RSA NETWITNESS® PLATFORM

リリース ノート

RSA NetWitness® Platform 11.4.1.0

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。

使用許諾契約

本ソフトウェアと関連ドキュメントは、Dell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

本製品はRSA 以外のサードパーティ製ソフトウェアを実装している場合があります。本製品を使用することにより、本製品のユーザは、本製品に含まれているサード 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

掲載される情報は、公開した時点でDellが正確であるとみなす情報であり、この情報は予告なく変更されることがあります。

10月 2020

目次

新機能

このドキュメントは、NetWitness Platform 11.4.1.0の機能拡張と修正について記述しています。NetWitness Platform 11.4.1.0の新規導入や更新を行う前にお読みください。

アップグレード パス

NetWitness Platform 11.4.1.0は次のアップグレード パスをサポートしています。

- RSA NetWitness® Platform 11.2.x.xから11.4.1.0
- RSA NetWitness® Platform 11.3.0.xから11.4.1.0
- RSA NetWitness® Platform 11.3.1.xから11.4.1.0
- RSA NetWitness® Platform 11.3.2.xから11.4.1.0
- RSA NetWitness® Platform 11.4.0.xから11.4.1.0

11.4.1.0へのアップグレードの詳細は、『Upgrade Guide for RSA NetWitness Platform 11.4.1』を参照してください。

機能拡張

NetWitness Platform 11.4.1.0は、次の機能拡張を提供します。

- カスタマ エクスペリエンス向上プログラム
- 調査
- Decoder、Log Decoder、Log Collectorサービス
- 管理
- 統合
- ESA(Event Stream Analysis)

カスタマ エクスペリエンス向上プログラム

RSA NetWitness Platformカスタマ エクスペリエンス向上プログラム(CEIP: Customer Experience Improvement Program) は、RSA NetWitnessを継続的に改善するためのイニシアティブです。お客様がCEIPを有効化すると、個々のユーザのRSA NetWitness Platformでの作業状況が分析されます。その際、ユーザのワークフローに割り込みを行ったり、ユーザ個人を特定することはありません。このプログラムにより、RSAはお客様の導入環境やライセンス利用状況に関する洞察と、表示されたページや実行されたアクションに関する分析を取得します。RSAはこれらの分析情報を将来のリリースに追加する新機能や拡張機能の優先度を決定するために使用します。詳細は、『*System Configuration Guide*』で「Configure the Customer Experience Improvement Program」を参照してください。

注： バージョン11.4.0.xまでは、RSA Live Feedbackのオプションとして Additional Feedback Insights(付加的なFeedback Insights) を提供していました。この機能はCEIPに包含されるため、今後このオプションを個別に選択することはできません。

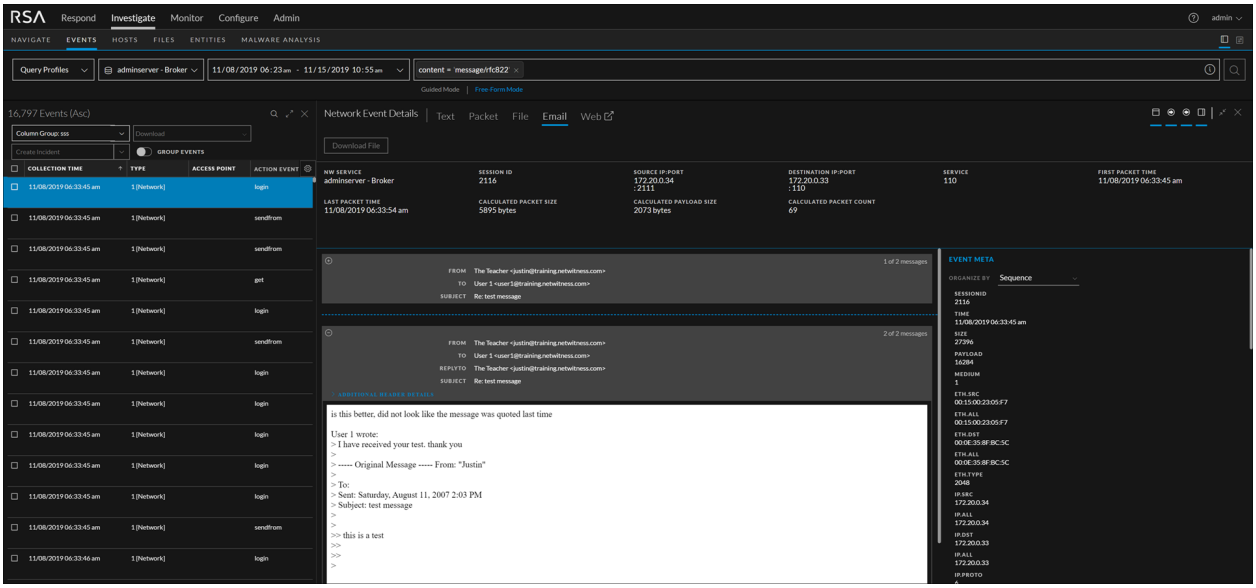
調査

イベント調査のパフォーマンス向上

調査のパフォーマンスが大幅に向上し、[イベント]ビューでのページの読み込み、再構築、右クリックの応答時間がより高速になりました。

[イベント]ビューでのメール再構築の改善

[イベント]ビューでメール再構築を簡単に実行できるよう再設計されました。アナリストは、[レガシー イベント]ビューでのメール再構築のフローと同様に、[イベント]ビューから直接メール セッションを再構築できます。詳細は、『*Investigate ユーザ ガイド*』で「[イベント]ビューでのイベントの再構築」を参照してください。



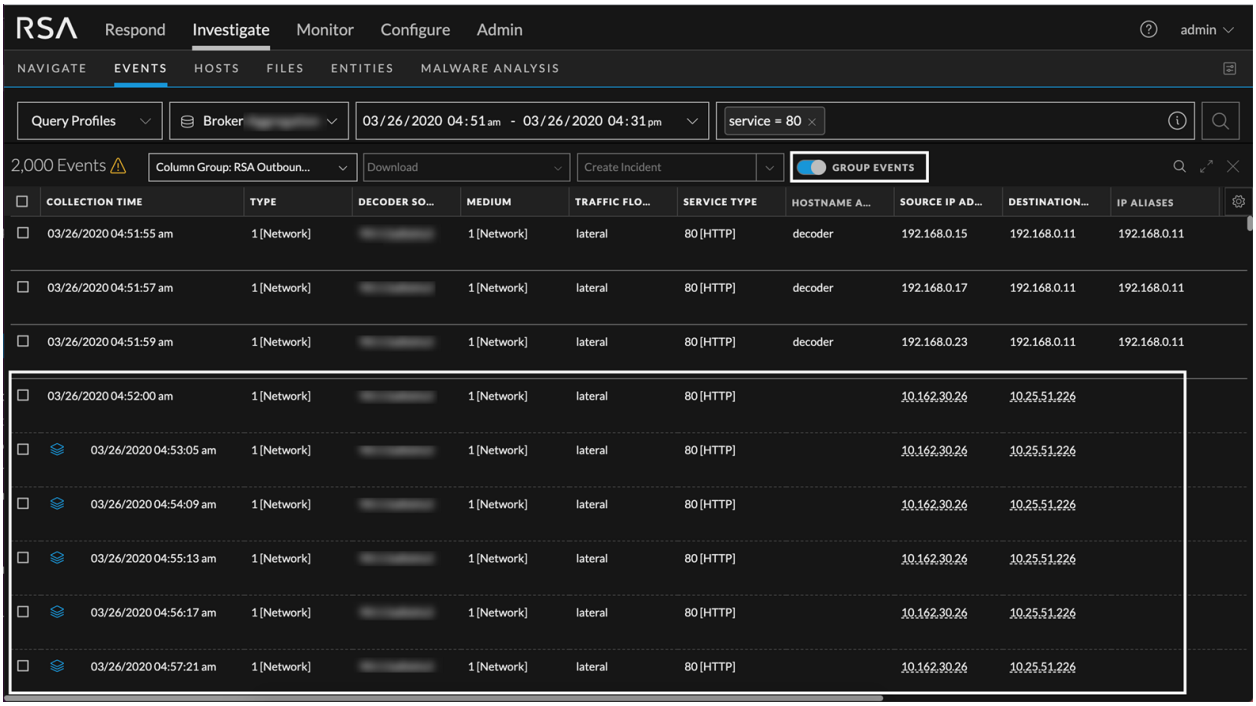
[イベント]ビューでの分割セッションと関連イベントのグループ化

[イベント]ビューには、デフォルトで、分割セッション内の各イベントと関連セッションがパースされた順に表示されます。その結果、関連イベントがリストの一か所にまとめて表示されない場合があります。分割セッションは次の理由により発生します。

- 元のイベントに含まれるトランザクションごとに個別のイベントが作成されたため、元のイベントが複数のサブパーツに分割された。
- 元のセッションのサイズがAssembler Maximum Size(デフォルト=32 MB) を超えるため、Network Decoderが取り込む際に分割された。
- 元のセッションの時間がAssembler Timeout Session(デフォルト=60秒) を超えるため、Network Decoderが取り込む際に分割された。

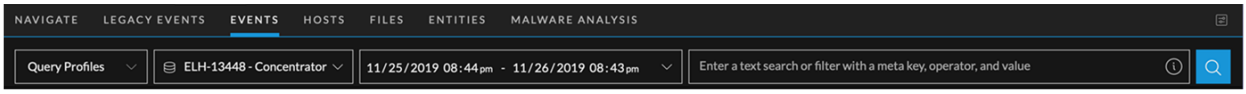
関連イベントは分割セッションとは異なります。関連イベントは、パターンに基づき、精査する価値のあるイベントがすぐにわかるようグループ化されたものです。各イベントは同じソースIPアドレス、宛先IPアドレス、ソース ポート、宛先ポートを持ちます。

イベント グループ機能は、キャプチャされたデータの中からより簡単に関係を検出できるよう、イベントをグループ化します。ユーザ インタフェースには、主イベントの下に後続イベントがネストされた状態で表示されるため、主イベントと後続イベントを簡単に把握できます。詳細は、『*IInvestigate ユーザ ガイド*』で「[イベント]ビューと[レガシー イベント]ビューでの分割セッションおよび関連セッションのイベントのグループ化」を参照してください。



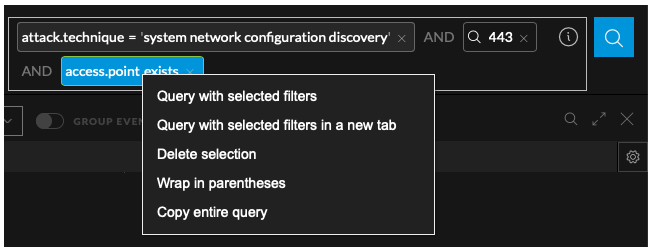
[イベント]ビューでのクエリ作成の高速化、簡略化

より簡単かつ高速にフィルタを作成し、クエリを構築できるよう、継続的にユーザ インタフェースの機能向上が行われています。詳細は、『*IInvestigate ユーザ ガイド*』で「[イベント]ビューでのイベントのフィルタリング」を参照してください。



- **ガイド モードの強力な自動入力機能と値候補表示機能、フリー フォーム クエリの入力および貼り付けが、モード切り換え不要で完全に統合されました。**クエリ バーに入力、貼り付けされたテキストは、簡易フィルタまたはフリー フォーム フィルタとして適切に解釈されます。メタ キー、演算子、値のシーケンスを入力し、Enterキーを押すことなく入力を続けた場合、自動的にフリー フォーム モードのオプションが有効になり、クエリの入力を続けることができます。
- **クエリ全体をクリップボードにコピーするオプションが追加されました。**1つのフィルタを選択して右クリックし、[**Copy entire query**]を選択します。クリップボードにコピーされた内容を他のアナリストと共有し

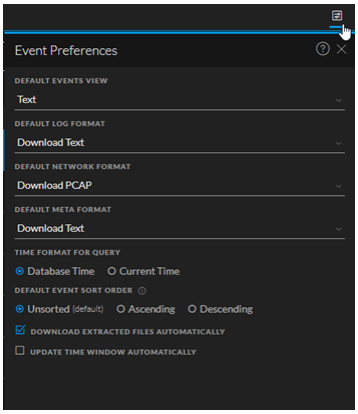
たり、クエリ バーに張り付 けることができます。



- **[イベント]ビューのクエリ バーでフィルタを作 成する時 、キーボード コマンドを使 用してすべてのフィル タを選 択(MacOSではCmd＋A、WindowsではCtrl＋A) し、クリップボードにコピー(MacOSでは Cmd＋C、WindowsではCtrl＋C) できます。**クリップボードにコピーしたテキストは、他 のアナリストと 共 有したり、クエリ バーに貼り付 ける(MacOSではCmd＋V 、WindowsではCtrl＋V) ことができま す。
- **クエリ作 成 時 のユーザ操 作 性を向 上 するため、フィルタ入 力 時 にメタ キーの後 に区 切りスペースなし で演 算 子(!=、=、<、<=、>、>=) が入 力 された場 合 、正 しい入 力 として受 け入 れるようになりまし た。**クエリ バーのフィルタには、メタ キーと演 算 子 の間 、演 算 子と値 の間 にスペースが必 要 です。フィ ルタ入 力 時 に値 や演 算 子 の候 補 を自 動 表 示 するため、原 則 としてほとんどの演 算 子 は区 切りス ペースを入 力 してから入 力 する必 要 があります。これらの演 算 子 が区 切りスペースなしで入 力 された 場 合 でも、値 の候 補 が自 動 的 に表 示 され、メタ キーと演 算 子 の間 には自 動 的 にスペースが追 加 さ れます。

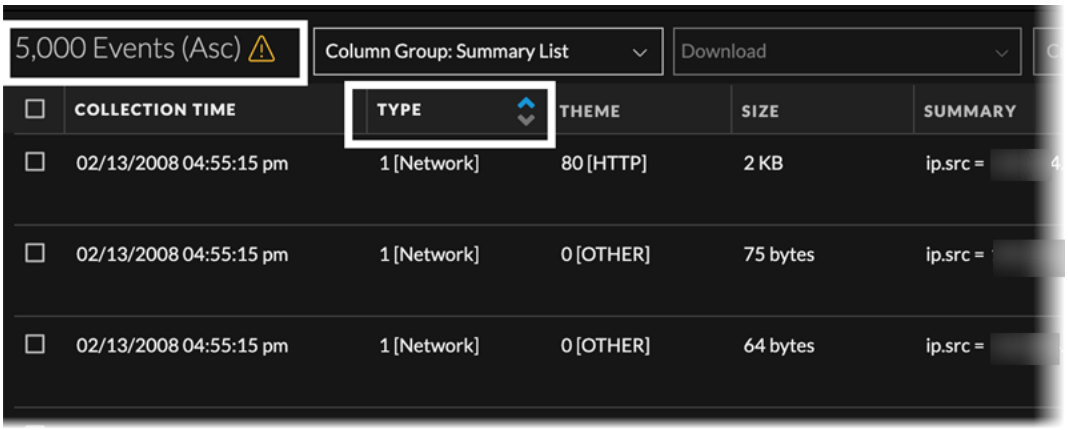
[イベント]ビューのイベント リストをソートなしで表 示 可 能 に

昇 順 または降 順 にソートしてイベントを表 示 するのに加 え、ソートなしで、コア サービスが処 理 した順 に イベントを表 示 するよう環 境 設 定 できます。ソートなしの場 合 、処 理 が高 速 になります。これは、一 致 するイベントが見 つかったら即 座 に表 示 するのと、すべてのコア サービスの応 答 を待 ってから指 定 された 順 に結 果 を並 べ替 えて表 示 する違 いによるものです。[ソートしない]を選 択 した場 合 、一 番 先 に一 致 したイベントから、ソートすることなくリストに表 示 されます。詳 細 は、『*Investigate ユーザ ガイド*』で 「[イベント]ビューの構 成 」を参 照 してください。



列 のソート設 定 の操 作 性 向 上

[イベント]リストの列 のソート設 定 が見 やすく、使 いやすくなりました。各 列 の昇 順 、降 順 を選 択 する矢 印 が目 立 つようになり、選 択 済 みの矢 印 を2回 目 にクリックすると簡 単 にソートなしの状 態 に戻 すことが できます。詳 細 は、『*IInvestigate ユーザ ガイド*』で「イベント リストでの列 と列 グループの使 用 」を参 照 し てください。



Decoder、Log Decoder、Log Collectorサービス

Log Decoderでのカスタム証明書の構成

Log Decoder上のSyslogリスナにカスタム証明書を構成できるようになりました。これにより、Syslogリスナで独自の信頼する証明書を使用できます。他のすべての機能では引き続きプリインストールされた証明書が使用されます。詳細は、『*Decoder Configuration Guide*』で「(Optional) Configure Custom Certificates on Log Decoders」を参照してください。

Log Collectorでのカスタム証明書の構成

Log Collector上のSyslogリスナにカスタム証明書を構成できるようになりました。これにより、Syslogリスナで独自の信頼する証明書を使用できます。他のすべての機能では引き続きプリインストールされた証明書が使用されます。詳細は、『*Log Collection Configuration Guide*』で「(Optional) Configure Custom Certificates on Log Collectors」を参照してください。

Log Collectorでのアドレス(IP/ホスト名) または名前によるイベント ソース検索

Log Collectorには、収集プロトコル(例 : ファイル収集) ごとに多くの事前構成されたイベント ソースが表示されます。イベント ソースのアドレス(IP/ホスト名) または名前によって検索し、目的のイベント ソースをより簡単に見つけられるようになりました。詳細は、『*Log Collection Configuration Guide*』で「Log Collection Event Sources Tab」を参照してください。

SSL/TLS証明書のSHA-256拇印のメタ データ生成

Network Decoderは、SHA-1ハッシュ形式に加えて、SSL/TLS証明書のSHA-256拇印のメタ データを生成し、調査と分析に使用できるようになりました。詳細は、『*Decoder Configuration Guide*』で「TLS Certificate Hashing」を参照してください。

管理

イベント ソース履歴チャートを[ヘルスモニタ]からイベント ソース管理に移動

履歴チャートを除き、イベント ソースに関するすべての情報は[ヘルスモニタ]ビューから、[イベント ソース]>[管理]ビューに既に移動していました。**11.4.1では、履歴チャートが移動しました。**以前のリリースでは、**[管理]>[ヘルスモニタ]**ビューの**[イベント ソース モニタリング]**タブから履歴チャートを表示できました。11.4.1では、**[管理]>[イベント ソース]**ビューの**[管理]**タブから表示できます。詳細は、『*Event Sources Management User Guide*』で「Historical Graph for System Stats」を参照してください。

Analyst UIでのSSO認証のサポート

複数のNetWitness Platformユーザ インタフェース インスタンスを導入した環境で、アナリストのシングル サイン オン(SSO) がサポートされるようになりました。

deploy_adminアカウントの管理を簡略化

deploy_adminアカウントは、すべてのNetWitness Platformで使用されるパスワード ベースのシステム アカウントです。deploy_adminアカウントは、すべてのホストで同期させておく必要があります。お客様の環境のポリシーによっては、このアカウントのパスワードを定期的に更新しなければならない場合があります。11.4.1以降、deploy_admin のパスワードは、NetWitness Server上のnw-manageスクリプトで一元的に管理できるようになりました。nw-manageスクリプトを実行すると、deploy_adminアカウントを使用するすべてのNetWitness Platformコンポーネント ホスト上でパスワードが更新されます。詳細は、『*System Maintenance Guide*』で「Manage the deploy_admin Account」を参照してください。

ウォーム スタンバイNW ServerのIPアドレス変更

セカンダリNW ServerのIPアドレスが、プライマリNW Serverと異なる場合、手動でフェイルオーバー処理を実施し、ウォーム スタンバイNW ServerのIPアドレスを変更することができます。手順の詳細は、『*Deployment Guide*』で「Fail Over Primary NW Server to Secondary NW Server with Different IP Address 」を参照してください。

統合

RSA SecurID Accessへの高リスク ユーザ名の転送をサポート

NetWitness PlatformとRSA SecurID Accessの統合により、NetWitness Respond Serverはインシデントに含まれる高リスク ユーザのActive Directoryユーザ名をRSA SecurID Accessに送信できます。Respond Serverでメタ データを構成する方法について、『*Respond Configuration Guide*』を参照してください。

ESA(Event Stream Analysis)

Nw-ShellでESAルール導入環境のトラブルシューティング メトリックを表示

Nw-Shellを使用して、ESA Correlation Serverから、各ESAルール導入環境のメトリックを表示できます。これらのメトリックには、導入環境で使用するデータ ソースのセッション数、ルールのメモリ使用状況などが含まれます。詳細は、『*Alerting with ESA Correlation Rules User Guide* 』で「Obtain Correlation Server Metrics for ESA Rule Deployment Troubleshooting Using Nw-Shell」を参照してください。

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。

セキュリティ修正

追跡番号	説明
ASOC-90460	CentOS 7 kernel security Update - https://access.redhat.com/errata/RHSA-2020:0374
ASOC-89324	CentOS 7 qemu-kvm Security Update - https://access.redhat.com/errata/RHSA-2020:0366
ASOC-89323	CentOS 7 kernel-rt Security Update - https://access.redhat.com/errata/RHSA-2020:0375
ASOC-88972	CentOS 7 java-1.8.0-openjdk Security Update - https://access.redhat.com/errata/RHSA-2020:0196
ASOC-88273	CentOS 7 fribidi Security Update - https://access.redhat.com/errata/RHSA-2019:4326
ASOC-88034	CentOS 7 java-11-openjdk Security Update - https://access.redhat.com/errata/RHSA-2020:0122
ASOC-87935	CentOS 7 SDL Security Update - https://access.redhat.com/errata/RHSA-2019:4024
ASOC-87912	CentOS 7 nss, nss-softokn, nss-util Security Update - https://access.redhat.com/errata/RHSA-2019:4190
ASOC-87313	CentOS 7 tcpdump Security Update - https://access.redhat.com/errata/RHSA-2019:3976
ASOC-87312	CentOS 7 kernel security Update - https://access.redhat.com/errata/RHSA-2019:3979

ログ収集の修正

追跡番号	説明
SACE-12961/ ASOC-89784	WinRMチャネルがPULL応答でブックマークとして1を返すと、ブックマークファイルが正しく動作しなくなりました。

管理の修正

追跡番号	説明
SACE-12969/ ASOC-90751	ユーザがNetWitness Platformにログインすると、前にログインしていたユーザの権限が適用されました。
SACE-12753	カスタム フィードの構成時、URLパスのホスト名だけが検証され、ファイル名とパスが検証されませんでした。
SACE-12563	フィードを編集する時、それまで選択していた導入先のデバイス グループが選択されていないため、現在どのデバイス グループに導入しているか判断できません。
SACE-11456/ ASOC-89259	NetWitness Platformユーザ インタフェースの応答が非常に遅く、30～45秒かかりました。

調査の修正

追跡番号	説明
ASOC-92592	UEBAのイベント調査時に、スラッシュ文字を含むメタ値から移行すると、[調査]>[イベント]ビューに結果が何も表示されませんでした。
ASOC-88157	FTPセッションからファイル名を取得するため、[調査]>[イベント]ビューでイベントを再構築する際、FTPシステム パーサで、ip.dstの代わりに間違ったメタ キー(ip.src) でクエリが実行されました。
SACE-13028	[イベント]ビューまたは[レガシー イベント]ビューから、ログをXML形式でエクスポートする時、不正な終了タグが使用されていました。正しい終了タグ`</Logs>`の代わりに、`<Logs/>`が使用されていました。
SACE-12498	ブラジルでの夏時間廃止後、プロファイルに構成されたタイムゾーン(Americas/Sao Paulo GMT -3) と[調査]ビューおよび[対応]ビューで使用されるタイムゾーン(Americas/Sao Paulo GMT -2) に1時間のずれがありました。

対応の修正

追跡番号	説明
ASOC-90551	[対応]ビューでテキスト再構築を使用する時、圧縮されたペイロードが表示されませんでした。 11.3.2および11.4でも、[対応]ビューで圧縮されたペイロード(例:gzip)を含むネットワーク セッションをパケット再構築する時に同様の状況が発生していました。
ASOC-88665	Respond Serverは、エンドポイントのファイル アラートにSHA256チェックサムが含まれていない場合、アラートの処理を停止する場合がありました。 11.3.2および11.4でも、問題のあるファイルのSHA256ハッシュを含んでいないエンドポイント イベントから生成されたアラートを処理する時、Respond Serverがアラートの処理を停止する場合がありました。その結果、アラートのリスク スコアの計算が失敗し、それ以降のアラートの処理でもエラーが発生していました。

ヘルスモニタの修正

追跡番号	説明
SACE-12973	[**管理**]>[**ヘルスモニタ**]>[**システム統計ブラウザ**]タブに、ファンのステータスとシステムの温度が表示されていませんでした。

コア サービス(Broker、Concentrator、Decoder、Archiver)の修正

追跡番号	説明
SACE-13098/ ASOC-87266	Packet Decoderが9.6Gで収集しているにもかかわらず、セッション レートが非常に低くなっていました。
SACE-8177/ ASOC-47223	Syslogフォワーダは、アプリケーション ルールで、メタを付加し、転送フラグがセットされたログのみを転送していました。

ESA(Event Stream Analysis) の修正

追跡番号	説明
SACE-12839	ESAルールのContext Hubエンリッチメントが古い値を使用してアラートを生成していました。 この問題は、Context Hubエンリッチメントの元となるリストが、上書きオプションが有効な自動更新リストの場合に発生します。リストの値が新しい値で上書きされても、古い値によってアラートがトリガーされていました。

Context Hubの修正

追跡番号	説明
SACE-13086/ ASOC-90987	定期実行フィードをContext Hubリストに変換する時、ステータスが失敗と表示されました。

Reporting Engineの修正

追跡番号	説明
SACE-11897/ ASOC-87262	既存のレポート スケジュールを編集する時、以前選択していなかったデータ ソースを選択できませんでした。

エンドポイントの修正

追跡番号	説明
SACE-12888/ ASOC-90565	エージェントを複数回インストールすると、**[調査]** > **[ホスト]**ビューに、名前が同じでエージェントIDが異なるホストが重複して表示されました。

更新の修正

追跡番号	説明
ASOC-92601	NW Serverホストをオフライン ユーザ インタフェースを使用して11.4.1.0にアップグレードできません。 この問題は、11.4.0.0または11.4.0.1から11.4.1にアップグレードする時に発生します。回避策は、既知の問題(ASOC-92601) を参照してください。 この問題は、11.4.1を将来のリリースにアップグレードする時には修正されています。
SACE-13125/ ASOC-90992	11.4.0.0にアップグレード後、PAMのケルベロス認証が失敗しました。
SACE-13119	11.4へのアップグレード後、[レガシー イベント]ビューでイベントを再構築し、イベント再構築ツールバーの[メタの表示]オプションを選択した時に、メタ データのドリルダウン オプションが表示されませんでした。
SACE-12649	11.3以降へのアップグレード後、Log CollectorはProofpointイベント ソースからログを受信しませんでした。
SACE-12586/ ASOC-86468	10.6.6システムでバージョン4.5のバックアップ スクリプトを実行した後、"verify Puppet Certs validity on SA Server"というエラーが表示されました。
SACE-12138/ ASOC-84298	NetWitnessリカバリツール(NRT) 実行時、カスタムのメタ グループとプロファイルがリストア処理の中でインポートされませんでした。
SACE-11531/ ASOC-79467	(Malware Analysis) 11.2.1.1へのアップグレード後、Threatgridモジュールが動作せず、HTTPプロキシ経由のRSA Cloud接続が動作しませんでした。
SACE-11196/ ASOC-77071	バージョン11.2.0.0をインストール後、/var/netwitness/common/repo/11.2.0.0にアクセスできるにもかかわらず、mongoのsa.repoテーブルには11.2.0.0 repoがダウンロード済みと表示されませんでした。

既知の問題

このリリースの未修正の問題の一覧は、次のURLを参照してください。
https://community.rsa.com/community/products/netwitness/documentation/known-issues回避策が存在する場合は、回避策の詳細が記載されているか、参照先のリンクが提供されます。

サポートされなくなった機能

次の表は、RSA NetWitness® Platform 11.3以降サポートされなくなった機能について説明しています。このリストは完全ではありません。追加の情報は、『*Release Notes for RSA NetWitness Platform 11.3*』などの、以前のバージョンのリリース ノートを参照してください。

11.3.0.0 以降でサポートされなくなった機能

機能	メモ
11.2以前のEvent Stream Analysisサービスの機能の一部	Event Stream Analysisサービス(11.2以前) の次の機能はRSA Correlationサービス(11.3以降) では提供されません。 1. 評価版ルールのメモリ スナップショット 2. ESAのSNMP通知 3. エンリッチメント ソースとしてのデータベースの使用 (Context Hubリストにより置換) 4. エンリッチメント ソースとしての Warehouse Analytics の使用(Context Hubリストにより置換) 5. エンリッチメント ソースとしてのデータベース接続の使用(Context Hubリストにより置換) 6. エンリッチメント ソースとしての自動更新インメモリ テーブルの使用(Context Hubリストにより置換) 7. キャプチャ時間による並べ替え 8. メモリプール
Endpoint Hybrid	11.3.0.0以降では、「Endpoint Hybrid」ホスト タイプはサポートされません。「Endpoint Log Hybrid」に置き換わりました。

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。

ドキュメント	参照場所
RSA NetWitness Platform 11.4 Product Documentation	https://community.rsa.com/community/products/netwitness/114
RSA NetWitness Platform 11.x Master Table of Contents	https://community.rsa.com/docs/DOC-81328
RSA NetWitness Platform 11.4 Upgrade Instructions	https://community.rsa.com/docs/DOC-110174
Upgrade Guide for RSA NetWitness Platform 11.4.1	https://community.rsa.com/docs/DOC-111158

製品ドキュメントへのフィードバック

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

サポート情報

NetWitness Platform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。

- 次の場所でNetWitness Platformのすべてのドキュメントを参照できます。
  https://community.rsa.com/community/products/netwitness/documentation
- RSA Linkの[**Search**]と[**Ask it**]を使用し、必要な情報を検索できます。
  https://community.rsa.com/welcome
- 更に情報が必要な場合は、カスタマ サポートにご連絡ください。

カスタマ サポートに連絡する時は、コンピュータにアクセスできる状態になっている必要があります。以下の情報を提供できるよう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、次の連絡先をご使用ください。

RSA Link	https://community.rsa.com にアクセスし、メイン メニューから[**My Cases**]をクリックしてください。
メール	support@rsa.com
各国のお問い合わせ窓口	https://community.rsa.com/docs/DOC-1294
コミュニティ	https://community.rsa.com/community/support
ベーシック サポート	月曜日から金曜日、現地時間の午前 9時から午後 5時まで利用可能です。
拡張サポート	新規の重大度1の問題について24時間365日の技術サポートを提供します。

ビルド番号

次の表は、NetWitness Platform 11.4.1.0の各コンポーネントのビルド番号です。

コンポーネント	バージョン番号
NetWitness Platform Audit Plugins	11.4.1.0-4590.5.7cab8ee42.el7.noarch.rpm
NetWitness Platform Appliance	11.4.1.0-10633.5.127b4ff3e.el7.x86_64.rpm
NetWitness Platform Archiver	11.4.1.0-10633.5.127b4ff3e.el7.x86_64.rpm
NetWitness Platform Broker	11.4.1.0-10633.5.127b4ff3e.el7.x86_64.rpm
NetWitness Platform Concentrator	11.4.1.0-10633.5.127b4ff3e.el7.x86_64.rpm
NetWitness Platform Config Management	11.4.1.0-2003202027.5.e51b6a1.el7.noarch.rpm
NetWitness Platform Config Server	11.4.1.0-200330083008.5.3174643.el7.centos.noarch.rpm
NetWitness Platform Console	11.4.1.0-10633.5.127b4ff3e.el7.x86_64.rpm
NetWitness Platform Content Server	11.4.1.0-200310125231.5.cf8d356.el7.centos.noarch.rpm
NetWitness Platform ContextHub Server	11.4.1.0-200330115543.5.8f124f1.el7.centos.noarch.rpm
NetWitness Platform Correlation Server	11.4.1.0-200330161146.5.713a22e.el7.centos.noarch.rpm
NetWitness Platform Decoder	11.4.1.0-10633.5.127b4ff3e.el7.x86_64.rpm
NetWitness Platform Deployment Upgrade	11.4.1.0-2003051317.5.bd9e71a.el7.noarch.rpm
NetWitness Platform Endpoint Agents	11.4.1.0-2003202121.5.134fc9d.el7.x86_64.rpm
NetWitness Platform Endpoint Broker Server	11.4.1.0-200326092625.5.1d933be.el7.centos.noarch.rpm
NetWitness Platform Endpoint Server	11.4.1.0-200326081352.5.b705b80.el7.centos.noarch.rpm

NetWitness Platform Integration Server	11.4.1.0-200326111855.5.e69c651.el7.centos.noarch.rpm
NetWitness Platform Investigate Server	11.4.1.0-200326142731.5.14e9737.el7.centos.noarch.rpm
NetWitness Platform Legacy Web Server	11.4.1.0-200330212815.5.a1c165f.el7.centos.noarch.rpm
NetWitness Platform License Server	11.4.1.0-200319042333.5.b03516e.el7.centos.noarch.rpm
NetWitness Platform Log Decoder	11.4.1.0-10633.5.127b4ff3e.el7.x86_64.rpm
NetWitness Platform Log Player	11.4.1.0-10633.5.127b4ff3e.el7.x86_64.rpm
NetWitness Platform Malware Analytics Server	11.4.1.0-200317130233.5.b4dfbd3.el7.centos.x86_64.rpm
NetWitness Platform Metrics Server	11.4.1.0-200331061305.5.0a40975.el7.centos.noarch.rpm
NetWitness Platform Orchestration Server	11.4.1.0-200305153237.5.672a8ed.el7.centos.noarch.rpm
NetWitness Platform Reporting Engine Server	11.4.1.0-5839.5.4d0df7192.el7.x86_64.rpm
NetWitness Platform Respond Server	11.4.1.0-200330180231.5.e793c97.el7.centos.noarch.rpm
NetWitness Platform Root CA Update	11.4.1.0-2002271414.5.1d71333.el7.noarch.rpm
NetWitness Platform SDK	11.4.1.0-10633.5.127b4ff3e.el7.x86_64.rpm
NetWitness Platform Security Server	11.4.1.0-200319044348.5.27f4710.el7.centos.noarch.rpm
NetWitness Platform Source Server	11.4.1.0-200310125546.5.5282be7.el7.centos.noarch.rpm
NetWitness Platform User Interface	11.4.1.0-200330184829.5.fad368da86.el7.centos.noarch.rpm
NetWitness Platform Workbench	11.4.1.0-10633.5.127b4ff3e.el7.x86_64.rpm
NetWitness Platform SA Tools	11.4.1.0-2003241602.5.ca28709.el7.noarch.rpm
NetWitness Platform SMS Runtime	11.4.1.0-4590.5.7cab8ee42.el7.x86_64.rpm
NetWitness Platform SMS Server	11.4.1.0-4593.5.2f80323e5.el7.x86_64.rpm

改訂履歴

日付	説明
2020年4月	ベータ
2020年4月	初回リリース
2020年4月15日	調査の新機能を訂正。「[イベント]ビューでのクエリ作成の高速化、簡略化」の4番目の項目から、先頭の「!」を削除。