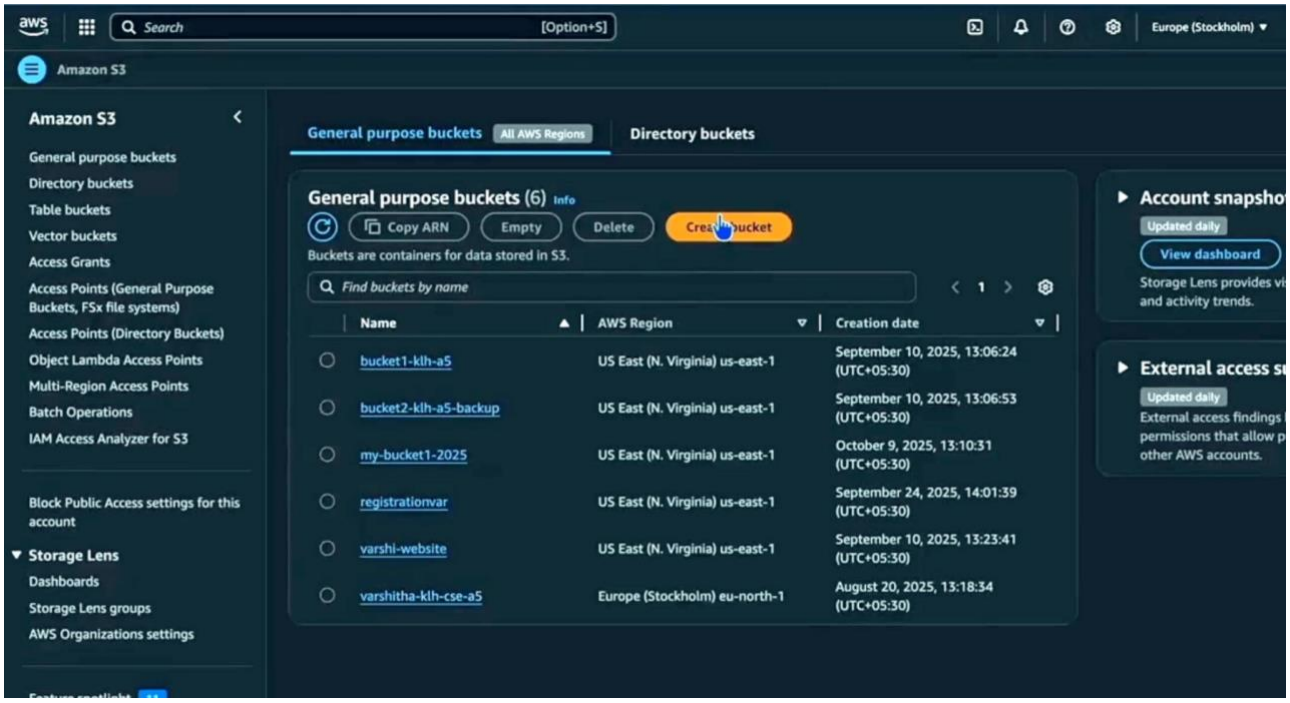
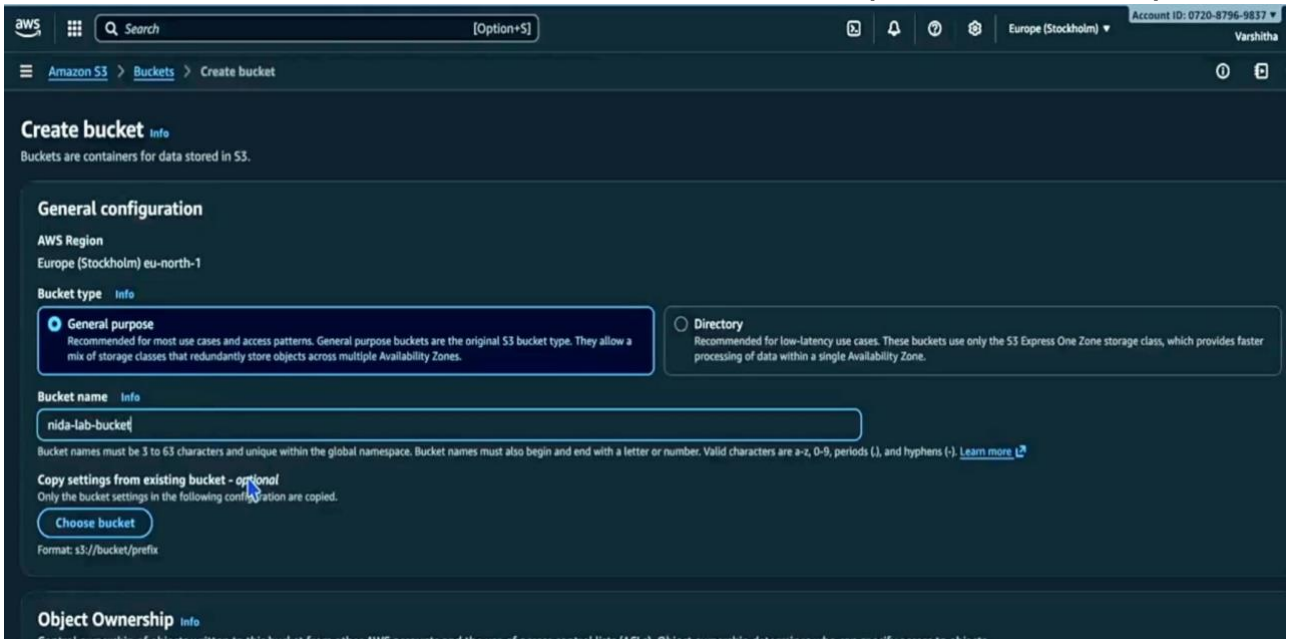
Create a Secure EC2 Instance with S3 Access using IAM

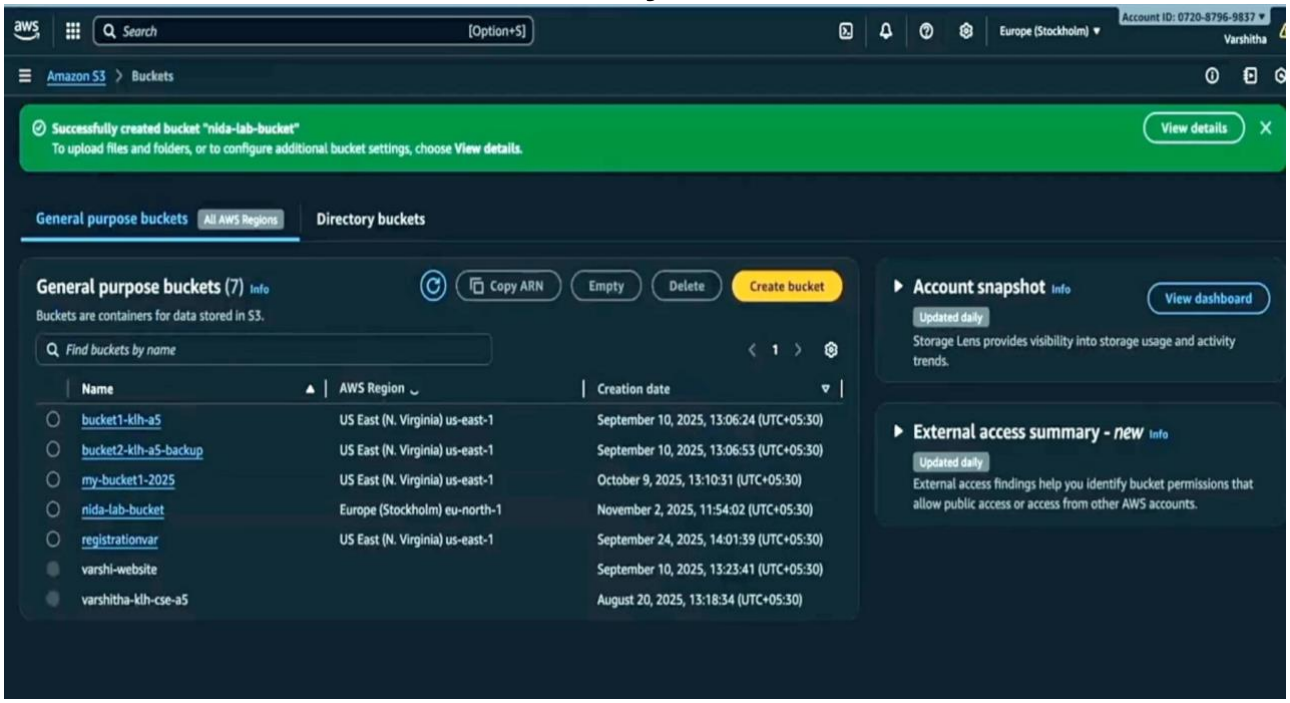
1. S3 Console — List of Buckets



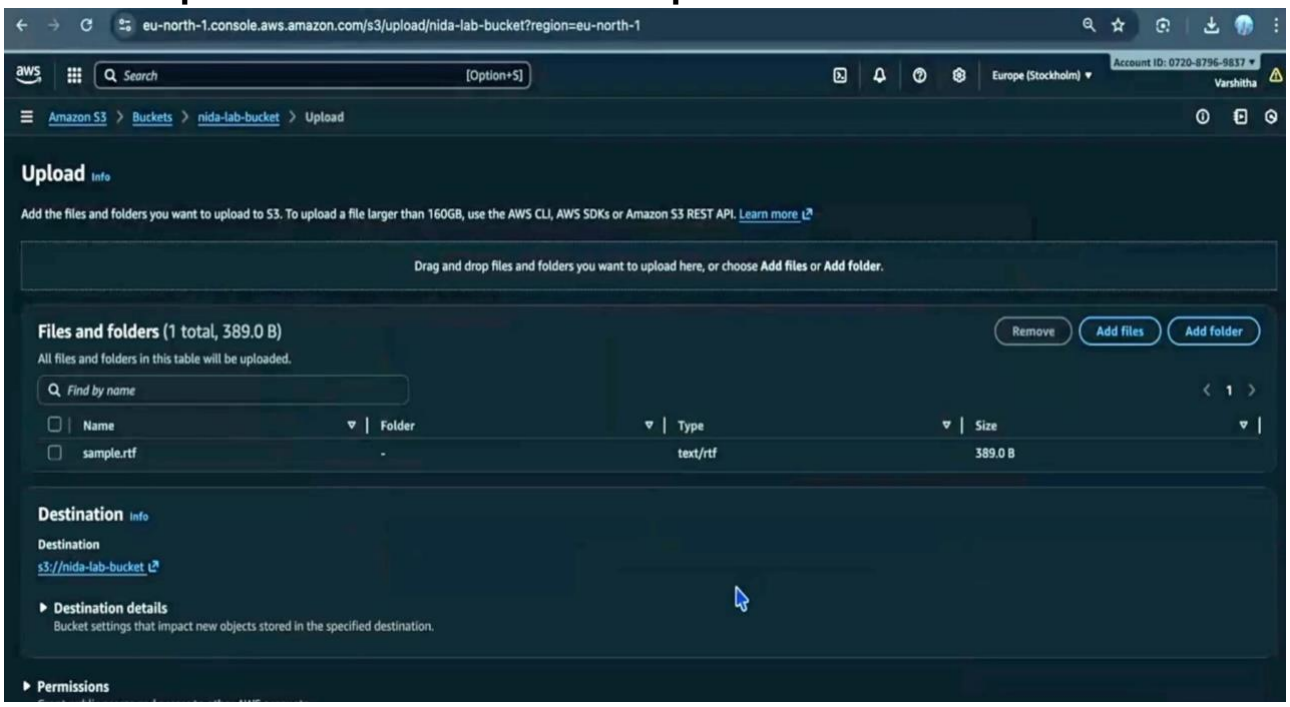
2. Create S3 Bucket — Enter bucket name (nida-lab-bucket)



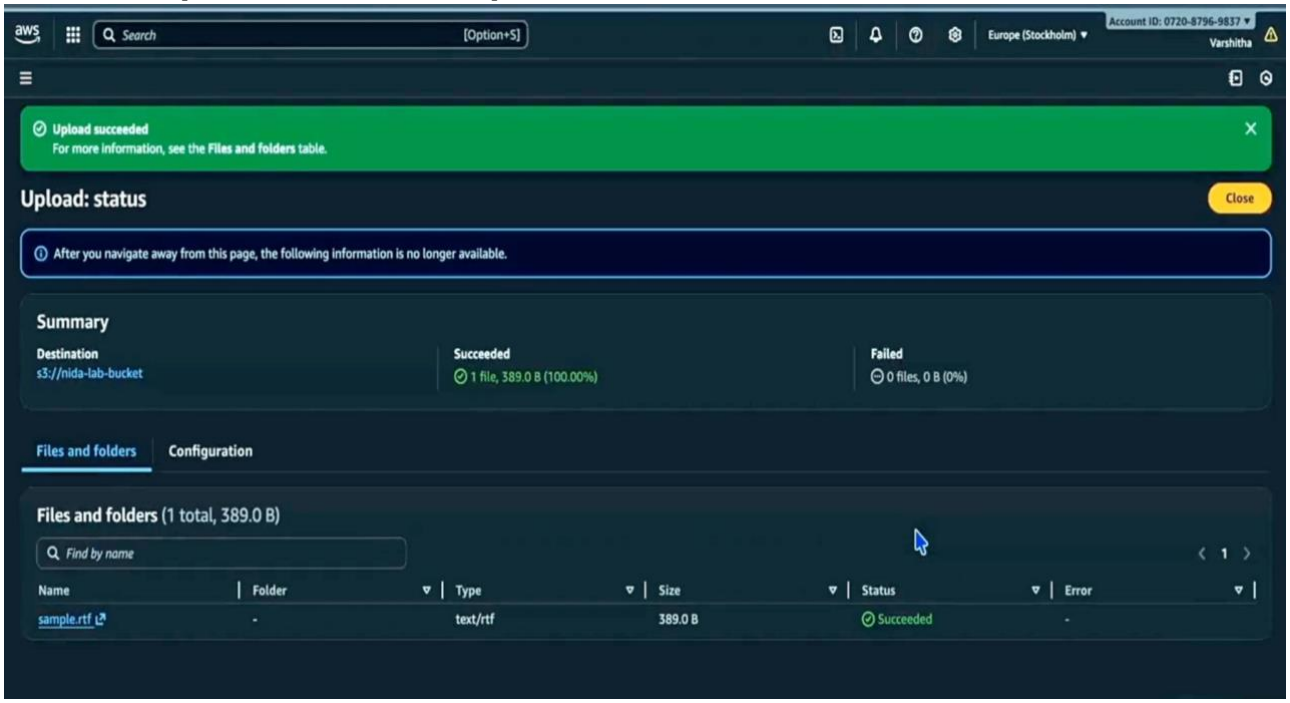
3. Bucket Created Successfully



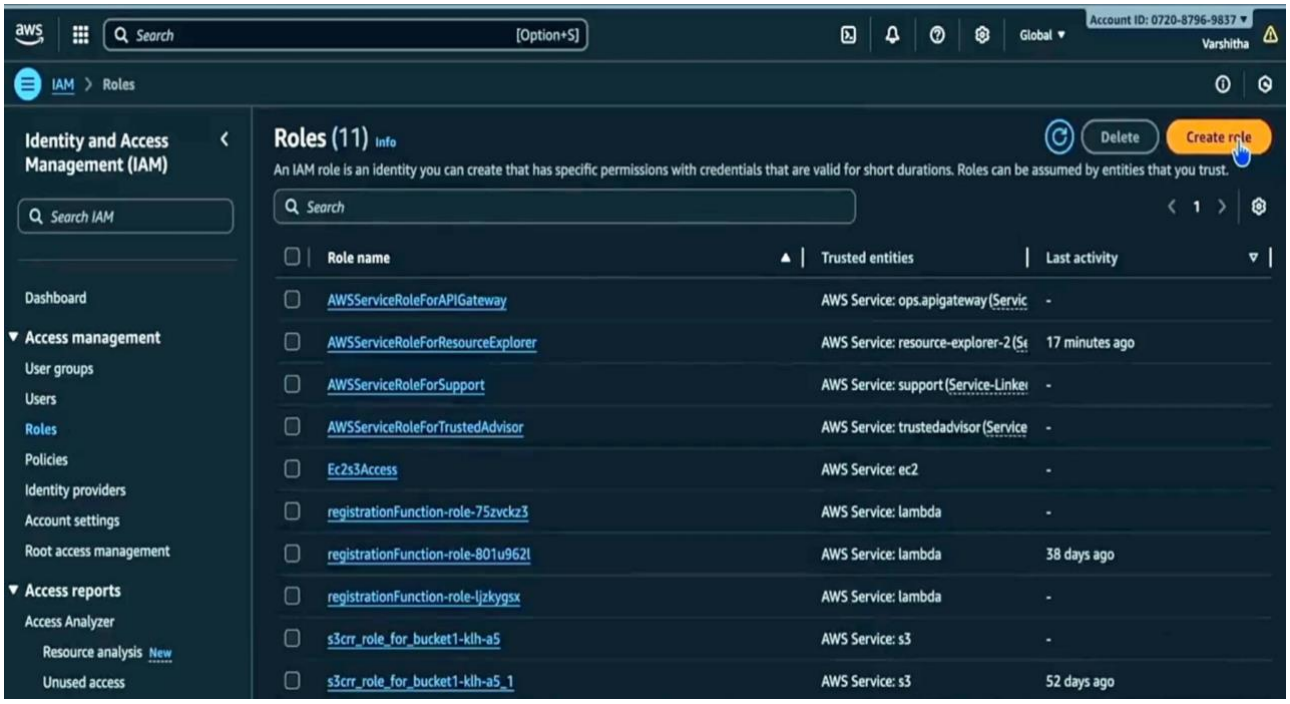
4. Upload File to S3 — Add sample.rtf



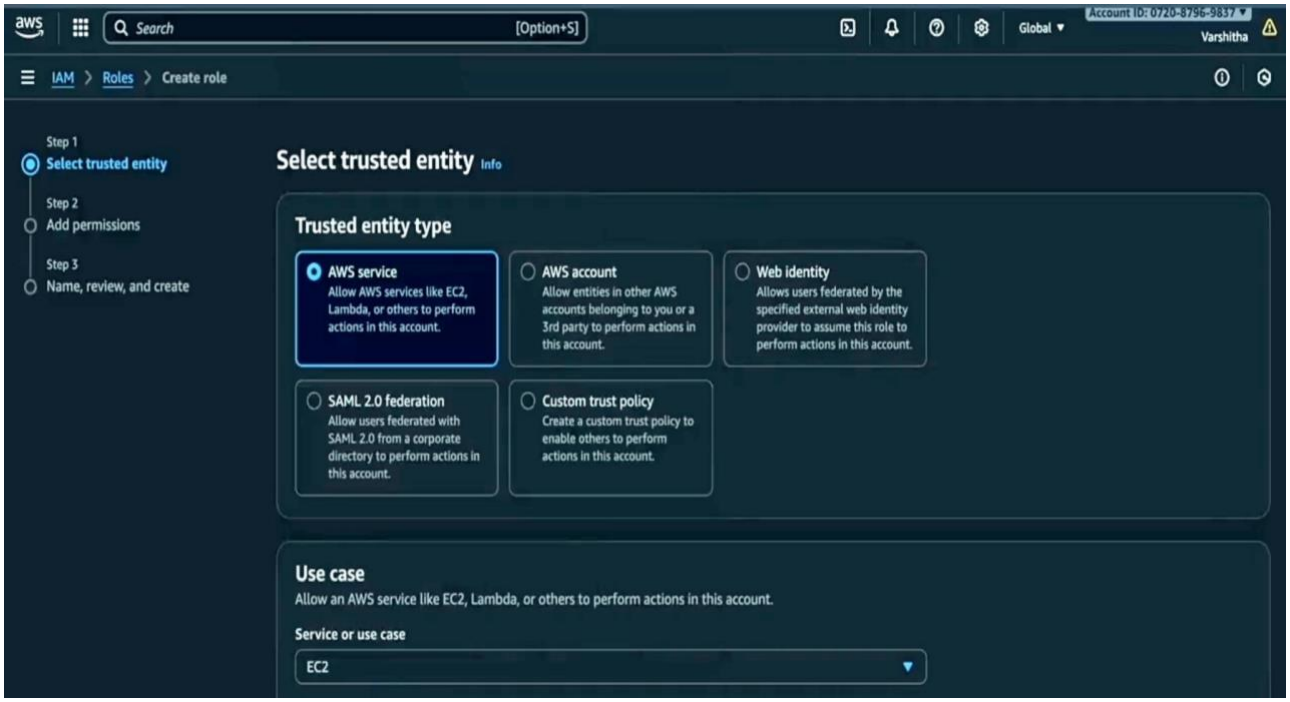
5. Upload Status — Upload succeeded



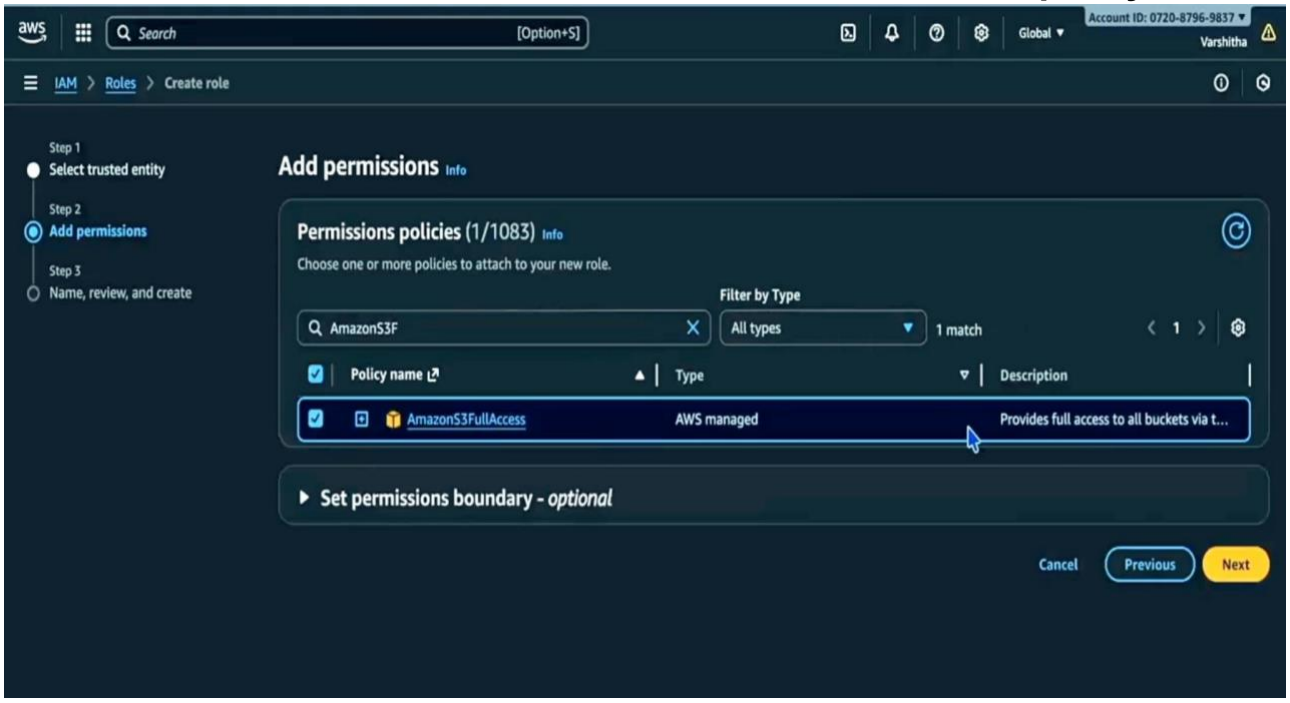
6. IAM Console



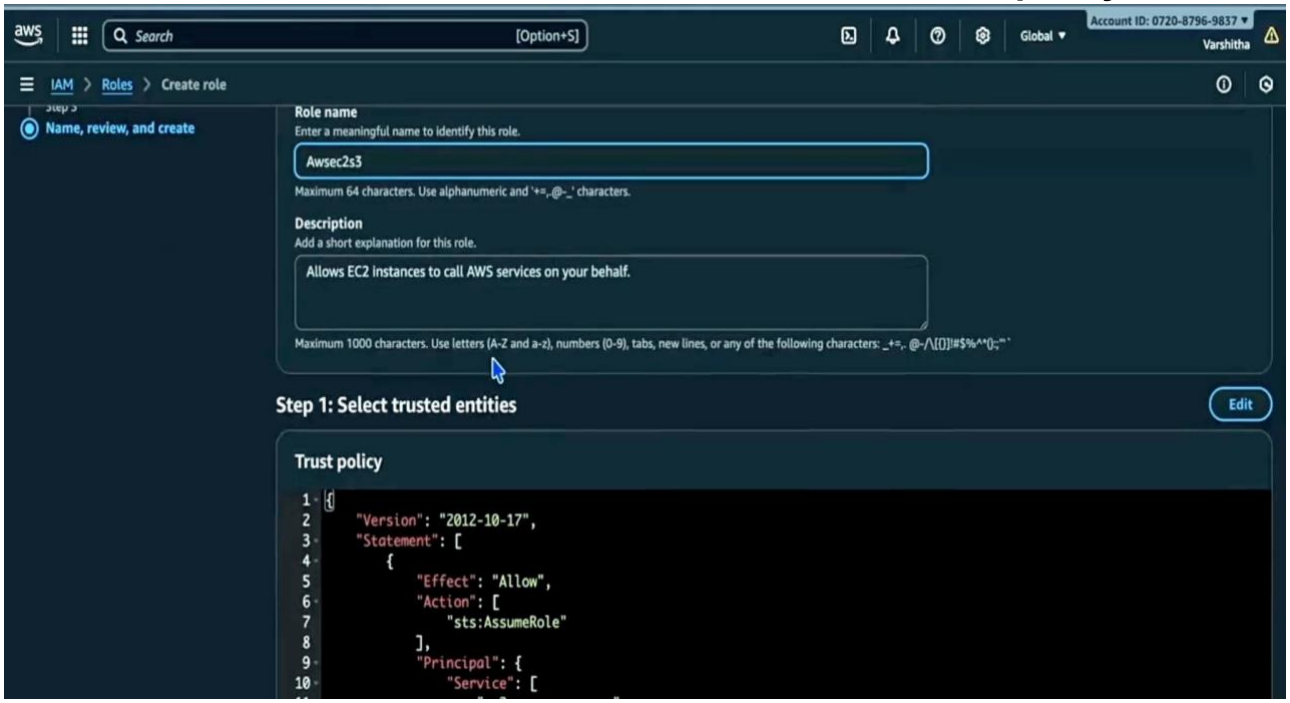
7. Create Role — Select trusted entity (AWS service → EC2)



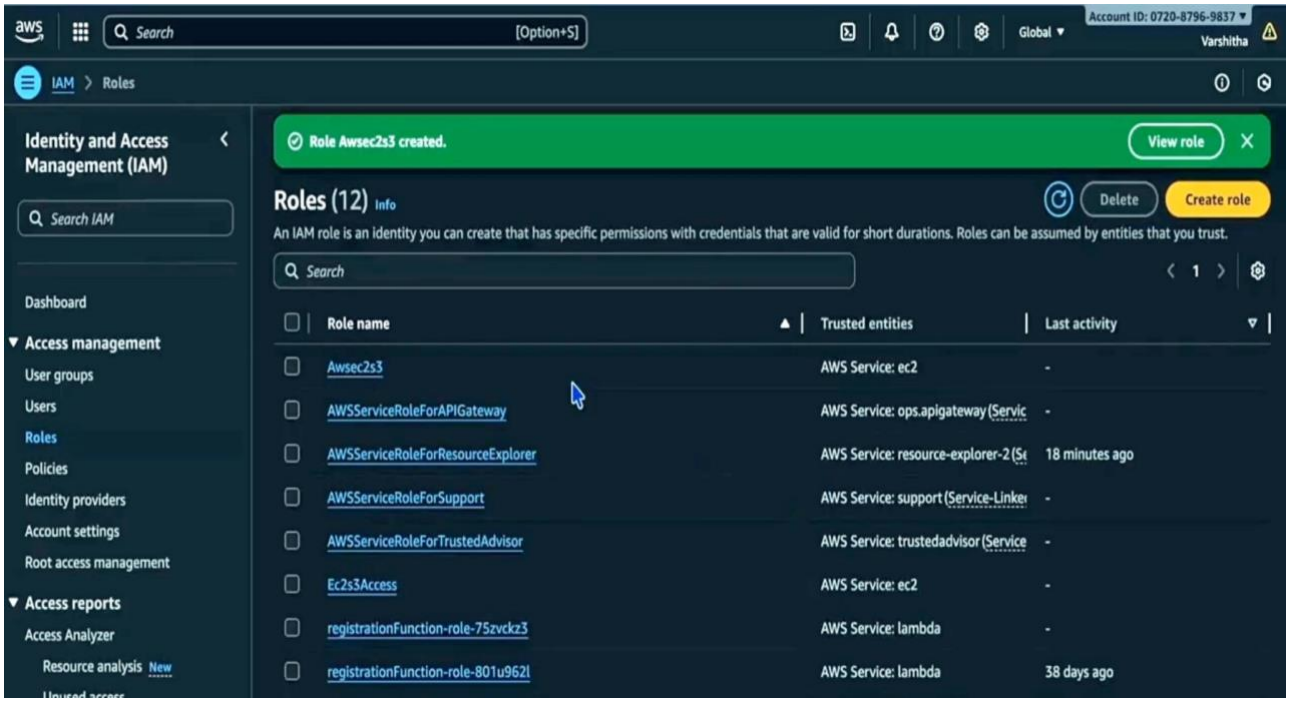
8. Add Permissions — Attach AmazonS3FullAccess policy



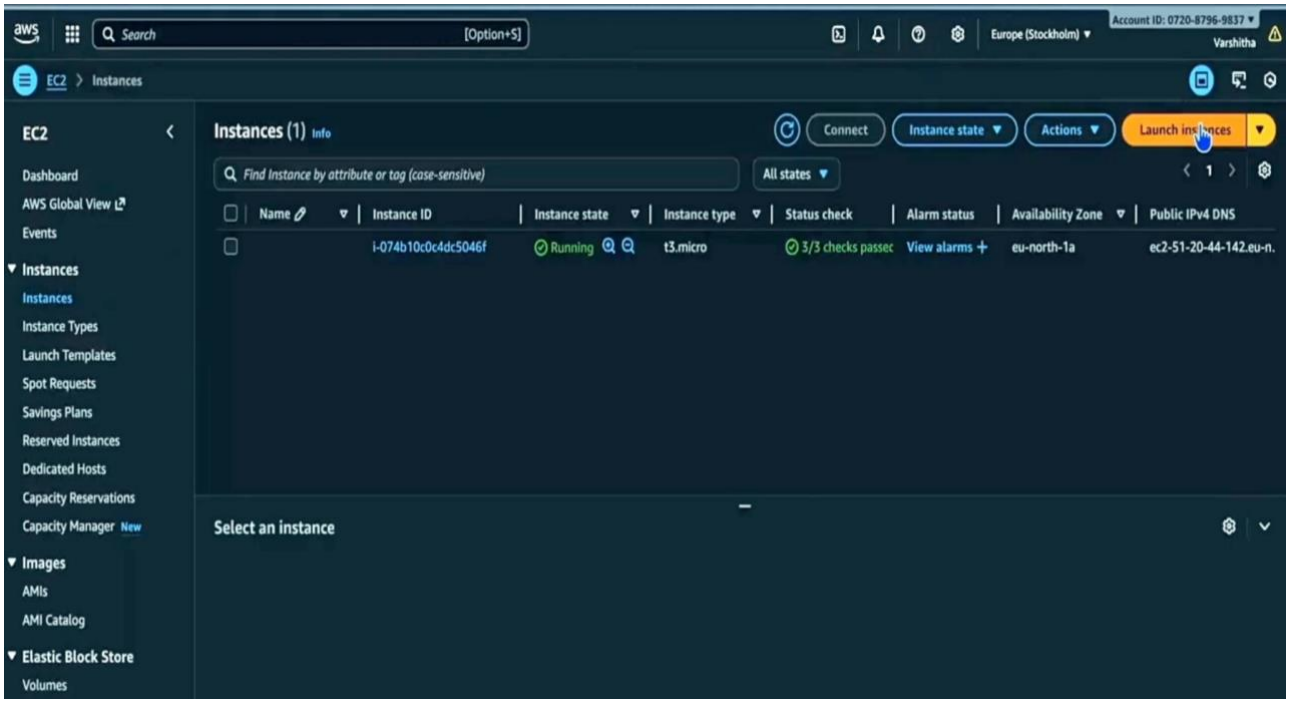
9. Role Details — Enter role name and review trust policy



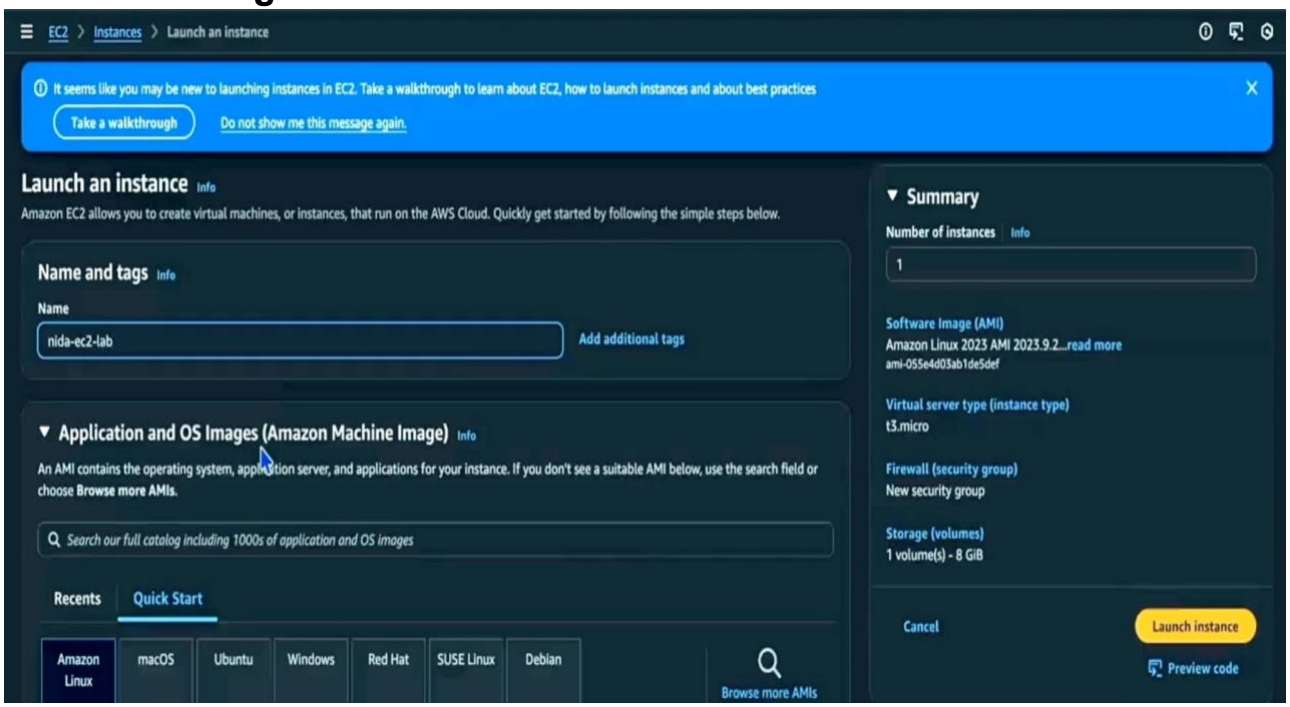
10. Role Created — Confirmation in Roles list



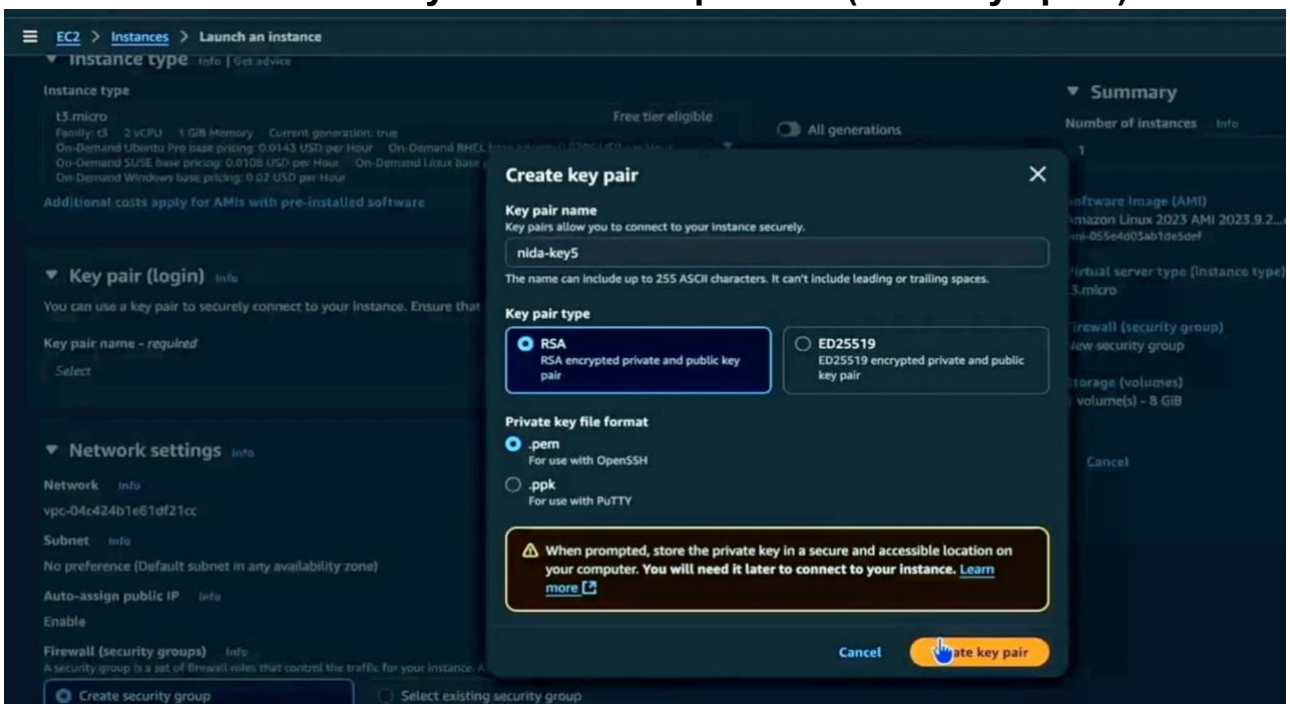
11. EC2 Console



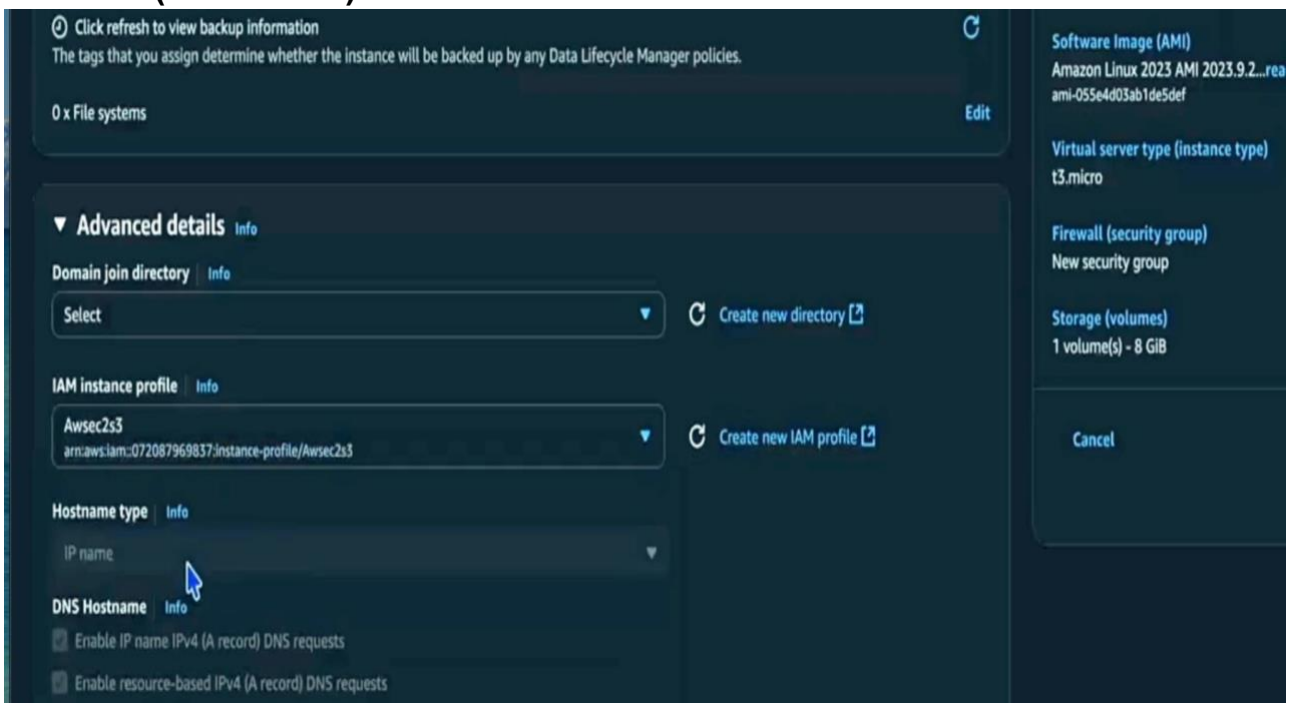
12. Launch Instance — Name, AMI selection and basic settings



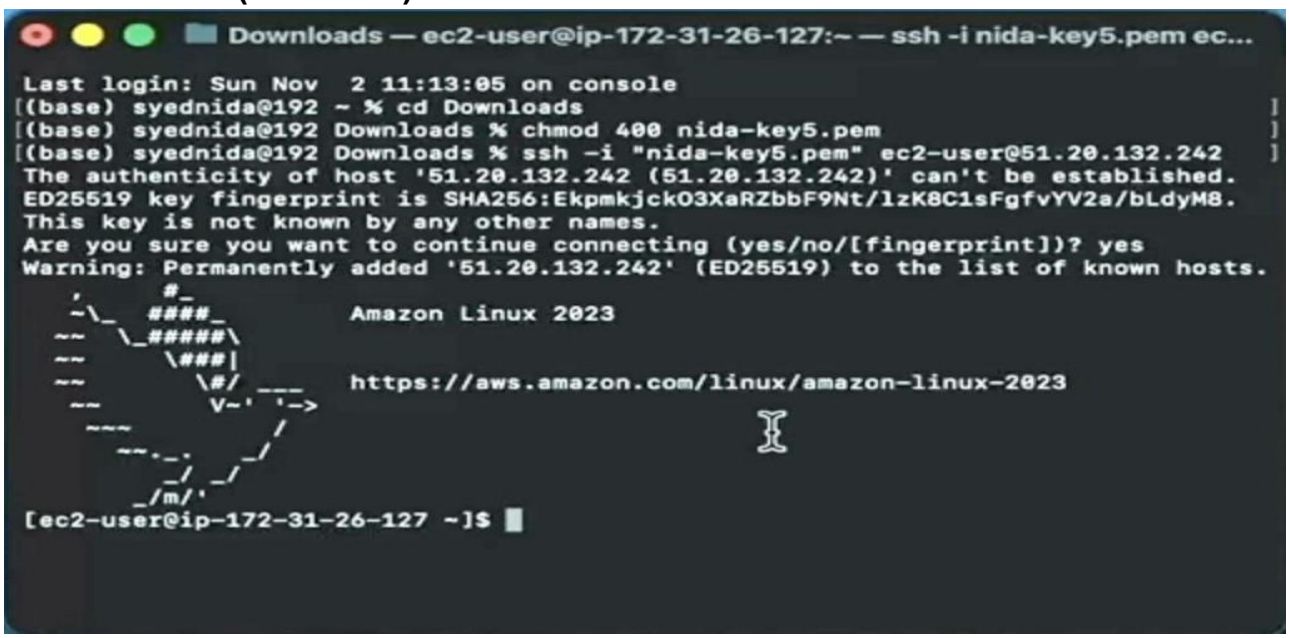
13. Create Key Pair — Save .pem file (nida-key5.pem)



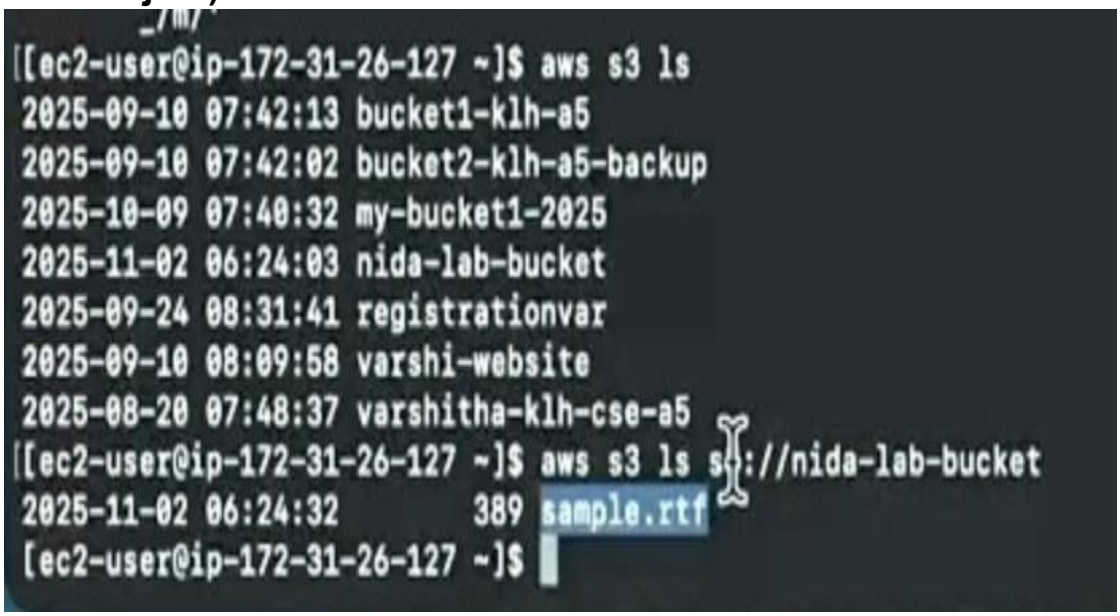
14. Advanced Details — IAM instance profile (Awsec2s3) attached



15. SSH Terminal — Successful SSH connection to EC2 (ec2-user)



16. AWS CLI — Verify S3 access (aws s3 ls and list object)



Conclusion

All steps were completed: an S3 bucket was created and a sample file uploaded. An IAM role with S3 access was created and attached to an EC2 instance. The EC2 instance successfully accessed the S3 bucket using the AWS CLI, confirming the configuration