RSA NETWITNESS® SUITE

Guide de mise à niveau des hôtes virtuels

pour la version 10.6.5 vers 11.1

Informations de contact

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

Marques commerciales

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

Contrat de licence

Licences tierces

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

Remarque sur les technologies de chiffrement

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

Distribution

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

juillet 2018

Sommaire

Introduction

Les instructions de ce guide s'appliquent exclusivement à la mise à niveau des hôtes virtuels vers RSA NetWitness Suite version 11.1. Reportez-vous au document *RSA NetWitness Suite Guide de mise à niveau des hôtes physiques* pour savoir comment procéder pour mettre à niveau les hôtes physiques de la version 10.6.5.x vers la version 11.1. Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

NetWitness Suite 11.1 est une version majeure qui a une incidence sur tous les produits de NetWitness Suite. Les composants de la suite sont les suivants : Serveur NetWitness (serveur d'administration, serveur de configuration, serveur d'intégration, serveur Investigate, serveur d'orchestration, serveur Respond et serveur de sécurité), Archiver, Broker, Concentrator, Context Hub, Decoder, Endpoint Hybrid, Endpoint Log Hybrid, ESA primaire, ESA secondaire, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector et Workbench.

Reportez-vous au *Guide de mise en route de RSA NetWitness Suite* pour vous familiariser avec les principales modifications apportées à l'interface utilisateur de la version 11.x. Reportez-vous au *Guide de déploiement de RSA NetWitness Suite* pour vous familiariser avec les principales modifications de la plate-forme dans la version 11.x.

Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

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

Mise à niveau de CentOS6 vers CentOS7

NetWitness Suite 11.1 est une version majeure qui implique la mise à niveau vers une version plus récente du système d'exploitation (CentOS6 vers CentOS7). En outre, l'environnement de plate-forme de la version 11.1 a été considérablement amélioré pour prendre en charge les types actuels et futurs de déploiement physique et virtuel. Ces modifications nécessitent une mise à niveau vers le nouvel environnement et une mise à niveau de la fonctionnalité.

Stratégie de mise à niveau de la version 11.1 de RSA NetWitness® Suite

Le premier chemin de mise à niveau pris en charge pour RSA NetWitness® Suite 11.1 est Security Analytics 10.6.5.x. Si vous exécutez une version de NetWitness Suite antérieure à la version 10.6.5.x, vous devez effectuer une mise à jour vers la version 10.6.5.x avant de passer à la mise à jour 11.1. Consultez le *Guide de mise à jour de RSA Security Analytics 10.6.5* (https://community.rsa.com/docs/DOC-85119) sur RSA Link.

Stratégie de mise à niveau d'hôte prise en charge

Vous devez mettre à niveau un hôte vers le même type d'hôte :

- Une même gamme d'appliance physique RSA vers une même gamme d'appliance physique RSA (autrement dit, la gamme 4 vers la gamme 4, la gamme 5 vers la gamme 5).
  RSA ne prend pas en charge d'hôtes physiques tiers dans la version 11.1.
- On-Prem Virtual vers On-Prem Virtual

Attention : La mise à niveau 11.1 ne prend pas en charge les mises à niveau de plate-forme mixte (par exemple, le physique vers le virtuel n'est pas pris en charge).

Le matériel, les déploiements, les services et les fonctions non pris en charge dans la version 11.1

RSA ne prend pas en charge la mise à niveau vers la version 11.1. du matériel, des déploiements, des services et des fonctions suivants.

- Appliance RSA tout-en-un
- Plusieurs déploiements Serveur NetWitness
- Le service IPDB
- Le serviceMalware Analysis co-localisé sur le serveur SA (la mise à niveau de Malware Analysis Entreprise est prise en charge dans la version 11.1.)
- Le service autonome Warehouse Connector (la mise à niveau d'un Warehouse Connector co-localisé est prise en charge dans la version 11.1.)
- La politique personnalisée d'Intégrité dans la version 10.6.x pour le Service Context Hub . Après la mise à niveau vers NetWitness 11.1, votre politique personnalisée n'est pas

présente. À la place, vous trouverez la politique de surveillance du serveur Context hub prête à l'emploi dans l'interface utilisateur, ce qui est spécifique à la version 11.1.

- Les déploiements renforcés du Guide d'implémentation technique de la sécurité (STIG) définis par la DISA (Defense Information Systems Agency).
- Warehouse Analytics (Science des données)

Les considérations relatives à la mise à niveau d'Event Stream Analysis (ESA)

Dans RSA NetWitness® Suite version 11.1, RSA a modifié la façon dont les règles de corrélation ESA stockent et transmettent les alertes générées par le système. Dans la version 11.1, ESA envoie toutes les alertes à un système d'alerte central. Le stockage local mongo dans ESA version 10.6.5.x a été retiré.

Attention : Si vous n'utilisez pas la gestion des incidents dans la version 10.6.5.x, réfléchissez bien avant d'effectuer la mise à niveau vers la version 11.1.

Les directives suivantes doivent vous aider à déterminer si vous devez ou non mettre à niveau vos hôtes ESA vers la version 11.1.

Dans votre déploiement 10.6.5.x, si vous avez :

- Un hôte ESA avec ou sans gestion des incidents configurée, optez pour la mise à niveau vers la version 11.1.
- Plusieurs hôtes ESA configurés pour utiliser la gestion des incidents – Le système continuera de regrouper les alertes de manière centralisée. Si le système est correctement dimensionné et fonctionne comme prévu dans la version 10.6.5.x, vous pouvez vous mettre à niveau vers la version 11.1.
- Plusieurs hôtes ESA non configurés pour utiliser la gestion des incidents et que vous vous connectez à des hôtes ESA individuels pour afficher les alertes, n'optez pas pour la mise à niveau vers la version 11.1.

Remarque : Si vous n'utilisez pas la gestion des incidents dans la version 10.6.5.x, vous ne pouvez pas afficher les alertes ESA de la version 10.6.5.x dans le composant Respond de la version 11.1 sans exécuter un script de migration. Utilisez le script de migration d'alerte ESA pour migrer ces alertes à l'emplacement qui permettra à Respond de les afficher dans la version 11.1. Reportez-vous à l'article *Instructions de migration d'alerte ESA* de base de connaissances (https://community.rsa.com/docs/DOC-81680) dans RSA Link pour obtenir des instructions sur la façon d'exécuter ce script.

Phases de la mise à niveau

RSA vous recommande d'échelonner les mises à niveau de l'hôte, comme décrit dans cette section. La mise à jour vers CentOS7 et la nécessité d'un accès physique ou iDRAC rend la mise à niveau vers la version 11.1 plus longue que pour la plupart des mises à niveau.

Attention : Si vous échelonnez la mise à niveau, vous :
• devez commencer par mettre à niveau les hôtes à la Phase 1, dans l'ordre indiqué.
• il est possible que les fonctions ne soient pas toutes opérationnelles avant la mise à jour de l'ensemble du déploiement.
• les fonctions d'administration du service ne seront pas disponibles avant la mise à niveau de tous les hôtes de votre déploiement.

Phase 1

Commencez par exécuter la Phase 1 et mettez à niveau les hôtes dans l'ordre suivant :

1. Hôte du serveur Security Analytics
2. Hôtes Event Stream Analysis
3. Hôtes Malware Analysis
4. Hôtes Broker (si vous ne disposez pas d'un Broker, mettez à niveau vos hôtes Concentrator)
   Le serveur NW 11.1 ne peut pas communiquer avec des services de base de la version 10.6.5.x pour la nouvelle fonction de procédure d'enquête. C'est pourquoi vous devez mettre à niveau les hôtes Broker ou Concentrator durant la Phase 1.

Phase 2

Mise à niveau du reste de vos hôtes.

RSA vous recommande de suivre l'ordre de la Phase 2 afin de réduire :

- la perte de fonctionnalité pendant la procédure d'enquête.
- l'interruption de service entraînée par de la capture des paquets et des logs.

Remarque : Sauf pour les hôtes Log Collection avec destinations d'événements en aval, il n'est techniquement pas nécessaire de mettre à niveau vos hôtes dans l'ordre indiqué dans la phase 2.

Il s'agit de l'ordre de mise à niveau des hôtes de la phase 2 recommandé par RSA.

1. Hôtes Decoder
2. Hôtes Concentrator

3. Hôtes Archiver
4. Hôtes Log Collection - Log Collectors sur les hôtes Log Decoder (LD), Virtual Log Collectors (VLC) et les Legacy Windows Collectors (LWC)
   Avant la mise à niveau d'un hôte de collecte des logs, vous devez le préparer pour la mise à niveau. Cette préparation consiste notamment à éviter que des données d'événement ne restent pas dans les files d'attente. Vous devez donc vous assurer que les destinations en aval des données d'événement (Log Collectors, Virtual Log Collectors et Log Decoders) sont actives et fonctionnent correctement.

   Si vous disposez de destinations de données d'événements en aval dans le Log Decoder, vous devez préparer et mettre à niveau les Log Collectors dans l'ordre suivant.

   a. LD (un LD à la fois)

   b. VLC et LWC

   Si vous n'avez pas de destinations de données d'événements en aval dans le Log Decoder, vous pouvez préparer et mettre à niveau plusieurs LD VLC et LWC en même temps.
5. Pour tous les autres hôtes

Reportez-vous à la section « Exécution en mode mixte » sous « Les bases » dans le *RSA NetWitness Suite - Guide de mise en route des hôtes et des services* pour :

- Les difficultés rencontrées lors de l'exécution dans ce mode.
- Exemples de mises à niveau échelonnées.

Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

Procédure d'enquête en mode mixte

Le mode mixte est opérationnel lorsque certains services sont mis à niveau vers la version 11.1 et d'autres sont toujours sur la version 10.6.5. Cela se produit lorsque la mise à niveau vers la version 11.1 est effectuée en plusieurs phases.

Remarque : Vous devez suivre la séquence de mise à niveau des hôtes, comme indiqué dans la section Phases de mise à niveau afin de garantir le bon fonctionnement de l'intégralité des fonctions de la procédure d'enquête. Le serveur Investigate version 11.1 est installé lors de la mise à niveau du serveur SA, mais les hôtes Broker doivent être mis à niveau vers la version 11.1 pour accéder à la vue Analyse d'événements. Si le service Broker n'est pas mis à niveau, les analystes voient une icône d'avertissement en regard du Broker et aucune donnée agrégée à ce service ne peut être affichée.

Après avoir effectué la mise à niveau de tous les services vers la version 11.1, lorsqu'un analyste mène une procédure d'enquête, le contrôle d'accès basé sur les rôles (RBAC) des téléchargements fonctionne correctement afin de limiter l'accès aux données restreintes.

En mode mixte (autrement dit, lorsque certains services sont mis à niveau vers la version 11.1 et d'autres sont encore sur la version 10.6.5), lorsqu'un analyste mène une procédure d'enquête, le RBAC n'est pas appliqué uniformément à l'affichage et aux téléchargements.

Si le paramètre `sdk.packets` n'a pas été désactivé sur les services de la version 10.6.x, les analystes disposant des autorisations de rôle méta SDK mis en place pour limiter l'affichage et la reconstruction du contenu d'un événement peuvent télécharger le fichier PCAP d'un événement dont le contenu est restreint. D'autres types de téléchargements semblent réussis, puis génèrent des erreurs en raison d'un manque d'autorisations et les données restent protégées.

Au cours d'une mise à jour par phases, vous pouvez désactiver le paramètre `sdk.packets` des services de la version 10.6.x afin d'empêcher l'analyste de télécharger des PCAP ou des logs en mode mixte. Après la mise à jour de tous les services vers la version 11.1 et la réactivation de `sdk.packets`, RBAC fonctionne correctement entre tous les services.

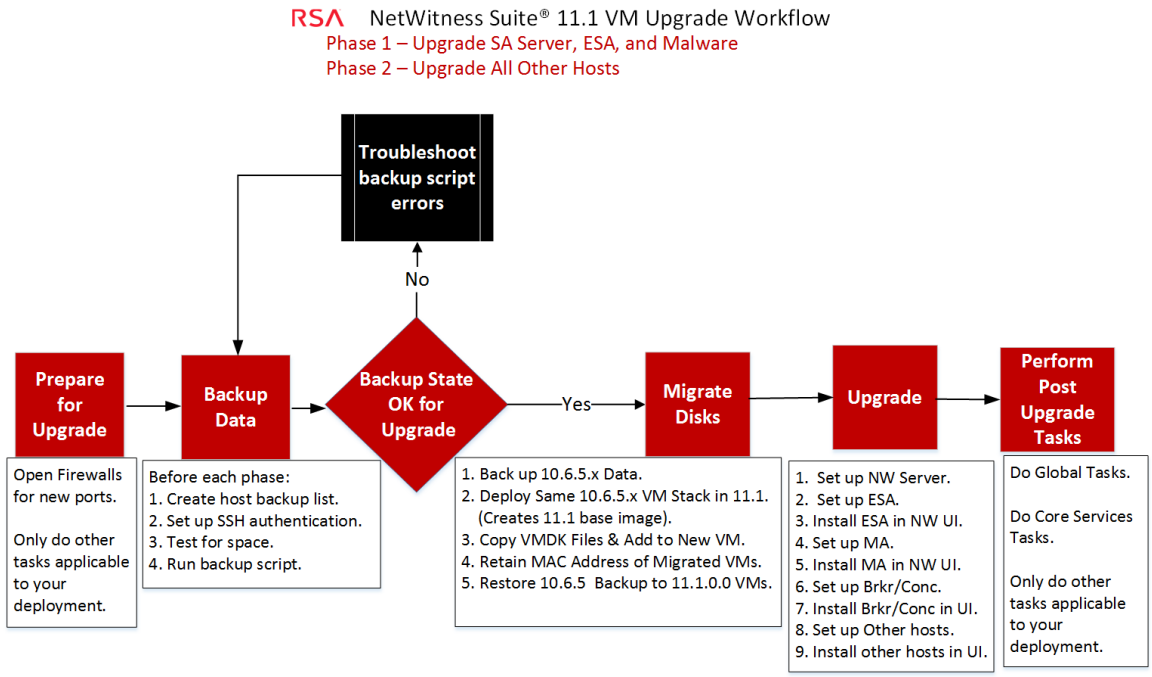
Le tableau suivant identifie ce que vous pouvez voir et télécharger dans la procédure d'enquête lorsque votre serveur NW est sur la version 11.1 connecté aux services d'une version inférieure.

Connecter la version du service	Vue concernée	Rôle d'utilisateur avec contenu à accès restreint	Autorisation d'affichage	Autorisation de téléchargement du contenu à accès restreint	Autorisation de téléchargement du contenu à accès restreint avec des erreurs
11.1 Broker -> 10.6.5.x Concentrator -> 10.6.5.x Packet Decoder/Log Decoder	Vue Événements	Analyste	Éléments RBAC autorisés	PCAP	Le fichier d'archive est téléchargé mais ne peut pas être décompressé
	Vue Reconstruction d'événement	Analyste	Éléments RBAC autorisés	PCAP	Le fichier d'archive est téléchargé mais ne peut pas être décompressé
	Vue Analyse d'événements	Analyste	Éléments RBAC autorisés	PCAP	Erreur lors de la récupération de la charge utile du service pour la charge utile, charge utile de la demande, charge utile de la réponse

Connecter la version du service	Vue concernée	Rôle d'utilisateur avec contenu à accès restreint	Autorisation d'affichage	Autorisation de téléchargement du contenu à accès restreint	Autorisation de téléchargement du contenu à accès restreint avec des erreurs
11.1 Broker -> 11.1 Concentrator ->11.1 Decoder/Log Decoder	Vue Reconstruction d'événement	Analyste et responsable de la confidentialité des données	Éléments RBAC autorisés	PCAP	Le fichier d'archive est téléchargé mais ne peut pas être décompressé la taille des PCAP et des logs téléchargés est de zéro octet

Connecter la version du service	Vue concernée	Rôle d'utilisateur avec contenu à accès restreint	Autorisation d'affichage	Autorisation de téléchargement du contenu à accès restreint	Autorisation de téléchargement du contenu à accès restreint avec des erreurs
11.1 Broker -> 11.0.0.x Concentrator -> 11.0.0.x Packet Decoder/Log Decoder	Vue Événements	Analyste	Éléments RBAC autorisés	Aucun(e)	Le fichier d'archive est téléchargé mais ne peut pas être décompressé Les fichiers PCAP et les logs sont téléchargés sous la forme de zéro octet
	Vue Reconstruction d'événement	Analyste	Éléments RBAC autorisés	Aucun(e)	Le fichier d'archive est téléchargé mais ne peut pas être décompressé Les fichiers PCAP et les logs sont téléchargés sous la forme de zéro octet

Connecter la version du service	Vue concernée	Rôle d'utilisateur avec contenu à accès restreint	Autorisation d'affichage	Autorisation de téléchargement du contenu à accès restreint	Autorisation de téléchargement du contenu à accès restreint avec des erreurs
	Vue Analyse d'événements	Analyste	Éléments RBAC autorisés	Aucun(e)	Erreur lors de la récupération de la charge utile du service pour la charge utile, charge utile de la demande, charge utile de la réponse Les fichiers PCAP et les logs sont téléchargés sous la forme de zéro octet



Contacter le support client

Reportez-vous à la page Contacter le support client RSA (https://community.rsa.com/docs/DOC-1294) dans RSA Link pour plus d'informations sur la manière d'obtenir de l'aide sur RSA NetWitness Suite version 11.1.

Tâches de préparation de la mise à niveau

Effectuez les tâches suivantes pour préparer la mise à niveau vers NetWitness Suite 11.1. Ces tâches sont organisées selon les catégories suivantes.

- Global
- Respond
- Reporting Engine

Global

Vous devez effectuer ces tâches, quelle que soit la façon dont vous déployez NetWitness Suite et les composants que vous utilisez.

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

Les tableaux suivants répertorient les nouveaux ports dans la version 11.1.

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

Hôte de serveur NW

Hôte source	Hôte de destination	Ports de destination	Commentaires
Hôtes NW	Serveur NW	TCP 4505, 4506	Ports Salt Master
Hôtes NW	Serveur NW	TCP 27017	MongoDB

Hôte ESA

Hôte source	Hôte de destination	Ports de destination	Commentaires
Serveur NW, NW Endpoint, ESA secondaire	ESA primaire	TCP 27017	MongoDB

Endpoint Hybrid ou Endpoint Log Hybrid

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

Hôte source	Hôte de destination	Ports de destination	Commentaires
Serveur Endpoint	Serveur NW	TCP 27017	MongoDB

Tous les ports de base NetWitness Suite sont répertoriés dans la rubrique « Architecture réseau et Ports » dans le *RSA NetWitness® Suite Guide de déploiement* au cas où la reconfiguration des pare-feu et des services NetWitness Suite serait nécessaire. Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

Tâche 2 - Enregistrer votre mot de passe `admin user` de la version 10.6.5.x

Enregistrez votre mot de passe `admin user` de la version 10.6.5.x. Vous en aurez besoin pour effectuer la mise à niveau.

Tâche 3 - Créer une sauvegarde du fichier `/etc/fstab`

Copiez le fichier `/etc/fstab` depuis toutes les machines virtuelles sur votre machine locale (l'hôte de sauvegarde ou la machine distante).

Remarque : Vous avez besoin de ce fichier pour restaurer une machine virtuelle avec les montages de stockage externe.

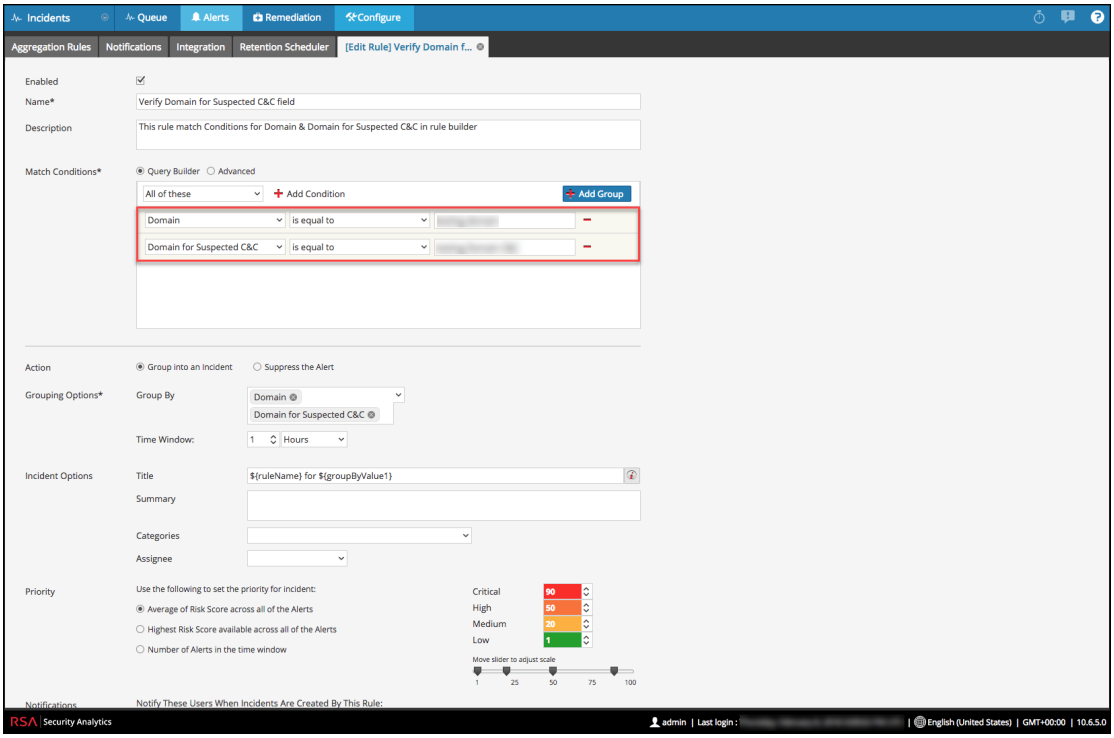
Respond

Tâche 4 : Vérifier les conditions de mise en correspondance des règles d'agrégation pour « Domaine » ou « Domaine de C&C suspect »

Notez les règles d'agrégation pour la gestion des incidents ayant des conditions de mise en correspondance à l'aide du domaine ou du domaine pour C&C suspect dans la liste déroulante du générateur de règles. Dans NetWitness Suite 11.1, vous devrez modifier ces règles pour utiliser le domaine après la mise à niveau vers la version 11.1, comme indiqué dans les tâches postérieures à la mise à niveau de Respond.

Vérifiez les éléments suivants pour chaque règle d'agrégation :

1. Dans le menu Security Analytics 10.6.5.x, sélectionnez **Incidents** > **Configurer** > onglet **Règles d'agrégation**, puis modifiez les règles pour afficher les conditions de mise en correspondance.
2. Dans la section **Conditions de mise en correspondance**, recherchez **Domaine** ou **Domaine de C&C suspect** répertoriés dans les listes déroulantes des conditions.



3. Notez le nom de la règle et la condition entière qui utilise **Domaine** ou **Domaine de C&C suspect**, y compris les opérateurs et les valeurs.

Reporting Engine

(Conditionnel) Tâche 5 - Dissocier le stockage externe

Si le Reporting Engine possède un stockage externe [tels qu'un réseau de stockage (SAN) ou un stockage rattaché au réseau (NAS) pour stocker les rapports], vous devez effectuer les opérations suivantes pour dissocier le stockage.

Dans les étapes suivantes :

- `/home/rsasoc/rsa/soc/reporting-engine/` est le répertoire de base du Reporting Engine.
- `/externalStorage/` correspond à l'emplacement où le stockage externe est monté.

1. Ouvrez une session SSH sur l'hôte Reporting Engine et saisissez vos informations d'identification `root` .
2. Arrêtez le service Reporting Engine.
   ```
   stop rsasoc_re
   ```
3. Passez à l'utilisateur `rsasoc`.
   ```
   su rsasoc
   ```
4. Modifiez pour passer au répertoire de base du Reporting Engine.
   ```
   cd /home/rsasoc/rsa/soc/reporting-engine/
   ```
5. Dissociez le répertoire `resultstore` monté sur le stockage externe.
   ```
   unlink /externalStorage/resultstore
   ```
6. Dissociez le répertoire `formattedReports` monté sur le stockage externe.
   ```
   unlink /externalStorage/formattedReports
   ```

Instructions de sauvegarde

La sauvegarde de vos données de configuration pour tous vos hôtes de la version 10.6.5.x est la première étape de la mise à niveau de Security Analytics 10.6.5.x vers NetWitness Suite 11.1.

Remarque : Vous devez impérativement placer les fichiers de certificat personnalisé et les fichiers de n'importe quelle autre autorité de certification (AC) dans le dossier `/root/customcerts` afin de garantir la sauvegarde de ces fichiers de certificat. Vos fichiers de certificat personnalisé placés dans ce répertoire seront restaurés automatiquement au cours du processus de mise à niveau. Après la mise à niveau vers la version 11.1, vos fichiers de certificat personnalisé seront situés dans `/etc/pki/nw/trust/import`. Pour plus d'informations sur la sauvegarde de ces types de fichiers, reportez-vous à l'étape 1 dans Pour tous les types d'hôte.

Attention : Ces services ne sont pas pris en charge dans le processus de mise à niveau et de sauvegarde 10.6.5.x.
- IPDB
- Serveurs tout-en-un
- Malware Analysis co-localisé sur le serveur Security Analytics
- Warehouse Connector autonome
- Warehouse Analytics (Datascience)

Les types d'hôtes suivants peuvent être sauvegardés et sont automatiquement restaurés au cours du processus de mise à niveau :

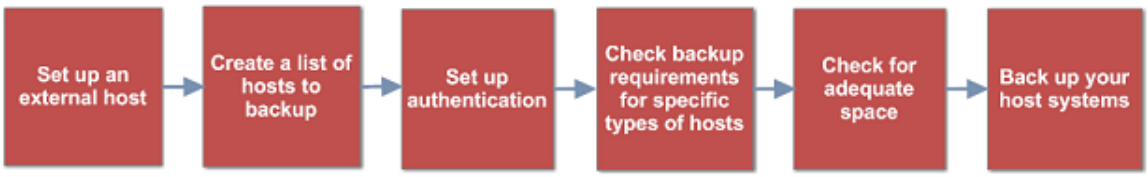
- **Serveur d'administration Security Analytics** (pouvant inclure Malware Analysis, Incident Management, Intégrité et Reporting Engine)
- **Malware Analysis** (autonome)
- **Archiver**
- **Broker**
- **Event Stream Analysis** (y compris la base de données de gestion des incidents et Context Hub)
- **Concentrator**
- **Log Decoder** (y compris le Log Collector local et Warehouse Connector, si installés)
- **Log Hybrid**
- **Packet Decoder** (y compris Warehouse Connector, si installé)

- **Packet Hybrid**
- **Virtual Log Collector**

Les types de fichiers suivants sont automatiquement sauvegardés, mais doivent être restaurés manuellement après le processus de mise à niveau :

- Fichiers de configuration PAM : Pour plus d'informations sur la restauration des fichiers de configuration PAM, reportez-vous à la « Tâche 5 - Reconfigurer le module PAM (Pluggable Authentication Module) dans la version 11.1. », dans la section « Global » des **Tâches postérieures à la mise à niveau**.
- `/etc/pfring/mtu.conf` et `/etc/init.d/pf_ring` : Pour restaurer ces fichiers, vous devez les récupérer manuellement. Les fichiers `/etc/pfring/mtu.conf` se trouvent dans `/var/netwitness/database/nw-backup/restore/etc/pfring/mtu.conf` et les fichiers `/etc/init.d/pf_ring` dans `/var/netwitness/database/nw-backup/restore/etc/init.d/pf_ring`. Pour plus d'informations sur la façon de restaurer ces fichiers, reportez-vous à « (Conditionnel) Tâche 2 - Restaurer des fichiers pour 10G Decoder » dans la section « Tâches associées au matériel » sous **Tâches postérieures à la mise à niveau**.

Le schéma suivant illustre par étapes le flux des tâches générales à effectuer pour sauvegarder vos hôtes.



Les sections suivantes décrivent ces tâches :

- Tâche 1 - Configurer un hôte externe pour la sauvegarde des fichiers
- Tâche 2 - Créer une liste des hôtes à sauvegarder
- Tâche 3 - Configurer l'authentification entre les hôtes de sauvegarde et les hôtes cibles
- Tâche 4 - Vérifier les conditions requises pour certains types d'hôtes en matière de sauvegarde
- Tâche 5 - Vérifier que vous disposez de suffisamment d'espace pour la sauvegarde
- Tâche 6 - Sauvegarder vos systèmes hôte
- Tâches postérieures à la sauvegarde

Tâche 1 - Configurer un hôte externe pour la sauvegarde des fichiers

Vous devez configurer un hôte externe à utiliser pour la sauvegarde des fichiers. L'hôte doit exécuter CentOS 6 avec une connectivité à la pile d'hôtes Security Analytics via le protocole SSH.

Remarque : Si vous n'êtes pas en mesure d'utiliser un hôte externe pour la sauvegarde des fichiers, contactez le support client RSA (https://community.rsa.com/docs/DOC-1294) pour obtenir une assistance.

Assurez-vous que les noms d'hôtes pour les systèmes à sauvegarder peuvent être résolus sur la machine hôte de sauvegarde, soit par DNS ou répertoriés dans le fichier `/etc/hosts`.

Remarque : Ces scripts sont conçus pour être exécutés uniquement sur CentOS 6. Vous devez exécuter ces scripts sur des machines CentOS 6.

Il existe plusieurs scripts à exécuter lors du processus de sauvegarde. Vous devez télécharger le fichier zip contenant les scripts (`nw-backup-v4.0.sh`) à partir de RSA Link à l'emplacement suivant : https://community.rsa.com/docs/DOC-81514 et le copier sur votre système de sauvegarde CentOS 6. Décompressez le fichier zip pour accéder aux scripts. Les scripts sont les suivants :

- `get-all-systems.sh` : Crée le fichier `all-systems` contenant la liste de tous vos serveurs et systèmes hôtes Security Analytics à sauvegarder.
- `ssh-propagate.sh` : Automatise le partage de clés entre les systèmes à sauvegarder et le système hôte de sauvegarde afin de ne pas être invité(e) à saisir vos mots de passe plusieurs fois.
- `nw-backup.sh` : Effectue la sauvegarde de vos hôtes.
- `azure-mac-retention.ps1` : S'applique uniquement si vous utilisez AZURE. Consultez le *Guide de déploiement d'AZURE* Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x. pour plus d'informations.

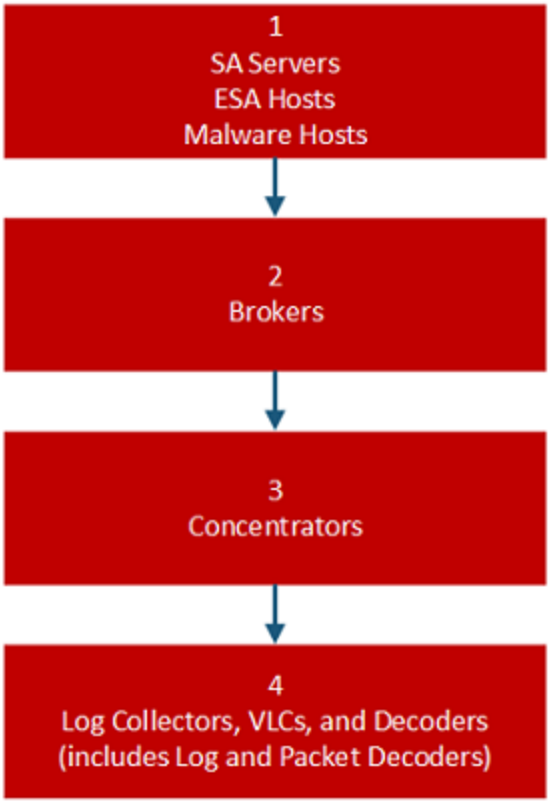
Remarque : Si vous avez utilisé les versions 10.6.x des scripts de sauvegarde et de restauration sur vos hôtes 10.6.5, vous devez toujours exécuter tous les scripts répertoriés ici.

Remarque : N'utilisez pas les scripts dans le fichier `nw-backup-v4.0.zip` pour les sauvegardes normales. Ces scripts sont conçus pour la mise à niveau à partir de la version 10.6.5.x vers la version 11.1.

Remarque : Les scripts de sauvegarde ne prennent pas en charge la sauvegarde des données pour les hôtes auquel un renforcement STIG a été appliqué.

Tâche 2 - Créer la liste des hôtes à sauvegarder

Le script utilisé pour la sauvegarde de vos fichiers dépend des fichiers `all-systems` et `all-systems-master-copy` contenant la liste des hôtes que vous souhaitez sauvegarder. Le fichier `all-systems-master-copy` contient la liste de tous vos hôtes. Le fichier `all-systems` est utilisé pour chaque session de sauvegarde et il contient uniquement les hôtes qui sont en cours de sauvegarde pour une session donnée. Exécutez le script `get-all-systems.sh` pour générer ces fichiers. RSA vous recommande de sauvegarder vos hôtes par groupes, plutôt que tous à la fois. L'ordre recommandé et le regroupement des hôtes pour les sessions de sauvegarde est présenté dans le schéma suivant :



Limitez chaque séance de sauvegarde à cinq hôtes afin de garantir un espace suffisant pour les fichiers de sauvegarde. Créez des fichiers `all-systems` pour vos sessions de sauvegarde en utilisant le fichier `all-systems-master-copy` comme référence, puis en modifiant manuellement le fichier `all-systems` pour qu'il contienne les hôtes spécifiques.

Pour générer les fichiers `all-systems` et `all-systems-master-copy` :

1. À partir de l'hôte sur lequel vous exécutez le processus de sauvegarde, convertissez le script `get-all-systems.sh` en exécutable avec la commande suivante :
   `chmod u+x get-all-systems.sh`
2. Au niveau racine, exécutez le script `get-all-systems.sh` :
   `./get-all-systems.sh <IP-Address-of-SA-Admin-Server>`
   Vous serez invité(e) à saisir le mot de passe pour chaque système hôte une fois par hôte.

Ce script enregistre les fichiers `all-systems` et `all-systems-master-copy` à l'emplacement `/var/netwitness/database/nw-backup/`.

3. Vérifiez que les fichiers `all-systems` et `all-systems-master-copy` ont été générés et qu'ils contiennent les hôtes appropriés.
4. Modifiez le fichier `all-systems` pour qu'il contienne uniquement les systèmes que vous sauvegardez. Pour ce faire, utilisez le fichier `all-systems-master-copy` comme référence, puis ouvrez le fichier `all-systems` dans un éditeur (tel que vi) et modifiez-le pour inclure uniquement les systèmes que vous souhaitez sauvegarder. RSA vous recommande de commenter les hôtes que vous ne souhaitez pas sauvegarder (ajoutez le signe dièse (#) au début de la ligne contenant l'hôte qui ne sera pas sauvegardé).
   Les exemples suivants montrent comment commenter la version 10.6.5 du serveur Security Analytics :
   `loghybrid,loghyb,172.16.0.1,45fe9de1-1a82-49d7-9bb1-7ac5fa1d18d8,10.6.5.0`
   `#nwserver,nwserv106,172.31.255.23,67a9a0eb-1300-4fba-838f-7be4d8cf5e65,10.6.5.0`

   Remarque : Si vous utilisez vi, veillez à inclure le chemin d'accès à l'emplacement du fichier `all-systems`.

Voici un exemple de fichier `all-systems-master-copy` :

`nwserver,`*`my-nw-server`*`,10.0.0.1,af922b9f-cd61-49cd-afdc-a48e558cec3e,10.6.5.0`
`archiver,`*`my-nw-archiver`*`,10.0.0.2,a65c1236-5e46-4117-8529-8ea837074bd0,10.6.5.0`
`concentrator,`*`my-nw-concentrator`*`,10.0.0.3,dc620e94-bcf5-4d51-83fe-c003cdfcd7a6,10.6.5.0`
`esa,`*`my-nw-esa`*`,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.5.0`
`logdecoder,`*`my-nw-logdecoder`*`,10.0.0.5,c8be5d45-e19e-4a8d-90ce-1cb2fe60077a,10.6.5.0`
`malwareanalysis,`*`my-nw-malwareanalysis`*`,10.0.0.6,2edc9585-7081-48c3-8f8c-e0d02aa0a2fd,10.6.5.0`
`packetdecoder,`*`my-nw-packetdecoder`*`,10.0.0.7,a8f2f574-3dd0-4b65-9cf7-d8141b78a192,10.6.5.0`
`vlc,`*`my-nw-vlc`*`,10.0.0.8,3ffefc4e-0b31-4951-bb77-dea5869fa98c,10.6.5.0`
`broker,`*`my-nw-broker`*`,10.0.0.9,0b65e7ce-61d5-4177-9647-c56ccfb0f737,10.6.5.0`

Et voici un exemple de fichier `all-systems` qui pourrait être utilisé dans la première session de sauvegarde, où seul le serveur Security Analytics, l'hôte ESA et l'hôte Malware Analysis sont sauvegardés :

```
nwserver,my-nw-server,10.0.0.1,af922b9f-cd61-49cd-afdc-
a48e558cec3e,10.6.5.0
#archiver,my-nw-archiver,10.0.0.2,a65c1236-5e46-4117-8529-
8ea837074bd0,10.6.5.0
#concentrator,my-nw-concentrator,10.0.0.3,dc620e94-bcf5-4d51-83fe-
c003cdfcd7a6,10.6.5.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.5.0
#logdecoder,my-nw-logdecoder,10.0.0.5,c8be5d45-e19e-4a8d-90ce-
1cb2fe60077a,10.6.5.0
malwareanalysis,my-nw-malwareanalysis,10.0.0.6,2edc9585-7081-48c3-8f8c-
e0d02aa0a2fd,10.6.5.0
#packetdecoder,my-nw-packetdecoder,10.0.0.7,a8f2f574-3dd0-4b65-9cf7-
d8141b78a192,10.6.5.0
#vlc,my-nw-vlc,10.0.0.8,3ffefc4e-0b31-4951-bb77-dea5869fa98c,10.6.5.0
#broker,my-nw-broker,10.0.0.9,0b65e7ce-61d5-4177-9647-
c56ccfb0f737,10.6.5.0
```

Informations de dépannage

- Veillez à enregistrer les copies des fichiers `all-systems` et `all-systems-master-copy` à un emplacement sécurisé. Suivez les recommandations suivantes :
  - Ne modifiez pas le fichier `all-systems-master-copy`.
  - Si vous créez plusieurs versions différentes du fichier `all-systems` (par exemple, pour plusieurs sessions de sauvegarde), assurez-vous que chaque version du fichier ne répertorie que les hôtes en cours de sauvegarde et que les autres hôtes font l'objet d'un commentaire.
    Pour plus d'informations, reportez-vous à la rubrique Tâches postérieures à la sauvegarde.
- Si des systèmes hôte sont arrêtés pendant l'exécution du script `get-all-systems.sh`, le script crée la liste des hôtes pour lesquels il ne trouve pas d'informations. Une fois le script terminé et le fichier `all-systems` créé, vous devez modifier manuellement le fichier `all-systems` et ajouter les informations manquantes pour ces hôtes.
- Le script `get-all-systems.sh` génère la liste des hôtes définis dans l'interface utilisateur Security Analytics. Assurez-vous que tous les hôtes et les services sont provisionnés correctement. Si des hôtes ou des services ne sont pas provisionnés correctement, ils ne seront pas sauvegardés. RSA vous recommande d'utiliser l'interface utilisateur Security Analytics lorsque vous ajoutez des hôtes et des services à Security Analytics, pour vous assurer qu'ils sont correctement provisionnés. Toutefois, si des hôtes ou des services n'ont pas

été définis dans l'interface utilisateur, vous devez les ajouter manuellement au fichier `all-systems`.

- À la fin du script `get-all-systems.sh`, le script vérifiera les différences entre les systèmes répertoriés par le serveur Security Analytics et ceux pour lesquels toutes les informations requises ont pu être trouvées. Si des noms de nœuds ou de systèmes sont signalés comme manquants, vérifiez l'existence de ces systèmes, que leurs services sont tous en cours d'exécution, et qu'ils communiquent correctement avec le serveur Security Analytics. (Ni les Collectors Windows d'ancienne génération, ni les collecteurs Cloud AWS ne seront ajoutés au fichier `all-systems` et ils peuvent représenter les différences. **N'AJOUTEZ PAS ces éléments manuellement au fichier `all-systems`.**)
- Si la syntaxe du fichier `all-systems` est incorrecte, le script échoue. Par exemple, s'il existe un espace supplémentaire au début ou à la fin d'une entrée d'hôte, le script échoue.

Tâche 3 - Configurer l'authentification entre les hôtes de sauvegarde et les hôtes cibles

RSA vous recommande d'exécuter le script `ssh-propagate.sh` pour automatiser le partage de clés entre l'hôte de sauvegarde et les systèmes hôtes.

Remarque : Si vous disposez de clés SSH protégées par des phrases de passe, vous pouvez utiliser `ssh-agent` pour gagner du temps. Pour plus d'informations, reportez-vous à la page man pour `ssh-agent`.

1. Sur le système hôte de sauvegarde externe, convertissez le script `ssh-propagate.sh` en exécutable avec la commande suivante :
   `chmod u+x ssh-propagate.sh`
2. Dans le répertoire racine, exécutez la commande suivante, où `<path-to-all-systems-file>` est le chemin d'accès au répertoire dans lequel le fichier `all-systems` est stocké :
   `ssh-propagate.sh <path-to-all-systems-file>`
3. Vous serez invité(e) à saisir le mot de passe une seule fois par hôte, mais vous n'aurez plus à le faire au cours du processus de sauvegarde.

Tâche 4 - Vérifier les conditions requises pour certains types d'hôtes en matière de sauvegarde

Après avoir créé le fichier `all-systems` à utiliser pour la sauvegarde, vous devez vérifier si les hôtes répertoriés doivent remplir des conditions précises avant d'exécuter le processus de sauvegarde.

Pour tous les types d'hôtes

Pour tous les types d'hôtes, procédez comme suit :

1. Sur le serveur Security Analytics, placez les fichiers de certificat personnalisé et les fichiers de n'importe quelle autre autorité de certification (AC) dans le dossier `/root/customcerts` afin de garantir la sauvegarde de ces fichiers de certificat. Vos fichiers de certificat personnalisé placés dans ce répertoire seront restaurés automatiquement au cours du processus de mise à niveau. Après la mise à niveau vers la version 11.1., vos fichiers de certificat personnalisé se trouveront dans `/etc/pki/nw/trust/import`.
   Vous pouvez convertir les certificats et clés d'autorité de certification en différents formats pour les rendre compatibles avec des types de serveurs ou de logiciels spécifiques à l'aide

d'OpenSSL. Par exemple, vous pouvez convertir un fichier PEM normal fonctionnant avec Apache en un fichier PFX (PKCS #12) et l'utiliser avec Tomcat ou IIS. Pour convertir les fichiers, ouvrez une session SSH pour le serveur Security Analytics et effectuez les chaînes de commande suivantes pour exécuter les conversions répertoriées.

Convertir un fichier DER (.crt .cer .der) au format PEM

```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

Convertir un fichier PEM au format DER

```
openssl x509 -outform der -in certificate.pem -out certificate.der
```

Convertir un fichier de certificat PEM et une clé privée au format PKCS #12 (.pfx .p12)

```
openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in certificate.crt -certfile CACert.crt
```

Convertir un fichier PKCS #12 (.p12 .pfx) contenant une clé privée et des certificats au format PEM

```
openssl pkcs12 -in keyStore.pfx -out keyStore.pem -nodes
```

> **Remarque :** Ajoutez le qualificateur suivant à la chaîne de commande :
> `-nocerts` pour convertir exclusivement des clés privées.
> `-nokeys` pour convertir exclusivement des certificats.

2. Enregistrez manuellement toutes les configurations personnalisées apportées à CentOS 6 (par exemple, les personnalisations de pilote) pour les restaurer après la mise à jour vers CentOS 7. Les configurations personnalisées apportées à CentOS 6 ne sont pas sauvegardées ni restaurées automatiquement.

Pour les hôtes ESA avec bases de données Mongo

Le mot de passe par défaut de la base de données Mongo 10.6.x est `netwitness`. Si vous avez personnalisé ce mot de passe, vous risquez de rencontrer une erreur lors de l'exécution du script de sauvegarde. Vous pouvez utiliser votre mot de passe de base de données Mongo personnalisé lors de la sauvegarde, ou vous pouvez rétablir le mot de passe `netwitness` avant d'exécuter le script `nw-backup.sh`.

1. Déterminez si le mot de passe de la base de données Mongo est `netwitness` ou s'il a été modifié.
2. S'il a été modifié, remplacez-le par `netwitness`, ou assurez-vous de connaître le mot de passe personnalisé afin de pouvoir le saisir lors de la sauvegarde.

Reportez-vous à la rubrique « Configuration d'ESA : Modifier le mot de passe MongoDB pour le compte administrateur » dans le *Guide de configuration de NetWitness Suite Event Stream Analysis*. Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

Pour les hôtes Broker, Concentrator ou Decoder : Arrêter la capture et l'agrégation des données

Outre les tâches décrites dans Pour tous les types d'hôte, pour les hôtes de Decoder, Concentrator ou Broker, arrêtez la capture et l'agrégation des données sur tous les systèmes que vous sauvegardez. Pour savoir comment procéder, reportez-vous à la section Annexe B. Arrêter et redémarrer la capture et l'agrégation des données

Log Collectors (LC) et Virtual Log Collectors (VLC) : Exécutez `prepare-for-migrate.sh`

Attention : Cette tâche arrête la collecte des logs. Vous devez donc effectuer cette étape immédiatement avant la mise à niveau afin de réduire la perte de collecte des événements. Effectuez cette tâche conformément aux tâches de sauvegarde et de mise à niveau indiquées dans le présent guide.

Conditions préalables

Les informations suivantes sont nécessaires avant de préparer les LC et les VLC pour la mise à niveau.

- Si le Lockbox a été initialisé sur le LC et VLC, vous devez connaître le mot de passe Lockbox. Il est nécessaire de reconfigurer le Lockbox après la mise à niveau.
- Si vous définissez le mot de passe utilisateur `logcollector` pour RabbitMQ, vous devez connaître le mot de passe pour le redéfinir après la mise à niveau.

Préparer les LC et VLC pour la mise à niveau

1. Ouvrez une session SSH sur le Log Collector.
2. Exécutez la chaîne de commande suivante.

   ```
   # /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --prepare
   ```

   Cette commande :

   - Arrête le service Agent Puppet.
   - Désactive les comptes de collecte des fichiers (« sftp » et tous les utilisateurs du groupe « téléchargement ») utilisés pour télécharger les fichiers log dans le Log Collector. Les fichiers log s'accumulent dans les sources d'événements jusqu'à ce que le Log Collector soit mis à niveau vers la version 11.1.

- Arrête tous les protocoles de collecte dans le service Log Collector.
- Enregistre la liste des comptes de plug-in et des comptes RabbitMQ.
- Configure le serveur RabbitMQ afin que les nouveaux événements n'y soient plus publiés. Les consommateurs d'événements dans les files d'attente, tels que les « shovels » et les Log Decoder Event Processors, continuent à s'exécuter.
- Attend que les files d'attente du Log Collector soient vides.
- Arrête le service Log Collector.
- Crée un fichier marqueur indiquant que le Log Collector a été correctement préparé pour la mise à niveau.

Informations de dépannage

Le script `prepare-for-migrate.sh` :

- Envoie des messages d'information, d'avertissement et d'erreur à la console.
- Enregistre le log de la session dans le répertoire `/var/log/backup/`.

Vous devez corriger les erreurs suivantes et reprendre la préparation. Contactez le support client RSA (https://community.rsa.com/docs/DOC-1294) pour obtenir de l'aide.

- Les files d'attente du Log Collector avec des événements, mais sans consommateurs sont disponibles.
- Impossible d'arrêter le service Puppet Agent.
- Impossible d'arrêter un protocole de collecte dans le service Log Collector.
- Impossible de bloquer les éditeurs d'événements vers le serveur RabbitMQ.
- Impossible d'utiliser les événements dans la file d'attente, ou processus trop long. Le script effectue 30 tentatives en attendant que les événements soient utilisés. Après chaque tentative, il est en veille pendant 30 secondes.
- Impossible d'arrêter le service Log Collector.

Pour plus d'informations sur la résolution des problèmes, reportez-vous à la section Annexe A. Dépannage.

Pour l'intégration avec Web Threat Detection, NetWitness SecOps Manager ou NetWitness Endpoint : Répertorier les noms d'utilisateur et les mots de passe RabbitMQ

Sur l'hôte 10.6.5.x, sur l'hôte du serveur Security Analytics, vous devez obtenir la liste de tous les mots de passe et noms d'utilisateur RabbitMQ afin de pouvoir restaurer les comptes d'utilisateur RabbitMQ une fois la mise à niveau vers la version 11.1 effectuée.

Pour obtenir la liste des mots de passe et des noms d'utilisateur RabbitMQ, exécutez la commande suivante :

```
rabbitmqctl list_users >> /root/rabbitmq_users.txt
```

Pour restaurer des comptes d'utilisateur RabbitMQ, reportez-vous à la section *Tâche 2 - Pour l'intégration avec Web Threat Detection, NetWitness SecOps Manager ou NetWitness Endpoint Configure Mutually Authenticated SSL* dans **Tâches postérieures à la mise à niveau**.

Pour Sources d'événements Bluecoat

Les sources d'événements Bluecoat ProxySG utilisent le protocole FTPS pour télécharger des fichiers log dans le Log Collector (LC) et dans le Virtual Log Collector (VLC). La documentation relative à la source d'événement contient les étapes de configuration du service VSFTPD dans VLC et LC.

- Si des informations sur les clés figurent dans le répertoire `/root/vsftpd/` de la version 10.6.5.x, elles seront sauvegardées et restaurées. **Si le matériel se trouvait à un autre emplacement, vous devez le sauvegarder et le restaurer manuellement.**
- Si le fichier `/etc/vsftpd/vsftpd.conf` existe dans la version 10.6.5.x, il est sauvegardé et restauré.

Tâche 5 - Vérifier que vous disposez de suffisamment d'espace pour la sauvegarde

Vous pouvez exécuter le script de test de sauvegarde pour vérifier l'espace disque requis pour la sauvegarde à l'aide de l'option `-t` décrite dans Tester des options. Exécutez le script sans réellement sauvegarder les fichiers ou arrêter les services. RSA vous conseille d'effectuer cette étape pour vous assurer d'avoir suffisamment d'espace pour la sauvegarde de sorte que toutes vos données soient prises en compte.

Pour vérifier l'espace disque suffisant :

1. Convertissez le script en exécutable à l'aide de la commande suivante :
   ```
   chmod u+x nw-backup.sh
   ```

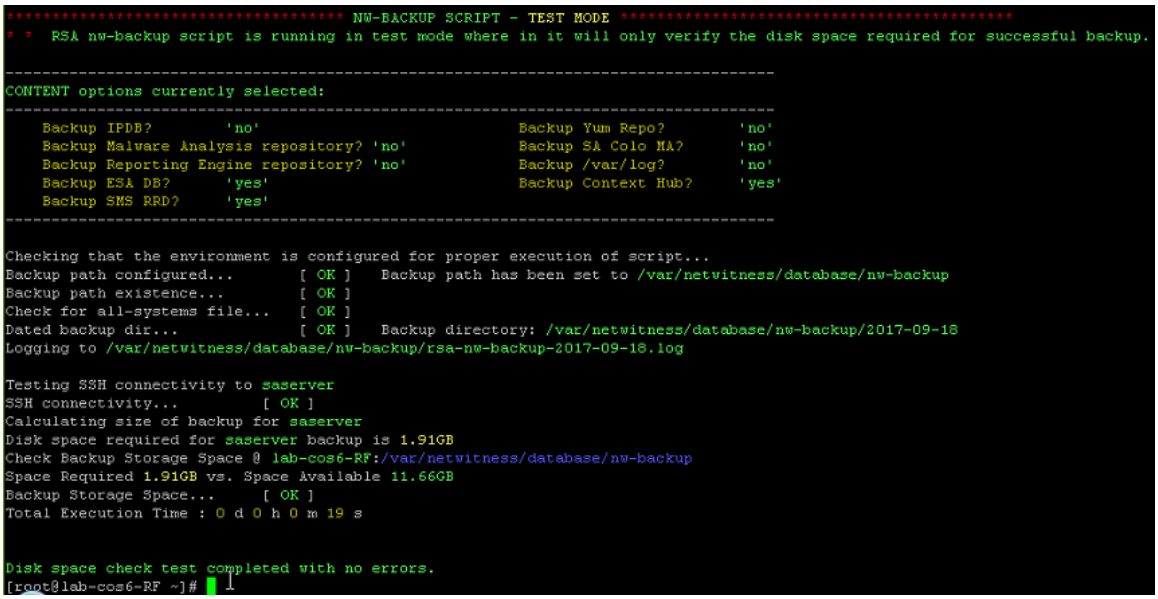
2. Exécutez la commande suivante au niveau du répertoire racine :

   `./nw-backup.sh -t`

   Le résultat affiche la quantité d'espace disque requise pour la sauvegarde.

> **Remarque :** La commande `./nw-backup.sh -t` s'exécute avec l'option `-d` par défaut. Toutefois, si vous recherchez des résultats plus précis pour l'espace disque, vous pouvez remplacer l'option `-d` par `-D`. L'option `-D` permet d'afficher la quantité d'espace requise sur chaque hôte pour les données qui seront sauvegardées, mais elle n'affiche pas la quantité d'espace disponible. S'il n'y a pas suffisamment d'espace disponible, l'option `-D` génère une erreur. Si vous souhaitez connaître la quantité d'espace disponible sur l'hôte cible, vous devez exécuter la commande `df -h` sur l'hôte.

Voici un exemple illustrant les résultats obtenus à l'aide de l'option `-t`.



Tâche 6 - Sauvegarder vos systèmes hôtes

Avant d'exécuter le script de sauvegarde pour effectuer la sauvegarde réelle, assurez-vous d'avoir suffisamment d'espace. Pour sauvegarder vos hôtes, exécutez le script `nw-backup.sh` à l'aide de l'option `-u`. Cette option est obligatoire pour la mise à niveau vers la version 11.1.

> **Remarque :** Le script arrête les services lorsqu'il s'exécute. Toutefois, vous pouvez arrêter les services manuellement avant d'exécuter le script, si nécessaire.

Lorsque vous exécutez le script de sauvegarde, vous pouvez choisir parmi plusieurs options décrites dans les sections suivantes.

Syntaxe :
`./nw-backup.sh [-u -t -d -D -l -x -e] <external-mnt> -b <backup file path>`

Options générales

`-u : This option is required for upgrading to 11.1. Enables the upgrade flag to run backup for upgrading to 11.1. It also enables disk space check (-d), backing up reporting engine reports (-r) and stores backup content locally (-l). Default: (no)`

`-d : enables disk space check in 'fast' mode (quick estimate of space using uncompressed data). Default: (no)`

`-D : enables disk space check in 'full' mode (estimate of space using compressed data, ~10X slower). Default: (no)`

`-l : stores backup content locally on each host (automatically set if -u is used). Default: (no)`

`-e <path to mount point> : copies backup files of all devices onto an external mount point. Default: (/mnt/external_backup)`

`-x : move all backup files to an external mount point. Default: (no) - COPY`

`-b <path to write backups> : path to the location for storing backup files on a backup server.` **`For upgrading to 11.1, please use the default location!`** `Default: (/var/netwitness/database/nw-backup)`

Remarque : Ne modifiez **pas** le chemin de sauvegarde en mode mise à niveau (-u).

Remarque : Lorsque vous exécutez une sauvegarde avec l'option `-u`, tous les services sont arrêtés. Si vous devez continuer à utiliser la machine 10.6.x après avoir exécuté la sauvegarde, redémarrez le système 10.6.x pour redémarrer les services.

Options avancées de sélection de contenu

`-c : back up Colocated Malware Analysis on SA servers. Default: (no)`

`-i : back up IPDB data (/var/netwitness/ipdbextractor). Default: (no)`

`-m : back up Malware Analysis File Repository. Default: (no)`

`-r : back up Reporting Engine Report Repository (automatically set if -u is used). Default: (no)`

`-v : back up system logs (/var/log). Default: (no)`

`-y : back up YUM Web Server & RPM Repository. Default: (no)`

`-S : If set: DISABLES back up of SMS RRD files. Default: (not-set)`

`-C : If set: DISABLES back up of Context-Hub configuration and database. Default: (not-set)`

`-E : If set: DISABLES back up of ESA Mongo database. Default: (not-set)`

Option de test

```
 -t : performs script test run for disk space check only. Services are
not stopped and excludes execution of backup. Can be combined with (-d)
or (-D) and other flags. Default: (-t)
```

Par exemple, la commande :
`./nw-backup.sh`
peut exécuter les options de sauvegarde comme définies dans l'en-tête du script lui-même.
OU la commande :
`./nw-backup.sh -ue /mnt/external_backup`
peut exécuter une sauvegarde normale à l'aide du chemin de sauvegarde défini dans le script, avec les options suivantes :

```
-u : enables the upgrade flag to run backup for upgrading to 11.1. It
also enables disk space check (-d), backing up reporting engine reports
(-r) and stores backup content locally (-l). Default: (no)

-e : Copy the backup files to external mount point, mounted on
/mnt/external_backup

For Help: ./nw-backup.sh -h
```

Lorsque vous exécutez le script, le texte suivant s'affiche en haut du script :

Attention :
```
RSA nw-backup script backs up configuration files, data, and
logs on the options provided in the script. It tars the content, with
options to store the backup files on the backup server, move or copy
them to external storage on a mount point (USB/NFS/SMB), or SCP them
back to the target host.
This backup script has been qualified on the following versions of
Security Analytics:
10.6.5.x
Use of this script on any other versions of the product may not give
expected results and may not be supported by RSA Customer
Service.Note: All non-RSA custom files, scripts, Cronjobs and other
important files should be placed in /root, /home/'user', OR /etc to be
included in the backup.
```

Pour exécuter le script de sauvegarde en vue de sauvegarder vos hôtes :

1. Assurez-vous que le fichier `all-systems` contient uniquement les hôtes à sauvegarder.
   Pour plus d'informations, reportez-vous à la section Tâche 2 - Créer la liste des hôtes à sauvegarder.
2. Convertissez le script en exécutable à l'aide de la commande suivante :
   `chmod u+x nw-backup.sh`
3. Commencez le processus de sauvegarde en exécutant la commande suivante au niveau du répertoire racine :
   `./nw-backup.sh -u`

Remarque : Vous devez utiliser l'option `-u` pour que vos fichiers soient restaurés correctement pendant la mise à niveau vers la version 11.1. N'apportez aucune modification à l'en-tête du script de sauvegarde pour le chemin de sauvegarde, car le chemin d'accès est spécifique à la mise à niveau et ces données doivent se trouver à un emplacement spécifique.

Le texte « `Backup completed with no errors` » s'affiche pour signaler la réussite de la sauvegarde.

Un fichier log, avec un nom semblable à l'exemple suivant, est créé dans le répertoire de sauvegarde qui fournit des informations sur les fichiers en cours de sauvegarde : `rsa-nw-backup-2017-03-15.log`

4. Lorsque la sauvegarde est terminée, pour vous assurer que les fichiers appropriés ont bien été sauvegardés, vous pouvez exécuter la commande suivante pour afficher la liste de tous les fichiers qui ont été sauvegardés :

   `tar -tzvf hostname-ip-address-backup.tar.gz`

   Les fichiers d'archive suivants sont créés :

   Pour tous les hôtes :

   fichiers `<hostname-IPaddress>-root.tar.gz`

   `<hostname-IPaddress>-backup.tar.gz`

   `tar checksum`

   `<hostname-IPaddress>-network.info.txt`

   Pour les serveurs Security Analytics :

   fichiers `<hostname-IPaddress>-root.tar.gz`

   `<hostname-IPaddress>-backup.tar.gz`

   `<hostname-IPaddress>-mongodb.tar.gz`

   `tar checksum`

   `<hostname-IPaddress>-network.info.txt`

   Pour les hôtes ESA :

   fichiers `<hostname-IPaddress>-root.tar.gz`

   `<hostname-IPaddress>-backup.tar.gz`

   `<hostname-IPaddress>-mongodb.tar.gz`

   `<hostname-IPaddress>-controldata-mongodb.tar.gz`

   `tar checksum`

   `<hostname-IPaddress>-network.info.txt`

Les fichiers d'archive se trouvent dans le répertoire `/var/netwitness/database/nw-backup`. Si les fichiers tar paraissent plus petits que prévus, ouvrez-les pour vous assurer que les fichiers ont été correctement sauvegardés.

Tâches postérieures à la sauvegarde

Tâche 1 - Enregistrer une copie du fichier `all-systems` et des fichiers tar de sauvegarde

Effectuez des copies du fichier `all-systems`, du fichier `all-systems-master-copy` et des fichiers tar de sauvegarde, puis placez ces copies à un emplacement sécurisé. Vous ne pouvez pas régénérer ces fichiers après la mise à niveau vers la version 11.1 du serveur Security Analytics (en particulier, le service Admin).

Tâche 2 - Vérifier que les fichiers de sauvegarde requis ont été générés

Après avoir exécuté les scripts de sauvegarde, plusieurs fichiers sont générés. Ces fichiers sont requis pour le processus de mise à niveau vers la version 11.1. Avant de commencer le processus de mise à niveau, vous devez vous assurer que les fichiers de sauvegarde requis sont sur les hôtes que vous mettez à niveau et veiller à effectuer les tâches suivantes.

Les fichiers suivants sont générés sur tous les hôtes par les scripts de sauvegarde :

- `all-systems`
- `all-systems-master-copy`
- `appliance_info`
- `service_info`
- `<hostname>-<host-IP-address>-backup.tar.gz`
- `<hostname>-<host-IP-address>-backup.tar.gz.sha256`
- `<hostname>-<host-IP-address>-root.tar.gz`
- `<hostname>-<host-IP-address>-root.tar.gz.sha256`
- `<hostname>-<host-IP-address>-network.info.txt`

Outre les fichiers répertoriés ci-dessus, les fichiers suivants seront générés sur le serveur Security Analytics et sur les hôtes ESA :

- `<hostname>-<host IP address>-mongodb.tar.gz`
- `<hostname>-<host IP address>-mongodb.tar.gz.sha256`

Le script de sauvegarde génère également les fichiers `controldata-mongodb.tar.gz` suivants.

Remarque : Le script de sauvegarde copie les fichiers suivants à partir de tous les hôtes ESA vers le chemin de sauvegarde du serveur Security Analytics.

- `<esa hostname>-<esa hostip>-controldata-mongodb.tar.gz`
- `<esa hostname>-<esa hostip>-controldata-mongodb.tar.gz.sha256`

Tâche 3 - (Conditionnel) Pour plusieurs hôtes ESA, copiez les fichiers `mongodb tar` sur l'hôte ESA primaire

Si vous disposez de plusieurs systèmes hôtes ESA dans votre entreprise, copiez les deux fichiers suivants depuis chaque hôte ESA dans le répertoire `/opt/rsa/database/nw-backup/` du système hôte principal ESA (l'hôte contenant le service ContextHub en cours d'exécution) :

- `<hostname>-<host-IP-address>-mongodb.tar.gz`
- `<hostname>-<host-IP-address>-mongodb.tar.gz.sha256`

Tâche 4 - Vérifier que tous les fichiers de sauvegarde requis se trouvent sur chaque hôte

Avant de la mise à niveau vers la version 11.1., assurez-vous que les bons fichiers existent sur les hôtes que vous mettez à niveau, comme décrit dans les listes suivantes.

Les emplacements des chemins de sauvegarde par défaut doivent être mentionnés ici afin que l'utilisateur sache y accédez et vérifier les fichiers.

Remarque : Les chemins d'accès par défaut pour les fichiers de sauvegarde sont :
- Serveurs Security Analytics :`/var/netwitness/database/nw-backup`
- Hôtes ESA :`/opt/rsa/database/nw-backup`
- Hôtes Malware : `/var/lib/rsamalware/nw-backup`

Fichiers requis pour les Serveur NetWitness

- `all-systems-master-copy`
- `<hostname>-<host-IP-address>-backup.tar.gz`
- `<hostname>-<host-IP-address>-backup.tar.gz.sha256`
- `<hostname>-<host-IP-address>-root.tar.gz`
- `<hostname>-<host-IP-address>-root.tar.gz.sha256`
- `<hostname>-<host-IP-address>-network.info.txt`
- `<hostname>-<host-IP-address>-mongodb.tar.gz`
- `<hostname>-<host-IP-address>-mongodb.tar.gz.sha256`
- `<esa-hostname>-<esa-host-IP-address>-controldata-mongodb.tar.gz`

- `<esa-hostname>-<esa-host-IP-address>-controldata-mongodb.tar.gz.sha256`

Fichiers requis pour les hôtes ESA

- `all-systems-master-copy`
- `<hostname>-<host-IP-address>-backup.tar.gz`
- `<hostname>-<host-IP-address>-backup.tar.gz.sha256`
- `<hostname>-<host-IP-address>-root.tar.gz`
- `<hostname>-<host-IP-address>-root.tar.gz.sha256`
- `<hostname>-<host-IP-address>-network.info.txt`
- `<hostname>-<host-IP-address>-mongodb.tar.gz`
- `<hostname>-<host-IP-address>-mongodb.tar.gz.sha256`

Fichiers requis pour tous les autres hôtes

- `all-systems-master-copy`
- `<hostname>-<host-IP-address>-backup.tar.gz`
- `<hostname>-<host-IP-address>-backup.tar.gz.sha256`
- `<hostname>-<host-IP-address>-root.tar.gz`
- `<hostname>-<host-IP-address>-root.tar.gz.sha256`
- `<hostname>-<host-IP-address>-network.info.txt`

Remarque : Les fichiers suivants sont situés dans le tar `<hostname>-<host-IP-address>-backup.tar.gz` sur tous les hôtes :
`appliance_info`
`service_info`

Remarque : Les chemins d'accès à l'emplacement des fichiers de sauvegarde et de restauration pour iptables, les configurations NAT, les comptes utilisateur et les entrées crontab sont affichés dans la liste suivante :

Chemins de sauvegarde :

`BUPATH=/opt/rsa/database/nw-backup` pour le moteur de corrélation ESA

`BUPATH=/var/lib/rsamalware/nw-backup` pour le service Malware

`BUPATH=/var/netwitness/database/nw-backup` pour tous les autres services

Emplacements de restauration :

`BUPATH/restore/etc/sysconfig` pour les règles Iptable

`BUPATH/restore/etc/sysconfig` pour les configurations NAT

`BUPATH/restore/etc` pour les entrées Crontab

`BUPATH/restore/etc` pour les comptes utilisateur (les utilisateurs se trouvent dans le fichier `passwd`, et les groupes se trouvent dans le fichier `group`. Ceux-ci ne sont pas restaurés au cours du processus de mise à niveau, mais peuvent être restaurés manuellement.

`BUPATH/restore/etc/ntp.conf` pour les configurations NTP (doivent être restaurées à l'aide de l'interface utilisateur NetWitness Suite)

Migration des disques durs de la version 10.6.5.x vers la version 11.1

Ces instructions vous expliquent comment mettre à niveau des hôtes virtuels de la version 10.6.5.x vers la version 11.1.

Attention : 1) Vous ne pouvez pas effectuer la migration si vous disposez d'un snapshot pour votre machine virtuelle.
2). Exécutez la sauvegarde immédiatement avant de mettre à niveau les hôtes pour chaque phase afin que les données ne soient pas obsolètes.
3.) Ce guide s'applique exclusivement aux mises à niveau des hôtes virtuels. Si votre déploiement contient aussi bien des hôtes physiques que virtuels, reportez-vous au document *RSA NetWitness® Suite 11.1 Instructions de mise à niveau des hôtes physiques* pour consulter les étapes de mise à niveau des hôtes physiques. Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

Remarque : Les machines doivent se trouver dans VMware ESX.

Cinq tâches doivent être réalisées pour migrer vos disques durs de déploiement de machines virtuelles (VM) de la version 10.6.5.x vers la version 11.1 :

Tâche 1 : Sauvegarder les données sur vos machines virtuelles 10.6.5.x.

Tâche 2 : Déployer la même pile de machine virtuelle dans la version 11.1 que celle disponible dans la version 10.6.5.x.

Tâche 3 : Copier les fichiers VMDK et les ajouter comme disque dur aux nouvelles machines virtuelles.

Tâche 4 : Conserver l'adresse MAC de la machine virtuelle de serveur SA mise à niveau.

Tâche 5 : Restaurer les données sauvegardées sur les machines virtuelles 10.6.5.x sur les machines virtuelles 11.1.

Tâche 1 : Sauvegarder les données sur vos machines virtuelles 10.6.5.x

1. Préparez le service Log Collector en vue de la migration :
   a. Connectez-vous au service Log Collector avec les informations d'identification racine.
   b. Accédez au répertoire `/opt/rsa/nwlogcollector/nwtools/` et exécutez la commande suivante :
   ```
   sh prepare-for-migrate.sh --prepare
   ```

Reportez-vous à la section Hôte Virtual Log Collector (VLC) pour obtenir des instructions détaillées relatives à la mise à niveau du VLC.

2. Téléchargez le fichier `.zip` contenant les scripts de sauvegarde 10.6.5.x à partir de RSA Link (https://community.rsa.com/docs/DOC-81514) sur l'hôte de sauvegarde externe.

   Remarque : Vous devez configurer un hôte externe à utiliser pour la sauvegarde des fichiers. L'hôte doit exécuter CentOS 6 avec une connectivité à la pile d'hôtes NetWitness Suite via le protocole SSH.

3. Exécutez les commandes suivantes à partir du répertoire `nw-backup/scripts` (reportez-vous à la section Instructions de sauvegarde pour obtenir une description détaillée des scripts de sauvegarde).

   ```
   ./get-all-systems.sh <SA-IP>
   ./ssh-propagate.sh <path-to-backup-directory/all-systems>
   ./nw-backup.sh -u
   ```

   (si vous disposez d'une VM Malware, remplacez `-m -u`par `-u` dans cette chaîne de commande (par exemple, `./nw-backup.sh -m -u`).

Tâche 2 : Déployer la même pile de machine virtuelle dans la version 11.1 que celle disponible dans la version 10.6.5.x

Vous devez installer la même pile d'hôte virtuel dans la version 11.1 que celle que vous aviez dans la version 10.6.5.x. Pour savoir comment procéder, reportez-vous au document *RSA NetWitness® Suite Guide d'installation d'un hôte virtuel 11.1*.Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

Les étapes suivantes sont les étapes générales de déploiement d'un hôte OVA dans l'environnement ESXi.

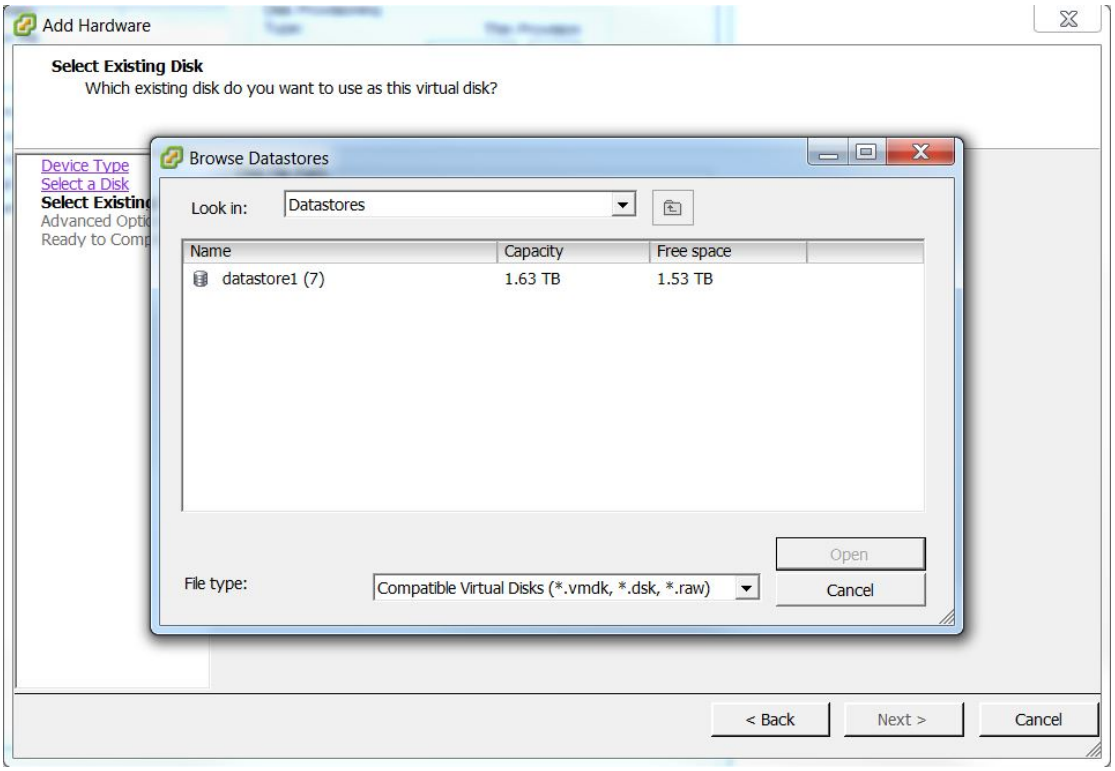
Téléchargez le fichier OVA 11.1 dans un répertoire local à partir du site RSA Link Download Central.

1. Connectez-vous à l'environnement ESXi.
2. Dans la liste déroulante **Fichier**, sélectionnez **Déployer le modèle OVF**.
   La boîte de dialogue Déployer le modèle OVA s'affiche.
3. Recherchez le répertoire local des fichiers OVA 11.1 que vous avez téléchargés.
4. Sélectionnez le fichier à déployer dans l'environnement virtuel, puis cliquez sur **Suivant**.
5. Sélectionnez la configuration appropriée de la machine virtuelle et cliquez sur **Suivant**.

6. Mettez sous tension la machine virtuelle, accédez à la console et connectez-vous à la machine.
   La machine virtuelle intègre désormais l'image de base 11.1 requise pour exécuter le programme d'installation (soit `nwsetup-tui`).

Tâche 3 - Copier les fichiers VMDK et les ajouter sous la forme d'un disque dur aux nouvelles machines virtuelles

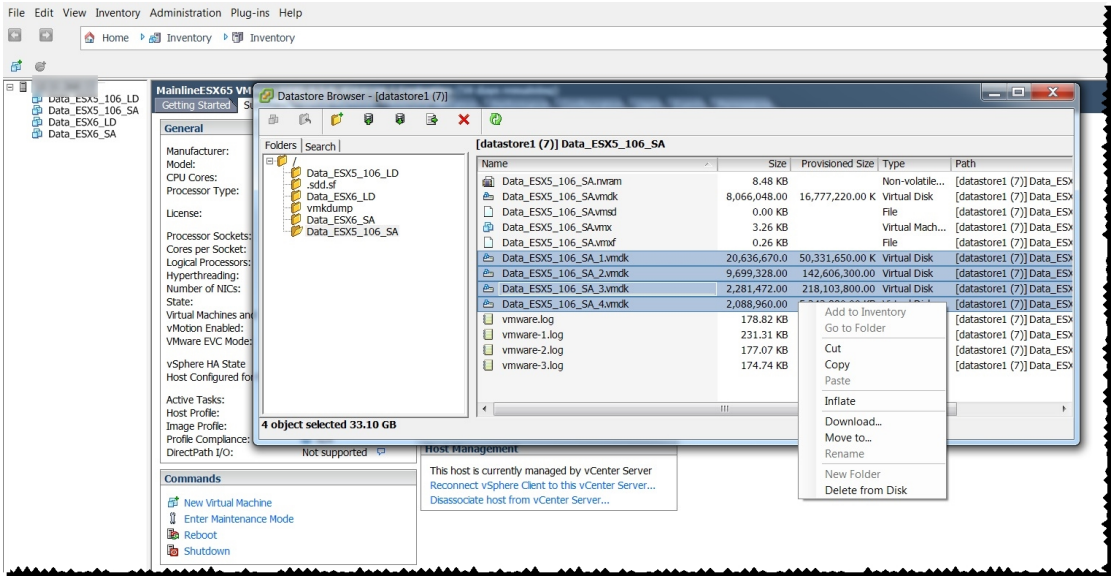
1. Mettez hors tension les machines virtuelles 10.6.5.x et 11.1.
2. Accédez au serveur ESX voulu, cliquez sur l'onglet **Configuration** > **Stockage**.
3. Cliquez avec le bouton droit sur le datastore requis et cliquez sur **Browse Datastore**.



4. Accédez à la machine virtuelle 10.6.5.x existante dans le datastore.
5. Sélectionnez tous les fichiers VMDK dans le datastore, cliquez avec le bouton droit, puis cliquez sur **Copier**.

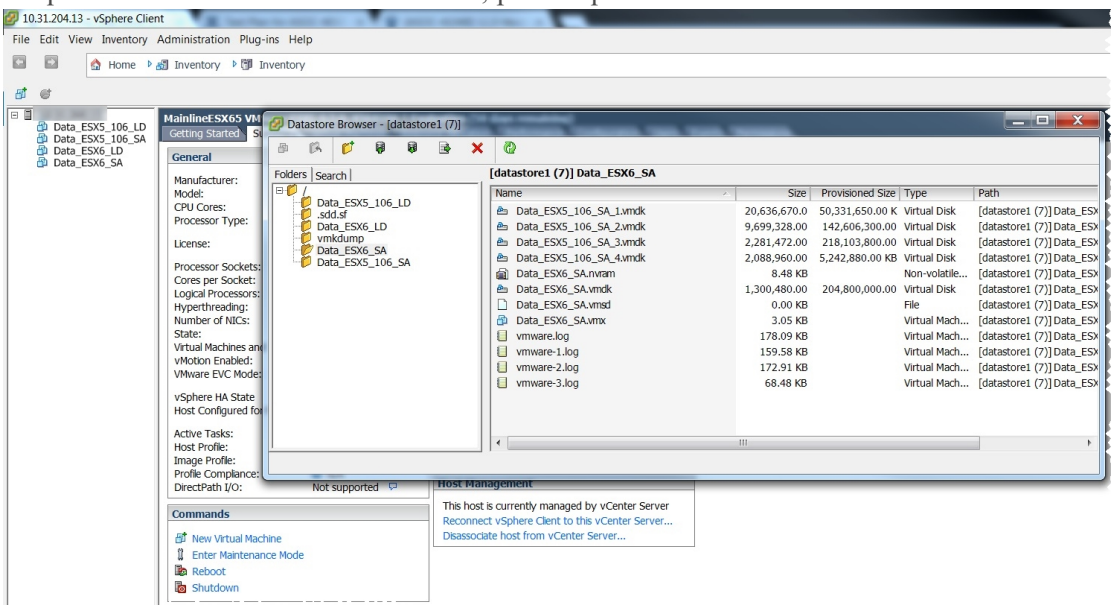
Attention : Ne copiez pas le fichier VMDK de base (par exemple, `Data_106_SA`), car il contient CentOS6.

Vous devez copier tous les fichiers VMDK numérotés. Par exemple, si le nom de la machine virtuelle 10.6.5.x est `Data_106_SA`, vous copierez tous les fichiers `Data_106_SA_1`, `Data_106_SA_2`, `Data_106_SA_3`, etc.



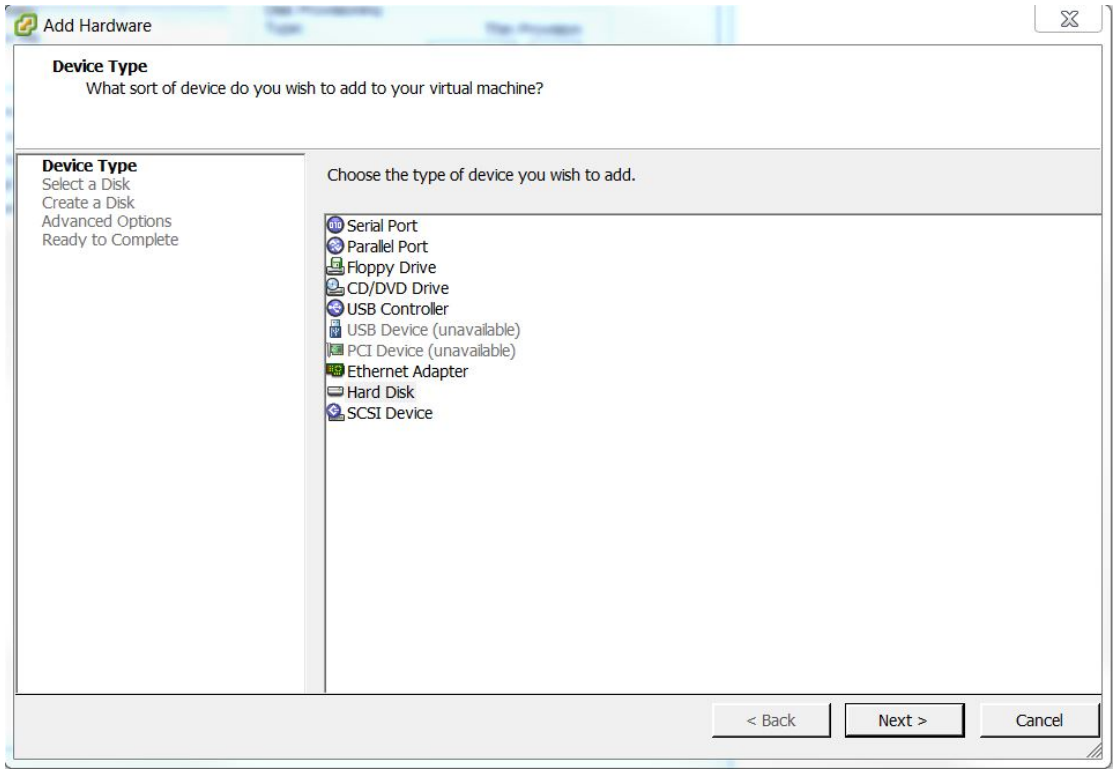
6. Accédez à la nouvelle machine virtuelle 11.1 dans le datastore.

7. Cliquez avec le bouton droit de la souris, puis cliquez sur **Coller**.



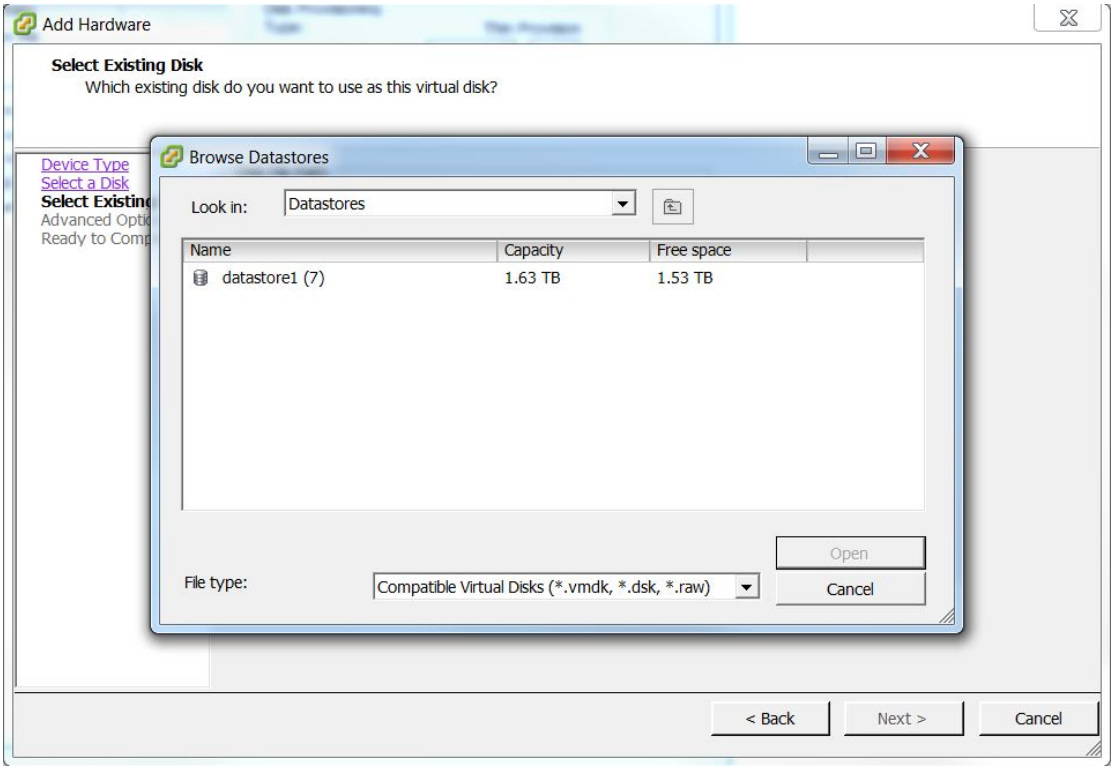
Remarque : Vous devez attendre jusqu'à ce que tous les fichiers VMDK de la machine virtuelle précédente soient intégralement copiés dans le datastore de la nouvelle machine virtuelle.

8. Sélectionnez la machine virtuelle 11.1, cliquez sur **Modifier les paramètres** > **Ajouter**.
9. Dans la boîte de dialogue, cliquez sur **Disque dur** > **Suivant**.

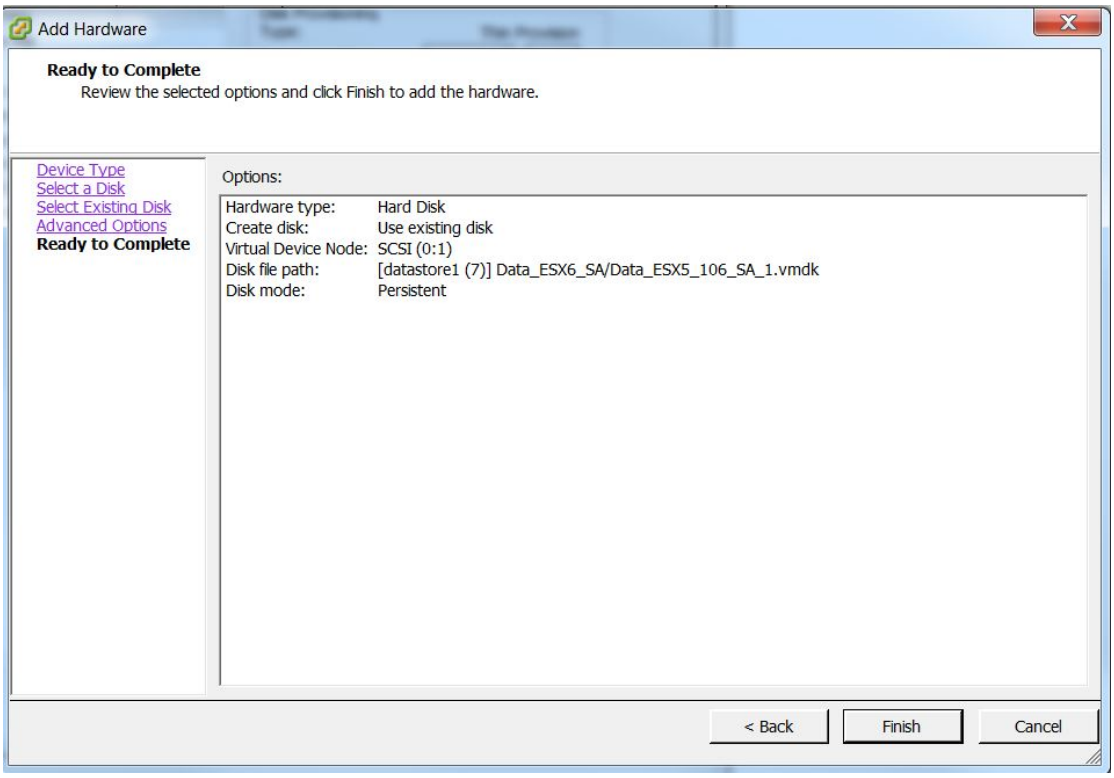


10. Cliquez sur **Disque dur déjà existant** > **Suivant**.

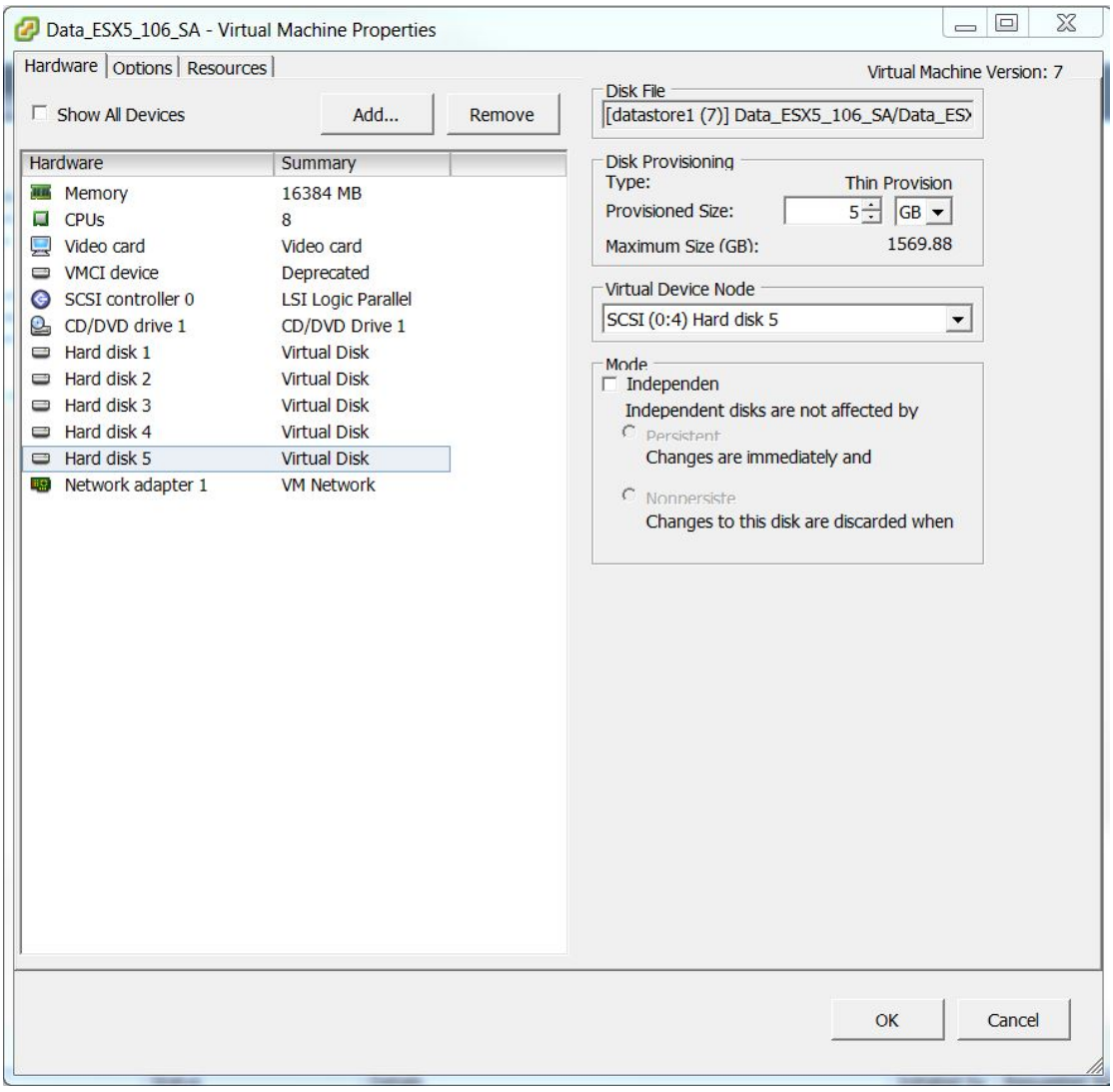
11. Cliquez sur **Parcourir** et accédez à l'emplacement du datastore dans lequel vous avez copié les fichiers vmdk.



12. Dans la machine virtuelle 11.1, sélectionnez le fichier VMDK à ajouter comme disque.



13. Répétez les étapes 8 à 12 pour chaque disque à ajouter.



14. Cliquez sur **OK**.

Tâche 4 : Conserver l'adresse MAC de la machine virtuelle de serveur SA mise à niveau.

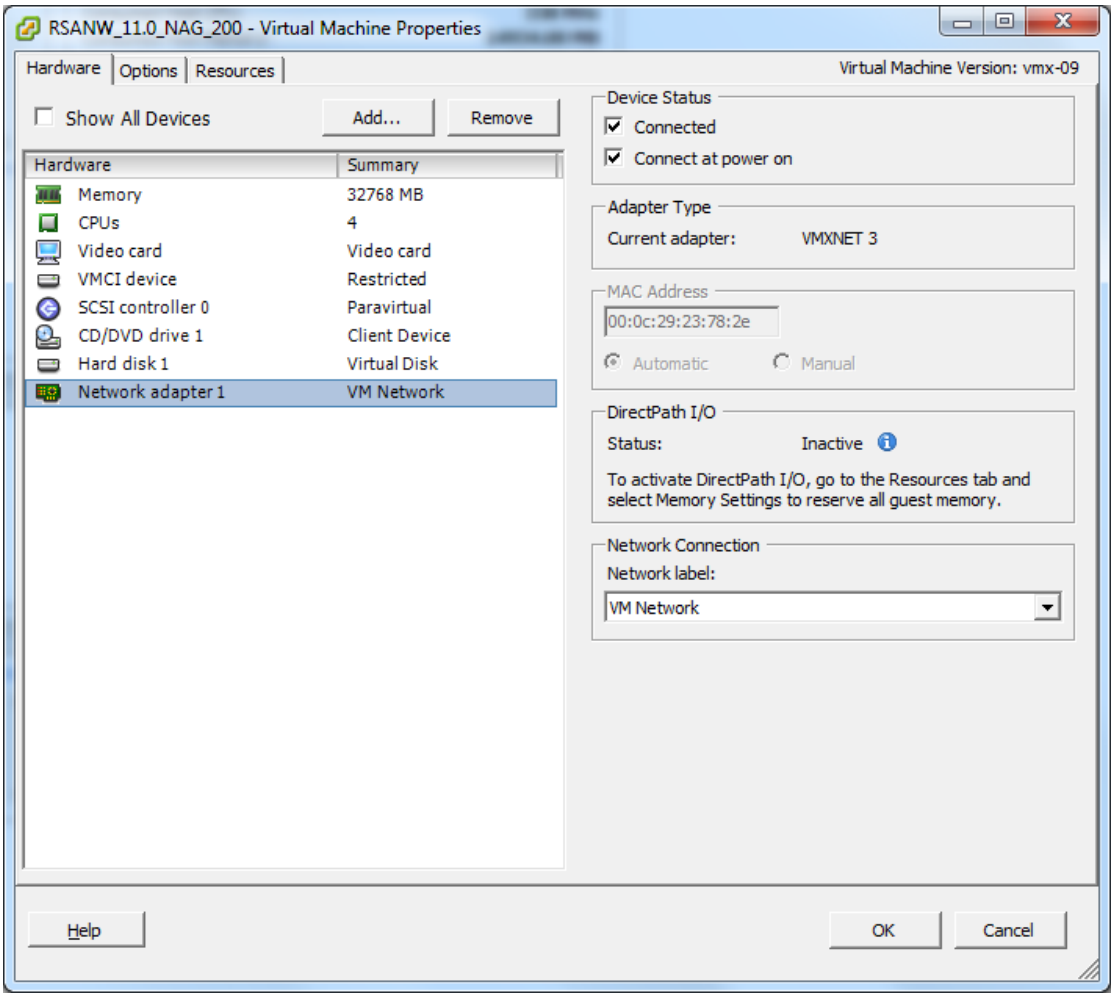
Pour conserver l'adresse MAC de la machine virtuelle de serveur Security Analytics (SA) mise à niveau :

Remarque : Ces étapes s'appliquent à la mise à niveau de la machine virtuelle du serveur SA (créée avec l'attribution d'adresse MAC « Automatique » sélectionnée) vers NetWitness Server 11.1. Pour les machines virtuelles dotées d'une adresse MAC statique, vous pouvez modifier l'adresse MAC en accédant à l'option Modifier les paramètres pour une machine virtuelle et en saisissant l'adresse MAC.

1. Connectez-vous au serveur vCenter.

   Remarque : Les versions de vCenter prises en charge sont les versions 5.5 à 6.5 inclus.

2. (Conditionnel) Si les deux machines virtuelles (NetWitness 10.6.5.x et 11.1) sont sous tension, **mettez-les hors tension**.
3. Cliquez sur l'onglet **Récapitulatif**, cliquez avec le bouton droit sur **Datastore** et recherchez l'emplacement du datastore.
4. Accédez au dossier de la machine virtuelle, puis téléchargez le fichier `.vmx` de la version 10.6.5.x et de la version 11.1 dans le référentiel local.
   Par défaut, la machine virtuelle générée avec l'adresse MAC est créée au format (comme le montre la figure ci-dessous).

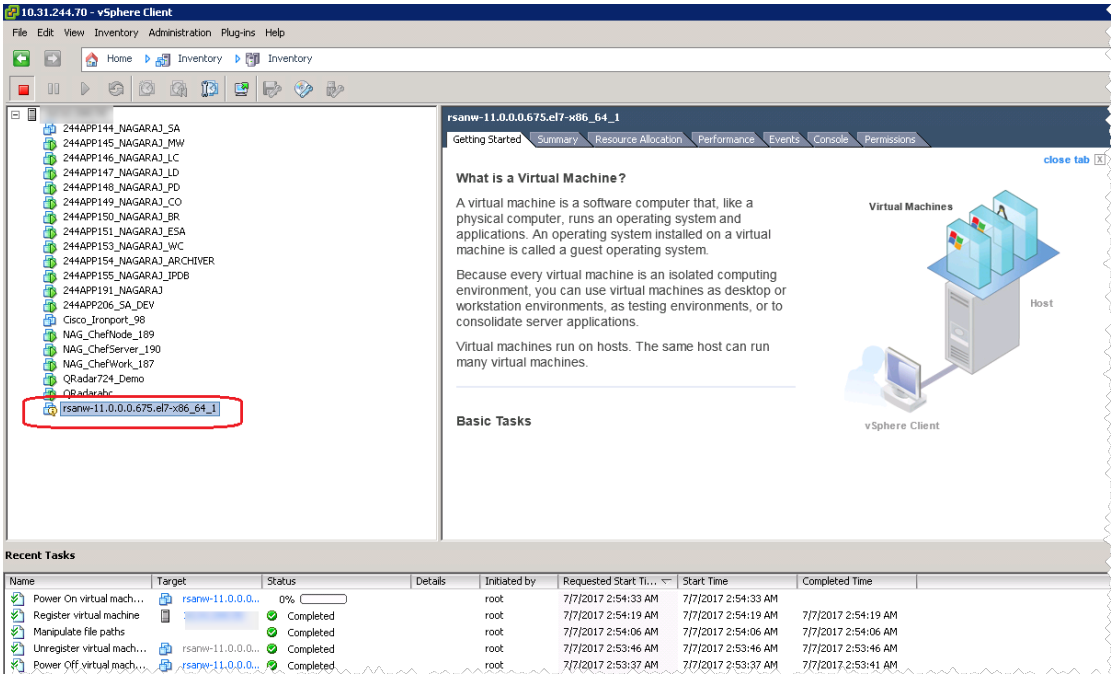


Remarque : 00:0c:29:XX:YY:ZZ – 00:0c:29 est l'identifiant spécifique d'une adresse MAC générée automatiquement. **00:50:56:XX:YY:ZZ – 00:50:56** est l'identifiant spécifique d'une adresse MAC statique ou générée manuellement. Ceci est valide uniquement si vCenter n'est pas déployé. Si vCenter est déployé, cette adresse MAC correspond à l'identifiant spécifique d'une adresse MAC générée automatiquement.

5. À l'aide d'un éditeur de texte, copiez les valeurs `uuid.location` et `ethernet0.generatedAddress` du fichier **.vmx** de la version 10.6.5.x dans le fichier **.vmx** de la version 11.1.

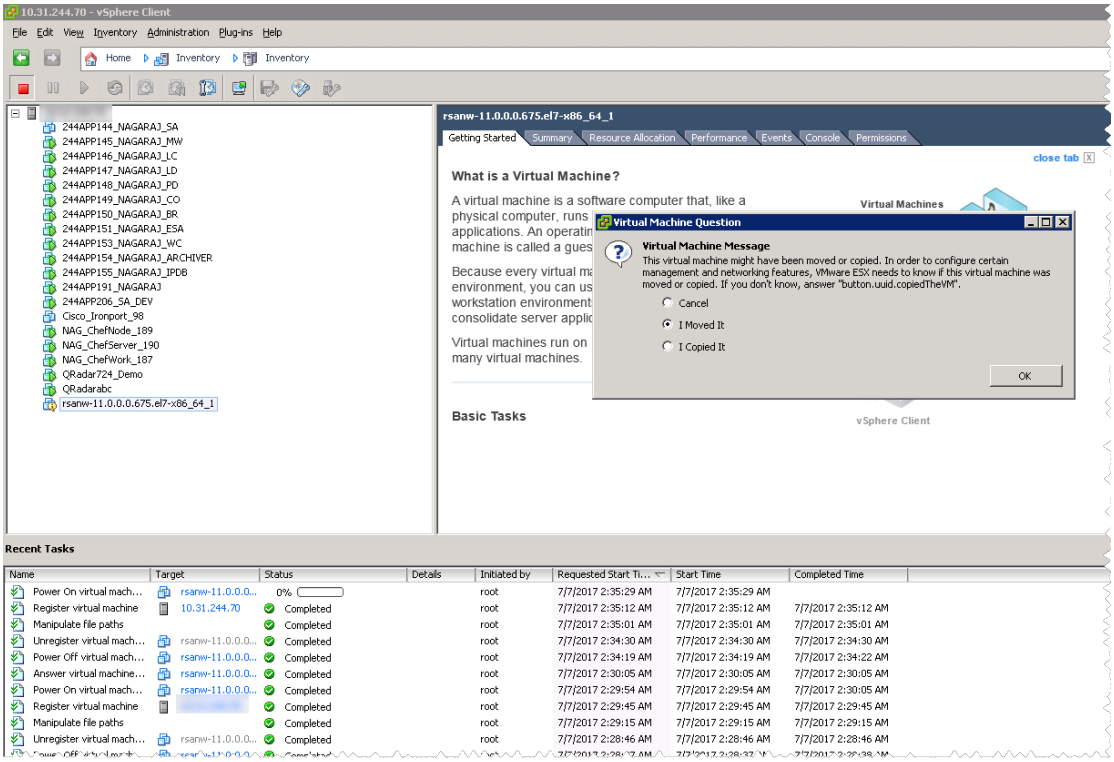
Remarque : Si vous avez déployé la pile 10.6.5.x sur le serveur ESX directement (et non pas via VCenter), vous devez copier la valeur de `uuid.bios` en plus de la valeur de `uuid.location` et `ethernet0.generatedAddress` depuis le fichier **.vmx** de la version 10.6.5.x dans le fichier **.vmx** de la version 11.1.

6. Supprimez les machines virtuelles 10.6.5.x et 11.1 de l'inventaire.
   a. Accédez au serveur vCenter.
   b. Cliquez avec le bouton droit sur les machines virtuelles 10.6.5.x et 11.1.
   c. Sélectionnez Supprimer de l'inventaire.
7. Chargez le fichier **.vmx** 11.1 modifié dans l'emplacement du datastore en le remplaçant par le fichier **.vmx** existant.
8. Dans le datastore, cliquez avec le bouton droit sur le fichier **.vmx** 11.1 et sélectionnez Ajouter à l'inventaire.
9. Accédez au serveur vCenter et **mettez sous tension** la machine virtuelle 11.1.
   Le message suivant s'affiche :
   The virtual machine might have been moved or copied. In order to configure certain management and networking features, VMware ESX needs to know if this virtual machine was moved or copied. If you don't know, answer "I Copied it."



10. Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Guest** > **Answer Question**.

Le résultat suivant s'affiche.



11. Sélectionnez **I moved It**.
12. Cliquez sur **OK**.
    L'adresse MAC est conservée dans l'adresse MAC de la version 10.6.5.x à la version 11.1.

Tâche 5 : Restaurer les données sauvegardées sur les machines virtuelles 10.6.5.x sur les machines virtuelles 11.1

Procédez comme suit pour mettre la machine virtuelle 11.1 **sous tension**.

1. Copiez les données sauvegardées du répertoire `nw-backup` vers les machines virtuelles 11.1.
   - Pour le serveur NW (serveur SA 10.6.5.x) :

     Remarque : Reportez-vous à la section Hôte Virtual Log Collector (VLC) pour obtenir des instructions détaillées relatives à la mise à niveau du VLC.

     a. Créez le répertoire `nwhome` sous `/tmp`.

     b. Montez `VolGroup00-nwhome` sur `/tmp/nwhome/`.

     ```
     mount /dev/mapper/VolGroup00-nwhome /tmp/nwhome/
     ```

c. Copiez le contenu du répertoire `/tmp/nwhome/` dans `/var/netwitness/`.
```
cp -r /tmp/nwhome/* /var/netwitness/
```

d. Montez `VolGroup02-redb` sur `/var/netwitness/database`.
```
mount /dev/mapper/VolGroup02-redb /var/netwitness/database/
```

> **Remarque :** Assurez-vous que le répertoire `/var/netwitness/database/nw-backup` existe et contient les fichiers tarball de l'appliance.

e. Démontez `VolGroup00-nwhome` de `/tmp/nwhome/`.
```
umount /tmp/nwhome
```

- Pour les services Archiver, Broker, Concentrator, Log Decoder/Log Collector et Packet Decoder :

> **Remarque :** Si votre service Decoder ou Log Decoder 10.6.5.x dispose de plusieurs interfaces réseau :
> 1. **Mettez hors tension** la machine virtuelle 11.1, la machine virtuelle Decoder 11.1 ou Log Decoder.
> 2. Accédez à **Modifier les paramètres** pour la machine virtuelle et ajoutez le nombre de cartes Ethernet requis.
> 3. Mettez la machine virtuelle **sous tension**.
> 4. Ajoutez les cartes Ethernet avant de restaurer les données sauvegardées.

a. Créez le répertoire `nwhome` sous `/tmp`.

b. Créez un montage temporaire `VolGroup00-nwhome` sur `/tmp/nwhome/`.
```
mount /dev/mapper/VolGroup00-nwhome /tmp/nwhome/
```

c. Copiez le contenu du répertoire `/tmp/nwhome/` dans `/var/netwitness/`.
```
cp -r /tmp/nwhome/* /var/netwitness/
```

d. Démontez `VolGroup00-nwhome` à partir de `/tmp/nwhome/`.
```
umount /tmp/nwhome
```

- Pour Malware Analysis (Malware co-localisé non pris en charge dans la mise à niveau 11.1) :

a. Créez le répertoire `apps` sous `/tmp/`.

b. Créez un montage `VolGroup01-apps` temporaire sur `/tmp/apps/`.
```
mount /dev/mapper/VolGroup01-apps /tmp/apps/
mkdir /var/netwitness/database
```

c. Copiez le répertoire`nw-backup` dans `/var/netwitness/`.
```
cp -r /tmp/apps/nw-backup /var/netwitness/database
```

d. Démontez `VolGroup01-apps` de `/tmp/apps/`.
```
umount /tmp/apps
```

- Pour Event Stream Analysis :

a. Créez le répertoire `apps` sous `/tmp/`

b. Créez un montage `VolGroup01-apps` temporaire sur `/tmp/apps/`.
```
mount /dev/mapper/VolGroup01-apps /tmp/apps/
mkdir /var/netwitness/database
```

c. Copiez le répertoire`nw-backup` dans`/var/netwitness`.
```
cp -r /tmp/apps/nw-backup /var/netwitness/database
```

d. Démontez `VolGroup01-apps` à partir de `/tmp/apps/`.
```
umount /tmp/apps
```

2. Montez les disques.

Remarque : Si vous avez configuré des points de montage externes sur les machines virtuelles de la pile pour l'un des répertoires suivants, remontez les points de montage externe à la place des montages suivants.

- Pour le serveur NW :
```
mount /dev/mapper/VolGroup01-ipdbext /var/netwitness/ipdbextractor/
mount /dev/mapper/VolGroup02-redb /var/netwitness/database/
```

Remarque : Assurez-vous que le répertoire `/var/netwitness/database/nw-backup` existe et contient les fichiers tarball de l'appliance.

- Pour Log Decoder/Log Collector :

Remarque : Les montages suivants ne sont pas requis pour Virtual Log Collector.

```
mount /dev/mapper/VolGroup01-decoroot /var/netwitness/logdecoder
mount /dev/mapper/VolGroup01-index /var/netwitness/logdecoder/index
mount /dev/mapper/VolGroup01-sessiondb
/var/netwitness/logdecoder/sessiondb
mount /dev/mapper/VolGroup01-metadb /var/netwitness/logdecoder/metadb
mount /dev/mapper/VolGroup01-logcoll /var/netwitness/logcollector
mount /dev/mapper/VolGroup01-packetdb
/var/netwitness/logdecoder/packetdb
```

- Pour Packet Decoder :
```
mount /dev/mapper/VolGroup01-decoroot /var/netwitness/decoder
mount /dev/mapper/VolGroup01-sessiondb
/var/netwitness/decoder/sessiondb
mount /dev/mapper/VolGroup01-index /var/netwitness/decoder/index
mount /dev/mapper/VolGroup01-metadb /var/netwitness/decoder/metadb
```

```
mount /dev/mapper/VolGroup01-packetdb
/var/netwitness/decoder/packetdb
```

- Pour Concentrator :
```
mount /dev/mapper/VolGroup01-concroot /var/netwitness/concentrator
mount /dev/mapper/VolGroup01-sessiondb
/var/netwitness/concentrator/sessiondb
mount /dev/mapper/VolGroup01-index /var/netwitness/concentrator/index
mount /dev/mapper/VolGroup01-metadb
/var/netwitness/concentrator/metadb
```
- Pour Archiver :
```
mount /dev/mapper/VolGroup01-archiver /var/netwitness/archiver
mount /dev/mapper/VolGroup02-workbench /var/netwitness/workbench
```
- Pour Broker :
```
mount /dev/mapper/VolGroup01-broker /var/netwitness/broker
```

8. Ajoutez les entrées de montage suivantes à `/etc/fstab`.
   - Pour le serveur NW :
```
/dev/mapper/VolGroup01-ipdbext /var/netwitness/ipdbextractor/ xfs
defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup02-redb /var/netwitness/database/ xfs
defaults,noatime,nosuid 1 2
```
   - Pour Log Decoder/Log Collector :

     Remarque : Les montages suivants ne sont pas requis pour Virtual Log Collector.

```
/dev/mapper/VolGroup01-decoroot /var/netwitness/logdecoder ext4
defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup01-index /var/netwitness/logdecoder/index xfs
defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup01-sessiondb
/var/netwitness/logdecoder/sessiondb xfs defaults,noatime,nosuid 1
2
/dev/mapper/VolGroup01-metadb /var/netwitness/logdecoder/metadb xfs
defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup01-logcoll /var/netwitness/logcollector xfs
defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup01-packetdb /var/netwitness/logdecoder/packetdb
xfs defaults,noatime,nosuid 1 2
```
   - Pour Packet Decoder :
```
/dev/mapper/VolGroup01-decoroot /var/netwitness/decoder ext4
```

```
defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup01-sessiondb /var/netwitness/decoder/sessiondb
xfs defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup01-index /var/netwitness/decoder/index xfs
defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup01-metadb /var/netwitness/decoder/metadb xfs
defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup01-packetdb /var/netwitness/decoder/packetdb
xfs defaults,noatime,nosuid 1 2
```

- Pour Concentrator :

```
/dev/mapper/VolGroup01-concroot /var/netwitness/concentrator ext4
defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup01-sessiondb
/var/netwitness/concentrator/sessiondb xfs defaults,nosuid,noatime
1 2
/dev/mapper/VolGroup01-index /var/netwitness/concentrator/index xfs
defaults,noatime,nosuid 1 2
/dev/mapper/VolGroup01-metadb /var/netwitness/concentrator/metadb
xfs defaults,noatime,nosuid 1 2
```

- Pour Archiver :

```
/dev/mapper/VolGroup01-archiver /var/netwitness/archiver xfs
defaults,nosuid,noatime 1 2
/dev/mapper/VolGroup02-workbench /var/netwitness/workbench xfs
defaults,nosuid,noatime 1 2
```

- Pour Broker :

```
/dev/mapper/VolGroup01-broker /var/netwitness/broker xfs
defaults,nosuid,noatime 1 2
```

Installation des hôtes virtuels dans la version 11.1

L'installation de la pile virtuelle 11.1 comprend deux phases à effectuer dans l'ordre indiqué.

- Phase 1 : Installer le serveur NW, Event Stream Analysis, Malware Analysis, et les hôtes Broker ou Concentrator

  Remarque : Pour Event Stream Analysis, si des modules C2 sont activés dans la version 10.6.5.x, ces modules entreront dans une phase de préparation après la mise à niveau du service Event Stream Analysis vers la version 11.1 et ne seront pas disponibles avant la fin de cette préparation.

- Phase 2 : Installer le reste des hôtes de composant

Phase 1 : Installer le serveur NW, Event Stream Analysis, Malware Analysis, et les hôtes Broker ou Concentrator

Tâche 1 : Installer Serveur NetWitness 11.1

Suivez les instructions indiquées dans Installer un hôte de serveur NW 11.1.

Tâche 2 : Installer ESA 11.1

Attention : Si des modules C2 sont activés dans la version 10.6.5.x, ces modules entreront dans une phase de préparation après la mise à niveau du service Event Stream Analysis vers la version 11.1 et ne seront pas disponibles avant la fin de cette préparation.

Pour installer vos hôtes ESA, suivez les instructions indiquées dans Installer un hôte de serveur 11.1 autre que NW.

1. Installez votre hôte ESA primaire via le programme d'installation, puis installez **ESA primaire** sur l'hôte dans l'interface utilisateur disponible dans la vue **Hôtes d'administration**.

   Remarque : Si vous disposez de plusieurs hôtes ESA dans votre entreprise, vous devez commencer par mettre à niveau l'hôte ESA primaire, sur lequel se trouvent tous les fichiers tar de sauvegarde `mongodb` (base de données Mongo) avant de mettre à niveau les hôtes secondaires ESA.

2. (Conditionnel) Si vous avez un hôte ESA secondaire, installez-le via le programme d'installation et installez **ESA secondaire** sur l'hôte dans l'interface utilisateur disponible dans la vue **Hôtes d'administration**.

Tâche 3 : Installer Malware Analysis 11.1

Suivez les instructions indiquées dans Installer un hôte de serveur autre que NW 11.1.

Tâche 4 : Configurer Broker ou Concentrator 11.1

Suivez les instructions indiquées dans Installer un hôte de serveur autre que NW 11.1.

Remarque : Si vous ne disposez pas d'un service Broker, mettez à niveau vos hôtes Concentrator. Le serveur NW 11.1 ne peut pas communiquer avec la version 10.6.5.x des services de base pour la nouvelle fonctionnalité Investigate. C'est pourquoi vous devez mettre à niveau les hôtes Broker ou Concentrator durant la Phase 1.

Phase 2 : Installer le reste des hôtes de composant

Reportez-vous à la section Annexe B. Arrêt et redémarrage de la capture et de l'agrégation des données pour obtenir des instructions sur la procédure d'arrêt et de redémarrage de la capture et de l'agrégation des données lors de la mise à niveau des hôtes Decoder, Concentrator et Log Collection.

Hôtes Decoder et Concentrator

1. Arrêtez la capture et l'agrégation des données.
2. Suivez les étapes indiquées dans Installer un hôte de serveur version 11.1 autre que NW.
3. Redémarrez la capture et l'agrégation des données.

Hôte Log Decoder

1. Assurez-vous que vous avez préparé le Log Collector, comme décrit dans la section Log Collectors (LC) et Virtual Log Collectors (VLC) : Exécuter prepare-for-migrate.sh » dans les **Instructions de sauvegarde**.
2. Arrêtez la capture des données sur le Log Decoder.
3. Suivez les étapes indiquées dans Installer un hôte de serveur version 11.1 autre que NW.
4. Redémarrez la capture des données sur le Log Decoder.

Remarque : Après avoir effectué la mise à niveau, vous allez redémarrer la collecte des logs à la fin de la Tâche 28 - Mettre à jour les règles d'incident identifiées dans le domaine dans la tâche de préparation de la mise à niveau des conditions de mise en correspondance indiquée dans **Tâches postérieures à la mise à niveau**

Hôte Virtual Log Collector

1. Assurez-vous que vous avez préparé l'hôte Virtual Log Collector, comme décrit dans la section Log Collectors (LC) et Virtual Log Collectors (VLC) : Exécuter prepare-for-migrate.sh » dans les **Instructions de sauvegarde**.
2. Sauvegardez la version 10.6.5.x de votre VLC en modifiant le fichier `all-systems` sur l'hôte sur lequel vous avez effectué la sauvegarde.
   a. Assurez-vous que le contenu du fichier `all-systems` comprend les informations suivantes avant d'effectuer cette étape.
   `vlc,<host-name>,<IP-address>,<UUID>,10.6.5.x`
   b. Exécutez la commande suivante pour créer une sauvegarde :
   `./nw-backup.sh -u`
   Reportez-vous à la section Instructions de sauvegarde pour obtenir les procédures détaillées de sauvegarde de l'hôte.
3. Vérifiez que l'hôte de sauvegarde contient la sauvegarde de VLC au format suivant :
   `<hostname>-<IPaddress>-root.tar.gz`
   `<hostname>-<IPaddress>-root.tar.gz.sha256`
   `<hostname>-<IPaddress>-backup.tar.gz`
   `<hostname>-<IPaddress>-backup.tar.gz.sha256`
   `<hostname-IPaddress>-network.info.txt`
   `all-systems-master-copy`
4. Mettez hors tension le VLC 10.6.5.x afin qu'une nouvelle machine virtuelle 11.1 soit créée avec la même configuration réseau.
5. Déployez un nouvel hôte de serveur autre que NW à l'aide du fichier OVA NetWitness Suite 11.1.
6. Connectez-vous à la console de machine virtuelle du nouveau VLC.
7. Mettez à jour la configuration réseau pour qu'elle soit identique à celle du VLC 10.6.5.x. Ces informations sont stockées dans le fichier de sauvegarde du VLC 10.6.5.x. `<hostname-IPaddress>-network.info.txt`.

   Remarque : Assurez-vous qu'IPv6 est désactivé.

   a. Modifiez le fichier `/etc/sysconfig/network-scripts/ifcfg-eth0` et mettez à jour les paramètres. Le contenu de `ifcfg-eth0` doit se présenter comme suit.
   `TYPE=Ethernet`
   `DEFROUTE=yes`
   `NAME=eth0`
   `UUID=<uuid>`

```
DEVICE=eth0
DNS1=<nameserver from <hostname>-<ipaddress>-network-info.txt>
DNS2=<nameserver from <hostname>-<ipaddress>-network-info.txt>
BOOTPROTO=static
IPADDR=<ipaddress from <hostname>-<ipaddress>-network-info.txt>
NETMASK=<netmask from <hostname>-<ipaddress>-network-info.txt>
GATEWAY=<gateway from <hostname>-<ipaddress>-network-info.txt>
NM_CONTROLLED=no
ONBOOT=yes
```

b. Exécutez la chaîne de commande suivante.

```
systemctl restart network.service
```

8. Créez le répertoire de sauvegarde.

```
# mkdir -p /var/netwitness/database/nw-backup/
```

9. Copiez la sauvegarde à partir de l'hôte de sauvegarde à partir de `/var/netwitness/database/nw-backup` vers le nouveau VLC dans le répertoire `/var/netwitness/database/nw-backup`.
10. Suivez les étapes 2 à 12 inclus dans Installer un hôte de serveur 11.1 autre que SA pour le reste des composants NetWitness Suite. Veillez à sélectionner **Log Collector** comme service à l'étape 12.

Configurer l'hôte de serveur NW 11.1

Assurez-vous que vous avez sauvegardé les données 10.6.5.x pour l'hôte de serveur SA. **Vous devez suivre les instructions indiquées dans Instructions de sauvegarde pour sauvegarder l'hôte.**

Attention : Exécutez la sauvegarde immédiatement avant la mise à niveau du serveur SA vers la version 11.1 afin que les données soient aussi récentes que possible. Vous devez créer le fichier **all-systems** avant de mettre à niveau le serveur SA, car vous ne pouvez plus le faire une fois que le serveur SA a été mis à niveau vers la version 11.1.

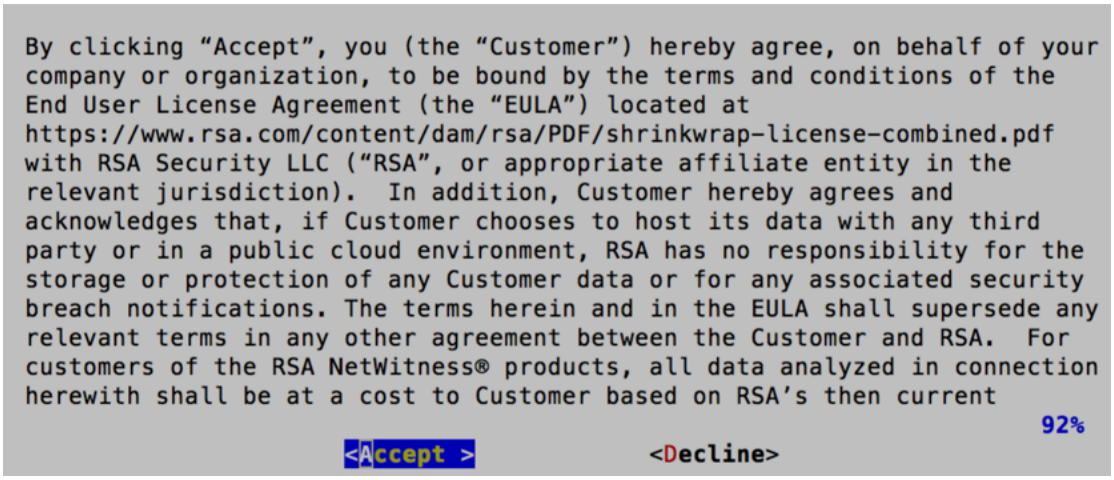
Pour installer la version 11.1 de l'hôte de serveur NW, procédez comme suit.

1. Connectez-vous à la console de la machine virtuelle du serveur NW 11.1, puis 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 la touche 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.

2. 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 11.1 ?** s'affiche.

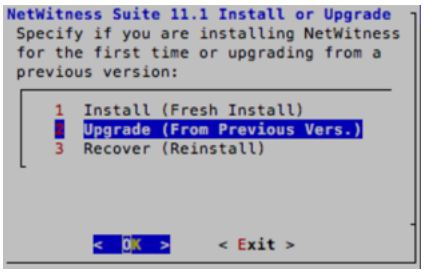
Attention : Si l'hôte choisi pour le serveur NW est incorrect et que vous terminez la mise à niveau, vous devez répéter les étapes 1 à 11 de Installer l'hôte de serveur NW 11.1 pour corriger cette erreur.

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

Choisissez **Non** si vous déjà mis à niveau le serveur NW vers la version 11.1.

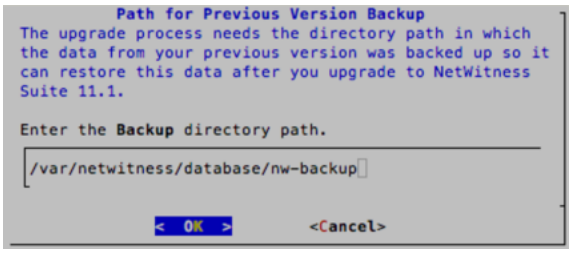
Le message **Installation ou Mise à niveau** s'affiche.

4. Utilisez la flèche vers le bas pour sélectionner **2 Mise à niveau (À partir de la version précédente)**, naviguez vers **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**.



L'invite du chemin de **sauvegarde** s'affiche.

5. Naviguez vers **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** si vous souhaitez conserver ce chemin d'accès. Sinon, modifiez le chemin d'accès, naviguez jusqu'à **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** pour le modifier.



Ce tableau répertorie les chemins de sauvegarde et de restauration par hôte/service.

Hôte	Chemin de sauvegarde	Chemin de restauration
Malware	`/var/lib/rsamlware/nw-backup`	`/var/netwitness/malware_analytics_server/nw-backup/restore`
Event Stream Analysis	`/opt/rsa/database/nw-backup`	`/var/netwitness/database/nw-backup/restore`
Serveur NW	`/var/netwitness/database/nw-backup`	`/var/netwitness/restore`
Pour tous les autres hôtes	`/var/netwitness/database/nw-backup`	`/var/netwitness/database/nw-backup/restore`

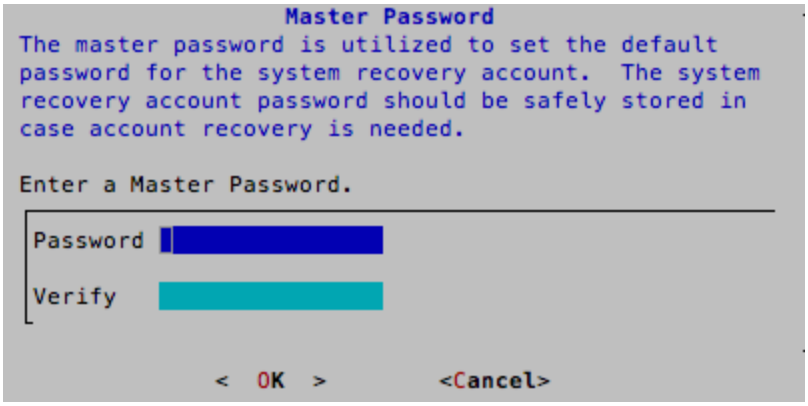
Le message **Mot de passe maître** s'affiche.

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

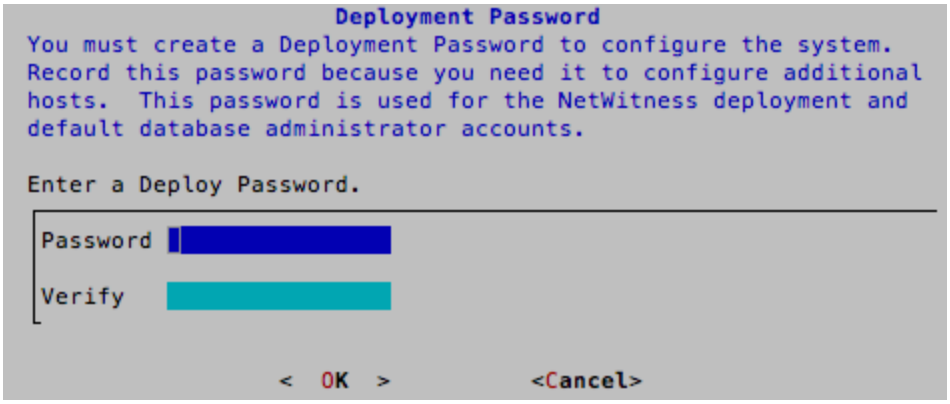
Aucun caractère ambigu n'est pris en charge pour le mot de passe maître et le mot de passe de déploiement. Par exemple :
l'espace { } [ ] ( ) / \ ' " ` ~ ; : .< > -

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



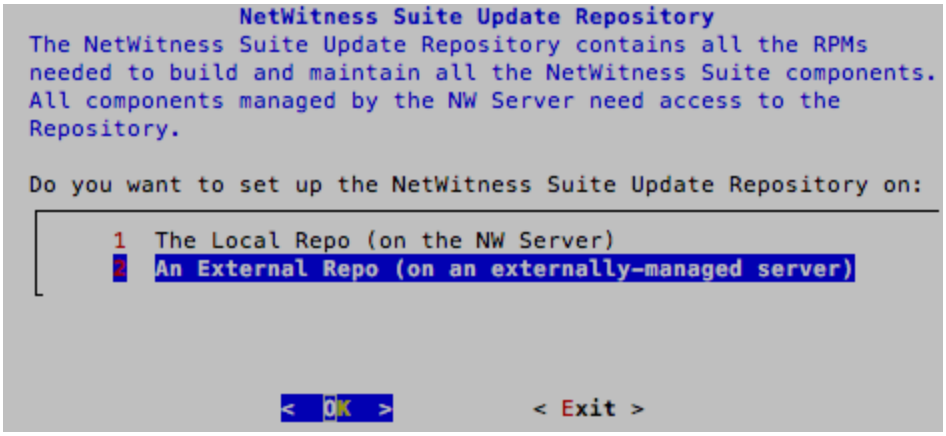
Le message **Mot de passe de déploiement** s'affiche.

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



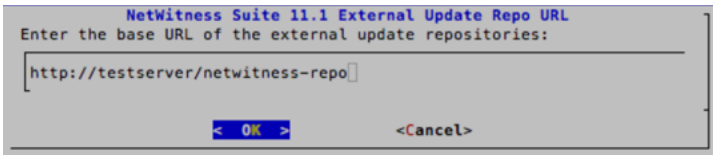
Le message **Mise à jour du référentiel** s'affiche.
Vous devez utiliser le même référentiel que celui que vous avez utilisé pour les hôtes de serveur NW pour tous les hôtes.

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



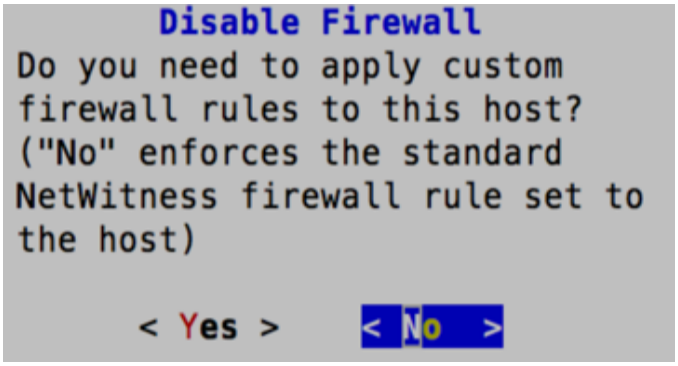
   Le message **Mise à jour du référentiel** s'affiche.
   Reportez-vous à la section Annexe D. Créer le référentiel externe pour obtenir des instructions.
   Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

9. Saisissez l'URL de base du référentiel externe NetWitness Suite (par exemple, **http:/testserver/netwitness-repo**), puis cliquez sur **OK**.

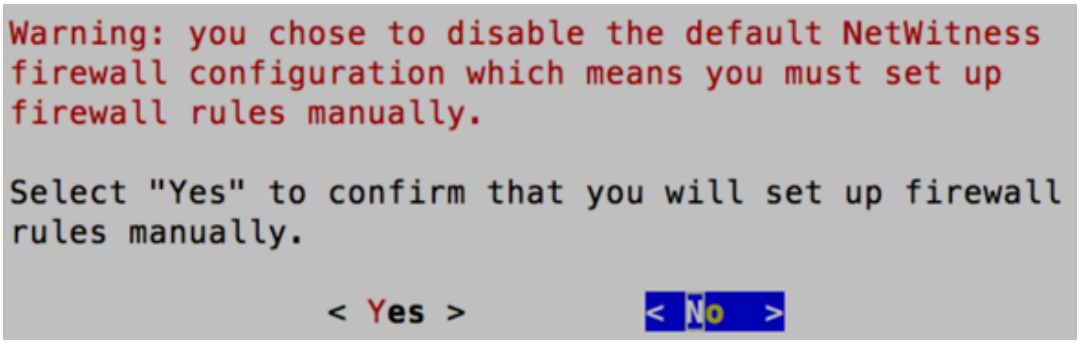


   Le message de **désactivation** ou d'utilisation de la configuration de **pare-feu** standard s'affiche.

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

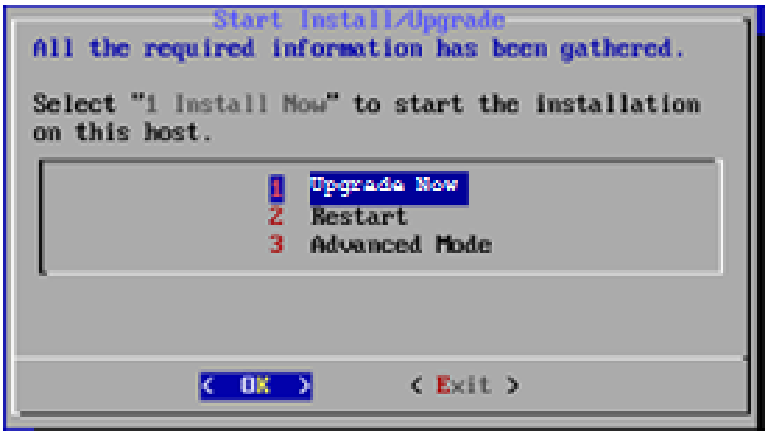


- Pour confirmer votre sélection, choisissez **Oui**, dans le cas contraire, choisissez **Non** pour utiliser la configuration du pare-feu standard.



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 11.1.).

11. Sélectionnez 1 **Mettre à niveau maintenant**, naviguez vers l'onglet **OK**, puis appuyez sur Entrée.



Lorsque **Installation terminée** s'affiche, la mise à niveau du serveur SA 10.6.5.x vers le serveur NW 11.1 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)
```

12. Effectuez les Serveur NW avant de mettre à niveau les hôtes de serveur autre que SA vers la version 11.1.

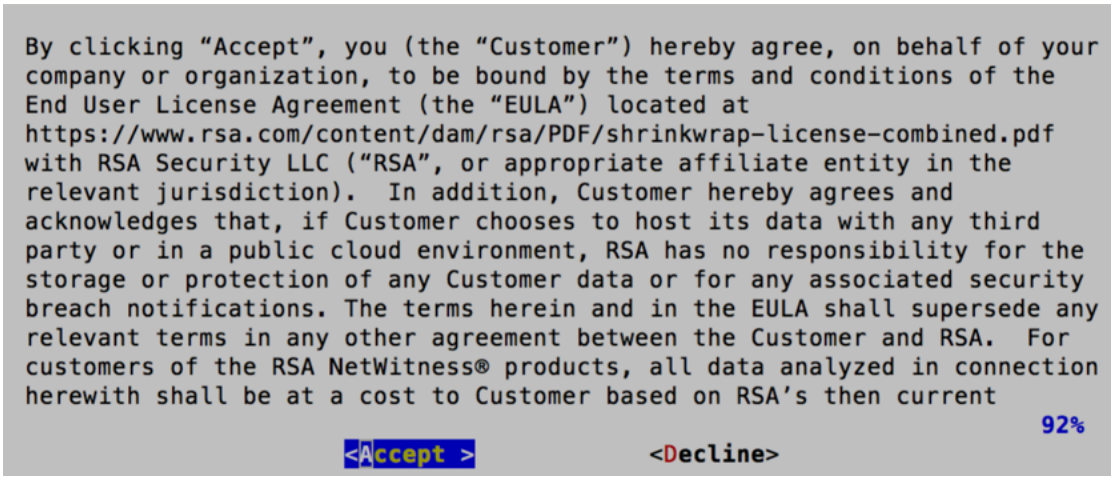
Installer la version 11.1 d'un hôte de serveur autre que NW

Veillez à sauvegarder les données 10.6.5.x pour l'hôte. **Vous devez suivre les instructions indiquées dans Instructions de sauvegarde pour sauvegarder l'hôte.**

Attention : Exécutez la sauvegarde immédiatement avant la mise à niveau de l'hôte vers la version 11.1 afin que les données soient aussi récentes que possible.

Pour installer la version 11.1 d'un hôte de serveur autre que NW, procédez comme suit :

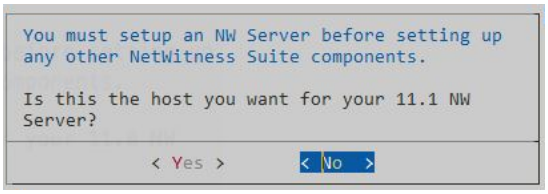
1. Connectez-vous à la console de la machine virtuelle du serveur autre que NW 11.1, puis exécutez la commande `nwsetup-tui`.
   Cette opération démarre le programme d'installation et les conditions générales d'utilisation s'affichent.
2. Naviguez jusqu'à **Accepter** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**.



   Le message **Est-ce l'hôte que vous souhaitez pour votre serveur NW 11.1 ?** s'affiche.

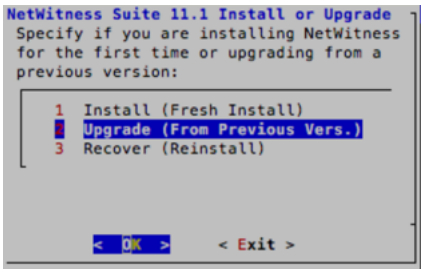
Attention : Si l'hôte choisi pour le serveur NW est incorrect et que vous terminez la mise à niveau, vous devez répéter les étapes 1 à 11 de Installer l'hôte de serveur NW 11.1 pour corriger cette erreur.

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



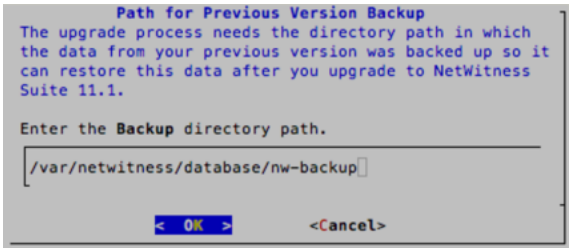
L'invite **Installation** ou **Mise à niveau** s'affiche (**Restaurer** ne s'applique pas à l'installation. Cette option est destinée à la fonctionnalité Reprise après sinistre dans la version 11.1.).

4. Utilisez la flèche vers le bas pour sélectionner **2 Mise à niveau (À partir de la version précédente)**, naviguez vers **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**.



L'invite du chemin de **sauvegarde** s'affiche.

5. Naviguez vers **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** si vous souhaitez conserver ce chemin d'accès. Sinon, modifiez le chemin d'accès, naviguez jusqu'à **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** pour le modifier.



Ce tableau répertorie les chemins de sauvegarde et de restauration par hôte/service.

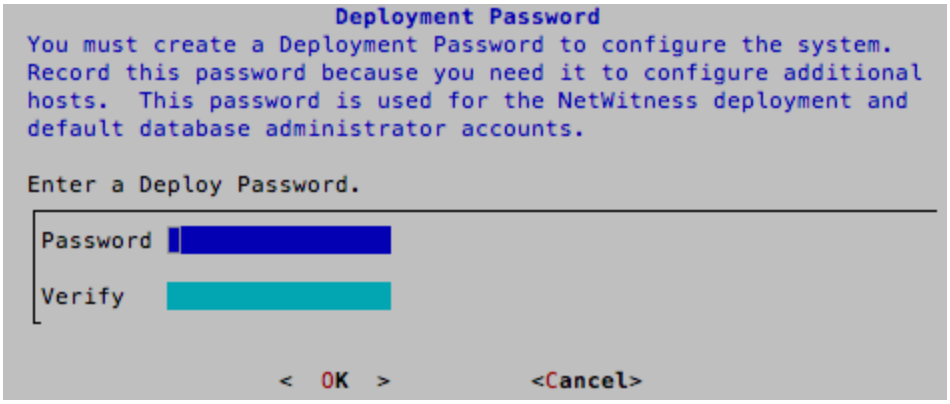
Hôte	Chemin de sauvegarde	Chemin de restauration
Malware	`/var/lib/rsamlware/nw-backup`	`/var/netwitness/malware_analytics_server/nw-backup/restore`

Hôte	Chemin de sauvegarde	Chemin de restauration
Event Stream Analysis	`/opt/rsa/database/nw-backup`	`/var/netwitness/database/nw-backup/restore`
Serveur NW	`/var/netwitness/database/nw-backup`	`/var/netwitness/restore`
Pour tous les autres hôtes	`/var/netwitness/database/nw-backup`	`/var/netwitness/database/nw-backup/restore`

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

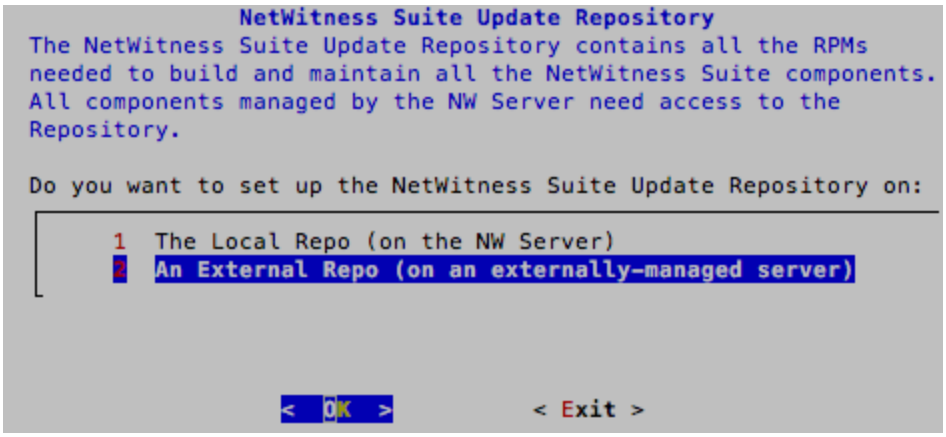
Remarque : Vous devez utiliser le même mot de passe de déploiement que vous avez utilisé lors de la mise à niveau du serveur NW.

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



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

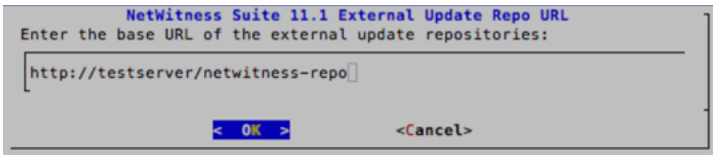
7. Utilisez les flèches vers le haut et vers le bas pour sélectionner **2 Un référentiel externe (sur un serveur géré en externe)**, naviguez jusqu'à **OK**, puis appuyez sur **Entrée**.



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

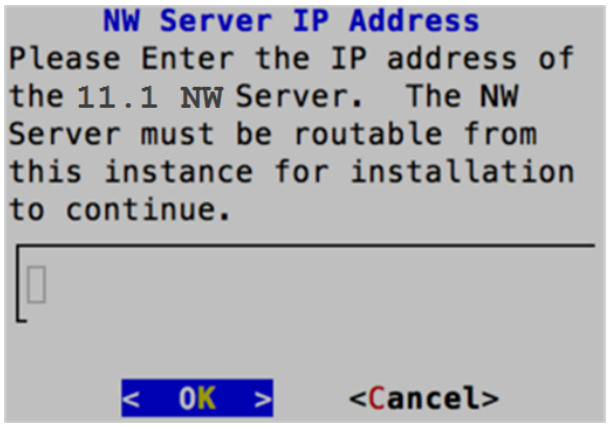
Les référentiels vous donnent accès aux mises à jour RSA et CentOS.

8. Saisissez l'URL de base du référentiel externe NetWitness Suite (par exemple, **http://testserver/netwitness-repo**), puis cliquez sur **OK**. Reportez-vous à la section Annexe D. Créer le référentiel externe pour obtenir des instructions sur la création de ce référentiel, ainsi que l'URL de référentiel externe afin que vous puissiez la saisir dans l'invite suivante.



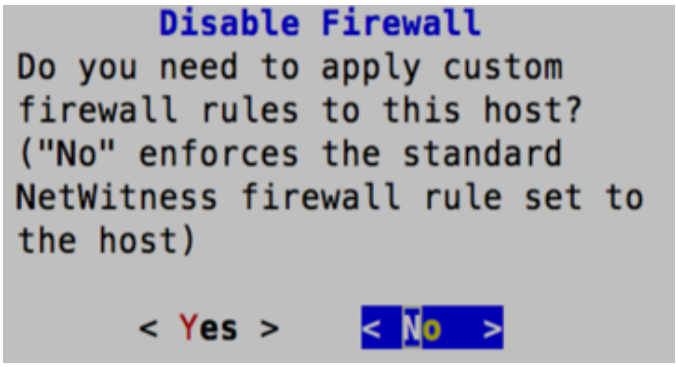
L'**adresse IP du serveur NW** s'affiche.

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

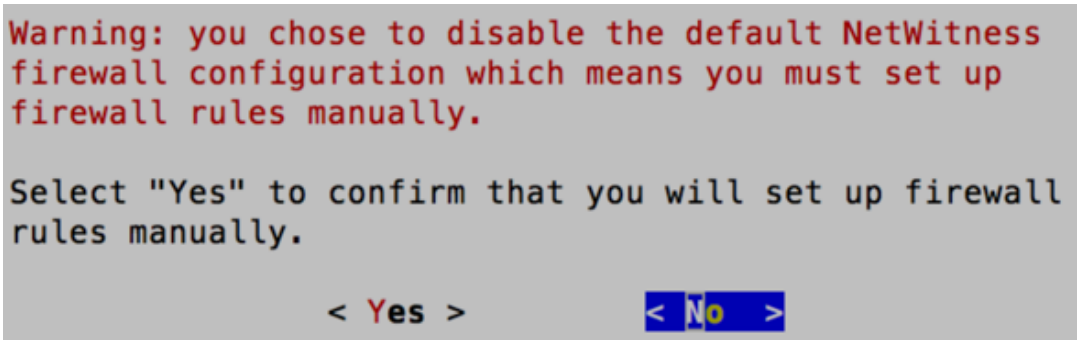


Le message de **désactivation** ou d'utilisation de la configuration de **pare-feu** standard s'affiche.

10. 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.



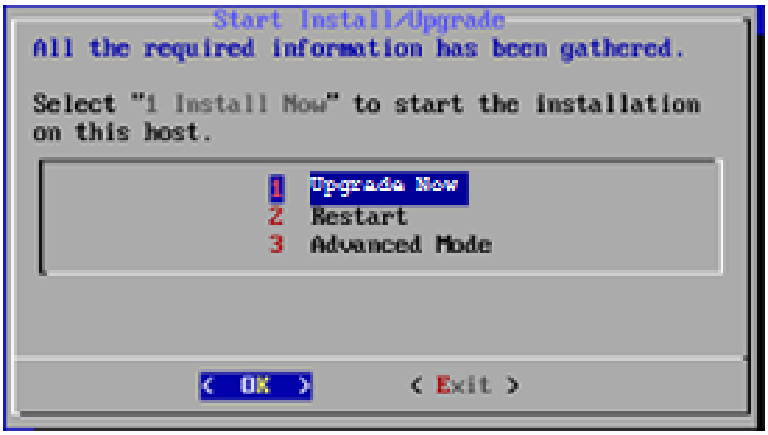
- Si vous sélectionnez **Oui**, confirmez votre sélection.



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

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 11.1.).

11. Sélectionnez 1 **Mettre à niveau maintenant**, naviguez vers l'onglet **OK**, puis appuyez sur **Entrée**.



Lorsque **Installation terminée** s'affiche, la mise à niveau de l'hôte vers la version 11.1 est terminée.

12. Installez le service sur cet hôte :

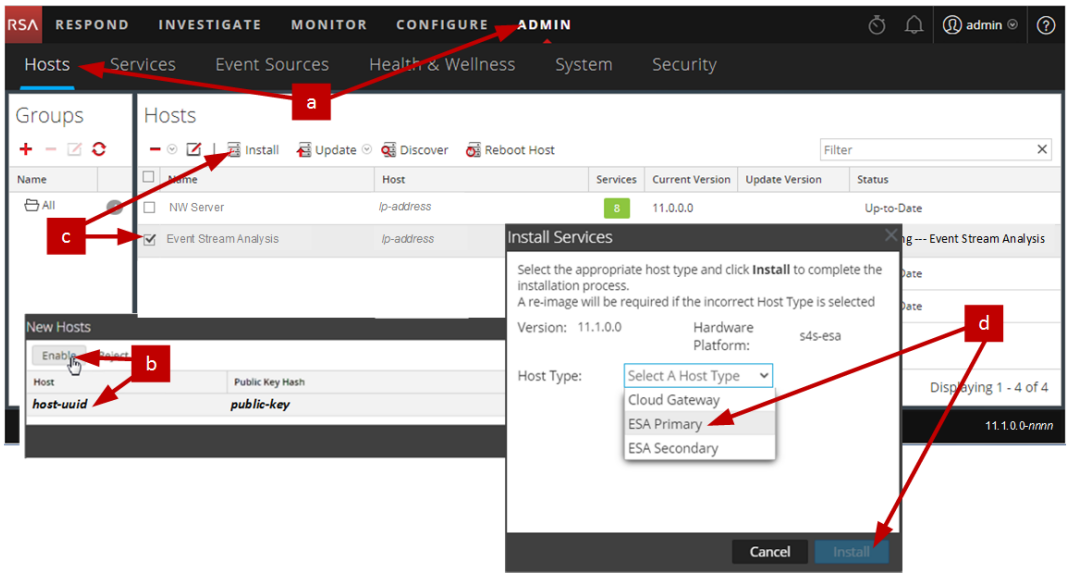
    a. Connectez-vous à NetWitness Suite, puis cliquez sur **ADMIN** > **Hôtes**.
    La boîte de dialogue **Nouveaux hôtes** s'affiche avec la vue **Hôtes** grisée en arrière-plan.

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

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

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



Vous avez terminé la mise à niveau de l'hôte de serveur autre que NW dans NetWitness Suite

Remarque : Lorsque vous effectuez la mise à niveau d'un hôte Respond de la version 10.6.5.x vers la version 11.1, Respond met un certain temps à revenir en ligne. Cela est dû au fait que Respond indexe les données pendant la restauration. La taille des données dans la base de données Mongo détermine la durée.

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

Reportez-vous au *Guide RSA NetWitness Legacy Windows Collection*. Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

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

Tâches postérieures à la mise à niveau

Cette section contient les tâches à réaliser après avoir effectué une mise à niveau de la version 10.6.5.x vers la version 11.1. Ces tâches sont organisées selon les catégories suivantes.

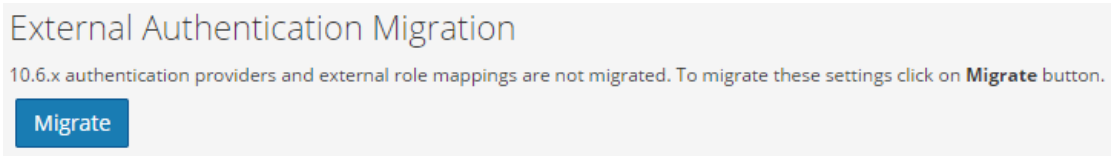
- Serveur NW
- RSA NetWitness® Endpoint
- RSA NetWitness® Endpoint Insights
- Event Stream Analysis
- Investigate
- Log Collection
- Reporting Engine
- Respond
- RSA NetWitness® SecOps Manager
  (RSA Archer Security Incident Management, RSA Archer Security Operations & Breach Management et RSA Archer Issues Management)
- Sauvegarde

Serveur NW

Tâche 1 - Migrer Active Directory (AD)

La première fois que vous vous connectez à l'interface utilisateur NetWitness Suite 11.1, vous devez cliquer sur le bouton Migrer pour effectuer la migration d'Active Directory.

1. Connectez-vous à NetWitness Suite 11.1 à l'aide de vos informations d'identification `admin user`.
2. Dans le menu **NetWitness Suite** 11.1, sélectionnez **ADMIN** > **SÉCURITÉ**, puis cliquez sur l'onglet **Paramètres**.
   La boîte de dialogue suivante s'affiche.

3. Cliquez sur **Migrer**.
   La migration est terminée et la boîte de dialogue se ferme.

Tâche 2 - Modifier la configuration AD migrée pour télécharger le certificat

Si vous vous êtes authentifié(e) via le serveur Active Directory (AD) et avez activé SSL pour la connexion AD dans la version 10.6.5.x, vous devez modifier la configuration AD migrée pour télécharger le certificat du serveur Active Directory.

Exécutez la procédure suivante pour modifier la configuration AD migrée afin de télécharger le certificat.

1. Dans le menu **NetWitness Suite** 11.1, sélectionnez **ADMIN** > **Sécurité**, puis cliquez sur l'onglet **Paramètres**.
2. Sous **Paramètres Active Directory**, sélectionnez une configuration Active Directory, puis cliquez sur  .

   La boîte de dialogue Modifier la configuration s'affiche.
3. Accédez au champ **Fichier de certificat**, cliquez sur **Parcourir** et sélectionnez un certificat à partir de votre réseau.
4. Cliquez sur **Enregistrer**.

Tâche 3 - Reconfigurer le module PAM (Pluggable Authentication Module) dans la version 11.1

Vous devez reconfigurer le PAM une fois la mise à niveau vers la version 11.1 effectuée. Pour obtenir des instructions, reportez-vous à la section *RSA NetWitness® Suite Configurer la fonctionnalité de connexion PAM dans le Guide de la sécurité du système et de la gestion des utilisateurs*. Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

Vous pouvez consulter vos fichiers de configuration 10.6.5.x PAM dans le répertoire **/etc.** de vos données de sauvegarde 10.6.5.x pour obtenir des informations.

Tâche 4 - Restaurer les serveurs NTP

Vous devez utiliser l'interface utilisateur NetWitness Suite 11.1 pour restaurer les configurations de serveur NTP. Informations de configuration du serveur NTP situées dans `$BUPATH/restore/etc/ntp.conf`. Utilisez le nom du serveur NTP et le nom d'hôte du fichier `/var/netwitness/restore/etc/ntp.conf`. Consultez la section « Configurer les serveurs NTP » dans *RSA NetWitness® Suite - Guide de configuration système* pour obtenir des instructions détaillées sur la façon d'ajouter des serveurs NTP. Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

Tâche 5 - Restaurer les licences pour les environnements sans accès à FlexNet Operations-On Demand

Si votre environnement n'a pas d'accès à FlexNet Operations-On Demand, vous devez à nouveau télécharger vos licences NetWitness Suite. Reportez-vous à l'« Étape 1. Enregistrer le serveur NetWitness » dans le *Guide de gestion des licenses de RSA NetWitness Suite* pour obtenir des instructions sur la façon de télécharger à nouveau des licences.Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

Tâche 6 - Mapper à nouveau la licence de serveur virtuel NW à l'adresse MAC de la version 10.6.5.x

Si vous mettez à niveau un serveur Security Analytics en cours d'exécution sur une machine virtuelle, placez l'hôte virtuel de serveur NW 11.1 à l'adresse MAC de la version 10.6.5.x pour conserver la licence. Reportez-vous à la section « Gestion des licences » : Étape 1. Enregistrer le serveur NetWitness » dans *RSA NetWitness Suite - Guide de gestion des licences* pour obtenir des instructions sur la façon de remapper une licence à une nouvelle adresse MAC. » Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

(Conditionnel) Tâche 7 - Si vous avez désactivé la configuration standard du pare-feu - Ajouter des IPtables personnalisés

Lors de la mise à niveau, vous avez la possibilité d'utiliser ces règles ou de les désactiver. Si vous les avez désactivées, suivez ces instructions comme une base de référence pour créer des ensembles de règles de pare-feu gérées par l'utilisateur sur tous les hôtes pour lesquels vous avez désactivé la configuration de pare-feu standard.

Remarque : Vous pouvez vous reporter à `$BUPATH/restore/etc/sysconfig/iptables` et à `$BUPATH/restore/etc/sysconfig/ip6tables` dans le dossier de restauration de la sauvegarde pour mettre à jour les fichiers `ip6tables` et `iptables`. Le fichier `/etc/netwitness/firewall.cfg` contient les règles de pare-feu standard `iptables`.

1. Ouvrez une session SSH sur chaque hôte, puis connectez-vous avec vos informations d'identification root.
2. Mettez à jour les fichiers suivants `ip6tables` et `iptables` avec les règles de pare-feu personnalisées.
   ```
   /etc/sysconfig/iptables
   /etc/sysconfig/ip6tables
   ```
3. Rechargez les services `iptables` et `ip6tables`.
   ```
   service iptables reload
   service ip6tables reload
   ```

(Conditionnel) Tâche 8 - Spécifier les ports SSL si vous n'avez jamais configuré les connexions approuvées

Effectuez cette tâche uniquement si n'avez jamais configuré les connexions approuvées. Vous n'avez pas configuré les connexions approuvées si vous avez :

- Utilisé l'image ISO de base pour la version 10.3.2 ou une version antérieure.
- Mis à jour le système exclusivement à l'aide de RPM pour obtenir la version 10.6.5.

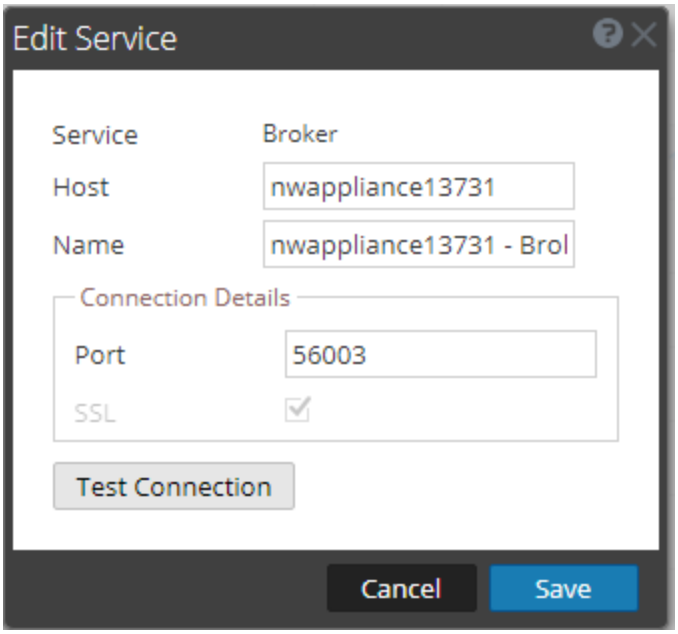
NetWitness Suite 11.1 ne peut pas communiquer avec les services de base pour ces clients, car ils utilisent un port 500XX non SSL. Vous devez mettre à jour les ports du service Core vers un port SSL dans la boîte de dialogue Modifier le service.

1. Dans le menu **NetWitness Suite** 11.1, sélectionnez **ADMIN** > **Services**.
2. Sélectionnez chaque service Core et remplacez son port non SSL par un port SSL.

Service	Non SSL	SSL
Broker	50003	56003
Concentrator	50005	56005
Decoder	50004	56004
Log Decoder	50002	56002

3. Cliquez sur (Modifier) depuis la barre d'outils de la vue **Services**.
   La boîte de dialogue Modifier le service s'affiche.

4. Modifiez le port de non SSL à SSL, comme indiqué dans le tableau, puis cliquez sur **Enregistrer** (par exemple, remplacez le port du Broker 50003 par 56003).



Tâche 9 - (Conditionnel) Corriger les modèles de journal d'audit qui ne sont pas mis à jour dans le fichier de configuration de sortie Logstash

Problème : Lorsqu'un utilisateur effectue une mise à jour de la version 10.6.5 vers la version 11.1 et de la version 11.0.0.0 vers la version 11.1, si un audit global est configuré, les modèles de journal d'audit ne sont pas mis à jour dans le fichier de configuration de sortie Logstash.

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

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

1. Dans le menu **NetWitness Suite** 11.1, sélectionnez **ADMIN** > **Système** > **Notifications globales**.
   La vue **Notifications globales** s'affiche.
2. Cliquez sur l'onglet **Serveurs**, sélectionnez n'importe quel serveur syslog.
3. Cliquez sur (icône de modification), puis cliquez sur **Enregistrer**.

RSA NetWitness® Endpoint

Tâche 10 - Reconfigurer un feed récurrent configuré à partir d'une ancienne version Endpoint parce que la version Java a changé.

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

1. Importez le certificat de l'autorité de certification NetWitness Endpoint dans le magasin de confiance NetWitness Suite, comme décrit dans « Exporter le certificat SSL de NetWitness Endpoint » dans la rubrique « Configurer des données contextuelles à partir de Endpoint via un feed récurrent » dans le *Guide d'intégration de RSA NetWitness Endpoint* pour importer le certificat.
   Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

RSA NetWitness® Endpoint Insights

(Facultatif) Tâche 11 - Installer Endpoint Hybrid ou Endpoint Log Hybrid

Voir :

Le *Guide d'installation des hôtes physiques RSA NetWitness Suite 11.1* pour obtenir des instructions relatives à l'installation sur un hôte physique.

Le *Guide d'installation des hôtes virtuels RSA NetWitness Suite 11.1* pour obtenir des instructions relatives à l'installation sur un hôte virtuel.

Tâche 12 - Reconfigurer les alertes Endpoint via le bus de messages

1. Sur le serveur NetWitness Endpoint, modifiez la configuration de l'hôte virtuel dans le fichier `C:\Program Files\RSA\ECAT\Server\ConsoleServer.exe` afin de reproduire la configuration suivante.
   ```
   <add key="IMVirtualHost" value="/rsa/system" />
   ```

   Remarque : Dans NetWitness Suite 11.1, l'hôte virtuel est `/rsa/system`. Pour les versions 10.6.5.x et antérieures, l'hôte virtuel est `/rsa/sa`.

2. Redémarrez le serveur API et le serveur de console.
3. Ouvrez une session SSH sur le serveur NW et connectez-vous avec les informations d'identification `root`.

4. Exécutez la commande suivante pour ajouter tous les certificats au magasin d'approbations.
   `orchestration-cli-client --update-admin-node`
5. Exécutez la commande suivante pour redémarrer le serveur RabbitMQ.
   `systemctl restart rabbitmq-server`
   Le compte NetWitness Endpoint doit être automatiquement disponible sur RabbitMQ.
6. Importez les fichiers `/etc/pki/nw/ca/nwca-cert.pem` et `/etc/pki/nw/ca/ssca-cert.pem` depuis le serveur NW et ajoutez-les aux magasins de certificats racines de confiance sur le serveur Endpoint.

Tâches Event Stream Analysis (ESA)

Tâche 13 - Reconfigurer la détection automatisée des menaces pour ESA

Si vous avez utilisé la détection automatisée des menaces dans la version 10.6.5.x, vous devez exécuter les étapes suivantes pour la reconfigurer à l'aide du service ESA Analytics dans la version 11.1.

1. Dans le menu **NetWitness Suite** 11.1, sélectionnez **ADMIN** > **Système** > **ESA Analytics**. Les modules Domaines suspects, les systèmes Commande et contrôle (C2) pour les paquets et C2 pour les logs, requièrent une liste blanche nommée « **domains_whitelist** ».
2. Conditionnel - Si votre liste blanche de détection automatisée des menaces précédente s'affiche dans l'onglet **Répertoires** du service Context Hub :
   a. Cliquez sur **ADMIN** > **Services**, sélectionnez le service Context Hub, dans le menu déroulant des commandes d'action (), cliquez sur **Vue** > **Configuration** > onglet **Listes**).
   b. Renommez votre ancienne liste blanche de détection automatisée des menaces « `domains_whitelist` » pour le module Domaines suspects.

Pour plus d'informations, reportez-vous au *Guide de détection automatisée des menaces pour NetWitness Suite* et à la section « Configurer ESA Analytics » du *Guide de configuration NetWitness Suite ESA*. Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

Tâche 14 - Pour l'intégration à Web Threat Detection, NetWitness SecOps Manager ou NetWitness Endpoint, configurer une SSL à authentification mutuelle

Si vous intégrez Web Threat Detection, NetWitness SecOps Manager ou NetWitness Endpoint, vous devez configurer une SSL à authentification mutuelle sur chaque système intégré afin que l'application puisse s'authentifier elle-même lors de la connexion au bus de messages RabbitMQ.

Remarque : Utilisez les noms d'utilisateur et les mots de passe RabbitMQ obtenus lors de la sauvegarde de vos données de la version 10.6.5.x (reportez-vous à la section Instructions de sauvegarde).

1. Créez un utilisateur sur le système hôte qui s'intègre à NetWitness Suite en vous connectant à l'hôte et en exécutant la commande `rabbitmqctl` suivante.

   ```
   > rabbitmqctl add_user <username> <password>
   ```

   Par exemple :

   ```
   > rabbitmqctl add_user wtd-incidents incidents
   ```

2. Définissez les autorisations des utilisateurs en exécutant la commande suivante (utilisez le nom d'utilisateur dans l'étape 1) :

   ```
   > rabbitmqctl set_permissions -p /rsa/system <username> ".*", ".*",
   ".*"
   ```

   Par exemple :

   ```
   > rabbitmqctl set_permissions -p /rsa/system wtd-incidents ".*",
   ".*", ".*"
   ```

Tâche 15 - Activer le Tableau de bord des indicateurs de malware et de menaces

Dans la version 11.1.0, le **Tableau de bord des indicateurs de menaces** de la version 10.6.5.x a été renommé **Tableau de bord des indicateurs de malware et de menaces**. Si vous utilisiez ce tableau de bord dans la version 10.6.5.x, vous devez :

1. Activez le **Tableau de bord des indicateurs de malware et de menaces** dans la version 11.1.

2. Définissez la nouvelle source de données pour les dashlets.

   Reportez-vous à la section « Dashlets » dans RSA Link (https://community.rsa.com/docs/DOC-81463) pour une description de Dashlets dans le cadre de NetWitness Suite.

Investigate

Tâche 16 - S'assurer que les rôles d'utilisateur disposent de rôles d'utilisateurs personnalisés avec les autorisations `Investigate-server` pour l'accès à la vue Analyse d'événements

Après la mise à niveau vers la version 11.1.0.0, les rôles d'utilisateur personnalisés ne disposent pas de l'autorisation `investigate-server.*` activée par défaut. Exécutez la procédure suivante pour vous assurer que les rôles d'utilisateur appropriés ont la possibilité d'accéder à Analyse d'événements.

1. Connectez-vous à NetWitness Suite 11.1.0.0 en tant qu'utilisateur `Admin`.
2. Dans le menu **NetWitness Suite** 11.1, sélectionnez **ADMIN** > **Sécurité**.
3. Cliquez sur l'onglet **Rôles**.
4. Sélectionnez les rôles ayant besoin d'autorisations `investigate-server.*` , puis cliquez sur (icône de modification).
5. Sélectionnez l'onglet **investigate-server** sous **Autorisations**.
6. Si la case investigate-server n'est pas cochée, cochez-la pour les utilisateurs ayant besoin d'accéder à Event Analysis.

7. Cliquez sur **Enregistrer**.

Log Collection

Tâche 17 - Réinitialiser les valeurs système stables pour Log Collector après la mise à niveau

Effectuez les tâches suivantes pour réinitialiser les valeurs système stables pour le Log Collector après la mise à niveau vers la version 11.1 afin de vérifier que tous les protocoles de collecte fonctionnent correctement.

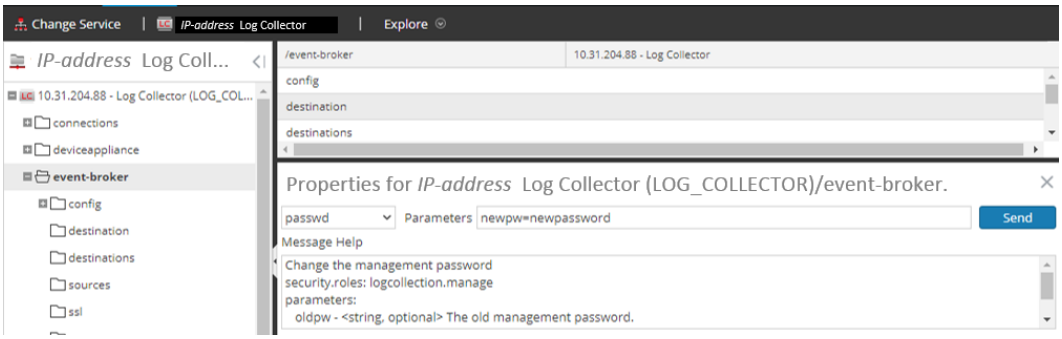
Réinitialiser les valeurs de système stable pour le Lockbox

Le Lockbox stocke la clé de chiffrement de la source d'événement et les autres mots de passe pour le Log Collector. Le service Log Collector ne peut pas ouvrir le Lockbox en raison des modifications des valeurs système stables. Par conséquent, vous devez réinitialiser les valeurs système stables pour le Lockbox. Consultez la section « Log Collection : Étape 3. Configurer un Lockbox » dans le *RSA NetWitness® Suite Guide de configuration de Log Collection* pour obtenir des instructions. Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

Mettre à jour le mot de passe du compte utilisateur RabbitMQ du service Log Collector

Si le mot de passe du compte utilisateur RabbitMQ du service Log Collector a été modifié, vous devez le saisir à nouveau après la mise à niveau vers la version 11.1.

1. Dans le menu **NetWitness Suite** 11.1, sélectionnez **ADMIN > Services**.
2. Sélectionnez le service Log Collector.
3. Cliquez sur  (Actions) > **Vue** > **Explorer**.
4. Cliquez avec le bouton droit sur `event-broker` > **Propriétés**.
5. Sélectionnez `passwd` dans la liste déroulante, saisissez `newpw=><newpassword>` dans les paramètres (où `<newpassword>` est le mot de passe du compte utilisateur RabbitMQ), puis cliquez sur **Envoyer**.



(Facultatif pour les mises à niveau à partir de la version 10.6.5.x avec le mode FIPS activé pour les Log Collectors, les Log Decoders et les Packet Decoders)

Tâche 18 - Activer le mode FIPS

Le mode FIPS 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 savoir comment activer le mode FIPS pour ces services, consultez la rubrique « Maintenance du système : Activer ou désactiver le mode FIPS » dans le *RSA NetWitness® Suite Guide de maintenance du système*. Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

Reporting Engine

Tâche 19 - Restaurer les certificats d'autorité de certification pour les serveurs Syslog externes pour Reporting Engine

Vous devez restaurer les certificats d'autorité de certification après la mise à niveau à partir de la sauvegarde effectuée avant la mise à niveau. Ce script de sauvegarde enregistre les certificats d'autorité de certification de la version 10.6.5.x dans le répertoire `/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.111-0.b15.el6_8.x86_64/jre/lib/security/cacerts`.

Exécutez la procédure suivante pour restaurer les certificats d'autorité de certification dans la version 11.1.

1. Ouvrez une session SSH sur l'hôte du serveur NW.
2. Exportez les certificats d'autorité de certification.
   ```
   keytool -export -alias <alias_name> -keystorepath_to_keystore_file -rfc -file path_to_certificate_file
   ```
3. Copiez le fichier pem d'autorité de certification dans le répertoire `/etc/pki/nw/trust/import`.

(Conditionnel) Tâche 20 - Restaurer le stockage externe pour le service Reporting Engine

Si vous disposez d'un stockage externe pour le service Reporting Engine (par exemple, réseau SAN ou NAS pour stocker les rapports), vous devez restaurer le montage que vous avez dissocié avant la mise à niveau. Consultez la section « Reporting Engine : Ajouter de l'espace supplémentaire pour les rapports volumineux » dans le *RSA NetWitness® Suite Guide de configuration de Reporting Engine* pour obtenir des instructions. Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

Respond

(Conditionnel) Tâche 21 - Restaurer les rôles Analyste personnalisés

Si vous disposiez de rôles Analyste personnalisés dans la version 10.6.5.x, vous devez les rétablir dans la version 11.1. Consultez « Ajouter un rôle et attribuer des autorisations » dans *RSA - NetWitness SuiteGuide de la sécurité du système et de la gestion des utilisateurs*. Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

Tâche 22 - Restaurer les clés personnalisées du service Respond

Dans la version 10.6.5.x, si vous avez ajouté l'utilisation d'une clé personnalisée dans la clause **Regrouper par**, c'est que le fichier `alert_rules.json` a été modifié. Le fichier `alert_rules.json` contient le schéma de règle d'agrégation. RSA a déplacé le fichier `alert_rules.json` vers le nouvel emplacement suivant : `/var/lib/netwitness/respond-server/scripts`

1. Copiez les clés personnalisées à partir du fichier `/opt/rsa/im/fields/alert_rules.json` dans le répertoire de sauvegarde.
   Ce répertoire correspond à l'emplacement où le fichier `alert_rules.json` est restauré à partir de la sauvegarde 10.6.5.x.
2. Accédez à `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` dans la version 11.1.
   Il s'agit du nouveau fichier pour la version 11.1.
3. Modifiez `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` pour inclure les clés personnalisées que vous avez copiées à l'étape 1.

Tâche 23 - Restaurer les scripts de normalisation personnalisés du service Respond

RSA a réintégré les scripts de normalisation du service Respond dans la version 11.1 et les a déplacés vers le nouvel emplacement suivant :
`/var/lib/netwitness/respond-server/scripts`
Si vous avez personnalisé ces scripts dans la version 10.6.5.x, vous devez :

1. Accéder au répertoire `/opt/rsa/im/scripts`.
   C'est dans ce répertoire que les scripts de normalisation du service Respond suivants sont restaurés à partir de la sauvegarde 10.6.5.x.
   `data_privacy_map.js`
   `normalize_alerts.js`
   `normalize_core_alerts.js`
   `normalize_ecat_alerts.js`
   `normalize_ma_alerts.js`
   `normalize_wtd_alerts.js`
   `utils.js`
2. Copiez n'importe quelle logique personnalisée à partir des scripts 10.6.5.x.
3. Accédez au répertoire `/var/lib/netwitness/respond-server/scripts`.
   Ce répertoire correspond à l'endroit où NetWitness Suite 11.1 stocke les scripts réintégrés.
4. Modifiez les nouveaux scripts afin d'inclure la logique personnalisée copiée à l'étape 2 depuis les scripts de la version 10.6.5.x.
5. Copiez n'importe quelle logique personnalisée à partir du fichier `/opt/rsa/im/fields/alert_rules.json`.
   Le fichier `alert_rules.json` contient le schéma de règle d'agrégation.

Tâche 24 - Ajouter des paramètres de notification de réponse pour les rôles personnalisés

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

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

Tâche 25 - Configurer manuellement les paramètres de notification de réponse

Les paramètres de notification d'Incident Management dans NetWitness Suite versions 10.6.5.x à 11.1 diffèrent des paramètres de notification de réponse disponibles dans la version 11.1. Ainsi, les paramètres des versions 10.6.5.x à 11.1 existantes ne seront pas transférés à la version 11.1.

Les paramètres de notification NetWitness Respond permettent d'envoyer des notifications par e-mail aux responsables du SOC et à l'analyste en charge de l'incident lors de sa création ou mise à jour.

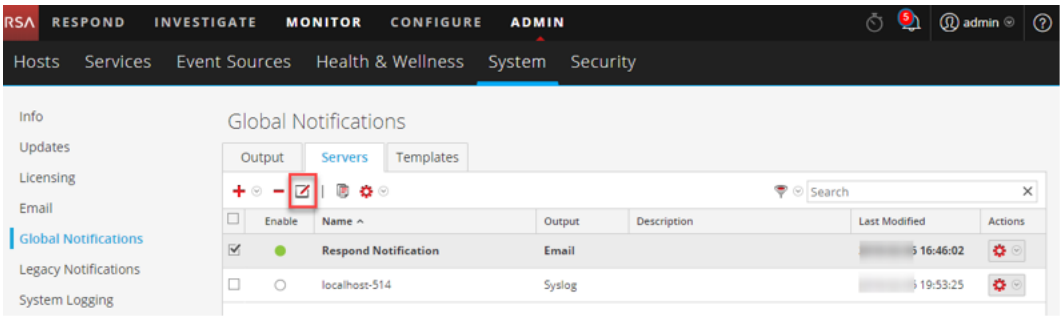
Pour configurer manuellement les paramètres de notification de réponse, accédez à **CONFIGURER** > **Notifications de réponse**. Reportez-vous à la procédure « Configurer les paramètres de notification de réponse » dans le *Guide de configuration NetWitness Respond*.

Les serveurs de notification des versions 10.6.5.x à 11.1 ne s'afficheront pas dans la liste déroulante du serveur de messagerie. Les serveurs de messagerie doivent être modifiés et enregistrés dans le panneau Serveurs de notifications globales (**ADMIN** > **Système** > **Notifications globales** > onglet **Serveur**).

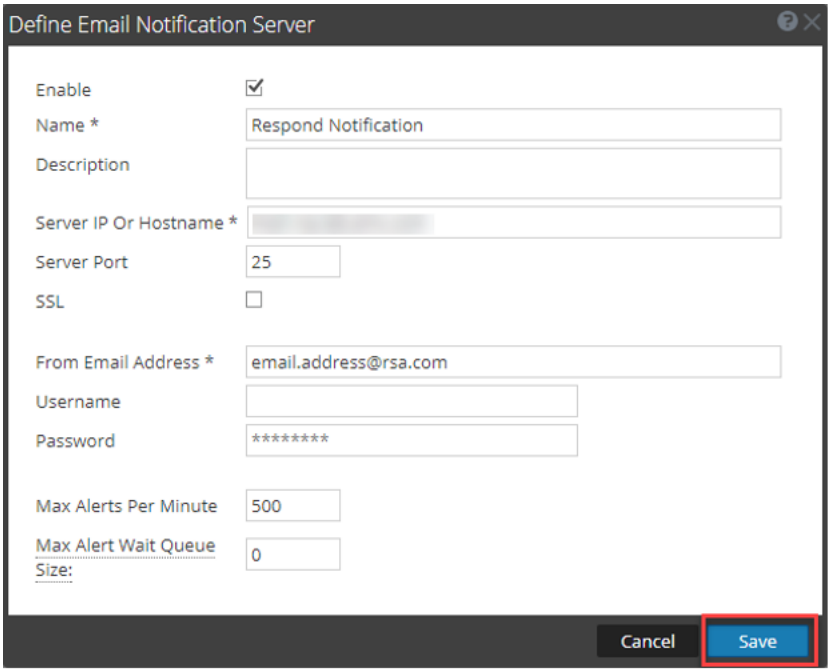
1. Dans le menu **NetWitness Suite** 11.1, sélectionnez **ADMIN** > **Système** > **Notifications globales** > **Serveur**.
2. Accédez à **CONFIGURER** > **Notifications de réponse**. La vue Paramètres de notification de réponse s'affiche.
3. Notez que les serveurs de notification par e-mail n'apparaissent pas dans la liste déroulante Serveurs de messagerie.
4. Cliquez sur le lien **Paramètres du serveur de messagerie**. Vous verrez le panneau Notifications globales.
5. Cliquez sur l'onglet **Serveurs**.

6. Pour chacun de vos serveurs de notification par e-mail :

   a. Sélectionnez le serveur de notification par e-mail et cliquez sur .



   b. Dans la boîte de dialogue Définir un serveur de notification par e-mail, saisissez les informations requises et cliquez sur **Enregistrer**.



7. Revenez à **CONFIGURER** > **Notifications de réponse**. Vos serveurs apparaîtront dans la liste déroulante **Serveur de messagerie**.
   Les modèles des notifications personnalisées Gestion des incidents ne peuvent pas être migrés vers la version 11.1. La version 11.1 ne prend en charge aucun modèle personnalisé.

Tâche 26 - Mettre à jour le groupe de règles des incidents par défaut en fonction des valeurs

Quatre des règles d'incident par défaut utilisent désormais l'« Adresse IP source » en tant que valeur Regrouper par. Pour mettre à jour les règles par défaut, modifiez la valeur Regrouper par des règles par défaut suivantes pour « Adresse IP source » :

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

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

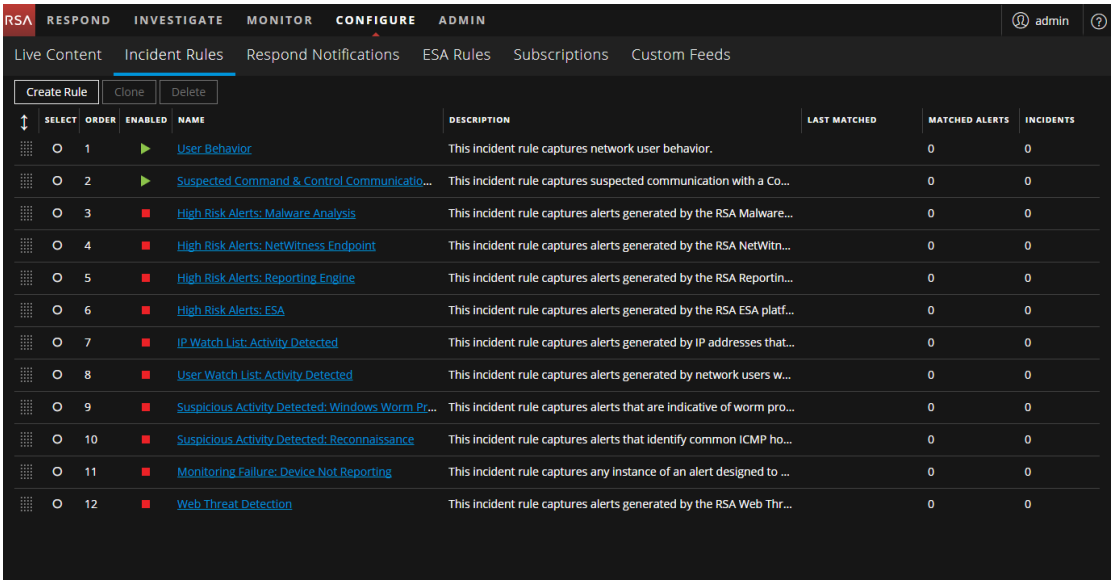
Tâche 27 - Ajouter le champ Regrouper par aux règles d'incident

Le champ **Regrouper par** n'est pas obligatoire dans la version 10.6.5, mais il est nécessaire dans la version 11.1. Après la mise à niveau vers

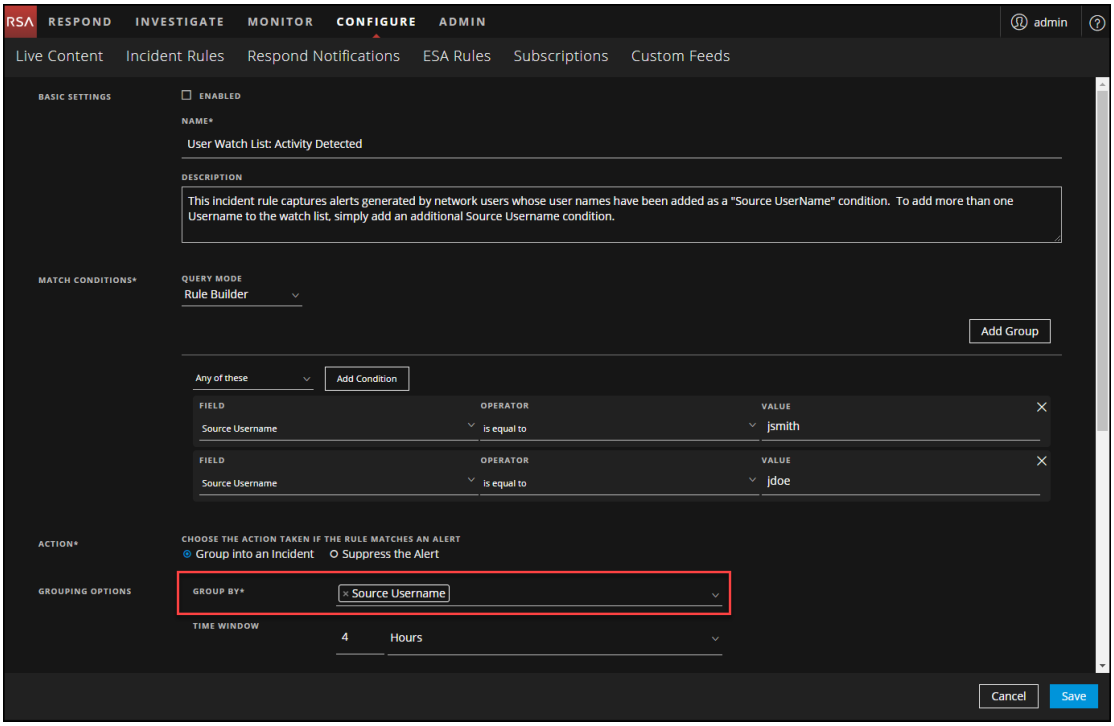
la version 11.1, certaines règles d'incident n'ont pas de champ **Regrouper par**, vous devez donc les ajouter aux règles ou les règles ne fonctionneront pas et ne créeront pas d'incidents.

Procédez comme suit pour chaque règle d'incident :

1. Dans le menu **NetWitness Suite** 11.1, accédez à **CONFIGURER** > **Règles d'incident**, puis cliquez sur le lien dans la colonne Nom de la règle que vous souhaitez mettre à jour.



2. Dans le champ Regrouper par, vérifiez qu'une valeur Regrouper par est sélectionnée. Si ce n'est pas le cas, sélectionnez-en une.



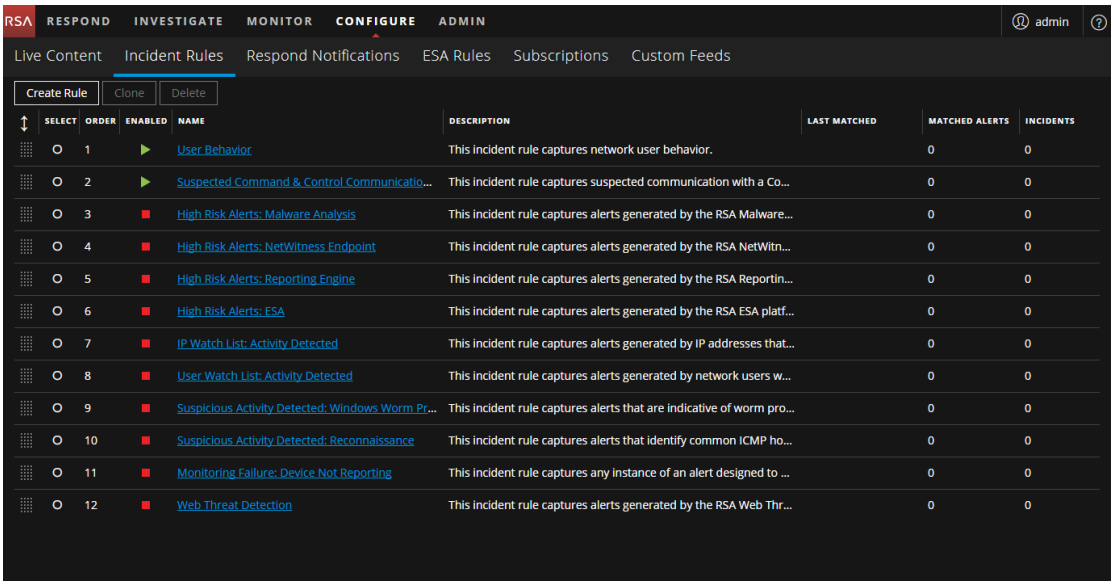
3. Cliquez sur **Enregistrer** pour mettre à jour la règle.
   Pour plus d'informations sur les règles d'incident, consultez le *Guide de configuration NetWitness Respond*. Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

Tâche 28 - Mettre à jour les règles d'incident identifiées dans le domaine dans la tâche de préparation de la mise à niveau des conditions de mise en correspondance

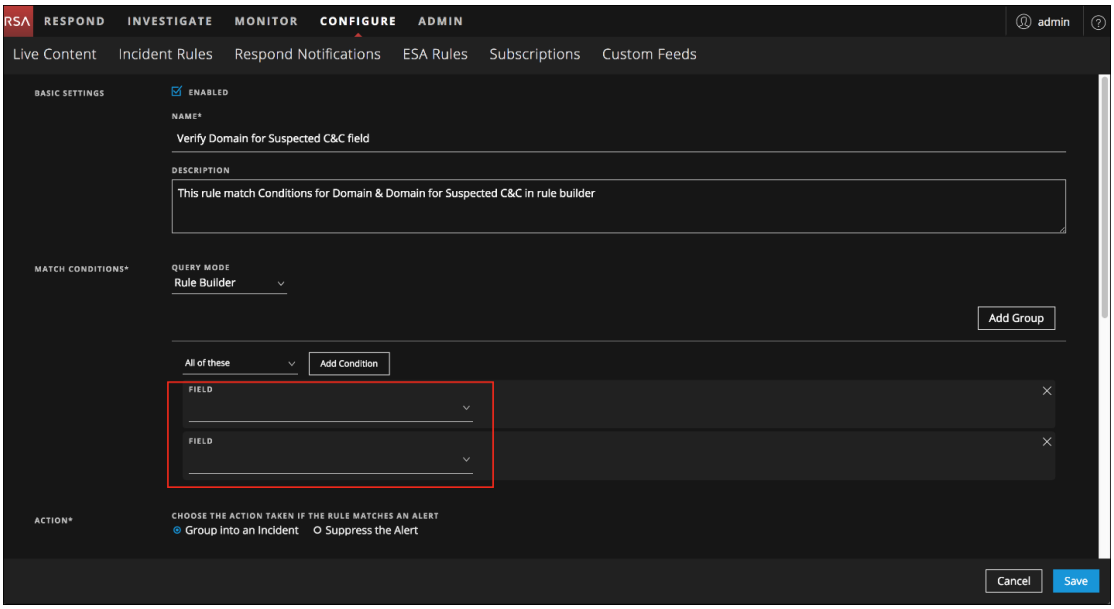
Modifiez les règles d'incident que vous avez identifiées à la tâche de préparation de la mise à niveau Tâche 4 : Vérifier les conditions de mise en correspondance des règles d'agrégation pour « Domaine » ou « Domaine de C&C suspect », contenant le domaine ou le domaine de C&C suspect dans les conditions de mise en correspondance du générateur de règles, pour n'utiliser que Domaine.

Pour chaque règle identifiée précédemment :

1. Dans le menu **NetWitness Suite** 11.1, sélectionnez **CONFIGURER** > **Règles de l'incident**, puis cliquez sur le lien dans la colonne Nom de la règle que vous souhaitez mettre à jour.



2. Dans la section **Conditions de mise en correspondance**, dans les cellules vides, sélectionnez **Domaine** dans la liste déroulante, puis sélectionnez les conditions que vous avez précédemment identifiées dans les tâches de pré-mise à niveau.



3. Cliquez sur **Enregistrer** pour mettre à jour la règle.
Pour plus d'informations sur les règles d'incident, consultez le *Guide de configuration NetWitness Respond*. Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

RSA NetWitness® SecOps Manager

(RSA Archer Security Incident Management, RSA Archer Security Operations & Breach Management et RSA Archer Issues Management)

Tâche 29 - Reconfigurer l'intégration de NW SecOps Manager

Pour plus d'informations sur la façon de reconfigurer NW SecOps pour Event Stream Analysis, Reporting Engine et Respond, reportez-vous au *Guide d'intégration de RSA Archer*. Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

Sauvegarde

Tâche 30 - Supprimer les fichiers associés à la sauvegarde des répertoires locaux de l'hôte

Attention : (1) Vous devez conserver une copie de tous les fichiers de sauvegarde sur un hôte externe. (2) Vérifiez que toutes vos données de sauvegarde sont restaurées dans 11.1 avant de supprimer les fichiers associés aux sauvegardes dans les répertoires locaux sur vos hôtes 11.1.

Sauvegarder les fichiers `.tar`

Une fois que tous les hôtes sont mis à niveau vers la version 11.1, vous devez supprimer :

- les fichiers de sauvegarde dans les répertoires locaux sur les hôtes.
- tous les fichiers des répertoires `nw-backup` et `restore` sur les hôtes.

Hôte	Chemin de sauvegarde	Chemin de restauration
Malware	`/var/lib/rsamlware/nw-backup`	`/var/netwitness/malware_analytics_server/nw-backup/restore`
Event Stream Analysis	`/opt/rsa/database/nw-backup`	`/var/netwitness/database/nw-backup/restore`
Serveur NW	`/var/netwitness/database/nw-backup`	`/var/netwitness/restore`

Hôte	Chemin de sauvegarde	Chemin de restauration
Pour tous les autres hôtes	`/var/netwitness/database/nw-backup`	`/var/netwitness/database/nw-backup/restore`

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 Suite 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`)
- Serveur NW
- Reporting Engine

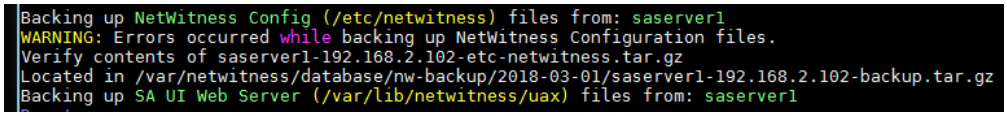
Interface de ligne de commande (CLI)

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

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

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. Reportez-vous à la rubrique « Configuration d'ESA : Modifiez le mot de passe MongoDB pour le compte administrateur » du *Guide de configuration d'Event Stream Analysis. Accédez à la* Table des matières principale *de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.*

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

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

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

Event Stream Analysis

Problème	Le service ESA se bloque après la mise à niveau vers la version 11.1.0.0 à partir d'une installation avec le mode FIPS activé.
Cause	Le service ESA pointe vers un magasin de clés non valide.

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

Service Log Collector (`nwlogcollector`)

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

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

Message d'erreur	`<timestamp> NwLogCollector_PostInstall: Lockbox Status : Not Found`
Cause	Le Lockbox du Log Collector n'a pas été configuré après la mise à jour.
Solution	(Conditionnel) Si vous utilisez le Lockbox de Log Collector, connectez-vous à NetWitness Suite et configurez le Lockbox, comme décrit dans la rubrique « Configurer les paramètres de sécurité Lockbox » du *Guide de configuration de Log Collection*. Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 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 Suite et redéfinissez le mot de passe de la valeur du système stable pour le Lockbox, comme décrit dans la rubrique « Réinitialiser la valeur système stable » de la rubrique « Configurer des paramètres de sécurité Lockbox » du *Guide de configuration de Log Collection*. Accédez à la Table des matières principale de NetWitness Logs & Packets 11.x afin de trouver tous les documents NetWitness Suite 11.x.

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

Serveur NW

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

Problème	Après la mise à niveau, vous remarquez que les logs d'audit ne sont pas transmis à l'installation d'audit global configurée, ou le message suivant s'affiche dans le fichier `sa.log`. `Syslog Configuration migration failed. Restart jetty service to fix this issue`
Cause	La migration de l'installation d'audit global du serveur NW de la version 10.6.5 vers la version 11.1.0.0 a échoué.
Solution	1. Ouvrez une session SSH sur le serveur NW. 2. Exécutez la commande suivante : `orchestration-cli-client --update-admin-node`

Service Reporting Engine

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

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

Annexe B. Arrêt et redémarrage de la capture et de l'agrégation des données

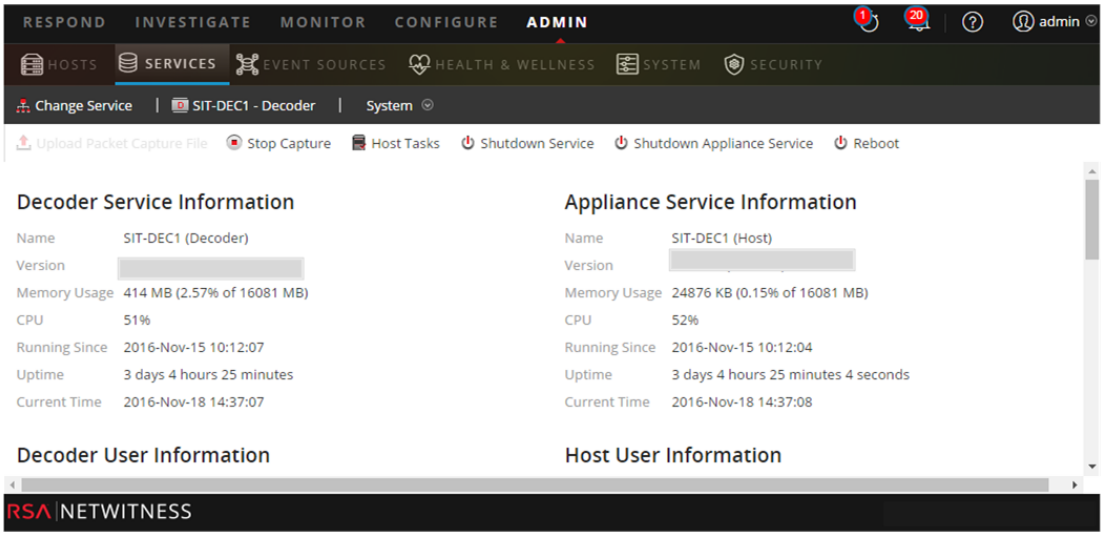
RSA vous recommande d'arrêter la capture et l'agrégation des paquets et des logs avant la mise à niveau d'un hôte Decoder, Concentrator et Broker vers la version 11.1.0.0. Si vous effectuez cette opération, vous devez redémarrer la capture et l'agrégation de paquets et des logs après la mise à jour de ces hôtes.

Arrêter la capture et l'agrégation des données

Arrêter la capture des paquets

Pour arrêter la capture des paquets :

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



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

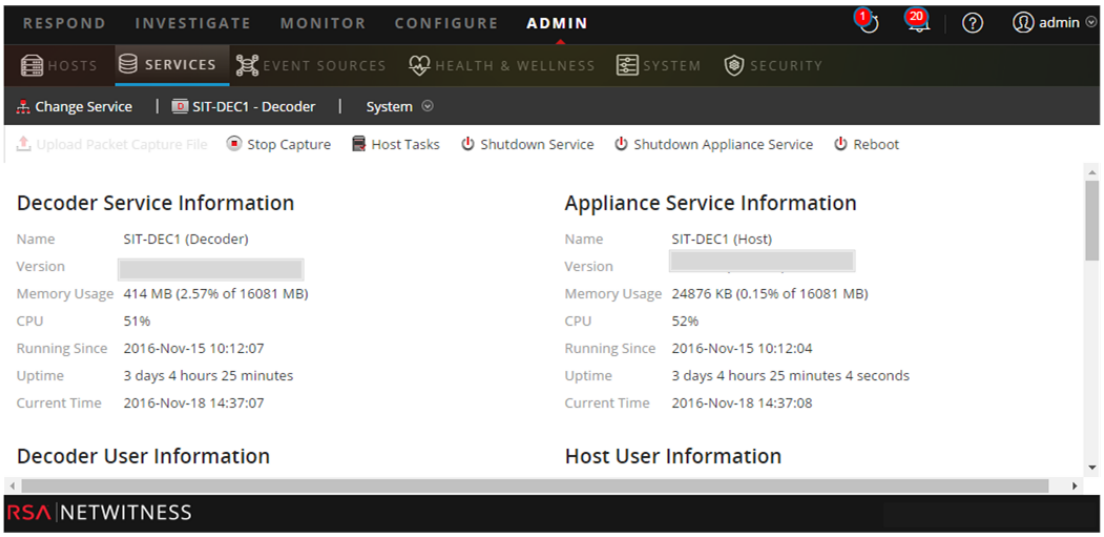
.

Arrêter la capture des logs

Pour arrêter la capture des logs :

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

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



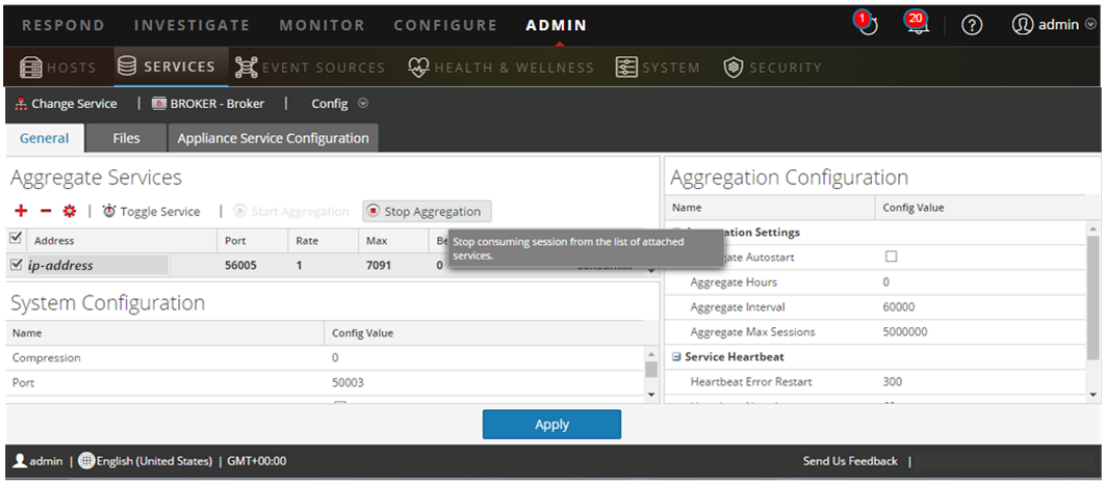
3. Sous  (actions), sélectionnez **Afficher** > **Système**.

4. Dans la barre d'outils, cliquez sur 

.

Arrêter l'agrégation

1. Connectez-vous à NetWitness Suite et accédez à **ADMIN** > **Services**.
2. Sélectionnez le service **Broker**.
3. Sous  (actions), sélectionnez **Afficher** > **Config**.
4. L'onglet **Général** s'affiche.



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

.

Démarrer la capture et l'agrégation des données

Redémarrez la capture/l'agrégation des paquets et des logs après la mise à jour vers la version 11.1.0.0.

Démarrer la capture des paquets

Pour démarrer la capture des paquets :

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

.

Démarrer la capture des logs

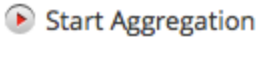
Pour démarrer la capture des logs :

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

.

Démarrer l'agrégation

Pour démarrer l'agrégation :

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

.

Annexe C. Utilisation d'IDRAC

De nombreux clients ont des sites distants avec un accès physique limité et une bande passante limitée depuis le bureau de l'administrateur. Si tel est le cas, vous pouvez utiliser iDRAC avec l'image ISO partagée à partir d'un partage NFS local pour les périphériques mis à niveau ou installés. Cela vous permet également d'utiliser un périphérique NetWitness existant en tant qu'hôte de partage.

Par exemple :

- Vous disposez des services Concentrator et Decoder sur un site à un emplacement géographique à distance.
- La bande passante est relativement faible pour ce site à partir du site de l'administrateur.
- La remise d'une clé USB et le fait qu'une personne la connecte aux boîtiers pendant la mise à jour n'est pas pratique.

Dans ce cas, vous pouvez :

1. Installer le rpm nfs-utils.
2. Configurer le partage NFS.
3. Configurer iDRAC pour se connecter à ce partage.
   Veillez à mettre à jour votre micrologiciel iDRAC Systèmes d'exploitation Windows et Linux pris en charge. Pour ce faire, téléchargez et exécutez les packages de mise à jour Dell pour les systèmes d'exploitation Windows et Linux pris en charge, sur le site Web du Support Dell http://www.support.dell.com. Pour plus d'informations, reportez-vous au Guide d'utilisation du Package de mise à jour Dell disponible sur le site Web de Support Dell http://topics-cdn.dell.com/pdf/dell-update-packages-v17.10.00_User's%20Guide_en-us.pdf.

4. Démarrez le média virtuel contenant le fichier ISO et poursuivez la mise à niveau.

Configurer le serveur NFS - Fichier de configuration du serveur NFS

1. Installez NFS et ses utilitaires communs en utilisant yum.
   ```
   yum install nfs-utils
   ```
2. Configurer le service NFS à exécuter au démarrage.
   ```
   chkconfig nfs on
   ```

3. Configurer le service rpcbind à exécuter au démarrage.
   Ce service est requis par le protocole NFS et doit être en cours d'exécution avant le démarrage de NFS.
   `chkconfig rpcbind on`
4. Démarrez le service rpcbind.
   `service rpcbind start`
5. Démarrez le service NFS.
   `service nfs start`
6. Créez un répertoire pour notre première exportation.
   `mkdir /exports/files`
7. Ouvrez le fichier d'exportation NFS dans un éditeur de texte.
   `vi /etc/exports`
8. Pour exporter le répertoire pour tous les utilisateurs avec accès en lecture seule, ajoutez la ligne suivante.
   `/exports/files *(ro)`
9. Enregistrez vos modifications et quittez l'éditeur.
   `:wq!`
10. Exportez le répertoire indiqué ci-dessus.
    `exportfs -a`
11. Désactivez les règles de pare-feu pendant l'exécution de mises à niveau.
    `service iptables stop`
12. Copiez le kit d'installation contenant le fichier ISO dans le répertoire `/exports/files` .

Démarrer iDRAC en mode de configuration NFS

Remarque : Vous devez vérifier que le micrologiciel idrac correspond au moins à la version 1.57.57 pour la gamme 4 (R620).

1. Connectez-vous à l'interface iDRAC.
2. Rattachez les médias via le partage de fichiers à distance.
   `<server ip>:/export/files/11.1.0.0.iso`
   Par exemple : `10.10.10.10:/exports/files/rsa-11.1.0.0.1948.el7-usb.iso`
3. Cliquez sur **Connecter**.
4. Lancez la **console**.

5. À partir du menu de **démarrage suivant**, sélectionnez **un DVD/CD virtuel**.
6. Réinitialisez le périphérique.

Annexe D. Créer le référentiel externe

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

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

1. Connectez-vous à l'hôte du serveur Web.
2. Créez le répertoire destiné à héberger le référentiel NW (`netwitness-11.1.0.0.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 11.1.0.0 sous `/var/netwitness/<your-zip-file-repo>`.
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0`
4. Créez les répertoires `OS` et `RSA` sous `/var/netwitness/<your-zip-file-repo>/11.1.0.0`.
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS`
   `mkdir -p /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA`
5. Décompressez le fichier `netwitness-11.1.0.0.zip` dans le répertoire `/var/netwitness/<your-zip-file-repo>/11.1.0.0`.
   `unzip netwitness-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0`
   La décompression de `netwitness-11.1.0.0.zip` résulte en deux fichiers zip (`OS-11.1.0.0.zip` et `RSA-11.1.0.0.zip`) et d'autres fichiers.
6. Décompressez le fichier :
   a. `OS-11.1.0.0.zip` dans le répertoire `/var/netwitness/<your-zip-file-repo>/11.1.0.0/OS`.
      `unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/OS-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/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.

../		
repodata/	03-Oct-2017 14:07	-
GConf2-3.2.6-8.el7.x86_64.rpm	03-Oct-2017 14:04	1047864
GeoIP-1.5.0-11.el7.x86_64.rpm	03-Oct-2017 14:04	1101952
Lib_Utils-1.00-09.noarch.rpm	03-Oct-2017 14:05	1589317
OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05	513864
OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:05	15440
PyYAML-3.11-1.el7.x86_64.rpm	03-Oct-2017 14:05	164056
SDL-1.2.15-14.el7.x86_64.rpm	03-Oct-2017 14:05	209280
acl-2.2.51-12.el7.x86_64.rpm	03-Oct-2017 14:04	82864
alsa-lib-1.1.1-1.el7.x86_64.rpm	03-Oct-2017 14:04	425260
at-3.1.13-22.el7.x86_64.rpm	03-Oct-2017 14:04	51824
atk-2.14.0-1.el7.x86_64.rpm	03-Oct-2017 14:04	257180
attr-2.4.46-12.el7.x86_64.rpm	03-Oct-2017 14:04	67184
audit-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	238516
audit-libs-2.6.5-3.el7_3.1.i686.rpm	03-Oct-2017 14:04	86772
audit-libs-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	87004
audit-libs-python-2.6.5-3.el7_3.1.x86_64.rpm	03-Oct-2017 14:04	72028
authconfig-6.2.8-14.el7.x86_64.rpm	03-Oct-2017 14:04	429080
autogen-libopts-5.18-5.el7.x86_64.rpm	03-Oct-2017 14:04	67624
avahi-libs-0.6.31-17.el7.x86_64.rpm	03-Oct-2017 14:04	62640

b. `RSA-11.1.0.0.zip` dans le répertoire `/var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA`.

```
unzip /var/netwitness/<your-zip-file-repo>/11.1.0.0/RSA-11.1.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.1.0.0/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.

../		
repodata/	03-Oct-2017 18:59	-
HostAgent-Linux-64-x86-en_US-1.2.25.1.0163-1.x8..>	03-Oct-2017 14:07	4836279
MegaCli-8.02.21-1.noarch.rpm	03-Oct-2017 14:07	1272689
OpenIPMI-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 14:07	176988
bind-utils-9.9.4-50.el7_3.1.x86_64.rpm	03-Oct-2017 14:07	207220
bzip2-1.0.6-13.el7.x86_64.rpm	03-Oct-2017 14:07	53120
cifs-utils-6.2-9.el7.x86_64.rpm	03-Oct-2017 14:07	86136
device-mapper-multipath-0.4.9-99.el7_3.3.x86_64..>	03-Oct-2017 14:07	132568
erlang-19.3-1.el7.centos.x86_64.rpm	03-Oct-2017 14:07	17252
fneserver-4.6.0-2.el7.x86_64.rpm	03-Oct-2017 18:17	1341432
htop-2.0.2-1.el7.x86_64.rpm	03-Oct-2017 14:07	100104
ipmitool-1.8.15-7.el7.x86_64.rpm	03-Oct-2017 14:07	410800
iptables-services-1.4.21-17.el7.x86_64.rpm	03-Oct-2017 14:07	51376
ixgbe-zc-4.1.5.6-dkms.noarch.rpm	03-Oct-2017 18:24	357084
java-1.8.0-openjdk-1.8.0.141-1.b16.el7_3.x86_64..>	03-Oct-2017 14:07	239660
jettyuax-9.0.7-1709271718.5.60d981d.el7.noarch.rpm	03-Oct-2017 18:18	6235736
lm_sensors-3.4.0-4.20160601gitf9185e5.el7.x86_6..>	03-Oct-2017 14:07	143496
lsof-4.87-4.el7.x86_64.rpm	03-Oct-2017 14:07	338448
mlocate-0.26-6.el7.x86_64.rpm	03-Oct-2017 14:07	115272
mongodb-org-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	5976
mongodb-org-mongos-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	12181727
mongodb-org-server-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	20608878
mongodb-org-shell-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	11768461
mongodb-org-tools-3.4.7-1.el7.x86_64.rpm	03-Oct-2017 14:07	51150888
net-snmp-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07	328576
net-snmp-utils-5.7.2-24.el7_3.2.x86_64.rpm	03-Oct-2017 14:07	201640
nfs-utils-1.3.0-0.33.el7_3.x86_64.rpm	03-Oct-2017 14:07	385888
nginx-1.12.1-1.el7.ngx.x86_64.rpm	03-Oct-2017 14:07	733472
nmap-ncat-6.40-7.el7.x86_64.rpm	03-Oct-2017 14:07	205460
ntp-4.2.6p5-25.el7.centos.2.x86_64.rpm	03-Oct-2017 14:07	560368
nwipdbextractor-11.0.0.0-6953.1.dccfe43.el7.x86..>	03-Oct-2017 18:18	31228560
nwwarehouseconnector-11.0.0.0-1950.5.a6e8b3c.el..>	03-Oct-2017 18:18	10593736
pfring-dkms-6.5.0-6.noarch.rpm	03-Oct-2017 18:24	75432
postgresql-9.2.23-1.el7_4.x86_64.rpm	03-Oct-2017 14:07	3173368

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 11.1.0.0 (nwsetup-tui).`nwsetup-tui`

Historique des révisions

Révision	Date	Description	Auteur
1.0	08 mars 2018	Version pour les opérations (RTO)	IDD