**How To Guides for AWS (Amazon Web Services)**

**Why are we using the cloud in w205?**

One of the major feedbacks we have received from industry is that MIDS graduates need to know at least the basics of the cloud. Most data science work is done in the cloud. We don't want someone to graduate from MIDS without knowing the basics of the cloud.

**Why are we using AWS in w205?**

There is actually a master plan where different courses will use different cloud vendors. This will give students exposure to different cloud vendors.

AWS is used by capstone, so since w205 is a required course, this will ensure that students go into capstone ready to use AWS. Capstone will assume knowledge of AWS and not have time to cover it.

AWS has AMIs (Amazon Machine Images) which allow the instructor to do 20 to 30 hours of setup work on Linux and create an AMI. Students can create a virual machine (VM) from the AMI saving 20 to 30 hours of setup time. The other cloud vendors don't have an image system that is even close to the functionality of AMIs. Since this is most student's first exposure to any cloud, we are trying to make the initial exposure as easy as possible.

* You will first need to create an AWS account at the link below:
  + [https://aws.amazon.com/Links to an external site.](https://aws.amazon.com/)

**We have a FAQ with the frequently asked questions about AWS that we get. If you have questions about AWS, please have a quick read through the FAQ:**

Amazon Web Services (AWS) - FAQ - Frequently Asked Questions

Why are we using the cloud in w205?

One of the major feedbacks we have received from industry is that MIDS graduates need to know at least the basics of the cloud. Most data science work is done in the cloud. We don't want someone to graduate from MIDS without knowing the basics of the cloud.

Why are we using AWS in w205?

There is actually a master plan where different courses will use different cloud vendors. This will give students exposure to different cloud vendors.

AWS is used by capstone, so since w205 is a required course, this will ensure that students go into capstone ready to use AWS. Capstone will assume knowledge of AWS and not have time to cover it.

AWS has AMIs (Amazon Machine Images) which allow the instructor to do 20 to 30 hours of setup work on Linux and create an AMI. Students can create a virual machine (VM) from the AMI saving 20 to 30 hours of setup time. The other cloud vendors don't have an image system that is even close to the functionality of AMIs. Since this is most student's first exposure to any cloud, we are trying to make the initial exposure as easy as possible.

Can't I just use my desktop for w205 and skip using AWS?

No.

AWS is a required element for w205.

Can I use another cloud vendor in place of AWS?

You must complete all labs and projects using AWS. If you want to gain experience using another cloud vendor, you are welcome to try porting your labs and projects over and running them there. However, instructors and TAs won't be able to use class time or office hours time supporting this. You would need to do it on your own.

Does AWS cost money?

Yes.

Amazon is a for-profit business that charges money for AWS to make profits for their shareholders.

Do students have to pay for AWS?

Yes.

Students are responsible for paying for their AWS usage.

Will 2U pay for AWS?

No.

Previously 2U had an arrangement to give students AWS credits through one of their partners, but that arrangement expired in Summer 2020. The 2U representative for UC Berkeley has told us that 2U has no plans to offer students AWS credits in the future.

Will UC Berkeley and/or iSchool pay for AWS?

No.

Under federal and state regulations, lab fees, which include computer lab fees, must be separate from tuition. AWS would fall in the category of computer lab fees.

Will AWS give us student credits?

Instructors will request credits. There is no guarantee that they will be granted. So, students should be prepared to pay their AWS fees without credits. Credits have typically run around $50 to $200 per student.

Will instructors let us know as soon as credits come in? Do I need to keep asking every day or two just in case?

Yes.

Instructors will let students know as soon as they come in and the last day to add has passed.

No.

There is no need to keep asking instructors if they have come in yet.

Do you know exactly how much w205 AWS usage will cost?

No.

AWS is billed by usage. Some students spend much less time than others and have much lower bills. Others spend much more time than others and have much higher bills.

Do you have an estimate of how much w205 AWS uage will cost?

Based on January 2020 pricing, which is subject to change without notice:

* The VM's EBS storage is 100 GiB. EBS is 8 cents per GiB per month. So, $8 a month.
* When the VM is running (assuming 2 CPUs and 8 GiB RAM) it is 9 cents per hour. If you run your VM 10 hours a week it would be less than $1 a week.
* Snapshots are stored in S3. Most snapshots will be a few GiB. S3 is billed at 2 cents per GiB. We recommend that you take a snapshot once a week and keep the last 3. Most students will want to keep more. It's a small price to pay for the safety of a backup so you don't lose your work.

**Can I use a smaller VM size to save money?**

No.

We have tested the VM with different sizes. The recommended size is the minimum size. If you try a smaller size, some processes will run out of memory and risk corruption of your VM. If your VM corrupts, you will lose everything and have to restore from the last snaphot.

**Can I use a larger size VM?**

Yes.

The recommended size is the absolute minimum. You can always safely run a larger size.

**Can I use spot instances to save money?**

No.

Spot instances are cheaper, but can be terminated at any time. If they are terminated, you will lose your VM and have to create a new one from the last snapshot.

Spot instances are suitable for people running processes that are frequently saving state to a location external to the VM.

What is the free tier? How much will it cover of what we will need for w205?

In terms of EBS and S3 allowances, it's worth less than $1 a month.

In terms of VM's, you can use a 1 CPU, 1 GiB VM for free.

The w205 VM will use all of the EBS allowance. After 1 or 2 snapshots, you will have used your S3 allowance. The w205 VM won't run in the free VM allowance.

What is the free 1 CPU, 1 GiB VM good for?

* Learning Linux command line, admin, etc.:
  + Small VMs will work for this. You could create a VM and learn without worrying about messing up. If you mess up, just throw away the VM and get a new one.
  + Practice Troubleshooting Linux: Curriculums can have AMIs with issues. The students would create a VM from the AMI, and then find and fix the problem. Great way to learn to how fix real linux problems.
* Cryptography experiments: They don't need a lot of cpu or memory to run and you want to run trillions of cases and add the results to summary tables. If you have some experiments that don't need a lot of memory nor cpu that you want to run for a long time, it's great.
* QC (quantum computing) experiments - QML (quantum machine learning experiments) - similar to cyptography experiments. We may want to run trillions of trials.

I received a message from AWS that I was over the free tier limit. What does this mean? Should I be worried?

Once you go over a free tier limit, AWS notifies you. The notifications are sent out once a day or so, so it may take a while before you are notified.

When you create the w205 VM, you will go over the EBS limit and be notified. When you create the first or second snapshot, you will be over the S3 limit and be notified. Since notifications go out once a day or so, you may get both in the same notification.

You do not need to be worried about these messages. They are normal.

**Create a security group and set firewall rules for our virtual router for our virtual private cloud in Amazon Web Services**

How to Guide: AWS - Creating a Security Group and Adding Firewall Rules to the Security Group

Video: [https://kevincrook.com/ucb/mids/w205/how\_to\_guides/aws/01\_aws\_security\_firewall\_rules.mp4Links to an external site.](https://kevincrook.com/ucb/mids/w205/how_to_guides/aws/01_aws_security_firewall_rules.mp4)

Every Virtual Machine (VM) in Amazon Web Services (AWS) is required to have a security group. AWS has a default security group. When you create (launch) a new VM, you can use the default security group, have it create a new security group, or use an existing security group.

It's best to first create a security group and add the firewall rules to the security group before we create our first VM. All the VM's we create for w205 can use the same security group. The instructions below will use the name **UCB\_MIDS\_w205\_Security**. You can use any name you want, however, if you use this name, all of our instructions will work as is.

**Create Security Group including Firewall Rules**

**Note: Since this video was filmed, AWS has made a change for first time users.  It appears that you now need to move to EC2 first, then change the region to N. Virginia.  After your first time using EC2, it will default to N. Virginia, and you won't have to worry about it again.**

**AWS => N. Virginia => Services => Compute => EC2 => Network & Security => Security Groups => Create New Security Group**

**Security Group Name:** UCB\_MIDS\_w205\_Security

**Description:** UCB\_MIDS\_w205\_Security

**Inbound Rules:**

For all rules, we need to give a source IP address or address range or wildcards. Here are a couple of common wildcards:

* 0.0.0.0/0 = wildcard for all IP addresses and subnets for IPv4 (IP version 4, the classic IP addresses)
* ::/0 = wildcard for all IP address and subnets for IPv6 (IP version 6, the new IP address scheme)

Here are the inbound rules we will need for the course. For now, we will stick with IPv4. (If you want to run IPv6, you will need to add the same rules for IPv6):

| **IP Version** | **Type** | **Protocol** | **Port range** | **Source** | **Description** |
| --- | --- | --- | --- | --- | --- |
| IPv4 | SSH | TCP | 22 | 0.0.0.0/0 | SSH |
| IPv4 | HTTPS | TCP | 443 | 0.0.0.0/0 | HTTPS |
| IPv4 | Custom TCP | TCP | 7473 | 0.0.0.0/0 | Neo4j web interface using HTTPS |
| IPv4 | Custom TCP | TCP | 7687 | 0.0.0.0/0 | Neo4j back end interface using Bolt |
| IPv4 | HTTP | TCP | 80 | 0.0.0.0/0 | HTTP |
| IPv4 | Custom TCP | TCP | 8888 | 0.0.0.0/0 | Jupyter Notebook server |

**Outbound Rules:**

AWS should create a default outbound rule that allows all outbound traffic.

Please double check that this is the case.

Occasionally, students report that the default outbound rule is missing.

ONLY IF it is missing, add an outbound rule: IP Version: IPv4, Type: All Traffic, Protocol: All (greyed), Port Range: All (greyed), Destination: 0.0.0.0/0

**Tags:** Key is Name, Value is UCB\_MIDS\_w205\_Security

**Click Create security group in lower right.**

**AWS-Create (Launch) a Virtual Machine (VM) from the w205 Amazon Machine Image (AMI)**

* An AMI is an image that VMs can be created from.
* An AMI has been created based on Amazon Linux with packages installed, configured, users created, groups created, directories created, ssh keys setup, etc. AMIs save you the effort of starting with base Amazon Linux and going through many pages and hours to get it configured for w205.
* Amazon Linux is derived from CentOS which is the open source version of Red Hat Linux. So, essentially we are using Red Hat Linux, which for professional server room use, is the dominant distribution.
* Generally, you only need to create a VM once. Once it is created, unless it get corrupted or damaged, you should not need to create another one. You will keep using the same VM, but start and stop it on an as needed basis (covered in another how to guide). Whenever the VM is running, you are charged by the minute.

**Create (launch) a new VM from the AMI**

**Current AMI: Spring 2024:  UCB\_MIDS\_w205\_AMI\_VERSION\_007     ami-0096f6b5a59dff70d**

* The AMI will change to keep the software current and to install new security certificates that expire once a year.
* Always go by the current AMI in this document, don't use an old one.
* Always verify the ami number. Anyone can create an AMI with the same name as mine. The only way to verify is if the ami number matches.
* AMIs are local to a region, so make sure you are in N.Virginia or you won't find it.

**AWS => N. Virginia => Services => Compute => EC2 => Instances => Instances => Launch Instances => Launch Instances**

* **Name and tags:**
  + UCB\_MIDS\_w205\_01
    - (change the 01 to 02, 03, 04, etc. if you already have w205 VMs)
  + Click "Add additional tags" to the right
  + Click "Resource types" dropdown
    - "Instances" should be checked already
    - Check "Volumes"
    - Check "Networks"
* **Application and OS Images (Amazon Machine Image):**
  + Enter the AMI Name from the previous section (changes each semester) and hit enter to search
  + Click the "Community AMIs" tab
  + Verify the ami-xxxx number matches exactly
    - For security reasons - anyone can create an AMI with the same name as the w205 one
  + Click the orange "Select" button
* **Instance Type:**
  + In the dropdown box, select "t2.large, 2vCPUs, 8 GiB memory"
* **Key Pair:**
  + Select "Create new key pair"
    - Unless you are a seasoned AWS user with an existing key pair you want to use
  + For "Key pair name" most students use something like UCB so they can use it for all of their UCB work
  + For "Key pair type" use "RSA"
  + For "Private key file format"
    - Mac - choose ".pem"
    - Windows
      * It's usually best to choose ".pem" and then convert it to PuTTY key format (later video) - allows you to have both formats
      * If you are sure you will never need the pem format, choose ".ppk" format
  + Click the orange "Create key pair"  button
  + It will download the private key to your browsers download location
    - Typically the "download" directory unless you have defaulted it to something else
    - Keep you private key private - if someone gets a hold of it, they can get into your VM
    - If you lose your private key, you will not be able to login to your VM
* **Network settings:**
  + Firewall (security groups)
    - Click "Select existing security group"
    - In the "Security groups" dropdown, choose the security group we created called "UCB\_MIDS\_w205\_Security"
* **Configure storage**
  + No changes needed, as storage information has already been configured in the AMI
* **Advanced details**
  + In the "Termination protection" dropdown, choose "Enable"
* **Summary (panel to the right)**
  + Click the orange "Launch instance" button

**Verify the VM is Running**

**AWS => N. Virginia => Services => Compute => EC2 => Instances => Instances**

You should see your instance in the running state.

Always let a new VM run for at least 15 minutes (or longer) before stopping it - it has a lot of setup that runs when it is booted the first time

Stop the VM

When you create a new VM, it is running.

Whenever the VM is running you are charged by the minute. If you are not going to use it until the next day or later, you may want to stop it to save billing.

There is a separate how to guide on starting and stopping the VM.

**How to start and stop our VM. We are charged per minute while our VM is running:**

**Starting the VM**

**AWS => N. Virginia => Services => Compute => EC2 => Instances => Instances => select instance => Instance State => Start Instance**

**Verify the VM is Running**

**AWS => N. Virginia => Services => Compute => EC2 => Instances => Instances**

You should see your instance in the running state.

**Stopping the VM**

First, make sure you have no Docker containers or clusters running. If you stop the VM while a Docker container or cluster is running you might corrupt the mounted volumes. For example, if the VM is stopped while Postgress is running, the Postgress mounted volume may corrupt and your database may be corrupted and unusable, and you will have to create a new database from scratch.

**AWS => N. Virginia => Services => Compute => EC2 => Instances => Instances => select instance => Instance State => Stop Instance**

**Suggestion:** since you have just stopped your VM, it's a great time to create a snapshot for a storage layer backup of your VM!

**How to take a VM level backup called a snapshot:**

A snapshot is a storage layer backup of your VM.

**Make absolutely sure your VM is stopped!**

Before you create a snapshot, you need to make sure your VM has been stopped. Linux uses buffered I/O which uses memory to cache parts of the file system, which makes it run much faster. However, the trade off is that since part of the file system is in memory, the VM will need to be stopped so the cache is written to the storage layer before the snapshot is taken.

**AWS => N. Virginia => Services => Compute => EC2 => Instances => Instances**

Make sure the Instance State says Stopped. If it is in progress, you will need to wait. You may need to refresh the web page to get it to update the Instance State.

If it's running, please see the How to Guide: AWS - Starting and Stopping a VM

**Create a Snapshot of a VM**

**AWS => N. Virginia => Services => Compute => EC2 => Elastic Block Store => Volumes => select volume => Actions => Create Snapshot**

Description: call it anything you like. I like to put part of the instance name and the date so it's easy to find, such as w205\_01\_2021\_12\_20

Tags: Key: Name, Value: same name as above

**Wait until the snapshot is finished before starting the VM again**

Wait until the snapshot is finished before starting the VM again, otherwise your snapshot will be no good! You may need to refresh to see the updates.

**Optional: How to create your own VM from a snapshot (you may want to wait until later this semester and come back and do this one):**

How to Guide: AWS - Creating an AMI from a Snapshot of a VM, then creating a new VM from the AMI

Video: [https://kevincrook.com/ucb/mids/w205/how\_to\_guides/aws/05\_aws\_ami\_from\_snapshot.mp4Links to an external site.](https://kevincrook.com/ucb/mids/w205/how_to_guides/aws/05_aws_ami_from_snapshot.mp4)

Hopefully this won't happen to you, but in case it does:

Let's say your VM won't boot. Somehow either you accidentally damaged it, or it somehow became corrupted. It's rare, but not impossible. Out of several hundred students per semester, a few will have this happen to them. Hopefully you will have taken our advice and taken frequent snapshots, so you have a snapshot to restore from.

Essentially, the procedures below allow you to create a new VM from the most recent snapshot if your current VM is damaged or corrupted.

**Create an AMI from the snapshot**

**AWS => N. Virginia => Services => Compute => EC2 => Elastic Block Store => Snapshots => select snapshot => Actions => Create image from snapshot**

Wait until the creation of the AMI is completed! You may need to refresh to see the updates.

**Create (launch) a new VM from the AMI you just created**

**AWS => N. Virginia => Services => Compute => EC2 => Images => AMIs => select AMI => Actions => Launch**

* **Step 1: Choose AMI** - Select the AMI you just created
* **Step 2: Choose an Instance Type** - t2.large, 2 vCPUs, 8 GiB memory
* **Step 3: Configure Instance Details** - Check "Protect against accidental termination"
* **Step 4: Add Storage**
* **Step 5: Add Tags** - Add: Key: Name Value: UCB\_MIDS\_w205\_01 (change the 01 to 02, 03, 04, etc. if you already have w205 VMs)
* **Step 6: Configure Security Group** - Select the existing security group that we previously created: UCB\_MIDS\_w205\_Security. It can be shared by all instances.
* **Step 7: Review Instance Launch** - Launch

**SSH Key Pairs**

If you have an existing key pair that you want to use, you can certainly use it. If you don't, you might want to create one called ucb or mids or w205. You will want to save the private key to a place on your laptop where you will remember where it's at. You will need it to login to your VM. If you loose it, you will loose access to your VM. You may want to back it up to a external hard drive, Google gdrive, etc. However, keep your private key private! If someone gets access to your private key, they can login to your VMs and install and run malware, launch cyber attacks from your VM, etc.

**Verify the Instance is running**

**AWS => N. Virginia => Services => Compute => EC2 => Instances => Instances**

You should see your instance in the running state.