



Deployment Guide

Security Groups
Amazon EC2

Table of Contents

Introduction	3
Solution Requirements	4
Prerequisites.....	4
Additional Information	4
Network Diagram	5
IP Addresses	6
Security Group 1 - Public Facing	6
Security Group 2 - Private Facing	6
Amazon EC2.....	7
Create Security Groups	7
Configure Security Groups	9
Security Group 1.....	11
Security Group 2.....	14

Introduction

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. It is designed to make web-scale computing easier for developers. Amazon EC2's simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity, both up and down, as your computing requirements change. Amazon EC2 changes the economics of computing by allowing you to pay only for capacity that you actually use. Amazon EC2 provides developers the tools to build failure resilient applications and isolate themselves from common failure scenarios.

By utilizing Amazon EC2, XenApp administrators can quickly build and deploy XenApp farms in the cloud to meet capacity demands, or simply grow an infrastructure at a lower cost of ownership.

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. It is designed to make web-scale computing easier for developers. Security Groups in Amazon EC2 allow you to separate different computing tiers for different degrees of separation.

This guide will walk through the steps to deploy Security Groups in the Amazon EC2 cloud, and apply them to a XenApp farm.

In order to setup a XenApp farm with Security Groups in EC2, you will need to sign up for the Amazon EC2 service.

Solution Requirements

- Security Groups for a XenApp farm in Amazon EC2

Prerequisites

- Citrix XenApp 5.0 Server Farm in Amazon EC2
- Amazon EC2 account

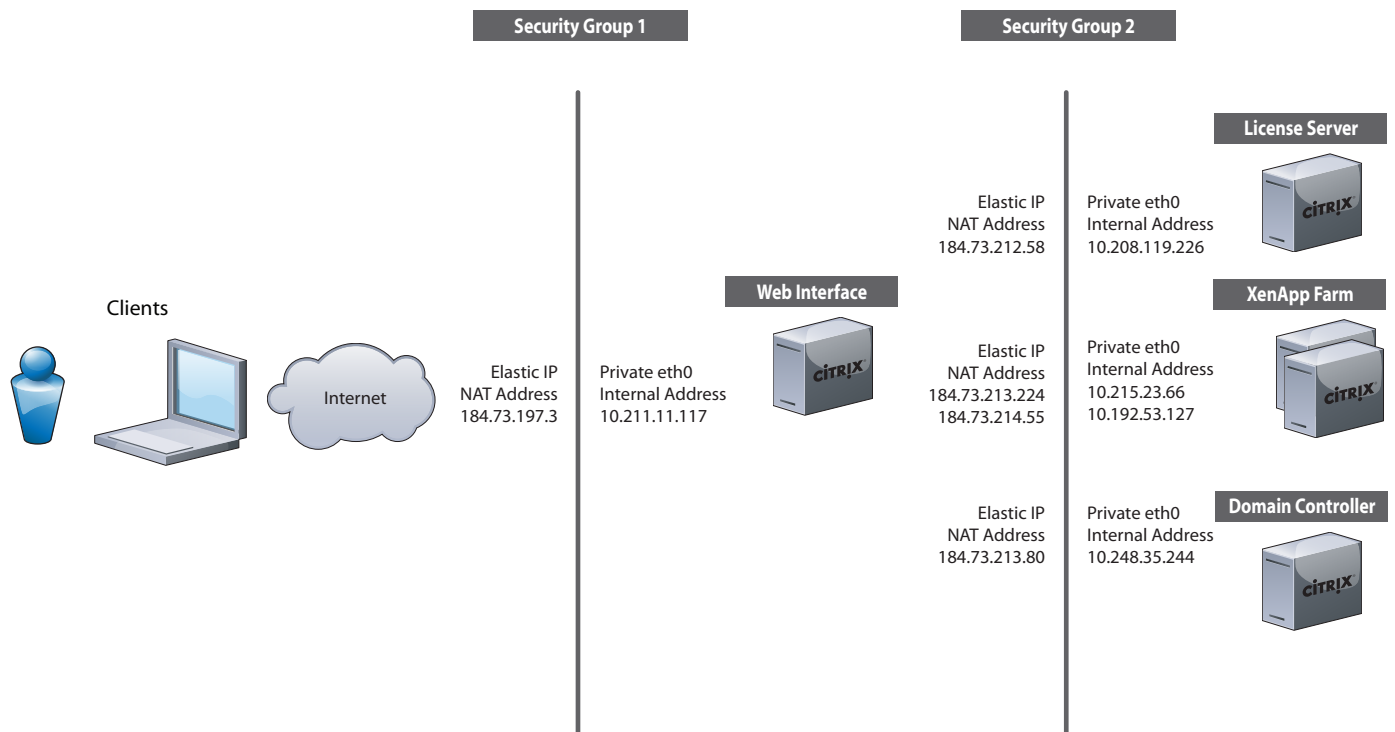
Additional Information

- <http://aws.amazon.com>
- <http://console.aws.amazon.com>

Network Diagram

The following is the Network that was used to develop this deployment guide.

Citrix XenApp "Amazon EC2" Logical Network Diagram



IP Addresses

Amazon Machine Image	IP Address
Active Directory, DNS	184.73.213.80
Citrix License Server	184.73.212.58
Citrix Web Interface/Secure Gateway	184.73.197.3
Citrix XenApp Server 1	184.73.213.224
Citrix XenApp Server 2	184.73.214.55

Security Group 1 - Public Facing

Method	Protocol	From Port	To Port	Source IP Address
HTTP	TCP	80	80	0.0.0.0/0
HTTPS	TCP	443	443	0.0.0.0/0

Security Group 2 - Private Facing

Method	Protocol	From Port	To Port	Source IP Address
HTTP	TCP	80	80	184.73.197.3/24
HTTPS	TCP	443	443	184.73.197.3/24
Custom	TCP	1494	1494	184.73.197.3/24
Custom	TCP	2598	2598	184.73.197.3/24

Amazon EC2

Create Security Groups

Connect to EC2:

Open a web browser and connect to:

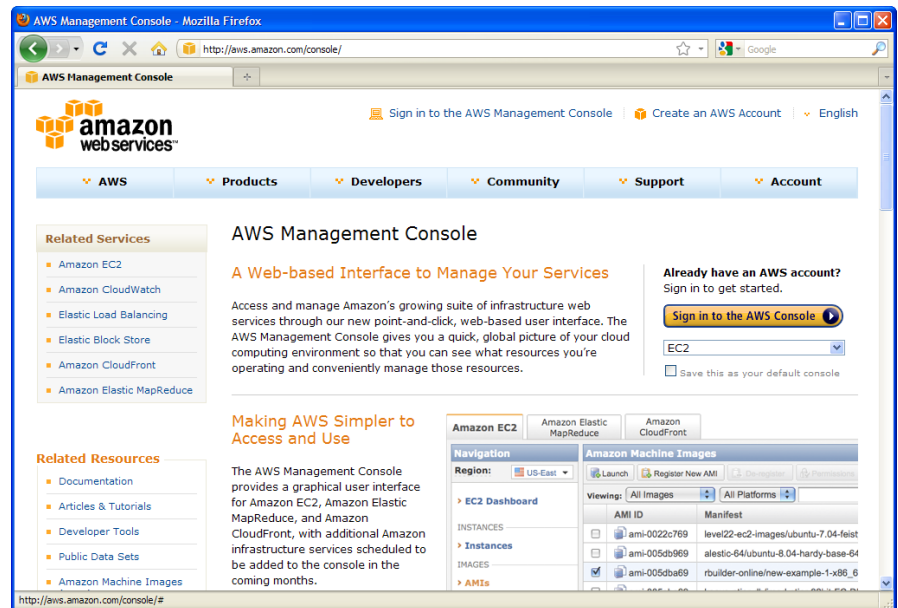
<http://aws.amazon.com/ec2/>



Connect to EC2:

Navigate to the EC2 console:

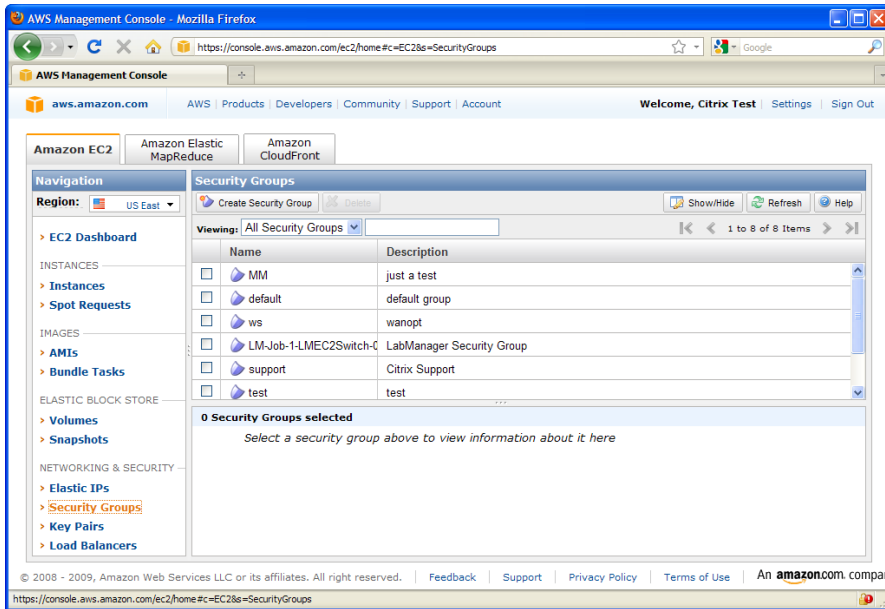
<http://console.aws.amazon.com/>



Create Security Group:

Once you have logged into the Amazon console, you will see the dashboard.

Select Security Groups.

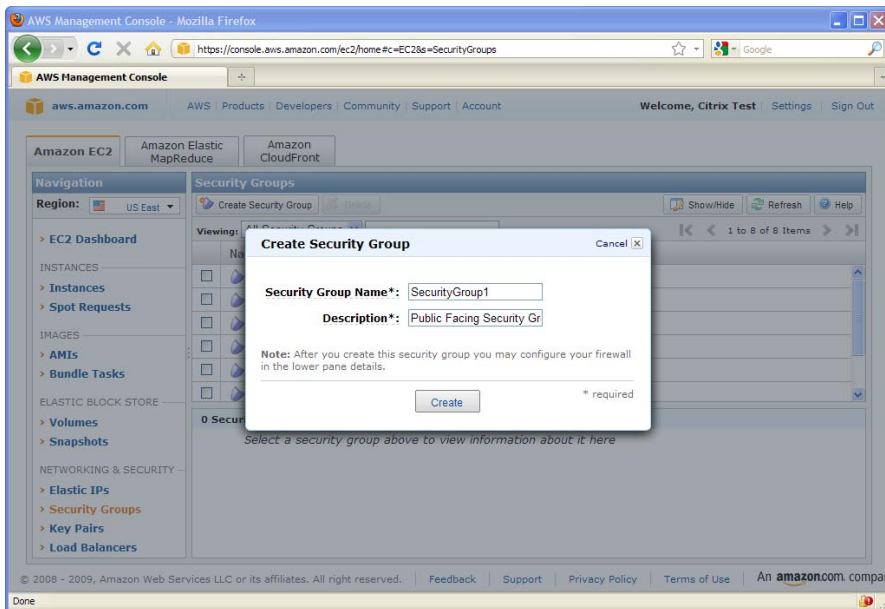


Create Security Group:

Select Create Security Group.

Name: Security Group 1

Desc: Public Facing

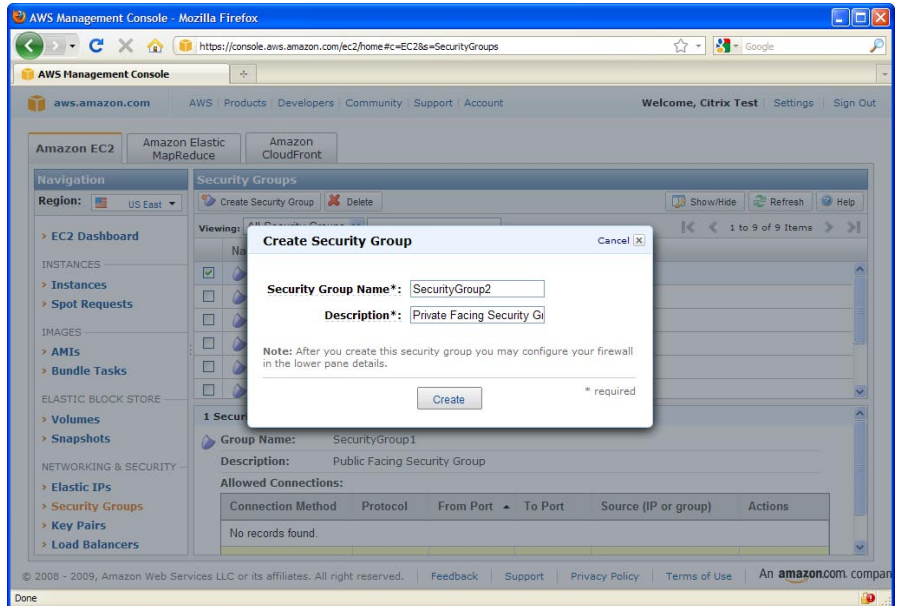


Create Security Groups:

Select Create Security Group again.

Name: Security Group 2

Desc: Private Facing



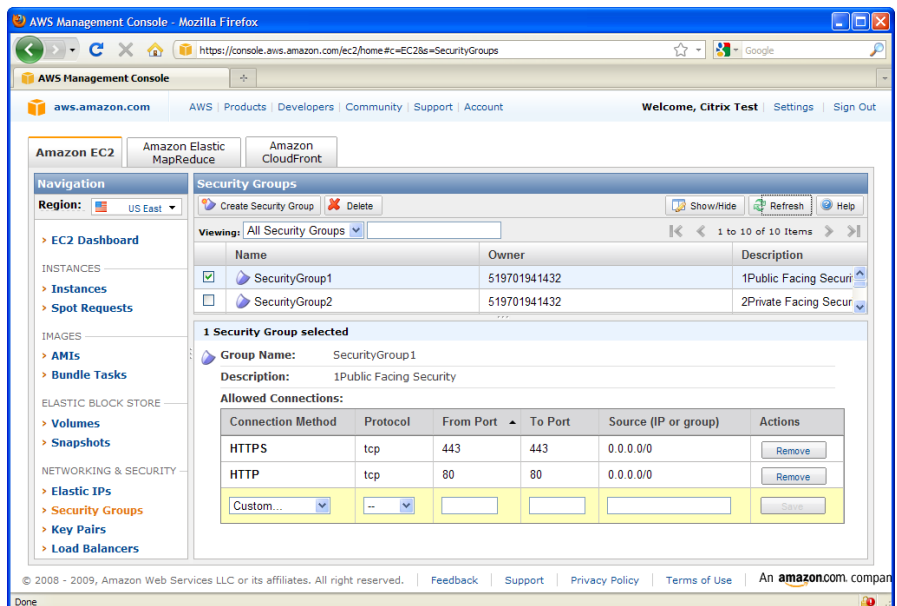
Configure Security Groups

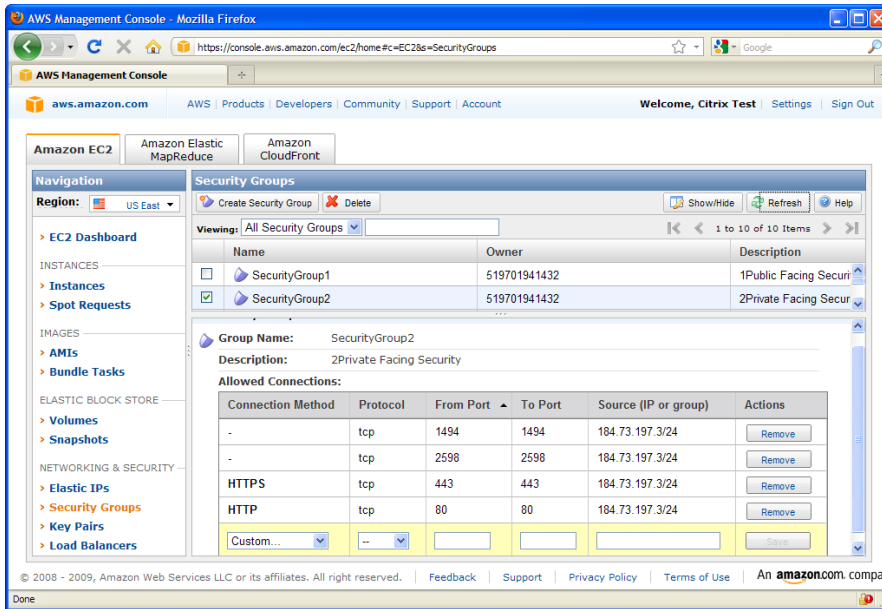
Once the Security Groups have been created, we need to configure them to allow specific port numbers in. Security Group 1 will allow connections to ports 80 and 443 from any source ip address. Security Group 2 will only allow port 80, 443, 1494 and 2598 from the source ip address of the Web Interface server.

Security Group 1:

Using the information from the tables at the beginning of this guide, we add two policies to allow connections to and from ports 80 and 443, from any source ip address.

Note: This is the Public Facing security policy.





Security Group 2:

Using the information from the tables at the beginning of this guide, we add four policies to allow connection to and from ports 80, 443, 1494 and 2598, only from source ip address of the Web Interface server.

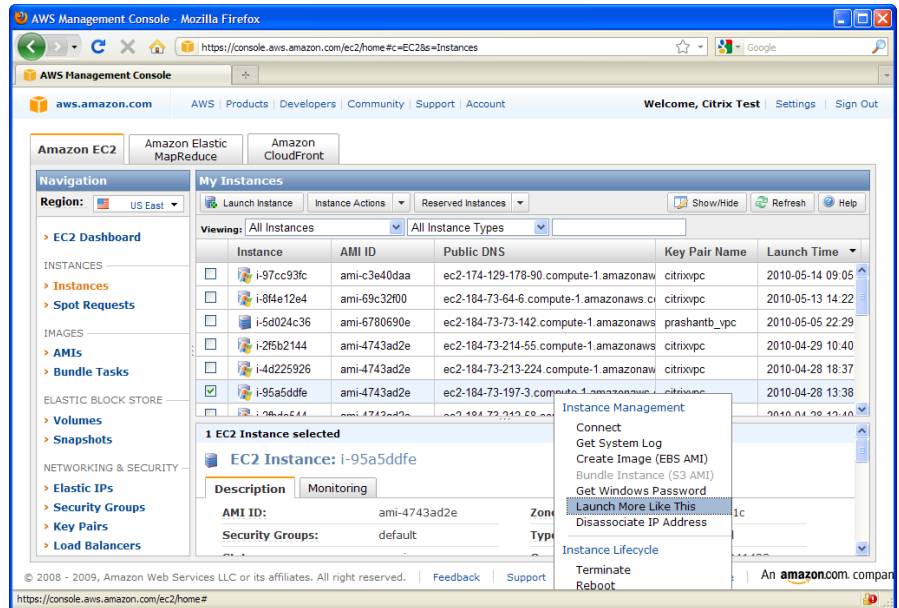
Note: This is the Private Facing security policy.

Security Group 1

Once the security groups have been created and configured, we need to launch our AMI's in those security groups. If your instance is already running, you may have to Create EBS Image, in order to launch it in a different security group. The server that should run in this security group should be the Web Interface server.

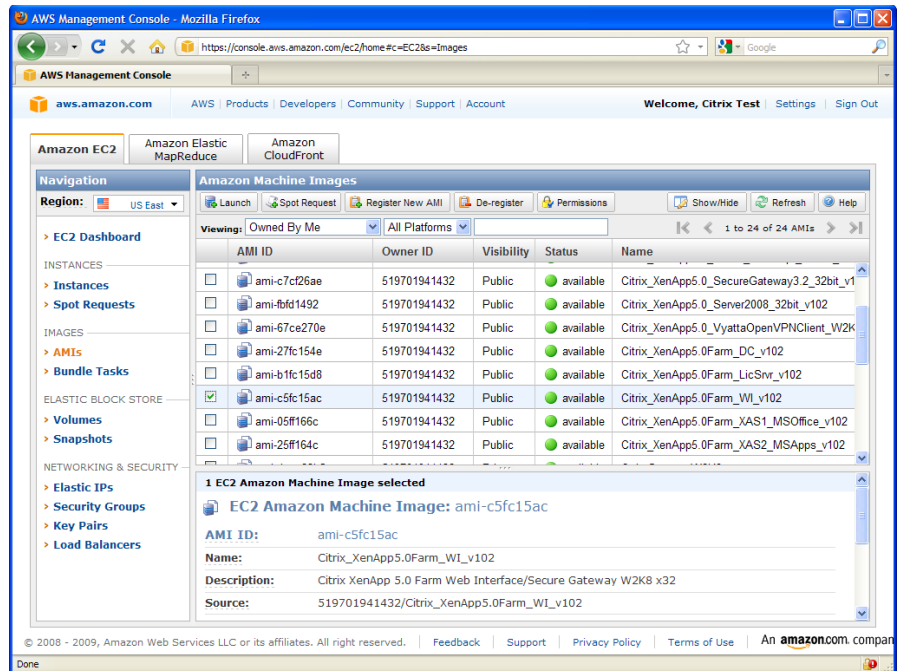
Security Group 1:

From the Amazon Console, select AMIs.



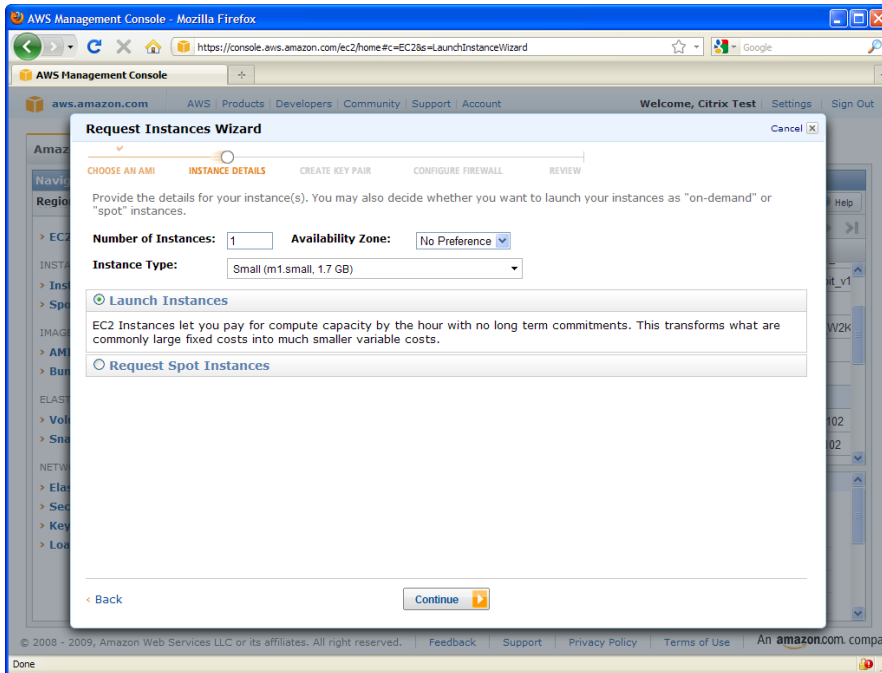
Security Group 1:

Select Launch.



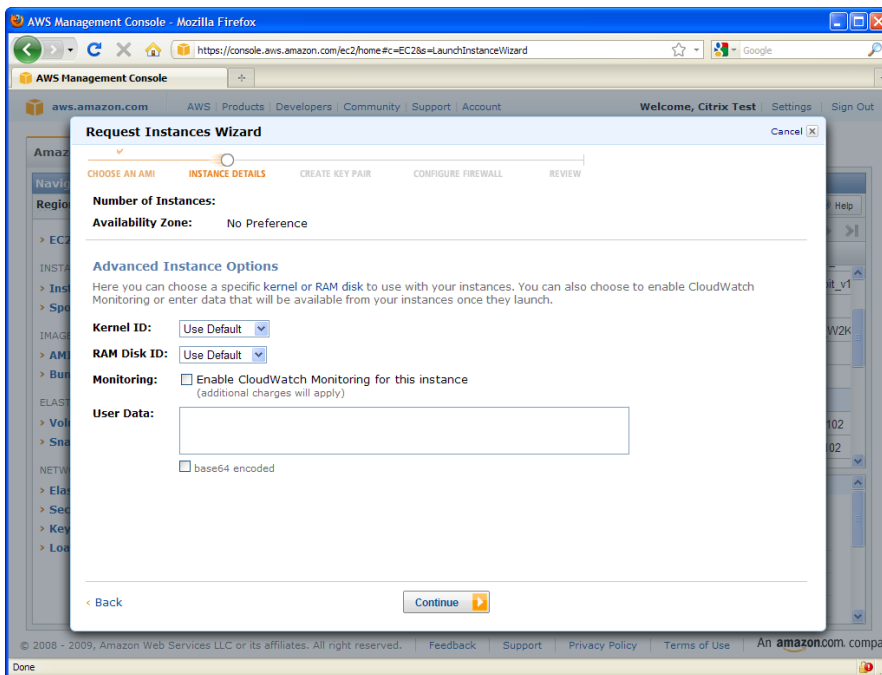
Security Group 1:

Select size of image to launch.



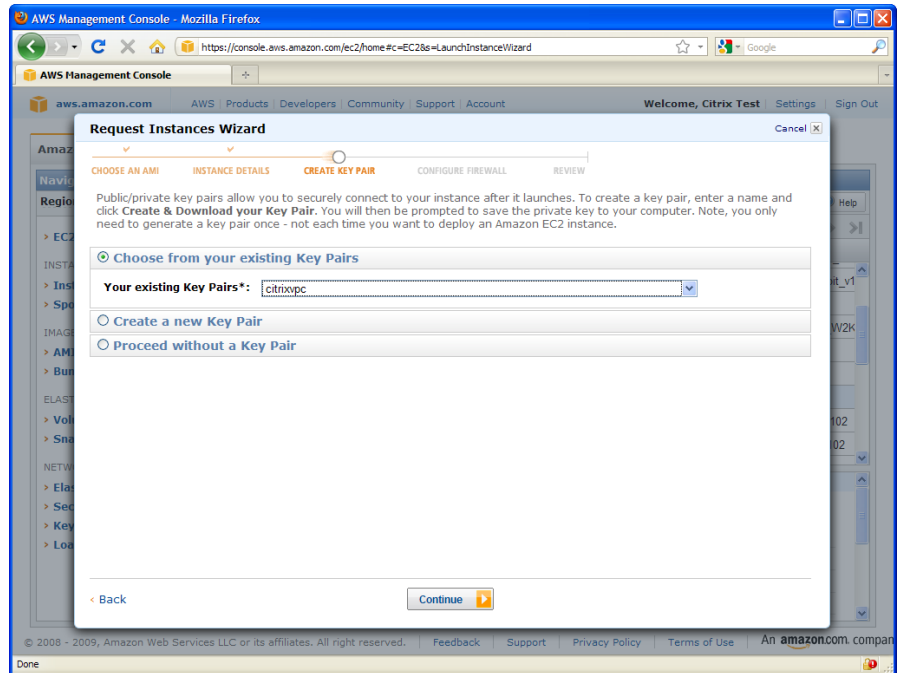
Security Group 1:

Select availability zone.



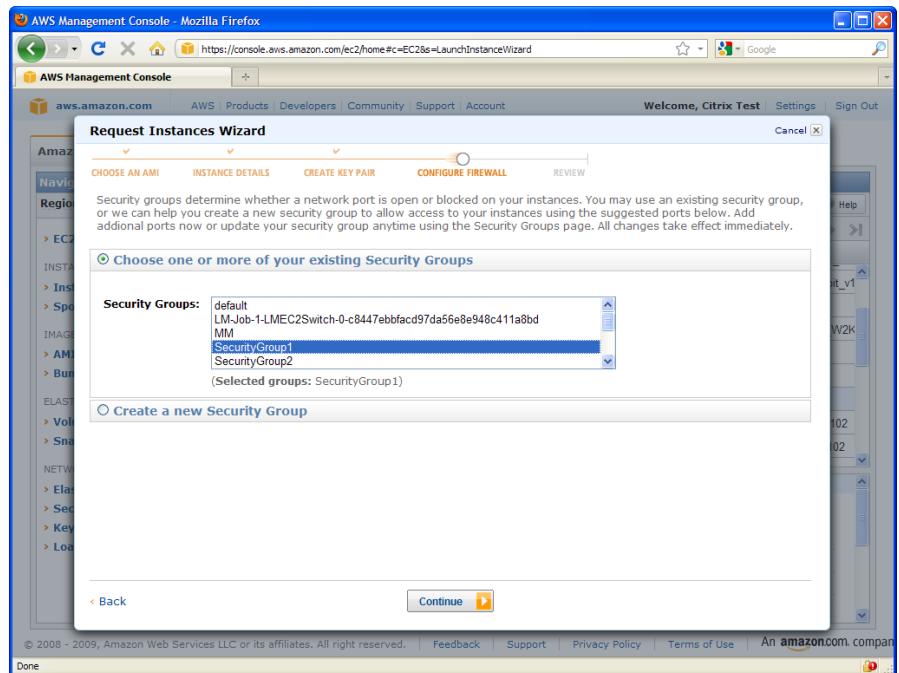
Security Group 1:

Select key pair.

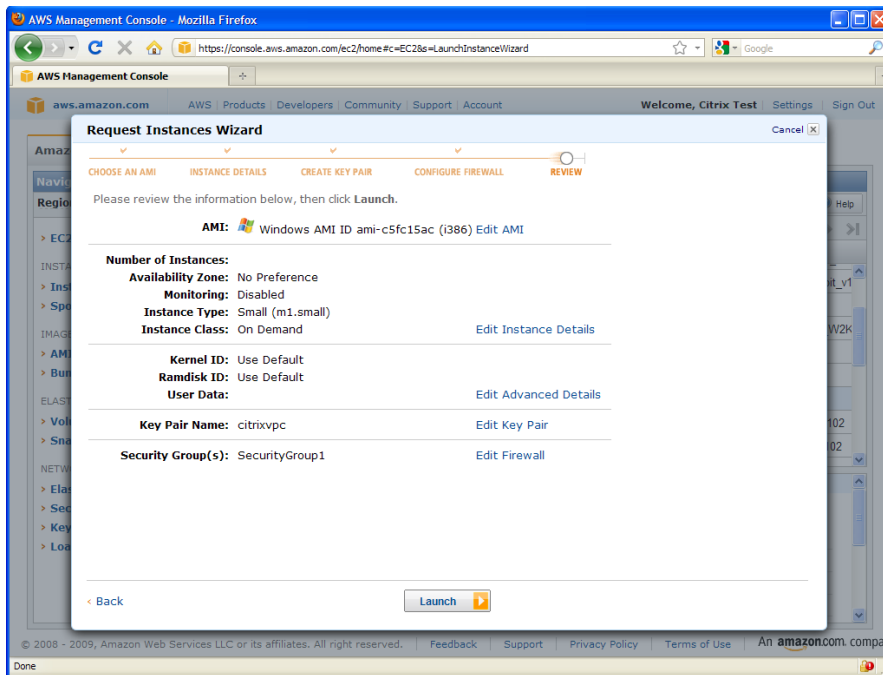


Security Group 1:

Select the Security Group 1 group to launch the AMI into.



Security Group 1: Review and Launch.



Security Group 2

Repeat the previous steps for Security Group 2. The servers that should run in this Security Group are the License Server, XenApp Servers and Domain Controller.

**Worldwide Headquarters**

Citrix Systems, Inc.
851 West Cypress Creek Road
Fort Lauderdale, FL 33309, USA
T +1 800 393 1888
T +1 954 267 3000

Americas

Citrix Silicon Valley
4988 Great American Parkway
Santa Clara, CA 95054, USA
T +1 408 790 8000

Europe

Citrix Systems International GmbH
Rheinweg 9
8200 Schaffhausen, Switzerland
T +41 52 635 7700

Asia Pacific

Citrix Systems Hong Kong Ltd.
Suite 3201, 32nd Floor
One International Finance Centre
1 Harbour View Street
Central, Hong Kong
T +852 2100 5000

Citrix Online Division

6500 Hollister Avenue
Goleta, CA 93117, USA
T +1 805 690 6400

www.citrix.com

About Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) is the leading provider of virtualization, networking and software as a service technologies for more than 230,000 organizations worldwide. Its Citrix Delivery Center, Citrix Cloud Center (C3) and Citrix Online Services product families radically simplify computing for millions of users, delivering applications as an on-demand service to any user, in any location on any device. Citrix customers include the world's largest Internet companies, 99 percent of *Fortune* Global 500 enterprises, and hundreds of thousands of small businesses and prosumers worldwide. Citrix partners with over 10,000 companies worldwide in more than 100 countries. Founded in 1989, annual revenue in 2008 was \$1.6 billion. The information in this publication is subject to change without notice.

THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. CITRIX SYSTEMS, INC. ("CITRIX"), SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR DIRECT, INCIDENTAL, CONSEQUENTIAL OR ANY OTHER DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS PUBLICATION, EVEN IF CITRIX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

This publication contains information protected by copyright. Except for internal distribution, no part of this publication may be photocopied or reproduced in any form without prior written consent from Citrix.

The exclusive warranty for Citrix products, if any, is stated in the product documentation accompanying such products. Citrix does not warrant products other than its own.

Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

© 2009 Citrix Systems, Inc., 851 West Cypress Creek Road, Ft. Lauderdale, Florida 33309-2009 U.S.A. All rights reserved.