RSA NETWITNESS® PLATFORM

Guide d'installation de l'hôte physique

pour la version 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.

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

Introduction **4**

Matériel pris en charge 4

Spécifications du matériel hôte Endpoint Hybrid ou Endpoint Log Hybrid 4

Spécifications du matériel hôte RSA NetWitness UEBA 4

Stockage externe attaché 5

Workflow de l'installation de l'hôte physique 5

Contactez le support client 6

Préparation de l'installation - ouvrir les ports de pare-feu **7**

Tâches d'installation **8**

Tâche 1 - Installation de la version 11.2 sur l'hôte du serveur NetWitness (serveur NW) 8

Tâche 2 - Installation de la version 11.2 sur tous les autres composants hôtes 21

Mettre à jour ou installer la Collection Windows d'ancienne génération **34**

Tâches à effectuer après l'installation **35**

Général 35

(Facultatif) Tâche 1 - reconfigurer les serveurs DNS après la mise à niveau 11.2 35

RSA NetWitness Endpoint Insights 36

(Facultatif) Tâche 2 - Installer Endpoint Hybrid ou Endpoint Log Hybrid 36

Activation FIPS 37

(Facultatif) Tâche 3 - Activer le mode FIPS 37

RSA NetWitness® UEBA 38

(Facultatif) Tâche 4 - Installer NetWitness UEBA 38

Annexe A. Dépannage **44**

Interface de ligne de commande (CLI) 45

Sauvegarde (script nw-backup) 46

Event Stream Analysis 48

Service Log Collector (nwlogcollector) 49

Serveur NW 51

Orchestration 51

Service Reporting Engine 52

NetWitness UEBA 53

Annexe B. Créer un référentiel externe **54**

Historique des révisions **56**

Introduction

Les instructions de ce guide s'appliquent exclusivement aux hôtes physiques. Reportez-vous au *Guide d'installation d'un hôte virtuel* de RSA *NetWitness Platform* pour obtenir des instructions sur la façon de configurer des hôtes virtuels dans la version 11.2.

Matériel pris en charge

Série 4, série 4S et série 5.

Reportez-vous aux guides de configuration du matériel RSA *NetWitness Platform* pour obtenir des informations détaillées sur chaque type de gamme (https://community.rsa.com/community/products/netwitness/hardware-setup-guides).

Spécifications du matériel hôte Endpoint Hybrid ou Endpoint Log Hybrid

Vous devez installer le nouvel hôte Endpoint Hybrid ou Endpoint log Hybrid sur le matériel de série 5 (Dell R730) ou de série 6 (matériel Dell R740). Consultez la section « (Facultatif) Tâche 2 - Installer Endpoint Hybrid ou Endpoint Log Hybrid » dans les Tâches à effectuer après l'installation pour obtenir des instructions sur l'installation d'Endpoint Hybrid et d'Endpoint Log Hybrid.

Spécifications du matériel hôte RSA NetWitness UEBA

Vous devez installer le nouvel hôte NetWitness UEBA sur le matériel S5 (appliance Dell R630). Consultez la section « (Facultatif) Tâche 3 - Installer NetWitness UEBA » dans les Tâches à effectuer après l'installation pour savoir comment installer NetWitness UEBA.

CARACTÉRISTIQUES TECHNIQUES DE LA SÉRIE 5 (DELL R630)

Caractéristique technique	Capacité
Modèle	Dell PowerEdge R630xl
Type de processeur	Intel Xeon E5 -2680v3
Vitesse du processeur	2,5 GHz
Cache	30 Mo
Nombre de cœurs	12
Nombre de processeurs	2
Nombre de threads	24
Mémoire totale	256 Go
Contrôleur de disque interne	Dell PERC H730
Contrôleur de disque interne	Dell PERC H830
Connectivité SAN (HBA) - En option	s.o.

Caractéristique technique	Capacité
Carte de gestion à distance	iDRAC8 Enterprise
Lecteurs	Total - 6 lecteurs 2 disques durs 2,5 pouces de 1 To 4 disques durs 2,5 pouces de 2 To
Châssis	1U
Poids	18,4 kg
Carte réseau*	Intégrée 2 X 10 Gbit cuivre 2 X 10 Gbit cuivre et 2 X 1 Gbit cuivre (D'autres options sont disponibles)
Dimensions	Hauteur : 4,28 cm x Largeur : 48,23 cm x Profondeur : 75,51 cm
Alimentation	1 100 W redondants
BTU/heure	4100 BTU/heure (max)
Ampères (spec)	1 100 W / 220 VCA = 5 A
Ampérage réel (post-démarrage)	2,1 A
Événements par seconde	EPS 100K
Débit	s.o.

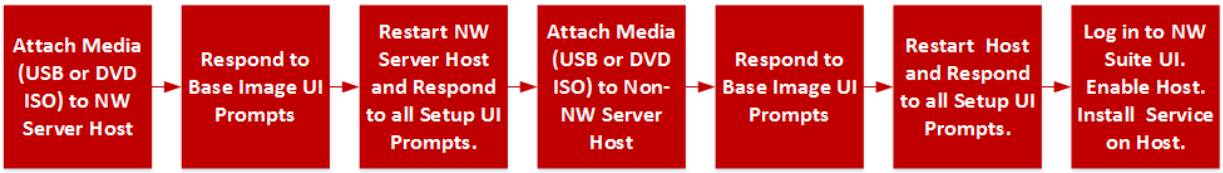
* Les options de la carte NIC sont disponibles pour une permutation avec la carte fille intégrée ou le module complémentaire.

Stockage externe attaché

Si vous avez un ou des périphérique(s) de stockage externe (par exemple, des DAC ou des PowerVaults) connecté(s) à un hôte physique, reportez-vous aux guides de configuration matérielle pour obtenir plus d'informations sur la configuration de ce stockage sur RSA Link (https://community.rsa.com/community/products/netwitness/hardware-setup-guides). »

Workflow de l'installation de l'hôte physique

Le schéma suivant illustre le workflow de l'installation de l'hôte physique RSA NetWitness® Platform 11.2.



Contactez le support client

Reportez-vous à la page Contactez le support client RSA (https://community.rsa.com/docs/DOC-1294) dans RSA Link pour plus d'informations sur la manière d'obtenir de l'aide sur RSA NetWitness Platform version 11.2.

Préparation de l'installation - ouvrir les ports de pare-feu

La rubrique « Architecture de réseau et ports » dans le Guide de déploiement *RSA NetWitness® Platform répertorie tous les ports dans un déploiement*. Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

Attention : N'effectuez l'installation que si les ports de votre pare-feu sont configurés.

Tâches d'installation

Cette rubrique contient les tâches à effectuer pour installer la version 11.2 de NetWitness Platform sur des hôtes physiques.

Deux tâches principales sont à effectuer dans l'ordre indiqué.

Tâche 1 - Installation de la version 11.2 sur l'hôte du serveur NetWitness (serveur NW)

Tâche 2 - Installation de la version 11.2 sur tous les autres composants hôtes

Tâche 1 - Installation de la version 11.2 sur l'hôte du serveur NetWitness (serveur NW)

Pour le serveur NW, cette tâche :

- Crée une image de base.
- Configure le serveur hôte NW 11.2.

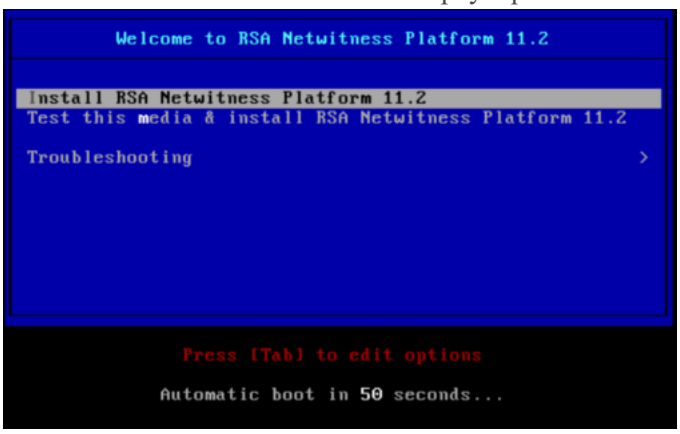
Pour installer la version 11.2 de l'hôte du serveur NW, procédez comme suit.

1. Créez une image de base sur l'hôte :
   a. Rattachez le média (ISO) à l'hôte.
      Reportez-vous aux *Instructions de clé de version pour RSA NetWitness Platform* pour plus d'informations.
      - Installations de l'hyperviseur, utilisez l'image ISO.
      - Média physique - utilisez l'image ISO pour créer un disque Flash de démarrage à l'aide de Universal Netboot Installer (UNetbootin) ou d'un autre outil d'imagerie adapté. Pour plus d'informations sur la création d'une clé de version à partir du fichier ISO, reportez-vous à *RSA NetWitness® PlatformInstructions de clé*. Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.
      - Installations de l'iDRAC - le type de média virtuel est :
        - **Un lecteur de disquette virtuel** pour des disques flash mappés.
        - **Un CD virtuel** pour des périphériques de médias optiques mappés ou du fichier ISO.
   b. Connectez-vous à l'hôte et redémarrez-le.

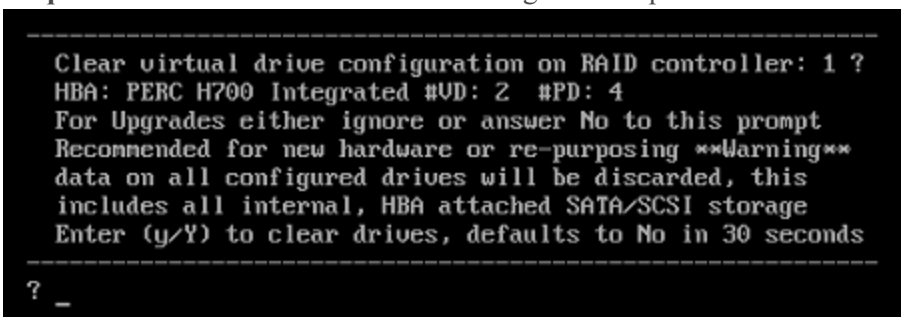
```
login: root
Password:
Last login: Tue Sep 19 13:27:15 on tty1
[root@saserver ~]# reboot
```

   c. Sélectionnez **F11** (dans le menu de démarrage) pendant le redémarrage pour sélectionner un périphérique de démarrage et démarrer le média connecté.
      Après vérification du système lors du démarrage, le menu d'installation suivant, **Bienvenue dans la RSA NetWitness Platform 11.2** s'affiche. Les graphiques du menu s'affichent différemment

si vous utilisez un média Flash USB physique.



d. Sélectionnez **Installer RSA NetWitness Platform 11.2** (sélection par défaut), puis appuyez sur **Entrée**.
Le programme d'installation s'exécute et s'arrête au message **Saisir (y/Y) pour effacer les disques** vous invitant à effectuer le formatage des disques.



e. Saisissez **Y** pour continuer.
L'action par défaut est No, donc si vous ignorez le message, No sera automatiquement sélectionné dans les 30 secondes et les disques ne seront pas effacés. Le message **Appuyer sur Entrée pour redémarrer** s'affiche.

```
  Clearing drive configuration in 15 seconds, <CTRL><ALT><DEL> to cancel
  Ignore or answer no to this prompt after restarting
  Re-labeling disks and virtual drives, clearing RAID configuration ...
  0 logical volume(s) in volume group "netwitness_vg00" now active


Adapter 0: Configuration is Cleared.

Exit Code: 0x00
Invalid or no RAID configuration found: RAID Level =  #HDD =

Adapter 0: Created VD 0

Adapter 0: Configured the Adapter!!

Exit Code: 0x00

Adapter 0: Created VD 1

Adapter 0: Configured the Adapter!!

Exit Code: 0x00

Run installation again after restart
Press enter to reboot
```

f. Appuyez sur **Entrée** pour redémarrer l'hôte.
Le programme d'installation vous demande à nouveau d'effacer les disques.

```
-------------------------------------------------------------
  Clear virtual drive configuration on RAID controller: 0 ?
  HBA: PERC H730P Mini #VD: 2  #PD: 4
  For Migrations either ignore or answer No to this prompt
  Recommended for new hardware or re-purposing **Warning**
  data on all configured drives will be discarded, this
  includes all internal, HBA attached SATA/SCSI storage
  Enter (y/Y) to clear drives, defaults to No in 30 seconds
-------------------------------------------------------------
```

g. Saisissez **N** car vous avez déjà effacé les disques.
Le message **Saisir Q (Quitter) ou R (Réinstaller)** s'affiche.

```
-------------------------------------------------
 No root level logical volumes found for Migration
 Assuming this system is new or being reinstalled
 Migration cannot proceed, system will be reimaged
 If you had intended to migrate please quit and
 contact support for assistance.
-------------------------------------------------
 Enter Q to Quit or R to Reinstall, Re-installing in 120 seconds?
```

h. Saisissez **R** pour installer l'image de base.
Le programme d'installation affiche les composants à mesure qu'ils sont installés, ce qui varie en fonction de l'appliance, puis redémarre.

> **Attention :** Ne réinitialisez pas le média rattaché (un média contenant le fichier ISO, par exemple une clé de version).

```
CentOS Linux 7 (Core)
Kernel 3.10.0-514.26.1.el7.x86_64 on an x86_64

NWAPPLIANCE9240 login: root
Password:
[root@NWAPPLIANCE9240 ~]#
```

i. Connectez-vous à l'hôte avec les informations d'identification `root` .

2. Exécutez la commande `nwsetup-tui` pour configurer l'hôte.

   Cette opération démarre le programme d'installation `nwsetup-tui` et les conditions générales d'utilisation s'affichent.

> **Remarque :** 1.) Lorsque vous parcourez les messages du programme d'installation, utilisez les touches directionnelles Haut et Bas pour naviguer entre les champs, utilisez la touche de tabulation pour naviguer d'une commande à l'autre (par exemple **<Oui>**, **<Non>**, **<OK>**, et **<Annuler>**. Appuyez sur **Entrée** pour enregistrer votre réponse et passer au message suivant.
> 2.) Le programme d'installation adopte le modèle de couleurs du poste de travail ou de la console que vous utilisez pour accéder à l'hôte.
> 3.) Si vous spécifiez des serveurs DNS pendant l'exécution du programme d'installation (`nwsetup-tui`), ils doivent OBLIGATOIREMENT être valides (valide dans ce contexte signifie valide lors de l'installation) et accessibles à `nwsetup-tui` pour continuer. Tous les serveurs DNS mal configurés provoquent l'échec de l'installation. Si vous avez besoin d'accéder à un serveur DNS après l'installation, ce dernier étant inaccessible pendant l'installation, (par exemple, pour déplacer un hôte après la configuration ayant un ensemble différent de serveurs DNS), reportez-vous à la section « (Facultatif) Tâche 1 - Reconfigurer les serveurs DNS après la mise à niveau 11.2 » dans les Tâches à effectuer après l'installation.
> Si vous ne spécifiez pas de serveurs DNS lors de la configuration (`nwsetup-tui`), vous devez sélectionner **1 Référentiel local (sur le serveur NW)** dans le message **NetWitness Platform Mise à jour du référentiel** à l'étape 12 (les serveurs DNS ne sont pas définis afin que le système ne puisse pas accéder au référentiel externe).

```
By clicking "Accept", you (the "Customer") hereby agree, on behalf of your
company or organization, to be bound by the terms and conditions of the
End User License Agreement (the "EULA") located at
https://www.rsa.com/content/dam/rsa/PDF/shrinkwrap-license-combined.pdf
with RSA Security LLC ("RSA", or appropriate affiliate entity in the
relevant jurisdiction).  In addition, Customer hereby agrees and
acknowledges that, if Customer chooses to host its data with any third
party or in a public cloud environment, RSA has no responsibility for the
storage or protection of any Customer data or for any associated security
breach notifications. The terms herein and in the EULA shall supersede any
relevant terms in any other agreement between the Customer and RSA.  For
customers of the RSA NetWitness® products, all data analyzed in connection
herewith shall be at a cost to Customer based on RSA's then current
                                                                    92%
                    <Accept >            <Decline>
```

3. Naviguez jusqu'à **Accepter** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**.
   Le message **Est-ce l'hôte que vous souhaitez pour votre serveur NW 11.2 ?** s'affiche.

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

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

            < Yes >        < No  >
```

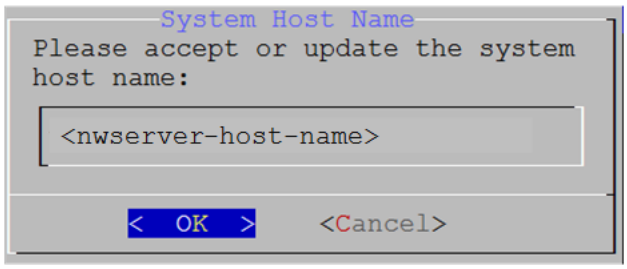
4. Naviguez jusqu'à **Oui** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**.
   Choisissez **Non** si vous avez déjà installé la version 11.2 sur le serveur NW.

   Attention : Si l'hôte choisi pour le serveur NW est incorrect et que vous terminez l'installation, vous devez redémarrer le programme d'installation et effectuer les étapes 2 à 14 pour corriger cette erreur.

   Le message **Installation ou Mise à niveau** s'affiche (**Restaurer** ne s'applique pas à l'installation. Cette option est destinée à la fonctionnalité Reprise après sinistre dans la version 11.2.).

```
NetWitness Platform 11.2 Install or Upgrade
Specify if you are installing NetWitness
for the first time or upgrading from a
previous version:

    1  Install (Fresh Install)
    2  Upgrade (From Previous Vers.)
    3  Recover (Reinstall)

            <  OK  >        < Exit >
```

5. Appuyez sur **Entrée**. **Installer (nouvelle installation)** est sélectionnée par défaut.
   Le message **Nom de l'hôte** s'affiche.

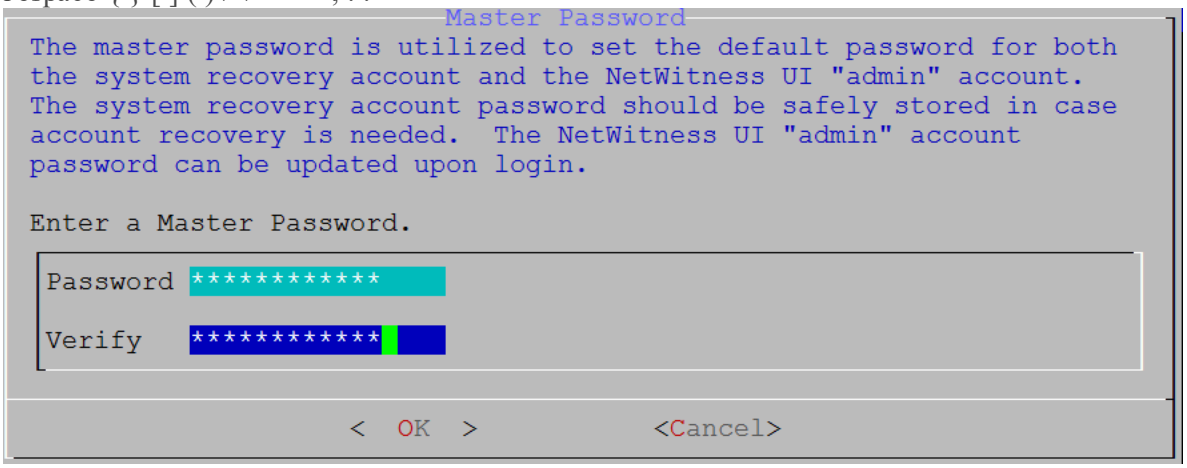


Attention : Si vous incluez "." dans un nom d'hôte, le nom d'hôte doit également inclure un nom de domaine valide.

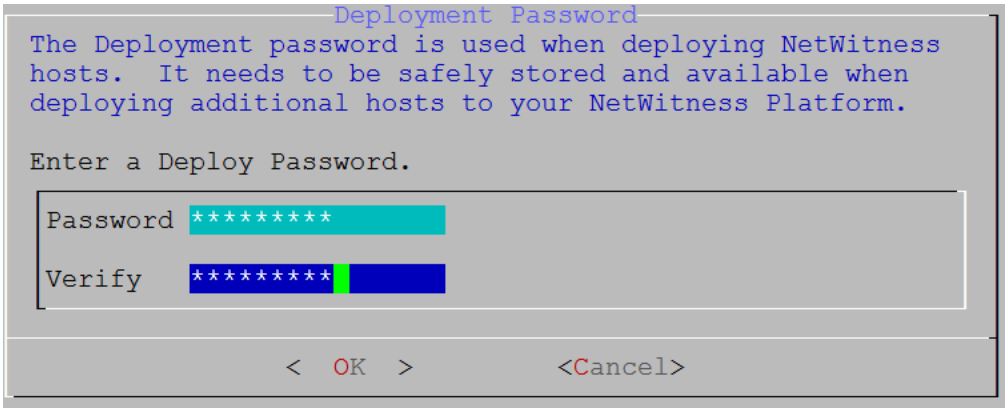
Le message **Mot de passe maître** s'affiche.

6. Appuyez sur **Entrée** si vous souhaitez conserver ce nom. Dans le cas contraire, naviguez jusqu'à **OK** à l'aide de la touche de tabulation et appuyez sur **Entrée** pour modifier le nom de l'hôte.
   Les caractères suivants sont pris en charge pour le mot de passe maître et le mot de passe de déploiement :
   - Symboles : ! @ # % ^ +
   - Numéros : 0-9
   - Caractères minuscules : a-z
   - Caractères majuscules : A-Z

   Aucun caractère ambigu n'est pris en charge pour le mot de passe maître et le mot de passe de déploiement. Par exemple :
   l'espace { } [ ] ( ) / \ ' " ` ~ ; : . < > -



7. Saisissez le **mot de passe**, appuyez sur la touche directionnelle Bas pour accéder à **Vérifier**, saisissez à nouveau le mot de passe, naviguez jusqu'à **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**.
   Le message **Mot de passe de déploiement** s'affiche.



8. Saisissez le **mot de passe**, appuyez sur la touche directionnelle Bas pour accéder à **Vérifier**, saisissez à nouveau le mot de passe, naviguez jusqu'à **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**.
   Une des invites conditionnelles suivantes s'affiche.

   - Si le programme d'installation détecte une adresse IP valide pour cet hôte, le message suivant s'affiche.

     ```
     IP Address <IP-address> is
     currently assigned to this
     host.  Do you still want to
     change network settings?

          < Yes >     < No  >
     ```

     Appuyez sur **Entrée** si vous souhaitez utiliser cette adresse IP et éviter de modifier les paramètres de votre réseau. Naviguez jusqu'à **Oui** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** si vous souhaitez modifier la configuration IP disponible sur l'hôte.

   - Si vous utilisez une connexion SSH, l'avertissement suivant s'affiche.

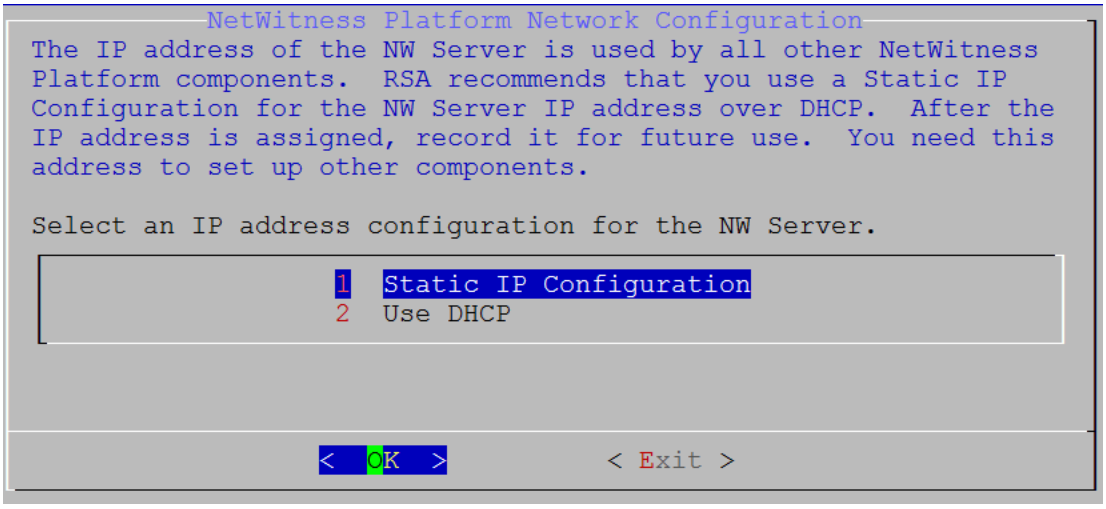
     Remarque : Si vous vous connectez directement à partir de la console hôte, l'avertissement suivant ne s'affichera pas.

     ```
     NetWitness Platform Network Configuration
      WARNING - You are currently running the
      NetWitness installation over an SSH
      connection.  Network configuration
      updates will result in restarting the
      network service which may cause the SSH
      session to terminate.

                    <  OK  >
     ```

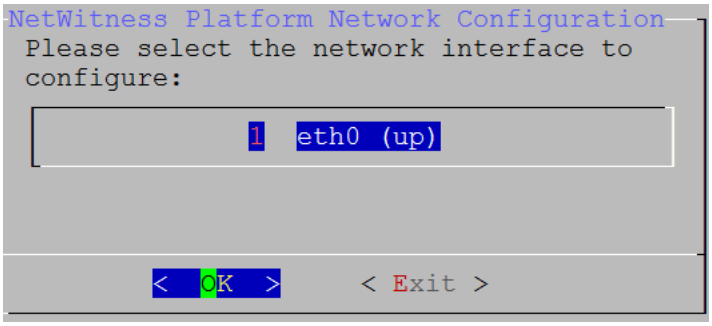
     Appuyez sur **Entrée** pour fermer le message d'avertissement.

   - Si le programme d'installation a détecté une configuration IP et que vous avez choisi de l'utiliser, le message **Mettre à jour le référentiel** s'affiche. Accédez à l'étape 12 et terminez l'installation.

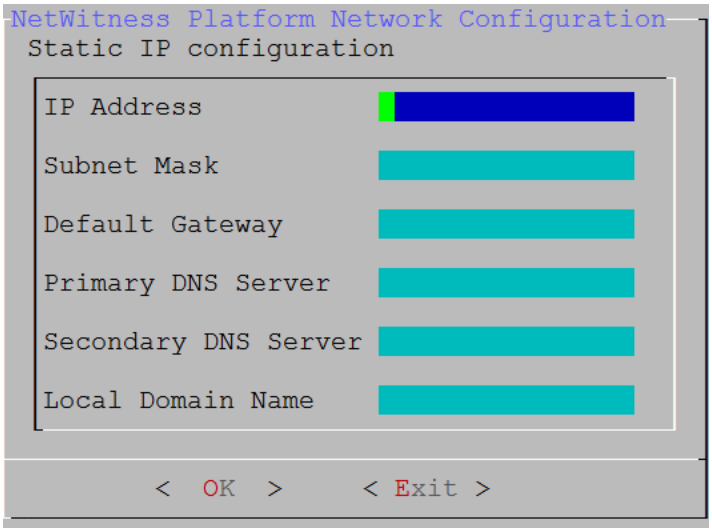
- Si le programme d'installation n'a pas détecté de configuration IP, ou si vous avez choisi de modifier la configuration IP, le message **Configuration réseau** s'affiche.



9. Naviguez jusqu'à **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** pour utiliser l'**adresse IP statique**.
   Si vous souhaitez utiliser **DHCP**, utilisez la touche directionnelle Bas jusqu'à 2 Utiliser DHCP, puis appuyez sur **Entrée**.
   Le message **Configuration de réseau** s'affiche.



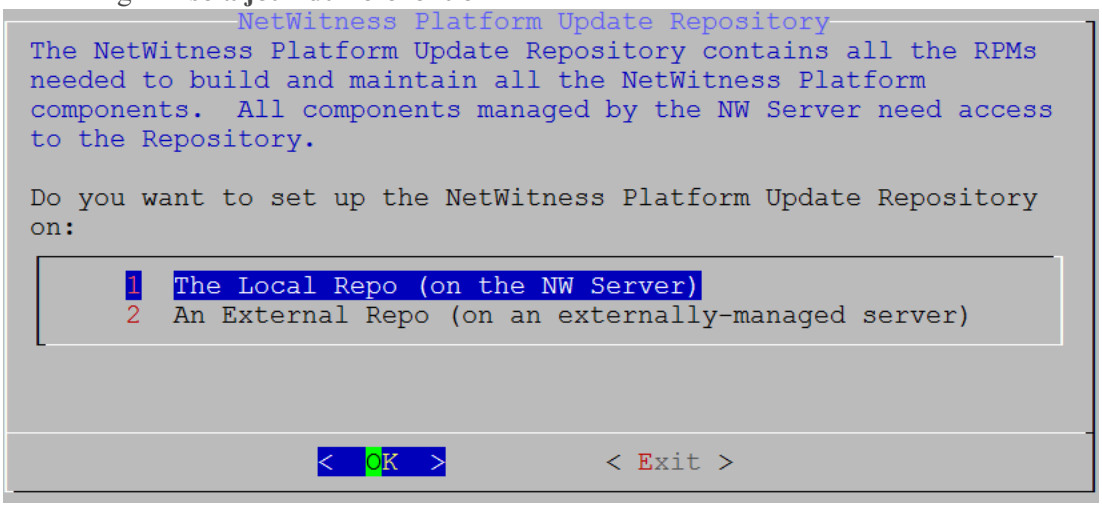
10. Utilisez la touche directionnelle Bas jusqu'à l'interface réseau que vous souhaitez, puis naviguez jusqu'à **OK** à l'aide de la touche de tabulation et appuyez sur **Entrée**. Si vous ne souhaitez pas continuer, naviguez jusqu'à **Quitter**
    à l'aide de la touche de tabulation.Le message **Configuration d'adresse IP statique** suivant s'affiche.



11. Saisissez les valeurs de configuration (en naviguant d'un champ à l'autre à l'aide de la touche directionnelle Bas), naviguez jusqu'à **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**. Si vous ne remplissez pas tous les champs obligatoires, un message d'erreur `All fields are required` s'affiche. Les champs **Serveur DNS secondaire** et **Nom de domaine local** ne sont pas obligatoires. Si vous utilisez une syntaxe ou une longueur de caractères incorrecte pour l'un des champs, un message d'erreur `Invalid <field-name>` s'affiche.

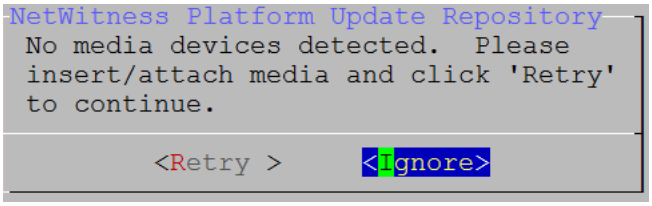
> **Attention :** Si vous sélectionnez le **serveur DNS**, assurez-vous que le serveur DNS est correct et que l'hôte peut y accéder avant de poursuivre l'installation.

Le message **Mise à jour du référentiel** s'affiche.

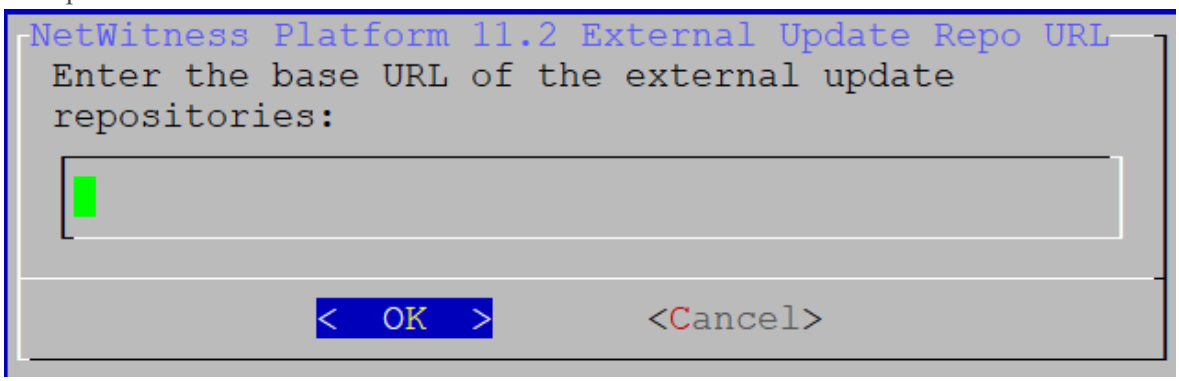


12. Appuyez sur **Entrée** pour choisir le **référentiel local** sur le serveur NW.
    Si vous souhaitez utiliser un référentiel externe, utilisez la touche directionnelle Bas pour naviguer jusqu'au **Référentiel externe**, naviguez jusqu'à **OK** à l'aide de la touche de tabulation et appuyez sur **Entrée**.

    - Si vous sélectionnez **1 Le référentiel local (sur le serveur NW)** dans le programme d'installation, assurez-vous que le média approprié est rattaché à l'hôte (média contenant le fichier ISO, par exemple une clé de version) à partir duquel NetWitness Platform 11.2.0.0 peut être installé. Si le programme ne détecte pas le média connecté, le message d'erreur suivant s'affiche.

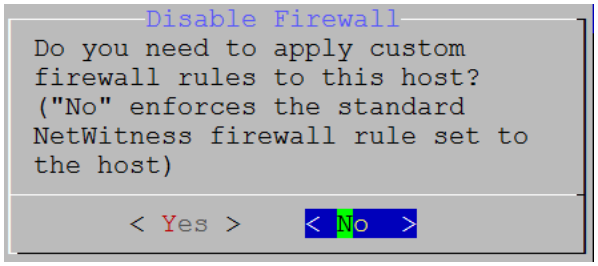


    - Si vous sélectionnez **2 Un référentiel externe (sur un serveur géré en externe)**, l'interface utilisateur vous invite à saisir une URL. Les référentiels vous donnent accès aux mises à jour RSA et CentOS. Reportez-vous à la section Annexe B. Créer un référentiel externe pour obtenir des instructions sur la création de ce référentiel, ainsi que l'URL de référentiel externe afin que vous puissiez la saisir dans l'invite suivante.



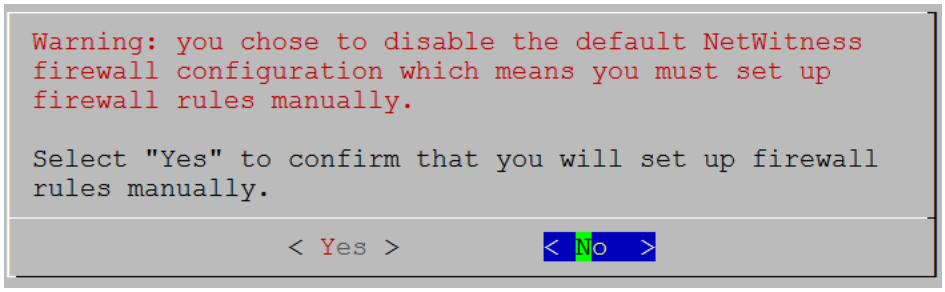
    Saisissez l'URL de base du référentiel externe NetWitness Platform, puis cliquez sur **OK**. Le

message **Démarrer l'installation** s'affiche.
Voir « Définir un référentiel externe avec les mises à jour RSA et de système d'exploitation » sous « Procédures liées aux hôtes et services » dans le *Guide de mise en route des hôtes et des services RSA NetWitness Platform* pour obtenir des instructions. Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.
Le message Désactiver le pare-feu s'affiche.

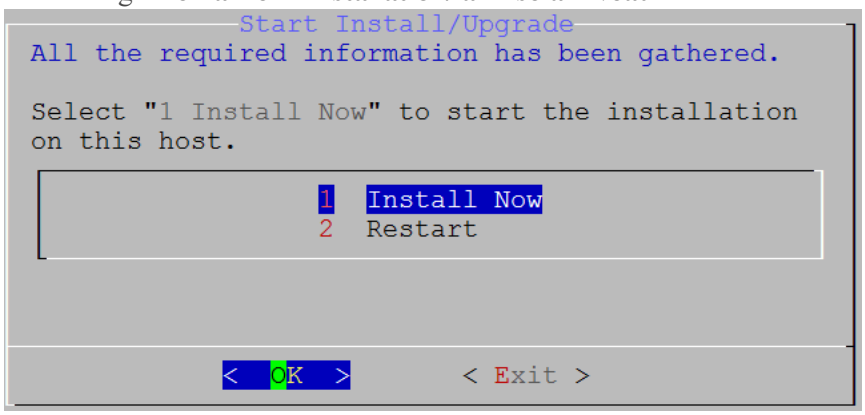


13. Naviguez vers l'onglet **Non** (par défaut) à l'aide de la touche de tabulation, puis appuyez sur **Entrée** pour utiliser la configuration de pare-feu standard. Naviguez vers l'onglet **Oui** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** pour désactiver la configuration de pare-feu standard.

- Pour confirmer votre sélection, choisissez **Oui**, dans le cas contraire, choisissez **Non** pour utiliser la configuration du pare-feu standard.



Le message **Démarrer l'installation/la mise à niveau** s'affiche.



14. Appuyez sur **Entrée** pour installer la version 11.2 sur le serveur NW.
    Lorsque le message **Installation terminée** s'affiche, c'est que vous avez installé le serveur NW 11.2 sur cet hôte.

> **Remarque :** Ignorez les erreurs de code de hachage similaires aux erreurs illustrées dans l'image suivante qui s'affichent lorsque vous lancez la commande `nwsetup-tui`. Yum n'utilise pas MD5 pour les opérations de sécurité afin qu'elles n'affectent pas la sécurité du système.

```
ValueError: error:3207A06D:lib(50):B_HASH_init:cr new
Checksum type 'md5' disabled
 (skipped due to only_if)
    * file[/etc/yum.repos.d/CentOS-Base.repo] action delete (up to date)
    * ruby_block[yum-cache-reload-CentOS-Base] action nothing (skipped due to action :nothing)
     (up to date)
  * yum_repository[Remove CentOS-CR repository] action delete
    * execute[yum clean all CentOS-CR] action runERROR:root:code for hash md5 was not found.
Traceback (most recent call last):
  File "/usr/lib64/python2.7/hashlib.py", line 129, in <module>
    globals()[__func_name] = __get_hash(__func_name)
  File "/usr/lib64/python2.7/hashlib.py", line 98, in __get_openssl_constructor
    f(usedforsecurity=False)
```

Tâche 2 - Installation de la version 11.2 sur tous les autres composants hôtes

Pour un hôte de serveur autre que NW, cette tâche :

- Crée une image de base.
- Configure l'hôte de serveur autre que NW 11.2.

Pour les hôtes ESA :

- Installez votre hôte ESA primaire, puis installez-y le service **ESA primaire** après avoir terminé d'exécuter le programme de configuration dans l'interface utilisateur au sein de la vue **ADMIN > Hôtes**.
- (Conditionnel) Si vous disposez d'un hôte ESA secondaire, installez-le, puis installez-y le service **ESA secondaire** après avoir terminé d'exécuter le programme de configuration dans l'interface utilisateur au sein de la vue **ADMIN > Hôtes**.

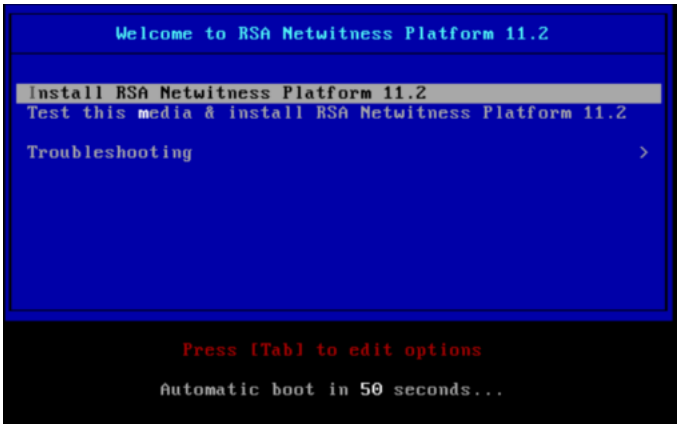
Pour installer NetWitness Platform version 11.2 sur un hôte de serveur autre que NW, procédez comme suit.

1. Créez une image de base sur l'hôte :
   a. Rattachez un média (un média contenant le fichier ISO, par exemple une clé de version) à l'hôte. Reportez-vous aux *Instructions de clé de version pour RSA NetWitness Platform* pour plus d'informations.
      - Installations de l'hyperviseur, utilisez l'image ISO.
      - Média physique - utilisez le fichier ISO pour créer un disque Flash de démarrage à l'aide de Universal Netboot Installer (UNetbootin) ou d'un autre outil d'imagerie adapté. Reportez-vous aux *RSA NetWitness® PlatformInstructions de clé de version* pour plus d'informations sur la création d'une clé de version à partir du fichier ISO. Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.
      - Installations de l'iDRAC - le type de média virtuel est :
        - **Un lecteur de disquette virtuel** pour des disques flash mappés.
        - **Un CD virtuel** pour des périphériques de médias optiques mappés ou du fichier ISO.

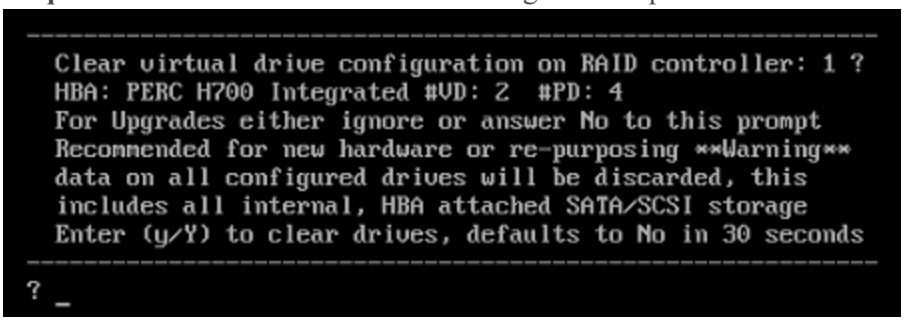
        Reportez-vous aux *Instructions de clé de version pour RSA NetWitness Platform* pour plus d'informations.e programme
   b. Connectez-vous à l'hôte et redémarrez-le.

```
login: root
Password:
Last login: Tue Sep 19 13:27:15 on tty1
[root@saserver ~]# reboot
```

c. Sélectionnez **F11** (dans le menu de démarrage) pendant le redémarrage pour sélectionner un périphérique de démarrage et démarrer le média connecté.
Après vérification du système lors du démarrage, le menu d'installation suivant, **Bienvenue dans la RSA NetWitness Platform 11.2** s'affiche. Les graphiques du menu s'affichent différemment si vous utilisez un média Flash USB physique.



d. Sélectionnez **Installer RSA NetWitness Platform 11.2** (sélection par défaut), puis appuyez sur **Entrée**.
Le programme d'installation s'exécute et s'arrête au message **Saisir (y/Y) pour effacer les disques** vous invitant à effectuer le formatage des disques.



e. Saisissez **Y** pour continuer.
L'action par défaut est No, donc si vous ignorez le message, No sera automatiquement sélectionné dans les 30 secondes et les disques ne seront pas effacés. Le message **Appuyer sur Entrée pour redémarrer** s'affiche.

```
  Clearing drive configuration in 15 seconds, <CTRL><ALT><DEL> to cancel
  Ignore or answer no to this prompt after restarting
  Re-labeling disks and virtual drives, clearing RAID configuration ...
  0 logical volume(s) in volume group "netwitness_vg00" now active


Adapter 0: Configuration is Cleared.

Exit Code: 0x00
Invalid or no RAID configuration found: RAID Level =  #HDD =

Adapter 0: Created VD 0

Adapter 0: Configured the Adapter!!

Exit Code: 0x00

Adapter 0: Created VD 1

Adapter 0: Configured the Adapter!!

Exit Code: 0x00

Run installation again after restart
Press enter to reboot
```

f. Appuyez sur **Entrée** pour redémarrer l'hôte.
Le programme d'installation vous demande à nouveau d'effacer les disques.

```
-------------------------------------------------------------
  Clear virtual drive configuration on RAID controller: 0 ?
  HBA: PERC H730P Mini #VD: 2  #PD: 4
  For Migrations either ignore or answer No to this prompt
  Recommended for new hardware or re-purposing **Warning**
  data on all configured drives will be discarded, this
  includes all internal, HBA attached SATA/SCSI storage
  Enter (y/Y) to clear drives, defaults to No in 30 seconds
-------------------------------------------------------------
```

g. Saisissez **N** car vous avez déjà effacé les disques.
Le message **Saisir Q (Quitter) ou R (Réinstaller)** s'affiche.

```
-------------------------------------------------
 No root level logical volumes found for Migration
 Assuming this system is new or being reinstalled
 Migration cannot proceed, system will be reimaged
 If you had intended to migrate please quit and
 contact support for assistance.
-------------------------------------------------
 Enter Q to Quit or R to Reinstall, Re-installing in 120 seconds?
```

h. Saisissez **R** pour installer l'image de base.
Le programme d'installation affiche les composants à mesure qu'ils sont installés, ce qui varie en fonction de l'appliance, puis redémarre.

> **Attention :** Ne réinitialisez pas le média rattaché (un média contenant le fichier ISO, par exemple une clé de version).

```
CentOS Linux 7 (Core)
Kernel 3.10.0-514.26.1.el7.x86_64 on an x86_64

NWAPPLIANCE9240 login: root
Password:
[root@NWAPPLIANCE9240 ~]#
```

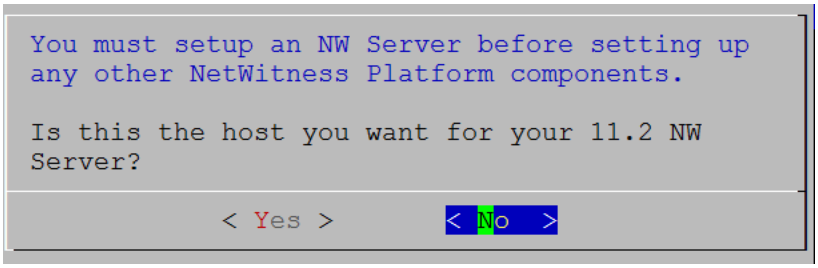
i. Connectez-vous à l'hôte avec les `root` informations d'identification.

2. Exécutez la commande `nwsetup-tui` pour configurer l'hôte.
Cette opération démarre le programme d'installation `nwsetup-tui` et les conditions générales d'utilisation s'affichent.

> **Remarque :** Si vous spécifiez des serveurs DNS pendant l'exécution du programme d'installation (`nwsetup-tui`), ils doivent OBLIGATOIREMENT être valides (valide dans ce contexte signifie valide lors de l'installation) et accessibles à `nwsetup-tui` pour continuer. Tous les serveurs DNS mal configurés provoquent l'échec de l'installation. Si vous avez besoin d'accéder à un serveur DNS après l'installation, ce dernier étant inaccessible pendant l'installation, (par exemple, pour déplacer un hôte après la configuration ayant un ensemble différent de serveurs DNS), reportez-vous à la section « (Facultatif) Tâche 1 - Reconfigurer les serveurs DNS après la mise à niveau 11.2 » dans les Tâches à effectuer après l'installation.
> Si vous ne spécifiez pas de serveurs DNS lors de la `nwsetup-tui`, vous devez sélectionner **1 Référentiel local (sur le serveur NW)** dans le message **NetWitness Platform Mise à jour du référentiel** à l'étape 11 (les serveurs DNS ne sont pas définis afin que le système ne puisse pas accéder au référentiel externe).

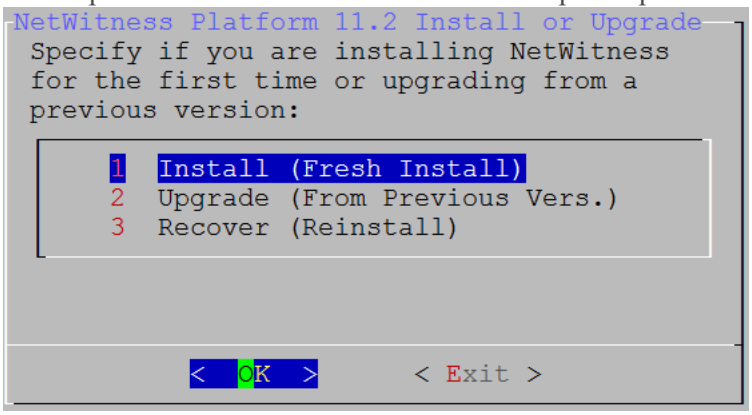
```
By clicking "Accept", you (the "Customer") hereby agree, on behalf of your
company or organization, to be bound by the terms and conditions of the
End User License Agreement (the "EULA") located at
https://www.rsa.com/content/dam/rsa/PDF/shrinkwrap-license-combined.pdf
with RSA Security LLC ("RSA", or appropriate affiliate entity in the
relevant jurisdiction).  In addition, Customer hereby agrees and
acknowledges that, if Customer chooses to host its data with any third
party or in a public cloud environment, RSA has no responsibility for the
storage or protection of any Customer data or for any associated security
breach notifications. The terms herein and in the EULA shall supersede any
relevant terms in any other agreement between the Customer and RSA.  For
customers of the RSA NetWitness® products, all data analyzed in connection
herewith shall be at a cost to Customer based on RSA's then current
                                                                    92%
                <Accept >              <Decline>
```

3. Naviguez jusqu'à **Accepter** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**.
   Le message **Est-ce l'hôte que vous souhaitez pour votre serveur NW 11.2 ?** s'affiche.

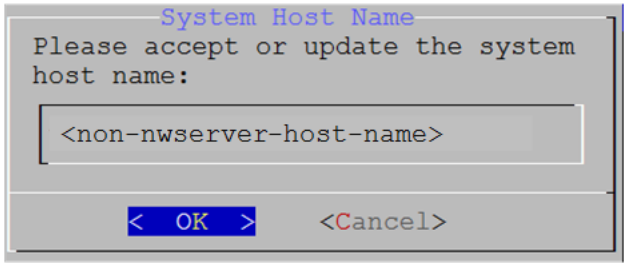


Attention : Si l'hôte choisi pour le serveur NW est incorrect et que vous terminez l'installation, vous devez redémarrer le programme d'installation et effectuer toutes les étapes 2 à 14 de la Tâche 1 - Installation de la version 11.2 sur l'hôte du serveur NetWitness (serveur NW) pour corriger cette erreur.

4. Appuyez sur **Entrée** (Non).
   Le message **Installation** ou **Mise à niveau** s'affiche (**Restaurer** ne s'applique pas à l'installation. Cette option est destinée à la fonctionnalité Reprise après sinistre dans la version 11.2.).



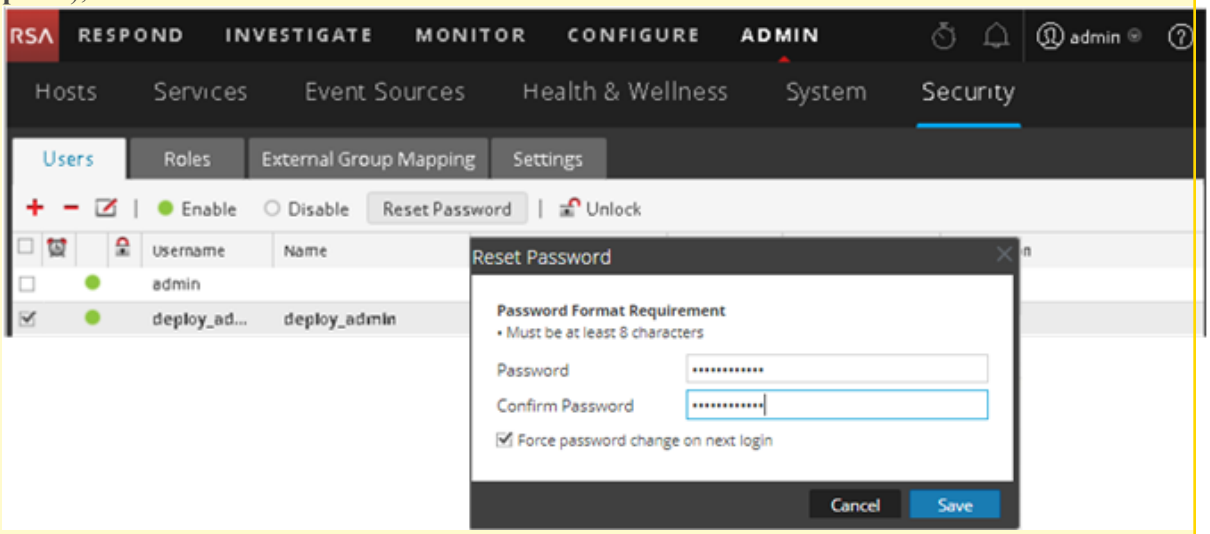
5. Appuyez sur **Entrée**. **Installer (nouvelle installation)** est sélectionnée par défaut.
   Le message **Nom de l'hôte** s'affiche.



Attention : Si vous incluez "." dans un nom d'hôte, le nom d'hôte doit également inclure un nom de domaine valide.

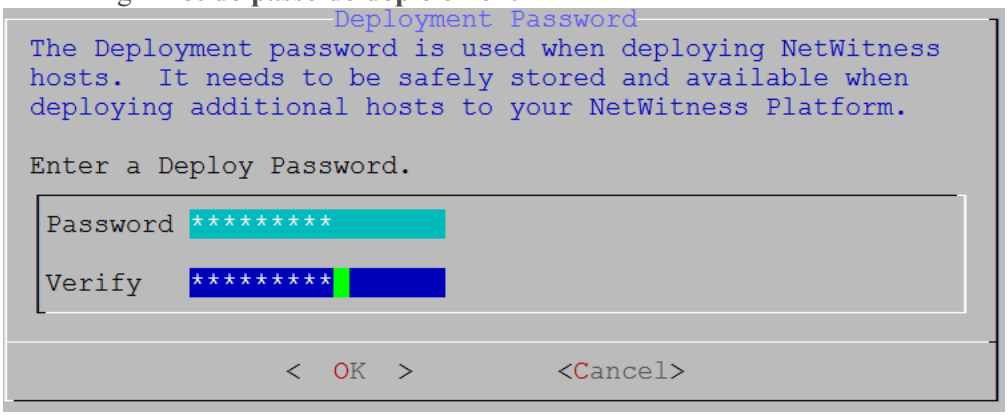
6. Appuyez sur **Entrée** si souhaitez conserver ce nom. Dans le cas contraire, naviguez jusqu'à **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** pour modifier le nom de l'hôte.
   Le message **Mot de passe maître** s'affiche.

Attention : Si vous modifiez le mot de passe utilisateur **deploy_admin** dans l'interface utilisateur NetWitness Platform (**ADMIN** > **Sécurité** > Sélectionner **deploy-admin - Réinitialiser le mot de passe**),



vous devez :
1. Ouvrir une session SSH sur l'hôte du serveur NW.
2. Exécuter le script `(/opt/rsa/saTools/bin/set-deploy-admin-password`.
3. Utiliser le nouveau mot de passe lors de l'installation de tous les nouveaux hôtes de serveur autres que NW.
4. Exécuter le script `(/opt/rsa/saTools/bin/set-deploy-admin-password` sur tous les hôtes de serveurs autres que NW dans votre déploiement.
5. Noter le mot de passe, car vous en aurez besoin plus tard dans l'installation.

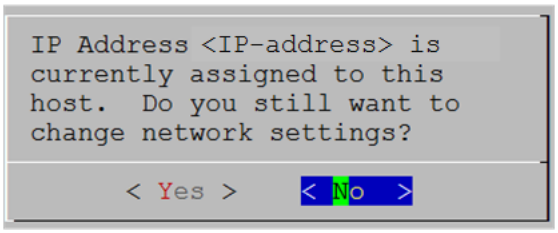
Le message **Mot de passe de déploiement** s'affiche.



Remarque : Vous devez utiliser le même mot de passe de déploiement que vous avez utilisé lors de l'installation du serveur NW.

7. Saisissez le **mot de passe**, appuyez sur la touche directionnelle Bas pour accéder à **Vérifier**, saisissez à nouveau le mot de passe, naviguez jusqu'à **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**.

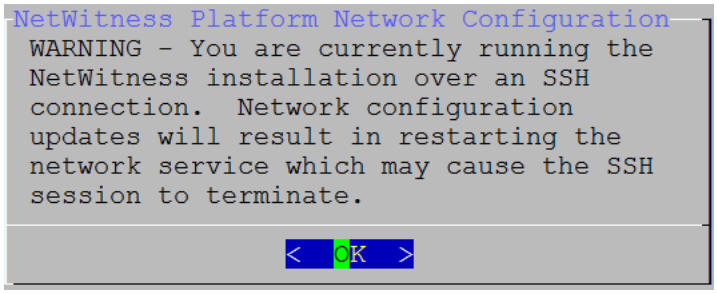
   - Si le programme d'installation détecte une adresse IP valide pour cet hôte, le message suivant s'affiche.

     Appuyez sur **Entrée** si vous souhaitez utiliser cette adresse IP et éviter de modifier les paramètres de votre réseau. Naviguez jusqu'à **Oui** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** si vous souhaitez modifier la configuration IP disponible sur l'hôte.

   - Si vous utilisez une connexion SSH, l'avertissement suivant s'affiche.

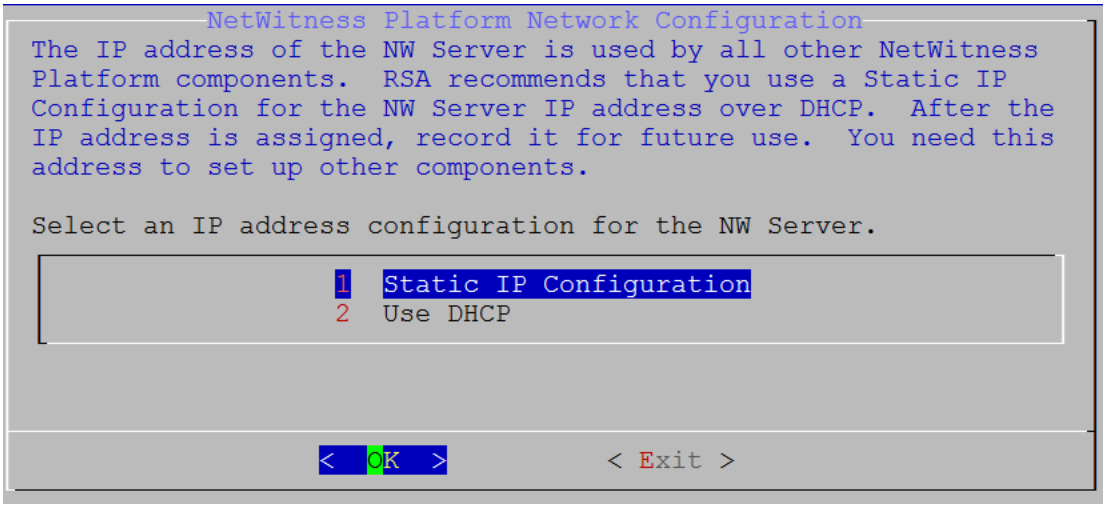
     Remarque : Si vous vous connectez directement à partir de la console hôte, l'avertissement suivant ne s'affichera pas.

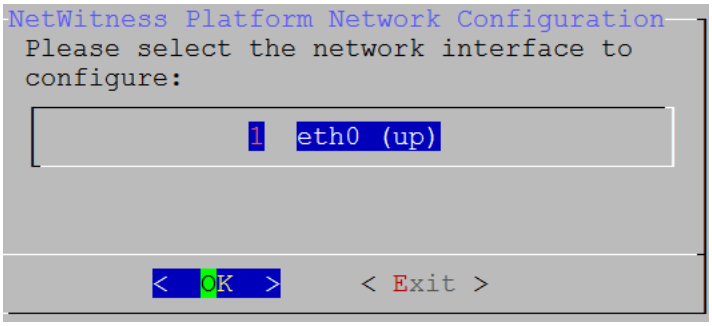
     Appuyez sur **Entrée** pour fermer le message d'avertissement.

   - Si le programme d'installation a détecté une configuration IP et que vous avez choisi de l'utiliser, le message **Mettre à jour le référentiel** s'affiche. Accédez à l'étape 11 et terminez l'installation.

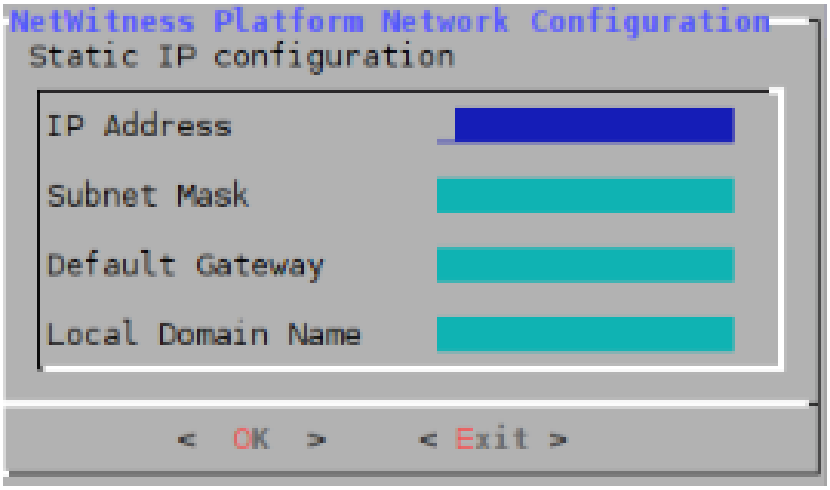
- Si le programme d'installation n'a pas détecté de configuration IP, ou si vous avez choisi de modifier la configuration IP, le message **Configuration réseau** s'affiche.



8. Naviguez jusqu'à **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** pour utiliser l'**adresse IP statique**.
   Si vous souhaitez utiliser **DHCP**, utilisez la touche directionnelle Bas jusqu'à 2 Utiliser DHCP, puis appuyez sur **Entrée**.
   Le message **Configuration de réseau** s'affiche.



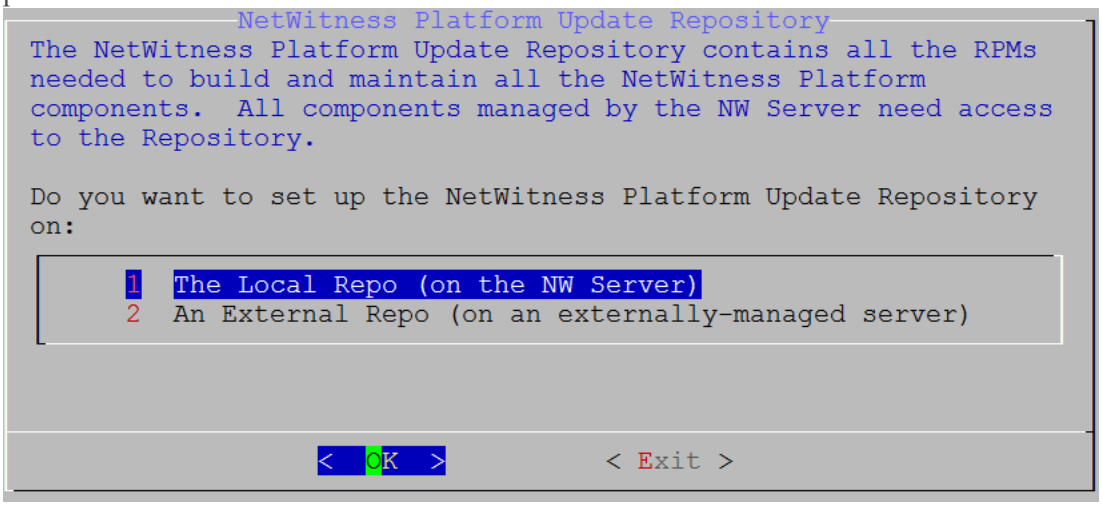
9. Utilisez la touche directionnelle Bas jusqu'à l'interface réseau que vous souhaitez, puis naviguez jusqu'à **OK** à l'aide de la touche de tabulation et appuyez sur **Entrée**. Si vous ne souhaitez pas continuer, naviguez jusqu'à **Quitter** à l'aide de la touche de tabulation.
   Le message **Configuration d'adresse IP statique** suivant s'affiche.



10. Saisissez les valeurs de configuration (en naviguant d'un champ à l'autre à l'aide de la touche directionnelle Bas), naviguez jusqu'à **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**.
    Si vous ne remplissez pas tous les champs obligatoires, un message d'erreur `All fields are required` s'affiche. Les champs **Serveur DNS secondaire** et **Nom de domaine local** ne sont pas obligatoires.
    Si vous utilisez une syntaxe ou une longueur de caractères incorrecte pour l'un des champs, un message d'erreur `Invalid <field-name>` s'affiche.

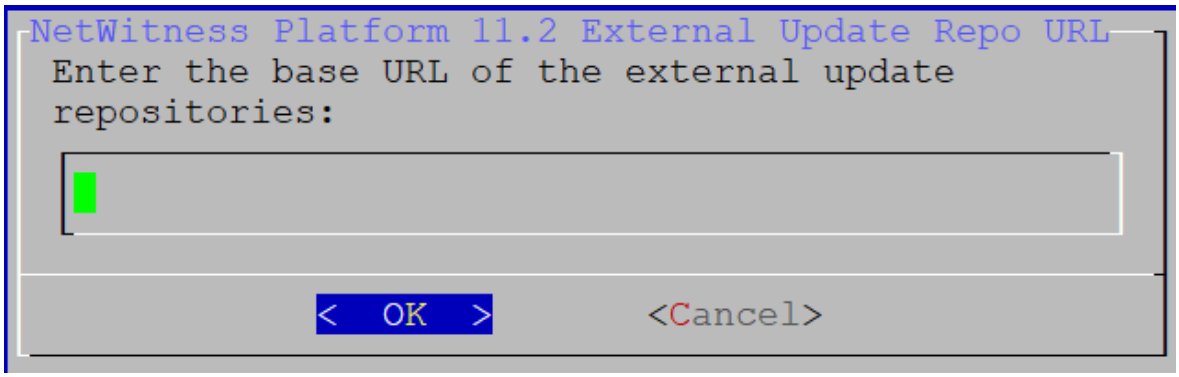
    > **Attention :** Si vous sélectionnez le **serveur DNS**, assurez-vous que le serveur DNS est correct et que l'hôte peut y accéder avant de poursuivre l'installation.

    Le message **Mise à jour du référentiel** s'affiche.
    Sélectionnez le même référentiel que celui sélectionné lors de l'installation de l'hôte du serveur NW pour tous les hôtes.

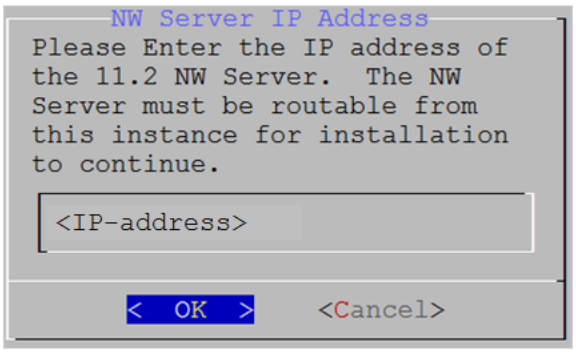


11. Appuyez sur **Entrée** pour choisir le **référentiel local** sur le serveur NW.
    Si vous souhaitez utiliser un référentiel externe, utilisez la touche directionnelle Bas pour naviguer jusqu'au **Référentiel externe**, naviguez jusqu'à **OK** à l'aide de la touche de tabulation et appuyez sur **Entrée**.

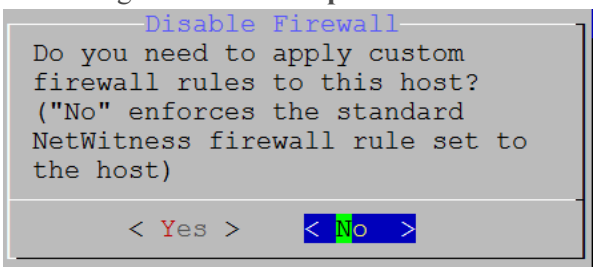
    - Si vous sélectionnez **1 Le référentiel local (sur le serveur NW)** dans le programme d'installation, assurez-vous que le média approprié est rattaché à l'hôte (média contenant le fichier ISO, par exemple une clé de version) à partir duquel NetWitness Platform 11.2.0.0 peut être installé.
    - Si vous sélectionnez **2 Un référentiel externe (sur un serveur géré en externe, et non sur le serveur NW)**, l'interface utilisateur vous invite à saisir une URL. Les référentiels vous donnent accès aux mises à jour RSA et CentOS. Reportez-vous à la section Annexe B. Créer un référentiel externe pour obtenir des instructions sur la création de ce référentiel, ainsi que l'URL de référentiel externe afin que vous puissiez la saisir dans l'invite suivante.



Saisissez l'URL de base du référentiel externe NetWitness Platform, naviguez jusqu'à **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**.
Le message **Adresse IP du serveur NW** s'affiche.



12. Saisissez l'adresse IP du serveur NW. Naviguez jusqu'à **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**.
Le message **Désactiver le pare-feu** s'affiche.



13. Naviguez vers l'onglet **Non** (par défaut) à l'aide de la touche de tabulation, puis appuyez sur **Entrée** pour utiliser la configuration de pare-feu standard. Naviguez vers l'onglet **Oui** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** pour désactiver la configuration de pare-feu standard.

- Pour confirmer votre sélection, choisissez **Oui**, dans le cas contraire, choisissez **Non** pour utiliser la configuration du pare-feu standard.

```
Warning: you chose to disable the default NetWitness
firewall configuration which means you must set up
firewall rules manually.

Select "Yes" to confirm that you will set up firewall
rules manually.

                < Yes >          < No  >
```

Le message **Démarrer l'installation** s'affiche.

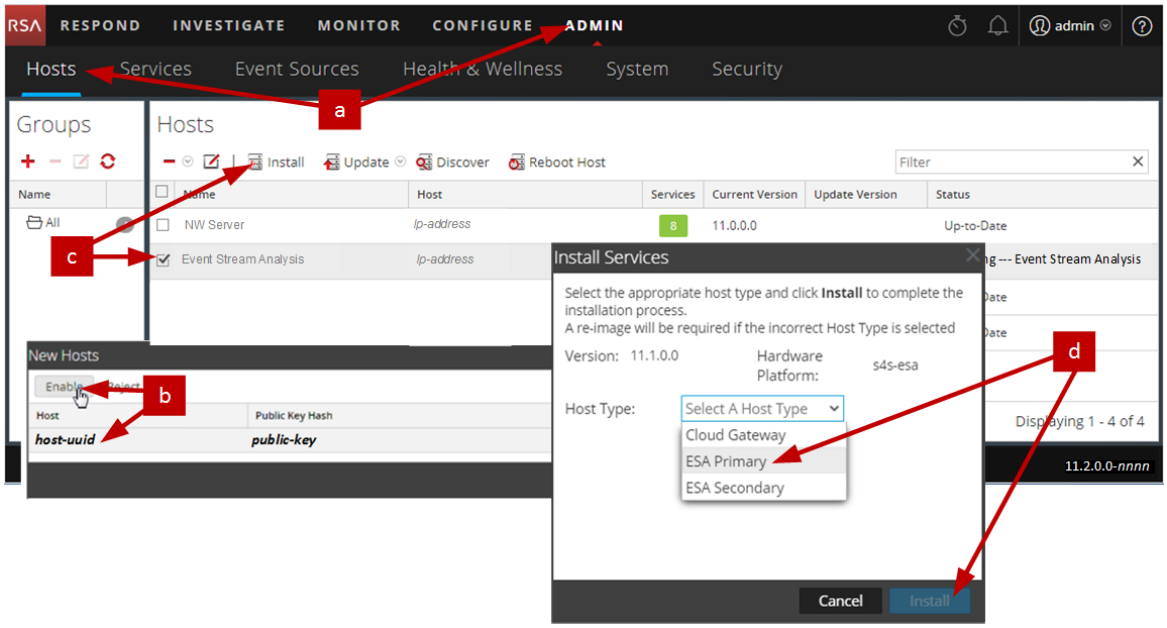
```
                Start Install/Upgrade
All the required information has been gathered.

Select "1 Install Now" to start the installation
on this host.

                1  Install Now
                2  Restart

              <  OK  >        < Exit >
```

14. Appuyez sur **Entrée** pour installer la version 11.2 sur le serveur NW.
    Lorsque **Installation terminée** s'affiche, vous disposez d'un hôte de serveur autre que NW générique avec un système d'exploitation compatible avec NetWitness Platform 11.2.
15. Installez le service de composants sur l'hôte.
    a. Connectez-vous à NetWitness Platform, puis accédez à **ADMIN** > **Hôtes**.
       La boîte de dialogue **Nouveaux hôtes** s'affiche avec la vue **Hôtes** grisée en arrière-plan.

       > **Remarque :** Si la boîte de dialogue **Nouveaux hôtes** ne s'affiche pas, cliquez sur **Découvrir** dans la barre d'outils de la vue Hôtes.

    b. Sélectionnez l'hôte dans la boîte de dialogue **Nouveaux hôtes**, puis cliquez sur **Activer**.
       La boîte de dialogue **Nouveaux hôtes** se ferme et l'hôte s'affiche dans la vue **Hôtes**.
    c. Sélectionnez cet hôte dans la vue **Hôtes** (par exemple, **Event Stream Analysis**), puis cliquez sur Install.
       La boîte de dialogue **Installer les services** s'affiche.

d. Sélectionnez le type d'hôte approprié (par exemple, **ESA primaire**) dans **Type d'hôte**, puis cliquez sur **Installer**.



Vous avez terminé l'installation de l'hôte de serveur autre que NW dans NetWitness Platform.

16. Suivez les étapes 1 à 15 pour le reste des composants de serveur autres que NW NetWitness Platform.

17. Exigences de licence complètes pour les services installés.
Pour plus d'informations, consultez le *Guide de gestion des licences de NetWitness Platform 11.2*.
Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

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 l'installation

Cette section contient les tâches à réaliser après avoir installé la version 11.2.

- Général
- RSA NetWitness® Endpoint Insights
- Activation FIPS
- RSA NetWitness® UEBA

Général

(Facultatif) Tâche 1 - reconfigurer les serveurs DNS après la mise à niveau 11.2

Sur NetWitness Server, effectuez les tâches suivantes pour reconfigurer le serveur DNS dans NetWitness Platform 11.2.

1. Connectez-vous à l'hôte de serveur avec vos informations d'identification`root` .
2. Modifiez le fichier `/etc/netwitness/platform/resolv.dnsmasq` :
   a. Remplacez l'adresse IP correspondant à `nameserver`.
   Si vous devez remplacer les deux serveurs DNS, remplacez les entrées IP pour les deux hôtes par des adresses valides.
   L'exemple suivant montre les deux entrées DNS.

   ```
   root@nw11sas5:~
   # Generated by NetworkManager
   nameserver nn.nn.55.15
   nameserver nn.nn.55.17
   search netwitness.local
   ~
   ```

   L'exemple suivant présente les nouvelles valeurs DNS.

   ```
   root@nw11sas5:~
   # Generated by NetworkManager
   nameserver nn.nn.44.37
   nameserver nn.nn.66.17
   search netwitness.local
   ~
   ```

   b. Enregistrez le fichier `/etc/netwitness/platform/resolv.dnsmasq`.
   c. Démarrez le DNS interne, exécutez la commande suivante :
   `systemctl restart dnsmasq`

RSA NetWitness Endpoint Insights

(Facultatif) Tâche 2 - Installer Endpoint Hybrid ou Endpoint Log Hybrid

Vous devez installer l'un des services suivants pour installer NetWitness Platform Endpoint Insights dans votre déploiement :

- Endpoint Hybrid
- Endpoint Log Hybrid

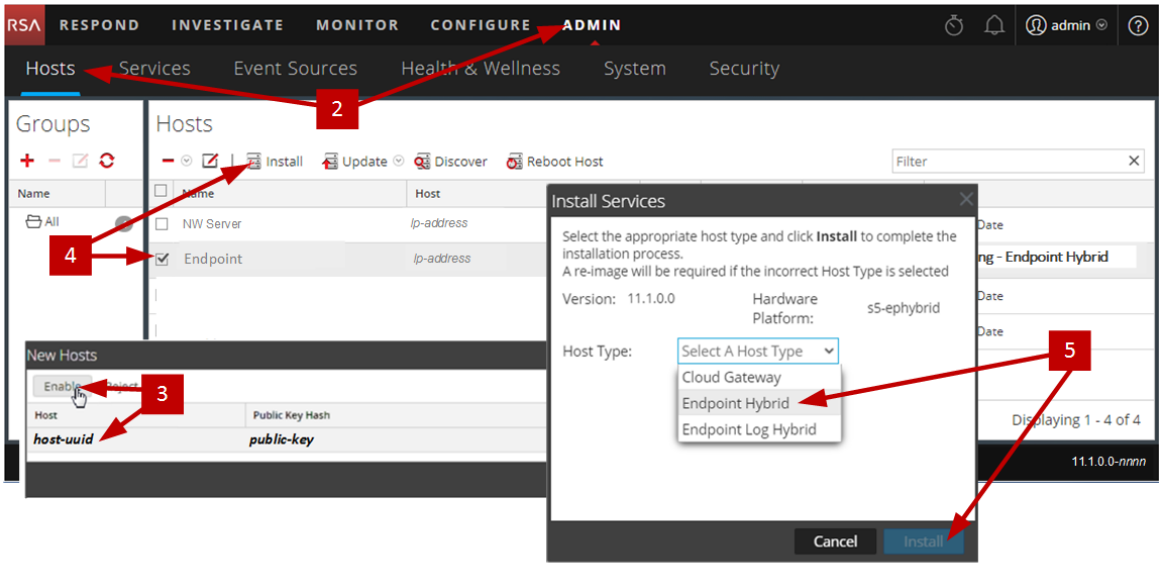
Attention : Vous ne pouvez installer qu'une seule instance des services ci-dessus dans votre déploiement.

Remarque : Vous devez installer Endpoint Hybrid ou Endpoint Log Hybrid sur l'appliance S5 ou Dell R730.

1. Effectuez les étapes 1 à 14 pour l'hôte physique ou les étapes 1 à 15 pour les hôtes virtuels sous « Tâche 2 - Installer ka version 11.2 sur les autres hôtes de composants » dans « Tâches d'installation » du *Guide d'installation de l'hôte physique de NetWitness Platform pour la version 11.2*. Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.
2. Connectez-vous à NetWitness Platform, puis cliquez sur **ADMIN** > **Hôtes**.
   La boîte de dialogue Nouveaux hôtes s'affiche avec la vue Hôtes grisée en arrière-plan.

   Remarque : Si la boîte de dialogue Nouveaux hôtes ne s'affiche pas, cliquez sur **Découvrir** dans la barre d'outils de la vue **Hôtes**.
3. Sélectionnez l'hôte dans la boîte de dialogue **Nouveaux hôtes**, puis cliquez sur **Activer**.
   La boîte de dialogue Nouveaux hôtes se ferme et l'hôte s'affiche dans la vue Hôtes.
4. Sélectionnez cet hôte dans la vue **Hôtes** (par exemple, **Endpoint**), puis cliquez sur Install.
   La boîte de dialogue Installer les services s'affiche.

5. Sélectionnez le service approprié, soit **Endpoint Hybrid**, soit **Endpoint Log Hybrid**, puis cliquez sur **Installer**.
   Endpoint Hybrid est utilisé en guise d'exemple dans la capture d'écran suivante.



6. Assurez-vous que tous les services Endpoint Hybrid ou Endpoint Log Hybrid sont en cours d'exécution.
7. Configurez le transfert des métadonnées Endpoint.
   Reportez-vous à la section *Guide de configuration d'Endpoint Insights* pour obtenir des instructions sur la façon de configurer le transfert des métadonnées Endpoint.Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.
8. Installez l'Agent Endpoint Insights.
   Reportez-vous à la section *Guide d'installation de l'agent Endpoint Insights* pour obtenir des instructions détaillées sur la façon d'installer l'agent. Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

Activation FIPS

(Facultatif) Tâche 3 - Activer le mode FIPS

Le mode FIPS (Federal Information Processing Standard) est activé sur tous les services à l'exception du Log Collector, du Log Decoder et du Decoder. Le mode FIPS ne peut pas être désactivé sur tous les services sauf Log Collector, Log Decoder et Decoder. Pour plus d'informations sur l'activation du mode FIPS pour ces services, consultez la rubrique « Activer ou désactiver FIPS » dans le *guide de maintenance du système RSA NetWitness Platform*. Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

RSA NetWitness® UEBA

(Facultatif) Tâche 4 - Installer NetWitness UEBA

Pour configurer NetWitness UEBA dans NetWitness Platform 11.2, vous devez installer et configurer le service NetWitness UEBA.

La procédure suivante vous montre comment installer le service NetWitness UEBA sur un type d'hôte NetWitness UEBA et configurer le service.

1. Effectuez les étapes 1 à 14 pour l'hôte physique ou les étapes 1 à 15 pour les hôtes virtuels sous « Tâche 2 - Installer la version 11.2 sur les autres hôtes de composants » dans « Tâches d'installation » du *Guide d'installation de l'hôte physique de la plate-forme NetWitness pour la version 11.2.*Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

   Remarque : Le mot de passe de l'interface utilisateur du serveur Web Kibana et Airflow est le même que le mot de passe admin de déploiement. Assurez-vous d'enregistrer ce mot de passe et de le stocker dans un emplacement sûr.

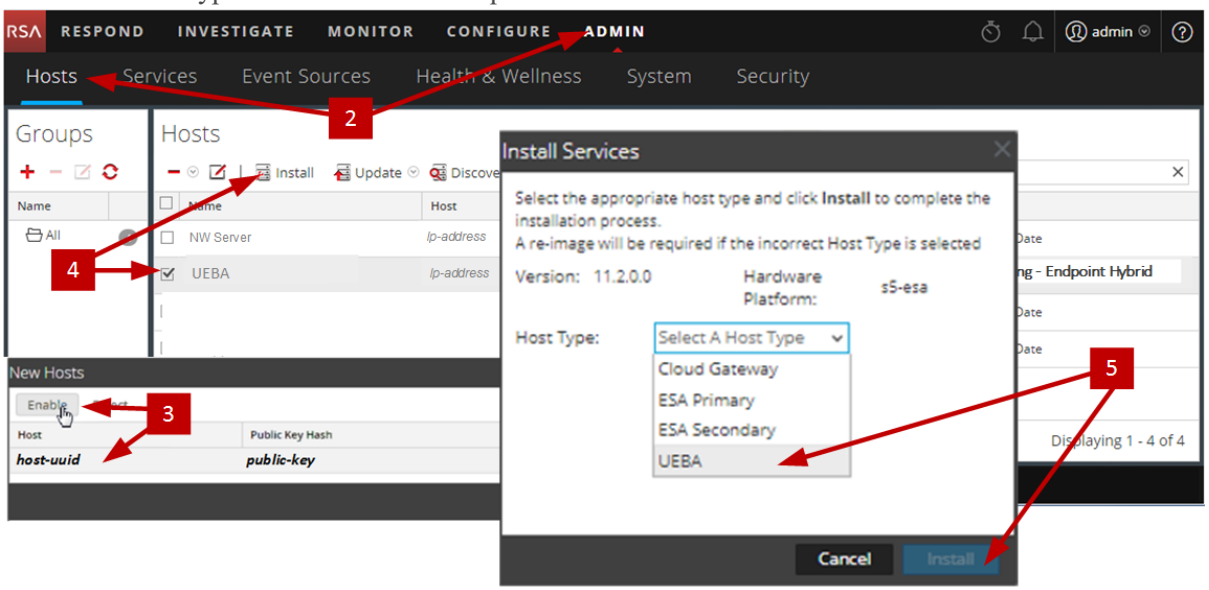
2. Connectez-vous à la plate-forme NetWitness et accédez à **ADMIN** > **Hôtes**.
   La boîte de dialogue Nouveaux hôtes s'affiche avec la vue Hôtes grisée en arrière-plan.

   Remarque : Si la boîte de dialogue Nouveaux hôtes ne s'affiche pas, cliquez sur **Découvrir** dans la barre d'outils de la vue **Hôtes**.

3. Sélectionnez l'hôte dans la boîte de dialogue **Nouveaux hôtes**, puis cliquez sur **Activer**.
   La boîte de dialogue Nouveaux hôtes se ferme et l'hôte s'affiche dans la vue Hôtes.

4. Sélectionnez cet hôte dans la vue **Hôtes** (par exemple, **UEBA**), puis cliquez sur Install.
   La boîte de dialogue Installer les services s'affiche.

5. Sélectionnez le type d'hôte **UEBA** et cliquez sur **Installer**.



6. Assurez-vous que le service UEBA est en cours d'exécution.

7. Exigences de licence complètes pour NetWitness UEBA.
   Pour plus d'informations, consultez le *Guide de gestion des licences de NetWitness Platform 11.2*. Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

   Remarque : La plate-forme NetWitness prend en charge la licence d'analyse de comportement utilisateur et entité (UEBA). Cette licence est utilisée en fonction du nombre d'utilisateurs. La licence d'essai prête à l'emploi est une licence d'essai de 90 jours. Dans le cas des licences UEBA, la période d'essai de 90 jours débute à partir du moment où le service UEBA est déployé sur le produit NetWitness Platform.

8. Configurez NetWitness UEBA.
   Vous devez configurer une source de données (Broker ou Concentrator), la date de début de collecte de données historiques et les schémas de données.

   IMPORTANT : CSi votre déploiement comporte plusieurs Concentrators, RSA vous recommande d'assigner le Broker sur votre hiérarchie de déploiement pour la source de données NetWitness UEBA.

   a. Déterminez la date la plus proche dans le NWDB du schéma de données que vous prévoyez de choisir (`AUTHENTICATION`, `FILE`, `ACTIVE_DIRECTORY` ou toute combinaison de ces schémas) à spécifier dans `startTime` à l'étape c. Si vous prévoyez de spécifier plusieurs schémas, utilisez la date la plus proche parmi tous les schémas. Si vous ne savez pas quel schéma de données choisir, vous pouvez spécifier les trois schémas de données (c'est-à-dire `AUTHENTICATION` `FILE`, et `ACTIVE_DIRECTORY`) pour qu'UEBA ajuste les modèles qu'il peut prendre en charge en fonction des fichiers journaux Windows disponibles. Vous pouvez utiliser l'une des méthodes suivantes pour déterminer la date de la source de données.

- Utilisez la date de rétention des données (c'est-à-dire, si la durée de rétention des données est de 48 heures, `startTime` = <48 heures avant l'heure actuelle>).
- Recherchez la date la plus proche dans NWDB.

b. Créez un compte d'utilisateur pour la source de données (Broker ou Concentrator) pour vous authentifier auprès de la source de données.

   i. Connectez-vous à la plate-forme NetWitness.

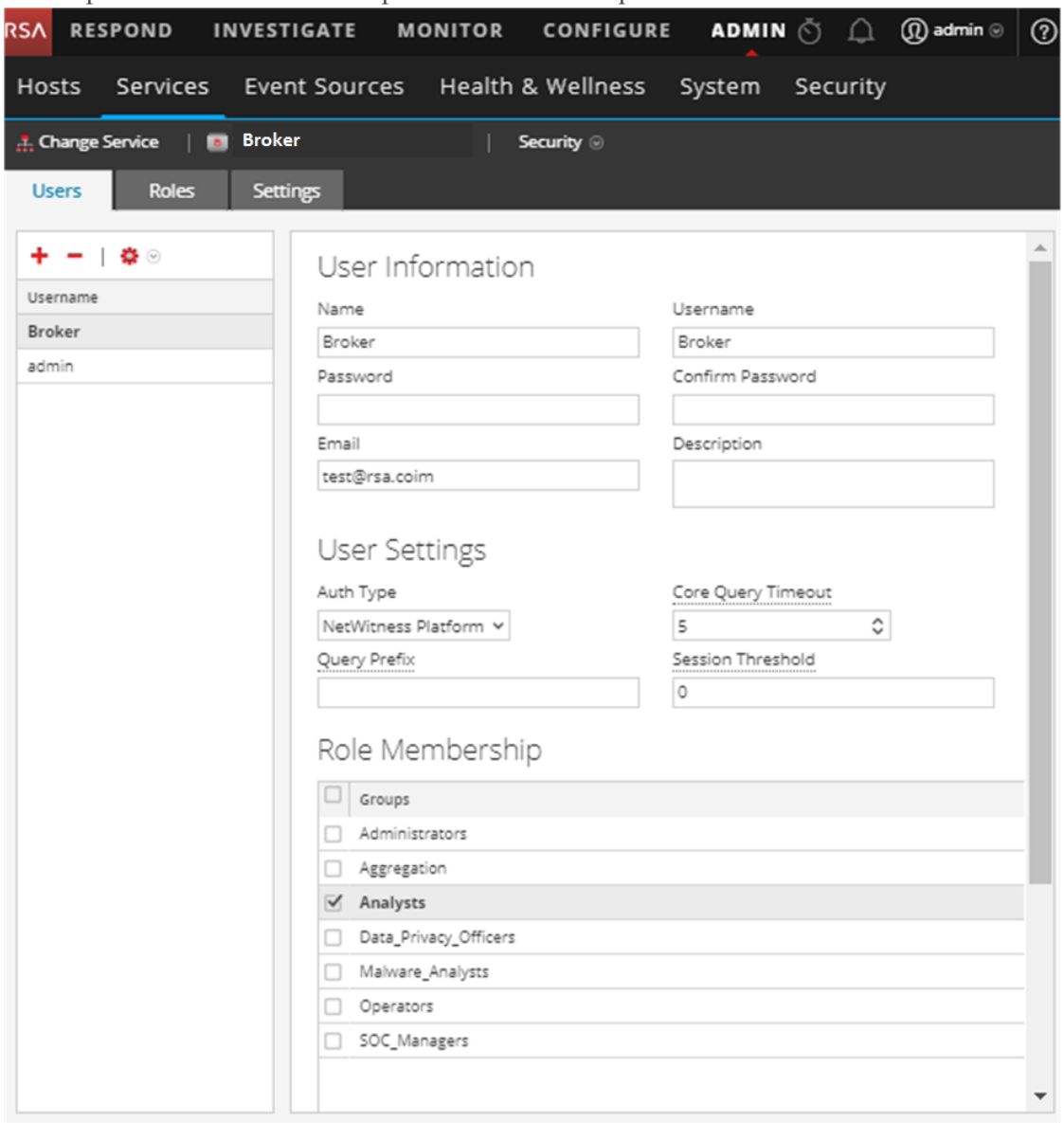
   ii. Accédez à **Administrateur** > **Services**.

   iii. Localisez le service de source de données (Broker ou Concentrator).

   Sélectionnez un service, puis (Actions) > **Vue** > **Sécurité**

   iv. Créez un nouvel utilisateur et affectez le rôle « Analystes » à cet utilisateur.

L'exemple suivant montre un compte d'utilisateur créé pour un Broker.



c. Connexion en SSH au serveur Netwitness UEBA.

d. Exécutez les commandes suivantes :
```
/opt/rsa/saTools/ueba-server-config -u <user> -p <password> -h <host> -o
<type> -t <startTime> -s <schemas> -v
```

Où :

Argument	Variable	Description
-u	<user>	Le nom d'utilisateur des informations d'identification pour l'instance Broker ou Concentrator que vous utilisez comme source de données.
-p	<password>	Le mot de passe des informations d'identification pour l'instance Broker ou Concentrator que vous utilisez comme source de données. Les caractères spéciaux suivants sont pris en charge dans un mot de passe. `!"#$%&()*+,-:;<=>?@[\]^_`\{\|}` Si vous souhaitez inclure un ou des caractères spéciaux, vous devez délimiter le mot de passe avec un signe d'apostrophe, par exemple : `sh /opt/rsa/saTools/bin/ueba-server-config -u brokeruser -p '!"UHfz?@ExMn#$' -h 10.64.153.104 -t 2018-08-01T00:00:00Z -s 'AUTHENTICATION FILE ACTIVE_DIRECTORY' -o broker -v`
-h	<host>	Adresse IP Broker ou Concentrator utilisé comme source de données. Actuellement, une seule source de données est prise en charge.
-o	<type>	Type d'hôte de source de données (`broker` ou `concentrator`).
-t	<startTime>	Heure de début historique de la collecte des données à partir de la source de données au format AAAA-MM-DDTHH-MM-SSZ (par exemple, `2018-08-15T00:00:00Z`). **Remarque :** Le script interprète l'heure que vous saisissez selon le fuseau UTC (temps universel coordonné) et il n'ajuste pas l'heure à votre fuseau horaire local.

Argument	Variable	Description
-s	<schemas>	Tableau de schémas de données. Si vous souhaitez spécifier plusieurs schémas, utilisez un espace pour séparer chaque schéma (par exemple, 'AUTHENTICATION FILE ACTIVE_DIRECTORY'). **Remarque :** Si vous spécifiez les trois schémas de données (c'est-à-dire AUTHENTICATION, FILE et ACTIVE_DIRECTORY), UEBA ajuste les modèles qu'il peut prendre en charge en fonction des journaux Windows disponibles.
-v		Mode explicite.

9. Finalisez la configuration de NetWitness UEBA en fonction des besoins de votre organisation. Reportez-vous au *Guide d'utilisation RSA NetWitness UEBA* pour en savoir plus. Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

Annexe A. Dépannage

Cette section décrit les solutions aux problèmes que vous pouvez rencontrer lors des installations et des mises à niveau. Dans la plupart des cas, NetWitness Platform crée des messages de log lorsqu'il rencontre ces problèmes.

Remarque : Si les solutions de dépannage suivantes ne vous permettent pas de résoudre un problème de mise à jour, contactez le support client (https://community.RSA.com/docs/DOC-1294).

Cette rubrique contient la documentation de dépannage des services, fonctionnalités et processus suivants :

- Interface de ligne de commande (CLI)
- Script de sauvegarde
- Event Stream Analysis
- Service Log Collector (`nwlogcollector`)
- Orchestration
- Serveur NW
- Reporting Engine
- NetWitness UEBA

Interface de ligne de commande (CLI)

Message d'erreur	L'interface de ligne de commande (CLI) affiche : « Échec de l'orchestration.» `Mixlib::ShellOut::ShellCommandFailed: Command execution failed. STDOUT/STDERR suppressed for sensitive resource in/var/log/netwitness/config-management/chef-solo.log`
Cause	Saisie du mauvais `deploy_admin` mot de passe dans `nwsetup-tui`.
Solution	Récupérez votre mot de passe `deploy_admin`. 1. Ouvrez une session SSH sur l'hôte du serveur NW. `security-cli-client --get-config-prop --prop-hierarchy nw.security-client --prop-name deployment.password` Exécutez la commande SSH sur l'hôte ayant échoué. 2. Exécutez à nouveau la commande `nwsetup-tui` à l'aide du mot de passe `deploy_admin` approprié.

Message d'erreur	`ERROR com.rsa.smc.sa.admin.web.controller.ajax.health. AlarmsController - Cannot connect to System Management Service`
Cause	NetWitness Platform considère Service Management Service (SMS) comme arrêté après une mise à niveau réussie, même si le service fonctionne.
Solution	Redémarrez le service SMS. `systemctl restart rsa-sms`

Message d'erreur	Vous recevez un message dans l'interface utilisateur vous invitant à redémarrer l'hôte après avoir mis à jour et redémarrer l'hôte hors connexion. SA Server IP-Address 8 version-number Reboot Host
Cause	Vous ne pouvez pas utiliser l'interface de ligne de commande (CLI) pour redémarrer l'hôte. Vous devez utiliser l'interface utilisateur.
Solution	Redémarrez l'hôte dans la vue Hôte dans l'interface utilisateur.

Sauvegarde (script `nw-backup`)

Message d'erreur	`WARNING: Incorrect ESA Mongo admin password for host <hostname>.`
Cause	Le mot de passe administrateur ESA Mongo contient des caractères spéciaux (par exemple, ! @# $% ^ qwerty)
Solution	Remplacez le mot de passe administrateur ESA mongo par la valeur initiale par défaut « netwitness » avant d'exécuter la sauvegarde.

Erreur	Erreurs de sauvegarde générées par le paramètre d'attribut `immutable`. Voici un exemple d'erreur qui peut s'afficher :
	`Backing up NetWitness Config (/etc/netwitness) files from: saserver1`
	`WARNING: Errors occurred while backing up NetWitness Configuration files.`
	`Verify contents of saserver1-192.168.2.102-etc-netwitness.tar.gz`
	`Located in /var/netwitness/database/nw-backup/2018-03-01/saserver1-192.168.2.102-backup.tar.gz`
	`Backing up SA UI Web Server (/var/lib/netwitness/uax) files from: saserver1`

Cause	Si l'un de vos fichiers a le paramètre immutable flag défini (pour éviter que le processus Puppet n'écrase un fichier personnalisé), le fichier ne sera pas inclus dans le processus de sauvegarde et une erreur sera générée.
Solution	Sur l'hôte contenant les fichiers avec le paramètre immutable flag défini, exécutez la commande suivante pour supprimer le paramètre immuable des fichiers : `chattr -i <filename>`

Erreur	Erreur lors de la création du fichier d'informations de configuration réseau en raison d'entrées incorrectes ou dupliquées dans le fichier de configuration réseau principal : `/etc/sysconfig/network-scripts/ifcfg-em1` Vérifiez le contenu de `/var/netwitness/logdecoder/packetdb/nw-backup/2018-02-23/S5-BROK-36-10.25.53.36-network.info.txt`
Cause	Il existe des entrées incorrectes ou dupliquées pour l'un des champs suivants : DEVICE, BOOTPROTO, IPADDR, NETMASK ou GATEWAY, trouvés lors de la lecture du fichier de configuration de l'interface Ethernet principal à partir de l'hôte en cours de sauvegarde.

Solution	Créez manuellement un fichier à l'emplacement de sauvegarde sur le serveur de sauvegarde externe, ainsi qu'à l'emplacement de sauvegarde local de l'hôte sur lequel les autres sauvegardes ont été exécutées. Le nom du fichier doit être au format `<hostname>-<hostip>-network.info.txt` et doit contenir les entrées suivantes :
	`DEVICE=<devicename> ; # from the host's primary ethernet interface config file`
	`BOOTPROTO=<bootprotocol> ; # from the host's primary ethernet interface config file`
	`IPADDR=<value> ; # from the host's primary ethernet interface config file`
	`NETMASK=<value> ; # from the host's primary ethernet interface config file`
	`GATEWAY=<value> ; # from the host's primary ethernet interface config file`
	`search <value> ; # from the host's /etc/resolv.conf file`
	`nameserver <value> ; # from the host's /etc/resolv.conf file`

Event Stream Analysis

Problème	Le service ESA se bloque après la mise à niveau vers la version 11.2.0.0 à partir d'une installation avec le mode FIPS activé.
Cause	Le service ESA pointe vers un magasin de clés non valide.

Solution	1. Ouvrez une session SSH sur l'hôte primaire ESA et connectez-vous.
	2. Dans le fichier `/opt/rsa/esa/conf/wrapper.conf`, remplacez la ligne suivante :
	`wrapper.java.additional.5=-Djavax.net.ssl.keyStore=/opt/rsa/esa/../carlos/keystore`
	par :
	`wrapper.java.additional.5=-Djavax.net.ssl.keyStore=/opt/rsa/carlos/keystore`
	3. Exécutez la commande suivante pour redémarrer ESA.
	`systemctl restart rsa-nw-esa-server`
	Remarque : si vous disposez de plusieurs hôtes ESA et que vous rencontrez le même problème, répétez les étapes 1 à 3 compris sur chaque hôte ESA secondaire.

Service Log Collector (`nwlogcollector`)

Les logs Log Collector sont publiés dans `/var/log/install/nwlogcollector_install.log` sur l'hôte qui exécute le service `nwlogcollector` .

Message d'erreur	`<timestamp>.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.`
Cause	Le Lockbox du Log Collector ne s'est pas ouvert après la mise à jour.
Solution	Connectez-vous à NetWitness Platform et redéfinissez la trace du système en réinitialisant le mot de passe de la valeur système stable pour le Lockbox, comme décrit dans « Réinitialiser la valeur système stable » dans la rubrique « Configurer des paramètres de sécurité Lockbox » du *Guide de configuration de Log Collection*. Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

Message d'erreur	`<timestamp> NwLogCollector_PostInstall: Lockbox Status : Not Found`
Cause	Le Lockbox du Log Collector n'a pas été configuré après la mise à jour.
Solution	Si vous utilisez le Lockbox de Log Collector, connectez-vous à NetWitness Platform et configurez le Lockbox, comme décrit dans la rubrique « Configurer les paramètres de sécurité Lockbox » du *Guide de configuration de Log Collection*. Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

Message d'erreur	`<timestamp>: NwLogCollector_PostInstall: Lockbox Status : Lockbox maintenance required: The lockbox stable value threshold requires resetting. To reset the system fingerprint, select Reset Stable System Value on the settings page of the Log Collector.`
Cause	Vous devez réinitialiser le champ du seuil de valeur stable pour le Lockbox du Log Collector.
Solution	Connectez-vous à NetWitness Platform et redéfinissez le mot de passe de la valeur du système stable pour le Lockbox, comme décrit dans la rubrique « Réinitialiser la valeur système stable » de la rubrique « Configurer des paramètres de sécurité Lockbox » du *Guide de configuration de Log Collection*. Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

Problème	Vous avez préparé un Log Collector à mettre à niveau et ne souhaitez plus le mettre à niveau pour l'instant.
Cause	Retard dans la mise à niveau.
Solution	Utilisez la chaîne de commande suivante pour restaurer un Log Collector dont la mise à niveau a été préparée afin qu'il fonctionne à nouveau normalement. `# /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --revert`

Serveur NW

Ces logs sont publiés dans `/var/netwitness/uax/logs/sa.log` sur l'hôte de serveur NW.

Problème	Après la mise à niveau, vous remarquez que les logs d'audit ne sont pas transmis à l'installation d'audit global configurée, ou le message suivant s'affiche dans le fichier `sa.log`. `Syslog Configuration migration failed. Restart jetty service to fix this issue`
Cause	La migration de l'installation d'audit global du serveur NW de la version 10.6.6.x vers la version 11.2.0.0 a échoué.
Solution	1. Ouvrez une session SSH sur le serveur NW. 2. Exécutez la commande suivante : `orchestration-cli-client --update-admin-node`

Orchestration

Ces logs du serveur d'orchestration sont publiés dans `/var/log/netwitness/orchestration-server/orchestration-server.log` sur l'hôte de serveur NW.

Problème	1. Échec de la tentative de mise à niveau d'un hôte de serveur non NW. 2. Nouvelle tentative échouée de mise à niveau pour cet hôte. Le message suivant s'affiche dans le fichier `orchestration-server.log`. `"'file' _virtual_ returned False: cannot import name HASHES""`
Cause	Salt Minion a peut-être été mis à niveau et n'a jamais redémarré sur un hôte de serveur non NW

Solution	1. SSH vers l'hôte de serveur non NW dont la mise à niveau a échoué.
	2. Exécutez les commandes suivantes.
	`systemctl unmask salt-minion`
	`systemctl restart salt-minion`
	3. Réessayez la mise à niveau de l'hôte de serveur non NW.

Service Reporting Engine

Les logs de mise à jour du Reporting Engine sont publiés dans le fichier `/var/log/re_install.log` sur l'hôte exécutant le service Reporting Engine.

Message d'erreur	`<timestamp> : Available free space in /var/netwitness/re-server/rsa/soc/reporting-engine [ ><existing-GB ] is less than the required space [ <required-GB> ]`
Cause	Échec de la mise à jour du Reporting Engine car vous ne disposez pas de suffisamment d'espace disque.
Solution	Libérez de l'espace disque pour disposer de l'espace requis mentionné dans le message log. Consultez la rubrique « Ajouter de l'espace supplémentaire pour les rapports volumineux » dans le *Guide de configuration de Reporting Engine* pour obtenir des instructions sur la façon de libérer de l'espace disque. Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

NetWitness UEBA

Problème	L'interface utilisateur n'est pas accessible.
Cause	Vous disposez de plus d'un service NetWitness UEBA existant dans votre déploiement NetWitness et vous ne pouvez disposer que du service NetWitness UEBA dans votre déploiement.

Solution	Effectuez les étapes suivantes pour supprimer le service NetWitness UEBA supplémentaire.
	1. SSH vers NW Server et exécutez les commandes suivantes pour interroger la liste des services NetWitness UEBA installés.
	`# orchestration-cli-client --list-services|grep presidio-airflow`
	`... Service: ID=7e682892-b913-4dee-ac84-ca2438e522bf, NAME=presidio-airflow, HOST=xxx.xxx.xxx.xxx:null, TLS=true`
	`... Service: ID=3ba35fbe-7220-4e26-a2ad-9e14ab5e9e15, NAME=presidio-airflow, HOST=xxx.xxx.xxx.xxx:null, TLS=true`
	2. Dans la liste des services, déterminez quelle instance du service `presidio-airflow` doit être supprimée (en examinant les adresses hôte).
	3. Exécutez la commande suivante pour supprimer le service supplémentaire de l'orchestration (utilisez l'ID de service correspondant dans la liste des services) :
	`# orchestration-cli-client --remove-service --id <ID-for-presidio-airflow-form-previous-output>`
	4. Exécutez la commande suivante pour mettre à jour le nœud 0 afin de restaurer NGINX :
	`# orchestration-cli-client --update-admin-node`
	5. Connectez-vous à NetWitness Platform, accédez à **ADMIN** > **Hôtes** et retirez l'hôte NetWitness UEBA supplémentaire.

Annexe B. Créer un référentiel externe

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

1. Connectez-vous à l'hôte du serveur Web.
2. Créez le répertoire `ziprepo` destiné à héberger le référentiel NW (`netwitness-11.2.0.0.zip`) sous `web-root` sur le serveur Web. Par exemple, si `/var/netwitness` est la racine Web, soumettez la chaîne de commande suivante.
   ```
   mkdir /var/netwitness/ziprepo
   ```
3. Créez le répertoire 11.2.0.0 sous `/var/netwitness/ziprepo`.
   ```
   mkdir /var/netwitness/ziprepo/11.2.0.0
   ```
4. Créez les répertoires `OS` et `RSA` sous `/var/netwitness/ziprepo/11.2.0.0`.
   ```
   mkdir /var/netwitness/ziprepo/11.2.0.0/OS
   mkdir /var/netwitness/ziprepo/11.2.0.0/RSA
   ```
5. Décompressez le fichier `netwitness-11.2.0.0.zip` dans le répertoire `/var/netwitness/ziprepo/11.2.0.0`.
   ```
   unzip netwitness-11.2.0.0.zip -d /var/netwitness/ziprepo/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.
6. Décompressez le fichier :
   a. `OS-11.2.0.0.zip` dans le répertoire `/var/netwitness/ziprepo/11.2.0.0/OS`.
      ```
      unzip /var/netwitness/ziprepo/11.2.0.0/OS-11.2.0.0.zip -d
      /var/netwitness/ziprepo/11.2.0.0/OS
      ```

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

   b. `RSA-11.2.0.0.zip` dans le répertoire `/var/netwitness/ziprepo/11.2.0.0/RSA`.
      ```
      unzip /var/netwitness/ziprepo/11.2.0.0/RSA-11.2.0.0.zip -d
      ```

```
/var/netwitness/ziprepo/11.2.0.0/RSA
```

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

L'URL externe pour le référentiel est `http://<web server IP address>/ziprepo`.

7. Utilisez `http://<web server IP address>/ziprepo` 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 (nwsetup-tui).

Historique des révisions

Révision	Date	Description	Auteur
1	15 août 2018	Version pour les opérations	IDD

1.1	24 septembre 2018	Mise à jour de la chaîne de commande du script de configuration UEBA dans les tâches postérieures à l'installation pour éviter toute confusion et supprimer l'extension `.sh` du script.
		Chaîne de commande incorrecte :
		`./ueba-server-config.sh -u <user> -p <password> -h <host> -o <type> -t <startTime> -s <schemas> -v`
		Chaîne de commande révisée :
		`/opt/rsa/saTools/ueba-server-config -u <user> -p <password> -h <host> -o <type> -t <startTime> -s <schemas> -v`
			IDD

1.2	10 octobre 2018	Plusieurs modifications ont été apportées à « Tâche 4 - Installer NetWitness UEBA » dans les tâches postérieures à l'installation (voir SADOCS-1592).	IDD
1.3	11 octobre 2018	Ajout d'une rubrique sur la configuration d'un stockage externe attaché pour l'amélioration de SADOCS-1597	IDD
1.4	29 novembre 2018	Ajout d'une note sur les licences UEBA Trail.	IDD