



# Guide de mise à jour

pour la version 11.0. x. x ou 11.1. x. x à 11.2



Copyright © 1994-2019 Dell Inc. or its subsidiaries. All Rights Reserved.

## **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](https://france.emc.com/legal/emc-corporation-trademarks.htm#rsa).

## **Contrat de licence**

Ce logiciel et la documentation qui l'accompagne sont la propriété de Dell et considérés comme confidentiels. Délivrés sous licence, ils ne peuvent être utilisés et copiés que conformément aux modalités de ladite licence et moyennant l'inclusion de la note de copyright ci-dessous. Ce logiciel et sa documentation, y compris toute copie éventuelle, ne peuvent pas être remis ou mis de quelque façon que ce soit à la disposition d'un tiers.

Aucun droit ou titre de propriété sur le logiciel ou sa documentation ni aucun droit de propriété intellectuelle ne vous est cédé par la présente. Toute utilisation ou reproduction non autorisée de ce logiciel et de sa documentation peut faire l'objet de poursuites civiles et/ou pénales.

Ce logiciel est modifiable sans préavis et ne doit nullement être interprété comme un engagement de la part de Dell.

## **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

---

<b>Introduction</b> .....	<b>5</b>
Stratégies de mise à jour .....	5
Fonctionnement en mode Mixte .....	5
Balise Entropy=log2 flag - Réinitialiser après mise à jour .....	5
<b>Tâches de préparation de la mise à jour</b> .....	<b>7</b>
Général .....	7
Tâche 1 - Passer en revue les ports de base et ouvrir les ports de pare-feu .....	7
Tâche 2 - Sauvegarder le fichier de configuration de Malware Analysis dans un autre répertoire ..	7
Tâche 3 - Arrêter la capture et l'agrégation des données .....	8
Hôtes Azure .....	10
Tâche 4 - (Conditionnel) Configuration requise pour la préparation de la mise à jour Azure Host	10
Endpoint Insights .....	11
Tâche 5 - (Conditionnel) Sauvegarde des mappages de métadonnées personnalisés existants avant d'appliquer la mise à jour 11.2 à l'hôte du point de terminaison .....	11
Reporting Engine .....	11
Tâche 6 - Configurer Reporting Engine pour les graphiques prêts à l'emploi .....	11
Répondre .....	11
Tâche 7 - (Conditionnel) Restaurer les clés personnalisées du service Respond .....	11
Tâche 8 - Sauvegarder les scripts de normalisation personnalisés du service Respond .....	12
<b>Tâches de mise à jour</b> .....	<b>13</b>
Appliquer les mises à jour à partir de la vue Hôtes (Accès Web) .....	13
Tâche 1. Renseigner le référentiel local ou Configurer un référentiel externe .....	13
Tâche 2. Appliquer les mises à jour à chaque hôte à partir de la vue Hôtes .....	14
Appliquer les mises à jour à partir de la ligne de commande (sans accès Web) .....	18
<b>Mettre à jour ou installer la Collection Windows d'ancienne génération</b> .....	<b>20</b>
<b>Tâches à effectuer après la mise à jour</b> .....	<b>21</b>
Général .....	22
Tâche 1 - Démarrer la capture et l'agrégation des données .....	22
Tâche 2 - Configurer les actions des menus contextuels d'Autorisations utilisateur .....	23
Serveur NW .....	25
Tâche 3 - (Conditionnel) Corriger les modèles de journal d'audit qui ne sont pas mis à jour dans le fichier de configuration de sortie Logstash .....	25
(Conditionnel) Tâche 4 - Reconfigurer l'authentification PAM pour Radius .....	25
Endpoint Insights .....	26
Tâche 5 - Reconfigurer un feed récurrent configuré à partir d'une ancienne version Endpoint parce que la version Java a changé. ....	26

Tâche 6 - Restaurer les mappages de métadonnées personnalisées des points de terminaison sauvegardés .....	26
Event Stream Analysis .....	27
(Conditionnel) Tâche 7 - Reconfigurer la règle d'agrégation « Communication de commande et contrôle suspect par domaine » pour la détection automatisée des menaces .....	27
Répondre .....	28
Tâche 8 - Obtenir la dernière version du schéma de la règle d'agrégation et restaurer les clés personnalisées du service Respond .....	28
Tâche 9 - Obtenir la dernière version des scripts de normalisation du service Respond et restaurer les scripts de normalisation personnalisés du service Respond .....	29
Tâche 10 - Ajouter les autorisations des paramètres de notification de réponse .....	29
Tâche 11 - Mettre à jour le groupe de règles de l'incident par défaut en fonction des valeurs .....	30
NetWitness UEBA .....	31
Tâche 12 - Installer NetWitness UEBA .....	31
<b>Annexe . Dépannage des installations et mises à jour de version .....</b>	<b>32</b>
<b>Annexe B. Renseigner le référentiel local .....</b>	<b>39</b>
<b>Annexe C. Configurer le référentiel externe .....</b>	<b>41</b>
<b>Historique des révisions .....</b>	<b>44</b>

## Introduction

---

RSA NetWitness® Platform 11.2.0.0 fournit des correctifs pour tous les produits de la plateforme. Les composants de la plateforme sont les suivants : NetWitness Server (serveur d'administration, serveur de configuration, serveur d'intégration, serveur Investigate, serveur d'orchestration, serveur Respond, serveur de sécurité et serveur source), Archiver, Broker, Concentrator, Context Hub, Decoder, Endpoint Hybrid, Endpoint Log Hybrid, ESA primaire, ESA secondaire, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, UEBA, Warehouse Connector et Workbench.

**Remarque :** Reporting Engine est installé sur l'hôte du serveur NW, Workbench est installé sur l'hôte Archiver, Warehouse Connector peut être installé sur l'hôte Decoder ou l'hôte Log Decoder.

Les instructions fournies dans ce guide s'appliquent aux hôtes physiques et virtuels (y compris AWS et le Cloud public Azure), sauf indication contraire.

## Stratégies de mise à jour

Les stratégies de mise à jour suivantes sont prises en charge par NetWitness Platform 11.2.0.0 :

- 11.0.x vers 11.2.0.0
- 11.1.x vers 11.2.0.0
- 10.6.6.x vers 11.2.0.0

Accédez à la [Table des matières principale](#) pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

Reportez-vous au *Guide de mise à niveau des hôtes physiques RSA NetWitness Platform 10.6.6.x vers la version 11.2* et au *Guide de mise à niveau des hôtes virtuels RSA NetWitness Platform 10.6.6.x vers la version 11.2* pour obtenir des instructions sur la façon d'effectuer une mise à niveau de la version 10.6.6.x vers la version 11.2.0.0.

## Fonctionnement en mode Mixte

L'exécution du mode Mixte se produit lorsque certains services sont mis à jour vers la dernière version et que d'autres services fonctionnent toujours avec des versions plus anciennes. Consultez « Fonctionnement en mode Mixte » dans le *Guide de mise en route des hôtes et des services RSA NetWitness Platform* pour plus d'informations.

## Balise Entropy=log2 flag - Réinitialiser après mise à jour

Si votre balise `Entropy=log2` est définie sur `false` (`Entropy="log2=false"`) dans la version 11.0.x.x, NetWitness réinitialise cette balise avec la valeur `true` (`Entropy="log2=true"`) après la mise à niveau vers la version 11.2 afin d'aligner toutes les sources et d'inclure les paquets et NetWitness Endpoint Insights. Si vous le souhaitez, vous pouvez définir la balise sur `false` pour conserver le calcul `log10` : `Entropy="log2=false"`.



## Tâches de préparation de la mise à jour

Effectuez les tâches suivantes pour préparer la mise à jour vers NetWitness Platform 11.2.0.0. Ces tâches sont organisées selon les catégories suivantes.

[Général](#)

[Hôtes Azure](#)

[Endpoint Insights](#)

[Reporting Engine](#)

[Respond](#)

### Général

#### Tâche 1- Passer en revue les ports de base et ouvrir les ports de pare-feu

Les tableaux suivants répertorient les nouveaux ports dans la version 11.2.0.0.

**Attention :** Assurez-vous que les nouveaux ports sont mis en œuvre et testés avant la mise à jour afin que cette mise à jour n'échoue pas suite à des ports manquants.

#### Endpoint Hybrid ou Endpoint Log Hybrid

Hôte source	Hôte de destination	Ports de destination	Commentaires
Endpoint Hybrid ou Endpoint Log Hybrid	Serveur NW	TCP 5672	Bus de messages
Serveur Endpoint	Serveur NW	TCP 27017	MongoDB

#### Tâche 2 - Sauvegarder le fichier de configuration de Malware Analysis dans un autre répertoire

1. Sauvegardez le fichier suivant dans un autre répertoire sûr.

```
/var/lib/netwitness/malware-analytics-server/spectrum/conf/malwareCEFDictionaryConfiguration.xml
```

Vous devez récupérer les valeurs des paramètres personnalisés à partir de cette sauvegarde après avoir mis à jour l'hôte Malware Analysis vers la version 11.2.0.0. La mise à jour crée un nouveau fichier de configuration avec tous les paramètres définis par défaut.

2. Supprimez le fichier suivant.

```
/var/lib/netwitness/malware-analytics-server/spectrum/conf/malwareCEFDictionaryConfiguration.xml
```



## Tâche 3 - Arrêter la capture et l'agrégation des données

### Arrêter la capture réseau

1. Connectez-vous à NetWitness Platform 11.0.x et accédez à **ADMIN > Services**.  
La vue Services s'affiche.
2. Sélectionnez chaque service **Decoder**.

The screenshot displays the NetWitness Platform interface. At the top, there is a navigation bar with tabs for Hosts, Services, Event Sources, Health & Wellness, System, and Security. The 'Services' tab is selected. Below the navigation bar, there is a toolbar with icons for 'Change Service', 'S5Decoder - Decoder', and 'System'. A secondary toolbar contains icons for 'Upload Packet Capture File', 'Stop Capture', 'Host Tasks', 'Shutdown Service', 'Shutdown Appliance Service', and 'Reboot'. The main content area is divided into four sections: 'Decoder Service Information', 'Appliance Service Information', 'Decoder User Information', and 'Host User Information'. Each section contains a table of service details.

Decoder Service Information		Appliance Service Information	
Name	S5Decoder (Decoder)	Name	S5Decoder (Host)
Version	11.1.0.0	Version	11.1.0.0
Memory Usage	2858 MB (2.54% of 110 GB)	Memory Usage	25964 KB (0.02% of 110 GB)
CPU	1%	CPU	0%
Running Since	2018-Feb-08 02:32:47	Running Since	2018-Feb-06 22:14:56
Uptime	11 hours 23 minutes 46 seconds	Uptime	1 day 15 hours 41 minutes 38 seconds
Current Time	2018-Feb-08 13:56:33	Current Time	2018-Feb-08 13:56:34

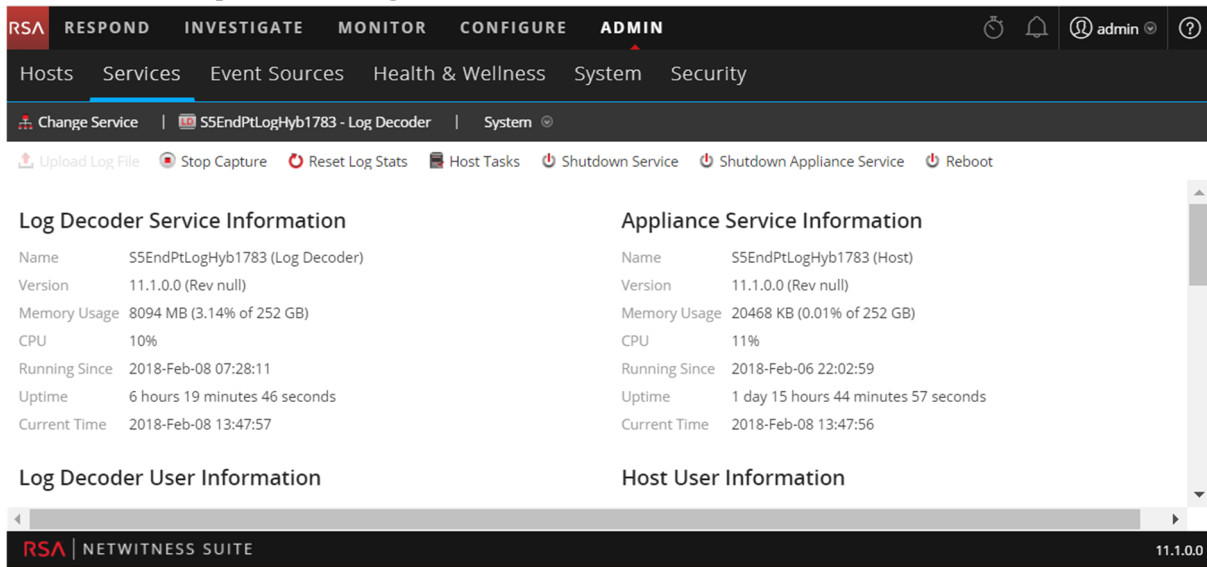
3. Sous  (actions), sélectionnez **Afficher > Système**.
4. Dans la barre d'outils, cliquez sur  **Stop Capture**.

### Arrêter la capture des logs

1. Connectez-vous à NetWitness Platform 11.0.x et accédez à **ADMIN > Services**.  
La vue Services s'affiche.



2. Sélectionnez chaque service **Log Decoder**.



3. Sous  (actions), sélectionnez **Afficher > Système**.

4. Dans la barre d'outils, cliquez sur  **Stop Capture**.

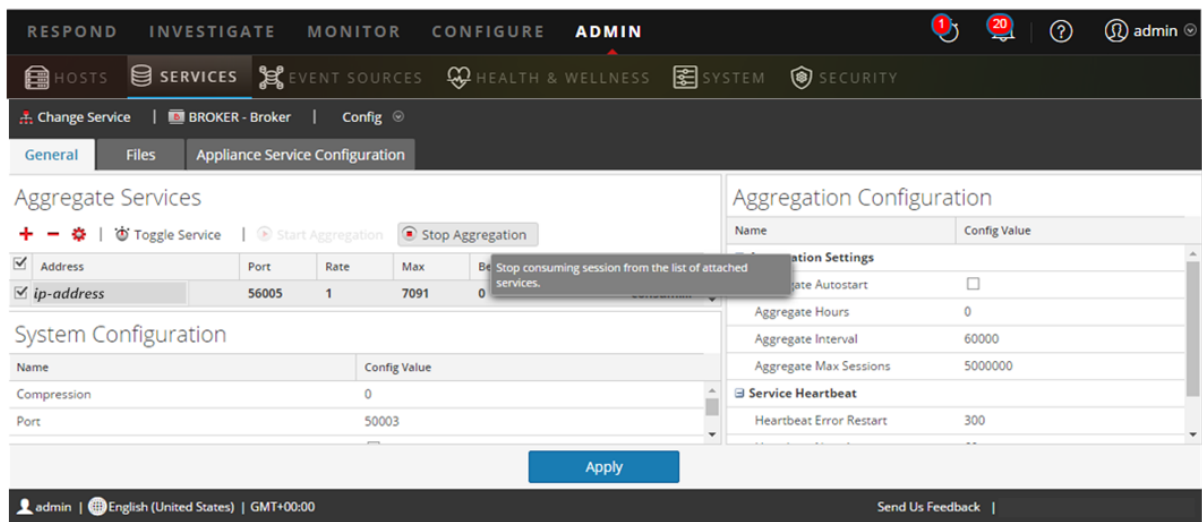
**Arrêter l'agrégation**

1. Connectez-vous à NetWitness Platform 11.0.x et accédez à **ADMIN > Services**.

2. Sélectionnez le service **Broker**.

3. Sous  (actions), sélectionnez **Afficher > Config**.

4. L'onglet **Général** s'affiche.



5. Sous **Services agrégés**, cliquez sur  **Stop Aggregation**.

## Hôtes Azure

### Tâche 4 - (Conditionnel) Configuration requise pour la préparation de la mise à jour Azure Host

Examinez votre déploiement d'hôte Azure pour les trois conditions suivantes et si nécessaire, exécutez les tâches en fonction de ces conditions.

- Si vous disposez d'une image de base Azure 11.0.0.0 sur l'hôte (même si vous avez mis à jour l'hôte vers 11.1.0. x), créez un référentiel Centos-Base.

**Attention :** Si le RPM `libgudev1-219-30.e17_3.9.x86_64` n'existe pas, n'effectuez pas les étapes suivantes.

1. Ouvrez une session SSH sur l'hôte du serveur NW.
  2. Exécutez la commande suivante depuis le répertoire NW Server Host `root` .  

```
yum remove libgudev1-219-30.e17_3.9.x86_64
```
  3. Créez un référentiel Centos-Base comme décrit à l'étape 6 de la procédure **CentOS 7.0+** (<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/create-upload-centos#centos-70>).
  4. Exécutez les chaînes de commande suivantes à partir du répertoire Hôte de serveur NW `root` .  

```
yum clean all
yum install WALinuxAgent
sudo systemctl enable waagent
```
  5. Supprimez le référentiel CentOS-base.
- Si le chemin d'accès à la mise à jour est 11.0.0. x à 11.2, remplissez le référentiel avec des packages supplémentaires.  
 Contactez le support client (<https://community.rsa.com/docs/DOC-1294>) pour le fichier `nw-azure-11.1-extras.zip`).
    1. Ouvrez une session SSH sur l'hôte du serveur NW.
    2. Accédez au `root` répertoire de l'hôte du serveur NW.
    3. Exécutez les chaînes de commande suivantes pour extraire le fichier zip Azure.  

```
mkdir -p /var/lib/netwitness/common/repo/11.2.0.0/OS/other+
unzip nw-azure-11.1-extras.zip -d
/var/lib/netwitness/common/repo/11.2.0.0/OS/other
```
    4. Si vous utilisez un référentiel externe,
  - Si vous utilisez un référentiel externe pour appliquer les mises à jour, mettez à jour le référentiel externe avec les packages supplémentaires.
    1. Après avoir configuré le contenu 11.2.0.0 sur le référentiel externe, accédez au `<base-directory>11.2.0.0/OS/other` de ce référentiel.

2. Exécutez la chaîne de commande suivante pour extraire le fichier zip Azure à partir du répertoire 11.2.0.0/OS du référentiel externe.  
`unzip nw-azure-11.1-extras.zip -d /<base-directory/11.2.0.0/OS/other`
3. Exécutez les commandes suivantes à partir du répertoire 11.2.0.0/OS du référentiel externe.  
`createrepo`

## Endpoint Insights

### Tâche 5 - (Conditionnel) Sauvegarde des mappages de métadonnées personnalisés existants avant d'appliquer la mise à jour 11.2 à l'hôte du point de terminaison

Dans 11.2, RSA a amélioré les mappages de métadonnées du point de terminaison pour s'aligner avec les modifications actuelles du modèle de données unifiées (UDM). Lorsque vous appliquez la mise à jour 11.2 à votre hôte Endpoint Insights, il efface le mappage personnalisé existant pour éviter de remplacer les mappages de métadonnées par défaut nouvellement ajoutés. Si vous souhaitez utiliser le mappage de métadonnées personnalisé existant, RSA vous recommande de sauvegarder les mappages personnalisés existants avant de mettre à jour l'hôte Endpoint Insights vers la version 11.2. Pour effectuer une sauvegarde :

1. Exécutez l'API `get-custom` via NW-Shell. La liste des mappages personnalisés s'affiche.
2. Copiez les mappages personnalisés manuellement dans un répertoire sécurisé.

Pour plus d'informations, voir le *Guide de configuration d'Endpoint Insights*. Accédez à la [Table des matières principale](#) pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

## Reporting Engine

### Tâche 6 - Configurer Reporting Engine pour les graphiques prêts à l'emploi

Pour que les graphiques prêts à l'emploi s'exécutent après la mise à jour, vous devez configurer la source de données par défaut à la page de Configuration de Reporting Engine avant d'effectuer la mise à jour. Si vous n'effectuez pas cette tâche, vous devez configurer manuellement la source de données après la mise à jour. Pour plus d'informations sur les sources de données Reporting Engine, consultez le *NetWitness Platform Guide de configuration de Reporting Engine 11.2*. Accédez à la [Table des matières principale](#) pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

## Répondre

### Tâche 7 - (Conditionnel) Restaurer les clés personnalisées du service Respond

Si vous avez ajouté des clés personnalisées dans `var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` pour les utiliser avec la clause `groupBy` de la version 11.0, copiez et enregistrez les clés personnalisées dans un fichier.

## Tâche 8 - Sauvegarder les scripts de normalisation personnalisés du service

### Respond

RSA a réintégré les scripts de normalisation du service Respond sont stockés dans le répertoire `/var/lib/netwitness/respond-server/scripts` pour la version 11.2.0.0. Vous devez les sauvegarder dans la version 11.0.x avant de passer à la version 11.2.0.0 afin de pouvoir les restaurer dans la version 11.2.0.0 comme décrit dans les tâches à effectuer après la mise à jour de [Répondre](#).

1. Accédez au répertoire `/var/lib/netwitness/respond-server/scripts`.
2. Sauvegardez les fichiers suivants :  
data\_privacy\_map.js  
normalize\_alerts.js  
normalize\_core\_alerts.js  
normalize\_ecat\_alerts.js  
normalize\_ma\_alerts.js  
normalize\_wtd\_alerts.js  
utils.js
3. (Conditionnel) Si vous avez ajouté une logique personnalisée dans la version 11.0.x ou dans une version précédente, copiez et enregistrez cette logique à partir des scripts sauvegardés afin de pouvoir la restaurer dans la version 11.2.0.0.

## Tâches de mise à jour

---

Effectuez les tâches suivantes pour effectuer la mise à jour de NetWitness Platform 11.0.x.x ou 11.1.x.x vers la version 11.2.0.0.

Deux méthodes permettent d'appliquer les mises à jour de version à un hôte.

**Remarque :** Si vous envisagez d'utiliser un référentiel de mise à jour pour NetWitness Platform 11.2.0.0 différent du référentiel que vous avez configuré pour la version 11.0.x.x ou 11.1.x.x, reportez-vous à la section [Annexe C. Configurer le référentiel externe](#) pour obtenir des instructions.

- Appliquer les mises à jour à partir de la vue Hôte (accès Web)
- Appliquer les mises à jour à partir de la ligne de commande (sans accès Web)

### Appliquer les mises à jour à partir de la vue Hôtes (Accès Web)

Vous devez effectuer deux tâches pour appliquer les mises à jour à partir de la vue Hôtes :

- Tâche 1. Renseigner le référentiel local ou Configurer un référentiel externe : vérifiez que vous disposez bien des dernières mises à jour de version.
- Tâche 2. Appliquer les mises à jour à chaque hôte à partir de la vue Hôtes.

#### Tâche 1. Renseigner le référentiel local ou Configurer un référentiel externe

Lorsque vous configurez votre serveur NW pour la version 11.2.0.0, vous sélectionnez le référentiel local ou un référentiel externe. La vue Hôtes récupère les mises à jour de version dans le référentiel que vous sélectionnez.

Si vous avez sélectionné le référentiel local, il est inutile de le configurer, mais vous devez vous assurer qu'il est renseigné avec les dernières mises à jour de version. Reportez-vous à la section [Annexe B. Renseigner le référentiel local](#) pour obtenir des instructions sur la façon de le renseigner avec la mise à jour de version.

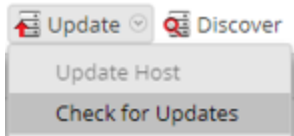
Si vous avez sélectionné un référentiel externe, vous devez le configurer. Reportez-vous à la section [Annexe C. Configurer le référentiel externe](#) pour obtenir des instructions sur la façon de configurer un référentiel externe.

## Tâche 2. Appliquer les mises à jour à chaque hôte à partir de la vue Hôtes

La vue Hôtes affiche les mises à jour de version logicielle disponibles dans votre référentiel de mises à jour local. Vous pouvez choisir d'appliquer les mises à jour que vous souhaitez à partir de cette vue.

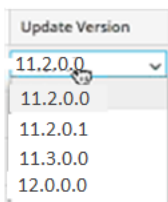
Cette procédure vous indique comment mettre à jour un hôte vers une nouvelle version de NetWitness Platform.

1. Connectez-vous à NetWitness Platform.
2. Accédez à **ADMIN > HÔTES**.
3. (Conditionnel) Vérifiez les dernières mises à jour.



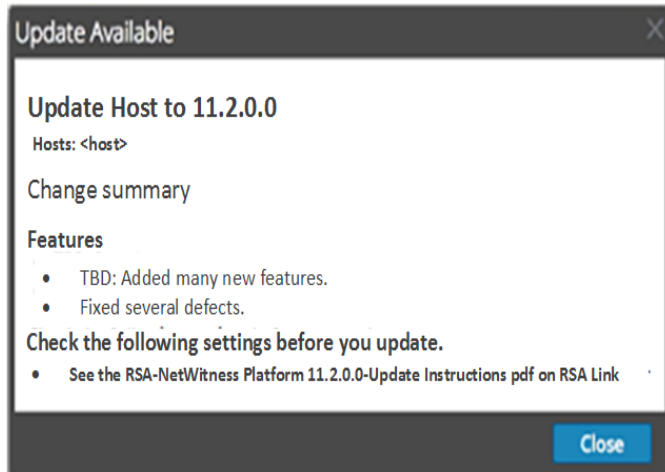
4. Sélectionnez un ou plusieurs hôtes.  
Vous devez d'abord mettre à jour le serveur NW vers la version la plus récente. Vous pouvez mettre à jour les autres hôtes dans l'ordre que vous préférez, mais RSA vous recommande de suivre les instructions figurant dans « Fonctionnement en mode Mixte » du *Guide de mise en route des hôtes et des services RSA NetWitness Platform* pour obtenir plus d'informations.  
**Mise à jour disponible** s'affiche dans la colonne **État** si vous disposez d'une version mise à jour dans le référentiel de mises à jour local pour les hôtes sélectionnés.

5. Sélectionnez la version que vous souhaitez appliquer à partir de la colonne **Mettre à jour la version**.



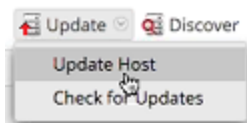
Si vous :

- Souhaitez mettre à jour un ou plusieurs hôtes de cette version après la mise à jour de l'hôte du Serveur NW, cochez la case à gauche des hôtes. Seules les versions des mises à jour actuellement prises en charge sont répertoriées.
- Pour afficher une boîte de dialogue avec les principales caractéristiques de la mise à jour et les informations sur les mises à jour, cliquez sur l'icône d'informations (i) à droite du numéro de version de mise à jour. La figure suivante donne un exemple de cette boîte de dialogue.

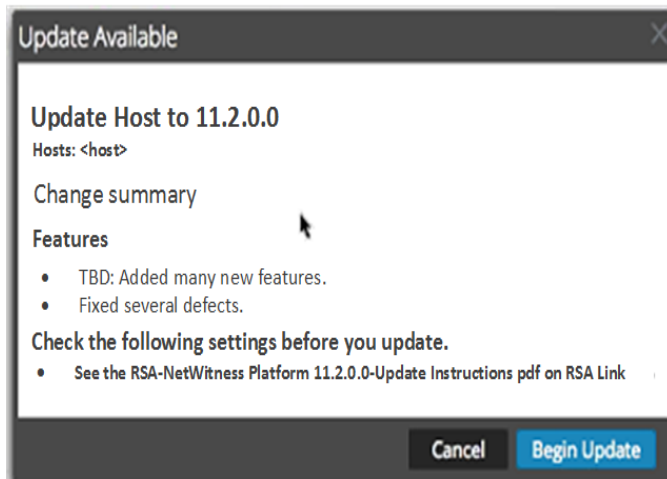


- Impossible de trouver la version souhaitée, sélectionnez **Mettre à jour > Rechercher les mises à jour** pour vérifier le référentiel pour les mises à jour disponibles. Si une mise à jour est disponible, le message « Les nouvelles mises à jour sont disponibles » s'affiche et la colonne **État** se met automatiquement à jour pour afficher les **mises à jour disponibles**. Par défaut, seules les mises à jour prises en charge par l'hôte sélectionné sont affichées.

6. Cliquez sur **Mettre à jour > Mettre à jour l'hôte** dans la barre d'outils.



Une boîte de dialogue s'affiche avec des informations sur la mise à jour sélectionnée. Cliquez sur **Commencer la mise à jour**.



La colonne **État** vous indique ce qui se passe dans chacune des phases suivantes de la mise à jour :

- Phase 1 - **Téléchargement des packages de mises à jour** -Télécharge les artéfacts du référentiel sur le Serveur NW applicable aux services sur l'hôte que vous avez choisi.
  - Phase 2 - **Configuration des packages de mise à jour** -Configure les fichiers de mise à jour au format approprié.
  - Phase 3 - **Mise à jour en cours** - Met l'hôte à jour vers la nouvelle version.
7. Lorsque vous voyez **Mise à jour en cours d'exécution**, actualisez le navigateur. Cela peut vous envoyer vers l'écran de connexion NetWitness. Si cela se produit, connectez-vous et revenez à la vue Hôte. Une fois l'hôte mis à jour, NetWitness Platform vous invite à **redémarrer l'hôte**.
8. (Conditionnel - Pour l'hôte avec stockage Unity uniquement) Si l'hôte (par exemple, l'hôte du décodeur réseau) dispose d'un stockage Unity configuré avec PowerPath sur 11.1.x.x et que la version de PowerPath installée est EMCPower.LINUX.6.3.0.b049, utilisez SSH pour vous connecter à l'hôte et soumettez les commandes suivantes pour installer la nouvelle version de PowerPath (c'est-à-dire, DellEMCPower.LINUX.6.4.0.b095).
- ```
systemctl stop nwdecoder
umount -R /var/netwitness/decoder
yum update DellEMCPower.LINUX-6.4.0.00.00-095.RHEL7.x86_64.rpm
```
9. Cliquez sur **Redémarrer l'hôte** dans la barre d'outils. NetWitness Platform indique l'état **Redémarrage...** jusqu'à ce que l'hôte soit de nouveau en ligne. Une fois que l'hôte est de nouveau en ligne, l'**État** affiche **À jour**. Contactez le support client si l'hôte ne revient pas en ligne.



**Remarque :** 1.) Si vous avez activé DISA STIG, l'ouverture des services de base peut prendre environ 5 à 10 minutes. Ce délai est dû à la génération de nouveaux certificats. 2.) Si vous disposez du stockage Unity, contrôlez l'état de PowerPath et vérifiez qu'il peut voir le périphérique Unity.

## Appliquer les mises à jour à partir de la ligne de commande (sans accès Web)

Si votre déploiement de RSA NetWitness Platform n'a pas d'accès Web, exécutez la procédure suivante pour appliquer une mise à jour de version.

1. Téléchargez le package de mise à jour .zip pour la version souhaitée (par exemple, netwitness-11.2.0.0.zip) à partir de RSA Link vers un répertoire local.
2. Ouvrez une session SSH sur l'hôte du serveur NW.
3. Créez un répertoire intermédiaire /tmp/upgrade/<version> pour la version que vous souhaitez (par exemple, /tmp/upgrade/11.2.0.0).  

```
mkdir -p /tmp/upgrade/11.2.0.0
```
4. Copiez le package de mise à jour .zip vers un répertoire sur le serveur NW autre que le répertoire intermédiaire (par exemple répertoire /tmp ).
5. Décompressez le package dans le répertoire temporaire que vous avez créé (par exemple, /tmp/upgrade/11.2.0.0).  

```
unzip /<download-location>/netwitness-11.2.0.0.zip -d /tmp/upgrade/11.2.0.0
```
6. Initialisez la mise à jour sur le serveur NW.  

```
upgrade-cli-client --init --version 11.2.0.0 --stage-dir /tmp/upgrade/
```
7. Appliquez la mise à jour au serveur NW.  

```
upgrade-cli-client --upgrade --host-addr <NW Server IP> --version 11.2.0.0
```
8. Connectez-vous à NetWitness Platform et redémarrez l'hôte du Serveur NW dans la vue Hôte.
9. Appliquez la mise à jour à chaque hôte du serveur NW.  

```
upgrade-cli-client --upgrade --host-addr <non-NW Server IP address> --version 11.2.0.0
```

La mise à jour est terminée lorsque l'interrogation est terminée.
10. (Conditionnel) Si l'hôte (par exemple, l'hôte du décodeur réseau) dispose d'un stockage Unity configuré avec PowerPath sur 11.1.x.x, et que la version de PowerPath installée est EMCPower.LINUX.6.3.0.b049, établissez une connexion SSH avec l'hôte et soumettez les commandes suivantes pour installer la nouvelle version de PowerPath (c'est-à-dire, DelleMCPower.LINUX.6.4.0.b095).  

```
systemctl stop nwdecoder
umount -R /var/netwitness/decoder
yum update DelleMCPower.LINUX-6.4.0.00.00-095.RHEL7.x86_64.rpm
```
11. Connectez-vous à NetWitness Platform et redémarrez l'hôte dans la vue Hôte.  

Vous pouvez vérifier la version appliquée à l'hôte avec la commande suivante :

```
upgrade-cli-client --list
```

**Remarque :** 1.) Si vous avez activé DISA STIG, l'ouverture des services de base peut prendre environ 5 à 10 minutes. Ce délai est dû à la génération de nouveaux certificats. 2.) Si vous disposez du stockage Unity, contrôlez l'état de PowerPath et vérifiez qu'il peut voir le périphérique Unity.



## Mettre à jour ou installer la Collection Windows d'ancienne génération

---

Reportez-vous au *Guide RSA NetWitness Legacy Windows Collection*. Accédez à la [Table des matières principale](#) pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

**Remarque :** après avoir mis à jour ou installé la Collection Windows d'ancienne génération, redémarrez le système pour vous assurer que Log Collection fonctionne correctement.

## Tâches à effectuer après la mise à jour

---

Effectuez les tâches suivantes après avoir effectué la mise à jour vers NetWitness Platform 11.2.0.0.

- [Général](#)
- [Serveur NW](#)
- [Endpoint Insights](#)
- [Event Stream Analysis](#)
- [Respond](#)
- [NetWitness UEBA](#)



## Général

Ces tâches s'appliquent à tous les clients NetWitness Platform 11.2.0.0



### Tâche 1 - Démarrer la capture et l'agrégation des données

Redémarrez la capture/agrégation du réseau et des logs après la mise à jour vers la version 11.2.0.0.


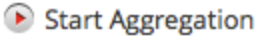
#### Démarrer la capture réseau

1. Dans le menu **NetWitness Platform**, sélectionnez **ADMIN > Services**.  
La vue Services s'affiche.
2. Sélectionnez chaque service **Decoder**.
3. Sous  (actions), sélectionnez **Afficher > Système**.
4. Dans la barre d'outils, cliquez sur  .

#### Démarrer la capture des logs


1. Dans le menu **NetWitness Platform**, sélectionnez **ADMIN > Services**.  
La vue Services s'affiche.
2. Sélectionnez chaque service **Log Decoder**.
3. Sous  (actions), sélectionnez **Afficher > Système**.
4. Dans la barre d'outils, cliquez sur  .

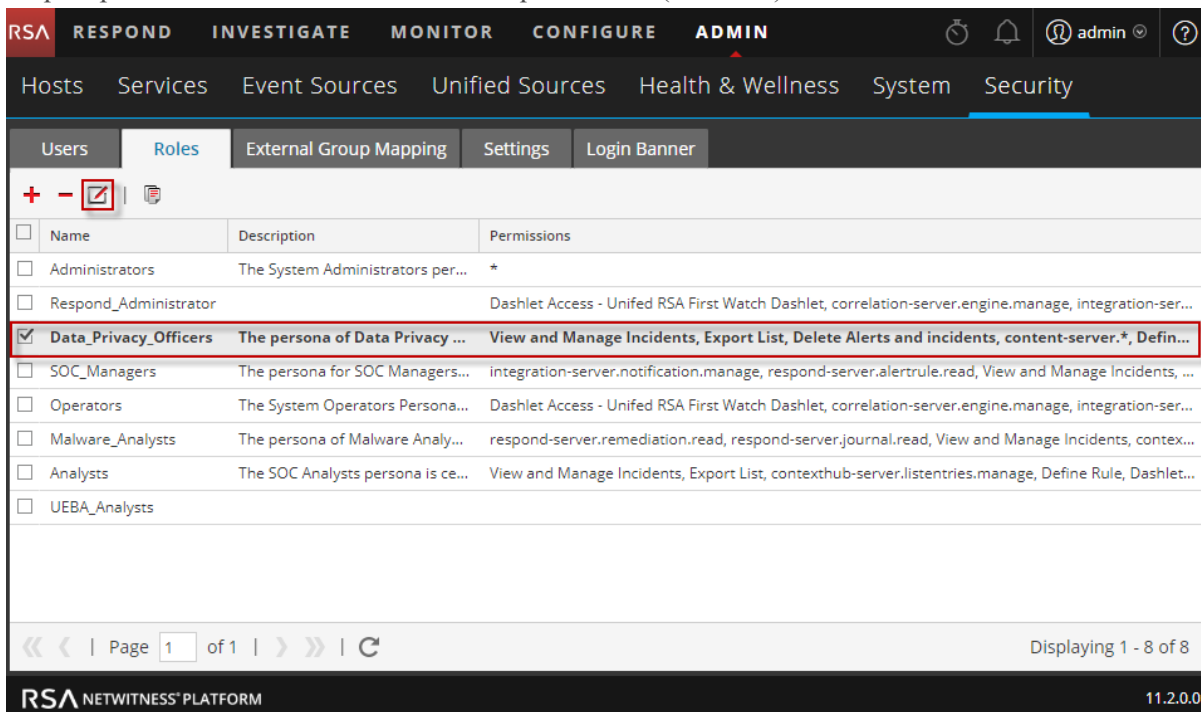
#### Démarrer l'agrégation

1. Dans le menu **NetWitness Platform**, sélectionnez **ADMIN > Services**.  
La vue Services s'affiche.
2. Pour chaque service Concentrator et Broker.
  - a. Sélectionnez le service.
  - b. Sous  (actions), sélectionnez **Vue > Config**.
  - c. Dans la barre d'outils, cliquez sur  .

## Tâche 2 - Configurer les actions des menus contextuels d'Autorisations utilisateur

Effectuez les étapes suivantes pour les rôles des **Analystes**, **Responsables du SOC**, **Agents de confidentialité des données** afin de configurer les actions de leur menu contextuel. Vous devez effectuer ces étapes pour les rôles des **Analystes**, **Responsables du SOC** et **Agents de confidentialité des données**.

1. Dans le menu **NetWitness Platform**, sélectionnez **ADMIN > Sécurité > Rôles**.
2. Double-cliquez sur le rôle d'utilisateur (par exemple **Agents de confidentialité des données**), ou cliquez pour sélectionner l'utilisateur et cliquez sur  (Modifier).



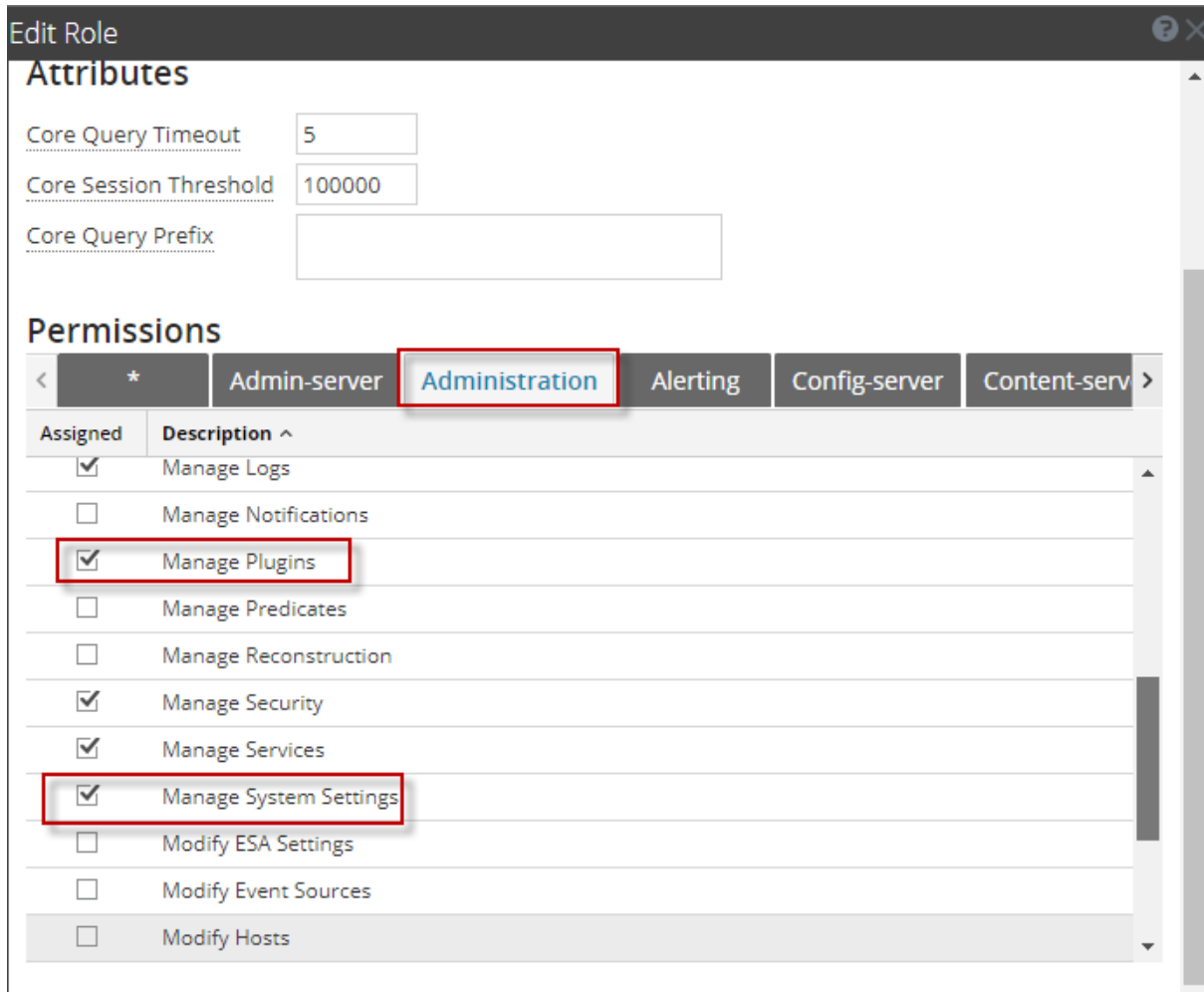
The screenshot shows the NetWitness Platform Admin console. The top navigation bar includes 'RSA', 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. The 'ADMIN' menu is expanded to show 'Hosts', 'Services', 'Event Sources', 'Unified Sources', 'Health & Wellness', 'System', and 'Security'. The 'Security' menu is further expanded to show 'Users', 'Roles', 'External Group Mapping', 'Settings', and 'Login Banner'. The 'Roles' tab is active, displaying a table of roles. The 'Data\_Privacy\_Officers' role is selected, and its permissions are highlighted with a red box.

| <input type="checkbox"/>            | Name                  | Description                       | Permissions                                                                                            |
|-------------------------------------|-----------------------|-----------------------------------|--------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/>            | Administrators        | The System Administrators per...  | *                                                                                                      |
| <input type="checkbox"/>            | Respond_Administrator |                                   | Dashlet Access - Unified RSA First Watch Dashlet, correlation-server.engine.manage, integration-ser... |
| <input checked="" type="checkbox"/> | Data_Privacy_Officers | The persona of Data Privacy ...   | View and Manage Incidents, Export List, Delete Alerts and incidents, content-server.*, Defini...       |
| <input type="checkbox"/>            | SOC_Managers          | The persona for SOC Managers...   | integration-server.notification.manage, respond-server.alertrule.read, View and Manage Incidents, ...  |
| <input type="checkbox"/>            | Operators             | The System Operators Persona...   | Dashlet Access - Unified RSA First Watch Dashlet, correlation-server.engine.manage, integration-ser... |
| <input type="checkbox"/>            | Malware_Analysts      | The persona of Malware Analy...   | respond-server.remediation.read, respond-server.journal.read, View and Manage Incidents, contex...     |
| <input type="checkbox"/>            | Analysts              | The SOC Analysts persona is ce... | View and Manage Incidents, Export List, contexthub-server.listentries.manage, Define Rule, Dashlet...  |
| <input type="checkbox"/>            | UEBA_Analysts         |                                   |                                                                                                        |

Page 1 of 1 | Displaying 1 - 8 of 8

RSA NETWITNESS® PLATFORM 11.2.0.0

3. Dans la vue **Modifier un rôle** sous **Autorisations**, cochez les cases à cocher **Gérer les logs**, **Gérer les plugins** et **Gérer les paramètres système**, puis cliquez sur **Enregistrer**.



The screenshot shows the 'Edit Role' window with the 'Administration' tab selected. The 'Attributes' section contains three input fields: 'Core Query Timeout' (5), 'Core Session Threshold' (100000), and 'Core Query Prefix' (empty). The 'Permissions' section shows a list of permissions with checkboxes. The 'Administration' tab is highlighted in red. The 'Manage Plugins' and 'Manage System Settings' permissions are also highlighted with red boxes.

| Assigned                            | Description ^          |
|-------------------------------------|------------------------|
| <input checked="" type="checkbox"/> | Manage Logs            |
| <input type="checkbox"/>            | Manage Notifications   |
| <input checked="" type="checkbox"/> | Manage Plugins         |
| <input type="checkbox"/>            | Manage Predicates      |
| <input type="checkbox"/>            | Manage Reconstruction  |
| <input checked="" type="checkbox"/> | Manage Security        |
| <input checked="" type="checkbox"/> | Manage Services        |
| <input checked="" type="checkbox"/> | Manage System Settings |
| <input type="checkbox"/>            | Modify ESA Settings    |
| <input type="checkbox"/>            | Modify Event Sources   |
| <input type="checkbox"/>            | Modify Hosts           |

4. Terminez les étapes 1 à 3 pour les rôles **Analystes** et **Responsables du SOC** en plus des **Agents de confidentialité des données**.




## Serveur NW

### Tâche 3 - (Conditionnel) Corriger les modèles de journal d'audit qui ne sont pas mis à jour dans le fichier de configuration de sortie Logstash

**Problème :** Lorsqu'un utilisateur effectue une mise à jour de la version 11.0.0.0 vers la version 11.2.0.0, si un audit global est configuré, les modèles de journal d'audit ne sont pas mis à jour dans le fichier de configuration de sortie Logstash.

**Contournement :** Si l'audit global est configuré, vous devez modifier l'une des entrées syslog sur les serveurs de notifications globales et cliquer sur Enregistrer pour appliquer la dernière configuration du journal d'audit.

Si vous avez configuré l'audit global dans la version 11.0.x, vous devez effectuer la procédure suivante pour appliquer la dernière configuration d'audit global.

1. Dans le menu **NetWitness Platform**, sélectionnez **ADMIN > Système > Notifications globales**. La vue **Notifications globales** s'affiche.
2. Cliquez sur l'onglet **Serveurs**, sélectionnez n'importe quel serveur syslog.
3. Cliquez sur  (icône de modification), puis cliquez sur **Enregistrer**.

### (Conditionnel) Tâche 4 - Reconfigurer l'authentification PAM pour Radius

Si vous avez configuré l'authentification PAM pour Radius dans la version 11.0.x.x à l'aide du package `pam_radius`, vous devez la reconfigurer dans la version 11.2.0.0 en utilisant le `pam_radius_auth` package pour obtenir de meilleures performances. Pour obtenir des instructions, reportez-vous à la section « Configurer la fonctionnalité de connexion PAM » dans le *Guide de la sécurité du système et de la gestion des utilisateurs RSA NetWitness® Platform 11.2*. Accédez à la [Table des matières principale](#) pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

## Endpoint Insights

### Tâche 5 - Reconfigurer un feed récurrent configuré à partir d'une ancienne version Endpoint parce que la version Java a changé.

Vous devez reconfigurer le feed récurrent d'une ancienne version Endpoint en raison de la modification dans la version de Java. Procédez comme suit pour résoudre ce problème.

1. Importez le certificat de l'autorité de certification NetWitness Endpoint dans le magasin de confiance NetWitness Platform, comme décrit dans « Exporter le certificat SSL de NetWitness Endpoint » dans la rubrique « Configurer des données contextuelles à partir de Endpoint via un feed récurrent » du *Guide d'intégration de RSA NetWitness Endpoint* pour importer le certificat. Accédez à la [Table des matières principale](#) pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

### Tâche 6 - Restaurer les mappages de métadonnées personnalisés des points de terminaison sauvegardés

RSA recommande de ne pas substituer les mappages par défaut 11,2, sauf si nécessaire. Si vous avez sauvegardé les mappages personnalisés 11.1.x.x, avant d'effectuer la mise à jour vers la version 11.2, examinez la liste des mappages personnalisés et restaurez uniquement ceux qui ne sont pas déjà dans les paramètres par défaut, à l'aide de `set-custom API` par l'intermédiaire de NW-Shell.

Pour modifier les mappages, consultez le *Guide de configuration de Endpoint Insights*. Accédez à la [Table des matières principale](#) pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

## Event Stream Analysis

Ces tâches s'appliquent aux clients NetWitness Platform 11.2.0.0 à l'aide d'Event Stream Analysis.

### (Conditionnel) Tâche 7 - Reconfigurer la règle d'agrégation « Communication de commande et contrôle suspect par domaine » pour la détection automatisée des menaces

Dans la version 11.0, la règle d'agrégation « Communication de commande et contrôle suspect par domaine » avec la condition Regrouper par sur « Domaine de C&C suspect » ne fonctionnait pas comme prévu et devait être remplacée par « Domaine » pour agréger les alertes et permettre la création d'incidents pour la condition « C&C suspect ». La condition « Domaine de C&C suspect » fonctionne correctement dans la version 11.2.0.0 et doit être utilisée en tant que condition Regrouper par pour la règle d'agrégation « Communication de commande et contrôle suspect par domaine » (connue sous le nom de règle d'incident dans la version 11.2.0.0).

Si vous avez remplacé la condition Regrouper par de la règle d'agrégation « Communication de commande et contrôle suspect par domaine » par « Domaine » pour la version 11.0, vous devrez la redéfinir sur « Domaine de C&C suspect » pour la version 11.2.0.0.

1. Dans le menu **NetWitness Platform**, sélectionnez **CONFIGURER > Règles de l'incident**.
2. Dans la liste Règles de l'incident, localisez la commande Communication et contrôle suspect par domaine, puis cliquez sur le lien dans le champ NOM pour l'ouvrir.
3. Dans la section Options de regroupement de la vue Détails de la règle d'incident, définissez le champ Regrouper par sur Domaine de C&C suspect, puis cliquez sur Enregistrer.

Pour plus d'informations, reportez-vous au Guide de détection automatisée des menaces pour NetWitness Platform et à la

section « Configurer ESA Analytics » du Guide de configuration NetWitness Platform ESA. Accédez à la [Table des matières principale](#) pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

## Répondre

### Tâche 8 - Obtenir la dernière version du schéma de la règle d'agrégation et restaurer les clés personnalisées du service Respond

Exécutez la procédure suivante pour obtenir la dernière version du schéma de la règle d'agrégation et pour restaurer les clés personnalisées de n'importe quel service Respond.

1. Supprimez le fichier `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json`.
2. Redémarrez le serveur Respond pour obtenir la dernière version du fichier `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json`.  

```
systemctl restart rsa-nw-respond-server
```
3. Si vous avez ajouté des clés personnalisées dans le fichier `var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` pour les utiliser dans la clause `groupBy` de la version 11.0, modifiez le fichier `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` et ajoutez les clés personnalisées précédemment enregistrées en tant que tâche de préparation de la mise à jour.

**Remarque :** De nouveaux champs Regrouper par ont été ajoutés au service Respond dans la version 11.2.0.0. Ces nouveaux champs Regrouper par ne seront pas visibles dans l'interface utilisateur de NetWitness Platform si vous n'obtenez pas la dernière version du fichier à partir du serveur.

## Tâche 9 - Obtenir la dernière version des scripts de normalisation du service

### Respond et restaurer les scripts de normalisation personnalisés du service

#### Respond

RSA a réintégré les scripts de normalisation du service Respond dans le répertoire `/var/lib/netwitness/respond-server/scripts 11.2.0.0`. Vous devez remplacer les anciennes versions.

Avant la mise à jour vers la version 11.2.0.0, vous sauvegardiez les fichiers suivants dans le répertoire

```
/var/lib/netwitness/respond-server/scripts .
```

```
data_privacy_map.js  
normalize_alerts.js  
normalize_core_alerts.js  
normalize_ecat_alerts.js  
normalize_ma_alerts.js  
normalize_wtd_alerts.js  
utils.js
```

Exécutez la procédure suivante pour obtenir la dernière version des scripts de normalisation.

1. Une fois que vous avez sauvegardé les fichiers répertoriés ci-dessus, supprimez le répertoire `/var/lib/netwitness/respond-server/scripts` et son contenu.
2. Redémarrez le serveur Respond.  

```
systemctl restart rsa-nw-respond-server
```
3. (Conditionnel) Modifiez les nouveaux fichiers afin d'inclure la logique personnalisée des scripts 11.0 ayant été sauvegardés.

**Remarque :** Les fichiers suivants ont été modifiés avec la version 11.2.0.0 :

```
normalize_alerts.js  
aggregation_rule_schema.json
```

## Tâche 10 - Ajouter les autorisations des paramètres de notification de réponse

**Remarque :** Si vous avez déjà configuré ces autorisations dans 11.1, vous pouvez ignorer cette tâche.

Les autorisations liées aux paramètres de notification de réponse permettent aux administrateurs de la vue Répondre, aux responsables de la confidentialité des données et aux responsables du SOC d'accéder aux paramètres de notification de réponse (**CONFIGURER > Notifications de réponse**), ce qui leur permet d'envoyer des notifications par e-mail lorsque des incidents sont créés ou mis à jour.

Pour accéder à ces paramètres, vous devez ajouter des autorisations supplémentaires à vos rôles utilisateur intégrés et existants dans NetWitness Platform. Vous devrez également ajouter des autorisations à vos rôles personnalisés. Consultez la rubrique « Autorisations des paramètres de notification de réponse » dans le *Guide de configuration de NetWitness Respond*. Pour des informations détaillées sur les autorisations utilisateurs, reportez-vous à la rubrique *Guide de la sécurité du système et de la gestion des utilisateurs*. Accédez à la [Table des matières principale](#) pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

## Tâche 11 - Mettre à jour le groupe de règles de l'incident par défaut en fonction des valeurs

Quatre des règles d'incidents par défaut utilisent désormais l'« Adresse IP source » en tant que valeur Regrouper par.

- Alertes de risque élevé : Reporting Engine
- Alertes de risque élevé : Malware Analysis
- Alertes de risque élevé : NetWitness Endpoint
- Alertes de risque élevé : ESA

Pour mettre à jour les règles par défaut, remplacez la valeur Regrouper par des règles par défaut ci-dessus par « Adresse IP source ».

**Remarque :** Si vous avez déjà mis à jour les valeurs Regrouper par des règles par défaut répertoriées ci-dessus dans 11.1, vous n'avez pas à le refaire.

1. Dans le menu **NetWitness Platform**, sélectionnez **CONFIGURER > Règles de l'incident**, puis cliquez sur la règle que vous souhaitez mettre à jour dans la colonne **Nom**. La vue **Détails de la règle d'incident** s'affiche.
2. Dans le champ **REGROUPER PAR**, sélectionnez la nouvelle valeur Regrouper par dans la liste déroulante.
3. Cliquez sur **Enregistrer** pour mettre à jour la règle.

Pour agréger les alertes NetWitness Endpoint en fonction de l'adresse IP du détecteur, exécutez les étapes suivantes pour cloner la règle d'incident NetWitness Endpoint par défaut et modifier l'adresse IP de Regrouper par.

1. Dans le menu **NetWitness Platform**, sélectionnez **CONFIGURER > Règles de l'incident**. La vue **Liste des règles de l'incident** s'affiche.
2. Sélectionnez les **Alertes à risque élevé : règle d'incident par défaut de NetWitness Endpoint** et cliquez sur **Cloner**. Vous recevrez un message indiquant que vous avez cloné avec succès la règle sélectionnée.
3. Remplacez le nom de la règle par un nom approprié, tel que alertes à risque élevé : IP du détecteur NetWitness Endpoint.
4. Dans le champ **REGROUPER PAR**, supprimez l'adresse **IP source** et ajoutez l'adresse **IP du détecteur**. Il est important que l'adresse IP du détecteur soit la seule valeur Regrouper par répertoriée.
5. Cliquez sur **Enregistrer** pour créer la règle.

Pour obtenir des informations détaillées, consultez le *Guide de configuration NetWitness Platform Respond*. Accédez à la [Table des matières principale](#) pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

## NetWitness UEBA

### Tâche 12 - Installer NetWitness UEBA

NetWitness UEBA est une nouvelle fonctionnalité de NetWitness® Platform 11.2.

Reportez-vous aux informations suivantes :

Le *Guide d'installation des hôtes physiques RSA NetWitness Platform 11.2* pour obtenir des instructions relatives à l'installation sur un hôte physique.

Le *Guide d'installation des hôtes virtuels RSA NetWitness Platform 11.2* pour obtenir des instructions relatives à l'installation sur un hôte virtuel.

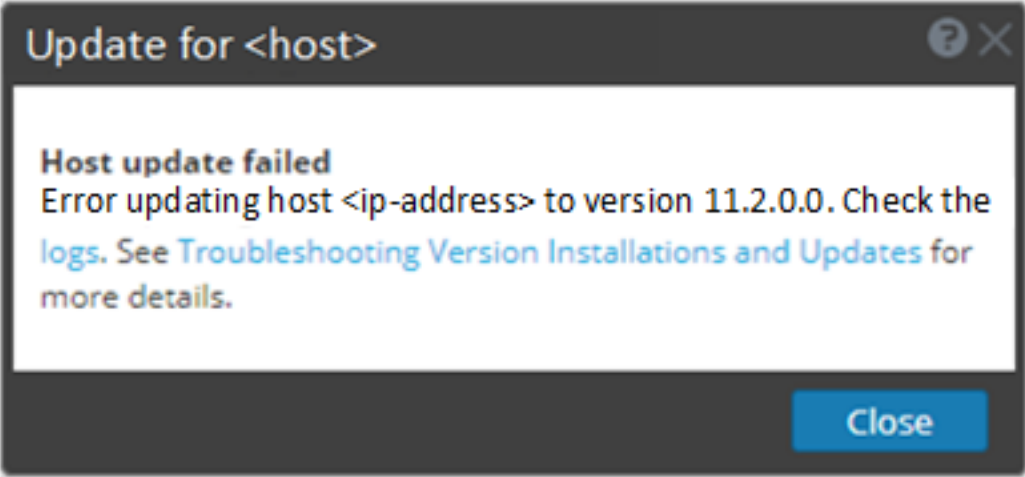
Le *Guide d'installation de RSA NetWitness UEBA* pour obtenir des informations sur UEBA.

Accédez à la [Table des matières principale](#) pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

6. Sélectionnez **Gérer les paramètres système** et **Gérer les plug-ins**.

## Annexe . Dépannage des installations et mises à jour de version

Cette section décrit les messages d'erreur affichés dans la vue **Hôtes** en cas de problèmes de mise à jour des versions de l'hôte et d'installation des services sur les hôtes dans la vue **Hôtes**. Si les solutions de dépannage suivantes ne vous permettent pas de résoudre un problème de mise à jour ou d'installation, contactez le support client (<https://community.RSA.com/docs/DOC-1294>).

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Message d'erreur | <p>Échec de la mise à jour de l'hôte</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Problème         | <p>Lorsque vous sélectionnez une version de mise à jour, puis cliquez sur <b>Mettre à jour &gt; Mettre à jour l'hôte</b>, le processus de téléchargement réussit, mais le processus de mise à jour échoue.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Solution         | <ol style="list-style-type: none"> <li>1. Essayez de nouveau d'appliquer la mise à jour de version à l'hôte. Souvent, cela est suffisant.</li> <li>2. Si vous ne pouvez pas appliquer la nouvelle mise à jour de version :       <ol style="list-style-type: none"> <li>a. Surveillez les logs suivants sur le serveur NW lors de sa progression (par exemple, soumettez la commande <code>tail -f</code> à partir de la ligne de commande) :           <pre> /var/netwitness/uax/logs/sa.log /var/log/netwitness/orchestration-server/orchestration-server.log /var/log/netwitness/deployment-upgrade/chef-solo.log /var/log/netwitness/config-management/chef-solo.log /var/lib/netwitness/config-management/cache/chef-stacktrace.out           </pre>           L'erreur s'affiche dans un ou plusieurs de ces logs.         </li> <li>b. Essayez de résoudre le problème et de réappliquer la mise à jour de version.           <ul style="list-style-type: none"> <li>• Cause 1 - Le mot de passe <code>deploy_admin</code> a expiré.<br/>Solution - Réinitialisez votre <code>deploy_admin</code> mot de passe.</li> </ul> </li> </ol> </li> </ol> |



Pour résoudre la Cause 1, procédez comme suit.

1. Dans le menu NetWitness Suite, sélectionnez **ADMIN > Sécurité > onglet Utilisateurs**.
2. Sélectionnez `deploy_admin`, puis cliquez sur **Réinitialiser le mot de passe**.
3. (Conditionnel) Si NetWitness Suite ne vous permet pas d'entrer le mot de passe `deploy_admin` ayant expiré dans la boîte de dialogue **Réinitialiser le mot de passe**, procédez comme suit.

- a. Réinitialisez `deploy_admin` pour utiliser un nouveau mot de passe.
- b. Sur tous les hôtes serveur autres que NW sur la version 11.x, exécutez la commande suivante à l'aide du mot de passe `deploy_admin` de correspondance à partir de l'hôte du serveur NW.

```
/opt/rsa/saTools/bin/set-deploy-admin-password
```

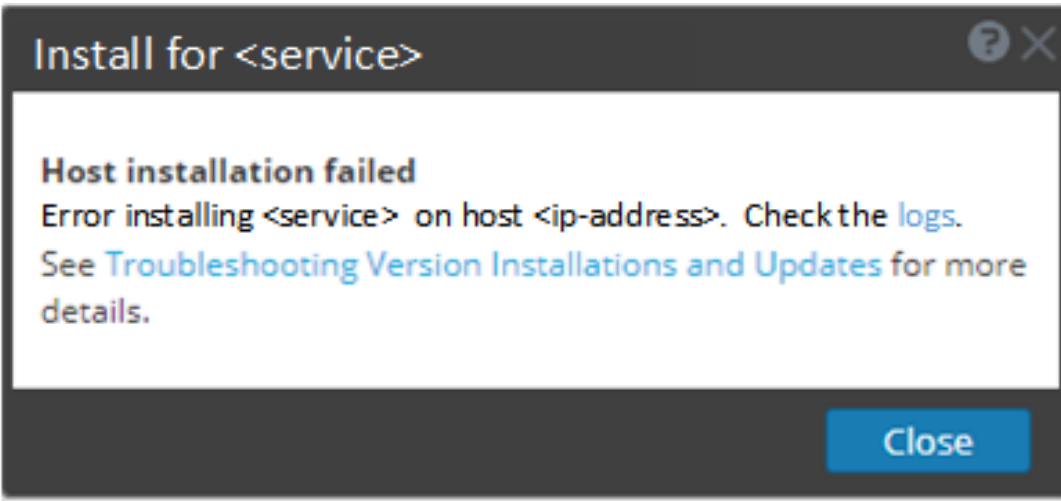
- Cause 2 - Le mot de passe `deploy_admin` a été modifié sur l'hôte serveur NW, pas sur les hôtes serveurs autres que NW.

Pour résoudre la Cause 2, procédez comme suit.

- Sur tous les hôtes serveur autres que NW sur la version 11.x, exécutez la commande suivante à l'aide du mot de passe `deploy_admin` de correspondance à partir de l'hôte du serveur NW.

```
/opt/rsa/saTools/bin/set-deploy-admin-password
```

3. Si vous ne pouvez toujours pas appliquer la mise à jour, collectez les logs comme indiqué à l'étape 2 et contactez le support client (<https://community.rsa.com/docs/DOC-1294>).

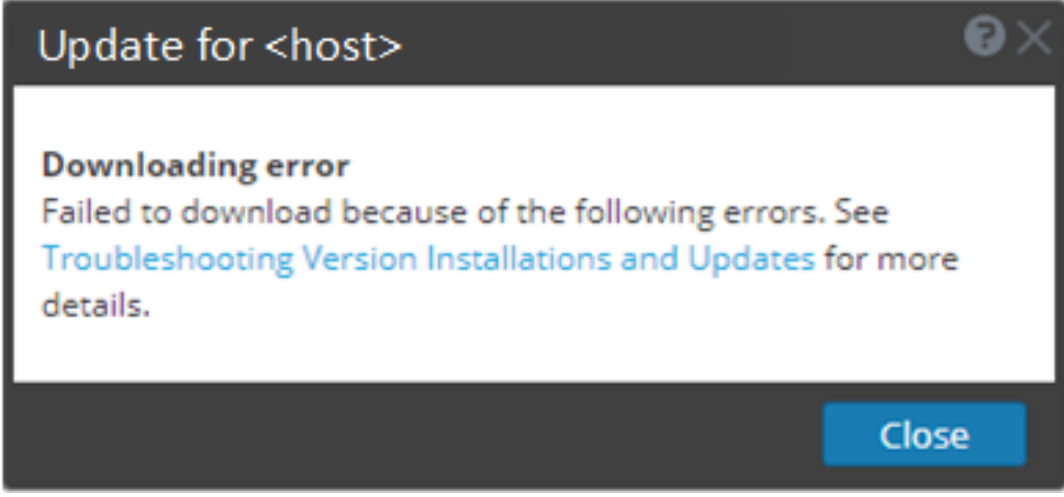
|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Message d'erreur</p> | <p>Échec de l'installation de l'hôte</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <p>Problème</p>         | <p>Lorsque vous sélectionnez un hôte, puis cliquez sur <b>Installer</b>, le processus du service d'installation échoue.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <p>Solution</p>         | <ol style="list-style-type: none"> <li>1. Essayez de réinstaller le service.<br/>Souvent, cela est suffisant.</li> <li>2. Si vous ne pouvez toujours pas installer le service :       <ol style="list-style-type: none"> <li>a. Surveillez les logs suivants sur le serveur NW lors de sa progression (par exemple, exécutez la chaîne de commande <code>tail -f</code> à partir de la ligne de commande) :           <pre>           /var/netwitness/uax/logs/sa.log           /var/log/netwitness/orchestration-server/orchestration-server.log           /var/log/netwitness/deployment-upgrade/chef-solo.log           /var/log/netwitness/config-management/chef-solo.log           /var/lib/netwitness/config-management/cache/chef-stacktrace.out           </pre>           L'erreur s'affiche dans un ou plusieurs de ces logs.         </li> <li>b. Tentez de résoudre le problème et réinstallez le service.           <ul style="list-style-type: none"> <li>• Cause 1 - Saisie du mot de passe <code>deploy_admin</code> erroné dans <code>nwsetup-tui</code>.<br/>Solution - Récupérez votre <code>deploy_admin</code> mot de passe.<br/>Pour résoudre la Cause 1, procédez comme suit.               <ol style="list-style-type: none"> <li>1. Dans le menu NetWitness Suite, sélectionnez <b>ADMIN &gt; Sécurité &gt; onglet Utilisateurs</b>.</li> <li>2. Sélectionnez <code>deploy_admin</code>, puis cliquez sur <b>Réinitialiser le mot de passe</b>.</li> <li>3. (Conditionnel) Si NetWitness Suite ne vous permet pas d'entrer le mot de passe <code>deploy_admin</code> ayant expiré dans la boîte de dialogue <b>Réinitialiser</b></li> </ol> </li> </ul> </li> </ol> </li> </ol> |

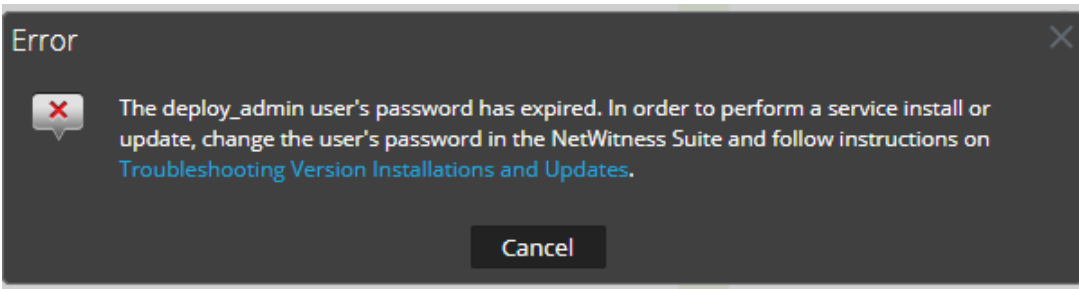
**le mot de passe**, procédez comme suit.

- a. Ouvrez une session SSH sur l'hôte du serveur NW.  


```
security-cli-client --get-config-prop --prop-hierarchy  
nw.security-client --prop-name  
platform.deployment.password -quiet
```
  - b. Exécutez une commande SSH sur l'hôte pour lequel l'installation/l'orchestration a échoué.
  - c. Exécutez la commande `nwsetup-tui` à l'aide du mot de passe `deploy_admin` approprié.
- Cause 2 - Le mot de passe `deploy_admin` a expiré.  
Pour résoudre la Cause 2, procédez comme suit.
    1. Dans le menu NetWitness Suite, sélectionnez **ADMIN > Sécurité > onglet Utilisateurs**.
    2. Sélectionnez `deploy_admin`, puis cliquez sur **Réinitialiser le mot de passe**.
    3. (Conditionnel) Si NetWitness Suite vous permet d'entrer le mot de passe `deploy_admin` ayant expiré dans la boîte de dialogue **Réinitialiser le mot de passe**, procédez comme suit.
      - a. Saisissez le mot de passe `deploy_admin` ayant expiré.
      - b. Désactivez la case à cocher Forcer le changement du mot de passe à la prochaine connexion.
      - c. Cliquez sur **Enregistrer**.
    4. (Conditionnel) Si NetWitness Suite ne vous permet pas d'entrer le mot de passe `deploy_admin` ayant expiré dans la boîte de dialogue Réinitialiser le mot de passe, procédez comme suit.
      - a. Réinitialisez `deploy_admin` pour utiliser un nouveau mot de passe.
      - b. Sur tous les hôtes du serveur NW et tous les autres hôtes 11.x, exécutez la commande suivante à l'aide du nouveau mot de passe `deploy_admin`.  

```
/opt/rsa/saTools/bin/set-deploy-admin-password
```
      - c. Sur l'hôte où l'installation/l'orchestration a échoué, exécutez la commande `nwsetup-tui` et utilisez le nouveau mot de passe `deploy_admin`.
3. Si vous ne pouvez toujours pas appliquer la mise à jour, collectez les logs comme indiqué à l'étape 2 et contactez le support client (<https://community.rsa.com/docs/DOC-1294>).

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Message d'erreur | <p><b>Erreur de téléchargement</b></p>                                                                                                                                                                                                                                                                                                                                                                                                  |
| Problème         | <p>Lorsque vous sélectionnez une version de mise à jour, puis cliquez sur <b>Mettre à jour</b> &gt; <b>Mettre à jour l'hôte</b>, le téléchargement démarre, mais ne parvient pas à terminer.</p>                                                                                                                                                                                                                                                                                                                          |
| Cause            | <p>Les fichiers de téléchargement de version peuvent être volumineux et prendre beaucoup de temps à télécharger. S'il existe des problèmes de communication pendant le téléchargement, celui-ci échoue.</p>                                                                                                                                                                                                                                                                                                               |
| Solution         | <ol style="list-style-type: none"> <li>1. Tentez un nouveau téléchargement.</li> <li>2. Si le téléchargement échoue, relancez le téléchargement en dehors de NetWitness Suite, comme décrit dans <a href="#">Appliquer les mises à jour à partir de la ligne de commande (sans accès Web)</a>.</li> <li>3. Si vous ne pouvez toujours pas télécharger le fichier de mise à jour, contactez le Support Clients (<a href="https://community.rsa.com/docs/DOC-1294">https://community.rsa.com/docs/DOC-1294</a>).</li> </ol> |

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Message d'erreur</b></p> | <p><code>deploy_admin</code> Le mot de passe de l'utilisateur a expiré</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <p><b>Cause</b></p>            | <p>Le mot de passe de l'utilisateur <code>deploy_admin</code> a expiré.</p> <p>Réinitialisez votre mot de passe <code>deploy_admin</code>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <p><b>Solution</b></p>         | <ol style="list-style-type: none"> <li>1. Dans le menu NetWitness Suite, sélectionnez <b>ADMIN &gt; Sécurité &gt; onglet Utilisateurs</b>.</li> <li>2. Sélectionnez <b>deploy_admin</b>, puis cliquez sur <b>Réinitialiser le mot de passe</b>.             <ul style="list-style-type: none"> <li>• Si NetWitness Suite vous permet d'entrer le mot de passe <code>deploy_admin</code> ayant expiré dans la boîte de dialogue <b>Réinitialiser le mot de passe</b>, procédez comme suit.                 <ol style="list-style-type: none"> <li>a. Saisissez le mot de passe <code>deploy_admin</code> ayant expiré.</li> <li>b. Désactivez la case à cocher <b>Forcer le changement du mot de passe à la prochaine connexion</b>.</li> <li>c. Cliquez sur <b>Enregistrer</b>.</li> </ol> </li> <li>• Si NetWitness Suite ne vous permet pas d'entrer le mot de passe <code>deploy_admin</code> ayant expiré dans la boîte de dialogue <b>Réinitialiser le mot de passe</b>.                 <ol style="list-style-type: none"> <li>a. Sur les hôtes du serveur NW et tous les autres hôtes 11.x, exécutez la commande suivante à l'aide du nouveau mot de passe <code>deploy_admin</code>.<br/> <code>/opt/rsa/saTools/bin/set-deploy-admin-password</code></li> <li>b. Sur l'hôte où l'installation/l'orchestration a échoué, exécutez la commande <code>nwsetup-tui</code> et utilisez le nouveau mot de passe <code>deploy_admin</code>.</li> </ol> </li> </ul> </li> </ol> |

|                         |                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Message d'erreur</b> | /var/log/netwitness/orchestration-server/orchestration-server.log présente une erreur similaire au message d'erreur suivant :<br>API Failure /rsa/orchestration/task/update-config-management [counter=10<br>reason=IllegalArgumentException<br>Exception::Version '11.0.0.n' is not supported                                                      |
| <b>Problème</b>         | Après la mise à jour de l'hôte du serveur NW vers la version 11.1, la seule stratégie de mise à jour pour les hôtes du serveur autres que NW est la version 11.1. Si vous tentez de mettre à jour un hôte serveur autre que NW vers un correctif 11.0.0.n (par exemple de la version 11.0.0.0 à la version 11.0.0.3), vous obtiendrez cette erreur. |
| <b>Solution</b>         | Deux options s'offrent à vous : <ul style="list-style-type: none"> <li>• Effectuez une mise à jour de l'hôte serveur autre que NW vers la version 11.1 ou</li> <li>• Ne mettez pas à jour l'hôte serveur autre que NW (conservez sa version actuelle).</li> </ul>                                                                                   |

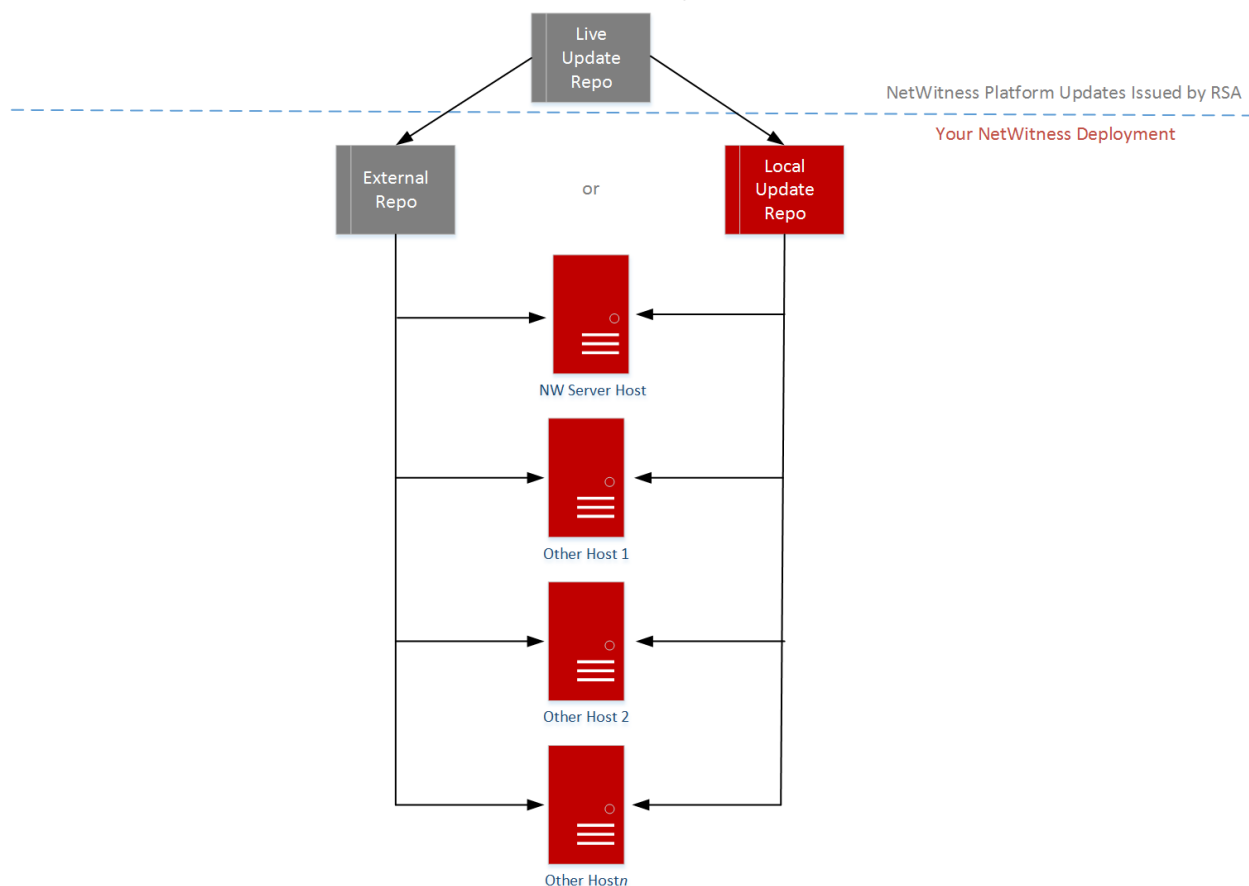
|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Message d'erreur</b> | Vous recevez un message dans l'interface utilisateur pour redémarrer l'hôte après avoir mis à jour et redémarré l'hôte hors connexion.<br> <p>The screenshot shows a host card with the following elements: a checkbox labeled 'SA Server', an 'IP-Address' field, a green button with the number '8', a 'version-number' field, and a red 'Reboot Host' button.</p> |
| <b>Cause</b>            | Vous ne pouvez pas utiliser l'interface de ligne de commande (CLI) pour redémarrer l'hôte. Vous devez utiliser l'interface utilisateur.                                                                                                                                                                                                                                                                                                                  |
| <b>Solution</b>         | Redémarrez l'hôte dans la vue Hôte dans l'interface utilisateur.                                                                                                                                                                                                                                                                                                                                                                                         |

## Annexe B. Renseigner le référentiel local

NetWitness Platform envoie les mises à jour de version dans le référentiel des mises à jour local à partir du référentiel Live Update. L'accès au référentiel de mises à jour Live Update nécessite et utilise les informations d'identification du compte Live configurées sous **ADMIN > SYSTÈME > Live**. En outre, vous devez cocher la case *Automatically download information about new updates every day* sous **ADMIN > SYSTÈME > Mises à jour** pour renseigner le référentiel local tous les jours.

Le schéma suivant illustre le mode d'obtention des mises à jour de version si votre déploiement NetWitness Platform dispose d'un accès au Web.

**RSA** NetWitness Platform® 11.x.x.x Version Update Workflow – Web Access



**Remarque :** Lorsque vous établissez la connexion initiale avec le référentiel Live Update, vous avez accès à tous les packages du système CentOS 7 et aux packages de production RSA. Ce téléchargement de plus de 2,5 Go de données nécessitera une durée indéterminée en fonction de la connexion Internet de votre serveur NW et du trafic du référentiel RSA. Il n'est pas obligatoire d'utiliser le référentiel Live Update. Vous pouvez également utiliser un référentiel externe, comme décrit dans la section [Configurer un référentiel externe avec des mises à jour RSA et OS](#).

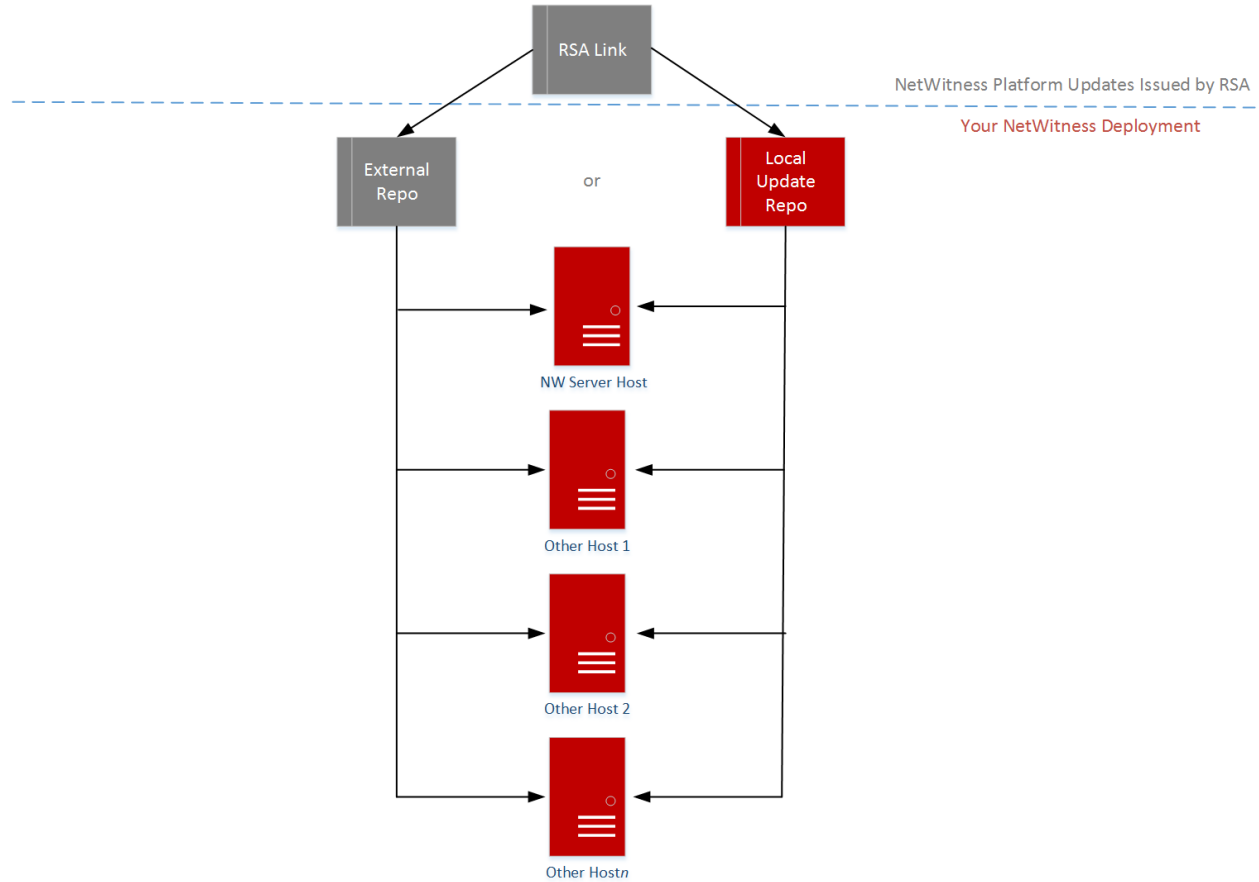
Pour vous connecter au référentiel Live Update, accédez à la vue **ADMIN > Système**, sélectionnez **Live Services** dans le panneau d'options et assurez-vous que les informations d'identification sont configurées (le voyant **Connexion** doit être vert). S'il n'est pas vert, cliquez sur **Démarrer la session** et connectez-vous.

**Remarque :** Si vous devez utiliser le serveur proxy pour accéder au référentiel Live Update, vous pouvez configurer l'hôte proxy, le nom d'utilisateur proxy et le mot de passe du proxy. Pour plus d'informations, consultez « Configurer le proxy pour NetWitness Platform » dans le *Guide de configuration NetWitness Platform 1.1*.

Reportez-vous à la section [Appliquer les mises à jour à partir de la ligne de commande \(Aucun accès Web\)](#) si votre déploiement NetWitness Platform n'a pas accès au Web.

Le schéma suivant illustre le mode d'obtention des mises à jour de version si votre déploiement NetWitness Platform ne dispose pas d'un accès au Web.

RSA NetWitness Platform® 11.x.x.x Version Update Workflow – No Web Access





## Annexe C. Configurer le référentiel externe

---

Exécutez la procédure suivante pour configurer un référentiel externe (référentiel).

**Remarque :** 1.) Pour effectuer cette procédure, un utilitaire de décompression doit être installé sur l'hôte. 2.) Vous devez savoir comment créer un serveur Web avant d'effectuer la procédure suivante.

1. (Conditionnel) Effectuez cette étape si vous disposez d'un référentiel externe et que vous souhaitez le remplacer.
  - Exemple 1 : Vous avez démarré l'hôte à partir d'un référentiel externe et vous souhaitez effectuer une mise à niveau à l'aide d'un référentiel local sur le serveur Admin.
    - a. Créez le fichier `/etc/netwitness/platform/repobase`.  
`vi /etc/netwitness/platform/netwitness/repobase`
    - b. Modifiez le fichier `repobase` de sorte que la seule information dans le fichier est l'URL suivante.  
`https://nw-node-zero/nwrpmrepo`
    - c. Suivez les instructions sur l'exécution de la mise à niveau à l'aide de l'outil `upgrade-client`.
  - Exemple 2 : Vous avez démarré l'hôte à partir du référentiel local sur le serveur Admin (hôte du serveur NW) et vous souhaitez utiliser un référentiel externe pour la mise à niveau.
    - a. Créez le fichier `/etc/netwitness/platform/repobase`.  
`vi /etc/netwitness/platform/netwitness/repobase`
    - b. Modifiez le fichier `repobase` de sorte que la seule information dans le fichier est l'URL suivante.  
`https://<webserver-ip>/<alias-for-repo>`
    - c. Suivez les instructions sur l'exécution de la mise à niveau à l'aide de l'outil `upgrade-client`.  
Les instructions figurent dans la rubrique [Appliquer les mises à jour à partir de la ligne de commande \(aucune accès Web\)](#).
2. Configurez le référentiel externe.
  - a. Connectez-vous à l'hôte du serveur Web
  - b. Créez le répertoire destiné à héberger le référentiel NW (`netwitness-11.2.0.0.zip`), par exemple `ziprepo`, sous `web-root` sur le serveur Web. Par exemple, `/var/netwitness` est la racine Web, exécutez la chaîne de commande suivante.  
`mkdir -p /var/netwitness/<your-zip-file-repo>`
  - c. Créez le répertoire `11.2.0.0` sous `/var/netwitness/<your-zip-file-repo>`.  
`mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0`
  - d. Créez les répertoires `OS` et `RSA` sous `/var/netwitness/<your-zip-file-repo>/11.2.0.0`.

```
mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS
mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA
```

e. Décompressez le fichier netwitness-11.2.0.0.zip dans le répertoire

```
/var/netwitness/<your-zip-file-repo>/11.2.0.0.
```

```
unzip netwitness-11.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0
```

La décompression de netwitness-11.2.0.0.zip résulte en deux fichiers zip (OS-11.2.0.0.zip et RSA-11.2.0.0.zip) et d'autres fichiers.

f. Décompressez le fichier :

i. OS-11.2.0.0.zip dans le répertoire /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS.

```
unzip /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS-11.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS
```

L'exemple suivant illustre la façon dont la structure de fichiers du système d'exploitation (OS) s'affiche une fois que vous décompressez le fichier.

| Parent Directory                                                        |                   | -    |
|-------------------------------------------------------------------------|-------------------|------|
| <a href="#">GeoIP-1.5.0-11.el7.x86_64.rpm</a>                           | 20-Nov-2016 12:49 | 1.1M |
| <a href="#">HostAgent-Linux-64-x86-en_US-1.2.25.1.0163-1.x86_64.rpm</a> | 03-Oct-2017 10:07 | 4.6M |
| <a href="#">Lib_Utils-1.00-09.noarch.rpm</a>                            | 03-Oct-2017 10:05 | 1.5M |
| <a href="#">OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm</a>                  | 20-Nov-2016 14:43 | 502K |
| <a href="#">OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm</a>              | 20-Nov-2016 14:43 | 15K  |
| <a href="#">PyYAML-3.11-1.el7.x86_64.rpm</a>                            | 19-Dec-2017 12:30 | 160K |
| <a href="#">SDL-1.2.15-14.el7.x86_64.rpm</a>                            | 25-Nov-2015 10:39 | 204K |
| <a href="#">acl-2.2.51-12.el7.x86_64.rpm</a>                            | 03-Oct-2017 10:04 | 81K  |
| <a href="#">adobe-source-sans-pro-fonts-2.020-1.el7.noarch.rpm</a>      | 13-Feb-2018 05:10 | 706K |
| <a href="#">alsa-lib-1.1.3-3.el7.x86_64.rpm</a>                         | 10-Aug-2017 10:52 | 421K |
| <a href="#">at-3.1.13-22.el7_4.2.x86_64.rpm</a>                         | 25-Jan-2018 17:56 | 51K  |
| <a href="#">atk-2.22.0-3.el7.x86_64.rpm</a>                             | 10-Aug-2017 10:53 | 258K |
| <a href="#">attr-2.4.46-12.el7.x86_64.rpm</a>                           | 03-Oct-2017 10:04 | 66K  |

ii. RSA-11.2.0.0.zip dans le répertoire /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA.

```
unzip /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA-11.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA
```

L'exemple suivant illustre l'affichage de la structure du fichier de mise à jour de la version de

RSA après décompression du fichier.

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

L'URL externe pour le référentiel est `http://<web server IP address>/<your-zip-file-repo>`.

- g. (Conditionnel - Pour Azure) Procédez comme suit pour mettre à jour Azure
  - i. `mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS/other`
  - ii. `unzip nw-azure-11.2-extras.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS/other`
  - iii. `cd /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS`
  - iv. `createrepo .`
- h. Utilisez `http://<web server IP address>/<your-zip-file-repo>` en réponse à l'invite **Entrez l'URL de base des référentiels de mises à jour externes** émanant du programme d'installation NW 11.2.0.0 (`nwsetup-tui`).

## Historique des révisions

| Révision | Date              | Description                                                                                                                     | Auteur |
|----------|-------------------|---------------------------------------------------------------------------------------------------------------------------------|--------|
| 1.0      | 15 août 2018      | Version pour les opérations                                                                                                     | IDD    |
| 1.1      | 04 septembre 2018 | Mises à jour post-RTO.                                                                                                          | IDD    |
| 1.2      | 09 octobre 2018   | Correction de la syntaxe dans les instructions « Appliquer la mise à jour à partir de la ligne de commande (pas d'accès Web) ». |        |