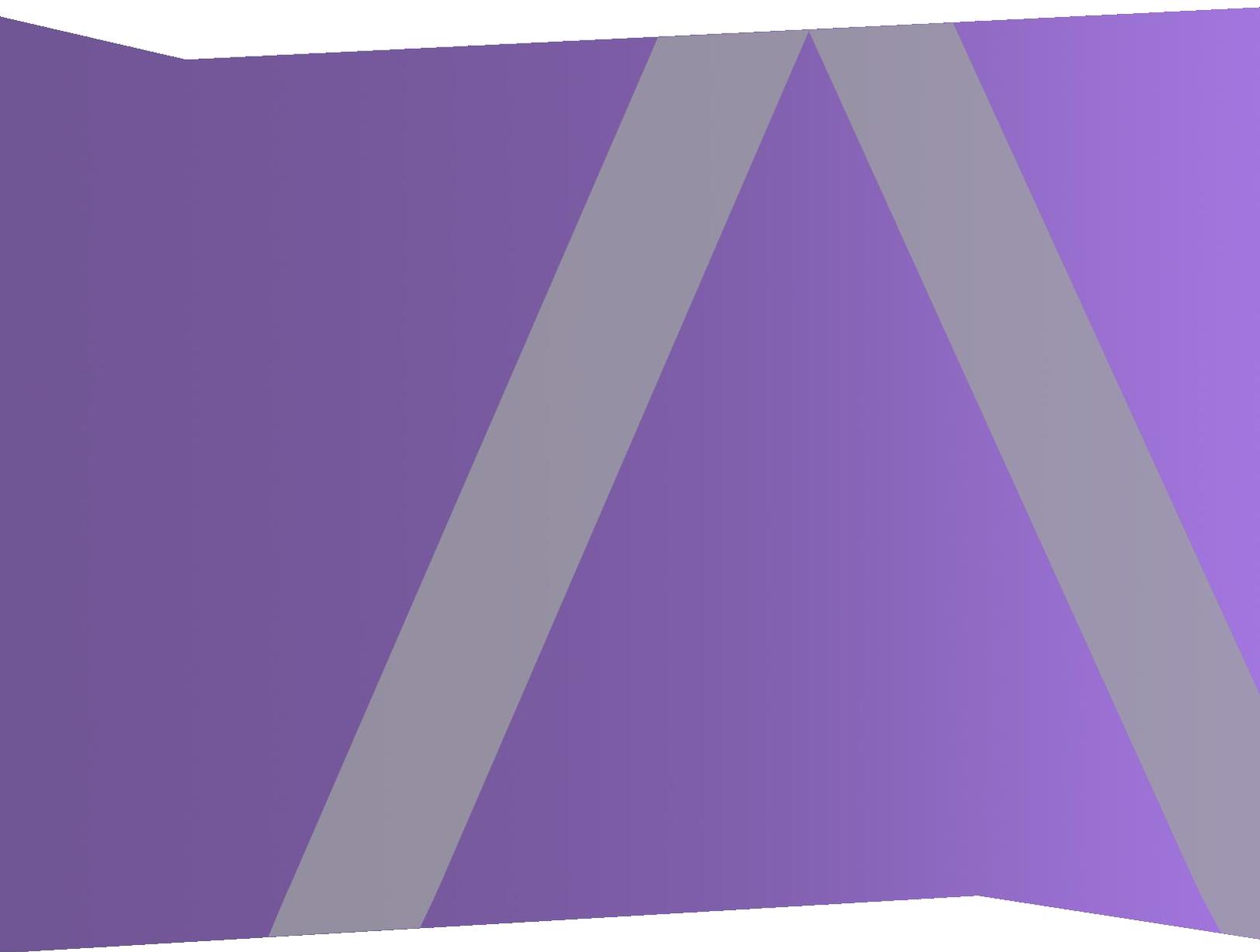




Guide de déploiement

pour la plate-forme RSA NetWitness® 11.3



Copyright © 1994-2019 Dell Inc. or its subsidiaries. All Rights Reserved.

Informations de contact

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

Marques commerciales

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

Contrat de licence

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

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

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

Licences tierces

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

Remarque sur les technologies de chiffrement

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

Distribution

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

juillet 2019

Sommaire

Les bases	5
Déploiement de base	6
Processus	6
Schéma de déploiement général NetWitness Platform	7
Schéma détaillé de déploiement des hôtes RSA NetWitness Platform	8
Options de déploiement	9
Procédures de configuration facultatives pour le déploiement	10
Agrégation de groupes	10
Recommandations à propos du déploiement d'agrégation de groupes RSA	10
Avantages de l'utilisation de l'agrégation de groupes	10
Configurer l'agrégation de groupes	12
Catégories hybrides sur le serveur NW	15
Deuxième serveur Endpoint	16
Hôte du serveur NW de secours à chaud	17
Procédures	17
Scénario de basculement planifié	18
Scénario de basculement requis sans remplacement de matériel	18
Scénario de basculement requis avec remplacement de matériel	18
Configuration du serveur NW secondaire en rôle de veille	19
Basculement du serveur NW principal vers le serveur NW secondaire	33
Retour arrière du serveur NW secondaire vers le serveur NW principal	34
Architecture réseau et ports	35
Schéma de l'architecture réseau NetWitness Platform	35
Schéma de l'architecture réseau NetWitness (paquets)	36
Schéma de l'architecture réseau de NetWitness Logs	37
Liste complète des hôtes et des ports de service et iDRAC NetWitness Platform	38
Hôte de serveur NW	39
Hôte Archiver	40
Hôte Broker	41
Hôte Concentrator	42
Endpoint Log Hybrid	43
Hôte Event Stream Analysis (ESA)	44
Ports iDRAC	45
Hôte Log Collector	46
Hôte de Log Decoder	47

Hôte Log Hybrid	48
Hôte Malware	50
Hôte de décodeur réseau	51
Hôte réseau hybride	52
Hôte UEBA	53
Architecture de NetWitness Endpoint	54
Intégration du point de terminaison NetWitness 4.4 avec la plate-forme NetWitness	54
Comment modifier le port UDP pour Endpoint Log Hybrid	55
Tâche 1 - Informer tous les agents qu'ils doivent utiliser un nouveau port UDP	55
Tâche 2 - Mettre à jour le port sur tous les hôtes Endpoint Log Hybrid dans votre environnement	55
Exigences du site et sécurité	57
Usages prévus de l'application	57
Service	57
Informations relatives à la sécurité	57
Sélection de site	57
Pratiques de manipulation de l'équipement	57
Avertissements relatifs à l'alimentation et à l'électricité	58
Avertissements relatifs au montage en rack	58
Refroidissement et circulation de l'air	58

Les bases

Ce guide décrit les exigences de base d'un déploiement NetWitness Platform. De plus, il présente des scénarios optionnels pour répondre aux besoins de votre entreprise. Même dans de petits réseaux, une planification peut garantir un déroulement sans accroc une fois que vous êtes prêt à mettre les hôtes en ligne.

Remarque : Ce document fait référence à des documents supplémentaires disponibles sur RSA Link. Accédez à la [Table des matières principale](#) pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

Il existe de nombreux facteurs à prendre en compte avant de déployer NetWitness Platform. Les éléments suivants ne sont que quelques-uns de ces facteurs. Vous devez estimer les besoins en matière de croissance et de stockage lorsque vous prenez ces facteurs en considération

- Taille de votre entreprise (nombre de sites et d'utilisateurs NetWitness Platform)
- Volume de données réseau et de logs à traiter
- Performances dont chaque rôle d'utilisateur NetWitness Platform a besoin pour travailler efficacement.
- Prévention des périodes d'interruption (comment éviter un point unique de défaillance).
- L'environnement dans lequel vous comptez exécuter NetWitness Platform
 - Les hôtes physiques RSA (logiciels en cours d'exécution sur le matériel fourni par RSA). Reportez-vous au *Guide d'Installation d'hôtes physiques RSA NetWitness® Platform* pour obtenir des instructions détaillées sur la façon de déployer les hôtes physiques RSA.
 - Logiciels uniquement fournis par RSA :
 - Hôtes virtuels (sur site)
Consultez le *Guide d'installation des hôtes virtuels RSA NetWitness® Platform* pour obtenir des instructions détaillées sur la façon de déployer des hôtes virtuels sur site.
 - vCloud :
 - Amazon Web Services (AWS)
Consultez le *Guide de déploiement AWS RSA NetWitness® Platform* pour obtenir des instructions détaillées sur la façon de déployer des hôtes virtuels dans AWS.
 - Azure
Consultez le *Guide d'installation Azure RSA NetWitness® Platform* pour obtenir des instructions détaillées sur la façon de déployer des hôtes virtuels dans Azure.

Déploiement de base

Avant de pouvoir déployer NetWitness Platform vous devez :

- Prendre en considération les exigences de votre entreprise et comprendre le processus de déploiement.
- Avoir une vue d'ensemble de la complexité et de la portée d'un déploiement NetWitness Platform.

Processus

Les composants et la topologie d'un réseau NetWitness Platform peuvent varier largement d'une installation à une autre et doivent être planifiés soigneusement avant le début du processus. La planification initiale comprend :

- La prise en compte des exigences liées au site et à la sécurité.
- L'examen de l'utilisation de l'architecture réseau et des ports.
- La prise en charge de l'agrégation de groupes sur les Concentrators et les Archivers ainsi que sur les hôtes virtuels .

Lorsque vous êtes prêt à commencer le déploiement, la séquence générale est la suivante :

- Pour les hôtes physiques RSA :
 1. Installez les hôtes physiques et connectez-les au réseau comme décrit dans les RSA NetWitness® Platform Guides de configuration du matériel et le *RSA NetWitness® Platform Guide d'Installation d'hôtes physiques*.
 2. Configurez les licences de NetWitness Platform comme décrit dans le *Guide d'octroi des licences RSA NetWitness® Platform*.
 3. Configurez les différents services et hôtes physiques comme décrit dans le *Guide de mise en route de l'hôte et des services RSA NetWitness® Platform*. Ce guide décrit aussi les procédures d'application des mises à jour et de préparation des mises à niveau des versions.
- Pour les hôtes virtuels sur site, suivez les instructions du *Guide de configuration de l'hôte virtuel RSA NetWitness® Platform*.
- Pour AWS, suivez les instructions du *Guide d'installation AWS RSA NetWitness® Platform*.
- Pour Azure, suivez les instructions du *Guide d'installation Azure RSA NetWitness® Platform*.

Lors de la mise à jour des hôtes et des services, suivez les directives recommandées dans la section « Exécution en mode mixte » dans le *Guide de mise en route de l'hôte et des services RSA NetWitness Platform*.

Vous devez également vous familiariser avec les Hôtes, Types d'hôte et Services qui sont utilisés dans le contexte de NetWitness Platform, également décrits dans le *Guide de mise en route des hôtes et des services RSA NetWitness Platform*.

Schéma de déploiement général NetWitness Platform

Le diagramme suivant illustre un déploiement NetWitness Platform basique sur plusieurs sites.

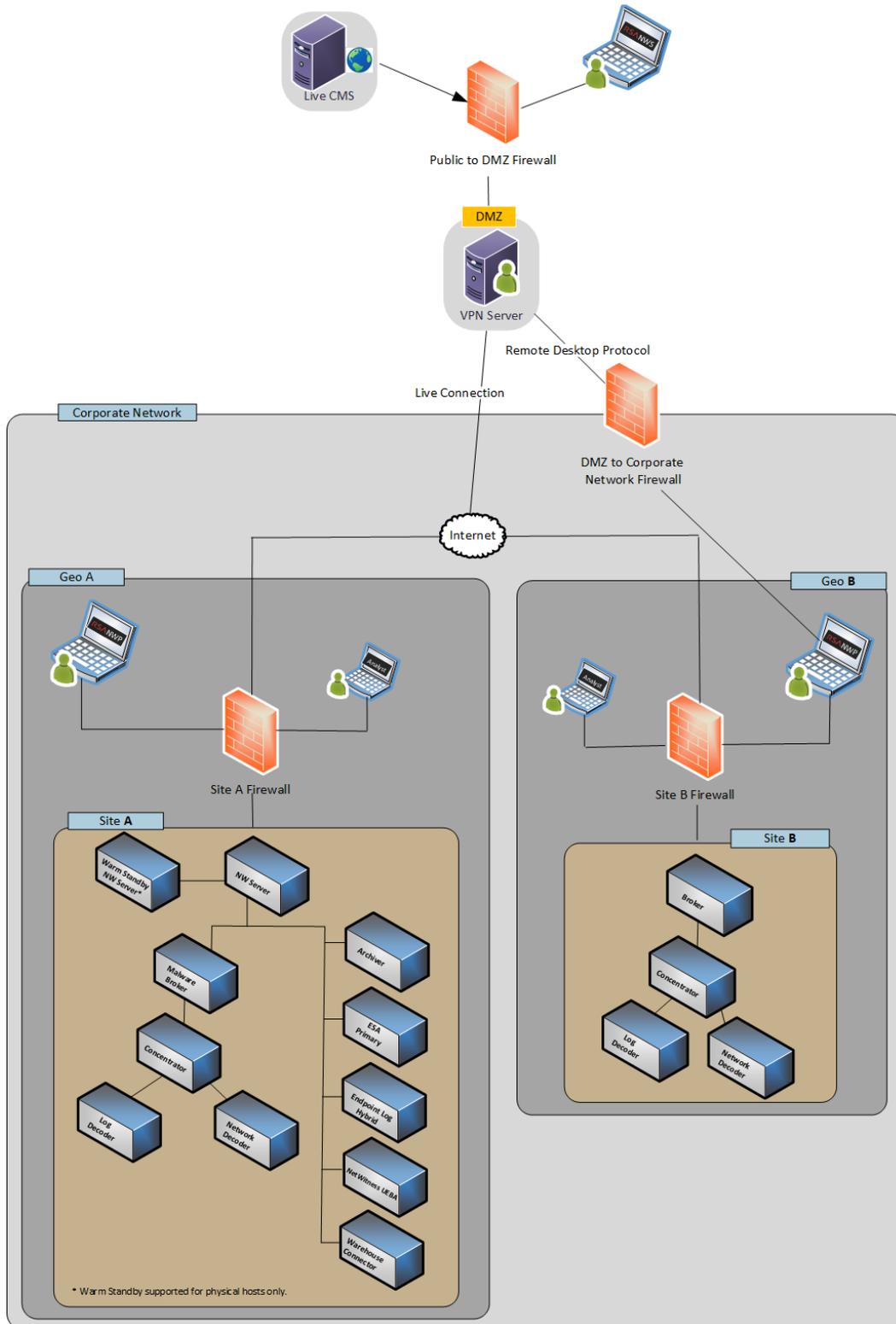
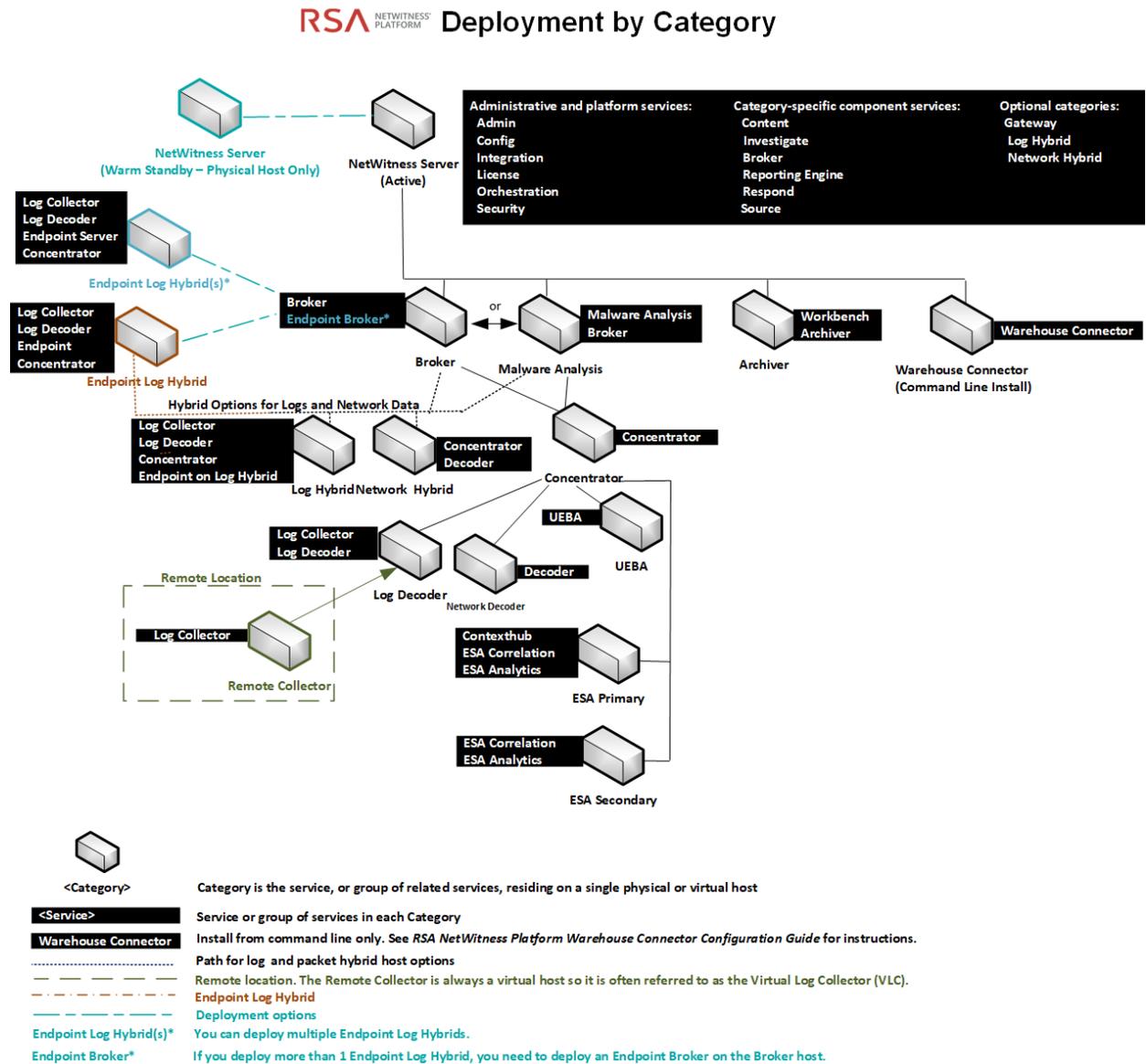


Schéma détaillé de déploiement des hôtes RSA NetWitness Platform

Le schéma suivant est un exemple de déploiement NetWitness Platform hébergé sur des machines physiques ou virtuelles. Pour obtenir des instructions sur l'installation de NetWitness Platform, reportez-vous au *Guide d'installation de l'hôte physique*, *Guide d'installation de l'hôte virtuel*, *Guide d'installation AWS*, ou au *Guide d'installation Azure*. Accédez à la [Table des matières principale](#) pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.



Options de déploiement

Vous déployez la plate-forme RSA NetWitness avec les options suivantes.

- Agrégation de groupes
- Deuxième serveur Endpoint
- Hôte du serveur NW de secours à chaud
- Catégories hybrides sur le serveur NW

Consultez les [Procédures de configuration facultatives pour le déploiement](#) pour obtenir des instructions.

Procédures de configuration facultatives pour le déploiement

[Agrégation de groupes](#)

[Catégories hybrides sur le serveur NW](#)

[Deuxième serveur Endpoint](#)

[Serveur NW de secours à chaud](#)

Agrégation de groupes

Utilisez l'agrégation de groupes pour configurer plusieurs services Archiver ou Concentrator en tant que groupe et partager les tâches d'agrégation entre eux. Vous pouvez configurer plusieurs services Archiver or Concentrator pour agréger de manière efficace plusieurs services Log Decoder et améliorer les performances des requêtes sur les données :

- Stockées dans l'Archiver.
- Traitées par le biais du Concentrator.

Recommandations à propos du déploiement d'agrégation de groupes RSA

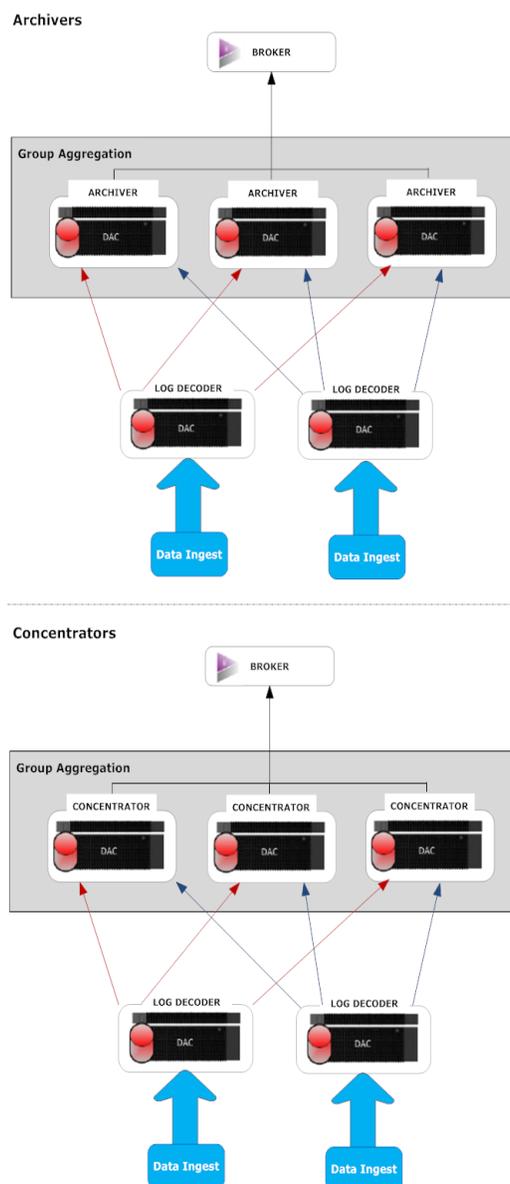
RSA recommande le déploiement suivant pour l'agrégation de groupes :

- 1 - 2 Log Decoders
- 3 - 5 Archivers ou Concentrators

Avantages de l'utilisation de l'agrégation de groupes

- Augmente la vitesse des requêtes RSA NetWitness® Platform.
- Améliore les performances des requêtes d'agrégation (nombre et somme) sur l'environnement.
- Améliore les performances du service de procédure d'enquête.
- Vous permet de stocker des données pour une durée plus longue à des fins de procédure d'enquête.

Le schéma suivant illustre l'agrégation de groupes.



Vous pouvez avoir un nombre quelconque de modules Archivers ou Concentrators regroupés qui forment un groupe d'agrégation. Les services Archiver or Concentrator du groupe divisent toute la session agrégée entre eux sur la base du nombre de sessions définies dans le paramètre Sessions d'agrégation maximum.

Par exemple, dans un groupe d'agrégation contenant 2 services Archiver ou 2 services Concentrator avec le paramètre Sessions d'agrégation maximum défini sur 10 000, les services divisent la session entre eux tel qu'illustré dans le tableau ci-dessous.

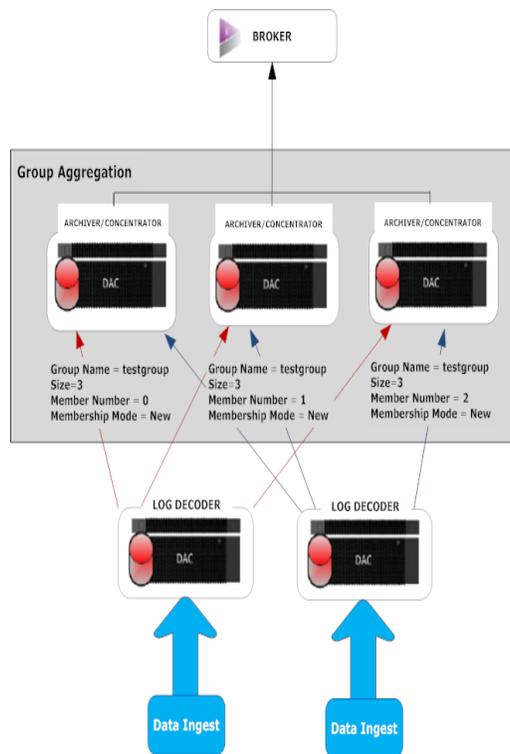
Archiver 0 ou Concentrator 0	Archiver 1 ou Concentrator 1
1 à 9 999	10 000 à 19 999
20 000 à 29 999	30 000 - 39 999
40 000 - 49 999	50 000 à 59 999

Configurer l'agrégation de groupes

Exécutez cette procédure pour configurer plusieurs services Archiver ou Concentrator sous la forme de groupes et partagez les tâches d'agrégation entre eux.

Conditions préalables

Planifiez la conception du réseau pour l'agrégation de groupes. La figure ci-après présente un exemple de configuration d'agrégation de groupes.



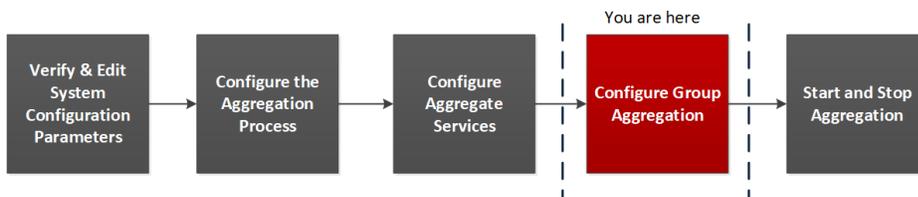
Veillez à bien examiner les paramètres d'agrégation de groupes dans le tableau suivant avant de créer un plan d'agrégation de groupes.

Paramètre	Description
Nom de groupe	Détermine le groupe auquel appartient l'Archiver ou le Concentrator. Vous pouvez ajouter autant de données d'agrégation de groupes d'un Log Decoder que voulu. Le paramètre Nom du groupe est utilisé par le Log Decoder pour identifier les services Archiver ou Concentrator qui interagissent. Tous les services Archiver ou Concentrator du groupe doivent porter le même nom de groupe.
Taille	Détermine le nombre de services Archiver ou Concentrator du groupe d'agrégation.
Numéro de membre	Détermine la position des services Archiver ou Concentrator dans le groupe d'agrégation. Pour un groupe de taille N, vous devez définir un numéro de membre de 0 à N-1 sur chaque service Archiver ou Concentrators dans le groupe d'agrégation. Par exemple : Si la taille du groupe d'agrégation est de 2, le numéro de membre de l'un des services Archiver ou Concentrator doit être défini sur 0 et le numéro de membre de l'autre Archiver ou Concentrator doit être défini sur 1.
Mode Adhésion	Il existe deux modes d'adhésion : <ul style="list-style-type: none"> • Nouveau : Permet d'ajouter un nouveau service Archiver ou Concentrator en tant que membre au groupe d'agrégation actuel ou de créer un tel groupe. Le service Archiver ou Concentrator n'agrège aucune session du service car les autres membres du groupe auraient déjà agrégé toutes les sessions sur le service. Ce service Archiver ou Concentrator n'agrègera que les nouvelles sessions telles qu'elles apparaissent sur le service. • Remplacer : Remplace un membre d'un groupe d'agrégation. Le service Archiver ou Concentrator lance l'agrégation à partir de la session la plus ancienne sur le service à partir duquel l'agrégation a lieu.

Remarque : Ce paramètre de mode d'adhésion a une incidence uniquement quand aucune session n'a été agrégée à partir du service. Après l'agrégation de certaines sessions, ce paramètre n'a aucun effet.

Configurer l'agrégation de groupes

Ce flux de travail affiche les procédures que vous avez terminées pour configurer l'agrégation de groupes.

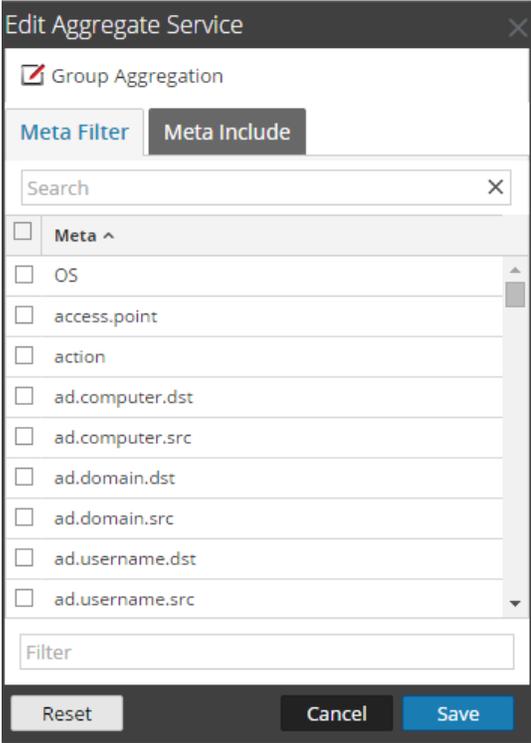


Effectuez la procédure suivante pour configurer l'agrégation de groupes.

1. Configurez plusieurs services Archiver ou Concentrator dans votre environnement. Veillez à ajouter le même Log Decoder en tant que source de données à tous les services.
2. Procédez comme suit sur tous les services Archiver ou Concentrator que vous voulez ajouter au groupe d'agrégation :

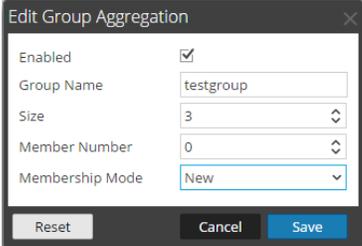
- a. Accédez à **ADMIN > Services**.
- b. Sélectionnez le service Archiver ou Concentrator, puis dans la colonne **Actions**, sélectionnez **Vue > Config**.
La vue Configuration du service Archiver ou Concentrator s'affiche.
- c. Dans la section **Services** agrégés, sélectionnez **Log Decoder**.
- d. Cliquez sur  **Toggle Service** pour modifier le statut de Log Decoder sur hors ligne s'il est en ligne.
- e. Cliquez sur .

La boîte de dialogue **Modifier le service agrégé** s'affiche.



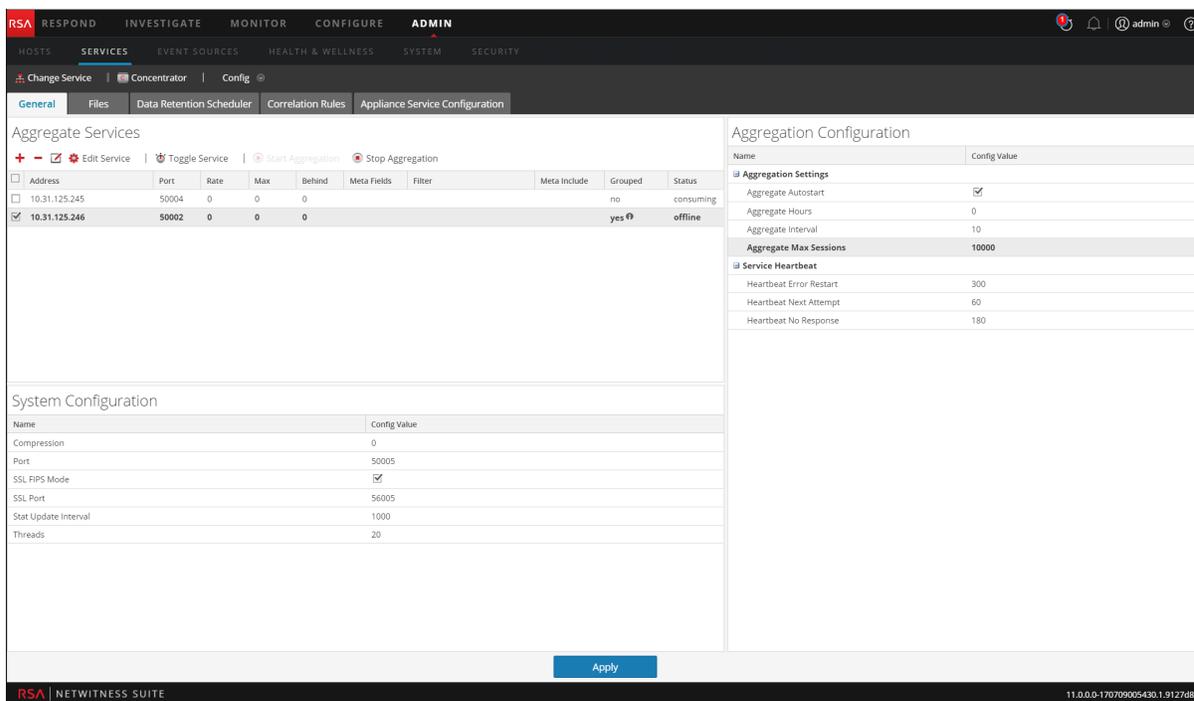
- f. Cliquez sur .

La boîte de dialogue **Modifier l'agrégation des groupes** s'affiche.



- g. Sélectionnez la case à cocher **Activé** et définissez les paramètres suivants :

- Dans le champ **Nom du groupe**, saisissez le nom du groupe.
 - Dans le champ **Taille**, sélectionnez le nombre de services Archiver ou Concentrator du groupe d'agrégation.
 - Dans le champ **Numéro de membre**, sélectionnez la position d'Archiver ou Concentrator dans le groupe d'agrégation.
 - Dans le menu déroulant **Mode Adhésion**, sélectionnez le mode.
- h. Cliquez sur **Enregistrer**.
- i. Dans la page de la vue Configuration du service, cliquez sur **Appliquer**.
- j. Effectuez l'étape **b** à l'étape **i** sur tous les autres services Archiver ou Concentrator qui doivent faire partie de l'agrégation de groupe.
3. Dans la section **Configuration de l'agrégation**, définissez le paramètre **Sessions d'agrégation max.** sur **10000**.



Catégories hybrides sur le serveur NW

Vous pouvez installer des catégories hybrides, telles que les catégories de services hybrides Log Hybrid et Network (paquet) sur un hôte physique de la gamme 6 (R640). Vous avez ainsi la possibilité de rattacher plusieurs périphériques de stockage PowerVault externe à l'hôte physique de la gamme 6 (R640).

Deuxième serveur Endpoint

Procédez comme suit pour déployer un deuxième serveur Endpoint.

1. Configurez un nouvel hôte de la plate-forme NetWitness.
 - Pour un hôte physique, réalisez les étapes 1 à 14 incluses dans la section « Tâche 2 - Installer 11.3 sur les autres composants hôtes » sous « Tâches d'installation » du *Guide d'installation de l'hôte physique*. Accédez à la [Table des matières principale](#) pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.
 - Pour un hôte virtuel, suivez les instructions du *Guide d'installation de l'hôte virtuel* dans la section « Tâche 2 - Installer 11.3 sur les autres composants hôtes » sous « Étape 4. Installer RSA NetWitness Platform. »

2. Utilisez le protocole SSH sur l'hôte que vous avez configuré à l'étape 1.

3. Exécutez la chaîne de commande suivante.

```
mkdir -p /etc/pki/nw/nwe-ca
```

Remarque : Vous n'avez pas besoin de modifier les autorisations.

4. Copiez les deux fichiers suivants à partir du serveur de terminal précédemment déployé sur le nouveau/deuxième serveur de terminal :

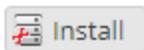
```
/etc/pki/nw/nwe-ca/nwerootca-cert.pem  
/etc/pki/nw/nwe-ca/nwerootca-key.pem
```

5. Installez le terminal sur l'hôte.

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

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

- b. Sélectionnez le nouvel hôte dans la boîte de dialogue **Nouveaux hôtes**, puis cliquez sur **Activer**. La boîte de dialogue **Nouveaux hôtes** se ferme et l'hôte s'affiche dans la vue Hôtes.
- c. Sélectionnez cet hôte dans la vue Hôtes (par exemple, Endpoint Server II), puis cliquez sur



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

- d. Sélectionnez **Terminal** dans **Type d'hôte**, puis cliquez sur **Installer**.

Hôte du serveur NW de secours à chaud

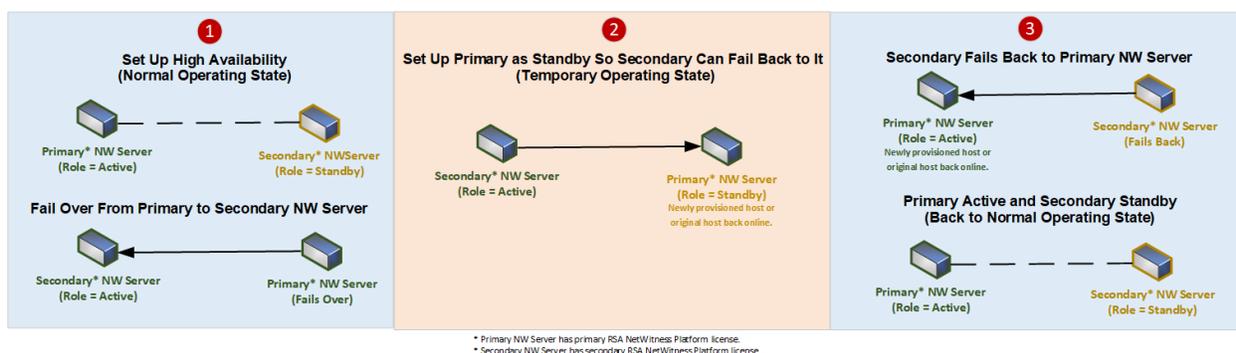
Le serveur NW de secours à chaud duplique les composants et les configurations critiques de votre hôte de serveur NW actif pour accroître la fiabilité.

Un serveur NW secondaire demeure en mode veille, et, lorsqu'il est configuré, reçoit des sauvegardes du serveur NW principal en mode actif, à intervalles réguliers. Si le serveur NW principal échoue (c'est-à-dire, s'il passe en mode hors ligne), la procédure de basculement doit être exécutée, ce qui permet au serveur NW secondaire d'assumer le rôle actif.

Lorsque vous configurez un serveur NW secondaire en tant que serveur de secours à chaud, une défaillance ou un commutateur planifié du serveur NW principal vers le serveur NW secondaire est désigné sous le terme de basculement. Vous effectuez une reprise après incident pour revenir à l'état de fonctionnement normal (à savoir, lorsque le serveur NW principal assure un rôle actif et le serveur NW secondaire un rôle de veille).

Le schéma suivant illustre le processus de basculement et de reprise après incident.

- 1 Configurez le serveur NW secondaire pour le définir en mode de veille (configuration initiale). Il s'agit de l'état de fonctionnement normal.
- 2 Le serveur NW principal bascule vers le serveur NW secondaire. Après le basculement, récupérez le serveur NW principal en ligne et configurez-le en mode de veille. Il s'agit d'un état de fonctionnement temporaire.
- 3 Faites basculer le serveur NW secondaire vers le serveur principal. Le serveur NW principal reprend le rôle actif, tandis que le secondaire reprend le rôle de veille. Il s'agit de l'état de fonctionnement normal.



IMPORTANT : Lors d'un basculement, vous devez attribuer la même adresse IP que le serveur NW principal au serveur NW secondaire afin que celui-ci puisse assumer le rôle actif.

Procédures

Effectuez les tâches suivantes pour configurer un serveur NW secondaire en rôle de veille pour le basculement :

- [Configurez un serveur NW secondaire dans le rôle de veille.](#)

Procédez comme suit lorsque cela est nécessaire pour maintenir la haute disponibilité.

- Basculez le serveur NW principal vers le serveur NW secondaire.
- Rebasculez le serveur NW secondaire vers le serveur NW primaire.

Scénario de basculement planifié

Ce scénario se produit lorsque vous planifiez un basculement (voir **Basculement planifié** à l'étape 3 de la procédure [Basculement du serveur NW principal vers le serveur NW secondaire](#)). Aucune action n'est requise de votre part une fois le processus de basculement terminé.

Scénario de basculement requis sans remplacement de matériel

Ce scénario se produit lorsque le serveur NW principal est défaillant (voir *Basculement requis* à l'étape 3 de la rubrique [Basculement du serveur NW principal vers le serveur NW secondaire](#)), mais que vous êtes en mesure de le restaurer aisément sans créer de nouvelle imagerie (par exemple, le serveur NW actif possède une RAM corrompue ou insuffisante). Vous n'avez pas besoin d'exécuter le `nwsetup-tui`, ni de contacter le support client (<https://community.rsa.com/docs/DOC-1294>) pour rétablir les licences appropriées dans les cas suivants :

1. L'état actif (serveur NW principal) bascule vers le mode de veille (serveur NW secondaire) et l'hôte secondaire assume temporairement le rôle de serveur NW actif.
2. Vous pouvez résoudre le problème du serveur NW principal (par exemple, installer la nouvelle RAM) et effectuer une reprise après incident vers celui-ci à partir de l'hôte secondaire.

Scénario de basculement requis avec remplacement de matériel

Ce scénario se produit lorsque le serveur NW actif échoue intégralement et que le matériel nécessite un remplacement. Par exemple, vous recevez une autorisation de retour marchandises (RMA). Vous devez exécuter la reconfiguration de l'hôte avec le `nwsetup-tui` et contacter le support client (<https://community.rsa.com/docs/doc-1294>) pour rétablir les licences. Si vous choisissez de reconstruire l'hôte de remplacement en veille temporaire (par exemple, jusqu'à ce que la reprise après incident planifiée se produise), vous devez répondre « **Oui** » à l'invite du **Mode de récupération de l'hôte de veille** `nw-setup-tui` durant la configuration de cette veille temporaire pour la reprise après incident (reportez-vous à l'étape 4 de la procédure [Configuration du serveur NW secondaire en rôle de veille](#) afin de comprendre le contexte de cette invite).

Configuration du serveur NW secondaire en rôle de veille

1. Avant d'installer un hôte de serveur NW secondaire pour le rôle de veille, vérifiez les points suivants :

- a. Le serveur NW principal exécute la version 11.3.
- b. Tous vos hôtes de composants exécutent la version 11.3

Si vous :

- installez la plate-forme Netwitness 11.3, suivez les instructions du *Guide d'installation des hôtes physiques RSA NetWitness Platform pour la version 11.3* ou du *Guide d'installation des hôtes virtuels RSA Netwitness Platform pour la version 11.3* ;
- effectuez une mise à niveau de la version 10.6. x vers la version 11.3, suivez les instructions du *Guide de mise à niveau des hôtes physiques RSA NetWitness Platform pour la version 10.6.6. x vers 11.3* ou le *Guide d'installation des hôtes virtuels RSA Netwitness Platform pour la version 11.3* ;
- effectuez une mise à jour depuis la version 11.x vers la version 11.3, suivez les instructions contenues dans le *Guide de la mise à jour de RSA NetWitness Platform depuis la version 11.x vers 11.3*.

Accédez à la [Table des matières principale](#) pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

2. Créez une image de base sur le serveur NW secondaire :

- a. Rattachez le média (ISO) à l'hôte.

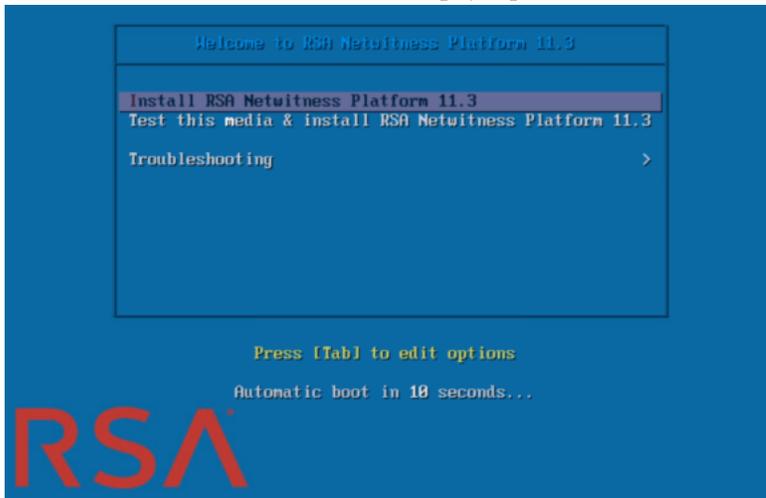
Reportez-vous aux *Instructions de clé de version pour RSA NetWitness Platform* pour plus d'informations.

- Installations de l'hyperviseur, utilisez l'image ISO.
- Support physique : utilisez le fichier ISO pour créer un support de lecteur Flash amorçable **Etcher**® ou un autre outil d'imagerie adapté à la gravure d'un système de fichiers Linux sur le lecteur USB. Pour plus d'informations sur la création d'une clé à partir du fichier ISO, reportez-vous à *RSA NetWitness® Platform Instructions de clé*. Le graveur est disponible à l'adresse: <https://etcher.io>.
- Installations de l'iDRAC - le type de média virtuel est :
 - **Un lecteur de disquette virtuel** pour des disques flash mappés.
 - **Un CD virtuel** pour des périphériques de médias optiques mappés ou du fichier ISO.

- b. Connectez-vous à l'hôte et redémarrez-le.

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

- c. Sélectionnez **F11** (dans le menu de démarrage) pendant le redémarrage pour sélectionner un périphérique de démarrage et démarrer le média connecté.
Après vérification du système lors du démarrage, le menu d'installation suivant, **Bienvenue dans la RSA NetWitness Platform 11.3** s'affiche. Les graphiques du menu s'affichent différemment si vous utilisez un média Flash USB physique.



- d. Sélectionnez **Installer RSA NetWitness Platform 11.3** (sélection par défaut), puis appuyez sur **Entrée**.

Le programme d'installation s'exécute et s'arrête au message **Saisir (y/Y) pour effacer les disques**, vous invitant à effectuer le formatage des disques.

```
-----  
Clear virtual drive configuration on RAID controller: 1 ?  
HBA: PERC H700 Integrated #UD: 2 #PD: 4  
For Upgrades either ignore or answer No to this prompt  
Recommended for new hardware or re-purposing **Warning**  
data on all configured drives will be discarded, this  
includes all internal, HBA attached SATA/SCSI storage  
Enter (y/Y) to clear drives, defaults to No in 30 seconds  
-----  
? _
```

- e. Saisissez **Y** pour continuer.

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

```

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

Adapter 0: Configuration is Cleared.

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

Adapter 0: Created VD 0

Adapter 0: Configured the Adapter!!

Exit Code: 0x00

Adapter 0: Created VD 1

Adapter 0: Configured the Adapter!!

Exit Code: 0x00

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

- f. Appuyez sur **Entrée** pour redémarrer l'hôte.

Le programme d'installation vous demande à nouveau d'effacer les disques.

```

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

- g. Saisissez **N** car vous avez déjà effacé les disques.

Le message **Saisir Q (Quitter) ou R (Réinstaller)** s'affiche.

```

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

- h. Saisissez **R** pour installer l'image de base.

Le programme d'installation affiche les composants à mesure qu'ils sont installés, ce qui varie en fonction de l'appliance, puis redémarre.

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

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

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

- i. Connectez-vous à l'hôte avec les informations d'identification `root` .
2. Exécutez la commande `nwsetup-tui`.

Remarque : 1.) Lorsque vous parcourez les messages du programme d'installation, utilisez les touches directionnelles Haut et Bas pour naviguer entre les champs, utilisez la touche de tabulation pour naviguer d'une commande à l'autre (par exemple `<Oui>`, `<Non>`, `<OK>`, et `<Annuler>`. Appuyez sur **Entrée** pour enregistrer votre réponse et passer au message suivant.

2.) Le programme d'installation adopte le modèle de couleurs du poste de travail ou de la console que vous utilisez pour accéder à l'hôte.

3.) Pendant le programme d'installation, lorsque vous êtes invité à configurer le réseau de l'hôte, veillez à spécifier la même configuration de réseau que celle utilisée pour l'installation d'origine de 11.x sur cet hôte (elles doivent être identiques).

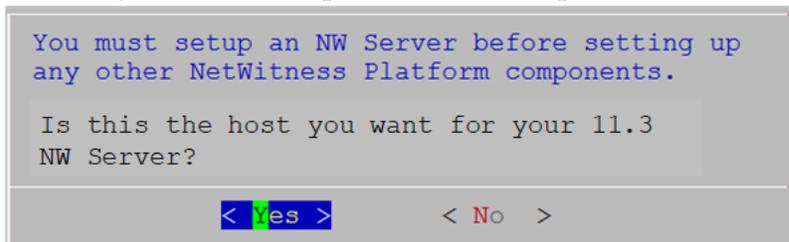
Cette opération démarre le programme d'installation `nwsetup-tui` et les conditions générales d'utilisation s'affichent.

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

92%

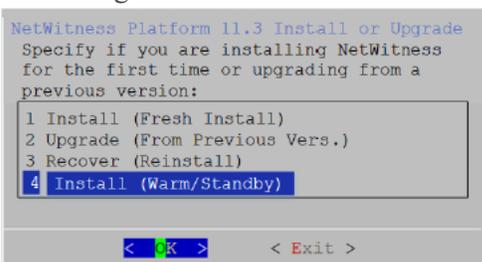
`<Accept >``<Decline>`

3. Naviguez jusqu'à **Accepter** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**. Le message **Est-ce l'hôte que vous souhaitez pour votre serveur NW 11.3 ?** s'affiche.

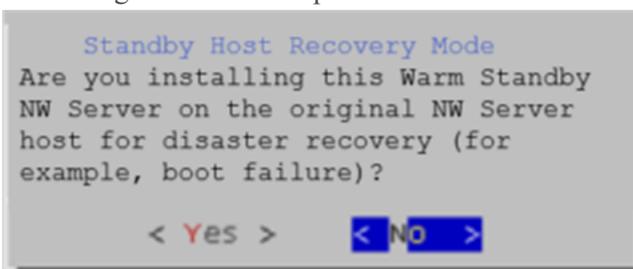


Votre réponse à cette invite identifie un hôte comme principal ou secondaire lors d'une nouvelle installation (et la réponse sélectionnée reste constante quel que soit le rôle actuel ou futur, c'est-à-dire actif ou en veille de l'hôte).

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



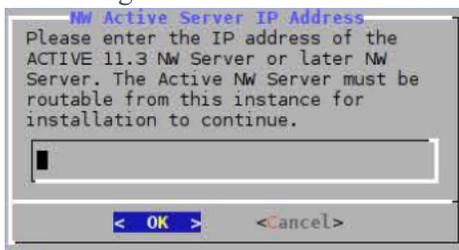
5. Accédez à **4 Installer (secours à chaud)** et appuyez sur **Entrée**. Le message **Mode de récupération de l'hôte de veille** s'affiche.



6. Utilisez la tabulation jusqu'aux options suivantes :

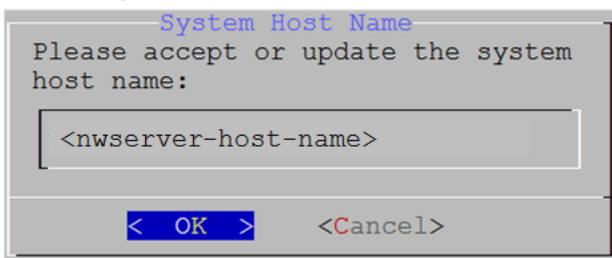
- **Non** et appuyez sur **Entrée** pour configurer un serveur NW secondaire avec le rôle de veille (scénario le plus courant).
- **Oui**, puis appuyez sur **Entrée** pour configurer un hôte précédemment utilisé en tant que serveur NW principal avec le rôle de veille afin de pouvoir exécuter un basculement et un retour arrière (scénario plus rare).

Le message Adresse IP du serveur NW Active s'affiche.



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

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



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

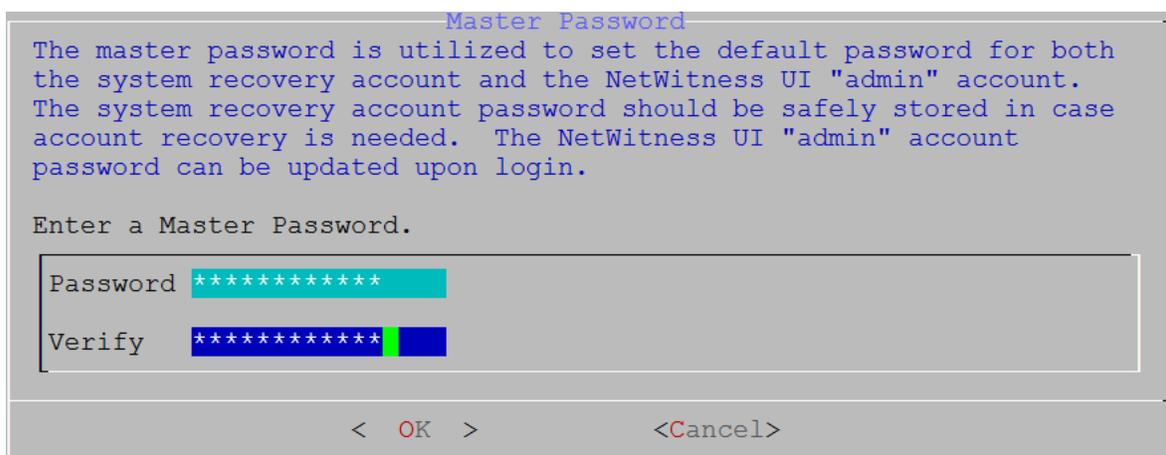
8. Appuyez sur **Entrée** si vous souhaitez conserver ce nom. Dans le cas contraire, naviguez jusqu'à **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** pour modifier le nom de l'hôte. Le message **Mot de passe maître** s'affiche.

Remarque : Vous devez utiliser les mêmes informations d'identification principales et de déploiement d'administrateur pour l'hôte du serveur NW de secours à chaud que celles que vous avez utilisées pour l'hôte du serveur NW actif.

Les caractères suivants sont pris en charge pour le mot de passe maître et le mot de passe de déploiement :

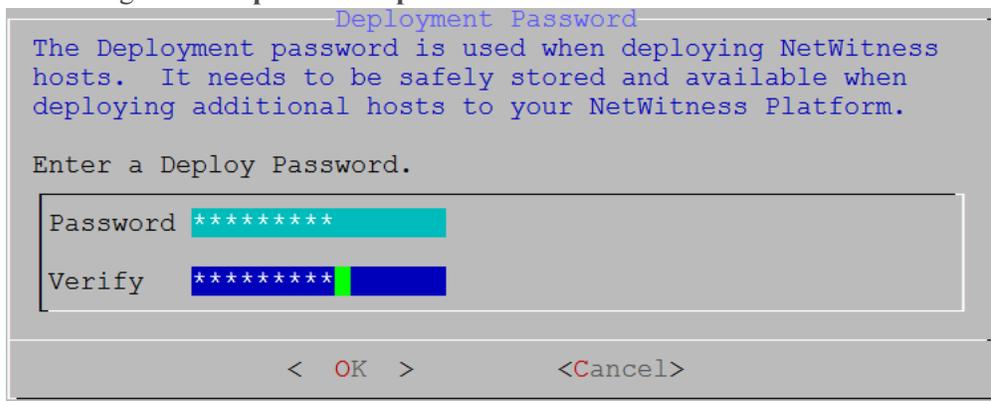
- Symboles : ! @ # % ^ +
- Caractères minuscules : a-z
- Caractères majuscules : A-Z

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



9. 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**.

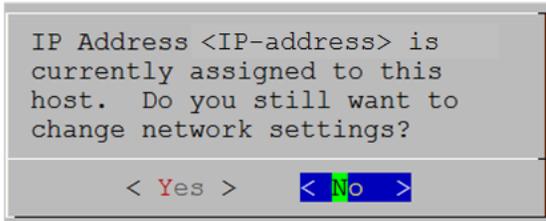
Le message **Mot de passe de déploiement** s'affiche.



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

Une des invites conditionnelles suivantes s'affiche.

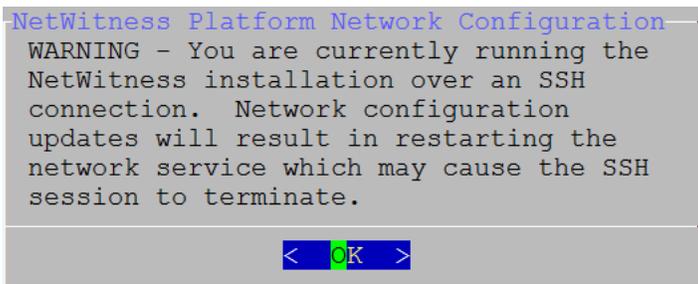
- Si le programme d'installation détecte une adresse IP valide pour cet hôte, le message suivant s'affiche.



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

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

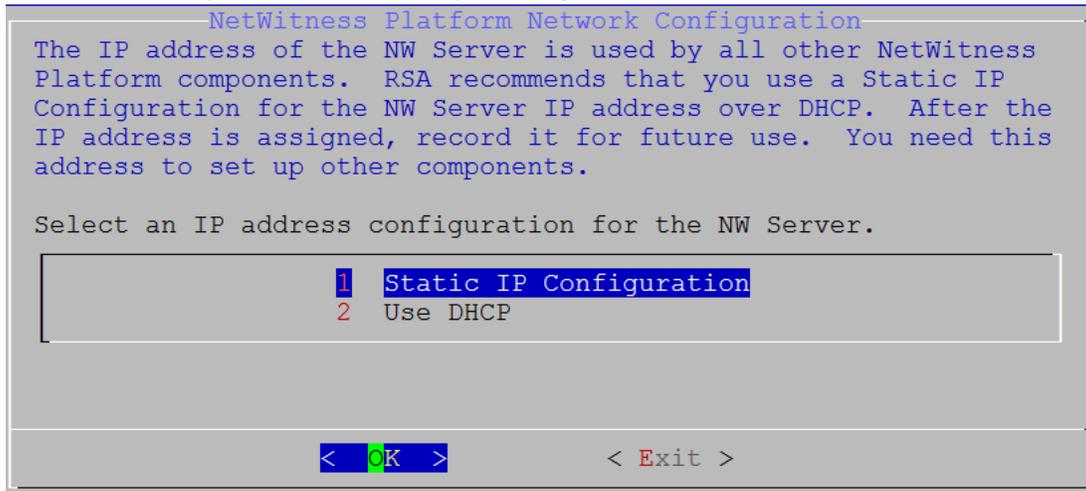
Remarque : Si vous vous connectez directement à partir de la console hôte, l'avertissement suivant ne s'affichera pas.



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

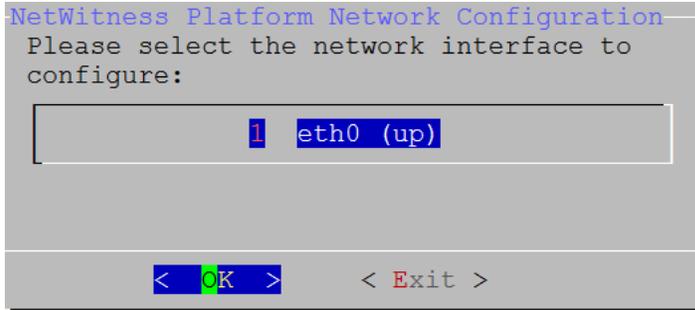
- Si le programme d'installation a détecté une configuration IP et que vous avez choisi de l'utiliser, le message **Mettre à jour le référentiel** s'affiche. Accédez à l'étape 12 à et terminez l'installation.

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

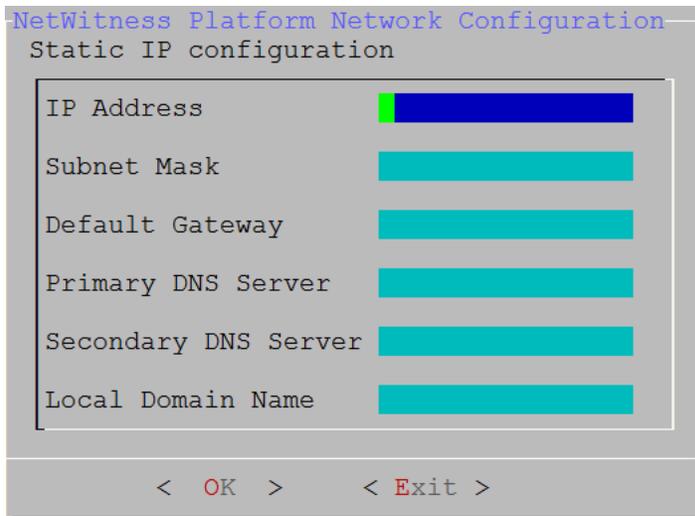


11. Naviguez jusqu'à **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** pour utiliser l'adresse IP statique.
Si vous souhaitez utiliser **DHCP**, utilisez la touche directionnelle Bas jusqu'à 2 Utiliser DHCP, puis appuyez sur **Entrée**.

Le message **Configuration de réseau** s'affiche.



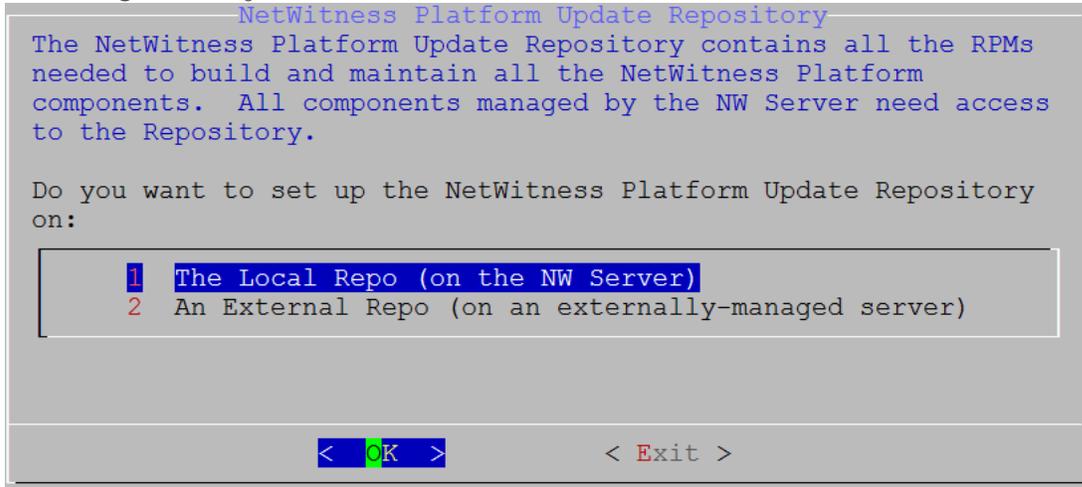
12. Utilisez la touche directionnelle Bas jusqu'à l'interface réseau que vous souhaitez, puis naviguez jusqu'à **OK** à l'aide de la touche de tabulation et appuyez sur **Entrée**. Si vous ne souhaitez pas continuer, naviguez jusqu'à **Quitter** à l'aide de la touche de tabulation. Le message **Configuration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



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

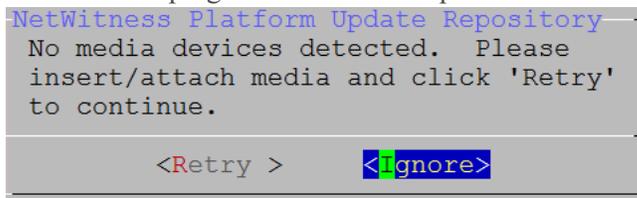
Attention : Si vous sélectionnez le **serveur DNS**, assurez-vous que le serveur DNS est correct et que l'hôte peut y accéder avant de poursuivre l'installation.

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

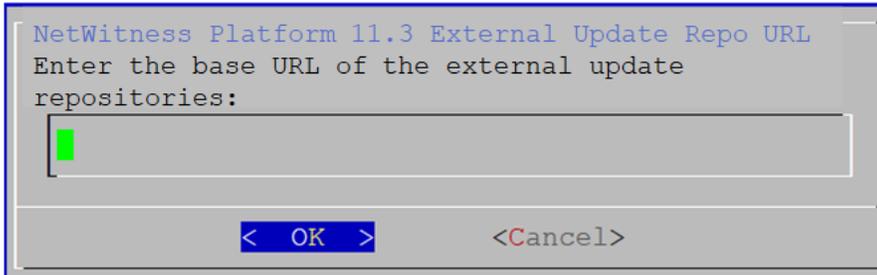


14. Appuyez sur **Entrée** pour choisir le **référentiel local** sur le serveur NW. Si vous souhaitez utiliser un référentiel externe, utilisez la touche directionnelle Bas pour naviguer jusqu'au **Référentiel externe**, naviguez jusqu'à **OK** à l'aide de la touche de tabulation et appuyez sur **Entrée**.

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

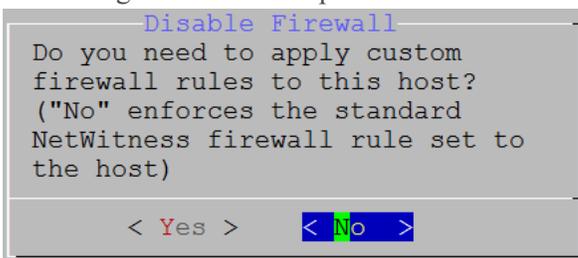


- Si vous sélectionnez **2 Un référentiel externe (sur un serveur géré en externe)**, l'interface utilisateur vous invite à saisir une URL. Les référentiels vous donnent accès aux mises à jour RSA et CentOS. Reportez-vous à la section [Annexe B. Créer un référentiel externe](#) pour obtenir des instructions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

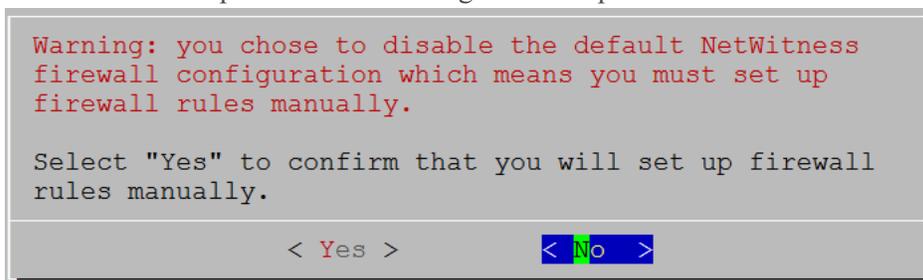


Saisissez l'URL de base du référentiel externe NetWitness Platform, puis cliquez sur **OK**. Le message **Démarrer l'installation** s'affiche.

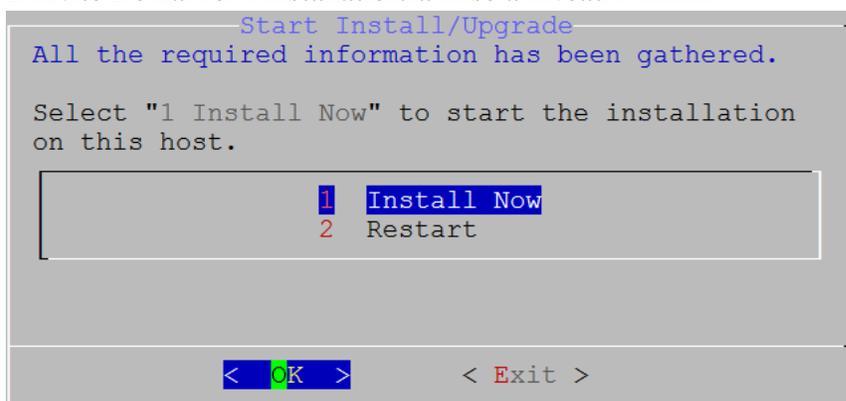
Voir « Définir un référentiel externe avec les mises à jour RSA et de système d'exploitation » sous « Procédures liées aux hôtes et services » dans le *Guide de mise en route des hôtes et des services RSA NetWitness Platform* pour obtenir des instructions. Accédez à la [Table des matières principale](#)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



15. Naviguez vers l'onglet **Non** (par défaut) à l'aide de la touche de tabulation, puis appuyez sur **Entrée** pour utiliser la configuration de pare-feu standard. Naviguez vers l'onglet **Oui** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** pour désactiver la configuration de pare-feu standard. Si vous sélectionnez **Oui**, confirmez votre sélection (sélectionnez **Oui** à nouveau) ou bien sélectionnez **Non** pour utiliser la configuration du pare-feu standard.



L'invite **Démarrer l'installation/la mise à niveau** s'affiche.



16. Appuyez sur **Entrée** pour installer la version 11.3 sur le serveur NW. Lorsque le message **Installation terminée** s'affiche, c'est que vous avez installé le serveur NW 11.3 sur cet hôte.

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

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

17. Vous disposez d'une licence pour le serveur NW secondaire.
 - a. Connectez-vous à l'interface utilisateur du serveur NW secondaire, cliquez sur **ADMIN > Système > Informations** et notez l'identifiant de la **Licence du serveur** sous **Informations sur la version**.
 - b. Utilisez le protocole SSH sur le serveur NW principal.
 - c. Modifiez le fichier `/opt/netwitness/flexnet/ls/local-configuration.yaml` et ajoutez le back up `hostid` (à savoir, l'**ID de serveur de licences**).
Il s'agit d'un exemple de la section du fichier `local-configuration.yaml` avant d'ajouter l'**ID de serveur de licences**.
Hostid of the backup server, if in fail over configuration.
#backup-hostid:
Il s'agit d'un exemple de la section du fichier `local-configuration.yaml` après l'ajout de l'adresse MAC (par exemple, `000c2918c80d`) de l'hôte du serveur NW de secours à chaud.
Hostid of the backup server, if in fail over configuration.
backup-hostid: "000c2918c80d"

- d. Redémarrez le service fneserver.


```
systemctl restart flexnetls-RSALM
```
 - e. (Conditionnel) Si votre déploiement de la plate-forme NetWitness n'est pas autorisé à accéder à Internet (Air Gap), vous devez :
 - i. Télécharger la demande de fonctionnalité à partir de l'interface utilisateur de la plate-forme NetWitness.
 - ii. Télécharger la demande auprès de FNO.
 - iii. Télécharger la réponse de FNO vers l'interface utilisateur de la plate-forme NetWitness.
18. Planifier la sauvegarde du serveur NW principal et copier ces données sauvegardées sur le serveur NW secondaire.
- a. Utiliser le protocole SSH sur le serveur NW principal.
 - b. Exécutez les commandes suivantes.


```
/opt/rsa/saTools/bin/schedule-standby-admin-data-sync -di <warm-standby-admin-server-ip>
```

Cela permet de sauvegarder les données du serveur NW principal et de copier le fichier d'archive de sauvegarde sur le serveur NW secondaire quotidiennement en vue d'une future utilisation de retour arrière. Cela permet également de planifier l'exécution quotidienne des sauvegardes et des copies. Vous pouvez afficher l'aide du script `schedule-standby-admin-data-sync` avec la chaîne de commande suivante.

```
/opt/rsa/saTools/bin/schedule-standby-admin-data-sync --help
```

Vous avez ainsi la possibilité de consulter l'aide suivante qui vous permettra de personnaliser la sauvegarde des données de l'hôte (par exemple, la fréquence de sauvegarde).

```
Schedule Data Synch between AdminServer and Standby AdminServer
Script also executes a synchronization each time.
```

Usage:

```
schedule-standby-admin-data-sync command [options]
```

Commands:

<code>-h, --help</code>	Display Help
<code>-d, --daily</code>	Schedule daily data synchronization
<code>-w, --weekly</code>	Schedule weekly data synchronization
<code>-c, --custom <crontab formatted></code>	Schedule custom data synchronization
<code>-</code>	i.e. to schedule for midnight on 1st and 10th of the month: '0 0 1,10 * *'
<code>-i, --standby-ip <ip address></code>	IP address of standby Admin Server
<code>-v, --verbose</code>	Enable verbose output

Basculement du serveur NW principal vers le serveur NW secondaire

Au départ, le serveur NW principal bascule vers le serveur NW secondaire. Un basculement subséquent, à savoir du serveur NW secondaire vers le serveur NW principal, appelé « retour arrière ». Effectuez la procédure suivante pour effectuer un basculement à partir du serveur NW principal vers le serveur NW secondaire.

1. Utilisez le protocole SSH sur le serveur NW secondaire.
2. Exécutez le script `nw-failover` avec les arguments appropriés. Par exemple :

```
nw-failover --make-active --ip-address <active-nw-server-host-ip> --name <primary-nw-server-hostname>
```

Une fois le script exécuté, le message suivant s'affiche.

```
*** Please update network ip and reboot host to complete the fail over process ***
```
3. Mettez à jour la configuration réseau CentOS pour permuter les adresses IP.
 - **Le basculement planifié** sur le serveur NW principal n'a pas échoué :
 - a. Utilisez le protocole SSH sur le serveur NW principal.
 - b. Attribuez une adresse IP inutilisée au serveur NW principal.
 - c. Exécutez le script de basculement avec les arguments appropriés pour attribuer le rôle de veille au serveur NW principal. Par exemple :

```
nw-failover --make-standby --ip-address <unused-ip-or-previous-standby-ip> --name <previous-standby-nw-server-hostname>
```
 - d. Arrêtez le serveur NW principal.
 - e. Utilisez le protocole SSH sur le serveur NW secondaire.
 - f. Attribuez l'adresse IP du serveur NW principal que vous avez enregistré sur le serveur NW secondaire.
 - **Basculement requis** - le serveur NW principal a échoué :
 - a. Utilisez le protocole SSH sur le serveur NW secondaire.
 - b. Attribuez l'adresse IP du serveur NW principal au serveur NW secondaire.

Remarque : En cas de défaillance majeure, il peut être nécessaire de provisionner un nouvel hôte ou de créer une nouvelle image du serveur NW principal, puis d'exécuter la procédure [Configuration du serveur NW secondaire en rôle de veille](#) pour que cet hôte crée un nouveau serveur NW principal afin que vous puissiez effectuer un retour arrière vers celui-ci.

4. Redémarrez l'hôte.

5. Assurez-vous que le basculement est correctement configuré.
 - a. Ouvrez une session SSH sur le serveur NW en veille.
 - b. Assurez-vous que le serveur NW actif :
 - i. Peut résoudre son UUID (identifiant universel unique).

```
source /usr/lib/netwitness/bootstrap/resources/nwcommon
2>/dev/null/dev/null
> nslookup $(getNodeID)
nslookup peut renvoyer l'adresse IP du serveur NW actif actuel.
```
 - ii. Correspond à la même adresse IP que celle qui a été résolue à l'étape précédente.

Retour arrière du serveur NW secondaire vers le serveur NW principal

Après un basculement à partir du serveur NW principal vers le serveur NW secondaire, vous devez effectuer un retour arrière vers la configuration initiale du serveur NW principal dans le rôle actif et le serveur NW secondaire dans le rôle de veille.

Vous devrez essentiellement suivre les mêmes étapes que celles décrites dans la section [Basculement du serveur NW principal vers le serveur NW secondaire](#) pour effectuer un retour arrière vers la configuration d'origine (à savoir, le serveur NW principal sera actif et le serveur NW secondaire sera en veille). La différence réside dans le fait que vous devez désormais effectuer le basculement du serveur NW secondaire vers le serveur NW principal.

Architecture réseau et ports

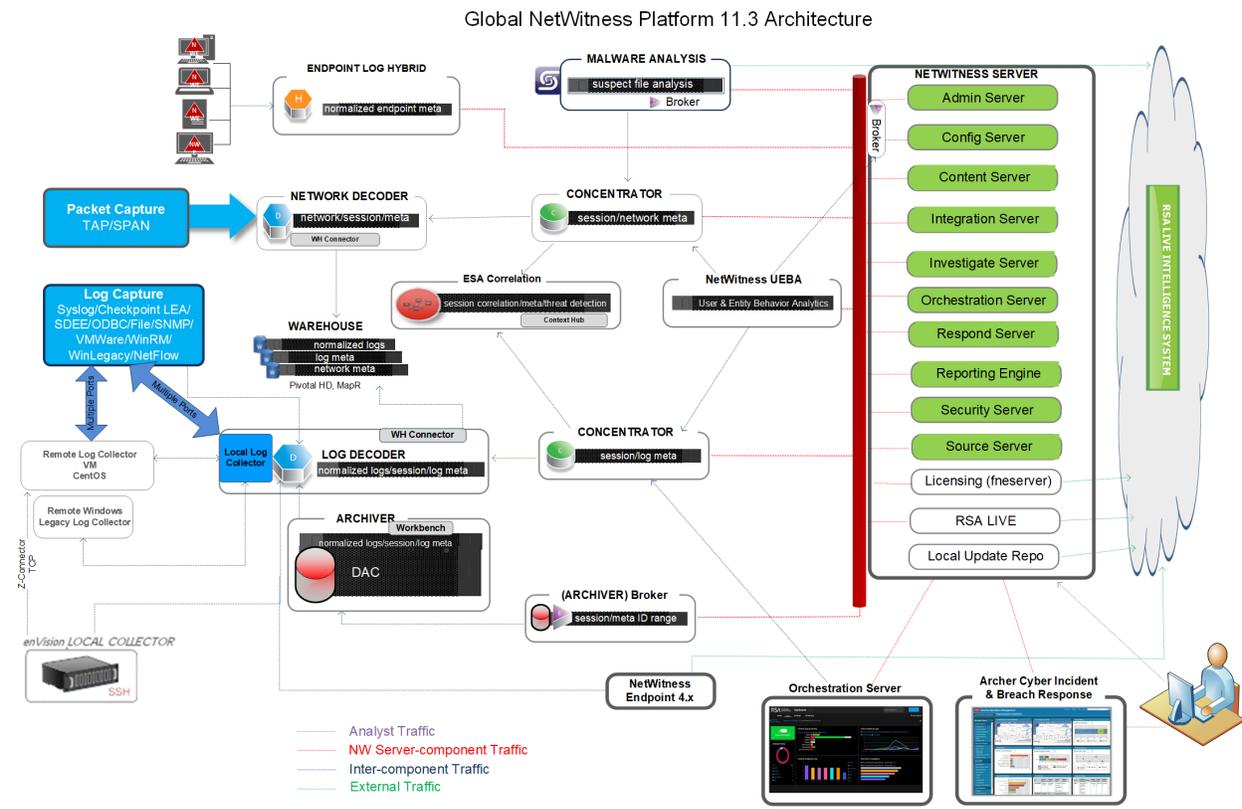
Reportez-vous au schéma et au tableau des ports suivants pour veiller à ce que tous les ports concernés soient ouverts et que les composants de votre déploiement NetWitness Platform puissent communiquer les uns avec les autres.

Reportez-vous à la section [Architecture de NetWitness Endpoint](#) à la fin de cette rubrique pour découvrir chaque schéma de l'architecture Endpoint.

Schéma de l'architecture réseau NetWitness Platform

Le schéma suivant illustre l'architecture réseau NetWitness Platform, y compris tous ses produits composants.

Remarque : Les hôtes de base NetWitness Platform doivent être en mesure de communiquer avec Serveur NetWitness (serveur primaire dans un déploiement avec plusieurs serveurs) via le port UDP 123 pour la synchronisation horaire Network Time Protocol (NTP).



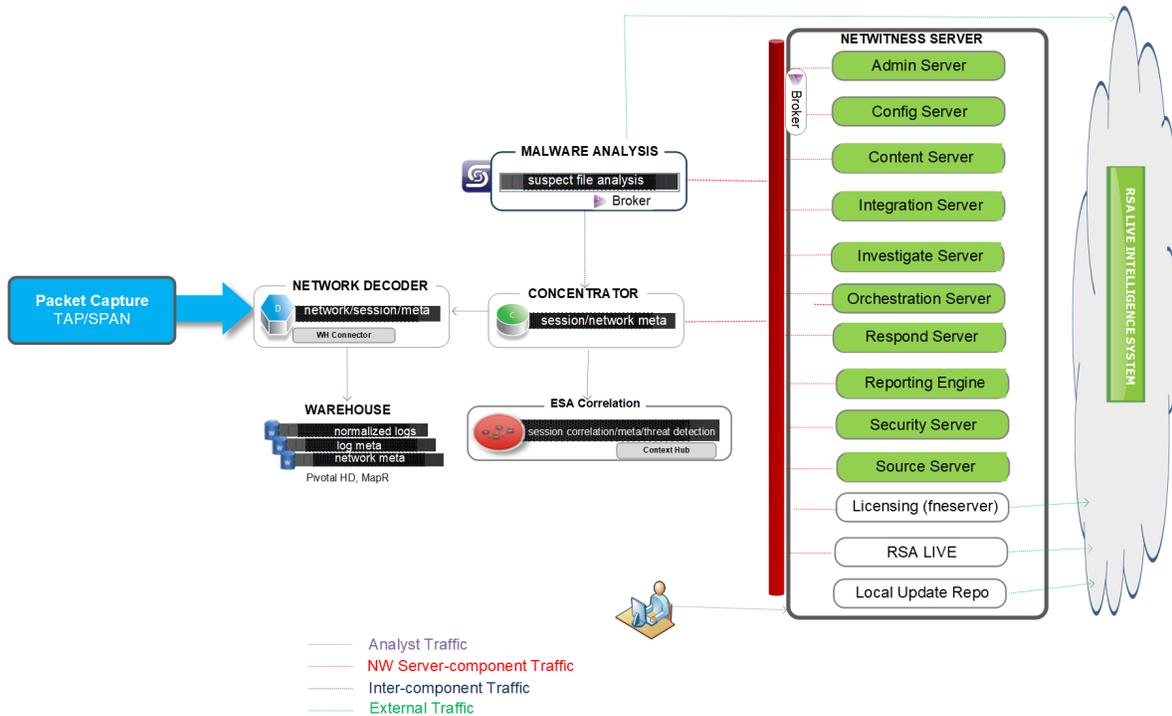
Note:
 Admin, Config, Content, Integration, Investigate, Orchestration, Respond, Security, and Source services come online automatically when you deploy the NW Server. The core service hosts use the Local Update Repository on the NetWitness Server to get the rpm packages (that is, version updates).
 NW Endpoint needs to access <https://cms.netwitness.com> to download Live Feeds.
 RSA recommends that you use the Broker at the top of your deployment hierarchy for UEBA data source.
 See *RSA NetWitness Platform Cloud Behavioral Analytics Gateway Configuration Guide* for information on the Cloud Gateway service.



Schéma de l'architecture réseau NetWitness (paquets)

Les schémas suivants illustrent l'architecture réseau NetWitness Endpoint Insights (paquets)

NetWitness Network 11.3 Architecture



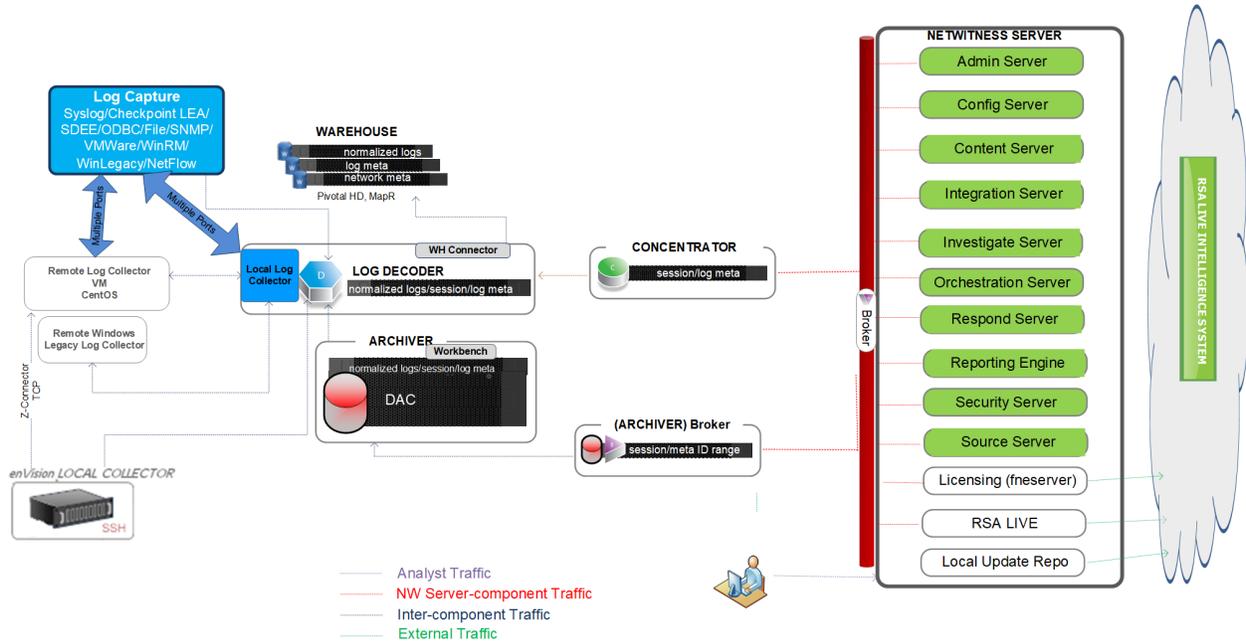
Notes:

Admin, Config, Content, Integration, Investigate, Orchestration, Respond, Security, and Source services come online automatically when you deploy the NW Server. The core service hosts use the Local Update Repository on the NetWitness Server to get the rpm packages (that is, version updates).

Schéma de l'architecture réseau de NetWitness Logs

Les schémas suivants illustrent l'architecture réseau de NetWitness Logs

NetWitness Logs 11.3 Architecture



Note: Admin, Config, Content, Integration, Investigate, Orchestration, Respond, Security, and Source services come online automatically when you deploy the NW Server. The core service hosts use the Local Update Repository on the NetWitness Server to get the rpm packages (that is, version updates).

Liste complète des hôtes et des ports de service et iDRAC NetWitness Platform

Remarque : Pour les ports utilisés dans la collecte des événements via NetWitness Logs, reportez-vous à la section « Les bases » du *Guide de déploiement de RSA NetWitness Suite Log Collection*. Accédez à la [Table des matières principale](#) pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.

Cette section contient les spécifications de port pour les hôtes suivants.

Hôte de serveur NW	Hôte Log Collector
Hôte Archiver	Hôte Log Decoder
Hôte Broker	Hôte Log Hybrid
Hôte Concentrator	Hôte Malware
Hôte Endpoint Log Hybrid	Hôte de décodeur réseau
Hôte Event Stream Analysis	Hôte réseau hybride
Ports iDRAC	Hôte UEBA

Hôte de serveur NW

Hôte source	Hôte de destination	Ports de destination	Commentaires
Station de travail Admin	Serveur NW	TCP 443, 80	nginx - IU NetWitness
Station de travail de l'administrateur	Serveur NW	TCP 15671	Interface utilisateur de gestion RabbitMQ
Station de travail Admin	Serveur NW	TCP 22	SSH
Hôtes NW	Serveur NW	TCP 53 UDP 53	DNS
Hôtes NW	Serveur NW	TCP 15671	Interface utilisateur de gestion RabbitMQ
Hôtes NW	Serveur NW	TCP 4505, 4506	Ports Salt Master
Hôtes NW	Serveur NW	TCP 443	Référentiel de mise à jour RSA
Hôtes NW	Serveur NW	TCP 5671	RabbitMQ-amqp
Hôtes NW	Serveur NW	UDP 123	NTP
Hôtes NW	Serveur NW	TCP 27017	MongoDB
Serveur NW	cloud.netwitness.com	TCP 443	Live
Serveur NW	cms.netwitness.com	TCP 443	Live
Serveur NW	smcupdate.emc.com	TCP 443	Live
Serveur NW	Serveur NFS	TCP 111, 2049, UDP 111, 2049	Installations iDRAC
Serveur NW	Hôtes NW	UDP 123	NTP
Serveur NW	NW Endpoint	TCP 443, 9443	Pour les intégrations NW Endpoint 4.x

Hôte Archiver

Hôte source	Hôte de destination	Ports de destination	Commentaires
Station de travail Admin	Archiver	TCP 15671	Interface utilisateur de gestion RabbitMQ
Archiver	Serveur NW	TCP 15671	Interface utilisateur de gestion RabbitMQ
Archiver	Serveur NW	TCP 443	Référentiel de mise à jour RSA
Station de travail Admin	Archiver	TCP 22	SSH
Serveur NW	Archiver	TCP 56008 (SSL), 50108 (REST)	Ports d'application Archiver
Serveur NW	Archiver	TCP 56006 (SSL), 50106 (REST)	Ports d'appliance NetWitness
Serveur NW	Archiver	TCP 5671	Bus de messages RabbitMQ (AMQPS) pour tous les hôtes NW.
Serveur NW	Archiver	TCP 514, 6514, 56007 (SSL), 50107 (REST), UDP 514	Ports d'application Workbench
Archiver	Serveur NFS	TCP 111 2049 UDP 111 2049	Installations iDRAC

Hôte Broker

Hôte source	Hôte de destination	Ports de destination	Commentaires
Station de travail Admin	Broker	TCP 15671	Interface utilisateur de gestion RabbitMQ
Broker	Concentrator	TCP 56005	Port d'application Concentrator
Broker	Serveur NW	TCP 15671	Interface utilisateur de gestion RabbitMQ
Broker	Serveur NW	TCP 443	Référentiel de mise à jour RSA
Station de travail Admin	Broker	TCP 22	SSH
Serveur NW	Broker	TCP 56003 (SSL), 50103 (REST)	Ports d'application Broker
Serveur NW	Broker	TCP 56006 (SSL), 50106 (REST)	Ports d'appliance NetWitness
Serveur NW	Broker	TCP 5671	Bus de messages RabbitMQ (AMQPS) pour tous les hôtes NW.
Broker	Serveur NW	TCP 111 2049 UDP 111 2049	Installations iDRAC
Endpoint Broker	Serveur NW	TCP 443	Référentiel de mise à jour RSA

Hôte Concentrator

Hôte source	Hôte de destination	Ports de destination	Commentaires
Station de travail Admin	Concentrator	TCP 15671	Interface utilisateur de gestion RabbitMQ
Concentrator	Log Decoder	TCP 56002	Port d'application Concentrator
Concentrator	Décodeur réseau	TCP 56004	Port d'application Concentrator
Concentrator	Serveur NW	TCP 15671	Interface utilisateur de gestion RabbitMQ
Concentrator	Serveur NW	TCP 443	Référentiel de mise à jour RSA
Station de travail Admin	Concentrator	TCP 22	SSH
Serveur NW	Concentrator	TCP 56005 (SSL), 50105 (REST)	Ports d'application Concentrator
Malware	Concentrator	TCP 56005 (SSL)	Malware
Serveur NW	Concentrator	TCP 56006 (SSL), 50106 (REST)	Ports d'appliance NetWitness
Serveur NW	Concentrator	TCP 5671	Bus de messages RabbitMQ (AMQPS) pour tous les hôtes NW.
Concentrator	Serveur NFS	TCP 111 2049 UDP 111 2049	Installations iDRAC

Endpoint Log Hybrid

Hôte source	Hôte de destination	Ports de destination	Commentaires
Agents Endpoint	Endpoint Log Hybrid	TCP 443 UDP 444	NGINX HTTPS NGINX UDP. Si le port UDP 444 n'est pas acceptable dans votre environnement , reportez-vous à la section Comment modifier le port UDP pour Endpoint Log Hybrid.
Agents Endpoint	Log Decoder ou Virtual Log Collector	TCP 514 (Syslog) UDP 514 (Syslog) TLS 6514	Windows Log Collection
Endpoint Log Hybrid	Log Decoder (externe)	TCP 50102 (REST) 56202 (Protobuf SSL) 50202 (Protobuf)	Pour transférer les métadonnées vers un Log Decoder externe
Endpoint Log Hybrid	Serveur NW	TCP 443	Référentiel de mise à jour RSA
Serveur NW	Endpoint Log Hybrid	TCP 7050	Trafic Web de l'interface utilisateur
Endpoint Log Hybrid	Serveur NW	TCP 5671	Bus de messages
Endpoint Log Hybrid	Serveur NW	TCP 27017	MongoDB
Serveur NW	Endpoint Log Hybrid	TCP 7054	Trafic Web de l'interface utilisateur
Serveur NW	Serveur NFS	TCP 111, 2049 UDP 111, 2049	Installations iDRAC

Hôte Event Stream Analysis (ESA)

Hôte source	Hôte de destination	Ports de destination	Commentaires
Station de travail Admin	ESA	TCP 15671	Interface utilisateur de gestion RabbitMQ
ESA primaire et secondaire	Serveur NW	TCP 15671	Interface utilisateur de gestion RabbitMQ
ESA primaire et secondaire	Serveur NW	TCP 443	Référentiel de mise à jour RSA
Station de travail Admin	ESA	TCP 22	SSH
Serveur NW, ESA secondaire	ESA primaire	TCP 27017	MongoDB
Serveur NW	ESA primaire	TCP 7005	Port de lancement Context Hub - (ESA primaire)
Serveur NW	ESA	TCP 50030 (SSL)	Port d'application ESA
Serveur NW	ESA	TCP 50035 (SSL)	Port d'application ESA
Serveur NW	ESA	TCP 50036 (SSL)	Port d'application ESA
Serveur NW	ESA	TCP 5671	Bus de messages RabbitMQ (AMQPS) pour tous les hôtes NW.
ESA primaire et secondaire	cms.netwitness.com	TCP 443	Live
ESA primaire et secondaire	Serveur NFS	TCP 111 2049 UDP 111 2049	Installations iDRAC
ESA primaire et secondaire	Active Directory	636 (SSL)/389 (Non SSL)	
Serveur NW	ESA	80 (HTTP)/ 443 (HTTPS)(REST)	
ESA primaire	Archer	443 (SSL)/80 (Non SSL)	
ESA primaire	ESA primaire	TCP 7007	Port de lancement

Ports iDRAC

Port	Fonction	Commentaires
22*	SSH	Port par défaut, configurable par l'intermédiaire duquel iDRAC écoute les connexions
443*	HTTP	Port par défaut, configurable par l'intermédiaire duquel iDRAC écoute les connexions
5 900*	Redirection du clavier et de la souris de la console virtuelle, médias virtuels, dossiers virtuels et partage de fichiers à distance.	Port par défaut, configurable par l'intermédiaire duquel iDRAC écoute les connexions
111, 2049	TCP	Hôtes NetWitness Platform vers le serveur NFS
111, 2049	UDP	Hôtes NetWitness Platform vers le serveur NFS

Hôte Log Collector

Hôte source	Hôte de destination	Ports de destination	Commentaires
Station de travail Admin	Log Collector	TCP 15671	Interface utilisateur de gestion RabbitMQ
Log Collector	Serveur NW	TCP 15671	Interface utilisateur de gestion RabbitMQ
Log Collector	Serveur NW	TCP 443	Référentiel de mise à jour RSA
Station de travail Admin	Log Collector	TCP 22	SSH
Log Collector	Sources d'événements de Log	Se référer au <i>Guide de configuration de Log Collection</i> . Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.	
Sources d'événements de Log	Log Collector	TCP 514 (Syslog) UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)"	Ports de Log Collection
Source d'événements de Log	Log Collector	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Ports de Log Collection FTP/S
Serveur NW	Log Collector	TCP 56001 (SSL), 50101 (REST)	Ports d'application de Log Collector
Serveur NW	Log Collector	TCP 56006 (SSL), 50106 (REST)	Ports d'appliance NetWitness
Serveur NW	Log Collector	TCP 5671	Bus de messages RabbitMQ (AMQPS) pour tous les hôtes NW.
Log Collector	Serveur NFS	TCP 111 2049 UDP 111 2049	Installations iDRAC
Log Collector	Virtuel Log Collector	TCP 5671	En mode Pull
Virtuel Log Collector	Log Collector	TCP 5671	En mode Push

Hôte de Log Decoder

Hôte source	Hôte de destination	Ports de destination	Commentaires
Station de travail Admin	Log Decoder	TCP 15671	Interface utilisateur de gestion RabbitMQ
Log Decoder	Serveur NW	TCP 443	Référentiel de mise à jour RSA
Station de travail Admin	Log Decoder	TCP 22	SSH
Log Decoder	Source d'événements de Log	Se référer au <i>Guide de configuration de Log Collection</i> . Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.	
Sources d'événements de Log	Log Decoder	TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)	Ports de Log Collection
Sources d'événements de Log	Log Decoder	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Ports de Log Collection FTP/S
Serveur NW	Log Decoder	TCP 56001 (SSL), 50101 (REST)	Ports d'application de Log Collector
Serveur NW	Log Decoder	TCP 56002 (SSL), 56202 (Endpoint), 50102 (REST)	Ports d'application Log Decoder
Serveur NW	Log Decoder	TCP 56006 (SSL), 50106 (REST)	Ports d'appliance NetWitness
Serveur NW	Log Decoder	TCP 5671	Bus de messages RabbitMQ (AMQPS) pour tous les hôtes NW.
Log Decoder	Log Collector	TCP 6514	
Log Decoder	Serveur NFS	TCP 111 2049 UDP 111 2049	Installations iDRAC

Hôte Log Hybrid

Hôte source	Hôte de destination	Ports de destination	Commentaires
Station de travail Admin	Log Hybrid	TCP 15671	Interface utilisateur de gestion RabbitMQ
Log Hybrid	Serveur NW	TCP 15671	Interface utilisateur de gestion RabbitMQ
Log Hybrid	Serveur NW	TCP 443	Référentiel de mise à jour RSA
Station de travail Admin	Log Hybrid	TCP 22	SSH
Log Collector	Source d'événements de Log	Se référer au <i>Guide de configuration de Log Collection</i> . Accédez à la Table des matières principale pour rechercher tous les documents sur NetWitness Platform Logs & Network 11.x.	
Sources d'événements de Log	Log Hybrid	TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)	Ports de Log Collection
Sources d'événements de Log	Log Hybrid	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Ports de Log Collection FTP/S
Serveur NW	Log Hybrid	TCP 56001 (SSL), 50101 (REST)	Ports d'application de Log Collector
Serveur NW	Log Hybrid	TCP 56002 (SSL), 56202 (Endpoint), 50102 (REST)	Ports d'application Log Decoder
Serveur NW	Log Hybrid	TCP 56005 (SSL), 50105 (REST)	Ports d'application Concentrator
Serveur NW	Log Hybrid	TCP 56006 (SSL), 50106 (REST)	Ports d'appliance NetWitness
Serveur NW	Log Hybrid	TCP 5671	Bus de messages RabbitMQ (AMQPS) pour tous les hôtes NW.

Hôte source	Hôte de destination	Ports de destination	Commentaires
Log Hybrid	Serveur NFS	TCP 111 2049 UDP 111 2049	Installations iDRAC

Hôte Malware

Hôte source	Hôte de destination	Ports de destination	Commentaires
Station de travail Admin	Malware	TCP 15671	Interface utilisateur de gestion RabbitMQ
Malware	Serveur NW	TCP 15671	Interface utilisateur de gestion RabbitMQ
Malware	Serveur NW	TCP 443	Référentiel de mise à jour RSA
Station de travail Admin	Malware	TCP 22	SSH
Serveur NW	Malware	TCP 60007	Ports d'application Malware
Serveur NW	Malware	TCP 56006 (SSL), 50106 (REST)	Ports d'appliance NetWitness
Serveur NW	Malware	TCP 5671	Bus de messages RabbitMQ (AMQPS) pour tous les hôtes NW.
Serveur NW	Malware	TCP 5432	Postgresql
Serveur NW	Malware	TCP 56003 (SSL), 50103 (REST)	Ports d'application Broker
Malware	panacea.threatgrid.com	TCP 443	Threatgrid
Malware	cloud.netwitness.com	TCP 443	Évaluation de la Communauté / Opswat
Malware	Serveur NFS	TCP 111 2049 UDP 111 2049	Installations iDRAC

Hôte de décodeur réseau

Hôte source	Hôte de destination	Ports de destination	Commentaires
Station de travail Admin	Décodeur réseau	TCP 15671	Interface utilisateur de gestion RabbitMQ
Décodeur réseau	Serveur NW	TCP 15671	Interface utilisateur de gestion RabbitMQ
Décodeur réseau	Serveur NW	TCP 443	Référentiel de mise à jour RSA
Station de travail Admin	Décodeur réseau	TCP 22	SSH
Serveur NW	Décodeur réseau	TCP 56004 (SSL), 50104 (REST)	Ports d'application de décodeur réseau
Serveur NW	Décodeur réseau	TCP 56006 (SSL), 50106 (REST)	Ports d'appliance NetWitness
Serveur NW	Décodeur réseau	TCP 5671	Bus de messages RabbitMQ (AMQPS) pour tous les hôtes NW.
Décodeur réseau	Serveur NFS	TCP 111 2049 UDP 111 2049	Installations iDRAC

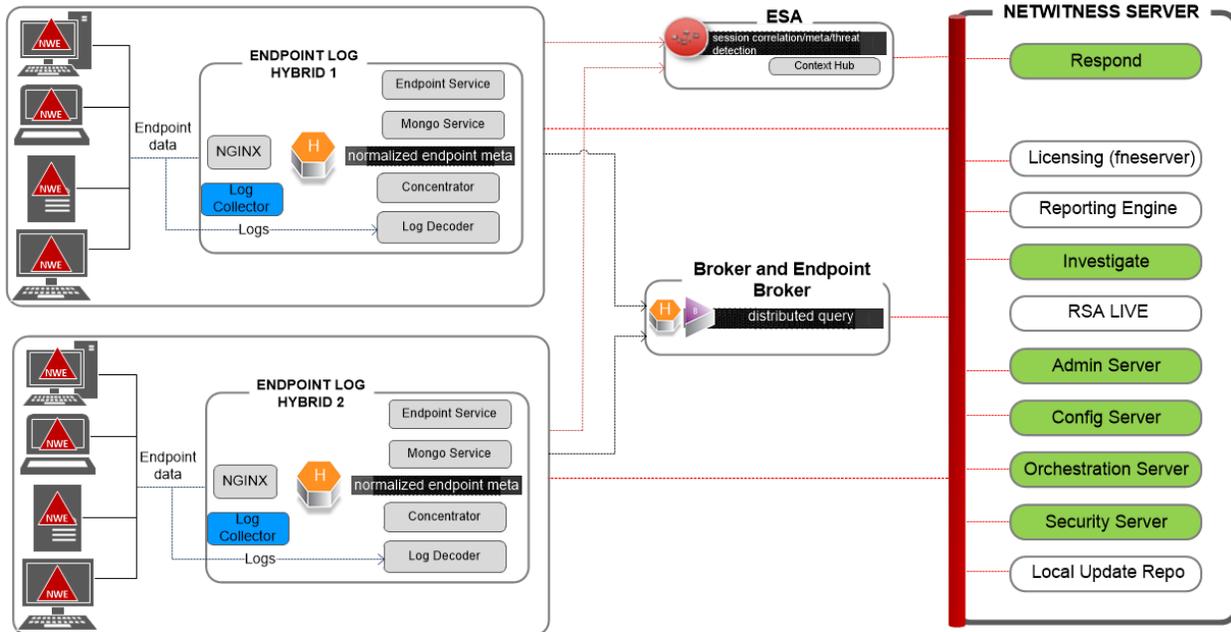
Hôte réseau hybride

Hôte source	Hôte de destination	Ports de destination	Commentaires
Station de travail Admin	Réseau hybride	TCP 15671	Interface utilisateur de gestion RabbitMQ
Réseau hybride	Serveur NW	TCP 15671	Interface utilisateur de gestion RabbitMQ
Réseau hybride	Serveur NW	TCP 443	Référentiel de mise à jour RSA
Station de travail Admin	Réseau hybride	TCP 22	SSH
Serveur NW	Réseau hybride	TCP 56004 (SSL), 50104 (REST)	Ports d'application de décodeur réseau
Serveur NW	Réseau hybride	TCP 56005 (SSL), 50105 (REST)	Ports d'application Concentrator
Serveur NW	Réseau hybride	TCP 56006 (SSL), 50106 (REST)	Ports d'appliance NetWitness
Serveur NW	Réseau hybride	TCP 5671	Bus de messages RabbitMQ (AMQPS) pour tous les hôtes NW.
Réseau hybride	Serveur NFS	TCP 111 2049 UDP 111 2049	Installations iDRAC

Hôte UEBA

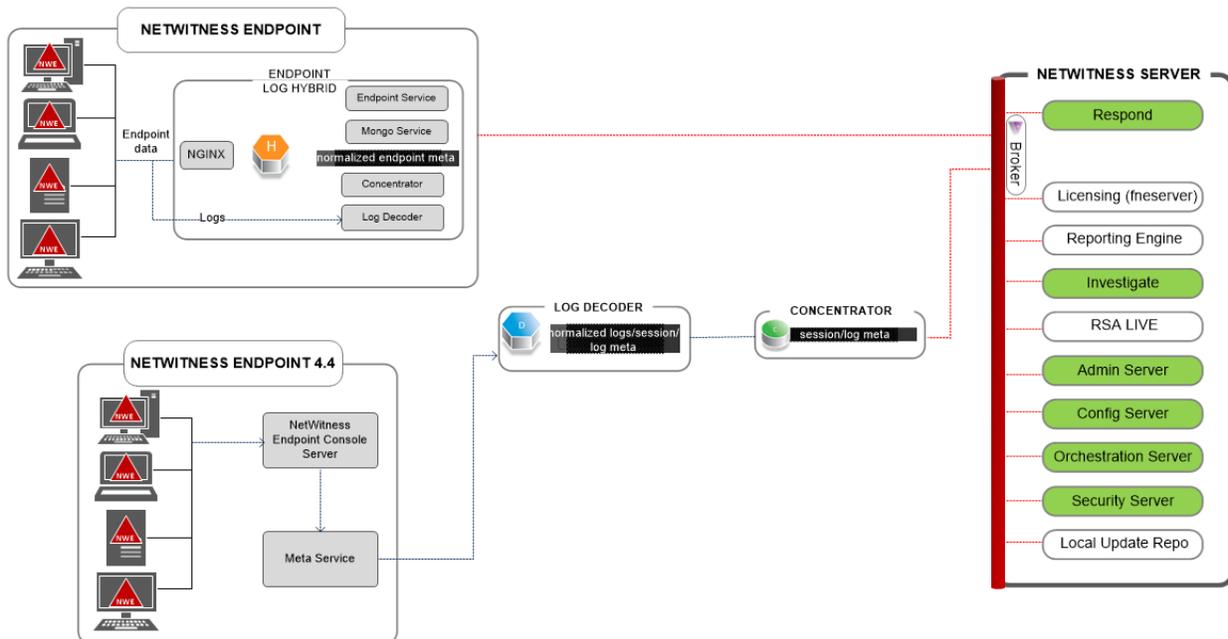
Hôte source	Hôte de destination	Ports de destination	Commentaires
Serveur UEBA	Serveur NW	TCP 443	Référentiel de mise à jour RSA
Serveur UEBA	Broker	TCP 56003 (SSL), 50103 (REST)	Ports d'application Broker
Serveur UEBA	Concentrator	TCP 56005 (SSL), 50105 (REST)	Ports d'application Concentrator
Station de travail Admin	Serveur UEBA	443	Surveillance de l'UEBA
Station de travail Admin	Serveur UEBA	22	SSH
Serveur UEBA	Serveur NW	15671	Transmission d'alertes UEBA à répondre
Serveur NW	Serveur NFS	TCP 111, 2049 UDP 111, 2049	Installations iDRAC

Architecture de NetWitness Endpoint



Note: Log Collector collects Windows logs from event sources.

Intégration du point de terminaison NetWitness 4.4 avec la plate-forme NetWitness



Pour plus d'informations sur les services exécutés sur Endpoint Log Hybrid, reportez-vous à la section *Guide de configuration de RSA NetWitness Endpoint*.

Comment modifier le port UDP pour Endpoint Log Hybrid

Les étapes suivantes vous indiquent comment modifier le port UDP 444 par défaut d'Endpoint Log Hybrid s'il n'est pas acceptable dans votre environnement. Cette procédure utilise 555 comme exemple pour remplacer le port UDP 444.

Il existe deux tâches dont vous avez besoin pour modifier le port UDP 444 par défaut d'Endpoint Log Hybrid :

Tâche 1 - Informer tous les agents qu'ils doivent utiliser un nouveau port UDP

Tâche 2 - Mettre à jour le port sur tous les hôtes Endpoint Log Hybrid dans votre environnement

Remarque : Si vous n'avez pas sélectionné l'option des règles de pare-feu personnalisées lors de l'exécution de `nwsetup-tui`, NetWitness Platform remplace les règles de pare-feu après un certain temps. Si c'est le cas, consultez l'article suivant de la base de connaissances 00036446 (<https://community.rsa.com/docs/DOC-93651>).

Tâche 1 - Informer tous les agents qu'ils doivent utiliser un nouveau port UDP

Procédez comme suit pour mettre à jour le port UDP dans la règle de réplication des données d'entreprise par défaut (EDR) et dans toutes les autres règles pour indiquer à tous les agents d'utiliser un nouveau port UDP.

1. Dans le menu **NetWitness Platform**, sélectionnez **ADMIN > Sources Endpoint > Règles**. La vue **Règles** s'affiche.
2. Sélectionnez la **Règle EDR par défaut**, puis cliquez sur **Modifier** dans la barre d'outils.
3. Déroulez jusqu'à **PORT UDP** et modifiez la valeur (par exemple, passez de **444** à **555**).
4. Cliquez sur **Publier la règle** au bas de la vue.

Tâche 2 - Mettre à jour le port sur tous les hôtes Endpoint Log Hybrid dans votre environnement

Ouvrez une session SSH pour chaque hôte Endpoint Log Hybrid de votre environnement avec les `admin` informations d'identification et effectuez les mises à jour suivantes.

1. Mettez les `iptables` règles à jour pour autoriser 555 à la place de 444.

- a. Dans le fichier suivant, remplacez 444 par 555 .

```
vi /etc/sysconfig/iptables
```

- b. Redémarrez `iptables` avec la chaîne de commande suivante.

```
systemctl restart iptables
```

- c. Vérifiez la modification grâce à la chaîne de commande suivante.

```
iptables -L -n
```

Voici un exemple de ce qui s'affiche lorsque la modification est correcte.

```
ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp multiport dports 555 /*  
EndpointNginxPort */ ctstate NEW
```

2. Mettez à jour la stratégie SELinux. 555 est le port de prédilection. Vous devez donc mettre à jour la règle SELinux pour autoriser ce port.
 - a. Exécutez la chaîne de commande suivante.

```
semanage port -a -t http_port_t -p udp 555
```

Si vous avez reçu des erreurs ou des avertissements Python, ignorez-les.
 - b. Vérifiez la modification grâce à la chaîne de commande suivante.

```
semanage port -l | grep http_port_t
```

Voici un exemple de ce qui s'affiche lorsque la modification est correcte.

```
http_port_t udp 555, 444
```
 - c. (Facultatif) Supprimez 444.
3. Mettez à jour la configuration nginx.
 - a. Modifiez le fichier suivant :

```
vi /etc/nginx/nginx.conf
```
 - b. Recherchez la chaîne suivante :

```
listen 444 udp;
```
 - c. Remplacez 444 par 555.
 - d. Redémarrez nginx avec la chaîne de commande suivante.

```
systemctl restart nginx
```
4. Vérifiez que les agents communiquent sur le nouveau port.
 - a. Exécutez la chaîne de commande suivante.

```
tcpdump -i eth0 port 555
```
 - b. Patientez 30 secondes, car le port envoie une balise toutes les 30 secondes. Si tout fonctionne correctement, des informations semblables à ce qui suit s'affichent.

```
09:20:12.571316 IP 10.40.15.103.60807 >
NiranjanEPS1.rsa.lab.emc.com.dsf: UDP, length 20
09:20:12.572433 IP NiranjanEPS1.rsa.lab.emc.com.dsf >
10.40.15.103.60807: UDP, length 1
```

Les deux lignes doivent être renvoyées. L'une est la demande de taille (20 octets) et l'autre correspond à la taille de la réponse (1 octet).

Exigences du site et sécurité

Lisez soigneusement et respectez tous les avertissements et précautions avant d'installer ou d'effectuer la maintenance de vos appareils RSA.

Usages prévus de l'application

Ce produit a été évalué comme équipement IT (ITE) pouvant être installé à l'intérieur d'un bureau, d'une école, d'une salle informatique ou d'un emplacement commercial. Ce périphérique n'est pas destiné à être branché à un câble de type extérieur.

Service

Aucun composant réparable par l'utilisateur n'est présent à l'intérieur de cet appareil. Veuillez contacter le support client en cas de dysfonctionnement. En cas de défaillance, une température élevée peut survenir à l'intérieur du système provoquant un signal d'alarme. Si l'alarme se déclenche, débranchez immédiatement l'appareil de la source d'alimentation et contactez le support client. Un fonctionnement prolongé du périphérique serait dangereux et pourrait causer des blessures ou des dommages matériels.

Informations relatives à la sécurité

Sélection de site

Le système est conçu pour fonctionner dans un environnement de bureau classique. Choisissez un site avec les caractéristiques suivantes :

- Être propre, sec et exempt de particules en suspension dans l'air (sans compter la poussière que l'on peut s'attendre à trouver normalement dans une pièce).
- Bénéficier d'une bonne ventilation et ne pas être exposé à une source de chaleur, y compris à la lumière directe du soleil et à des radiateurs.
- Ne pas être exposé à des sources de vibrations ou de chocs physiques.
- Être éloigné des champs magnétiques puissants produits par les appareils électriques.
- Dans les régions qui sont sensibles aux orages électriques, nous vous recommandons de brancher le système à un parasurtenseur.
- Être doté d'une prise murale avec mise à la terre.
- Laisser suffisamment d'espace pour accéder aux câbles d'alimentation servant de dispositifs principaux de coupure du courant pour le produit.

Pratiques de manipulation de l'équipement

Réduisez le risque de blessures ou de dommages matériels par les actions suivantes :

- Se conformer aux exigences de santé et de sécurité au travail lors du déplacement ou du soulèvement du périphérique.
- Utiliser une aide mécanique ou toute autre assistance appropriée lors du déplacement ou du soulèvement du périphérique.
- Réduire le poids de l'appareil pour faciliter la manipulation en supprimant tous les composants facilement détachables.

Avertissements relatifs à l'alimentation et à l'électricité

Attention : Le bouton d'alimentation désigné par la marque d'alimentation de secours, n'éteint PAS complètement l'alimentation secteur du système. Une alimentation de secours de 5 V est active lorsque le système est branché. Pour couper l'alimentation du système, vous devez débrancher le cordon d'alimentation secteur de la prise murale.

- N'essayez pas de modifier ni d'utiliser un cordon d'alimentation s'il ne s'agit pas du type exact requis. Un autre cordon d'alimentation est requis pour chaque alimentation du système.
- Ce produit ne contient aucune pièce réparable par l'utilisateur. N'ouvrez pas le système.
- Lorsque vous remplacez une alimentation remplaçable à chaud, débranchez le câble de l'alimentation à remplacer, avant de la retirer du serveur.

Avertissements relatifs au montage en rack

- Le rack doit être fixé à un support inamovible pour l'empêcher de basculer lorsque vous sortez le serveur ou un élément. Le rack doit être installé conformément aux instructions du fabricant du rack.
- Le montage de l'équipement dans le rack doit être effectué soigneusement afin d'éviter tout danger lié à une charge mécanique inégale.
- Ne sortez qu'un seul élément du rack à la fois.
- Pour éviter tout choc électrique, vous devez disposer d'une mise à la terre de sécurité pour le rack et pour chaque équipement qui y est installé.

Refroidissement et circulation de l'air

L'installation de l'équipement ne doit pas compromettre la quantité d'aération nécessaire au fonctionnement sûr de l'équipement.