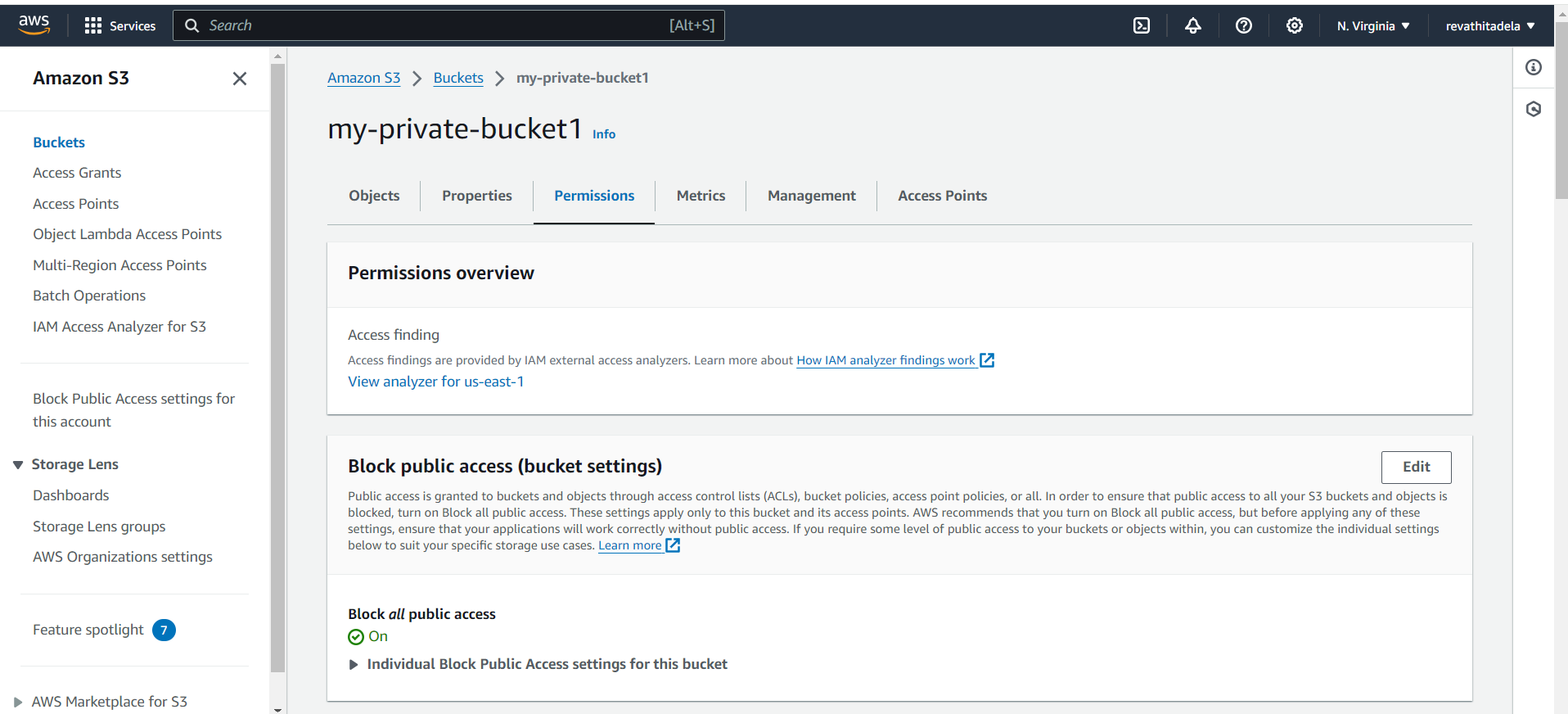
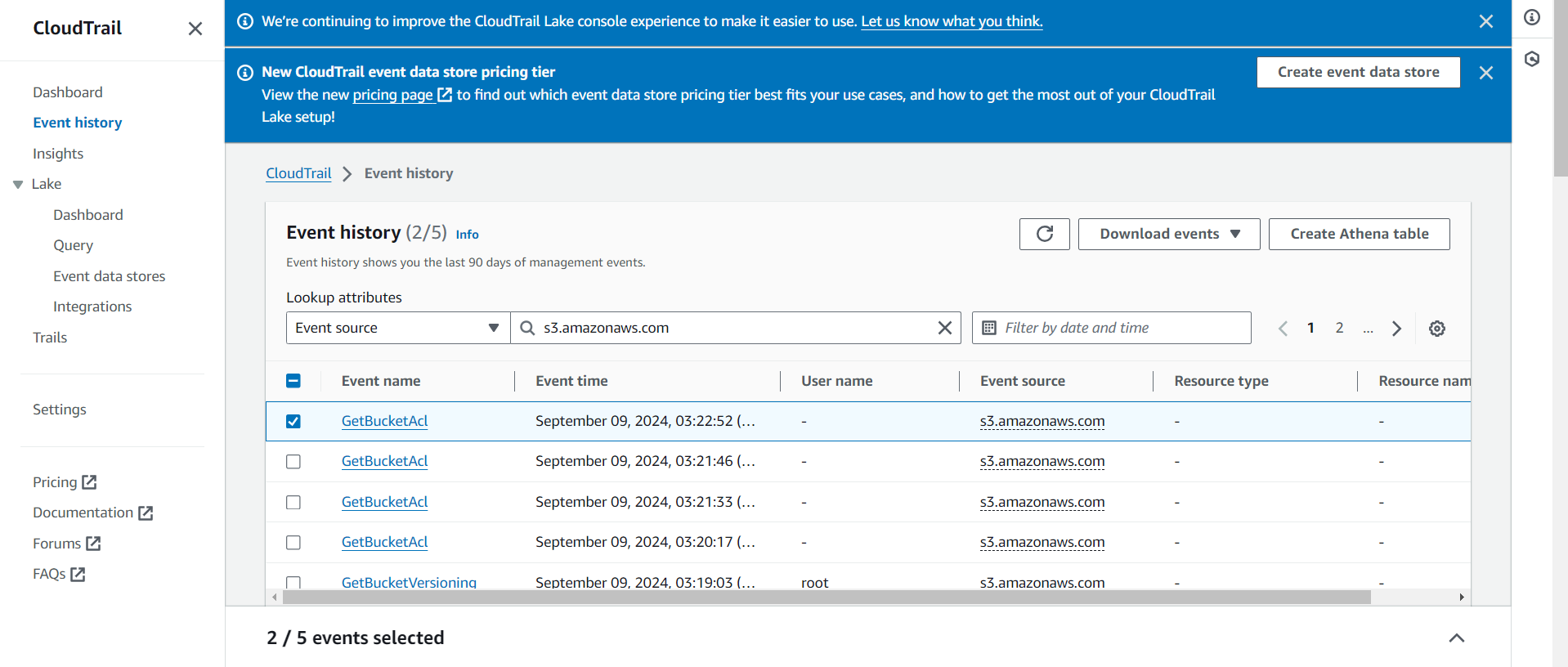


A screenshot of a computer

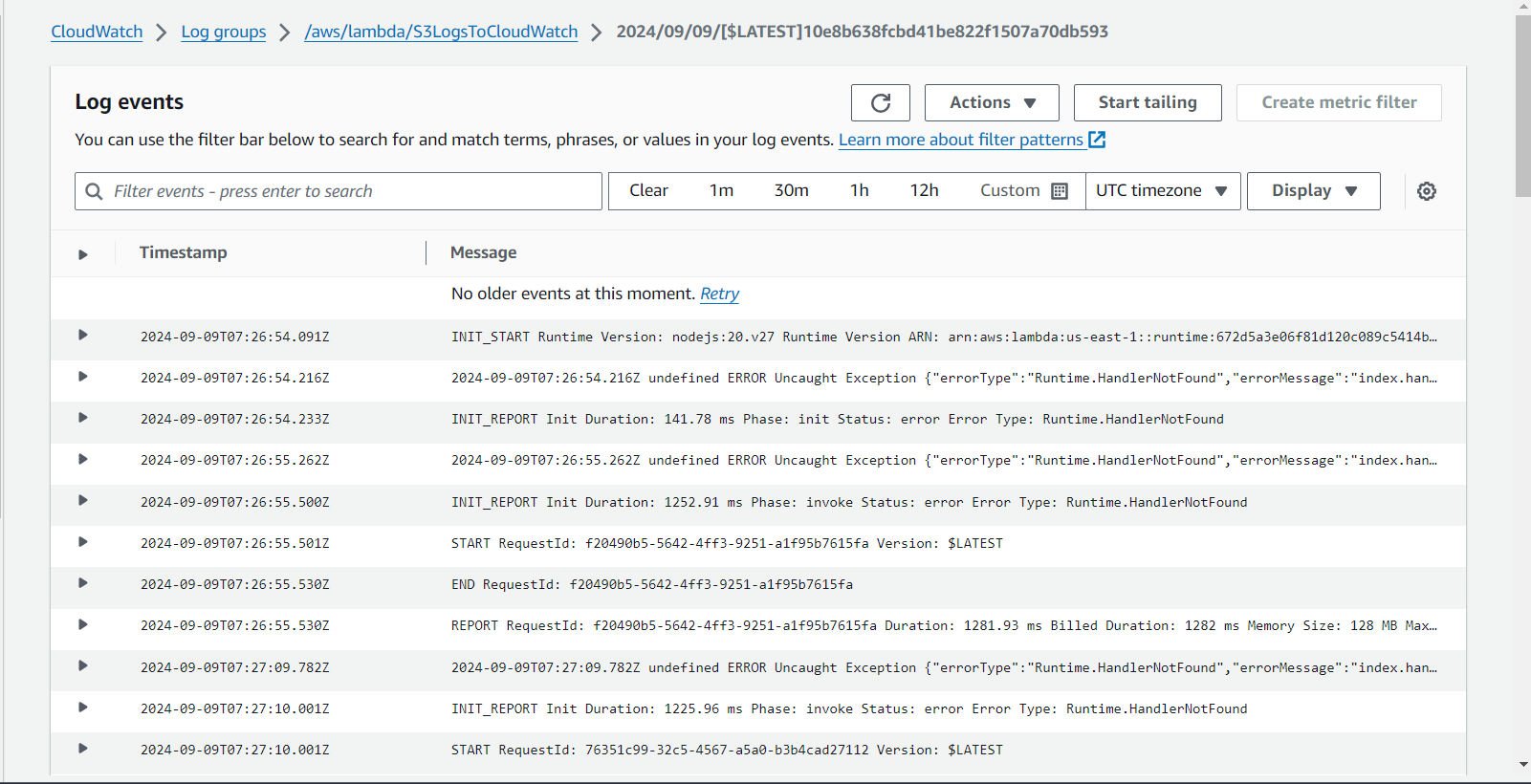
Description automatically generated





A screenshot of a computer

Description automatically generated



A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Output Log:

Here's a step-by-step guide to completing the task:

### \*\*1. Create an S3 Bucket with No Public Access & Enable Logging\*\*

1. \*\*Create an S3 Bucket\*\*:

- Go to the \*\*S3 Console\*\* in AWS.

- Click \*\*Create bucket\*\*.

- Enter the \*\*Bucket name\*\* (e.g., `my-private-bucket`).

- Uncheck the \*\*Block all public access\*\* option to prevent public access.

- Click \*\*Create bucket\*\*.

2. \*\*Upload Files to the S3 Bucket\*\*:

- Open your created bucket.

- Click \*\*Upload\*\* and select files to upload.

- Ensure no public access permissions are granted to the objects.

3. \*\*Enable CloudWatch Logs for S3\*\*:

To monitor uploads and track actions on the bucket using CloudWatch:

- In \*\*S3\*\*, select your bucket.

- Go to the \*\*Properties\*\* tab.

- Scroll down to \*\*Server Access Logging\*\*.

- Enable logging and select a destination S3 bucket for the logs.

- To view logs, set up CloudWatch:

1. Go to the \*\*CloudWatch Console\*\*.

2. Create a new log group or use an existing one.

3. Set up a log stream to view the S3 bucket logs.

### \*\*2. Launch Two EC2 Instances\*\*

1. \*\*Launch EC2 Instances\*\*:

- Go to the \*\*EC2 Console\*\*.

- Click \*\*Launch Instance\*\*.

- Choose the AMI (Amazon Linux 2 or Ubuntu).

- Select instance type (e.g., `t2.micro`).

- In \*\*Network settings\*\*, ensure both instances are in the same VPC and subnets.

- Configure \*\*security groups\*\* to allow traffic on HTTP/HTTPS (port 80/443).

- Launch the instances.

2. \*\*Install Web Server on Both Instances\*\*:

- After the instances are running, SSH into each instance.

- Install a web server (e.g., Apache or Nginx):

```bash

sudo yum install httpd -y # Amazon Linux 2

sudo systemctl start httpd

sudo systemctl enable httpd

```

3. \*\*Test the Web Servers\*\*:

- Confirm that the web server is running by accessing the instance's public IP.

### \*\*3. Set Up an Application Load Balancer (ALB)\*\*

1. \*\*Create a Load Balancer\*\*:

- Go to the \*\*EC2 Console\*\*.

- In the left-hand menu, select \*\*Load Balancers\*\*.

- Click \*\*Create Load Balancer\*\* and select \*\*Application Load Balancer\*\*.

- Choose \*\*internet-facing\*\*.

- Select the VPC where your EC2 instances are running.

- Choose \*\*two public subnets\*\*.

2. \*\*Configure the Load Balancer\*\*:

- For the security group, allow inbound traffic on HTTP (port 80).

- Create a new target group for your instances.

- Register both EC2 instances in this target group.

3. \*\*Test Load Balancer\*\*:

- Once the load balancer is active, use its \*\*DNS name\*\* to access your application.

- The traffic will be routed to your EC2 instances, and the \*\*ALB's IP\*\* will be seen as the source of the traffic.

### \*\*4. Monitor with CloudWatch\*\*

1. \*\*Enable CloudWatch Metrics for ALB\*\*:

- Go to the \*\*CloudWatch Console\*\*.

- Create an alarm or view metrics for the load balancer to monitor request rates, latency, and healthy host counts.

2. \*\*View CloudWatch Logs for S3\*\*:

- Go to \*\*CloudWatch Logs\*\*.

- Select the log group for your S3 bucket to view access and error logs.

By following these steps, you will have:

1. An S3 bucket with no public access.

2. Logs for file uploads available in CloudWatch.

3. Two EC2 instances connected to an Application Load Balancer.