



Immersion Day

*Getting Started with Windows Server on
Amazon EC2*

November 2020

Table of Contents

Overview.....	3
Launch a Web Server Instance	4
Browse the Web Server.....	11
Connecting To Your Windows Instance.....	12
Appendix – Additional EC2 Concepts.....	14
Change the Instance Type.....	14
Black Belt Booting	16

Overview

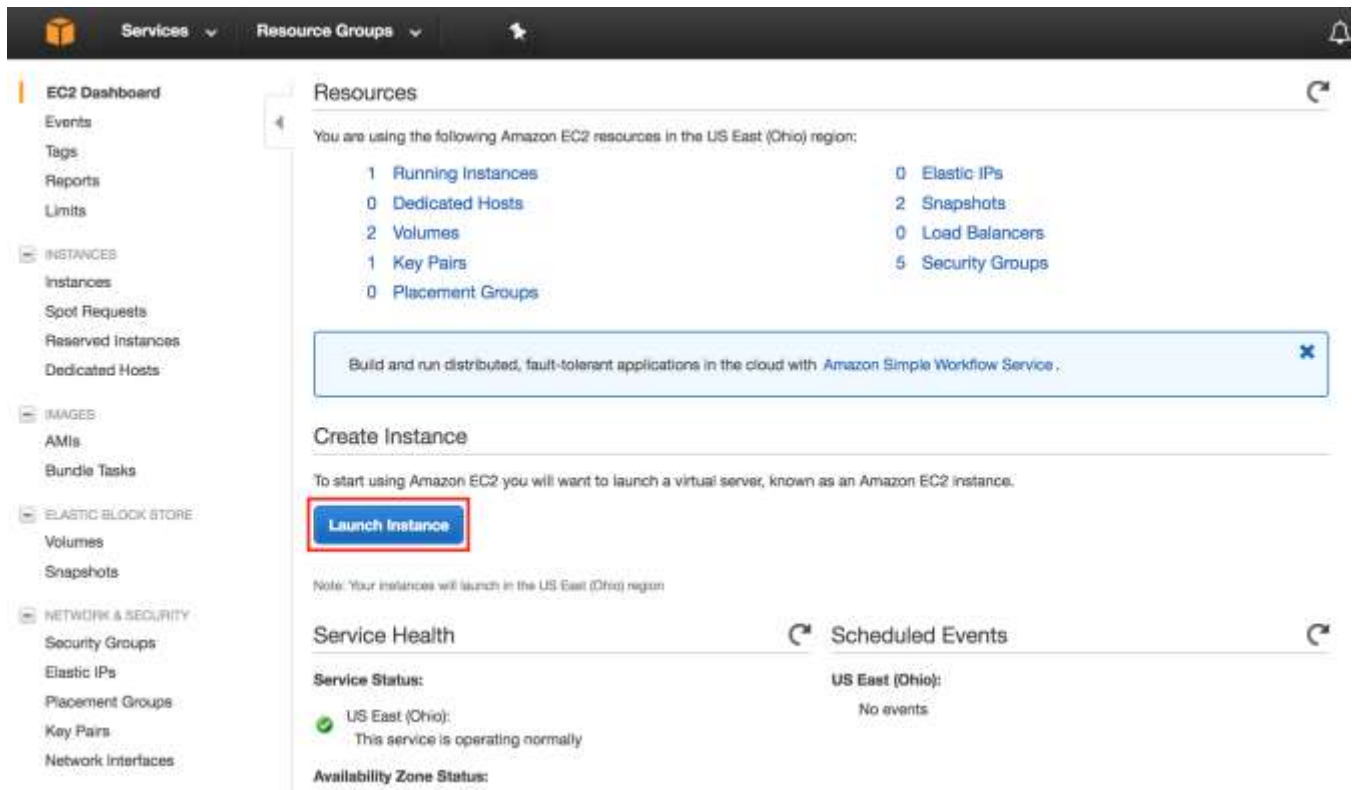
Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. Amazon EC2's simple web service interface allows you to obtain and configure capacity with minimal friction. Amazon EC2 reduces the time required to obtain and boot new server instances to 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.

This lab will walk you through launching, configuring, and customizing an EC2 web server using the AWS Management Console.

Launch a Web Server Instance

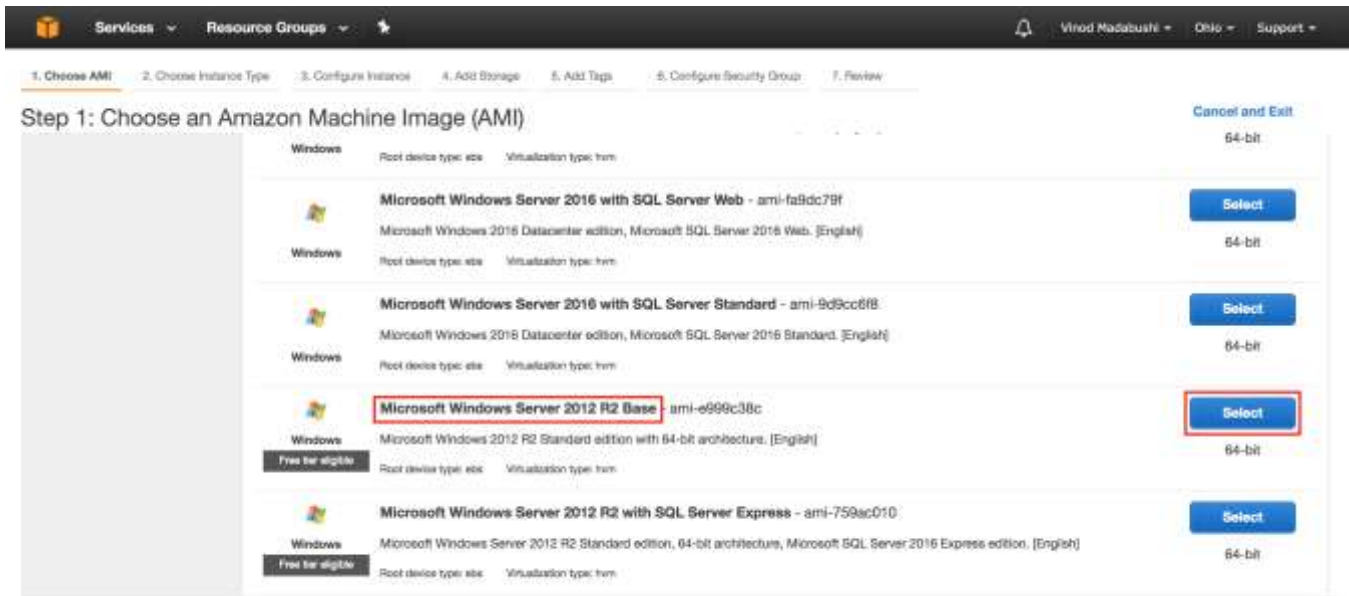
In this example we will launch a Windows Server 2012 R2 instance with the IIS web server installed upon boot.

1. Sign into the AWS Management Console and open the Amazon EC2 console at <https://console.aws.amazon.com/ec2>.
2. Click on **Launch Instance**

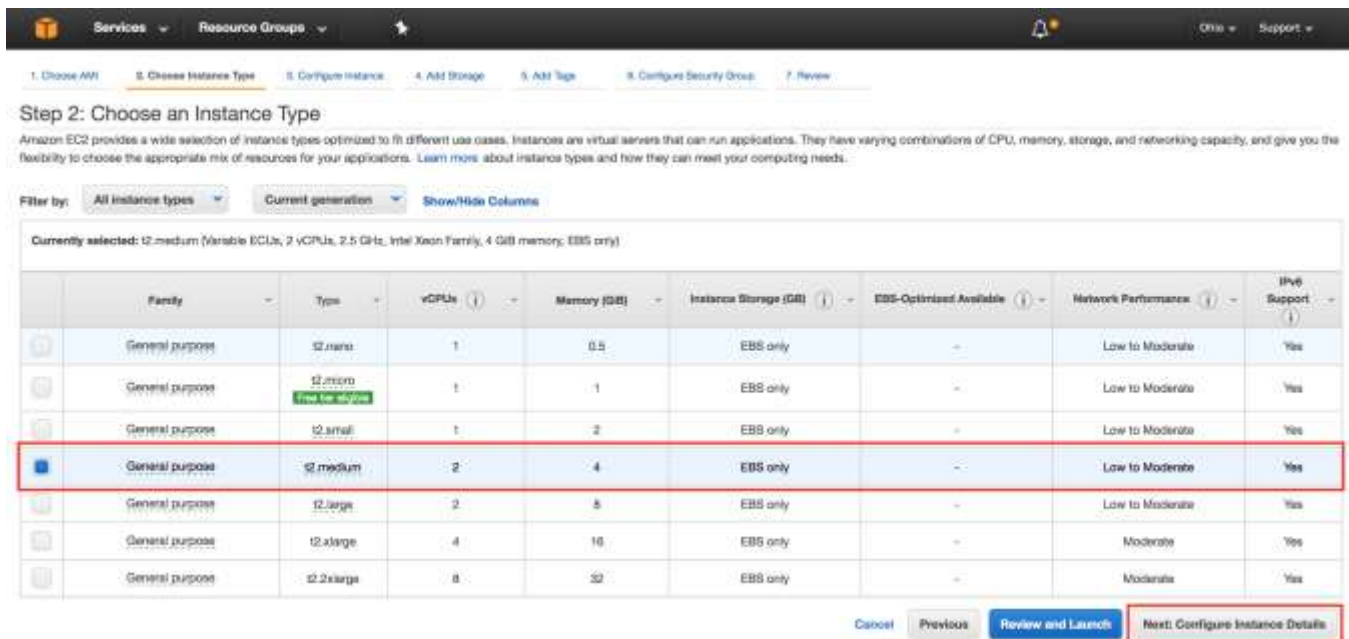


3. Scroll down and click **Select** on the Windows Server 2012 R2 Base AMI.

Getting Started with Windows Server on Amazon EC2



4. In the **Choose Instance Type** tab, select the **t2.medium** instance size and click **Next: Configure Instance Details**



5. On the **Configure Instance Details** page, keep all the predefined settings as they are. Expand the **Advanced Details** section, copy/paste the following script into the User Data field.

Immersion Day

Getting Started with Windows Server on Amazon EC2

```
<powershell>
Import-Module ServerManager;
Install-WindowsFeature Web-Server -IncludeManagementTools -IncludeAllSubFeature
remove-item -recurse c:\inetpub\wwwroot\*
(New-Object System.Net.WebClient).DownloadFile("https://immersionday-labs.s3.amazonaws.com/ec2-
windows.zip", "c:\inetpub\wwwroot\ec2-windows.zip")

$shell = new-object -com shell.application
$zip = $shell.Namespace("c:\inetpub\wwwroot\ec2-windows.zip")
foreach($item in $zip.items())
{
$shell.Namespace("c:\inetpub\wwwroot\").copyhere($item)
}
</powershell>
```

You can also reference it from,

<https://immersionday-labs.s3.amazonaws.com/ec2-windows-lab-userdata.txt> copy/paste the script into the User Data field (this PowerShell script will install/start IIS and deploy a simple web page) and click **Next: Add Storage**:

Step 3: Configure Instance Details

Shutdown behavior: ☐ Stop

Enable termination protection: ☐ Protect against accidental termination

Monitoring: ☐ Enable CloudWatch detailed monitoring
Additional charges apply

Tenancy: ☐ Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy

Elastic Graphics: ☐ Add Graphics Acceleration
Additional charges apply

T2/T3 Unlimited: ☐ Enable
Additional charges may apply

Advanced Details

User data: ☐ As text ☐ As file ☐ Input is already base64 encoded

```
<powershell>
Import-Module ServerManager;
Install-WindowsFeature Web-Server -IncludeManagementTools -IncludeAllSubFeature
remove-item -recurse c:\inetpub\wwwroot\*
(New-Object System.Net.WebClient).DownloadFile("https://immersionday-labs.s3.amazonaws.com/ec2-
windows.zip", "c:\inetpub\wwwroot\ec2-windows.zip")

$shell = new-object -com shell.application
$zip = $shell.Namespace("c:\inetpub\wwwroot\ec2-windows.zip")
foreach($item in $zip.items())
{
$shell.Namespace("c:\inetpub\wwwroot\").copyhere($item)
}
</powershell>
```

Buttons: Cancel Previous Review and Launch **Next: Add Storage**

For further information on User Data please refer to the documentation at -

<http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2-instance-metadata.html>.

On the **Step 4: Add Storage** screen, Click **Next: Add Tags** to accept the default Storage Device Configuration and move to the Step 5: Add Tags screen.

Next, choose a “friendly name” for your instance. This name, more correctly known as a tag, will appear in the console once the instance launches. It makes it easy to keep track of running machines in a complex environment. Name yours according to this format: “[Your Name] Web Server”.

Getting Started with Windows Server on Amazon EC2

Then click **Next: Configure Security Group**.

Step 5: Add Tags
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)
Name	John Doe Web Server

[Add another tag](#) (Up to 50 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

For further information on Tags please refer to the documentation at - http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html.

- You will be prompted to create a new security group, which will be your firewall rules. On the assumption that we are building out a Web server, name this security group according to this format “[Your Name] Web Server”, and open ports 3389 and 80. Click the **Review and Launch** button after configuring the security group.

Step 6: Configure Security Group
A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group ☐ Select an existing security group

Security group name: John Doe Web Server

Description: This rule allows RDP & HTTP access to John Doe Web Server

Type	Protocol	Port Range	Source
RDP	TCP	3389	Custom 0.0.0.0/0
HTTP	TCP	80	Custom 0.0.0.0/0

[Add Rule](#)

Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

[Cancel](#) [Previous](#) [Review and Launch](#)

- Review your choices, and then click **Launch**. *Note the two warning boxes at the top of the page, these are to warn you about possible configuration issues. In this lab we are creating a Windows server that has RDP access that is “open to the world” this is something that you wouldn’t normally do.*

Getting Started with Windows Server on Amazon EC2

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.

Warning: Improve your instances' security. Your security group, John Doe Web Server, 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](#)

Warning: Your instance configuration is not eligible for the free usage tier. To launch an instance that's eligible for the free usage tier, check your AMI selection, instance type, configuration options, or storage devices. Learn more about [free usage tier](#) eligibility and usage restrictions. [Learn more about the usage tier](#)

AMI Details [Edit AMI](#)

Microsoft Windows Server 2016 Base - ami-b291cbd7
 Microsoft Windows 2016 Datacenter edition, (English)
 Root Device Type: ebs Whataboution type here
 If you plan to use this AMI for an application that benefits from Microsoft License Mobility, fill out the License Mobility Form. Don't show me this again

Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance

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

8. Now you need to create a public/private keypair. When this instance launches, you will connect to it via Remote Desktop using the credentials for “administrator”. For Windows instances, EC2 automatically generates a password and encrypts with your public key. To decrypt the encrypted password, you will use your private key. Let's create a new public/private keypair.

Select an existing key pair or create a new key pair [X](#)

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair [↕](#)

Select a key pair [↕](#)

No key pairs found

No key pairs found
 You don't have any key pairs. Please create a new key pair by selecting the [Create a new key pair](#) option above to continue.

[Cancel](#) [Launch Instances](#)

9. Enter a name for the key pair using the following format: [YourName]-KeyPair and click

Download Key Pair.

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair

Key pair name

JohnDoe-keyPair




Download Key Pair

You have to download the private key file (*.pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created.


Cancel Launch Instances

10. Your browser will download the private portion of the key pair to your PC. It will have a name like *JohnDoe-KeyPair.pem*. Note the location of this file because you will need it later to decrypt the administrator password.
11. Now click the **Launch Instances** button to launch your Windows web server.
12. The next screen will confirm that your instance is now launching. Click the **View Instances** button. Once your instance has launched, you will see the “[Your Name] Web Server” instance as well as the Availability Zone the instance is in and its publicly routable DNS name.

Getting Started with Windows Server on Amazon EC2


[Services](#)
[Resource Groups](#)


Ohio
[Support](#)

Launch Status


Get notified of estimated charges
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can connect to them from the instances screen. [Find out how to connect to your instances.](#)

▼ Here are some helpful resources to get you started

- [Amazon EC2: User Guide](#)
- [How to connect to your Windows instance](#)
- [Amazon EC2: Microsoft Windows Guide](#)
- [Learn about AWS Free Usage Tier](#)
- [Amazon EC2: Discussion Forum](#)

While your instances are launching you can also

- [Create status check alarms to be notified when these instances fail status checks.](#) (Additional charges may apply)
- [Create and attach additional EBS volumes.](#) (Additional charges may apply)
- [Manage security groups](#)

View Instances

Browse the Web Server

Now you will browse to the Web Server site that was installed on the Instance using the PowerShell script defined in the **User Data** section during creation of the instance.

1. Wait for the instance to pass the Status Checks. For Windows instances, this could take up to 20 minutes.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
John Doe Web Server	i-062ef25652624ef41	t2.medium	us-east-2c	pending	Initializing	None

When complete, you will see the Status Checks have passed.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status
John Doe Web Server	i-062ef25652624ef41	t2.medium	us-east-2c	running	2/2 checks passed	None

2. Open a new browser tab and browse the Web Server by entering the EC2 instance's Public DNS name into the browser. The EC2 instance's Public DNS name can be found in the console by reviewing the "Public DNS" column. You should see a page that looks similar to this:

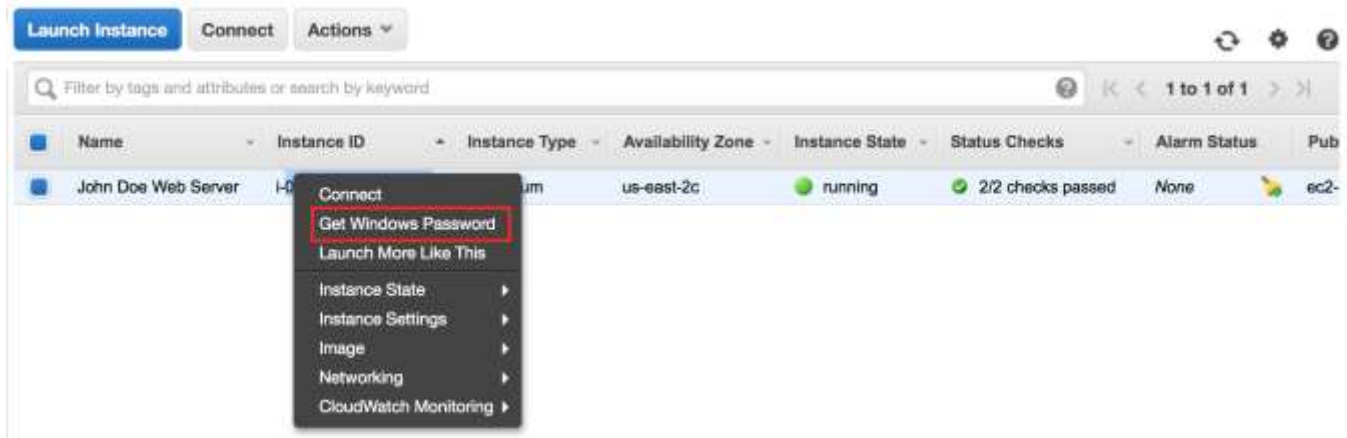


Great Job: You have built your first web server!

Connecting To Your Windows Instance

To connect to the Windows desktop, we will use a RDP client. If you're using a Windows PC, use the bundled Remote Desktop application. For Mac users, if you don't have a RDP client already installed, download [Microsoft Remote Desktop](#).

1. Retrieve the automatically generated, encrypted Windows password by right clicking your instance and selecting **Get Windows Password**.



2. On the next screen, click the Choose File button and select the private key file that was automatically downloaded earlier when you launched the instance. Then click **Decrypt Password** to obtain the Administrator password.



3. The decrypted Administrator password should look something like this:



Note that since only you have the private key, it's important to understand the automatically generated password can only be decrypted by you. So it's important to keep this key secure. Generally, the automatically generated password is changed by the customer after first login. If the automatically generated password is not changed and the private key is lost, there's no way to recover the password.

4. Start your RDP application and connect to the hostname of your instance. The hostname can be found in a couple of different places. For example, in the web console, you'll see hostname listed as the **Public DNS** of the instance.



5. In your RDP application, use **Administrator** as the username along with the decrypted password. Once connected, you will have access to the Windows desktop. At this point, feel free to explore Windows. You should change the Administrator password to something friendlier or easy to remember (but still secure of course).

Appendix – Additional EC2 Concepts

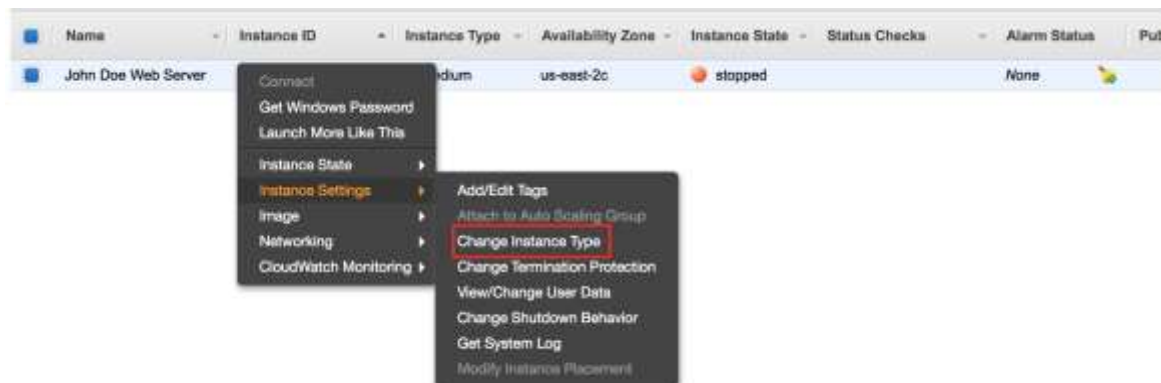
Change the Instance Type

Did you know that you can change the instance type that an AMI is running on? This is very useful when you need a larger (or smaller) or perhaps different type of instance to run a workload. This only works with EBS-backed instances (what we're running here). There is no particular reason to change the instance type in this lab, but the following steps outline how easy it is to do in AWS.

1. In the AWS Console, select your lab instance, then right-click on it and hover over **Instance State** and select **Stop** (NOT Terminate). Then select **Yes, Stop** to confirm.



2. After it has stopped, right-click on it again, hover over **Instance Settings** and select **Change Instance Type**.



3. After going through the options and selecting your new instance type, right-click your lab instance and select **Start**.

Elastic IPs

How do you set up practical DNS names for your web server? Using an address such as `http://ec2-75-101-197-112.compute-1.amazonaws.com/` is cumbersome. Setting up a DNS record that points to `http://www.yourdomain.com` is easy enough – until you reboot the server and the underlying DNS name and IP address both change.

AWS offers Elastic IP (EIP) Addresses, which are actually NAT addresses that operate at a regional level. That is, an Elastic IP Address works across Availability Zones, within a single region.

Assign an EIP to your Web Server as follows:

1. Sign into the AWS Management Console and open the Amazon EC2 console at <https://console.aws.amazon.com/ec2>.
2. Click on the **Elastic IPs** link in the left hand panel of the AWS EC2 Console.
3. Click **Allocate New Address**, then click **Yes, Allocate** at the prompt, then click **Close**. We will now associate the address with your Web Server instance. If you change instances, it's as simple as allocating the address to the new instance.
4. Select the EIP in the console and then click **Actions | Associate Address**.
5. In the instance field select the Web Server instance you previously created, then click **Associate**.

You can now create a DNS “A” record in your own DNS server that points `www.yourdomain.com` to the EIP IP Address you created.

Two Important Notes:



1. As long as an Elastic IP address is associated with a running instance, there is no charge for it. However, an address that is not associated with a running instance costs \$0.01/hour. This prevents address hoarding; however, it also means that you need to delete any addresses you create, or you will incur an ongoing charge.
2. Load balancing requires CNAME records instead of “A” records. So Elastic IP is not required for load-balanced applications.

Black Belt Booting

There are a number of advanced techniques that offer additional power and flexibility when booting instances. For example, some organizations maintain a series of generic instances, and customize the images upon launch.

Common techniques include:

- Automatically check for updates upon each boot.
- Looking in a well-known location, such as in a S3 bucket, for data or a script to tell the instance which packages to load.
- Pass **User Data** to the instance to accomplish each of the above, or possibly instead of the other approaches.

For more details on User Data please refer to -

<http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2-instance-metadata.html>.