RSA NETWITNESS® SUITE

Guide de déploiement AWS

pour la version 11.0

Informations de contact

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

Marques commerciales

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

Contrat de licence

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

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

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

Licences tierces

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

Remarque sur les technologies de chiffrement

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

Distribution

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

février 2018

Sommaire

Présentation du déploiement AWS

Avant de pouvoir déployer RSA NetWitness® Suite dans Amazon Web Services (AWS) vous devez :

- Comprendre les exigences de votre entreprise.
- Connaître le périmètre d'un déploiement NetWitness Suite.

Lorsque vous êtes prêt(e) à commencer le déploiement :

- Assurez-vous de disposer d'une licence « Débit » NetWitness Suite.
- Pour la capture de paquets dans AWS, vous pouvez acheter une des solutions tierces suivantes. Si vous utilisez une de ces solutions tierces, un responsable de compte et un ingénieur de services professionnels vous seront attribués qui travailleront en étroite collaboration avec les équipes RSA.
  - Gigamon® GigVUE 5.0
  - f5BIG-IP 12.1.0

Recommandations en matière d'environnement AWS

Les instances AWS ont les mêmes fonctions que les hôtes matériels NetWitness Suite. RSA vous conseille d'effectuer les tâches suivantes lorsque vous configurez votre environnement AWS.

- En fonction des ressources nécessaires aux différents composants, suivez les bonnes pratiques pour utiliser le système et les volumes de stockage Elastic Block Store (EBS) dédiés de manière appropriée.
- Assurez-vous que la capacité de traitement fournit une vitesse d'écriture de 10 % supérieure à la capture soutenue requise et au taux de réception pour le déploiement.
- Créez des répertoires Concentrator pour la base de données de l'index sur le disque SSD IOPS provisionné.

Abréviations et autre terminologie utilisée dans ce guide

Abréviations	Description
AMI	Amazon Machine Image

Abréviations	Description
AWS	Amazon Web Services
BYOL	Bring your own licensing (Utiliser ses propres licences)
CPU	Central Processing Unit (Unité centrale)
Instances dédiées	Les instances dédiées AWS s'exécutent dans un VPC sur du matériel dédié à un seul et unique client. Les instances dédiées sont physiquement isolées au niveau du matériel hôte des instances appartenant à d'autres comptes AWS. Les instances dédiées peuvent partager le matériel avec d'autres instances du même compte AWS qui ne sont pas des instances dédiées. Consultez la documentation AWS « Amazon EC2 - Instances dédiées », (https://aws.amazon.com/ec2/purchasing-options/dedicated-instances/) pour plus d'informations sur les instances dédiées.
Optimisation EBS	Une instance optimisée Amazon EBS utilise une pile de configuration optimisée et fournit une capacité supplémentaire, dédiée aux E/S d'Amazon EBS. Cette optimisation offre les meilleures performances pour vos volumes EBS en réduisant les conflits d'accès entre les E/S d'Amazon EBS et le reste du trafic de votre instance. Consultez la documentation AWS « Amazon EBS - Instances optimisées » (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSOptimized.html) pour plus d'informations sur les instances optimisées EBS.
Volume EBS	Le volume EBS (Elastic Block Store) est un volume de stockage haute disponibilité fiable que vous pouvez joindre à n'importe quelle instance en cours d'exécution se trouvant dans la même zone de disponibilité. Consultez la documentation AWS « Amazon EBS - Volumes » (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSOptimized.html) pour plus d'informations sur les volumes EBS.

Abréviations	Description
Instance EC2	Serveur virtuel dans AWS Elastic Compute Cloud (EC2) pour l'exécution des applications sur l'infrastructure AWS. Voir aussi **Instance**.
Amélioration de la mise en réseau activée	L'amélioration de la mise en réseau fournit plus de bande passante, des performances supérieures de paquets par seconde et un temps de latence plus faible entre les instances. Si votre taux de paquets par seconde semble avoir atteint son plafond, vous devez envisager d'adopter l'amélioration de la mise en réseau, car vous avez probablement atteint les seuils supérieurs du pilote de l'interface réseau de la machine virtuelle (VIF). Consultez la documentation AWS « Comment activer et configurer l'amélioration de la mise en réseau sur mes instances EC2 » (https://aws.amazon.com/premiumsupport/knowledge-center/enable-configure-enhanced-networking/) pour plus d'informations sur l'amélioration de la mise en réseau.
EPS	Événements par seconde
Go	Gigaoctet. 1 Go = 1 000 000 000 octets
Gb	Gigabit. 1 Go = 1 000 000 000 bits
Gbit/s	Gigabits par seconde ou milliards de bits par seconde. Cette unité mesure la bande passante sur un support de transmission des données numériques, comme la fibre optique.
GHz	GigaHertz 1 GHz = 1 000 000 000 Hz
Disque dur	Disque dur
Instance	Hôte virtuel dans AWS (autrement dit, la machine virtuelle ou le serveur dans l'infrastructure AWS sur lesquels vous exécutez des applications ou des services). Voir aussi **Instances EC2**.

Abréviations	Description
Type d'instance	Spécifie le CPU et la RAM nécessaire pour une instance. Reportez-vous à la documentation AWS « Types d'instance Amazon EC2 » (https://aws.amazon.com/ec2/instance-types/) pour plus d'informations sur les types d'instance.
E/S par seconde	Entrées/sorties par seconde
Mbits/s	Mégabits par seconde, ou des millions de bits par seconde. Cette unité mesure la bande passante sur un support de transmission des données numériques, comme la fibre optique.
Sur site	Les hôtes sur site sont installés et exécutés sur les ordinateurs sur le site (dans le bâtiment) de l'organisation utilisant les hôtes, plutôt que dans AWS.
PPS	Paquets par seconde
RAM	Random Access Memory (également nommé mémoire)
Groupe de sécurité	Ensemble de règles de pare-feu. Consultez la documentation « Architecture de réseau et ports » dans RSA Link (https://community.rsa.com/docs/) pour obtenir la liste complète des ports que vous devez configurer pour l'ensemble des composants NetWitness Suite.
SSD	Solid-State Drive (Disque SSD)
Balise	Identificateur significatif pour l'instance AWS.
Fournisseur TAP	Fournisseur de réseau TAP
vCPU	Virtual Central Processing Unit (Unité de traitement central virtuelle, également nommée processeur virtuel)

Abréviations	Description
VM	Machine virtuelle
VPC	Cloud public virtuel
vRAM	Virtual Random Access Memory (également nommé mémoire virtuelle)

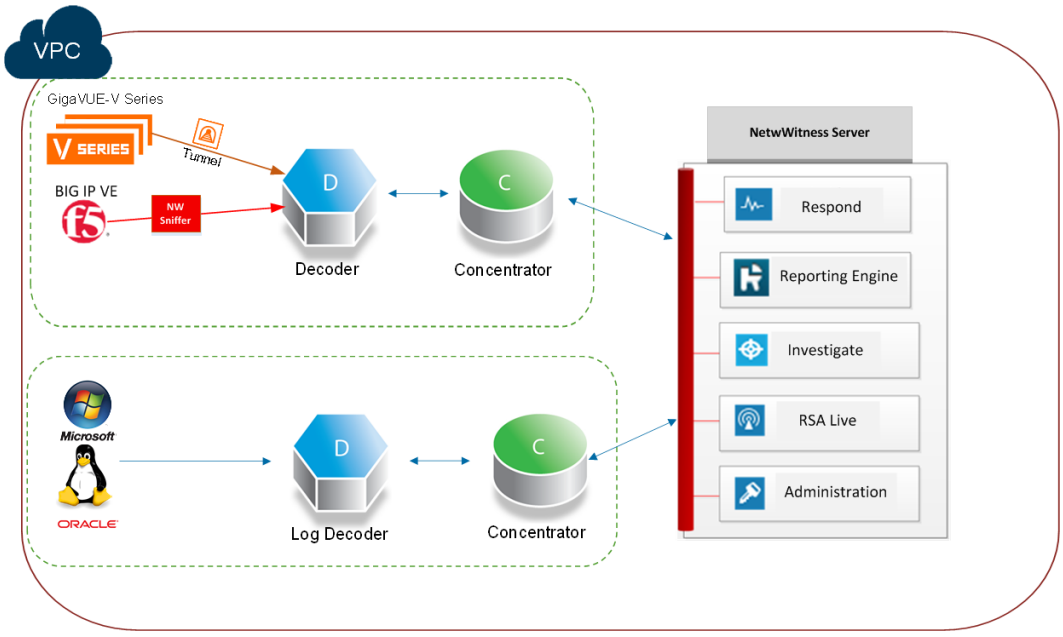
Scénarios de déploiement AWS

Les schémas suivants illustrent des scénarios de déploiement AWS courants. Dans les schémas :

- **La gamme GigaVUE** (Solution Gigamon®) est une solution basée sur agent qui utilise **l'encapsulation** (mise en œuvre par l'administrateurNetWitness Suite) afin de faciliter la capture de données de paquet dans AWS.
- **BIG-IP** (f5® Solution) est une solution de répartition de charge qui utilise un Packet Decoder agissant comme un renifleur (personnalisé par l'administrateurNetWitness Suite) afin de faciliter la capture des paquets dans AWS.
- **Decoder** collecte les données de paquets. Le **Decoder** capture, analyse et reconstruit tout le trafic réseau des couches 2 à 7.
- **Log Decoder** collecte les logs. Le **Log Decoder** collecte les événements de log de centaines de périphériques et de sources d'événements.
- **Concentrator** indexe les métadonnées extraites d'un réseau ou les données des fichiers log afin d'autoriser l'interrogation et l'analytique en temps réel à l'échelle de l'entreprise tout en facilitant le reporting et la génération d'alertes.
- Hôtes Serveur NetWitness,**Respond**, **Reporting**, **Investigate**, **gestion de contenu Live**, **Administration** et autres aspects de l'interface utilisateur.

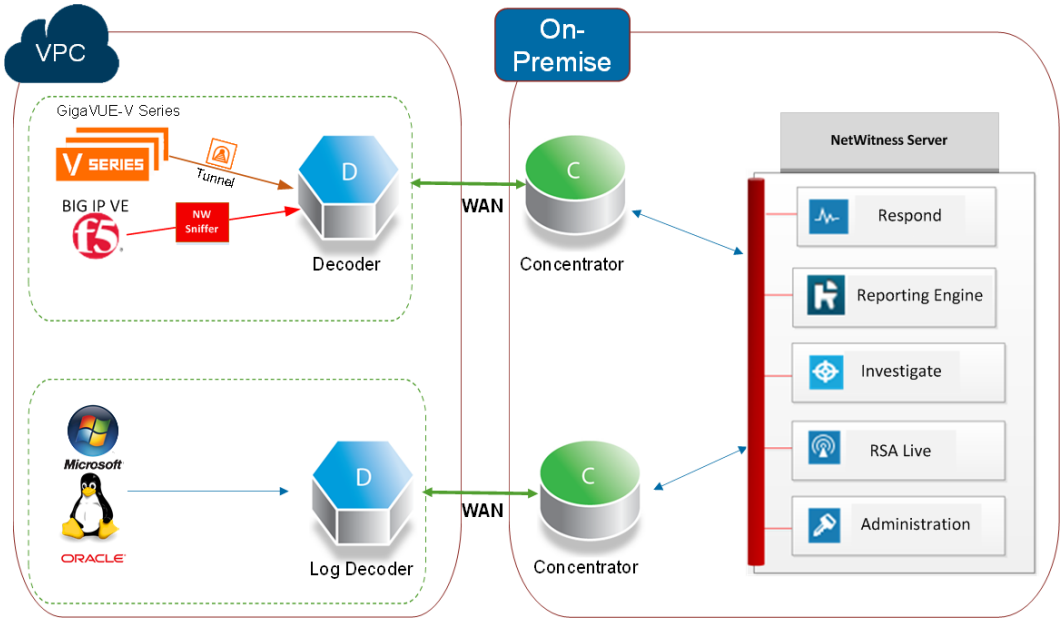
Visibilité VPC complète de la pile NetWitness Suite (solution de paquets)

Ce schéma présente tous les composants NetWitness Suite (pile complète) déployés dans AWS.


VPC
GigaVUE-V Series
V SERIES
Tunnel
BIG IP VE
NW Sniffer
D
Decoder
C
Concentrator
NetwWitness Server
Respond
Reporting Engine
Investigate
RSA Live
Administration
Microsoft
ORACLE
D
Log Decoder
C
Concentrator

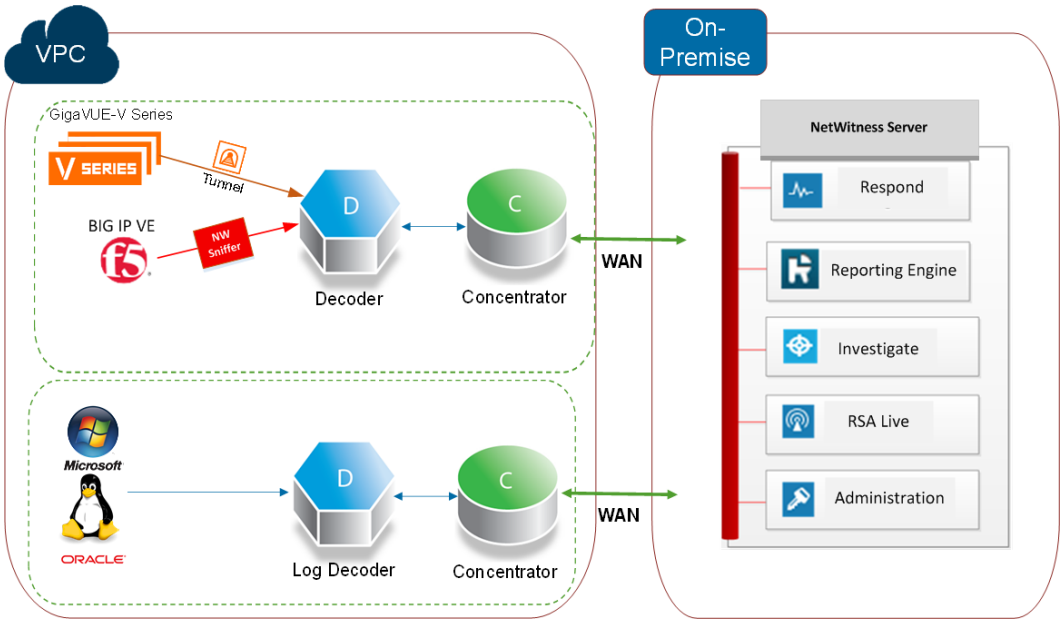
Déploiement hybride - Decoder et Log Decoder (solution de paquets)

Ce schéma présente le Decoder et Log Decoder déployés dans AWS avec tous les autres composants NetWitness Suite déployés sur votre site.



Déploiement hybride - Decoder, Log Decoder et Concentrator (solution de paquets)

Ce schéma présente le Decoder, Log Decoder et le Concentrator déployés dans AWS avec tous les autres composants NetWitness Suite déployés sur votre site.



Conditions préalables

Les éléments suivants sont nécessaires avant de commencer le processus d'intégration :

- Un accès à la console AWS
- Un réseau routable (et des groupes de sécurité AWS adaptés) dédié aux conteneurs afin de transférer des données vers NetWitness Suite Decoder.

Services pris en charge

RSA fournit les services NetWitness Suite suivants.

- Serveur NetWitness
- Archiver
- Broker
- Concentrator

- Event Stream Analysis
- Log Decoder
- Decoder
- Remote Log Collector

Déploiement AWS

Cette rubrique contient les règles et les tâches générales à suivre pour déployer les composants RSA NetWitness® Suite dans AWS.

Règles

Vous devez respecter les règles suivantes lors du déploiement de NetWitness Suite dans AWS.

- Ouvrez une session SSH sur l'instance NetWitness Suite au moins une fois après le déploiement pour initialiser le système.
- Avant d'activer les tableaux de bord prêts à l'emploi, définissez la source de données par défaut dans la page de configuration de Reporting Engine. vers une instance
- Si vous redémarrez l'instance Packet Decoder, le tunnel n'est pas conservé. Créez à nouveau le tunnel sur Packet Decoder et redémarrez le service Decoder.
- Utilisez toujours des adresses IP privées lorsque vous provisionnez des instances AWS NetWitness Suite.

Remarque : Si vous attribuez une adresse IP publique à l'hôte du serveur NetWitness, mettez à jour le fichier de configuration /etc/nginx/conf.d/nginx.conf comme suit :

```
location /nwrpmrepo
{
alias /var/lib/netwitness/common/repo;
index index.html index.htm;
allow <Subnet-Gateway>/Subnet mask ;
#example
# allow 10.0.0.1/25;
deny all;
autoindex on;
}
```

Liste de contrôle

Étape	Description	√
1	Établir l'environnement AWS	
2	Rechercher des fichiers AMI NetWitness Suite	

Étape	Description	√
3	Démarrer une instance et configurer un hôte	
4	Configurer les hôtes (instances) dans NetWitness Suite	
5	Configurer la capture de paquets	

Établir l'environnement AWS

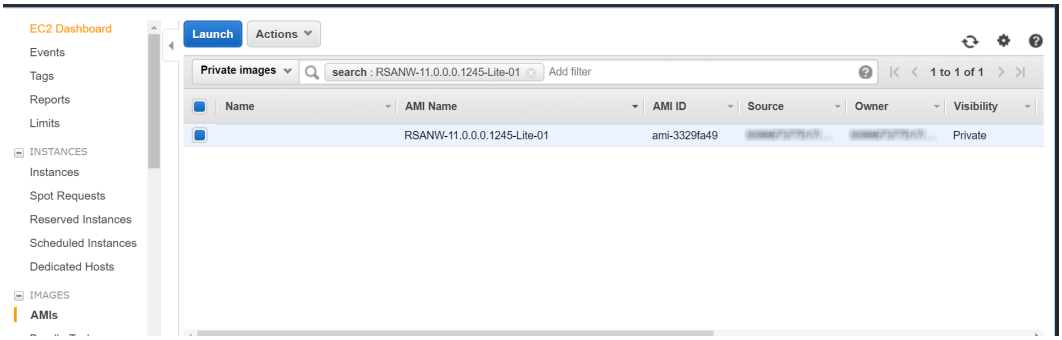
1. Assurez-vous que vous disposez d'un environnement AWS avec la capacité d'atteindre ou de dépasser les instructions NetWitness Suite relatives aux performances décrites dans Conseils de configuration de l'instance AWS .
2. Passez à l'Rechercher des fichiers AMI NetWitness Suite.

Rechercher des fichiers AMI NetWitness Suite

Recherchez des fichiers NW - AMI au sein du référentiel public/partagé/de communauté. Utilisez « RSANW » comme mot clé pour rechercher des fichiers AMI.

Remarque : Reportez-vous à la documentation **Recherche des AMI partagés** d'AWS (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usingsharedamis-finding.html) pour obtenir des instructions supplémentaires.

1. Ouvrez la console Amazon EC2 (nouveau compte abonné) sur https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez des fichiers AMI.
3. Dans le premier filtre, sélectionnez Images publiques.
4. Saisissez « RSANW » dans le champ de recherche pour rechercher les fichiers AMI NetWitness Suite.



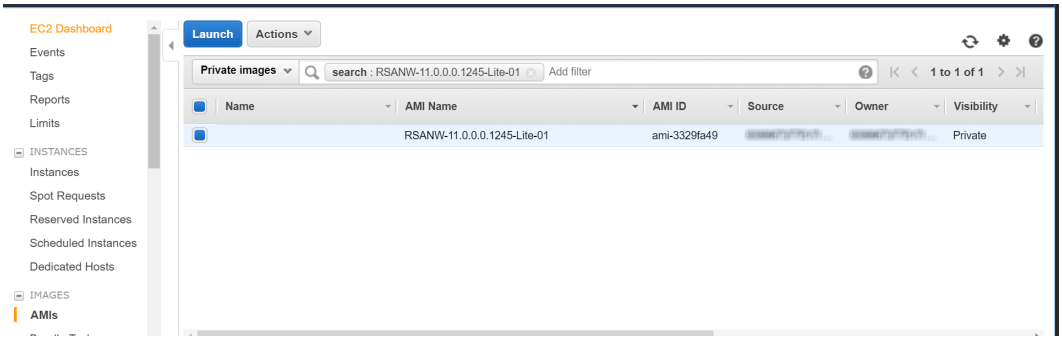
Remarque : Contactez le support client RSA (https://community.rsa.com/docs/DOC-1294) pour accéder à **RSANW-11.0.0.0.1245-Full-01**.

5. Passez à l'Démarrer une instance et configurer un hôte.

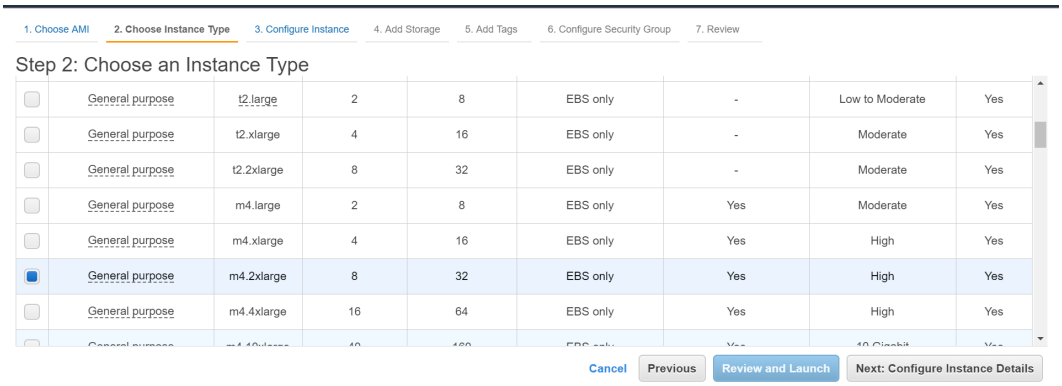
Démarrer une instance et configurer un hôte

Remarque : Consultez la documentation AWS « Launching an Instance » (Démarrage d'une instance) (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html) pour obtenir des instructions supplémentaires.

1. Sélectionnez une instance dans la grille (par exemple, **RSA-NW-Concentrator-11.0.0.0-01**), puis cliquez sur **Démarrer**.

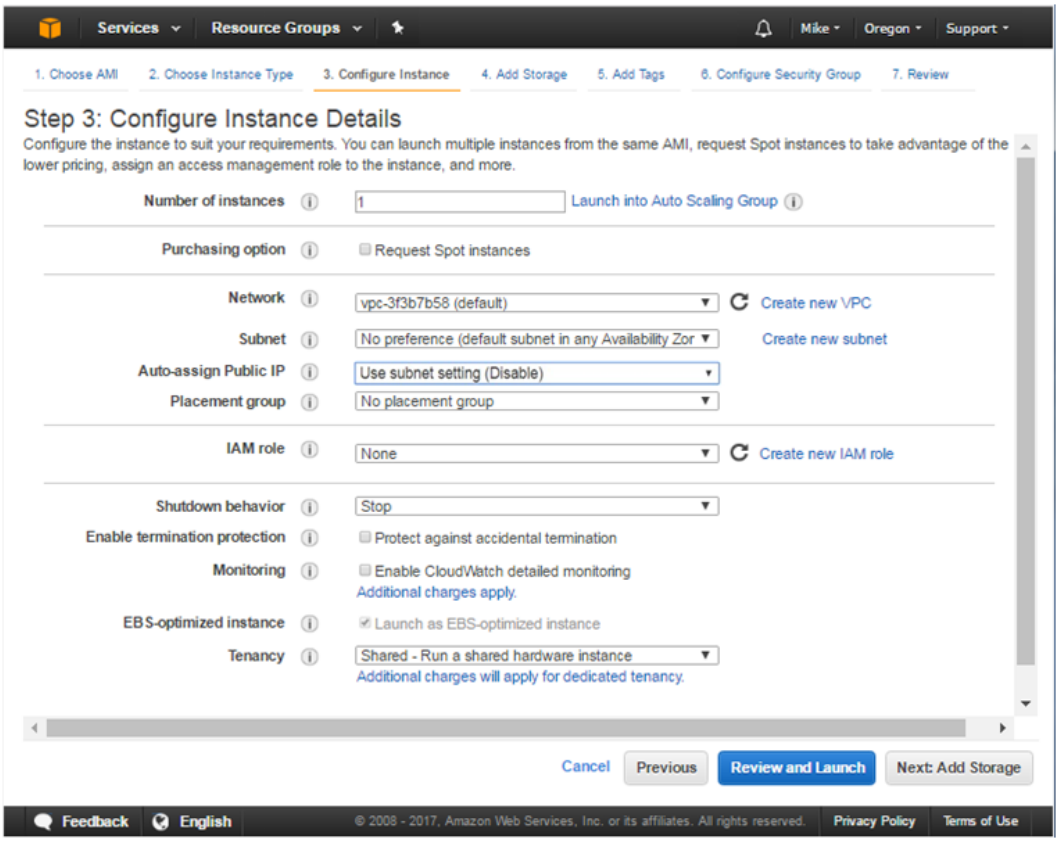


2. Choisissez la RAM et les CPU en sélectionnant le type d'instance.
   Reportez-vous à la section Conseils de configuration de l'instance AWS pour obtenir des instructions sur la configuration de l'instance EC2 en fonction des conditions requises pour le composant NetWitness Suite (autrement dit, le service) pour lequel vous lancez une instance. L'exemple suivant présente le type d'instance **m4.2xlarge** sélectionné avec **8** CPU et **32** Go de RAM.



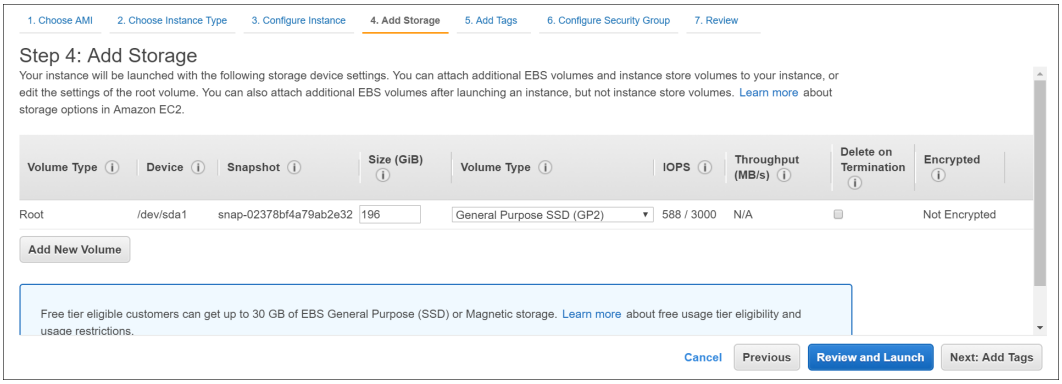
	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
	General purpose	m4.large	2	8	EBS only	Yes	Moderate	Yes
	General purpose	m4.xlarge	4	16	EBS only	Yes	High	Yes
	General purpose	m4.2xlarge	8	32	EBS only	Yes	High	Yes
	General purpose	m4.4xlarge	16	64	EBS only	Yes	High	Yes

3. Cliquez sur **Suivant : Configurer les détails de l'instance** en bas à droite de la page**Étape 2 : Choisir un type d'instance**.
   La page **Étape 3. Configurer les détails de l'instance** s'affiche.
   Pour NetWitness Suite, le sous-réseau et le VPC sont définis par défaut pour les valeurs dans l'exemple suivant.



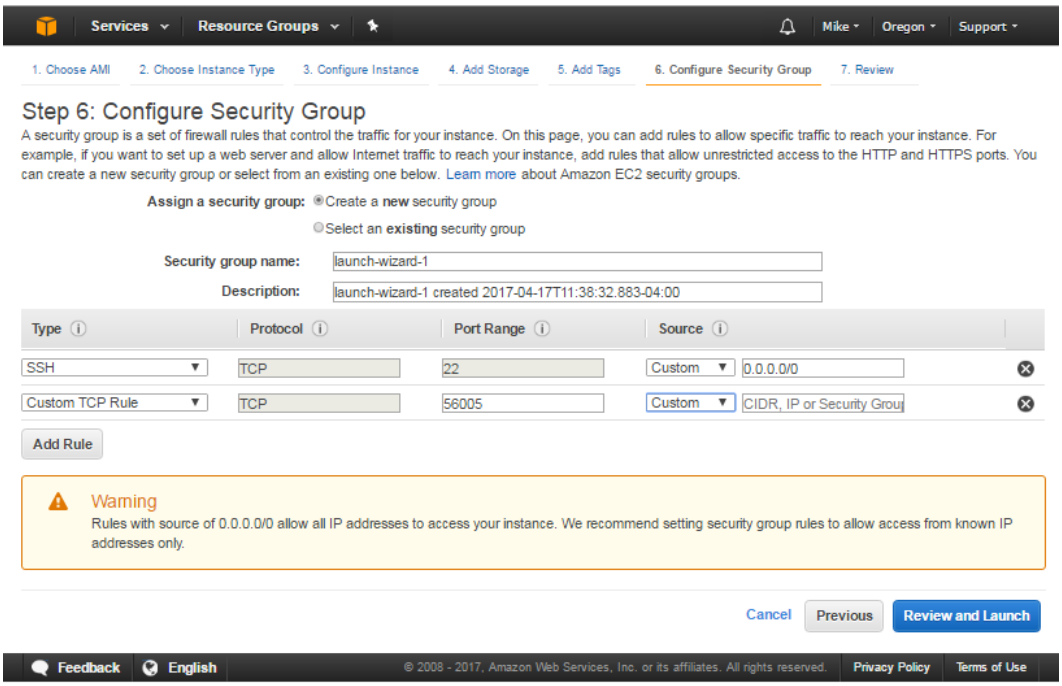
4. Cliquez sur **Suivant : Ajouter de l'espace de stockage** en bas à droite de la page **Étape 3 : Configurer les informations détaillées de l'instance**.
   La page **Étape 4. Ajouter de l'espace de stockage** s'affiche.

Reportez-vous à la section Conseils de configuration de l'instance AWS pour obtenir des instructions sur la configuration du stockage en fonction des conditions requises au composant NetWitness Suite (autrement dit, le service) pour lequel vous lancez une instance.



5. Cliquez sur **Suivant : Ajouter des balises** en bas à droite de la page **Étape 4 : Ajouter de l'espace de stockage**.
   La page **Étape 5. Ajouter des balises** s'affiche. Saisissez le nom de votre instance.
6. Cliquez sur **Suivant : Configurer le groupe de sécurité** en bas à droite de la page **Étape 5 : Ajouter des balises**.
   La page **Étape 6. Configurer le groupe de sécurité** s'affiche.
   a. Sélectionnez la case d'option « Créer un **nouveau** groupe de sécurité ».
   b. Créez une règle affichant tous les pare-feu pour le composant NetWitness Suite. Vous devez configurer le groupe de sécurité correctement pour configurer l'instance (hôte) à partir de l'interface utilisateur NetWitness Suite et pour y ouvrir une session SSH.

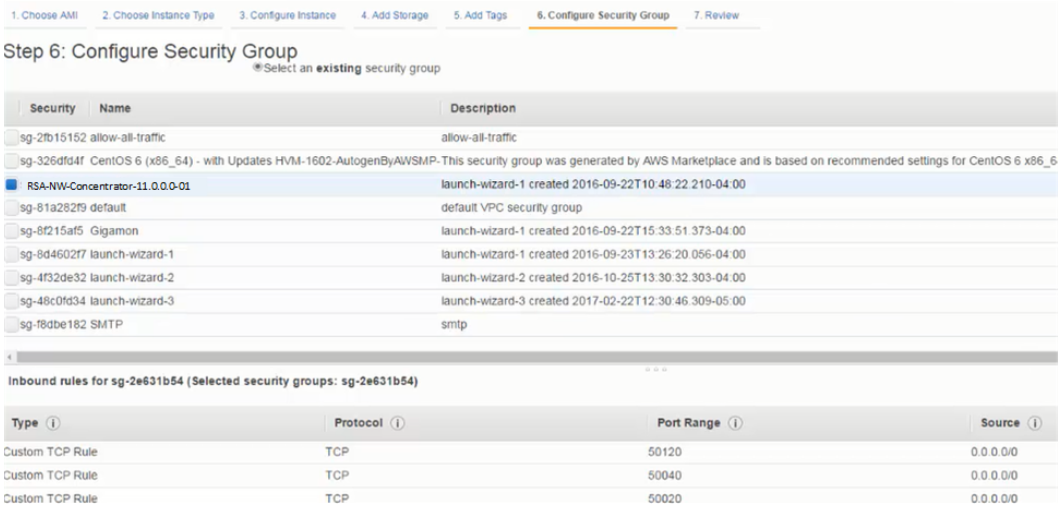
   Remarque : Consultez la documentation « Network Architecture and Ports » (Architecture de réseau et ports) dans RSA Link (https://community.rsa.com/docs/DOC-83050) pour obtenir la liste complète des ports que vous devez configurer pour l'ensemble des composants NetWitness Suite.



Remarque : Après avoir configuré un groupe de sécurité, vous pouvez le modifier à tout moment.

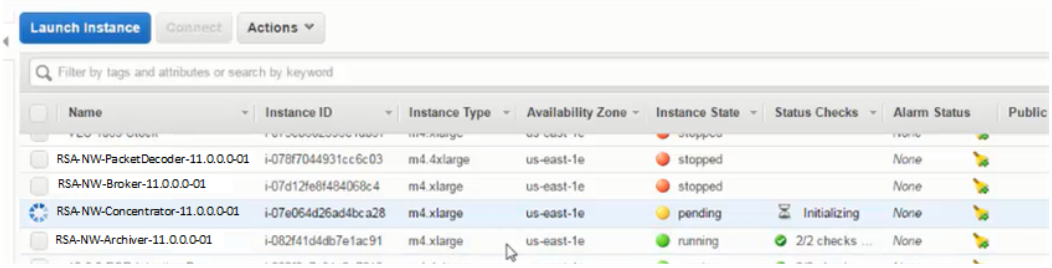
7. Cliquez sur **Vérifier et démarrer** en bas à droite de la page **Étape 6 : Configurer un groupe de sécurité**.
   La page **Étape 7. Vérifier le démarrage de l'instance** s'affiche.
8. Cliquez sur **Démarrer** en bas à droite de la page **Étape 7. Vérifier le démarrage de l'instance**.
   La boîte de dialogue **Sélectionner une paire de clés existante ou créer une nouvelle paire de clés** s'affiche.
9. Choisissez **Continuer sans la paire de clés**.

10. Cliquez sur **Démarrer l'instance**.
    AWS affiche les informations suivantes, à mesure qu'elle génère l'instance.



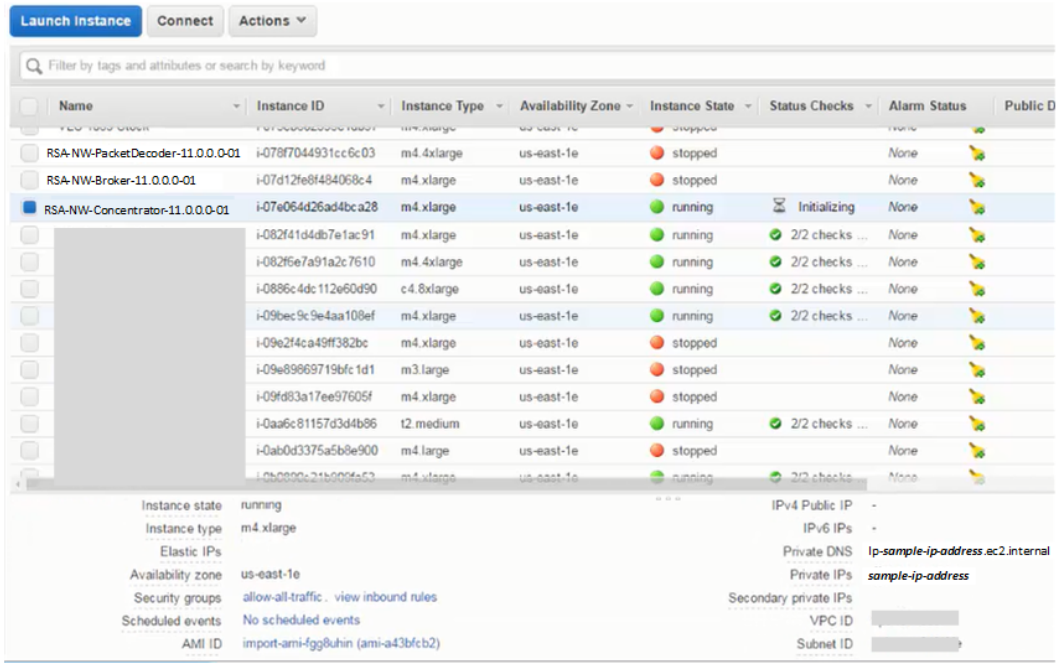
11. Cliquez sur **Afficher les instances**.

12. Sélectionnez **Instances** dans le panneau de navigation de gauche pour vérifier toutes les instances en cours d'initialisation par AWS (par exemple, **NW-Concentrator**).



L'adresse IP pour le nouvel hôte **RSA-NW-Concentrator-11.0.0.0-01** est ***sample-ip-***

address.



13. Ouvrez une session SSH sur l'instance nouvellement créée en utilisant les informations d'identification NetWitness Suite par défaut.
14. Accédez à l'Configurer les hôtes (instances) dans NetWitness Suite.

Tâches d'installation

Tâche 1 - Installation de la version 11.0.0.0 sur l'hôte du serveur NetWitness (serveur NW)

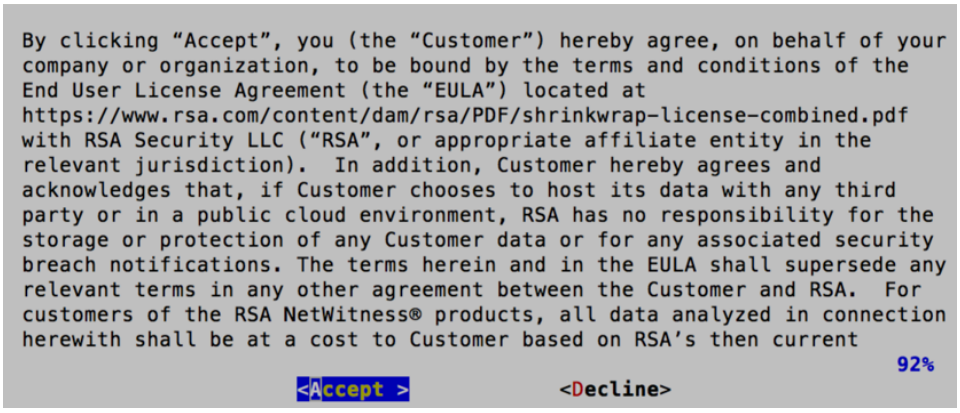
Remarque : Vous pouvez effectuer cette tâche pour l'instance RSANW-11.0.0.0.1245-Full-01.

1. Exécutez la commande `nwsetup-tui` pour configurer l'hôte.

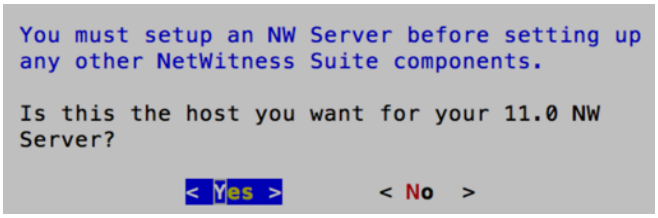
Cette opération démarre le programme d'installation et les conditions générales d'utilisation s'affichent.

Remarque : 1.) Lorsque vous parcourez les messages du programme d'installation, utilisez les touches directionnelles Haut et Bas pour naviguer entre les champs, utilisez la touche de tabulation pour naviguer d'une commande à l'autre (par exemple **<Oui>**, **<Non>**, **<OK>** et **<Annuler>**. Appuyez sur **Entrée** pour enregistrer votre réponse et passer au message suivant.
2.) Le programme d'installation adopte le modèle de couleurs du poste de travail ou de la console que vous utilisez pour accéder à l'hôte.
3.) Si vous spécifiez des serveurs DNS pendant l'exécution du programme d'installation (`nwsetup-tui`), ils doivent OBLIGATOIREMENT être valides (dans ce contexte, cela signifie valides lors de l'installation) et accessibles à `nwsetup-tui` pour continuer. Tous les serveurs DNS mal configurés provoquent l'échec de l'installation. Si vous avez besoin d'accéder au serveur DNS après l'installation, ce dernier étant inaccessible pendant l'installation, (par exemple, pour déplacer un hôte après la configuration qui aurait un ensemble différent de serveurs DNS), reportez-vous à la section Tâches à effectuer après l'installation.
Si vous ne spécifiez pas de serveurs DNS lors de la configuration (`nwsetup-tui`), vous devrez sélectionner **1 Référentiel local (sur le serveur NW)** dans le message **NetWitness Suite Mise à jour du référentiel** à l'étape 12 (les serveurs DNS ne sont pas définis afin que le système ne puisse pas accéder au référentiel externe).

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



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



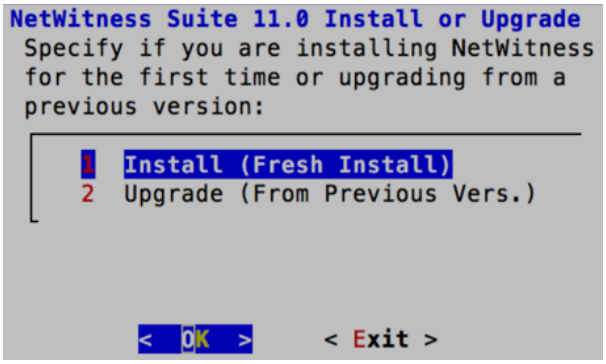
Naviguez jusqu'à **Oui** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**.

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

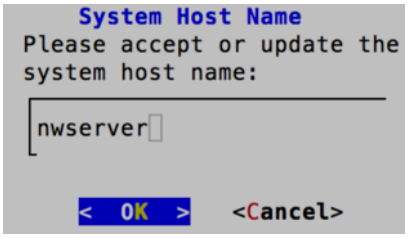
Attention : Si l'hôte choisi pour le serveur NW est incorrect et que vous terminez l'installation, vous devrez redémarrer le programme d'installation (étape 2) pour effectuer toutes les étapes suivantes pour corriger cette erreur.

4. Appuyez sur **Entrée** (Installation est sélectionnée par défaut).

   Le message Installation ou Mise à niveau s'affiche.



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



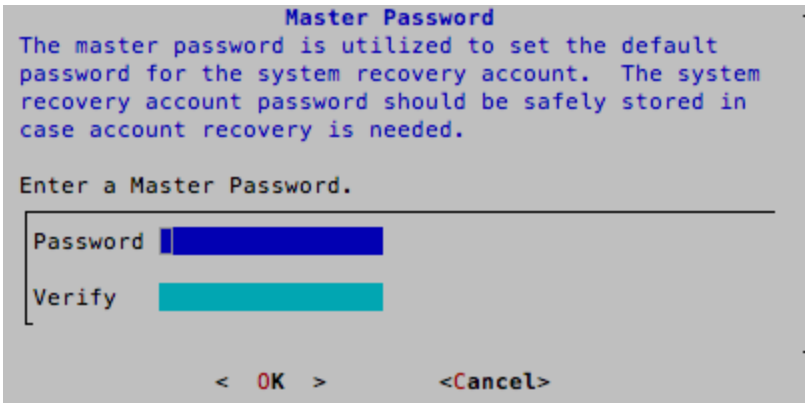
   Appuyez sur **Entrée** si vous souhaitez conserver ce nom. Dans le cas contraire, naviguez jusqu'à **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** pour modifier le nom de l'hôte.

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

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

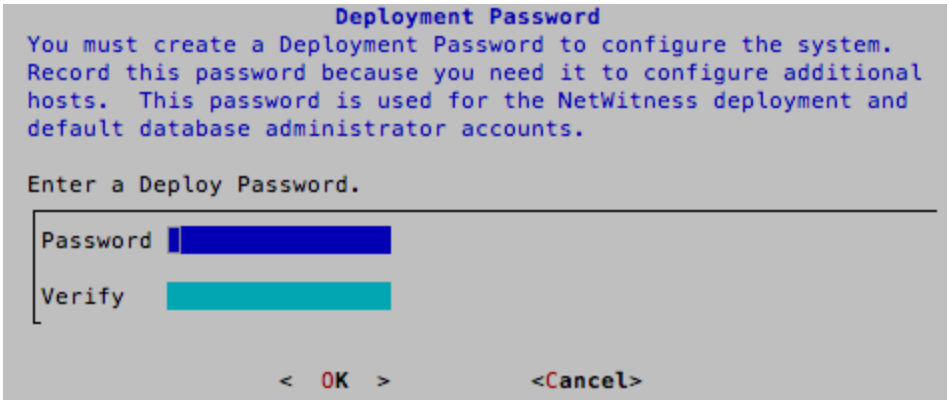
   - Symboles : ! @ # % ^ +
   - Numéros : 0-9
   - Caractères minuscules : a-z
   - Caractères majuscules : A-Z

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



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**.

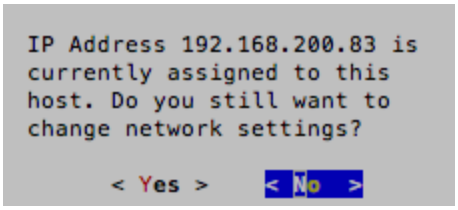
7. Le message « Mot de passe de déploiement » s'affiche.



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**.

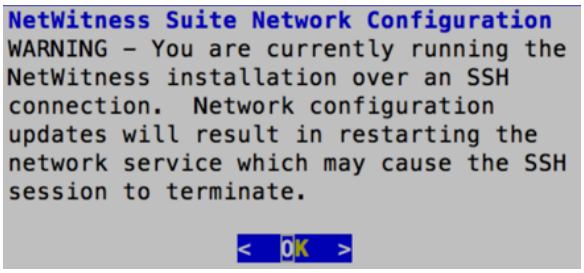
8. Si :

- 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.

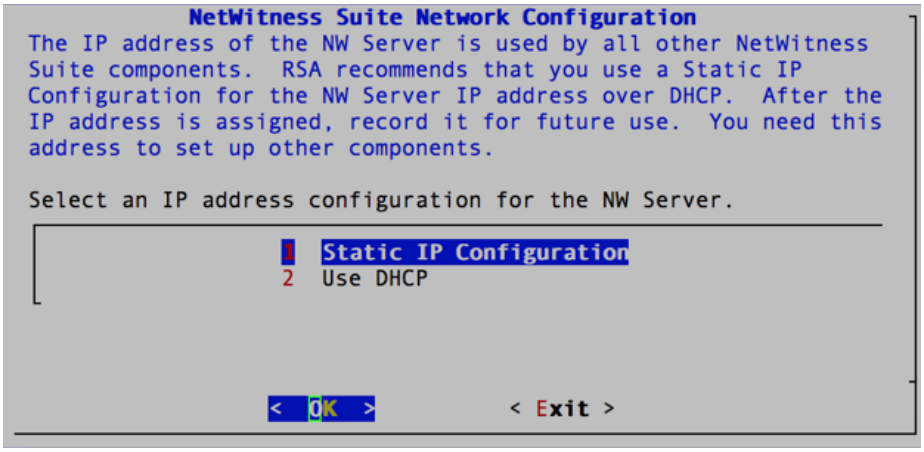
- Vous utilisez une connexion SSH, l'avertissement suivant s'affiche.



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

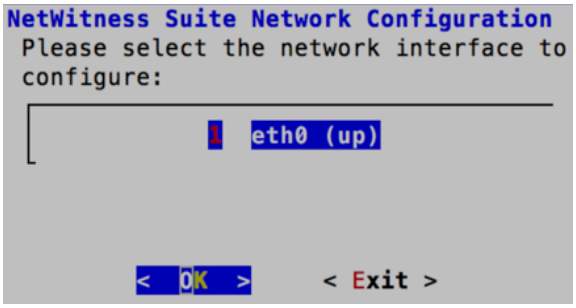
- Si le programme d'installation a détecté une configuration IP et que vous avez choisi de l'utiliser, le message Mettre à jour le référentiel s'affiche. Accédez à l'étape 12 et terminez l'installation.

- 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.



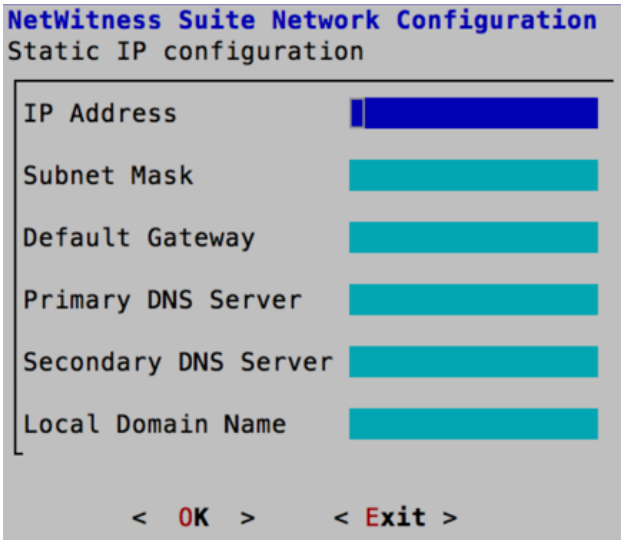
  Naviguez jusqu'à **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** pour utiliser l'**adresse IP statique**.
  Si vous souhaitez utiliser **DHCP**, utilisez la touche directionnelle Bas jusqu'à 2 Utiliser DHCP, puis appuyez sur **Entrée**.

9. Le message Configuration de réseau s'affiche.



   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, accédez à **Quitter** à l'aide de la touche de tabulation

10. Le message Configuration d'adresse IP statique s'affiche.



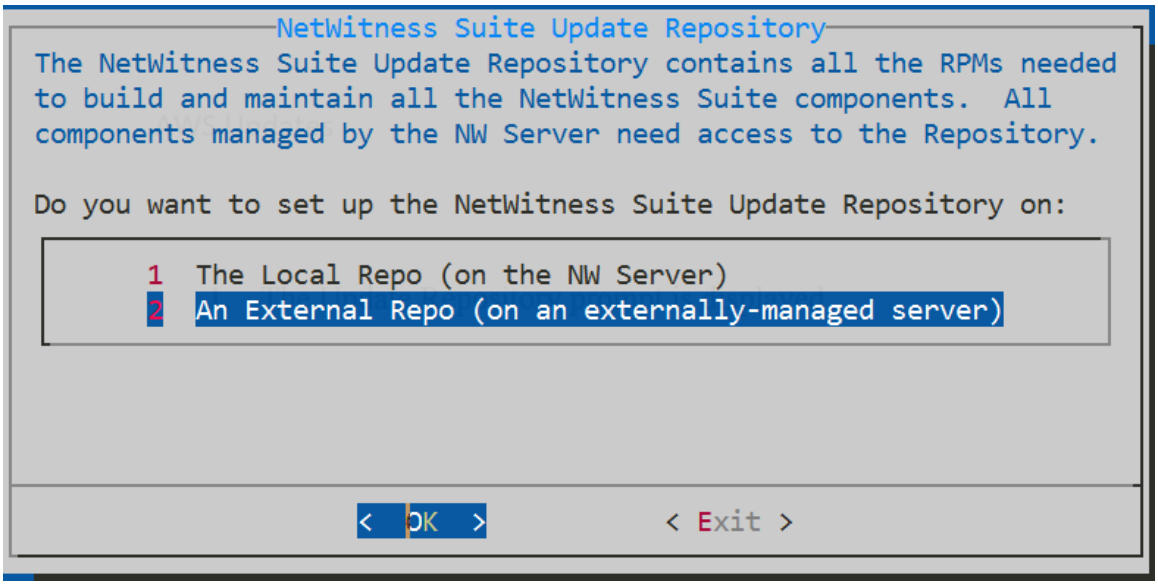
Saisissez les valeurs de configuration (en naviguant d'un champ à l'autre à l'aide de la touche directionnelle Bas), naviguez jusqu'à **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**.

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

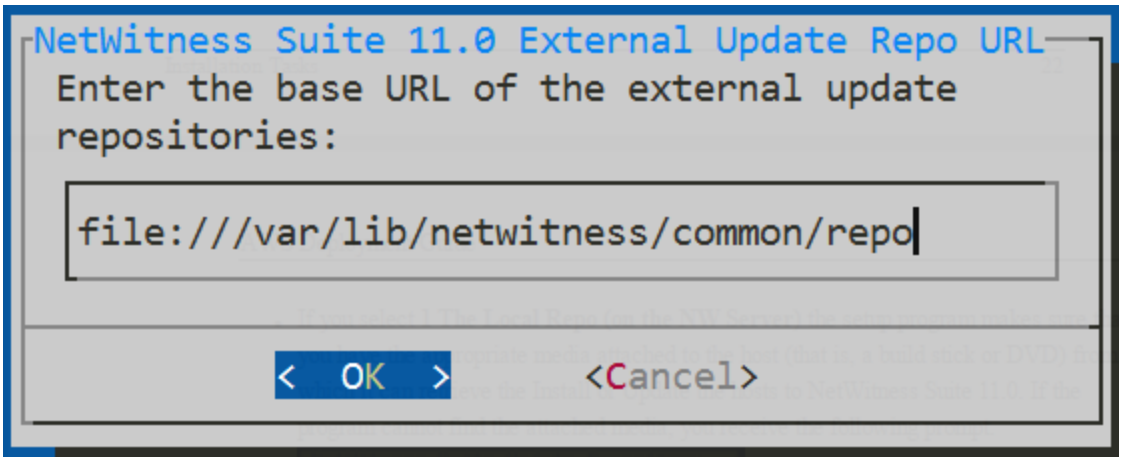
Si la syntaxe ou la longueur de caractères utilisées pour un de ces champs est incorrecte, le message d'erreur *Nom du champ*non valide s'affiche.

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

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



Si vous sélectionnez **2 Un référentiel externe (sur un serveur géré en externe)**, l'interface utilisateur vous invite à saisir une URL.

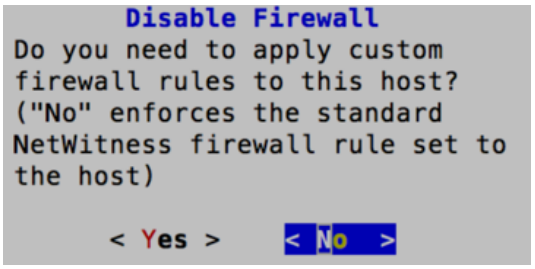


Utilisez l'URL par défaut du référentiel externe NetWitness Suite, puis cliquez sur **OK**.

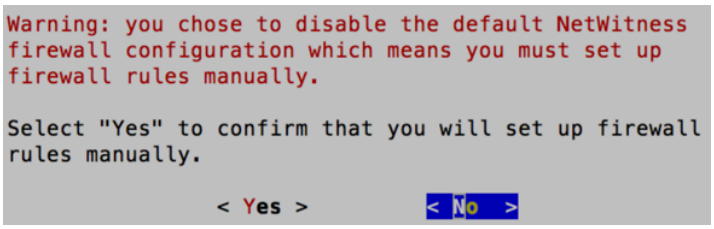
12. Appliquez la configuration de pare-feu standard, puis appuyez sur **Entrée**.

    - Désactivez la configuration standard, naviguez jusqu'à **Oui** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**.

      Le message Désactiver le pare-feu s'affiche.

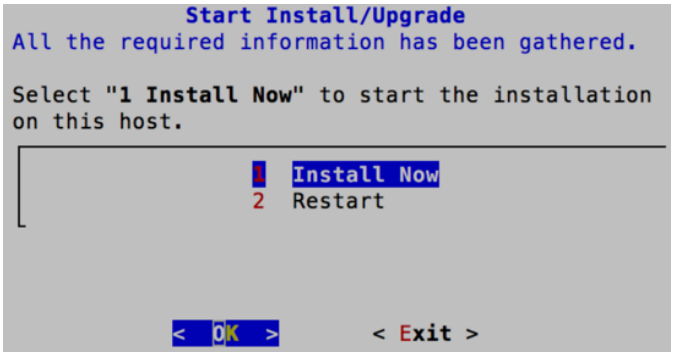
      

      Le message Confirmer la désactivation de la configuration du pare-feu s'affiche.



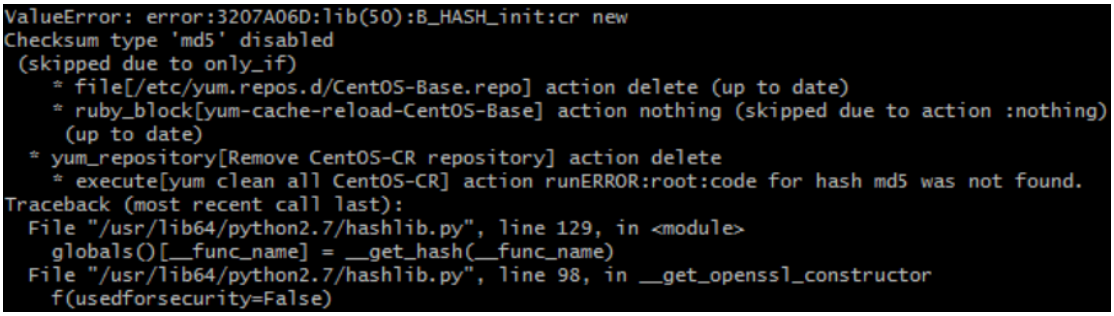
Naviguez jusqu'à **Oui** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** pour confirmer. (Appuyez sur **Entrée** pour utiliser la configuration de pare-feu standard).

13. Appuyez sur **Entrée** pour installer la version 11.0.0.0 sur le serveur NW.
    Le message Démarrer l'installation s'affiche.



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

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.



Tâche 2 - Installation de la version 11.0.0.0 sur tous les autres composants hôtes

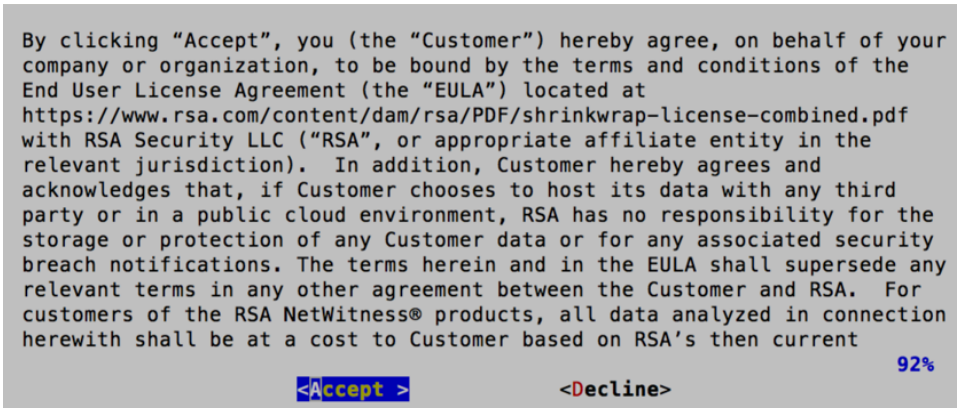
Remarque : Vous pouvez effectuer cette tâche pour une instance RSANW-11.0.0.0.1245-Lite-01.

1. Exécutez la commande `nwsetup-tui` pour configurer l'hôte.

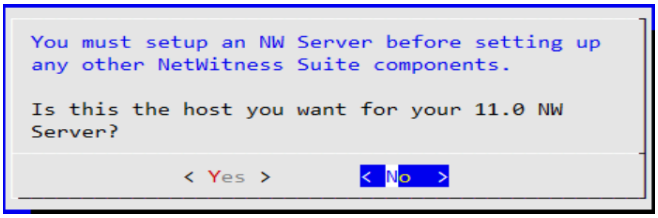
Cette opération démarre le programme d'installation et les conditions générales d'utilisation s'affichent.

Remarque : 1.) Lorsque vous parcourez les messages du programme d'installation, utilisez les touches directionnelles Haut et Bas pour naviguer entre les champs, utilisez la touche de tabulation pour naviguer d'une commande à l'autre (par exemple **<Oui>**, **<Non>**, **<OK>** et **<Annuler>**. Appuyez sur **Entrée** pour enregistrer votre réponse et passer au message suivant.
2.) Le programme d'installation adopte le modèle de couleurs du poste de travail ou de la console que vous utilisez pour accéder à l'hôte.
3.) Si vous spécifiez des serveurs DNS pendant l'exécution du programme d'installation (`nwsetup-tui`), ils doivent OBLIGATOIREMENT être valides (dans ce contexte, cela signifie valides lors de l'installation) et accessibles à `nwsetup-tui` pour continuer. Tous les serveurs DNS mal configurés provoquent l'échec de l'installation. Si vous avez besoin d'accéder au serveur DNS après l'installation, ce dernier étant inaccessible pendant l'installation, (par exemple, pour déplacer un hôte après la configuration qui aurait un ensemble différent de serveurs DNS), reportez-vous à la section Tâches à effectuer après l'installation.
Si vous ne spécifiez pas de serveurs DNS lors de la configuration (`nwsetup-tui`), vous devez sélectionner **1 Référentiel local (sur le serveur NW)** dans le message **NetWitness Suite Mise à jour du référentiel** à l'étape 12 (les serveurs DNS ne sont pas définis afin que le système ne puisse pas accéder au référentiel externe).

2. Naviguez jusqu'à **Accepter**, puis appuyez sur **Entrée**.



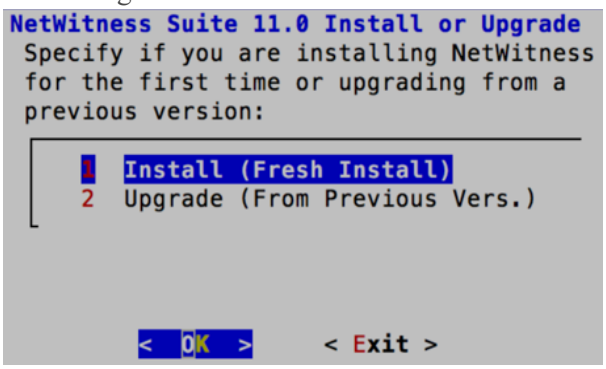
3. Le message « S'agit-il du serveur NW ? » s'affiche.



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

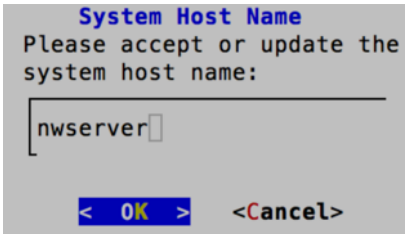
Attention : Si l'hôte choisi pour le serveur NW est incorrect et que vous terminez l'installation, vous devrez redémarrer le programme d'installation (étape 2) pour effectuer toutes les étapes suivantes pour corriger cette erreur.

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



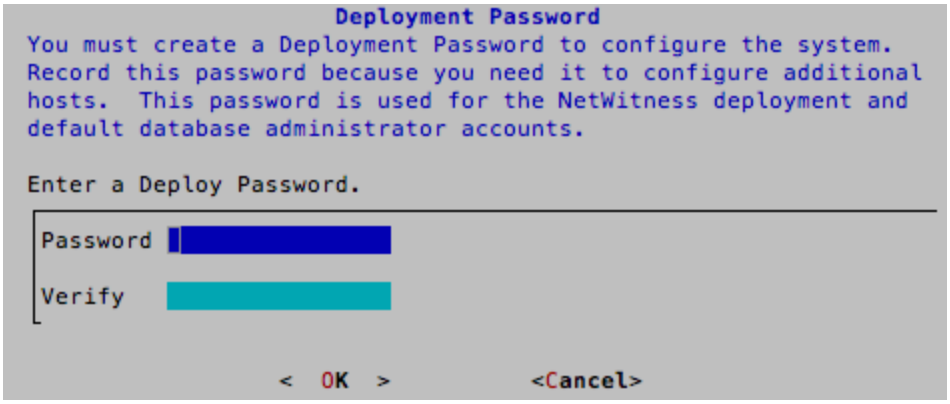
Appuyez sur **Entrée** (Installation est sélectionnée par défaut).

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



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.

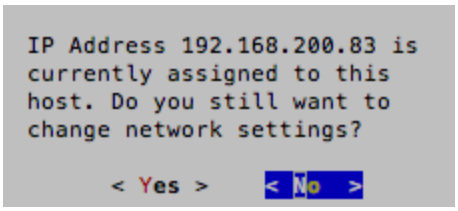
6. Le message « Mot de passe de déploiement » s'affiche.



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**.

7. Si :

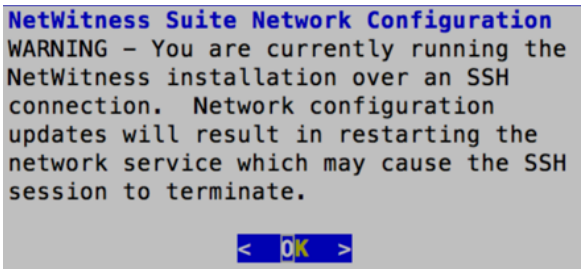
Le programme d'installation détecte une adresse IP valide pour cet hôte, le message suivant s'affiche.



Appuyez sur **Entrée** si vous souhaitez utiliser cette adresse IP et éviter de modifier les paramètres de votre réseau.

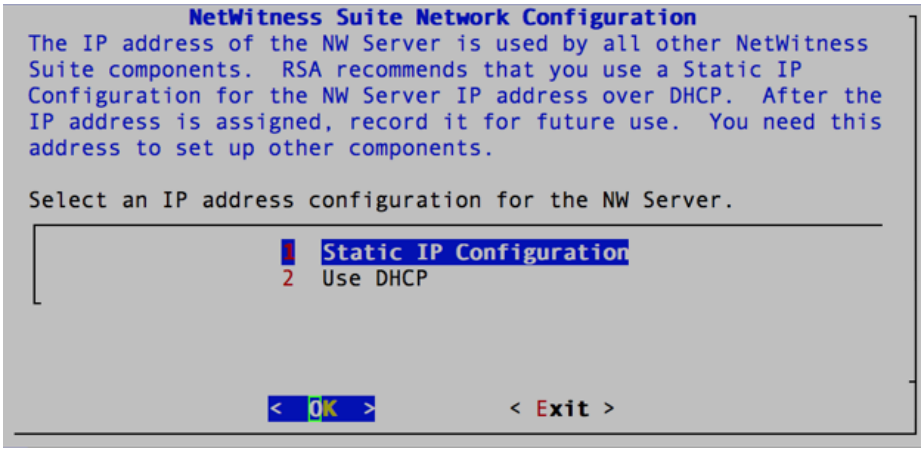
Naviguez jusqu'à **Oui** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** si vous souhaitez modifier la configuration IP disponible sur l'hôte.

Vous utilisez une connexion SSH, l'avertissement suivant s'affiche.



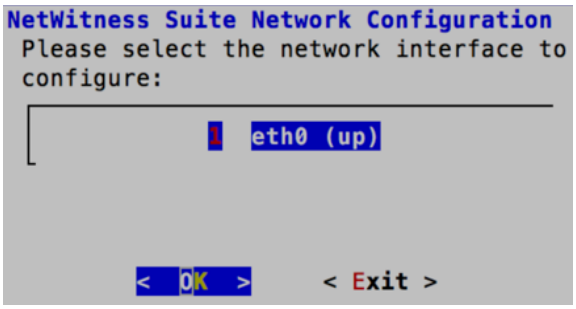
Appuyez sur **Entrée** pour fermer le message d'avertissement. Si le programme d'installation a détecté une configuration IP et que vous avez choisi de l'utiliser, le message Mettre à jour le référentiel s'affiche. Accédez à l'étape 12 et terminez l'installation.

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.



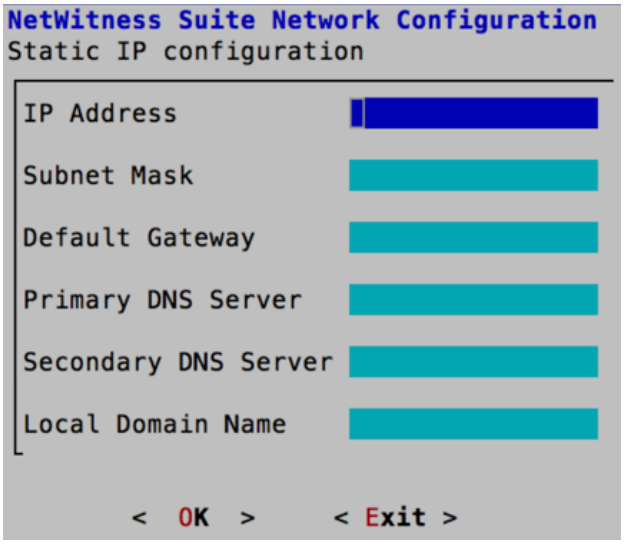
Naviguez jusqu'à **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** pour utiliser l'**adresse IP statique**.
Si vous souhaitez utiliser **DHCP**, utilisez la touche directionnelle Bas jusqu'à 2 Utiliser DHCP, puis appuyez sur **Entrée**.

8. Le message Configuration de réseau s'affiche.



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.

9. Le message Configuration d'adresse IP statique s'affiche.

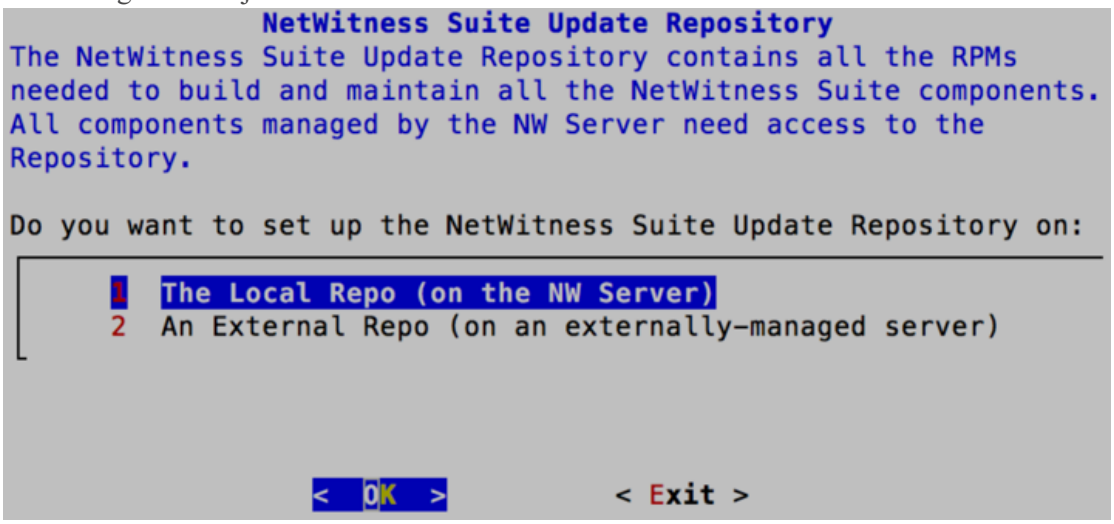


Saisissez les valeurs de configuration (en naviguant d'un champ à l'autre à l'aide de la touche directionnelle Bas), naviguez jusqu'à **OK** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**.

10. Si vous ne remplissez pas tous les champs obligatoires, le message d'erreur Tous les champs sont obligatoires s'affiche (les champs **Serveur DNS primaire**, **Serveur DNS secondaire** et **Nom de domaine local** ne sont pas obligatoires).
    Si la syntaxe ou la longueur de caractères utilisées pour un de ces champs est incorrecte, le message d'erreur *Nom du champ* non valide s'affiche.

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

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

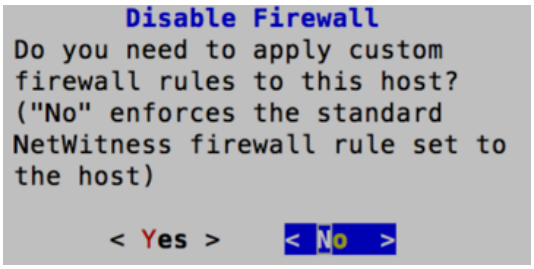


Appuyez sur **Entrée** pour choisir le **référentiel local** sur le serveur NW.

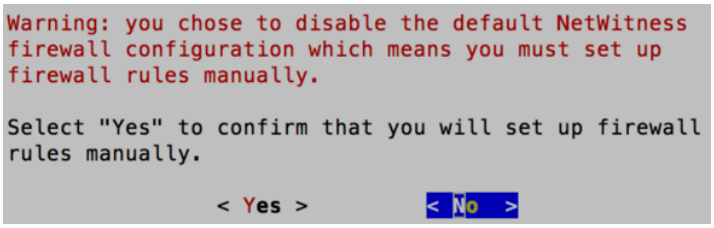
12. Pour :

    - Appliquer la configuration de pare-feu standard, appuyez sur **Entrée**.
    - Désactiver la configuration standard, naviguez jusqu'à **Oui** à l'aide de la touche de tabulation, puis appuyez sur **Entrée**.

      Le message Désactiver le pare-feu s'affiche.

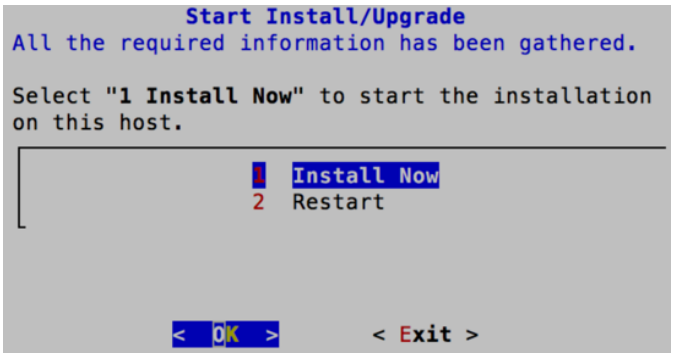
      

      Le message Confirmer la désactivation de la configuration du pare-feu s'affiche.

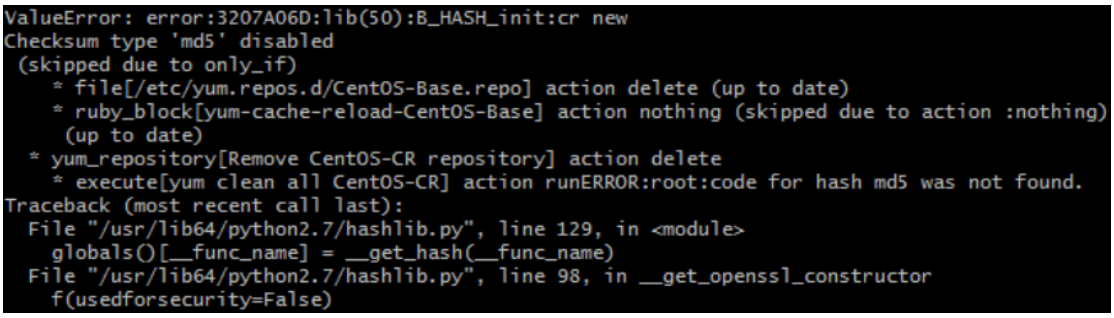
      Naviguez jusqu'à **Oui** à l'aide de la touche de tabulation, puis appuyez sur **Entrée** pour confirmer. (Appuyez sur **Entrée** pour utiliser la configuration de pare-feu standard).

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

    Appuyez sur **Entrée** pour installer la version 11.0 sur le serveur NW.
    Lorsque le message « Installation terminée » s'affiche, c'est que vous avez installé le serveur NW 11.0.0.0 sur cet hôte.

    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.



Configurer les hôtes (instances) dans NetWitness Suite

Configurez les différents hôtes et services comme décrit dans le *Guide de configuration des hôtes et des services RSA NetWitness® Suite* . Ce guide décrit aussi les procédures d'application des mises à jour et de préparation des mises à niveau des versions.

Remarque : Après avoir correctement démarré une instance, AWS lui attribue un nom d'hôte par défaut. Consultez la documentation « Modifier le nom et le nom d'hôte d'un hôte » dans RSA Link (https://community.rsa.com) pour obtenir des instructions sur la modification d'un nom d'hôte.

Configurer la capture de paquets

Vous pouvez intégrer une des solutions tierces suivantes au service Packet Decoder pour capturer des paquets dans le Cloud AWS :

- Gigamon® GigaVUE
- f5® BIG-IP

Intégrer Gigamon GigaVUE avec le service Packet Decoder

Deux tâches principales sont à effectuer pour configurer la solution de capture de paquets du fournisseur TAP tiers Gigamon® :

Tâche 1. Intégrer la solution Gigamon®.

Tâche 2. Configurer un tunnel sur Packet Decoder.

Tâche 1. Intégrer la solution Gigamon

La plate-forme de visibilité Gigamon® pour AWS sera disponible sur AWS Marketplace et activée par une licence BYOL. Une évaluation gratuite de trente jours sera également disponible.

Pour plus d'informations sur la solution Gigamon®, reportez-vous à la fiche produit de la plate-forme de visibilité Gigamon : « Gigamon® Visibility Platform for AWS Data Sheet » (https://www.gigamon.com/sites/default/files/resources/datasheet/ds-gigamon-visibility-platform-for-aws-4095.pdf).

Pour plus de détails sur le déploiement, reportez-vous au guide de mise en route de la plate-forme de visibilité Gigamon® pour AWS : « Gigamon® Visibility Platform for AWS Getting Started Guide » (https://www.gigamon.com/sites/default/files/resources/deployment-guide/dg-visibility-platform-for-aws-getting-started-guide-4111.pdf).

Une fois la « Session de surveillance » déployée dans le Gigamon GigaVUE-FM, vous pouvez configurer le tunnel du service Packet Decoder.

Tâche 2. Configurer un tunnel sur le service Packet Decoder

1. Ouvrez une session SSH sur le service Decoder.
2. Exécutez les chaînes de commandes suivantes.

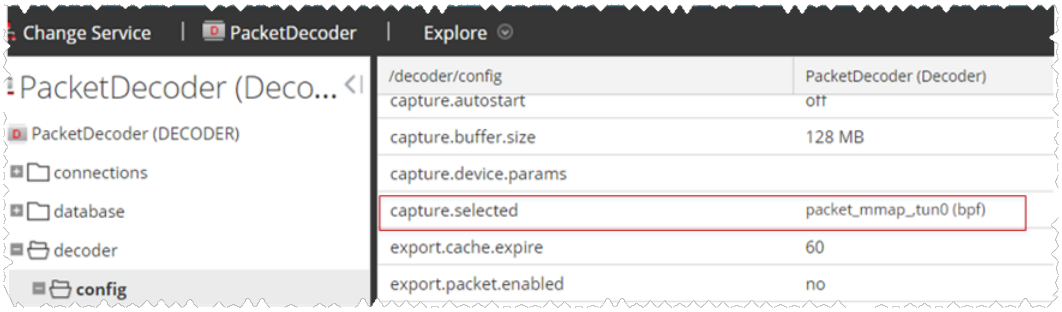
```
$ sudo ip link add tun0 type gretap local any remote <ip_address_of_
VSERIES_NODE_TUNNEL_INTERFACE> ttl 255

$ sudo ip link set tun0 up mtu <MTU-SIZE>

$ sudo ifconfig (to verify if the tunnel tun0 is being listed in the
list of interfaces)

$ sudo lsmod | grep gre ( to make sure if the below kernel modules
are running:

ip_gre 18245 0

ip_tunnel 25216 1)

If they are not running then execute the below commands to enable the
modules

$ sudo modprobe act_mirred

$ sudo modprobe ip_gre
```

3. Créez une règle de pare-feu dans le service Packet Decoder pour autoriser le trafic via le tunnel.
   a. Ouvrez le fichier `iptables`.
      `vi /etc/sysconfig/iptables`
   b. Ajoutez la ligne `-A INPUT -p gre -j ACCEPT` avant l'instruction `commit`.
   c. Redémarrez `iptables` en exécutant les commandes suivantes.
      `service iptables restart`

4. Définissez l'interface dans le service Packet Decoder.

   a. Connectez-vous à NetWitness Suite, sélectionnez le nœud `decoder/config` dans la vue Explorer du service Packet Decoder.

   b. Définissez la commande `capture.selected = packet_mmap_,tun0`.

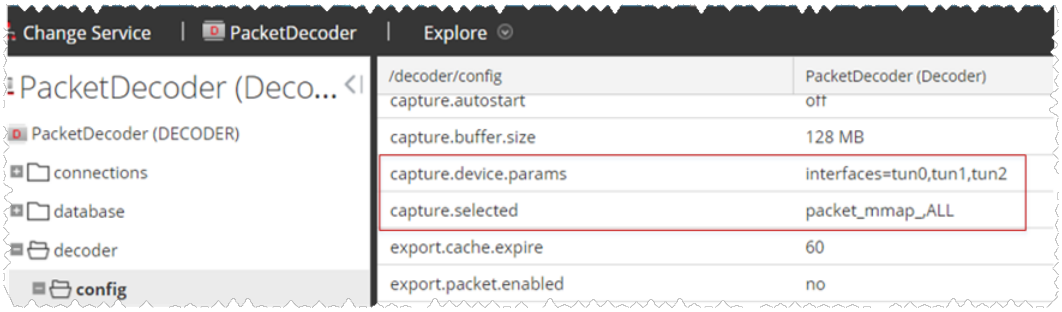


5. (Conditionnel) - Si vous avez plusieurs tunnels sur le service Packet Decoder.

   a. Redémarrez le service Decoder après avoir créé le tunnel dans le service Packet Decoder.

   b. Connectez-vous à NetWitness Suite, sélectionnez le nœud `decoder/config` dans la vue Explorer du service Packet Decoder et définissez les paramètres suivants.

   ```
   capture.device.params = interfaces=tun0,tun1,tun2
   capture.selected = packet_mmap_,All
   ```



6. Redémarrez le service Decoder.

   ```
   $ sudo restart nwdecoder
   ```

   L'utilisateur doit maintenant être prêt à capturer le trafic réseau dans le service Decoder.

Procédez comme suit pour créer un nouveau projet et obtenir la clé de votre projet.

Intégrer f5® BIG-IP au service Packet Decoder

IG-IP Virtual Edition (VE) est un serveur virtuel et un répartiteur de charge à la volée. Un exemple d'utilisation courant serait pour la zone f5® d'être un serveur Web virtuel qui présente une adresse IP/un nom d'hôte unique gérant les demandes vers un pool de serveurs Web dans le Cloud.

Tout le trafic vers RSA NetWitness® Suite transite par le serveur virtuel f5® BIG-IP VE.

Les fonctions BIG-IP du serveur virtuel clonent tout le trafic vers un ordinateur désigné en réécrivant les adresses Mac et en les insérant dans un sous-réseau partagé avec le renifleur de destination. Ce document explique comment configurer le service Decoder en tant que renifleur.

Informations relatives au déploiement de f5® BIG-IP VE

f5® BIG-IP VE pour AWS sera disponible sur AWS Marketplace et activé par une licence BYOL. Une évaluation gratuite de trente jours sera également disponible.

Pour plus d'informations sur cette solution, reportez-vous à la fiche produit f5® BIG-IP DNS (https://www.f5.com/pdf/products/big-ip-dns-datasheet.pdf).

Tâche 1 : Configurer une instance de serveur virtuel BIG-IP VE

Configurer une instance de serveur virtuel BIG-IP VE selon les instructions fournies dans la documentation « BIG-IP Virtual Edition 12.1.0 and Amazon Web Services: Multi-NIC Manual » (https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-ve-multi-nic-setup-amazon-ec2-12-1-0.html). Effectuez toutes les étapes jusqu'à la fin, « Création d'un serveur virtuel ».

Ce serveur virtuel effectue la capture des paquets. Vous devrez peut-être créer plusieurs serveurs virtuels en fonction de votre volume.

Dans le cadre de la création du serveur virtuel, vous devez disposer d'au moins un serveur dans votre domaine NetWitness Suite pour gérer le trafic acheminé par le serveur virtuel (par exemple, vous pouvez créer une autre instance dans AWS pour héberger le serveur interne).

Tâche 2 : Créer un pool de clones

1. Assurez-vous que votre service Decoder dispose d'une interface réseau sur le même sous-réseau que l'une des interfaces réseau de l'instance BIG-IP VE.
   Le pool de clones envoie des paquets au service Decoder en réécrivant les adresses MAC et en les envoyant à une interface réseau. La réécriture des adresses MAC peut être utilisée pour acheminer les paquets vers un autre sous-réseau.
2. Configurez le pool de clones au sein du serveur virtuel BIG-IP VE en fonction des instructions fournies dans l'article « K13392 : Configuring the BIG-IP system to send traffic to an intrusion detection system (11.x - 13.x) » (https://support.f5.com/kb/en-us/solutions/public/13000/300/sol13392.html) relatif à la configuration du système BIG-IP pour acheminer le trafic vers un système de détection des intrusions.
   Ce document explique comment créer le pool de clones et comment faire copier à un serveur virtuel existant le trafic vers le pool de clones. Dans ce cas, il faut placer l'instance du service Decoder dans le pool de clones.

Instructions

Les instructions suivantes vous aideront à configurer correctement la capture de paquets à l'aide de BIG-IP VE.

- L'instance du service Decoder doit avoir sa propre adresse IP sur l'un des sous-réseaux identiques à ceux de BIG-IP VE. BIG-IP utilise cette adresse IP pour identifier le service Decoder comme faisant partie du pool de clones.
- Lorsque vous ajoutez l'instance du service Decoder au pool de clones, BIG-IP vous demande un numéro de port en plus de l'adresse IP. Ce numéro de port n'a pas d'importance pour le trafic cloné. Le service Decoder recevra tout le trafic cloné, quel que soit le numéro de port utilisé ici.
- Par défaut, le sous-réseau AWS, partagé par le service Decoder et BIG-IP VE, n'autorisera pas le trafic cloné à passer de l'interface BIG-IP VE à l'interface du service Decoder. Vous devez désactiver la **`source/dest. check`** sur les interfaces réseau du service Decoder, mais aussi de BIG-IP VE dans AWS.
- Par défaut, l'instance du service Decoder ne doit disposer que d'une seule interface réseau, eth0. Le service Decoder capture le trafic sur cette interface, mais il peut également y recevoir le trafic d'administration. RSA recommande d'utiliser des règles réseau pour exclure le trafic ssh et nwdecoder du flux de capture. Il s'agit des ports 22 (ssh) et 50004/56004 (nwdecoder).

Conseils de résolution des problèmes

Il convient de dépanner deux zones si les paquets ne sont pas acceptés par le service Decoder.

- Assurez-vous que BIG-IP VE envoie ces paquets à l'interface appropriée.
  L'instance BIG-IP VE contient tcpdump. Veillez à l'utiliser pour vérifier que les paquets clonés sont envoyés à l'interface prévue. Dans le cas contraire, la configuration du pool de clones ou du serveur virtuel générera un problème.
- Assurez-vous que le service Decoder reçoit des paquets.
  `tcpdump` est installé sur le service Decoder. Utilisez-le pour vérifier que le service Decoder reçoit les paquets. S'il ne capture pas les paquets, vérifiez que
  - La **`source/dest. check`** AWS est arrêtée.
  - Le service Decoder se trouve sur le même sous-réseau que l'interface dont se sert BIG-IP VE pour cloner les paquets.

Conseils de configuration de l'instance AWS

Remarque : Ces recommandations ont été qualifiées pour RSA Security Analytics version 10.6.3. Ces recommandations peuvent être utilisées comme base pour 11.0.0.0 et ajustées en fonction des besoins.

Remarque : Pour obtenir une description des termes et des abréviations utilisés dans cette rubrique, reportez-vous à la section Abréviations et autre terminologie utilisées dans ce guide.

Cette rubrique contient les paramètres de configuration de l'instance minimale AWS recommandés pour les composants virtuels RSA NetWitness® Suite de la pile.

- Instance EC2 :
  - Type d'instance minimale - **m4-2xlarge** est le type d'instance minimale requis pour les fichiers AMI des composant NetWitness Suite afin qu'ils puissent fonctionner.
  - Ajustements du type d'instance - vous devez ajuster le type d'instance en fonction de votre taux d'acquisition, du contenu et des analyseurs, des rapports sur les tableaux de bord, des rapports planifiés, des procédures d'enquête et des utilisateurs actifs.
  - Paramètres recommandés - les paramètres recommandés pour l'instance du composant SA figurant dans les tableaux ci-dessous ont été calculés dans les conditions suivantes.
    - Taux d'acquisition de 15 000 EPS et utilisation de 1,5 Gbit/s.
    - Tous les composants ont été intégrés.
    - Le flux de log comprenait un Log Decoder, un Concentrator et un Archiver.
    - Le flux de paquets comprenait un Packet Decoder et un Concentrator.
    - Respond recevait des alertes de Reporting Engine et d'Event Stream Analysis.
    - La charge en arrière-plan comprenait des rapports, des graphiques, des alertes, des procédures d'enquête et des réponses.
- Volumes EBS (stockage)

  Contactez le support client RSA (https://community.rsa.com/docs/DOC-1294) pour obtenir de l'aide sur la façon d'augmenter le nombre de volumes en fonction de vos besoins de stockage à l'aide de la Calculatrice de dimensionnement et de définition du périmètre RSA.

  Remarque : Le volume d'index du Concentrator doit être alloué sur le disque SSD IOPS provisionné.

- Index
- Méta
- Session
- Paquet

Archiver

Instance EC2			
EPS	**Type d'instance**	**Amélioration de la mise en réseau activée**	**Type de location : Dédiée - Exécuter une instance dédiée**
5 000	m4.xlarge Nombre de CPU : 4 Mémoire : 16 Go	Non	Oui
10 000	m4.2xlarge Nombre de CPU : 8 Mémoire : 32 Go	Non	Oui
15 000	m4.4xlarge Nombre de CPU : 16 Mémoire : 64 Go	Non	Oui

Volumes EBS (stockage)			
Volumes	**Périphérique**	**Type de volume**	**Débit IOPS/de base**
/ (racine)	/dev/sda1	Usage général de disque SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	Usage général de disque SSD	N/A
archiver	/dev/sdg	Disque dur à débit optimisé	240 Mo/s
workbench	/dev/sdh	Disque dur à débit optimisé	N/A

Broker

Instance EC2		
Type d'instance	**Amélioration de la mise en réseau activée**	**Type de location - Dédiée - Exécuter une instance dédiée**
m4.xlarge Nombre de CPU : 4 Mémoire : 16 Go	Non	Oui

Volumes EBS (stockage)			
Volumes	**Périphérique**	**Type de volume**	**Débit IOPS/de base**
/ (racine)	/dev/sda1	Usage général de disque SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	Usage général de disque SSD	N/A
broker	/dev/sdg	Usage général de disque SSD	N/A

Concentrator - Flux de log

Instance EC2			
EPS	**Type d'instance**	**Amélioration de la mise en réseau activée**	**Type de location - Dédiée - Exécuter une instance dédiée**
5 000	m4.xlarge Nombre de CPU : 4 Mémoire : 16 Go	Non	Oui
10 000	m4.2xlarge Nombre de CPU : 8 Mémoire : 32 Go	Non	Oui
15 000	m4.4xlarge Nombre de CPU : 16 Mémoire : 64 Go	Non	Oui

Volumes EBS (stockage)			
Volumes	**Périphérique**	**Type de volume**	**Débit IOPS/de base**
/ (racine)	/dev/sda1	Usage général de disque SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	Usage général de disque SSD	N/A
index,session	/dev/sdg	IOPS provisionnées	10 000
metadb	/dev/sdh	Disque dur à débit optimisé	240 Mo/s

Solutions de flux de paquets

Concentrator - Solution Gigamon

Instance EC2			
Mbit/s-Gbit/s	Type d'instance	Amélioration de la mise en réseau activée	Type de location - Dédiée - Exécuter une instance dédiée
500 Mbits/s	c4.4xlarge Nombre de CPU : 16 Mémoire : 30 Go	Non	Oui
1 000 Mbits/s	c4.8xlarge Nombre de CPU : 36 Mémoire : 60 Go	Non	Oui
1,5 Gbit/s	m4.10xlarge Nombre de CPU : 40 Mémoire : 160 Go	Non	Oui

Concentrator - Solution f5 BIG-IP

À mettre à jour lorsque les tests de performances f5 BIG-IP sont terminés.

Instance EC2			
Mbit/s-Gbit/s	**Type d'instance**	**Amélioration de la mise en réseau activée**	**Type de location - Dédiée - Exécuter une instance dédiée**
230 Mbits/s	m4.4xlarge Nombre de CPU : 16 Mémoire : 64 Go	Non	Non

Volumes EBS (stockage)			
Volumes	**Périphérique**	**Type de volume**	**Débit IOPS/ de base**
/ (racine)	/dev/sda1	Usage général de disque SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	Usage général de disque SSD	N/A
index,session	/dev/sdg	IOPS provisionnées	15 000
metadb	/dev/sdh	Disque dur à débit optimisé	240 Mo/s

Decoder - Solution Gigamon

Instance EC2			
Mbit/s-Gbit/s	Type d'instance	Amélioration de la mise en réseau activée	Type de location - Dédiée - Exécuter une instance dédiée
500 Mbits/s	c4.2xlarge Nombre de CPU : 8 Mémoire : 15 Go	Oui	Oui
1 000 Mbits/s	c4.4xlarge Nombre de CPU : 16 Mémoire : 30 Go	Oui	Oui
1,5 Gbit/s	c4.8xlarge Nombre de CPU : 36 Mémoire : 60 Go	Oui	Oui

Decoder : Solution f5 BIG-IP

À mettre à jour lorsque les tests de performances f5 BIG-IP sont terminés.

Instance EC2			
Mbit/s-Gbit/s	Type d'instance	Amélioration de la mise en réseau activée	Type de location - Dédiée - Exécuter une instance dédiée
230 Mbits/s	m4.4xlarge Nombre de CPU : 16 Mémoire : 64 Go	Non	Non

Volumes EBS (stockage)			
Volumes	**Périphérique**	**Type de volume**	**Débit IOPS/de base**
/ (racine)	/dev/sda1	Usage général de disque SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	Usage général de disque SSD	N/A
index,session,méta	/dev/sdg	Disque dur à débit optimisé	240 Mo/s
paquet	/dev/sdh	Disque dur à débit optimisé	240 Mo/s

ESA et Context Hub sur la base de données Mongo

	Instance EC2		
EPS	**Type d'instance**	**Amélioration de la mise en réseau activée**	**Type de location - Dédiée - Exécuter une instance dédiée**
9 000	m4.2xlarge Nombre de CPU : 8 Mémoire : 32 Go	Non	Oui
18 000	r4.2xlarge Nombre de CPU : 8 Mémoire : 61 Go	Non	Oui
Taux d'agrégation de 30 000	r4.4xlarge Nombre de CPU : 16 Mémoire : 122 GB	Non	Oui

Volumes EBS (stockage)			
Volumes	**Périphérique**	**Type de volume**	**Débit IOPS/de base**
/ (racine)	/dev/sda1	Usage général de disque SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	Usage général de disque SSD	N/A
apps (/opt/rsa)	/dev/sdg	Usage général de disque SSD	N/A

Log Collector (Protocoles de collecte de fichiers, Syslog et Netflow)

Instance EC2			
EPS	**Type d'instance**	**Amélioration de la mise en réseau activée**	**Type de location - Dédiée - Exécuter une instance dédiée**
30 000 NON SSL	c4.2xlarge Nombre de CPU : 8 Mémoire : 15 Go	Non	Oui

Volumes EBS (stockage)			
Volumes	**Périphérique**	**Type de volume**	**Débit IOPS/de base**
/ (racine)	/dev/sda1	Usage général de disque SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	Usage général de disque SSD	N/A
logcollector	/dev/sdg	Usage général de disque SSD	N/A

Log Decoder

Instance EC2			
EPS	**Type d'instance**	**Amélioration de la mise en réseau activée**	**Type de location - Dédiée - Exécuter une instance dédiée**
5 000	c4.2xlarge Nombre de CPU : 8 Mémoire : 15 Go	Oui	Oui
10 000	c4.4xlarge Nombre de CPU : 16 Mémoire : 30 Go	Oui	Oui
15 000	c4.8xlarge Nombre de CPU : 36 Mémoire : 60 Go	Oui	Oui

Volumes EBS (stockage)			
Volumes	**Périphérique**	**Type de volume**	**Débit IOPS/de base**
/ (racine)	/dev/sda1	Usage général de disque SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	Usage général de disque SSD	N/A
index,session,méta	/dev/sdg	Disque dur à débit optimisé	240 Mo/s
paquet	/dev/sdh	Disque dur à débit optimisé	240 Mo/s

Serveur NetWitness, Reporting Engine, Respond et intégrité

Instance EC2		
Type d'instance	**Amélioration de la mise en réseau activée**	**Type de location - Dédiée - Exécuter une instance dédiée**
m4.2xlarge Nombre de CPU : 8 Mémoire : 32 Go	Non	Oui
m4.4xlarge Nombre de CPU : 16 Mémoire : 64 Go	Non	Oui

Volumes EBS (stockage)			
Volumes	**Périphérique**	**Type de volume**	**Débit IOPS/de base**
/ (racine)	/dev/sda1	Usage général de disque SSD	N/A
usr,var,opt,home,tmp	/dev/sdf	Usage général de disque SSD	N/A
uax,ipdb	/dev/sdg	Usage général de disque SSD	N/A
redb,rehome	/dev/sdh	Usage général de disque SSD	N/A