RSA NETWITNESS® PLATFORM

リリース ノート

バージョン11.2

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://japan.emc.com/legal/emc-corporation-trademarks.htm#rsa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、EMC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

この製品には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

EMC Corporation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。

目次

はじめに

このドキュメントは、RSA NetWitness® Platform 11.2.0.0の機能拡張と修正について記述しています。RSA NetWitness® Platform 11.2.0.0を新規導入または更新する前にお読みください。

新機能

RSA NetWitness®Platform11.2.0.0リリースでは、ログ、パケット、およびエンドポイントの調査のための新機能と機能拡張が提供されています。このリリースでは、ユーザとエンティティの行動分析機能が追加され、ユーザを基点として攻撃および異常を検知し調査することができます。

NetWitness UEBA(User and Entity Behavior Analysis)

RSA NetWitness® UEBAはRSA NetWitness® Platformに統合されました。NetWitness UEBAは、包括的なユーザおよびエンティティの行動分析を行い、高度な内部攻撃やユーザの異常を検知、調査、対応することができます。

NetWitness UEBAは、次の機能を提供します。

- 動的な統計的異常値分析により、行動のベースライン作成、行動のモデリング、ピア グループ分析を行い、異常行動、ラテラル移動、内部脅威、データ窃取を検知します。
- 調整不要の機械学習アルゴリズムにより、不審な行動から異常を識別します。
- ユーザおよびアラートのリスク スコア モデルを生成し、高リスク インジケータの重大度と優先度のみを上昇させ、アラート疲労や誤検知を削減します。

NetWitness UEBAサービスの導入。NetWitness UEBAは、NetWitness PlatformのAdmin Serverから構成および導入できます。NetWitness UEBA Serverは、NetWitness PlatformのサービスからWindowsログ データを収集し、データを処理し、NetWitness GUIに結果を表示します。NetWitness Endpoint Insightsエージェントが導入されている場合は、そこで収集されたWindowsログデータも分析します。UEBAの導入の詳細については、『*物理ホスト インストール ガイド*』または『*仮想ホスト インストール ガイド*』を参照してください。

バージョン11.2では、UEBAは次のようなさまざまなWindowsのログ ソースを標準サポートしています。

- Windows Active Directory
- Windowsログオンおよび認証アクティビティ
- Windowsファイル サーバ

ユーザの行動ベースライン作成。機械学習モデルを履歴データおよびリアルタイム データに適用することにより、行動のベースラインが作成されます。行動のベースラインは、異常の識別、組織や個人のメトリックの可視化に役立ちます。標準のモデリング ポリシーでは、30日の学習期間が必要です。この期間を超える履歴データが保存されている場合は、もっと前の履歴データから学習を開始するよう学習期間を変更できます。これらのベースラインと比較して異常な行動のみが、異常または侵害と判定されます。

上位アラートと高リスク ユーザの調査。アナリストは、事前定義されたOOTB(既成) のダッシュボードとレポートを活用して、上位アラート(丸1時間以内に一連のインジケータによりトリガーされたアラート) と高リスク ユーザ(リスク スコアの高いユーザ) を調査できます。アナリストは、優先的に対処すべきユーザのリストを表示し、より深い調査を行い、リスク スコアを減らすことができます。

NetWitness UEBAのライセンス。NetWitness UEBAのライセンスは、組織内のユーザの総数をベースとします。ユーザとは、ネットワーク アクセスおよびログインの認証情報を持つ個人を意味します。ユーザ数が購入したライセンスを5%超えると、新しいライセンスを購入する必要があります。詳細については、RSA営業担当者にお問い合わせください。ライセンスの詳細については、『*ライセンス管理ガイド*』を参照してください。

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

NetWitness Respond

[インシデントの詳細]ビューからイベント分析に直接アクセス。インシデントの[インジケータ]パネルから[調査]の[イベント分析]ビューにシームレスにアクセスできます。インシデントを詳しく調査するため、[対応]ビューでイベントのイベント タイプのハイパーリンクをクリックして、[イベント分析]ビューを開くことができます。

NetWitness RespondからRSA Archerにインシデントを送信する機能を追加。RSA ArcherがContext Hubのデータ ソースとして構成されている場合、インシデントをArcher Cyber Incident & Breach Responseに送信できます。この構成を行うと、NetWitness Respondには、[Send to Archer]ボタンとArcherへの送信ステータスが表示されます。また、インシデント リストのフィルタにより、Archerに送信されたインシデントを抽出できます。インシデントをArcherに送信すると、インシデントのジャーナルに自動的にエントリーが追加されます。

インシデントからRSA Archerへの移行。RSA Archer® Cyber Incident & Breach Responseが管理するデバイスの詳細情報やその他の情報を表示するため、特定のエンティティからRSA Archerに移行できます。対象となるエンティティは、IPアドレス、ホスト、およびMacアドレスです。下線付きで表示されたエンティティについて、ビジネス ユニット、デバイス名、デバイス タイプなどの属性を[コンテキスト ルックアップ]パネルに表示できます。詳細については、『*NetWitness Respondユーザ ガイド*』を参照してください。

[アラート リスト]ビューからの手動インシデント作成の改善。アラートから手動でインシデントを作成するときに、優先度、割り当て先、およびカテゴリを指定できます。

ノード グラフでノード タイプを非表示にする機能の追加。ノード グラフ上でエンティティ間の相互関係をさらに調査するため、ノード グラフに表示するノード タイプを選択できます。この機能は、ノード グラフに100個以上のノードが含まれるような場合には特に役立ちます。

割り当て済みインシデントと未割り当てインシデントのフィルタの調整。[インシデント リスト]の[フィルタ]パネルでは、割り当て先と未割り当てのインシデントを同時にフィルタに指定できなくなりました。[未割り当てのインシデントのみを表示]を選択すると、[割り当て先]ドロップダウン リストが無効になります。[割り当て先]ドロップダウン リストで担当者を選択すると、[未割り当てのインシデントのみを表示]オプションが無効になります。

[インシデント リスト]のソートのユーザ エクスペリエンス向上。リストの列ヘッダーの任意の場所をクリックして、ソート順を切り替えることができます。上矢印または下矢印をクリックしてリストをソートする必要がなくなりました。

詳細については、『*NetWitness Respondユーザ ガイド*』と『*NetWitness Respond構成ガイド*』を参照してください。

NetWitness Investigate

[イベント分析]ビューのメタ値のコンテキスト情報。[ナビゲーション]ビューおよび[イベント]ビューで以前に使用可能だった[コンテキスト ルックアップ]パネルが[イベント分析]ビューに追加されました。[コンテキスト ルックアップ]パネルには、Context Hubでイベントの構成要素(IPアドレス、ユーザ、ホスト、ドメイン、MACアドレス、ファイル名、ファイル ハッシュ)に関連づけられた詳細情報が表示されます。イベントのメタ値を操作して、関連するインシデント、アラート、カスタム リスト、RSA Archer資産情報、Active Directoryからの詳細情報、NetWitness Endpoint Thick Clientなどからより深い洞察を得ることができます。詳細については、『*NetWitness Investigateユーザ ガイド*』の「データポイントの追加コンテキストの表示」を参照してください。

[イベント分析]ビューのメタ値からArcherへの移行。[イベント分析]ビューに下線付きで表示されるIPアドレス、Mac、ホストなどのエンティティからRSA Archerに移行して、デバイスの詳細情報を表示できるようになりました。

[イベント分析]ビューのフリーフォーム クエリ。既存の基本クエリ(Guided)モードに加え、Free-Formモードが利用できるようになりました。Free-Formモードでは、アナリストは複雑なクエリ テキストを入力できます。Free-FormモードとGuidedモードを切り替えることができます。詳細については、『*NetWitness Investigateユーザ ガイド*』の「[イベント分析]ビューでの結果のフィルタ」を参照してください。

プロファイルの機能拡張:プロファイル グループ、新規および更新されたプロファイル、階層リンクへのプロファイルのプレ クエリの表示。詳細については、『*NetWitness Investigateユーザ ガイド*』の「プロファイルを使用したカスタム ビューのカプセル化」を参照してください。

- プロファイル グループを使用すると、プロファイルを論理グループに分けて管理できます(例:異なるユースケースごと、異なるユーザごとなど)。既存および新規のプロファイルをプロファイル グループに移動できます。
- RSA Endpoint Analysisという名前の新しいOOTBプロファイルが追加されました。このプロファイルは、`device.type=nwendpoint`というプレ クエリ、RSA Endpoint Analysisメタ グループ、RSA Endpoint Analysis列グループを使用します。
- RSA Threat Analysisプロファイルが更新され、次の3つのメタ キーが置換されました。

  `risk.warning` → `behavior of compromise (boc)`
  `risk.suspicious` → `indicator of compromise (ioc)`
  `risk.informational` → `enabler of compromise (eoc)`
- [ナビゲート]ビューまたは[イベント]ビューでプロファイルを選択すると、そのプロファイルのプレ クエリが階層リンクに表示されます。

検索オプションの構成の向上。検索オプションを構成するためのメニューが再編成され、わかりやすく選択できるようになりました。詳細については、『*NetWitness Investigateユーザ ガイド*』の「[ナビゲート]ビューおよび[イベント]ビューの構成」を参照してください。

[テキスト分析]パネルの向上。[イベント分析]ビューでは、データ表示の操作性を改善するための変更を行いました。

- 新しいページ移動コントロールを使用すると、イベント リストのページをより柔軟に移動できます。
- [テキスト分析]パネルで再構築されたイベントに最大バイト数を超えるリクエストまたはレスポンスが含まれる場合、ヘッダーにはメッセージがトランケートされたことが表示されます。これにより、レンダリングするには大きすぎるイベントを[テキスト分析]に表示するときに、できるだけ多くのデータが提供されます。

イベント ソース管理

アイドル状態のイベントソースの識別。新しい属性は、各イベント ソースから最後にログを受信してからの経過日数を表示します。この属性を使用すると、一定期間(たとえば、90日間)アイドル状態のイベント ソースをグループ化して、調査したり一括削除できます。

Context Hub

属性をインポートまたはエクスポートするオプション。[コンテキスト ルックアップ]パネルの属性を管理し、RSA Archerのデバイス詳細情報からユーザが必要とする属性を表示できるようになりました。RSA Archerのデバイス アプリケーションの必要な属性を構成し、コンテキスト パネルにこれらの属性を表示できます。これを実現するため、既存の属性をファイルにエクスポートし、そこに新しい属性を追加して、更新された属性のセットをインポートできます。これらの属性は、インシデントのコンテキストまたは[イベント分析]ビューでイベントを表示するときに、インポートされた順序で[コンテキスト ルックアップ]パネルに表示されます。詳細については、『*Context Hub構成ガイド*』を参照してください。

NetWitness Serverに実装されたサービス

新しいContentサービス。新しい**Content** サービスは、RSA提供とユーザ作成のParserルールを管理します。UIから、Parser ルールを追加できるようになりました。Contentサービスは、このドキュメントの後半の「ログ解析」セクションで説明する[ログParserルール]タブで使用されます。

Log DecoderとNetwork Decoder

標準pcapngファイルのサポート。よりオープンなデータベース形式を提供するため、Network Decoderは標準のpcapng形式のファイルを書き込めるようになりました。11.2を新規インストールすると、この機能はデフォルトで有効になります。以前のバージョンから11.2にアップグレードする場合は、pcapng形式のデータベース ファイルを手動で有効にする必要があります。その結果、空きディスク領域が約4%減少する可能性があります(pcapngファイルはnwdbファイルよりも多くの領域を必要とするため)。10 Gbpsのキャプチャでpcapng形式を使用することもできます。この場合、パフォーマンスの大幅な低下はありません(1%未満)。

新しい構成ノードを有効にします。

```
/database/config/packet.file.type = 'netwitness' or 'pcapng'
```

新しいGeoIP2 Parser。新しいGeoIP2 Parserは、IPアドレスを地理情報に変換し、最新のMaxmind GeoIPパッケージを提供し、IPv4に加えIPv6アドレスをサポートしています。GeoIP2 Parserは、`ip.src`、`ip.dst`、`ipv6.src`および`ipv6.dst`を読み込んで、GeoIP情報を生成します。GeoIP2 Parserは、Decoderではデフォルトで有効になっています。詳細については、『*DecoderおよびLog Decoder構成ガイド*』の「GeoIP2およびGeoIPのParser」を参照してください。

IPv4およびIPv6メタデータでのGeoIP検索。任意のIPv4またはIPv6メタデータでGeoIP検索を実行できるようになったため、`ip.src`と`ip.dst`にフォーカスしていないシナリオでも地理情報を理解できるようになりました。

- Lua ParserにGeoIP2情報への完全なアクセスを提供する新しいLua APIがあります。Lua APIは、GeoIP2データベースから要求された情報を返します。Parserは、この情報を自由に使用して、メタを作成したり、独自の分析を実行できます。
- `config`ノードの`parsers.options`を使用して、任意のIPv4またはIPv6キーでGeoIP2メタデータを生成するように、ネイティブGeoIP2 Parserを構成できます。

詳細については、『*DecoderおよびLog Decoder構成ガイド*』の「GeoIP2およびGeoIPのParser」を参照してください。

TLS証明書のハッシュ。Network Decoderは、パケット ストリームに含まれる証明書のハッシュを生成できます。このハッシュは、TLSハンドシェイク中に検出されたDERエンコード証明書のSHA-1値です。ハッシュ データは`cert.checksum`キーに書き込まれます。生成されたハッシュを使用すると、公開されたSSLブラックリストのハッシュとネットワークトラフィックを比較することができます。詳細については、『*DecoderおよびLog Decoder構成ガイド*』の「TLS証明書のハッシュ」を参照してください。

ユーザ インタフェース

[ログParserルール]タブの移動。バージョン11.1で[管理]>[イベント ソース]にあった[ログParserルール]タブは、バージョン11.2では[構成]ビューに移動しました。

言語サポートの追加。[ユーザ環境設定]に新しい[言語]オプションが追加され、言語を選択できるようになりました。言語を選択すると、NetWitness Platform全体のテキストがその言語に変更されます。詳細については、『*NetWitness Platform スタート ガイド*』を参照してください。

NetWitnessのブランド変更。NetWitness 11.2製品は、ユーザ インターフェイス、ドキュメント、およびその他の関連事項にわたって以下のようにブランド変更されました。

1. RSA NetWitness® Suite → RSA NetWitness® Platform
2. RSA NetWitness® Packets → RSA NetWitness® Network
3. RSA NetWitness® Logs and Packets → RSA NetWitness® Logs & Network
4. Packet Hybridホスト タイプ → Network Hybridホスト タイプ
5. Packet Decoderホスト タイプ → Network Decoderホスト タイプ
6. RSA NetWitness® SecOps Manager → RSA Archer® Cyber Incident & Breach Response

管理

[調査]コンテキスト メニュー アクションの構成。[調査]で利用可能な右クリック アクションが、UIの[コンテキスト メニュー]ページを使用して、異なるフィールドやグループを指定して構成できるようになりました。[管理]＞[システム]の[コンテキスト メニュー]ページを使用して、新しいコンテキスト メニュー アクションを作成し、管理することができます。UIを使用して構成したコンテキスト メニュー アクションは、[調査]の[ナビゲート]ビュー、[イベント]ビュー、および[イベント分析]ビューで、メタ キーを右クリックするとアクションとして表示されます。[イベント分析]ビューでも、メタ キーの右クリック アクションがサポートされています。

ログイン バナーの改善。ログイン バナーのテキストを完全にカスタマイズできるようになり、セキュリティ対策が強化されました。

ログ解析

[ログParserルール]タブの拡張。既存のログParserの拡張、カスタム ログParserの追加、ログParserのログParserルールの更新を行う機能が追加されました。ログParserルールは、イベント ソースのログからメタ情報を抽出する方法を変更します。ログParserルールを追加して、既存のログParserを拡張したり、Unknownに分類される可能性のあるメッセージからメタを抽出するデフォルト ログParserに追加することもできます。詳細については、RSA Linkの『*ログParser カスタマイズ ガイド*』を参照してください。11.1では、ログParserルールは読み取り専用でした。

アップグレード手順

RSA NetWitness® Platform 11.2.0.0では、以下のアップグレード パスがサポートされます。

- RSA NetWitness® Platform 10.6.6.xから11.2.0.0
- RSA NetWitness® Platform 11.0.xまたは11.1.xから11.2.0.0

11.2.0.0へのアップグレードの詳細については、製品ドキュメントセクションに記載されているアップグレード ガイドを参照してください。

修正された問題

本セクションでは、前回のメジャー リリース以降に修正された問題について説明します。

セキュリティ

トラッキング番号	説明
ASOC-58379	CentOS 7のglibcの重大度=中のセキュリティ更新 : https://access.redhat.com/errata/RHSA-2018:0805
ASOC-58373	CentOS 7のカーネルのセキュリティ更新 : https://access.redhat.com/errata/RHSA-2018:1629
ASOC-58376	dhcpのセキュリティ更新 : https://access.redhat.com/errata/RHSA-2018:1453
ASOC-58374	procps-ngのセキュリティ更新 : https://access.redhat.com/errata/RHSA-2018:1700
ASOC-58381	ntpのセキュリティ更新 https://access.redhat.com/errata/RHSA-2018:0855
ASOC-58384	gccのセキュリティ更新 https://access.redhat.com/errata/RHSA-2018:0849
ASOC-58380	krb5のセキュリティ更新 https://access.redhat.com/errata/RHSA-2018:0666
ASOC-50151	openssshのセキュリティ更新 https://access.redhat.com/errata/RHSA-2018:0980
ASOC-58367	openjdkのセキュリティ更新 https://access.redhat.com/errata/RHSA-2018:1649
ASOC-58377	libvorbisのセキュリティ更新 https://access.redhat.com/errata/RHSA-2018:1058
ASOC-52448	Authconfigのセキュリティ更新https://access.redhat.com/errata/RHSA-2017:2285
ASOC-52439	Libx11のセキュリティ更新https://access.redhat.com/errata/RHSA-2017:1865

トラッキング番号	説明
ASOC-52443	NetworkManagerのセキュリティ更新 https://access.redhat.com/errata/RHSA-2017:2299
ASOC-52444	Bashのセキュリティ更新 https://access.redhat.com/errata/RHSA-2017:2299
ASOC-52445	Openldapのセキュリティ更新 https://access.redhat.com/errata/RHSA-2017:1852
ASOC-49815	Systemdのセキュリティ更新 https://access.redhat.com/errata/RHSA-2018:0260

アプリケーションに関する問題

トラッキング番号	説明
ASOC-46483	[対応]ビューおよび一部の[調査]ビューで、アイドル状態のユーザがログオフされる

調査

トラッキング番号	説明
ASOC-51011	10.6.5から11.xにアップグレードすると、11.0の次の3つの新しいメタ グループおよび11.1の同名の列グループが作成されない: RSA Endpoint Analysis、RSA Outbound HTTP、RSA Outbound SSL/TLS
ASOC-50702	11.1にアップグレードした後、Log Decoder(table-map.xml) とConcentrator (index-concentrator.xml) の定義で一致しないデータ タイプがある。
ASOC-50924	IPV6メタ値に未サポートの特殊文字を指定して、直接クエリまたはリンク経由のクエリを実行しようとすると、[イベント分析]ビューまたは[ナビゲート]ビューでエラーが発生する。
ASOC-50771	[イベント分析]リンクをクリックするか、いずれかのイベントを右クリックして、[イベント]ビュー経由でイベント分析にアクセスした場合、メタ値の右クリック オプションが機能しない。
ASOC-49854	無期限にサービス セレクタ ビジー カーソルをロードし続ける。

トラッキング番号	説明
ASOC-50712	[調査ページのロードを最適化]オプションが無効な場合、[イベント]ビューでカスタム列グループにメタ エンティティを追加できない。
ASOC-50349	[イベント]ビューでメタ エンティティを含むカスタム列グループを作成し、[イベント分析]ビューで使用すると、メタ エンティティに含まれるメタ キーが結果ページに表示されない。
ASOC-50041	[イベント分析]ビューでセミコロンを含むメタ値を右クリックして、新しいタブの[ナビゲート]ビューでドリルダウンしようとすると、「チャートをビルドできません」というエラーが表示される。
ASOC-45198	URLを変更し、新しいURLが制限付きイベントをポイントする場合、前のクエリの再構築されたコンテンツが[イベント分析]ビューに残り、エラー メッセージが表示されない。
ASOC-48945	[イベント分析]ビューで、アクセスできないセッションへのクエリを入力すると、データが表示されず、エラー メッセージも表示されない。
ASOC-48710	[イベント分析]ビューで調査中に「予期しないエラーが発生しました」というエラー メッセージが返される。

対応

トラッキング番号	説明
ASOC-40749	Respond Administratorは、調査でのクエリ実行もダッシュボードでのLiveダッシュレットの表示もできない。
ASOC-41891	NetWitness SecOps Manager 1.3.1.2のSecurity Analytics Incident Managementリンクが NetWitness Suite 11.1.0.0.で有効ではない
ASOC-46834	ルール ビルダで「Domain for Suspected C&C」と「Domain」を選択できない
ASOC-50911	MongoDBへの再接続後に集計が停止する
ASOC-51480	検知器IPを含むEndpointイベントがEndpointインシデント ルールによって統合されず、現在のデフォルトのインシデント ルールの一致条件ではインシデントが作成されない。『*NetWitness Respond構成ガイド*』の「デフォルト インシデント ルールの設定と検証」のトピックを参照してください。

ESA(Event Stream Analysis)

トラッキング番 号	説 明
ASOC-50201	［ヘルス モニタ］ビューでEvent Stream Analyticsの新しいポリシーを作 成する時 、「ESA Rule Memory Usage」統 計を使 用する新しいルールを追 加しようとすると、導 入 済みのすべてのESAルールがリストに表 示されない。

サポートされない機能

次の表に、RSA NetWitness® Platform 11.1以降のリリースでサポートされなくなった機能に関する情報を示します。

11.1.0.0以降のリリースでサポートされなくなった機能

番号	機能	注
1	Malware Colo	11.1.0.0以降のリリースでは、共存型のMalware Analysisはサポートされません。Malware Analysisは、スタンドアロンのMalware Analysisの使用によってサポートされます。
2	AIO(オールインワン)の導入	オールインワンの導入はサポートされません。新規インストールからAIOは削除されました。
3	スタンドアロンWarehouse Connector	スタンドアロンWarehouse Connectorはサポートされません。
4	管理機能	1. パスワードを忘れた場合のリンク。 2. パスワードの有効期限が切れたときのユーザへのメール通知。 3. ADユーザのテスト/検索。
5.	Pivotal	Pivotalはサポートされません。
6.	Warehouse Analytics	Warehouse Analyticsはサポートされません。

今後のリリースでサポート予定の機能

次の機能は、11.2では利用できませんが、今後のリリースで利用可能になる予定です。

番号	機能	注
1	IPDBレポート作成	IPDB Extractorサービスは、11.2.0.0 ではサポートされませんが、今後のリリースで利用可能になります。

番号	機能	注
2	STIG	STIG強化されたホストがある場合は、11.2.0.0にアップグレードできません。これは、バックアップ スクリプトがサポートしていないためです。
3	複数のSecurity Analytics Server (NetWitness Server) のサポート	複数サーバの導入環境はサポートされません。
4	PKI認証	PKI認証の機能は11.2.0.0では利用できません。
6	Endpoint Analytics	エンドポイント スキャン データでは、リスク スコアやIOC計算などの分析はサポートされていません。
7	Endpoint Remediation	対応機能(封じ込め/ブロック) はサポートされていません。
8	Endpoint Tracking	ネットワーク イベントの追跡はサポートされていません。
9	Endpoint Kernelモード	Endpointエージェントは現在ユーザ モードで機能し、Kernel モードでの検知はサポートしていません。
10	Endpointファイル レピュテーション	OPSWAT、YARA、Reversing Labルックアップなどのファイル レピュテーションはサポートされていないため、ファイルをホワイトリストやブラックリストに追加することはできません。

既知の問題

このセクションでは、本リリースで未解決の問題について説明します。回避策に関する情報がある場合は、その詳細の説明または参照先を記載します。

11.2へのアップグレードに関連する既知の問題

10.6.6から11.2へのアップグレード、11.1または11.1.xから11.2への更新により、以下の問題が発生します。

10.6.6から11.2にアップグレードすると、定期実行のSTIX Feedが失敗する

トラッキング番号: ASOC-61227

問題: Security Analytics 10.6.6をNetWitness Platform 11.2にアップグレードすると、HTTPS URLが指定された定期実行のSTIX Feedが失敗します。これは、10.6.xではデフォルトですべての証明書が信頼されているためです。しかし、11.2では異なります。11.2では、[すべての証明書を信頼]オプションが用意されており、このオプションはデフォルトで無効になっています。

回避策: [構成]>[カスタムFeed]に移動し、失敗したFeedを編集します。[すべての証明書を信頼]オプションを有効にするか、有効なSSL証明書をアップロードして問題を解決します。追加の質問がある場合は、RSAカスタマー サポートにお問い合わせください。

NetWitness Platform 11.2へのアップグレード時にライセンスの詳細がAWSクラウドに保持されない

トラッキング番号: ASOC-61614

問題: Security Analytics 10.6.6からNetWitness Platform 11.2にアップグレードすると、ライセンス サーバIDが保持されません。このため管理サーバは、外部のバックエンド システムからライセンス サーバの詳細を取得できず、サービスにライセンスを付与できません。

回避策: 『*ライセンス管理ガイド*』の「Access Download Central(Download Centralへのアクセス) 」および「Register the Server (Online)(サーバの登録(オンライン) 」のトピックに記載された手順に従って、外部のバックエンド システムからライセンスの詳細を取得し、新しいライセンス サーバIDを登録します。

10.6.6から11.2.0.0へのアップグレード後、オフライン ライセンスが保持されない

トラッキング番号: ASOC-41757

問題: Download Centralから入手した新しいレスポンスbinファイルをアップロードしても、オフライン ライセンスが機能しません。古いファイルは`/var/lib/fneserver`にリストアされていますが、ライセンスは非アクティブのままです。

回避策: 以下の手順を実行して、ライセンスをリストアします。

1. Download Centralから、新しいレスポンスbinファイルを生成します。
2. 11.2.0.0のNetwitness Serverホスト(AdminServer) にSSHでログインします。
3. `/var/lib/fneserver/`からra*ファイル(3つのファイル) を移動します。

4. RSA NetWitness 11.2.0.0 UIにadminユーザでログインし、[**管理**]>[**システム**]>[**License Details**]タブに移動します。
5. [**ライセンスの更新**]をクリックします。
6. Download Centralから入手したレスポンス ファイルをアップロードします。[**管理**]>[**システム**]>[**ライセンス**]>[**設定**]タブに移動します。
7. [**アップロード**]をクリックします。

注: オンライン モード(RSA Netwitness Suite 11.2.0.0がインターネットに接続されている場合)でのアップグレードは正常に完了し、11.2.0.0へのアップグレード後にすべてのライセンスがリストアされます。

10.6.6から11.2へのアップグレード後に、静的チャートの調査リンクが無効になる

トラッキング番号: ASOC-42136

問題: データ ソースがNetWitness Suite Broker(このサービスはデフォルトで利用可能)に設定された静的チャート(レポートの結果がチャート形式)で調査リンクが無効になっています。

回避策: この問題には、次の2つの解決策があります。

- 静的チャートで結果を表示するルールは、表形式でも表示できます。表形式では、調査リンクが正常に機能します。
- または、以下の手順を実行して問題を解決できます。
  1. NetWitness Suite BrokerをReporting Engineのデータ ソースから削除し、同じ名前で再び追加します。
  2. 静的チャートのレポートが、スケジュール設定されたレポートである場合は、次回の実行時から調査リンクが正常に機能します。
  3. レポートがアドホック レポートである場合は、レポートを再実行すると調査リンクが有効になります。

10.6.6から11.2へのアップグレード後、標準提供(OOTB)チャートを使用してGeoマップ ダッシュレットを作成できない

トラッキング番号: ASOC-41896

問題: Netwitness Suite 11.2.0.0にアップグレードすると、標準提供のチャートを使用してGeoマップ ダッシュレットを作成することができません。この問題は、カスタム ダッシュボードでGeoマップ ダッシュレットを使用し、そのダッシュレットが標準提供のチャートを使用している場合に発生します。

回避策: Geoマップ ダッシュレットで使用する必要のある標準提供チャートのデータ ソースを手動で更新する必要があります。または、同じ標準提供ルールを使用して、新しいチャートを作成し、それをGeoマップ ダッシュレットで使用します。

11.xから11.2へのアップグレード後、Entropy Parserを使用してペイロードのインデックスを作成していた場合は、Entropy Parserがインデックス バケットを使用できるよう、インデックス ファイルにbucketフラグを追加する必要がある

トラッキング番号: ASOC-45721

問題: バージョン11.0からバージョン11.2にアップグレード後、Decoder(パケットのみ) でEntropy Parserを使用して、ペイロードのインデックスを作成していた場合は、新しいインデックス バケット機能を活用するため、インデックス ファイルにbucketフラグを追加する必要があります。

注: バージョン11.1以降からバージョン11.2にアップグレードする場合は、この変更を行う必要はありません。

回避策: Entropy Parserがインデックス バケットを使用できるよう、インデックス ファイルにbucketフラグを追加します。

1. NetWitness Suiteメニューで、[**管理**]>[**サービス**]を選択します。
   [サービス]ビューが表示されます。
2. Decoderからトラフィックを集計しているConcentratorサービスを選択します。
3.  (アクション) で、[**表示**]>[**構成**]を選択し、[**ファイル**]タブを選択します。
4. `index-concentrator-custom.xml file`を選択し、`payload.req`と`payload.res`の`bucket`フラグを`true`に設定します。例:
   ```
   <key description="Payload Size Request" format="UInt 32"
   level="IndexNone" bucket="true" name="payload.req"
   valueMax="500000"/>
   <key description="Payload Size Response" format=UInt32"
   level="IndexNone" bucket="true" name="payload.res"
   valueMaz="500000"/>
   ```
5. [**適用**]をクリックします。
6. `index-concentrator-custom.xml`ファイルへの変更を反映するため、次のコマンドを実行し、Concentratorサービスを再起動する必要があります。
   ```
   systemctl restart nwconcentrator
   ```

UEBA

プロキシが構成された環境で更新を行うと、ライセンスの詳細が自動的に更新されない

トラッキング番号: ASOC-52366

問題:プロキシが構成された環境で更新を行うと、ライセンスの詳細が自動的に更新されません。さらに、[License Details]ビューの[ライセンスの更新]ボタンをクリックしても更新されません。この問題は、ライセンス サーバへの通信が確立されていないために発生します。

回避策:管理者は、オフライン モードを使用してライセンスの詳細を手動でダウンロードし、NetWitness Platform UIから最新のライセンスの詳細をアップロードする必要があります。詳細については、『*ライセンス管理ガイド*』を参照してください。

エンドポイント

Nginxがリクエスト サイズが1MBを超えるPOSTリクエストを拒否する

トラッキング番号:ASOC-56236

問題:Nginxサーバをアップグレードすると、デフォルトのペイロード サイズが1MBに設定されます。このため、データのPOSTリクエストが1MBを超えると失敗します。

回避策:Nginx構成ファイル(`/etc/nginx/conf.d/nginx.conf`) に次の設定を追加し、Nginxサーバを再起動します。

```
client_max_body_size 100M
```

*nwelcfgファイルの生成とコピーにより、タイムスタンプが更新されない

トラッキング番号:ASOC-49847

問題:Endpoint Insightsエージェントをインストールした後、管理者が任意のコピー方法またはサードパーティのエンドポイント管理ツールを使って、ログ収集の構成ファイルを更新する場合、構成ファイルのタイムスタンプは、エージェントの時刻ではなく、Endpoint Serverの時刻のままになります。その結果、Endpointエージェントと Endpoint Serverのタイム ゾーンが異なる場合、タイムスタンプの更新が正しく認識されません。

回避策:構成ファイルをコピーした後、Endpointエージェントで次のコマンドを実行します (nwelcfgファイルは%programdata%\NWEAgent\フォルダにあります) : `copy /b <filename.nwelcfg> +,,`

Respond

特定のアラート ルールのすべてのアラートを削除した後、フィルタからそのアラート ルールが適切に削除されない

トラッキング番号:ASOC-59243

問題:[アラート リスト]ビュー([対応]>[アラート]) では、アラート名によりフィルタし、そのアラート名のアラートをすべて表示し、削除できます。アラートの削除後、フィルタからアラート名を明示的に削除しなければ、次回[アラート リスト]ビューを読み込むときに、フィルタにアラート名がそのまま残ります。しかし、そのアラート名のアラートは既にすべて削除されているため、[フィルタ]パネルにはそのアラート名のチェックボックスが表示されません。このため、[アラート リスト]ビューにアクセスすると、引き続きゼロ件の結果が表示されます。

回避策: [アラート リスト]ビューを更新または再ロードする前に、[フィルタ]パネルでアラート名のチェックボックスをクリアし、フィルタを削除できます。[アラート リスト]ビューを既に更新または再ロードした場合、非表示のフィルタを削除する唯一の方法は、[**フィルタのリセット**]ボタンを押して、非表示のアラート名フィルタを含むすべてのフィルタを削除することです。

既存のインシデントに手動でアラートを追加すると、インシデントにフラグが設定されない

トラッキング番号: ASOC-52428

問題: [対応]ビューでアラートを手動でインシデントに追加した場合、メタ値にカーソルを合わせてもハイライト表示されません。インシデントに自動的に追加されたアラートの場合、カーソルを合わせるとハイライト表示されます。

回避策: なし。

韓国語のマルウェア イベント ファイル名が[対応]ビューに正しく表示されない

トラッキング番号: ASOC-40159

問題: Malware Analysisから受信したアラートに韓国語の文字が含まれる場合は、[対応]ビューに正しく表示されません。

回避策: なし。

ESAルールの重大度の高/低がRSA Archerに入力されない

トラッキング番号: ARCHER-47101

問題: 重大度が高または低のESAアラートがRSA Archerに転送されたとき、RSA Archer UIの[セキュリティアラートの優先度]フィールドに値が設定されません。

回避策: なし。

RSA Archer Cyber Incident & Breach Responseとの統合を有効にしても、インシデントとタスクが利用可能

トラッキング番号: ASOC-39886

問題: Respond ServerサービスでArcher Cyber Incident & Breach Response(NetWitness SecOps Manager)との統合を有効化すると、それ以降、すべてのインシデントがArcher Cyber Incident & Breach Responseで管理されます。以前のバージョンでは、SecOpsを有効化すると、インシデントと改善タスクは表示されなくなりました。NetWitness Platform 11.0.0.xでは、ユーザは引き続き、[対応]ビューでインシデントとタスクにアクセスできます([対応]＞[インシデント]および[対応]＞[タスク]) 。また、NetWitness Platformでインシデントを作成することもできます。[対応]の[アラート リスト]ビュー([対応]＞[アラート]) または[調査]ビューでインシデントを作成した場合、そのインシデントはArcher Cyber Incident & Breach Responseには送信されません。

回避策: Respond ServerサービスでArcher Cyber Incident & Breach Response(NetWitness SecOps Manager) の統合を有効化した場合は、[対応]ビューの [インシデント リスト] ビュー、[インシデントの詳細]ビュー、[タスク リスト]ビューを使用しないでください。また、[対応]の[アラート リスト]ビューや[調査]ビューからインシデントを作成しないでください。

移行したインシデントでは、[概要]パネルにイベント数が常に0と表示される

トラッキング番号: ASOC-38026

問題: 移行したインシデントの場合、インシデントの[概要]パネルの[要因]フィールドには、イベントの数が常に0(ゼロ) と表示されます。これは、NetWitness Platform 11.0.0.x以降では想定された動作です ([概要]パネルにアクセスするには、[対応]＞[インシデント]に移動します。インシデントのリストでインシデントをクリックすると、右側に[概要]パネルが表示されます。また、インシデントのリストで[ID]または[名前]フィールドにあるリンクをクリックすると、[インシデントの詳細]ビューが表示され、左側に[概要]パネルが表示されます) 。

回避策: なし。

インメモリー テーブル エンリッチメントの情報が、ESAアラートに表示されない

トラッキング番号: ASOC-37533

問題: [対応]の[アラート]ビューに、ESA相関ルールのカスタム エンリッチメントを表示できません。

回避策: なし。

Archer Cyber Incident & Breach Responseとの統合設定は、ユーザ インタフェースから参照できる必要がある

トラッキング番号: ASOC-25127

問題: Archer Cyber Incident & Breach Response(NetWitness SecOps Manager) にすべてのインシデントを送信するための統合設定は、ユーザ インタフェースから参照できる必要があります。

回避策: Archer Cyber Incident & Breach Response(NetWitness SecOps Manager) の部分的統合のためのユーザ インタフェースは、11.0.0.xでは削除されました。管理者は、Respond Serverサービスの[エクスプローラ]ビューから統合を完了できます。

Log Collector

Log CollectorサービスではFIPSがデフォルトで無効になっている

トラッキング番号: ASOC-41841

問題: 11.2.0.0でFIPSを有効にしても、Log Collectorサービスではデフォルトでが無効になります。

注: アップグレード後に、11.2.0.0でFIPSを有効にしても、無効になります。

回避策: Log CollectorサービスでFIPSを有効にするには、次の手順を実行します。

1. Log Collectorサービスを停止します。
2. `/etc/systemd/system/nwlogcollector.service.d/nwlogcollector-opts-managed.conf` ファイルを開きます。

3. 次の変数の値をoffに変更します。

   ```
   Environment="OWB_ALLOW_NON_FIPS=on"
   ```

   変更後:

   ```
   Environment="OWB_ALLOW_NON_FIPS=off"
   ```

4. `systemctl daemon-reload`コマンドを実行して、システム デーモンを再ロードします。

5. Log Collectorサービスを再起動します。

6. ユーザ インタフェースで、Log CollectorサービスのFIPSモードを設定します。

   注: アップグレードの場合、11.2.0.0でFIPSを有効にした場合は、このステップを実行する必要はありません。

   a. [**管理**]>[**サービス**]に移動します。

   b. Log Collectorサービスを選択し、[**表示**]>[**構成**]に移動します。

   c. [SSL FIPS Mode]のチェックボックスを選択し、[**適用**]をクリックします。

   注: Log DecoderとPacket DecoderでFIPSを有効にするには、 `/sys/config`の`ssl.fips`をONに設定し、サービスを再起動します。

調査

インポートした調査プロファイルが[プロファイル]ドロップダウン メニューに表示されない

トラッキング番号: ASOC-61230

問題: [ナビゲート]ビューまたは[イベント]ビューで[プロファイルの管理]ダイアログを使用して、プロファイルをインポートすると、新しくインポートされたプロファイルは[プロファイル]ドロップダウン メニューに追加されません。

回避策: ブラウザ ウィンドウを更新すると、追加したプロファイルが表示されます。

[イベント分析]ビューでログ イベントとネットワーク イベントが別々に表示される

トラッキング番号: ASOC-60941

問題: [イベント]ビューでイベントを時間でソートすると、ネットワーク イベントとログ イベントを区別することなくすべてのイベントが時間順に表示されますが、[イベント分析]ビューでは、ソート方法が異なります。[イベント分析]ビューでは、ログ イベントとネットワーク イベントが混在することなく、代わりに、すべてのログ イベントを時間順にソートし、その後にすべてのネットワーク イベントを時間順にソートしたものが表示されます。

回避策: ログ イベントとネットワーク イベントを区別することなく表示する場合は、[イベント]ビューを使用します。

[イベント]ビューから大きなPCAPを抽出し、5分後にタイムアウトした場合、ジョブトレイのエラー メッセージにクエリ時間が8時間と表示される

トラッキング番号: ASOC-60464

問題: [イベント]ビューで、[エクスポート]>[すべてのPCAPのエクスポート]を使用して10万セッション未満のPCAPをエクスポートすると、5分のパケット コール タイムアウトにより、ダウンロードが失敗する場合があります。タイムアウトした場合、ジョブトレイのエラー メッセージに、タイムアウトの時間が8時間(2880万ミリ秒)と誤って表示されます。

回避策: なし。

investigate-server*権限のないユーザが[イベント分析]ビューにアクセスした時に適切なエラー メッセージが表示されない

トラッキング番号: ASOC-60366

問題: 管理者がユーザにinvestigate-server*権限を割り当てていない場合、[イベント分析]ビューでセッションを表示しようとすると、permission deniedエラーが表示されるべきです。代わりに、内部サーバ エラーが表示されます。

回避策: なし。

[イベント分析]ビューでは、ユーザ名などのActive Directoryのメタ値に、コンテキスト データが利用できることを示す下線が表示されない

トラッキング番号: ASOC-58853

問題: アナリストが[イベント分析]ビューで作業している場合、Active Directoryのメタデータにコンテキスト エンリッチメントがあることを示すインジケータが表示されません。Active Directoryのメタ値にカーソルを移動して、関連するコンテキストがあるかどうかを確認し、[コンテキスト ルックアップ]パネルを開く必要があります。

回避策: メタ値にカーソルを移動するか、メタ値を選択し、[**コンテキストの表示**]ボタンをクリックして、Active Directoryに関連するコンテキストがあるかどうかを確認します。

ドリルダウン ポイントのURLが非常に長い場合、[イベント分析]ビューでクエリを実行すると、エラー(414リクエスト エラー) が返される

トラッキング番号: ASOC-50196

問題: いくつかの状況で非常に長いクエリが作成される可能性がありますが、特にInternet Explorerを使用している場合、他のブラウザよりも文字数制限が短いため、対応できない可能性が高くなります。[レポート]から[イベント分析への移行]を実行すると、非常に長いクエリが生成される可能性があります。また、[ナビゲート]ビューでの移動の数により非常に長いクエリが作成される可能性があります。

回避策: [イベント分析]ビューでURLが長すぎて処理できない場合は、[ナビゲート]ビューまたは[イベント]ビューで作業します。

[イベント分析]ビューのクエリビルダは、フィルタにスペースが含まれていると応答しない

トラッキング番号: ASOC-49427

問題: フィルタを追加する時、<meta key>の前、<meta key>と<operator>の間、<operator>の後にスペースを追加すると、クエリビルダが応答しなくなり、[Query Events]ボタンも無効になるため、他のフィルタを追加できなくなります。

回避策: 既存のフィルタをクリックしてから、クエリビルダをクリックします。これで解決しない場合は、ページを更新します。

カスタムFeed

STIX Feedの進捗バーのステータスが完了にならない

トラッキング番号: ASOC-40642

問題: 一部のSTIX Feedで、FeedがDecoderに正常にプッシュされていても、進捗バーのステータスが完了にならない場合があります。

回避策: なし。

ESA(Event Stream Analysis)

アップグレードまたはESAホストのリブートにより、ESA CHルールが無効になる

トラッキング番号: ASOC-60511

問題: Context Hubを使用するESAルールを導入している場合、ESAホストをリブートすると、そのルールが無効になる場合があります。この問題は、ESAホスト上でのContext HubサービスとEvent Stream Analysisサービスの起動順序が原因で発生します。

回避策: この問題を解決するには、次のいずれかを実行します。

- [構成]>[ESAルール]>[サービス]タブに移動し、Context Hubを使用するため無効化されてしまったルールを有効にします。
- Event Stream Analysisサービスを再起動します。

カスタムメタを使用するESAルールがESA Serverに導入されない

トラッキング番号: ASOC-60367

問題: 11.2で新しいカスタムメタキーを追加した場合、それらのメタキーを使用するESAルールが導入されない可能性があります。この問題は、Event Stream AnalysisサービスがConcentratorから新しいカスタムメタの情報を必要とするために発生します。

回避策: カスタムメタを含むESA相関ルールを導入するには、次の手順を実行します。

1. index-concentrator-custom.xmlファイルにカスタムメタキーを追加します([管理]>[サービス]で[Concentrator]を選択し、[アクション]>[表示]>[構成]>[ファイル]タブを選択)。

2. Concentratorを再起動します([管理] > [サービス] で [Concentrator] を選択し、[アクション] > [再起動] を選択) 。
3. ConcentratorがEvent Stream Analysisサービスのデータ ソースとして構成されていることを確認します([管理] > [サービス] で [Event Stream Analysis] を選択し、[アクション] > [表示] > [構成] > [データ ソース] タブを選択) 。
4. Event Stream Analysisサービスを再起動します([アクション] > [再起動]) 。
5. 新しいメタ キーがメタ キー参照のリストに追加されていることを確認します([構成] > [ESAルール] > [設定] タブ > [メタ キー参照]) 。
6. カスタム メタを含むESAルールを導入します。

エンリッチメントで配列メタを使用するESAルールを導入できない

トラッキング番号 : ASOC-47584

問題 : ESAのエンリッチメント ソースとしてインメモリ テーブル(テーブル列のタイプは文字列) を構成し、ホワイトリスト条件を使用するESAルールを作成し、文字列リストの列を文字列配列イベント メタ キーにマッピングします。このルールを導入すると、文字列配列から文字列へのデータタイプの変換は許可されないため、ルールは無効になります。

回避策 : なし。

エンリッチメント ソースを使用するESAルールで、最初のステートメントでは[大文字と小文字を区別しない] オプションが機能しない

トラッキング番号 : ASOC-49906

問題 : エンリッチメント ソースを使用するESAルールを作成する場合、最初のステートメントで [大文字と小文字を区別しない] オプションを有効にすると、結果が返されません。この問題は、最初のステートメント以外(つまり、サブステートメント) では発生しません。

回避策 : 新しいルールを作成する場合、現在は [大文字と小文字を区別しない] オプションが無効になっています。エンリッチメント ステートメントで [大文字と小文字を区別しない] オプションが有効になっている既存のルールの場合、オプションは引き続き有効ですが、ユーザがESAルールを開くと、オプションを無効にして更新したルールを保存するようプロンプトが表示されます。

ESAの圧縮レベルを、他のアプライアンスと同様に設定することができない

トラッキング番号 : ASOC-26481

問題 : 管理者が [エクスプローラ] ビューを使用しても、その他のアプライアンスと同様には、ESAの圧縮レベルを設定できません。

回避策 : 圧縮レベルの変更が反映されるように、ESAからConcentratorソースを削除し、再度追加します。

1. ESAからConcentratorデータ ソースを削除します ([管理] > [サービス] に移動し、Event Stream Analysisサービスを選択して、[アクション] メニューで [表示] > [構成] を選択します。[構成] ビューの [データ ソース] タブでConcentratorデータ ソースを削除します) 。

2. ESAの圧縮レベルを設定します ([エクスプローラ]ビューに移動し、ノード リストで Workflow/Source/nextgenAggregationSourceに移動して、CompressionLevelを設定します) 。
3. Concentratorデータ ソースをESAに再度追加します ([構成]ビューの[データ ソース]タブに戻り、Concentratorデータ ソースを追加します) 。

クエリ ベース集計を使用したログの自動脅威検出により、Event Stream Analysisサービスが応答しなくなる

トラッキング番号 : ASOC-25174

問題 : リソース使用率が高いためにEvent Stream Analysisが応答しなくなる場合があります。wrapper設定の調整が必要になる場合があります。

回避策 : `wrapper.conf`ファイルのping時間の設定変更が必要になる場合があります。次の手順を実行します。

1. **[管理]＞[サービス]＞[Event Stream Analysis]＞[エクスプローラ]**に移動し、**`/opt/rsa/esa/conf/`**フォルダに移動します。
2. 設定を、次の値に変更します。
   `wrapper.ping.timeout=300`
3. 次の行をファイルの末尾に追加します。
   `wrapper.restart.delay=40`
   `wrapper.ping.timeout.action=RESTART`
4. Event Stream Analysisサービスを再起動します。

ESAに配列演算子の警告が表示される

トラッキング番号 : ASOC-14157

問題 : 詳細ルールを作成するときに、anyOfなどの配列演算子が失敗します。次に例を挙げます。

```
SELECT * FROM
Event(
alias_host.anyOf(i => i.length()>50)
);
```

このルールにより、次のようなエラーが発生します。

```
Logger name:
com.espertech.esper.epl.enummethod.dot.PropertyExprEvaluatorScalarArray
Thread: pipeline-sessions-0
Level : WARN
Message : Expected array-type input from property 'alias_host' but received class
java.util.Vector
```

回避策 : あいまいな比較を実行するためには、まず、配列を文字列に変換します。次に例を挙げます。

SELECT * from Event **(cast(alias_host, string)**LIKE '%TESTHOST%');

注 : バージョン10.5、10.5.0.1、10.6で開発されたEPLで配列演算子を使用していた場合は、前述の回避策を使用するためにEPLを変更する必要があります。

外部データベースをホストしているサーバがダウンした場合、導入が失敗する

トラッキング番号 : ASOC-9011

問題 : データベースをルールのエンリッチメント ソースとして使用するようにデータベース接続を構成します。データベースへの参照は、ESAがそのデータベースを使用するルールを導入しない場合でもすべてのESAに導入されます。データベースをホストしているサーバがダウンした場合、新しいルールの導入が失敗します。

回避策 : データベースをホストしているサーバを再起動します。

レポート

非表示オプションと調査オプションが、Windows 10オペレーティング システム上のGoogle ChromeとMozilla Firefoxブラウザでサポートされていない

トラッキング番号 : ASOC-37590

問題 : Windows 10オペレーティング システム上のChromeまたはFirefoxブラウザを使用している場合は、チャートのデータ ポイントをクリックしても、非表示オプションと調査オプションが表示されません。ただし、これらのオプションは、Internet Explorerブラウザを使用すると使用できます。

回避策 : ChromeおよびFirefoxブラウザで、タッチ機能を無効化します。このオプションをChromeで無効にするには、次の手順を使用します。

1. Chromeブラウザで「chrome://flags/」に移動します。
2. 「Touch Events API」フラグの「Disabled」オプションを選択します。
3. ブラウザを再起動します。

このオプションをFirefoxで無効にするには、次の手順を使用します。

1. 「about:config」に移動します。
2. 「危険性を承知の上で使用する」をクリックします。
3. 「dom.w3c_touch_events.enabled」という「設定名」を見つけます。
4. 「値」列を0に更新します。
5. ブラウザを再起動します。

イベント ソース管理

イベント ソースが手動で作成された場合、[Parserマッピングの管理]ウィンドウで、ログParserの[表示名]が空白になる

トラッキング番号: ASOC-53914

問題: [管理]>[イベント ソース]>[検出]ビューから[Parserマッピングの管理]ウィンドウを開くと、手動で作成されたイベント ソースにマッピングされたログParserの表示名が空白になります。

回避策: マッピングのウィンドウを閉じて、再度開きます。

自動マッピングされたアドレスに一部のタイプが表示されない

トラッキング番号: ASOC-48328

問題: 自動マッピングされた既存のイベント ソースに新しいアプリケーションが追加された場合、イベント ソースの[検出]ビューにタイプが表示されるまでに時間がかかり、その間自動マッピングと表示されなくなる可能性があります。

回避策: なし。

メモリー不足によりSMSサービスがクラッシュする

トラッキング番号: ASOC-62575

問題: アクティブなイベント ソースが大量にある場合、システムのログ統計メッセージの処理が追いつかず、SMSサービスが**java.lang.OutOfMemoryError: Java heap space** エラーでクラッシュする可能性があります。

回避策: この問題が発生した場合、回避策について、RSAカスタマー サポートにお問い合わせください。

コア サービス

Broker、Concentrator、Archiverでは、サービスの[構成]ビューの[SSL FIPS Mode]チェック ボックスを変更してもFIPSモードをオフにできないため、チェックボックスを変更不可にするべきである

トラッキング番号: ASOC-41902

問題: 11.0.0.x以降では、Broker、Concentrator、Archiverは常にFIPSが有効であり、管理者が、FIPSと非FIPSを切り替えることはできません。管理者は、[SSL FIPS Mode]チェック ボックスを使用して、Log Decoder、Packet Decoder、Log CollectorのFIPSモードのオンとオフを切り替えることはできます。

回避策: なし。

カスタムFeed構成: 高度なオプション、複数のmetacallbackによるXMLファイル無効のエラー

トラッキング番号: ASOC-40867

問題: Netwitness Platformは、複数のコールバックが存在する、XML用のFeedのアップロードをサポートしていません。

回避策: NwConsoleを使用するか、DecoderのREST URLを直接使用して、アドホックFeedをアップロードすることができます。この方法は、定期実行Feedには使用できません。

製品ドキュメント

本リリースでは、以下のドキュメントが提供されています。

ドキュメント	URL
RSA NetWitness Platform 11.2 オンライン ドキュメント	https://community.rsa.com/community/products/netwitness/112
RSA NetWitness Platform 11.2 アップグレード ガイド	https://community.rsa.com/community/products/netwitness/112/content?filterID=contentstatus%5Bpublished%5D~category%5Binstallation-upgrade%5D
RSA NetWitness Platform 11.2 アップグレード チェックリスト	仮想ホスト アップグレード チェックリスト(バージョン10.6.6.xから11.2) 物理ホスト アップグレード チェックリスト(バージョン10.6.6.xから11.2)
RSA NetWitness Platform ハードウェア セットアップ ガイド	https://community.rsa.com/community/products/netwitness/hardware-setup-guides
RSA NetWitness PlatformのRSA コンテンツ	https://community.rsa.com/community/products/netwitness/rsa-content

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ときは、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

質問やサポートについては、以下の連絡先までお問い合わせください。

RSA Link	https://community.rsa.com
メール	support@rsa.com
各国のお問い合わせ先	http://japan.emc.com/support/rsa/contact/phone-numbers.htm
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。

改訂履歴

リビジョン	日付	説明
1.0	2018年8月15日	Release to Operations