RSA NETWITNESS® PLATFORM

Guide de l'utilisateur de l'outil de récupération

pour la version 11.2

Informations de contact

RSA Link à l'adresse https://community.rsa.com contient une base de connaissances qui répond aux questions courantes et fournit des solutions aux problèmes connus, de la documentation produit, des discussions communautaires et la gestion de dossiers.

Marques commerciales

Pour obtenir la liste des marques commerciales de RSA, rendez-vous à l'adresse suivante : france.emc.com/legal/emc-corporation-trademarks.htm#rsa.

Contrat de licence

Licences tierces

Ce produit peut inclure des logiciels développés par d'autres entreprises que RSA. Le texte des contrats de licence applicables aux logiciels tiers présents dans ce produit peut être consulté sur la page de la documentation produit du site RSA Link. En faisant usage de ce produit, l'utilisateur convient qu'il est pleinement lié par les conditions des contrats de licence.

Remarque sur les technologies de chiffrement

Ce produit peut intégrer une technologie de chiffrement. Étant donné que de nombreux pays interdisent ou limitent l'utilisation, l'importation ou l'exportation des technologies de chiffrement, il convient de respecter les réglementations en vigueur lors de l'utilisation, de l'importation ou de l'exportation de ce produit.

Distribution

Dell estime que les informations figurant dans ce document sont exactes à la date de publication. Ces informations sont modifiables sans préavis.

mars 2019

Sommaire

Reprise après sinistre (instructions de sauvegarde et restauration)

Vous pouvez utiliser l'outil de restauration NetWitness Recoverty Tool (NRT) pour sauvegarder et restaurer des données à partir des systèmes hôtes NetWitness Server et des composants. Le NRT est un script que vous exécutez à partir de la ligne de commande pour sauvegarder et restaurer les données sur les hôtes pour les RMA, les actualisations matérielles et les exigences générales de sauvegarde et de restauration. Reportez-vous à Reprise après sinistre dans le déploiement Azure pour prendre connaissance des étapes spécifiques sur la façon d'effectuer une reprise après sinistre pour les hôtes déployés dans des machines virtuelles Azure.

Remarque : Vous devez exécuter le NRT sur chaque système hôte localement. Vous ne pouvez pas l'exécuter à partir d'hôtes distants ou d'un hôte externe.

Les types d'hôtes suivants peuvent être sauvegardés et restaurés.

Remarque : Dans le script NRT, les termes suivants en gras sont appelés catégories.

- **Serveur d'administration NetWitness** (peut inclure Répondre, Intégrité et Reporting Engine)
- **Malware** Analyse de malware (autonome)
- **Archiver** Archiveur de logs
- **Broker** Courtier autonome
- **Concentrator** Réseau ou log
- **Decoder** Décodeur de réseau
- **Endpoint Hybrid**
- **Endpoint Log Hybrid**
- **Event Stream Analysis (ESA) primaire** Base de données de gestion des incidents et Context Hub comprise
- **ESA secondaire**
- **Gateway** Passerelle Cloud
- **Log Collector** Virtual Log Collecteur inclus si installé
- **Log Decoder** Log Collector local et Warehouse Connector inclus, si installés
- **Log Hybrid**
- **Network Hybrid**
- **UEBA** User Entity and Behavior Analytics
- **Warehouse**

Utilisation de base de NetWitness Recovery Tool

Vous pouvez utiliser le NRT pour sauvegarder des données à l'aide de l'option `export`. Pour restaurer des données, utilisez l'option `import`. L'utilisation de base de l'outil consiste à exécuter la commande suivante à partir du niveau du répertoire racine :

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

Les commandes et les options que vous pouvez utiliser avec cet outil sont décrits dans les tableaux suivants.

Commandes et options	Description
`-h, --help`	Afficher l'aide sur les commandes et les options. Par exemple, spécifiez : `nw-recovery-tool --help-categories` pour obtenir une liste de tous les noms de catégories valides.
`-e, --export`	Exporter les données ou la configuration.
`-i, --import`	Importer les données ou la configuration.
`-d, --dump-dir <path>`	Chemin d'exportation ou d'importation des données (par exemple, `/var/netwitness/backup`).
`-C, --category <name>`	Sélectionner les composants par catégorie. Les noms de catégories valides sont `AdminServer`, `Archiver`, `Broker`, `Concentrator`, `Decoder`, `EndpointHybrid`, `EndpointLogHybrid`, `ESAPrimary`, `ESASecondary`, `Gateway`, `LogCollector`, `LogDecoder`, `LogHybrid`, `Malware`, `NetworkHybrid`, `UEBA` et `Warehouse`. Vous pouvez spécifier une seule ou plusieurs catégories. Par exemple : `--category AdminServer` uniquement pour le serveur d'administration. `--category AdminServer --category Gateway` pour le serveur d'administration et la passerelle Cloud.
`-p, --deploy-password <pwd>`	Spécifier un mot de passe de déploiement. Cela n'est nécessaire que si la catégorie ou le composant sélectionné inclut Mongo (pour les hôtes tels que AdminServer, Endpoint ou ESA Primary).

Conditions obligatoires

Assurez-vous que les conditions suivantes sont remplies :

- Lisez l'intégralité du document avant de sauvegarder les données. Le document couvre tous les scénarios de déploiement, de sorte que vous pouvez vous assurer que vous disposez de toutes les informations nécessaires pour sauvegarder et restaurer votre implémentation de la plate-forme NetWitness avant d'effectuer ce processus.
- Exécutez le NRT pour la sauvegarde et la restauration locales, sur chaque système sauvegardé ou restauré. Vous ne pouvez pas exécuter le NRT sur un hôte externe, ni sauvegarder ou restaurer plusieurs hôtes simultanément. Toutefois, vous pouvez sauvegarder plusieurs composants sur le même système à ordinateur central simultanément.
- Exportez et importez des données sur le même hôte. Si un hôte échoue et que vous avez besoin de construire un nouveau système, le nouveau système doit avoir les mêmes paramètres d'identité (c.-à-d. la même adresse IP) et doit être sur la même version de NetWitness Suite
- Assurez-vous qu'il y a suffisamment d'espace disque à l'emplacement de sauvegarde (`/var/netwitness/backup` est le répertoire recommandé) avant l'exécution de la commande d'exportation dans l'outil nw-recovery. N'utilisez pas un répertoire `tmp` , car il se remplirait rapidement et pourrait provoquer une panne du système.
- Vérifiez le dimensionnement des disques Malware et ajustez-les avant de les sauvegarder. Le tableau suivant montre la taille maximale des bases de données Malware que vous pouvez sauvegarder par type de matériel, ainsi que les actions que vous pouvez réaliser pour les réduire à la taille maximale.

Hôte	Matériel source	Matériel cible	Base de données	Taille maximale pour la sauvegarde	Actions pour réduire au maximum la taille de la sauvegarde
Malware	Hybride série 4S	Core série 6	`/var/netwitness`	2,5 To	Configurer un transfert. Purger les données dont vous n'avez pas besoin de la base de données.

- Restaurez l'image ISO exacte que chaque hôte avait au moment de la sauvegarde.
- Si vous avez plusieurs services co-localisés sur un seul hôte, incluez tous les services dans une seule chaîne pour les commandes `import` et `export` dans l'outil nw-recovery.

Remarque : 1.) Lorsque vous exécutez le NRT, les services Malware, Reporting Engine et PostgreSQL sont arrêtés et redémarrés pendant les processus de sauvegarde (exportation) et de restauration (importation). La collecte de logs et de paquets n'est pas arrêtée.

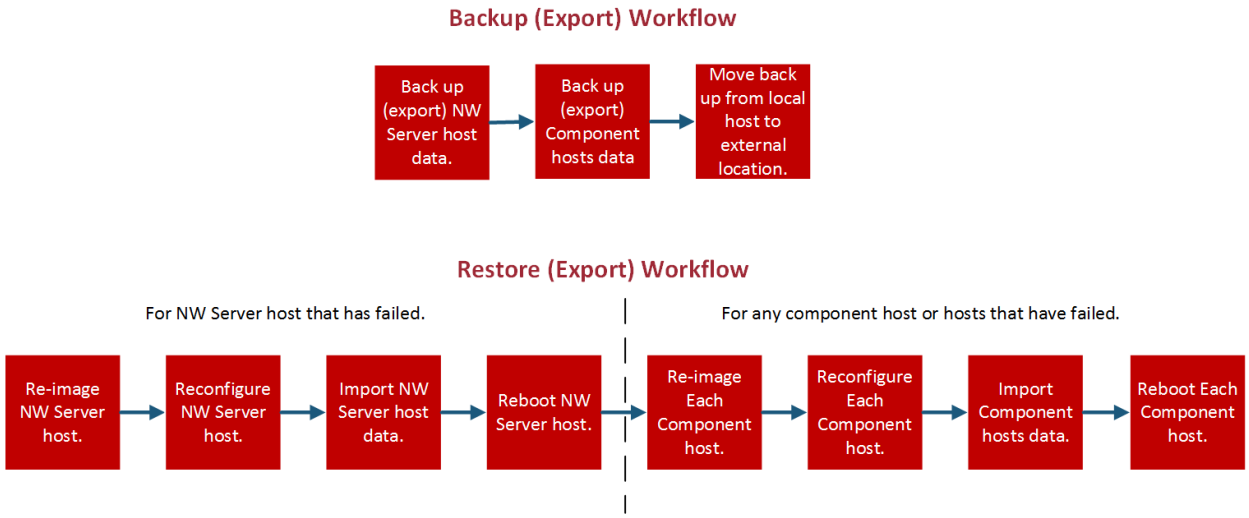
Workflow de reprise après sinistre

Le schéma suivant illustre les tâches de reprise après sinistre de haut niveau.

Remarque : Il vous suffit de restaurer un hôte s'il est en échec. Cela signifie que vous pouvez restaurer un hôte unique ou toute combinaison d'hôtes en fonction de l'hôte ou des hôtes en échec.

Le schéma suivant présente les tâches de :

- Sauvegarde (à effectuer le plus rapidement possible et le plus souvent possible)
- Restauration (uniquement nécessaire si vous avez besoin de restaurer vos données)



Sauvegarde et restauration des données des hôtes 11.x

Les procédures de sauvegarde et de restauration des données sont différentes pour les systèmes à ordinateur central NetWitness Server et les systèmes de composants.

Attention : 1.) Ne supprimez pas les hôtes de composants (c'est-à-dire tout hôte autre que l'hôte du serveur NW) de la vue Hôtes (Admin > Hôtes) à partir de l'interface utilisateur lorsque vous effectuez la procédure de reprise après sinistre suivante. 2.) Vous devez conserver (restaurer) le « nom d'hôte » qui existait avant l'exécution de la procédure de reprise après sinistre. 3.) Assurez-vous d'enregistrer votre mot de passe principal et stockez-le dans un endroit sûr afin de pouvoir accéder au système en cas de reprise après sinistre.

Sauvegarde et restauration de données sur le NetWitness Server 11.x

Remarque : Si vous utilisez le stockage partagé pour exporter des données à partir de plusieurs hôtes (par exemple, un montage ou un lecteur partagé), utilisez des sous-dossiers spécifiques à l'hôte pour le chemin à l'emplacement des fichiers exportés pour chaque hôte, afin d'éviter d'écraser les données exportées d'un hôte avec un autre. Par exemple, vous pouvez utiliser un chemin semblable à `--dump-dir /mnt/storage/<host-specific-name>` pour le chemin à l'emplacement des fichiers exportés.

Sauvegarde des données sur un hôte NetWitness Server

Effectuez cette procédure sur un système à ordinateur central 11. x NetWitness Server existant et fonctionnel.

1. Saisissez la commande suivante au niveau root :

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

   Remarque : Si un service (par exemple, Passerelle Clouddans la boîte de dialogue Confirmez la mise à jour,) est co-localisé sur le serveur NW avec le serveur d'administration plutôt que sur son propre hôte dédié, vous devez l'inclure dans la chaîne de commande. Par exemple : `nw-recovery-tool--export --dump-dir /var/netwitness/backup --category AdminServer --category Gateway`

2. Remplacez `/var/netwitness/backup` par le chemin à l'emplacement d'exportation des données.

   a. Assurez-vous que cet emplacement dispose d'un espace suffisant pour stocker les données de sauvegarde.

   b. Le chemin au répertoire de sauvegarde doit se trouver sur l'hôte local. Toutefois, les fichiers de sauvegarde peuvent se trouver sur un montage réseau ou un périphérique externe.

3. Lorsque vous êtes invité à saisir le mot de passe d'administration du déploiement, saisissez le mot de passe ou incluez l'argument supplémentaire suivant pour la commande `nw-recovery-tool` :

   `--deploy-password <password>`

   Remarque : Utilisez le mot `deploy_admin` de passe existant qui a été utilisé lors de la première installation de l'hôte.

   Les données sont sauvegardées sur l'hôte NetWitness Server à l'emplacement que vous avez configuré à l'étape 2.

4. Déplacez les données sauvegardées de l'hôte local vers un serveur externe ou une clé USB.

Restauration des données sur un hôte NetWitness Server

1. Dupliquez l'image de l'hôte NetWitness Server en utilisant les mêmes paramètres de configuration de réseau de l'hôte d'origine. Pour plus d'informations sur la duplication de l'image de l'hôte NetWitness Server, voir « Tâche 1 - Installer 11.2 sur l'hôte NetWitness Server » dans le *Guide d'installation de l'hôte physique de la version 11.2*

   a. **Facultatif** Si vous devez établir une connectivité réseau avant de pouvoir extraire des données de sauvegarde, par exemple, si elles se trouvent sur un hôte distant, exécutez le script suivant en utilisant les mêmes informations d'adresse IP, de sous-réseau, de passerelle, de DNS et de domaine que l'hôte d'origine :

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

   Par exemple :

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

   En option : Pour spécifier un ou des serveurs DNS, incluez le paramètre supplémentaire suivant :

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

   En option : Pour définir le nom de domaine local, incluez le paramètre supplémentaire suivant :

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

   b. (**Facultatif**) Si vous utilisez DHCP, exécutez le script suivant :

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

   Par exemple :

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

   c. Ajoutez les données de sauvegarde au chemin du répertoire de sauvegarde sur l'hôte local, par exemple :

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

2. Exécutez la commande `nwsetup-tui`. Cela déclenche le programme d'installation.

   Remarque : Pendant le programme d'installation, lorsque vous êtes invité à configurer le réseau de l'hôte, veillez à spécifier la même configuration de réseau que celle utilisée pour l'installation d'origine de 11.x sur cet hôte.

3. Lorsque vous y êtes invité, sélectionnez l'option de type d'installation **3 : Restaurer (réinstaller)**, cliquez sur **OK**, puis saisissez le chemin au répertoire de sauvegarde contenant les données de sauvegarde.

4. Une fois l'installation terminée avec succès, assurez-vous que l'hôte exécute la version exacte et le correctif des données qui ont été sauvegardées :

   - Si les données étaient sur un système 11.x mis à jour vers une version ultérieure du correctif, mettez à jour l'hôte en suivant les instructions de mise à jour des systèmes hors connexion du guide de mise à jour à la même version de correctif que celui qui était précédemment en cours d'exécution sur l'hôte (la version/le correctif exacts pour lesquels les données ont été

sauvegardées).

- Si les données étaient sur une version majeure (par exemple, 11.x) qui n'avait pas été mise à jour vers une version de correctif ultérieure, vous n'avez pas besoin de mettre à jour le système à ordinateur central.

5. Lorsque l'hôte est en cours d'exécution à la version correcte, exécutez la commande suivante sur le NetWitness Server pour restaurer les données :

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

   Remarque : Si un service est co-localisé sur le serveur NW avec le serveur d'administration plutôt que sur son propre hôte dédié, vous devez l'inclure dans la chaîne de commande. Par exemple :
   `nw-recovery-tool--import--dump-dir /var/netwitness/backup --category AdminServer --category Gateway`

6. (Facultatif) Pour les clients utilisant des règles de pare-feu personnalisées (c'est-à-dire qui ont répondu « Oui » à l'invite nwsetup-tui « Désactiver le pare-feu » lors de l'installation), restaurez le fichier `/etc/sysconfig/iptables` à partir de la copie de sauvegarde située dans le fichier `<dump-dir>/unmanaged/etc/sysconfig/iptables`.

7. Redémarrez l'hôte NetWitness Server.

Sauvegarde et restauration des données sur d'autres hôtes de composants

Effectuez ces procédures sur un système à ordinateur central de composants 11.x existant et fonctionnel.

Sauvegarde des données sur un hôte de composant

1. Saisissez la commande suivante au niveau root :
   `nw-recovery-tool --export --dump-dir /var/netwitness/backup --category <category name>`
   où le nom de la catégorie est l'un des suivants :
   `Archiver, Broker, Concentrator, Decoder, EndpointHybrid, EndpointLogHybrid, ESAPrimary, ESASecondary, LogCollector, LogDecoder, LogHybrid, Malware, NetworkHybrid, UEBA`

   Remarque : 1.) Utilisez la catégorie qui correspond au type d'hôte. 2.) Si les services sont co-localisés sur un hôte de composants plutôt que sur son propre hôte dédié, vous devez l'inclure dans la chaîne de commande. Par exemple, un Warehouse Connector réside sur un hôte Log Decoder. Voici un exemple de la chaîne de commande :
   `nw-recovery-tool--export --dump-dir /var/netwitness/backup --category LogDecoder --category Warehouse`

2. **(Facultatif)** Remplacez `/var/netwitness/backup` par le chemin menant à l'emplacement d'exportation des données.
   a. Assurez-vous que cet emplacement dispose d'un espace suffisant pour stocker les données de sauvegarde.
   b. Le chemin au répertoire de sauvegarde doit se trouver sur l'hôte local. Toutefois, les fichiers de sauvegarde peuvent se trouver sur un montage réseau ou un périphérique externe.

3. Pour les systèmes **EndpointHybrid**, **EndpointLogHybrid** et **ESAPrimary**, vous pouvez exporter les données d'application stockées dans la base de données en exécutant la commande suivante :
   `nw-recovery-tool --export --dump-dir /var/netwitness/backup --component mongo`
   Vous pouvez remplacer `/var/netwitness/backup` par le chemin à l'emplacement d'exportation des données.

   Remarque : 1.) Assurez-vous qu'il y a suffisamment d'espace dans l'emplacement d'exportation pour les fichiers provenant de la base de données Mongo. 2.) Vous pouvez sauvegarder les données d'hôte **EndpointHybrid**, **EndpointLogHybrid** ou **ESAPrimary** et la base de données Mongo dans une seule chaîne de commande. Par exemple, `nw-recovery-tool --export --dump-dir /var/netwitness/backup --category EndpointHybrid --component mongo`

   Lorsque vous êtes invité à saisir le mot de passe d'administration du déploiement, saisissez le mot de passe ou incluez l'argument supplémentaire suivant pour la commande `nw-recovery-tool` :
   `--deploy-password <password>`

4. Pour **Malware**, vous pouvez exporter des données d'application à partir de la base de données d'application Malware en exécutant la commande suivante :
   `nw-recovery-tool --export --dump-dir /var/netwitness/backup --component postgresql`
   Vous pouvez remplacer `/var/netwitness/backup` par le chemin menant à l'emplacement d'exportation des données.

   Remarque : Assurez-vous qu'il y a suffisamment d'espace dans l'emplacement d'exportation pour les fichiers provenant de la base de données Malware.

5. Déplacez les données sauvegardées de l'hôte local vers un serveur externe ou une clé USB.

Restauration des données sur un hôte de composant

1. Dupliquez l'image de l'hôte de composant en utilisant les mêmes paramètres de configuration de réseau que l'hôte d'origine. Pour plus d'informations sur la duplication de l'image de l'hôte de composant, voir « Tâche 2 - Installer 11.x sur d'autres hôtes de composants » dans le *Guide d'installation de l'hôte physique de la version 11.x*
2. **Facultatif** Si vous devez établir une connectivité réseau avant de pouvoir extraire des données de sauvegarde, par exemple, si elles se trouvent sur un hôte distant, exécutez le script suivant en utilisant les mêmes informations d'adresse IP, de sous-réseau, de passerelle, de DNS et de domaine que l'hôte d'origine :
   `netconfig --static --interface <name> --ip <address> --netmask <netmask> --gateway <gateway>`
   Par exemple :
   `netconfig --static --interface eth0 --ip 192.168.1.100 --netmask 255.255.255.0 --gateway 192.168.1.1`
   Facultatif : Pour spécifier un ou des serveurs DNS, incluez le paramètre supplémentaire suivant :
   `--dns <address>`
   Facultatif : Pour définir le nom de domaine local, incluez le paramètre supplémentaire suivant :
   `--domain <name>`

   a. **(Facultatif)** Si vous utilisez DHCP, exécutez le script suivant :
      `netconfig --dhcp --interface <name>`
      Par exemple :
      `netconfig --dhcp --interface eth0`

   b. Ajoutez les données de sauvegarde au chemin du répertoire de sauvegarde sur l'hôte local, par exemple, `/var/netwitness/backup`.

3. Exécutez la commande `nwsetup-tui`. Cela déclenche le programme d'installation.

   Remarque : Pendant le programme d'installation, lorsque vous êtes invité à configurer le réseau de l'hôte, veillez à spécifier la même configuration de réseau que celle utilisée pour l'installation d'origine de 11.x sur cet hôte.

4. Lorsque vous y êtes invité, sélectionnez l'option de type d'installation **3 : Restaurer (réinstaller)**, cliquez sur **OK**, puis saisissez le chemin menant au répertoire contenant les données de sauvegarde.

5. Après avoir terminé la configuration de la commande `nwsetup-tui`, vous devez réinstaller les services appropriés (excepté EndpointHybrid et EndpointLogHybrid) sur l'hôte à l'aide de la commande Install de la vue Hôtes dans l'interface utilisateur de la plate-forme NetWitness. Pour EndpointHybrid et EndpointLogHybrid, vous devez utiliser le client de interface de ligne de commande de l'orchestration sur le serveur d'administration pour installer les services Endpoint. Exécutez la commande suivante :

   ```
   orchestration-cli-client --hostaddr-as-id -i -o <host IP Address> --
   category <EndpointHybrid or EndpointLogHybrid> --version <version>
   ```

   Par exemple :

   ```
   orchestration-cli-client --hostaddr-as-id -i -o 192.168.200.83 --category
   EndpointLogHybrid --version 11.2.0.0
   ```

   Remarque : Le numéro de version doit correspondre à la version du support utilisé pour dupliquer l'image de l'hôte.

6. Une fois l'installation du service terminée, assurez-vous que l'hôte exécute la même version et le même correctif que ceux des données sauvegardées :

   - Si les données étaient sur un système 11.x mis à jour vers une version ultérieure du correctif, mettez à jour l'hôte en suivant les instructions de mise à jour des systèmes hors connexion pour la même version de correctif que celui qui était précédemment en cours d'exécution sur l'hôte (la version/le correctif exacts pour lesquels les données ont été sauvegardées).
   - Si les données étaient sur une version majeure (par exemple, 11.x) qui n'avait pas été mise à jour vers une version de correctif ultérieure, vous n'avez pas besoin de mettre à jour le système à ordinateur central.

7. Lorsque l'hôte est en cours d'exécution à la version correcte, revenez au niveau root de l'hôte de composants et exécutez la commande suivante pour restaurer les données :

   ```
   nw-recovery-tool --import --dump-dir /var/netwitness/backup --category
   <category name>
   ```

   Remarque : Si les services sont co-localisés sur un hôte de composants plutôt que sur son propre hôte dédié, vous devez l'inclure dans la chaîne de commande. Par exemple, un Warehouse Connector réside sur un hôte Log Decoder. Voici un exemple de cette chaîne de commande :
   `nw-recovery-tool--import --dump-dir /var/netwitness/backup --category LogDecoder --category Warehouse`

8. Pour les systèmes**EndpointHybrid**, **EnpointLogHybrid** et **ESAPrimary**, vous pouvez importer les données d'application à restaurer en exécutant la commande suivante :

   ```
   nw-recovery-tool --import --dump-dir /var/netwitness/backup --component
   mongo
   ```

   Lorsque vous êtes invité à saisir le mot de passe d'administration du déploiement, saisissez le mot de passe ou incluez l'argument supplémentaire suivant pour la commande `nw-recovery-tool` :
   `--deploy-password <password>`

9. Pour **Malware**, vous pouvez importer des données d'application de la base de données d'application Malware à restaurer en exécutant la commande suivante :

   ```
   nw-recovery-tool --import --dump-dir /var/netwitness/backup --component
   postgresql
   ```

10. Pour un Décoder, un Log Decoder, un Concentrator, un Archiver, un Network Hybrid ou un Log Hybrid configuré avec un stockage externe (JBOD/SAN/Unity/PowerVault) :

    a. Analysez le fichier `<dump-dir>/unmanaged/etc/fstab` pour les périphériques avec des points de montage qui n'existent pas dans le fichier système `/etc/fstab`.

    IMPORTANT : Si vous effectuez une migration vers un nouveau matériel hôte (c'est-à-dire un nouvel hôte Decoder, Log Decoder, Concentrator, Archiver, Network Hybrid ou Log Hybrid), avant de passer à l'étape suivante, vous devez :
    1. Mettre hors tension l'ancien hôte matériel et le périphérique de stockage externe qui lui est rattaché.
    2. Rattachez le périphérique de stockage externe au nouveau matériel hôte.
    3. Mettre sous tension le nouvel matériel hôte et le périphérique de stockage externe qui lui est rattaché.

    b. Effectuez les étapes suivantes pour chaque périphérique de la copie de sauvegarde de `<dump-dir>/unmanaged/etc/fstab`.

        i. Vérifiez que l'appareil correspondant est présent et rattaché. Si ce n'est pas le cas, rattachez-le. Si l'appareil n'est plus applicable, ignorez-le et passez à l'appareil suivant.

        ii. Assurez-vous que le répertoire de point de montage existe sur le système de fichiers. Dans le cas contraire, créez le répertoire avec la commande `mkdir <path>` .

        iii. Ajoutez l'entrée `fstab` de la copie de sauvegarde vers le fichier système `/etc/fstab`.

    c. Exécutez la commande suivante sur chaque hôte.
    `mount -a`

11. A partir de ASOC-59466 (Facultatif) Pour les clients utilisant des règles de pare-feu personnalisées (c'est-à-dire qui ont répondu « Oui » à l'invite nwsetup-tui « Désactiver le pare-feu » lors de l'installation), restaurez le fichier `/etc/sysconfig/iptables` de la copie de sauvegarde située dans le fichier `<dump-dir>/unmanaged/etc/sysconfig/iptables`.

12. Redémarrez l'hôte du composant.

Actualisation matérielle uniquement - Utiliser un espace supplémentaire dans les nouveaux hôtes matériels

Reportez-vous au *Guide de réglage Core de la plate-forme RSA NetWitness* (https://community.rsa.com/docs/doc-95938

) pour savoir comment utiliser tout l'espace disponible sur votre nouveau matériel.

Reprise après sinistre dans le déploiement Azure

La section vous indique comment sauvegarder et restaurer la plate-forme NetWitness 11.x déployée sur des hôtes virtuels Azure (également appelés machines virtuelles dans cette section). Les deux tâches majeures de sauvegarde et de restauration des données 11.x dans un déploiement Azure sont les suivantes :

- Tâche 1 - Sauvegarder et exporter des données
- Tâche 2 - Restaurer et importer des données

Tâche 1 - Sauvegarder et exporter des données

1. Exportez les données en exécutant les commandes `nw-recovery-tool --export` comme décrit dans Reprise après sinistre (instructions de sauvegarde et restauration).

Tâche 2 - Restaurer et importer des données

Vous devez vous référer au *Guide de mise à niveau de la version 10.6.5 à 11.2 Azure* pour effectuer cette tâche. Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

1. Supprimez la machine virtuelle.

   Attention : Ne supprimez pas les ressources (par exemple, ne supprimez pas les disques, l'interface réseau, etc.).

2. Effectuez les étapes suivantes pour les hôtes AdminServer, Broker, ESA, Endpoint et Log Collector (où l'hôte = `--category`).

   a. Supprimez toutes les ressources à l'exception de la carte d'interface réseau de l'ancienne VM 11.2.

   b. Déployez la nouvelle machine virtuelle 11.2 avec le même disque et les mêmes ressources et éteignez-la.
   Consultez le *Guide de déploiement Azure 11.2* pour obtenir des instructions détaillées sur la façon de déployer un hôte virtuel dans Azure.

   c. Exécutez `azure-mac-retention.ps1` à partir de la machine locale.
   Consultez le *Guide de mise à niveau Azure de la version 10.6.5 à 11.2* pour savoir comment exécuter ce script.

   d. Suivez la procédure de restauration NRT pour l'hôte respectif, comme décrit dans Restauration des données sur un hôte de composant.

   e. Après avoir restauré NRT, l'hôte de composant, restaurez les fichiers suivants.

      - `/etc/fstab`
      - `/etc/hosts` (si le nom d'hôte n'est pas modifié)

- `/etc/waagent.conf`
- `/etc/logrotate.d/waagent.logrotate`
- `/etc/krb5.conf` à partir du dossier `<dump-dir>/unmanaged`

3. Effectuez les étapes suivantes pour les hôtes Log Decoder, Concentrator et Archiver (où l'hôte = `--category`).
   a. Supprimez toutes les ressources à l'exception des disques nommées en **externe** et la carte d'interface réseau de l'ancienne VM 11.2.
   b. Déployez la nouvelle machine virtuelle 11.2 avec le même disque et les mêmes ressources que ceux répertoriés dans le *Guide de déploiement Azure 11.2* et éteignez-la.

      Remarque : Ne créez pas le disque **externe**. Créez uniquement les disques **nwhome**.

   c. Exécutez `azure-mac-retention.ps1` à partir de la machine locale.
      Consultez le *Guide de mise à niveau Azure de la version 10.6.5 à 11.2* pour savoir comment exécuter ce script.
   d. Suivez la procédure de restauration NRT pour les hôtes respectifs, comme décrit dans Restauration des données sur un hôte de composant.
   e. Après avoir restauré NRT, l'hôte de composant, restaurez les fichiers suivants.
      - `etc/fstab`
      - `/etc/hosts` (si le nom d'hôte n'est pas modifié)
      - `/etc/waagent.conf`
      - `etc/logrotate.d/waagent.logrotate`
      - `/etc/krb5.conf`

Reprise après sinistre dans le déploiement AWS

La section vous indique comment sauvegarder et restaurer la plate-forme NetWitness 11.x déployée sur des hôtes virtuels AWS (également appelés machines virtuelles dans cette section). Les deux tâches majeures de sauvegarde et de restauration des données 11.x dans un déploiement AWS sont les suivantes :

- Tâche 1 - Sauvegarder et exporter des données
- Tâche 2 - Restaurer et importer des données

Tâche 1 - Sauvegarder et exporter des données

1. Exportez les données en exécutant les commandes `nw-recovery-tool --export` comme décrit dans Reprise après sinistre (instructions de sauvegarde et restauration).
2. Enregistrez les adresses IP. Vous devez les consulter plus tard dans le processus de reprise après sinistre.
   Reportez-vous au *Guide de mise à niveau de la version 10.6.5 à 11.2 AWS* pour savoir comment conserver les adresses IP. Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

Tâche 2 - Restaurer et importer des données

Vous devez vous référer au *Guide de mise à niveau de la version 10.6.5 à 11.2 AWS* pour effectuer cette tâche.

1. Supprimez la machine virtuelle.

   Attention : Ne supprimez pas les ressources (par exemple, ne supprimez pas les disques).

2. Effectuez les étapes suivantes pour les hôtes AdminServer, Broker, ESA (principal/secondaire), Endpoint Hybrid, Endpoint Log Hybrid et Log Collector (où l'hôte = `--category`).

   a. Supprimez toutes les ressources de l'ancienne VM 11.2.

   b. Déployez la nouvelle machine virtuelle 11.2 avec la même adresse IP, le même disque et les mêmes ressources et éteignez-la.
   Consultez le *Guide de déploiement AWS 11.2* pour obtenir des instructions détaillées sur la façon de déployer un hôte virtuel dans AWS.

   c. Suivez la procédure de restauration NRT pour l'hôte respectif, comme décrit dans Restauration des données sur un hôte de composant.

   d. Après avoir restauré NRT, l'hôte de composant, restaurez les fichiers suivants.

      - `/etc/fstab`
      - `/etc/hosts` (si le nom d'hôte n'est pas modifié)

3. Effectuez les étapes suivantes pour les hôtes Log Decoder, Decoder (Network Decoder), Concentrator et Archiver (où l'hôte = `--category`).

   a. Supprimez toutes les ressources de l'ancienne VM 11.2 sauf les **disques externes**.

   b. Déployez la nouvelle machine virtuelle 11.2 avec la même adresse IP, le même disque et les mêmes ressources que ceux répertoriés dans le *Guide de déploiement AWS 11.2* et éteignez-la.

      Remarque : Ne créez pas le disque **externe**. Créez uniquement les disques **nwhome**.

   c. Suivez la procédure de restauration NRT pour les hôtes respectifs, comme décrit dans Restauration des données sur un hôte de composant.

   d. Après avoir restauré NRT, l'hôte de composant, restaurez les fichiers suivants.

      - `etc/fstab`
      - `/etc/hosts` (si le nom d'hôte n'est pas modifié)
      - `/etc/krb5.conf`