



仮想ホスト インストールガイド

バージョン 11.2



連絡先情報

RSA Link(<https://community.rsa.com>) では、よくある質問への回答や、既知の問題の解決方法を含むナレッジベースを公開しています。また、製品ドキュメント、コミュニティ ディスカッション、ケース管理なども公開されています。

商標

RSAの商標のリストについては、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

仮想ホスト インストールガイド	5
仮想環境での導入に関する基本情報	6
「仮想ホストインストールガイド」で使用される略語	6
サポートされる仮想ホスト	7
インストールメディア	7
仮想環境の推奨事項	7
仮想ホストの推奨システム要件	8
シナリオ1	8
シナリオ2	10
シナリオ3	13
シナリオ4	15
Legacy Windows Collectorのサイジングガイドライン	15
仮想環境でのNetWitness Platform仮想ホストのインストール	16
前提条件	16
ステップ1. 仮想ホストの導入	16
前提条件	16
手順	16
ステップ2. ネットワークの構成	20
前提条件	20
手順	20
ファイアウォールで開くポートの確認	20
ステップ3. NetWitness Platformのデータベースの構成	20
タスク1: データストアの初期構成の確認	20
PacketDBに割り当てられた初期スペース	20
初期データベース サイズ	21
PacketDBマウント ポイント	21
タスク2: 最適なデータストア スペースの構成の確認	22
仮想ドライブ スペースの使用率	23
タスク3: 新しいボリュームの追加と既存のファイルシステムの拡張	24
AdminServer	27
ESAPrimary/ESASecondary/Malware	28
LogCollector	28
LogDecoder	28
Concentrator	30

Archiver	32
Decoder	33
RSA NetWitness Platformのインストール	35
ステップ4. ホスト固有のパラメータの構成	51
仮想環境でのログ収集の構成	51
仮想環境でのパケット収集の構成	51
サードパーティの仮想タップの使用	52
ステップ5. インストール後のタスク	53
全般	53
RSA NetWitness Endpoint Insights	53
FIPSの有効化	55
NetWitness UEBA(User Entity Behavior Analytics)	55
付録A:トラブルシューティング	61
CLI(コマンドラインインタフェース)	62
バックアップ(nw-backupスクリプト)	63
Event Stream Analysis	65
Log Collectorサービス(nwlogcollector)	66
NW Server	68
Orchestration	68
Reporting Engineサービス	69
NetWitness UEBA	70
付録B:外部リポジトリの作成	71
改訂履歴	73

仮想ホスト インストールガイド

このドキュメントは、仮想環境で稼働するRSA NetWitness® Platform 11.2.0.0ホストのインストールと構成の手順を説明しています。

仮想環境での導入に関する基本情報

このトピックでは、仮想環境にRSA NetWitness Platform 11.2.0.0を導入するための一般的なガイドラインと要件について説明します。

「仮想ホスト インストールガイド」で使用される略語

略語	説明
CPU	中央処理装置
EPS	秒あたりのイベントの数
VMware ESX	エンタープライズ クラスのタイプ1ハイパーバイザー。サポート対象のバージョンは、6.5、6.0、5.5
GB	ギガバイト。1 GB = 1,000,000,000バイト
Gb	ギガビット。1 Gb = 1,000,000,000ビット。
Gbps	ギガビット/秒、つまり10億ビット/秒。光ファイバーなどの デジタル データ転送メディアの帯域幅を表します。
GHz	ギガヘルツ。1 GHz = 1,000,000,000 Hz
IOPS	1秒あたりのI/O処理数
Mbps	メガビット/秒、つまり100万ビット/秒。光ファイバーなどの デジタル データ転送メディアの帯域幅を表します。
NAS	ネットワーク接続型ストレージ
OVF	オープン仮想化形式
OVA	Open Virtual Appliance。このガイドでは、OVAは Open Virtual Hostを意味します。
RAM	ランダム アクセス メモリ(メモリとも呼ばれる)
SAN	ストレージ エリア ネットワーク
SSD/EFD HDD	ソリッド ステート ドライブ/エンタープライズ フラッシュドライブのハード ディスクドライブ
SCSI	Small Computer System Interface
SCSI(SAS)	ハード ドライブやテープドライブなどのストレージ デバイスにデータを転送するためのポイントツーポイント シリアル プロトコルです。
vCPU	仮想中央処理装置(仮想プロセッサとも呼ばれる)
vRAM	仮想ランダム アクセス メモリ(仮想メモリとも呼ばれる)
RSA NetWitness UEBA	RSA NetWitness User and Entity Behavior Analysis

サポートされる仮想ホスト

次のNetWitness Platformホストを仮想ホストとして仮想環境にインストールできます。仮想環境によって提供される機能を継承できます。

- NetWitness Server
- Event Stream Analysis: ESAプライマリとESAセカンダリ
- Archiver
- Broker
- Concentrator
- Log Decoder
- Malware Analysis
- Decoder
- Remote Log Collector
- Endpoint Hybrid
- Endpoint Log Hybrid
- UEBA(User and Entity Behavior Analysis)

次のVMwareインフラストラクチャの概念に精通している必要があります。

- VMware vCenter Server
- VMware ESXi
- 仮想マシン

VMwareの概念については、VMwareの製品ドキュメントを参照してください。

仮想ホストは、OVAとして提供されます。仮想インフラストラクチャにOVAファイルを導入し、仮想マシンを構築する必要があります。

インストールメディア

インストールメディアは、OVAパッケージの形式で提供され、Download Central (<https://download.rsasecurity.com>) からダウンロードしてインストールすることができます。製品を購入いただくと、OVAにアクセスできるようになります。

仮想環境の推奨事項

OVAパッケージによりインストールされる仮想ホストは、NetWitness Platformハードウェアホストと同じ機能を持ちます。つまり、仮想ホストを導入する際に、バックエンドハードウェアを考慮する必要があります。RSAでは、仮想環境の設定時に、次のタスクを実行することを推奨します。

- さまざまなコンポーネントのリソース要件に基づき、ベスト プラクティスに沿ったシステムおよび専用のストレージを適切に導入します。
- バックエンドのディスクは、導入環境に必要な収集レートよりも一貫して10%以上高速な書き込み速度を達成できるよう構成します。
- Concentratorのメタ データベースとインデックス データベースのディレクトリは、SSD/EFD HDD上に構築します。
- データベース コンポーネントがOS(オペレーティング システム) コンポーネントから独立している(つまり、独立した物理システム上にある) 場合、次のいずれかの直接接続を使用します。
 - 仮想ホストごとに2つの8 Gbpsファイバー チャネルを使用したSAN
または
 - 6 Gbpsシリアル アタッチSCSI(SAS)

注: 1.) 現時点では、NetWitness Platformは仮想環境でのNASの使用をサポートしません。
2.) Decoderでは、継続的スループット要件を満たしていれば、どのようなストレージ構成でもかまいません。SANへの標準の8 Gbpsファイバー チャネルリンクは、10 Gbでのパケット データの読み書きには不十分です。10G DecoderをSANに接続する場合は、複数のファイバー チャネルを使用する必要があります。

仮想ホストの推奨システム要件

次の表は、EPSレート(ログ)または収集レート(パケット)に基づき、各コンポーネントの仮想ホストのvCPU、vRAM、読み取り/書き込みIOPSの推奨要件を示しています。

- ストレージの割り当ては、「ステップ3.NetWitness Platformのデータベースの構成」で説明します。
- vRAMおよびvCPUの推奨値は、収集レート、構成、有効化されたコンテンツによって異なります。
- 推奨値は、ログについては最大25,000 EPSの取得レートで、パケットについては最大2 Gbpsの取得レートで、SSLなしでテストされています。
- 以下の表に記載されているすべてのコンポーネントのvCPUの仕様は、Intel Xeon CPU @2.59 Ghzです。
- すべてのポートは、ログでは15,000 EPSで、パケットでは1.5 Gbpsで、SSLでテストされています。

注: 新機能と拡張機能をインストールして試用する場合、前述の推奨値と異なる場合があります。

シナリオ1

これらの表の要件は、次の条件で計算されました。

- すべてのコンポーネントが統合されている。
- ログ ストリームには、Log Decoder、Concentrator、Archiverが含まれる。
- パケット ストリームには、Network DecoderとConcentratorが含まれる。

- バックグラウンド負荷には、1時間ごとのレポートと日次レポートがある。
- チャートが構成されている。

Log Decoder

EPS	CPU	メモリ	読み取りIOPS	書き込みIOPS
2,500	6個または15.60 GHz	32 GB	50	75
5,000	8個または20.79 GHz	32 GB	100	100
7,500	10個または25.99 GHz	32 GB	150	150

Network Decoder

Mbps	CPU	メモリ	読み取りIOPS	書き込みIOPS
50	4個または10.39 GHz	32 GB	50	150
100	4個または10.39 GHz	32 GB	50	250
250	4個または10.39 GHz	32 GB	50	350

Concentrator - ログストリーム

EPS	CPU	メモリ	読み取りIOPS	書き込みIOPS
2,500	4個または10.39 GHz	32 GB	300	1,800
5,000	4個または10.39 GHz	32 GB	400	2,350
7,500	6個または15.59 GHz	32 GB	500	4,500

Concentrator - パケット ストリーム

Mbps	CPU	メモリ	読み取りIOPS	書き込みIOPS
50	4個または10.39 GHz	32 GB	50	1,350
100	4個または10.39 GHz	32 GB	100	1,700
250	4個または10.39 GHz	32 GB	150	2,100

Archiver

EPS	CPU	メモリ	読み取りIOPS	書き込みIOPS
2,500	4個または10.39 GHz	32 GB	150	250
5,000	4個または10.39 GHz	32 GB	150	250
7,500	6個または15.59 GHz	32 GB	150	350

シナリオ2

これらの表の要件は、次の条件で計算されました。

- すべてのコンポーネントが統合されている。
- ログストリームには、Log Decoder、Concentrator、Warehouse Connector、Archiverが含まれる。
- パケット ストリームには、Network Decoder、Concentrator、Warehouse Connectorが含まれる。
- Event Stream Analysisでは、90K EPSで3台のHybrid Concentratorから集計する。
- Respondは、Event Stream Analysis、Reporting Engineからアラートを受信する。
- バックグラウンド 負荷には、レポート、チャート、アラート、調査、Respondが含まれる。
- アラートが構成されている。

Log Decoder

EPS	CPU	メモリ	読み取りIOPS	書き込みIOPS
10,000	16個または41.58 GHz	50 GB	300	50
15,000	20個または51.98 GHz	60 GB	550	100

Network Decoder

Mbps	CPU	メモリ	読み取りIOPS	書き込みIOPS
500	8個または20.79 GHz	40 GB	150	200
1,000	12個または31.18 GHz	50 GB	200	400
1,500	16個または41.58 GHz	75 GB	200	500

Concentrator - ログ ストリーム

EPS	CPU	メモリ	読み取りIOPS	書き込みIOPS
10,000	10個または25.99 GHz	50 GB	1,550 + 50	6,500
15,000	12個または31.18 GHz	60 GB	1,200 + 400	7,600

Concentrator - パケット ストリーム

Mbps	CPU	メモリ	読み取りIOPS	書き込みIOPS
500	12個または31.18 GHz	50 GB	250	4,600
1,000	16個または41.58 GHz	50 GB	550	5,500
1,500	24個または62.38 GHz	75 GB	1,050	6,500

Warehouse Connector - ログ ストリーム

EPS	CPU	メモリ	読み取りIOPS	書き込みIOPS
10,000	8個または20.79 GHz	30 GB	50	50
15,000	10個または25.99 GHz	35 GB	50	50

Warehouse Connector - パケット ストリーム

Mbps	CPU	メモリ	読み取りIOPS	書き込みIOPS
500	6個または15.59 GHz	32 GB	50	50
1,000	6個または15.59 GHz	32 GB	50	50
1,500	8個または20.79 GHz	40 GB	50	50

Archiver - ログ ストリーム

EPS	CPU	メモリ	読み取りIOPS	書き込みIOPS
10,000	12個または31.18 GHz	40 GB	1,300	700
15,000	14個または36.38 GHz	45 GB	1,200	900

ESA(Event Stream Analysis) とContext Hub

EPS	CPU	メモリ	読み取りIOPS	書き込みIOPS
90,000	32個または83.16 GHz	94 GB	50	50

NWS1 : NetWitness Serverと共存コンポーネント

NetWitness Server、Jetty、Broker、Respond、Reporting Engineは同じマシンで稼働します。

CPU	メモリ	読み取りIOPS	書き込みIOPS
12個または31.18 GHz	50 GB	100	350

シナリオ3

これらの表の要件は、次の条件で計算されました。

- すべてのコンポーネントが統合されている。
- ログ ストリームには、Log DecoderとConcentratorが含まれる。
- パケット ストリームには、Network DecoderとConcentratorが含まれる。
- Event Stream Analysisでは、90K EPSで3台のHybrid Concentratorから集計する。
- Respondは、Event Stream Analysis、Reporting Engineからアラートを受信する。
- バックグラウンド負荷には、1時間ごとのレポートと日次レポートがある。
- チャートが構成されている。

Log Decoder

EPS	CPU	メモリ	読み取りIOPS	書き込みIOPS
25,000	32個または83.16 GHz	75 GB	250	150

Network Decoder

Mbps	CPU	メモリ	読み取りIOPS	書き込みIOPS
2,000	16個または41.58 GHz	75 GB	50	650

Concentrator - ログ ストリーム

EPS	CPU	メモリ	読み取りIOPS	書き込みIOPS
25,000	16個または41.58 GHz	75 GB	650	9,200

Concentrator - パケット ストリーム

Mbps	CPU	メモリ	読み取りIOPS	書き込みIOPS
2,000	24個または62.38 GHz	75 GB	150	7,050

Log Collector(ローカルおよびリモート)

リモート Log Collectorは、リモート ホストで実行されるLog Collectorサービスであり、仮想環境に導入されます。

EPS	CPU	メモリ	読み取りIOPS	書き込みIOPS
15,000	8個または20.79 GHz	8 GB	50	50
30,000	8個または20.79 GHz	15 GB	100	100

シナリオ4

これらの表の要件は、Endpoint Hybridの次の条件で計算されました。

- すべてのコンポーネントが統合されている。
- Endpoint Serverがインストールされている。
- ログストリームには、Log DecoderとConcentratorが含まれる。

Endpoint Hybrid

エージェント	CPU	メモリ	IOPS値	
5,000	16個または42 GHz	32 GB	読み取りIOPS	書き込みIOPS
			Log Decoder	250
			Concentrator	150
			MongoDB	250

Log Collector(ローカルおよびリモート)

リモートLog Collectorは、リモートホストで実行されるLog Collectorサービスであり、仮想環境に導入されます。

EPS	CPU	メモリ	読み取りIOPS	書き込みIOPS
15,000	8個または20.79 GHz	8 GB	50	50
30,000	8個または20.79 GHz	15 GB	100	100

Legacy Windows Collectorのサイジングガイドライン

Legacy Windows Collectorのサイジングのガイドラインについては、「RSA NetWitness Platform Legacy Windows 収集のアップグレードおよびインストール」を参照してください。

UEBA

CPU	メモリ	読み取りIOPS	書き込みIOPS
16個または2.4GHz	64 GB	500	500

注: RSAでは、ログ収集ボリュームが小さい場合にのみ、仮想ホストにUEBAを導入することを推奨します。RSAでは、ログ収集ボリュームが中程度以上の場合、「物理ホスト インストールガイド」の「RSA NetWitness UEBAホストのハードウェア仕様」で説明されている物理ホストにUEBAを導入することを推奨します。UEBAに使用するホスト(仮想または物理)を選択する際のアドバイスについては、カスタマーサポート (support@rsa.com) にお問い合わせください。

仮想環境でのNetWitness Platform仮想ホストのインストール

仮想環境にRSA NetWitness® Platformをインストールするには、次の手順を順番に沿って実行します。

前提条件

以下の項目について確認します。

- 前セクションに記載された要件を満たすVMware ESX Serverを使用する必要があります。サポートされるVMware ESX Serverのバージョンは、6.5、6.0、5.5です。
- VMware ESX ServerにログオンするためのvSphere 4.1 Client、vSphere 5.0 Client、vSphere 6.0 Clientのいずれかが必要です。
- VMware ESX Server上で仮想マシンを作成するための管理者権限が必要です。

ステップ1. 仮想ホストの導入

vSphereクライアントを使用してvCenter ServerまたはVMware ESX Server上にOVAファイルを導入するには、次のステップを実行します。

前提条件

以下の項目について確認します。

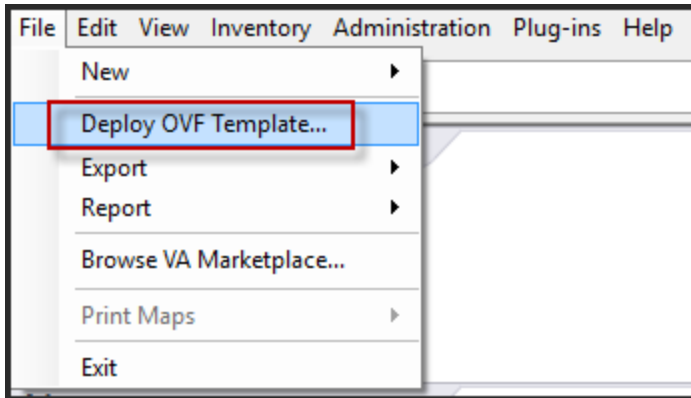
- 仮想ホストのネットワークIPアドレス、ネットマスク、ゲートウェイIPアドレス。
- クラスターを作成する場合は、すべての仮想ホストのネットワーク名。
- DNSまたはホスト情報。
- 仮想ホストにアクセスするパスワード。デフォルトのユーザー名はrootで、デフォルトのパスワードはnetwitnessです。
- NetWitness Platform仮想ホスト パッケージ ファイル(たとえば、rsanw-11.2.0.xxxx.el7-x86_64.ova)。(このパッケージは、Download Central(<https://community.rsa.com>) からダウンロードしてください)。

手順

注: 次の手順は、ESXi環境でOVAホストを導入する例です。表示される画面は、この例とは異なる場合があります。

OVAホストを導入するには、次の手順を実行します。

1. VMware ESXi環境にログオンします。
2. [ファイル]ドロップダウンで、[OVFテンプレートのデプロイ]を選択します。



3. [OVFテンプレートのデプロイ]ダイアログが表示されます。[OVFテンプレートのデプロイ]ダイアログで、仮想環境に導入するホストのOVF(例: V11.2 GOLD\\rsanw-11.2.0.0.1948.el7-x86_64.ova)を

選択し、[次へ]をクリックします。

Deploy OVF Template

Source
Select the source location.

Source
OVF Template Details
Name and Location
Storage
Disk Format
Ready to Complete

Deploy from a file or URL

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

- ダイアログに従って進むと、[名前と場所]のダイアログが表示されます。指定した名前は、サーバのホスト名には反映されません。ESXiでインベントリを参照する時に使用されます。
- この名前を記録し、[次へ]をクリックします。
さらにダイアログを進むと、ストレージ オプションが表示されます。

Storage
Where do you want to store the virtual machine files?

Select a destination storage for the virtual machine files:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Pr
datastore1	Non-SSD	144.00 GB	3.74 GB	140.26 GB	VMFS5	Support
datastore2	Non-SSD	18.18 TB	15.87 TB	7.84 TB	VMFS5	Support

Source
[OVF Template Details](#)
[End User License Agreement](#)
[Name and Location](#)
Storage
Disk Format
Network Mapping
Ready to Complete

6. ストレージ オプションで、仮想ホストのデータストアの場所を指定します。

注:この場所は、ホストOS(オペレーティングシステム)専用です。NetWitness Platformデータベース用の追加ボリュームをセットアップおよび構成する場合に、同じデータストアを使用する必要はありません(次のセクションで説明します)。

7. [次へ]をクリックします。
ネットワーク マッピングのオプションが表示されます。

Network Mapping

What networks should the deployed template use?

Source Networks	Destination Networks
Network 1	VM Network

Description:
The Network 1 network

8. デフォルト値をそのまま使用して、[次へ]をクリックします。

注:ここでネットワーク マッピングを構成することもできますが、RSAではデフォルト値をそのまま使用し、OVAの構成後にネットワーク マッピングを構成することを推奨します。OVAの構成は「[ステップ4: ホスト固有のパラメータの構成](#)」で行います。

デプロイ ステータスを示すステータス ウィンドウが表示されます。

7% Deploying rsanw-...

Deploying rsanw-...

Deploying disk 1 of 1

☒ Close this dialog when completed

Cancel

デプロイが完了すると、vSphere内のVMware ESXi上の指定されたリソース プールに新しい仮想アプライアンスが表示されます。この時点で、コア仮想ホストはインストールされていますが、まだ構成されていません。

ステップ2. ネットワークの構成

仮想アプライアンスのネットワークを構成するには、次のステップを実行します。

前提条件

以下の項目について確認します。

- 仮想ホストのネットワークIPアドレス、ネットマスク、ゲートウェイIPアドレス。
- クラスターを作成する場合は、すべての仮想ホストのネットワーク名。
- DNSまたはホスト情報。

手順

すべての仮想ホストをネットワーク上に導入するには、以下のステップを実行します。

ファイアウォールで開くポートの確認

NetWitness Platformヘルプの「[導入ガイド](#)」にある「[ネットワークアーキテクチャとポート](#)」トピックの内容を確認して、NetWitness Platformサービスとファイアウォールを構成します。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。

ステップ3. NetWitness Platformのデータベースの構成

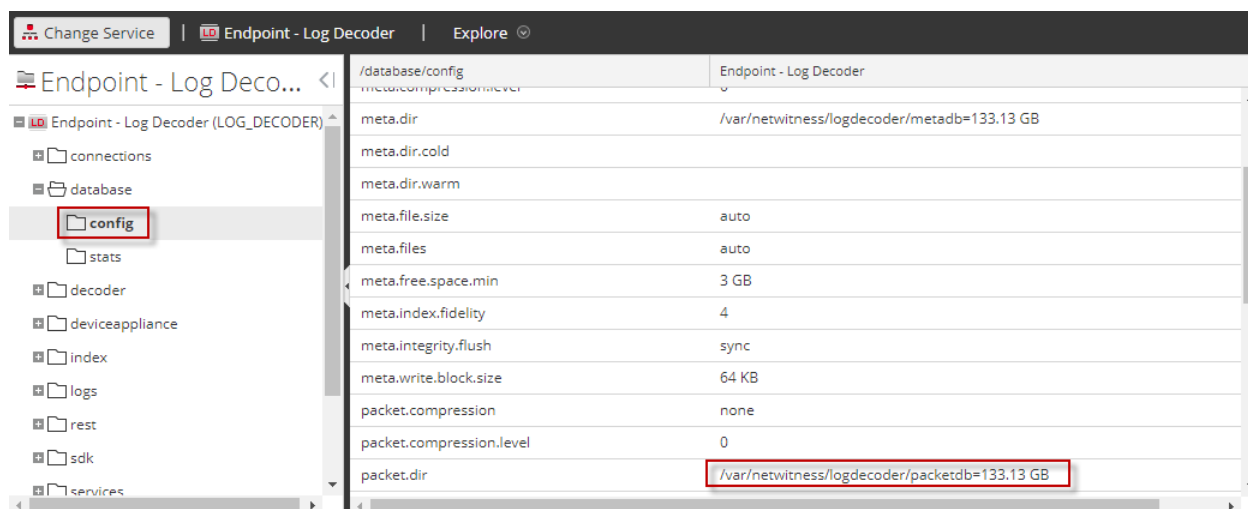
OVAからデータベースを導入する場合、初期データベース領域の割り当てではNetWitness Serverに十分に対応できない可能性があります。初期導入後、データストアのステータスを確認し、拡張する必要があります。

タスク1: データストアの初期構成の確認

エンタープライズのニーズに対応するための十分なドライブスペースがあるかどうかを確認するために、初期導入後にデータストアの構成を確認します。このトピックでは、例として、OVA(Open Virtualization Archive) ファイルから導入した後、Log DecoderホストのPacketDBのデータストア構成を確認します。

PacketDBに割り当てられた初期スペース

PacketDBに割り当てられたスペースは約133.13 GBです。次のNetWitness Platformの[エクスプローラ]ビューの例では、OVAから導入した直後のPacketDBのサイズを示しています。



初期データベース サイズ

デフォルトでは、データベースのサイズは、データベースが格納されているファイルシステム サイズの95%に設定されます。Log DecoderホストにSSHでログインし、`df -k`コマンドを実行して、ファイルシステムとそのサイズを表示します。コマンドの出力として、次のような情報が表示されます。

```
[root@LogDecoder ~]# df -kh
Filesystem                                Size  Used Avail Use% Mounted on
/dev/mapper/netwitness_vg00-root          30G   3.0G   27G  10% /
devtmpfs                                 16G    0    16G   0% /dev
tmpfs                                     16G   12K    16G   1% /dev/shm
tmpfs                                     16G   25M    16G   1% /run
tmpfs                                     16G    0    16G   0% /sys/fs/cgroup
/dev/mapper/netwitness_vg00-usrhome       10G   33M    10G   1% /home
/dev/mapper/netwitness_vg00-varlog        10G   42M    10G   1% /var/log
/dev/mapper/netwitness_vg00-nwhome       141G  396M   140G   1% /var/netwitness
/dev/sda1                                1014M   73M   942M   8% /boot
tmpfs                                     3.2G    0    3.2G   0% /run/user/0
[root@LogDecoder ~]#
```

PacketDB マウント ポイント

データベースは、`netwitness_vg00` ボリューム グループの `packetdb` 論理 ボリューム にマウントされています。`netwitness_vg00` が、ファイル システム を拡張 する計画の出発点です。

netwitness_vg00の初期状態

`netwitness_vg00` のステータスを確認するには、以下の手順に従ってください。

1. Log DecoderホストにSSHでログインします。
2. `lvs` (Logical Volumes Show) コマンドを実行し、`netwitness_vg00` でグループ化された論理ボリュームを表示します。

```
[root@nwappliance32431 ~]# lvs netwitness_vg00.
```

コマンドの出力として、次のような情報が表示されます。

```
[root@LogDecoder ~]# vgs
VG                #PV #LV #SN Attr   VSize   VFree
netwitness_vg00   1    5  0 wz--n- <194.31g 100.00m
```

3. pvs(Physical Volumes Show) コマンドを実行し、特定のグループに含まれる物理ボリュームを表示します。

```
[root@nwapplance32431 ~]# pvs
```

コマンドの出力として、次のような情報が表示されます。

```
[root@LogDecoder ~]# pvs
PV                VG                Fmt  Attr PSize   PFree
/dev/sda2         netwitness_vg00   lvm2 a--  <194.31g 100.00m
```

4. vgs(Volume Groups Show) コマンドを実行し、特定のボリューム グループの合計サイズを表示します。

```
[root@nwapplance32431 ~]# vgs
```

コマンドの出力として、次のような情報が表示されます。

```
[root@LogDecoder ~]# vgs
VG                #PV #LV #SN Attr   VSize   VFree
netwitness_vg00   1    5  0 wz--n- <194.31g 100.00m
```

タスク2: 最適なデータストアスペースの構成の確認

仮想NetWitness Platform導入環境全体で最適なパフォーマンスを実現するには、様々なホストのデータストアスペース構成オプションを確認する必要があります。データストアは仮想ホストの構成に必要であり、適切なサイズはホストによって異なります。

注: (1) データストアスペースの最適化に関する推奨については、「[RSA NetWitness Platform コア データベース チューニング ガイド](#)」の「最適化の手法」を参照してください。(2) 仮想ドライブの構成およびSizing & Scoping Calculatorの使用に関するサポートについては、カスタマー サポートにお問い合わせください。

仮想ドライブ スペースの使用率

次の表に、パケットとログの各ホストについて、最適なディスク構成を示します。このトピックの末尾に、パケットおよびログ収集の両環境について、パーティション分割およびサイズ設定の例を示します。

Decoder			
永続 データストア	キャッシュ データストア		
PacketDB	SessionDB	MetaDB	Index
Sizing & Scoping Calculatorで計算された値の100%	100 Mb/秒の持続トラフィックの場合、6 GBで4時間のキャッシュ	100 Mb/秒の持続トラフィックの場合、60 GBで4時間のキャッシュ	100 Mb/秒の持続トラフィックの場合、3 GBで4時間のキャッシュ

Concentrator		
永続 データ ストア	キャッシュ データストア	
MetaDB	SessionDB Index	Index
PacketDBの10%として計算 1:1の保存比率に必要	一般的なインターネット ゲートウェイで見られる標準的なマルチ プロトコル ネットワーク環境で、1 TBのPacketDBについて30 GB	ConcentratorのMetaDBの計算値の5%。高速アクセスのために高速なスピンドルまたはSSDを推奨

Log Decoder			
永続 データストア	キャッシュ データストア		
PacketDB	SessionDB	MetaDB	Index
Sizing & Scoping Calculatorで計算された値の100%	1,000 EPSの持続トラフィックの場合、1 GBで8時間のキャッシュ	1,000 EPSの持続トラフィックの場合、20 GBで8時間のキャッシュ	1,000 EPSの持続トラフィックの場合、0.5 GBで4時間のキャッシュ

Log Concentrator		
永続 データストア	キャッシュ データストア	
MetaDB	SessionDB Index	Index
PacketDBの100%として計算 1:1の保存比率に必要	保存日数ごとに1,000 EPSの持続トラフィックで3 GB	ConcentratorのMetaDBの計算値の5%。高速アクセスのために高速なスピンドルまたはSSDを推奨

タスク3: 新しいボリュームの追加と既存のファイルシステムの拡張

データストアの初期構成を確認した後、必要性があると判断した場合には新しいボリュームを追加します。このトピックでは、例として仮想Packet/Log Decoderホストを使用します。

以下の順序で作業を行います。

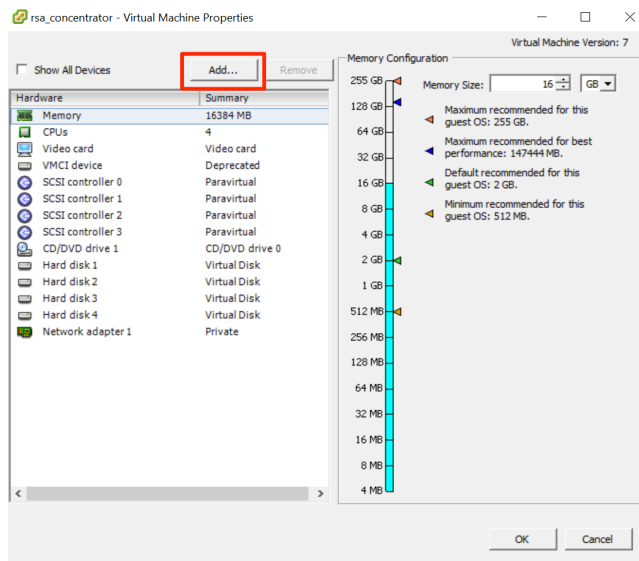
1. 新しいディスクの追加
2. 新しいディスクでの新しいボリュームの作成
3. 新しいパーティションでのLVM物理ボリュームの作成
4. 物理ボリュームによるボリューム グループの拡張
5. ファイルシステムの拡張
6. サービスの開始
7. サービスが実行されていることの確認
8. LogDecoderパラメータの再構成

新しいディスクの追加

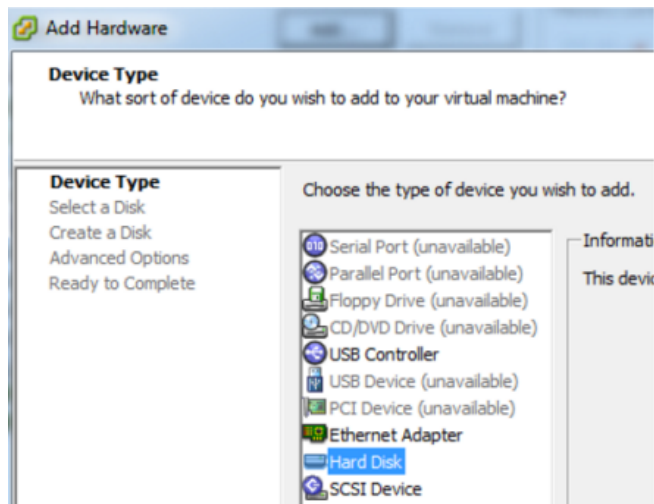
この手順では、同じデータストアに新しい100 GBのディスクを追加する方法を示します。

注: 別のデータストアにディスクを追加する手順は、ここに示す手順と同様です。

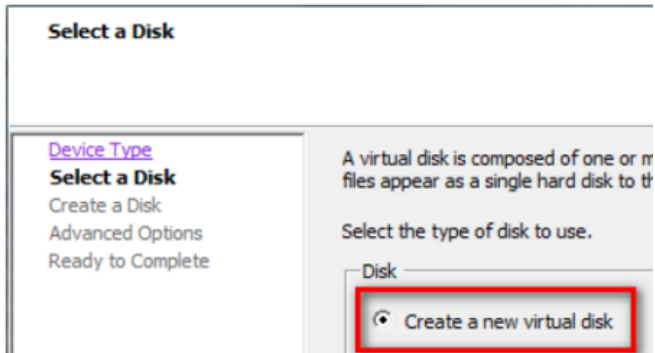
1. マシンをシャットダウンし、[仮想マシンのプロパティ]を編集します。[ハードウェア]タブをクリックし、[追加]をクリックします。



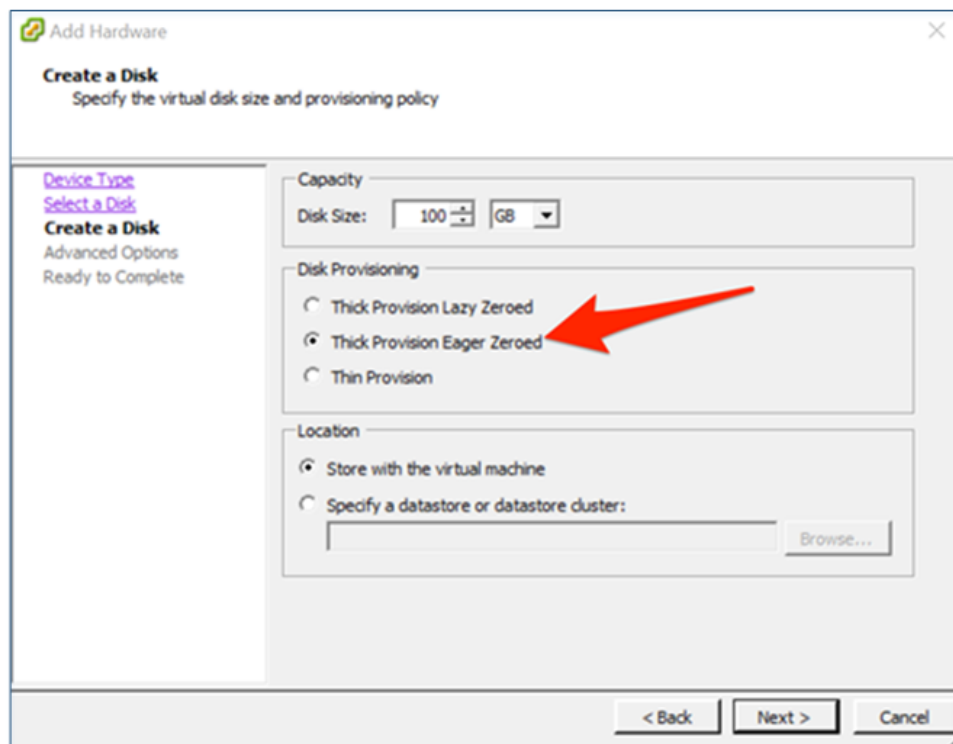
2. デバイスタイプとして、[ハード ディスク]を選択します。



3. [新規仮想ディスクを作成]を選択します。

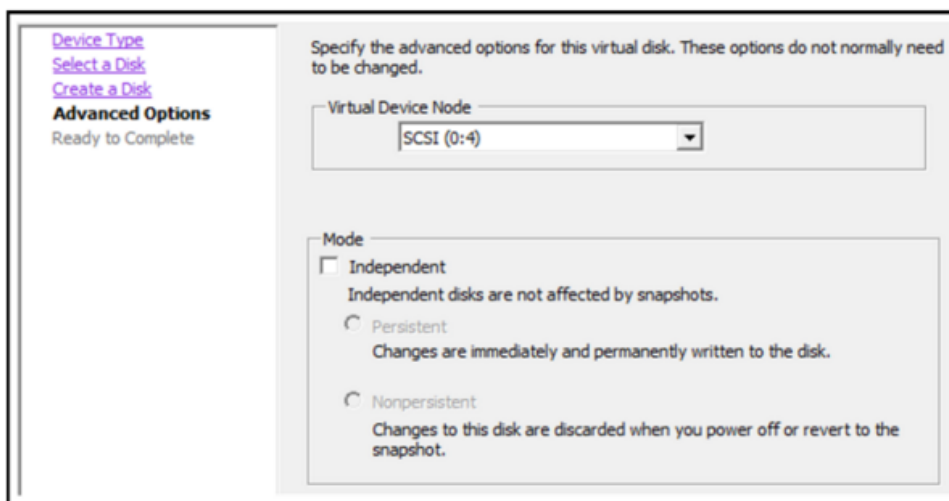


4. 新しいディスクのサイズと、新しいディスクを作成する場所 (同じデータストアまたは別のデータストア) を選択します。



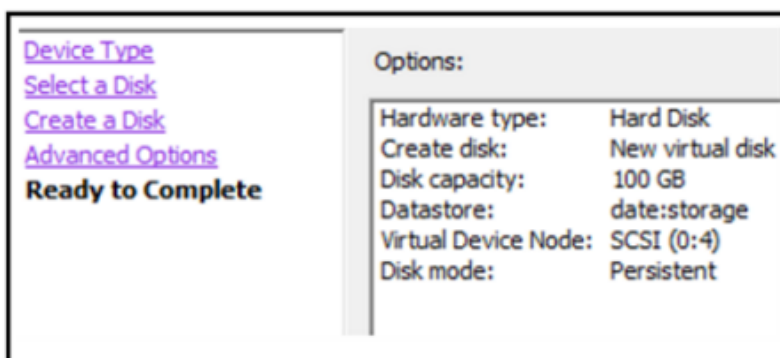
注意: パフォーマンス上の理由から、すべてのスペースを割り当てます。

5. 提案された仮想デバイスノードを承認します。



注: 仮想デバイスノードは環境によって異なりますが、適切な `/dev/sdX` にマッピングされます。

6. 設定を確認します。



Extending File Systems

Follow the instructions provides to extend the file systems for the various components.

AdminServer

Attach external disk for extension of `/var/netwitness/` (refer to the steps in attaching the disk) partition. Create an additional disk with suffix as `nwhome`.

If a single disk is attached, follow these steps:

1. Execute `lsblk` and get the physical volume name, for example if you attach one 2TB disk.
2. `pvccreate <pv_name>` . ex suppose the PV name is `/dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

RSA recommended partition for AdminServer (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness/	2TB	SSD	Read/Write

ESAPrimary/ESASSecondary/Malware

Attach external disk for extension of /var/netwitness/ partition, create an external disk with suffix as nwhome.

If a single disk is attached, follow these steps:

1. Execute `lsblk` and get the physical volume name, for example, if you attach one 6TB disk
2. `pvccreate <pv_name>` . ex suppose the PV name is /dev/sdc
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 5.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

RSA recommended partition for ESAPrimary/ESASSecondary (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness/	6TB	HDD	Read/Write

LogCollector

Attach an external disk for extension of /var/netwitness/ partition, create an external disk with suffix as nwhome.

1. Execute `lsblk` and get the physical volume name, for example if you attach one 500GB disk
2. `pvccreate <pv_name>` . ex suppose the PV name is /dev/sdc
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 600G /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

RSA recommended partition for LogCollector (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness/	500GB	HDD	Read/Write

LogDecoder

Attach an external disk for extension of /var/netwitness/ partition, create an external disk with suffix as nwhome, attach other external disks for Logdecoder database partition. For extending /var/netwitness partition follow these steps:

注: No other partition should reside on this partition, only to be used for /var/netwitness/partition

1. Execute `lsblk` and get the physical volume name, suppose if you had add attach one 2TB disk
2. `pvcreate <pv_name>` . ex suppose the PV name is `/dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

Other partitions are also required. Create the following four partitions on volume group logdecodersmall

Folder	LVM	Volume Group
/var/netwitness/logdecoder	decoroot	logdecodersmall
/var/netwitness/logdecoder/index	index	logdecodersmall
/var/netwitness/logdecoder/metadb	metadb	logdecodersmall
/var/netwitness/logdecoder/sessiondb	sessiondb	logdecodersmall

Follow these steps to create the partitions:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/sdd`
3. `vgcreate -s 32 logdecodersmall /dev/sdd`
4. `lvcreate -L <disk_size> -n <lvm_name> logdecodersmall`
5. `mkfs.xfs /dev/logdecodersmall/<lvm_name>`
6. Repeat steps 5 and 6 for all the LVM's mentioned

The following four partitions should be on volume group logdecoder and should be in single RAID 0 array

Folder	LVM	Volume Group
/var/netwitness/logdecoder/packetdb	packetdb	logdecoder

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/sde`
3. `vgcreate -s 32 logdecoder /dev/sde`
4. `lvcreate -L <disk_size> -n packetdb logdecoder`
5. `mkfs.xfs /dev/logdecoder/packetdb`

RSA recommends below sizing partition for LogDecoder (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness/	1TB	HD D	Read/Write
/dev/logdecodersmall/decoroot	/var/netwitness/logdecoder	10GB	HD D	Read/Write
/dev/logdecodersmall/index	/var/netwitness/logdecoder/index	30GB	HD D	Read/Write
/dev/logdecodersmall/metadb	/var/netwitness/logdecoder/metadb	370GB	HD D	Read/Write
/dev/logdecodersmall/sessiondb	/var/netwitness/logdecoder/sessiondb	3TB	HD D	Read/Write
/dev/logdecoder/packetdb	/var/netwitness/logdecoder/packetdb	18TB	HD D	Read/Write

Create each directory and mount the LVM on it in a serial manner, except /var/netwitness which will be already created.

注: Create the folder /var/netwitness/logdecoder and mount on /dev/logdecodersmall/decoroot then create the other folders and mount them.

After that add the below entries in /etc/fstab in the same order and mount them using mount -a.

```
/dev/logdecodersmall/decoroot /var/netwitness/logdecoder xfs noatime,nosuid 1 2
/dev/logdecodersmall/index /var/netwitness/logdecoder/index xfs noatime,nosuid 1 2
/dev/logdecodersmall/metadb /var/netwitness/logdecoder/metadb xfs noatime,nosuid 1 2
/dev/logdecodersmall/sessiondb /var/netwitness/logdecoder/sessiondb xfs noatime,nosuid 1 2
/dev/logdecoder/packetdb /var/netwitness/logdecoder/packetdb xfs noatime,nosuid 1 2
```

Concentrator

Attach external disk for extension of /var/netwitness/ partition, Create an external disk with suffix as nwhome, attach other external disks for Concentrator database partition. If there are multiple disks, create a Raid 0 array.

For extending /var/netwitness partition follow below steps:

注: No other partition should reside on this partition, only to be used for /var/netwitness/partition

1. Execute `lsblk` and get the physical volume name, for example if if you attach one 2TB disk
2. `pvcreate <pv_name>` . ex suppose the PV name is `/dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`

Below four partition are also required on volume group concentrator and should be in single RAID 0 array

Folder	LVM	Volume Group
<code>/var/netwitness/concentrator</code>	Root	Concentrator
<code>/var/netwitness/ concentrator /sessiondb</code>	index	Concentrator
<code>/var/netwitness/ concentrator /metadb</code>	metadb	Concentrator

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/md0`
3. `vgcreate -s 32 concentrator /dev/md0`
4. `lvcreate -L <disk_size> -n <lvm_name> concentrator`
5. `mkfs.xfs /dev/concentrator/<lvm_name>`
6. Repeat steps 5 and 6 for all the LVM's mentioned

Below four partitions should be on volume group index and should be in single RAID 0 array

Folder	LVM	Volume Group
<code>/var/netwitness/concentrator/index</code>	index	index

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/md1`
3. `vgcreate -s 32 index /dev/md1`
4. `lvcreate -L <disk_size> -n index index`
5. `mkfs.xfs /dev/index/index`

RSA recommends below sizing partition for Concentrator (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness/	1TB	HDD	Read/Write
/dev/concentrator/decoroot	/var/netwitness/concentrator	10GB	HDD	Read/Write
/dev/concentrator/metadb	/var/netwitness/concentrator/metadb	370GB	HDD	Read/Write
/dev/concentrator/sessiondb	/var/netwitness/concentrator/sessiondb	3TB	HDD	Read/Write
/dev/index/index	/var/netwitness/concentrator/index	2TB	SSD	Read/Write

Create each directory and mount the LVM on it in a serial manner, except `/var/netwitness` which will be already created.

注: Create the folder `/var/netwitness/concentrator` and mount on `/dev/concentrator/decoroot` then create the other folders and mount them.

After that add the below entries in `/etc/fstab` in the same order

```
/dev/concentrator/root /var/netwitness/concentrator xfs noatime,nosuid 1 2
/dev/concentrator/sessiondb /var/netwitness/concentrator/sessiondb xfs
noatime,nosuid 1 2
/dev/concentrator/metadb /var/netwitness/concentrator/metadb xfs
noatime,nosuid 1 2 2
/dev/index/index /var/netwitness/concentrator/index xfs noatime,nosuid 1 2
```

Archiver

Attach an external disk for extension of `/var/netwitness/` partition, create an external disk with suffix as `nwhome`, attach other external disks for Archiver database partition. If there are multiple disks, create a Raid 0 array.

For extending `/var/netwitness` partition follow these steps:

注: No other partition should reside on this partition, only to be used for `/var/netwitness/partition`

1. Execute `lsblk` and get the physical volume name, suppose if you had add attach one 2TB disk
2. `pvcreeate <pv_name> . ex suppose the PV name is /dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`

Below four partitions are required on volume group archiver and should be in single RAID 0 array

Folder	LVM	Volume Group
/var/netwitness/archiver	Archiver	archiver

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/md0`
3. `vgcreate -s 32 archiver /dev/md0`
4. `lvcreate -L <disk_size> -n archiver archiver`
5. `mkfs.xfs /dev/archiver/archiver`

RSA recommends below sizing partition for archiver (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness/	1TB	HDD	Read/Write
/dev/archiver/archiver	/var/netwitness/archiver	4TB	HDD	Read/Write

Create each directory and mount the LVM on it in a serial manner, except `/var/netwitness` which will be already created.

After that add the below entries in `/etc/fstab` in the same order

```
/dev/archiver/archiver /var/netwitness/archiver xfs noatime,nosuid 1 2
```

Decoder

Attach an external disk for extension of `/var/netwitness/` partition, create an external disk with suffix as `nwhome`, attach other external disks for decoder database partition. For extending `/var/netwitness` partition follow these steps:

注: No other partition should reside on this partition, only to be used for `/var/netwitness/partition`

1. Execute `lsblk` and get the physical volume name, suppose if you had add attach one 2TB disk
2. `pvcreate <pv_name>` . ex suppose the PV name is `/dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

Below four partition should be on volume group `decodersmall`

Folder	LVM	Volume Group
/var/netwitness/decoder	decoroot	decodersmall
/var/netwitness/decoder/index	index	decodersmall
/var/netwitness/decoder/metadb	metadb	decodersmall
/var/netwitness/decoder/sessiondb	sessiondb	decoersmall

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/sdd`
3. `vgcreate -s 32 logdecodersmall /dev/sdd`
4. `lvcreate -L <disk_size> -n <lvm_name> logdecodersmall`
5. `mkfs.xfs /dev/logdecodersmall/<lvm_name>`
6. Repeat steps 5 and 6 for all the LVM's mentioned

Below partition should be on volume group logdecoder and should be in single RAID 0 array

Below four partition should be on volume group logdecoder and should be in single RAID 0 array

Folder	LVM	Volume Group
/var/netwitness/logdecoder/packetdb	packetdb	decoder

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/sde`
3. `vgcreate -s 32 decoder /dev/sde`
4. `lvcreate -L <disk_size> -n packetdb decoder`
5. `mkfs.xfs /dev/decoder/packetdb`

RSA recommends below sizing partition for Decoder (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness	1TB	HDD	Read/Write
/dev/decodersmall/decoroot	/var/netwitness/decoder	10GB	HDD	Read/Write

LVM	Folder	Size	Disk Type	Caching
/dev/decodersmall/index	/var/netwitness/decoder/index	30GB	HDD	Read/Write
/dev/decodersmall/metadb	/var/netwitness/decoder/metadb	370GB	HDD	Read/Write
/dev/decodersmall/sessiondb	/var/netwitness/decoder/sessiondb	3TB	HDD	Read/Write
/dev/decoder/packetdb	/var/netwitness/decoder/packetdb	18TB	HDD	Read/Write

Create each directory and mount the LVM on it in serial manner, except /var/netwitness which will be already created.

注: Create the folder /var/netwitness/decoder and mount on /dev/decodersmall/decoroot then create the other folders and mount them.

After that add the below entries in /etc/fstab in the same order and mount them using mount -a.

```

/dev/decodersmall/decoroot /var/netwitness/decoder xfs noatime,nosuid 1 2
/dev/decodersmall/index /var/netwitness/decoder/index xfs noatime,nosuid 1 2
/dev/decodersmall/metadb /var/netwitness/decoder/metadb xfs noatime,nosuid 1 2
/dev/decodersmall/sessiondb /var/netwitness/decoder/sessiondb xfs
noatime,nosuid 1 2
/dev/decoder/packetdb /var/netwitness/decoder/packetdb xfs noatime,nosuid 1 2

```

RSA NetWitness Platformのインストール

主なタスクは2つあり、次の順序で完了してNetWitness Platform11.2をインストールします。

1. タスク1: NW(NetWitness) Serverホストに11.2.0.0をインストール
2. タスク2: その他のコンポーネントのホストに11.2.0.0をインストール

タスク1: NW Serverホストに11.2.0.0をインストール

このタスクにより、NW Serverホスト上に次の項目がインストールされます。

- 11.2.0.0 NW Serverの基盤プラットフォーム。
- NW Serverコンポーネント(つまり、Admin Server、Config Server、Orchestration Server、Integration Server、Broker、Investigate Server、Reporting Engine、Respond Server、Security Server)。
- その他のコンポーネントまたはサービスのインストールに必要なRPMファイルを保存したりポジトリ。

1. 11.2.0.0環境を導入します。
 - a. 新しいVMを追加します。
 - b. ストレージを構成します。
 - c. ファイアウォールを設定します。
2. `nwsetup-tui` コマンドを実行します。これにより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。

`nwsetup-tui` 実行中に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ため、システムは外部リポジトリに接続できません)。

```
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%

<Accept >

<Decline>

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。

```
You must setup an NW Server before setting up
any other NetWitness Platform components.
```

```
Is this the host you want for your 11.2 NW
Server?
```

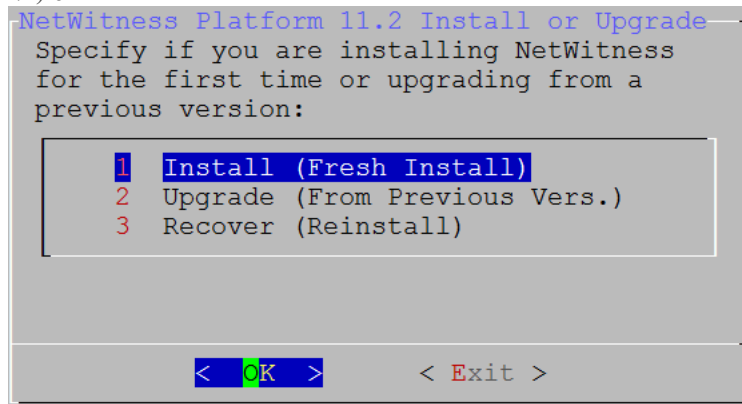
< Yes >

< No >

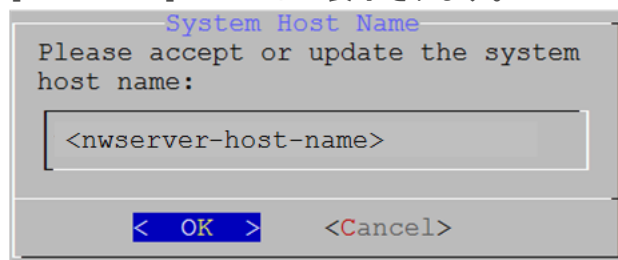
4. Tabキーで[Yes]に移動し、Enterキーを押します。

注意:間違ったホストをNW Serverとしてセットアップした場合は、セットアッププログラムを再度実行し、ステップ3以降のステップ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. 現在の名前を使用する場合は、Enterキーを押します。別の名前を使用する場合は、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。
7. [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>

8. [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 { } [] () / \ ' " ` ~ ; : . < > -

9. 下向きの矢印で[Password]に移動して入力し、下向きの矢印で[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 *****

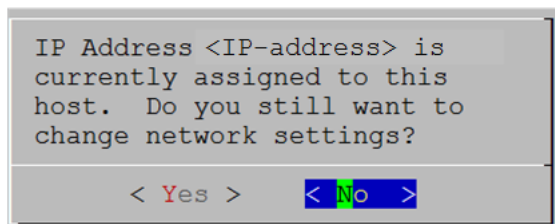
Verify *****

< OK > <Cancel>

10. [Password]に入力し、下向きの矢印で[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。

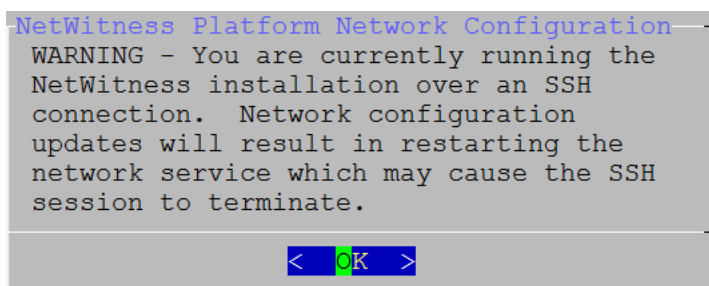
- セットアッププログラムが、このホストの有効なIPアドレスを検出すると、次のプロンプトが表示されます。



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。

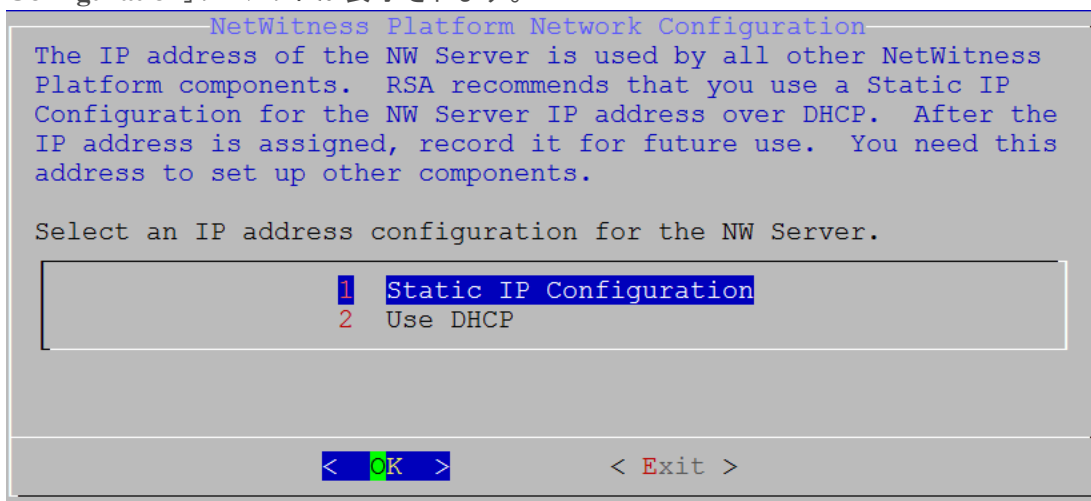
注: ホスト コンソールから直接接続している場合には、次の警告は表示されません。



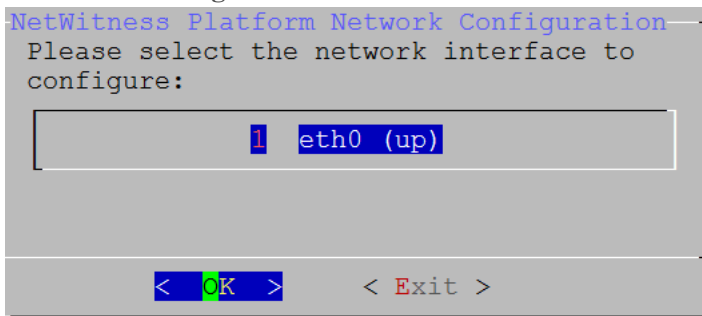
Enterキーを押して、警告プロンプトを閉じます。

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

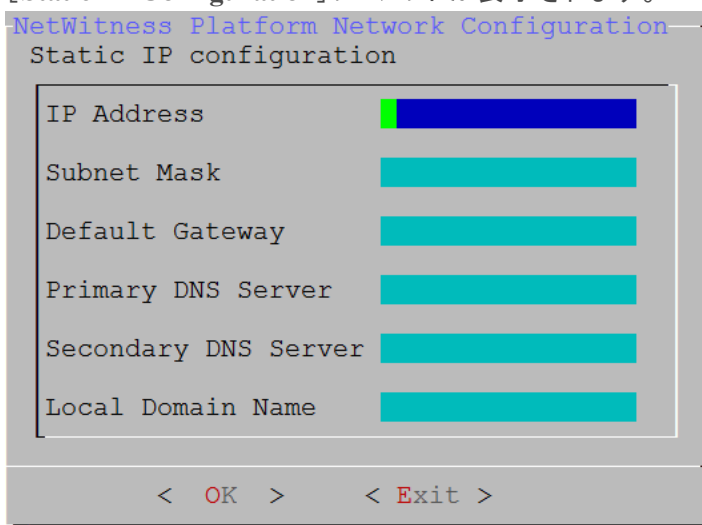
- セットアッププログラムがIPアドレスを検出し、構成をそのまま使用するように選択した場合は、[Update Repository] プロンプトが表示されます。ステップ12に移動し、インストールを完了します。
- IPアドレスが検出されなかった場合、または既存のIP構成を変更する場合は、[Network Configuration] プロンプトが表示されます。



11. 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。



12. 下向きの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。作業を続行しない場合は、Tabキーで[Exit]に移動します。
[Static IP Configuration]プロンプトが表示されます。

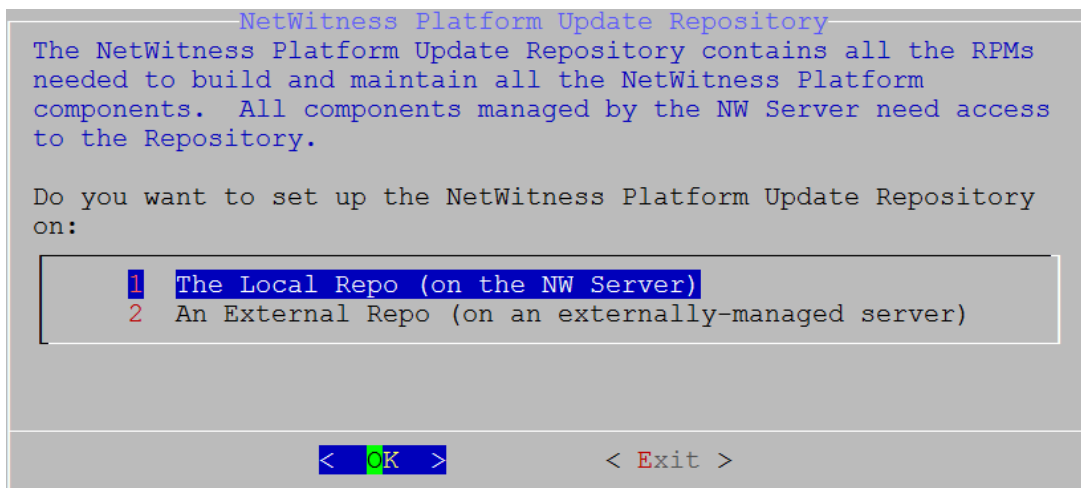


13. 値を入力し(下向き矢印を使用してフィールド間を移動)、Tabキーを使用して[OK]を選択し、Enterキーを押します。
すべての必須フィールドが入力されていないと、「All fields are required」エラーメッセージが表示されます([Secondary DNS Server]フィールドと[Local Domain Name]フィールドは必須ではありません)。
フィールドのいずれかに誤った構文や文字の長さを使用すると、「Invalid <field-name>」エラーメッセージが表示されます。

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。

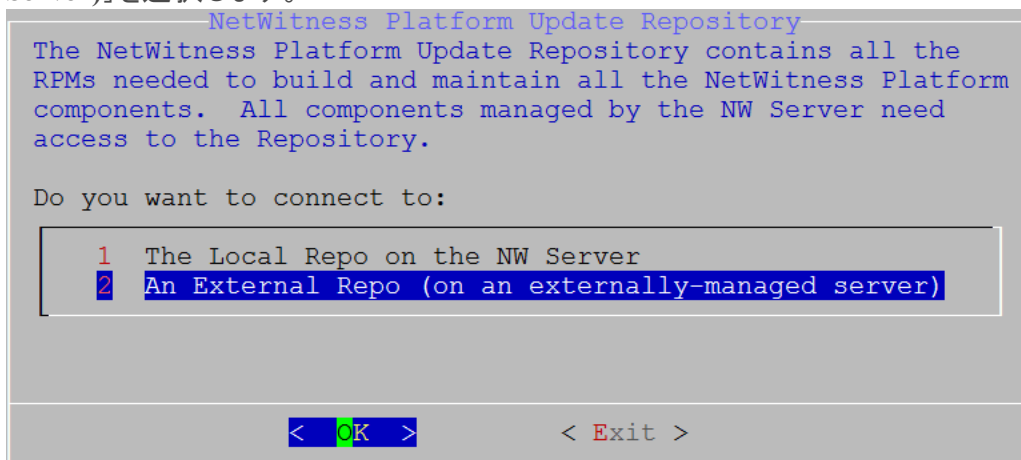
[Update Repository]プロンプトが表示されます。

14. 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時に選択したのと同じリポジトリを選択します。



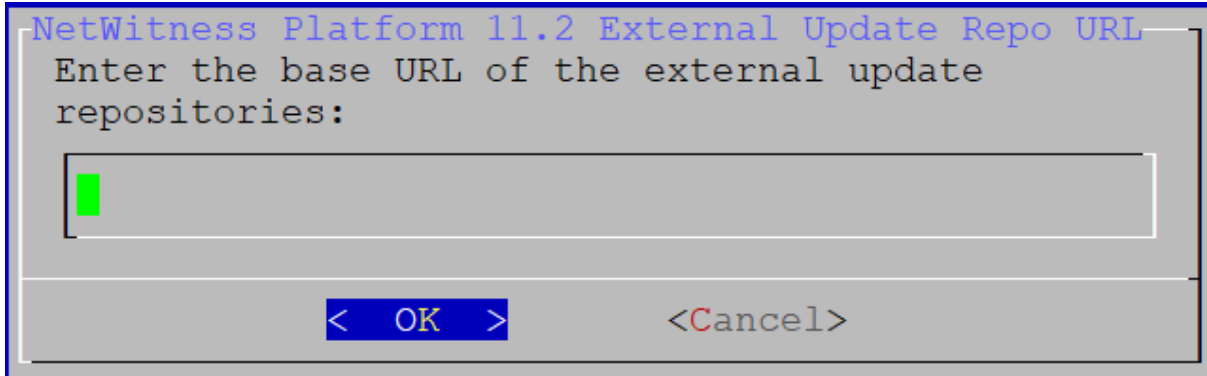
[Local Repo on the NW Server]を選択する場合は、Enterキーを押します。外部リポジトリを使用する場合は、下向き矢印を使用して[External Repo]へ移動し、Tabキーを使用して[OK]を選択し、Enterキーを押します。セットアッププログラムで[1 The Local Repo (on the NW Server)]を選択する場合、NetWitness Platform 11.2.0.0をインストールできる適切なメディア(ビルド スティックなどISOファイルを含むメディア)を接続していることを確認してください。

15. 下向き矢印と上向き矢印を使用して、[2 An External Repo (on an externally-managed Server)]を選択します。



[External Update Repo URL] プロンプトが表示されます。外部リポジトリを設定する手順については、「[付録B: 外部リポジトリの作成](#)」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。

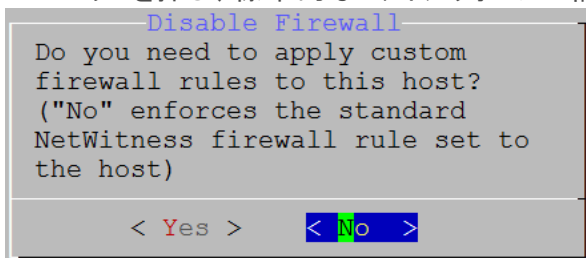
16. 「[付録B: 外部リポジトリの作成](#)」の手順に従い、NetWitness Platformの外部リポジトリのベースURL (たとえば、`http://testserver/netwitness-repo`)を入力し、[OK]をクリックします。



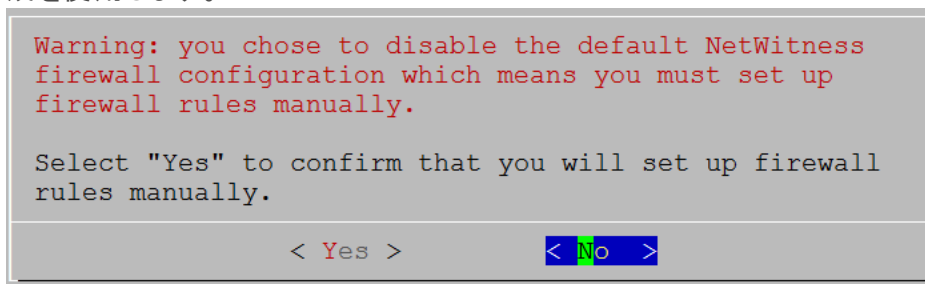
標準的なファイアウォール構成を使用するか、無効化するかを選択するプロンプトが表示されます。

17. 標準的なファイアウォールの構成を使用する場合は、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。Tabキーで[Yes]に移動し、

Enterキーを押し、標準的なファイアウォールの構成を無効化します。

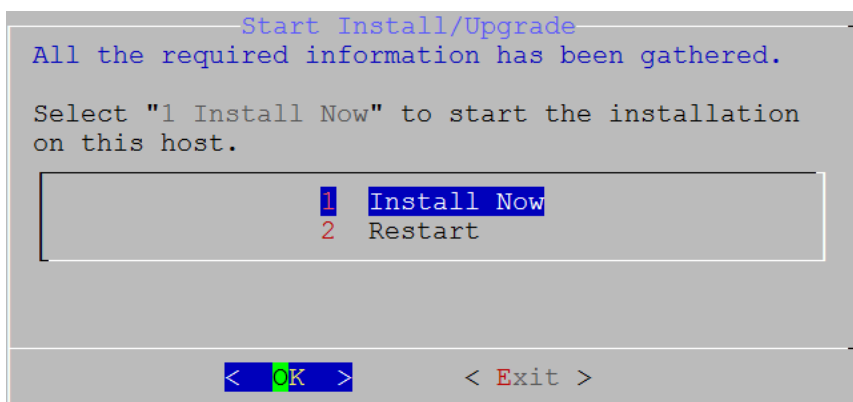


- [Yes]を選択して選択を確定するか、あるいは[No]を選択して標準的なファイアウォールの構成を使用します。



[Start Install/Upgrade] プロンプトが表示されます。

18. Enterキーを押すと、11.2.0.0がNW Serverホストにインストールされます([Install Now]がデフォルト値)。



「Installation complete」が表示されると、11.2 NW Serverのインストールが完了します。

注: `nwsetup-tui` コマンドを開始するときに表示される、次のスクリーンショットに示すようなハッシュコードのエラーは無視します。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

機能 サービスの場合、非NW Serverホストで次のタスクを実行します。

- 11.2.0.0の基盤プラットフォームのインストール。
 - NW Serverの更新リポジトリから11.2.0.0 RPMファイルをサービスに適用。
1. 11.2.0.0 OVAを導入します。
 2. `nwsetup-tui`コマンドを実行し、ホストを設定します。
これにより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` 実行中に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ため、システムは外部リポジトリに接続できません)。

```
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%

<Accept>

<Decline>

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: 間違ったホストをNW Serverとしてセットアップした場合は、セットアッププログラムを再度実行し、[タスク1: NW Serverホストに11.2.0.0をインストール](#)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。

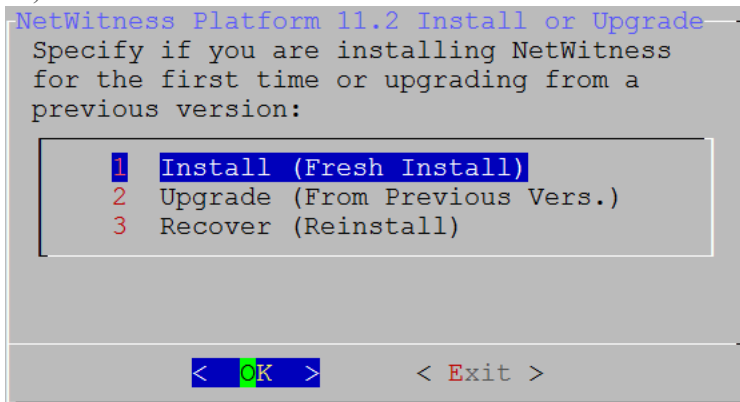
```
You must setup an NW Server before setting up
any other NetWitness Platform components.
```

```
Is this the host you want for your 11.2 NW
Server?
```

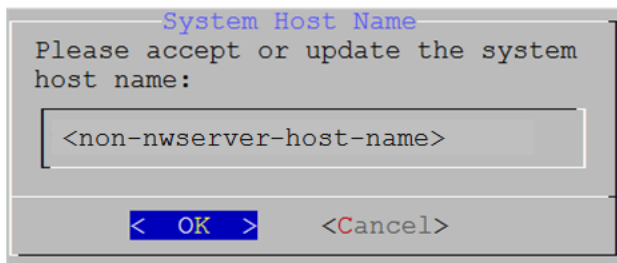
< Yes >

< No >

4. **Enter**キーを押し、[No]を選択します。
[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)。



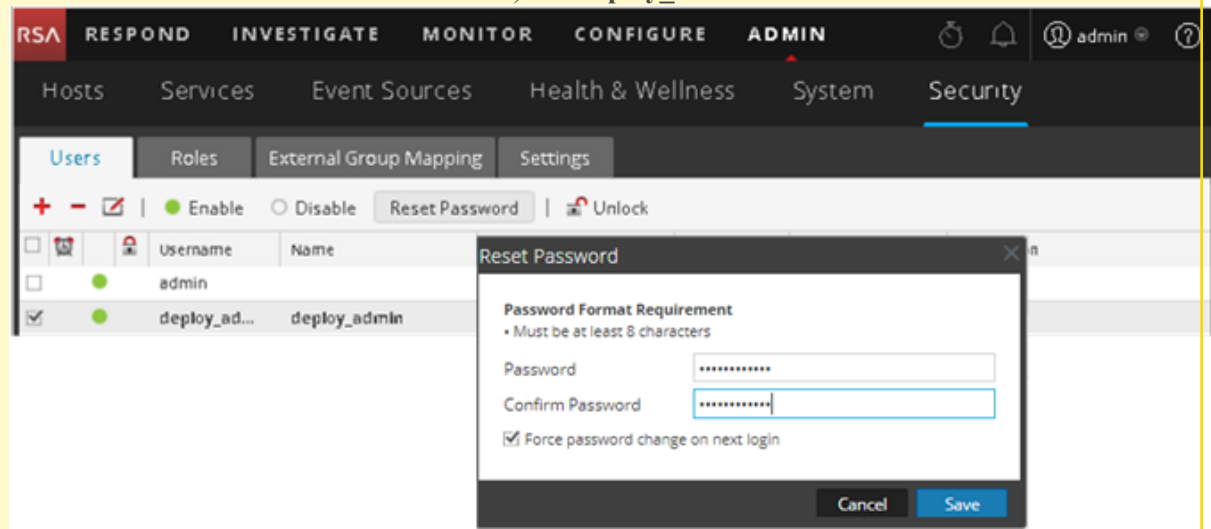
5. **Enter**キーを押します。[Install (Fresh Install)]がデフォルトで選択されています。
[Host Name]プロンプトが表示されます。



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. 現在のホスト名を使用する場合は、**Enter**キーを押します。別のホスト名を使用する場合は、ホスト名を編集して、**Tab**キーで[OK]を選択し、**Enter**キーを押します。

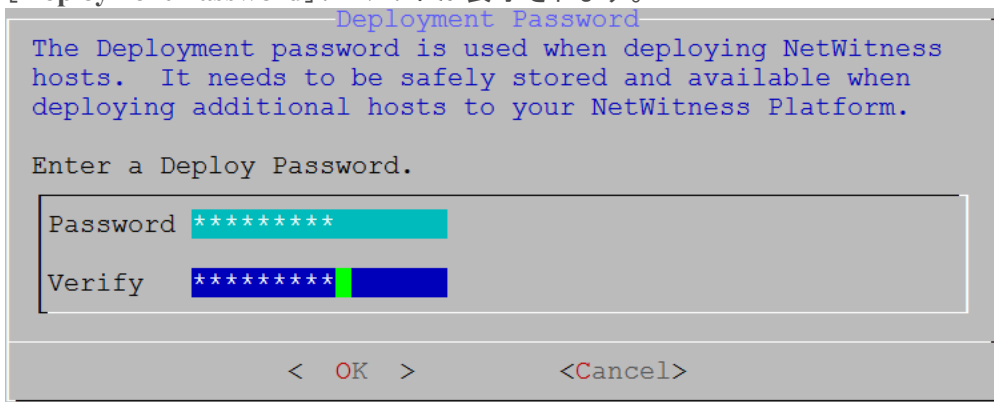
注意: NetWitness Platform ユーザー インタフェース([管理] > [セキュリティ] に進み、**deploy-admin** を選択し、[パスワードのリセット]をクリック) で、**deploy_admin** ユーザのパスワードを変更する場合



、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。

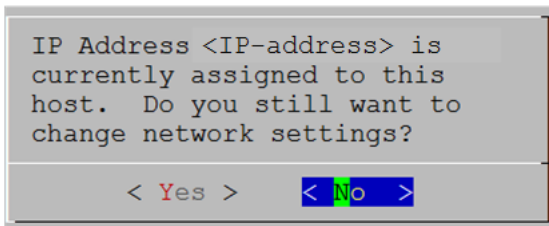


注: NW Serverのインストール時に使用したのと同じ導入パスワードを使用する必要があります。

7. [Password]に入力し、下向きの矢印で[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。

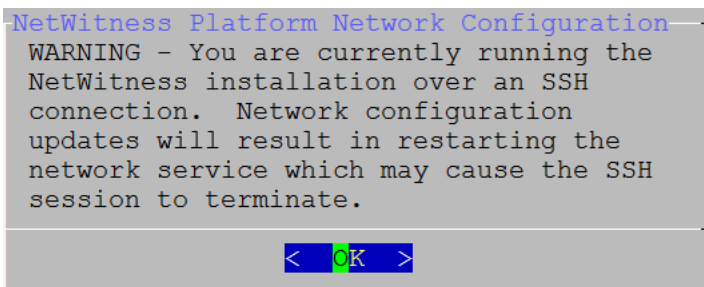
次のオプション プロンプトのいずれかが表示されます。

- 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。



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。

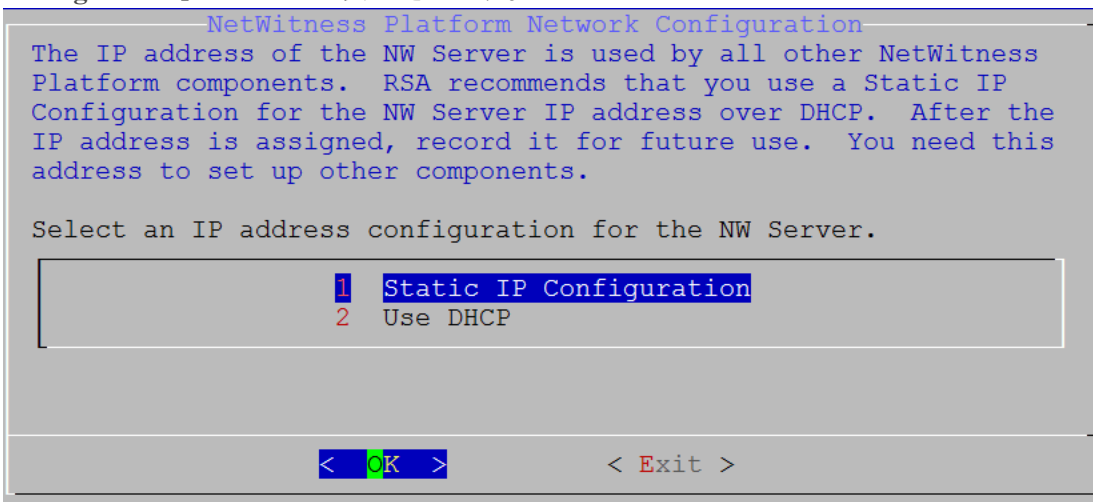
- SSH接続を使用している場合は、次の警告が表示されます。



Enterキーを押して、警告プロンプトを閉じます。

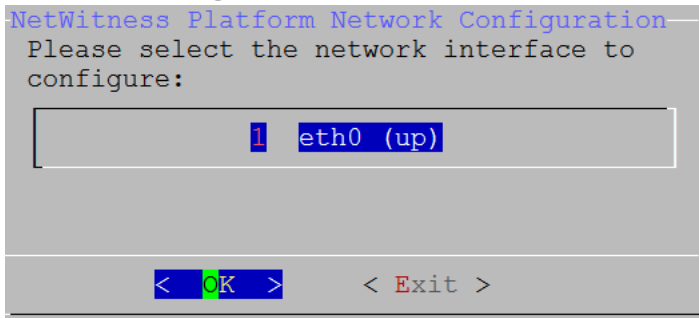
注: ホスト コンソールから直接接続している場合、上記の警告は表示されません。

- セットアップ プログラムがIPアドレスを検出し、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。
- IPアドレスが検出されなかった場合、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。



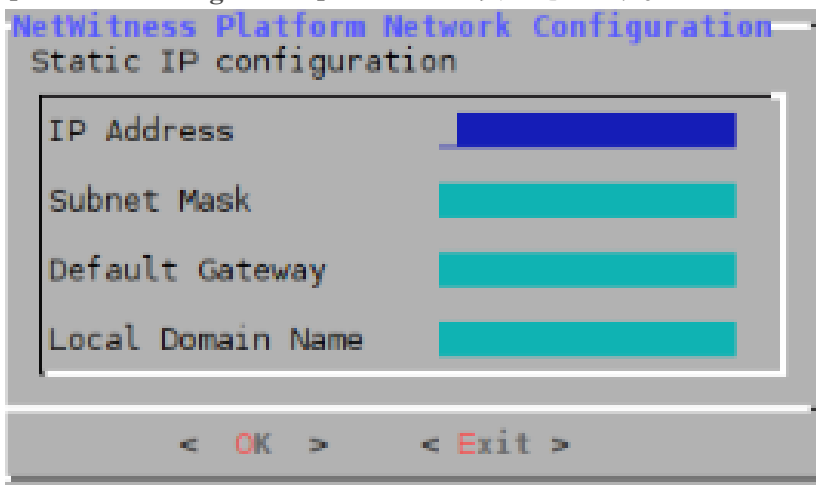
- Static IPを使用する場合は、Tabキーで[OK]に移動し、Enterキーを押します。
DHCPを使用する場合、下向き矢印で[2 Use DHCP]に移動し、Enterキーを押します。

[Network Configuration]プロンプトが表示されます。



9. 下向きの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。作業を続行しない場合は、Tabキーで[Exit]に移動します。

[Static IP Configuration]プロンプトが表示されます。

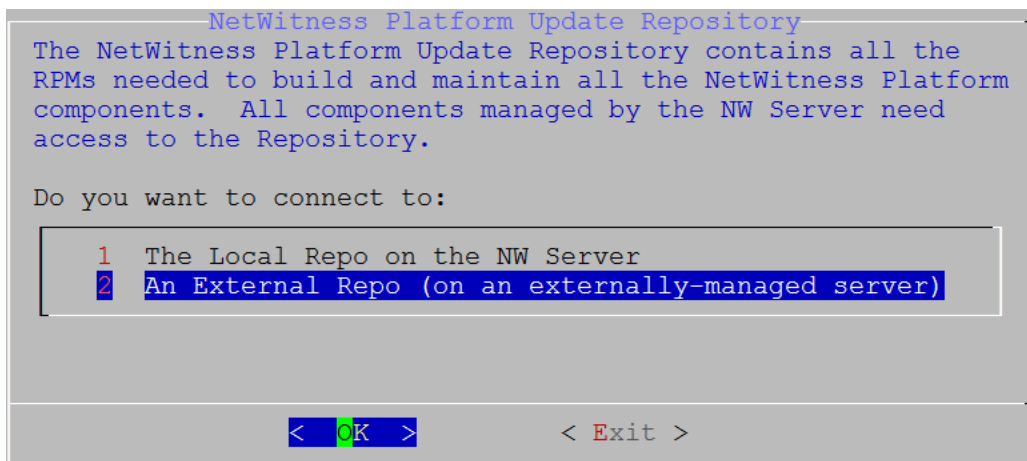


10. 値を入力し(下向き矢印を使用してフィールド間を移動)、Tabキーを使用して[OK]を選択し、Enterキーを押します。
すべての必須フィールドが入力されていないと、「All fields are required」エラーメッセージが表示されます([Secondary DNS Server]フィールドと[Local Domain Name]フィールドは必須ではありません)。
フィールドのいずれかに誤った構文や文字の長さを使用すると、「Invalid <field-name>」エラーメッセージが表示されます。

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。

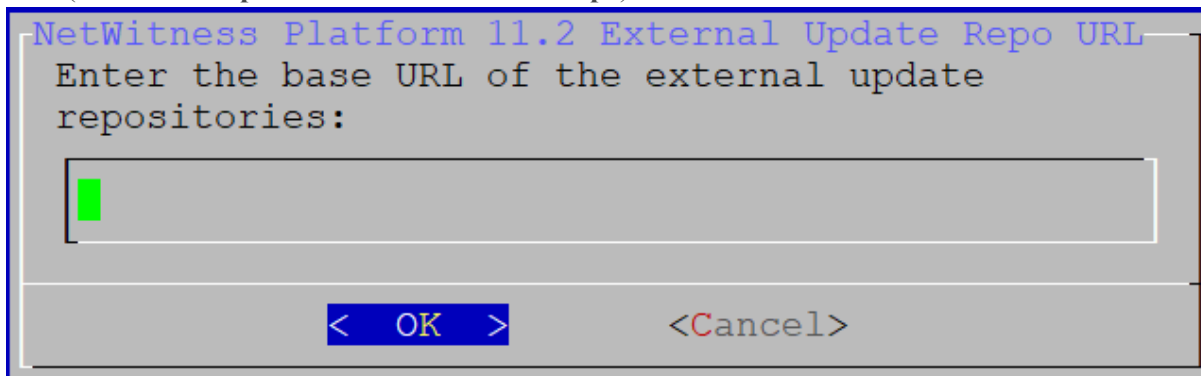
[Update Repository]プロンプトが表示されます。

11. 下向き矢印と上向き矢印を使用して、[2 An External Repo (on an externally-managed Server)]を選択し、Tabキーを使用して[OK]に移動し、Enterを押します。



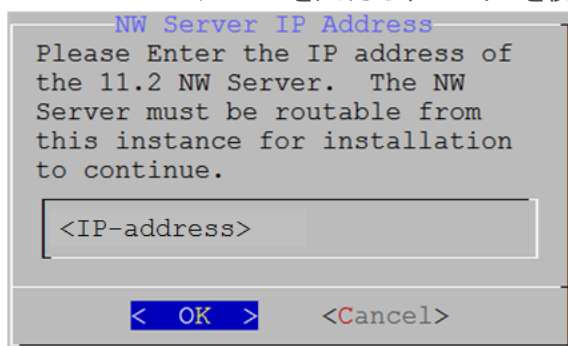
[External Update Repo URL] プロンプトが表示されます。
リポジトリを経由して、RSAの更新とCentOSの更新にアクセスします。

12. 前のセクションでNW Serverのセットアップに使用したNetWitness Platform外部リポジトリのベースURL(たとえば、<http://testserver/netwitness-repo>)を入力し、[OK]をクリックします。



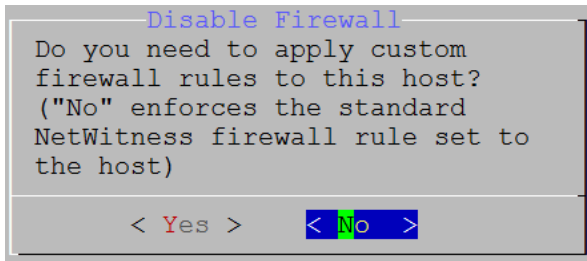
[NW Server IP Address] プロンプトが表示されます。

13. NW ServerのIPアドレスを入力し、Tabキーを使用して[OK]を選択し、Enterキーを押します。

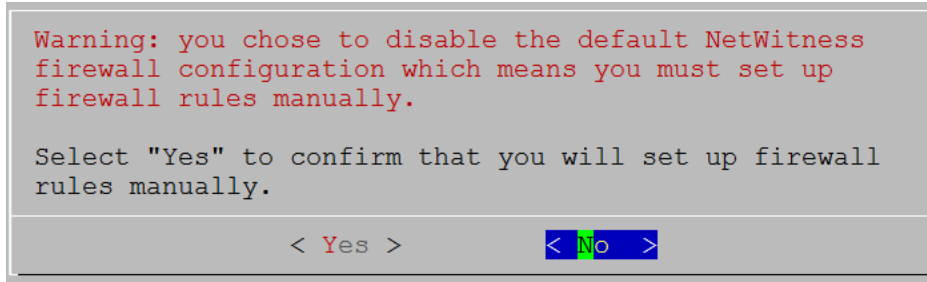


標準的なファイアウォール構成を使用するか、無効化するかを選択するプロンプトが表示されます。

14. 標準的なファイアウォールの構成を使用する場合は、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。



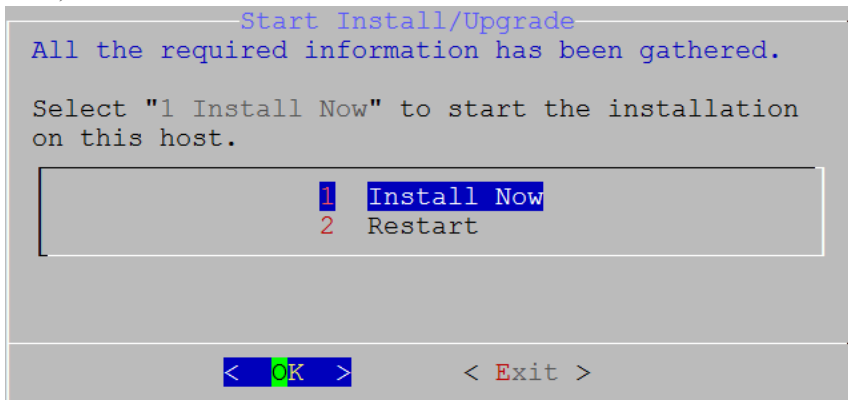
- [Yes]を選択すると、選択が確定します。



- [No]を選択すると、標準的なファイアウォールの構成が適用されます。

[Start Install]プロンプトが表示されます。

15. Enterキーを押すと、11.2.0.0が非NW Serverホストにインストールされます([Install Now]がデフォルト値)。




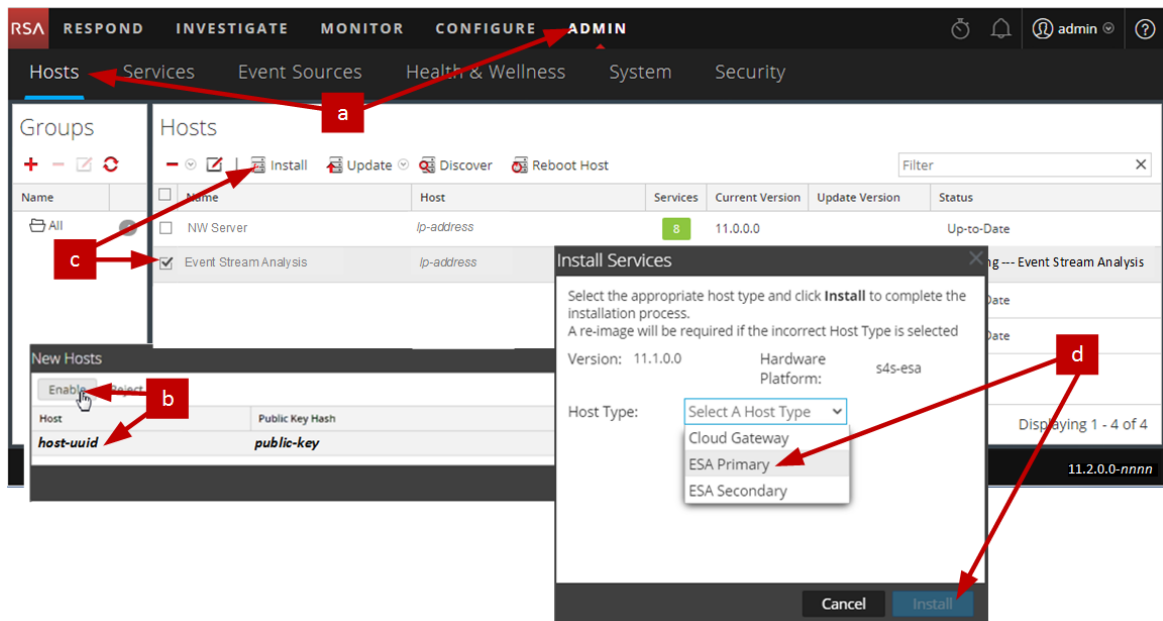
「Installation complete」が表示されたら、NetWitness Platform 11.2.0.0と互換性を持つオペレーティングシステムが稼働する汎用ホストのインストールが完了します。

16. コンポーネント サービスをこの非NW Server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]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ます。([ホスト]ビューはバックグラウンドでグレー表示されています。)

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. 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の非NW Serverホストのインストールが完了しました。

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。
18. NetWitness Platformの残りの非NW Serverコンポーネントについて、ステップ1～16を実行します。

ステップ4. ホスト固有のパラメータの構成

仮想環境でログ収集とパケット収集を行うには、アプリケーション固有のパラメータを構成する必要があります。

仮想環境でのログ収集の構成

ログ収集は、DecoderのIPアドレスに対してログを送信することにより、簡単に実行できます。Decoderの管理インターフェースでは、トラフィックをリッスンする適切なインターフェースを選択できます(デフォルトで選択されていない場合)。

仮想環境でのパケット収集の構成

VMware環境ではパケット収集のために2つのオプションが用意されています。第1のオプションはvSwitchを無差別モードに設定すること、第2のオプションはサードパーティの仮想タップを使用することです。

vSwitchの無差別モードへの設定

仮想または物理にかかわらず、スイッチを無差別モードに設定するオプションには、制限があります(無差別モードは、SPANポート(Ciscoサービス)およびポートミラーリングとも呼ばれます)。仮想または物理にかかわらず、パケット収集の場合には、コピーするトラフィック量およびタイプに応じて容易にポート使用率の超過につながり、パケットの損失を招きます。タップは、物理または仮想のいずれかにかかわらず、想定されるトラフィックを100%(損失無し)収集することを意図して設計されています。

無差別モードはデフォルトで無効に設定されています。特に必要でない場合には、有効にしないでください。仮想マシン内で実行するソフトウェアは、無差別モードに入ることが許可されている場合、vSwitchを経由するすべてのトラフィックを監視できます。しかし、同時にポート使用率の超過によるパケット損失も招きます。

無差別モードを許可するようにポートグループまたは仮想スイッチを構成する方法

1. vSphereクライアントを使用してVMware ESXi/ESXホストまたはvCenter Serverにログオンします。
2. インベントリ内でVMware ESXi/ESXホストを選択します。
3. [構成]タブを選択します。
4. [ハードウェア]セクションで、[ネットワーク]をクリックします。
5. 無差別モードを有効にする仮想スイッチの[プロパティ]を選択します。
6. 変更する仮想スイッチまたはポートグループを選択し、[編集]をクリックします。
7. [セキュリティ]タブをクリックします。[無差別モード]ドロップダウンメニューで、[承諾]を選択します。

サードパーティの仮想タップの使用

仮想タップのインストール方法は、ベンダーに応じて異なります。インストール手順については、ベンダーのドキュメントを参照してください。仮想タップは一般的に統合が容易であり、タップのユーザインタフェースによってコピーするトラフィックやタイプを効率的に選択できます。

仮想タップは、収集したトラフィックをGREトンネルにカプセル化します。選択するタイプに応じて、次のいずれかのシナリオが該当します。

- トンネルの終端には外部ホストが必要です。この外部ホストは、トラフィックをDecoderインタフェースに転送します。
- トンネルは、Decoderインタフェースにトラフィックを直接送信し、そこでNetWitness Platformがトラフィックのカプセル化を解除します。

ステップ5. 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。

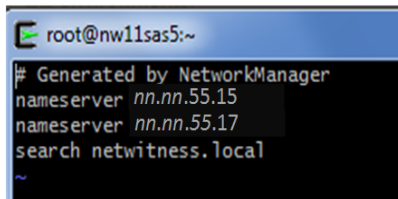
- 全般
- RSA NetWitness® Endpoint Insights
- FIPSの有効化
- RSA NetWitness UEBA(User Entity Behavior Analytics)

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

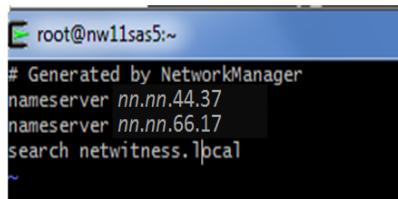
NetWitness Platform 11.2のDNSサーバを再構成するには、NetWitness Serverで次の手順を実行します。

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エントリーを示します。



```
root@nw1sas5:~  
# 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エントリーを示します。



```
root@nw1sas5:~  
# 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。

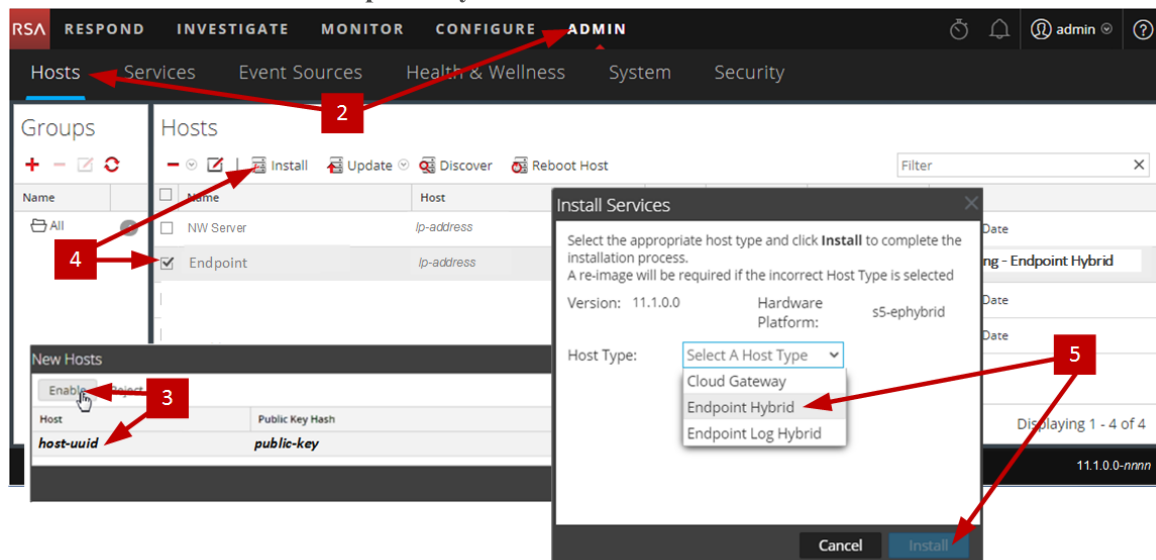
- Endpoint Hybrid
- Endpoint Log Hybrid

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。

NetWitness UEBA(User Entity Behavior Analytics)

(オプション) タスク3: NetWitness UEBAのインストール

前提条件: 仮想環境のストレージの追加

仮想マシンには、デフォルトで約104 GBのストレージが導入されます。NetWitness UEBAをインストールするには、仮想環境のストレージ領域を少なくとも800 GBに増やす必要があります。

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。

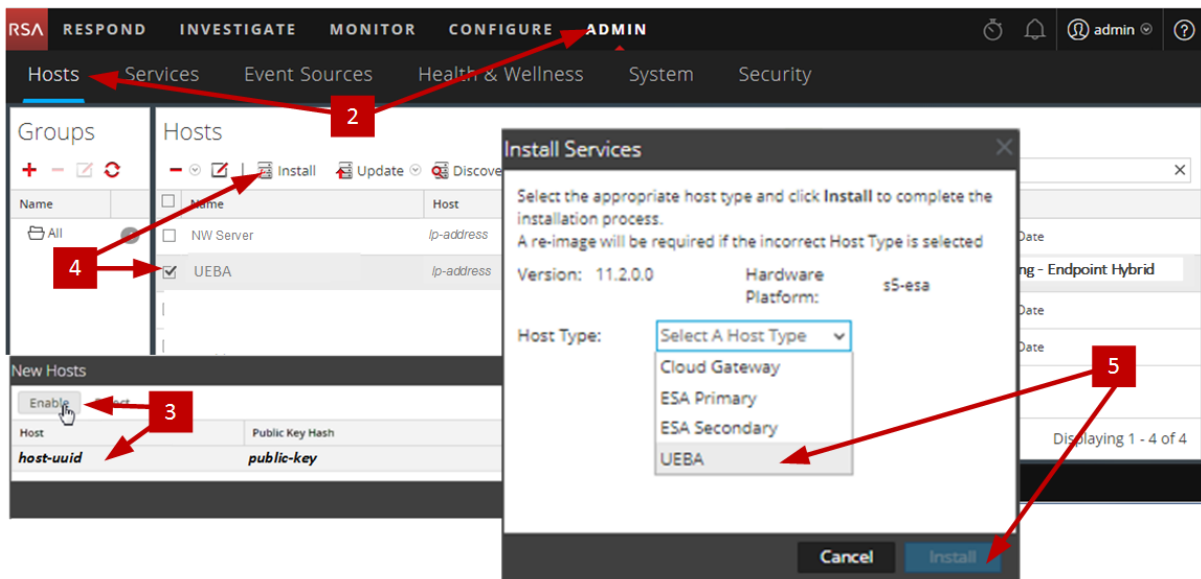
1. 物理ホストの場合は、「*NetWitness Platform バージョン11.2 インストールガイド*」にある「インストールタスク」の「タスク2 - その他のコンポーネント ホストへの11.2のインストール」のステップ1 - 14を実行します。仮想ホストの場合は、ステップ1 - 15を実行します。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

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

Plarform 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 NetWitness Platform Admin console interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The ADMIN tab is active, showing a sub-menu with Hosts, Services, Event Sources, Health & Wellness, System, and Security. The Security section is expanded, showing Change Service, Broker, and Security options. The Broker option is selected, leading to the 'Users' management page. On the left, a list of users shows 'Broker' and 'admin'. The main area displays the 'User Information' and 'User Settings' for the 'Broker' user. The 'User Information' section includes fields for Name (Broker), Username (Broker), Password, Confirm Password, Email (test@rsa.coim), 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.

User Information	
Name	Broker
Username	Broker
Password	
Confirm Password	
Email	test@rsa.coim
Description	

User Settings	
Auth Type	NetWitness Platform
Core Query Timeout	5
Query Prefix	
Session Threshold	0

Role Membership	
<input type="checkbox"/>	Groups
<input type="checkbox"/>	Administrators
<input type="checkbox"/>	Aggregation
<input checked="" type="checkbox"/>	Analysts
<input type="checkbox"/>	Data_Privacy_Officers
<input type="checkbox"/>	Malware_Analysts
<input type="checkbox"/>	Operators
<input type="checkbox"/>	SOC_Managers

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>	<p>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。</p> <pre>!"#\$%&()*+,-.:;<=>?@[\\]^_`{ }</pre> <p>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：</p> <pre>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</pre>
-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>	<p>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)。</p> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>注: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。</p> </div>
-s	<schemas>	<p>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')。</p> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>注: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。</p> </div>
-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	<p>CLI(コマンド ライン インタフェース)に、「Orchestration failed.」と表示される。</p> <pre>Mixlib::ShellOut::ShellCommandFailed: Command execution failed. STDOUT/STDERR suppressed for sensitive resource in/var/log/netwitness/config-management/chef-solo.log</pre>
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"> 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。 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。

エラー メッセー ジ	<pre>ERROR com.rsa.smc.sa.admin.web.controller.ajax.health. AlarmsController - Cannot connect to System Management Service</pre>
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	<p>SMSサービスを再起動します。</p> <pre>systemctl restart rsa-sms</pre>

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	<p>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。</p> <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 <filename></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<hostname>-<hostip>-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=<devicename> ; # from the host's primary ethernet interface config file BOOTPROTO=<bootprotocol> ; # from the host's primary ethernet interface config file IPADDR=<value> ; # from the host's primary ethernet interface config file NETMASK=<value> ; # from the host's primary ethernet interface config file GATEWAY=<value> ; # from the host's primary ethernet interface config file search <value> ; # from the host's /etc/resolv.conf file nameserver <value> ; # 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">1. ESAプライマリホストにSSHで接続し、ログインします。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/keystore3. 次のコマンドを実行し、ESAを再起動します。 systemctl restart rsa-nw-esa-server <div>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。</div>

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><timestamp>.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の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、「 マスター目次 」で確認できます。

エラーメッセージ	<code><timestamp> 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、「 マスター目次 」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、「 マスター目次 」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。 # /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --revert

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	<p>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。</p> <p>または</p> <p>次のメッセージが<code>sa.log</code>に記録されました。</p> <pre>Syslog Configuration migration failed. Restart jetty service to fix this issue</pre>
原因	<p>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。</p>
解決策	<ol style="list-style-type: none"> SSHでNW Serverに接続します。 次のコマンドを実行します。 <pre>orchestration-cli-client --update-admin-node</pre>

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"> 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。 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。 <p><code>orchestration-server.log</code>に次のメッセージが記録されます。</p> <pre>"'file' _virtual_ returned False: cannot import name HASHES"</pre>
原因	<p>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。</p>
解決策	<ol style="list-style-type: none"> 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。 次のコマンドを実行します。 <pre>systemctl unmask salt-minion systemctl restart salt-minion</pre> <ol style="list-style-type: none"> 非NW Serverホストのアップグレードを再試行します。

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、「 マスター目次 」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">1. 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>2. 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3. 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 <ID-for-presidio-airflow-form-previous-output></pre>4. 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>5. NetWitness Platformにログインし、[管理]>[ホスト]に移動し、余分なNetWitness UEBAホストを削除します。

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。

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. 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) をホストするディレクトリを作成します (例: Webサーバの web-root の下の 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>
```
3. 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
```
4. 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
```
5. 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。
6. 以下のように解凍します。
 - a. 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	-
 GeoIP-1.5.0-11.el7.x86_64.rpm	20-Nov-2016 12:49 1.1M
 HostAgent-Linux-64-x86-en_US-1.2.25.1.0163-1.x86_64.rpm	03-Oct-2017 10:07 4.6M
 Lib_Utils-1.00-09.noarch.rpm	03-Oct-2017 10:05 1.5M
 OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm	20-Nov-2016 14:43 502K
 OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm	20-Nov-2016 14:43 15K
 PyYAML-3.11-1.el7.x86_64.rpm	19-Dec-2017 12:30 160K
 SDL-1.2.15-14.el7.x86_64.rpm	25-Nov-2015 10:39 204K
 acl-2.2.51-12.el7.x86_64.rpm	03-Oct-2017 10:04 81K
 adobe-source-sans-pro-fonts-2.020-1.el7.noarch.rpm	13-Feb-2018 05:10 706K
 alsa-lib-1.1.3-3.el7.x86_64.rpm	10-Aug-2017 10:52 421K
 at-3.1.13-22.el7_4.2.x86_64.rpm	25-Jan-2018 17:56 51K
 atk-2.22.0-3.el7.x86_64.rpm	10-Aug-2017 10:53 258K
 attr-2.4.46-12.el7.x86_64.rpm	03-Oct-2017 10:04 66K

- b. 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
 fmeserver-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。

- 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17日	Release to Operations	IDD
1.1	2018年11月29日	UEBA評価ライセンスに関する注を追加。	IDD

