RSA NETWITNESS® PLATFORM

リリース ノート

バージョン11.2.1

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 4

新機能 4

NetWitness UEBA(User and Entity Behavior Analysis) 4

修正された問題 4

セキュリティ 4

サーバ 5

レポート 5

調査 5

ヘルス モニタ 6

Event Stream Analysis 6

コア サービス 6

ビルド番号 6

アップグレード手順 7

既知の問題 8

UEBA 8

製品ドキュメント 9

製品ドキュメントに関するフィードバック 9

カスタマー サポートへのお問い合わせ 9

改訂履歴 10

はじめに

このドキュメントは、NetWitness Platform 11.2.1.0の機能拡張と修正について記述しています。NetWitness Platform 11.2.1.0を新規導入または更新する前にお読みください。

新機能

NetWitness Platform 11.2.1.0 リリースでは、次の機能拡張が提供されます。

NetWitness UEBA(User and Entity Behavior Analysis)

リモート アクセス モデルのサポート。UEBAは、リモート デスクトップ プロトコルを使用したリモート コンピュータへのユーザ アクセス モデルをサポートします。このモデルは、各ユーザが通常アクセスするリモート コンピュータを定義し、異常なアクセスを検知します。詳細については、*RSA NetWitness UEBAユーザ 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-61704	Yum-utilsのセキュリティ更新 https://access.redhat.com/errata/RHSA-2018:2285
ASOC-61929	カーネルのセキュリティ 更新 https://access.redhat.com/errata/RHSA-2018:2384
ASOC-60399	Openjdkのセキュリティ更新 https://access.redhat.com/errata/RHSA-2018:2242
ASOC-59638	Gnupg2のセキュリティ 更新 https://access.redhat.com/errata/RHSA-2018:2181

トラッキング番号	説明
ASOC-62742	postgresql のセキュリティ更新 https://access.redhat.com/errata/RHSA-2018:2557
ASOC-62744	Bindのセキュリティ更新 https://access.redhat.com/errata/RHSA-2018:2570
ASOC-59640	Pythonのセキュリティ 更新 https://access.redhat.com/errata/RHSA-2018:2123

サーバ

トラッキング番号	説明
SACE-10385/ SACE-10364	[ヘルス モニタ]ビューに更新されたページが表示されない。
SACE-9850	[チャート]ビューで、昇順または降順でソートしても結果が表示されない。

レポート

トラッキング番号	説明
SACE-10456	[ルール]ビューで、WHERE句を定義すると、各条件の後にスペースが自動的に追加される。

調査

トラッキング番号	説明
SACE-10329	[調査]ビューでクエリを実行するとき、[クエリ]ダイアログに6文字までしか入力できない。
SACE-10162	調査のメタ グループを使用したクエリで、CIDR形式のIP アドレスがサポートされない。

トラッキング番号	説明
SACE-10060	整数タイプのメタキーの場合、Intelli Senseのドロップ ダウンに演算子が表示されない。

ヘルス モニタ

トラッキング番号	説明
SACE-10237	イベント ソースをエクスポートすると、無効なCSVファイルが作成される。

Event Stream Analysis

トラッキング番号	説明
SACE-9793	Whoisサービスを構成するとエラーが発生する。

コア サービス

コア サービスには、Broker、Concentrator、Decoder、Log Decoderが含まれます。

トラッキング番号	説明
SACE-10222	Concentratorの再起動時に、ログの出力が欠落する。

ビルド番号

以下の表は、NetWitness Platform 11.2.1.0の各種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 Platform Web Server	11.2.1-x
NetWitness Platform Decoder	11.2.1-x
NetWitness Platform Concentrator	11.2.1-x

NetWitness Platform Broker	11.2.1-x
NetWitness Platform Log Decoder	11.2.1-x
NetWitness Platform Archiver (Workbench)	11.2.1-x
NetWitness Platform Event Stream Analysis Server	11.2.1-x
NetWitness Platform Appliance	11.2.1-x
NetWitness Platform Archiver	11.2.1-x
NetWitness Platform Cloud Gateway Server	11.2.1-x
NetWitness Platform Concentrator	11.2.1-x
NetWitness Platform Console	11.2.1-x
NetWitness Platform Endpoint Server	11.2.1-x
NetWitness Platform Investigate Server	11.2.1-x
NetWitness Platform Legacy Web Server	11.2.1-x
NetWitness Platform Log Player	11.2.1-x
NetWitness Platform Respond Server	11.2.1-x
NetWitness Platform SDK	11.2.1-x

アップグレード手順

NetWitness Platform 11.2.1.0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 11.1.0.0から11.2.1.0
- RSA NetWitness® Platform 11.1.0.1から11.2.1.0
- RSA NetWitness® Platform 11.1.0.2から11.2.1.0
- RSA NetWitness® Platform 11.1.0.3から11.2.1.0
- RSA NetWitness® Platform 11.2.0.0から11.2.1.0
- RSA NetWitness® Platform 11.2.0.1から11.2.1.0

11.2.1.0へのアップグレードの詳細については、インストールとアップグレードセクションに記載されているアップグレード手順を参照してください。

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。

注: 11.2.1.0よりも前のリリースの既知の問題は、パッチ リリースで修正されている場合があります。RSA Link(https://community.rsa.com/) でパッチのリリース ノートを参照してください。

UEBA

UEBAポリシーに統計が重複してリストされる

トラッキング番号: ASOC-70119

問題: UEBAポリシーでルールを作成すると、[統計]ドロップダウン リストに重複する値が表示されます。

回避策:

1. 次のコマンドを使用してMongoDBにログインします:
   `mongo admin -u deploy_admin -p {`**パスワードを入力します**`}`
2. MongoDBで次のコマンドを実行します:
```
use sms;
db.getCollection('sms_statdefinition').find({componentId
:"presidioairflow"})
db.getCollection('sms_statdefinition').deleteMany({componentId
:"presidioairflow"})
```

UEBAサービスに誤ったバージョンが表示される

トラッキング番号: ASOC-69605

問題: NetWitness Platformを11.2.1に更新すると、**[管理]**>**[ホスト]**ビューに誤ったUEBAバージョンが表示される。

回避策: UEBAサービスを更新する必要があります。

1. **[管理]**>**[ホスト]**に移動します。
2. UEBAホストを選択します。
3. ツールバーの[**更新**]>[**ホストの更新**]をクリックします。
4. [**更新を開始**]をクリックします。

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

製品ドキュメントに関するフィードバック

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

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	2018/12/17	第2稿