Question 1:

Working with s3 buckets
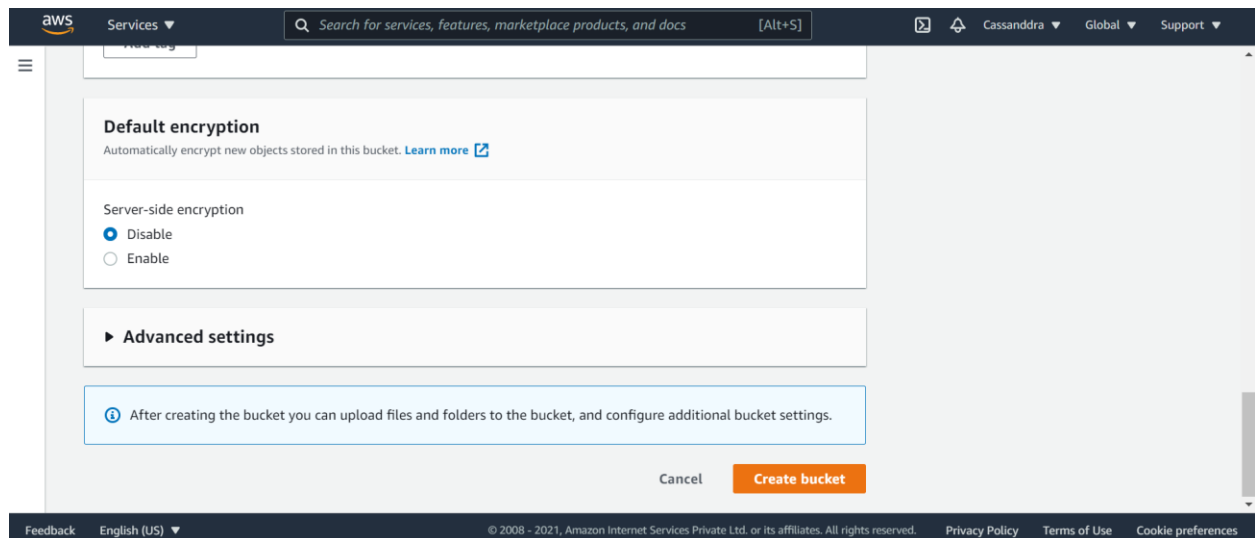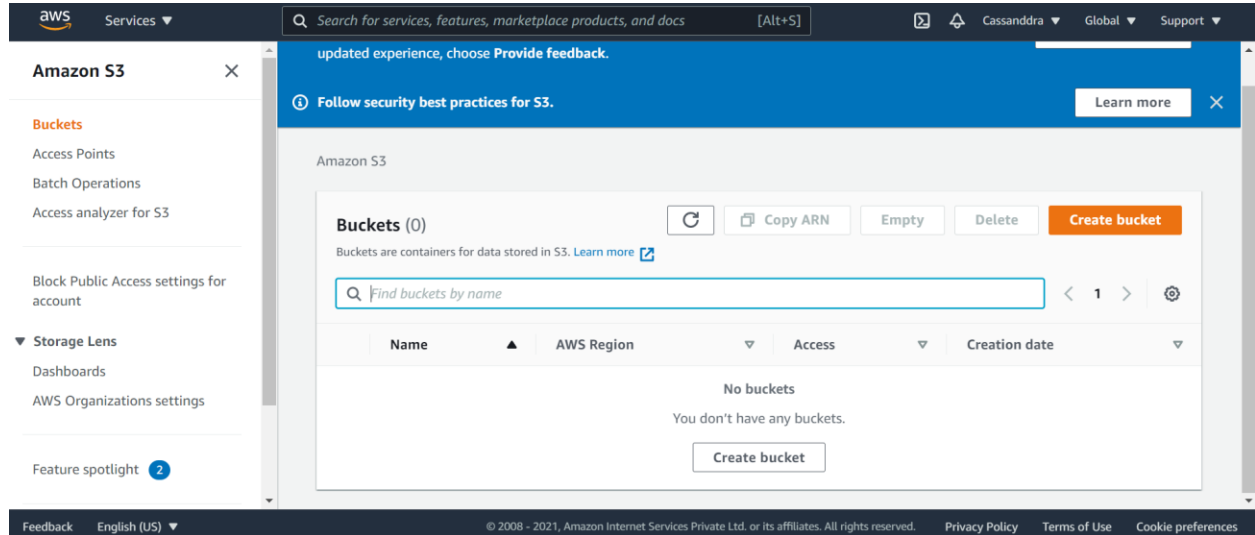
#created a bucket as assignment1lu

uploaded an object in the bucket

Question 2:

Creating an ec2 instance.
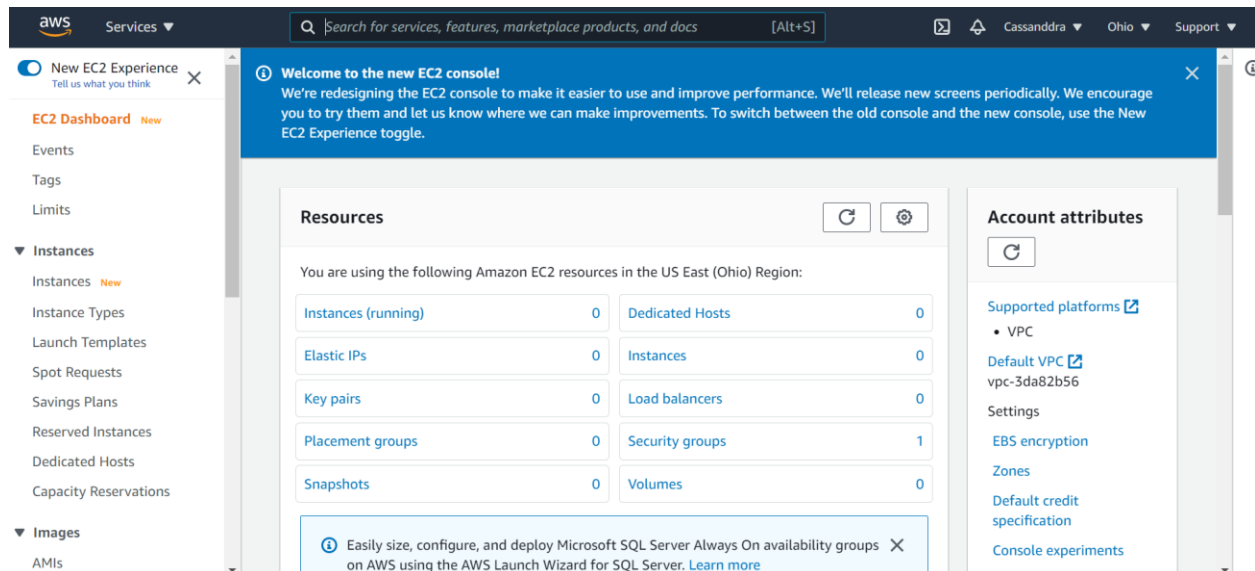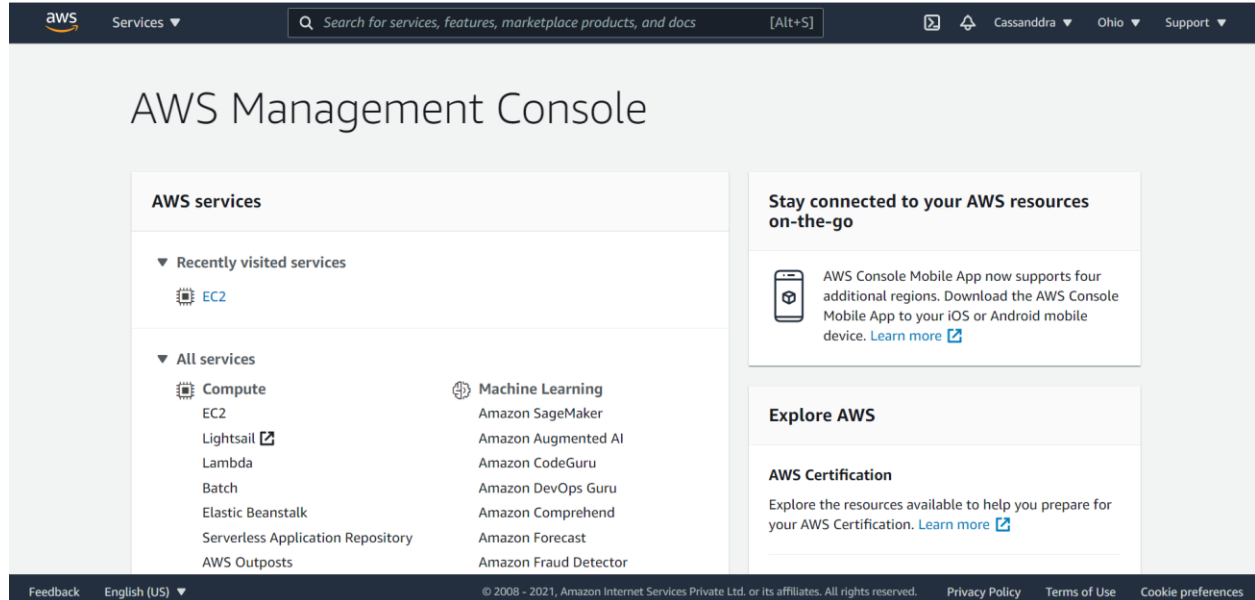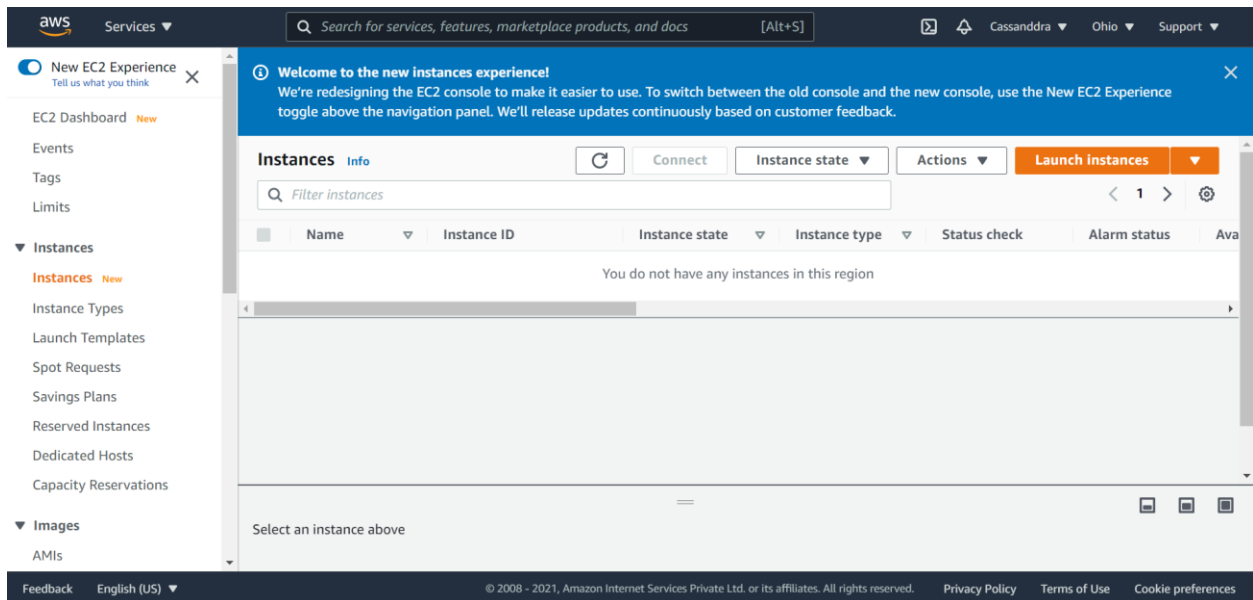
#creating an ec2 through the 7 step procedure
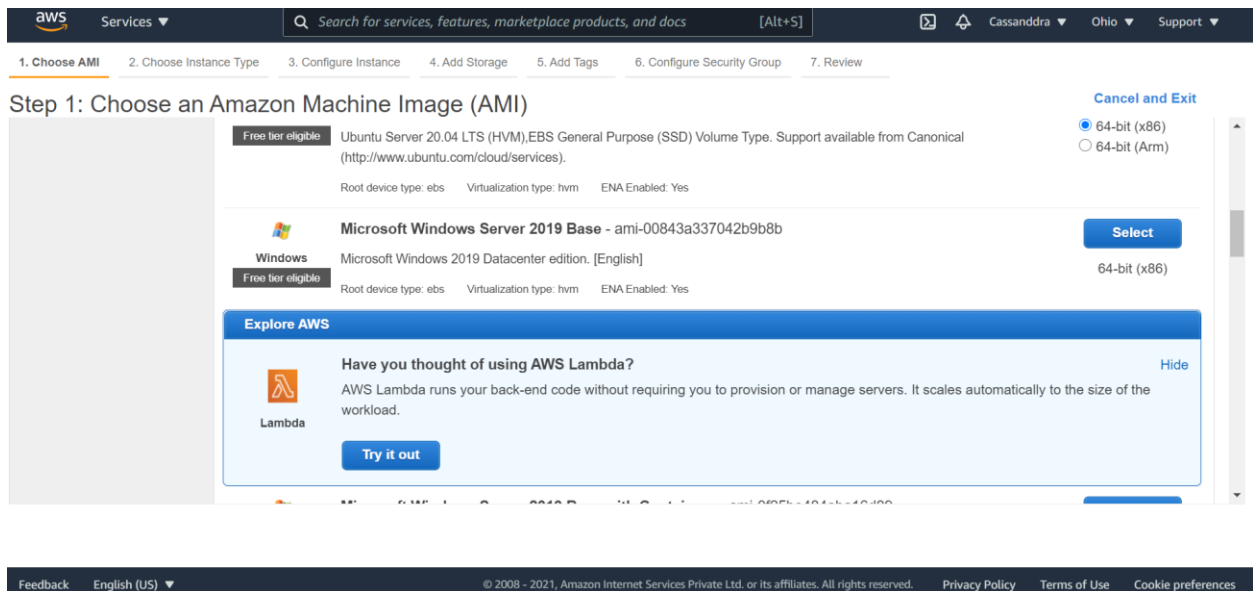
1. Choose AMI   2. Choose Instance Type   3. Configure Instance   4. Add Storage   5. Add Tags   6. Configure Security Group   7. Review

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by: All instance families ▼   Current generation ▼   **Show/Hide Columns**

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

	Family ▼	Type ▼	vCPUs ⓘ ▼	Memory (GiB) ▼	Instance Storage (GB) ⓘ ▼	EBS-Optimized Available ⓘ ▼	Network Performance ⓘ ▼	IPv6 Support ⓘ ▼
☐	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
☑	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
☐	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
☐	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes

Cancel   Previous   **Review and Launch**   Next: Configure Instance Details

---

1. Choose AMI   2. Choose Instance Type   3. Configure Instance   4. Add Storage   5. Add Tags   6. Configure Security Group   7. Review

Step 3: Configure Instance Details

Credit specification ⓘ   ☐ Unlimited
Additional charges may apply

▼ Advanced Details

Enclave ⓘ   ☐ Enable
Metadata accessible ⓘ   Enabled ⬍
Metadata version ⓘ   V1 and V2 (token optional) ⬍
Metadata token response hop limit ⓘ   1 ⬍
User data ⓘ   ⦿ As text ○ As file ☐ Input is already base64 encoded
(Optional)

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

1. Choose AMI   2. Choose Instance Type   3. Configure Instance   **4. Add Storage**   5. Add Tags   6. Configure Security Group   7. Review

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/sda1	snap-0bfcc22a65369905c	30	General Purpose SSD (gp2) ▾	100 / 3000	N/A	☑	Not Encrypte ▾

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

---

1. Choose AMI   2. Choose Instance Type   3. Configure Instance   4. Add Storage   **5. Add Tags**   6. Configure Security Group   7. Review

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.
A copy of a tag can be applied to volumes, instances or both.

Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances ⓘ	Volumes ⓘ	Network Interfaces ⓘ

This resource currently has no tags

Choose the Add tag button or click to add a Name tag.
Make sure your IAM policy includes permissions to create tags.

Add Tag   (Up to 50 tags maximum)

Cancel   Previous   **Review and Launch**   Next: Configure Security Group

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

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

Security group name: `launch-wizard-1`

Description: `launch-wizard-1 created 2021-02-25T21:27:26.306+05:30`

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ	
All traffic ▾	All	0 - 65535	Anywhere ▾ 0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop	⊗

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**

---

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

▼ AMI Details Edit AMI

Microsoft Windows Server 2019 Base - ami-00843a337042b9b8b

Free tier eligible Microsoft Windows 2019 Datacenter edition. [English]

Root Device Type: ebs Virtualization type: hvm

If you plan to use this AMI for an application that benefits from Microsoft License Mobility, fill out the License Mobility Form. Don't show me this again

▼ Instance Type Edit instance type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	-	1	1	EBS only	-	Low to Moderate

▼ Security Groups Edit security groups

Security group name launch-wizard-1
Description launch-wizard-1 created 2021-02-25T21:27:26.306+05:30

Cancel Previous **Launch**

1. Choose AMI   2. Choose Instance Type   3. Configure Instance   4. Add Storage   5. Add Tags   6. Configure Security Group   7. Review

Step 7: Review Instance Launch

▼ Security Groups   Edit security groups

Security group name   launch-wizard-1
Description   launch-wizard-1 created 2021-02-25T21:27:26.306+05:30

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ
All traffic	All	All	0.0.0.0/0	
All traffic	All	All	::/0	

▶ Instance Details   Edit instance details

▶ Storage   Edit storage

▶ Tags   Edit tags

Cancel   Previous   Launch

#creating a new key pair

1. Choose AMI   2. Choose Instance Type   3. Configure Instance   4. Add Storage   5. Add Tags   6. Configure Security Group   7. Review

Step 7: Review Instance L

▼ Security Groups

Security group name   launch-
Description   launch-

Select an existing key pair or create a new key pair ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Create a new key pair ▾

Key pair name
Cassy

Download Key Pair

💬 You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Edit security groups

Edit instance details

Edit storage

Edit tags

Cancel   Previous   Launch

Launch Status

✅ **Your instances are now launching**
The following instance launches have been initiated: i-022dc7c5b61b26f4a   View launch log

ℹ️ **Get notified of estimated charges**
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. Find out how to connect to your instances.

▼ Here are some helpful resources to get you started

Launch Status

continue to accrue until you stop or terminate your instances.

Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. Find out how to connect to your instances.

▼ Here are some helpful resources to get you started

- How to connect to your Windows instance
- Learn about AWS Free Usage Tier

- Amazon EC2: User Guide
- Amazon EC2: Microsoft Windows Guide
- Amazon EC2: Discussion Forum

While your instances are launching you can also

- Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)
- Create and attach additional EBS volumes (Additional charges may apply)
- Manage security groups

View Instances

#the instance passed the 2/2 checks

EC2 > Instances > i-022dc7c5b61b26f4a > Connect to instance

Connect to instance Info

Connect to your instance i-022dc7c5b61b26f4a using any of these options

Session Manager   **RDP client**

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

Download remote desktop file

When prompted, connect to your instance using the following details:

Public DNS

🗐 ec2-3-16-216-163.us-east-2.compute.amazonaws.com

User name

🗐 Administrator

EC2 > Instances > i-022dc7c5b61b26f4a > Get windows password

Get Windows password Info

Retrieve and decrypt the initial Windows administrator password for this instance.

To decrypt the password, you will need your key pair for this instance.

ⓘ **Key pair associated with this instance**
Cassy

Browse to your key pair:

⤒ Browse

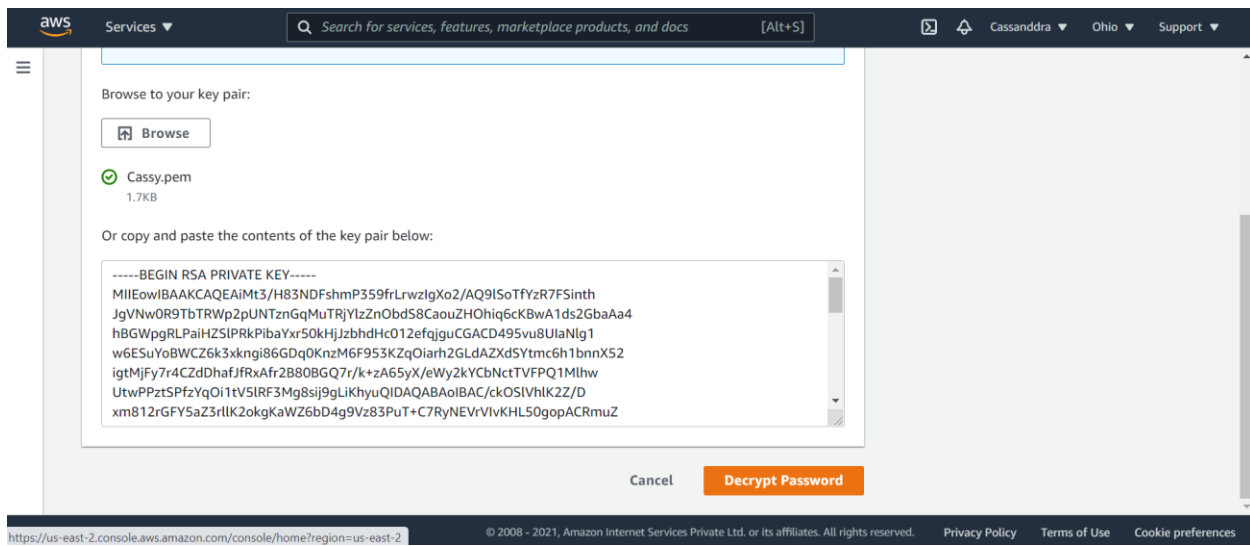Or copy and paste the contents of the key pair below:

-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAiMt3/H83NDFshmP359frLrwzIgXo2/AQ9lSoTfYzR7FSinth
JgVNw0R9TbTRWp2pUNTznGqMuTRjYlzZnObdS8CaouZHOhiq6cKBwA1ds2GbaAa4
hBGWpgRLPaiHZSlPRkPibaYxr50kHjJzbhdHc012efqjguCGACD495vu8UIaNlg1
w6ESuYoBWCZ6k3xkngi86GDq0KnzM6F953KZqOiarh2GLdAZXdSYtmc6h1bnnX52
igtMjFy7r4CZdDhafJfRxAfr2B80BGQ7r/k+zA65yX/eWy2kYCbNctTVFPQ1Mlhw
UtwPPztSPfzYqOi1tV5lRF3Mg8sij9gLiKhyuQIDAQABAoIBAC/ckOSlVhlK2Z/D
xm812rGFY5aZ3rllK2okgKaWZ6bD4g9Vz83PuT+C7RyNEVrVIvKHL50gopACRmuZ

#created an ec2 instance