

## Lab 3

### CREATE YOUR FIRST AMAZON EC2 INSTANCE (WINDOWS)



## STEP 1: Log In to the Amazon Web Service Console

This laboratory experience is about Amazon Web Services and you will use the AWS Management Console in order to complete all the lab steps.

The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with 'Services' and 'Cost Explorer' tabs, and a user profile for 'Antonio Ang' in the 'Oregon' region. The main content area is titled 'Amazon Web Services' and is divided into several categories of services:

- Compute:** EC2 (Virtual Servers in the Cloud), Lambda PREVIEW (Run Code in Response to Events).
- Storage & Content Delivery:** S3 (Scalable Storage in the Cloud), Storage Gateway (Integrates On-Premises IT Environments with Cloud Storage), Glacier (Archive Storage in the Cloud), CloudFront (Global Content Delivery Network).
- Database:** RDS (MySQL, Postgres, Oracle, SQL Server, and Amazon Aurora), DynamoDB (Predictable and Scalable NoSQL Data Store), ElastiCache (In-Memory Cache), Redshift (Managed Petabyte-Scale Data Warehouse Service).
- Networking:** VPC (Isolated Cloud Resources), Direct Connect (Dedicated Network Connection to AWS), Route 53 (Scalable DNS and Domain Name Registration).
- Administration & Security:** Directory Service (Managed Directories in the Cloud), Identity & Access Management (Access Control and Key Management), Trusted Advisor (AWS Cloud Optimization Expert), CloudTrail (User Activity and Change Tracking), Config PREVIEW (Resource Configurations and Inventory), CloudWatch (Resource and Application Monitoring).
- Deployment & Management:** Elastic Beanstalk (AWS Application Container), OpsWorks (DevOps Application Management Service), CloudFormation (Templated AWS Resource Creation), CodeDeploy (Automated Deployments).
- Analytics:** EMR (Managed Hadoop Framework), Kinesis (Real-time Processing of Streaming Big Data), Data Pipeline (Orchestration for Data-Driven Workflows).
- Application Services:** SQS (Message Queue Service), SWF (Workflow Service for Coordinating Application Components), AppStream (Low Latency Application Streaming), Elastic Transcoder (Easy-to-use Scalable Media Transcoding), SES (Email Sending Service), CloudSearch (Managed Search Service).
- Mobile Services:** Cognito (User Identity and App Data Synchronization), Mobile Analytics (Understand App Usage Data at Scale), SNS (Push Notification Service).
- Enterprise Applications:** WorkSpaces (Desktops in the Cloud), Zocalo (Secure Enterprise Storage and Sharing Service).

On the right side, there are additional resources and service health information:

- Additional Resources:** Getting Started (See our documentation to get started and learn more about how to use our services.), AWS Console Mobile App (View your resources on the go with our AWS Console mobile app, available from Amazon Appstore, Google Play, or iTunes.), AWS Marketplace (Find and buy software, launch with 1-Click and pay by the hour.).
- Service Health:** All services operating normally. Updated: Nov 20 2014 12:57:00 GMT-0800. Service Health Dashboard.
- Set Start Page:** Console Home.

The AWS Management Console is a web control panel for managing all your AWS resources, from EC2 instances to SNS topics. The console enables cloud management for all aspects of the AWS account, including managing security credentials, or even setting up new IAM Users.

## Log in to the AWS Management Console

In order to start the laboratory experience, open the Amazon Console by clicking this button:

[Open AWS Console](#)

Log in with the username **xxxxx** and the password **xxxxx**.



Account:

User Name:

Password:



I have an MFA Token [\(more info\)](#)

Sign In

[Sign in using root account credentials](#)

[Terms of Use](#) [Privacy Policy](#)

© 1996-2014, Amazon Web Services, Inc. or its affiliates.

## Select the right AWS Region

Amazon Web Services is available in different regions all over the world, and the console lets you provision resources across multiple regions. You usually choose a region that best suits your business needs to optimize your customer's experience, but you must use the region **US West (Oregon)** for this laboratory.

You can select the **US West (Oregon)** region using the upper right dropdown menu on the AWS Console page.

Antonio Ang ▾ Region ▾ Support ▾

US East (N. Virginia)

| **US West (Oregon)**

US West (N. California)

EU (Ireland)

EU (Frankfurt)

Asia Pacific (Singapore)

Asia Pacific (Tokyo)

Asia Pacific (Sydney)

South America (São Paulo)

## STEP 2: Create a Windows EC2 instance

You can launch an EC2 instance using the EC2 launch wizard.

Select the EC2 service from the Management Console dashboard:

### Compute



### EC2

Virtual Servers in the Cloud

From the EC2 dashboard, click **Launch Instance**.

**EC2 Dashboard**

- Events
- Tags
- Reports
- Limits
- INSTANCES
  - Instances
  - Spot Requests
  - Reserved Instances
- IMAGES
  - AMIs
  - Bundle Tasks

**Resources**

You are using the following Amazon EC2 resources in the US West (Oregon) region:

0 Running Instances	1 Elastic IPs
0 Volumes	0 Snapshots
0 Key Pairs	0 Load Balancers
0 Placement Groups	2 Security Groups

**Create Instance**

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

**Launch Instance**

Note: Your Instances will launch in the US West (Oregon) region

The **Choose an Amazon Machine Image (AMI)** page displays a list of basic configurations called **Amazon Machine Images (AMIs)** that serve as templates for your instance. Select the **Microsoft Windows Server 2012 R2 Base** AMI.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

## Step 1: Choose an Amazon Machine Image (AMI)

Cancel and Exit

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace, or you can select one of your own AMIs.

Quick Start < 1 to 22 of 22 AMIs >

**My AMIs**

**AWS Marketplace**

**Community AMIs**

☐ Free tier only (1)

	<b>Amazon Linux AMI 2014.09.2 (HVM) - ami-dfc39aef</b>	<b>Select</b>
Amazon Linux	The Amazon Linux AMI is an EBS backed image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Apache HTTPD, Docker, PHP, MySQL, PostgreSQL, and other packages.	64-bit
Root device type: ebs	Virtualization type: hvm	
	<b>Red Hat Enterprise Linux 6.6 (HVM), SSD Volume Type - ami-0b5f073b</b>	<b>Select</b>
Red Hat	Red Hat Enterprise Linux version 6.6 (HVM), EBS General Purpose (SSD) Volume Type	64-bit
Root device type: ebs	Virtualization type: hvm	
	<b>SUSE Linux Enterprise Server 12 (HVM), SSD Volume Type - ami-d7450be7</b>	<b>Select</b>
SUSE Linux	SUSE Linux Enterprise Server 12 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.	64-bit
Root device type: ebs	Virtualization type: hvm	
	<b>Ubuntu Server 14.04 LTS (HVM), SSD Volume Type - ami-29ebb519</b>	<b>Select</b>
Ubuntu	Ubuntu Server 14.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical ( <a href="http://www.ubuntu.com/cloud/services">http://www.ubuntu.com/cloud/services</a> ).	64-bit
Root device type: ebs	Virtualization type: hvm	
	<b>Microsoft Windows Server 2012 R2 Base - ami-59f2d769</b>	<b>Select</b>
Windows	Microsoft Windows 2012 R2 Standard edition with 64-bit architecture. [English]	64-bit
Root device type: ebs	Virtualization type: hvm	

On the **Choose an Instance Type** page, do **not** change any options and click **Next: Configure Instance Details**.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

## Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by: **All instance types** **Current generation** **Show/Hide Columns**

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs (1)	Memory (GiB)	Instance Storage (GiB) (1)	EBS-Optimized Instance (1)	Network Performance (1)
	General purpose	t2.micro <b>Free tier eligible</b>	1	1	EBS only	-	Low to Moderate
	General purpose	t2.small	1	2	EBS only	-	Low to Moderate

[Cancel](#)
[Previous](#)
[Review and Launch](#)
[Next: Configure Instance Details](#)

On the **Configure Instance Details** tab, check the selected **Network (VPC)** and **Subnet**. Change them if needed and then click **Next : Add Storage**.


1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review


### Step 3: Configure Instance Details


Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot Instances to take advantage of the lower pricing, assign an access management role to the instance, and more.


Number of instances ① 1


Purchasing option ① ☐ Request Spot Instances

Network ① vpc-a144e4c4 (10.0.0.0/16)  Create new VPC

Subnet ① subnet-6931e2e2 (10.0.0.0/24) | Public-A | us-west-2a  Create new subnet  
251 IP Addresses available


Auto-assign Public IP ① Use subnet setting (Disable) 

IAM role ① None 



Shutdown behavior ① Stop 


Enable termination protection ① ☐ Protect against accidental termination



Monitoring ① ☐ Enable CloudWatch detailed monitoring  
Additional charges apply.

Tenancy ① Shared tenancy (multi-tenant hardware)   
Additional charges will apply for dedicated tenancy.

▼ Network Interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses
eth0	New network interface 	subnet-6931e2e2 (F) 	Auto-assign	Add IP



Cancel  **Review and Launch** 

On the **Add Storage** tab, do **not** change any options and click the **Review and Launch** button.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review


## Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

**⚠ Improve your instances' security. Your security group, launch-wizard-2, is open to the world.**

Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

**AMI Details**

 **Microsoft Windows Server 2012 R2 Base - ami-69f2d769**

Free tier eligible

Microsoft Windows 2012 R2 Standard edition with 64-bit architecture. [English]

Root Device Type: ebs Virtualization type: hvm

[Edit AMI](#)

**Instance Type**

Instance Type	Architecture	OS	Storage	Network Performance
t2.micro	Variable	1	1	EBS only

[Edit instance type](#)

**Security Groups**

Security group name launch-wizard-2

Description launch-wizard-2 created 2015-02-24T11:51:55.470+01:00

Type	Protocol	Port Range	Source
RDP	TCP	3389	0.0.0.0/0

[Edit security groups](#)

**Instance Details**

**Storage**

[Edit instance details](#)

[Edit storage](#)

[Cancel](#) [Previous](#) **Launch**

On the **Review Instance Launch** page, click **Launch**.

In the **Select an existing key pair or create a new key pair** dialog box, select **create a new key pair**. Type a new key pair name (e.g., TestKeys), and **Download Key Pair**.

Click **Launch Instances**.

A confirmation page will let you know that your instance is launching. Click **View Instances** to close the confirmation page and return to the console.

On the Instances screen, you can view the status of your instance. It will take a short time for your instance to be launched. When you launch an instance, its initial state is *pending*. After the instance starts, its state changes to *running*, and it receives a public DNS name.



Launch Instance Connect Actions

Search: i-1344401f Add filter

Name	Status	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS	Public IP	Key Name
		i-1344401f	t2.micro	us-west-2a	running	2/2 checks passed	None	ec2-52-10-185-68.us-west-2.compute.amazonaws.com	52.10.185.68	windows

Instance: i-1344401f Public DNS: ec2-52-10-185-68.us-west-2.compute.amazonaws.com

Description

Instance ID: i-1344401f

Instance state: running

Instance type: t2.micro

Private DNS: ip-172-31-14-69.us-west-2.compute.internal

Private IPs: 172.31.14.69

Secondary private IPs:

VPC ID: vpc-955df3f0

Subnet ID: subnet-e5648b2

Network interfaces: eth0

Source/dest. check: True

EBS-optimized: False

Root device type: ebs

Root device: /dev/sda1

Block devices: /dev/sda1

Public DNS: ec2-52-10-185-68.us-west-2.compute.amazonaws.com

Public IP: 52.10.185.68

Elastic IP: -

Availability zone: us-west-2a

Security groups: launch-wizard-2. view rules

Scheduled events: No scheduled events

AMI ID: Windows\_Server-2012-R2\_RTM-English-64Bit-Base-2015.02.11 (ami-692d7f96)

Platform: windows

IAM role: -

Key pair name: windows

Owner: 820056880012

Launch time: February 24, 2015 12:00:28 PM UTC+1 (less than one hour)

Termination protection: False

Lifecycle: normal

Monitoring: basic

Alarm status: None

Kernel ID: -

RAM disk ID: -

### STEP 3: Retrieve the Administrator password using the Keypair

Amazon EC2 uses public-key cryptography to encrypt and decrypt login information. Public-key cryptography uses a public key to encrypt a piece of data, such as a password, then the recipient uses the private key to decrypt the data. The public and private keys are known as a key pair. To log in to your instance, you must create a key pair, specify the name of the key pair when you launch the instance, and provide the private key when you connect to the instance.

Linux instances have no password, and you use a keypair to log in using SSH. **Windows** instances have an auto-generated Administrator password that you can retrieve using the keypair file.

Wait a few minutes after the instance is running, and then select the EC2 service from the Management Console dashboard:

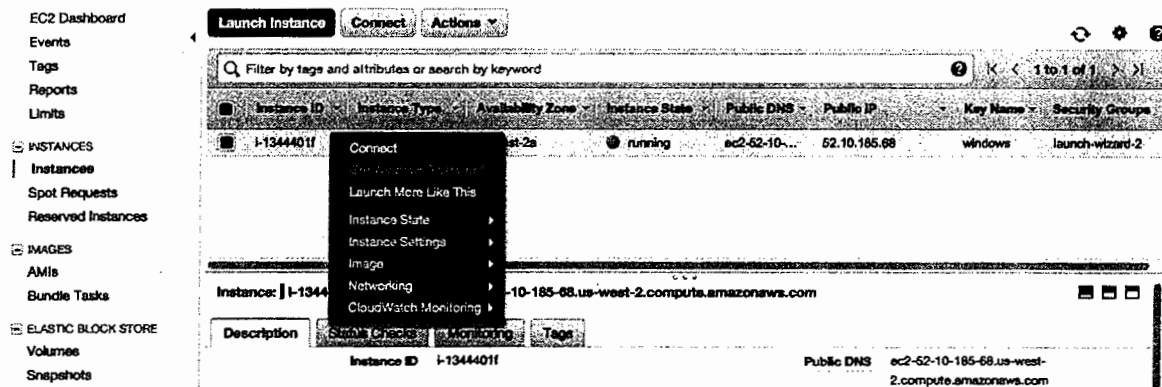
Compute



EC2

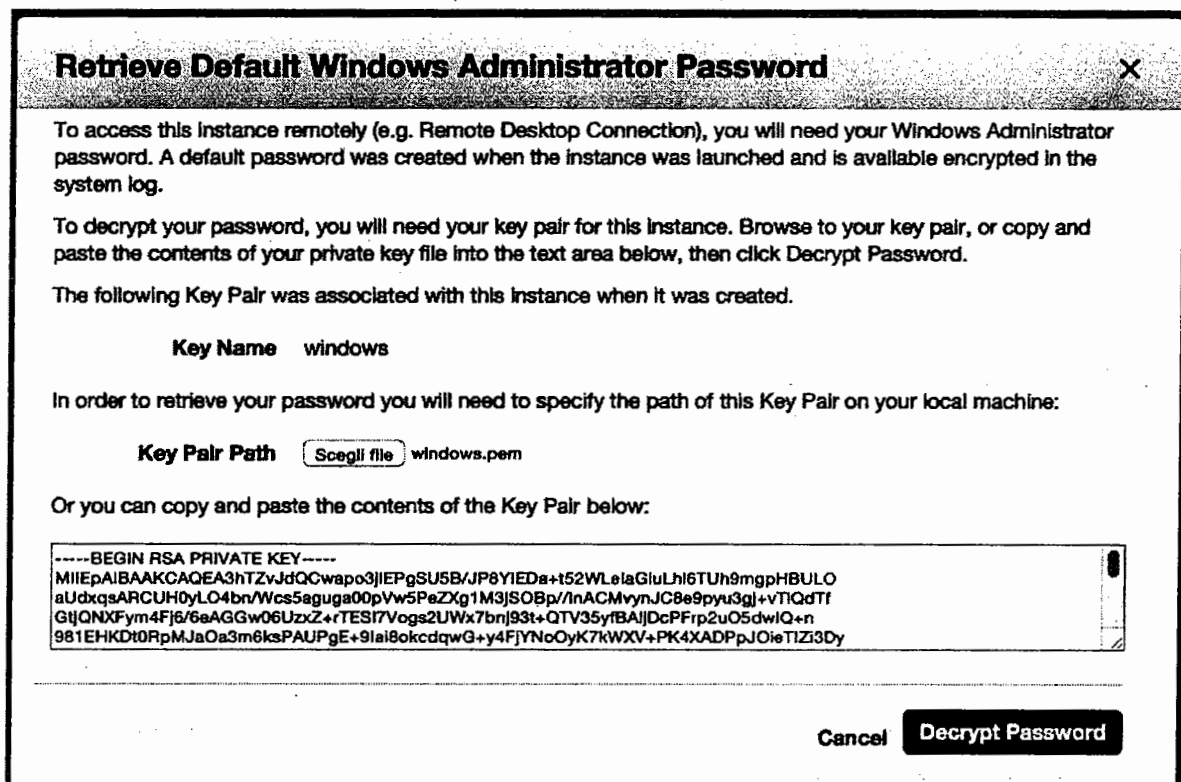
Virtual Servers in the Cloud

On the **Instances** page, select your instance, right click on it and then click **Get Windows Password**.

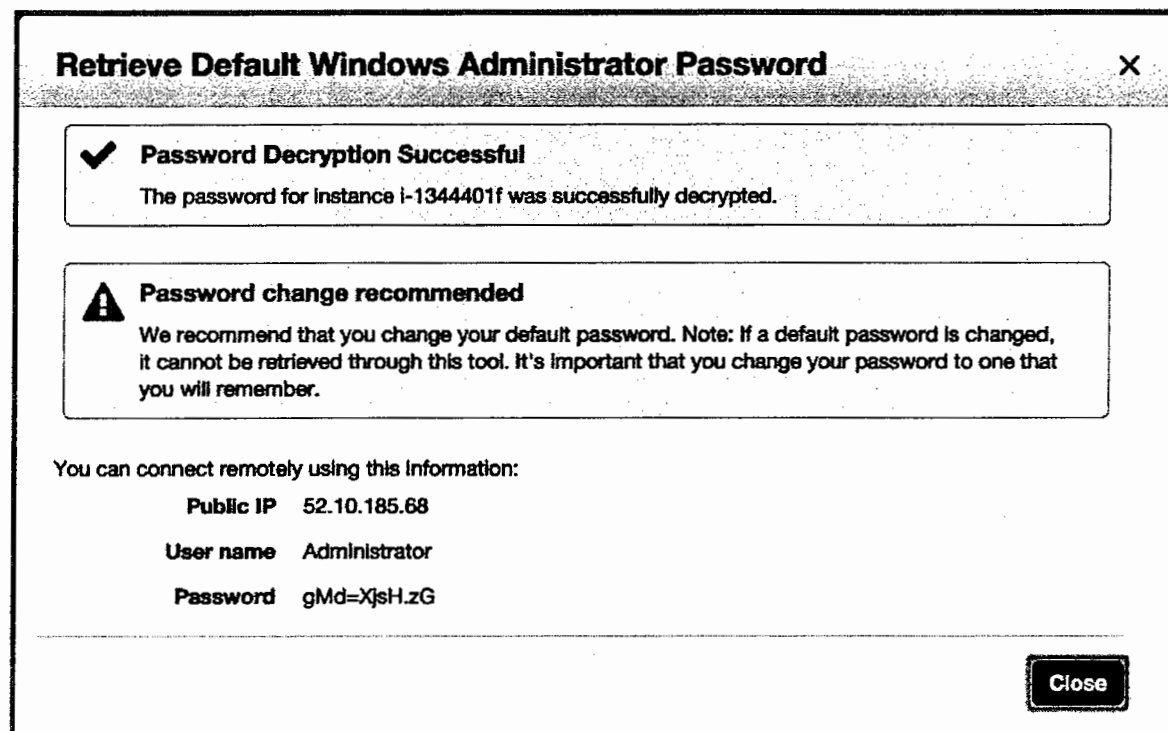


In the **Retrieve Default Windows Administrator Password** dialog box, click **Choose File**, browse to the private key file (.pem) that you previously downloaded, and then click **Open**.

Click **Decrypt Password**.



The console displays the default Administrator password for the instance. Save the password or copy it to the clipboard, as you will need it to authenticate to the instance.



#### STEP 4: Connect to a Windows instance using a Remote Desktop connection

You can connect to a server running Windows from another computer using the **Remote Desktop Protocol (RDP)**. RDP is a proprietary protocol developed by Microsoft.

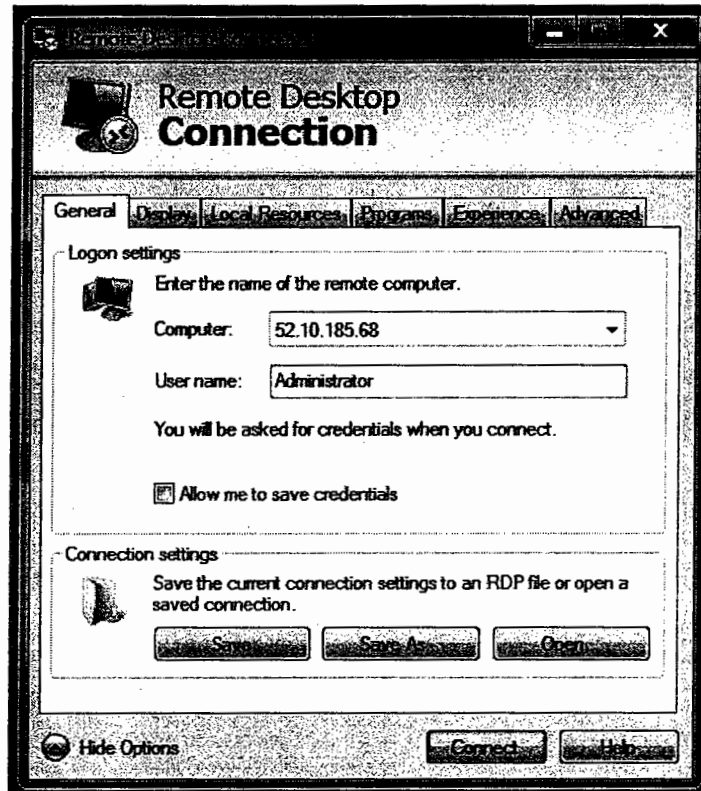
**Remote Desktop** clients exist for all versions of Microsoft Windows, GNU/Linux, and OS X operating systems. RDP servers are built into Windows operating systems and they listen on **TCP** port **3389** and **UDP** port **3389**.

Using the built-in Remote Desktop Client on Windows

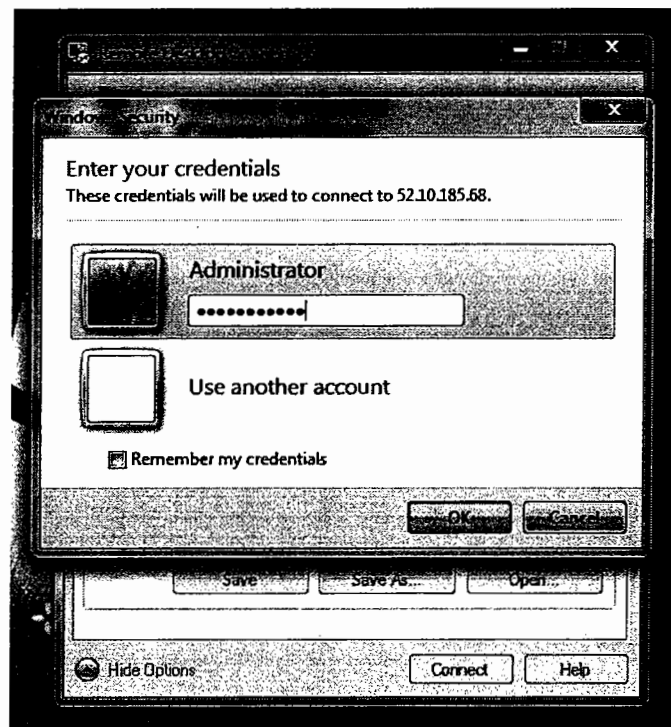
If you're using **Windows 7**, you can launch the Remote Desktop Connection client from the Start Menu. Navigate to the *Accessories* group and click the *Remote Desktop Connection* shortcut.

If you're using **Windows 8** or greater, you can launch the Remote Desktop Connection from the Start screen. Switch to the *Start* screen, type the word "remote" and then click the *Remote Desktop Connection* search result.

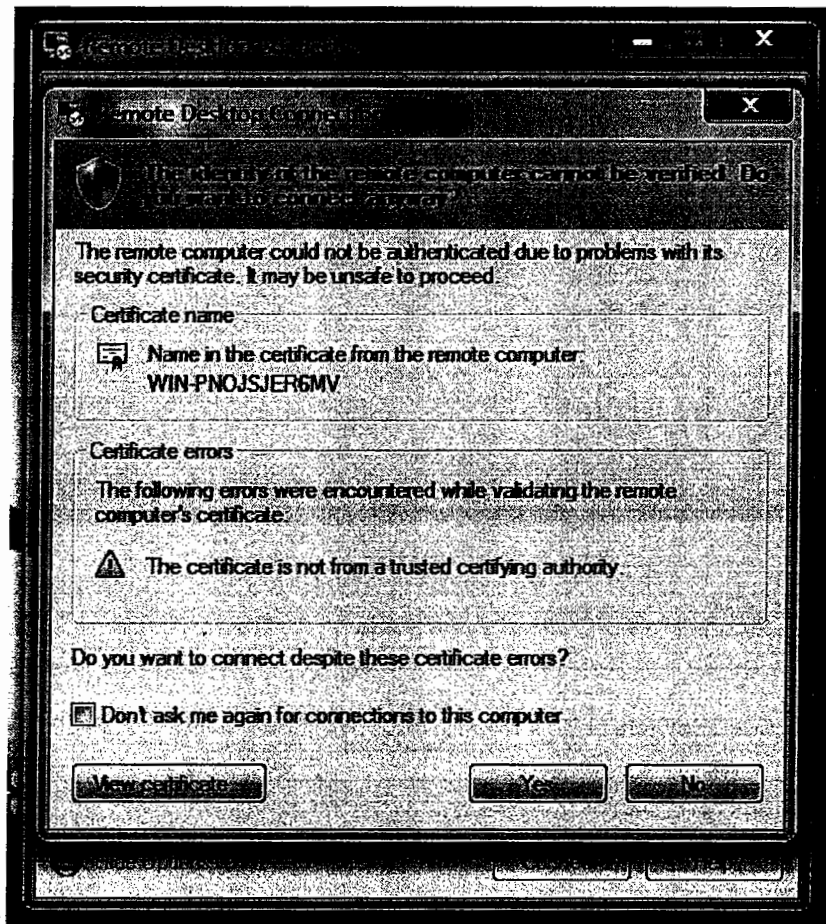
Once the Remote Desktop Connection client is launched, you'll be able to type the instance public IP and connect right away.



Enter your Administrator username and password when the Windows Security window appears.



You'll see a warning about the server name on the certificate not matching the computer name you entered. As long as the certificate name displayed is something you recognize, it's safe to click Yes and continue.



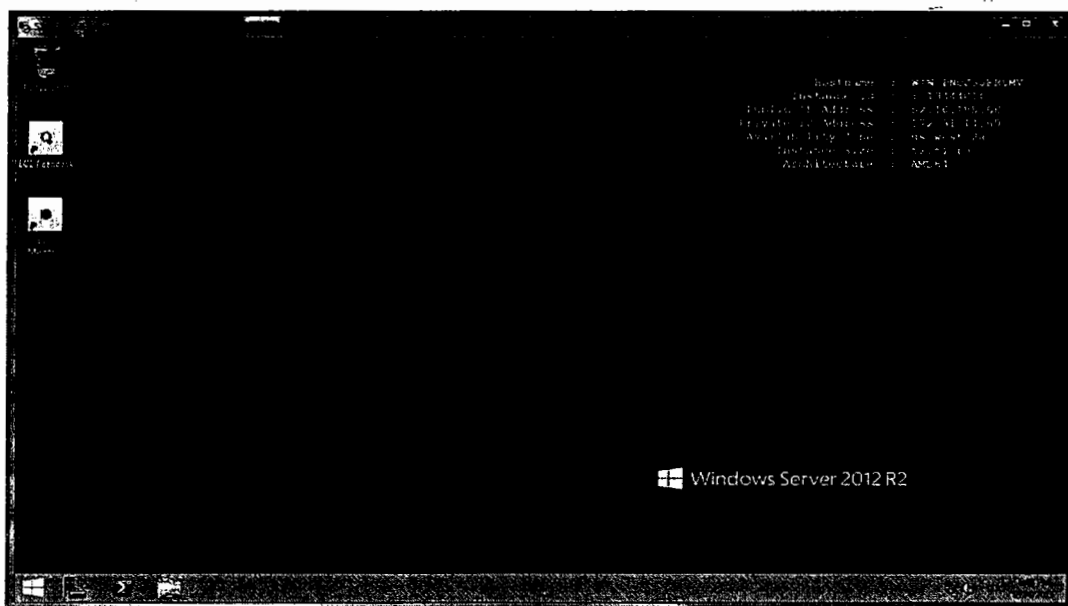
Ok, you are in. The Remote Desktop connection has been successfully established and you are able to see the server desktop of the Administrator user.



#### STEP 5: Get the EC2 instance metadata (Windows)

Now you are ready to send the first commands to your EC2 Windows instance. Let's check the EC2 instance metadata by hitting a specific AWS node only available from the instance itself.

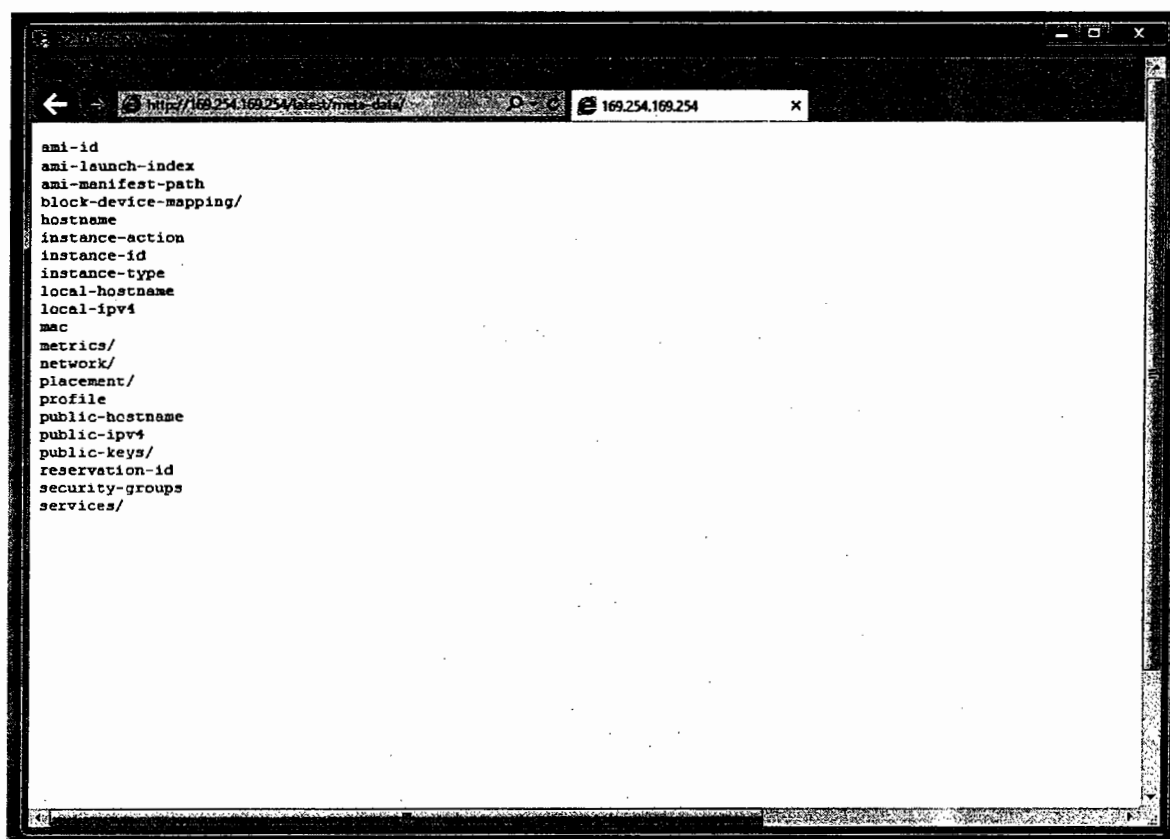
**Instance metadata** is data about your instance that you can use to configure or manage the running instance. You can find a recap of the most important instance metadata (hostname, instance ID and type, public and private IP address and the availability zone) on the desktop of your Windows instance.



If you want to retrieve and use them in a PowerShell script, you can query a private link-local IP address using the HTTP protocol.

You can list all instance metadata types by browsing the following page using Internet Explorer:

<http://169.254.169.254/latest/meta-data/>



You can easily check the list of security groups attached to the instance, its ID, the hostname, or the ID of the AMI on which the instance was based. These HTTP resources are extremely useful if you want to automate the setup of new instances:

<http://169.254.169.254/latest/meta-data/security-groups>

<http://169.254.169.254/latest/meta-data/ami-id>

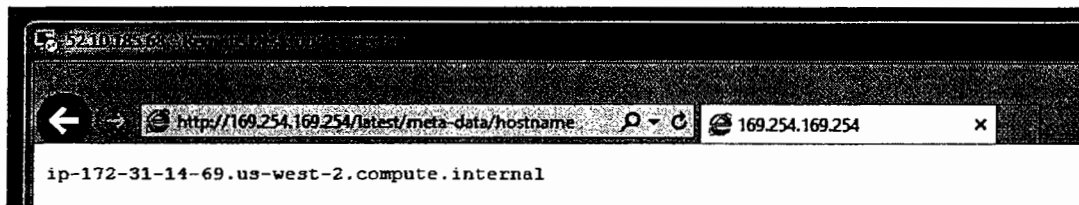
<http://169.254.169.254/latest/meta-data/hostname>

<http://169.254.169.254/latest/meta-data/instance-id>

<http://169.254.169.254/latest/meta-data/instance-type>

Here is a sample response that you can read by querying the hostname metadata resource.





## STEP 6: Terminate an EC2 instance

When you've decided that you no longer need an instance, you can terminate it.

Select the EC2 service from the Management Console dashboard:

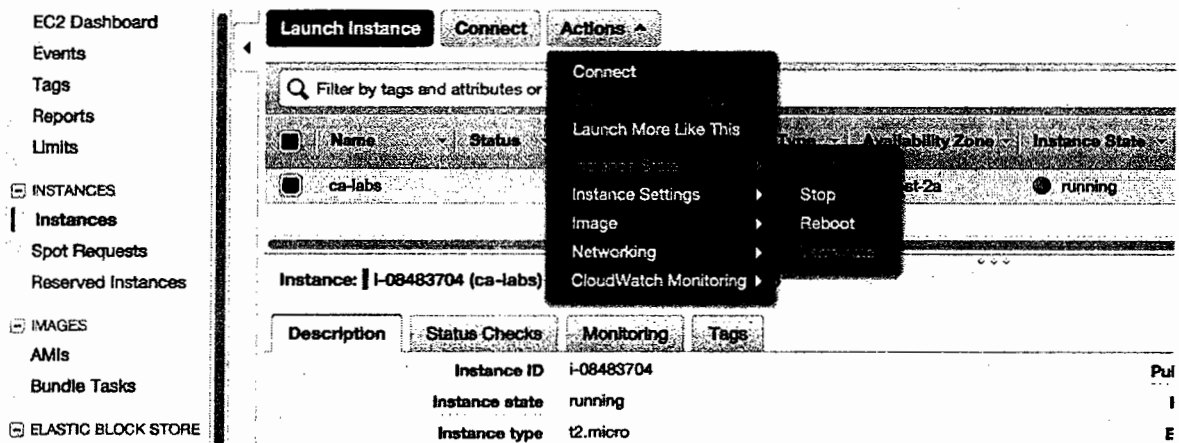
### Compute



### EC2

Virtual Servers in the Cloud

In the navigation pane, click **Instances**.



Select the instance windows, click **Actions**, select **Instance State**, and then click **Terminate**.

Click **Yes, Terminate** when prompted for confirmation.

Terminate Instances

Warning

On an EBS-backed instance, the default action is for the root EBS volume to be deleted when the instance is terminated. Storage on any local drives will be lost.

Are you sure you want to terminate these instances?  
i-08483704 (ca-labs)

Clean up associated resources

Associated resources may incur costs after these instances are terminated.

Release attached Elastic IPs

Cancel

Yes, Terminate

Now your instance is completely destroyed.

Launch Instance

Connect

Actions

Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name	Status	Instance ID	Instance Type	Availability Zone	Instance State
<input type="checkbox"/>	ca-labs		i-08483704	t2.micro	us-west-2a	terminated