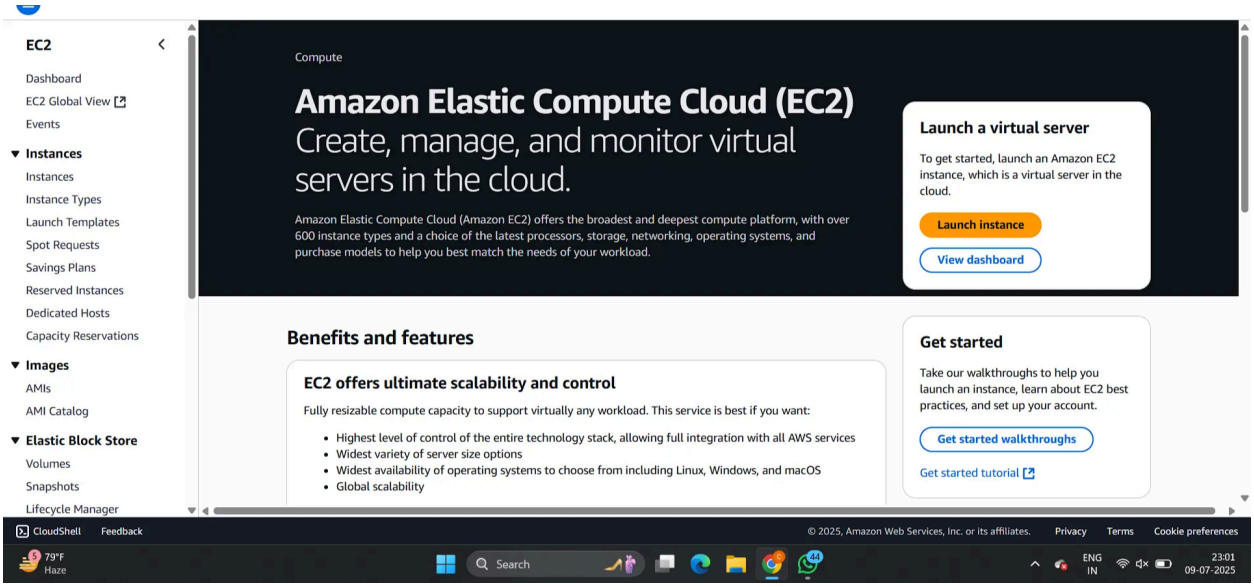
AWS Console Exploration (Read-Only Access)

Objective:

Explore the AWS Management Console with a focus on EC2 services, key pair formats, and configurations using **read-only access**. Document findings, provide screenshots, and prepare questions for follow-up.

1. Understand EC2 Options Before Deployment



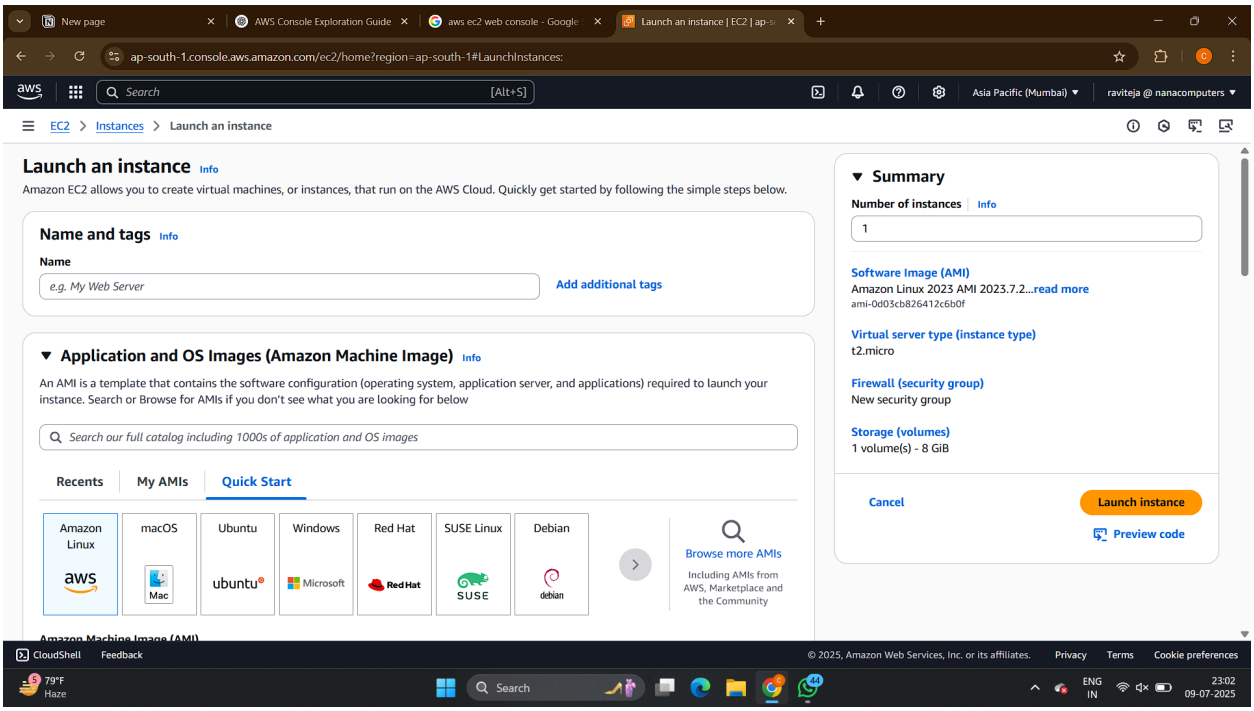
Instance Types Reviewed:

Category	Description	Example Types	Use Cases
General Purpose	Balanced CPU, memory, networking	t2, t3, t4g, m5	Web servers, dev/test
Compute Optimized	High-performance processors	c5, c6g	HPC, gaming servers
Memory Optimized	High memory-to-vCPU ratio	r5, x1e, z1d	In-memory DBs, analytics
Storage Optimized	High IOPS/disk throughput	i3, d3	NoSQL DBs, data warehousing

Category	Description	Example Types	Use Cases
Accelerated Computing	GPU/FPGA-based acceleration	p3, g4ad	ML, AI, graphic rendering

AMI Selection:

Type	Description	Example
Free-tier eligible	Amazon Linux 2, Ubuntu	`ami-0abcdef1234567890`
Licensed AMIs	Windows Server, RHEL, SUSE – billed hourly	Paid images



Security Groups:

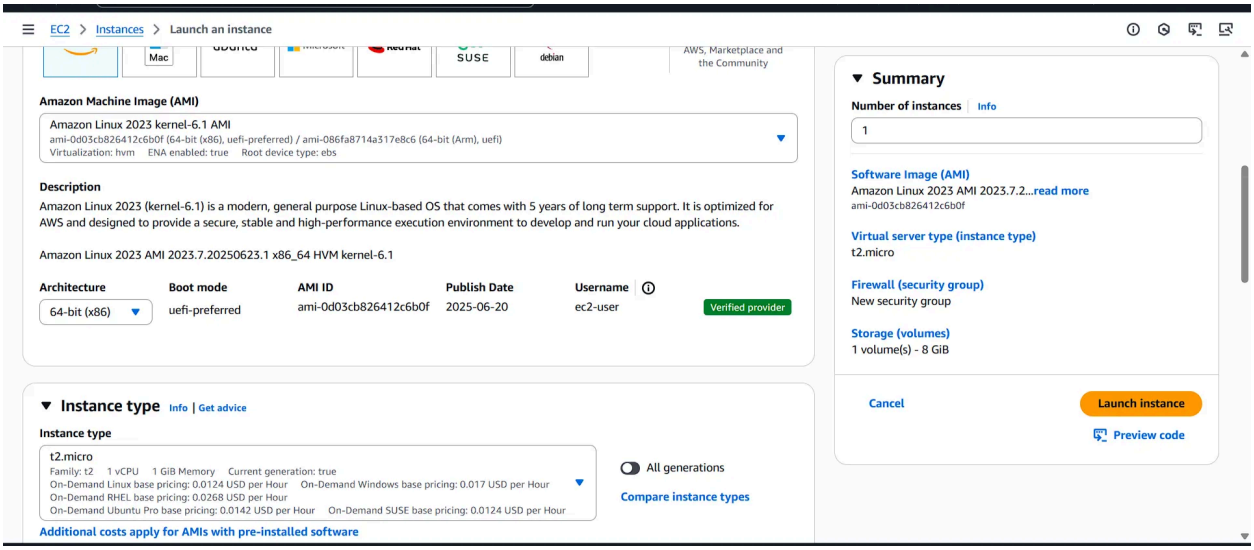
- **Inbound rules:** Allow incoming traffic to EC2 (e.g., SSH port 22, HTTP port 80)
- **Outbound rules:** Control outgoing traffic
- **Default SG:** Allows all outbound, no inbound by default

EC2 Storage – EBS Volume Types:

Type	Description	Best For
gp3	General-purpose SSD	Most workloads (default)
io1/io2	Provisioned IOPS SSD	High-performance DBs
st1	Throughput-optimized HDD	Big data, log processing
sc1	Cold HDD (infrequent access)	Archival
Magnetic (Standard)	Previous generation	Not recommended for new use

2. Explore AWS Console – Read-Only EC2 Access

EC2 Dashboard:



- View instance launch process: AMI → Instance type → Key pair → Network → Storage → Security Group → Review → Launch
- Even in read-only mode, you can click through each step

VPC Settings:

- Default VPC exists per region
- Contains default subnets, route tables, internet gateways

- Custom VPCs can be created for isolated networking needs

Security Group Configuration:

- Default: No inbound rules, allow all outbound
- Custom rules can allow access via port (e.g., SSH for Linux, RDP for Windows)

Screenshot: Security Group detail with rule types

3. Review PPK & Key Pair Formats

Key Pair Types:

Format	OS / Tool	Description
.pem	Linux/macOS, CLI tools	Used by OpenSSH (chmod 400 for SSH)
.ppk	Windows (PuTTY)	PuTTY Private Key format

Convert PEM to PPK:

Steps using PuTTYgen:

1. Open PuTTYgen (download from https://www.puttygen.com/)
2. Click "Load", select `.pem` file (choose “All Files” in file type)
3. Click “Save private key” → generates `.ppk` file
4. Use in PuTTY to connect to EC2