



更新ガイド

バージョン 11.0.x.xまたは11.1.x.xから11.2



Copyright © 1994-2019 Dell Inc. or its subsidiaries. All rights Reserved.

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、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、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

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

この資料に記載される情報は、発行日時点で正確であるとみなされます。この情報は予告なく変更されることがあります。

2月 2019

目次

概要	5
更新パス	5
混在モードでの実行	5
更新後にEntropy=log2をリセット	5
更新準備タスク	6
全般	6
タスク1: コア ポートを確認してファイアウォール ポートを開く	6
タスク2: Malware Analysis構成 ファイルを別のディレクトリにバックアップする	6
タスク3: データ収集と集計の停止	7
Azureホスト	9
タスク4: (オプション) Azureホストの更新要件	9
Endpoint Insights	10
タスク5: (オプション) 11.2更新プログラムをEndpointホストに適用する前に既存のカスタム メタデー タ マッピングをバックアップ	10
Reporting Engine	10
タスク6: Reporting Engineの標準提供のチャートを構成する	10
Respond	10
タスク7: (オプション) Respondサービスのカスタム キーのリストア	10
タスク8: Respondサービスのカスタム正規化 スクリプトのバックアップ	10
更新タスク	12
[ホスト]ビューから更新を適用する(Webアクセスあり)	12
タスク1: ローカル リポジトリに更新を配置するか、外部リポジトリをセットアップする	12
タスク2: [ホスト]ビューから各ホストに更新を適用する	13
コマンド ラインから更新を適用する(Webアクセスなし)	17
Legacy Windows収集の更新またはインストール	18
更新後のタスク	19
全般	20
タスク1: データ収集と集計の開始	20
タスク2: コンテキスト メニュー アクションのユーザ権限の設定	21
NW Server	23
(オプション) タスク3: Logstash出力構成ファイルで更新されていない監査ログ テンプレートの修正	23
(オプション) タスク4: PAM Radius認証の再構成	23
Endpoint Insights	24
タスク5: Javaバージョンの変更により、レガシーEndpointからの定期実行Feedを再構成	24
タスク6: バックアップしたEndpointカスタム メタデータ マッピングのリストア	24

Event Stream Analysis	25
(オプション)タスク7:自動脅威検出の「Suspected Command and Control Communication By Domain」統合ルールを再構成	25
Respond	26
タスク8:統合ルールスキーマの最新バージョンを取得してRespondサービスのカスタムキーをリストアする	26
タスク9:Respondサービスの正規化スクリプトの最新バージョンの取得、カスタム正規化スクリプトのリストア	27
タスク10:対応の通知設定の権限の追加	27
タスク11:デフォルトのインシデントルールのGroup By値の更新	28
NetWitness UEBA	29
タスク12:NetWitness UEBAのインストール	29
付録A:インストールと更新のトラブルシューティング	30
付録B:ローカルリポジトリへの更新の配置	37
付録C:外部リポジトリのセットアップ	39
改訂履歴	42

概要

RSA NetWitness® Platform 11.2.0.0には、Platformのすべての製品の修正が含まれています。NetWitness Platformのコンポーネントは、NetWitness Server(Admin Server、Config Server、Integration Server、Investigate Server、Orchestration Server、Respond Server、Security Server、Source Server)、Archiver、Broker、Concentrator、Context Hub、Decoder、Endpoint Hybrid、Endpoint Log Hybrid、ESAプライマリ、ESAセカンダリ、Log Collector、Log Decoder、Malware Analysis、Reporting Engine、UEBA、Warehouse Connector、Workbenchで構成されます。

注 : Reporting EngineはNW Serverホストにインストールされます。WorkbenchはArchiverホストにインストールされます。Warehouse ConnectorはDecoderまたはLog Decoderホストにインストールすることができます。

特に記載のない限り、このガイド内の手順は物理ホストと仮想ホスト(AWSとAzure Public Cloudを含む)のどちらにも適用されます。

更新パス

NetWitness Platform 11.2.0.0では、以下の更新パスがサポートされます。

- 11.0.xから11.2.0.0
- 11.1.xから11.2.0.0
- 10.6.6.xから11.2.0.0

NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

10.6.6.xから11.2.0.0にアップグレードする手順については、『*RSA NetWitness Platform 物理ホスト アップグレード ガイド(10.6.6.xから11.2)*』と『*RSA NetWitness Platform 仮想ホスト アップグレード ガイド(10.6.6.xから11.2)*』を参照してください。

混在モードでの実行

混在モードでの実行は、最新バージョンに更新されたサービスと、古いバージョンのままのサービスが混在するときに生じます。詳細については、『*RSA NetWitness Platform ホストおよびサービス スタート ガイド*』の「混在モードでの実行」を参照してください。

更新後にEntropy=log2をリセット

11.0.x.xでEntropy=log2フラグをfalse (Entropy="log2=false")に設定していた場合、NetWitness 11.2に更新した後、このフラグはtrue (Entropy="log2=true")にリセットされます。これは、すべてのソースがパケットとNetWitness Endpoint Insightsを含むようフラグを揃えるために実施されます。必要な場合は、フラグをfalseに戻してlog10の計算:Entropy="log2=false"を引き続き使用することができます。

更新準備タスク

NetWitness Platform 11.2.0.0に更新するには次の手順を実行します。これらのタスクは、次のカテゴリに分類されます。

[全般](#)

[Azureホスト](#)

[Endpoint Insights](#)

[Reporting Engine](#)

[Respond](#)

全般

タスク1: コアポートを確認してファイアウォールポートを開く

次の表は、11.2.0.0での新しいポートを示します。

注意: ポートに接続できないことが原因で更新が失敗しないよう、新しいポートを開いたら、更新前にテストします。

Endpoint HybridまたはEndpoint Log Hybrid

ソース ホスト	宛先ホスト	宛先ポート	コメント
Endpoint HybridまたはEndpoint Log Hybrid	NW Server	TCP 5672	メッセージ バス
Endpoint Server	NW Server	TCP 27017	MongoDB

タスク2: Malware Analysis構成ファイルを別のディレクトリにバックアップする

1. 次のファイルを別の安全なディレクトリにバックアップします。

```
/var/lib/netwitness/malware-analytics-  
server/spectrum/conf/malwareCEFDictionaryConfiguration.xml
```

Malware Analysisホストを11.2.0.0に更新した後、カスタムパラメータ値をこのバックアップから取得する必要があります。更新によって新しい構成ファイルが作成され、すべてのパラメータはデフォルト値に設定されます。

2. 次のファイルを削除します。

```
/var/lib/netwitness/malware-analytics-  
server/spectrum/conf/malwareCEFDictionaryConfiguration.xml
```

タスク3: データ収集と集計の停止

ネットワーク収集の停止

1. NetWitness Platform 11.0.xにログインし、[管理] > [サービス]に移動します。
[サービス]ビューが表示されます。
2. **Decoder**サービスを選択します。

The screenshot displays the NetWitness Platform Admin console interface. The top navigation bar includes tabs for Hosts, Services, Event Sources, Health & Wellness, System, and Security. The 'Services' tab is active, and the 'S5Decoder - Decoder' service is selected. Below the navigation, there are several action buttons: Upload Packet Capture File, Stop Capture, Host Tasks, Shutdown Service, Shutdown Appliance Service, and Reboot. The main content area is divided into four sections: Decoder Service Information, Appliance Service Information, Decoder User Information, and Host User Information. The Decoder Service Information section shows details for the S5Decoder (Decoder) service, including its name, version (11.1.0.0), memory usage (2858 MB), CPU usage (1%), and running time (2018-Feb-08 02:32:47). The Appliance Service Information section shows details for the S5Decoder (Host) service, including its name, version (11.1.0.0), memory usage (25964 KB), CPU usage (0%), and running time (2018-Feb-06 22:14:56). The Decoder User Information and Host User Information sections are currently empty. The bottom of the page features the RSA | NETWITNESS SUITE logo and the version number 11.1.0.0.

3.  (アクション) で、[表示] > [システム]を選択します。
4. ツールバーで  **Stop Capture** をクリックします。

ログ収集の停止

1. NetWitness Platform 11.0.xにログインし、[管理] > [サービス]に移動します。
[サービス]ビューが表示されます。

2. Log Decoder サービスを選択します。

The screenshot shows the NetWitness Platform Admin console. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. Below the navigation bar, there are tabs for 'Hosts', 'Services', 'Event Sources', 'Health & Wellness', 'System', and 'Security'. The 'Services' tab is active, and the 'Log Decoder' service is selected. The main content area displays two columns of service information:

Log Decoder Service Information		Appliance Service Information	
Name	S5EndPtLogHyb1783 (Log Decoder)	Name	S5EndPtLogHyb1783 (Host)
Version	11.1.0.0 (Rev null)	Version	11.1.0.0 (Rev null)
Memory Usage	8094 MB (3.14% of 252 GB)	Memory Usage	20468 KB (0.01% of 252 GB)
CPU	10%	CPU	11%
Running Since	2018-Feb-08 07:28:11	Running Since	2018-Feb-06 22:02:59
Uptime	6 hours 19 minutes 46 seconds	Uptime	1 day 15 hours 44 minutes 57 seconds
Current Time	2018-Feb-08 13:47:57	Current Time	2018-Feb-08 13:47:56

Below the service information, there are sections for 'Log Decoder User Information' and 'Host User Information'. The bottom of the console shows the 'RSA NETWITNESS SUITE' logo and the version '11.1.0.0'.

3. (アクション) で、[表示] > [システム] を選択します。

4. ツールバーで Stop Capture をクリックします。

集計の停止

1. NetWitness Platform 11.0.x にログインし、[管理] > [サービス] に移動します。

2. Broker サービスを選択します。

3. (アクション) で、[表示] > [構成] を選択します。

4. [全般] タブが表示されます。

The screenshot shows the NetWitness Platform Admin console with the 'BROKER - Broker' service selected. The 'Config' tab is active, and the 'General' sub-tab is selected. The main content area displays the 'Aggregate Services' table and the 'Aggregation Configuration' settings.

Aggregate Services				
<input checked="" type="checkbox"/>	Address	Port	Rate	Max
<input checked="" type="checkbox"/>	ip-address	56005	1	7091

Aggregation Configuration	
Name	Config Value
Aggregate Autostart	<input type="checkbox"/>
Aggregate Hours	0
Aggregate Interval	60000
Aggregate Max Sessions	5000000
Service Heartbeat	
Heartbeat Error Restart	300

At the bottom of the configuration page, there is an 'Apply' button. The bottom of the console shows the 'admin' user, language 'English (United States)', and time zone 'GMT+00:00'.

5. [サービスの集計] の下にある、 Stop Aggregation をクリックします。

Azureホスト

タスク4: (オプション) Azureホストの更新要件

ご使用のAzureホスト導入環境で次の3つの条件を確認し、該当する場合は必要なタスクを実行します。

- 11.0.0.0のAzureベース イメージを使用している場合(ホストを11.1.0.xに更新した場合も含む)は、CentOS-Baseリポジトリを作成します。

注意: libgudev1-219-30.e17_3.9.x86_64 RPMが存在しない場合は、以下の手順を実行しないでください。

1. SSHでNW Server ホストに接続します。
 2. NW Serverホストのroot ディレクトリから次のコマンドを実行します。

```
yum remove libgudev1-219-30.e17_3.9.x86_64
```
 3. CentOS 7.0+の処理手順(<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/create-upload-centos#centos-70>)のステップ6に記載されているとおりに、CentOS-Baseリポジトリを作成します。
 4. NW Serverホストのroot ディレクトリから次のコマンドを実行します。

```
yum clean all
yum install WALinuxAgent
sudo systemctl enable waagent
```
 5. CentOS-Baseリポジトリを削除します。
- 11.0.0.xから11.2に更新する場合は、追加のパッケージをリポジトリに設定します。
nw-azure-11.1-extras.zipファイルについては、RSAカスタマー サポート(support@rsa.com) までお問い合わせください。
 1. SSHでNW Server ホストに接続します。
 2. NW Serverホスト上のroot ディレクトリに移動します。
 3. 次のコマンドを実行してAzure Zipファイルを解凍します。

```
mkdir -p /var/lib/netwitness/common/repo/11.2.0.0/OS/other+
unzip nw-azure-11.1-extras.zip -d
/var/lib/netwitness/common/repo/11.2.0.0/OS/other
```
 - 外部リポジトリを使用して更新プログラムを適用する場合は、追加のパッケージを外部リポジトリに追加します。
 1. 外部リポジトリに11.2.0.0のコンテンツをセットアップした後、外部リポジトリの<base-directory>11.2.0.0/OS/otherに移動します。
 2. 外部リポジトリの11.2.0.0/OSディレクトリから次のコマンドを実行して、Azure Zipファイルを解凍します。

```
unzip nw-azure-11.1-extras.zip -d /<base-directory>/11.2.0.0/OS/other
```

3. 外部リポジトリの11.2.0.0/OSディレクトリから次のコマンドを実行します。

```
createrepo
```

Endpoint Insights

タスク5: (オプション) 11.2更新プログラムをEndpointホストに適用する前に既存のカスタムメタデータ マッピングをバックアップ

11.2では、Endpointメタデータ マッピングが機能拡張され、現在のUDM(統合データモデル)の変更と整合するようになりました。Endpoint Insightsホストに11.2の更新を適用すると、新しく追加されるデフォルトのメタデータ マッピングが上書きされるのを防ぐため、既存のカスタム マッピングがクリアされます。既存のカスタムメタデータ マッピングを使用する必要がある場合は、Endpoint Insightsホストを11.2に更新する前に、既存のカスタム マッピングをバックアップしておいてください。バックアップするには、次の手順を実行します。

1. nw-shellを使用して、`get-custom` APIを実行します。カスタム マッピングのリストが表示されます。
2. カスタム マッピングを安全なディレクトリに手動でコピーします。

詳細については、『*Endpoint Insights 構成ガイド*』を参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

Reporting Engine

タスク6: Reporting Engineの標準提供のチャートを構成する

標準提供のチャートを更新後に実行するには、更新を実行する前に、Reporting Engineの構成ページでデフォルト データソースを構成しておく必要があります。このタスクを実行しない場合は、更新後に手動でデータソースを設定する必要があります。Reporting Engineのデータソースの詳細については、「*NetWitness Platform 11.2 Reporting Engine 構成ガイド*」を参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

Respond

タスク7: (オプション) Respondサービスのカスタム キーのリストア

11.0で、groupBy句で使用するためにカスタム キーを`/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json`に追加した場合は、カスタム キーをファイルにコピーして保存します。

タスク8: Respondサービスのカスタム正規化スクリプトのバックアップ

11.2.0.0では、Respondサービスの正規化スクリプトが再設計され、`/var/lib/netwitness/respond-server/scripts`ディレクトリに保存されます。11.2.0.0に更新する前に、11.0.xのスクリプトをバックアップします。そうすれば、更新後のタスクの「[Respond](#)」の説明に従い、11.2.0.0にリストアできます。

1. `/var/lib/netwitness/respond-server/scripts`ディレクトリに移動します。
2. 次のファイルをバックアップします。
data_privacy_map.js
normalize_alerts.js
normalize_core_alerts.js
normalize_ecat_alerts.js
normalize_ma_alerts.js
normalize_wtd_alerts.js
utils.js
3. (オプション) 11.0.xまたはそれ以前のリリースでカスタム ロジックを追加した場合、バックアップしたスクリプトからロジックをコピーすることにより、11.2.0.0にリストアできます。

更新タスク

NetWitness Platform 11.0.x.xまたは11.1.x.xを11.2.0.0に更新するには、次の手順を実行します。
ホストにバージョンの更新を適用する方法は2つあります。

注 : NetWitness Platform 11.2.0.0で11.0.x.xまたは11.1.x.xと異なる更新リポジトリ(repo) を使用する予定の場合は、「[付録C: 外部リポジトリのセットアップ](#)」の手順を参照してください。

- [\[ホスト\]ビューから更新を適用する\(Webアクセスあり\)](#)
- [コマンド ラインから更新を適用する\(Webアクセスなし\)](#)

[ホスト]ビューから更新を適用する(Webアクセスあり)

[ホスト]ビューから更新を適用するには、2つのタスクを完了する必要があります。

- タスク1: ローカルリポジトリに更新を配置するか、外部リポジトリをセットアップする。リポジトリに最新のバージョン更新が含まれることを確認します。
- タスク2: [ホスト]ビューからそれぞれのホストに更新を適用する。

タスク1: ローカルリポジトリに更新を配置するか、外部リポジトリをセットアップする

11.2.0.0でNW Serverをセットアップする際に、ローカルリポジトリまたは外部リポジトリを選択します。[ホスト]ビューでは、選択したリポジトリからバージョン更新を取得します。

ローカルリポジトリを選択した場合、セットアップする必要はありませんが、最新バージョンの更新を取り込む必要があります。バージョン更新を配置する手順については、「[付録B: ローカルリポジトリへの更新の配置](#)」を参照してください。

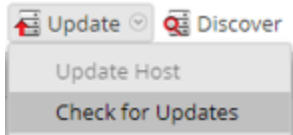
外部リポジトリを選択した場合は、セットアップする必要があります。外部リポジトリをセットアップする手順については、「[付録C: 外部リポジトリのセットアップ](#)」を参照してください。

タスク2: [ホスト]ビューから各ホストに更新を適用する

[ホスト]ビューには、ローカル更新リポジトリにある使用可能なソフトウェアの更新バージョンが表示されます。[ホスト]ビューから必要な更新を選択して適用します。

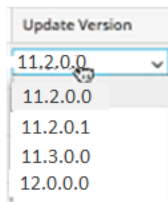
この手順では、ホストをNetWitness Platformの新しいバージョンに更新する方法について説明します。

1. NetWitness Platformにログインします。
2. [管理]>[ホスト]に移動します。
3. (オプション) 最新の更新をチェックします。




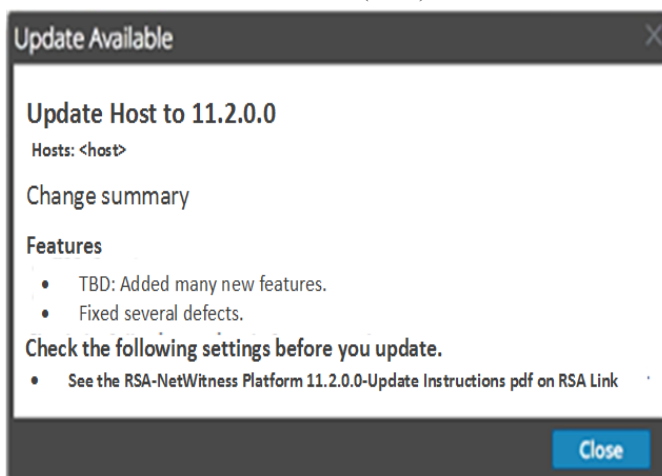
4. 1つまたは複数のホストを選択します。
最初にNW Serverを最新バージョンに更新する必要があります。その他のホストは任意の順序で更新することができますが、『RSA NetWitness Platformホストおよびサービス スタート ガイド』の「混在モードでの実行」のガイドラインに従うことを推奨します。
選択したホストの更新バージョンがローカル更新リポジトリにある場合は、[ステータス]列に[更新あり]が表示されます。

5. [更新のバージョン]列から適用するバージョンを選択します。



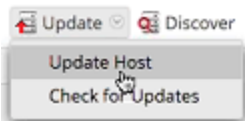
次の手順に従ってください。

- 複数のホストを同じバージョンに更新する場合は、NW Serverホストを更新した後、対象ホストの左のチェックボックスを選択します。現在サポートされている更新バージョンのみが表示されます。
- 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。次のようなダイアログが表示されます。

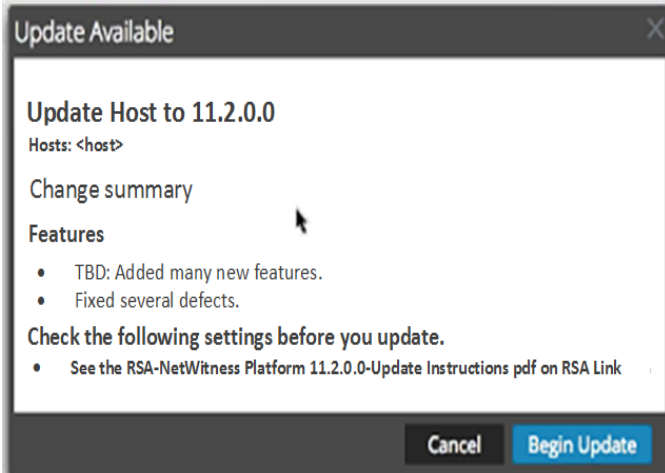


- 目的のバージョンが見つからない場合は、[更新]>[更新の確認]を選択し、リポジトリ内の使用可能な更新をチェックします。更新が利用可能な場合、「新しい更新が利用可能です」というメッセージが表示され、[ステータス]列が自動的に更新されて、[更新あり]が表示されます。デフォルトでは、選択したホストでサポートされている更新のみが表示されます。

6. ツールバーの[更新]>[ホストの更新]をクリックします。



選択した更新に関する情報を示すダイアログが表示されます。[更新を開始]をクリックします。



[ステータス]列には、次のような更新の各段階の状況が表示されます。

- ステージ1: **更新パッケージのダウンロード** - 選択したホスト上のサービスに適用されるリポジトリアーティファクトをNW Serverにダウンロードします。
 - ステージ2: **更新パッケージの構成** - 更新ファイルを正しい形式に構成します。
 - ステージ3: **更新中** - ホストを新しいバージョンに更新しています。
7. 「更新が進行中です」が表示されたら、ブラウザをリフレッシュします。
この操作により、[NetWitnessログイン]画面が表示される場合があります。この画面が表示されたら、ログインして[ホスト]ビューに戻ります。
ホストの更新が完了すると、NetWitness Platformが**ホストの再起動**を求めるメッセージを表示します。
8. (オプション: Unityストレージを使用するホストの場合のみ) 11.1.x.xのホスト(たとえばNetwork Decoderホスト)にUnityストレージがPowerPathで構成されており、PowerPathのバージョンがEMC Power.LINUX.6.3.0.b049の場合は、SSHを使用してホストに接続し、次のコマンドを実行して新しいバージョンのPowerPath(DellEMC Power.LINUX.6.4.0.b095)をインストールします。
- ```
systemctl stop nwdecoder
umount -R /var/netwitness/decoder
yum update DellEMC Power.LINUX-6.4.0.00.00-095.RHEL7.x86_64.rpm
```
9. ツールバーの[ホストの再起動]をクリックします。  
NetWitness Platformは、ホストがオンラインに戻るまで、[ステータス]に[再起動中]と表示します。ホストがオンラインに戻ると、[ステータス]には[最新]と表示されます。ホストがオンラインに戻らない場合は、カスタマーサポートにお問い合わせください。

注: 1.) DISA STIGが有効化されている場合には、コア サービスが起動するまでに5～10分程度かかります。この遅延は新しい証明書を生成するために生じます。2.) Unityストレージを使用している場合は、PowerPathのステータスを確認し、UnityデバイスがPowerPathによって認識可能であることを確認します。



## コマンド ラインから更新を適用する(Webアクセスなし)

RSA NetWitness Platform導入環境でWebアクセスが不可能な場合は、次の手順に従ってバージョン更新を適用します。

1. 目的のバージョンの.zip更新パッケージ(たとえば、netwitness-11.2.0.0.zip)をRSA Linkからローカル ディレクトリにダウンロードします。
2. SSHでNW Serverホストに接続します。
3. 目的のバージョン用に/tmp/upgrade/<version>ステージング ディレクトリを作成します(たとえば、/tmp/upgrade/11.2.0.0)。  

```
mkdir -p /tmp/upgrade/11.2.0.0
```
4. .zip更新パッケージを、ステージング ディレクトリ以外のNW Server上のディレクトリ( /tmp など)にコピーします。
5. 作成したステージング ディレクトリ(たとえば、/tmp/upgrade/11.2.0.0)にパッケージを解凍します。  

```
unzip /<download-location>/netwitness-11.2.0.0.zip -d /tmp/upgrade/11.2.0.0
```
6. NW Serverで更新を初期化します。  

```
upgrade-cli-client --init --version 11.2.0.0 --stage-dir /tmp/upgrade/
```
7. NW Serverに更新を適用します。  

```
upgrade-cli-client --upgrade --host-addr <NW Server IP> --version 11.2.0.0
```
8. NetWitness Platformにログインし、[ホスト]ビューでNW Serverホストを再起動します。
9. 非NW Serverの各ホストに更新を適用します。  

```
upgrade-cli-client --upgrade --host-addr <non-NW Server IP address> --version 11.2.0.0
```

更新は、ポーリングが完了した時点で完了します。
10. (オプション: Unityストレージを使用するホストの場合のみ) 11.1.x.xのホスト(たとえばNetwork Decoderホスト)にUnityストレージがPowerPathで構成されており、PowerPathのバージョンがEMC Power.LINUX.6.3.0.b049の場合は、SSHを使用してホストに接続し、次のコマンドを実行して新しいバージョンのPowerPath( DellEMC Power.LINUX.6.4.0.b095)をインストールします。  

```
systemctl stop nwdecoder
umount -R /var/netwitness/decoder
yum update DellEMC Power.LINUX-6.4.0.00.00-095.RHEL7.x86_64.rpm
```
11. NetWitness Platformにログインし、[ホスト]ビューでホストを再起動します。  
次のコマンドを使用して、ホストに適用されたバージョンを確認できます。  

```
upgrade-cli-client --list
```

**注:** 1.) DISA STIGが有効化されている場合には、コア サービスが起動するまでに5~10分程度かかります。この遅延は新しい証明書を生成するために生じます。2.) Unityストレージを使用している場合は、PowerPathのステータスを確認し、UnityデバイスがPowerPathによって認識可能であることを確認します。

---

## Legacy Windows収集の更新またはインストール

---

「RSA NetWitness Legacy Windows収集ガイド」を参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

**注:** Legacy Windows収集のインストールまたは更新の後、正常にログを収集するため、システムを再起動します。

## 更新後のタスク

---

NetWitness Platform 11.2.0.0への更新後に、次のタスクを実行します。

- [全般](#)
- [NW Server](#)
- [Endpoint Insights](#)
- [Event Stream Analysis](#)
- [Respond](#)
- [NetWitness UEBA](#)



## 全般

これらのタスクは、NetWitness Platform 11.2.0.0のすべてのお客様が実行する必要があります。



### タスク1: データ収集と集計の開始

11.2.0.0に更新した後、ネットワークおよびログの収集と集計を再開します。



#### ネットワーク収集の開始

1. NetWitness Platform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サービスを選択します。
3.  (アクション) で、[表示] > [システム]を選択します。
4. ツールバーで  Start Capture をクリックします。

#### ログ収集の開始


1. NetWitness Platform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. Log Decoderサービスを選択します。
3.  (アクション) で、[表示] > [システム]を選択します。
4. ツールバーで  Start Capture をクリックします。

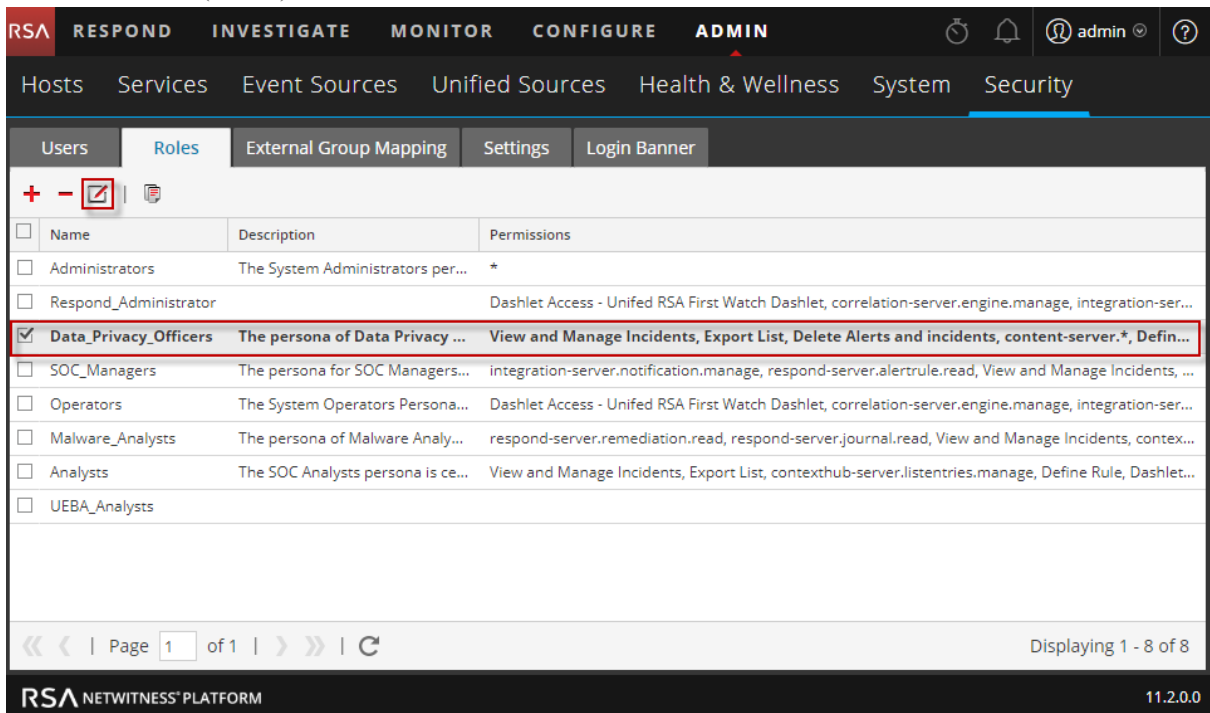
#### 集計の開始

1. NetWitness Platform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. それぞれのConcentratorおよびBrokerサービスについて:
  - a. サービスを選択します。
  - b.  (アクション) で、[表示] > [構成]を選択します。
  - c. ツールバーで  Start Aggregation をクリックします。

## タスク2: コンテキスト メニュー アクションのユーザ権限の設定

Analysts、SOC Managers、Data Privacy Officersの各ロールにコンテキスト メニュー アクションの権限を設定するには、次の手順を実行します。以下の手順は、Analysts、SOC Managers、Data Privacy Officersの各ロールに対して実行する必要があります。

1. NetWitness Platformメニューで、[管理] > [セキュリティ] > [ロール]を選択します。
2. ユーザロール(たとえば[Data Privacy Officers])をダブルクリックするか、ユーザロールをクリックして選択してから  (編集) をクリックします。



| <input type="checkbox"/>            | Name                  | Description                       | Permissions                                                                                           |
|-------------------------------------|-----------------------|-----------------------------------|-------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/>            | Administrators        | The System Administrators per...  | *                                                                                                     |
| <input type="checkbox"/>            | Respond_Administrator |                                   | Dashlet Access - Unifed RSA First Watch Dashlet, correlation-server.engine.manage, integration-ser... |
| <input checked="" type="checkbox"/> | Data_Privacy_Officers | The persona of Data Privacy ...   | View and Manage Incidents, Export List, Delete Alerts and incidents, content-server.*, Defin...       |
| <input type="checkbox"/>            | SOC_Managers          | The persona for SOC Managers...   | integration-server.notification.manage, respond-server.alertrule.read, View and Manage Incidents, ... |
| <input type="checkbox"/>            | Operators             | The System Operators Persona...   | Dashlet Access - Unifed RSA First Watch Dashlet, correlation-server.engine.manage, integration-ser... |
| <input type="checkbox"/>            | Malware_Analysts      | The persona of Malware Analy...   | respond-server.remediation.read, respond-server.journal.read, View and Manage Incidents, contex...    |
| <input type="checkbox"/>            | Analysts              | The SOC Analysts persona is ce... | View and Manage Incidents, Export List, contexthub-server.listentries.manage, Define Rule, Dashlet... |
| <input type="checkbox"/>            | UEBA_Analysts         |                                   |                                                                                                       |

Page 1 of 1 | Displaying 1 - 8 of 8

RSA NETWITNESS® PLATFORM 11.2.0.0

3. [ロールの編集]ビューの[権限]セクションで、[Manage Logs]、[Manage Plugins]、[Manage System Settings]の各チェックボックスをオンにして、[保存]をクリックします。

The screenshot shows the 'Edit Role' window with the 'Permissions' section expanded. The 'Administration' tab is selected. The following table represents the permissions listed:

| Assigned                            | Description ^          |
|-------------------------------------|------------------------|
| <input checked="" type="checkbox"/> | Manage Logs            |
| <input type="checkbox"/>            | Manage Notifications   |
| <input checked="" type="checkbox"/> | Manage Plugins         |
| <input type="checkbox"/>            | Manage Predicates      |
| <input type="checkbox"/>            | Manage Reconstruction  |
| <input checked="" type="checkbox"/> | Manage Security        |
| <input checked="" type="checkbox"/> | Manage Services        |
| <input checked="" type="checkbox"/> | Manage System Settings |
| <input type="checkbox"/>            | Modify ESA Settings    |
| <input type="checkbox"/>            | Modify Event Sources   |
| <input type="checkbox"/>            | Modify Hosts           |

4. Data Privacy Officersと同様に、AnalystsとSOC Managersの各ロールに対してステップ1～3を実行します。


## NW Server

### (オプション) タスク3: Logstash出力構成ファイルで更新されていない監査ログテンプレートの修正

**問題:** 11.0.0.0から11.2.0.0への更新時、グローバル監査が構成されている場合、Logstash出力構成ファイルで監査ログテンプレートが更新されません。

**回避策:** グローバル監査が構成されている場合、グローバル通知サーバのいずれかのsyslogエントリを編集し、[保存]をクリックして最新の監査ログの構成を適用する必要があります。

11.0.xでグローバル監査が構成されている場合、最新のグローバル監査の構成を適用するために、次の手順を実行する必要があります。

1. NetWitness Platformメニューで、[管理] > [システム] > [グローバル通知]の順に選択します。  
[グローバル通知]ビューが表示されます。
2. [サーバ]タブをクリックして、任意のsyslogサーバを選択します。
3.  (編集アイコン) をクリックして、[保存]をクリックします。

### (オプション) タスク4: PAM Radius認証の再構成

11.0.x.xでpam\_radiusパッケージを使用してPAM Radius認証を構成した場合、パフォーマンスを向上させるために、11.2.0.0ではpam\_radius\_auth package を使用して再構成する必要があります。手順については、『RSA NetWitness® Platform 11.2システム セキュリティとユーザ管理ガイド』の「PAMログイン機能の構成」を参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

## Endpoint Insights

### タスク5: Javaバージョンの変更により、レガシーEndpointからの定期実行Feedを再構成

Javaバージョンの変更により、レガシーEndpointの定期実行Feedを再構成する必要があります。この問題を解決するには、次の手順を実行します。

1. 『*RSA NetWitness Endpoint統合ガイド*』にある「繰り返しFeedを通じたEndpointからのコンテキストデータの構成」トピックの「NetWitness EndpointのSSL証明書のエクスポート」の説明に従い、NetWitness Endpoint CA証明書をNetWitness Platformのトラストストアにインポートします。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

### タスク6: バックアップしたEndpointカスタムメタデータマッピングのリストア

必要な場合を除き、11.2のデフォルトマッピングを上書きしないでください。11.2に更新する前に、11.1.x.xのカスタムマッピングをバックアップした場合は、カスタムマッピングのリストを確認し、まだデフォルトに含まれていないマッピングだけを、nw-shell経由でset-custom APIを使用してリストアします。

マッピングを変更するには、『*Endpoint Insights構成ガイド*』を参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。



## Event Stream Analysis

これらのタスクは、NetWitness Platform 11.2.0.0のEvent Stream Analysisを使用する場合に実行してください。

### (オプション) タスク7: 自動脅威検出の「Suspected Command and Control Communication By Domain」統合ルールを再構成

11.0では、「Suspected Command & Control Communication By Domain」統合ルールのGroup By条件「Domain by Suspected C&C」が期待どおりに機能していなかったため、「Suspected C&C」のインシデントを作成するためにはGroupBy条件を「Domain」に変更する必要がありました。「Domain by Suspected C&C」条件は11.2.0.0では正常に機能し、「Suspected Command & Control Communication By Domain」統合ルール(11.2.0.0ではインシデントルールに名称変更)のGroup By条件として使用できません。

11.0で「Suspected Command & Control Communication By Domain」統合ルールのGroup By条件を「Domain」に変更した場合、11.2.0.0では「Domain by Suspected C&C」に戻す必要があります。

1. NetWitness Platformメニューで、[構成] > [インシデントルール]を選択します。
2. インシデントルールの一覧で、「Suspected Command & Control Communication by Domain」ルールを見つけ、[名前]フィールドのリンクをクリックして開きます。
3. [インシデントルールの詳細]ビューの[グループ化オプション]セクションで、[Group By]フィールドを[Domain]から[Suspected C&C]に変更し、[保存]をクリックします。

詳細については、『NetWitness Platform自動脅威検出ガイド』および

『NetWitness Platform ESA構成ガイド』の「ESA Analyticsの構成」セクションを参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

## Respond

### タスク8: 統合ルールスキーマの最新バージョンを取得してRespondサービスのカスタム キーをリストアする

次の手順を実行して、統合ルールスキーマの最新バージョンを取得してRespondサービスのカスタム キーをリストアします。

1. `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` ファイルを削除します。
2. Respond Serverを再起動して、`/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` ファイルの最新バージョンを取得します。  
`systemctl restart rsa-nw-respond-server`
3. 11.0で、groupBy句で使用するため`/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` ファイルにカスタム キーを追加した場合、`/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` ファイルを変更して、更新準備タスクで保存しておいたカスタム キーを追加します。

**注:** 11.2.0.0では、Respondに新しい[Group By]フィールドが追加されました。サーバから新しいバージョンのファイルを取得しないと、新しい[Group By]フィールドはNetWitness Platformユーザインタフェースに表示されません。

## タスク9: Respondサービスの正規化スクリプトの最新バージョンの取得、カスタム正規化スクリプトのリストア

11.2.0.0では、Respondサービス正規化スクリプトが再設計され、`/var/lib/netwitness/respond-server/scripts`ディレクトリに格納されます。以前のバージョンを置換する必要があります。

11.2.0.0への更新前に、次のファイルを`/var/lib/netwitness/respond-server/scripts`ディレクトリからバックアップしました。

```
data_privacy_map.js
normalize_alerts.js
normalize_core_alerts.js
normalize_ecat_alerts.js
normalize_ma_alerts.js
normalize_wtd_alerts.js
utils.js
```

正規化スクリプトの最新バージョンを取得するには、次の手順を実行します。

1. 前述のファイルをバックアップした後、`/var/lib/netwitness/respond-server/scripts`ディレクトリとそのコンテンツを削除します。
2. Respond Serverを再起動します。

```
systemctl restart rsa-nw-respond-server
```
3. (オプション) バックアップされた11.0スクリプトのカスタム ロジックが含まれるよう、新しいファイルを編集します。

**注:** 11.2.0.0のリリースで、次のファイルが変更されました。

```
normalize_alerts.js
aggregation_rule_schema.json
```

## タスク10: 対応の通知設定の権限の追加

**注:** この権限を11.1ですでに構成してある場合は、このタスクをスキップしてかまいません。

対応の通知設定の権限により、Respond Administrators、Data Privacy Officers、SOC Managersは対応の通知の設定([構成]>[対応の通知])にアクセスし、インシデントが作成または更新されたときにメール通知を送信することが可能になります。

これらの設定にアクセスするには、既存のNetWitness Platformの標準のユーザーロールに権限を追加する必要があります。カスタム ロールにも権限を追加する必要があります。『*NetWitness Respond構成ガイド*』の「対応の通知設定の権限」トピックを参照してください。ユーザ権限の詳細については、「システムセキュリティとユーザ管理ガイド」を参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

## タスク11: デフォルトのインシデント ルールのGroup By値の更新

デフォルトのインシデント ルールのうち次の4つは、Group By値として「Source IP Address」を使用するようになりました。

- High Risk Alerts: Reporting Engine
- High Risk Alerts: Malware Analysis
- High Risk Alerts: NetWitness Endpoint
- High Risk Alerts: ESA

デフォルトのルールを更新するには、前述のデフォルトのルールのGroup By値を「Source IP Address」に変更します。

**注:** 前述したデフォルトのルールのGroup By値を11.1ですでに更新している場合は、再度更新する必要はありません。

1. **NetWitness Platform**メニューで、**[構成]** > **[インシデント ルール]**を選択して、更新するルールの**[名前]**列をクリックします。**[インシデント ルールの詳細]**ビューが表示されます。
2. **[GROUP BY]**フィールドで、ドロップダウン リストから新しいGroup By値を選択します。
3. **[保存]**をクリックしてルールを更新します。

NetWitness Endpointのアラートを検知器のIPアドレスに基づいて統合するには、次の手順を実行して、デフォルトのNetWitness Endpointインシデント ルールを複製し、Group ByのIPアドレスを変更します。

1. **NetWitness Platform**メニューで、**[構成]** > **[インシデント ルール]**を選択します。**[インシデント ルールのリスト]**ビューが表示されます。
2. **[High Risk Alerts: NetWitness Endpoint]** デフォルト インシデント ルールを選択して、**[複製]**をクリックします。選択したルールの複製が正常に作成されたというメッセージが表示されます。
3. ルール名を適切な名前に変更します(たとえば「High Risk Alerts: NetWitness Endpoint Detector IP」)。
4. **[GROUP BY]**フィールドで、**[Source IP Address]**を削除して、**[Detector IP Address]**を追加します。**[Detector IP Address]**が**[Group By]**に表示される唯一の値であることが重要です。
5. **[保存]**をクリックしてルールを作成します。

詳細については、『*NetWitness Platform Respond構成ガイド*』を参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

## NetWitness UEBA

### タスク12: NetWitness UEBAのインストール

NetWitness UEBAはNetWitness® Platform 11.2から新しく導入された機能です。

以下を参照してください。

『*RSA NetWitness Platform 11.2物理ホスト インストールガイド*』(物理ホストのインストールの手順)。

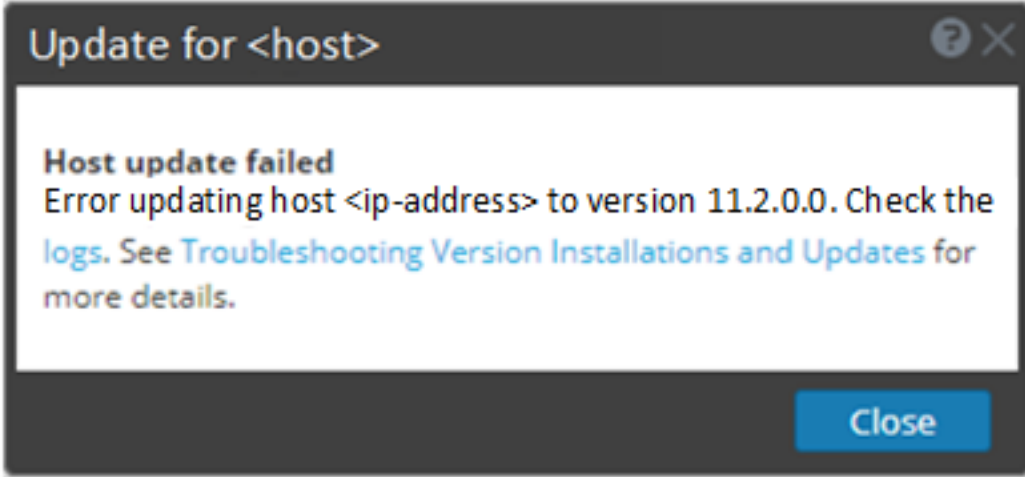
『*RSA NetWitness Platform 11.2仮想ホスト インストールガイド*』(仮想ホストのインストールの手順)。

『*RSA NetWitness UEBAユーザガイド*』(UEBAに関する情報)。

NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

## 付録A: インストールと更新のトラブルシューティング

このセクションでは、[ホスト]ビューでのホスト バージョンの更新およびホストへのサービスのインストールで問題が発生した場合に、[ホスト]ビューに表示されるエラーメッセージについて説明します。次のトラブルシューティングの解決策で解決できない更新またはインストールの問題がある場合は、カスタマー サポートにお問い合わせください。

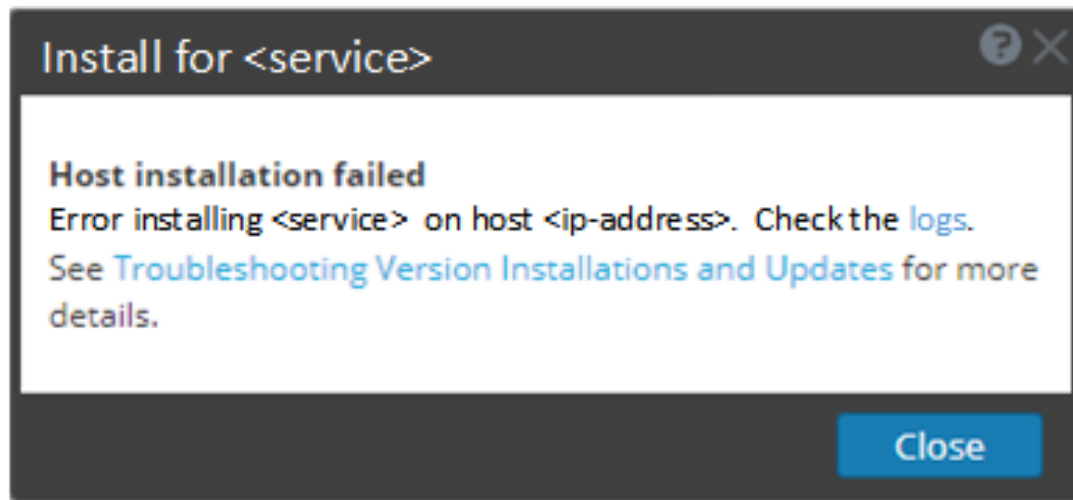
|              |                                                                                                         |
|--------------|---------------------------------------------------------------------------------------------------------|
| エラー<br>メッセージ | <p>ホストの更新に失敗しました</p>  |
|              | 問題                                                                                                      |
| 解決策          |                                                                                                         |

2. `deploy_admin`を選択し、[パスワードのリセット]をクリックします。
3. (オプション) [パスワードのリセット]ダイアログで有効期限が切れた`deploy_admin`のパスワードの再使用が拒否される場合は、次の手順を実行します。
  - a. `deploy_admin`のパスワードを新しいパスワードにリセットします。
  - b. 11.xのすべての非NW Serverホストで、次のコマンドを実行し、NW Serverと同じ`deploy_admin`のパスワードを指定します。

```
/opt/rsa/saTools/bin/set-deploy-admin-password
```
- 原因2:`deploy_admin`のパスワードがNW Serverホストで変更されたが、非NW Serverホストでは変更されていない。  
原因2を解決するには、次の手順を実行します。
  - 11.xのすべての非NW Serverホストで、次のコマンドを実行し、NW Serverと同じ`deploy_admin`のパスワードを指定します。

```
/opt/rsa/saTools/bin/set-deploy-admin-password
```
3. それでも更新を適用できない場合は、ステップ2のログを収集して、カスタマーサポートにお問い合わせください。

## ホストのインストールに失敗しました

エラー  
メッセー  
ジ

問題

ホストを選択して[インストール]をクリックすると、サービスのインストールプロセスが失敗します。

解決策

1. サービスのインストールを再度試行します。  
多くの場合、これで問題は解決します。
2. それでもサービスをインストールできない場合は、次の手順を実行します。
  - a. 実行時にNW Server上の次のログを監視します(たとえば、コマンドラインからtail -fコマンドを実行します)。
 

```

/var/netwitness/uax/logs/sa.log
/var/log/netwitness/orchestration-server/orchestration-server.log
/var/log/netwitness/deployment-upgrade/chef-solo.log
/var/log/netwitness/config-management/chef-solo.log
/var/lib/netwitness/config-management/cache/chef-stacktrace.out

```

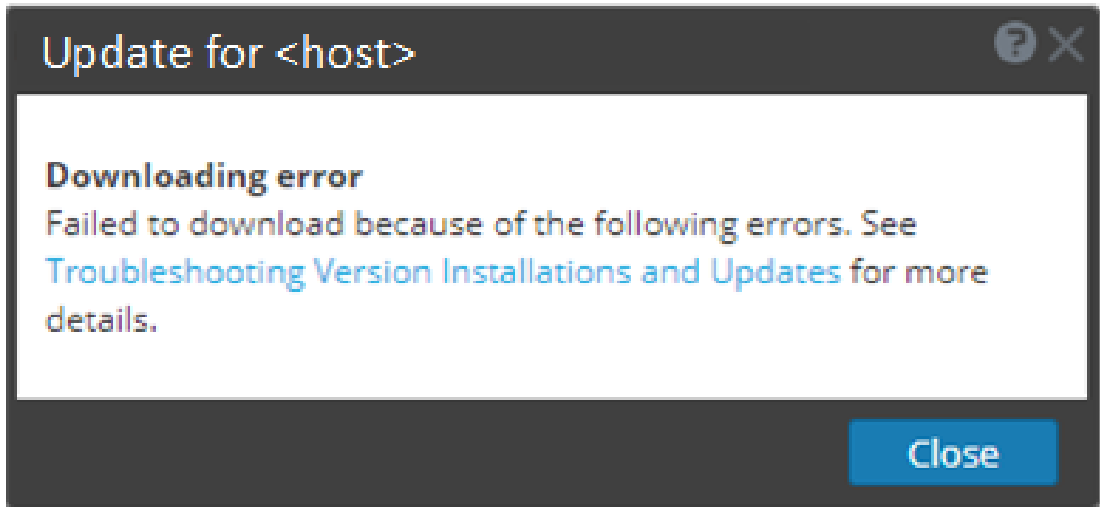
 これらのログの1つ以上にエラーが表示されます。
  - b. 問題を解決し、サービスを再インストールします。
    - 原因1: nwsetup-tuiで間違ったdeploy\_adminのパスワードを指定した。  
解決策: deploy\_admin のパスワードを復旧します。  
原因1を解決するには、次の手順を実行します。
      1. NetWitness Suiteメニューで、[管理] > [セキュリティ] > [ユーザ]タブの順に選択します。
      2. deploy\_adminを選択し、[パスワードのリセット]をクリックします。
      3. (オプション) [パスワードのリセット]ダイアログで有効期限が切れたdeploy\_adminのパスワードの再使用が拒否される場合は、次の手順を実行します。
        - a. SSHでNW Serverホストに接続し、次のコマンドを実行します。



```
security-cli-client --get-config-prop --prop-hierarchy
nw.security-client --prop-name
platform.deployment.password -quiet
```


- b. インストール/オーケストレーションに失敗したホストにSSHで接続します。
  - c. 正しいdeploy\_adminのパスワードを使用してnwsetup-tuiを再実行します。
- 原因2: deploy\_adminのパスワードの有効期限が切れている。  
原因2を解決するには、次の手順を実行します。
    1. NetWitness Suiteメニューで、[管理] > [セキュリティ] > [ユーザ] タブの順に選択します。
    2. deploy\_adminを選択し、[パスワードのリセット]をクリックします。
    3. (オプション) [パスワードのリセット]ダイアログで有効期限が切れたdeploy\_adminのパスワードを再使用できる場合は、次の手順を実行します。
      - a. 期限が切れたdeploy\_adminのパスワードを入力します。
      - b. [次回ログイン時にパスワードの変更を強制]チェックボックスをクリアします。
      - c. [保存]をクリックします。
    4. (オプション) [パスワードのリセット]ダイアログで有効期限が切れたdeploy\_adminのパスワードの再使用を拒否される場合は、次の手順を実行します。
      - a. deploy\_adminのパスワードを新しいパスワードにリセットします。
      - b. 11.xのNW Serverホストとそれ以外のすべてのホストで、次のコマンドを実行し、新しいdeploy\_adminのパスワードを指定します。

```
/opt/rsa/saTools/bin/set-deploy-admin-password
```
      - c. インストール/オーケストレーションに失敗したホストで、nwsetup-tuiを実行し、新しいdeploy\_adminのパスワードを指定します。
3. それでも更新を適用できない場合は、ステップ2のログを収集して、カスタマー サポートにお問い合わせください。

| ダウンロード エラー       |                                                                                                                                                                                                                                                        |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| エラー<br>メッセ<br>ージ |                                                                                                                                                                      |
| 問題               | 更新バージョンを選択し、[更新]>[ホストの更新]をクリックすると、ダウンロードが開始されますが異常終了します。                                                                                                                                                                                               |
| 原因               | バージョンのダウンロード ファイルのサイズが大きく、ダウンロードに時間がかかる場合があります。ダウンロード中に通信の問題が発生すると、ダウンロードは失敗します。                                                                                                                                                                       |
| 解決<br>策          | <ol style="list-style-type: none"><li>1. 再度ダウンロードしてください。</li><li>2. それでもダウンロードが失敗する場合は、「<a href="#">コマンド ラインから更新を適用する(Webアクセスなし)</a>」の説明に従って、NetWitness Suite以外からのダウンロードを試みてください。</li><li>3. それでも更新ファイルをダウンロードできない場合は、カスタマー サポートにお問い合わせください。</li></ol> |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| エラーメッセージ | <p>deploy_adminユーザのパスワードの有効期限が切れています</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 原因       | <p>deploy_adminのパスワードの有効期限が切れています。</p> <p>deploy_adminのパスワードをリセットします。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 解決策      | <ol style="list-style-type: none"><li>1. NetWitness Suiteメニューで、[管理] &gt; [セキュリティ] &gt; [ユーザ] タブの順に選択します。</li><li>2. <b>deploy_admin</b>を選択し、[パスワードのリセット]をクリックします。<ul style="list-style-type: none"><li>• [パスワードのリセット]ダイアログで有効期限が切れた<b>deploy_admin</b>のパスワードを再使用できる場合は、次の手順を実行します。<ol style="list-style-type: none"><li>a. 期限が切れた<b>deploy_admin</b>のパスワードを入力します。</li><li>b. [次回ログイン時にパスワードの変更を強制]チェックボックスをオフにします。</li><li>c. [保存]をクリックします</li></ol></li><li>• [パスワードのリセット]ダイアログで有効期限が切れた<b>deploy_admin</b>のパスワードを再使用できない場合は、次の手順を実行します。<ol style="list-style-type: none"><li>a. 11.xのNW Serverホストとそれ以外のすべてのホストで、次のコマンドを実行し、新しい<b>deploy_admin</b>のパスワードを指定します。<br/><code>/opt/rsa/saTools/bin/set-deploy-admin-password</code></li><li>b. インストール/オーケストレーションに失敗したホストで、<code>nwsetup-tui</code>を実行し、新しい<b>deploy_admin</b>のパスワードを指定します。</li></ol></li></ul></li></ol> |

|           |                                                                                                                                                                                                                                                            |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| エラー メッセージ | <pre>/var/log/netwitness/orchestration- server/orchestration-server.logに、次のようなエ ラーが記録されました。 API Failure /rsa/orchestration/task/update- config-management [counter=10 reason=IllegalArgumentException Exception::Version '11.0.0.n' is not supported</pre> |
| 問題        | <p>NW Serverホストを11.1に更新した後、非NW Serverホストの唯一の更新パスは11.1になります。非NW Serverホストに11.0.0.nのパッチを適用しようとする(たとえば、11.0.0.0から11.0.0.3)、このエラーが表示されます。</p>                                                                                                                  |
| 解決策       | <p>2つの選択肢があります。</p> <ul style="list-style-type: none"> <li>• 非NW Serverホストを11.1に更新します。</li> <li>• 非NW Serverホストを更新しません(現在のバージョンを維持)。</li> </ul>                                                                                                            |

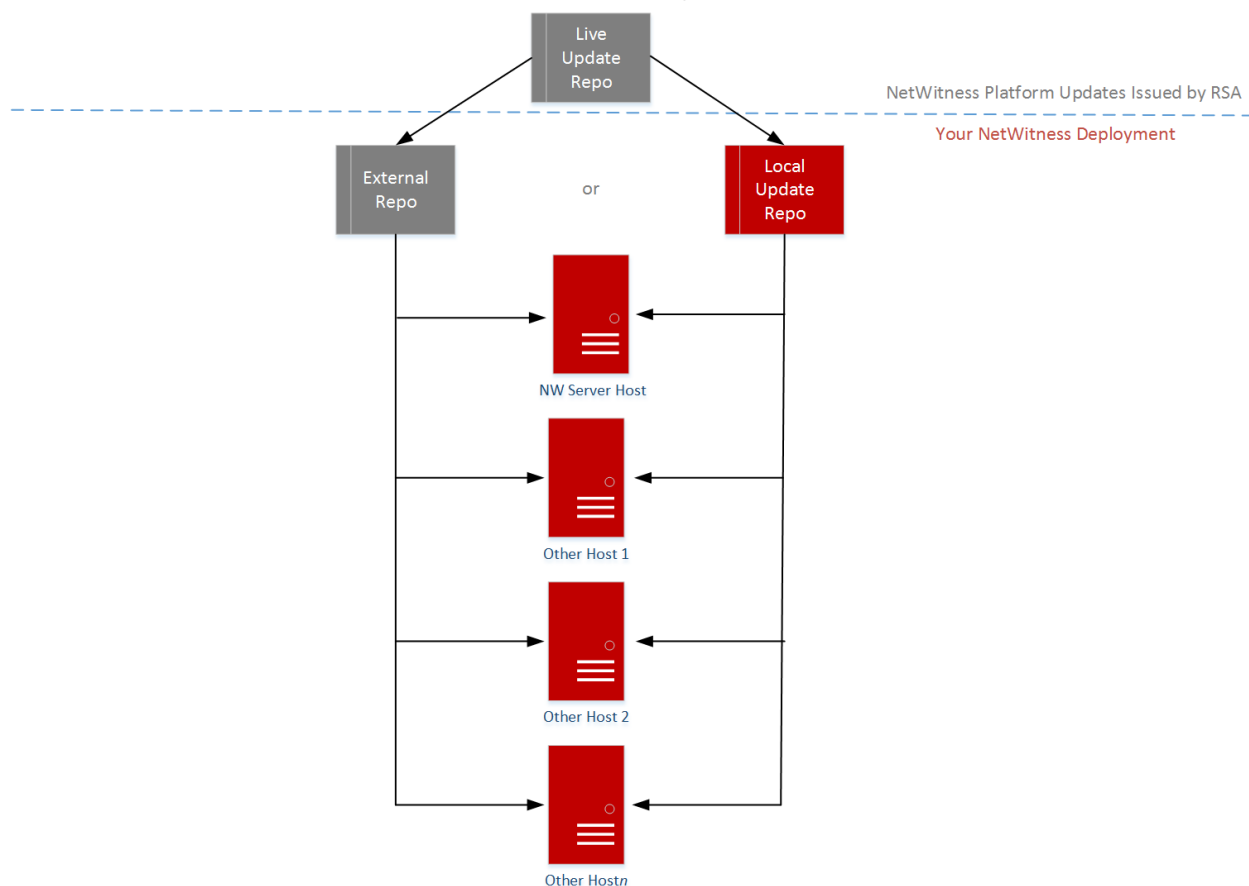
|           |                                                                                                                                                          |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| エラー メッセージ | <p>ホストをオフラインで更新してリブートした後に、ユーザ インタフェースにホストをリブートするようメッセージが表示されます。</p>  |
| 原因        | <p>CLIを使用してホストをリブートすることはできません。ユーザ インタフェースを使用する必要があります。</p>                                                                                               |
| 解決策       | <p>ユーザ インタフェースの[ホスト]ビューでホストを再起動します。</p>                                                                                                                  |

## 付録B: ローカルリポジトリへの更新の配置

NetWitness Platformは、バージョンの更新をLive更新リポジトリからローカル更新リポジトリに送信します。Live更新リポジトリへのアクセスには、[管理]>[システム]>[Live]で構成したLiveアカウントの認証情報を使用する必要があります。さらに、最新の更新を毎日取得して、ローカルリポジトリに配置するために、[管理]>[システム]>[更新]の[Automatically download information about new updates every day]チェックボックスをオンにする必要があります。

次の図は、Webアクセスが可能なNetWitness Platform導入環境で、バージョンの更新を取得する方法を示しています。

RSA NetWitness Platform® 11.x.x.x Version Update Workflow – Web Access



**注:** Live更新リポジトリに最初に接続する場合、CentOS 7のシステムパッケージとRSA製品パッケージすべてにアクセスすることになります。この同期では、2.5GBを超えるデータがダウンロードされます。同期に要する時間は、使用するNW Serverのインターネット接続環境やRSA Live更新リポジトリのトラフィックによって異なります。Live更新リポジトリの使用は必須ではありません。また、「[RSAおよびOS更新の外部リポジトリのセットアップ](#)」の説明に従って、外部リポジトリを使用することもできます。

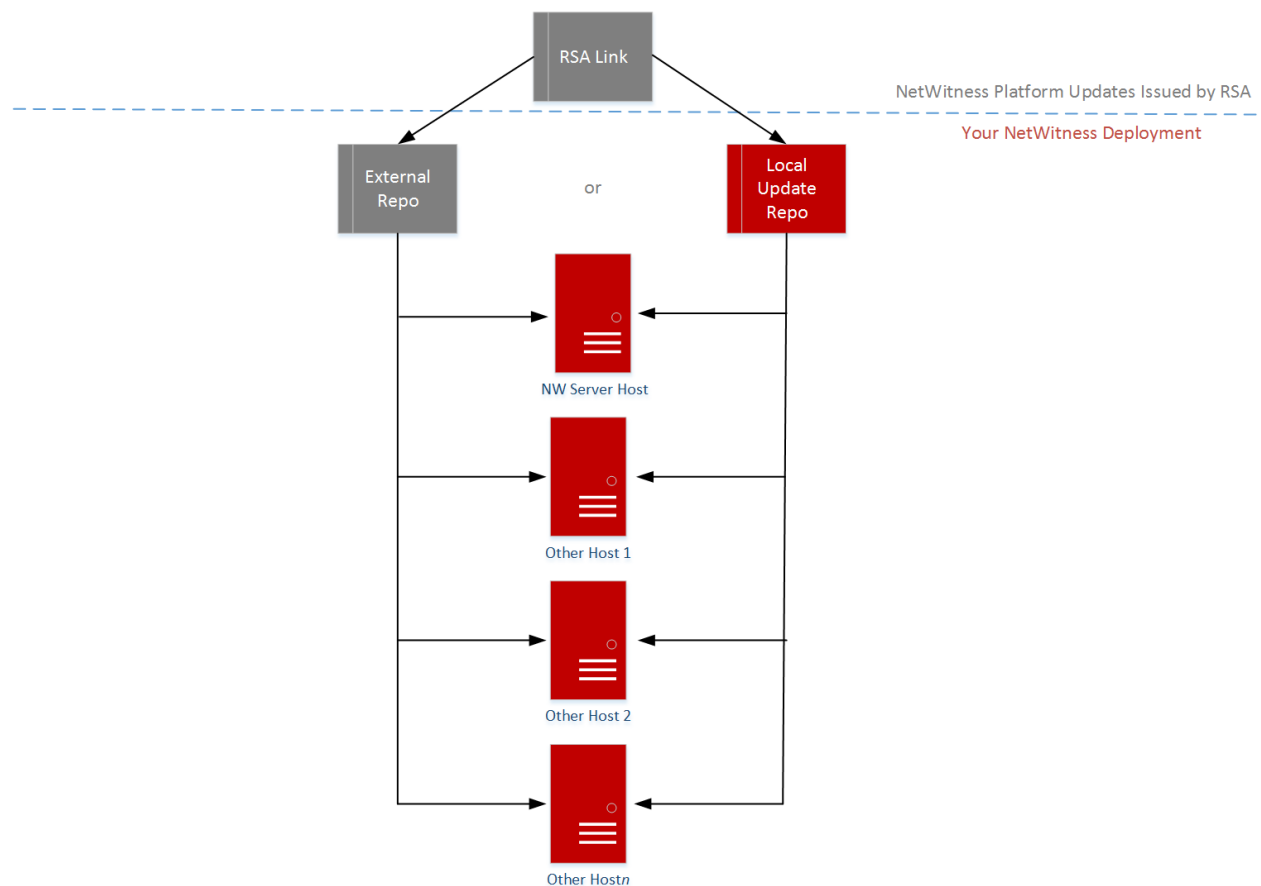
Live更新リポジトリに接続するには、[管理]>[システム]ビューに移動し、オプションパネルで[Liveサービス]を選択して、認証情報が構成されていることを確認します([接続済み]ボタンが緑色)。緑色でない場合は、[サインイン]をクリックして、接続します。

注: Live更新リポジトリへの接続にプロキシを使用する必要がある場合、プロキシホスト、プロキシユーザ名、プロキシパスワードを構成できます。詳細については、『*NetWitness Platform 11.2 システム構成ガイド*』の「NetWitness Platformのプロキシの構成」を参照してください。

WebアクセスができないNetWitness Platform導入環境の場合は、「[コマンドラインから更新を適用する \(Webアクセスなし\)](#)」を参照してください。

次の図は、WebアクセスがないNetWitness Platform導入環境で、バージョンの更新を取得する方法を示しています。

RSA NetWitness Platform® 11.x.x.x Version Update Workflow – No Web Access



## 付録C: 外部リポジトリのセットアップ

外部リポジトリ (Repo) をセットアップするには、次の手順を実行します。

注: 1.) この手順を完了するには、ホストに解凍ユーティリティがインストールされている必要があります。2.) 次の手順を実行する前に、Webサーバの作成方法を理解する必要があります。

1. (オプション) 外部リポジトリがあり、それを上書きする場合に、この手順を実行します。
  - ケース1: 外部リポジトリからホストをセットアップしたが、Admin Server上のローカルリポジトリを使用してアップグレードしたい場合。
    - a. `/etc/netwitness/platform/repo`ファイルを作成します。  
`vi /etc/netwitness/platform/netwitness/repo`
    - b. `repo`ファイルを編集して、ファイル内の情報が次のURLだけになるようにします。  
`https://nw-node-zero/nwrpmrepo`
    - c. `upgrade-cli-client` ツールを使用したアップグレードの手順を完了します。
  - ケース2: Admin Server(NW Serverホスト)のローカルリポジトリからホストをセットアップしたが、外部リポジトリを使用してアップグレードしたい場合。
    - a. `/etc/netwitness/platform/repo`ファイルを作成します。  
`vi /etc/netwitness/platform/netwitness/repo`
    - b. `repo`ファイルを編集して、ファイル内の情報が次のURLだけになるようにします。  
`https://<webserver-ip>/<alias-for-repo>`
    - c. `upgrade-cli-client` ツールを使用したアップグレードの手順を完了します。  
「[コマンドラインから更新を適用する\(Webアクセスなし\)](#)」の手順を参照します。
2. 外部リポジトリをセットアップします。
  - a. Webサーバホストにログインします
  - b. NWリポジトリ(`netwitness-11.2.0.0.zip`)をホストするディレクトリを作成します(例: Webサーバの`web-root`の下に`ziprepo`)。たとえば、`/var/netwitness`が`web-root`の場合、次のコマンドを実行します。  
`mkdir -p /var/netwitness/<your-zip-file-repo>`
  - c. `11.2.0.0`ディレクトリを`/var/netwitness/<your-zip-file-repo>`の下に作成します。  
`mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0`
  - d. OSおよびRSAディレクトリを`/var/netwitness/<your-zip-file-repo>/11.2.0.0`の下に作成します。  
`mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS`  
`mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA`
  - e. `netwitness-11.2.0.0.zip`ファイルを`/var/netwitness/<your-zip-file-repo>/11.2.0.0`ディレクトリに解凍します。  
`unzip netwitness-11.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0`

netwitness-11.2.0.0.zipを解凍すると、2つのzipファイル(OS-11.2.0.0.zipおよびRSA-11.2.0.0.zip)とその他のファイルがいくつか現れます。

f. 以下のように解凍します。

i. OS-11.2.0.0.zipを /var/netwitness/<your-zip-file-repo>/11.2.0.0/OSディレクトリに解凍します。

```
unzip /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS-11.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS
```

次の例は、ファイル解凍後のOS(オペレーティングシステム)ファイルの構造を示しています。

| Parent Directory                                                        | -                      |
|-------------------------------------------------------------------------|------------------------|
| <a href="#">GeoIP-1.5.0-11.el7.x86_64.rpm</a>                           | 20-Nov-2016 12:49 1.1M |
| <a href="#">HostAgent-Linux-64-x86-en_US-1.2.25.1.0163-1.x86_64.rpm</a> | 03-Oct-2017 10:07 4.6M |
| <a href="#">Lib_Utils-1.00-09.noarch.rpm</a>                            | 03-Oct-2017 10:05 1.5M |
| <a href="#">OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm</a>                  | 20-Nov-2016 14:43 502K |
| <a href="#">OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm</a>              | 20-Nov-2016 14:43 15K  |
| <a href="#">PyYAML-3.11-1.el7.x86_64.rpm</a>                            | 19-Dec-2017 12:30 160K |
| <a href="#">SDL-1.2.15-14.el7.x86_64.rpm</a>                            | 25-Nov-2015 10:39 204K |
| <a href="#">acl-2.2.51-12.el7.x86_64.rpm</a>                            | 03-Oct-2017 10:04 81K  |
| <a href="#">adobe-source-sans-pro-fonts-2.020-1.el7.noarch.rpm</a>      | 13-Feb-2018 05:10 706K |
| <a href="#">alsa-lib-1.1.3-3.el7.x86_64.rpm</a>                         | 10-Aug-2017 10:52 421K |
| <a href="#">at-3.1.13-22.el7_4.2.x86_64.rpm</a>                         | 25-Jan-2018 17:56 51K  |
| <a href="#">atk-2.22.0-3.el7.x86_64.rpm</a>                             | 10-Aug-2017 10:53 258K |
| <a href="#">attr-2.4.46-12.el7.x86_64.rpm</a>                           | 03-Oct-2017 10:04 66K  |

ii. RSA-11.2.0.0.zipを/var/netwitness/<your-zip-file-repo>/11.2.0.0/RSAディレクトリに解凍します。

```
unzip /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA-11.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA
```



次の例は、ファイル解凍後のRSAバージョン更新ファイルの構造を示しています。

|                                                      |                        |
|------------------------------------------------------|------------------------|
| Parent Directory                                     | -                      |
| MegaCli-8.02.21-1.noarch.rpm                         | 03-Oct-2017 10:07 1.2M |
| OpenIPMI-2.0.19-15.el7.x86_64.rpm                    | 03-Oct-2017 10:07 173K |
| bind-utils-9.9.4-51.el7_4.2.x86_64.rpm               | 22-Jan-2018 09:03 203K |
| bzip2-1.0.6-13.el7.x86_64.rpm                        | 03-Oct-2017 10:07 52K  |
| cifs-utils-6.2-10.el7.x86_64.rpm                     | 10-Aug-2017 11:14 85K  |
| device-mapper-multipath-0.4.9-111.el7_4.2.x86_64.rpm | 25-Jan-2018 17:56 134K |
| dnsmasq-2.76-2.el7_4.2.x86_64.rpm                    | 02-Oct-2017 19:36 277K |
| elasticsearch-5.6.9.rpm                              | 17-Apr-2018 09:37 32M  |
| erlang-19.3-1.el7.centos.x86_64.rpm                  | 03-Oct-2017 10:07 17K  |
| finereader-4.6.0-2.el7.x86_64.rpm                    | 27-Feb-2018 09:11 1.3M |
| htop-2.1.0-1.el7.x86_64.rpm                          | 14-Feb-2018 19:23 102K |
| i40e-zc-2.3.6.12-1dkms.noarch.rpm                    | 04-May-2018 11:08 399K |
| ipmitool-1.8.18-5.el7.x86_64.rpm                     | 10-Aug-2017 12:41 441K |
| iptables-services-1.4.21-18.3.el7_4.x86_64.rpm       | 08-Mar-2018 09:20 51K  |
| ixgbe-zc-5.0.4.12-dkms.noarch.rpm                    | 04-May-2018 11:08 374K |

Repoの外部urlは<http://<web server IP address>/<your-zip-file-repo>>です。

- g. (オプション: Azureの場合): Azureの更新の場合は、次の手順を実行します。
- `mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS/other`
  - `unzip nw-azure-11.2-extras.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS/other`
  - `cd /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS`
  - `createrepo .`
  - NW 11.2.0.0セットアッププログラム(`nwsetup-tui`)が[Enter the base URL of the external update repositories]プロンプトを表示したら、`http://<web server IP address>/<your-zip-file-repo>`と入力します。

## 改訂履歴

| リビジョン | 日付         | 説明                                      | 作成者 |
|-------|------------|-----------------------------------------|-----|
| 1.0   | 2018年8月15日 | Release to Operations                   | IDD |
| 1.1   | 2018年9月4日  | RTO後の更新。                                | IDD |
| 1.2   | 2018年10月9日 | 「コマンドラインから更新を適用する(Webアクセスなし)」の手順の構文を修正。 |     |