#### **Amazon Web Services Console**

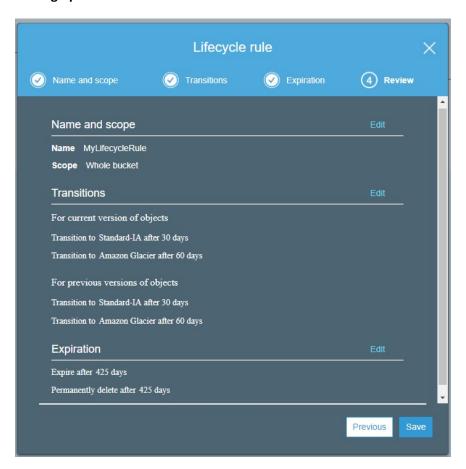
Kin Cheng

### Setting up Identity Access Management (IAM)

### Welcome to Identity and Access Management IAM users sign-in link: https://kincheng101.signin.aws.amazon.com/console 🚑 Customize **IAM Resources** Users: 1 Roles: 10 Identity Providers: 0 Groups: 1 Customer Managed Policies: 4 Security Status 5 out of 5 complete. Delete your root access keys $\checkmark$ Activate MFA on your root account $\checkmark$ Create individual IAM users $\checkmark$ Use groups to assign permissions Apply an IAM password policy $\checkmark$

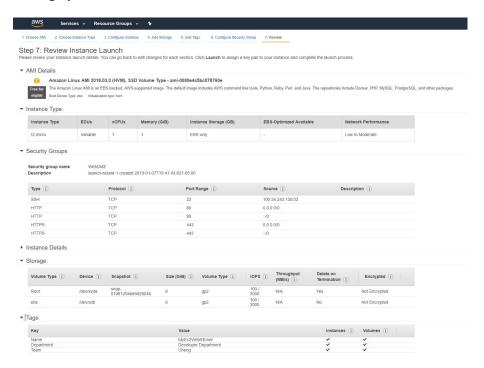
- 1. Created user kin.cheng within a group called TeamCheng
- 2. TeamCheng has a policy of AdministratorAccess to grant highest level of access
- 3. Activated Multi-Factor Authentication for enchanced security
- 4. Configured strict password policy (I.e. password length, expiration, no password reuse)

## **Setting up S3 buckets**



- 1. Created bucket called kin.cheng.project.folder (global access)
- 2. By default, S3 buckets and items within are private. Configure to allow public access to bucket
- 3. Make each individual object in bucket public
- 4. Set Lifecycle rules to transition files from Standard to:
  - a. Standard-IA (infrequently accessed) after 30 days
  - b. Glacier after 60 days
- 5. Set Expiration after 425 days
- 6. Turn on Versioning to preserve, retrieve, and restore every version of every object in the S3 bucket

# **Setting up EC2**



- 1. Select Linux operating system. Default image includes Python, MySQL, PRstgreSQL, and other packages
- 2. Choose t2.micro which has low to moderate network performance
- 3. Add tags such as {"Name": "MyEc2WebServer", "Department": "Developer Department"}
- 4. Add Security Group as a virtual firewall for this instance.
- 5. Use CloudWatch to monitor resources and cost of ownership