NetWitness® Platform

バージョン12.4.0.0

リリース ノート

NETWITNESS
Platform

連絡先

NetWitnessコミュニティ(https://community.netwitness.com) では、よくある質問への回答や、既知の問題の解決方法を含むナレッジベースを公開しています。また、製品ドキュメント、コミュニティ ディスカッション、ケース管理なども公開されています。

商標

RSAおよびその他の商標は、RSA Security LLCまたはその関連会社(「RSA」) の商標または登録商標です。RSAの商標のリストについては、https://www.rsa.com/en-us/company/rsa-trademarksを参照してください。その他の商標は、それぞれの所有者の商標または登録商標です。

使用許諾契約

本ソフトウェアと関連ドキュメントは、RSA Security LLCまたはその関連会社が著作権を保有しており、使用許諾契約に従って提供されます。本ソフトウェアと関連ドキュメントの使用と複製は、使用許諾契約の条項に従い、上記の著作権を侵害しない場合のみ許諾されます。本ソフトウェアと関連ドキュメント、およびその複製物を他人に提供することは一切認められません。

本使用許諾契約によって、本ソフトウェアと関連ドキュメントの所有権およびその他の知的財産権が譲渡されることはありません。本ソフトウェアと関連ドキュメントを不正に使用または複製した場合、民事および刑事上の責任が課せられる可能性があります。

本ソフトウェアは予告なく変更されることがありますので、あらかじめご承知おきください。

サード パーティ ライセンス

本製品にはRSA以外のサード パーティによって開発されたソフトウェアが含まれます。本製品内のサード パーティ製ソフトウェアに適用される使用許諾契約の内容については、NetWitnessコミュニティの製品ドキュメント ページで確認できます。本製品を使用することにより、本製品のユーザーは、これらの使用許諾契約の条項に同意したものとみなされます。

暗号技術に関する注意

本製品には、暗号技術が組み込まれています。これらの暗号技術の使用、輸入、輸出は、各国の法律で禁止または制限されています。本製品を使用、輸入、輸出する場合は、各国における使用または輸出入に関する法律に従わなければなりません。

ディストリビューション

本文書に記載される、RSA Security LLCまたはその関連会社(「RSA」) のいかなるソフトウェアの使用、複製、配布にも、適切なソフトウェア ライセンスが必要です。

RSAは、この資料に記載される情報が、発行日時点で正確であるとみなしています。この情報は予告なく変更されることがあります。

この資料に記載される情報は、「現状有姿」の条件で提供されています。RSAは、この資料に記載される情報に関する、どのような内容についても表明保証条項を設けず、特に、商品性や特定の目的への適応性に対する黙示的保証はいたしません。

その他

この製品、このソフトウェア、関連ドキュメント、およびコンテンツには、このドキュメントの発行日の時点で有効なNetWitnessの標準利用規約が適用されます。利用規約は https://www.netwitness.com/standard-form-agreements/でご確認いただけます。

2024年3月

目次

12.4.0.0リリースの新機能

NetWitness 12.4.0.0リリース ノートには、新機能、機能拡張、セキュリティ修正、アップグレード パス、修正された問題、既知の問題、サポートが終了した機能、ビルド番号、セルフヘルプ リソースが記載されています。

機能拡張

次のセクションでは、機能分野ごとに拡張内容を詳細に説明します。

- アップグレード
- SASE機能
- Investigate
- Respond
- 対応アクション
- Insight
- User and Entity Behavior Analytics
- エンドポイント
- ポリシーベースのコンテンツ一元管理(CCM)
- Concentrator、Decoder、Log Collector、Archiverサービス
- ログ統合
- セキュリティ

このセクションで言及されているドキュメントを見つけるには、https://community.netwitness.com/t5/netwitness-platform-online/netwitness-platform-all-documents/ta-p/676246を参照してください。

「製品ドキュメント」セクションには、このリリースのドキュメントへのリンクが記載されています。

アップグレード

次のセクションでは、アップグレード関連の新しい拡張機能について説明します。

Alma OSの移行

RedHatは、CentOS Linux 7が2024年6月30日にサポート終了(EOL)になることを発表しました。この変更に対処するために、NetWitness Platformは新しいバージョンのAlmaLinuxと統合されました。NetWitness 12.4バージョンにアップグレードすると、CentOS 7.9からAlmaLinux 8.9に自動的に移行されます。NetWitness Platform 12.4のアップグレード プロセスは、以前のアップグレードと同様に、簡単で通常通り行われます。AlmaLinux OSにアップグレードするために特定の手順を実行する必要はありません。
AlmaLinuxは、以下の重要なメリットと新機能を提供します。

- AlmaLinuxへのアップグレードは本質的に自動化されたプロセスであり、手動による介入は不要です。
- 管理者が実際のアップグレード プロセスを実行する前に問題を発見、緩和するのに役立つアップグレード前ツールが付属しています。
- 時間と管理労力を節約します。
- インストール済みアプリケーションの制御が保持されます。
- ほとんどの構成情報が保持されます。

NetWitness Platformは、CentOS 7.9からAlmaLinux 8.9に移行する際に、アップグレード プロセスを合理化し、時間とリソースを節約して、インストール済みアプリケーションと構成の制御を保持します。

SASE機能

次のセクションでは、SASEの新しい拡張機能について説明します。

NetWitness SASEの統合

- **NetWitness SASEとPalo Alto Networksの統合** - NetWitnessとPalo Alto Prisma SASEの統合により、ネットワークとログを完全に可視化できます。この技術面のカスタム統合により、NetWitnessユーザーは、オンプレミス、ハイブリッド、クラウド導入環境にわたるリモートおよび分散ネットワーク内のデバイスとサービスの動作や、それらの間の通信についてインサイトを得ることができます。NetWitnessとPalo Alto SASEの統合により、お客様は脅威の検出と対応のための完全な可視性を維持しながら、SASEの柔軟性とその本質的セキュリティのメリットを活用できるようになります。
- **NetWitness SASEとSymantec by Broadcomの統合(プライベート プレビュー モード)** - NetWitnessとSymantec by Broadcom SASEの統合により、ネットワークとログを完全に可視化できます。この技術面のカスタム統合により、NetWitnessユーザーは、オンプレミス、ハイブリッド、クラウド導入環境にわたるリモートおよび分散ネットワーク内のデバイスとサービスの動作や、それらの間の通信についてインサイトを得ることができます。NetWitnessとBroadcom SASEの統合により、お客様は脅威の検出と対応のための完全な可視性を維持しながら、SASEの柔軟性とその本質的セキュリティのメリットを活用できるようになります。

> **注 :**12.4リリースでは、NetWitness SASEとSymantec by Broadcomの統合はプライベート プレビュー モードです。

詳細については、『Broadcom SASE 12.4構成ガイド』と『Palo Alto Prisma SASE 12.4構成ガイド』を参照してください。

NetWitness SASEハイブリッド クラウド構成

管理者はSASEのハイブリッド クラウド モデルを選択できるようになりました。SASEハイブリッド クラウド構成はデータ主導型の設計です。SASEハイブリッド クラウドは、NetWitnessプラットフォーム コンポーネント間のより効率的で安全な通信を実現します。NetWitness Admin Serverには、NetWitnessオーバーレイ ネットワークと定義されたNetWitnessノードを、Google Cloud Platform(GCP) の各リージョンに導入するスクリプト「nw-create-cloud-hybrid」が含まれています。NetWitnessピアツーピア ネットワーク(nw-ppn) は、NetWitnessコンポーネント間の相互認証された安全なPKIベースの通信を提供します。

詳細については、『SASE 12.4インストール ガイド』を参照してください。

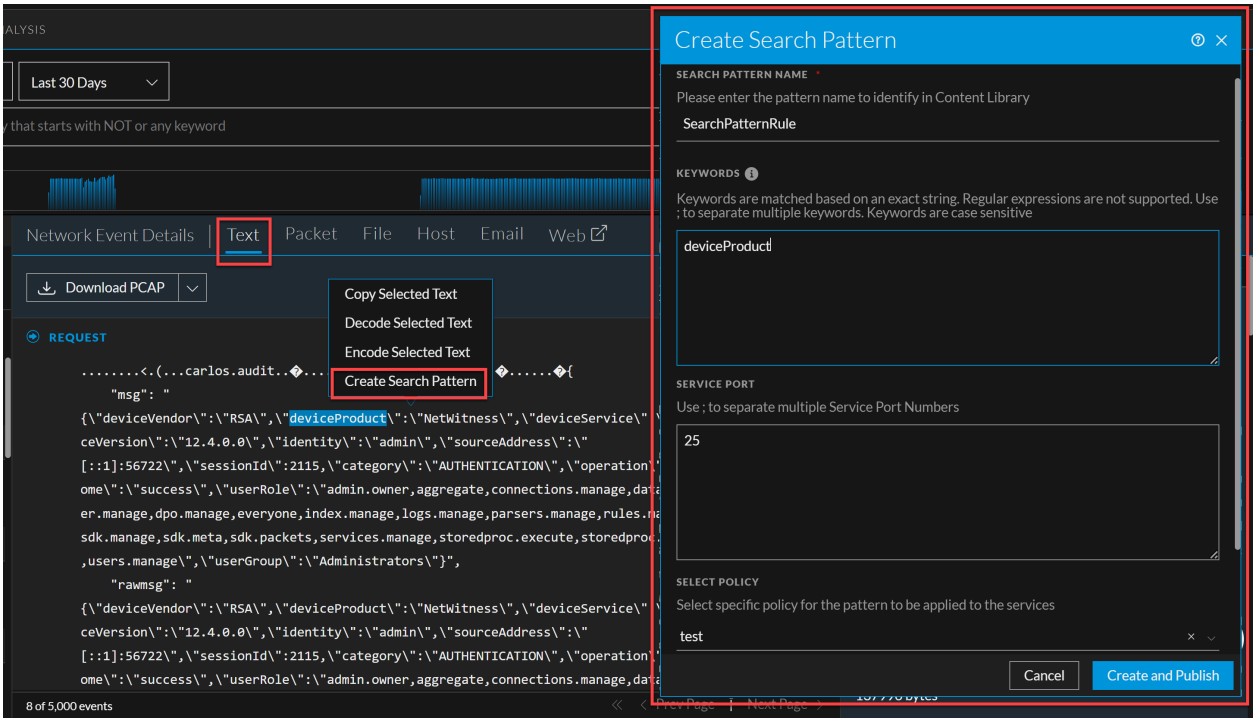
Investigate

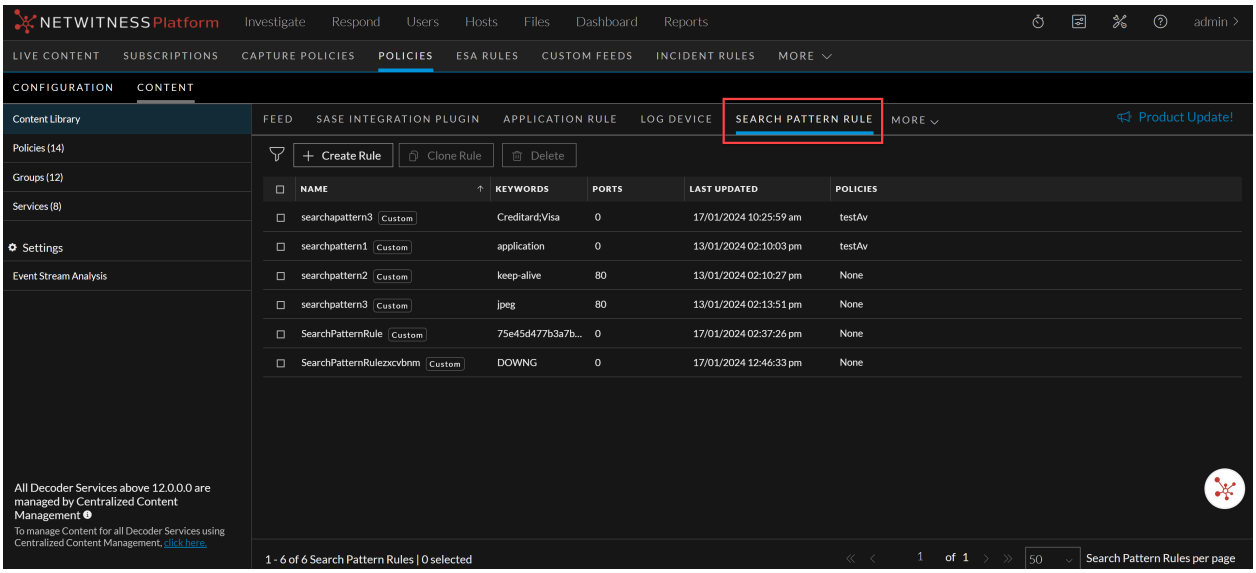
次のセクションでは、Investigateコンポーネントの新しい拡張機能について説明します。

インタラクティブなネットワーク パーサの作成

[**Investigate**] > [**イベント**]ビューでは、選択した完全一致パターン、またはテキスト セッション再構築の際にネットワークトラフィックで見つかったキーワードを、ネットワーク パーサに変換できます。この合理化されたプロセスにより、ユーザーはパーサの作成方法を理解していなくても、インシデント(将来の検出など) をトリガーするためのメタを生成できます。

[**構成**) > [**ポリシー**] > [**コンテンツ ライブラリー**] > [**その他**] > [**検索パターン ルール**]ビューからキーワードを使用して、ネットワーク パーサを作成することもできます。

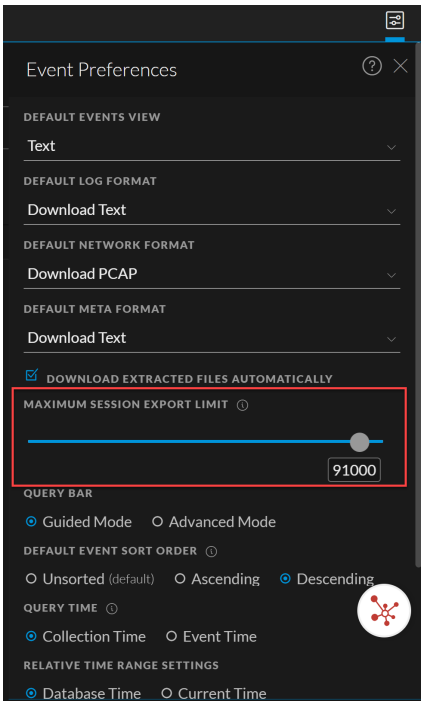




詳細については、『*NetWitness Investigateユーザー ガイド*』の「**テキスト タブでの検索パターンの作成**」トピックと、『*ポリシーベースのコンテンツー元管理ガイド*』の「**検索パターン ルールの管理**」トピックを参照してください。

イベント テーブルに表示されているセッションよりも多くのセッションをダウンロードする

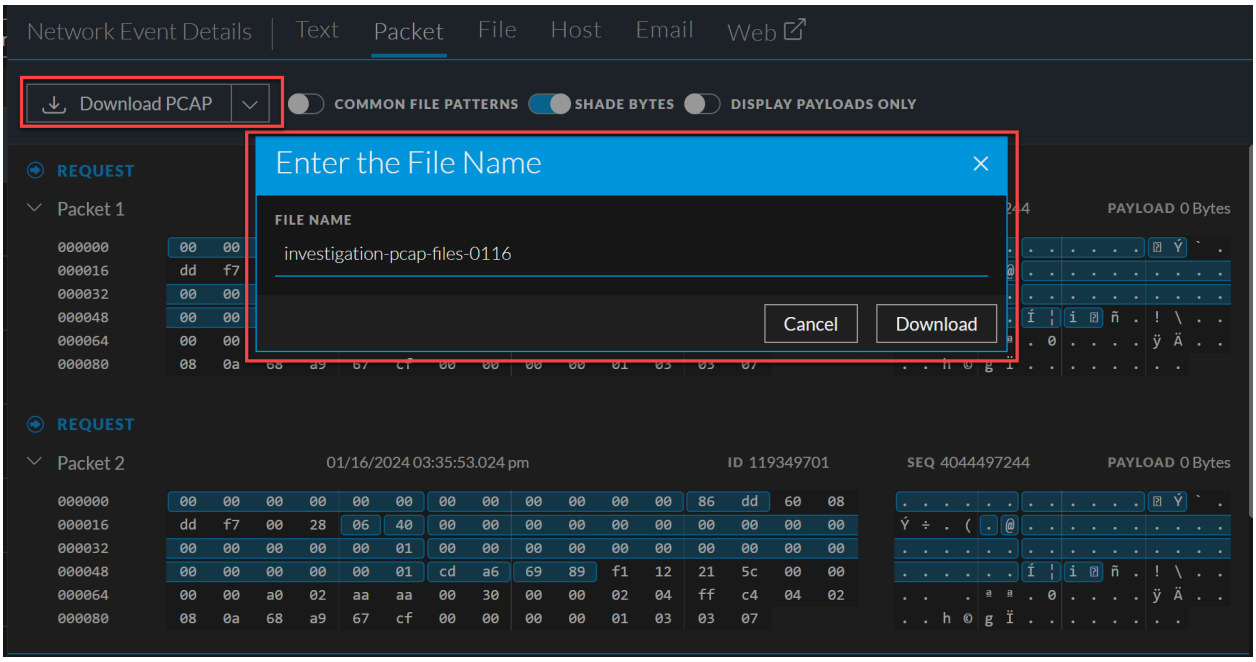
新しいユーザー設定である［**最大セッション エクスポート制限**］が、［**Investigate**］>［**イベント**］ビューの［**イベント設定**］パネルに追加されました。アナリストはこの設定により、［**すべてダウンロード**］メニュー オプションを使用してエクスポートに使用できるセッションの数を調整できます。この機能強化により、エクスポートされたセッションの数が、イベント テーブルに表示されるセッションの数に依存しなくなりました。



詳細については、『*NetWitness Investigateユーザー ガイド*』のトピック「［**イベント**］**ビューのユーザー環境設定の設定**」を参照してください。

カスタム名 でファイルをダウンロード するオプション

アナリスト は、 [**イベント**] パネル ビューからイベント ファイルをダウンロード するときにカスタム名 を使 用 できるようになりました。カスタム名 を使 用 すると、ダウンロードしたイベント ファイルの分 類 と管 理 が容 易 になり、アナリスト の時 間 と労 力 を節 約 できます。



詳 細 については、『*NetWitness Investigateユーザー ガイド*』のトピック「 [**イベント**] **ビューでのデータのダウンロード**」を参 照 してください。

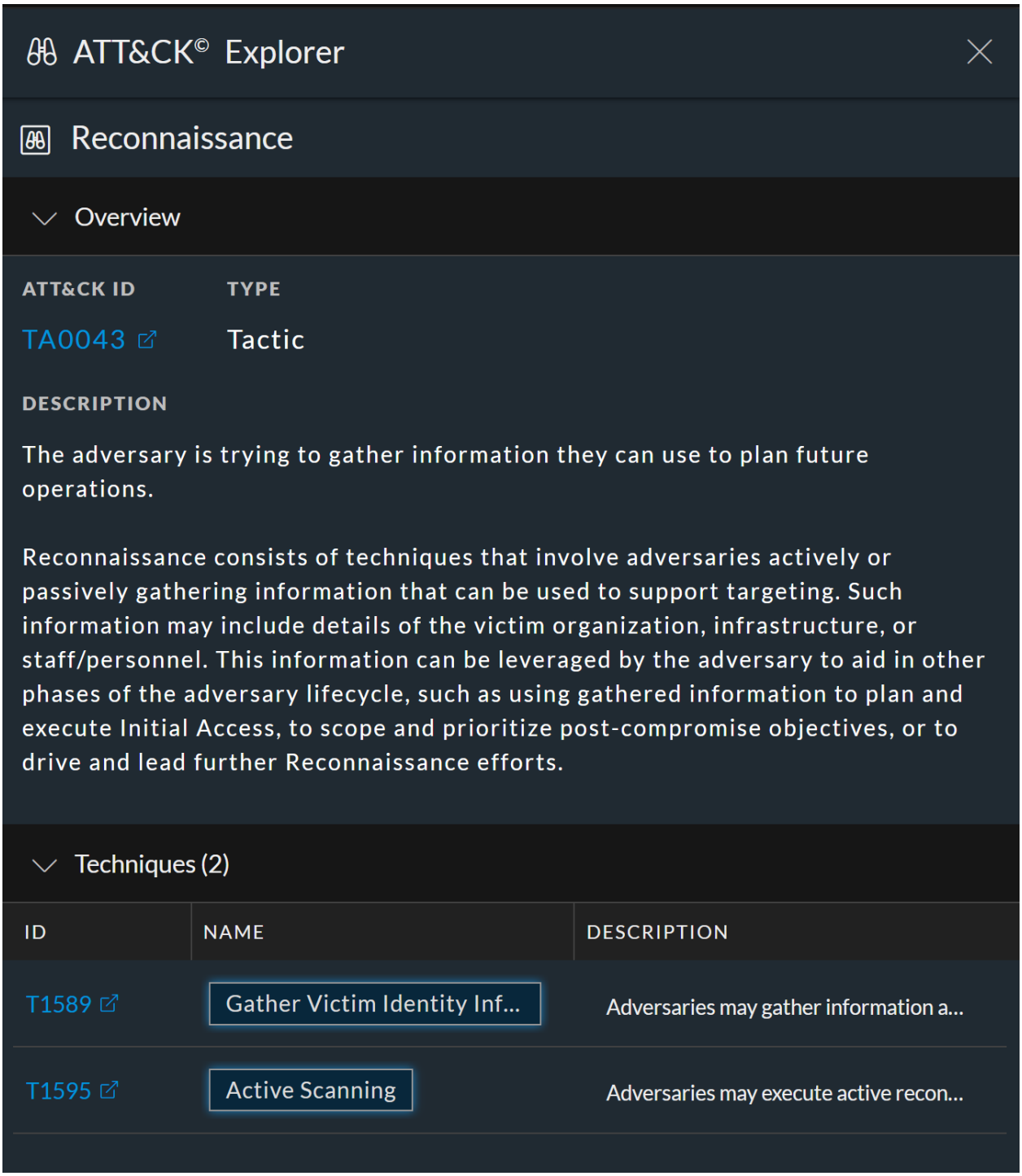
Respond

次 のセクションでは、Respondコンポーネント の新 しい拡 張 機 能 について説 明 します。

MITRE ATT&CK®とNetWitnessの統 合

MITRE ATT&CK®は、攻 撃 者 のテクニックと戦 術 に関 する厳 選 されたナレッジベースであり、攻 撃 者 の行 動 を適 切 なレベルで分 類 し、それに対 する具 体 的 な防 御 方 法 を提 供 します。アナリスト は、指 定 された戦 術 、テクニック、およびサブテクニックの概 要 リスト とその詳 細 を表 示 し、環 境 内 の潜 在 的 な脅 威 と脆 弱 性 がMITRE ATT&CKフレームワークにどのように関 連 づけられているかを知 ることができます。

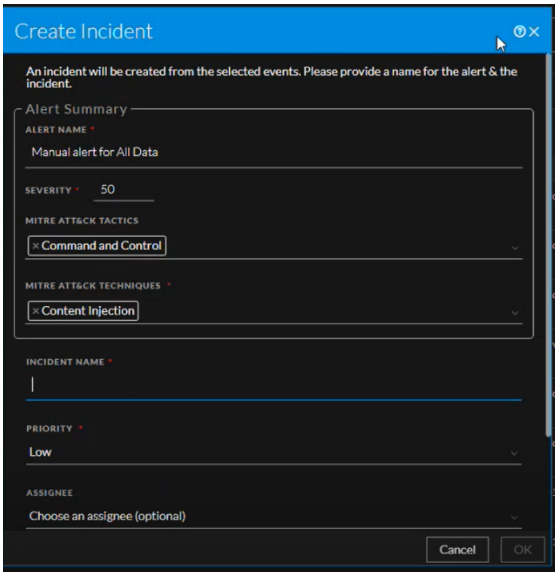
新 しい [**ATT&CK© Explorer**] パネルでは、 [**Respond**] ビューのインシデント に関 連 した攻 撃 者 の戦 術 とテクニックに関 する情 報 を確 認 できます。



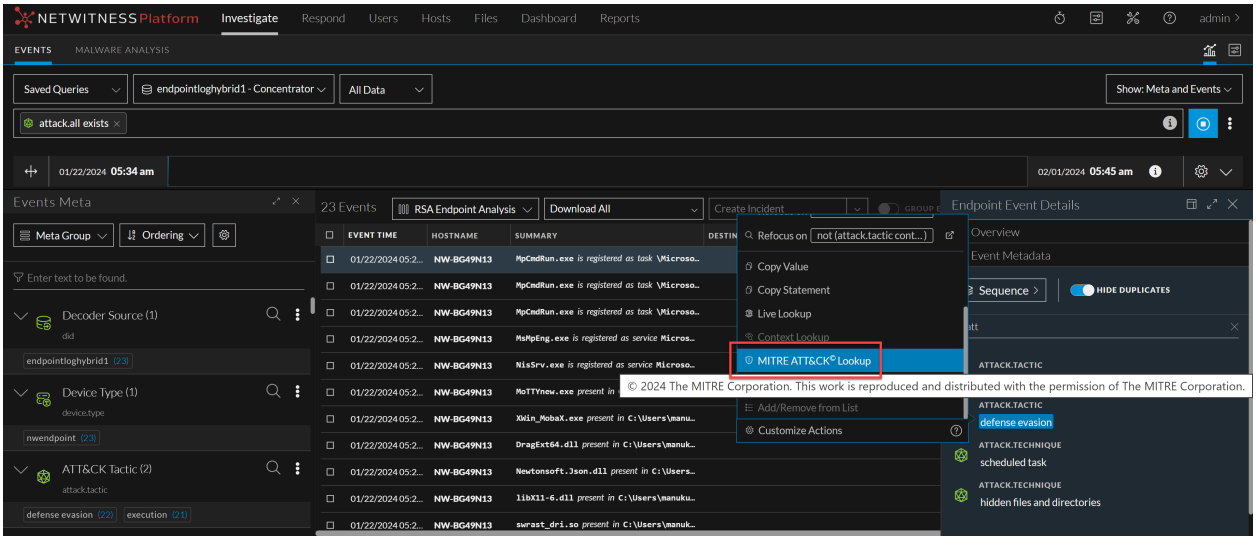
NetWitness LiveはMITRE ATT&CKフレームワークと連携しているため、アナリストは**アプリケーション ルール**と**Event Stream Analysisルール**に関連するMITRE ATT&CKの戦術とテクニックを確認できます。[サービスの詳細]右パネル(**(構成)** > [**ポリシー**] > [**コンテンツ**] > [**コンテンツ ライブラリー**] > [**アプリケーション ルール**]または [**Event Stream Analysisルール**]を選択して、行をクリックし、[サービスの詳細]右パネルを選択) が強化され、MITRE ATT&CKの戦術とテクニックに関する情報が提供されるようになりました。

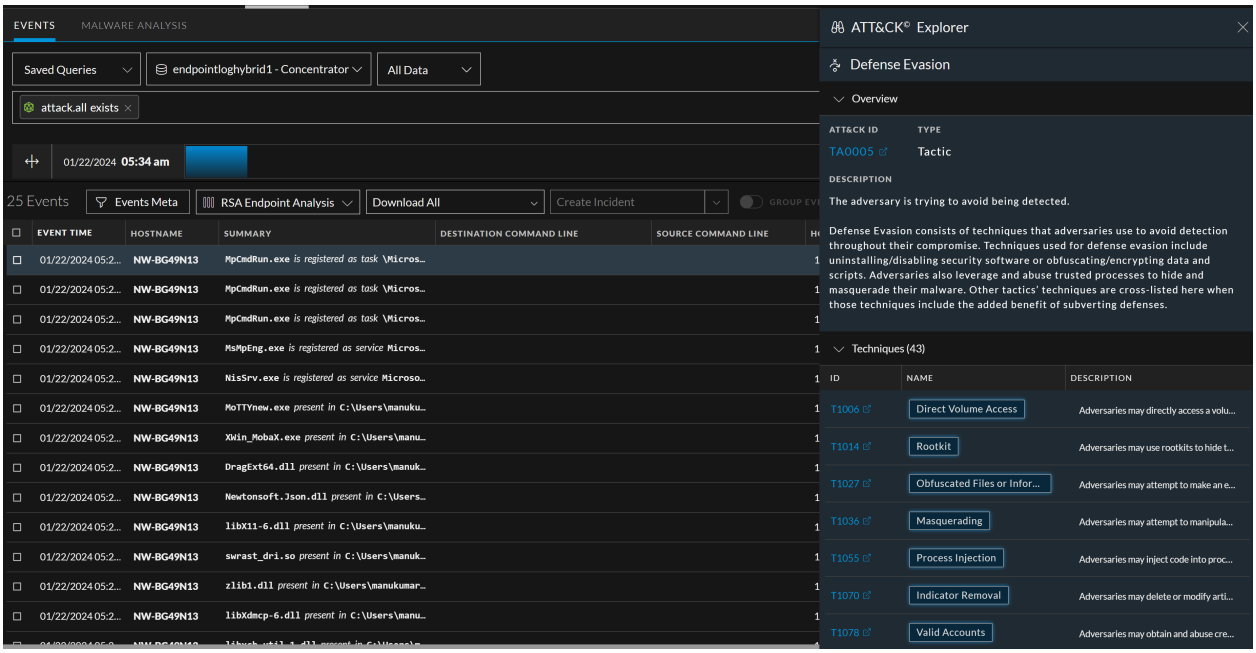
カスタムの**アプリケーション ルール**または**Event Stream Analysisルール**を作成するときに、MITRE ATT&CKの戦術とテクニックにタグを付けることができます。

［**Investigate**］> ［**イベント**］ビューからインシデントを作成するときに、MITRE ATT&CKの戦術とテクニックを選択することもできます。



これに伴い、［**イベント メタデータ**］パネルの**ATTACK.TACTIC**メタキーと**ATTACK.TECHNIQUE**メタキーが**MITRE ATT&CK© Lookup**統合によって強化され、イベントに関連する特定の戦術やテクニックに関する詳細情報を取得できるようになりました。





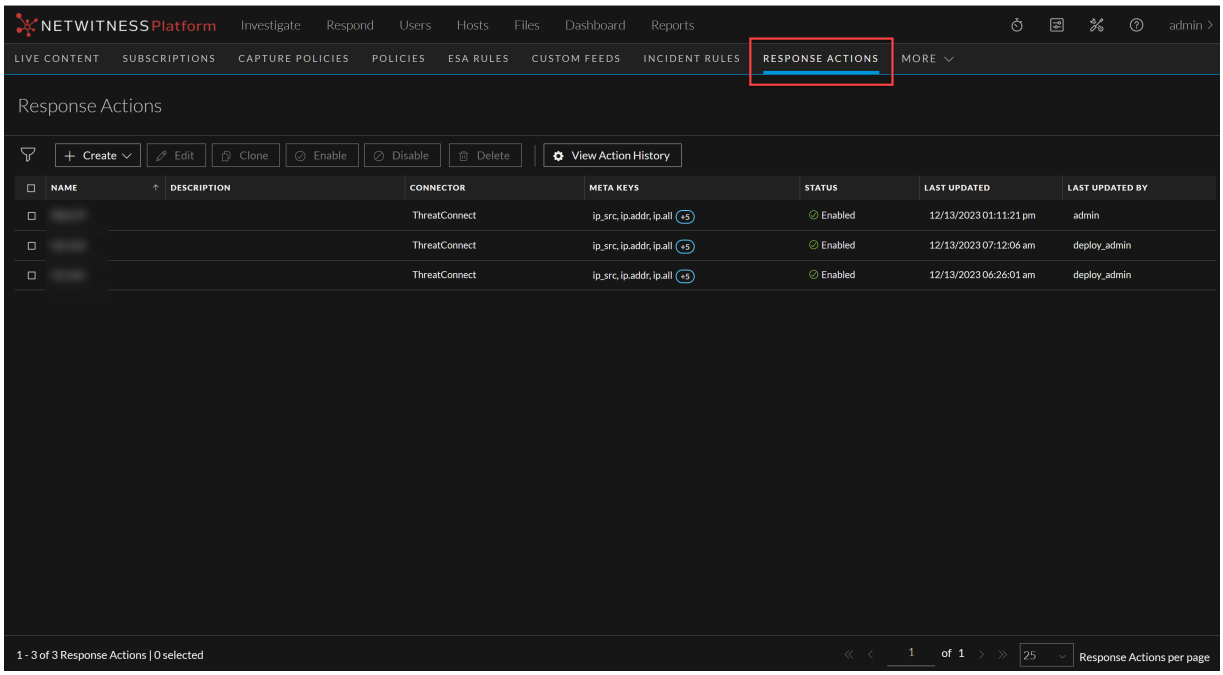
［**MITRE ATT&CK© Lookup**］をクリックすると、新しい［**ATT&CK© Explorer**］パネルが表示されます。

詳細については、『NetWitness Respond 12.4ユーザー ガイド』、『*NetWitness Investigateユーザー ガイド*』、および『*ポリシーベースのコンテンツー元管理ガイド*』を参照してください。

対応アクション

対応アクションは、イベントのトリアージ後に、ThreatConnectなどのサードパーティー製ツールまたはコネクタを使用して、構成済みメタに対して実行される事後操作です。**（構成）** > ［**その他**］に追加された新機能である［**対応アクション**］を使用して、次のアクションを実行できます。

- ［**Respond**］、［**Investigate**］、［**ホスト**］、および［**ユーザー**］ビューで使用できるサポート対象メタの対応アクションを作成し、管理します。
- 構成されたメタに対してクイック アクションを実行し、追加のパラメーターを含んだメタをコネクタにポストすることで、さらなるアクションを実行できるようにします。



詳細については、『NetWitness 12.4対応アクション構成ガイド』を参照してください。

Insight

次のセクションでは、Insightコンポーネントの新しい拡張機能について説明します。

RespondビューのInsightアラートをホワイトリストに登録する

管理者とアナリストは、［**Respond**］>［**アラート**］ビューで生成された不要で反復的なInsightアラートをホワイトリストに登録できるようになりました。この機能強化により、IPアドレスや資産タイプなどの特定の値を選択し、これらの値に対して不要なアラートが生成されないようにホワイトリスト条件を定義できるようになりました。この機能強化を使用すると、アナリストは、信頼性が高く安全であることがわかっている特定のIPアドレスや資産タイプを除外することで、アラート管理プロセスを合理化できます。この最適化により、［**Respond**］>［**アラート**］ビューで生成される不要なアラートが最小限に抑えられ、アラートの確認と分析に必要な時間と労力が削減されます。

詳細については、『*NetWitnessドキュメント ポータル*』の「**NetWitness Insight**セクションを参照してください。

User and Entity Behavior Analytics

次のセクションでは、UEBAコンポーネントの新しい拡張機能について説明します。

Cisco Adaptive Security Appliance(ASA) およびFortinet VPNデバイスのサポート

NetWitness UEBAは、Cisco ASAおよびFortinet VPNデバイスのサポートを追加しました。この機能拡張により、UEBAはCisco ASAとFortinet VPNのログを処理できるようになりました。ユーザー アクティビティ情報の収集と分析にお役立てください。

詳細については、『UEBA構成ガイド』の「**UEBAでサポートされるソース(スキーマ別)** 」セクション(英語) を参照してください。

UEBAのパフォーマンスが向上

12.4.0.0バージョンのUEBAでは、次のパフォーマンス向上が加えられています。

- モデルを並行して生成、保存できるように、集計モデルと累積モデルが最適化されました。
- 集計とスコア付けを並行して実行できるように、時間ごとのスコア集計タスクが最適化されました。

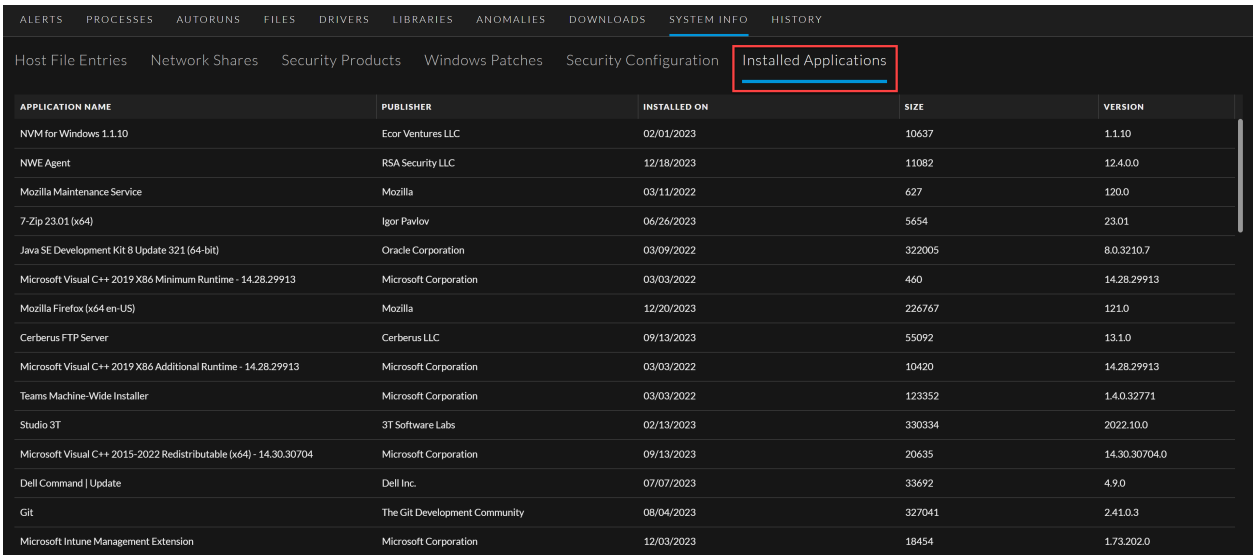
サポートされているスケールの詳細については、『UEBA構成ガイド』のトピック「**12.4のスケールあたりの学習期間**」を参照してください。

エンドポイント

次のセクションでは、Endpointコンポーネントの新しい拡張機能について説明します。

インストールされているアプリケーションの表示

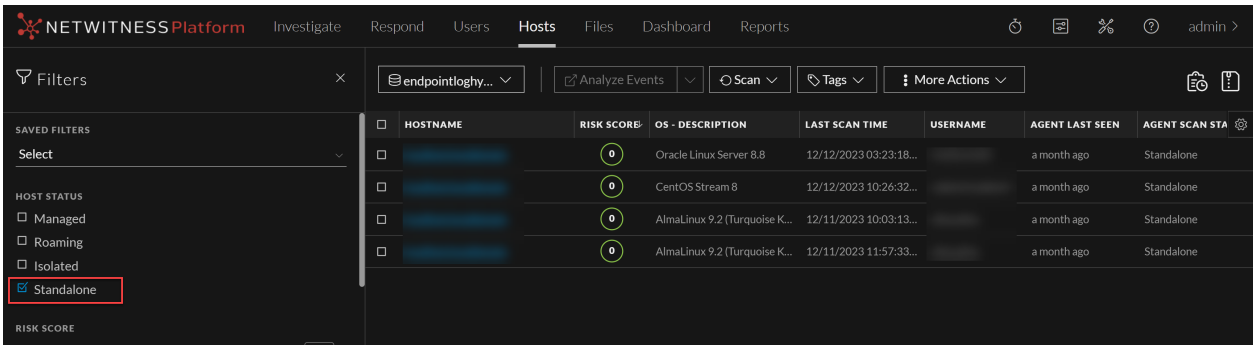
［**ホストの詳細**］>［**システム情報**］ビューが強化され、アナリストはWindowsマシンにインストールされているさまざまなアプリケーションに関する情報を表示できるようになりました。



詳細については、『*NetWitness Endpoint 12.4ユーザー ガイド*』を参照してください。

Linuxエージェントのスタンドアロン スキャン

管理者は、Linuxホスト上でオフラインまたはスタンドアロン スキャンを実行して、エアギャップされたLinuxマシン上で脅威分析を実行できます。



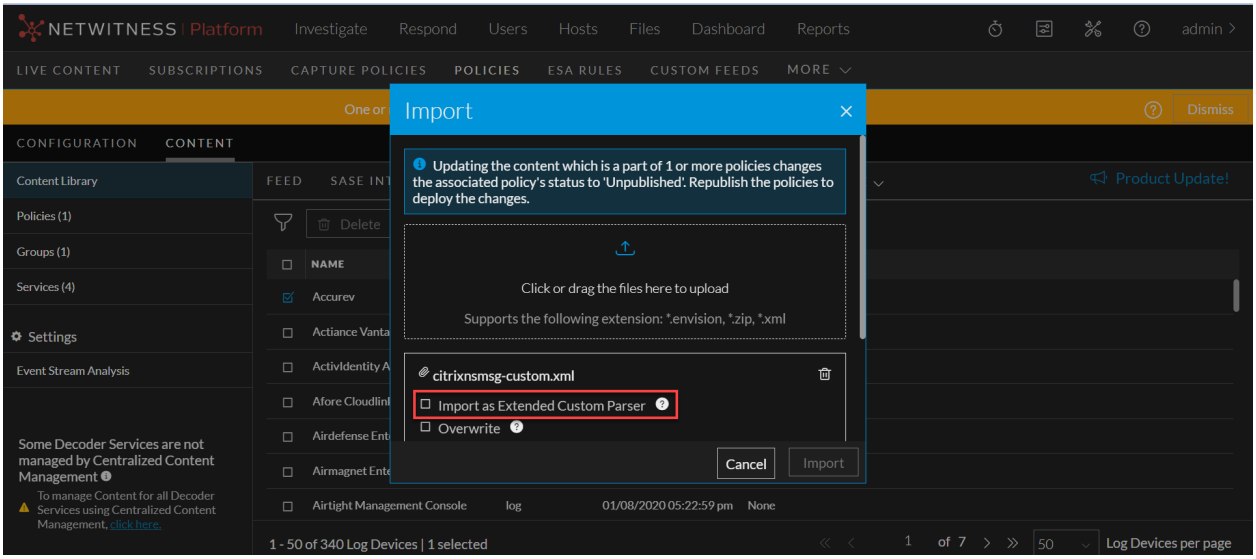
詳細については、『*NetWitness Endpoint 12.4ユーザー ガイド*』を参照してください。

ポリシーベースのコンテンツー元管理(CCM)

12.4.0.0バージョンのCCMに対して次の機能強化が加えられています。

CCMを介したカスタム パーサの適切な動作とサービスへの導入のための機能強化

個々のXML(ログ デバイス コンテンツ タイプ)をコンテンツ ライブラリーにインポートする機能が導入されました。基本パーサまたは拡張パーサをスタンドアロンXMLファイルとしてアップロードできます。XMLファイルをインポートするときに、対応する基本パーサに関連づけることで(オプション)、事実上拡張パーサとして扱うことができます。スタンドアロンXMLを拡張パーサとしてインポートするには、[**インポート**]画面で **拡張カスタム パーサとしてインポート**]を選択します。



コンテンツ ライブラリーでは、基本パーサと拡張パーサが別々の項目として表示されるようになり、明確でわかりやすくなりました。この分離により、ユーザーはライブラリー内の両方のタイプのパーサを簡単に識別して管理できます。さらに、拡張パーサがポリシーに追加されると、対応する基本パーサも自動的にポリシーに追加されます。この合理化された統合により、ユーザーのプロセスがシンプルになり、ポリシーの作成時または編集時に基本パーサと拡張パーサを手動でリンクする必要がなくなりました。

詳細については、『*ポリシーベースのコンテンツー元管理ガイド*』の「**コンテンツ ライブラリーへのコンテンツのインポート**」セクションを参照してください。

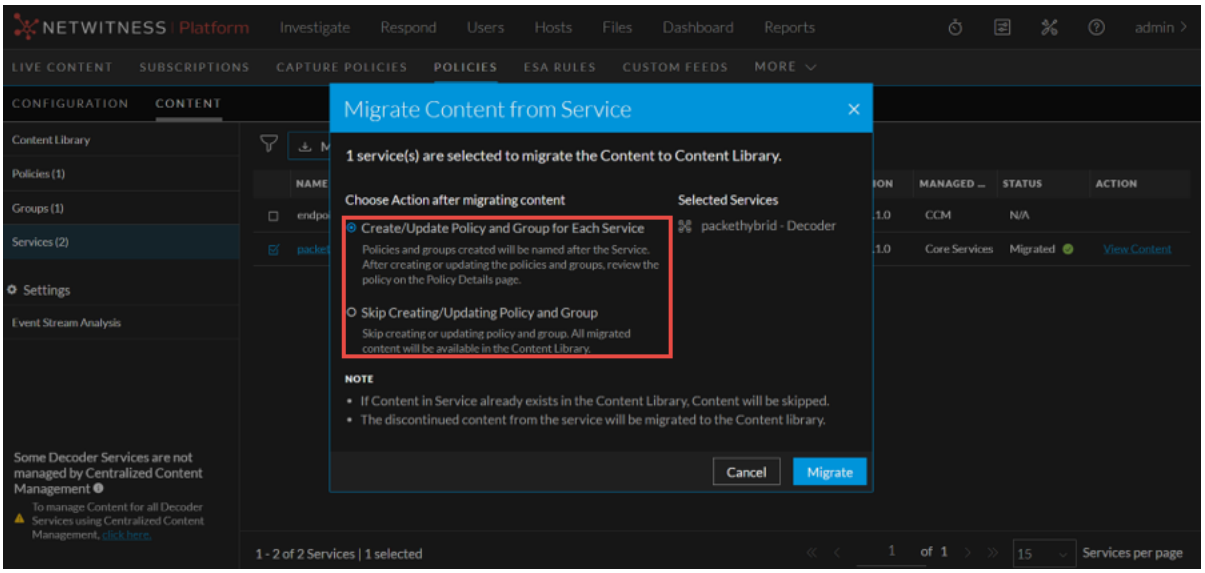
グループからサービスを削除する際の機能強化

グループからサービスを削除する際に、サービスからコンテンツを削除した後でグループからサービスを削除するか、コンテンツを削除せずにサービスをグループから削除するかを選択できます。

詳細については、『*ポリシーベースのコンテンツ一元管理ガイド*』の「**グループの編集**」、「**ポリシーの編集**」、および「**ポリシーの削除**」セクションを参照してください。

サービスからコンテンツを再移行する機能

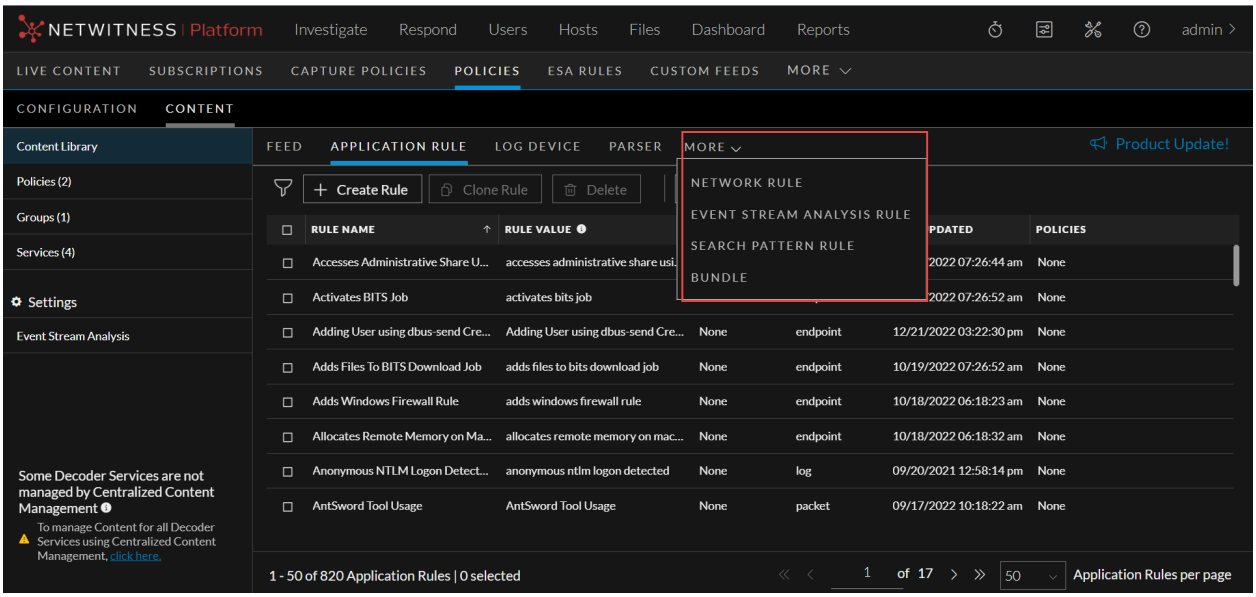
CCMの機能が強化され、コンテンツがすでに移行されているか、グループやポリシーに割り当てられている場合でも、サービスから再移行できるようになりました。すでにポリシーに関連づけられているサービスからコンテンツを移行する際に、移行されたコンテンツで関連ポリシーを更新することが可能です。サービスの再移行後にサービスの既存のポリシーとグループを更新するため、［**サービスのコンテンツを移行**］ページで使用できるオプションが［**各サービスのポリシーとグループを作成/更新**］と［**ポリシーとグループの作成/更新をスキップ**］に更新されました。



詳細については、『*ポリシーベースのコンテンツ一元管理ガイド*』の「**サービスのコンテンツを移行**」セクションを参照してください。

ユーザー インターフェイスの機能拡張

［**その他**］ナビゲーション メニューがCCM UIに追加され、バンドル、検索パターン、統合がデフォルトで表示されるようになりました。［**その他**］メニューからコンテンツ タイプを選択すると、そのコンテンツ タイプが［**その他**］メニューの左側に表示されます。

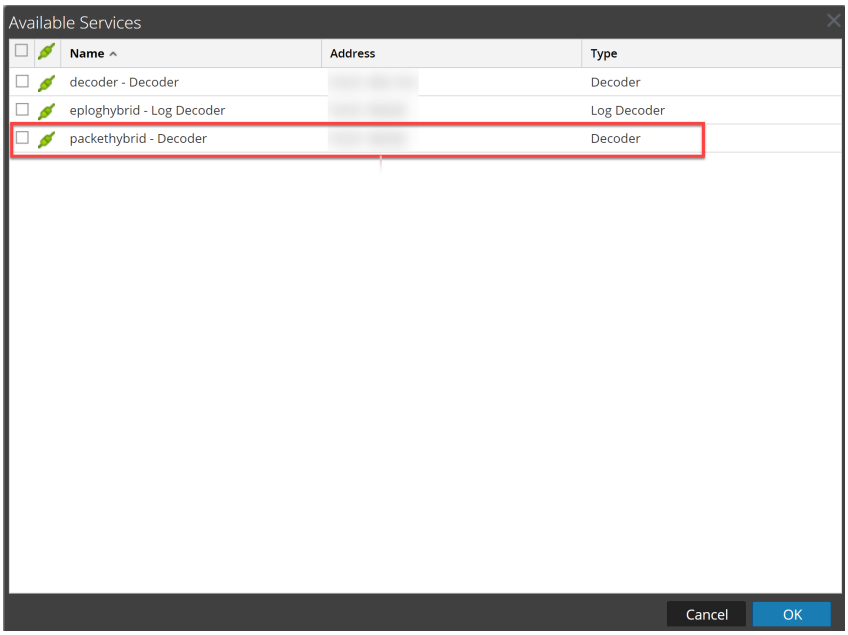


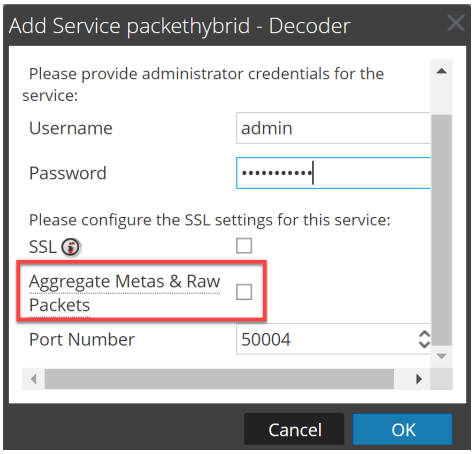
Concentrator、Decoder、Log Collector、Archiverサービス

12.4.0.0バージョンでは、Concentrator、Decoder、Log Collector、Archiverサービスに対して次の機能強化が加えられています。

Packet Decoderの選択的保存

このリリースでは、NDRのお客様に選択的保存オプションが提供されます。これによりお客様は、重要な証拠を保持してフォレンジックと脅威ハンティングで優れた成果を達成し続けつつ、必要な保存要件を積極的に緩和できるようになります。これを実現する手段として、管理者は (管理) > [サービス] > [構成]ビュー > [全般]タブを使用して、ArchiverのPacket Decoderホストをデータソースとしてシームレスに構成できます。さらに管理者は、新しい [メタとrawパケットの集計]オプションを使用して、必要な集計タイプを選択できるようになりました。このようにして管理者は、メタデータ値のみに基づいてDecoderサービスを集計するか、メタデータ値とrawパケットの両方に基づいて集計するかを選択できます。





詳細については、『*Archiver構成ガイド*』の「**Packet Decoderをデータ ソースとしてArchiverに追加する**」トピックを参照してください。

基本認証でのIPアドレスの使用を廃止する機能

Netwitnessは、Windowsコレクション基本認証でのIPアドレスの使用を廃止しました。これに伴い、基本認証の構成中に、イベント ソース アドレスでFQDNを使用し、同じFQDNのエントリーを「/etc/hosts」に追加する必要があります。

Decoderからサード パーティー製ツールにメタをストリーミングする新しいユーティリティー

ネットワーク上のDecoderから他のサードーパーティー製ツールにメタをストリーミングするベータ ユーティリティーが導入され、NetWitness Platformと他の製品を簡単に統合できるようになりました。メタデータのすべてまたは一部をストリーミングして、ユースケースに応じてサード パーティー製ツールに送信される量を制限できます。

詳細については、『メタ エクスポート インストールおよび構成ガイド』を参照してください。

ログ統合

NetWitness Platformは、ログの収集と解析のために次のイベント ソースの統合をサポートしています。特に指定のない限り、これらのサービスはNetWitness Platform 12.2.0.0以降でサポートされます。

- Palo Alto Prisma Access
- VMware vSphere
- DeepInspect
- GCP Windows VMログ(GCPプラグイン経由)

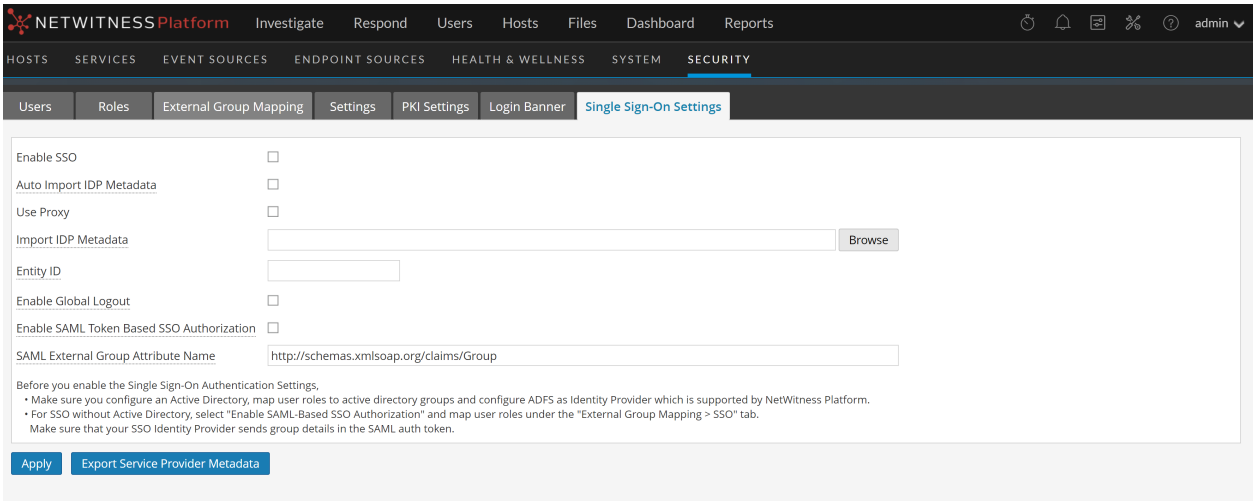
注 :12.4以降、VMwareプラグインはVMwareのイベントとタスクの収集にも使用できます。

パーサ サービスの統合の詳細については、『NetWitness Platform統合ガイド』を参照してください。

セキュリティ

NetWitnessのActive Directory(AD) 構成に依存しないシングル サインオン(SSO) 認証

NetWitness Platformバージョン12.4以降、NetWitnessは、NetWitnessのAD構成に依存しないSSOを提供します。これにより、ADFSから受信したSAML認証トークンに埋め込まれているユーザー グループのリストを使用し、NetWitnessですでに設定されているユーザー グループと照合してユーザーを認証できます。ユーザーは、ユーザー認証のためにNetWitness内でActive Directory設定を構成したり、それに依存したりする必要がなくなります。NetWitnessは、Azure ADFSとMicrosoft ADFSの両方をサポートするようになりました。



詳細については、『*システム セキュリティとユーザー管理ガイド*』の「**シングル サインオン認証の設定**」トピックを参照してください。

セキュリティ修正

セキュリティ修正の詳細については、https://community.netwitness.com/t5/netwitness-platform-advisories/ct-p/netwitness-advisories#securityを参照してください。

アップグレード パス

NetWitness 12.4.0.0では、次のアップグレード パスがサポートされます。

- NetWitness 12.3.1.0から12.4.0.0へ
- NetWitness 12.3.0.0から12.4.0.0へ
- NetWitness 12.2.0.1から12.4.0.0へ
- NetWitness 12.2.0.0から12.4.0.0へ

12.4.0.0へのアップグレードの詳細については、『NetWitness 12.4.0.0アップグレード ガイド』を参照してください。

重要：11.7.xまたは11.7.x.xバージョンから12.4.0.0バージョンにアップグレードする場合は、12.4にアップグレードする前に、まず12.2.0.0または12.3.0.0バージョンにアップグレードする必要があります。

NetWitness Platformの製品バージョン ライフ サイクル

プライマリー サポート終了(EOPS)が到来するバージョンについては、「NetWitness Platformの製品バージョン ライフ サイクル」のリストを参照してください。

以前のリリースでの新機能(11.7から12.3.1.0)

このセクションでは、サポートされる以前のすべてのリリースの新機能と機能拡張について説明します。

詳細については、https://community.netwitness.com/t5/netwitness-platform-online/what-s-new-in-previous-releases-11-7-to-12-1-1/ta-p/695650を参照してください。

12.4.0.0リリースで修正済みの問題

このセクションでは、12.4.0.0バージョンで修正された問題を示します。

修正された問題の詳細については、NetWitnessコミュニティー ポータルのNetWitness® Platform既知の問題リスト(https://community.netwitness.com/t5/netwitness-platform-known-issues/netwitness-platform-known-issues/ta-p/571872) で 修正されたバージョン］列を参照してください。

ポリシーベースのコンテンツー元管理(CCM) の修正

追跡番号	説明
ASOC-142018	CCMから公開されたログ デバイスのコンテンツは、サービスのコンテンツが削除されても無効になりません。
ASOC-141524	ESAルールを編集または更新しても、ESAルールを保存できませんでした。NetWitness UIおよびSAのログには、ルールの保存中の実行時例外が示されていました。また、トラブルシューティングでは、**RSA OSINT Non-IP Threat Intel Feed**でユニークIDがポリシーに関連付けられませんでした。この問題は、コンテンツ ポリシー コレクション内の複数のドキュメントで発生しました。

12.4.0.0リリースの既知の問題

本リリースで解決されていない問題は、NetWitnessコミュニティー ポータルの「NetWitness® Platformの既知の問題リスト」に記載されています。https://community.netwitness.com/t5/netwitness-platform-known-issues/netwitness-platform-known-issues/ta-p/571872

12.4.0.0コンポーネントのビルド番号

次の表は、NetWitness 12.4.0.0の各コンポーネントのビルド番号の一覧です。

コンポーネント	バージョン番号
NetWitness管理サーバー	rsa-nw-admin-server-12.4.0.0-240117024246.5.165a1f70.el8.alma.noarch.rpm
NetWitness Advanced Analyticsコンテンツ	rsa-nw-advanced-analytics-content-12.4.0.0-231212110357.5.9b3b362.el8.alma.noarch.rpm
NetWitness Advanced Analytics サーバー	rsa-nw-advanced-analytics-server-12.4.0.0-231212110325.5.9b3b362.el8.alma.noarch.rpm
NetWitness Appliance	rsa-nw-appliance-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Archiver	rsa-nw-archiver-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Auditプラグイン	rsa-audit-plugins-12.4.0.0-4892.5.9d0750b41.el8.noarch.rpm
NetWitness Audit RT	rsa-audit-rt-12.4.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitnessブートストラップ	rsa-nw-bootstrap-12.4.0.0-2401240926.5.a3d68ef.el8.noarch.rpm
NetWitness Broker	rsa-nw-broker-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Carlos RT	rsa-carlos-rt-12.4.0.0-2787.5.721a8daa7.el7.x86_64.rpm
NetWitness Cloud	rsa-nw-cloud-12.4.0.0-12867.5.957818c84.el8.x86_64.rpm

NetWitness Cloud Connectorサーバー	rsa-nw-cloud-connector-server-12.4.0.0-240116135943.5.4220688.el8.alma.noarch.rpm
NetWitness Cloud Linkサーバー	rsa-nw-cloud-link-server-12.4.0.0-240117032857.5.d4a8422.el8.alma.noarch.rpm
NetWitness Collectd	rsa-collectd-12.4.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Collectd SMS	rsa-collectd-sms-12.4.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitnessコンポーネント ディスクリプタ	rsa-nw-component-descriptor-12.4.0.0-2402080831.5.a403c19.el8.noarch.rpm
NetWitness Concentrator	rsa-nw-concentrator-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Config Management	rsa-nw-config-management-12.4.0.0-2402050947.5.b7e9f64.el8.noarch.rpm
NetWitness Config Server	rsa-nw-config-server-12.4.0.0-240109020724.5.dc657b7.el8.alma.noarch.rpm
NetWitnessコンソール	rsa-nw-console-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitnessコンテンツ サーバー	rsa-nw-content-server-12.4.0.0-240109040529.5.314fc043.el8.alma.noarch.rpm
NetWitness ContextHubサーバー	rsa-nw-contexthub-server-12.4.0.0-240122010054.5.d98d0ac61.el8.alma.noarch.rpm

NetWitness Correlation Server (ESA)	rsa-nw-correlation-server-12.4.0.0-240117103632.5.61d080a9.el8.alma.noarch.rpm
NetWitness Dashboardコンテンツ	rsa-nw-dashboard-content-20231220155210-5.noarch.rpm
NetWitness Decoder	rsa-nw-decoder-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Decoder Analyticsコンテンツ	rsa-nw-decoder-analytics-content-20231220155210-5.noarch.rpm
NetWitness Decoderコンテンツ	rsa-nw-decodercontent-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness導入環境アップグレード	rsa-nw-deployment-upgrade-12.4.0.0-2402050945.5.1903a3b.el8.noarch.rpm
NetWitness Endpointエージェント	rsa-nw-endpoint-agents-12.4.0.0-2402061657.5.db93b9a.el8.x86_64.rpm
NetWitness Endpoint Brokerサーバー	rsa-nw-endpoint-broker-server-12.4.0.0-240103053136.5.8430874.el8.alma.noarch.rpm
NetWitness Endpoint Decoder Analyticsコンテンツ	rsa-nw-endpointdecoder-analytics-content-20231220155210-5.noarch.rpm
NetWitness Endpointサーバー	rsa-nw-endpoint-server-12.4.0.0-240125030031.5.12c246114.el8.alma.noarch.rpm
NetWitness ESPER Enterprise	rsa-nw-esper-enterprise-12.4.0.0-2311071130.5.04c15de.el8.alma.noarch.rpm
NetWitness Integration Server	rsa-nw-integration-server-12.4.0.0-240117101347.5.0ed5cc33.el8.alma.noarch.rpm

NetWitness Investigate Server	rsa-nw-investigate-server-12.4.0.0-240109023320.5.2a0d2764.el8.alma.noarch.rpm
NetWitness Legacy Webサーバー	rsa-nw-legacy-web-server-12.4.0.0-240122162503.5.40628dd.el8.almalinux.noarch.rpm
NetWitnessライセンス サーバー	rsa-nw-license-server-12.4.0.0-240111044400.5.a6108af.el8.alma.noarch.rpm
NetWitness Log Collector	rsa-nw-logcollector-12.4.0.0-15127.5.527ec7727.el8.x86_64.rpm
NetWitness Log Collectorコンテンツ	rsa-nw-logcollectorcontent-20240105141144-5.x86_64.rpm
NetWitness Log Collector Perl	rsa-nw-logcollector-perl-12.4.0.0-15127.5.527ec7727.el8.x86_64.rpm
NetWitness Log Collectorツール	rsa-nw-logcollector-tools-12.4.0.0-15127.5.527ec7727.el8.x86_64.rpm
NetWitness Log Decoder	rsa-nw-logdecoder-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Log Decoder Analyticsコンテンツ	rsa-nw-logdecoder-analytics-content-20231220155210-5.noarch.rpm
NetWitness Log Decoder Baseコンテンツ	rsa-nw-logdecoder-base-content-20240124060008-5.x86_64.rpm
NetWitness Log Player	rsa-nw-logplayer-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm

NetWitness Malware Analytics サーバー	rsa-nw-malware-analytics-server-12.4.0.0-240207115909.5.1511622.el8.almalinux.x86_64.rpm
NetWitnessメタ エクスポート ユーティリティー	rsa-nw-metaexport-utility-12.4.0.0-110124.5.el8.x86_64.rpm
NetWitness Metricsサーバー	rsa-nw-metrics-server-12.4.0.0-240109050254.5.c078db1.el8.alma.noarch.rpm
NetWitnessノード インフラストラクチャ サーバー	rsa-nw-node-infra-server-12.4.0.0-240116091133.5.70861f6.el8.alma.noarch.rpm
NetWitnessオーケストレーションCli	rsa-nw-orchestration-cli-12.4.0.0-2401091103.5.7317baa.el8.noarch.rpm
NetWitnessオーケストレーション サーバー	rsa-nw-orchestration-server-12.4.0.0-240119064852.5.a87bb81f.el8.alma.noarch.rpm
NetWitnessプレースホルダー	rsa-nw-placeholder-12.4.0.0-2310040926.5.cebd204.el8.noarch.rpm
NetWitness Presidio Airflow	rsa-nw-presidio-airflow-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio構 成 サーバー	rsa-nw-presidio-configserver-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidioコア	rsa-nw-presidio-core-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm

NetWitness Presidio Elasticsearch 初期化	rsa-nw-presidio-elasticsearch-init-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio Ext NetWitness	rsa-nw-presidio-ext-netwitness-12.4.0.0-2401151152.5.18bd06b.el8.noarch.rpm
NetWitness Presidioマネージャー	rsa-nw-presidio-manager-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio出 力	rsa-nw-presidio-output-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio UI	rsa-nw-presidio-ui-12.4.0.0-2402270745.5.0844250.el8.noarch.rpm
NetWitness Protobuf	rsa-protobufs-rt-12.4.0.0-928.5.6254aabd8.el8.x86_64.rpm
NetWitnessリカバリ ツール	rsa-nw-recovery-tool-12.4.0.0-2401230435.5.f34a9fd.el8.noarch.rpm
NetWitnessリレー サーバー	rsa-nw-relay-server-12.4.0.0-240112083607.5.6d41796.el8.alma.noarch.rpm
NetWitness Reporting Engineサーバー	rsa-nw-re-server-12.4.0.0-5996.5.b76234be4.el8.x86_64.rpm
NetWitness Respondサーバー	rsa-nw-respond-server-12.4.0.0-240110052505.5.1eda6132f.el8.alma.noarch.rpm
NetWitness Response Actionsサーバー	rsa-nw-response-actions-server-12.4.0.0-240116034125.5.0af5d71.el8.alma.noarch.rpm

NetWitness Root CAアップデート	rsa-nw-root-ca-update-12.4.0.0-2401221231.5.96cd15b.el8.noarch.rpm
NetWitness SA Tools	rsa-sa-tools-12.4.0.0-2401251338.5.89600eb.el8.noarch.rpm
NetWitnessセキュリティCli	rsa-nw-security-cli-12.4.0.0-2401091103.5.18ab320.el8.noarch.rpm
NetWitnessセキュリティ サーバー	rsa-nw-security-server-12.4.0.0-240123034132.5.11d93f41.el8.alma.noarch.rpm
NetWitnessシェル	rsa-nw-shell-12.4.0.0-240108140410.5.0b0d73f5.el8.alma.noarch.rpm
NetWitnessSOSレポート プラグイン	rsa-nw-sosreport-plugins-12.4.0.0-2401162235.5.af21a76.el8.noarch.rpm
NetWitness SMS Runtime RT	rsa-sms-runtime-rt-12.4.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness SMS Server	rsa-sms-server-12.4.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitnessソース サーバー	rsa-nw-source-server-12.4.0.0-240207074107.5.4b84868b1.el8.alma.noarch.rpm
NetWitnessソース サーバー コンテンツ	rsa-nw-sourceserver-content-20240105141144-5.x86_64.rpm
NetWitnessユーザー インターフェイス	rsa-nw-ui-12.4.0.0-240131063757.5.d1b137ecbc.el8.alma.noarch.rpm

NetWitness Workbench	rsa-nw-workbench-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm

NetWitness Platformのヘルプ情報

製品ドキュメント

このリリースでは、次のドキュメントが提供されます。

マニュアル	参照場所
NetWitness Platformマスター目次	https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation
NetWitness Platform 12.4.0.0 Product Documentation	https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation
NetWitness Platform 12.4.0.0アップグレード ガイド	https://community.netwitness.com/t5/rsa-netwitness-platform-staged/upgrade-guide-for-12-4/ta-p/709308
NetWitness Analytics on Cloud	NetWitness Analytics on Cloudリリースの新機能と拡張機能の詳細については、次の「新機能」セクションを確認してください。 UEBAクラウドについては、https://docs.netwitness.com/netwitnessueba/release_information/whats_new/をご覧ください。 Insightについては、https://docs.netwitness.com/netwitnessinsight/release-information/insight_whatsnew/をご覧ください。

セルフ ヘルプ リソース

NetWitnessのインストールおよび使用について支援が必要な場合は、次の情報をご利用ください。

- NetWitnessに関するすべてのドキュメントは、次の場所から参照できます。
  https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation

- 特定の情報を見つけるには、NetWitnessコミュニティー ポータルの［Search］および［Create a Post］フィールドを使用します(https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions) 。
- NetWitnessのナレッジベース：https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base
- ガイドの「トラブルシューティング」セクションを参照します。
- NetWitness® Platformのブログ投稿も参照してください。
- さらに支援が必要な場合は、カスタマー サポートにお問い合わせください。

カスタマー サポートへのお問い合わせ

カスタマー サポートに連絡する場合は、コンピューターを操作できる状態である必要があります。以下の情報を提供できるように準備しておいてください。

- お使いのNetWitness Platform製品またはアプリケーションのバージョン番号
- お使いのハードウェアのタイプ

質問や支援が必要な場合は、以下の連絡先までお問い合わせください。

NetWitnessコミュニティ ポータル	https://community.netwitness.com メイン メニューで［Support］>［Case Portal］>［View My Cases］をクリックします。
各国のお問い合わせ窓口	https://community.netwitness.com/t5/support/ct-p/support
コミュニティ	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions
NW更新	https://update.netwitness.com/
LiveUI	https://live.netwitness.com

NetWitness教育サービス

登録すると、NetWitnessのコースや、NetWitness教育サービスおよびトレーニングに関する追加リソースにアクセスできるようになります。

NetWitness教育ポータル	https://netwitness.sabacloud.com/Saba/Web_spf/NA10P2PRD088/guestapp/home;spf-url=guest%2Fguestlearningcatalog

NetWitness教育サービス コースカタログ	https://community.netwitness.com/t5/netwitness-education-courses/tkb-p/netwitness-training
NetWitness教育サービストレーニング スケジュール	https://community.netwitness.com/t5/netwitness-education-blog/netwitness-instructor-led-training-schedule/ba-p/655826
NetWitness教育サービス サポート連絡先	education.support@netwitness.com

製品ドキュメントへのフィードバック

NetWitness Platformのドキュメントに関するフィードバックは、feedbacknwdocs@netwitness.comまでメールで送信してください。