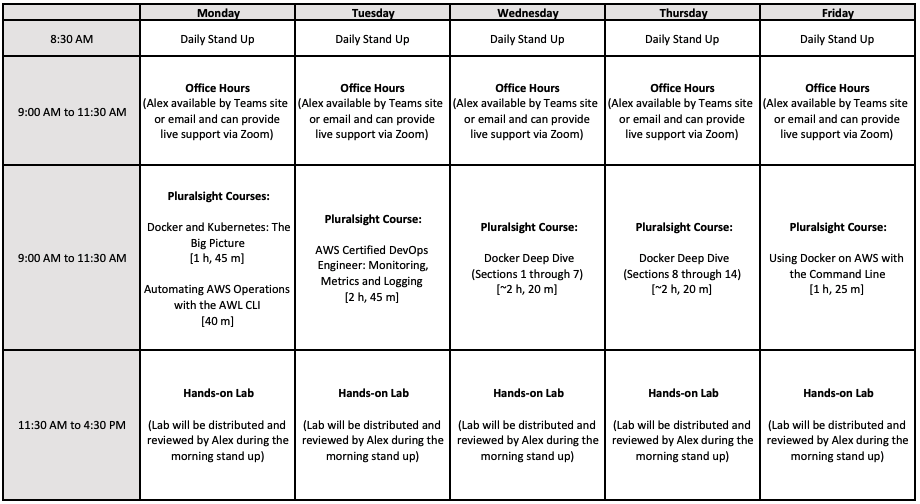
Use the class cheat sheet and materials for reference: <https://bitbucket.org/lmcohort2/materials/src/master/cheatsheet.md>



## S3 Auditing Script

In many organizations (not all :P), security is important. Public s3 buckets can cause all sorts of problems from leaking sensitive information to racking up billing costs. Let's write a tool that will notify us if there is a public bucket or objects in our account. (turns out there WAS when I was putting this together, someone from last cohort also had 1000s of object in their bucket)

Before you start any coding, think about the following.

How can you tell if a bucket is publically accessible or not? What about objects in the bucket? Is there a fool-proof way? We wouldn't want our script to miss something.

Our objective, write a python (or bash if you want to) script that will log all buckets that are public or contain objects that are publically accessible to a file. Our log file should contain information about every bucket and object audited with WARNING level logs for every public bucket.

For logging, I recommend reading. <https://docs.python.org/2/howto/logging.html#logging-basic-tutorial>

You can find all the violations in your log by grepping:

grep "WARNING" audit.log

## Lambda + SNS your audit script

Wouldn't it be nice if we didn't have to check a file to see the results? Much less download a script, configure aws CLI, and acquire permissions to run the script.

Copy your script and make a lambda. This lambda should cause an email to be sent with all of the offending buckets (no duplicates!) in the email body.

Run your lambda with the following

|  |
| --- |
| aws lambda invoke --invocation-type Event --function-name <YOUR LAMBDA) /tmp/lambda-outfile |