RSA NETWITNESS® SUITE

Guide de déploiement Azure

pour la version 11.0.0.0

Informations de contact

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

Marques commerciales

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

Contrat de licence

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

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

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

Licences tierces

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

Remarque sur les technologies de chiffrement

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

Distribution

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

mars 2018

Sommaire

Guide de déploiement Azure

Avant de pouvoir déployer RSA NetWitness® Suite dans Azure 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 NetWitness Suite « Débit ».
- Utilisez Chrome comme navigateur (Internet Explorer n’est pas pris en charge).

Recommandations en matière d'environnement Azure

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

- En fonction des besoins en ressources des différents composants, suivez les bonnes pratiques pour utiliser le système et le stockage dédié de manière appropriée.
- Créez des répertoires Concentrator pour la base de données de l’index sur un disque SSD.

Abréviations et autre terminologie utilisées dans ce guide

Abréviations	Description
Azure	Azure est la plate-forme de Cloud computing public de Microsoft. Elle fournit un éventail de services Cloud, comme le calcul, l’analytique, le stockage et la mise en réseau. Vous pouvez piocher dans ces services pour développer et de faire évoluer de nouvelles applications ou exécuter des applications existantes, dans le Cloud public.
BYOL	Utiliser ses propres licences (Bring your own licensing)
CPU	Unité centrale
EPS	Événements par seconde

Abréviations	Description
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
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 Azure.
RAM	Random Access Memory (également nommé mémoire)
Sécurité	Ensemble de règles de pare-feu. Consultez le déploiement : 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.
SSD	Disque SSD
CPU virtuels	Unité de traitement central virtuelle (également nommée processeur virtuel)
VHD	Disque dur virtuel (Virtual Hard Disk)
VM	Machine virtuelle

Abréviations	Description
vRAM	Mémoire virtuelle. Il s’agit de la mémoire d’une machine virtuelle.

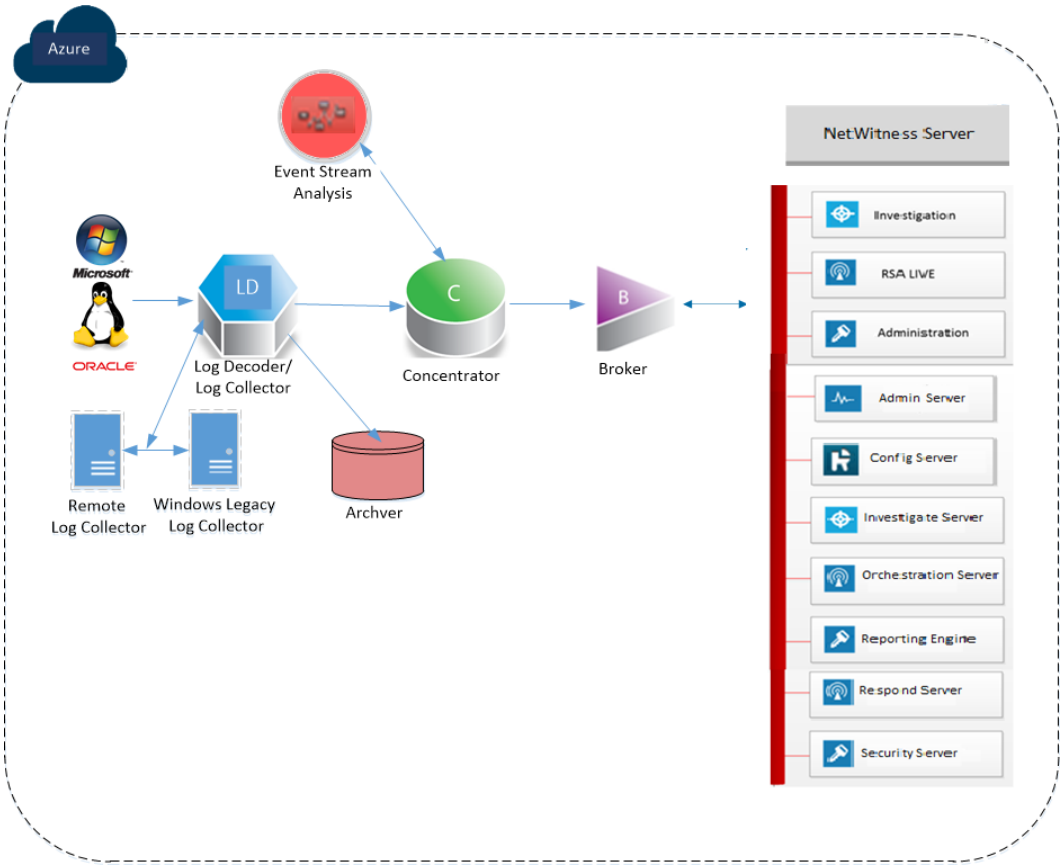
Scénarios de déploiement Azure

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

- **Log Decoder** reçoit les logs collectés par le Log Collector. Le Log Collector collecte 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**, **RSA Live**, **Administration** et autres aspects de l'interface utilisateur.

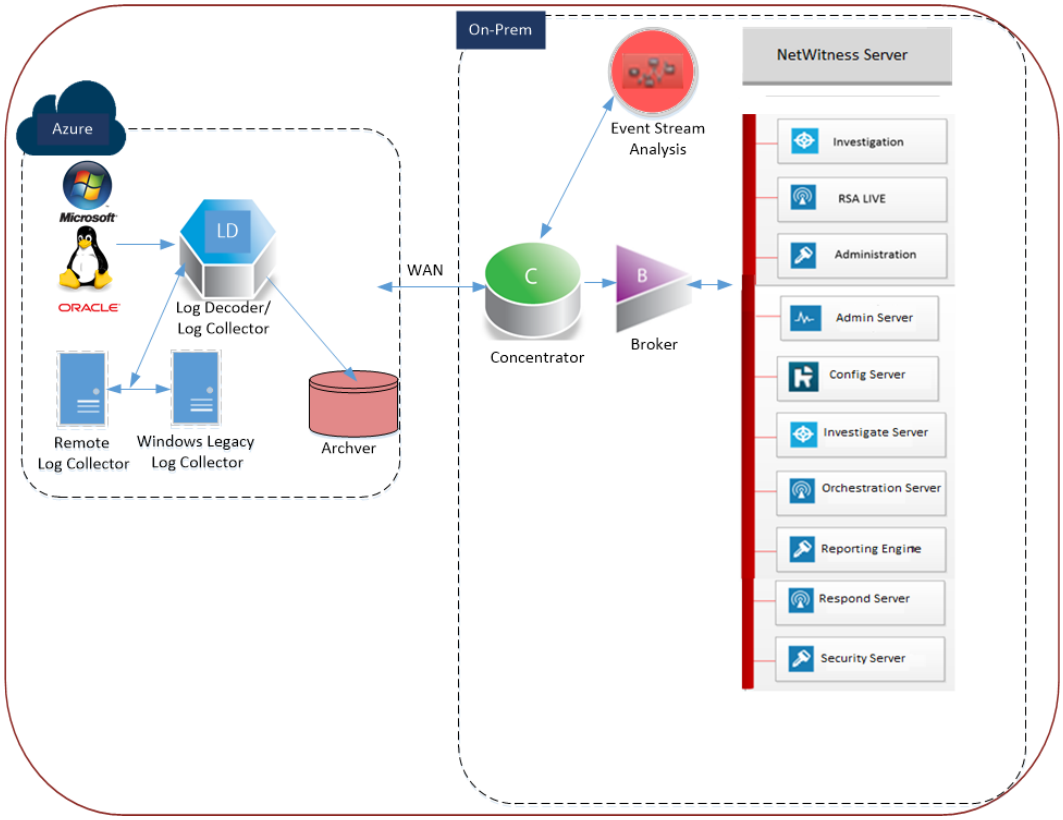
Visibilité Azure complète de la pileNetWitness Suite

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



Déploiement hybride - Log Decoder

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



Services pris en charge

RSA fournit les services NetWitness Suite suivants.

- Serveur NetWitness
- Serveur d'administration
- Serveur de configuration
- Serveur Enquêter
- Serveur d'orchestration
- Reporting Engine
- Serveur Respond
- Serveur de sécurité

- Archiver
- Broker
- Concentrator
- Event Stream Analysis
- Log Decoder
- Remote Log Collector

Conseils de configuration de machine virtuelle Azure

Remarque : Ces recommandations ont été qualifiées pour RSA Security Analytics version 10.6.4. 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 Guide de déploiement Azure.

Cette rubrique contient les paramètres de configuration de machines virtuelles Azure recommandés pour les composants virtuels NetWitness Suite (NW) de la pile.

- Machine virtuelle :
  - Les paramètres recommandés dans les tableaux du composant NetWitness Suite de la machine virtuelle ci-dessous ont été calculés dans les conditions suivantes.
    - Taux d'acquisition de 15 000 EPS.
    - Tous les composants ont été intégrés.
    - Le flux de log comprenait un Log Decoder, un Concentrator et un Archiver.
    - Incident Management recevait des alertes de Reporting Engine et d'Event Stream Analysis.
    - La charge en arrière-plan comprenait des rapports, des graphiques, des alertes, des procédure d'enquête et la gestion des incidents.
- VHD (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 : Pour les taux d'EPS plus élevés, le volume d'index de Concentrator doit être alloué aux disques SSD.

Taille de la machine virtuelle			
Composant	**EPS**	**Traitement**	**Taille de la machine virtuelle**
Archiver	15 000	Nombre de CPU : 16 Mémoire : 112 Go	D14 standard v2
Broker	15 000	Nombre de CPU : 4 Mémoire : 14 Go	DS3 Standard v2
Concentrator	15 000	Nombre de CPU : 16 Mémoire : 112 Go	DS14 Standard v2
ESA et Context Hub	15 000	Nombre de CPU : 20 Mémoire : 140 Go	D15 standard v2
Log Collector	15 000 NON SSL	Nombre de CPU : 8 Mémoire : 16 Go	F8 standard
Log Decoder	15 000	Nombre de CPU : 16 Mémoire : 112 Go	D14 standard v2
Serveur NW*	15 000	Nombre de CPU : 16 Mémoire : 112 Go	D14 standard v2

* Reporting Engine, Respond et Intégrité peuvent résider sur le même hôte Serveur NetWitness.

Liste de contrôle et règles du déploiement Azur

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

Règles

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

- Utilisez toujours des adresses IP privées lorsque vous provisionnez les machines virtuelles Azure NetWitness Suite.
- 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.

Liste de contrôle

Étape	Description	√
1.	Étape 1. Déployer l'hôte du serveur NW dans Azure	
2.	Étape 2. Déployer les services de base des composants dans Azure	
3.	Étape 3. Configurer les machines virtuelles hôtes dans RSA NetWitness® Suite .	

Étape 1. Déployer l'hôte du serveur NW dans Azure

Effectuez les tâches suivantes pour déployer un Serveur NetWitness (Serveur NW) sur une machine virtuelle (VM) dans l'environnement Cloud Azure.

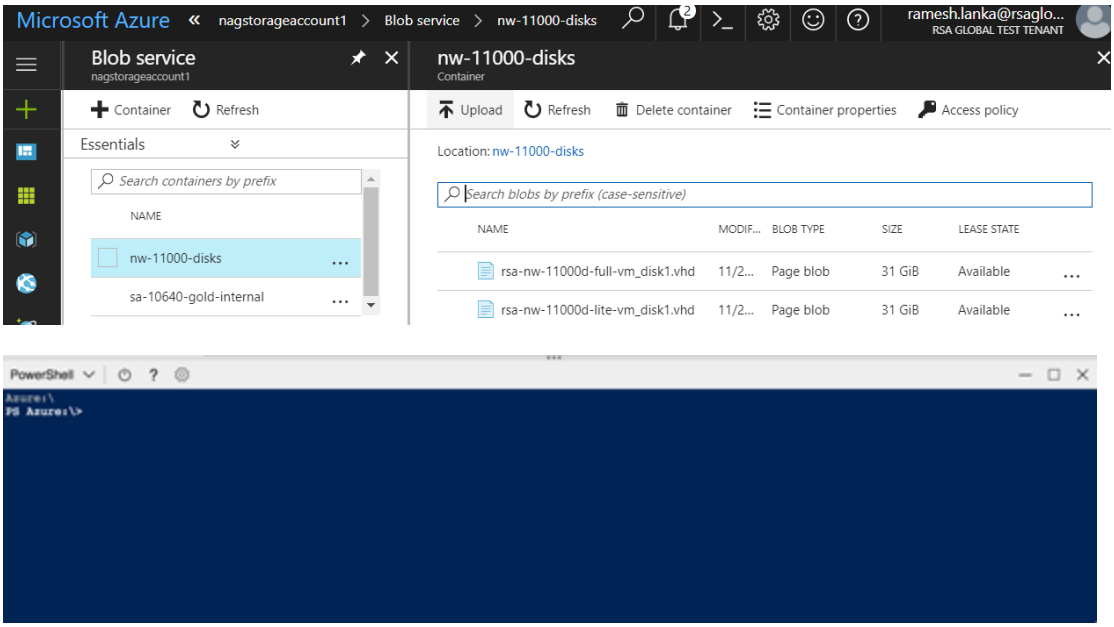
Remarque : Il n'est pas obligatoire de déployer le serveur SA dans l'environnement Cloud Azure pour déployer d'autres composants (reportez-vous à la section Scénarios de déploiement Azure).

- Tâche 1. -Télécharger Serveur NW des disques durs virtuels
- Tâche 2. - Créer Serveur NWune image
- Tâche 3. Créer une machine virtuelle (VM)

Tâche 1. - Télécharger Serveur NW des disques durs virtuels

Procédez comme suit pour télécharger Serveur NW des disques durs virtuels vers Azure.

1. Contactez le Support client RSA (https://community.rsa.com/docs/DOC-1294) pour ouvrir une demande d'assistance demandant les VHD du serveur NW. Une licence valide de débit sera nécessaire.
2. Le support client met à jour le dossier avec des URI VHD.
3. Via le portail Azure, ouvrez la CLI Powershell.



- Vous aurez besoin d'un compte de stockage, d'un service blob et d'une configuration de conteneur. C'est là que les VHD seront copiés. Une fois en place, vous pouvez exécuter la commande suivante au sein de la CLI Powershell du portail Azure.
  Par exemple :
  `az storage blob copy start --account-name customerstorageacct --destination-container nwserver --destination-blob rsa-nw-11000d-full-vm_disk1.vhd --source-uri 'https://netwitnessazure.blob.core.windows.net/nwvhdstore/rsa-nw-11000d-full-vm_disk1.vhd?sv=2017-04-17&ss=b&srt=co&sp=rl&se=2017-11-30T16:40:02Z&st=2017-11-30T08:40:02Z&spr=https&sig=tBETVk9y%2BpTFNjAsgulzirXK99MVRt18GNRBSEsx97k%3D'"`

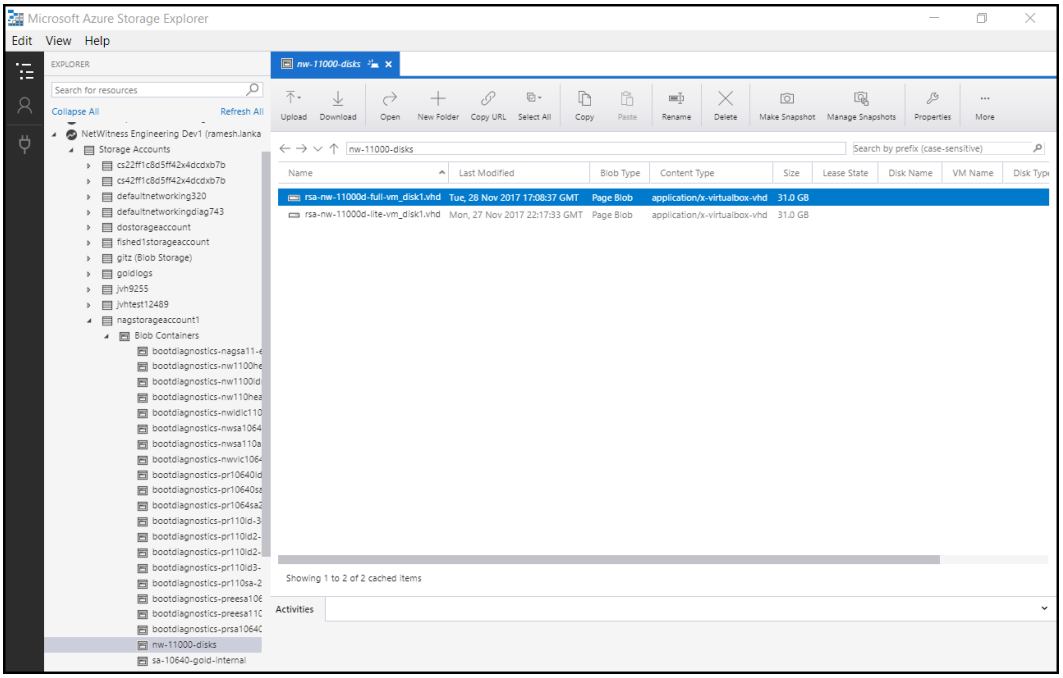
  Les indicateurs mis en surbrillance dans la commande ci-dessus devront être mis à jour. La commande ci-dessus copiera le VHD. Du fait qu'il existe deux VHD, version Lite et complète, il faut réaliser deux téléchargements.

  --account-name : Nom du compte de stockage.

- --destination-container : nom du conteneur.
- --destination-blob : nom du blob de destination ou du VHD du serveur NW. Si l'existe, il sera remplacé.
- --source-uri : un URI de token SAS sera fourni dans le cas du support client RSA.

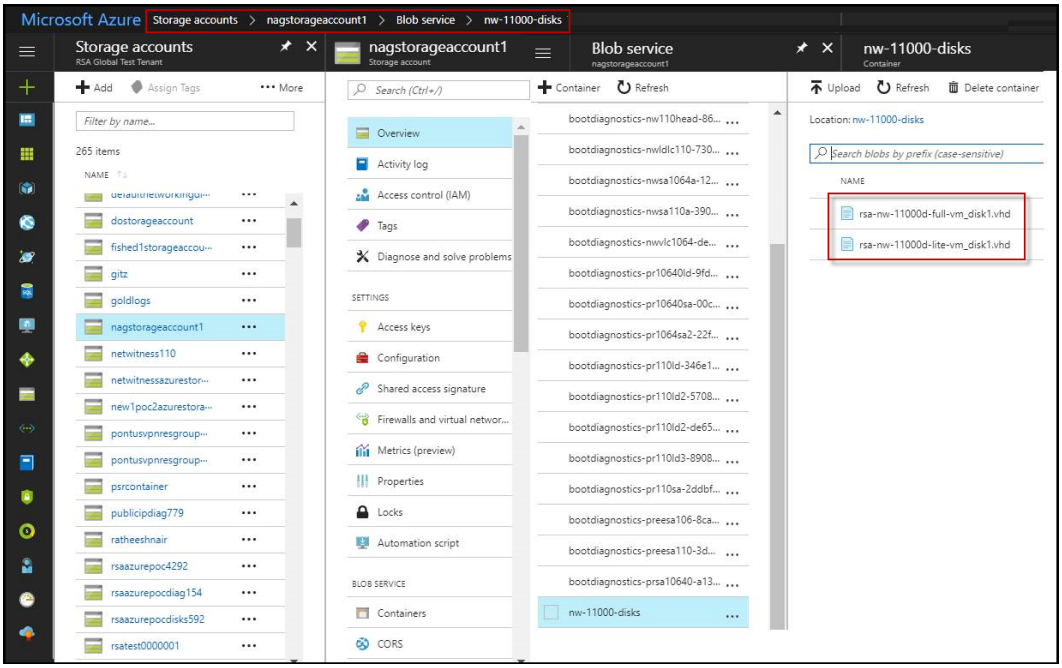
4. Lorsque les VHD sont correctement copiés, vous devez créer une image et une machine virtuelle.
5. Vérifiez que tous les VHD du serveur NW sont téléchargés dans le Cloud Azure.

Remarque : Vous pouvez également utiliser l'utilitaire Windows de l'Explorateur de Microsoft Azure Storage (http://storageexplorer.com/) pour vérifier que tous les disques durs virtuels à partir de l'emplacement d'abonnement suivant existent. Cet utilitaire facilite la gestion du contenu de votre système de stockage.



a. Connectez-vous au portail Azure (https://portal.azure.com).

b. Dans le volet de droite, cliquez sur **Comptes de stockage** > **netwitnessazurestorage1** > **Service Blob** > **nwazurevhdstore**.



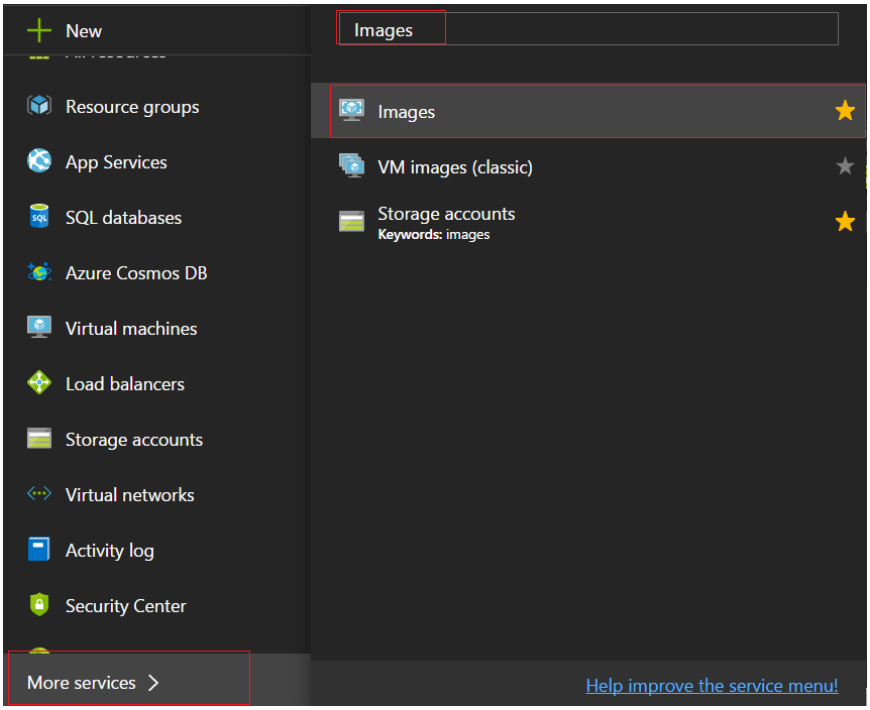
6. (Facultatif) Dans l'Explorateur Azure, accédez au groupe **NetWitness** > **Comptes de stockage** > **netwitnessazurestorage1**) > **Conteneurs Blob** > **nwazurevhdstore**). La capture d'écran suivante montre un exemple de contenu d'un conteneur de stockage.

Tâche 2. - Créer l'image serveur NW

Procédez comme suit pour créer une image serveur NW dans Azure à partir de disques durs virtuels téléchargés.

1. Connectez-vous à https://portal.azure.com.
2. Dans le volet de gauche, cliquez sur **Plus de services** et filtrer par images.

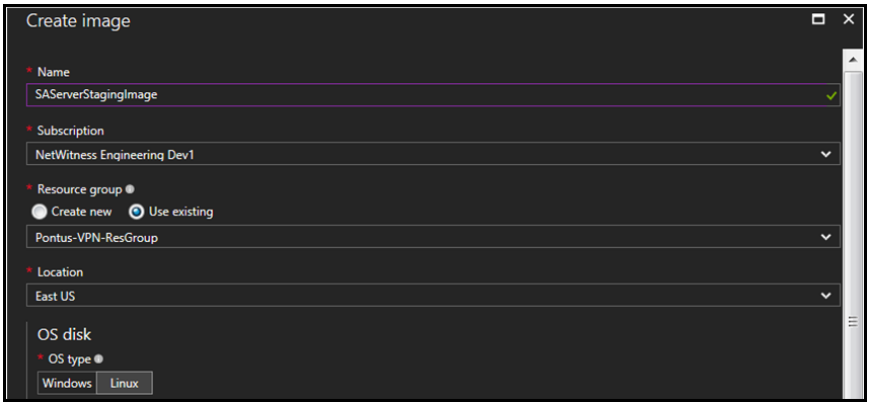
3. Cliquez sur **Images**.



4. Créez et configurez l'image.

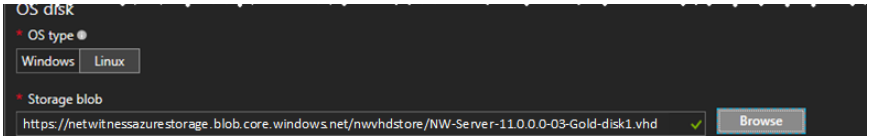
   a. Cliquez sur **Ajouter**.

   b. Saisissez un nom pour l'image, sélectionnez le groupe de ressources approprié, sélectionnez un emplacement valide et définissez le disque du système d'exploitation sous Linux.
   Dans le **Blob de stockage**, naviguez vers l'emplacement où les disques durs virtuels ont été téléchargés.

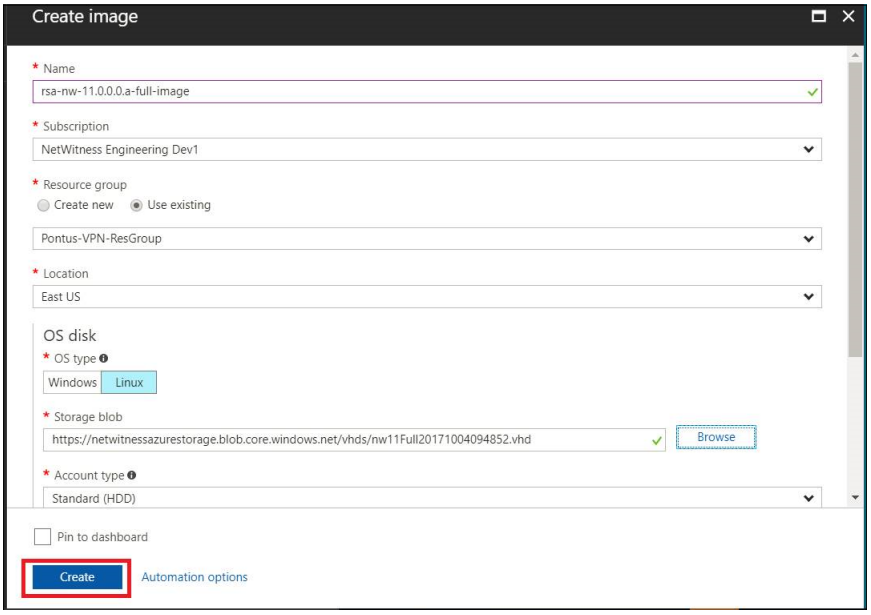


   c. Sélectionnez **https://netwitnessazurestorage.blob.core.windows.net/nwvhdstore/SA-Server-11.0.0.0-03-Gold-disk1.vhd** dans le champs du **Stockage blob du disque du**

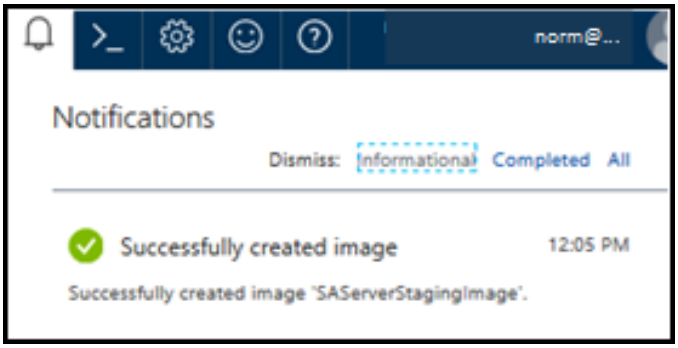
système d'exploitation.



d. Assurez-vous que **Standard (disque dur)** est sélectionné pour le **Type de compte**.
La capture d'écran suivante illustre la vue **Créer une Image** terminée.



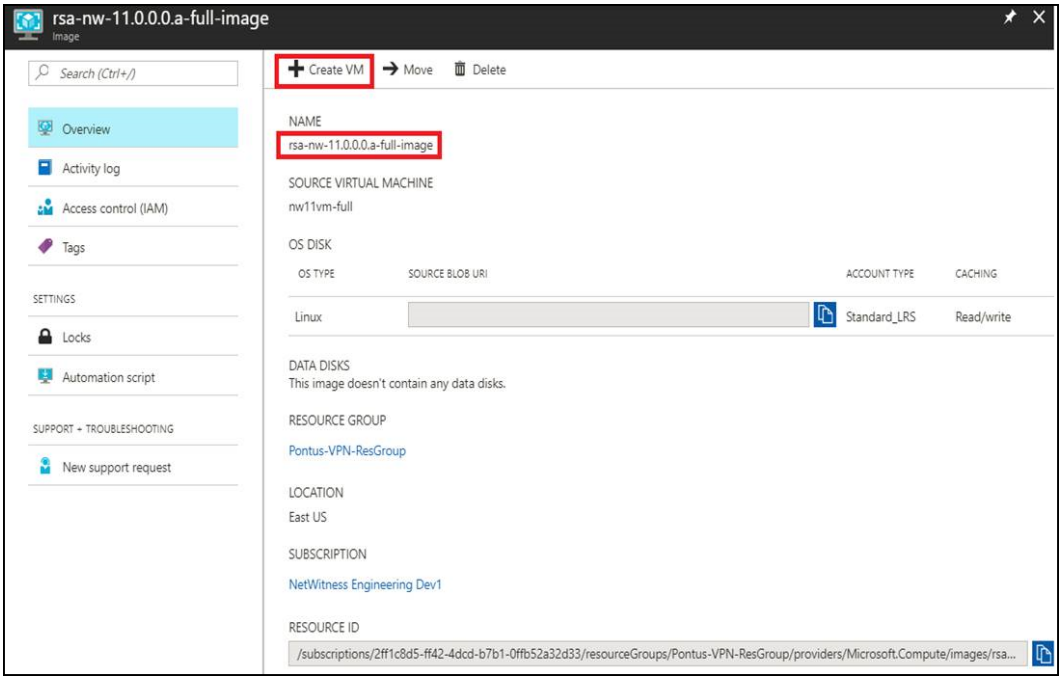
e. Cliquez sur **Créer** pour créer l'Image.
La confirmation suivante s'affiche lors de la création de l'image.



Tâche 3. Créer une machine virtuelle (VM)

Procédez comme suit pour créer une machine virtuelle dans Azure à partir de l'image serveur SA.

1. Accédez à **Images**, puis cliquez sur **Créer une machine virtuelle**.



Section **1 Informations de base - Configurer des paramètres de base**est sélectionnée.

2. Définir des valeurs pour tous les champs.

   a. Dans le champ **Nom**, saisissez un nom défini par l'utilisateur (par exemple, **NWServer1100**).

   b. Dans le champ **Type de disque de la machine virtuelle**, sélectionnez**Disque dur** dans la liste déroulante.

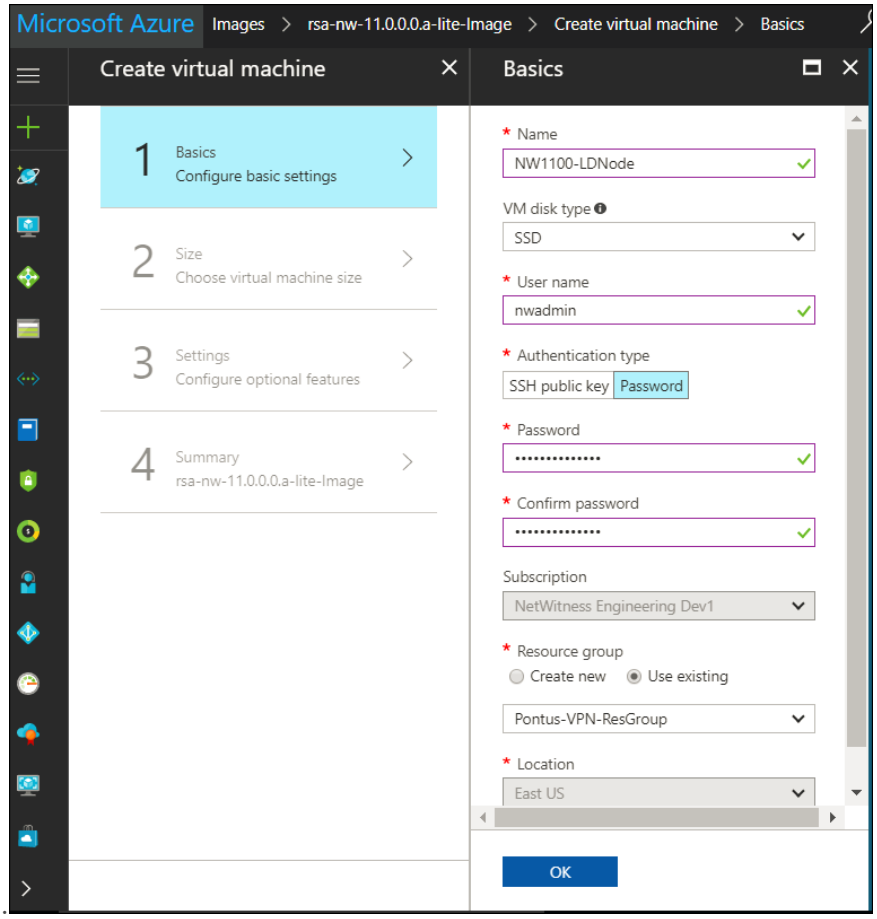
   Attention : Le nom d'utilisateur et le mot de passe que vous définissez sont utilisés pour vous connecter au système en tant qu'utilisateur non-administrateur. N'utilisez pas l'utilisateur root (la connexion ne dispose pas des autorisations de superutilisateur). Vous devez modifier le mot de passe root lors de la première connexion à la machine virtuelle en exécutant la commande`su passwd root`. Ceci est une étape critique à ne pas manquer. Vous ne pouvez pas utiliser `root` comme nom d'utilisateur (spécifique à Azure).

   c. Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur valide.

   d. Dans le champ **Type d'authentification**, cliquez sur **Mot de passe** et saisissez un mot de passe fort qui est une combinaison de lettres en minuscule, en majuscule, de chiffres ainsi qu'un symbole (par exemple, **Netwitness@123**).

   e. Assurez-vous que les valeurs sélectionnées dans les champs **Abonnement**, **Groupe de ressources et Emplacement** sont corrects.

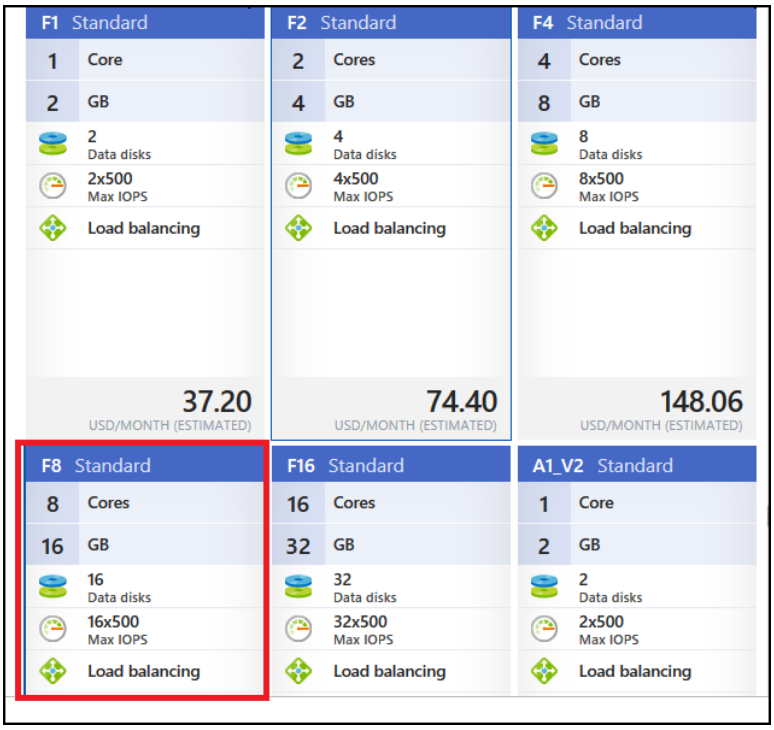
f. Cliquez sur **OK**



La section **2 Dimension - Choisir une taille pour la machine virtuelle** est sélectionnée.

3. Cliquez sur ***taille-requise-en-fonction-de-la-capacité*** (par exemple, **F8 Standard**), puis cliquez sur **Sélectionner**.

Remarque : Le dimensionnement repose sur les exigences de capacité de votre entreprise (reportez-vous à la section Conseils de configuration de machine virtuelle Azure pour connaître les recommandations RSA pour les tailles de machines virtuelles en fonction des taux de capture des logs. La taille minimale recommandée par RSA pour le serveur SA est **F8 Standard**.



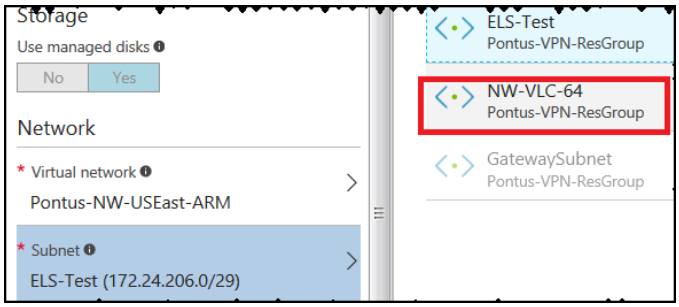
La section **3 Paramètres : Configurer les fonctions en option** est sélectionnée.

4. Cliquez et définissez les champs.

   a. Dans le champ **Stockage**, assurez-vous que **Utilisez gérer les disques** est réglé sur **Oui**.

   b. Dans le champ **Réseau**, sélectionnez :

   - Un **Réseau virtuel** et un **Sous-réseau** valides.



   - **Aucune** pour l'**Adresse IP publique**.
     RSA vous recommande **Aucune** pour l'**Adresse IP publique** (cela n'est pas obligatoire). Vous pouvez attribuer une adresse IP publique, mais il est contraire aux bonnes pratiques d'attribuer une adresse IP publique à des données basées dans Cloud Azure.

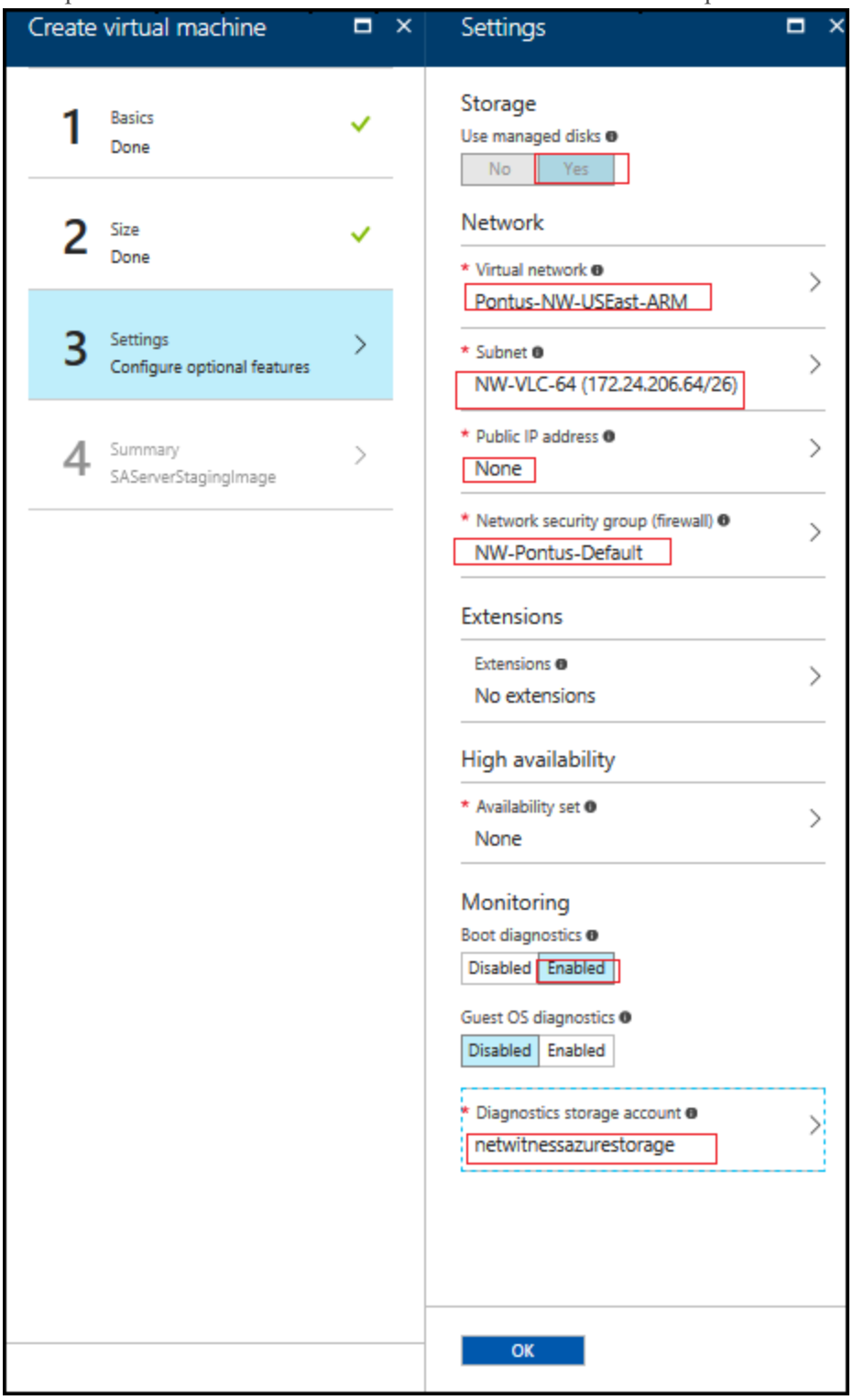
   - Un **Groupe de sécurité réseau** valide.
     Pour plus d'informations sur les groupes de sécurité réseau, consultez la

documentation de Microsoft Azure (https://docs.microsoft.com/fr-fr/azure/virtual-network/virtual-networks-nsg).

c. Dans le champ Surveillance, sélectionnez :

- **Activé** pour **Démarrer les diagnostics**
- **Activé** pour les **Diagnostics des systèmes d'exploitation invités**
- Un **compte de stockage de diagnostics valide**

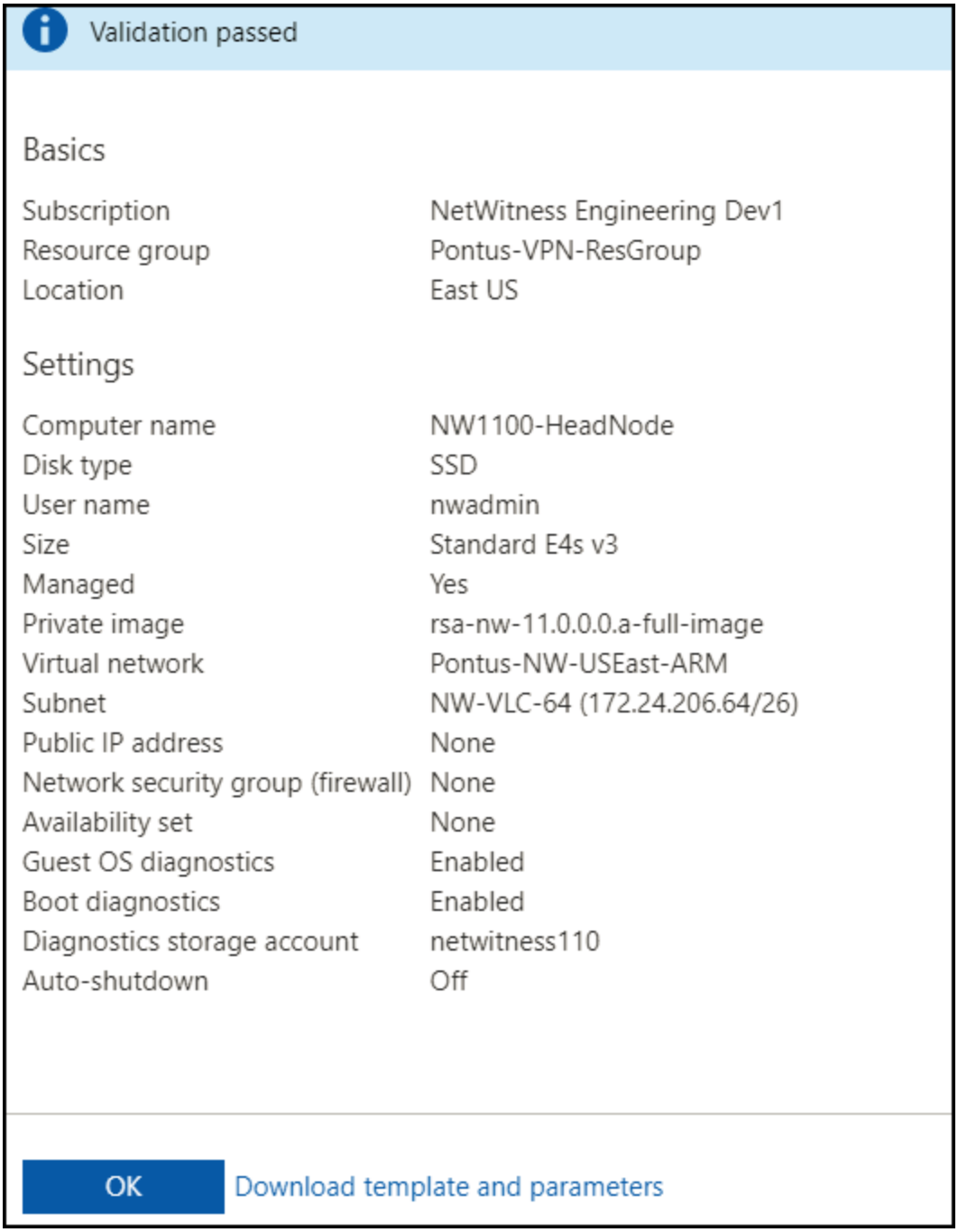
La capture d'écran suivante illustre un Panneau Paramètres complété.



d. Cliquez sur **OK**.

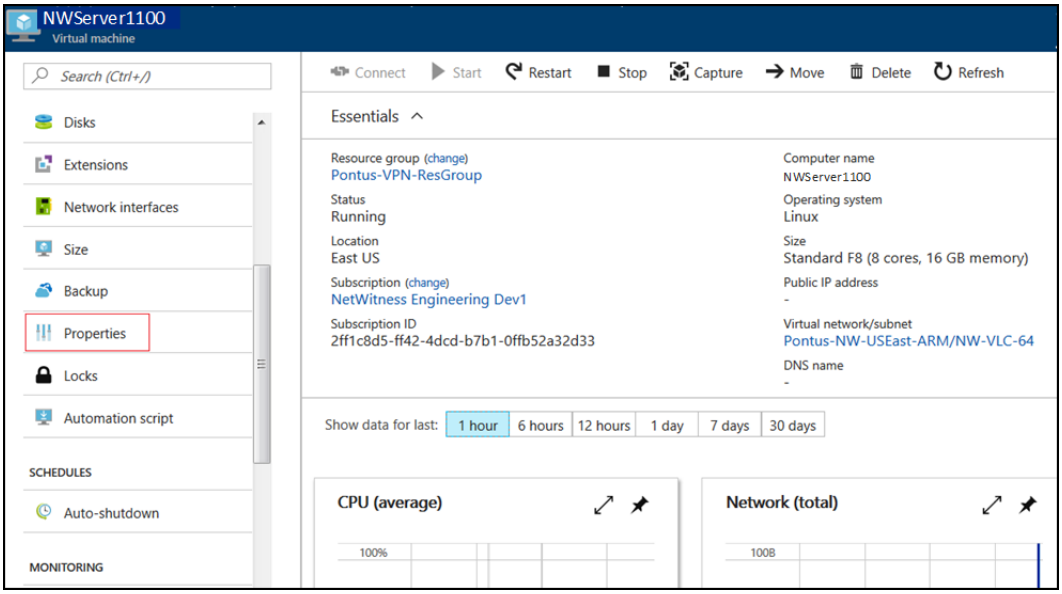
La section **4 Résumé – SAServerStagingImage** est sélectionnée.

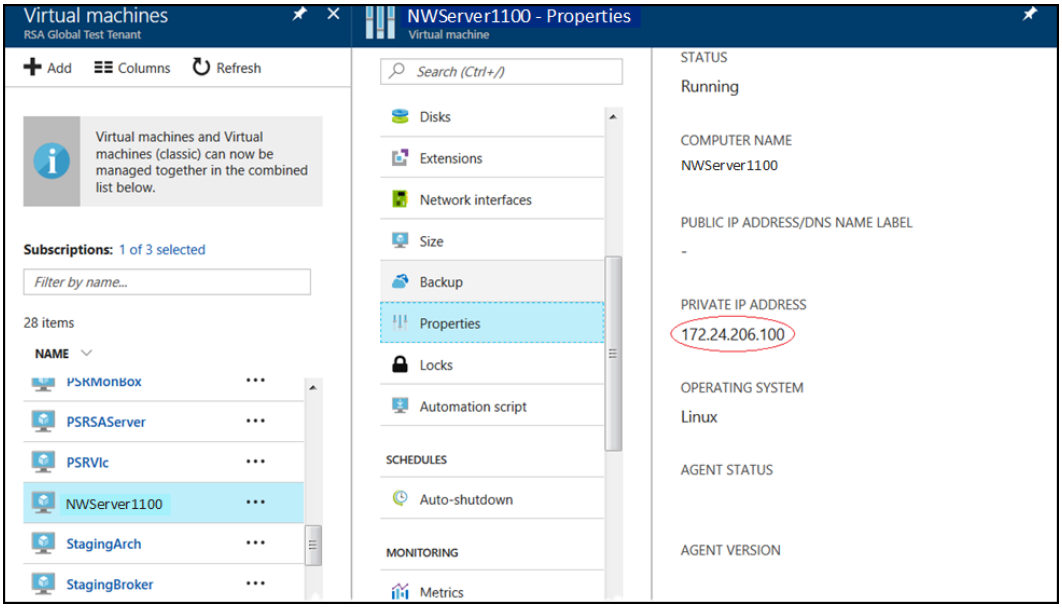
5. Vérifiez que la Validation a bien été effectuée, puis cliquez sur **OK**.



Vous savez que le déploiement de machines virtuelles de serveur NW est réussi lorsque l'état de la machine virtuelle s'affiche comme **En cours d'exécution**.

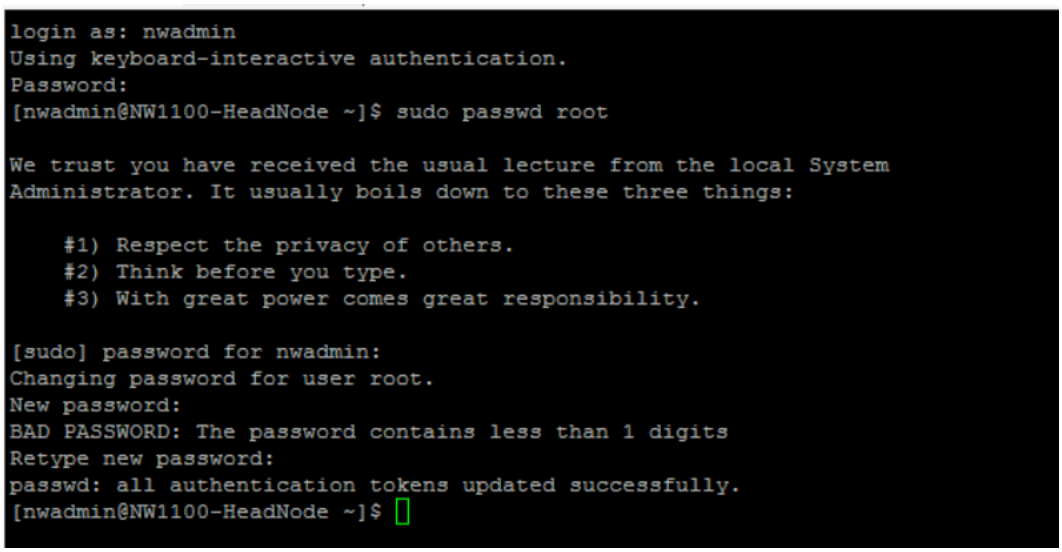
6. Cliquez sur **Propriétés** pour afficher plus d'informations sur l'**Adresse IP**.





7. Ouvrez une session SSH sur la machine virtuelle avec le nom d'utilisateur que vous avez spécifié à l'étape 2d de la Tâche 3 et réinitialisez le mot de passe **root**. Utilisez la chaîne de commande `su passwd root` pour réinitialiser le mot de passe root, comme illustré dans la

capture d'écran suivante.



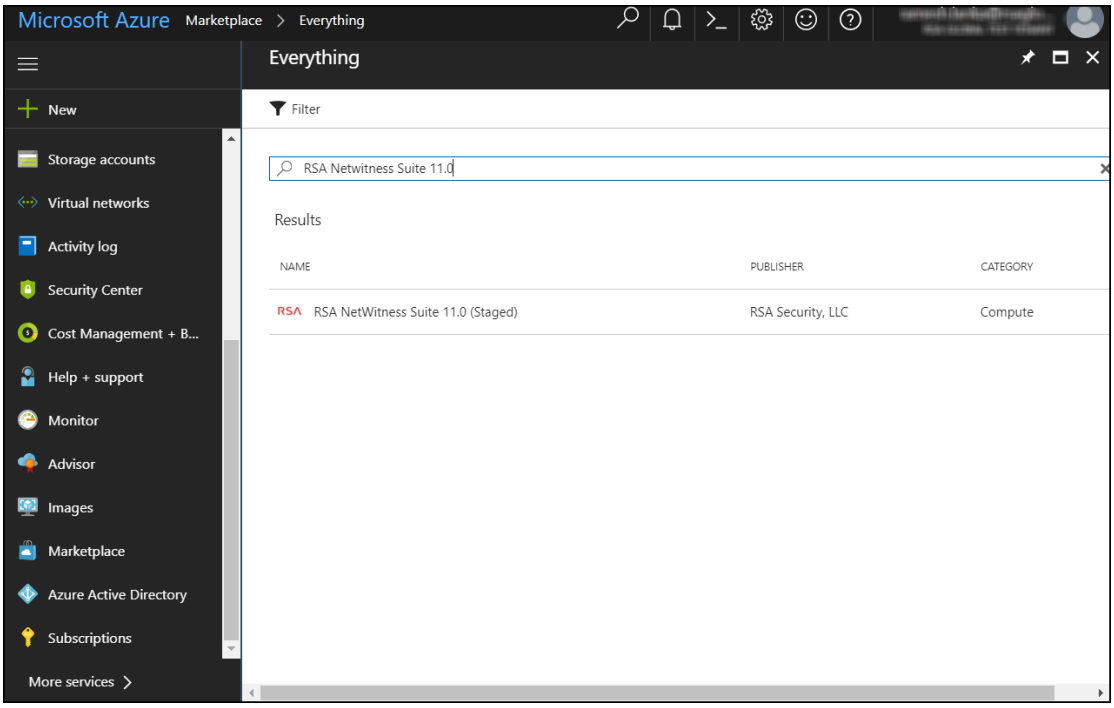
8. Fermez la session SSH en cours et ouvrez-en une nouvelle avec le nom d'utilisateur et le mot de passe **root** créés à l'étape précédente.

Remarque : L'étape 8 est une étape critique, à effectuer une seule fois lors d'un nouveau déploiement. Si vous n'effectuez pas cette étape, l'Interface utilisateur de Security Analytics se chargera pas.

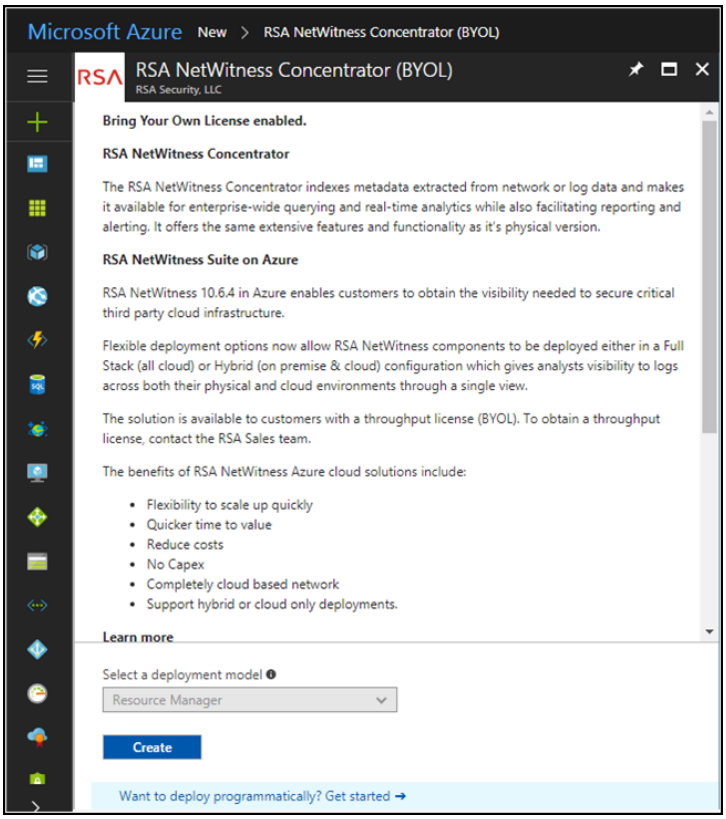
Étape 2. Déployer les services de base des composants dans Azure

Exécutez la procédure suivante pour configurer les services des composants RSA NetWitness® Suite de base sur des machines virtuelles (VM) dans l'environnement Cloud Azure.

1. Accédez à azuremarketplace.microsoft.com et connectez-vous avec vos informations d'identification.
2. Recherchez RSA.



3. Cliquez sur le service de base RSA NetWitness® Suite (par exemple, **RSA NetWitness Concentrator**), puis cliquez sur **Créer**.



L'assistant **Créer une machine virtuelle** s'affiche avec la section **1 Informations de base** sélectionnée.

4. Fournissez les informations de base.

   a. Spécifiez le **Nom** d'une machine virtuelle (par exemple, **Concentrator**).

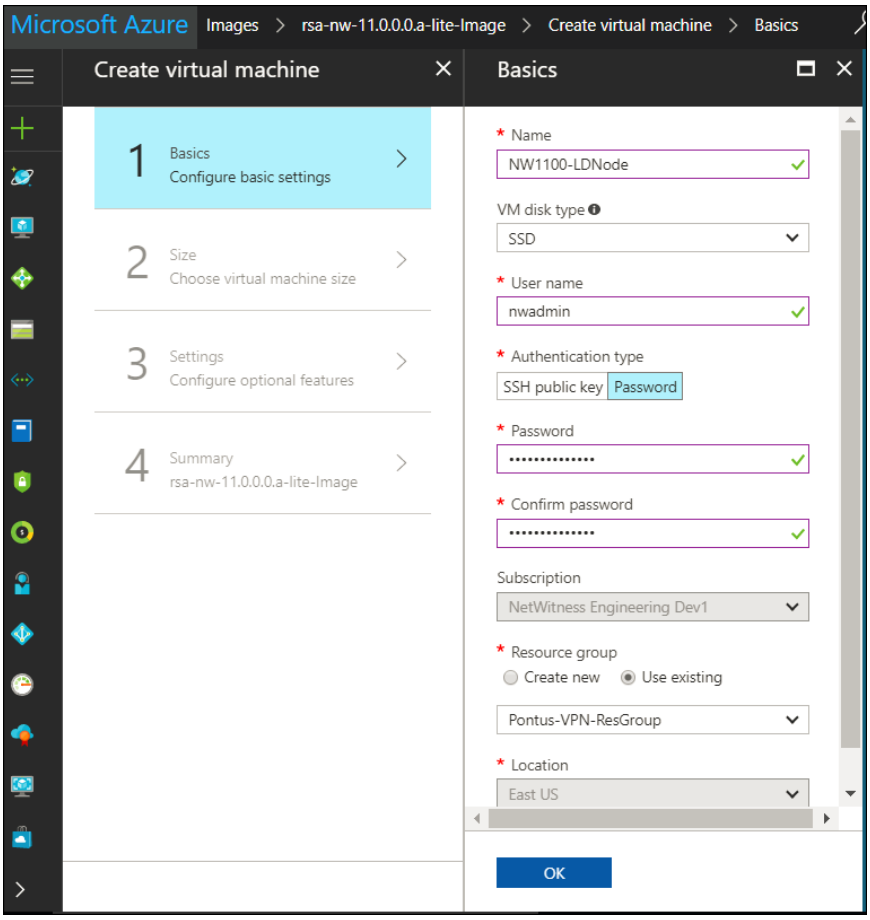
   b. Sélectionnez **SSD** pour le **type de disque de la machine virtuelle** du Concentrator. Sélectionnez les disques durs de tous les autres composants.

      Les disques SSD sont plus performants que les disques durs.

   c. Sélectionnez **Mot de passe** en guise de **Type d'authentification**.

   d. Saisissez vos informations d'identification (c'est-à-dire le **Nom d'utilisateur** et le **Mot de passe**), puis **confirmez le mot de passe**.

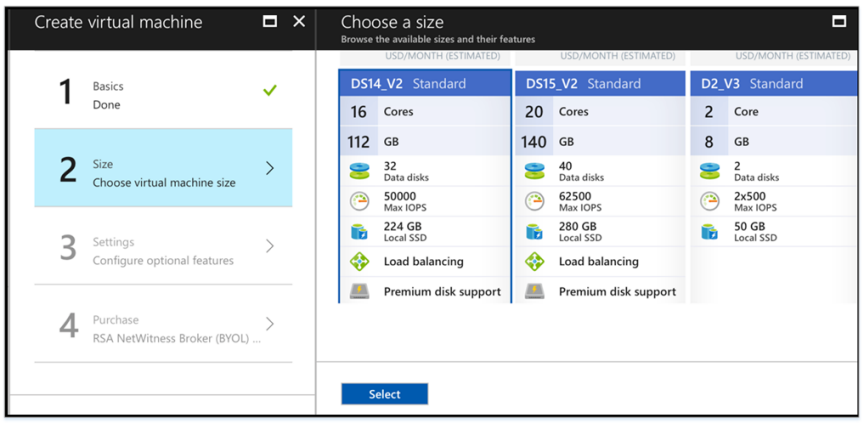
   e. Cliquez sur le bouton **OK**.



Azure valide vos caractéristiques de **base** et la section **2 Taille** est sélectionnée.

5. Cliquez sur la taille de la machine virtuelle appropriée (par exemple, **Standard DS14 v2** pour le Concentrator) correspondant au service, puis cliquez sur **Sélectionner** pour la **taille** d'une machine virtuelle.

   Reportez-vous à la section Conseils de configuration de machine virtuelle Azure pour connaître les tailles de machines virtuelles recommandées par RSA pour chaque service.



Azure valide vos caractéristiques de **Taille** et la section **3 Paramètres** est sélectionnée.

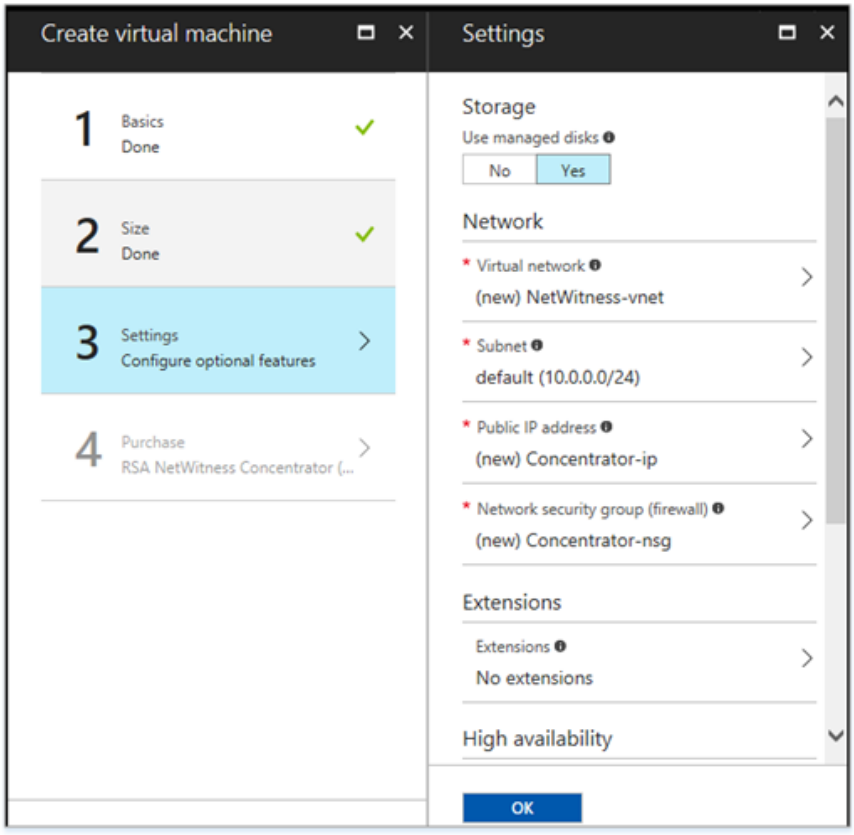
6. Définissez les **paramètres**.

   a. Dans le champ **Stockage**, assurez-vous que **Utiliser les disques gérés** est défini sur **Oui**.

   b. Sous **Réseau** :

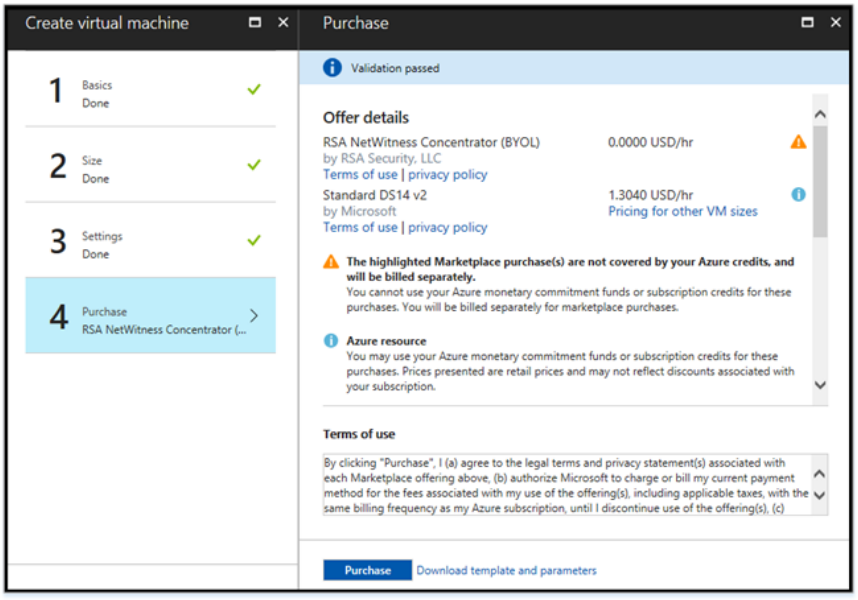
   - Définissez le **Réseau virtuel**, le **Sous-réseau** et l'**Adresse IP publique** en fonction des exigences de votre réseau.
   - Indiquez un **Groupe de sécurité réseau** valide.

     Pour plus d'informations sur les groupes de sécurité réseau, consultez la documentation Microsoft Azure (https://docs.microsoft.com/fr-fr/azure/virtual-network/virtual-networks-nsg). Consultez le déploiement : 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 RSA NetWitness® Suite .



   c. Cliquez sur le bouton **OK**.

Azure valide votre machine virtuelle et la section **4 Achat** est sélectionnée.



7. Cliquez sur **Achat** pour créer le principal service de composant de RSA Security Analytics (par exemple, **Concentrator**) pour la machine virtuelle dans Azure.
8. Configurez la machine virtuelle hôte dans RSA NetWitness® Suite 11.0.0.

   Reportez-vous à l'Étape 3. Configurer les machines virtuelles hôtes dans RSA NetWitness® Suite . pour obtenir des instructions.
9. Répétez les étapes 1 à 8 incluse pour le reste des services de composants principaux de RSA Security Analytics.

Étape 3. Configurer les machines virtuelles hôtes dans RSA NetWitness® Suite .

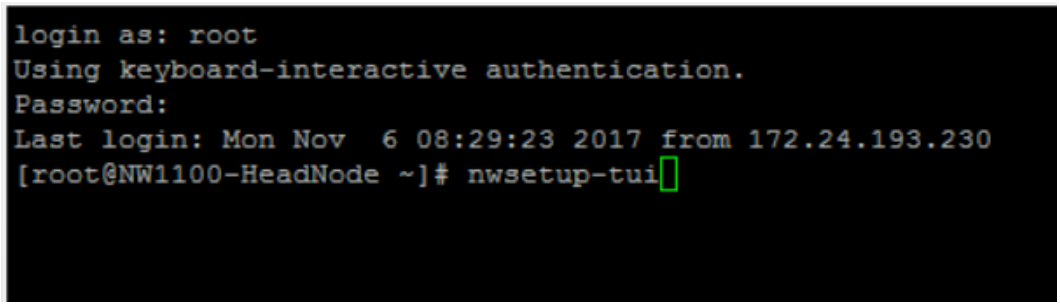
Configurez les différents hôtes et services comme décrit dans le RSA NetWitness® Suite - *Guide de configuration de l'hôte et des services*. Ce guide décrit aussi les procédures d'application des mises à jour et de préparation des mises à niveau des versions.

Remarque : Après avoir correctement créé une machine virtuelle, Azure lui attribue un nom d'hôte par défaut. Dans le document « Modifier le nom et le nom d'hôte d'un hôte », consultez *Modifier l'hôte* dans l'aide ((https://community.rsa.com/docs/DOC-41716) dans RSA NetWitness® Suite pour obtenir des instructions sur la modification d'un nom d'hôte.

1. Ouvrez une session SSH sur l'hôte en utilisant les informations d'identification que vous avez renseignées dans la section **1 Informations de base** de l'assistant **Créer une machine virtuelle** lors de la création de la machine virtuelle dans Azure (dans l'élément 4d de l'Étape 2. Déployer les services de base des composants dans Azure).
2. Réinitialisez le mot de passe pour la **racine**.

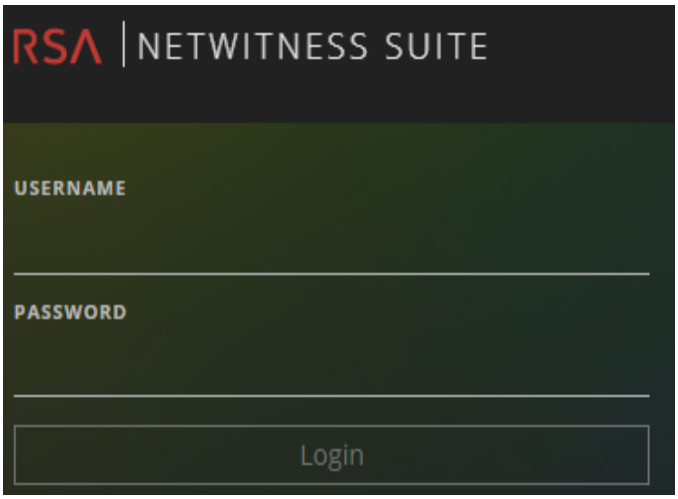
```
login as: nwadmin
Using keyboard-interactive authentication.
Password:
[nwadmin@NW1100-HeadNode ~]$ sudo passwd root

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for nwadmin:
Changing password for user root.
New password:
BAD PASSWORD: The password contains less than 1 digits
Retype new password:
passwd: all authentication tokens updated successfully.
[nwadmin@NW1100-HeadNode ~]$
```

3. Ouvrez une session SSH sur l'hôte en utilisant le nom d'utilisateur **racine** et le mot de passe créé à l'étape précédente, puis indiquez à NetWitness Suite une adresse IP pour le provisionnement.



Reportez-vous à la section Tâches d'installation et à la section Configurer les hôtes (Instances) dans le *Guide de déploiement AWS pour RSA NetWitness11.0.0.0.*

4. Connectez-vous à RSA NetWitness Suite.



5. Accédez à **Administration** > **Hôtes**.

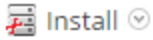
   La boîte de dialogue **Nouveaux hôtes** s'affiche avec les machines virtuelles hôtes que vous avez créées dans Azure.

6. Sélectionnez l'hôte à activer.

   L'option de menu **Activer** devient active.

7. Cliquez sur **Activer**.

8. Sélectionnez l'hôte que vous avez activé.

9. Cliquez sur  et sélectionnez le composant que vous avez déployé dans Azure (par exemple, Event Stream Analysis). Pour plus d'informations, reportez-vous au *Guide de mise en route des hôtes et des services pour la version 11.0.0.0*.

Historique des révisions

Révision	Date	Description
1	21 janvier	Première version