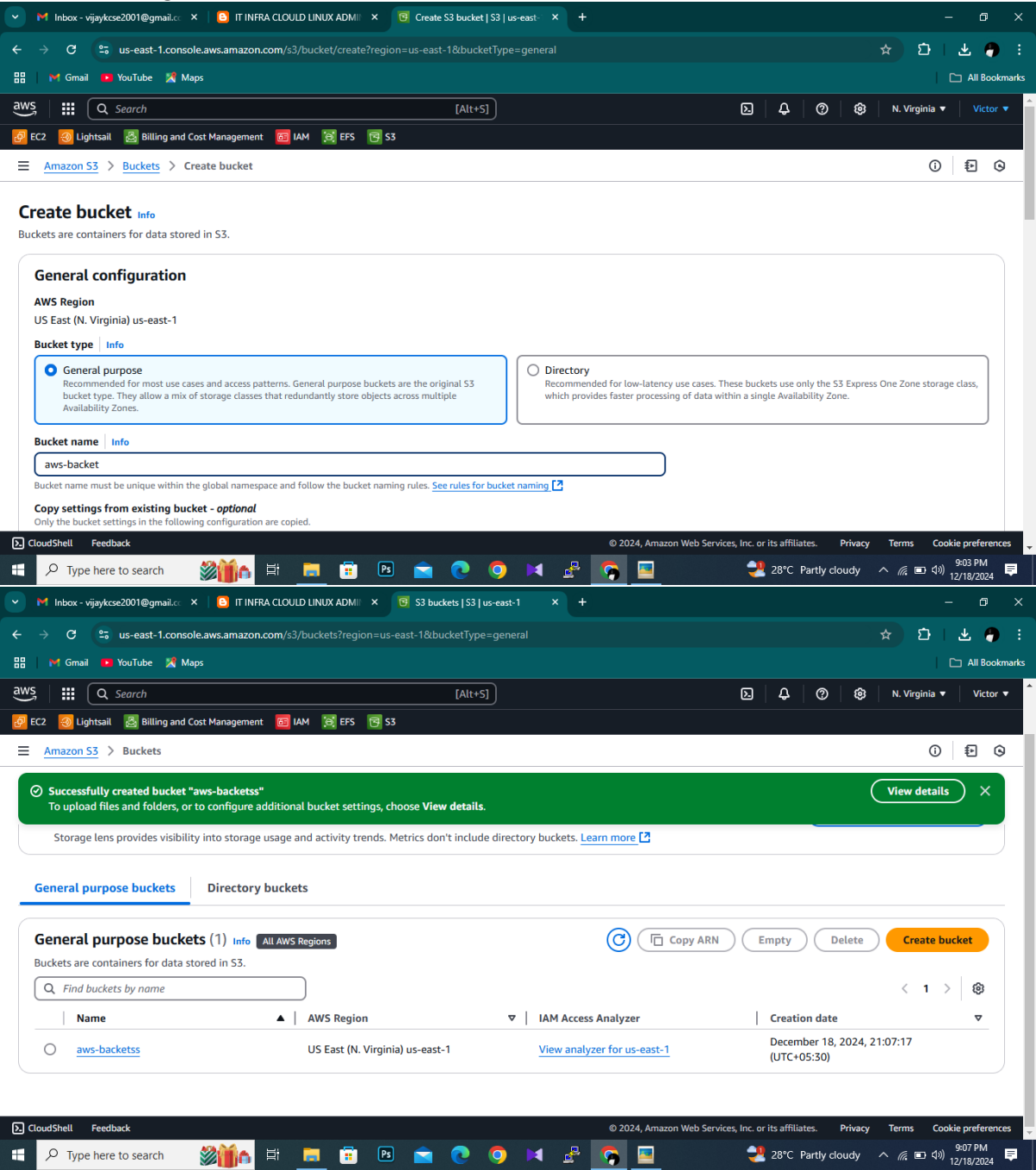
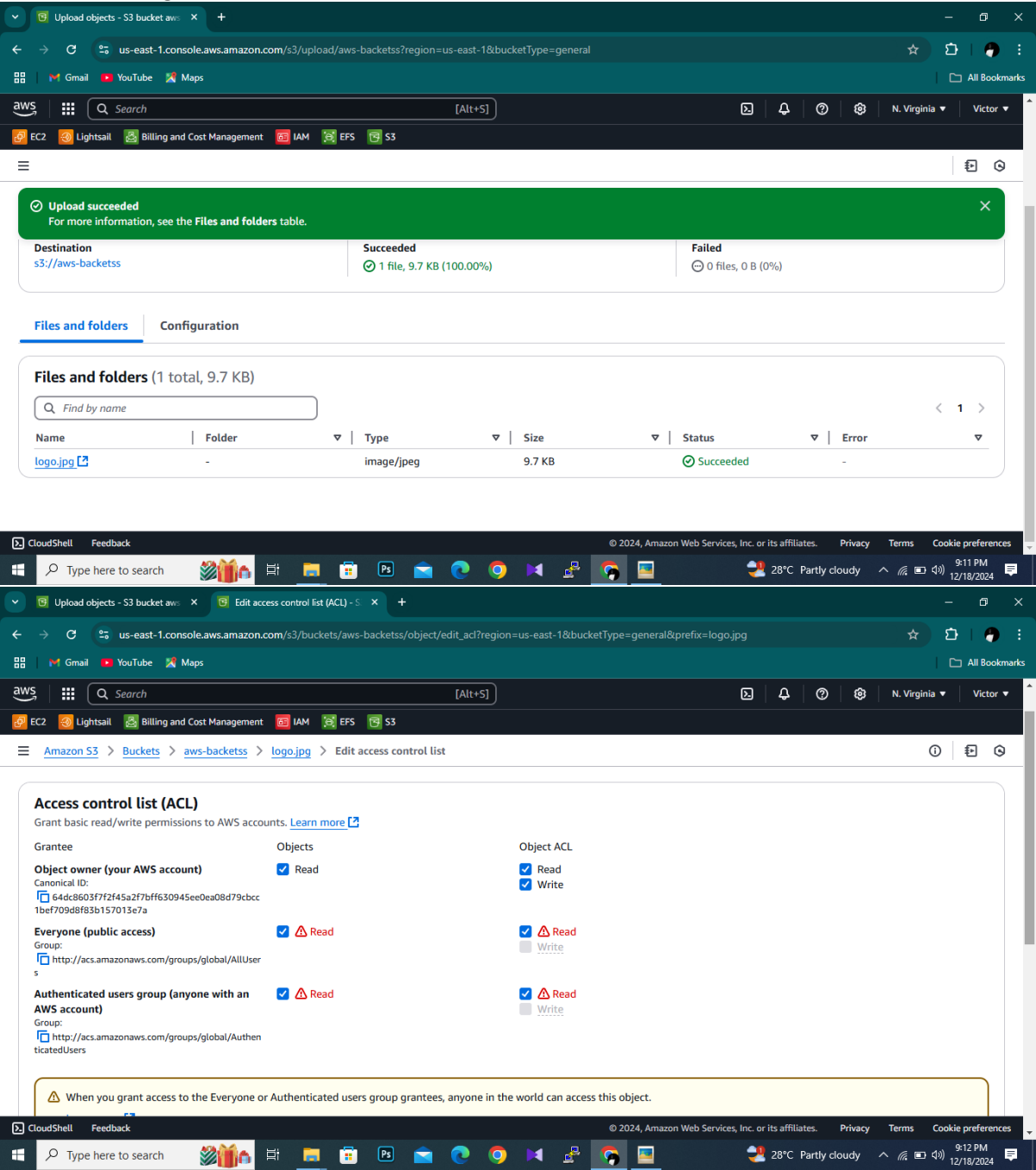


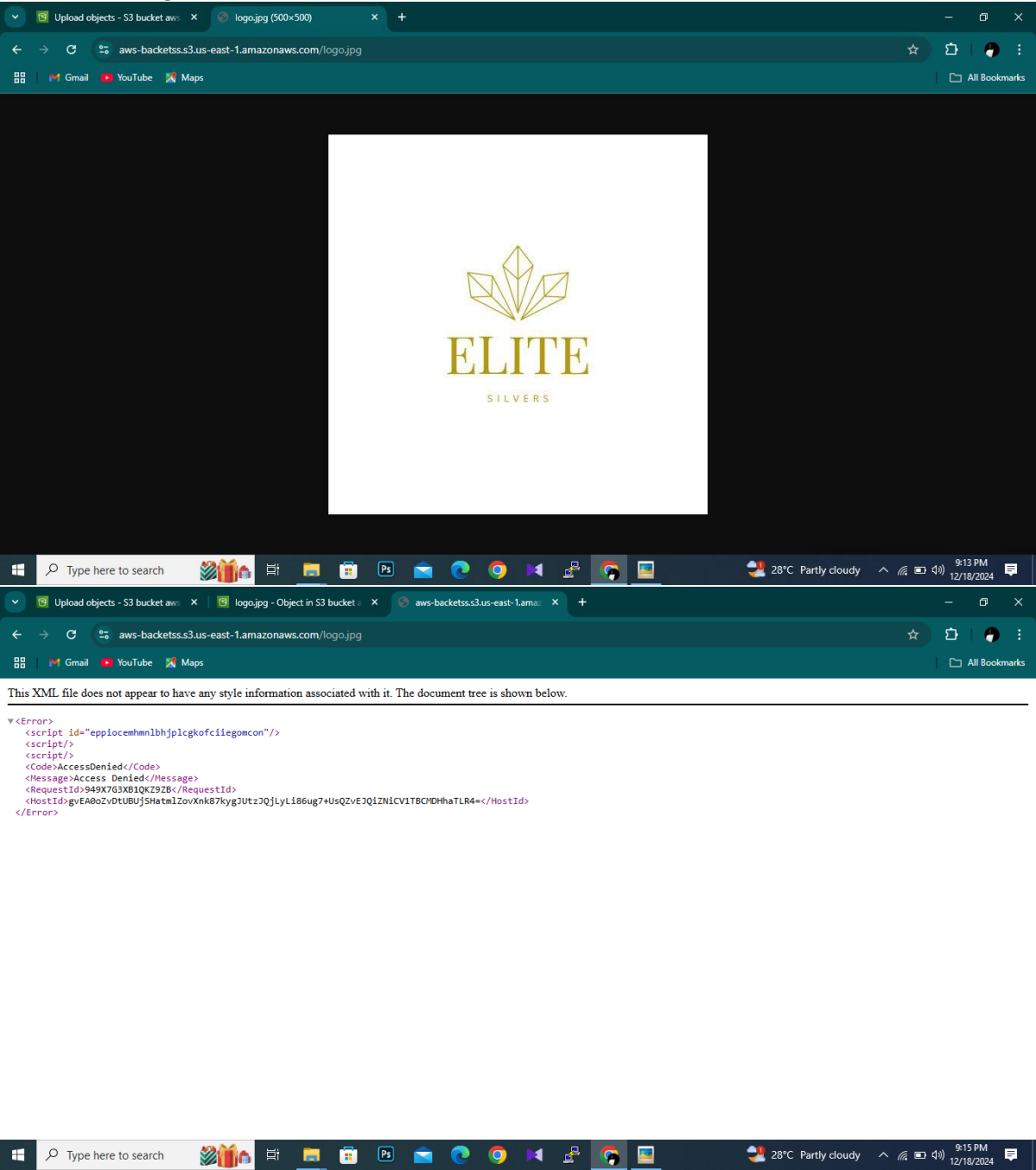
Expertly built and managed Amazon S3 buckets, implementing policies for access control and security. Utilized S3 and Glacier for efficient storage and backup solutions. Configured bucket policies to restrict access, enabled default encryption for data security, and set up S3 buckets for seamless sharing of static website content.



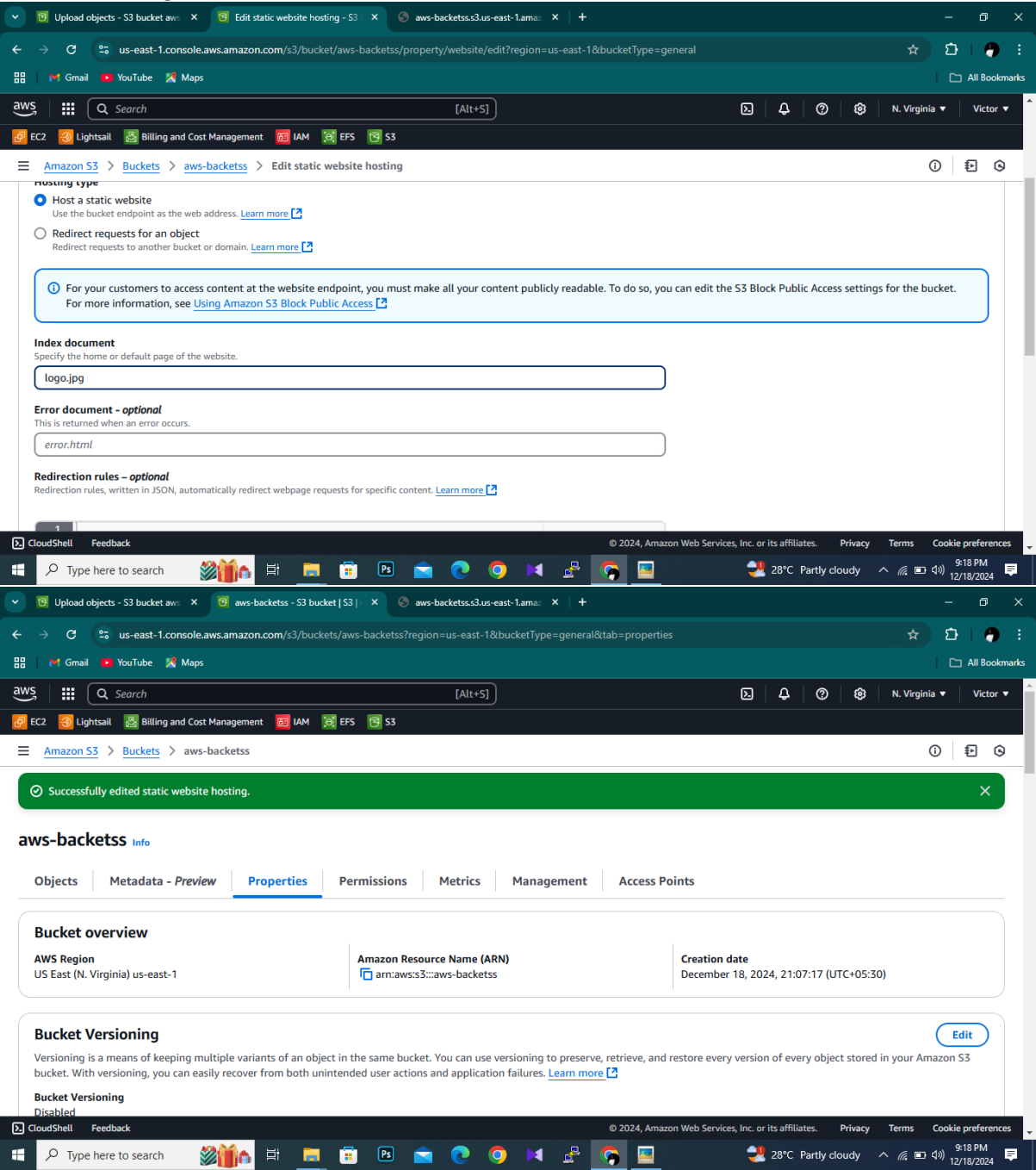
Expertly built and managed Amazon S3 buckets, implementing policies for access control and security. Utilized S3 and Glacier for efficient storage and backup solutions. Configured bucket policies to restrict access, enabled default encryption for data security, and set up S3 buckets for seamless sharing of static website content.



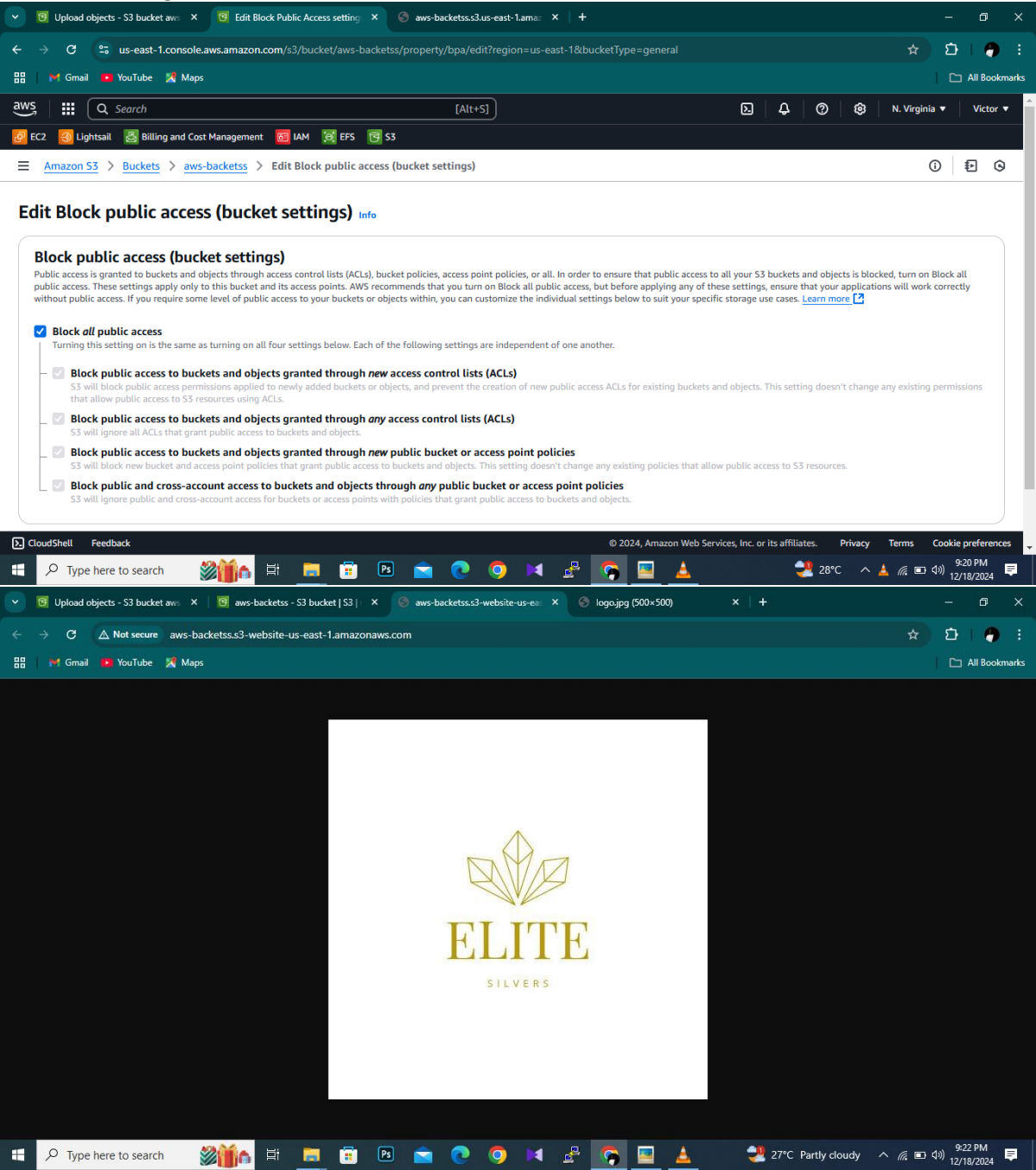
Expertly built and managed Amazon S3 buckets, implementing policies for access control and security. Utilized S3 and Glacier for efficient storage and backup solutions. Configured bucket policies to restrict access, enabled default encryption for data security, and set up S3 buckets for seamless sharing of static website content.



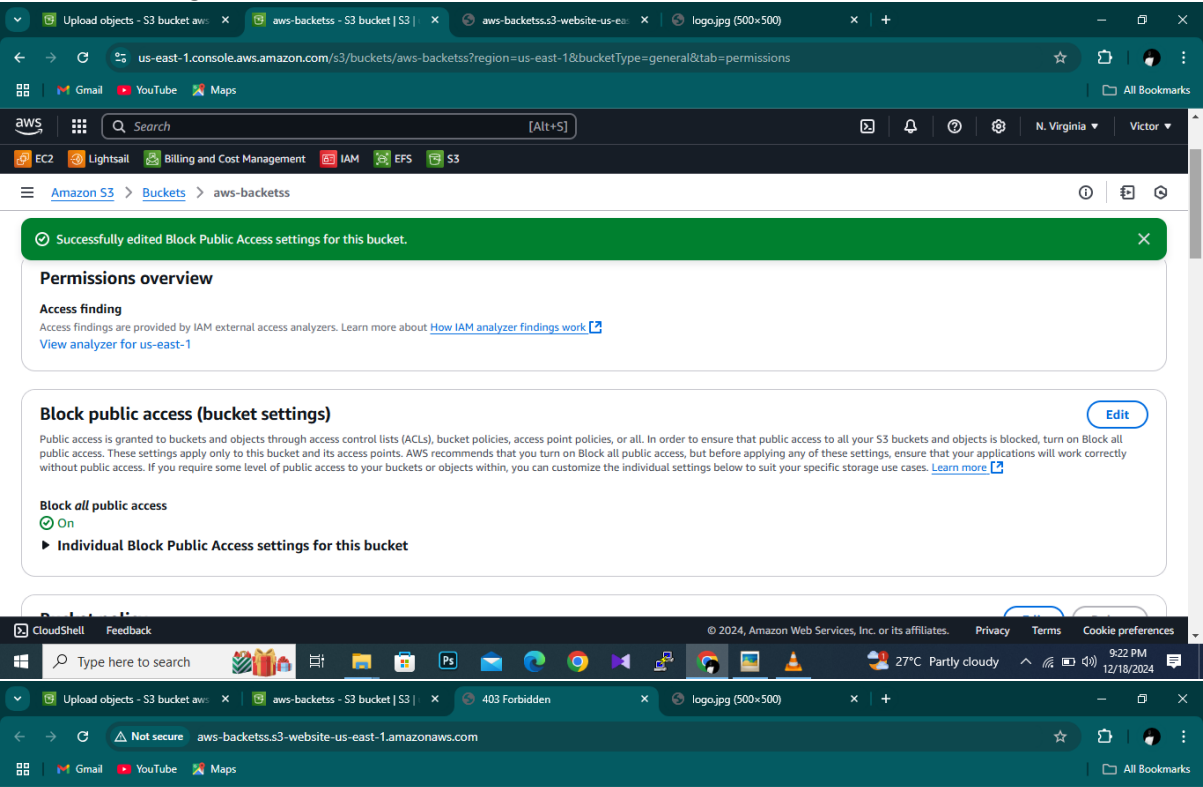
Expertly built and managed Amazon S3 buckets, implementing policies for access control and security. Utilized S3 and Glacier for efficient storage and backup solutions. Configured bucket policies to restrict access, enabled default encryption for data security, and set up S3 buckets for seamless sharing of static website content.



Expertly built and managed Amazon S3 buckets, implementing policies for access control and security. Utilized S3 and Glacier for efficient storage and backup solutions. Configured bucket policies to restrict access, enabled default encryption for data security, and set up S3 buckets for seamless sharing of static website content.



Expertly built and managed Amazon S3 buckets, implementing policies for access control and security. Utilized S3 and Glacier for efficient storage and backup solutions. Configured bucket policies to restrict access, enabled default encryption for data security, and set up S3 buckets for seamless sharing of static website content.



## 403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: 0KXQX800119RXB8M
- HostId: uVRE/AhR/RTQ/xks43kpK9sr5Eaw4x++vSFBu/mbtzTkjL2r4W/SLvzIPFnMHFvYvT7LYUHzoEg=



Expertly built and managed Amazon S3 buckets, implementing policies for access control and security. Utilized S3 and Glacier for efficient storage and backup solutions. Configured bucket policies to restrict access, enabled default encryption for data security, and set up S3 buckets for seamless sharing of static website content.

**Create lifecycle rule** [Info](#)

**Lifecycle rule configuration**

**Lifecycle rule name**

Up to 255 characters

Choose a rule scope

☐ Limit the scope of this rule using one or more filters

☒ Apply to all objects in the bucket

**⚠ Apply to all objects in the bucket**  
If you want the rule to apply to specific objects, you must use a filter to identify those objects. Choose "Limit the scope of this rule using one or more filters". [Learn more](#)

☒ I acknowledge that this rule will apply to all objects in the bucket.

☐ Expire current versions of objects

☐ Permanently delete noncurrent versions of objects

☒ Delete expired object delete markers or incomplete multipart uploads  
These actions are not supported when filtering by object tags or object size.

**Delete expired object delete markers or incomplete multipart uploads**

**Expired object delete markers**  
This action will remove expired object delete markers and may improve performance. An expired object delete marker is removed if all noncurrent versions of an object expire after deleting a versioned object. This action is not available when "Expire current versions of objects" is selected. [Learn more](#)

☒ Delete expired object delete markers

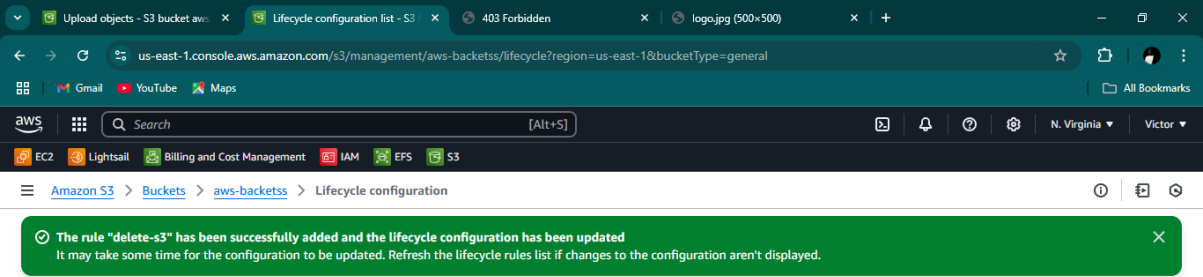
**Incomplete multipart uploads**  
This action will stop all incomplete multipart uploads, and the parts associated with the multipart upload will be deleted. [Learn more](#)

☒ Delete incomplete multipart uploads

**Number of days**

Integer must be greater than 0.

Expertly built and managed Amazon S3 buckets, implementing policies for access control and security. Utilized S3 and Glacier for efficient storage and backup solutions. Configured bucket policies to restrict access, enabled default encryption for data security, and set up S3 buckets for seamless sharing of static website content.



**Lifecycle configuration** [Info](#)

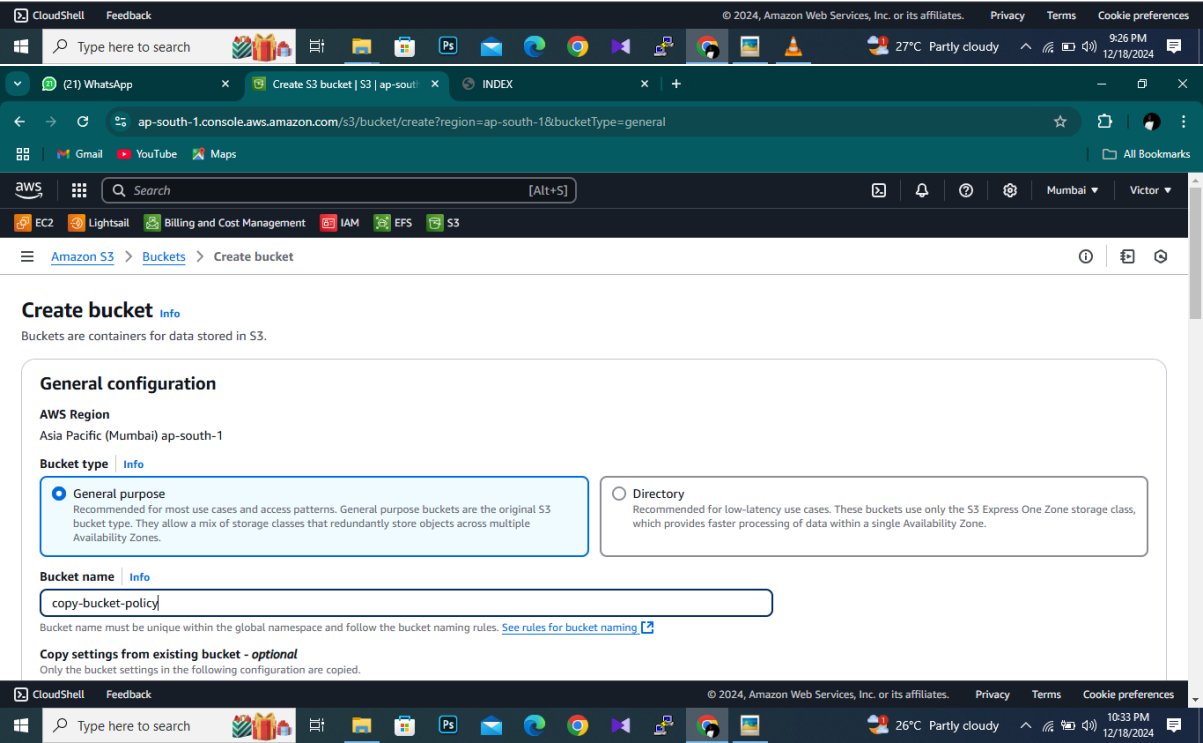
To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle. A lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. Lifecycle rules run once per day.

**Lifecycle rules (1)**

Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time. [Learn more](#)

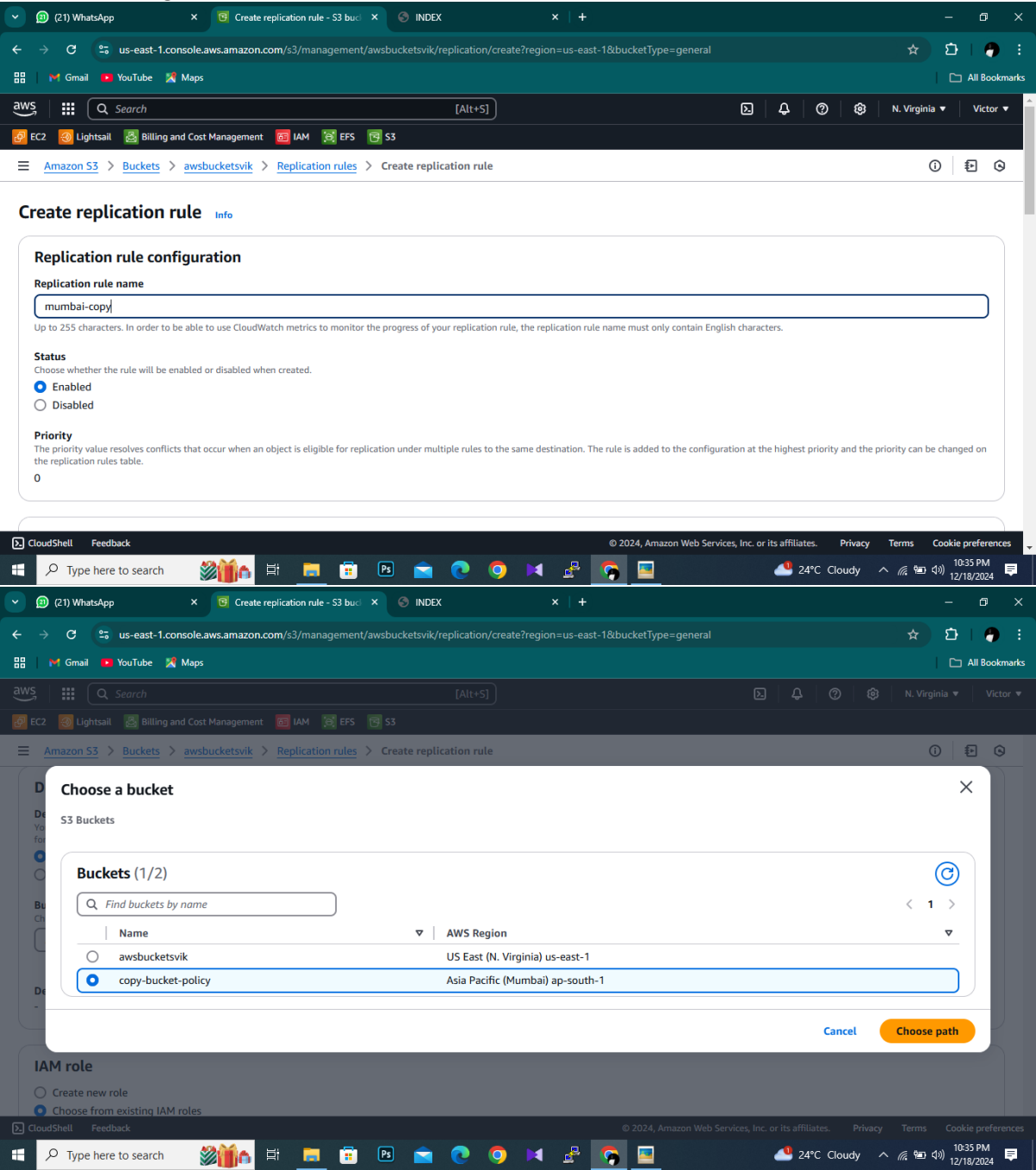
< 1 >

Lifecycle rule na...	Status	Scope	Current version ...	Noncurrent vers...	Expired object d...	Incomplete multipa...
<a href="#">delete-s3</a>	Enabled	Entire bucket	-	-	Permanently delete	Permanently delete

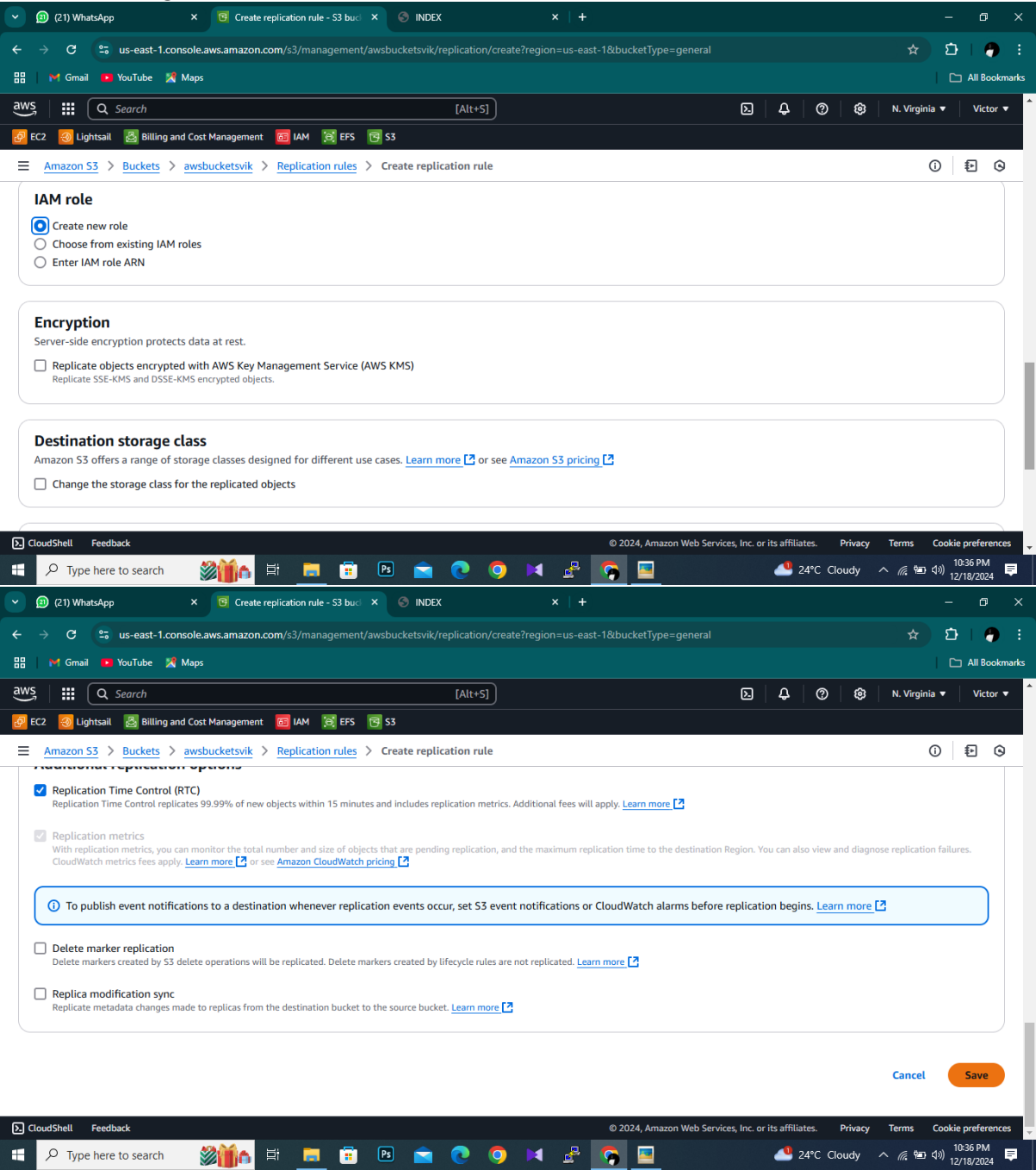




Expertly built and managed Amazon S3 buckets, implementing policies for access control and security. Utilized S3 and Glacier for efficient storage and backup solutions. Configured bucket policies to restrict access, enabled default encryption for data security, and set up S3 buckets for seamless sharing of static website content.



Expertly built and managed Amazon S3 buckets, implementing policies for access control and security. Utilized S3 and Glacier for efficient storage and backup solutions. Configured bucket policies to restrict access, enabled default encryption for data security, and set up S3 buckets for seamless sharing of static website content.



Expertly built and managed Amazon S3 buckets, implementing policies for access control and security. Utilized S3 and Glacier for efficient storage and backup solutions. Configured bucket policies to restrict access, enabled default encryption for data security, and set up S3 buckets for seamless sharing of static website content.

