RSA NETWITNESS® SUITE

Guide de mise à niveau Azure

pour la version 11.0.0.0

Informations de contact

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

Marques commerciales

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

Contrat de licence

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

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

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

Licences tierces

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

Remarque sur les technologies de chiffrement

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

Distribution

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

mars 2018

Sommaire

Introduction

Les instructions de ce guide s'appliquent à la mise à niveau d'Azure pour RSA NetWitness Suite 10.6.4.x vers 11.0.0.0 exclusivement. 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 10.6.4.x vers la version 11.0. Accédez à la Table des matières principale pour la version 11.0 trouver des documents NetWitness Suite 11.0. Ce document suppose que les appliances se trouvent dans le Cloud Azure.

NetWitness Suite 11.0 est une version majeure qui a une incidence sur tous les produits de la gamme NetWitness Suite. Les composants de la gamme sont : Serveur NetWitness (serveur NW), Archiver, Broker, Concentrator, Context Hub, Decoder, Analytique comportementale de l'entité, Event Stream Analysis, Investigate, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Response et Workbench.

Mise à niveau de CentOS6 vers CentOS7

NetWitness Suite 11.0 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 11.0 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 11.0 de RSA NetWitness® Suite

Le chemin de mise à niveau pris en charge pour RSA NetWitness® Suite 11.0 est Security Analytics 10.6.4.x. Si vous exécutez une version de NetWitness Suite antérieure à la version 10.6.4.x, vous devez effectuer une mise à jour vers la version 10.6.4.x avant de passer à la mise à jour 11.0. Consultez le *Guide mise à jour de RSA Security Analytics 10.6.4* sur RSA Link (https://community.rsa.com/docs/DOC-79055).

Attention : Un problème connu se produit pour les utilisateurs d'Active Directory configurés dans la version 10.6.4.x. Vous avez deux possibilités pour résoudre ce problème :
• Appliquer le correctif 10.6.4.2 avant de sauvegarder vos données pour la mise à niveau vers la version 11.0.
• Si vous n'avez pas réussi à appliquer le correctif 10.6.4.2, vous pouvez appliquer le correctif 11.0.0.1 immédiatement après la mise à niveau vers la version 11.0.

Le matériel, les déploiements, les services et les fonctions non pris en charge dans la version 11.0

RSA ne prend pas en charge la mise à niveau vers la version 11.0. 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 11.0.)
- Le service autonome Warehouse Connector (la mise à niveau d'un Warehouse Connector co-localisé est prise en charge dans la version 11.0.)
- La politique personnalisée d'intégrité dans la version 10.6.x pour le Service Context Hub . Après la mise à niveau vers NetWitness 11.0, 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 11.0.
- 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)

- Malware Analysis
- Packet Decoder

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

Dans RSA NetWitness® Suite version 11.0, RSA a modifié la façon dont les règles de corrélation ESA stockent et transmettent les alertes générées par le système. Dans la version 11.0, ESA envoie toutes les alertes à un système d'alerte central. Le stockage local mongo dans ESA version 10.6.4.x a été retiré.

Attention : Si vous n'utilisez pas la gestion des incidents dans la version 10.6.4.x, réfléchissez bien avant d'effectuer la mise à niveau vers la version 11.0.

Les directives suivantes doivent vous aider à déterminer si vous devez ou non mettre à niveau vos hôtes ESA vers la version 11.0.

Dans votre déploiement 10.6.4.x, si vous avez :

- Un hôte ESA avec ou sans gestion des incidents configurée, optez pour la mise à niveau vers la version 11.0.
- 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 10.6.4.x, vous pouvez vous mettre à niveau vers la version 11.0.
- 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 11.0.

Remarque : Si vous n'utilisez pas la gestion des incidents dans la version 10.6.4.x, vous ne pouvez pas afficher les alertes ESA de la version 10.6.4.x dans le composant Respond de la version 11.0 sans exécuter un script de migration. Utiliser le script de migration d'alerte ESA pour migrer ces alertes à l'emplacement qui permettra à Respond de les afficher dans la version 11.0. Reportez-vous à l'article *Instructions de migration d'alerte ESA de la version 10.6.4.x à la version 11.0* 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.

Modifications d'attribut d'utilisateur et de rôle affectant Enquête

Les modifications suivantes ont une incidence sur la manière dont NetWitness Suite version 11.0 gère les attributs d'utilisateur et de rôle dans le composant Enquête.

- Les attributs d'utilisateur
  . Lorsque vous effectuez une mise à niveau vers la version 11.0, les attributs d'utilisateur (préfixe de requête, délai d'expiration de session et seuil de requête) disponibles dans SA version 10.6.4.x n'existent plus. Les mêmes attributs sont désormais disponibles au niveau du rôle.
  Pour contourner ce problème, si vous utilisiez les attributs d'utilisateur pour restreindre l'accès des utilisateurs, appliquez le correctif RSA NetWitness® Suite de la version 11.0.0.1 immédiatement après la mise à niveau vers la version 11.0.0.0.
- Les attributs d'utilisateur et de rôle (Préfixe de requête) ne sont pas applicables pour examiner l'analyse d'évènement. Les attributs d'utilisateur et de rôle, principalement le préfixe de requête, ne s'appliquent pas à la nouvelle enquête de l'analyse d'événement. N'importe quel utilisateur peut modifier l'URL dans le navigateur pour accéder aux données dont l'accès est normalement restreint, même lorsque le préfixe de requête est appliqué.
  Pour contourner ce problème, appliquez le correctif RSA NetWitness® Suite de la version 11.0.0.1 immédiatement après la mise à niveau vers la version 11.0.0.0.

Attention : Si vous avez configuré les attributs d'utilisateur ou de rôle dans la version 10.6.4.x, y compris le préfixe de requête, appliquez le correctif RSA NetWitness® Suite de la version 11.0.0.1 immédiatement après la mise à niveau vers la version 11.0.0.0. Après avoir appliqué ce correctif, suivez les instructions du correctif pour appliquer les contrôles de sécurité supplémentaires.

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 11.0 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 Broker (si vous ne disposez pas d'un Broker, mettez à niveau vos hôtes Concentrator)
   Le serveur NW 11.0 ne peut pas communiquer avec des services de base de la version

10.6.4.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.

Dans la Phase 2 (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 suivant. 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.

1. Hôtes Concentrator
2. Hôtes Archiver
3. 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.
4. Pour tous les autres hôtes

Reportez-vous à la section « Exécution en mode mixte » sous « Les bases » dans le Guide de mise en route des hôtes et des services de RSA *NetWitness Suite version 11.0* pour :

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

Accédez à la Table des matières principale pour la version 11.0 trouver des documents NetWitness Suite 11.0.

Procédure d'enquête en mode mixte

Le mode mixte est opérationnel lorsque certains services sont mis à niveau vers la version 11.0 et d'autres sont toujours sur la version 10.6.x. Cela se produit lorsque la mise à niveau vers la version 11.0 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 de procédure d'enquête version 11.0 est installé lors de la mise à niveau du serveur SA, mais les hôtes Broker doivent être mis à niveau vers la version 11.0 pour accéder à la vue Analyse d'événements.

Après avoir effectué la mise à niveau de tous les services vers la version 11.0, 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 11.0 et d'autres sont encore sur la version 10.6.x), 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 télécharger, 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 11.0, RBAC fonctionne correctement entre tous les services.

Le tableau suivant identifie ce que vous pouvez voir et télécharger dans Investigate lorsque votre Serveur NetWitness est sur la version 11.0 connecté aux services d'une version inférieure.

Connecter la version du service	Vue concernée	Rôle d'utilisateur	Autorisation d'affichage	Téléchargement réussi	Téléchargement avec des erreurs
Broker 11.0 -> Concentrator 10.x	Vue Événements	Analyste		PCAP	Le fichier d'archive est téléchargé mais ne peut pas être décompressé
	Vue Reconstruction d'événement	Analyste		PCAP	Le fichier d'archive est téléchargé mais ne peut pas être décompressé
	Vue Analyse d'événements	AnalysteLDsLDWCsLWCla vue A'		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	Autorisation d'affichage	Téléchargement réussi	Téléchargement avec des erreurs
	Vue Reconstruction d'événement	Administrateur			Le fichier d'archive est téléchargé mais ne peut pas être décompressé
Broker 11.0 -> Concentrator 11.0	Vue Reconstruction d'événement Vue Reconstruction d'événement	Analyste et responsable de la confidentialité des données	Éléments RBAC autorisés		Le fichier d'archive est téléchargé mais ne peut pas être décompressé la taille des PCAP et des logs téléchargés est de zéro octet

1. Set up NW Server.
2. Set up ESA.
3. Install ESA in NW UI.
4. Set up Brkr/Conc.
5. Install Brkr/Conc in UI.
6. Set up Other hosts.
7. Install other hosts in UI.

Contactez le support client

Reportez-vous à la page Contactez le support client RSA (https://community.rsa.com/docs/DOC-1294) dans RSA Link pour plus d'informations sur la manière d’obtenir de l’aide sur RSA NetWitness Suite version 11.0.

Tâches de préparation de la mise à niveau

Effectuez les tâches suivantes pour préparer la mise à niveau vers la version 11.0 de NetWitness Suite. Ces tâches sont organisées selon les catégories suivantes.

- Global
- Reporting Engine
- Respond et Incident Management

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

Le tableau suivant répertorie les nouveaux ports dans la version 11.0.

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

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 pour la version 11.0 trouver des documents NetWitness Suite 11.0.

Tâche 2 - Enregistrer votre mot de passe `admin user` de la version 10.6.4.x

Enregistrez votre mot de passe `admin user` de la version 10.6.4.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.

Reporting Engine

(Conditionnel) Tâche 4 - 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`

Respond et Incident Management

(Conditionnel) Tâche 5 - Désactiver la rétention des données dans Incident Management

Exécutez la procédure suivante pour désactiver les tâches de rétention des données dans Incident Management dans la version 10.6.4.x

1. Connectez-vous à RSA Security Analytics 10.6.4.x.
2. Accédez à **Incident Management** > **Configurer** > **Planificateur de rétention**.
3. Désactivez la case à cocher **Activer le planificateur de rétention des données**, puis cliquez sur **Appliquer**.

Instructions de sauvegarde

La sauvegarde de vos données de configuration pour tous vos hôtes de la version 10.6.4.x est la première étape de la mise à niveau de la version 10.6.4.x vers la version 11.0.0.0.

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 11.0.0.0, 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'hôtes.

Attention : 1) Ces services ne sont pas pris en charge dans le processus de mise à niveau et de sauvegarde 10.6.4.x.
- IPDB
- Serveurs tout-en-un
- Malware Analysis co-localisé sur le serveur NetWitness
- Warehouse Connector autonome

2) Un problème connu se produit si des utilisateurs d'Active Directory sont configurés dans la version 10.6.4.x. Vous avez deux possibilités pour résoudre ce problème :
• Appliquer le correctif 10.6.4.2 avant de sauvegarder vos données pour la mise à niveau vers la version 11.0.
• Si vous n'avez pas réussi à appliquer le correctif 10.6.4.2, vous pouvez appliquer le correctif 11.0.0.1 immédiatement après la mise à niveau vers la version 11.0.

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

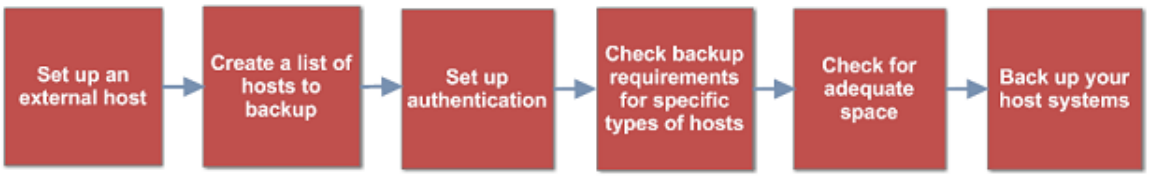
- **Serveur NetWitness** (Malware Analysis, NetWitness Respond, Intégrité et Reporting Engine peuvent être concernés)
- **Archiver**
- **Broker**
- **Event Stream Analysis** (y compris Context Hub et la base de données NetWitness Respond)
- **Concentrator**
- **Log Decoder** (y compris le Log Collector local et Warehouse Connector, si installés)
- **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 11.0.0.0 », 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.

Remarque : Si vous rencontrez des problèmes au cours du processus de sauvegarde ou de mise à niveau et que vous perdez des données, vous pouvez restaurer les données et redémarrer le processus. Pour plus d'informations sur la restauration des données perdues, consultez la section « Restaurer des données après la défaillance du système » du *Guide de maintenance du système*.

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 la 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 via le protocole SSH pour la pile des hôtes NetWitness Suite.

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.

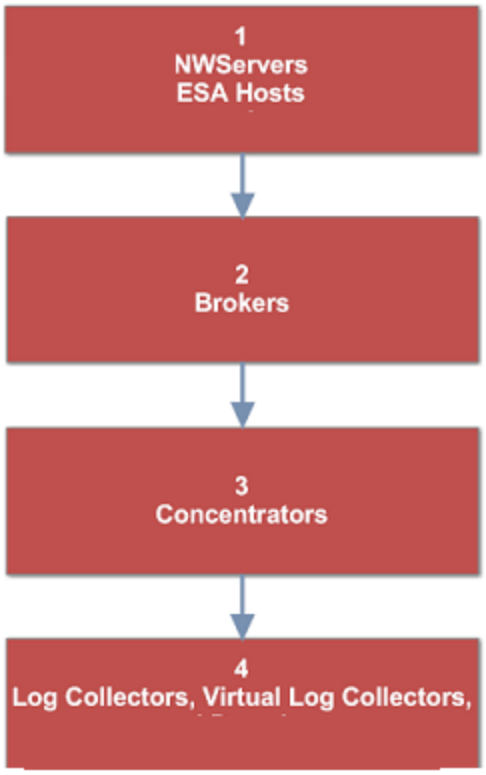
Il existe plusieurs scripts à exécuter lors du processus de sauvegarde. Vous devez télécharger le fichier zip contenant les scripts (`nw-backup-v3.0.zip`) à partir de RSA Link à l'emplacement suivant : https://community.rsa.com/docs/DOC-81514 et le copier sur votre système de sauvegarde CentOS 6. Cliquez sur le lien **Script de sauvegarde de logs et paquets RSA NetWitness 11.0 (nw-sauvegarde v3.0.sh)** et 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 Serveur NetWitness et systèmes hôtes 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.

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-NetWitness-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.

> **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,10.6.4.0
archiver,my-nw-archiver,10.0.0.2,a65c1236-5e46-4117-8529-
8ea837074bd0,10.6.4.0
concentrator,my-nw-concentrator,10.0.0.3,dc620e94-bcf5-4d51-83fe-
c003cdfcd7a6,10.6.4.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.4.0
logdecoder,my-nw-logdecoder,10.0.0.5,c8be5d45-e19e-4a8d-90ce-
1cb2fe60077a,10.6.4.0
vlc,my-nw-vlc,10.0.0.8,3ffefc4e-0b31-4951-bb77-dea5869fa98c,10.6.4.0
broker,my-nw-broker,10.0.0.9,0b65e7ce-61d5-4177-9647-
c56ccfb0f737,10.6.4.0
```

Voici un exemple de fichier `all-systems` basé sur le fichier `all-systems-master-copy` pouvant être utilisé dans la première session de sauvegarde :

```
saserver,my-nw-server,10.0.0.1,af922b9f-cd61-49cd-afdc-
a48e558cec3e,10.6.4.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.4.0
```

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), veillez à supprimer les entrées existantes du fichier afin que le fichier contienne uniquement les hôtes qui sont actuellement en cours de

sauvegarde.
Pour plus d'informations, reportez-vous à la rubrique Tâches postérieures à la mise à niveau.

- 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 NetWitness Suite. 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 NetWitness Suite lorsque vous ajoutez des hôtes et des services à NetWitness Suite, 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 Serveur NetWitness 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 NetWitness. (Ni les Collectors Windows d'ancienne génération, ni les Azure Cloud Collectors 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 NetWitness, 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 11.0.0.0, 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 Serveur NetWitness 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 Concentrator ou Broker : Arrêter la capture et l'agrégation des données

Outre les tâches décrites dans Pour tous les types d'hôtes, pour les hôtes 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. Arrêt et redémarrage de la capture et de 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 11.0.0.0.
   - 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 le Dépannage, reportez-vous à la rubrique 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 10.6.4.x, sur l'hôte Serveur NetWitness, vous devez obtenir la liste de tous les mots de passe et les noms d'utilisateur RabbitMQ afin de pouvoir restaurer les comptes d'utilisateur RabbitMQ une fois la mise à niveau vers la version 11.0.0.0 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 10.6.4.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 10.6.4.x, il est sauvegardé et restauré.

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

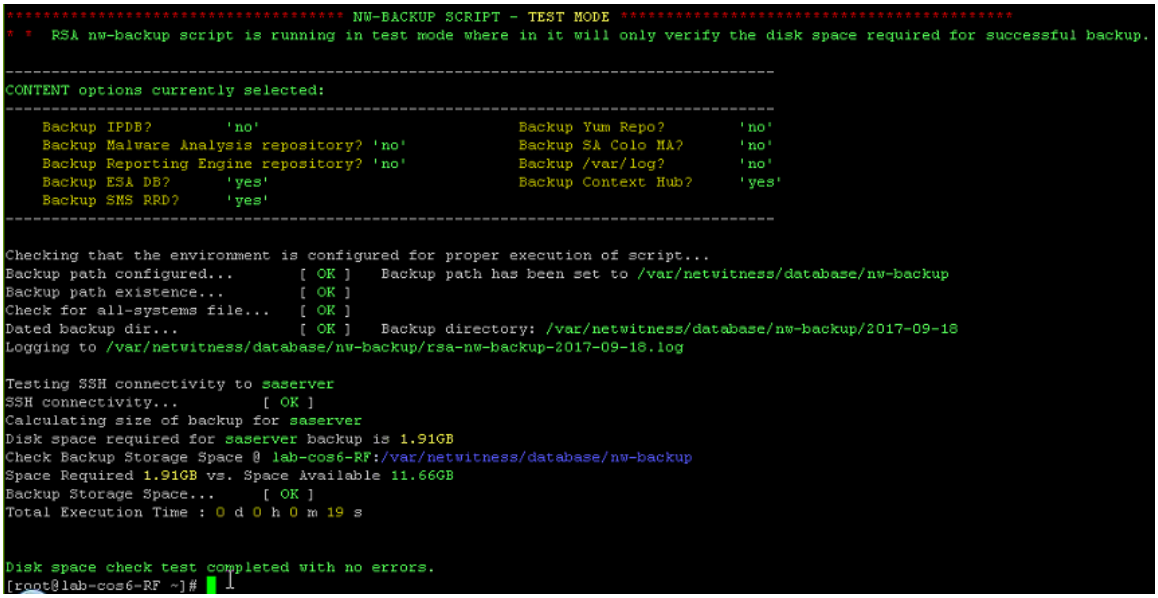
Vous pouvez exécuter le script de test de sauvegarde pour vérifier l'espace disque requis pour la sauvegarde à l'aide de l'option `-t` décrite dans Tester des options. Exécutez le script sans réellement sauvegarder les fichiers ou arrêter les services. RSA vous conseille d'effectuer cette étape pour 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 hôte

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 11.0.0.0.

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 -u -l -x -e <external-mnt> -b <backup file path>
```

Options générales

`-u : This option is required for upgrading to 11.0. Enables the upgrade flag to run backup for upgrading to 11.0. 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 11.0, 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).

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 11.0. 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:
10.6.3.x and 10.6.4.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.
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 <additional options as needed>`

   Remarque : Vous devez utiliser l'option `-u` pour que vos fichiers soient restaurés correctement pendant la mise à niveau vers la version 11.0.0.0.

   Le texte « `Backup completed with no errors` » s'affiche, signale 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 Serveur NetWitnesss :

   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 11.0.0.0 du Serveur NetWitness (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 11.0.0.0. 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 Serveur NetWitness 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 pour le chemin de sauvegarde de l'hôte Serveur NetWitness.

- <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 principal

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 11.0.0.0, 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 :
- HôtesServeur NetWitness :`/var/netwitness/database/nw-backup`
- Hôtes ESA :`/opt/rsa/database/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 10.6.4.x vers la version 11.0

Ces instructions vous expliquent comment mettre à niveau des machines virtuelles NetWitness Azure 10.6.4.x vers 11.0.0.0 sur Azure Cloud Platform.

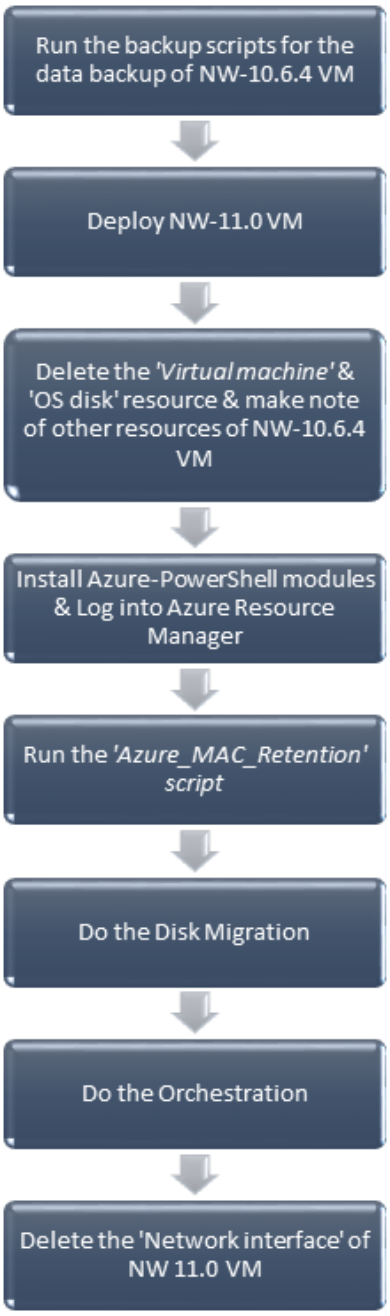
Conditions préalables :

- Téléchargez et installez la dernière version d'Azure PowerShell sur https://github.com/Azure/azure-powershell/releases sur une machine Windows.
- Télécharger cette même dernière version des modules Azure dans le compte d'automatisation. [https://docs.microsoft.com/fr-fr/azure/automation/automation-update-azure-modules]

Remarque : Azure PowerShell 4.4.1 a été utilisé pour la qualification.

Remarque : les deux versions des machines virtuelles doivent se trouver sur le même réseau virtuel et dans le même groupe de ressources pour la migration.

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 des hôtes physiques et virtuels, reportez-vous au document « Instructions de mise à niveau des hôtes physiques *RSA NetWitness® Suite 11.0* » pour consulter les étapes de mise à niveau des hôtes physiques. Accédez à la Table des matières principale pour la version 11.0 trouver des documents NetWitness Suite 11.0.



Réalisez les tâches suivantes pour migrer vos disques durs de déploiement de machines virtuelles (VM) de la version 10.6.4.x vers la version 11.0 :

Tâche 1 - Déployer la machine virtuelle NW 11.0

Tâche 2 - Supprimer la ressource de machine virtuelle et de disque du système d'exploitation de la machine virtuelle NW 10.6.4

Tâche 3 - Installer les modules Azure PowerShell sur un ordinateur Windows local

Tâche 4 - Rétention d'IP : exécuter le script PowerShell

Tâche 5 - Migrer le disque

Tâche 6 - Restaurer les données

Tâche 1 - Déployer la machine virtuelle NW 11.0

1. Déployez les machines virtuelles NW 11.0. Consultez le guide de déploiement Azure pour la version 11.0.0.0.
2. Mettez HORS tension les machines virtuelles 10.6.4.x et 11.0.
3. Dans le Portail Azure, accédez aux machines virtuelles.
4. Cliquez sur <Nom_de_la_VM>.
5. Cliquez sur Présentation et puis cliquez sur Arrêter.

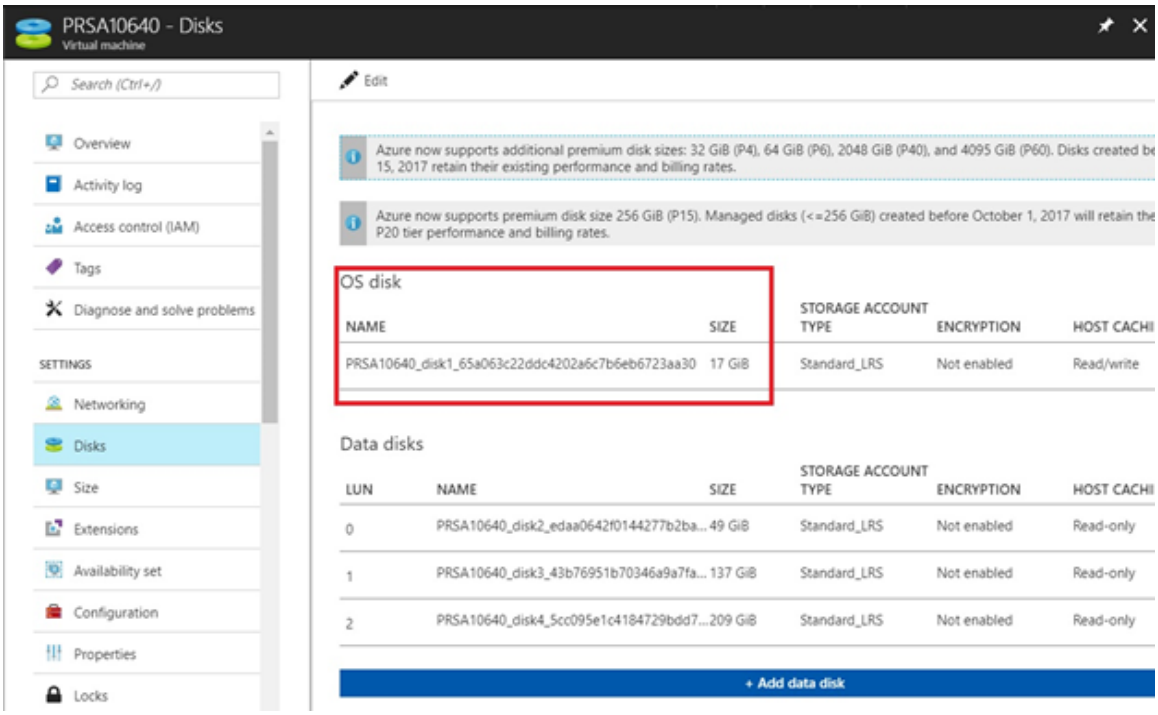
Tâche 2 - Supprimer la ressource de machine virtuelle et de disque du système d'exploitation de la machine virtuelle NW 10.6.4

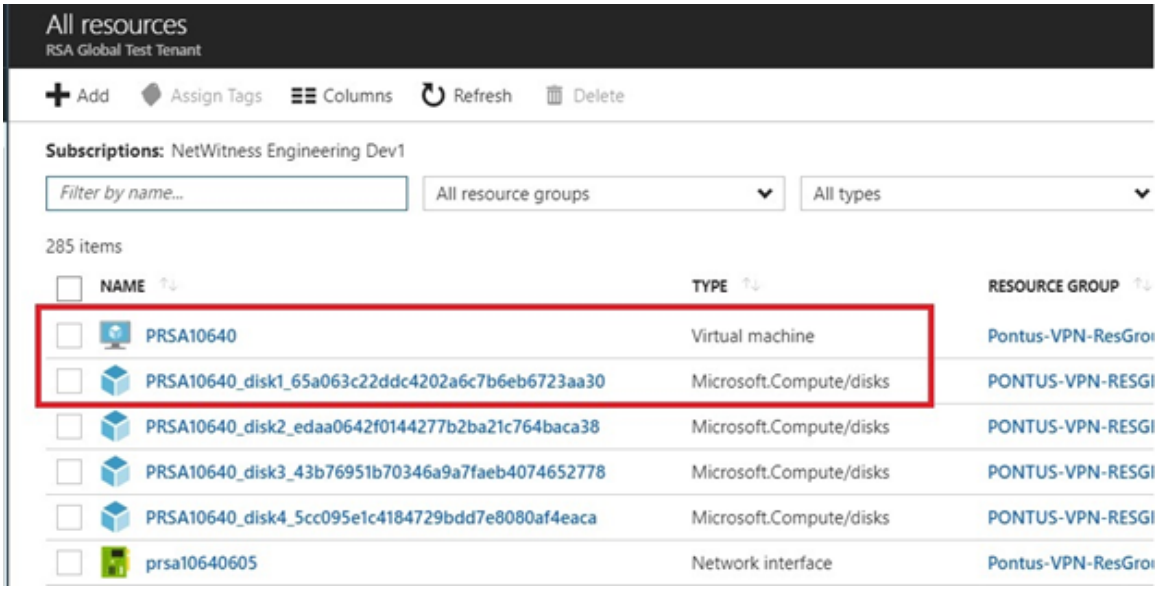
Prenez note de toutes les autres ressources telles que les disques de données et l'interface réseau.

1. Supprimez la ressource « machine virtuelle » et le « disque du système d'exploitation » (généralement disk1 de la machine virtuelle) de la machine virtuelle NW 10.6.4 et prenez note des disques de données et de l'interface réseau.

Remarque : supprimez uniquement ces 2 ressources et conservez toutes les autres ressources des machines virtuelles NW 10.6.4 telles que « Interface réseau », « Groupe de sécurité réseau » et « Disques de données ») et prenez note de ces interfaces réseau et disques de données.

2. Dans le Portail Azure, accédez à toutes les ressources. Sélectionnez le Nom_de_la_VM_NW_10.6.4.
3. Cliquez sur Supprimer.


PRSA10640 - Disks
Virtual machine
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
SETTINGS
Networking
Disks
Size
Extensions
Availability set
Configuration
Properties
Locks
Edit
Azure now supports additional premium disk sizes: 32 GiB (P4), 64 GiB (P6), 2048 GiB (P40), and 4095 GiB (P60). Disks created be
15, 2017 retain their existing performance and billing rates.
Azure now supports premium disk size 256 GiB (P15). Managed disks (<=256 GiB) created before October 1, 2017 will retain the
P20 tier performance and billing rates.
OS disk
NAME
SIZE
STORAGE ACCOUNT TYPE
ENCRYPTION
HOST CACHI
PRSA10640_disk1_65a063c22ddc4202a6c7b6eb6723aa30
17 GiB
Standard_LRS
Not enabled
Read/write
Data disks
LUN
NAME
SIZE
STORAGE ACCOUNT TYPE
ENCRYPTION
HOST CACHI
0
PRSA10640_disk2_edaa0642f0144277b2ba...
49 GiB
Standard_LRS
Not enabled
Read-only
1
PRSA10640_disk3_43b76951b70346a9a7fa...
137 GiB
Standard_LRS
Not enabled
Read-only
2
PRSA10640_disk4_5cc095e1c4184729bdd7...
209 GiB
Standard_LRS
Not enabled
Read-only
+ Add data disk


All resources
RSA Global Test Tenant
Add
Assign Tags
Columns
Refresh
Delete
Subscriptions: NetWitness Engineering Dev1
Filter by name...
All resource groups
All types
285 items
NAME
TYPE
RESOURCE GROUP
PRSA10640
Virtual machine
PRSA10640_disk1_65a063c22ddc4202a6c7b6eb6723aa30
Microsoft.Compute/disks
PONTUS-VPN-RESGI
PRSA10640_disk2_edaa0642f0144277b2ba21c764baca38
Microsoft.Compute/disks
PONTUS-VPN-RESGI
PRSA10640_disk3_43b76951b70346a9a7faeb4074652778
Microsoft.Compute/disks
PONTUS-VPN-RESGI
PRSA10640_disk4_5cc095e1c4184729bdd7e8080af4eaca
Microsoft.Compute/disks
PONTUS-VPN-RESGI
prsa10640605
Network interface

Tâche 3 - Installer les modules Azure PowerShell sur un ordinateur Windows local

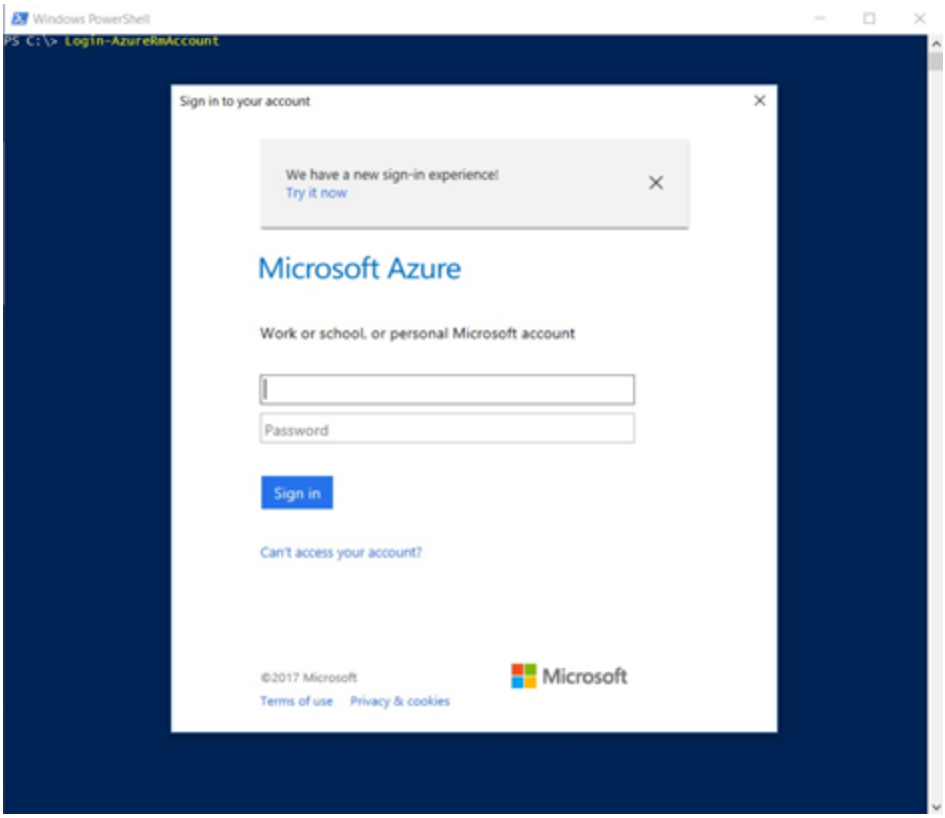
Installez les modules Azure PowerShell sur une machine Windows locale et connectez-vous à Azure Resource Manager.

Accédez à Azure PowerShell sur la machine Windows où vous avez installé les modules Azure PowerShell et connectez-vous à Azure Resource Manager à l'aide de la commande ci-dessous.

Remarque : assurez-vous de suivre les étapes indiquées dans la section Conditions préalables ci-dessus avant d'exécuter cette commande.

```
Login-AzureRmAccount
```

Connectez-vous à l'aide des informations d'identification Azure dans la fenêtre qui s'affiche.



Tâche 4 - Rétention d'IP : exécuter le script PowerShell

Exécutez le script PowerShell pour la rétention MAC pour tous les composants NW. Adresse MAC et rétention des IP :

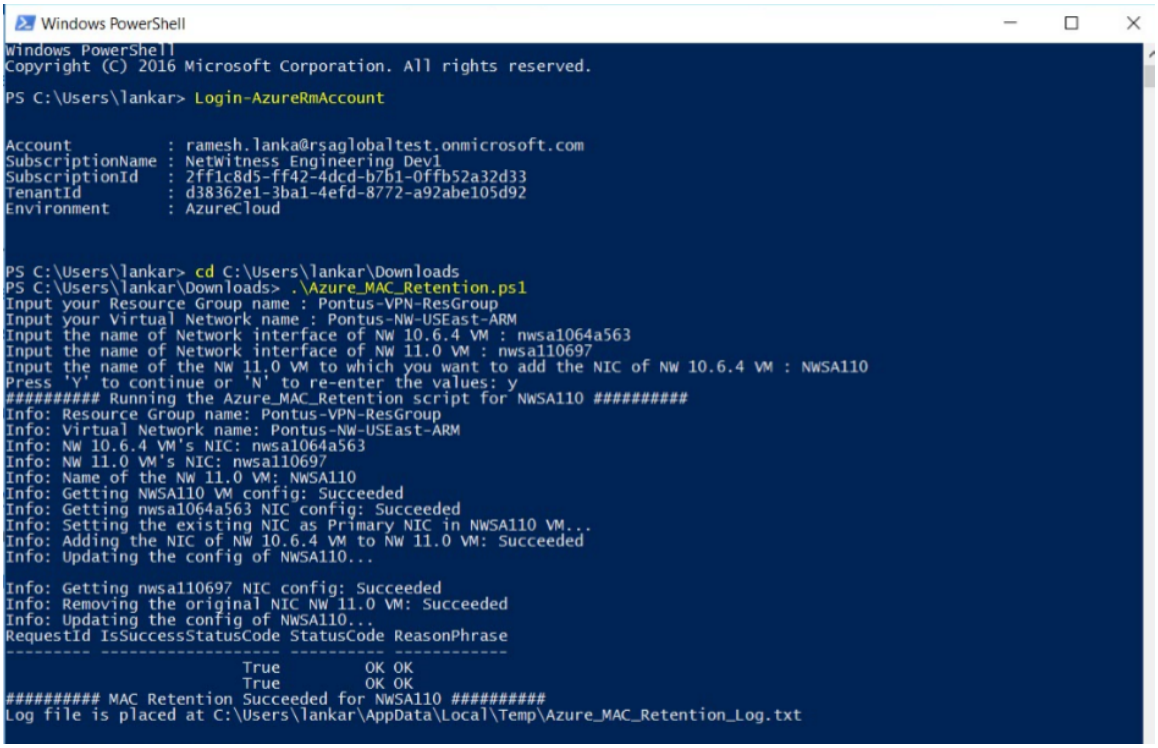
Les adresses MAC et IP sont liées à la ressource de l'interface réseau d'une machine virtuelle.

Le portail Azure ne vous permet pas de :

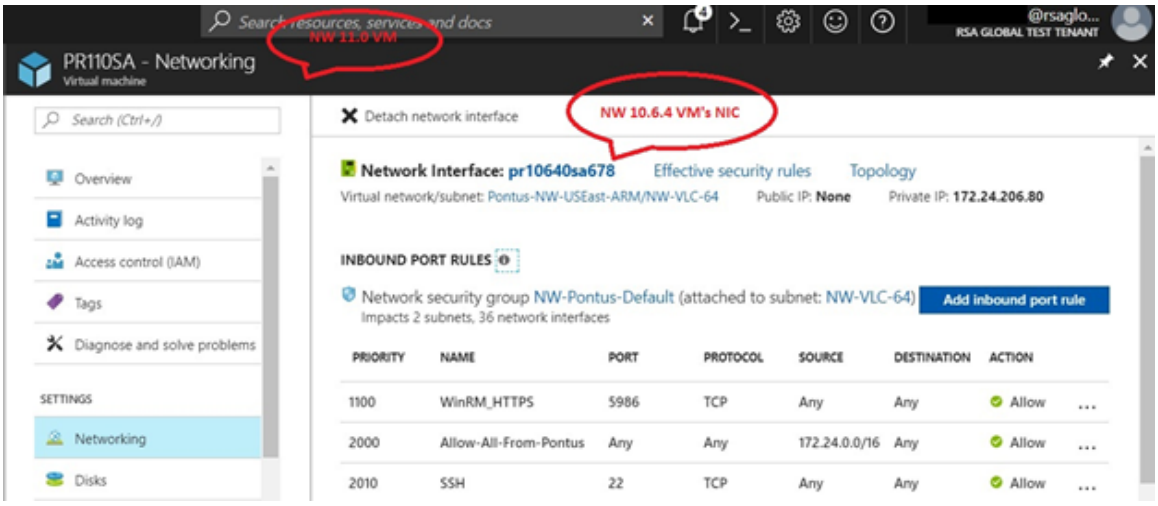
- Spécifier une interface réseau existante à ajouter lors de la création de la machine virtuelle.
- Créer une machine virtuelle avec plusieurs interfaces réseau.
- Spécifier un nom pour l'interface réseau (le Portail crée l'interface réseau avec un nom par défaut).

Cela est possible à l'aide d'Azure PowerShell. [https://docs.microsoft.com/fr-fr/azure/virtual-network/virtual-network-network-interface-vm]

Cliquez ici pour télécharger et exécuter le script en fournissant les paramètres requis sur la machine Windows installée avec Azure PowerShell pour conserver l'interface réseau à partir de la machine virtuelle NW 10.6.4 vers la machine virtuelle 11.0.



Vous serez en mesure de voir la carte réseau de la machine virtuelle NW 10.6.4 rattachée à la VM 11.0 dans les paramètres de mise en réseau, après l'exécution réussie du script.

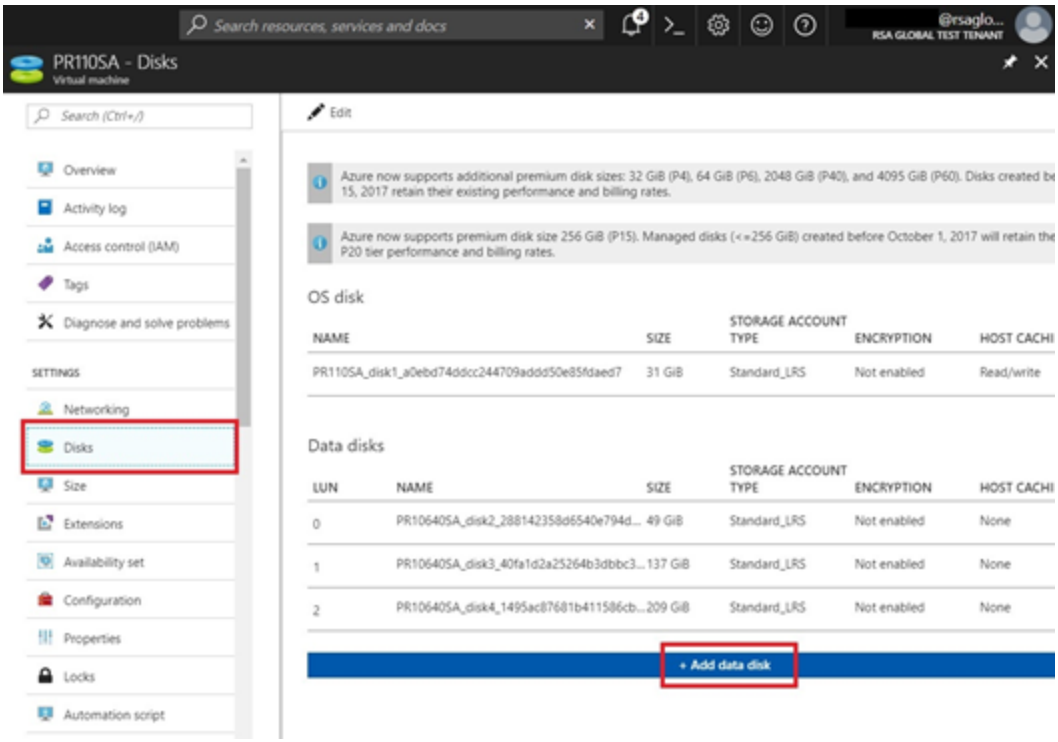


Tâche 5 - Migrer le disque

Ajoutez tous les disques (à l'exception du Disque du système d'exploitation) de la machine virtuelle NW 10.6.4 vers la machine virtuelle NW 11.0 correspondante sous les paramètres des Disques.

Dans le Portail Azure, accédez aux machines virtuelles et à Nom_de_la_VM_11.0. Cliquez sur **Disques** avec le bouton droit de la souris, puis cliquez sur **Ajouter un disque de données**. Sélectionnez tous les disques de la machine virtuelle NW 10.6.4 correspondante dont vous avez pris note précédemment dans la liste déroulante qui s'affiche.

Cliquez sur **Enregistrer**.



Mettez sous tension la machine virtuelle NW 11.0 et connectez-vous avec les informations d'identification fournies lors de son déploiement, puis définissez le mot de passe root en tant que netwitness.

Tâche 6 - Restaurer les données

Copiez les données de la machine virtuelle NW 10.6.4 sauvegardée (nw-backup) vers la machine virtuelle NW 11.0.

Remarque : restaurez d'abord les données du serveur SA, suivi par les autres composants.

Pour SA, LD/LC, Virtual Log Collector, Concentrator, Archiver, Broker :

1. Créez un répertoire sous `/tmp/`, intitulé `nwhome`.
2. Montez `VolGroup00-nwhome` sur `/tmp/nwhome/`.

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

3. Copiez le contenu du répertoire `/tmp/nwhome/` dans `/var/netwitness/`.

```
cp -R /tmp/nwhome/* /var/netwitness/
```

4. Démontez `VolGroup00-nwhome` à partir de `/tmp/nwhome/`.

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

Pour ESA :

1. Créez un répertoire sous `/tmp/` intitulé apps.
2. Montez `VolGroup01-apps` temporairement sur `/tmp/apps/`.

```
mount /dev/mapper/VolGroup01-apps /tmp/apps/
```

3. Copiez le répertoire `nw-backup` à partir d'ici sur `/var/netwitness`.

```
cp /tmp/apps/database/nw-backup /var/netwitness
```

4. Démontez `VolGroup01-apps` à partir de `/tmp/apps/`.

```
umount /dev/mapper/VolGroup01-apps /tmp/apps/
```

Effectuez le montage du disque en exécutant les commandes ci-dessous :

Pour le serveur NW :

```
mount /dev/mapper/VolGroup01-ipdbext /var/netwitness/ipdbextractor/
mount /dev/mapper/VolGroup02-redb /var/netwitness/database/
```

Ajoutez les entrées ci-dessous pour ces montages dans `/etc/fstab` :

```
/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 LogDecoder/LogCollector :

```
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
```

Ajoutez les entrées ci-dessous pour ces montages dans `/etc/fstab` :

```
/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 LogCollector virtuel :

```
mount /dev/mapper/VolGroup01-logcoll /var/netwitness/logcollector
```

Ajoutez l'entrée ci-dessous pour ces montages dans `/etc/fstab` :

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

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
```

Ajoutez les entrées ci-dessous pour ces montages dans `/etc/fstab` :

```
/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 :

```
mount /dev/mapper/VolGroup01-archiver /var/netwitness/archiver
```

```
mount /dev/mapper/VolGroup02-workbench /var/netwitness/workbench
```

Ajoutez les entrées ci-dessous pour ces montages dans `/etc/fstab` :

```
/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 :

```
mount /dev/mapper/VolGroup01-broker /var/netwitness/broker
```

Ajoutez l'entrée ci-dessous pour ces montages dans `/etc/fstab` :

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

Tâche 7 - Supprimer toutes les ressources Interface réseau du déploiement NW 11.0

1. Dans le Portail Azure, accédez à Toutes les ressources.
2. Cliquez sur <Nom_de_l'interface_réseau_NW_11.0> et sélectionnez Supprimer.

Installation des hôtes virtuels dans la version 11.0

L'installation de la pile virtuelle 11.0 comprend deux phases à effectuer dans l'ordre indiqué.

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

  Remarque : Pour Event Stream Analysis, si des modules C2 sont activés dans la version 10.6.4.x, ces modules entreront dans une phase de préparation après la mise à niveau du service Event Stream Analysis vers la version 11.0 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 et les hôtes Broker ou Concentrator

Tâche 1 : Installer Serveur NetWitness 11.0

Suivez les instructions indiquées dans Installer un hôte de serveur NW 11.0.

Tâche 2 : Installer ESA 11.0

Attention : Si des modules C2 sont activés dans la version 10.6.4.x, ces modules entreront dans une phase de préparation après la mise à niveau du service Event Stream Analysis vers la version 11.0 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 11.0 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 : Configurer Broker ou Concentrator 11.0

Suivez les instructions indiquées dans Installer un hôte de serveur autre que NW 11.0.

Remarque : Si vous ne disposez pas d'un service Broker, mettez à niveau vos hôtes Concentrator. Le serveur NW 11.0 ne peut pas communiquer avec la version 10.6.4.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 Concentrator

1. Arrêtez la capture et l'agrégation des données.
2. Suivez les étapes indiquées dans Installer un hôte de serveur version 11.0 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) : Exécutez prepare-for-migrate.sh.
2. Arrêtez la capture des données sur le Log Decoder.
3. Suivez les étapes indiquées dans Installer un hôte de serveur version 11.0 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 11 - Réinitialiser les valeurs système stables pour Log Collector après la mise à niveau 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) : Exécutez prepare-for-migrate.sh.
2. Sauvegardez la version 10.6.4.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>,10.6.4.0`

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 10.6.4.x afin qu'une nouvelle machine virtuelle 11.0 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 11.0.

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 10.6.4.x. Ces informations sont stockées dans le fichier de sauvegarde du VLC 10.6.4.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 11.0 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 11.0

Assurez-vous que vous avez sauvegardé les données 10.6.4.x pour l'hôte de serveur SA. **Vous devez suivre les instructions indiquées dans** Instructions de sauvegarde **pour sauvegarder l'hôte.**

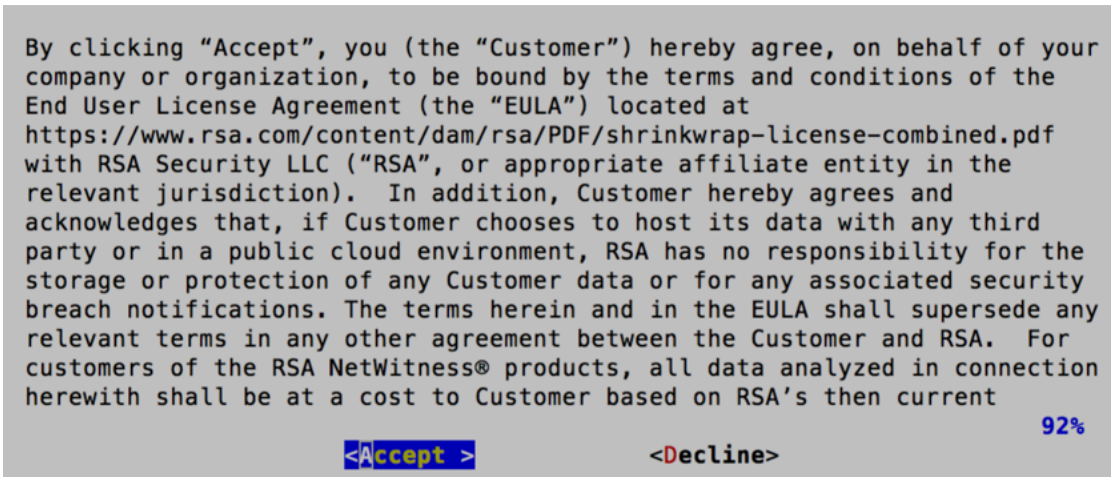
Attention : Exécutez la sauvegarde immédiatement avant la mise à niveau du serveur SA vers la version 11.0 afin que les données soient aussi récentes que possible. Vous devez créer le fichier **all-systems** avant de mettre à niveau le serveur SA, car vous ne pouvez plus le faire une fois que le serveur SA a été mis à niveau vers la version 11.0.

Pour installer la version 11.0 de l'hôte de serveur NW, procédez comme suit.

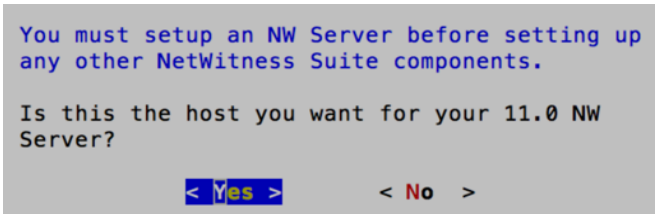
1. Mettez sous tension la machine virtuelle du serveur NW et exécutez la commande `nwsetup-tui`.

   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.

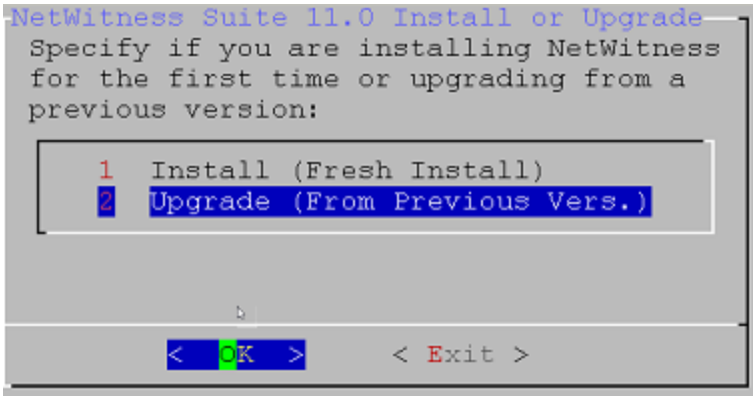


2. Naviguez jusqu'à **Accepter** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**.
   Le message « S'agit-il du serveur NW ? » s'affiche.



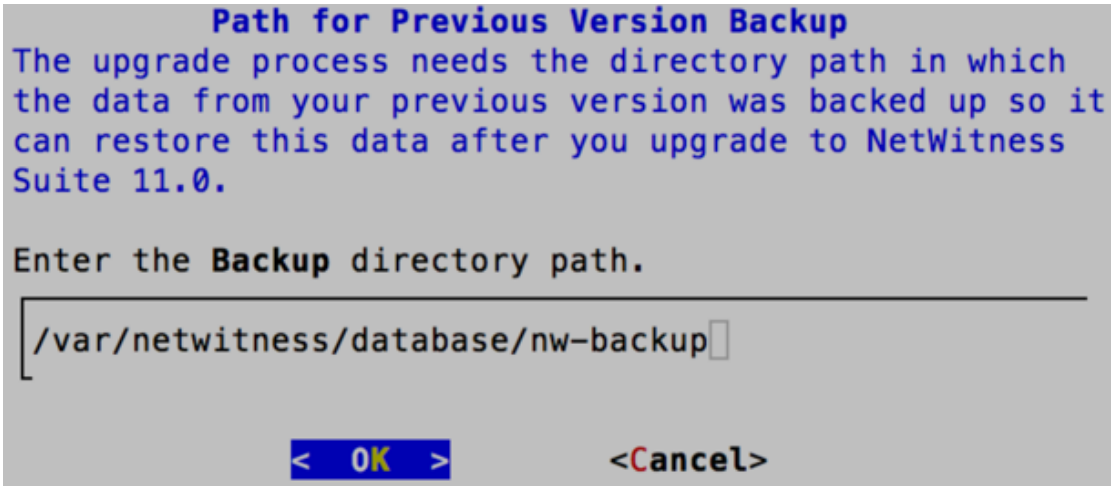
Attention : Si l'hôte choisi pour le serveur NW est incorrect et que vous terminez la mise à niveau, vous devez répéter les étapes 1 à 11 de Installer l'hôte de serveur NW 11.0 pour corriger cette erreur.

3. Naviguez jusqu'à **Oui** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**.
   Choisissez Non si vous avez déjà mis à niveau le serveur NW vers la version 11.0.
   Le message Installation ou Mise à niveau s'affiche.



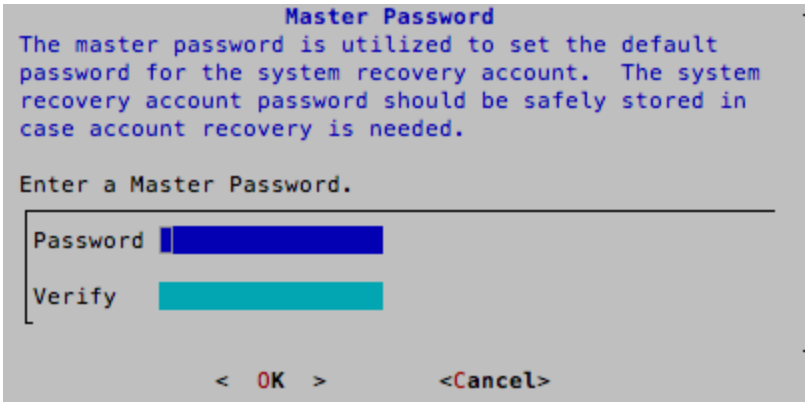
4. Utilisez la flèche vers le bas pour sélectionner **2 Mise à niveau (À partir de la version précédente)**, naviguez vers **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**.

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.
   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

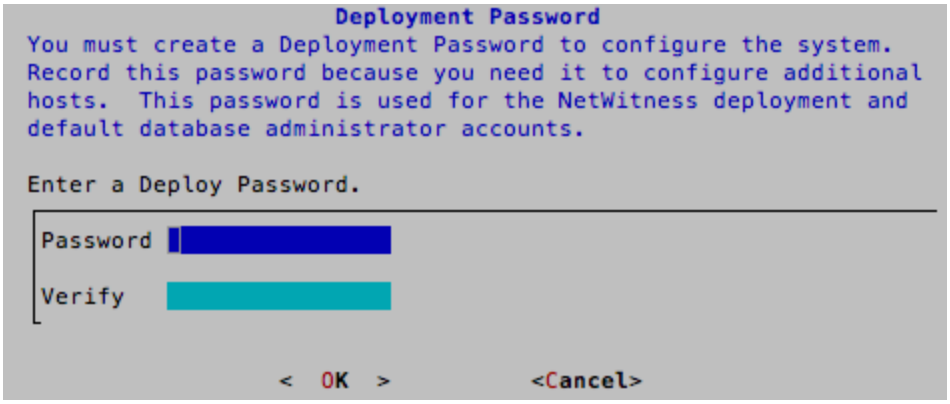
   Aucun caractère ambigu n'est pris en charge pour le mot de passe maître et le mot de passe de déploiement (par exemple : l'espace { } [ ] ( ) / \ ' " ` ~ , ; : . < > -).



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

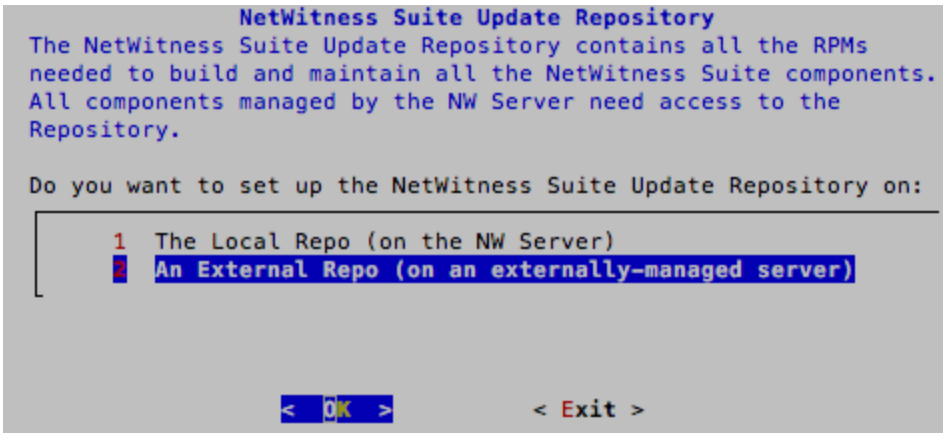
tabulation, puis appuyez sur **Entrée**.

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



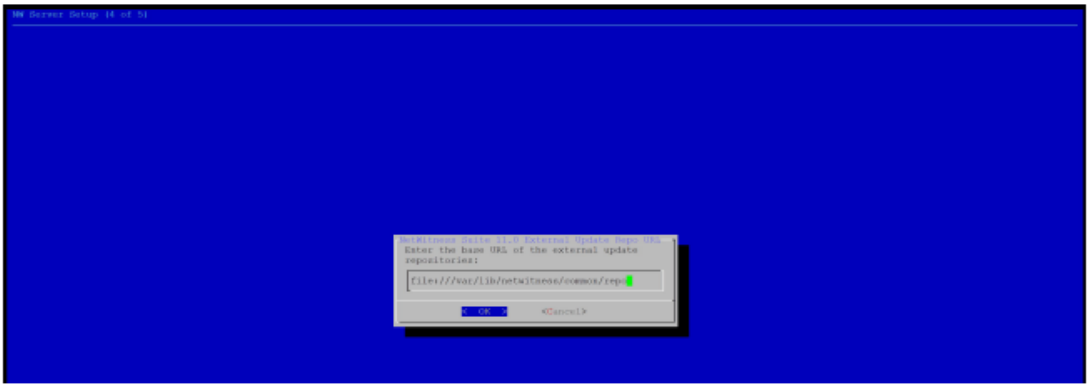
7. Saisissez le **mot de passe**, appuyez sur la touche directionnelle Bas pour accéder à **Vérifier**, saisissez à nouveau le mot de passe, naviguez jusqu'à **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**.

   Le message Mise à jour du référentiel s'affiche.



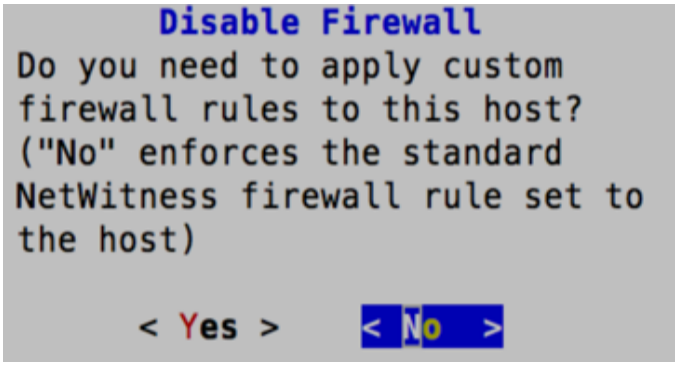
   Vous devez utiliser le même référentiel que celui que vous avez utilisé pour les hôtes de serveur NW pour tous les hôtes.

8. Utilisez les flèches vers le haut et vers le bas pour sélectionner **2 Un référentiel externe (sur un serveur géré en externe)**. L'interface utilisateur vous invite à saisir une URL.



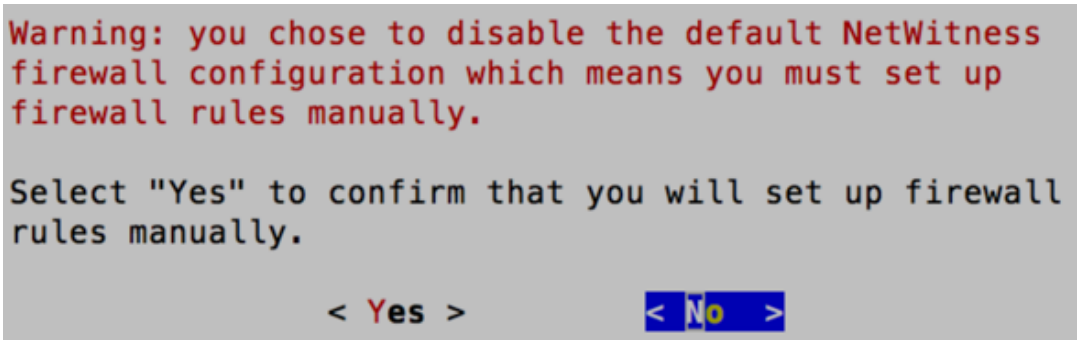
Voir « Définir un référentiel externe avec les mises à jour RSA et de système d'exploitation » sous « Procédures liées aux hôtes et services » dans le *Guide de mise en route des hôtes et des services RSA NetWitness Suite 11.0* pour obtenir des instructions.Accédez à la Table des matières principale pour la version 11.0 trouver des documents NetWitness Suite 11.0.

9. Saisissez l'URL de base du référentiel externe NetWitness Suite, puis cliquez sur **OK**. Le message de désactivation ou d'utilisation de la configuration de pare-feu standard s'affiche.



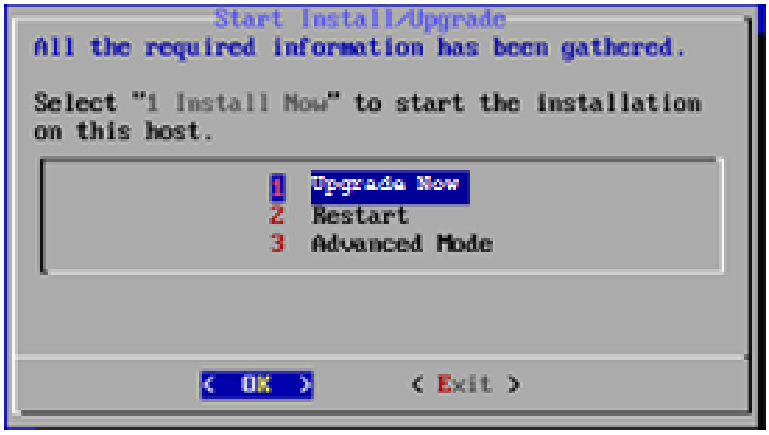
10. Naviguez vers l'onglet **Non** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** pour utiliser la configuration de pare-feu standard. Naviguez vers l'onglet **Oui** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** pour désactiver la configuration de pare-feu standard.

- Si vous sélectionnez Oui, confirmez votre sélection.



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

L'invite de démarrage de la mise à niveau s'affiche.



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 10.6.4.x vers le serveur NW 11.0 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)
```

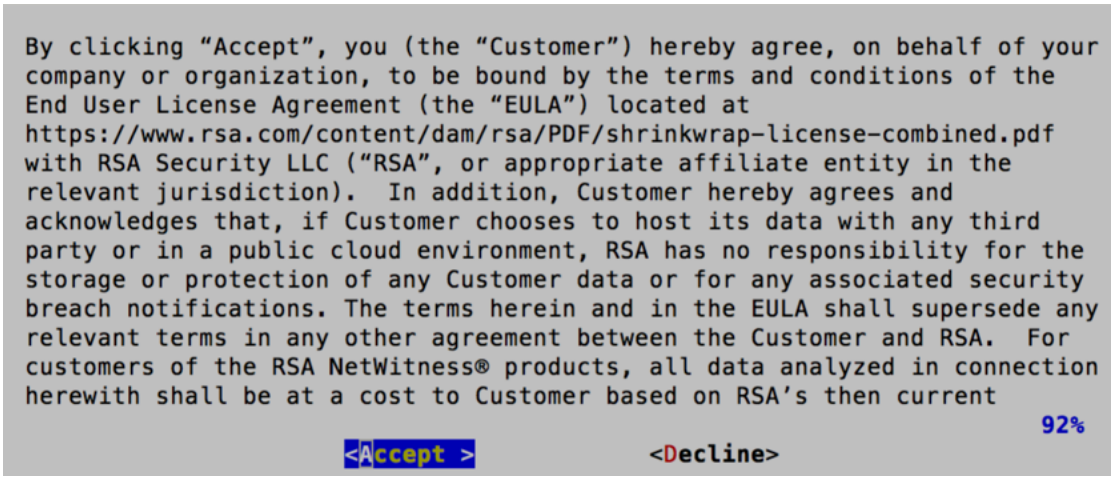
Installer la version 11.0 d'un hôte de serveur autre que NW

Veillez à sauvegarder les données 10.6.4.x pour l'hôte. **Vous devez suivre les instructions indiquées dans** Instructions de sauvegarde **pour sauvegarder l'hôte.**

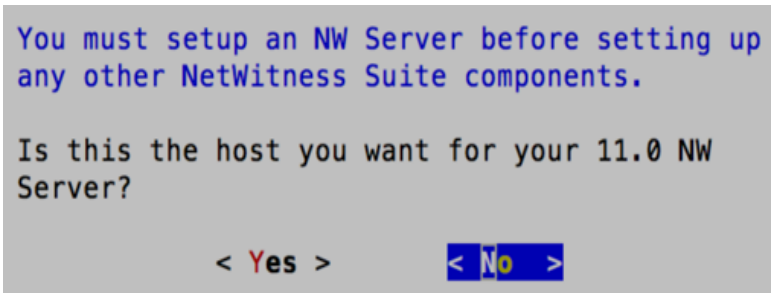
Attention : Exécutez la sauvegarde immédiatement avant la mise à niveau de l'hôte vers la version 11.0 afin que les données soient aussi récentes que possible.

Pour installer la version 11.0 d'un hôte de serveur autre que NW, procédez comme suit :

1. **Mettez sous tension** la machine virtuelle du serveur autre que NW et exécutez la commande `nwsetup-tui`.
   Cette opération démarre le programme d'installation et les conditions générales d'utilisation s'affichent.

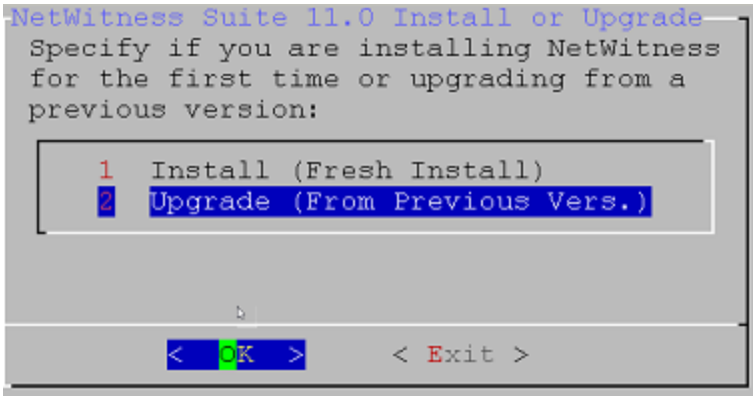


2. Naviguez jusqu'à **Accepter** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**.
   Le message « S'agit-il du serveur NW ? » s'affiche.

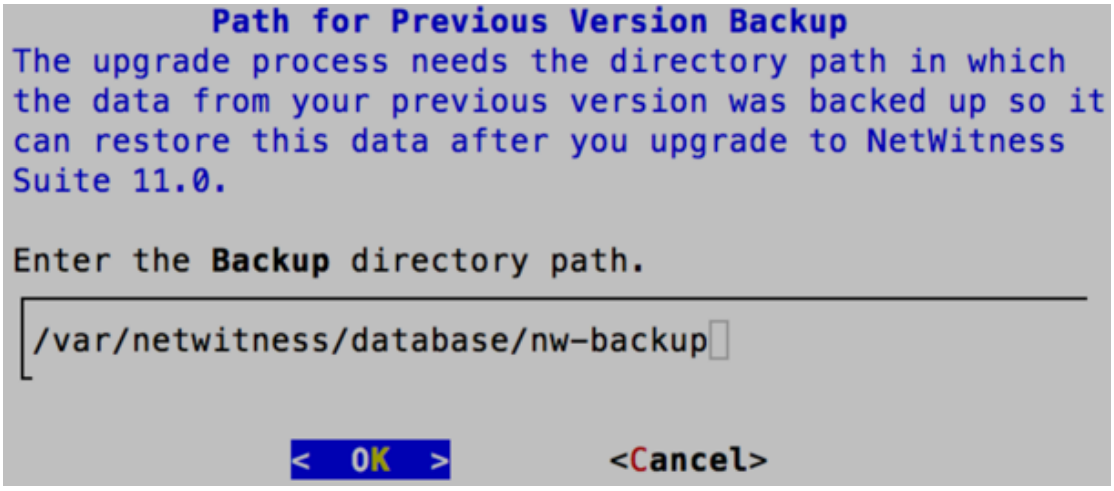


Attention : Si l'hôte choisi pour le serveur NW est incorrect et que vous terminez la mise à niveau, vous devez répéter les étapes 1 à 11 de Installer l'hôte de serveur NW 11.0 pour corriger cette erreur.

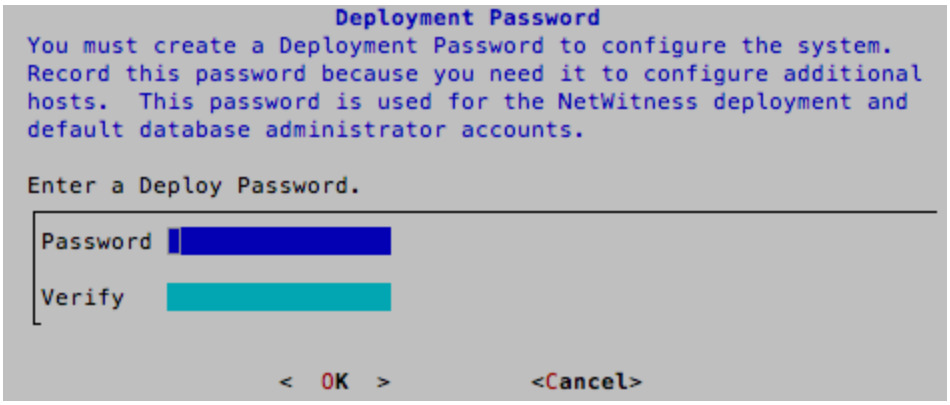
3. Naviguez jusqu'à **Non** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**.
   Le message Installation ou Mise à niveau s'affiche.



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.

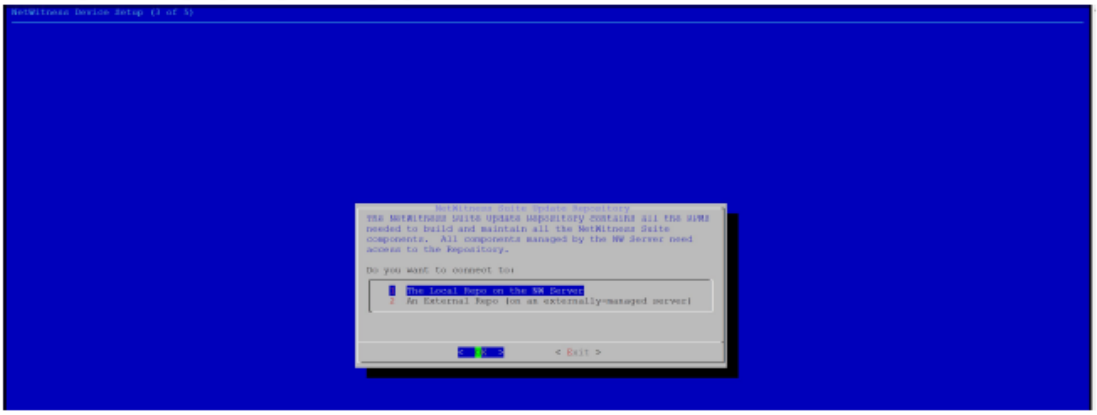


5. Naviguez vers **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** si vous souhaitez conserver ce chemin d'accès. Sinon, modifiez le chemin d'accès, naviguez jusqu'à **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** pour le modifier.
   Le message « Mot de passe de déploiement » s'affiche.



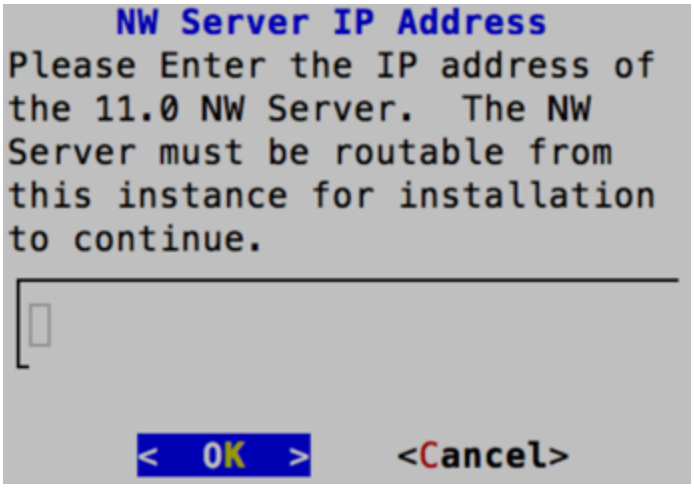
Remarque : Vous devez utiliser le même mot de passe de déploiement que vous avez utilisé lors de la mise à niveau du serveur NW.

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.

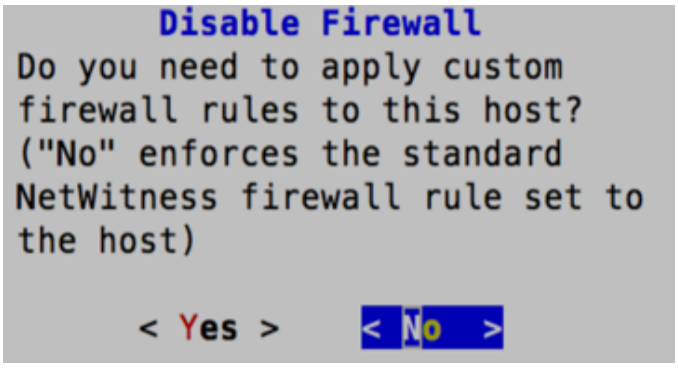


7. Utilisez les flèches vers le bas et vers le haut pour sélectionner **1 Le référentiel local (sur le serveur NW)**, naviguez jusqu'à **OK** avec la touche de tabulation, puis appuyez sur **Entrée**.

8. Saisissez l'URL de base du référentiel externe NetWitness Suite et cliquez sur **OK**.
   L'adresse IP du serveur NW s'affiche.

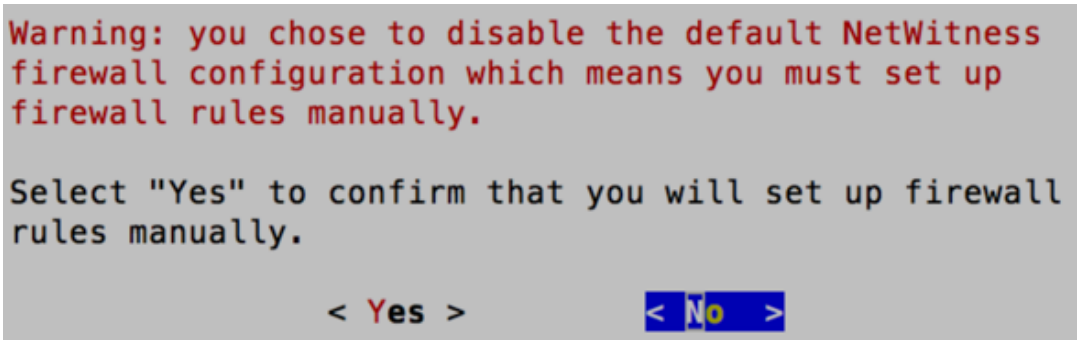


9. Saisissez l'adresse IP du serveur NW, naviguez jusqu'à **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**.
   Le message de désactivation ou d'utilisation de la configuration de pare-feu standard s'affiche.



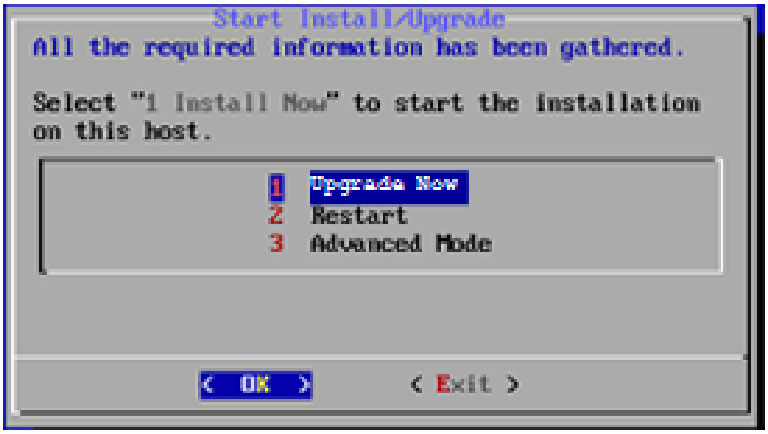
10. Naviguez vers l'onglet **Non** à l'aide de la touche de tabulation, puis appuyez sur Entrée pour utiliser la configuration standard du pare-feu. Naviguez vers l'onglet **Oui** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** pour désactiver la configuration de pare-feu standard.

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



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

L'invite de démarrage de la mise à niveau s'affiche.



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 11.0 est terminée.
12. Installez le service sur cet hôte :
    a. Connectez-vous à NetWitness Suite.
    Saisissez `https://<NW-Server-IP-Address>/login` dans votre navigateur pour accéder à l'écran de connexion NetWitness Suite
    b. Cliquez sur **ADMIN** > **Hôtes**.
    La boîte de dialogue **Nouveaux hôtes** s'affiche avec la vue **Hôtes** grisée en arrière-plan.

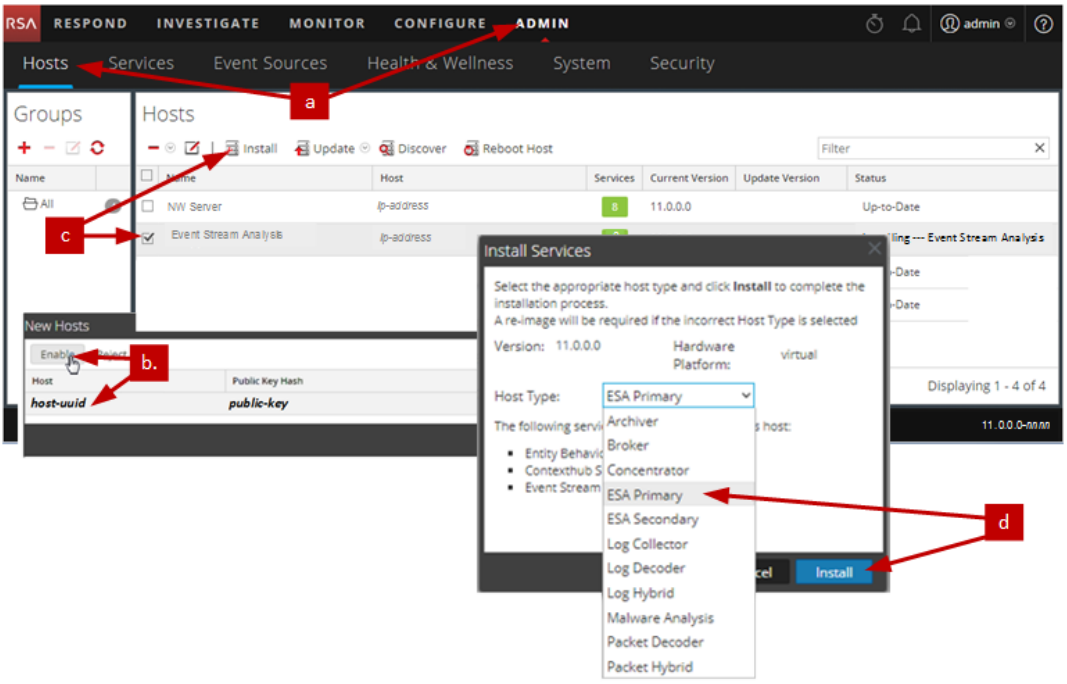
    > **Remarque :** Si la boîte de dialogue **Nouveaux hôtes** ne s'affiche pas, cliquez sur **Découvrir** dans la barre d'outils de la vue Hôtes.

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

d. Sélectionnez cet hôte (par exemple, **Event Stream Analysis**), puis cliquez sur Install

La boîte de dialogue **Installer les services** s'affiche.

e. 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

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

Reportez-vous au *Guide RSA NetWitness 11.0 Legacy Windows Collection* dans RSA Link (https://community.rsa.com/docs/DOC-75593) pour en savoir plus sur la façon d'installer ou de mettre à jour la Collection Windows d'ancienne génération.

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 10.6.4.x vers la version 11.0. Ces tâches sont organisées selon les catégories suivantes.

- Global
- NetWitness Endpoint
  RSA prend en charge NetWitness Endpoint versions 4.3.0.4, 4.3.0.5 et 4.4 uniquement pour NetWitness Suite 11.0.
- Event Stream Analysis
- Log Collection
- Reporting Engine
- Respond
- RSA NetWitness SecOps Manager
- Security

Tâches globales

Tâche 1 - 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 11.0 avant de supprimer les fichiers associés aux sauvegardes dans les répertoires locaux sur vos hôtes 11.0.

Sauvegarder les fichiers `.tar`

Une fois que tous les hôtes sont mis à niveau vers la version 11.0, 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
Event Stream Analysis	`/opt/rsa/database/nw-backup`	`/var/netwitness/database/nw-backup/restore`

Hôte	Chemin de sauvegarde	Chemin de restauration
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`

Tâche 2 - Restaurer les serveurs NTP

Vous devez utiliser l'interface utilisateur NetWitness Suite 11.0 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 11.0 - Guide de configuration système* pour obtenir des instructions détaillées sur la façon d'ajouter des serveurs NTP. Accédez à la Table des matières principale pour la version 11.0 trouver des documents NetWitness Suite 11.0.

Tâche 3 - 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 pour la version 11.0 trouver des documents NetWitness Suite 11.0.

Tâche 4 - Mapper à nouveau la licence de serveur virtuel NW à l'adresse MAC de la version 10.6.4.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 11.0 à l'adresse MAC de la version 10.6.4.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 pour la version 11.0 trouver des documents NetWitness Suite 11.0.

(Conditionnel) Tâche 5 - Si vous avez désactivé la configuration de pare-feu standard - 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 6 - 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 10.6.4.

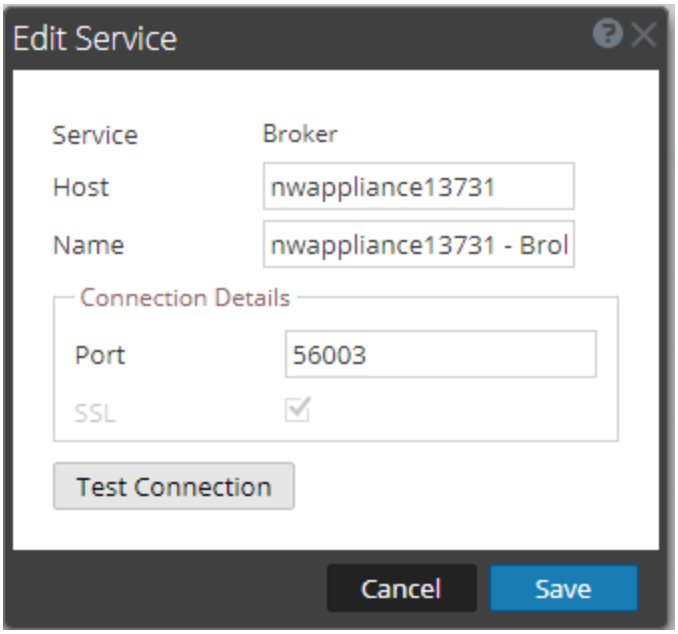
NetWitness Suite 11.0 ne peut pas communiquer avec les services de base pour ces clients, car ils utilisent un port 500XX non SSL. Vous devez mettre à jour les ports du service Core vers un port SSL dans la boîte de dialogue Modifier le service.

1. Connectez-vous à NetWitness Suite
2. Accédez à **ADMIN** >**Services**.

3. 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

4. Cliquez sur (Modifier) depuis la barre d'outils de la vue **Services**.
   La boîte de dialogue Modifier le service s'affiche.
5. Modifiez le port de non SSL à SSL, comme indiqué dans le tableau, puis cliquez sur **Enregistrer** (par exemple, modifiez le port du Broker de 50003 à 56003).



NetWitness Endpoint

Tâche 7 - Reconfigurer les alertes Endpoint via le bus de messages

1. Sur le server 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 11.0, l'hôte virtuel est `/rsa/system`. Pour les versions 10.6.4.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 8 - Reconfigurer la détection automatisée des menaces pour ESA

Si vous avez utilisé la détection automatisée des menaces dans 10.6.4.x, vous devez exécuter les étapes suivantes pour la reconfigurer à l'aide du service ESA Analytics dans 11.0.

1. Connectez-vous à NetWitness Suite 11.0
2. Cliquez sur **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**».
3. Conditionnel - Si votre liste blanche de détection automatisée des menaces précédente s'affiche dans l'onglet **Listes** 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 pour la version 11.0 trouver des documents NetWitness Suite 11.0.

Tâche 9 - 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 10.6.4.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. Définir les autorisations des utilisateurs en exécutant la commande suivante (utilisez le nom d'utilisateur de l'étape 1) :

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

   Par exemple :

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

Tâche 10 - Activer le Tableau de bord des indicateurs de malware et de menaces

Dans la version 11.0.0, le **Tableau de bord des indicateurs de menaces** de la version 10.6.4.x a été renommé **Tableau de bord des indicateurs de malware et de menaces**. Si vous utilisiez ce tableau de bord dans la version 10.6.4.x, vous devez :

1. Activer le **Tableau de bord des indicateurs de malware et de menaces** dans la version 11.0.
2. Définir la nouvelle source de données pour les dashlets.
   Reportez-vous à la section « Dashlets » dans RSA Link (https://community.rsa.com/docs/DOC-81463).

Collecte de journaux

Tâche 11 - Réinitialiser les valeurs système stables pour Log Collector après la mise à niveau

Effectuez les tâches suivantes pour réinitialiser les valeurs système stables pour Log Collector après la mise à niveau vers la version 11.0 pour vous assurer que tous les protocoles de collecte fonctionnent correctement.

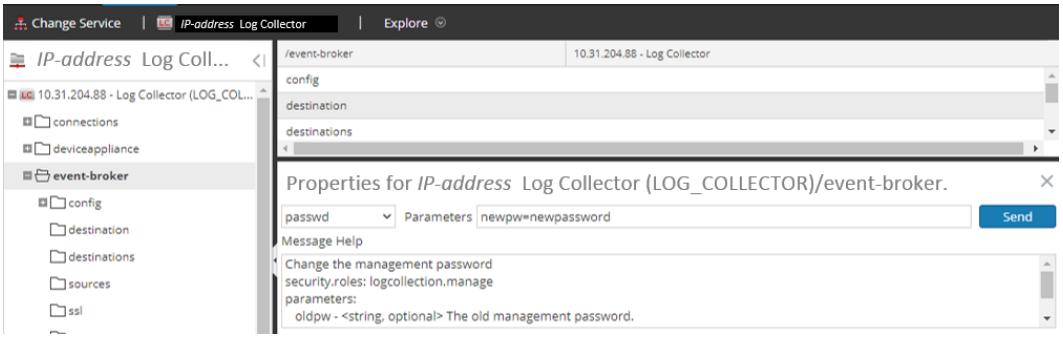
Réinitialiser les valeurs de système stable pour le Lockbox

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 « Collecte des logs : 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 pour la version 11.0 trouver des documents NetWitness Suite 11.0.

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 11.0.

1. Connectez-vous à NetWitness Suite.
2. Cliquez sur **ADMIN > Services**.
3. Sélectionnez le service Log Collector.
4. Cliquez sur  (Actions) > **Vue** > **Explorer**.
5. Cliquez avec le bouton droit sur `event-broker` > **Propriétés**.
6. 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 10.6.4.x avec le mode FIPS activé pour les Log Collectors, les Log Decoders et les Packet Decoders) Tâche 12 - 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 pour la version 11.0 trouver des documents NetWitness Suite 11.0.

Reporting Engine

Tâche 13 - 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 10.6.4.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 11.0.

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 14 - 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 pour la version 11.0 trouver des documents NetWitness Suite 11.0.

Respond

Tâche 15 - Restaurer les clés personnalisées du service Respond

Dans la version 10.6.4.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 10.6.4.x.
2. Accédez à `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json` dans la version 11.0.
   Il s'agit du nouveau fichier pour la version 11.0.
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 16 - Restaurer les scripts de normalisation personnalisés du service Respond

RSA a réintégré les scripts de normalisation du service Respond dans la version 11.0 et les a déplacés vers le nouvel emplacement suivant :
`/var/lib/netwitness/respond-server/scripts`
Si vous avez personnalisé ces scripts dans la version 10.6.4.x, vous devez :

1. Accédez 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 10.6.4.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 10.6.4.x.
3. Accédez au répertoire `/var/lib/netwitness/respond-server/scripts`.
   Ce répertoire correspond à l'endroit où NetWitness Suite 11.0 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 10.6.4.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.

(Conditionnel) Tâche 17 - Activer la rétention des données de la gestion des incidents de la version 10.6.4.x désactivée précédemment

Exécutez la procédure suivante pour activer les tâches de rétention des données de la gestion des incidents désactivées avant la mise à niveau.

1. Connectez-vous à RSA NetWitness® Suite .
2. Accédez à **ADMIN** > **Services**, puis sélectionnez le **Serveur de réponse**.
3. Cliquez sur  (Actions), **Vue** > **Explorer**.
4. Accédez au nœud `respond/dataretention`.
5. Définissez le paramètre `enable` sur `true`.

(Conditionnel) Tâche 18 - Restaurer les rôles Analyste personnalisés.

Si vous aviez des rôles personnalisés Analyste dans la version 10.6.4.x, vous devez les rétablir dans la version 11.0. Reportez-vous à la section *Ajout de rôles et attribution d'autorisations pour les rôles* dans *RSA NetWitness Suite - Guide de Warehouse Analytics*. Accédez à la Table des matières principale pour la version 11.0 trouver des documents NetWitness Suite 11.0.

NetWitness SecOps Manager

Tâche 19 - 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 pour la version 11.0 trouver des documents NetWitness Suite 11.0.

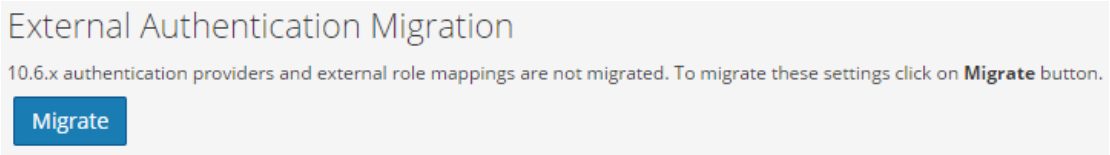
Sécurité

Tâche 20 - Migrer Active Directory (AD)

La première fois que vous vous connectez à l'interface utilisateur NetWitness Suite 11.0, vous devez cliquer sur le bouton Migrer pour effectuer la migration d'Active Directory.

Attention : Si vous n'avez pas effectué la mise à niveau à partir de 10.6.4.2, vous devez appliquer le correctif 11.0.0.1 immédiatement avant de vous connecter à NetWitness Suite 11.0 et de migrer Active Directory. Il n'est pas nécessaire d'appliquer le correctif 11.0.0.1 si vous avez effectué la mise à niveau de la version 10.6.4.2 vers la version 11.0.

1. Connectez-vous à NetWitness Suite à l'aide de vos informations d'identification `admin user`.
2. Cliquez sur **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 21 - Modifier la configuration AD migrée pour télécharger le certificat

Si vous utilisez un certificat auto-signé dans le serveur Active Directory (AD) et que SSL est activé pour la connexion Active Directory dans 10.6.4.x, vous devez modifier la configuration AD migrée afin de télécharger le certificat (le certificat auto-signé ou le certificat d'autorité de certification).

Exécutez la procédure suivante pour modifier la configuration AD migrée afin de télécharger le certificat (le certificat auto-signé ou le certificat d'autorité de certification).

1. Connectez-vous à NetWitness Suite.
2. Cliquez sur **ADMIN** > **Sécurité**, puis cliquez sur l'onglet **Paramètres**.
3. Sous **Paramètres Active Directory**, sélectionnez une configuration Active Directory, puis cliquez sur  .

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

Tâche 22. Corriger l'échec d'authentification dans la version 11.0

Les utilisateurs ne peuvent pas se connecter à l'interface utilisateur NetWitness Suite après la mise à niveau vers la version 11.0, car l'interface ne peut pas récupérer les informations du compte utilisateur à partir de MongoDB.

- Appliquez le correctif 11.0.0.1 permettant de résoudre ce problème immédiatement après la mise à niveau vers la version 11.0.

Tâche 23 - Reconfigurer le module PAM (Pluggable Authentication Module) dans la version 11.0

Vous devez reconfigurer le PAM une fois la mise à niveau vers la version 11.0 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 pour la version 11.0 trouver des documents NetWitness Suite 11.0.

Vous pouvez consulter vos fichiers de configuration 10.6.4.x PAM dans le répertoire **/etc.** de vos données de sauvegarde 10.6.4.x pour obtenir des informations.

Annexe A. Dépannage

Cette rubrique décrit les problèmes que vous pouvez rencontrer lors de la mise à niveau des solutions. 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 :

- Programme d'installation de la version 11.0 (`nwsetup-tui`)
- Sauvegarde
- Event Stream Analysis
- Généralités
- Service Log Collector (`nwlogcollector`)
- Serveur NW
- Reporting Engine

Programme d'installation de la version 11.0 (`nwsetup-tui`)

Problème	Le programme d'installation de l'hôte (`nwsetup-tui`) se ferme et crée le message d'erreur suivant dans `/var/log/netwitness/bootstrap/launch/security-server/security-server.log` :
	`<yyyy-mm-dd hh:mm:ss,nnn> [ main] ERROR SystemOperation|Service startup failed. Running in safe mode org.h2.jdbc.JdbcSQLException: The database is read only [90097-193]`
	`at org.h2.message.DbException.getJdbcSQLException(DbException.java:345) ...`
	`at org.springframework.jdbc.datasource.AbstractDriverBasedDataSource.getConnection (AbstractDriverBasedDataSource.java:159)`
	`at com.rsa.asoc.security.upgrade.legacy.MigrationDatabase.<init>(MigrationDatabase.java:113)`

Cause	La base de données H2 requiert l'autorisation en écriture pour effectuer l'installation de l'hôte.

Solution	Dans la ligne de commande du serveur NW, indiquez les droits d'écriture sur `H2.db`, redémarrez le serveur NW et redémarrez le programme d'installation nwsetup-tui.
	`chmod o+w /var/lib/netwitness/uax/db/platform.h2.db`
	`systemctl restart rsa-nw-security-server.service`
	`nwsetup-tui`

Sauvegarde (script `nw-backup`)

Message	`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 : Modifier le mot de passe MongoDB pour le compte administrateur » du *RSA NetWitness® Suite Guide de Configuration d'Event Stream Analysis. Accédez à la* Table des matières principale *pour la version 11.0 trouver des documents NetWitness Suite 11.0.*

Event Stream Analysis

Problème	Le service ESA se bloque après la mise à niveau vers la version 11.0 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. Pour redémarrer ESA, exécutez la commande suivante :
	`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.

Général

Les logs mentionnés dans cette rubrique sont publiés dans `/var/log/install/install.log` sur l'hôte de serveur NW.

Message	`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 à l'aide de la commande ci-dessous. `systemctl restart rsa-sms`

Message	`<timestamp> <host>: SMS_PostInstall: INFO: Free disk space on /opt is nGB` `<timestamp> <host>: SMS_PostInstall: WARN: Disk space check failed on /opt. The available disk space nGB is less than the recommended minimum disk space of 10GB.`
Cause	Espace disque faible ou insuffisant alloué par le service SMS.
Solution	RSA vous recommande de fournir un minimum de 10 Go d'espace disque pour que le service SMS puisse s'exécuter de façon optimale.

Problème	Après avoir exécuté le programme d'installation d'un hôte de serveur autre que NW, vous devez accéder à l'interface utilisateur, activer l'hôte et installer le service sur l'hôte dans la vue Hôtes. Si le message « Install error View Details » s'affiche dans la colonne **État** de la vue Hôtes, l'hôte a perdu la connectivité suite à des problèmes réseau.
Solution	Réinstallez le service sur l'hôte dans la vue hôtes.

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	`<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 pour la version 11.0 trouver des documents NetWitness Suite 11.0.

Message	*`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 pour la version 11.0 trouver des documents NetWitness Suite 11.0..

Message	`<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 pour la version 11.0 trouver des documents NetWitness Suite 11.0.

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 10.6.4 vers la version 11.0 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	`<timestamp> : Available free space in /home/rsasoc/rsa/soc/reporting-engine [ existing-GB ] is less than the required space [ required-GB ]`
Cause	Échec de la mise à jour du Reporting Engine car vous ne disposez pas de suffisamment d'espace disque.
Solution	Libérez de l'espace disque pour disposer de l'espace requis mentionné dans le message log. Consultez la rubrique « Ajouter de l'espace supplémentaire pour les rapports volumineux » dans le *Guide de configuration de Reporting Engine* pour obtenir des instructions sur la façon de libérer de l'espace disque. Accédez à la Table des matières principale pour la version 11.0 trouver des documents NetWitness Suite 11.0.

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

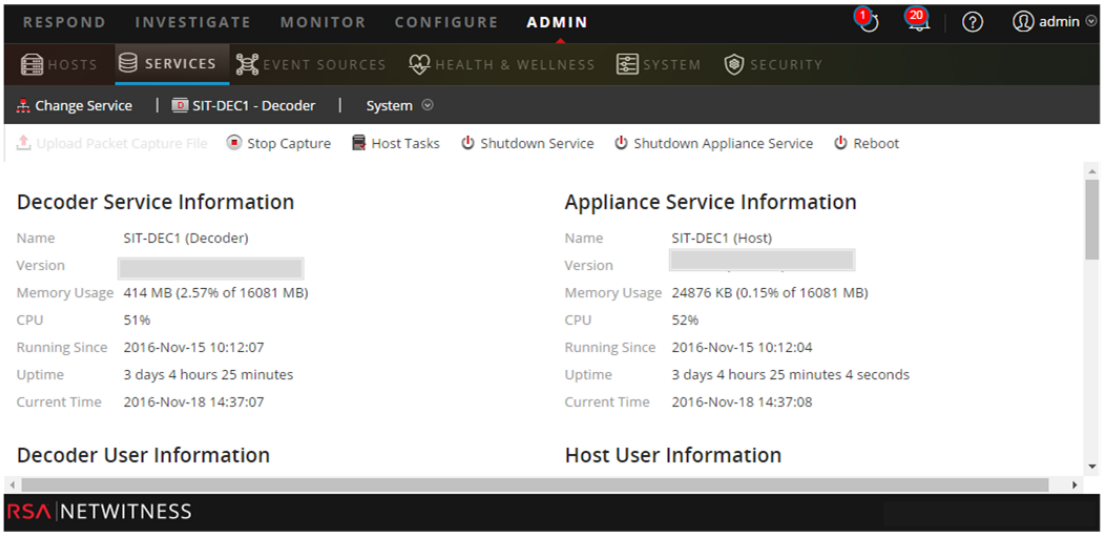
RSA vous recommande d'arrêter la capture et l'agrégation des paquets et des logs avant la mise à niveau d'un hôte Decoder, Concentrator et Broker vers la version 11.0. Si vous effectuez cette opération, vous devez redémarrer la capture et l'agrégation de paquets et des logs après la mise à jour de ces hôtes.

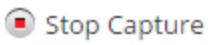
Arrêter la capture et l'agrégation des données

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 

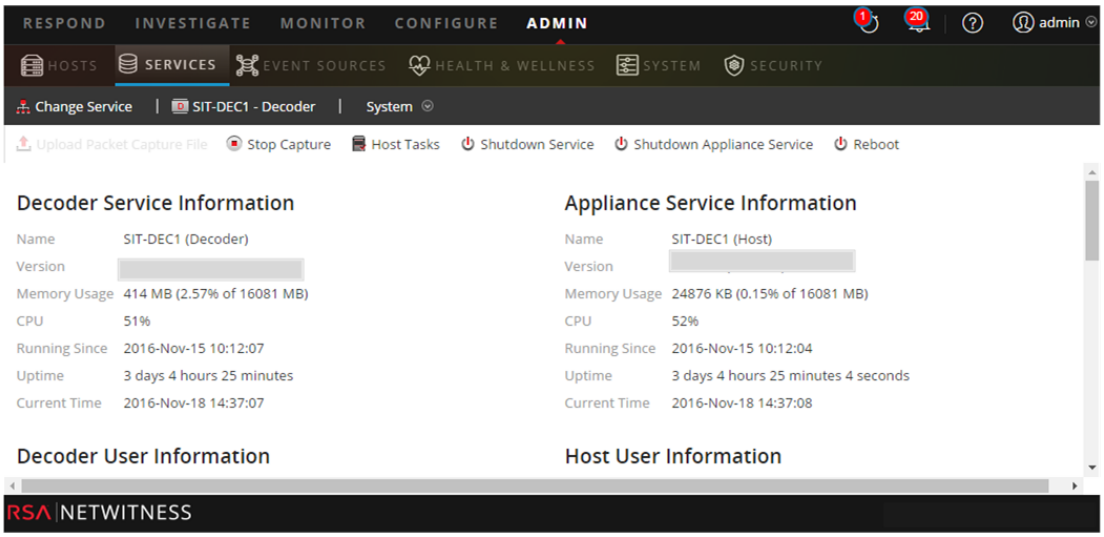
.

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**.



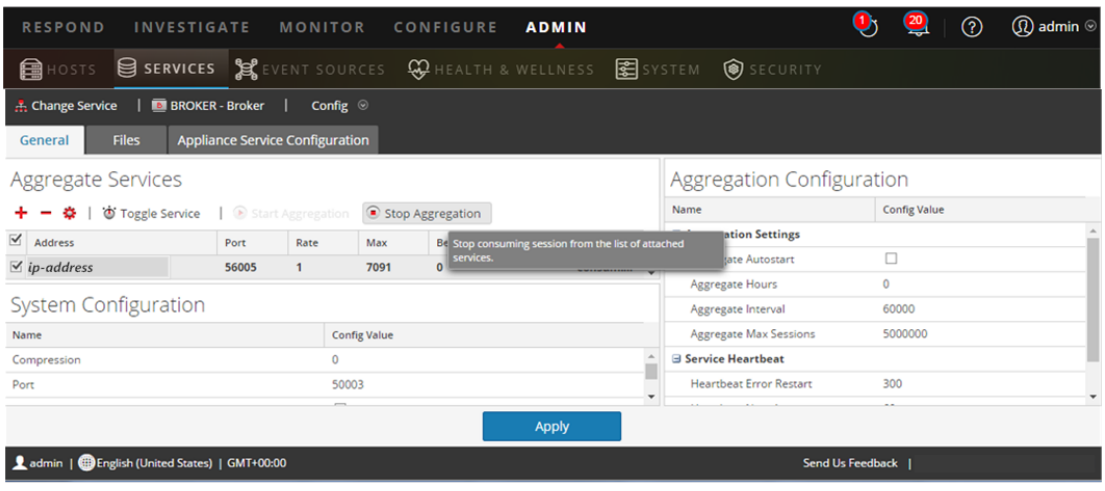
3. Sous  (actions), sélectionnez **Afficher** > **Système**.

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 et l'agrégation des paquets et des logs après la mise à jour vers 11.0.

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

Lors de la mise à niveau de la version 10.6.4.x vers la version 11.0, le service Broker est redémarré et lance alors automatiquement l'agrégation.

Historique des révisions

Révision	Date	Description	Auteur
1	16 octobre 2017	Version pour les opérations	IDD
1.1	25 octobre 2017	Modifications : • Les sections « Active Directory » et « Modifications d'attribut d'utilisateur et de rôle affectant Enquête » ont été modifiées pour faire référence aux correctifs 10.6.4.2 et 11.0.0.1. • Corriger l'échec d'authentification dans la version 11.0	IDD