Condo Daily Report 8-16-21

Monday

* Arrived this morning, and studied for AWS cloud practitioner
  + Took practice exam
  + Reviewed flash cards
* Checked status of Tableau Server
  + Post update, all functions were normal
* Morning meeting with tech and analysts
  + Discussed tasks over the next several weeks
* Passed Cloud Practitioner Exam
* Began researching Cloudwatch
  + In a virtual environment Applied monitors to CPU usage on EC2 instances, and VPC monitors to check inbound request traffic
* Began researching pushing CloudTrail Logs into an S3 bucket
  + In a virtual environment created an S3 bucket, edited permissions of the bucket to allow cloud trail to write logs into a directory inside the bucket
  + Went to cloudtrail and created a new trail that brings the logs from cloudtrail tracking user activity by seeing their interactions with AWS API’s, and dumps it into the S3 bucket
    - Enabled cloudwatch tracking on this cloudtrail trail to monitor activity
  + Created a table in Athena for the cloudtrail log information
    - This allows easy querying to make it easier to assess users who are potential risks
* Implemented CloudTrail log Dump in Bear Cognition (production environment)
  + Created a bucket named bear-cognition-logs in the us-1-east region
  + Created a trail that brings the logs into the s3 bucket
  + The logs successfully went into the bucket
  + Created a table in Athena for the log info in the bucket
  + The queries work and the table is formatted for AWS standard
* Began researching how to make a stream for cloudwatch logs into the S3 buckets
  + Updated the permissions for the bucket to allow traffic into the S3 bucket
* Created a cloudwatch alarm to notify when portal server is at or above 75% usage
* Research how to monitor network requests using cloudwatch