RSA® NetWitness

Version11.7

リリース ノート

連絡先情報

RSA Link(https://community.rsa.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 Conferenceのロゴ、RSA、その他の商標は、RSA Security LLCまたはその関連会社(「RSA」)の商標です。RSAの商標のリストについては、https://www.rsa.com/ja-jp/company/rsa-trademarksを参照してください。その他の商標は、各社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、RSA Link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。

配布

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、本文書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。

本文書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では、本文書に記載される情報に関するいかなる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に対する適応性に対する黙示的保証は提供しません。

12月 2021

目次

新機能

NetWitness 11.7は、セキュリティ オペレーション センター(SOC) のすべてのロールに新機能と機能拡張を提供します。

アップグレード パス

NetWitness 11.7.0.0では、以下のアップグレード パスがサポートされます。

- NetWitness 11.5.3.2から11.7.0.0へ
- NetWitness 11.6.0.0から11.7.0.0へ
- NetWitness 11.6.0.1から11.7.0.0へ
- NetWitness 11.6.1.0から11.7.0.0へ
- NetWitness 11.6.1.1から11.7.0.0へ

11.7.0.0へのアップグレードの詳細については、『NetWitness 11.7アップグレード ガイド』を参照してください。

セキュリティ修正

セキュリティに関する修正の詳細については、『セキュリティ アドバイザリー』を参照してください。

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。

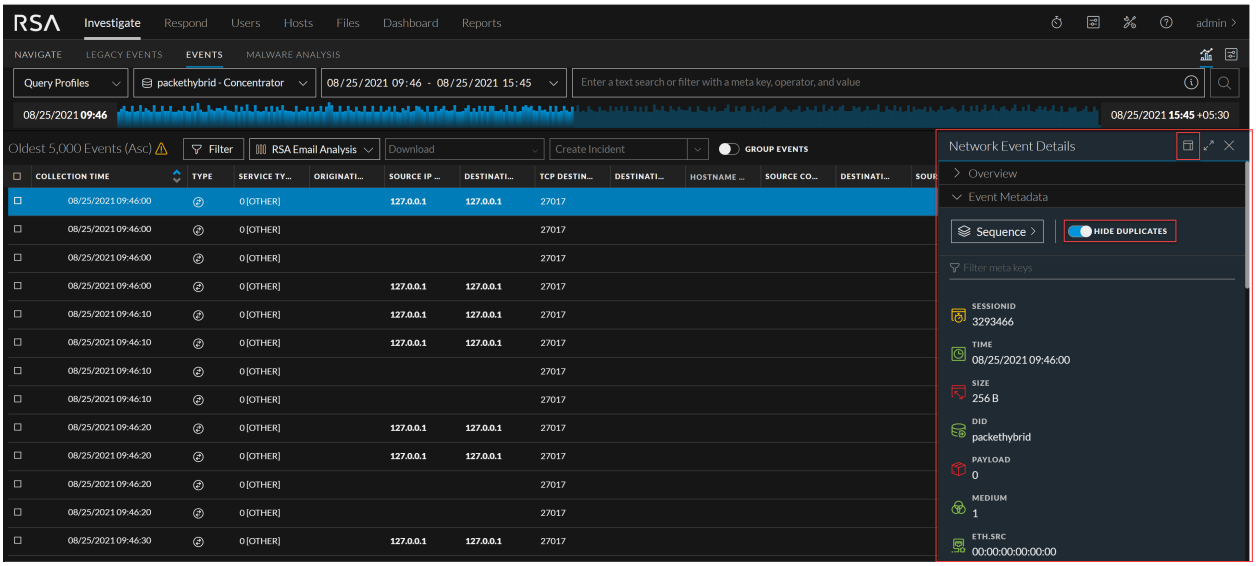
- 調査
- エンドポイントの調査
- Concentrator、Decoder、Log Decoderサービス
- Event Stream Analysis(ESA)
- プラットフォーム
- アップグレード
- NetWitnessサービス

このセクションに記載されているドキュメントを見つけるには、NetWitness 11.x Master Table of Contentsにアクセスしてください。製品ドキュメントには、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。

調査

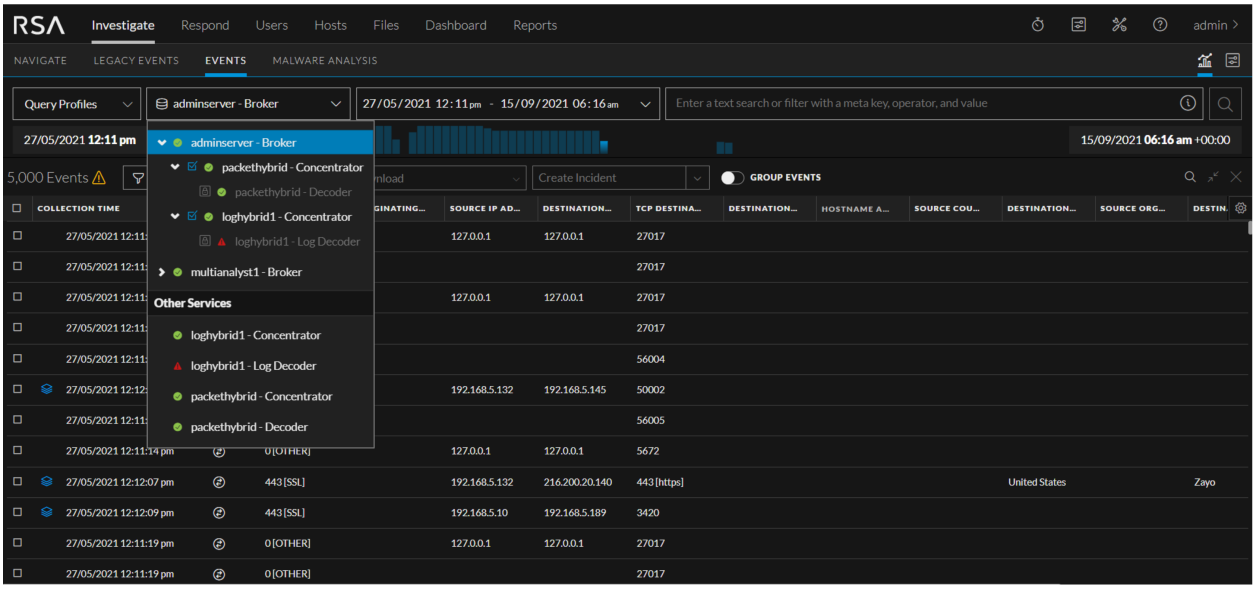
メタのみのイベントの再構築

アナリストがイベントをレビューするときに、新しいコンパクト メタデータ ビューと拡張メタデータ ビューでは、生データが存在しないユース ケースであっても、イベントの高レベルの詳細な情報を表示する代替ワークフローが提供されます。



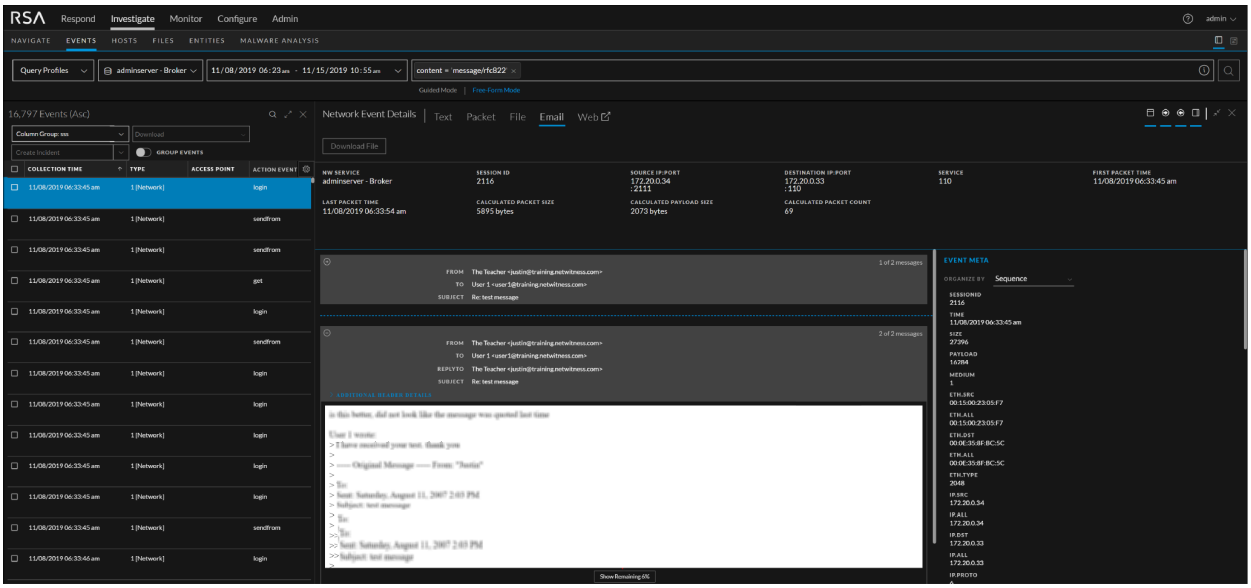
ブローカー クエリー エクスペリエンスの向上

トップレベルのブローカーでのアナリストのクエリーでは、デフォルトで、サブサービスの1つが接続できなくなったり、タイム アウトしたりしたときに部分的な結果が提供されるようになりました。さらに、ブローカーに接続されているものの階層ビューを使用して、アナリストは、必要な場合に、クエリーの前に特定のサブサービスを除外することができます。



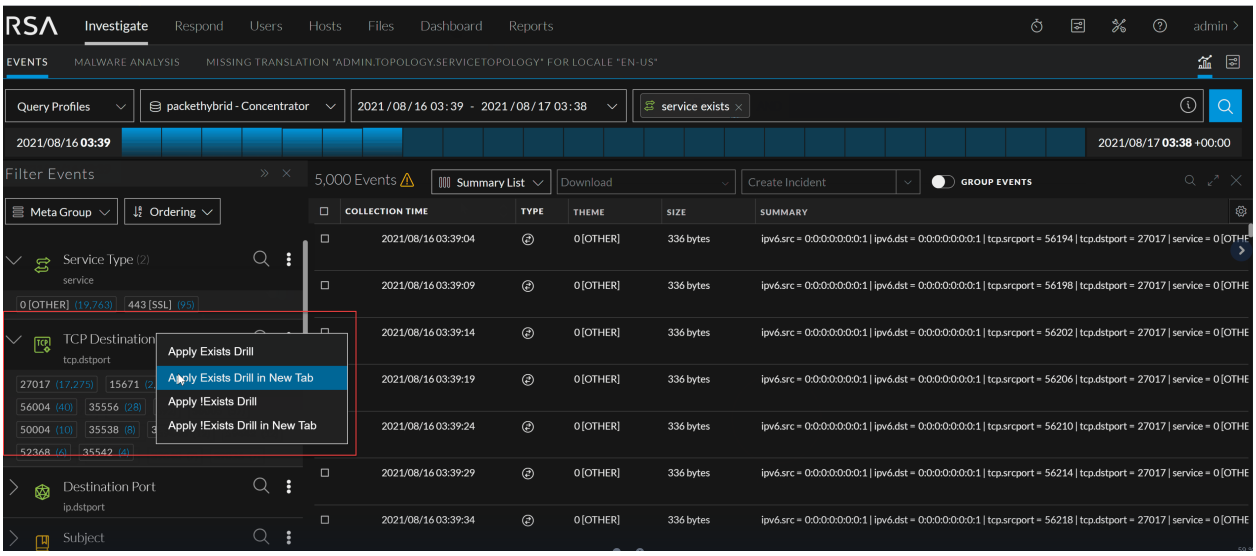
Eメールの再構築の改善

アナリストは、［Eメール］ビューに用意されている［すべてのEメールを展開］オプションを使用して、1回のセッションですべてのEメールの内容を表示することができます。



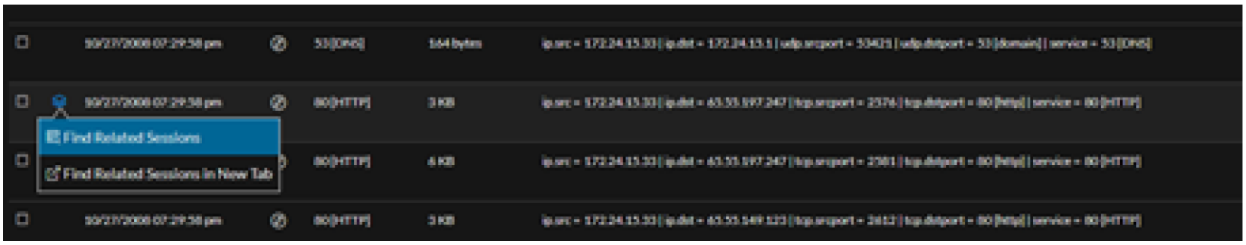
［イベント フィルター］パネルでのメタキーとクエリーの直接対話

メタ キー名を直接クリックして、メタ キーのみのクエリーを生成することにより、クエリーを作成するためのアナリストの手順が合理化されました。または、クエリー バーを直接操作することなく、［イベント フィルター］パネル内で、キーと値のペアの組み合わせによる検索を実行できます。



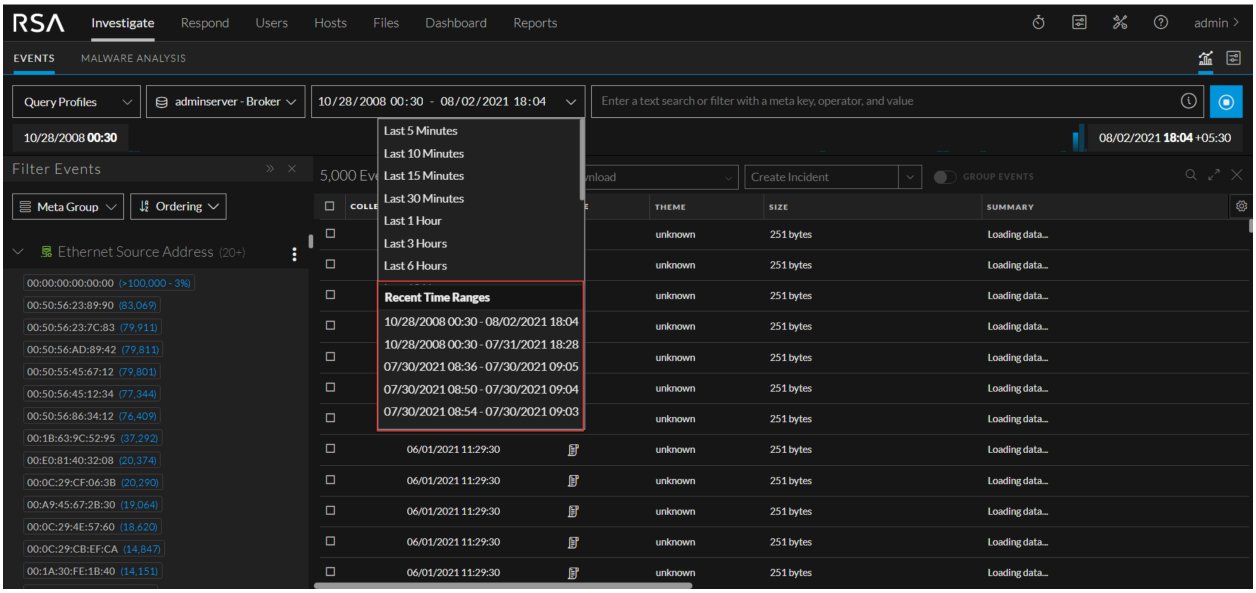
ネットワーク フラグメントの識別

アナリストは、イベントのアイコンにカーソルを合わせることで、イベントに関連するセッションを表示して、分析と調査を実行できます。



保存された時間範囲

アナリストは、最後に使用した5つの時間範囲を利用して将来の検索を行うことで調査時間を節約できます。保存された時間範囲は［最近の時間範囲］セクションに表示されます。

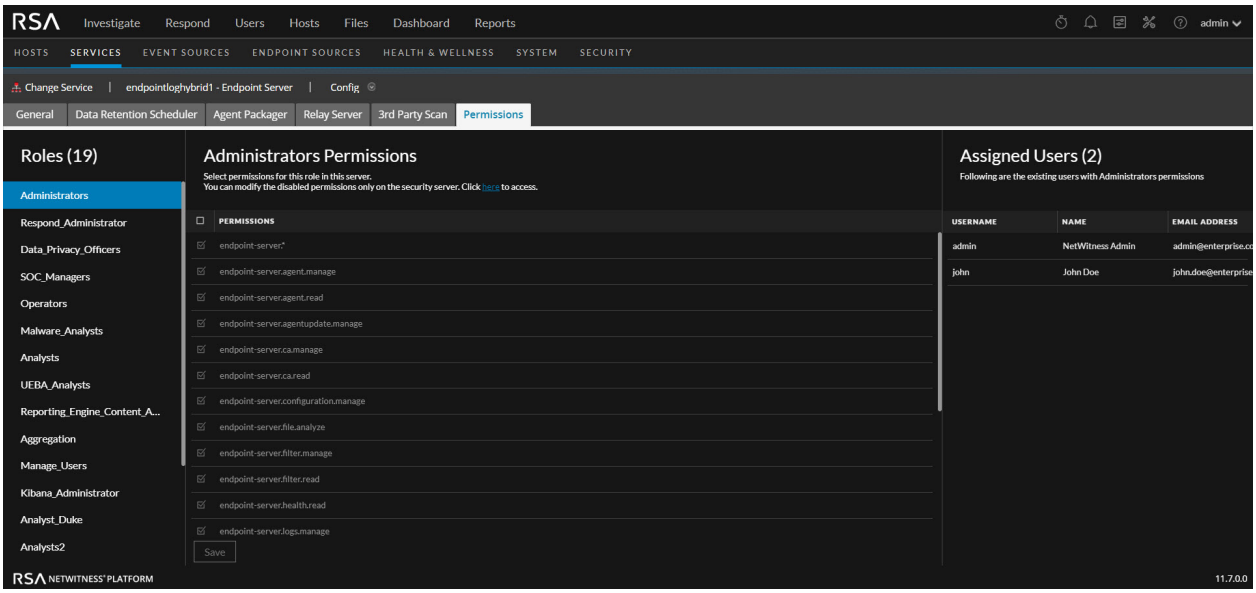


詳細については、『Investigateユーザー ガイド』を参照してください。

エンドポイントの調査

Endpoint Serverのロールベースのきめ細かいアクセス制御

強化されたRBAC(ロールベースのアクセス制御)を使用して管理者は、すべてではなく、特定のEndpoint Serverへのアクセスを許可したり、取り消したりできます。また、endpoint-server.file.analyzeおよびendpoint-server.tag.manageと呼ばれる新しいアクセス許可の追加により、ユーザー権限管理の柔軟性が向上します。個々のEndpoint Serverのアクセス許可の管理の詳細については、『NetWitness Endpoint構成ガイド』を参照してください。

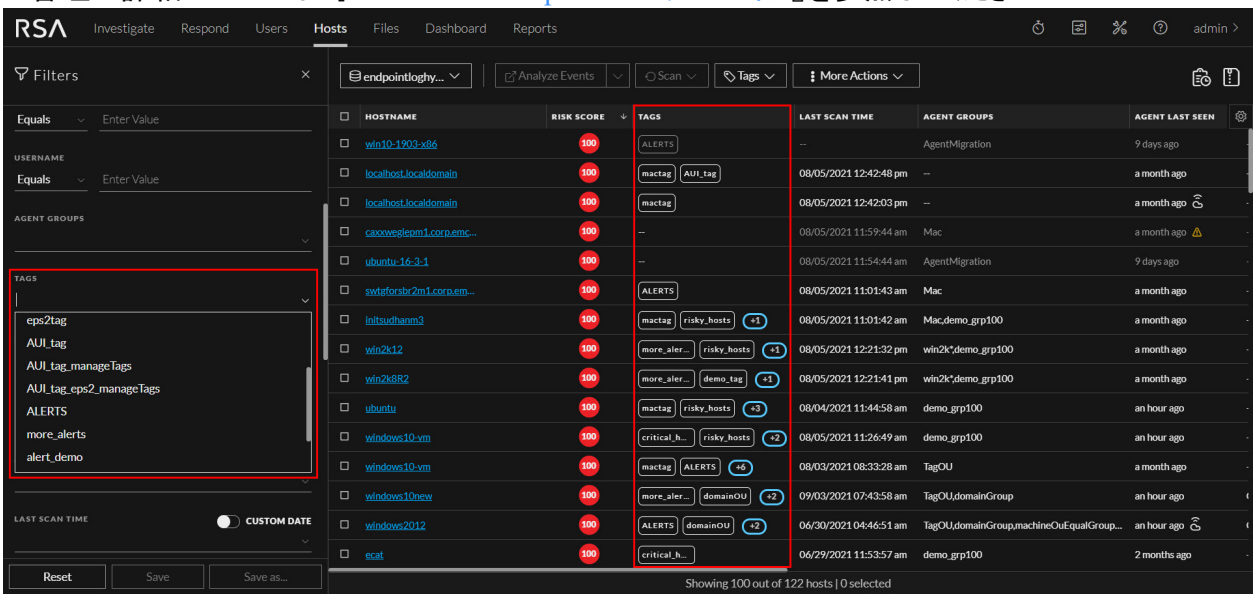


*endpoint-server.agent.manage*から削除され、*endpoint-server.file.analyze*に追加された権限

ファイルの分析、ローカル コピーの保存、OPSWATによるスキャンの権限は、*endpoint-server.agent.manage*から削除され、*endpoint-server.file.analyze*と呼ばれる新しい権限に追加されました。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』を参照してください。

タグを使用したホスト管理

アナリストは、ホストを管理するためのタグを作成できます。カスタム テキスト(英数字と特殊文字の組み合わせが可能)のタグを作成して、ホストに割り当てることができます。タグに基づいてホスト グループを作成し、[ホスト]ビューでフィルター ペインを使用してタグでホストをフィルター処理することができます。管理者は、タグの作成および割り当てと同時に、エージェント パッケージャーを生成することができます。これらのタグは、Endpointエージェントのインストール時にデフォルトでホストに追加されます。タグの管理の詳細については、『NetWitness Endpointユーザー ガイド』を参照してください。



拡張されたWindowsエージェントによる、レジストリーを対象とした永続化手法の検出のサポート

拡張されたWindowsエージェントにより、Windowsレジストリーを使用する永続化手法が検出されます。レジストリー モニターの信頼性が向上し、疑わしいアクティビティが、強化された方法で検出されます。詳細については、『NetWitness Endpointユーザ ガイド』を参照してください。

疑わしいスレッドの検出の強化

疑わしいスレッドの検出の機能のこの拡張により、さまざまな方法を使用して、疑わしいスレッドがより効果的に検出され、報告されるようになります。この機能拡張では、アナリストが、疑わしいスレッドに関連するすべての詳細と機能に、以前と同様にアクセスできます。詳細については、『NetWitness Endpointユーザー ガイド』を参照してください。

管理者特権で開いたコマンド プロンプトからの、ブロックされたファイルの削除

ホストで管理者特権で開いたコマンドプロンプトでdeleteコマンドを使用して、ホスト上のブロックされたファイルを削除できます。

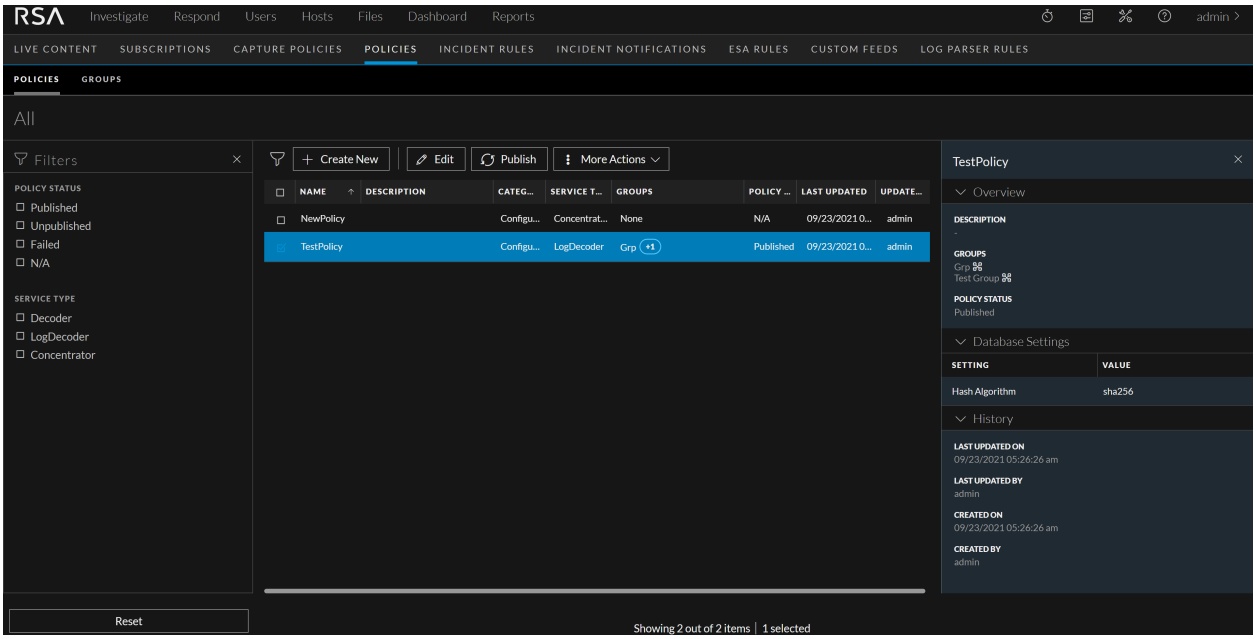
Concentrator、Decoder、Log Decoderサービス

一元化された構成管理の導入

一般的なNetWitnessコア サービス(Concentrator、Decoder、Log Decoder) の構成の管理を、単一のポリシーベースのインターフェイスから一元的に実行し、複数のサービスに分散することができます。一元化された構成管理により管理者は、以下を実行できます。

- 同様のハードウェア プロファイルまたは他の基準に基づいて、同じサービス タイプのグループを作成する
- ポリシーにCIを追加して設定をカスタマイズする。ポリシーに含まれない設定はデフォルトのままになる
- カスタマイズされた設定を、1つのステップで任意の数のサービスに適用する
- グループ内のすべてのサービスを再開して変更を適用する
- アイコンで示されるサービスの再開、未公開のポリシー、コンプライアンス違反のサービスなど、アクションが必要な場合に表示する
- ポリシーまたはグループへの変更をすばやく元に戻す

  詳細については、『ホストおよびサービス スタート ガイド』を参照してください。



クエリーの正確さの向上

オプションのインデックス構成をメタ キーごとに使用して、デフォルトのキー/値検索をNグラム レイアウトに拡張することができます。この組み合わせにより、クエリーおよびレポート機能を使用できるだけでなく、最大値のしきい値に達した場合でも、完全で正確な検索結果が得られます。

詳細については、『コア データベース チューニング ガイド』の「Nグラム」を参照してください。

Event Stream Analysis(ESA)

イベントとインシデントの永続化機能の強化

アナリストは、インシデントに含まれるイベントを永続化することによって、経過時間に関係なく、将来もインシデントを表示できるようになります。アナリストは次の操作を実行できます。

- インシデント レベルとアラート レベルで複数のイベントを固定するか、固定を解除する
- イベントが永続化された時期の詳細を表示する
- 永続化されたイベントのステータス(完了、一部完了、なし) を確認する
- 管理者は、ユーザーにアクセス許可を設定して、特定のインシデントに関連付けられたrawデータを永続化することができます。

詳細については、『Respondユーザー ガイド』を参照してください。

プラットフォーム

バックアップ機能とリストア機能の強化

新しく導入されたNetWitnessリカバリー ラッパー ツールにより、個々または複数のホストのバックアップとリストアが一元的に実行されます。このツールを使用すると、カスタム ファイルをリストアに組み込み、サポートされているすべての導入インストール(物理、仮想、クラウド) を処理することができます。

NetWitnessリカバリー ツールを使用して管理者は、以下を実行できます。

- 個々、特定、またはすべてのホストを一度にバックアップ(エクスポート) する
- 個々のホストを一台ずつリストア(インスポート) する
- バックアップおよびリストア中にファイルまたはフォルダーをカスタマイズする
- NetWitnessホストからリモート ホストの場所に(およびその逆方向に) バックアップ データをコピーする

詳細については、『*NetWitness*用NetWitnessリカバリー ツール ユーザー ガイド』の「ディザスター リカバリー(バックアップとリストア) 」トピックを参照してください。

アップグレード

アップグレード前チェック ユーティリティの導入

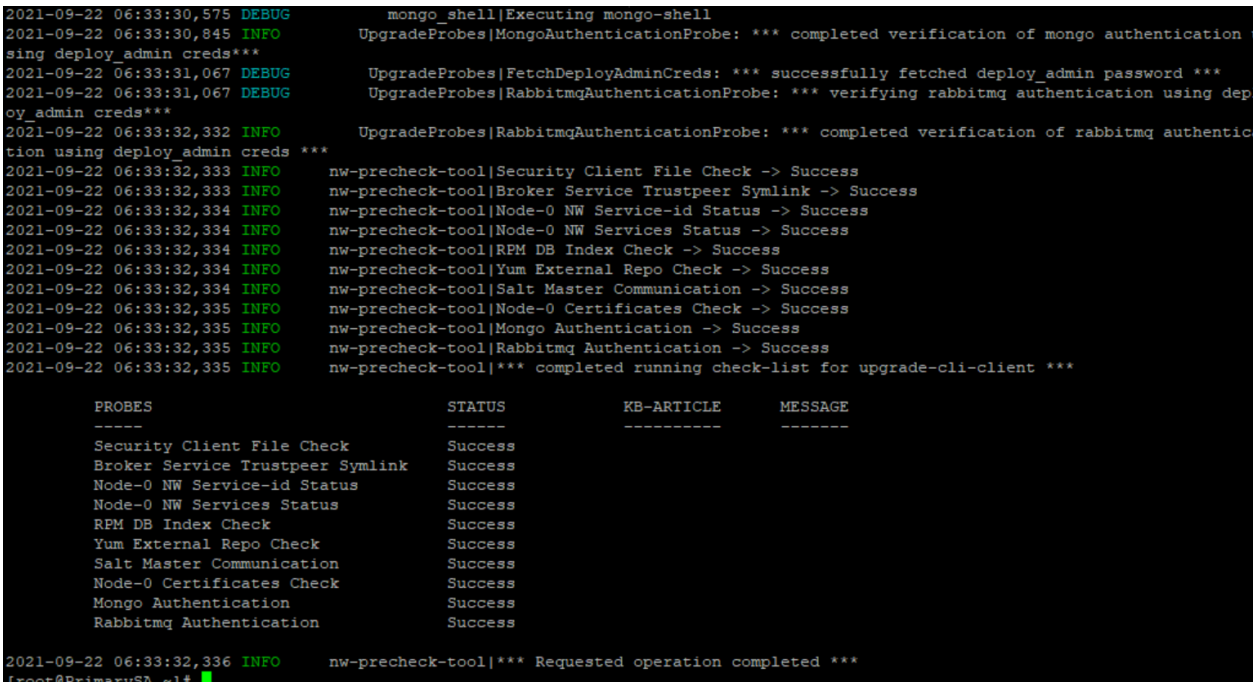
現在のNetWitnessセットアップを管理者が分析し、アップグレードに影響を与える可能性のある状態を特定するための新しいヘルス チェック ユーティリティが導入されました。問題が検出された場合は、アップグレードを続行する前に問題を解決できます。

アップグレード前チェックでは、次のことを確認します。

- **セキュリティ クライアント ファイル チェック** :`security-client-amqp.yml`ファイルが存在しないことを確認する
- **Node-0 NWサービスIDステータス** :すべてのサービスIDがノード0のサービスと一致していることを確認する

- **ブローカー サービストラストピア シンボリックリンク** :ブローカーのシンボリックリンク ファイル (`/etc/netwitness/ng/broker/trustpeers/`) が破損していないことを確認する
- **ノード0 NWサービス ステータス** :ノード0のすべてのサービスのステータスを確認する
- **Yum外部リポジトリー チェック** :外部リポジトリーが使用可能でないことを確認する
- **RPM DBインデックス チェック** :RPM DBが破損していないかどうかを確認する
- **ソルト マスター通信** :ノード0からすべてのノードへのソルト通信を確認する
- **ノード0証明書のチェック** :欠落しているか、期限が切れているか、無効な証明書があるかどうかを確認する
- **Mongo認証** :Mongoクライアントを使用して、`security-cli-client`から取得した`deploy_admin`認証情報を検証する
- **RabbitMQ認証** :RabbitMQを使用して、`security-cli-client`から取得した`deploy_admin`認証情報を検証する

詳細については、『NetWitness 11.7用 アップグレード ガイド』を参照してください。



NetWitnessサービス

NetWitnessサービストポロジー マップの導入

サービスの収集と集約を表すすべてのNetWitnessコア サービスの階層レイアウトのビューにより、管理者とアナリストは、サービスの導入や、オンラインまたはオフラインのサービスに関する洞察をすばやく得ることができます。このトポロジーには、Broker、Concentrator、Log Decoder、Packet Decoder、Hybrids、Log Collectorサービスのみが表示されます。詳細については、『システムおよびセキュリティ ユーザー管理ガイド』を参照してください。

注：Reporting Engine、Malware Analysis、UEBA、Endpoint Server、Cloud Linkサービス、Warehouse Connectorはサポートされていません。

修正された問題

このセクションでは、最後のメジャー リリース後に修正された問題のリストを提供します。修正された問題の詳細については、RSA Linkに掲載されている「RSA NetWitness® Platformの既知の問題リスト」の「修正された問題」列を参照してください。

管理の修正

追跡番号	説明
ASOC-105322、SACE 14678	NetWitness Active Directory外部グループ マッピングは、同じ名前の異なるドメインに対する同じグループ名をサポートしていません。

セキュリティ修正

管理の修正

追跡番号	説明
ASOC-112493	[構成] > [キャプチャ ポリシー]で、新しいキャプチャ ポリシーを作成しようとすると、キャプチャ ポリシーの導入が失敗します。その結果、[公開ステータス]と[サービスの割り当て]でステータスが[失敗]として表示されます。
ASOC-112805	[管理者] > [システム] > [ジョブ]で他のユーザーが作成した[イベント]と[ジョブ]のどちらのダウンロードも管理者には許可されません。

Context Hubの修正

追跡番号	説明
ASOC-112636	[構成] > [カスタム フィード] > [フィード]でSTIXカスタム フィードを構成している間に、ソース、タイムスタンプ、信頼度、参考資料などの観測データ(STIX xmlファイルで *sightings_count=1*) を[列の定義]プレビューで使用できません。

ログ収集の修正

追跡番号	説明
ASOC-112547	[構成]ウィンドウの[Local Collector] > [宛先グループ]で、50を超えるリモートの宛先のLog Collectorを追加すると、ページ設定が機能しません。その結果、50を超える宛先Log CollectorはUIには表示されません。

エンドポイントの修正

追跡番号	説明
ASOC-112285	Endpoint Serverの1つにファイル(別の複数のEndpoint Serverに存在する) をダウンロードした後、ファイルのローカル コピーを、他のEndpoint Server(ファイルがダウンロードされていない) から保存しようとすると、エラー メッセージ「**ダウンロードは失敗しました。詳細については、監査ログを確認してください。**」が表示されます。ファイルのダウンロード ステータスが [**ダウンロード済み**] から [**ファイルがサーバーで削除済み**] に変更されます。

対応の修正

追跡番号	説明
ASOC-111459	[**構成**] > [**インシデント ルール**] ページでインシデント ルールを編集し、変更を保存すると、しばらくした後に、その変更が元に戻されます。したがって、これらのインシデント ルールに関連付けられているインシデントが、新しい変更に従って作成されません。

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 11.xマスター目次	https://community.rsa.com/t5/netwitness-platform-online/rsa-netwitness-platform-11-x-master-table-of-contents/ta-p/567788
NetWitness 11.7製品ドキュメント	https://community.rsa.com/t5/netwitness-platform/ct-p/netwitness-documentation
NetWitness 11.7アップグレード ガイド	https://community.rsa.com/t5/netwitness-platform-online/upgrade-to-netwitness-platform-11-7/ta-p/655210

製品ドキュメントへのフィードバック

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

NetWitness Platformのヘルプ情報

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。
  HTML：https://community.rsa.com/community/products/netwitness/documentation
- 特定のグループを見つけるには、RSA Linkの［**検索**］フィールドを使用します。
  https://community.rsa.com/
- NetWitnessのナレッジベース：https://community.rsa.com/community/products/netwitness/knowledge-base
- NetWitnessのトラブルシューティング：https://community.rsa.com/community/products/netwitness/documentation/troubleshooting
- NetWitnessブログの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RSA NetWitness Platform製品またはアプリケーションのバージョン
- 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。

RSA Link	https://community.rsa.com メイン メニューで、［**サポート**］>［**ケース ポータル**］>［**ケースの管理**］の順に選択します。
各国のお問い合わせ窓口	https://community.rsa.com/t5 https://community.rsa.com/t5/support-information/how-to-contact-rsa-support/ta-p/563897-information/how-to-contact-rsa-support/ta-p/563897
コミュニティ	https://community.rsa.com/t5/rsa-Community/ct-p/support

ビルド番号

以下の表は、NetWitness 11.7.0.0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 Audit Plugins	rsa-audit-plugins-11.7.0.0-4695.5.36a93c8d9.el7.noarch.rpm
NetWitness Appliance	rsa-nw-appliance-11.7.0.0-12232.5.66442bab8.el7.x86_64.rpm
NetWitness Archiver	rsa-nw-archiver-11.7.0.0-12232.5.66442bab8.el7.x86_64.rpm
NetWitness Broker	rsa-nw-broker-11.7.0.0-12232.5.66442bab8.el7.x86_64.rpm
NetWitness Concentrator	rsa-nw-concentrator-11.7.0.0-12232.5.66442bab8.el7.x86_64.rpm
NetWitness Config Management	rsa-nw-config-management-11.7.0.0-2109091739.5.be0ffac.el7.noarch.rpm
NetWitness Config Server	rsa-nw-config-server-11.7.0.0-210908042413.5.a52e0dc.el7.centos.noarch.rpm
NetWitness Console	rsa-nw-console-11.7.0.0-12232.5.66442bab8.el7.x86_64.rpm
NetWitness Content Server	rsa-nw-content-server-11.7.0.0-210906060842.5.022d0d1.el7.centos.noarch.rpm
NetWitness ContextHub Server	rsa-nw-contexthub-server-11.7.0.0-210908050143.5.589ec75.el7.centos.noarch.rpm
NetWitness Correlation Server(ESA)	rsa-nw-correlation-server-11.7.0.0-210914062311.5.730e55a.el7.centos.noarch.rpm
NetWitness Decoder	rsa-nw-decoder-11.7.0.0-12232.5.66442bab8.el7.x86_64.rpm
NetWitness Deployment Upgrade	rsa-nw-deployment-upgrade-11.7.0.0-2105111629.5.286995c.el7.noarch.rpm
NetWitness Endpoint Agents	rsa-nw-endpoint-agents-11.7.0.0-2109081645.5.da02ba9.el7.x86_64.rpm
NetWitness Endpoint Broker Server	rsa-nw-endpoint-broker-server-11.7.0.0-210928085116.5.ad9d4df.el7.centos.noarch.rpm
NetWitness Endpoint Server	rsa-nw-endpoint-server-11.7.0.0-210908061251.5.fc23872.el7.centos.noarch.rpm
NetWitness Integration Server	rsa-nw-integration-server-11.7.0.0-210908043046.5.db06a9d.el7.centos.noarch.rpm
NetWitness Investigate Server	rsa-nw-investigate-server-11.7.0.0-210908094032.5.dd152ed.el7.centos.noarch.rpm
NetWitness Legacy Web Server	rsa-nw-legacy-web-server-11.7.0.0-210909082049.5.751fea3.el7.centos.noarch.rpm

NetWitness License Server	rsa-nw-license-server-11.7.0.0-210908100642.5.3aee2de.el7.centos.noarch.rpm
NetWitness Log Collector	rsa-nw-logcollector-11.7.0.0-14991.5.3a09b7b7d.el7.x86_64.rpm
NetWitness Log Decoder	rsa-nw-logdecoder-11.7.0.0-12232.5.66442bab8.el7.x86_64.rpm
NetWitness Log Player	rsa-nw-logplayer-11.7.0.0-12232.5.66442bab8.el7.x86_64.rpm
NetWitness Malware Analytics Server	rsa-nw-malware-analytics-server-11.7.0.0-210830055027.5.a674232.el7.centos.x86_64.rpm
NetWitness Metrics Server	rsa-nw-metrics-server-11.7.0.0-210907081327.5.411da23.el7.centos.noarch.rpm
NetWitness Orchestration Server	rsa-nw-orchestration-cli-11.7.0.0-2107281202.5.da1fa1d.el7.noarch.rpm
NetWitnessリカバリ ツール	rsa-nw-recovery-tool-11.7.0.0-2109201121.5.407f9ac.el7.noarch.rpm
NetWitness Reporting Engine Server	rsa-nw-re-server-11.7.0.0-5903.5.a09535ea0.el7.x86_64.rpm
NetWitness Respond Server	rsa-nw-respond-server-11.7.0.0-210914062602.5.b62650d.el7.centos.noarch.rpm
NetWitness Root CA Update	rsa-nw-root-ca-update-11.7.0.0-2105111632.5.7e09f04.el7.noarch.rpm
NetWitness SDK	
NetWitness Security Server	rsa-nw-security-server-11.7.0.0-210816032325.5.c946840.el7.centos.noarch.rpm
NetWitness Source Server	rsa-nw-source-server-11.7.0.0-210906022225.5.12e033b.el7.centos.noarch.rpm
NetWitnessユーザ インターフェイス	rsa-nw-ui-11.7.0.0-210907091711.5.65a67f4557.el7.centos.noarch.rpm
NetWitness Workbench	rsa-nw-workbench-11.7.0.0-12232.5.66442bab8.el7.x86_64.rpm
NetWitness SA Tools	rsa-sa-tools-11.7.0.0-2109140601.5.680134e.el7.noarch.rpm
NetWitness SMS Runtime	rsa-sms-runtime-rt-11.7.0.0-4695.5.36a93c8d9.el7.x86_64.rpm
NetWitness SMS Server	rsa-sms-server-11.7.0.0-4695.5.36a93c8d9.el7.x86_64.rpm

改訂履歴

日付	説明
2021年11月	ベータ