RSA® NetWitness Platform

Version11.6

リカバリ ツール ユーザ ガイド

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 Conferenceのロゴ、RSA、その他の商標は、RSA Security LLCまたはその関連会社(「RSA」)の商標です。RSAの商標のリストについては、https://www.rsa.com/ja-jp/company/rsa-trademarksを参照してください。その他の商標は、各社の商標または登録商標です。

使用許諾契約

本ソフトウェアと関連ドキュメントは、RSA Security LLCまたはその関連会社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

本製品には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

本文書に記載される、RSA Security LLCまたはその関連会社(「RSA」)のいかなるソフトウェアの使用、複製、配布にも、適切なソフトウェアライセンスが必要です。

RSAは、本文書に記載される情報が、発行日時点で正確であるとみなしています。この情報は予告なく変更されることがあります。

本文書に記載される情報は、「現状有姿」の条件で提供されています。RSAでは、本文書に記載される情報に関するいかなる内容についても表明保証条項を設けず、特に、商品性や特定の目的に対する適応性に対する黙示的保証は提供しません。

7月 2021

目次

災害復旧(バックアップとリストアの手順)

NetWitnessリカバリツール(NRT)を使用して、NetWitness Serverホストおよびコンポーネント ホストのデータをバックアップおよびリストアすることができます。NRTは、RMA、ハードウェア更新、一般的なバックアップおよびリストアの要件に対応するために、対象ホストのコマンドラインで実行するスクリプトです。Azure VMにデプロイされたホストの災害復旧手順については、「Azure導入環境での災害復旧」を参照してください。

注: NRTは各ホスト上でローカルに実行する必要があります。リモート ホストや外部ホストから実行することはできません。

次のタイプのホストをバックアップおよびリストアできます。

注: NRTスクリプトでは、太字の部分(単語間のスペースは除く)をカテゴリとして指定します。

- **NetWitness Admin Server**(Broker、Investigate、Respond、Health and Wellness、Reporting Engineを含む)
- **AnalystUI**(Broker、Investigate、Respond、Reporting Engineを含む)
- **Archiver**(Log Archiver(WorkbenchおよびArchiver))
- **Broker**(スタンドアロンBroker)
- **Concentrator**(NetworkまたはLog Concentrator)
- **Decoder**(Network Decoder(パケット))
- **Endpoint**(Endpointエージェント)
- **Endpoint Broker**(Endpoint Broker)
- **Endpoint Log Hybrid**(Log Collector、Log Decoder、Endpoint Server、Concentrator)
- **ESA Primary**(Contexthub、ESA Correlation、Incident Managementデータベース)
- **ESA Secondary**(ESA Correlation)
- **Gateway**(Cloud Gateway)
- **Log Hybrid Retention**(保存用に最適化されたLog Hybird。RSAシリーズ6 Hybridハードウェアで選択)
- **Log Collector**(Log Collector およびインストールされている場合は Virtual Log Collector を含む)
- **Log Decoder**(Log Decoder、およびインストールされている場合は Local Log Collector および Warehouse Connector を含む)
- **Log Hybrid**(Log Collector、Log Decoder、Concentrator)
- **Malware**(Malware AnalysisおよびBroker)
- **Network Hybrid**(ConcentratorおよびDecoder)
- **Search**(Health & Wellness ベータ ホスト)

- **UEBA**(User Entity and Behavior Analytics)
- **Warehouse**(Warehouse Connector)

NetWitnessリカバリツールの基本的な使用方法

NRTを使用してデータをバックアップする場合は、exportオプションを指定します。データをリストアする場合は、importオプションを指定します。ルート ディレクトリレベルで、次の形式でコマンドを実行します。

```
nw-recovery-tool [command] [option]
```

使用可能なコマンドとオプションは、次の表のとおりです。

コマンドとオプション	説明
-h, --help	コマンドとオプションに関するヘルプを表示します。例えば、 次のコマンドを実行すると、有効なカテゴリ名のリストが表示されます:nw-recovery-tool --help-categories
-e, --export	データまたは構成をエクスポートします。
-i, --import	データまたは構成をインポートします。
-d, --dump-dir <path>	エクスポートするデータの保存場所のパス、またはインポートするデータの保存場所のパスを指定します(例:/var/netwitness/backup)。
-C, --category <name>	対象のコンポーネントをカテゴリによって選択します。 有効なカテゴリ名は、AdminServer、AnalystUI、Archiver、Broker、Concentrator、Decoder、Endpoint、EndPointBroker,、EndpointLogHybridLogHybrid、ESAPrimary、ESASecondary、Gateway、LogHybridRetention、LogCollector、LogDecoder、LogHybrid、Malware、NetworkHybrid、Search、UEBA、Warehouseです。 1つのカテゴリを指定するか、同一ホストに複数のカテゴリが共存する場合は複数のカテゴリを指定できます。以下に例を示します。 • --category AdminServer(管理サーバのみを指定) --category AdminServer --category Gateway(管理サーバとCloud Gatewayを指定) • --category ESAPrimary(ESA Primaryのみを指定) • --category Broker(Brokerのみを指定) --category Broker --category EndpointBroker(BrokerとEndpoint Brokerを指定)

前提条件

以下の条件を満たしていることを確認してください。

- データをバックアップする前に、このドキュメントを最後までお読みください。NetWitness Platformのバックアップとリストアの手順を開始する前に必要な情報を確認できるよう、このドキュメントにはすべての導入シナリオが網羅されています。
- NRTはバックアップの場合もリストアの場合も、バックアップまたはリストアする各ホストでローカルに実行してください。NRTを他のホストから実行したり、バックアップやリストアを複数のホストで同時に実行することはできません。ただし、同一ホスト上の複数のコンポーネントを同時にバックアップすることはできます。
- データのエクスポートおよびインポートは、同一ホスト上で実行する必要があります。ホストに障害が発生し、新しいホストを導入する場合は、新しいホストに元のホストと全く同じ識別パラメータ(例えば、IPアドレス)を設定し、同一バージョンのNetWitness Platformを実行する必要があります。
- NRTのexportコマンドを実行する前に、バックアップの保存場所(`/var/netwitness/backup`を推奨) に十分な空きディスク領域があることを確認してください。短時間で一杯になり、システム クラッシュの原因となる可能性があるため、`tmp`ディレクトリは使用しないでください。
- Malwareホストをバックアップする前に、ディスク サイズを確認し、調整してください。次の表に、ハードウェアのタイプ別にバックアップできるMalwareデータベースの最大サイズと、最大サイズ以内に削減する方法を示します。

ホスト	ソース ハードウェア	ターゲット ハードウェア	データベース	バックアップの最大サイズ	バックアップの最大サイズまで削減する処理
Malware	4Sシリーズ Hybrid	6シリーズ Core	`/var/netwitness`	2.5TB	ロールオーバーを構成する。 データベースから不要なデータを消去する。

- バックアップを取得したホストが使用していたのと同一のISOイメージをリストアします。
- 単一のホストに複数のサービスが共存する場合は、nw-recoveryツールの`import`および`export`コマンドの1つのコマンド文字列に、すべてのサービスを含めてください。

注: NRT実行時、バックアップ(export) またはリストア(import) のどちらの場合も、Malware、Reporting Engine、およびPostgresqlサービスの停止と再起動が行われます。

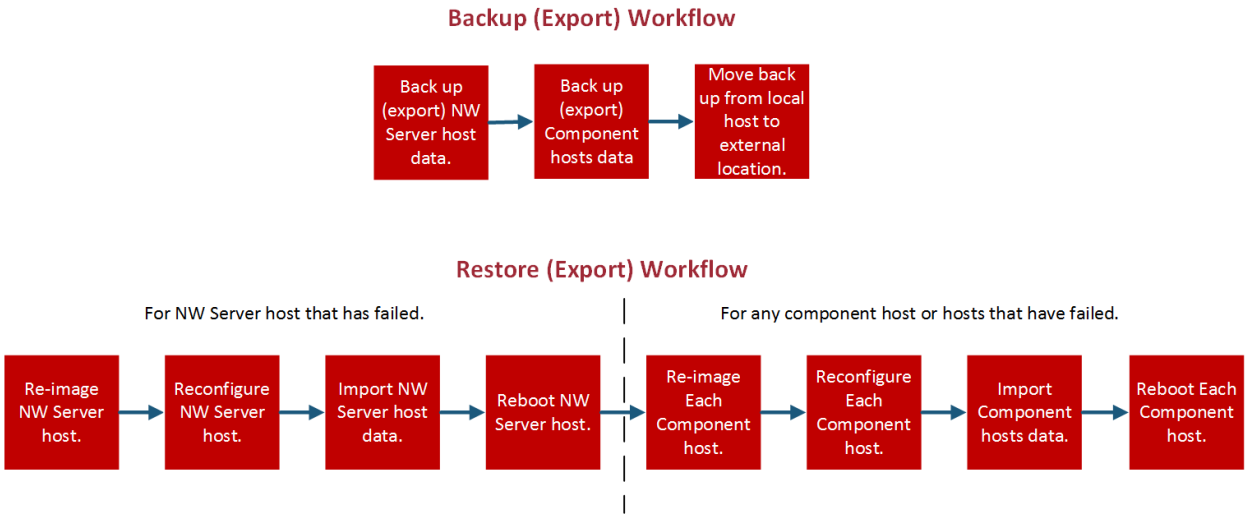
災害復旧のワークフロー

次の図は、災害復旧タスクの概要を示しています。

注: 復旧が必要なのは、障害が発生したホストのみです。つまり、単一のホストに障害が発生した場合は単一のホストを復旧し、複数のホストで障害が発生した場合は複数のホストを復旧します。

図には次のタスクが含まれます。

- バックアップ(初回はできるだけ早期に実行し、以降は可能な頻度で実行)。
- リストア(データをリストアする必要がある場合のみ実行)。



11.xホストでのデータのバックアップとリストア

データのバックアップとリストアの手順は、NetWitness Serverホストとコンポーネント ホストで異なります。

注意: 1.) 本ドキュメントの災害復旧手順を実行する際に、UIの[ホスト]ビュー([管理]>[ホスト]) でコンポーネント ホスト(=NetWitness Serverホスト以外のホスト)を削除しないでください。2.) 災害復旧手順を実行する前に使用していた既存のホスト名を継続して使用する必要があります。

11.x NetWitness Serverでのデータのバックアップとリストア

注： 複数のホストからエクスポートするデータを共有ストレージ(たとえば、共有マウントや共有ドライブ)に保存する場合、エクスポートするデータの保存場所のパスには、ホストごとに固有のサブフォルダを追加し、エクスポートしたデータが別のホストのデータによって上書きされないようにしてください。たとえば、`--dump-dir /mnt/storage/<host-specific-name>`のようにエクスポートするデータの保存場所のパスを指定します。

NetWitness Serverホストでのデータのバックアップ

この手順は、正常に稼働中の既存の11.x NetWitness Serverホスト システムで実行します。

1. 以下のコマンドをrootレベルで実行します。

```
nw-recovery-tool --export --dump-dir /var/netwitness/backup --category
AdminServer
```

注： サービスがそのサービス専用のホストにインストールされているのではなく、他のカテゴリのサービスと同じホストに共存している場合は、コマンドラインにはそれらのサービスも追加する必要があります。`Gateway`または`EndpointBroker`が共存する場合は、次の例のように指定します：

```
nw-recovery-tool--export --dump-dir /var/netwitness/backup --category
AdminServer --category Gateway
nw-recovery-tool--export --dump-dir /var/netwitness/backup --category
Broker --category EndpointBroker
```

2. `/var/netwitness/backup`は、エクスポートするデータの保存場所のパスに置き換えます。
   a. 指定した場所にバックアップしたデータを保存するのに十分な空き領域があることを確認してください。
   b. バックアップ ディレクトリのパスには、ローカル ホスト上の場所を指定する必要があります。ただし、ネットワーク共有マウントや外部デバイスにデータを保存することはできます。

データは、ステップ2で指定した、NetWitness Serverホスト上の保存場所にバックアップされます。

3. バックアップ データをローカル ホストから別のサーバまたはUSBスティックに移動します。

NetWitness Serverホストでのデータのリストア

1. NetWitness Serverホストを再イメージ化し、元のホストと同じネットワーク構成を設定します。NetWitness Serverホストの再イメージ化の詳細については、バージョン11.6の『物理ホスト インストール ガイド』の「タスク1：NetWitness Serverホストに11.6をインストール」を参照してください。

   a. **(オプション)** バックアップデータの取得にネットワーク接続の確立が必要な場合(例えば、バックアップデータがリモートホスト上に存在する場合など)、次のスクリプトを実行し、元のホストと同じIPアドレス、サブネット、ゲートウェイ、DNS、ドメインの情報を指定します。

   ```
   netconfig --static --interface <name> --ip <address> --netmask <netmask>
   --gateway <gateway>
   ```

   以下に例を示します。

   ```
   netconfig --static --interface eth0 --ip 192.168.1.100 --netmask
   255.255.255.0 --gateway 192.168.1.1
   ```

   (オプション) DNSサーバを指定する場合は、次のパラメータを追加します。

   ```
   --dns <address>
   ```

   (オプション) ドメイン名を指定する場合は、次のパラメータを追加します。

   ```
   --domain <name>
   ```

   b. **(オプション)** DHCPを使用している場合は、次のスクリプトを実行します。

   ```
   netconfig --dhcp --interface <name>
   ```

   以下に例を示します。

   ```
   netconfig --dhcp --interface eth0
   ```

   c. バックアップ データを、ローカル ホスト上のバックアップ ディレクトリのパスに追加します。例：

   ```
   /var/netwitness/backup
   ```

2. `nwsetup-tui`コマンドを実行します。これにより、セットアップ プログラムが開始します。

   注： セットアップ プログラムの途中で、ホストのネットワーク構成の入力を求められたら、このホストに元々設定されていたものと完全に同じネットワーク構成を指定してください。

3. インストール タイプを選択するプロンプトが表示されたら、[**2:Recover (Reinstall)**]を選択し、[**OK**]をクリックします。次に、バックアップ データを保存したバックアップ ディレクトリのパスを入力します。
4. インストールが正常に完了したら、バックアップ データと完全に同じリリースおよびパッチ バージョンが実行されていることを確認します。
   - データをバックアップした11.xシステムに、パッチが適用されていた場合は、ホストを同一のパッチ バージョンに更新します。更新手順は、そのパッチ バージョンの更新ガイドのオフライン更新手順に従います。
   - データをバックアップした11.xシステムが、メジャーリリース バージョン(例：11.x)を実行し、それ以降のパッチを適用していない場合、ホストを更新する必要はありません。
5. ホストが正しいバージョンを実行していることが確認できたら、NetWitness Serverで次のコマンドを実行し、データをリストアします。

   ```
   nw-recovery-tool --import --dump-dir /var/netwitness/backup --category
   AdminServer
   ```

注： サービスがそのサービス専用のホストにインストールされているのではなく、他のカテゴリのサービスと同じホストに共存している場合は、コマンドラインにはそれらのサービスも追加する必要があります。GatewayまたはEndpointBrokerが共存する場合は、次の例のように指定します：

```
nw-recovery-tool--import --dump-dir /var/netwitness/backup --category
AdminServer --category Gateway
nw-recovery-tool--import --dump-dir /var/netwitness/backup --category
Broker --category EndpointBroker
```

6. (オプション) カスタム ファイアウォール ルールを使用する場合、または、/etc/hostsにカスタム エントリーを追加する場合：
   a. (オプション) カスタム ファイアウォール ルールを使用する場合 (つまり、インストール時にnwsetup-tuiコマンドの[Disable Firewall]プロンプトで「Yes」を選択した場合) は、/etc/sysconfig/iptablesファイルをバックアップの<dump-dir>/unmanaged/etc/sysconfig/iptablesファイルからリストアします。
   b. (オプション) /etc/hostsにカスタム エントリーを追加する場合は、/etc/hosts.usersファイルを、バックアップの<dump-dir>/unmanaged/etc/hosts.userからホスト上の/etcにリストアします。
   c. ステップ6aまたは6bを実行した場合は、次のコマンドを実行してホストを更新します。
      nw-manage --refresh-host --host-key <ID, IP, hostname or display name of host>
7. NetWitness Serverホストをリブートします。

注： /etc/hostに更にカスタム エントリーを追加したい場合は、カスタム エントリーを/etc/hosts.usersファイルに追加してから、ホストを更新する必要があります (ステップ6cを参照)。

他のコンポーネント ホストでのデータのバックアップとリストア

次の手順は、既存の正常に稼働中の11.xコンポーネント ホストで実行する必要があります。

コンポーネント ホストでのデータのバックアップ

1. 以下のコマンドをrootレベルで実行します。
   `nw-recovery-tool --export --dump-dir /var/netwitness/backup --category <category name>`
   category nameには、次のいずれか1つを指定します。
   `AdminServer、AnalystUI、Archiver、Broker、Concentrator、Decoder、Endpoint、EndPointBroker,、EndpointLogHybrid、ESAPrimary、ESASecondary、Gateway、LogHybridRetention、LogCollector、LogDecoder、LogHybrid、Malware、NetworkHybrid、Search、UEBA、Warehouse`

   注： 1.) ホスト タイプに一致するカテゴリーを指定します。2.) 任意のサービスが専用ホストではなく、他のコンポーネント ホスト上に共存している場合は、そのサービスをコマンド ラインに追加する必要があります。例えば、Warehouse ConnectorがLog Decoderホストに共存している場合、以下にコマンド文字列の例を示します。
   `nw-recovery-tool--export --dump-dir /var/netwitness/backup --category LogDecoder --category Warehouse`

2. **(オプション)** `/var/netwitness/backup`は、データのエクスポート先の場所のパスに置き換えます。
   a. 指定した場所にバックアップしたデータを保存するのに十分な空き領域があることを確認してください。
   b. バックアップ ディレクトリのパスには、ローカル ホスト上の場所を指定する必要があります。ただし、ネットワーク共有マウントや外部デバイスにデータを保存することはできます。

3. **Endpoint Log Hybrid**および**ESA Primary**ホストの場合は、次のコマンドを実行して、データベース内のアプリケーション データをエクスポートすることができます。
   `nw-recovery-tool --export --dump-dir /var/netwitness/backup --component mongo`
   `/var/netwitness/backup`は、データのエクスポート先の場所のパスに置き換えます。

   注： 1.) 指定した場所にエクスポートしたMongoデータベースのファイルを保存するのに十分な空き領域があることを確認してください。2.) 単一のコマンドで、**Endpoint Log Hybrid**または**ESA Primary**のホスト データとMongoデータベースをバックアップできます。例：`nw-recovery-tool --export --dump-dir /var/netwitness/backup --category EndpointLogHybrid --component mongo`

4. **Malware**の場合は、次のコマンドを実行して、Malwareデータベース内のアプリケーション データをエクスポートすることができます。
   `nw-recovery-tool --export --dump-dir /var/netwitness/backup --component postgresql`
   `/var/netwitness/backup`は、データのエクスポート先の場所のパスに置き換えます。

注： 指定した場所にエクスポートしたMalwareデータベースのファイルを保存するのに十分な空き領域があることを確認してください。

5. バックアップ データをローカル ホストから別のサーバまたはUSBスティックに移動します。

コンポーネント ホストでのデータのリストア

1. コンポーネント ホストを再イメージ化し、元のホストと同じネットワーク構成を設定します。コンポーネント ホストの再イメージ化の詳細については、バージョン11.xの『*物理ホスト インストール ガイド*』の「タスク2: その他のコンポーネントのホストに11.xをインストール」を参照してください。
2. **(オプション)** バックアップ データを取得するためにネットワーク接続を確立する必要がある(バックアップ データがリモート ホスト上に存在するなど) 場合は、元のホストと同じIPアドレス、サブネット、ゲートウェイ、DNS、ドメインの情報を使用して、次のスクリプトを実行します。
   `netconfig --static --interface <name> --ip <address> --netmask <netmask> --gateway <gateway>`
   以下に例を示します。
   `netconfig --static --interface eth0 --ip 192.168.1.100 --netmask 255.255.255.0 --gateway 192.168.1.1`
   オプション: DNSサーバを指定する場合は、次のパラメータを追加します。
   `--dns <address>`
   オプション:ドメイン名を指定する場合は、次のパラメータを追加します。
   `--domain <name>`
   a. (**オプション**) DHCPを使用している場合は、次のスクリプトを実行します。
      `netconfig --dhcp --interface <name>`
      例:
      `netconfig --dhcp --interface eth0`
   b. バックアップ データを、ローカルホスト上のバックアップ ディレクトリのパスに追加します。
      例: `/var/netwitness/backup`
3. `nwsetup-tui`コマンドを実行します。これにより、セットアップ プログラムが開始します。

注： セットアップ プログラムの途中で、ホストのネットワーク構成の入力を求められたら、このホストに元々設定されていたものと完全に同じネットワーク構成を指定してください。

4. インストール タイプを選択するプロンプトが表示されたら、[**2:Recover (Reinstall)**]を選択し、[**OK**]をクリックします。次に、バックアップ データを保存したバックアップ ディレクトリのパスを入力します。

5. nwsetup-tuiコマンドによるセットアップが完了したら、NetWitness Platformユーザー インタフェイスの[ホスト]ビューから[**インストール**]コマンドを使用して、ホスト上に適切なサービスを再インストールする必要があります。
6. サービスのインストールが完了したら、バックアップ データと完全に同じリリースおよびパッチバージョンが実行されていることを確認します。
   - データをバックアップした11.xシステムに、パッチが適用されていた場合は、ホストを同一のパッチバージョンにアップデートします。アップデート手順は、そのパッチ バージョンのオフライン アップデート手順に従います。
   - データをバックアップした11.xシステムが、メジャーリリース バージョン(例 : 11.x) を実行し、それ以降のパッチを適用していない場合、ホストを更新する必要はありません。
7. ホストが正しいバージョンを実行していることを確認できたら、コンポーネント ホストのrootレベルに戻り、次のコマンドを実行してデータをリストアします。
   ```
   nw-recovery-tool --import --dump-dir /var/netwitness/backup --category
   <category name>
   ```
   注 : サービスが専用ホストではなく、コンポーネント ホスト上に他のサービスと共存している場合は、コマンドラインにはそれらのサービスも追加する必要があります。例えば、Warehouse ConnectorがLog Decoderホストに共存している場合、以下は、このコマンド文字列の例です。
   ```
   nw-recovery-tool--import --dump-dir /var/netwitness/backup --category
   LogDecoder --category Warehouse
   ```
8. **EnpointLogHybrid**および**ESAPrimary**システムの場合は、次のコマンドを実行し、アプリケーション データをリストアすることができます。
   ```
   nw-recovery-tool --import --dump-dir /var/netwitness/backup --component
   mongo
   ```
9. **Malware**ホストの場合は、次のコマンドを実行して、Malwareデータベースのアプリケーション データをリストアできます。
   ```
   nw-recovery-tool --import --dump-dir /var/netwitness/backup --component
   postgresql
   ```

10. 外部ストレージ(DAC/SAN/Unity/PowerVault) が構成されたDecoder、Log Decoder、Concentrator、Archiver、Network Hybrid、Log Hybridの場合、次の手順を実行します。

    a. <dump-dir>/unmanaged/etc/fstabファイルの中身を確認し、システムの/etc/fstabファイルに存在しないデバイスのマウント ポイントがないか確認します。

    重要: 新しいホスト ハードウェア(つまり、Decoder、Log Decoder、Concentrator、Archiver、Network Hybrid、Log Hybridの新しいホスト) に移行している場合は、次のステップに進む前に、以下を実行する必要があります。
    1.古いハードウェア ホストと接続された外部ストレージ デバイスの電源をオフにします。
    2.外部ストレージ デバイスを新しいホスト ハードウェアに接続します。
    3.新しいホスト ハードウェアと接続された外部ストレージ デバイスの電源をオンにします。

    a. <dump-dir>/unmanaged/etc/fstabのバックアップ コピーに含まれている各デバイスについて、次のステップを実行します。

        i. 対応するデバイスが存在し、接続されていることを確認します。接続されていない場合は、接続します。今後使用しないデバイスはスキップし、次のデバイスを確認します。

        ii. ファイル システムにマウント ポイントのディレクトリが存在することを確認します。存在しない場合は、mkdir <path>コマンドを実行してディレクトリを作成します。

        iii. バックアップのファイル内のfstabエントリを、システムの/etc/fstabのファイルに追加します。

        注意: シリーズ5または6ハイブリッドの場合は、「付録 A.復旧後のシリーズ5および6 HybridでのfstabのFstabの変更」の指示に従って、バックアップされたデータを/etc/fstabディレクトリにリストアする必要があります。

    b. 次のコマンドを各ホストで実行します。

    ```
    mount -a
    ```

11. (オプション) カスタム ファイアウォール ルールを使用する場合、または、/etc/hostsにカスタム エントリーを追加する場合 :

    a. (オプション) カスタム ファイアウォール ルールを使用する場合(つまり、インストール時にnwsetup-tuiコマンドの[Disable Firewall]プロンプトで「Yes」を選択した場合) は、/etc/sysconfig/iptablesファイルをバックアップの<dump-dir>/unmanaged/etc/sysconfig/iptablesファイルからリストアします。

    b. (オプション) /etc/hostsにカスタム エントリーを追加する場合は、/etc/hosts.usersファイルを、バックアップの<dump-dir>/unmanaged/etc/hosts.userからホスト上の/etcにリストアします。

    c. ステップ11aまたは11bを実行した場合は、次のコマンドを実行してホストを更新します。

    ```
    nw-manage --refresh-host --host-key <ID, IP, hostname or display name of host>
    ```

12. コンポーネント ホストをリブートします。

ハードウェア更新の場合のみ: 新しいホスト ハードウェアに追加されたディスク領域の使用

新しいハードウェアで使用可能なディスク領域をすべて使用する方法については、『RSA NetWitness Platformコア データベース チューニング ガイド』を参照してください。RSA NetWitness Platform 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。

Azure導入環境での災害復旧

このセクションでは、Azure仮想ホスト(VMとも記載)に導入されたNetWitness Platform 11.xのバックアップとリストアの方法について説明します。Azure導入環境での11.xのバックアップおよびリストアには、次の2つの主要なタスクが含まれます。

- タスク 1 - データのバックアップとエクスポート
- タスク 2 - データのリストアとインポート

タスク 1 - データのバックアップとエクスポート

1. `nw-recovery-tool --export`コマンドを実行して、データをエクスポートします。この手順は、このドキュメントの「災害復旧(バックアップとリストアの手順)」で説明しています。

タスク 2 - データのリストアとインポート

このタスクを完了するには、『10.6.6.x to 11.3 Azureアップグレード ガイド』を参照する必要があります。RSA NetWitness Platform 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。

1. VMを削除します。

   注意: リソース(例えば、ディスク、ネットワーク インタフェースなど)は削除しないでください。

2. NW Serverホスト、Brokerホスト、ESAホスト、Endpoint Log Hybridホスト、Log Collectorホスト(ホスト = `--category`)で、次の手順を実行します。

   a. 古い11.6 VMから、ネットワーク インタフェース カードを除くすべてのリソースを削除します。

   b. 同じディスクとリソースを使用して11.6 VMを新規に導入し、パワーオフします。
   新しい仮想ホストをAzureに導入する詳しい手順については、『Azureインストール ガイド』を参照してください。

   c. ローカル マシンで、`azure-mac-retention.ps1`を実行します。
   このスクリプトを実行する手順については、『*10.6.6 to 11.3 Azure Upgrade Guide*』を参照してください。

   d. それぞれのホストのNRTリストアの手順に従います。詳細は、「災害復旧(バックアップとリストアの手順)」に記載されています。

   e. NRTによるコンポーネント ホストのリストアが完了したら、バックアップの <dump-dir>/unmanaged フォルダから次のファイルをリストアします。

      - `/etc/fstab`
      - `/etc/hosts`(ホスト名が変更されていない場合)
      - `/etc/waagent.conf`

- /etc/logrotate.d/waagent.logrotate
- /etc/krb5.conf (<dump-dir>/unmanagedフォルダから)

3. Log Decoderホスト、Concentratorホスト、Archiverホスト(ホスト = --category) で、次の手順を実行します。
   a. 古い11.6 VMから、**external**という名前のディスクおよびネットワーク インタフェース カードを除くすべてのリソースを削除します。
   b. 同じディスクとリソースを使用して11.6 VMを新規に導入し、パワーオフします。新しいVMをAzureに導入する手順については、『Azureインストール ガイド』を参照してください。

      注 : externalディスクは作成しないでください。nwhomeディスクのみを作成します。

   c. ローカル マシンで、azure-mac-retention.ps1を実行します。
      このスクリプトを実行する手順については、『*10.6.6 to 11.3 Azure Upgrade Guide*』を参照してください。
   d. 「コンポーネント ホストでのデータのリストア」の手順に従い、各ホストでNRTを実行し、データをリストアします。
   e. NRTによるコンポーネント ホストのリストアが完了したら、バックアップの <dump-dir>/unmanaged フォルダから次のファイルをリストアします。
      - etc/fstab
      - /etc/hosts(ホスト名が変更されていない場合)
      - /etc/waagent.conf
      - etc/logrotate.d/waagent.logrotate
      - /etc/krb5.conf

AWS導入環境での災害復旧

このセクションでは、AWS仮想ホスト(VMとも記載)に導入されたNetWitness Platform 11.xのバックアップとリストアの方法について説明します。AWS導入環境での11.xのバックアップおよびリストアには、次の2つの主要なタスクが含まれます。

- タスク 1 - データのバックアップとエクスポート
- タスク 2 - データのリストアとインポート

タスク 1 - データのバックアップとエクスポート

1. `nw-recovery-tool --export`コマンドを実行して、データをエクスポートします。この手順は、このドキュメントの「災害復旧(バックアップとリストアの手順)」で説明しています。
2. IPアドレスを記録します。これは、後で災害復旧手順を参照する必要があります。IPアドレスを保持する方法については、『AWSアップグレード ガイド(10.6.6から11.3)』を参照してください。RSA NetWitness Platform 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

タスク 2 - データのリストアとインポート

このタスクを完了するには、『*AWSアップグレード ガイド(10.6.6から11.3)*』を参照する必要があります。

1. VMを削除します。

   注意: リソースは削除しないでください(たとえば、ディスクは削除しないでください)。

2. NW Serverホスト、Brokerホスト、ESA(プライマリ/セカンダリ)ホスト、Endpoint Log Hybridホスト、Log Collectorホスト(ホスト = `--category`)で、次の手順を実行します。

   a. 古い11.6 VMから、すべてのリソースを削除します。

   b. 同じIPアドレス、ディスク、リソースを使用して、11.6 VMを新規に導入し、パワーオフします。新しい仮想ホストをAWSに導入する手順については、『AWSインストール ガイド』を参照してください。

   c. 「コンポーネント ホストでのデータのリストア」の手順に従い、各ホストでNRTを実行し、データをリストアします。

   d. NRTによるコンポーネント ホストのリストアが完了したら、バックアップの <dump-dir>/unmanaged フォルダから次のファイルをリストアします。

      - `/etc/fstab`
      - `/etc/hosts`(ホスト名が変更されていない場合)

3. Log Decoderホスト、Decoder(Network Decoder)ホスト、Concentratorホスト、Archiverホスト(ホスト = `--category`)で、次の手順を実行します。

a. 古い11.6 VMから、**external**ディスクを除くすべてのリソースを削除します。

b. 同じIPアドレス、ディスク、リソース(『AWSインストール ガイド』に記載)を使用して11.6 VMを新規に導入し、パワーオフします。

> **注：** **external**ディスクは作成しないでください。**nwhome**ディスクのみを作成します。

c. 「コンポーネント ホストでのデータのリストア」の手順に従い、各ホストでNRTを実行し、データをリストアします。

d. NRTによるコンポーネント ホストのリストアが完了したら、バックアップの <dump-dir>/unmanaged フォルダから次のファイルをリストアします。

- `etc/fstab`
- `/etc/hosts`(ホスト名が変更されていない場合)
- `/etc/krb5.conf`

付録 A.復旧後のシリーズ5および6 Hybridでのfstabの変更

注: この付録の手順は、Hybridハードウェアに11.4を新規インストールしたホストで障害が発生した場合、実行する必要はありません。

シリーズ5またはシリーズ6のNetwork Hybridで、11.2.x.x.または11.3.x.x.から11.4にアップグレードし、障害が発生した場合、復旧時にシリーズ5またはシリーズ6 Hybridの`/etc/fstab`ファイルを変更する必要があります。

災害復旧シナリオでの復旧タスクは以下のようになります。

1. 新しいシリーズ5またはシリーズ6 Hybridを、11.4のISOを使用し、Network Hybridとして再イメージ化します。
2. バックアップしたデータと構成をインポートします(`nw-recovery-tool --import`)。
3. 復旧した`/etc/fstab`ファイルを手動で変更します。

障害発生前のetc/fstabファイルの例

11.4にアップグレードしたシリーズ5またはシリーズ6 Hybridの外部ストレージ構成のバックアップの例を示します。

黄色で色付けされた部分はアップグレードされたシステムの内部ストレージです。この構成は、アップグレード時に、前リリースから引き継がれます。内部ストレージのレイアウトは11.4(新規インストール)で変更されました。このため、災害復旧時には、外部ストレージに関する部分(緑色で色付け)だけを、新しい`etc/fstab`ファイルにコピーする必要があります。

`nw-recovery-tool --export`コマンドを使用してデータまたは構成をエクスポートすると、ストレージの構成は、`<back-location>/unmanaged/etc/fstab`に保存されます。この`fstab`ファイルには、内部ストレージ(黄色で色付け)と外部ストレージ(緑色で色付け)の両方の構成が含まれます。10.6または11.xから11.4にアップグレードされたシリーズ5またはシリーズ6のNetwork Hybridのfstabファイルには、次の例のようなストレージ構成が含まれます。

```
/dev/mapper/netwitness_vg00-root / xfs defaults 0 0 UUID=906e2a3d-3b59-46d1-
975d-fa2b8467d009
/boot xfs defaults 0 0 /dev/mapper/netwitness_vg00-usrhome
/home xfs nosuid 0 0
/dev/mapper/netwitness_vg00-varlog /var/log xfs defaults 0 0
/dev/mapper/netwitness_vg00-nwhome /var/netwitness xfs nosuid,noatime 0 0
/dev/mapper/concentrator-vlnwc /var/netwitness/concentrator xfs noatime,nosuid
0 0
/dev/mapper/index-vlnwci /var/netwitness/concentrator/index xfs noatime,nosuid
0 0
/dev/mapper/concentrator-vlnwcm /var/netwitness/concentrator/metadb xfs
noatime,nosuid 0 0
/dev/mapper/concentrator-vlnwcs /var/netwitness/concentrator/sessiondb xfs
noatime,nosuid 0 0
/dev/mapper/decoderpacket-vlnwd /var/netwitness/decoder xfs noatime,nosuid 0 0
/dev/mapper/decoderpacket-vlnwdi /var/netwitness/decoder/index xfs
noatime,nosuid 0 0
```

```
/dev/mapper/decodermeta-vlnwdm /var/netwitness/decoder/metadb xfs
noatime,nosuid 0 0
/dev/mapper/decoderpacket-vlnwdp /var/netwitness/decoder/packetdb xfs
noatime,nosuid 0 0
/dev/mapper/decoderpacket-vlnwds /var/netwitness/decoder/sessiondb xfs
noatime,nosuid 0 0
/dev/mapper/netwitness_vg00-swap swap swap defaults 0 0
/var/netwitness/decoder /var/netwitness/logdecoder none defaults,rbind 0 0
/dev/concentrator0/sessiondb /var/netwitness/concentrator/sessiondb0 xfs
noatime,nosuid 1 2
/dev/concentrator0/metadb /var/netwitness/concentrator/metadb0 xfs
noatime,nosuid 1 2
/dev/decoder0/packetdb /var/netwitness/decoder/packetdb0 xfs noatime,nosuid 1
```

復旧後のetc/fstabファイルの例 - 変更前

11.4 ISOを使用して11.4をインストールした後、リカバリツールを実行して以前の構成をリストアすると、/etc/fstabファイルは次の例のようになります。

```
#
# /etc/fstab
# Created by anaconda on Thu Dec 5 17:31:26 2019
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/netwitness_vg00-root / xfs defaults 0 0
UUID=d84db66c-fce6-4fec-9f84-b3449861f664 /boot xfs defaults 0 0
/dev/mapper/netwitness_vg00-usrhome /home xfs nosuid 0 0
/dev/mapper/netwitness_vg00-varlog /var/log xfs defaults 0 0
/dev/mapper/netwitness_vg00-nwhome /var/netwitness xfs nosuid,noatime 0 0
/dev/mapper/netwitness_vg00-swap swap swap defaults 0 0
/dev/hybrid-decoder-meta/decoroot /var/netwitness/decoder xfs noatime,nosuid 1
2
/dev/packet/packetdb /var/netwitness/decoder/packetdb xfs noatime,nosuid 1 2
/dev/hybrid-concentrator/root /var/netwitness/concentrator xfs noatime,nosuid
1 2
/dev/index/index /var/netwitness/concentrator/index xfs noatime,nosuid 1 2
```

注: 外部ストレージの構成が含まれていないことがわかります。前段の外部ストレージ構成(緑色で色付け)を新しく導入したHybridの/etc/fstabファイルに追加する必要があります。

復旧後のetc/fstabファイルの例 - 変更後

更新後の/etc/fstabは次の例のようになります。

```
#
# /etc/fstab
# Created by anaconda on Thu Dec 5 17:31:26 2019
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/netwitness_vg00-root / xfs defaults 0 0
UUID=d84db66c-fce6-4fec-9f84-b3449861f664 /boot xfs defaults 0 0
/dev/mapper/netwitness_vg00-usrhome /home xfs nosuid 0 0
/dev/mapper/netwitness_vg00-varlog /var/log xfs defaults 0 0
/dev/mapper/netwitness_vg00-nwhome /var/netwitness xfs nosuid,noatime 0 0
/dev/mapper/netwitness_vg00-swap swap swap defaults 0 0
/dev/hybrid-decoder-meta/decoroot /var/netwitness/decoder xfs noatime,nosuid 1
2
/dev/packet/packetdb /var/netwitness/decoder/packetdb xfs noatime,nosuid 1 2
/dev/hybrid-concentrator/root /var/netwitness/concentrator xfs noatime,nosuid
1 2
/dev/index/index /var/netwitness/concentrator/index xfs noatime,nosuid 1 2
/dev/concentrator0/sessiondb /var/netwitness/concentrator/sessiondb0 xfs
noatime,nosuid 1 2
/dev/concentrator0/metadb /var/netwitness/concentrator/metadb0 xfs
noatime,nosuid 1 2
/dev/decoder0/packetdb /var/netwitness/decoder/packetdb0 xfs noatime,nosuid 1
```