lab

lab title

Introduction to AWS

V1.37

Course title

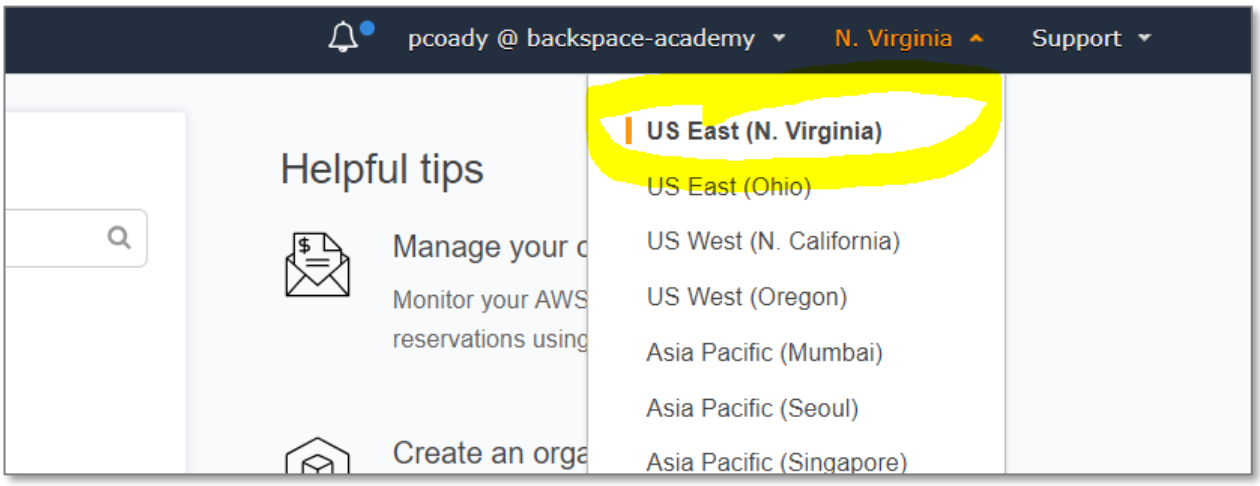
BackSpace Academy
AWS Certified Associate

Table of Contents

Contents

About the Lab

Please note that not all AWS services are supported in all regions. Please use the US-East-1 (North Virginia) region for this lab.



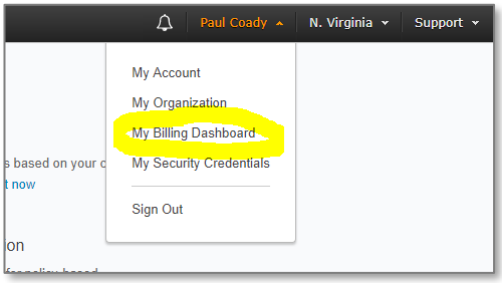
These lab notes are to support the hands on instructional videos of the Introduction to AWS section of the AWS Certified Associate Course.

Please note that AWS services change on a weekly basis and it is extremely important you check the version number on this document to ensure you have the lastest version with any updates or corrections.

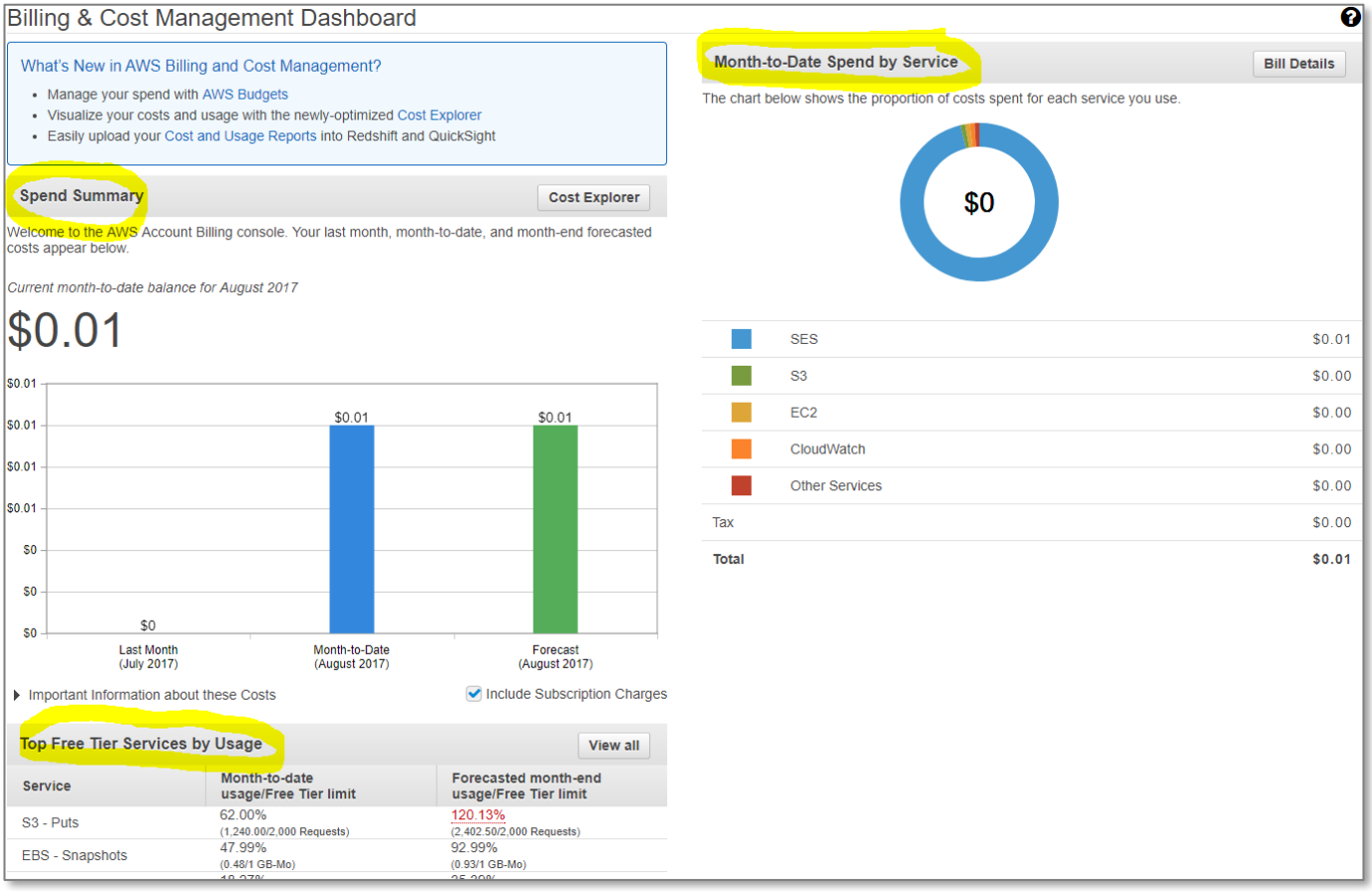
Checking your AWS Usage and Monthly Bill

In this section we will learn how to use the AWS Billing & Cost Management Dashboard to keep track of costs.

From the AWS management console select 'My Billing Dashboard" from the account drop down menu.



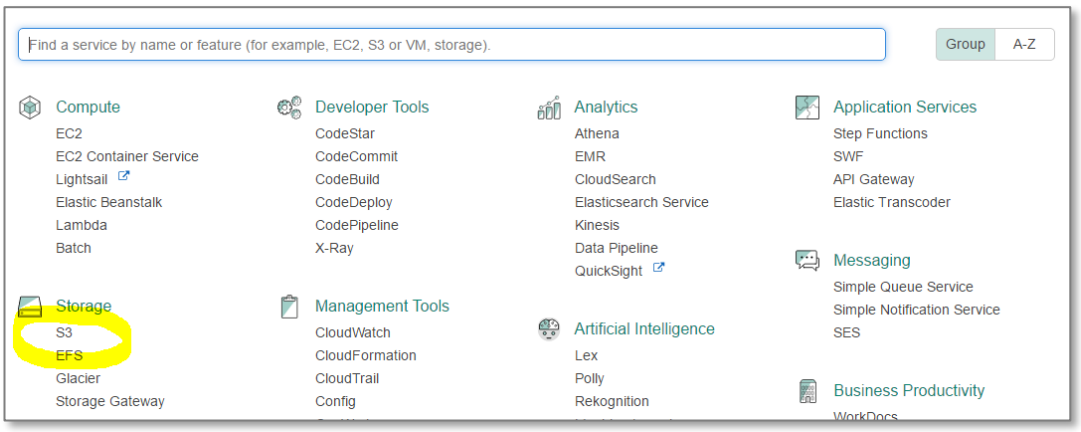
You will now see your total spend summary, spend by service and forecast spend.



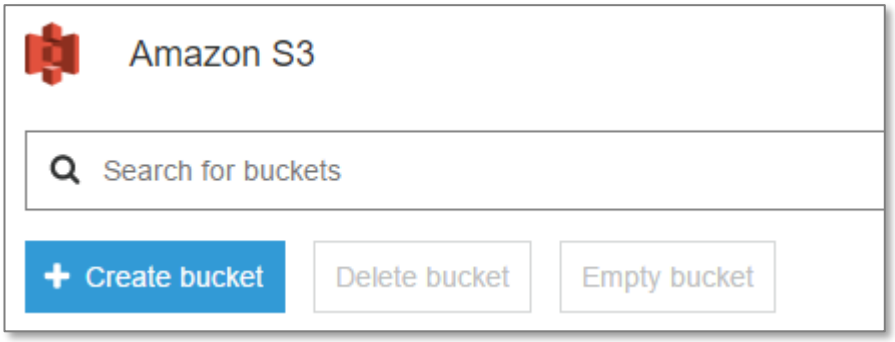
Creating an S3 Bucket and Uploading Files

In this section we will create an S3 bucket, upload files to it and download files from it.

Click on the services menu and select S3.



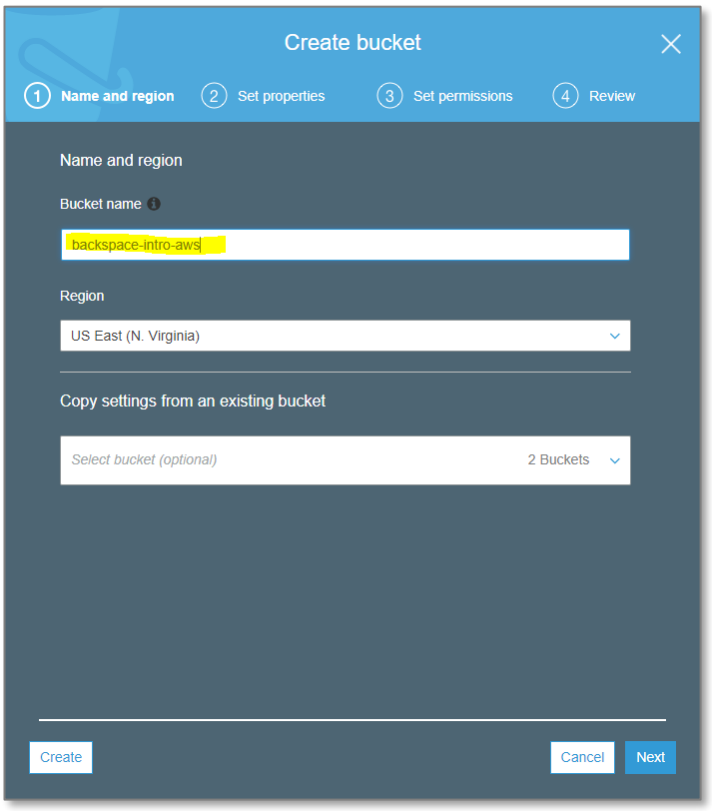
Click on Create Bucket



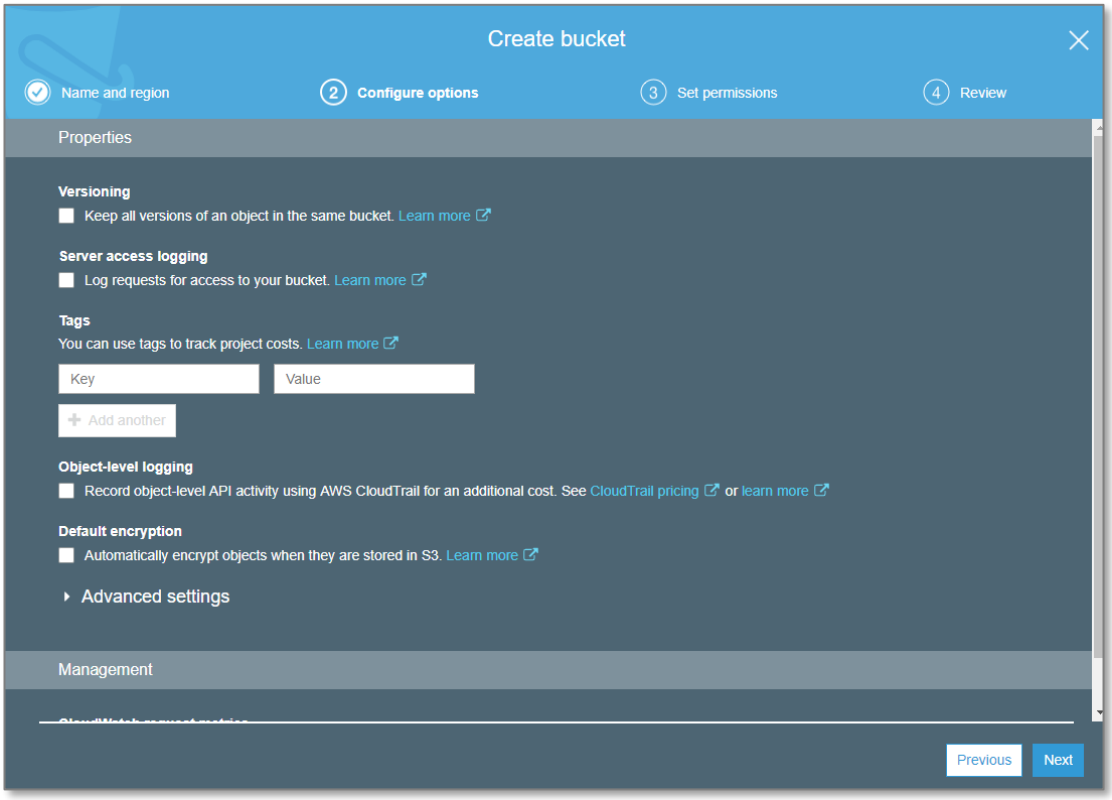
The create bucket dialog box will appear.

Enter a unique name for your bucket (it will need to different from the one below)

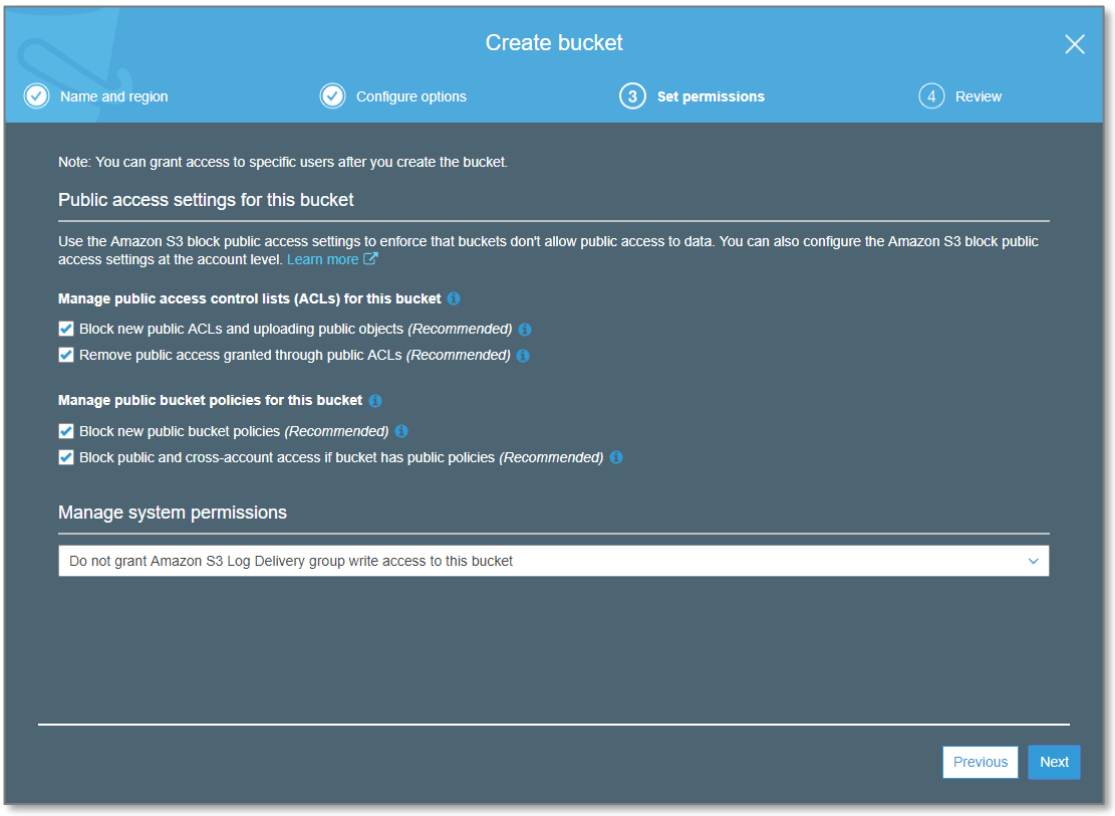
Click 'Next"



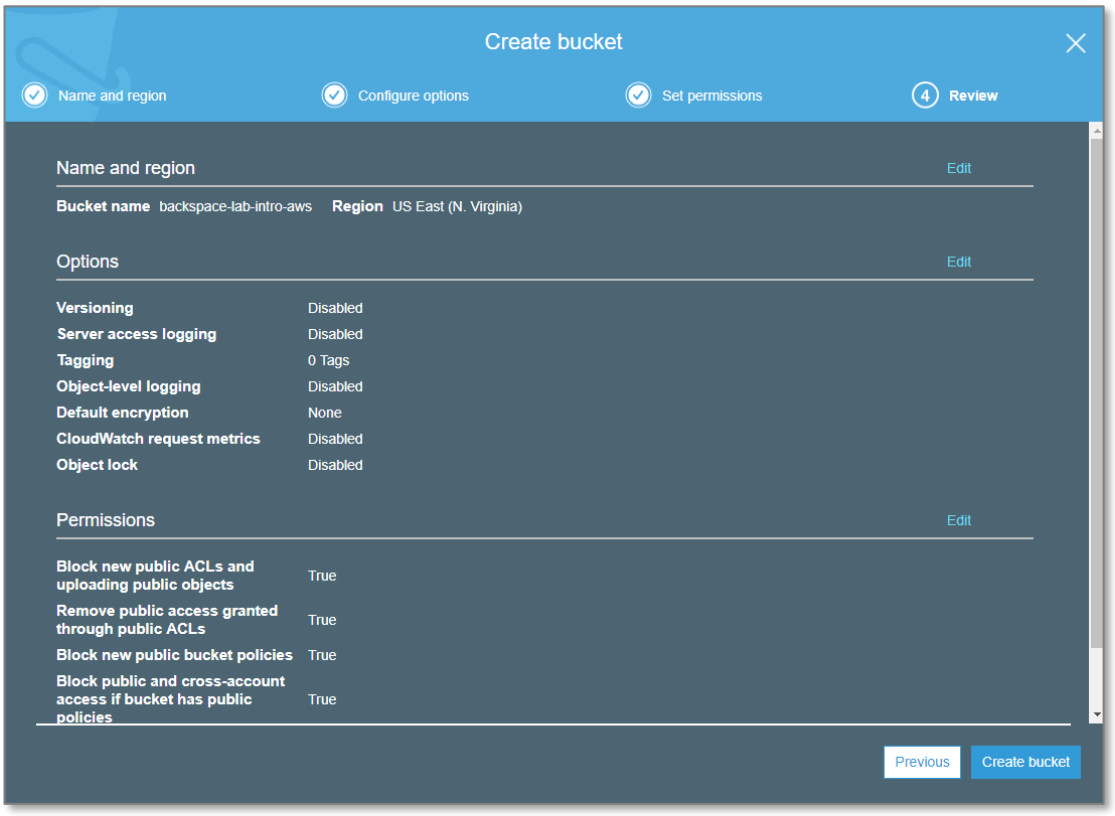
Leave as is and click 'Next"



Leave as is and click 'Next"

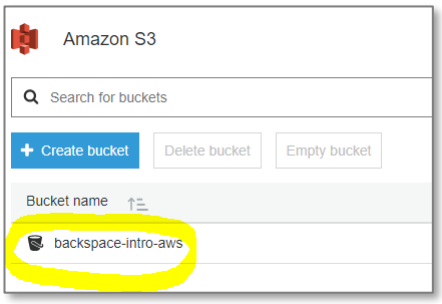


Click 'Create Bucket"

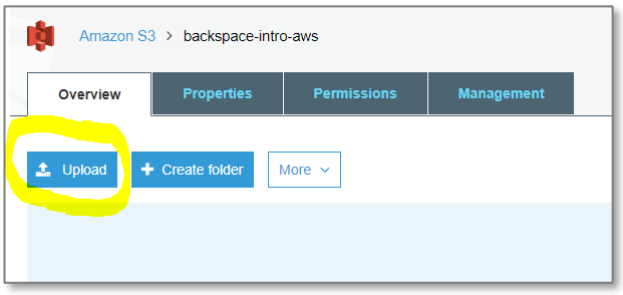


Uploading Files to your Bucket

Click on the link to the bucket

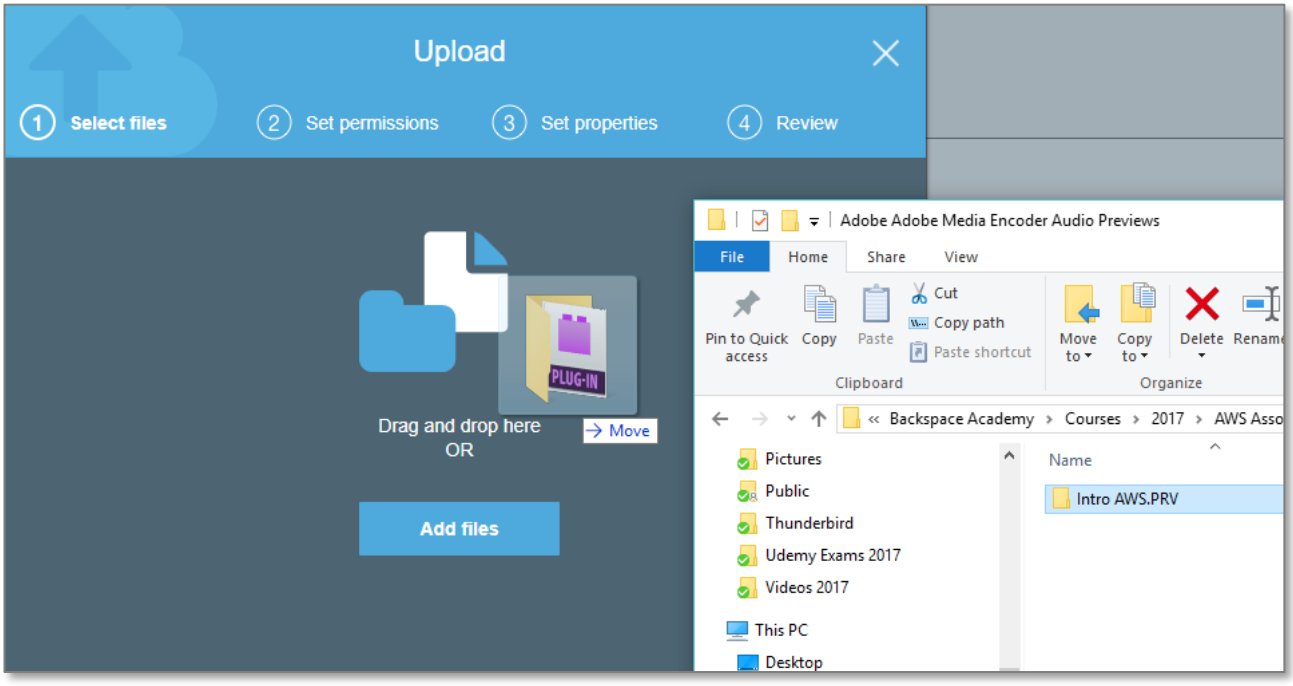


Select 'Upload"

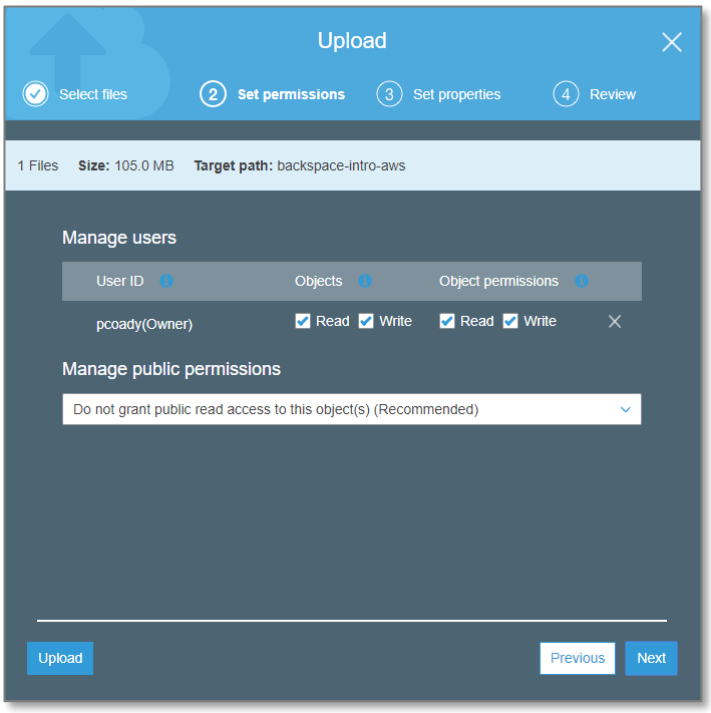


Drag a folder with files onto the form.

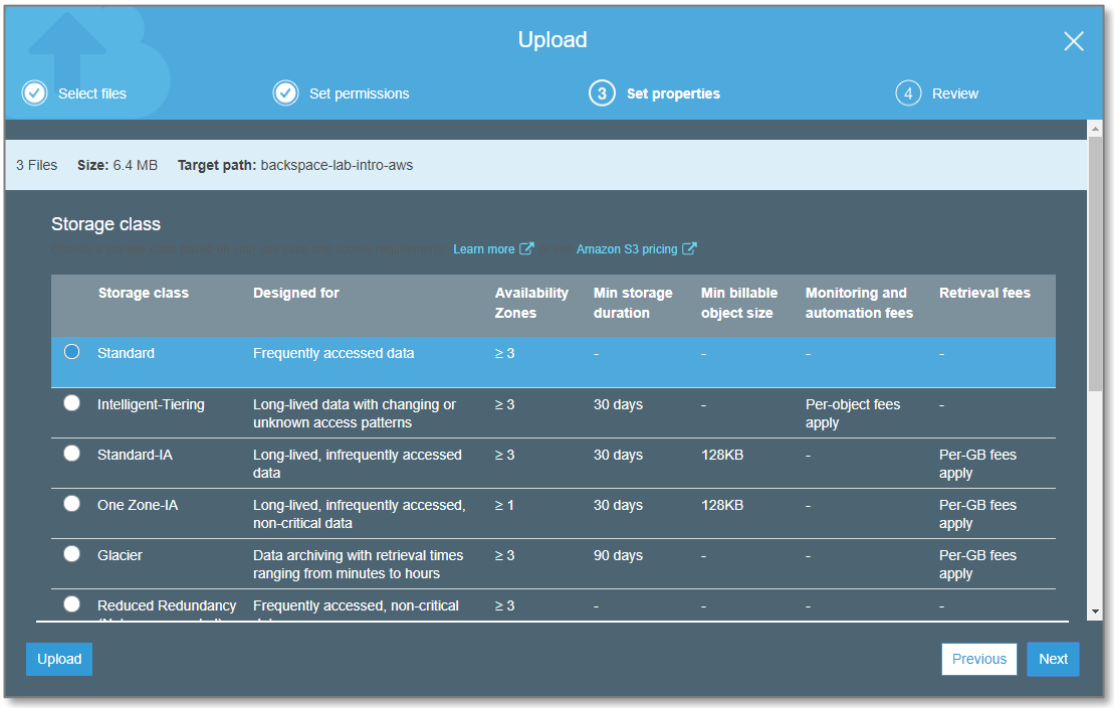
Click Next



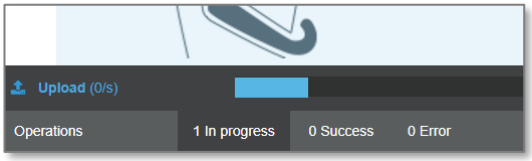
Leave as is and click 'Next"



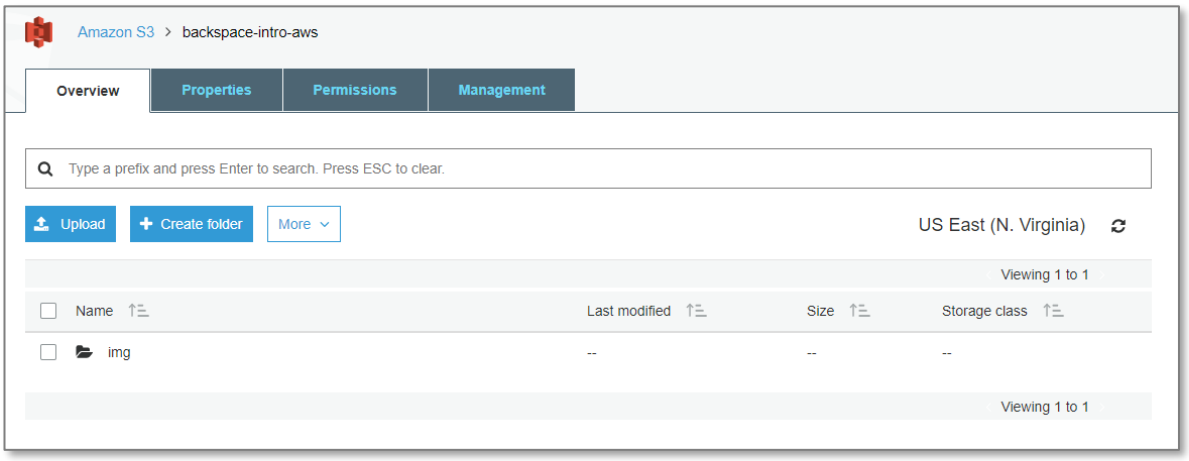
Leave as is and click 'Next"



Click 'Upload"

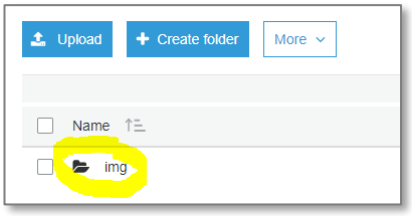


Your upload will eventually complete.

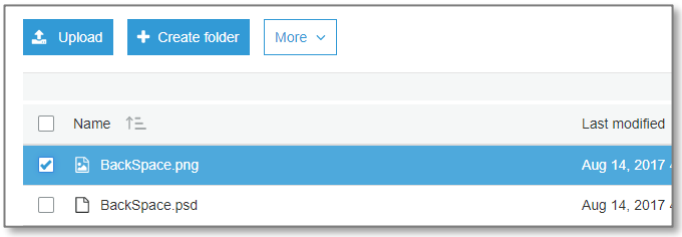


Downloading files from your bucket

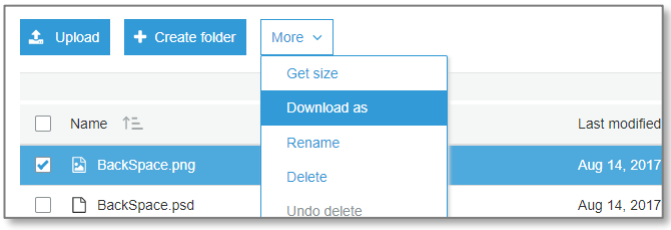
Click the link for your folder



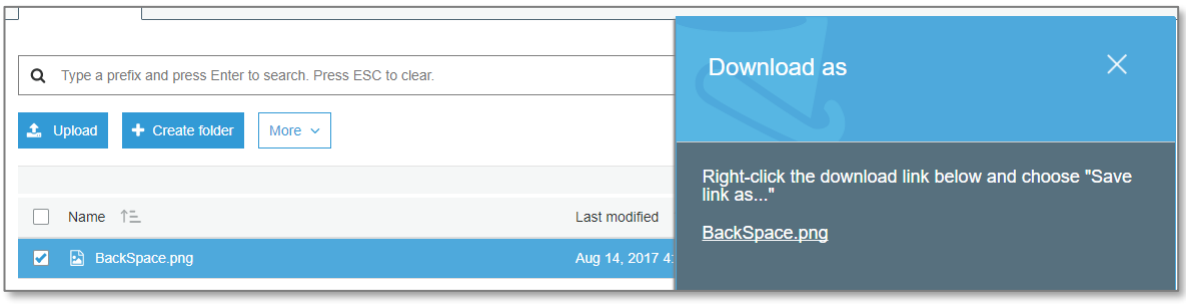
Select a file



Select “More”, “Download As”



Click the download link to download the file.



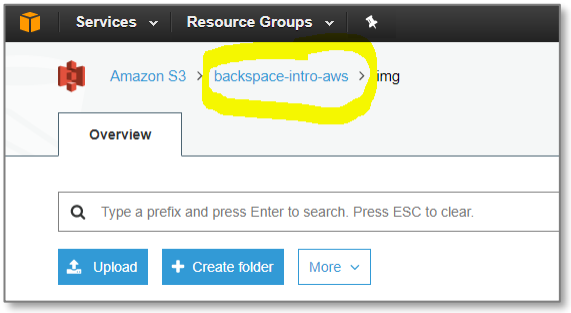
Troubleshooting

If you get the following screen it means you have clicked on the Object URL and not the download link as detailed above. You cannot access files directly from a URL as they have private access.

Clean Up

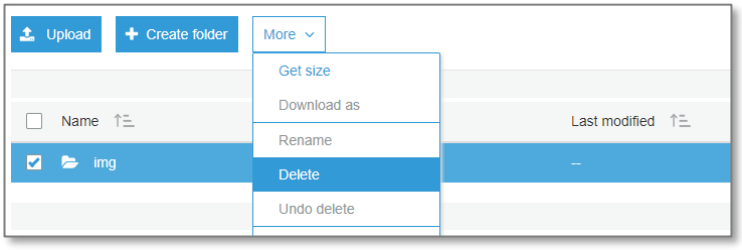
We will now delete the files and bucket so that you will not be billed by AWS.

Go back to your bucket by clicking its link.

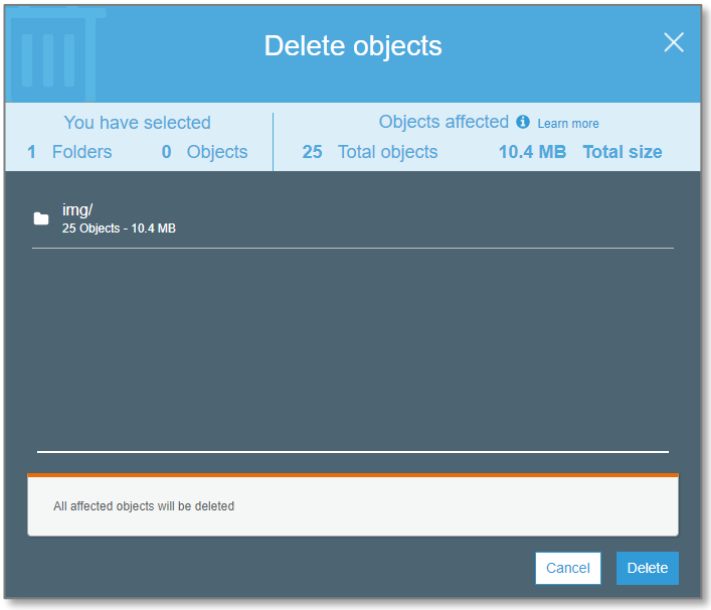


Select the folder

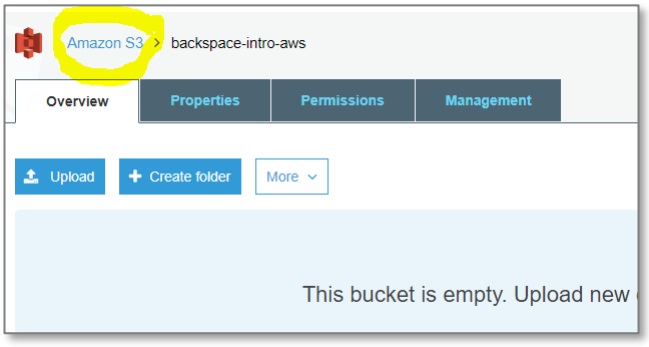
Select “More”, “Delete”



Click “Delete”

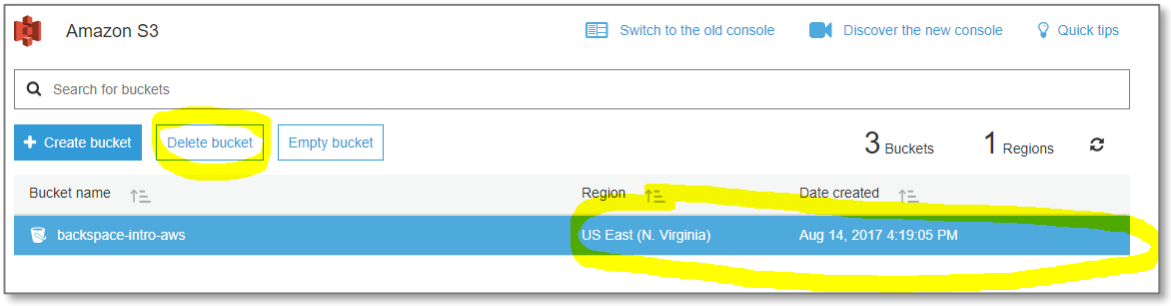


Go back to the S3 dashboard by clicking the link

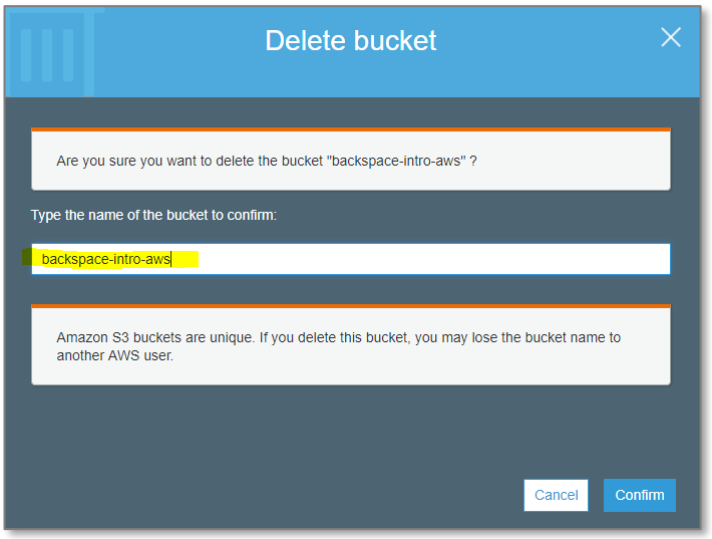


Click on the bucket line but not on the bucket link to select the bucket.

Click “Delete Bucket”



Confirm the name of the bucket to delete



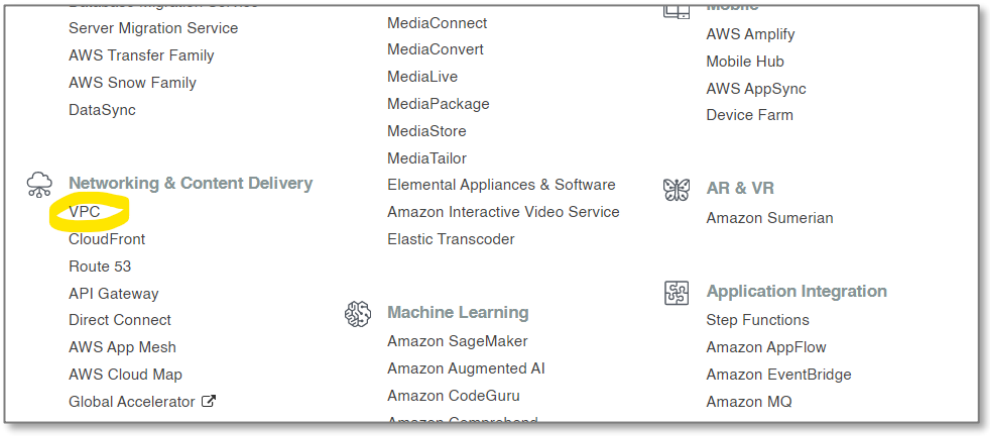
Creating a SQL Database with RDS

In this section, we will use the Relational Database Service to create a database. We will also connect into the database.

Creating a Security Group

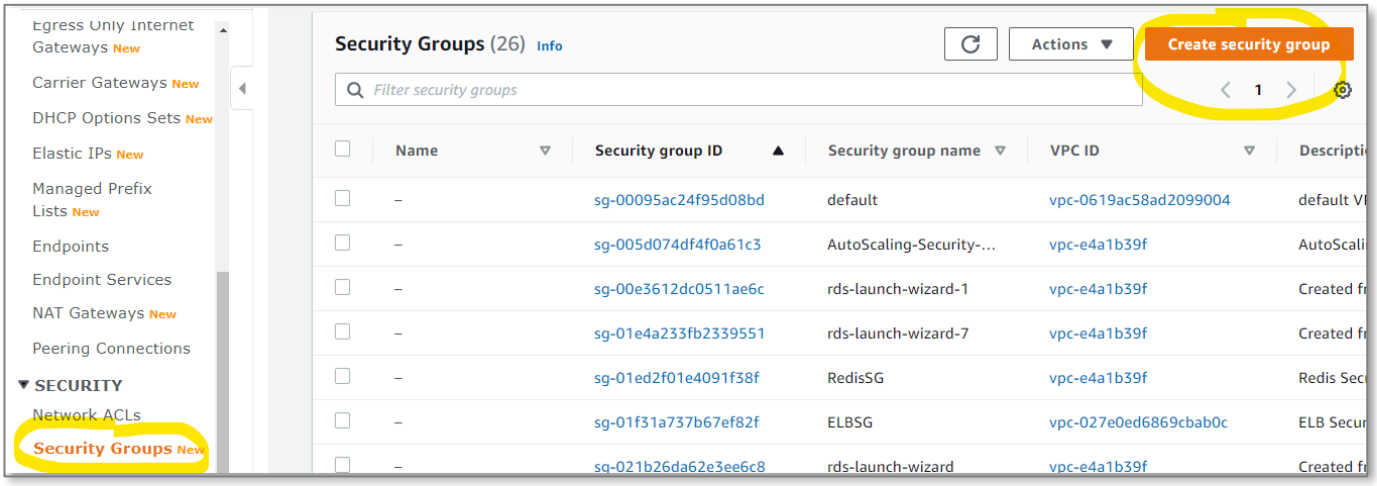
By default, inbound access from the Internet to our database instance is blocked. We will create a security group that defines an inbound rule that allows access from the Internet. We can then associate this security group to our database instance.

From the AWS console select *VPC* from the Networking & Content Delivery services.



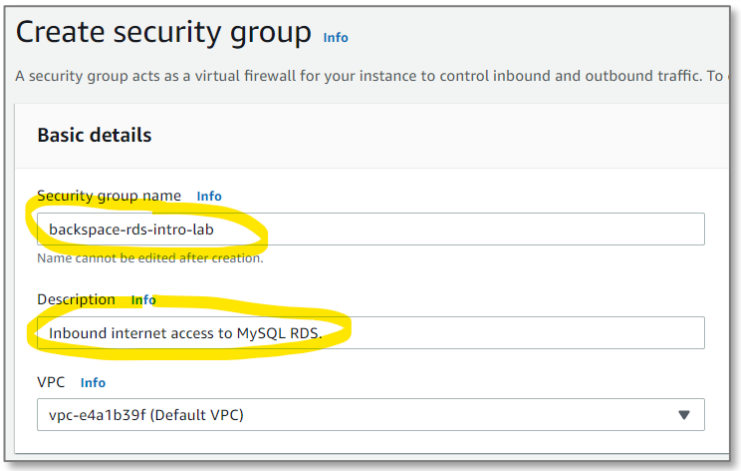
Select *Security > Security Groups*

Click *Create security group*



Give it the name *backspace-rds-intro-lab*

Give it a description

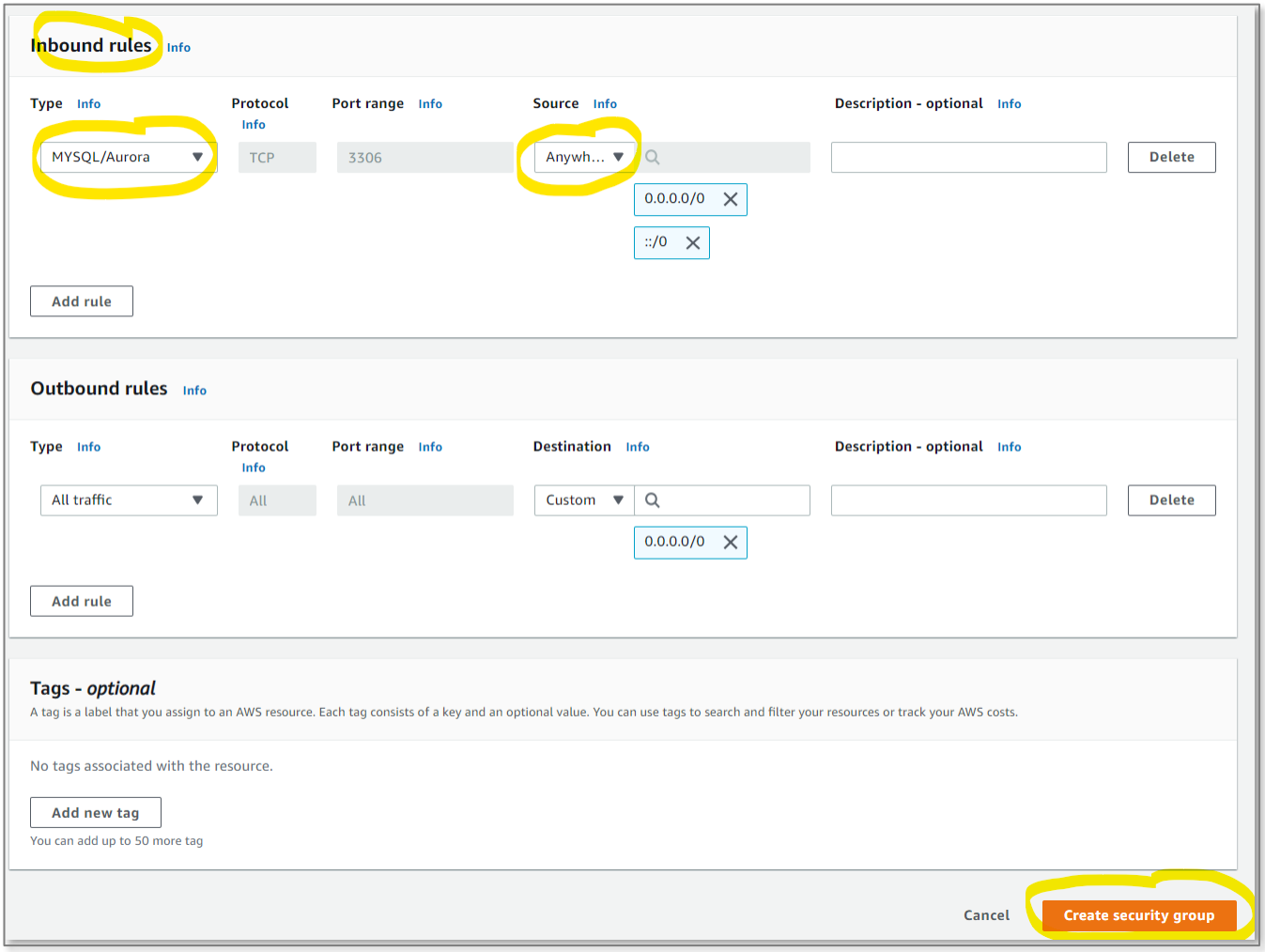


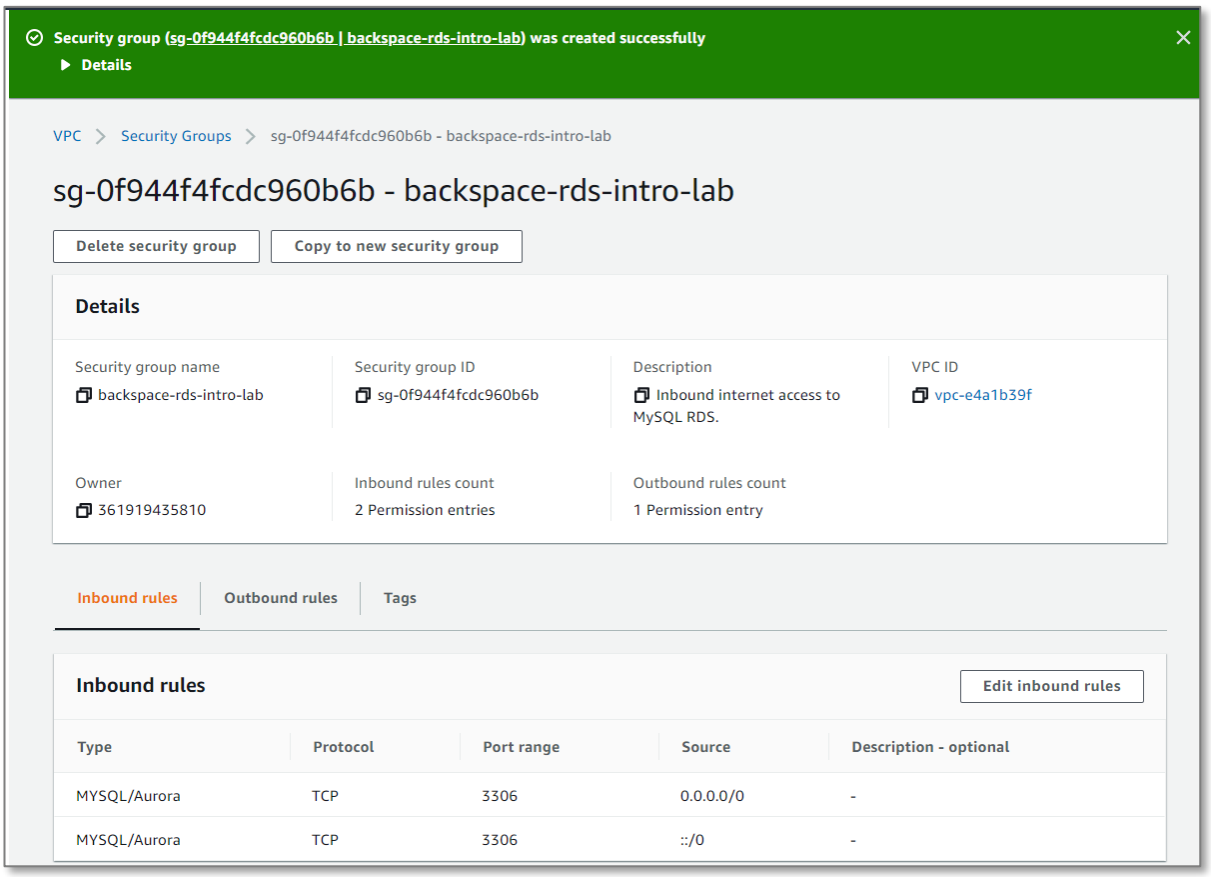
Click *Add rule* for Inbound rules

Select type *MySQL/Aurora*

Select source *Anywhere*

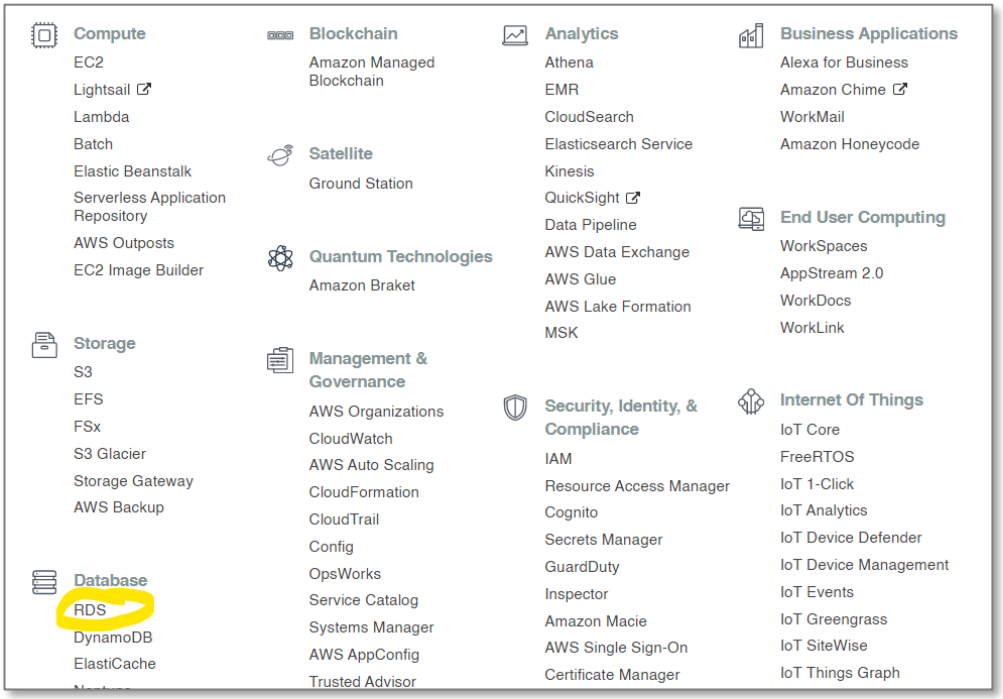
Click *Create security group*





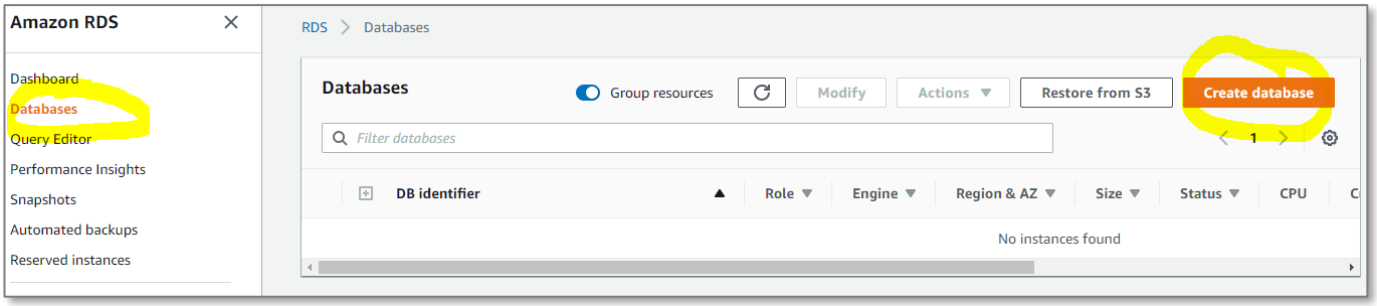
Creating an RDS Database

From the AWS console select *RDS* from the Database services.

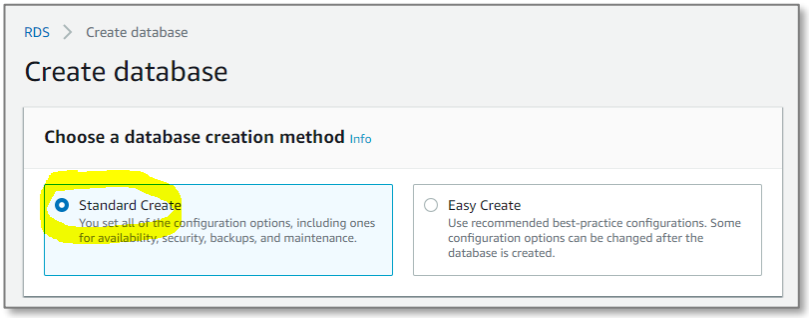


Select ‘Databases”

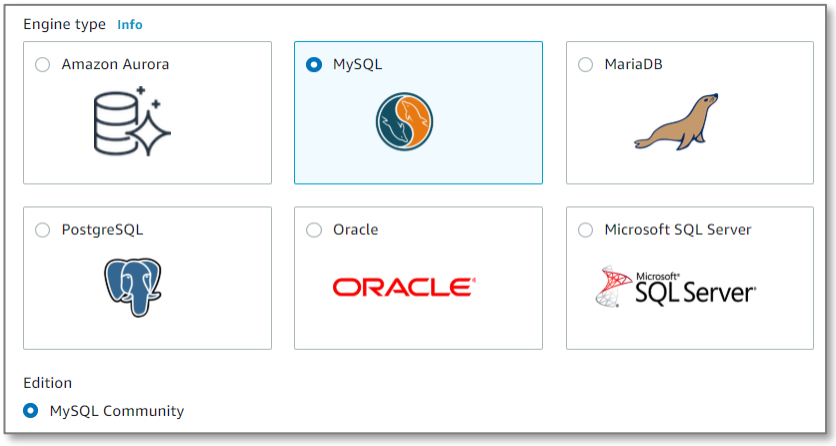
Select ‘Create database”



Select *Standard Create*



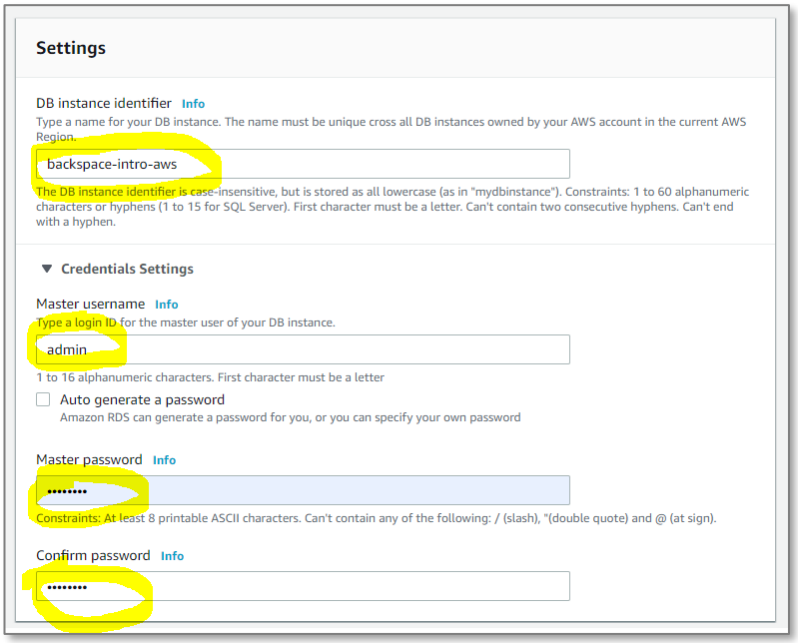
Select *MySQL*



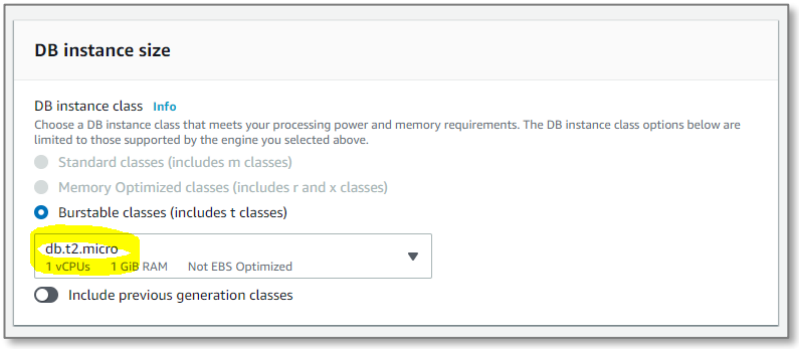
Select *Free Tier*

In the *Settings* section give your instance a name/identifier.

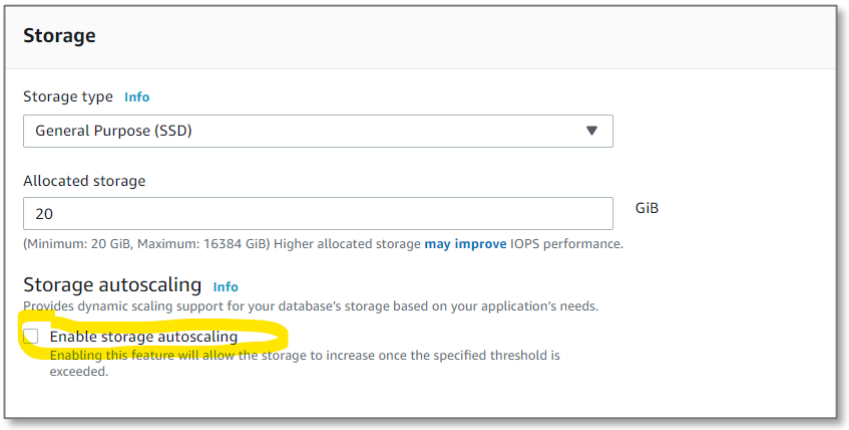
Fill in a master username and password (remember this we will need it later)



In the *DB Instance size* section select db.t2.micro instance class



Uncheck *Enable storage autoscaling*



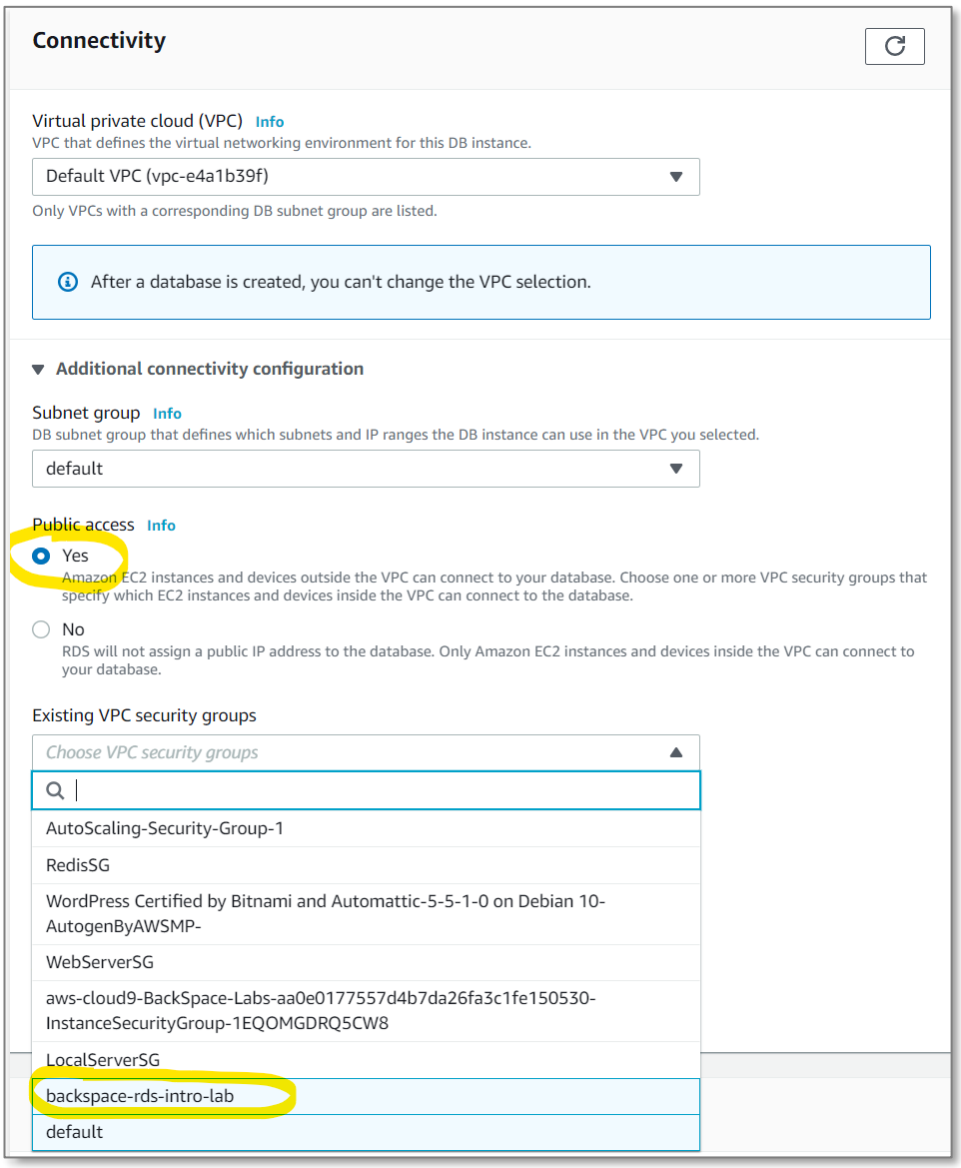
Scroll down to *Connectivity*

Expand *Additional connectivity configuration*

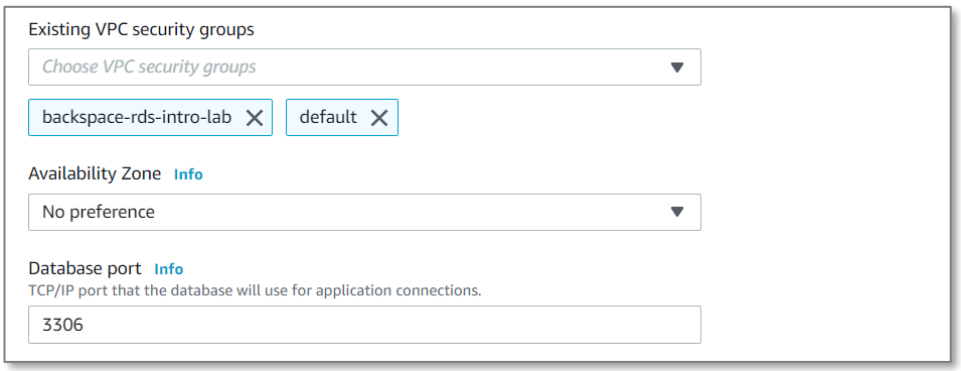
Select *yes* for *publicly accessible* (we will look at security later in the course)

Select *Create new for VPC security group*

Select the *backspace-rds-intro-lab* security group we created previously (click outside the list after selecting to close the list)



Click outside the list to add the security group. You should then see the security group added.

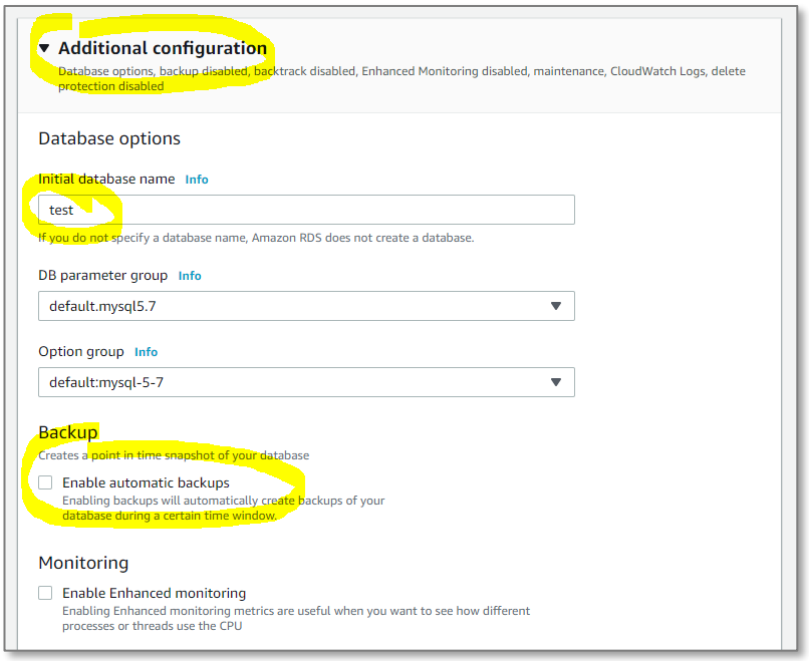


Scroll down and expand *Additional configuration*

Enter a database name.

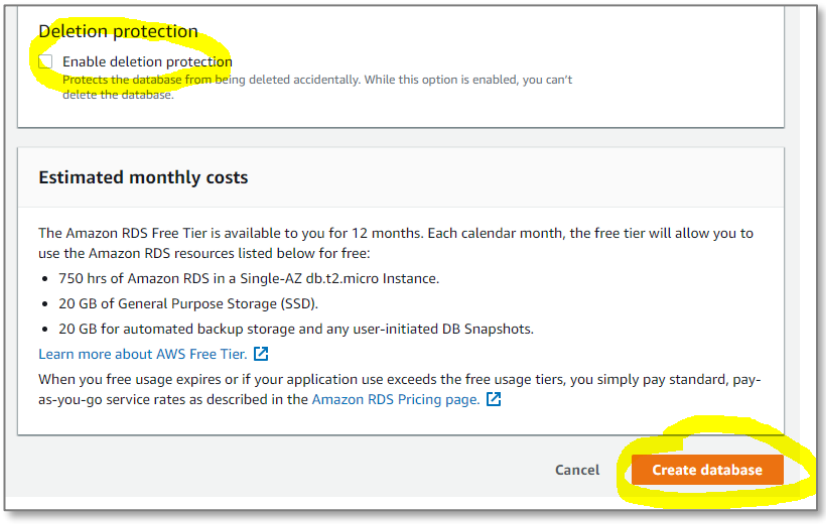
Uncheck *Enable automatic backups*

Leave all other options default.

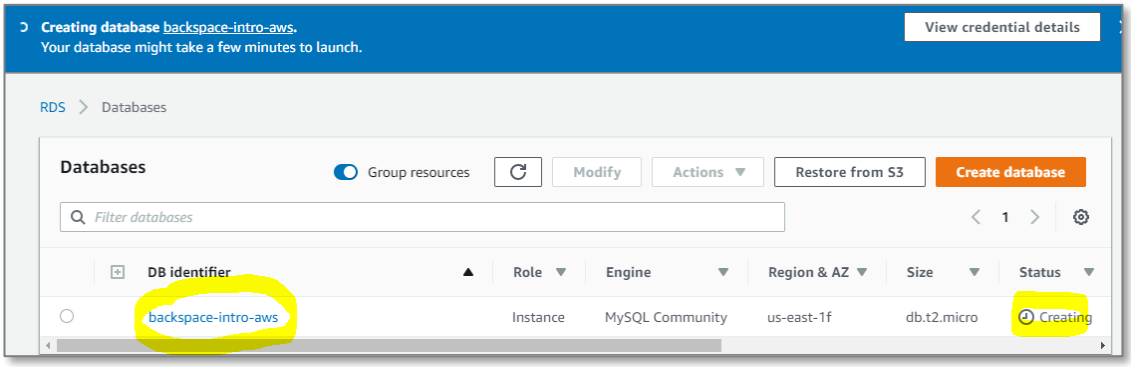


Uncheck *Enable deletion protection* (we want to delete it easily when finished)

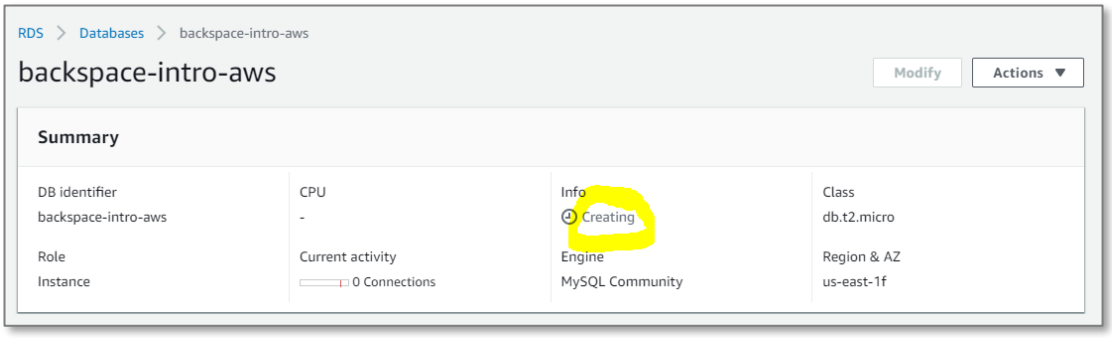
Click 'Create database"



Click on the database details link



Your instance will show status 'creating".



Connecting to your RDS Instance

To connect to your MySQL Database you will need to download and install the MySQL Workbench.

Instructions for Windows:

https://dev.mysql.com/doc/workbench/en/wb-installing-windows.html

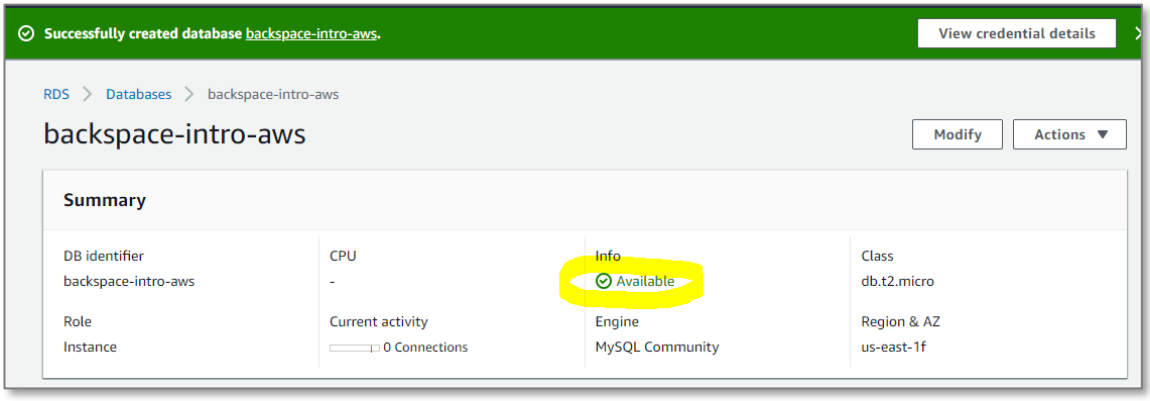
Instructions for Mac:

https://dev.mysql.com/doc/workbench/en/wb-installing-mac.html

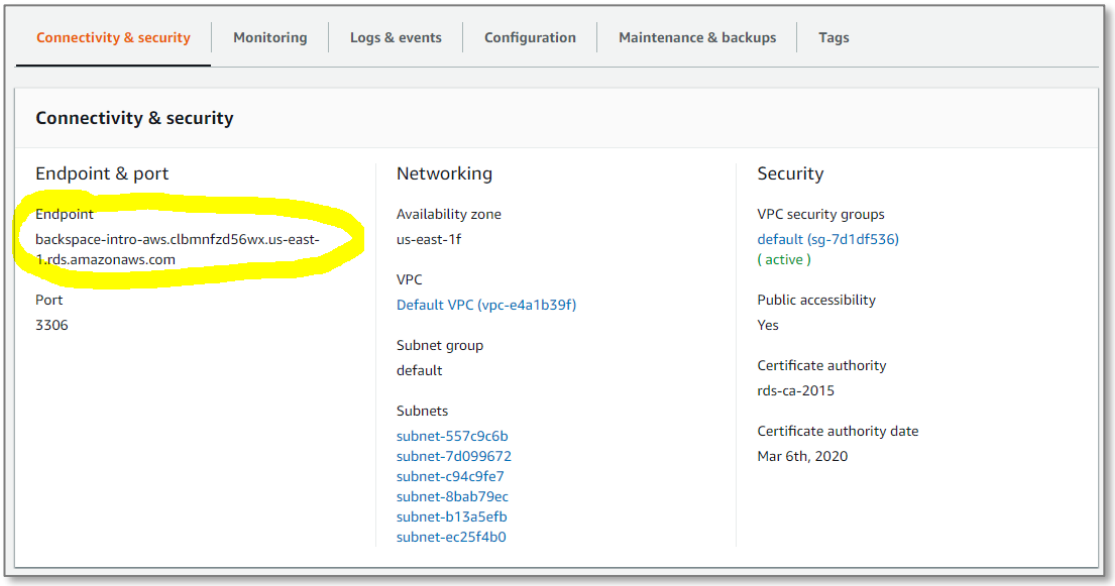
Instructions for Linux:

https://dev.mysql.com/doc/workbench/en/wb-installing-linux.html

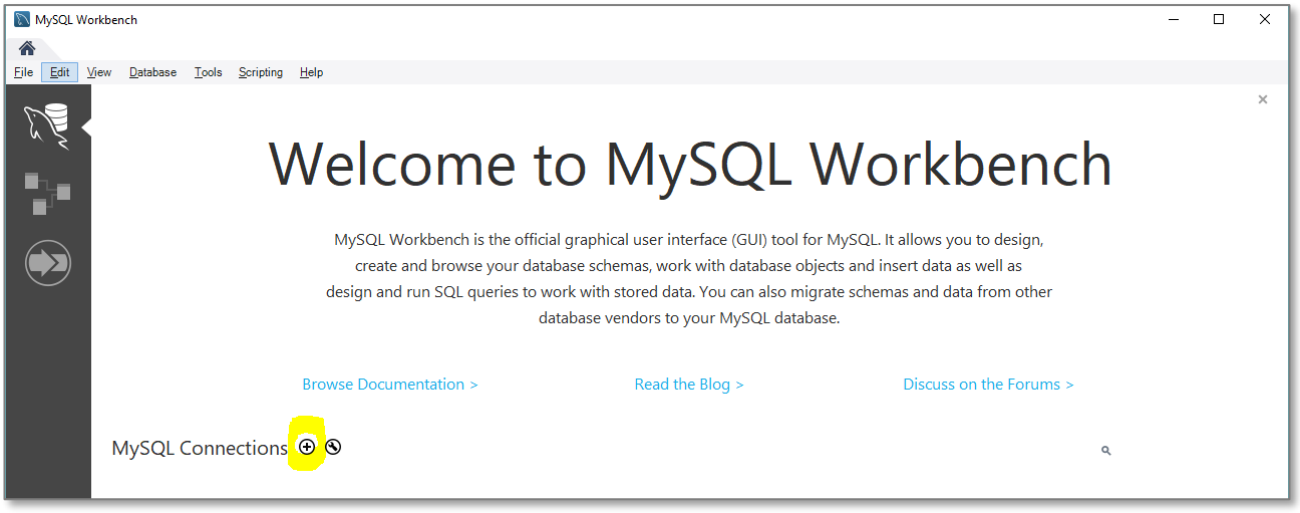
Wait for your instance status to be 'available"



Scroll down and copy the database server endpoint



Open the MySQL Workbench application click to add a new connection



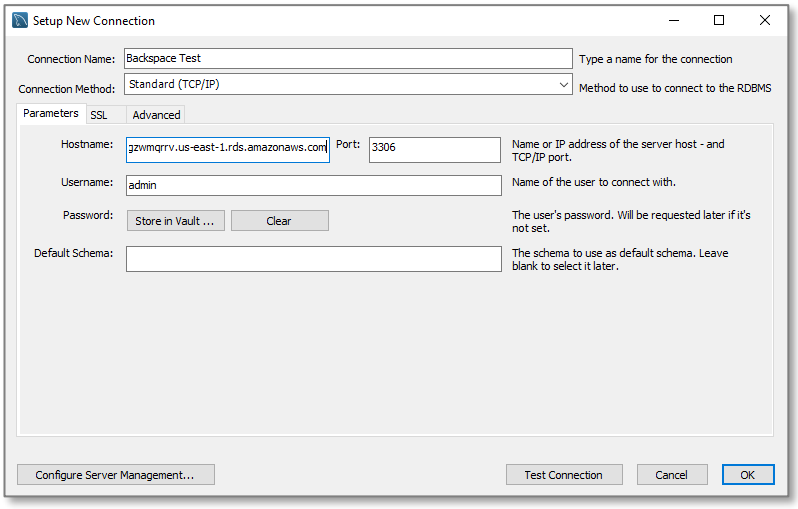
Give the connection a name.

The Hostname will be the RDS server endpoint.

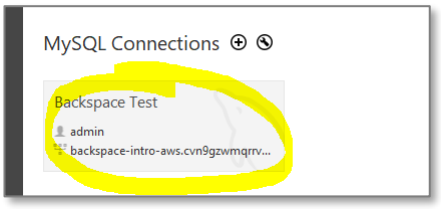
The port will be 3306.

The Username will be the master username we created in RDS (i.e. admin)

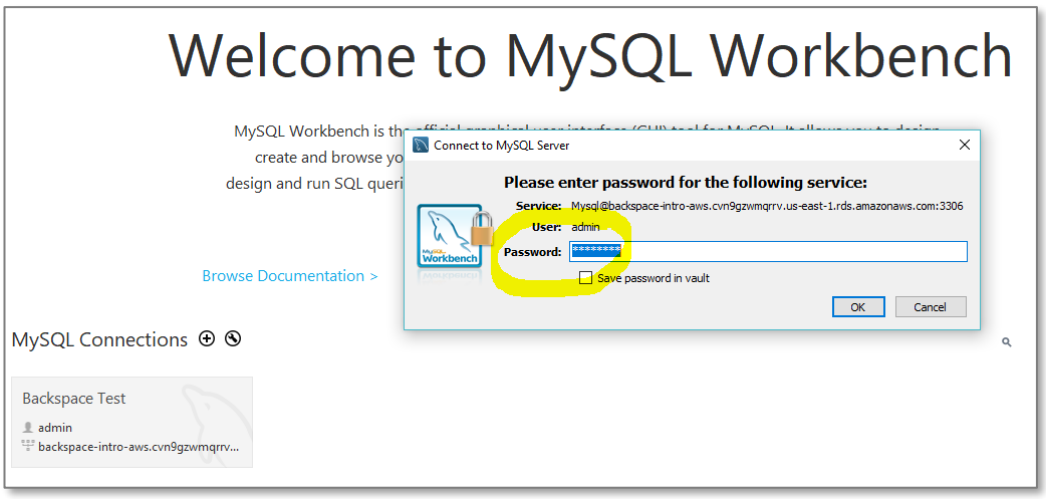
Click OK



Click on the Connection

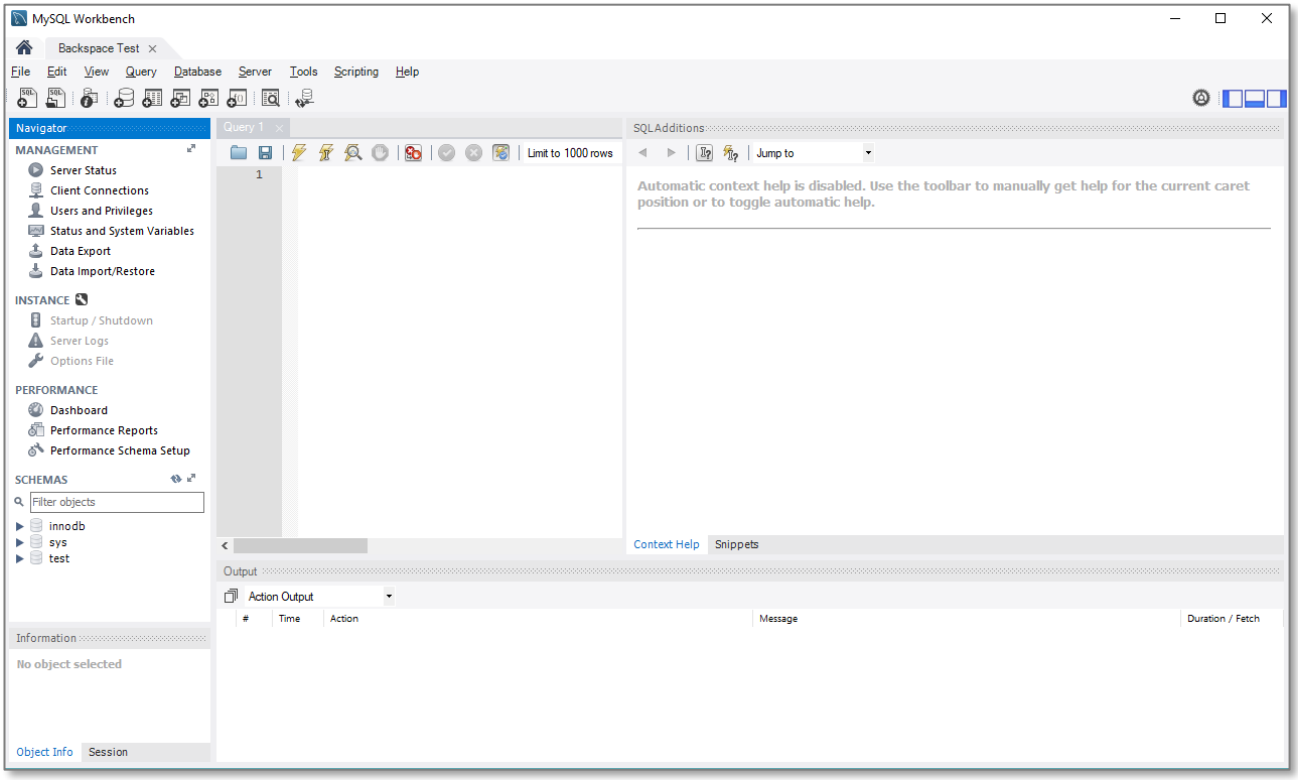


Enter the password you created in RDS for your master username

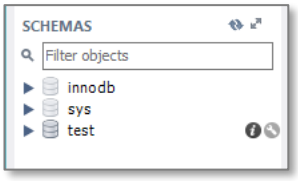


You will soon be connected to your database server

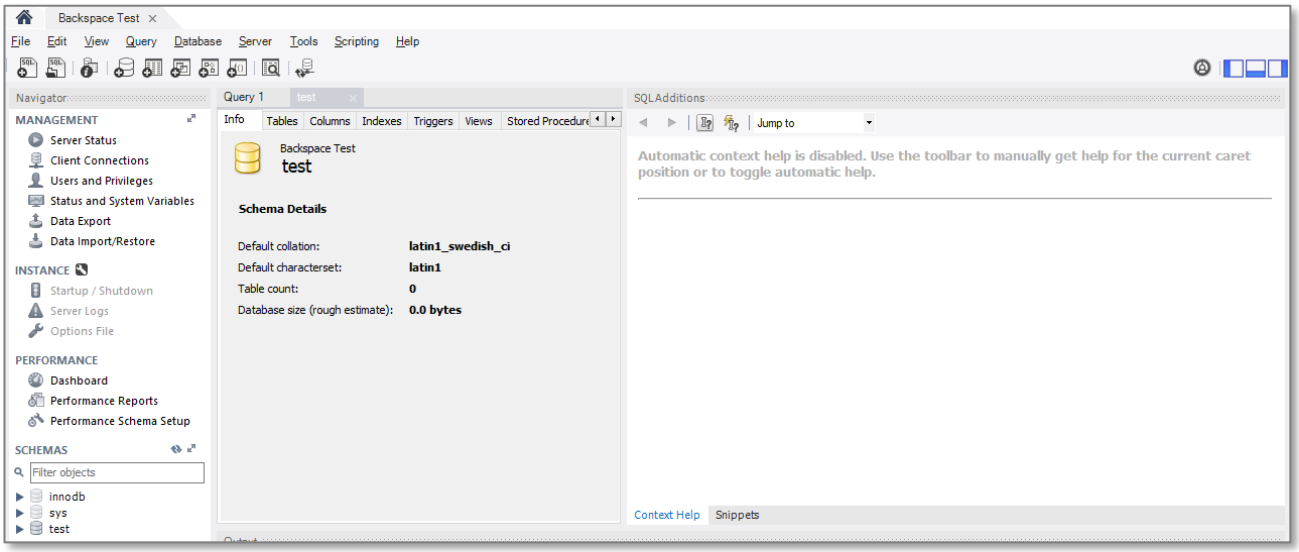
If you cannot connect then please see the 'Troubleshooting Connection Issues" below.



Hover over the 'test" database under 'SCHEMAS" and click the information icon to get information about the database that was created by us in RDS.



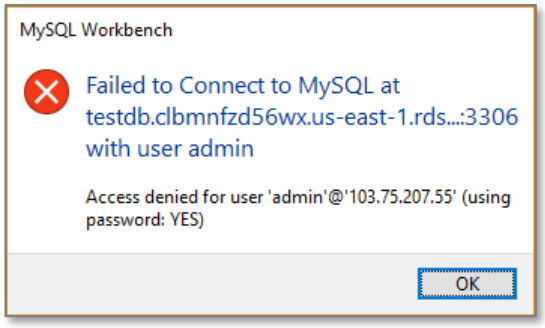
You then get an information screen for the database.



Troubleshooting Connection Issues

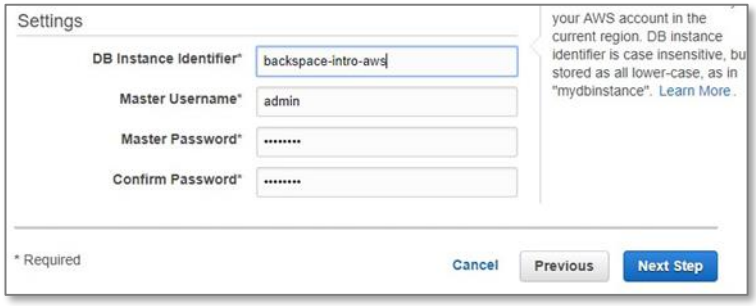
If you are getting connection errors then check the following:

Wrong Username / Password

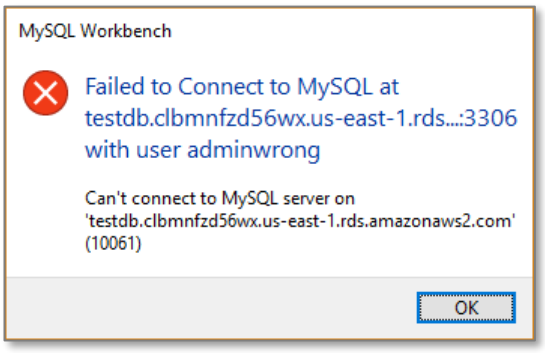


Make sure you use the correct username and password.

The username and password must be the one created when the RDS instance was created.



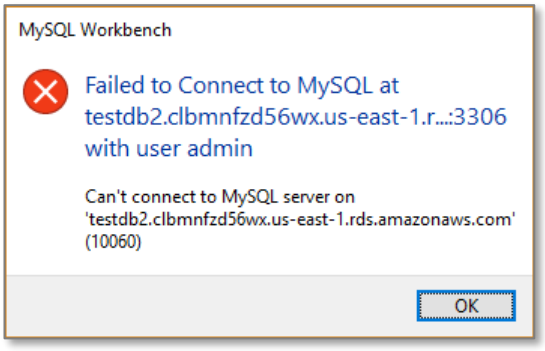
Bad Connection String



This error means nothing exists at the endpoint. Check the connection endpoint and port are correct.

The hostname will be the RDS Instance Connection Endpoint without :3306 on the end.

No Connection



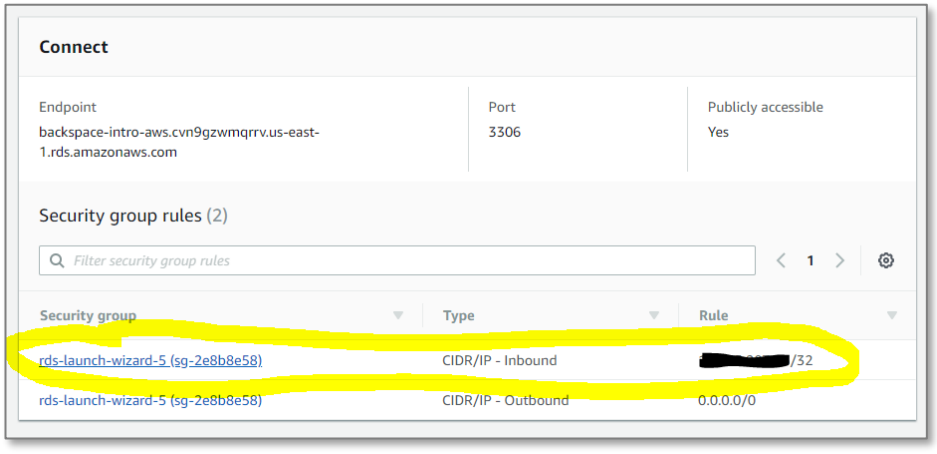
This error means your server exists but you are unable to connect to it. This can be caused by:

- You have not selected 'public' when creating instance and the security group inbound rules will be incorrect. This will block traffic to your instance. See *Security Group Inbound Rules* below.
- You have a dynamic IP address or multiple IP addresses passing through a load balancer. See *Security Group Inbound Rules* below.
- Firewall at your end is blocking access to port 3306. See *Client-side Firewall* below.

Security Group Inbound Rules

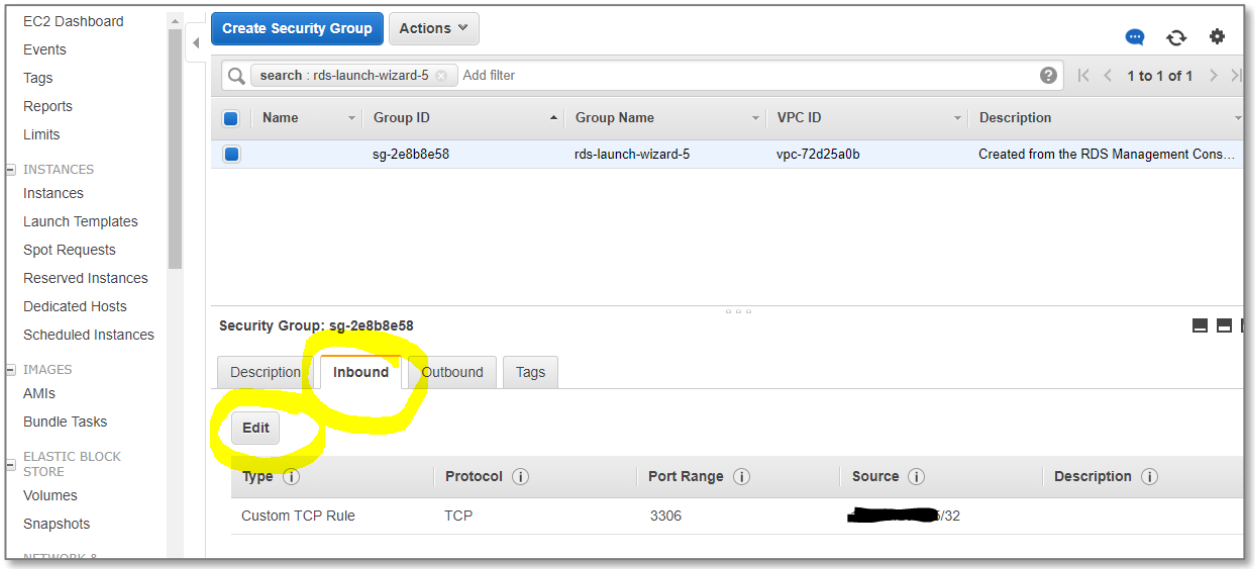
If you did not select *yes* for *publicly accessible* as detailed, your security group will block remote access.
The security group may have an inbound rule for your IP address. If you are using a dynamic IP address or you are connecting from different networks then this will need to be changed to "anywhere" for the lab.

Click the security group

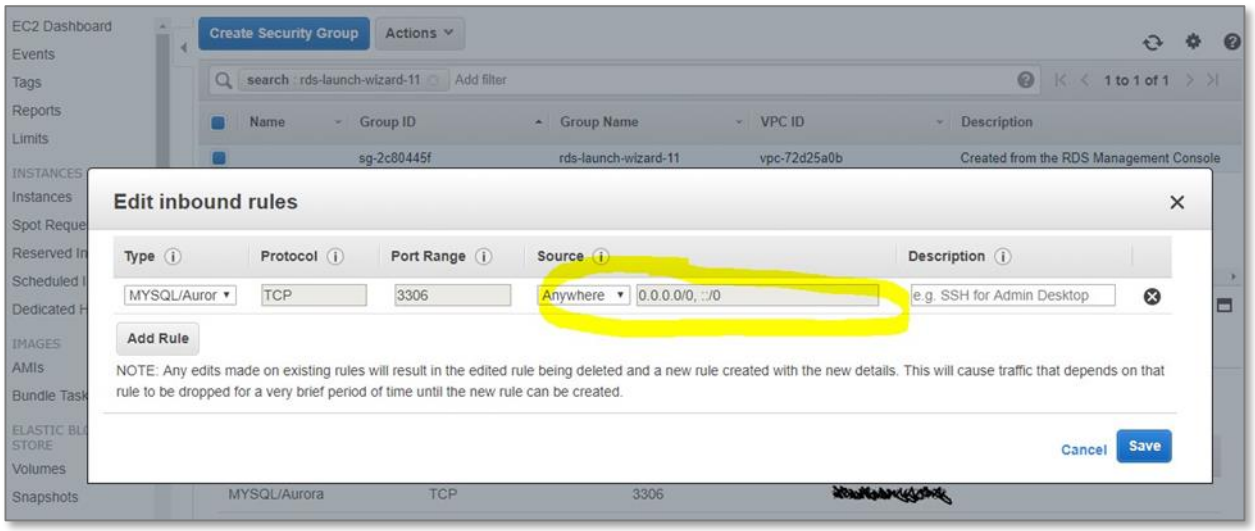


You will be taken to the EC2 console

Select the “Inbound” tab
Click “Edit”



Change inbound rule to “Anywhere” 0.0.0.0/0, ::/0



Client-side Firewall

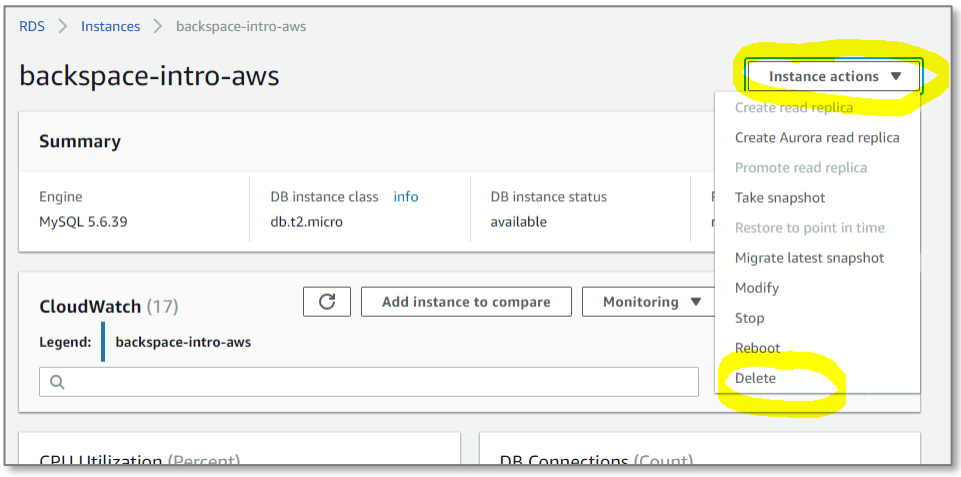
If you are still having problems connecting, a firewall at your end may be preventing access on port 3306. This is common if you are connecting from your work environment as port 3306 traffic may be blocked.

Clean Up

To avoid incurring charges from AWS we will terminate the instance.

Go back to the RDS console.

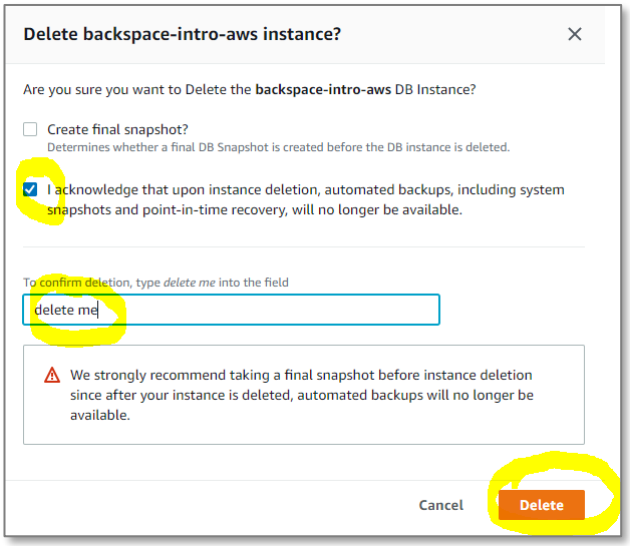
Click 'Instance Actions", 'Delete" to terminate the instance



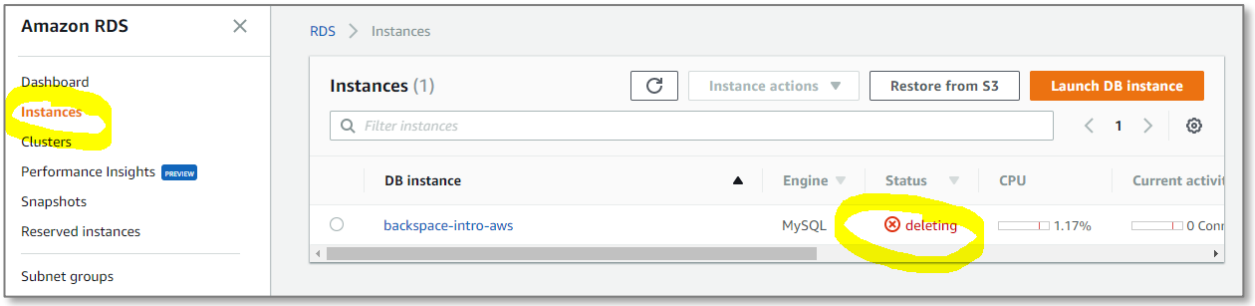
Select 'No" for 'Create final snapshot"

Check 'I acknowledge that upon instance deletion, automated backups, including system snapshots and point-in-time recovery, will no longer be available."

Click 'Delete"



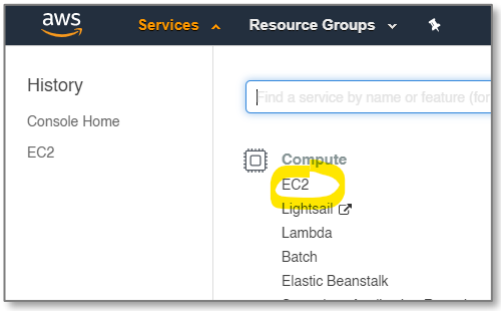
Click on 'Instances" to see it status as 'deleting"



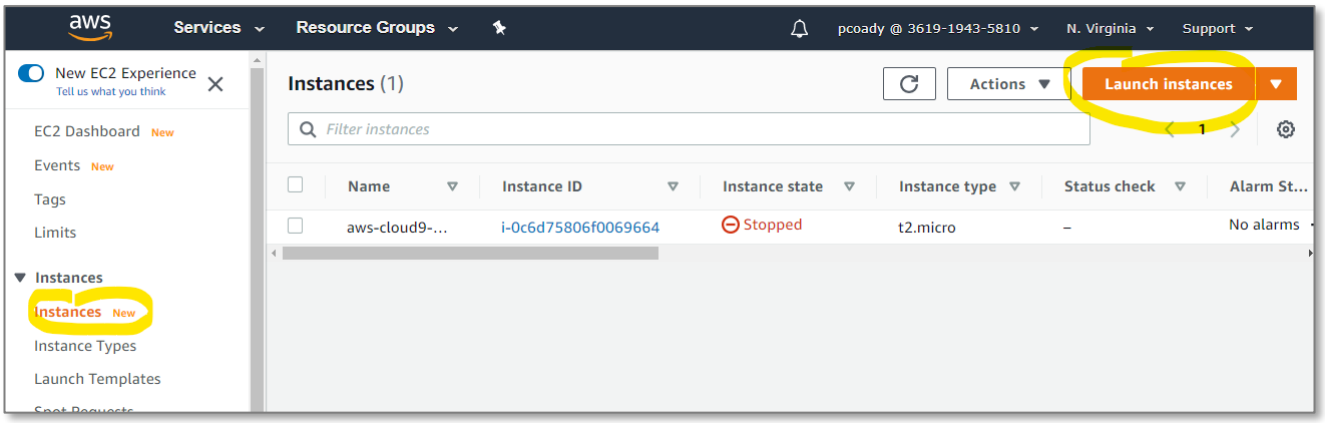
Creating a Web Server with EC2

In this section, we will launch a publicly accessible WordPress application on Amazon EC2.

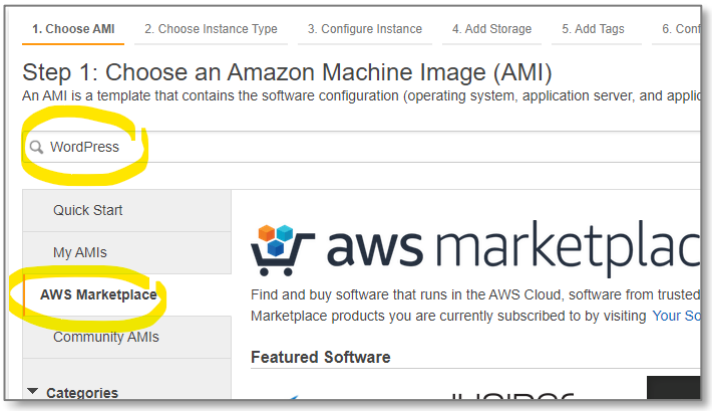
From the AWS console select EC2 from the Compute services.



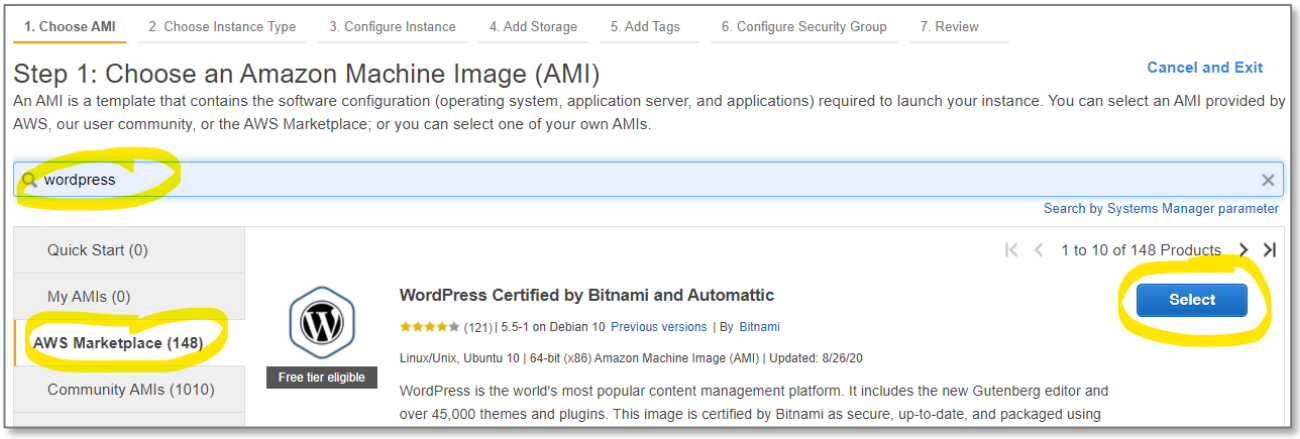
Select Instances - Launch Instances



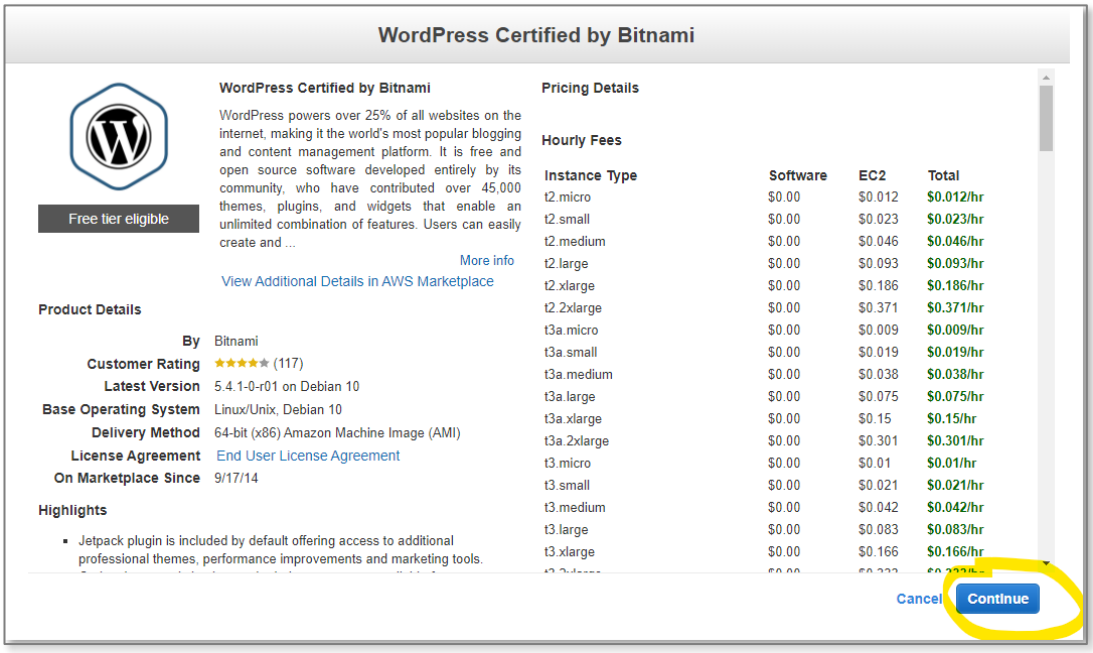
Select the AWS Marketplace and search for WordPress



Select the Bitnami AMI

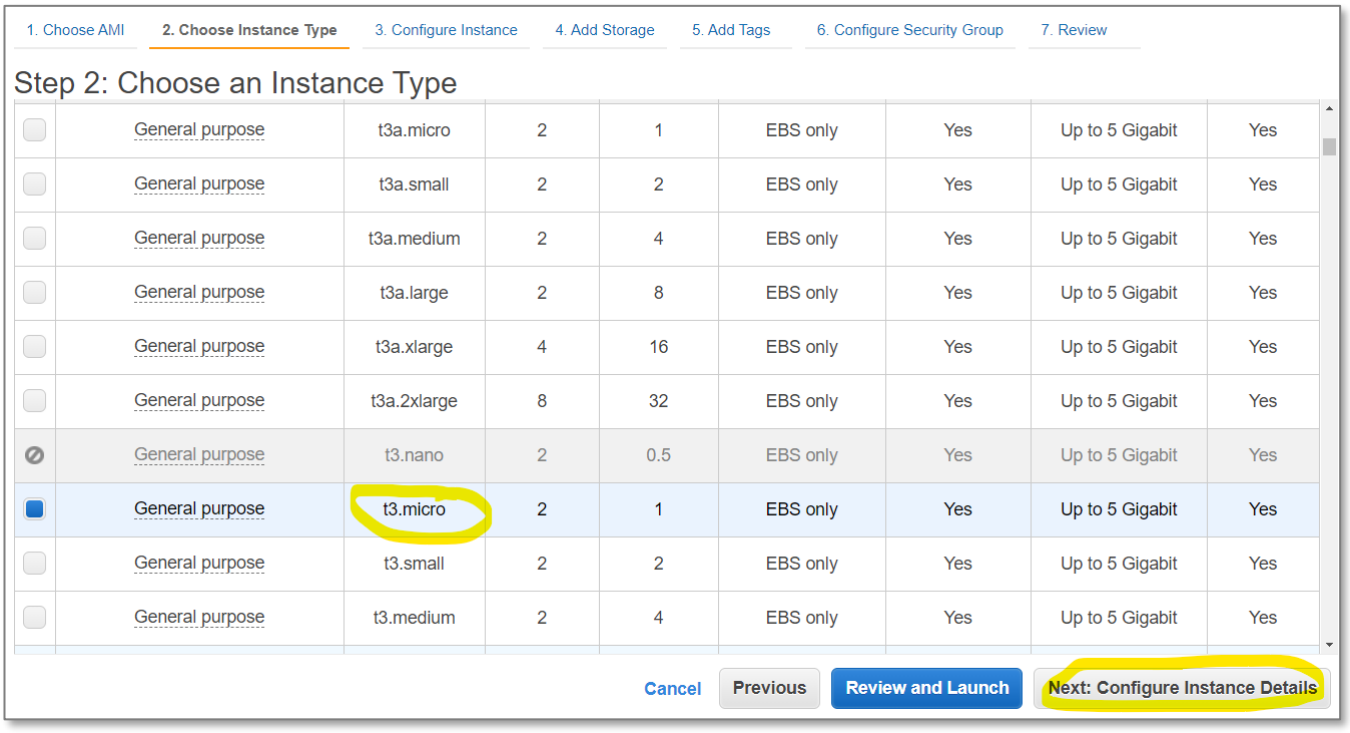


Click Continue



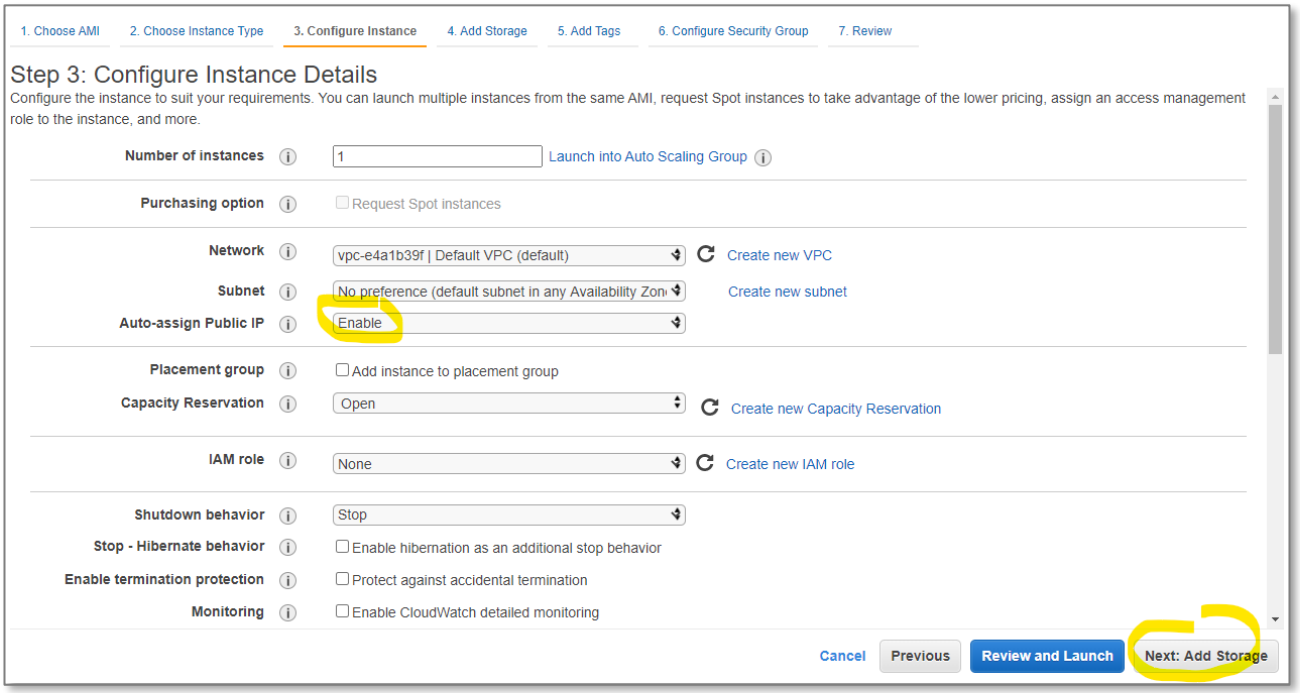
Choose the **t3 Micro** instance.

Click Next: Configure Instance Details

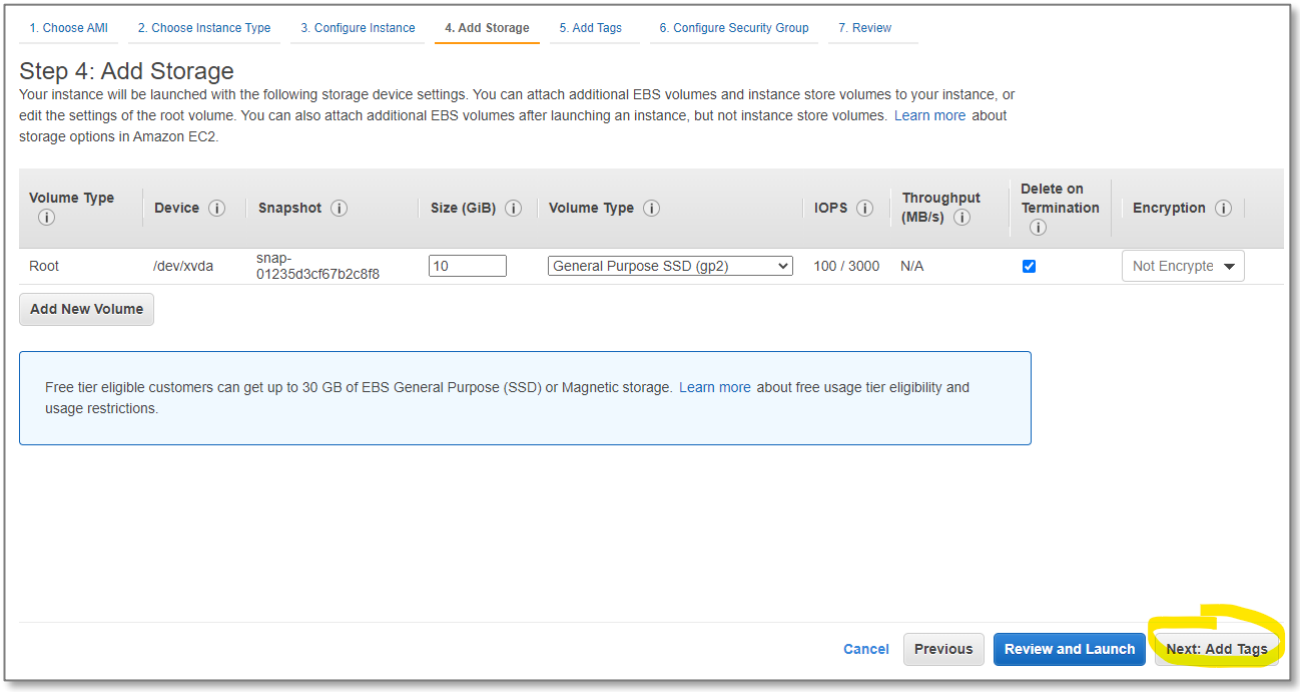


Select enable for Auto-assign Public IP

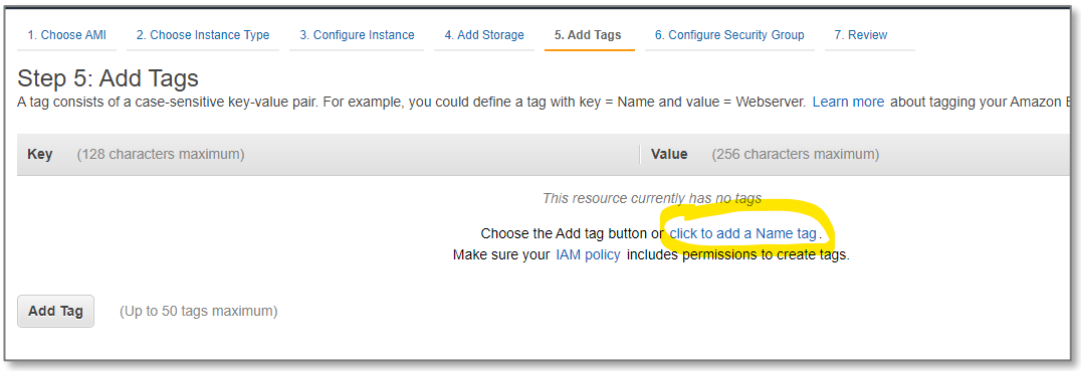
Click Next: Add Storage



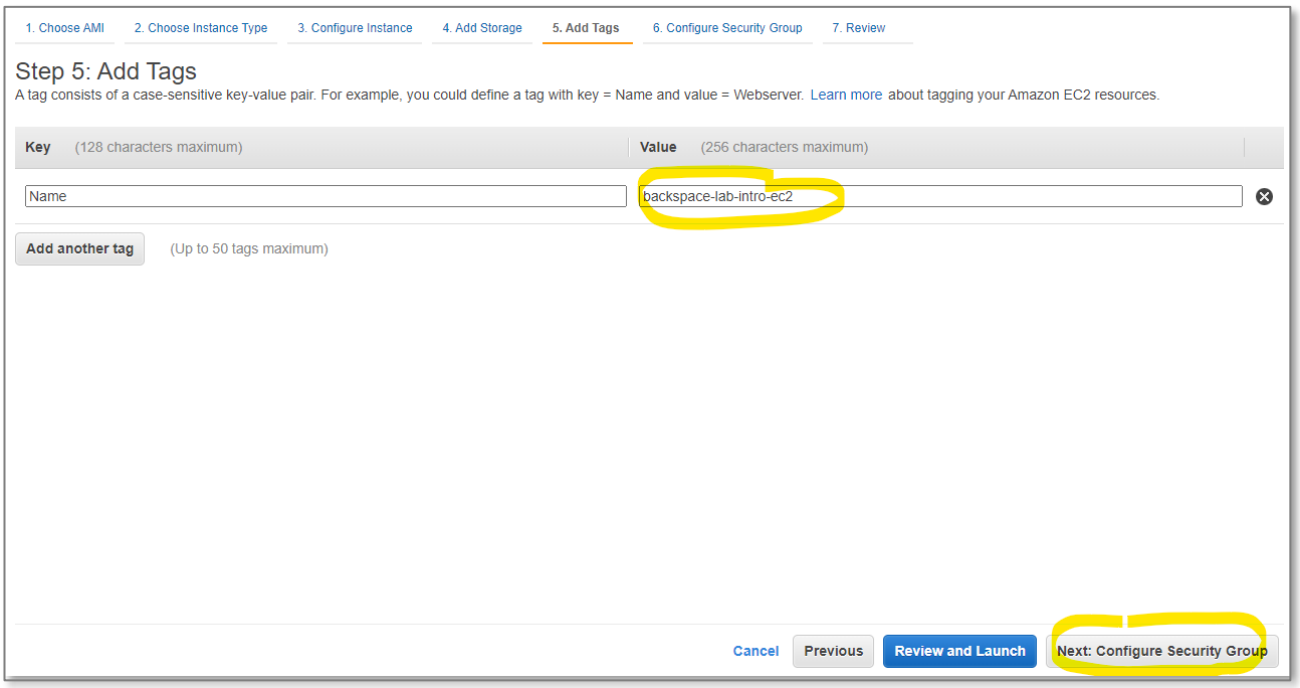
Click Next: Add Tags



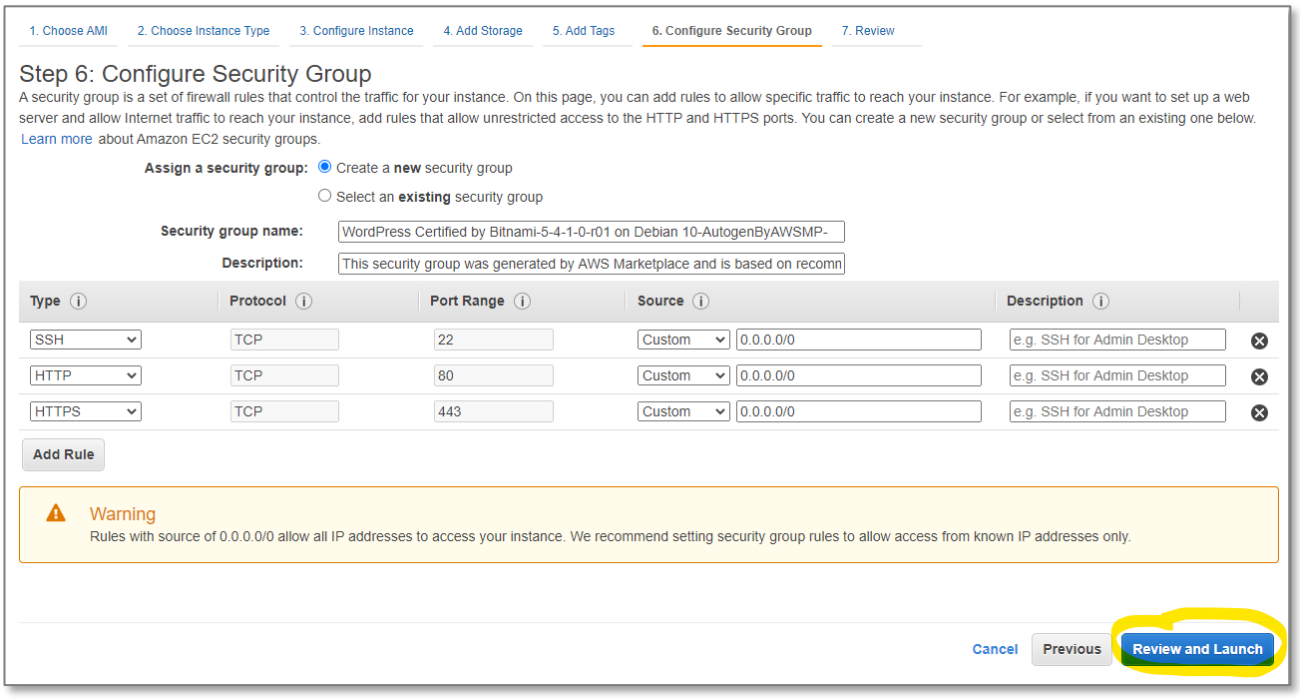
Click click to add a Name tag



Give it a name and click Next: Configure Security Group



Click Review and Launch

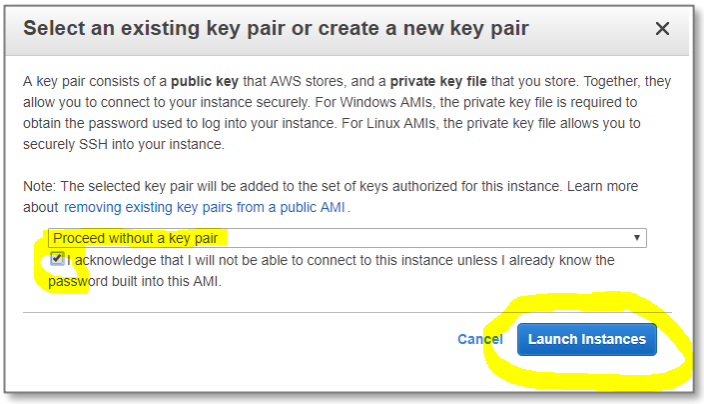


Click Launch

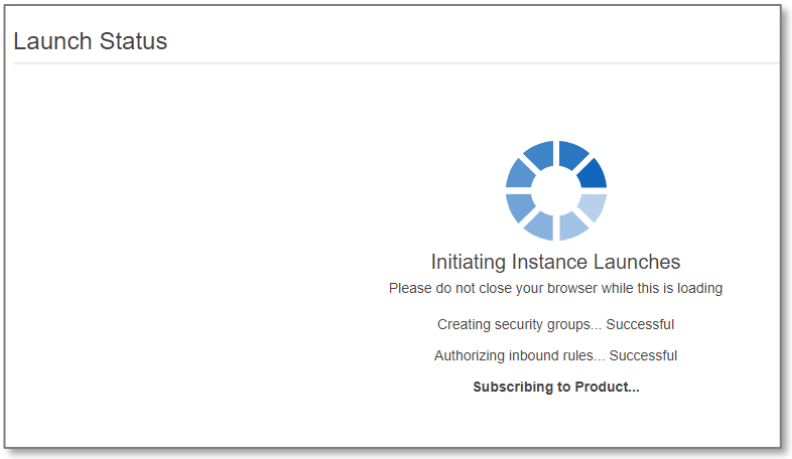
Select “Proceed without a key pair”

Select “I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI.”

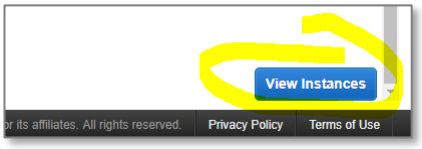
Click “Launch Instances”



Wait for launch to initiate



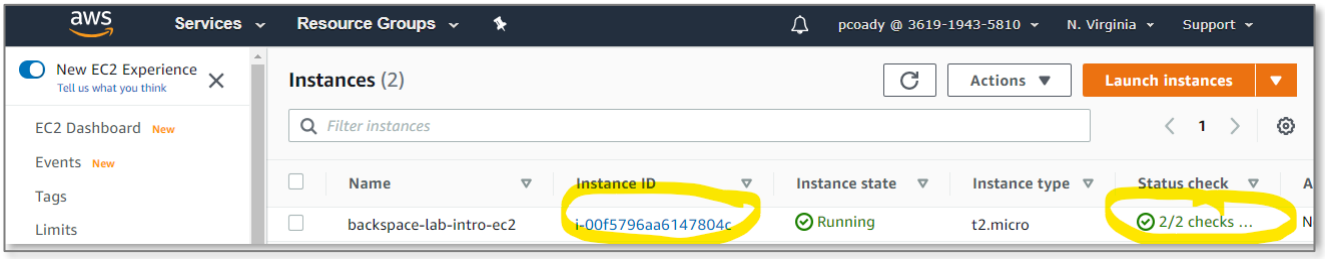
When the launch process has started scroll to the bottom of the page and click “View Instances”



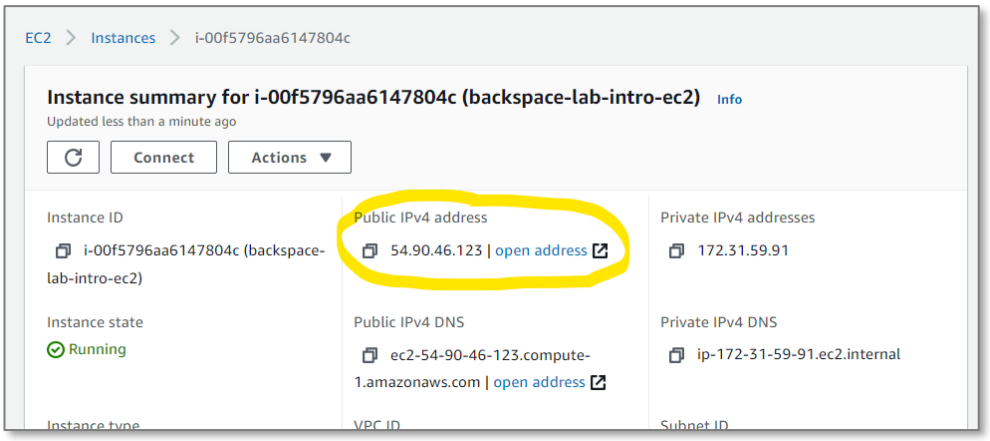
After a few minutes, the status of the instance will change to running and status checks will be completed (you will need to refresh the screen to see any changes).

Viewing your web server

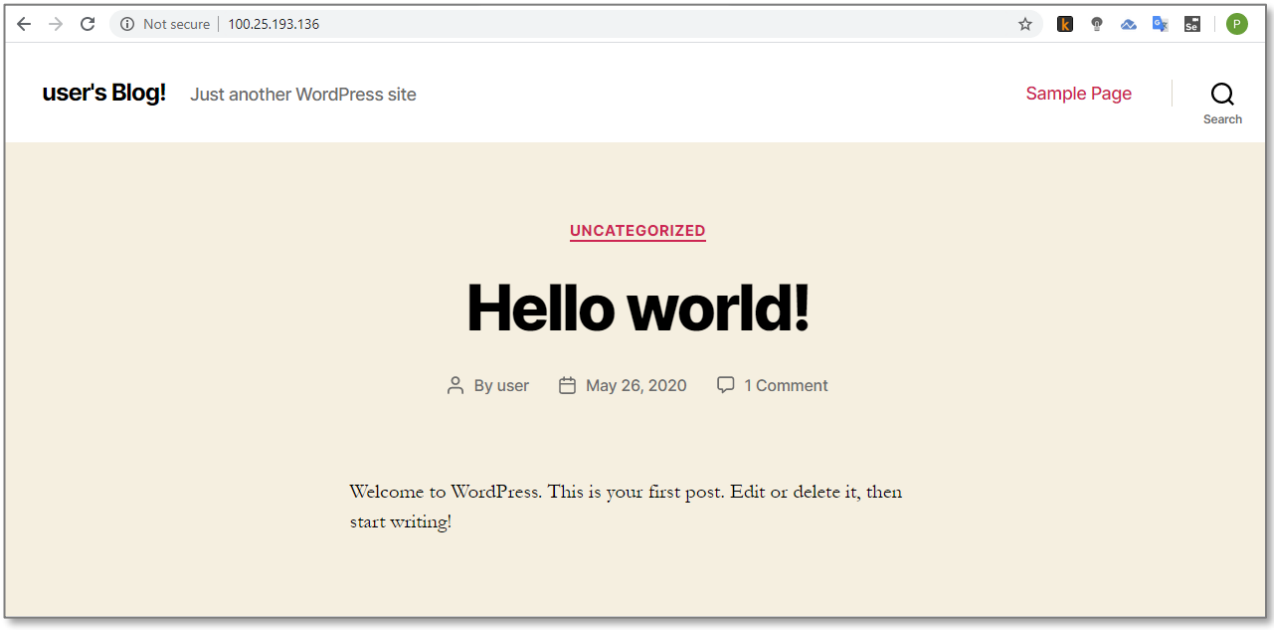
After the Status checks have completed click on the Instance ID to select the instance.



Open the public IP address of your web server.



Navigate to the IP address in your browser.



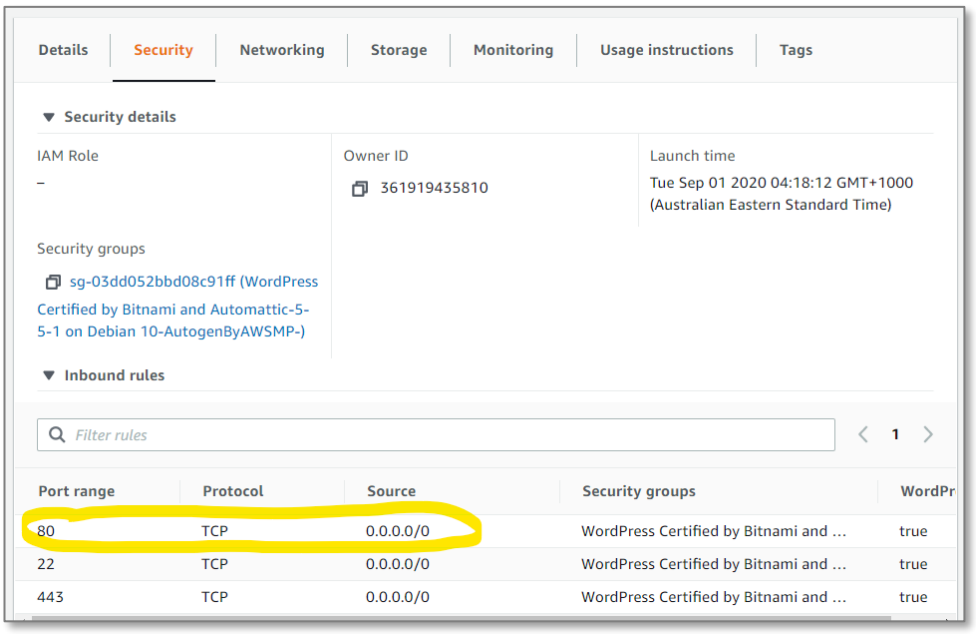
Troubleshooting viewing your WordPress application

If you cannot view your website it probably hasn't finished the launch process completely.

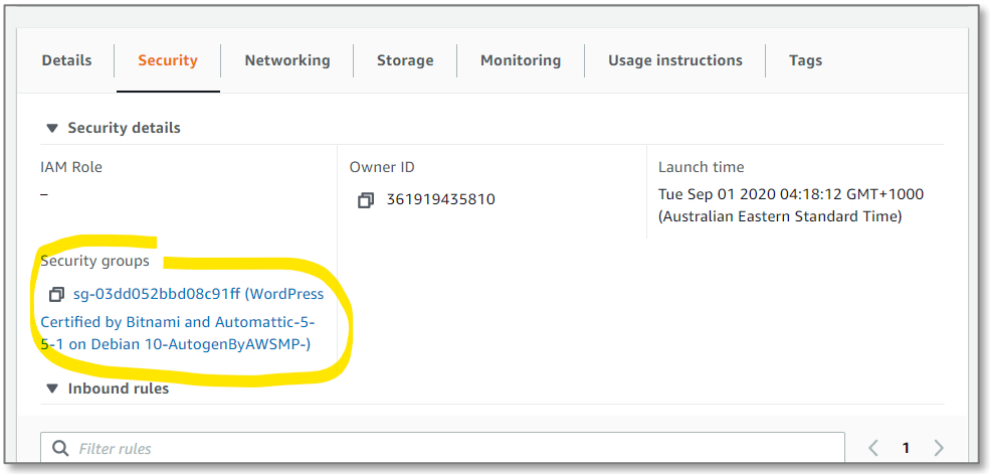
If after quite some time you still can't view your website, it may be that your security group does not allow inbound requests on port 80 (http). The inbound rules should include:

80 tcp 0.0.0.0/0

Scroll down and click on the Security tab

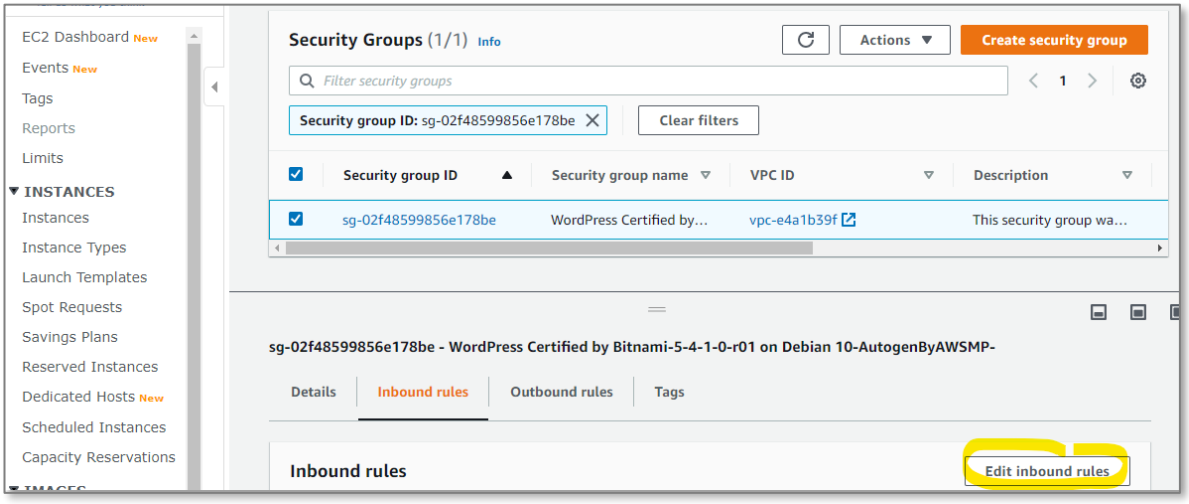


If the rule is not present you will need to add it by clicking on the security group to open it:



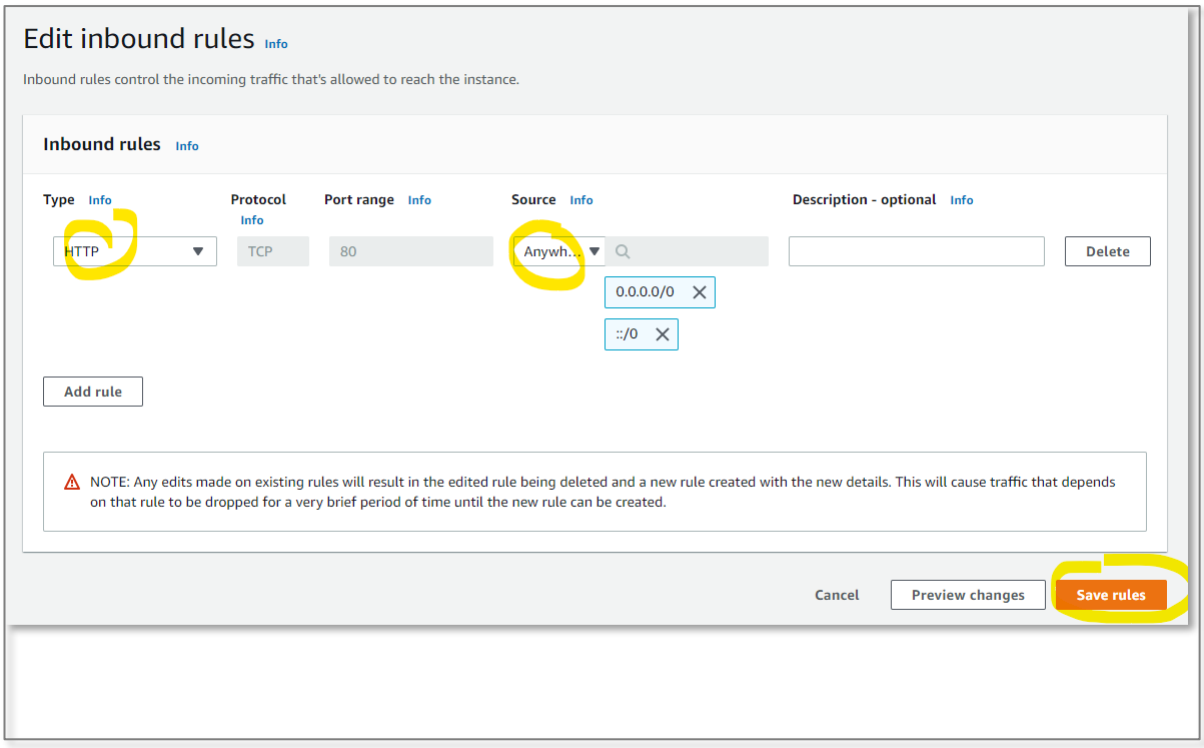
Click on the Inbound rules tab

Click on Edit



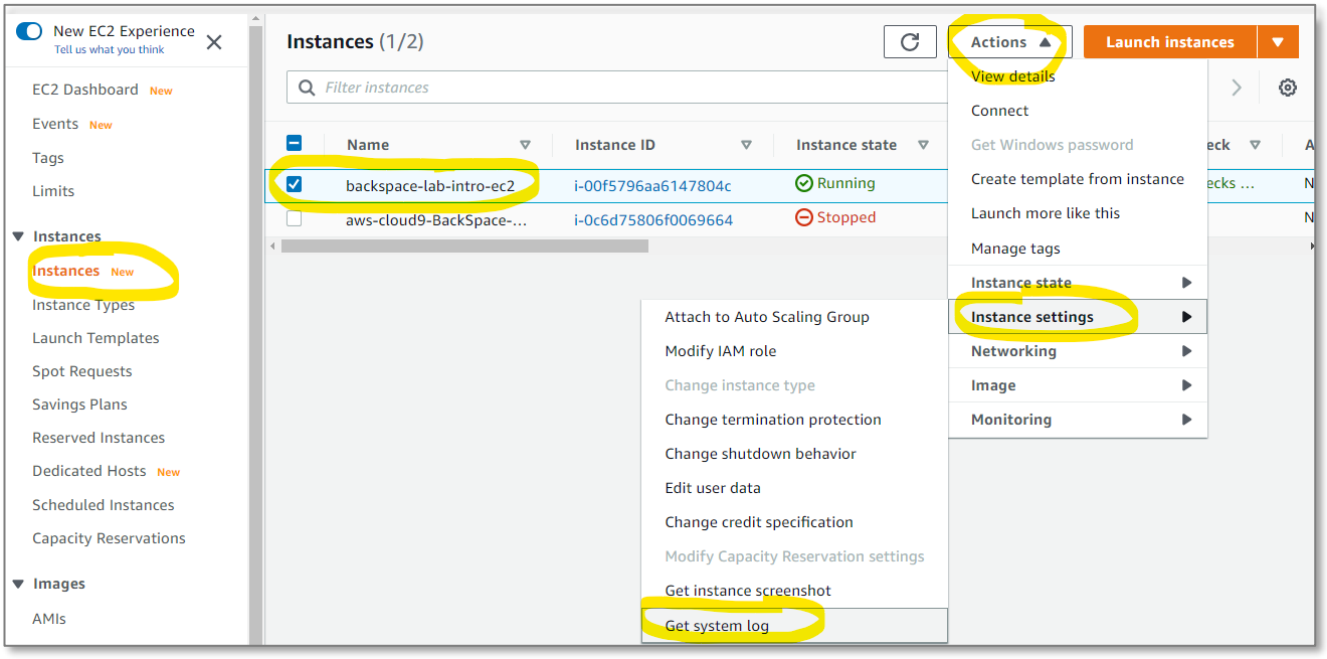
Add a rule for HTTP and Anywhere

Click Save rules

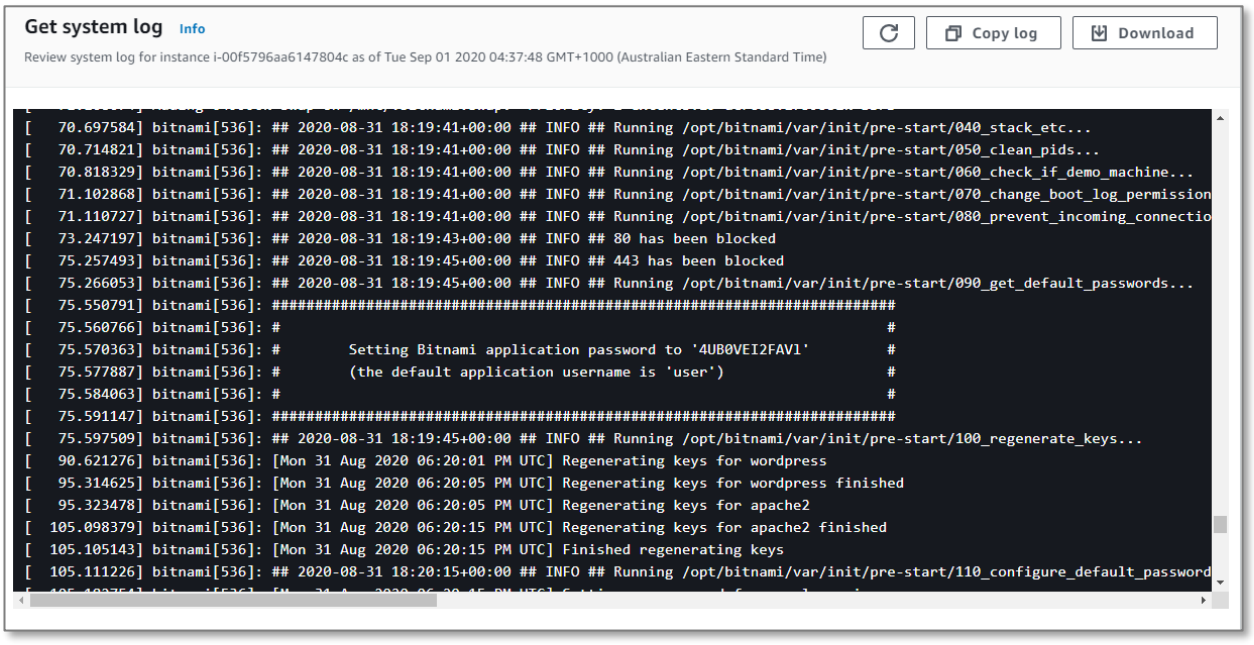


Finding the Username and Password for your WordPress application

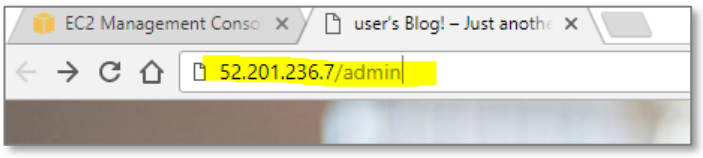
Go back to the EC2 console and select “Instance Settings”, “Get System Log”. Do not click on connect.



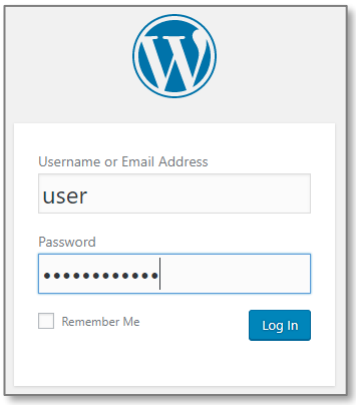
Scroll up until you find the log entry for the application username and password and copy it.



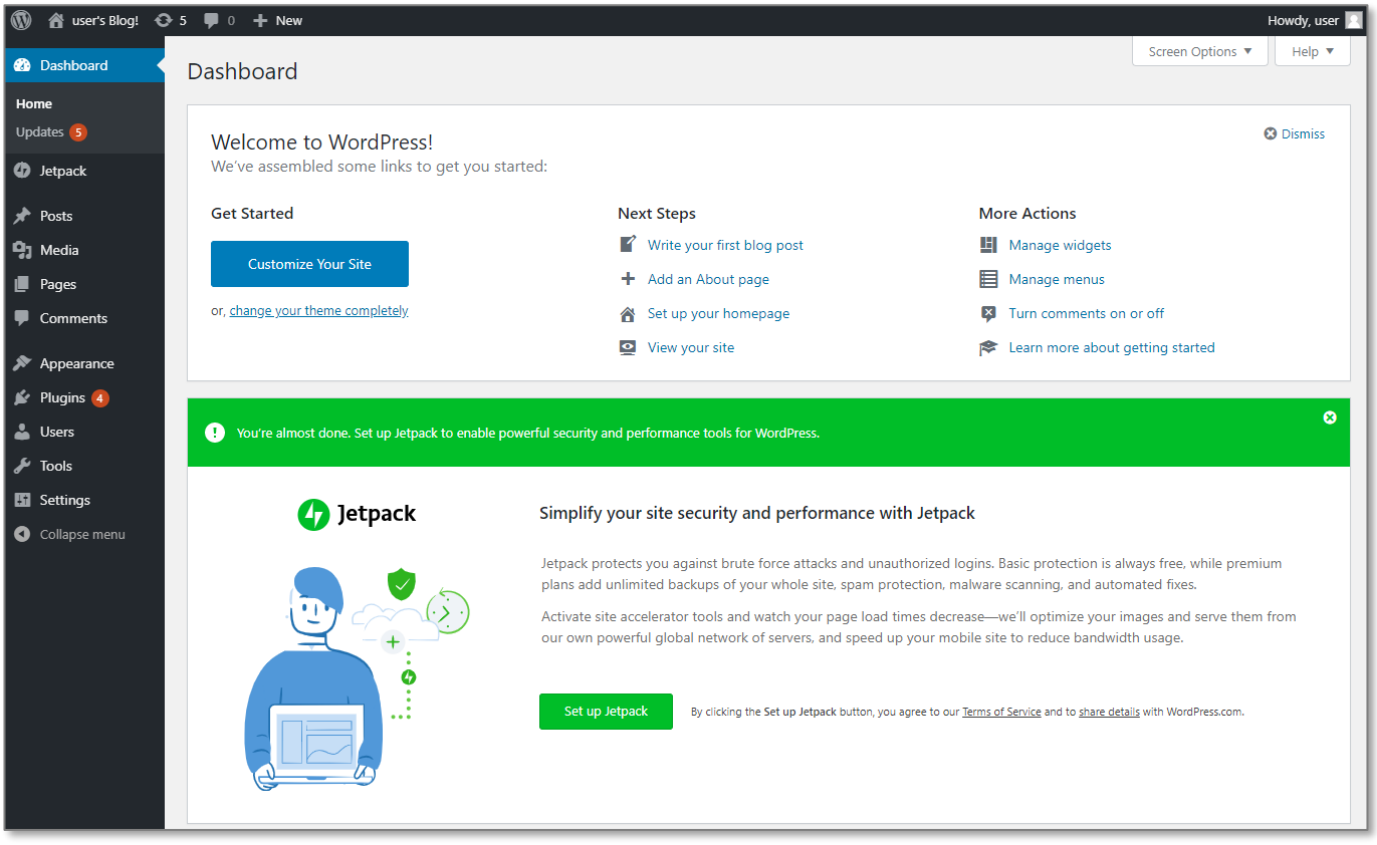
Go to the admin subdirectory of your website in your browser



Enter Username “user” and paste in the password

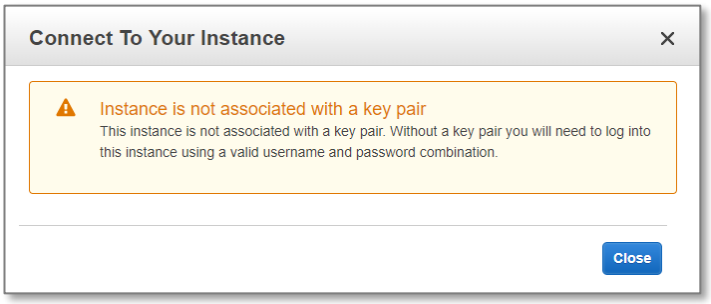


You will now be in the admin section of your WordPress application



Troubleshooting logging in to the WordPress application

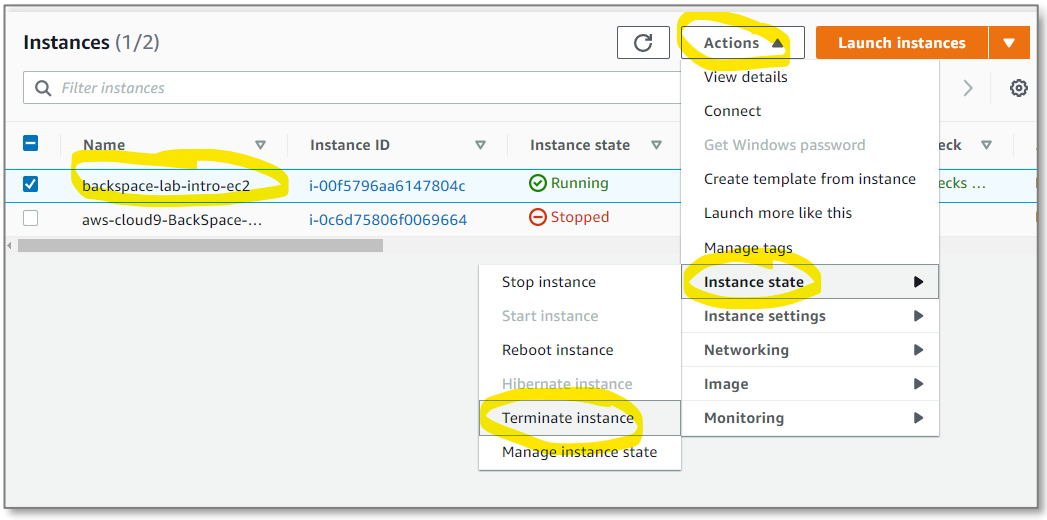
If you get the following message:



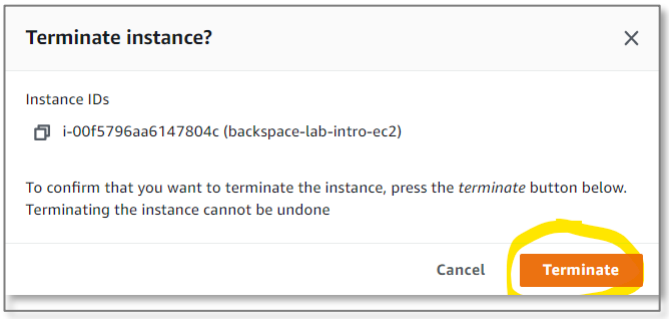
You have tried to connect to the Linux operating system by clicking on “Connect”. Do not click on connect, select “Actions – “Instance settings” - “Get System Log” as detailed previously.

Clean up

Select “Actions”, “Instance State”, “Terminate”.



Make sure you terminate the instance so that you are not billed for it any more.

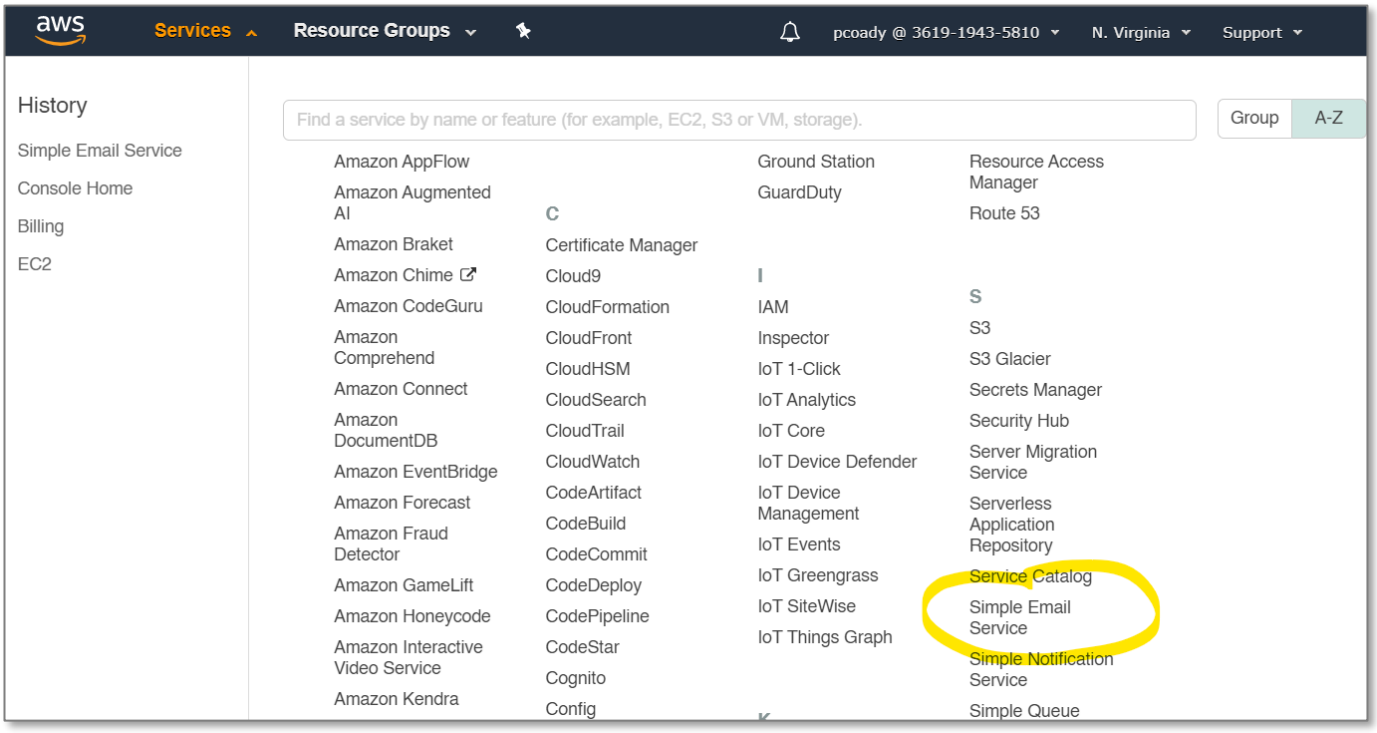


Sending Emails with Amazon SES

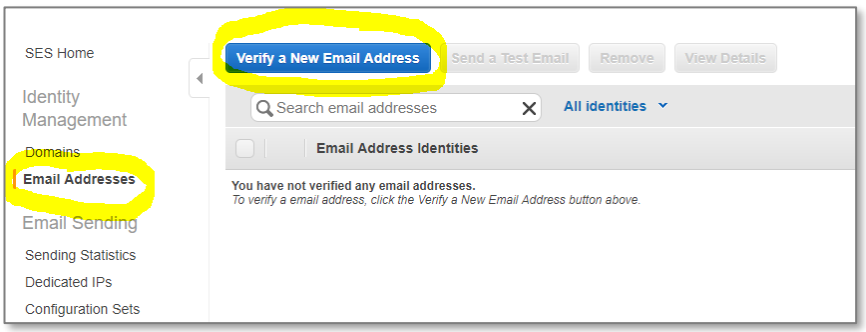
In this section, we will use the Simple Email Service to send an email.

From the AWS console select *Simple Email Service*

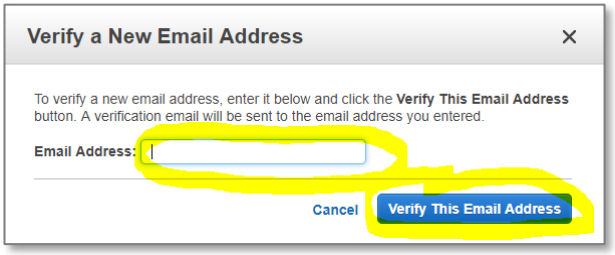
Click on 'Email addresses"



Click on 'Verify a New Email Address"

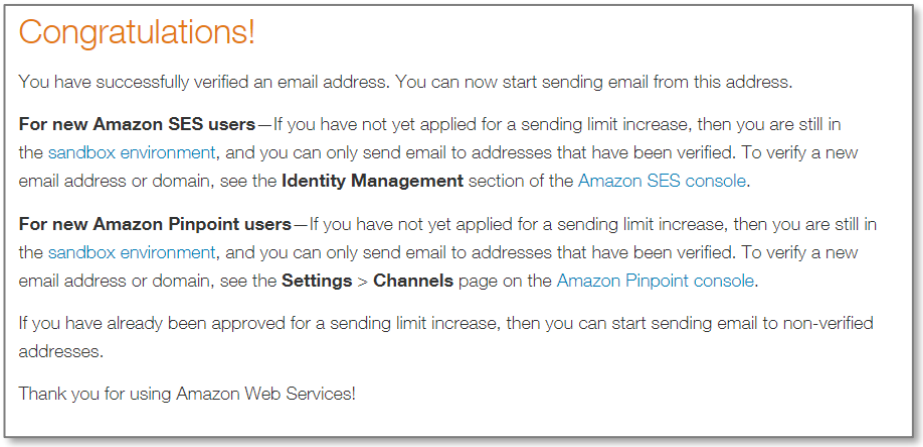


Enter your email address and click 'Verify this Email Address"

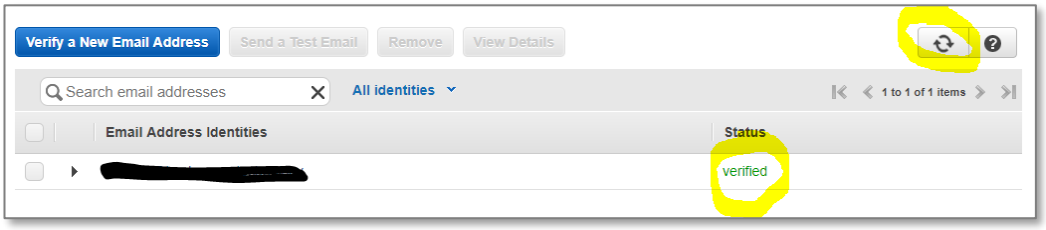


When you receive your verification email click on the supplied link.

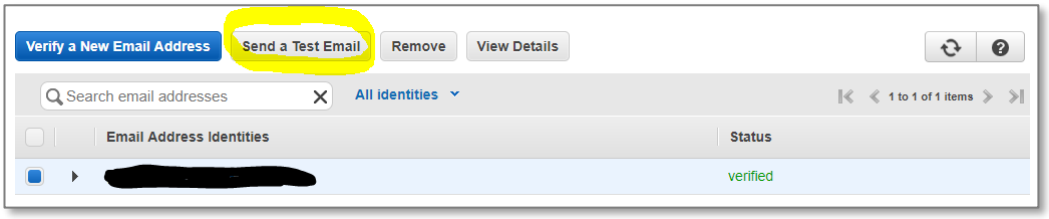
You will then receive a success page



Go back to the SES console page and refresh the information to see the email has been verified

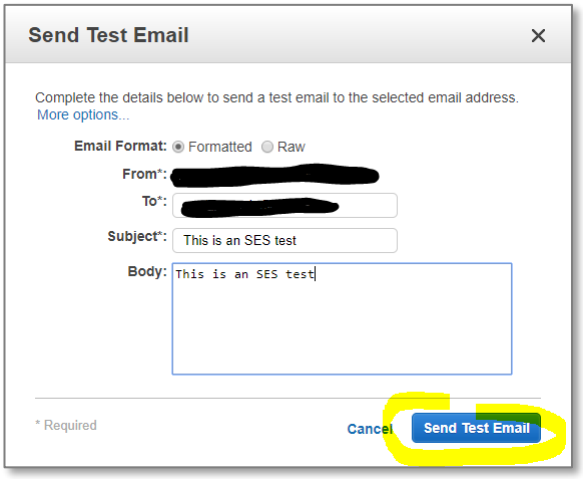


Click on the email address and select 'Send a test email"



Enter the same email address for from and to.

Fill out the email information and click 'Send test email"



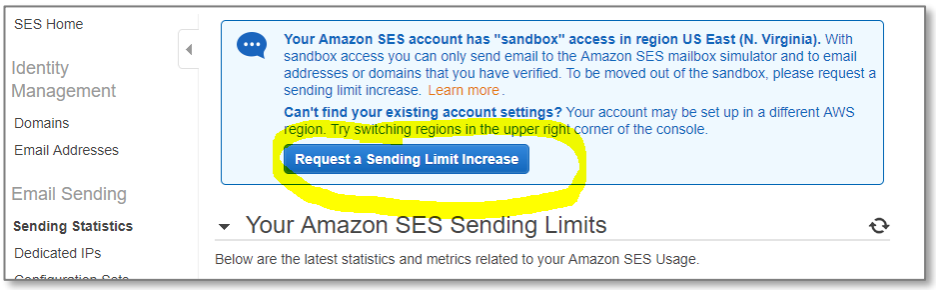
Check your email to see if it worked.

Requesting full access to SES

New accounts only have sandbox access but this can be changed by applying to AWS.

Click on 'Sending Statistic"

Click on 'Request a Sending Limit Increase"

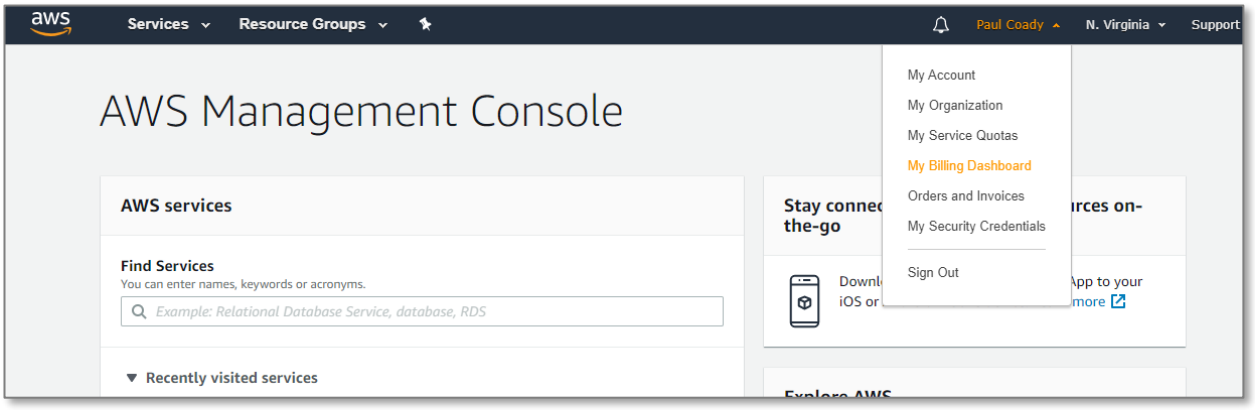


Creating a Billing Alert with CloudWatch and SNS

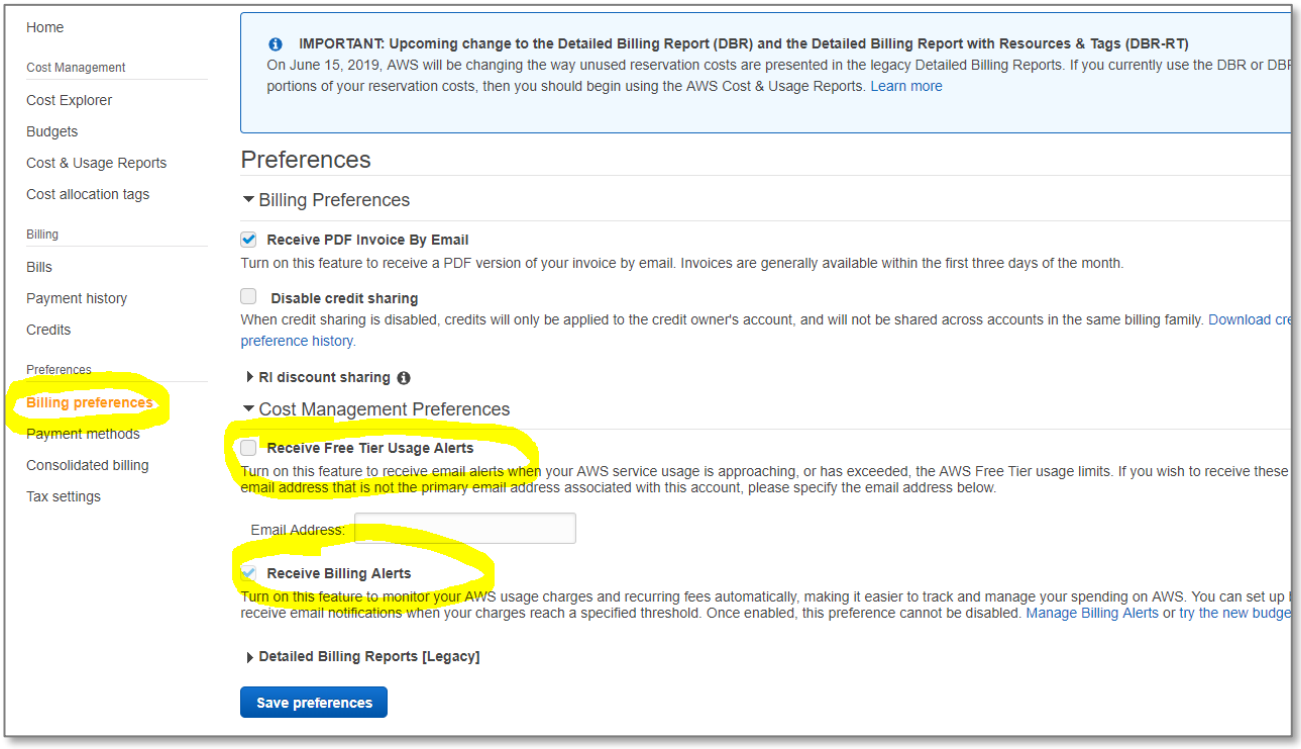
In this section, we will create a CloudWatch billing alert that will send an email through the Simple Notification Service whenever our estimated monthly bill exceeds a certain level.

Enabling Billing Alerts

From the AWS management console select 'My Billing Dashboard" from the account drop down menu.



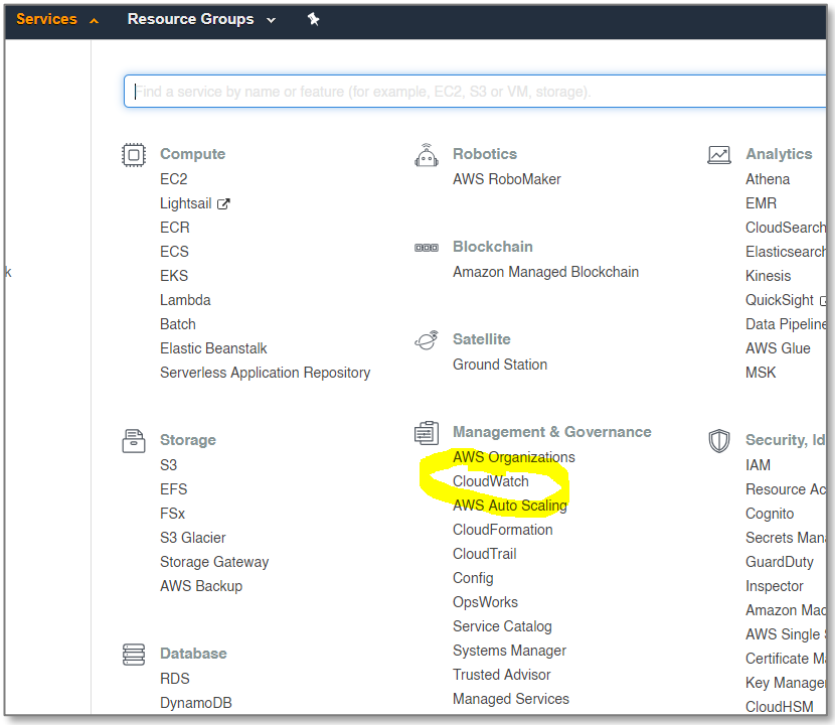
Select *Billing Preferences*
Check *Receive Free Tier Usage Alerts*
Check *Receive Billing Alerts*



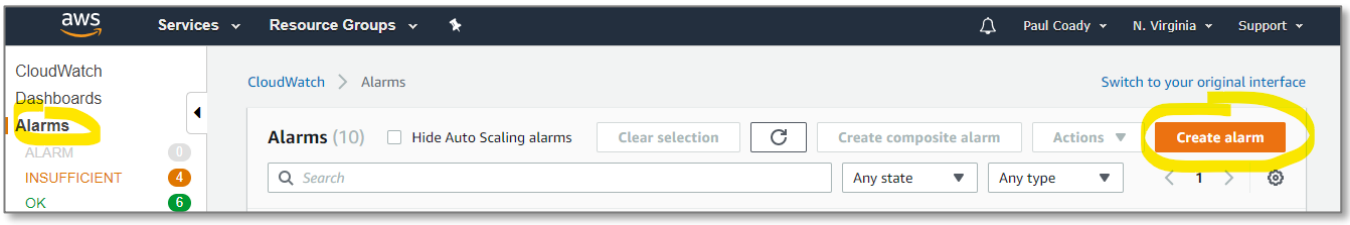
Click *Save preferences*

Creating a CloudWatch Alarm

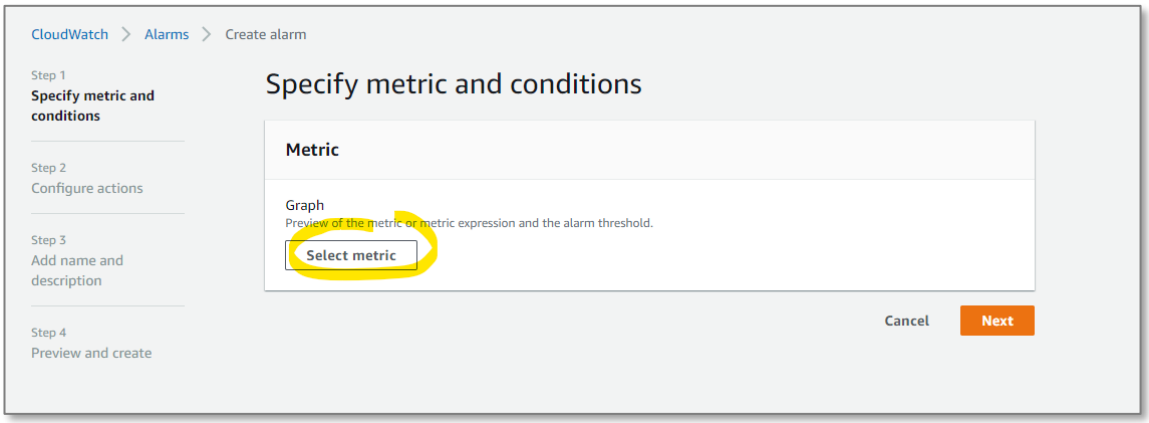
Click the Services menu and select 'CloudWatch" from 'Management& Governance"



Click on 'Alarms", 'Create Alarm"

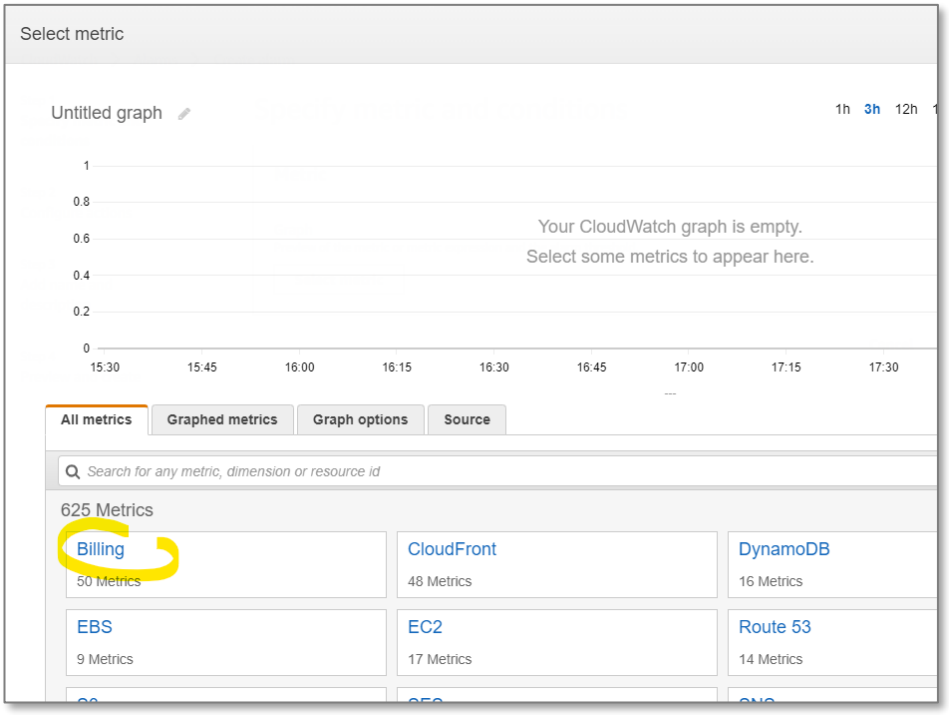


Click *Select metric*



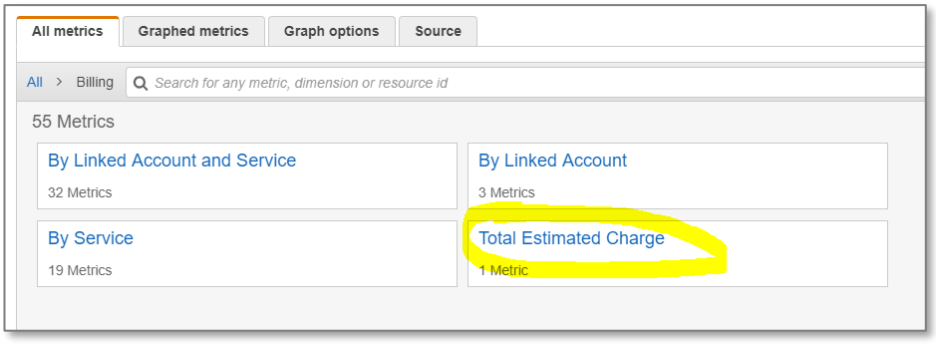
Search *Billing*

If you do not see any billing metrics it is most probably you are not operating in the US-East1 (N. Virginia) region. Please ensure you always operate from the US-East region during the course.



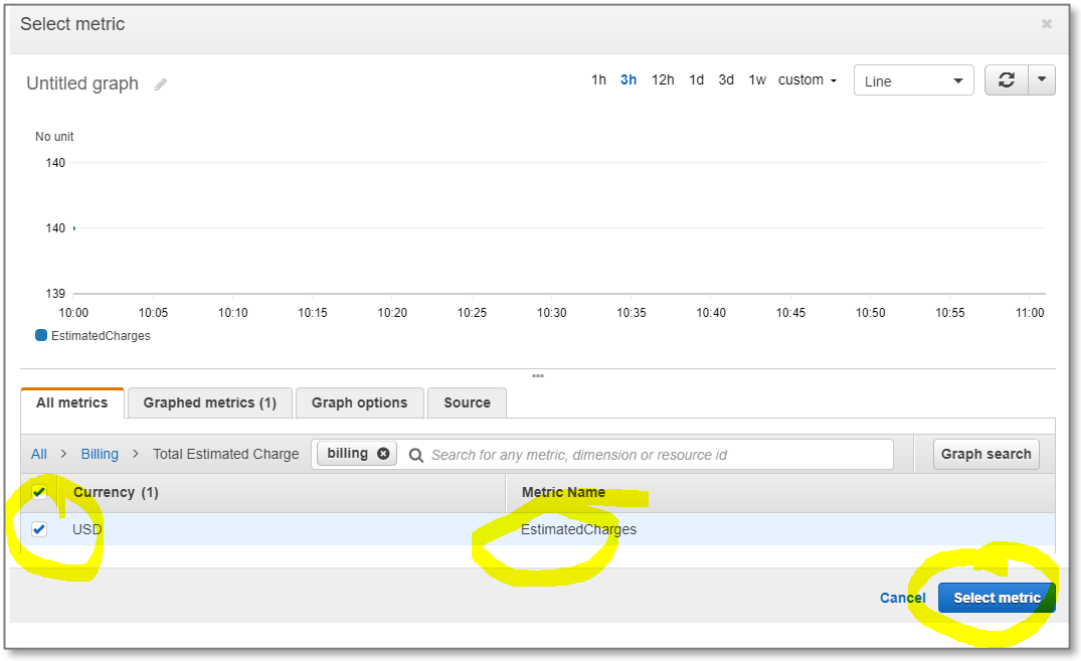
If you do not see any billing metrics it is most probably you are not operating in the US-East1 (N. Virginia) region. Please ensure you always operate from the US-East region during the course.

Select *Total Estimated Charge* from the billing metrics.



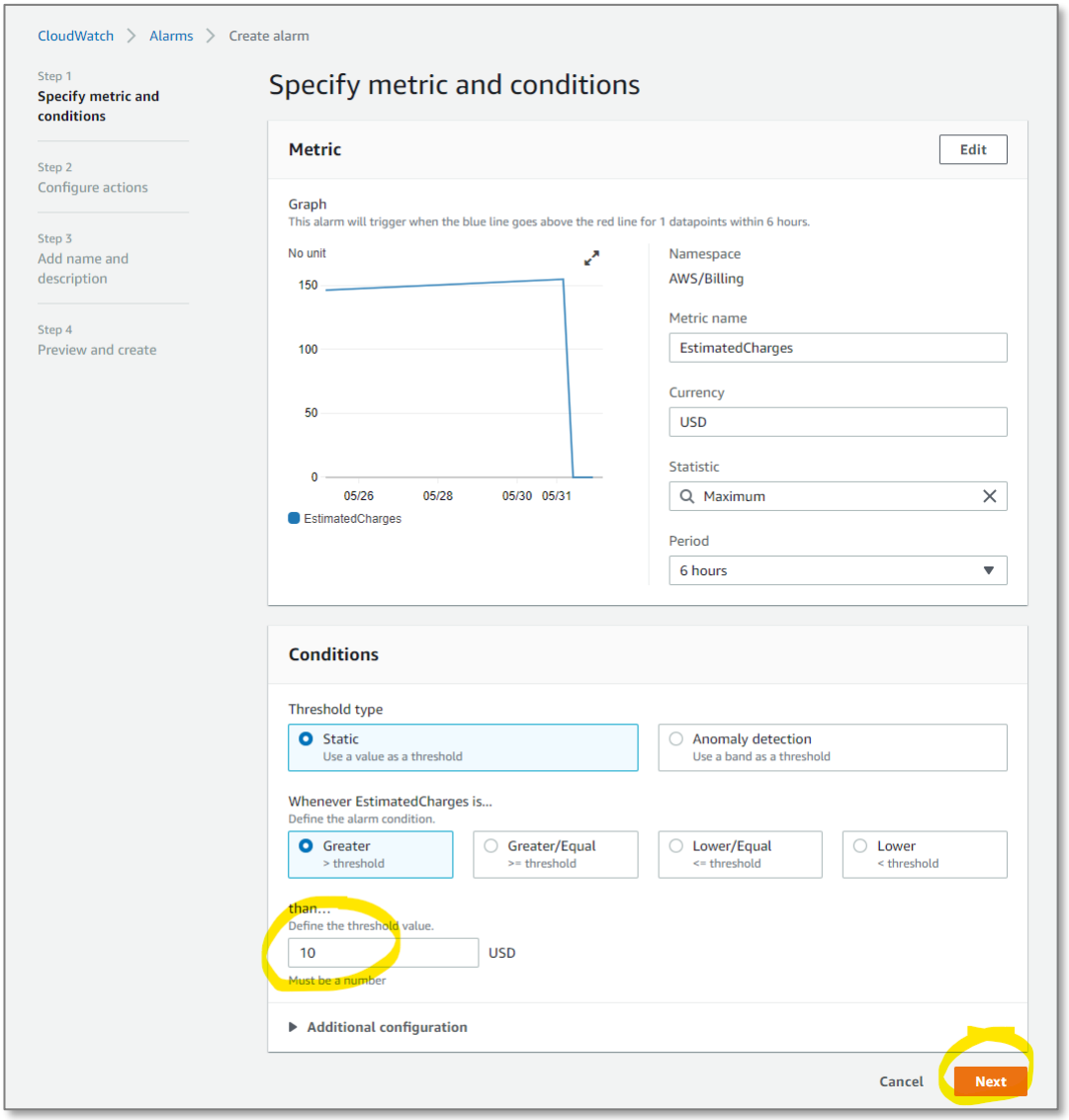
Select EstimatedCharges metric

Click *Select metric*



Set the alarm threshold to not exceed $10

Click *Next*



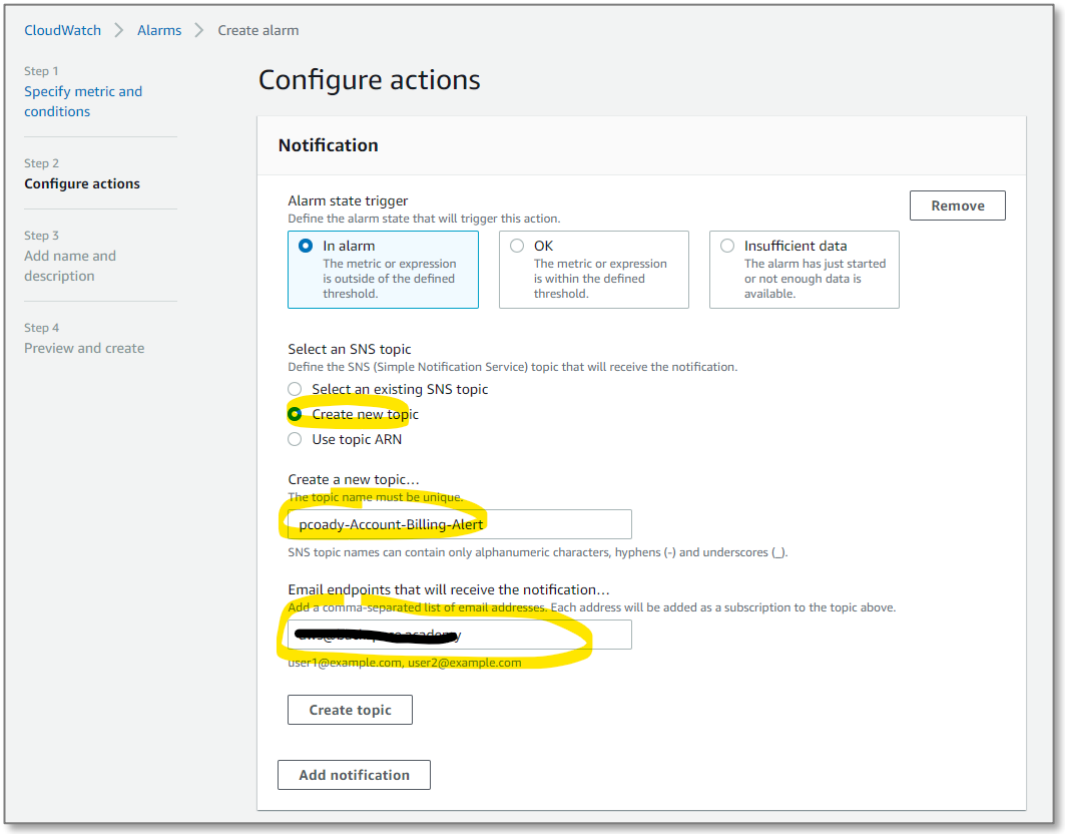
Select *in Alarm* for notification

Select *Create new topic*

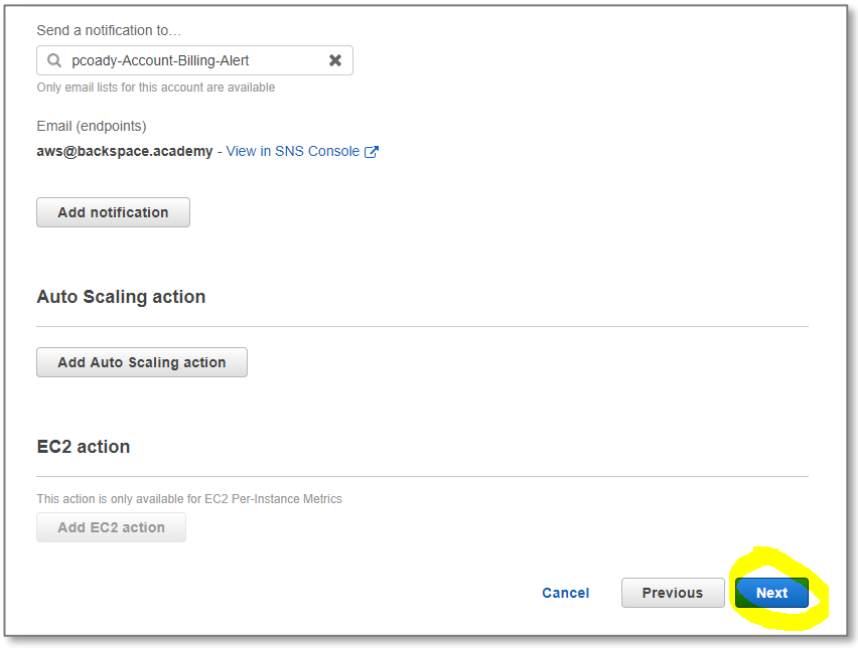
Enter a unique topic name

Enter an email address to receive the alert

Click *Create Topic*

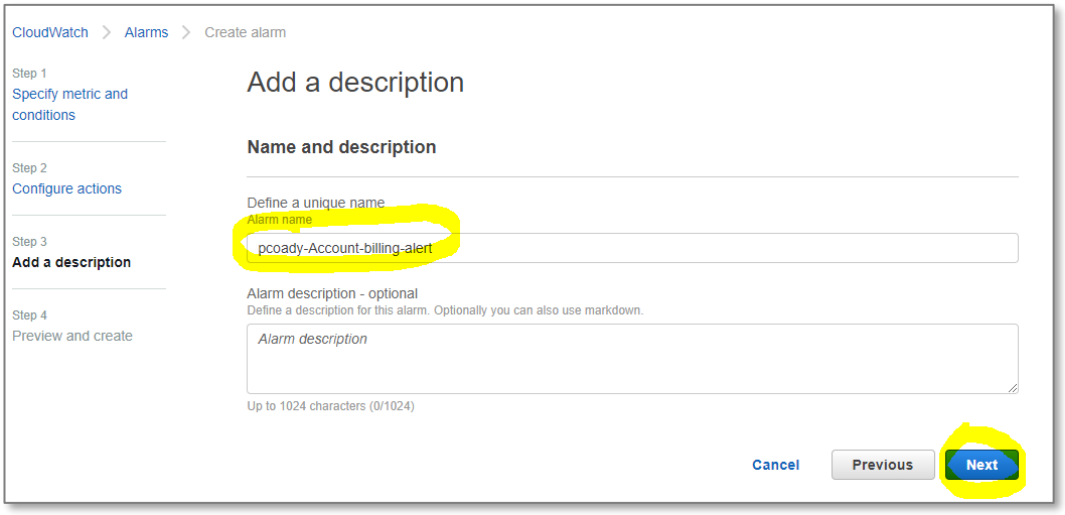


Click *Next*

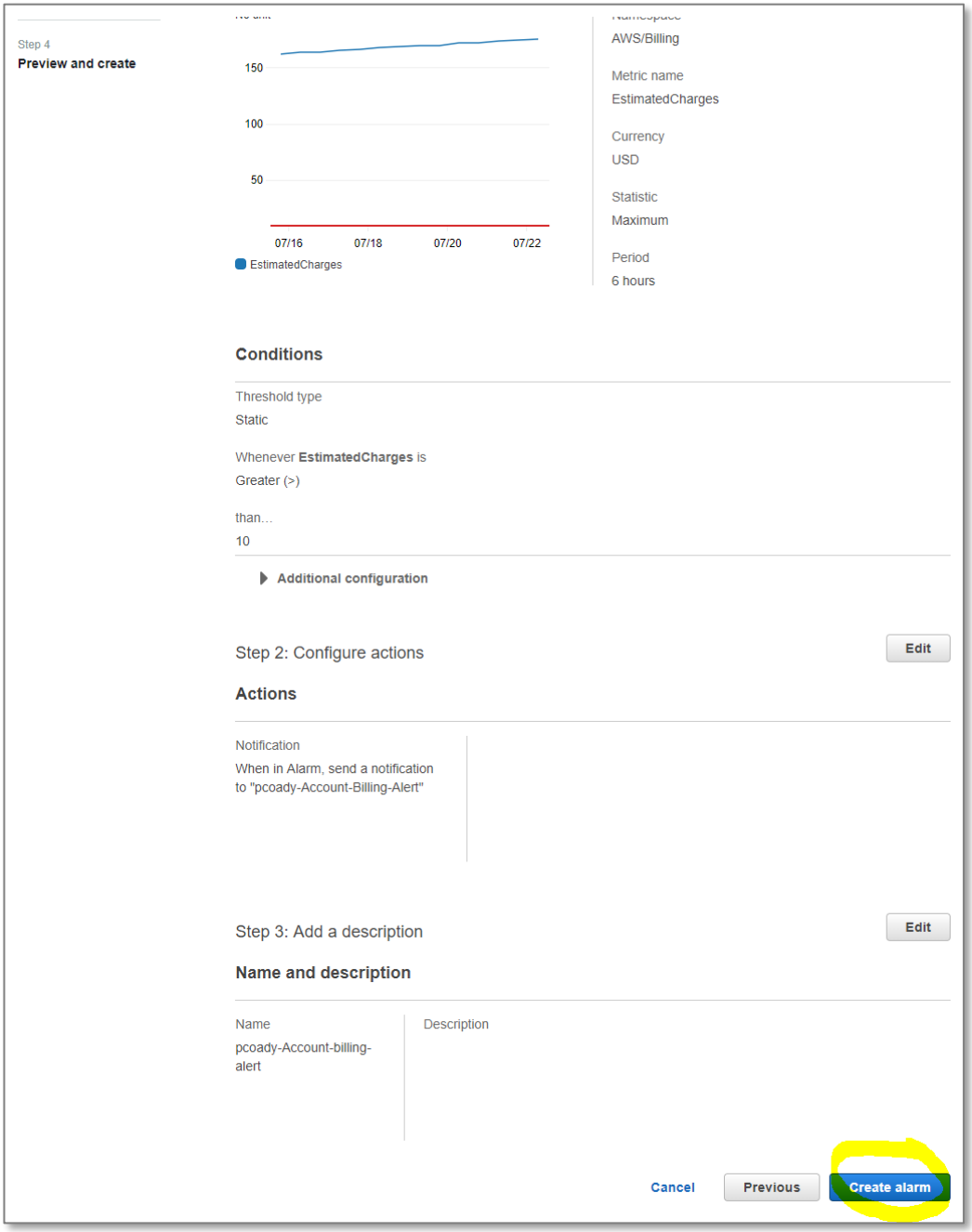


Give the alarm a unique name

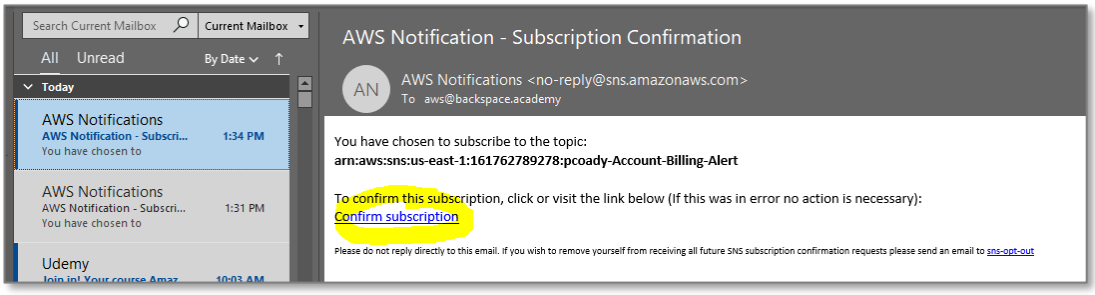
Click *Next*



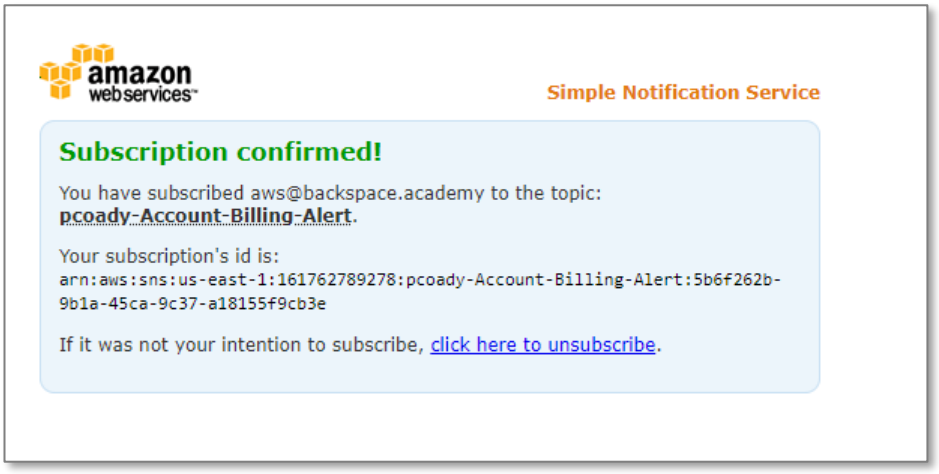
Click *Create alarm*



If you haven't already confirmed your email a confirmation email will be sent to you.

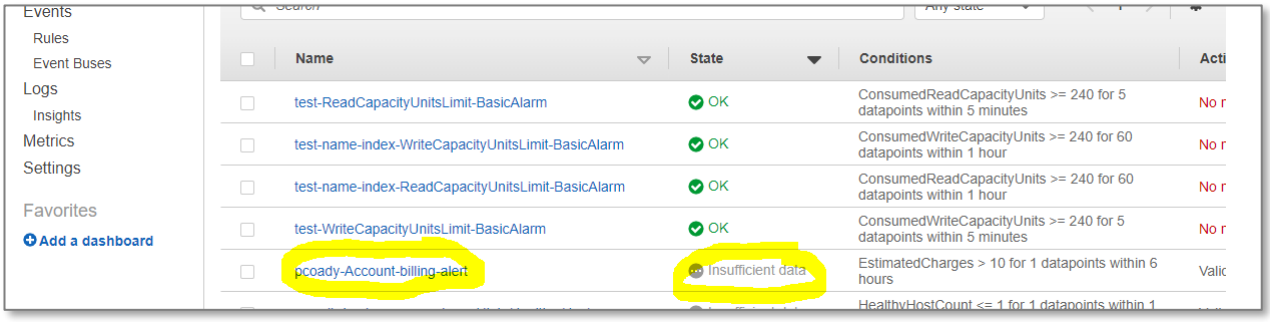


Click on the link in the email to confirm the SNS subscription

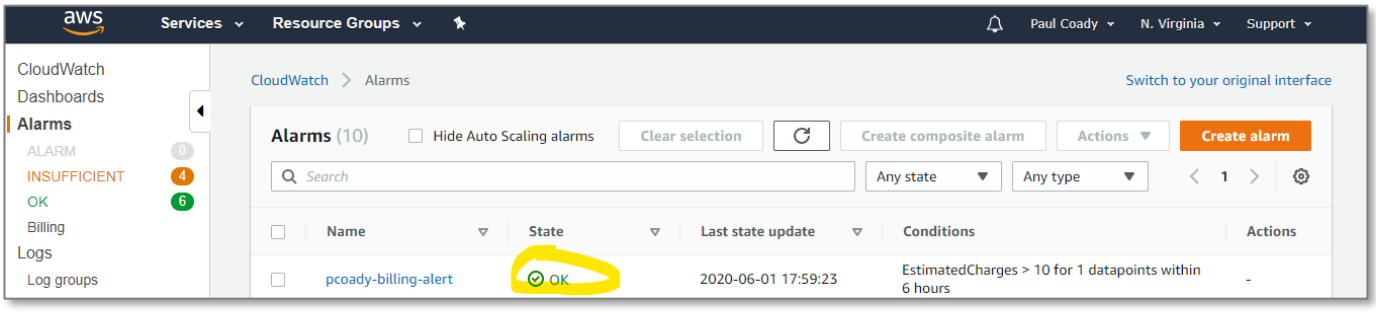


Go back to the CloudWatch console and refresh the screen.

The Alarm State will be INSUFFICIENT_DATA until enough data has been collected by CloudWatch



After a few days you will have plenty of billing data to view

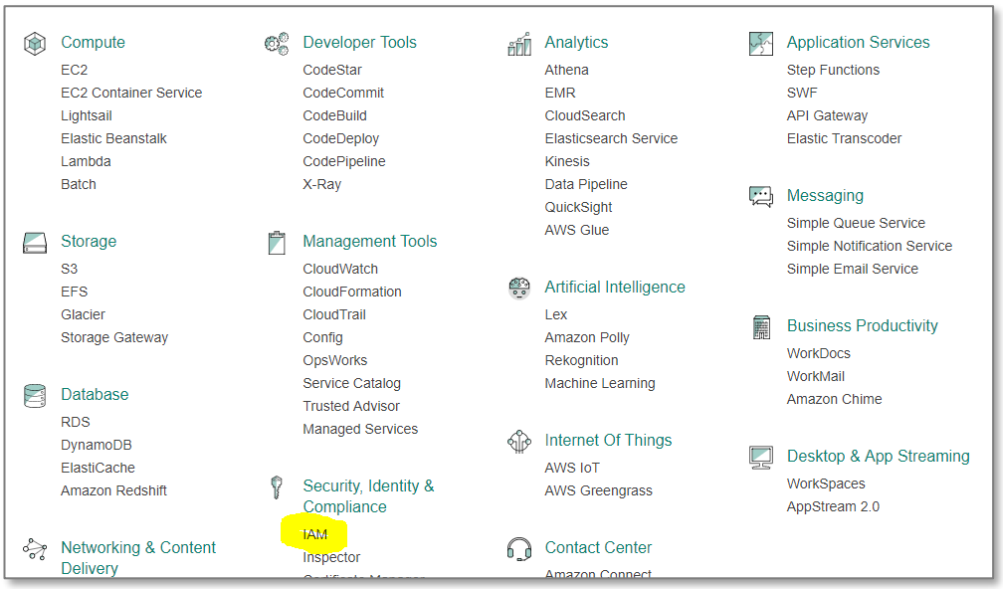


Creating an IAM User

In this section, we will use the Identity and Access Management (IAM) service to create a user with console access and programmatic access.

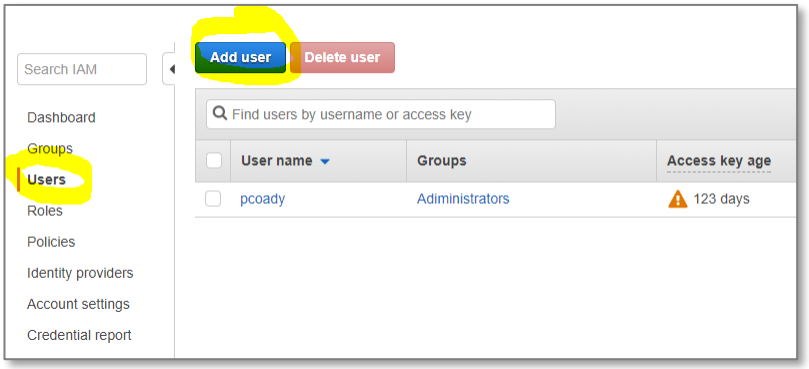
From the AWS console click 'Services"

Select 'IAM" from the Security, Identity & Compliance services.

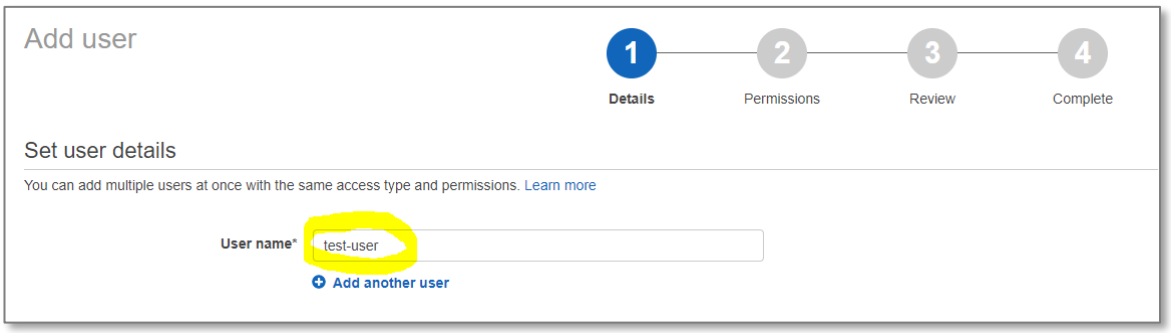


Select 'Users"

Click 'Add user"

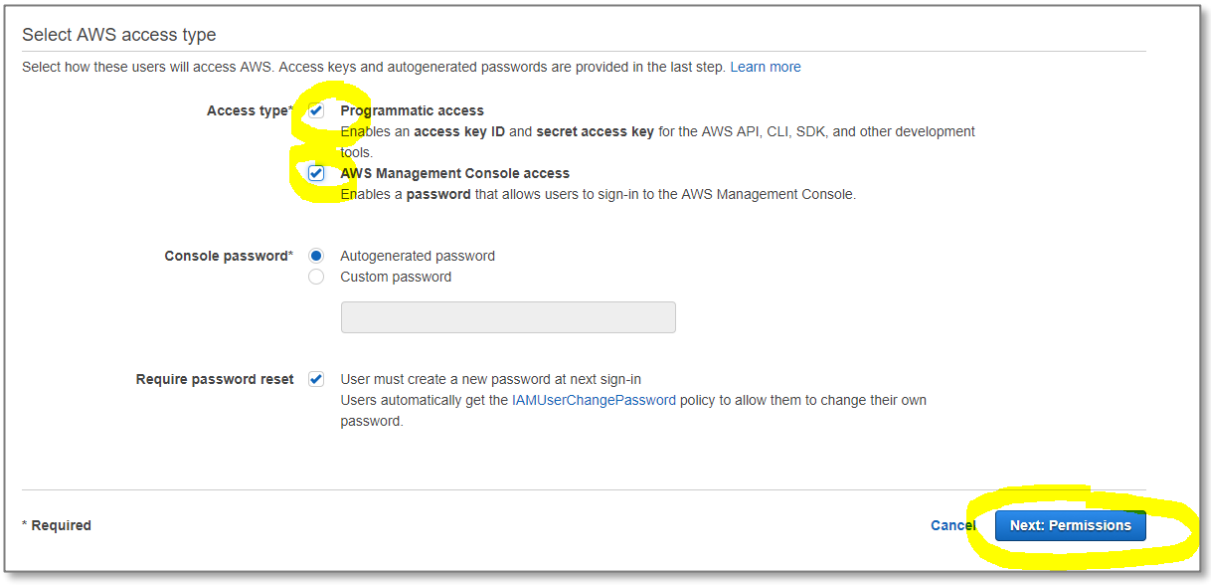


Give the user a name



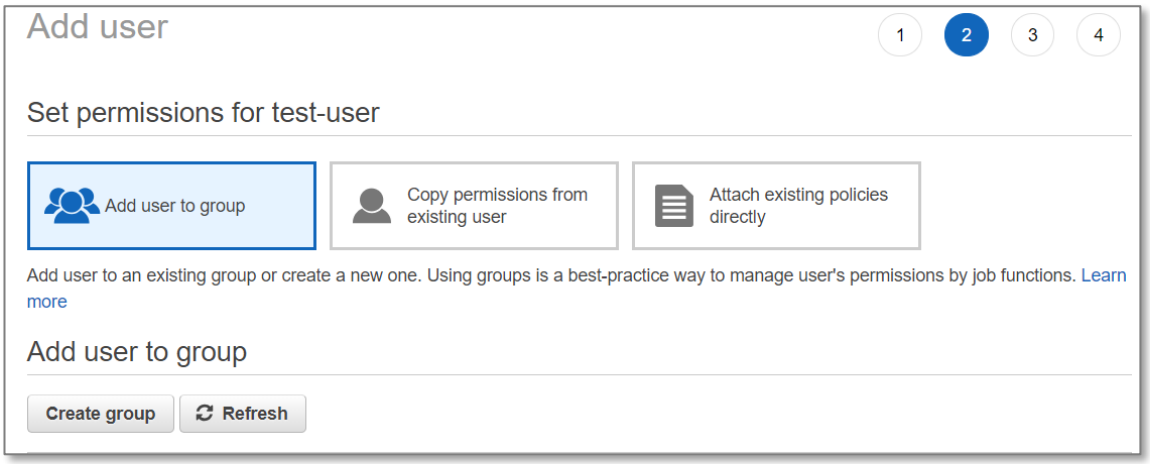
Check 'Programmatic access"

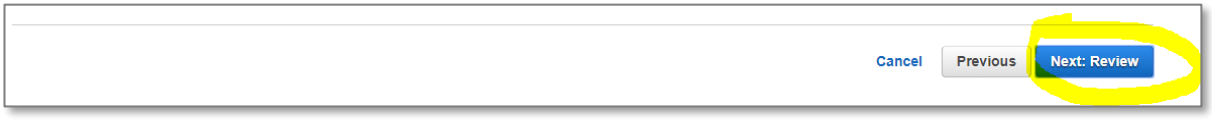
Check 'AWS Management Console access"



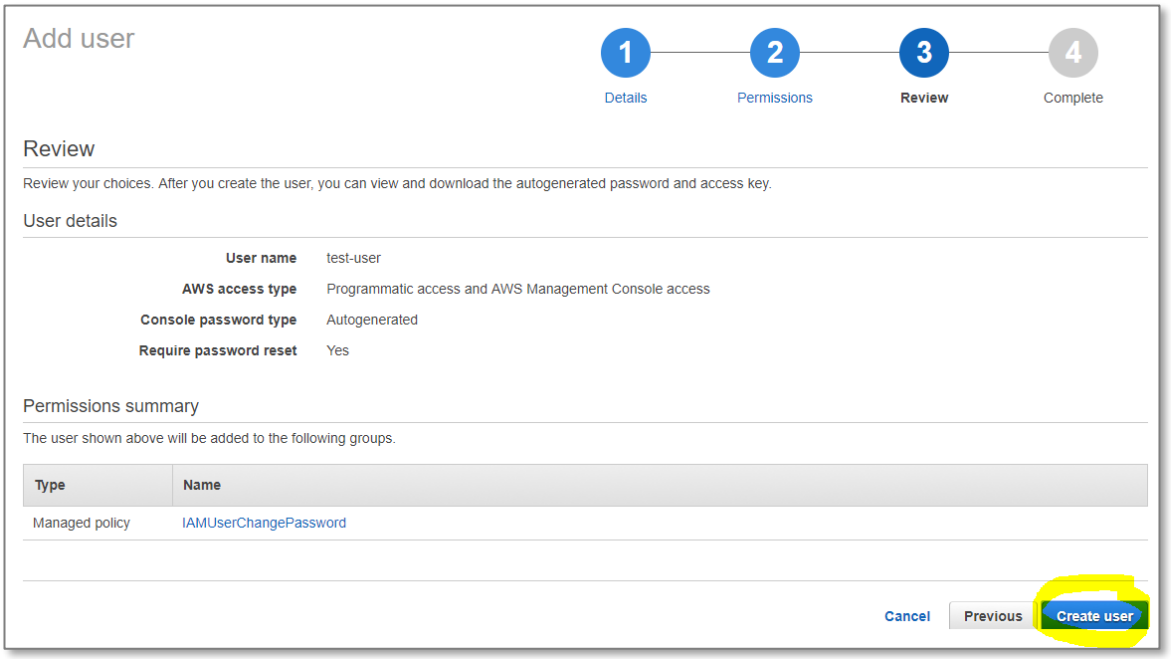
We won't set any permissions for the user at this point.

Click 'Next Review"



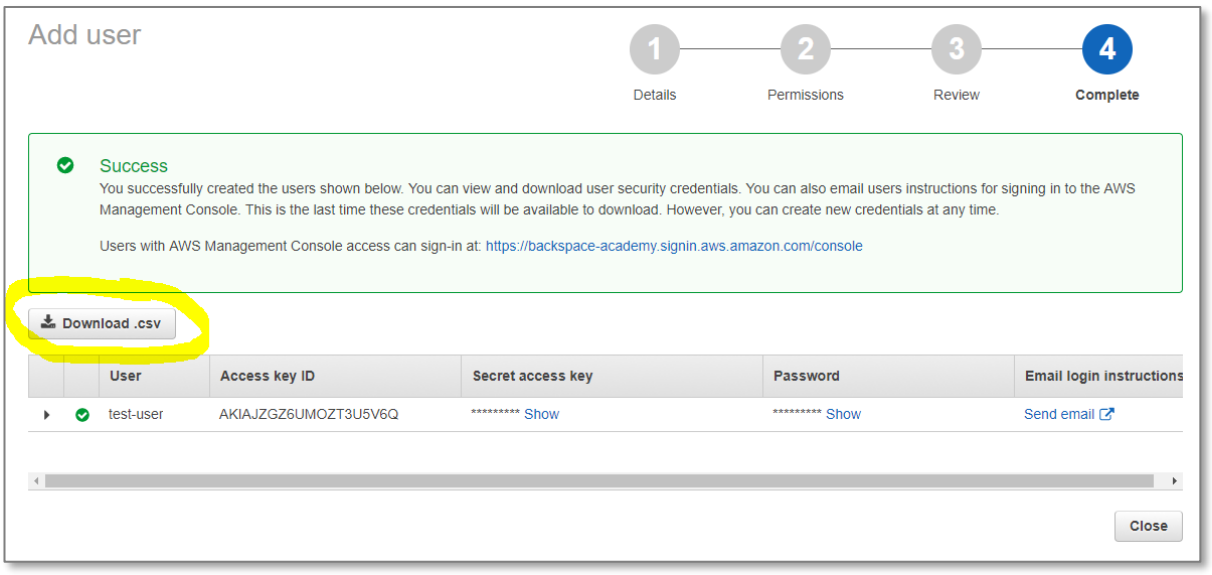


Click 'Create user"



Download the csv file containing the user credentials (access key and secret access key) to a safe location.

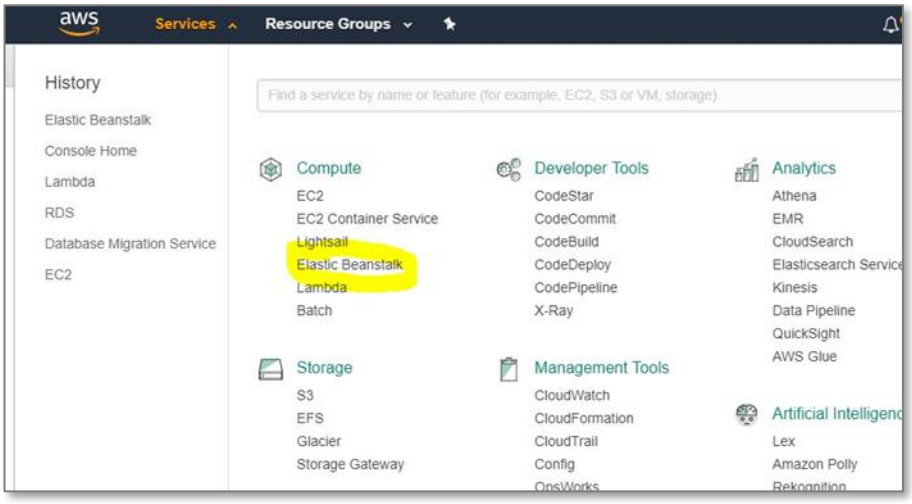
You will need this for access using the Command Line Interface (CLI) later in the course.



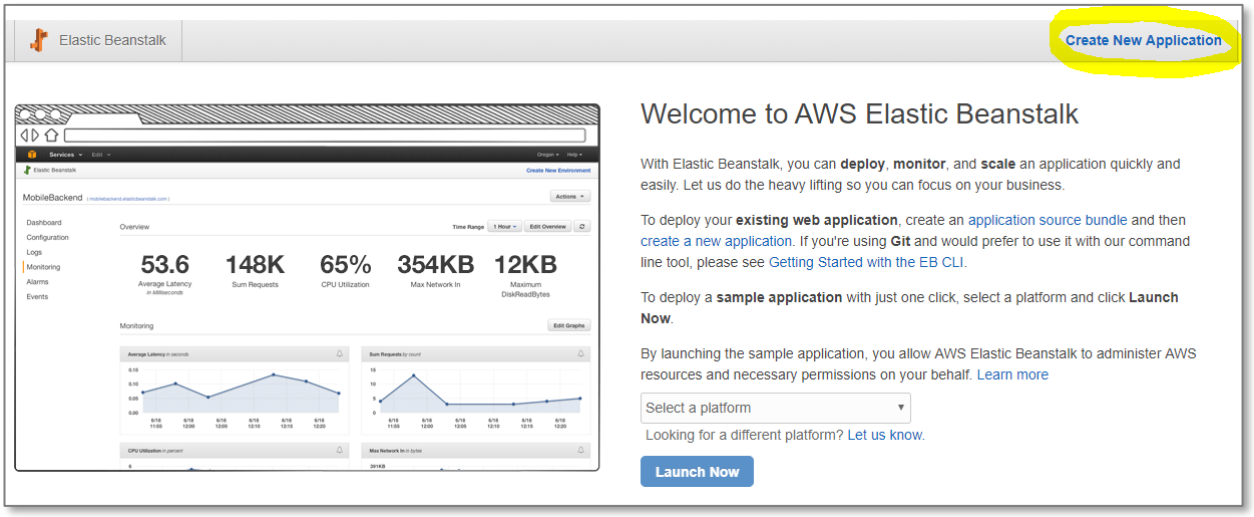
Creating a Highly Available Architecture with Elastic Beanstalk

In this section, we will create a highly available and fault tolerant architecture using the AWS Elastic Beanstalk service.

Click on the services menu and select *Elastic Beanstalk*

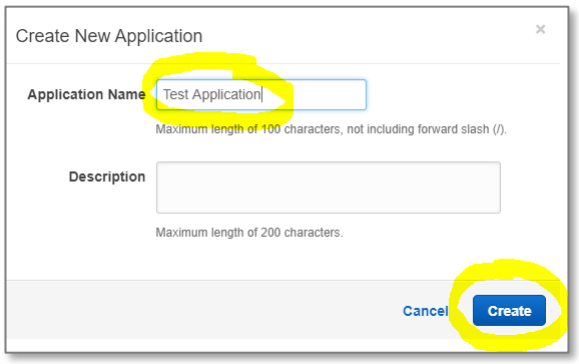


Click 'Create New Application"



Give your application a name *Test Application*.

Click "Create"

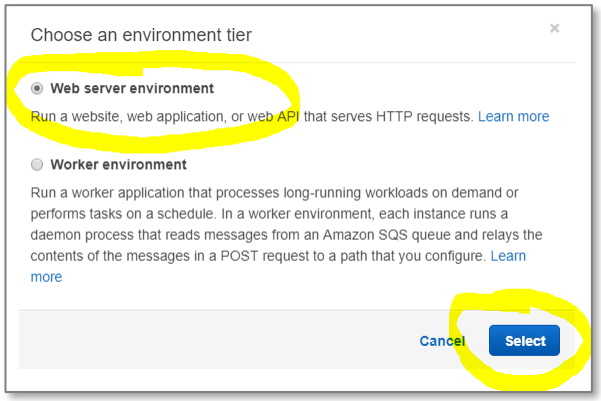


Your application will now be created.

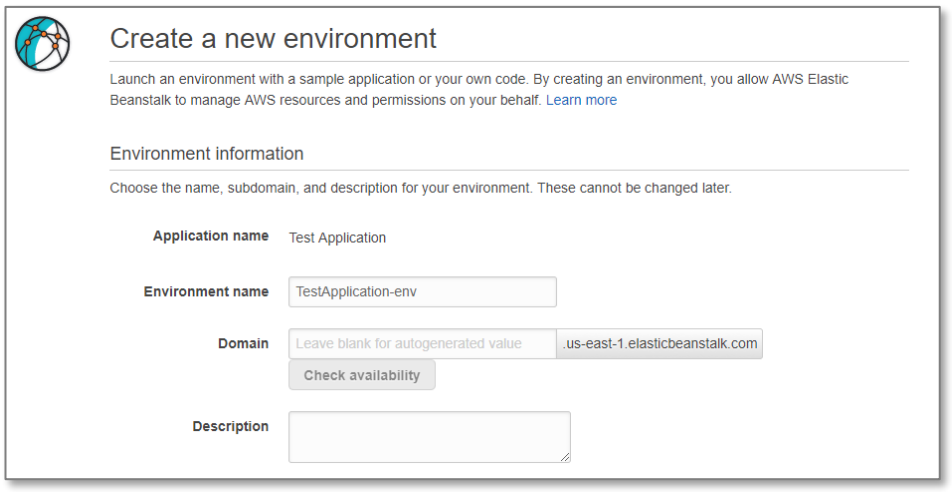
Select “Actions” - “Create Environment”

Select “Web server environment”

Click “Select”



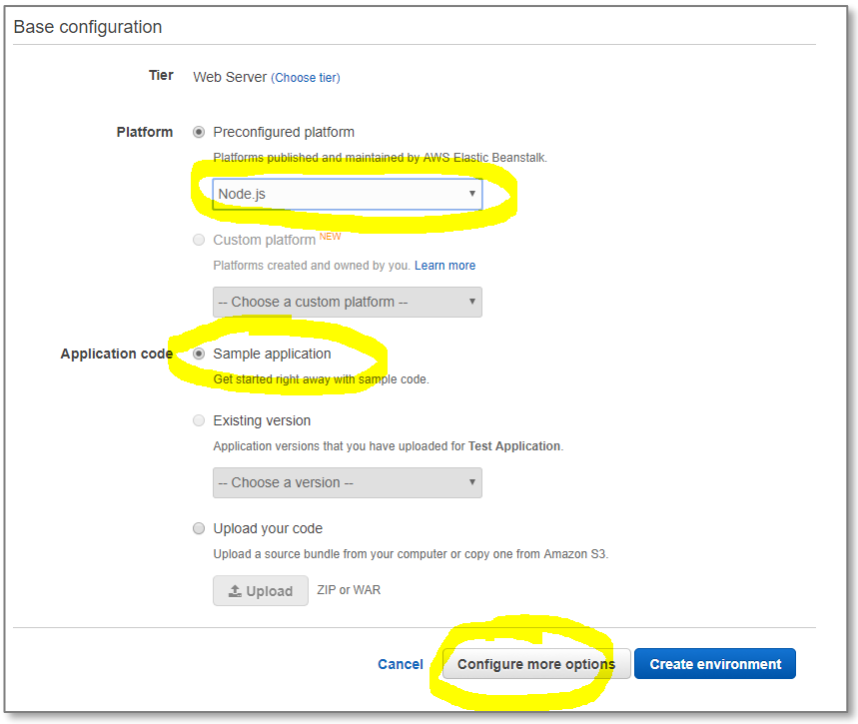
Leave Environment information with default values



Select *Node.Js* as the platform

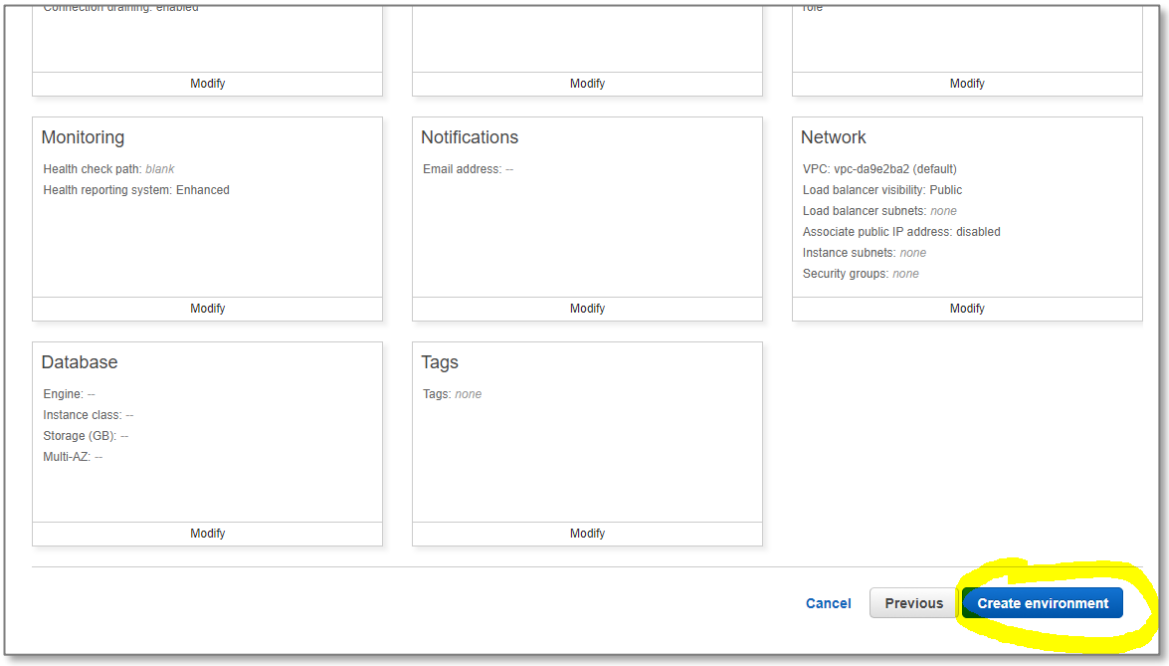
Select *Sample Application* for Application Code

Click *Configure More Options*

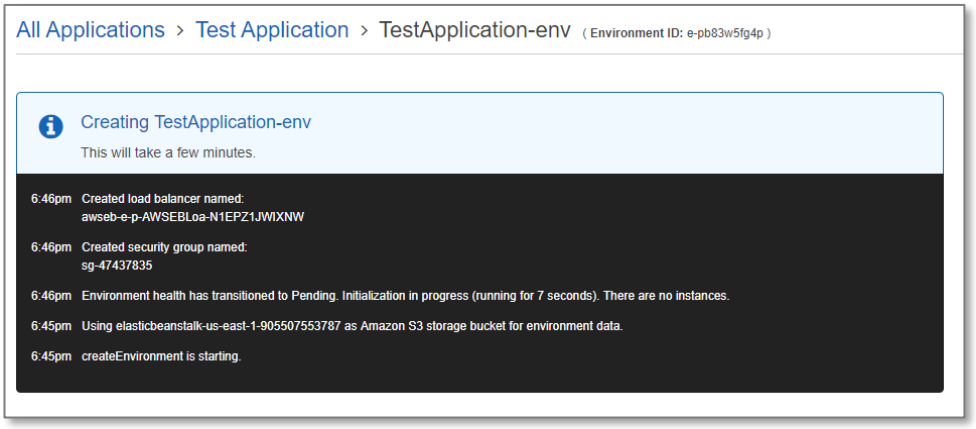


Select *High availability*

Scroll down and click *Create environment*

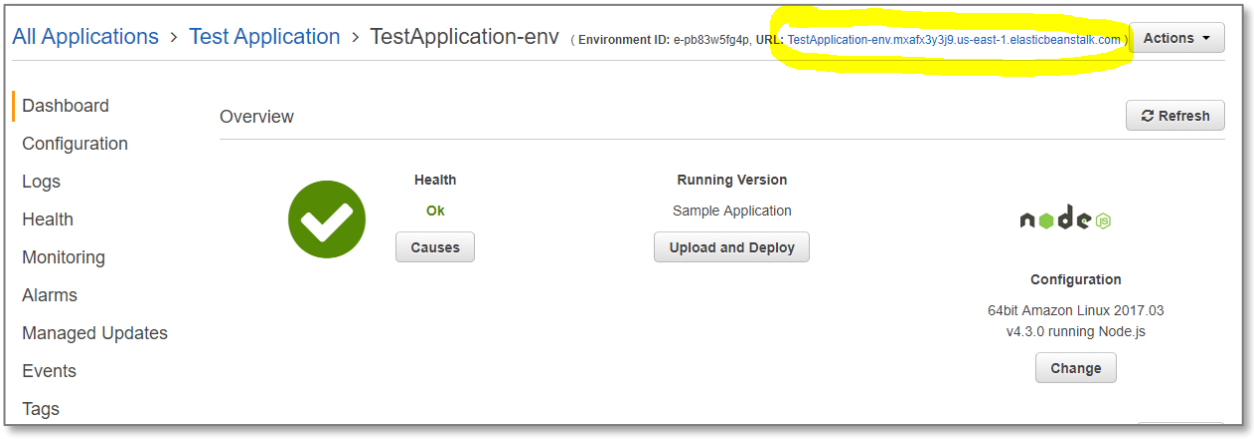


Your environment will start being created



After some time, your environment will be created.

Click on the website url

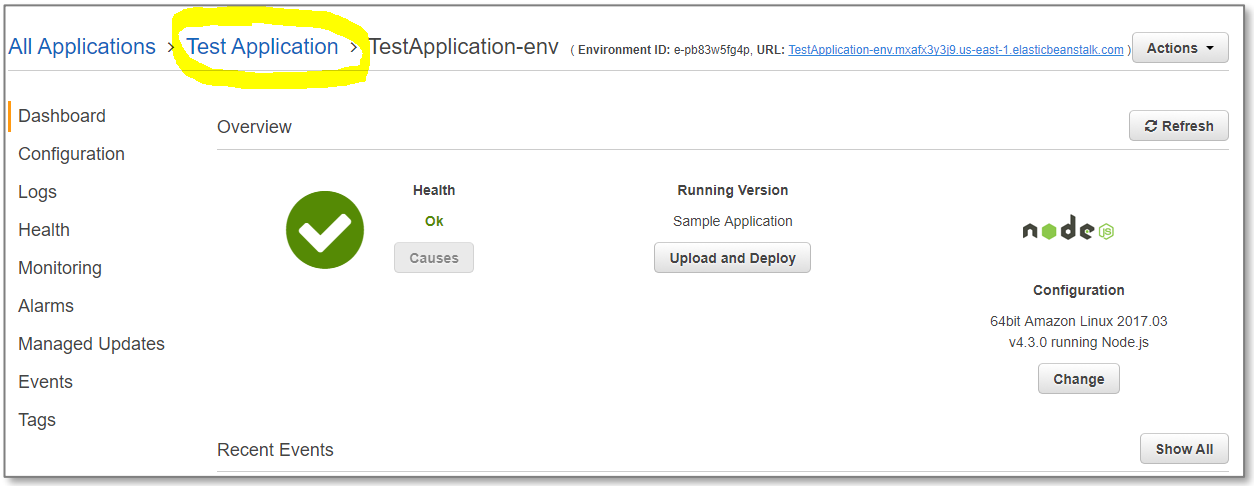


You will now see the Sample Application

Clean Up

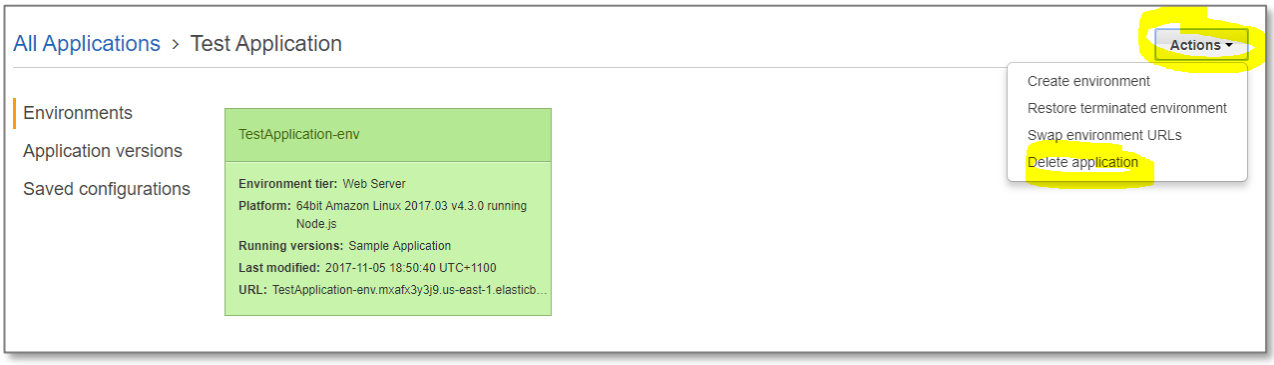
We will now delete the environment so that you will not be billed by AWS.

Navigate back to the Test Application

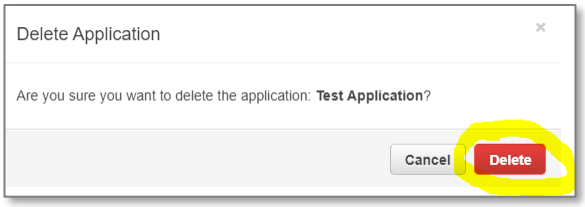


Click Actions

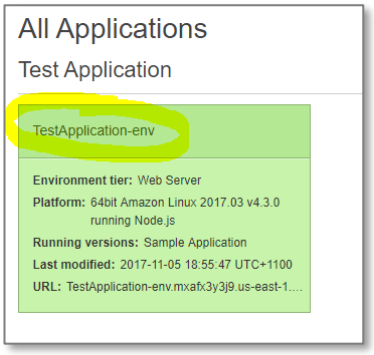
Select Delete Application



Click “Delete”



Click on the environment



You will now see your environment is being terminated.