



Guide d'installation d'un hôte virtuel

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.

février 2019

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	7
Recommandations en matière d'environnement virtuel	7
Configuration matérielle recommandée pour l'hôte virtuel	8
Scénario un	8
Scénario deux	10
Troisième scénario	13
Quatrième scénario	15
Instructions de dimensionnement pour les collecteurs Windows d'ancienne génération	15
Installer l'hôte virtuel NetWitness Platform dans l'environnement virtuel	17
Conditions préalables	17
Étape 1. Déployer l'hôte virtuel pour créer la machine virtuelle	17
Conditions préalables	17
Procédure	17
Étape 2. Configuration du réseau.	21
Conditions préalables	21
Procédure	21
Vérifier les ports de pare-feu ouverts	21
Étape 3. Configurer les bases de données pour prendre en charge NetWitness Platform	21
Tâche 1. Passer en revue la configuration initiale du datastore	21
Espace initiale alloué à PacketDB	21
Taille de la base de données (initiale)	22
Point de montage PacketDB	22
Tâche 2. Examiner la configuration optimale d'espace du datastore	23
Rapports d'espace disque virtuel	24
Tâche 3. Ajouter un nouveau volume et étendre les systèmes de fichiers existants	25
AdminServer	28
ESAPrimary/ESASSecondary/Malware	29
LogCollector	29
LogDecoder	29
Concentrator	31

Archiver	33
Decoder	34
Installer RSA NetWitness Platform	36
Étape 4. Configurer les paramètres spécifiques de l'hôte	53
Configurer la réception de logs dans l'environnement virtuel	53
Configurer la capture de paquets dans l'environnement virtuel	54
Utiliser une interface TAP virtuelle tierce	54
Étape 5. Tâches à effectuer après l'installation	55
Général	55
RSA NetWitness Endpoint Insights	55
Activation FIPS	57
Analytique comportementale de l'entité et de l'utilisateur NetWitness (UEBA)	58
Annexe A. Dépannage	64
Interface de ligne de commande (CLI)	65
Sauvegarde (script nw-backup)	66
Event Stream Analysis	68
Service Log Collector (nwlogcollector)	69
Serveur NW	71
Orchestration	71
Service Reporting Engine	72
NetWitness UEBA	73
Annexe B. Créer un référentiel externe	74
Historique des révisions	76

Guide de configuration de l'hôte virtuel

Ce document fournit des instructions sur l'installation et la configuration des hôtes RSA NetWitness® Platform 11.2.0.0 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 Platform 11.2.0.0 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
Mbits/s	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)
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)
RSA NetWitness UEBA	Analytique comportementale de l'entité et de l'utilisateur RSA NetWitness

Hôtes virtuels pris en charge

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

- NetWitness Server
- Event Stream Analysis : ESA primaire et secondaire
- Archiver
- Broker
- Concentrator
- Log Decoder
- Malware Analysis
- Decoder
- Remote Log Collector
- Endpoint Hybrid
- Endpoint Log Hybrid
- Analytique comportementale de l'entité et de l'utilisateur (UEBA)

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 Platform. 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.
- 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 Platform 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 Platform ».
- 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 11.2.0.0 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 Network 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

Décodeur réseau

Mbits/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

Archiver

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 Network Decoder, un Concentrator et un Warehouse Connector.
- Event Stream Analysis agrégeait à 90 000 EPS, à partir de trois Concentrators Hybrid.
- Respond 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 des réponses.
- 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

Décodeur réseau

Mbits/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

NWS1 : Serveur NetWitness et composants co-localisés

NetWitness Server, Jetty, Broker, Respond 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 Network Decoder et le Concentrator.
- Event Stream Analysis agrégeait à 90 000 EPS, à partir de trois Concentrators Hybrid.
- Respond 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

Décodeur réseau

Mbits/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

Quatrième scénario

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

- Tous les composants ont été intégrés.
- Endpoint Server est installé.
- Le flux de log comprenait un Log Decoder et un Concentrator.

Endpoint Hybrid

Agents	CPU	Mémoire	Valeurs IOPS		
5000	16 ou 42 GHz	32 Go		IOPS en lecture	IOPS en écriture
			Log Decoder	250	150
			Concentrator	150	7 050
			MongoDb	250	150

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 Platform Legacy Windows Collection Update & Installation* pour prendre connaissance des recommandations de dimensionnement pour le collecteur Windows d'ancienne génération.

UEBA

CPU	Mémoire	IOPS en lecture	IOPS en écriture
16 ou 2,4 GHz	64 Go	500	500

Remarque : RSA vous recommande de déployer UEBA uniquement sur un hôte virtuel si le volume de collecte de fichiers log est faible. Si le volume de collecte de fichiers log est modéré à élevé, RSA vous recommande de déployer UEBA sur l'hôte physique décrit sous « Spécifications du matériel hôte RSA NetWitness UEBA » dans le Guide d'installation de l'hôte physique. Contactez le support technique (<https://community.rsa.com/docs/DOC-1294>) pour obtenir des conseils sur le choix de l'hôte virtuel ou physique à utiliser pour UEBA.

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

Exécutez les procédures suivantes dans leur ordre numéroté pour installer RSA NetWitness® Platform 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.
- Client vSphere 4.1, 5.0 ou 6.0 installé pour se connecter au serveur VMware ESX.
- des droits administrateur pour créer les machines virtuelles sur le serveur VMware ESX.

Étape 1. Déployer l'hôte virtuel pour créer la machine virtuelle

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 :

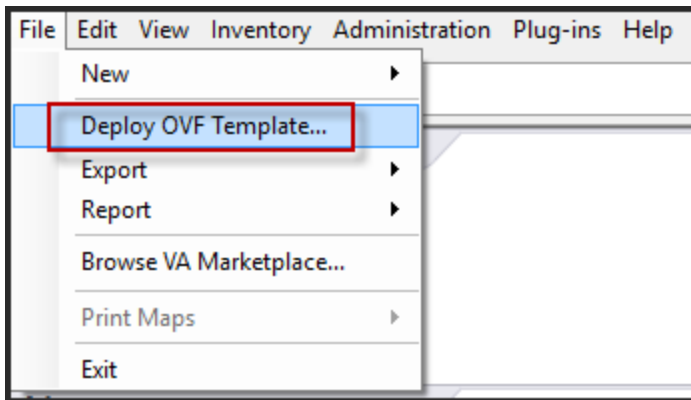
- Adresses IP réseau, masque de réseau et adresses IP de passerelle pour l'hôte virtuel.
- Noms réseau de tous les hôtes virtuels, si vous créez un cluster.
- Informations DNS ou hôte
- Mot de passe pour l'accès à l'hôte virtuel. Par défaut, le nom d'utilisateur est `root` et le mot de passe par défaut est `netwitness`.
- Le fichier de package de l'hôte virtuel NetWitness Platform, par exemple, `rsanw-11.2.0.xxxx.el7-x86_64.ova`. (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.

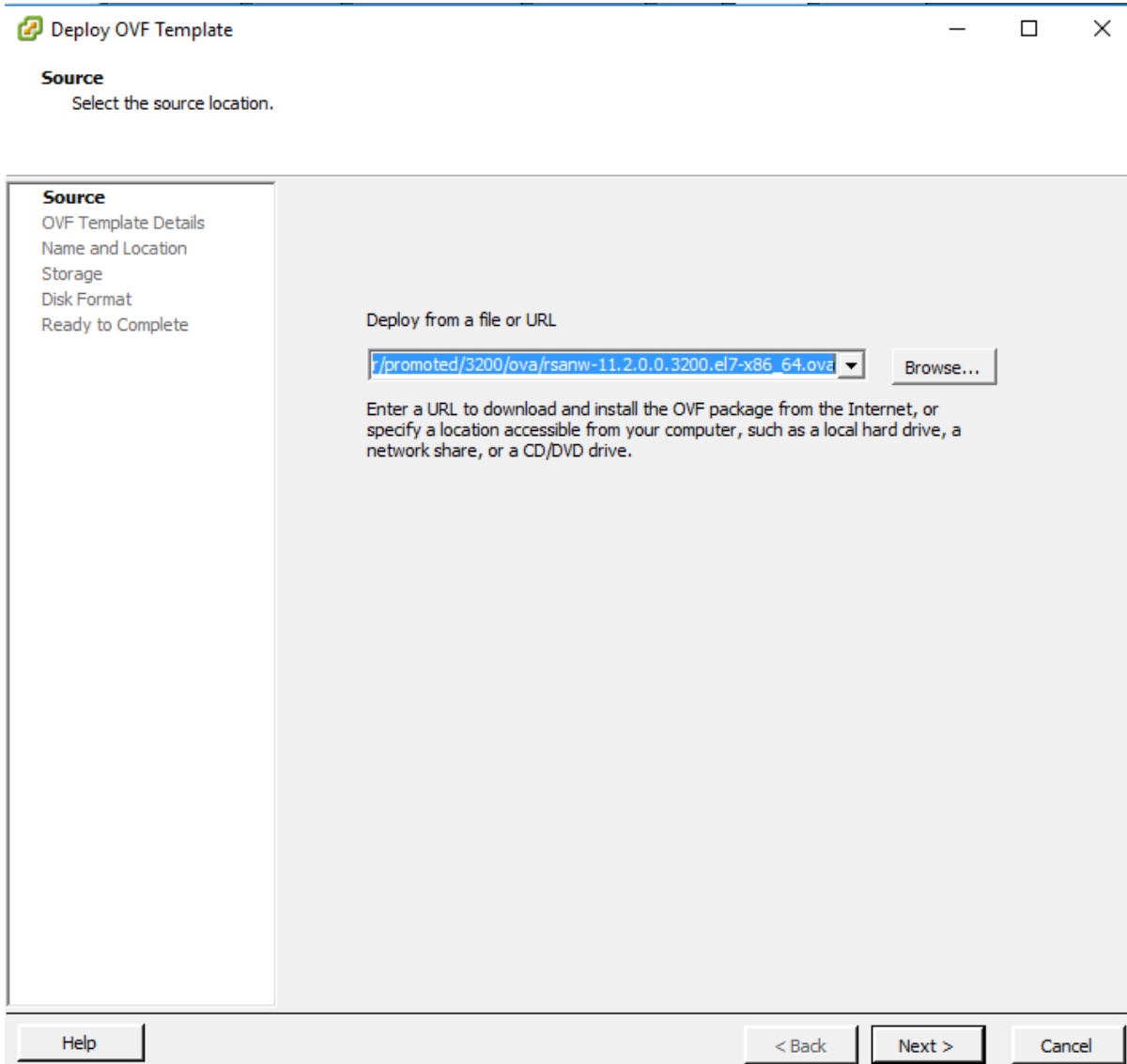
Pour déployer l'hôte OVA :

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

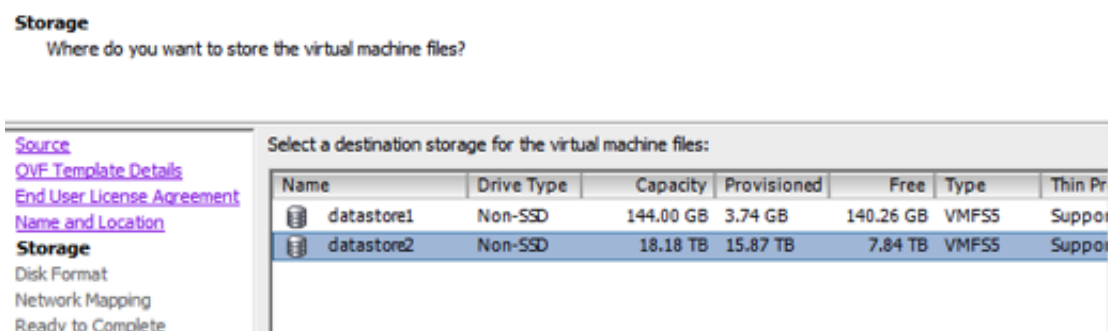


3. La boîte de dialogue Déployer le modèle OVF s'affiche. Dans la boîte de dialogue **Déployer le modèle OVF**, sélectionnez l'OVF pour l'hôte que vous souhaitez déployer dans l'environnement

virtuel (par exemple, **V11.2 GOLD\\rsanw-11.2.0.0.1948.el7-x86_64.ova**), 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 Platform sur certains hôtes (abordés dans les rubriques suivantes).

7. Cliquez sur **Suivant**.

Les options Mappage de réseau s'affichent.

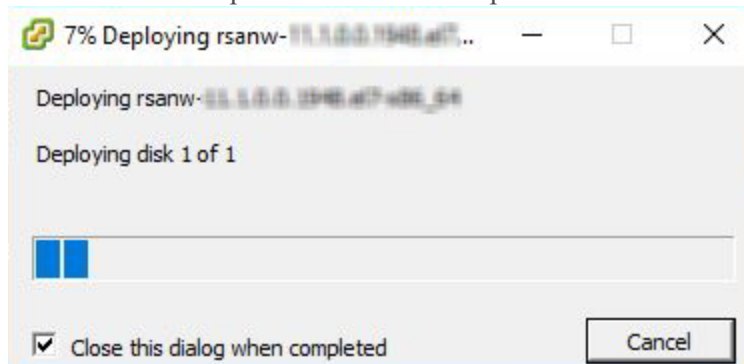
Network Mapping

What networks should the deployed template use?

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. Configuration du réseau.

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 Platform pour pouvoir configurer les services NetWitness Platform et vos pare-feu. 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.

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

NetWitness Platform

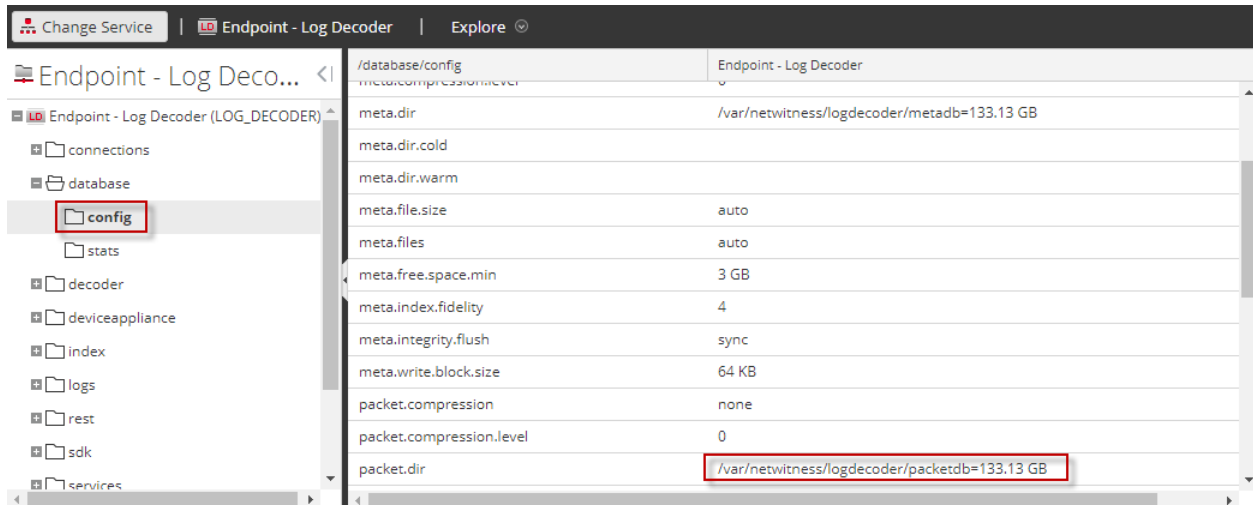
Lorsque vous déployez des bases de données à partir de l'OVA, l'allocation d'espace initial de la base de données peut ne pas être suffisant pour prendre en charge NetWitness Server. Vous devez examiner l'état des datastores après le déploiement initial et de les développer.

Tâche 1. Passer en revue la configuration initiale du datastore

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 PacketDB est d'environ 133,13 Go). L'exemple de vue Explorer suivant de NetWitness Platform affiche la taille de la PacketDB après le déploiement initial à partir du fichier OVA.



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@LogDecoder ~]# df -kh
Filesystem                                Size  Used Avail Use% Mounted on
/dev/mapper/netwitness_vg00-root          30G   3.0G   27G   10% /
devtmpfs                                 16G     0   16G    0% /dev
tmpfs                                     16G   12K   16G    1% /dev/shm
tmpfs                                     16G   25M   16G    1% /run
tmpfs                                     16G     0   16G    0% /sys/fs/cgroup
/dev/mapper/netwitness_vg00-usrhome       10G   33M   10G    1% /home
/dev/mapper/netwitness_vg00-varlog        10G   42M   10G    1% /var/log
/dev/mapper/netwitness_vg00-nwhome       141G  396M  140G    1% /var/netwitness
/dev/sda1                                1014M   73M  942M    8% /boot
tmpfs                                     3.2G     0   3.2G    0% /run/user/0
[root@LogDecoder ~]#
```

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

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

Tâche 2. Examiner 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 Platform 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 Platform 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
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	
MetaDB	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.

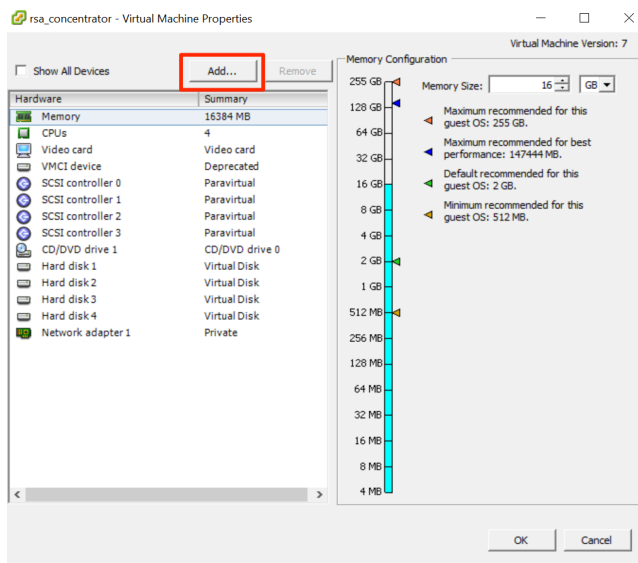
1. Ajouter un nouveau disque
2. Créer des volumes sur le nouveau disque
3. Créer un volume physique LVM sur la nouvelle partition
4. Étendre le groupe de volumes avec un volume physique
5. Étendre le système de fichiers
6. Démarrer les services
7. S'assurer que les services sont en cours d'exécution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

Ajouter un nouveau disque

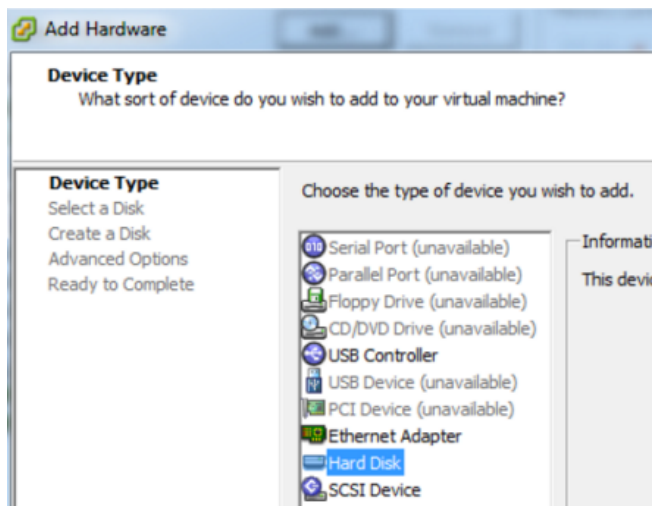
Cette procédure vous indique comment ajouter un nouveau disque de 100 Go dans le même datastore.

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

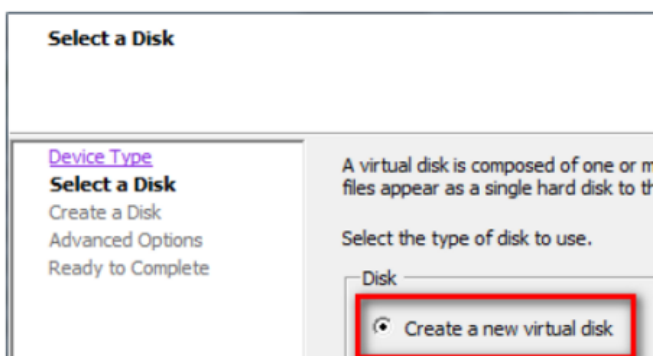
1. Arrêtez la machine, modifiez les **Propriétés de la machine virtuelle**, cliquez sur l'onglet **Matériel**, puis cliquez sur **Ajouter**.



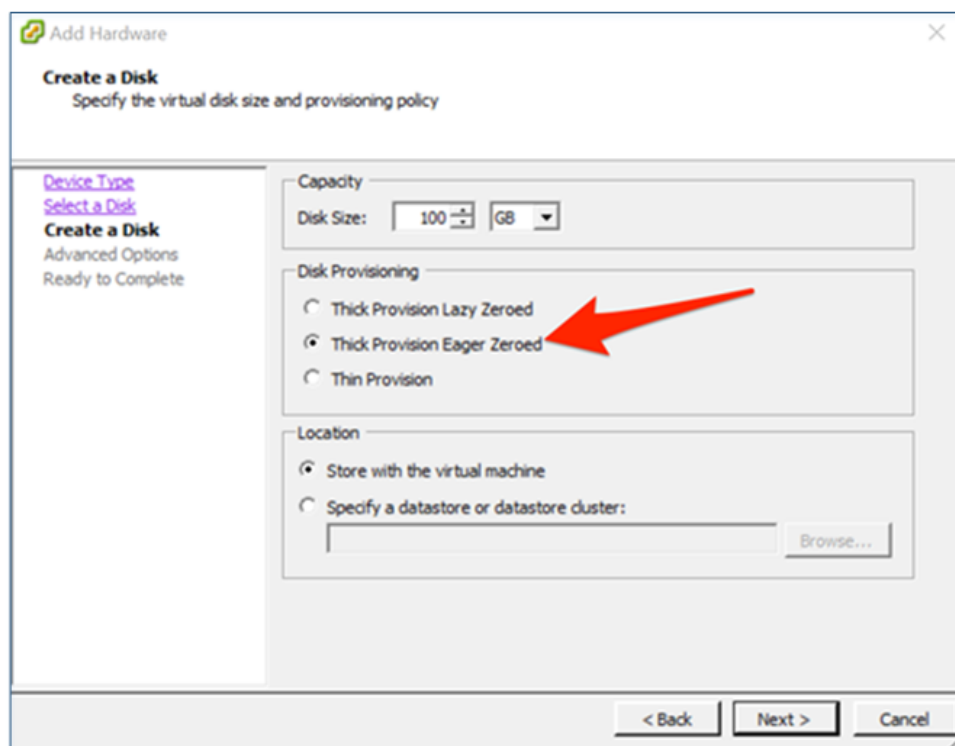
2. Dans la liste des types de périphérique, sélectionnez **Disque dur**.



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.

Device Type
Select a Disk
Create a Disk
Advanced Options
Ready to Complete

Specify the advanced options for this virtual disk. These options do not normally need to be changed.

Virtual Device Node
SCSI (0:4)

Mode

☐ Independent
Independent disks are not affected by snapshots.

☒ Persistent
Changes are immediately and permanently written to the disk.

☐ Nonpersistent
Changes to this disk are discarded when you power off or revert to the snapshot.

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

6. Confirmez les paramètres.

Device Type
Select a Disk
Create a Disk
Advanced Options
Ready to Complete

Options:

Hardware type:	Hard Disk
Create disk:	New virtual disk
Disk capacity:	100 GB
Datastore:	date:storage
Virtual Device Node:	SCSI (0:4)
Disk mode:	Persistent

Extending File Systems

Follow the instructions provided to extend the file systems for the various components.

AdminServer

Attach external disk for extension of /var/netwitness/ (refer to the steps in attaching the disk) partition. Create an additional disk with suffix as nwhome.

If a single disk is attached, follow these steps:

1. Execute `lsblk` and get the physical volume name, for example if you attach one 2TB disk.
2. `pvccreate <pv_name>` . ex suppose the PV name is /dev/sdc
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

RSA recommended partition for AdminServer (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness/	2TB	SSD	Read/Write

ESAPrimary/ESASecondary/Malware

Attach external disk for extension of /var/netwitness/ partition, create an external disk with suffix as nwhome.

If a single disk is attached, follow these steps:

1. Execute `lsblk` and get the physical volume name, for example, if you attach one 6TB disk
2. `pvccreate <pv_name>` . ex suppose the PV name is /dev/sdc
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 5.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

RSA recommended partition for ESAPrimary/ESASecondary (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness/	6TB	HDD	Read/Write

LogCollector

Attach an external disk for extension of /var/netwitness/ partition, create an external disk with suffix as nwhome.

1. Execute `lsblk` and get the physical volume name, for example if you attach one 500GB disk
2. `pvccreate <pv_name>` . ex suppose the PV name is /dev/sdc
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 600G /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

RSA recommended partition for LogCollector (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness/	500GB	HDD	Read/Write

LogDecoder

Attach an external disk for extension of /var/netwitness/ partition, create an external disk with suffix as nwhome, attach other external disks for Logdecoder database partition. For extending /var/netwitness partition follow these steps:

Remarque : No other partition should reside on this partition, only to be used for /var/netwitness/partition

1. Execute `lsblk` and get the physical volume name, suppose if you had add attach one 2TB disk
2. `pvcreate <pv_name>` . ex suppose the PV name is `/dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

Other partitions are also required. Create the following four partitions on volume group logdecodersmall

Folder	LVM	Volume Group
/var/netwitness/logdecoder	decoroot	logdecodersmall
/var/netwitness/logdecoder/index	index	logdecodersmall
/var/netwitness/logdecoder/metadb	metadb	logdecodersmall
/var/netwitness/logdecoder/sessiondb	sessiondb	logdecodersmall

Follow these steps to create the partitions:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/sdd`
3. `vgcreate -s 32 logdecodersmall /dev/sdd`
4. `lvcreate -L <disk_size> -n <lv_name> logdecodersmall`
5. `mkfs.xfs /dev/logdecodersmall/<lv_name>`
6. Repeat steps 5 and 6 for all the LVM's mentioned

The following four partitions should be on volume group logdecoder and should be in single RAID 0 array

Folder	LVM	Volume Group
/var/netwitness/logdecoder/packetdb	packetdb	logdecoder

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/sde`
3. `vgcreate -s 32 logdecoder /dev/sde`
4. `lvcreate -L <disk_size> -n packetdb logdecoder`
5. `mkfs.xfs /dev/logdecoder/packetdb`

RSA recommends below sizing partition for LogDecoder (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness/	1TB	HD D	Read/Write
/dev/logdecodersmall/decoroot	/var/netwitness/logdecoder	10GB	HD D	Read/Write
/dev/logdecodersmall/index	/var/netwitness/logdecoder/index	30GB	HD D	Read/Write
/dev/logdecodersmall/metadb	/var/netwitness/logdecoder/metadb	370GB	HD D	Read/Write
/dev/logdecodersmall/sessiondb	/var/netwitness/logdecoder/sessiondb	3TB	HD D	Read/Write
/dev/logdecoder/packetdb	/var/netwitness/logdecoder/packetdb	18TB	HD D	Read/Write

Create each directory and mount the LVM on it in a serial manner, except /var/netwitness which will be already created.

Remarque : Create the folder /var/netwitness/logdecoder and mount on /dev/logdecodersmall/decoroot then create the other folders and mount them.

After that add the below entries in /etc/fstab in the same order and mount them using mount -a.

```

/dev/logdecodersmall/decoroot /var/netwitness/logdecoder xfs noatime,nosuid 1 2
/dev/logdecodersmall/index /var/netwitness/logdecoder/index xfs noatime,nosuid 1 2
/dev/logdecodersmall/metadb /var/netwitness/logdecoder/metadb xfs noatime,nosuid 1 2
/dev/logdecodersmall/sessiondb /var/netwitness/logdecoder/sessiondb xfs noatime,nosuid 1 2
/dev/logdecoder/packetdb /var/netwitness/logdecoder/packetdb xfs noatime,nosuid 1 2

```

Concentrator

Attach external disk for extension of /var/netwitness/ partition, Create an external disk with suffix as nwhome, attach other external disks for Concentrator database partition. If there are multiple disks, create a Raid 0 array.

For extending /var/netwitness partition follow below steps:

Remarque : No other partition should reside on this partition, only to be used for /var/netwitness/partition

1. Execute `lsblk` and get the physical volume name, for example if you attach one 2TB disk
2. `pvcreate <pv_name>` . ex suppose the PV name is `/dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`

Below four partition are also required on volume group concentrator and should be in single RAID 0 array

Folder	LVM	Volume Group
<code>/var/netwitness/concentrator</code>	Root	Concentrator
<code>/var/netwitness/ concentrator /sessiondb</code>	index	Concentrator
<code>/var/netwitness/ concentrator /metadb</code>	metadb	Concentrator

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/md0`
3. `vgcreate -s 32 concentrator /dev/md0`
4. `lvcreate -L <disk_size> -n <lvm_name> concentrator`
5. `mkfs.xfs /dev/concentrator/<lvm_name>`
6. Repeat steps 5 and 6 for all the LVM's mentioned

Below four partitions should be on volume group index and should be in single RAID 0 array

Folder	LVM	Volume Group
<code>/var/netwitness/concentrator/index</code>	index	index

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/md1`
3. `vgcreate -s 32 index /dev/md1`
4. `lvcreate -L <disk_size> -n index index`
5. `mkfs.xfs /dev/index/index`

RSA recommends below sizing partition for Concentrator (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness/	1TB	HDD	Read/Write
/dev/concentrator/decoroot	/var/netwitness/concentrator	10GB	HDD	Read/Write
/dev/concentrator/metadb	/var/netwitness/concentrator/metadb	370GB	HDD	Read/Write
/dev/concentrator/sessiondb	/var/netwitness/concentrator/sessiondb	3TB	HDD	Read/Write
/dev/index/index	/var/netwitness/concentrator/index	2TB	SSD	Read/Write

Create each directory and mount the LVM on it in a serial manner, except `/var/netwitness` which will be already created.

Remarque : Create the folder `/var/netwitness/concentrator` and mount on `/dev/concentrator/decoroot` then create the other folders and mount them.

After that add the below entries in `/etc/fstab` in the same order

```
/dev/concentrator/root /var/netwitness/concentrator xfs noatime,nosuid 1 2
/dev/concentrator/sessiondb /var/netwitness/concentrator/sessiondb xfs
noatime,nosuid 1 2
/dev/concentrator/metadb /var/netwitness/concentrator/metadb xfs
noatime,nosuid 1 2 2
/dev/index/index /var/netwitness/concentrator/index xfs noatime,nosuid 1 2
```

Archiver

Attach an external disk for extension of `/var/netwitness/` partition, create an external disk with suffix as `nwhome`, attach other external disks for Archiver database partition. If there are multiple disks, create a Raid 0 array.

For extending `/var/netwitness` partition follow these steps:

Remarque : No other partition should reside on this partition, only to be used for `/var/netwitness/partition`

1. Execute `lsblk` and get the physical volume name, suppose if you had add attach one 2TB disk
2. `pvcreeate <pv_name> . ex suppose the PV name is /dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`

Below four partitions are required on volume group archiver and should be in single RAID 0 array

Folder	LVM	Volume Group
/var/netwitness/archiver	Archiver	archiver

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/md0`
3. `vgcreate -s 32 archiver /dev/md0`
4. `lvcreate -L <disk_size> -n archiver archiver`
5. `mkfs.xfs /dev/archiver/archiver`

RSA recommends below sizing partition for archiver (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness/	1TB	HDD	Read/Write
/dev/archiver/archiver	/var/netwitness/archiver	4TB	HDD	Read/Write

Create each directory and mount the LVM on it in a serial manner, except `/var/netwitness` which will be already created.

After that add the below entries in `/etc/fstab` in the same order

```
/dev/archiver/archiver /var/netwitness/archiver xfs noatime,nosuid 1 2
```

Decoder

Attach an external disk for extension of `/var/netwitness/` partition, create an external disk with suffix as `nwhome`, attach other external disks for decoder database partition. For extending `/var/netwitness` partition follow these steps:

Remarque : No other partition should reside on this partition, only to be used for `/var/netwitness/partition`

1. Execute `lsblk` and get the physical volume name, suppose if you had add attach one 2TB disk
2. `pvcreate <pv_name>` . ex suppose the PV name is `/dev/sdc`
3. `vgextend netwitness_vg00 /dev/sdc`
4. `lvextend -L 1.9T /dev/netwitness_vg00/nwhome`
5. `xfs_growfs /dev/mapper/netwitness_vg00-nwhome`

Below four partition should be on volume group decodersmall

Folder	LVM	Volume Group
/var/netwitness/decoder	decoroot	decoderssmall
/var/netwitness/decoder/index	index	decoderssmall
/var/netwitness/decoder/metadb	metadb	decoderssmall
/var/netwitness/decoder/sessiondb	sessiondb	decoerssmall

Follow these steps:

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/sdd`
3. `vgcreate -s 32 logdecoderssmall /dev/sdd`
4. `lvcreate -L <disk_size> -n <lv_name> logdecoderssmall`
5. `mkfs.xfs /dev/logdecoderssmall/<lv_name>`
6. Repeat steps 5 and 6 for all the LVM's mentioned

Below partition should be on volume group logdecoder and should be in single RAID 0 array

Below four partition should be on volume group logdecoder and should be in single RAID 0 array

Folder	LVM	Volume Group
/var/netwitness/logdecoder/packetdb	packetdb	decoder

1. Execute `lsblk` and get the physical volume names from the output
2. `pvcreate /dev/sde`
3. `vgcreate -s 32 decoder /dev/sde`
4. `lvcreate -L <disk_size> -n packetdb decoder`
5. `mkfs.xfs /dev/decoder/packetdb`

RSA recommends below sizing partition for Decoder (Can be changed based on the retention days)

LVM	Folder	Size	Disk Type	Caching
/dev/netwitness_vg00/nwhome	/var/netwitness	1TB	HDD	Read/Write
/dev/decoderssmall/decoroot	/var/netwitness/decoder	10GB	HDD	Read/Write

LVM	Folder	Size	Disk Type	Caching
/dev/decodersmall/index	/var/netwitness/decoder/index	30GB	HDD	Read/Write
/dev/decodersmall/metadb	/var/netwitness/decoder/metadb	370GB	HDD	Read/Write
/dev/decodersmall/sessiondb	/var/netwitness/decoder/sessiondb	3TB	HDD	Read/Write
/dev/decoder/packetdb	/var/netwitness/decoder/packetdb	18TB	HDD	Read/Write

Create each directory and mount the LVM on it in serial manner, except /var/netwitness which will be already created.

Remarque : Create the folder /var/netwitness/decoder and mount on /dev/decodersmall/decoroot then create the other folders and mount them.

After that add the below entries in /etc/fstab in the same order and mount them using mount -a.

```
/dev/decodersmall/decoroot /var/netwitness/decoder xfs noatime,nosuid 1 2
/dev/decodersmall/index /var/netwitness/decoder/index xfs noatime,nosuid 1 2
/dev/decodersmall/metadb /var/netwitness/decoder/metadb xfs noatime,nosuid 1 2
/dev/decodersmall/sessiondb /var/netwitness/decoder/sessiondb xfs
noatime,nosuid 1 2
/dev/decoder/packetdb /var/netwitness/decoder/packetdb xfs noatime,nosuid 1 2
```

Installer RSA NetWitness Platform

Deux tâches principales sont à effectuer dans l'ordre indiqué ci-dessous pour installer NetWitness Platform 11.2

1. Tâche 1 - Installation de la version 11.2.0.0 sur l'hôte du serveur NetWitness (NW)
2. Tâche 2 - Installation de la version 11.2.0.0 sur tous les autres composants hôtes

Tâche 1 - Installation de la version 11.2.0.0 sur l'hôte du serveur NW

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

- La plate-forme environnementale du serveur NW 11.2.0.0.

- Les composants des serveurs NW (à savoir, serveur d'administration, serveur de configuration, serveur d'orchestration, serveur d'intégration, Broker, serveur Investigate, Reporting Engine, serveur Respond et serveur de sécurité).
 - Un référentiel contenant les fichiers RPM requis pour installer les autres composants ou services fonctionnels.
1. Déployez votre environnement 11.2.0.0 :
 - a. Ajoutez une nouvelle machine virtuelle.
 - 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 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 au 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 postérieures à 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 Platform 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).

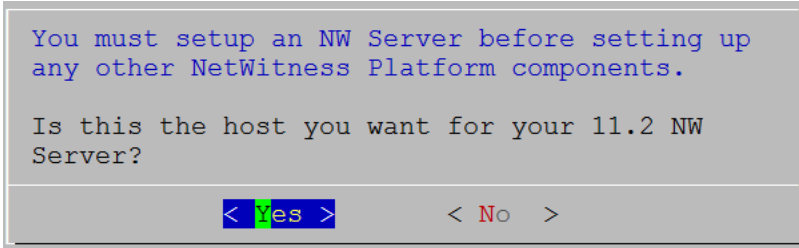
By clicking "Accept", you (the "Customer") hereby agree, on behalf of your company or organization, to be bound by the terms and conditions of the End User License Agreement (the "EULA") located at <https://www.rsa.com/content/dam/rsa/PDF/shrinkwrap-license-combined.pdf> with RSA Security LLC ("RSA", 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>

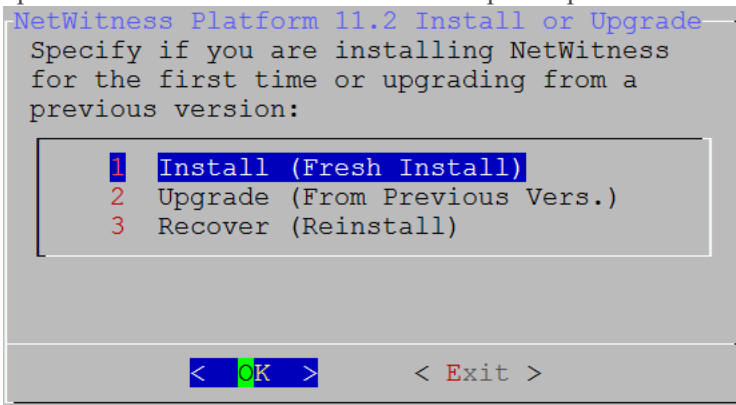
3. Naviguez jusqu'à **Accepter** à l'aide de la touche de tabulation, puis appuyez sur Entrée.
Le message **Est-ce l'hôte que vous souhaitez pour votre serveur NW 11.2 ?** s'affiche.



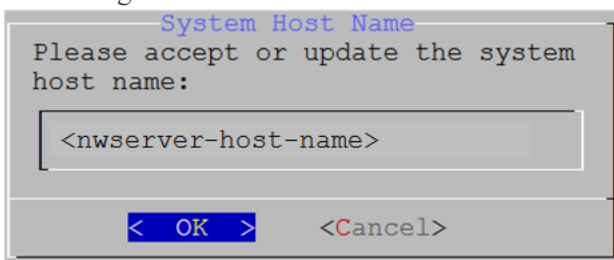
4. Naviguez jusqu'à **Oui** à l'aide de la touche de tabulation, puis appuyez sur Entrée.

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.

L'invite **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.



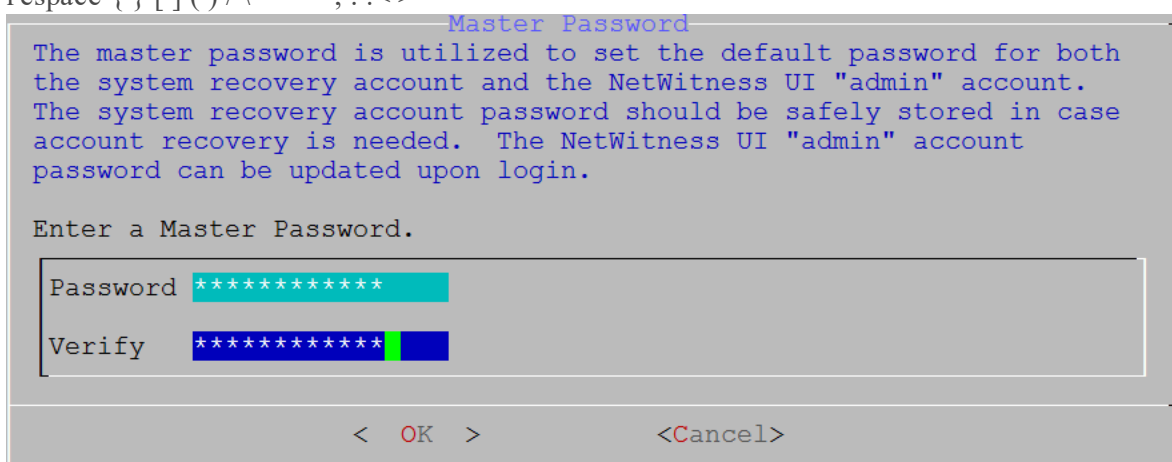
Attention : Si vous incluez "." dans un nom d'hôte, le nom d'hôte doit également inclure un nom de domaine valide.

6. Appuyez sur **Entrée** si 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.
7. 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 { } [] () / \ ' " ` ~ ; : . < > -



8. 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 { } [] () / \ ' " ` ~ ; : . < > -

9. 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.

10. 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.

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.

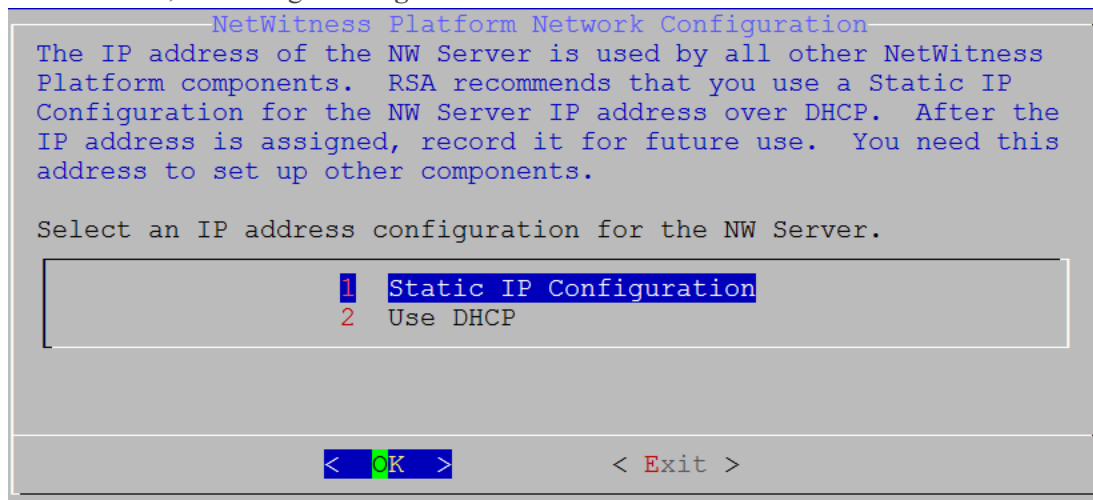
- Si vous utilisez une connexion SSH, l'avertissement suivant s'affiche.

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.

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

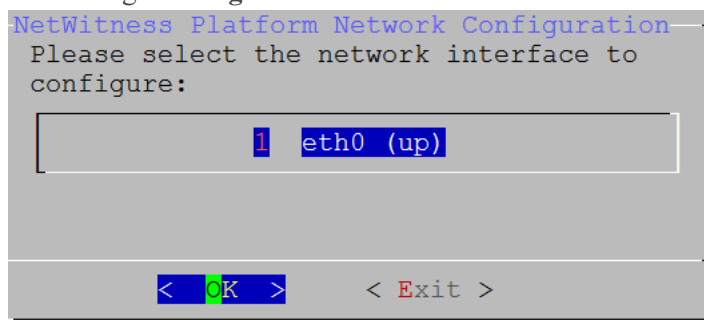
- Si le programme d'installation a détecté une configuration IP et que vous avez choisi de l'utiliser, le message **Mettre à jour le référentiel** s'affiche. Accédez à l'étape 12 à et terminez l'installation.
- Si aucune configuration d'IP n'a été trouvée ou que vous avez choisi de modifier la configuration d'IP existante, le message **Configuration réseau** s'affiche.



11. 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.



12. 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 de l'adresse IP statique** s'affiche.

NetWitness Platform Network Configuration
Static IP configuration

IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Default Gateway	<input type="text"/>
Primary DNS Server	<input type="text"/>
Secondary DNS Server	<input type="text"/>
Local Domain Name	<input type="text"/>

< OK > < Exit >

13. 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, le message d'erreur `All fields are required` s'affiche (les champs **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 est incorrecte, 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 **Mise à jour du référentiel** s'affiche.

14. Sélectionnez le même référentiel que celui sélectionné lors de l'installation de l'hôte du serveur NW pour tous les hôtes.

NetWitness Platform Update Repository

The NetWitness Platform Update Repository contains all the RPMs needed to build and maintain all the NetWitness Platform components. All components managed by the NW Server need access to the Repository.

Do you want to set up the NetWitness Platform Update Repository on:

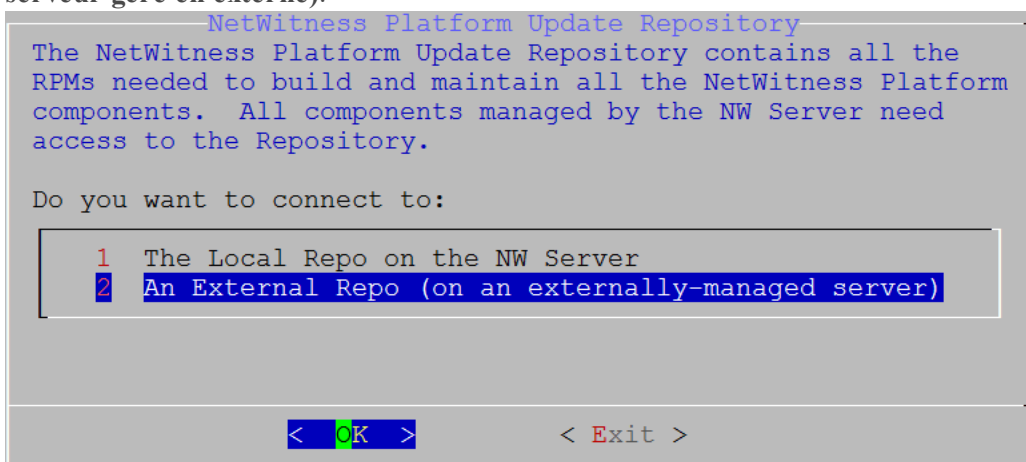
1	The Local Repo (on the NW Server)
2	An External Repo (on an externally-managed server)

< OK > < Exit >

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.

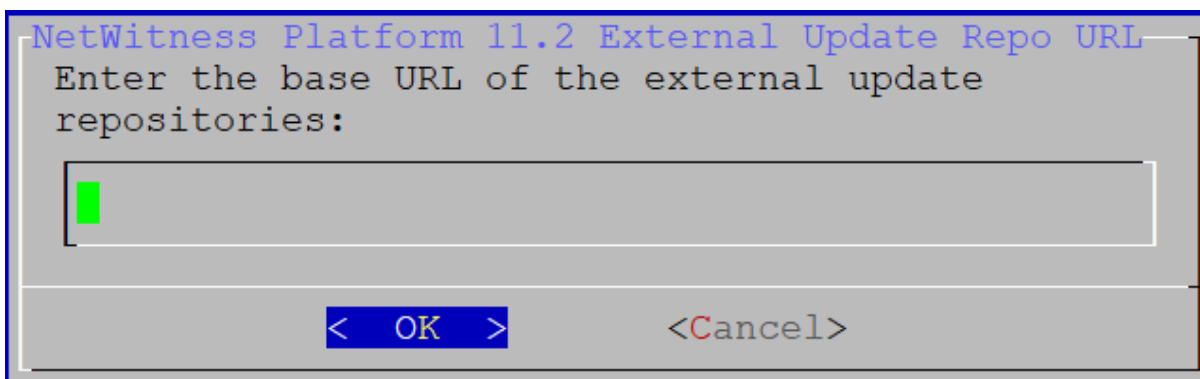
15. Utilisez les flèches vers le haut et vers le bas pour sélectionner **2 Un référentiel externe (sur un serveur géré en externe)**.



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

Reportez-vous à la section [Annexe B. Créer un référentiel externe](#) pour obtenir des instructions sur la façon de configurer un référentiel externe. Accédez à la [Table des matières principale](#) pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

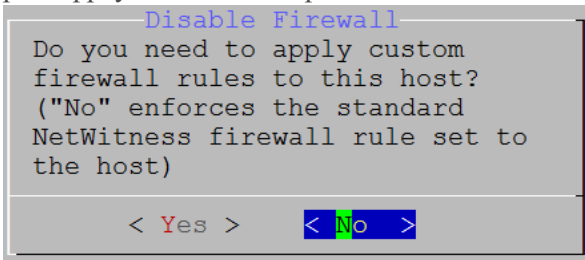
16. Entrez l'URL de base du référentiel externe de NetWitness Platform à partir des instructions fournies à l'[Annexe B. Créer un référentiel externe](#) (par exemple, <http://testserver/netwitness-repo>), puis cliquez sur **OK**.



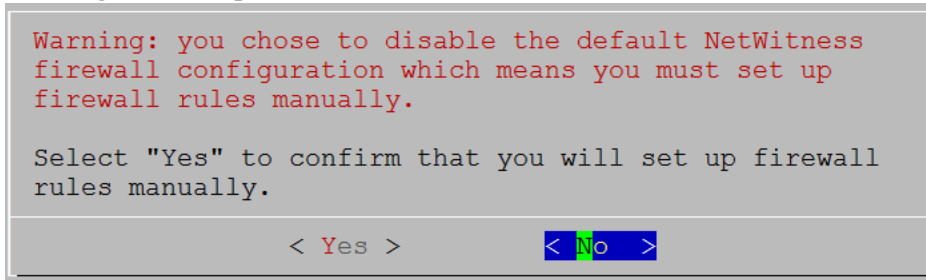
Le message de **désactivation** ou d'utilisation de la configuration standard de **pare-feu** s'affiche.

17. 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. Accédez à l'option **Oui** à l'aide de la touche de tabulation,

puis appuyez sur **Entrée** pour désactiver la configuration de pare-feu standard.

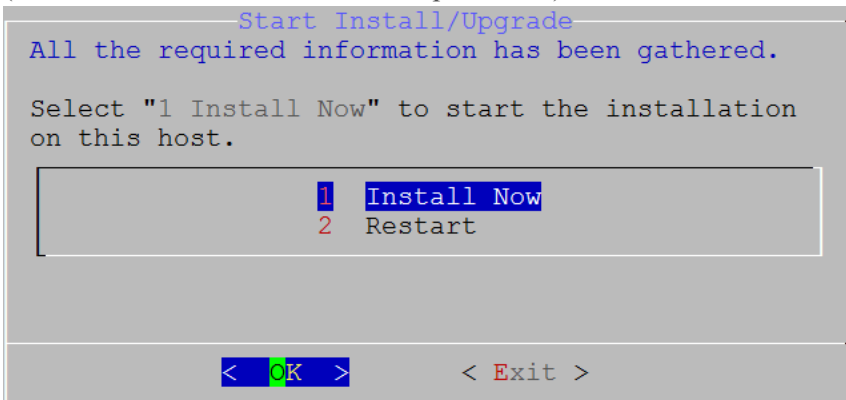


- Pour confirmer votre sélection, choisissez **Oui**, dans le cas contraire, choisissez **Non** pour utiliser la configuration du pare-feu standard.



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

- Appuyez sur la touche **Entrée** pour installer la version 11.2.0.0 sur le serveur autre que NW (**Installer maintenant** est la valeur par défaut).



Lorsque **Installation terminée** s'affiche, la mise à niveau du serveur NW 10.6.6 vers le serveur NW 11.2 est terminée.

Remarque : Ignorez les erreurs de code de hachage similaires aux erreurs illustrées dans la capture d'écran 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 service fonctionnel, effectuez les tâches suivantes sur un hôte de serveur autre que NW.

- Installez la plate-forme environnementale 11.2.0.0.
 - Appliquez les fichiers RPM 11.2.0.0 au service à partir du référentiel de mise à jour du serveur NW.
1. Déployez les fichiers OVA 11.2.0.0.
 2. 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 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 postérieures à 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 Platform 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

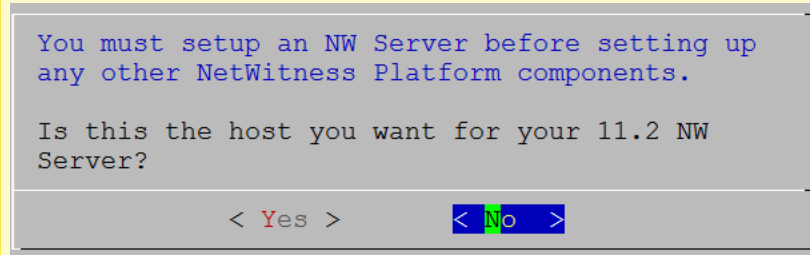
92%

<Accept >

<Decline>

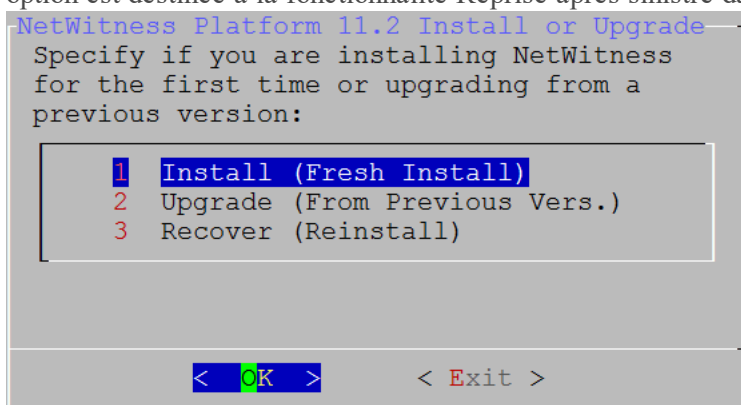
3. Naviguez jusqu'à **Accepter** à l'aide de la touche de tabulation, puis appuyez sur Entrée.
Le message **Est-ce l'hôte que vous souhaitez pour votre serveur NW 11.2 ?** s'affiche.

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 11.2.0.0 sur l'hôte du serveur NW](#) pour corriger cette erreur.



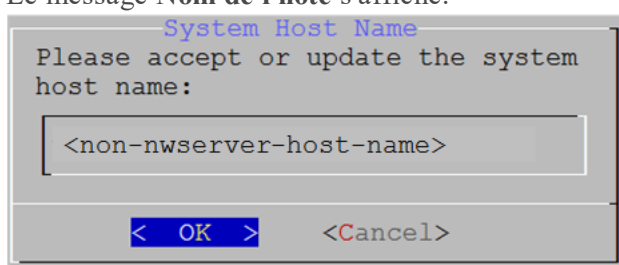
4. Appuyez sur **Entrée** (Non).

L'invite **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.

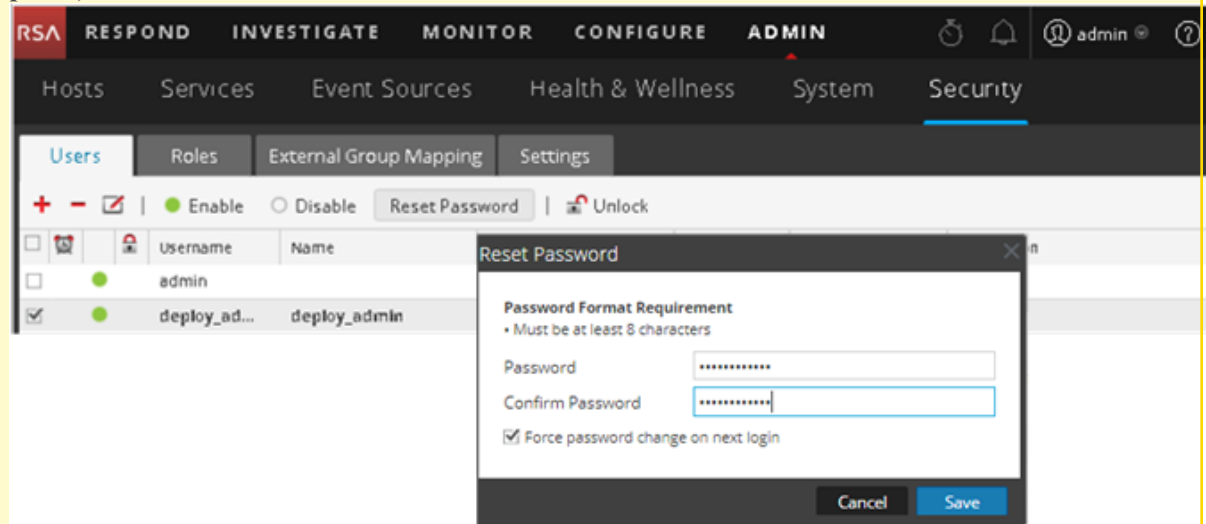
Le message **Nom de l'hôte** s'affiche.



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

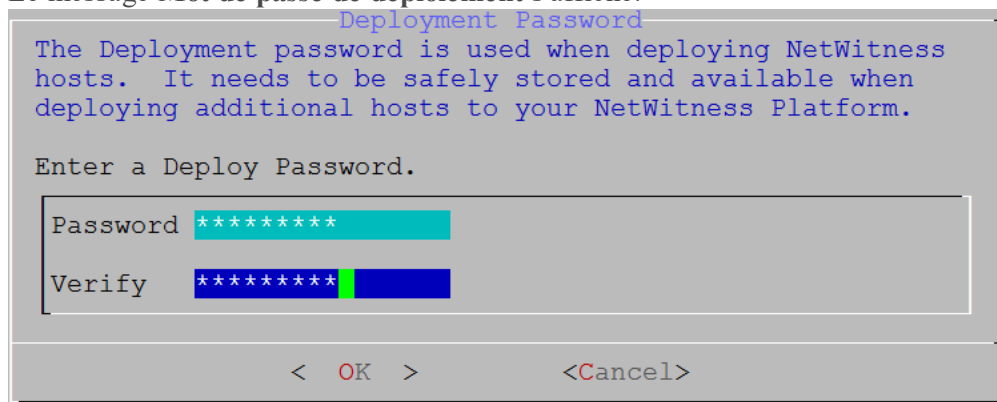
Attention : Si vous modifiez le mot de passe utilisateur **deploy_admin** dans l'interface utilisateur NetWitness Platform (**ADMIN>Sécurité >Sélectionner deploy-admin - Réinitialiser le mot de passe**),



vous devez :

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

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

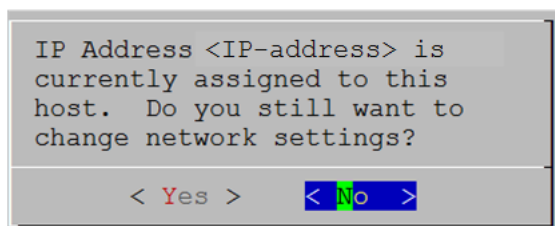


Remarque : Vous devez utiliser le même mot de passe de déploiement que vous avez utilisé lors de l'installation du serveur NW.

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**.

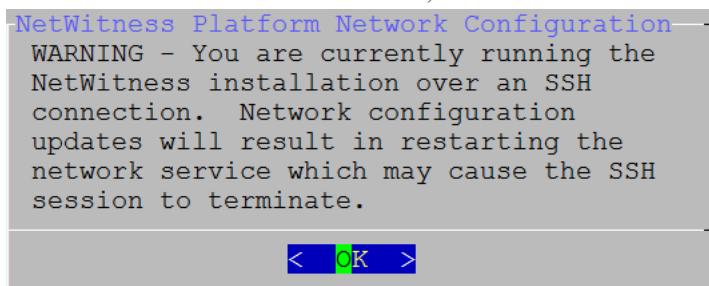
Une des invites conditionnelles suivantes s'affiche.

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



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.

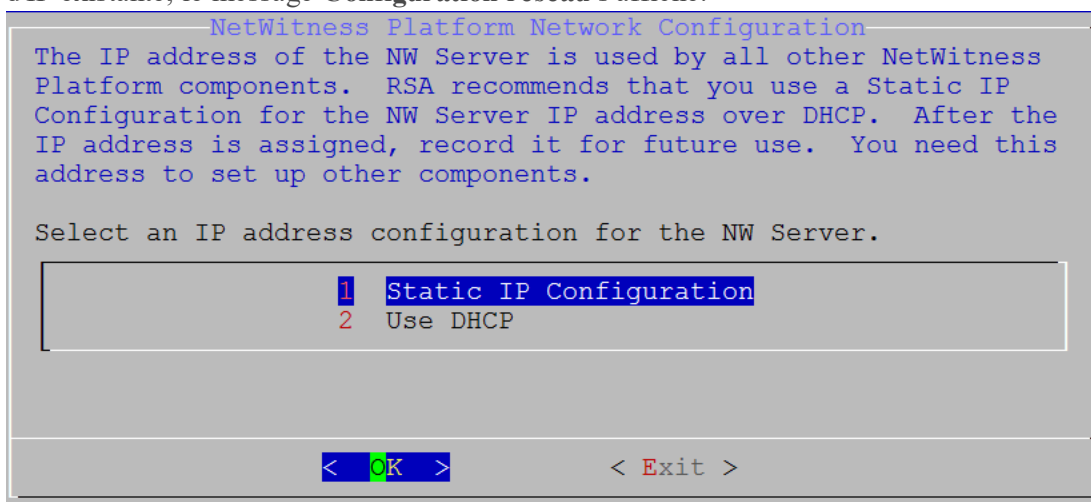
- Si vous utilisez une connexion SSH, l'avertissement suivant s'affiche.



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

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

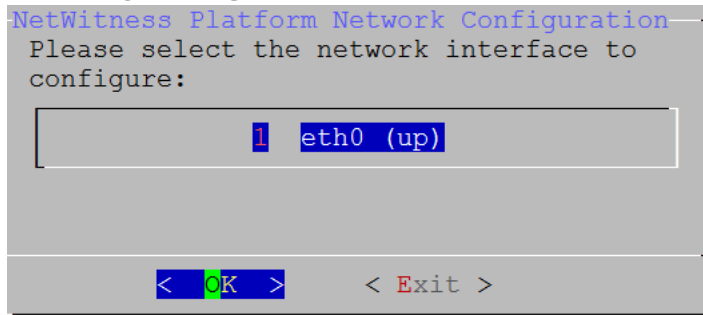
- Si le programme d'installation a détecté une configuration IP et que vous avez choisi de l'utiliser, le message **Mettre à jour le référentiel** s'affiche. Accédez à l'étape 11 à et terminez l'installation.
- Si aucune configuration d'IP n'a été trouvée ou que vous avez choisi de modifier la configuration d'IP existante, le message **Configuration réseau** s'affiche.



8. Naviguez jusqu'à **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** pour utiliser l'adresse IP statique.

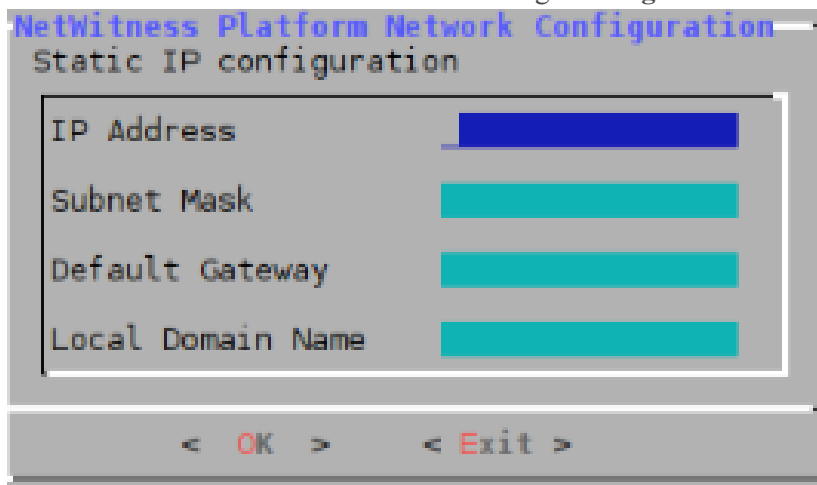
Si vous souhaitez utiliser **DHCP**, utilisez la touche directionnelle Bas jusqu'à **2 Utiliser DHCP**, puis appuyez sur **Entrée**.

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 de l'adresse IP statique** 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**.

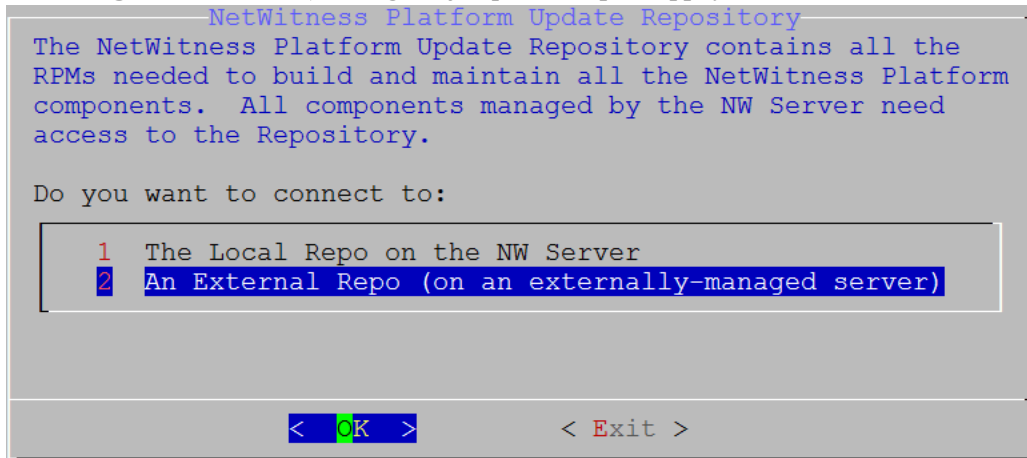
Si vous ne remplissez pas tous les champs obligatoires, le message d'erreur `All fields are required` s'affiche (les champs **Serveur DNS secondaire** et **Nom de domaine local** ne sont pas obligatoires.)

Si la syntaxe ou la longueur de caractères utilisées pour un de ces champs est incorrecte, 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 **Mise à jour du référentiel** s'affiche.

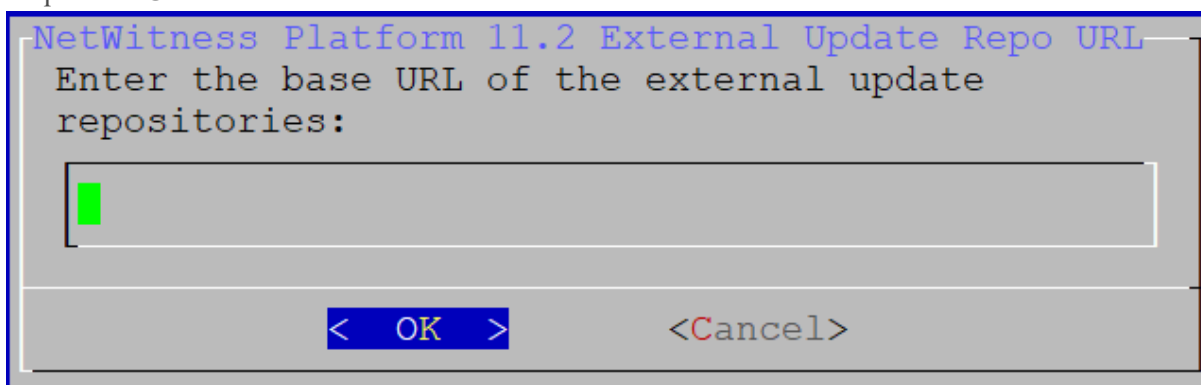
11. Utilisez les flèches vers le haut et vers le bas pour sélectionner **2 Un référentiel externe (sur un serveur géré en externe)**, naviguez jusqu'à **OK**, puis appuyez sur **Entrée**.



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

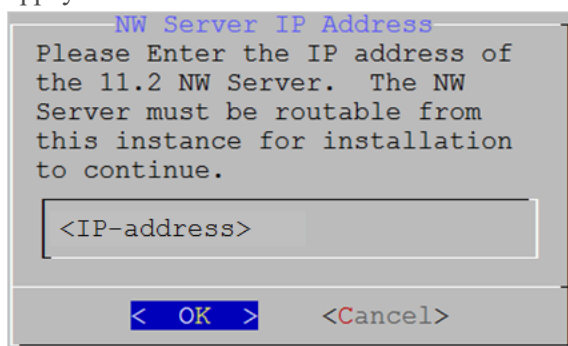
Les référentiels vous donnent accès aux mises à jour RSA et CentOS.

12. Saisissez l'URL de base du référentiel externe NetWitness Platform permettant de configurer le serveur NW dans la section précédente (par exemple, **http://testserver/netwitness-repo**), puis cliquez sur **OK**.



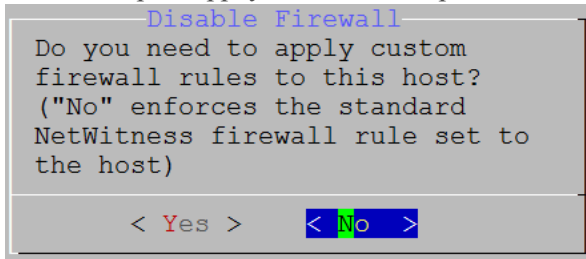
L'**adresse IP du serveur NW** s'affiche.

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

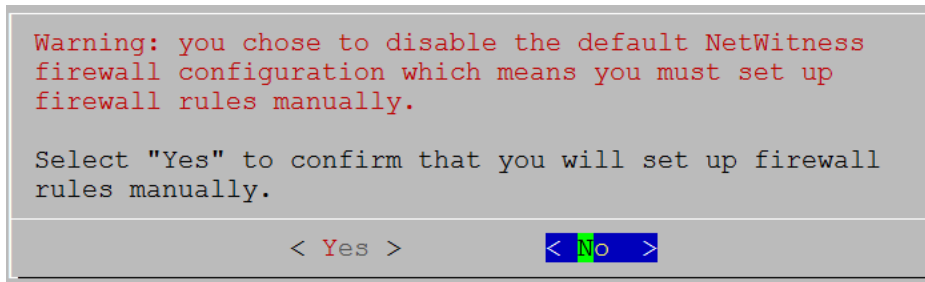


Le message de **désactivation** ou d'utilisation de la configuration de **pare-feu** standard s'affiche.

14. 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.



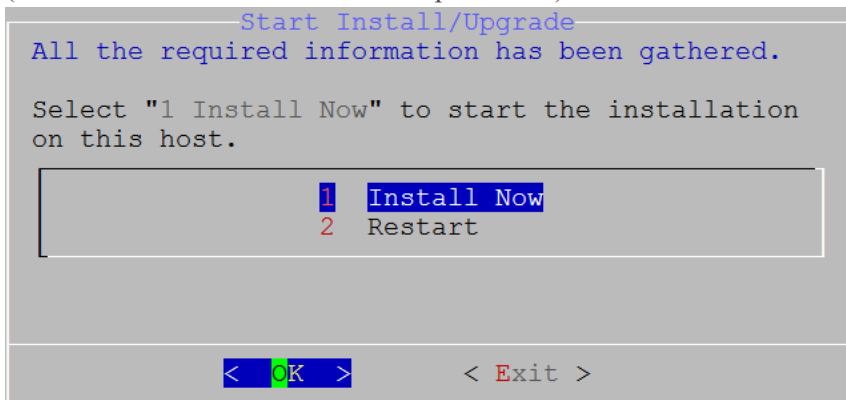
- Si vous sélectionnez **Oui**, confirmez votre sélection.



- Si vous sélectionnez **Non**, la configuration du pare-feu standard est appliquée.

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



15. Appuyez sur la touche **Entrée** pour installer la version 11.2.0.0 sur le serveur autre que NW (**Installer maintenant** est la valeur par défaut).

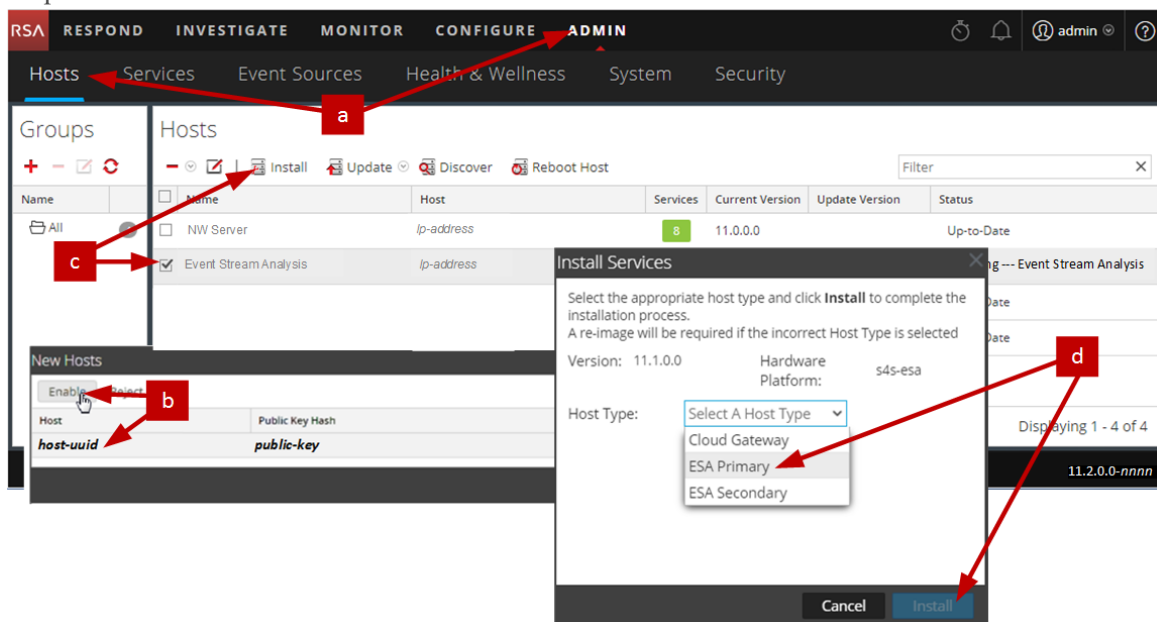


Lorsque **Installation terminée** s'affiche, vous disposez d'un hôte générique (noeud x) avec un système d'exploitation compatible avec NetWitness Platform 11.2.0.0.

16. Installez un service de composants sur l'hôte de serveur autre que NW.
- 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.

- 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 (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.

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

Étape 4. Configurer les paramètres spécifiques de l'hôte

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

Configurer la réception de logs dans l'environnement virtuel

La réception de logs 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 paquets 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 causant une perte de paquets en raison d'une over-subscription 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 de vSphere Client.
2. Sélectionnez l'hôte ESXi/ESX dans l'inventaire.
3. Cliquez sur l'onglet **Configuration**.
4. Dans la section **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 les 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 vers l'interface du service Decoder, où NetWitness Platform gère la désencapsulation du trafic.

Étape 5. Tâches à effectuer après l'installation

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

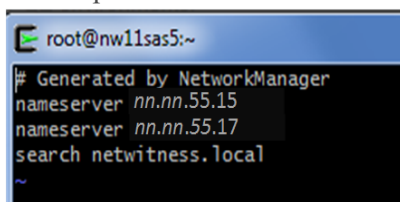
- Généralités
- RSA NetWitness® Endpoint Insights
- Activation FIPS
- Analytique comportementale de l'entité et de l'utilisateur RSA NetWitness (UEBA)

Général

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

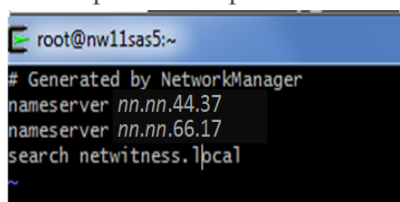
Sur NetWitness Server, effectuez les tâches suivantes pour reconfigurer le serveur DNS dans NetWitness Platform 11.2.

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 la 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.

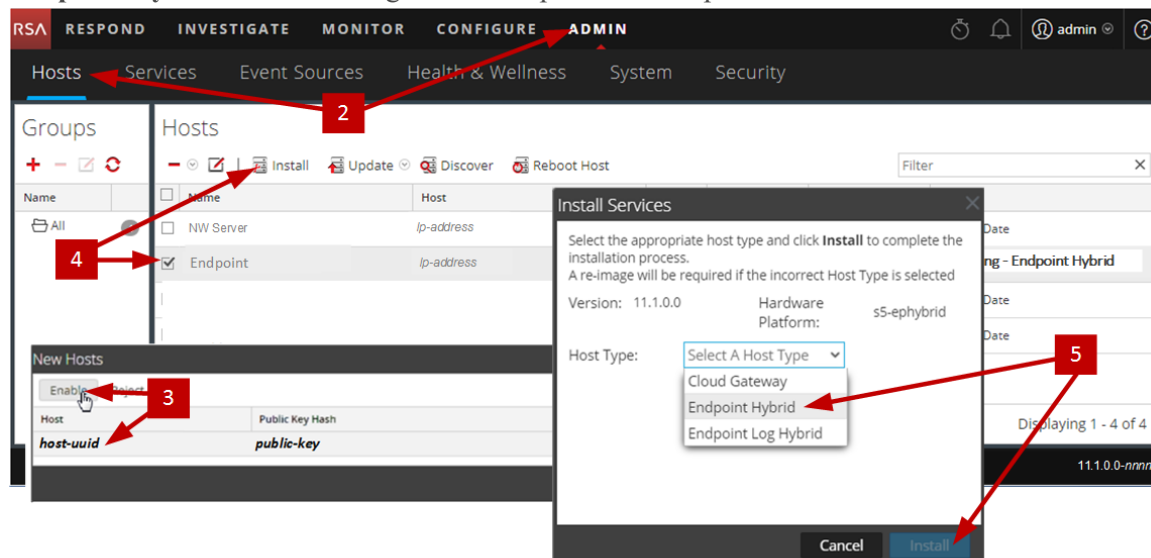
2. Connectez-vous à NetWitness Platform, puis cliquez sur **ADMIN > Hôtes**.
La boîte de dialogue Nouveaux hôtes s'affiche avec la vue Hôtes grisée en arrière-plan.

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.

- 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.



- Assurez-vous que tous les services Endpoint Hybrid ou Endpoint Log Hybrid sont en cours d'exécution.
- 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.
- 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.

Analytique comportementale de l'entité et de l'utilisateur NetWitness (UEBA)

(Facultatif) Tâche 3 - Installer NetWitness UEBA

Condition préalable : Augmenter le stockage pour le déploiement virtuel

Les machines virtuelles sont déployées avec environ 104 Go dans le montage de stockage par défaut. Pour installer NetWitness UEBA, vous devez augmenter l'espace de stockage dans votre environnement virtuel jusqu'à au moins 800 Go.

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.

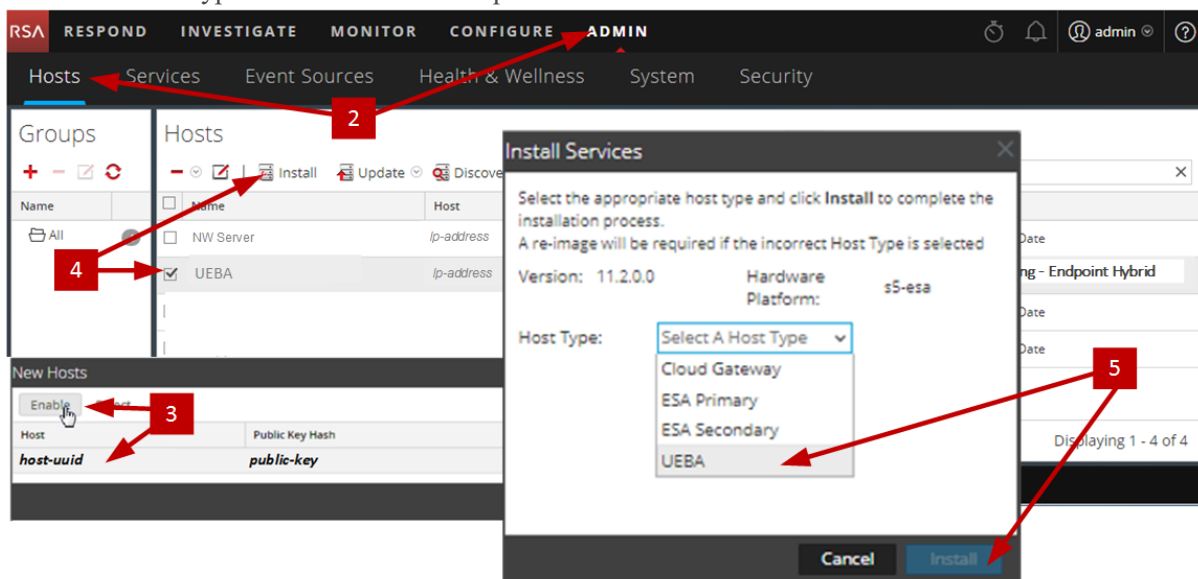
2. Connectez-vous à la plate-forme NetWitness et accédez à **ADMIN > Hôtes**.
La boîte de dialogue Nouveaux hôtes s'affiche avec la vue Hôtes grisée en arrière-plan.

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.

The screenshot shows the RSA NetWitness Platform Admin console. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The ADMIN tab is active, and the 'Security' sub-tab is selected. The 'Users' page is open, showing a list of users on the left and a detailed form for the 'Broker' user on the right.

User Information

Name	Broker	Username	Broker
Password		Confirm Password	
Email	test@rsa.coim	Description	

User Settings

Auth Type	NetWitness Platform	Core Query Timeout	5
Query Prefix		Session Threshold	0

Role Membership

<input type="checkbox"/>	Groups
<input type="checkbox"/>	Administrators
<input type="checkbox"/>	Aggregation
<input checked="" type="checkbox"/>	Analysts
<input type="checkbox"/>	Data_Privacy_Officers
<input type="checkbox"/>	Malware_Analysts
<input type="checkbox"/>	Operators
<input type="checkbox"/>	SOC_Managers

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>	<p>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.</p> <p>!"#\$%&()*+,-.;<=>?@[\\]^_`{ }</p> <p>Si vous souhaitez inclure un ou des caractères spéciaux, vous devez délimiter le mot de passe avec un signe d'apostrophe, par exemple :</p> <pre>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</pre>
-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>	<p>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).</p> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>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.</p> </div>

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.

- 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 <code>deploy_admin</code> mot de passe dans <code>nwsetup-tui</code> .
Solution	Récupérez votre mot de passe <code>deploy_admin</code> . 1. Ouvrez une session SSH sur l'hôte du serveur NW. <code>security-cli-client --get-config-prop --prop-hierarchy nw.security-client --prop-name deployment.password</code> Exécutez la commande SSH sur l'hôte ayant échoué. 2. Exécutez à nouveau la commande <code>nwsetup-tui</code> à l'aide du mot de passe <code>deploy_admin</code> 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. <code>systemctl restart rsa-sms</code>

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. <div> <input type="checkbox"/> SA Server <div>IP-Address</div> <div>8</div> <div>version-number</div> <div>Reboot Host</div> </div>
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	<p>Erreurs de sauvegarde générées par le paramètre d'attribut immutable. Voici un exemple d'erreur qui peut s'afficher :</p> <pre>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</pre>
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 : <code>chattr -i <filename></code>

Erreur	<p>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 : <code>/etc/sysconfig/network-scripts/ifcfg-em1</code></p> <p>Vérifiez le contenu de <code>/var/netwitness/logdecoder/packetdb/nw-backup/2018-02-23/S5-BROK-36-10.25.53.36-network.info.txt</code></p>
Cause	<p>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.</p>
Solution	<p>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 <code><hostname>-<hostip>-network.info.txt</code> et doit contenir les entrées suivantes :</p> <pre>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</pre>

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	<ol style="list-style-type: none"> 1. Ouvrez une session SSH sur l'hôte primaire ESA et connectez-vous. 2. Dans le fichier <code>/opt/rsa/esa/conf/wrapper.conf</code>, remplacez la ligne suivante : <code>wrapper.java.additional.5=-Djavax.net.ssl.keyStore=/opt/rsa/esa/../carlos/keystore</code> par : <code>wrapper.java.additional.5=-Djavax.net.ssl.keyStore=/opt/rsa/carlos/keystore</code> 3. Exécutez la commande suivante pour redémarrer ESA. <code>systemctl restart rsa-nw-esa-server</code> <div> 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. </div>

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	<code><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.</code>
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 <i>Guide de configuration de Log Collection</i> . Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

Message d'erreur	<code><timestamp> NwLogCollector_PostInstall: Lockbox Status : Not Found</code>
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 <i>Guide de configuration de Log Collection</i> . 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 <i>Guide de configuration de Log Collection</i> . 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 <code>sa.log</code> . <code>Syslog Configuration migration failed. Restart jetty service to fix this issue</code>
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	<ol style="list-style-type: none">1. Ouvrez une session SSH sur le serveur NW.2. Exécutez la commande suivante : <code>orchestration-cli-client --update-admin-node</code>

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	<ol style="list-style-type: none">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 <code>orchestration-server.log</code> . <code>"'file' _virtual_ returned False: cannot import name HASHES"</code>
Cause	Salt Minion a peut-être été mis à niveau et n'a jamais redémarré sur un hôte de serveur non NW
Solution	<ol style="list-style-type: none">1. SSH vers l'hôte de serveur non NW dont la mise à niveau a échoué.2. Exécutez les commandes suivantes. <code>systemctl unmask salt-minion</code> <code>systemctl restart salt-minion</code>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 <i>Guide de configuration de Reporting Engine</i> 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	<p>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.</p>
Solution	<p>Effectuez les étapes suivantes pour supprimer le service NetWitness UEBA supplémentaire.</p> <ol style="list-style-type: none"> 1. SSH vers NW Server et exécutez les commandes suivantes pour interroger la liste des services NetWitness UEBA installés. <pre># 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</pre> 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) : <pre># orchestration-cli-client --remove-service --id <ID-for-presidio-airflow-form-previous-output></pre> 4. Exécutez la commande suivante pour mettre à jour le nœud 0 afin de restaurer NGINX : <pre># orchestration-cli-client --update-admin-node</pre> 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).

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

1. Connectez-vous à l'hôte du serveur Web.
2. Créez le répertoire destiné à héberger le référentiel NW (`netwitness-11.2.0.0.zip`), par exemple `ziprepo`, sous `web-root` sur le serveur Web. Par exemple, `/var/netwitness` est la `web-root`, soumettez la chaîne de commande suivante.
`mkdir -p /var/netwitness/<your-zip-file-repo>`
3. Créez le répertoire `11.2.0.0` sous `/var/netwitness/<your-zip-file-repo>`.
`mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0`
4. Créez les répertoires `OS` et `RSA` sous `/var/netwitness/<your-zip-file-repo>/11.2.0.0`.
`mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS`
`mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA`
5. Décompressez le fichier `netwitness-11.2.0.0.zip` dans le répertoire `/var/netwitness/<your-zip-file-repo>/11.2.0.0`.
`unzip netwitness-11.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0`
 La décompression de `netwitness-11.2.0.0.zip` résulte en deux fichiers zip (`OS-11.2.0.0.zip` et `RSA-11.2.0.0.zip`) et d'autres fichiers.
6. Décompressez le fichier :
 - a. `OS-11.2.0.0.zip` dans le répertoire `/var/netwitness/<your-zip-file-repo>/11.2.0.0/OS`.
`unzip /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS-11.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS`
 L'exemple suivant illustre la façon dont la structure de fichiers du système d'exploitation (OS) s'affiche une fois que vous décompressez le fichier.

	Parent Directory	-
	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/<your-zip-file-repo>/11.2.0.0/RSA.
 unzip /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA-11.2.0.0.zip -d
 /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA
 L'exemple suivant illustre l'affichage de la structure du fichier de mise à jour de la version de RSA après décompression du fichier.

	Parent Directory	-
	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
	fmeserver-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>/<your-zip-file-repo>`.

7. Utilisez `http://<web server IP address>/<your-zip-file-repo>` en réponse à l'invite **Entrez l'URL de base des référentiels de mises à jour externes** émanant du programme d'installation NW 11.2.0.0 (nwsetup-tui).

Historique des révisions

Révision	Date	Description	Auteur
1	17 août 2018	Version pour les opérations	IDD
1.1	29 novembre 2018	Ajout d'une note sur les licences UEBA Trail.	IDD