AWS Exam - feb 2025, John Bryce

Section 1: Multiple Choice Questions (MCQs)

1. **C**
2. **A**
3. **C**

4. **A**
5. **B**

6. **B**
7. **A**

8. **B**
9. **C**

10. **C**
11. **A**

12. AWS Landing Zones are essentially blueprints for setting up a secure, multi-account AWS environment that adheres to best practices right from the start. They help organizations quickly establish a standardized architecture by automating the provisioning of accounts, networks, and security baselines. Here's how they contribute to multi-account governance such as Standardized Account Structure, Centralized Governance, security and Compliance Automation Scalability and Flexibility.

13. AWS WAF (Web Application Firewall) is designed to protect web applications by monitoring, filtering, and blocking malicious HTTP and HTTPS traffic before it reaches your backend servers. Here one of many ways to protect your traffic in aws like Real-Time Monitoring and Logging:
AWS WAF integrates with Amazon CloudWatch, providing real-time metrics and logs that help you analyze traffic patterns and quickly identify potential security issues.

14. AWS Snowball is a secure, physical data transfer device designed to move large amounts of data into or out of the AWS Cloud. Here's what makes it valuable and when you should use it,
High-Volume Data Transfer:
Snowball is ideal for transferring terabytes to petabytes of data when network bandwidth is limited, unreliable, or too costly for a timely online transfer.
Physical Data Transport:
Instead of sending data over the internet, you load your data onto the Snowball device, which is then physically shipped back to AWS. This method can significantly reduce transfer times for large datasets.

15. AWS Backup and manual snapshot backups both serve the purpose of data protection, but they differ significantly in functionality, management, and automation. Here are the key differences:

Policy Enforcement & Compliance:

- **AWS Backup: Enables you to enforce backup policies organization-wide, ensuring compliance with governance and regulatory standards.**
- **Manual Snapshots: Lack centralized policy control, making it challenging to ensure uniform compliance.**

Integration with Other AWS Services:

- **AWS Backup: Seamlessly integrates with services like AWS Organizations, allowing centralized backup management across your entire AWS estate.**
- **Manual Snapshots: Limited to the native backup capabilities of each individual service.**

16. AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that helps safeguard your AWS applications by detecting and mitigating DDoS attacks in real time. Here is one example:

Automated Detection & Mitigation:

- **AWS Shield Standard: Automatically protects your applications against common network and transport layer DDoS attacks (like SYN/UDP floods or reflection attacks) without any additional configuration. It leverages AWS's global infrastructure to detect abnormal traffic patterns and immediately starts mitigating the attack.**
- **AWS Shield Advanced: Offers enhanced detection capabilities with deeper visibility into sophisticated attacks. It provides additional mitigation strategies, which can be tailored to your application's specific needs.**

17. AWS Transit Gateway and VPC Peering both enable communication between VPCs, but they differ significantly in architecture, scalability, routing, and management. Here's a breakdown of the key differences:

Connectivity Model

- **AWS Transit Gateway:**
  - **Hub-and-Spoke Architecture: Acts as a central hub where multiple VPCs, on-premises networks, and even remote offices connect.**
  - **Transitive Routing: Allows any connected network to communicate with any other through the central gateway.**
- **VPC Peering:**
  - **Direct Connection: Establishes a one-to-one relationship between two VPCs.**
  - **No Transitive Routing: If VPC A is peered with VPC B and VPC B is peered with VPC C, A cannot communicate with C through B.**

Routing and Performance

- **AWS Transit Gateway:**
  - **Centralized Routing Tables: Offers centralized control over routing, making it easier to manage network paths and security boundaries across multiple connections.**
  - **Efficient Data Flow: Designed to handle high throughput and optimized for scenarios with multiple interconnections.**
- **VPC Peering:**
  - **Distributed Routing: Each VPC maintains its own routing tables, and routing is only configured for the directly connected peers.**
  - **Low Latency: Provides direct paths between two VPCs, which may result in lower latency in simple, pairwise scenarios.**

18. AWS Step Functions is a fully managed service that simplifies the orchestration of complex workflows by allowing you to coordinate multiple AWS services into serverless workflows like:

<u>Orchestration of AWS Services:</u>
It seamlessly integrates with services like AWS Lambda, ECS, Batch, and more. This allows you to break down complex processes into smaller, independent tasks that are executed in a specific order, reducing the need to write custom orchestration code.

19. AWS Control Tower simplifies and automates the process of managing multiple AWS accounts by providing a centralized, secure, and compliant multi-account environment. You can do is with Automated Landing Zone Setup: AWS Control Tower sets up a standardized, multi-account environment (called a landing zone) following AWS best practices. This includes configuring foundational services like identity management, logging, and security controls from the start. And with Pre-Configured Guardrails:
It implements preventive and detective guardrails—predefined policies that enforce compliance, security, and operational best practices across all accounts.
20. AWS Outposts plays a pivotal role in hybrid cloud solutions by seamlessly extending AWS infrastructure, services, and tools to on-premises environments. This integration brings several key benefits:

<u>Consistent Cloud Experience On-Premises:</u>
Outposts provides the same hardware, APIs, and management tools as in AWS regions, ensuring that developers and operations teams can build and manage applications uniformly across both environments.

<u>Low Latency and Local Data Processing:</u>
For applications requiring real-time processing or minimal latency, keeping compute and storage resources on-premises with Outposts ensures data is processed locally while still leveraging AWS services.

<u>Data Residency and Compliance:</u>
Organizations with strict regulatory or data residency requirements can store and process sensitive data on-site, while still benefiting from AWS's robust cloud capabilities.

And more.

21. AWS Elastic File System (EFS), Amazon S3, and Amazon EBS each provide storage solutions with distinct characteristics tailored to different use cases. Here's how EFS compares to S3 and EBS:

AWS Elastic File System (EFS)

- **Type: Fully managed, scalable network file system.**
- **Access: Provides a standard file system interface (NFS), enabling multiple EC2 instances or containers to share files concurrently.**
- **Scalability: Automatically scales as you add or remove files.**
- **Use Cases:**
  - **Shared File Storage: Ideal for applications where multiple instances need simultaneous access to the same files (e.g., content management systems, web serving, and collaborative tools).**
  - **Lift-and-Shift Applications: Good for legacy applications that expect a POSIX-compliant file system.**
  - **Big Data & Analytics: Can be used as a repository for data that is concurrently processed by multiple instances.**
  - **Container Storage: Supports containerized applications requiring persistent, shared storage.**

Amazon S3

- **Type: Object storage service.**
- **Access: Uses RESTful APIs; doesn’t offer POSIX file system semantics.**
- **Scalability: Highly scalable and designed for storing vast amounts of unstructured data.**
- **Use Cases:**
  - **Data Lakes & Big Data Analytics: Stores and organizes large datasets for analytics and machine learning.**
  - **Backup & Archiving: Durable storage for backups, archives, and disaster recovery.**
  - **Static Content Hosting: Ideal for hosting static websites, images, videos, and other unstructured content.**
  - **Application Data Storage: Serves as a backend for applications that can work with objects rather than files.**

Amazon EBS

- **Type: Block storage.**
- **Access: Provides low-level storage volumes that attach directly to EC2 instances (typically one instance at a time, with some exceptions).**
- **Performance: Offers high-performance, low-latency storage suitable for transactional workloads.**
- **Use Cases:**
  - **Databases & Transactional Applications: Perfect for applications requiring consistent low-latency block storage (e.g., relational databases, NoSQL databases).**

- **Boot Volumes & Persistent Storage: Used as the primary storage for operating systems and application data on EC2 instances.**
- **High-Performance Workloads: Provides configurable IOPS for performance-intensive applications.**

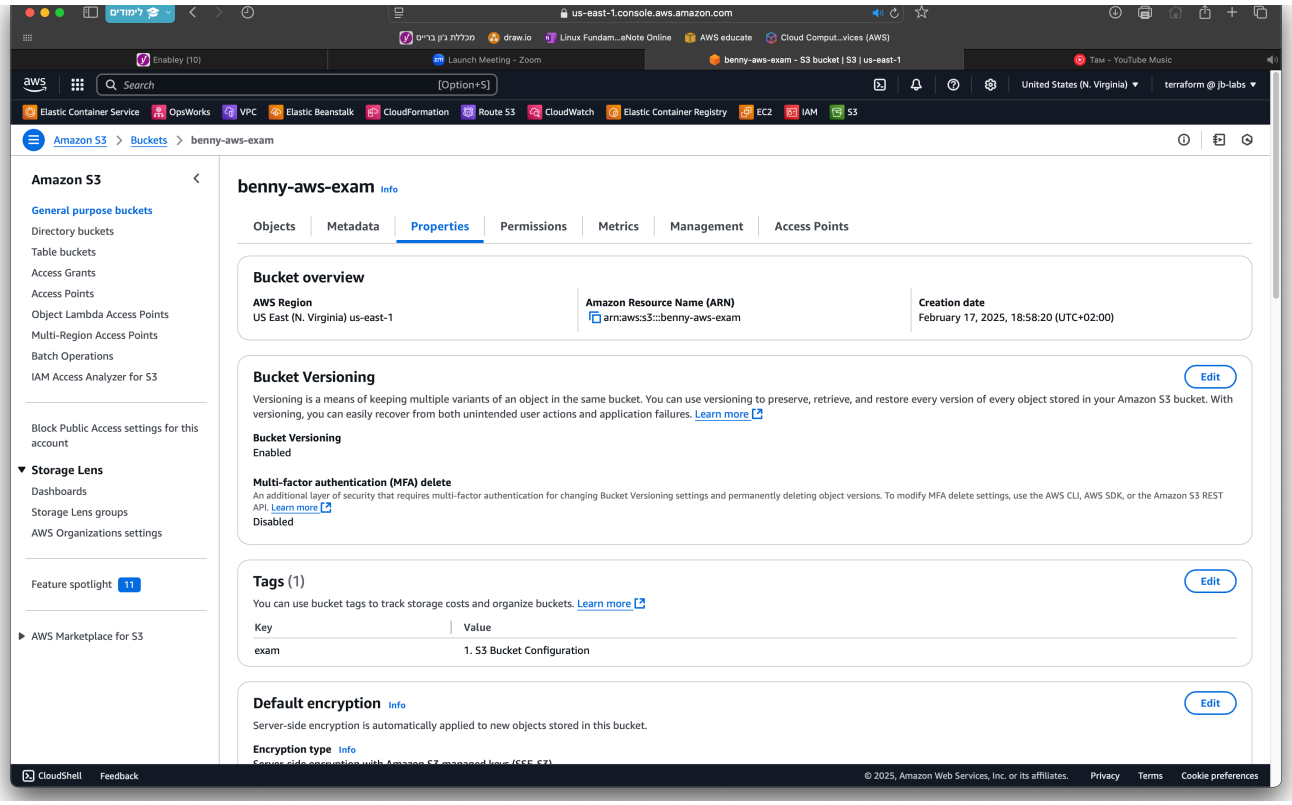
Summary

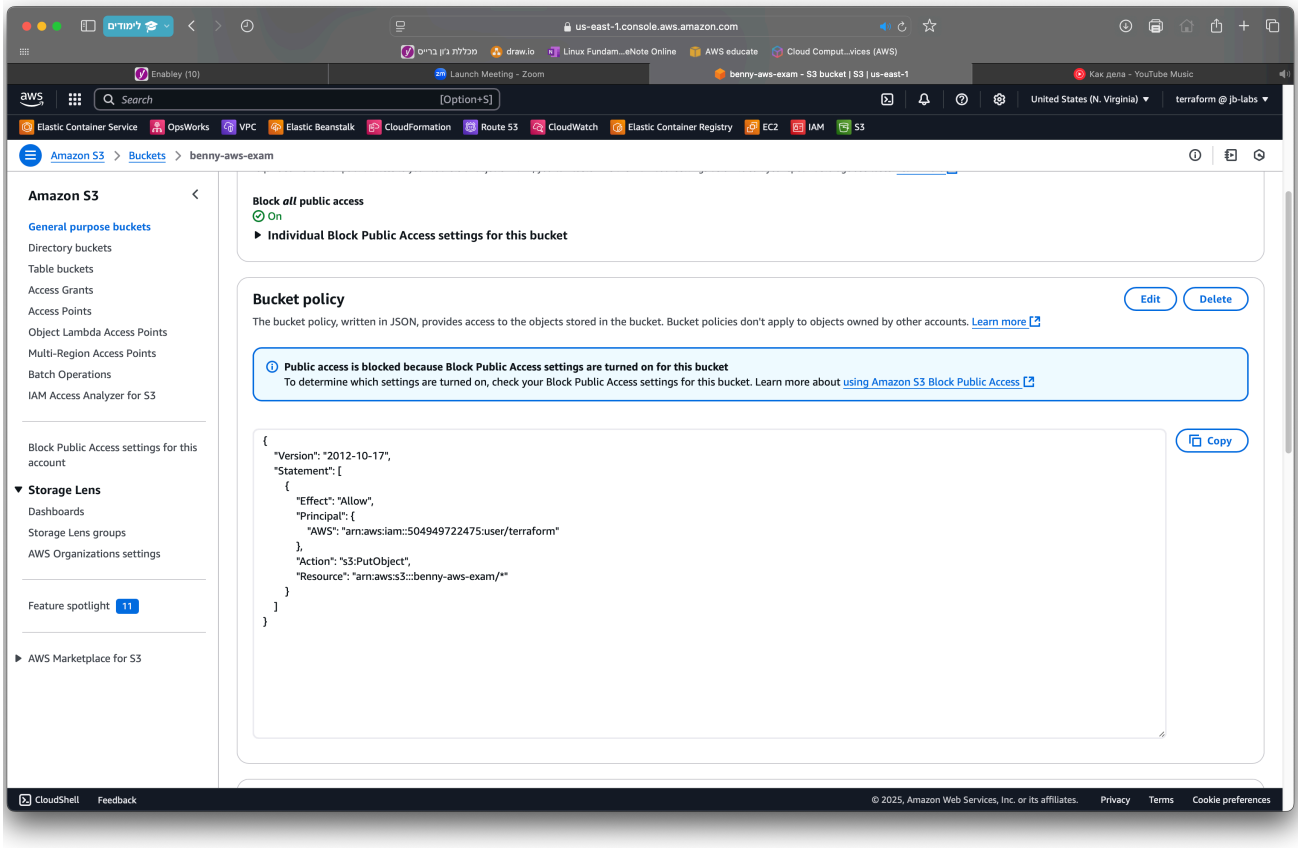
- **EFS is best when you need a scalable, shared file system with standard file system semantics accessible by multiple instances concurrently.**
- **S3 is ideal for storing and retrieving massive amounts of unstructured data, serving as a data lake, backup solution, or content repository.**
- **EBS is tailored for high-performance, single-instance block storage, suitable for databases, boot volumes, and applications requiring low-latency access.**

By understanding these differences, you can choose the right storage solution based on your application's access patterns, performance needs, and scalability requirements.

Section 2: Hands-on UI-Based Questions

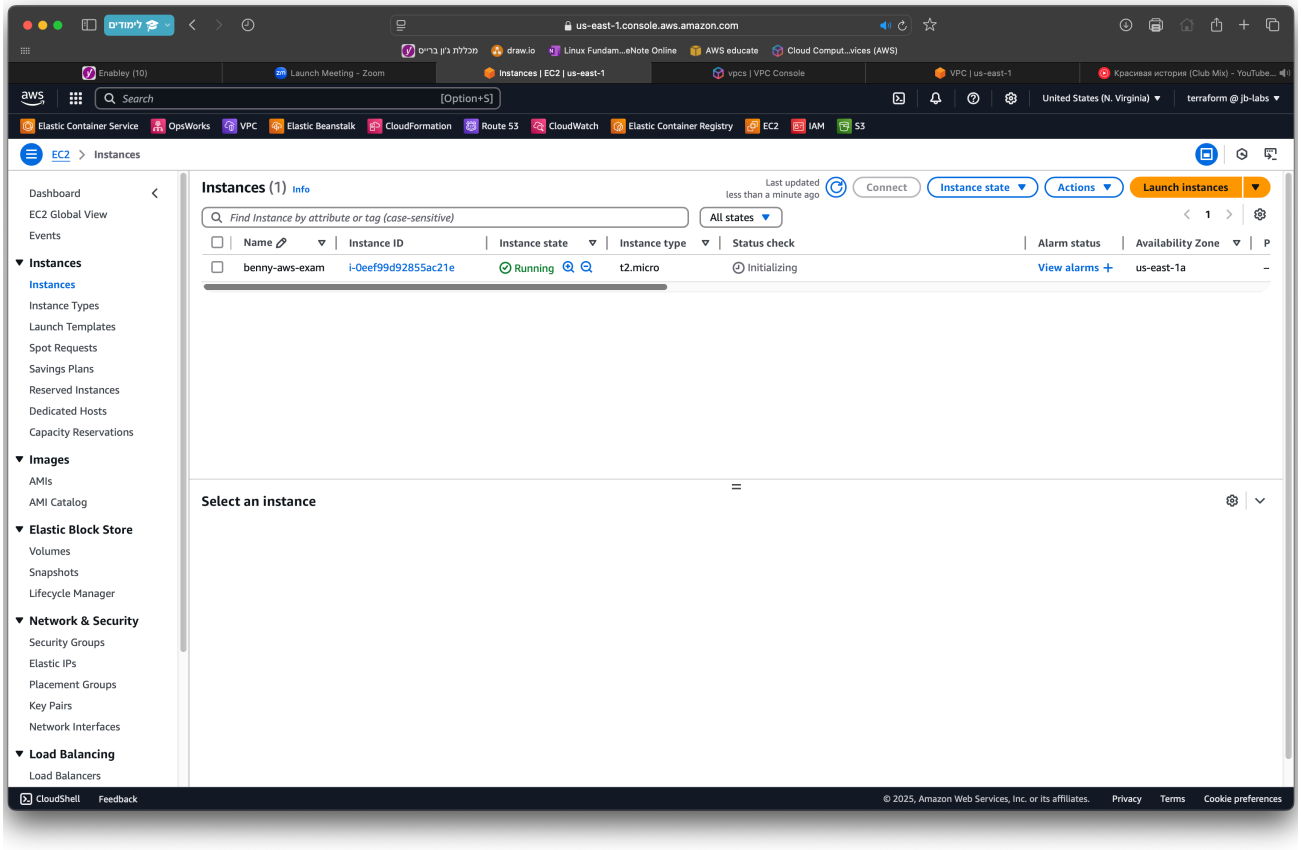
1. S3 Bucket Configuration



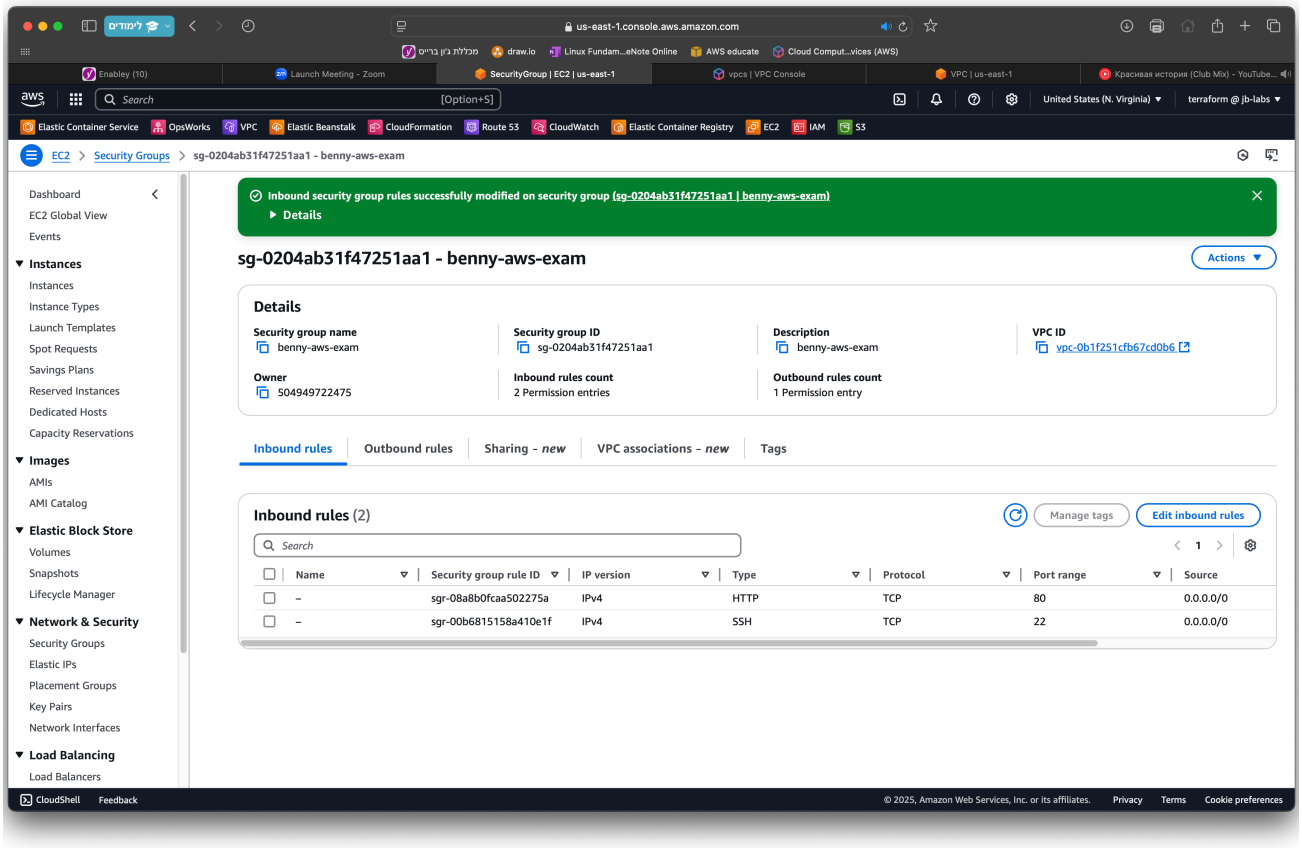


IAM Policy to prevent other users to upload

2. Launch an EC2 Instance



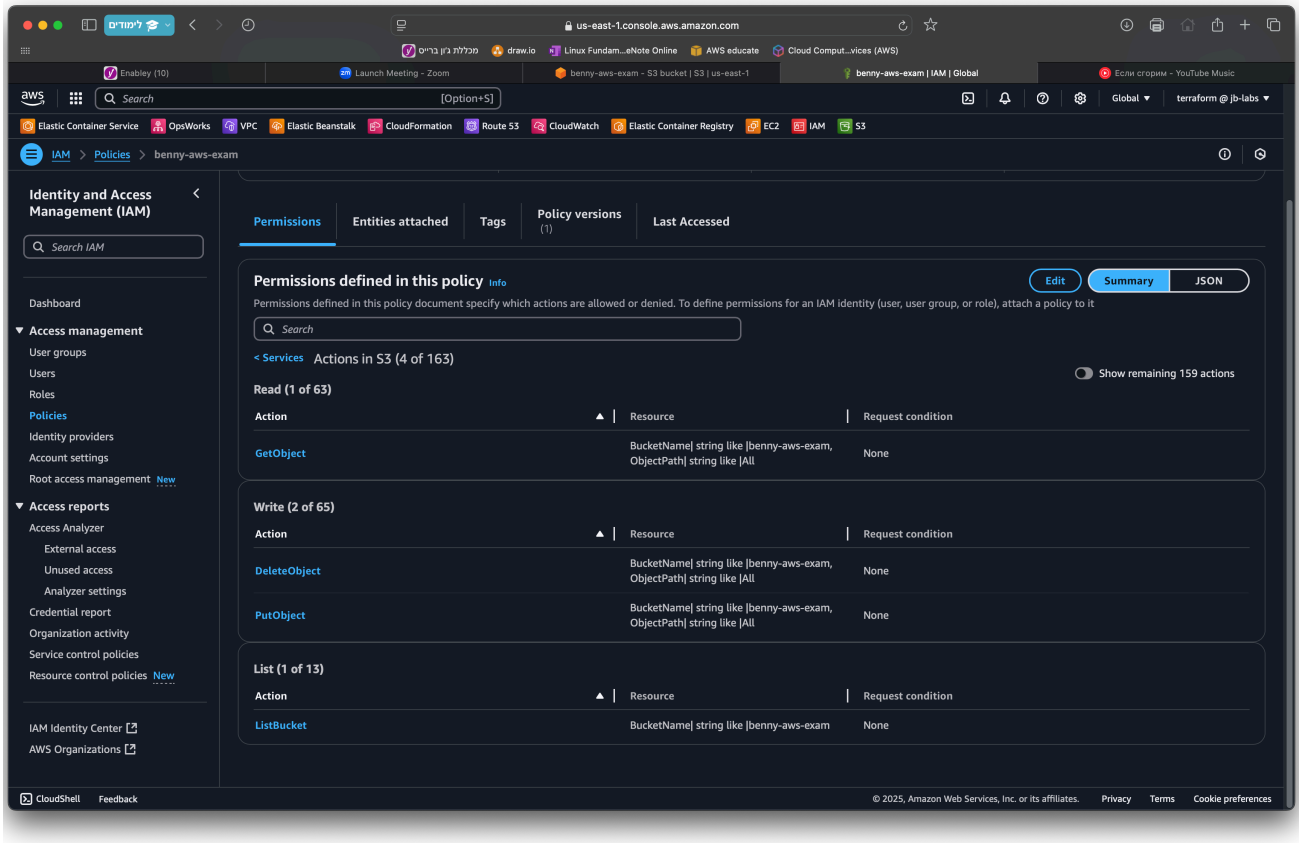
EC2 t2.micro



SSH and HTTP port

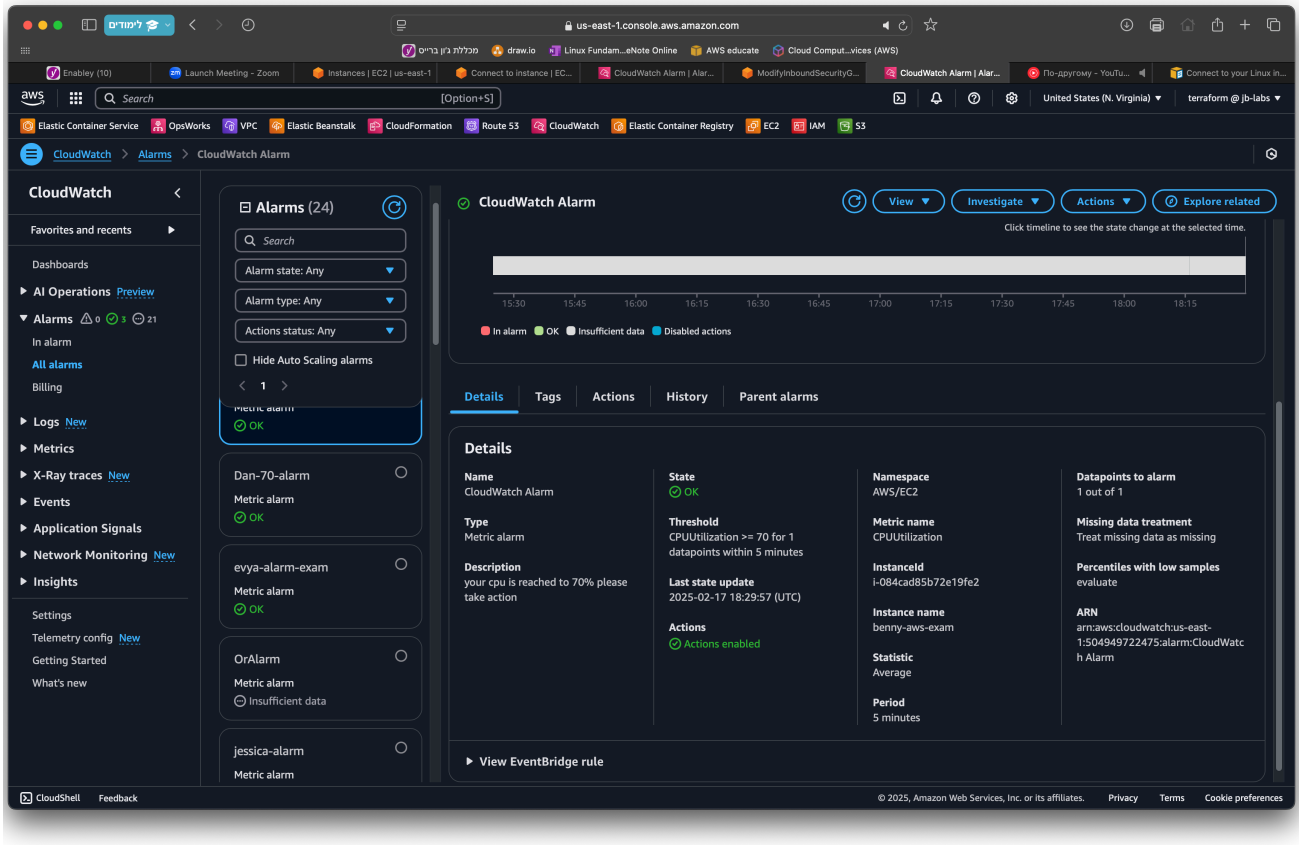
3. Configure an IAM User with S3 Access

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "s3:ListBucket"
         ],
         "Resource": "arn:aws:s3:::benny-aws-exam"
      },
      {
         "Effect": "Allow",
         "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
         ],
         "Resource": "arn:aws:s3:::benny-aws-exam/*"
      }
   ]
}
```



Policy that give access to specific s3 bucket access

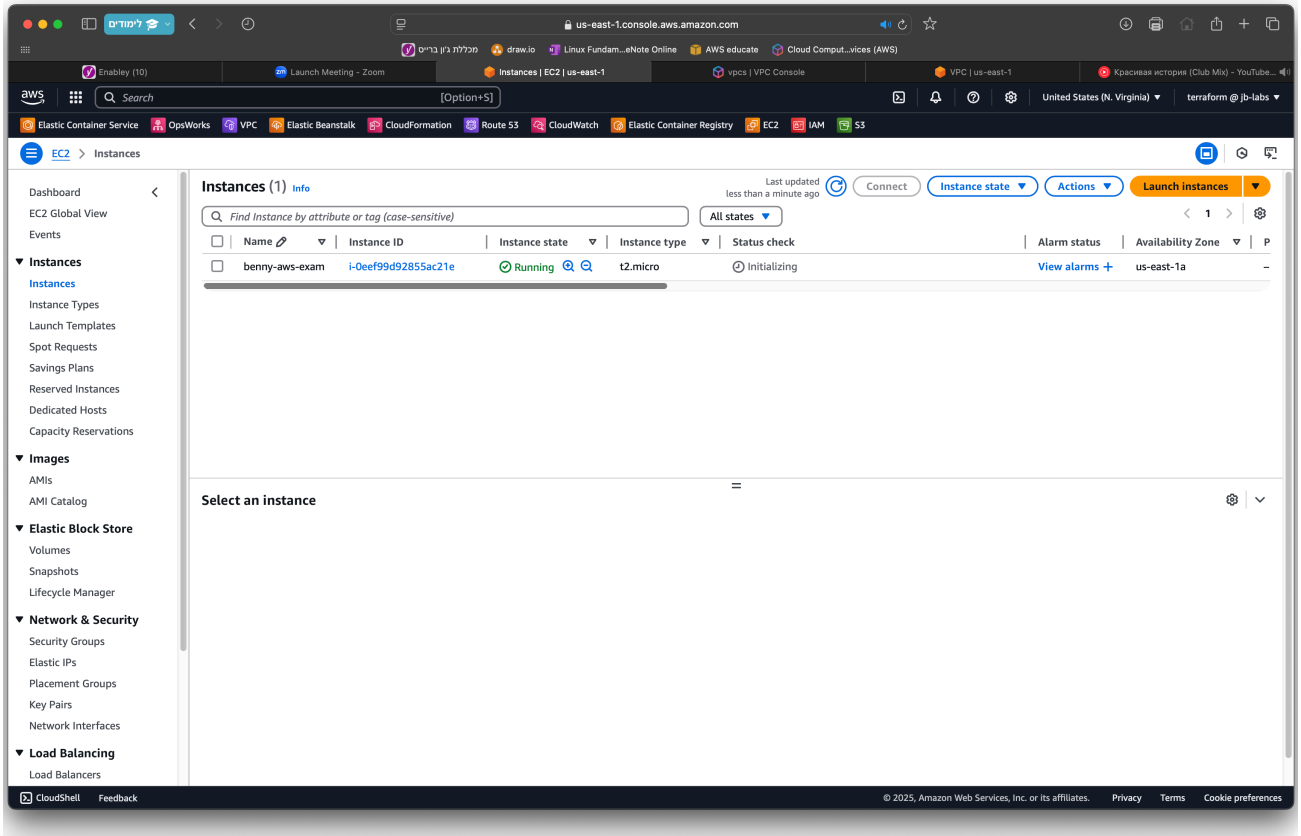
Set Up a CloudWatch Alarm

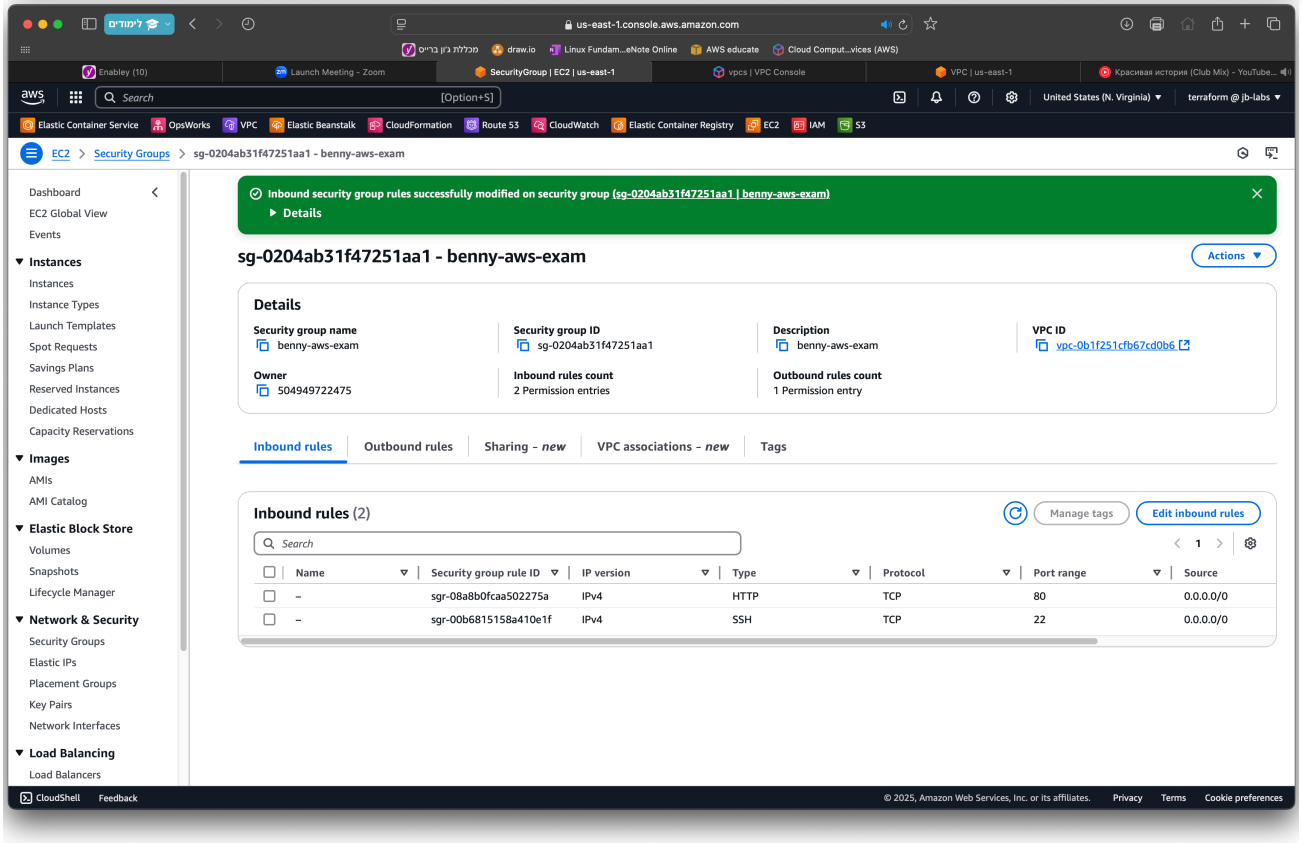


Alarm on EC2 that trigger wen cpu is loaded over 70%

Section 3: Hands-on advanced

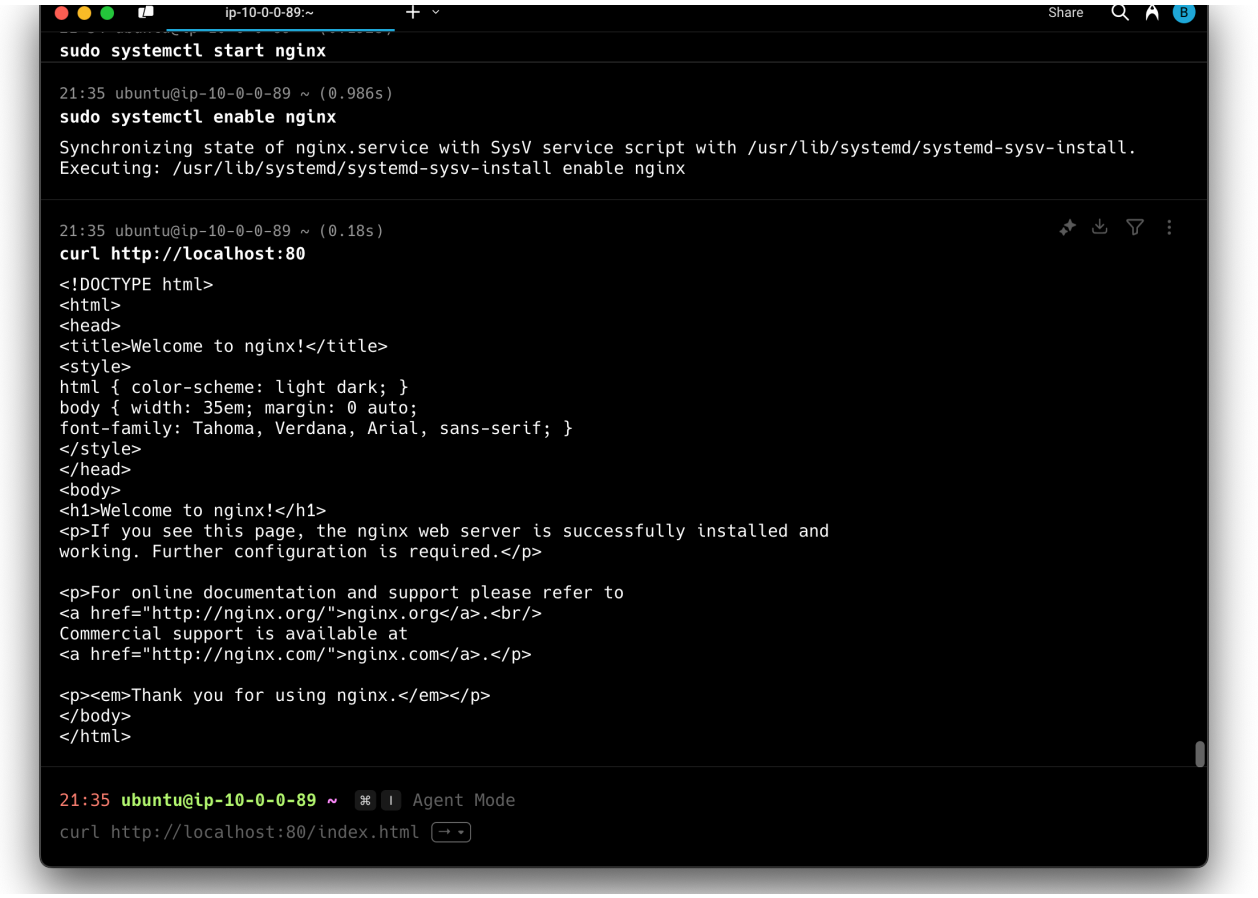
1. Deploy an Auto Scaling Group with a Single EC2 Instance



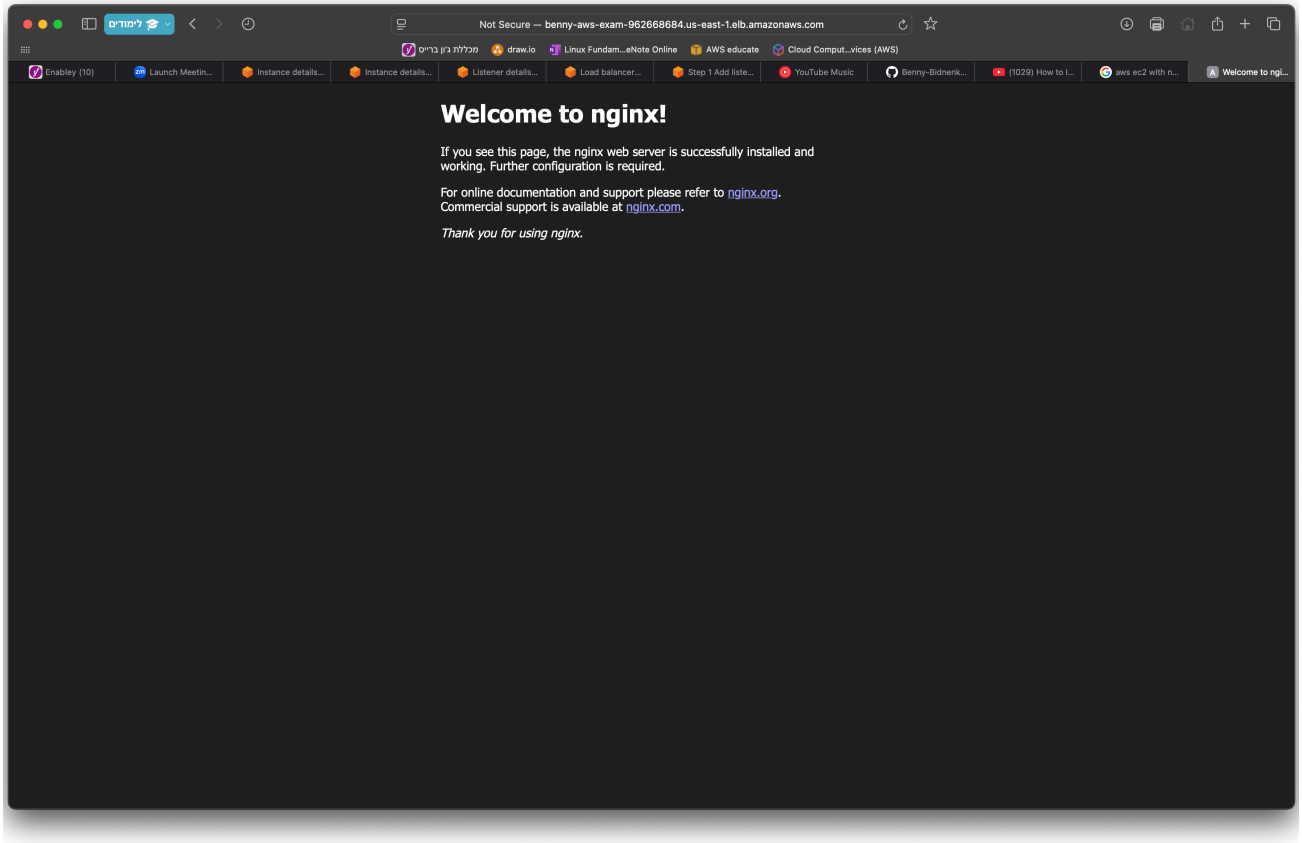


Type of ec2 and open ports

2. Connect to the EC2 Instance and Install Nginx

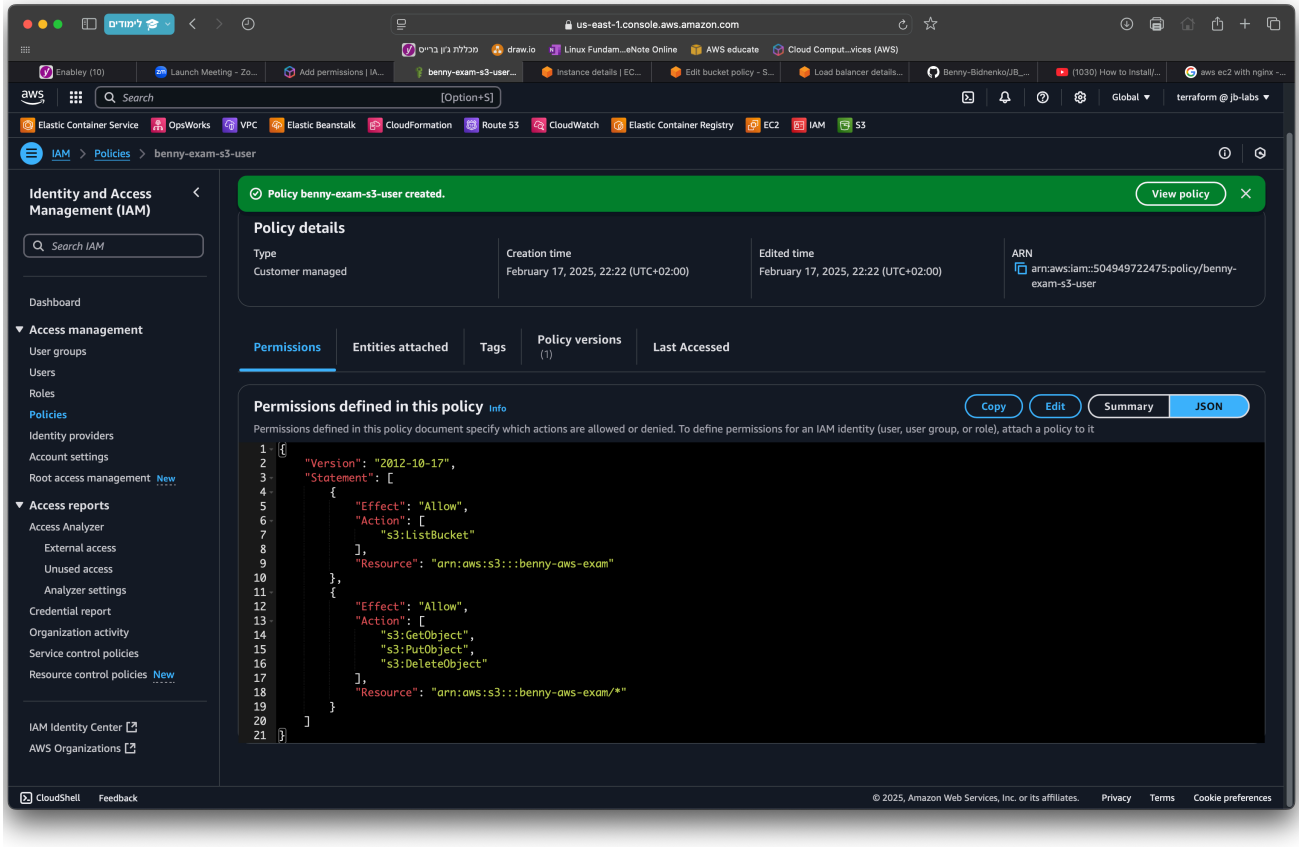


Connected to ec2 and nginx installed



Access the Web Page via the Load Balancer

4. IAM User Setup for S3 Access



User S3 can Access to S3 bucket only