CyberLearners Cloud Security

Group 2

GENERATING S3 PRESIGNED URL USING CLOUDSHELL

TEAM MEMBERS

JANE OHIA

EZEASOR ONYINY

AIM OF THE PROJECT

- To create an S3 bucket.
- To grant a temporary or short term access to an S3 bucket.
- To share and upload objects in Amazon S3 without requiring AWS security credentials or permission.
- To create a URL that provides federated users with direct access to AWS Management Console.

RELATION TO SECURITY

- Cloud users face security threats both from outside and inside of the cloud environment.
- In the cloud, the responsibility of securing the environment is divided among potentially many parties, including the cloud user, the cloud vendor, and others. Nonetheless, the cloud user must take a chunk of the responsibility of protecting and securing their resources stored on the cloud.
- When using the Amazon Web Service (AWS) cloud provider, a user is able to store their data and resources in the cloud using the Amazon Simple Storage Service also known as Amazon S3.

RELATION TO SECURITY

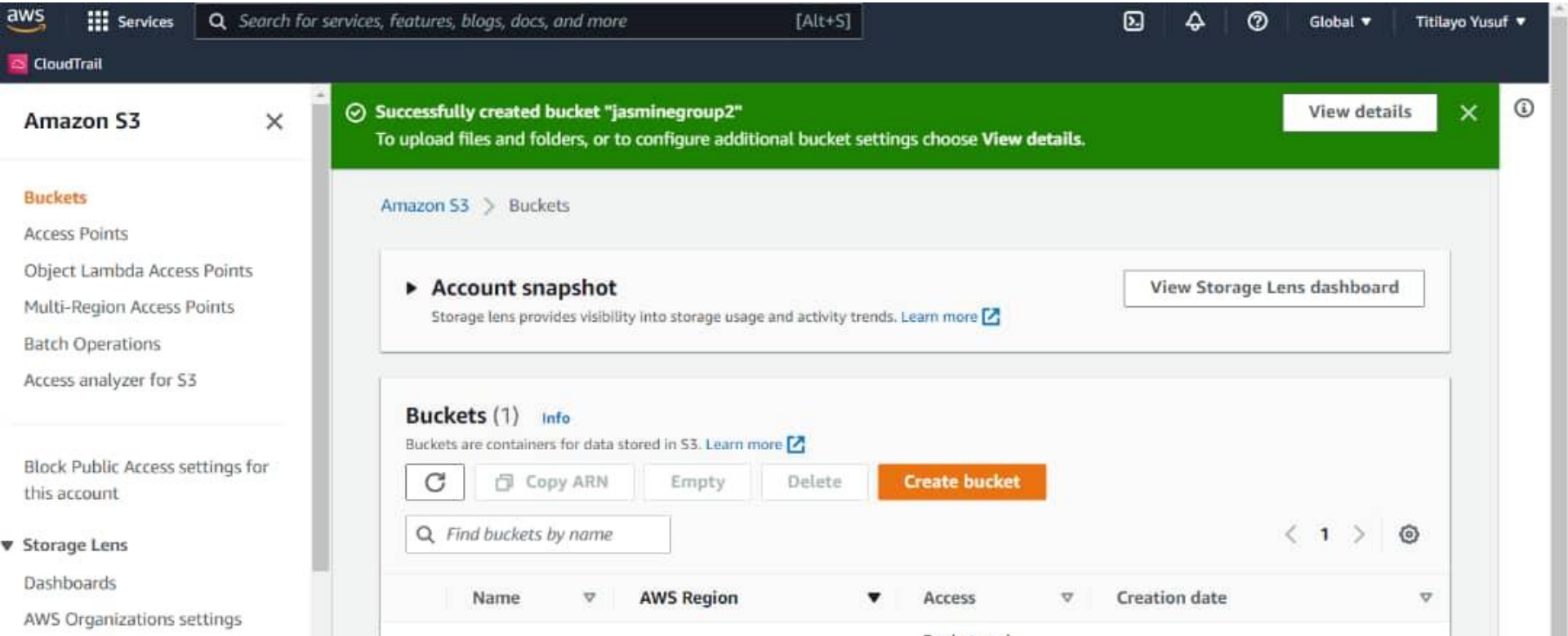
- The Amazon S3 is a scalable, high-speed, web-based cloud storage service. The service is designed for online backup and archiving of data and applications on AWS. Objects stored in S3 are by default configured to be private and only the object owner has permission to access them.
- That being said, these objects or files stored in the S3 bucket can be shared with, viewed, and altered by third parties who are either granted permission to do so by the owner or maliciously gain unauthorized access to its resources.
- One of the ways a user can securely share the objects stored in S3 with another party by granting them access is by creating a presigned URL, using their own security credentials to grant permission to view or download the object within a specified time period determined by the owner. Therefore, the presigned URL is valid for a specified duration after which the third party ceases to gain access

RELATION TO SECURITY

- The use of presigned URLs in sharing S3 objects is important in maintaining the security and integrity of data and applications stored in the cloud because:
  - It provides short-term access to a private object in your S3 bucket.
  - It specifies which specific object the owner of the bucket wants to share so that the recipient of the URL does not have access to all the contents of the bucket.
  - It minimizes the risk of unauthorized access to your bucket because a person must have the URL link before they can access it.
- In conclusion, like all cloud services, this service must be secured to prevent unauthorized access to its resources from parties other than the owner.

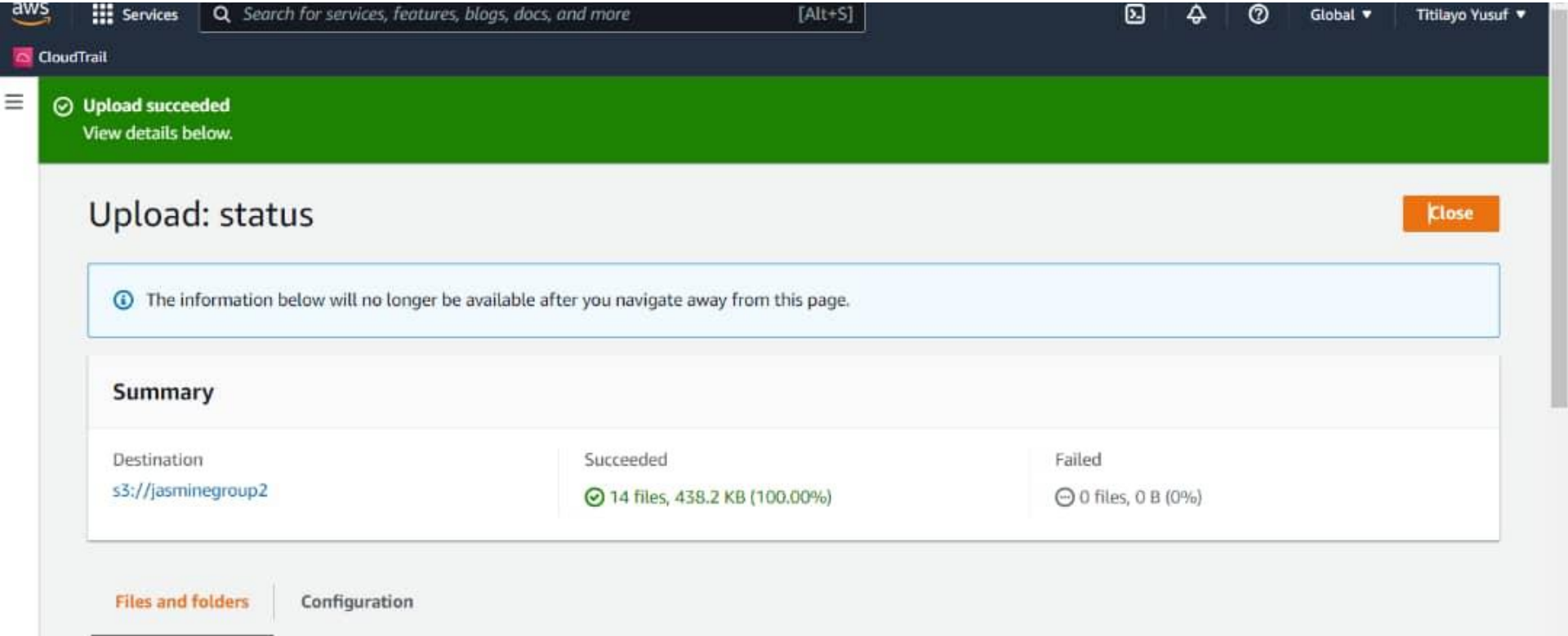
GENERATE S3 PRESIGNED URL USING CLOUDSHELL

1. Create a bucket



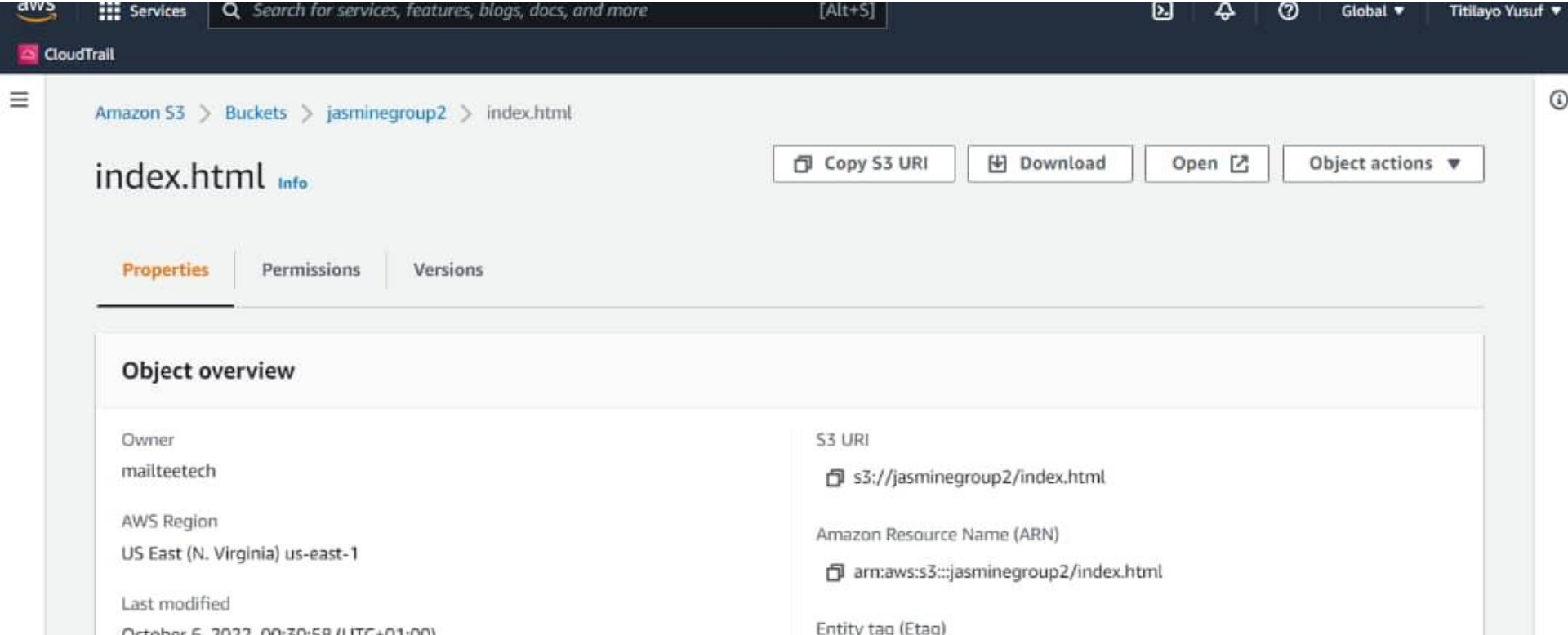
GENERATE S3 PRESIGNED URL USING CLOUDSHELL

2. Upload file into the bucket.



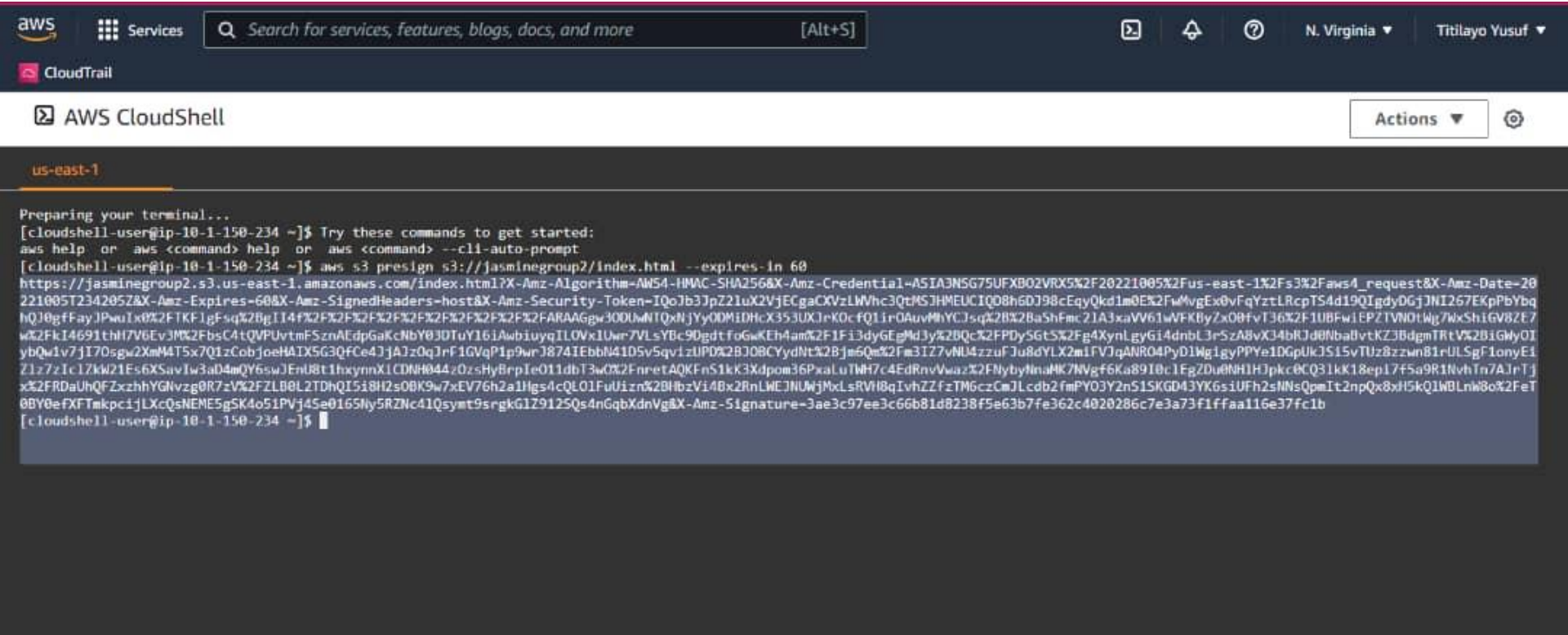
GENERATE S3 PRESIGNED URL USING CLOUDSHELL

3. Copy the S3 URL.



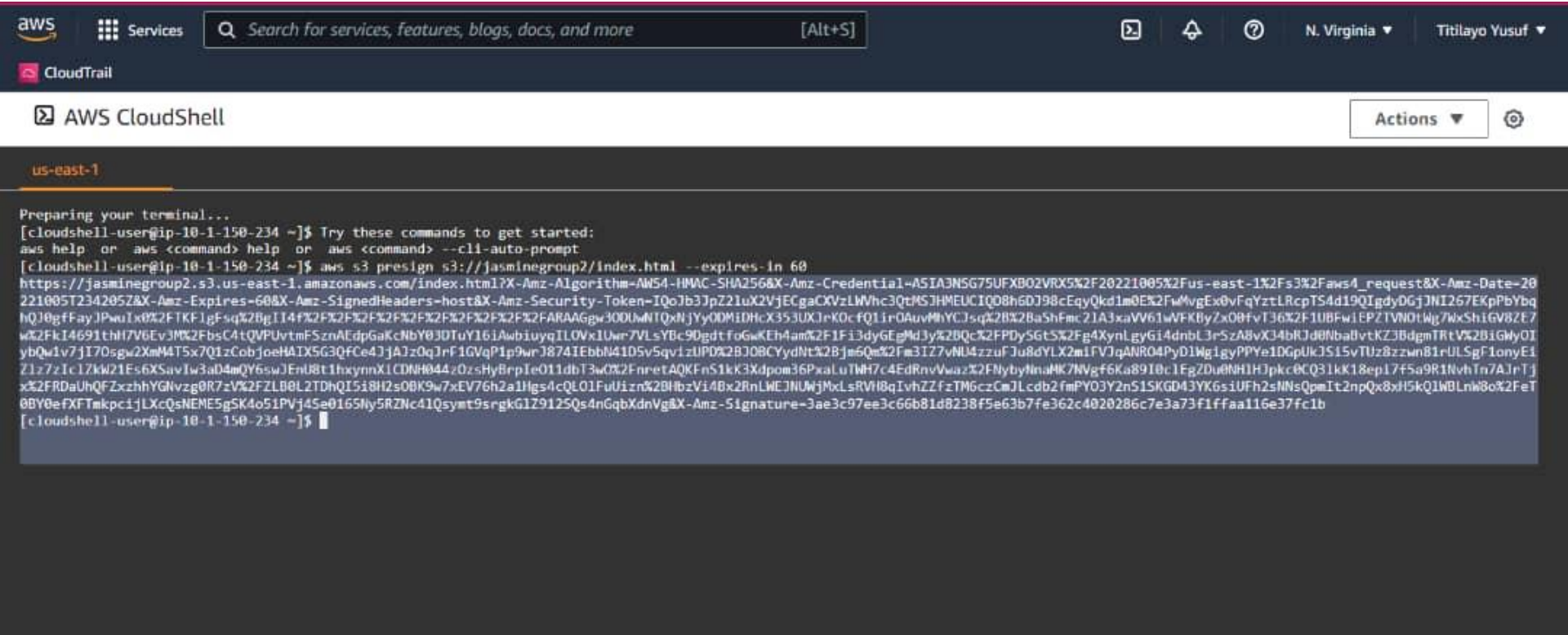
GENERATE S3 PRESIGNED URL USING CLOUDSHELL

4. Open CloudShell input code “aws s3 presign (URL) –expires-60”.



GENERATE S3 PRESIGNED URL USING CLOUDSHELL

5. Copy result and open in new tab .



IMPLICATIONS WHEN USING PRESIGNED URLS

- A presigned URL is used to generate a URL that can be used to access an Amazon S3 bucket and that means anyone with access to it can perform actions like the original signing user. This is a privacy concern because there is a possibility of unintended users having access to the bucket. It could also be a monetary concern if thousands of people are able to access it and incur cost on the root account.
- To mitigate this risk, a short expiration can be used on the signed URL, also using long expiration times is not just insecure but also unnecessary because presigned URLs should be used right after signing which makes the default of 15 minutes more than enough.
- Also, when CloudFront is used for edge caching, a user can download a file and the next user does not need to go all the way to the bucket but get it from a cache in closer proximity. An expired URL can be found in the cache and then a second request by a user won't go all the way to S3 to check it. As a result, if somebody accesses a signed URL when it is valid it will be available for everybody close to that location. If an attacker gains access to an expired signed URL he can try to find an edge where the file is still available.

LESSON LEARNT

- Objects stored S3 buckets can be shared securely by using presigned URLs..
- S3 bucket is private by default unless otherwise configured by the owner.
- Presigned URLs have an expiration date and time.
- Securing S3 buckets is the responsibility of the user or owner

THE END