|  |  |
| --- | --- |
| Document Management | |
| **Title** | XenDesktop 7.x on Google Cloud Engine (GCE) |
| **Product** | XenDesktop, XenApp |
| **Purpose** | Design guide for XenDesktop 7.6 on Google Cloud Engine, including an overview of solution architecture and implementation. |
| **Owner** | Peter Bats |
| **Feedback** |  |
| **Document ID** |  |
| **Revision History** |  |

XenDesktop® 7.6 on  
Google Cloud Engine (GCE

Design Guide

May 22, 2015

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Revision | Change Description | Updated By | Date |
| 0.1 | Document Created | Peter Bats | May15, 2015 |
| 1.0 | Final Draft | Peter Bats | June 17, 2015 |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[About This Design Guide 5](#_Toc422175042)

[Overview 5](#_Toc422175043)

[Use Case 5](#_Toc422175044)

[Business Objectives 6](#_Toc422175045)

[Technical Objectives 6](#_Toc422175046)

[Citrix XenDesktop 7.6 on GCE 6](#_Toc422175047)

[XenDesktop 7.6 on GCE Architecture 9](#_Toc422175048)

[User Group 12](#_Toc422175049)

[Access Layer 14](#_Toc422175050)

[Desktop Layer 17](#_Toc422175051)

[Control Layer 20](#_Toc422175052)

[Management and Operations 22](#_Toc422175053)

[Solution Capabilities and Constraints 22](#_Toc422175054)

[GCE as an IaaS Platform 22](#_Toc422175055)

[Networking 22](#_Toc422175056)

[Storage 22](#_Toc422175057)

[Provisioning 23](#_Toc422175058)

[Secure Access 23](#_Toc422175059)

[Microsoft Instances and Services Used for this Guide 23](#_Toc422175060)

[Citrix Components Supported in GCE for this Solution 24](#_Toc422175061)

[Scenario: Augmenting On-Premises Services with XenDesktop 7.6 Workers Hosted in GCE 25](#_Toc422175062)

[Set Up the VPC Network 26](#_Toc422175063)

[Create the VPC Network Infrastructure 26](#_Toc422175064)

[Add Security Groups 29](#_Toc422175065)

[Configure DHCP Options 38](#_Toc422175066)

[Set up the XenApp or XenDesktop Infrastructure Instances 40](#_Toc422175067)

[Launch and Configure a Domain Controller Amazon Machine Image (AMI) 40](#_Toc422175068)

[Launch Remaining XenApp or XenDesktop AMIs 44](#_Toc422175069)

[Launch the NetScaler AMI 45](#_Toc422175070)

[Conclusion 50](#_Toc422175071)

[Additional Resources 51](#_Toc422175072)

# 

## About This Design Guide

This Citrix Design Guide provides an overview of the XenDesktop® 7.6 on Google Cloud Engine (GCE solution architecture and implementation. This design has been created through architectural design best practices obtained from Citrix Consulting Services and thorough lab testing, and it is intended to provide guidance for solution evaluation and the introduction of proof of concepts.

The Design Guide incorporates generally available products into the design and employs repeatable processes for the deployment, operation, and management of components within the solution.

## Overview

Citrix customers wanting to leverage public cloud Infrastructure as a Service (Iaas) in order to expand their on-premises datacenter capabilities, without investing in new capital resources, can now host and provision desktops and applications using XenDesktop 7.6 within GCE. This capability enables faster proof of concept and pilot builds for migration to XenDesktop 7 for existing XenDesktop implementations or as part of a new or hybrid XenDesktop implementation where the leverage of public cloud infrastructure is preferred.

This document provides high-level design guidance using a sample implementation of XenDesktop 7.6 Hosted Shared and Server Virtual Desktop Infrastructure (VDI) FlexCast® models within the GCE cloud.

* Hosted Shared Desktops are built upon Windows Server 2008 R2 and Windows Server 2012 R2 RDS Session Host servers where multiple user sessions execute on a single shared server instance.
* Server VDI Desktops are built upon Windows Server 2008 R2 and Windows Server 2012 R2 for use cases where a single user requires a VDI-based dedicated or pooled server instance, which provides an execution environment that is not shared.

Used in conjunction with the XenDesktop Modular Reference Architecture, this document provides basic best-practice guidance for companies looking to leverage Citrix and GCE cloud technologies to deliver a state-of-the-art solution for their users.

## Use Case

Let us assume “XenCloud Corp.” (XenCloud) plans to leverage Google and Citrix technologies to deliver a hosted desktop solution for their accounting department. The solution will provide value to the department by enabling access to hosted desktops and applications from any device. The value of this solution for XenCloud is most evident in the ability to quickly bring new desktop services on line through a subscription to GCE infrastructure services rather than a protracted capital investment and datacenter build out project. Since the new desktops are an extension of the existing XenCloud datacenter, the infrastructure already in place at XenCloud will be connected to GCE through an IPSEC Site-to-Site VPN. This connectivity enables the GCE-hosted XenDesktop infrastructure components to communicate with the XenCloud corporate Active Directory and back-office services like Microsoft Exchange or Microsoft Lync, as well as the corporate Secure Remote Access services enabled through Citrix NetScaler Universal Gateway™.

The objective of this guide is to outline XenCloud’s business considerations and show how hosting their new XenDesktop 7.6 Windows Server-based FlexCast models in GCE could address them.

### Business Objectives

* Provide secure access to desktops and applications for the accounting team
* Avoid the need to build new infrastructure within the XenCloud datacenter
* Leverage as much existing corporate infrastructure as possible to align with current IT practices and policies and to keep new expenses as low as possible
* Use monthly programmatic funding instead of capital expenses for this project
* Manage the service within a public cloud environment in order to scale based on seasonal resource requirements
* Provide support for any device, enabling temporary contractors to “bring your own device” (BYOD)

### Technical Objectives

* Quickly design and implement an environment to establish the value and metrics
* Ensure high availability of critical components to ensure business continuity
* Implement an “n+1” highly available solution to avoid any business interruption
* Support access from user-owned devices that vary in form factor and operating system

## Citrix XenDesktop 7.6 on GCE

XenCloud selected XenDesktop as their solution since it enables the best user experience across the public Internet from any device according to independent analysis and, after reviewing the Citrix XenDesktop Modular Reference Architecture and GCE IaaS capabilities, they believed they could build a solution without a large upfront capital investment.

The Citrix XenDesktop 7.6 solution (see Figure 1) hosted on GCE consisted of a small number of components:

* Hosted Shared workers (Windows Server RDS Session Host enabling session isolation)
* Server VDI Workers (Windows Server pooled or dedicated VDI-based instance isolation)
* An GCE local Active Directory Domain Controller (DC) that is a member of the XenCloud corporate forest
* An GCE local File Server for the storage of Roaming User Profiles for the XenDesktop users

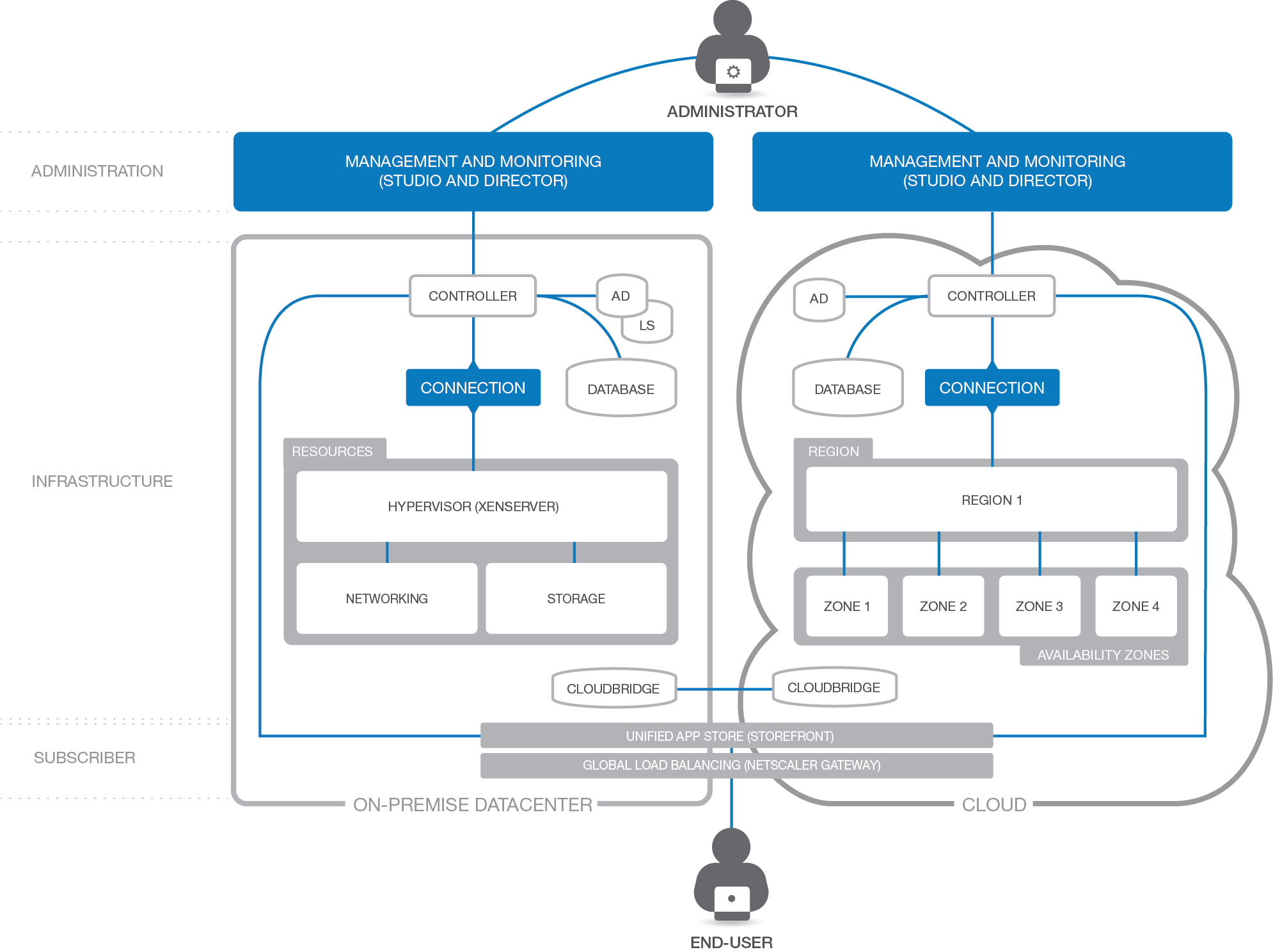


Figure . Architectural diagram of hybrid XenDesktop deployment.

The remaining components were already in place in the XenCloud on-premises corporate datacenter.

A brief description of key Citrix components follows:

* **Citrix Receiver.** Citrix Receiver is an easy-to-install client software component that lets you access your documents, applications and desktops from any of your devices including smartphones, tablets and PCs.
* **Citrix XenDesktop Delivery Controllers.** These XenDesktop 7.6 Servers are used to manage and deliver the Windows applications and desktops.
* **Hosted Shared Workers.** These XenDesktop 7.6 workloads, leveraging Windows Server Remote Desktop Services Session Host as the foundation, are used to deliver shared hosted applications and desktops for most users.
* **Server VDI Workers.** These XenDesktop 7.6 workloads, using Windows Server without the Remote Desktop Services Session Host role, provide VDI-based instance- or server-level isolation of an individual server instance for those users that require more customization or administrative control of their virtual desktop.
* **Citrix License Server.** The Citrix License Server hosts all the licenses that enable Citrix products and features.
* **NetScaler Unified Gateway.** NetScaler Unified Gateway is a secure application and data access solution that provides administrators granular application- and data-level control while empowering users with remote access from anywhere.
* **StoreFront Services.** StoreFront Services provides authentication and resource delivery services for Citrix Receiver, enabling users to create centralized enterprise stores to deliver desktops, applications, and other resources to users on any device, anywhere.

## XenDesktop 7.6 on GCE Architecture

Once XenCloud had completed their assessment and concluded that a Citrix XenDesktop 7.6 solution on GCE could meet their objectives, they quickly moved into the design phase. XenCloud wanted a simple, easy process to determine the hardware and storage sizing to support their individual implementation based on the needs of their subscribers. XenCloud used Citrix [Project Accelerator](http://project.citrix.com)—an open, web-based application where you can manage your move to virtualized desktops and applications based on best practices of Citrix’s top consultants—to assist with the user assessment and environment design. In conjunction with project accelerator guidance, XenCloud made the following design decisions:

* To remain consistent with the true outputs of the Project Accelerator tool we have left the original graphic outputs of the Project Accelerator that show “Windows 7” or “Windows 8.1” as one of the desktop images to deploy, the actual implementation on GCE must use Windows Server 2008 R2 or Windows Server 2012 instances to enable “Server VDI” for these desktops. Windows Client operating systems are not supported for hosting on GCE at this time (<https://cloud.google.com/compute/docs/operating-systems/>).] The output of Project Accelerator is only part of the data used to design the complete solution, and some GCE-specific adjustments must be made in order to remain compliant with Microsoft licensing. More detail is available in the “[Solution Capabilities and Constraints](#_Solution_Capabilities_and)” section of this guide on page 22.
* High availability is important for a robust solution, so an “N+1” configuration was chosen to ensure that the solution sizing included a spare server to handle user capacity in the event of a failure.
* All users would need to connect to GCE over an encrypted connection through an IPSEC based Site-to-Site VPN between GCE and the XenCloud corporate network. Secure remote access would be provided by the NetScaler Unified Gateway within the corporate network.
* Active Directory and DNS/DHCP would be provisioned in GCE to reduce login times for this solution.
* A variety of financial applications as well as MS Office would be made available as part of the standard desktop image for this group of users.

The following architecture (see Figure 2 and Figure 3) is a visual representation of the solution as recommended by [Citrix Project Accelerator.](http://project.citrix.com/)  Where Figure 2 shows the on-premises resources, Figure 3 shows the GCE-hosted resources. Additional considerations that leverage this output as the base are documented later in this guide. The following diagrams represents XenCloud’s projected hardware and infrastructure requirements based on a team of 2325 users, spread over multiple types of users: Customer Service reps, Sales – Mobile, Sales – Normal, Sales – Developers, Accounting – Task Workers and Accounting – Content Creators.

Each layer of the architecture diagrams is discussed in detail in the following sections.

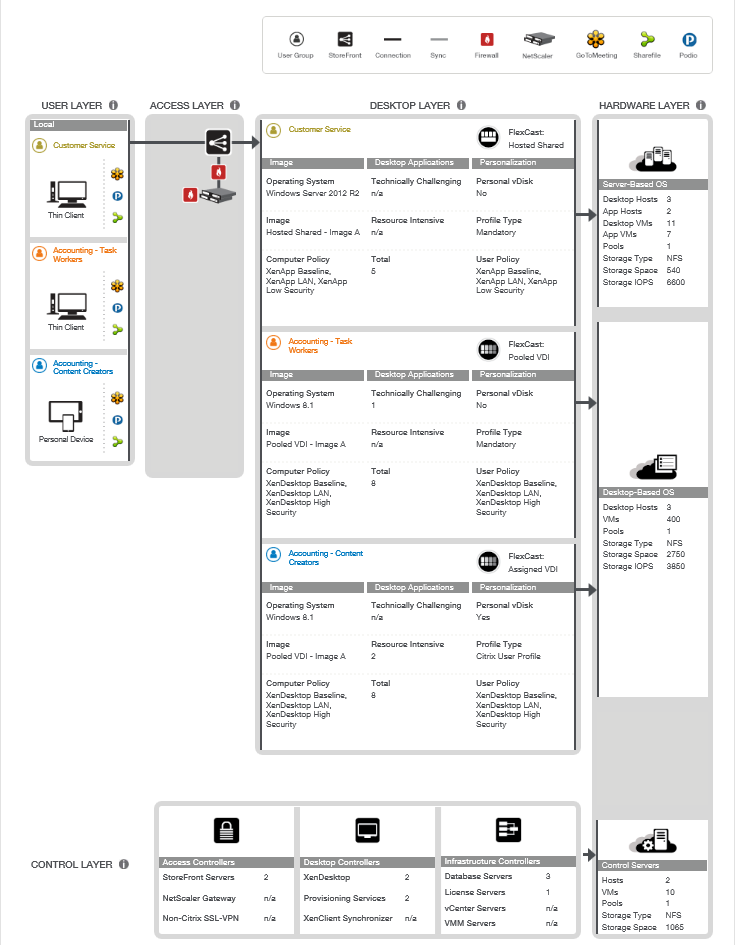


Figure . Project Accelerator output for XenCloud on-premises resources for hybrid Desktop as a Service (DaaS) project.

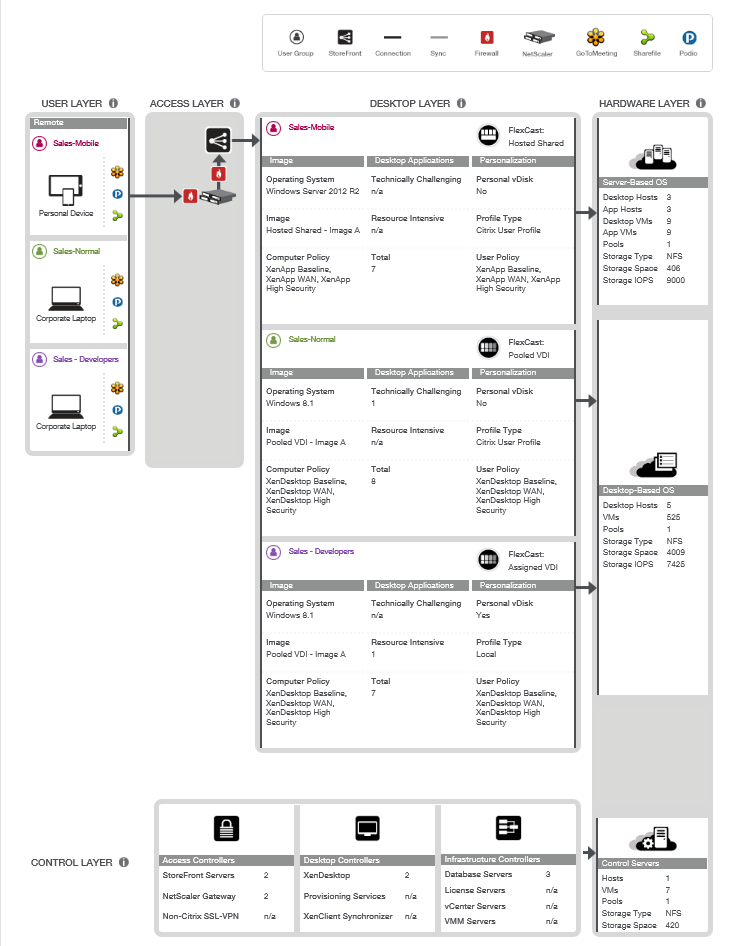


Figure . Project Accelerator output for XenCloud GCE resources for DaaS project.

### User Group

The user group layer (see Figure 4) represents the subscriber types that will access the GCE or on-premises hosted desktops or applications from their own end-point devices. Although the graphic represents these devices as “Corporate Laptops” and “Personal Devices,” these devices can be anything from a smartphone or tablet to a PC, Mac, or Linux desktop or laptop. These user groups represent the use cases of “Task Worker” or “Content Creator.” The details of what is delivered to these different user groups are enabled within the desktop layer, behind the access layer section.

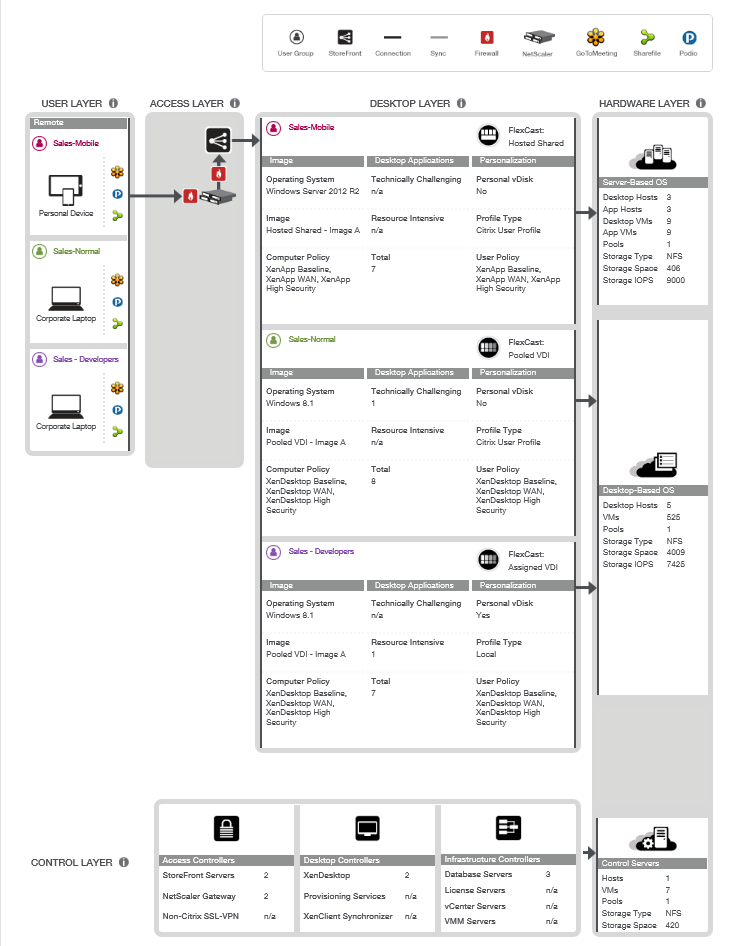


Figure 4. The user group layer includes subscribers that access the GCE or on-premises hosted desktops or application from their own devices.

Contoso requires the following Citrix component on each end-point device:

* **Citrix Receiver.** Citrix Receiver is a universal thin client that runs on virtually any device operating platform, including ChromeOS, Windows, Mac, Linux, iOS and Android. This is the one client users need to access business-critical apps and data from today’s latest tablet and smartphone devices and improve their mobility. Citrix Receiver can be downloaded and installed by employees on their personal devices.

### Access Layer

The access layer (see Figure 5) consists of the servers responsible for providing connectivity to the entire XenDesktop 7.6 environment on-premises and on GCE.

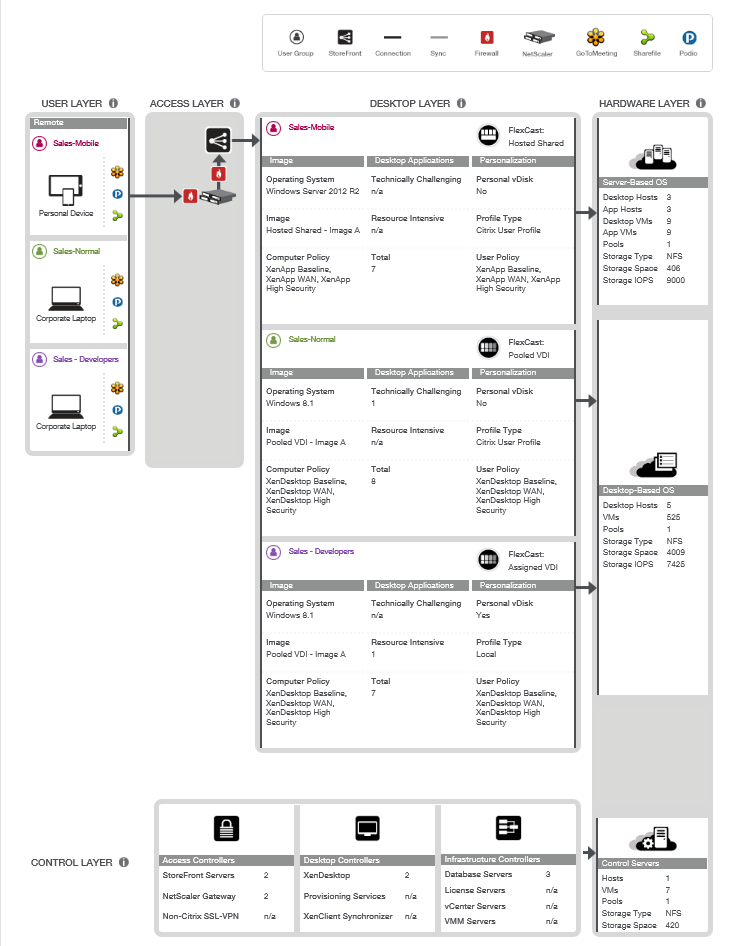


Figure 5: The access layer provides connectivity to the hybrid XenDesktop 7.6 environment.

XenCloud’s solution required the following Citrix components to provide secure remote access:

* StoreFront Services. StoreFront Servicesprovides a self-service subscription service to desktops and applications via an enterprise app store, giving users convenient access to all the resources they need. XenCloud created a centralized enterprise app store with StoreFront Services within their on-premises datacenter to enumerate and aggregate the resources available for each user. XenCloud deployed a pair of StoreFront servers to ensure high availability.

Table . StoreFront Service Configuration.

|  |  |
| --- | --- |
| StoreFront Services Servers | |
| Instances | 2 StoreFront Server VMs |
| Virtual Machine Configurations | |
| Memory | 4 GB RAM |
| Processor | 2 vCPUs |
| Hard Drive | 60 GB |
| Installed Software | |
| Web Interface | StoreFront 2.6 |
| Windows Server | Windows Server 2012 |
| IIS | 7.5 or greater |
| Microsoft .NET Framework | 4.0 |
| Ports Utilized | |
| StoreFront | 80, 443 |

* NetScaler Unified Gateway. NetScaler Unified Gateway is a secure application and data access solution that gives administrators granular application and data-level control while empowering users with remote access from anywhere. IT administrators gain a single point of management for controlling access and limiting actions within sessions based on user identity and the endpoint device. The results are better application security, data protection and compliance management.  
    
  NetScaler Unified Gateway works in conjunction with StoreFront Services to authenticate the user and create an SSL tunnel between the end user and NetScaler Gateway to ensure secure remote access from any device. NetScaler Gateway requires either a physical or a virtual NetScaler appliance. XenCloud selected two physical NetScaler MPX appliances to host NetScaler Gateway in an active/active mode to ensure secure access is highly available and maximum capacity.

Table . NetScaler Gateway Configuration.

|  |  |
| --- | --- |
| NetScaler Gateway | |
| Instances | |
| NetScaler MPX | 2 physical NetScaler MPX-5500 |
| Build | 10.1 |
| Throughput | 500 Mbps |
| Ports Utilized | |
| DMZ | 80, 443 |
| Internal | 80, 443, 1494, and 2598 |

Citrix recommends installing NetScaler Gateway in the network DMZ. When installed in the DMZ, NetScaler Gateway participates on two networks: a private network and the Internet with a publicly routable IP address. NetScaler Gateway can be used to partition local area networks internally in the organization for access control and security by creating partitions between wired or wireless networks and between data and voice networks.

### Desktop Layer

The desktop layer (see Figure 6) represents the separate use cases that XenCloud will service: plans for 500 users to access Sales – Mobile resources, 500 users to access Sales – Normal resources, and 25 users to access Sales – Developers resources.

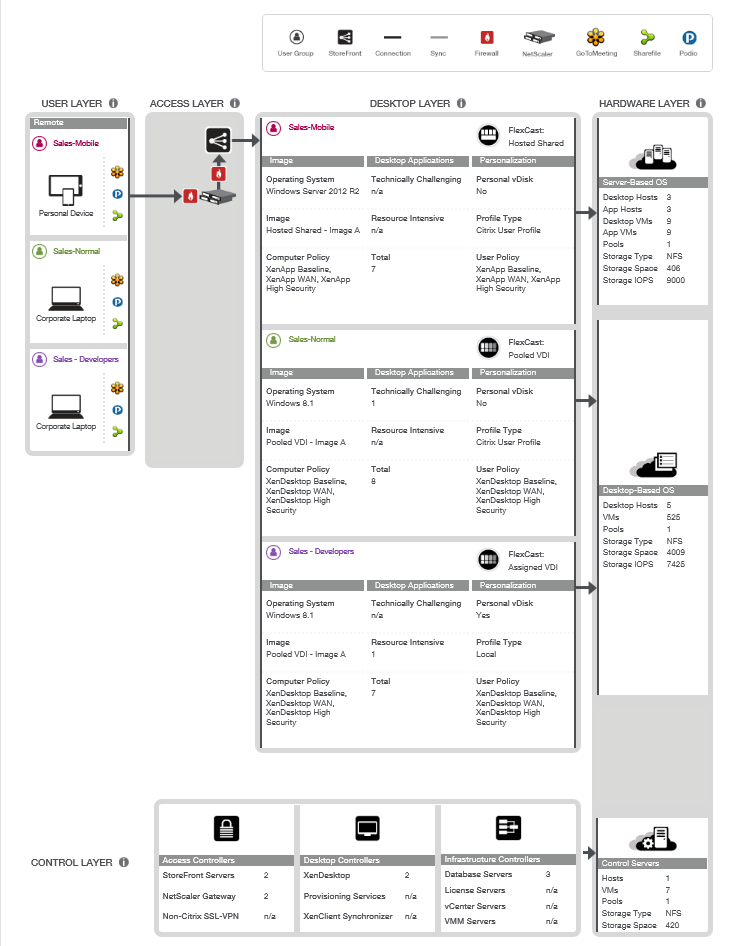


Figure 6: The desktop layer includes the various use cases that are planned for this solution.

The XenCloud solution required the following Citrix components to provide the desktop layer:

* **Citrix XenDesktop Delivery controllers.** These XenDesktop 7.6 Infrastructure Servers are used to manage and deliver the Windows or Linux applications and desktops.

|  |  |
| --- | --- |
| XenDesktop Controller Servers | |
| Instances | 2 XenDesktop Controllers |
| Virtual Machine Configurations | |
| Instance Type | XenServer |
| Memory | 7.5 GB RAM |
| Processor | 2 vCPUs |
| Disk | 60 GB HD |
| Installed Software | |
| XenDesktop Version | 7.6 |
| Winders Server | Windows Server 2012 R2 |

* **Hosted Shared Workers.** These XenDesktop 7.6 workloads, leveraging Windows Server Remote Desktop Services Session Host as the foundation, are used to deliver shared hosted applications and desktops for most users.

|  |  |
| --- | --- |
| Hosted Shared Desktop Workers | |
| Instances | 9 XenApp Desktop Workers |
| Virtual Machine Configurations | |
| Instance Type | N1-standard-8 |
| Memory | 30 GB RAM |
| Processor | 8 vCPUs |
| Disk | 160 GB HD |
| Installed Software | |
| XenDesktop VDA Version | 7.6 |
| Winders Server | Windows Server 2012 R2 – Hosted Shared |
| Hosted Shared App Workers | |
| Instances | 9 XenApp Application Workers |
| Virtual Machine Configurations | |
| Instance Type | N1-standard-8 |
| Memory | 30 GB RAM |
| Processor | 8 vCPUs |
| Disk | 160 GB HD |
| Installed Software | |
| XenDesktop VDA Version | 7.6 |
| Winders Server | Windows Server 2012 R2 – Hosted Shared |

|  |  |
| --- | --- |
| Pooled VDI Desktop Workers | |
| Instances | 500 Pooled VDI Desktop Workers |
| Virtual Machine Configurations | |
| Instance Type | N1-standard-1 |
| Memory | 3.75 GB RAM |
| Processor | 1 vCPUs |
| Disk | 50 GB HD |
| Installed Software | |
| XenDesktop VDA Version | 7.6 |
| Winders Server | Windows Server 2012 R2 – Server VDI |

* **Server VDI Workers.** These XenDesktop 7.6 workloads, using Windows Server without the Remote Desktop Services Session Host role, provide VDI-based VM or server-level isolation of an individual server instance for those users that require more customization or administrative control of their virtual desktop.

|  |  |
| --- | --- |
| Pooled VDI Desktop Workers | |
| Instances | 500 Pooled VDI Desktop Workers |
| Virtual Machine Configurations | |
| Instance Type | N1-standard-1 |
| Memory | 3.75 GB RAM |
| Processor | 1 vCPUs |
| Disk | 50 GB HD |
| Installed Software | |
| XenDesktop VDA Version | 7.6 |
| Winders Server | Windows Server 2012 R2 – Server VDI |
| Assigned VDI Desktop Workers | |
| Instances | 25 Assigned VDI Desktop Workers |
| Virtual Machine Configurations | |
| Instance Type | N1-highcpu-4 |
| Memory | 15 GB RAM |
| Processor | 4 vCPUs |
| Disk | 60 GB HD (SSD) |
| Installed Software | |
| XenDesktop VDA Version | 7.6 |
| Winders Server | Windows Server 2012 R2 – Server VDI |

### Control Layer

The control layer (see Figure 7) contains all the infrastructure components required to support the access and desktop layers. The Access Controllers and Desktop Controllers were previously discussed in their respective sections. This section outlines XenCloud’s implementation of the Infrastructure Controllers and Control Hosts placed on-premises to decrease WAN traffic for logon and the potential increased logon times that can result.

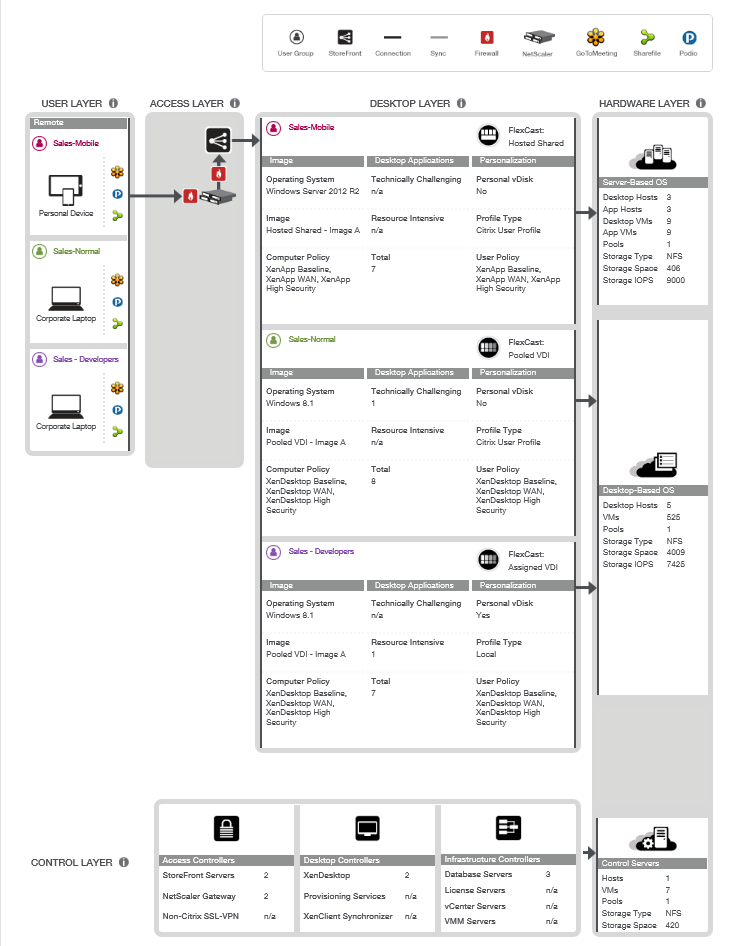


Figure 7. The control layer includes the components required to support the access and desktop layers.

According to the Project Accelerator, XenCloud’s solution required the following Citrix and Microsoft infrastructure components within the control layer:

* Active Directory**.** Citrix XenDesktop and XenApp leverage Active Directory for authentication and policy setting enforcement on both users and computers.

|  |  |
| --- | --- |
| Active Directory Controller Requirements | |
| Instances | 2 Active Directory Controllers |
| Virtual Machine Configurations | |
| Instance Type | N1-standard-1 |
| Memory | 3.75 GB RAM |
| Processor | 1 vCPUs |
| Disk | 60 GB HD |
| Installed Software | |
| Winders Server | Windows Server 2012 R2 |

* **SQL Server Database (SQL Mirroring)**. The SQL Server Database provides high availability with automatic failover Database Services used by XenDesktop 7.6.

|  |  |
| --- | --- |
| SQL Server Requirements | |
| Instances | 3 SQL Server database servers |
| Virtual Machine Configurations | |
| Instance Type | c3.xlarge |
| Memory | 7.5 GB RAM |
| Processor | 4 vCPUs |
| Disk | 60 GB |
| Installed Software | |
| SQL Server version | SQL 2012 |
| Authentication | Mixed |
| TCP/IP | Enabled |
| Named Pipes | Enabled |
| IP Address | 10.16.3.50 |
| Port | 1436 |
| Disk space data files | 60Gb |
| Disk space log files | 20Gb |
| Winders Server | Windows Server 2012 |

## Management and Operations

For day-to-day administration, Desktop Director was leveraged to manage and support the environment. Support staff and administrators were granted access to the console.

Administrators manage the site using Citrix Studio. This console handles all site-level responsibilities including policies, device and user allocations. Only senior administrators are granted access to the Citrix Studio. The console was installed on each XenDesktop controller for high availability.

## Solution Capabilities and Constraints

The Project Accelerator outputs provide the base sizing and architecture. The following sections provide additional considerations, tools and optimizations specific to Google Cloud Engine (GCE) platform itself. By taking these additional factors into consideration, along with the base sizing and architecture, a complete hybrid solution in the XenCloud datacenter and GCE could be implemented.

The following sections outline some of the considerations within GCE that have influenced this design beyond the recommendations from the Project Accelerator.

### GCE as an IaaS Platform

The GCE platform has evolved to include several technologies that enable Infrastructure as a Service (IaaS). This section provides a brief overview of those technologies that are leveraged as a part of the Citrix XenDesktop solution on GCE.

More information about GCE and Windows VM Instance capabilities can be found at:

* <https://cloud.google.com/compute/docs/operating-systems/windows>

#### Networking

A GCE project can contain multiple networks, where each network enables a logically isolated section of the GCE Cloud where you can launch GCE resources in a virtual network that you define. Administrators have complete control over the virtual networking environment, through adding or removing customized firewalls, to control access to the GCE VM instances in this virtual network.

The example in this guide uses a single virtual network for all GCE-hosted XenDesktop 7.6 workloads. An IPSEC Site-to-Site VPN connection was used between XenCloud’s on-premises corporate datacenter and the GCE-hosted virtual network.

More information regarding GCE Networking can be found at <https://cloud.google.com/compute/docs/networking>

#### Storage

The scenario in this document leverages Google Compute Engine’s persistent disk storage as primary storage for VM instances provisioned within GCE. In addition, a Windows Server 2012R2 File Server has been configured within GCE as a shared file service for the storage of user profiles and data. Additional storage can be allocated within the environment as required for other workloads not documented in this guide.

More information about GCE storage options can be found at <https://cloud.google.com/compute/docs/disks/>

**Important!** Because Citrix Provisioning Services and Citrix Machine Creation Services are not supported with GCE at this time, the storage calculations from the Project Accelerator can differ significantly from the storage actually used. Please confirm your storage requirements as part of your cost models.

#### Provisioning

The provisioning of VM Instances within GCE is accomplished through manual creation of the VM instances through the GCE Console. Larger scale environments can be provisioned using GCE scripts. The console UI examples in this guide are used for the sake of clarity, while it is generally recommended that a Citrix Service Provider (CSP) or enterprise deployments leverage the XenDesktop SDK and GCE scripts to ensure continuity when provisioning instances over time or at larger scale.

More information about AWS CloudFormation and samples can be found at <http://aws.amazon.com/cloudformation/aws-cloudformation-templates>

#### Secure Access

For the scenario in this guide, secure access to desktops and applications within GCE is provided through the on-premises NetScaler Gateway when connecting to GCE-hosted workloads. The connections made through the NetScaler Gateway are then passed through the Site-to-Site VPN to the GCE-hosted desktops and applications (see Figure 8).

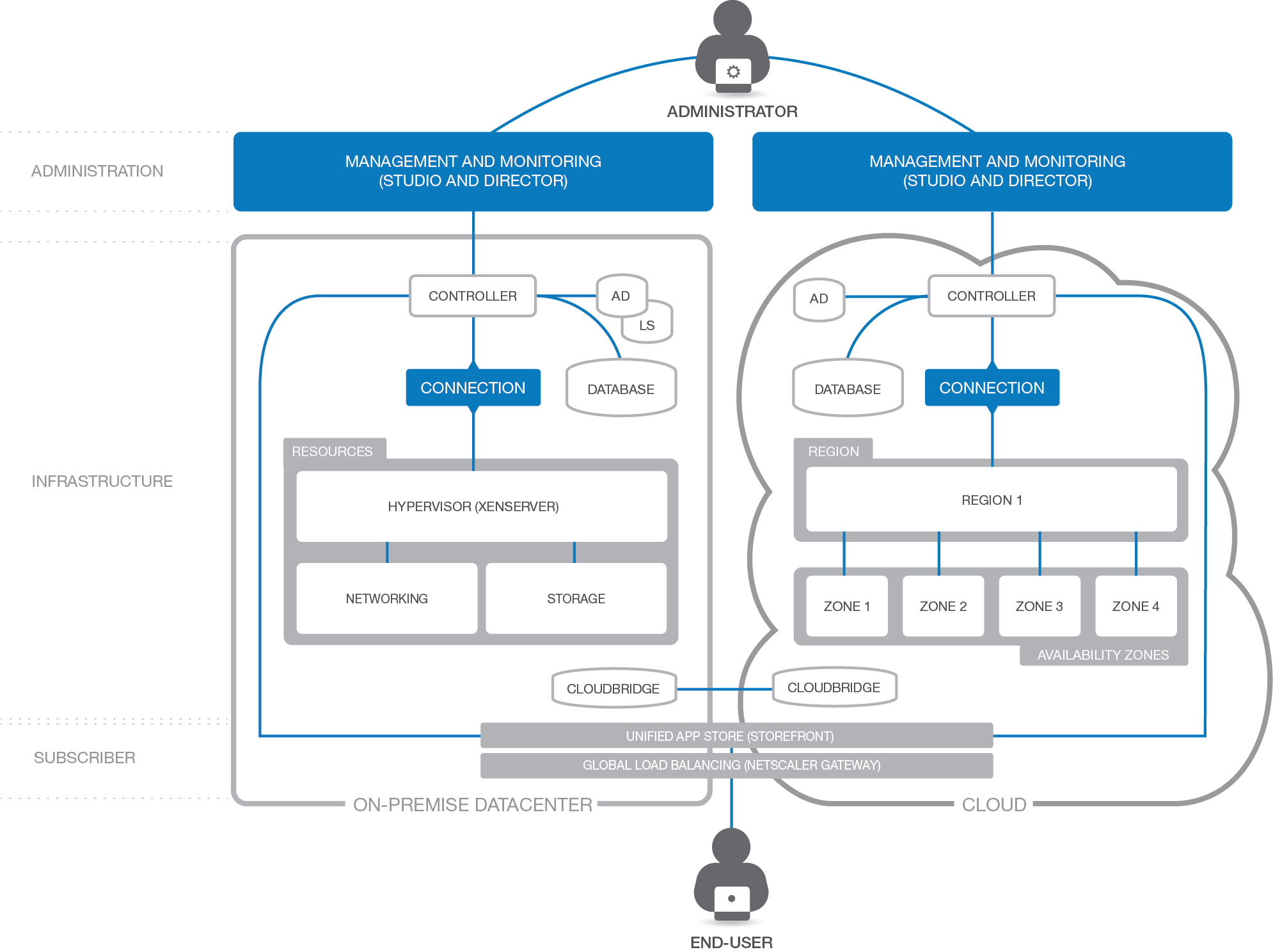


Figure 8. Citrix NetScaler Gateway provides unified and secure access to on-premises and GCE-hosted desktops and applications.

More information about Citrix NetScaler Gateway can be found at <http://www.citrix.com/edocs>.

### Microsoft Instances and Services Used for this Guide

Microsoft Windows Server 2012 R2 Datacenter Instances were used for all Windows Servers in this guide. Some of the roles and services enabled on various servers include:

* Active Directory Services
* File Services
* Internet Information Services
* Microsoft SQL Server 2012 Service Pack 1
* .NET 3.5
* .NET 4.0
* Remote Desktop Services
* Remote Desktop Service License Server

### Citrix Components Supported in GCE for this Solution

The following Citrix components for this solution are currently supported within GCE:

* Citrix XenDesktop 7.6 Delivery controllers, Hosted Shared Workers and Server VDI Workers

## Scenario: Augmenting On-Premises Services with XenDesktop 7.6 Workers Hosted in GCE

The following sections walk through creation of a GCE virtual network to be used for XenDesktop. This scenario augments on-premises services with XenDesktop 7.6 workers hosted in GCE. The key steps include:

* Creating the GCE virtual network. This includes creating the virtual network infrastructure, adding firewall rules, and configuring routes.
* Configuring and launching the XenApp and XenDesktop infrastructure instances.

Figure 9 shows the sample architecture used for this scenario.

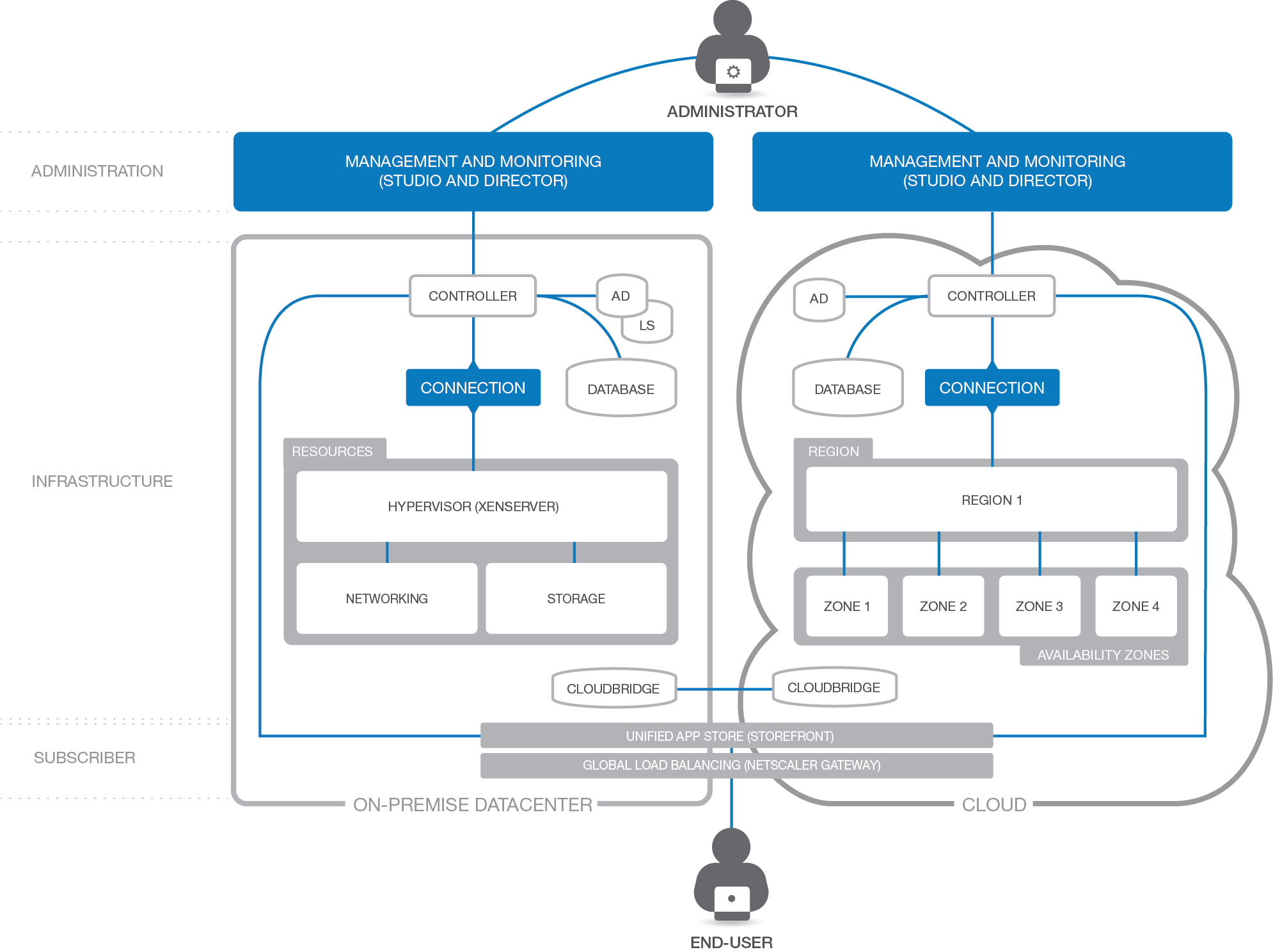


Figure 9. Sample architecture used by the scenario to augment on-premises services with XenDesktop 7.6 controllers and workers hosted in GCE.

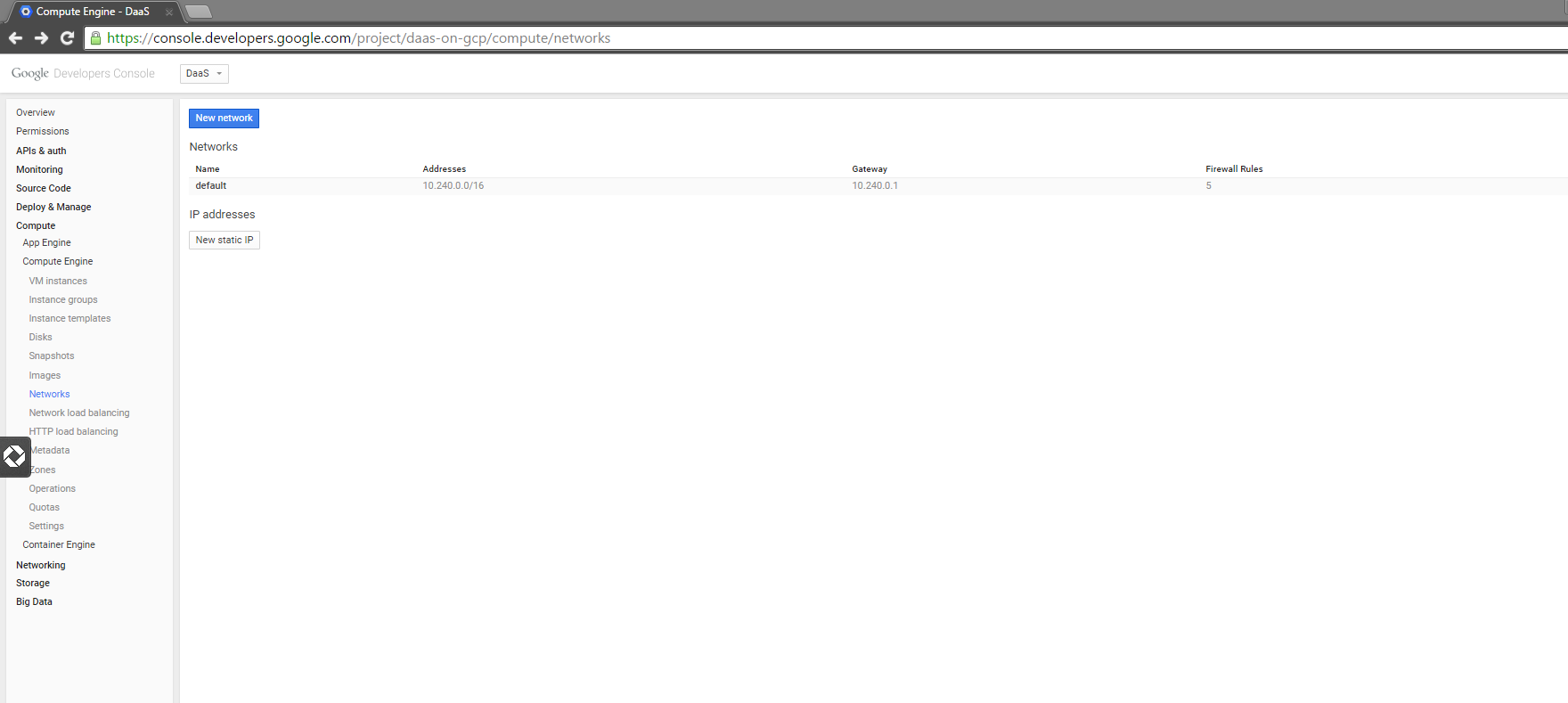
### Set Up the Virtual Network

The following sections cover the key steps in setting up the virtual network: creating the virtual network infrastructure, adding firewall rules, and configuring routes.

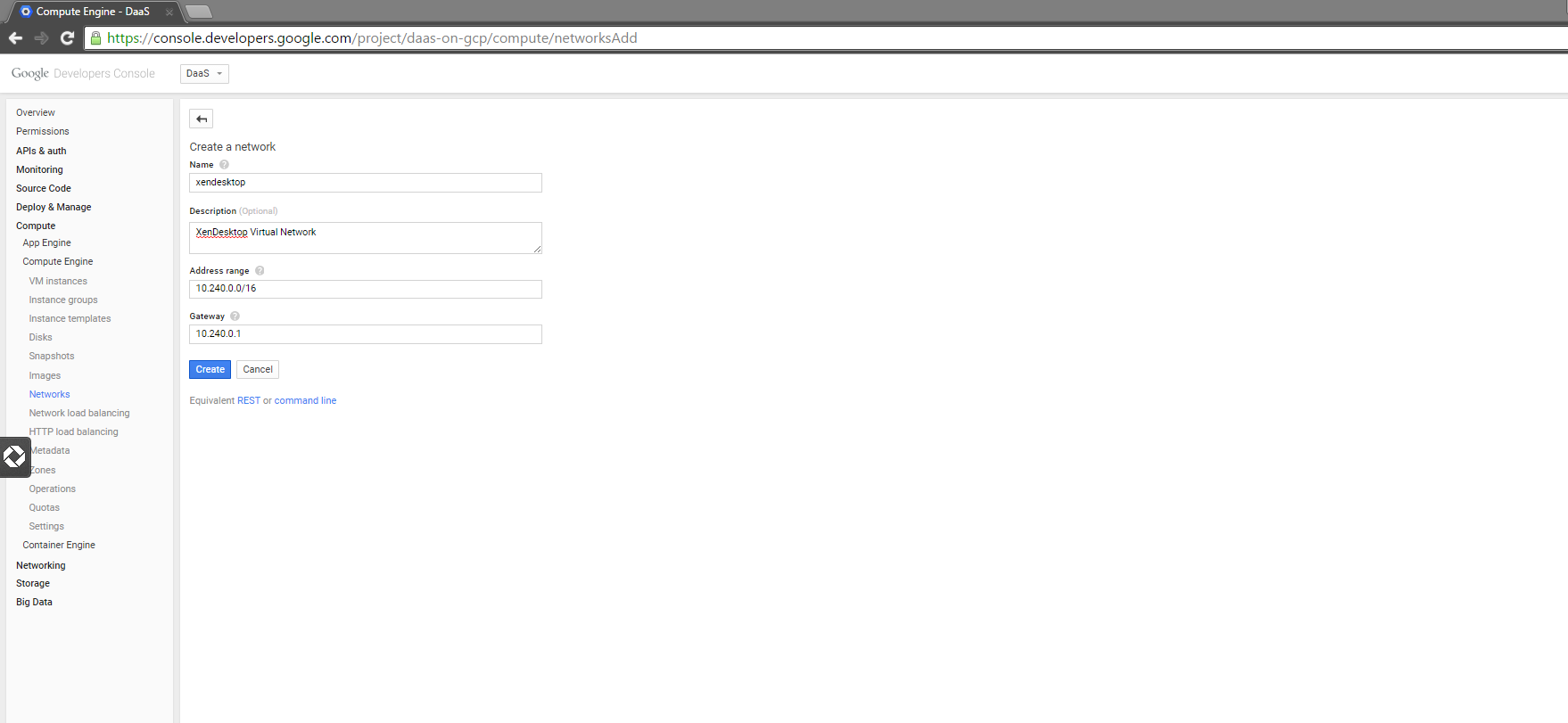
#### Create the Virtual Network Infrastructure

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

1. Log in to your GCE Console, and navigate to the Compute Engine\Networks node. Click **New network**.



1. Provide the network name, address range and gateway for your GCE based virtual network.



**Note:** To create a hybrid setup between your on-premises environment and AWS:

1. Select **VPC with Public and Private Subnets and Hardware VPN**.
2. Alternatively, use a NetScaler VPX Platinum Edition enabling NetScaler Gateway as well as CloudBridge Connector. The CloudBridge Connector enables a WAN-optimized VPN function between your on-premises environment and your Amazon VPC.
3. Next, the wizard displays the default settings for the VPC and provides an opportunity to make adjustments. This sample deployment uses the default network settings. Adjust these settings accordingly, and then click **Create VPC**.



1. A confirmation message is displayed, indicating the VPC has been successfully created.



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

#### Add Security Groups

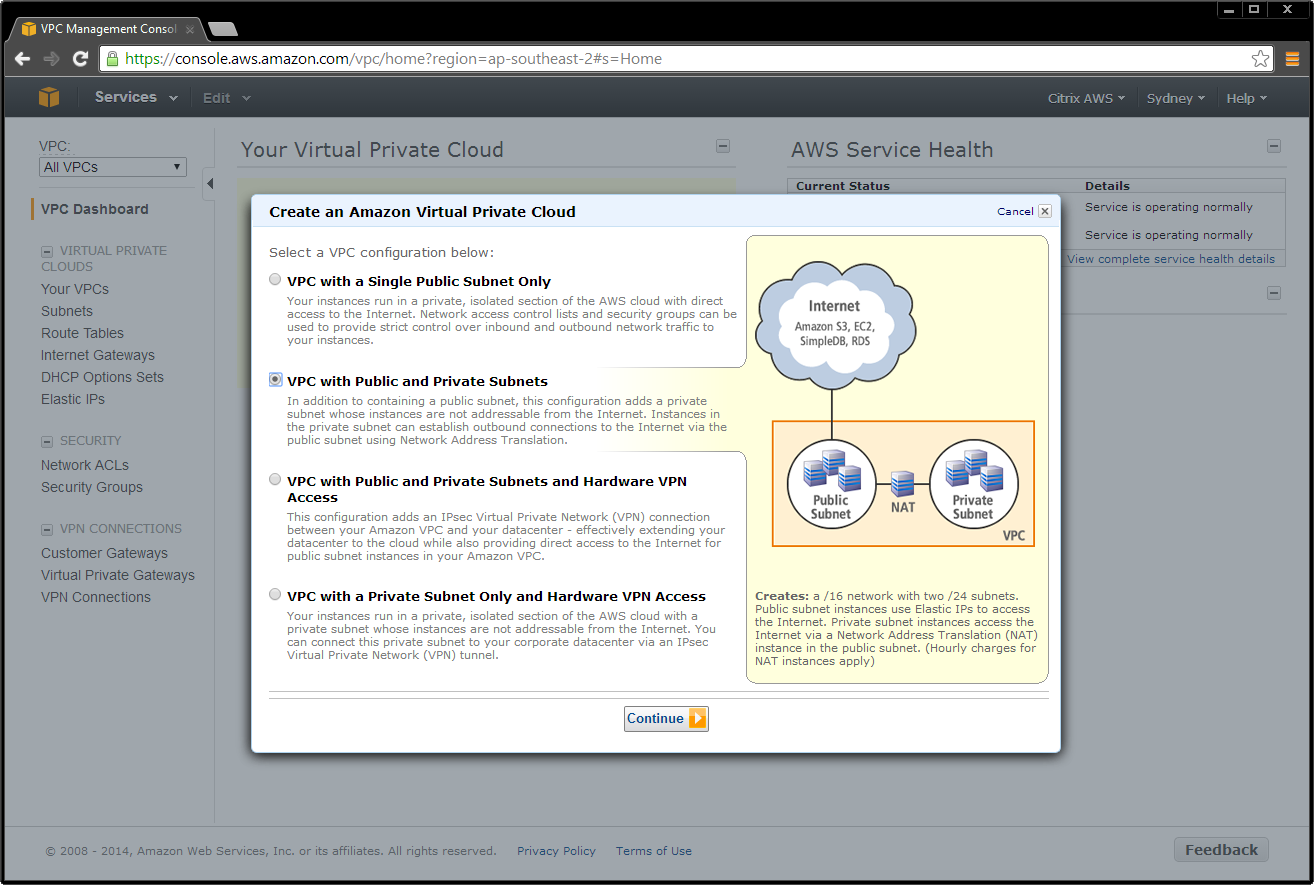
The security groups in Amazon VPC provide communication between the Internet and public network, and the public and private network. The security groups contain ACLs and are the basis of the firewalls for the subnets and instances used in this deployment.

You must create the following security groups:

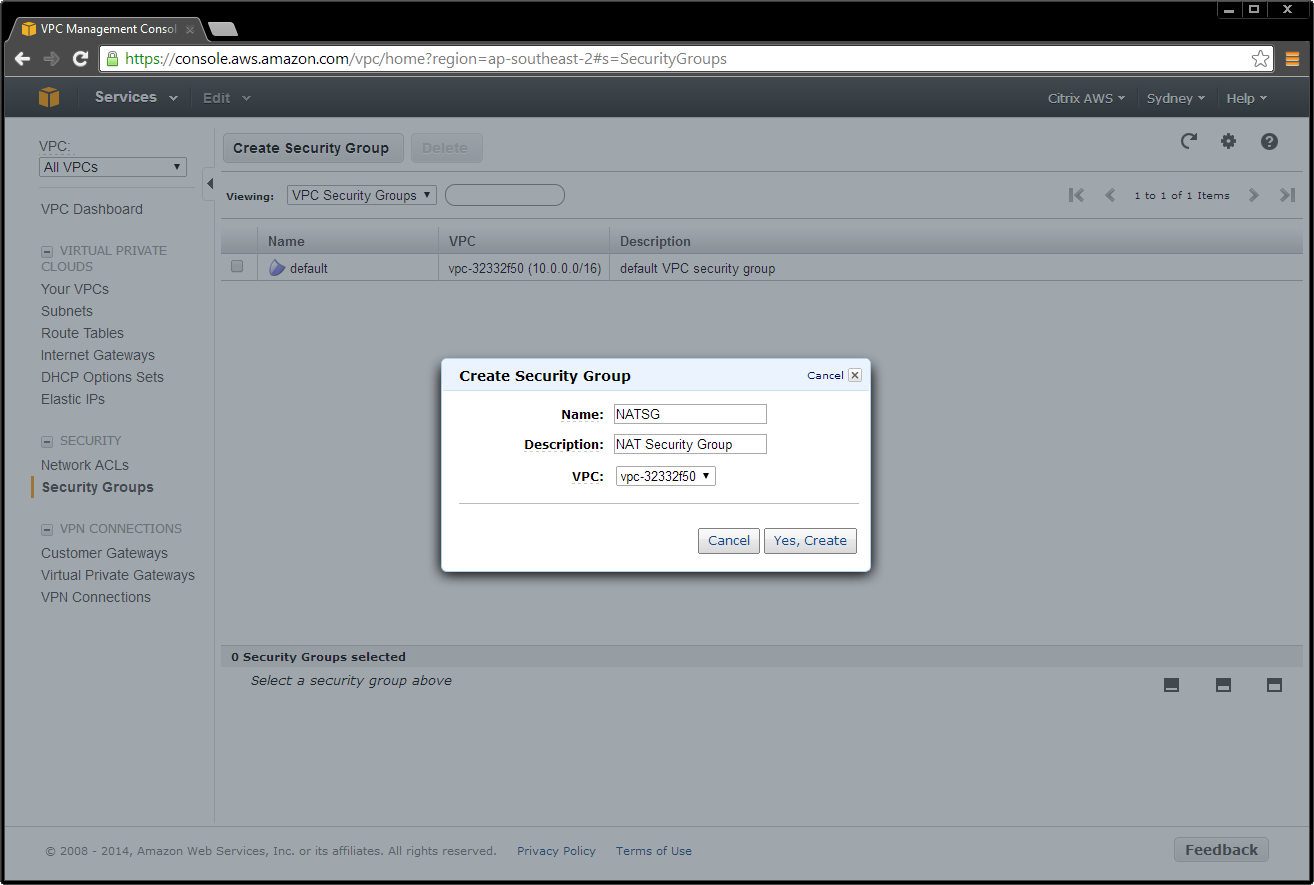
* NAT security group
* Public security group
* Private security group

##### Add NAT Security Group

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



1. Add ACL rules for inbound and outbound traffic. Select:
   1. Create a new rule
   2. Port number
   3. 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.

Create ACL rules to match the inbound and outbound traffic table (see Table 3).

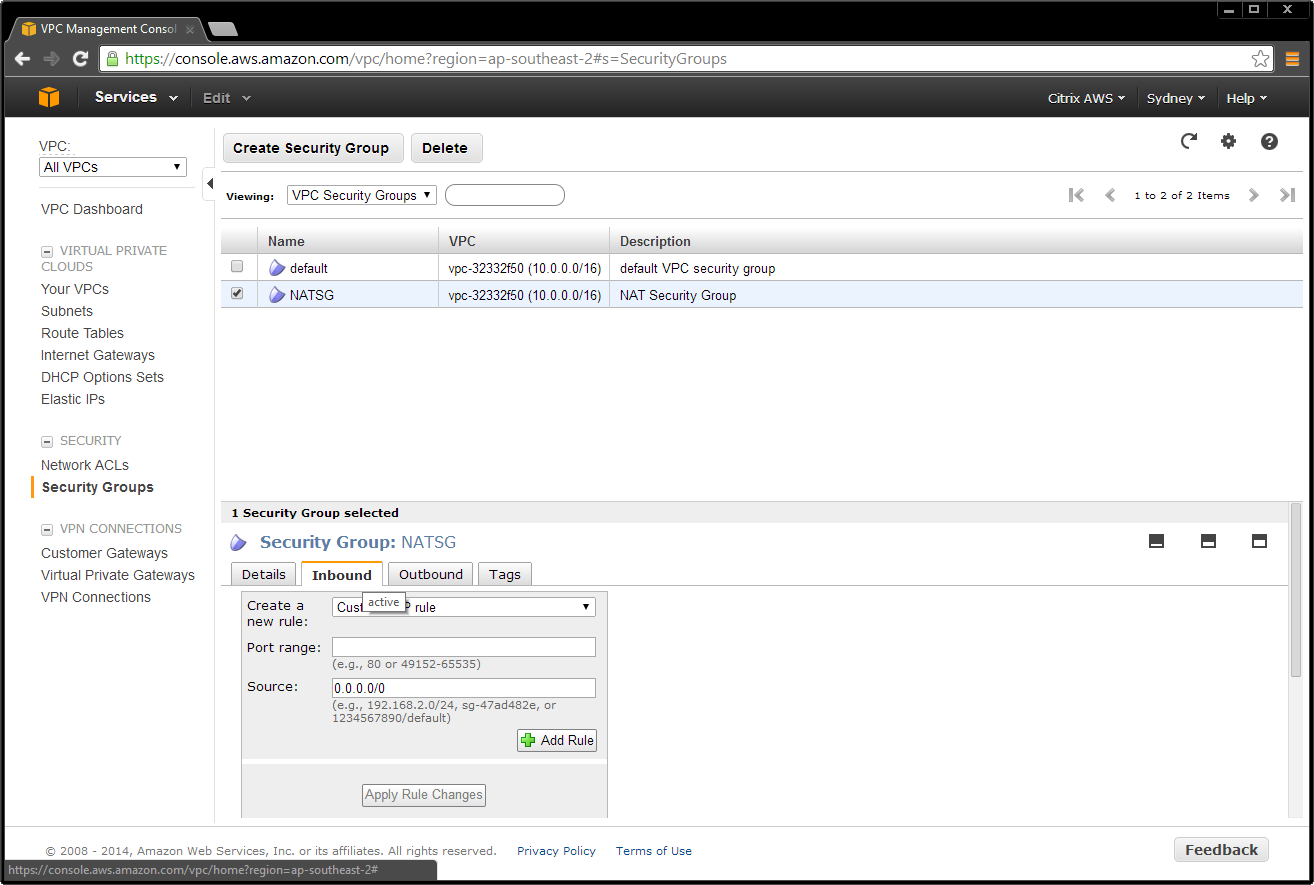


Table . NAT security group rules.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 |  |  |  |

#### Routing packets to the Internet

To be able to sent packets to the Internet an instance must have an [external IP address](https://cloud.google.com/compute/docs/instances_and_network#externaladdresses). If you create a route that sends packets to the Internet from a particular instance, that instance must also have an external IP. If you create a route that sends packets to the Internet gateway, but the source instance doesn't have an external IP address, the packet will be dropped.

#### Configuring a NAT gateway

You can create more complicated networking scenarios by making changes to the Routes collection. This section describes how you can set up a network address translation (NAT) gateway instance that can route traffic from our internal-only virtual machine instances to the Internet. This allows you to use one external IP address to send traffic from multiple virtual machine instances but only expose a single virtual machine to the Internet.

Create a virtual machine to act as a NAT gateway on the previously created xendesktop network

$ gcloud compute instances create nat-gateway --network xendesktop --can-ip-forward \  
         --zone us-central1-a \  
         --image debian-7 \  
         --tags nat

[Tag](https://cloud.google.com/compute/docs/instances#tags) any virtual machine instances without an external IP address that will use the gateway instance with the tag internal, or create a new virtual machine without an external IP address and tag the instance with the internal tag.

# Add tags to an existing instance ...  
$ gcloud compute instances add-tags existing-instance --tags internal  
  
# Or create a new virtual machine without an external IP address  
$ gcloud compute instances create example-instance --network xendesktop --no-address --zone us-central1-a --image "https://www.googleapis.com/compute/v1/projects/windows-cloud/global/images/windows-server-2008-r2-dc-v20150511" --tags internal

Create a route to send traffic destined to the Internet through your gateway instance.

$ gcloud compute routes create internal-internet-route --network xendesktop \  
         --destination-range 0.0.0.0/0 \  
         --next-hop-instance nat-gateway \  
         --next-hop-instance-zone us-central1-a \  
         --tags internal --priority 800

Setting the priority of this route ensures that this route wins if there are any other conflicting routes. 1000 is the default priority and a value lower than 1000 will take precedent.

Next, log onto your NAT gateway instance and configure iptables to NAT internal traffic to the Internet.

$ gcloud compute ssh nat-gateway --zone us-central1-a

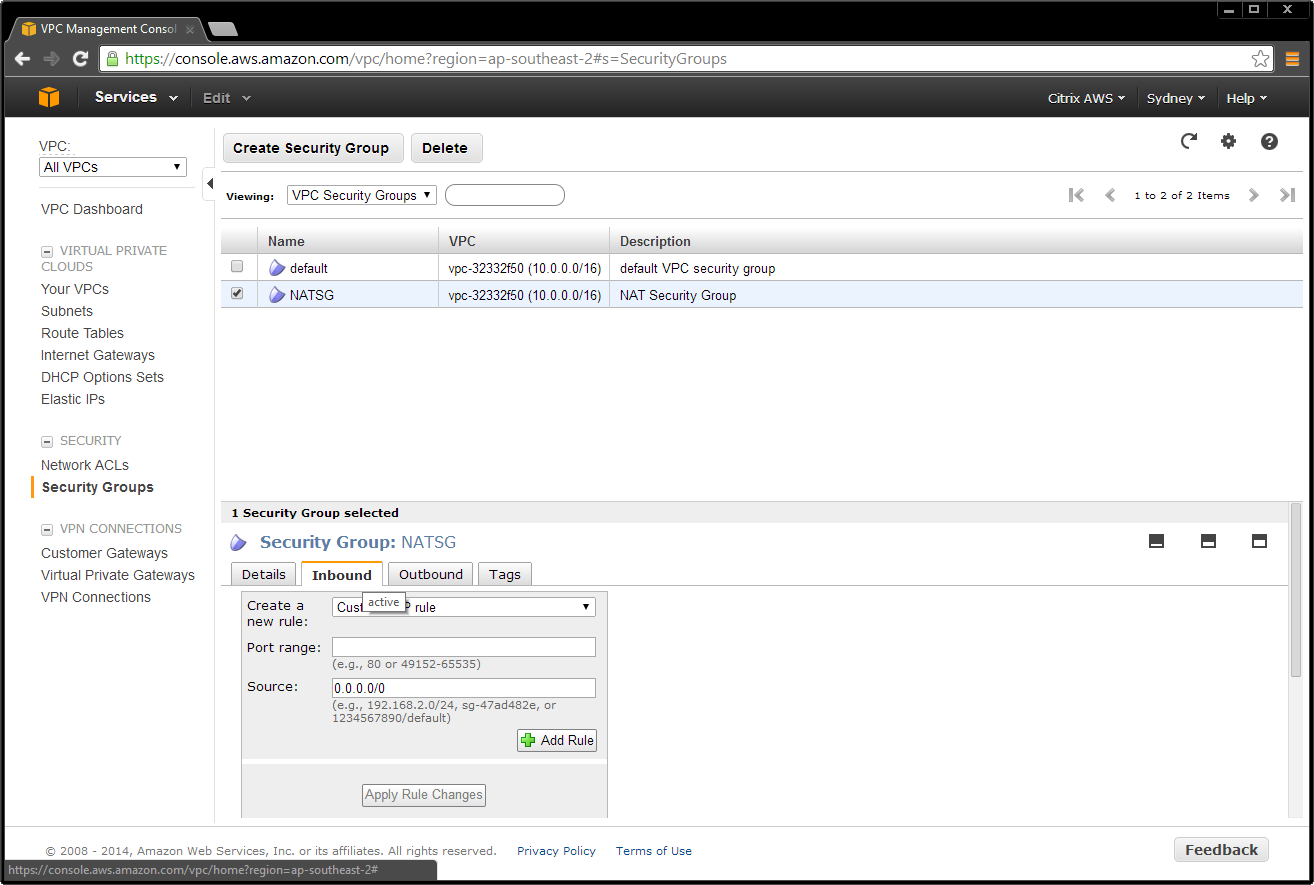
On your instance, configure iptables:

user@nat-gateway:~$ sudo sh -c "echo 1 > /proc/sys/net/ipv4/ip\_forward"  
user@nat-gateway:~$ sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

The first sudo command tells the kernel that you want to allow IP forwarding. The second sudo command masquerades packets received from internal instances as if they were sent from the NAT gateway instance.

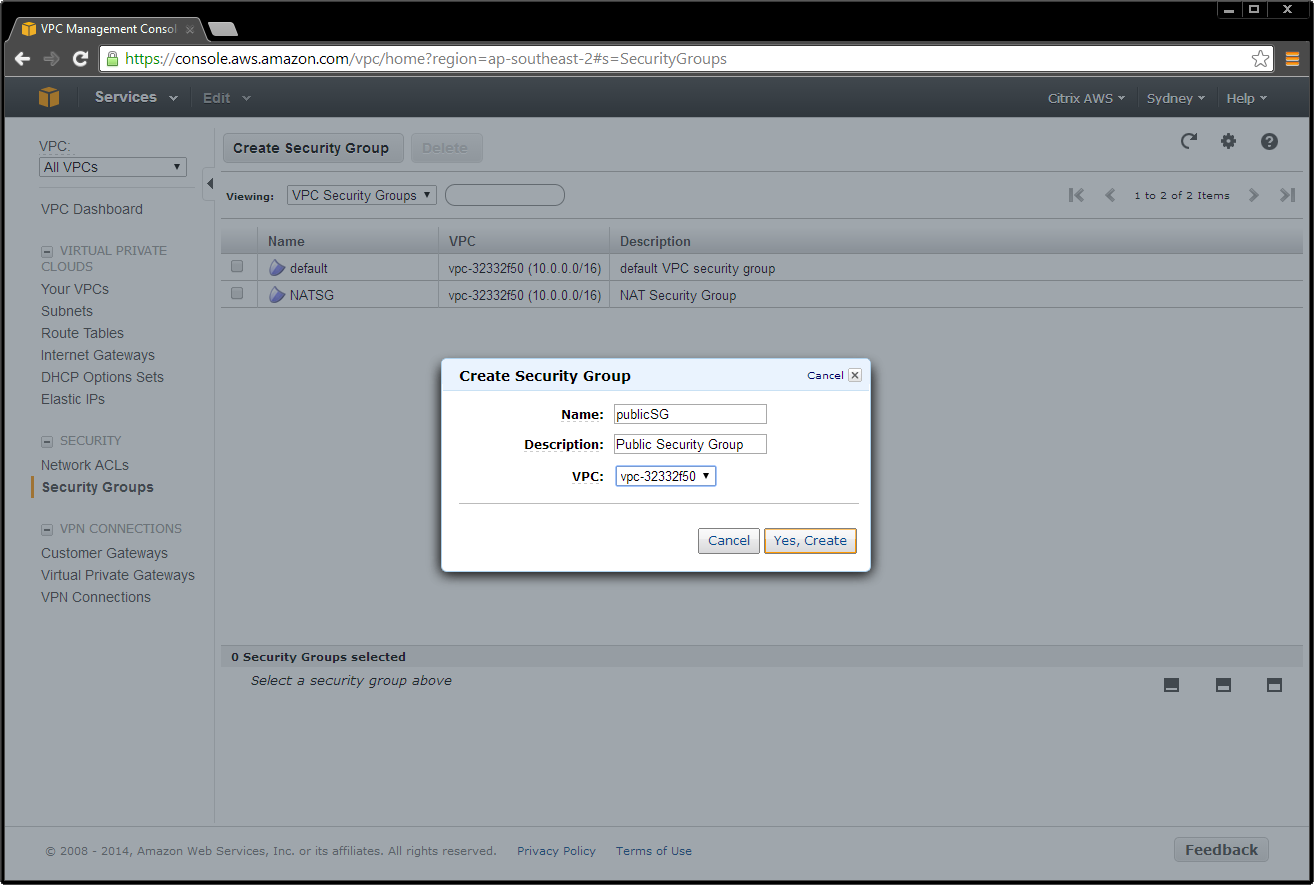
**Note:** You should also consider saving these commands in a [startup script](https://cloud.google.com/compute/docs/howtos/startupscript) because these settings will not persist if the instance is rebooted. It is also useful to have these settings saved, in case you want to start a new NAT gateway virtual machine.

1. 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**.



1. Add ACL rules for inbound and outbound traffic. Select:
   1. Create a new rule
   2. Port number
   3. 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 public network security group (publicSG) rules table (see Table 4).

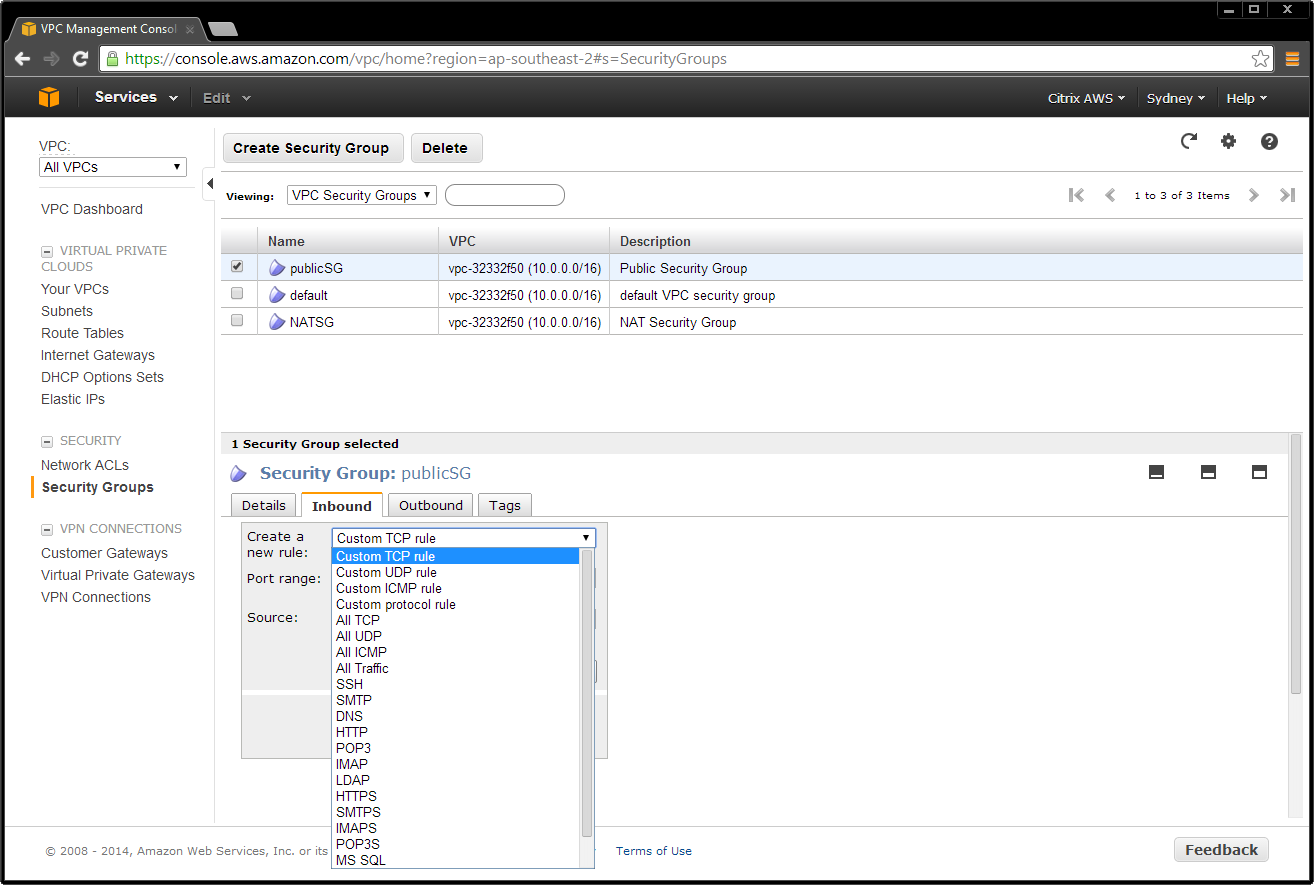


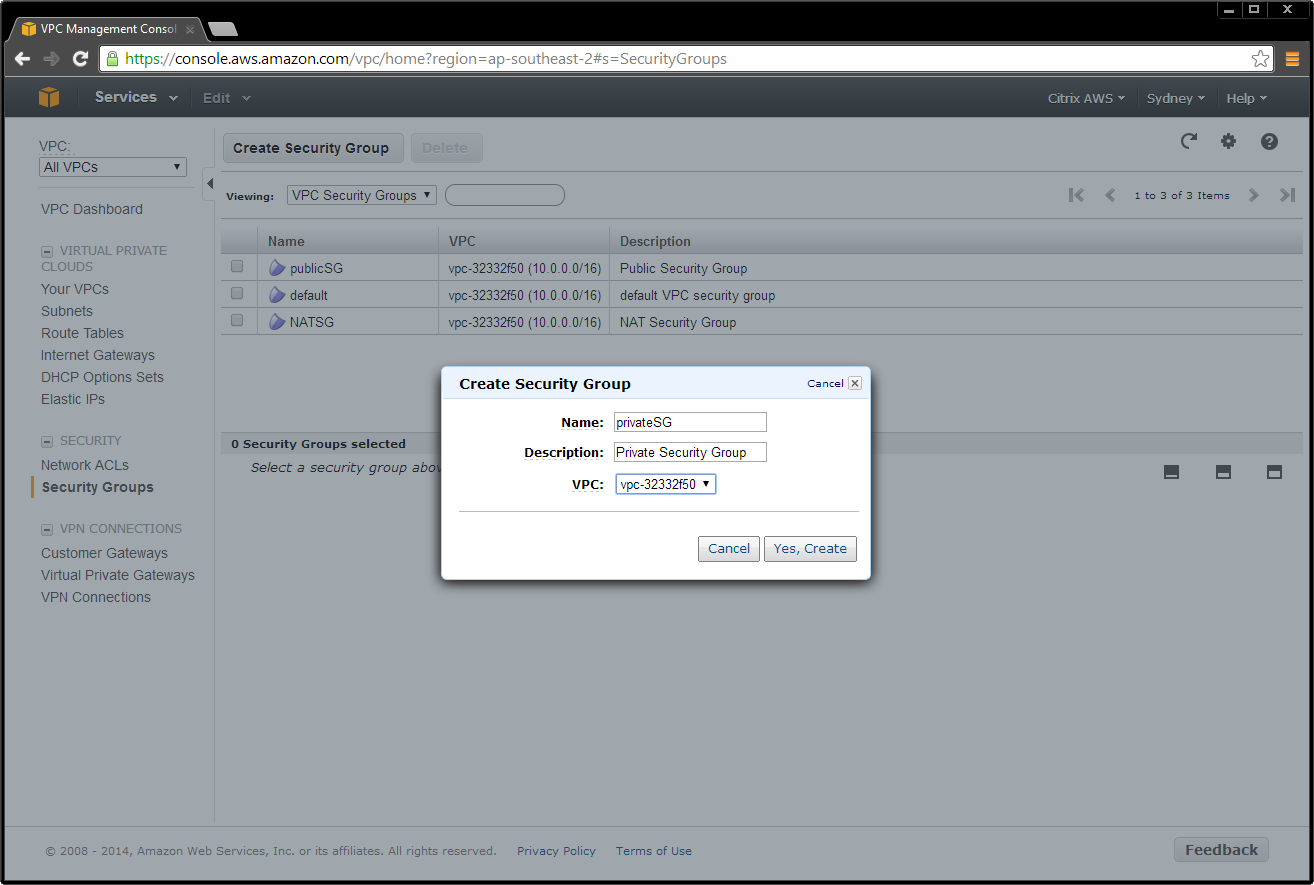
Table . Public network security group (publicSG) rules.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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**.



1. Add ACL rules for inbound and outbound traffic. Select:
   1. Create a new rule
   2. Port number
   3. 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 private network security group (privates) rules table (see Table 5).

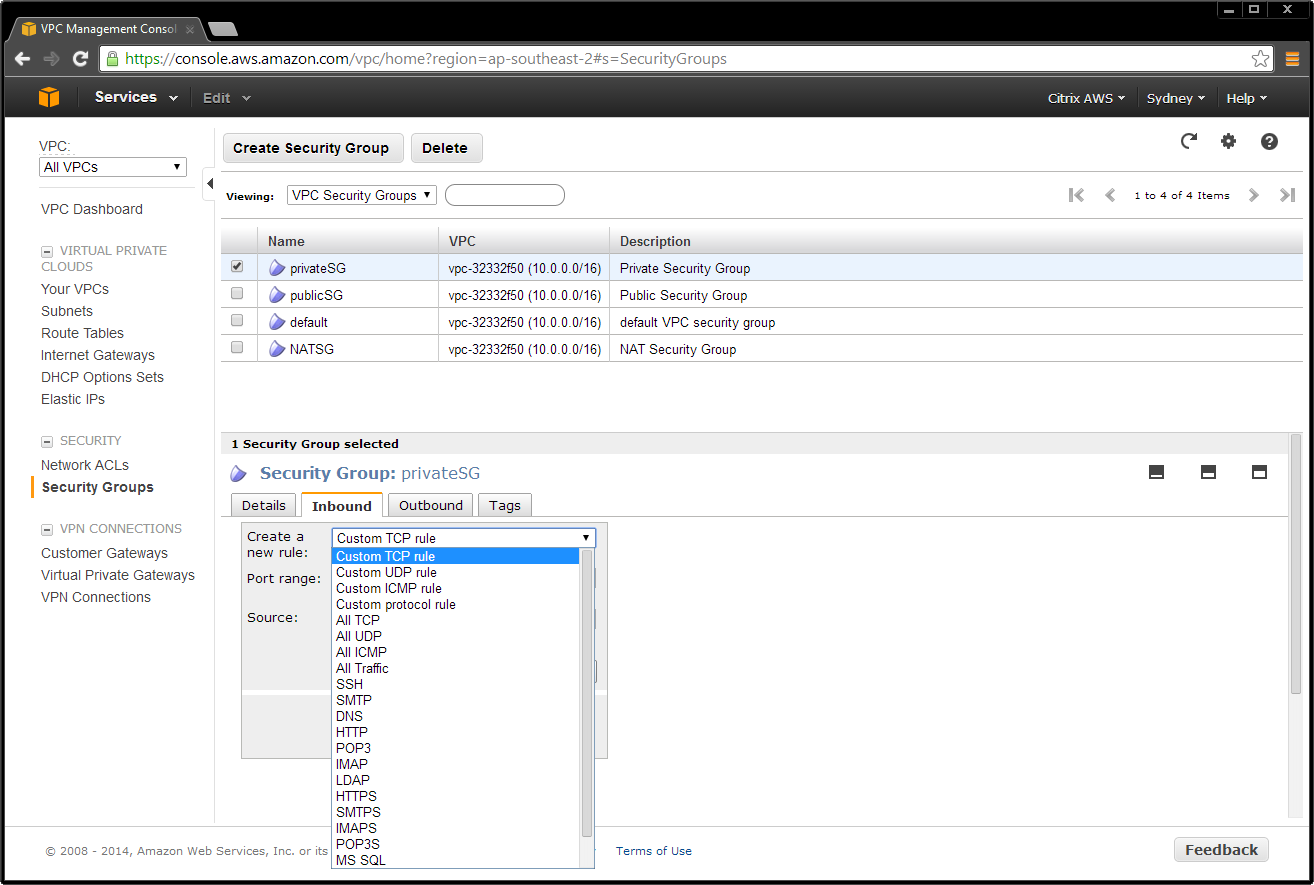


Table . Private network security group (privateSG) rules.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Inbound | | | Outbound | | |
| **Type** | **Traffic** | **Source** | **Type** | **Traffic** | **Source** |
| All | All | NATSG | All | All | 0.0.0.0/0 |
|  | All | privateSG |  | All | privates |
| ICMP | All | publicSG | ICMP | All | 0.0.0.0/0 |
| TCP | 54 (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 |  |  |  |

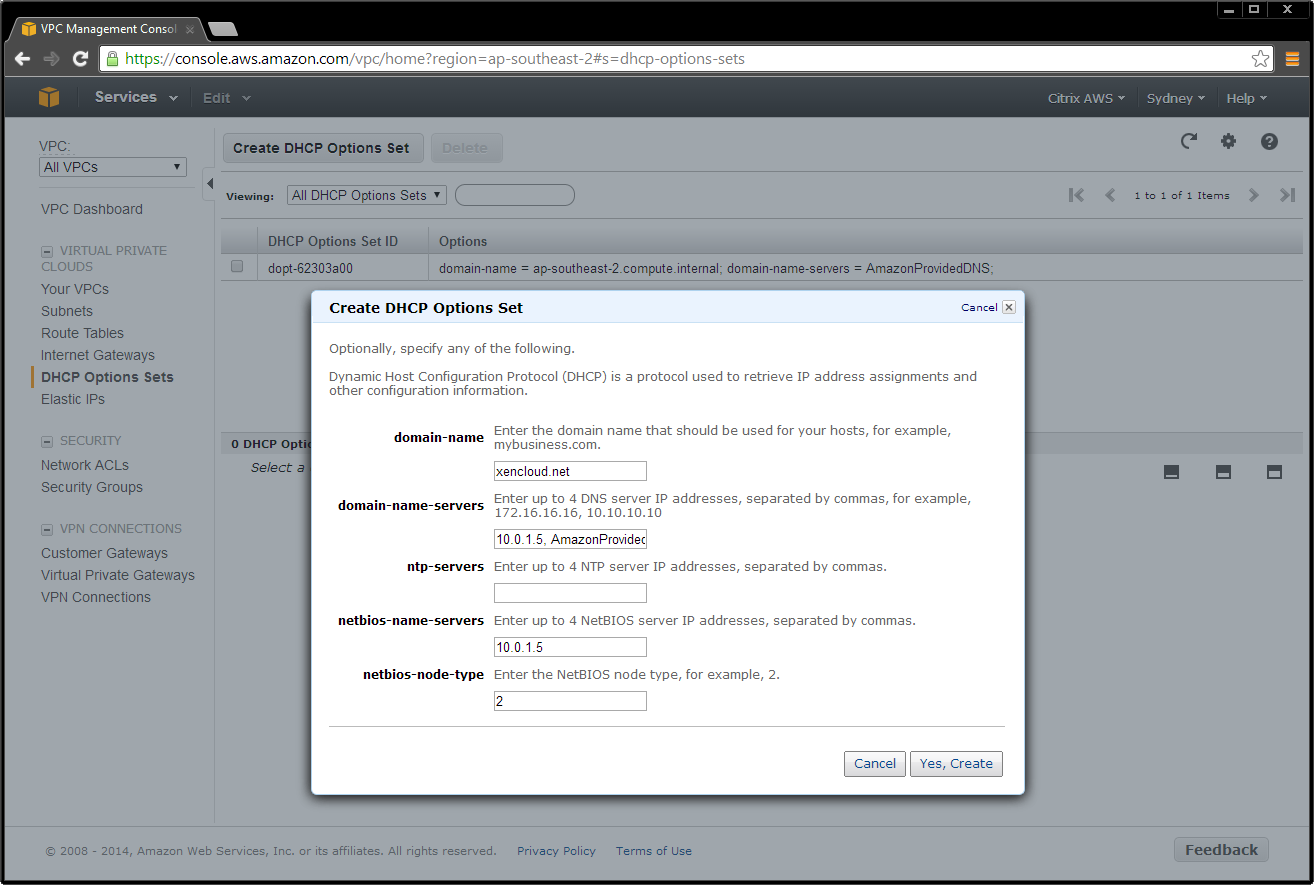
#### Configure DHCP Options

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:

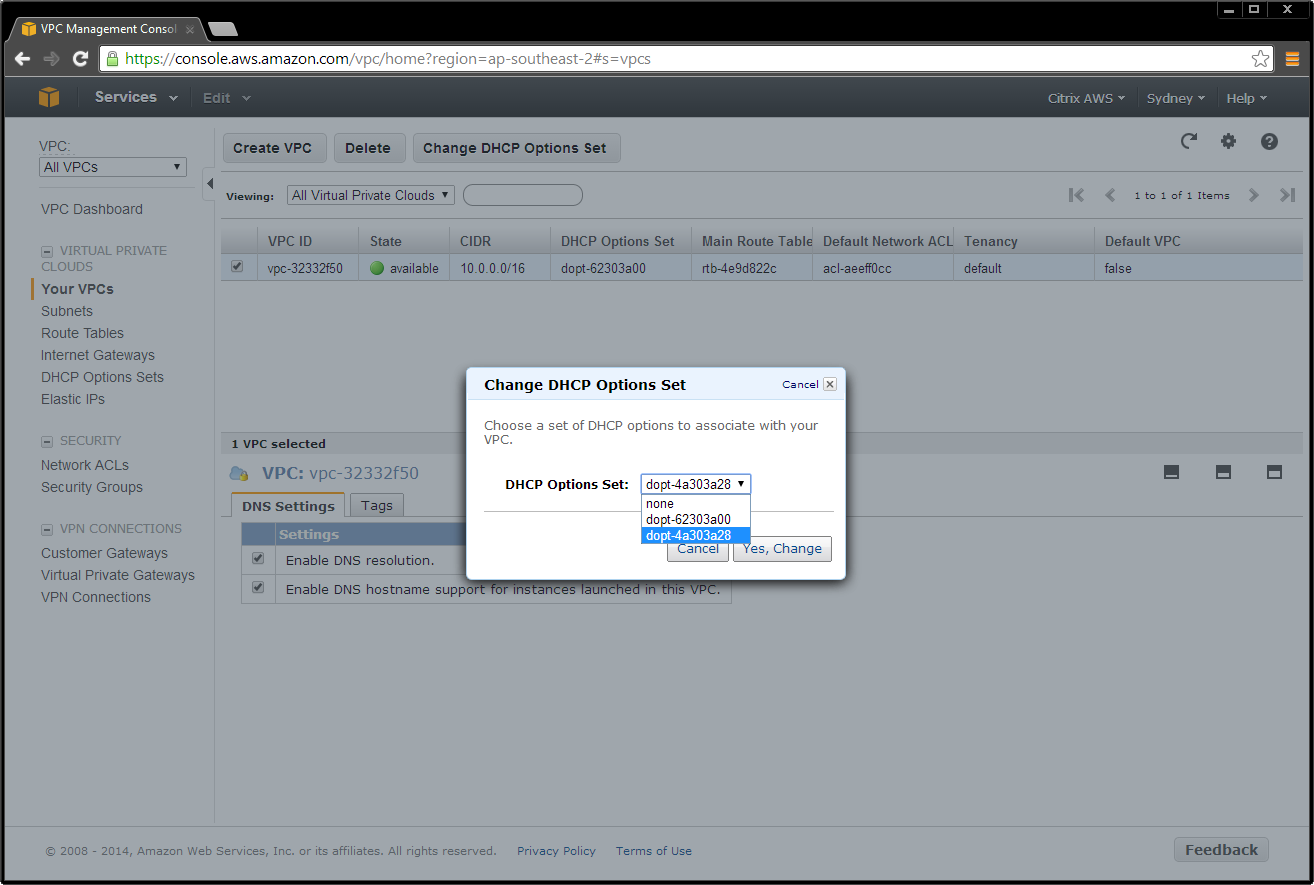
* Create a new DHCP options set that contains your DNS server IP address.
* Add an open-source DNS server on the Internet in case a server needs to access the Internet.

##### Create a DHCP Options Set

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



1. 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

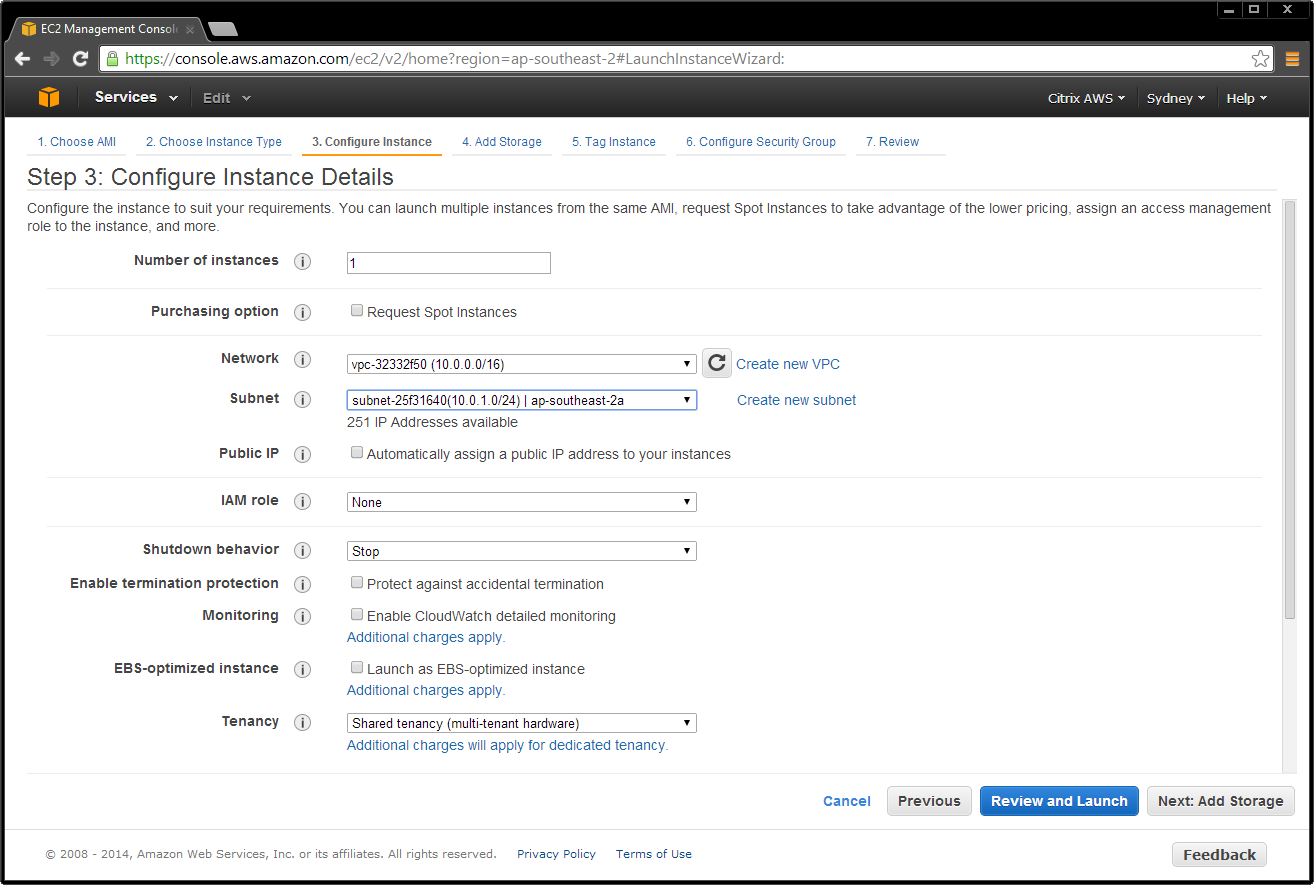
The following sections walk through setting up the following Amazon machine images (AMIs):

* Domain Controller AMI
* Remaining XenApp or XenDesktop AMIs
* NetScaler AMI

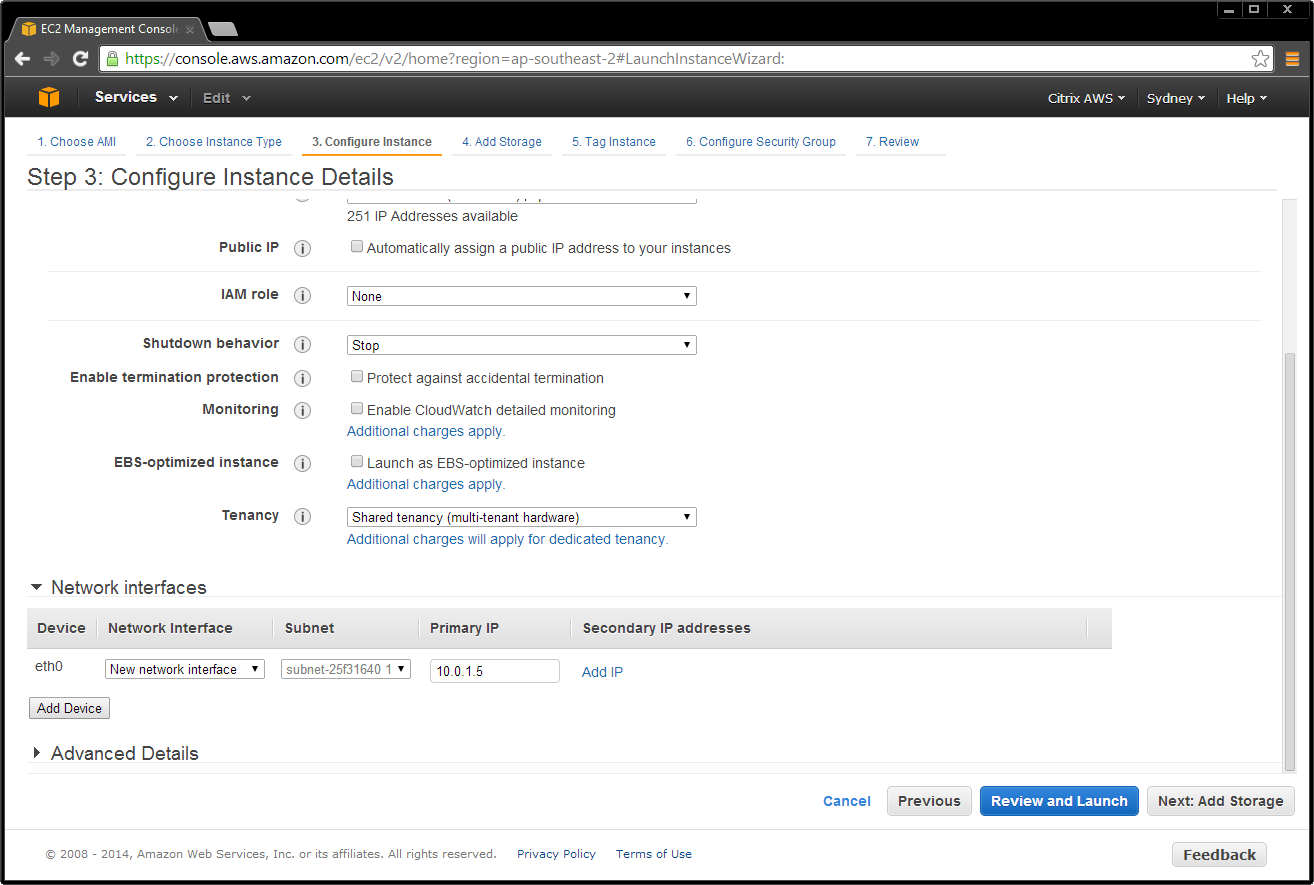
#### Launch and Configure a Domain Controller Amazon Machine Image (AMI)

Create a domain controller for the site as follows:

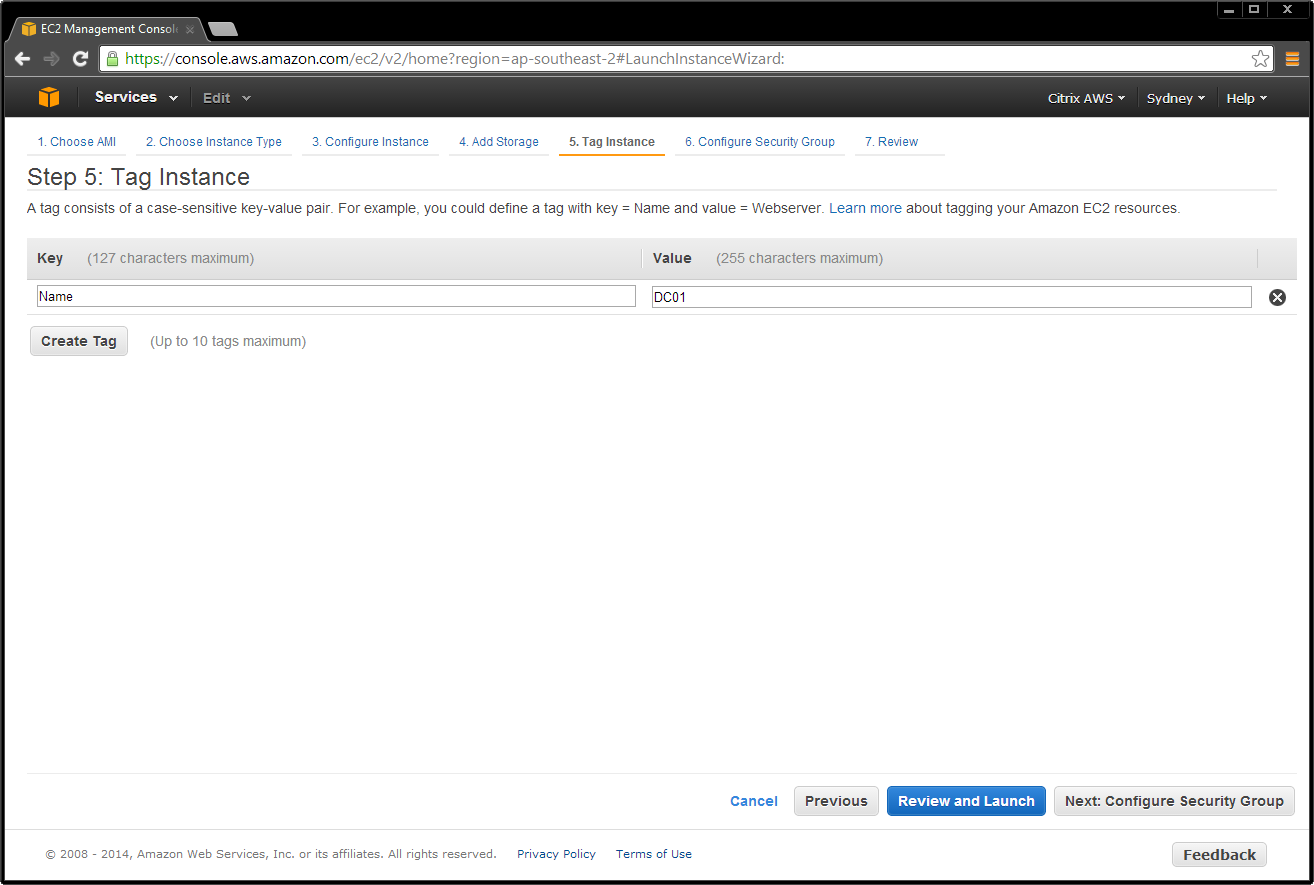
1. Select **AMI**s in the EC2 tab**.**
2. Depending on operating system you use, perform a search in the Amazon AMIs for **Windows Server 2012 Base** or **Windows Server 2008 R Base**. Ensure that the machine is deployed to your subnet, and make sure it is in the private subnet 10.0.1.0/24**.**



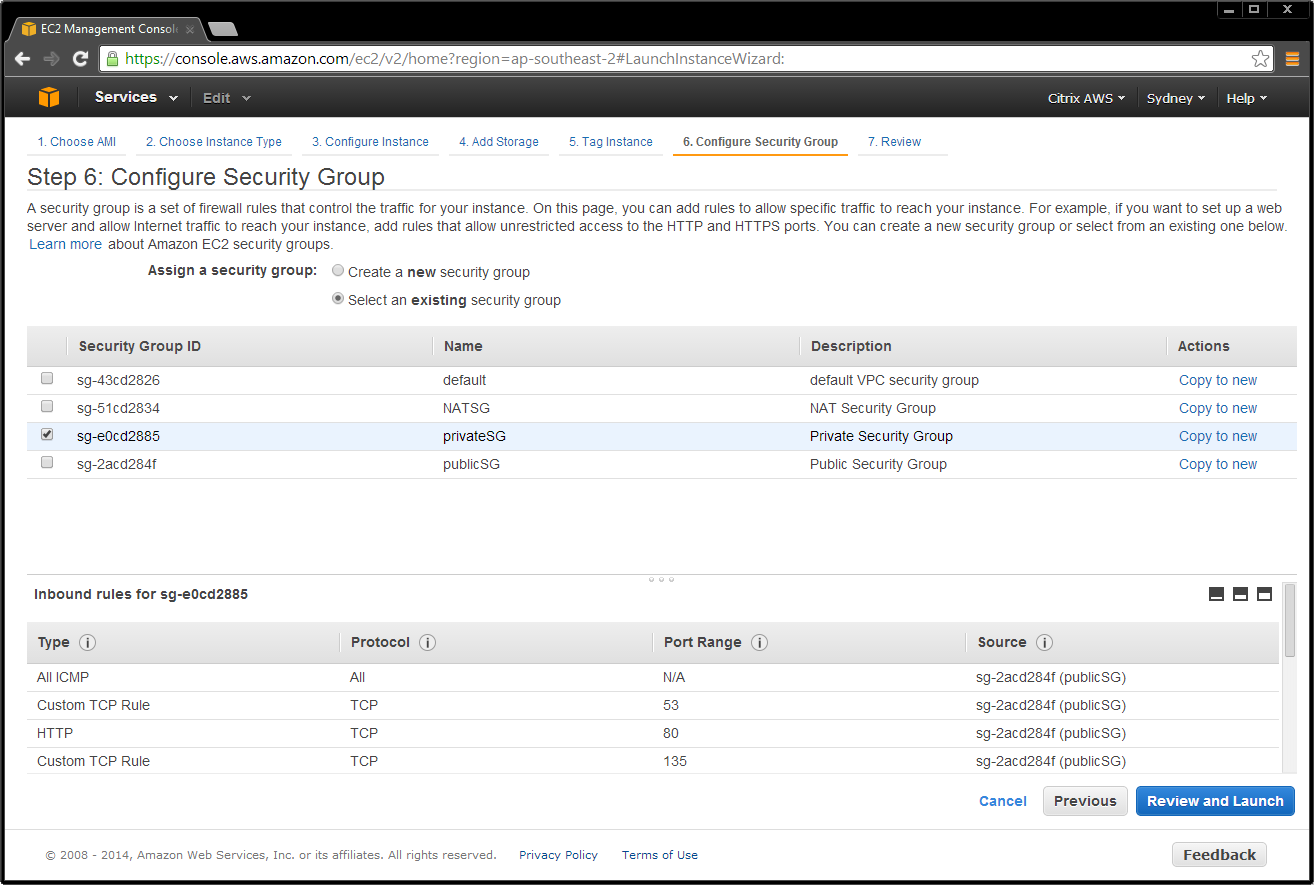
1. Assign the IP address for this server.



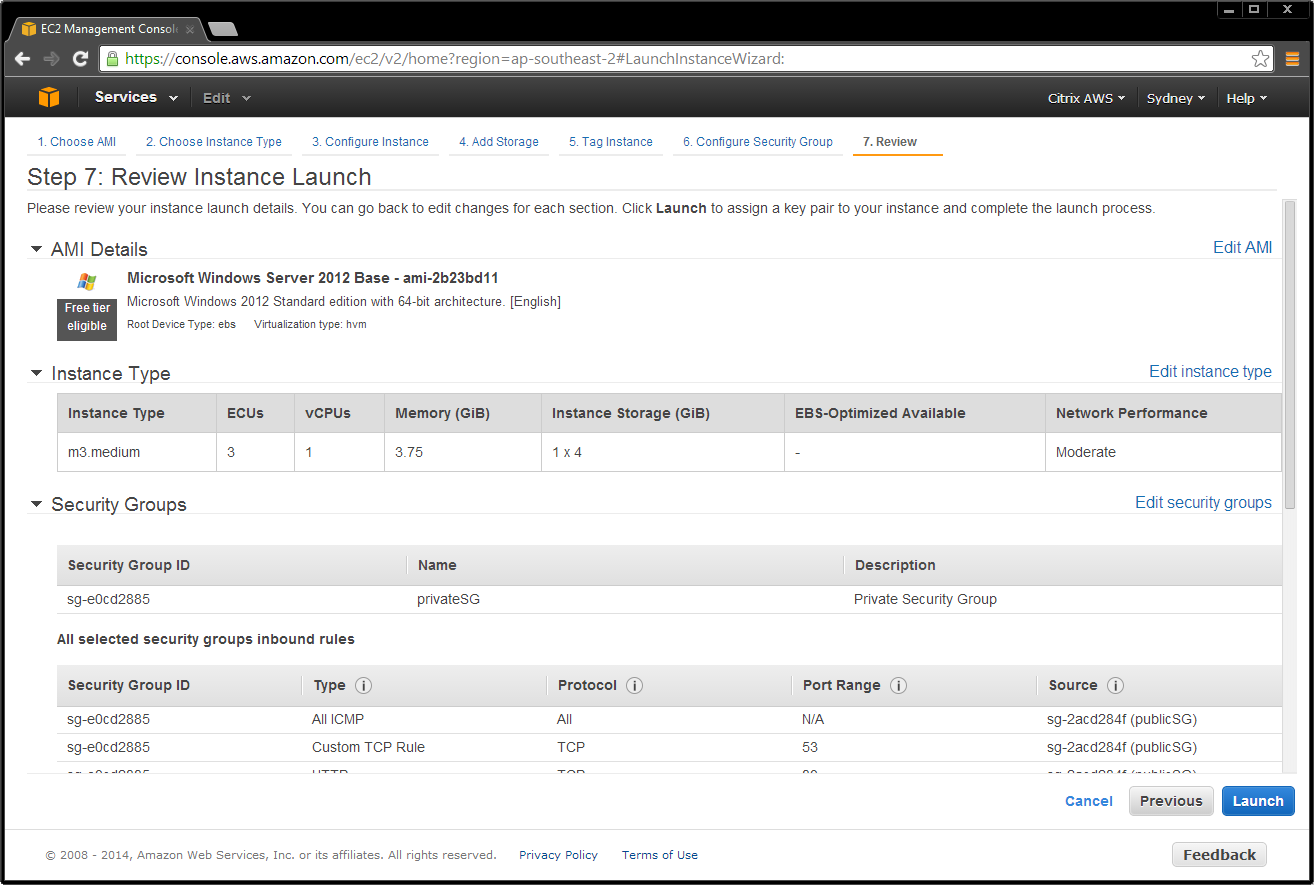
1. Assign a friendly name to the AMI to make it easily identifiable in the Amazon console.



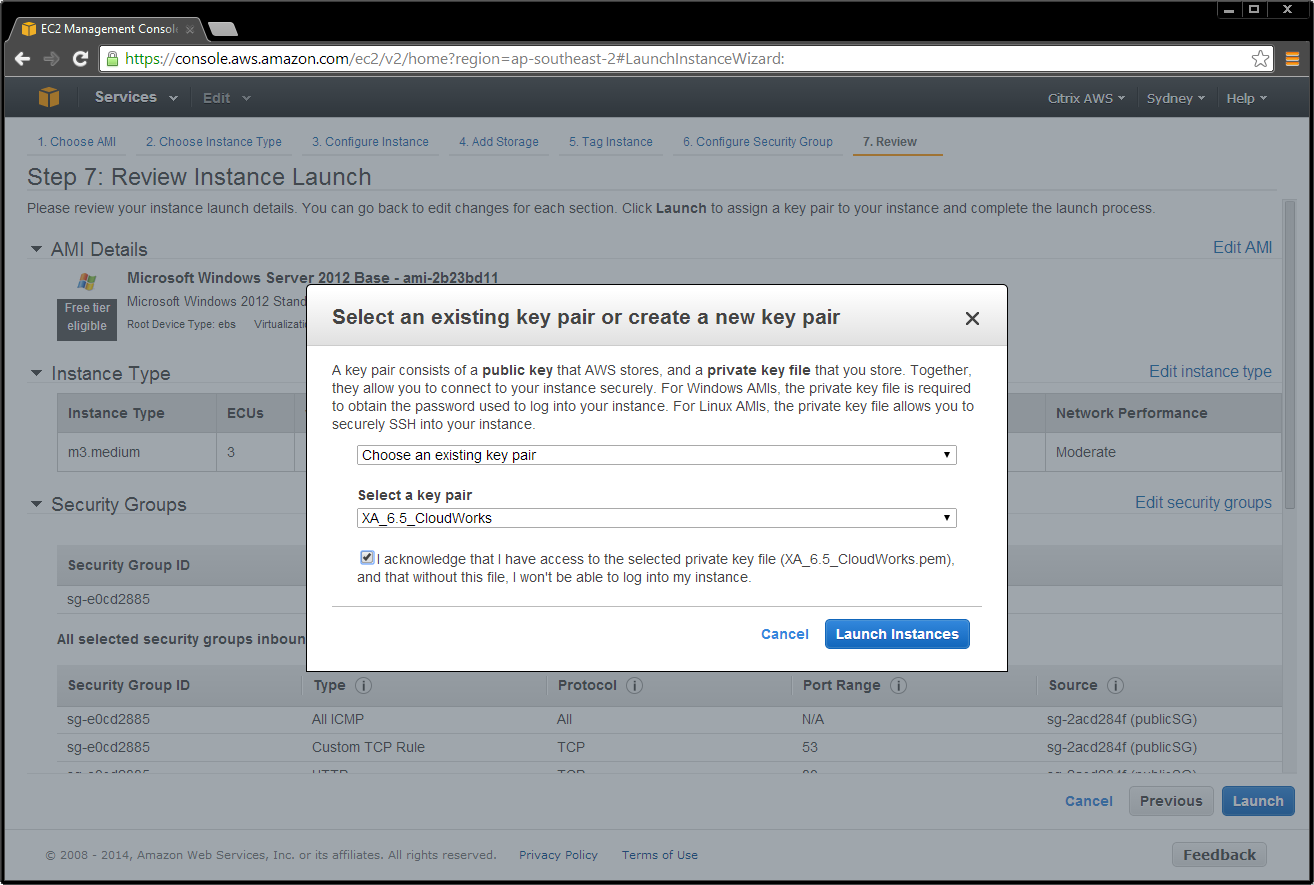
1. Place the domain controller in the network by launching the AMI into the appropriate network and security group. This example places the domain controller in the private network.



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



1. Choose an existing AWS key pair, or create a new one.

****

#### Launch Remaining XenApp or XenDesktop AMIs

Launch the remaining XenApp or XenDesktop AMIs using the parameters in Table 6. (Note that AMI IDs will change per region and after release of updates by AWS.) 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.

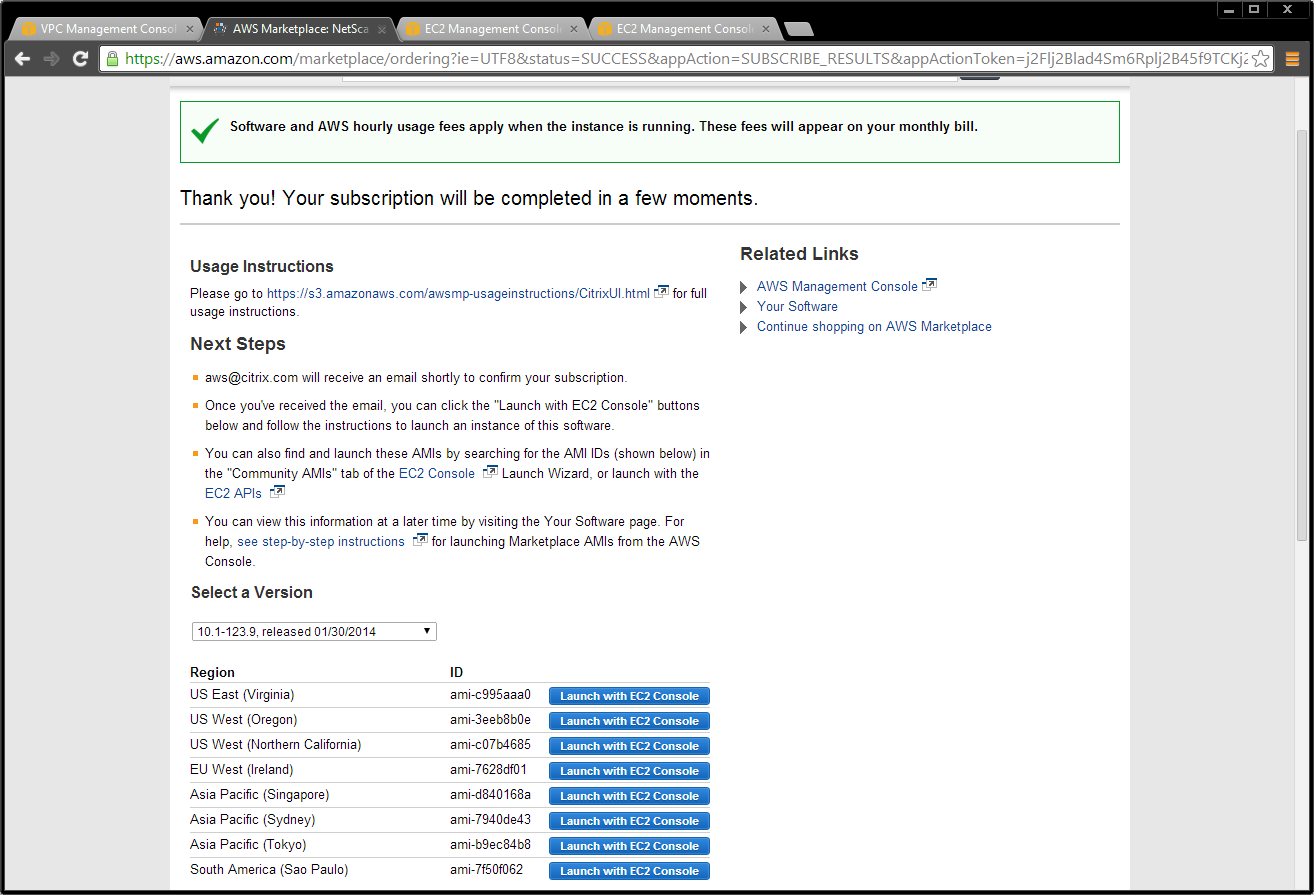
Table . XenApp / XenDesktop AMI parameters per function for AWS region US-East-1.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Function | AMI Name | AMI ID | Network | IP Address |
| Domain Controller | Microsoft Windows Server 2012 Base | ami-aede32c6 | private | 10.0.1.5 |
| Microsoft Windows Server 2012 R2 Base | ami-088c6460 | private | 10.0.1.5 |
| Microsoft Windows Server 2012 R2 Base | ami-9ed834f6 | private | 10.0.1.5 |
| Delivery Controller | Microsoft Windows Server 2012 with SQL Standard | ami-eed83486 | private | DHCP |
| Microsoft Windows Server 2012 R2 with SQL Standard | ami-048c646c | private | DHCP |
| Microsoft Windows Server 2008 R2 with SQL | ami-acd539c4 | private | DHCP |
| VDA Master | Microsoft Windows Server 2012 Base | ami-aede32c6 | private | DHCP |
| Microsoft Windows Server 2012 R2 Base | ami-088c6460 | private | DHCP |
| Microsoft Windows Server 2008 R2 Base | ami-9ed834f6 | private | DHCP |
| Bastion | Microsoft Windows Server 2012 Base | ami-aede32c6 | public | DHCP |
| Microsoft Windows Server 2012 R2 Base | ami-088c6460 | public | DHCP |
| Microsoft Windows Server 2008 R2 Base | ami-9ed834f6 | public | DHCP |
| NetScaler VPX | [NetScaler VPX Platinum Edition - 10 Mbps](https://aws.amazon.com/marketplace/pp/B00A9ZLKFK) | ami-a55c44cc | public/private | 10.0.1.100 |

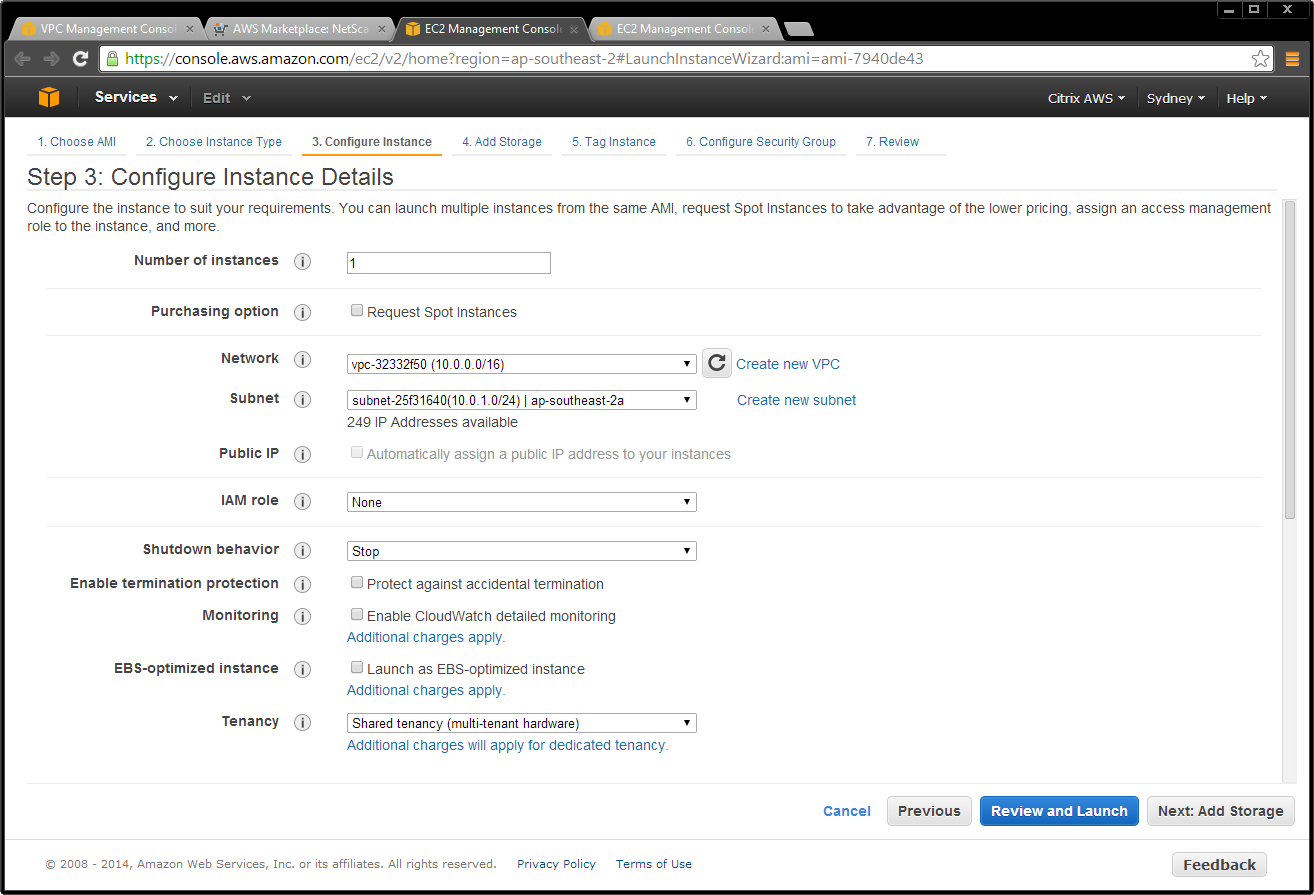
#### Launch the NetScaler AMI

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/awsmp-usageinstructions/CitrixUI.html>.

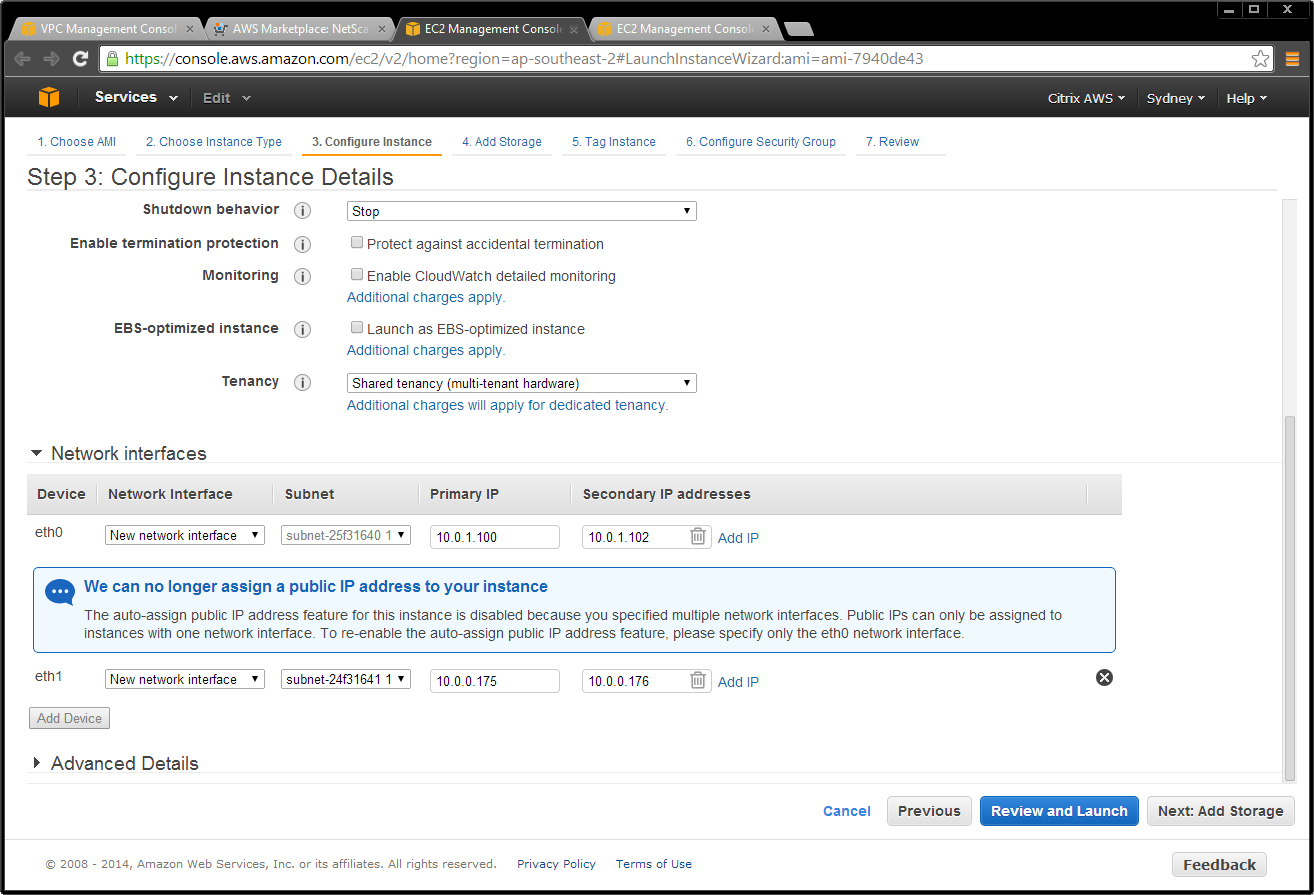


1. Deploy the instance into the private subnet.

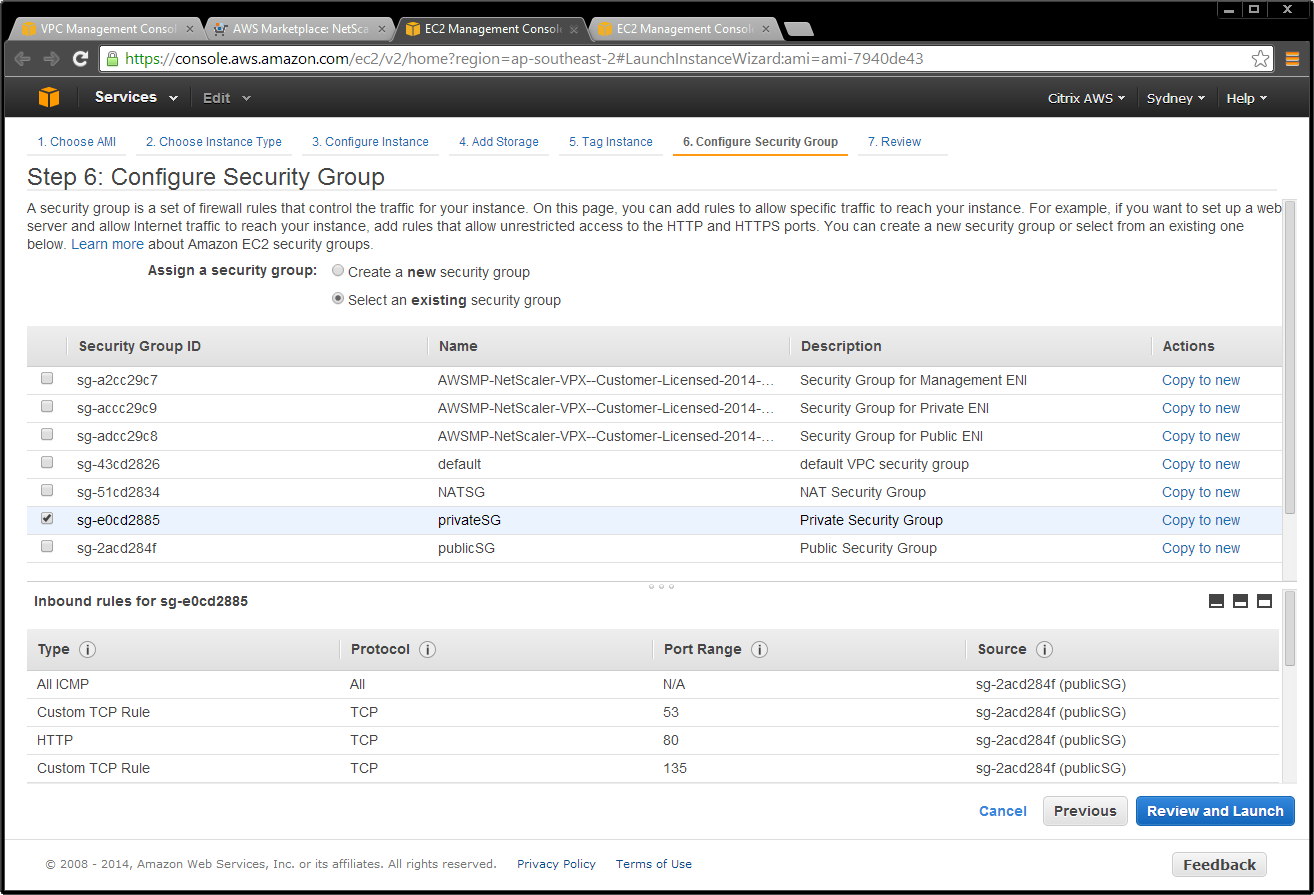


1. Ensure that this instance has two interfaces:

* Public subnet
* Private subnet:
  + eth0 is connected to the private subnet
  + Primary IP address (NSIP) is 10.0.1.100
  + Secondary IP address (SNIP) is 10.0.1.102

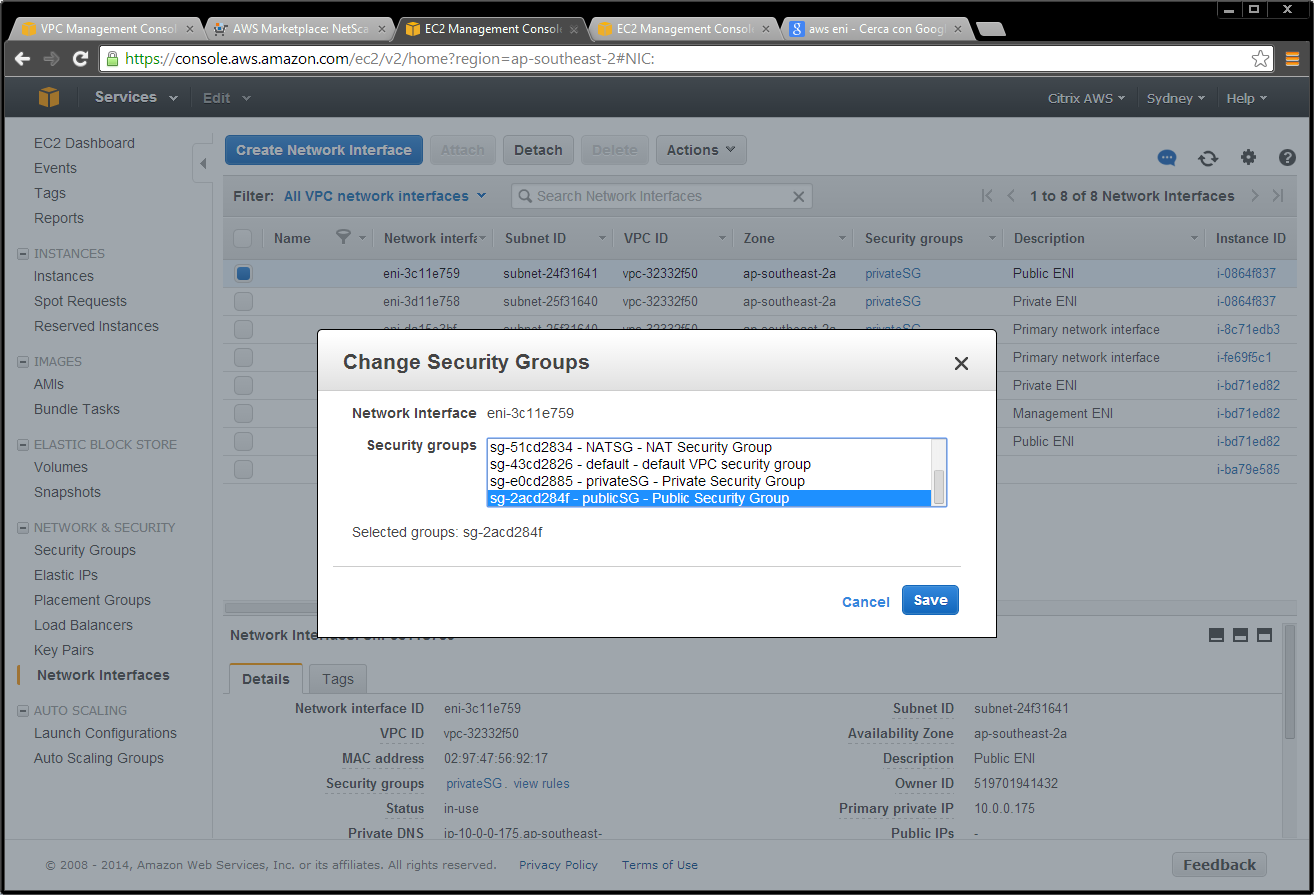


1. Deploy the instance into the private security group.

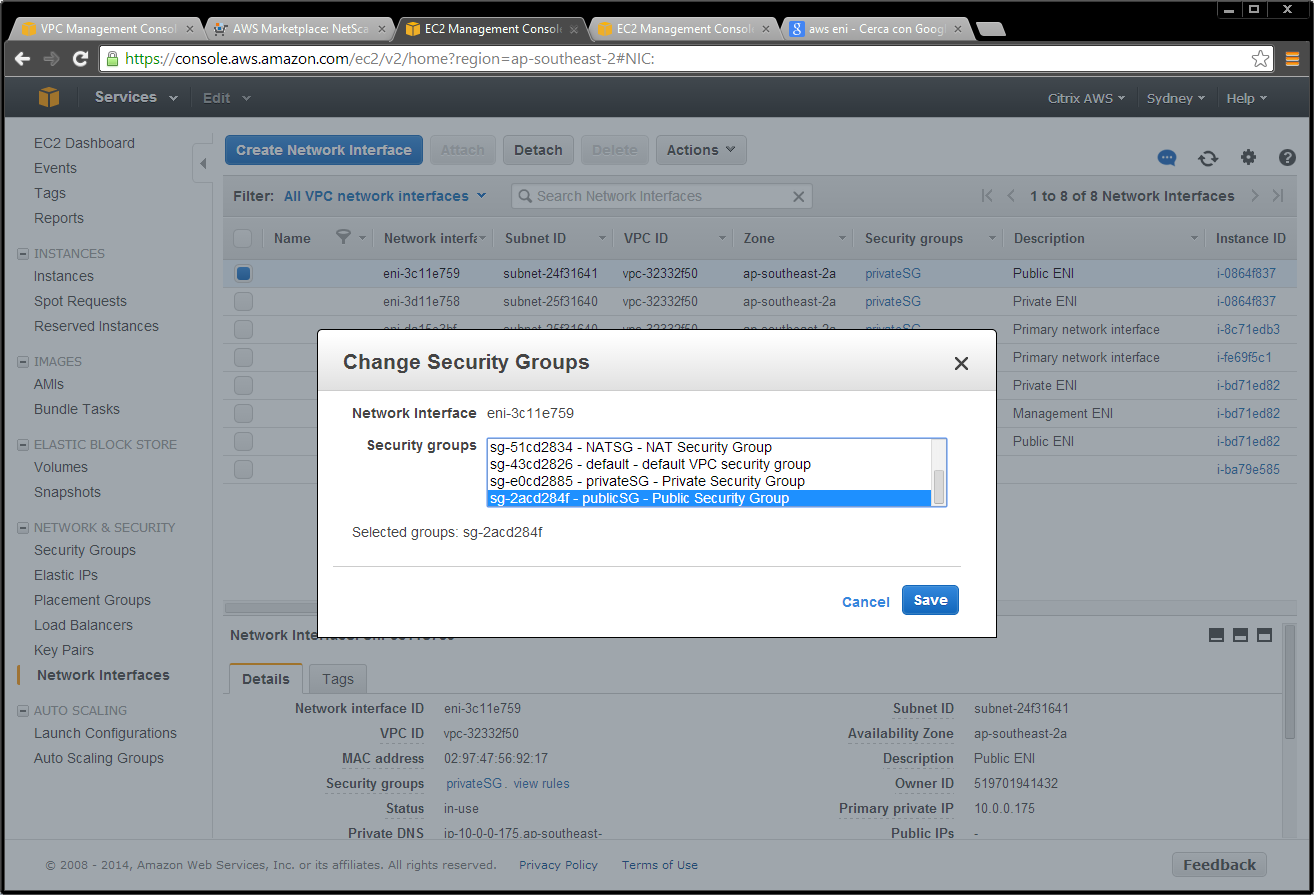


1. Configure the NetScaler AWS elastic network interfaces (ENIs) to be part of their respective security groups.

* 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.
  1. Public ENI – Public Security Group:

****

* 1. Private ENI – Private Security Group:



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



Once the networking and compute instances are in place, the standard XenDesktop installation procedures as outlined in the product documentation can be followed. There are no special considerations when implementing XenDesktop delivery controllers or worker servers within AWS as proposed in this sample design.

## Conclusion

By cross-referencing the Citrix Project Accelerator and XenDesktop Modular Reference Architecture, Contoso was able to implement a hybrid XenDesktop solution spanning the Contoso on-premises enterprise datacenter and AWS’s EC2 environment. Leveraging public cloud infrastructure such as AWS virtually eliminated any need for a new Contoso capital investment, allowing them to bring their new service online quickly in a globally available, state-of-the-art cloud-hosted infrastructure.

By leveraging Citrix XenDesktop 7.5, Contoso was capable of providing an industry-leading desktop virtualization solution, ensuring the best user experience across any device, as enabled by Citrix technologies such as [HDX](http://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-hdx-technologies.pdf)™.

### Additional Resources

[Citrix XenDesktop Product Web Site](http://www.citrix.com/products/xendesktop/overview.html)

[Citrix XenDesktop Modular Reference Architecture](http://support.citrix.com/servlet/KbServlet/download/30706-102-697507/XD%20-%20Modular%20Reference%20Architecture.pdf) [pdf]

[How to Deploy Xenapp and Xendesktop with Amazon Web Services](http://support.citrix.com/article/CTX140427)

[Flexing to the Cloud with Citrix XenDesktop and Amazon Web Services](https://citrix.sharefile.com/d/s87be5ee38a24b578)

[NetScaler On AWS Overview](http://www.citrix.com/products/netscaler-application-delivery-controller/platforms/aws.html)

[Citrix Project Accelerator](http://project.citrix.com/)

[Amazon Web Services Web Site](http://aws.amazon.com/)

[Citrix HDX technologies](http://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-hdx-technologies.pdf)