Amazon Web Services

AWS

AWS Academy
Getting Set Up

- You'll receive an email invite soon
- From instructure.com
- Click on Get Started

AWS Academy
Getting Set Up

- You'll likely have to Create My Account
- Select a Password and Time Zone
- Uncheck the AWS Spam
- Agree to Use Policy
- Register

AWS Academy
Getting Set Up

- https://awsacademy.instructure.com/login/canvas

AWS Academy
Getting Set Up

- Go into Modules

- Select "Launch AWS Academy Learner Lab"

- Note: Safari security policy prevents the Vocareum frame from loading

  - Use Firefox for this

AWS Academy
Getting Set Up

- Skim through the terms of service

- Scroll down and accept

AWS Academy
Getting Set Up

Lab Account Status   **AWS Terminal**   **Start Lab Button**   **Enter Full Screen**

AWS Academy
Getting Set Up

- Click Start Lab Button
- This takes a good 3-5 minutes the very first time to start

---
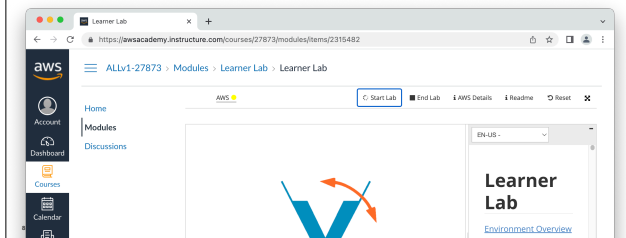
AWS Academy
Getting Set Up

- AWS Account Status Button goes green
- Click the AWS Account Status button to load the AWS Console
- Current Active Lab Session Time Displayed. 4 hours per session
- Total Lab $ Allowance used across all lab sessions. Don't go over this!
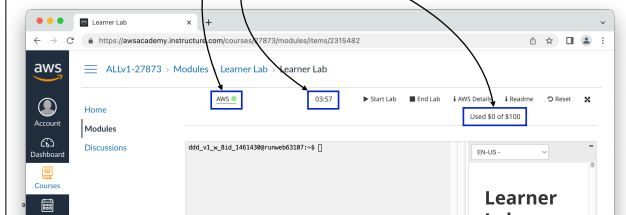
AWS Academy
AWS Console Overview

- AWS Console
- Search for Services
- Pin Favorite Services
- Select Region
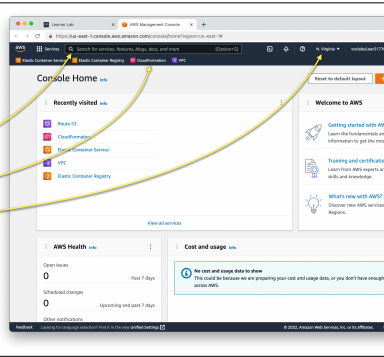
**AWS Academy**
AWS Console Overview

- Can only use regions:
  - N. Virginia (us-east-1)
  - Oregon (us-west-2)
- For simplicity I recommend using N. Virginia (us-east-1)
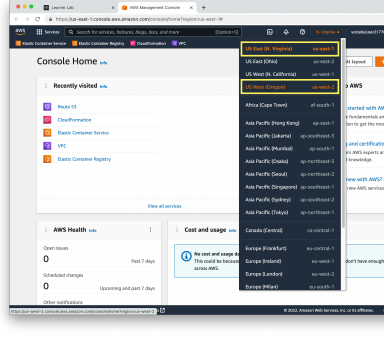
# AWS Credentials

EC2 Security
Download SSH Keys

- Click on AWS Details

- Download the PEM file

  - May need the PPK file if you are using Putty on Windows

- You'll need this for SSH Terminal access and File Transfer

- Save someplace you'll remember!

13
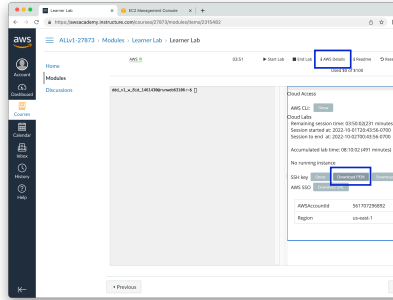
AWS VS Code Extension
Not required, but highly recommended. Simplifies many things

- In VS Code go to the Extensions section of the left mode sidebar

- Search for AWS

- Install the "AWS Toolkit" extension from Amazon Web Services

14
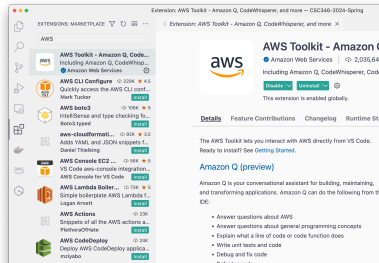
AWS VS Code Extension
Configuration

- Turn off all of AWS "AI" spam

- Click the little Gear next to the Uninstall button

- Choose "Extension Settings"

- Scroll through and uncheck anything "Code Whisper" related.

- Close Settings

15
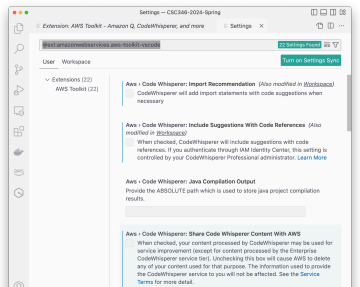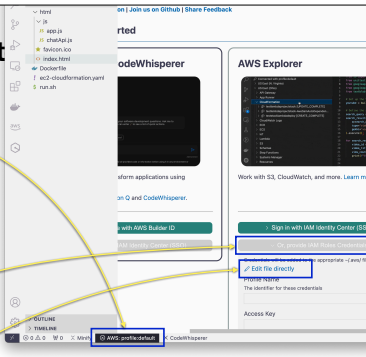
AWS VS Code Extension

Configuration

- Click on the AWS Extension in the left sidebar

- Click on the three "…" menu in the upper pane and uncheck everything except "Explorer"
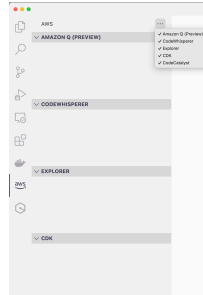
AWS VS Code Ext

Configuration

- At the bottom of the window there should be a section that says "AWS: profile"

  - Restart VS Code if this isn't showing up

- Click on that to bring up a Getting Started document

- Under AWS Explorer click on the "Or provide IAM Roles Credentials"

- Click on "Edit file directly"

AWS VS Code Ext

Configuration

- A new "credentials" document will open.

- We will paste in credentials we get from AWS Academy
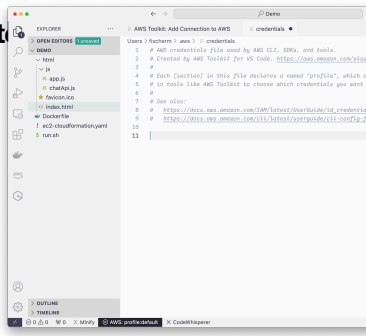
CLI Credentials
Download SSH Keys

- Go back to AWS Academy

- Click on AWS Details

- Click on the "Show" button next to AWS CLI

19
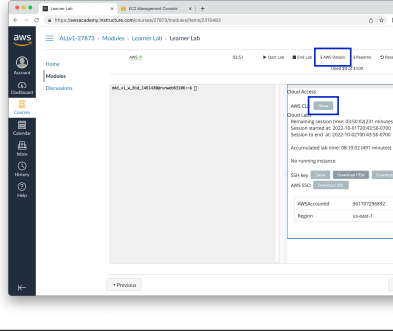
CLI Credentials
Download SSH Keys

- A text box with credential information including the following is displayed:

  - aws_access_key_id

  - aws_secret_access_key

  - aws_session_token

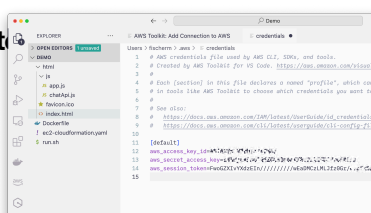- Copy all of the text inside the box, including [default]
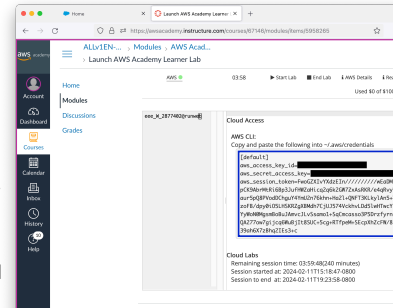
20

AWS VS Code Ext...
Configuration

- A new "credentials" document will open.

- We will paste in credentials we get from AWS Academy

- Save the document

21
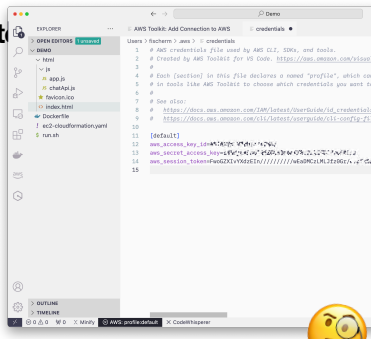
AWS VS Code Extension

Configuration

- A new "credentials" document will open.

- We will paste in credentials we get from AWS Academy

- Save the document

Important!

You will have to get new CLI credentials for each AWS Academy Lab session. Sessions are only valid for 4 hours at a time.

Copy them into this file and replace the old ones each time.

AWS VS Code Extension

Configuration

- Click on the "AWS: profile" in the window footer again to open the profile selection

- You should see your new default profile in the list now

- Click on that line to activate it.
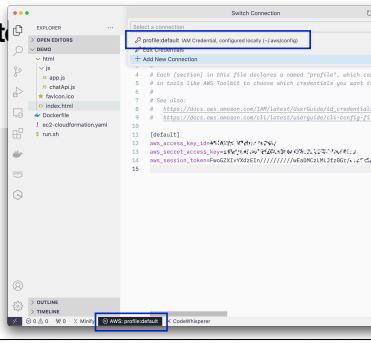
AWS VS Code Extension

Configuration

- Clicking on the AWS Extension in the left sidebar will now bring up the resource browser for the current region (us-east-1)

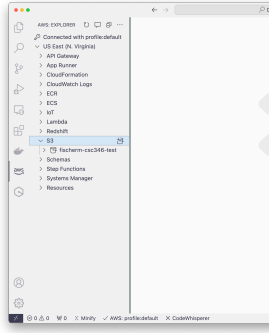- There's probably nothing there yet since this is a new empty account
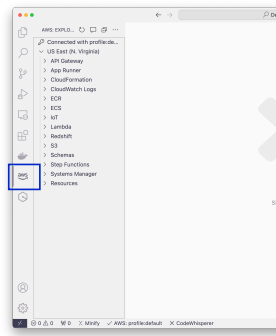
AWS VS Code Extension

Configuration

- Click on the S3 section

- Click on the little +Bucket Icon

- Enter in the name of your bucket

  - Note bucket names must be globally unique among all AWS accounts

- Hit the "Return" key to make it
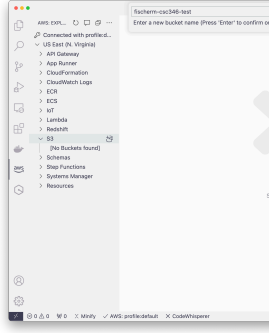
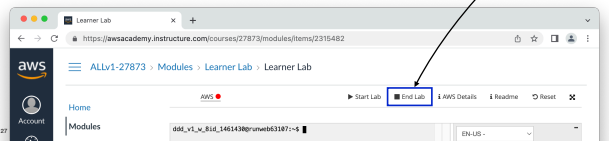## AWS VS Code Extension

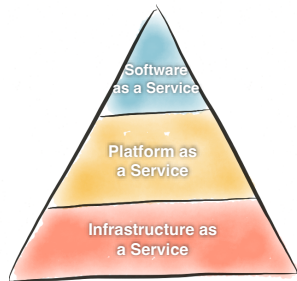**Configuration**

- You made your first cloud resource!

AWS Academy

End Lab Session

- When you're done, make a habit of ending your lab session in AWS Academy.

- If you forget, it will automatically time out after 4 hours, but you're charged for any running resources during that whole time.

End Lab Button

AWS Overview

Software as a Service

Platform as a Service

Infrastructure as a Service

SaaS

PaaS

IaaS

SaaS
PaaS
IaaS

box

AWS RDS

AWS EC2

Less
Maintenance

More $$
Less Time

SaaS

PaaS

IaaS

More
Control

Less $$
More Time

AWS Services
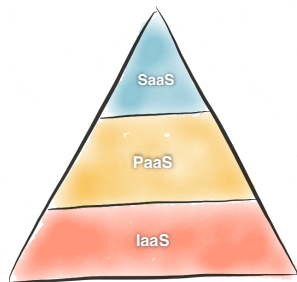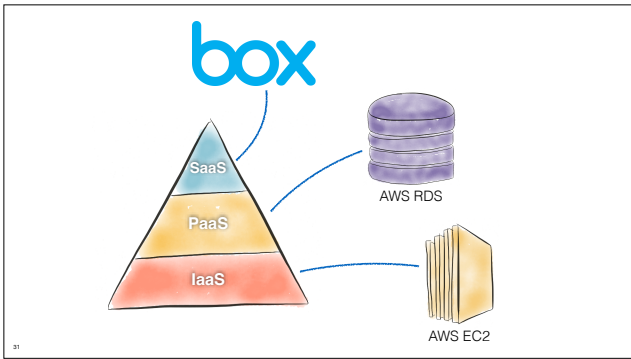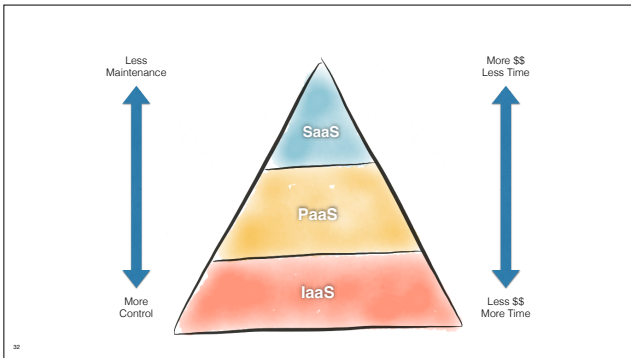
Three Main Categories

Compute	Storage	Network
EC2	S3	S3
RDS	RDS	VPC
Lambda	EBS	VPN

34

Compare On-Prem to Cloud

On-Prem	AWS
VMWare	EC2
Isilon / Synology / NAS	EFS
F5 bigIP	ELB / ALB
Firewalls	Security Groups

35

EC2

- Elastic Cloud Compute
- Virtual Machines (VMs)
- Linux or Windows
- Basic Server Building Block
- Provision, log in, configure as you like

36

EBS

- Elastic Block Storage
- Standard block storage attached to EC2 instances
- Multiple volumes can be attached to an instance
- Snapshots

EFS

- Elastic File System
- Amazon's Managed NFS Service
- Unix-centric shared file system
  - Mount a single file system across many application hosts
  - Store application files that need to be shared

S3

- Simple Storage System
- Basic Object Storage
  - Key/Value Pairs
  - NOT Block Storage! Cannot directly attach to EC2 Instances
- Good for storing lots of data independent of a single server
- Access through APIs and HTTP
- Much cheaper than EBS

RDS

- Relational Database Service
- PaaS for Databases
  - Oracle, MSSQL, MySQL, PostgresSQL, Aurora
  - AWS manages the servers, minor patching
  - Less management on your part, also less configurability

ELB / ALB

- Elastic Load Balancer / Application Load Balancer
- Simpler, dumber versions of an F5
- Accepts incoming traffic on some port, balances to n backend servers
- Usually public-facing, in public subnets
- SSL/TLS Termination

Regions

- Geographic location of AWS data centers
- Oregon, Virginia, London, etc.
- Each Region contains multiple physical data centers, each with independent power and networking
- Resources must be specified in a particular Region
  - We use Oregon (us-west-2) for almost everything

Availability Zone

- Within a region, there are multiple Availability Zones
- Each AZ has separate power and networking
- Designed for physical redundancy
- High Availability is achieved by deploying resources into multiple AZs
- Many services (RDS, ELBs, etc) are Multi-AZ capable

43

VPC

- Virtual Private Cloud
- AWS's Network Construct
- Subnets, Route Table, ACLs, VPNs, etc.
- Almost all compute resources must be assigned to a subnet in a VPC
  - (EC2, RDS, ELBs, EFS, etc)

44

AWS Shared Responsibility Model
https://aws.amazon.com/compliance/shared-responsibility-model/

CUSTOMER RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD			
CUSTOMER DATA			
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT			
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION			
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION	SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)	NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)	

AWS RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD			
SOFTWARE			
COMPUTE	STORAGE	DATABASE	NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE			
REGIONS	AVAILABILITY ZONES	EDGE LOCATIONS	

45

Permissions Model

Can I push this button?

Permissions in 3 parts

Someone   Does something   To something
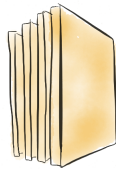
`ec2:RunInstance`

Permissions in 3 parts

Principal   Action   Resource

`ec2:RunInstance`

IAM

- Identity & Access Management
- Controls who can do which actions to what resources

49

IAM User

- A user entity
- Could be configured with web console access (or not)
- Could be configured with API access keys (or not)
- Can have Roles assigned to it, and belong to groups

50

IAM Role

- A collection of 0 or more Policies
- Roles can be attached to users and services

51

IAM Policy

- A set of instructions allowing or denying an action to be performed on some resource
- Policies are assigned to Users or Roles
- JSON Document

52

IAM Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "logs:DescribeLogGroups"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "logs:Describe*",
                "logs:FilterLogEvents",
                "logs:GetLogEvents"
            ],
            "Resource": "arn:aws:logs:*:123412341234:log-group:kf*",
            "Effect": "Allow"
        }
    ]
}
```

This Action

Is allowed on **ALL** resources

These Actions

Are allowed **ONLY** on these resources

53

There Are Lots of Actions

54

Demo