# WEEK 7 ASSIGNMENT 1

**Large-Scale Data Storage Systems – DATA-5400 | Spring 2020**

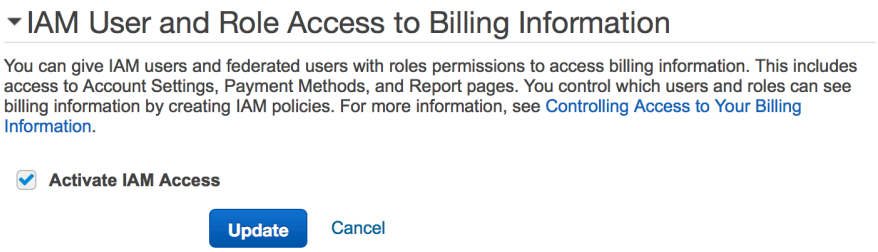
**Christina Morgenstern**

---

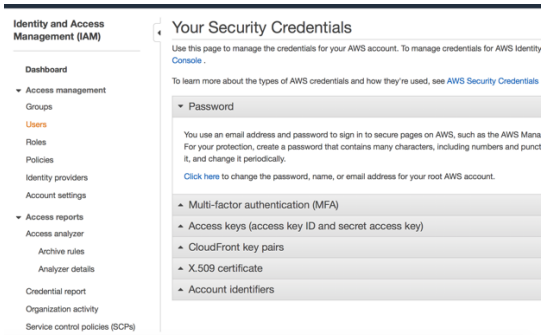
Securing AWS resources is important to specify who can access which services as well as to keep your data protected.

## I. Creating users on AWS

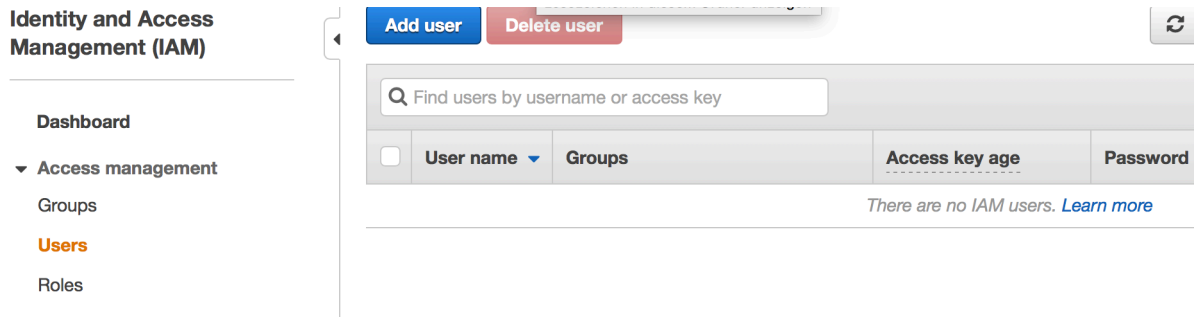
Enable access to billing to other users within my account settings. Go to IAM User and Role Access to Billing Information and Activate IAM Access.



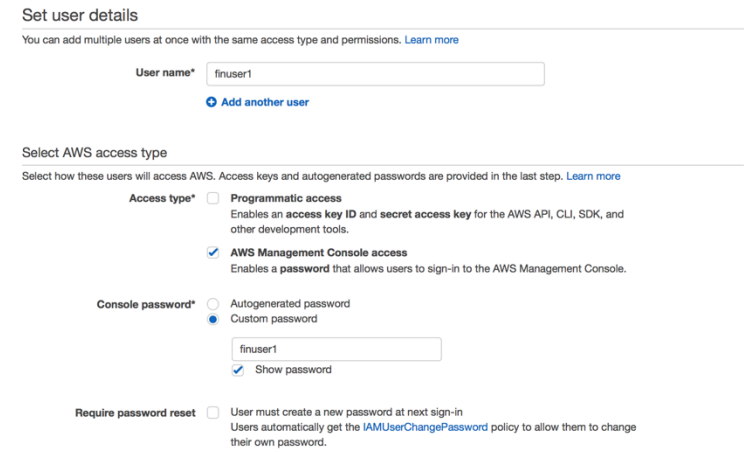

In the Identity and Access Management section choose Users in the left hand panel.

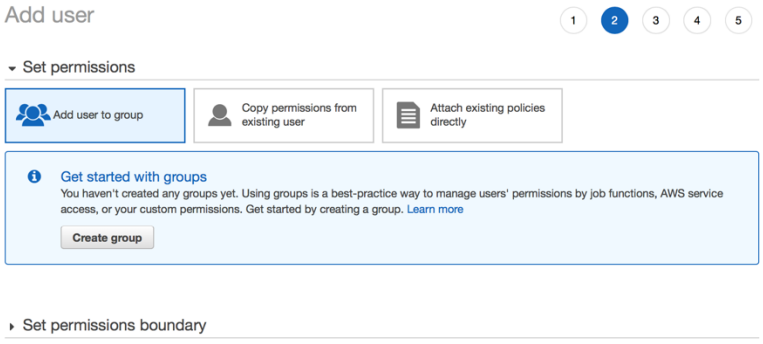


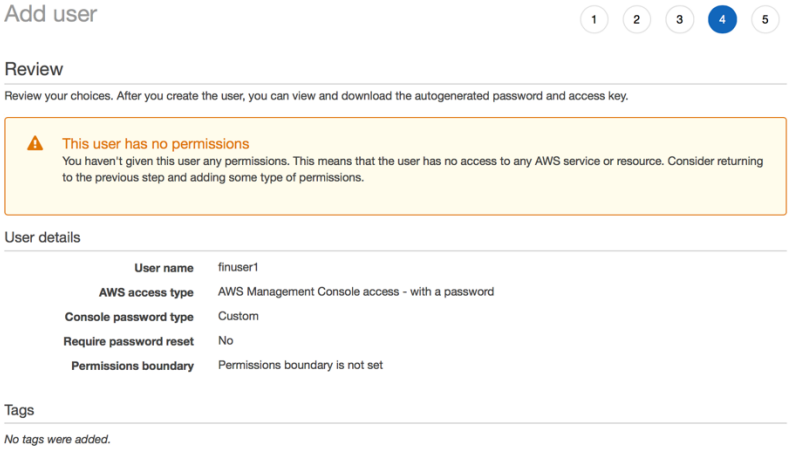

To add a new user select Add user.



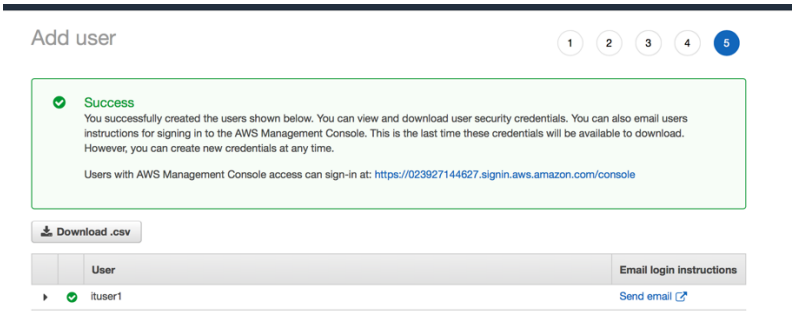
The Wizard guides through the set-up process and helps specifying user details, like user name and password, as well as access information. In our case finuser1, a prospective user from the finance department, was created.



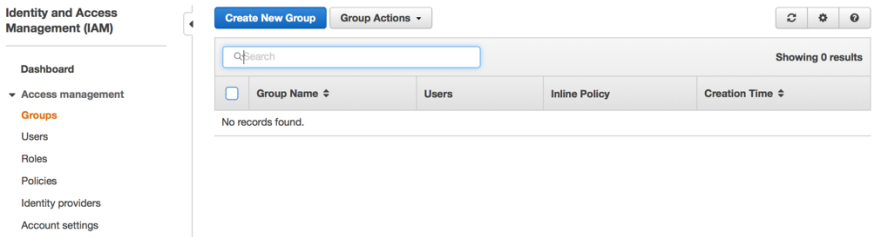



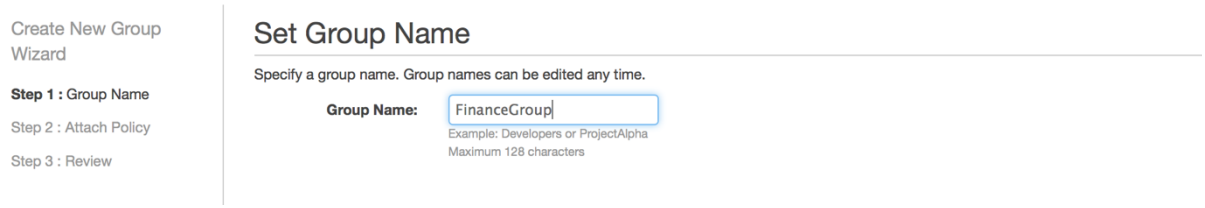
The previous steps were repeated to create a second user, ituser1, a potential user from the IT department.



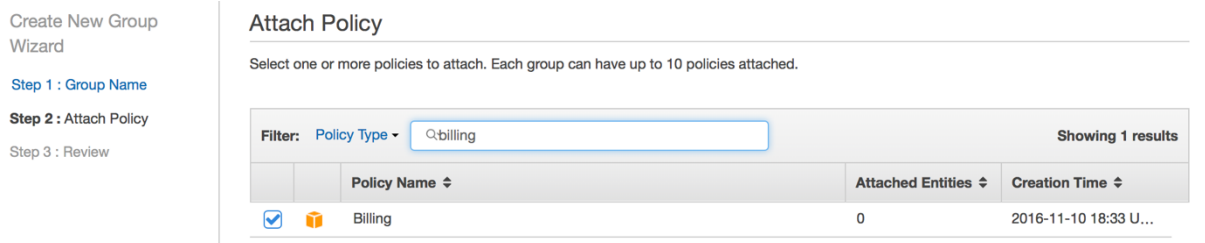

The assigned users finuser1 and ituser1 should be assigned to separate groups. Groups were created through navigating to the left-hand panel and selecting Create New Group.

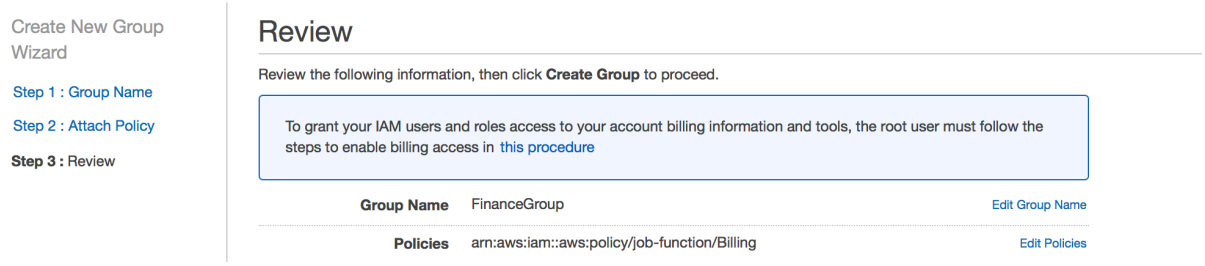


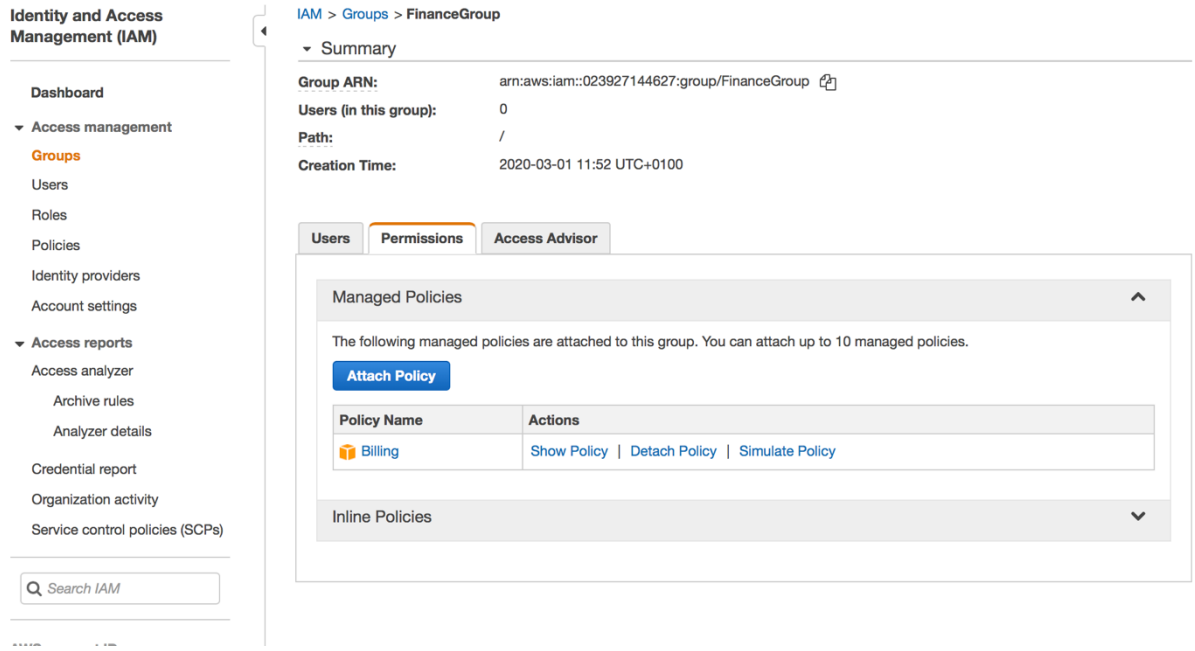

The create New Group Wizard guides through the set-up process.
First, specify a group name, such as FinanceGroup, the group responsible for dealing with e.g. salaries.



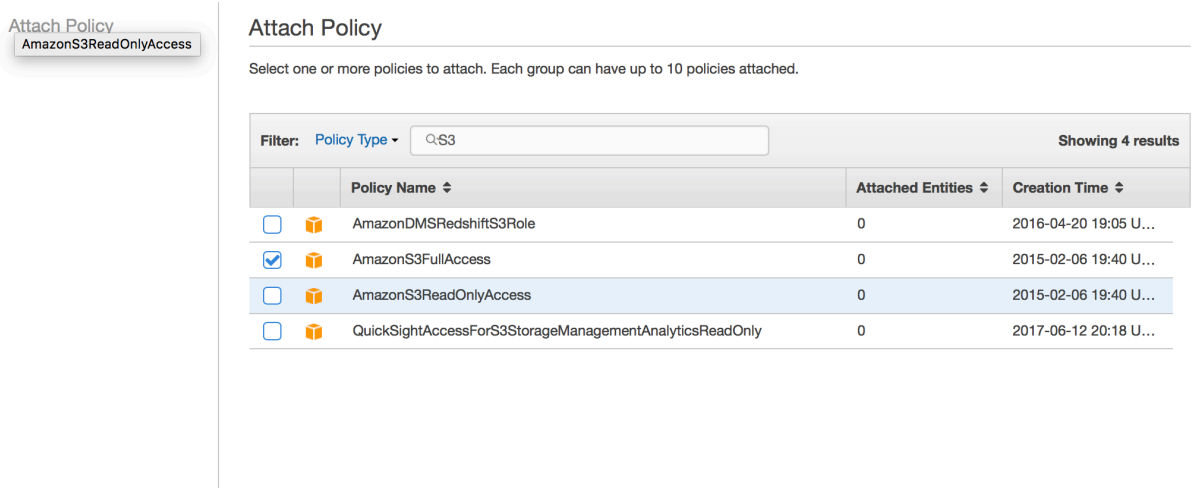

Attach group relevant policies in the second step. The FinanceGroup should have access to Billing and full S3 services. Attach the policy through searching for the respective terms and selecting the policy type.



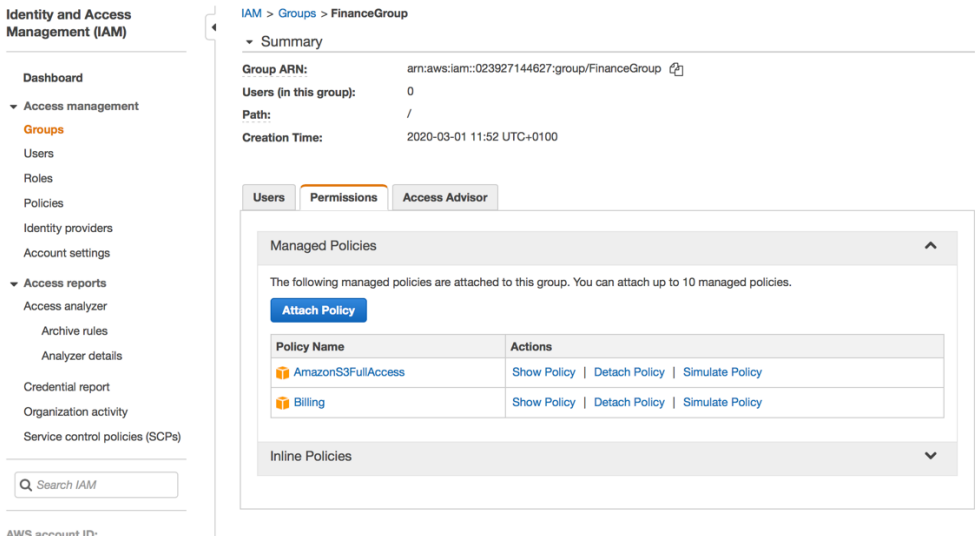





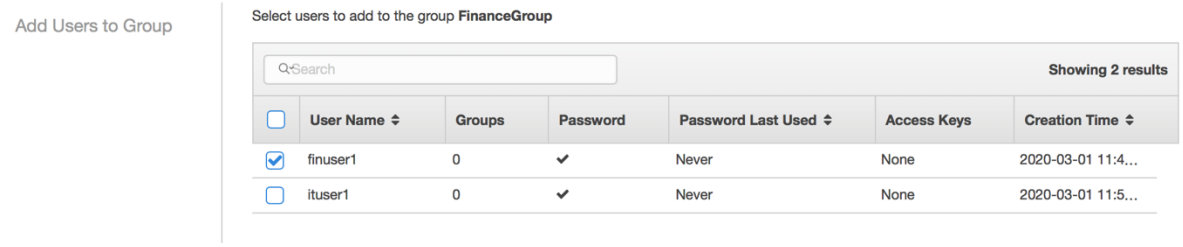

Repeat the steps for attaching a further policy that allows for full access to S3.



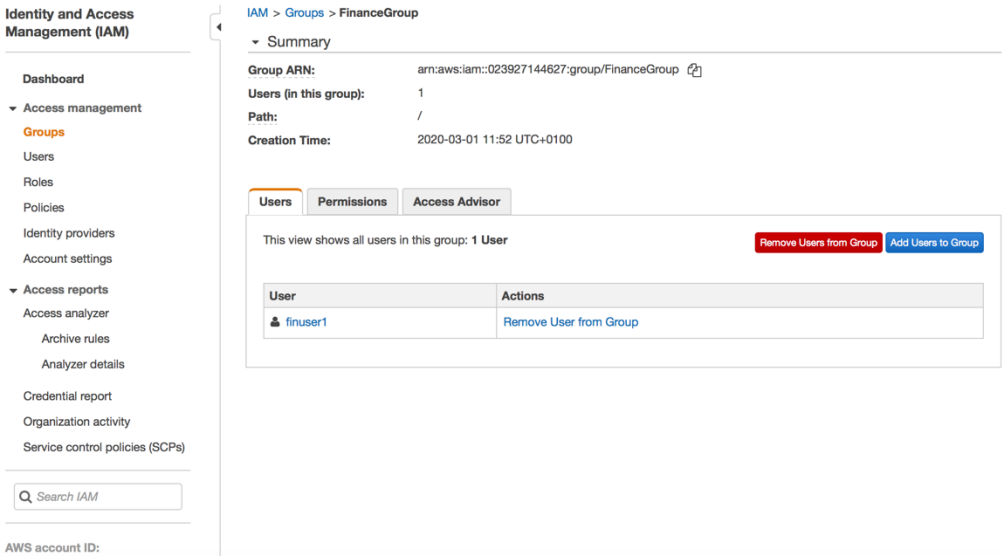

The FinanceGroup has obtained permissions to access the billing and S3 full access.



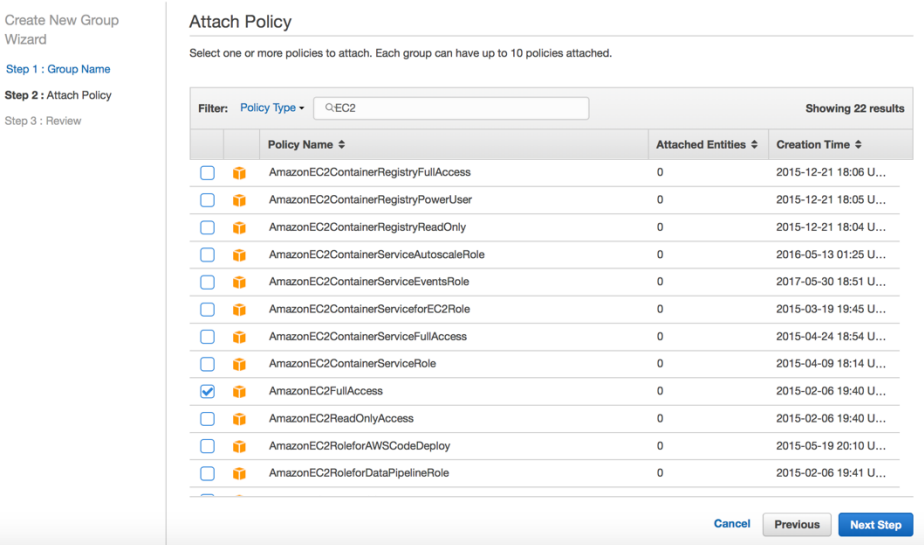
Add finuser1 to the FinanceGroup.



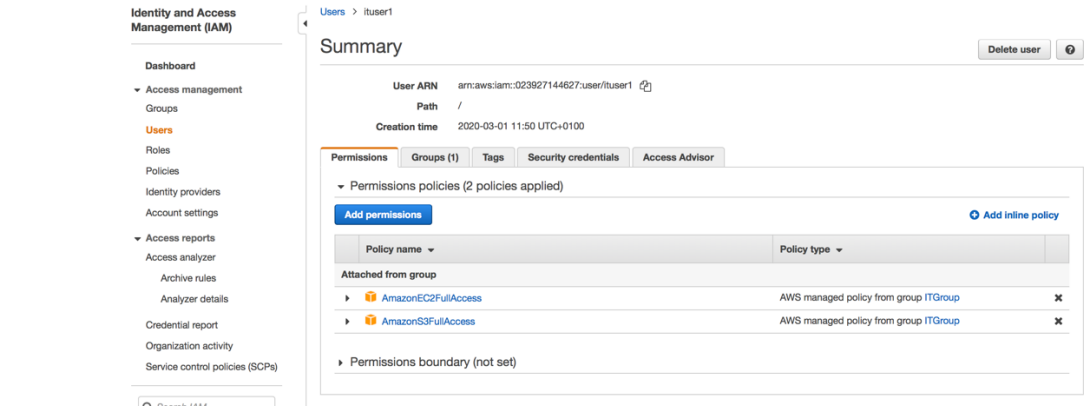

Summary of FinanceGroup with one user.



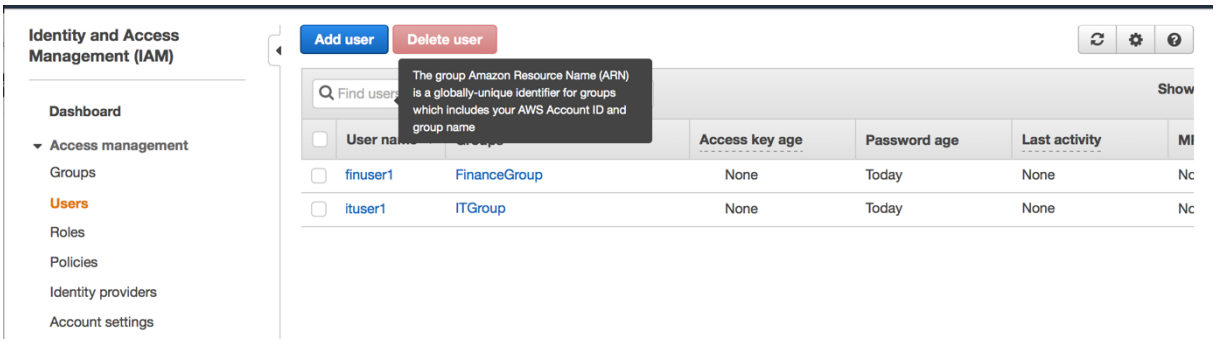

Selecting policies can also be done in one go through ticking the relevant policy names from the list. The ITGroup should get full access to both, EC2 and S3.



The ituser1 has access to EC2 and S3.

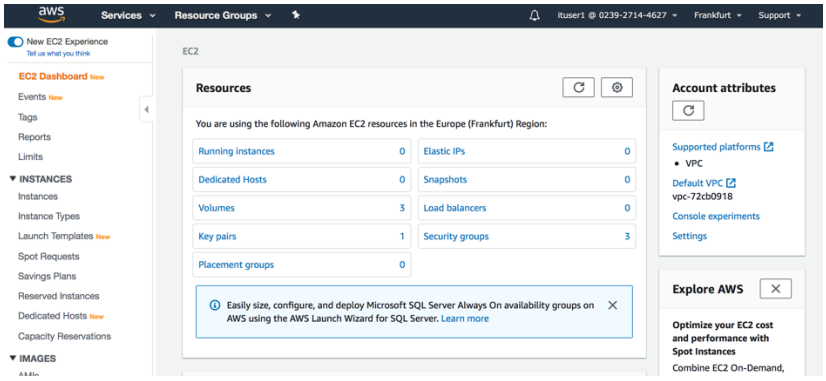



Summary of groups and assigned users.

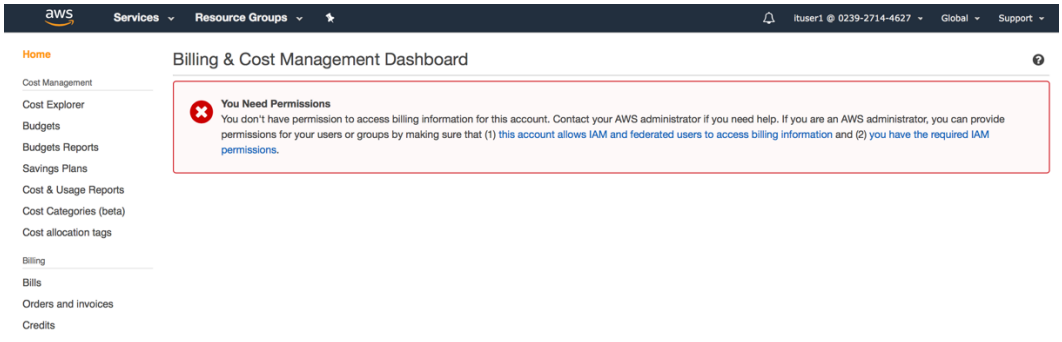



To confirm the settings and permissions of each user, log onto the console using my Account ID as well as user name and password of either the two users, ituser1 and finuser1, as specified above.

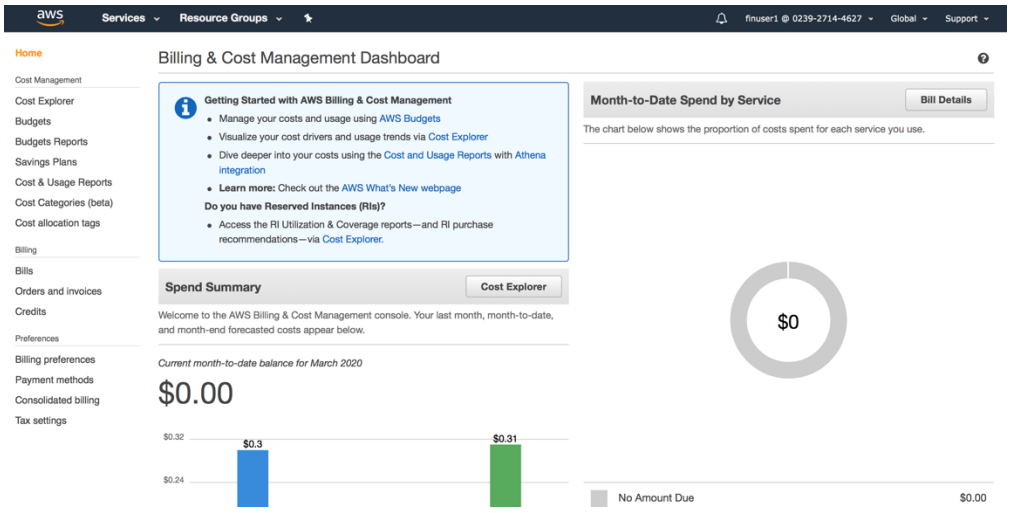
Log on as ituser1 who has access to S3 and EC2.



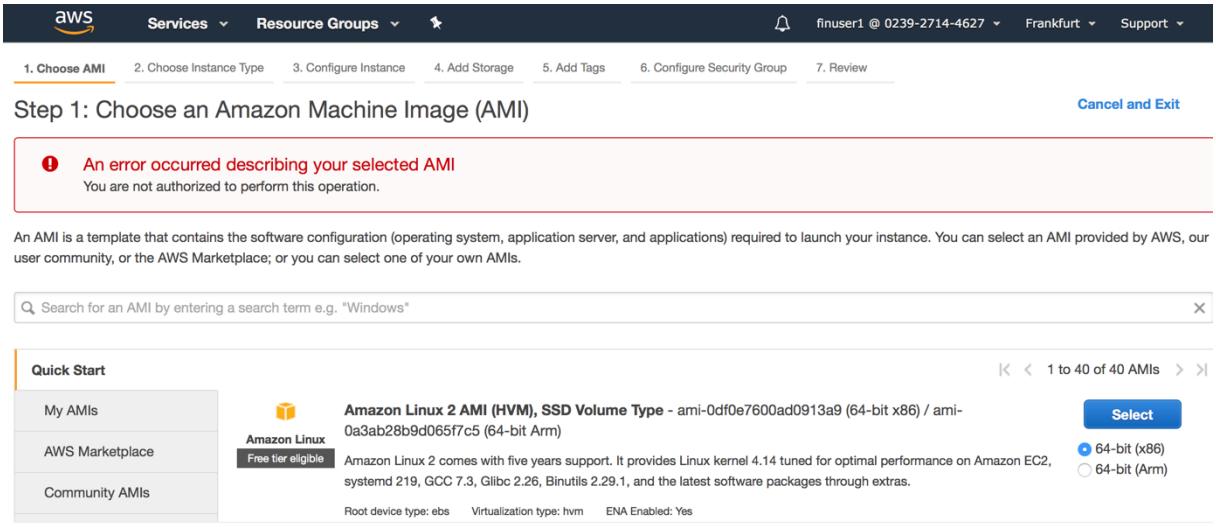

Access to billing information by ituser1 is prohibited.



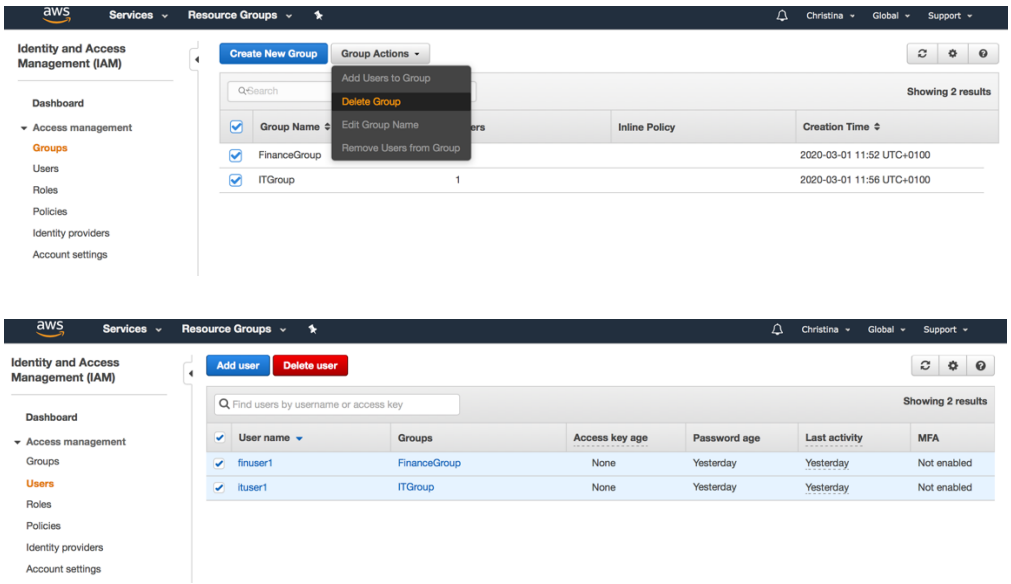
In contrast, finuser1, can see the billing and cost management dashboard.




However, setting up an EC2 instance is not possible for the finuser1.

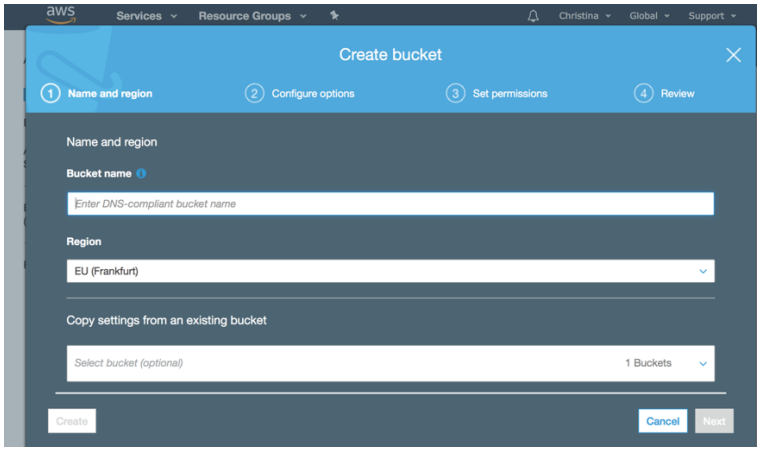


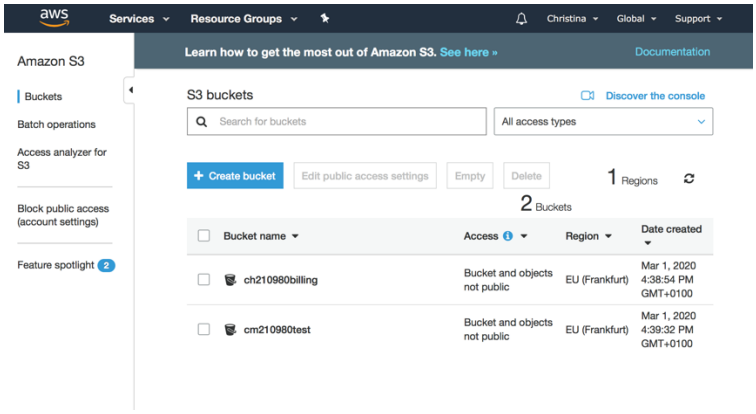

Delete groups and users as follows:



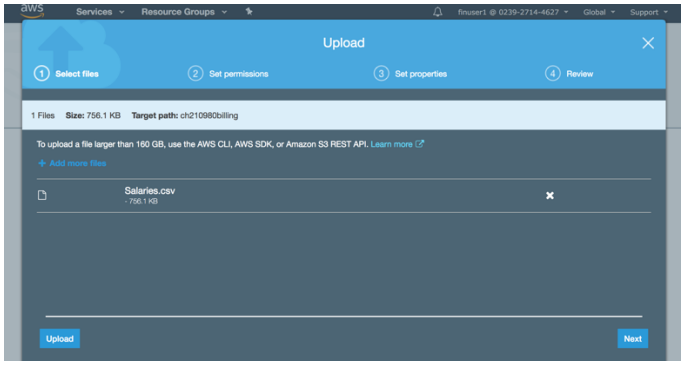
## II. S3 bucket policy

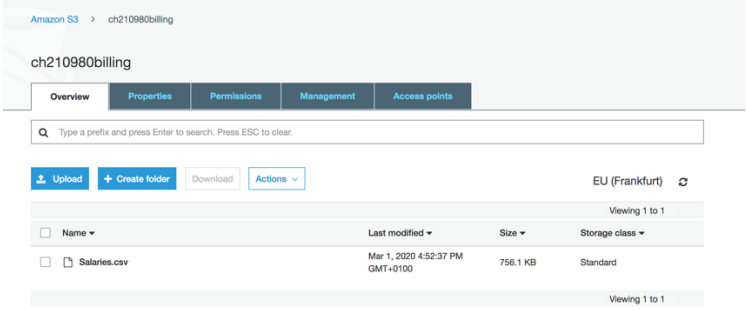
Create an S3 bucket named ch210980billing within the console.



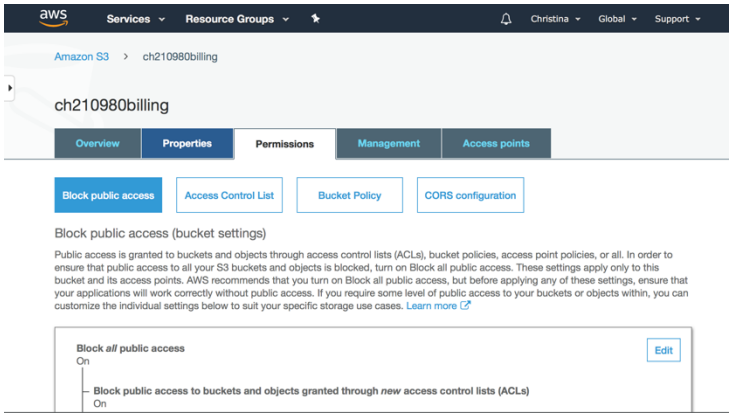




Upload the file salaries.csv into the bucket.

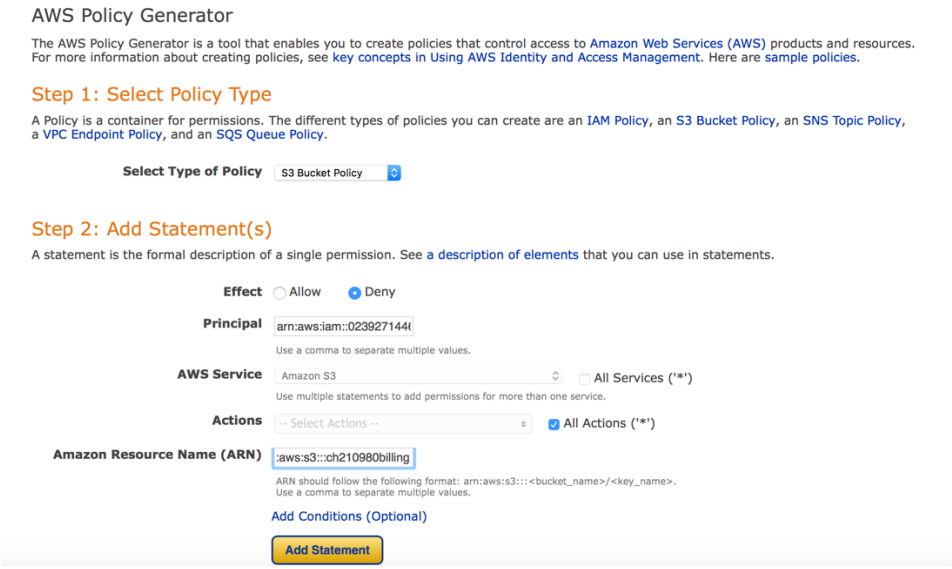


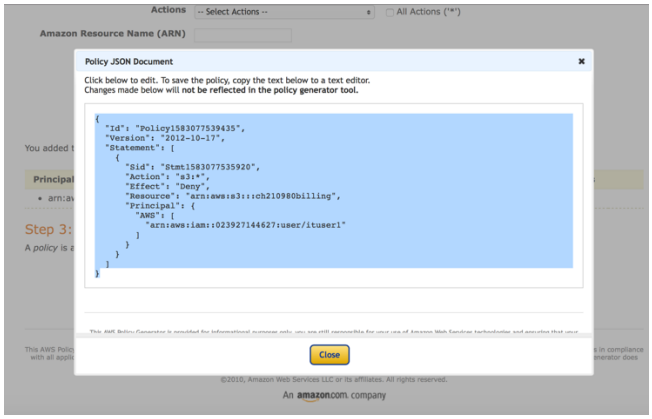
Create a bucket policy so that only User1 can read the contents.
Select the Permissions tab

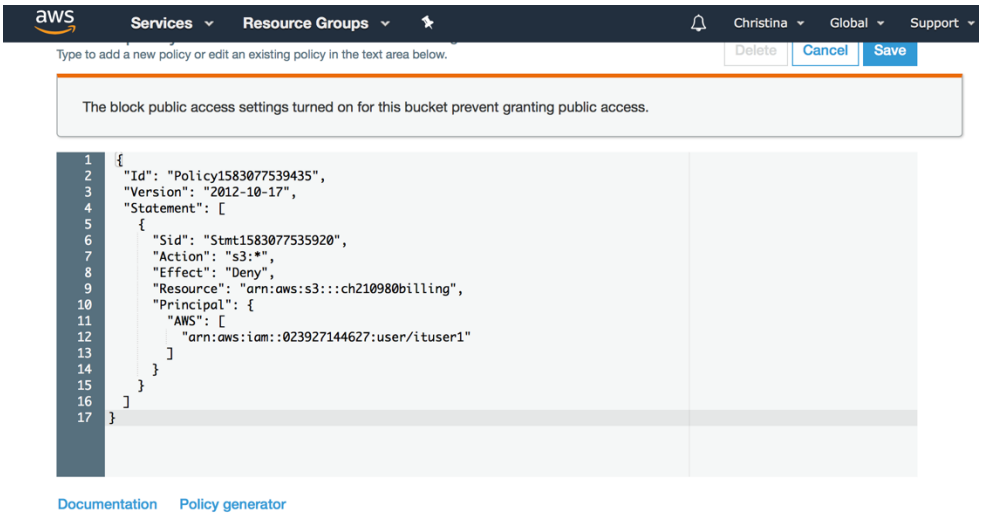



The AWS Policy Generator wizard helps in creating policies controlling AWS resources. Select S3 Bucket Policy as Policy Type. The effect should be a Deny, because we would like to block access to the S3 bucket.

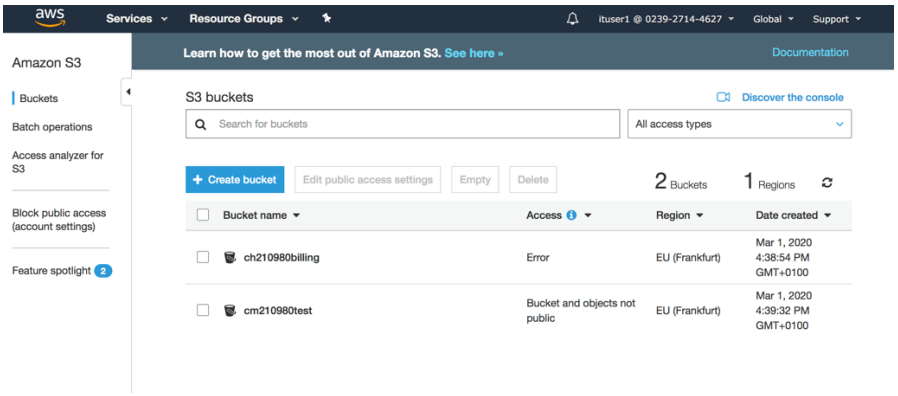


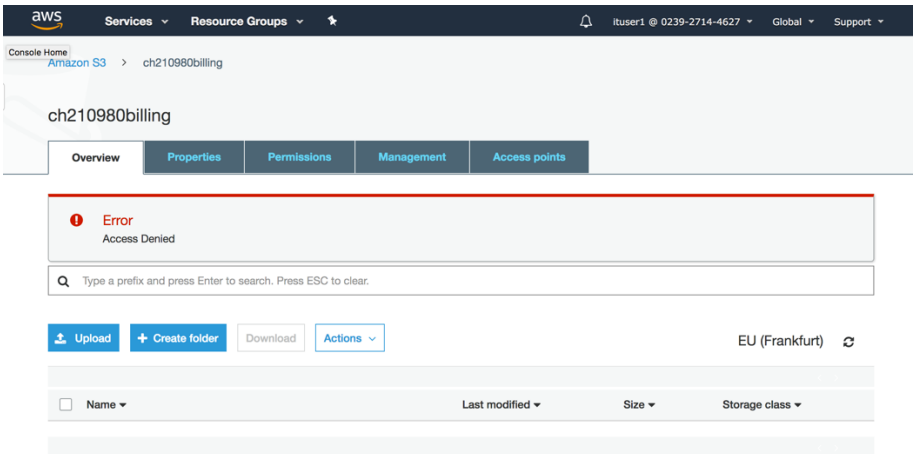

The Policy Generator produces a JSON file which needs to be amended in the Resource section and the AWS section. In this case ituser1 is prohibited from gaining access to the S3 billing bucket because it contains information on salaries.





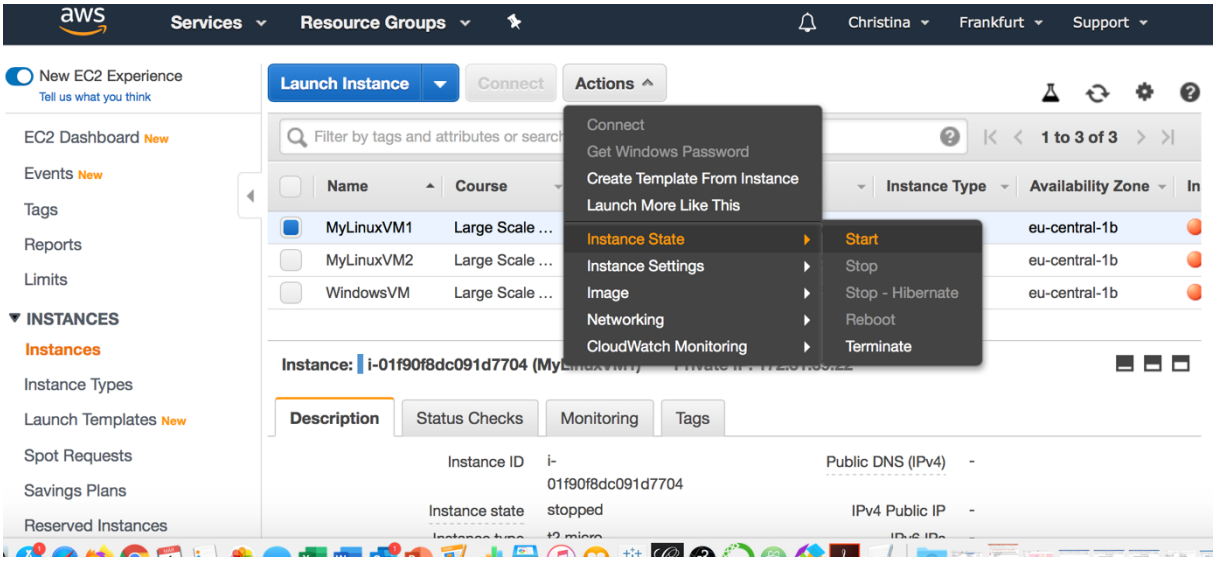

When logging onto the console as the ituser1 and trying to access the S3 bucket ch210980billing, an error message occurs and I am blocked from accessing the resource.

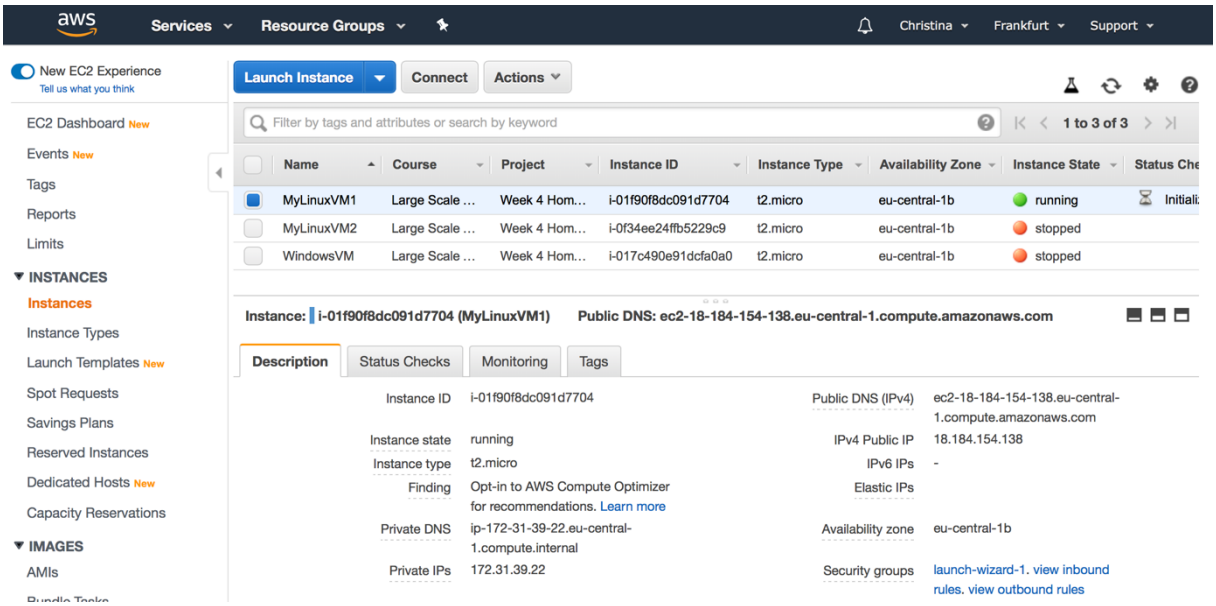


## III. Modify EC2 security settings

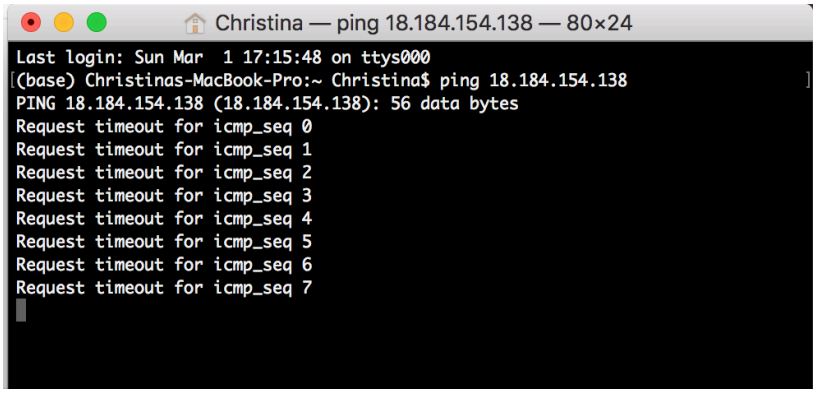
Start the Linux virtual machine MyLinuxVM1 within the EC2 dashboard.



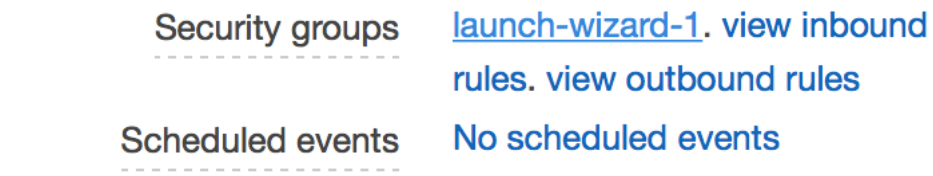

Try to ping the VM using the Terminal window on my Mac.

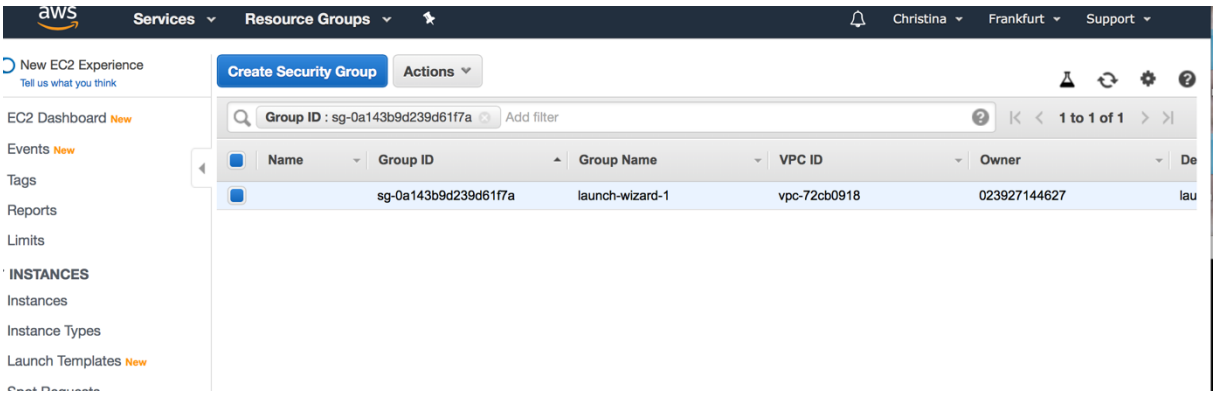
`ping` IP address

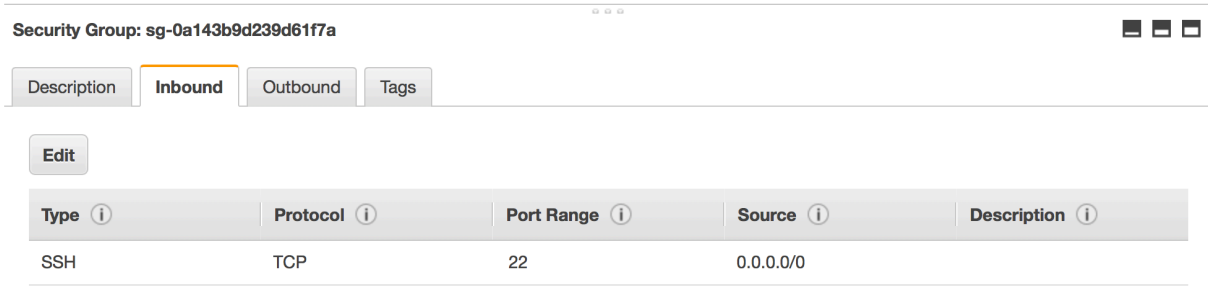



Ping doesn´t allow to connect to the VM by default.

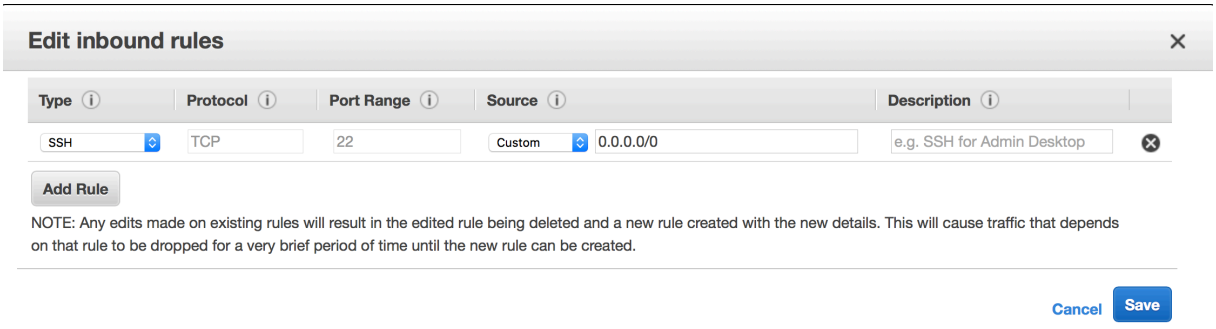
Amend the security settings to allow ping and launch the wizard.

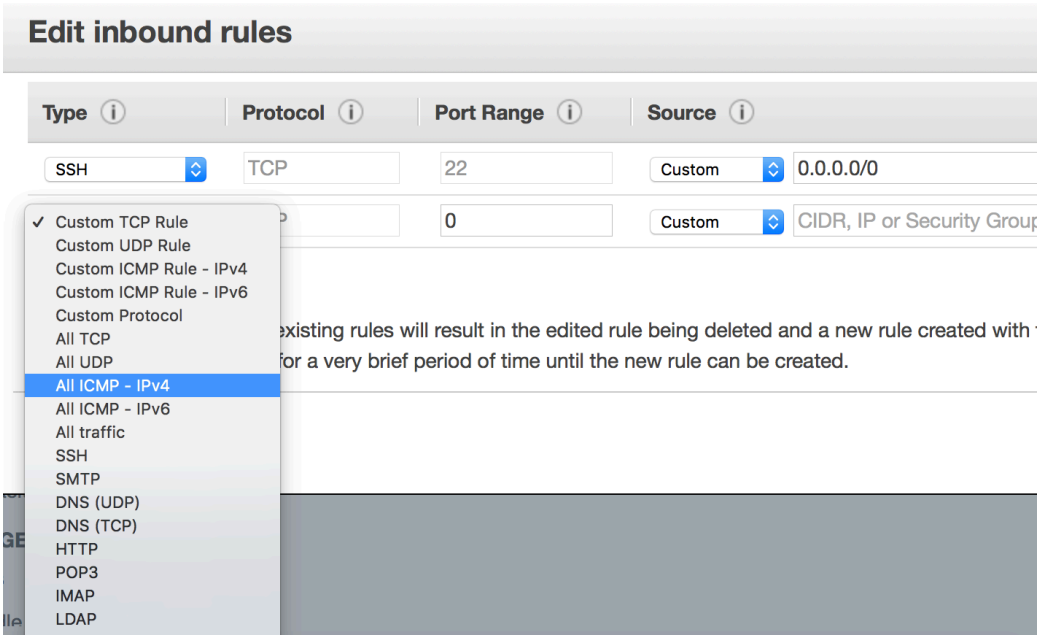


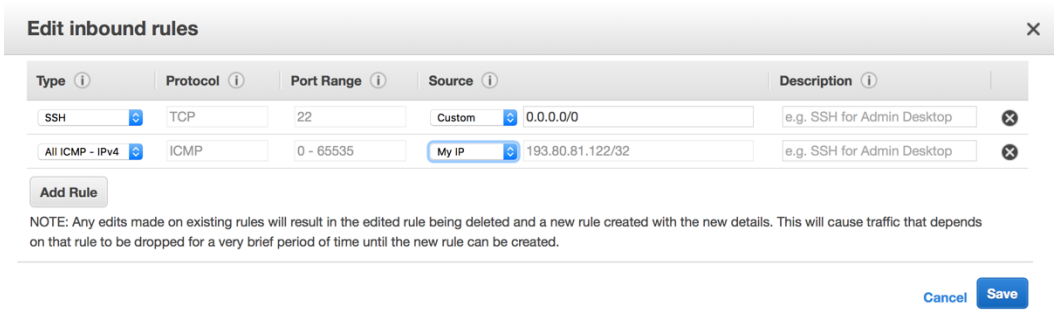




Edit inbound rules through adding a new rule.

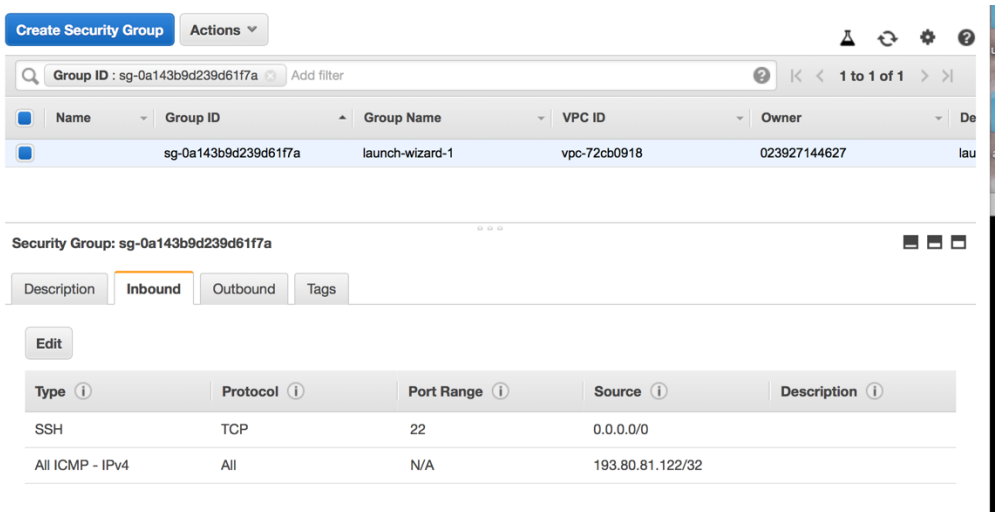




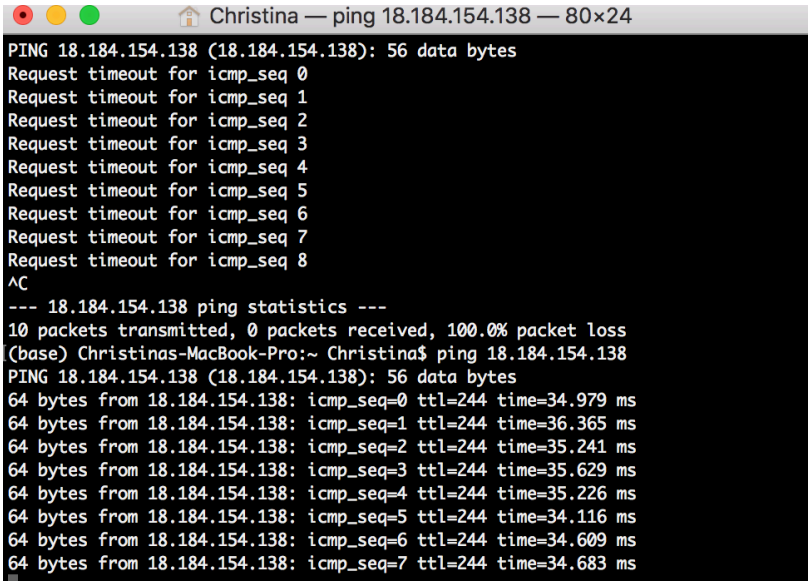

This rule should allow connecting from my IP address to the VM using ping.




Overview of security settings of MyLinuxVM1.



Ping is now enabled with my IP address.




Once the previously generated permission is removed, ping is disabled again.