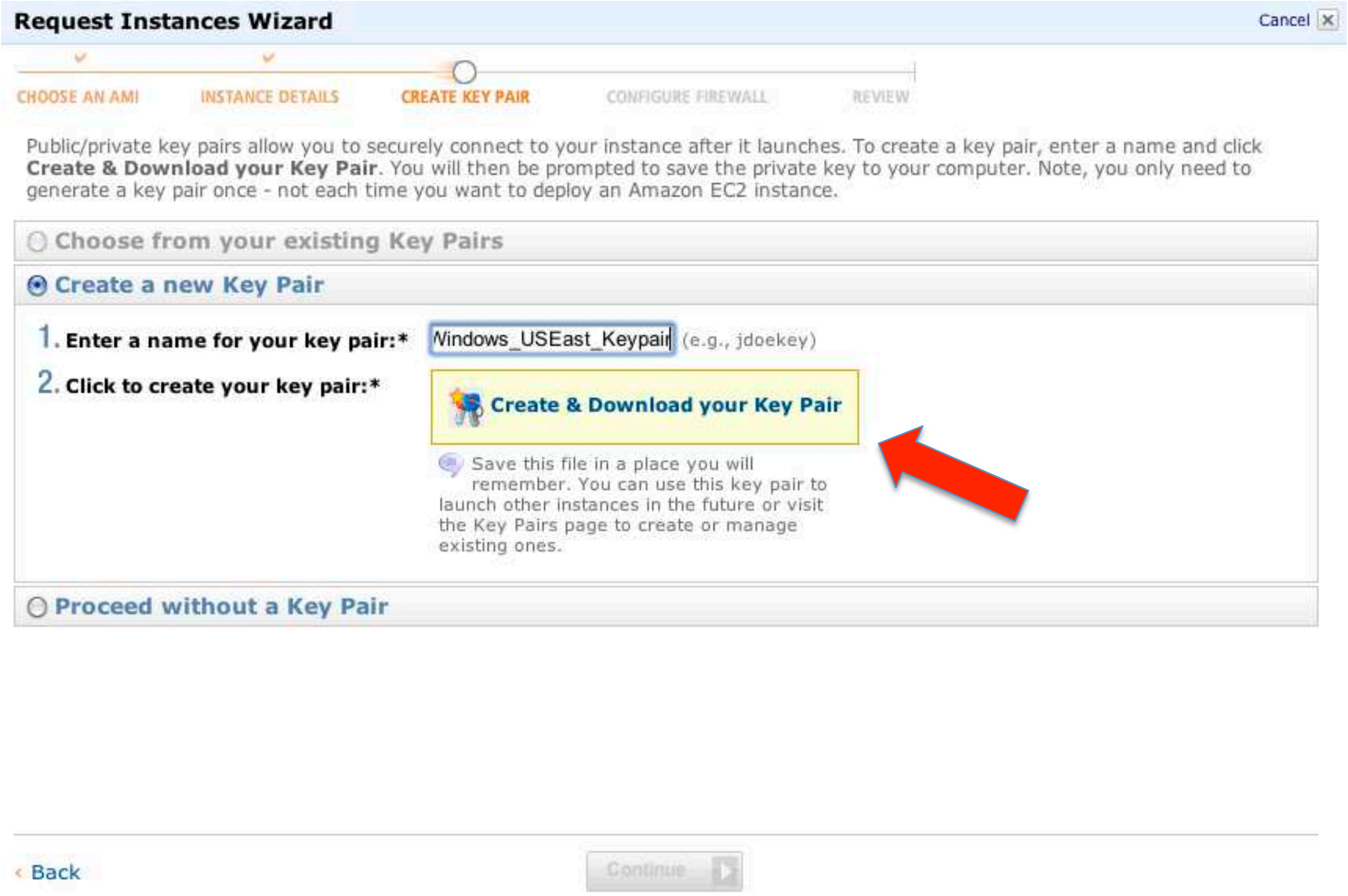
Key Pair for Accessing the Instance



Request Instances Wizard

Public/private key pairs allow you to securely connect to your instance after it launches. To create a key pair, enter a name and click **Create & Download your Key Pair**. You will then be prompted to save the private key to your computer. Note, you only need to generate a key pair once - not each time you want to deploy an Amazon EC2 instance.

○ Choose from your existing Key Pairs

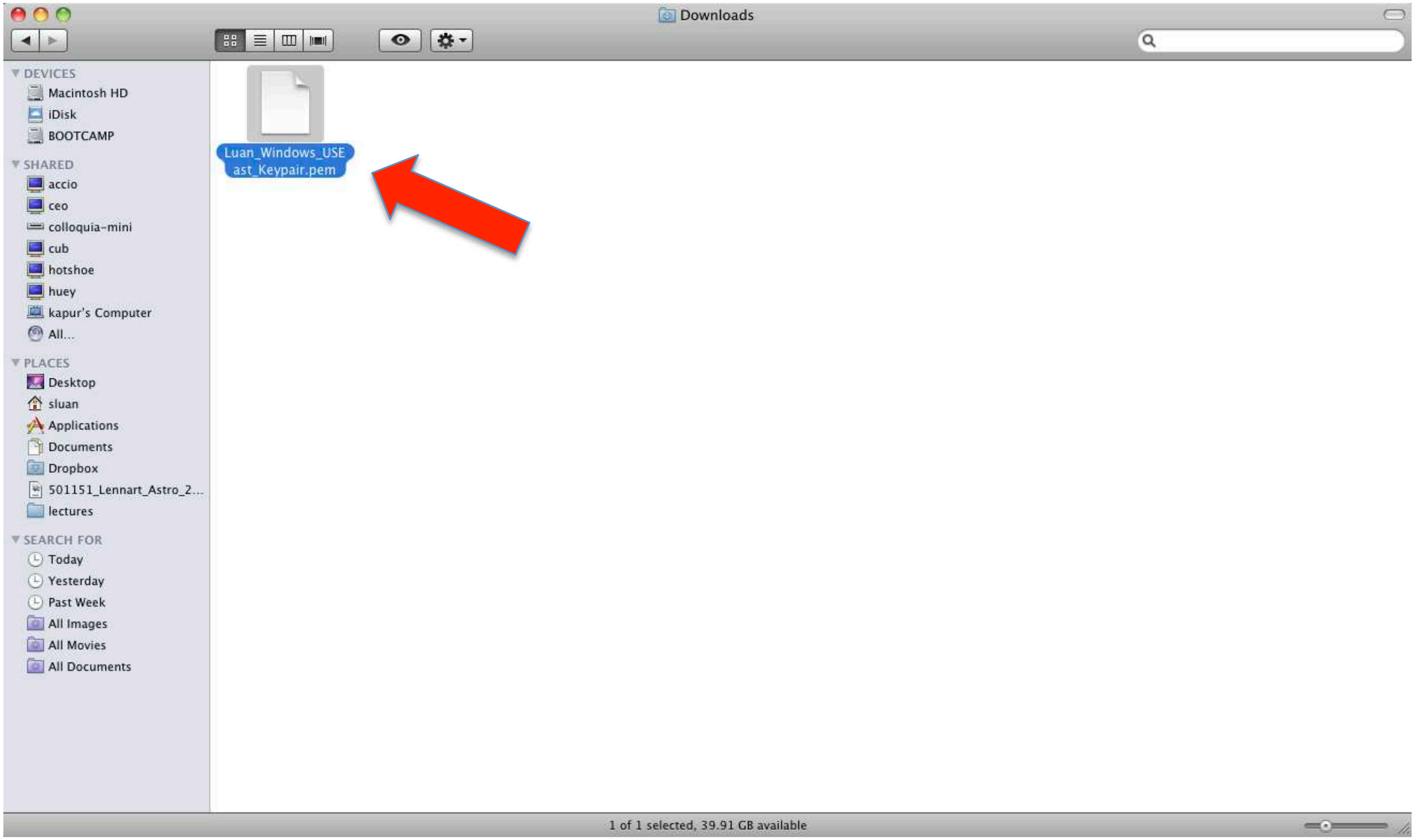
● Create a new Key Pair

1. **Enter a name for your key pair:*** Windows_USEast_Keypair (e.g., jdoekey)
2. **Click to create your key pair:*** Create & Download your Key Pair

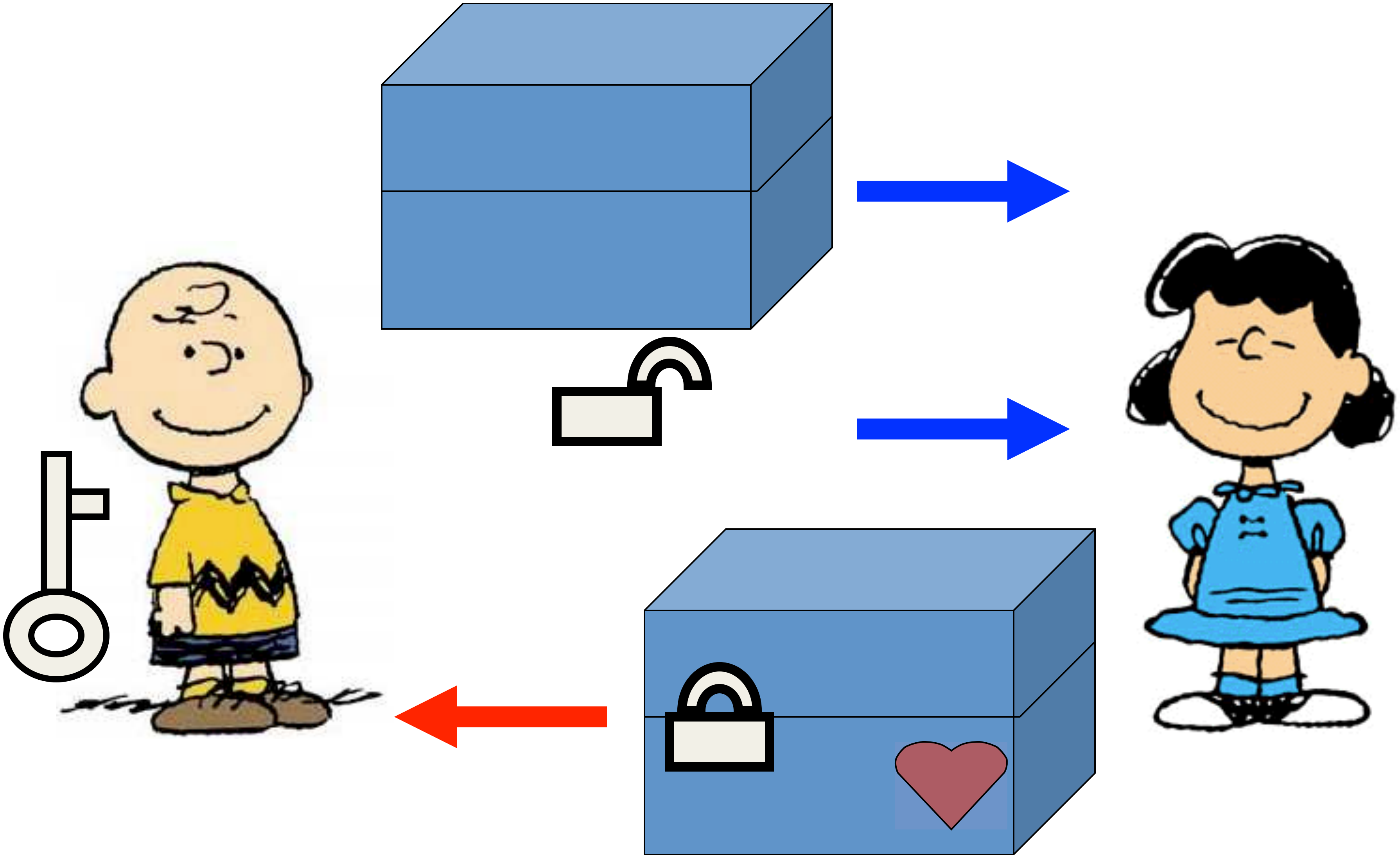
Save this file in a place you will remember. You can use this key pair to launch other instances in the future or visit the Key Pairs page to create or manage existing ones.

○ Proceed without a Key Pair

Key Pair File



Public Key System



Key Idea

The key for public system is to construct a one – way encryption function f which is easy to encrypt but hard to decrypt.

For example, the lock box with a lock open is a one - way function. It is easy to put the letter in the box and lock it (i.e., encrypt), but is hard to open the box once it is locked (decrypt).

RSA Public Key System

- Developed by Ron Rivest, Adi Shamir, Len Adleman in 1977, who later shared the 2002 Turing Award.
- The idea of RSA system is based on number theory in particular the factorization of large numbers.

Number Theory behind RSA

Let p and q be distinct primes and k is any integer.

Then :

(a) For any integer a with $GCD\left(a,pq\right)=1$,

$a^{k\left(p-1\right)\left(q-1\right)} \bmod pq = 1$

(b) For any integer a, $a^{k\left(p-1\right)\left(q-1\right)+1} \bmod pq = a$.

Example

$$p = 5,\ q = 7,\ a = 19$$

$$GCD(a, pq) = 1$$

$$k = 3,\ a^{k(p-1)(q-1)} = 19^{3\times4\times6} = 19^{72}$$

$$= 1.1755991641121183246595167229728 \times 10^{92}$$

$$a^{k(p-1)(q-1)} \bmod pq = 1$$

$$a^{k(p-1)(q-1)+1} = 19^{3\times4\times6+1} = 19^{73}$$

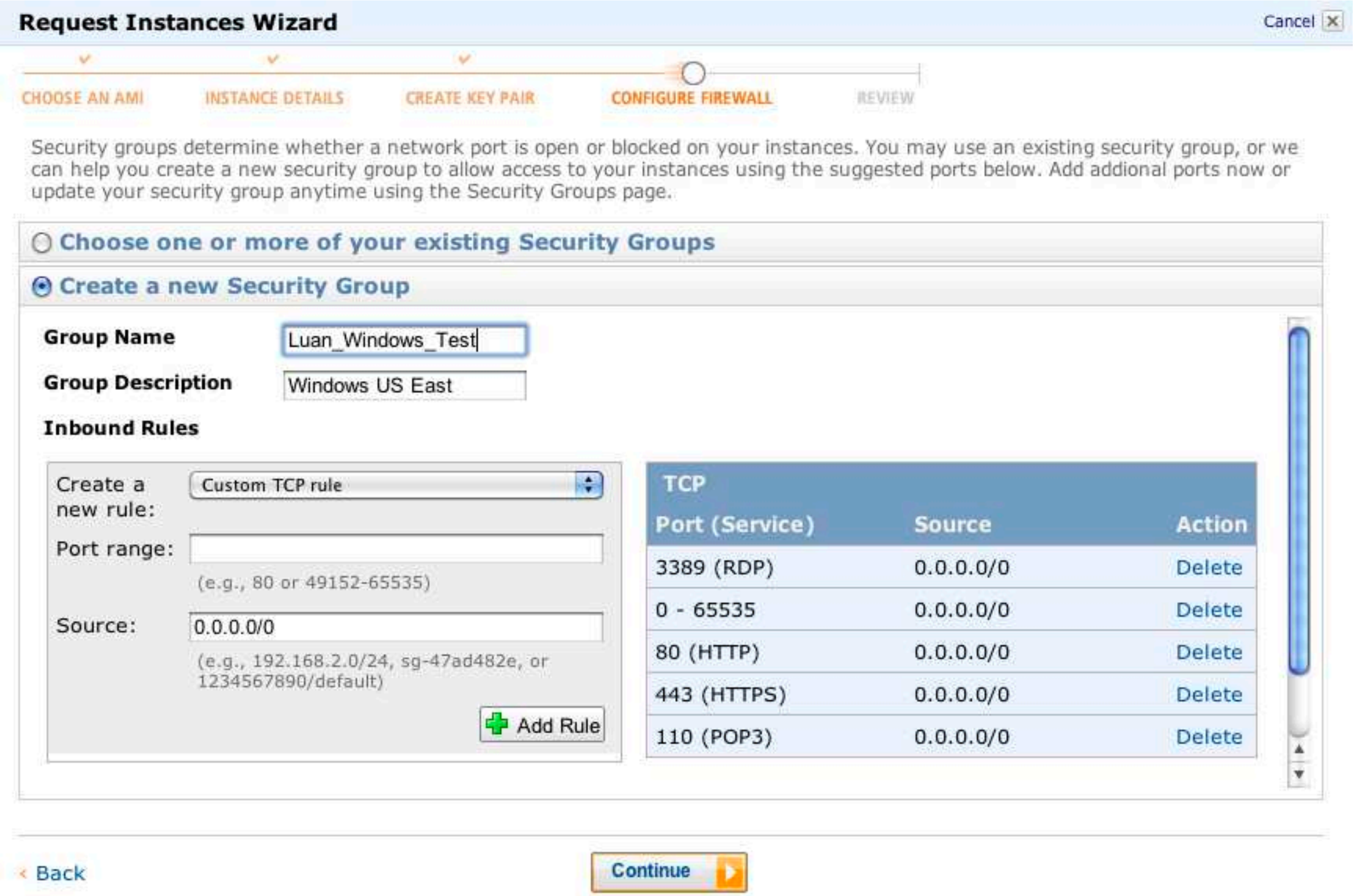
$$= 2.2336384118130248168530817736483 \times 10^{93}$$

$$a^{k(p-1)(q-1)+1} \bmod pq = 19.$$

How to use the theorem?

- Suppose we have two primes p and q.
  - $m = pq$
  - $n =(p - 1)(q - 1)$
  - s: GCD(s, n) = 1
- Announce m and s.
- Encoding
  - Someone wants to send me a message a.
  - Encryption rule: send me $b = a^s \bmod m$
- Decoding:
  - GCD(s, n)=1, then $ts + kn = 1$
  - $b^t \bmod m = (a^s)^t \bmod m = a^{-kn+1} \bmod m = a$

Security Rules



Security groups determine whether a network port is open or blocked on your instances. You may use an existing security group, or we can help you create a new security group to allow access to your instances using the suggested ports below. Add addional ports now or update your security group anytime using the Security Groups page.

○ Choose one or more of your existing Security Groups

● Create a new Security Group

Group Name	Luan_Windows_Test
Group Description	Windows US East

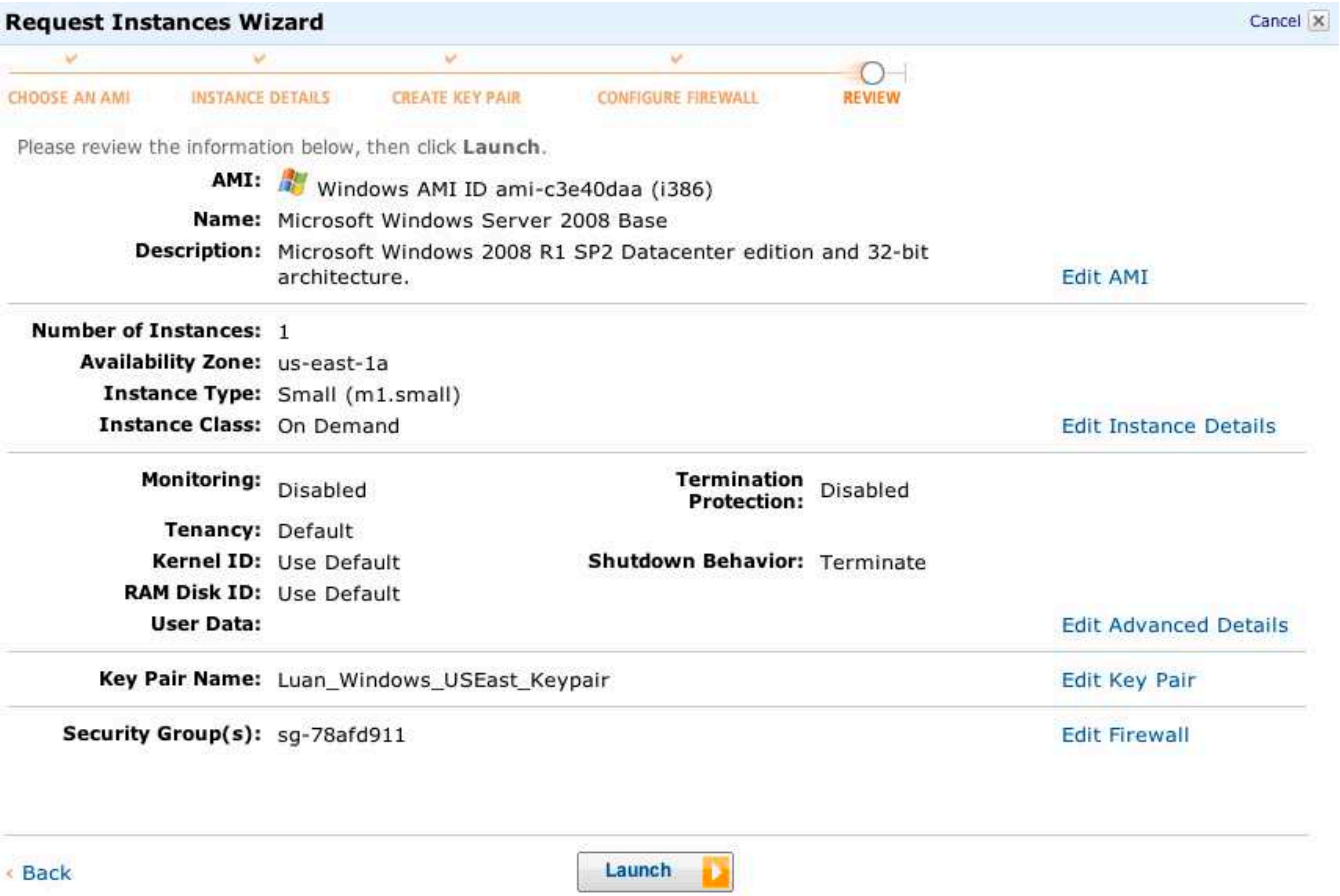
Inbound Rules

Create a new rule:	Custom TCP rule
Port range:	(e.g., 80 or 49152-65535)
Source:	0.0.0.0/0 (e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)

TCP

Port (Service)	Source	Action
3389 (RDP)	0.0.0.0/0	Delete
0 - 65535	0.0.0.0/0	Delete
80 (HTTP)	0.0.0.0/0	Delete
443 (HTTPS)	0.0.0.0/0	Delete
110 (POP3)	0.0.0.0/0	Delete

Summary



Please review the information below, then click **Launch**.

AMI: Windows AMI ID ami-c3e40daa (i386)
Name: Microsoft Windows Server 2008 Base
Description: Microsoft Windows 2008 R1 SP2 Datacenter edition and 32-bit architecture.

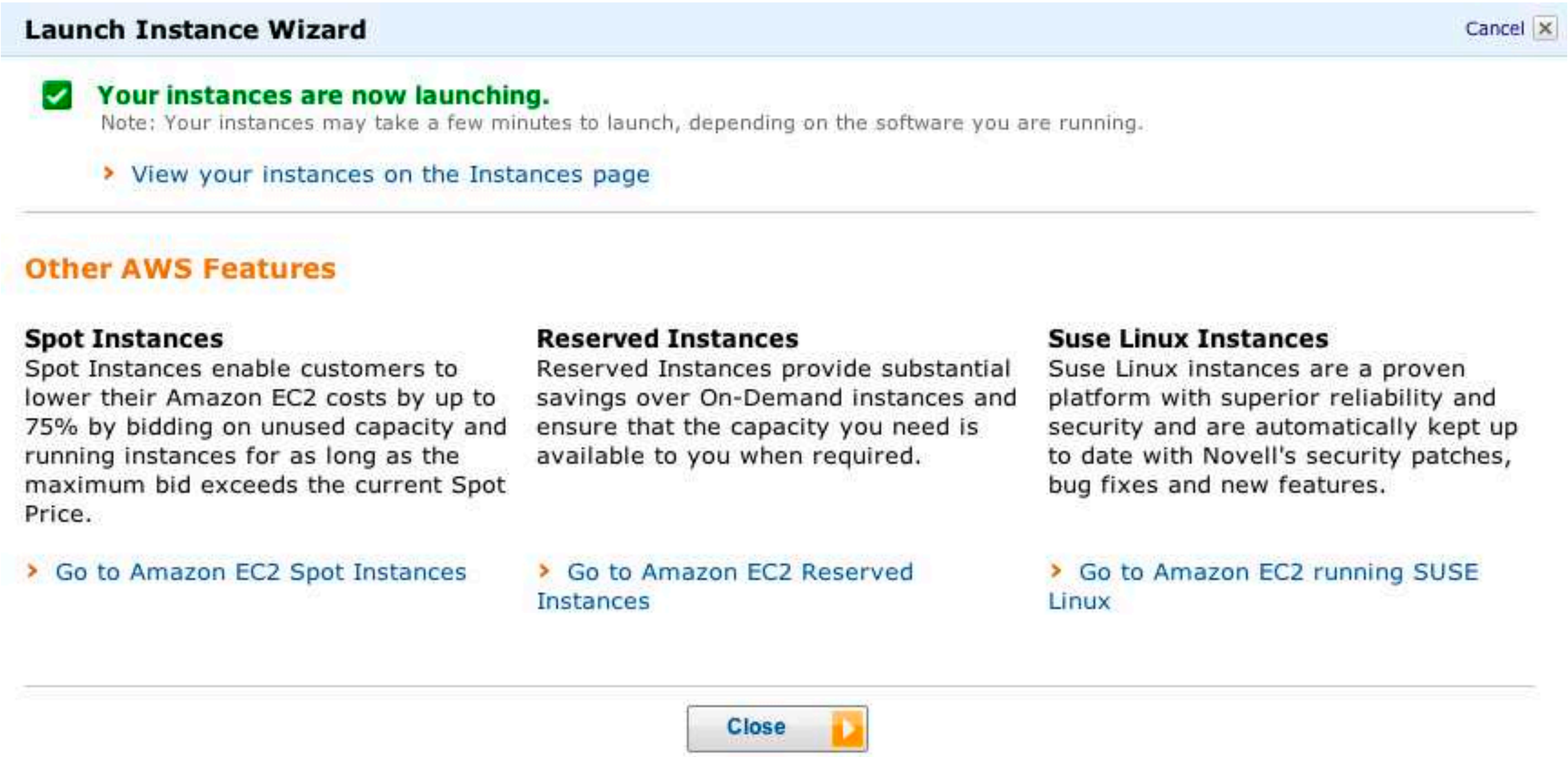
Number of Instances: 1
Availability Zone: us-east-1a
Instance Type: Small (m1.small)
Instance Class: On Demand

Monitoring: Disabled
Termination Protection: Disabled
Tenancy: Default
Kernel ID: Use Default
Shutdown Behavior: Terminate
RAM Disk ID: Use Default
User Data:

Key Pair Name: Luan_Windows_USEast_Keypair

Security Group(s): sg-78afd911

Launched



Launch Instance Wizard

☑ **Your instances are now launching.**

Note: Your instances may take a few minutes to launch, depending on the software you are running.

› View your instances on the Instances page

Other AWS Features

Spot Instances
Spot Instances enable customers to lower their Amazon EC2 costs by up to 75% by bidding on unused capacity and running instances for as long as the maximum bid exceeds the current Spot Price.

› Go to Amazon EC2 Spot Instances

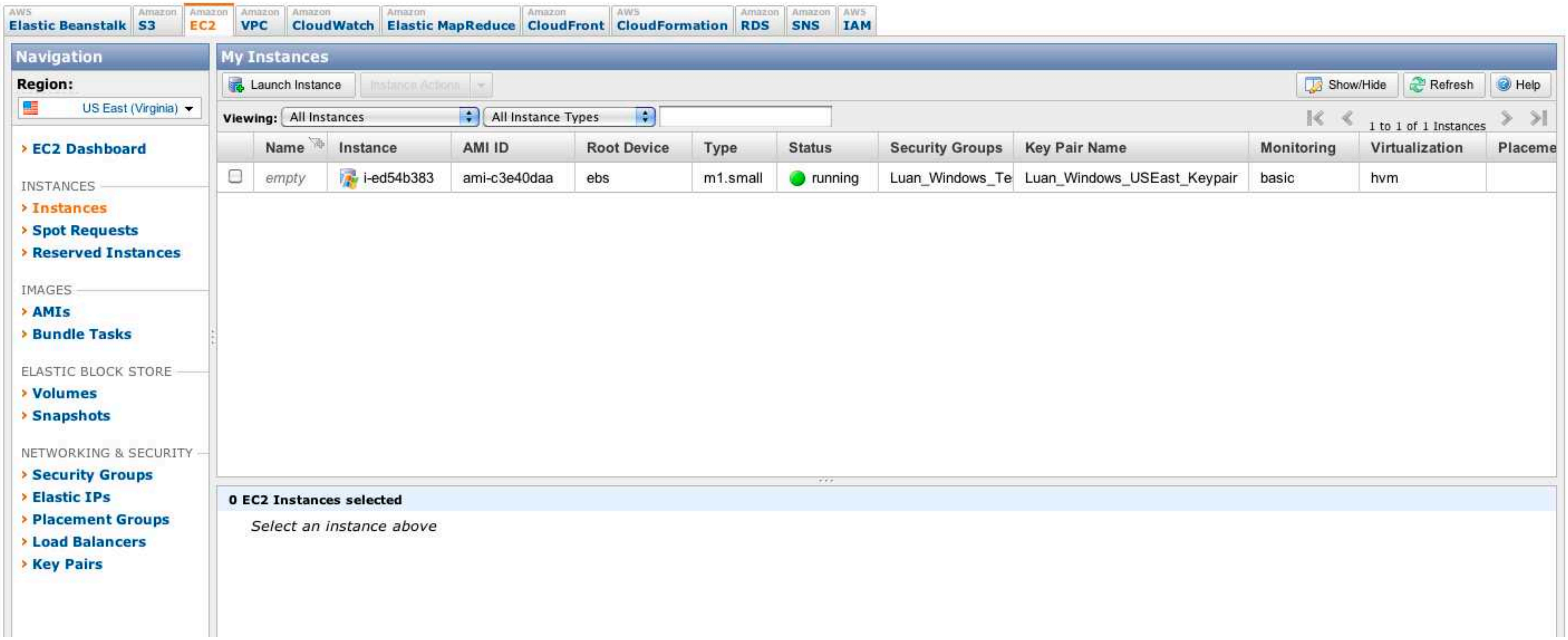
Reserved Instances
Reserved Instances provide substantial savings over On-Demand instances and ensure that the capacity you need is available to you when required.

› Go to Amazon EC2 Reserved Instances

Suse Linux Instances
Suse Linux instances are a proven platform with superior reliability and security and are automatically kept up to date with Novell's security patches, bug fixes and new features.

› Go to Amazon EC2 running SUSE Linux

AWS Console

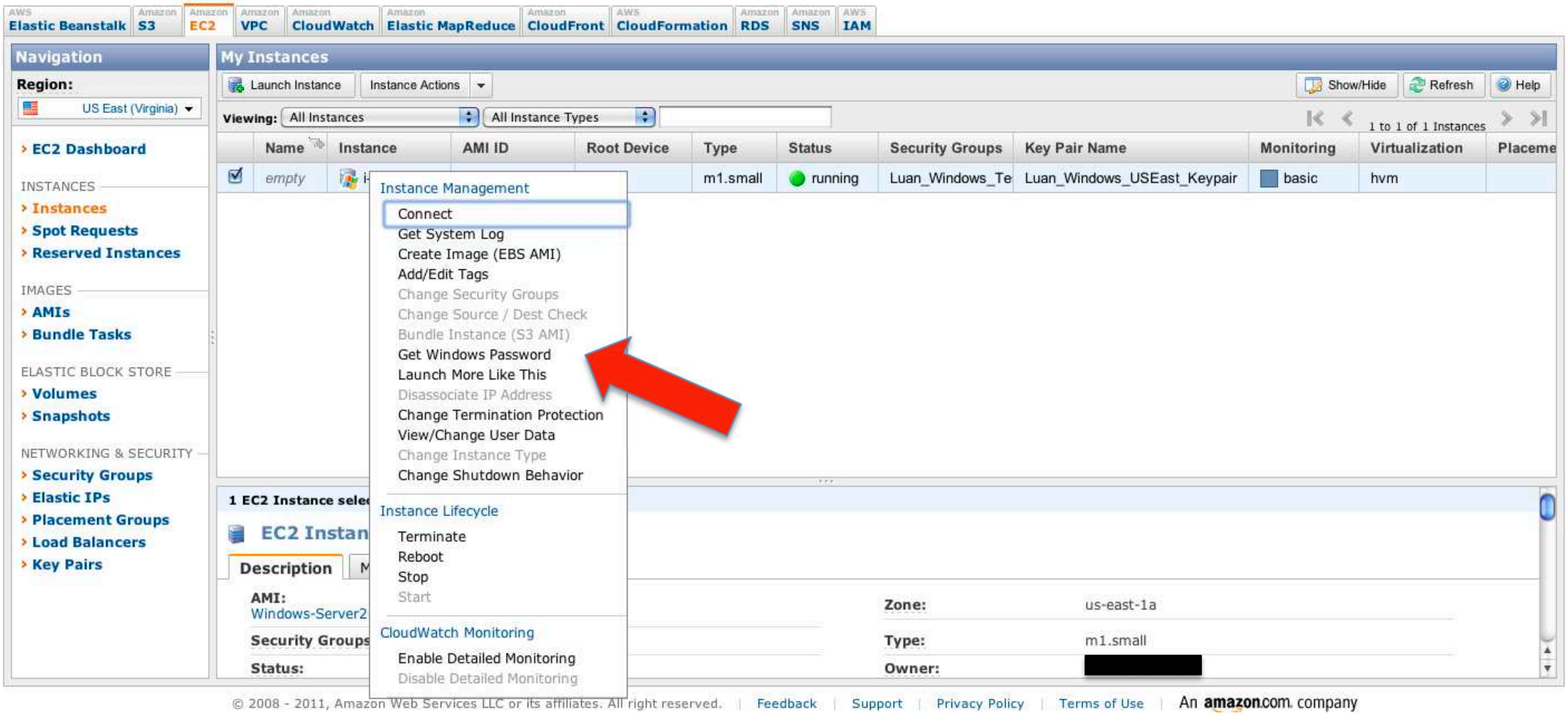


	Name	Instance	AMI ID	Root Device	Type	Status	Security Groups	Key Pair Name	Monitoring	Virtualization	Placeme
□	*empty*	i-ed54b383	ami-c3e40daa	ebs	m1.small	● running	Luan_Windows_Te	Luan_Windows_USEast_Keypair	basic	hvm	

0 EC2 Instances selected

Select an instance above

Retrieve Windows Password



	Name	Instance	AMI ID	Root Device	Type	Status	Security Groups	Key Pair Name	Monitoring	Virtualization	Placeme
☑	*empty*	i-			m1.small	● running	Luan_Windows_Te	Luan_Windows_USEast_Keypair	▨ basic	hvm	

AMI: Windows-Server2

Security Groups

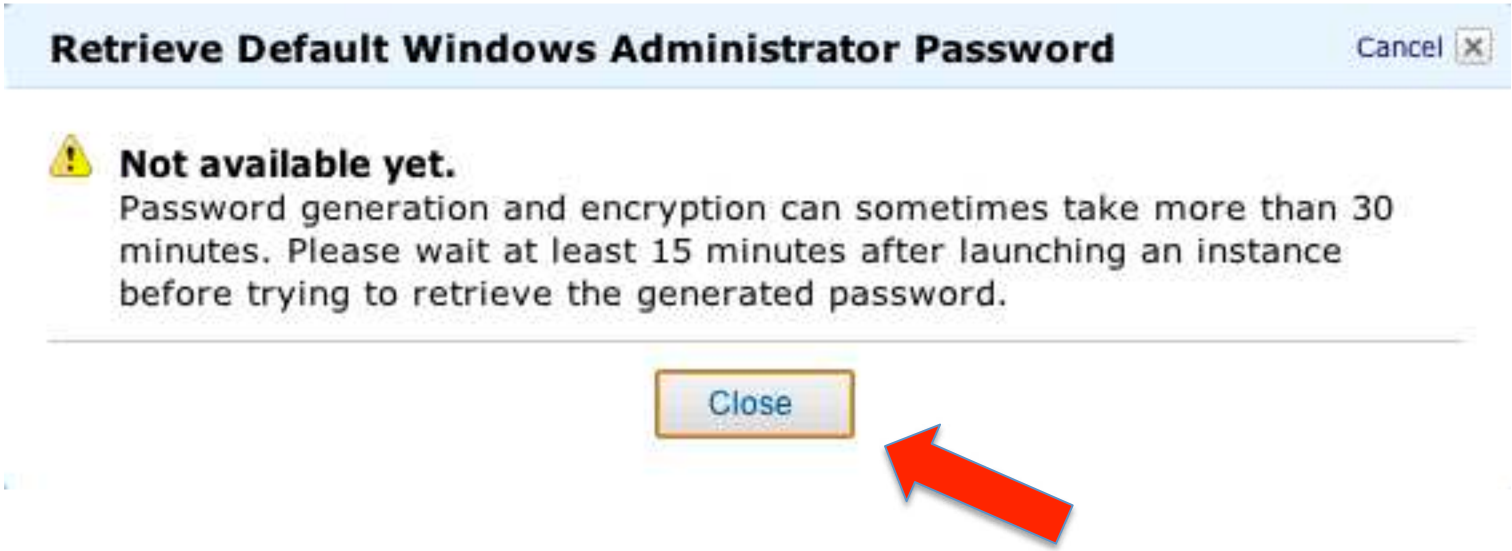
Status:

Zone: us-east-1a

Type: m1.small

Owner: [redacted]

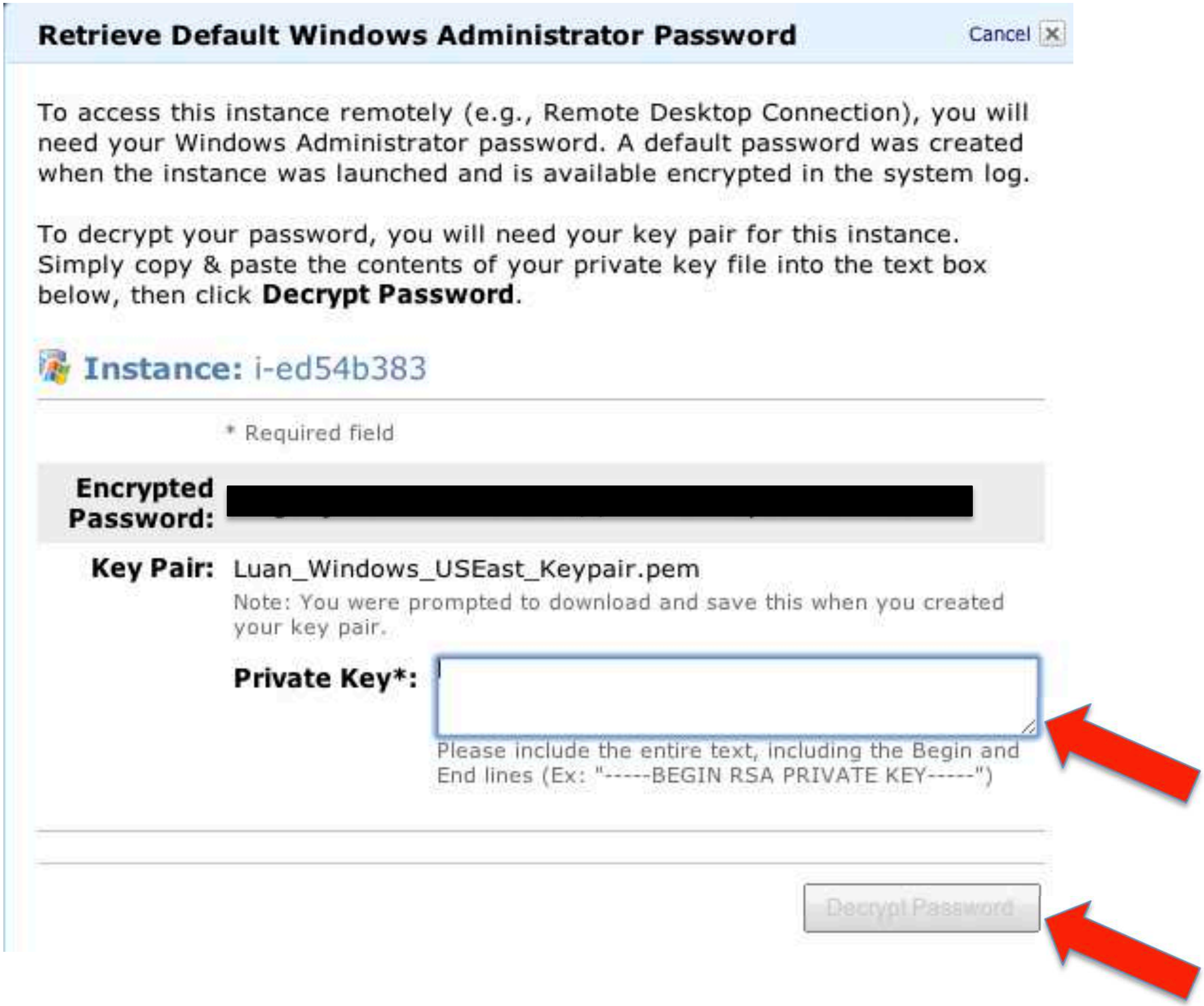
Retrieving Password (cont.)



Retrieve Default Windows Administrator Password

⚠ **Not available yet.**
Password generation and encryption can sometimes take more than 30 minutes. Please wait at least 15 minutes after launching an instance before trying to retrieve the generated password.

Retrieving Password (cont.)



Retrieve Default Windows Administrator Password

To access this instance remotely (e.g., Remote Desktop Connection), you will need your Windows Administrator password. A default password was created when the instance was launched and is available encrypted in the system log.

To decrypt your password, you will need your key pair for this instance. Simply copy & paste the contents of your private key file into the text box below, then click **Decrypt Password**.

Instance: i-ed54b383

* Required field

Encrypted Password: [redacted]

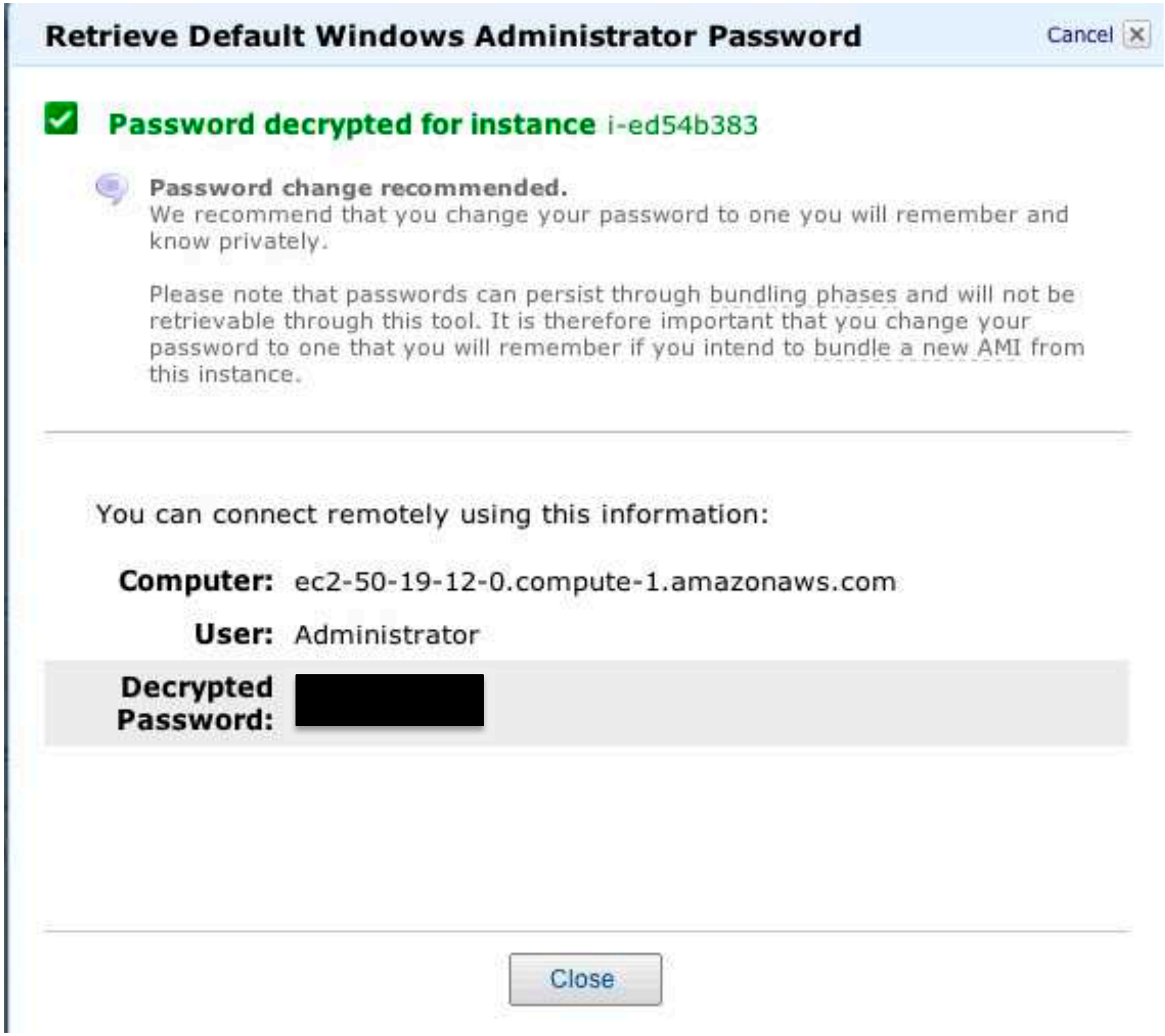
Key Pair: Luan_Windows_USEast_Keypair.pem

Note: You were prompted to download and save this when you created your key pair.

Private Key*:

Please include the entire text, including the Begin and End lines (Ex: "-----BEGIN RSA PRIVATE KEY-----")

After 15 Minutes



Retrieve Default Windows Administrator Password

✓ **Password decrypted for instance** i-ed54b383

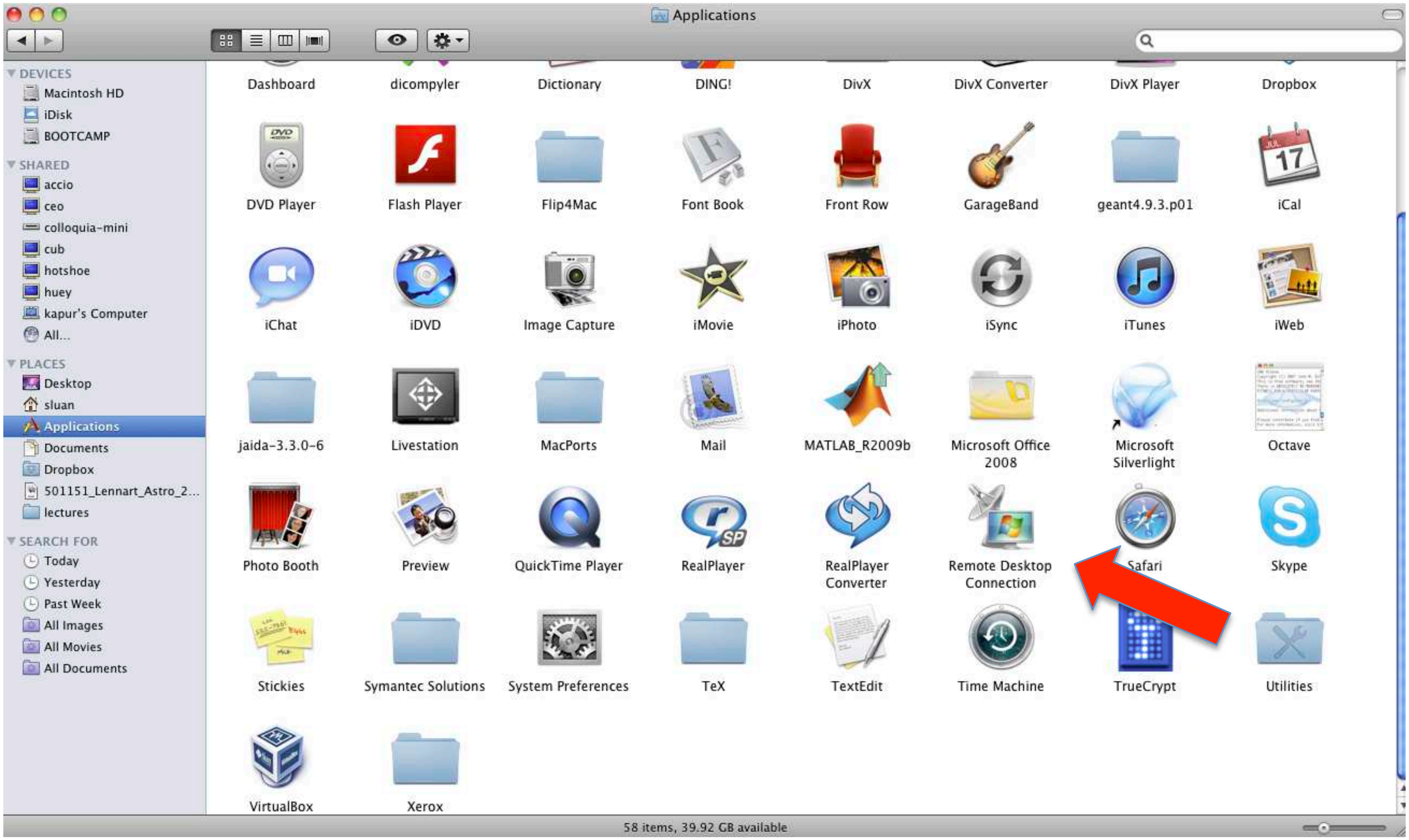
Password change recommended.
We recommend that you change your password to one you will remember and know privately.

Please note that passwords can persist through bundling phases and will not be retrievable through this tool. It is therefore important that you change your password to one that you will remember if you intend to bundle a new AMI from this instance.

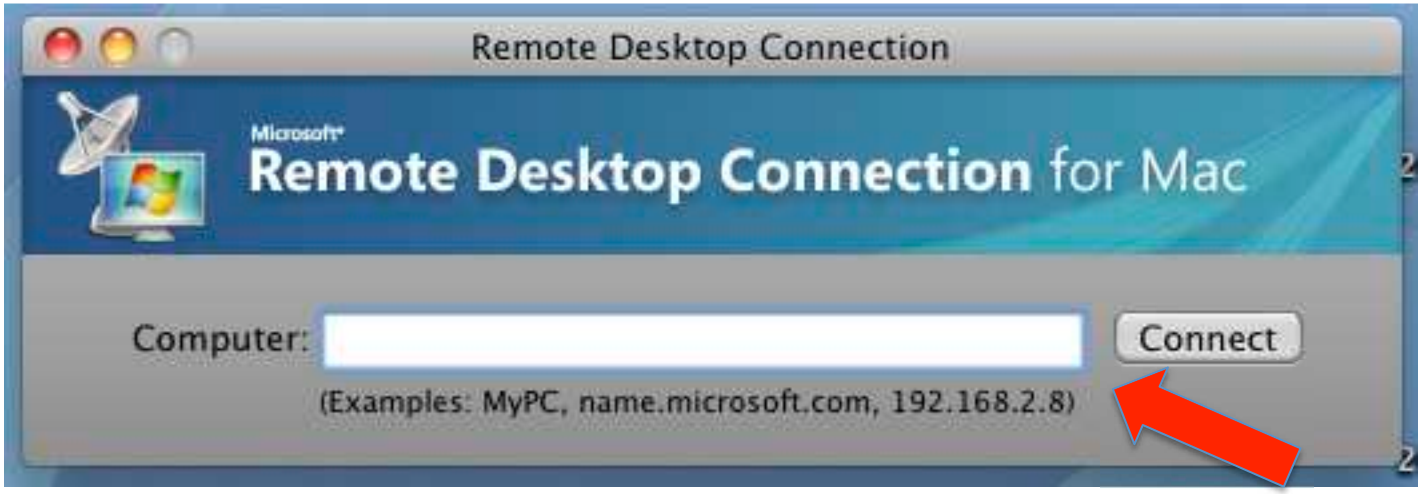
You can connect remotely using this information:

Computer:	ec2-50-19-12-0.compute-1.amazonaws.com
User:	Administrator
Decrypted Password:	[redacted]

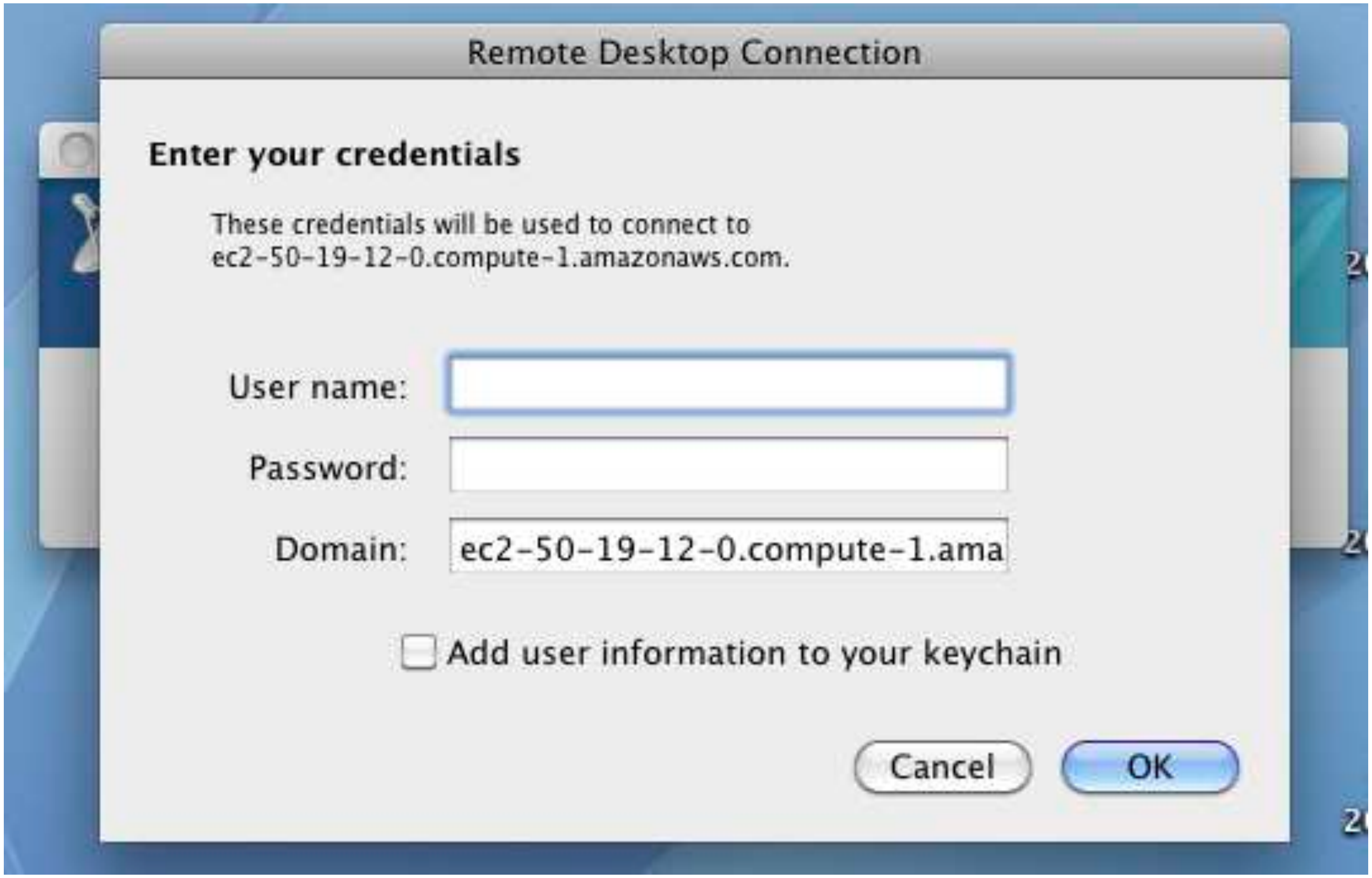
Connecting to Windows



Connecting to Windows (cont.)


Remote Desktop Connection
Microsoft®
Remote Desktop Connection for Mac
Computer:
Connect
(Examples: MyPC, name.microsoft.com, 192.168.2.8)

Connecting to Windows (cont.)



Remote Desktop Connection

Enter your credentials

These credentials will be used to connect to ec2-50-19-12-0.compute-1.amazonaws.com.

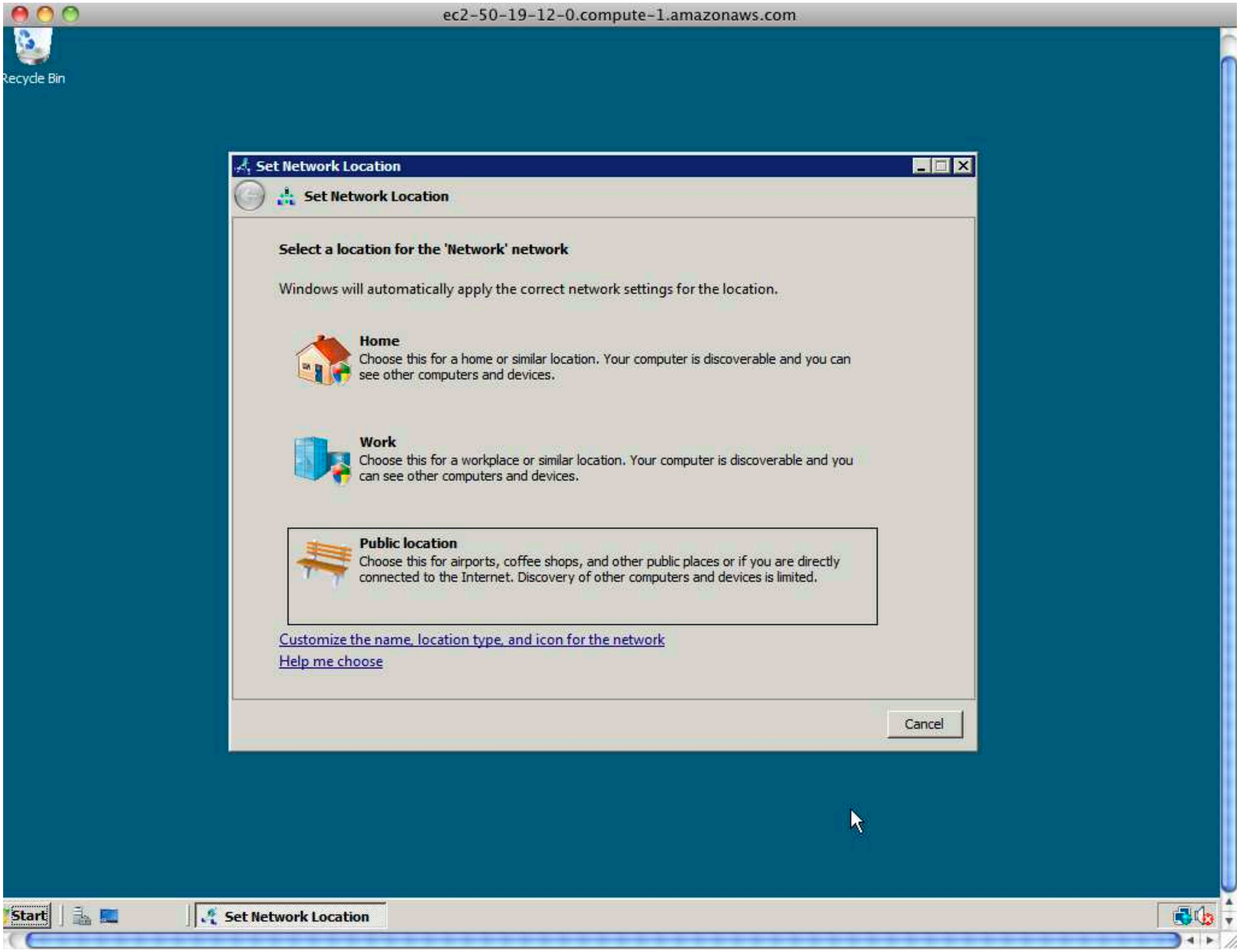
User name:

Password:

Domain: ec2-50-19-12-0.compute-1.ama

□ Add user information to your keychain

Connecting to Windows (cont.)



Set Network Location

Select a location for the 'Network' network

Windows will automatically apply the correct network settings for the location.

Home
Choose this for a home or similar location. Your computer is discoverable and you can see other computers and devices.

Work
Choose this for a workplace or similar location. Your computer is discoverable and you can see other computers and devices.

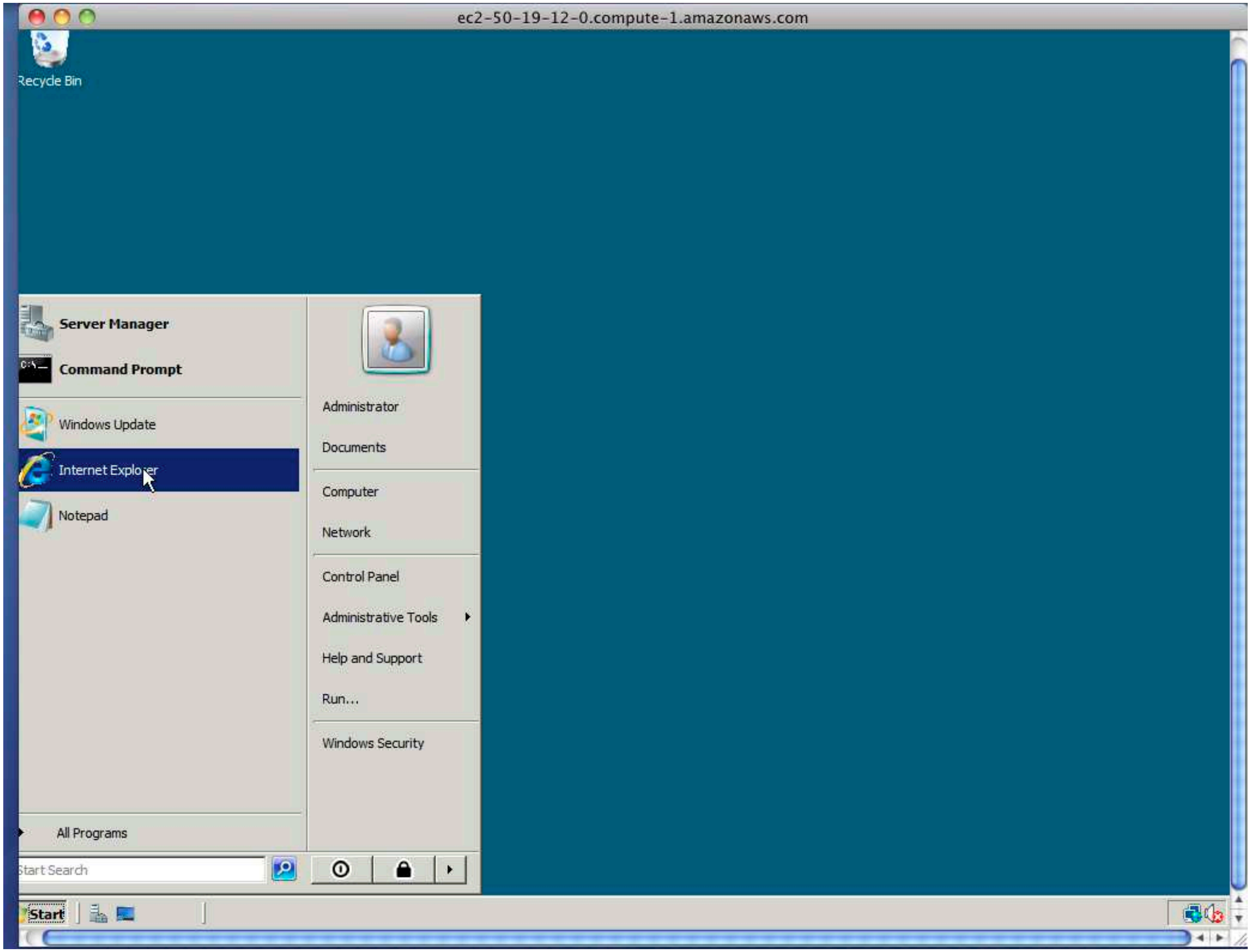
Public location
Choose this for airports, coffee shops, and other public places or if you are directly connected to the Internet. Discovery of other computers and devices is limited.

Customize the name, location type, and icon for the network

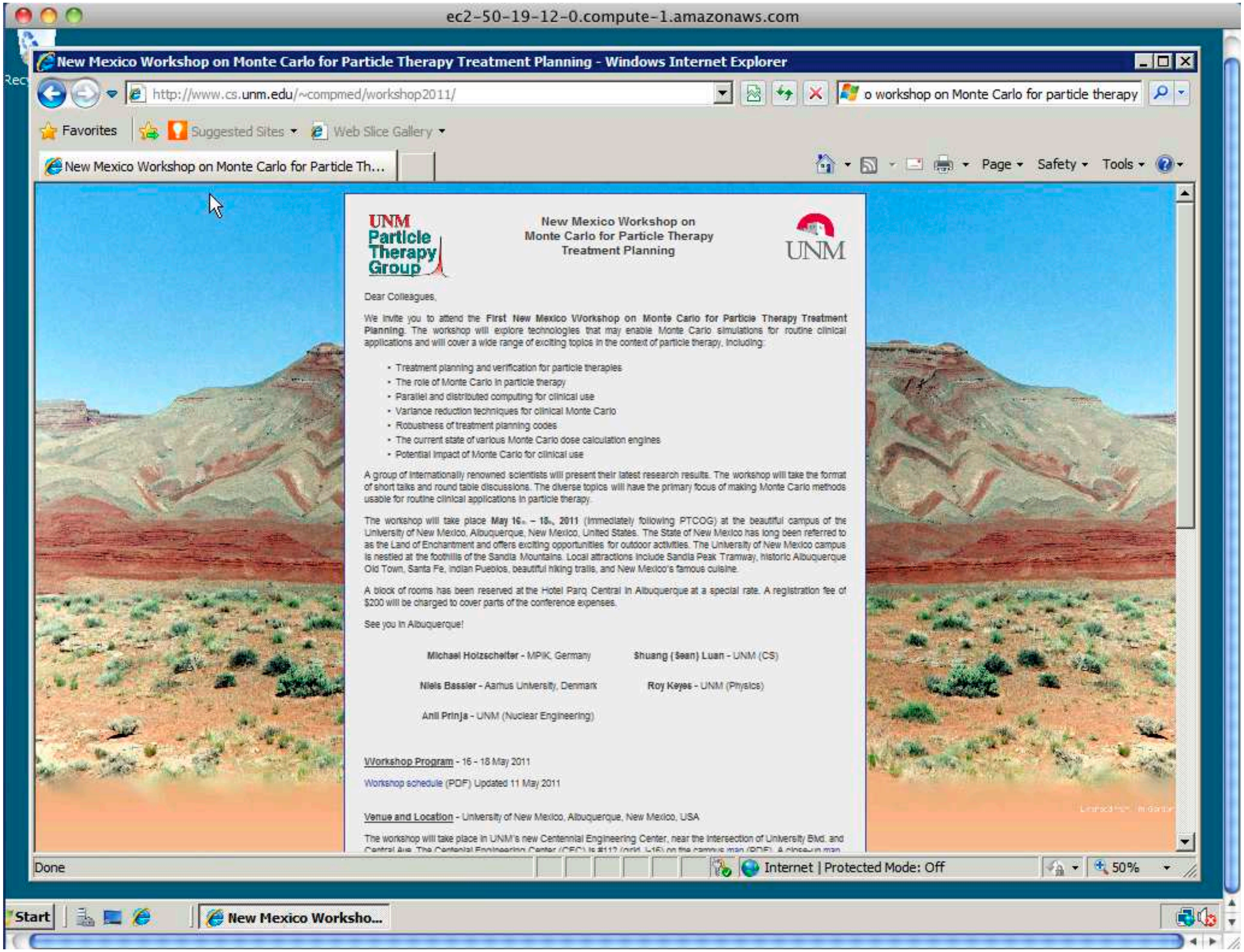
Help me choose

Cancel

Using Windows



Using Windows (cont.)


ec2-50-19-12-0.compute-1.amazonaws.com
New Mexico Workshop on Monte Carlo for Particle Therapy Treatment Planning - Windows Internet Explorer
http://www.cs.unm.edu/~compmed/workshop2011/
o workshop on Monte Carlo for particle therapy
Favorites
Suggested Sites
Web Slice Gallery
New Mexico Workshop on Monte Carlo for Particle Th...
Page
Safety
Tools
UNM Particle Therapy Group
UNM
Done
Internet | Protected Mode: Off
50%
Start
New Mexico Worksho...

New Mexico Workshop on Monte Carlo for Particle Therapy Treatment Planning

Dear Colleagues,

We invite you to attend the **First New Mexico Workshop on Monte Carlo for Particle Therapy Treatment Planning**. The workshop will explore technologies that may enable Monte Carlo simulations for routine clinical applications and will cover a wide range of exciting topics in the context of particle therapy, including:

- Treatment planning and verification for particle therapies
- The role of Monte Carlo in particle therapy
- Parallel and distributed computing for clinical use
- Variance reduction techniques for clinical Monte Carlo
- Robustness of treatment planning codes
- The current state of various Monte Carlo dose calculation engines
- Potential impact of Monte Carlo for clinical use

A group of internationally renowned scientists will present their latest research results. The workshop will take the format of short talks and round table discussions. The diverse topics will have the primary focus of making Monte Carlo methods usable for routine clinical applications in particle therapy.

The workshop will take place **May 16th – 18th, 2011** (immediately following PTCOG) at the beautiful campus of the University of New Mexico, Albuquerque, New Mexico, United States. The State of New Mexico has long been referred to as the Land of Enchantment and offers exciting opportunities for outdoor activities. The University of New Mexico campus is nestled at the foothills of the Sandia Mountains. Local attractions include Sandia Peak Tramway, historic Albuquerque Old Town, Santa Fe, Indian Pueblos, beautiful hiking trails, and New Mexico's famous cuisine.

A block of rooms has been reserved at the Hotel Parq Central in Albuquerque at a special rate. A registration fee of $200 will be charged to cover parts of the conference expenses.

See you in Albuquerque!

Michael Holzscheiter - MPIK, Germany   **Shuang (Sean) Luan** - UNM (CS)

Niels Bassler - Aarhus University, Denmark   **Roy Keyes** - UNM (Physics)

Anil Prinja - UNM (Nuclear Engineering)

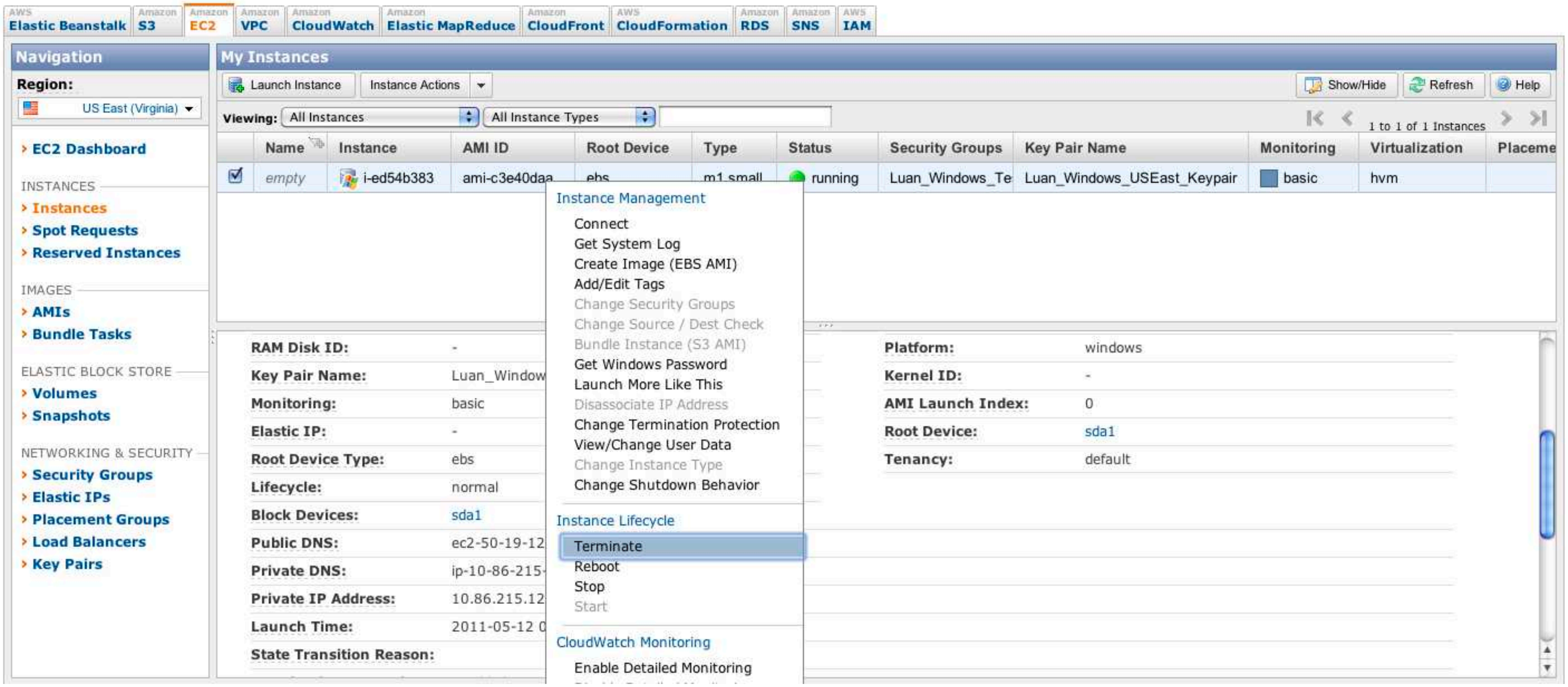
Workshop Program - 16 - 18 May 2011

Workshop schedule (PDF) Updated 11 May 2011

Venue and Location - University of New Mexico, Albuquerque, New Mexico, USA

The workshop will take place in UNM's new Centennial Engineering Center, near the intersection of University Blvd. and Central Ave. The Centenial Engineering Center (CEC) is #117 (grid J-16) on the campus map (PDF). A close-up map

Terminate Windows Instance

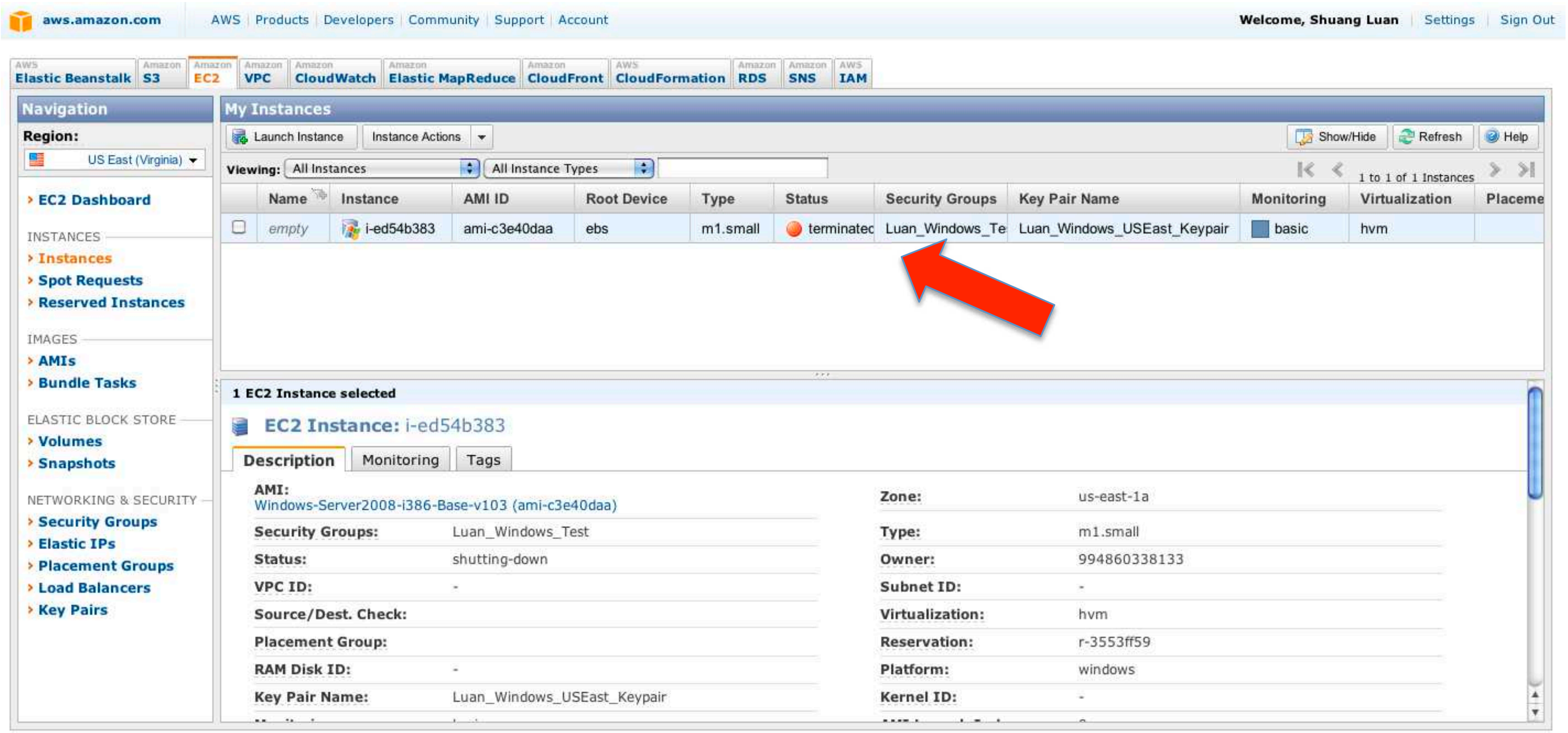


	Name	Instance	AMI ID	Root Device	Type	Status	Security Groups	Key Pair Name	Monitoring	Virtualization	Placeme
☑	empty	i-ed54b383	ami-c3e40daa	ebs	m1.small	● running	Luan_Windows_Te	Luan_Windows_USEast_Keypair	basic	hvm	

RAM Disk ID:	-
Key Pair Name:	Luan_Window
Monitoring:	basic
Elastic IP:	-
Root Device Type:	ebs
Lifecycle:	normal
Block Devices:	sda1
Public DNS:	ec2-50-19-12
Private DNS:	ip-10-86-215-
Private IP Address:	10.86.215.12
Launch Time:	2011-05-12 0
State Transition Reason:	

Platform:	windows
Kernel ID:	-
AMI Launch Index:	0
Root Device:	sda1
Tenancy:	default

Instance Terminated



	Name	Instance	AMI ID	Root Device	Type	Status	Security Groups	Key Pair Name	Monitoring	Virtualization	Placeme
□	*empty*	i-ed54b383	ami-c3e40daa	ebs	m1.small	● terminatec	Luan_Windows_Te	Luan_Windows_USEast_Keypair	basic	hvm	

1 EC2 Instance selected

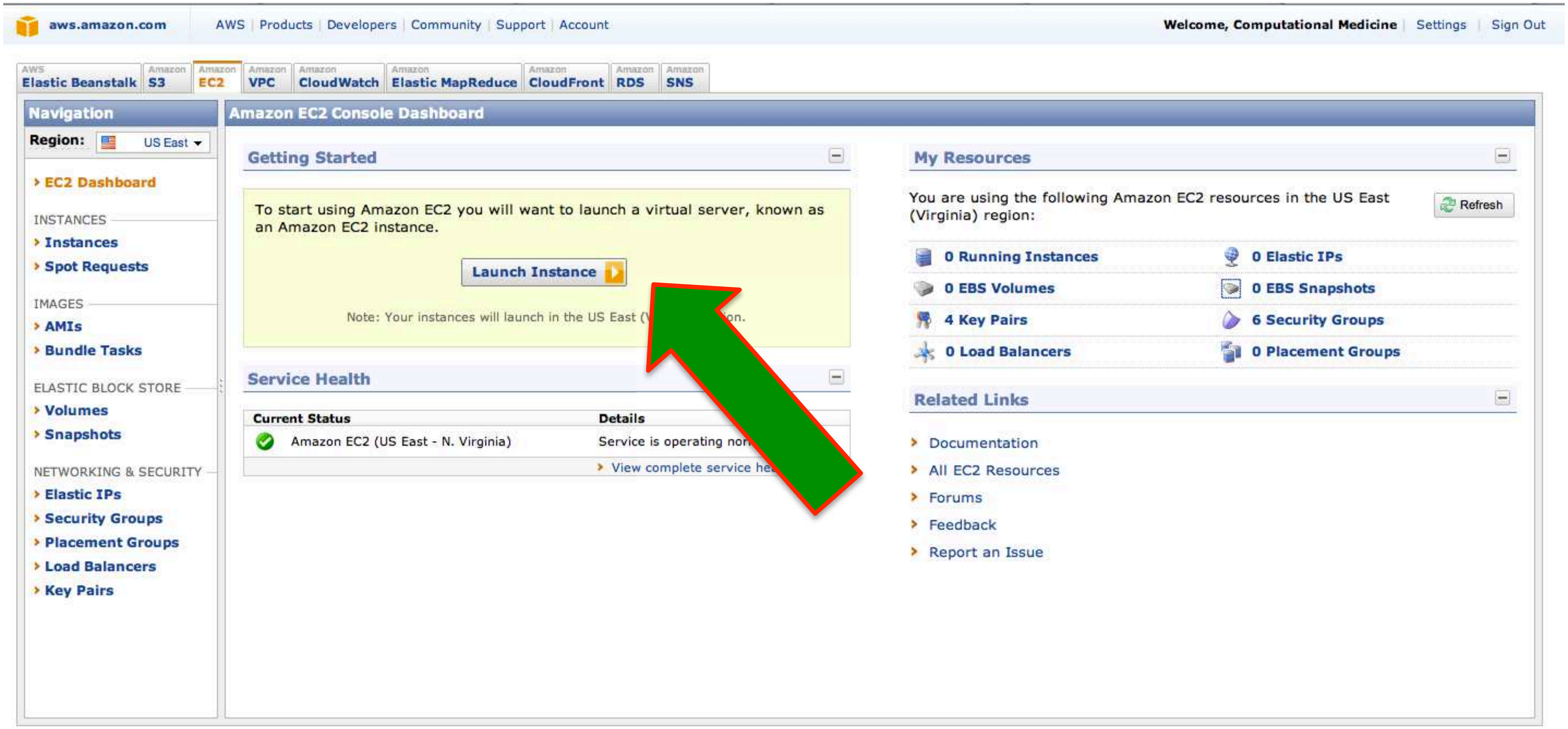
EC2 Instance: i-ed54b383

AMI:	Windows-Server2008-i386-Base-v103 (ami-c3e40daa)	**Zone:**	us-east-1a
Security Groups:	Luan_Windows_Test	**Type:**	m1.small
Status:	shutting-down	**Owner:**	994860338133
VPC ID:	-	**Subnet ID:**	-
Source/Dest. Check:		**Virtualization:**	hvm
Placement Group:		**Reservation:**	r-3553ff59
RAM Disk ID:	-	**Platform:**	windows
Key Pair Name:	Luan_Windows_USEast_Keypair	**Kernel ID:**	-

Overview

- Understanding AMI (Amazon Machine Image)
- Launching, using and shutting down a Windows instance.
- Launching, using and shutting down a Linux instance.

EC2 Tab in the Management Console



To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

Note: Your instances will launch in the US East (V   on.

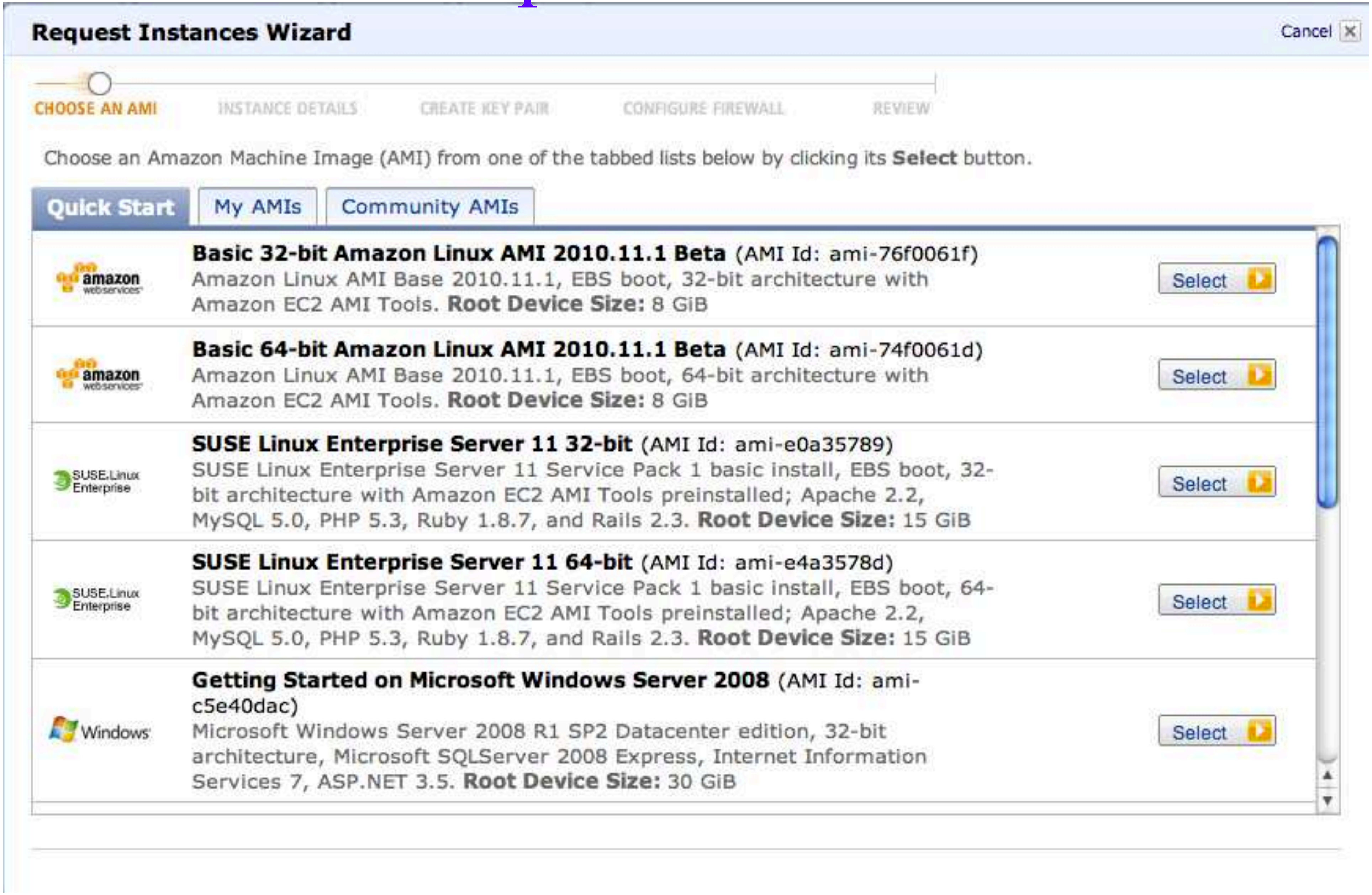
Current Status	Details
✓ Amazon EC2 (US East - N. Virginia)	Service is operating nor

View complete service he

You are using the following Amazon EC2 resources in the US East (Virginia) region:

0 Running Instances	0 Elastic IPs
0 EBS Volumes	0 EBS Snapshots
4 Key Pairs	6 Security Groups
0 Load Balancers	0 Placement Groups

Request Instance



Choose an Amazon Machine Image (AMI) from one of the tabbed lists below by clicking its **Select** button.

Basic 32-bit Amazon Linux AMI 2010.11.1 Beta (AMI Id: ami-76f0061f)
Amazon Linux AMI Base 2010.11.1, EBS boot, 32-bit architecture with Amazon EC2 AMI Tools. **Root Device Size:** 8 GiB

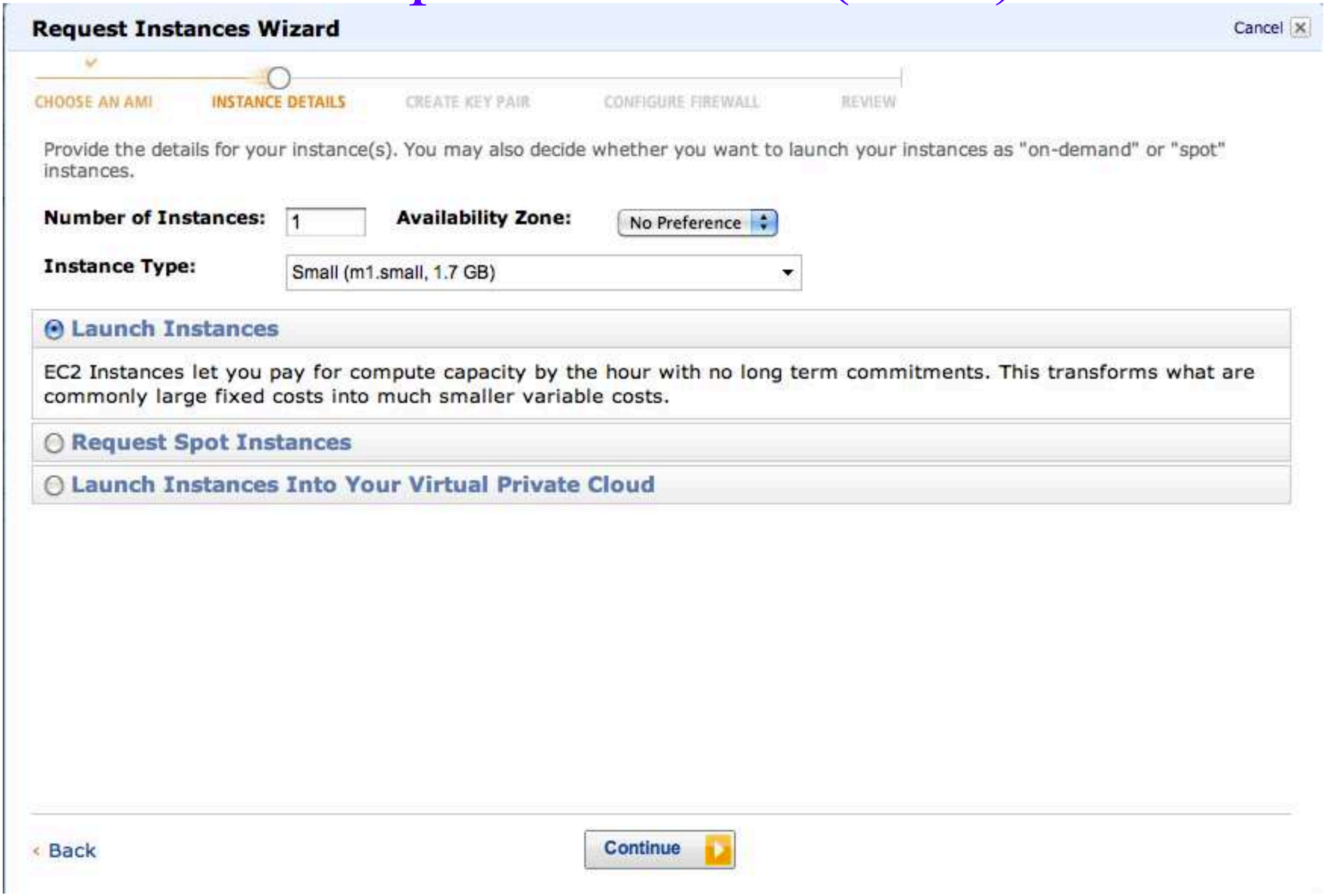
Basic 64-bit Amazon Linux AMI 2010.11.1 Beta (AMI Id: ami-74f0061d)
Amazon Linux AMI Base 2010.11.1, EBS boot, 64-bit architecture with Amazon EC2 AMI Tools. **Root Device Size:** 8 GiB

SUSE Linux Enterprise Server 11 32-bit (AMI Id: ami-e0a35789)
SUSE Linux Enterprise Server 11 Service Pack 1 basic install, EBS boot, 32-bit architecture with Amazon EC2 AMI Tools preinstalled; Apache 2.2, MySQL 5.0, PHP 5.3, Ruby 1.8.7, and Rails 2.3. **Root Device Size:** 15 GiB

SUSE Linux Enterprise Server 11 64-bit (AMI Id: ami-e4a3578d)
SUSE Linux Enterprise Server 11 Service Pack 1 basic install, EBS boot, 64-bit architecture with Amazon EC2 AMI Tools preinstalled; Apache 2.2, MySQL 5.0, PHP 5.3, Ruby 1.8.7, and Rails 2.3. **Root Device Size:** 15 GiB

Getting Started on Microsoft Windows Server 2008 (AMI Id: ami-c5e40dac)
Microsoft Windows Server 2008 R1 SP2 Datacenter edition, 32-bit architecture, Microsoft SQLServer 2008 Express, Internet Information Services 7, ASP.NET 3.5. **Root Device Size:** 30 GiB

Request Instance (cont.)



Provide the details for your instance(s). You may also decide whether you want to launch your instances as "on-demand" or "spot" instances.

Number of Instances: 1

Availability Zone: No Preference

Instance Type: Small (m1.small, 1.7 GB)

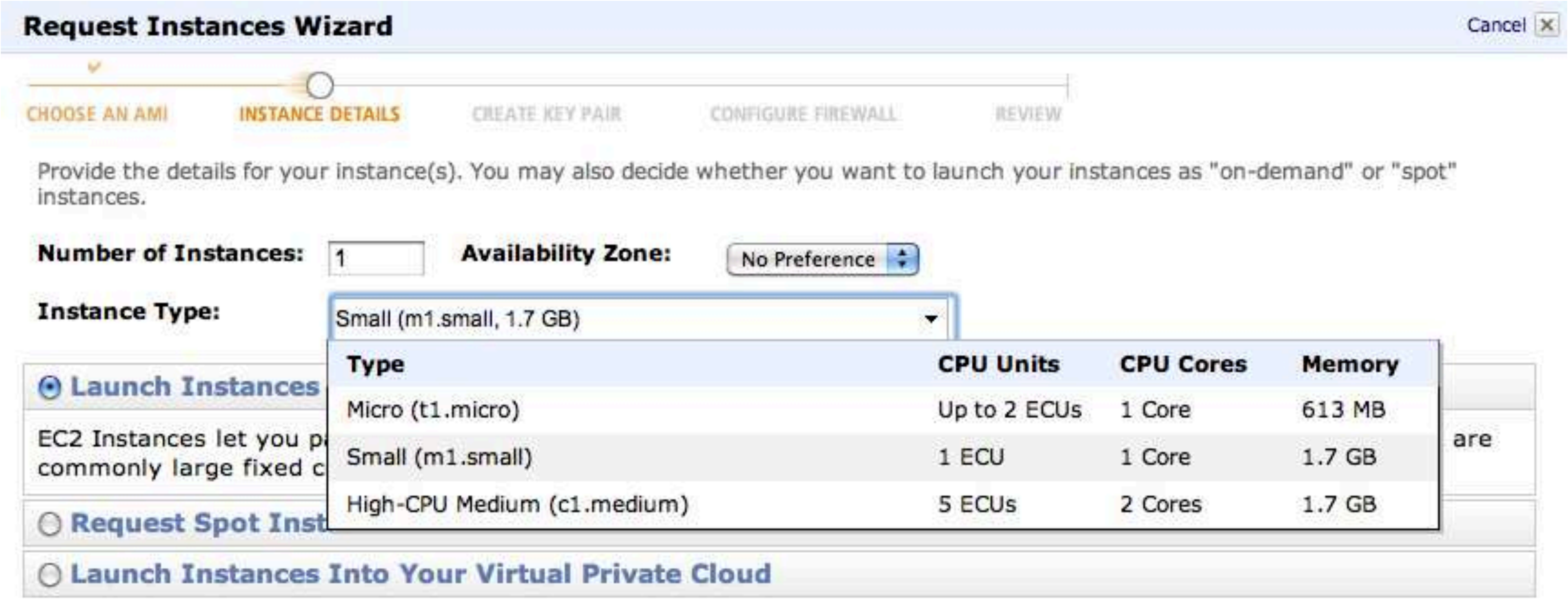
● Launch Instances

EC2 Instances let you pay for compute capacity by the hour with no long term commitments. This transforms what are commonly large fixed costs into much smaller variable costs.

○ Request Spot Instances

○ Launch Instances Into Your Virtual Private Cloud

Request Instance (cont.)



Request Instances Wizard

Cancel ☒

Provide the details for your instance(s). You may also decide whether you want to launch your instances as "on-demand" or "spot" instances.

Number of Instances: 1 **Availability Zone:** No Preference

Instance Type: Small (m1.small, 1.7 GB)

Type	CPU Units	CPU Cores	Memory
Micro (t1.micro)	Up to 2 ECUs	1 Core	613 MB
Small (m1.small)	1 ECU	1 Core	1.7 GB
High-CPU Medium (c1.medium)	5 ECUs	2 Cores	1.7 GB

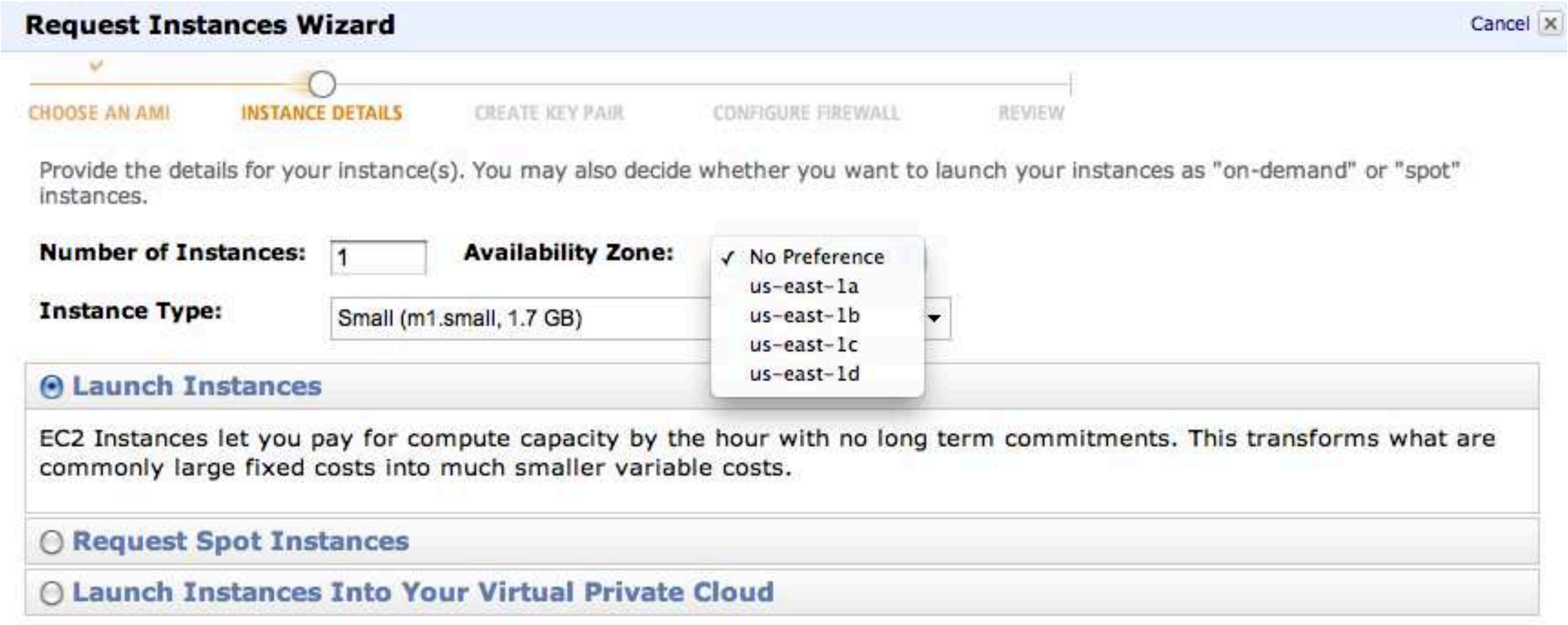
● **Launch Instances**

EC2 Instances let you pa are
commonly large fixed c

○ **Request Spot Inst**

○ **Launch Instances Into Your Virtual Private Cloud**

Request Instance (cont.)



Request Instances Wizard

Provide the details for your instance(s). You may also decide whether you want to launch your instances as "on-demand" or "spot" instances.

Number of Instances: 1

Availability Zone:
✓ No Preference
us-east-1a
us-east-1b
us-east-1c
us-east-1d

Instance Type: Small (m1.small, 1.7 GB)

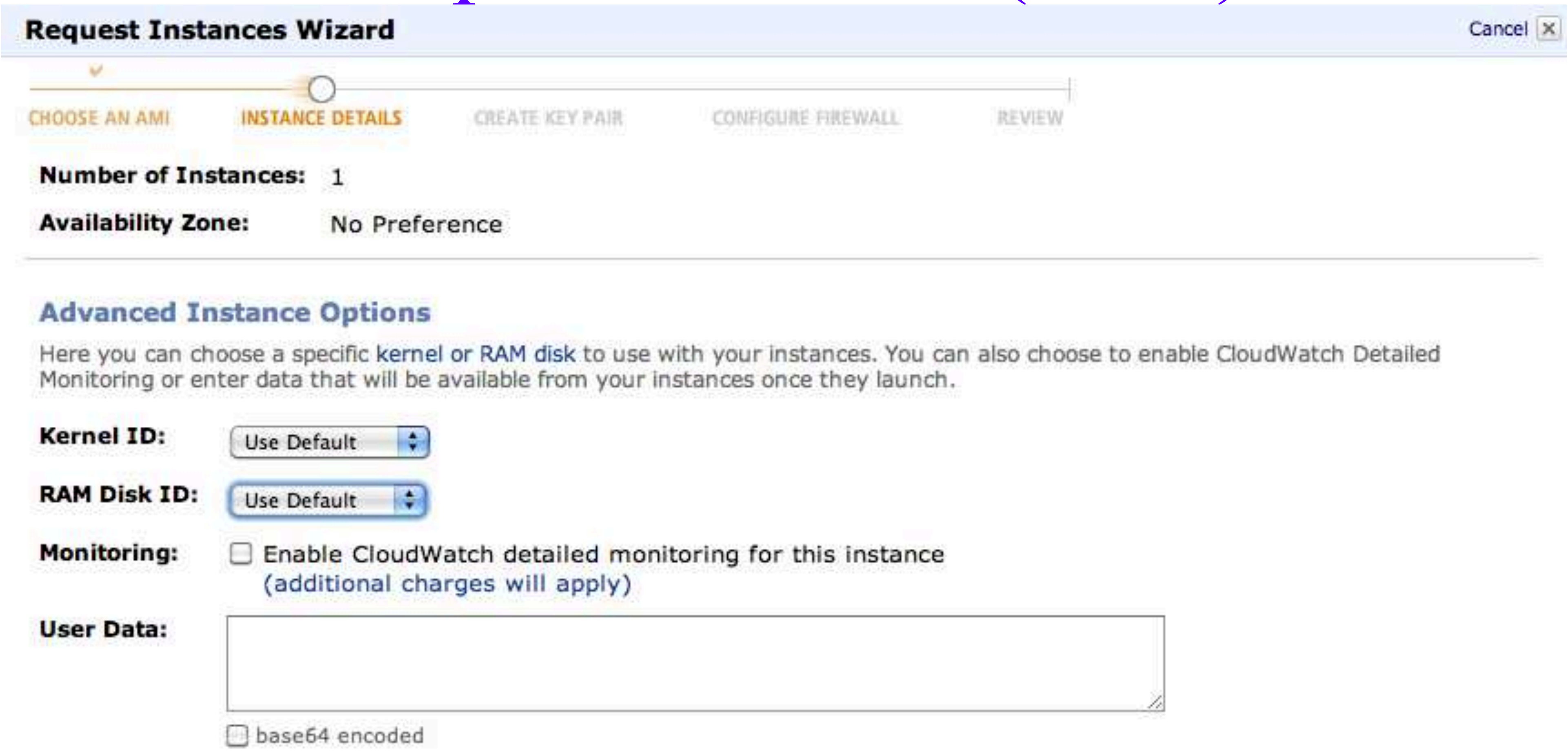
● **Launch Instances**

EC2 Instances let you pay for compute capacity by the hour with no long term commitments. This transforms what are commonly large fixed costs into much smaller variable costs.

○ **Request Spot Instances**

○ **Launch Instances Into Your Virtual Private Cloud**

Request Instance (cont.)



Number of Instances: 1

Availability Zone: No Preference

Advanced Instance Options

Here you can choose a specific kernel or RAM disk to use with your instances. You can also choose to enable CloudWatch Detailed Monitoring or enter data that will be available from your instances once they launch.

Kernel ID: Use Default

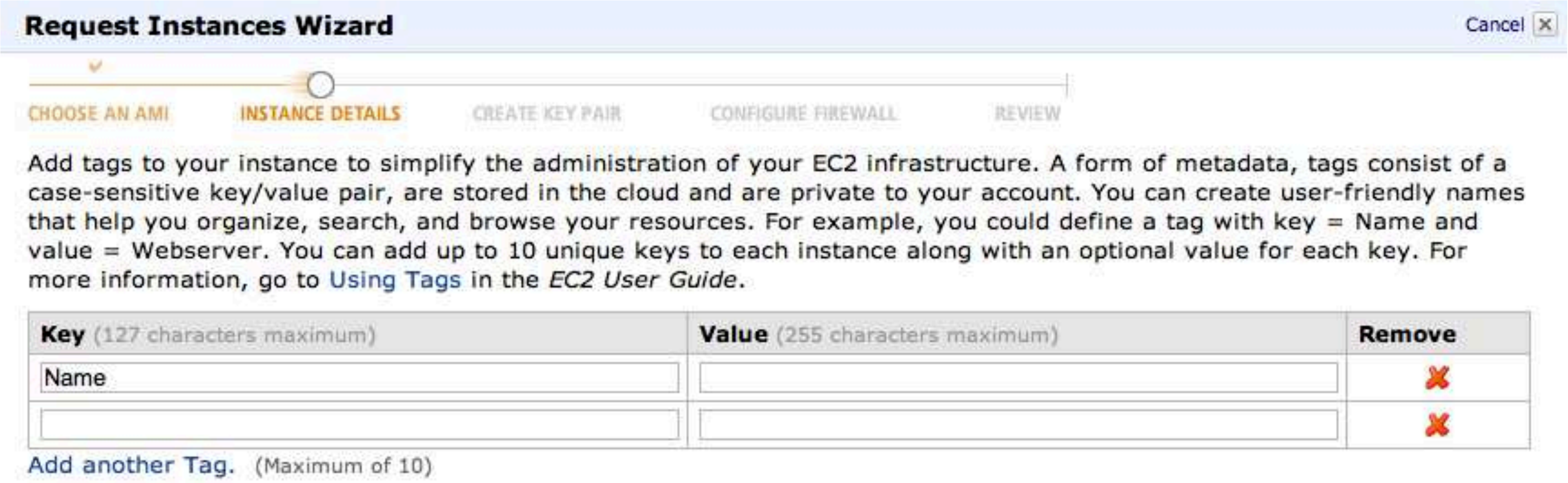
RAM Disk ID: Use Default

Monitoring: □ Enable CloudWatch detailed monitoring for this instance (additional charges will apply)

User Data:

□ base64 encoded

Request Instance (cont.)

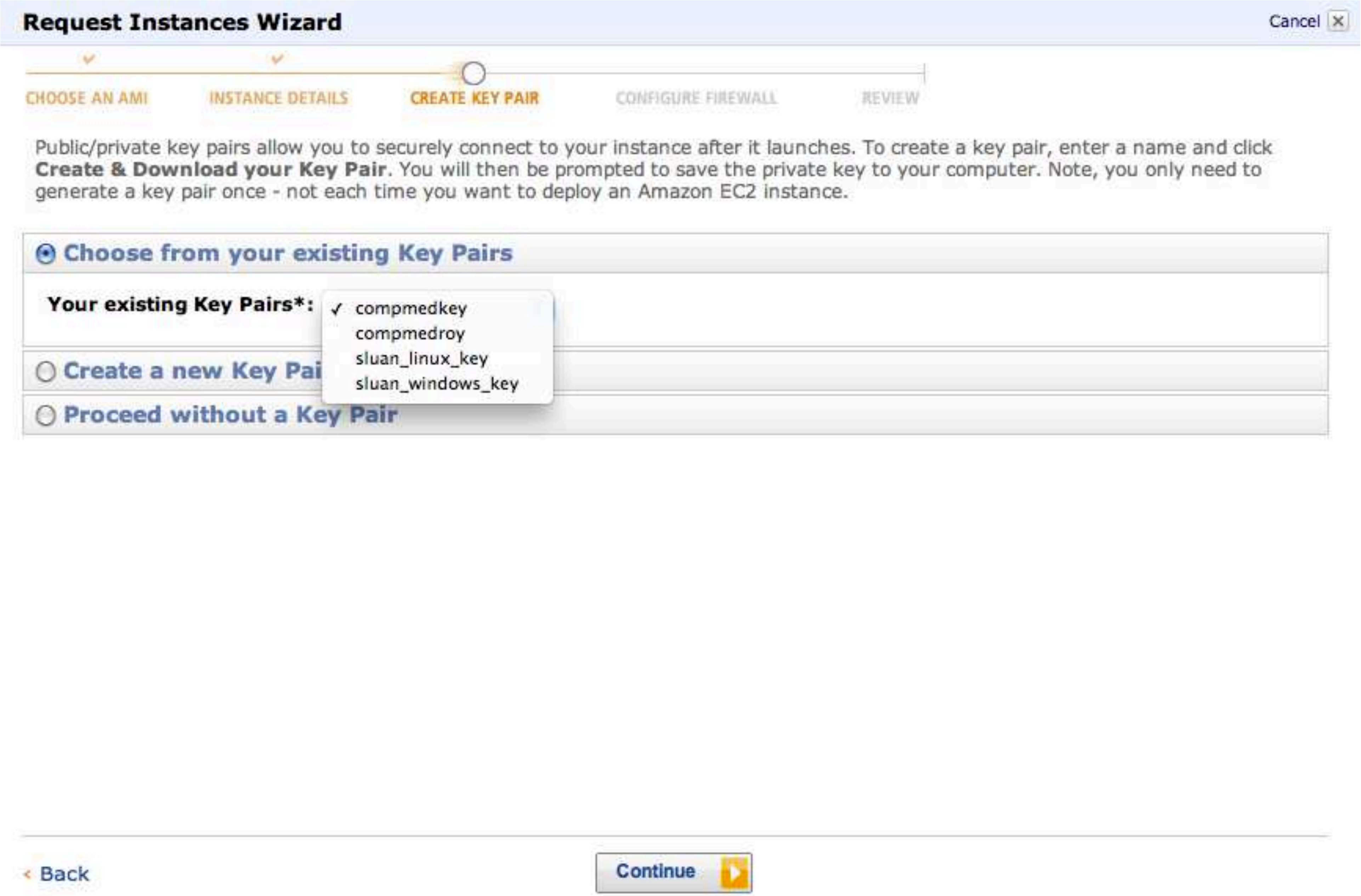


Add tags to your instance to simplify the administration of your EC2 infrastructure. A form of metadata, tags consist of a case-sensitive key/value pair, are stored in the cloud and are private to your account. You can create user-friendly names that help you organize, search, and browse your resources. For example, you could define a tag with key = Name and value = Webserver. You can add up to 10 unique keys to each instance along with an optional value for each key. For more information, go to Using Tags in the *EC2 User Guide*.

Key (127 characters maximum)	**Value** (255 characters maximum)	**Remove**
Name		✘
		✘

Add another Tag. (Maximum of 10)

Request Instance (cont.)



Public/private key pairs allow you to securely connect to your instance after it launches. To create a key pair, enter a name and click **Create & Download your Key Pair**. You will then be prompted to save the private key to your computer. Note, you only need to generate a key pair once - not each time you want to deploy an Amazon EC2 instance.

● Choose from your existing Key Pairs

Your existing Key Pairs*: ✓ compmedkey

compmedroy

sluan_linux_key

sluan_windows_key

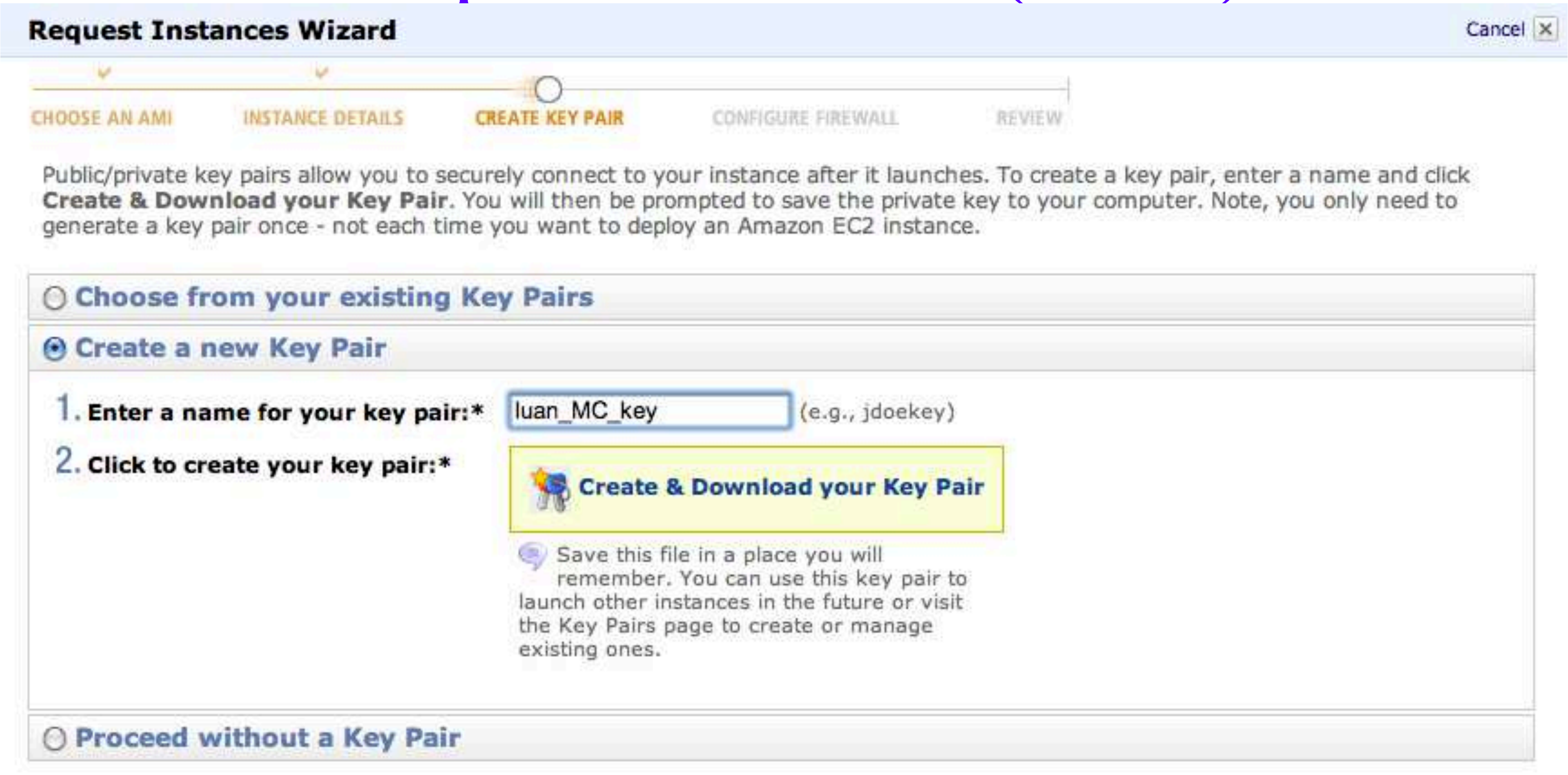
○ Create a new Key Pai

○ Proceed without a Key Pair

Key Pair

- A key pair is a security credential similar to a password, which you use to securely connect to your instance once it's running.

Request Instance (cont.)



Request Instances Wizard

Public/private key pairs allow you to securely connect to your instance after it launches. To create a key pair, enter a name and click **Create & Download your Key Pair**. You will then be prompted to save the private key to your computer. Note, you only need to generate a key pair once - not each time you want to deploy an Amazon EC2 instance.

○ **Choose from your existing Key Pairs**

● **Create a new Key Pair**

1. **Enter a name for your key pair:*** luan_MC_key (e.g., jdoekey)
2. **Click to create your key pair:*** **Create & Download your Key Pair**

Save this file in a place you will remember. You can use this key pair to launch other instances in the future or visit the Key Pairs page to create or manage existing ones.

○ **Proceed without a Key Pair**

Secure Shell (SSH)

- Designed to replace Telnet, which send information, notably passwords, in plaintext.
- Intended to provide confidentiality and integrity of data over an unsecured network such as the Internet.
- Uses public-key cryptography to authenticate the remote computer and the user.

SSH Preparation: Client

- As a user, you generate an “identity” on the client system by running the ssh-keygen.
- This program creates a subdirectory $HOME/.ssh and inserts in it two files named identity and identity.pub which contain your private and public keys for your account on the client system.
- This latter file can then be appended to a file $HOME/.ssh/authorized_keys that should reside on any/all servers where you will make ssh connections.

SSH Preparation: Server

- As a system administrator, you generate a public and private key pair for the system itself.
- If someone wants to fake the server, they will have to break into the system and steal its private key.
- The biggest task is collecting and distributing the keys that identify all the hosts which run ssh.

SSH Authentication

- A user attempts to SSH into the server.
- The server sends its PUBLIC KEY to the user.
- The user checks to see if the PUBLIC KEY exists already in its system. If not, the user is warned. Once the user accepts the key, it is added to the trusted list.
- The user uses the server's PUBLIC KEY to encrypt all communications to the server.
- At the initial stage, this would include user name, password.

SSH Authentication (cont.)

- The user also sends it's PUBLIC KEY to the server. (NOT the same as the Server's PUBLIC KEY).
- The server uses it's own PRIVATE KEY to decrypt all communications from the user (encrypted using the server's PUBLIC KEY). The server then uses the user's PUBLIC KEY to encrypt all communications to the user.
- The user uses it's PRIVATE KEY to decrypt all communications sent by the server (encrypted using the user's PUBLIC KEY).