



# 物理ホスト インストールガイド

バージョン 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](http://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

---

<b>概要</b>	<b>4</b>
サポート対象のハードウェア	4
Endpoint HybridまたはEndpoint Log Hybridホストのハードウェア仕様	4
RSA NetWitness UEBAホストのハードウェア仕様	4
外部接続ストレージ	5
物理ホストのインストールワークフロー	5
カスタマーサポートへのお問い合わせ	6
<b>インストールの準備：ファイアウォールポートを開く</b>	<b>7</b>
<b>インストールタスク</b>	<b>8</b>
タスク1: NetWitness Server(NW Server) ホストへの11.2のインストール	8
タスク2: その他のコンポーネントのホストへの11.2のインストール	21
<b>Legacy Windows収集の更新またはインストール</b>	<b>33</b>
<b>インストール後のタスク</b>	<b>34</b>
全般	34
(オプション)タスク1: 11.2インストール後のDNSサーバの再構成	34
RSA NetWitness Endpoint Insights	35
(オプション)タスク2: Endpoint HybridまたはEndpoint Log Hybridのインストール	35
FIPSの有効化	36
(オプション)タスク3 - FIPSモードの有効化	36
RSA NetWitness® UEBA	37
(オプション)タスク4: NetWitness UEBAのインストール	37
<b>付録A: トラブルシューティング</b>	<b>42</b>
CLI(コマンドラインインタフェース)	43
バックアップ(nw-backupスクリプト)	44
Event Stream Analysis	46
Log Collectorサービス(nwlogcollector)	47
NW Server	49
Orchestration	49
Reporting Engineサービス	50
NetWitness UEBA	51
<b>付録B: 外部リポジトリの作成</b>	<b>52</b>
<b>改訂履歴</b>	<b>54</b>

## 概要

このガイドの手順は、物理ホストにのみ適用されます。11.2の仮想ホストをセットアップする方法については、『RSA NetWitness Platform 仮想ホスト インストールガイド』を参照してください。

### サポート対象のハードウェア

シリーズ4、シリーズ4S、シリーズ5。

各シリーズタイプの詳細については、『RSA NetWitness Platformハードウェア構成ガイド』 (<https://community.rsa.com/community/products/netwitness/hardware-setup-guides>) を参照してください。

### Endpoint HybridまたはEndpoint Log Hybridホストのハードウェア仕様

新しいEndpoint HybridホストまたはEndpoint Log Hybridホストは、シリーズ5( Dell R730) ハードウェアまたはシリーズ6( Dell R740) ハードウェアにインストールする必要があります。Endpoint HybridまたはEndpoint Log Hybridをインストールする手順については、「[インストール後のタスク](#)」の「(オプション) タスク 2: Endpoint HybridまたはEndpoint Log Hybridのインストール」を参照してください。

### RSA NetWitness UEBAホストのハードウェア仕様

新しいNetWitness UEBAホストは、シリーズ5( Dell R630) ハードウェアにインストールする必要があります。NetWitness UEBAをインストールする手順については、「[インストール後のタスク](#)」の「(オプション) タスク3: NetWitness UEBAのインストール」を参照してください。

#### シリーズ5( DELL R630) の仕様

仕様	容量
モデル	Dell PowerEdge R630xl
プロセッサタイプ	インテルXeon E5 -2680v3
プロセッサ速度	2.5 GHz
キャッシュ	30MB
コア数	12
プロセッサ数	2
スレッド数	24
総メモリ	256 GB
内蔵ディスクコントローラー	Dell PERC H730
外部ディスクコントローラー	Dell PERC H830
SAN接続(HBA) -オプション	該当なし
リモート管理カード	iDRAC8 Enterprise

仕様	容量
ドライブ数	合計- 6ドライブ 1TB、2.5インチHDD×2 2TB、2.5インチHDD×4
シャーシ	1U
重量	18.4 kg( 40.5 lbs.)
NICカード*	オンボード 10 Gb銅線×2 10 Gb銅線×2、1 Gb銅線×2 (他のオプションも利用可能)
寸法	高さ: 4.28 cm( 1.68インチ) 幅: 48.23 cm( 18.98インチ) 奥行き: 75.51 cm( 29.72インチ)
電源	1100W 冗長
BTU/時	4100 BTU/時( 最大)
アンペア(仕様)	1100W / 220VAC = 5A
実際の消費電流(起動後)	2.1アンペア
EPS(秒あたりのイベントの数)	100K EPS
スレーブット	該当なし

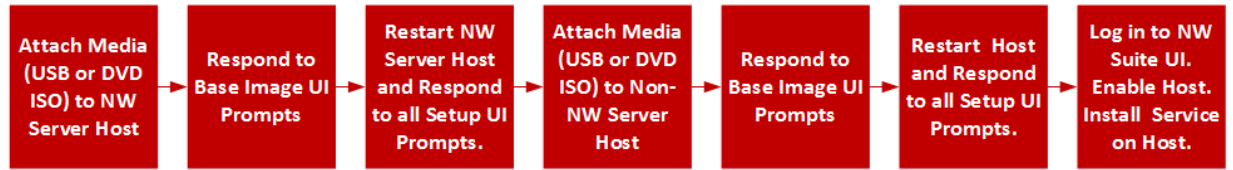
\* NICカードのオプションは、オンボード ドーター カードとのスワップまたはアドオンの場合に利用可能です。

## 外部接続ストレージ

外部ストレージ デバイス(DACやPowerVaultなど)を物理ホストに接続する場合は、これらのストレージを構成する方法について、RSA Linkの『ハードウェア構成ガイド』(<https://community.rsa.com/community/products/netwitness/hardware-setup-guides>)を参照してください。

## 物理ホストのインストールワークフロー

次の図では、RSA NetWitness® Platform 11.2の物理ホストのインストールワークフローを示します。



## カスタマー サポート へのお問い合わせ

RSA NetWitness Platform 11.2に関する支援が必要な場合には、RSAカスタマー サポートにお問い合わせください。

## インストールの準備 : ファイアウォール ポートを開く

---

「RSA NetWitness® Platform 導入ガイド」の「ネットワークアーキテクチャとポート」トピックに、導入時のすべてのポートが一覧表示されています。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。

**注意 :** ファイアウォール側でポートの構成が必要な場合には、構成が完了してからインストール作業を開始してください。

## インストール タスク

このトピックでは、NetWitness Platform 11.2を物理ホスト上にインストールするために必要なタスクについて説明します。

主要なタスクは2つあり、次の順番で完了する必要があります。

タスク1: NetWitness Server( NW Server) ホストへの11.2のインストール

タスク2: その他のすべてのコンポーネントのホストへの11.2のインストール

### タスク1: NetWitness Server( NW Server) ホストへの11.2のインストール

NW Serverでは、次のタスクを実行します。

- ベース イメージの作成。
- 11.2 NW Serverホストのセットアップ。

次の手順を実行して、11.2 NW Serverホストをインストールします。

1. ホストで、ベース イメージを作成します。
  - a. ホストにメディア(ISO)を接続します。

詳細については、「[RSA NetWitness Platformビルド スティックの作成手順](#)」を参照してください。

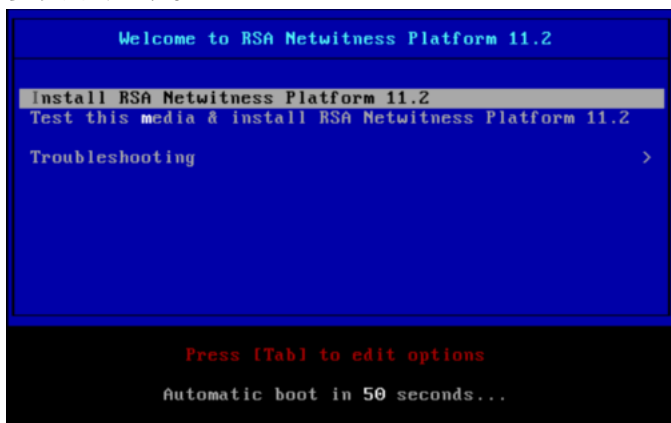
    - ハイパーバイザーのインストール: ISOイメージを使用します。
    - 物理メディア: ISOを使用し、Universal Netboot Installer( UNetbootin) または他の適切なイメージング ツールを使用して起動可能なフラッシュドライブ メディアを作成します。ISOからビルド スティックを作成する方法の詳細については、「[RSA NetWitness® Platformビルド スティックの作成手順](#)」を参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。
    - iDRACのインストール: 仮想メディア タイプは、次の通りです。
      - 仮想フロッピー(フラッシュドライブをマッピングする場合)。
      - 仮想CD(光学メディア デバイスまたはISOファイルをマッピングする場合)。
  - b. ホストにログインし、リブートします。

```
login: root
Password:
Last login: Tue Sep 19 13:27:15 on tty1
[root@saserver ~]# reboot
```
  - c. 再起動中にF11(起動メニュー)を選択し、ブート デバイスを選択して、接続されているメディアから起動します。

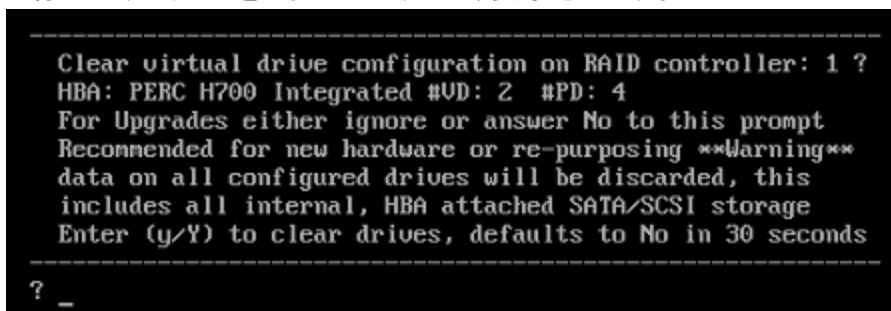
起動時のシステム チェックの後、[Welcome to RSA NetWitness Platform 11.2] インストールメニューが表示されます。物理USBフラッシュメディアを使用する場合、メニュー画面の表示は多



少異なります。



- d. [Install RSA NetWitness Platform 11.2] (デフォルトの選択) を選択し、Enterキーを押します。インストールプログラムが実行され、[Enter (y/Y) to clear drives] プロンプトが表示されたところで停止し、ドライブをフォーマットするよう要求されます。



- e. 「Y」と入力して、作業を続行します。  
デフォルトのアクションは「No」となっているため、プロンプトを無視すると、30秒後に「No」が選択され、ドライブはクリアされません。[Press enter to reboot]プロンプトが表示されます。

```
Clearing drive configuration in 15 seconds, <CTRL><ALT><DEL> to cancel
Ignore or answer no to this prompt after restarting
Re-labeling disks and virtual drives, clearing RAID configuration ...
0 logical volume(s) in volume group "netwitness_ug00" now active

Adapter 0: Configuration is Cleared.

Exit Code: 0x00
Invalid or no RAID configuration found: RAID Level = #HDD =

Adapter 0: Created VD 0

Adapter 0: Configured the Adapter!!

Exit Code: 0x00

Adapter 0: Created VD 1

Adapter 0: Configured the Adapter!!

Exit Code: 0x00

Run installation again after restart
Press enter to reboot
```

- f. Enterキーを押して、ホストをリブートします。  
インストールプログラムにより、ドライブを再度クリアするよう要求されます。

```
-----
Clear virtual drive configuration on RAID controller: 0 ?
HBA: PERC H730P Mini #VD: 2 #PD: 4
For Migrations either ignore or answer No to this prompt
Recommended for new hardware or re-purposing **Warning**
data on all configured drives will be discarded, this
includes all internal, HBA attached SATA/SCSI storage
Enter (y/Y) to clear drives, defaults to No in 30 seconds
-----
```

- g. ドライブはすでに消去されているため、「N」を入力します。  
[Enter Q (Quit) or R (Reinstall)]プロンプトが表示されます。

```
-----
No root level logical volumes found for Migration
Assuming this system is new or being reinstalled
Migration cannot proceed, system will be reimaged
If you had intended to migrate please quit and
contact support for assistance.
-----
Enter Q to Quit or R to Reinstall, Re-installing in 120 seconds?
```

- h. 「R」を入力し、ベース イメージをインストールします。  
インストール プログラムにより、インストール中のコンポーネントが表示されます。表示されるコンポーネントはアプライアンスによって異なります。その後、再起動します。

**注意:** 接続されたメディア(ビルド スティックなどISOファイルを含むメディア) から再起動しないでください。

```
CentOS Linux 7 (Core)
Kernel 3.10.0-514.26.1.el7.x86_64 on an x86_64

NWAPPLIANCE9248 login: root
Password:
[root@NWAPPLIANCE9248 ~]#
```

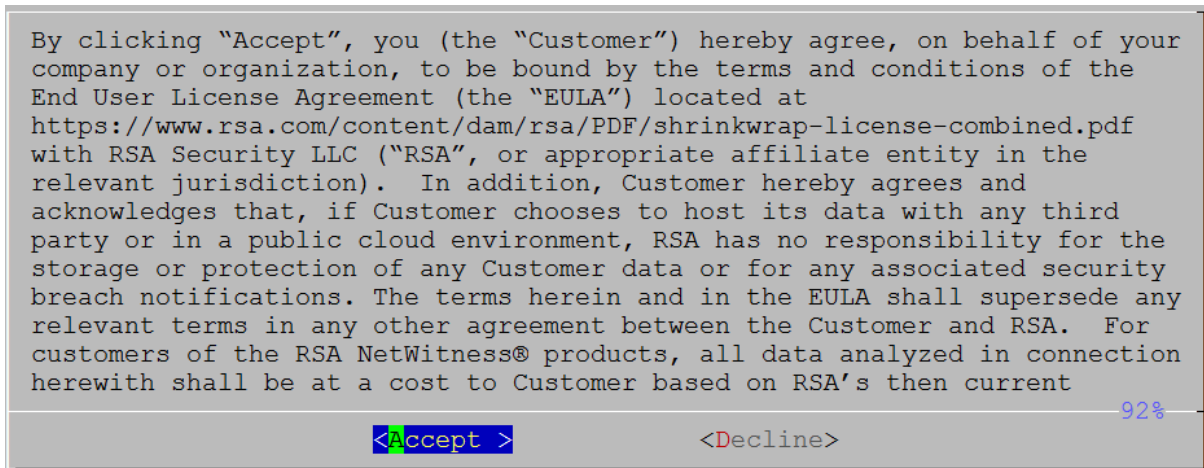
- i. root 認証情報を使用してホストにログオンします。
2. `nwsetup-tui` コマンドを実行し、ホストをセットアップします。  
`nwsetup-tui` (セットアッププログラム) が開始され、EULAが表示されます。

**注:** 1.) セットアッププログラムのプロンプト間を移動する場合、フィールド間の移動には下向き矢印と上向き矢印を使用し、コマンド間(<Yes>、<No>、<OK>、<Cancel>など)の移動にはTabキーを使用します。コマンドの選択を確定し、次のプロンプトに移動するには、Enterキーを押します。

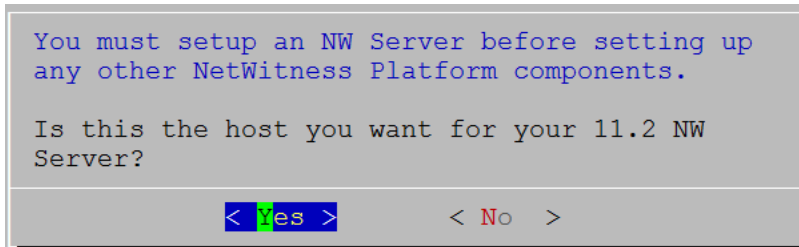
2.) セットアッププログラムは、ホストへのアクセスに使用中のデスクトップまたはコンソールのカラースキームを採用します。

3.) セットアッププログラム(`nwsetup-tui`) 実行時にDNSサーバを指定する場合、DNSサーバが有効であり(この場合の有効とはセットアップを実行する間有効であることを意味します)、`nwsetup-tui` からアクセスできる必要があります。DNSサーバの構成に誤りがあると、セットアップが失敗します。セットアップ中にアクセスできないDNSサーバに、セットアップ後にアクセスする必要がある場合(たとえば、セットアップ後に異なるDNSサーバを使用する環境にホストを移動する場合には、「[インストール後のタスク](#)」の「(オプション) タスク1: 11.2インストール後のDNSサーバの再構成」を参照してください)。

セットアップ(`nwsetup-tui`) 実行時にDNSサーバを指定しない場合、ステップ12の[NetWitness Platform Update Repositoryプロンプトで、[1 The Local Repo (on the NW Server)]]を選択する必要があります(DNSサーバが定義されていないので、システムが外部リポジトリにアクセスできないため)。



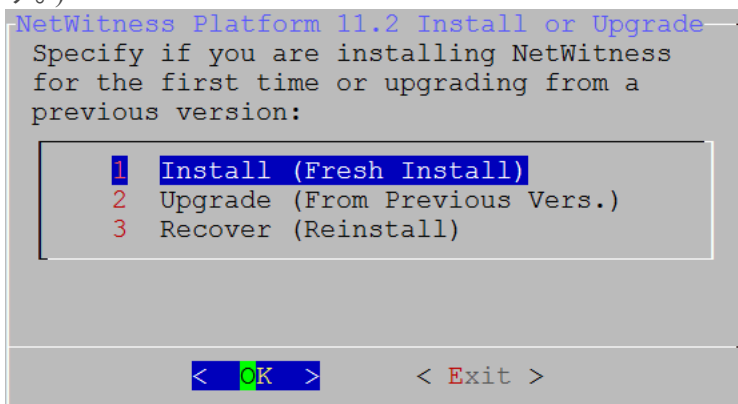
3. Tabキーで[Accept]に移動し、Enterキーを押します。  
[Is this the host you want for your 11.2 NW Server]プロンプトが表示されます。



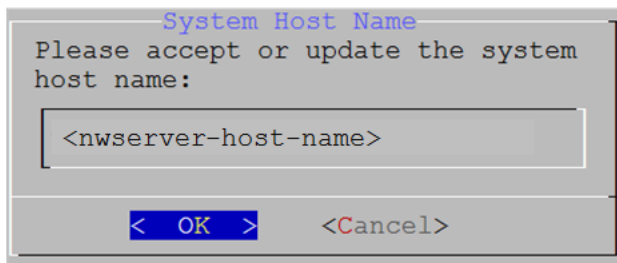
4. Tabキーで[Yes]に移動し、Enterキーを押します。  
NW Serverにすでに11.2をインストールした場合は、[No]を選択します。

**注意:** NW Serverに間違ったホストを選択してセットアップを完了した場合、セットアッププログラムを再度実行し(ステップ2~14)をすべて完了して誤りを修正する必要があります。

[Install or Upgrade]プロンプトが表示されます(Recoverは使用できません。11.2の災害復旧用です。)



5. Enterキーを押します。[Install (Fresh Install)]がデフォルトで選択されています。  
「Host Name」プロンプトが表示されます。



**注意:** ホスト名に「.」を含める場合は、有効なドメイン名も含める必要があります。

現在の名前を使用する場合は、**Enter**キーを押します。

6. 変更する場合は、ホスト名を編集して、Tabキーで[OK]に移動し、Enterキーを押します。  
[Master Password]プロンプトが表示されます。マスターパスワードと導入パスワードで使用可能な文字の一覧を、次に示します。

- 記号: ! @ # % ^ +
- 数字: 0~9
- 小文字: a~z
- 大文字: A~Z

マスターパスワードと導入パスワードでは、紛らわしい文字は使用できません。例:  
スペース { } [ ] ( ) / \ ' " ` ~ ; : . < > -

Master Password

The master password is utilized to set the default password for both the system recovery account and the NetWitness UI "admin" account. The system recovery account password should be safely stored in case account recovery is needed. The NetWitness UI "admin" account password can be updated upon login.

Enter a Master Password.

Password	*****
Verify	*****

< OK >                      <Cancel>

7. [Password]に入力し、下向き矢印で[Verify]に移動し、パスワードを再入力し、Tabキーで[OK]に移動し、Enterキーを押します。  
[Deployment Password]プロンプトが表示されます。

Deployment Password

The Deployment password is used when deploying NetWitness hosts. It needs to be safely stored and available when deploying additional hosts to your NetWitness Platform.

Enter a Deploy Password.

Password	*****
Verify	*****

< OK >                      <Cancel>

8. [Password]に入力し、下向き矢印で[Verify]に移動し、パスワードを再入力し、Tabキーで[OK]に移動し、Enterキーを押します。

次のオプション プロンプトのいずれかが表示されます。

- セットアッププログラムが、このホストの有効なIPアドレスを検出すると、次のプロンプトが表示されます。

```
IP Address <IP-address> is
currently assigned to this
host. Do you still want to
change network settings?

< Yes > < No >
```

このIPアドレスを使用し、ネットワーク設定を変更しない場合は、Enterキーを押します。ホストのIP構成を変更する場合、Tabキーで[Yes]に移動し、Enterキーを押します。

- SSH接続を使用している場合は、次の警告が表示されます。

**注:**ホスト コンソールから直接接続している場合には、次の警告は表示されません。

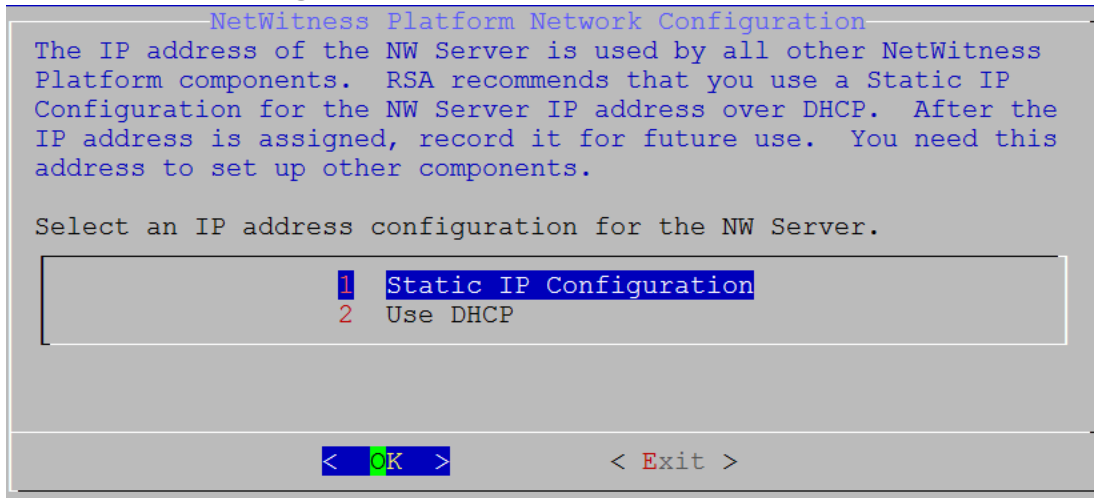
```
NetWitness Platform Network Configuration
WARNING - You are currently running the
NetWitness installation over an SSH
connection. Network configuration
updates will result in restarting the
network service which may cause the SSH
session to terminate.

< OK >
```

Enterキーを押して、警告プロンプトを閉じます。

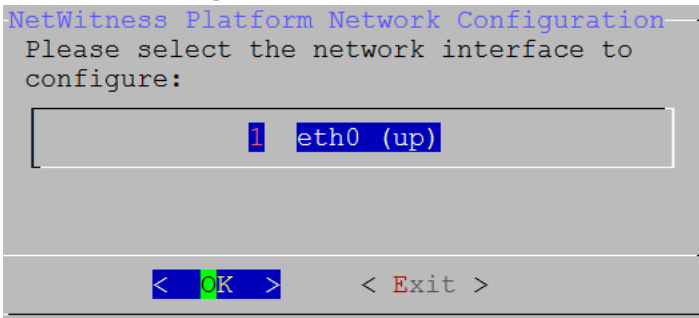
- セットアッププログラムがIPアドレスを検出し、その構成をそのまま使用するよう選択した場合は、[Update Repository]プロンプトが表示されます。ステップ12に移動し、インストールを完了します。

- セットアッププログラムがIPアドレスを検出できなかった場合、または既存のIP構成を変更する場合は、[Network Configuration]プロンプトが表示されます。

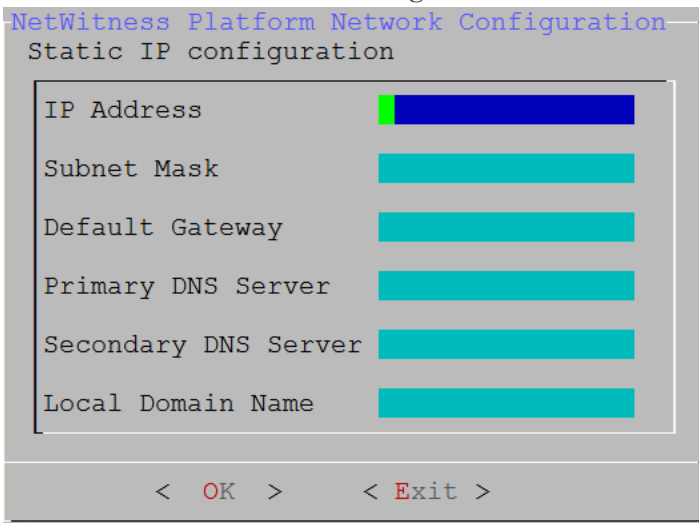




- Static IPを使用する場合は、Tabキーで[OK]に移動し、Enterキーを押します。DHCPを使用する場合、下向き矢印で[2 Use DHCP]に移動し、Enterキーを押します。[Network Configuration]プロンプトが表示されます。



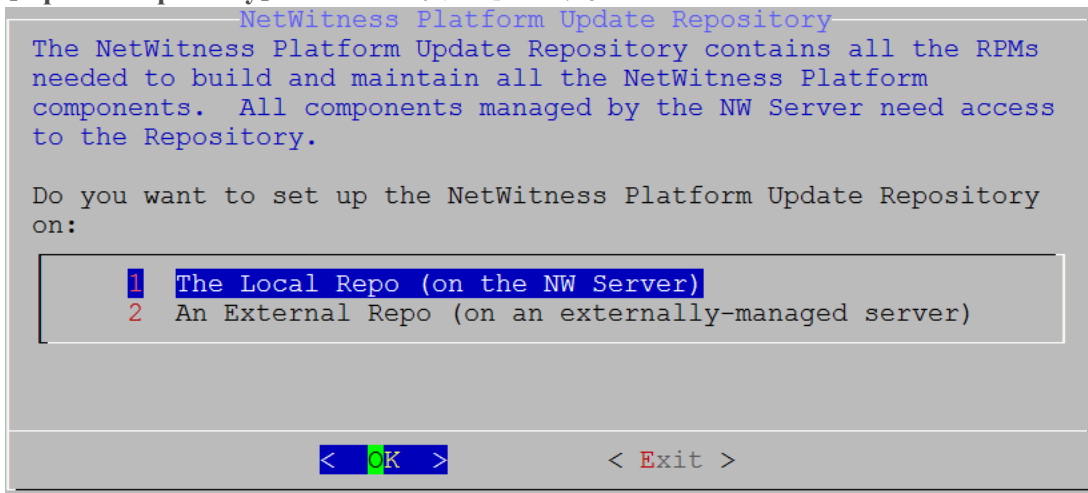
- 下向き矢印で使用するネットワーク インタフェースに移動し、Tabキーを使用して[OK]に移動し、Enterキーを押します。続行しない場合は、Tabキーを使用して[Exit]を選択します。[Static IP Configuration]プロンプトが表示されます。



- 設定値を入力し(下向き矢印を使用してフィールド間を移動)、Tabキーを使用して[OK]を選択し、Enterキーを押します。すべての必須フィールドが入力されていないと、「All fields are required」エラーメッセージが表示されます([Secondary DNS Server]フィールドと[Local Domain Name]フィールドは必須ではありません)。いずれかのフィールドで間違った構文や文字の長さを使用すると、「Invalid <field-name>」エラーメッセージが表示されます。

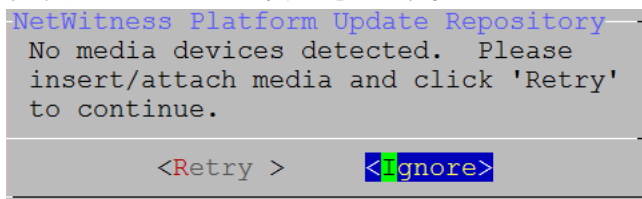
**注意:** DNSサーバを指定する場合は、インストールを続行する前に、DNSサーバの設定が正しく、ホストからアクセスできることを確認してください。

[Update Repository]プロンプトが表示されます。

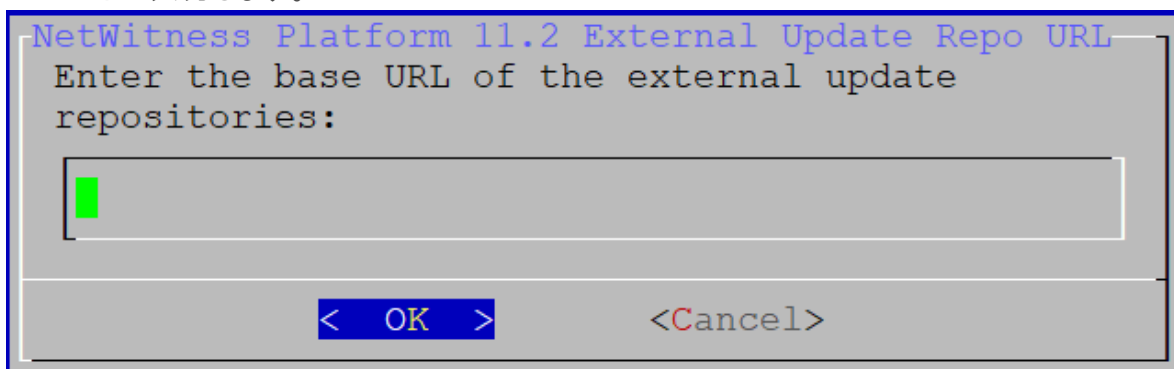


12. [Local Rep on the NW Server]を選択する場合は、Enterキーを押します。  
外部リポジトリを使用する場合は、下向き矢印を使用して[External Repo]へ移動し、Tabキーを使用して[OK]を選択し、Enterキーを押します。

- セットアッププログラムで[1 The Local Repo (on the NW Server)]を選択する場合、NetWitness Platform 11.2.0.0のインストール用の適切なメディア(ビルド スティックなどのISOファイルを含むメディア)が接続されていることを確認してください。プログラムが接続メディアを見つけれない場合、次のプロンプトが表示されます。



- [2 An External Repo (on an externally-managed Server)]を選択する場合、URLを入力するプロンプトが表示されます。リポジトリにアクセスして、RSAの更新とCentOSの更新を取得します。「[付録B: 外部リポジトリの作成](#)」を参照して、リポジトリと外部リポジトリURLを作成し、次のプロンプトで入力します。



NetWitness Platform外部リポジトリのベースURLを入力し、[OK]をクリックします。[Start Install]プロンプトが表示されます。

手順については、『*RSA NetWitness Platformホストおよびサービス スタート ガイド*』の「ホストとサー

ビスの手順」の「RSAおよびOS更新の外部リポジトリのセットアップ」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。

[Disable Firewall]プロンプトが表示されます。

```
Disable Firewall
Do you need to apply custom
firewall rules to this host?
("No" enforces the standard
NetWitness firewall rule set to
the host)
< Yes > < No >
```

13. 標準的なファイアウォールの構成を使用するには、Tabキーを使用して[No](デフォルト)に移動し、Enterキーを押します。標準的なファイアウォールの構成を無効化するには、Tabキーを使用して[Yes]に移動し、Enterキーを押します。

- 選択を確定する場合は、[Yes]を選択します。標準的なファイアウォールの構成を使用する場合は、[No]を選択します。

```
Warning: you chose to disable the default NetWitness
firewall configuration which means you must set up
firewall rules manually.

Select "Yes" to confirm that you will set up firewall
rules manually.
< Yes > < No >
```

[Start Install/Upgrade]プロンプトが表示されます。

```
Start Install/Upgrade
All the required information has been gathered.

Select "1 Install Now" to start the installation
on this host.

1 Install Now
2 Restart

< OK > < Exit >
```

14. Enterキーを押して、NW Serverに11.2をインストールします。  
「Installation complete」が表示されたら、このホストへの11.2 NW Serverのインストールは完了です。

**注:** `nwsetup-tui`コマンドを開始するときに表示される、次の図に示すようなハッシュコードのエラーは無視してください。Yumは、セキュリティ操作にMD5を使用しないため、システムセキュリティに影響することはありません。

```
ValueError: error:3207A06D:lib(50):B_HASH_init:cr new
Checksum type 'md5' disabled
(skipped due to only_if)
* file[/etc/yum.repos.d/CentOS-Base.repo] action delete (up to date)
* ruby_block[yum-cache-reload-CentOS-Base] action nothing (skipped due to action :nothing)
(up to date)
* yum_repository[Remove CentOS-CR repository] action delete
* execute[yum clean all CentOS-CR] action runERROR:root:code for hash md5 was not found.
Traceback (most recent call last):
  File "/usr/lib64/python2.7/hashlib.py", line 129, in <module>
    globals()[__func_name] = __get_hash(__func_name)
  File "/usr/lib64/python2.7/hashlib.py", line 98, in __get_openssl_constructor
    f(usedforsecurity=False)
```

## タスク2: その他のコンポーネントのホストへの11.2のインストール

非NW Serverでは、次のタスクを実行します。

- ベース イメージの作成。
- 11.2 非NW Serverホストのセットアップ。

ESAホストでは、次の手順を実行します。

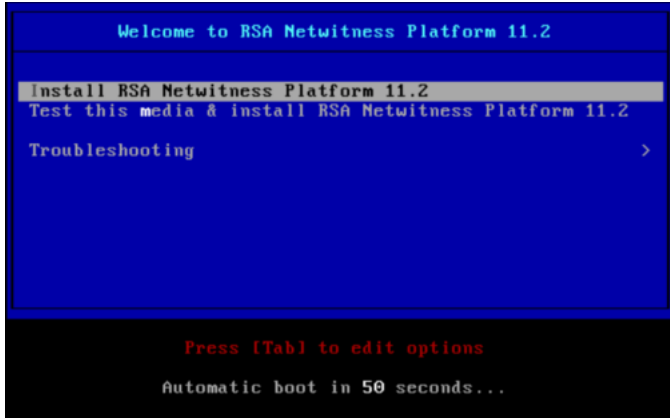
- プライマリESAホストをインストールします。セットアッププログラムを完了後、UIの[管理]>[ホスト]ビューで、ESAプライマリサービスをホストにインストールします。
- (オプション) セカンダリESAホストを使用する場合、セットアッププログラムを完了後、UIの[管理]>[ホスト]ビューで、ESAセカンダリサービスをホストにインストールします。

次の手順を実行して、NetWitness Platform 11.2を非NW Serverホストにインストールします。

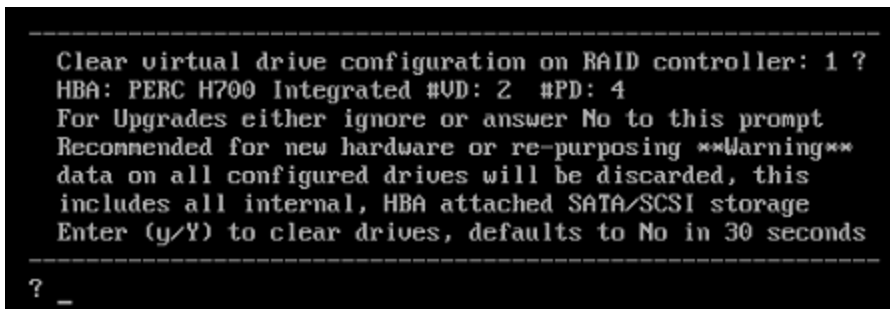
1. ホストで、ベースイメージを作成します。
  - a. ホストにメディア(ビルド スティックなどISOファイルを含むメディア)を接続します。  
詳細については、「*RSA NetWitness Platform*ビルド スティックの作成手順」を参照してください。
    - ハイパーバイザーのインストール: ISOイメージを使用します。
    - 物理メディア: ISOファイルを使用し、Universal Netboot Installer(UNetbootin)または他の適切なイメージングツールを使用して起動可能なフラッシュドライブメディアを作成します。ISOファイルからビルド スティックを作成する方法の詳細については、「*RSA NetWitness® Platform*ビルド スティックの作成手順」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。
    - iDRACのインストール: 仮想メディアタイプは、次の通りです。
      - 仮想フロッピー(フラッシュドライブをマッピングする場合)。
      - 仮想CD(光学メディア デバイスまたはISOファイルをマッピングする場合)。  
詳細については、「*RSA NetWitness Platform*ビルド スティックの作成手順」を参照してください。
  - b. ホストにログインし、リブートします。

```
login: root
Password:
Last login: Tue Sep 19 13:27:15 on tty1
[root@saserver ~]# reboot
```

- c. 再起動中にF11(起動メニュー)を選択し、ブート デバイスを選択して、接続されているメディアから起動します。  
起動時のシステム チェックの後、[Welcome to RSA NetWitness Platform 11.2] インストールメニューが表示されます。物理USBフラッシュメディアを使用する場合、メニュー画面の表示は多少異なります。



- d. [Install RSA NetWitness Platform 11.2] (デフォルトの選択) を選択し、Enterキーを押します。インストールプログラムが実行され、[Enter (y/Y) to clear drives] プロンプトが表示されたところで停止し、ドライブをフォーマットするよう要求されます。



- e. 「Y」と入力して、作業を続行します。  
デフォルトのアクションは「No」となっているため、プロンプトを無視すると、30秒後に「No」が選択され、ドライブはクリアされません。[Press enter to reboot]プロンプトが表示されます。

```
Clearing drive configuration in 15 seconds, <CTRL><ALT><DEL> to cancel
Ignore or answer no to this prompt after restarting
Re-labeling disks and virtual drives, clearing RAID configuration ...
0 logical volume(s) in volume group "netwitness_vg00" now active

Adapter 0: Configuration is Cleared.

Exit Code: 0x00
Invalid or no RAID configuration found: RAID Level = #HDD =

Adapter 0: Created VD 0

Adapter 0: Configured the Adapter!!

Exit Code: 0x00

Adapter 0: Created VD 1

Adapter 0: Configured the Adapter!!

Exit Code: 0x00

Run installation again after restart
Press enter to reboot
```

- f. Enterキーを押して、ホストをリブートします。  
インストールプログラムにより、ドライブを再度クリアするよう要求されます。

```
-----
Clear virtual drive configuration on RAID controller: 0 ?
HBA: PERC H730P Mini #VD: 2 #PD: 4
For Migrations either ignore or answer No to this prompt
Recommended for new hardware or re-purposing **Warning**
data on all configured drives will be discarded, this
includes all internal, HBA attached SATA/SCSI storage
Enter (y/Y) to clear drives, defaults to No in 30 seconds
-----
```

- g. ドライブはすでに消去されているため、「N」を入力します。  
[Enter Q (Quit) or R (Reinstall)]プロンプトが表示されます。

```
-----
No root level logical volumes found for Migration
Assuming this system is new or being reinstalled
Migration cannot proceed, system will be reimaged
If you had intended to migrate please quit and
contact support for assistance.
-----
Enter Q to Quit or R to Reinstall, Re-installing in 120 seconds?
```

- h. 「R」を入力し、ベース イメージをインストールします。  
インストールプログラムにより、インストール中のコンポーネントが表示されます。表示されるコンポーネントはアプライアンスによって異なります。その後、再起動します。

**注意:** 接続されたメディア(ビルド スティックなどISOファイルを含むメディア) から再起動しないでください。

```
CentOS Linux 7 (Core)
Kernel 3.10.0-514.26.1.el7.x86_64 on an x86_64

NWAPPLIANCE9240 login: root
Password:
[root@NWAPPLIANCE9240 ~]#
```

- i. root 認証情報を使用してホストにログオンします。
2. `nwsetup-tui` コマンドを実行し、ホストをセットアップします。  
`nwsetup-tui` (セットアッププログラム) が開始され、EULAが表示されます。

**注:** セットアッププログラム(`nwsetup-tui`) 実行時にDNSサーバを指定する場合、DNSサーバが有効であり(この場合の有効とはセットアップを実行する間有効であることを意味します)、`nwsetup-tui` からアクセスできる必要があります。DNSサーバの構成に誤りがあると、セットアップが失敗します。セットアップ中にアクセスできないDNSサーバに、セットアップ後にアクセスする必要がある場合(たとえば、セットアップ後に異なるDNSサーバを使用する環境にホストを移動する場合)には、「[インストール後のタスク](#)」の「(オプション) タスク1: 11.2インストール後のDNSサーバの再構成」を参照してください。

`nwsetup-tui` 実行時にDNSサーバを指定しない場合、ステップ11の[NetWitness Platform Update Repository]プロンプトで、[1 The Local Repo (on the NW Server)]を選択する必要があります(DNSサーバが定義されていないので、システムが外部リポジトリにアクセスできないため)。

```
By clicking "Accept", you (the "Customer") hereby agree, on behalf of your
company or organization, to be bound by the terms and conditions of the
End User License Agreement (the "EULA") located at
https://www.rsa.com/content/dam/rsa/PDF/shrinkwrap-license-combined.pdf
with RSA Security LLC ("RSA", or appropriate affiliate entity in the
relevant jurisdiction). In addition, Customer hereby agrees and
acknowledges that, if Customer chooses to host its data with any third
party or in a public cloud environment, RSA has no responsibility for the
storage or protection of any Customer data or for any associated security
breach notifications. The terms herein and in the EULA shall supersede any
relevant terms in any other agreement between the Customer and RSA. For
customers of the RSA NetWitness® products, all data analyzed in connection
herewith shall be at a cost to Customer based on RSA's then current
```

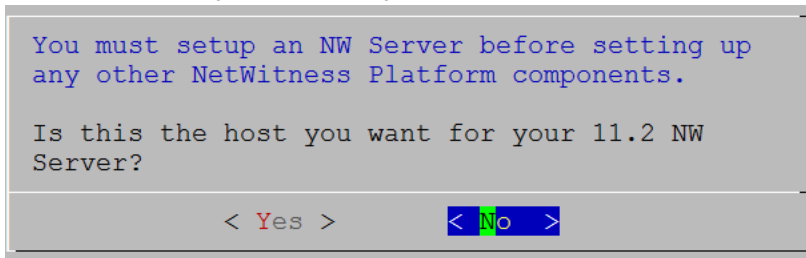
92%

&lt;Accept &gt;

&lt;Decline&gt;

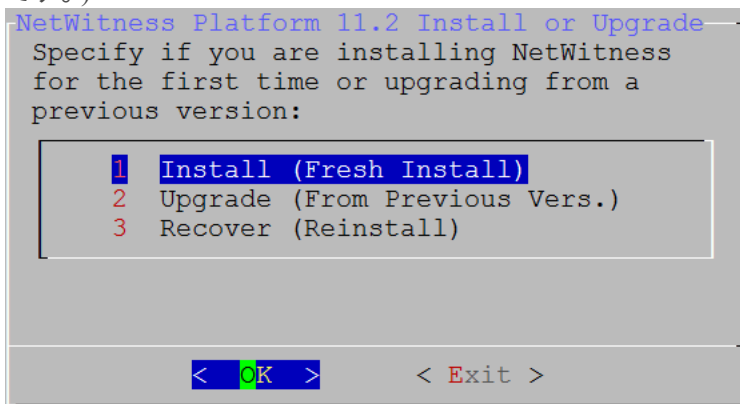


3. Tabキーで[Accept]に移動し、Enterキーを押します。  
[Is this the host you want for your 11.2 NW Server]プロンプトが表示されます。

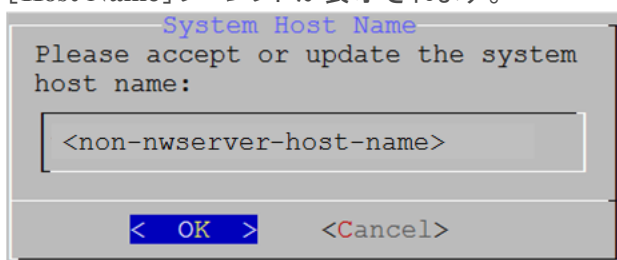


**注意:** NW Serverに間違ったホストを選択してインストールを完了した場合は、セットアッププログラムを再度実行し、「[タスク1: NetWitness Server\( NW Server\) ホストへの11.2のインストール](#)」のステップ2~14を完了して誤りを修正する必要があります。

4. Enterキーを押します。(No)  
[Install or Upgrade]プロンプトが表示されます。(Recoverは選択できません。11.2の災害復旧用です。)



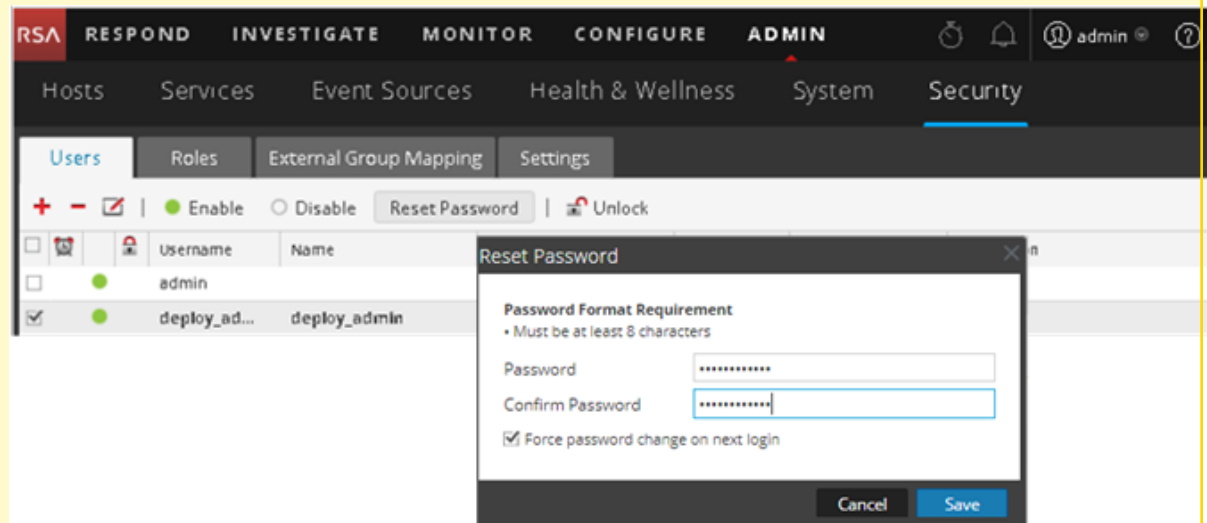
5. Enterキーを押します。[Install (Fresh Install)]がデフォルトで選択されています。  
[Host Name]プロンプトが表示されます。



**注意:** ホスト名に「.」を含める場合は、有効なドメイン名も含める必要があります。

6. この名前を使用する場合は、Enterキーを押します。ホスト名を変更する場合は、Tabキーで[OK]を選択し、Enterキーを押します。  
[Master Password]プロンプトが表示されます。

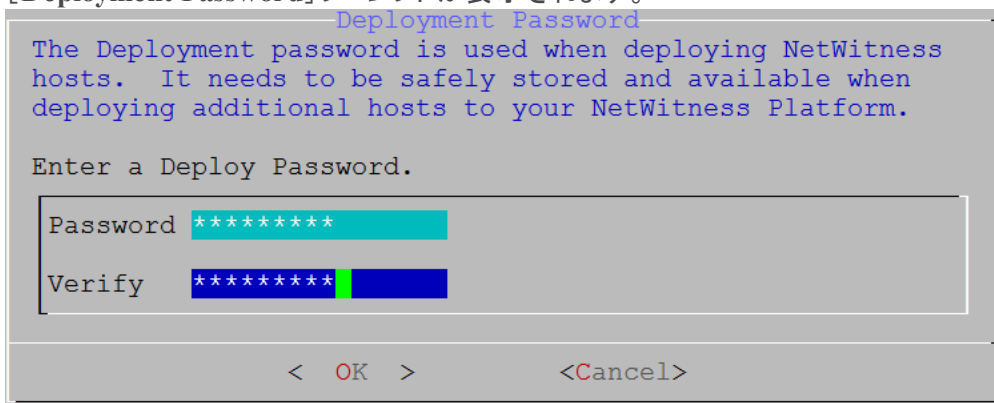
**注意:** NetWitness Platformユーザ インタフェース ([管理] > [セキュリティ])に進み、`deploy-admin`を選択し、[パスワードのリセット]をクリック)で、`deploy_admin`ユーザのパスワードを変更する場合、



次の手順を実行する必要があります。

1. SSHでNW Serverホストに接続します。
2. `/opt/rsa/saTools/bin/set-deploy-admin-password`スクリプトを実行します。
3. 非NW Serverホストを新しくインストールする場合は、新しいパスワードを使用します。
4. 導入環境内のすべての非NW Serverホスト上で、`/opt/rsa/saTools/bin/set-deploy-admin-password`スクリプトを実行します。
5. 今後のインストールで参照する可能性があるため、パスワードをメモします。

[Deployment Password]プロンプトが表示されます。



**注:** NW Serverのインストール時に使用したのと同じ導入パスワードを使用する必要があります。

7. [Password]に入力し、下向き矢印で[Verify]に移動し、パスワードを再入力し、Tabキーで[OK]に移動し、Enterキーを押します。
  - セットアッププログラムが、このホストの有効なIPアドレスを検出すると、次のプロンプトが表示されます。

```
IP Address <IP-address> is
currently assigned to this
host. Do you still want to
change network settings?

< Yes > < No >
```

このIPアドレスを使用し、ネットワーク設定を変更しない場合は、Enterキーを押します。ホストのIP構成を変更する場合、Tabキーで[Yes]に移動し、Enterキーを押します。

- SSH接続を使用している場合は、次の警告が表示されます。

**注:** ホスト コンソールから直接接続している場合には、次の警告は表示されません。

```
NetWitness Platform Network Configuration
WARNING - You are currently running the
NetWitness installation over an SSH
connection. Network configuration
updates will result in restarting the
network service which may cause the SSH
session to terminate.

< OK >
```

Enterキーを押して、警告プロンプトを閉じます。

- セットアッププログラムがIPアドレスを検出し、その構成をそのまま使用するよう選択した場合は、[Update Repository]プロンプトが表示されます。ステップ11に移動し、インストールを完了します。
- セットアッププログラムがIPアドレスを検出できなかった場合、または既存のIP構成の変更を選択した場合は、[Network Configuration]プロンプトが表示されます。

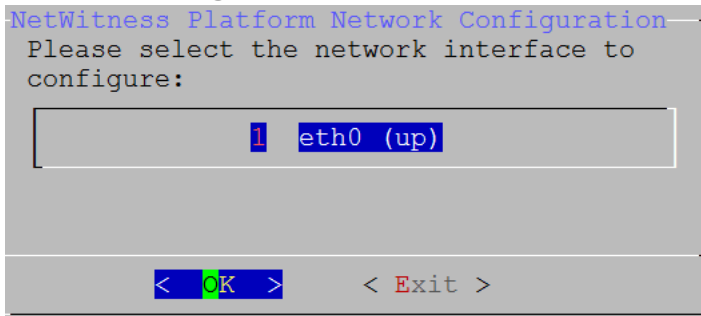
```
NetWitness Platform Network Configuration
The IP address of the NW Server is used by all other NetWitness
Platform components. RSA recommends that you use a Static IP
Configuration for the NW Server IP address over DHCP. After the
IP address is assigned, record it for future use. You need this
address to set up other components.

Select an IP address configuration for the NW Server.

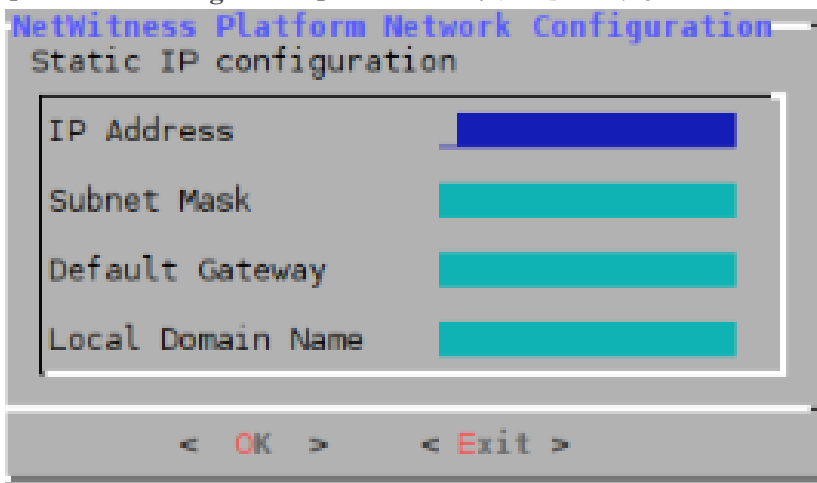
1 Static IP Configuration
2 Use DHCP

< OK > < Exit >
```

- Static IPを使用する場合は、Tabキーで[OK]に移動し、Enterキーを押します。  
DHCPを使用する場合は、下向き矢印で[2 Use DHCP]に移動し、Enterキーを押します。  
[Network Configuration]プロンプトが表示されます。



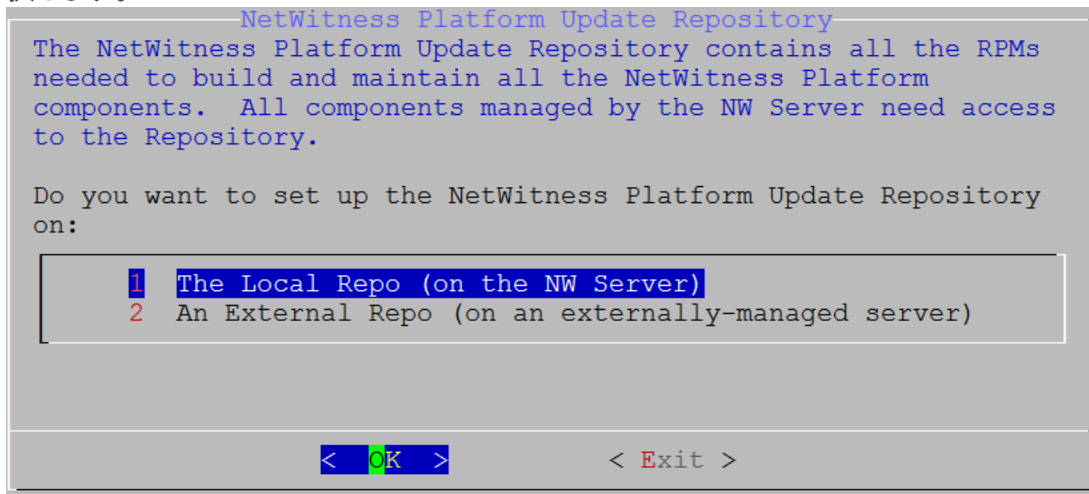
- 下向き矢印で使用するネットワーク インタフェースに移動し、Tabキーを使用して[OK]に移動し、Enterキーを押します。続行しない場合は、Tabキーを使用して[Exit]を選択します。  
[Static IP Configuration]プロンプトが表示されます。



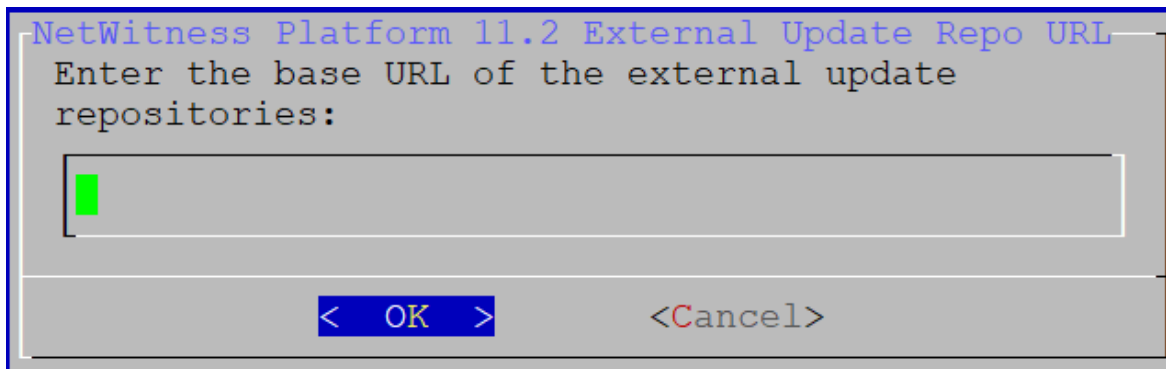
10. 設定値を入力し(下向き矢印を使用してフィールド間を移動)、Tabキーを使用して[OK]を選択し、Enterキーを押します。  
 すべての必須フィールドが入力されていないと、「All fields are required」エラーメッセージが表示されます([Secondary DNS Server]フィールドと[Local Domain Name]フィールドは必須ではありません)。  
 いずれかのフィールドで間違った構文や文字の長さを使用すると、「Invalid <field-name>」エラーメッセージが表示されます。

**注意:** DNSサーバを選択する場合は、インストールを続行する前に、DNSサーバの設定が正しく、ホストからアクセスできることを確認してください。

[Update Repository]プロンプトが表示されます。  
 すべてのホストについて、NW Serverホストをインストールしたときに選択したのと同じリポジトリを選択します。

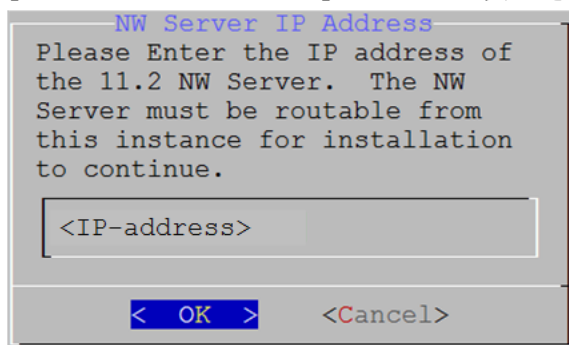


11. Enterキーを押すと、[Local Repo on the NW Server]が選択されます。  
 外部リポジトリを使用する場合は、下向き矢印を使用して[External Repo]へ移動し、Tabキーを使用して[OK]を選択し、Enterを押します。
- セットアッププログラムで[1 The Local Repo (on the NW Server)]を選択する場合、NetWitness Platform 11.2.0.0のインストール用の適切なメディア(ビルド スティックなどのISOファイルを含むメディア)が接続されていることを確認してください。
  - [2 An External Repo (a server managed externally - not on the NW Server)]を選択する場合、URLを入力するプロンプトが表示されます。リポジトリにアクセスして、RSAの更新とCentOSの更新を取得します。「[付録B: 外部リポジトリの作成](#)」を参照して、リポジトリと外部リポジトリURLを作成し、次のプロンプトで入力します。

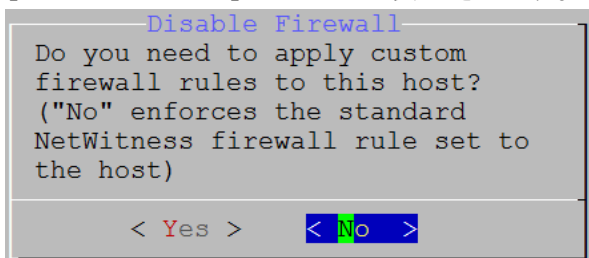


NetWitness Platform外部リポジトリのベースURLを入力し、Tabキーを使用して[OK]を選択し、Enterキーを押します。

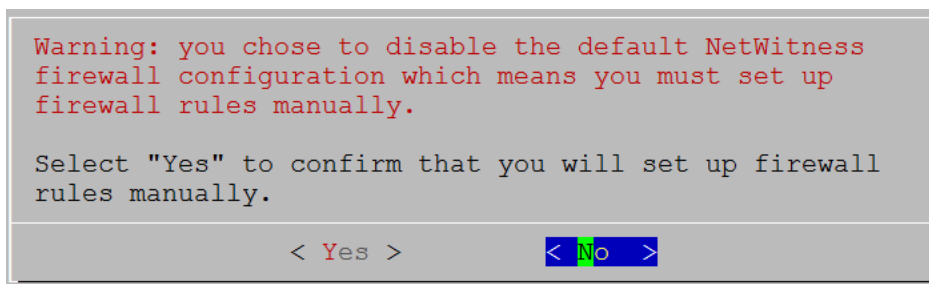
[NW Server IP Address]プロンプトが表示されます。



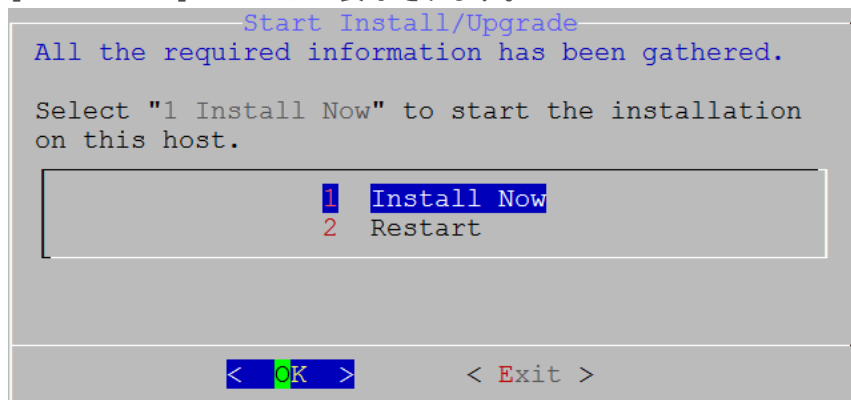
12. NW ServerのIPアドレスを入力します。Tabキーを使用して[OK]を選択し、Enterキーを押します。  
[Disable Firewall]プロンプトが表示されます。





13. 標準的なファイアウォールの構成を使用するには、Tabキーを使用して[No](デフォルト)に移動し、Enterキーを押します。標準的なファイアウォールの構成を無効化するには、Tabキーを使用して[Yes]に移動し、Enterキーを押します。
  - 選択を確定する場合は、[Yes]を選択します。標準的なファイアウォールの構成を使用する場合は、[No]を選択します。



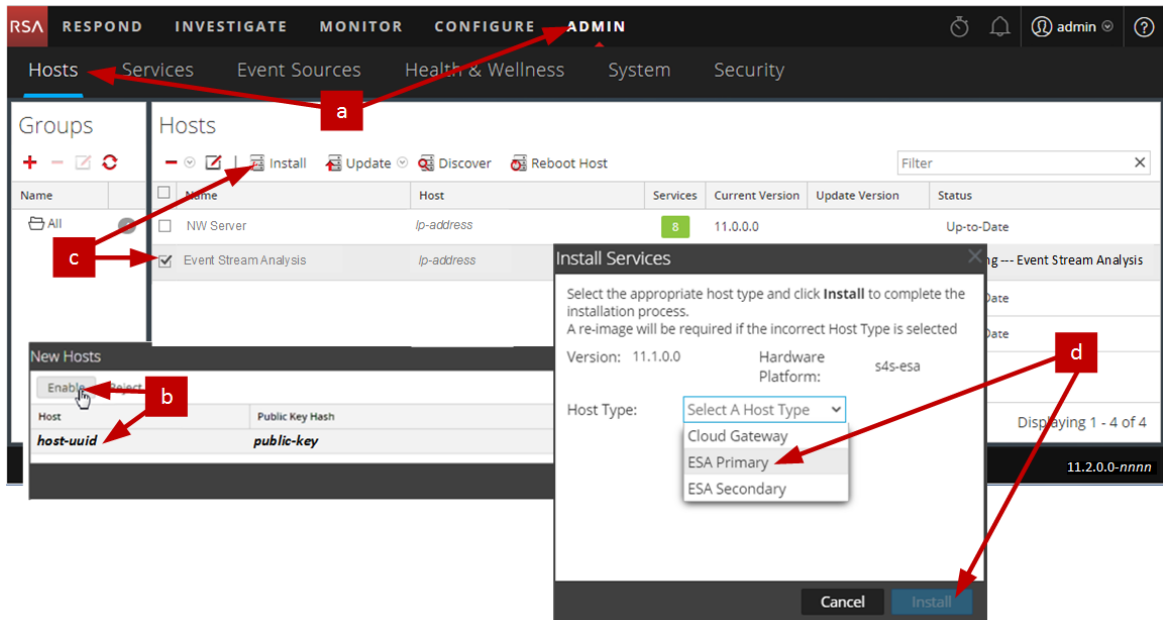
[Start Install]プロンプトが表示されます。



14. Enterキーを押して、非NW Serverのサーバに11.2をインストールします。  
「Installation complete」が表示されたら、NetWitness Platform 11.2と互換性を持つオペレーティングシステム稼働する汎用非NW Serverホストのインストールが完了します。
15. コンポーネント サービスをホストにインストールします。
  - a. NetWitness Platformにログインし、[管理]>[ホスト]に移動します。  
[新しいホスト]ダイアログが表示され、[ホスト]ビューがバックグラウンドでグレー表示されます。

注:[新しいホスト]ダイアログが表示されない場合、[ホスト]ビューのツールバーで[検出]をクリックします。
  - b. [新しいホスト]ダイアログでホストを選択し、[有効化]をクリックします。  
[新しいホスト]ダイアログが閉じ、[ホスト]ビューにホストが表示されます。
  - c. [ホスト]ビューでそのホストを選択し(たとえばEvent Stream Analysis)、 Install  をクリックします。  
[サービスのインストール]ダイアログが表示されます。

- d. [ホスト タイプ]で適切なホスト タイプ(たとえば、ESAプライマリ)を選択し、[インストール]をクリックします。



NetWitness Platformで非NW Serverホストのインストールが完了しました。

16. 残りのNetWitness Platform 非NW Serverのコンポーネントについて、ステップ1～15を実行します。
17. インストールされたサービスのライセンス要件をすべて満たします。  
詳細については、『*NetWitness Platform 11.2ライセンス管理ガイド*』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。



## 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。

## インストール後のタスク

このトピックでは、11.2をインストールした後に完了する必要があるタスクを示します。

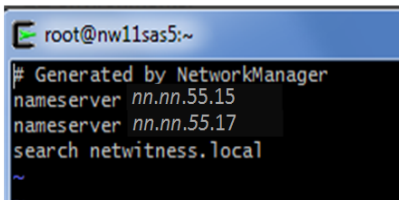
- 全般
- RSA NetWitness® Endpoint Insights
- FIPSの有効化
- RSA NetWitness® UEBA

### 全般

#### (オプション) タスク1: 11.2インストール後のDNSサーバの再構成

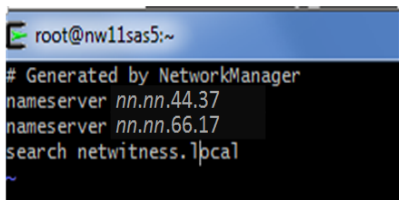
NetWitness Platform 11.2のDNSサーバを再構成するには、NetWitness Serverで次の手順を実行します。

1. `root` 認証情報で、サーバホストにログインします。
2. `/etc/netwitness/platform/resolv.dnsmasq` ファイルを編集します。
  - a. `nameserver` のIPアドレスを置換します。  
両方のDNSサーバを置換する必要がある場合、両方のIPアドレスを置換します。  
次の例は、既存のDNSエントリを示します。



```
root@nw11sas5:~  
# Generated by NetworkManager  
nameserver nn.nn.55.15  
nameserver nn.nn.55.17  
search netwitness.local  
~
```

次の例は、置換後の新しいDNSエントリを示します。



```
root@nw11sas5:~  
# Generated by NetworkManager  
nameserver nn.nn.44.37  
nameserver nn.nn.66.17  
search netwitness.local  
~
```

- b. `/etc/netwitness/platform/resolv.dnsmasq` ファイルを保存します。
- c. 次のコマンドを実行して内部DNSを再起動します:  
`systemctl restart dnsmasq`

## RSA NetWitness Endpoint Insights

### (オプション) タスク2: Endpoint HybridまたはEndpoint Log Hybridのインストール

導入環境にNetWitness Platform Endpoint Insightsをインストールするには、次のいずれかのサービスをインストールする必要があります。



- Endpoint Hybrid
- Endpoint Log Hybrid

**注意:** 導入環境には、上記のサービスの1つのインスタンスしかインストールできません。

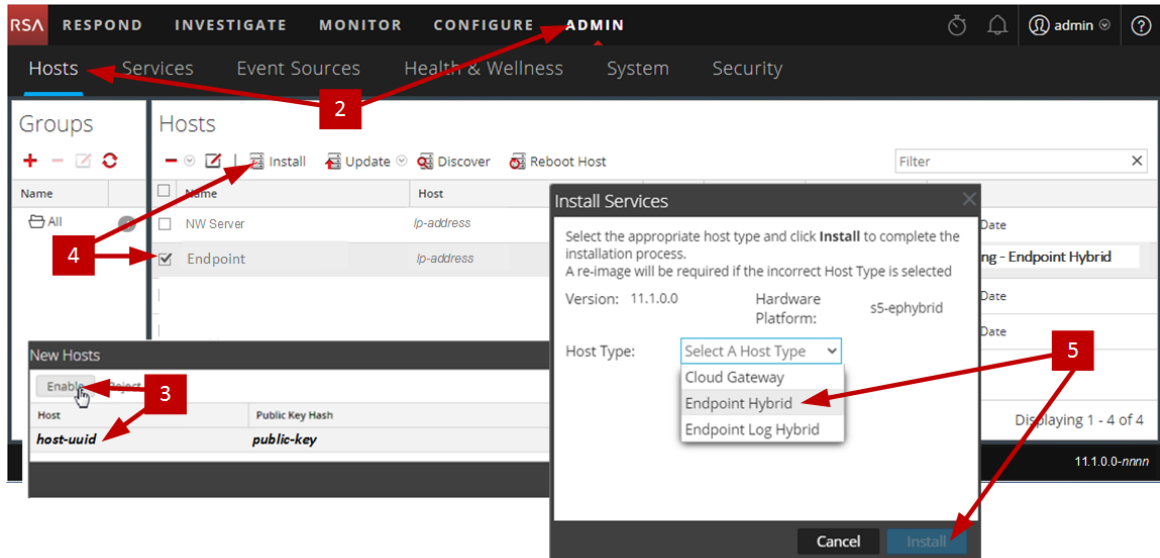
**注:** S5またはDell R730アプライアンスにEndpoint HybridまたはEndpoint Log Hybridをインストールする必要があります。

1. 物理ホストの場合は、「*NetWitness Platform バージョン11.2 インストールガイド*」にある「インストール タスク」の「タスク2 - その他のコンポーネント ホストへの11.2のインストール」のステップ1 - 14を実行します。仮想ホストの場合は、ステップ1 - 15を実行します。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。
2. NetWitness Platformにログインし、[管理] > [ホスト]の順にクリックします。  
[新しいホスト]ダイアログが表示され、[ホスト]ビューがバックグラウンドでグレー表示されます。

**注:** [新しいホスト]ダイアログが表示されない場合、[ホスト]ビューのツールバーで[検出]をクリックします。

3. [新しいホスト]ダイアログでホストを選択し、[有効化]をクリックします。  
[新しいホスト]ダイアログが閉じ、[ホスト]ビューにホストが表示されます。
4. [ホスト]ビューでそのホストを選択し(たとえばEndpoint)、 Install  をクリックします。  
[サービスのインストール]ダイアログが表示されます。

- 適切なサービス(Endpoint HybridまたはEndpoint Log Hybrid)を選択し、[インストール]をクリックします。  
次のスクリーンショットではEndpoint Hybridが例として使用されています。



- すべてのEndpoint HybridまたはEndpoint Log Hybridサービスが実行中であることを確認します。
- エンドポイント メタ転送を構成します。  
エンドポイント メタ転送を構成する手順については、『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。
- Endpoint Insightsエージェントをインストールします。  
エージェントをインストールする手順の詳細については、「Endpoint Insightsエージェント インストールガイド」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。

## FIPSの有効化

### (オプション) タスク3 - FIPSモードの有効化

Log Collector、Log Decoder、Decoderを除くすべてのサービスではFIPS(連邦情報処理標準)が有効になっています。Log Collector、Log Decoder、Decoder以外のサービスではFIPSを無効にできません。これらのサービスでFIPSを有効にする方法については、『RSA NetWitness Platform システムメンテナンスガイド』の「FIPSの有効化/無効化」トピック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。

## RSA NetWitness® UEBA

### (オプション) タスク4: NetWitness UEBAのインストール

NetWitness Platform 11.2でNetWitness UEBAをセットアップするには、NetWitness UEBAサービスをインストールして構成する必要があります。


次の手順では、NetWitness UEBAホスト タイプにNetWitness UEBAサービスをインストールし、サービスを構成する方法を示します。

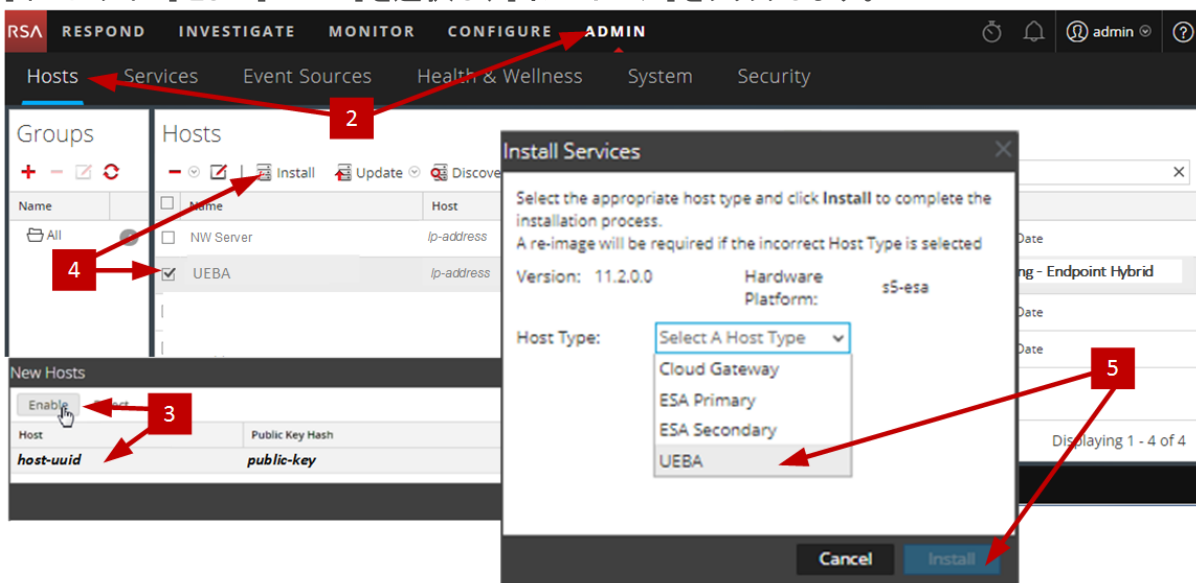
1. 物理ホストの場合は、「*NetWitness Platform バージョン11.2 インストールガイド*」にある「インストールタスク」の「タスク2 - その他のコンポーネント ホストへの11.2のインストール」のステップ1 - 14を実行します。仮想ホストの場合は、ステップ1 - 15を実行します。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

**注:** KibanaおよびAirflow Webサーバのユーザ インタフェースのパスワードは、deploy\_adminのパスワードと同じです。このパスワードを記録し、安全な場所に保存するようにしてください。

2. NetWitness Platformにログインし、[管理] > [ホスト]の順にクリックします。  
[新しいホスト]ダイアログが表示され、[ホスト]ビューがバックグラウンドでグレー表示されます。

**注:** [新しいホスト]ダイアログが表示されない場合、[ホスト]ビューのツールバーで[検出]をクリックします。

3. [新しいホスト]ダイアログでホストを選択し、[有効化]をクリックします。  
[新しいホスト]ダイアログが閉じ、[ホスト]ビューにホストが表示されます。
4. [ホスト]ビューでそのホストを選択し(たとえばUEBA)、 Install をクリックします。  
[サービスのインストール]ダイアログが表示されます。
5. [ホスト タイプ]として[UEBA]を選択し、[インストール]をクリックします。




6. UEBAサービスが実行中であることを確認します。
7. NetWitness UEBAのライセンス要件を満足する必要があります。  
詳細については、『*NetWitness Platform 11.2ライセンス管理ガイド*』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。

**注:** NetWitness Platformは、UEBA( User and Entity Behavior Analytics) ライセンスをサポートしています。このライセンスは、ユーザ数に基づいています。標準提供の評価版ライセンスは、90日間有効です。UEBAライセンスの場合、UEBAサービスをNetWitness Platform製品に導入した時点から、90日の評価期間が開始します。

8. NetWitness UEBAを構成します。  
データソース( BrokerまたはConcentrator)、履歴データの収集開始日、およびデータスキーマを構成する必要があります。

**重要:** 導入環境に複数のConcentratorがある場合、導入階層の最上位のBrokerをNetWitness UEBAデータソースとして割り当てることを推奨します。

- a. 選択するデータスキーマ( AUTHENTICATION、FILE、ACTIVE\_DIRECTORY、またはこれらのスキーマの任意の組み合わせ)のNWDB上の最も早い日付を決定し、ステップdのstartTimeに指定します。複数のスキーマを指定する場合は、すべてのスキーマの中で最も早い日付を使用します。どのデータスキーマを選択すればよいかわからない場合は、3つすべてのデータスキーマ( AUTHENTICATION、FILE、ACTIVE\_DIRECTORY)を指定すれば、使用可能なWindowsログに基づいてサポートできるモデルをUEBAが調整します。以下のいずれかの方法を使用して、データソースの日付を決定することができます。
  - データ保存期間を使用します( データ保存期間が48時間の場合、startTimeには現在の時刻から48時間以内の日時を指定します)。
  - NWDBから最も古い日付を検索します。
- b. データソース( BrokerまたはConcentrator) への認証に使用するユーザアカウントを作成します。
  - i. NetWitness Platformにログインします。
  - ii. [管理] > [サービス]に移動します。
  - iii. データソース サービス( BrokerまたはConcentrator) を探します。  
  
サービスを選択し、 (アクション) > [表示] > [セキュリティ]を選択します。
  - iv. 新しいユーザを作成し、そのユーザにAnalystsロールを割り当てます。

次の例は、Broker用に作成されたユーザアカウントを示しています。

The screenshot displays the RSA NetWitness Platform Admin console. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. The 'ADMIN' section is active, showing 'Hosts', 'Services', 'Event Sources', 'Health & Wellness', 'System', and 'Security'. The 'Security' section is expanded to show 'Users', 'Roles', and 'Settings'. The 'Users' tab is selected, and the 'Broker' user is highlighted in the list. The main content area shows the configuration for the 'Broker' user, including fields for Name, Username, Password, Confirm Password, Email, and Description. The 'User Settings' section includes 'Auth Type' (NetWitness Platform), 'Core Query Timeout' (5), 'Query Prefix', and 'Session Threshold' (0). The 'Role Membership' section shows a list of roles with 'Analysts' selected.

c. Netwitness UEBAホストにSSHでログインします。

## d. 次のコマンドを実行します。

```
/opt/rsa/saTools/ueba-server-config -u <user> -p <password> -h <host> -o
<type> -t <startTime> -s <schemas> -v
```

各項目の意味は次のとおりです。

引数	変数	説明
-u	<user>	データソースとして使用するBrokerまたはConcentratorの認証情報(ユーザ名)。
-p	<password>	データソースとして使用するBrokerまたはConcentratorの認証情報(パスワード)。パスワードで使用できるのは次の特殊文字です。 !"#\$%&()*+,-.:;<=>?@[\\]^_`{ } 特殊文字を使用する場合は、アポストロフでパスワードを囲む必要があります。例: sh /opt/rsa/saTools/bin/ueba-server-config -u brokeruser -p '! "UHfz?@ExMn#\$' -h 10.64.153.104 -t 2018-08-01T00:00:00Z -s 'AUTHENTICATION FILE ACTIVE_DIRECTORY' -o broker -v
-h	<host>	データソースとして使用するBrokerまたはConcentratorのIPアドレス。現在、サポートされているデータソースは1つだけです。
-o	<type>	データソース ホスト タイプ(brokerまたはconcentrator)。
-t	<startTime>	データソースから履歴データの収集を開始する時刻(YYYY-MM-DDTHH-MM-SSZ形式。例:2018-08-15T00:00:00Z)。 <b>注:</b> このスクリプトは、入力された時刻をUTC(協定世界時)として解釈し、ローカルタイムゾーンの調整はしません。
-s	<schemas>	データスキーマ。複数のスキーマを指定する場合は、各スキーマをスペースで区切ります(例:'AUTHENTICATION FILE ACTIVE_DIRECTORY')。 <b>注:</b> 3つすべてのデータスキーマ(AUTHENTICATION、FILE、ACTIVE_DIRECTORY)を指定すれば、使用可能なWindowsログに基づいてサポートできるモデルをUEBAが調整します。
-v		冗長モード。



9. 組織のニーズに応じて、NetWitness UEBAの構成を実行します。  
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。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:トラブルシューティング

このセクションでは、インストールとアップグレードで発生する可能性のある問題の解決策について説明します。ほとんどの場合、これらの問題が発生すると、NetWitness Platformがログメッセージを出力します。

**注:** 次のトラブルシューティングの解決策で解決できないアップグレード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。


このセクションでは、次のサービス、機能、プロセスのトラブルシューティングについて記載しています。

- [CLI\(コマンド ライン インタフェース\)](#)
- [バックアップ スクリプト](#)
- [Event Stream Analysis](#)
- [Log Collectorサービス\(nwlogcollector\)](#)
- [Orchestration](#)
- [NW Server](#)
- [Reporting Engine](#)
- [NetWitness UEBA](#)

## CLI(コマンド ライン インタフェース)

エラー メッセ ージ	CLI(コマンド ライン インタフェース)に、「Orchestration failed.」と表示される。 Mixlib::ShellOut::ShellCommandFailed: Command execution failed. STDOUT/STDERR suppressed for sensitive resource in/var/log/netwitness/config-management/chef-solo.log
原因	nwsetup-tuiで間違ったdeploy_adminのパスワードを指定しました。
解決策	<p>deploy_adminのパスワードを取得します。</p> <ol style="list-style-type: none"> <li>SSHでNW Serverホストに接続し、次のコマンドを実行します。  <pre>security-cli-client --get-config-prop --prop-hierarchy nw.security- client --prop-name deployment.password</pre>           SSHで失敗したホストに接続します。</li> <li>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。</li> </ol>

エラー メッセ ージ	ERROR com.rsa.smc.sa.admin.web.controller.ajax.health. AlarmsController - Cannot connect to System Management Service
原因	アップグレードの完了後、SMS( Service Management Service) が実行されているにもかかわらず、NetWitness Platformはこのサービスがダウンしていると認識します。
解決策	SMSサービスを再起動します。 systemctl restart rsa-sms

エラー メッセ ージ	<p>ホストをオフラインで更新してリポートした後に、ユーザ インタフェースにホストをリポートするようメッセージが表示されます。</p> 
原因	CLIを使用してホストをリポ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。
解決策	ユーザ インタフェースの[ホスト]ビューでホストをリポートします。

## バックアップ(`nw-backup`スクリプト)

エラーメッセージ	WARNING: Incorrect ESA Mongo admin password for host <hostname>.
原因	ESA MongoDB adminのパスワードに特殊文字が含まれています(「!@#\$\$%^」など)。
解決策	バックアップを実行する前に、ESA MongoDB adminのパスワードをデフォルトの「netwitness」に変更します。

エラー	immutable属性の設定が原因でバックアップエラーが発生します。表示されるエラーの例を示します。 <pre>Backing up NetWitness Config (/etc/netwitness) files from: saserver1 WARNING: Errors occurred while backing up NetWitness Configuration files. Verify contents of saserver1-192.168.2.102-etc-netwitness.tar.gz Located in /var/netwitness/database/nw-backup/2018-03-01/saserver1-192.168.2.102-backup.tar.gz Backing up SA UI Web Server (/var/lib/netwitness/uax) files from: saserver1</pre>
原因	immutable(変更不可)フラグが設定されたファイルがある場合(例えば、Puppetプロセスがカスタマイズしたファイルを上書きしないようにするため)、バックアップにはそのファイルが含まれず、エラーが生成されます。
解決策	immutableフラグが設定されたファイルが存在するホストで、次のコマンドを実行し、ファイルのimmutableフラグを削除します。 <code>chattr -i &lt;filename&gt;</code>

エラー	<p>Error creating Network Configuration Information file due to duplicate or bad entries in primary network configuration file: /etc/sysconfig/network-scripts/ifcfg-em1</p> <p>Verify contents of /var/netwitness/logdecoder/packetdb/nw-backup/2018-02-23/S5-BROK-36-10.25.53.36-network.info.txt</p>
原因	<p>次のいずれかのフィールドで、不正または重複したエントリーがあります: DEVICE、BOOTPROTO、IPADDR、NETMASK、GATEWAY。このエラーは、バックアップされるホストのプライマリEthernetインタフェース構成ファイルの読み取り時に検出されたものです。</p>
解決策	<p>外部バックアップ サーバのバックアップ場所、およびホスト上のローカルなバックアップ場所(この場所には他のバックアップがステージングされています)に、ファイルを手動で作成します。ファイル名の形式は&lt;hostname&gt;-&lt;hostip&gt;-network.info.txtで、次のエントリーを含める必要があります。</p> <pre>DEVICE=&lt;devicename&gt; ; # from the host's primary ethernet interface config file BOOTPROTO=&lt;bootprotocol&gt; ; # from the host's primary ethernet interface config file IPADDR=&lt;value&gt; ; # from the host's primary ethernet interface config file NETMASK=&lt;value&gt; ; # from the host's primary ethernet interface config file GATEWAY=&lt;value&gt; ; # from the host's primary ethernet interface config file search &lt;value&gt; ; # from the host's /etc/resolv.conf file nameserver &lt;value&gt; ; # from the host's /etc/resolv.conf file</pre>

## Event Stream Analysis

問題	FIPSが有効化された構成で11.2.0.0にアップグレードした後、ESA サービスがクラッシュします。
原因	ESA サービスが、無効なキーストアを参照しています。
解決策	<ol style="list-style-type: none"><li>1. ESAプライマリホストにSSHで接続し、ログインします。</li><li>2. /opt/rsa/esa/conf/wrapper.confファイル内の次の行を変更します。 wrapper.java.additional.5=- Djavax.net.ssl.keyStore=/opt/rsa/esa/../carlos/keystore 変更後: wrapper.java.additional.5=- Djavax.net.ssl.keyStore=/opt/rsa/carlos/keystore</li><li>3. 次のコマンドを実行し、ESAを再起動します。 systemctl restart rsa-nw-esa-server</li></ol> <p>注: 複数のESAホストがあり、同じ問題が発生する場合は、各ESAセカンダリホストでステップ1から3を繰り返します。</p>

## Log Collectorサービス(`nwlogcollector`)

Log Collectorのログは、`nwlogcollector` サービスを実行しているホスト上の `/var/log/install/nwlogcollector_install.log`に保存されます。

エラーメッセージ	<code>&lt;timestamp&gt;.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.</code>
原因	更新後、Log CollectorのLockboxを開くことができませんでした。
解決策	NetWitness Platformにログインし、LockboxのStable System Valueをリセットすることにより、システムフィンガープリントをリセットします。詳細については、「ログ収集の構成ガイド」の「Lockboxのセキュリティ設定の構成」トピックにある「Stable System Valueのリセット」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、「 <a href="#">マスター目次</a> 」で確認できます。

エラーメッセージ	<code>&lt;timestamp&gt; NwLogCollector_PostInstall: Lockbox Status : Not Found</code>
原因	更新後、Log CollectorのLockboxが構成されていません。
解決策	Log CollectorのLockboxを使用する場合は、NetWitness Platformにログインし、Lockboxを構成します。詳細については、『ログ収集の構成ガイド』の「Lockboxのセキュリティ設定の構成」トピック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、「 <a href="#">マスター目次</a> 」で確認できます。。

エラーメッセージ	<timestamp>: NwLogCollector_PostInstall: Lockbox Status : Lockbox maintenance required: The lockbox stable value threshold requires resetting. To reset the system fingerprint, select Reset Stable System Value on the settings page of the Log Collector.
原因	Log CollectorのLockboxのStable System Value閾値フィールドをリセットする必要があります。
解決策	NetWitness Platformにログインし、LockboxのStable System Valueをリセットします。詳細については、「ログ収集の構成ガイド」の「Lockboxのセキュリティ設定の構成」トピックにある「Stable System Valueのリセット」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、「 <a href="#">マスター目次</a> 」で確認できます。
問題	Log Collectorのアップグレードを準備していましたが、現時点ではアップグレードしないことにしました。
原因	アップグレードの遅延。
解決策	次のコマンドを実行して、アップグレードの準備をしていたLog Collectorを元の状態に戻し、通常の運用を再開します。 <pre># /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --revert</pre>



## NW Server

これらのログは、NW Serverホスト上の`/var/netwitness/uax/logs/sa.log`に書き込まれます。

問題	アップグレード後、監査ログが、グローバル監査に設定された宛先に転送されていないことが分かりました。 または 次のメッセージが <code>sa.log</code> に記録されました。 <code>Syslog Configuration migration failed. Restart jetty service to fix this issue</code>
原因	NW Serverのグローバル監査設定は、10.6.6.xから11.2.0.0への移行に失敗しました。
解決策	<ol style="list-style-type: none"> <li>SSHでNW Serverに接続します。</li> <li>次のコマンドを実行します。 <code>orchestration-cli-client --update-admin-node</code></li> </ol>

## Orchestration

Orchestration Serverのログは、NW Serverホスト上の`/var/log/netwitness/orchestration-server/orchestration-server.log`に書き込まれます。

問題	<ol style="list-style-type: none"> <li>非NW Serverホストをアップグレードしようとしたますが、失敗しました。</li> <li>このホストのアップグレードを再試行しましたが、再度失敗しました。</li> </ol> <p><code>orchestration-server.log</code>に次のメッセージが記録されます。 <code>''file' _virtual_ returned False: cannot import name HASHES''</code></p>
原因	失敗した非NW Serverホストでsalt minionがアップグレードされ、再起動されていない可能性があります。
解決策	<ol style="list-style-type: none"> <li>アップグレードに失敗した非NW ServerホストにSSHで接続します。</li> <li>次のコマンドを実行します。 <code>systemctl unmask salt-minion</code> <code>systemctl restart salt-minion</code></li> <li>非NW Serverホストのアップグレードを再試行します。</li> </ol>

## Reporting Engineサービス

Reporting Engineの更新ログは、Reporting Engineを実行しているホスト上の/var/log/re\_install.logファイルに保存されます。

エラーメッセージ	<timestamp> : Available free space in /var/netwitness/re-server/rsa/soc/reporting-engine [ ><existing-GB ] is less than the required space [ <required-GB> ]
原因	Reporting Engineの更新は、十分なディスク領域がないために失敗しました。
解決策	ログメッセージに示されている必要な容量に合わせてディスク領域を解放します。ディスク領域を解放する方法については、「 <i>Reporting Engine構成ガイド</i> 」の「サイズの大きなレポートに対応するためのスペースの追加」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、「 <a href="#">マスター目次</a> 」で確認できます。

## NetWitness UEBA

問題	ユーザ インタフェースにアクセスできません。
原因	NetWitness導入環境に複数のNetWitness UEBAサービスが存在しています(1つのNetWitness UEBAサービスしか導入できません)。
解決策	<p>余分なNetWitness UEBAサービスを削除するには、次の手順を実行します。</p> <ol style="list-style-type: none"><li>NW ServerにSSHで接続し、次のコマンドを実行して、インストールされているNetWitness UEBAサービスのリストを照会します。 <pre># orchestration-cli-client --list-services grep presidio-airflow ... Service: ID=7e682892-b913-4dee-ac84-ca2438e522bf, NAME=presidio-airflow, HOST=xxx.xxx.xxx.xxx:null, TLS=true ... Service: ID=3ba35fbe-7220-4e26-a2ad-9e14ab5e9e15, NAME=presidio-airflow, HOST=xxx.xxx.xxx.xxx:null, TLS=true</pre></li><li>サービスのリストから、ホストアドレスをもとに、削除するpresidio-airflowサービスを決定します</li><li>次のコマンドを実行し、Orchestrationから余分なサービスを削除します。サービスのリストに表示された、サービスIDを指定します。 <pre># orchestration-cli-client --remove-service --id &lt;ID-for-presidio-airflow-form-previous-output&gt;</pre></li><li>次のコマンドを実行し、ノード0を更新してNGINXをリストアします。 <pre># orchestration-cli-client --update-admin-node</pre></li><li>NetWitness Platformにログインし、<b>[管理]</b> &gt; <b>[ホスト]</b>に移動し、余分なNetWitness UEBAホストを削除します。</li></ol>

## 付録B: 外部リポジトリの作成

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。

1. Webサーバホストにログインします。
2. NWリポジトリ (netwitness-11.2.0.0.zip) をホストするziprepoディレクトリをWebサーバのweb-root 下に作成します。たとえば、/var/netwitnessがWebルートの場合は、次のコマンドを実行します。

```
mkdir /var/netwitness/ziprepo
```

3. 11.2.0.0 ディレクトリを/var/netwitness/ziprepoの下に作成します。

```
mkdir /var/netwitness/ziprepo/11.2.0.0
```

4. OSおよびRSAディレクトリを/var/netwitness/ziprepo/11.2.0.0の下に作成します。

```
mkdir /var/netwitness/ziprepo/11.2.0.0/OS
mkdir /var/netwitness/ziprepo/11.2.0.0/RSA
```

5. netwitness-11.2.0.0.zipファイルを/var/netwitness/ziprepo/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/ziprepo/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。
```

6. 以下のように解凍します。

- a. OS-11.2.0.0.zipを/var/netwitness/ziprepo/11.2.0.0/OSディレクトリに解凍します。

















```
unzip /var/netwitness/ziprepo/11.2.0.0/OS-11.2.0.0.zip -d
/var/netwitness/ziprepo/11.2.0.0/OS
```

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

- b. RSA-11.2.0.0.zipを/var/netwitness/ziprepo/11.2.0.0/RSAディレクトリに解凍します。

```
unzip /var/netwitness/ziprepo/11.2.0.0/RSA-11.2.0.0.zip -d
```

```
/var/netwitness/ziprepo/11.2.0.0/RSA
```

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

Repoの外部urlはhttp://<web server IP address>/ziprepoです。

7. NW 11.2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>/ziprepoと入力します。

## 改訂履歴

バージョン	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24日	<p>混乱を回避するため、インストール後のタスクのUEBA構成スクリプト コマンドを更新し、スクリプトから.sh 拡張子を削除。</p> <p>不正なコマンド:</p> <pre>./ueba-server-config.sh -u &lt;user&gt; -p &lt;password&gt; -h &lt;host&gt; -o &lt;type&gt; -t &lt;startTime&gt; -s &lt;schemas&gt; -v</pre> <p>修正後のコマンド:</p> <pre>/opt/rsa/saTools/ueba-server-config -u &lt;user&gt; -p &lt;password&gt; -h &lt;host&gt; -o &lt;type&gt; -t &lt;startTime&gt; -s &lt;schemas&gt; -v</pre>	IDD
1.2	2018年10月10日	インストール後のタスクの「タスク4: NetWitness UEBAのインストール」にいくつかの変更を加えました( <a href="#">SADOCS-1592</a> を参照)。	IDD
1.3	2018年10月11日	外部接続ストレージ構成に関するトピックを追加( <a href="#">SADOCS-1597</a> の機能拡張)。	IDD
1.4	2018年11月29日	UEBA評価ライセンスに関するメモを追加。	IDD