XenApp 7.5 et XenDesktop 7.5

Déployer XenApp 7.5 et XenDesktop 7.5 avec Amazon VPC

Préparé par : Peter Bats

Rédactrice : Linda Belliveau

Version : 4.0

Dernière mise à jour : avril 29, 2014

Table des matières

Introduction

Ce document décrit la configuration de Citrix XenApp ou XenDesktop avec le VPC Amazon Web Services (AWS).

Configuration requise

Pour déployer un site XenApp ou XenDesktop 7.5 dans un VPC Amazon, assurez-vous que les conditions préalables sont remplies et associez les AMI AWS Marketplace à votre compte comme suit.

Conditions préalables

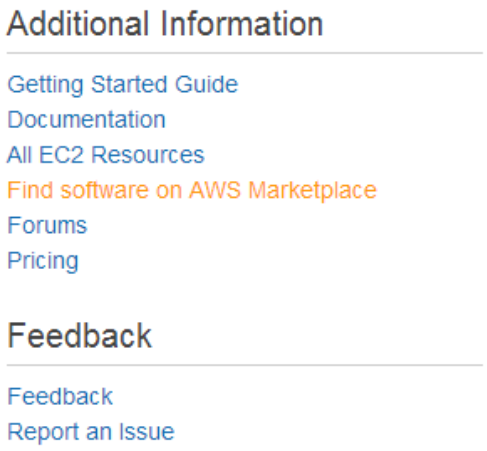
Effectuez les opérations suivantes avant de commencer :

- Prévoyez une journée pour l'implémentation du déploiement.
- Assurez-vous qu'un environnement AWS est configuré et opérationnel. Il doit être doté d'un compte AWS actif et de préférence d'un compte Identity and Access Management (IAM) AWS qui peut être utilisé pour ce déploiement spécifique.
- Pour cette preuve de concept (PDC), l'utilisateur IAM doit disposer de droits d'administration sur votre environnement AWS. Pour de plus amples informations sur les droits dont vous avez besoin, consultez la rubrique Préparerl'installation de XenApp et XenDesktop.
- Inscrivez-vous à l'aide de votre compte AWS auprès de l'AMI NetScaler VPX dans AWS Marketplace.

Associer les AMI AWS Marketplace à votre compte

Le modèle CloudFormation utilise les AMI AWS Marketplace. Associez les AMI à votre compte avant de procéder à l' installation, comme suit.

1. Dans la console AWS, sélectionnez **Find software on AWS MarketPlace** (Rechercher des logiciels sur AWS MarketPlace) sous la section des informations supplémentaires à droite de la console.



2. Recherchez **NetScaler VPX Platinum Edition – 10 Mbps** et sélectionnez **version 10.1-123.9**.

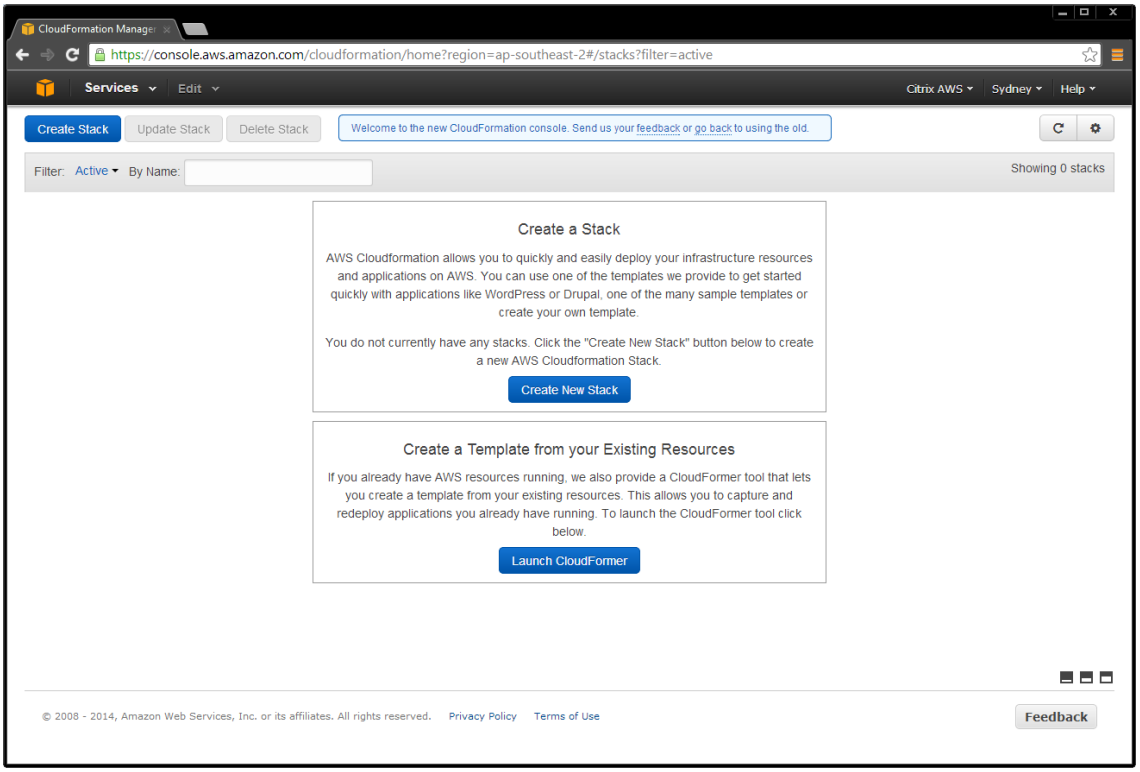
3. Connectez-vous à votre compte AWS.

Déploiement automatique à l'aide d'un modèle CloudFormation AWS

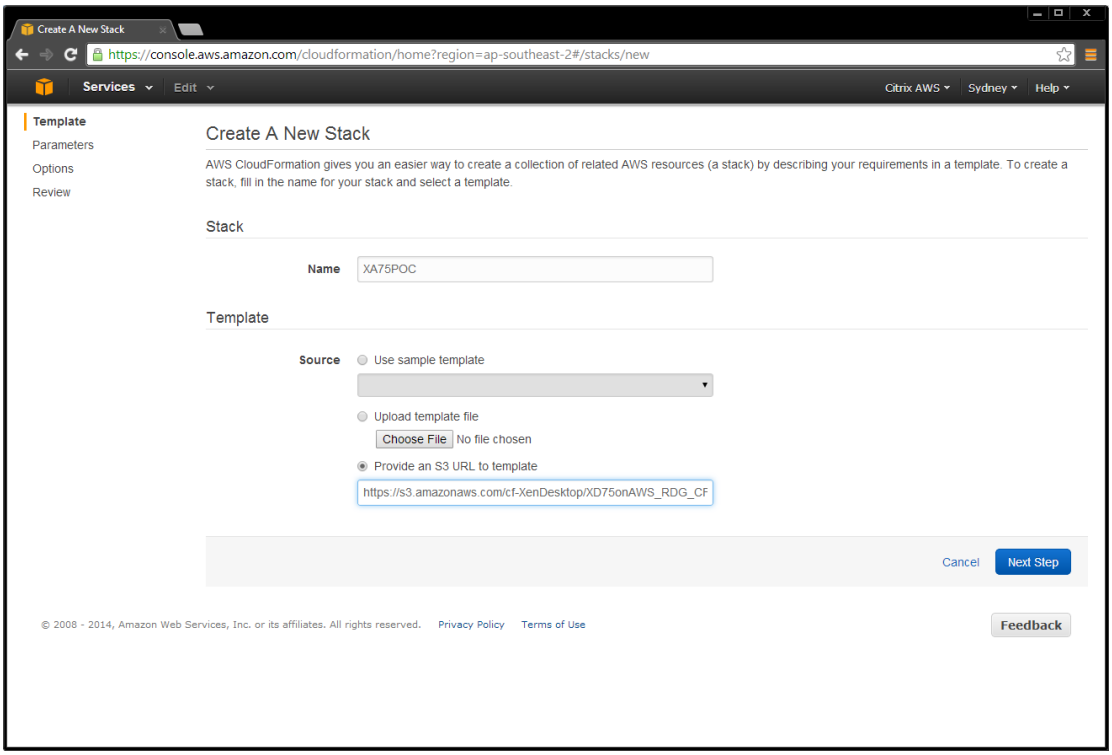
Création d'une pile d'infrastructure XenApp ou XenDesktop à l'aide du modèle CloudFormation

La procédure suivante indique comment utiliser le modèle CloudFormation pour automatiser la création de toutes les ressources nécessaires à un site XenApp ou XenDesktop dans le cloud Amazon EC2.

1. Sur l'onglet de la console CloudFormation Stack, utilisez le menu déroulant dans le coin supérieur droit pour sélectionner la région dans laquelle vous souhaitez créer l'environnement.



2. Cliquez sur **Create New Stack** (Créer une nouvelle pile).
3. Nommez la pile, puis pointez vers le modèle CloudFormation JSON disponible sur https://s3.amazonaws.com/cf-XenDesktop/XD75NSonAWS_CF_v1_2.json, puis cliquez sur **Continue**.



4. Spécifiez les paramètres à exécuter par le script. Le modèle contient les informations suivantes, notamment des explications succinctes pour chaque paramètre, et affiche les valeurs par défaut suivantes.

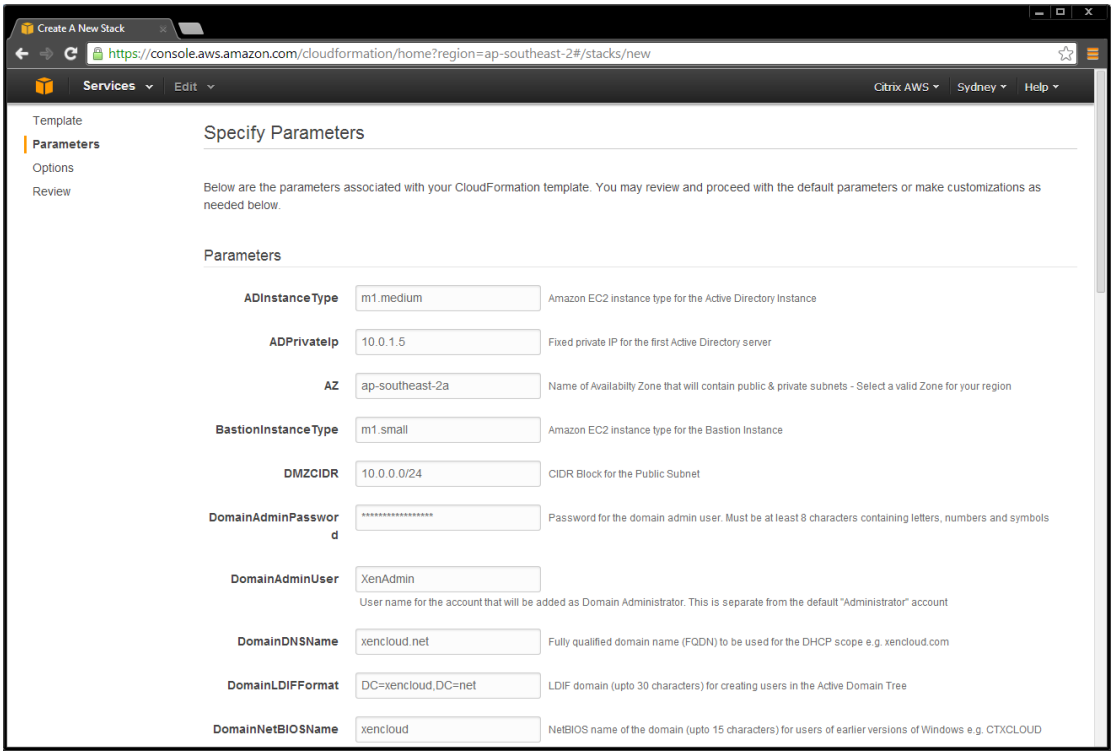
Valeur par défaut	Valeur par défaut	Description
ADInstanceType	m1.medium	Type d'instance Amazon EC2 pour l'instance Active Directory
ADPrivateIP	10.0.1.5	Adresse IP privée fixe pour le serveur Active Directory
AZ		Nom de la zone de disponibilité qui contiendra les sous-réseaux publics et privés. Sélectionnez une zone valide pour votre région
BastionInstanceType	m1.small	Type d'instance Amazon EC2 pour l'instance Bastion
DMZCDIR	10.0.0.0/24	Bloc CIDR pour le sous-réseau public
DomainAdminPassword	Fourni par l'utilisateur	Mot de passe de l'utilisateur Admin du domaine. Il doit comporter au moins huit caractères et contenir des lettres, des chiffres et des symboles
DomainAdminUser	Xenadmin	Nom d'utilisateur du compte qui sera ajouté en tant qu'administrateur de domaine. Celui-ci est distinct du compte d'administrateur par défaut
DomainDNSName	xencloud.net	Nom de domaine complet (FQDN) à utiliser pour l'étendue DHCP ; par exemple, xencloud.com
DomainLDIFFormat	DC=xencloud, DC=net	Domaine LDIF (jusqu'à 30 caractères) pour la création d'utilisateurs dans l'arborescence de domaine Active Directory
DomainNetBIOSName	XENCLOUD	Nom NetBIOS du domaine (jusqu'à 15 caractères) pour les utilisateurs de versions antérieures de Windows ; par exemple, XENCLOUD
IAMUserAccessKey	Fourni par l'utilisateur	Clé d'accès de l'utilisateur IAM utilisée pour créer et configurer les différentes instances
KeyPairName	Fourni par l'utilisateur	Paires de clés publiques/privées qui vous permettent de vous connecter de manière sécurisée à l'instance après son démarrage
NATInstanceType	m1.small	Type d'instance Amazon EC2 pour les instances NAT
NSCloudFormationURL	https://s3.amazonaws.com/cf-XenApp/NS_VPX_PLT_10M	URL publique du modèle NetScaler VPX CloudFormation v4.4

	B_Template_v4.4.json	
NSMIP	10.0.1.102	L'adresse SNIP ou MIP privée fixe de la carte réseau NetScaler connectée au sous-réseau privé doit se situer dans la plage CIDR du sous-réseau privé
NSNSIP	10.0.1.100	L'adresse IP privée fixe de la carte réseau NetScaler connectée au sous-réseau privé doit se situer dans la plage CIDR du sous-réseau privé
NSSNIP	10.0.0.175	L'adresse IP publique fixe de la carte réseau NetScaler connectée au sous-réseau public doit se situer dans la plage CIDR du sous-réseau public
NSVIP	10.0.0.176	L'adresse VIP fixe de la carte réseau NetScaler connectée au sous-réseau public doit se situer dans la plage CIDR du sous-réseau public
PrivateCIDR	10.0.1.0/24	Bloc CIDR pour le sous-réseau privé
RestoreModePassword	Fourni par l'utilisateur	
SecretAccessKey	Fourni par l'utilisateur	Clé d'accès secrète de l'utilisateur IAM à utiliser
ServerNetBIOSName	DC01	Nom NetBIOS du serveur Active Directory (jusqu'à 15 caractères)
VDAInstanceType	c1.xlarge	Type d'instance Amazon EC2 pour l'instance principale VDA
VdaName	VDAMaster	Serveur XenApp principal qui détient le rôle de collecteur de données préféré de la batterie ainsi que le serveur SQL Server
VPCCIDR	10.0.0.0/16	Serveur XenApp secondaire qui détient le rôle de collecteur de données préféré de la batterie
VPCName	VPC POC XenDesktop 7.5	Serveur qui héberge le rôle StoreFront. Exécute la version 1.2 de StoreFront avec la base de données sur le serveur XENAPP.
XD7DDCInstanceType	m3.large	Serveur d'installation utilisé pour créer la batterie de serveurs à l'aide des scripts PowerShell App Delivery Setup. Peut être mis hors tension après création de la batterie.
XD7ISOLocation	https://s3.amazonaws.com/cf-XenDesktop/ISO/XenApp_and_XenDesktop_7_5.iso	Serveur de traduction d'adresse réseau (NAT) qui offre un accès sortant à Internet aux serveurs dans le sous-réseau privé
XDAdminPassword	Fourni par l'utilisateur	Instance NetScaler VPX utilisée pour fournir la fonctionnalité de proxy ICA au serveur StoreFront

XDAdminUser	XDFarmAdmin

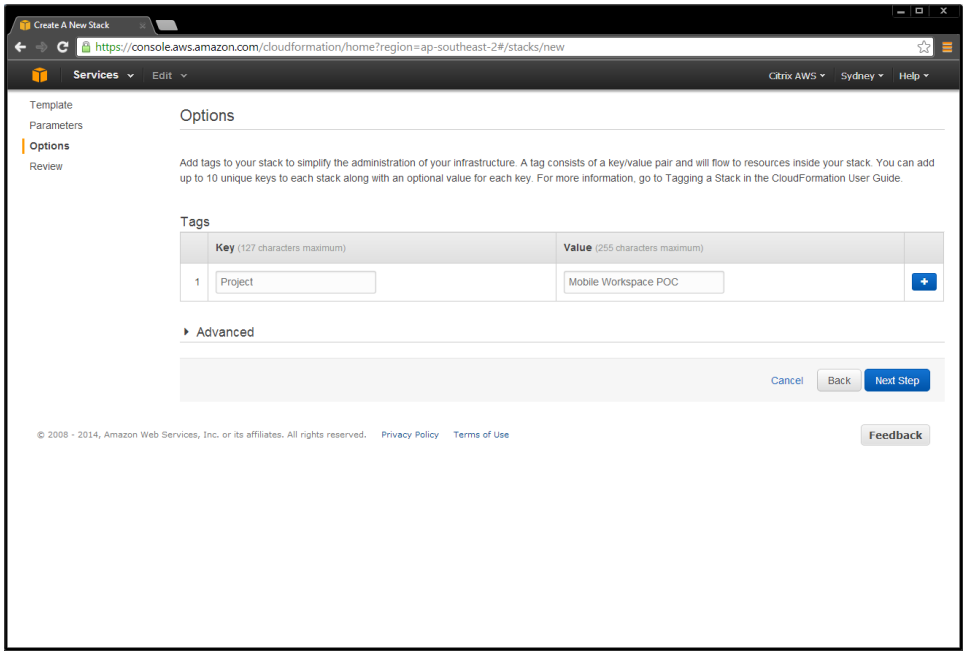
5. Plusieurs versions du firmware NetScaler VPX sont prises en charge. Sélectionnez la version souhaitée en choisissant le modèle JSON approprié à partir de l'une des versions suivantes du firmware :

NSCloudFormationURL	Firmware
https://s3.amazonaws.com/cf-XenApp/NS_VPX_Template_v3.json	10.0-71.6008.e
https://s3.amazonaws.com/cf-XenApp/NS_VPX_Template_v4.json	10.1-119.7
https://s3.amazonaws.com/cf-XenApp/NS_VPX_Template_v4.1.json	10.1-120.13



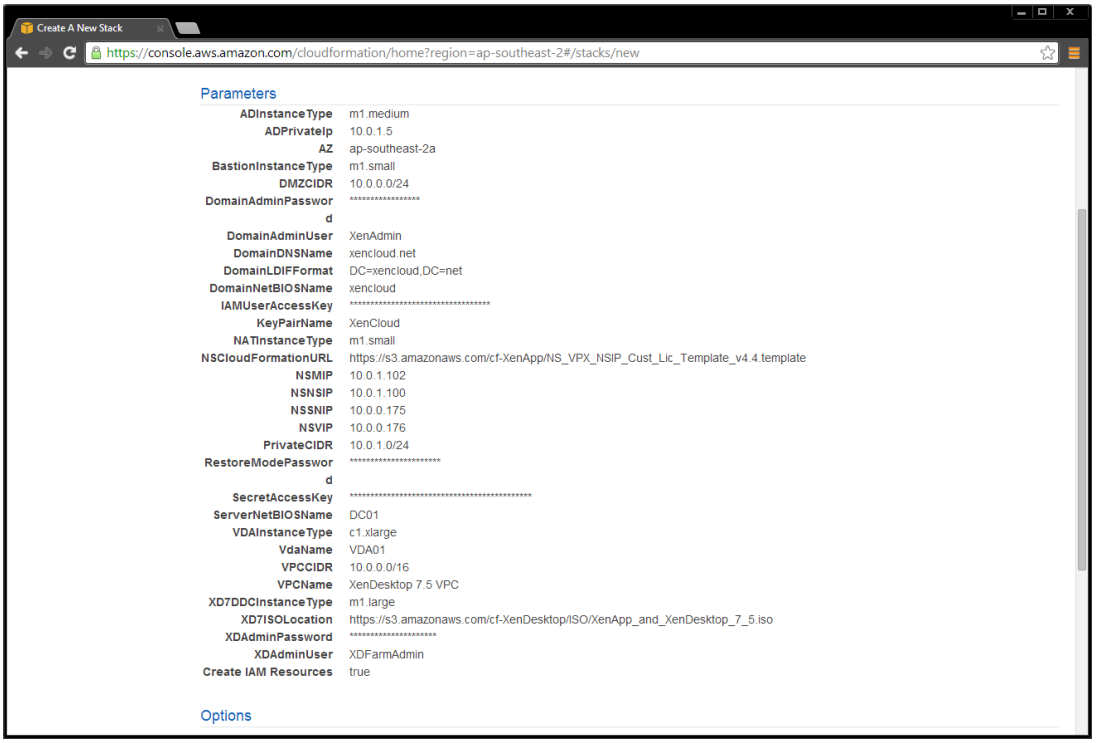
6. Après avoir spécifié les paramètres requis, sélectionnez la case **I acknowledge that this template may create IAM resources** (Je reconnais que ce modèle peut créer des ressources IAM), puis cliquez sur **Continue**.

7. Ajoutez des balises supplémentaires sur l'écran suivant et cliquez sur **Continue**.

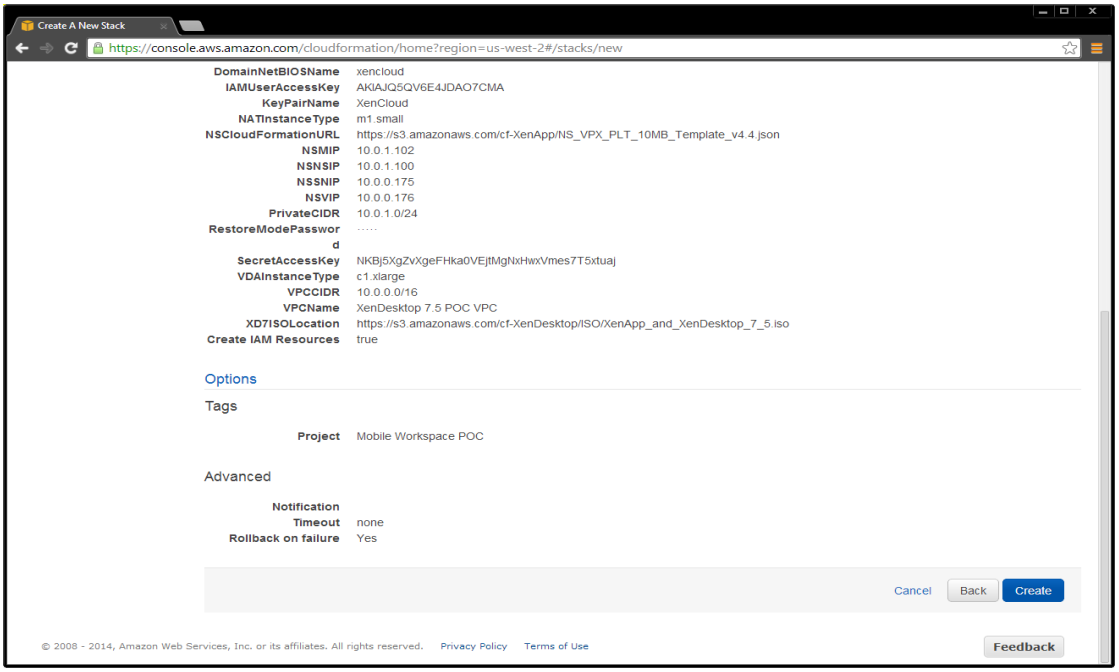


Vérifiez que les valeurs fournies sont adaptées à votre environnement.

Remarque : il est important de vous assurer que la zone de disponibilité, vos informations d'identification et votre paire de clés d'accès sont correctes. Si ce n'est pas le cas, revenez en arrière et corrigez l'erreur, sinon la création du modèle échouera. Ceci fait, cliquez sur **Continue** pour démarrer le processus de création de la pile.

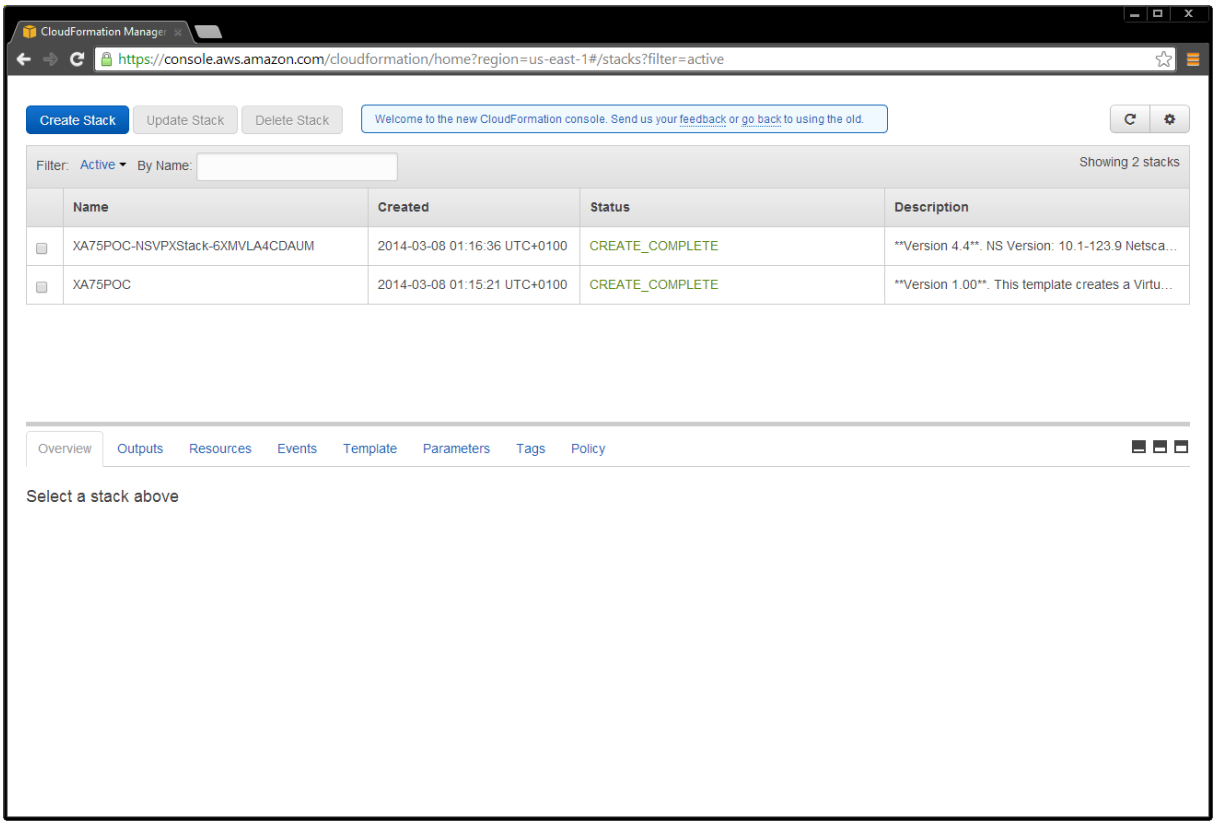


8. Sur l'écran récapitulatif, cliquez sur **Create**.

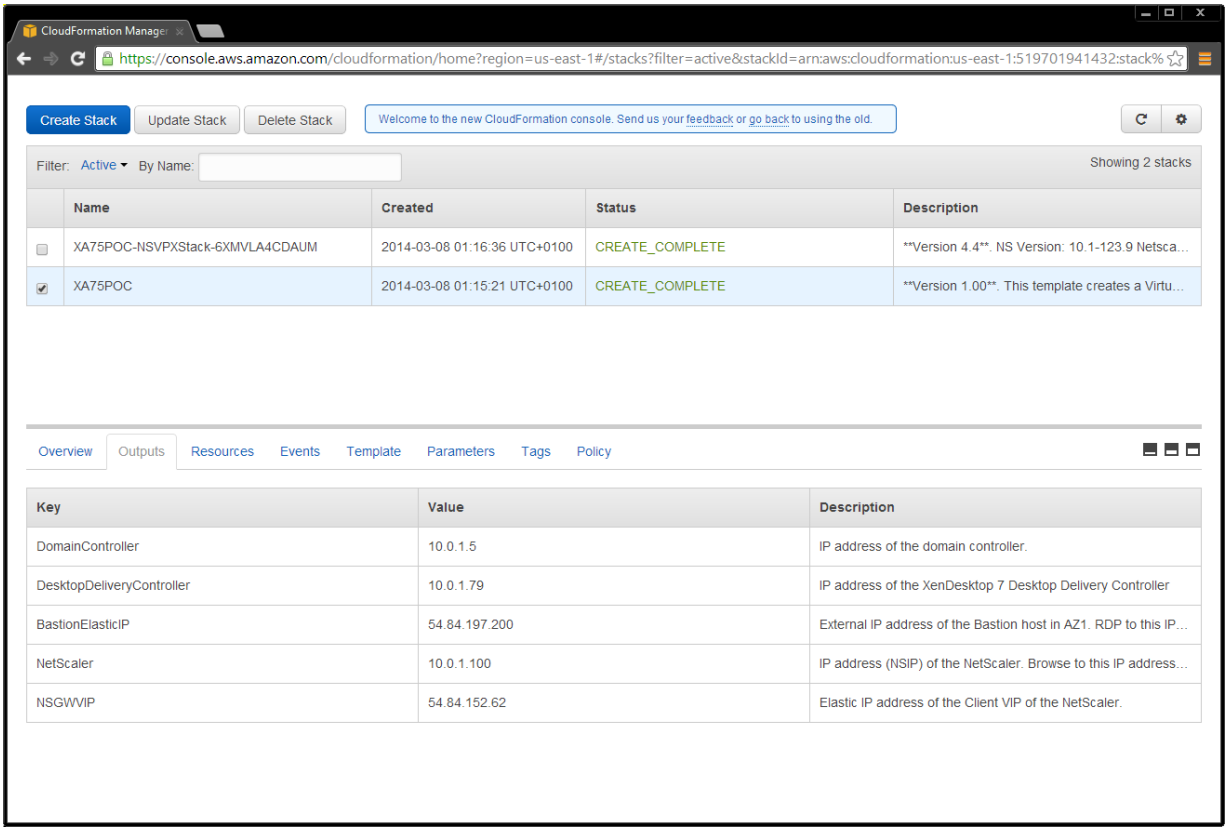


Le modèle CloudFormation génère l'environnement en fonction des paramètres que vous avez spécifiés ; le modèle s'affichera dans la console CloudFormation une fois le processus terminé.

Il contient deux piles CloudFormation : l'une pour l'infrastructure EC2 et l'autre pour le NetScaler VPX.

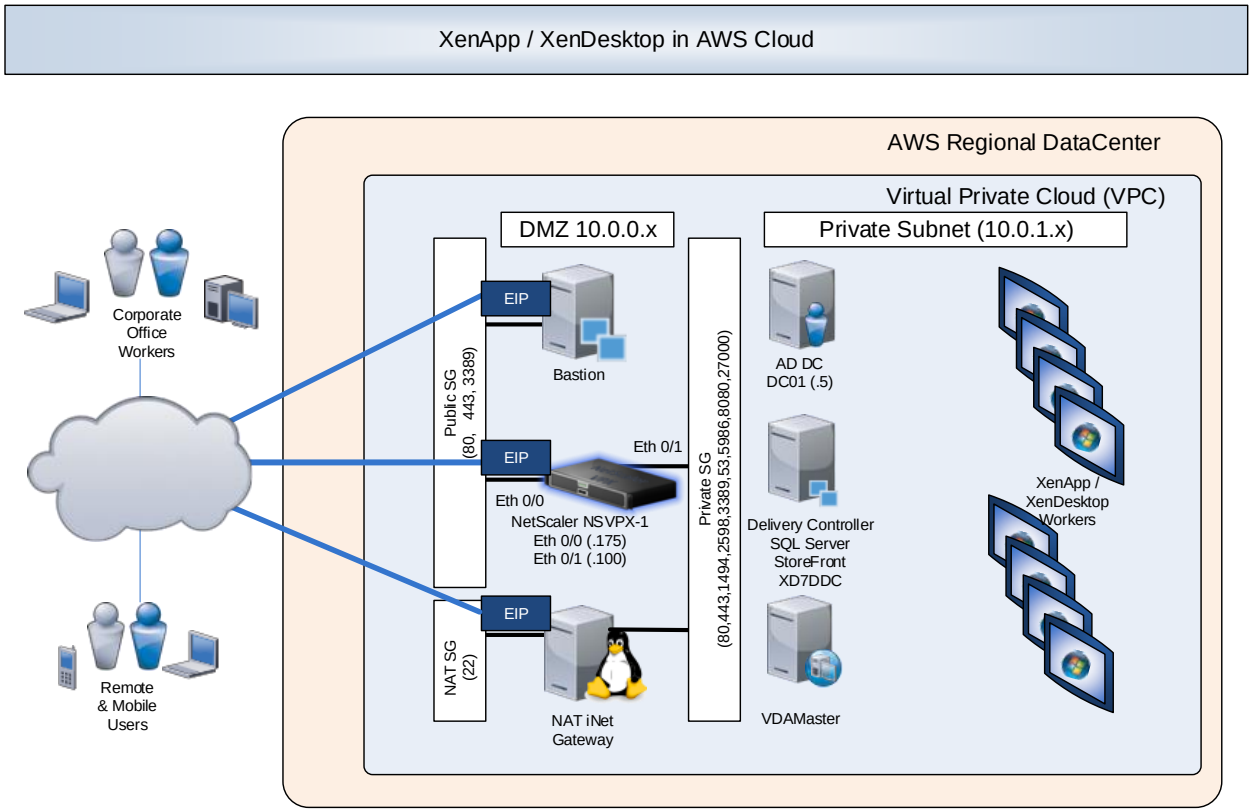


9. Lorsque vous sélectionnez l'onglet Outputs dans la pile d'infrastructure, vous pouvez voir les adresses IP des composants principaux.



Si vous sélectionnez les valeurs par défaut, le modèle génère une infrastructure de site XenApp ou XenDesktop dans le cloud AWS semblable à l'exemple suivant :

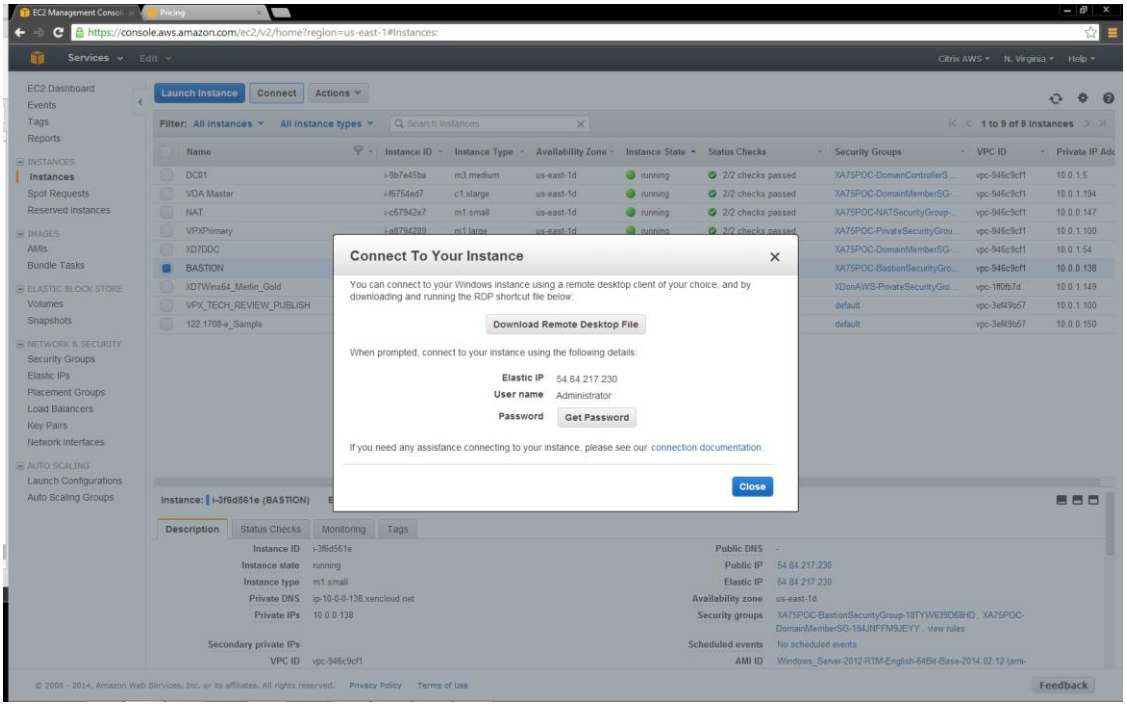
Infrastructure de site utilisant le modèle CloudFormation



Configurer XenApp ou XenDesktop sur l'infrastructure AWS

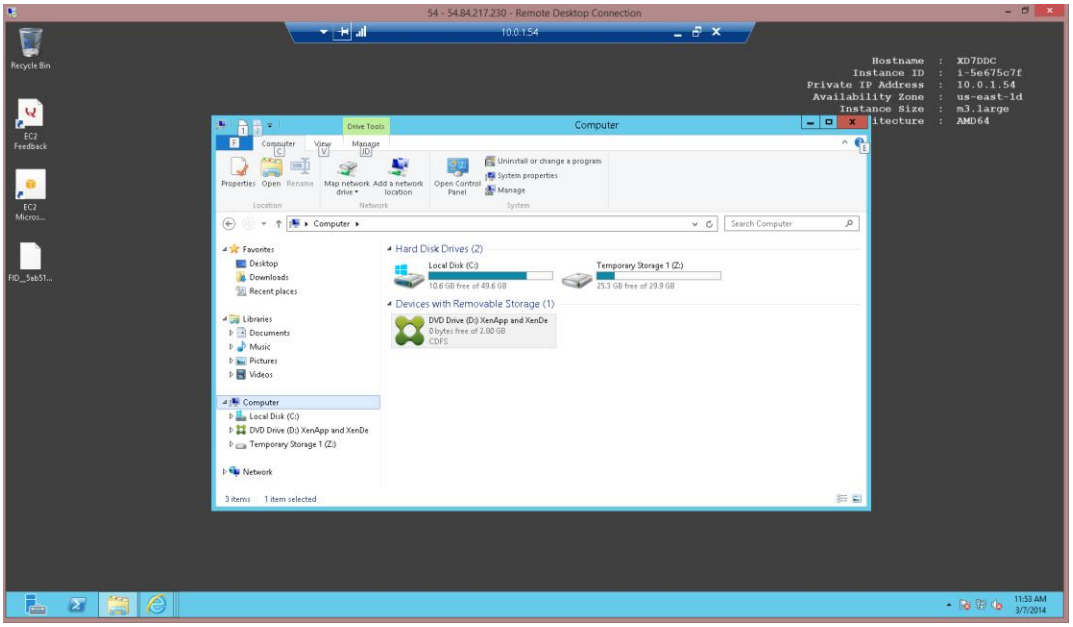
Après avoir installé AWS à l'aide d'un modèle CloudFormation AWS, vous pouvez configurer XenApp ou XenDesktop afin de mettre à disposition des applications et bureaux virtuels à partir de AWS.

1. À partir de la console de gestion des instances EC2, sélectionnez **Download Desktop File** (Télécharger fichier de bureau) pour vous connecter à l'hôte Bastion à l'aide de RDP.
2. Ouvrez une session avec les informations d'identification d'administrateur de domaine que vous avez fournies lors de la création de la pile CloudFormation.



3. À partir de l'hôte Bastion, connectez-vous via RDP au Delivery Controller (le contrôleur est **xd7ddc.xencloud.net** lorsque vous utilisez le nom de domaine par défaut), et ouvrez une session en tant qu'administrateur de domaine à l'aide des paramètres **DomainAdminUser** et **DomainAdminPassword** fournis durant la création de la pile.

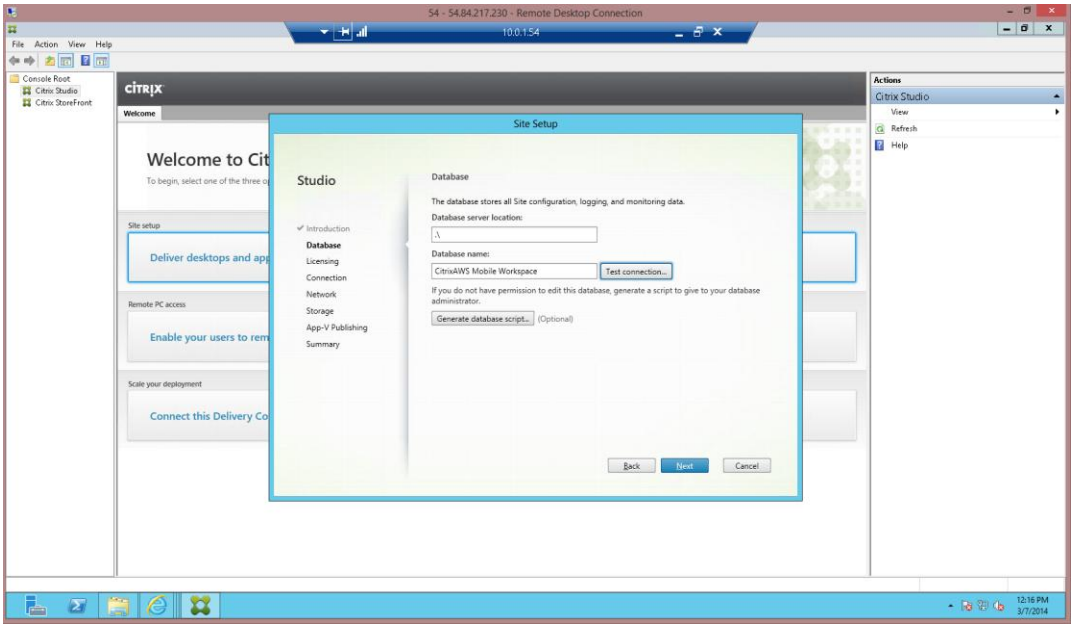
4. Le support du produit XenApp et XenDesktop 7.5 est déjà monté. Exécutez **AutoSelect.exe** pour démarrer l'installation.



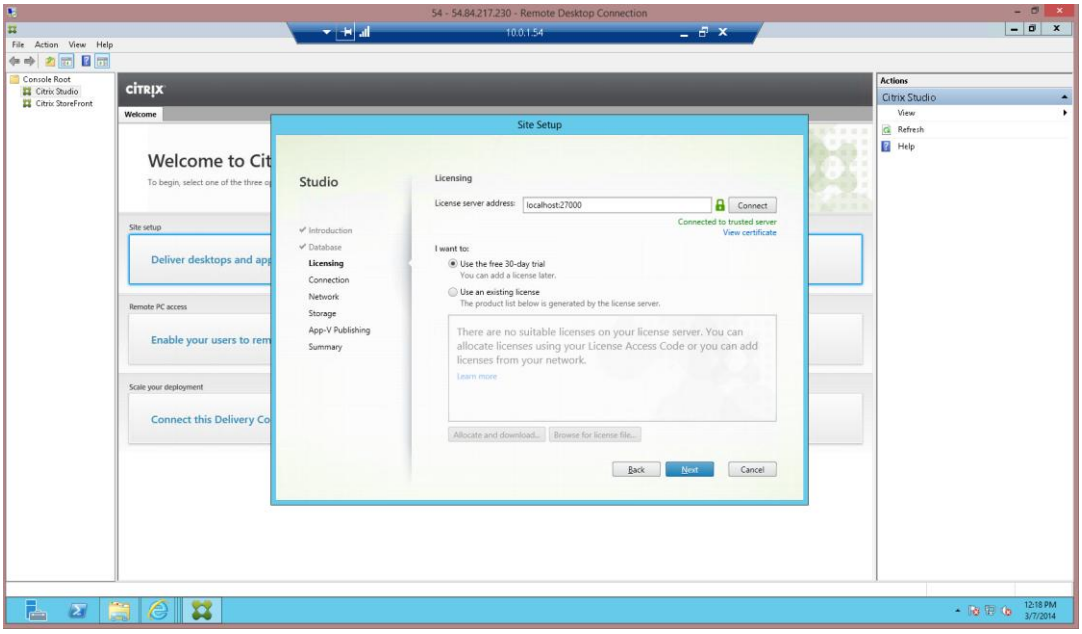
Remarque : le format du fichier des informations d'identification pour le compte AWS racine, récupéré sur https://console.aws.amazon.com/iam/home?#security_credential est différent de celui des fichiers d'informations d'identification téléchargés pour les utilisateurs AWS standard. Pour cette raison, Studio ne peut pas utiliser le fichier pour remplir les champs API et de clé secrète lors de la création d'une connexion. Vérifiez que vous utilisez des fichiers d'informations d'identification IAM lors de l'administration de Studio.

5. Installez XenApp ou XenDesktop en fonction des besoins de votre environnement.
    a. Sélectionnez le **Delivery Controller**.
    b. Sélectionnez **All Core Components** (Tous les composants principaux).
    c. Suivez les instructions de l'assistant pour procéder à l'installation du Delivery Controller.
6. Démarrez Citrix Studio, puis suivez les instructions de l'assistant pour créer le site. Notez que le modèle CloudFormation a pré-installé SQL Server 2012 sur le Delivery Controller.

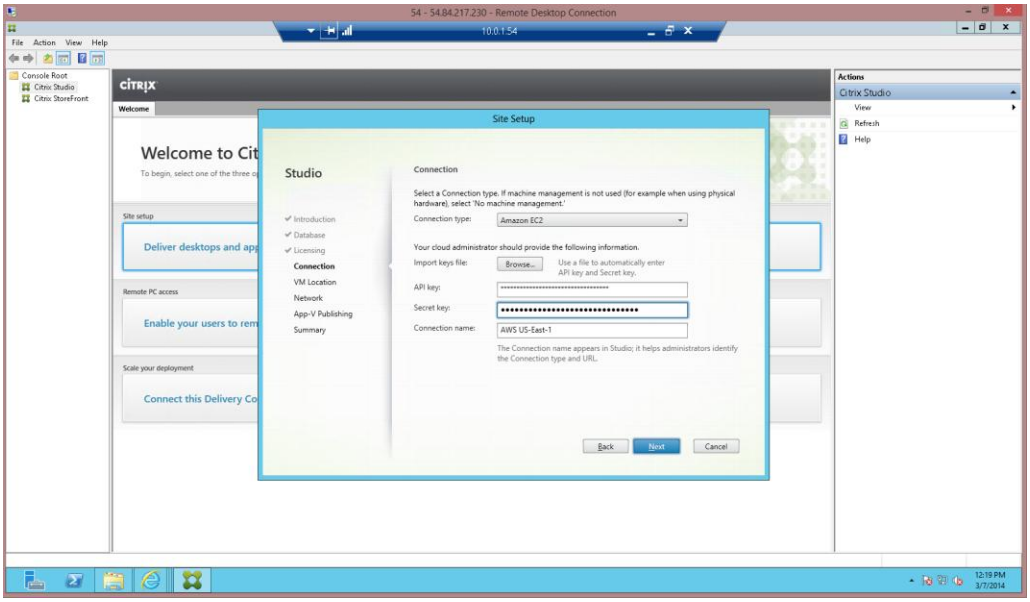
7. Sélectionnez l'hôte local en tant qu'emplacement du serveur de base de données, et autorisez l'assistant à créer la base de données.



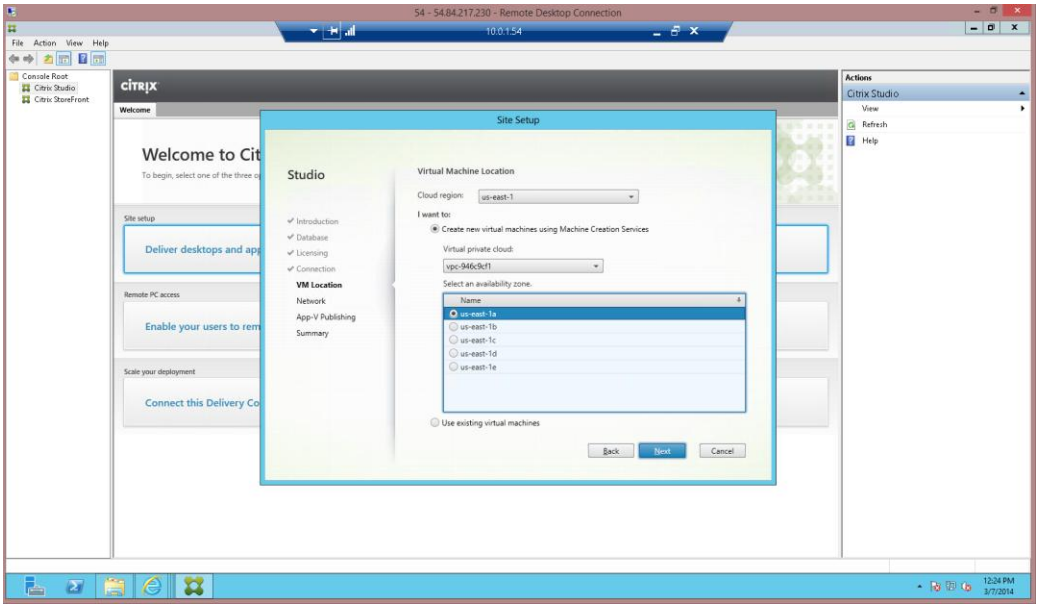
8. Procédez à l'installation du gestionnaire de licences.



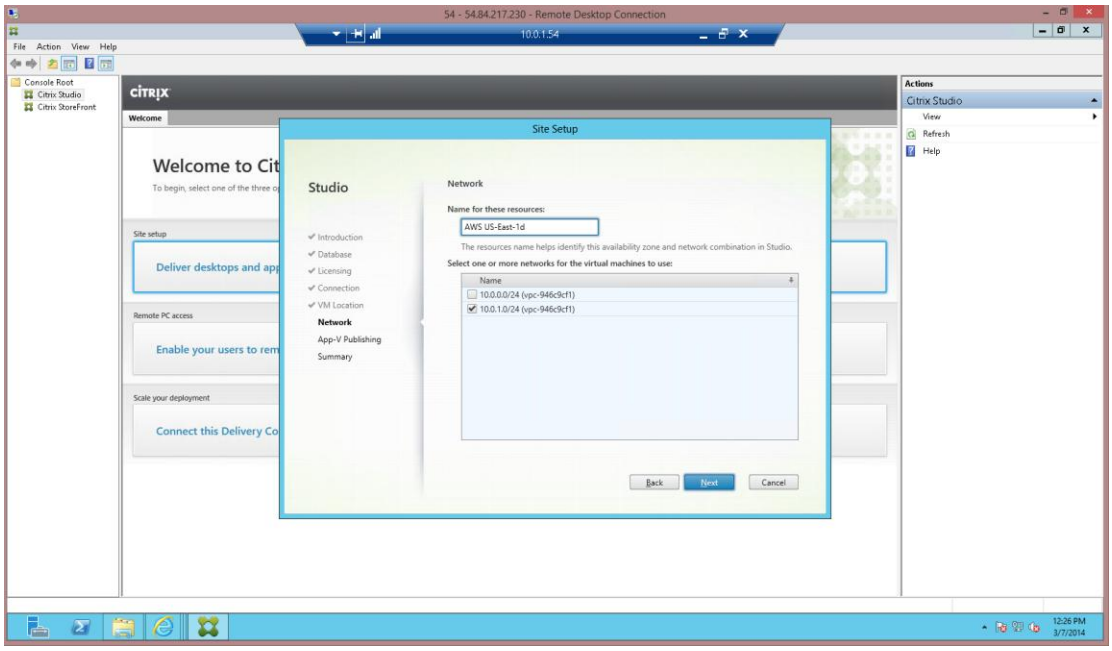
9. Entrez vos informations d'identification d'accès à AWS afin d'autoriser le Delivery Controller à provisionner des instances sur AWS.



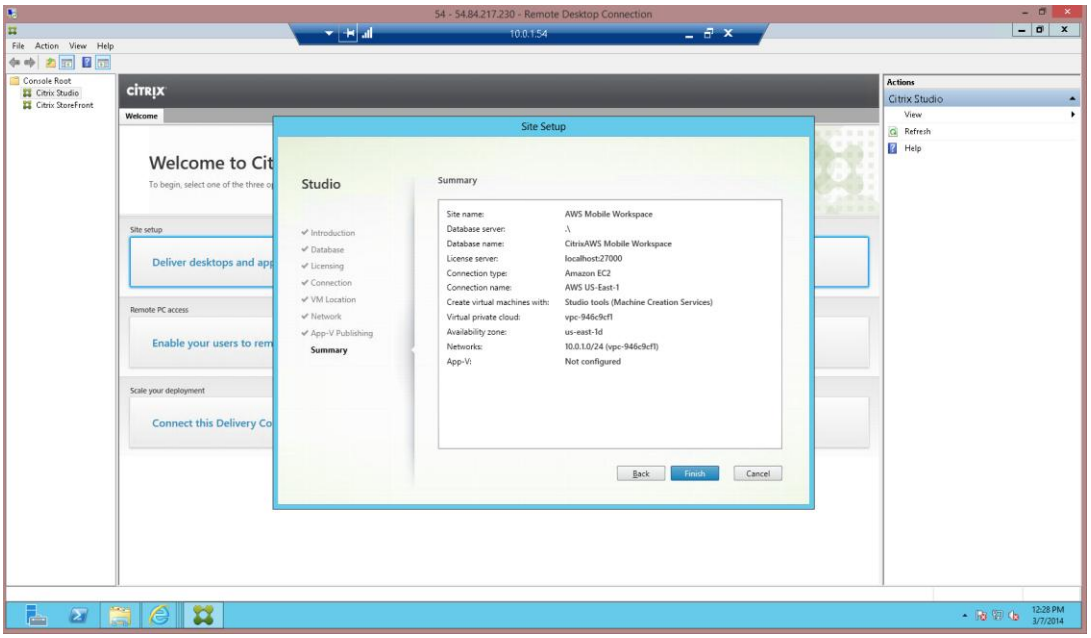
10. Sélectionnez la région AWS, votre VPC et la zone de disponibilité pour cette connexion.



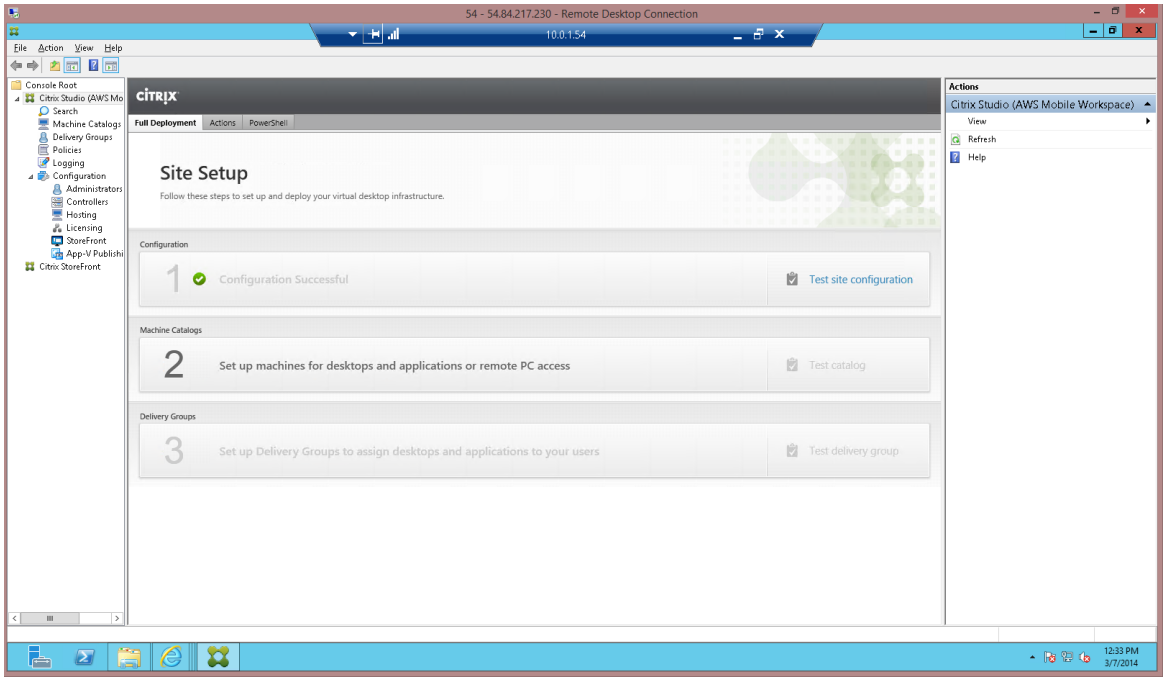
11. Sélectionnez les sous-réseaux chargés d'héberger les instances, puis entrez un nom. Dans cet exemple, le sous-réseau privé **10.0.1.0/24** est sélectionné afin d'accéder aux VDA exécutés dans ce réseau privé, comme indiqué dans le diagramme Infrastructure de site utilisant le modèleCloudFormation.



12. Ignorez la configuration de l'option App-V Publishing afin de terminer l'installation du site. Vous pouvez ajouter cette fonctionnalité ultérieurement.



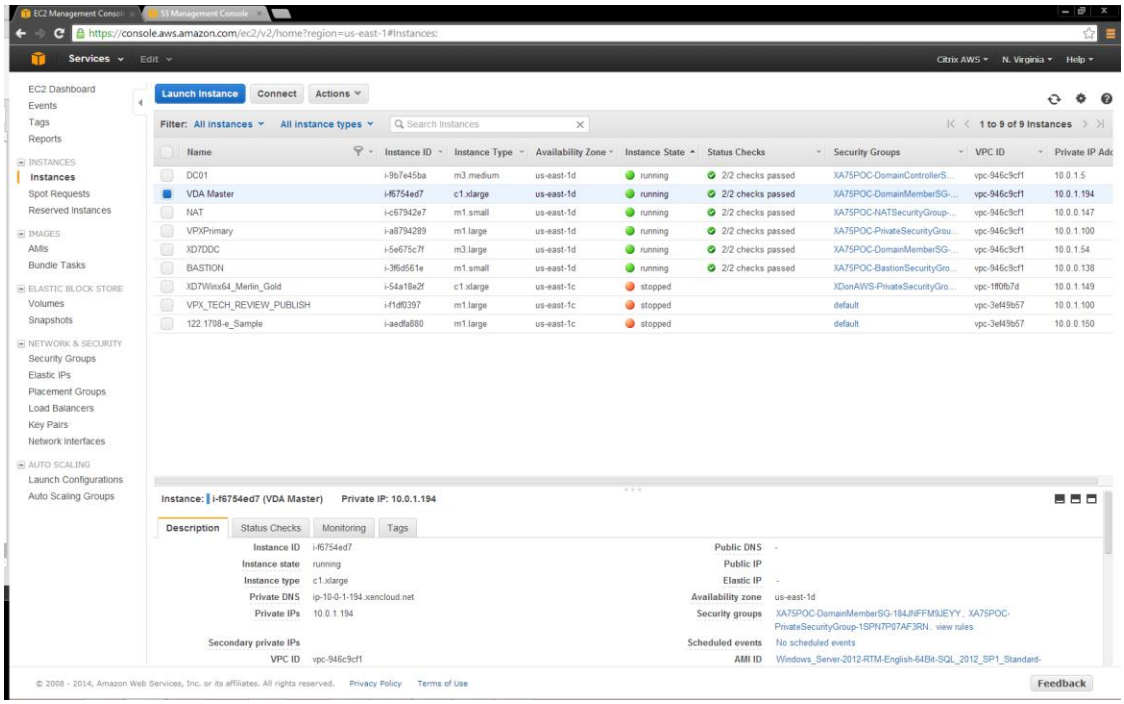
Une fois la configuration terminée, l'assistant affiche la page Création d'un site.



Configurer la machine VDA principale

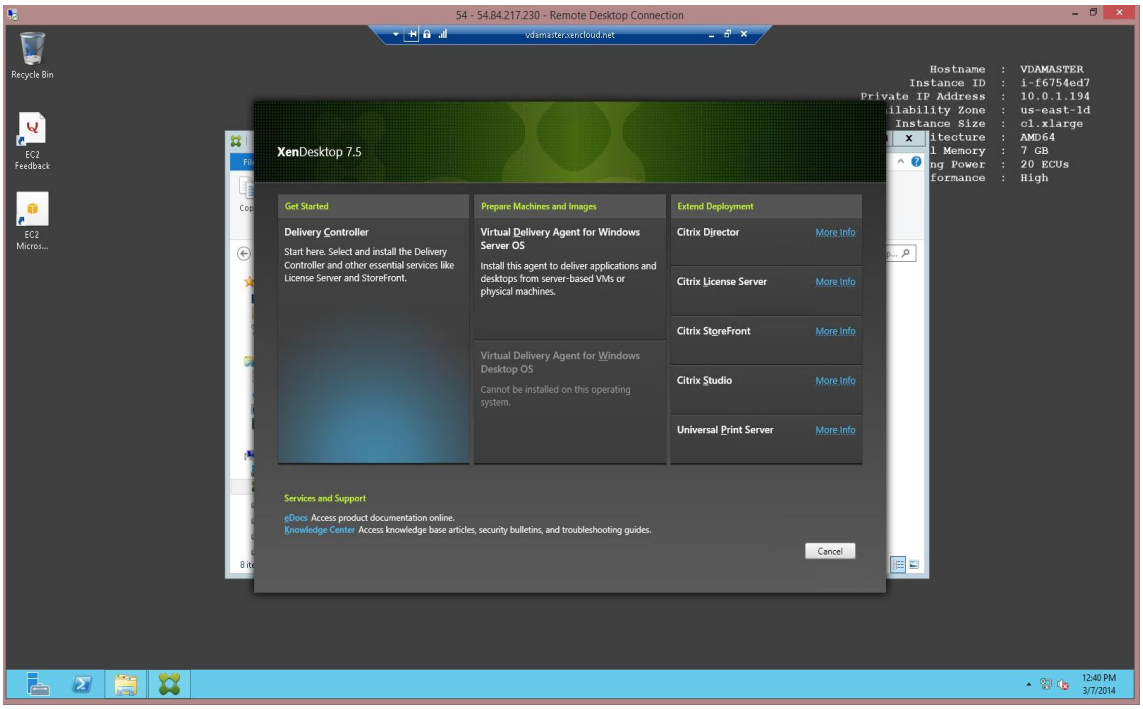
Une fois que vous avez configuré le Delivery Controller, vous devez configurer une image principale en configurant une machine VDA principale.

1. À partir de l'hôte Bastion, connectez-vous via RDP au VDA principal (vous pouvez trouver l'adresse IP dans la console EC2), et ouvrez une session en tant qu'**administrateur de domaine** à l'aide des paramètres **DomainAdminUser** et **DomainAdminPassword** fournis durant la création de la pile.

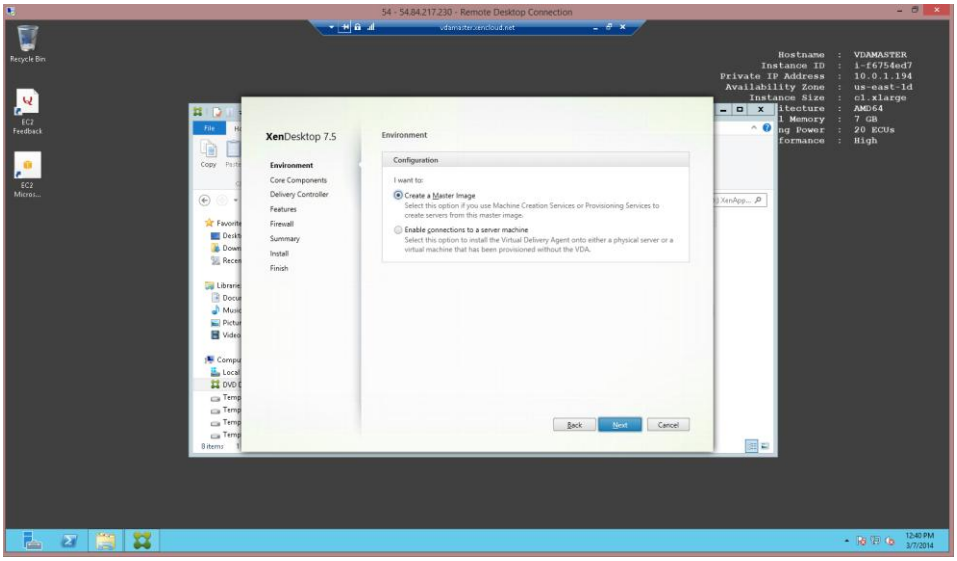


2. Le support du produit XenApp et XenDesktop 7.5 est déjà monté. Exécutez **AutoSelect.exe** pour démarrer l'installation.

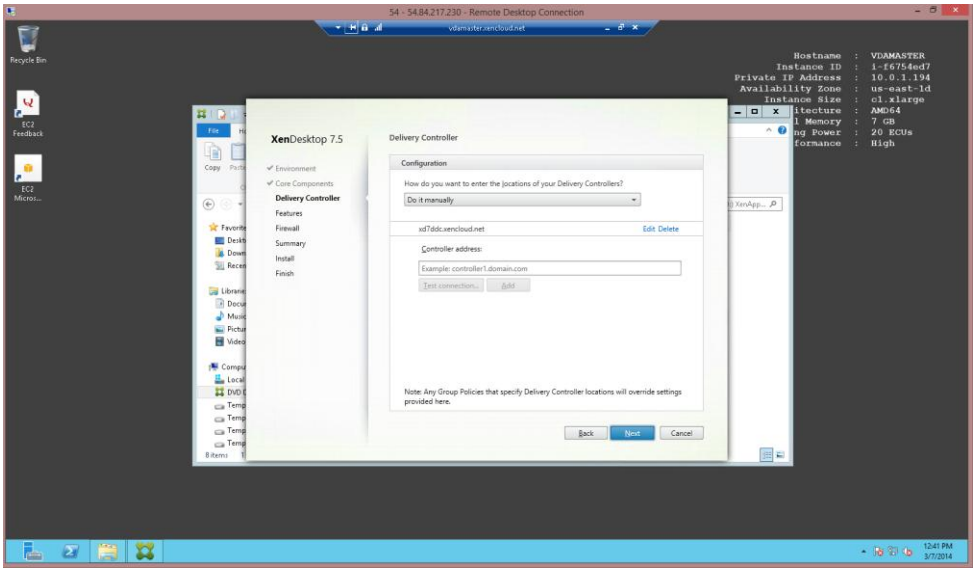
3. Sélectionnez **Virtual Delivery Agent pour système d'exploitation Windows Server** pour l'installation de XenApp Worker. Voir la rubrique Server VDI pour plus d'informations sur la configuration de la fonctionnalité Server VDI sur un VDA principal.



10. Sélectionnez **Créer une image principale**.

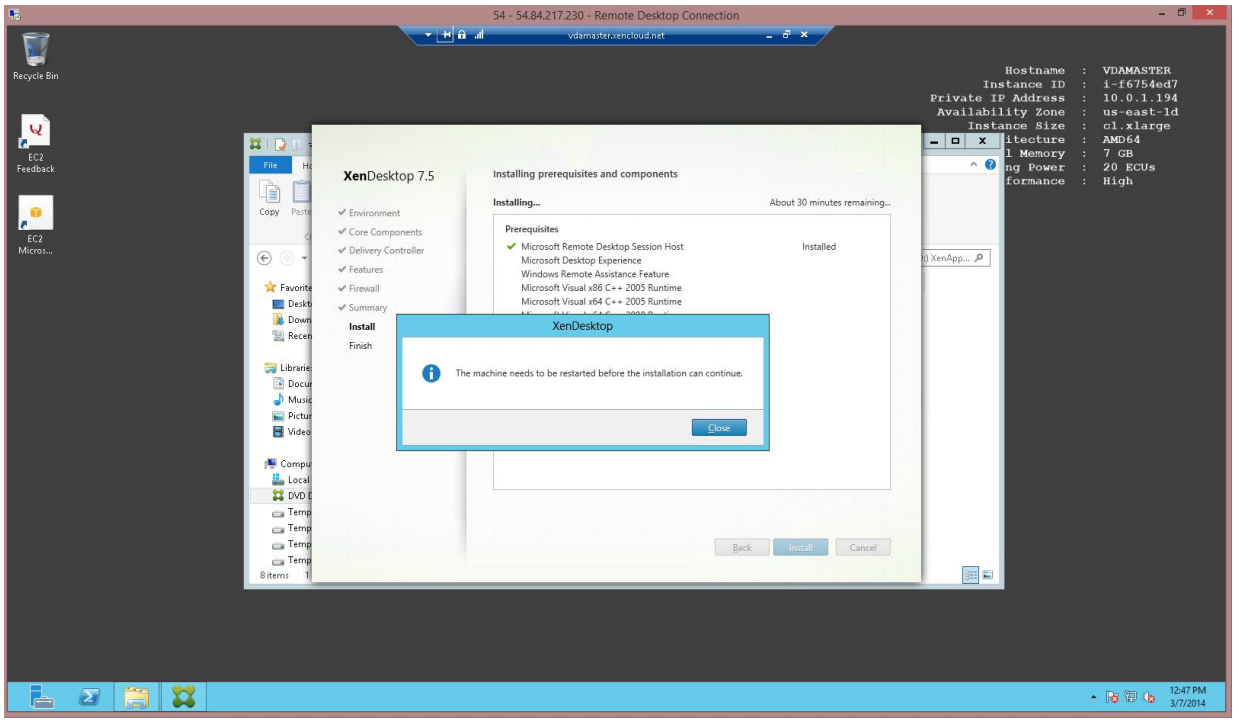


11. Fournissez le nom de domaine complet (FQDN) du Delivery Controller que vous avez configuré précédemment dans ce processus.



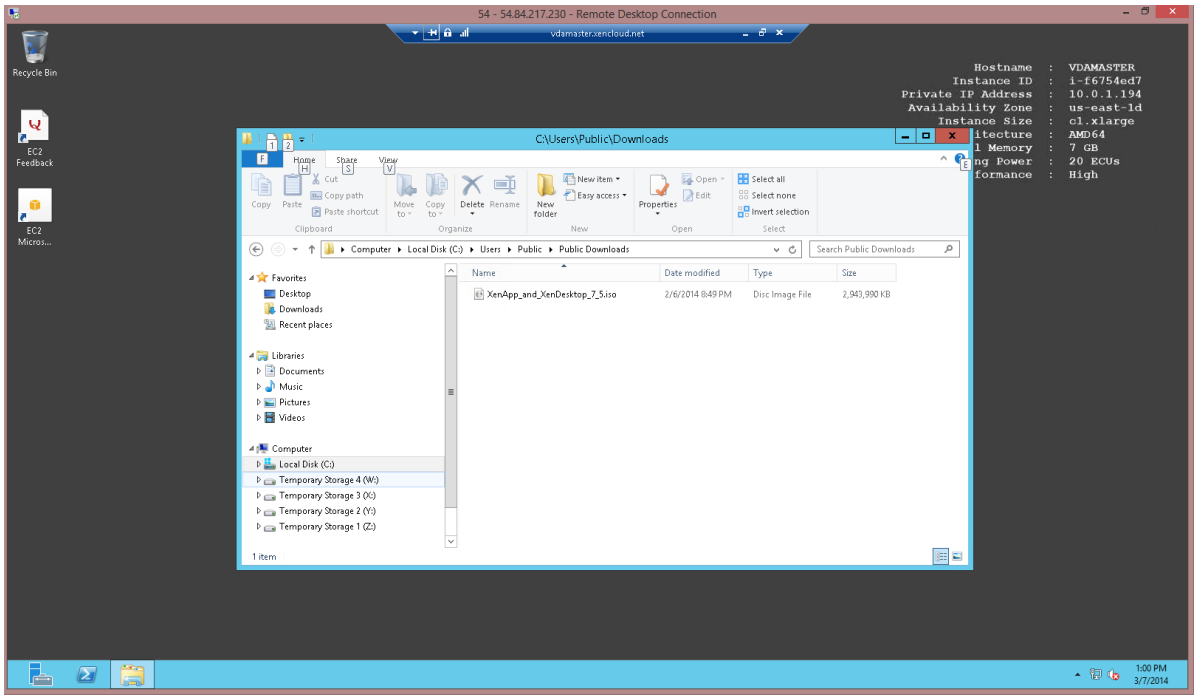
12. Vérifiez les paramètres spécifiés pour le VDA principal, puis sélectionnez **Installer** pour procéder à l'installation du VDA principal.

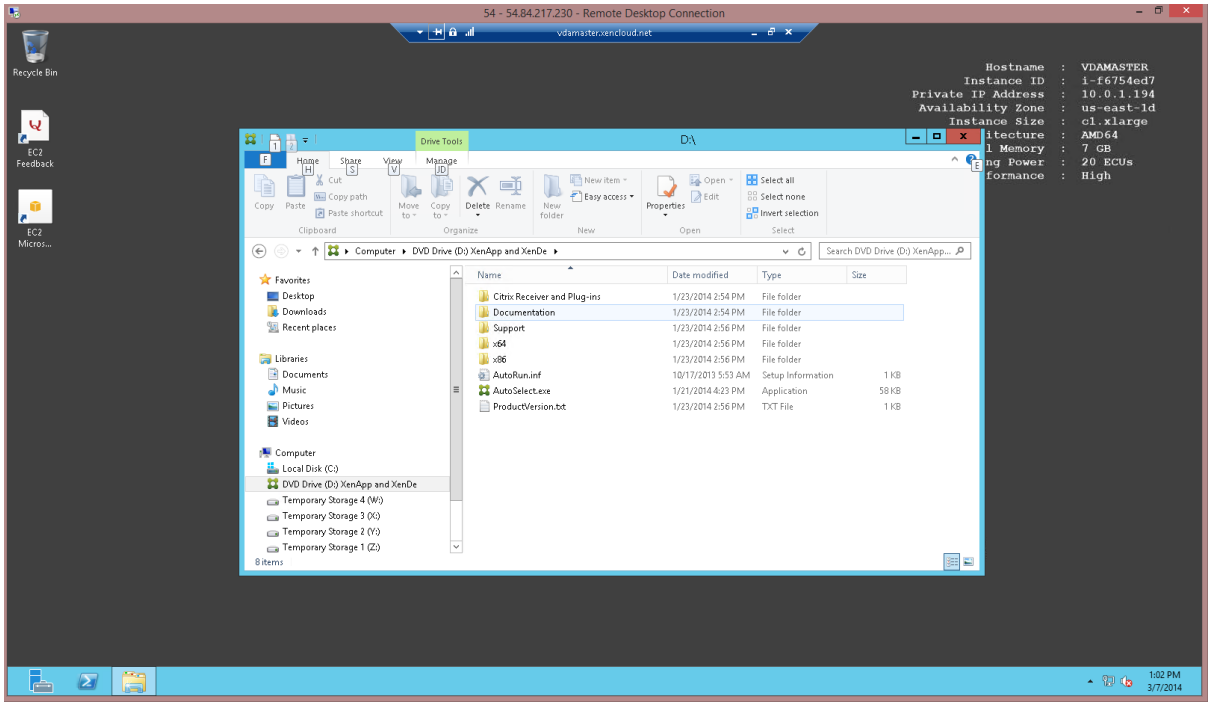
Remarque : vous devez redémarrer la machine pour terminer l'ajout de l'hôte de session Bureau à distance de Microsoft. Vous pouvez redémarrer à partir de l'instance ; vous n'avez pas besoin d'utiliser la console AWS pour redémarrer. Après le redémarrage, il faut parfois plusieurs minutes pour que l'instance réponde de nouveau aux connexions RDP.



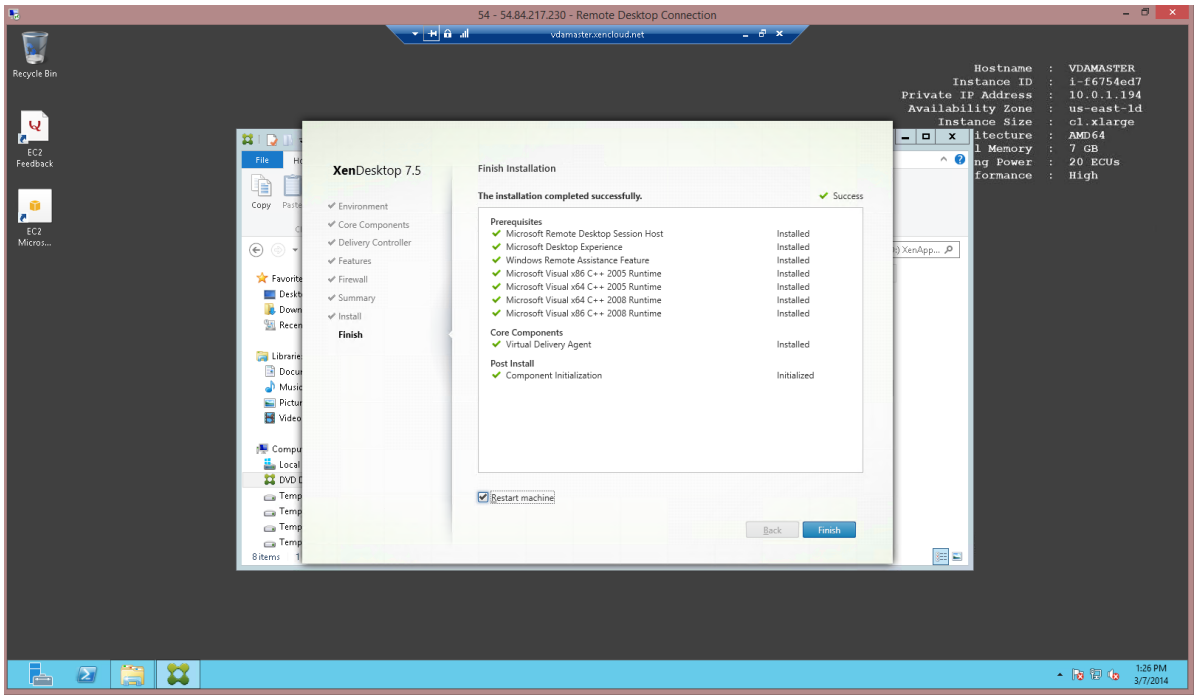
13. Après le redémarrage de la machine, ouvrez une session sur le VDA principal. Le support d'installation de XenApp et XenDesktop n'est plus monté (il recherche le support) et l'installation ne peut pas continuer.

14. Cliquez sur **Annuler** et remontez le support à partir de son emplacement. Par exemple, `C:\Utilisateurs\Public\Téléchargements`.



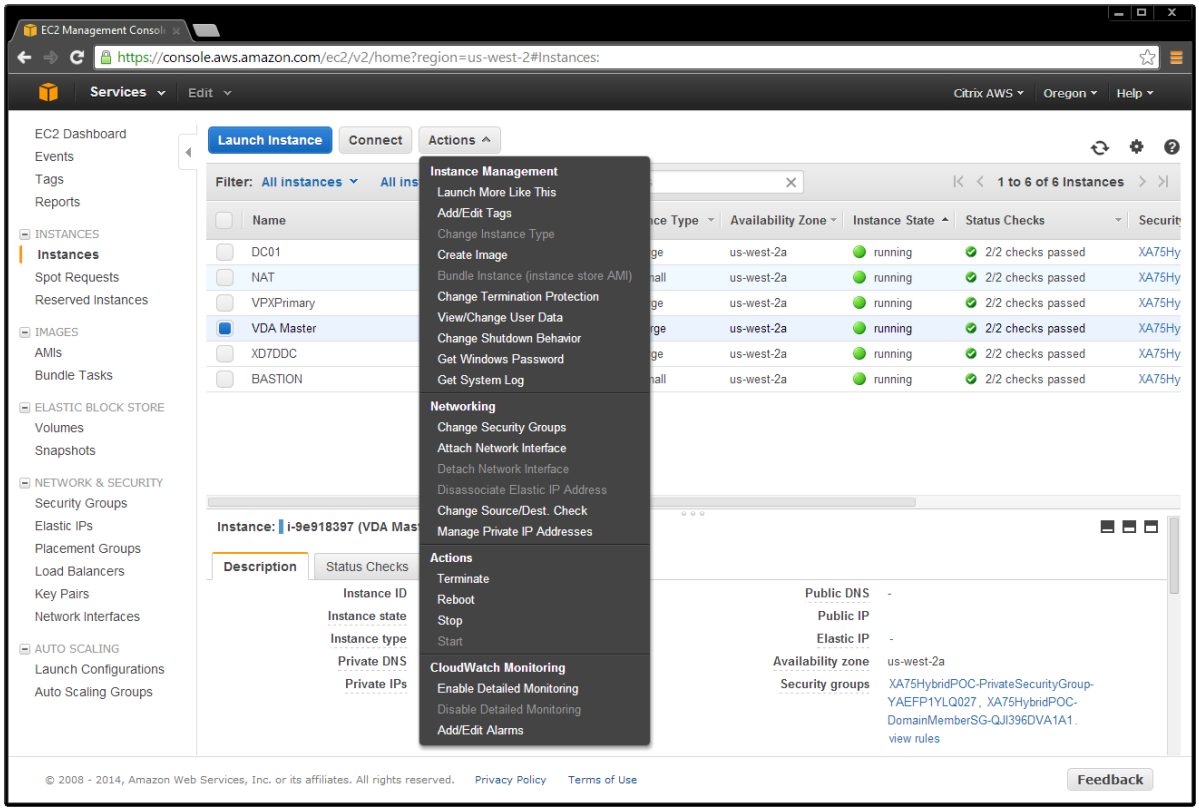


15. Lorsque le support est monté, sélectionnez **Installation de Virtual Delivery Agent pour Windows**, et l'installation se poursuit automatiquement là ou vous l'aviez laissée.
16. Redémarrez la machine.

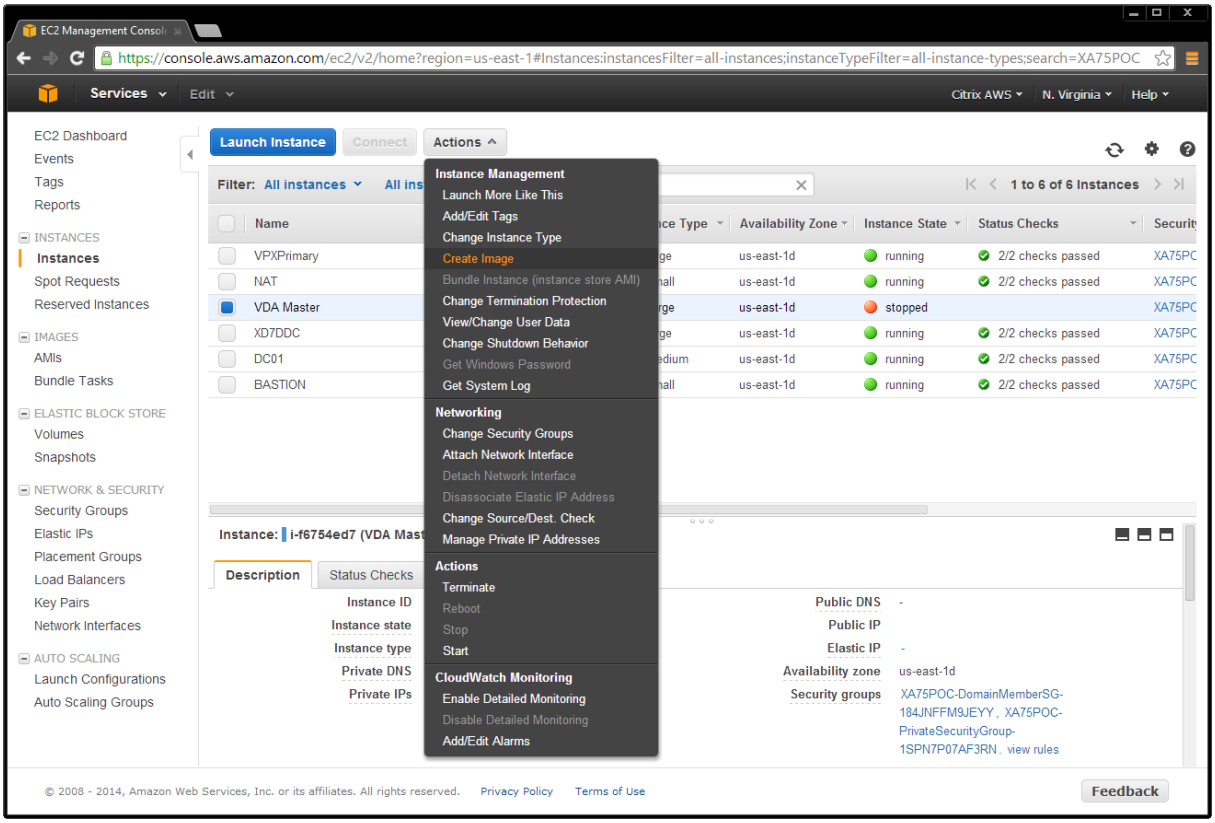


17. Une fois l'installation du VDA terminée, installez les applications qui seront publiées ou mises à disposition sur les bureaux des utilisateurs sur le VDA principal.

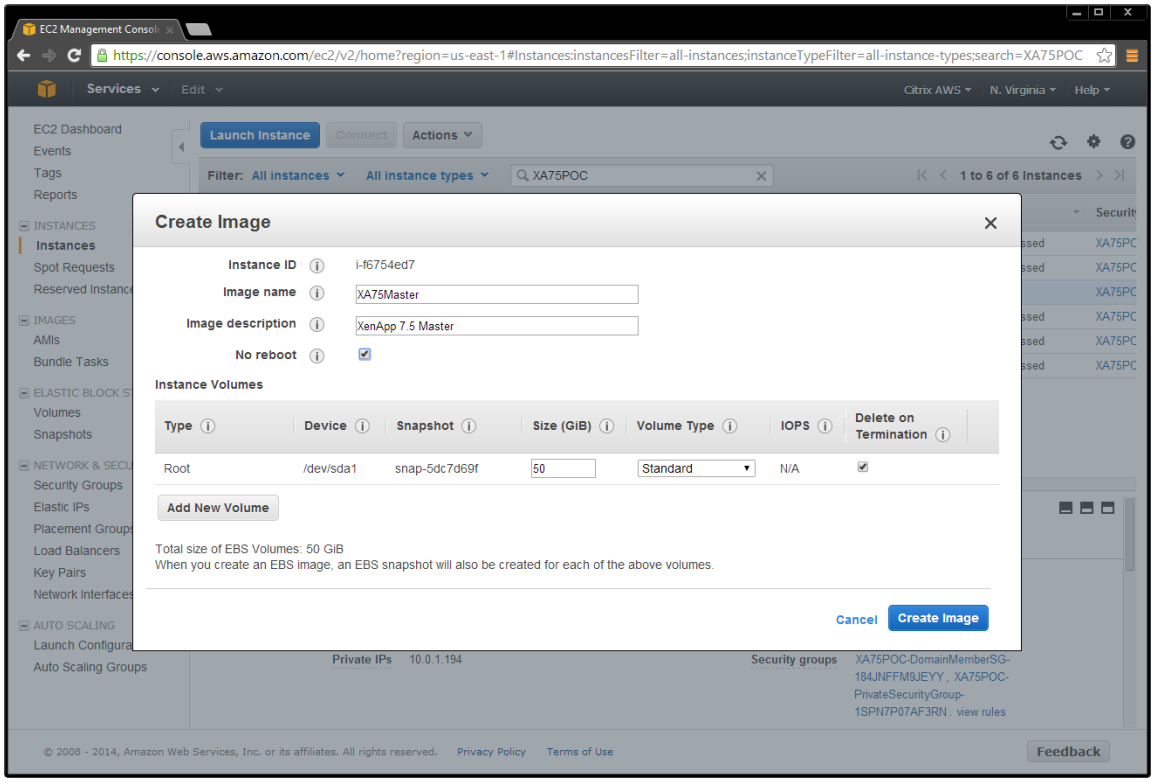
18. Après avoir installé des logiciels supplémentaires, à partir de la console EC2, sélectionnez **Actions > Stop** pour arrêter l'image principale du VDA.



19. Une fois l'image arrêtée, créez une AMI à partir de votre VDA principal en sélectionnant **Actions > Create Image**.



20. Attribuez un nom et une description, puis cliquez sur **Create Image**.



Important : l'option **Delete on Termination** (Supprimer une fois l'image créée) est sélectionnée par défaut. **Ne modifiez pas ce paramètre**. Le produit suppose que les volumes de disques racines sont supprimés automatiquement par Amazon. Si vous désélectionnez cette case, des fuites de volumes dans le stockage EBS risquent de se produire dans le déploiement.

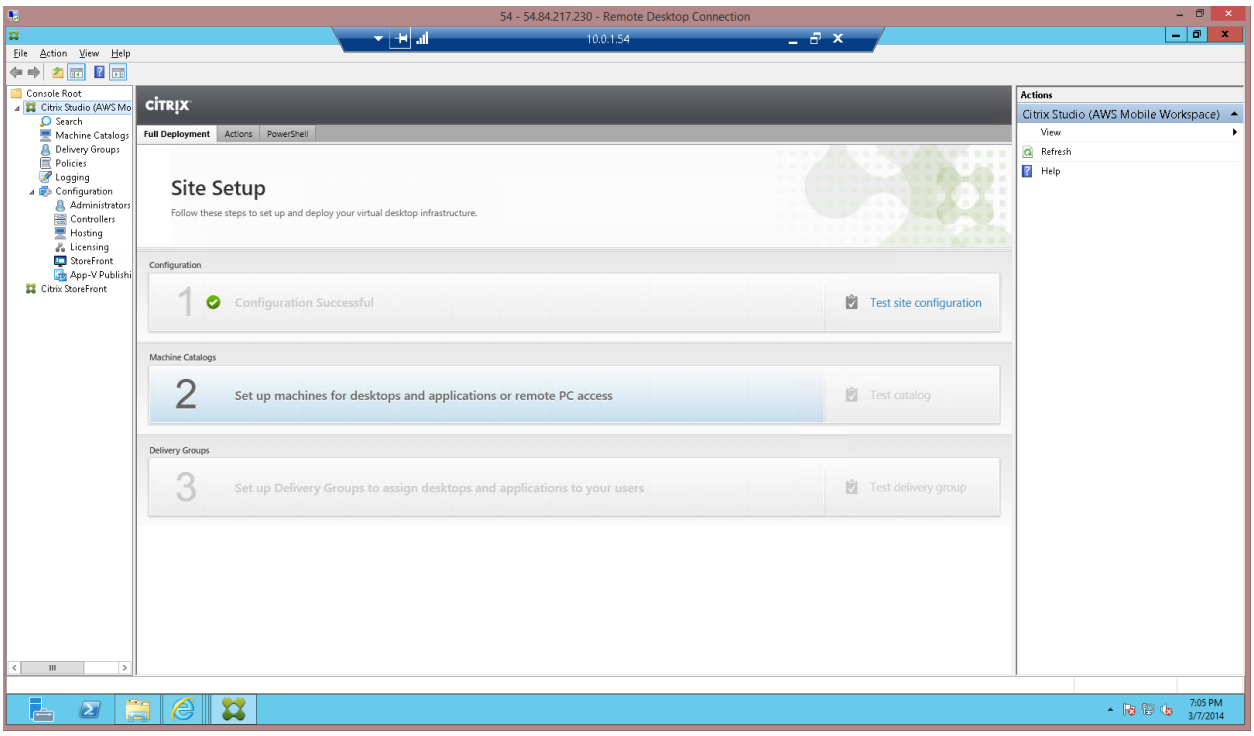
Selon la taille du volume de l'instance, la création de l'image peut prendre beaucoup de temps. Vous devez attendre que l'image soit entièrement créée avant de pouvoir l'afficher dans Studio.

Lorsque le processus de création de l'AMI est terminé, définissez des machines dans Studio à l'aide de l'AMI du VDA principal.

Définir des machines dans Studio à l'aide de l'AMI du VDA principal

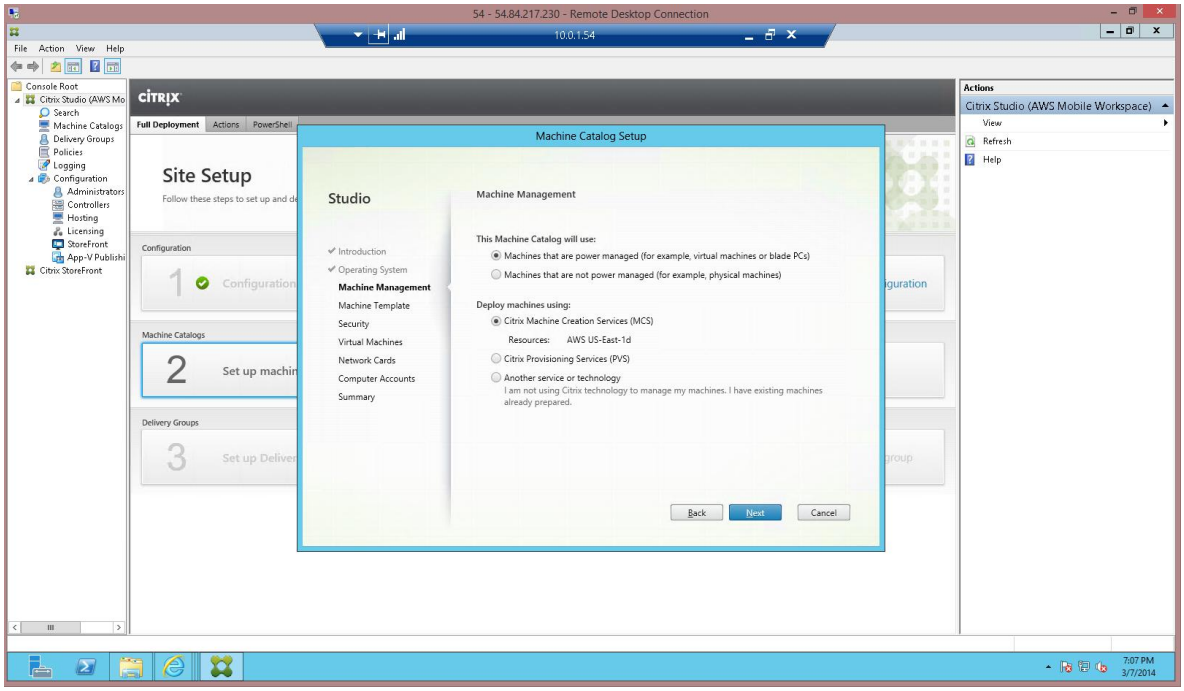
Maintenant que l'AMI principale est configurée, utilisez Studio pour provisionner des bureaux et des applications en créant un catalogue de machines.

1. Ouvrez Studio sur le Delivery Controller et sélectionnez **l'option 2**.



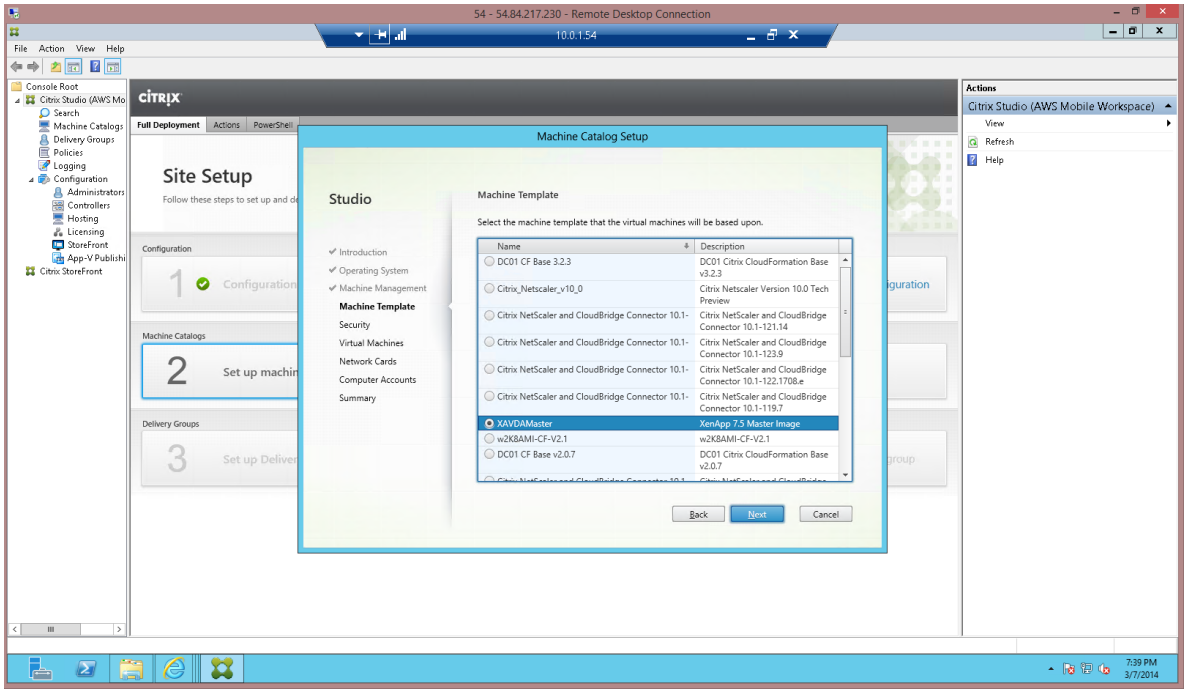
2. Sélectionnez **OS serveur**. Si votre configuration est dotée de la fonctionnalité Server VDI sur un système d'exploitation de bureau, vous pouvez également choisir l'option **OS de bureau**.

3. Pour permettre à XenApp ou XenDesktop de contrôler le provisioning de machines dans AWS, sélectionnez les paramètres indiqués dans cet exemple :



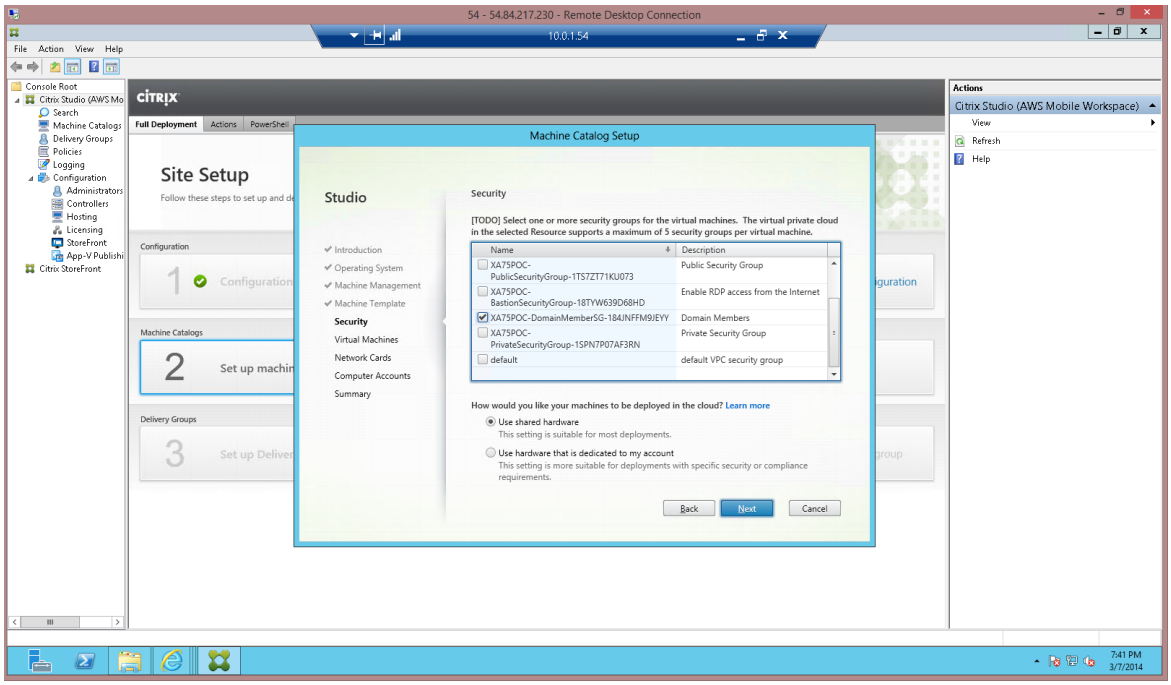
Remarque : AWS ne prend pas en charge Citrix Provisioning Services.

4. Sélectionnez le modèle de machine que l'AMI a créé dans la console EC2 comme décrit dans la section Configurer la machine VDA principale.

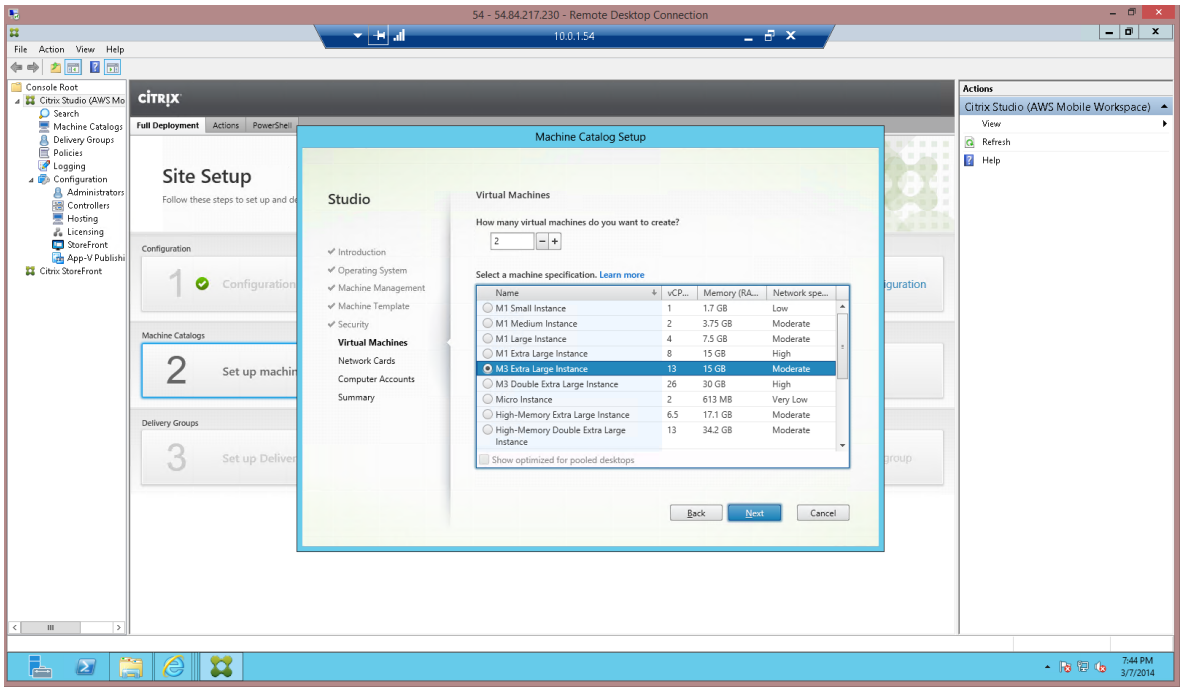


5. Sélectionnez les groupes de sécurité requis. Dans cet exemple, vous devez sélectionner le groupe de sécurité Domain Members ainsi que le groupe de sécurité privé **PrivateSecurityGroup**. Cela garantit la communication entre le contrôleur de domaine et les VDA.

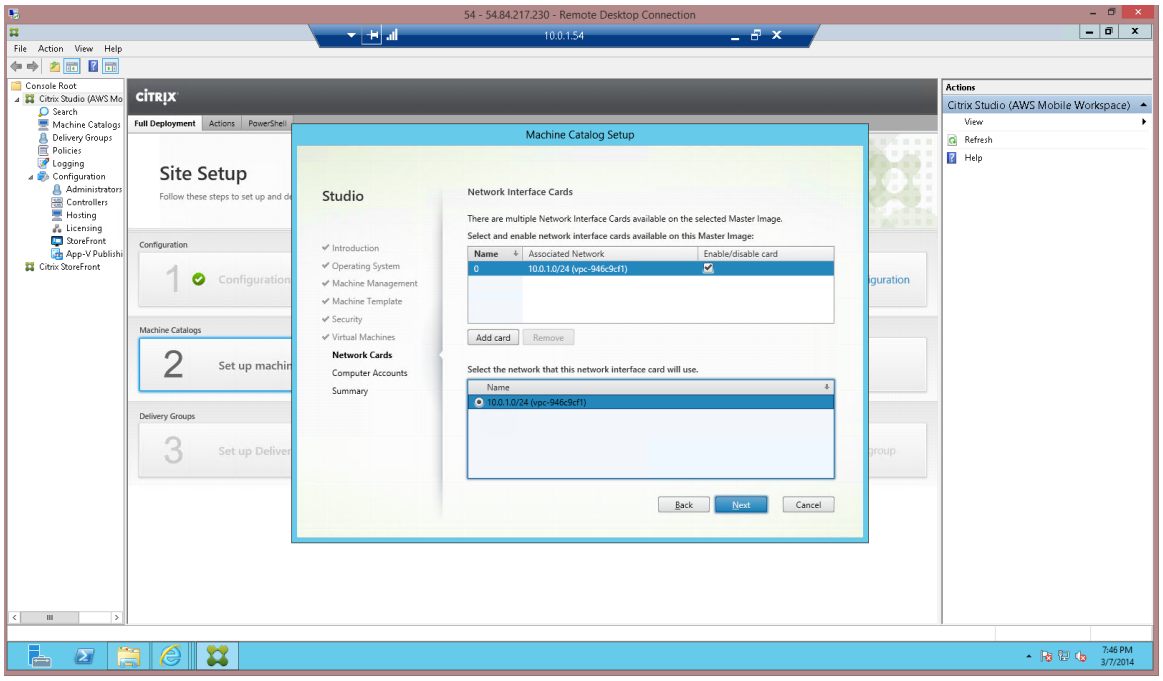
   Vous pouvez également indiquer que du matériel dédié est requis pour héberger vos instances. **Utiliser le matériel partagé** est la valeur par défaut.



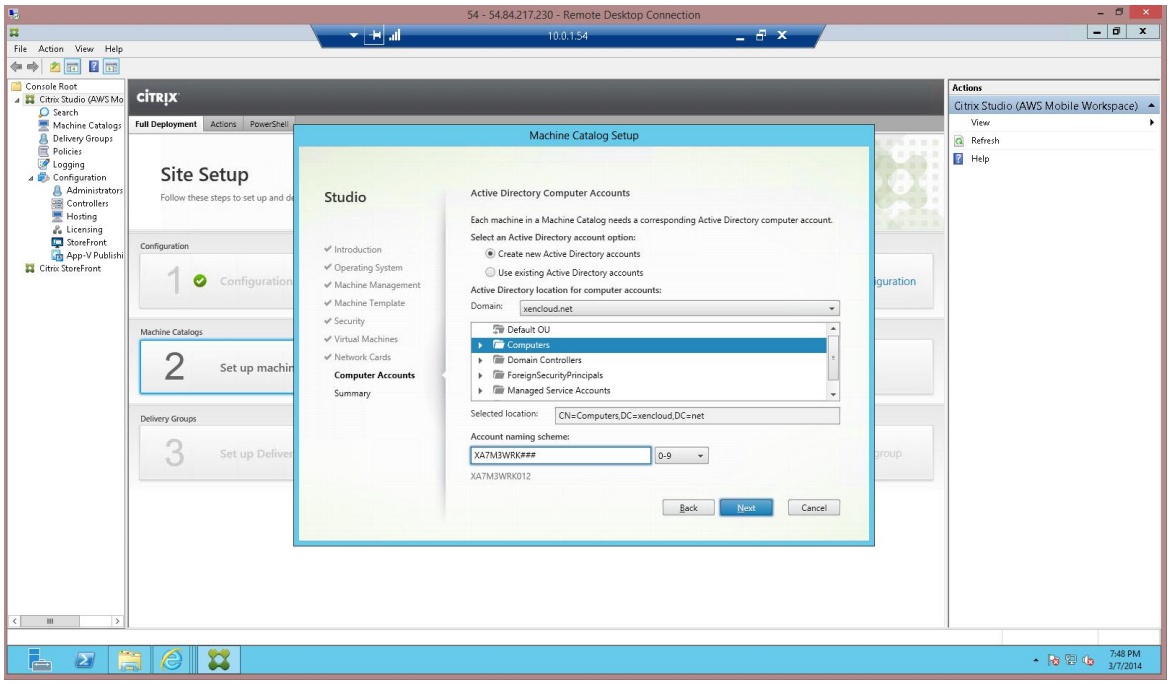
6. Sélectionnez le nombre de machines et le type d'instance pour le catalogue de machines.



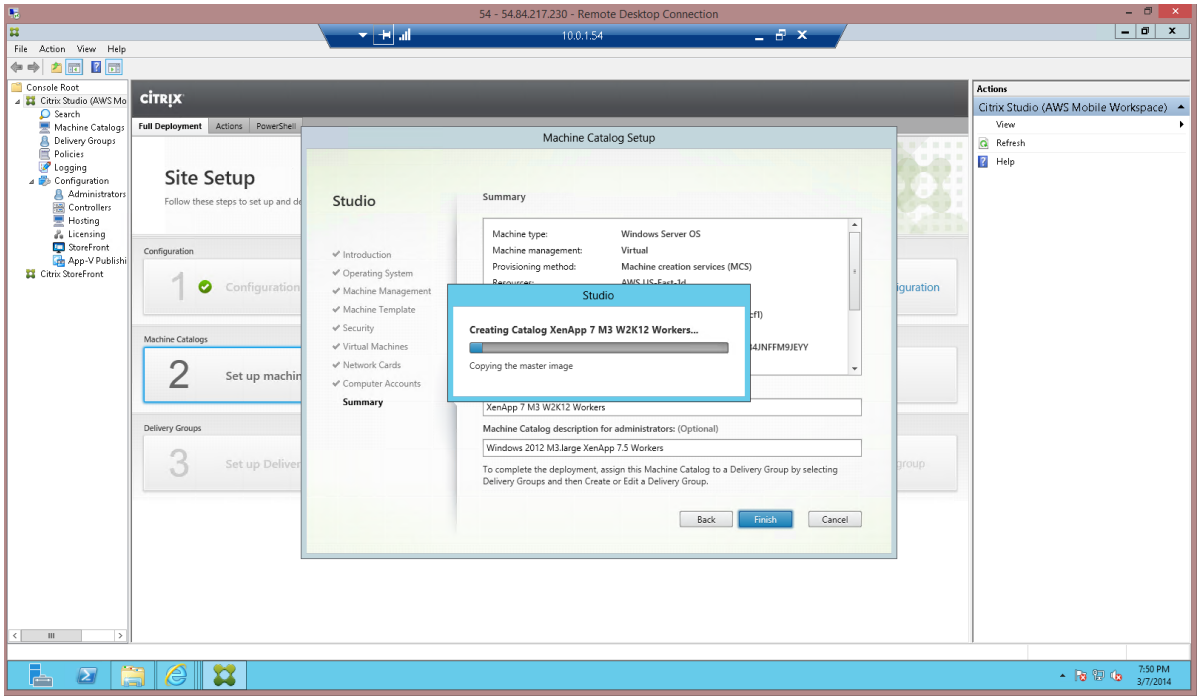
7. Sélectionnez la configuration réseau.



8. Configurez les comptes d'ordinateurs.



9. Entrez un nom et cliquez sur **Terminer**. Veuillez noter que le processus de copie de l'image principale peut prendre beaucoup de temps. Il peut prendre de 30 à 40 minutes ou plus si le catalogue contient beaucoup de machines.



Définir des groupes de mise à disposition

Après avoir configuré des machines dans le catalogue de machines, configurez des groupes de mise à disposition afin de spécifier les utilisateurs autorisés à accéder aux applications ou bureaux que vous souhaitez fournir. Les groupes de mise à disposition sont généralement basés sur les caractéristiques de l'utilisateur, telles que la fonction qu'il occupe ou sa région géographique.

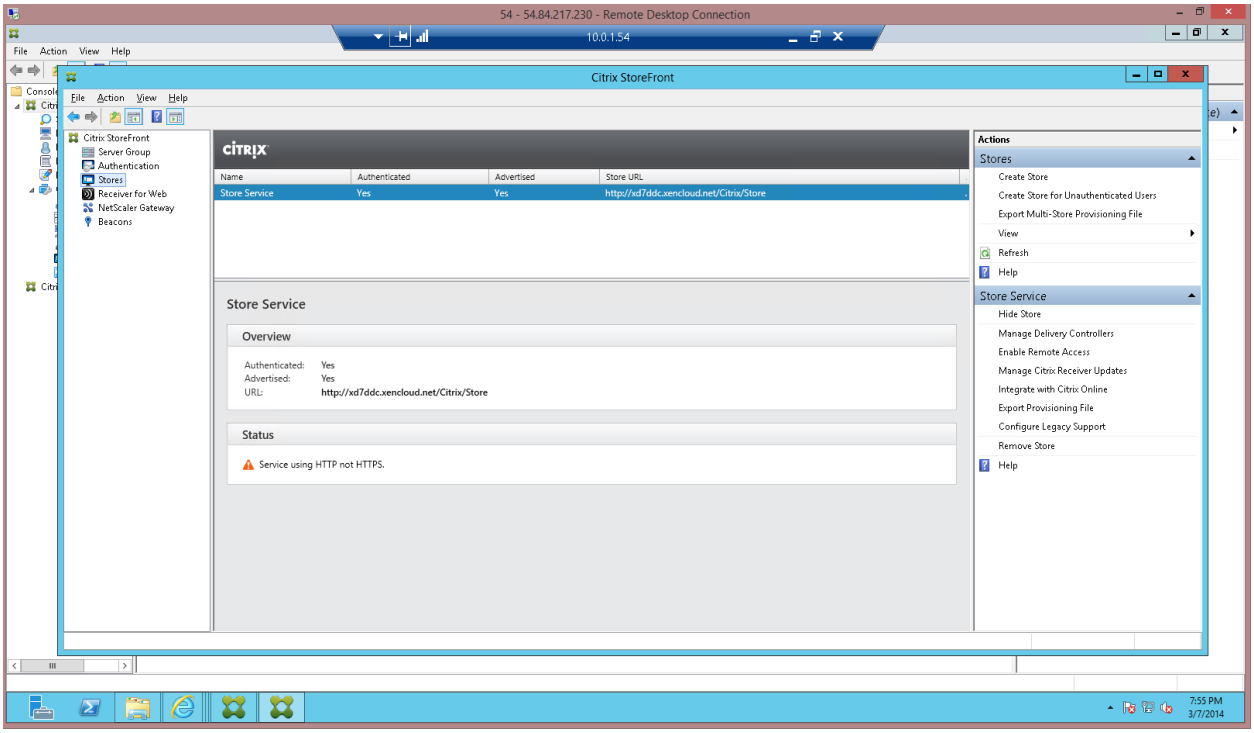
1. Dans Studio, sélectionnez le nœud Groupe de mise à disposition et cliquez sur **Créer un groupe de mise à disposition**.
2. Cliquez sur **Ajouter des machines**, sélectionnez un catalogue de machines pour ce groupe de mise à disposition, et entrez le nombre de machines que le groupe utilise dans le catalogue de machines.
3. Sur la page Utilisateurs, cliquez sur **Ajouter des utilisateurs** pour ajouter les utilisateurs ou les groupes d'utilisateurs pouvant accéder aux bureaux ou applications. Vous pouvez sélectionner des groupes d'utilisateurs en effectuant une recherche ou en entrant une liste d'utilisateurs et de groupes Active Directory en les séparant par des points-virgules. Pour les groupes de mise à disposition avec OS de bureau, vous pouvez importer les données de l'utilisateur depuis un fichier après création du groupe.
4. Sur la page Type de mise à disposition, sélectionnez ce que les bureaux mettent à la disposition des utilisateurs :
    - Applications uniquement
    - Bureaux uniquement
    - Applications et bureaux
5. Sur la page StoreFront, sélectionnez les URL StoreFront à envoyer à Citrix Receiver afin que Receiver puisse se connecter à StoreFront sans intervention de la part de l'utilisateur. Notez que ce paramètre s'applique aux Receiver exécutés sur les VDA.
6. Sur la page Étendues, définissez les administrateurs autorisés à accéder au groupe de mise à disposition.
7. Sur la page Résumé, vérifiez toutes les informations et entrez un nom d'affichage visible par les utilisateurs et administrateurs ainsi qu'un nom de groupe de mise à disposition descriptif que seuls les administrateurs peuvent voir.

Configurer l'accès distant à NetScaler Gateway

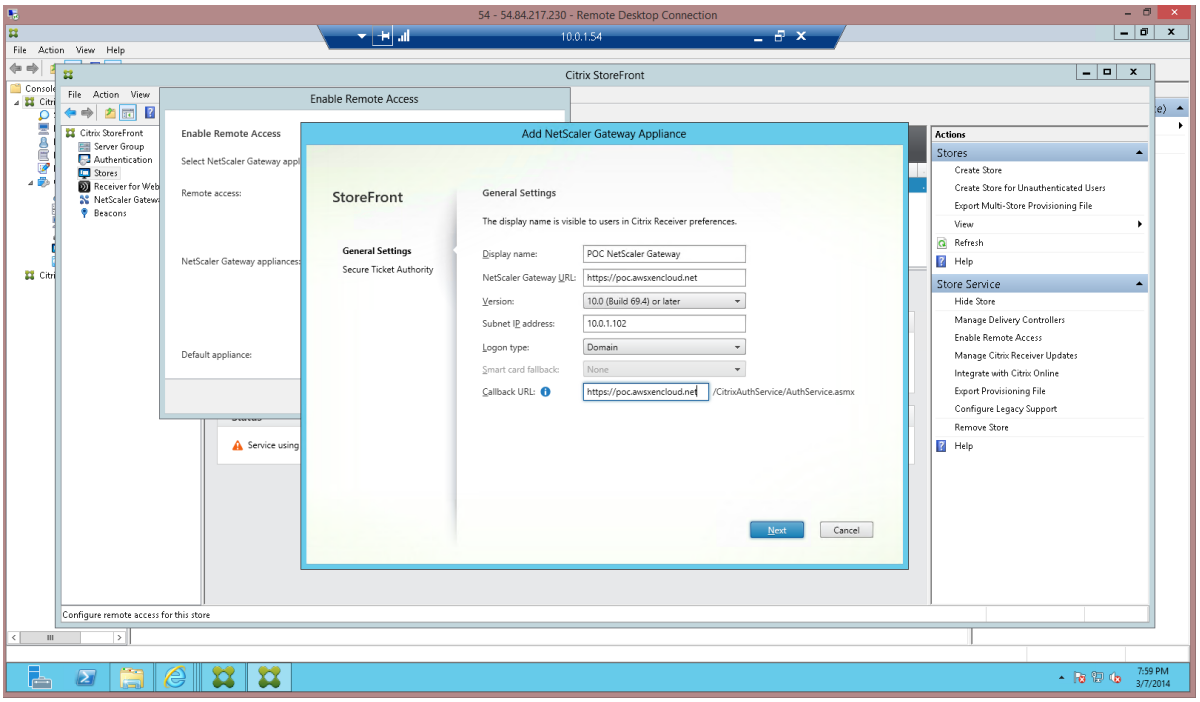
Après avoir provisionné des bureaux et des applications au travers de Studio, configurez l'accès à StoreFront en configurant l'accès distant à NetScaler Gateway. Les utilisateurs distants accèdent et s'authentifient auprès de NetScaler Gateway. Après validation, NetScaler Gateway transmet la demande de l'utilisateur à StoreFront, qui génère une liste des applications et bureaux disponibles.

Configurer StoreFront

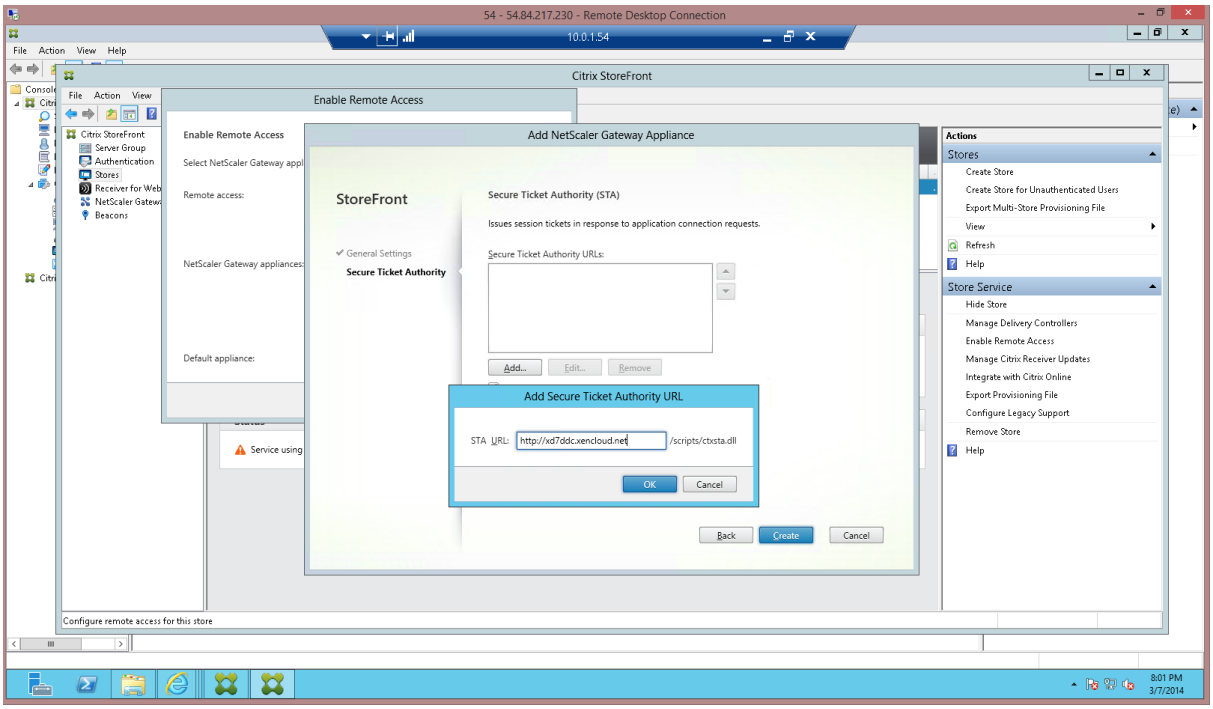
1. Exécutez la console d'administration StoreFront sur le Delivery Controller et activez l'accès distant.



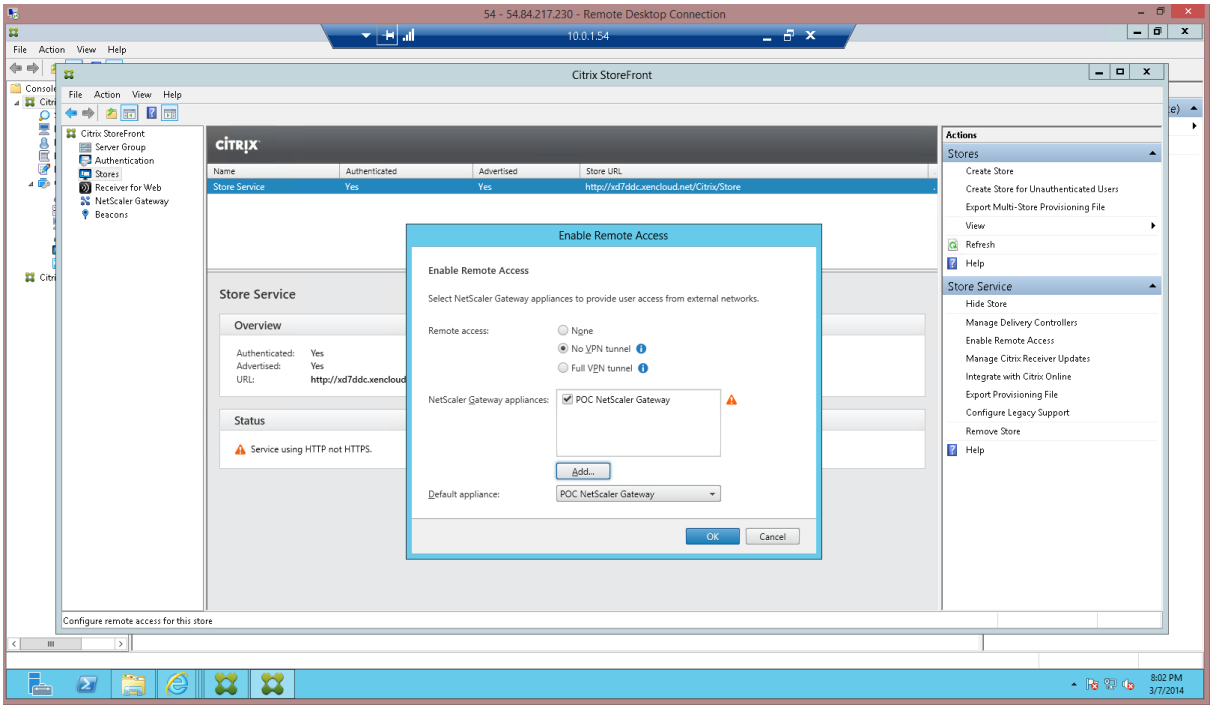
2. Dans l'assistant d'accès à distance à StoreFront, entrez les paramètres de votre configuration NetScaler publique, telle que le nom de domaine complet et l'adresse IP du sous-réseau (SNIP) NetScaler. Dans cet exemple, l'adresse **SNIP** est **10.0.1.102**.



3. Ajoutez la Secure Ticket Authority (STA), qui est le Delivery Controller.

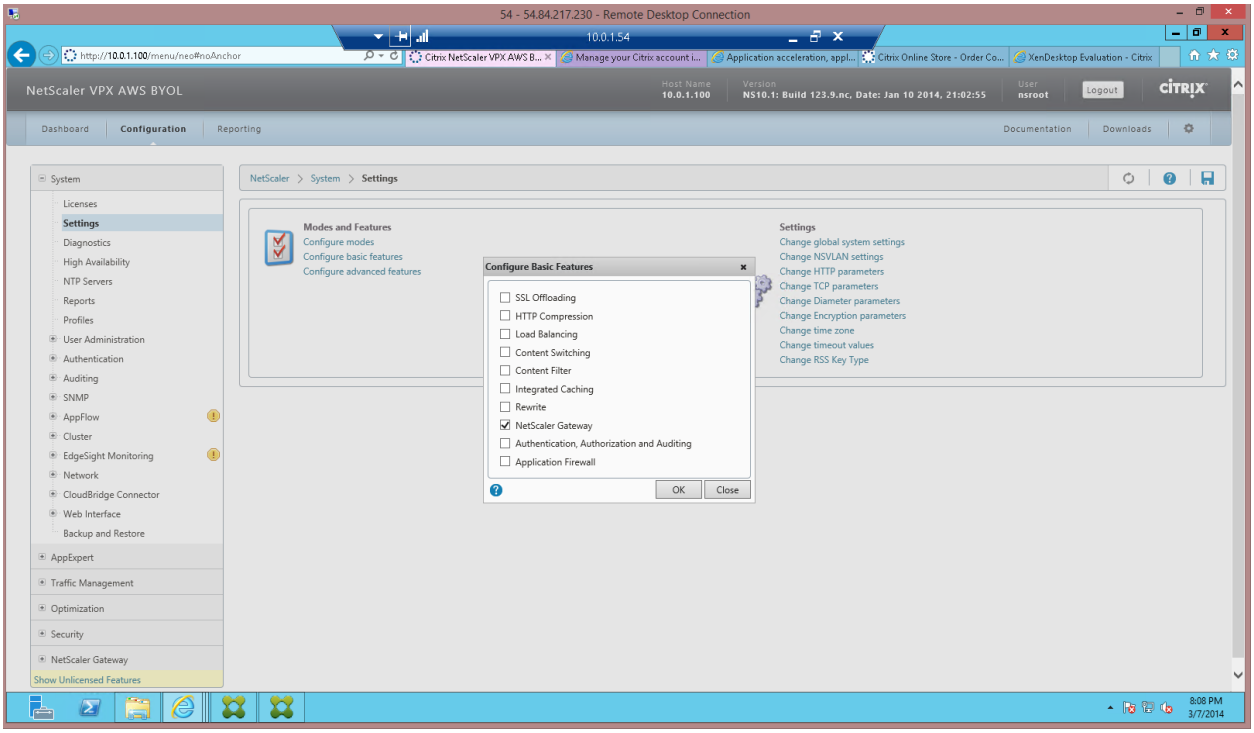


4. Cliquez sur **OK**, puis sur **Créer** pour compléter la définition de NetScaler Gateway pour StoreFront.



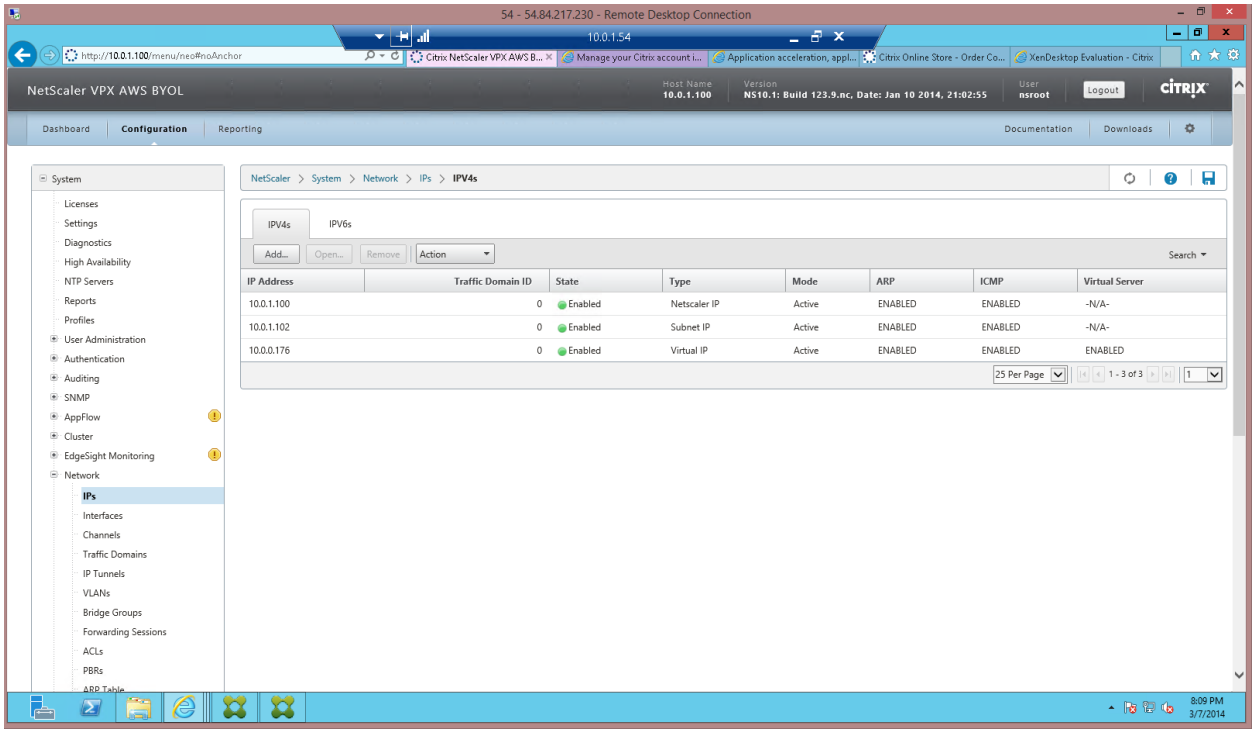
5. Cliquez sur **OK** pour terminer le processus d'activation de l'accès à distance.
6. Activez la fonction NetScaler Gateway.
    a. Connectez une machine sur le sous-réseau privé à l'adresse SNIP (10.0.1.100).
    b. Ouvrez une session à NetScaler.

7. Sur NetScaler Gateway, vous devez utiliser l'adresse IP de sous-réseau et activer le transfert MAC.



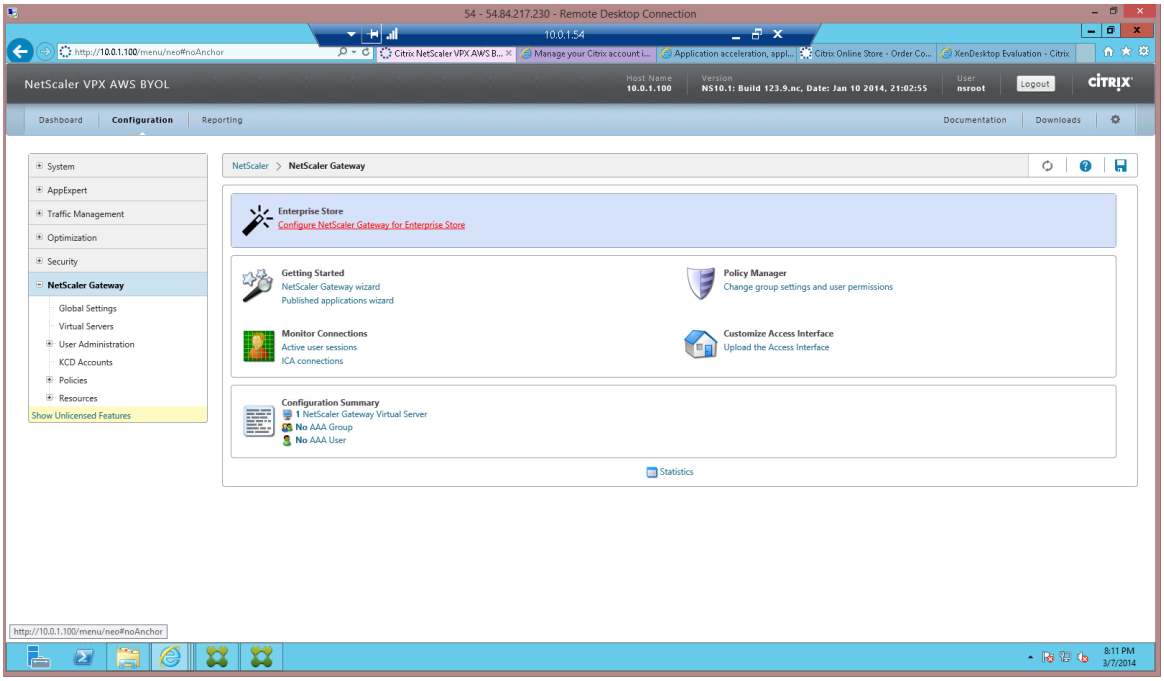
8. Créez les connexions réseau suivantes :
    a. **SNIP** avec l'adresse IP **10.0.1.102** sur le serveur NetScaler
    b. **VIP** avec l'adresse IP **10.0.0.176** sur le client NetScaler

Le modèle CloudFormation ou la procédure de configuration manuelle a déjà configuré ces adresses sur la couche AWS de NetScaler VPX.

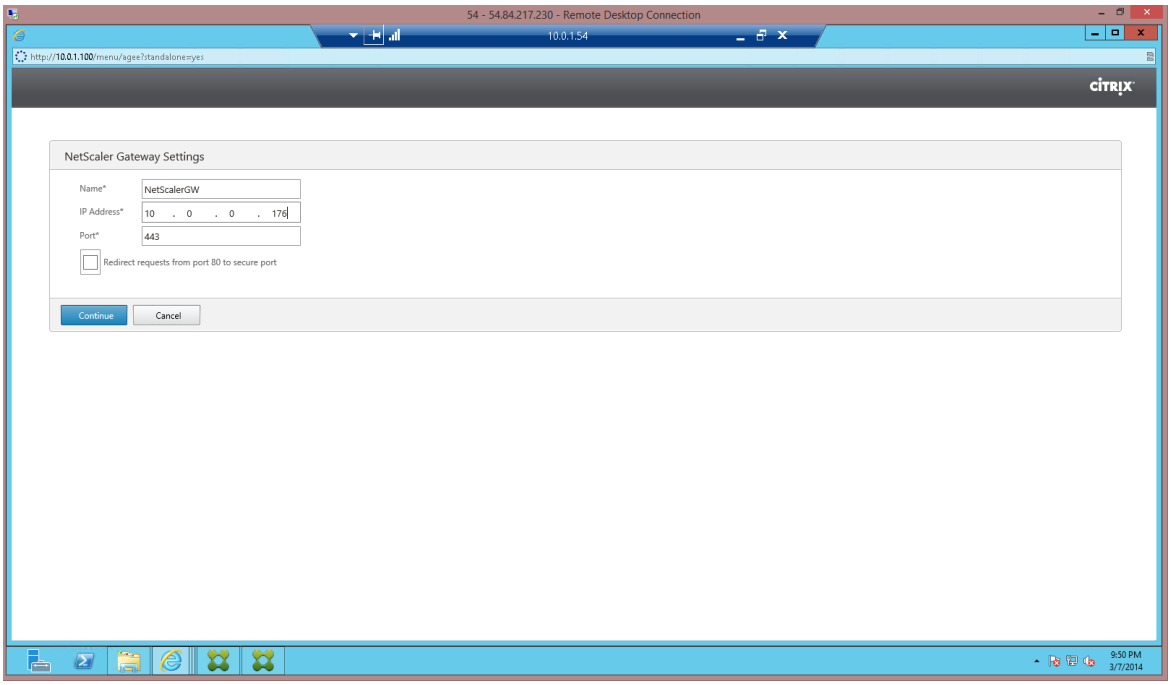


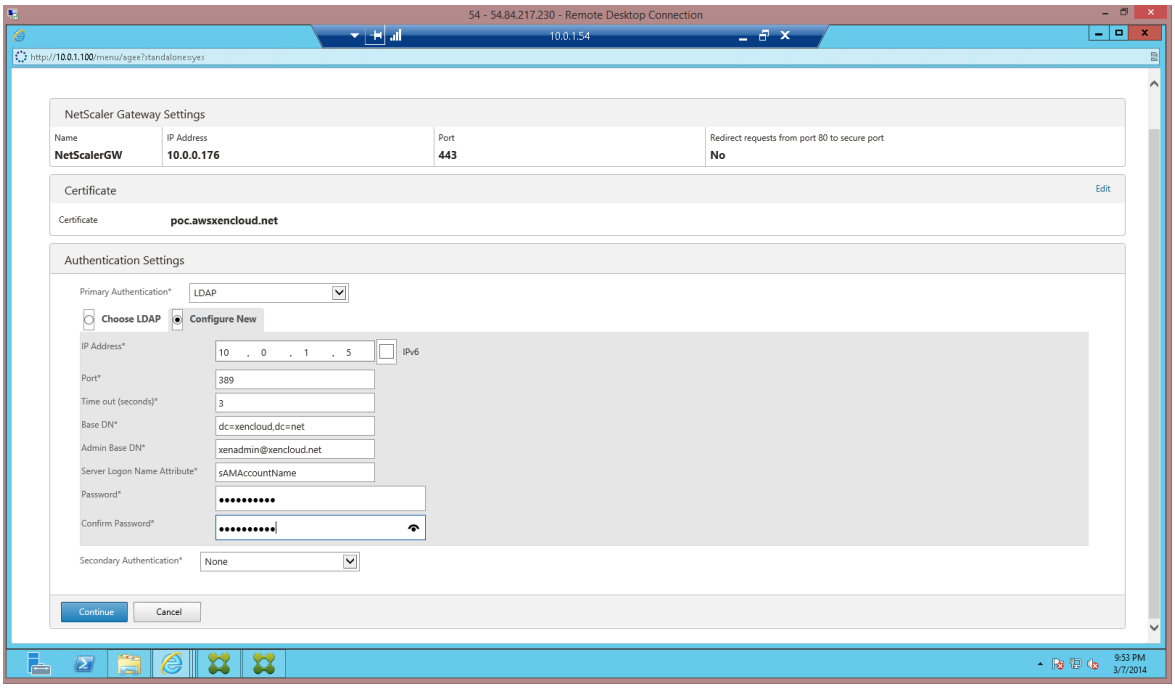
Configurer NetScaler Gateway à l'aide de l'assistant Enterprise Store

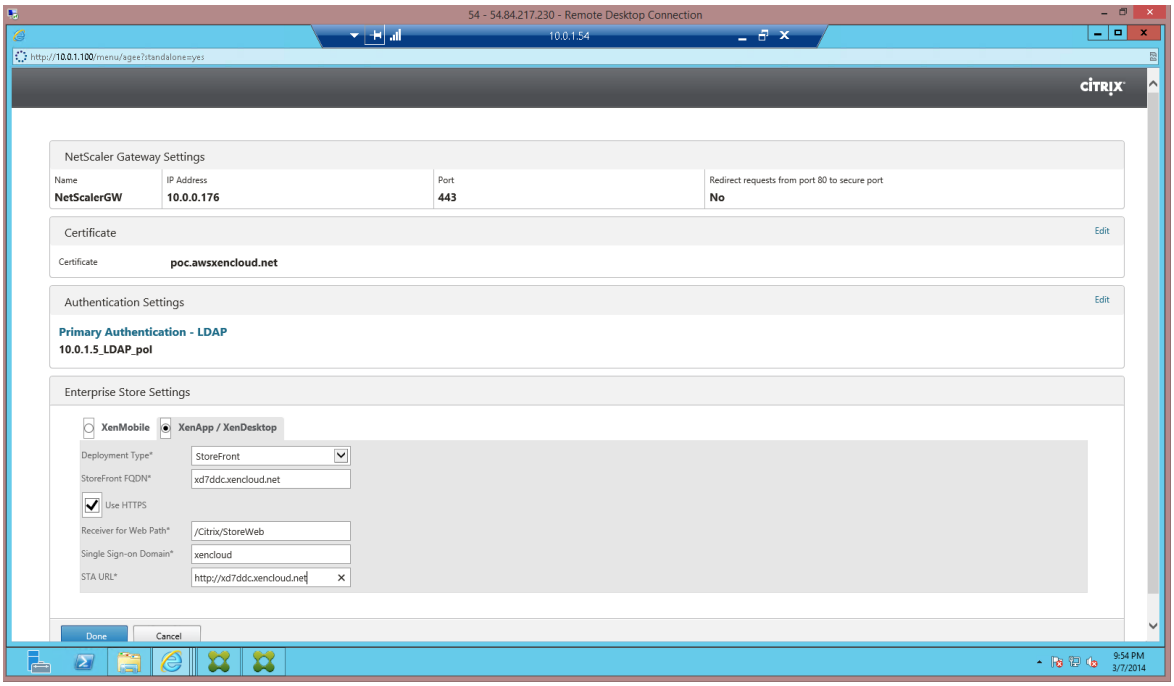
1. Lancez l'assistant Enterprise Store.



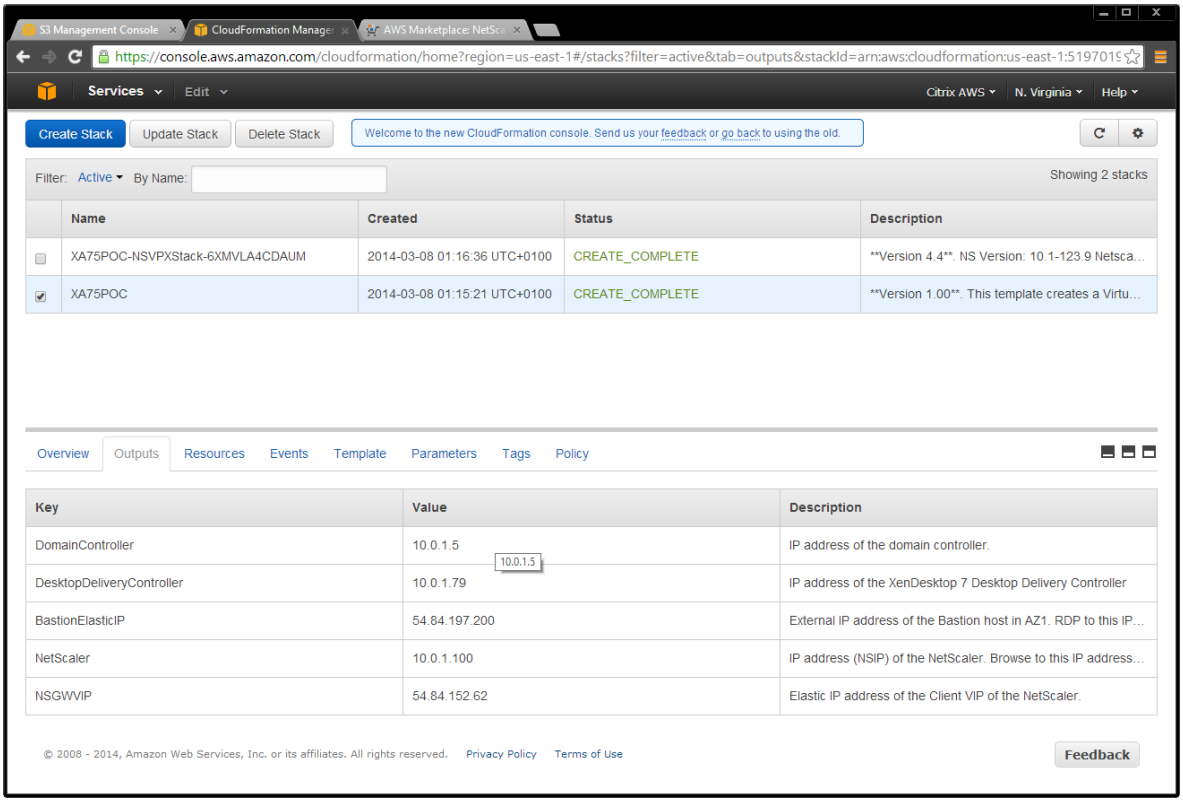
2. Assurez-vous que l'adresse VIP utilisée pour le serveur virtuel NetScaler Gateway est définie sur **10.0.0.176**. Le modèle CloudFormation configure cette adresse VIP afin qu'elle pointe vers une adresse IP élastique.



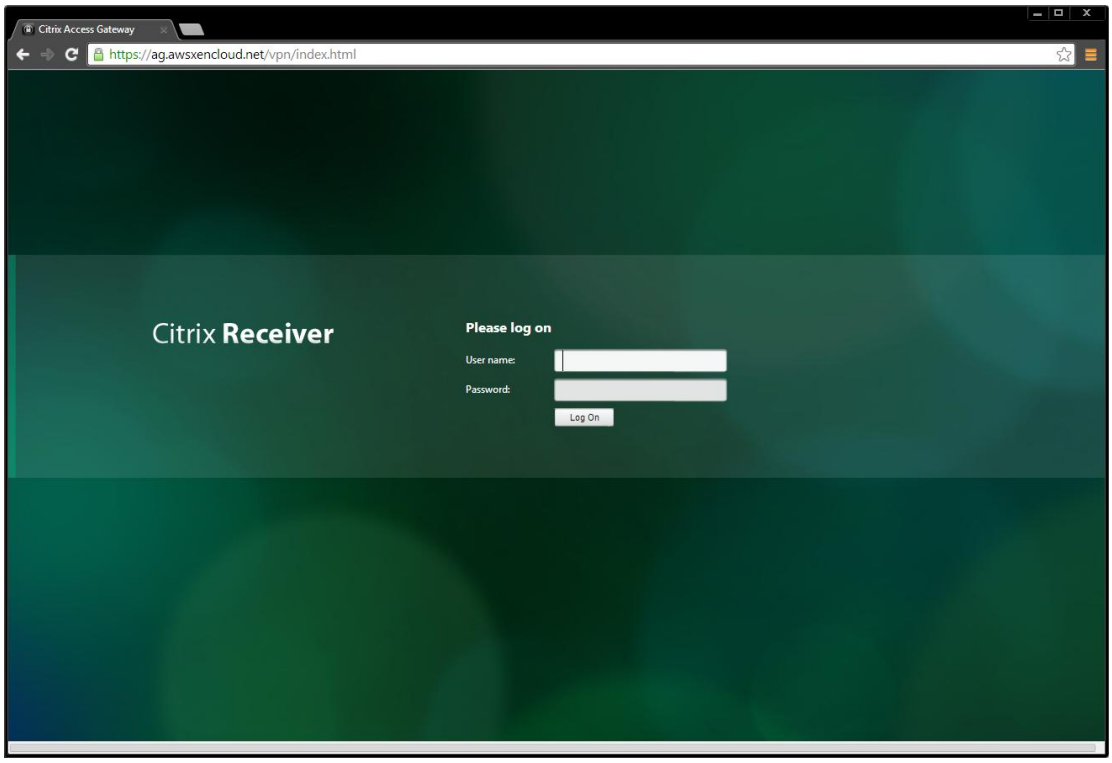


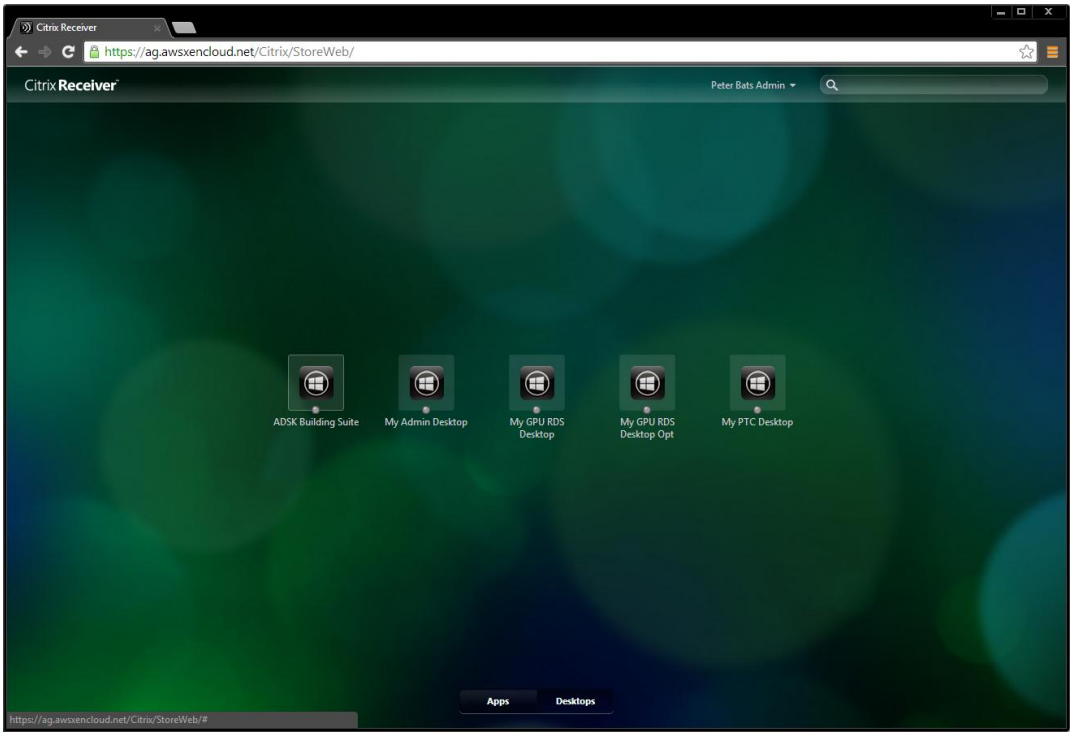


3. Recherchez l'adresse IP élastique de votre adresse VIP à l'aide de la console EC2. La section de sortie CloudFormation affiche l'adresse EIP associée à l'adresse VIP (NSGWVIP).



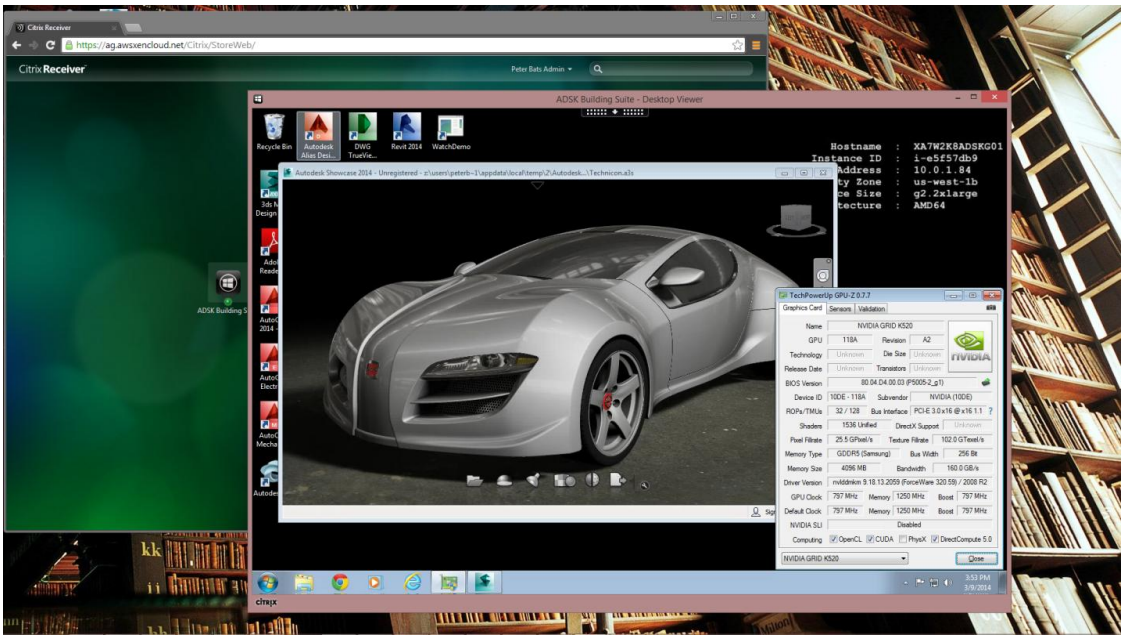
4. Procédez à la configuration de XenApp ou XenDesktop :
   - Placez un certificat sur votre boîtier NetScaler Gateway et affectez-le dans le DNS. Vous pouvez également placer une entrée dans votre fichier hôtes pointant vers l'adresse IP élastique.
   - Créez un groupe de mise à disposition et publiez des applications et des bureaux.



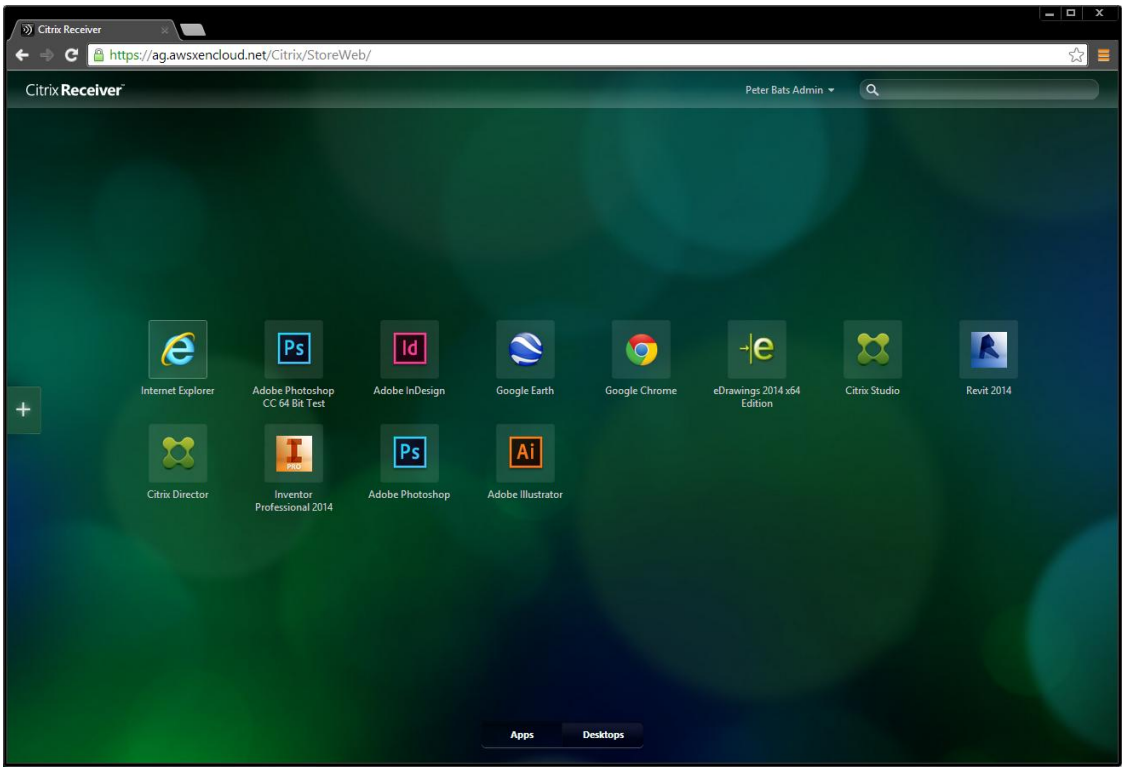


Exemples

L'exemple suivant illustre un bureau lancé à l'aide d'une instance AWS g2.2xlarge (modèle), qui permet la prise en charge de HDX 3D Pro :



L'exemple suivant illustre des applications :



L'exemple suivant illustre des applications lancées :

Créer des AMI modèle à partir d'autres modèles

Vous pouvez créer des AMI modèle en lançant une instance à partir d'une machine virtuelle (VM) que vous avez importée à partir de Citrix XenServer, Microsoft Hyper-V, VMware Workstation où VMware vSphere. Pour créer l'AMI modèle, vous pouvez :

- Exporter vos images Windows ou modèles existants à partir de votre environnement de virtualisation local à l'aide des outils de virtualisation de l'environnement.
- Importer l'image ou le modèle vers Amazon EC2 à l'aide de la ligne de commande Amazon EC2 ou des outils API.

Consultez la section Importing EC2 Instances dans le AWS EC2 User guide pour obtenir des instructions détaillées sur l'importation de VM.

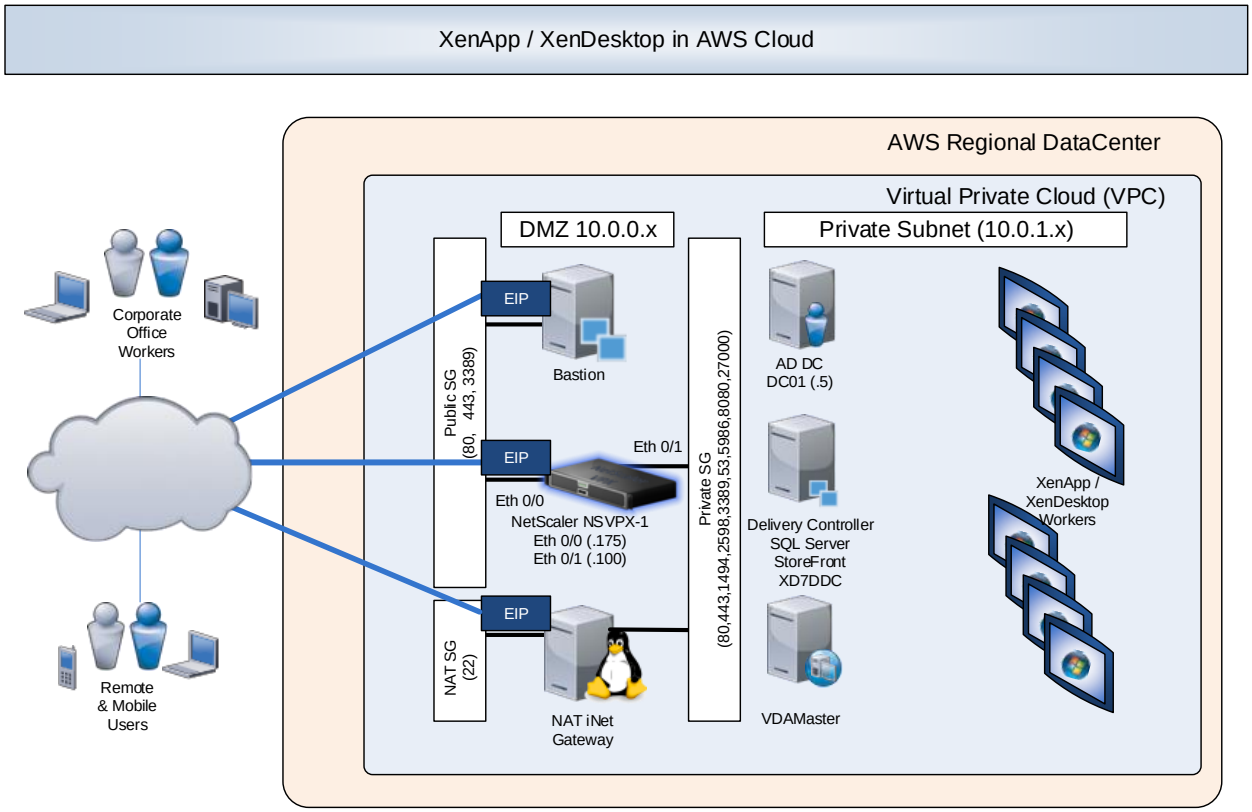
Une fois que vous avez importé votre modèle et créé une instance comme décritdans la section Importing EC2 Instances, vous pouvez en faire une AMI comme avec toute autre instance.

Annexe

Déployer manuellement XenApp et XenDesktop dans AWS

Une solution alternative à l'utilisation d'un modèleCloudFormation AWS consiste à déployer XenApp et XenDesktop sur AWS à l'aide de procédures manuelles, comme illustré dans l'exemple suivant.

Infrastructure de site déployée manuellement



Sécurité et mappages de pare-feu

Cette section dresse la liste des spécificités réseau utilisées dans cet exemple d'installation manuelle.

Groupe de sécurité NAT

Entrant				Sortant		
Type	**Trafic**	**Source**		**Type**	**Trafic**	**Source**
Tout	Tout	privateSG		Tout	Tout	0.0.0.0/0
TCP	22 (SSH)	0.0.0.0/0				

Règles du groupe de sécuritépublicSG

Entrant				Sortant		
Type	**Trafic**	**Source**		**Type**	**Trafic**	**Source**
Tout	Tout	publicSG		Tout	Tout	0.0.0.0/0
	Tout	publicSG			Tout	privateSG
ICMP	Tout	0.0.0.0/0		ICMP	Tout	0.0.0.0/0
TCP	22 (SSH)	0.0.0.0/0				
	80 (HTTP)	0.0.0.0/0				
	443 (HTTPS)	0.0.0.0/0				
	1494 (CA)	0.0.0.0/0				
	2598 (Sess)	0.0.0.0/0				
	3389 (RDP)	0.0.0.0/0				

Règles du groupe de sécurité privateSG

Entrant				Sortant		
Type	**Trafic**	**Source**		**Type**	**Trafic**	**Source**
Tout	Tout	NATSG		Tout	Tout	0.0.0.0/0
	Tout	privateSG			Tout	privateSG
ICMP	Tout	publicSG		ICMP	Tout	0.0.0.0/0
TCP	53 (DNS)	publicSG		UDP]	52 (DNS)	0.0.0.0/0
	80 (HTTP)	publicSG				
	135	publicSG				
	389	publicSG				
	443 (HTTPS)	publicSG				
	1494 (CA)	publicSG				
	2598 (Sess)	publicSG				
	3389 (RDP)	publicSG				
	49152 - 65535	publicSG				
UDP	53 (DNS)	publicSG				
	389 (LDAP)	publicSG				

AMI pertinentes pour sites XenApp et XenDesktop dans la région US-East-1

Fonction	Nom de l'AMI	ID de l'AMI	Réseau	Adresse IP
Contrôleur de domaine	Microsoft Windows Server 2012 Base Microsoft Windows Server 2008 R2 Base	ami-814642e8 ami-37b1b45e	privé	10.0.1.5
Delivery Controller	Microsoft Windows Server 2012 avec SQL Microsoft Windows Server 2008 R2 avec SQL	ami-e743478e ami-a1b9bcc8	privé	10.0.1.15
NetScaler Gateway	NetScaler VPX édition Platinum - 10 Mbits/s	ami-c995aaa0	Public SNIP VIP Privé NSIP SNIP	 10.0.0.175 10.0.0.176 10.0.1.100 10.0.1.102
Bastion	Microsoft Windows Server 2012 Base Microsoft Windows Server 2008 R2 Base	ami-814642e8 ami-37b1b45e	public	DHCP
NAT	ami-vpc-nat-1.1.0-beta.x86-64-ebs	ami-f619c29f	public	DHCP
VDAMaster	Microsoft Windows Server 2012 Base Microsoft Windows Server 2008 R2 Base	ami-814642e8 ami-37b1b45e	privé	DHCP

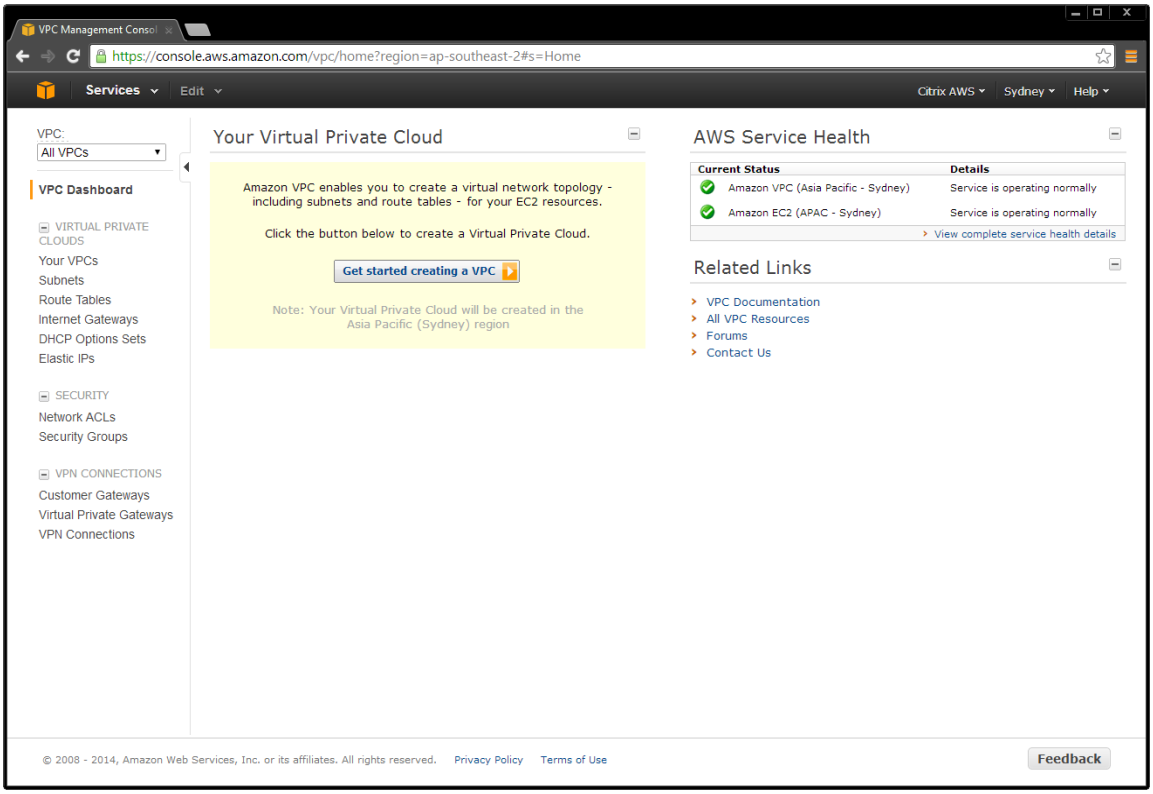
Remarque : l'assistant Amazon VPC crée automatiquement le serveur NAT. Par conséquent, vous n'avez pas besoin de créer l'AMI.

Configurer le réseau VPC

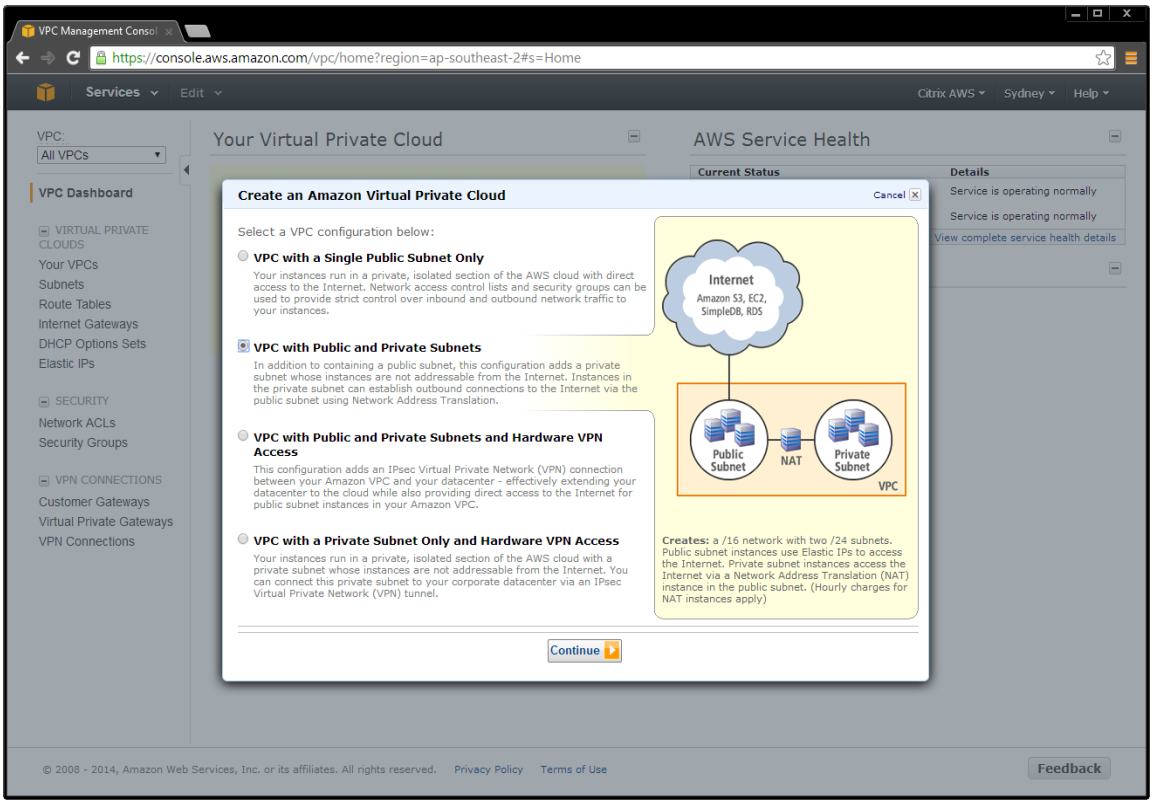
Créer l'infrastructure réseau VPC

La création d'un site implique la création d'une infrastructure réseau VPC (Virtual Private Cloud) dans votre compte Amazon Web Services.

1. Connectez-vous à votre compte AWS et accédez à l'onglet VPC. Cliquez sur **Get Started Creating your VPC** (Création de votre VPC).



2. Sélectionnez **VPC with Public and Private Subnets** (VPC avec sous-réseaux public et privés).



3. Pour créer une configuration hybride dans votre environnement local :
   a. Sélectionnez **VPC with Public and Private Subnets and Hardware VPN** (VPC avec sous-réseaux public et privés et VPN matériel).
   b. Vous pouvez également déployer CloudBridge sur votre boîtier NetScaler, ce qui crée le VPN pour vous.

Cet exemple de déploiement utilise les paramètres réseau par défaut. Ajustez-les en conséquence.

Create an Amazon Virtual Private Cloud Cancel

VPC with Public and Private Subnets

Please review the information below, then click **Create VPC**.

One VPC with an Internet Gateway

IP CIDR block: 10.0.0.0/16 (65,531 available IPs) Edit VPC IP CIDR Block

Two Subnets

Public Subnet: 10.0.0.0/24 (251 available IPs) Edit Public Subnet IP Range

Private Subnet: 10.0.1.0/24 (251 available IPs) Edit Private Subnet IP Range

Additional subnets can be added after the VPC has been created.

One NAT Instance with an Elastic IP Address

Instance Type: m1.small Edit NAT Instance Type

Key Pair Name: Edit Key Pair

Note: Instance rates apply. View rates.

Hardware Tenancy

Tenancy: Default Edit Hardware Tenancy

Back

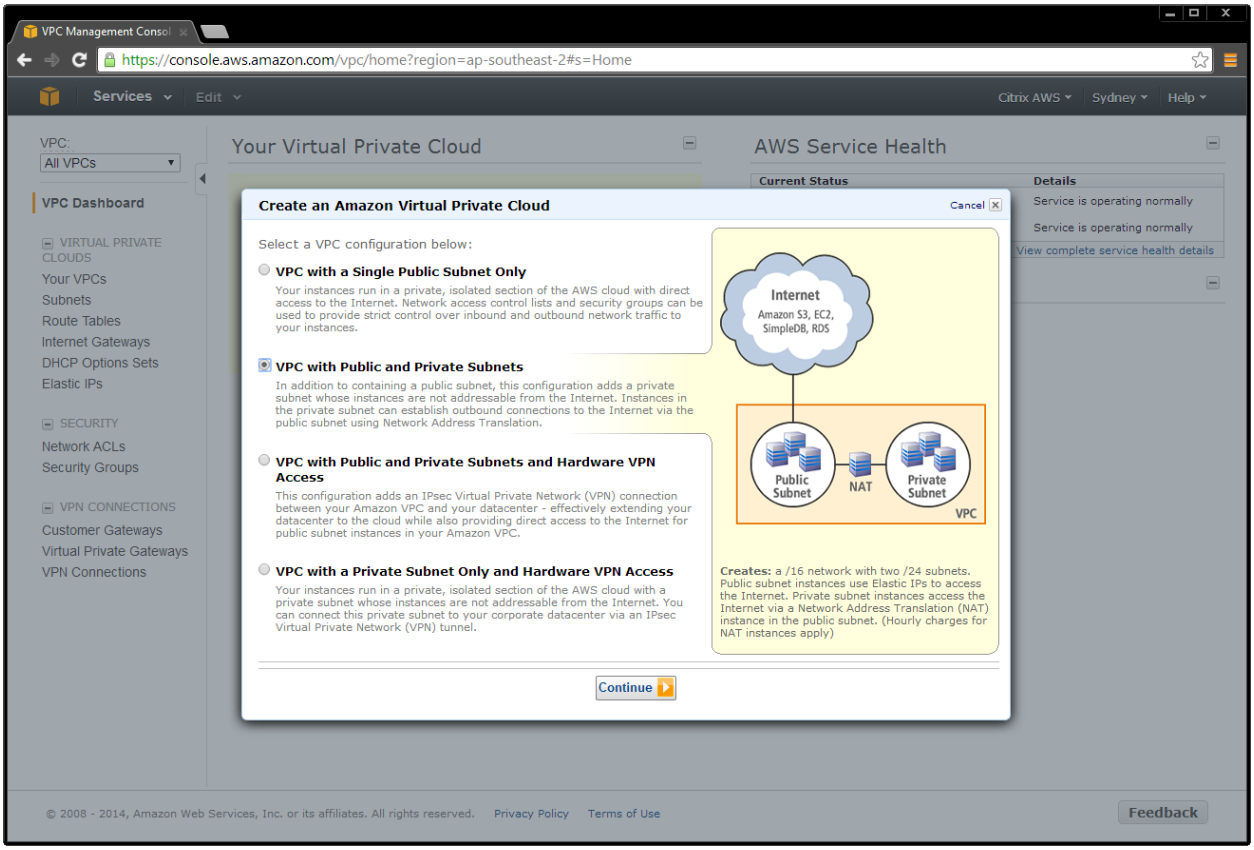
Create VPC

Create an Amazon Virtual Private Cloud Cancel

VPC with Public and Private Subnets

Your VPC has been successfully created.
You can now launch instances into your VPC.

Close



Lorsque le VPC est automatiquement créé, il comprend les sous-réseaux publics et privés, le routeur, la passerelle NAT et la passerelle Internet.

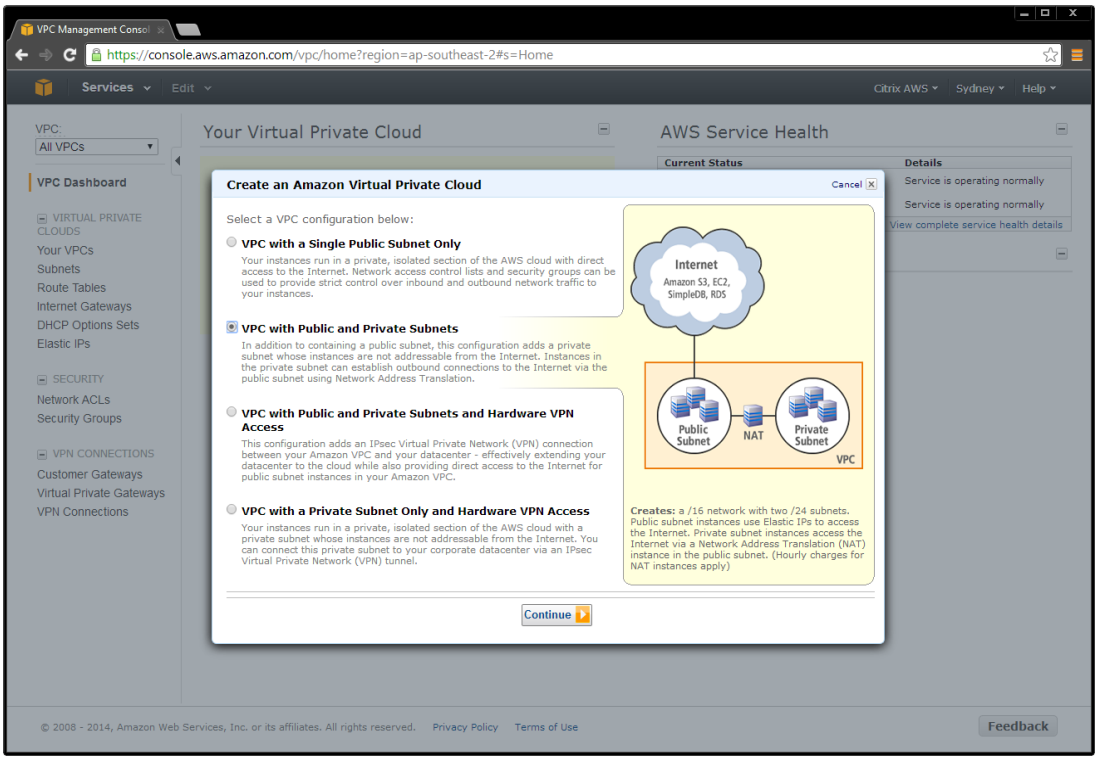
Ajouter des groupes de sécurité

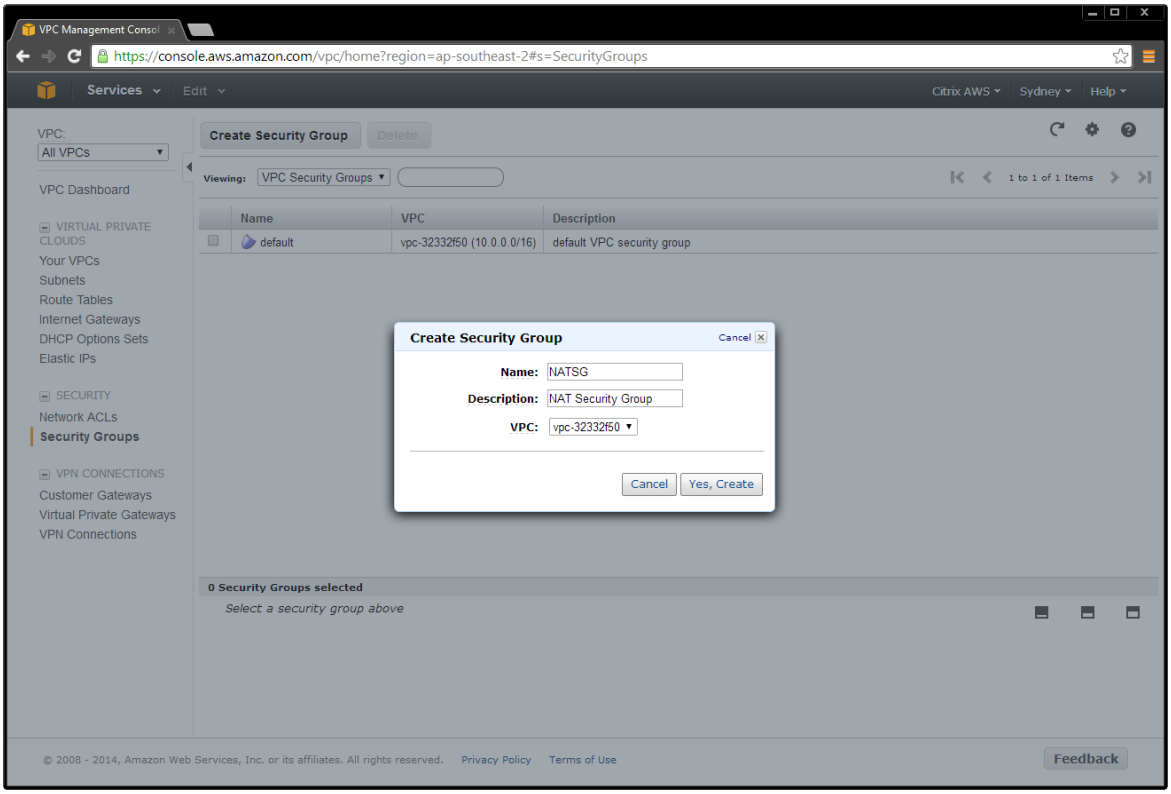
Les groupes de sécurité dans Amazon VPC assurent les communications entre Internet et le réseau public et entre le réseau public et le réseau privé. Les groupes de sécurité contiennent des listes de contrôle d'accès (ACL) et constituent la base des pare-feu affichés dans le réseau de tâches.

Vous devez créer les groupes de sécurité suivants.

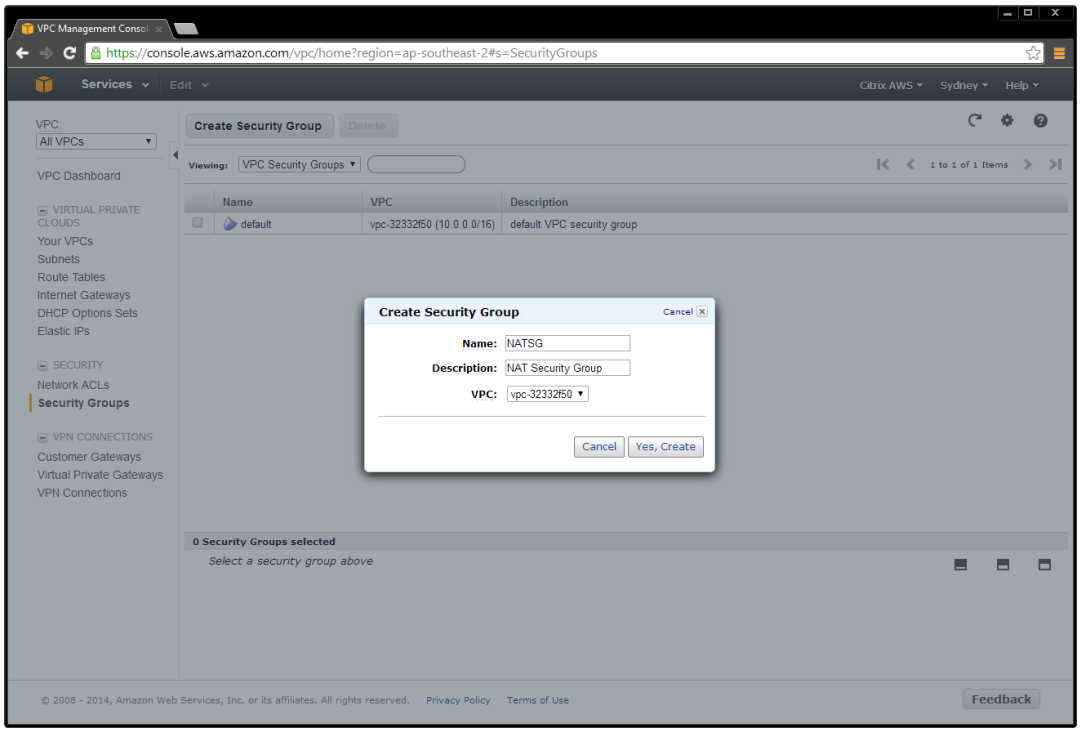
Ajouter un groupe de sécurité NAT

1. Sur l'onglet VPC, sélectionnez **Security Groups > Create Security Group** (Groupes de sécurité > Créer un groupe de sécurité).



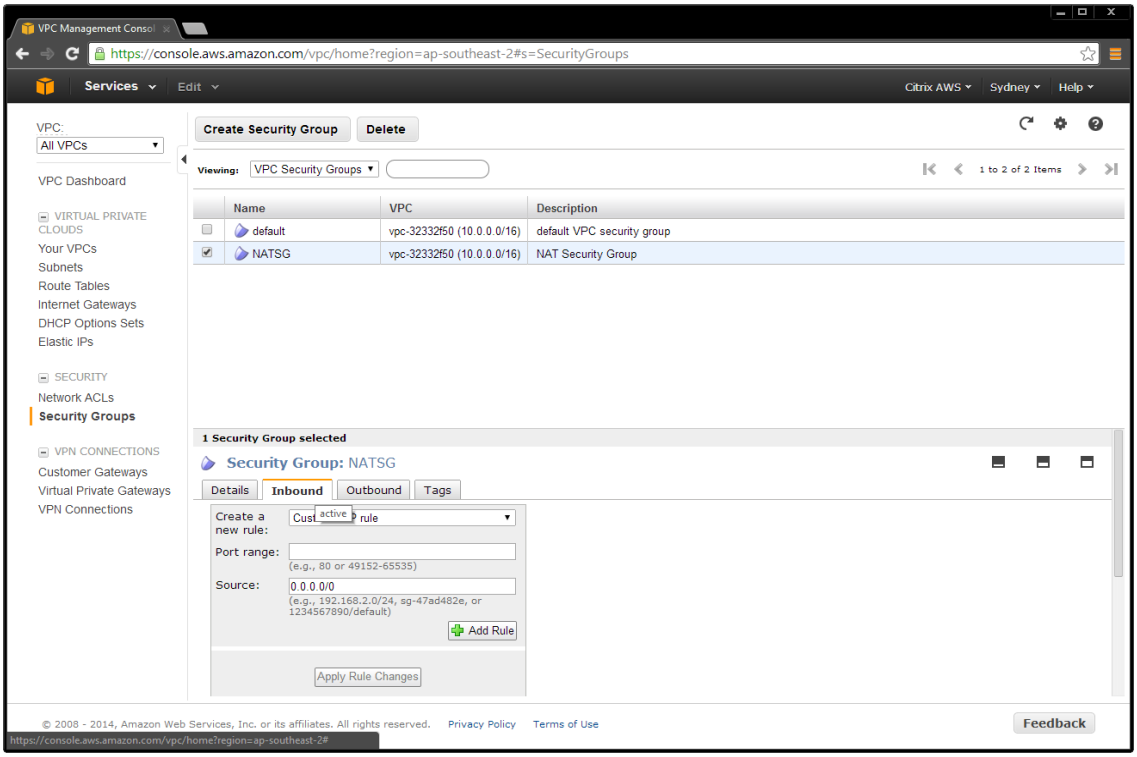


2. Ajoutez des règles de liste de contrôle d'accès pour le trafic entrant et sortant. Sélectionnez :
    a. Create a new rule (permet de créer une nouvelle règle)
    b. Port range (permet de spécifier le numéro de port)
    c. Source (permet de définir l'adresse IP source)



Remarque : une adresse IP source de 0.0.0.0/0 indique que vous voulez autoriser tout le trafic entrant ou sortant.

3. Créez des règles de liste de contrôle d'accès correspondant au tableau du trafic entrant et sortant.



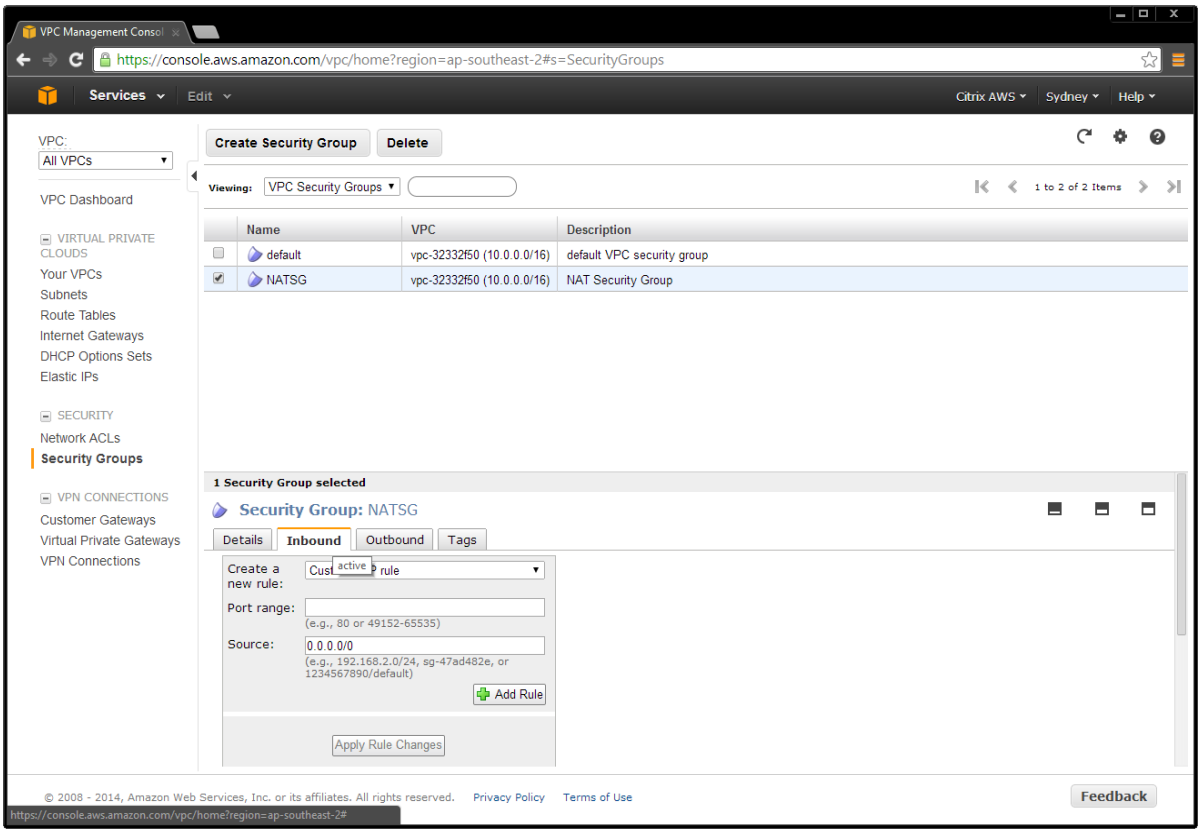
Règles du groupe de sécurité NAT

Entrant				Sortant		
Type	**Trafic**	**Source**		**Type**	**Trafic**	**Source**
Tout	Tout	privateSG		Tout	Tout	0.0.0.0/0
TCP	22 (SSH)	0.0.0.0/0				

Instance NAT

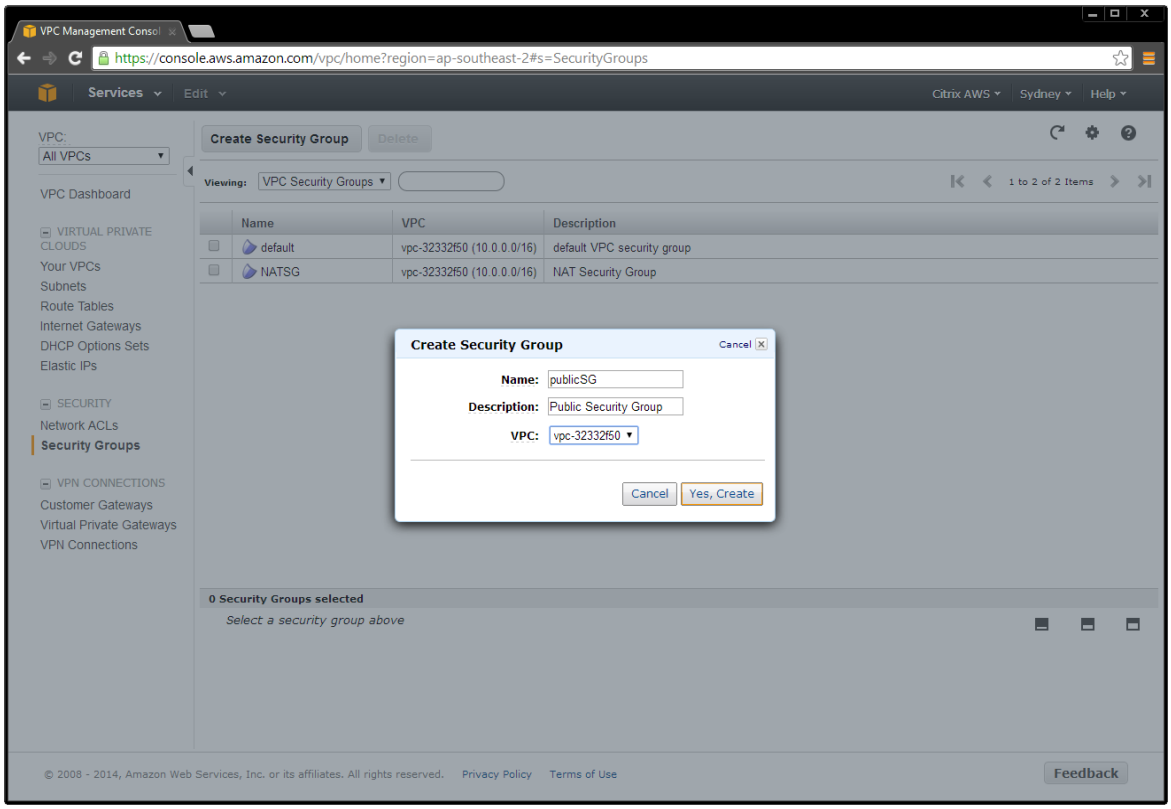
L'assistant VPC crée l'instance NAT.

Accédez à la page et EC2/instances et localisez l'instance. Cliquez avec le bouton droit sur l'instance et modifiez le groupe de sécurité sur **NATSG**.



Ajouter un groupe de sécurité public

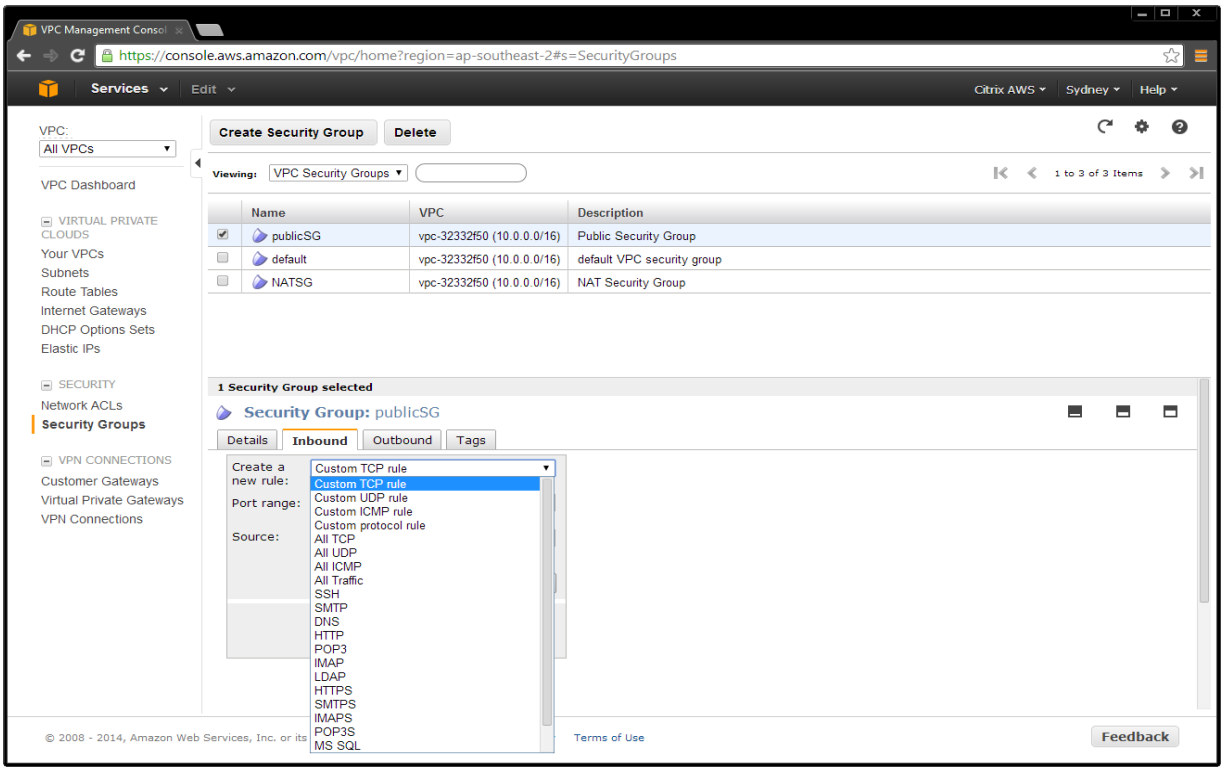
1. Sur l'onglet VPC, sélectionnez **Security Groups > Create Security Group** (Groupes de sécurité > Créer un groupe de sécurité).



2. Ajoutez des règles de liste de contrôle d'accès pour le trafic entrant et sortant. Sélectionnez :
    a. Create a new rule (permet de créer une nouvelle règle)
    b. Port range (permet de spécifier le numéro de port)
    c. Source (permet de définir l'adresse IP source)

Remarque : si vous entrez une adresse IP source de **0.0.0.0/0,** tout le trafic entrant ou sortant est autorisé**.**

3. Créez des règles ACL correspondant au tableau **des règles du groupe de sécurité publicSG.**

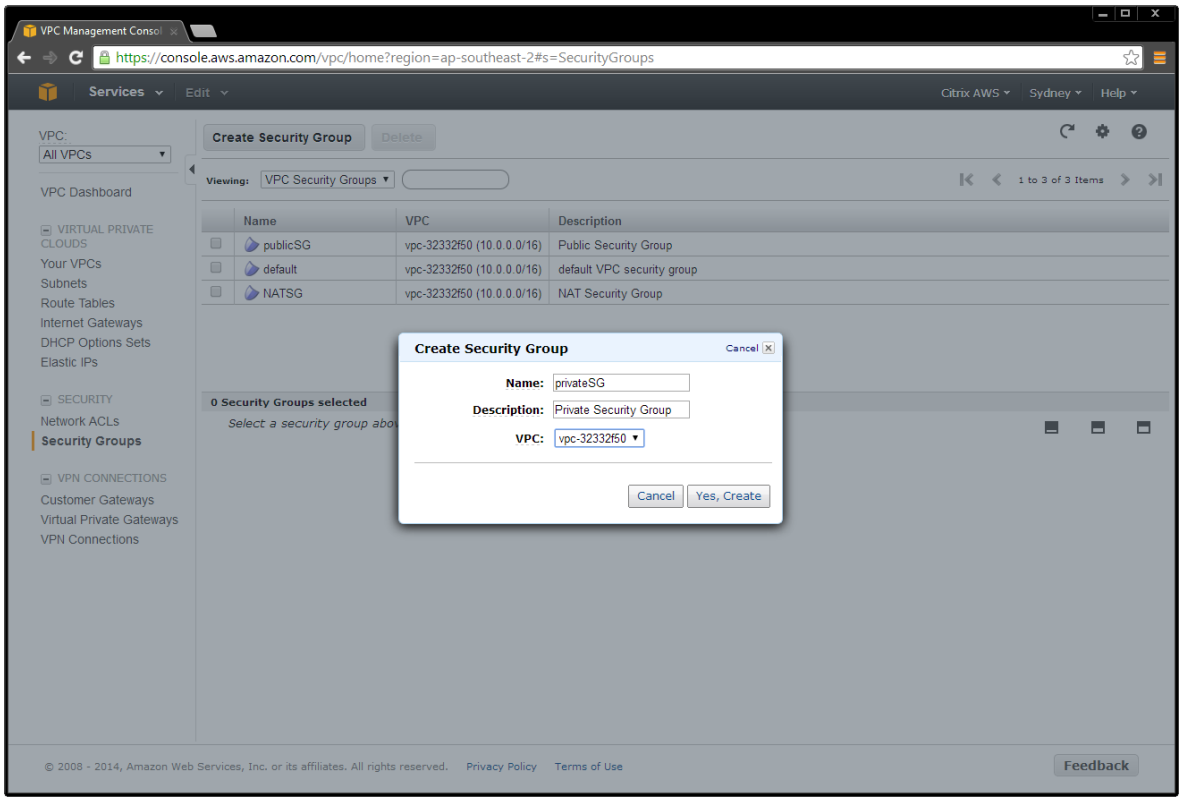


Règles du groupe de sécurité publicSG

Entrant				Sortant		
Type	**Trafic**	**Source**		**Type**	**Trafic**	**Source**
Tout	Tout	publicSG		Tout	Tout	0.0.0.0/0
	Tout	publicSG			Tout	privateSG
ICMP	Tout	0.0.0.0/0		ICMP	Tout	0.0.0.0/0
TCP	22 (SSH)	0.0.0.0/0				
	80 (HTTP)	0.0.0.0/0				
	443 (HTTPS)	0.0.0.0/0				
	1494 (CA)	0.0.0.0/0				
	2598 (Sess)	0.0.0.0/0				
	3389 (RDP)	0.0.0.0/0				

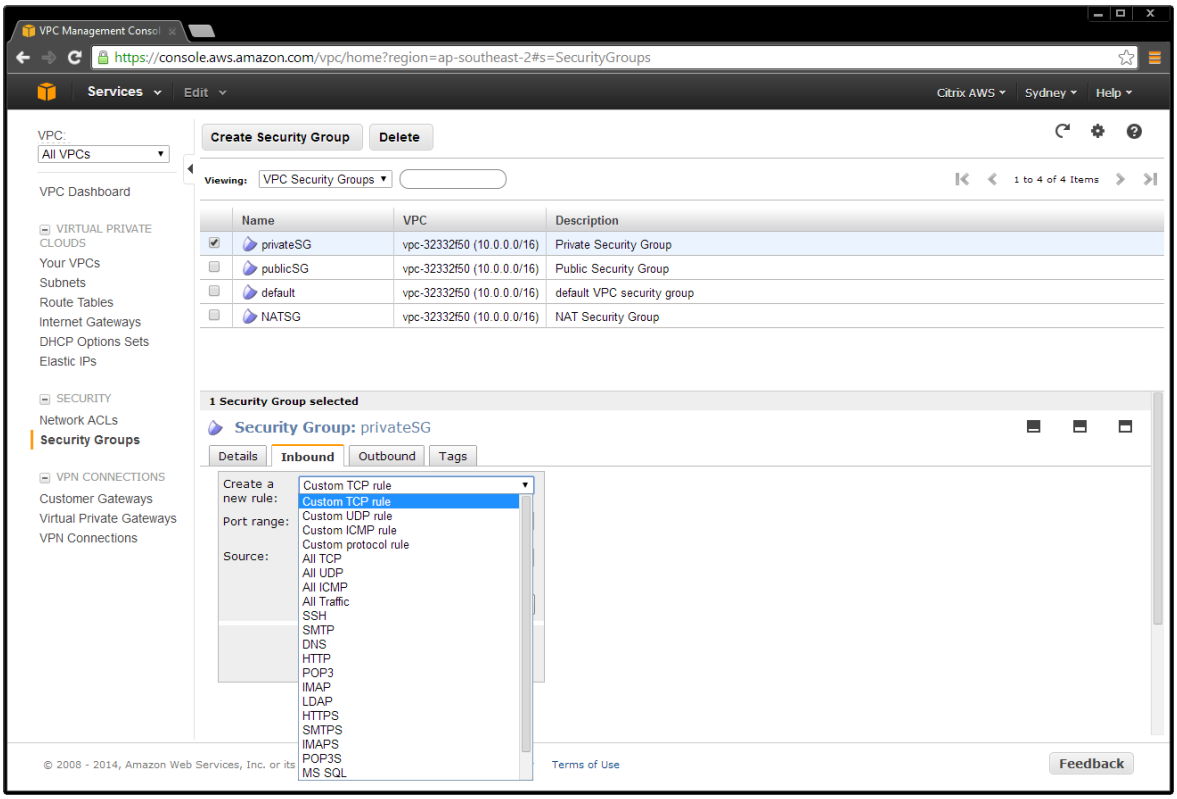
Ajouter un groupe de sécurité privé

1. Sur l'onglet VPC, sélectionnez **Security Groups > Create Security Group** (Groupes de sécurité > Créer un groupe de sécurité).



4. Ajoutez des règles de liste de contrôle d'accès pour le trafic entrant et sortant. Sélectionnez :
    a. Create a new rule (permet de créer une nouvelle règle)
    b. Port range (permet de spécifier le numéro de port)
    c. Source (permet de définir l'adresse IP source)

Remarque : si vous entrez une adresse IP source de 0.0.0.0/0, tout le trafic entrant ou sortant est autorisé. Créez des règles ACL correspondant au tableau.



Règles du groupe de sécurité privateSG

Entrant				Sortant		
Type	**Trafic**	**Source**		**Type**	**Trafic**	**Source**
Tout	Tout	NATSG		Tout	Tout	0.0.0.0/0
	Tout	privateSG			Tout	privateSG
ICMP	Tout	publicSG		ICMP	Tout	0.0.0.0/0
TCP	53 (DNS)	publicSG		UDP]	52 (DNS)	0.0.0.0/0
	80 (HTTP)	publicSG				
	135	publicSG				
	389	publicSG				
	443 (HTTPS)	publicSG				
	1494 (CA)	publicSG				
	2598 (Sess)	publicSG				
	3389 (RDP)	publicSG				
	49152 - 65535	publicSG				
UDP	53 (DNS)	publicSG				
	389 (LDAP)	publicSG				

Options DHCP

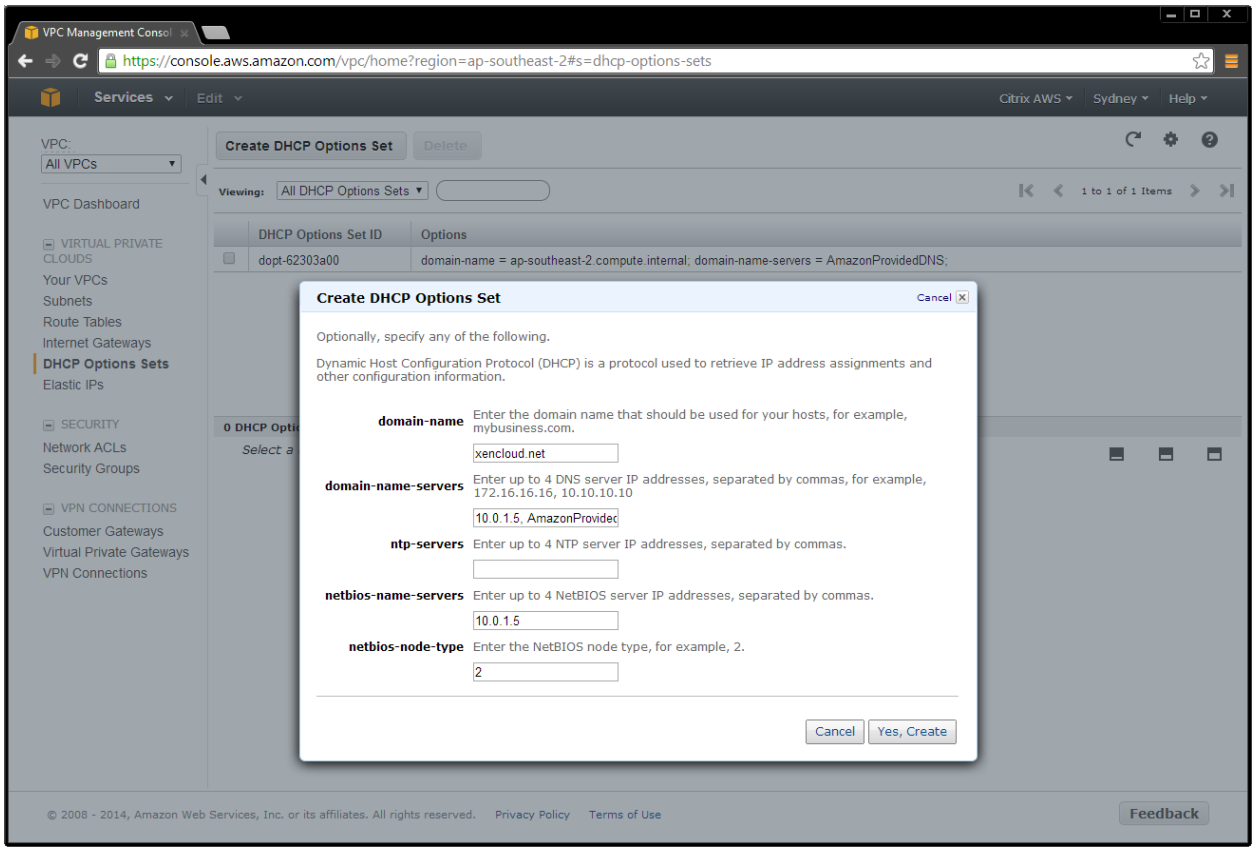
Créer un ensemble d'options DHCP

Un contrôleur de domaine exécute le DNS dans le réseau privé. Le contrôleur permet aux serveurs Citrix de s'authentifier et de communiquer entre eux. Pour implémenter cette communication :

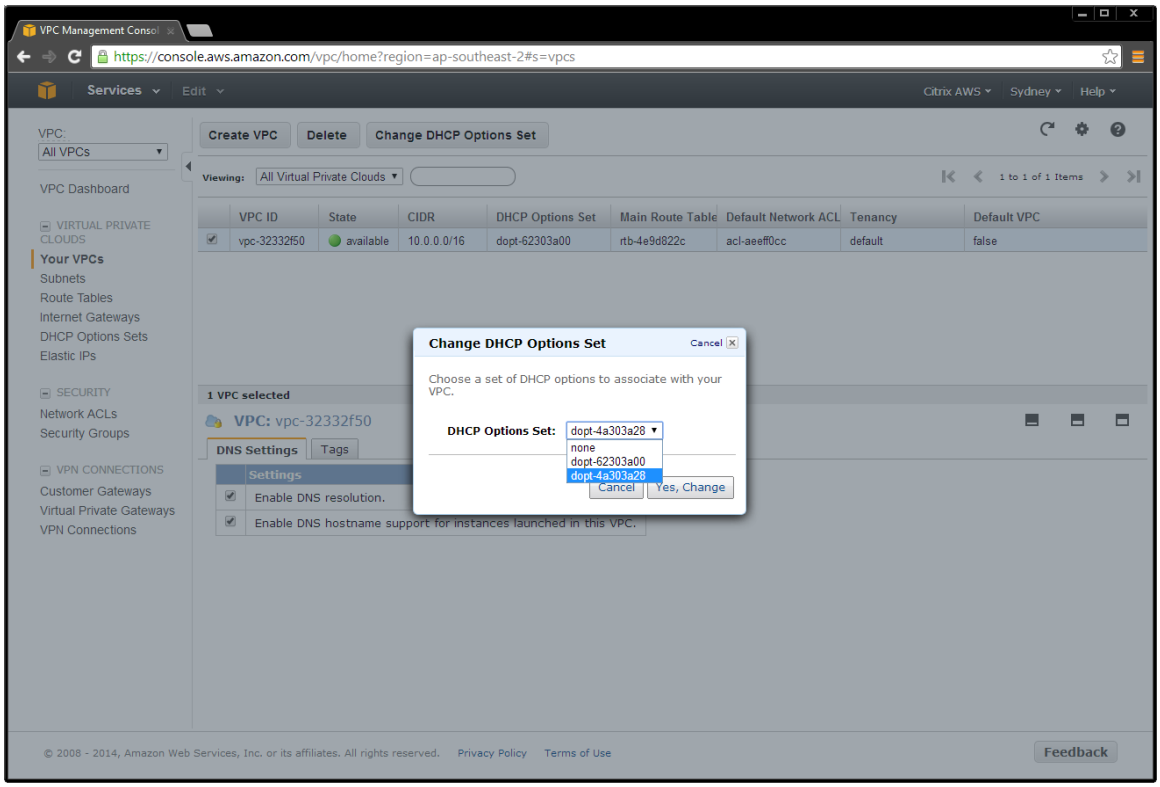
- Créez un nouvel ensemble d'options DHCP contenant l'adresse IP de votre serveur DNS.
- Ajoutez un serveur DNS open-source sur Internet au cas où un serveur ait besoin d'accéder à Internet.

Ensemble d'options DHCP

1. Accédez à l'onglet VPC, puis sélectionnez **DHCP Options Set > Create DHCP Options Set** (Ensemble d'options DHCP > Créer un ensemble d'options DHCP).



2. Sélectionnez le VPC, cliquez avec le bouton droit sur votre sélection, puis choisissez **Change DHCP Options Set to the new set** (Changer l'ensemble d'options DHCP au profit du nouvel ensemble).

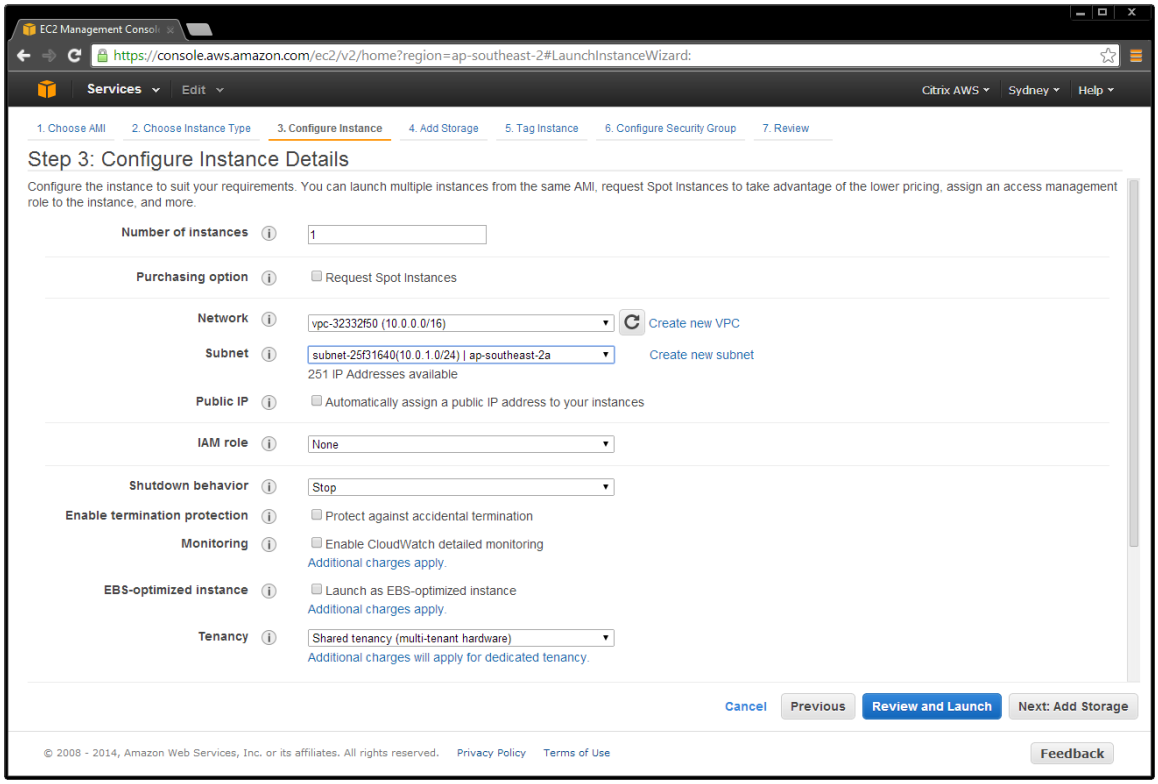


Configurer les instances d'infrastructure XenApp ou XenDesktop

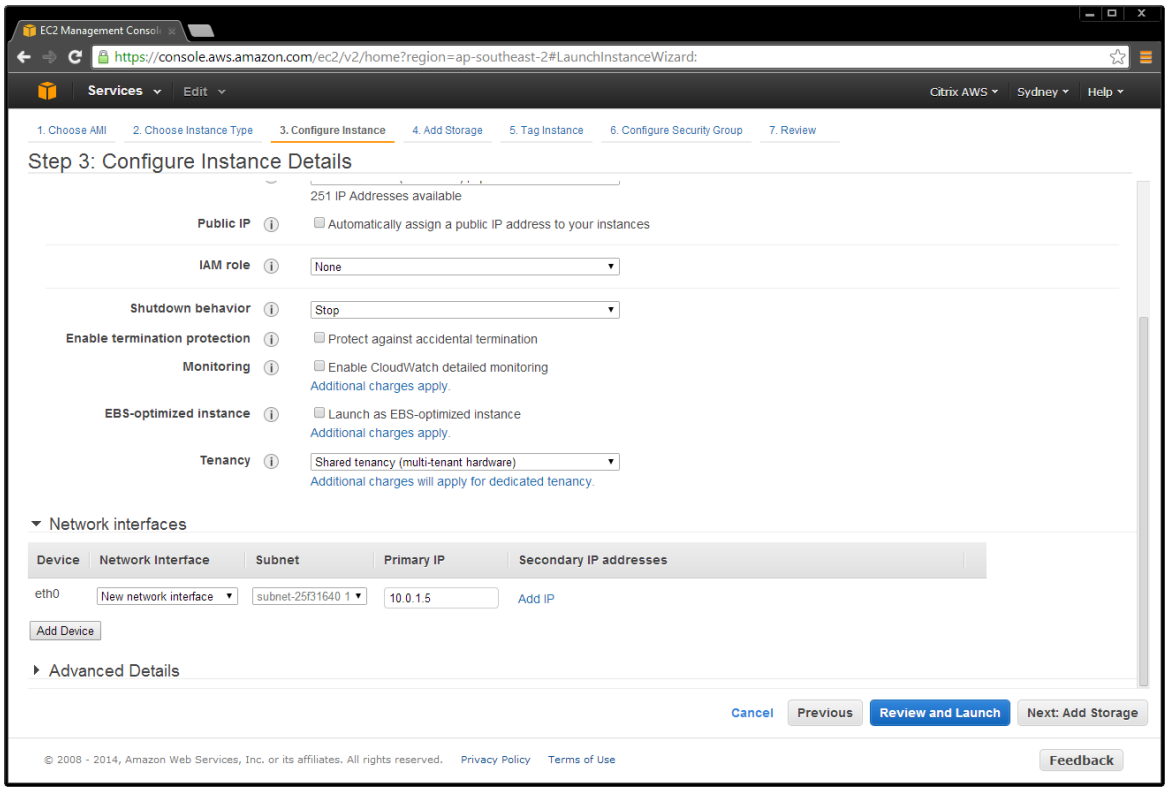
Lancer et configurer une AMI de contrôleur de domaine

Créez un contrôleur de domaine pour le site comme suit.

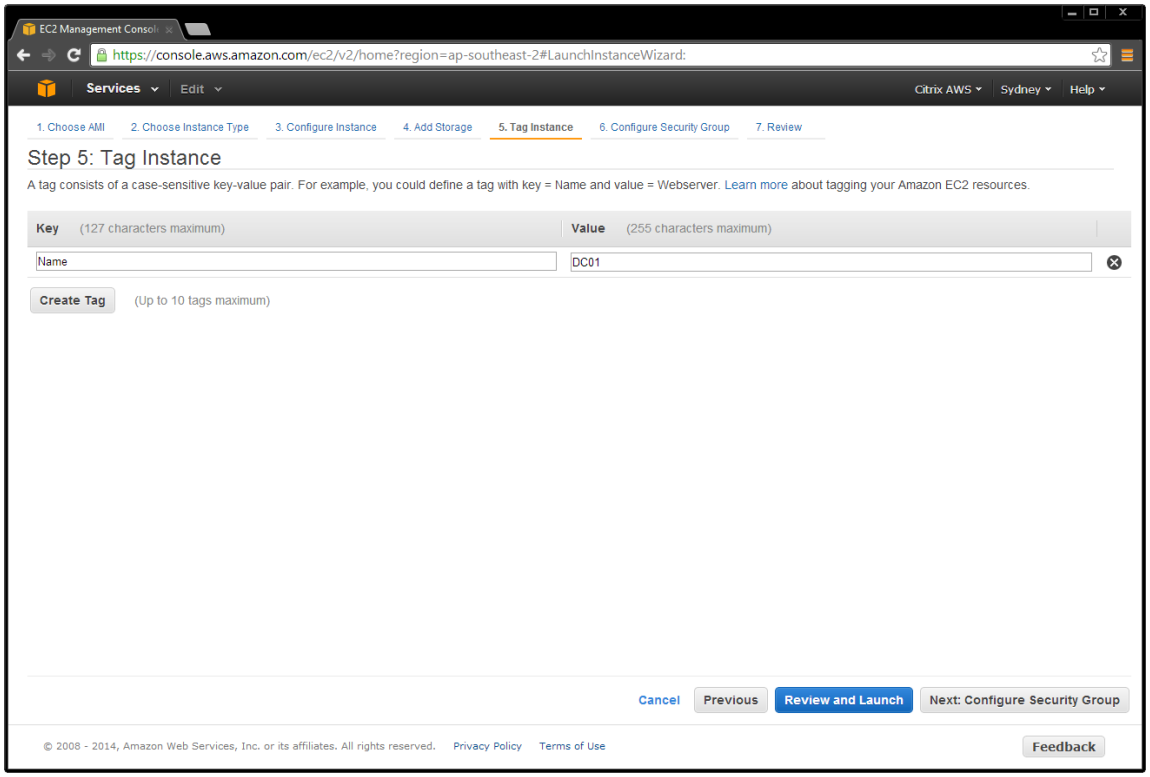
1. Sélectionnez les **AMI** dans l'onglet EC2**.**
2. En fonction du système d'exploitation que vous utilisez, effectuez une recherche dans les AMI Amazon sur **Windows Server 2012 Base** où **Windows Server 2008 R Base**. Assurez-vous que la machine est déployée dans votre sous-réseau et qu'elle figure dans le sous-réseau privé **10.0.1.0/24.**



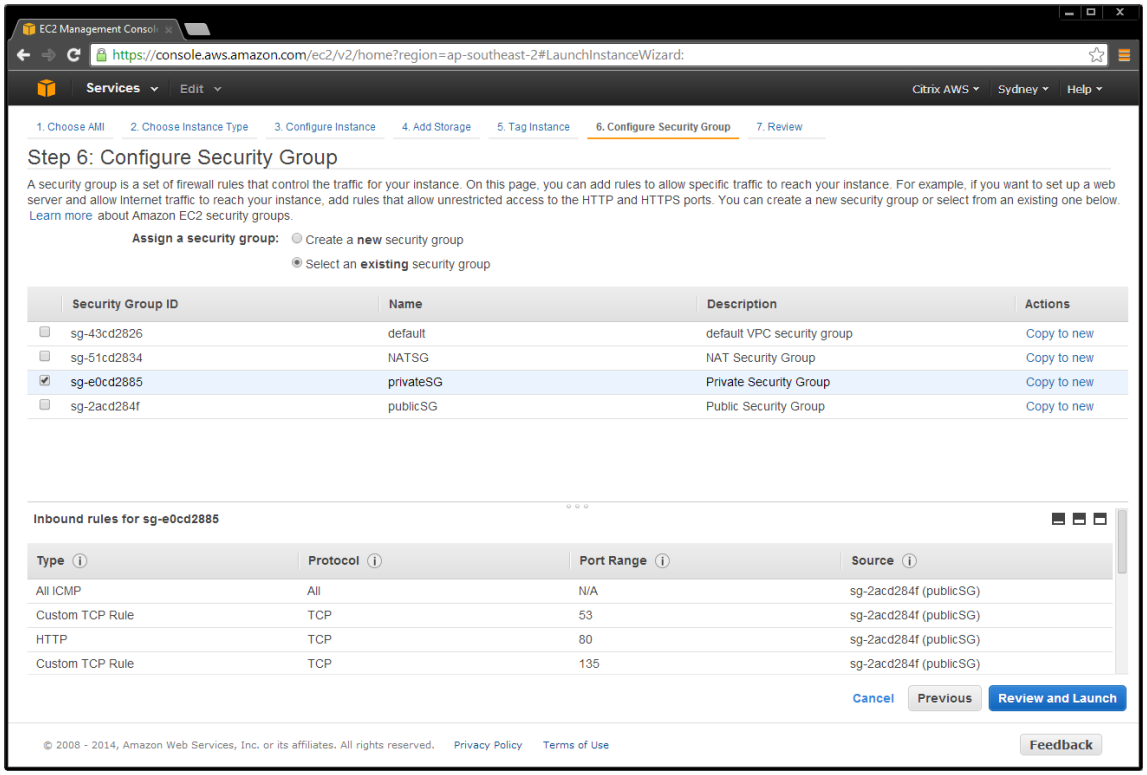
3. Attribuez l'adresse IP pour ce serveur.



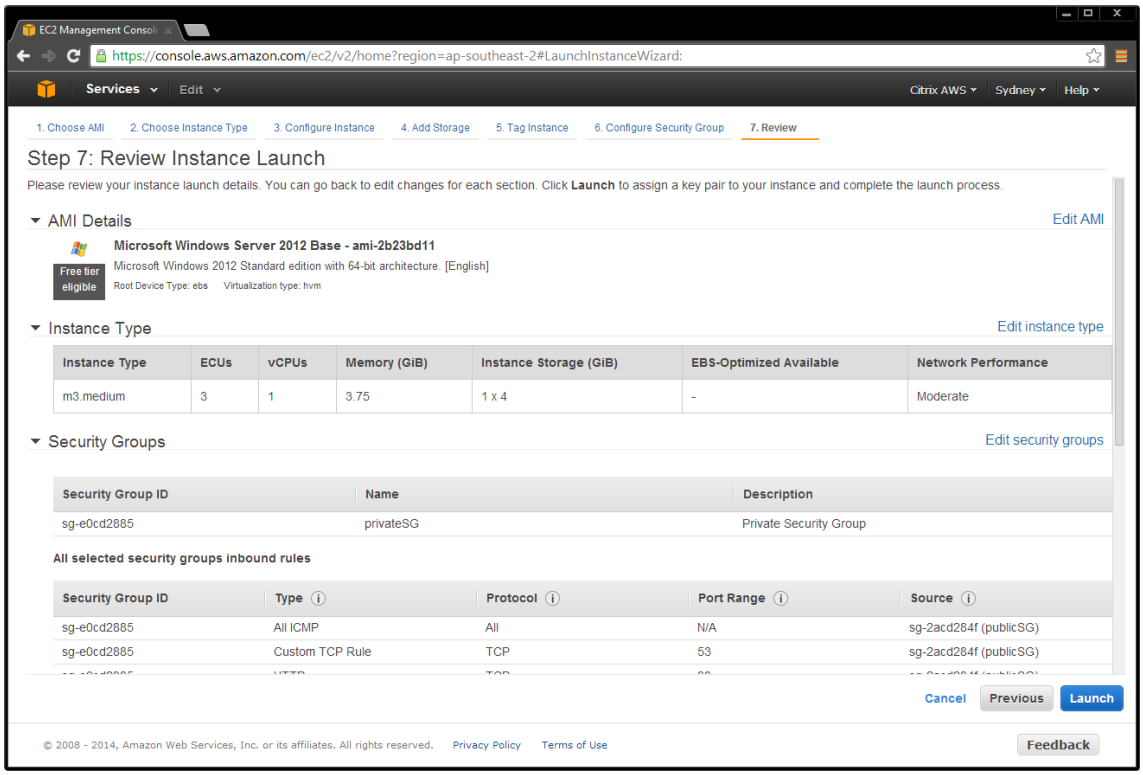
4. Donnez un nom convivial à l'AMI afin qu'elle soit facilement identifiable dans la console Amazon.



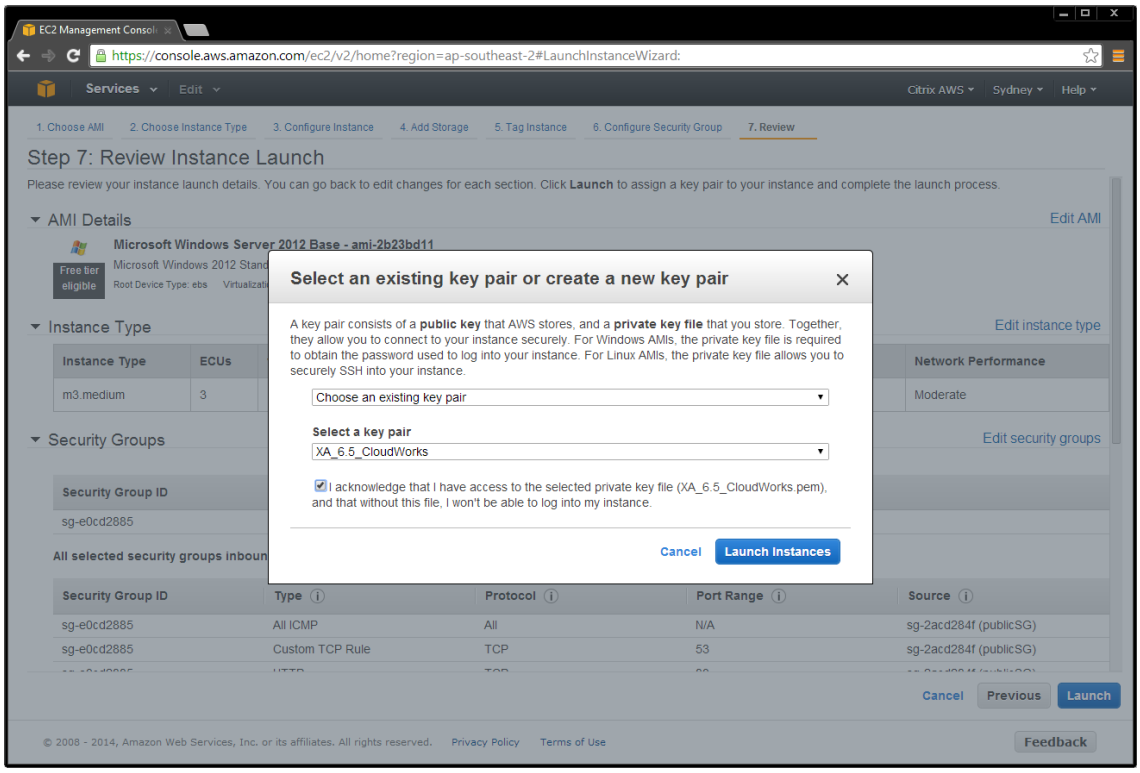
5. Placez le contrôleur de domaine dans le réseau en lançant l'AMI dans le réseau et le groupe de sécurité appropriés. Cet exemple place le contrôleur de domaine dans le réseau privé.



6. Vérifiez les paramètres, puis sélectionnez **Launch** (Lancer).



7. Choisissez une paire de clés AWS existante ou créez-en une nouvelle.



Lancer les AMI XenApp ou XenDesktop restantes

Lancez les AMI XenApp ou XenDesktop restantes à l'aide des paramètres figurant dans le tableau suivant. Veillez à les lancer dans le réseau correct (privé où public le cas échéant), et attribuez une adresse IP et les adresses IP élastiques.

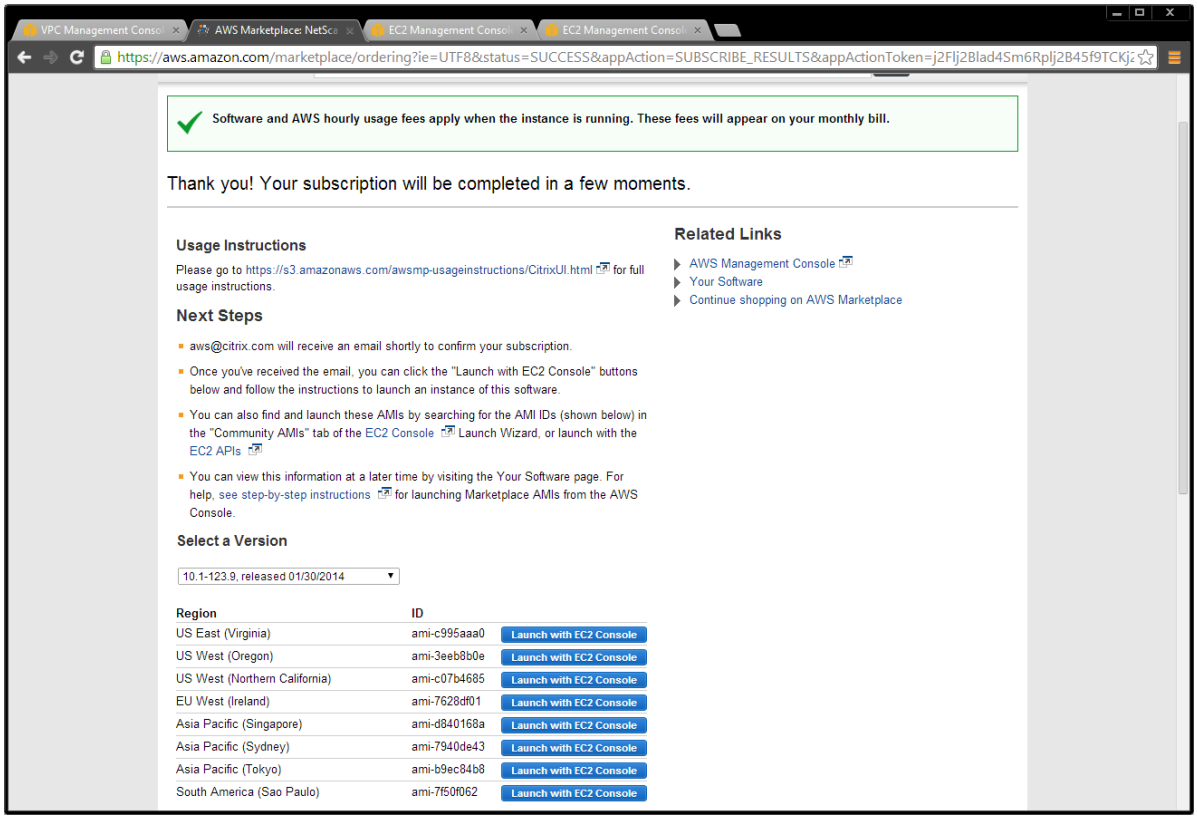
> **Remarque :** l'assistant Amazon VPC crée automatiquement le serveur NAT, vous n'avez donc pas besoin de cette AMI.

Fonction	Nom de l'AMI	ID de l'AMI	Réseau	Adresse IP
Contrôleur de domaine	Microsoft Windows Server 2012 Base	ami-814642e8	privé	10.0.1.5
	Microsoft Windows Server 2008 R2 Base	ami-37b1b45e	privé	10.0.1.5
Delivery Controller	Microsoft Windows Server 2012 avec SQL	ami-e743478e	privé	DHCP
	Microsoft Windows Server 2008 R2 avec SQL	ami-a1b9bcc8	privé	DHCP
VDA principal	Microsoft Windows Server 2012 Base	ami-814642e8	privé	DHCP
	Microsoft Windows Server 2008 R2 Base	ami-37b1b45e	privé	DHCP
Bastion	Microsoft Windows Server 2012 Base	ami-814642e8	public	DHCP
	Microsoft Windows Server 2008 R2 Base	ami-37b1b45e	public	DHCP
NetScaler VPX	NetScaler VPX édition Platinum - 10 Mbits/s	ami-c995aaa0	public/privé	10.0.1.100

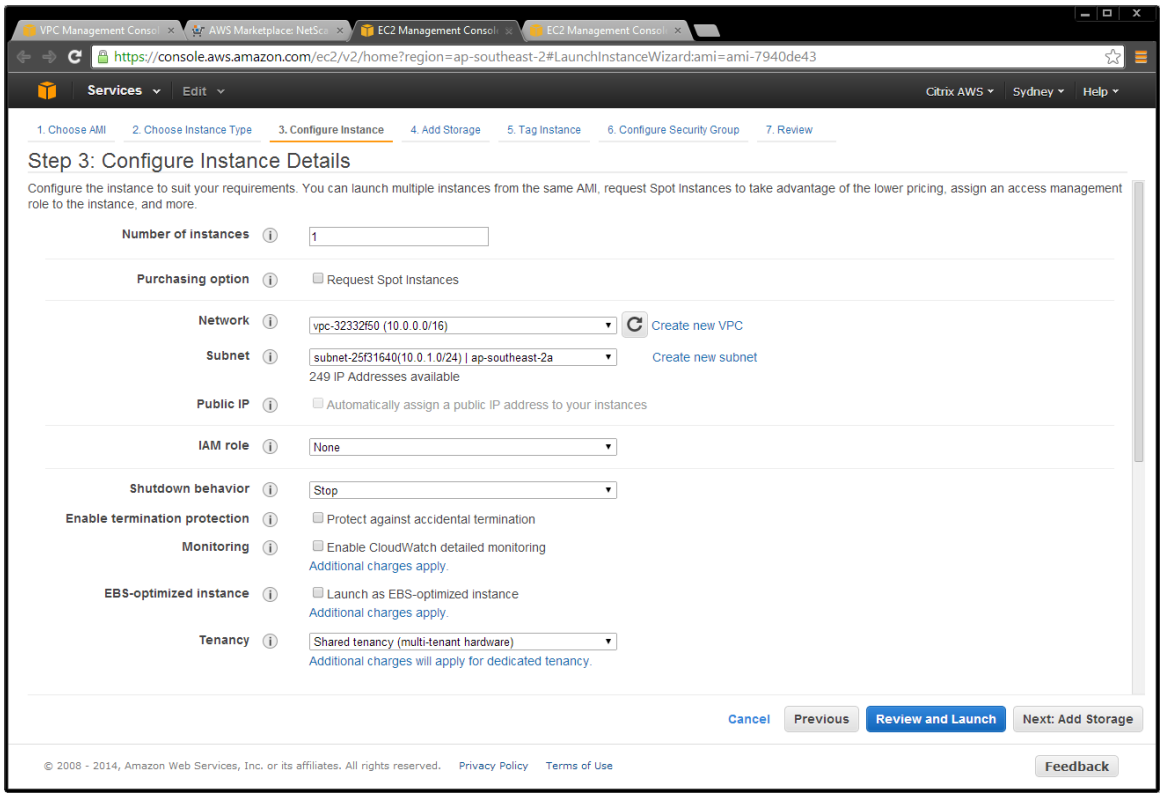
Lancer l'AMI NetScaler

1. Vérifiez que vous êtes abonné à NetScaler VPX dans AWS Marketplace.
2. Dans la section **Community AMIs** de l'assistant de lancement de la console EC2, lancez l'AMI et recherchez les **ID d'AMI**.

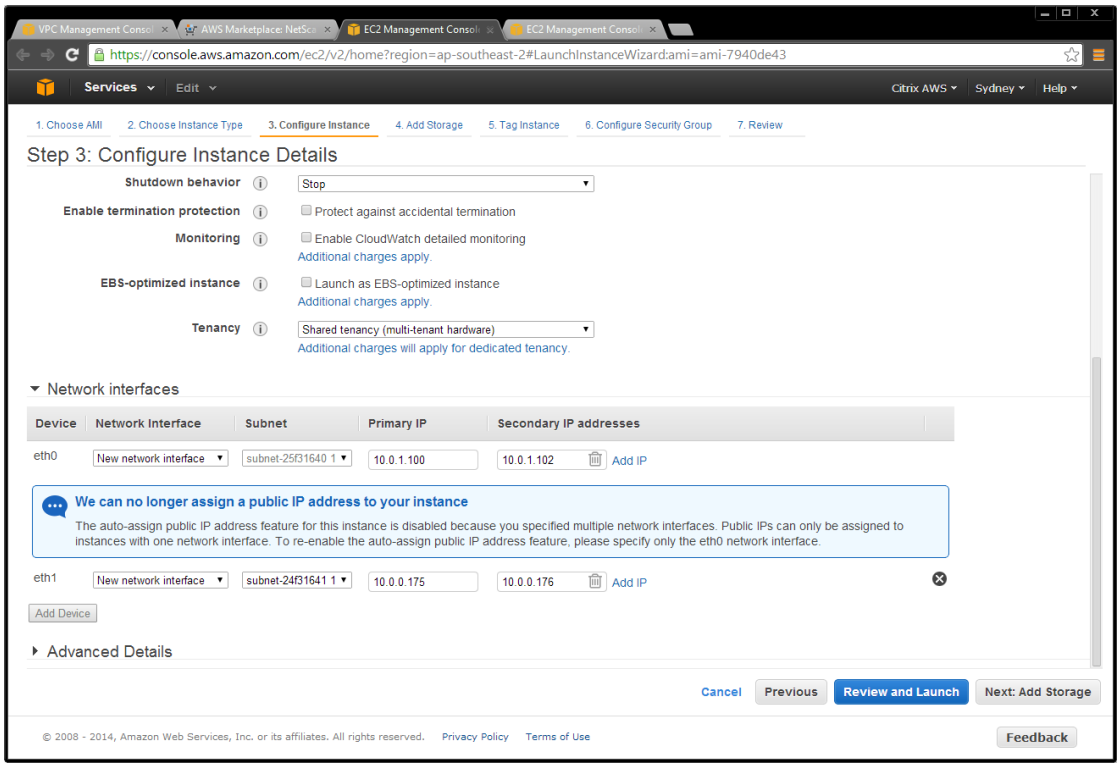
Pour obtenir des instructions détaillées, veuillez consulter https://s3.amazonaws.com/awsmp-usageinstructions/CitrixUI.html.



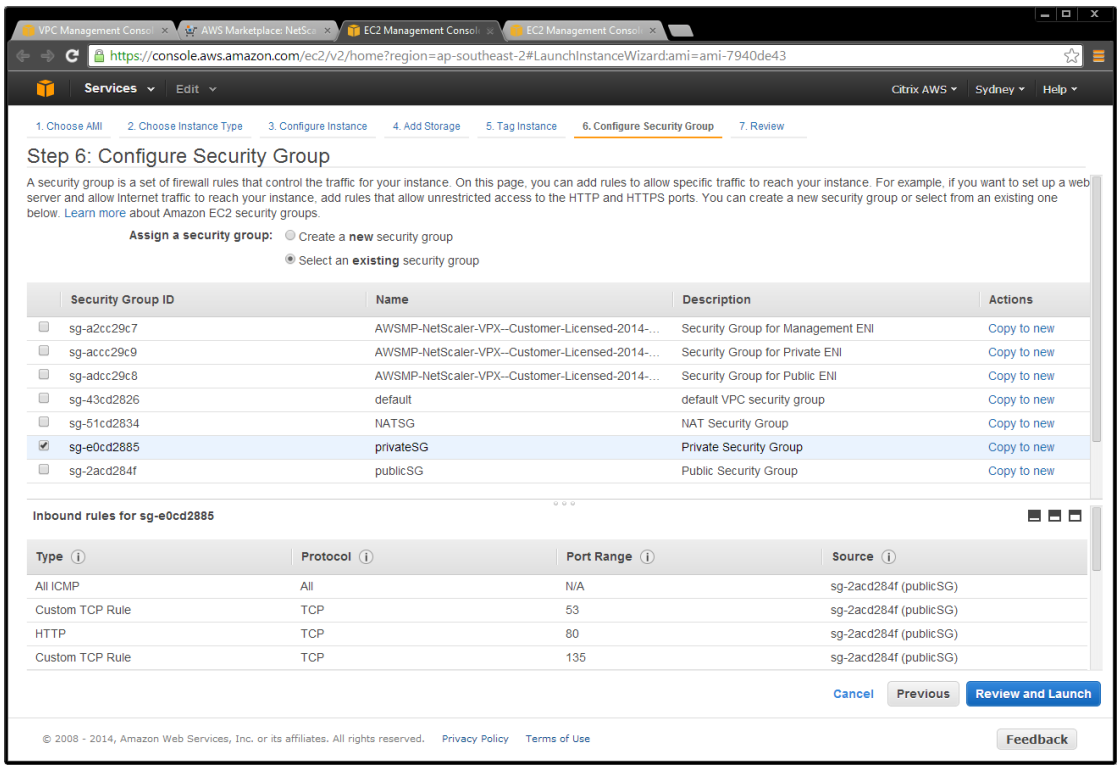
3. Déployez l'instance dans le sous-réseau privé.



4. Assurez-vous que cette instance dispose de deux interfaces :
   - Sous-réseau public
   - Sous-réseau privé :
     i. **eth0** est connecté au sous-réseau privé
     ii. L'adresse IP principale (NSIP) est 10.0.1.100
     iii. L'adresse IP secondaire (SNIP) est 10.0.1.102

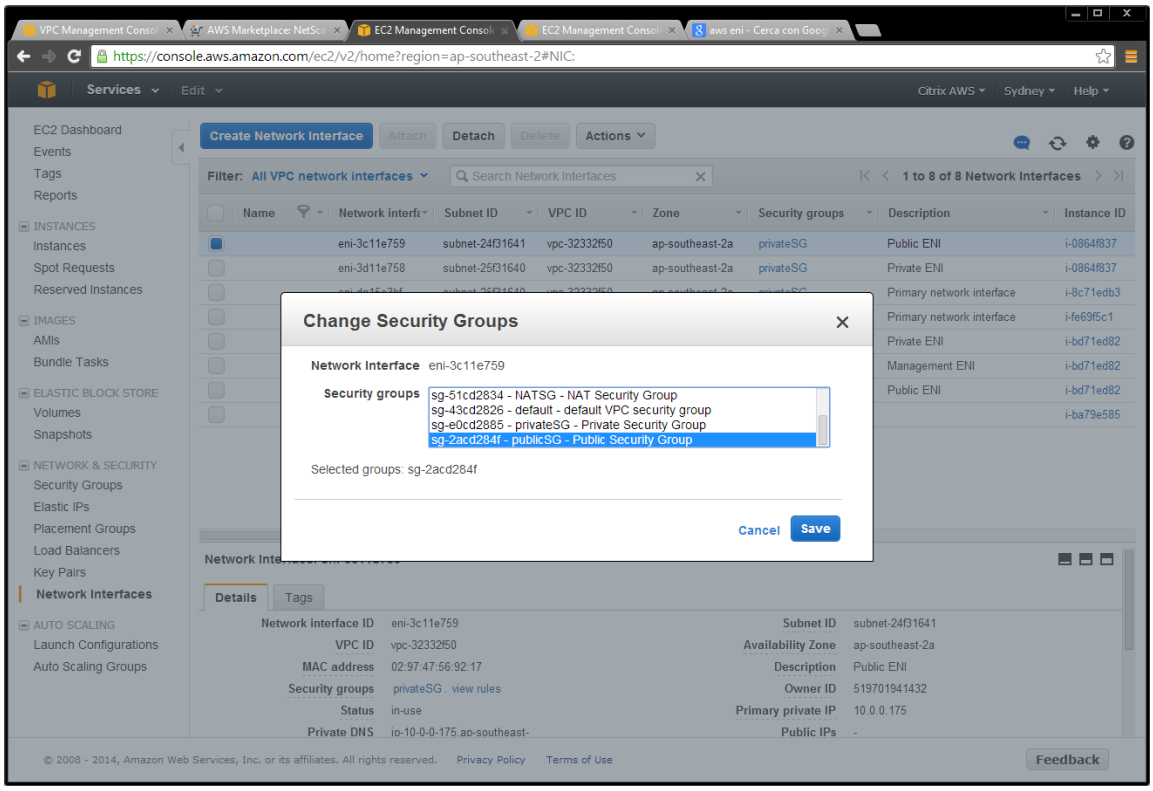


5. Déployez l'instance dans le groupe de sécurité privé.

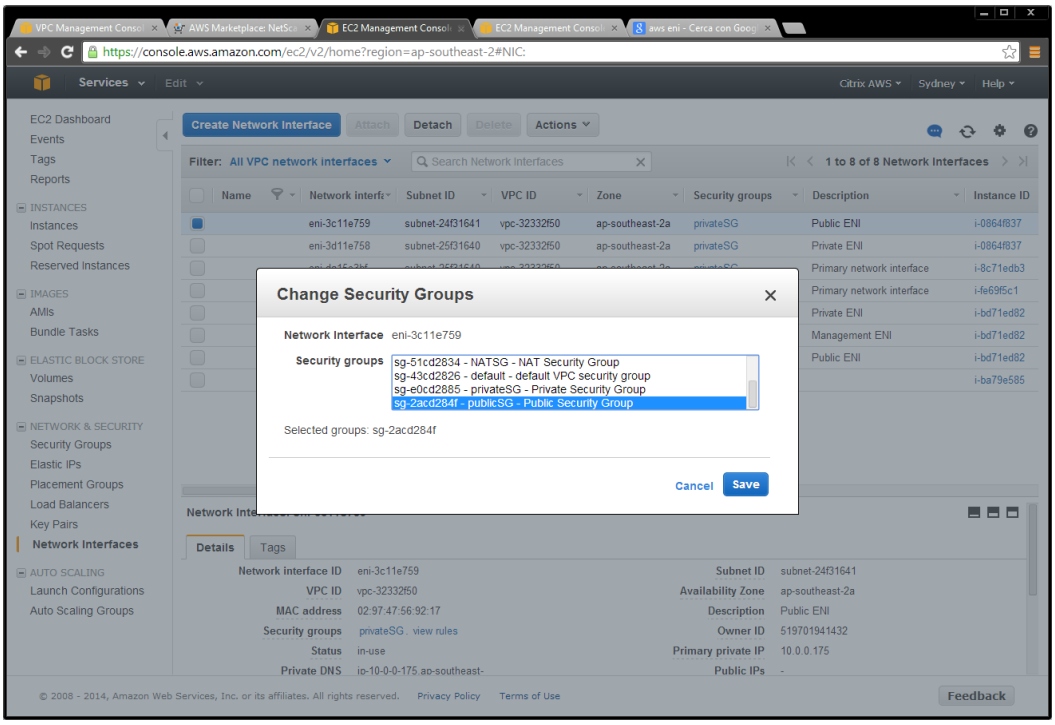


6. Configurez les interfaces réseau élastiques NetScaler (ENI AWS) de manière à ce qu'elles fassent partie de leurs groupes de sécurité respectifs.
    - L'ENI du sous-réseau public doit faire partie du groupe de sécurité public
    - L'ENI du sous-réseau privé doit faire partie du groupe de sécurité privé

ENI publique – Groupe de sécurité public



ENI privée – Groupe de sécurité privé



7. Attribuez une adresse IP élastique à l'ENI publique NetScaler – associée à l'adresse IP virtuelle (10.0.0.176).