

# Deploy XenApp 7.5 and XenDesktop 7.5 with Amazon VPC

Prepared by: Peter Bats

Commissioning Editor: Linda Belliveau

Version: 4.0

Last Updated: April 23, 2014

# Table of Contents

Introduction .....	4
Requirements.....	4
Prerequisites .....	4
Link AWS Marketplace AMIs to your account .....	5
Automated deployment using an AWS CloudFormation template .....	6
XenApp or XenDesktop Infrastructure Stack Creation using the CloudFormation template .....	6
Set up XenApp or XenDesktop on the AWS Infrastructure .....	16
Configure the Master VDA machine .....	22
Set up machines in Studio using the Master VDA AMI .....	31
Set up Delivery Groups .....	36
Set up NetScaler Gateway Remote Access .....	37
Set up StoreFront .....	37
Configure NetScaler Gateway using the Enterprise Store wizard .....	41
Create template AMIs from other templates .....	47
Appendix .....	48
Manually deploy XenApp and XenDesktop in AWS .....	48
Security and firewall mappings.....	49
Set up the VPC network .....	52
Create the VPC network infrastructure .....	52
Add security groups .....	56
Add public security group .....	61
Add Private Security Group.....	63
DHCP options .....	65
Create a DHCP options set .....	65
Set up the XenApp or XenDesktop infrastructure instances .....	68

# Introduction

This document describes setting up Citrix XenApp or XenDesktop with the Amazon Web Services (AWS) Virtual Private Cloud (VPC).

## Requirements

To deploy a XenApp or XenDesktop 7.5 Site in an Amazon VPC, ensure that you complete the prerequisites and link AWS Marketplace AMIs to your account as follows.

## Prerequisites

Make sure you perform the following before you begin:

- Plan to take one day for the first-time implementation of the deployment.
- Have an AWS environment set up and running, with an active AWS account and preferably an AWS Identity and Access Management user account that can be used for this specific deployment.
- For this proof of concept (POC) deployment, the IAM user must have administrative rights to your AWS environment. For information about the rights you need, see the XenApp and XenDesktop topic [Prepare to Install](#).
- Subscribe with your AWS account to the NetScaler VPX AMI located in AWS Marketplace.

## Link AWS Marketplace AMIs to your account

The CloudFormation template uses AWS Marketplace AMIs. Link the AMIs to your account before beginning the install as follows.

1. From the AWS console, select **Find software on AWS Marketplace** under the additional information section on the right side of the console.

### Additional Information

---

[Getting Started Guide](#)

[Documentation](#)

[All EC2 Resources](#)

[Find software on AWS Marketplace](#)

[Forums](#)

[Pricing](#)

### Feedback

---

[Feedback](#)

[Report an Issue](#)

2. Search for **NetScaler VPX Platinum Edition – 10 Mbps**, and select **version 10.1-123.9**.

The screenshot shows the product page for NetScaler VPX Platinum Edition - 10 Mbps. On the left is the Citrix logo. To the right of the logo, the product name is displayed in orange: "NetScaler VPX Platinum Edition - 10 Mbps". Below the name, it says "Sold by: Citrix" and "See product video". A paragraph of descriptive text follows, mentioning features like L4-7 load balancing, application acceleration, and security. Below the description, there are two rows of information: "Customer Rating" with a note "Be the first to review this product" and "Latest Version" with the value "10.1-120.13 (Other available versions)". On the right side of the page, there is a yellow "Continue" button and a small grey box with text: "You will have an opportunity to review your order before launching or being charged."

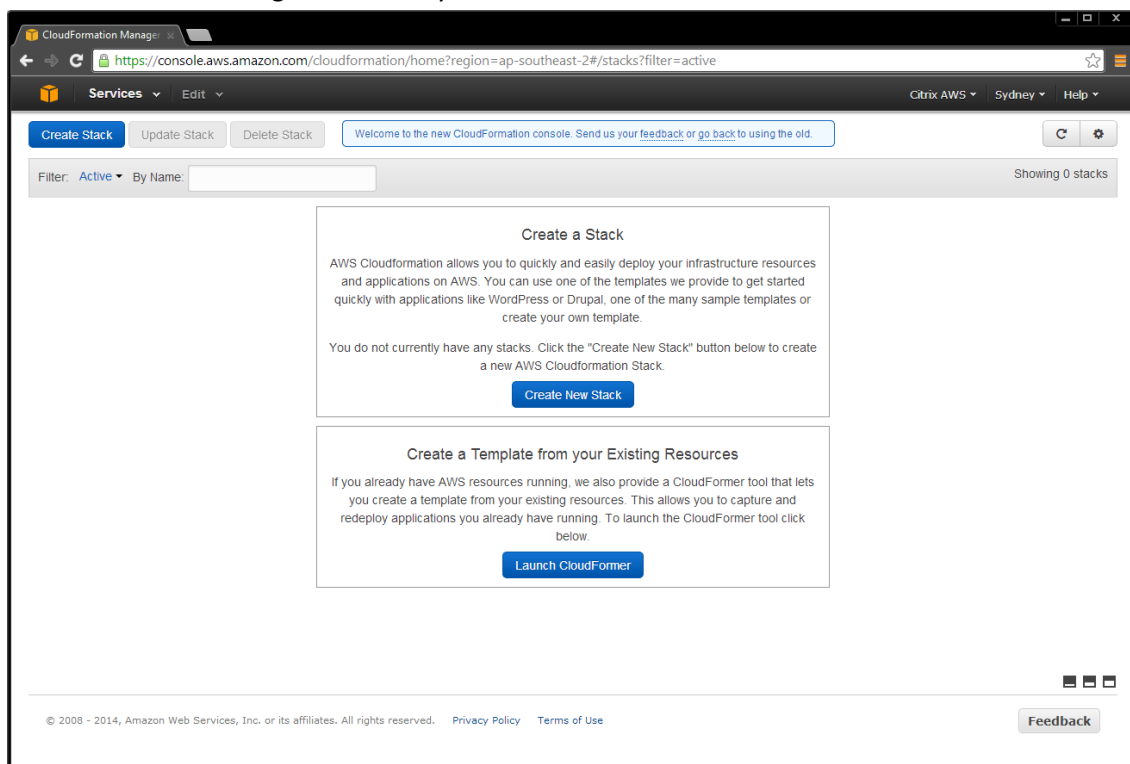
3. Select and register to your AWS account.

# Automated deployment using an AWS CloudFormation template

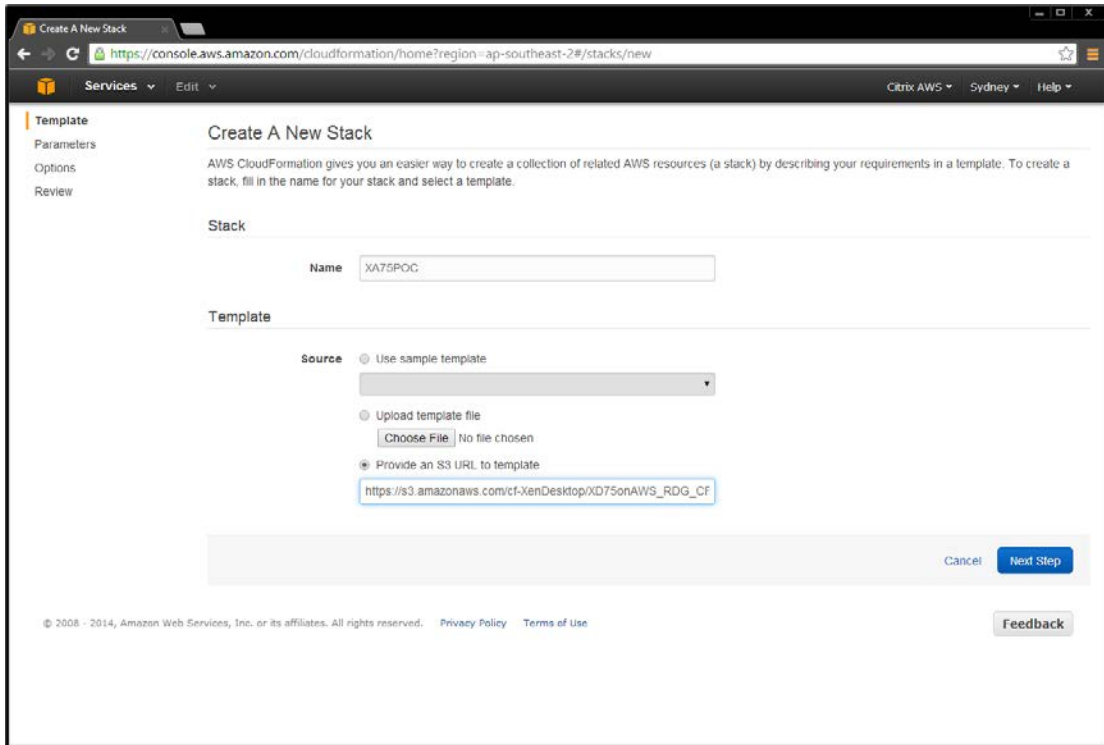
## XenApp or XenDesktop Infrastructure Stack Creation using the CloudFormation template

The following steps show how to use the CloudFormation template to automate building all necessary resources in the Amazon EC2 cloud for a XenApp or XenDesktop Site.

1. On the CloudFormation Stack console tab, use the drop-down box in the upper-right-hand corner to select the region in which you want to build the environment.



2. Click **Create New Stack**.
3. Provide the stack name, and point to the CloudFormation JSON template available at [https://s3.amazonaws.com/cf-XenDesktop/XD75NSonAWS\\_CF\\_v1\\_2.json](https://s3.amazonaws.com/cf-XenDesktop/XD75NSonAWS_CF_v1_2.json), and click **Continue**.



4. Provide parameters for the script to run. The template provides the following information, including brief explanations for each parameter, and displays the following default values.

Default	Default Value	Description
<b>ADInstanceType</b>	m1.medium	Amazon EC2 instance type for the Active Directory Instance
<b>ADPrivateIP</b>	10.0.1.5	Fixed private IP for the Active Directory server
<b>AZ</b>		Name of Availability Zone that will contain public and private subnets. Select a valid zone for your region.
<b>BastionInstanceType</b>	m1.small	Amazon EC2 instance type for the Bastion instance
<b>DMZCDIR</b>	10.0.0.0/24	CIDR Block for the public subnet
<b>DomainAdminPassword</b>	User Provided	Password for the domain admin user. Must be at least eight characters and contain letters, numbers, and symbols.
<b>DomainAdminUser</b>	Xenadmin	User name for the account that will be added as a domain administrator. This is separate from the default administrator account.
<b>DomainDNSName</b>	xencloud.net	Fully qualified domain name (FQDN) to be used for the DHCP scope; for example, xencloud.com
<b>DomainLDIFFormat</b>	DC=xencloud,DC=net	LDIF domain (up to 30 characters) for creating users in the Active Domain Tree
<b>DomainNetBIOSName</b>	XENCLOUD	NetBIOS name of the domain (up to 15 characters) for users of earlier versions of Windows; for example, XENCLOUD
<b>IAMUserAccessKey</b>	User Supplied	IAM user access key used to create and configure the various instances
<b>KeyPairName</b>	User Supplied	Public/private key pairs allow you to securely connect to your instance after it launches
<b>NATInstanceType</b>	m1.small	Amazon EC2 instance type for the NAT instances
<b>NSCloudFormationURL</b>	<a href="https://s3.amazonaws.com/cf-XenApp/NS_VPX_PLT_10MB_Template_v4.4.json">https://s3.amazonaws.com/cf-XenApp/NS_VPX_PLT_10MB_Template_v4.4.json</a>	The public URL for the NetScaler VPX CloudFormation v4.4 template
<b>NSMIP</b>	10.0.1.102	Fixed private MIP or SNIP for the NetScaler NIC connected to the private subnet should be within the CIDR of the private subnet
<b>NSNSIP</b>	10.0.1.100	Fixed private IP for the NetScaler NIC connected to the private subnet should be within the CIDR of the private subnet
<b>NSSNIP</b>	10.0.0.175	Fixed public IP for the NetScaler NIC



		connected to the public subnet, should be within the CIDR of the public subnet
<b>NSVIP</b>	10.0.0.176	Fixed VIP for the NetScaler NIC connected to the public subnet, should be within the CIDR of the public subnet
<b>PrivateCIDR</b>	10.0.1.0/24	CIDR block for private subnet
<b>RestoreModePassword</b>	User Supplied	
<b>SecretAccessKey</b>	User Supplied	IAM user secret access key to be used
<b>ServerNetBIOSName</b>	DC01	NetBIOS name of the AD server (up to 15 characters)
<b>VDAInstanceType</b>	c1.xlarge	Amazon EC2 instance type for the VDA master instance
<b>VdaName</b>	VDAMaster	Primary XenApp server holding the most preferred data collector role for the farm as well as the SQL server
<b>VPCCIDR</b>	10.0.0.0/16	Secondary XenApp server holding the preferred data collector role for the farm
<b>VPCName</b>	XenDesktop 7.5 POC VPC	Server hosting the StoreFront role. Runs version 1.2 of StoreFront with the database on the XENAPP server.
<b>XD7DDCInstanceType</b>	m3.large	Install server used to build the server farm using the App Delivery Setup PowerShell scripts. Can be powered down after the farm is built.
<b>XD7ISOLocation</b>	<a href="https://s3.amazonaws.com/cf-XenDesktop/ISO/XenApp_and_XenDesktop_7_5.iso">https://s3.amazonaws.com/cf-XenDesktop/ISO/XenApp_and_XenDesktop_7_5.iso</a>	Network address translation server, which allows outbound access to the Internet for the servers in the private subnet
<b>XDAdminPassword</b>	User supplied	NetScaler VPX instance that is used to provide ICA proxy functionality for the StoreFront server
<b>XDAdminUser</b>	XDFarmAdmin	

- Different firmware versions of the NetScaler VPX are supported. Select the version you want by choosing the appropriate JSON template from one of the following firmware versions:

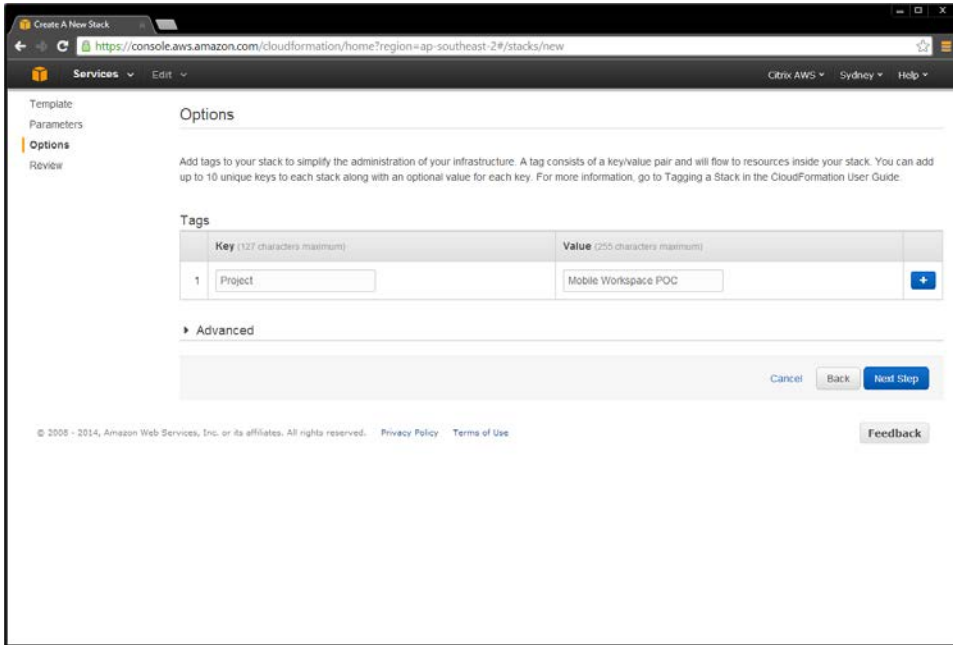
NSCloudFormationURL	Firmware
<a href="https://s3.amazonaws.com/cf-XenApp/NS_VPX_Template_v3.json">https://s3.amazonaws.com/cf-XenApp/NS_VPX_Template_v3.json</a>	10.0-71.6008.e
<a href="https://s3.amazonaws.com/cf-XenApp/NS_VPX_Template_v4.json">https://s3.amazonaws.com/cf-XenApp/NS_VPX_Template_v4.json</a>	10.1-119.7
<a href="https://s3.amazonaws.com/cf-XenApp/NS_VPX_Template_v4.1.json">https://s3.amazonaws.com/cf-XenApp/NS_VPX_Template_v4.1.json</a>	10.1-120.13

The screenshot shows the 'Specify Parameters' page in the AWS CloudFormation console. The page title is 'Specify Parameters' and it includes a navigation sidebar with 'Template', 'Parameters', 'Options', and 'Review'. The main content area contains the following parameters:

- ADInstanceType**: m1.medium (Amazon EC2 instance type for the Active Directory instance)
- ADPrivateIp**: 10.0.1.5 (Fixed private IP for the first Active Directory server)
- AZ**: ap-southeast-2a (Name of Availability Zone that will contain public & private subnets - Select a valid Zone for your region)
- BastionInstanceType**: m1.small (Amazon EC2 instance type for the Bastion instance)
- DMZCIDR**: 10.0.0/24 (CIDR Block for the Public Subnet)
- DomainAdminPassword**: [Redacted] (Password for the domain admin user. Must be at least 8 characters containing letters, numbers and symbols)
- DomainAdminUser**: XenAdmin (User name for the account that will be added as Domain Administrator. This is separate from the default "Administrator" account)
- DomainDNSName**: xencloud.net (Fully qualified domain name (FQDN) to be used for the DHCP scope e.g. xencloud.com)
- DomainLDIFFormat**: DC=xencloud,DC=net (LDIF domain (upto 30 characters) for creating users in the Active Domain Tree)
- DomainNetBIOSName**: xencloud (NetBIOS name of the domain (upto 15 characters) for users of earlier versions of Windows e.g. CTXCLDUD)

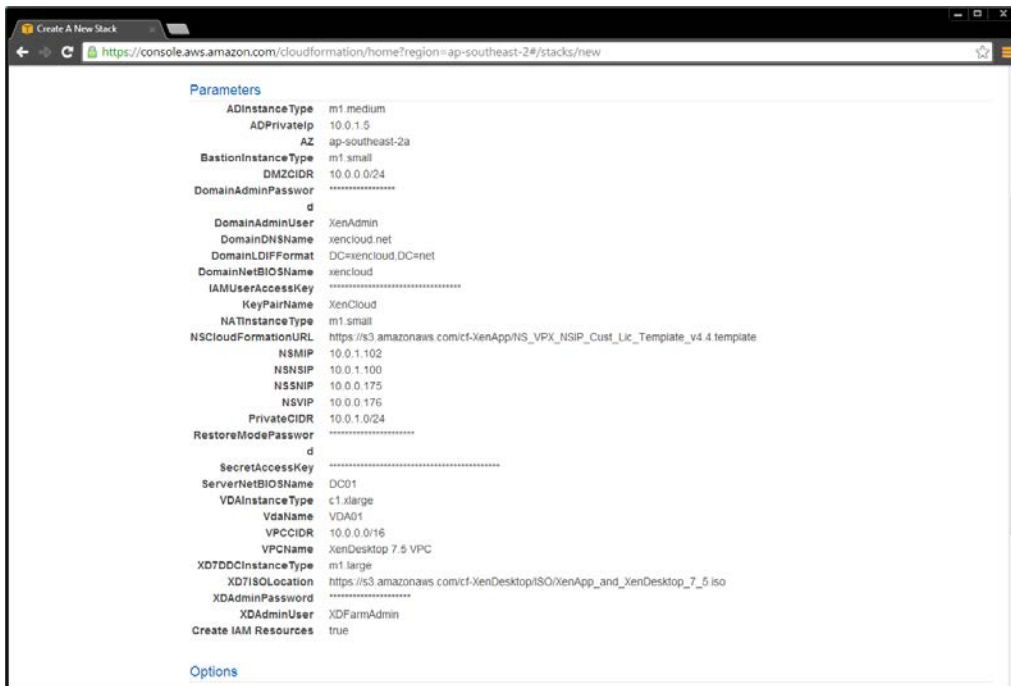
- After specifying the required parameters, select **I acknowledge that this template may create IAM resources** check box, and click **Continue**.

7. Add any additional tags on the next screen, and click **Continue**.



Verify that the values provided match your environment.

**Note:** It is important to ensure that the availability zone, your access credentials and keypair are correct. If not, go back and correct the error; otherwise, the template creation will fail. Once correct, click **Continue** to start the stack build process.



8. Click **Create** on the stack creation information screen.

Create A New Stack

https://console.aws.amazon.com/cloudformation/home?region=us-west-2#/stacks/new

**DomainNetBIOSName** xencloud  
**IAMUserAccessKey** AKIAJQ5QV6E4JDAO7CMA  
**KeyPairName** XenCloud  
**NAInstanceType** m1.small  
**NSCloudFormationURL** https://s3.amazonaws.com/cf-XenApp/NS\_VPX\_PLT\_10MB\_Template\_v4.4.json  
**NSMIP** 10.0.1.102  
**NSNSIP** 10.0.1.100  
**NSSNIP** 10.0.0.175  
**NSVIP** 10.0.0.176  
**PrivateCIDR** 10.0.1.0/24  
**RestoreModePassword** .....  
**SecretAccessKey** NKBJ5XgZvXgeFHka0VEjIMgtWtwXmes7T5xtuaj  
**VDAInstanceType** c1.xlarge  
**VPCCIDR** 10.0.0.0/16  
**VPCName** XenDesktop 7.5 POC VPC  
**XD7ISOLocation** https://s3.amazonaws.com/cf-XenDesktopISO/XenApp\_and\_XenDesktop\_7\_5\_iso  
**Create IAM Resources** true

**Options**

**Tags**

**Project** Mobile Workspace POC

**Advanced**

**Notification**  
**Timeout** none  
**Rollback on failure** Yes

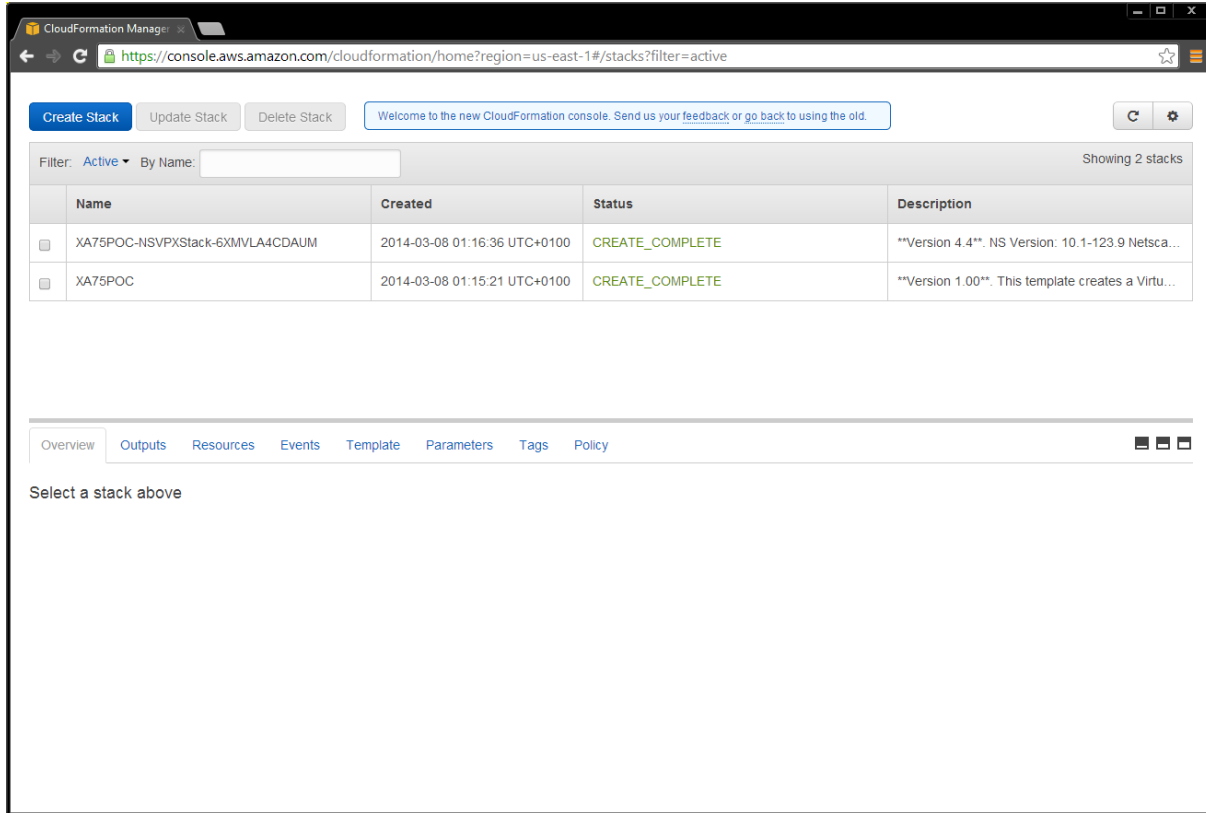
Cancel Back Create

© 2008 - 2014, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Feedback

The CloudFormation template builds the environment according to the parameters you specified; the template will appear in the CloudFormation Console when completed.

It displays two CloudFormation stacks: one for the EC2 Infrastructure and one for the NetScaler VPX.



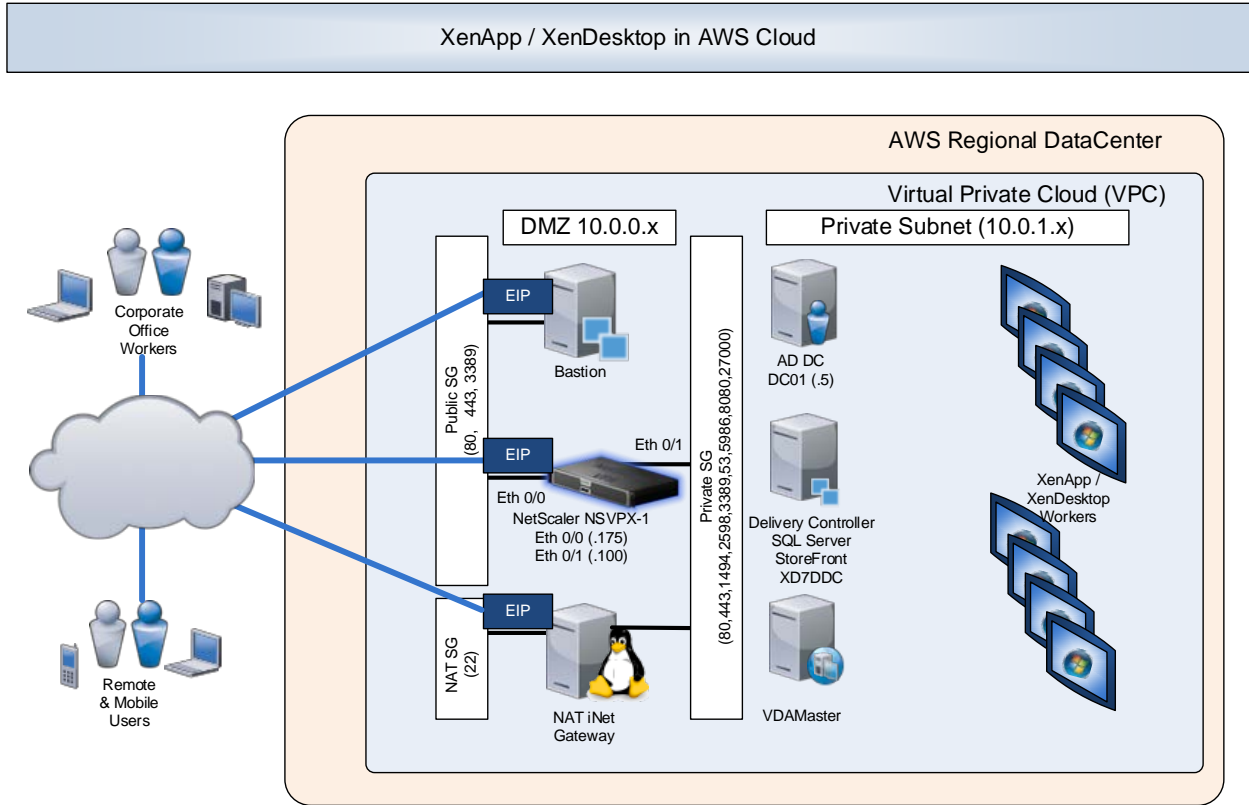
9. When you select the Outputs section of the Infrastructure Stack, the IP addresses of the main components appear.

The screenshot shows the AWS CloudFormation console interface. At the top, there are buttons for 'Create Stack', 'Update Stack', and 'Delete Stack'. Below these is a filter section with 'Active' selected and a search box. A table lists two stacks, with the 'XA75POC' stack selected. Below the stack list, there are tabs for 'Overview', 'Outputs', 'Resources', 'Events', 'Template', 'Parameters', 'Tags', and 'Policy'. The 'Outputs' tab is active, displaying a table of stack outputs.

Key	Value	Description
DomainController	10.0.1.5	IP address of the domain controller.
DesktopDeliveryController	10.0.1.79	IP address of the XenDesktop 7 Desktop Delivery Controller
BastionElasticIP	54.84.197.200	External IP address of the Bastion host in AZ1. RDP to this IP...
NetScaler	10.0.1.100	IP address (NSIP) of the NetScaler. Browse to this IP address...
NSGWVIP	54.84.152.62	Elastic IP address of the Client VIP of the NetScaler.

If you select the default values, the template constructs a XenApp or XenDesktop Site infrastructure in the AWS cloud similar to the following example:

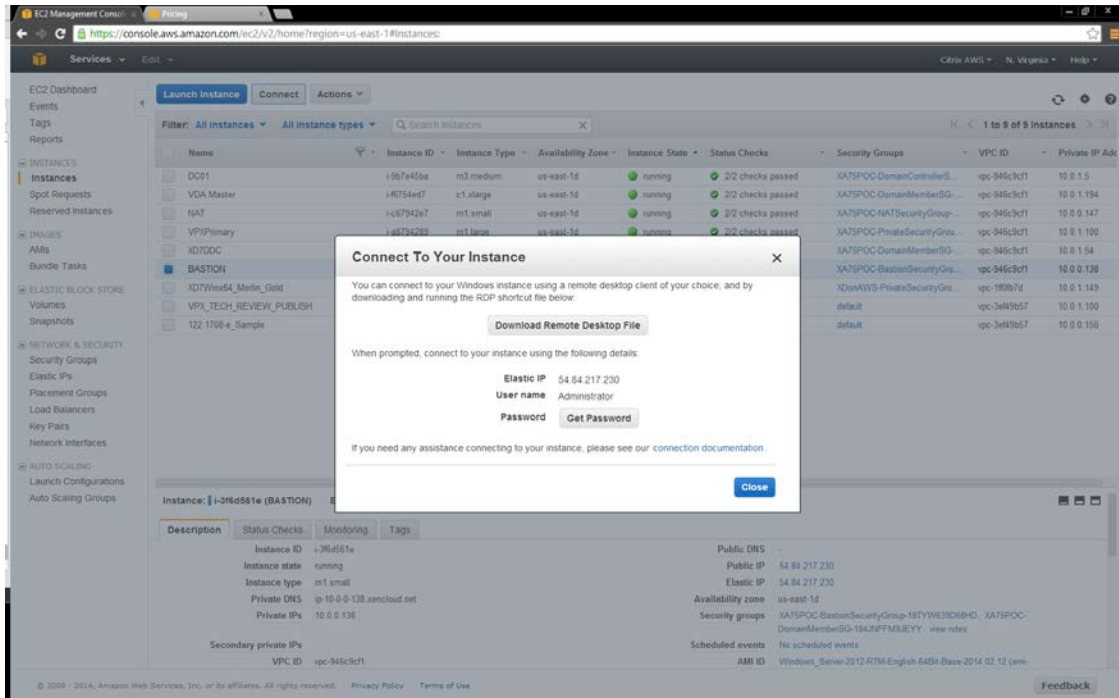
### Site infrastructure using the CloudFormation template



# Set up XenApp or XenDesktop on the AWS Infrastructure

Once you have setup AWS using an AWS CloudFormation template, you can configure XenApp or XenDesktop to deliver virtual desktops and applications from AWS.

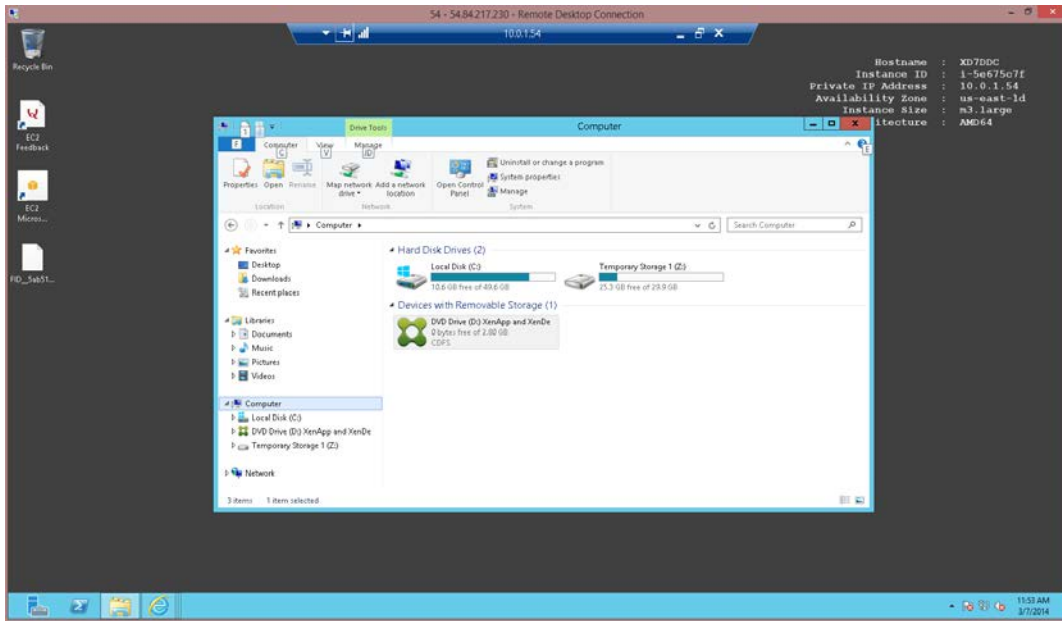
1. From the EC2 instances management console, select **Download Desktop File** to connect to the Bastion host using RDP.
2. Log in with the domain administrator credentials you provided during the CloudFormation Stack creation.



3. From the Bastion host, RDP to the Delivery Controller (the controller is **xd7ddc.xencloud.net** when using the default domain name), and log in as the domain administrator using again the **DomainAdminUser** and **DomainAdminPassword** provided as parameters during the stack creation event.



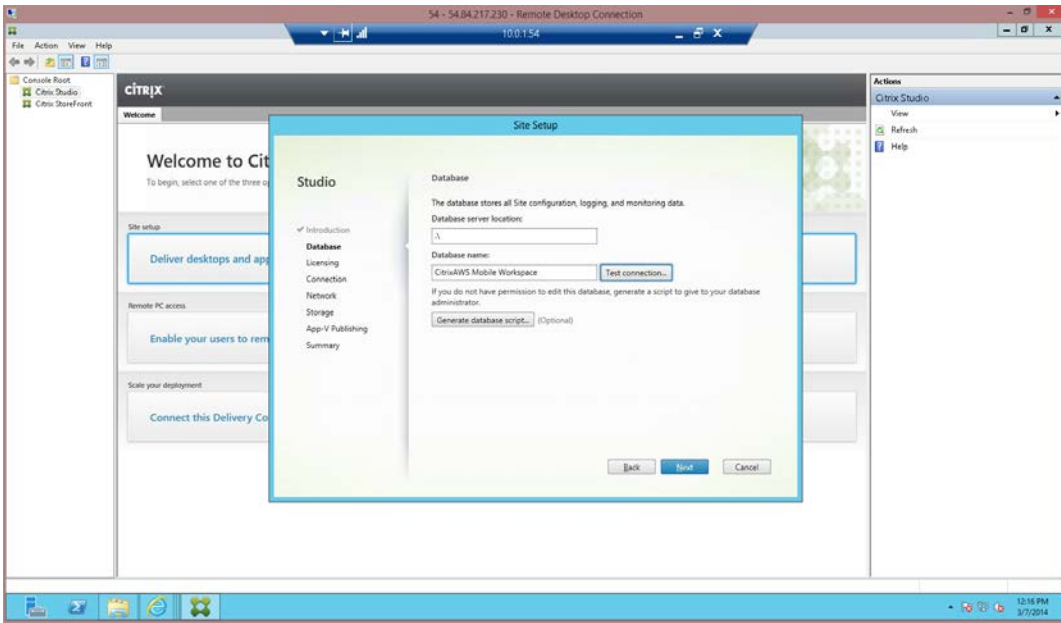
4. The XenApp and XenDesktop 7.5 product media is already mounted. Run **AutoSelect.exe** to start the installation.



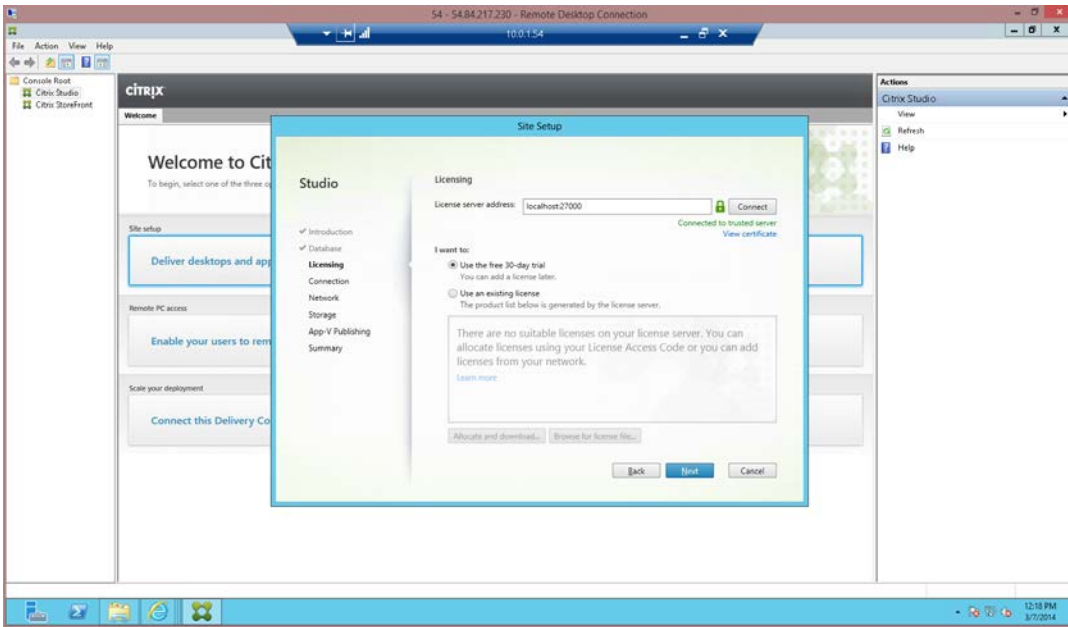
**Note:** The credentials file for the root AWS account, retrieved from [https://console.aws.amazon.com/iam/home?#security\\_credential](https://console.aws.amazon.com/iam/home?#security_credential) is not in the same format for credentials files downloaded for standard AWS users. Because of this, Studio cannot use the file to populate the API and secret key fields when creating a connection. Ensure that you are using IAM credentials files when administering Studio.

5. Install XenApp or XenDesktop as required for your environment.
  - a. Select the **Delivery Controller**.
  - b. Select **All Core Components**.
  - c. Follow the wizard instructions to complete the Delivery Controller Installation.
6. Start Citrix Studio, and follow the wizard to create the site. Note that the CloudFormation template has preinstalled SQL Server 2012 on the Delivery Controller.

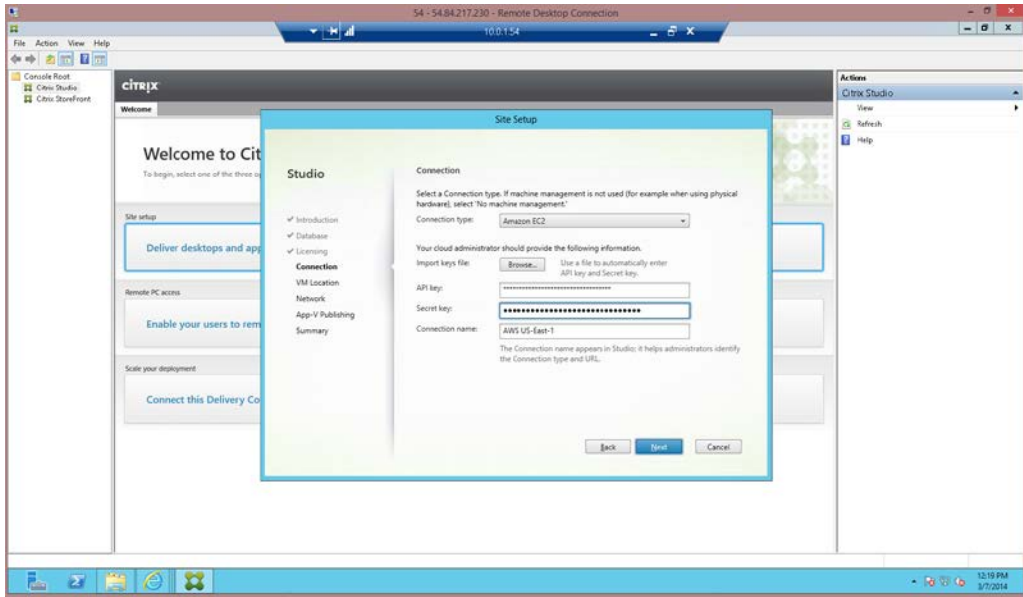
7. Select the local host as the database server location, and allow the wizard to create the database.



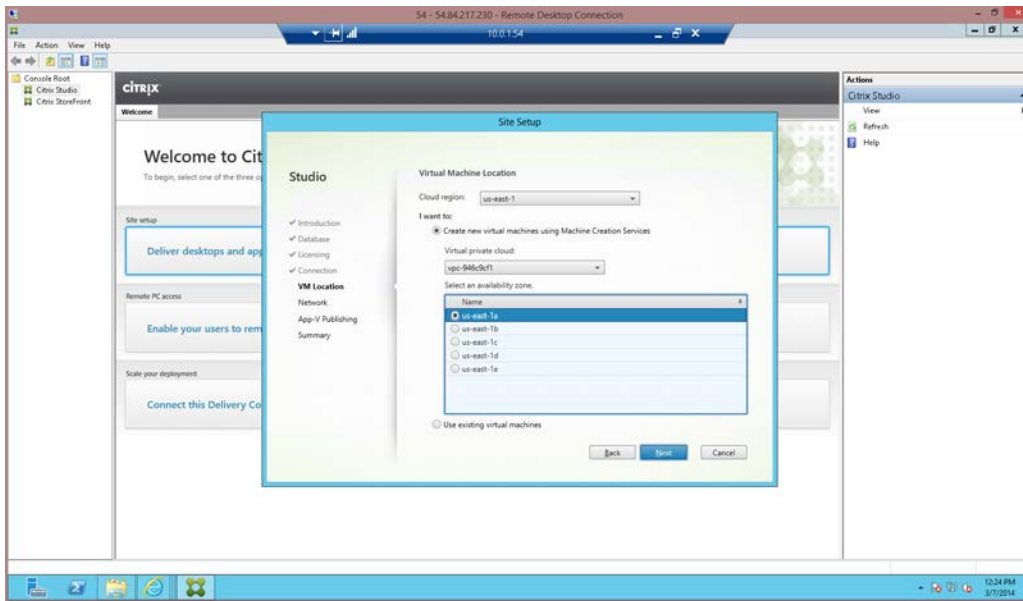
8. Complete the licensing setup.



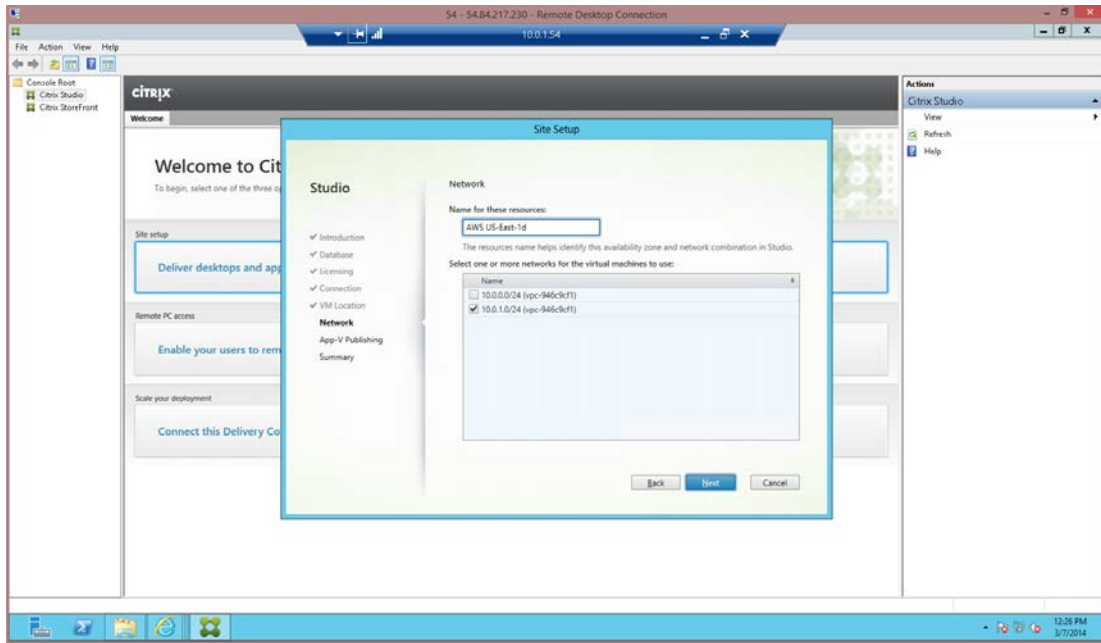
9. Provide your AWS access credentials to allow the Delivery Controller to provision instances on AWS.



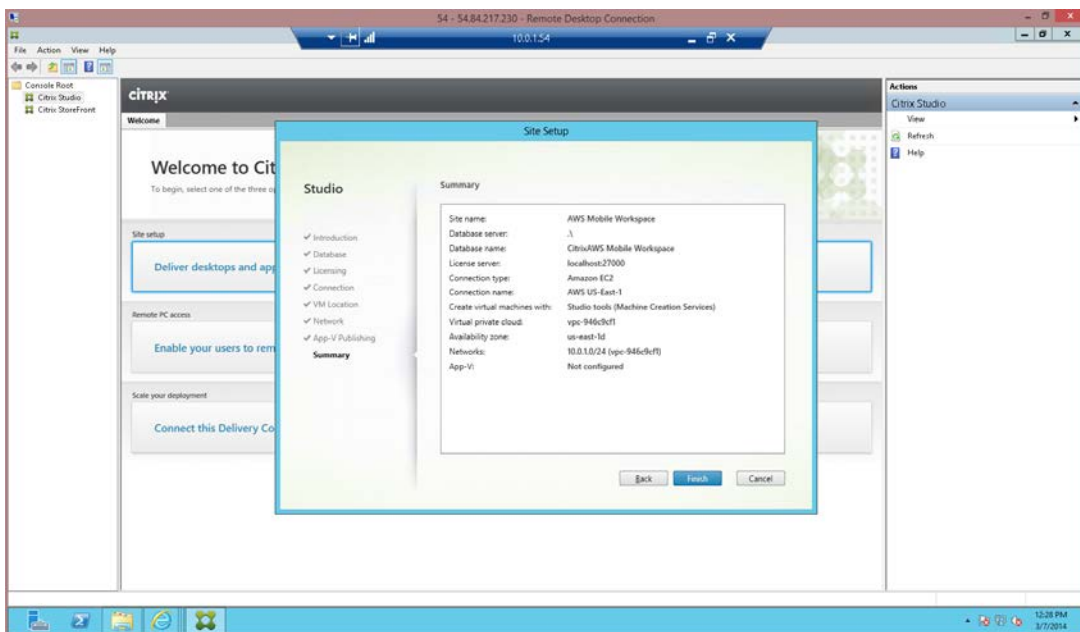
10. Select the AWS region, your VPC, and the desired availability zone for this connection.



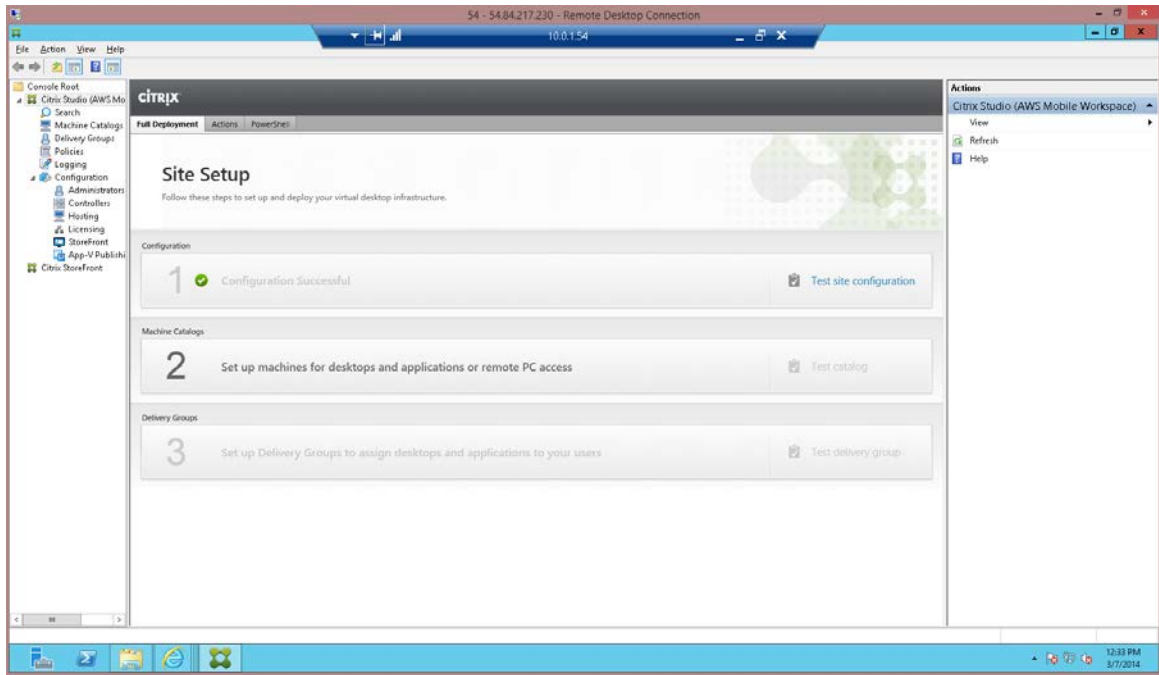
11. Select the subnets to host your instances, and then enter a name. In this example, the private subnet, **10.0.1.0/24** is selected to access the VDAs running in this private network, as shown in [Site Infrastructure using the CloudFormation template](#).



12. Skip the configuration for the App-V Publishing option to complete the Site setup. You can add this feature later.



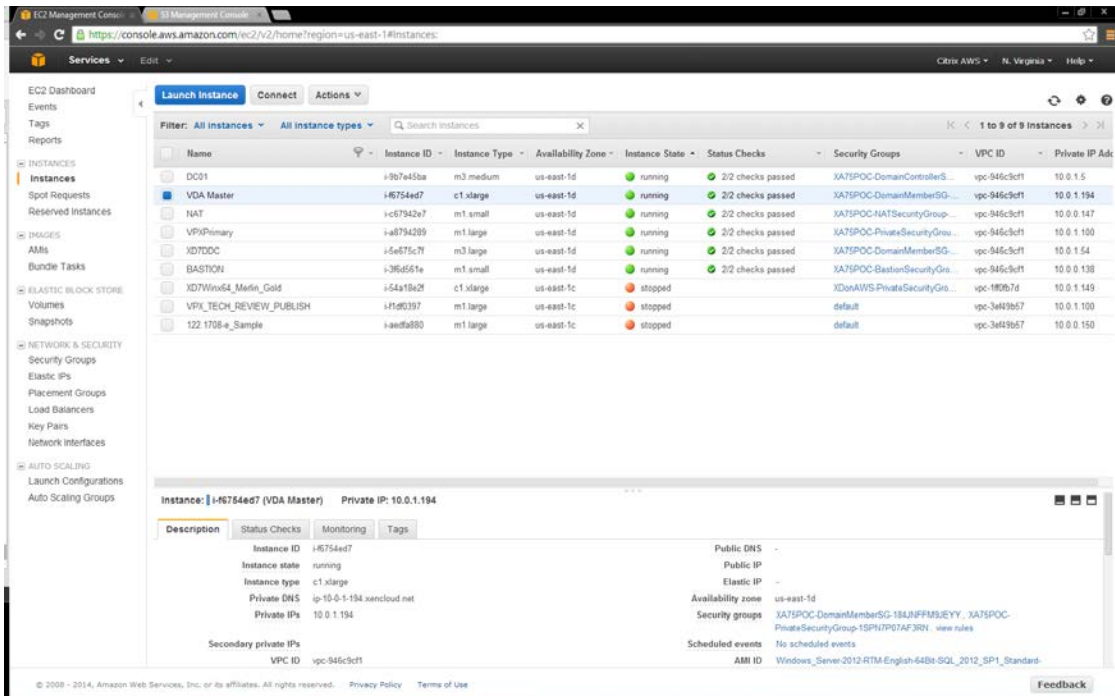
When the configuration completes, the wizard displays the Site Setup page.



## Configure the Master VDA machine

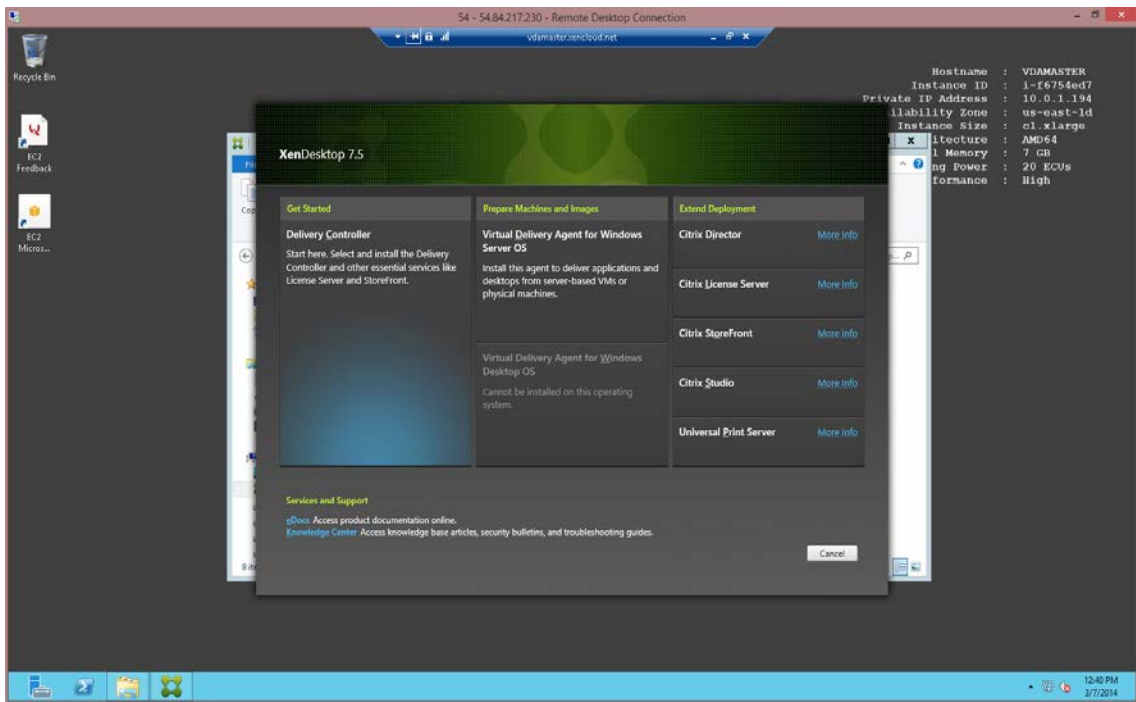
Once you have configured the Delivery Controller, you must configure a master image by configuring a master VDA machine.

1. From the Bastion host, RDP to the VDA Master (you can find the IP address from the EC2 console), and log in as the **domain administrator**, using again the **DomainAdminUser** and **DomainAdminPassword** provided as parameters during the stack creation event. Private IP addresses?

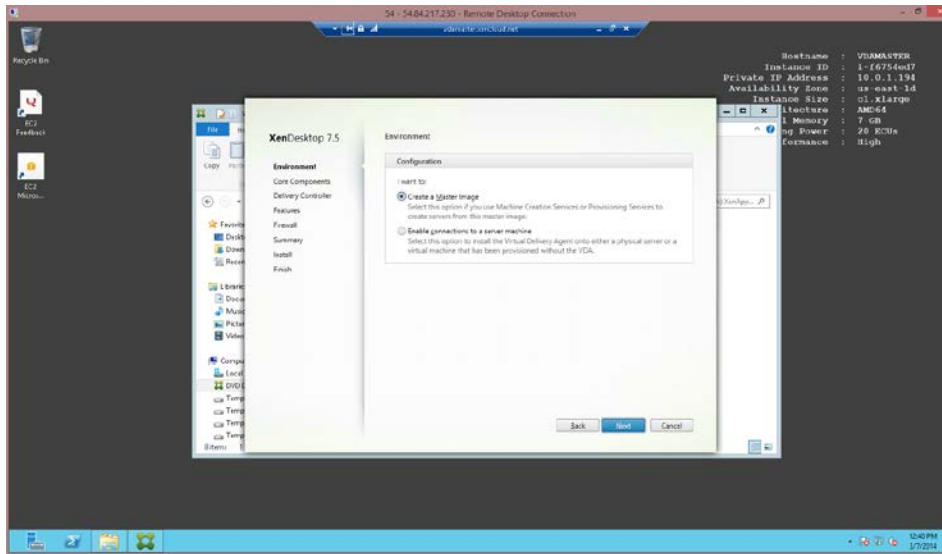


2. The XenApp and XenDesktop 7.5 product media is already mounted. Run **AutoSelect.exe** to start the installation.

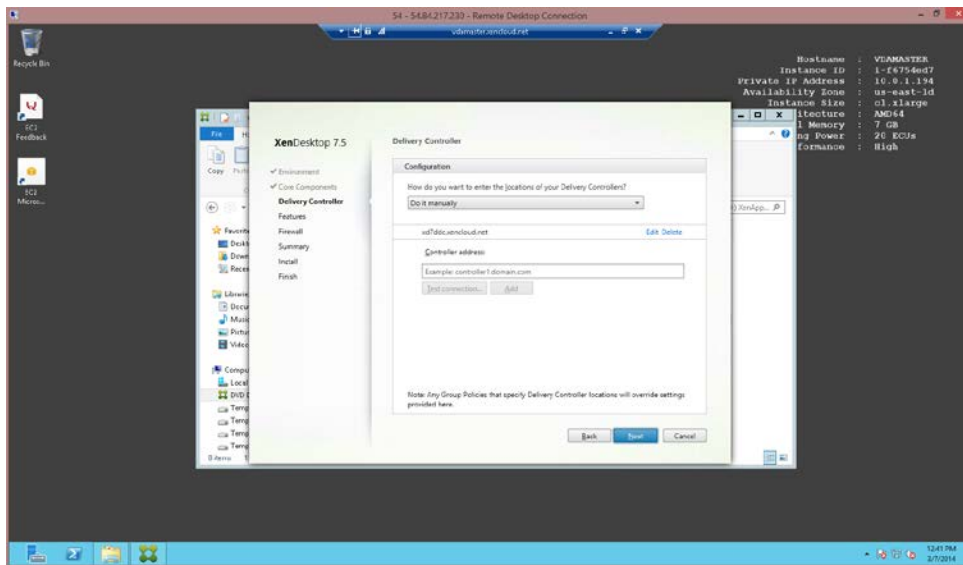
3. Select **Virtual Delivery Agent for Windows Server OS** for a XenApp Worker installation. See [Server VDI](#) for information on setting up a Server VDI Master VDA.



10. Select **Create a Master Image**.



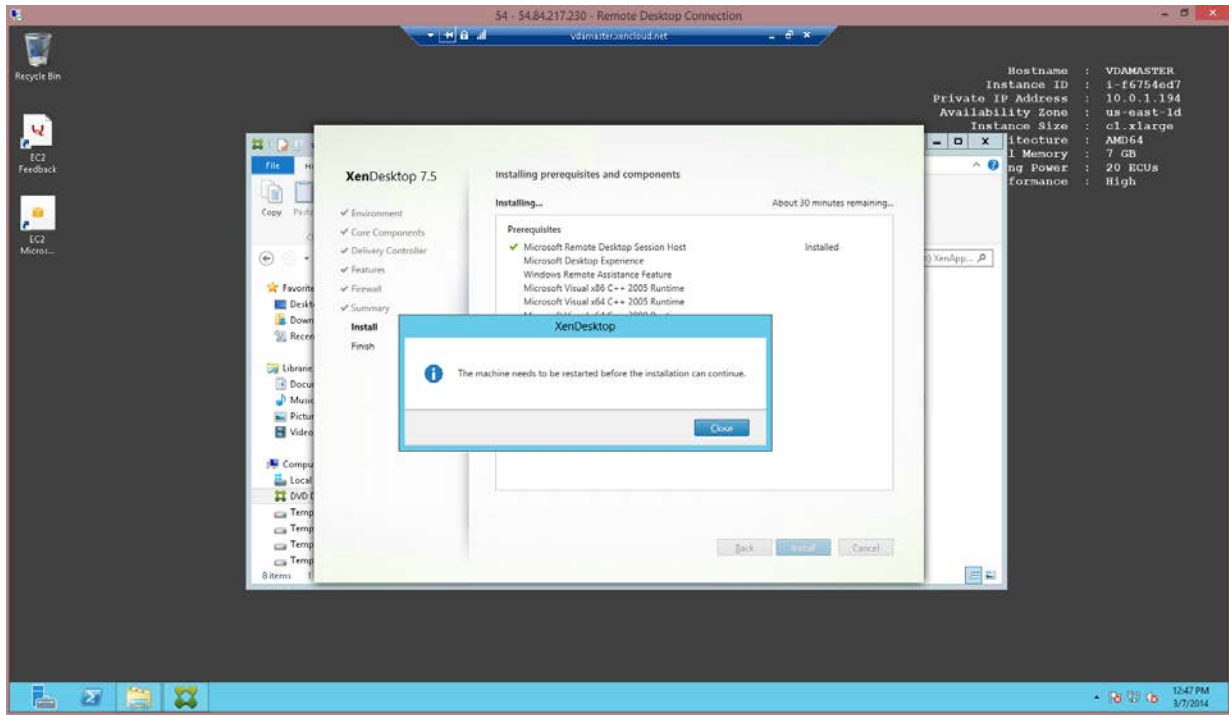
11. Supply the FQDN of the Delivery Controller you configured earlier in this process.



12. Review the specified settings for the Master VDA, and then select **Install** to complete the VDA Master installation.

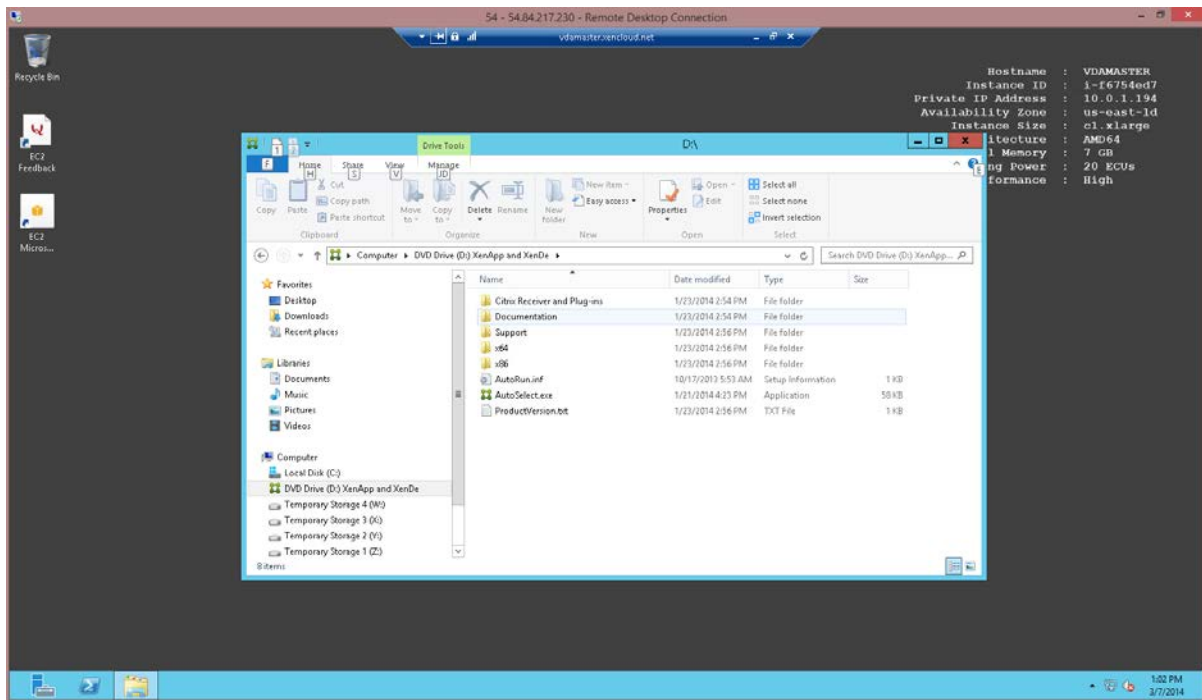
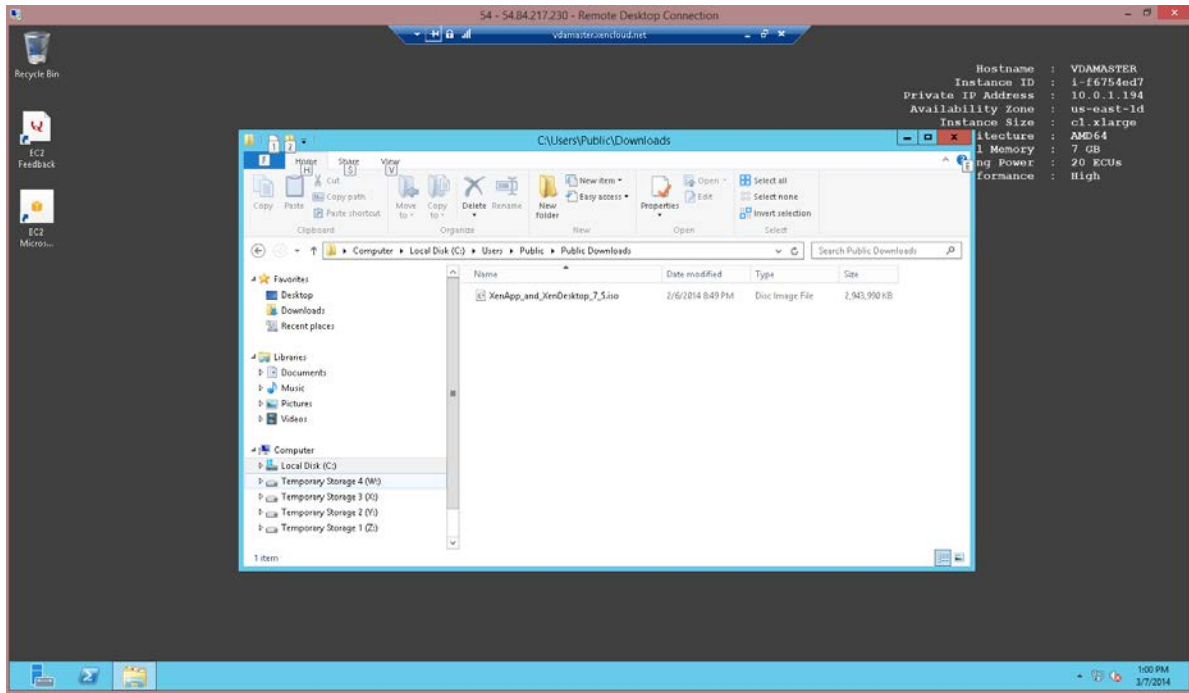


**Note:** You must reboot the machine to complete the addition of the Microsoft Remote Desktop Session host. You can reboot from within the instance; you do not need to use the AWS console to do so. It can take several minutes after reboot before the instance responds to RDP connections again.

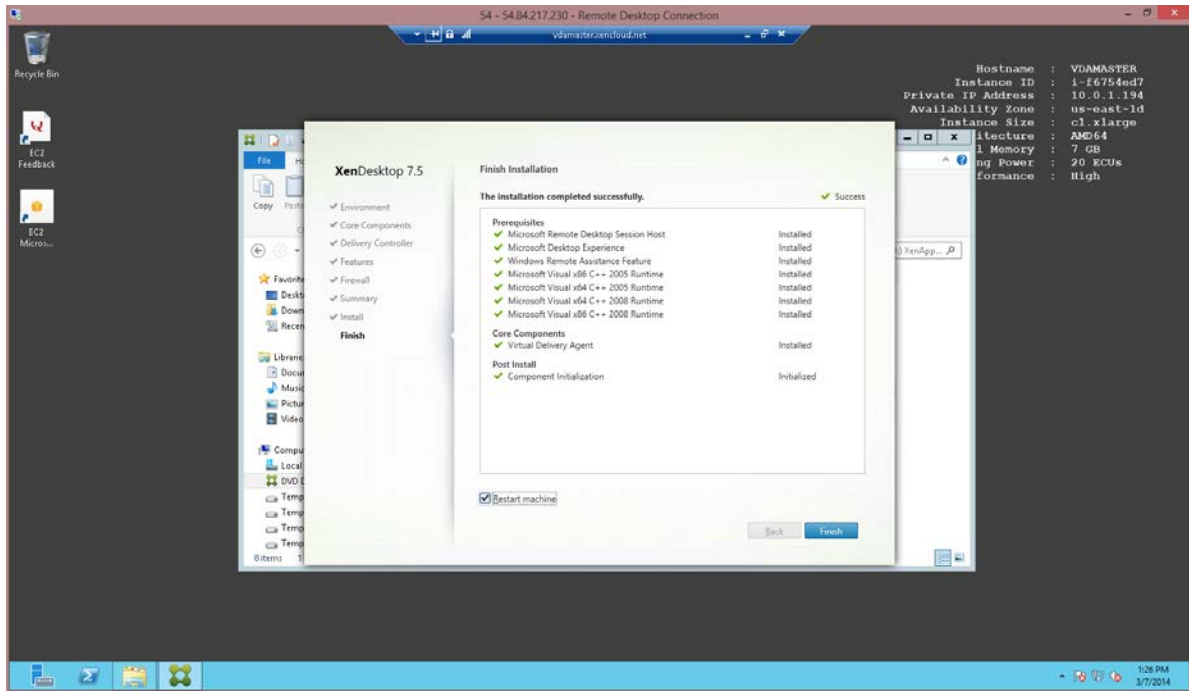


13. After the machine reboots, log in to the Master VDA. The XenApp and XenDesktop product media is no longer mounted (it searches for the media), and the installation does not continue.

14. Click **Cancel**, and remount the media from its location. For example, C:\Users\Public\Downloads.

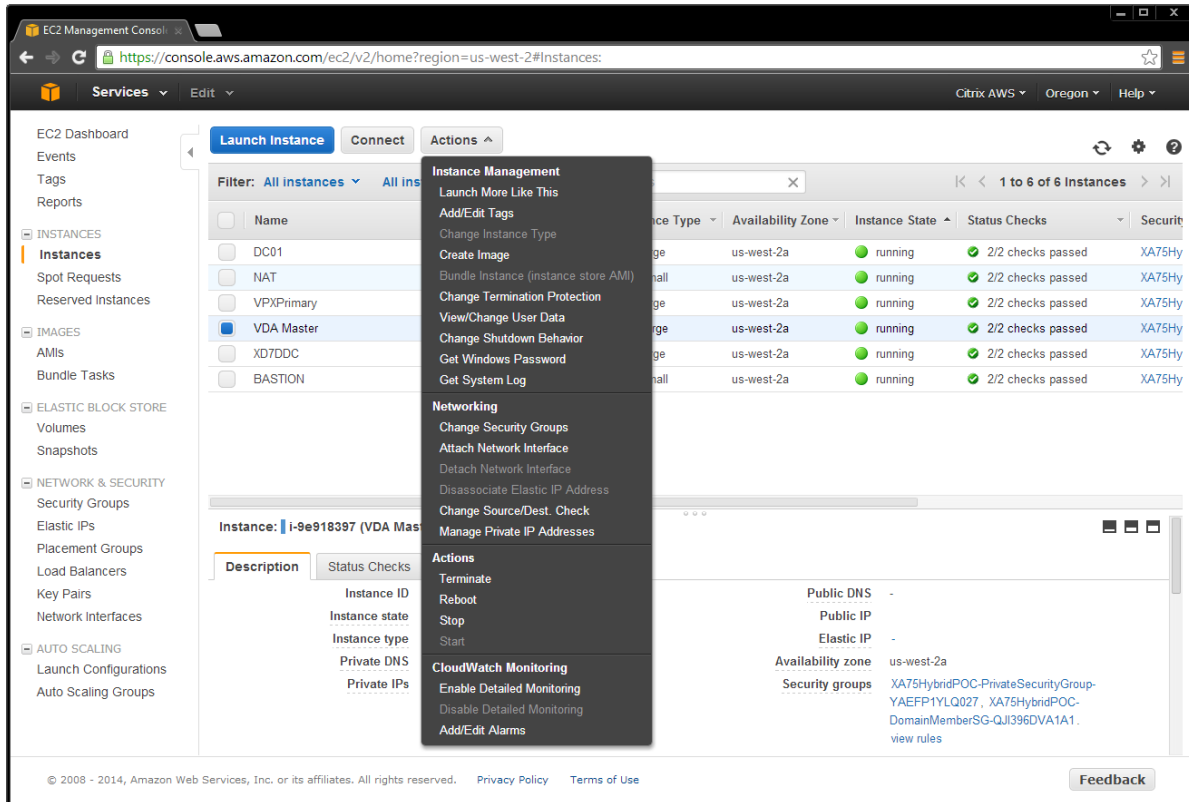


15. When the media is mounted, select the **Virtual Delivery Agent for Windows installation**, which automatically continues from where it left off.
16. Restart the machine.

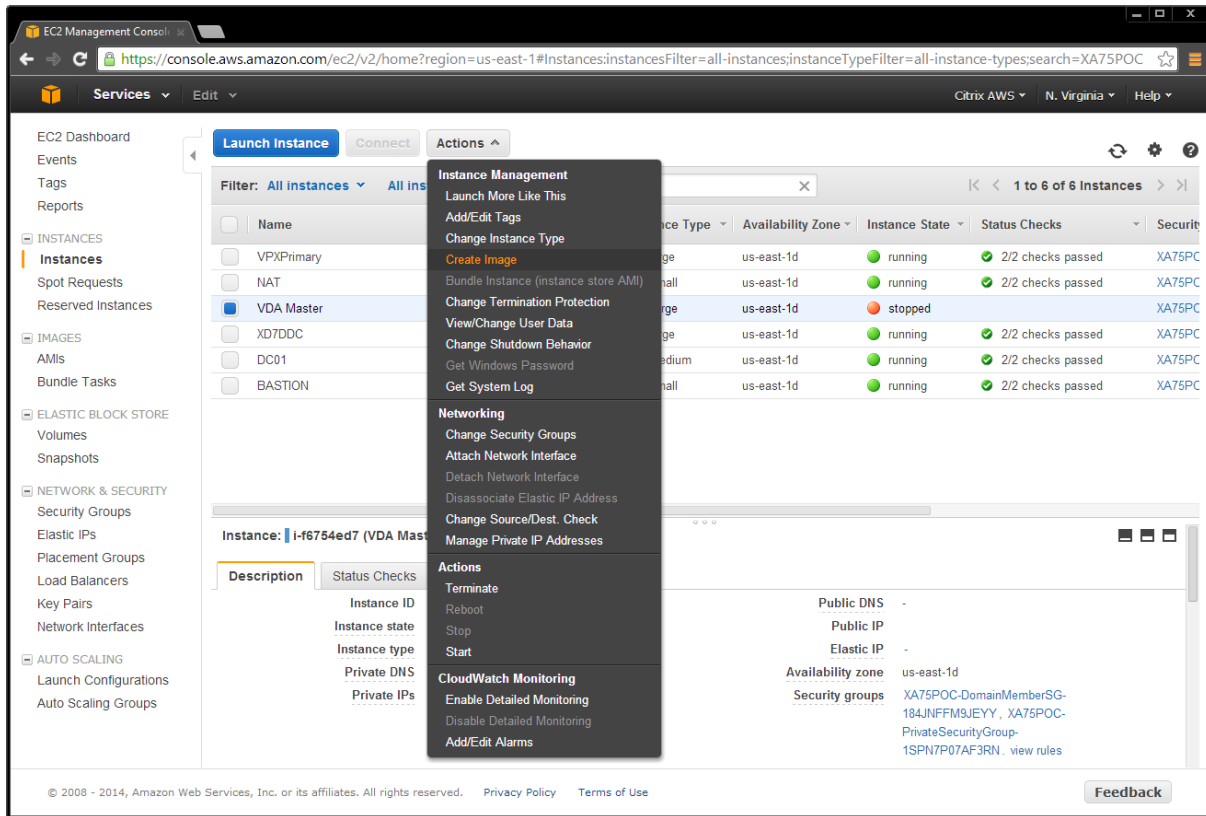


17. After the VDA installation completes, install applications that will be published or available on the users' desktops on the master VDA.

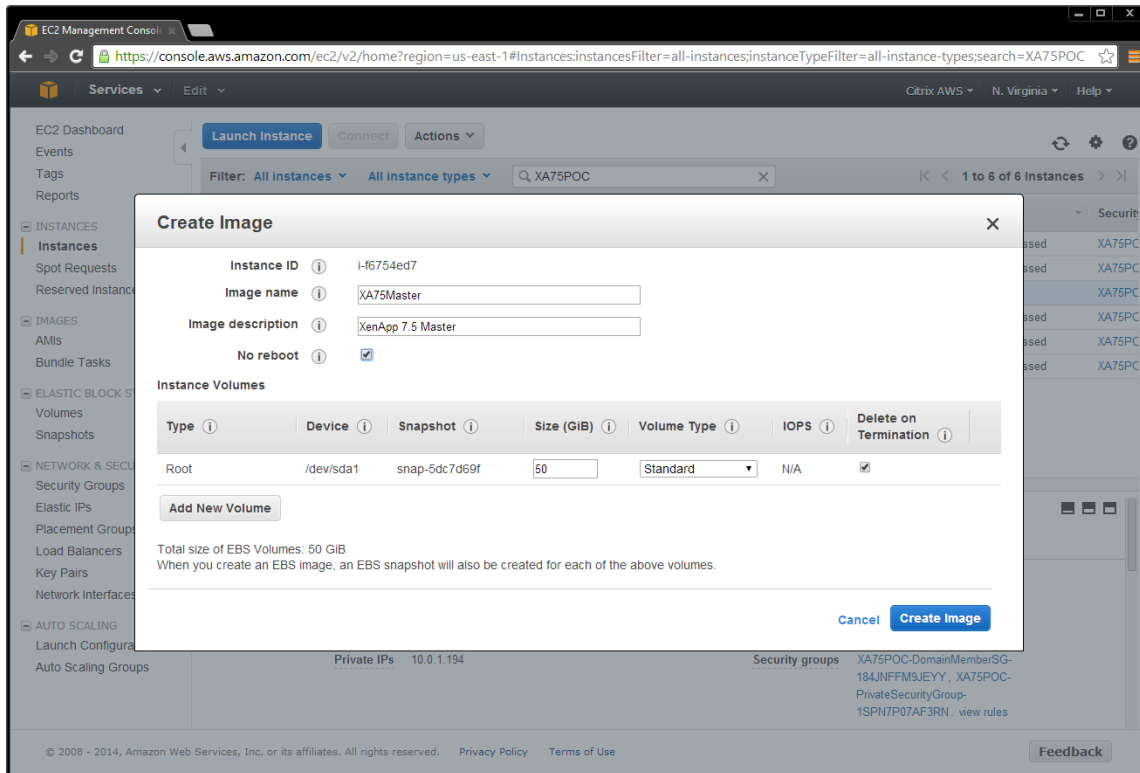
18. After installing additional software, from the EC2 Console, select **Actions > Stop** to shut down the VDA Master Image.



19. After shutdown, create an AMI from your Master VDA by selecting **Actions > Create Image**.



20. Assign a name and description, and then click **Create Image**.



**Important:** By default, **Delete on Termination** is selected. **Do not change this setting.** The product works on the assumption that root disk volumes are deleted automatically by Amazon. Unchecking this box can cause the deployment to leak volumes in EBS storage.

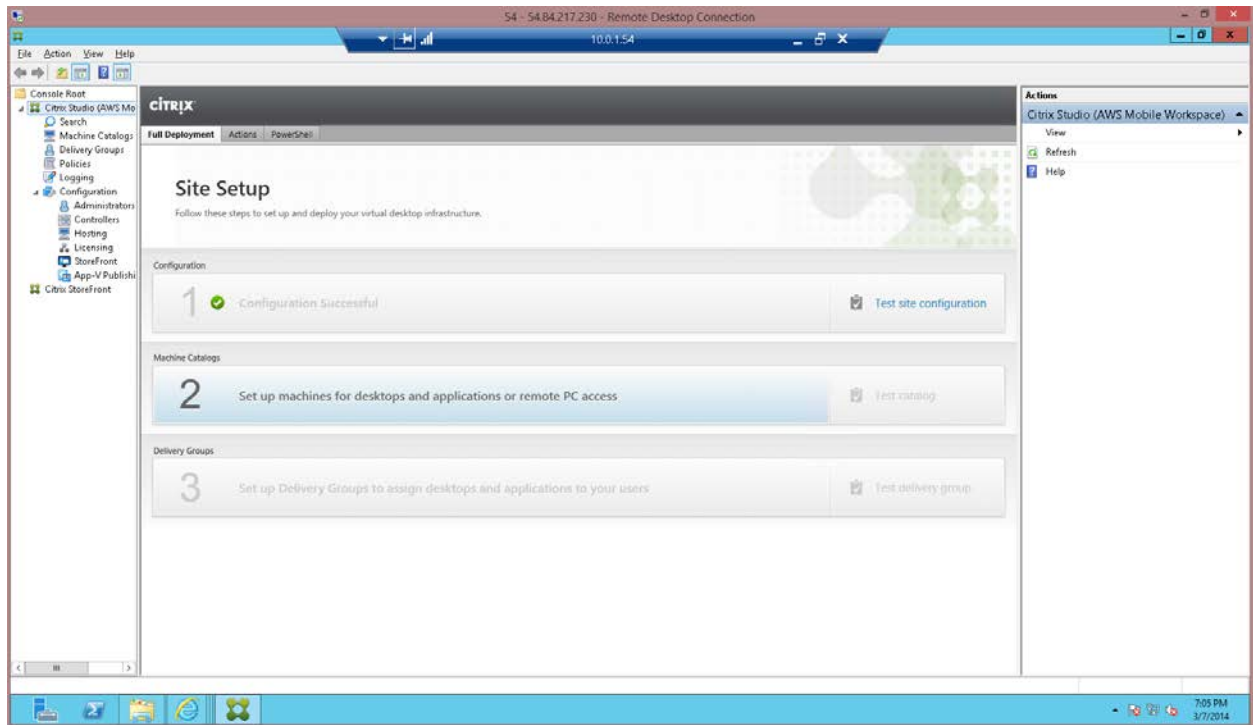
Depending on the size of the instance volume, image creation can take a long time. You must wait until the image is fully created before you can see it in Studio.

When the AMI creation process completes, set up machines in Studio using Master VDA AMI.

## Set up machines in Studio using the Master VDA AMI

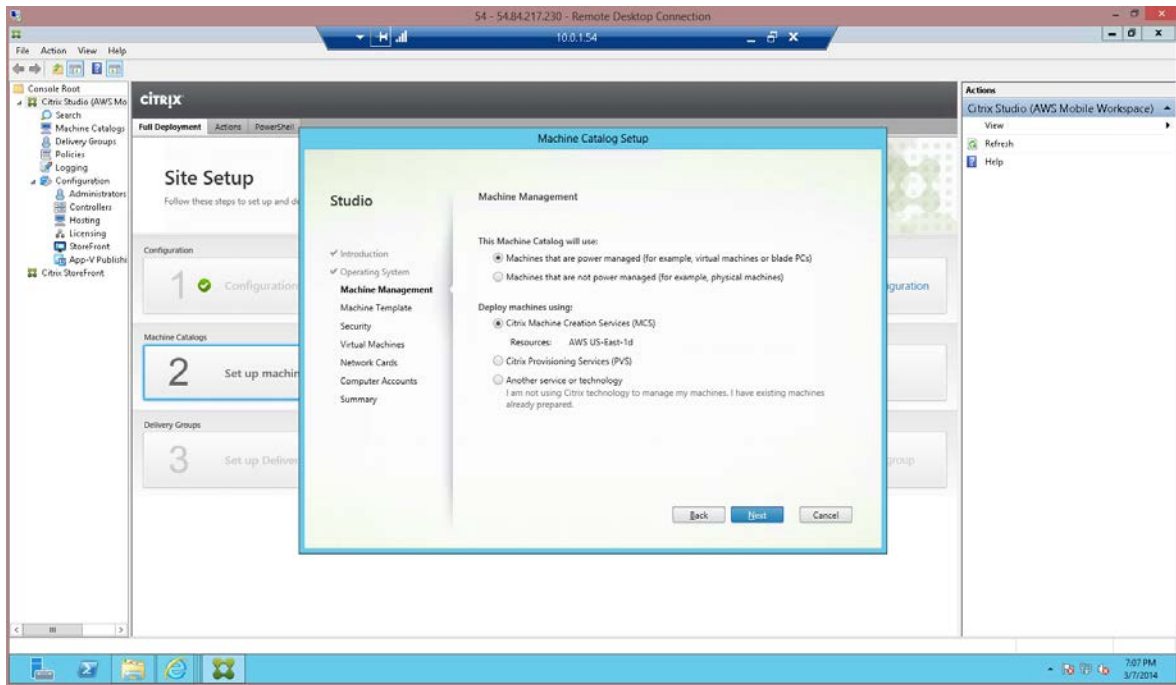
Now that the master AMI is configured, use Studio to provision applications and desktops by creating a machine catalog.

1. Open Studio on the Delivery Controller and select **Option 2**.



2. Select **Server OS**. If your configuration has Server VDI available on a Desktop OS, you can alternatively choose the **Desktop OS** option.

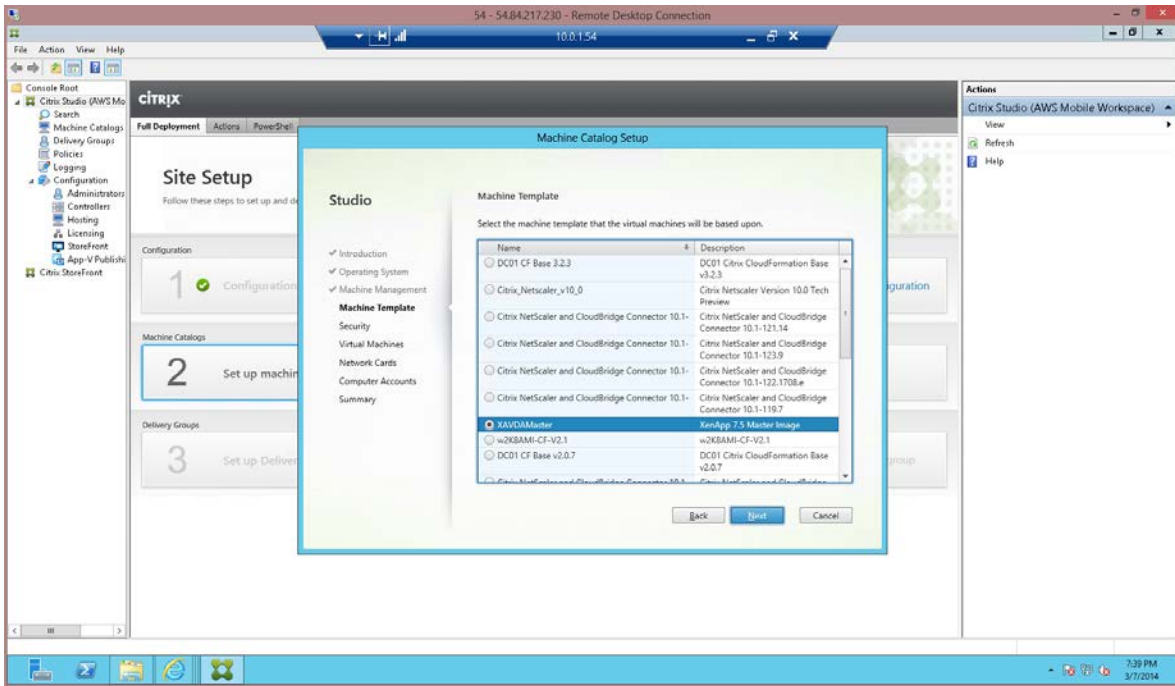
- To enable XenApp or XenDesktop to control machine provisioning in AWS, select the settings shown in this example:



**Note:** AWS does not support Citrix Provisioning Services.

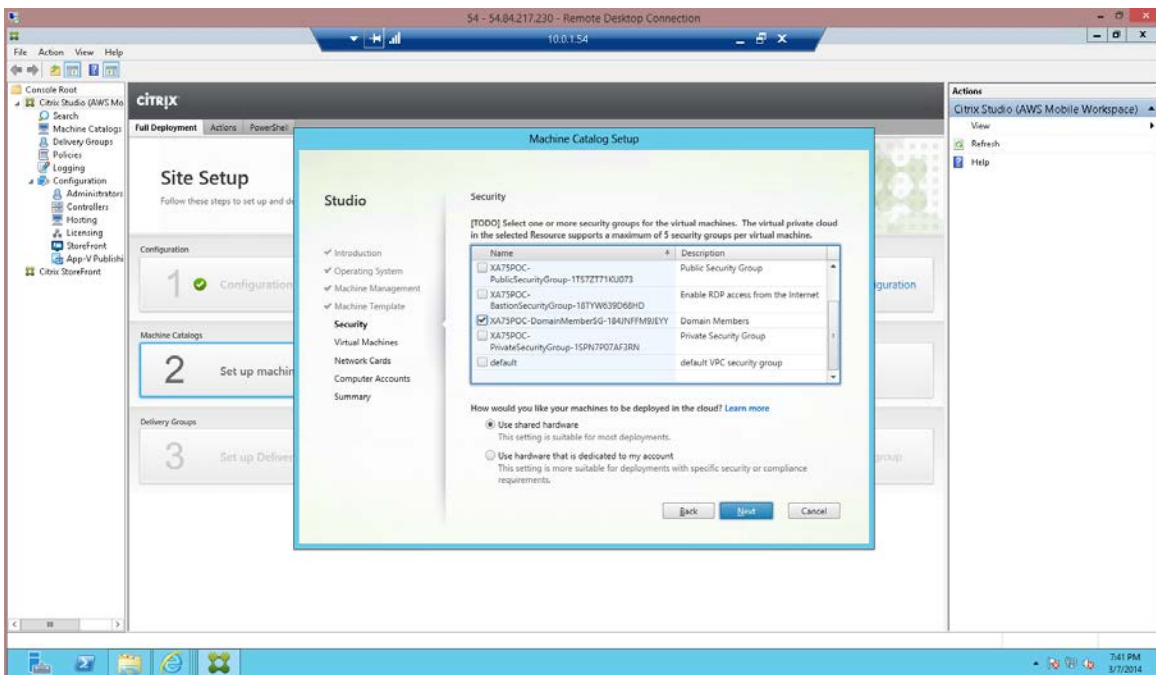


- Select the machine template the AMI created in the EC2 console as described in [Configure the Master VDA machine](#).

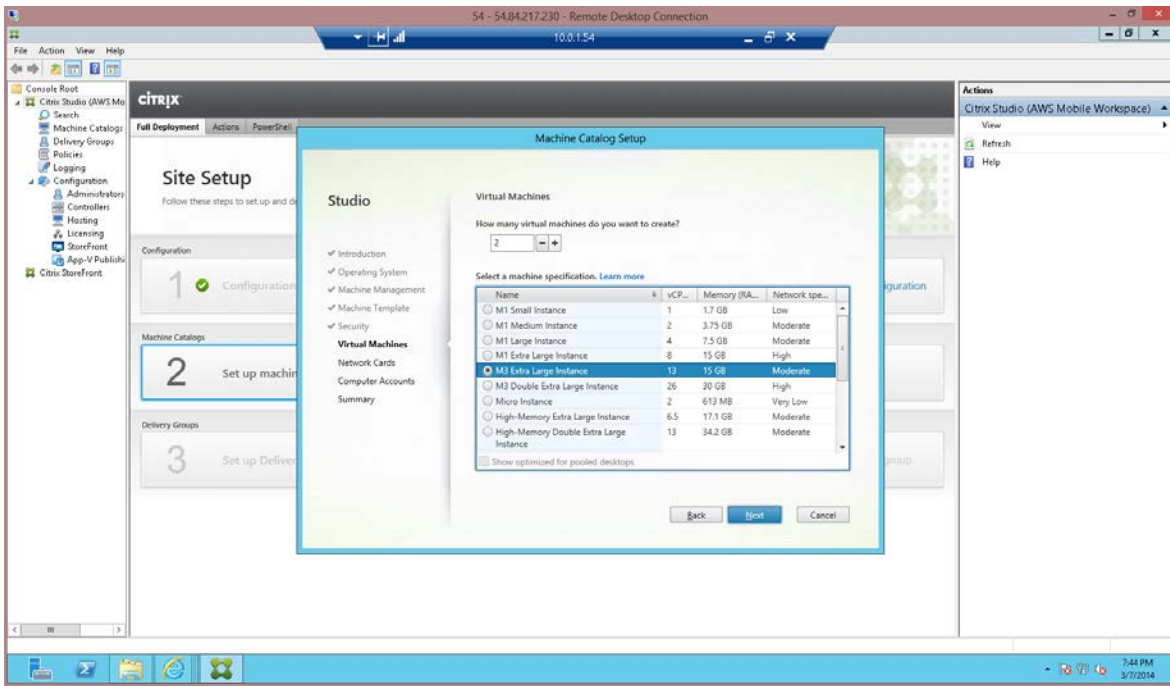


- Select the required security groups. In this example, you must select the **DomainMemberSG** Security as well as the private security group **PrivateSecurityGroup**. This ensures communication between the Domain controller and the VDAs.

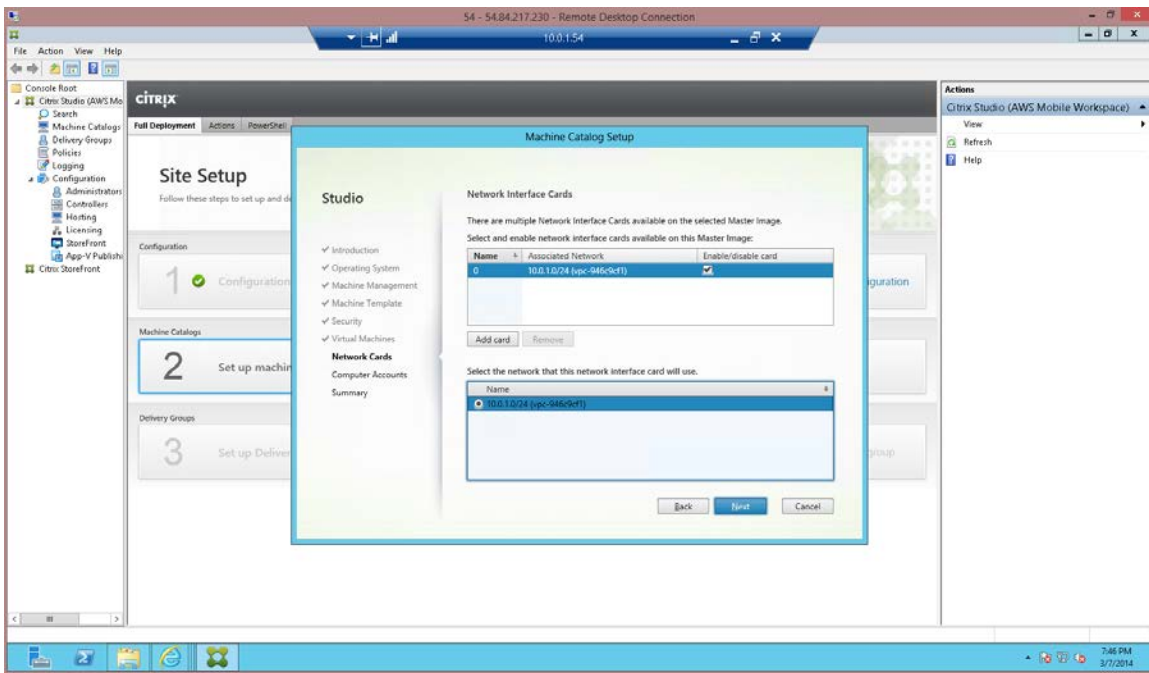
You can also indicate that dedicated hardware is required to host your instances. **Use Shared Hardware** is the default.



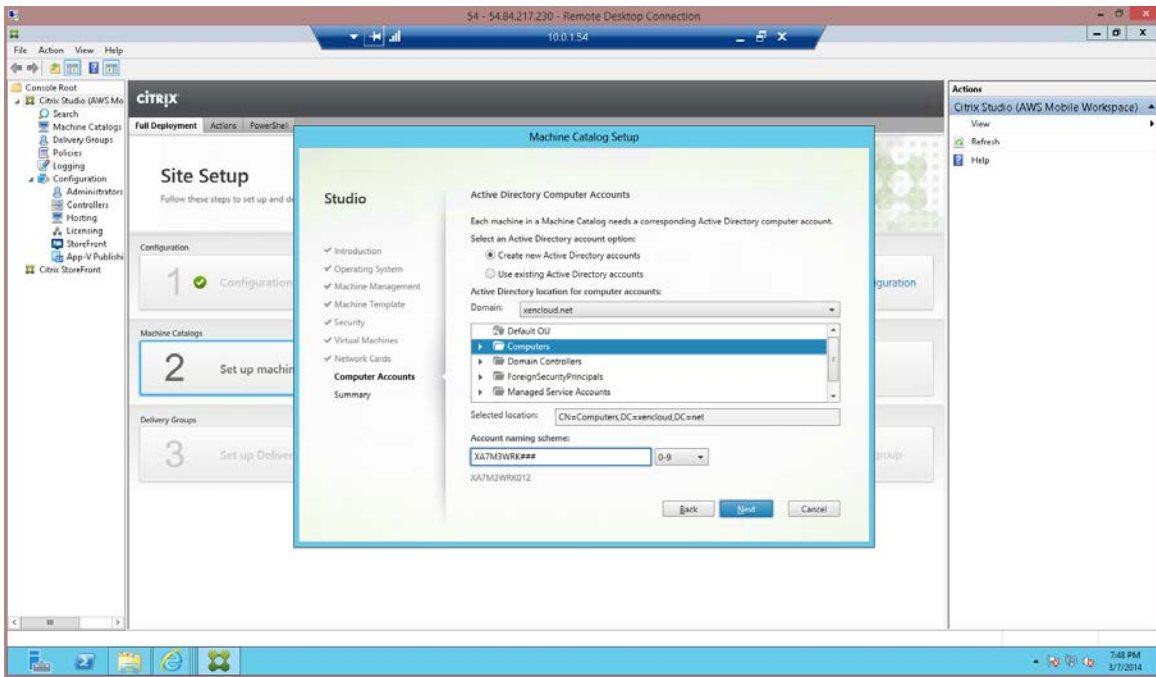
6. Select the number of machines and instance type to for the machine catalog.



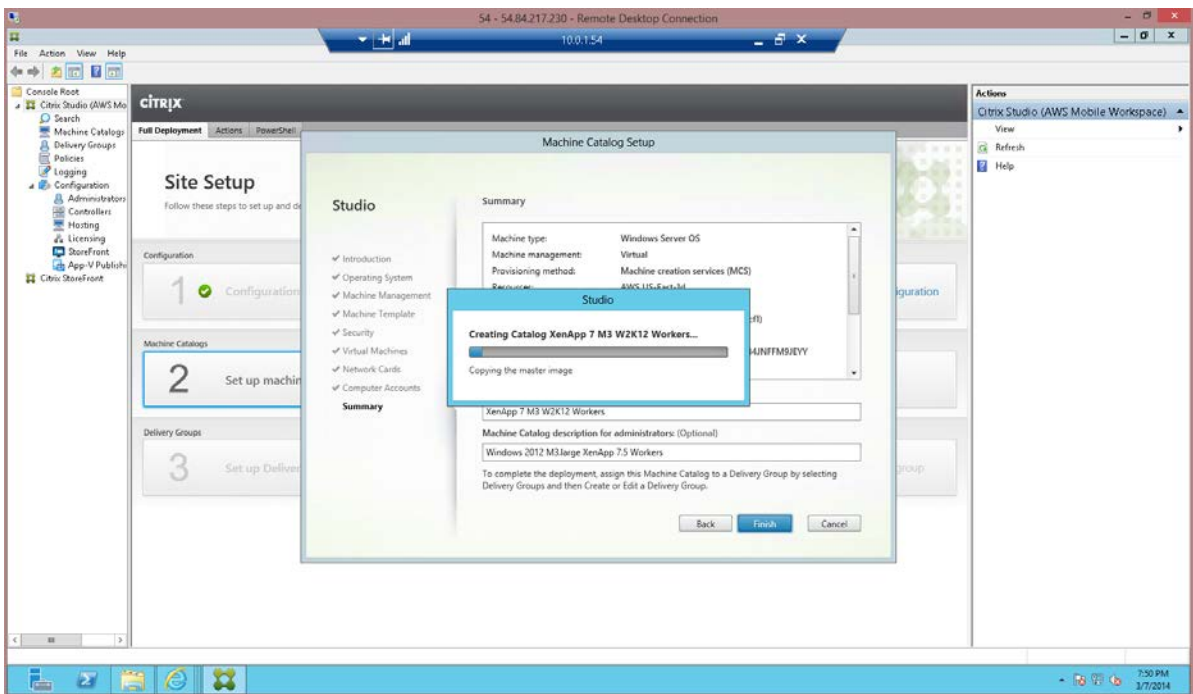
7. Select the networking configuration.



8. Configure the computer accounts.



9. Enter a name, and click **Finish**. Note that the process of copying the master image can take a long time to complete. It may take 30 to 40 minutes, or more if there are a lot of machines in the catalog.



## Set up Delivery Groups

After setting up machines in the machine catalog, configure Delivery Groups to specify which users can access desktops or applications that you want to provide. Delivery Groups are usually based on user characteristics, such as job function or geographical region.

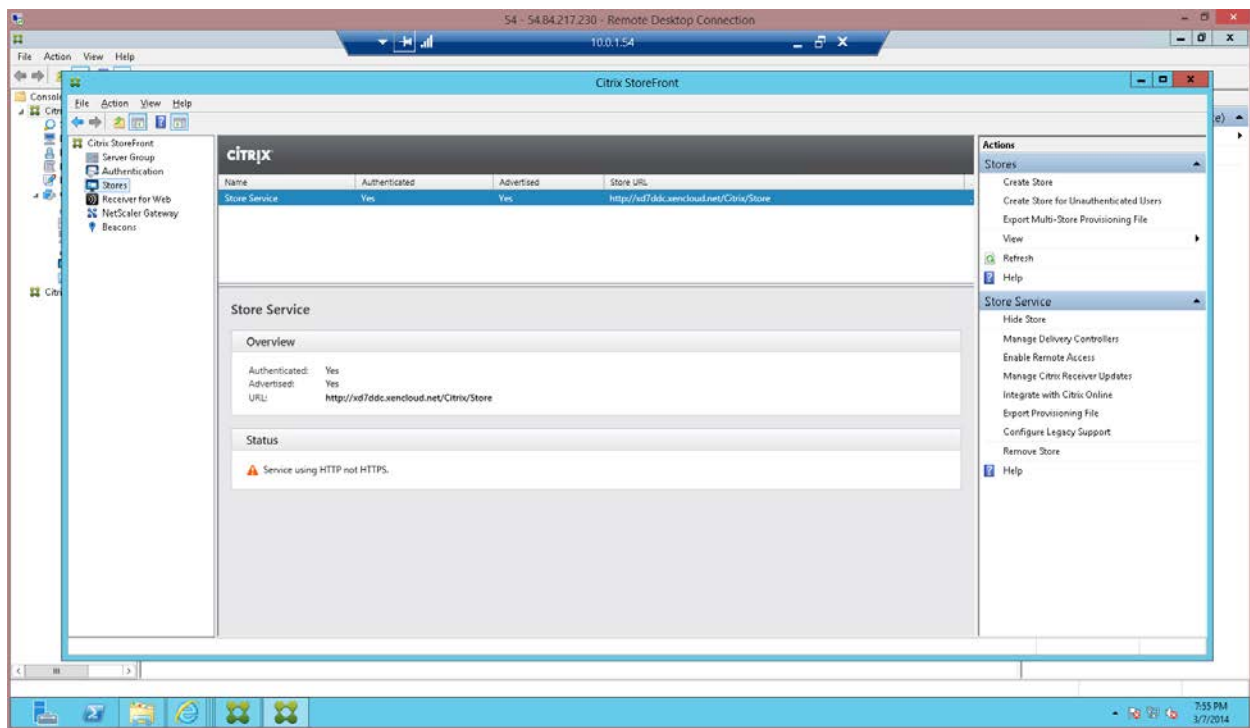
1. In Studio, select the Delivery group node and click **Create Delivery Group**.
2. Click **Add Machines**, select a machine catalog for this Delivery Group, and then enter the number of machines the group consumes from the machine catalog.
3. On the Users page, click **Add users** to add the users or user groups that can access the desktops or applications. You can select user groups by browsing or entering a list of Active Directory users and groups each separated by a semicolon. For Desktop OS Delivery Groups, you can import user data from a file after you create the group.
4. On the Delivery Type page, select what the desktops deliver to users:
  - Applications only
  - Desktops only
  - Applications and desktops
5. On the StoreFront page, select StoreFront URLs to be pushed to Citrix Receiver so that Receiver can connect to a StoreFront without user intervention. Note that this setting is for Receiver running on VDAs.
6. On the Scopes page, define which administrators can access the Delivery Group.
7. On the Summary page, check all details and then enter a display name that users and administrators see and a descriptive Delivery Group name that only administrators see.

## Set up NetScaler Gateway Remote Access

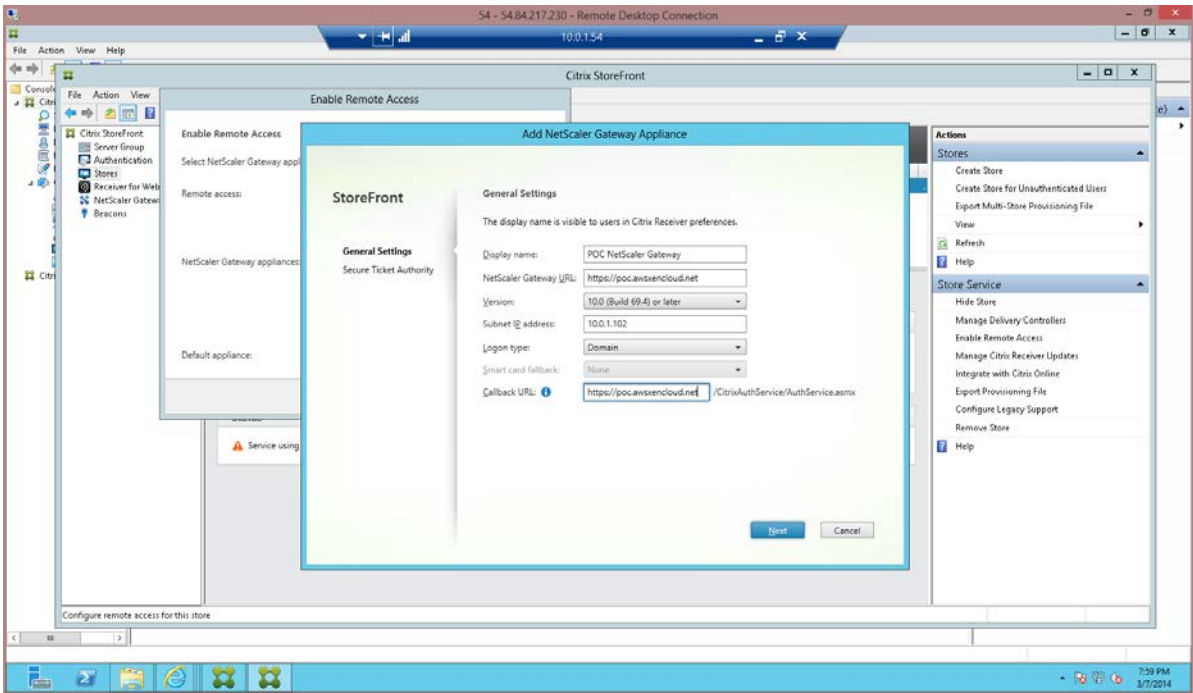
After provisioning applications and desktops through Studio, set up access to StoreFront by configuring remote access to NetScaler Gateway. Remote users access and authenticate to the NetScaler Gateway. Upon successful validation, NetScaler Gateway forwards the user request to StoreFront, which generates a list of available application and desktop resources.

### Set up StoreFront

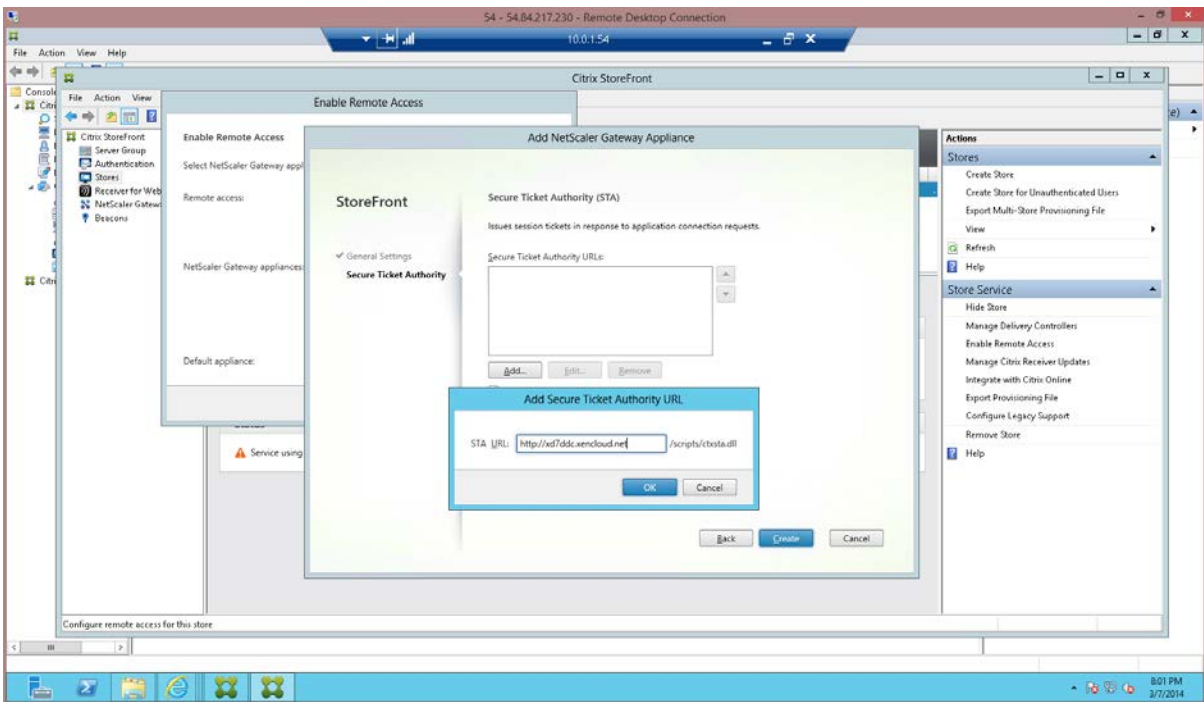
1. Run the StoreFront administration console on the Delivery Controller and enable remote access.



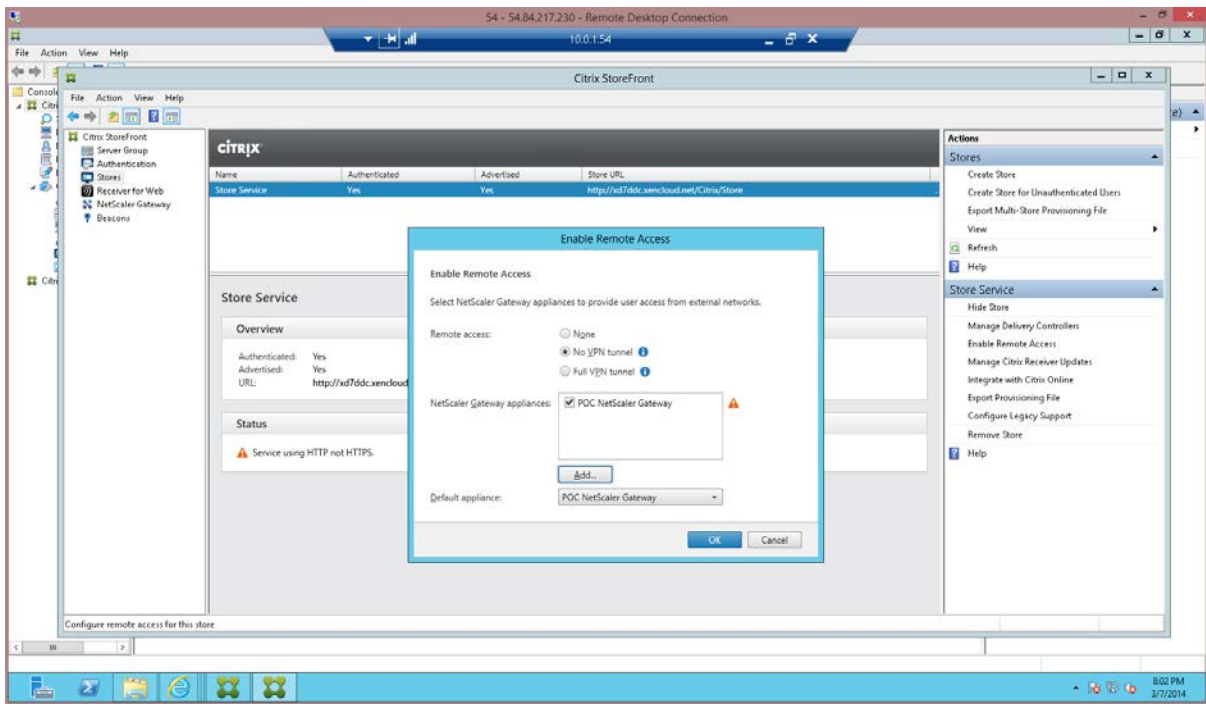
2. In the StoreFront Remote Access wizard, enter the parameters of your public NetScaler configuration, such as the FQDN and the NetScaler subnet IP address (SNIP). In this example, the **SNIP is 10.0.1.102**.



3. Add the Secure Ticket Authority (STA), which is the Delivery Controller.

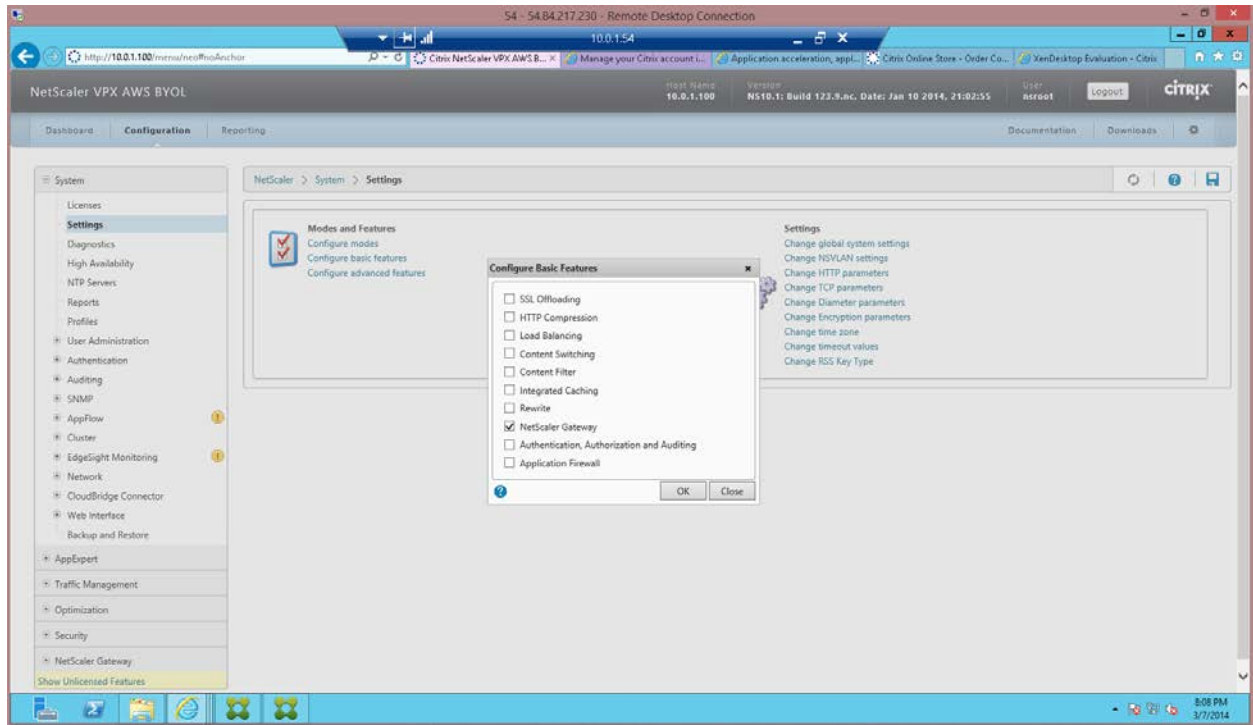


- Click **OK**, and then click **Create** to complete the NetScaler Gateway definition for StoreFront.



- Click **OK** to complete the remote access enabling process.
- Enable the NetScaler Gateway function.
  - Connect a machine on the private subnet to the NSIP (10.0.1.100).
  - Log in to the NetScaler GUI.

7. On the NetScaler Gateway, you must use the subnet IP and enable MAC-based forwarding.

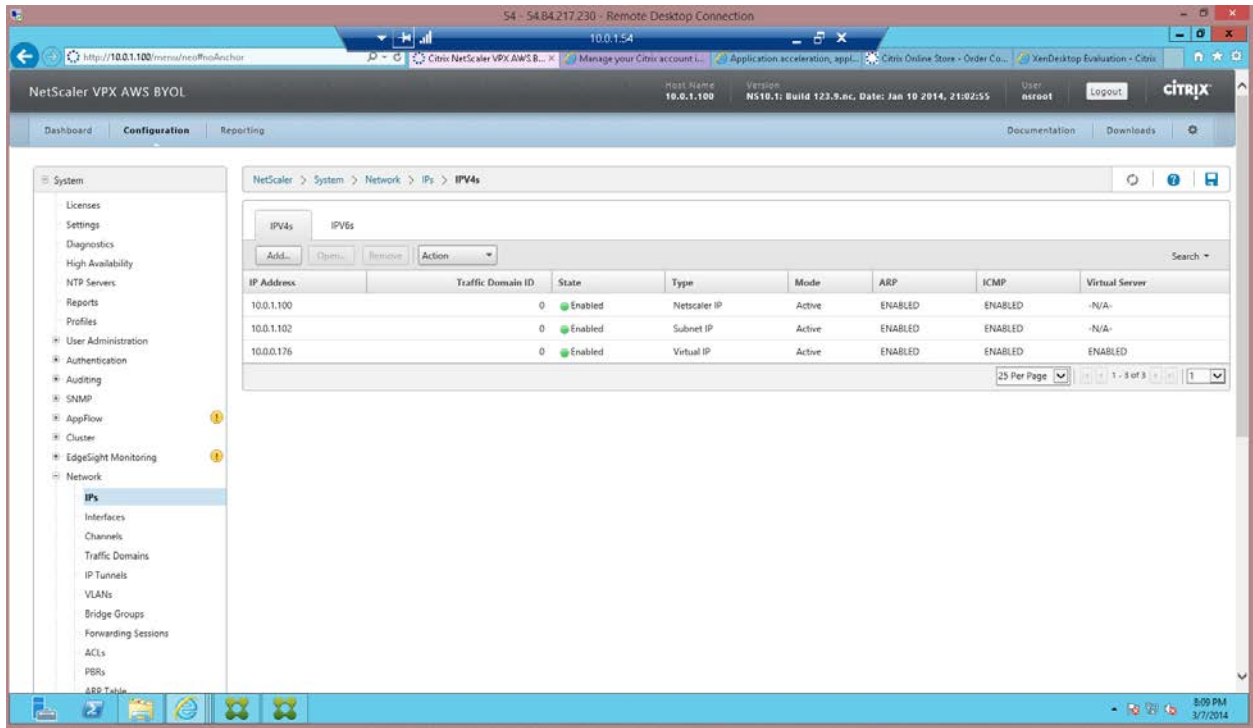


8. Create the following network connections:

- a. **SNIP** with IP address **10.0.1.102** on the NetScaler server
- b. **VIP** with IP address **10.0.0.176** on the NetScaler client

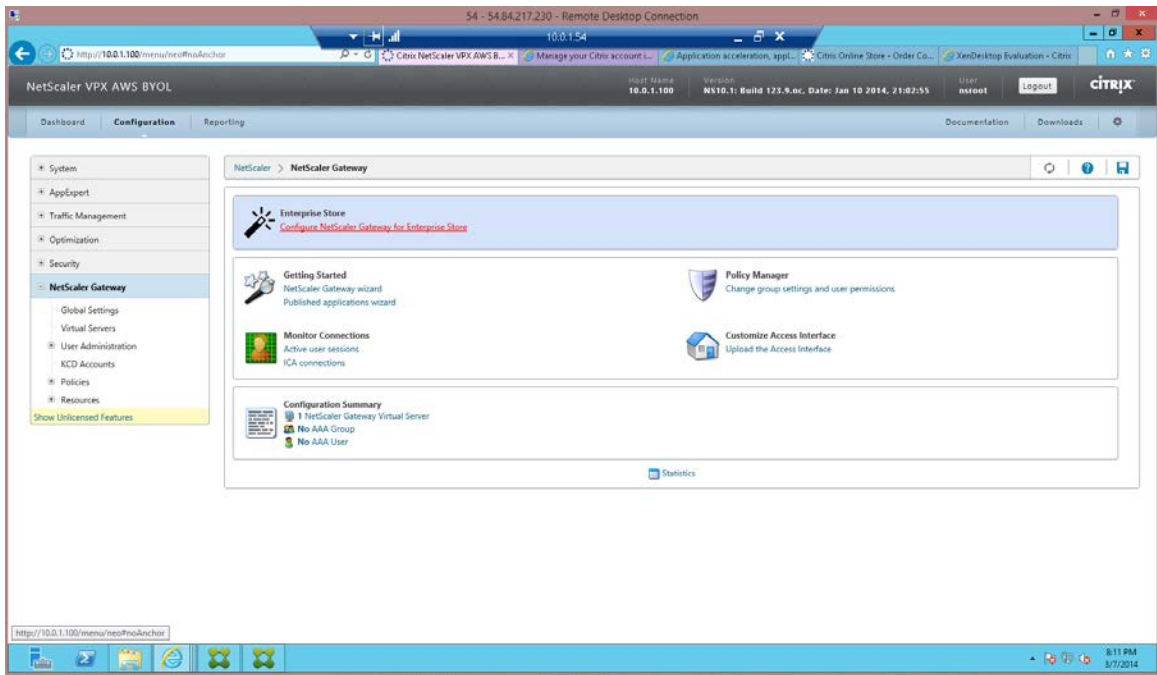


The CloudFormation template or the manual setup procedure has already configured these addresses at the AWS layer for the NetScaler VPX.

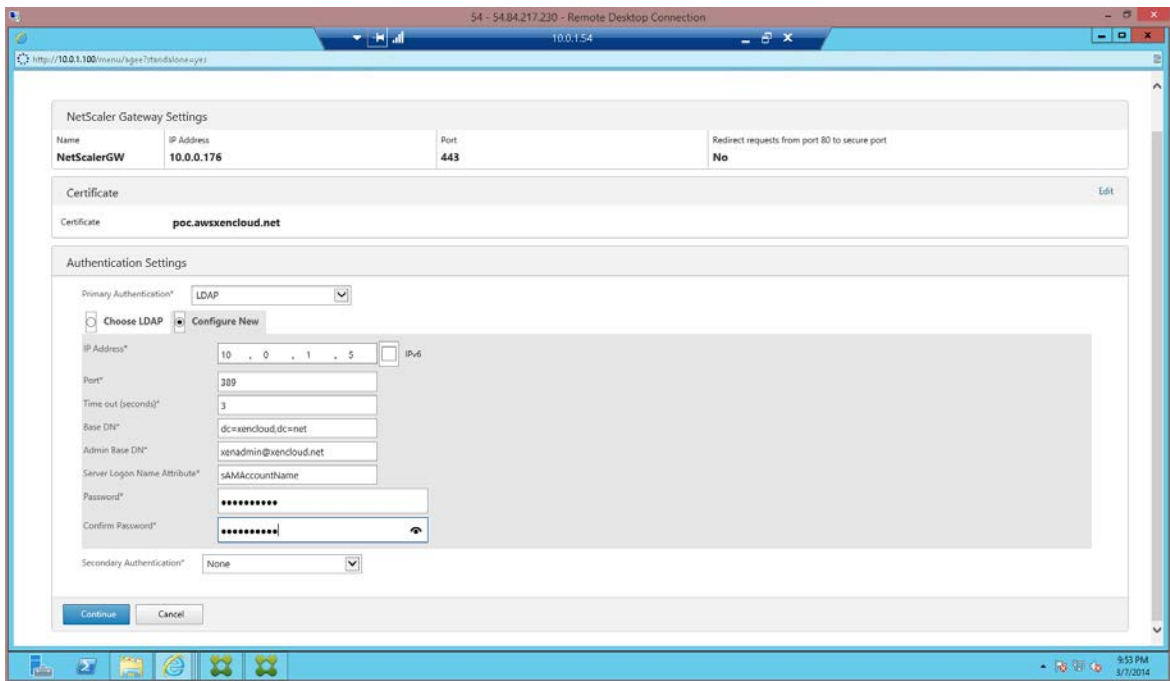
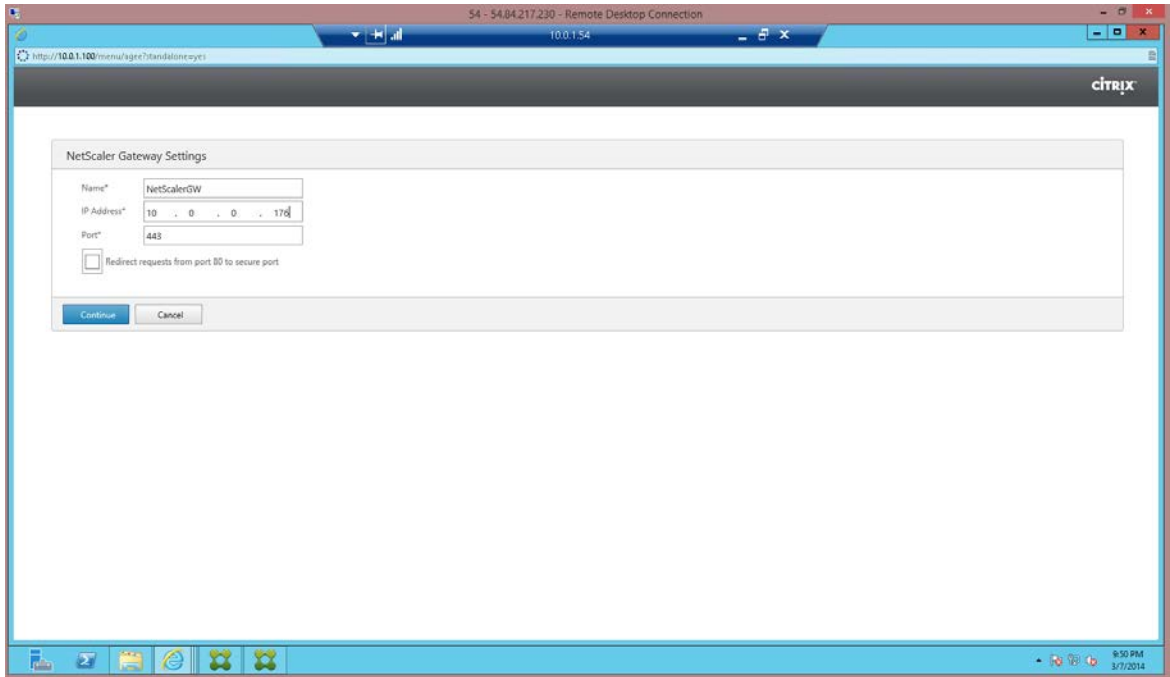


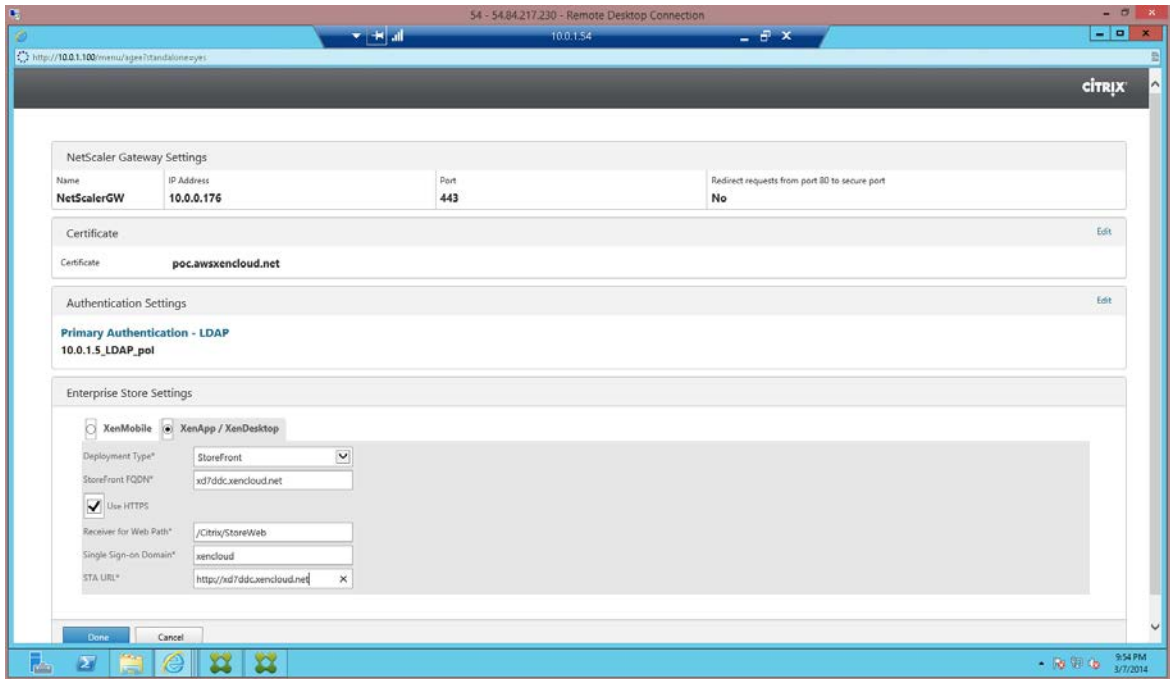
## Configure NetScaler Gateway using the Enterprise Store wizard

1. Launch the Enterprise Store wizard.

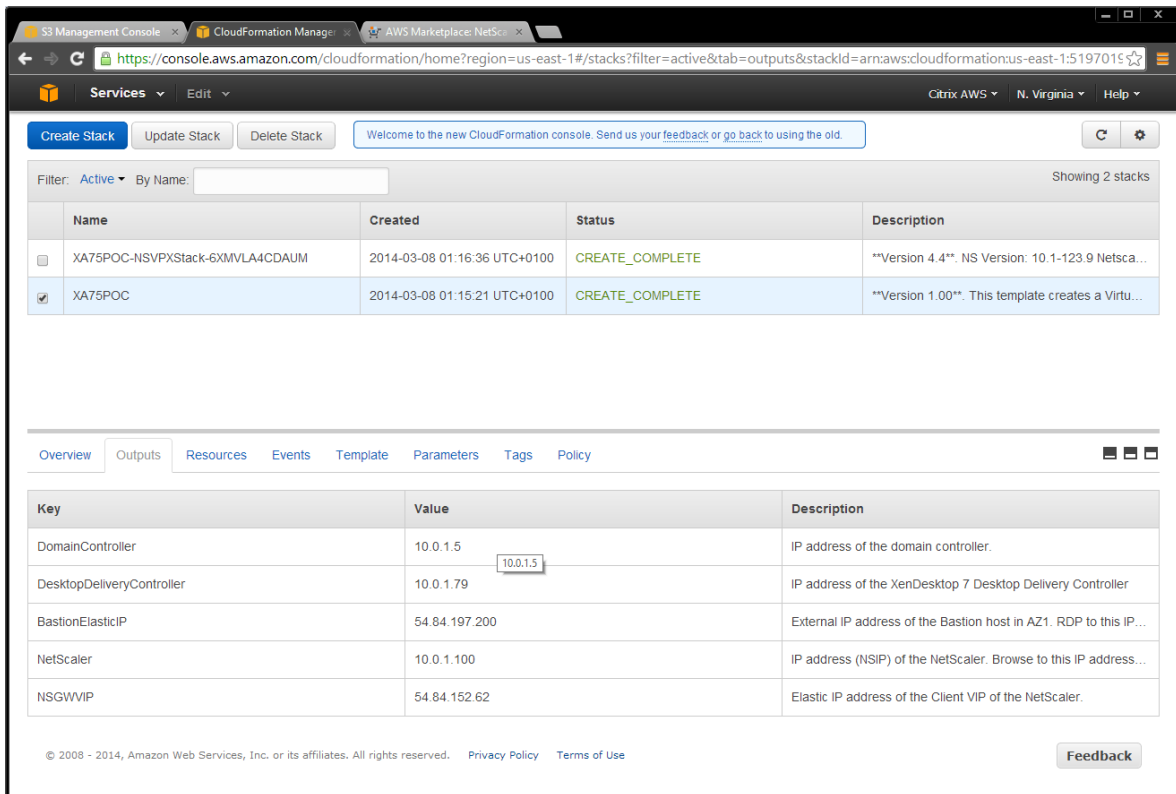


2. Ensure that the VIP used for the NetScaler Gateway virtual server is set to **10.0.0.176**. The CloudFormation template configures this VIP to point to an elastic IP address.

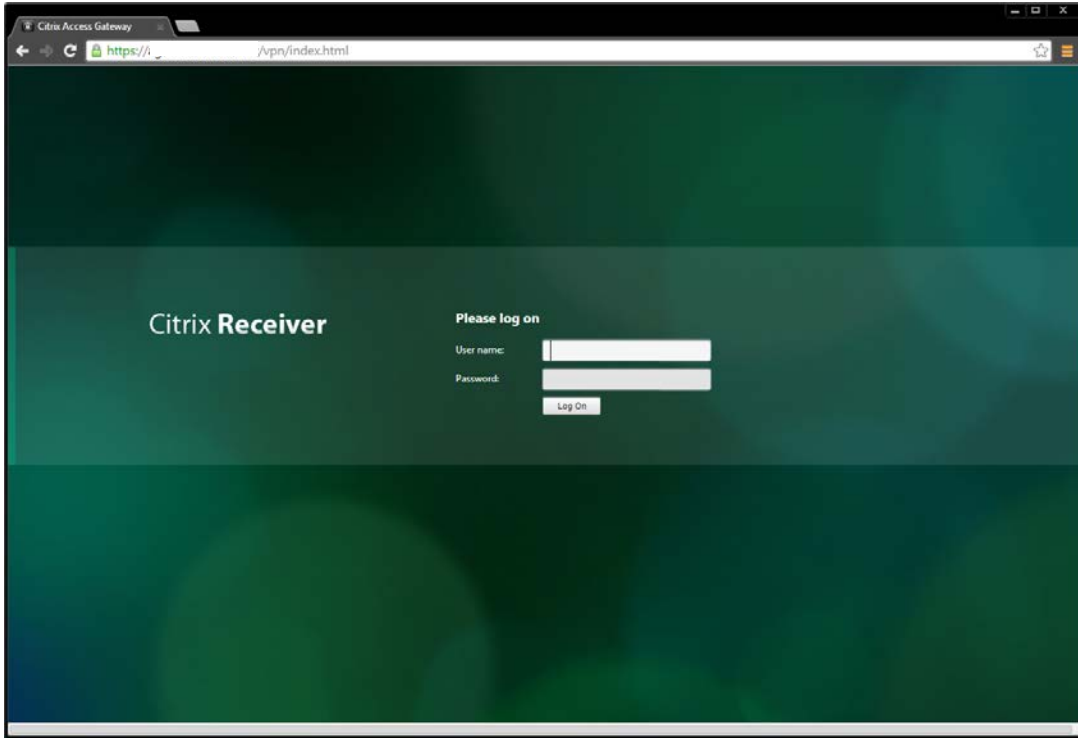


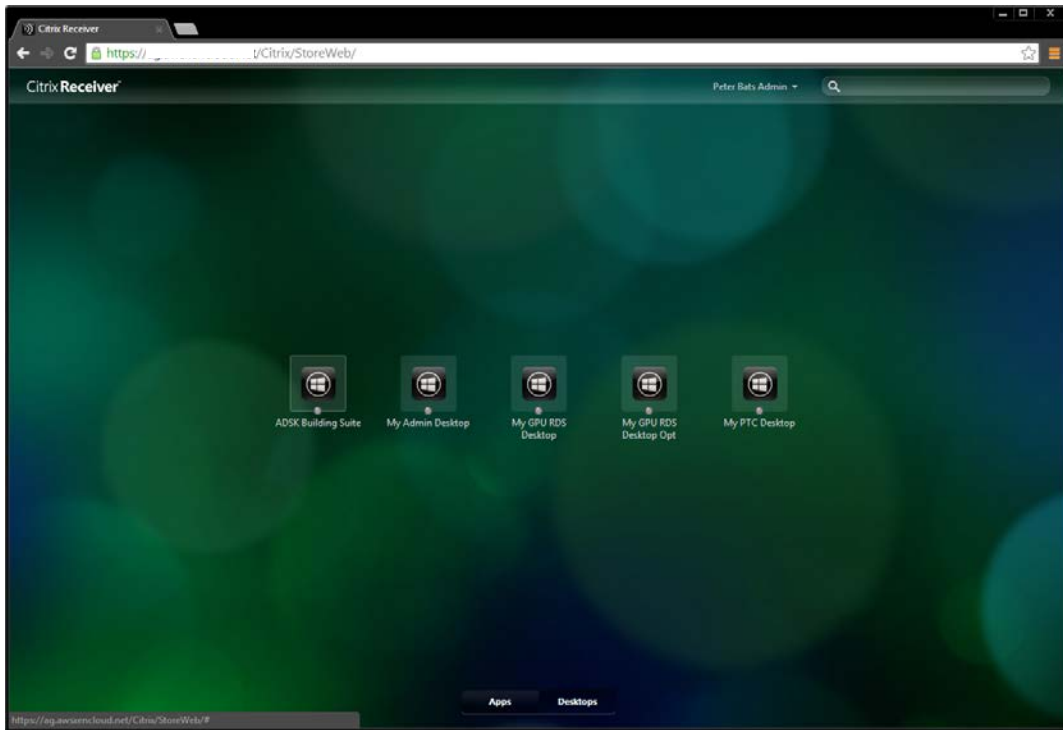


- Look up the elastic IP address for your VIP using the EC2 console. The CloudFormation output section shows the EIP associated with the VIP (NSGWVIP).



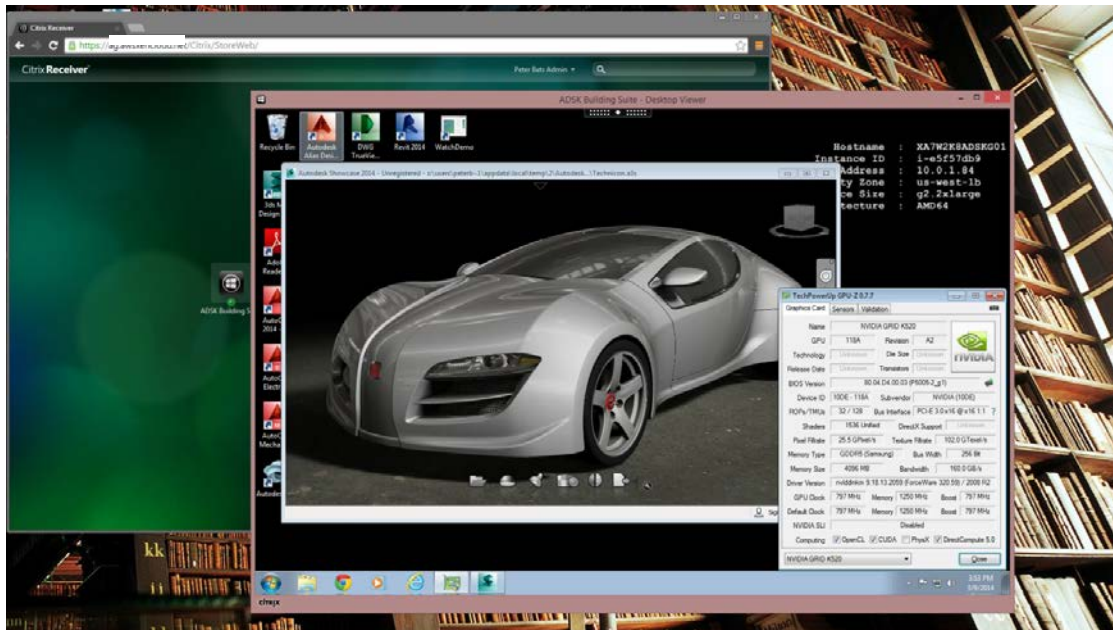
4. Complete the XenApp or XenDesktop configuration:
  - Place a certificate on your NetScaler Gateway, and assign this in DNS. Alternatively, place an entry in your hosts file to the elastic IP address.
  - Create a Delivery Group from your XenApp or XenDesktop machines and publish your applications and desktops.



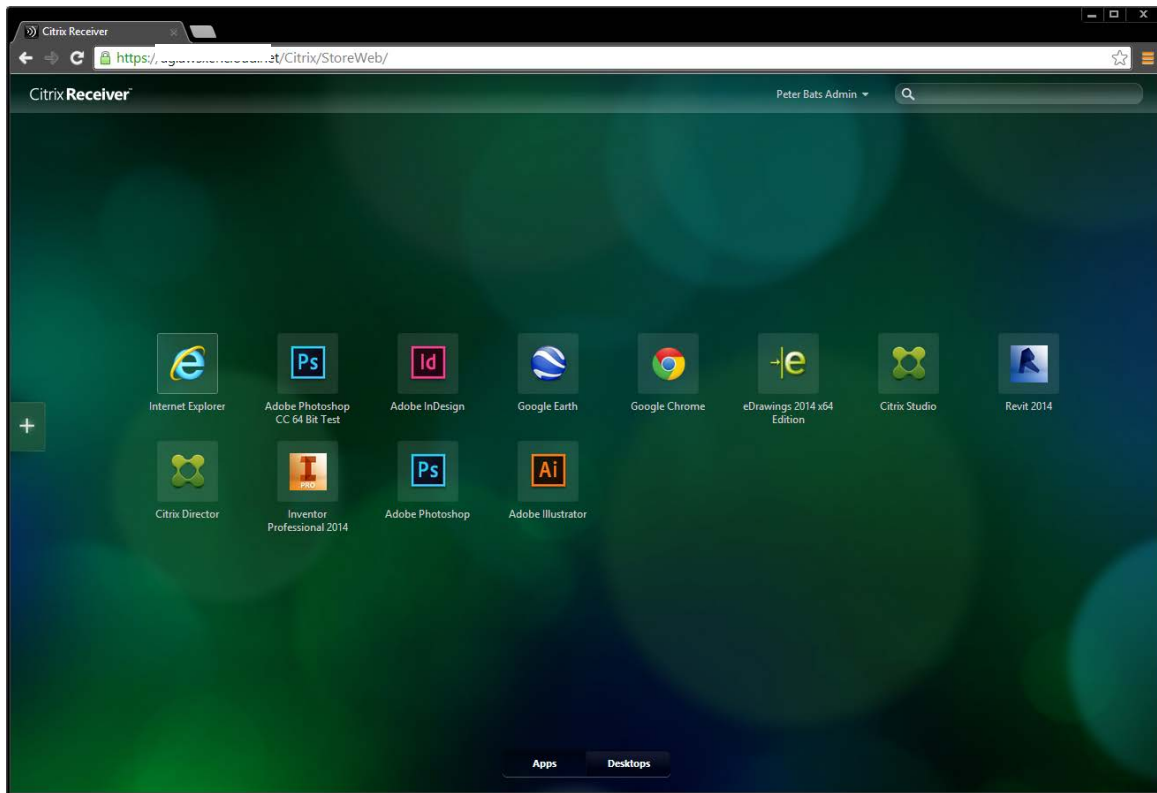


## Examples

The following example shows a desktop launched using an AWS g2.2xlarge instance (template), which allows for HDX 3D Pro support:



The following example shows applications available in Receiver:



The following example shows launched applications:



## Create template AMIs from other templates

You can create template AMIs by launching an instance from a virtual machine (VM) that you imported from Citrix XenServer, Microsoft Hyper-V, VMware Workstation, or VMware vSphere. You create the template AMI by:

- Exporting your existing Windows images or template from your on-premises virtualization environment using the environment's virtualization tools.
- Importing the image or template to Amazon EC2 using the Amazon EC2 command line or API tools.

See the [Importing EC2 Instances](#) in the [AWS EC2 User guide](#) for detailed instructions on importing existing VMs.

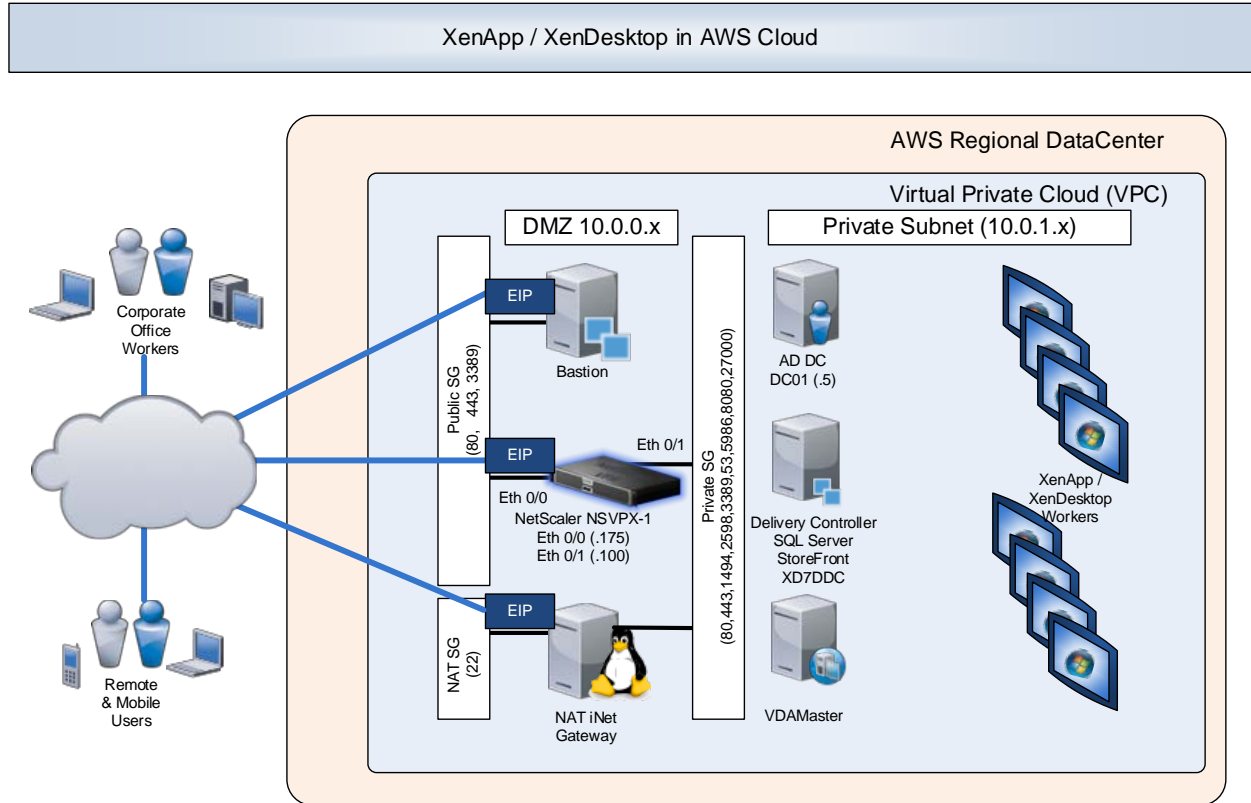
Once you import your template, and create an instance from it as described in [Importing EC2 Instances](#), you can turn it in to an AMI as with any other instance.

# Appendix

## Manually deploy XenApp and XenDesktop in AWS

An alternative to using an [AWS CloudFormation template](#), you can deploy XenApp and XenDesktop on AWS using manual procedures, as shown in the following example.

Site infrastructure using the manual deployment





## Security and firewall mappings

This section lists network specifics used in this manual set up example.

### NAT Security Group

Inbound				Outbound		
Type	Traffic	Source		Type	Traffic	Source
All	All	privateSG		All	All	0.0.0.0/0
TCP	22 (SSH)	0.0.0.0/0				

### Public Network Security Group (publicSG) rules

Inbound				Outbound		
Type	Traffic	Source		Type	Traffic	Source
All	All	publicSG		All	All	0.0.0.0/0
	All	publicSG			All	privateSG
ICMP	All	0.0.0.0/0		ICMP	All	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				

**Private Network Security Group (privateSG) rules**

Inbound				Outbound		
Type	Traffic	Source		Type	Traffic	Source
All	All	NATSG		All	All	0.0.0.0/0
	All	privateSG			All	privateSG
ICMP	All	publicSG		ICMP	All	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				

**Relevant AMIs for XenApp and XenDesktop Site in US-East-1**

Function	AMI Name	AMI ID	Network	IP Address
Domain Controller	Microsoft Windows Server 2012 Base	ami-814642e8	private	10.0.1.5
	Microsoft Windows Server 2008 R2 Base	ami-37b1b45e		
Delivery Controller	Microsoft Windows Server 2012 with SQL	ami-e743478e	private	10.0.1.15
	Microsoft Windows Server 2008 R2 with SQL	ami-a1b9bcc8		
NetScaler Gateway	NetScaler VPX Platinum Edition - 10 Mbps	ami-c995aaa0	Public	
			SNIP	10.0.0.175
			VIP	10.0.0.176
			Private	
			NSIP	10.0.1.100
SNIP	10.0.1.102			
Bastion	Microsoft Windows Server 2012 Base	ami-814642e8	public	DHCP
	Microsoft Windows Server 2008 R2 Base	ami-37b1b45e		
NAT	ami-vpc-nat-1.1.0-beta.x86-64-ebs	ami-f619c29f	public	DHCP
VDAMaster	Microsoft Windows Server 2012 Base	ami-814642e8	private	DHCP
	Microsoft Windows Server 2008 R2 Base	ami-37b1b45e		

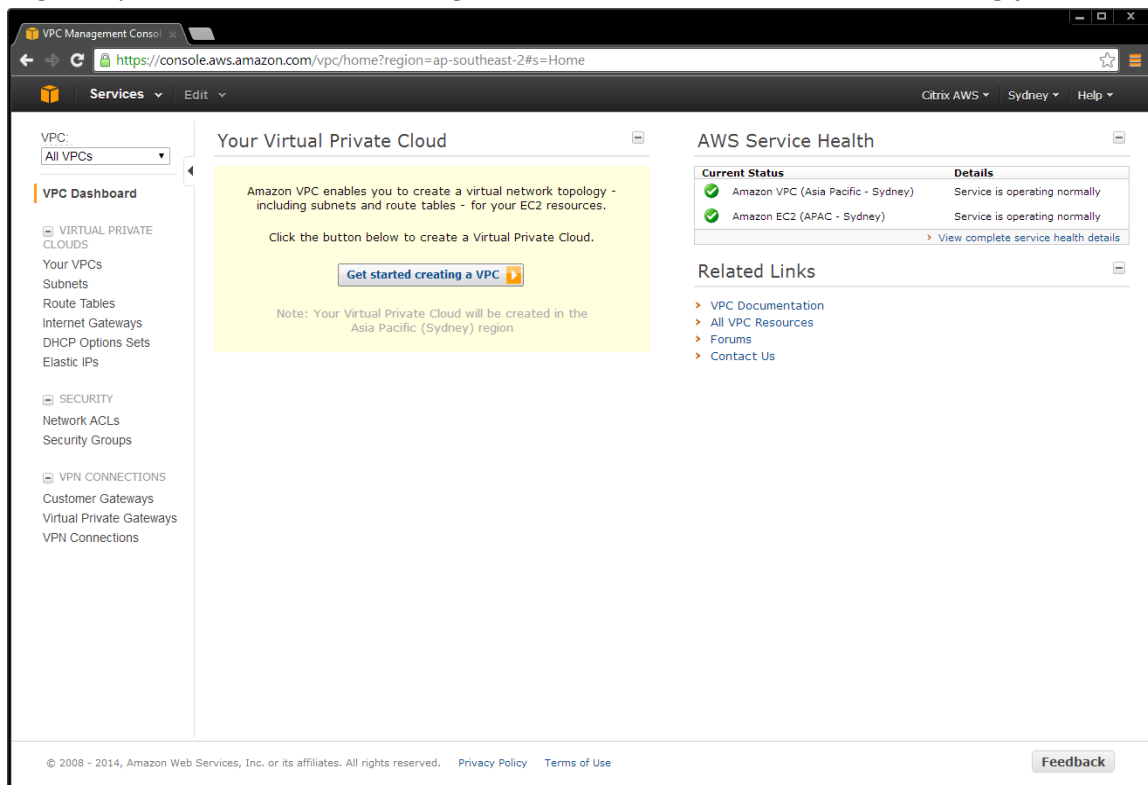
**Note:** The Amazon VPC wizard automatically creates the NAT server. Therefore, you do not need to create the AMI.

# Set up the VPC network

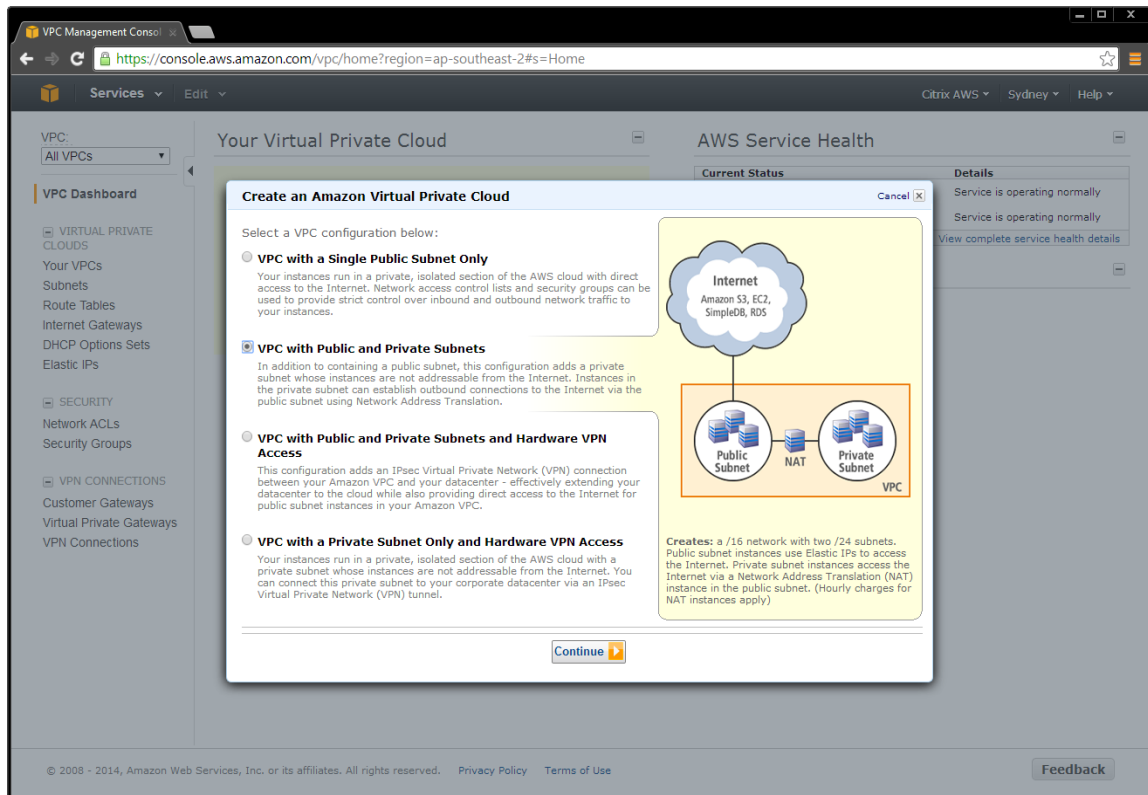
## Create the VPC network infrastructure

Creating a Site involves creating the Virtual Private Cloud (VPC) network infrastructure in your Amazon Web Services account.

1. Log in to your AWS account, and navigate to the VPC tab. Click **Get Started Creating your VPC**.



## 2. Select VPC with Public and Private Subnets.



## 3. To create a hybrid setup between your on premise environment:

- a. Select **VPC with Public and Private Subnets and Hardware VPN**.
- b. Alternatively, deploy the CloudBridge on your NetScaler, which creates the VPN for you.

This sample deployment uses the default network settings. Adjust them accordingly.

**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](#)

---

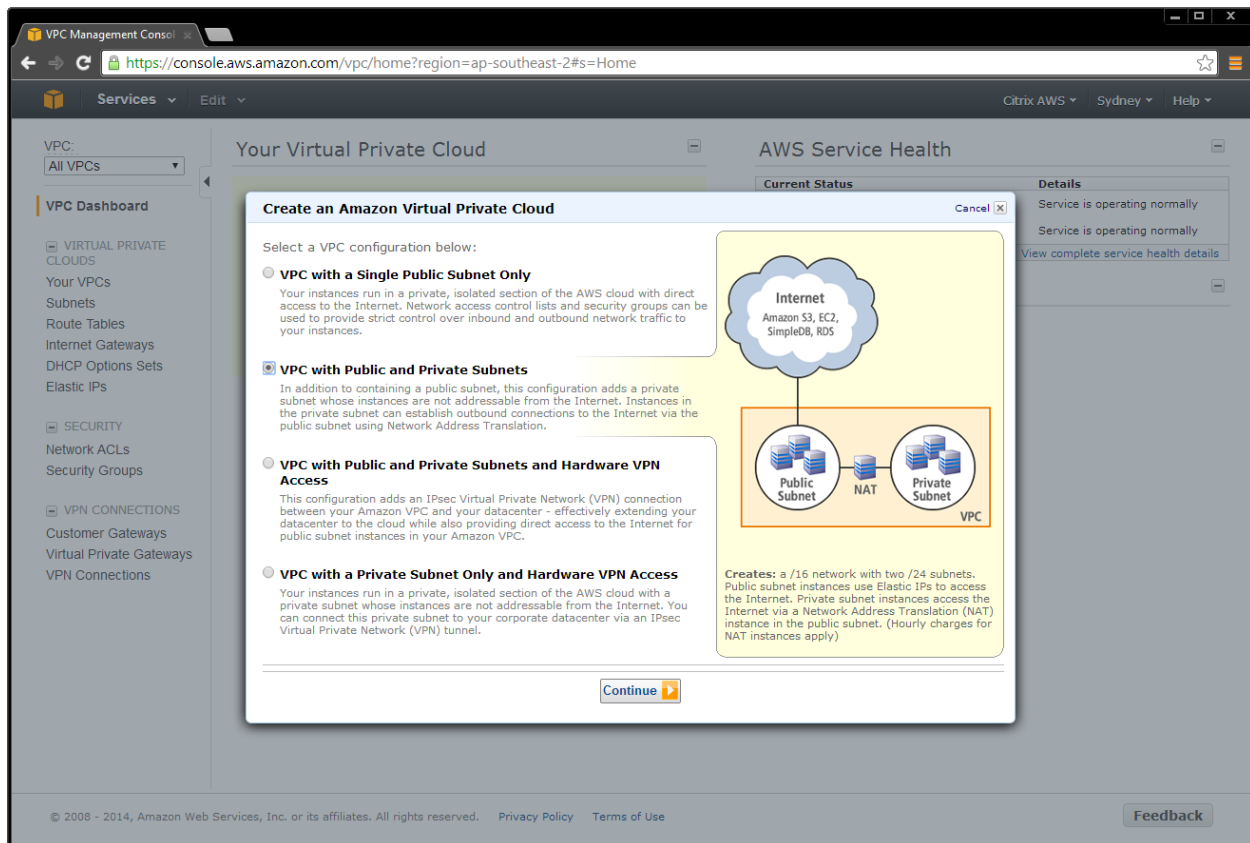
[Back](#)

**Create 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.



When the VPC is automatically created, it includes the public and private subnets, the router, NAT gateway, and the Internet gateway.

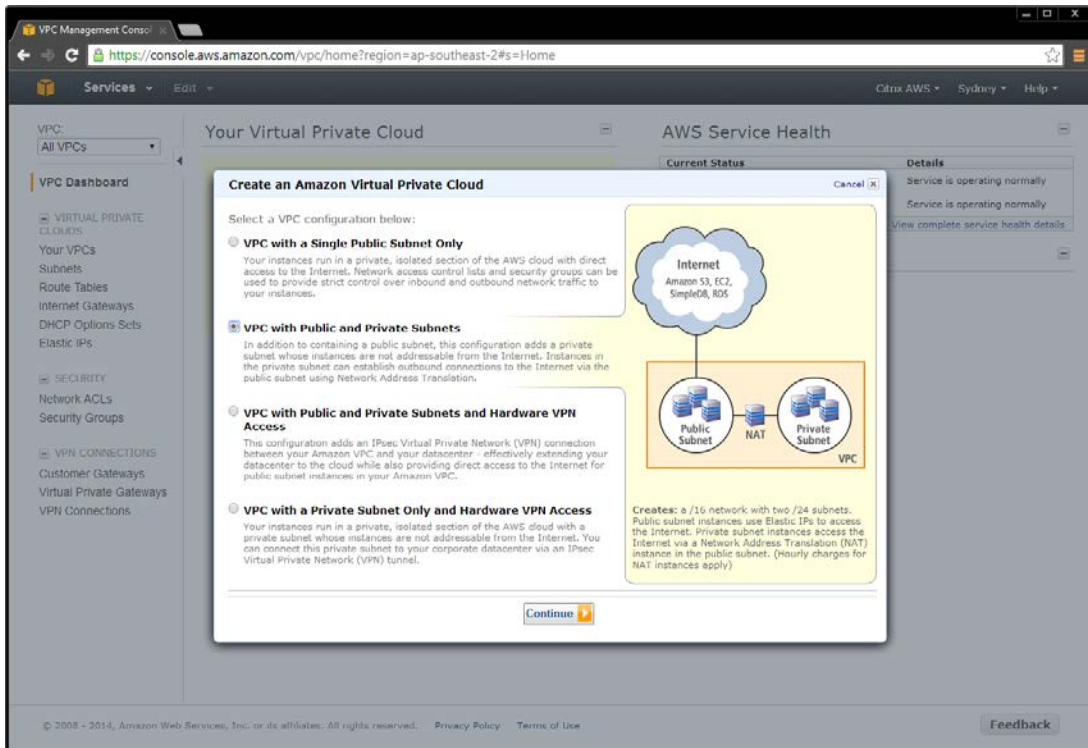
## Add security groups

The security groups in Amazon VPC provide communication between the Internet and public network, and the public and private network. The security groups contain ACLs and are the basis of the firewalls shown in the [network diagram](#).

You must create the following security groups.

### Add NAT Security Group

1. On the VPC tab, select **Security Groups > Create Security Group**.





The screenshot displays the AWS VPC Management Console interface. A modal dialog titled "Create Security Group" is open in the center, with the following fields:

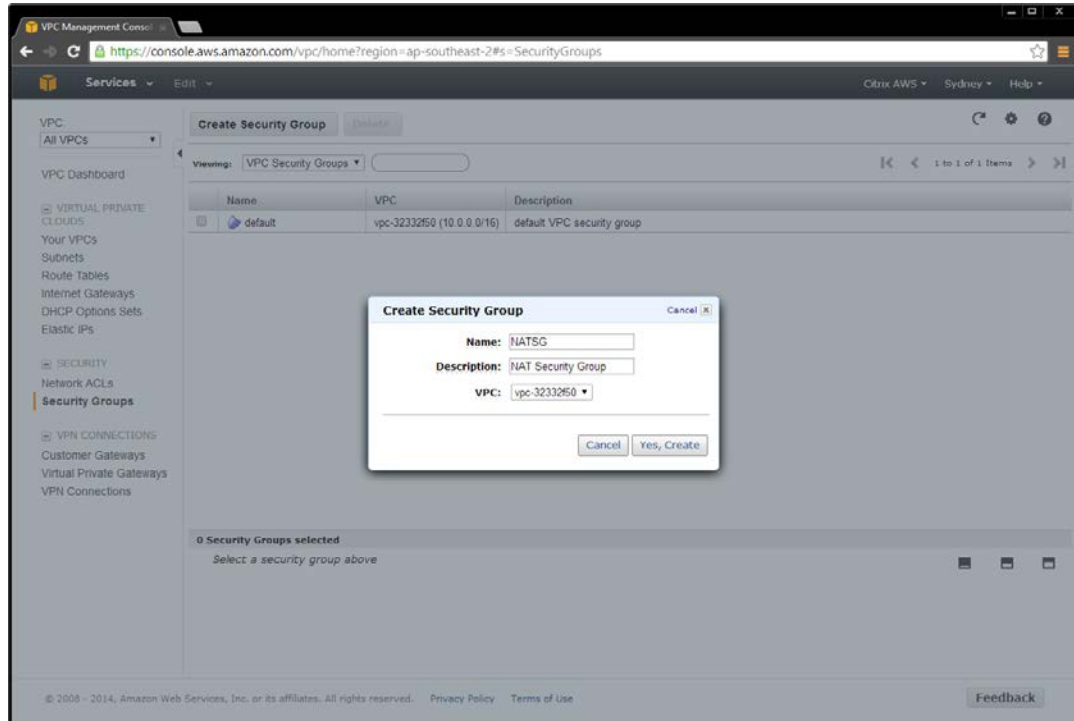
- Name:** NATSG
- Description:** NAT Security Group
- VPC:** vpc-32332f50

Buttons for "Cancel" and "Yes, Create" are visible at the bottom of the dialog. In the background, a table lists existing security groups:

Name	VPC	Description
default	vpc-32332f50 (10.0.0.0/16)	default VPC security group

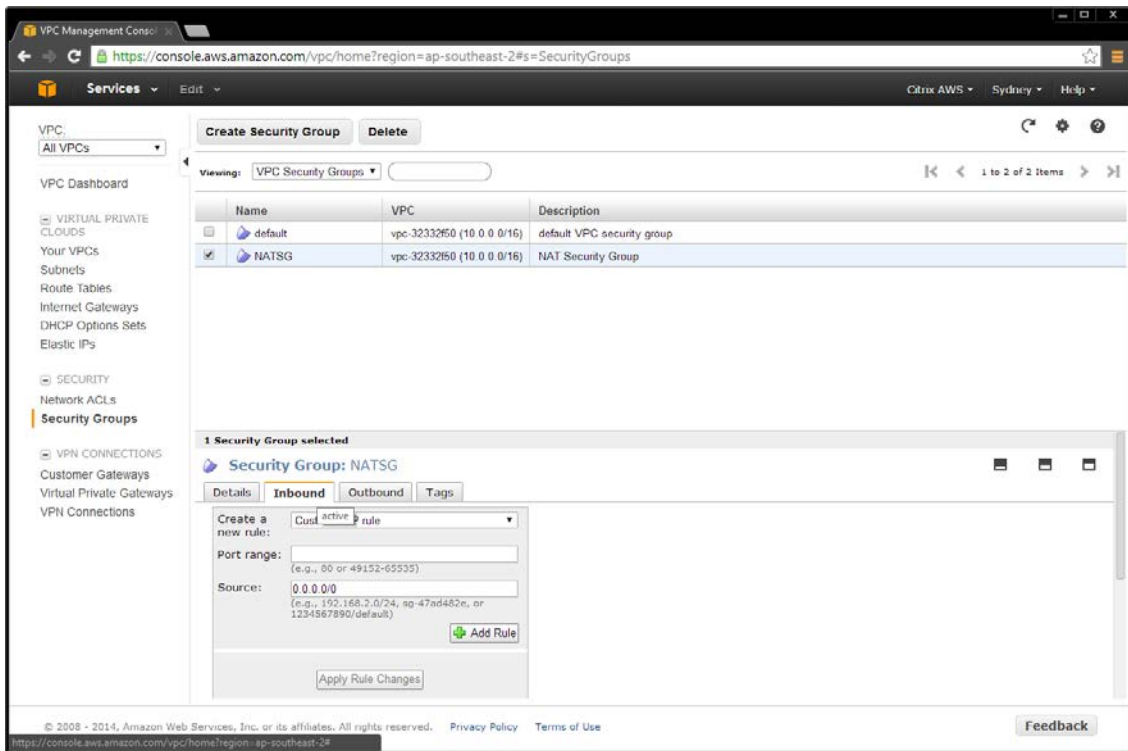
The console footer includes the text: © 2008 - 2014, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use and a Feedback button.

2. Add ACL rules for inbound and outbound traffic. Select:
  - a. Create a new rule
  - b. Port number
  - c. Source IP address



**Note:** A source IP address of 0.0.0.0/0 indicates that you want to allow all inbound or outbound traffic.

3. Create ACL rules to match the inbound and outbound traffic table.



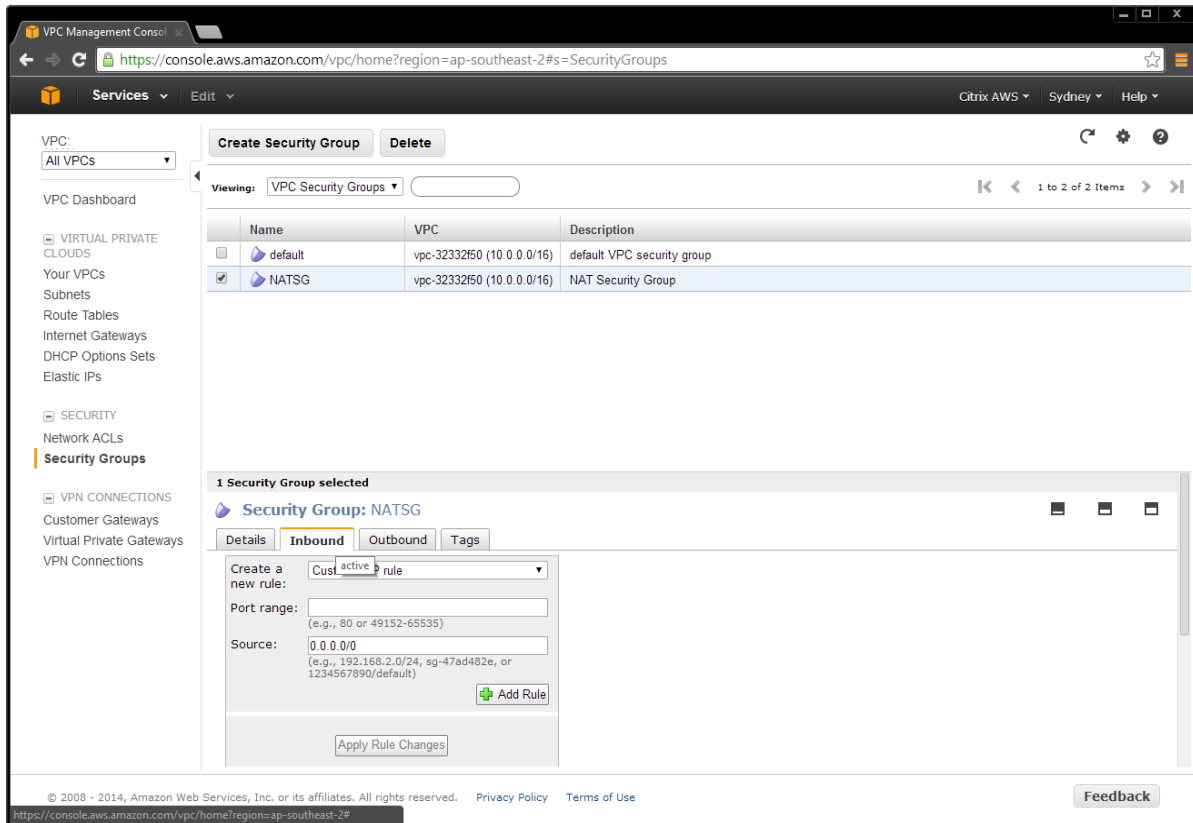
## NAT Security Group rules

Inbound			Outbound		
Type	Traffic	Source	Type	Traffic	Source
All	All	privateSG	All	All	0.0.0.0/0
TCP	22 (SSH)	0.0.0.0/0			

## NAT instance

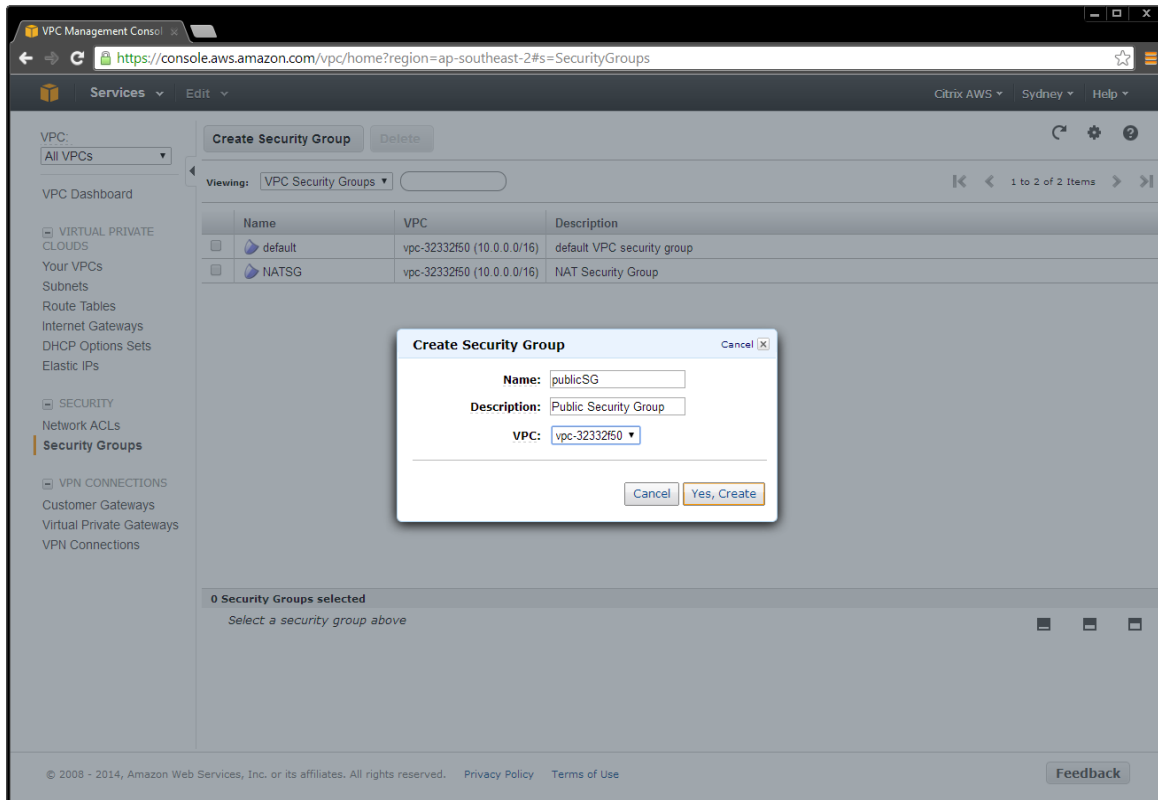
The VPC Wizard creates the NAT instance.

Go to the EC2/Instances page, and locate the instance. Right-click the instance, and change the security group to **NATSG**.



## Add public security group

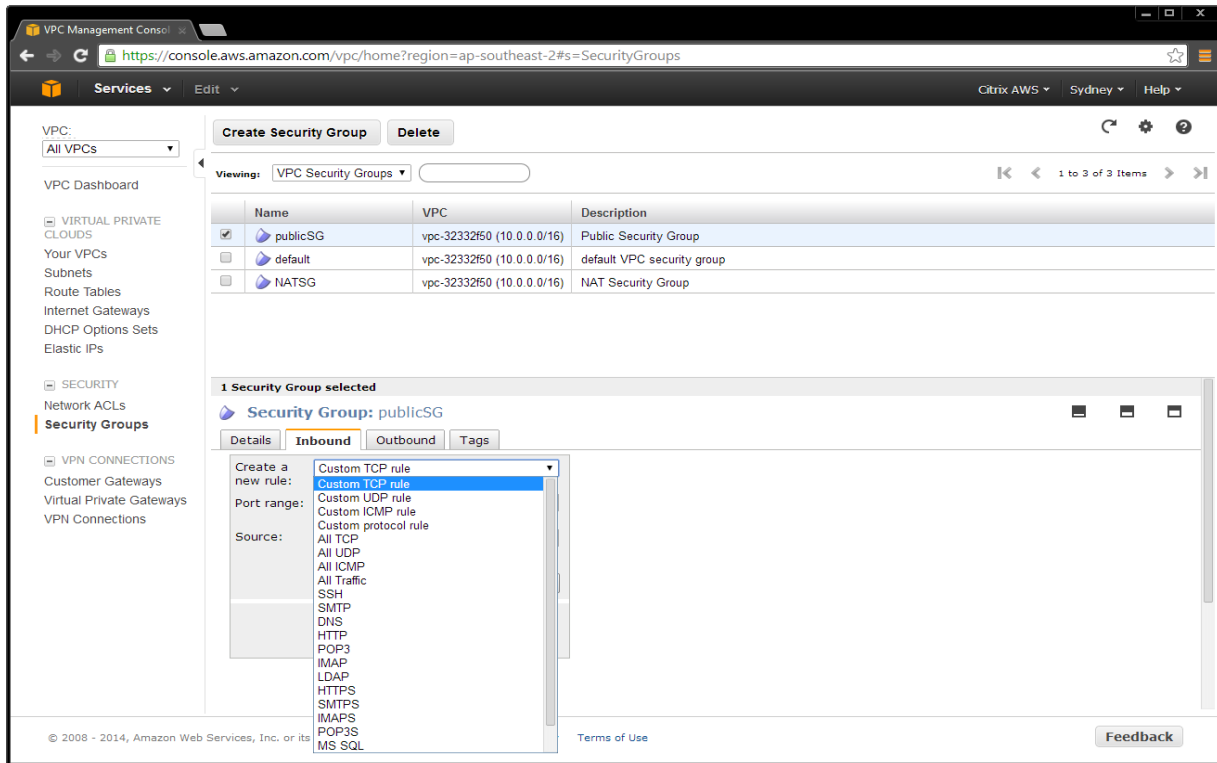
1. On the VPC tab, select **Security Groups > Create Security Group**.



2. Add ACL rules for inbound and outbound traffic. Select:
  - a. Create a new rule
  - b. Port number
  - c. Source IP address

**Note:** Entering a Source IP address of **0.0.0.0/0** allows all inbound or outbound traffic.

3. Create ACL rules to match the **Public Network Security Group (publicSG)** rules table.

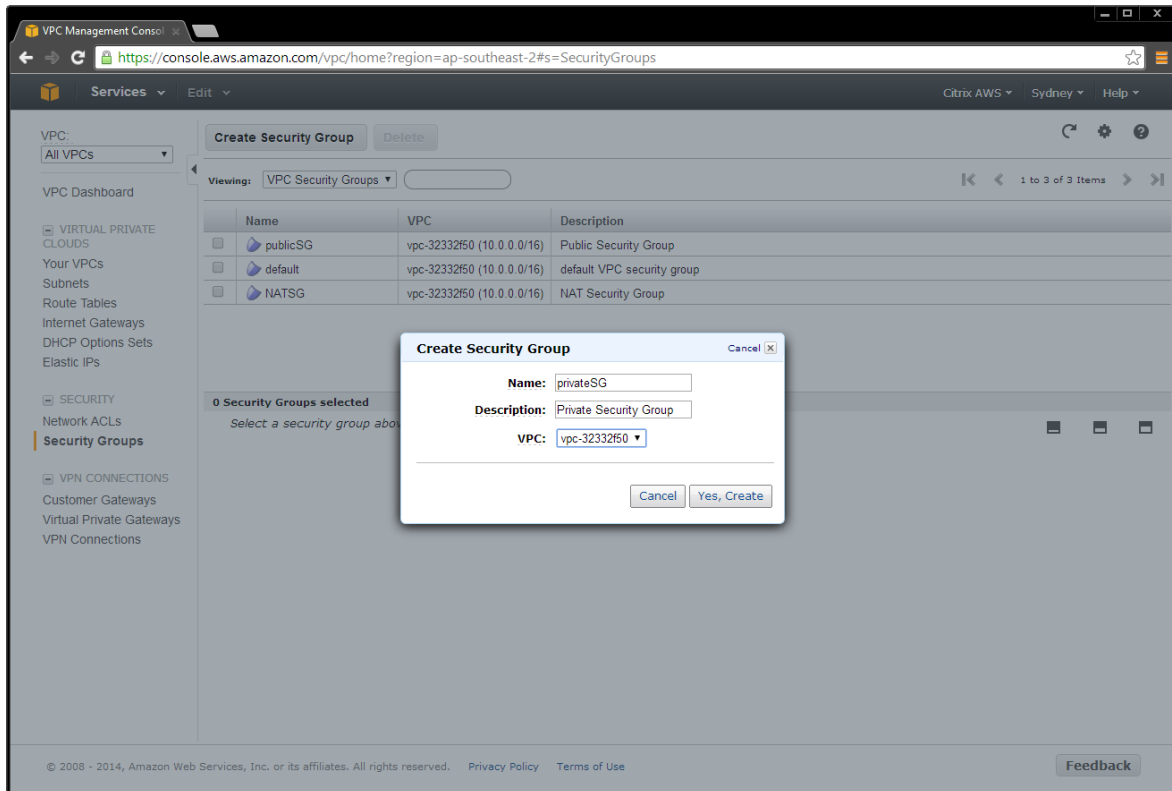


Public Network Security Group (publicSG) rules

Inbound			Outbound		
Type	Traffic	Source	Type	Traffic	Source
All	All	publicSG	All	All	0.0.0.0/0
	All	publicSG		All	privateSG
ICMP	All	0.0.0.0/0	ICMP	All	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			

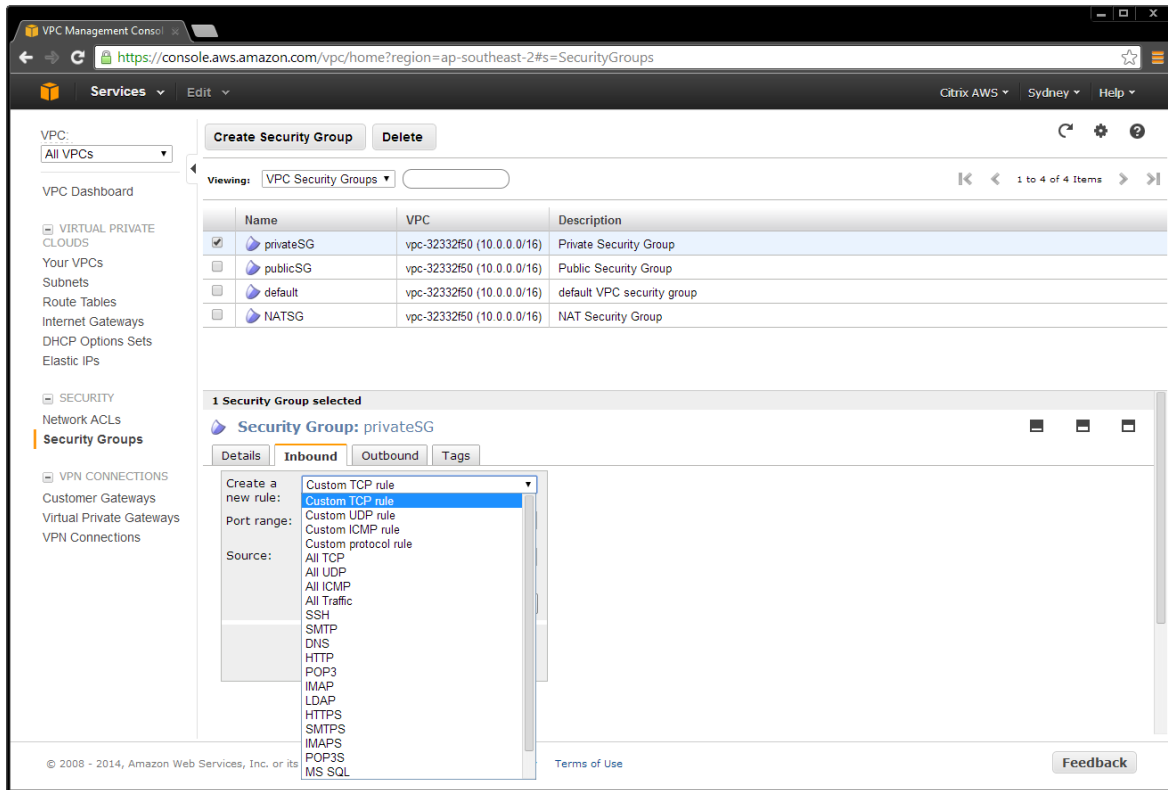
## Add Private Security Group

1. On the VPC tab, select **Security Groups > Create Security Group**.



4. Add ACL rules for inbound and outbound traffic. Select:
  - a. Create a new rule
  - b. Port number
  - c. Source IP address

**Note:** Entering a Source IP address of 0.0.0.0/0 allows all inbound or outbound traffic. Create ACL rules to match the table.





## Private Network Security Group (privateSG) rules

Inbound				Outbound		
Type	Traffic	Source		Type	Traffic	Source
All	All	NATSG		All	All	0.0.0.0/0
	All	privateSG			All	privateSG
ICMP	All	publicSG		ICMP	All	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				

## DHCP options

### Create a DHCP options set

There is a domain controller running DNS in the private network. The controller enables Citrix servers to authenticate and communicate with each other. To implement this communication:

- Create a new DHCP options set that contains your DNS server IP address.
- Add an open-source DNS server on the Internet in case a server needs to access the Internet.

## DHCP Options Set

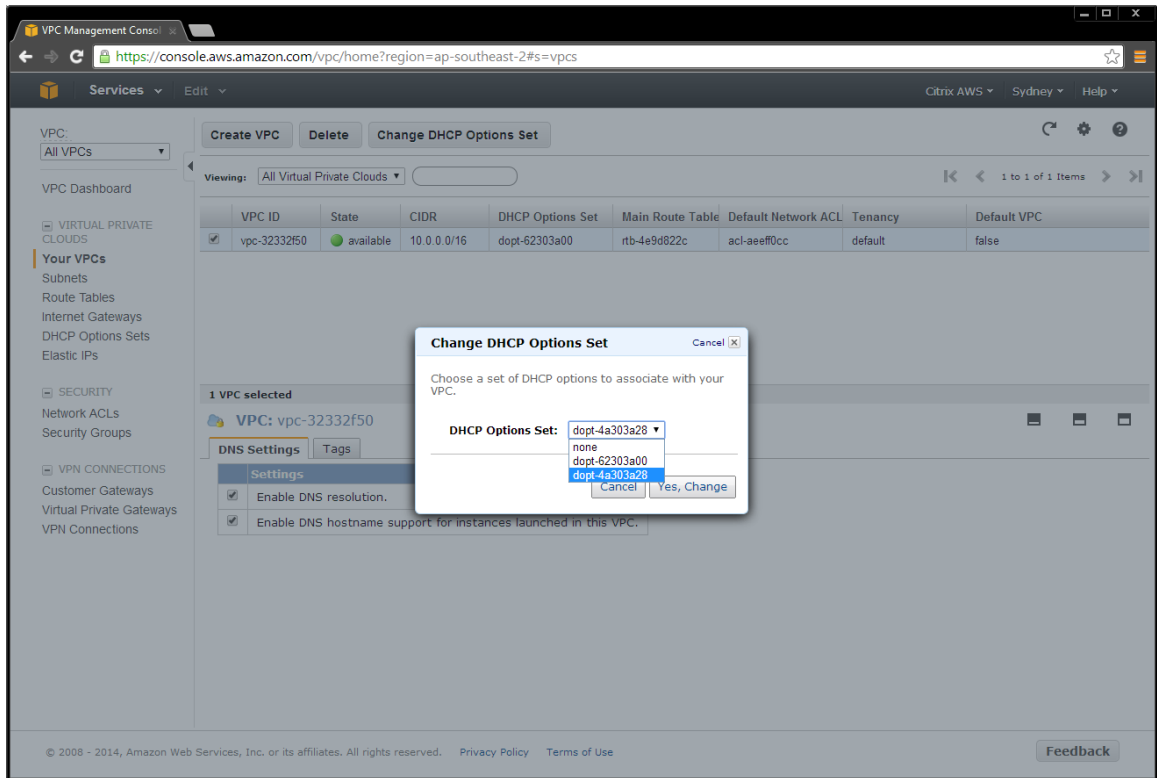
1. Navigate to the VPC tab, and select **DHCP Options Set** > **Create DHCP Options Set**.

The screenshot shows the AWS VPC Management Console interface. The main content area displays a table of DHCP Options Sets with one entry: ID 'dopt-62303a00' and options 'domain-name = ap-southeast-2.compute.internal, domain-name-servers = AmazonProvidedDNS;'. A modal dialog box titled 'Create DHCP Options Set' is open, providing instructions and input fields for the following parameters:

- domain-name**: Enter the domain name that should be used for your hosts, for example, mybusiness.com. Input: `xencloud.net`
- domain-name-servers**: Enter up to 4 DNS server IP addresses, separated by commas, for example, 172.16.16.16, 10.10.10.10. Input: `10.0.1.5, AmazonProvidedDNS`
- ntp-servers**: Enter up to 4 NTP server IP addresses, separated by commas. Input: (empty)
- netbios-name-servers**: Enter up to 4 NetBIOS server IP addresses, separated by commas. Input: `10.0.1.5`
- netbios-node-type**: Enter the NetBIOS node type, for example, 2. Input: `2`

The dialog box includes 'Cancel' and 'Yes, Create' buttons. The footer of the console shows copyright information for Amazon Web Services, Inc. and a 'Feedback' button.

2. Select the VPC, right-click on your selection, and choose **Change DHCP Options Set to the new set**.



## Set up the XenApp or XenDesktop infrastructure instances

### Launch and configure a domain controller AMI

Create a domain controller for the Site as follows.

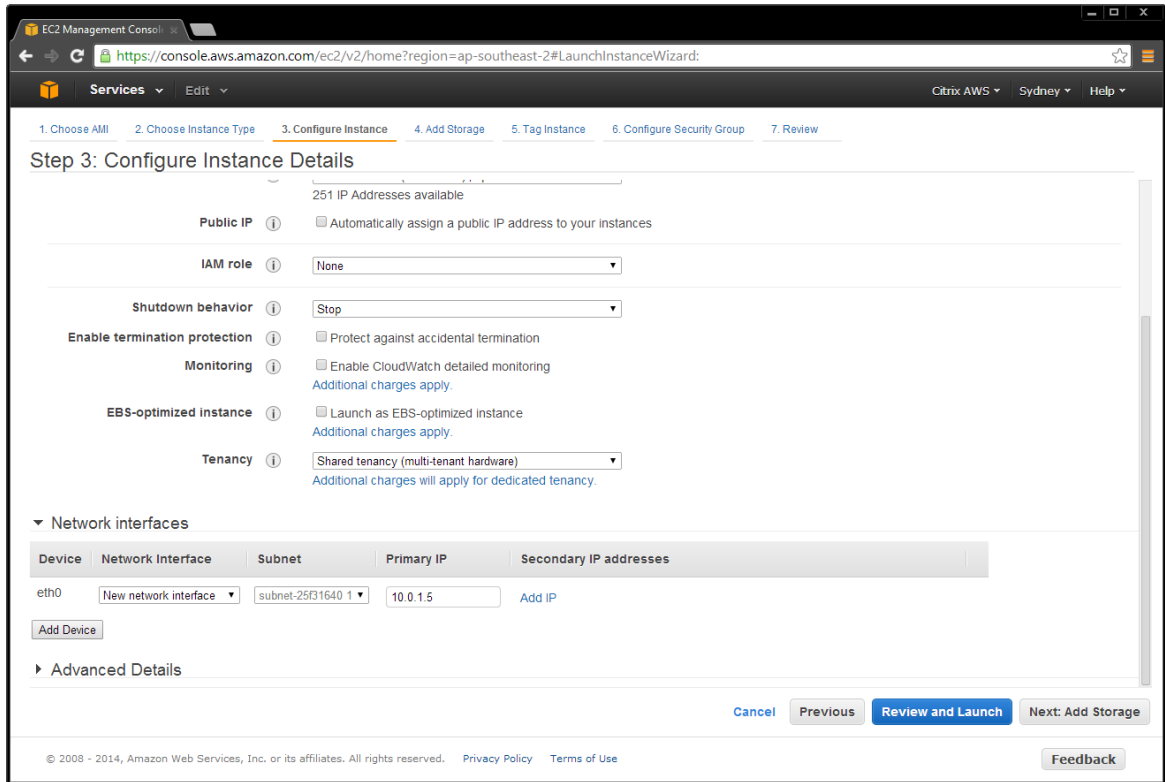
1. Select **AMIs** in the EC2 tab.
2. Depending on operating system you use, perform a search in the Amazon AMIs for **Windows Server 2012 Base** or **Windows Server 2008 R Base**. Ensure that the machine is deployed to your subnet, and make sure it is in the private subnet **10.0.1.0/24**.

The screenshot shows the AWS Management Console interface for configuring an EC2 instance. The page is titled "Step 3: Configure Instance Details" and includes a progress bar with steps: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance (active), 4. Add Storage, 5. Tag Instance, 6. Configure Security Group, and 7. Review. The main content area contains several configuration sections:

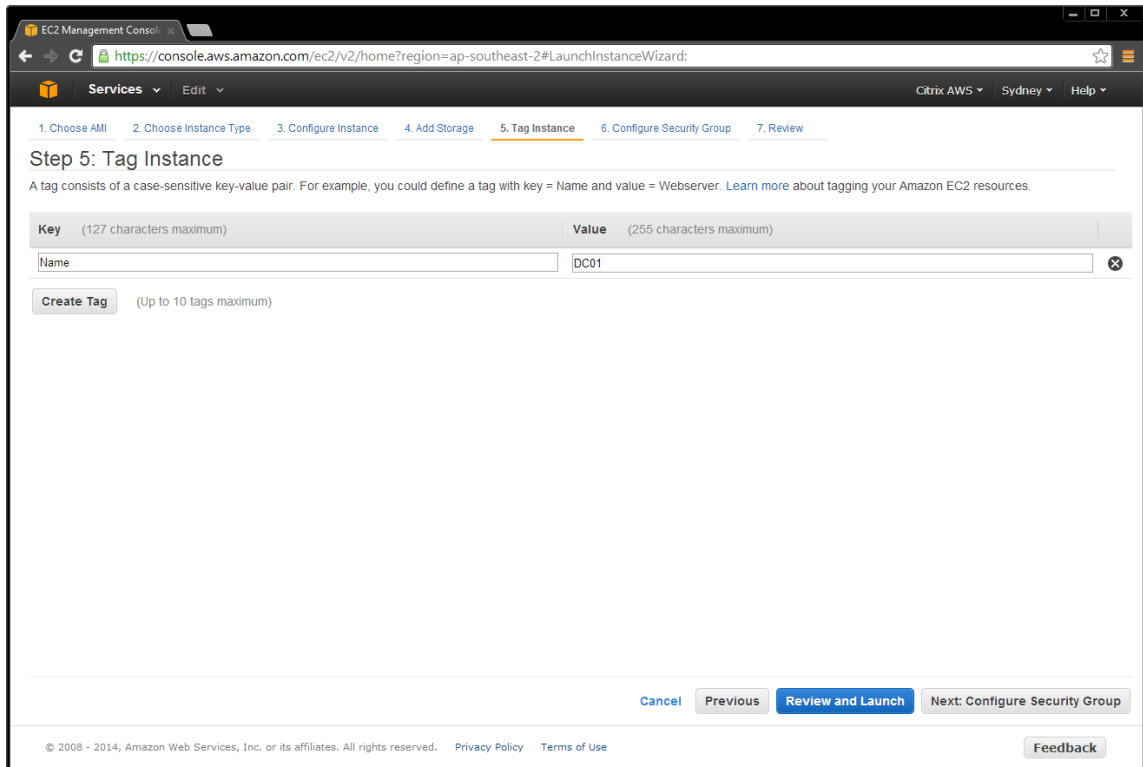
- Number of instances:** A text input field containing the value "1".
- Purchasing option:** A checkbox labeled "Request Spot Instances" which is currently unchecked.
- Network:** A dropdown menu showing "vpc-32332f50 (10.0.0.0/16)" with a "Create new VPC" link.
- Subnet:** A dropdown menu showing "subnet-25f31640(10.0.1.0/24) | ap-southeast-2a" with a "Create new subnet" link. Below the dropdown, it states "251 IP Addresses available".
- Public IP:** A checkbox labeled "Automatically assign a public IP address to your instances" which is unchecked.
- IAM role:** A dropdown menu showing "None".
- Shutdown behavior:** A dropdown menu showing "Stop".
- Enable termination protection:** A checkbox labeled "Protect against accidental termination" which is unchecked.
- Monitoring:** A checkbox labeled "Enable CloudWatch detailed monitoring" which is unchecked. Below it, it says "Additional charges apply."
- EBS-optimized instance:** A checkbox labeled "Launch as EBS-optimized instance" which is unchecked. Below it, it says "Additional charges apply."
- Tenancy:** A dropdown menu showing "Shared tenancy (multi-tenant hardware)". Below it, it says "Additional charges will apply for dedicated tenancy."

At the bottom of the form, there are navigation buttons: "Cancel", "Previous", "Review and Launch" (highlighted in blue), and "Next: Add Storage". A "Feedback" button is located at the bottom right. The footer contains copyright information: "© 2008 - 2014, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use".

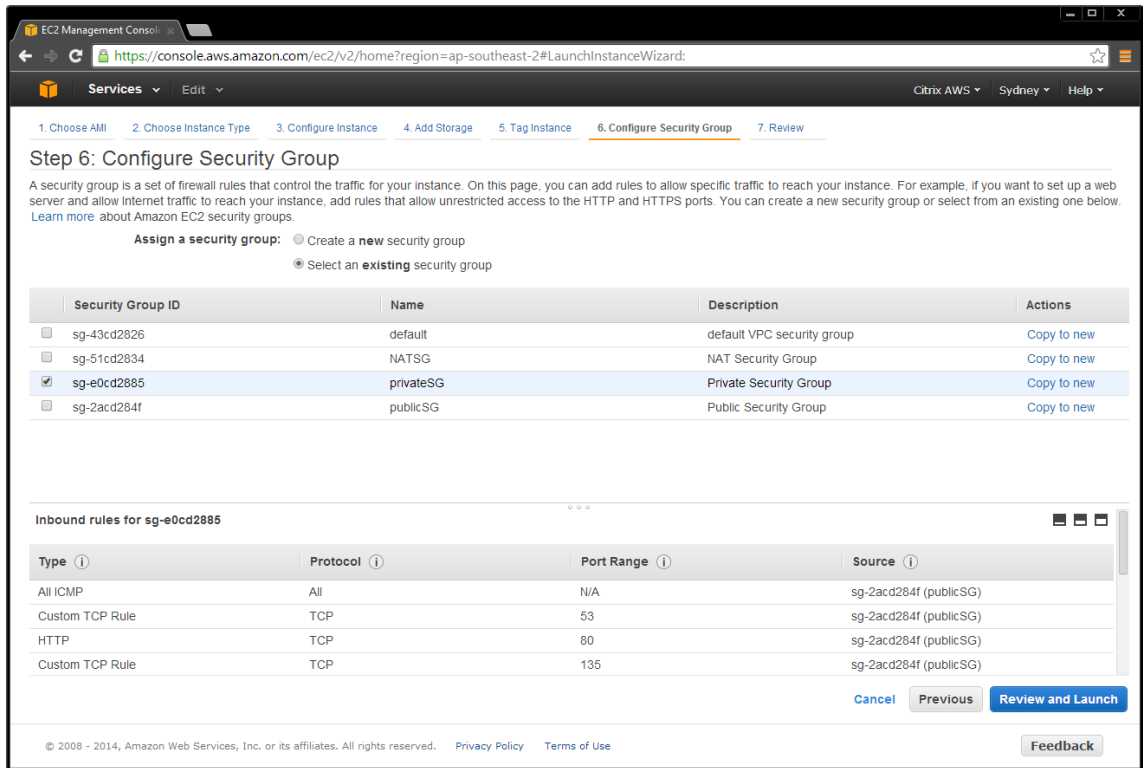
3. Assign the IP address for this server.



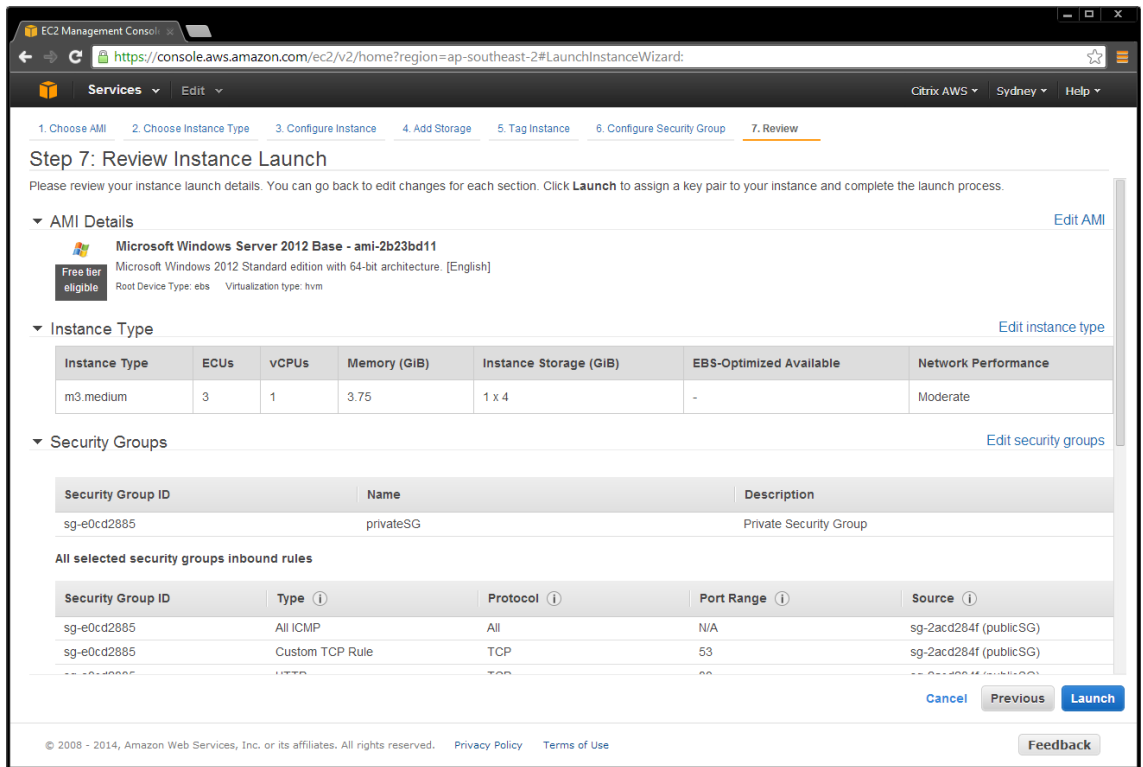
4. Assign a friendly name to the AMI to make it easily identifiable in the Amazon console.



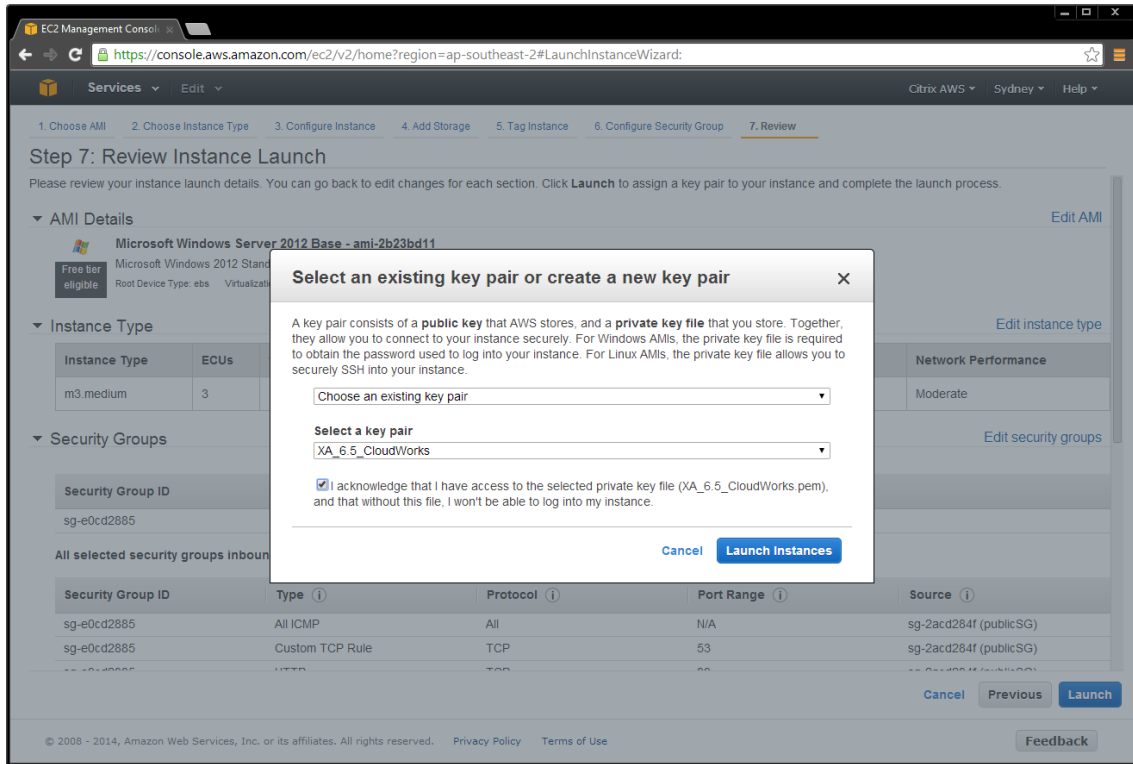
- Place the domain controller in the network by launching the AMI into the appropriate network and security group. This example places the domain controller in the private network.



- Review the settings, and then select **Launch**.



7. Choose an existing AWS keypair, or create a new one.



## Launch remaining XenApp or XenDesktop AMIs

Launch the remaining XenApp or XenDesktop AMIs using the parameters in the following table. Ensure that you launch them into the correct network (private or public as applicable), and assign an IP address and the elastic IP addresses.

**Note:** The Amazon VPC wizard automatically creates the NAT server, so you should not need this AMI.

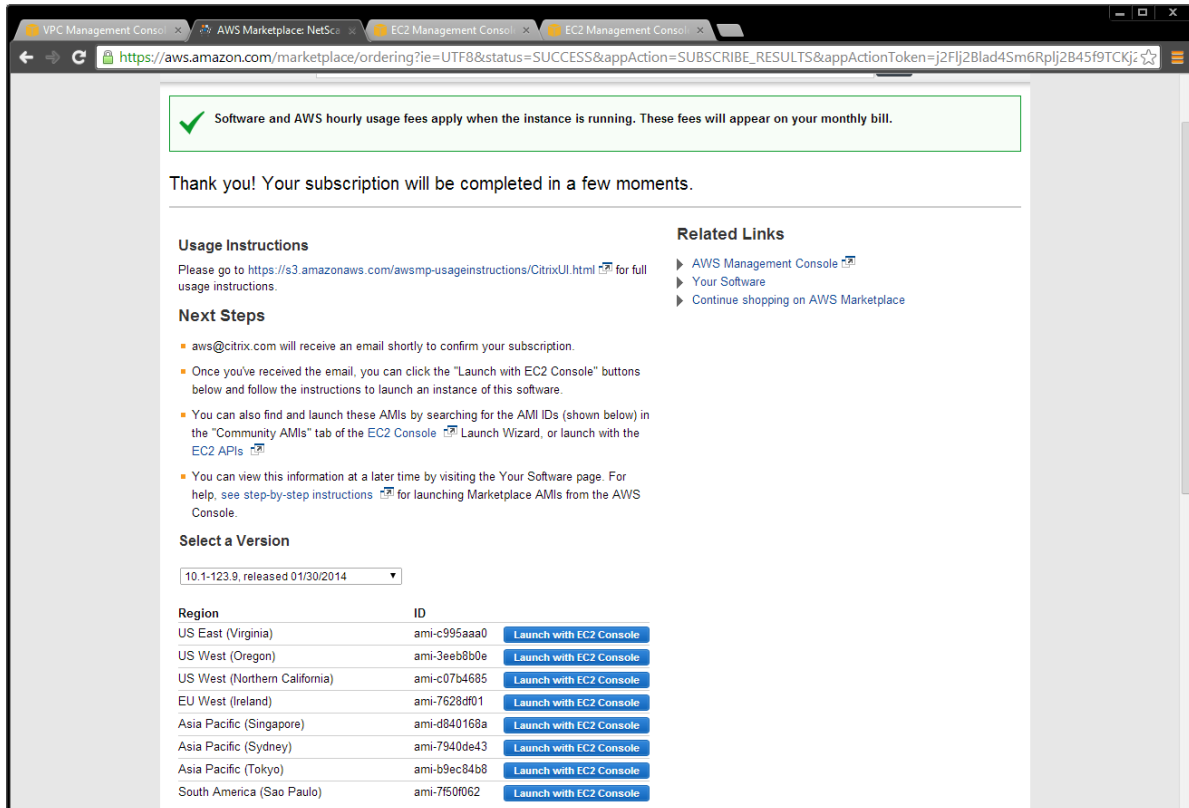
Function	AMI Name	AMI ID	Network	IP Address
Domain Controller	Microsoft Windows Server 2012 Base	ami-814642e8	private	10.0.1.5
	Microsoft Windows Server 2008 R2 Base	ami-37b1b45e	private	10.0.1.5
Delivery Controller	Microsoft Windows Server 2012 with SQL	ami-e743478e	private	DHCP
	Microsoft Windows Server 2008 R2 with SQL	ami-a1b9bcc8	private	DHCP
VDA Master	Microsoft Windows Server 2012 Base	ami-814642e8	private	DHCP
	Microsoft Windows Server 2008 R2 Base	ami-37b1b45e	private	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 Platinum Edition - 10 Mbps	ami-c995aaa0	public/private	10.0.1.100



## Launch the NetScaler AMI

1. Ensure that you subscribe to NetScaler VPX in the AWS Marketplace.
2. In **Community AMIs** of the EC2 Console launch wizard, launch the AMI searching for the **AMI IDs**.

For detailed instructions, see <https://s3.amazonaws.com/awsmvp-usageinstructions/CitrixUI.html>.



Software and AWS hourly usage fees apply when the instance is running. These fees will appear on your monthly bill.

Thank you! Your subscription will be completed in a few moments.

**Usage Instructions**  
Please go to <https://s3.amazonaws.com/awsmvp-usageinstructions/CitrixUI.html> for full usage instructions.

**Next Steps**

- aws@citrix.com will receive an email shortly to confirm your subscription.
- Once you've received the email, you can click the "Launch with EC2 Console" buttons below and follow the instructions to launch an instance of this software.
- You can also find and launch these AMIs by searching for the AMI IDs (shown below) in the "Community AMIs" tab of the EC2 Console Launch Wizard, or launch with the EC2 APIs.
- You can view this information at a later time by visiting the Your Software page. For help, see step-by-step instructions for launching Marketplace AMIs from the AWS Console.

**Related Links**

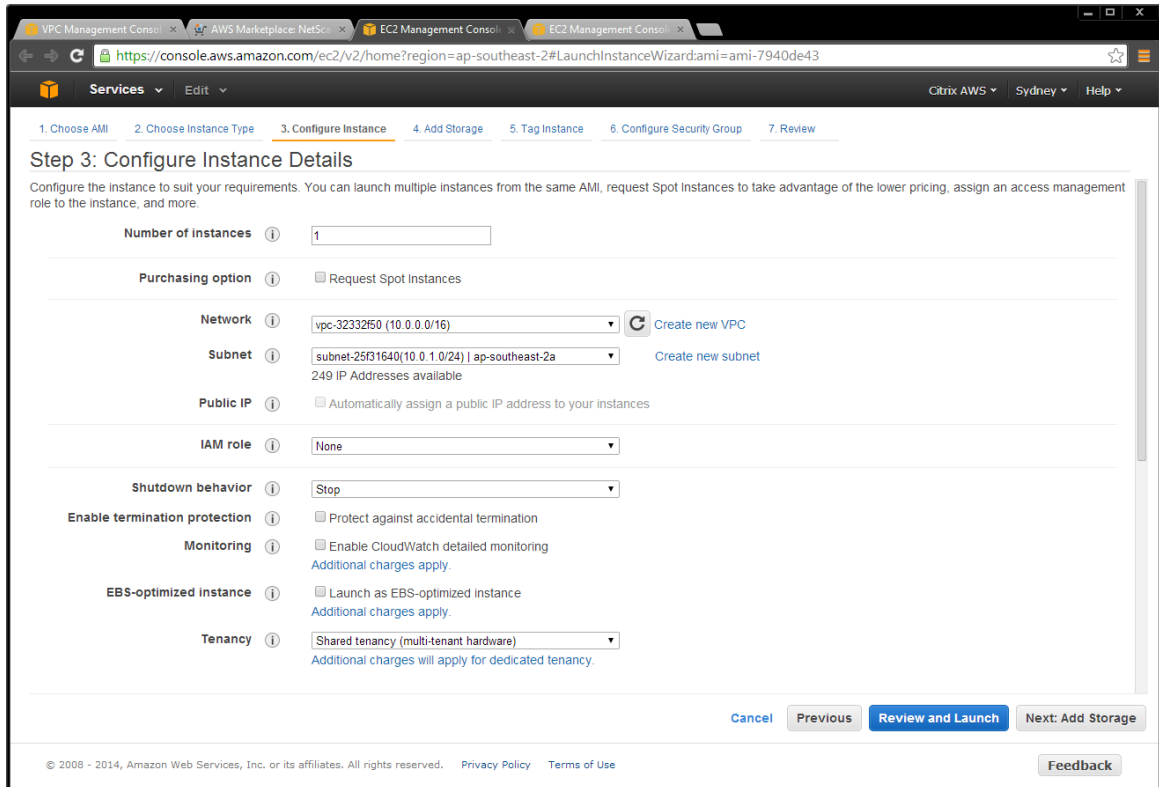
- AWS Management Console
- Your Software
- Continue shopping on AWS Marketplace

**Select a Version**

10.1-123.9, released 01/30/2014

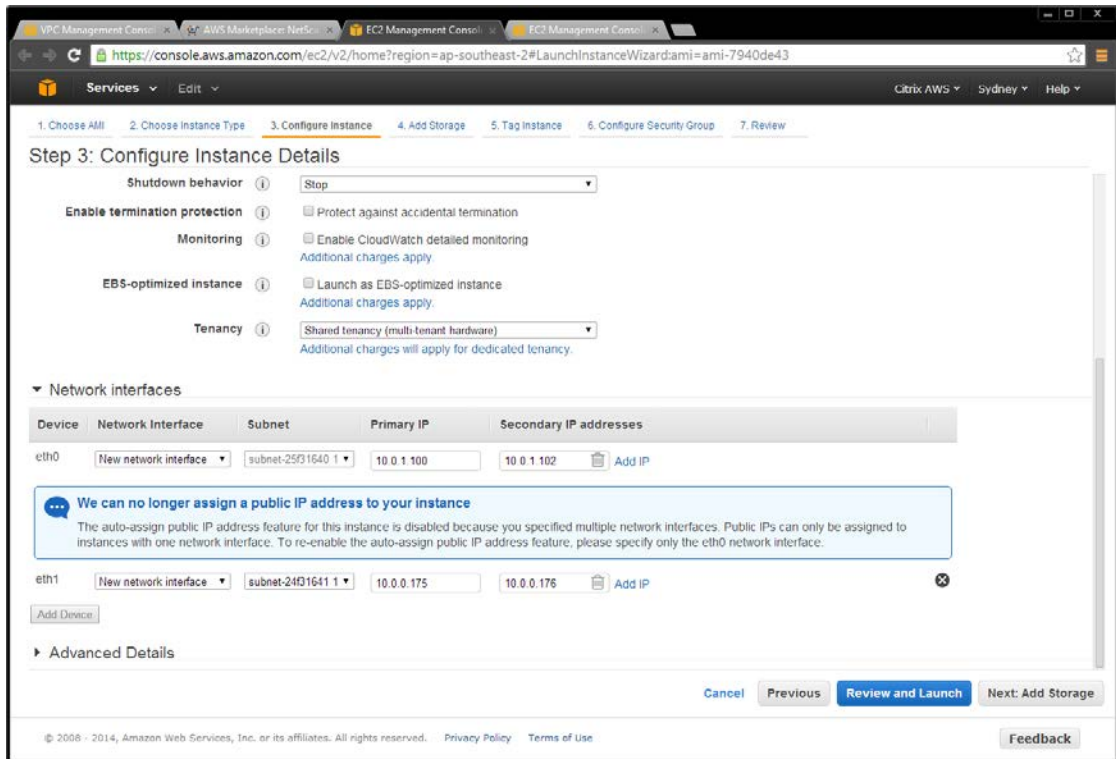
Region	ID	Launch with EC2 Console
US East (Virginia)	ami-c995aaa0	Launch with EC2 Console
US West (Oregon)	ami-3eeb8b0e	Launch with EC2 Console
US West (Northern California)	ami-c07b4685	Launch with EC2 Console
EU West (Ireland)	ami-7628df01	Launch with EC2 Console
Asia Pacific (Singapore)	ami-d840168a	Launch with EC2 Console
Asia Pacific (Sydney)	ami-7940de43	Launch with EC2 Console
Asia Pacific (Tokyo)	ami-b9ec84b8	Launch with EC2 Console
South America (Sao Paulo)	ami-7f50f062	Launch with EC2 Console

3. Deploy the instance into the private subnet.

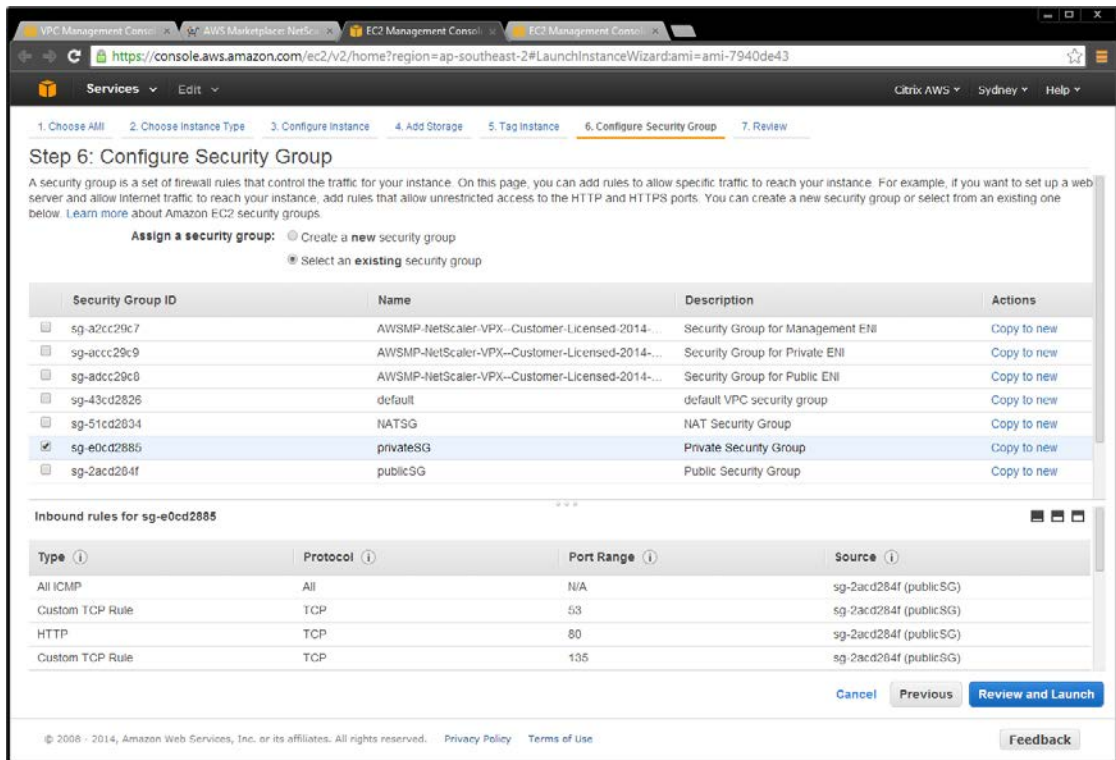


4. Ensure that this instance has two interfaces:

- Public subnet
- Private subnet:
  - i. **eth0** is connected to the private subnet
  - ii. Primary IP address (NSIP) is 10.0.1.100
  - iii. Secondary IP address (SNIP) is 10.0.1.102

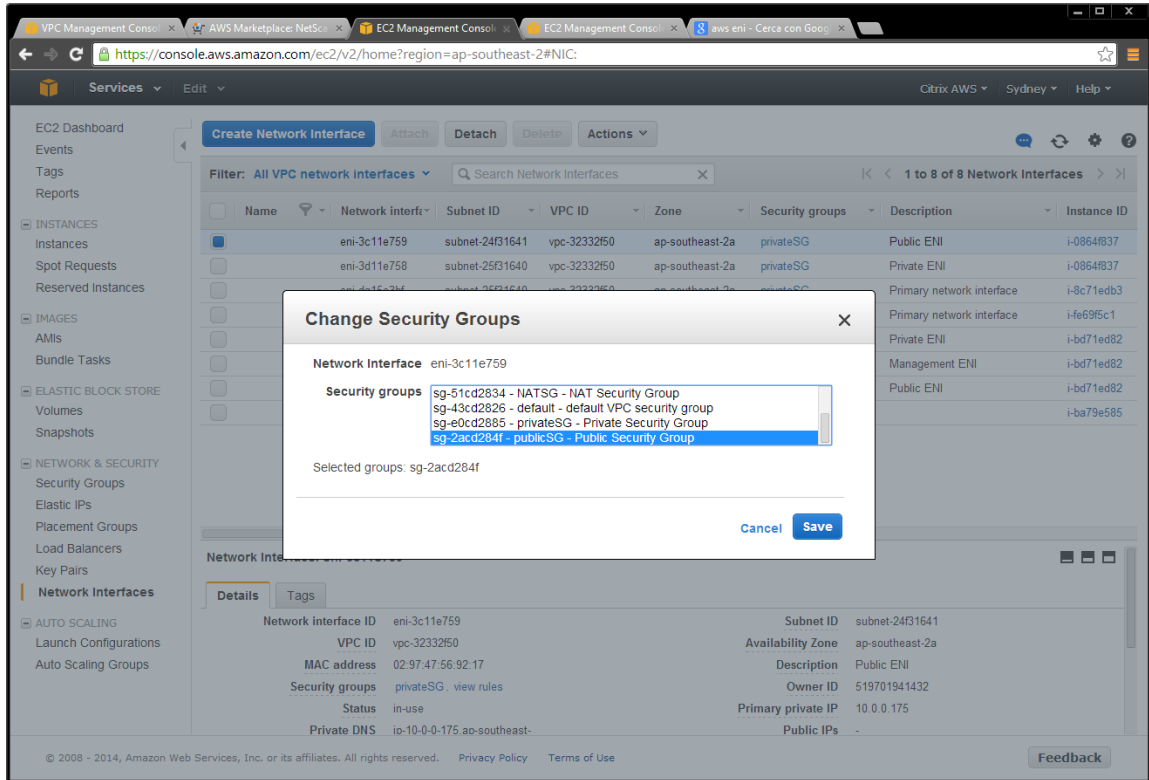


5. Deploy the instance into the private security group.

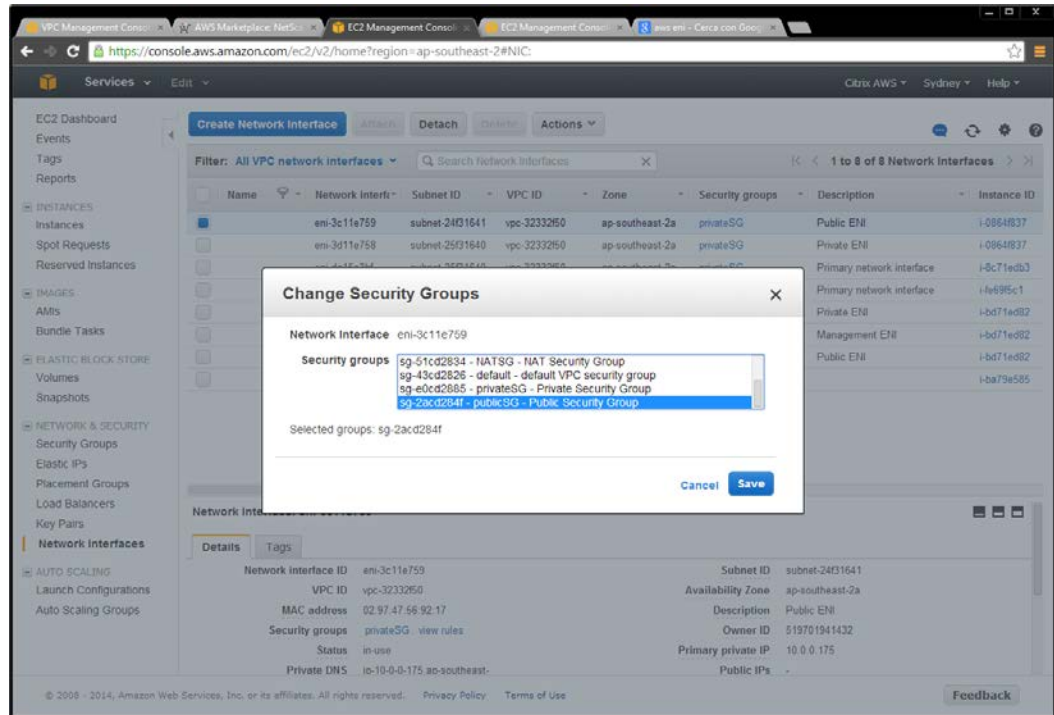


6. Configure the NetScaler ENIs (AWS elastic network interfaces) to be part of their respective security groups.
  - Public-subnet-facing ENI needs to be part of the public security group
  - Private-subnet-facing ENI needs to be part of the private security group

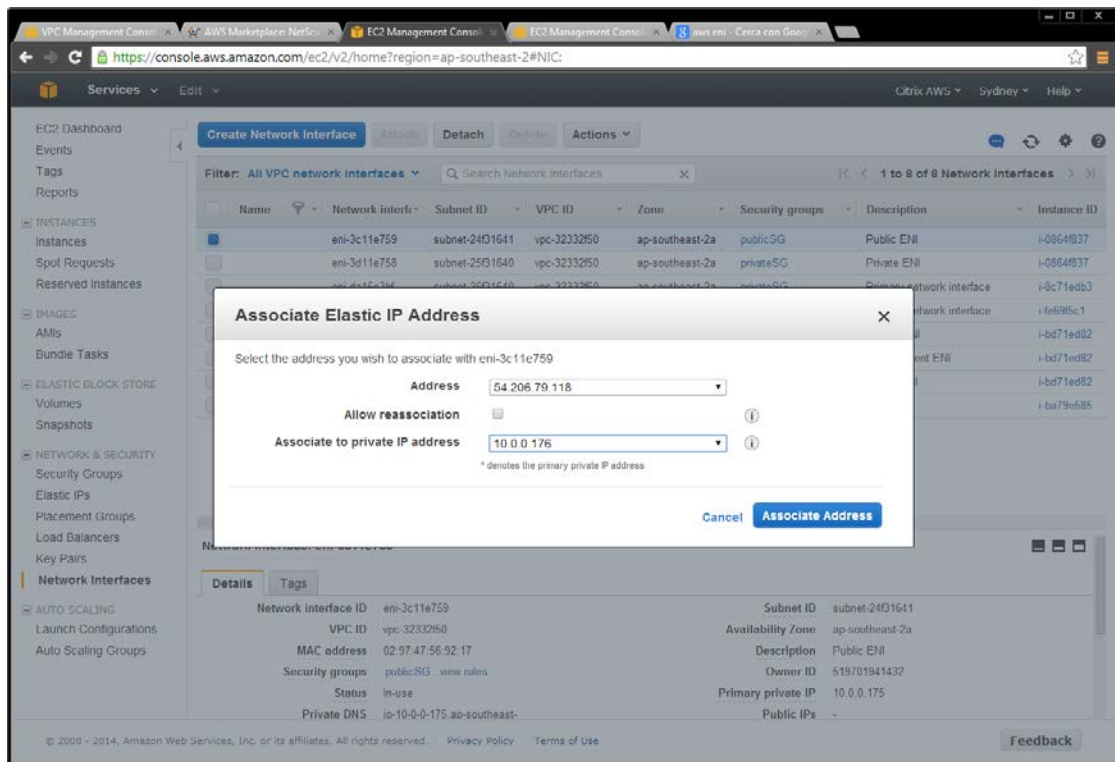
### Public ENI – Public Security Group



## Private ENI – Private Security Group



7. Assign an elastic IP address to the NetScaler public ENI – associated to the VIP (10.0.0.176).



The screenshot displays the AWS Management Console interface. A modal dialog titled "Change Security Groups" is open, showing the configuration for Network Interface "eni-3d11e758". The dialog lists the following security groups:

- sg-51cd2034 - NATSG - NAT Security Group
- sg-43cd2826 - default - default VPC security group
- sg-e0cd2885 - privateSG - Private Security Group** (Selected)
- sg-28cd284f - publicSG - Public Security Group

The "Selected groups" field contains "sg-e0cd2885". The dialog has "Cancel" and "Save" buttons.

In the background, the "Network Interfaces" table is visible:

Name	Network interface	Subnet ID	VPC ID	Zone	Security groups	Description	Instance ID
	eni-3c11e759	subnet-24f31641	vpc-32332f50	ap-southeast-2a	privateSG	Public ENI	i-0864f837
	eni-3d11e758	subnet-29f31640	vpc-32332f50	ap-southeast-2a	privateSG	Private ENI	i-0864f837
	eni-24f31641	subnet-29f31640	vpc-32332f50	ap-southeast-2a	privateSG	Primary network interface	i-8c71edb3
	eni-29f31640	subnet-24f31641	vpc-32332f50	ap-southeast-2a	privateSG	Primary network interface	i-4e695c1
	eni-24f31641	subnet-29f31640	vpc-32332f50	ap-southeast-2a	privateSG	Private ENI	i-bd71ed82
	eni-29f31640	subnet-24f31641	vpc-32332f50	ap-southeast-2a	privateSG	Management ENI	i-bd71ed82
	eni-24f31641	subnet-29f31640	vpc-32332f50	ap-southeast-2a	privateSG	Public ENI	i-bd71ed82
	eni-29f31640	subnet-24f31641	vpc-32332f50	ap-southeast-2a	privateSG	Public ENI	i-ba79e585

Below the table, the details for Network Interface ID "eni-3d11e758" are shown:

Network interface ID	eni-3d11e758	Subnet ID	subnet-29f31640
VPC ID	vpc-32332f50	Availability Zone	ap-southeast-2a
MAC address	02:44:48:37:fe:58	Description	Private ENI
Security groups	privateSG <a href="#">view rules</a>	Owner ID	519701941432
Status	in-use	Primary private IP	10.0.1.100
Private DNS	ip-10-0-1-100.ap-southeast-	Public IPs	-