Condo Daily Report 8-18-21

Wednesday

* Arrived at BC began to review some of the cloudwatch activities I had done the day before
  + The logs were still successfully transferring in the S3 bucket
  + Reviewed a spike in outgoing network traffic
    - Decided that there needed to be network logs
* Continued research on the CloudWatch agent
* Haven’t installed it yet on to the instances
  + Installed it again on the practice instance with success
  + The metrics for the instance were displayed and customizable
* Researched integration of lambda functions and cloud watch
* Was able to write a lambda function that takes the data from an EC2 instance and makes it accessible through a cloud watch event
  + When this event is triggered, a flow goes into the respected log group
* Created a lambda function that monitors all instance states
  + The logs were put into a log group called aws/lambda/EC2InstanceChange
* Created another lambda function that monitors volume, creation and movement
  + Did this in the virtual environment and did not implement on bear cognition environment
* Had a meeting reviewing weekly activities
  + Talked about cloudwatch
* Cloud trail integration is still working very well
  + Daily logs being collected from user api calls
* Researched how to integrate cloudwatch and VPC’s
* Decided lambda was not the route and to use logflows in the vpc service
* Created an IAM role for a logflow from BearCogVPC to CloudWatch Logs
  + The IAM role needed service permissions
  + It also needed a custom policy that was obtained from aws documentation
* Created a new log group in cloudwatch(BearVPCFL)
* Attempted to make a logflow that connected BearVPCFL to the vpc and it failed
  + Reviewed forums
  + Followed more tutorial videos
  + Rechecked IAM permissions
  + Had to delete a tag and create a new IAM role
  + This fixed the problem
* Pointed BearVPCFL’s stream into the S3 bucket to move the logs
* Queried the logs to see what request caused the spikes
  + Did this using log insights in cloudwatch
  + Exported the queried information in a csv format
  + Made it into a excel workbook and color coated based on instance and if it was outgoing or incoming traffic
  + Sent the color coated workbook to Kayce for review
* Need to find a way for log groups to automatically push their logs into the s3 bucket daily