NetWitness® Platform

バージョン12.4

リカバリ ツール ユーザ ガイド

NETWITNESS
Platform

連絡先

NetWitnessコミュニティ(https://community.netwitness.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およびその他の商標は、RSA Security LLCまたはその関連会社(「RSA」) の商標または登録商標です。RSAの商標のリストについては、https://www.rsa.com/en-us/company/rsa-trademarksを参照してください。その他の商標は、それぞれの所有者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、NetWitnessコミュニティ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、本製品のユーザーは、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。

ディストリビューション

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

この資料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は、この資料に記載される情報に関する、どのような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への適応性に対する黙示的保証はいたしません。

その他

この製品、このソフトウェア、関連ドキュメント、およびコンテンツには、このドキュメントの発行日の時点で有効なNetWitnessの標準利用規約が適用されます。利用規約は https://www.netwitness.com/standard-form-agreements/でご確認いただけます。

2024年3月

目次

災害復旧(バックアップとリストアの手順)

NetWitnessホストのバックアップとリストアは、次のいずれかを使用して実行できます。

- (推奨) NetWitnessリカバリー ラッパー ツール
- NetWitnessリカバリー ツール(NRT)

(推奨) NetWitnessリカバリー ラッパー ツール

注:NetWitnessリカバリー ラッパー ツールはNetWitness11.6.1.4以降でサポートされています。(500 GBを超える)大量のデータを処理するホストの場合は、NetWitnessリカバリー ツール(`nw-recovery-tool`)を使用してバックアップすることをお勧めします。

NetWitnessリカバリー ラッパー ツール(NRWT)は、サポートされているすべてのインストール オプション(物理ホスト、仮想ホスト、AWS、およびAzure)のバックアップを簡単に作成できる一元的なバックアップおよびリストア ツールです。

NRWTの機能は次のとおりです。

- 一度に個々のホスト、特定のホスト、またはすべてのホストをバックアップ(エクスポート)する。
- 一度に個々のホストをリストア(インポート)する。
- バックアップとリストアに含めるファイルまたはフォルダーをカスタマイズする。
- バックアップ データをリモート ホストとNetwitnessホストの間でコピーする(次の条件を満たす場合)。
  - リモート ホストに各NetWitnessホストからSSH経由でアクセスできる。
  - 認証情報が正しい。
  - 指定された場所にバックアップを格納する十分な空き領域がある(エクスポートの場合)。

- 指定された場所に有効なバックアップ データがある(インポートの場合) 。

- (バージョン11.7.1以降の場合) EndpointおよびESAインスタンスのMongoデータベースをバックアップする。
- (バージョン11.7.1以降の場合) Brokerサービスが実行されているNetWitnessノードのBrokerインデックスを含む。
- (バージョン11.7.1以降の場合) ユーザーが提供したカスタムのフィールドとフォルダーをバックアップする。
- (バージョン12.3以降の場合) データのエクスポート中およびインポート中には、コマンド ライン インターフェイス(CLI) にパスワードを入力しないでください。
- (オプション) (バージョン12.3以降の場合) NetWitness Server、またはその他のコンポーネント ホスト システムに非rootユーザーとしてログインし、データのバックアップとリカバリーを実行します。NetWitness Server、またはその他のコンポーネント ホスト システムにログインするには、次のログイン認証情報を使用する必要があります。
  - ユーザー名 :**nwnrt**
  - パスワード :**netwitness**

  注 : NetWitness Server、またはその他のコンポーネント ホスト システムに非rootユーザーとしてログインするために、rootユーザーは、**su nwnrt**というユーザー名を使用する必要があります。
- (バージョン12.3以降の場合) グループ ホストとカテゴリー ホストをバックアップします。

以前の実行の詳細については、管理サーバーの`/var/log/netwitness/recovery-tool/nw-recovery-wrapper.log`にあるNRWTのログで確認できます。

NetWitnessリカバリー ラッパー ツールの基本的な使用方法

NRWT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-wrapper [command] [option]
```

このツールで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。以下に例を示します。 指定した次のコマンド：nw-recovery-wrapper --helpを実行すると、サポートされている操作と引数の一覧が表示されます。
-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)。
--host-key HOST_KEY [HOST_KEY ...]	ホストIP、ID、または表示名を指定します。
--host-all	すべてのホストに指定します(エクスポートでのみサポートされます)。
--category-group CATEGORY_GROUP [CATEGORY_GROUP ...]	ホスト グループとサービス グループに指定します(エクスポートでのみサポートされます)。
--host-group HOST_GROUP [HOST_GROUP ...]	UIホスト ページで作成されたホスト グループを指定します(エクスポートでのみサポートされます)。
--include CUSTOM_PATH [CUSTOM_PATH ...]	カスタムパスまたはファイルを指定します。

コマンドとオプション	説明
--remote-location REMOTE_LOCATION	リモート ホスト構成のリモート ホストのパスを指定します。
--remote-ip REMOTE_IP	リモート ホスト構成のリモート ホストのIPを指定します。
--remote-password REMOTE_PASSWORD	リモート ホスト構成のリモート ホストのパスワードを指定します。
--remote-user REMOTE_USER	リモート ホスト構成のユーザーを指定します。 (オプション) リモート ホスト構成のユーザー。指定しない場合は、デフォルトのrootユーザーです。

前提条件

- 各NetWitnessホストでバックアップを行うために十分なディスク領域がダンプ ディレクトリーに存在することを確認してください。
- 有効なホスト キーを入力します。ホスト キーとして指定できるのは、ホストID、IPアドレス、または表示名です。

NRTラッパーを使用したバックアップ：

1. NetWitnessホストのバックアップを作成し、各ホストのローカル ダンプ ディレクトリーに格納します。

```
nw-recovery-wrapper export --dump-dir <dir> --host-key <Host 1 IP/ID/Name>
<Host 2 IP/ID/Name>......<Host N IP/ID/Name>

nw-recovery-wrapper export --dump-dir <dir> --host-all
```

> **注 :nwnrtまたはsu nwnrtというユーザー名でログインしている場合は、NetWitness Serverホストまたはその他のコンポーネント ホストでNetWitnessリカバリー ラッパー ツールを使用してバックアップ/リカバリー アクションを実行している間に実行するコマンドの前にsudoと入力する必要があります。**
> **例 :NetWitnessリカバリー ラッパー ツールを使用してNetWitnessホストをバックアップするための最初のステップは、ログイン後に、次のコマンドを実行することです。**

```
sudo nw-recovery-wrapper export --dump-dir <dir> --host-key <Host 1
IP/ID/Name> <Host 2 IP/ID/Name>......<Host N IP/ID/Name>
```

2. (オプション) リカバリー ツールで事前定義されているもの以外でバックアップとリストアに含めるカスタムのファイルまたはフォルダーを追加します。

> **注 :カスタムのファイルまたはディレクトリがNetWitnessホストで利用できることを確認してください。利用できない場合、それらのファイルまたはディレクトリは無視されます。**

```
nw-recovery-wrapper export --dump-dir <dir> --include-file <custom files>/-
-include-dir --host-key <Host 1 IP/ID/Name> <Host 2 IP/ID/Name>......<Host
N IP/ID/Name>
nw-recovery-wrapper export --dump-dir <dir> --include-file <custom files>/-
-include-dir --host-all
```

3. (オプション) バックアップ データをリモートにコピーします。

注 :次の情報を確認します。
- リモート コピー操作の引数、--remote-ip、--remote-locationに有効な値が指定されていること。
- リモート ホストのIPが有効であり、すべてのNetWitnessホストからSSH経由でアクセスできること。
- リモート ホストの場所(--remote-location) に、バックアップを格納する十分な領域があること。

```
nw-recovery-wrapper export --dump-dir <dir> --host-key <Host 1 IP/ID/Name>
<Host 2 IP/ID/Name>......<Host N IP/ID/Name> --remote-ip <IP ADDRESS of
remote host> --remote-location <remote-location-where-backups-should-be-
copied-to>
nw-recovery-wrapper export --dump-dir <dir> --host-all --remote-ip <IP
ADDRESS of remote host> --remote-location <remote-location-where-backups-
should-be-copied-to>
```

注 :
- オプションの引数--remote-userの値を指定しなかった場合は、デフォルトのrootになります。
- 引数が指定されていない場合は、オプションの引数--remote-password <remote-password>でsshキーが使用されます。

注 :パスワードなしでエクスポートを実行するには、すべてのNetWitnessノードで、次の手順を実行します。
1. ssh-keygen(パスフレーズなし)
2. ssh-copy-id <remote - username>@<remote - ip>
ステップ3を実行してSSH接続を確認し、リモート マシンを終了します。
3.ssh <remote - username>@<remote - ip>

例 :

adminserverの場合、バックアップ フォルダーの名前は「adminserver-backup-2021-09-08-12:48:13」のようになります。

4. カスタムファイルまたはフォルダーを含むバックアップ(エクスポート) を作成し、リモートにコピーします。

注 :次の情報を確認します。
- カスタムのファイルまたはディレクトリーがNetWitnessホストで使用可能であること(使用できない場合は、それらのファイルまたはディレクトリーが無視されます) 。
- 有効な値が、リモート コピー操作の引数、--remote-ip、--remote-locationに指定されていること。
- リモート ホストのIPが有効で、すべてのNetWitnessホストからSSH経由でアクセスできること。
- リモート ホストの場所(--remote-location) に、バックアップを格納する十分な領域があること。

```
nw-recovery-wrapper export --dump-dir <dir> --include <custom files/folder>
--host-key <Host 1 IP/ID/Name> <Host 2 IP/ID/Name>......<Host N IP/ID/Name>
--remote-ip <IP ADDRESS of remote host> --remote-location <remote-location-
where-backups-should-be-copied-to>
```

```
nw-recovery-wrapper export --dump-dir <dir> --include <custom files/folder>
--host-all --remote-ip <IP ADDRESS of remote host> --remote-location
<remote-location-where-backups-should-be-copied-to>
```

注：
- オプションの引数 :引数を指定しなかった場合は、`--remote-user`が、デフォルトのrootになります。
- 引数が指定されていない場合は、オプションの引数`--remote-password <remote-password>`でsshキーが使用されます。

注 :パスワードなしでエクスポートを実行するには、すべてのNetWitnessノードで、次の手順を実行します。
1. ssh-keygen(パスフレーズなし)
2. ssh-copy-id <remote - username>@<remote - ip>

ステップ3を実行してSSH接続を確認し、リモート マシンを終了します。
3.ssh <remote - username>@<remote - ip>

例：

Admin Serverの場合は、バックアップ フォルダーの名前が「adminserver-backup-2021-09-08-12:48:13」になります。

5. (バージョン11.7.1以降の場合) (オプション) Mongoサービスを含めます。

注 :以下を確認します。
- MongoサービスがNetWitnessホストで実行中である。
- 複数の値を含む`--host-all and --host-key`は、Mongoを含める操作ではサポートされていません。

```
nw-recovery-wrapper export --dump-dir <dir> --host-key <Host 1 IP/ID/Name>
--include-mongo
```

6. (バージョン11.7.1以降の場合) (オプション) Brokerインデックスを含めます。

注 :以下を確認します。
- BrokerサービスがNetWitnessホストで実行中である。

```
nw-recovery-wrapper export --dump-dir <dir> --host-key <Host 1 IP/ID/Name>
<Host 2 IP/ID/Name>......<Host N IP/ID/Name> --include-broker-index
```

```
nw-recovery-wrapper export --dump-dir <dir> --host-all --include-broker-
index
```

7. (バージョン11.7.1以降の場合) (オプション) MongoおよびBrokerインデックスを含めてバックアップ(エクスポート)します。

注 :以下を確認します。
- MongoサービスがNetWitnessホストで実行中である。
- BrokerサービスがNetWitnessホストで実行中である。
- 複数の値を含む`--host-all and --host-key`は、Mongoを含める操作ではサポートされていません。

```
nw-recovery-wrapper export --dump-dir <dir> --host-key <Host 1 IP/ID/Name>
--include-mongo --include-broker-index
```

8. (バージョン11.7.1以降の場合) (オプション) リモートの場所、Brokerインデックス、Mongoにコピーして、カスタムのファイルやフォルダーを含めてバックアップ(エクスポート)します。

```
nw-recovery-wrapper export --dump-dir <dir> --include-broker-index --
include-mongo ---include-file <custom files>/--include-dir <custom folders>
--host-key <Host 1 IP/ID/Name> --remote-ip <IP ADDRESS of remote host> --
remote-location <remote-location-where-backups-should-be-copied-to>
```

注 :パスワードなしでエクスポートを実行するには、すべてのNetWitnessノードで、次の手順を実行します。
1. ssh-keygen(パスフレーズなし)
2. ssh-copy-id <remote - username>@<remote - ip>
ステップ3を実行してSSH接続を確認し、リモート マシンを終了します。
3.ssh <remote - username>@<remote - ip>

9. (バージョン12.3以降の場合) `/admin/appliances`ページで作成された特定のグループに固有のすべてのホストをバックアップします。

```
nw-recovery-wrapper export --dump-dir <dump location> --host-group <UI host
group>
```

例 :

```
nw-recovery-wrapper export --dump-dir /var/netwitness/Test-backup --host-
group TestGroup
```

10. (バージョン12.3以降の場合) 環境内のLog Hybrid、Log Collector、スタンドアロンBrokerなど、特定のカテゴリーに固有のすべてのホストをバックアップします。

```
nw-recovery-wrapper export --dump-dir <dump location> --category-group
<category name>
```

例：

```
nw-recovery-wrapper export --dump-dir /var/netwitness/Test-backup --
category-group LogDecoder
```

注 :以下を確認します。
- カスタムのファイルまたはディレクトリーが、バックアップされるNetWitnessホストに存在すること。存在しない場合は、そのファイルまたはディレクトリーがスキップされます。
- `--remote-ip`、`--remote-location`などのフィールドがリモート コピー操作で必須であること。
- リモート ホストIP認証情報が有効であり、すべてのNetWitnessホストからSSH経由でアクセス可能であること。
- リモート ホストの場所(`--remote-location`) に、バックアップの格納に十分なスペースがあること。
- MongoサービスがNetWitnessホストで実行中であること。
- BrokerサービスがNetWitnessホストで実行中であること。
- 複数の値を含む`--host-all`,`--host-key`、`--category-group`、`--host-group`は、Mongoのinclude操作ではサポートされていません。
- 引数が指定されていない場合は、オプションの引数`--remote-password <remote-password>`でsshキーが使用されます。

NRTラッパーでサポートされるリストア(インポート) オプション

注意 :システム レベルの変更を伴うため、インポート コマンドは慎重に使用してください。

1. ホストを一度に1つずつリストア(インポート) します(IPアドレス、ホスト名、またはホストIDを使用) 。
   `nw-recovery-wrapper import --dump-dir <dir> --host-key <Host IP/ID/Name>`
2. カスタムのファイルまたはフォルダーをリストアします(該当する場合) 。

   注 :カスタムのファイルまたはディレクトリがNetWitnessホストで利用できることを確認してください。利用できない場合、それらのファイルまたはディレクトリは無視されます。

   ```
   nw-recovery-wrapper import --dump-dir <dir> --include-file <custom files>/-
   -include-dir --host-key <Host IP/ID/Name>
   ```

3. リモートの場所からリストアします。

   注 :次の情報を確認します。
   - データがバックアップされているリモート ホストの場所が`--remote-location`で指定されている。
   - リモート ホストのIPが有効で、すべてのNetWitnessホストからSSH経由でアクセスできる。
   - リモート ホストの場所(`--remote-location`) に、バックアップの格納に十分な領域がある。

```
nw-recovery-wrapper import --remote-ip <IP address of remote host> --
remote-location <location-of-backup-on-remote-host> --dump-dir <dir> --
host-key <Host IP/ID/Name>
```

注：
- オプションの引数：引数を指定しない場合は、`--remote-user`がデフォルトでrootになります。
- 引数が指定されていない場合は、オプションの引数`--remote-password <remote-password>`でsshキーが使用されます。

注：パスワードなしのインポートを実行するには、すべてのNetWitnessノードで、次のステップを実行します。
1. ssh-keygen(パスフレーズなし)
2. ssh-copy-id <remote - username>@<remote - ip>

ステップ3を実行してSSH接続を確認し、リモート マシンを終了します。
3.ssh <remote - username>@<remote - ip>

たとえば、adminserverの場合、バックアップ フォルダーの名前は「adminserver-backup-2021-09-08-12:48:13」のようにします。

```
nw-recovery-wrapper import --dump-directory <dir> --host-key <host-1> --
remote-ip <remote-ip> --remote-location /home/adminserver-backup-2021-09-
08-12:48:13
```

注：
- オプションの引数：引数を指定しなかった場合は、`--remote-user`が、デフォルトのrootになります。
- 引数が指定されていない場合は、オプションの引数`--remote-password <remote-password>`でsshキーが使用されます。

4.

注：パスワードなしのインポートを実行するには、すべてのNetWitnessノードで、次のステップを実行します。
1. ssh-keygen(パスフレーズなし)
2. ssh-copy-id <remote - username>@<remote - ip>

ステップ3を実行してSSH接続を確認し、リモート マシンを終了します。
3.ssh <remote - username>@<remote - ip>

5.

カスタムのファイルまたはフォルダーを含むリモートの場所からデータをリストアします。

注：次の情報を確認します。
- カスタムファイルまたはディレクトリーがNetWitnessホストで使用可能である(使用不可の場合は、そのファイルやディレクトリーが無視されます) 。
- データがバックアップされるリモート ホストの場所が`--remote-location`に含まれている。
- リモート ホストのIPが有効で、すべてのNetWitnessホストからSSH経由でアクセスできる。
- リモート ホストの場所(`--remote-location`) に、バックアップの格納に十分な領域がある。

```
nw-recovery-wrapper import --dump-dir <dir> --include <custom files/folder>
--host-key <host1> --remote-ip <IP ADDRESS of remote host> --remote-
location <remote-location-where-backups-should-be-copied-to>
```

たとえば、管理サーバーの場合、バックアップ フォルダーの名前は「adminserver-backup-2021-09-08-12:48:13」のようになります。

注：
- オプションの引数 :引数を指定しなかった場合は、`--remote-user`が、デフォルトのrootになります。
- 引数が指定されていない場合は、オプションの引数`--remote-password <remote-password>`でsshキーが使用されます。

6.

注 :パスワードなしのインポートを実行するには、すべてのNetWitnessノードで、次のステップを実行します。
1. ssh-keygen(パスフレーズなし)
2. ssh-copy-id <remote - username>@<remote - ip>
ステップ3を実行してSSH接続を確認し、リモート マシンを終了します。
3.ssh <remote - username>@<remote - ip>

7.

(バージョン11.7.1以降の場合) (オプション) Mongoサービスをリストアします。

注 :以下を確認します。
- MongoサービスがNetWitnessホストで実行中である。
- 複数の値を含む`--host-all and --host-key`は、Mongoを含める操作ではサポートされていません。

```
nw-recovery-wrapper import --dump-dir <dir> --host-key <Host 1 IP/ID/Name>
--include-mongo
```

8.

(バージョン11.7.1以降の場合) (オプション) Brokerインデックスをリストアします。

注 :以下を確認します。
- BrokerサービスがNetWitnessホストで実行中である。
- `--host-all option is not support for include broker index operation`。

```
nw-recovery-wrapper import --dump-dir <dir> --host-key <Host 1 IP/ID/Name>
--include-broker-index
```

9.

(バージョン11.7.1以降の場合) (オプション) MongoおよびBrokerインデックスをリストアします。

注 :以 下を確 認します。
- MongoサービスがNetWitnessホスト で実 行 中 である。
- BrokerサービスがNetWitnessホスト で実 行 中 である。
- 複 数 の値 を含 む`--host-all and --host-key`は、Mongoを含 める操 作 ではサポート されて いません。

```
nw-recovery-wrapper import --dump-dir <dir> --host-key <Host 1 IP/ID/Name>
--include-mongo --include-broker-index
```

10. (バージョン11.7.1以 降 の場 合) (オプション) リモート の場 所 、Brokerインデックス、Mongoにコピーし て、カスタムのファイルやフォルダーをリスト アします。

注 :以 下を確 認します。
- カスタムのファイルまたはディレクト リーが、バックアップされるNetWitnessホスト に存 在 すること。存 在しない場 合 は、そのファイルまたはディレクト リーのバックアップがスキップされます。
- `--remote-ip`、`--remote-location`などのフィールド がリモート コピー操 作 で必 須 であること。
- リモート ホストIP認 証 情 報 が有 効 であり、すべてのNetWitnessホスト からSSH経 由 でアクセス可 能 であること。
- リモート ホスト の場 所 (`--remote-location`) に、バックアップの格 納 に十 分 なスペースがあるこ と。
- MongoサービスがNetWitnessホスト で実 行 中 である。
- BrokerサービスがNetWitnessホスト で実 行 中 である。
- 複 数 の値 を含 む`--host-all and --host-key`は、Mongoを含 める操 作 ではサポート されて いません。

```
nw-recovery-wrapper import --dump-dir <dir> --include-file <custom files>/-
-include-dir <custom folders> --include-mongo --include-broker-index --
host-key <host1> --remote-ip <IP ADDRESS of remote host> --remote-location
<remote-location-where-backups-should-be-copied-to>
```

注 :
- オプションの引 数 :引 数 を指 定しなかった場 合 は、`--remote-user`が、デフォルト のrootになりま す。
- 引 数 が指 定されていない場 合 は、オプションの引 数 `--remote-password <remote-password>`でsshキーが使 用されます。

注 :パスワードなしのインポート を実 行 するには、すべてのNetWitnessノード で、次 のステップを実 行します。
1. ssh-keygen(パスフレーズなし)
2. ssh-copy-id <remote - username>@<remote - ip>
ステップ3を実 行してSSH接 続 を確 認し、リモート マシンを終 了します。
3.ssh <remote - username>@<remote - ip>

ステータスのチェック

以 下 のコマンドを使 用して、バックアップまたはリスト アのステータスを確 認 することができます。

`/var/log/netwitness/recovery-tool/recovery.log`

トラブルシューティング

エラー メッセージ	バックアップまたはリストア中にNRTラッパーでエラーが発生しました。
解決策	次のいずれかを実行します。 • バックアップに失敗したホストにログインし、`/var/log/netwitness/recovery-tool/recovery.log`を確認します。 • ノード0でデバッグ モード(`nw-recovery-wrapper -l debug`) で実行し、各ホストのリカバリー ログを取得します。

エラー メッセージ	リモート コピー操作のパスワードが正しくないため、NRTラッパーにエラーが発生します(`--remote-password`) 。
原因	リモート コピーで間違ったパスワードを複数回入力すると、NRWTは失敗します。SFTPでSSHが使用されるため、その間はシステムでのSSHがロックされます。
解決策	しばらく待ってから再試行する必要があります。

エラー メッセージ	特定のホストでの長時間の実行後にNRTラッパーでエラーが発生しますが、バックアップは進行中のままです。たとえば、EndpointまたはESAノードです。
原因	NRTアーキテクチャは、ユーザー データではなく、構成をバックアップするよう設計されています。また、Admin Server(SA) とnodexの間の通信にソルトを使用します。特定のホストに大量のデータが存在するため、ソルト通信がタイムアウトしたときに、この問題が発生します。

解決策	特定のホストにSSHで接続し、`/var/log/netwitness/recovery-tool/recovery.log`でバックアップ ステータスを確認します。 バックアップされるデータが大量である場合は、特定のホストにログインして「nw-recovery-tool」を使用することをお勧めします。

NetWitnessリカバリー ツール(NRT)

NetWitnessリカバリー ツール(NRT) を使用して、NetWitness Serverホスト システム NetWitnessサーバとコンポーネント ホスト システムのデータのバックアップおよびリストアを実行できます。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]
```

このツールで使 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、 指 定した次 のコマンド :`nw-recovery-tool --help-categories` を実 行すると、有 効なすべてのカテゴリ名 のリストが得られます。
`-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`) 。

コマンドとオプション	説明
-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)
--remote-location <path>	リモート バックアップ ファイルのパス。
--remote-ip <IP>	リモート マシンのIP。
--remote-user <name>	リモート マシンのユーザー名、(オプションで) リモート ホスト構成用のユーザー。指定しない場合は、デフォルトのrootユーザーです。
--remote-password <pass>	リモート マシンのパスワード。

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たために、新しいホストを導入する必要がある場合は、元のホストとまったく同じアイデンティティ パラメーター(IPアドレスなど) を、新しいホストに設定し、同一バージョンのNetWitness Suite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、バックアップの格納場所(推奨ディレクトリーは `/var/netwitness/backup`) 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を実行すると、バックアップ(export) とリストア(import) のどちらのプロセス中にも、Malware、Reporting Engine、Postgresqlの各サービスが停止し、再起動されます。

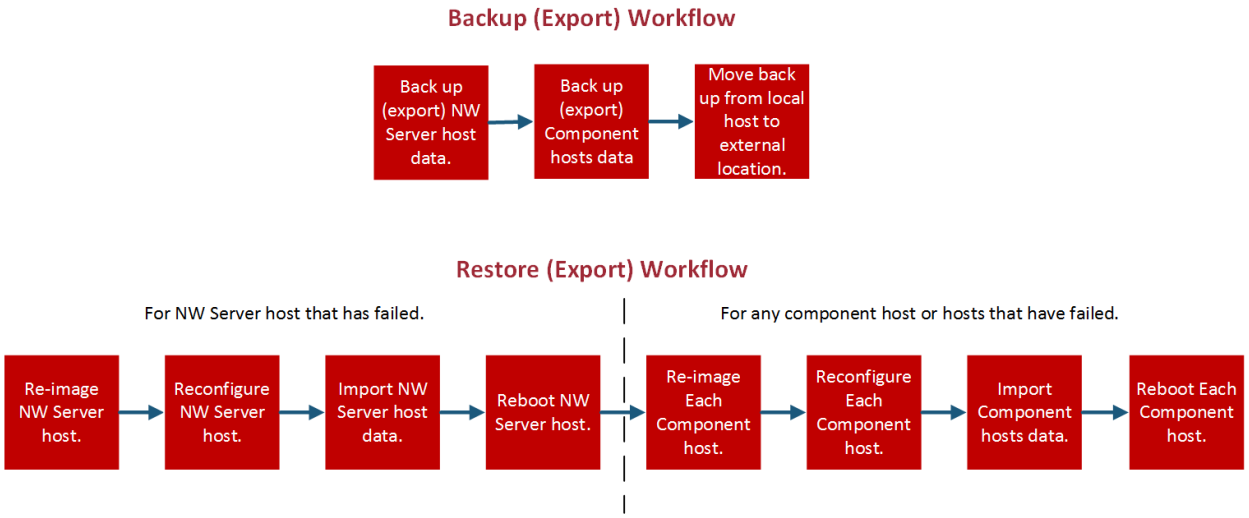
災害復旧のワークフロー

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、以降は可能な限り頻繁に頻度で実行) 。
- 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) 。



ホスト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 システムとコンポーネント ホスト システムで異なります。

注意 :1.) 次のディザスター リカバリー手順の実行中に、ユーザー インターフェイスの [ホスト]ビュー([ (管理)] > [**ホスト**]) でコンポーネント ホスト(つまり、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。

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、稼働中の既存の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レベルで入力します。

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

注 :nwnrtまたは**su nwnrt**というユーザー名でログインしている場合は、NetWitness Serverホストまたはその他のコンポーネント ホストでNetWitnessリカバリー ツールを使用してバックアップ/リカバリー アクションを実行している間に実行するコマンドの前に**sudo**と入力する必要があります。
例 :NetWitnessリカバリー ツールを使用してNetWitness Serverホスト上のデータをバックアップするための最初のステップは、ログイン後に、次のコマンドを実行することです。

```
sudo 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バックアップファイル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。
4. (オプション) バックアップ データをリモートにコピーします。

注 :次の情報を確認します。
- - リモート コピー操作の引数、`--remote-ip`、`--remote-location`に有効な値が指定されていること。
- リモート ホストのIPが有効であり、すべてのNetWitnessホストからSSH経由でアクセスできること。
- リモート ホストの場所(`--remote-location`) に、バックアップを格納する十分な領域があること。

```
nw-recovery-tool --export --dump-dir /var/netwitness/backup --category
AdminServer --remote-ip <IP ADDRESS of remote host> --remote-location
<remote-location-where-backupsshould-be-copied-to>
```

注 :
- オプションの引数`--remote-user`の値を指定しなかった場合は、デフォルトのrootになります。
- 引数が指定されていない場合は、オプションの引数`--remote-password <remote-password>`でsshキーが使用されます。

注 :パスワードなしでエクスポートを実行するには、すべてのNetWitnessノードで、次の手順を実行します。
1. ssh-keygen(パスフレーズなし)
2. ssh-copy-id <remote - username>@<remote - ip>
ステップ3を実行してSSH接続を確認し、リモート マシンを終了します。
3.ssh <remote - username>@<remote - ip>

NetWitness Serverホストでのデータのリストア

1.
元のホストと同じネットワーク構成を使用してNetWitness Serverホストを再イメージ化します。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 12.4物理ホスト インストール ガイド』の「NetWitnessサーバー(NWサーバー) ホストおよびその他のコンポーネント ホストへの12.4のインストール」を参照してください。

a.
(オプション) バックアップ データを取得する前にネットワーク接続を確立する必要がある場合 (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) 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>
```

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
```

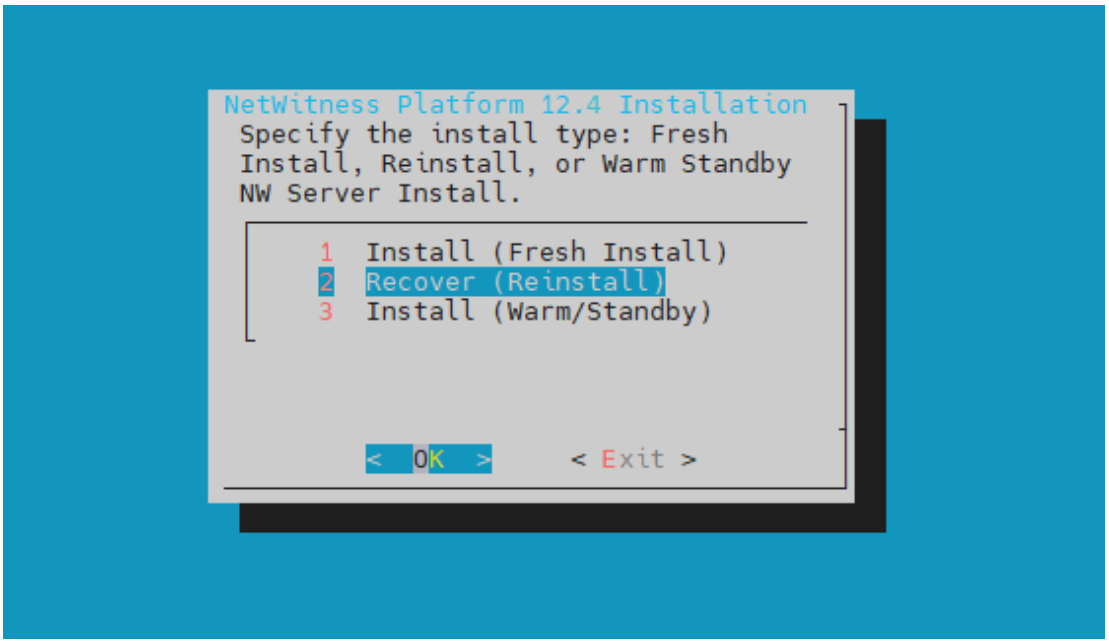
c.
バックアップ データを、ローカル ホスト上のバックアップ ディレクトリのパスに追加します。例 :

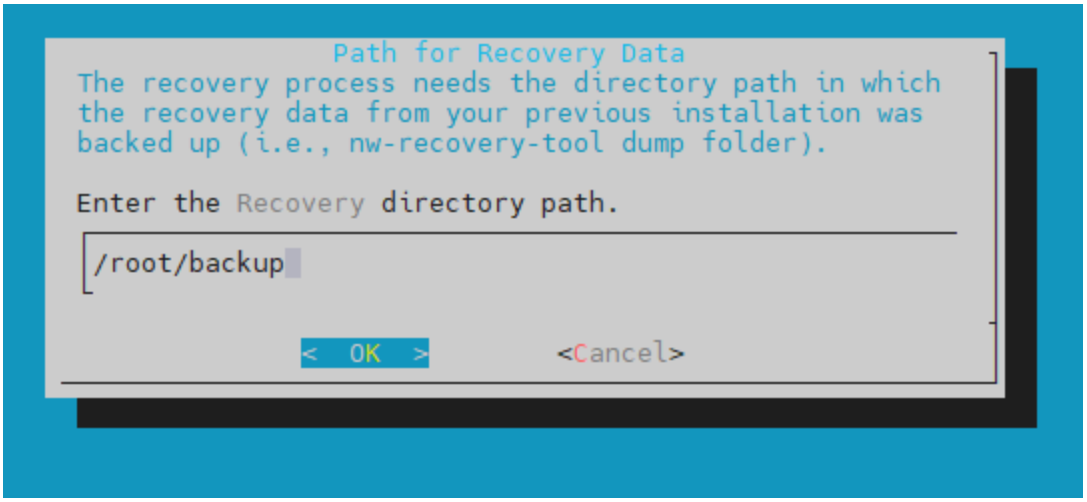
```
/var/netwitness/backup
```

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: プロンプトが表示されたら、インストールタイプのオプションを選択します。** [b>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。





リカバリ パスの場所に指定されるファイル パスはフォルダ構造になっている必要があります。tar.gzファイルまたは圧縮ファイルの場合は、解凍する必要があります。tar.gzファイルは、必要に応じてコマン

ド「`tar -zxvf /root/backup.tar.gz`」を使 用して抽 出 できます。
パスには、`/root/`、`/var/netwitness/backup`、または同 様 のパスを指 定 できます。
admin-server のバックアップ ファイルには、以 下 に示 すフォルダが含 まれます。

```
[root@122-NwAdminTest backup]# ll
total 8
drwxr-xr-x.  5 root root   39 Feb  8 14:13 files
drwxr-xr-x. 17 root root 4096 Feb  8 14:13 mongo
drwxr-xr-x.  2 root root   37 Feb  8 14:14 recovery
drwxr-xr-x.  2 root root   42 Feb  8 14:13 reporting
drwxr-xr-x.  4 root root   43 Feb  8 14:13 sms
drwxr-xr-x.  3 root root   17 Feb  8 14:13 unmanaged
-rw-r--r--.  1 root root    9 Feb  8 14:13 version.info
[root@122-NwAdminTest backup]#
```

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。

- より新 しいパッチ リリースにアップデート されているシステムにデータがある場 合 は、以 前 にホストで実 行 されていたもの(データがバックアップされた正 確 なリリース バージョンまたはパッチ バージョン) と同 じパッチ バージョンの『アップデート ガイド』にある、システムのオフライン アップデート の手 順 に従 って、ホストをアップデート します。

- データが存 在 しているのがメジャー リリース バージョン(12.3など) であり、それ以 降 のパッチ バージョンにアップデート されていない場 合 は、ホスト システムを更 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) リモートの場所からバックアップをリストアします。

注 :次の情報を確認します。
- リモート コピー操作の引数、--remote-ip、--remote-locationに有効な値が指定されていること。
- リモート ホストのIPが有効であり、すべてのNetWitnessホストからSSH経由でアクセスできること。
- リモート ホストの場所(--remote-location) に、バックアップを格納する十分な領域があること。

```
nw-recovery-tool --import --dump-dir /var/netwitness/backup --category
AdminServer --remote-ip <IP ADDRESS of remote host> --remote-location
<location-of-backup-on-remote-host>
```

注 :
- オプションの引数--remote-userの値を指定しなかった場合は、デフォルトのrootになります。
- 引数が指定されていない場合は、オプションの引数--remote-password <remote-password>でsshキーが使用されます。

注 :パスワードなしでエクスポートを実行するには、すべてのNetWitnessノードで、次の手順を実行します。
1. ssh-keygen(パスフレーズなし)
2. ssh-copy-id <remote - username>@<remote - ip>
ステップ3を実行してSSH接続を確認し、リモート マシンを終了します。
3.ssh <remote - username>@<remote - ip>

7. (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のカスタム エントリーを使用する場合：

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7aまたは7b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>
```

8. 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 順を、既 存 の稼 働 中 のコンポーネント ホスト システムで実 行 します。

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レベルで入 力 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 :nwnrtまたはsu nwnrtというユーザー名 でログインしている場 合 は、NetWitness Serverホストまたはその他 のコンポーネント ホストでNetWitnessリカバリー ツールを使 用 してバックアップ/リカバリー アクションを実 行 している間 に実 行 するコマンド の前 にsudoと入 力 する必 要 があります。
   例 :NetWitnessリカバリー ツールを使 用 してコンポーネント ホスト 上 のデータをバックアップするための最 初 のステップは、ログイン後 に、次 のコマンドを実 行 することです。
   `sudo nw-recovery-tool --export --dump-dir /var/netwitness/backup --category <category name>`

   注 :1.) ホスト タイプにー 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) バックアップ データをリモート にコピーします。

   注 :次 の情 報 を確 認 します。
   - リモート コピー操 作 の引 数 、`--remote-ip`、`--remote-location`に有 効 な値 が指 定 されていること。
   - リモート ホスト のIPが有 効 であり、すべてのNetWitnessホスト からSSH経 由 でアクセスできること。
   - リモート ホスト の場 所 (`--remote-location`) に、バックアップを格 納 する十 分 な領 域 があること。

   ```
   nw-recovery-tool --export --dump-dir /var/netwitness/backup --category
   <category name> --remote-ip <IP ADDRESS of remote host> --remote-location
   <remote-location-where-backupsshould-be-copied-to>
   ```

注：
- オプションの引数`--remote-user`の値を指定しなかった場合は、デフォルトのrootになります。
- 引数が指定されていない場合は、オプションの引数`--remote-password <remote-password>`でsshキーが使用されます。

注：パスワードなしでエクスポートを実行するには、すべてのNetWitnessノードで、次の手順を実行します。
1. ssh-keygen(パスフレーズなし)
2. ssh-copy-id <remote - username>@<remote - ip>
ステップ3を実行してSSH接続を確認し、リモート マシンを終了します。
3.ssh <remote - username>@<remote - ip>

3. **(オプション)** `/var/netwitness/backup`を、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 バックアップファイルを保存することはできます。
4. **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`

5. **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。

6. 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 12.4物理ホスト インストール ガイド』の「NetWitnessサーバー(NWサーバー) ホストおよびその他のコンポーネント ホストへの12.4のインストール」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: プロンプトが表示されたら、インストールタイプのオプションを選択します。** [**<b>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。
   リカバリ パスの場所に指定されるファイル パスはフォルダ構造になっている必要があります。tar.gzファイルまたは圧縮ファイルの場合は、解凍する必要があります。tar.gzファイルは、必要に応じてコマンド「`tar -zxvf /root/backup.tar.gz`」を使用して抽出できます。
   パスは、`/root/`、`/var/netwitness/backup`、または任意のパスにすることができます。

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。
   - より新しいパッチ リリースにアップデートされているシステムにデータがある場合は、以前にホストで実行されていたもの(データがバックアップされた正確なリリース バージョンまたはパッチ バージョン) と同じパッチ バージョンの『アップデート ガイド』にある、システムのオフライン アップデートの手順に従ってホストをアップデートします。
   - データが存在しているのがメジャー リリース バージョン(12.3など) であり、それ以降のパッチ バージョンにアップデートされていない場合は、ホスト システム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. (オプション) リモートの場所からバックアップ データをリストアします。

   注 :次の情報を確認します。
   - リモート コピー操作の引数、--remote-ip、--remote-locationに有効な値が指定されていること。
   - リモート ホストのIPが有効であり、すべてのNetWitnessホストからSSH経由でアクセスできること。
   - リモート ホストの場所(--remote-location) に、バックアップを格納する十分な領域があること。

   ```
   nw-recovery-tool --import --dump-dir /var/netwitness/backup --category
   <category name> --remote-ip <IP ADDRESS of remote host> --remote-location
   <location-of-backup-on-remote-host>
   ```

   注 :
   - オプションの引数--remote-userの値を指定しなかった場合は、デフォルトのrootになります。
   - 引数が指定されていない場合は、オプションの引数--remote-password <remote-password>でsshキーが使用されます。

注 :パスワードなしでエクスポートを実行するには、すべてのNetWitnessノードで、次の手順を実行します。
1. ssh-keygen(パスフレーズなし)
2. ssh-copy-id <remote - username>@<remote - ip>
ステップ3を実行してSSH接続を確認し、リモート マシンを終了します。
3.ssh <remote - username>@<remote - ip>

9. **EnpointLogHybrid**および**ESAPrimary**システムの場合は、次のコマンドを実行してアプリケーション 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
   ```
10. **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 データをインポートしてリストアできます。
    ```
    nw-recovery-tool --import --dump-dir /var/netwitness/backup --component postgresql
    ```

11. 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。

    b. <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。

    c. 次のコマンドを各ホストで実行します。

    ```
    mount -a
    ```

12. (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にのカスタム エントリーを追加使用する場合 :

    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12aまたは12b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>
    ```

13. 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、『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。［NetWitnessの全バージョンのドキュメント］ページに移動し、問題のトラブルシューティングのためのNetWitness Platformの各ガイドを見つけます。

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とも呼ばれる)に導入されたNetWitness Platform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導入環境でのデータ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。「NetWitnessの全バージョンのドキュメント」ページに移動し、問題のトラブルシューティングのためのNetWitness Platformの各ガイドを見つけます。

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. ネットワーク インターフェイス カードを除き、古い12.3 VMのリソースをすべて削除します。

   b. 同じディスクとリソースを使用して12.4 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. **external**という名前のディスクおよびネットワーク インターフェイス カードを除き、古い12.3 VMのリソースをすべて削除します。
   b. 同じディスクとリソースを使用して12.4 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導入環境でのデータ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。[NetWitnessの全バージョンのドキュメント]ページに移動し、問題のトラブルシューティングのためのNetWitness Platformの各ガイドを見つけます。

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12.3 VMのリソースをすべて削除します。
   b. 同じIPアドレス、ディスク、リソースを使用して、12.4 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. **externalディスク**を除き、古い12.3 VMのリソースをすべて削除します。

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12.4 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、ハイブリッドが11.4の新規インストールであった場合のディザスター状況には適用されません。

シリーズ5またはシリーズ6のネットワーク ハイブリッドを11.2.x.xまたは11.3.x.xから11.4にアップグレードしており、ディザスターが発生した場合は、シリーズ5またはシリーズ6のハイブリッド用に`/etc/fstab`ファイルを変更する必要があります。

以下は、このディザスター シナリオからリカバリーするためのタスクを示します。

1. 11.4 ISOを使用して、新しいシリーズ5またはシリーズ6ハイブリッドのイメージをネットワーク ハイブリッドとして作成します。
2. バックアップしたデータまたは構成(`nw-recovery-tool --import`)をインポートします。
3. リカバリーした`/etc/fstab`ファイルを変更します。

ディザスター発生前のetc/fstabファイルの例

次のデータは、11.4にアップグレードされたシリーズ5または6ハイブリッドの外部ストレージ構成バックアップの例です。

黄色でハイライト表示されているデータは、アップグレードされたシステムの内部ストレージに対応しています。この構成は、アップグレード プロセス中に以前のリリースから継承されます。このレイアウトは11.4で変更されました(新規インストール)。ディザスター リカバリーの一環として、外部ストレージ(緑色でハイライト表示)に対応するエントリーのみを新しい`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、ストレージ構成の詳細が`<back-location>/unmanaged/etc/fstab`に保存されます。`fstab`ファイルには、内部ストレージ構成(黄色でハイライト表示)と外部ストレージ構成(緑色でハイライト表示)の両方が含まれています。アップグレードされた(10.6または11.xから11.4)シリーズ5またはシリーズ6ネットワーク ハイブリッドの内容は、次のストレージ構成のようになります。

```
/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
```

リカバリー後 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、リカバリー ツールを実 行して以 前 のすべての構 成をリスト アした後 、`/etc/fstab`ファイルは次 の例 のように表 示 されます。

```
#
# /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 :ご覧のとおり、外部ストレージ構成がありません。新しく作成されたハイブリッド上の`/etc/fstab`ファイルに、外部ストレージ構成(上記で緑色でハイライト表示)を追加する必要があります。

リカバリー後のetc/fstabファイルの例 - 変更後

この更新を行った後、`/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
```