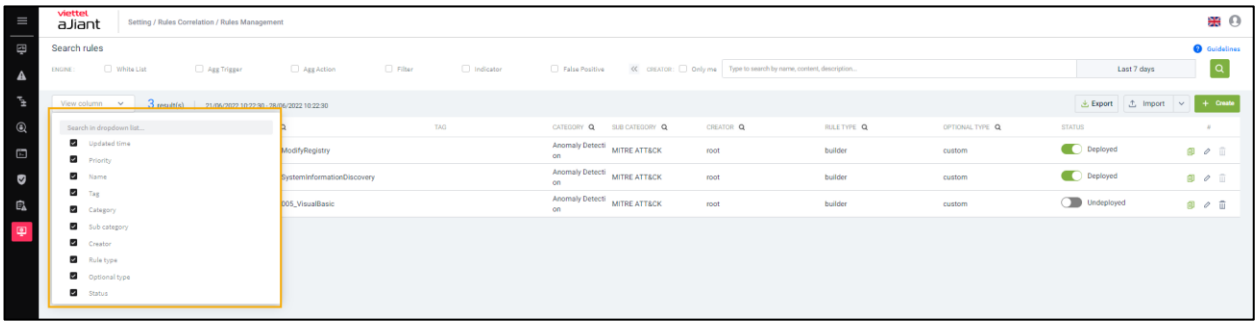
ユーザーが相関画面に表示する列を選択できるようにします。

実施手順：

- 「View column」のコンボボックスをクリックします。画面にチェックボックス形式の列選択リストが表示されます。

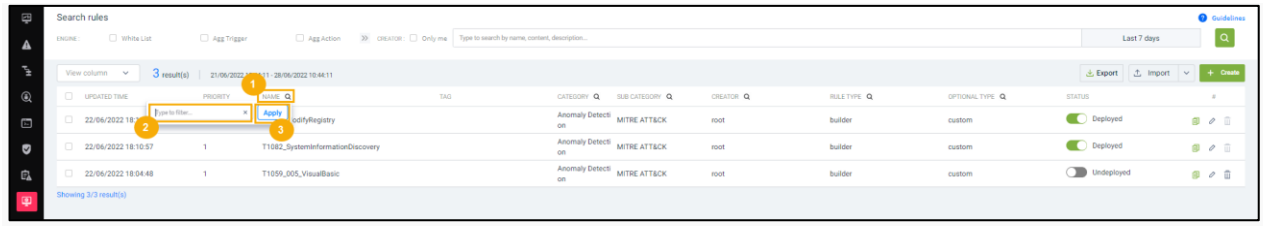


- 表示したい列名を選択してください。



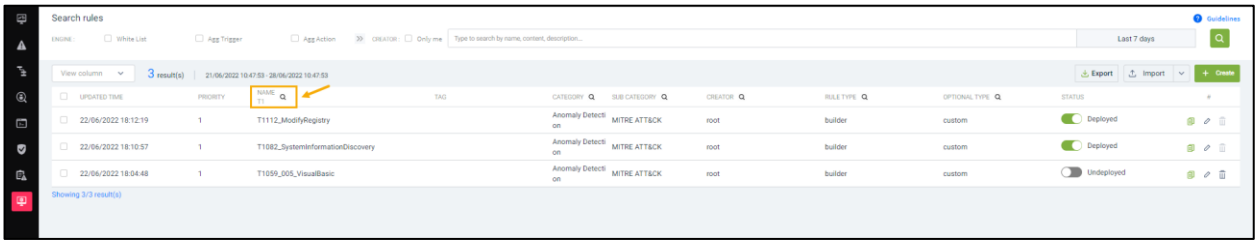
1 – 高速検索サポート

- ルール名で検索する
- アイコンをクリックして検索バーを表示します。



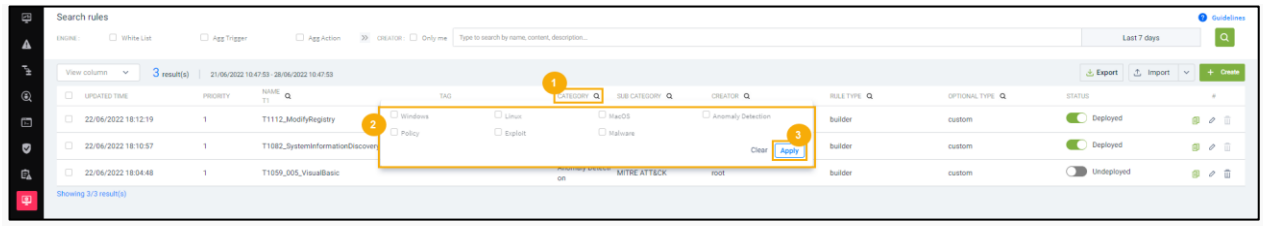
- 検索したいルール名を入力してください。

- 検索結果を表示するには、Enterキーを押してください。



カテゴリー別検索：検索支援は、Windows、Linux、MacOSの3つのデフォルトタイプで構成されています。

- アイコンをクリックして、カテゴリの一覧を表示します。



- 検索したいカテゴリーを選択してください。

- 「適用」をクリックしてください。

サブカテゴリー検索：展開タイプ別の迅速な検索支援で、デフォルトの3種類は以下の通りです：Metre ATT&CK、マルウェア、疑わしい行動。

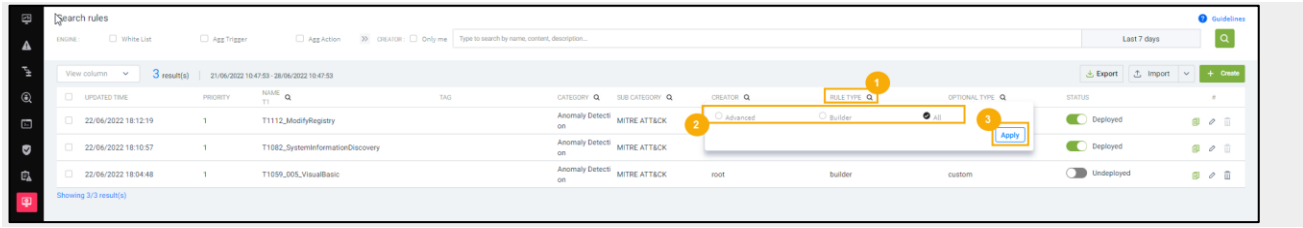
- アイコンをクリックして検索バーを表示します。

- 検索したいサブカテゴリーを選択してください。
- 「適用」をクリックしてください。

クリエイターを探す

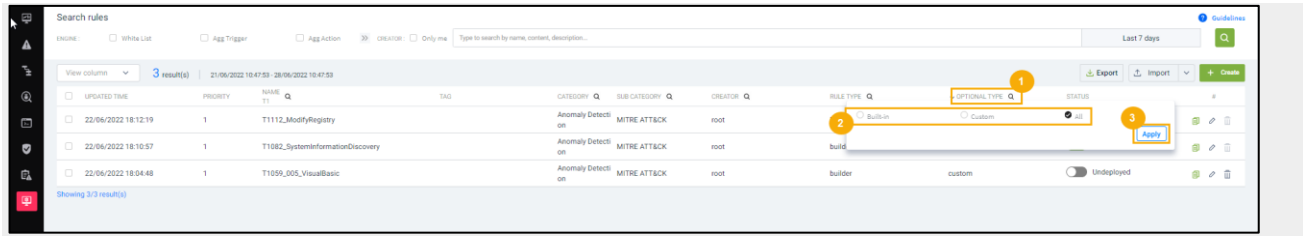
- アイコンをクリックして検索バーを表示します。
- 検索したい作成者名を入力してください。
- 「適用」をクリックしてください。

検索ルールタイプ：高速検索をサポートする3つのデフォルトタイプは、Advanced、Builder、Allです。



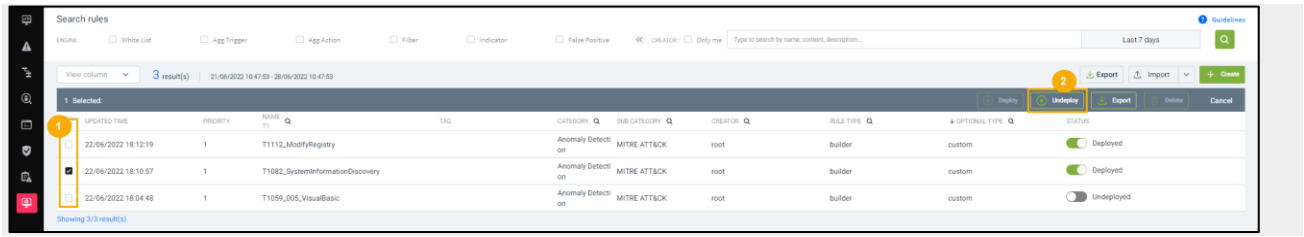
- アイコンをクリックして、ルールタイプのリストを表示します。
- 「検索したい『ルールタイプ』をクリックしてください。」
- 「適用」をクリックしてください。

Optionalタイプの検索：組み込み（Built-in）、カスタム（Custom）、すべて（All）の3つのデフォルトタイプによる高速検索をサポートします。

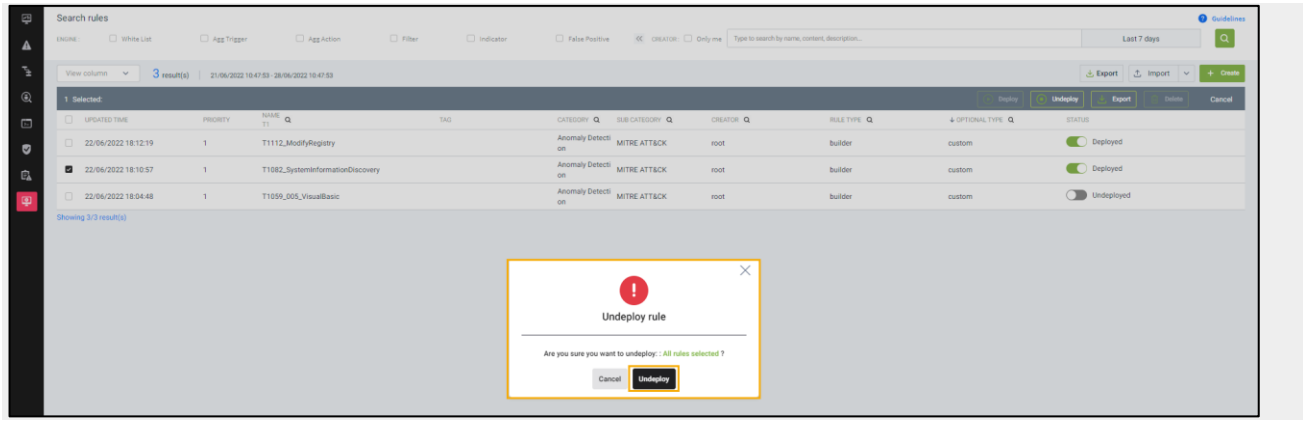


- アイコンをクリックして、オプションタイプの一覧を表示します。
- 「オプション」タイプをクリックして検索したい;
- 「適用」をクリックしてください。

複数のルールのデプロイおよびアンデプロイをサポートする



- 同じ状態の「Deploy」または「Undeploy」である複数のチェックボックスをクリックしてください。
- 「デプロイ/アンデプロイ」ボタンをクリックしてください。
- 表示されたポップアップで「デプロイ/アンデプロイ」を選択して、デプロイまたはアンデプロイを実行します。



3.9.2 ルール相関の新規追加

目的：ユーザーが新しい相関ルールを完全に設定できる機能。

概要

+ エンジン：以下の詳細情報を持つ6つのエンジンで構成されています。

- ホワイトリストは、システムが処理する必要のないイベントを迅速に除外するステートレスエンジンです。ホワイトリストのルールに一致するイベントは処理フローから除外されます。

- Agg_triggerとAgg_actionは、類似したイベントをグループ化するステートフルエンジンです。各集約ルールには、グループ化の条件（類似イベントの定義）やグループ化の時間間隔（例：30秒、1分、2分など）が含まれています。グループ化条件に一致するイベントは保存され、一定時間後に数量を付けた1つのイベントとして返されます。グループ化条件に一致しないイベントは、数量1として即座に返されます。

- フィルターは、条件をフィルタリングしてインジケーターに送るステートレスエンジンです。

- インジケーターは、フィルターを満たすイベントに対して検査および統計処理を行うステートフルエンジンです。インジケーターの入力はフィルターを満たすイベントであり、出力はインジケーターイベントまたはアラートイベントです。インジケーターは、同一対象に対する一定時間内（タイムウィンドウ）の件数（カウント）統計をサポートし、あらかじめ定められた期間内に同一対象に対してアラートが繰り返されることを防止します。各ルールインジケーターは、同種の条件を同一システム上でのみ評価します。

- FalsePositiveエンジンはステートレスエンジンであり、誤検知されたアラートを除外します。各アラートはFalsePositiveルールに一致するとドロップされます。

+ Debug/Not Debugはエンジンの二つの状態です。デバッグ操作を行うと、エンジンの条件を満たすログがデバッグ画面のCorrelationに表示されます。

+ 条件：各エンジンは、イベント、非イベント、アラートイベント、非アラートイベント、蓄積、関数、非関数など、異なる条件をサポートします。条件の詳細および使用方法については以下をご参照ください。

- イベント：イベントフィールドに使用されます；
- Not Event: イベントがある場合にのみ作成されます。
- アラート：アラートフィールドに使用されます。
- アラートなし：アラートイベントがどのくらいの期間発生していないかを確認する。
- 蓄積：イベントの条件を一定数満たすものをグループ化し、アラートを生成する。

- 関数：関数とは機能のことです。注意：ブール関数の場合、返り値はtrueまたはfalseです。

- Not Function: Not functionでは、使用される関数はfunctionと同じです。しかし、返される値はtrue/falseが逆になります。

+ 演算子：

- 基本的な演算子には、=、!=、>、<、>=、<= があります。

- 入力：フィールドの値がリスト内にあるかどうかを確認します。

  - 演算子の左側：確認するフィールド名。

  - 演算子の右側：チェックする値のリストは「,」で区切られています。

- 含む：検査が必要な値を含むフィールドの値をチェックする。

  - 演算子の左側：チェックするフィールド名（このフィールドは配列または文字列の値である必要があります）；

  - 演算子の右側：検査する値。

- 代入する：あるフィールドの値を変数に割り当てること。

  - 演算子の左側：代入するフィールド名；

  - 演算子の右側：代入する変数名。

- Matches: フィールドの値が正規表現のパターンに一致するかどうかを検証します。

- 演算子の左側：検査するフィールド名；
- 演算子の右側：正規表現の文字列。

- 時間設定：一定期間内の条件をチェックする機能で、Agg_trigger、Agg_action、およびIndicatorのエンジンにのみ存在します。

- カウント：一定期間内にカウントされたイベント数が条件を満たしているかどうかを確認します。

+ グループ化／グループ解除：ユーザーがANDまたはORの演算子内で条件を迅速にまとめたり分割したりできるようにします。グループ化／グループ解除の手順は以下の通りです。

- グループ化する

- グループ化するフィールドをクリックしてください。
- 「グループを選択」画面で、グループ化の各手順の詳細を表示します。

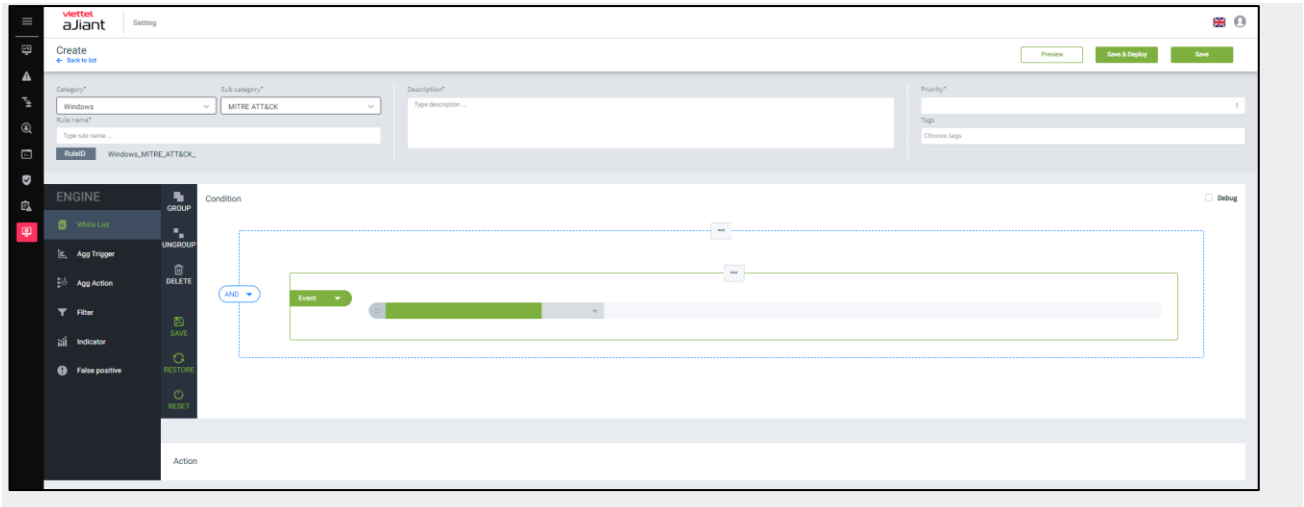
- グループ分け：

- グループ化したいアイテムをクリックしてください。
- グループからの削除を選択 詳細画面でグループ分割の手順を実行する

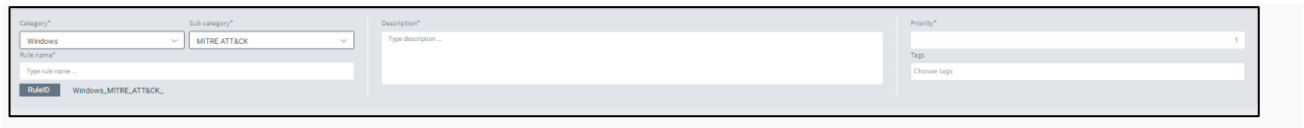
+ 復元：直近の「保存」ボタンを押した直後に自動的にリセットされます。
+ リセット：リセット条件を実行する（初期状態に戻す）。
+ 削除：現在フォーカスされている条件を削除する；

ルール相関の新規追加手順：

- Correlation画面で「Create」ボタンを選択すると、システムは新しいルール作成画面を表示します。

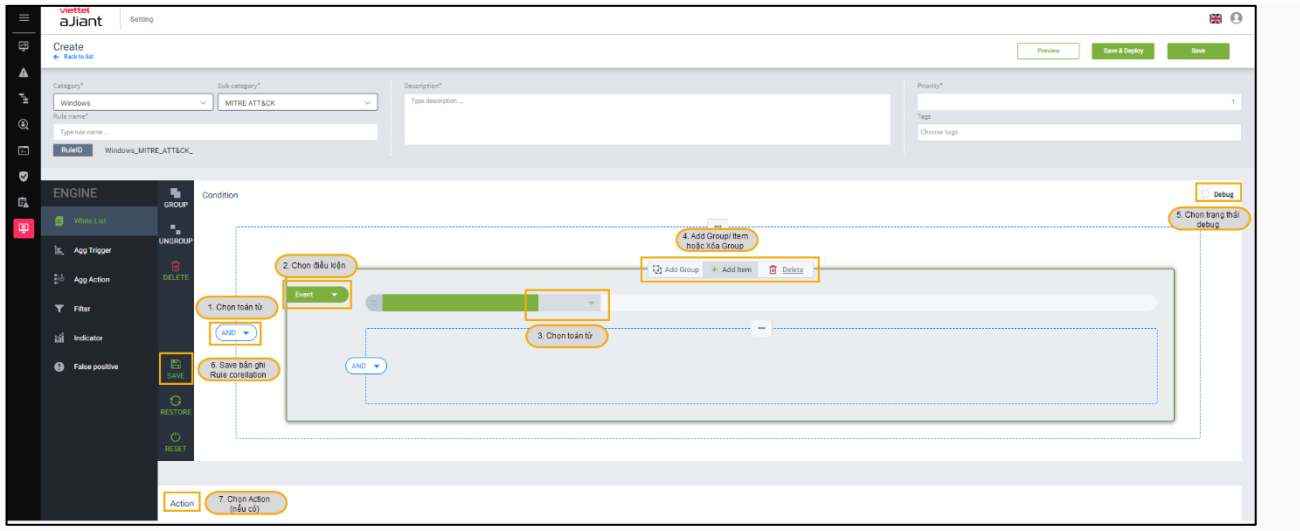


- ルールの情報を入力してください。



注意：(*)印のある項目は必須入力です。

- エンジンを選択し、対応するイベント、非イベント、アラート、非アラート、蓄積、関数の条件を入力してください。



- 「保存」を押して条件を保存し、「復元」を押すと直前に保存した状態に戻ります。
- 「アクション」で、そのエンジンに対して実行するアクションを選択してください。

各エンジンに対応するアクションを追加する手順：ユーザーが条件作成の手順を完了し、保存を押すと、画面に各エンジンごとのアクションが表示されます。各エンジンには対応するアクションが含まれます。Agg_triggerエンジンにはアクションはありません。

ホワイトリスト：4つのチェックボックス形式のアクションを含みます：ドロップ、アグリゲートへの移行、アラート、アクティブリスト。ユーザーはこれら4つのアクションのうちいずれか1つを必ず選択する必要があります。条件を満たすログが投入されると、ユーザーが選択した4つのアクションのうちのいずれかが実行されます。4つのアクションの詳細な機能は以下の通りです。

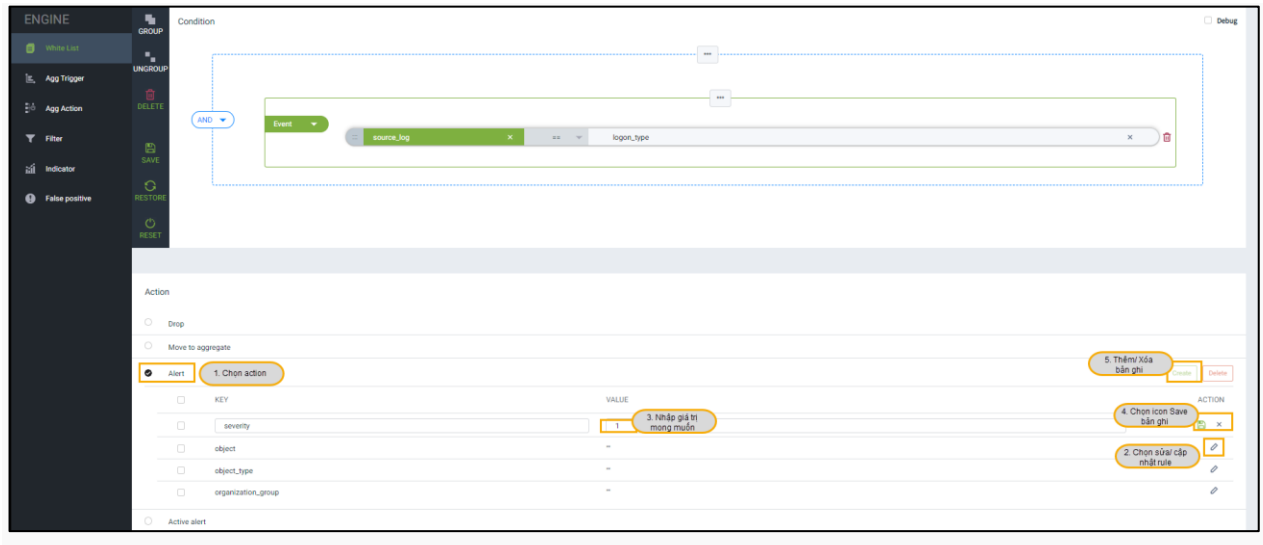
- ドロップ：条件を満たすログは処理フローから除外されます。
- アグリゲートへの移行：条件を満たしたログはアグリゲートエンジンに送られ、引き続き処理されます。

- アラート：Alertにキーと値のフィールドを追加すると、条件を満たすログがAlert管理画面に表示されます。

- アクティブリストの一覧：アクティブリストの各値は、画面上のアクティブリスト表示に追加されます。

アラートアクション／アクティブリストにフィールドを追加する手順：

- ステップ5.1：追加したいアクションをクリックしてください。
- ステップ5.2：「編集」ボタンをクリックして、フィールドに値を入力します。
- ステップ5.3：フィールドに値を入力する；
- ステップ5.4：「保存」ボタンをクリックしてください。
- ステップ5.5：「Add」ボタンをクリックして、Alertに新しいフィールドを追加します。



+ 直前に作成したアクションを削除するには、「削除」アイコンをクリックしてください。

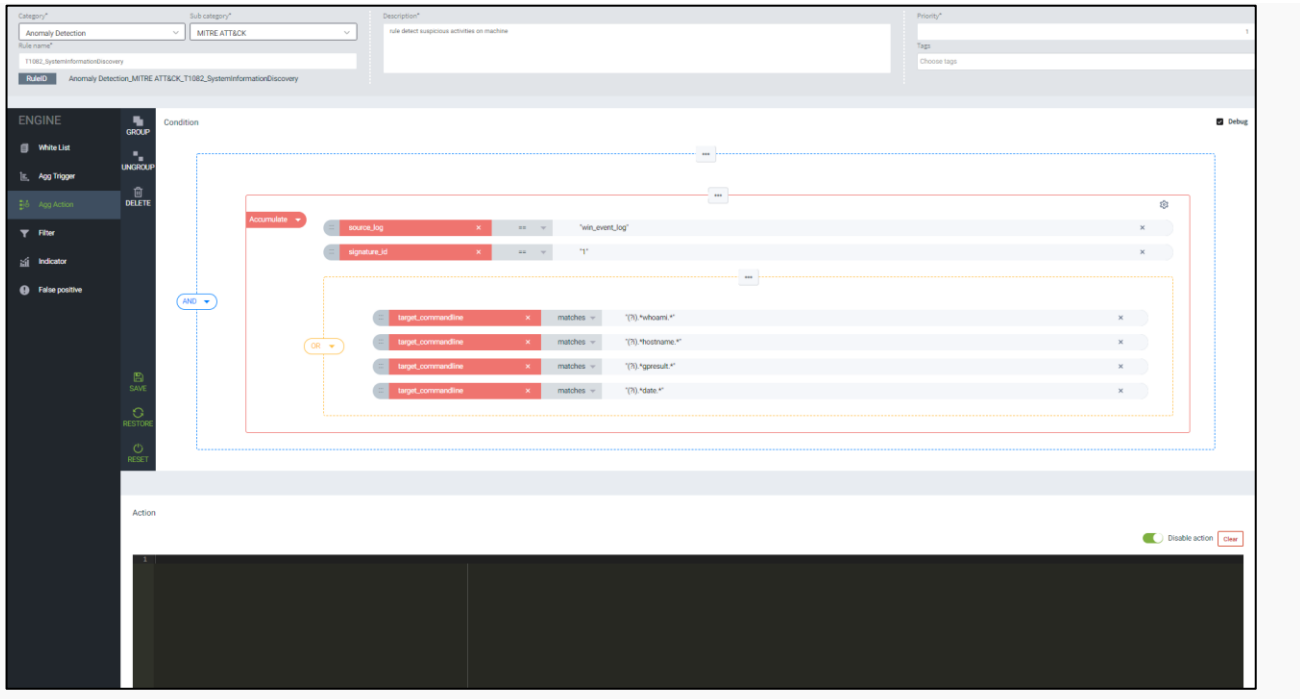
+ アクションを編集するには、「編集」アイコンをクリックしてください。

注意：使用者の目的に応じて、異なるフィールドで複数のアクションを作成することが可能です。

Agg_action: このエンジンでは、ユーザーがコードを追加する操作を行うことができます。

コード追加アクションのためのフィールド追加手順

- ステップ5.1：条件と演算子をすべて入力します。「保存」をクリックしてください。
- ステップ5.2：アクション項目で、「アクションを有効にする」アイコンをクリックします。
- ステップ5.3：コードの内容を入力する。
- ステップ5.4：「クリア」ボタンを選択すると、コードの入力内容がすべて削除されます。



フィルター：3つのアクションで構成されています。Alert（アラート）、Enrichment（エンリッチメント）、およびActiveリスト。ユーザーは同じエンジン内で1つまたは複数のアクションを選択できます。3つのアクションの機能詳細は以下の通りです。

- 拡張：アラートにフィールドを追加する；
- アラートとアクティブリスト（エンジンのホワイトリストのようなもの）。

エンジンフィルターのアクションに対する追加、新規作成、削除の操作は、エンジンホワイトリストのフィールドを追加する場合と同様です。

インジケーター：アラートアクション。インジケーターエンジンのアクションに対する追加、編集、削除の操作は、ホワイトリストエンジンのフィールド追加時と同様です。

FalsePositive:　エンリッチメント操作。FalsePositiveエンジンのアクションに対する追加、新規作成、編集、削除の操作は、ホワイトリストエンジンにフィールドを追加する場合と同様です。

- 「保存」を押してルールをシステムに保存します。ユーザーがシステムに保存すると同時にコレラルエンジンにデプロイしたい場合は、「保存してデプロイ」を押してください。

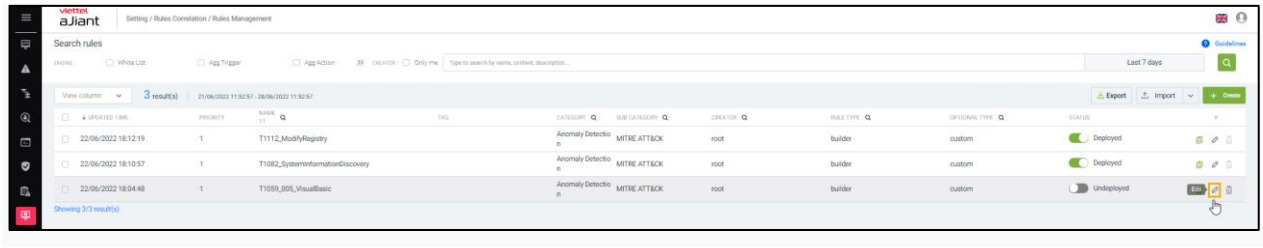
注意：エラーが発生した場合、ユーザーは「プレビュー」ボタンを押してエラーを確認できます。

ルール相関の修正

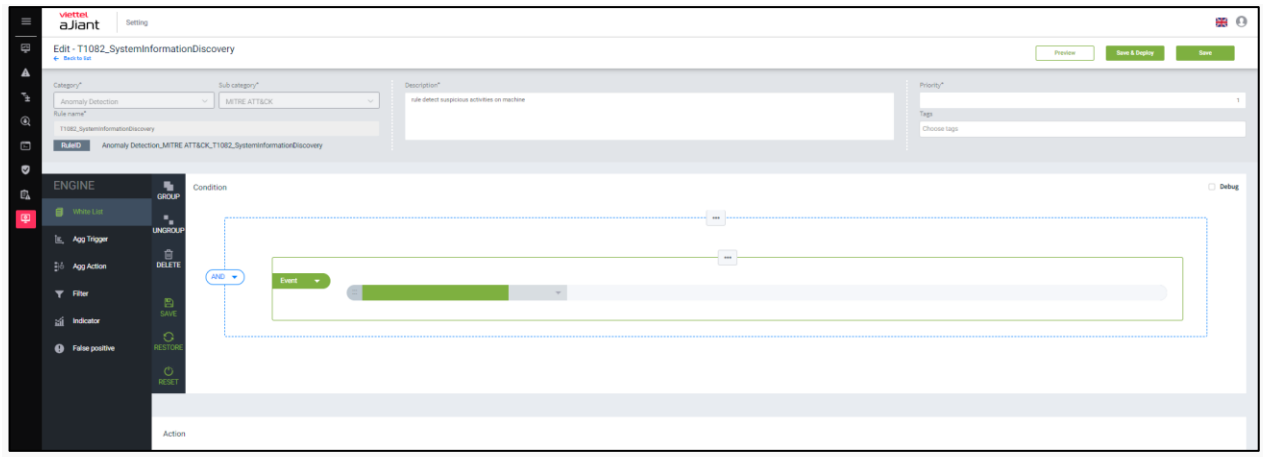
ユーザーが作成したルールを編集できるようにします。

実施手順：

- ルール管理画面で、編集したいルールの編集アイコンをクリックしてください。



- 編集画面で、修正する情報を入力してください。



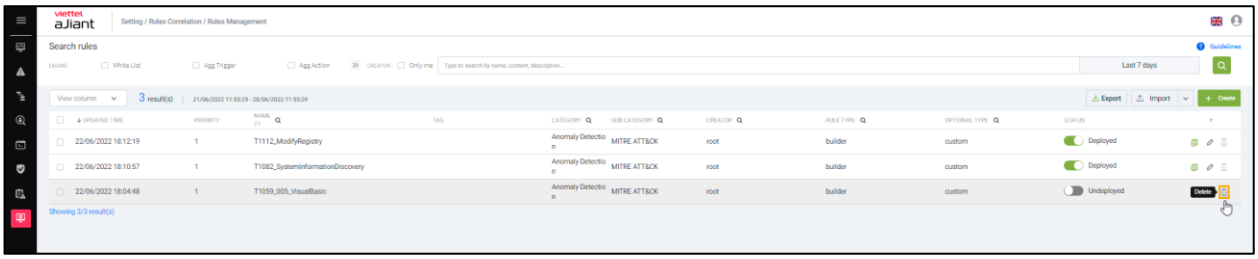
注意：rule、category、subcategoryの各フィールドは編集できません。

- 「保存」ボタンを押してルールをシステムに保存します。ユーザーがシステムに保存すると同時にコリレーションエンジンにデプロイしたい場合は、「保存してデプロイ」を押してください。

保存のみを行ったルールの編集については、ユーザーがルール管理画面で「再デプロイ」をクリックしなければ、そのルールはシステムに反映されません。

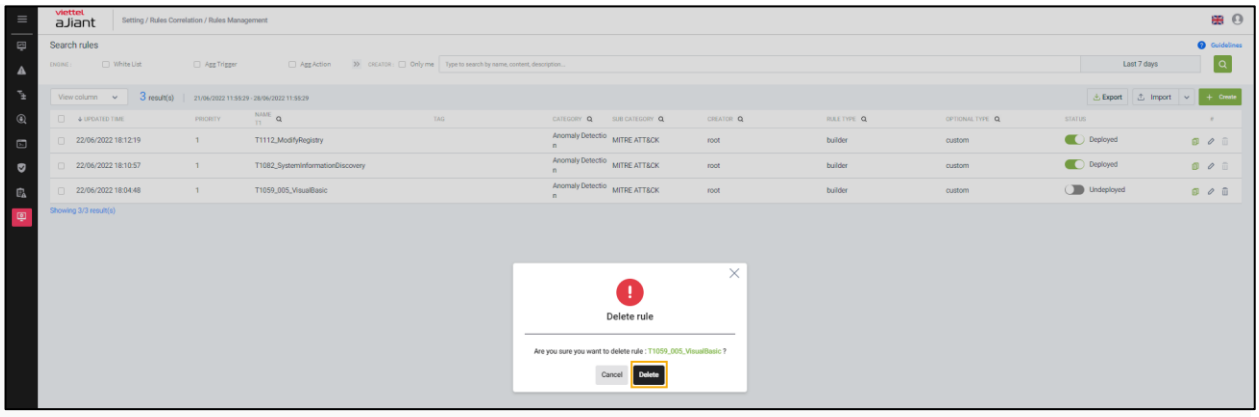
注意：エラーが発生した場合、ユーザーは「プレビュー」ボタンを押してエラーを確認できます。

3.9.3 ルール相関の削除

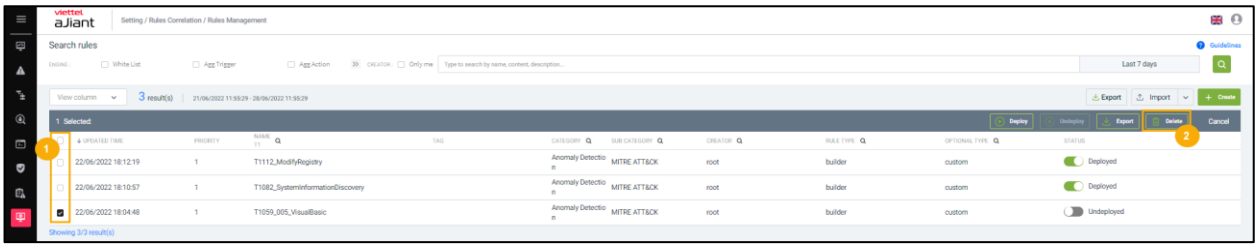


ルールを1つ削除する手順：

- 削除したいルールの「削除」アイコンをクリックしてください。
- 画面に削除確認のメッセージが表示され、「キャンセル」または「削除」を選択してください。

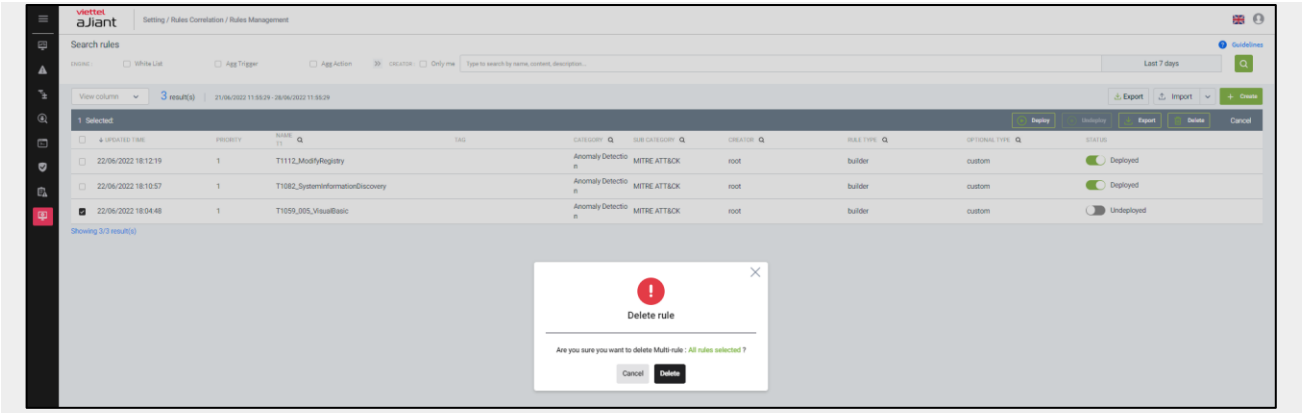


+ 「削除」を選択すると、選択したルールは表示画面から消えます。



複数のルールを削除する手順：

- 削除したいルールをクリックして選択してください（「すべてのルールを選択」をクリックするとすべて削除できます）。
- 画面に削除確認のメッセージが表示され、「キャンセル」または「削除」を選択してください。



- 「削除」を選択すると、すべてのルールが画面から削除されます。「キャンセル」を選択すると、直前の操作が取り消されます。

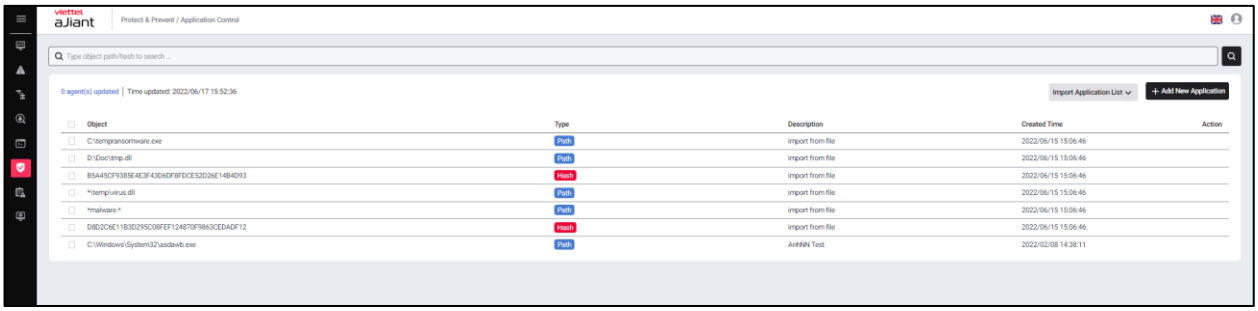
3.10 保護と予防

3.10.1 アプリケーション制御

目的：アプリケーションコントロール機能は、ユーザー端末上で実行を許可しないアプリケーションやプロセスを設定することを可能にします。アプリケーションやプロセスは、ハッシュ値（MD5、SHA1、SHA256）またはパスに基づいて識別されます。

ブロックされたアプリケーション／プロセスの一覧を表示する

「Protect & Prevention」タブをクリックし、「Application control」を選択すると、ユーザーの端末で使用を禁止されているすべてのアプリケーションやプロセスが表示されます。

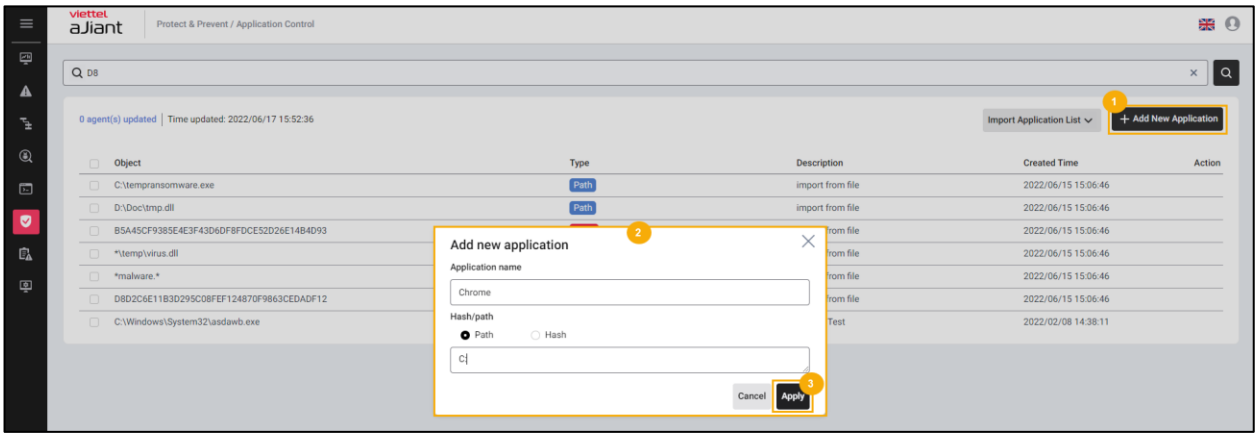


ブロックされているアプリケーション／プロセスを検索する

ユーザーは、ブロックされたアプリケーションのハッシュコードまたはパスで検索できます。

ブロックされたアプリ/プロセスの新規追加

「Add new」をクリックして、新しいブロック対象のアプリケーションやプロセスを追加します。ユーザーはパスまたはハッシュコード（MD5、SHA1、SHA256）でブロックを選択できます。



既存ファイルからアプリケーション/プロセスを新規追加する

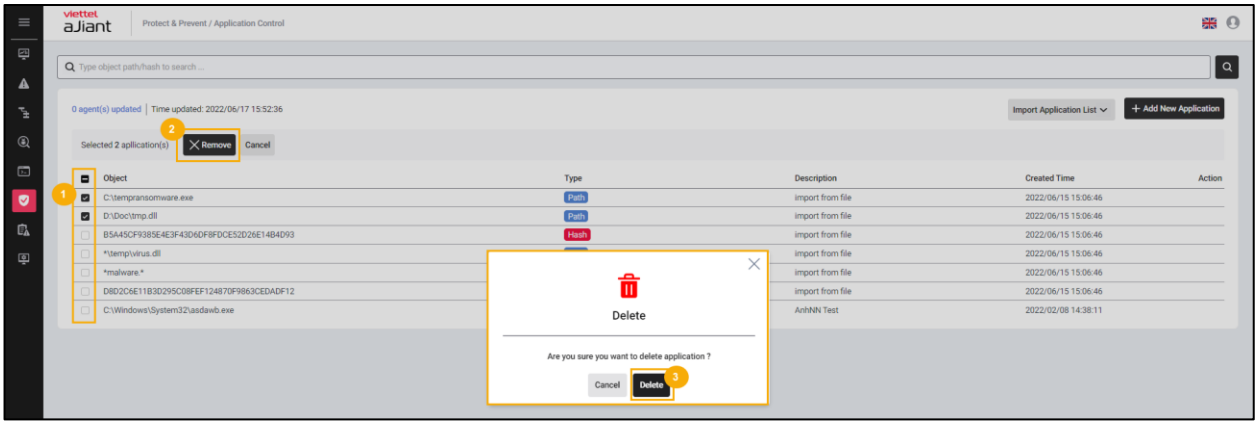
ユーザーは、既存のテンプレートに従った.csvファイルからブロックされたアプリケーションやプロセスを現在のアプリケーションリストに新規追加することができます。

「インポート」をクリックし、アップロードするファイルのパスを選択して「開く」をクリックすると、システムが自動的にブロックすべきアプリケーションのリストをシステムに追加します。

リスト内のブロックされたアプリ/プロセスを削除する

システムは、ブロックされた1つまたは複数のアプリケーションの削除をサポートします。

削除したい各アプリケーションをクリックし、「削除」アイコンをクリックするか、各アプリケーションの先頭にあるチェックボックスをクリックしてから「削除」ボタンをクリックしてください。



新しいリストに正常に更新されたエージェント数の更新フロー

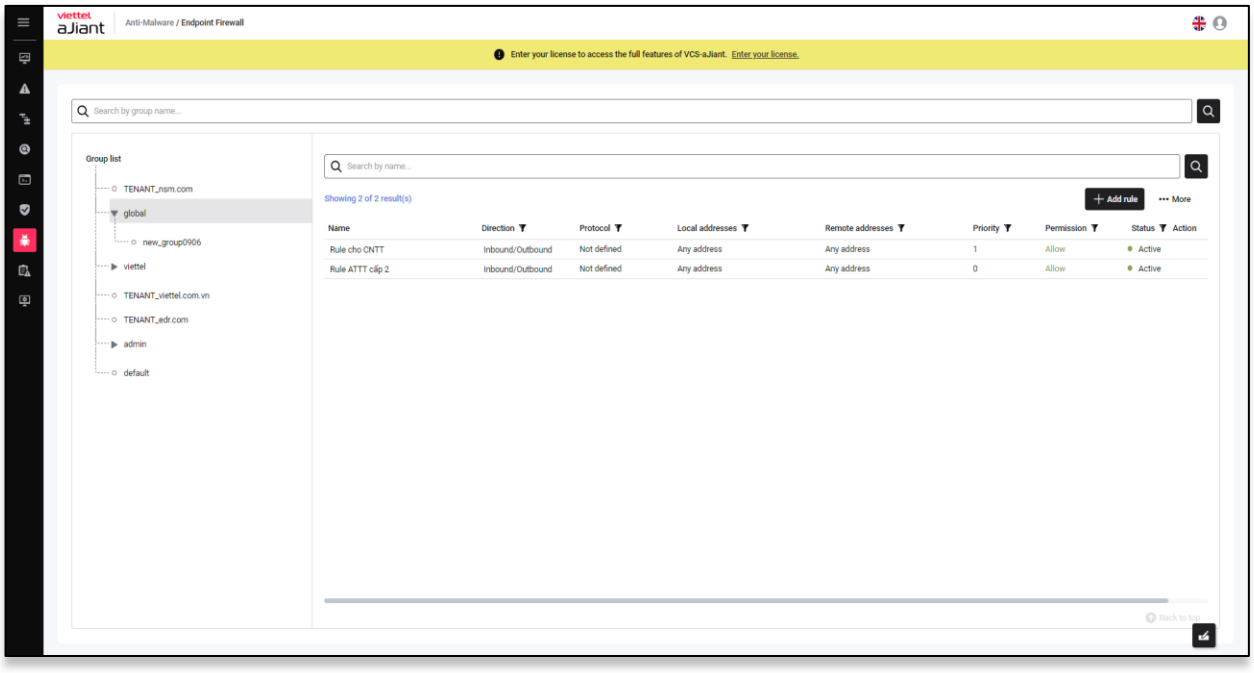
ユーザーがインターフェース上でプロセスリストを追加・編集・削除すると、システムはこのリストをエージェントにファイル更新のフロー（3分ごと）で配信します。エージェントは新しい設定を受け取ると、イベントID=101のログを生成しサーバーに送信、イベント検索画面に表示されます。その後、システムはアプリケーションコントロール画面上で新しい設定リストを更新したエージェント数を自動的に更新します。

3.10.2 エンドポイントファイアウォール

目的：エンドポイントファイアウォール機能は、ユーザー端末上でブロックまたは許可する接続を設定できるようにします。これには、アプリケーション、IP、ポート、またはIPとポートの組み合わせによるブロックが含まれ、TCP、UDP、ICMP、ICMPv6、IGMPプロトコルをサポートし、IPv4およびIPv6に対応し、インバウンドおよびアウトバウンド接続をサポートします。

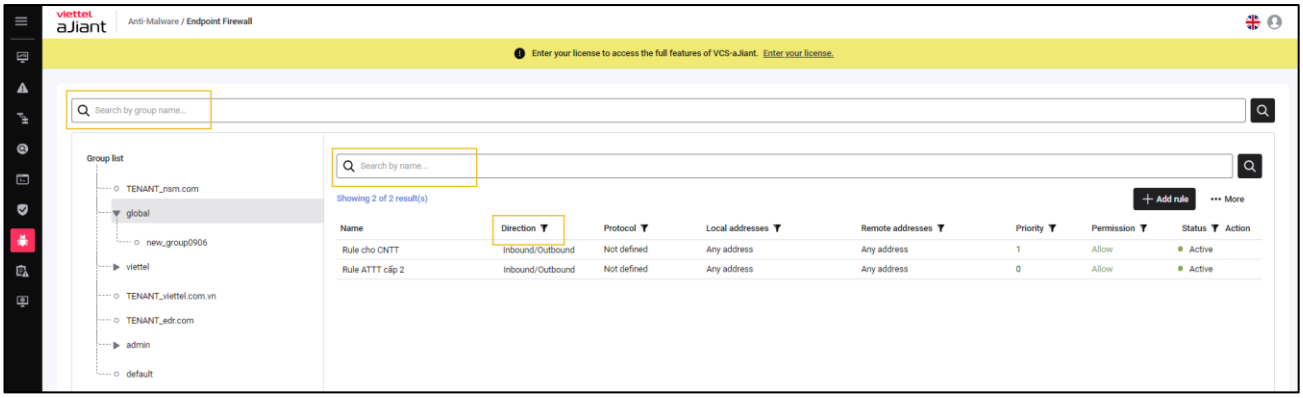
ブロックされた接続の一覧を表示する

Alti-Malwareタブをクリックし、Endpoint Firewallを選択すると、ユーザーグループごとにブロックされたすべての接続リストが表示されます。



ブロックされた接続を検索する

ユーザーは、ファイアウォールの一覧画面で、ユーザーグループ別、ファイアウォールルール名別、または各条件（名前、接続タイプ（インバウンド/アウトバウンド）、IPアドレスなど）の値によるフィルタリングで検索することができます。



ブロックされた接続を新規追加する

グループを選択し、「新規追加」ボタンをクリックして、ポップアップで接続情報を入力すると、接続がブロックされます。

+ 名前：作成したい条件の名前；

+ プログラム：ユーザーのコンピュータ上でブロックまたは許可する必要があるプログラム。例：「%ProgramFiles% (x86)\アプリケーション名.exe」

+ プロトコル：未定義、ICMP、TCP、UDP、ICMPv6、IGMP

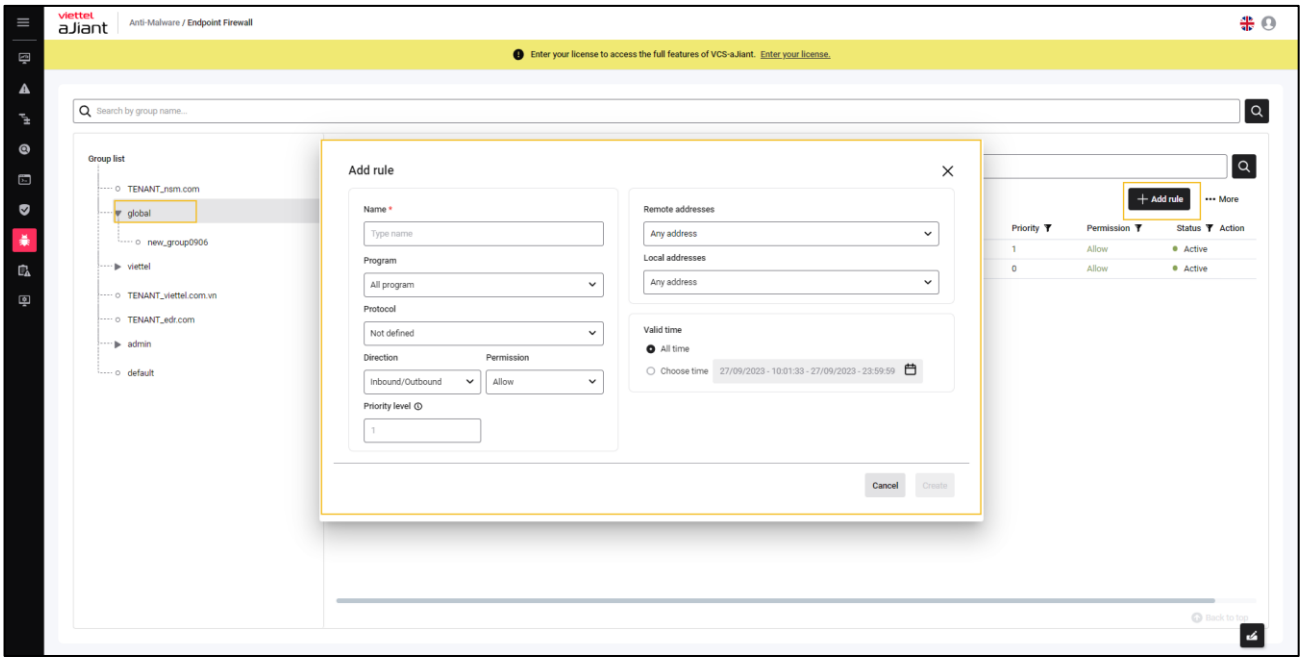
+ ポート：ブロックするポート番号。すべてのポートをブロックする場合は「0」を入力してください。

+ 方向：インバウンド、アウトバウンド、インバウンド／アウトバウンド

+ 許可：許可する／ブロックする

+ リモートアドレス／ローカルアドレス：IPv4、IPv6、およびIPレンジをサポート。

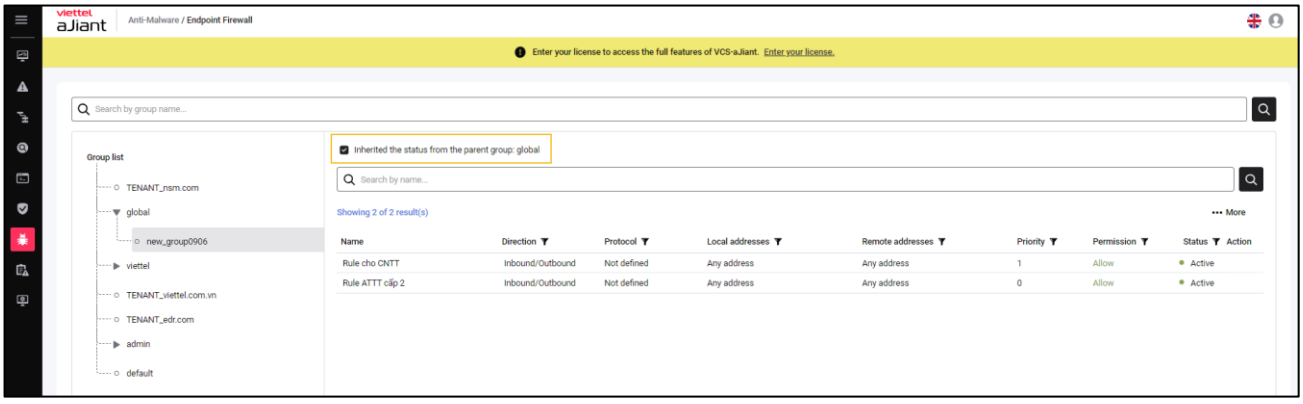
+ 有効期間：条件が有効となる期間



注意：親グループからの継承ルール

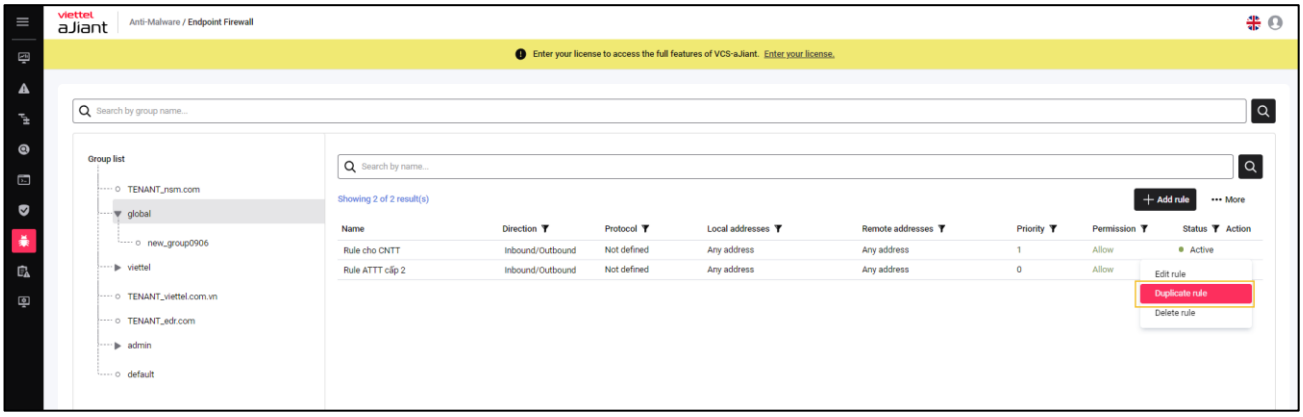
+ 「親グループからステータスを継承する」を選択すると、子グループは親グループのすべての条件を継承し、継承した条件の追加や変更はできません。

+ 「親グループからステータスを継承する」を選択しない場合、子グループは親グループから継承されず、新規追加や条件の削除が可能になります。



既存の条件からコピーを作成する

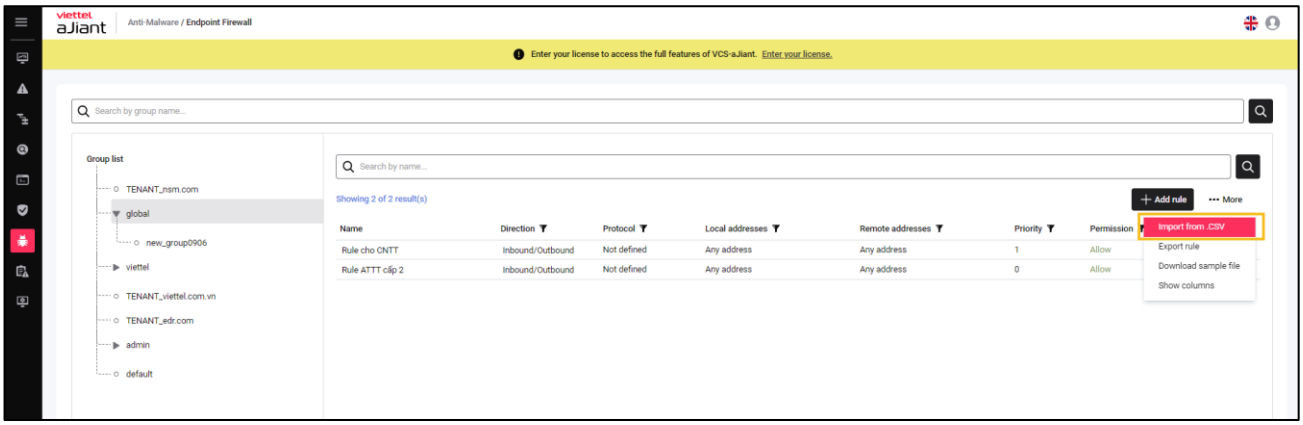
コピーを作成する条件を選択し、アクションを実行して、複製ルールを選択してください。



既存ファイルからブロックされた接続を新規追加する

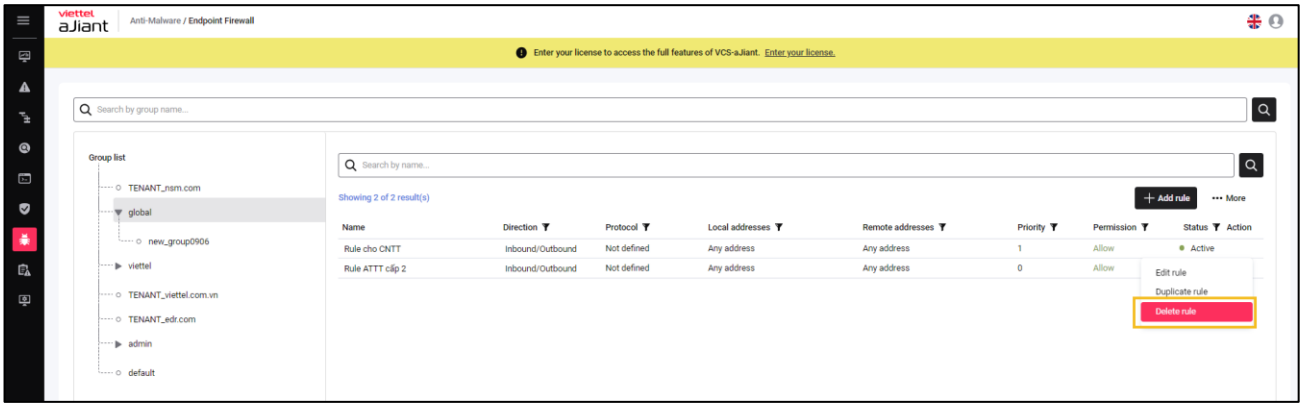
ユーザーは、既存のテンプレートに従った.csvファイルからブロックされたアプリケーションやプロセスを現在のアプリケーションリストに新規追加することができます。

「.CSVからインポート」ボタンをクリックし、アップロードするファイルのパスを選択して「開く」ボタンをクリックすると、システムが自動的にブロックすべきアプリケーションのリストをシステムに追加します。



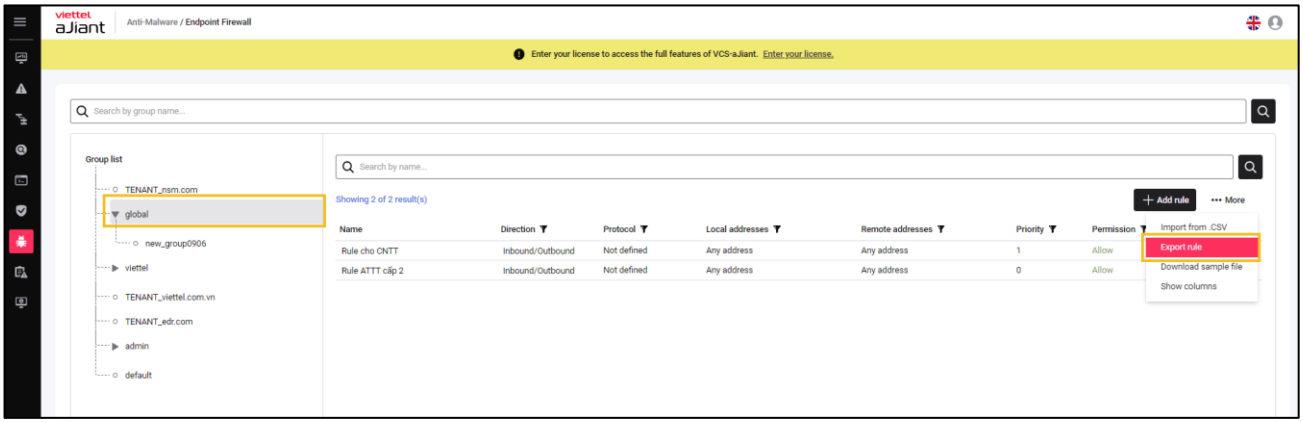
ブロックされた接続をリストから削除する

削除する各接続をクリックし、「削除」アイコンをクリックしてください。



条件データの出力

ユーザーグループを選択し、「More」を選んでから「Export　Rule」を選択し、選択したグループのすべての条件情報を含むCSVファイルをエクスポートします。



3.11　アンチマルウェア

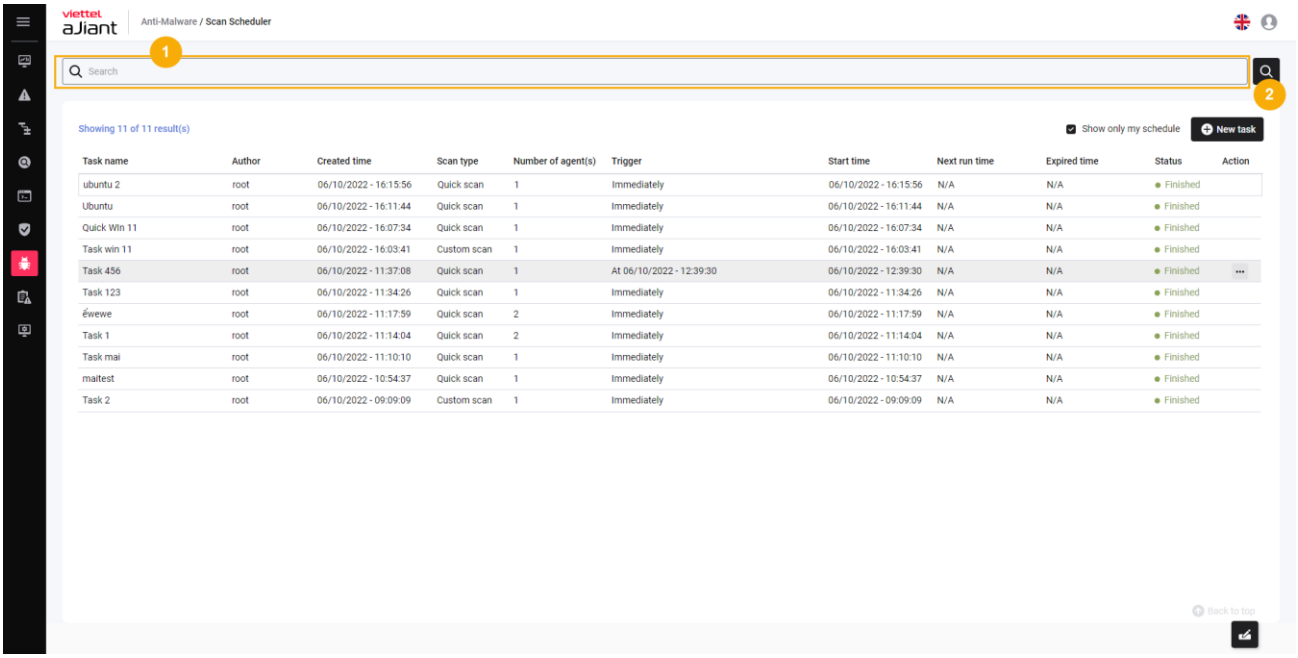
3.11.1　スキャンスケジュール

目的：スキャンスケジュール機能は、ユーザーがリモートのクライアント端末でウイルススキャンのスケジュールを設定できるようにします。

スキャンスケジュールタスクの検索

目的：スキャンスケジュールタスク検索機能は、ユーザーがタスク名に基づいて各クライアントのスキャンスケジュールを検索できるようにします。

実施手順：



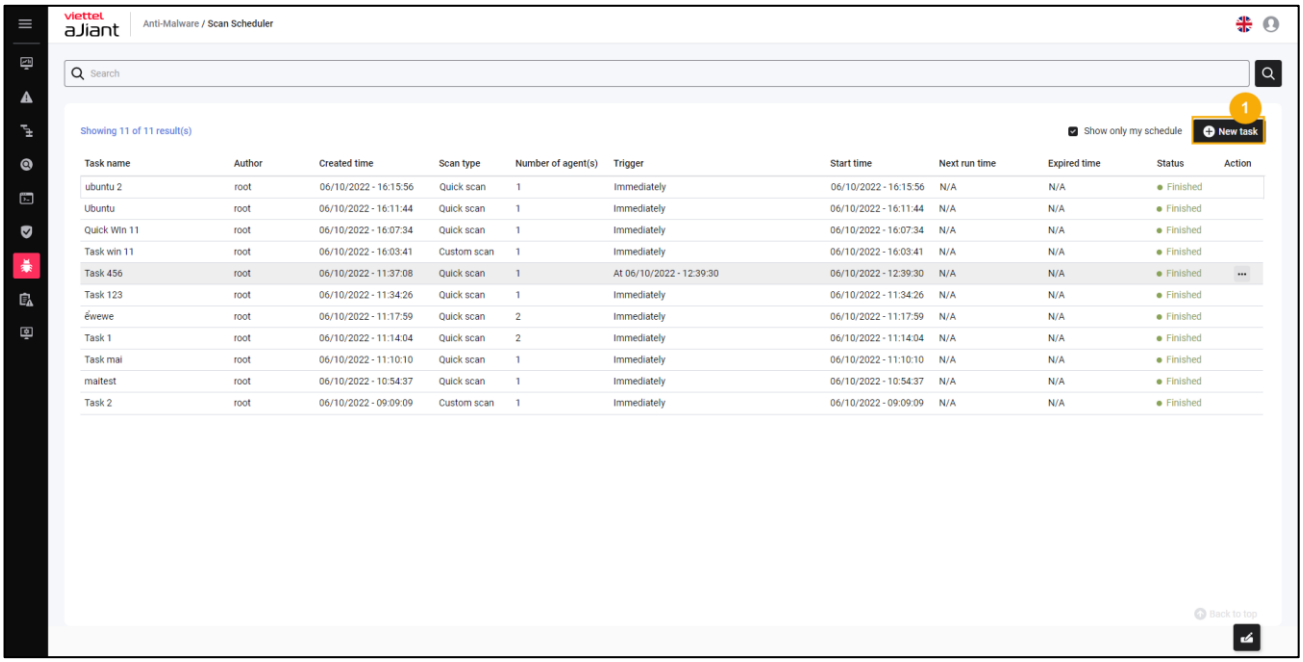
- ユーザーが検索キーワードを入力します。
- ボタンを選択するか、Enterキーを押して、入力したキーワードで検索操作を確定してください。
- システムは検索キーワードに基づいてスキャンスケジュールの一覧を表示します。

スキャンスケジュールタスクの新規追加

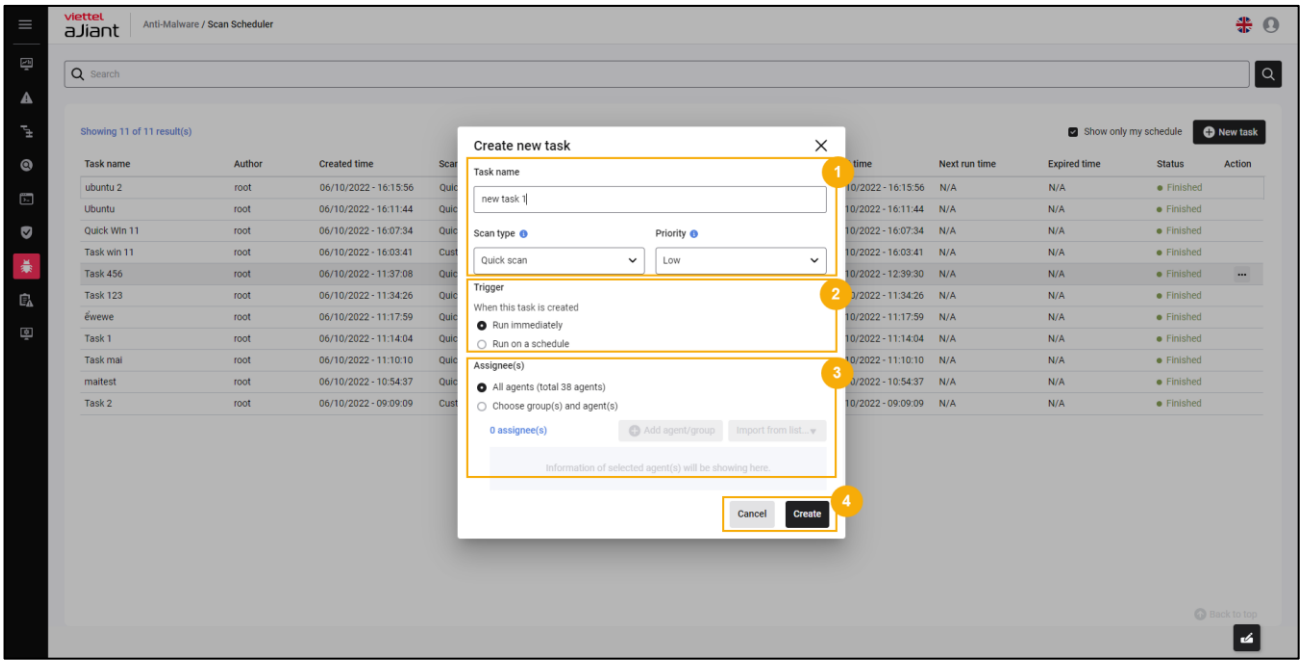
目的：ユーザーが新しいスキャンスケジュールを追加し、時間設定およびワークステーション情報を構成できるようにすること。

実施手順：

- スケジュールスキャンの一覧画面で、ユーザーは「新しいタスク」ボタンを選択します。



- システムは新しいスキャンスケジュール追加画面を表示し、ユーザーは以下の情報を入力します：



1 – スキャンスケジュール情報には、タスク名、スキャンタイプ、優先度が含まれます。

タスク名：ユーザーがスキャンスケジュール名を入力する。

スキャンタイプ：ユーザーは3種類のスキャンの中から1つを選択します。許可されるもの：

+ クイックスキャン：疑わしいファイルやフォルダを迅速にチェックする。

+ 全体スキャン：コンピュータ内のすべてのファイルとフォルダを検査します。このプロセスは完了までに数時間かかる場合があります。

+ カスタムスキャン：コンピューター内の特定のファイルまたはフォルダーをスキャンすることをユーザーに許可します。

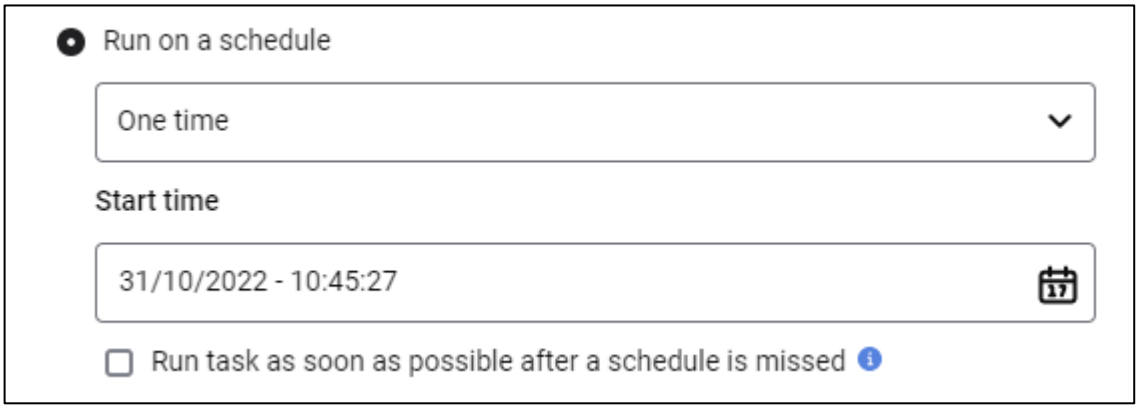
優先度：ユーザーがスキャン速度を選択し、システムリソースの使用レベルを変更できるようにします。優先度を高く設定すると、システムは高速にスキャンしますが、CPUリソースを多く

消費します。同様に、優先度を低く設定すると、スキャンは遅くなりますが、CPUリソースを節約します。

2 – トリガー情報は、ユーザーがスキャンスケジュールの種類を選択できるようにします。

即時実行：タスクが正常に作成された後、ユーザーが各ワークステーションで直ちにスキャンをスケジュールできるようにします。

スケジュール実行：ユーザーが自身の設定に基づいてスキャンのスケジュールを設定できるようにします。



+ スケジュール：
  - 一回実行: 一度だけスキャンをスケジュールする;
  - 毎日：毎日のスキャンスケジュール設定；
  - 週間：週次スキャンのスケジュール設定;
  - 毎月：月次スキャンのスケジュール設定；
+ 開始時間：ユーザーがスキャンスケジュールの開始時間を入力できるようにすること

+ 例：スケジュール：毎日、開始時間：2022年8月15日 03:00:00。これは毎日午前3時にスキャンを実行するスケジュール設定を意味します。

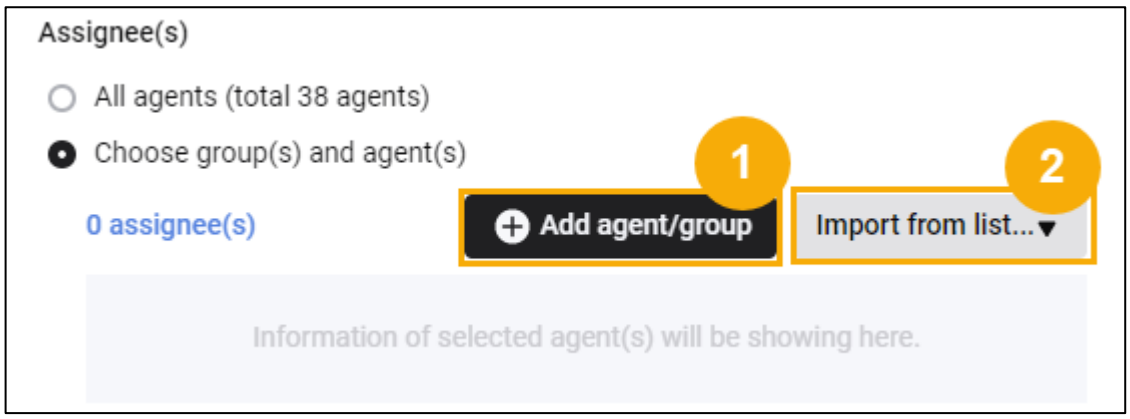
+ スケジュールが遅れた場合にできるだけ早くタスクを実行する：ユーザーが前回のスケジュールが失敗した直後に再スキャンのスケジュールを設定できるようにします。

3 – 譲受人情報：ユーザーがスケジュールを受け取るワークステーションの情報を設定できるようにします。

すべてのエージェント：ログインしているユーザーが管理するすべてのワークステーションでスケジュールを設定する。

エージェントまたはグループを選択してください：

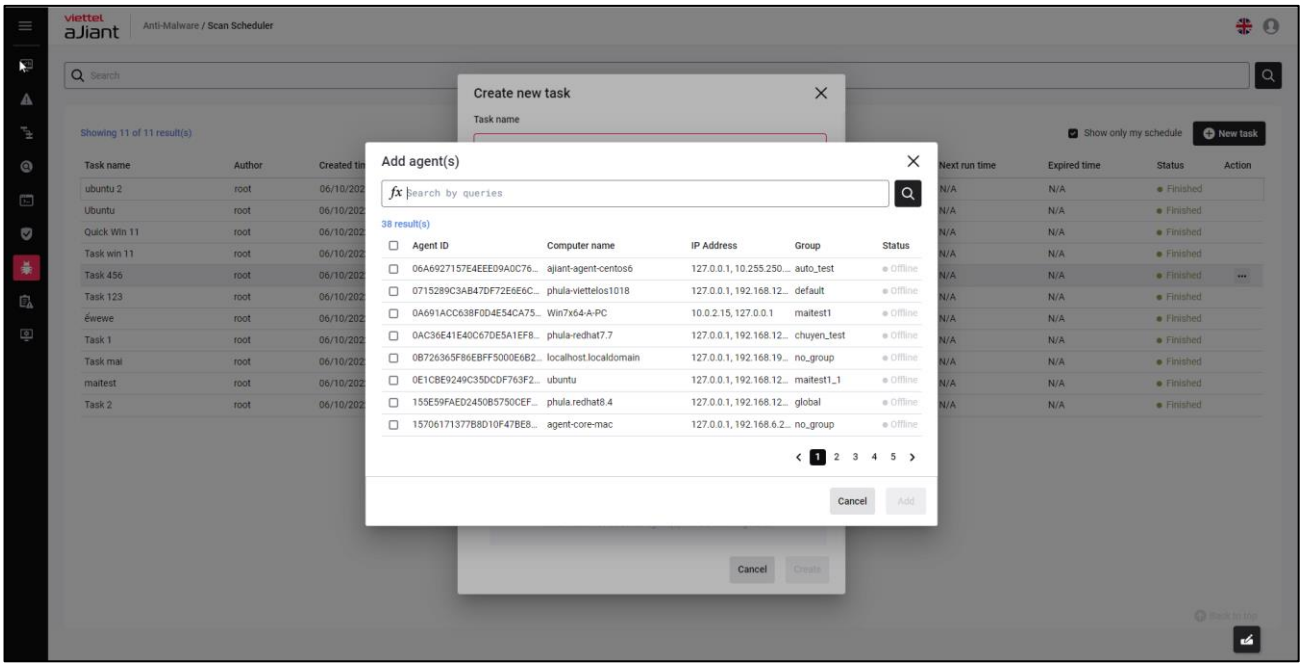
+ 目的：ワークステーションまたはワークステーショングループの設定および選択を可能にすること。



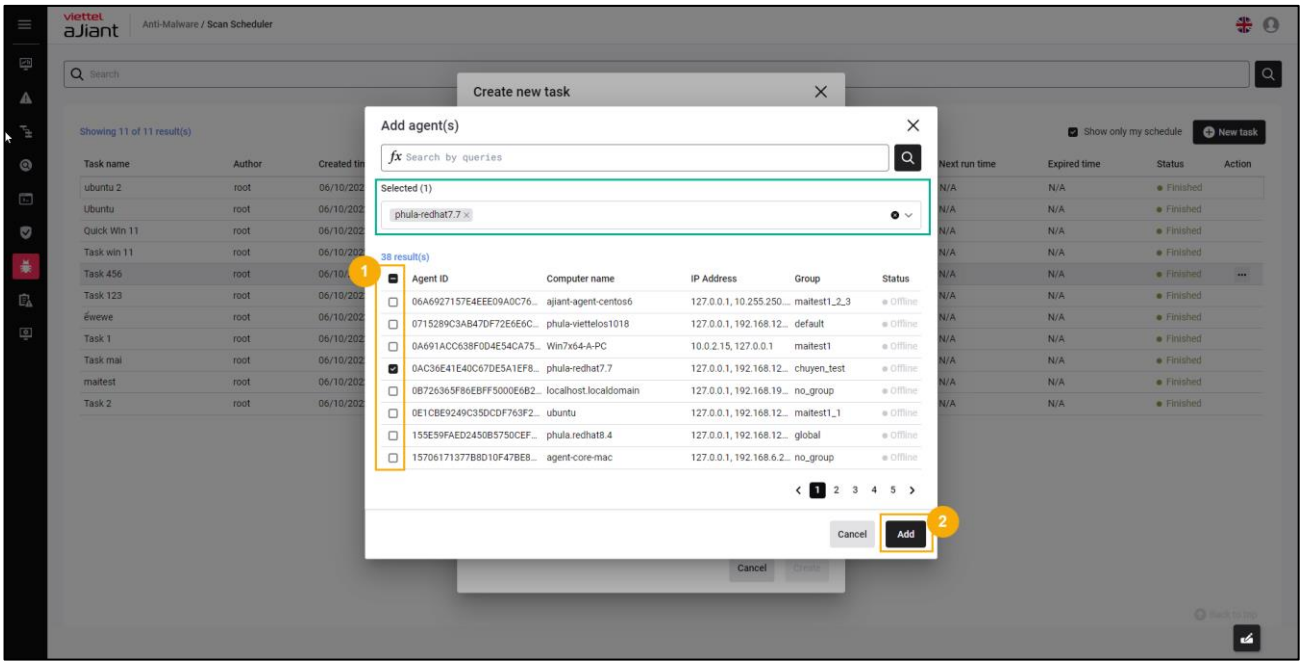
+ 実施手順：エージェントまたはグループの追加

- エージェントまたはグループの追加 - ユーザーは「エージェントを追加」を選択します。

システムはワークステーション選択のポップアップを表示します。



- ワークステーションの検索：
  - 「エージェント追加」ポップアップでは、ユーザーはAgentID、コンピュータ名、IPアドレス、グループ、ステータスなどの情報フィールドを使ってワークステーションを検索できます。
  - ユーザーはアイコンを選択するか、Enterキーを押して検索を確定します。
  - システムはクエリに基づいてワークステーションのリストを表示します。
- スキャンスケジュールを実行するために、1台または複数のワークステーションを選択してください。



- 「Add」ボタンを選択してAgent/Groupの情報を追加します → HTはAgent/Groupの一覧に戻ります。
- または「キャンセル」ボタンを選択して、エージェント/グループ情報の追加操作を中止してください。

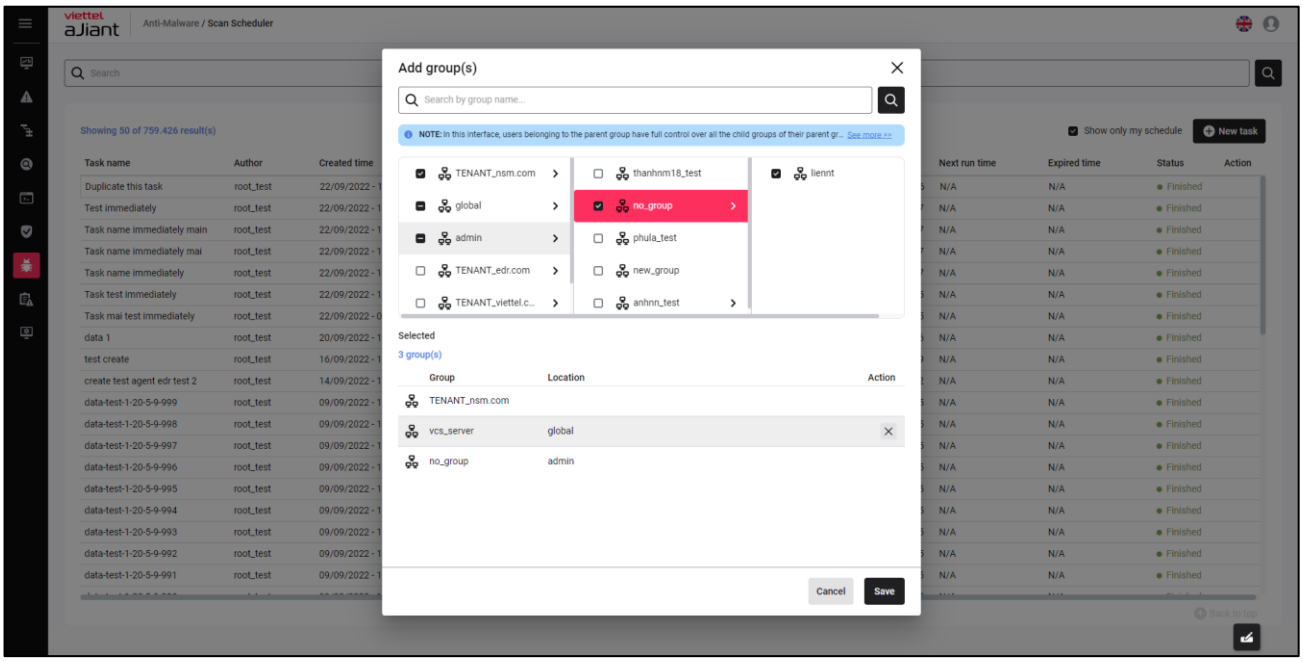
➔ 選択されたワークステーションのリストは、自動的に選択されたワークステーション情報枠に追加されます。

- エージェントまたはグループの追加 - ユーザーは「グループを追加」を選択します。システムはグループ選択のポップアップを表示します。
  - グループを検索する:
    - 「グループ追加」ポップアップでは、ユーザーは「グループ名」フィールドのクエリに基づいてワークステーションを検索できます。

- ユーザーはアイコンを選択するか、Enterキーを押して検索を確定します。

➔ システムはグループの一覧を表示します。

- スキャンスケジュールを実行するグループを一つ以上選択してください：



- 「Add」ボタンを選択してAgent/Groupの情報を追加します → HTはAgent/Groupの一覧に戻ります。
- または「キャンセル」ボタンを選択して、エージェント/グループ情報の追加操作をキャンセルしてください。

➔ 選択されたワークステーションのリストは、選択されたグループ情報枠に自動的に追加されます。

+ .CSVからのインポート：ユーザーが以下の方法でワークステーションのリストをアップロードできるようにします。

- 「リストからインポート」ボタンを選択してください。
- 「Download sample file」を選択すると、ワークステーションのサンプルリストファイルをダウンロードできます。
- ユーザーはワークステーションの情報を入力し、「.CSVからインポート」ボタンを選択してワークステーションのリストファイルをアップロードします。

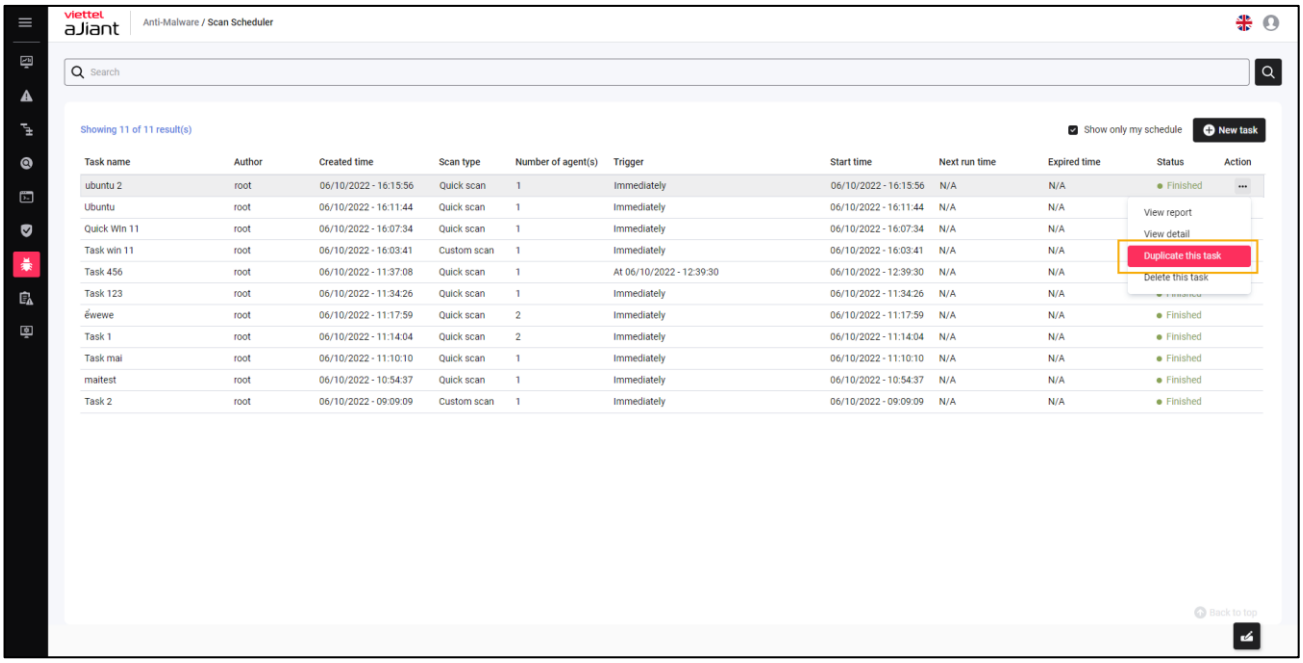
- ユーザーは「作成」ボタンを選択して、新しいスキャンスケジュールの追加操作を完了します。または、「キャンセル」ボタンを選択して、新しいスキャンスケジュールの追加操作を中止します。

スケジュールタスクの複製

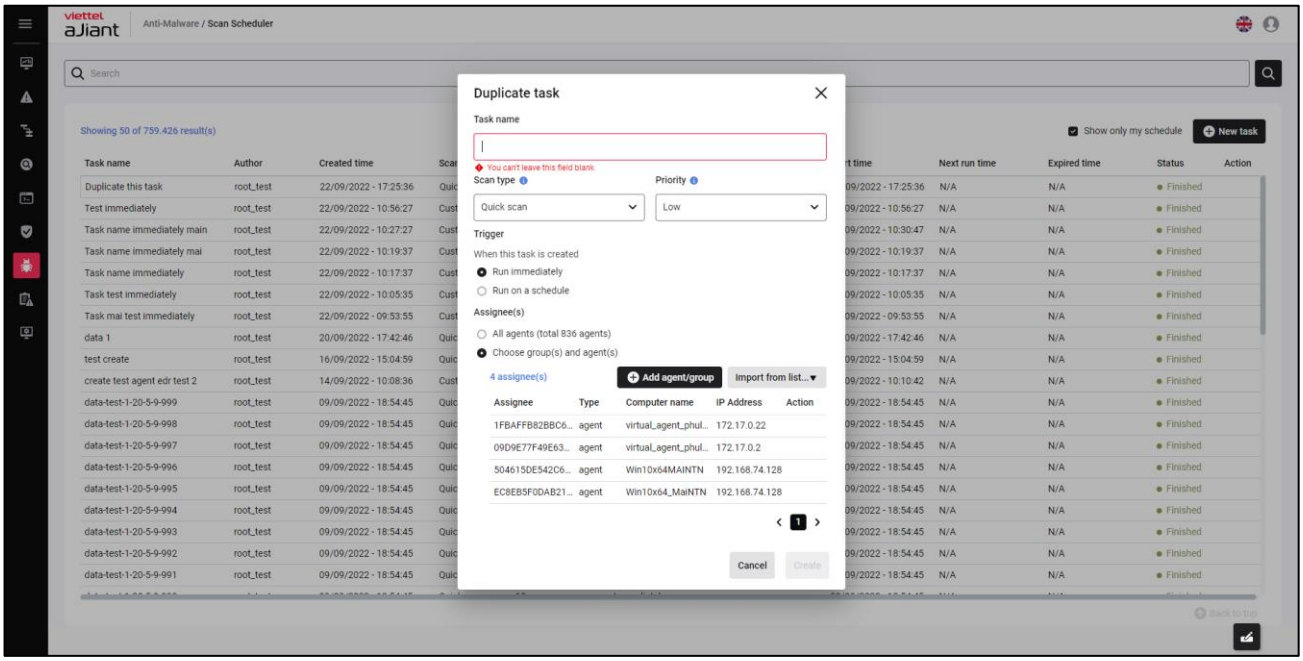
目的：ユーザーがスキャンスケジュールを複製できるようにすること。

実施手順：

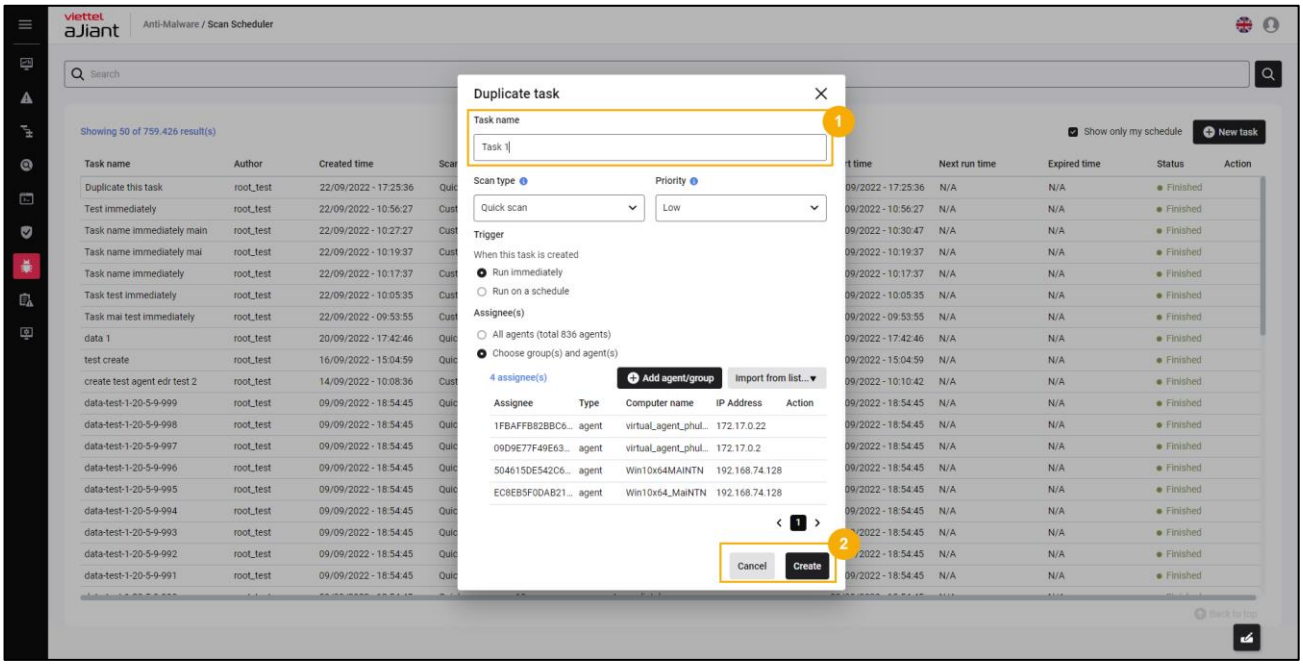
- タスク一覧画面で、ユーザーは複製したいタスクのレコードを選択します。



- システムは「タスクの複製」画面を表示し、ユーザーはタスク名を再入力して、複製前にすべての情報を再確認します。



- ユーザーは「作成」ボタンを選択してスキャンスケジュールの複製操作を完了します。または、「キャンセル」ボタンを選択してスキャンスケジュールの複製操作を中止します。



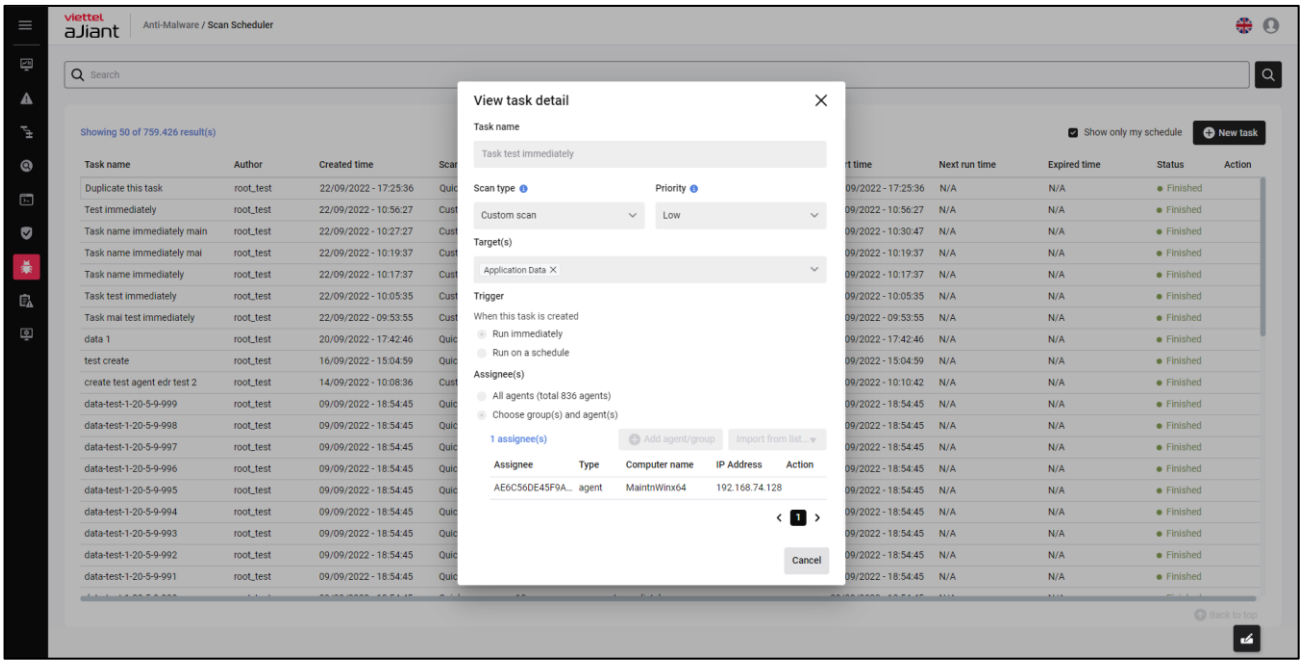
詳細を見る

目的：ユーザーがスキャンスケジュールの詳細情報を閲覧できるようにすること。

実施手順：

- タスクリスト画面で、ユーザーは詳細を確認したいタスクのレコードの「詳細表示」を選択します。

➔ スケジュールスキャン詳細画面表示システム



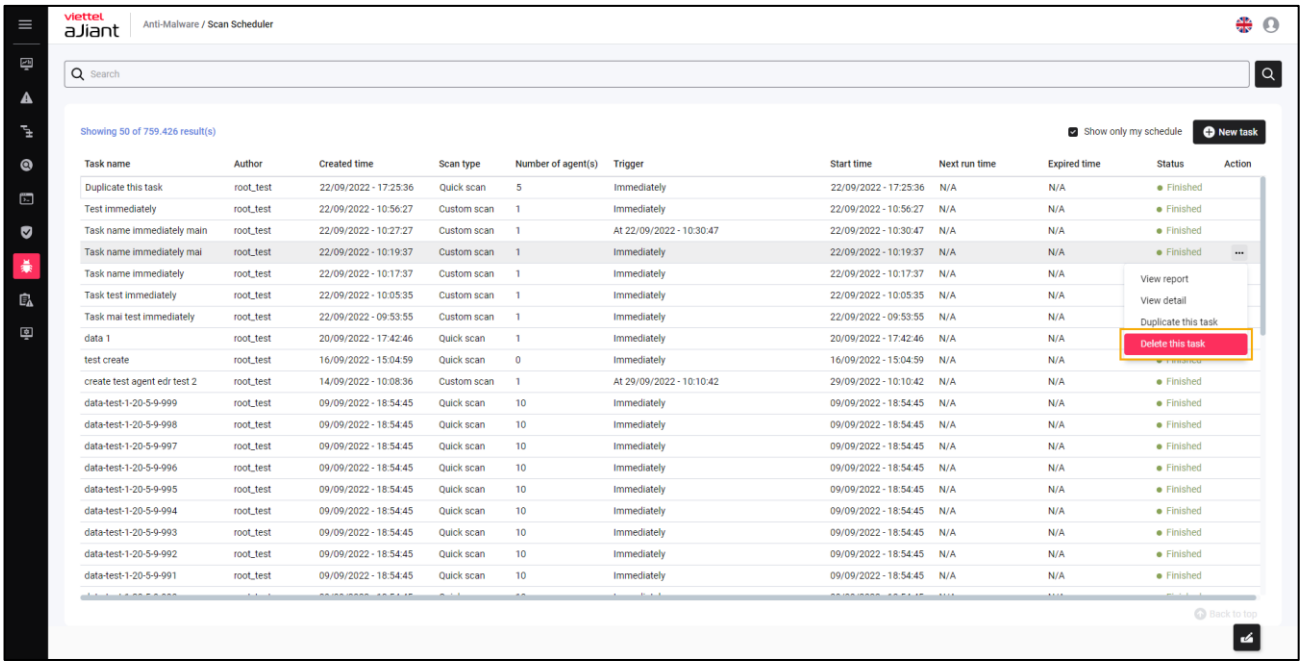
- ユーザーは「キャンセル」ボタンまたは「閉じる」アイコンを選択して、スキャンスケジュールの詳細表示をキャンセルします。

スケジュールタスクを削除する

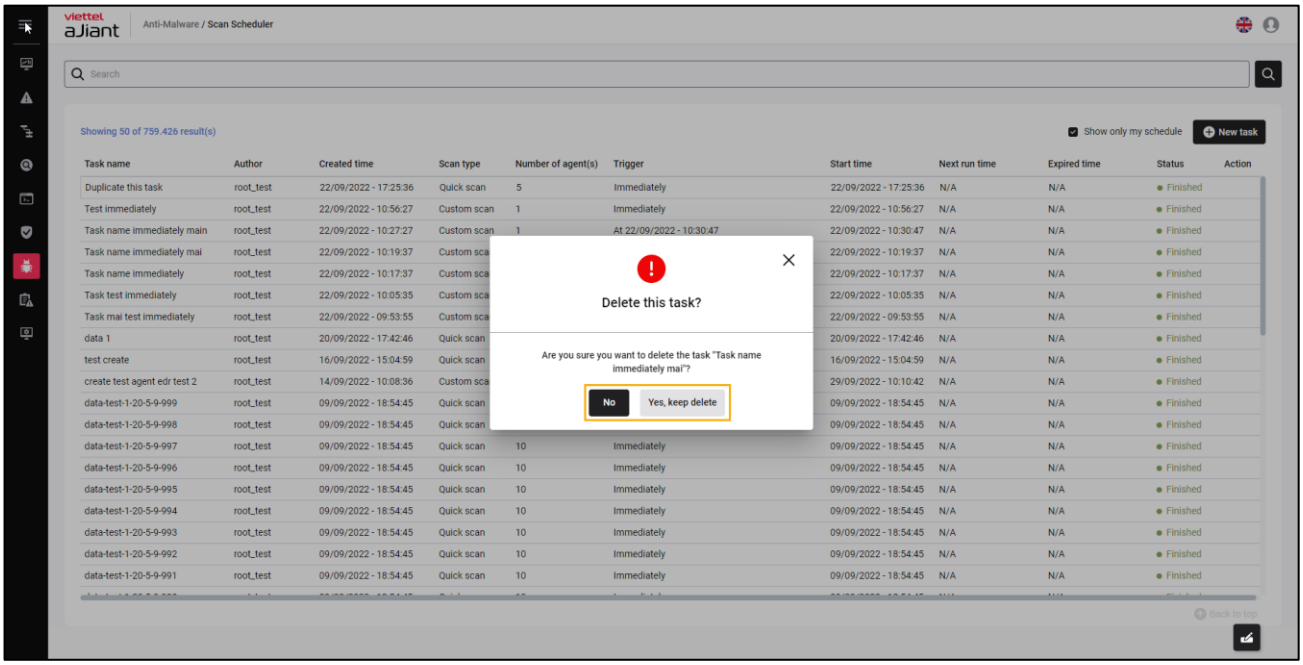
目的：タスクリスト内のスキャンスケジュールの削除を許可すること。

実施手順：

- タスクリスト画面で、ユーザーは削除したいタスクの「このタスクを削除」を選択します。



- システムは「削除確認」のポップアップ画面を表示します。ユーザーは「いいえ」を選択してスキャンスケジュールの削除操作をキャンセルするか、「はい、削除を続行」を選択して削除操作を続けます。

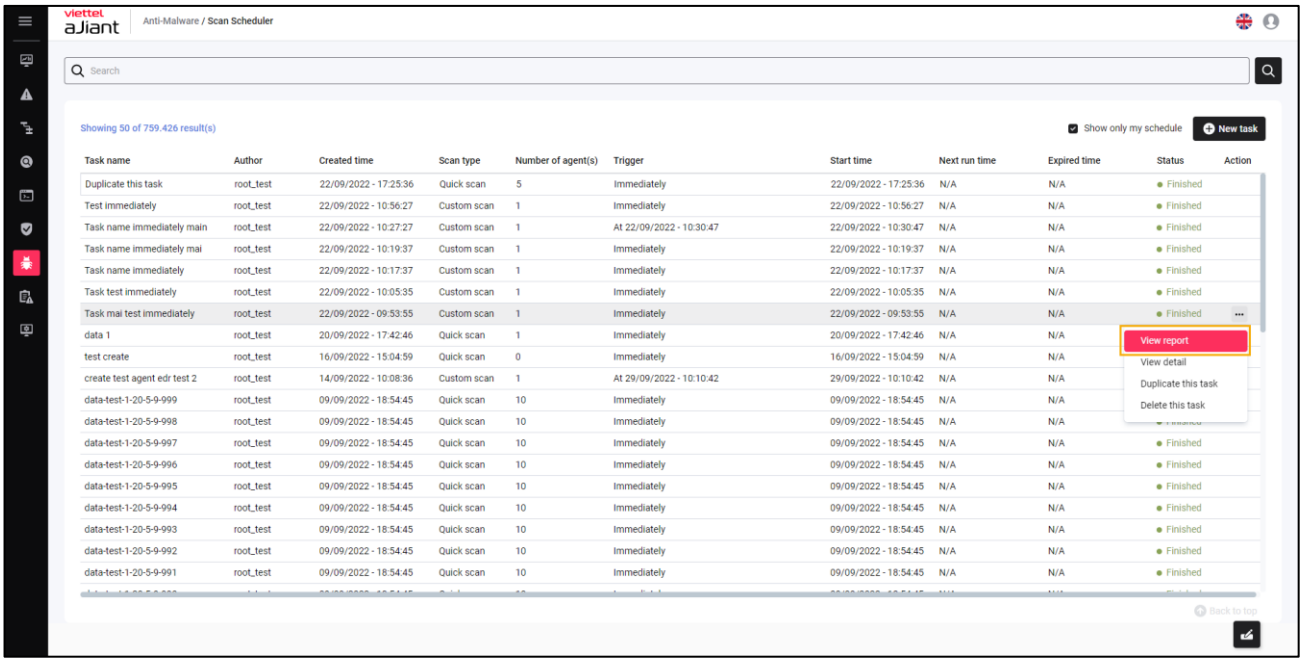


レポートを見る

目的：ユーザーがスキャンスケジュールのレポートを閲覧できるようにすること。

実施手順：

- タスクリスト画面で、ユーザーはレポートを表示したいタスクのレコードを選択します。

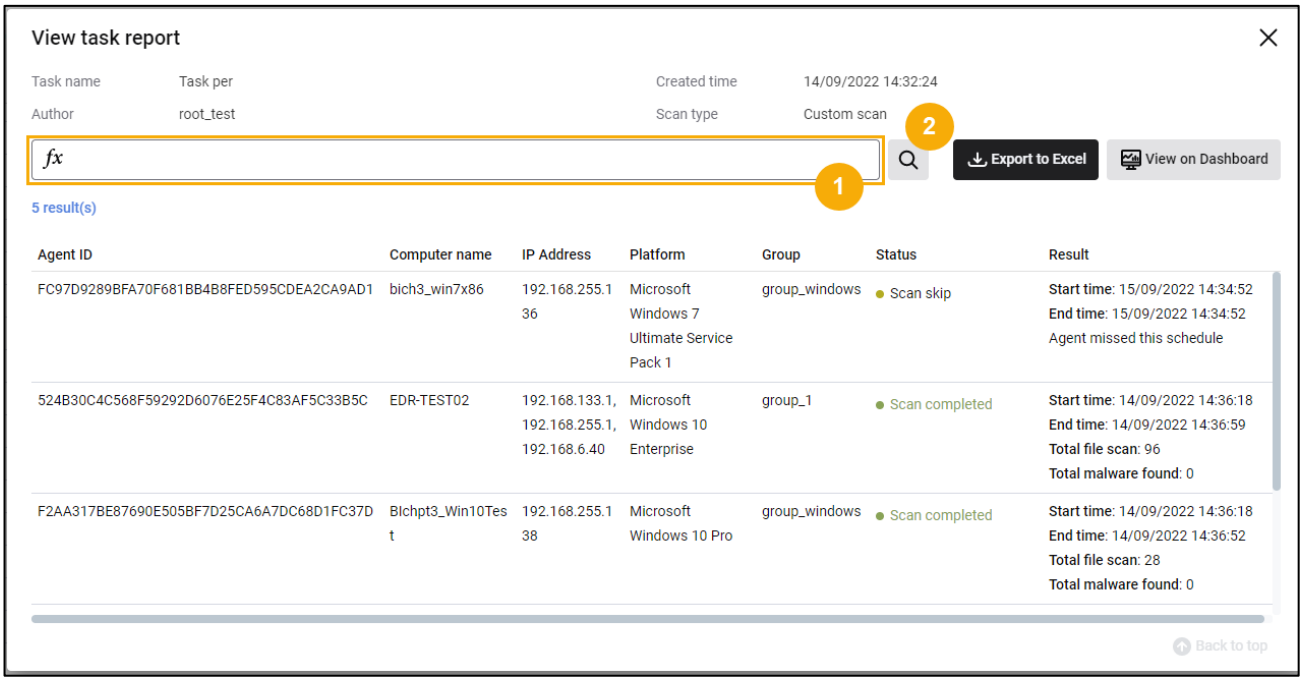


- レポート表示画面システム：

1 – 検索:

目的：レポート内の情報（AgentID、コンピュータ名、IPアドレス、プラットフォーム、グループ、ステータス、結果）を検索できるようにすること。

実施手順：

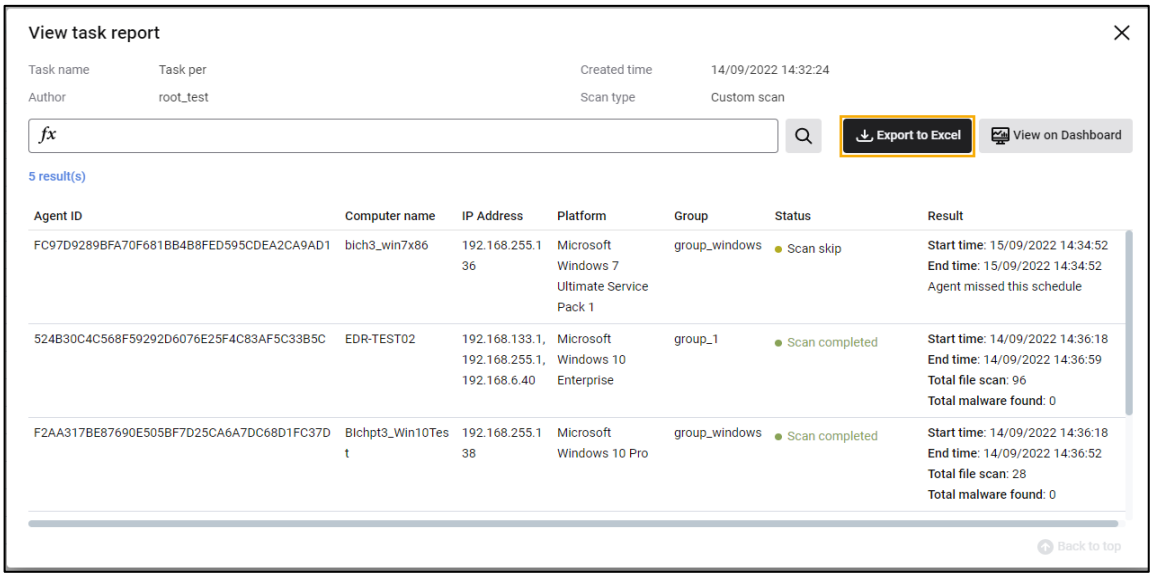


+ ユーザーは検索情報を入力し、アイコンを選択するか、Enterキーを押して検索を確定します。

➔ システムはクエリ実行後にスキャンスケジュールのレポート結果リストを表示します。

2 – エクセルにエクスポートする

目的：ユーザーがスキャンスケジュール結果のレポートをExcelファイル形式でダウンロードできるようにすること。

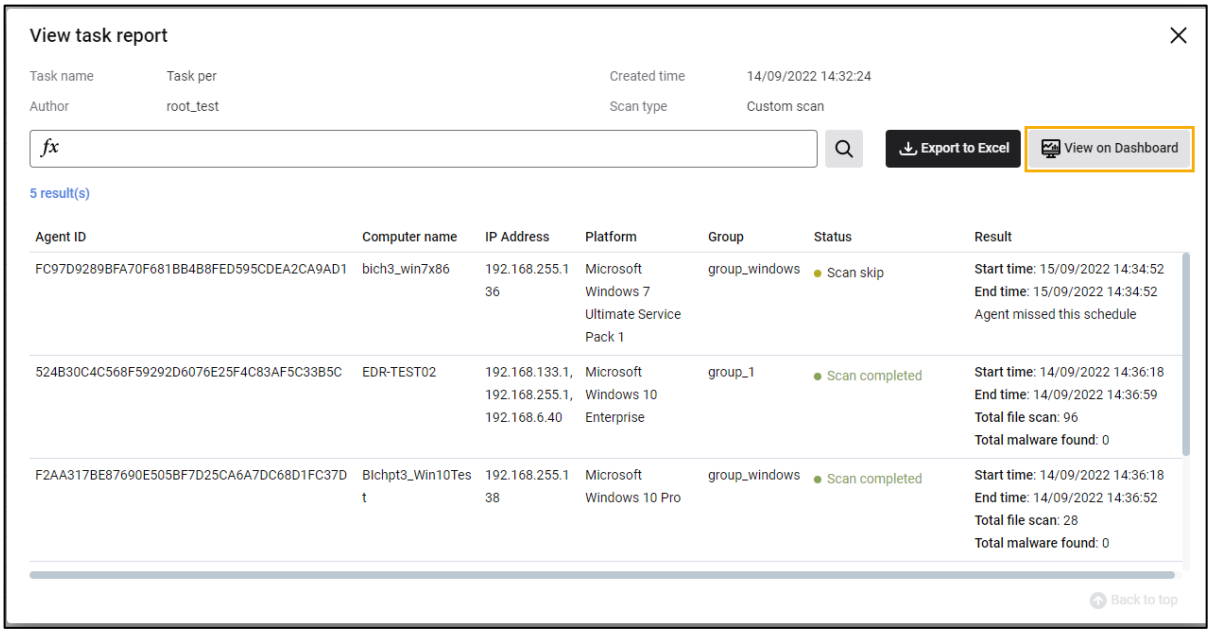


実行手順：タスクレポート画面で、ユーザーは「Excelにエクスポート」ボタンを選択します。

➔ システムはスキャンスケジュールレポートの結果ファイルのダウンロードを許可します。

3 – ダッシュボードで表示する

目的：システムのアンチマルウェア統計レポートの閲覧を許可すること



実施手順：タスクレポート画面で、ユーザーは「ダッシュボードで表示」ボタンを選択します。

➔ システムのアンチマルウェア統計レポートページへのナビゲーションシステム。

3.11.2 デバイス制御

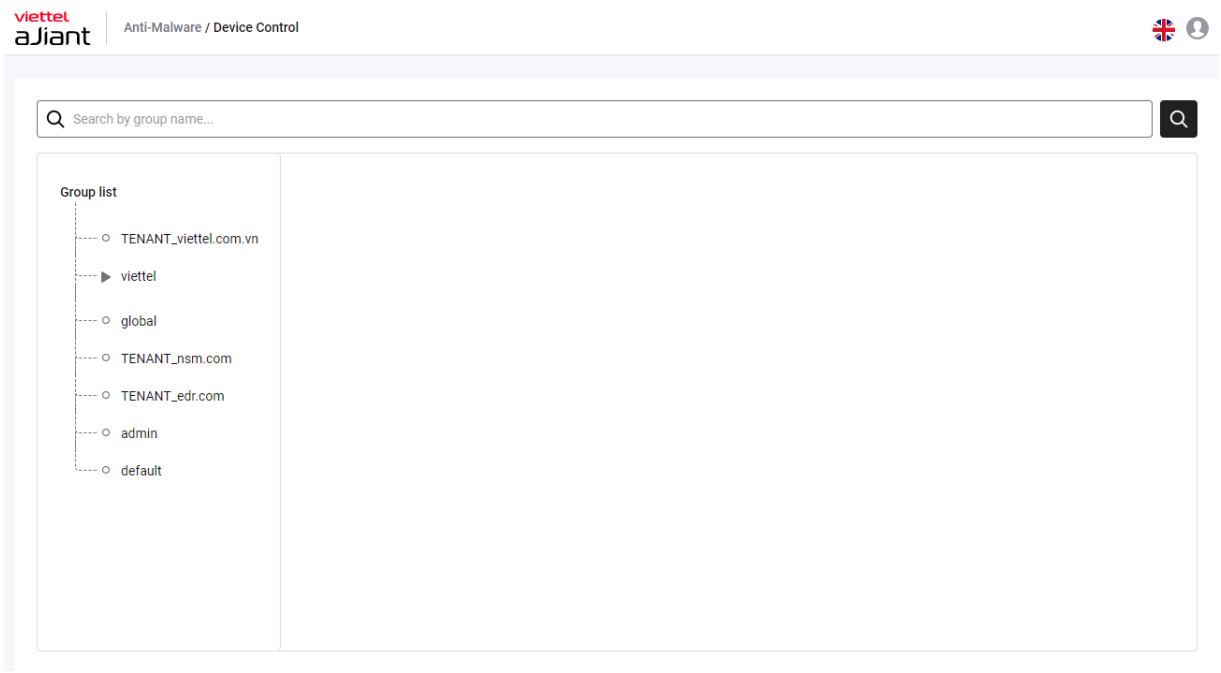
機能：USBドライブ、Bluetoothデバイス、書き込み可能なCDおよびDVDなどの外部機器を通じて、重要なデータの制御および保護を可能にします。

目的：USB機器、CD、DVDおよびその他の周辺機器は非常に便利ですが、組織に対して実際の脅威をもたらすこともあります。したがって、情報の管理とエンドユーザーのコンピュータへのアクセスを行う周辺機器の制御が必要です。

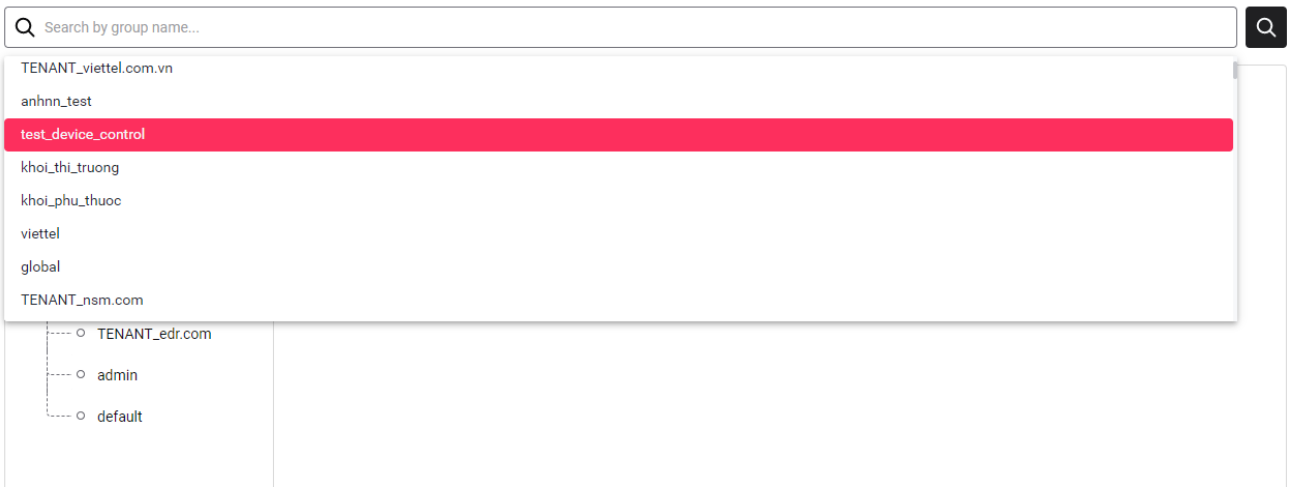
グループを検索する

目的：グループ検索機能は、ユーザーがツリー構造に従ってグループリストを表示できるようにします。

デバイスコントロール機能に入ったときの画面インターフェース：アンチマルウェア／デバイスコントロール



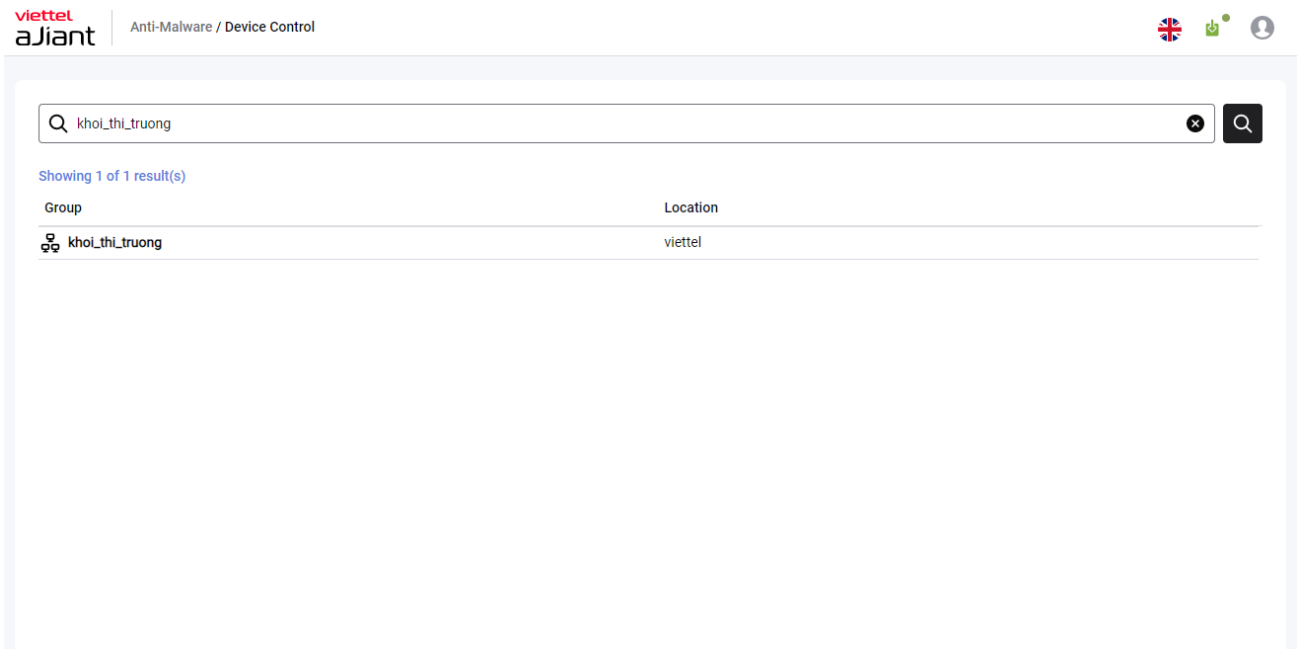
ステップ1：ユーザーは「グループ名で検索」にキーワードを入力します（テキストに基づくキーワードの候補が表示されます）。



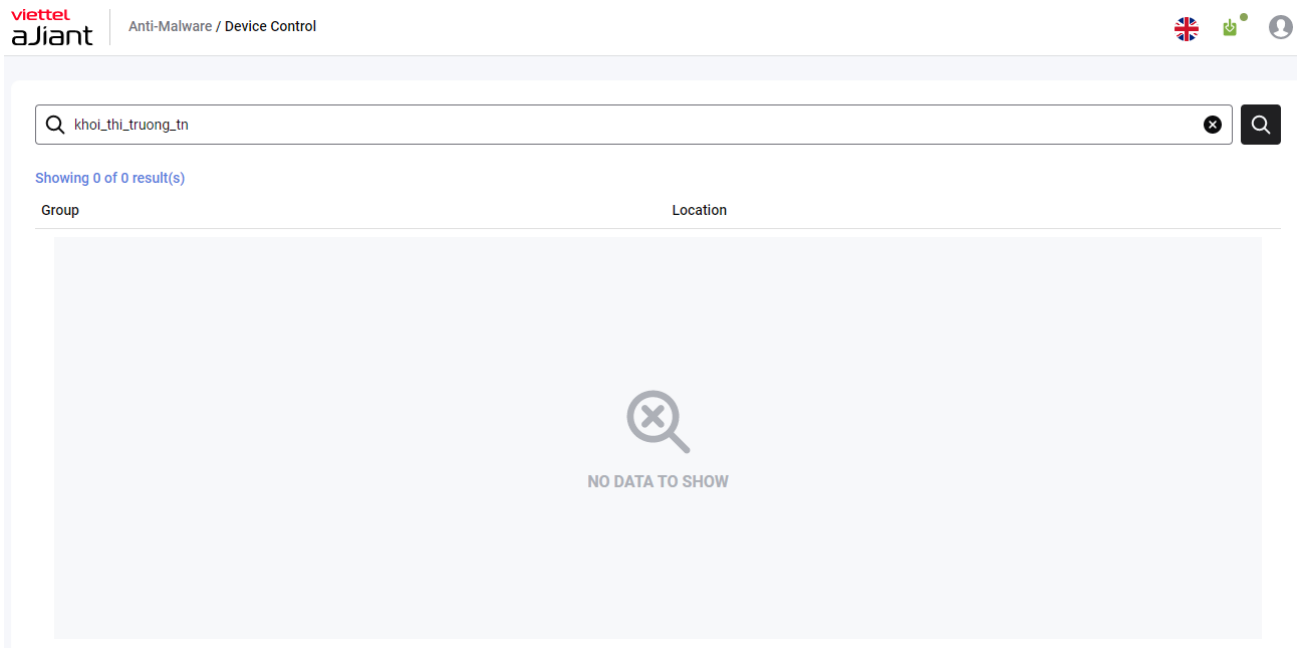
ステップ2：ボタンを選択するか、Enterキーを押して、入力したキーワードで検索操作を確定します。

ステップ3：システムは検索キーワードに基づいてリストを表示します。

結果があれば返されます。



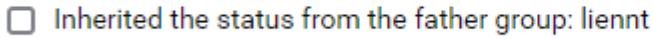
検索しても結果がありません。



各グループのデバイス一覧

希望のグループを選択すると、画面にデバイスタイプの表が表示されます。

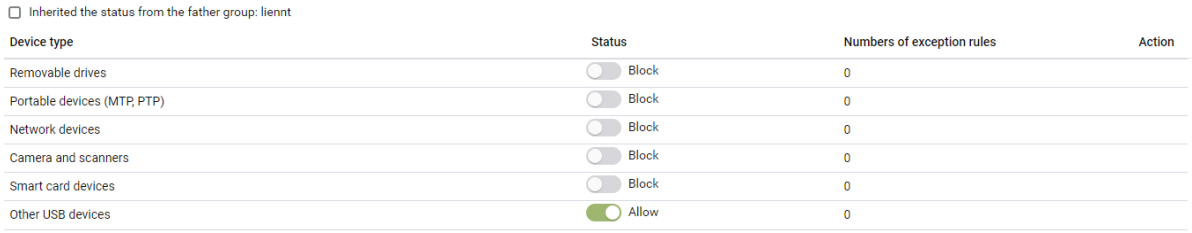
チェックボックスがあります。



下位グループで「継承」を選択すると、最も近い親グループのステータスと例外を継承します。

編集権限はなく、閲覧のみ可能です。一方、「継承」を解除すると、追加・編集・削除の権限が付与されます。

機器一覧表には以下の情報項目が含まれます：



+ デバイスタイプ：デバイス名を固定表示
+ ステータス：許可/ブロック 各グループごとに各デバイスタイプのアクセス権限状態を表示

+ 例外ルールの数：各グループごとに各種デバイスの例外ルールの数を表示する

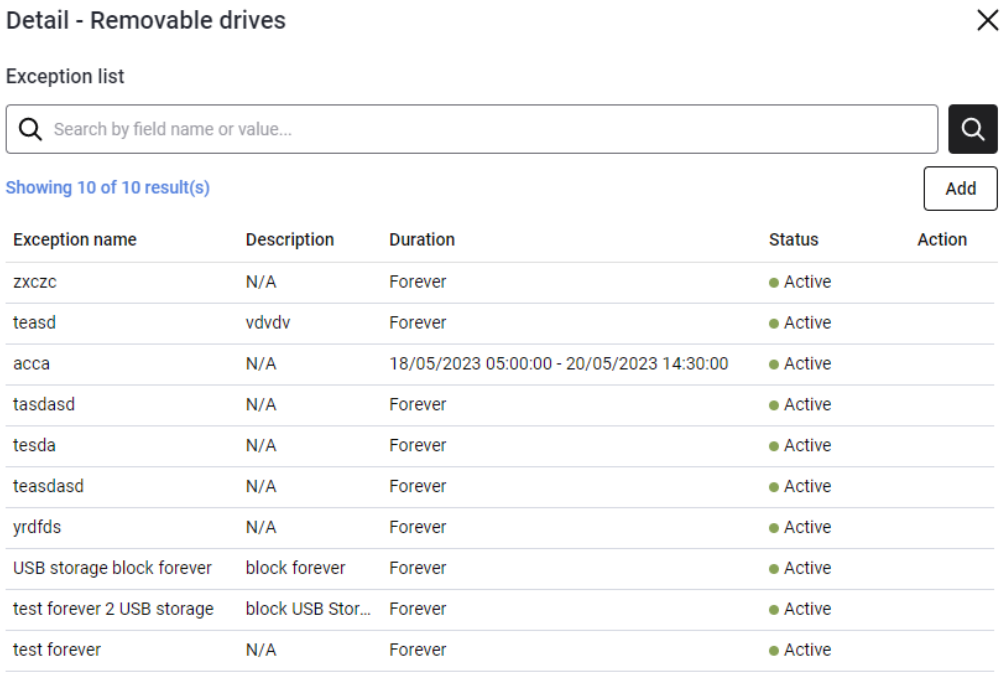
+ 操作：各レコードの「アクション」列にマウスをホバーすると「編集例外」アイコンを表示（アイコンをクリックすると「例外リスト」タブを表示）

例外画面

目的：

ユーザーがグループごとにデバイスの例外リストを閲覧できるようにします。

例外リスト一覧



- 例外規則の数 = 0

>> 「表示するデータがありません」というメッセージを表示する

- 例外ルールの数 != 0

>> デバイスに対応する例外リストを表示する

検索結果がありません。

>>「表示するデータがありません」というメッセージを表示する

検索結果があります

>>名前フィールドの一部または全体と一致する文字列を大文字・小文字を区別せずに入力してください。テキスト入力を開始すると、入力欄の隅にクリアアイコンが表示されます。検索ボタンをクリックするか、Enterキーを押してください。

常に以下の情報項目を含む例外リスト表を表示すること：

1. 例外名 - 例外の名前を表示する

2. 説明 - 適用される例外の情報説明

3. デバイス - デバイス名を表示する

4. 期間 - 例外の期間を表示する

5. ステータス - 例外の状態を表示します。Expired（期限切れ）とActive（有効）が含まれます。

もし例外が現在の時間に対して許容される期間を超えている場合、ステータスを「Expired」と表示します。

+ 例外が現在の時間に対して許容される期間内である場合、ステータスを「アクティブ」と表示します。

6. 行動：

追加ボタン：新しい例外を作成できます。

「n件中x件を表示」

- x: リスト表に表示されているレコードの数をカウントする

- y: 記録されたすべてのレコードの総数をカウントすること

例外リストのテーブルに最大20件のレコード

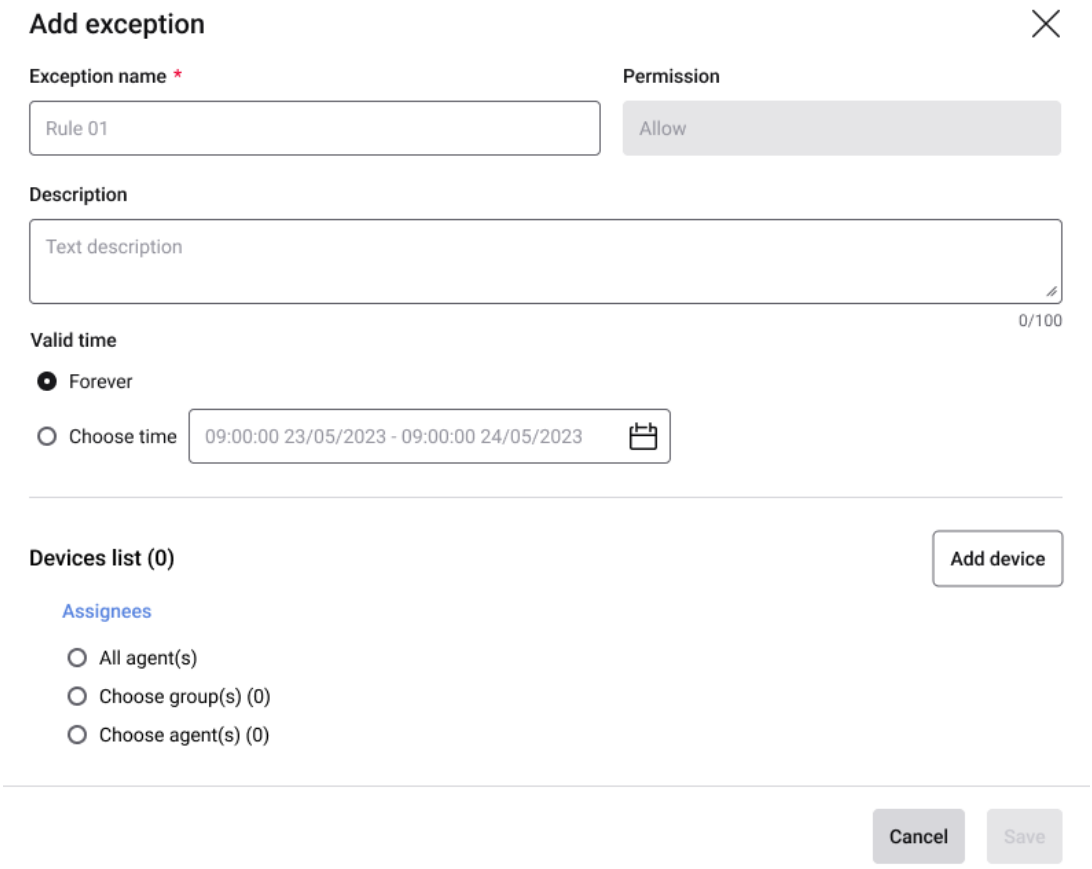
→
データテーブルのページ分割は、レコードが20件を超える場合に行います。ユーザーがページを選択すると、そのページに対応するデータテーブルが表示されます。

→ デフォルトで最初のページを表示する

→ レコードの表示順序は作成・編集日時の新しいものが上に表示され、古いレコードは下に移動します。

例外の追加画面

目的：新たに例外を作成し、各部門が特定のエンドユーザーに対してデバイスへのアクセスを許可する例外を設定できるようにする（個別の業務目的に対応するため）。



- 例外名：例外の名前を入力してください（必須、重複不可）。文字はアルファベット、数字（1, 2, 3, ... 0）を使用し、大文字・小文字は区別しません。500文字以内で入力してください。
- 権限 - 例外のアクセス権限を表示（無効化形式で）

  アクセス許可されたデバイスの種類が「許可」の場合、例外のアクセス許可は「ブロック」となります。
  + アクセス権限が「ブロック」に設定されているデバイスの場合、例外のアクセス権限は「許可」となります。

- 説明：例外の作成に関する情報の説明
- 有効期間 - 例外の有効期限を選択可能にする

  ラジオボタンを設置し、ユーザーに2つの選択肢を提供するために：

  - Forever：永久に許可／ブロックする

  - 絶対時間範囲 → 表示形式は dd/mm/yyyy hh:mm:ss - dd/mm/yyyy hh:mm:ss（デフォルトは現在時刻から未来までで、操作時間が長く例外を追加する際にエラーが発生しないように、5分の差分を設けています）

もし少なくとも1件の例外レコードが存在する場合、以下の情報項目を含む例外一覧表を表示します。

1. 例外名 - 例外の名前を表示する
2. 説明 - 適用される例外の情報説明
3. デバイス - デバイス名を表示する
4. 期間 - 例外の期間を表示する

5. ステータス - 例外の状態を表示します。Expired（期限切れ）とActive（有効）が含まれます。

例外が現在の時間に対して許容される期間を超えている場合、ステータスを「Expired」と表示します。

+ 例外が現在の時間に対して許容される期間内である場合、ステータスを「アクティブ」と表示する。

6. 行動：

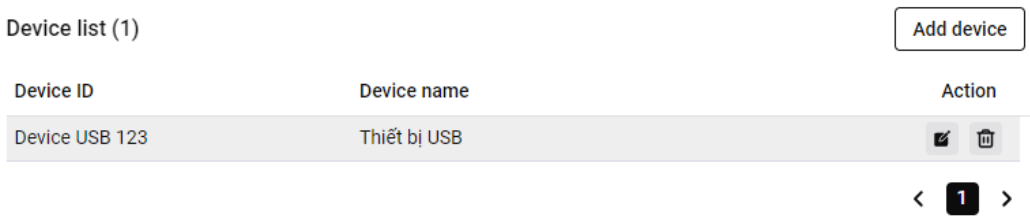
- 追加ボタン：新しい例外を作成できます。

デバイスリスト（デフォルトで少なくとも1件のデバイスレコード）

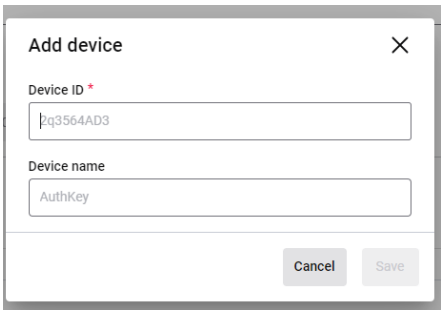
デバイスがない場合：「デバイスを追加」ボタンのみ表示する

デバイスがある場合：「デバイス追加」ボタンを表示し、以下の列を含むテーブルを表示します：デバイスコントロールID、アクション（マウスを乗せると編集アイコンと削除アイコンを表示）。

- ユーザーが閲覧権限のみを持っている場合、追加、編集、削除はできず、閲覧のみ可能です。



「Add　device」ボタンをクリックすると、例外デバイス作成のための情報入力用のポップアップが表示されます。



情報は以下の通りです：

- デバイスID：アルファベット、数字、特殊文字を含み、周辺機器のIDであり、必須項目です。
- デバイス名：デバイスの名前を表示します。空欄にすることも可能です。

デバイスIDが入力されていない場合、保存ボタンは無効になります。

必要な情報をすべて入力すると、保存ボタンが利用可能になります。

「キャンセル」ボタンを押すか、閉じるアイコンをクリックすると、ポップアップ画面が閉じます。

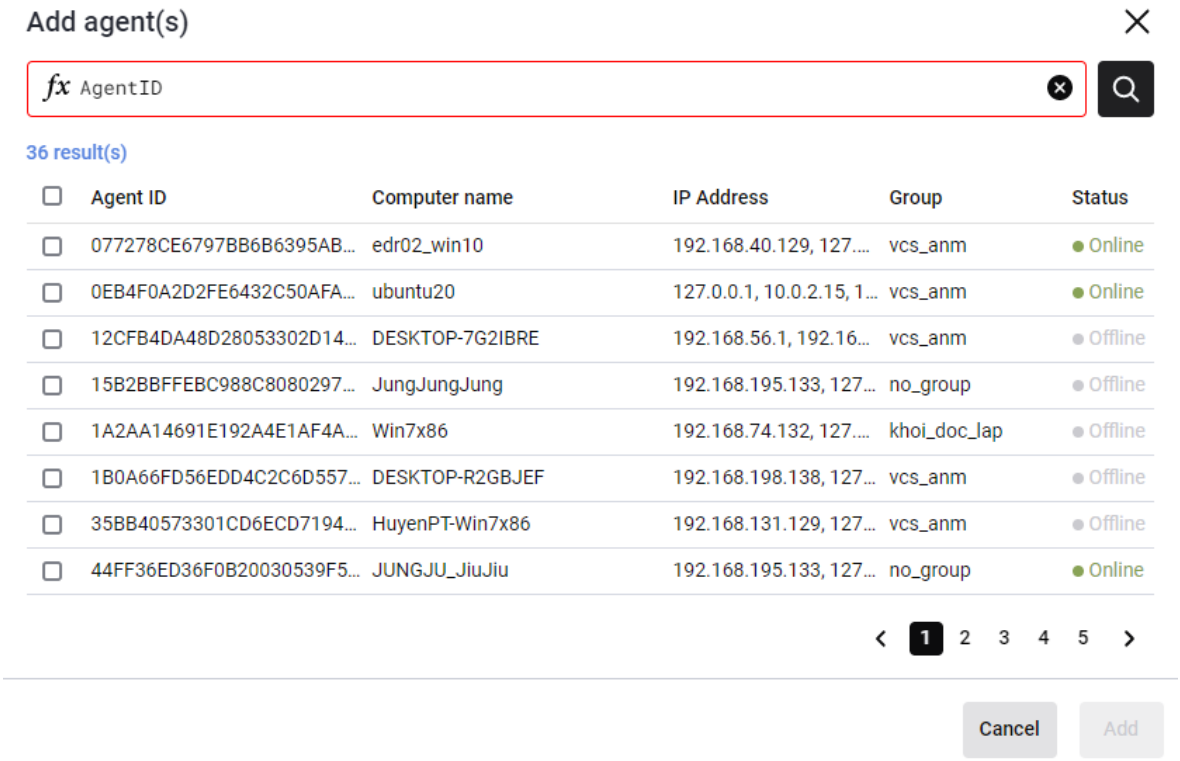
例外追加画面に戻る

Assignessにはユーザーが選択できる3つのオプションがあります（1つだけ選択可能）。

- 「All agent(s)」を選択すると、この例外デバイスに対してすべてのエージェントの許可/ブロックが適用されます。
- 「Choose agent(s) (0)」を選択すると、ユーザーはこの例外デバイスに対して1つまたは複数のエージェントを許可またはブロックすることができます。

この時点で「エージェント追加」ボタンが表示されます。

ボタンをクリックすると対応するポップアップが表示されます（該当グループに属するエージェントのみが「エージェントを追加」部分に表示されます）。



検索：

ユーザーがAgentID、コンピューター名、IPアドレスに基づいてシステム内の提案クエリ情報を検索するためのキーを入力できるようにします。

デフォルトは空欄で、入力必須ではなく、特殊文字の入力を許可します。

>> クエリの内容が正しいフォーマットかどうかを確認するには、クリックしてください：

データ検索を実行し、条件を満たすデータがあるか確認します：nameフィールドの一部または全体と一致する文字列を入力し、大文字・小文字を区別しません。テキスト入力を開始すると、入力欄の隅にクリアアイコンが表示されます。

=> 検索ボタンをクリックするか、エンターキーを押してください

- 常に「Agent ID」「コンピュータ名」「IPアドレス」「グループ」「ステータス」の各情報欄を表示する。

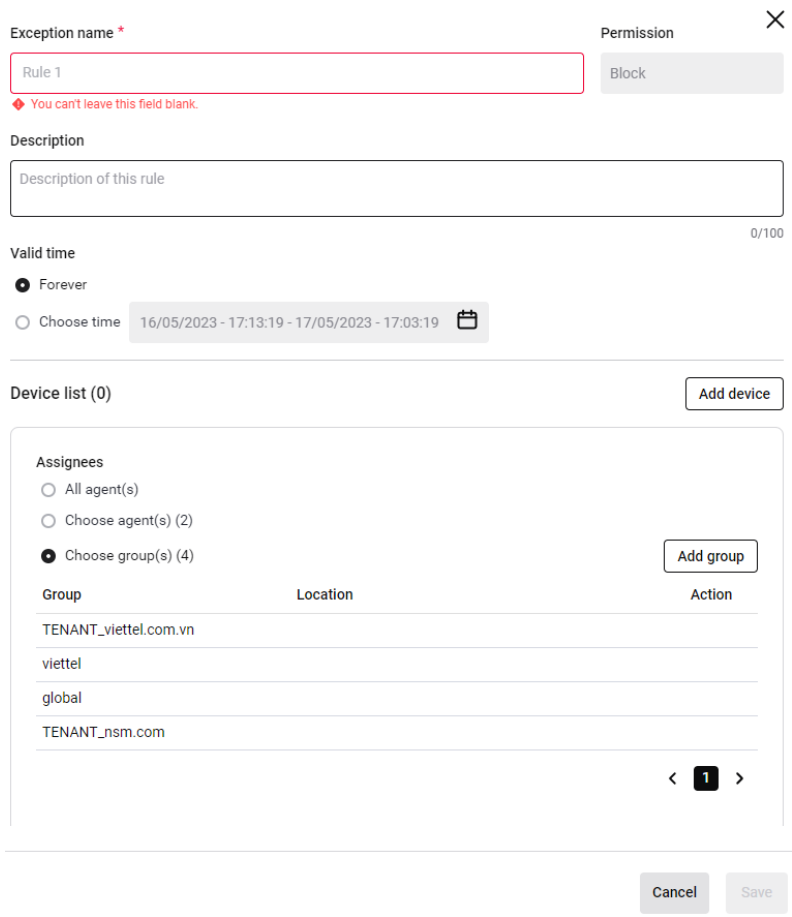
+ 条件を満たすデータがない場合、「データなし」と通知する。

+ 条件を満たすデータがある場合：対応するリストを表示する；

  - チェックボックス：1人または複数のエージェントを選択可能、デフォルトでは未選択。
  - エージェントID：エージェントID情報を表示する
  - コンピュータ名：デバイス（コンピュータ）情報の表示
  - IPアドレス：デバイス（ワークステーション）のIPアドレス情報を表示します。
  - グループ：エージェントのグループ情報を表示する
  - ステータス：エージェントの稼働状況情報を表示：オンライン／オフライン
  - ページネーションがあり、最低8件のレコードがあります。

適切だと思われるエージェントを選択すると、[追加]ボタンが有効になります。
「Add」ボタンをクリックすると、ユーザーは1人または複数のエージェントを「Add Exception」セクションに正常に選択したことになります。

エージェントの追加が完了した後、例外追加画面に戻ります。
以下の項目が表示されます：エージェントID、コンピューター名、IPアドレス、グループ、ステータス
この画面では、アクション列（削除アイコン）を追加表示し、最大5件のレコードを表示し、それ以上はページ分割します。



- 「Choose group(s) (0)」を選択すると、ユーザーはこのデバイスのブロックを許可する1つまたは複数のグループを選択できます。デフォルトでは、ログインしているユーザーが管理するグループのリストが表示されます。

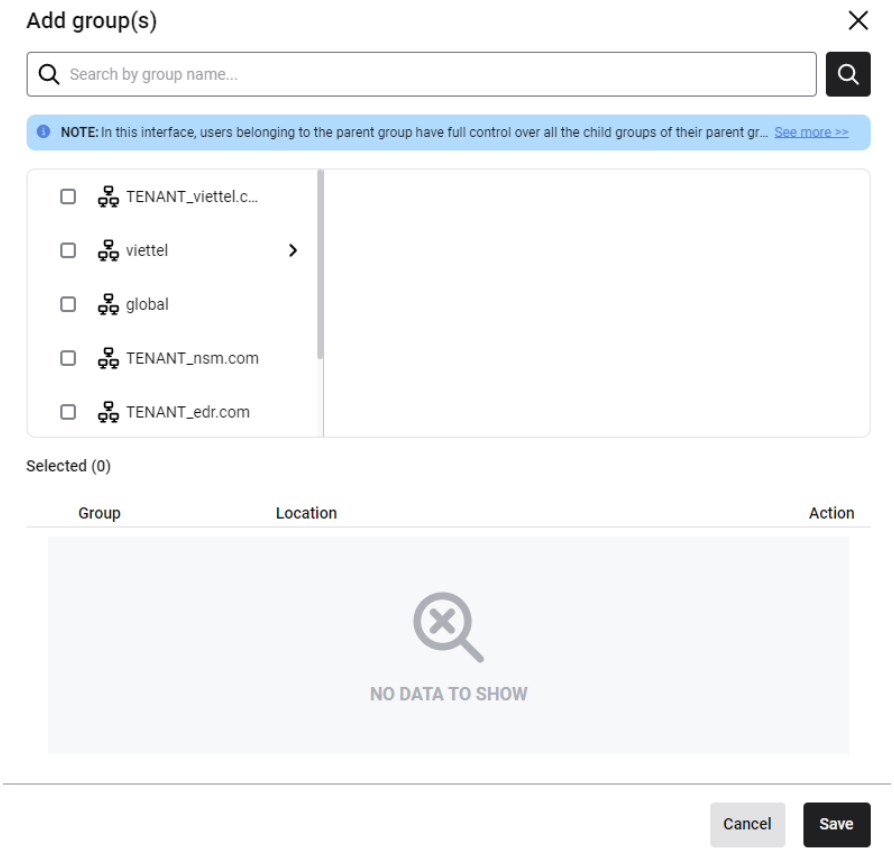
グループ一覧はツリー形式で表示し、グループ一覧内で重複をチェックすること。

検索ボックス：ユーザーがシステム内のグループ名に基づいてグループ情報を検索するためのキーワードを入力できるようにします。

デフォルトは空欄で、入力必須ではありません。前後の空白はトリムされ、特殊文字の入力が許可されています。

検索ボタンをクリックし、システム内にある検索キーに関連するグループ情報を検索してください。

チェックボックス項目：1つまたは複数のグループを選択可能、デフォルトでは未選択。



グループの重複を確認してください。

デフォルトでは、ユーザーがレコードを選択しない場合、結果は表示されません。

もし少なくとも1件のレコードが存在する場合、ページネーションと選択されたエージェント数を表示します。

チェックボックス：エージェントが関連するグループの中で所属している1つまたは複数のグループを選択します。デフォルトでは未選択（チェックなし）です。

列の属性には、グループ、場所、アクションが含まれます。どれを選択すると、それに対応するSelected(0)が表示されます。

グループ：エージェントのグループ情報を表示する

場所：グループの関連ツリーの位置を表示する；

例：root/ TT GPSP/EDR

操作：（削除）そのグループを選択したくない場合

もしグループを選択しない場合 >> 「データなし」を返します。

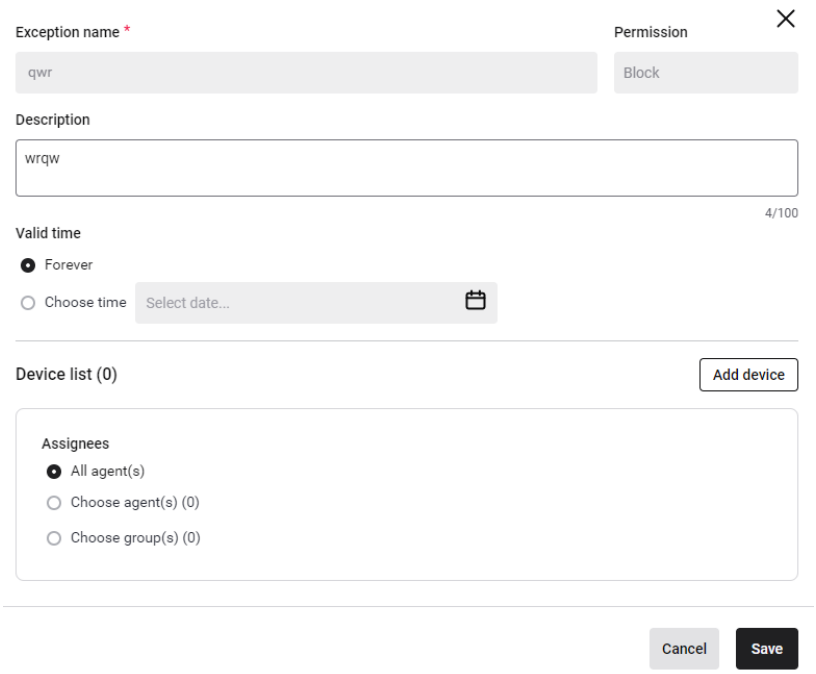
適切なグループを選択した後、ユーザーは「保存」ボタンをクリックして成功すると、例外追加画面に戻ります。この時、ポータルは「例外が正常に追加されました」というメッセージを表示します。

グループを選択したくない場合は、「キャンセル」をクリックして、例外追加画面に戻ってください。

必要な情報がAdd Exceptionに入力されたら、ユーザーは「保存」を選択してこの例外のすべての情報を保存します。>> そのグループの例外リスト画面に戻ります。

例外リスト画面では、アクション部分に編集アイコンと削除アイコンがあります。

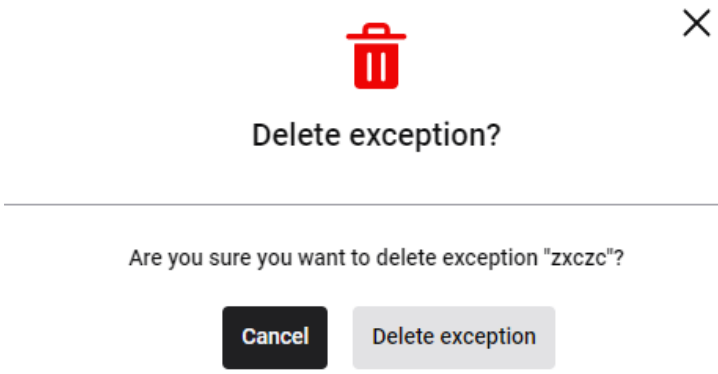
編集アイコンを選択すると、同様の画面が表示されます。



Exception nameとPermissionのみがロックされており、変更できません。それ以外はユーザーが自由に変更可能です。

編集後、「保存」をクリックして情報を保存します。この時、ポータルに「例外の編集が成功しました」という通知が表示されます。

アイコンを削除する場合、ポップアップを表示します。



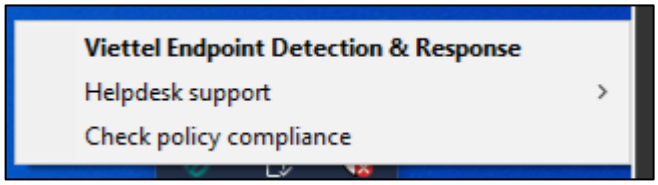
「Delete exception」ボタンを選択すると、ユーザーはこの例外に同意したことになります。この時、ポータルは「例外を正常に削除しました」という通知を表示します。

キャンセルを選択すると、デバイスリスト画面に戻ります。

3.12 メイン

エージェントがインストールされている端末の情報セキュリティ状況を迅速に確認できる機能。

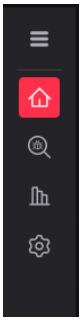
タスクバーでアイコンを探し、右クリックして「Viettel Endpoint Detection & Response」を選択してください。



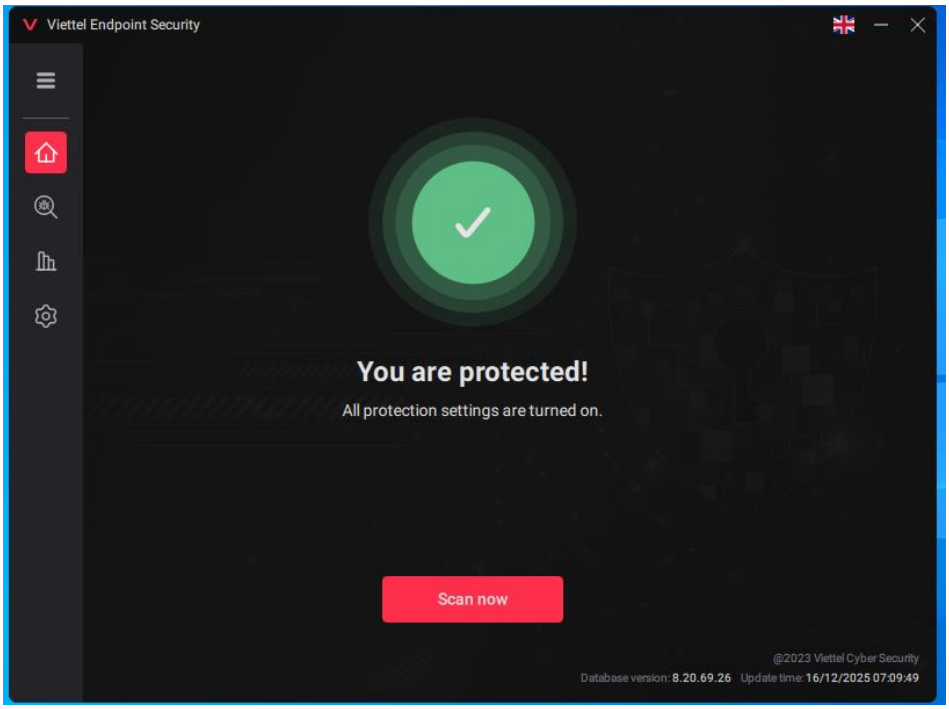
システムは以下の情報を表示します：

+ 英語とベトナム語の2言語で表示されます。

+ サイドバーには、ホーム、ウイルススキャン、レポート、設定といった主要機能のアイコンが表示されます。サイドバーは折りたたみや展開が可能です。



+ マルウェアが存在せず、リアルタイム保護が有効になっているか、すべてのマルウェアが処理済みの場合：



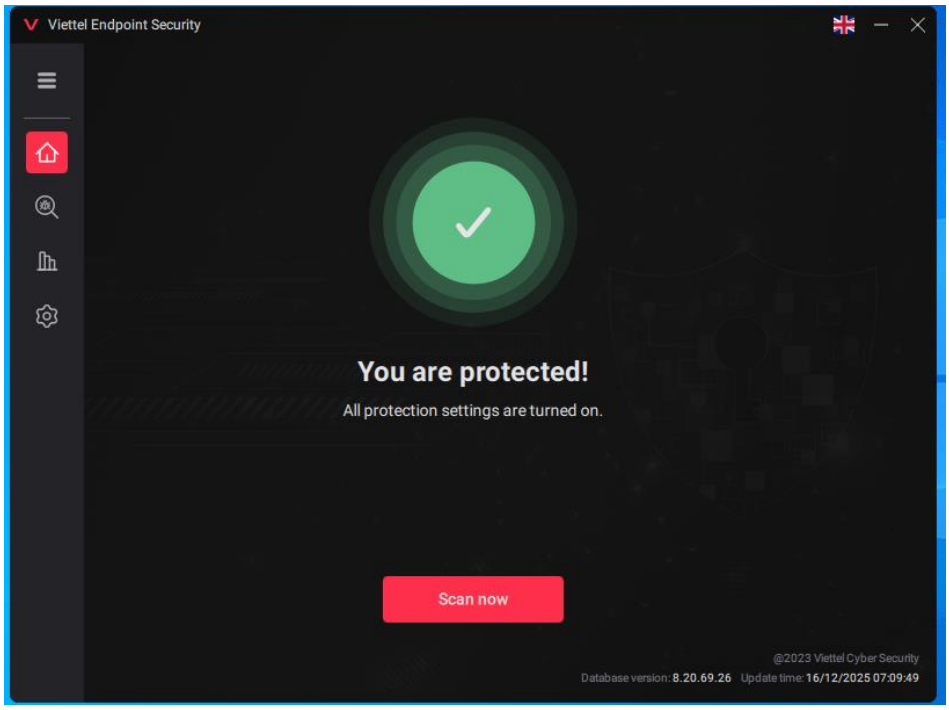
+ リアルタイム保護が有効になっていないため、少なくとも1つのマルウェアが検出された場合

バージョン情報：ユーザーの端末にインストールされているエージェントのバージョン情報、更新日時、および製品サポート情報が画面の隅に表示されます。

3.13 保護

目的：ユーザーが自らシステムを操作して、コンピュータ上のマルウェアをスキャンおよび処理できるようにすること。

スキャンの種類は1つのみ許可します：クイックスキャン、フルスキャン、カスタムスキャン（クイックスキャン、全体スキャン、フォルダスキャン）



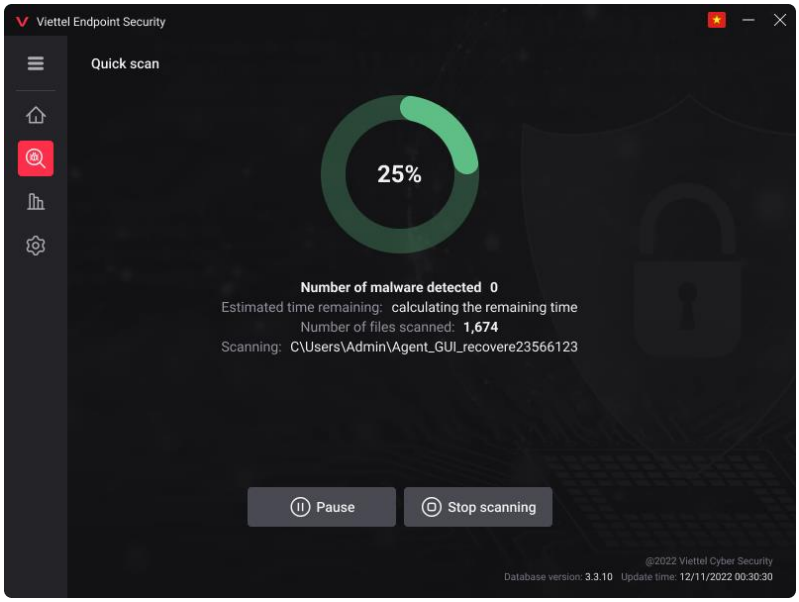
サポートされているスキャン方式には以下が含まれます。

+ エージェントのインターフェースからスキャン方法を選択する。

- クイックスキャン：事前に定義された複数のフォルダーを対象にスキャンを行います。これらのフォルダーはマルウェアが頻繁に発生する場所です。選択したフォルダーに含まれるすべてのファイルおよびサブフォルダーをスキャンします。
- フルスキャン：ユーザーのコンピュータ内のすべてのファイルとフォルダをスキャンする。
- カスタムスキャン：コンテキストスキャンと同様に、この形式を選択すると、エージェントはファイルエクスプローラーを表示し、ユーザーがスキャンするファイルまたはフォルダーを1つ選択できるようにします。

+ ファイルエクスプローラーから直接選択し、複数のファイルやフォルダーを選択可能で、右クリックしてスキャン（コンテキストスキャン）を選択できる。

適切な方法を選択した後、システムはマルウェアのスキャンと処理を実行します。



+ スキャン全体の進行状況をパーセント表示する

+ 検出されたマルウェアの数を表示する

+ スキャン終了までの推定残り時間を表示する

+ スキャン済みファイル数を表示する

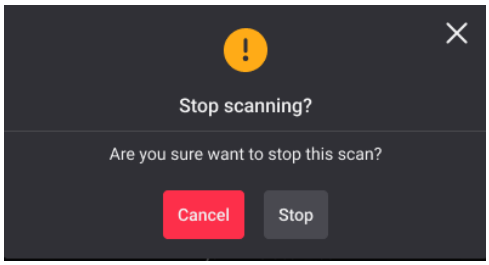
+ スキャン中のファイルパスを表示する

スキャン中の操作を以下のようにサポートします：

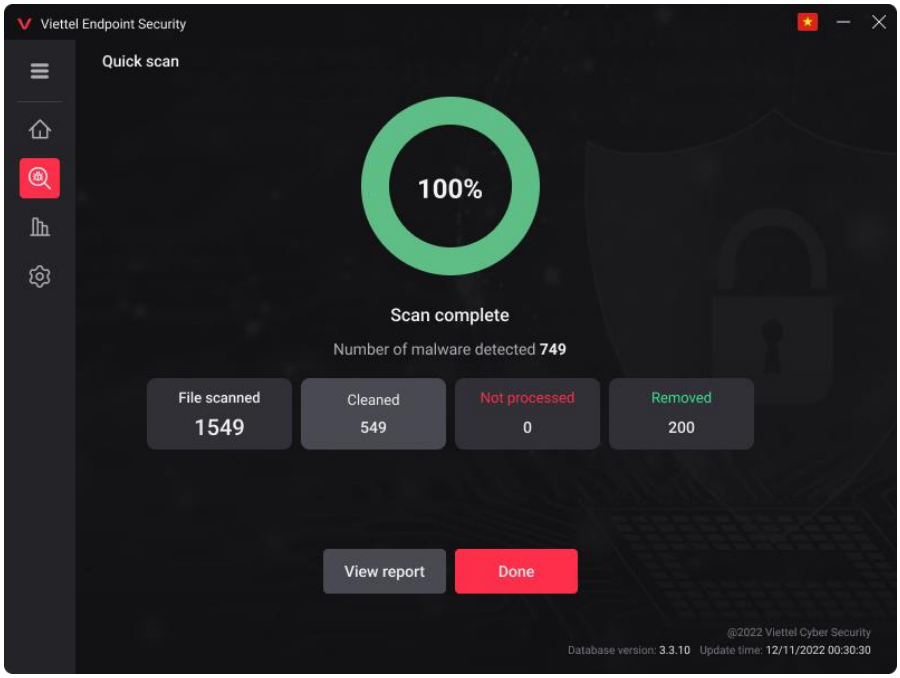
スキャンプロセスの終了を許可する;

スキャンプロセスの一時停止を許可する;

「一時停止」ボタンをクリックすると、同時にボタンが「再開」に切り替わり、この時点でスキャンを続行するために選択できるようになります。



スキャンが完了したら、スキャン結果を表示します。



+ スキャン済みファイル数：スキャンされたファイルの数を表示します

+ クリーン済み：駆除されたファイルの総数を表示します

+ 未処理: 未処理のファイル総数を表示

+ 削除済み：削除されたファイルの総数を表示

これらのボタンは、関連するレポートの該当部分に直接リンクすることができます。

またはボタンをクリックして、スキャン結果の全体レポートを表示できます。

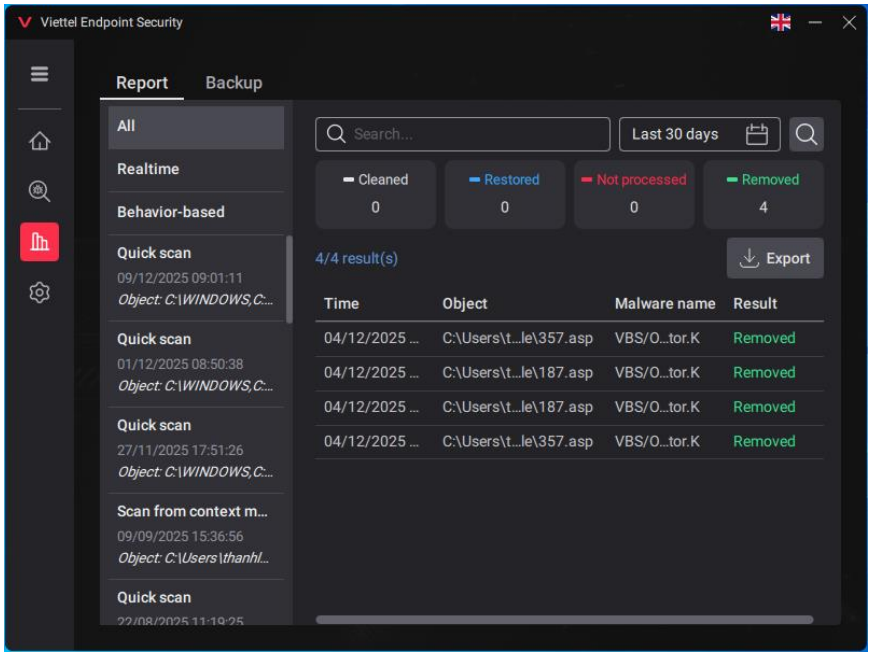
「完了」をクリックして、Protectionのメイン画面に戻ります。

スキャンの過程で、エージェントが直接削除できないdll形式のマルウェアが読み込まれていることを検出した場合、エージェントはスキャンを完了するために再起動を要求するポップアップを表示します。

3.14 報告書

目的：デバイスのマルウェア検出レポートを集計し、リストに記載されたマルウェアの総数を表示すること。

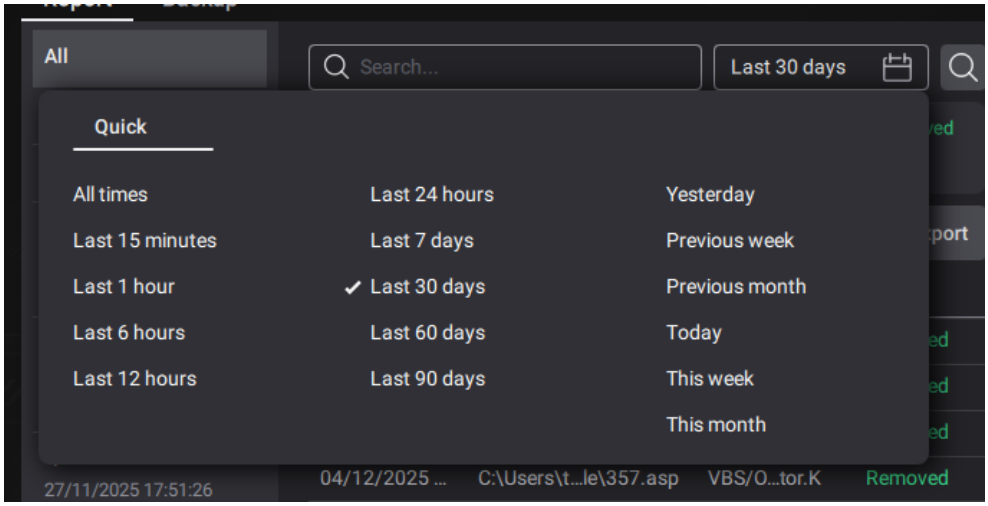
a. タブレポート（報告書）



- 検索条件に合致する結果がない場合は、「データがありません」という状態を表示します。

- ユーザーが「すべて」を選択した場合：
+ マルウェア一覧：検出されたすべてのマルウェアを表示します。
- ユーザーが手動スキャンを選択した場合：
+ スキャン回数リスト：過去30日間のスキャン履歴リストを表示します。
+ デフォルト：直近のスキャンを選択し、対応するマルウェアリストをユーザーに表示する。
+ マルウェアリスト：ユーザーが選択したスキャン回で検出されたすべてのマルウェアを表示します。
- ユーザーがリアルタイムを選択した場合：
+ マルウェア一覧：リアルタイムで検出されたすべてのマルウェアを表示します

  - 時間による検索：現在までの情報セキュリティ状況を監視するための期間を調整可能で、デフォルトは前日からの期間となっています。



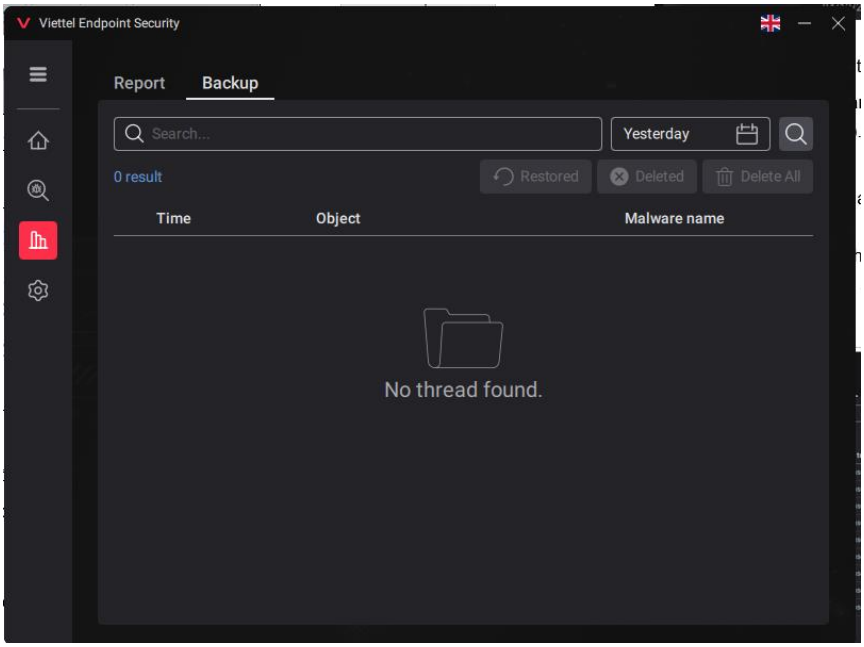
  - マルウェアの検出結果による検索

レポートの項目では、ユーザーが選択した項目に基づいて、全ての報告書を端末にダウンロードすることができます。

b. タブバックアップ

目的：バックアップ中のマルウェアファイル一覧の情報提供

ユーザーは検索したい時間を選択してから検索ボタンをクリックすると、検索条件に基づいたリストが表示されます。



処理される前のマルウェアを含むファイルはすべて、元の状態で「Backup」フォルダに保存されます。「Backup」フォルダの整理やファイルの復元を行うために、本製品は以下の機能を提供します。

複数または単一のファイルを選択して復元することを許可します。

バックアップフォルダから1つまたは複数のファイルを選択して削除することを許可します。

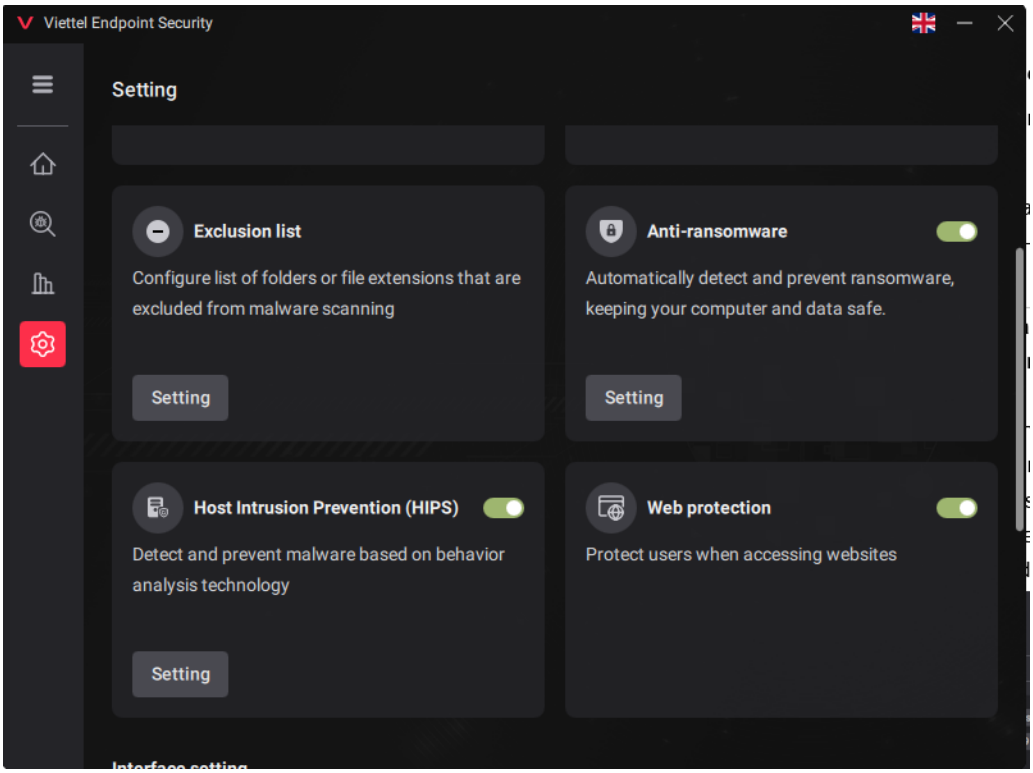
バックアップフォルダ内のすべての既存ファイルを一括で迅速に削除することを許可する。

- 検索条件に合致する結果がない場合は、「該当する結果が見つかりません」と表示してください。

3.15 設定

目的：各エージェント端末での設定構成

設定ページ内のすべての内容を検索キーワードで検索できるようにする。



a. 保護設定：ポータル上と各エージェントごとに2つのポリシー設定箇所（自己防衛およびリアルタイム保護）があるため。

- 自己防衛：自己防衛のオン・オフを許可します。→ エージェントのリソースを保護し、外部の不正な干渉から守ります。- 未だ完全に更新されていません。

- リアルタイム保護：コンピュータを包括的に保護し、マルウェアがコンピュータ上に現れた瞬間に自動で検出・駆除します（デバイスのオン/オフ）。
- 除外リスト：除外フォルダーの選択を許可（リアルタイム保護によるスキャン対象外）；除外フォルダーの新規追加／編集

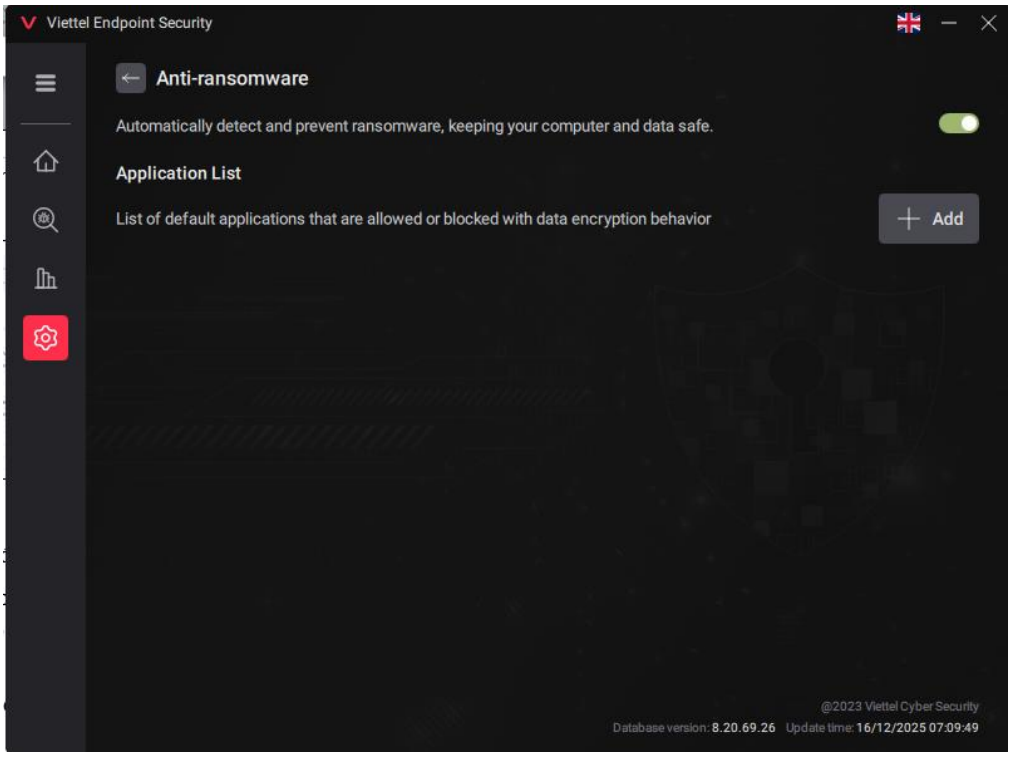
- 拡張機能：リアルタイム保護によってスキャンされない除外対象の拡張子（ファイルタイプ）を新規追加および編集できるようにする。

b. インターフェース設定

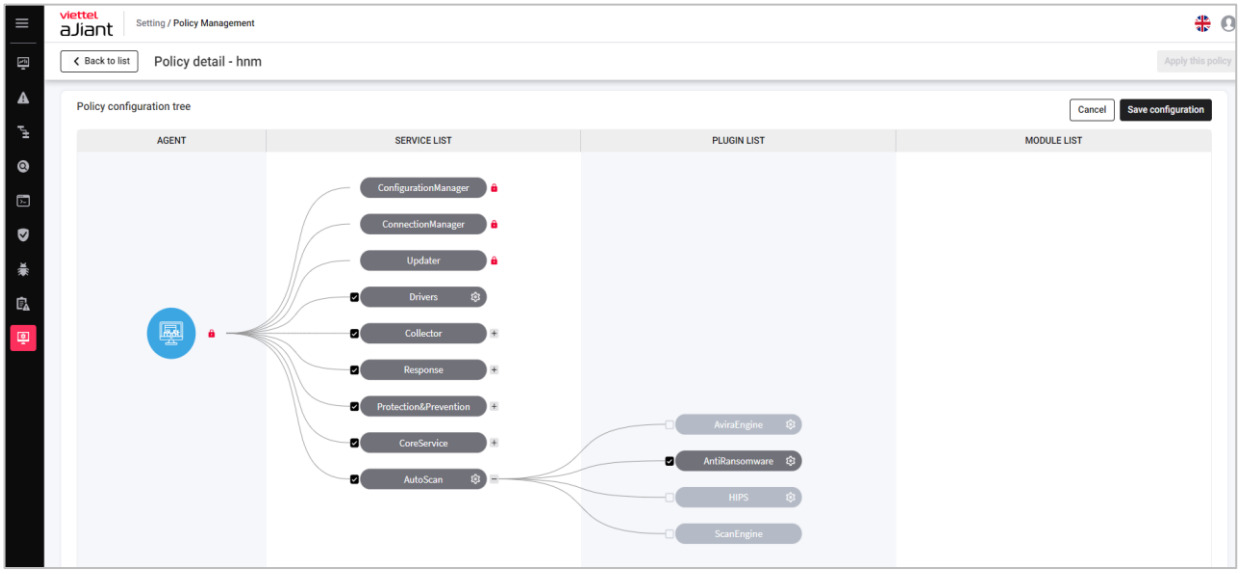
- 通知のオン・オフを許可 → システムからスキャン指示があった場合やマルウェアを検出した際に、デバイス画面に通知を表示します。
- 言語: 英語/ベトナム語の選択を許可する

c. アンチランサムウェア（ランサムウェア対策）

- ユーザーがランサムウェア保護モードをオンまたはオフに切り替えられるようにします。システムは自動的にランサムウェアを検出し、コンピュータを保護します。



注意：機能を使用するには、ポータルでポリシー「アンチランサムウェア」を有効にする必要があります。



- アプリケーションリスト：ユーザーが選択したアプリケーションに対して、これらのアプリがデータを暗号化するマルウェアの疑いのある動作を行うことを許可します。

d. バックアップ設定（Cài đặt sao lưu）：ユーザーがバックアップファイルの保存情報を設定できるようサポートします。

- バックアップサイズの制限を表示するオプションを選択し、同時にバックアップファイルの保存サイズ制限を入力できるようにします。

  （最大5120MBまで設定可能→
  5GBの閾値に達した際の通知：バックアップファイルのサイズが上限に達しました！システムはバックアップから最も古いファイルを削除します）

  最大保存容量を超えないように、最大保存容量に達した際には保存領域内の最も古いファイルが自動的に削除されます。

3.16 VESAutoScan

コマンドは、マルウェアのスキャン管理、レポートの閲覧、および検出されたマルウェアのバックアップの操作を可能にします。

サポートされている機能を一覧表示するコマンドを実行してください。

```
$ VESAutoScan -h
使い方: VESAutoScan <コマンド>

スキャンおよび保護サービスの管理

コマンド:
  scan                    スキャンセッションの管理
  |- start                スキャンセッションを開始
  |  |- <files> ...       スキャンするファイルパス
  |- stop                 スキャンセッションを停止
  |  |- <id>              停止するスキャンセッションのID
  |- show                 スキャンセッションの詳細表示
  |  |- <id>              照会するスキャンセッションのID
  |- list                 実行中のスキャンセッション一覧表示

  report                  スキャンレポートの管理
  |- list                 すべてのスキャンレポート一覧表示
  |  |- <type>            レポートの種類（realtime、manual、all）
  |- show                 スキャンレポートの詳細表示
  |  |- <id>              表示するレポートID（realtimeまたはレポート番号）
  |- search               スキャンレポート内のファイル検索
  |  |- <str>             ファイルパス内の検索文字列

  backup                  バックアップファイルの管理
  |- restore              バックアップファイルの復元
  |  |- <id>              復元するファイルのID
  |  |- <output-path>     復元ファイルの出力パス
  |- list                 すべてのバックアップファイル一覧表示
  |- search               バックアップファイルの検索
  |  |- <str>             ファイル名内の検索文字列

  show                    スキャンサービス情報の表示
  |- version              バージョン表示
  |- database-version     データベースバージョン表示

フラグ:
  -h, --help     コンテキストに応じたヘルプを表示

詳細は "VESAutoScan <コマンド> --help" を実行してください。
```

3.16.1 サブコマンドスキャン

スキャンセッションの管理、ユーザーが手動でスキャンセッションを作成できるようにし、この方法で作成されたスキャンセッションを管理することを可能にします。

a. スキャンセッションを開始する

ユーザーはマルウェアスキャンを行う場所を指定できます。複数の場所を指定することも可能です。

```
$ VESAutoScan スキャン開始 /home/ /usr/
パス: /home
パス: /usr
スキャン開始成功、ID: 1
スキャンの詳細を表示するには、コマンド `VESAutoScan scan show 1` を使用してください。
```

b. スキャンセッションを1回停止する

ユーザーがスキャンセッションの停止を指定する

```
$ VESAutoScan スキャン停止 1
停止成功
```

c. 1つのスキャンセッションの状態を表示する

ユーザーが表示するスキャンセッションを指定します。

```
$ VESAutoScan スキャン表示 1
+----+---------+----------+--------------+------------------+-----------------+
| ID | 状態    | 進行状況 | スキャン済みファイル数 | 検出されたマルウェア数 | クリーン済みマルウェア数 |
+----+---------+----------+--------------+------------------+-----------------+
|  1 | 停止中  | 9.00%    |        30231 |                0 |               0 |
+----+---------+----------+--------------+------------------+-----------------+
```

d. コマンドラインを使用して作成された現在実行中のスキャンセッションを一覧表示してください。

スキャン中のセッションとスキャン位置を表示する

```
$ VESAutoScan スキャンリスト
+---------+------------+
| スキャンID | ロケーション |
+---------+------------+
|       1 | /usr,/home |
+---------+------------+
```

3.16.2 サブコマンドレポート

a. スキャン履歴と情報を一覧表示してください。

ユーザーはレポートの種類を指定できます。「realtime」はリアルタイムのマルウェアスキャンレポート、「manual」は手動スキャンのレポート、「all」はすべてのレポートを表示するための指定です。

```
$ VESAutoScan レポート一覧 リアルタイム
+-----------------------------+
| リアルタイムスキャンレポート |
+-----------+-----------------+
| レポートID | 検出されたマルウェア数 |
+-----------+-----------------+
| realtime  |               2 |
+-----------+-----------------+
```

```
$ VESAutoScan レポート一覧（手動スキャン）
+-------------------------------------------------------------------------------------------------------
-------+
| 手動スキャンレポート
|
+-----------+--------------------------+------------+-------+--------------+------------------+---
-------+
| レポートID | タイムスタンプ              | 場所        | ファイル数 | スキャン済みファイル数 | 検出されたマルウェア数 |
状態      |
+-----------+--------------------------+------------+-------+--------------+------------------+---
-------+
|         1 | 2025-07-10T17:46:32+07:00 | /usr,/home | 30231 | 312837       |                0 | 停
止中    |
|         2 | 2025-07-10T17:53:01+07:00 | /usr,/home | 31795 | 312838       |                0 | ス
キャン中 |
+-----------+--------------------------+------------+-------+--------------+------------------+---
-------+
```

```
$ VESAutoScan レポート一覧
+-----------------------------+
| リアルタイムスキャンレポート |
+-----------+-----------------+
| レポートID | 検出されたマルウェア数 |
+-----------+-----------------+
| realtime  |               2 |
+-----------+-----------------+

+-------------------------------------------------------------------------------------------------------------
-------+
| 手動スキャンレポート
|
+-----------+---------------------------+------------+-------+--------------+------------------+---
-------+
| レポートID | タイムスタンプ              | 場所        | ファイル数 | スキャン済みファイル数 | 検出されたマルウェア数 |
状態      |
+-----------+---------------------------+------------+-------+--------------+------------------+---
-------+
|         1 | 2025-07-10T17:46:32+07:00 | /usr,/home | 30231 | 312837       |                0 | 停
止中    |
|         2 | 2025-07-10T17:53:01+07:00 | /usr,/home | 56013 | 312838       |                0 | ス
キャン中 |
+-----------+---------------------------+------------+-------+--------------+------------------+---
-------+
```

b. レポートの詳細情報を表示する

ユーザーは表示するレポートのIDを指定できます。「realtime」を指定すると、リアルタイムでのマルウェアスキャン機能の詳細レポートを表示できます。

```
$ VESAutoScan レポート リアルタイム表示
+---------------+-----------------------+-------------+
| ファイルパス   | マルウェア名            | ステータス   |
+---------------+-----------------------+-------------+
| /adware+virus | ADWARE/Patched.Ren.Gen | 削除済み     |
+---------------+-----------------------+-------------+
|               | 合計                   | 1           |
+---------------+-----------------------+-------------+
```

```
$ VESAutoScan レポート表示 3
+-----------+--------------------------+----------+------+-------------+-----------------+------
----+
| レポートID | タイムスタンプ              | 場所      | ファイル数 | スキャン済みファイル数 | 検出されたマルウェア数 | 状態
|
+-----------+--------------------------+----------+------+-------------+-----------------+------
----+
|         3 | 2025-07-10T18:13:19+07:00 | /home    |  496 | 153052       |                1 | スキャン
中 |
+-----------+--------------------------+----------+------+-------------+-----------------+------
----+
+--------------------+------------------------+-------------+
| ファイルパス        | マルウェア名            | 状態        |
+--------------------+------------------------+-------------+
| /home/adware+virus | ADWARE/Patched.Ren.Gen | 削除済み    |
+--------------------+------------------------+-------------+
|                    | 合計                   | 1           |
+--------------------+------------------------+-------------+
```

c. 過去に検出されたファイルまたはマルウェアを検索する

ユーザーは検索するファイルのパスの一部を指定できます。

```
$ VESAutoScan レポート検索ホーム
+-----------------------------------------------------------+
| レポートID: 3                                              |
+--------------------+------------------------+-------------+
| ファイルパス        | マルウェア名            | 状態        |
+--------------------+------------------------+-------------+
| /home/adware+virus | ADWARE/Patched.Ren.Gen | 削除済み    |
+--------------------+------------------------+-------------+
|                    | 合計                   | 1           |
+--------------------+------------------------+-------------+
```

3.16.3 サブコマンドバックアップ

a. 検出され、復元可能なファイルを一覧表示してください。

```
$ VESAutoScan バックアップリスト
+---------+--------------------+
| ファイルID | ファイルパス         |
+---------+--------------------+
|       1 | /adware+virus      |
|       2 | /home/adware+virus |
+---------+--------------------+
|   合計   | 2                  |
+---------+--------------------+
```

b. 検出され、復元可能なファイルを検索する

ユーザーは検索するファイルへのパスの一部を指定します。

```
$ VESAutoScan バックアップ検索 ホーム
+---------+--------------------+
| ファイルID | ファイルパス          |
+---------+--------------------+
|       2 | /home/adware+virus |
+---------+--------------------+
|   合計   | 1                  |
+---------+--------------------+
```

c. ファイルを1つ復元する

ユーザーはバックアップするファイルのIDと、復元後のファイル名を指定できます。ファイル名は絶対パスまたは相対パスで指定可能です。

復元されたファイルはzip形式で圧縮されており、パスワードは「infected」に設定されています。

```
$ VESAutoScan バックアップ復元 2 /home/linux/malware
アドウェア＋ウイルスを /home/linux/malware.zip に復元中
パスワード「infected」で /home/linux/malware.zip への復元に成功しました
```

3.16.4 サブコマンド show

a. マルウェアスキャン管理サービスのバージョンを表示する

```
$ VESAutoScan バージョン表示
バージョン: 3.3.0.545.e8d14fe
ビルド: 2025-06-09T10:30:04+0000
```

b. データベースのバージョンを表示する

```
$ VESAutoScan show database-version
データベースバージョン: 8.20.57.224
更新日時: 2025年10月7日 17時55分30秒
```