



リリースノート

バージョン11.2.0.1



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

リリースノート	4
修正された問題	4
サーバの修正	4
Malware Analysisの修正	4
Event Source Managementの修正	4
コア サービスの修正	4
ビルド番号	5
更新手順	6
更新タスク	6
タスク1: Decoderサービスを無効にする	6
タスク2: パッチの更新	6
オンライン(Liveサービスに接続可): NetWitnessユーザ インタフェースを使用した更新	6
前提条件	7
手順	7
オフライン(Liveサービスへの接続不可): コマンド ライン インタフェースを使用した更新	8
前提条件	8
手順	8
CLIによる更新のための外部リポジトリ更新手順	9
更新後のタスク	10
タスク1(オプション): カスタム証明書 の移動	10
タスク2(オプション): PAM Radius認証の再構成	10
タスク3: Respond Serverの再起動	11
タスク4: 10Gドライバの場所の変更	11
製品ドキュメント	13
製品ドキュメントに関するフィードバック	13
カスタマー サポートへのお問い合わせ	13
カスタマー サポートに連絡するための準備	14
改訂履歴	14

リリースノート

このドキュメントは、NetWitness Platform 11.2.0.1の修正について記述しています。NetWitness Platform 11.2.0.1を新規導入または更新する前にお読みください。

修正された問題

このドキュメントは、NetWitness Platform 11.2.0.1で修正された問題について記述しています。

サーバの修正

トラッキング番号	説明
ASOC-64089	ローカリゼーションを有効にすると、アプリケーションの言語設定がリセットされる。このため、NetWitness Platform 11.2.0.0では、言語としてフランス語、ドイツ語、日本語を選択できない。

Malware Analysisの修正

トラッキング番号	説明
SACE-9874	古いバージョンのハッシュURLコールを使用すると、Malware Analysisにウイルス対策ベンダーの詳細が表示されない。

Event Source Managementの修正

トラッキング番号	説明
ASOC-62575	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 <code>java.lang.OutOfMemoryError: Java heap space</code> エラーでクラッシュする場合があった。

コアサービスの修正

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-10191	save.session.countがAutoに設定されていると、Log Decoderサービスが再生成される。
SACE-10283	Parserのディレクトリ構造が正しくないため、Log DecoderでmetaDBが再生成される。
SACE-10336	10Gネットワークカードドライバが原因でNetwork Decoderがクラッシュする。

ビルド番号

以下の表は、NetWitness Platform 11.2.0.1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 Platform Decoder	11.2.0.1-9473.5
NetWitness Platform Concentrator	11.2.0.1-9473.5
NetWitness Platform Broker	11.2.0.1-9473.5
NetWitness Platform Log Decoder	11.2.0.1-9473.5
NetWitness Platform Archiver (Workbench)	11.2.0.1-9473.5
NetWitness Platform Event Stream Analysis Server	11.2.0.1-448.5
NetWitness Platform Appliance	11.2.0.1-9473.5
NetWitness Platform Archiver	11.2.0.1-9473.5
NetWitness Platform Console	11.2.0.1-9473.5
NetWitness Platform Legacy Web Server	11.2.0.1-181010193532.5
NetWitness Platform Log Player	11.2.0.1-9473.5
NetWitness Platform SDK	11.2.0.1-9473.5

更新手順

NetWitness Platform バージョン11.2.0.1に更新するには、このセクションの情報を確認し、更新タスクを実行する必要があります。

NetWitness Platform 11.2.0.1では、以下の更新パスがサポートされます。

- NetWitness Platform 11.2.0.0から11.2.0.1
- NetWitness Platform 11.1.0.3から11.2.0.1

11.2.0.0でサポートされる更新パスについては、バージョン11.0.x.xまたは11.1.x.xから11.2への更新ガイドを参照してください。

11.2.0.1パッチの更新は、次のいずれかの方法で適用できます。


- NetWitness Serverがインターネット経由でLiveサービスに接続できる場合、NetWitness Platformのユーザインタフェースを使用してパッチを適用できます。
- NetWitness Serverがインターネット経由でLiveサービスに接続できない場合、CLI(コマンドラインインタフェース)を使用してパッチを適用できます。

更新タスク

タスク1: Decoderサービスを無効にする

11.2.0.1に更新する前に、Network DecoderおよびNetwork Hybridサービスで[Capture Autostart]を無効にする必要があります。

[Capture Autostart]を無効にするには、次の手順を実行します。

1. [管理] > [サービス]に移動します。
[管理]の[サービス]ビューが表示されます。
2. Network DecoderまたはNetwork Hybridサービスを選択し、 > [表示] > [構成]を選択します。
選択したNetwork DecoderまたはNetwork Hybridのサービスの[構成]ビューが表示されます。
3. [Decoderの構成]パネルで、[Capture Autostart]の選択を解除し、[適用]をクリックします。

タスク2: パッチの更新

インターネット接続の有無に応じて、次の更新方法のいずれかを選択します。

オンライン(Liveサービスに接続可) : NetWitnessユーザ インタフェースを使用した更新

この方法は、NetWitness ServerがLiveサービスに接続されており、パッケージを入手できる場合に使用できます。

注: 11.1.0.3から11.2.0.1にはオンラインで更新することができます。11.1.0.xから11.2.0.1に更新する場合は、最初にNetWitness Platform 11.2.0.0にアップグレードしてから11.2.0.1に更新する必要があります。

注: NetWitness ServerがLiveサービスにアクセスできない場合は、[オフライン\(Liveサービスへの接続不可\): コマンドライン インタフェースを使用した更新](#)を実行します。

前提条件

以下の項目を確認します。

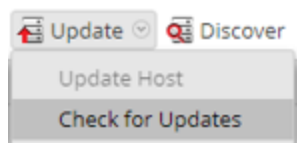
1. [管理] > [システム] > [更新]で、[新しい更新の情報を毎日自動的にダウンロード]チェックボックスがオンになっていることを確認します。
2. [管理] > [ホスト] > [更新] > [更新の確認]を実行し、更新の有無を確認します。[ホスト]ページに[更新あり]ステータスが表示されることを確認します。
3. [更新のバージョン]列に11.2.0.1が表示されることを確認します。


注: カスタム証明書を使用する場合は、カスタム証明書を/etc/pki/nw/trust/import/ディレクトリから/root/certに移動します。次の手順を実行します。

- 1.) `mkdir /root/cert`
- 2.) `mv /etc/pki/nw/trust/import/* /root/cert`

手順

1. [管理] > [ホスト]に移動します。
2. NetWitness Server(nw-server) ホストを選択します。
3. 最新の更新をチェックします。



4. 選択したホストの更新バージョンがローカル更新リポジトリにある場合は、[ステータス]列に[更新あり]と表示されます。
5. [更新のバージョン]列で[11.2.0.1]を選択します。
次の手順を実行します。
 - 各更新の主な機能と更新に関する情報をダイアログに表示したい場合は、更新バージョン番号の右側にある情報アイコン()をクリックします。
 - 目的のバージョンが見つからない場合は、[更新] > [更新の確認]を選択し、リポジトリ内の使用可能な更新をチェックします。更新が利用可能な場合、「新しい更新が利用可能です」というメッ

ページが表示され、[ステータス]列が自動的に更新されて、[更新あり]と表示されます。デフォルトでは、選択したホストでサポートされている更新のみが表示されます。

6. ツールバーの[更新]>[ホストの更新]をクリックします。
7. [更新を開始]をクリックします。
8. [ホストの再起動]をクリックします。
9. 他のホストについても、ステップ6~8を繰り返します。

注: NetWitness Admin Serverを更新して再起動した後でのみ、複数のホストを選択して同時に更新することができます。ESA、Endpoint Insights、Malware Analysisホストは、NW Admin ServerまたはNetWitness Admin Serverと同じバージョンに更新する必要があります。

注: 11.2.0.1ではすべてのコンポーネントが変更されたわけではないため、更新を適用した後でも一部のコンポーネントに異なるバージョン番号が表示される可能性があります。このリリースで更新されたコンポーネントのリストについては、「[ビルド番号](#)」を参照してください。

オフライン(Liveサービスへの接続不可): コマンドラインインタフェースを使用した更新

この方法は、NetWitness ServerがLiveサービスに接続されていない場合に使用できます。

前提条件

以下の項目を確認します。

- RSA Link(<https://community.rsa.com/>) > NetWitness Platform > Downloads > RSA NetWitness Logs and Network > Version 11.2 > PATCHESから下記のファイルをローカルディレクトリにダウンロードします。このファイルには、NetWitness Platform 11.2.0.1のすべての更新ファイルが含まれます。
netwitness-11.2.0.1.zip

手順

NW Admin Serverとその他のコンポーネントホストで、更新の手順を実行する必要があります。

注: 11.1.0.3から11.2.0.1に更新する場合は、NetWitness Platform 11.2.0.0の更新(netwitness-11.2.0.0.zip)をダウンロードし、11.2.0.1のファイルと共にステージングフォルダに配置する必要があります。11.1.0.xから11.2.0.1に更新する場合は、最初にNetWitness Platform 11.2.0.0にアップグレードしてから11.2.0.1に更新する必要があります。

注: PDFからコマンドをコピーしてLinux SSHターミナルに貼り付けても、正しく入力できません。コマンドを手入力することを推奨します。

1. 11.2.0.1のステージングのため、NetWitness Server上に/tmp/upgrade/11.2.0.1ディレクトリを作成し、そこにzipパッケージを解凍します。

```
unzip netwitness-11.2.0.1.zip -d /tmp/upgrade/11.2.0.1
```


注:作成したステージング ディレクトリに.zipファイルをコピーし、その場所で解凍した場合は、解凍後、元の.zipファイルを忘れずに削除してください。

2. 次のコマンドを実行して、更新を初期化します。

```
upgrade-cli-client --init --version 11.2.0.1 --stage-dir /tmp/upgrade
```

3. 次のコマンドを実行して、NetWitness Serverを更新します。

```
upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version 11.2.0.1
```

4. コンポーネント ホストの更新が成功した時は、NetWitness UIからホストを再起動します。

5. 各コンポーネント ホストでステップ3~4を繰り返します。コマンドのIPアドレスは、更新するコンポーネントホストのIPアドレスに変更します。

注:NetWitness Serverで、`upgrade-cli-client --list`コマンドを実行すると、すべてのホストのバージョンをチェックすることができます。`upgrade-cli-client`のヘルプを表示するには、`upgrade-cli-client --help`コマンドを使用します。

注:更新処理中に次のエラーが表示される場合があります:

```
2017-11-02 20:13:26.580 ERROR 7994 - [ 127.0.0.1:5671]
o.s.a.r.c.CachingConnectionFactory : Channel shutdown: connection error;
protocol method: #method<connection.close>(reply-code=320, reply-
text=CONNECTION_FORCED - broker forced connection closure with reason
'shutdown', class-id=0, method-id=0)
```

パッチは正常にインストールされます。何のアクションを取る必要もありません。ホストを新しいバージョンに更新する際に他のエラーが発生した場合、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](#))。

CLIIによる更新のための外部リポジトリ更新手順

注:外部リポジトリでは、11.2.0.0と同じディレクトリの下に、11.2.0.1のリポジトリを作成する必要があります。

1. 11.2.0.1のステージングのため、NetWitness Server上に/tmp/upgrade/11.2.0.1ディレクトリを作成し、そこにzipパッケージを解凍します。

```
unzip netwitness-11.2.0.1.zip -d /tmp/upgrade/11.2.0.1
```

注:作成したステージング ディレクトリに.zipファイルをコピーし、その場所で解凍した場合は、解凍後、元の.zipファイルを忘れずに削除してください。

2. 次のコマンドを実行して、更新を初期化します。

```
upgrade-cli-client --init --version 11.2.0.1 --stage-dir /tmp/upgrade
```

3. 次のコマンドを実行して、NetWitness Serverを更新します。

```
upgrade-cli-client --upgrade --host-addr <IP of Netwitness Server> --version
11.2.0.1
```

4. コンポーネント ホストの更新が成功した時は、NetWitness UIからホストを再起動します。

5. 各コンポーネント ホストでステップ3~4を繰り返します。コマンドのIPアドレスは、更新するコンポーネントホストのIPアドレスに変更します。

注:NetWitness Serverで、`upgrade-cli-client --list`コマンドを実行すると、すべてのホストのバージョンをチェックすることができます。`upgrade-cli-client`のヘルプを表示するには、`upgrade-cli-client --help`コマンドを使用します。

注:更新処理中に次のエラーが表示される場合があります:

```
2017-11-02 20:13:26.580 ERROR 7994 - [ 127.0.0.1:5671]
```

```
o.s.a.r.c.CachingConnectionFactory : Channel shutdown: connection error;
protocol method: #method<connection.close>(reply-code=320, reply-
text=CONNECTION_FORCED - broker forced connection closure with reason
'shutdown', class-id=0, method-id=0)
```

パッチは正常にインストールされます。何のアクションを取る必要もありません。ホストを新しいバージョンに更新する際に他のエラーが発生した場合、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](#))。

更新後のタスク

タスク1(オプション):カスタム証明書の移動

カスタム証明書を外部ディレクトリから `/etc/pki/nw/trust/import`ディレクトリに移動します。

タスク2(オプション):PAM Radius認証の再構成

11.2.x.xで`pam_radius`パッケージを使用してPAM Radius認証を構成していた場合、11.2.0.1では`pam_radius_auth`パッケージを使用して再構成する必要があります。

Admin Serverが稼働するNW Serverで以下のコマンドを実行する必要があります。

注:11.x.x.xで`pam_radius`を構成した場合、以下のステップを実行して既存のバージョンをアンインストールするか、ステップ2に進みます。

ステップ1:既存のパッケージを確認し、既存の `pam_radius`をアンインストールします

```
rpm -qi |grep pam_radius
yum erase pam_radius
```

ステップ2:次のコマンドを実行して、`pam_radius_auth` パッケージをインストールします。

```
yum install pam_radius_auth
```

ステップ3: RADIUS構成ファイル/etc/raddb/serverを次のように編集し、RADIUSサーバの構成を追加します。

```
# server[:port] shared_secret timeout (s)
server secret 3
```

例: 111.222.33.44 secret 1

ステップ4: NetWitness ServerのPAM構成ファイル/etc/pam.d/securityanalyticsを編集し、次の行を追加します。ファイルが存在しない場合は、ファイルを作成し、次の行を追加します。

```
auth sufficient pam_radius_auth.so
```

ステップ5: 次のコマンドを実行して、/etc/raddb/serverのファイルへの書き込み権限を付与します。

```
chown netwitness:netwitness /etc/raddb/server
```

ステップ6: 次のコマンドを実行して、pam_radius_authライブラリをコピーします。

```
cp /usr/lib/security/pam_radius_auth.so /usr/lib64/security/
```

ステップ7: pam_radius_auth構成に変更を加えた後で、次のコマンドを実行して、jettyサーバを再起動します。

```
systemctl restart jetty
```

タスク3: Respond Serverの再起動

次のコマンドを実行し、Respond Serverを再起動します。

```
systemctl restart rsa-nw-respond-server
```

タスク4: 10Gドライバの場所の変更


現在のカーネルの正しい場所に10Gドライバを配置する必要があります。

ステップ1: 10G Decoderを使用している場合は、11.2.0.1への更新後に以下のコマンドを実行し、Decoderホストをリポートします。上書きを確認するプロンプトが表示されたら、Yをクリックします。

- cp /var/lib/dkms/ixgbe-zc/5.3.7.14/\$(uname -r)/x86_64/module/ixgbe_zc.ko.xz /lib/modules/\$(uname -r)/extra/
- cp /var/lib/dkms/i40e-zc/2.4.6.14/\$(uname -r)/x86_64/module/i40e_zc.ko.xz /lib/modules/\$(uname -r)/extra/
- cp /var/lib/dkms/pfring/6.5.0.14/\$(uname -r)/x86_64/module/pf_ring.ko.xz /lib/modules/\$(uname -r)/extra/

ステップ2: [Capture Autostart]の設定を、[タスク1: Decoderサービスを無効にする](#)の手順に従い無効化した場合は、Network DecoderサービスおよびNetwork Hybridサービスで[Capture Autostart]を再度有効にする必要があります。

[Capture Autostart]を有効にするには、次の手順を実行します。

1. [管理]>[サービス]に移動します。
[管理]の[サービス]ビューが表示されます。
2. Network DecoderまたはNetwork Hybridサービスを選択し、 > [表示]> [構成]を選択します。
選択したNetwork DecoderまたはNetwork Hybridのサービスの[構成]ビューが表示されます。
3. [Decoderの構成]パネルで、[Capture Autostart]を選択し、[適用]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	場所
RSA NetWitness Platform 11.2.0.0 オンラインドキュメント	https://community.rsa.com/community/products/netwitness/112

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

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/rsa-customer-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。

カスタマーサポートに連絡するための準備

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

改訂履歴

リビジョン	日付	説明
0.1	10月25日	最終ドラフト