



lab



lab title

Introduction to AWS

V1.37



Course title

BackSpace Academy  
AWS Certified Associate



# ▶ Table of Contents

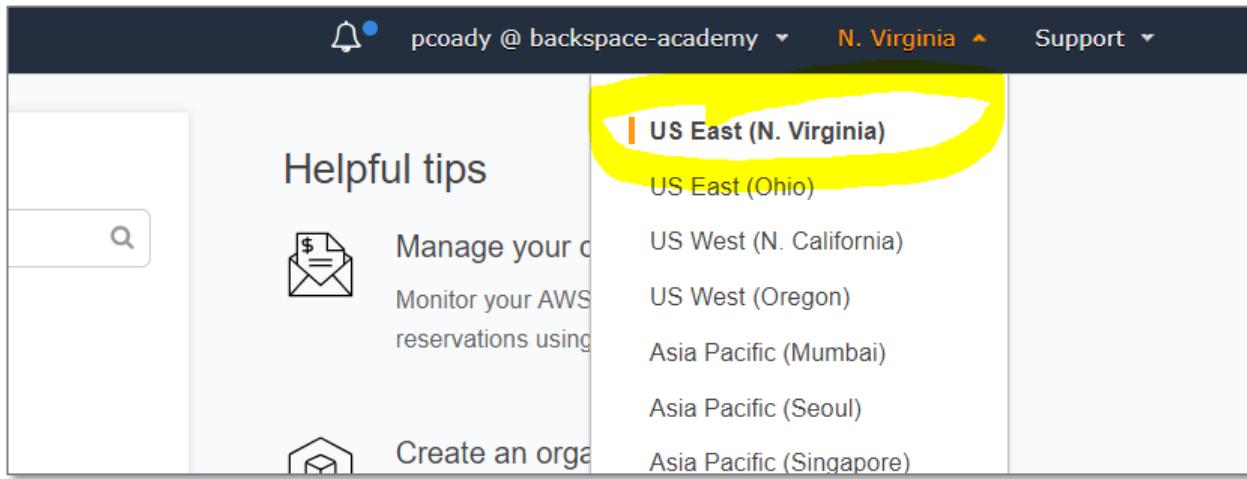
## Contents

<b>Table</b> of Contents .....	1
<b>About</b> the Lab .....	3
<b>Checking</b> your AWS Usage and Monthly Bill .....	4
<b>Creating</b> an S3 Bucket and Uploading Files .....	5
Uploading Files to your Bucket.....	8
Downloading files from your bucket .....	10
Troubleshooting.....	11
Clean Up.....	11
<b>Creating</b> a SQL Database with RDS.....	14
Creating a Security Group.....	14
Creating an RDS Database .....	17
Connecting to your RDS Instance .....	23
Troubleshooting Connection Issues .....	27
Clean Up.....	29
<b>Creating</b> a Web Server with EC2.....	31
Viewing your web server .....	36
Troubleshooting viewing your WordPress application .....	38
Finding the Username and Password for your WordPress application.....	40
Troubleshooting logging in to the WordPress application .....	43
Clean up .....	43
<b>Sending</b> Emails with Amazon SES .....	45
Requesting full access to SES .....	47
<b>Creating</b> a Billing Alert with CloudWatch and SNS.....	48
Enabling Billing Alerts .....	48
Creating a CloudWatch Alarm .....	49
<b>Creating</b> an IAM User.....	58
<b>Creating</b> a Highly Available Architecture with Elastic Beanstalk .....	61
Clean Up.....	65



# ► 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.

**Billing & Cost Management Dashboard**

**What's New in AWS Billing and Cost Management?**

- Manage your spend with AWS Budgets
- Visualize your costs and usage with the newly-optimized Cost Explorer
- Easily upload your Cost and Usage Reports into Redshift and QuickSight

**Month-to-Date Spend by Service**

The chart below shows the proportion of costs spent for each service you use.

Service	Amount
SES	\$0.01
S3	\$0.00
EC2	\$0.00
CloudWatch	\$0.00
Other Services	\$0.00
Tax	\$0.00
<b>Total</b>	<b>\$0.01</b>

**Spend Summary**

Welcome to the AWS Account Billing console. Your last month, month-to-date, and month-end forecasted costs appear below.

Current month-to-date balance for August 2017

**\$0.01**

Bar chart showing Current month-to-date balance for August 2017:

Period	Amount
Last Month (July 2017)	\$0
Month-to-Date (August 2017)	\$0.01
Forecast (August 2017)	\$0.01

Important Information about these Costs  Include Subscription Charges

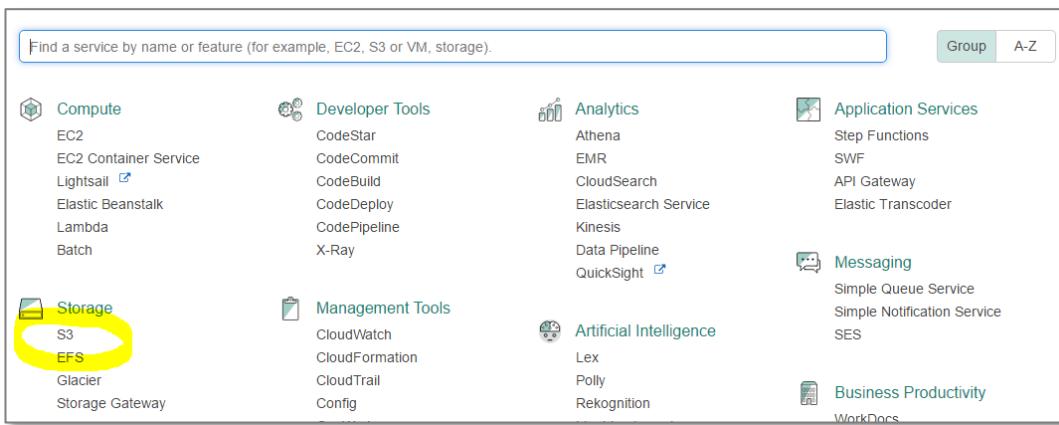
**Top Free Tier Services by Usage**

Service	Month-to-date usage/Free Tier limit	Forecasted month-end usage/Free Tier limit
S3 - Puts	62.00% (1,240,000/2,000 Requests)	120.13% (2,402,500/2,000 Requests)
EBS - Snapshots	47.99% (0.48/1 GB-Mo)	92.99% (0.93/1 GB-Mo)

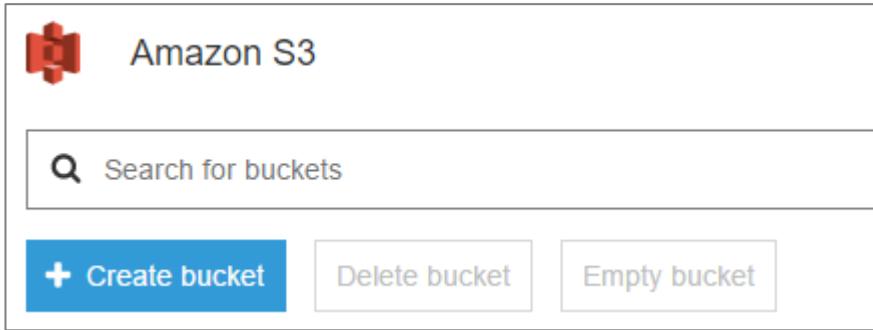
# ▶ Creating an S3 Bucket and Uploading Files

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.



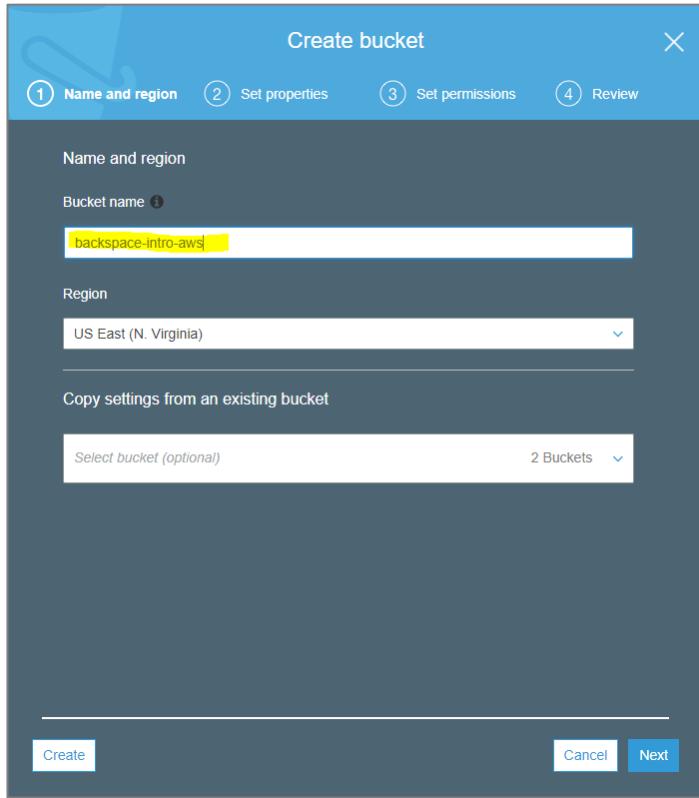
Click on Create Bucket



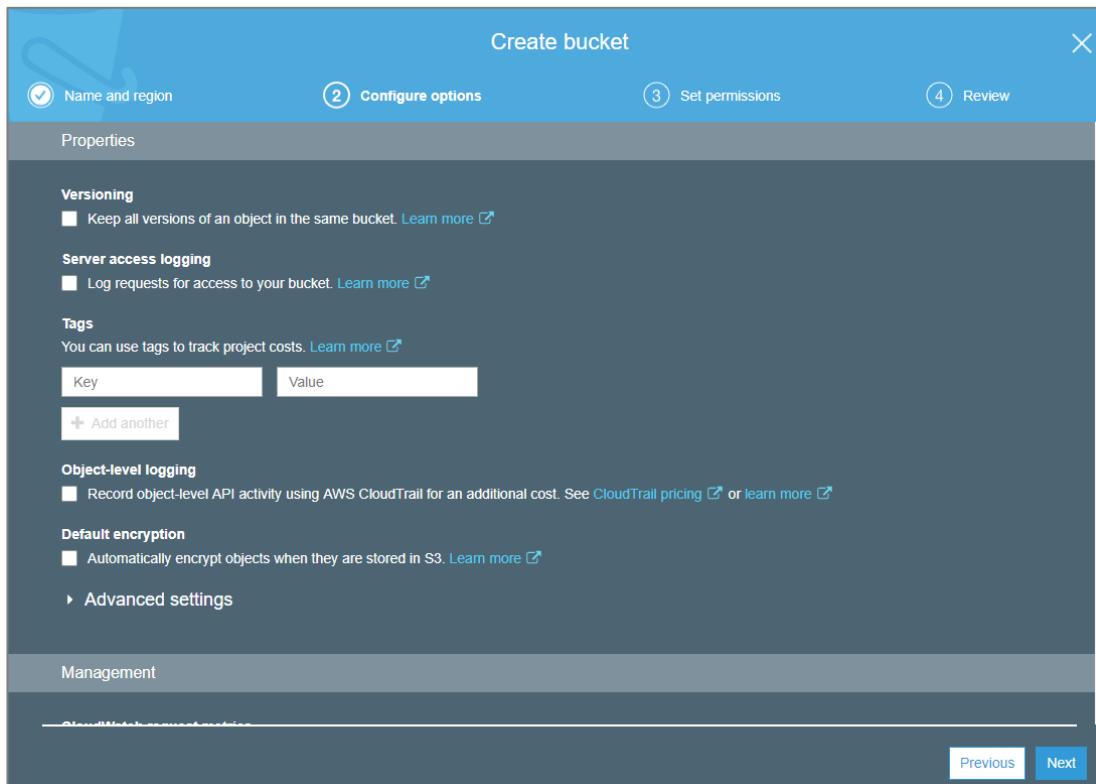
The create bucket dialog box will appear.

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

Click 'Next'



Leave as is and click 'Next"



Leave as is and click 'Next"

Create bucket

① Name and region   ② Configure options   ③ Set permissions   ④ Review

Note: You can grant access to specific users after you create the bucket.

**Public access settings for this bucket**

Use the Amazon S3 block public access settings to enforce that buckets don't allow public access to data. You can also configure the Amazon S3 block public access settings at the account level. [Learn more](#)

**Manage public access control lists (ACLs) for this bucket**

- Block new public ACLs and uploading public objects (Recommended)
- Remove public access granted through public ACLs (Recommended)

**Manage public bucket policies for this bucket**

- Block new public bucket policies (Recommended)
- Block public and cross-account access if bucket has public policies (Recommended)

**Manage system permissions**

Do not grant Amazon S3 Log Delivery group write access to this bucket

Previous   Next

Click 'Create Bucket"

Create bucket

① Name and region   ② Configure options   ③ Set permissions   ④ Review

**Name and region**

**Bucket name** backspace-lab-intro-aws   **Region** US East (N. Virginia)

**Options**

Versioning	Disabled
Server access logging	Disabled
Tagging	0 Tags
Object-level logging	Disabled
Default encryption	None
CloudWatch request metrics	Disabled
Object lock	Disabled

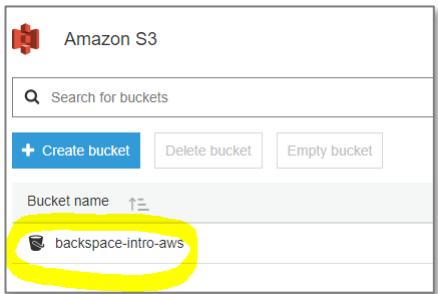
**Permissions**

Block new public ACLs and uploading public objects	True
Remove public access granted through public ACLs	True
Block new public bucket policies	True
Block public and cross-account access if bucket has public policies	True

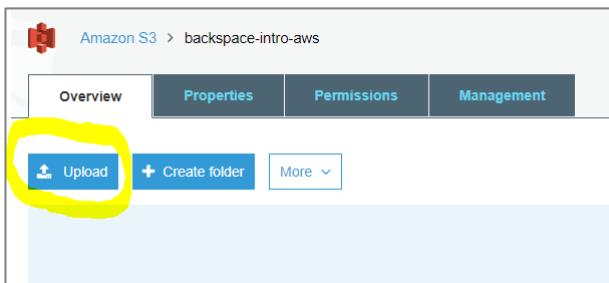
Previous   Create bucket

## Uploading Files to your Bucket

Click on the link to the bucket

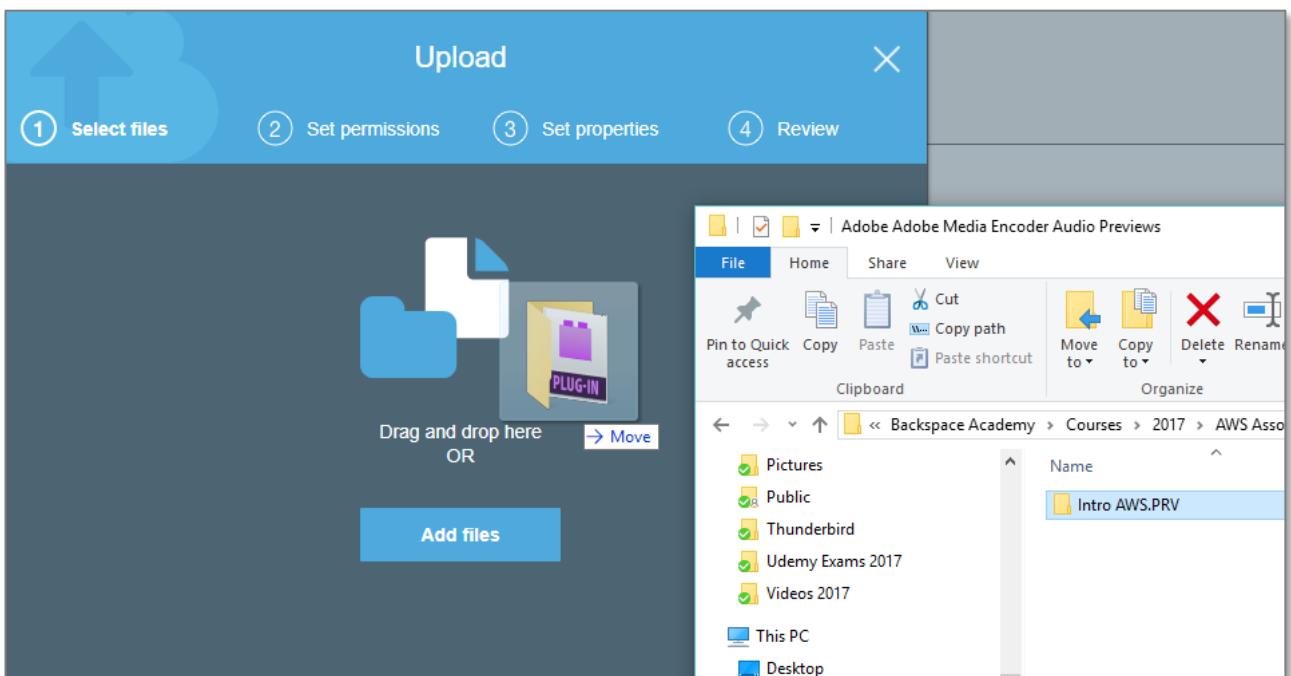


Select 'Upload'

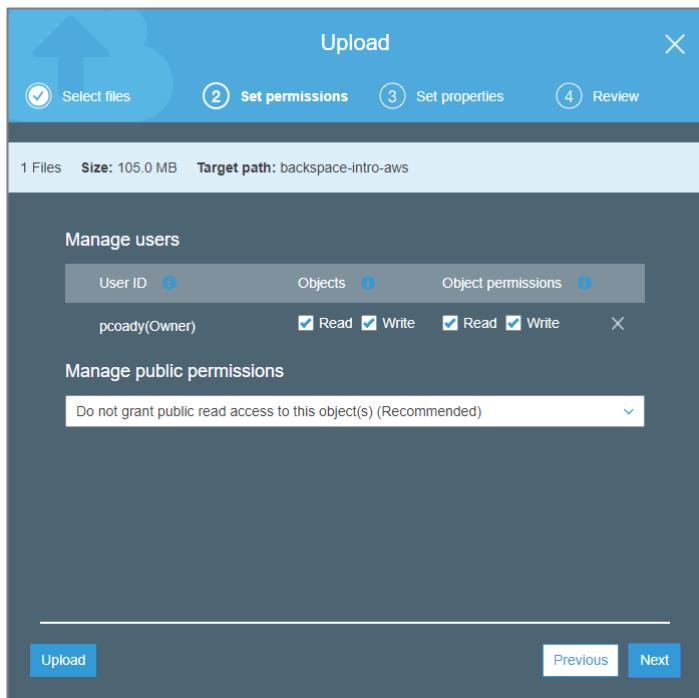


Drag a folder with files onto the form.

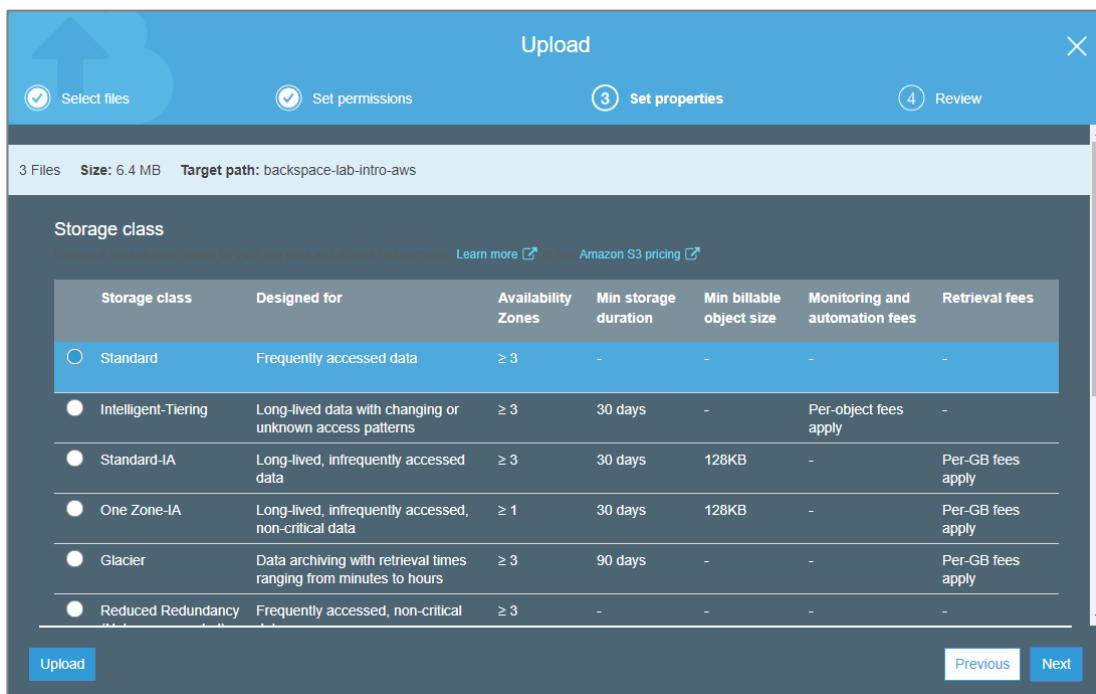
Click Next



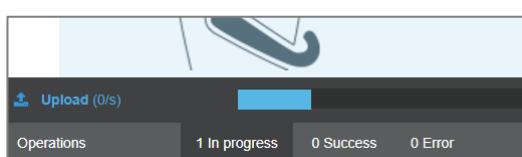
Leave as is and click 'Next"



Leave as is and click 'Next"



Click 'Upload"



Your upload will eventually complete.

Amazon S3 > backspace-intro-aws

Overview Properties Permissions Management

Type a prefix and press Enter to search. Press ESC to clear.

Upload + Create folder More

US East (N. Virginia)

Name Last modified Size Storage class

img

Viewing 1 to 1

## Downloading files from your bucket

Click the link for your folder

Upload + Create folder More

Name

img

Select a file

Upload + Create folder More

Name Last modified

BackSpace.png Aug 14, 2017

BackSpace.psd Aug 14, 2017

Select "More", "Download As"

Upload + Create folder More

Get size

Download as

Rename

Delete

Undo delete

Name

BackSpace.png

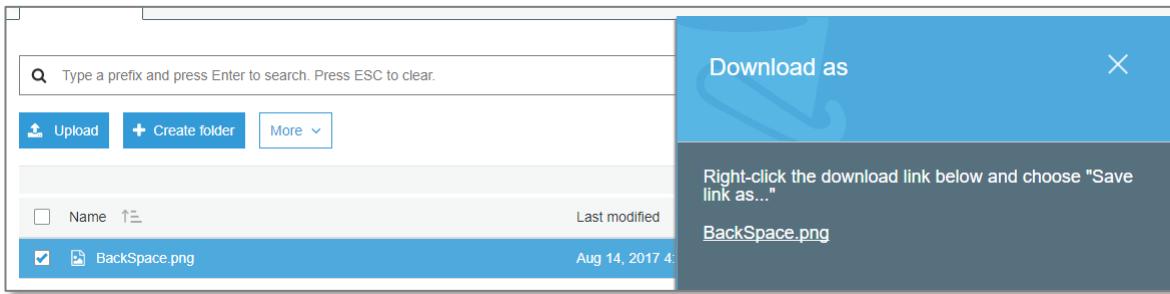
BackSpace.psd

Last modified

Aug 14, 2017

Aug 14, 2017

Click the download link to download the file.



## Troubleshooting

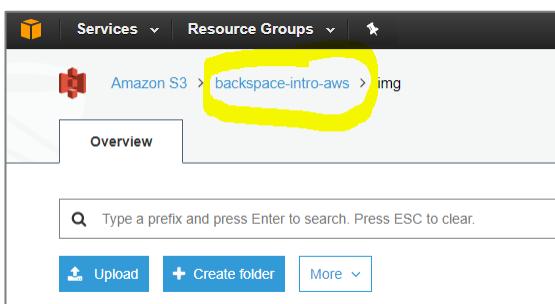
If you get the following screen it means you have clicked on the Object URL and not the download link as detailed above. You cannot access files directly from a URL as they have private access.



## Clean Up

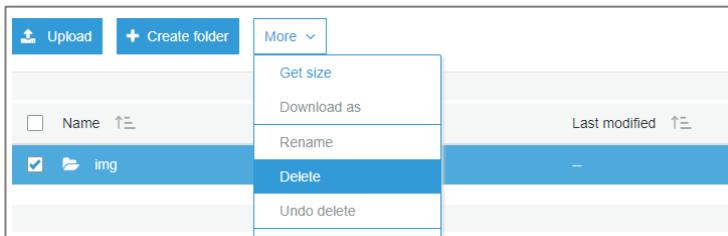
We will now delete the files and bucket so that you will not be billed by AWS.

Go back to your bucket by clicking its link.

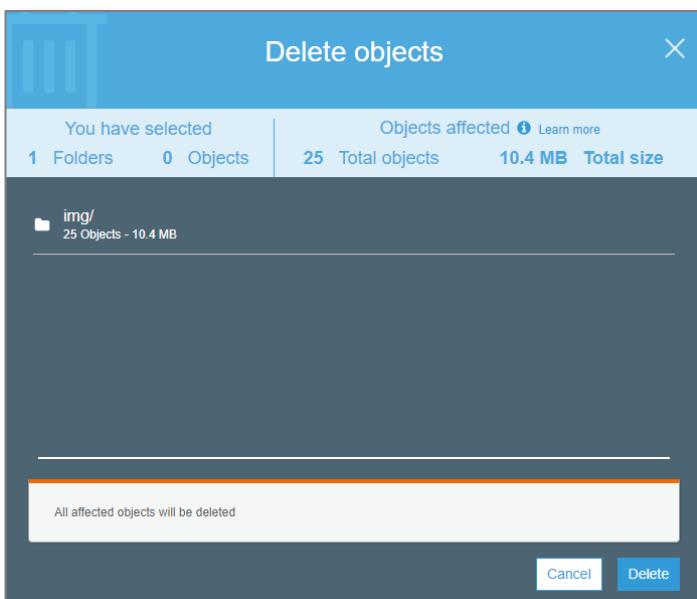


Select the folder

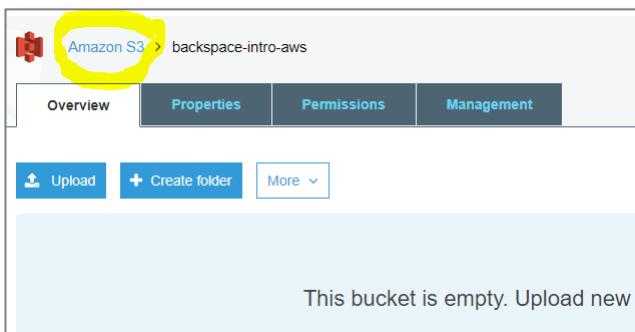
Select “More”, “Delete”



Click "Delete"



Go back to the S3 dashboard by clicking the link

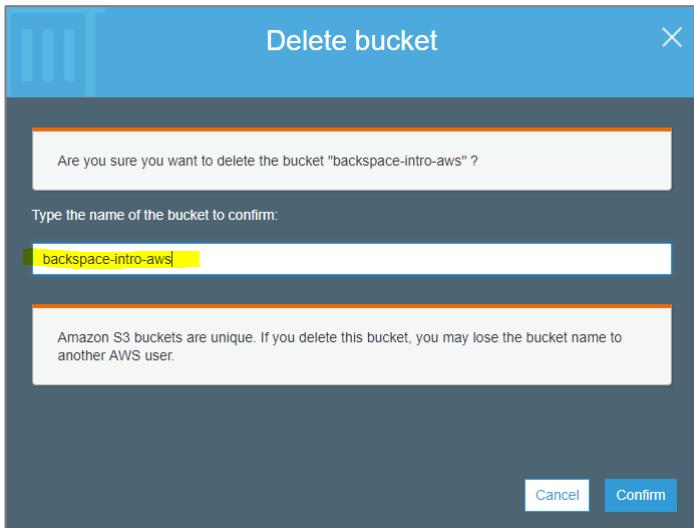


Click on the bucket line but not on the bucket link to select the bucket.

Click "Delete Bucket"

The screenshot shows the Amazon S3 console interface. At the top, there's a navigation bar with links to 'Switch to the old console', 'Discover the new console', and 'Quick tips'. Below the navigation is a search bar labeled 'Search for buckets'. Underneath the search bar are three buttons: '+ Create bucket', 'Delete bucket' (which is highlighted with a yellow box), and 'Empty bucket'. To the right of these buttons, it says '3 Buckets' and '1 Regions'. A circular icon is also present. Below this, a table lists one bucket: 'backspace-intro-aws'. The table has columns for 'Bucket name', 'Region', and 'Date created'. The bucket details are: 'backspace-intro-aws' (Bucket name), 'US East (N. Virginia)' (Region), and 'Aug 14, 2017 4:19:05 PM' (Date created). A large yellow circle highlights the entire row for the bucket.

Confirm the name of the bucket to delete



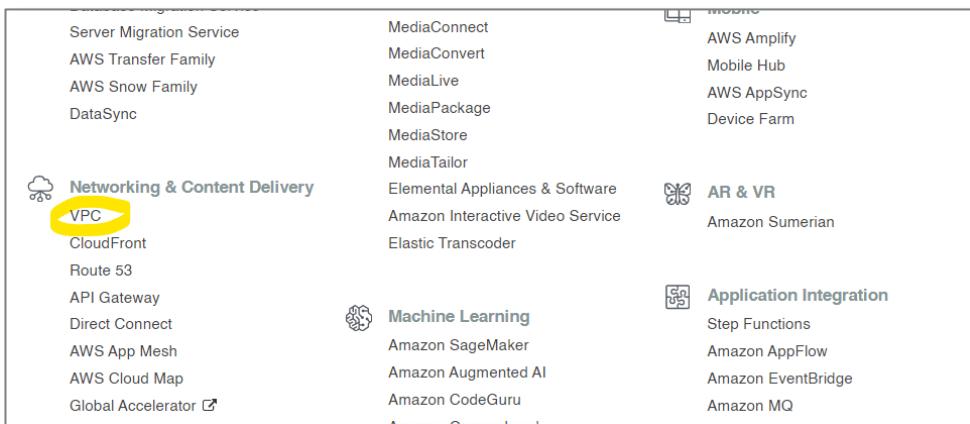
# Creating a SQL Database with RDS

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*

The screenshot shows the AWS VPC Security Groups page. On the left, there's a sidebar with various network-related options like Egress Only Internet Gateways, Carrier Gateways, DHCP Options Sets, Elastic IPs, Managed Prefix Lists, Endpoints, Endpoint Services, NAT Gateways, Peering Connections, and SECURITY (Network ACLs and Security Groups). The 'Security Groups' option is highlighted with a yellow circle. The main area displays a table titled 'Security Groups (26)'. The table has columns for Name, Security group ID, Security group name, VPC ID, and Description. A new row is being added, indicated by a dashed border and a 'Create security group' button at the top right of the table area, which is also highlighted with a yellow circle.

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

Give it a description

The screenshot shows the 'Create security group' dialog box. It has a 'Basic details' section. Under 'Security group name', the value 'backspace-rds-intro-lab' is entered, with a note below stating 'Name cannot be edited after creation.' Under 'Description', the value 'Inbound internet access to MySQL RDS.' is entered. At the bottom, under 'VPC', the value 'vpc-e4a1b39f (Default VPC)' is selected. Both the 'Security group name' and 'Description' fields are highlighted with a yellow circle.

Click *Add rule* for Inbound rules

Select type *MySQL/Aurora*

Select source *Anywhere*

Click *Create security group*

**Inbound rules** [Info](#)

Type	Protocol	Port range	Source	Description - optional
MySQL/Aurora	TCP	3306	Anywhere	
			0.0.0.0/0	<a href="#">Delete</a>
			::/0	<a href="#">Delete</a>

[Add rule](#)

**Outbound rules** [Info](#)

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	Custom	
			0.0.0.0/0	<a href="#">Delete</a>

[Add rule](#)

**Tags - optional**  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

[Add new tag](#)  
You can add up to 50 more tag

[Cancel](#) **Create security group**

Security group (sg-0f944f4fc960b6b | backspace-rds-intro-lab) was created successfully

Details

VPC > Security Groups > sg-0f944f4fc960b6b - backspace-rds-intro-lab

### sg-0f944f4fc960b6b - backspace-rds-intro-lab

Delete security group Copy to new security group

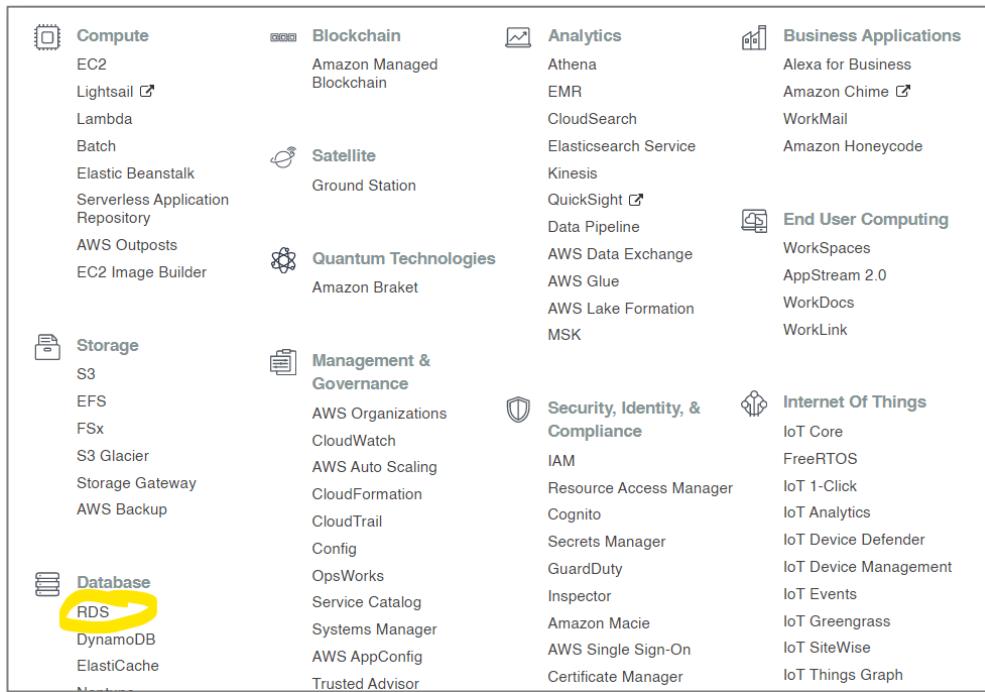
Details			
Security group name backspace-rds-intro-lab	Security group ID sg-0f944f4fc960b6b	Description Inbound internet access to MySQL RDS.	VPC ID vpc-e4a1b39f
Owner 361919435810	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules Outbound rules Tags

Inbound rules				
Type	Protocol	Port range	Source	Description - optional
MYSQL/Aurora	TCP	3306	0.0.0.0/0	-
MYSQL/Aurora	TCP	3306	::/0	-

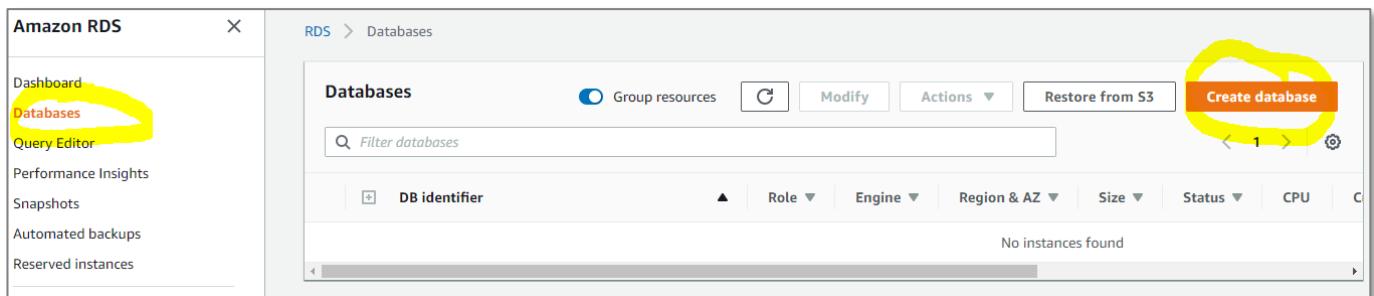
## Creating an RDS Database

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

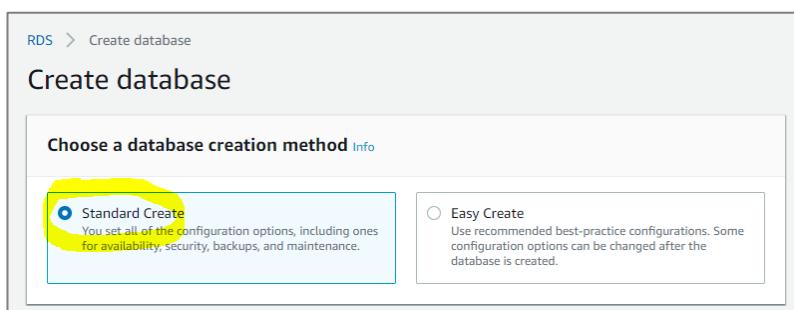


Select 'Databases'

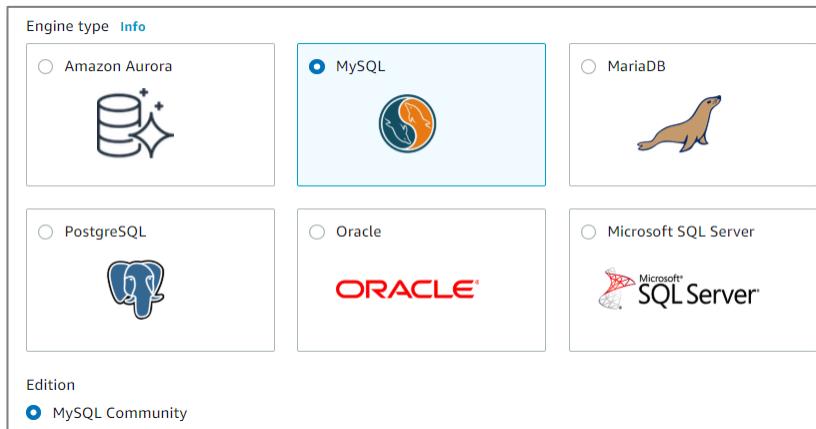
Select 'Create database'



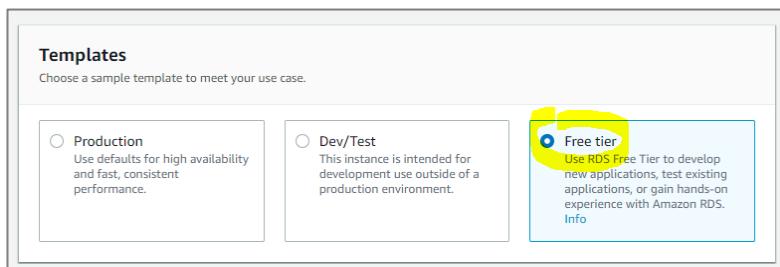
Select Standard Create



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)

**Settings**

**DB instance identifier** [Info](#)  
Type a name for your DB instance. The name must be unique cross all DB instances owned by your AWS account in the current AWS Region.

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens (1 to 15 for SQL Server). First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

**Credentials Settings**

**Master username** [Info](#)  
Type a login ID for the master user of your DB instance.

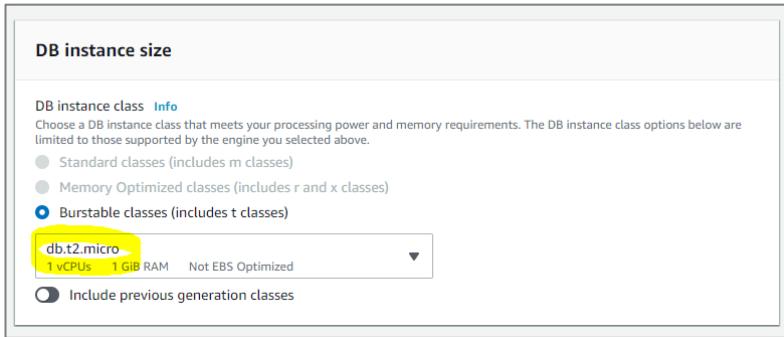
1 to 16 alphanumeric characters. First character must be a letter

Auto generate a password  
Amazon RDS can generate a password for you, or you can specify your own password

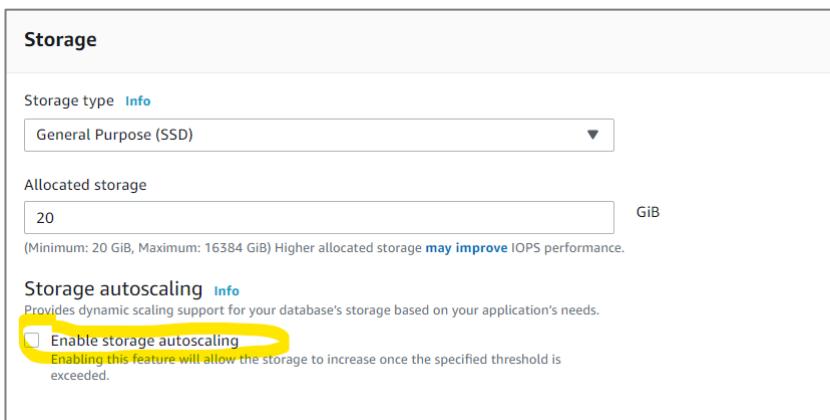
**Master password** [Info](#)  
  
Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), "(double quote) and @ (at sign).

**Confirm password** [Info](#)

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)

**Connectivity**

Virtual private cloud (VPC) [Info](#)  
VPC that defines the virtual networking environment for this DB instance.

Default VPC (vpc-e4a1b39f)

Only VPCs with a corresponding DB subnet group are listed.

**After a database is created, you can't change the VPC selection.**

▼ Additional connectivity configuration

Subnet group [Info](#)  
DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.

default

Public access [Info](#)

Yes  
Amazon EC2 instances and devices outside the VPC can connect to your database. Choose one or more VPC security groups that specify which EC2 instances and devices inside the VPC can connect to the database.

No  
RDS will not assign a public IP address to the database. Only Amazon EC2 instances and devices inside the VPC can connect to your database.

Existing VPC security groups

Choose VPC security groups

AutoScaling-Security-Group-1  
RedisSG  
WordPress Certified by Bitnami and Automattic-5-5-1-0 on Debian 10-AutogenByAWSMP-  
WebServerSG  
aws-cloud9-BackSpace-Labs-aa0e0177557d4b7da26fa3c1fe150530-InstanceSecurityGroup-1EQOMGDRQ5CW8  
LocalServerSG  
**backspace-rds-intro-lab**  
default

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

Existing VPC security groups

Choose VPC security groups

backspace-rds-intro-lab X default X

Availability Zone [Info](#)

No preference

Database port [Info](#)  
TCP/IP port that the database will use for application connections.

3306

Scroll down and expand *Additional configuration*

Enter a database name.

Uncheck *Enable automatic backups*

Leave all other options default.

**Additional configuration**  
Database options, backup disabled, backtrack disabled, Enhanced Monitoring disabled, maintenance, CloudWatch Logs, delete protection disabled

**Database options**

Initial database name [Info](#)  
test  
If you do not specify a database name, Amazon RDS does not create a database.

DB parameter group [Info](#)  
default.mysql5.7

Option group [Info](#)  
default:mysql-5-7

**Backup**  
Creates a point in time snapshot of your database

Enable automatic backups  
Enabling backups will automatically create backups of your database during a certain time window.

**Monitoring**

Enable Enhanced monitoring  
Enabling Enhanced monitoring metrics are useful when you want to see how different processes or threads use the CPU

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

Click 'Create database'

**Deletion protection**

Enable deletion protection  
Protects the database from being deleted accidentally. While this option is enabled, you can't delete the database.

**Estimated monthly costs**

The Amazon RDS Free Tier is available to you for 12 months. Each calendar month, the free tier will allow you to use the Amazon RDS resources listed below for free:

- 750 hrs of Amazon RDS in a Single-AZ db.t2.micro Instance.
- 20 GB of General Purpose Storage (SSD).
- 20 GB for automated backup storage and any user-initiated DB Snapshots.

[Learn more about AWS Free Tier.](#)

When your free usage expires or if your application usage exceeds the free usage tiers, you simply pay standard, pay-as-you-go service rates as described in the [Amazon RDS Pricing page](#).

Cancel **Create database**

Click on the database details link

The screenshot shows the AWS RDS Databases page. At the top, a message says "Creating database backspace-intro-aws. Your database might take a few minutes to launch." with a "View credential details" button. Below this, the "Databases" section has a "Create database" button. A yellow box highlights the "DB identifier" column, which lists "backspace-intro-aws". Another yellow box highlights the "Status" column, which shows "Creating".

Your instance will show status 'creating'.

The screenshot shows the AWS RDS Database instance page for "backspace-intro-aws". It includes a "Summary" table with the following data:

DB identifier	CPU	Info	Class
backspace-intro-aws	-	Creating	db.t2.micro
Role	Current activity	Engine	Region & AZ
Instance	0 Connections	MySQL Community	us-east-1f

## 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'

RDS > Databases > backspace-intro-aws

## backspace-intro-aws

**Summary**

DB identifier backspace-intro-aws	CPU -	Info Available	Class db.t2.micro
Role Instance	Current activity 0 Connections	Engine MySQL Community	Region & AZ us-east-1f

Scroll down and copy the database server endpoint

Connectivity & security | Monitoring | Logs & events | Configuration | Maintenance & backups | Tags

### Connectivity & security

<b>Endpoint</b> backspace-intro-aws.clbmnfz56wx.us-east-1.rds.amazonaws.com	<b>Networking</b> Availability zone us-east-1f  VPC Default VPC (vpc-e4a1b39f)  Subnet group default  Subnets subnet-557c9c6b subnet-7d09672 subnet-c94c9fe7 subnet-8bab79ec subnet-b13a5efb subnet-ec25f4b0	<b>Security</b> VPC security groups default (sg-7d1df536) ( active )  Public accessibility Yes  Certificate authority rds-ca-2015  Certificate authority date Mar 6th, 2020
--	--	--

Open the MySQL Workbench application click to add a new connection

MySQL Workbench

Welcome to MySQL Workbench

MySQL Workbench is the official graphical user interface (GUI) tool for MySQL. It allows you to design, create and browse your database schemas, work with database objects and insert data as well as design and run SQL queries to work with stored data. You can also migrate schemas and data from other database vendors to your MySQL database.

Browse Documentation >    Read the Blog >    Discuss on the Forums >

MySQL Connections

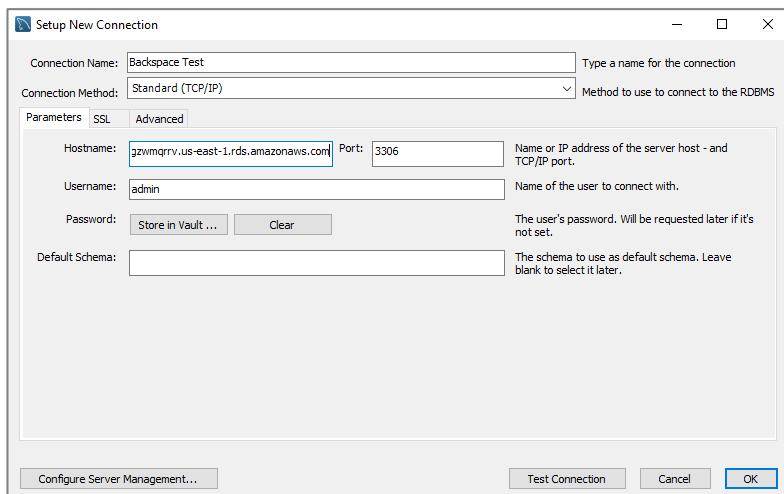
Give the connection a name.

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)

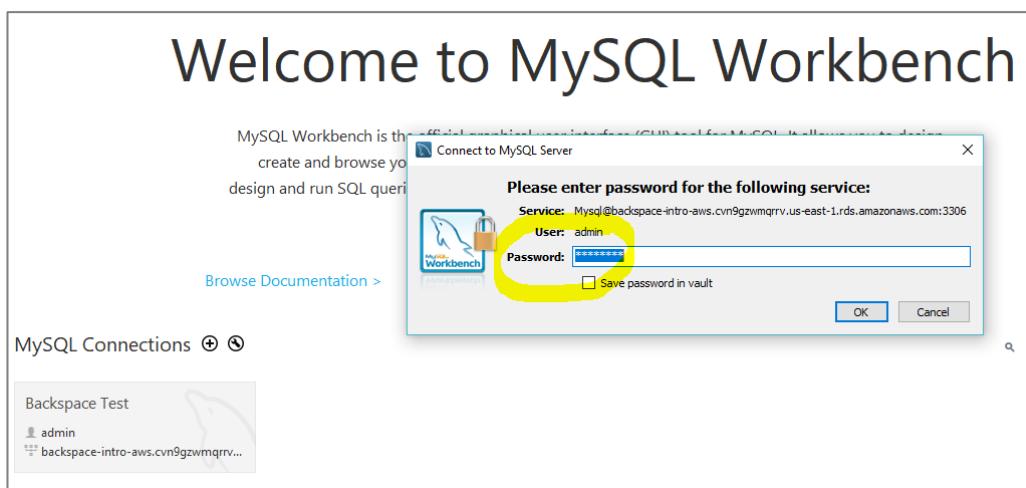
Click OK



Click on the Connection

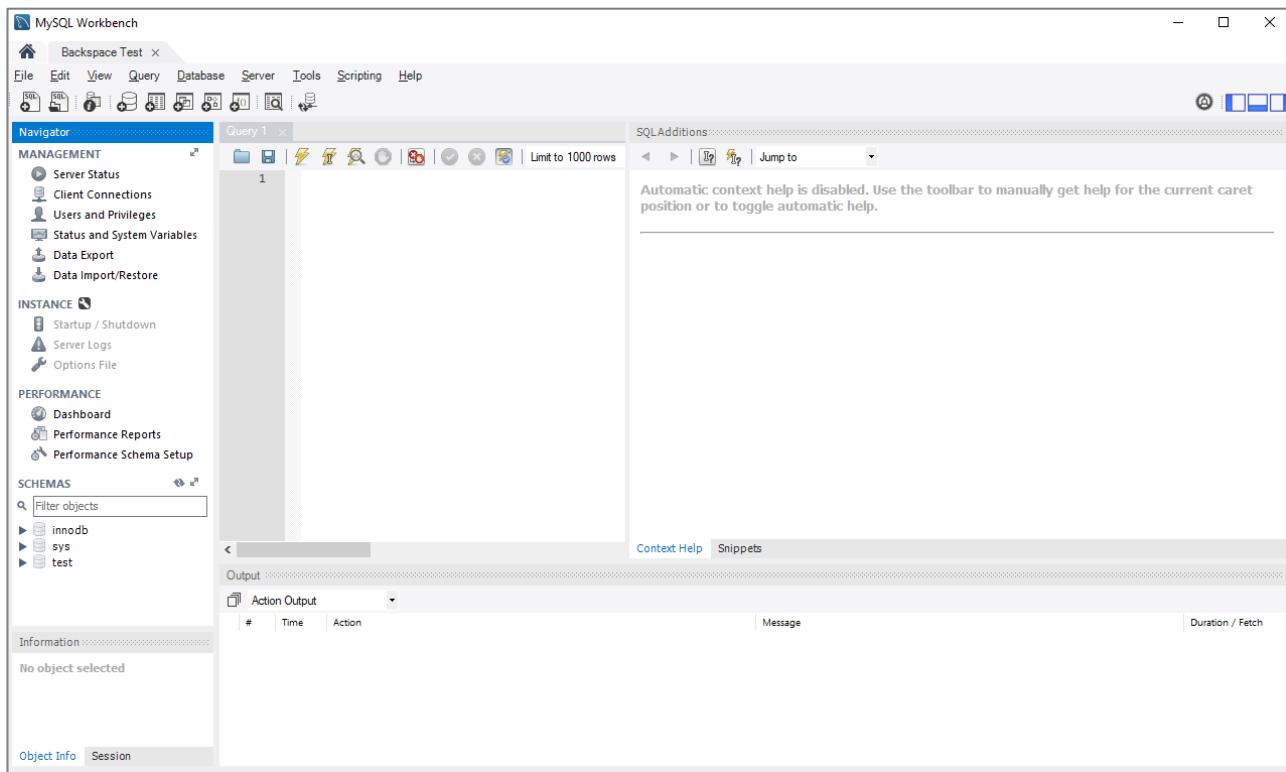


Enter the password you created in RDS for your master username

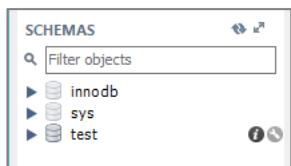


You will soon be connected to your database server

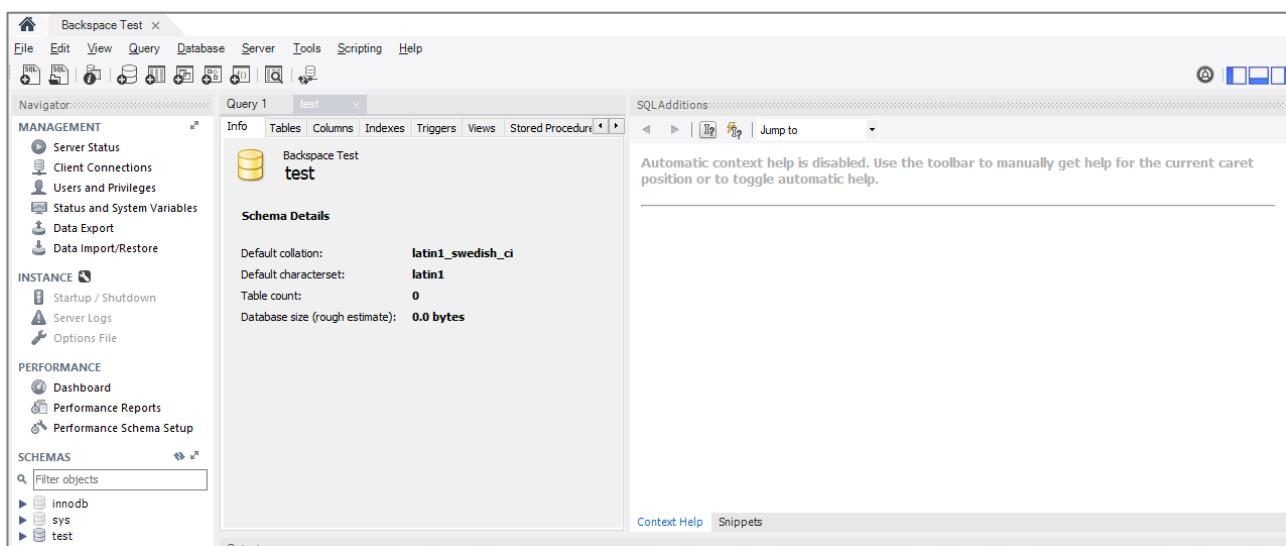
If you cannot connect then please see the 'Troubleshooting Connection Issues' below.



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.



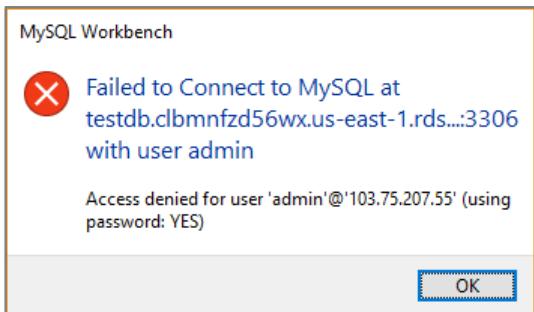
You then get an information screen for the database.



## Troubleshooting Connection Issues

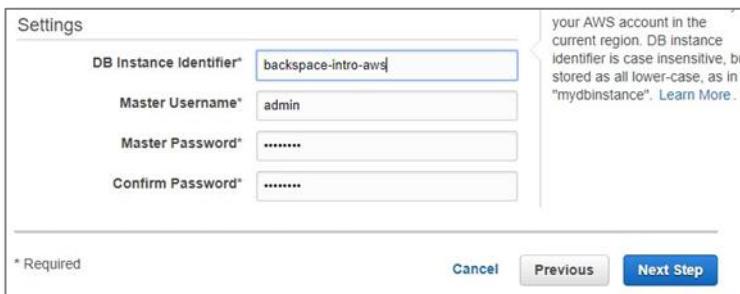
If you are getting connection errors then check the following:

### Wrong Username / Password

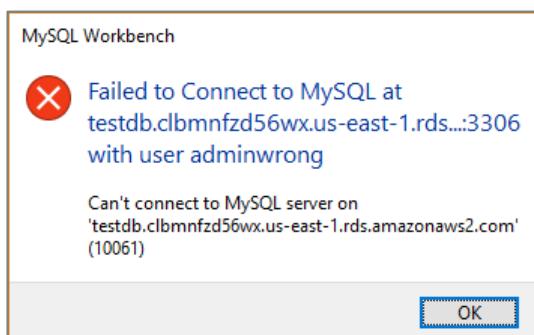


Make sure you use the correct username and password.

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



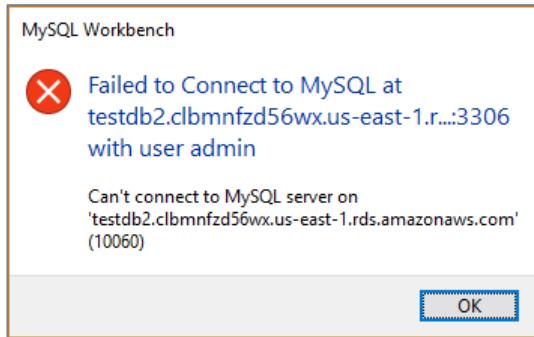
### Bad Connection String



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

The screenshot shows the "Connect" section of the AWS RDS console. It displays the endpoint, port (3306), and "Publicly accessible" status (Yes). Below this, the "Security group rules (2)" section is shown. A yellow circle highlights the first row of the table, which lists the security group "rds-launch-wizard-5 (sg-2e8b8e58)", the type "CIDR/IP - Inbound", and the rule "0.0.0.0/0".

Security group	Type	Rule
rds-launch-wizard-5 (sg-2e8b8e58)	CIDR/IP - Inbound	0.0.0.0/0
rds-launch-wizard-5 (sg-2e8b8e58)	CIDR/IP - Outbound	0.0.0.0/0

You will be taken to the EC2 console

Select the “Inbound” tab

Click “Edit”

The screenshot shows the AWS EC2 Dashboard with the 'Create Security Group' button at the top. On the left, there's a sidebar with various navigation links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, AMIs, and Elastic Block Store. The main area displays a table of security groups. One row is selected, showing 'sg-2e8b8e58' as the Name, 'rds-launch-wizard-5' as the Group Name, and 'vpc-72d25a0b' as the VPC ID. Below the table, a tab bar shows 'Description', 'Inbound' (which is highlighted with a yellow circle), 'Outbound', and 'Tags'. An 'Edit' button is also highlighted with a yellow circle. A table below lists a single rule: Type is 'Custom TCP Rule', Protocol is 'TCP', Port Range is '3306', and Source is '████████/32'.

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

This screenshot shows the 'Edit inbound rules' dialog box overlaid on the EC2 Security Groups page. The dialog has fields for Type (MySQL/Aurora), Protocol (TCP), Port Range (3306), and Source (which is highlighted with a yellow circle). The source dropdown is set to 'Anywhere' and the IP range is '0.0.0.0/0, ::/0'. There's also a note about edits deleting existing rules and creating new ones. At the bottom are 'Cancel' and 'Save' buttons.

### *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

RDS > Instances > backspace-intro-aws

### backspace-intro-aws

**Summary**

Engine	DB instance class info	DB instance status available
MySQL 5.6.39	db.t2.micro	

**CloudWatch (17)** Add instance to compare Monitoring ▾

Legend: backspace-intro-aws

CPU Utilization (Percent) DB Connections (Count)

Instance actions ▾

- Create read replica
- Create Aurora read replica
- Promote read replica
- Take snapshot
- Restore to point in time
- Migrate latest snapshot
- Modify
- Stop
- Reboot
- Delete**

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"

Are you sure you want to Delete the **backspace-intro-aws** DB Instance?

Create final snapshot?  
Determines whether a final DB Snapshot is created before the DB instance is deleted.

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

To confirm deletion, type *delete me* into the field  
**delete me**

⚠ We strongly recommend taking a final snapshot before instance deletion since after your instance is deleted, automated backups will no longer be available.

Cancel **Delete**

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

Amazon RDS

RDS > Instances

**Instances (1)**

DB instance	Engine	Status	CPU	Current activity
backspace-intro-aws	MySQL	<b>deleting</b>	1.17%	0 Conn

Filter instances

Instances

Clusters

Performance Insights PREVIEW

Snapshots

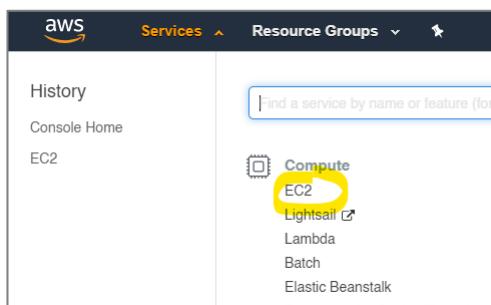
Reserved instances

Subnet groups

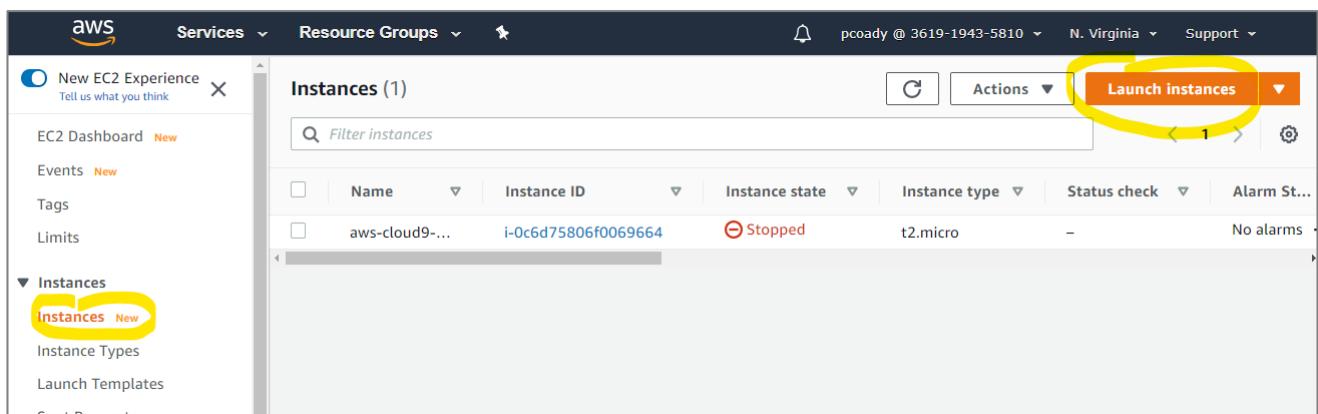
# Creating a Web Server with EC2

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

The screenshot shows the AWS Marketplace interface. At the top, there is a navigation bar with tabs: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, and 6. Continue. Below the navigation bar, the title "Step 1: Choose an Amazon Machine Image (AMI)" is displayed. A sub-instruction states: "An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance." On the left, there is a search bar with the text "WordPress" and a magnifying glass icon. Below the search bar is a sidebar with categories: Quick Start, My AMIs, AWS Marketplace (which is highlighted with a yellow circle), and Community AMIs. To the right of the sidebar, the "aws marketplace" logo is visible, along with a sub-instruction: "Find and buy software that runs in the AWS Cloud, software from trusted Marketplace products you are currently subscribed to by visiting Your Software Subscriptions." Below the sidebar, there is a "Featured Software" section.

## Select the Bitnami AMI

The screenshot shows the AWS Marketplace search results for "wordpress". The search bar at the top has "wordpress" typed into it. On the left, the sidebar shows categories: Quick Start (0), My AMIs (0), AWS Marketplace (148) (which is highlighted with a yellow circle), and Community AMIs (1010). In the main content area, a product card for "WordPress Certified by Bitnami and Automattic" is displayed. The card includes a star rating of ★★★★☆ (121), a release date of 8/26/20, and a description stating it's a "Free tier eligible" Linux/Unix, Ubuntu 10 | 64-bit (x86) Amazon Machine Image (AMI). A "Select" button is highlighted with a yellow circle. At the bottom of the page, there are navigation links: "1 to 10 of 148 Products" and "Next >".

## Click Continue

The screenshot shows the "WordPress Certified by Bitnami" product details page. At the top, the title "WordPress Certified by Bitnami" is displayed. On the left, there is a "Free tier eligible" badge, a large Bitnami logo, and sections for "Product Details" (By Bitnami, Customer Rating ★★★★☆ (117), Latest Version 5.4.1-0-r01 on Debian 10, Base Operating System Linux/Unix, Debian 10, Delivery Method 64-bit (x86) Amazon Machine Image (AMI), License Agreement End User License Agreement, On Marketplace Since 9/17/14), "Highlights" (Jetpack plugin is included by default offering access to additional professional themes, performance improvements and marketing tools), and "Pricing Details". The "Pricing Details" section shows a table of "Hourly Fees" for various instance types. The "Continue" button at the bottom right is highlighted with a yellow circle.

Instance Type	Software	EC2	Total
t2.micro	\$0.00	\$0.012	\$0.012/hr
t2.small	\$0.00	\$0.023	\$0.023/hr
t2.medium	\$0.00	\$0.046	\$0.046/hr
t2.large	\$0.00	\$0.093	\$0.093/hr
t2.xlarge	\$0.00	\$0.186	\$0.186/hr
t2.2xlarge	\$0.00	\$0.371	\$0.371/hr
t3a.micro	\$0.00	\$0.009	\$0.009/hr
t3a.small	\$0.00	\$0.019	\$0.019/hr
t3a.medium	\$0.00	\$0.038	\$0.038/hr
t3a.large	\$0.00	\$0.075	\$0.075/hr
t3a.xlarge	\$0.00	\$0.15	\$0.15/hr
t3a.2xlarge	\$0.00	\$0.301	\$0.301/hr
t3.micro	\$0.00	\$0.01	\$0.01/hr
t3.small	\$0.00	\$0.021	\$0.021/hr
t3.medium	\$0.00	\$0.042	\$0.042/hr
t3.large	\$0.00	\$0.083	\$0.083/hr
t3.xlarge	\$0.00	\$0.166	\$0.166/hr
t3.2xlarge	\$0.00	\$0.332	\$0.332/hr

Choose the **t3 Micro** instance.

Click Next: Configure Instance Details

Step 2: Choose an Instance Type

	General purpose	t3a.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	General purpose	t3a.small	2	2	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	General purpose	t3a.medium	2	4	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	General purpose	t3a.large	2	8	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	General purpose	t3a.xlarge	4	16	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	General purpose	t3a.2xlarge	8	32	EBS only	Yes	Up to 5 Gigabit	Yes
<input checked="" type="checkbox"/>	General purpose	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
<input checked="" type="checkbox"/>	General purpose	t3.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	General purpose	t3.small	2	2	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	General purpose	t3.medium	2	4	EBS only	Yes	Up to 5 Gigabit	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

Select enable for Auto-assign Public IP

Click Next: Add Storage

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	1	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot Instances	
Network	vpc-e4a1b39f   Default VPC (default)	<input type="button"/> Create new VPC
Subnet	No preference (default subnet in any Availability Zone)	<input type="button"/> Create new subnet
Auto-assign Public IP	Enable	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open	<input type="button"/> Create new Capacity Reservation
IAM role	None	<input type="button"/> Create new IAM role
Shutdown behavior	Stop	
Stop - Hibernate behavior	<input type="checkbox"/> Enable hibernation as an additional stop behavior	
Enable termination protection	<input type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring	

Cancel Previous Review and Launch Next: Add Storage

## Click Next: Add Tags

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-01235d3cf67b2c8f8	10	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Cancel Previous Review and Launch **Next: Add Tags**

## Click click to add a Name tag

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 instances.

Key	(128 characters maximum)	Value	(256 characters maximum)
This resource currently has no tags. Choose the Add tag button or <a href="#">click to add a Name tag</a> . Make sure your <a href="#">IAM policy</a> includes permissions to create tags.			

Add Tag (Up to 50 tags maximum)

Give it a name and click Next: Configure Security Group

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

Key	(128 characters maximum)	Value	(256 characters maximum)
Name		backspace-lab-intro-ec2	<input type="button" value="X"/>
<a href="#">Add another tag</a> (Up to 50 tags maximum)			

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

Click Review and Launch

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group:  Create a **new** security group  Select an **existing** security group

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom	0.0.0.0/0
HTTP	TCP	80	Custom	0.0.0.0/0
HTTPS	TCP	443	Custom	0.0.0.0/0

[Add Rule](#)

**Warning**  
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

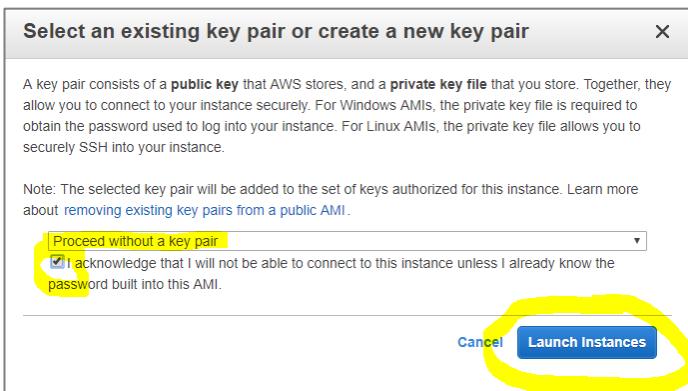
[Cancel](#) [Previous](#) [Review and Launch](#)

Click Launch

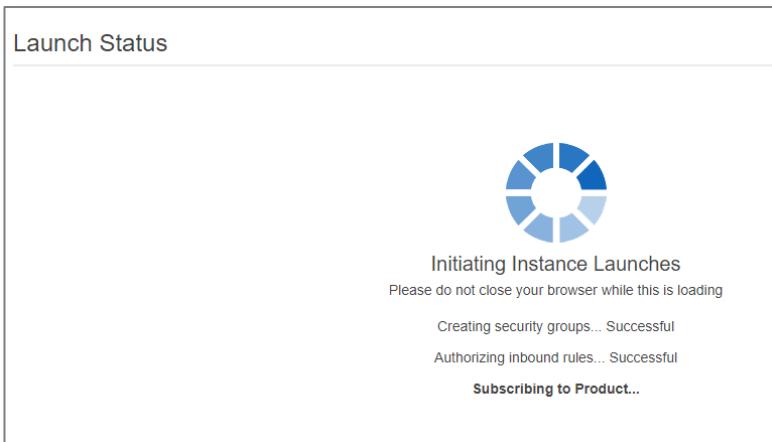
Select “Proceed without a key pair”

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.

The screenshot shows the AWS EC2 Instances page with one instance listed:

Name	Instance ID	Instance state	Instance type	Status check
backspace-lab-intro-ec2	i-00f5796aa6147804c	Running	t2.micro	2/2 checks ...

Two specific fields are highlighted with yellow circles: the Instance ID (i-00f5796aa6147804c) and the Status check (2/2 checks ...).

Open the public IP address of your web server.

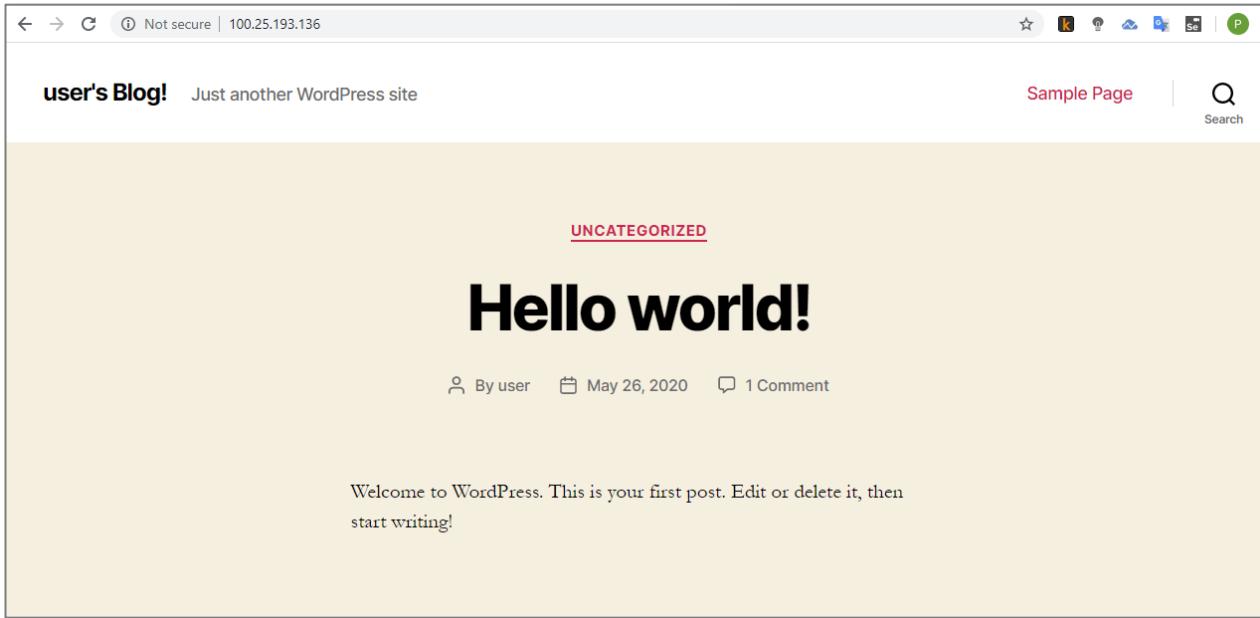
The screenshot shows the Instance summary for the instance i-00f5796aa6147804c. The Public IPv4 address (54.90.46.123) is highlighted with a yellow circle.

Instance ID	Public IPv4 address	Private IPv4 addresses
i-00f5796aa6147804c (backspace-lab-intro-ec2)	54.90.46.123   open address	172.31.59.91

Other details shown include:

- Instance state: Running
- Instance type: t2.micro
- Public IPv4 DNS: ec2-54-90-46-123.compute-1.amazonaws.com | open address
- VPC ID: Not explicitly shown in the table, but implied by the context.

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

The screenshot shows the 'Security' tab of a Lambda function's configuration. It includes sections for 'Security details' and 'Inbound rules'. The 'Inbound rules' section displays a table with three rows:

Port range	Protocol	Source	Security groups	WordPr
80	TCP	0.0.0.0/0	WordPress Certified by Bitnami and ...	true
22	TCP	0.0.0.0/0	WordPress Certified by Bitnami and ...	true
443	TCP	0.0.0.0/0	WordPress Certified by Bitnami and ...	true

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

The screenshot shows the 'Security' tab of a Lambda function's configuration. It includes sections for 'Security details' and 'Inbound rules'. The 'Security details' section shows the IAM role and owner information. The 'Inbound rules' section is partially visible at the bottom.

Click on the Inbound rules tab

Click on Edit

EC2 Dashboard [New](#)

Events [New](#)

Tags

Reports

Limits

**INSTANCES**

- Instances
- Instance Types
- Launch Templates
- Spot Requests
- Savings Plans
- Reserved Instances
- Dedicated Hosts [New](#)
- Scheduled Instances
- Capacity Reservations

**IMAGES**

Security Groups (1/1) [Info](#)

Filter security groups

Security group ID: sg-02f48599856e178be [X](#) Clear filters

Security group ID	Security group name	VPC ID	Description
sg-02f48599856e178be	WordPress Certified by...	vpc-e4a1b39f <a href="#">X</a>	This security group wa...

sg-02f48599856e178be - WordPress Certified by Bitnami-5-4-1-0-r01 on Debian 10-AutogenByAWSMP-

Details Inbound rules Outbound rules Tags

Inbound rules [Edit inbound rules](#)

Add a rule for HTTP and Anywhere

Click Save rules

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules [Info](#)

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>
HTTP <a href="#">X</a>	TCP	80	Anywhere <a href="#">▼</a>	0.0.0.0/0 <a href="#">X</a>
				::/0 <a href="#">X</a>

Add rule

**NOTE:** Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

Cancel Preview changes [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.

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with various navigation options like EC2 Dashboard, Events, Tags, Limits, Instances (which is selected and has its own sub-menu for Instances and Instance Types), Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, and Images. The main area displays two instances: 'backspace-lab-intro-ec2' (Instance ID: i-00f5796aa6147804c, State: Running) and 'aws-cloud9-BackSpace...' (Instance ID: i-0c6d75806f0069664, State: Stopped). A context menu is open over the running instance, with 'Actions' at the top followed by 'View details', 'Connect', 'Get Windows password', 'Create template from instance', 'Launch more like this', 'Manage tags', 'Instance state' (which has 'Instance settings' under it), 'Networking', 'Image', and 'Monitoring'. The 'Get system log' option is highlighted with a yellow circle.

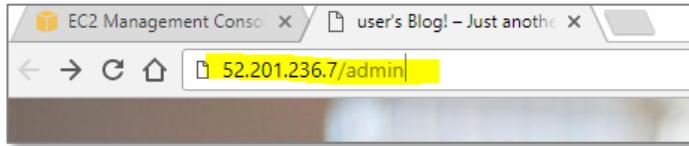
Scroll up until you find the log entry for the application username and password and copy it.

The screenshot shows the 'Get system log' page for instance i-00f5796aa6147804c. The log output is displayed in a scrollable text area. One notable entry is:

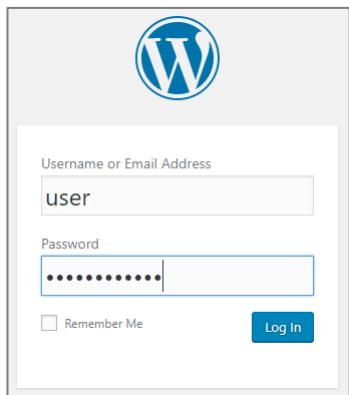
```
[ 75.570363] bitnami[536]: #      Setting Bitnami application password to '4UB0VEI2FAV1' #  
[ 75.577887] bitnami[536]: #      (the default application username is 'user') #  
[ 75.584063] bitnami[536]: #
```

This indicates that the application password has been successfully set to '4UB0VEI2FAV1'.

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

Welcome to WordPress!

We've assembled some links to get you started:

**Get Started**

- Customize Your Site
- or, [change your theme completely](#)

**Next Steps**

- Write your first blog post
- Add an About page
- Set up your homepage
- View your site

**More Actions**

- Manage widgets
- Manage menus
- Turn comments on or off
- Learn more about getting started

**Jetpack**

Simplify your site security and performance with Jetpack

Jetpack protects you against brute force attacks and unauthorized logins. Basic protection is always free, while premium plans add unlimited backups of your whole site, spam protection, malware scanning, and automated fixes.

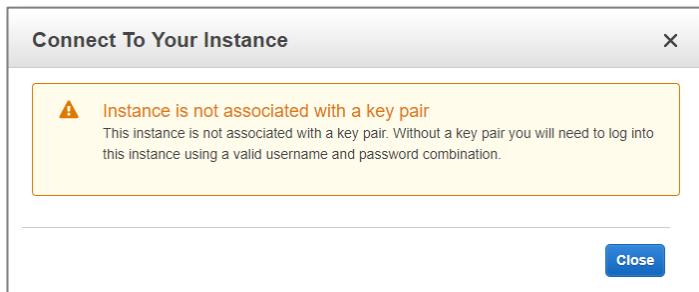
Activate site accelerator tools and watch your page load times decrease—we'll optimize your images and serve them from our own powerful global network of servers, and speed up your mobile site to reduce bandwidth usage.

**Set up Jetpack**

By clicking the Set up Jetpack button, you agree to our [Terms of Service](#) and to [share details](#) with WordPress.com.

## Troubleshooting logging in to the WordPress application

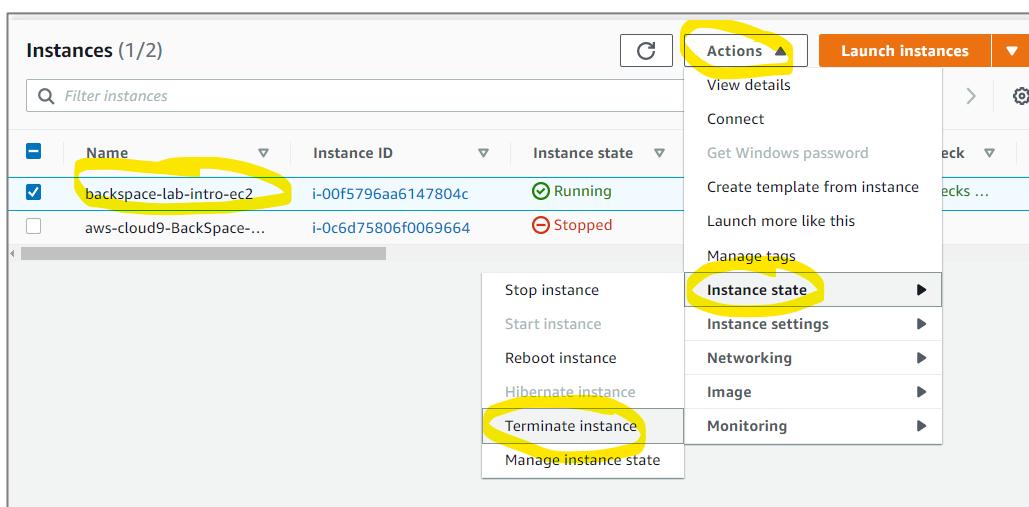
If you get the following message:



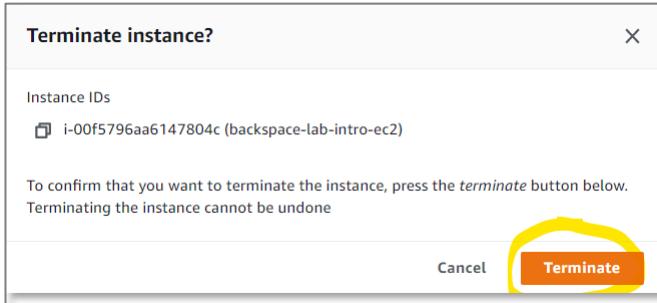
You have tried to connect to the Linux operating system by clicking on “Connect”. Do not click on connect, select “Actions – “Instance settings” - “Get System Log” as detailed previously.

## 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*

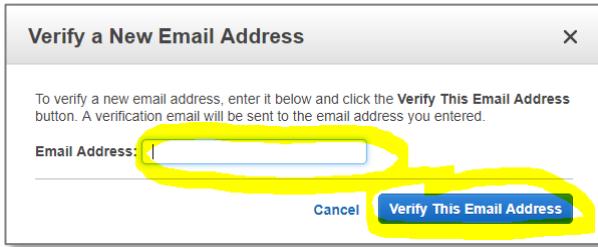
Click on 'Email addresses'

Find a service by name or feature (for example, EC2, S3 or VM, storage).			
Simple Email Service	Amazon AppFlow	Ground Station	Resource Access Manager
Console Home	Amazon Augmented AI	GuardDuty	Route 53
Billing	Amazon Braket	Certificate Manager	
EC2	Amazon Chime	Cloud9	I
	Amazon CodeGuru	CloudFormation	IAM
	Amazon Comprehend	CloudFront	Inspector
	Amazon Connect	CloudHSM	IoT 1-Click
	Amazon DocumentDB	CloudSearch	IoT Analytics
	Amazon EventBridge	CloudTrail	IoT Core
	Amazon Forecast	CloudWatch	IoT Device Defender
	Amazon Fraud Detector	CodeArtifact	IoT Device Management
	Amazon GameLift	CodeBuild	IoT Events
	Amazon Honeycode	CodeCommit	IoT Greengrass
	Amazon Interactive Video Service	CodeDeploy	IoT SiteWise
	Amazon Kendra	CodePipeline	IoT Things Graph
		CodeStar	
		Cognito	
		Config	
		Kinesis	
		Lambda	S
		Machine Learning	S3
		Media Services	S3 Glacier
		MQ	Secrets Manager
		MTurk	Security Hub
		Nimble Studio	Server Migration Service
		OpsWorks	Serverless Application Repository
		Pinpoint	Service Catalog
		Rekognition	Simple Email Service
		Rekognition Custom Labels	Simple Notification Service
		Rekognition Video	Simple Queue Service
		Transcribe	
		Transcribe Medical	
		Voice ID	
		WorkLink	
		WorkMail	
		WorkSpaces	
		WorkSpaces Web	
		XRay	
		Yield	

Click on 'Verify a New Email Address'

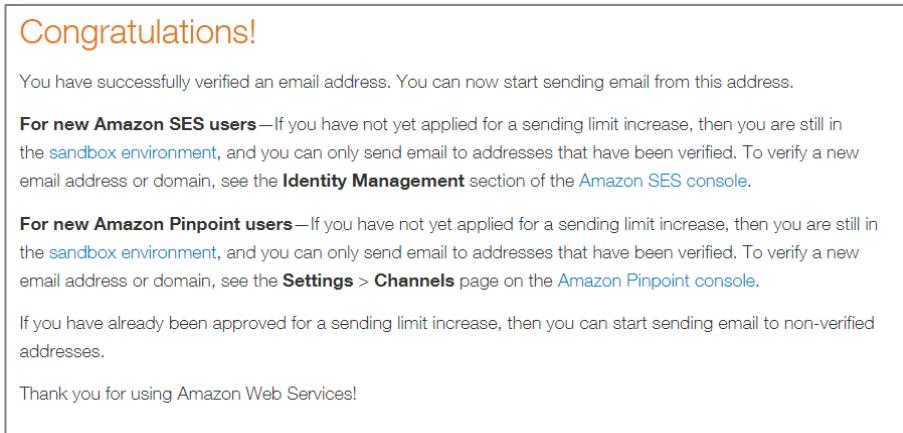
The screenshot shows the AWS SES console. On the left, a sidebar lists navigation options: SES Home, Identity Management, Domains, Email Addresses (which is highlighted with a yellow oval), and Email Sending, Sending Statistics, Dedicated IPs, and Configuration Sets. The main content area has a header with buttons for 'Verify a New Email Address' (highlighted with a yellow oval), 'Send a Test Email', 'Remove', and 'View Details'. Below this is a search bar labeled 'Search email addresses' and a dropdown menu set to 'All identities'. A section titled 'Email Address Identities' contains a message stating 'You have not verified any email addresses.' and a note to 'To verify a email address, click the Verify a New Email Address button above.'

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

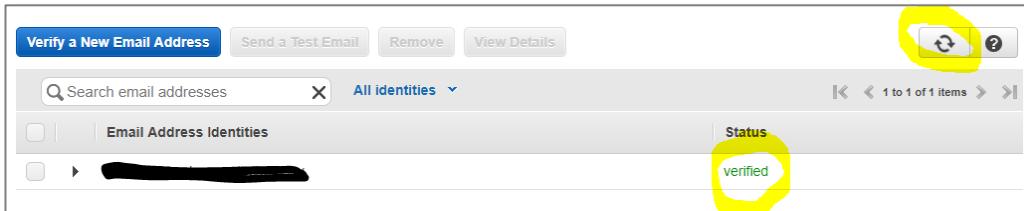


When you receive your verification email click on the supplied link.

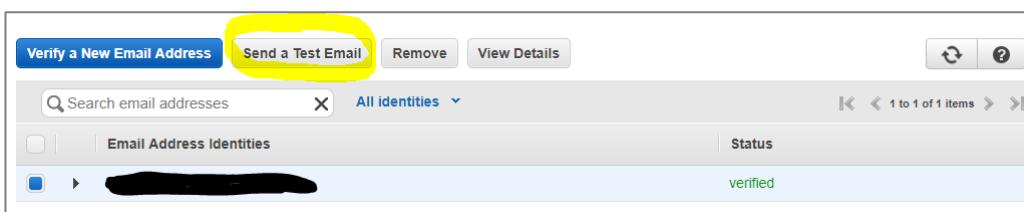
You will then receive a success page



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

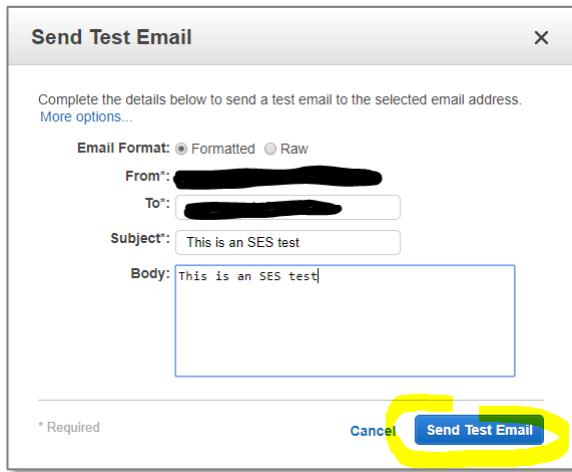


Click on the email address and select 'Send a test email'



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'

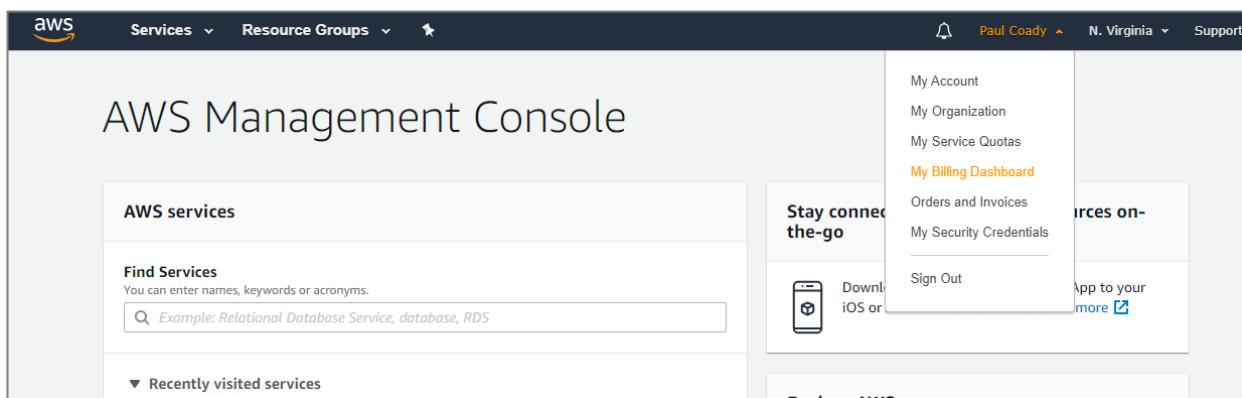
The screenshot shows the "Your Amazon SES Sending Limits" section of the AWS SES console. On the left is a navigation menu with "Sending Statistics" selected. A callout box points to the "Request a Sending Limit Increase" button, which is highlighted with a yellow circle. The main area displays a message about sandbox access and a link to learn more.

# ▶ 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.



The screenshot shows the AWS Management Console homepage. At the top right, there is a user dropdown menu with the name "Paul Coady" and a "N. Virginia" region selection. A dropdown arrow points to a list of options: "My Account", "My Organization", "My Service Quotas", "My Billing Dashboard" (which is highlighted in orange), "Orders and Invoices", and "My Security Credentials". Below this list, there are links for "Stay connected-the-go" (with "Download iOS or Android app" and "Sign Out"), and "Explore AWS". On the left side of the page, there is a sidebar titled "AWS services" with a "Find Services" search bar and a "Recently visited services" section.

Select *Billing Preferences*

Check *Receive Free Tier Usage Alerts*

Check *Receive Billing Alerts*

**IMPORTANT: Upcoming change to the Detailed Billing Report (DBR) and the Detailed Billing Report with Resources & Tags (DBR-RT)**

On June 15, 2019, AWS will be changing the way unused reservation costs are presented in the legacy Detailed Billing Reports. If you currently use the DBR or DBR-RT portions of your reservation costs, then you should begin using the AWS Cost & Usage Reports. [Learn more](#)

## Preferences

- Billing Preferences**
  - Receive PDF Invoice By Email**  
Turn on this feature to receive a PDF version of your invoice by email. Invoices are generally available within the first three days of the month.
  - Disable credit sharing**  
When credit sharing is disabled, credits will only be applied to the credit owner's account, and will not be shared across accounts in the same billing family. [Download credit preference history](#).
  - RI discount sharing**
- Cost Management Preferences**
  - Receive Free Tier Usage Alerts**  
Turn on this feature to receive email alerts when your AWS service usage is approaching, or has exceeded, the AWS Free Tier usage limits. If you wish to receive these email address that is not the primary email address associated with this account, please specify the email address below.
  - Email Address:
  - Receive Billing Alerts**  
Turn on this feature to monitor your AWS usage charges and recurring fees automatically, making it easier to track and manage your spending on AWS. You can set up to receive email notifications when your charges reach a specified threshold. Once enabled, this preference cannot be disabled. [Manage Billing Alerts](#) or [try the new budget](#)

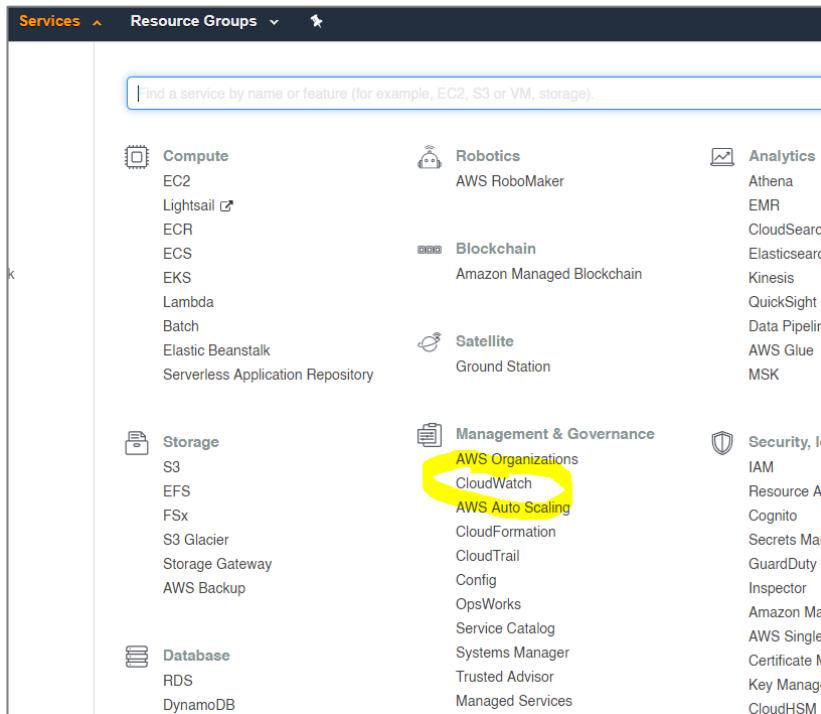
**Detailed Billing Reports [Legacy]**

**Save preferences**

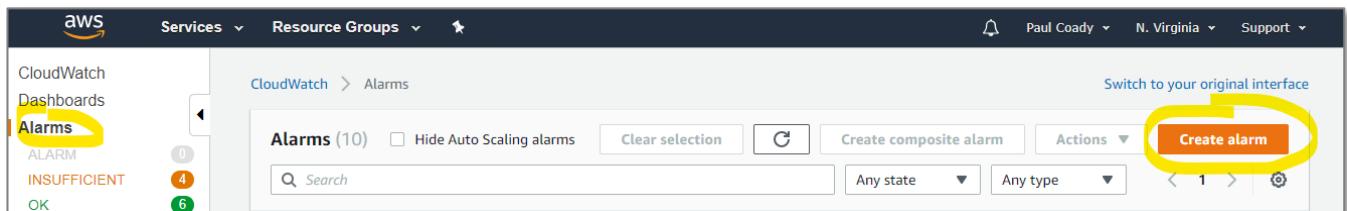
Click *Save preferences*

## Creating a CloudWatch Alarm

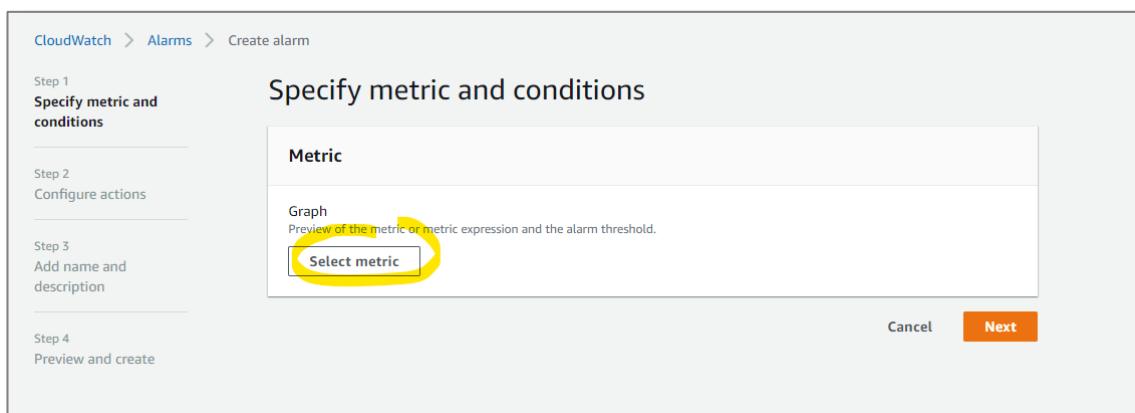
Click the Services menu and select 'CloudWatch' from 'Management & Governance'



Click on 'Alarms", 'Create Alarm"

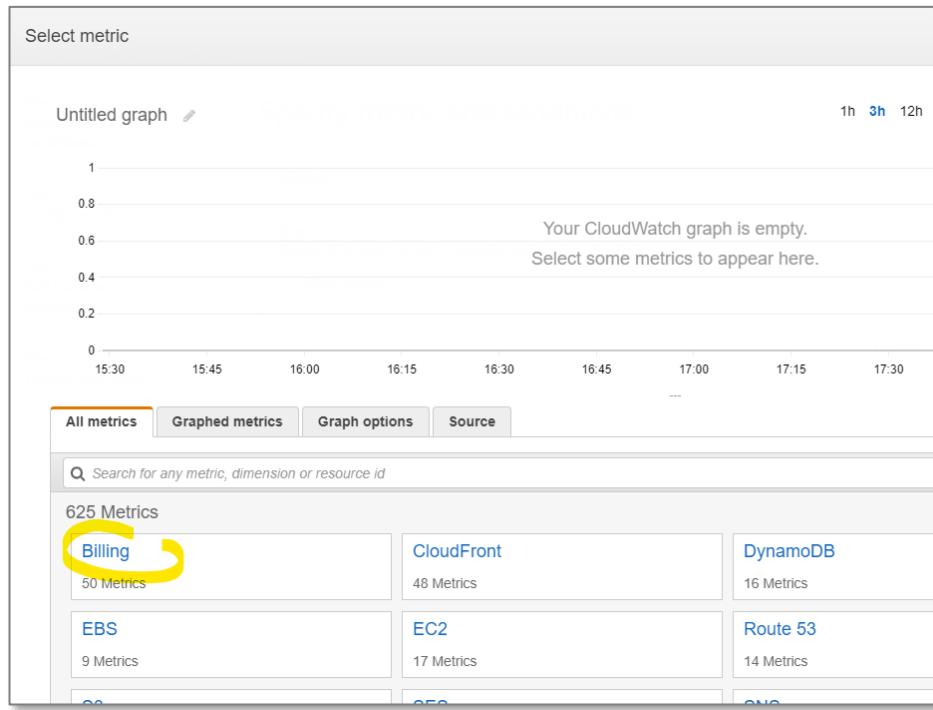


Click Select metric



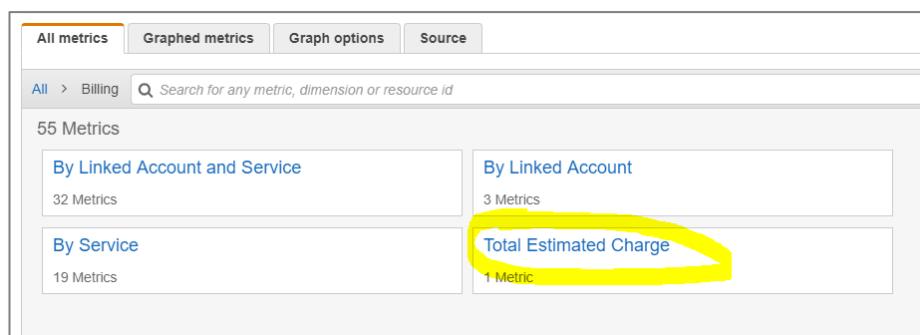
Search Billing

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.



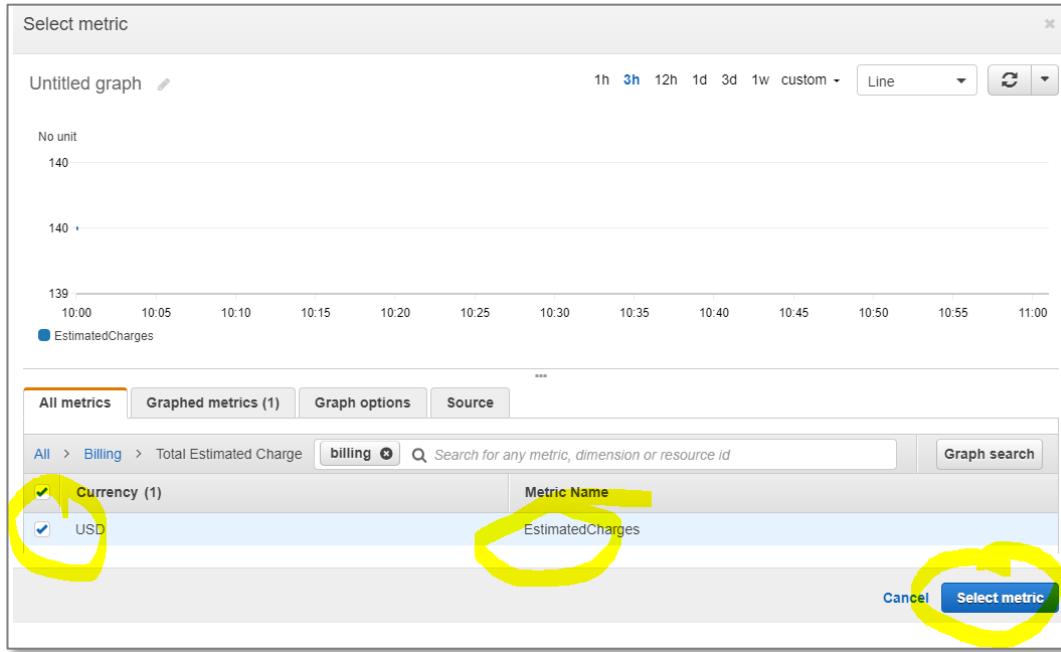
If you do not see any billing metrics it is most probably you are not operating in the US-East1 (N. Virginia) region. Please ensure you always operate from the US-East region during the course.

Select *Total Estimated Charge* from the billing metrics.



Select EstimatedCharges metric

### Click *Select metric*



Set the alarm threshold to not exceed \$10

Click Next

CloudWatch > Alarms > Create alarm

Step 1 Specify metric and conditions

Step 2 Configure actions

Step 3 Add name and description

Step 4 Preview and create

## Specify metric and conditions

**Metric**

Graph  
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 6 hours.

No unit

Namespaces  
AWS/Billing

Metric name: EstimatedCharges

Currency: USD

Statistic: Maximum

Period: 6 hours

**Conditions**

Threshold type:

- Static Use a value as a threshold
- Anomaly detection Use a band as a threshold

Whenever EstimatedCharges is...

Define the alarm condition:

- Greater > threshold
- Greater/Equal >= threshold
- Lower/Equal <= threshold
- Lower < threshold

than... Define the threshold value.

10 USD

Must be a number

Additional configuration

Cancel **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*

CloudWatch > Alarms > Create alarm

**Configure actions**

Step 1 Specify metric and conditions

Step 2 Configure actions

Step 3 Add name and description

Step 4 Preview and create

**Notification**

Alarm state trigger Define the alarm state that will trigger this action.

In alarm The metric or expression is outside of the defined threshold.

OK The metric or expression is within the defined threshold.

Insufficient data The alarm has just started or not enough data is available.

**Select an SNS topic**  
Define the SNS (Simple Notification Service) topic that will receive the notification.

Select an existing SNS topic

Create new topic

Use topic ARN

Create a new topic...  
The topic name must be unique.  
pcoady-Account-Billing-Alert

SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores (\_).

Email endpoints that will receive the notification...  
Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.

[REDACTED]  
user1@example.com, user2@example.com

**Create topic**

**Add notification**

Click Next

Send a notification to...

pcoady-Account-Billing-Alert x

Only email lists for this account are available

Email (endpoints)

**aws@backspace.academy** - View in SNS Console ↗

**Add notification**

**Auto Scaling action**

**Add Auto Scaling action**

**EC2 action**

This action is only available for EC2 Per-Instance Metrics

**Add EC2 action**

**Cancel** **Previous** **Next**

Give the alarm a unique name

Click Next

CloudWatch > Alarms > Create alarm

Step 1  
Specify metric and conditions

Step 2  
Configure actions

Step 3  
**Add a description**

Step 4  
Preview and create

### Add a description

Name and description

Define a unique name

Alarm name

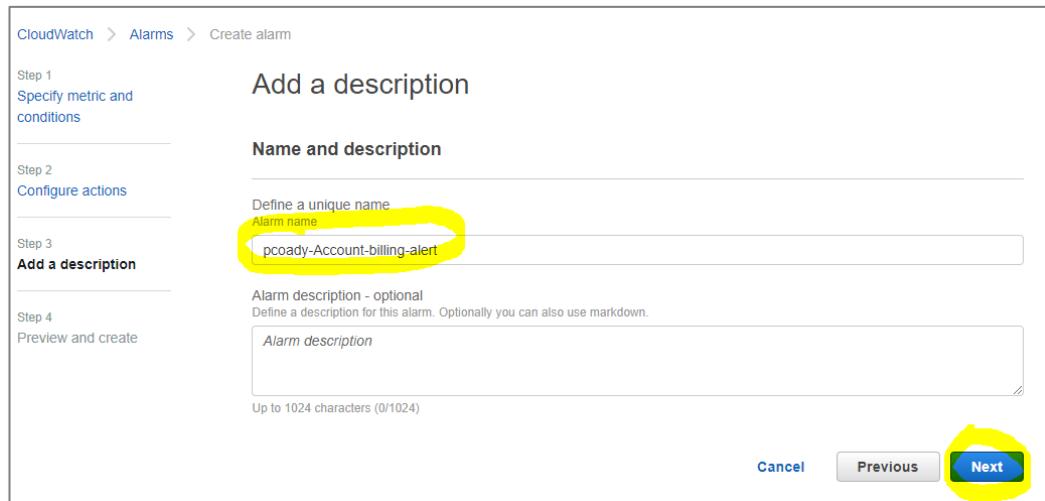
Alarm description - optional

Define a description for this alarm. Optionally you can also use markdown.

Alarm description

Up to 1024 characters (0/1024)

Cancel Previous **Next**



Click *Create alarm*

Step 4  
Preview and create

EstimatedCharges

Namespace: AWS/Billing  
Metric name: EstimatedCharges  
Currency: USD  
Statistic: Maximum  
Period: 6 hours

**Conditions**

Threshold type: Static  
Whenever EstimatedCharges is Greater (>) than... 10

► Additional configuration

Step 2: Configure actions Edit

**Actions**

Notification  
When in Alarm, send a notification to "pcoady-Account-Billing-Alert"

Step 3: Add a description Edit

**Name and description**

Name	Description
pcoady-Account-billing-alert	

Cancel Previous Create alarm

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

Search Current Mailbox Current Mailbox

All Unread By Date ↑

Today

AWS Notifications AWS Notification - Subscr... 1:34 PM You have chosen to

AWS Notifications AWS Notification - Subscr... 1:31 PM You have chosen to

Udemy Join in! Your course Amazon 10:03 AM

**AWS Notification - Subscription Confirmation**

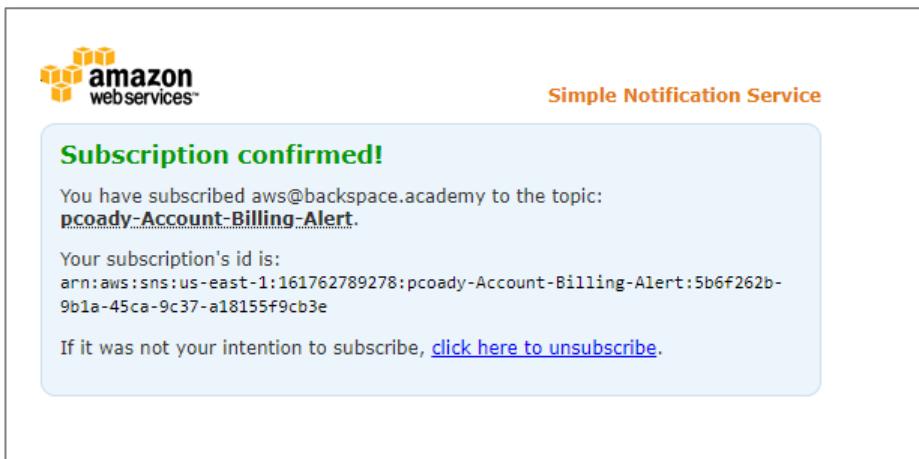
AN AWS Notifications <no-reply@sns.amazonaws.com>  
To aws@backspace.academy

You have chosen to subscribe to the topic:  
arn:aws:sns:us-east-1:161762789278:pcoady-Account-Billing-Alert

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):  
[Confirm subscription](#)

Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to [sns-opt-out](#)

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

	Name	State	Conditions	Action
	test-ReadCapacityUnitsLimit-BasicAlarm	OK	ConsumedReadCapacityUnits >= 240 for 5 datapoints within 5 minutes	No r
	test-name-index-WriteCapacityUnitsLimit-BasicAlarm	OK	ConsumedWriteCapacityUnits >= 240 for 60 datapoints within 1 hour	No r
	test-name-index-ReadCapacityUnitsLimit-BasicAlarm	OK	ConsumedReadCapacityUnits >= 240 for 60 datapoints within 1 hour	No r
	test-WriteCapacityUnitsLimit-BasicAlarm	OK	ConsumedWriteCapacityUnits >= 240 for 5 datapoints within 5 minutes	No r
	pcoady-Account-billing-alert	INSUFFICIENT DATA	EstimatedCharges > 10 for 1 datapoints within 6 hours HealthyHostCount <= 1 for 1 datapoints within 1 hour	Valid

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

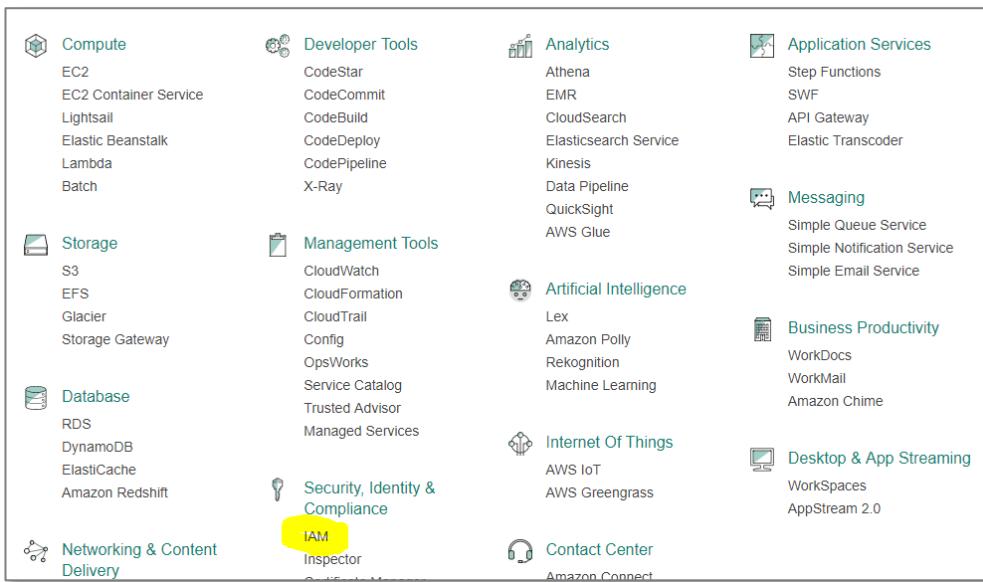
	Name	State	Last state update	Conditions	Actions
	pcoady-billing-alert	OK	2020-06-01 17:59:23	EstimatedCharges > 10 for 1 datapoints within 6 hours	

# 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.

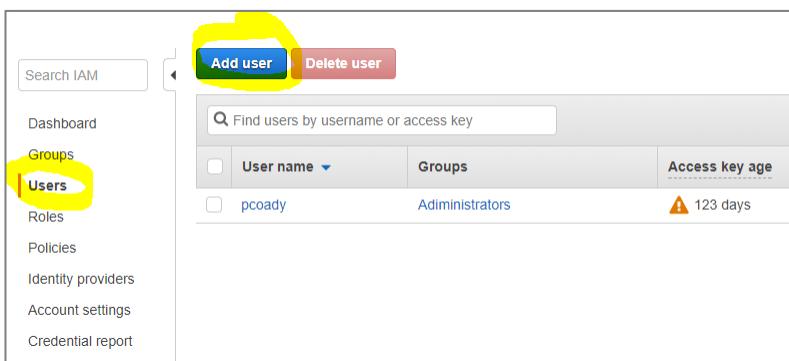
From the AWS console click 'Services'

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



Select 'Users'

Click 'Add user'



Give the user a name

Add user

1 Details    2 Permissions    3 Review    4 Complete

**Set user details**

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name\*  + Add another user

Check 'Programmatic access'

Check 'AWS Management Console access'

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

**Access type\***  **Programmatic access**  
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

**AWS Management Console access**  
Enables a **password** that allows users to sign-in to the AWS Management Console.

**Console password\***  Autogenerated password  
 Custom password

**Require password reset**  User must create a new password at next sign-in  
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

\* Required Cancel Next: Permissions

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

Click 'Next Review"

Add user

1 Details    2 Permissions    3 Review    4 Complete

**Set permissions for test-user**

Add user to group Copy permissions from existing user Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

**Add user to group**

Create group Refresh



Click 'Create user'

Add user

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	test-user
AWS access type	Programmatic access and AWS Management Console access
Console password type	Autogenerated
Require password reset	Yes

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Managed policy	IAMUserChangePassword

Cancel Previous **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.

Add user

Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://backspace-academy.signin.aws.amazon.com/console>

**Download .csv**

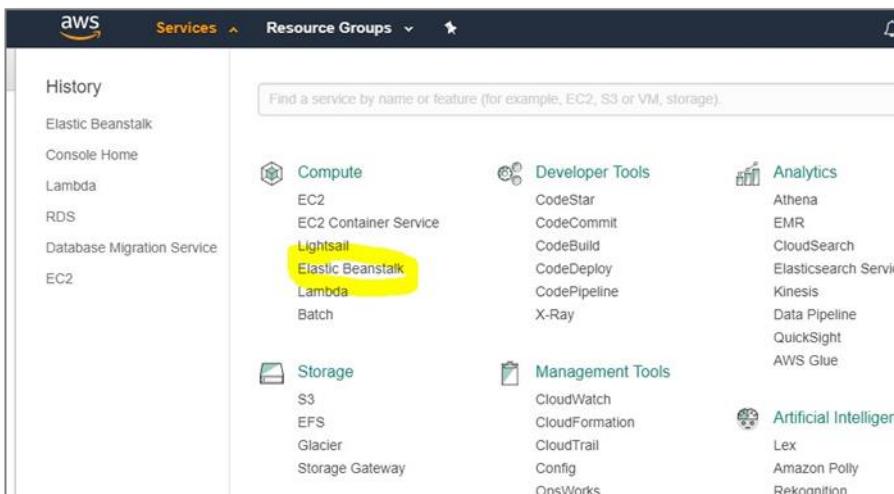
User	Access key ID	Secret access key	Password	Email login instructions
test-user	AKIAJZGZ6UMOZT3U5V6Q	***** Show	***** Show	Send email

Close

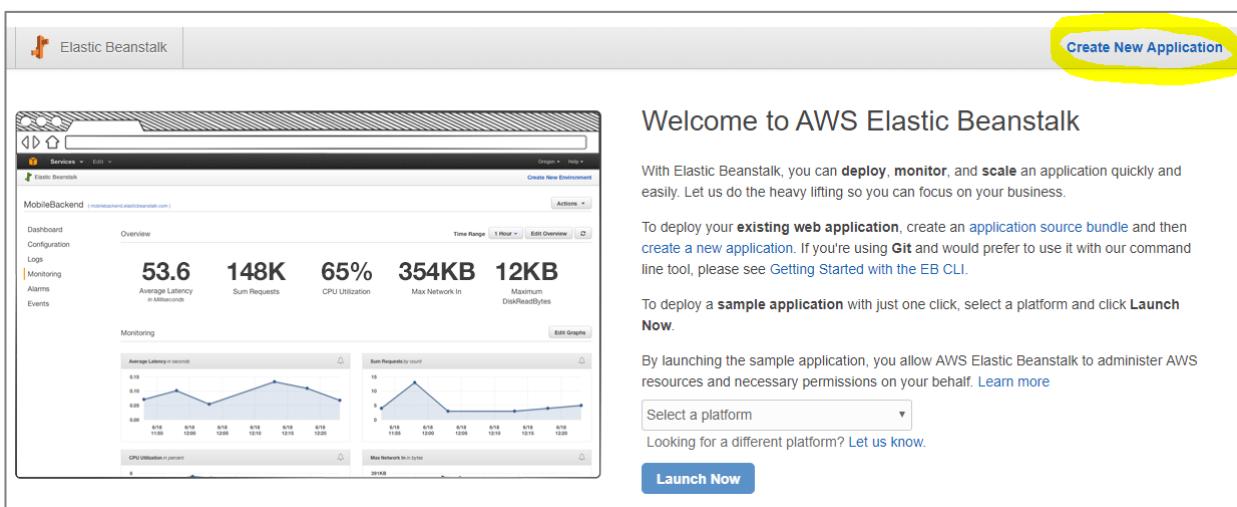
# Creating a Highly Available Architecture with Elastic Beanstalk

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*

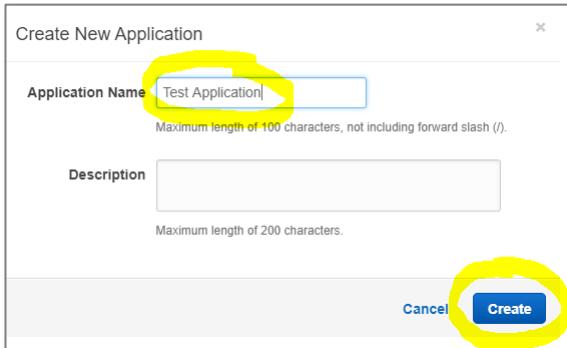


Click 'Create New Application'



Give your application a name *Test Application*.

Click "Create"



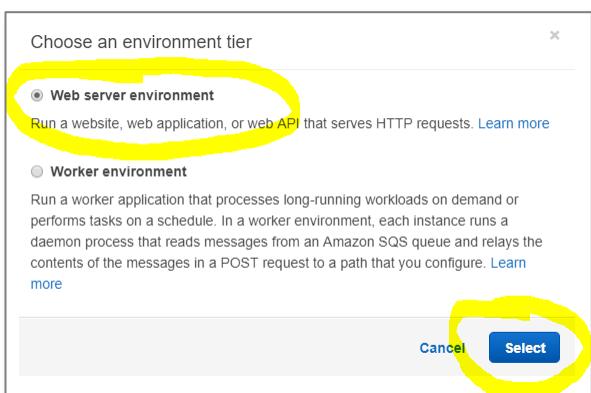
Your application will now be created.

Select “Actions” - “Create Environment”

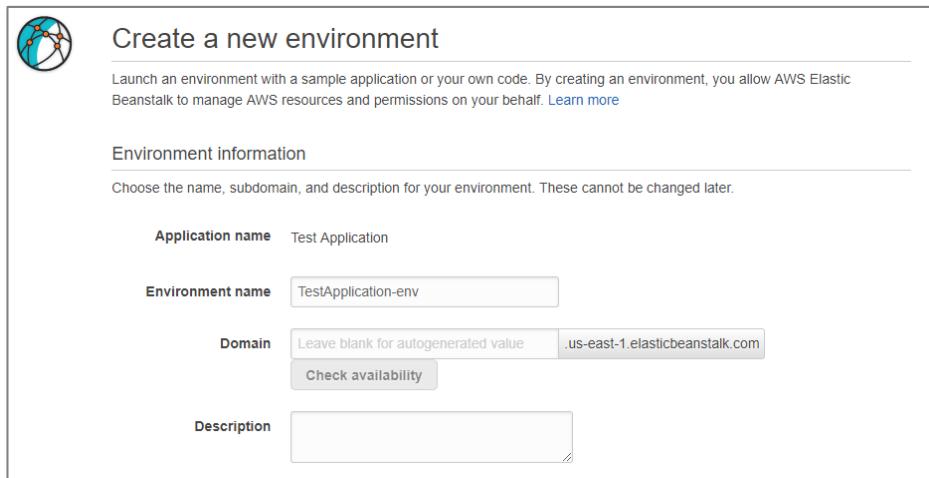


Select “Web server environment”

Click “Select”



Leave Environment information with default values



**Create a new environment**

Launch an environment with a sample application or your own code. By creating an environment, you allow AWS Elastic Beanstalk to manage AWS resources and permissions on your behalf. [Learn more](#)

**Environment information**

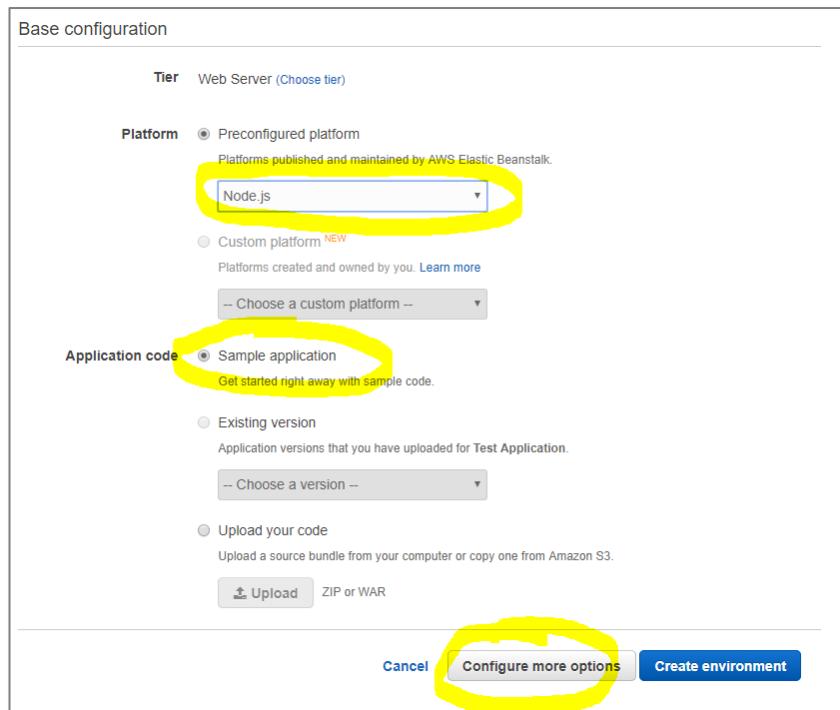
Choose the name, subdomain, and description for your environment. These cannot be changed later.

Application name	Test Application
Environment name	TestApplication-env
Domain	Leave blank for autogenerated value .us-east-1.elasticbeanstalk.com <a href="#">Check availability</a>
Description	(empty)

Select *Node.Js* as the platform

Select *Sample Application* for Application Code

Click *Configure More Options*



**Base configuration**

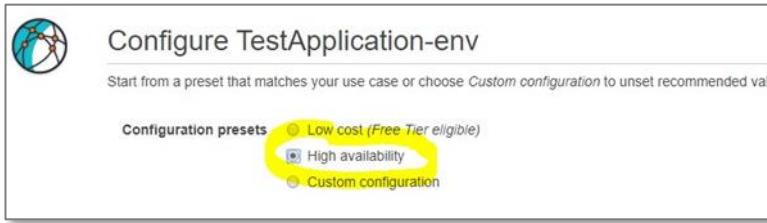
**Tier** Web Server ([Choose tier](#))

**Platform**  Preconfigured platform  
Platforms published and maintained by AWS Elastic Beanstalk.  
Node.js (highlighted with yellow circle)  
 Custom platform [NEW](#)  
Platforms created and owned by you. [Learn more](#)

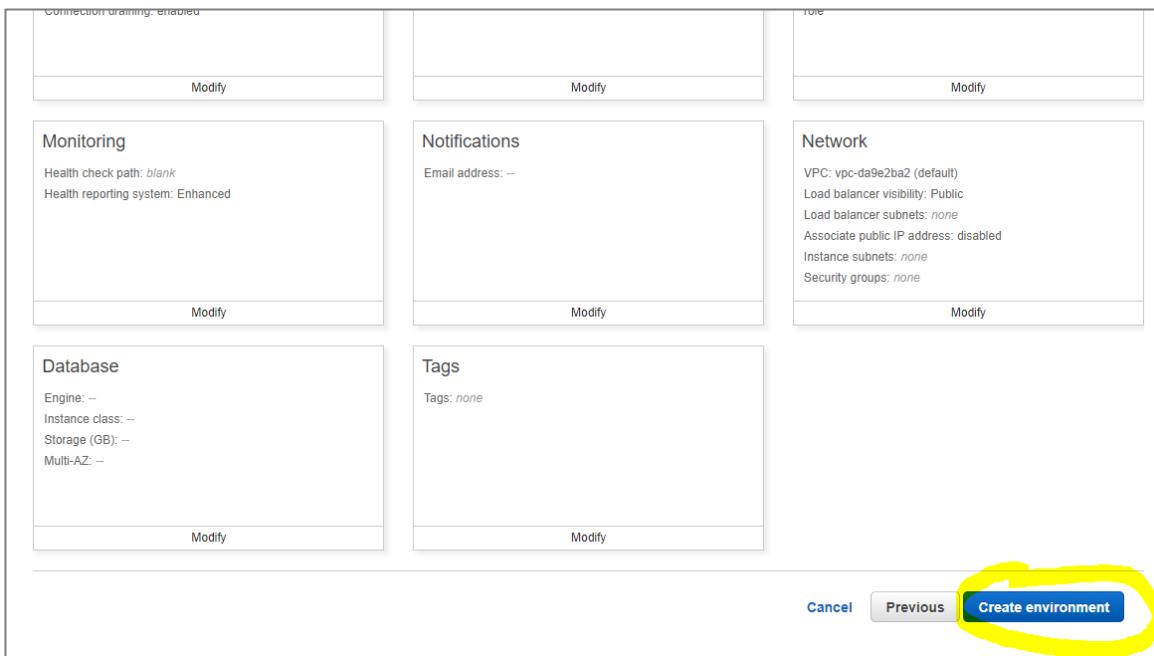
**Application code**  Sample application  
Get started right away with sample code.  
 Existing version  
Application versions that you have uploaded for Test Application.  
 Upload your code  
Upload a source bundle from your computer or copy one from Amazon S3.  
[Upload ZIP or WAR](#)

[Cancel](#) [Configure more options](#) (highlighted with yellow circle) [Create environment](#)

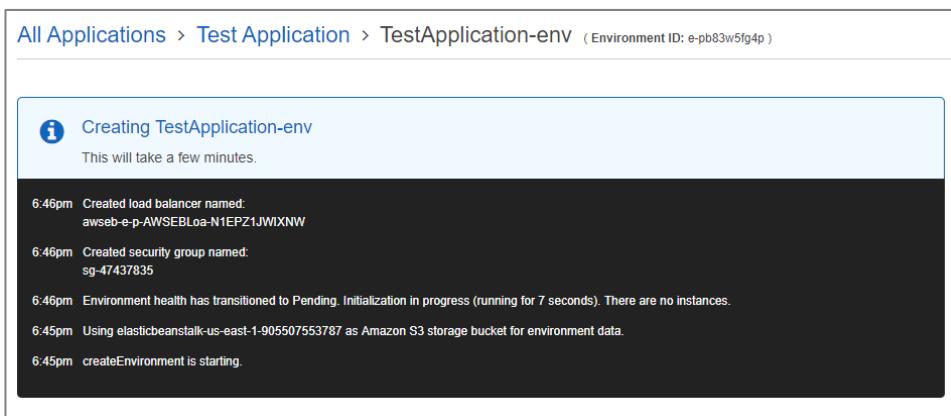
Select *High availability*



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

All Applications > Test Application > TestApplication-env (Environment ID: e-pb83w5fg4p, URL: [TestApplication-env.mxafx3y39.us-east-1.elasticbeanstalk.com](http://TestApplication-env.mxafx3y39.us-east-1.elasticbeanstalk.com)) Actions ▾

**Overview**

**Health** Ok **Running Version** Sample Application

**Logs** **Configuration** **Upload and Deploy**

**Logs** **Configuration** **Upload and Deploy**

**Health** **Configuration** **Upload and Deploy**

**Monitoring** **Configuration** **Upload and Deploy**

**Alarms** **Configuration** **Upload and Deploy**

**Managed Updates** **Configuration** **Upload and Deploy**

**Events** **Configuration** **Upload and Deploy**

**Tags** **Configuration** **Upload and Deploy**

You will now see the Sample Application

Congratulations

Your first AWS Elastic Beanstalk Node.js application is now running on your own dedicated environment in the AWS Cloud

**What's Next?**

- [AWS Elastic Beanstalk overview](#)
- [AWS Elastic Beanstalk concepts](#)
- [Deploy an Express Application to AWS Elastic Beanstalk](#)
- [Deploy an Express Application with Amazon ElastiCache to AWS Elastic Beanstalk](#)
- [Deploy a Geddy Application with Amazon ElastiCache to AWS Elastic Beanstalk](#)
- [Customizing and Configuring a Node.js Container](#)
- [Working with Logs](#)

## Clean Up

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

Navigate back to the Test Application

All Applications > Test Application > TestApplication-env (Environment ID: e-pb83w5fg4p, URL: [TestApplication-env.mxafx3y39.us-east-1.elasticbeanstalk.com](http://TestApplication-env.mxafx3y39.us-east-1.elasticbeanstalk.com)) Actions ▾

**Overview**

**Health** Ok **Running Version** Sample Application

**Logs** **Configuration** **Upload and Deploy**

**Logs** **Configuration** **Upload and Deploy**

**Health** **Configuration** **Upload and Deploy**

**Monitoring** **Configuration** **Upload and Deploy**

**Alarms** **Configuration** **Upload and Deploy**

**Managed Updates** **Configuration** **Upload and Deploy**

**Events** **Configuration** **Upload and Deploy**

**Tags** **Configuration** **Upload and Deploy**

**Recent Events** **Show All**

## Click Actions

### Select Delete Application

All Applications > Test Application

Environments

Application versions

Saved configurations

TestApplication-env

Environment tier: Web Server  
Platform: 64bit Amazon Linux 2017.03 v4.3.0 running Node.js  
Running versions: Sample Application  
Last modified: 2017-11-05 18:50:40 UTC+1100  
URL: TestApplication-env.mxafr3y3j9.us-east-1.elasticib...

Create environment  
Restore terminated environment  
Swap environment URLs  
Delete application

### Click "Delete"

Delete Application

Are you sure you want to delete the application: **Test Application**?

Cancel **Delete**

### Click on the environment

All Applications

Test Application

TestApplication-env

Environment tier: Web Server  
Platform: 64bit Amazon Linux 2017.03 v4.3.0 running Node.js  
Running versions: Sample Application  
Last modified: 2017-11-05 18:55:47 UTC+1100  
URL: TestApplication-env.mxafr3y3j9.us-east-1....

You will now see your environment is being terminated.

All Applications > [Test Application](#) > TestApplication-env ( Environment ID: e-pb83w5fg4p, URL: [TestApplication-env.mxafx3y3j9.us-east-1.elasticbeanstalk.com](#) ) [Actions](#) ▾

[Dashboard](#)

[Configuration](#)

[Logs](#)

[Health](#)

[Monitoring](#)

[Alarms](#)

[Managed Updates](#)

[Events](#)

[Tags](#)

Elastic Beanstalk is terminating your environment.  
[View Events](#)

Overview [Refresh](#)

 [Health](#)  
Ok [Causes](#)

[Running Version](#)  
Sample Application [Upload and Deploy](#)

 [Configuration](#)

64bit Amazon Linux 2017.03  
v4.3.0 running Node.js [Change](#)