



Guide de configuration des hôtes virtuels

pour la version 11.0.0.0



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 d'EMC 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 d'EMC.

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

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

février 2018

Sommaire

Guide de configuration de l'hôte virtuel	5
Déploiement virtuel de base	6
Abréviations utilisées dans le Guide de déploiement virtuel	6
Hôtes virtuels pris en charge	7
Supports d'installation	8
Recommandations en matière d'environnement virtuel	8
Configuration matérielle recommandée pour l'hôte virtuel	9
Scénario un	9
Scénario deux	10
Troisième scénario	13
Log Collector (local et distant)	14
Instructions de dimensionnement pour les collecteurs Windows d'ancienne génération ...	14
Installer l'hôte virtuel NetWitness Suite dans l'environnement virtuel	15
Conditions préalables	15
Étape 1. Déployer l'hôte virtuel	15
Conditions préalables	15
Procédure	15
Étape 2. Configurer le réseau et installer RSA NetWitness	19
Conditions préalables	19
Procédure	19
Vérifier les ports de pare-feu ouverts	19
Tâches d'installation	19
Étape 3. Configurer les bases de données pour prendre en charge NetWitness Suite	35
Tâche 1. Passer en revue la configuration initiale du magasin de données	36
Espace initiale alloué à PacketDB	36
Taille de la base de données (initiale)	36
Point de montage PacketDB	37
Tâche 2. Examinez la Configuration optimale d'espace du Datastore	38
Rapports d'espace disque virtuel	38

Tâche 3. Ajouter un nouveau volume et étendre les systèmes de fichiers existants	40
Créer un volume physique LVM sur la nouvelle partition	47
Étape 4. Configurer les paramètres spécifiques de l'hôte	52
Configurer la réception de log dans l'environnement virtuel	52
Configurer la capture de paquet dans l'environnement virtuel	53
Utiliser une interface TAP virtuelle tierce	53

Guide de configuration de l'hôte virtuel

Ce document fournit des instructions sur l'installation et la configuration des hôtes RSA NetWitness® Suite s'exécutant dans un environnement virtuel.

Déploiement virtuel de base

Cette rubrique fournit des instructions et des exigences générales en matière de déploiement de RSANetWitness Suite11.0.0.0 dans un environnement virtuel.

Abréviations utilisées dans le Guide de déploiement virtuel

Abréviations	Description
CPU	Unité centrale
EPS	Événements par seconde
VMware ESX	Hyperviseur de type 1 de classe entreprise, versions prises en charge : 6.5, 6.0 et 5.5
Go	Gigaoctet. 1 Go = 1 000 000 000 octets
Gb	Gigabit. 1 Go = 1 000 000 000 bits
Gbit/s	Gigabits par seconde ou milliards de bits par seconde. Cette unité mesure la bande passante sur un support de transmission des données numériques, comme la fibre optique.
GHz	GigaHertz 1 GHz = 1 000 000 000 Hz
E/S par seconde	Entrées/sorties par seconde
Mbit/s	En mégabits par seconde, ou des millions de bits par seconde. Cette unité mesure la bande passante sur un support de transmission des données numériques, comme la fibre optique.
NAS	NAS (Network Attached Storage)
OVF	Open Virtualization Format
OVA	Open Virtual Appliance. Dans ce guide, OVA signifie Hôte virtuel ouvert (Open Virtual Host).
RAM	Random Access Memory (également nommé mémoire)

Abréviations	Description
SAN	Storage Area Network
SSD/EFD HDD	Disque SSD/disque Flash d'entreprise
SCSI	Small Computer System Interface
SCSI (SAS)	Protocole de série de point à point qui déplace les données vers et depuis les périphériques de stockage tels que les disques durs et les lecteurs de bande.
CPU virtuels	Unité de traitement central virtuelle (également nommée processeur virtuel)
vRAM	Virtual Random Access Memory (également nommé mémoire virtuelle)

Hôtes virtuels pris en charge

Vous pouvez installer les hôtes NetWitness Suite suivants dans votre environnement virtuel sous forme d'hôtes virtuels et hériter de fonctionnalités fournies par votre environnement virtuel :

- Serveur NetWitness
- Event Stream Analysis : ESA primaire et secondaire
- Archiver
- Broker
- Concentrator
- Log Decoder
- Malware Analysis
- Decoder
- Remote Log Collector

Vous devez être familiarisé avec les concepts d'infrastructure VMware suivants :

- VMware vCenter Server
- VMware ESXi
- Machine virtuelle

Pour plus d'informations sur les concepts VMware, reportez-vous à la documentation produit VMware.

Les hôtes virtuels sont fournis sous la forme de fichiers OVA. Vous devez déployer le fichier OVA en tant que machine virtuelle dans votre infrastructure virtuelle.

Supports d'installation

Les supports d'installation se présentent sous la forme de packages OVA , qui peuvent être téléchargés et installés à partir de Download Central (<https://download.rsasecurity.com>). Dans le cadre de votre commande, RSA vous donne accès au modèle OVA.

Recommandations en matière d'environnement virtuel

Les hôtes virtuels installés avec les packages OVA ont les mêmes fonctionnalités que les hôtes matériels NetWitness Suite. Cela signifie que lorsque vous mettez en œuvre des hôtes virtuels, vous devez tenir compte du matériel back-end. RSA vous conseille d'effectuer les tâches suivantes lorsque vous configurez votre environnement virtuel.

- En fonction des besoins en ressources des différents composants, suivez les bonnes pratiques pour utiliser le système et le stockage dédié de manière appropriée.
- Assurez-vous que les configurations de disques back-end fournissent une vitesse d'écriture de 10 % supérieure à la capture soutenue requise et au taux de réception pour le déploiement.
- Pour le fichier OVA, 32 Go de RAM par appliance hôte sont requis.
- Créez des répertoires Concentrator pour les bases de métadonnées et les bases de données d'index SSD/EFD HDD.
- Si les composants de base de données sont séparés des composants du système d'exploitation (OS) installé (autrement dit, sur un système physique séparé), fournissez une connectivité directe de l'une des façons suivantes :
 - Deux ports SAN Fibre Channel de 8 Gbit/s par hôte virtuel,
ou
 - une connectivité d'interface SAS (Serial Attached SCSI) de 6 Gbit/s

Remarque : 1.) Actuellement, NetWitness Suite ne prend pas en charge le NAS (Network Attached Storage) pour les déploiements virtuels.
2.) Le Decoder accepte toutes les configurations de stockage pouvant satisfaire les besoins en débit soutenu. La liaison Fibre Channel 8 Gbit/s standard à un SAN est insuffisante pour lire et écrire des données de paquets à 10 Gbit/s. Vous devez utiliser plusieurs canaux Fibre Channel lors de la configuration avec la connexion d'un **Decoder 10G** vers le SAN.

Configuration matérielle recommandée pour l'hôte virtuel

Les tableaux suivants répertorient la configuration matérielle recommandée pour les éléments vCPU, vRAM et IOPS en lecture et en écriture pour les hôtes virtuels selon l'EPS ou le taux de capture de chaque composant.

- L'allocation du stockage est décrite dans l'étape 3, « Configurer des bases de données selon la suite NetWitness Suite ».
- Les recommandations vRAM et CPU peuvent varier en fonction des taux de capture, de la configuration et du contenu activé.
- Les recommandations ont été testées à des taux de réception allant jusqu'à 25 000 EPS pour les logs et deux Gbit/s pour les paquets, sans SSL.
- Les caractéristiques de CPU virtuel pour tous les composants répertoriés dans les tableaux suivants sont
CPU Intel Xeon à 2,59 GHz.
- Tous les ports sont testés SSL à 15 000 EPS pour les logs et 1,5 Gbit/s pour les paquets.

Remarque : Les valeurs recommandées ci-dessus peuvent être différentes pour une installation 11.0.0.0 lorsque vous installez les nouvelles fonctionnalités et améliorations.

Scénario un

Les exigences décrites dans ces tableaux ont été calculées dans les conditions indiquées ci-dessous.

- Tous les composants ont été intégrés.
- Le flux de log comprenait un Log Decoder, un Concentrator et un Archiver.
- Le flux de paquets comprenait un Packet Decoder et un Concentrator.
- La charge en arrière-plan comprenait des rapports horaires et journaliers.
- Les graphiques étaient configurés.

Log Decoder

EPS	CPU	Mémoire	IOPS en lecture	IOPS en écriture
2 500	6 ou 15,60 GHz	32 Go	50	75
5 000	8 ou 20,79 GHz	32 Go	100	100
7 500	10 ou 25,99 GHz	32 Go	150	150

Packet Decoder

Mbit/s	CPU	Mémoire	IOPS en lecture	IOPS en écriture
50	4 ou 10,39 GHz	32 Go	50	150
100	4 ou 10,39 GHz	32 Go	50	250
250	4 ou 10,39 GHz	32 Go	50	350

Concentrator - Flux de log

EPS	CPU	Mémoire	IOPS en lecture	IOPS en écriture
2 500	4 ou 10,39 GHz	32 Go	300	1 800
5 000	4 ou 10,39 GHz	32 Go	400	2 350
7 500	6 ou 15,59 GHz	32 Go	500	4 500

Concentrator - Flux de paquets

Mbit/s	CPU	Mémoire	IOPS en lecture	IOPS en écriture
50	4 ou 10,39 GHz	32 Go	50	1 350
100	4 ou 10,39 GHz	32 Go	100	1 700
250	4 ou 10,39 GHz	32 Go	150	2 100

Achiver

EPS	CPU	Mémoire	IOPS en lecture	IOPS en écriture
2 500	4 ou 10,39 GHz	32 Go	150	250
5 000	4 ou 10,39 GHz	32 Go	150	250
7 500	6 ou 15,59 GHz	32 Go	150	350

Scénario deux

Les exigences décrites dans ces tableaux ont été calculées dans les conditions indiquées ci-dessous.

- Tous les composants ont été intégrés.
- Le flux de log comprenait un Log Decoder, un Concentrator, un Warehouse Connector et un Archiver.
- Le flux de paquets comprenait un Packet Decoder, un Concentrator et un Warehouse Connector.
- Event Stream Analysis agrégeait à 90 000 EPS, à partir de trois Concentrators Hybrid.
- Incident Management recevait des alertes de Reporting Engine et d'Event Stream Analysis.
- La charge en arrière-plan comprenait des rapports, des graphiques, des alertes, des procédures d'enquête et la gestion des incidents.
- Les alertes étaient configurées.

Log Decoder

EPS	CPU	Mémoire	IOPS en lecture	IOPS en écriture
10 000	16 ou 41,58 GHz	50 Go	300	50
15 000	20 ou 51,98 GHz	60 Go	550	100

Packet Decoder

Mbit/s	CPU	Mémoire	IOPS en lecture	IOPS en écriture
500	8 ou 20,79 GHz	40 Go	150	200
1 000	12 or 31,18 GHz	50 Go	200	400
1 500	16 ou 41,58 GHz	75 Go	200	500

Concentrator - Flux de log

EPS	CPU	Mémoire	IOPS en lecture	IOPS en écriture
10 000	10 ou 25,99 GHz	50 Go	1 550 + 50	6 500
15 000	12 or 31,18 GHz	60 Go	1 200 + 400	7 600

Concentrator - Flux de paquets

Mbit/s	CPU	Mémoire	IOPS en lecture	IOPS en écriture
500	12 or 31,18 GHz	50 Go	250	4 600
1 000	16 ou 41,58 GHz	50 Go	550	5 500
1 500	24 or 62,38 GHz	75 Go	1 050	6 500

Warehouse Connector - Flux de log

EPS	CPU	Mémoire	IOPS en lecture	IOPS en écriture
10 000	8 ou 20,79 GHz	30 Go	50	50
15 000	10 ou 25,99 GHz	35 Go	50	50

Warehouse Connector - Flux de paquets

Mbit/s	CPU	Mémoire	IOPS en lecture	IOPS en écriture
500	6 ou 15,59 GHz	32 Go	50	50
1 000	6 ou 15,59 GHz	32 Go	50	50
1 500	8 ou 20,79 GHz	40 Go	50	50

Archiver - Flux de log

EPS	CPU	Mémoire	IOPS en lecture	IOPS en écriture
10 000	12 or 31,18 GHz	40 Go	1 300	700
15 000	14 ou 36,38 GHz	45 Go	1 200	900

Event Stream Analysis (ESA) avec Context Hub

EPS	CPU	Mémoire	IOPS en lecture	IOPS en écriture
90 000	32 ou 83,16 GHz	94 Go	50	50

Serveur NetWitness et composants co-implantés

Serveur NetWitness, Jetty, Broker, Incident Management et Reporting Engine sont dans le même emplacement.

CPU	Mémoire	IOPS en lecture	IOPS en écriture
12 or 31,18 GHz	50 Go	100	350

Troisième scénario

Les exigences décrites dans ces tableaux ont été calculées dans les conditions indiquées ci-dessous.

- Tous les composants ont été intégrés.
- Le flux de log comprenait un Log Decoder et un Concentrator.
- Le flux de paquets comprenait un Packet Decoder et un Concentrator.
- Event Stream Analysis agrégeait à 90 000 EPS, à partir de trois Concentrators Hybrid.
- Incident Management recevait des alertes de Reporting Engine et d'Event Stream Analysis.
- La charge en arrière-plan comprenait des rapports horaires et journaliers.
- Les graphiques étaient configurés.

Log Decoder

EPS	CPU	Mémoire	IOPS en lecture	IOPS en écriture
25 000	32 ou 83,16 GHz	75 Go	250	150

Packet Decoder

Mbit/s	CPU	Mémoire	IOPS en lecture	IOPS en écriture
2 000	16 ou 41,58 GHz	75 Go	50	650

Concentrator - Flux de log

EPS	CPU	Mémoire	IOPS en lecture	IOPS en écriture
25 000	16 ou 41,58 GHz	75 Go	650	9 200

Concentrator - Flux de paquets

Mbit/s	CPU	Mémoire	IOPS en lecture	IOPS en écriture
2 000	24 or 62,38 GHz	75 Go	150	7 050

Log Collector (local et distant)

Le Remote Log Collector est un service Log Collector qui s'exécute sur un hôte distant et le Remote Collector est déployé virtuellement.

EPS	CPU	Mémoire	IOPS en lecture	IOPS en écriture
15 000	8 ou 20,79 GHz	8 Go	50	50
30 000	8 ou 20,79 GHz	15 Go	100	100

Instructions de dimensionnement pour les collecteurs Windows d'ancienne génération

Reportez-vous à *RSA NetWitness Suite Legacy Windows Collection Update & Installation* pour prendre connaissance des recommandations de dimensionnement pour le collecteur Windows d'ancienne génération.

Installer l'hôte virtuel NetWitness Suite dans l'environnement virtuel

Exécutez les procédures suivantes dans leur ordre numérotée pour installer RSA NetWitness® Suite dans un environnement virtuel.

Conditions préalables

Assurez-vous d'avoir :

- un serveur VMware ESX satisfaisant aux exigences décrites dans la rubrique ci-dessus. Les versions prises en charge sont 6.5, 6.0 et 5.5.
- vSphere 4.1 Client ou vSphere 5.0 Client installé pour se connecter au serveur VMware ESX.
- des droits d'administrateur pour créer les machines virtuelles sur le serveur VMware ESX.

Étape 1. Déployer l'hôte virtuel

Effectuez les étapes suivantes pour déployer le fichier OVA sur vCenter Server ou ESX Server à l'aide du client vSphere.

Conditions préalables

Assurez-vous d'avoir :

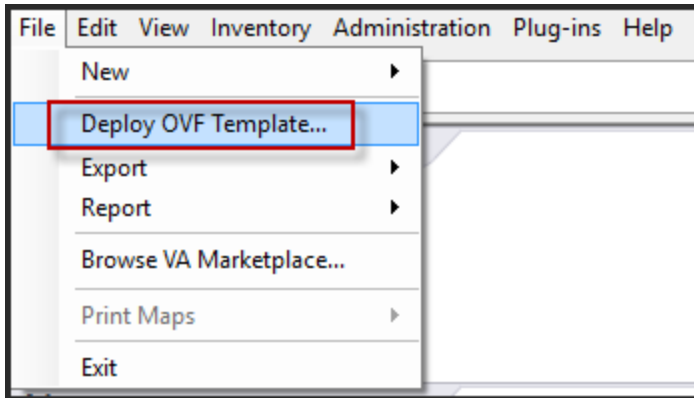
- Adresses IP réseau, masque de réseau et adresses IP de passerelle pour l'hôte virtuel.
- Noms réseau de tous les hôtes virtuels, si vous créez un cluster.
- Informations DNS ou hôte
- Mot de passe pour l'accès à l'hôte virtuel. Par défaut, le nom d'utilisateur est `root` et le mot de passe par défaut est `netwitness`.
- Le fichier de package de l'hôte virtuel NetWitness Suite. (Vous pouvez télécharger ce package à partir de Download Central [<https://community.rsa.com>].)

Procédure

Remarque : Les instructions suivantes illustrent un exemple de déploiement d'un hôte OVA dans l'environnement VMware ESXi. Les écrans que vous voyez peuvent être différents à partir de cet exemple.

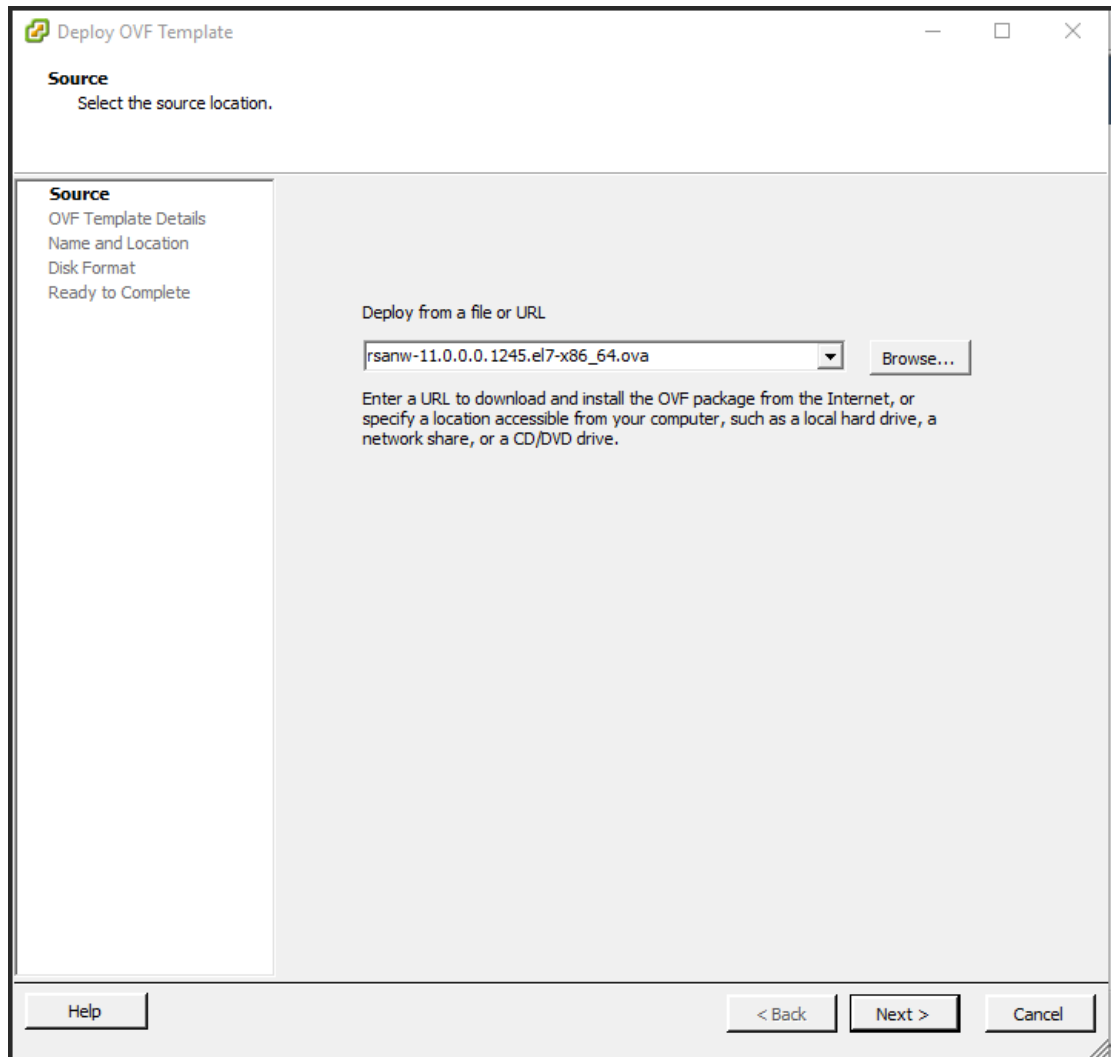
Pour déployer l'hôte OVA :

1. Connectez-vous à l'environnement ESXi.
2. Dans la liste déroulante **Fichier**, sélectionnez **Déployer le modèle OVF**.

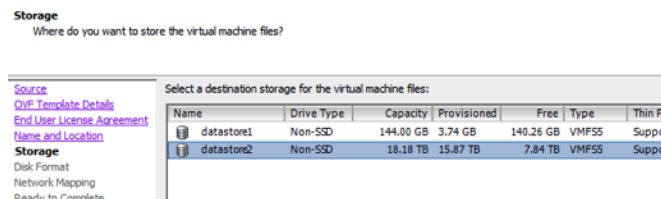


3. La boîte de dialogue Déployer le modèle OVF s'affiche. Dans la boîte de dialogue **Déployer le modèle OVF**, sélectionnez l'OVF pour l'hôte que vous souhaitez déployer dans l'environnement virtuel (par exemple, **V11.0 GOLD\OVFImge\v11_SA_OVF\nwreux_**

OVF11.ovf), puis cliquez sur **Suivant**.



4. La boîte de dialogue Nom et emplacement s'affiche. Le nom désigné ne reflète pas le nom d'hôte du serveur. Le nom affiché est utile pour la référence d'inventaire dans ESXi.
5. Notez le nom et cliquez sur **Suivant**.
Les Options de stockage s'affichent.

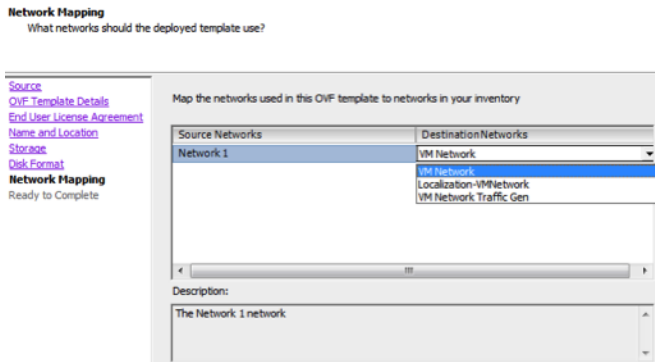


6. Pour les Options de stockage, désignez l'emplacement du datastore pour l'hôte virtuel.

Remarque : Cet emplacement est exclusivement pour le système d'exploitation hôte (OS). Il ne doit pas forcément s'agir du même datastore que celui nécessaire lors de l'installation et de la configuration de volumes supplémentaires pour les bases de données NetWitness Suite sur certains hôtes (abordés dans les rubriques suivantes).

7. Cliquez sur **Suivant**.

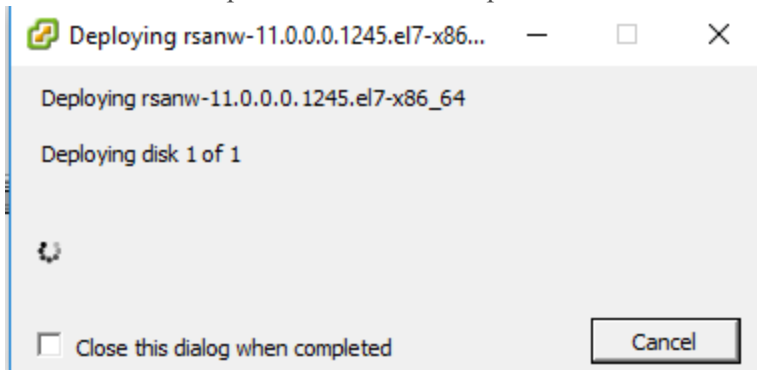
Les options Mappage de réseau s'affichent.



8. Conservez les valeurs par défaut et cliquez sur **Suivant**.

Remarque : Si vous souhaitez configurer le mappage de réseau, vous pouvez sélectionner ici des options, mais RSA vous recommande de conserver les valeurs par défaut et de réserver le mappage réseau pour la suite, lorsque l'OVA aura été configuré dans [Étape 4 : Configurer les paramètres spécifiques de l'hôte](#).

Une fenêtre d'état présentant l'état du déploiement s'affiche.



Une fois le processus terminé, le nouvel OVA est présenté dans le pool de ressources désigné, visible sur ESXi dans vSphere. L'hôte virtuel principal est alors installé, mais il n'est pas encore configuré.

Étape 2. Configurer le réseau et installer RSA NetWitness

Effectuez les étapes suivantes pour configurer le réseau de l'appliance virtuelle.

Conditions préalables

Assurez-vous d'avoir :

- Adresses IP réseau, masque de réseau et adresses IP de passerelle pour l'hôte virtuel.
- Noms réseau de tous les hôtes virtuels, si vous créez un cluster.
- Informations DNS ou hôte

Procédure

Suivez la procédure cidessous pour tous les hôtes virtuels afin de les récupérer sur votre réseau.

Vérifier les ports de pare-feu ouverts

consultez la rubrique *Architecture réseau et ports* dans le *Guide de déploiement* dans l'aide de NetWitness Suite pour pouvoir configurer les services NetWitness Suite et vos pare-feu.

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

Deux tâches principales sont à effectuer dans l'ordre indiqué pour installer NetWitness Suite 11.0.0.0

Tâches d'installation

Tâche 1 - Installation de la version 11.0.0.0 sur Serveur NetWitness (nœud 0)

Tâche 2 - Installation de la version 11.0.0.0 sur d'autres composants NetWitness Suite (nœud x)

Tâche 1 - Installation de la version 11.0.0.0 sur Serveur NetWitness (nœud 0)

Sur l'hôte que vous avez déployé pour le serveur NW (nœud 0), cette tâche installe :

- La plate-forme environnementale du serveur NW 11.0.0.0.
- Les composants du serveur NW (c'est-à-dire les services Admin, Config, Orchestration, Service Management et Security).
- Un référentiel contenant les fichiers RPM requis pour installer les autres composants ou services fonctionnels.

1. Déployez votre environnement 11.0.0.0 :
 - a. Provisionnez les hôtes.
 - b. Configurez le stockage.
 - c. Configurez les pare-feu.
2. Exécutez la commande `nwsetup-tui`. Cette opération démarre le programme d'installation 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 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 au serveur DNS après l'installation, ce dernier étant inaccessible pendant l'installation, (par exemple, pour déplacer un hôte après la configuration qui aurait un ensemble différent de serveurs DNS), reportez-vous à la rubrique [Tâche 1. Reconfigurer les serveurs DNS après l'installation de la version 11.0.0.0](#) dans les Tâches à effectuer après l'installation.

Si vous ne spécifiez pas de serveurs DNS pendant `nwsetup-tui`, vous devez sélectionner **1 Référentiel local (sur le serveur NW)** dans le message **NetWitness Suite** **Mettre à jour le 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

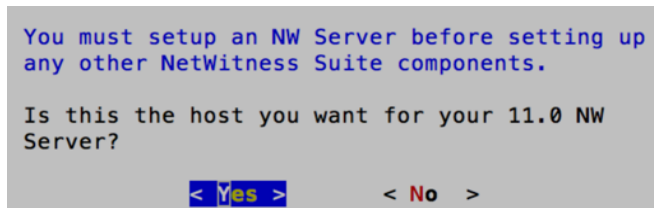
92%

<Accept >

<Decline>

3. Naviguez jusqu'à **Accepter** à l'aide de la touche Tabulation, puis appuyez sur Entrée.

Le message « S'agit-il du serveur NW ? » s'affiche.

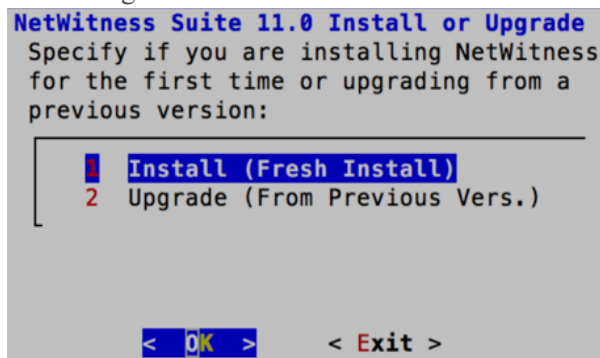


4. Naviguez jusqu'à **Oui** à l'aide de la touche Tabulation, puis appuyez sur Entrée.

Choisissez **Non** si vous avez déjà installé la version 11.0.0.0 sur le serveur NW.

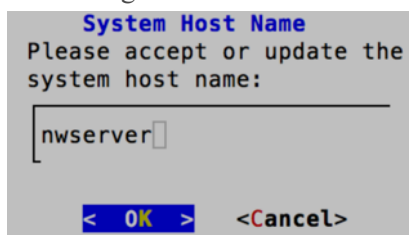
Attention : Si l'hôte choisi pour le serveur NW est incorrect et que vous terminez l'installation, vous devez redémarrer le programme d'installation (étape 3) et effectuer toutes les étapes suivantes pour corriger cette erreur.

Le message Installation ou Mise à niveau s'affiche.



5. Appuyez sur Entrée (Installation est sélectionnée par défaut).

Le message « Nom de l'hôte » s'affiche.



6. Appuyez sur Entrée si vous souhaitez conserver ce nom. Sinon, naviguez jusqu'à **OK** à l'aide de la touche Tabulation et appuyez sur Entrée pour modifier le nom de l'hôte.

Le message « Mot de passe maître » s'affiche.

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 { } [] () / \ ' " ` ~ , ; : . < > -).

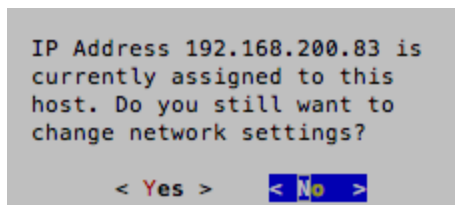
7. Cliquez sur la flèche vers le bas jusqu'à **Mot de passe** et saisissez-le, cliquez sur la flèche vers le bas jusqu'à **Vérifier** et saisissez à nouveau le mot de passe, naviguez jusqu'à **OK** à l'aide de la touche Tabulation et appuyez sur Entrée.

Le message « Mot de passe de déploiement » s'affiche.

8. Cliquez sur la flèche vers le bas jusqu'à **Mot de passe** et saisissez-le, cliquez sur la flèche vers le bas jusqu'à **Vérifier** et saisissez à nouveau le mot de passe, naviguez jusqu'à **OK** à l'aide de la touche Tabulation et appuyez sur Entrée.

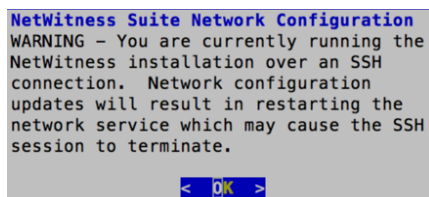
Invites conditionnelles :

- 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 évitez de modifier les paramètres réseau. Naviguez jusqu'à **Oui** à l'aide de la touche Tabulation et appuyez sur Entrée si vous souhaitez modifier la configuration IP disponible sur l'hôte.

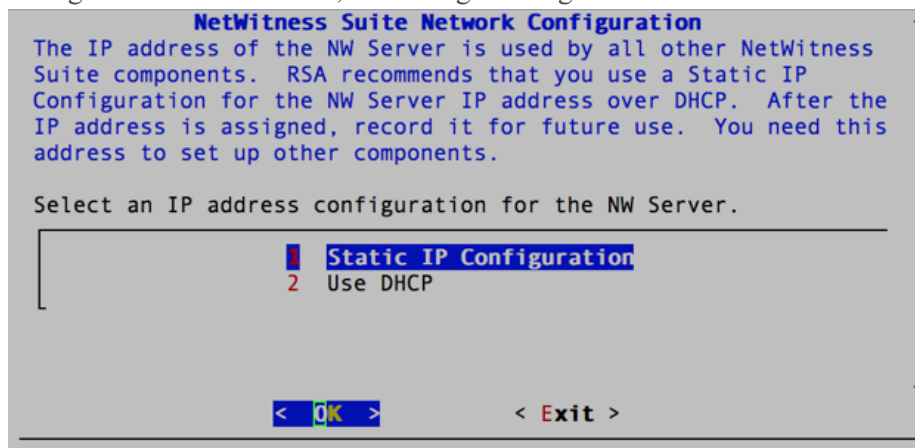
- Si vous utilisez une connexion SSH, l'avertissement suivant s'affiche.



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 à et terminez l'installation.

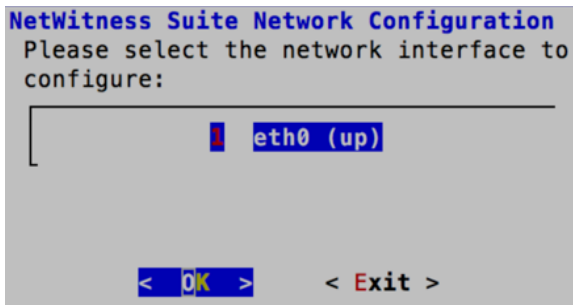
Si aucune configuration d'IP n'a été trouvée ou que vous avez choisi de modifier la configuration d'IP existante, le message Configuration réseau s'affiche.



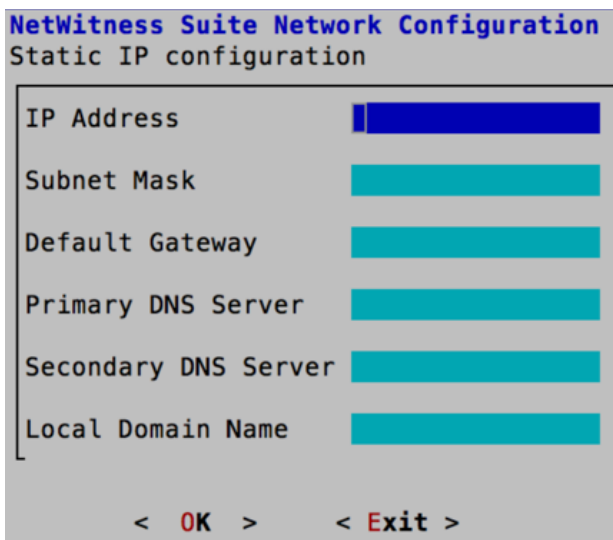
9. Naviguez jusqu'à **OK** à l'aide de la touche Tabulation et appuyez sur **Entrée** pour utiliser IP statique.

Si vous souhaitez utiliser **DHCP**, utilisez la touche directionnelle Bas jusqu'à 2 Utiliser DHCP et 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 Tabulation et appuyez sur Entrée. Si vous ne souhaitez pas continuer, naviguez jusqu'à **Exit** à l'aide de la touche Tabulation. Le message Configuration de l'adresse IP statique s'affiche.



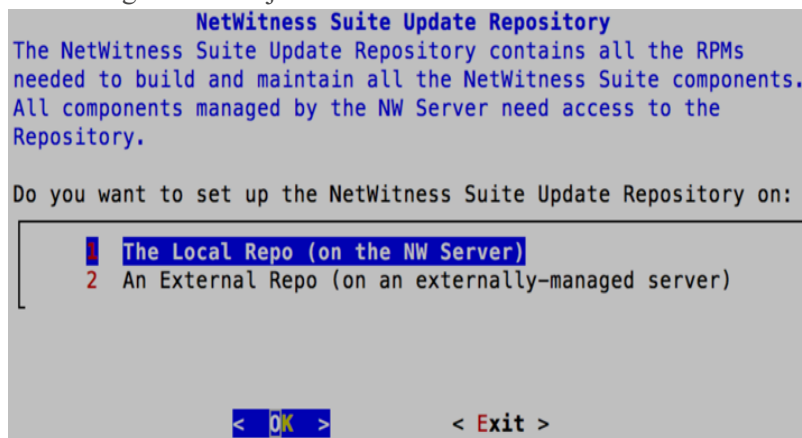
11. Saisissez les valeurs de configuration (en navigant d'un champ à l'autre à l'aide de la touche directionnelle Bas), naviguez jusqu'à **OK** à l'aide de la touche Tabulation et appuyez sur Entrée.

Si vous ne remplissez pas tous les champs obligatoires, le message d'erreur **Tous les champs sont obligatoires** s'affiche (les champs **serveur DNS primaire**, **serveur DNS secondaire**, et **nom de domaine Local** ne sont pas obligatoires).

Si la syntaxe ou la longueur de caractères utilisées pour un de ces champs sont incorrectes, le message d'erreur **Nom du champ non valide** 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 Mettre à jour le référentiel s'affiche.



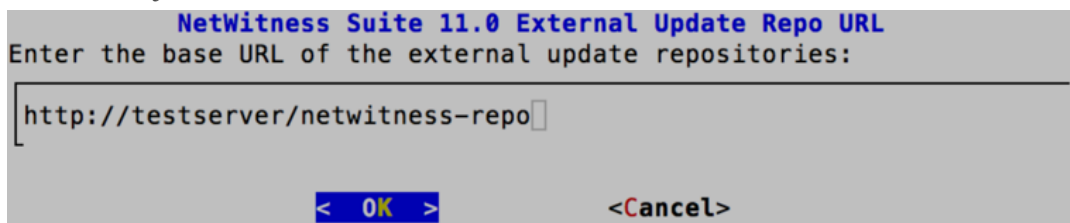
12. Appuyez sur Entrée pour choisir le **référentiel local** sur le serveur NW.

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 Tabulation et appuyez sur Entrée.

- Si vous sélectionnez **1 Le référentiel local (sur le serveur NW)**, le programme d'installation vérifie que le média approprié (c'est-à-dire une clé ou un DVD) est associé à l'hôte pour qu'il puisse l'utiliser pour récupérer l'installation ou mettre à jour les hôtes vers NetWitness Suite 11.0.0.0. Si le programme ne détecte pas le média connecté, le message d'erreur suivant s'affiche.

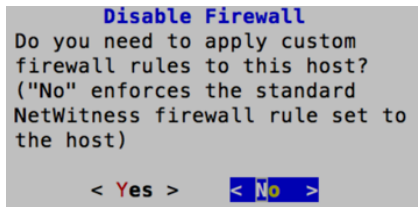


- Si vous sélectionnez **2 Un référentiel externe (sur un serveur géré en externe)**, l'interface utilisateur vous invite à saisir une URL. Les référentiels vous donnent accès aux mises à jour RSA et CentOS.



Saisissez l'URL de base du référentiel externe NetWitness Suite, puis cliquez sur **OK**. Le message Démarrer l'installation s'affiche.

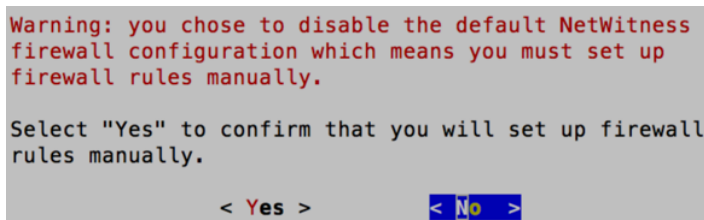
Le message Désactiver le pare-feu s'affiche.



13. Objectif

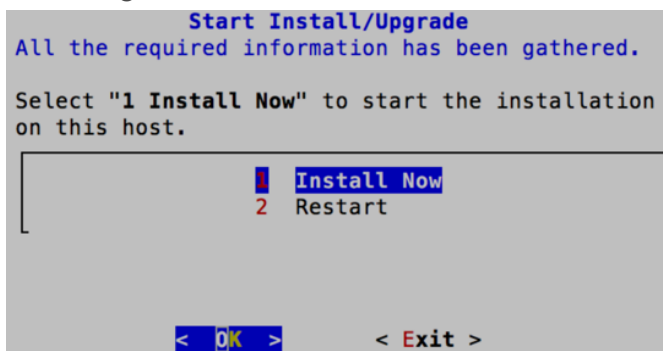
- Appliquer la configuration standard du pare-feu, appuyez sur Entrée.
- Désactivez la configuration standard, naviguez jusqu'à **Oui** à l'aide de la touche Tabulation et appuyez sur Entrée.

Le message de confirmation de la désactivation de la configuration du pare-feu s'affiche.



Naviguez jusqu'à **Oui** à l'aide de la touche Tabulation et appuyez sur Entrée pour confirmer (appuyez sur Entrée pour utiliser la configuration standard du pare-feu).

Le message Démarrer l'installation s'affiche.



14. Appuyez sur Entrée pour installer la version 11.0.0.0 sur le serveur NW.

Lorsque « Installation terminée » s'affiche, vous avez installé le serveur NW 11.0.0.0 sur cet hôte.

Tâche 2 - Installer la version 11.0 sur d'autres composants NetWitness Suite (nœud x)

Pour un hôte de service fonctionnel (nœud x), cette tâche :

- Installe la plate-forme environnementale 11.0.0.0.
 - Applique les fichiers RPM 1 au service à partir du référentiel de mise à jour du serveur NW.
1. Connectez la clé de version à l'hôte.
Pour savoir comment procéder pour créer une clé de version, reportez-vous à « Clé de version RSA NetWitness® Suite ».
 2. Installez CentOS7 comme système d'exploitation (OS) d'hôte.
Pour plus d'instructions, reportez-vous à la rubrique [Annexe A. Installer CentOS7 sur l'hôte](#).
 3. Exécutez la commande `nwsetup-tui` pour configurer l'hôte.
Cette opération démarre le programme d'installation 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 au serveur DNS après l'installation, ce dernier étant inaccessible pendant l'installation, (par exemple, pour déplacer un hôte après la configuration qui a un ensemble différent de serveurs DNS), reportez-vous à la rubrique [Reconfigurer les serveurs DNS après la mise à niveau 11.0.0.0](#).

Si vous ne spécifiez pas de serveurs DNS pendant `nwsetup-tui`, vous devez sélectionner **1 Référentiel local (sur le serveur NW)** dans le message **NetWitness Suite Mettre 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

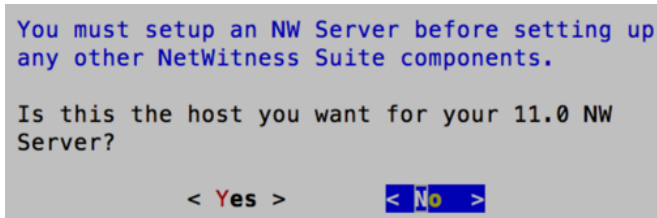
92%

<Accept >

<Decline>

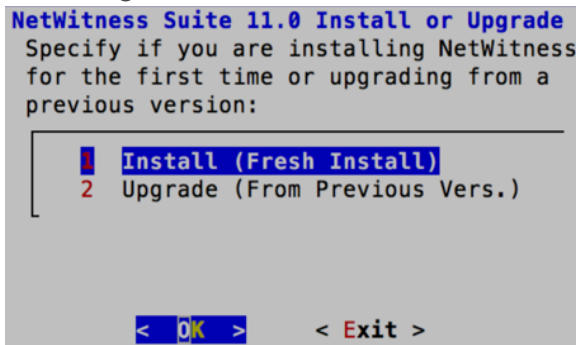
4. Naviguez jusqu'à **Accepter** à l'aide de la touche Tabulation, puis appuyez sur Entrée.

Le message « S'agit-il du serveur NW ? » s'affiche.



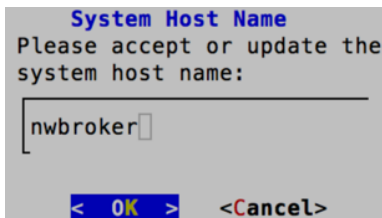
5. Appuyez sur Entrée (Non).

Le message Installation ou Mise à niveau s'affiche.



6. Appuyez sur Entrée (Installation est sélectionnée par défaut).

Le message « Nom de l'hôte » s'affiche.

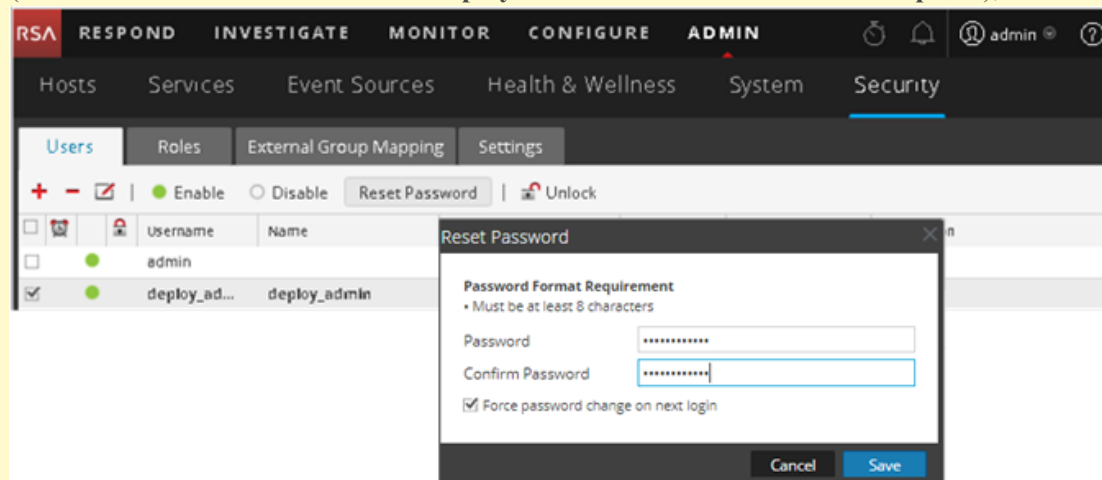


7. Appuyez sur Entrée si vous souhaitez conserver ce nom. Sinon, naviguez jusqu'à **OK** à l'aide de la touche Tabulation et appuyez sur Entrée pour modifier le nom de l'hôte.

Attention :

Scénario 1

Après avoir mis à niveau le serveur NW vers la version 11.0.0.0, si vous changez le mot de passe utilisateur **deploy_admin** dans l'interface utilisateur NetWitness Suite (ADMIN>Sécurité > sélectionner **deploy-admin - Réinitialiser le mot de passe**),



vous devez :

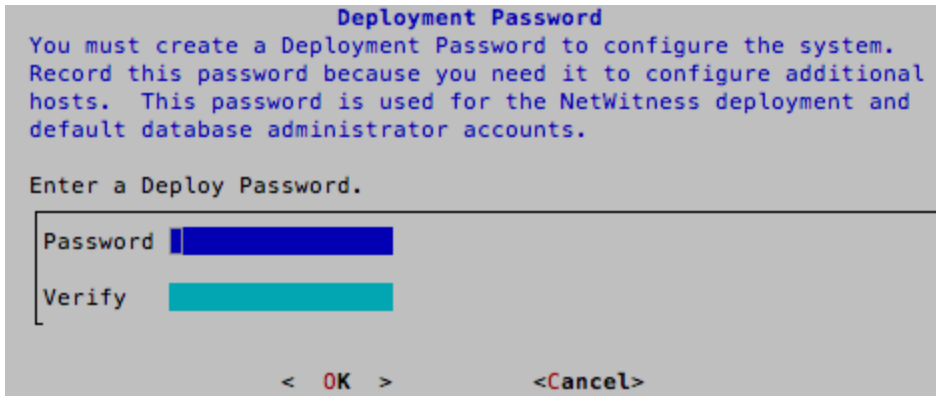
1. Ouvrir une session SSH sur l'hôte du serveur NW.
2. Exécuter le script (/opt/rsa/saTools/bin/set-deploy-admin-password.
3. Utiliser le nouveau mot de passe lors de la mise à niveau des nouveaux hôtes de serveur autre que NW.

Scénario 2

Après avoir mis à niveau le serveur NW et les hôtes de serveur autre que NW vers la version 11.0.0.0, si vous modifiez le mot de passe utilisateur **deploy_admin** dans l'interface utilisateur NetWitness Suite, vous devez :

1. Exécuter le script (/opt/rsa/saTools/bin/set-deploy-admin-password sur tous les hôtes de serveurs autre que NW dans votre déploiement.
2. Noter le mot de passe, car vous en aurez besoin plus tard dans l'installation.

Le message « Mot de passe de déploiement » s'affiche.

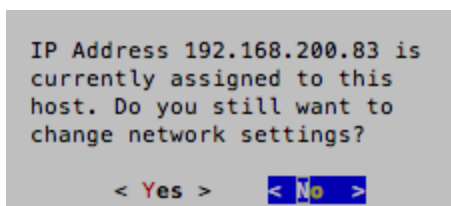


Remarque : Vous devez utiliser le même mot de passe de déploiement que vous avez utilisé lors de la mise à niveau du serveur NW.

8. Cliquez sur la flèche vers le bas jusqu'à **Mot de passe** et saisissez le mot de passe, cliquez sur la flèche vers le bas jusqu'à **Vérifier** et saisissez à nouveau le mot de passe, naviguez jusqu'à **OK** à l'aide de la touche Tabulation et appuyez sur Entrée.

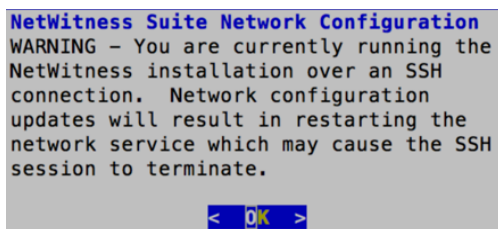
Invites conditionnelles :

- 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 évitez de modifier les paramètres réseau. Naviguez jusqu'à **Oui** à l'aide de la touche Tabulation et appuyez sur Entrée si vous souhaitez modifier la configuration IP disponible sur l'hôte.

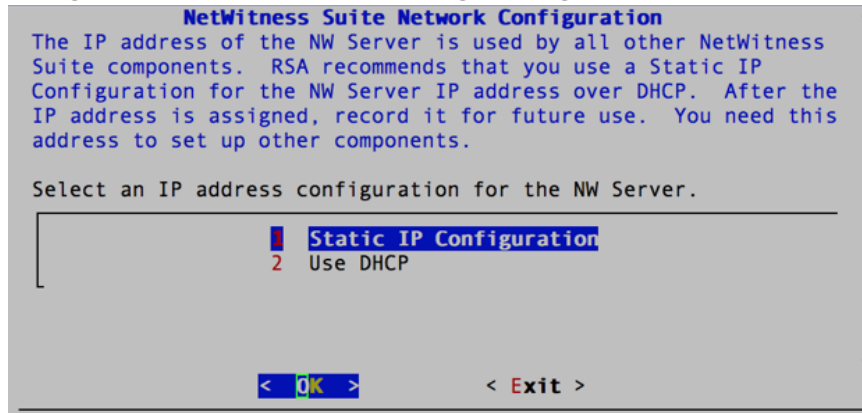
- Si vous utilisez une connexion SSH, l'avertissement suivant s'affiche.



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 à et terminez l'installation.

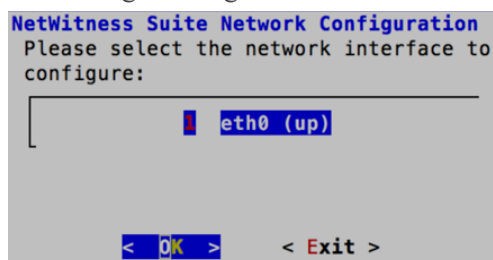
Si aucune configuration d'IP n'a été trouvée ou que vous avez choisi de modifier la configuration d'IP existante, le message Configuration réseau s'affiche.



9. Naviguez jusqu'à **OK** à l'aide de la touche Tabulation et appuyez sur Entrée pour utiliser IP statique.

Si vous souhaitez utiliser **DHCP**, utilisez la touche directionnelle Bas jusqu'à 2 Utiliser DHCP et 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 Tabulation et appuyez sur Entrée. Si vous ne souhaitez pas continuer, naviguez jusqu'à **Exit** à l'aide de la touche Tabulation. Le message Configuration de l'adresse IP statique

s'affiche.

NetWitness Suite Network Configuration
Static IP configuration

IP Address

Subnet Mask

Default Gateway

Primary DNS Server

Secondary DNS Server

Local Domain Name

< **OK** > < **Exit** >

11. Saisissez les valeurs de configuration (en navigant d'un champ à l'autre à l'aide de la touche directionnelle Bas), naviguez jusqu'à **OK** à l'aide de la touche Tabulation et appuyez sur Entrée.

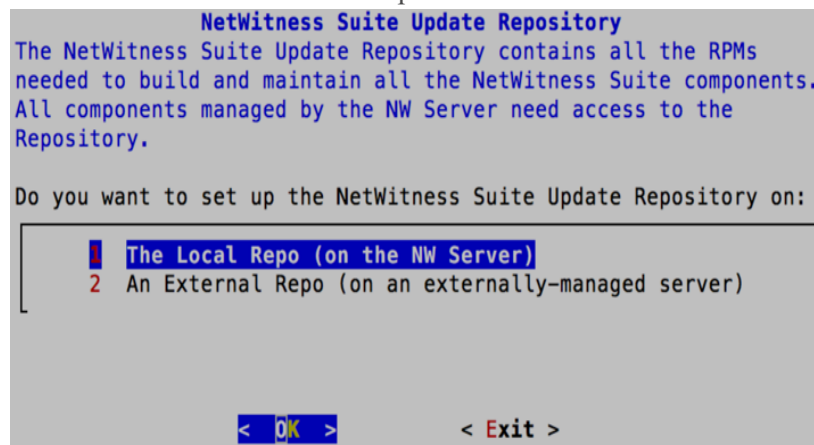
Si vous ne remplissez pas tous les champs obligatoires, le message d'erreur **Tous les champs sont obligatoires** s'affiche (les champs Serveur DNS primaire, serveur DNS secondaire et Nom de domaine local ne sont pas obligatoires).

Si la syntaxe ou la longueur de caractères utilisées pour un de ces champs sont incorrectes, le 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 Mettre à jour le référentiel s'affiche.

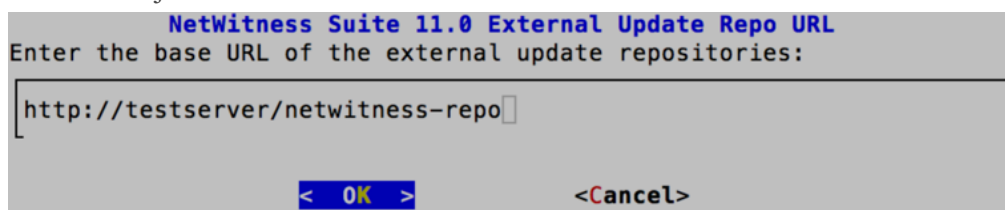
Sélectionnez le même référentiel que celui que vous avez sélectionné lors de la mise à niveau de l'hôte du serveur NW pour tous les hôtes.



12. Appuyez sur Entrée pour choisir le **Référentiel local** sur le serveur NW.

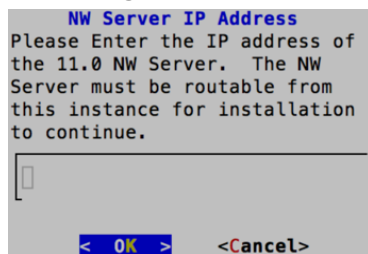
Si vous souhaitez utiliser un référentiel externe, utilisez la touche directionnelle Bas pour naviguer jusqu'au **Référentiel externe**, naviguez jusqu'à **OK** à l'aide de la touche Tabulation et appuyez sur Entrée.

- Si vous sélectionnez **1 Le référentiel local (sur le serveur NW)**, le programme d'installation vérifie que le média approprié (c'est-à-dire une clé ou un DVD) est associé à l'hôte pour qu'il puisse l'utiliser pour récupérer l'installation ou mettre à jour les hôtes vers NetWitness Suite 11.0.0.0.
- 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.



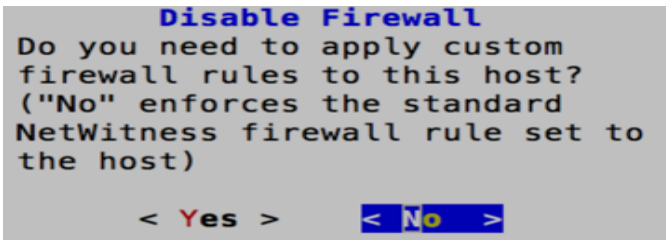
Saisissez l'URL de base du référentiel externe NetWitness Suite, puis cliquez sur **OK**.

Le message Adresse IP du serveur NW s'affiche.



13. Saisissez l'adresse IP du serveur NW. Naviguez jusqu'à **OK** à l'aide de la touche Tabulation, puis appuyez sur Entrée.

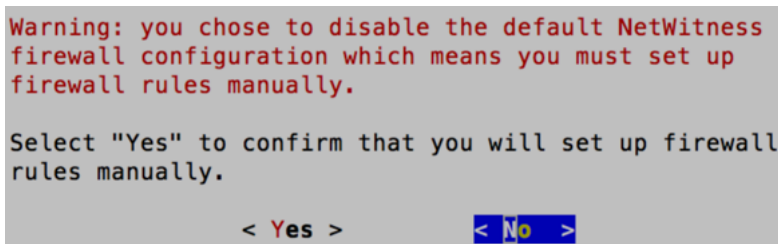
Le message Désactiver le pare-feu s'affiche.



14. Objectif

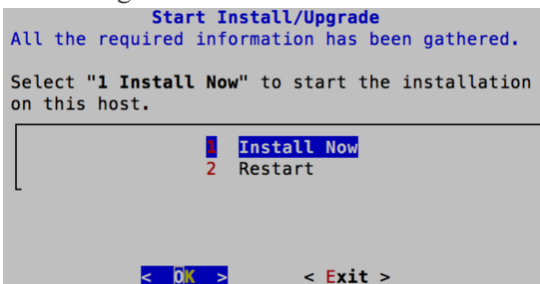
- Appliquer la configuration standard du pare-feu, appuyez sur Entrée.
- Désactivez la configuration standard, naviguez jusqu'à **Oui** à l'aide de la touche Tabulation et appuyez sur Entrée.

Le message de confirmation de la désactivation de la configuration du pare-feu s'affiche.



Naviguez jusqu'à **Oui** à l'aide de la touche Tabulation et appuyez sur Entrée pour confirmer (appuyez sur Entrée pour utiliser la configuration standard du pare-feu).



Le message Démarrer l'installation s'affiche.



15. Appuyez sur Entrée pour installer la version 11.0.0.0 sur le serveur NW. Lorsque « Installation terminée » s'affiche, vous disposez d'un hôte générique (noeud x) avec un système d'exploitation compatible avec NetWitness Suite 11.0.0.0.
16. Installez le service de composants sur l'hôte de nœud x.
- a. Cliquez sur **ADMIN > Hôtes**.

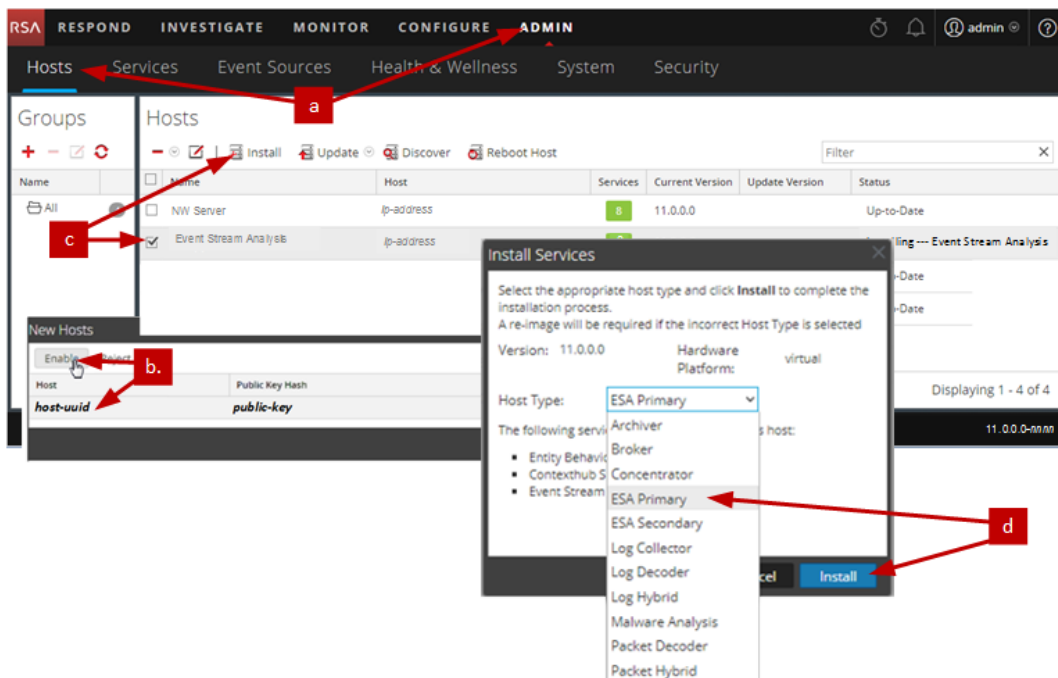
La boîte de dialogue **Nouveaux hôtes** s'affiche avec la vue **Hôtes** grisée en arrière-plan.

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

- b. Sélectionnez un hôte de serveur autre que NW dans la vue **Hôtes**.
- c. Cliquez sur 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**.
- d. Sélectionnez cet hôte (par exemple, **Event Stream Analysis**), puis cliquez sur  **Install** 

La boîte de dialogue **Services d'installation** s'affiche.

- e. Sélectionnez le service approprié (par exemple, **ESA primaire**), puis cliquez sur **Installer**.



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

17. Suivez les étapes 1 à 15 pour le reste des composants de serveur autre que NW NetWitness Suite.

Étape 3. Configurer les bases de données pour prendre en charge NetWitness Suite

Lorsque vous déployez des bases de données à partir de l'OVA, l'allocation d'espace initial de la base de données peut ne pas être suffisant pour prendre en charge Serveur NetWitness. Vous

devez examiner l'état des datastores après le déploiement initial et de les développer.

Tâche 1. Passer en revue la configuration initiale du magasin de données

Passez en revue la configuration du datastore après le déploiement initial afin de déterminer si vous disposez de suffisamment d'espace disque pour répondre aux besoins de votre entreprise. Par exemple, cette rubrique passe en revue la configuration du datastore de la PacketDB sur l'hôte Log Decoder après le déploiement à partir d'un fichier OVA (Open Virtualization Archive).

Espace initiale alloué à PacketDB

L'espace alloué pour la PacketDB est très faible (environ 98 Go). L'exemple de vue Explorer suivant de NetWitness Suite affiche la taille de la PacketDB après le déploiement initial à partir du fichier OVA.

Property	Value
hash.dir	
manifest.dir	
meta.compression	none
meta.compression.level	0
meta.dir	/var/netwitness/logdecoder/metadb=28.48 GB
meta.dir.cold	
meta.dir.warm	
meta.file.size	3 GB
meta.files	50
meta.free.space.min	267 MB
meta.index.fidelity	1
meta.integrity.flush	sync
meta.write.block.size	64 KB
packet.compression	none
packet.compression.level	0
packet.dir	/var/netwitness/logdecoder/packetdb=98.74DB

Taille de la base de données (initiale)

Par défaut, la taille de la base de données est définie à 95 % de la taille du système de fichiers sur lequel réside la base de données. Définissez le SSH sur l'hôte Log Decoder et saisissez la chaîne de commande `df -k` pour afficher le système de fichiers et sa taille. Le résultat suivant est un exemple des informations renvoyées par cette chaîne de cette commande.

```
[root@nwappliance32431 ~]# df -k
Filesystem            1K-blocks    Used Available Use% Mounted on
/dev/mapper/netwitness_vg00-root 31441920 3148972 28292948 11% /
devtmpfs              16462812     0 16462812  0% /dev
tmpfs                 16474132     12 16474120  1% /dev/shm
tmpfs                 16474132  41492 16432640  1% /run
tmpfs                 16474132     0 16474132  0% /sys/fs/cgroup
/dev/mapper/netwitness_vg00-usrhome 10475520  32984 10442536  1% /home
/dev/mapper/netwitness_vg00-varlog 10475520  72868 10402652  1% /var/log
/dev/mapper/netwitness_vg00-nwhome 146950036 399908 146550128  1% /var/netwitness
/dev/sda1             1038336    88448  949888  9% /boot
tmpfs                  3294828     0  3294828  0% /run/user/0
```

Point de montage PacketDB

La base de données est montée sur le volume logique `packetdb` dans le groupe de volumes `netwitness_vg00`. `netwitness_vg00` est l'emplacement dans lequel vous démarrez votre planification d'extension pour le système de fichiers.

État initial de `netwitness_vg00`

Pour passer en revue l'état de `netwitness_vg00`, procédez comme suit :

1. définissez le SSH sur l'hôte Log Decoder.
2. Saisissez la chaîne de commande `lvs` (affichage des volumes logiques) pour déterminer quels volumes logiques sont regroupés dans `netwitness_vg00`.

```
[root@nwappliance32431 ~]# lvs netwitness_vg00.
```

Le résultat suivant est un exemple des informations renvoyées par cette chaîne de cette commande.

```
[root@nwappliance32431 ~]# lvs netwitness_vg00
LV      VG          Attr      LSize   Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
nhome   netwitness_vg00 -wi-ao--- 140.21g
root    netwitness_vg00 -wi-ao--- 30.00g
swap    netwitness_vg00 -wi-ao--- 4.00g
usrhome netwitness_vg00 -wi-ao--- 10.00g
varlog  netwitness_vg00 -wi-ao--- 10.00g
```

3. Saisissez la chaîne de commande `pvs` (affichage des volumes physiques) pour déterminer quels volumes physiques appartiennent à un groupe spécifique.

```
[root@nwappliance32431 ~]# pvs
```

Le résultat suivant est un exemple des informations renvoyées par cette chaîne de cette commande.

```
[root@nwappliance32431 ~]# pvs
PV          VG          Fmt Attr PSize  PFree
/dev/sda2  netwitness_vg00 lvm2 a-- 194.31g 100.00m
```

4. Saisissez la chaîne de commande `vgs` (affichage des groupes de volumes) pour afficher la taille totale du groupe de volumes spécifique.

```
[root@nwappliance32431 ~]# vgs
```

Le résultat suivant est un exemple des informations renvoyées par cette chaîne de cette commande.

```
[root@nwappliance32431 ~]# vgs
VG          #PV #LV #SN Attr   VSize  VFree
netwitness_vg00 1  5  0 wz--n- 194.31g 100.00m
```

Tâche 2. Examinez la Configuration optimale d'espace du Datastore

Vous devez consulter les options de configuration de l'espace de datastore pour les différents hôtes obtenir des performances optimales de votre déploiement NetWitness Suite virtuel. Les datastores sont nécessaires pour la configuration de l'hôte virtuel, et taille appropriée dépend de l'hôte.

Remarque : (1.) Reportez-vous à la rubrique « **Techniques d'optimisation** » dans le [Guide d'optimisation de la base de données RSA NetWitness Suite Core](#) pour obtenir des recommandations sur l'optimisation de l'espace du datastore. (2.) Contactez l'assistance clientèle pour obtenir de l'aide dans la configuration de vos disques virtuels et l'utilisation de la Calculatrice de dimensionnement et de définition du périmètre.

Rapports d'espace disque virtuel

Le tableau suivant fournit des configurations optimales pour les hôtes de logs et de paquets. D'autres exemples de partitionnement et de dimensionnement pour les deux environnements, de capture de paquet et de réception de journal, sont fournis à la fin de cette rubrique.

Decoder			
Datastores persistants	Datastores de cache		
PacketDB	SessionDB	MetaDB	Index
100 % tel que calculé par la Calculatrice de dimensionnement et de définition du périmètre	6 Go par 100 Mb/s de trafic soutenu fournissent 4 heures de cache	60 Go par 100 Mb/s de trafic soutenu fournissent 4 heures de cache	3 Go par 100 Mb/s de trafic soutenu fournissent 4 heures de cache

Concentrator		
Datastores persistants	Datastores de cache	
MetaDB	SessionDB Index	Index

Concentrator		
Calculé comme 10% du PacketDB requis pour un taux de rétention de 1:1	30 Go par 1 To de PacketDB pour des déploiements réseau multi-protocole standard comme on peut le voir sur des passerelles Internet typiques	5 % de la valeur MetaDB sur le Concentrator. Préférence pour une grande vitesse de rotation ou SSD pour un accès rapide

Log Decoder			
Datastores persistants	Datastores de cache		
PacketDB	SessionDB	MetaDB	Index
100 % tel que calculé par la Calculatrice de dimensionnement et de définition du périmètre	1 Go par 1 000 EPS de trafic soutenu fournit 8 heures de cache	20 Go par 1 000 EPS de trafic soutenu fournit 8 heures de cache	0,5 Go par 1 000 EPS de trafic soutenu fournit 4 heures de cache

Log Concentrator		
Datastores persistants	Datastores de cache	
	SessionDB Index	Index
Calculé comme 100% du PacketDB requis pour un taux de rétention de 1:1	3 Go par 1 000 EPS de trafic soutenu par jour de rétention	5 % de la valeur MetaDB sur le Concentrator. Préférence pour une grande vitesse de rotation ou SSD pour un accès rapide

Tâche 3. Ajouter un nouveau volume et étendre les systèmes de fichiers existants

Après avoir vérifié la configuration initiale de votre datastore, vous pouvez décider d'ajouter un nouveau volume. Cette rubrique prend un hôte virtuel Packet/Log Decoder comme exemple.

Exécutez ces tâches dans l'ordre suivant.

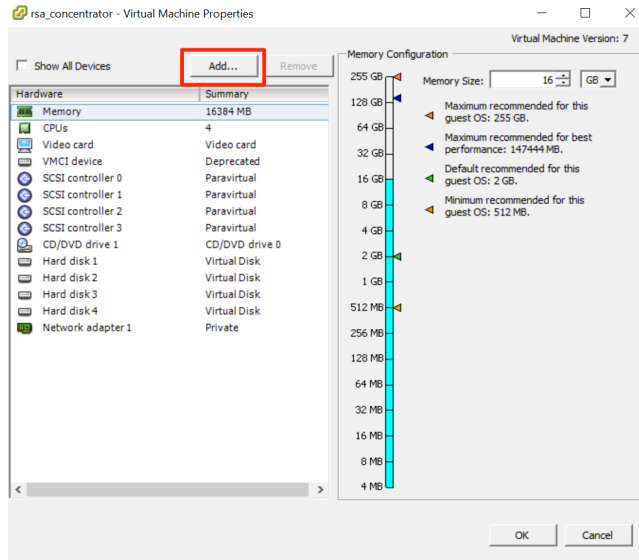
1. Ajouter un nouveau disque
2. Créer des volumes sur le nouveau disque
3. Créer un volume physique LVM sur la nouvelle partition
4. Étendre le groupe de volumes avec un volume physique
5. Étendre le système de fichiers
6. Démarrer les services
7. S'assurer que les services sont en cours d'exécution
8. Reconfigurer les paramètres de LogDecoder

Ajouter un nouveau disque

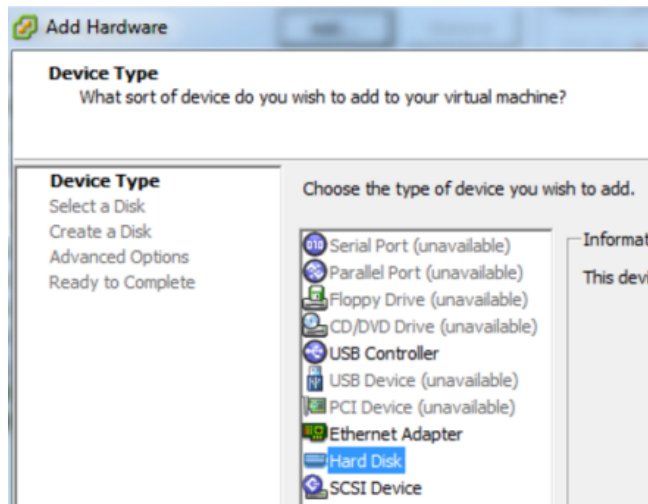
Cette procédure vous indique comment ajouter un nouveau disque de 100 Go dans le même datastore.

Remarque : La procédure à suivre pour ajouter un disque sur un datastore différent est similaire à la procédure indiquée ici.

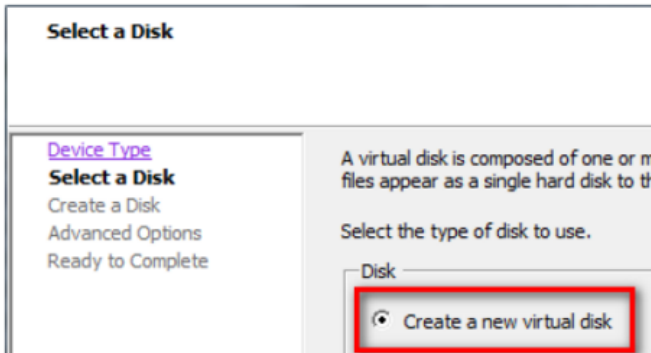
1. Arrêtez la machine, modifiez les **Propriétés de la machine virtuelle**, cliquez sur l'onglet **Matériel**, puis cliquez sur **Ajouter**.



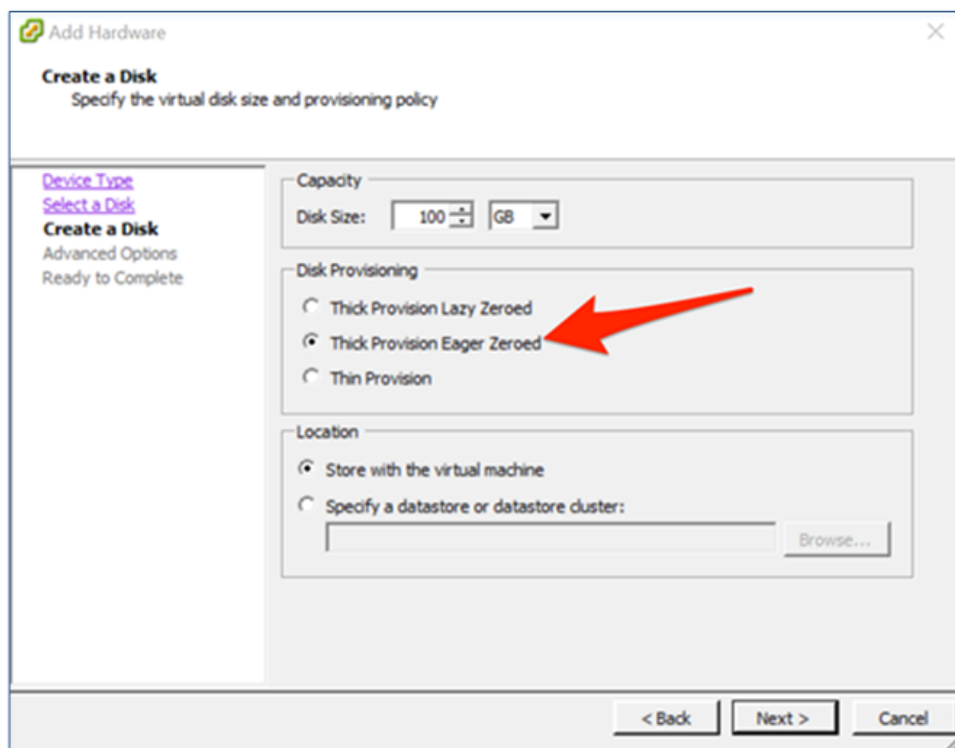
2. Dans la liste des types de périphérique, sélectionnez **Disque dur**.



3. Sélectionnez **Créer un nouveau disque virtuel**.

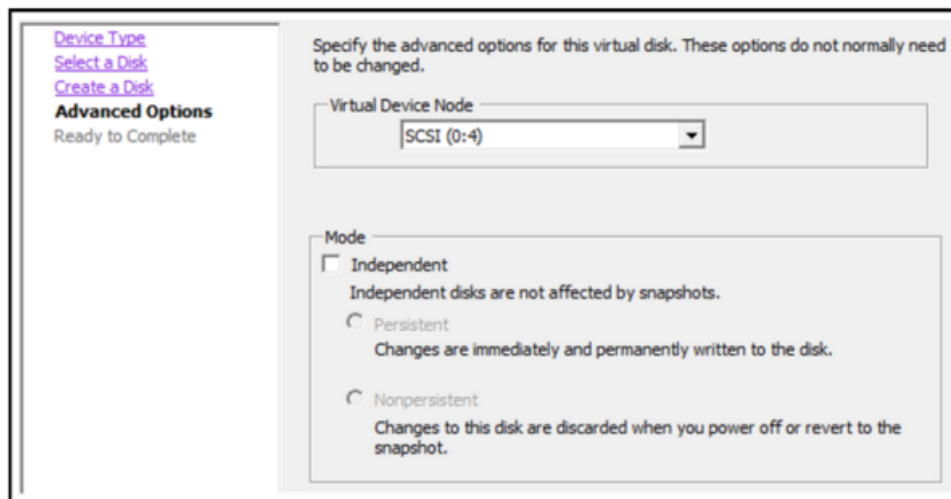


4. Choisissez la taille du nouveau disque et son emplacement (dans le même datastore ou un datastore différent).



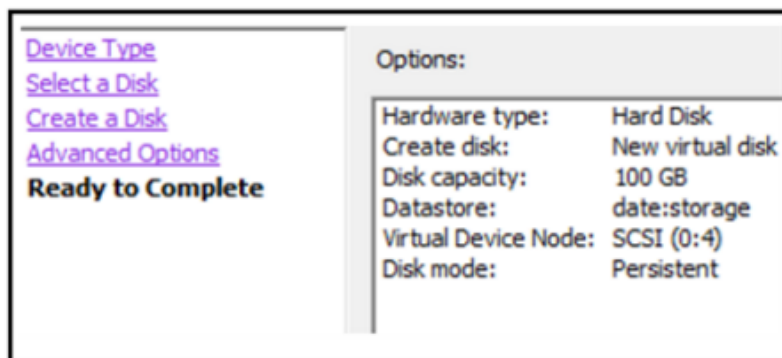
Attention : Pour des raisons de performances, allouez tout l'espace.

5. Approuvez le nœud de périphérique virtuel proposé.



Remarque : Le nœud de périphérique virtuel peut varier, mais il correspond aux mappages /dev/sdX.

6. Confirmez les paramètres.



7. Démarrez la machine virtuelle.
8. Ouvrez une session SSH sur la machine.
9. Redémarrez la machine et saisissez la commande suivante.

```
lsblk
```

Le résultat suivant s'affiche en indiquant le nouveau disque.

```
[root@NWAPPLIANCE2599 database]# lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
fd0                                  2:0      1    4K  0 disk
sda                                  8:0      0 195.3G  0 disk
├─sda1                               8:1      0     1G  0 part /boot
└─sda2                               8:2      0 194.3G  0 part
   ├─netwitness_vg00-nwhome          253:15   0 140.2G  0 lvm  /var/netwitness
   ├─netwitness_vg00-varlog          253:16   0    10G  0 lvm  /var/log
   ├─netwitness_vg00-usrhome          253:17   0    10G  0 lvm  /home
   ├─netwitness_vg00-root             253:18   0    30G  0 lvm  /
   └─netwitness_vg00-swap             253:19   0     4G  0 lvm  [SWAP]
sdb                                  8:16     0   48G  0 disk
├─sdb1                               8:17     0   48G  0 part
│   ├─VolGroup00-usr                 253:6    0     4G  0 lvm
│   ├─VolGroup00-usrhome              253:7    0     2G  0 lvm
│   ├─VolGroup00-var                   253:8    0     4G  0 lvm
│   ├─VolGroup00-log                   253:9    0     4G  0 lvm
│   ├─VolGroup00-tmp                   253:10   0     6G  0 lvm
│   ├─VolGroup00-vartmp                 253:11   0     2G  0 lvm
│   ├─VolGroup00-opt                   253:12   0     4G  0 lvm
│   ├─VolGroup00-rabmq                 253:13   0    10G  0 lvm
│   └─VolGroup00-nwhome                253:14   0    12G  0 lvm
sdc                                  8:32     0  104G  0 disk
├─sdc1                               8:33     0  104G  0 part
│   ├─VolGroup01-decoroot              253:0    0     20G  0 lvm  /var/netwitness/logdecoder
│   ├─VolGroup01-index                 253:1    0     10G  0 lvm  /var/netwitness/logdecoder/index
│   ├─VolGroup01-sessiondb             253:2    0     30G  0 lvm  /var/netwitness/logdecoder/sessiondb
│   └─VolGroup01-metadb                253:3    0    44G  0 lvm  /var/netwitness/logdecoder/metadb
sdd                                  8:48     0  168G  0 disk
├─sdd1                               8:49     0  168G  0 part
│   ├─VolGroup01-logcoll               253:4    0     64G  0 lvm  /var/netwitness/logcollector
│   └─VolGroup01-packetdb              253:5    0    104G  0 lvm  /var/netwitness/logdecoder/packetdb
sde                                  8:64     0    10G  0 disk
sr0                                  11:0     1 1024M  0 rom
[root@NWAPPLIANCE2599 database]#
```

Remarque : 1.) Vous obtenez l'erreur **unknown partition table** (table de partition inconnue) car le nouveau disque n'a pas été initialisé. 2.) **sd 2:0:4:0** se rapporte au nœud de périphérique virtuel **SCSI:0:4** qui s'est affiché lorsque vous avez ajouté le nouveau périphérique. 3.) Le nouveau périphérique de disque est **sde** (ou /dev/sde).

10. Saisissez la chaîne de commande suivante pour arrêter le service.

```
root@LogDecoderGM ~] # service nwlogcollector stop; service
nwlogdecoder stop.
```

Cette procédure utilise le Log Decoder en tant qu'exemple.

Si vous souhaitez arrêter les services sur un Concentrator, vous devez saisir :

```
service nwconcentrator stop
```

Si vous souhaitez arrêter les services sur un Packet Decoder, vous devez saisir :

```
service nwdecoder stop
```

Créer des volumes sur un nouveau disque

1. Ouvrez une session SSH sur l'hôte LogDecoder.
2. Créez une partition sur le nouveau disque et remplacez son type par Linux LVM.

```
[root@NWAPPLIANCE2599 ~]# fdisk /dev/sde
```

L'invite et les informations suivantes s'affichent :

```
[root@NWAPPLIANCE2599 database]# fdisk /dev/sde
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table
Building a new DOS disklabel with disk identifier 0x7cab96b5.

Command (m for help): _
```

3. Saisissez p.

Les informations suivantes s'affichent.

```
Command (m for help): p

Disk /dev/sde: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x2a0cf37b

   Device Boot      Start         End      Blocks   Id  System
Command (m for help):
```

Le type de partition par défaut est **Linux (83)**. Vous devez le remplacer par **Linux LVM (8e)**.

4. Saisissez n.

L'invite suivante s'affiche.

```
Command (m for help): n
Partition type:
   p   primary (0 primary, 0 extended, 4 free)
   e   extended
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048):
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-20971519, default 20971519):
Using default value 20971519
Partition 1 of type Linux and of size 10 GiB is set

Command (m for help): _
```

Partition 1 of type Linux and of size 10 GB is set

1. À l'invite `Command m for help:`, saisissez `t`.

L'invite et les informations suivantes s'affichent :

```
Command (m for help): t
Selected partition 1
Hex code (type L to list all codes): 8e
Changed type of partition 'Linux' to 'Linux LVM'

Command (m for help):
```

2. Saisissez `8e`.

L'invite et les informations suivantes s'affichent :

Changed system type of partition 1 to 8e (Linux LVM).

Command (m for help):

3. Saisissez `p`.

Les informations suivantes s'affichent.

```
Command (m for help): p

Disk /dev/sde: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x2a0cf37b

   Device Boot      Start         End      Blocks   Id  System
/dev/sde1          2048     20971519     10484736   8e  Linux LVM

Command (m for help):
```

4. À l'invite `Command (m for help):`, saisissez `w`.

La nouvelle table de partition est écrite sur le disque et `fdisk` ferme le shell `root`.

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
[ 9838.504920] sde: sde1
Syncing disks.
[root@NWAPPLIANCE2599 database]# _
```

La nouvelle partition `/dev/sde1` est créée sur le nouveau disque.

5. Effectuez l'une des étapes suivantes pour vérifier que la nouvelle partition existe.

- Saisissez `dmesg | tail`.

Les informations suivantes s'affichent.

```
[root@NWAPPLIANCE2599 database]# dmesg | tail
[ 773.090059] XFS (dm-2): Mounting U4 Filesystem
[ 773.214176] XFS (dm-2): Ending clean mount
[ 785.595678] XFS (dm-3): Mounting U4 Filesystem
[ 785.750078] XFS (dm-3): Ending clean mount
[ 802.874171] XFS (dm-4): Mounting U4 Filesystem
[ 803.020083] XFS (dm-4): Starting recovery (logdev: internal)
[ 803.041709] XFS (dm-4): Ending recovery (logdev: internal)
[ 813.249001] XFS (dm-5): Mounting U4 Filesystem
[ 813.439422] XFS (dm-5): Ending clean mount
[ 9838.504920] sde: sde1
[root@NWAPPLIANCE2599 database]#
```

- Saisissez `fdisk /dev/sde`
- Saisissez `p`

Les informations suivantes s'affichent.

```
[root@NWAPPLIANCE2599 database]# fdisk /dev/sde
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Command (m for help): p

Disk /dev/sde: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x2a0cf37b

   Device Boot      Start         End      Blocks    Id System
/dev/sde1                2048     20971519     10484736    8e  Linux LVM

Command (m for help): _
```

Créer un volume physique LVM sur la nouvelle partition

1. Ouvrez une session SSH sur l'hôte LogDecoder.
2. Saisissez la chaîne de commande suivante pour créer un LVM (Logical Volume Manager) sur la nouvelle partition.

```
[root@LogDecoderGM ~]# pvcreate /dev/sde1
```

3. Les informations suivantes s'affichent.

```
[root@NWAPPLIANCE2599 database]# pvcreate /dev/sde1
Physical volume "/dev/sde1" successfully created.
[root@NWAPPLIANCE2599 database]#
```

Étendre le groupe de volumes avec un volume physique

1. Ouvrez une session SSH sur l'hôte LogDecoder.
2. Saisissez la chaîne de commande suivante pour créer un LVM (Logical Volume Manager) sur la nouvelle partition.

```
[root@LogDecoderGM ~]# pvs
```

Les informations suivantes s'affichent.

```
[root@NWAPPLIANCE2599 database]# pvs
  PU          VG          Fmt Attr PSize  PFree
  /dev/sda2   netwitness_vg00  lvm2 a-- 194.31g 100.00m
  /dev/sdb1   VolGroup00       lvm2 a--  48.00g   0
  /dev/sdc1   VolGroup01       lvm2 a-- 104.00g   0
  /dev/sdd1   VolGroup01       lvm2 a-- 168.00g   0
  /dev/sde1                   lvm2 ---  10.00g  10.00g
[root@NWAPPLIANCE2599 database]#
```

netwitness_vg00 se compose des volumes physiques /dev/sdc1 et /dev/sdd1, et du système LVM. Notez que le nouveau volume /dev/sde1 dispose de 10 Go d'espace disponible.

3. Pour ajouter le volume physique à netwitness_vg00.
 - a. Saisissez `vgextend netwitness_vg00 /dev/sde1`.

Les informations suivantes s'affichent.

```
Volume group "netwitness_vg00" successfully extended
```

- b. Saisissez `pvs`.

Les informations suivantes s'affichent.

```
[root@NWAPPLIANCE2599 database]# vgextend netwitness_vg00 /dev/sde1
Volume group "netwitness_vg00" successfully extended
[root@NWAPPLIANCE2599 database]# pvs
  PU          VG          Fmt Attr PSize  PFree
  /dev/sda2   netwitness_vg00  lvm2 a-- 194.31g 100.00m
  /dev/sdb1   VolGroup00       lvm2 a--  48.00g   0
  /dev/sdc1   VolGroup01       lvm2 a-- 104.00g   0
  /dev/sdd1   VolGroup01       lvm2 a-- 168.00g   0
  /dev/sde1   netwitness_vg00  lvm2 a--  10.00g  10.00g
[root@NWAPPLIANCE2599 database]#
```

Le volume a été ajouté à netwitness_vg00, mais il n'a pas encore été étendu (vous disposez toujours de 10 Go d'espace libre). Il existe plusieurs volumes logiques dans netwitness_vg00 ; cet exemple utilise PacketDB.

4. Pour étendre le volume logique PacketDB afin qu'il utilise les 10 Go d'espace disponible.

a. Saisissez `lvs netwitness_vg00`.

Les informations suivantes s'affichent.

```
[root@NWAPPLIANCE2599 database]# lvs
LV      VG      Attr      LSize   Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
nwhome  netwitness_vg00 -wi-ao--- 140.21g
root    netwitness_vg00 -wi-ao--- 30.00g
swap    netwitness_vg00 -wi-ao---  4.00g
usrhome netwitness_vg00 -wi-ao--- 10.00g
varlog  netwitness_vg00 -wi-ao--- 10.00g
[root@LogDecoder ~]#
```

b. Saisissez `lvextend -L+9.5G /dev/netwitness_vg00/nwhome`.

Les informations suivantes s'affichent.

```
[root@NWAPPLIANCE2599 database]# lvextend -L+9.5G /dev/netwitness_vg00/nwhome
Size of logical volume netwitness_vg00/nwhome changed from 140.21 GiB (35894 extents) to 149.71 GiB (38326 extents).
Logical volume netwitness_vg00/nwhome successfully resized.
[root@NWAPPLIANCE2599 database]#
```

c. Saisissez `lvs netwitness_vg00`.

Les informations suivantes s'affichent.

```
[root@NWAPPLIANCE2599 database]# lvs netwitness_vg00
LV      VG      Attr      LSize   Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
nwhome  netwitness_vg00 -wi-ao--- 149.71g
root    netwitness_vg00 -wi-ao--- 30.00g
swap    netwitness_vg00 -wi-ao---  4.00g
usrhome netwitness_vg00 -wi-ao--- 10.00g
varlog  netwitness_vg00 -wi-ao--- 10.00g
[root@NWAPPLIANCE2599 database]#
```

The packetdb Logical Volume has been expanded to 149.71 GB, but the `/var/netwitness` filesystem still has 140.21 GB.

Étendre le système de fichiers

1. Ouvrez une session SSH sur l'hôte LogDecoder.
2. Saisissez la chaîne de commande suivante pour créer un LVM (Logical Volume Manager) sur la nouvelle partition.

```
[root@LogDecoderGM ~]# xfs_growfs /var/netwitness/
```

Les informations suivantes s'affichent.

```
[root@NWAPPLIANCE2599 database]# xfs_growfs /var/netwitness/
meta-data=/dev/mapper/netwitness_vg00-nwhome isize=256   agcount=4, agsize=9188864 blks
        =                               sectsz=512   attr=2, projid32bit=1
        =                               crc=0        finobt=0 spinodes=0
data     =                               bsize=4096   blocks=36755456, imaxpct=25
        =                               sunit=0      swidth=0 blks
naming   =version 2                       bsize=4096   ascii-ci=0 ftype=0
log      =internal                       bsize=4096   blocks=17947, version=2
        =                               sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                            extsz=4096   blocks=0, rtextents=0
data blocks changed from 36755456 to 39245824
[root@NWAPPLIANCE2599 database]# _
```

Démarrer les services

Saisissez la chaîne de commande suivante pour démarrer les services sur l'hôte LogDecoder.

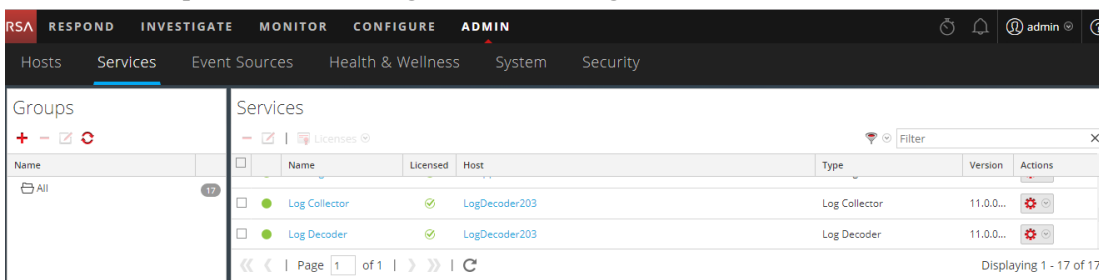
```
[root@LogDecoderGM ~]# service nwlogcollector start; service
nwlogdecoder start
```

Les informations suivantes s'affichent.

```
nwlogcollector start/running, process 4069
nwlogdecoder start/running, process 4069
```

S'assurer que les services sont en cours d'exécution

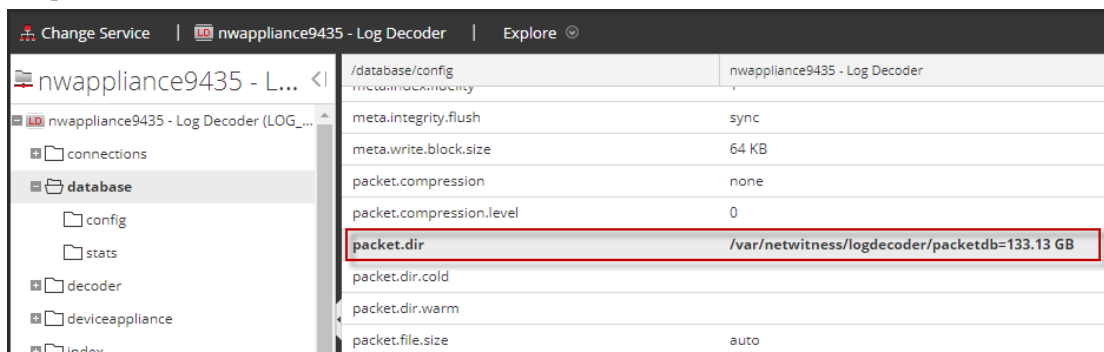
1. Connectez-vous à NetWitness Suite.
2. Cliquez sur **Administration** > **Services**.
3. Assurez-vous que les services Log Collector et Log Decoder sont en cours d'exécution.



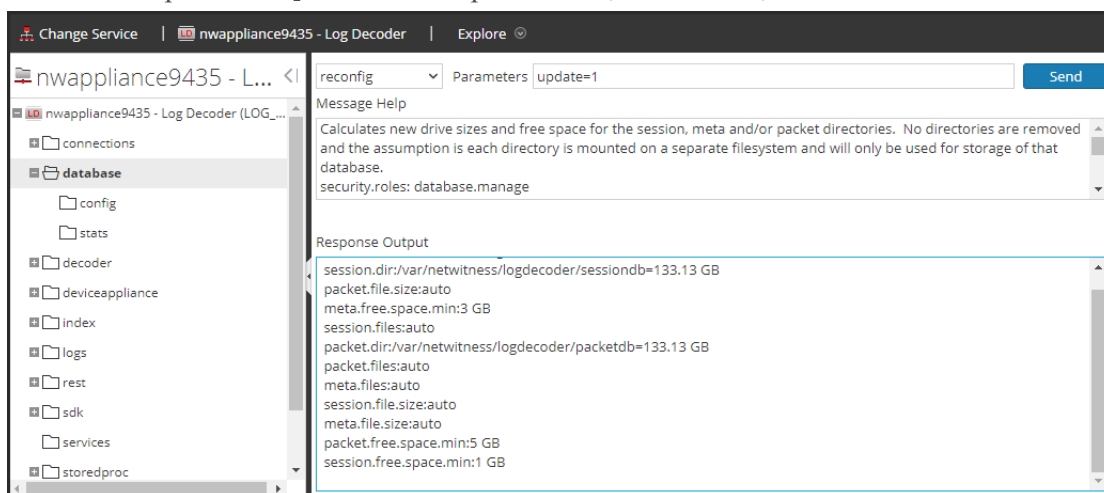
Reconfigurer les paramètres Log Decoder

1. Connectez-vous à NetWitness Suite.
2. Cliquez sur **Administration** > **Services**.
3. Sélectionnez le service LogDecoder.
4. Sous Actions, sélectionnez **Vue** > **Explorer**.

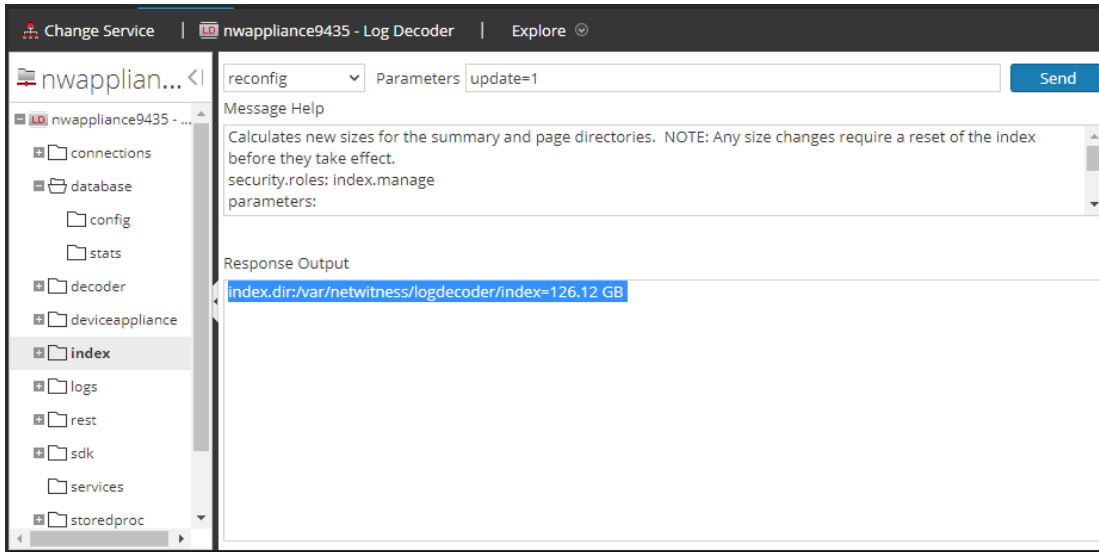
5. Cliquez sur database > config > packet.dir.



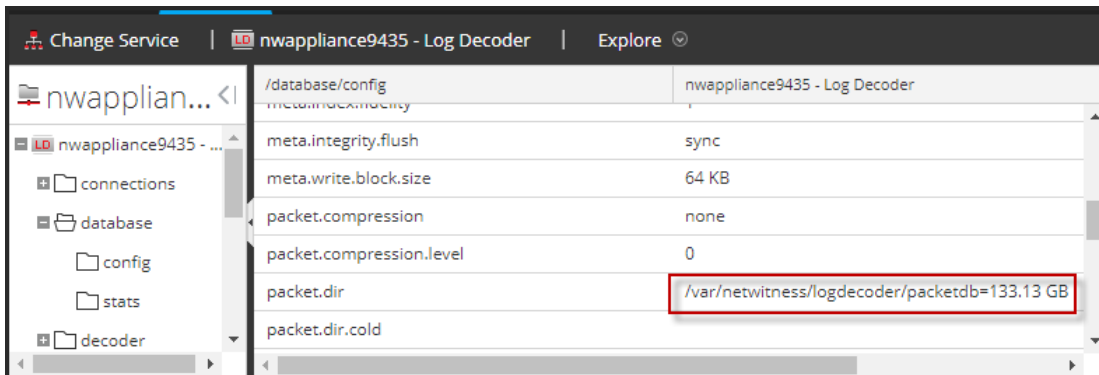
6. Cliquez avec le bouton droit sur database, cliquez sur **Propriétés**, sélectionnez la commande **reconfig**, spécifiez **update=1** dans **Paramètres**, puis cliquez sur **Envoyer**. La valeur de paramètre packetdb est passé de 98,74 Go à 133,13 Go.



7. Cliquez avec le bouton droit sur `index`, cliquez sur **Propriétés**, sélectionnez la commande **reconfig**, spécifiez **update=1** dans **Paramètres**, puis cliquez sur **Envoyer**.



8. Fermez la boîte de dialogue Propriétés pour revenir à la vue Explorer. La valeur de paramètre `packet.dir` est maintenant 133,13 Go (95 % de 203 Go).



Étape 4. Configurer les paramètres spécifiques de l'hôte

Certains paramètres spécifiques de l'application sont nécessaires pour configurer la réception de log et la capture de paquets dans l'environnement virtuel.

Configurer la réception de log dans l'environnement virtuel

La réception de log s'effectue facilement par l'envoi des logs à l'adresse IP que vous avez spécifiée pour Decoder. L'interface de gestion du Decoder vous permet ensuite de sélectionner l'interface appropriée pour écouter le trafic, si elle n'a pas déjà été sélectionnée par défaut.

Configurer la capture de paquet dans l'environnement virtuel

Il existe deux options pour la capture de paquets dans un environnement VMware. La première option consiste à configurer votre vSwitch en mode Proximité, et la seconde à utiliser une interface TAP virtuelle tierce.

Définir un vSwitch en mode Proximité

L'option consistant à placer un switch, virtuel ou physique, en mode Proximité, également décrite en tant que port SPAN (services Cisco) ou mise en miroir du port, comporte des limites. Qu'elle soit virtuelle ou physique, selon la quantité et le type de trafic copié, la capture de paquets peut facilement mener à l'over-subscription du port, qui provoque une perte de paquets. Les interfaces TAP, physiques ou virtuelles, sont conçues et prévues pour offrir une capture de 100 % sans perte du trafic souhaité.

Le mode Proximité est désactivé par défaut et ne doit pas être activé sauf en cas de besoin spécifique. Le logiciel s'exécutant dans une machine virtuelle peut être capable de surveiller tout le trafic transitant sur un vSwitch s'il est autorisé à entrer en mode Proximité et s'il cause une perte de paquets en raison d'un surabonnement du port.

Pour configurer un groupe de ports ou un switch virtuel afin d'autoriser le mode Proximité :

1. Connectez-vous à l'hôte ESXi/ESX ou vCenter Server à l'aide du client vSphere.
2. Sélectionnez l'hôte ESXi/ESX dans l'inventaire.
3. Cliquez sur l'onglet **Configuration**.
4. Dans la rubrique **Matériel**, cliquez sur **Mise en réseau**.
5. Sélectionnez les **Propriétés** du switch virtuel pour lequel vous souhaitez activer le mode Proximité.
6. Sélectionnez le switch virtuel ou le groupe de ports que vous souhaitez modifier, puis cliquez sur **Modifier**.
7. Cliquez sur l'onglet **Sécurité**. Dans le menu déroulant **Mode Proximité**, sélectionnez **Accepter**.

Utiliser une interface TAP virtuelle tierce

Les méthodes d'installation d'une interface TAP virtuelle varient selon le fournisseur. Reportez-vous à la documentation du fournisseur pour obtenir des instructions d'installation. Les interfaces TAP virtuelles sont habituellement faciles à intégrer. En outre, l'interface utilisateur de l'accès TAP simplifie la sélection et le type de trafics à copier.

Les interfaces TAP virtuelles encapsulent le trafic capturé dans un tunnel GRE. Selon le type que vous choisissez, l'un de ces scénarios peut s'appliquer :

- Un hôte externe est requis pour l'achèvement du tunnel, et l'hôte externe dirige le trafic vers l'interface du service Decoder.
- Le tunnel envoie le trafic directement à l'interface du service Decoder, où NetWitness Suite gère la désencapsulation du trafic.