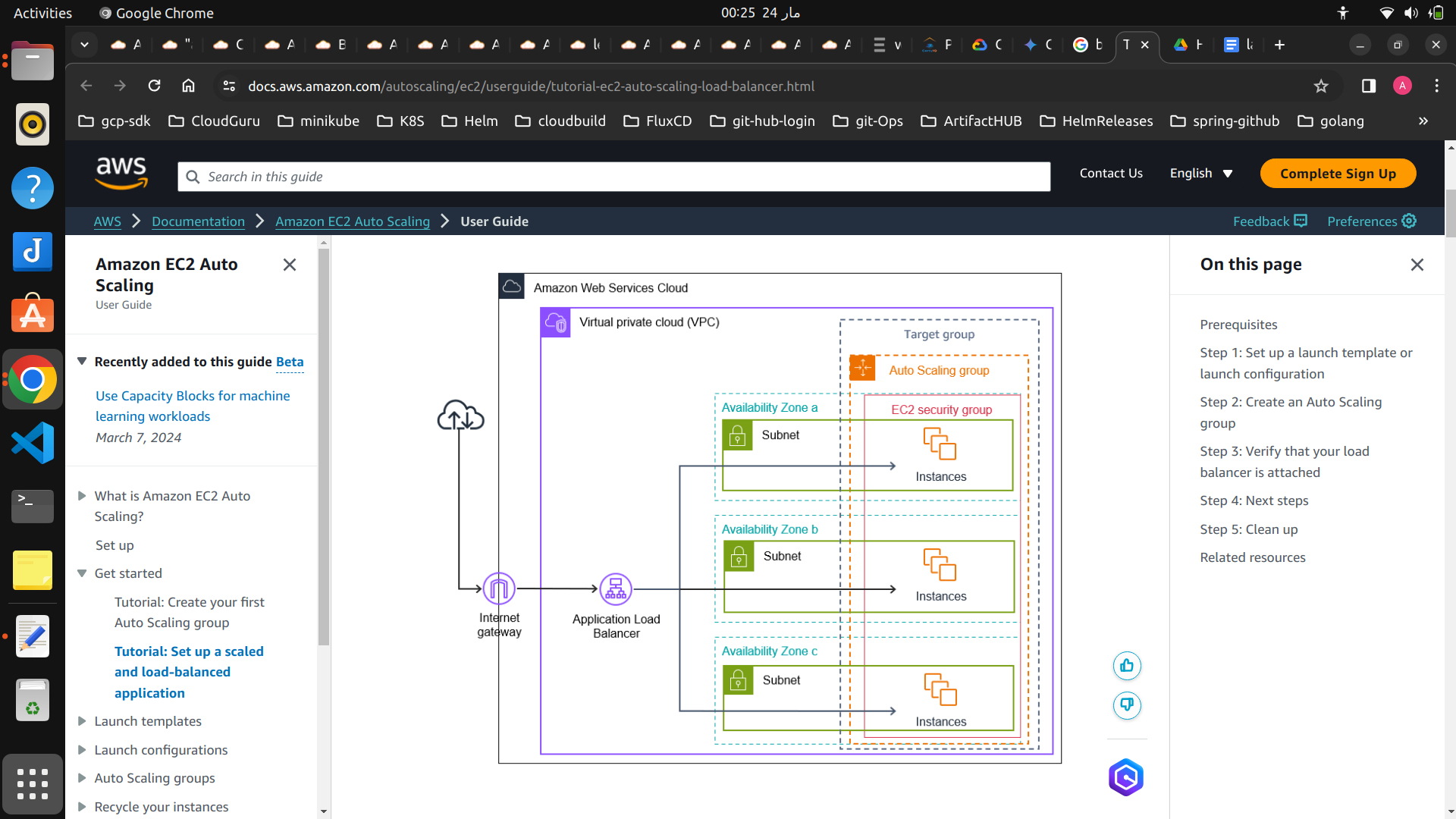
**The Situation:**

**A data analyst on your team needs to collaborate with an external consultant on a specific dataset. However, due to data privacy regulations, you cannot grant the consultant direct access to the entire dataset in the S3 bucket.**

**Challenge: "One of our data analysts needs to share a specific portion of a large dataset stored in S3 with an external consultant. However, due to data privacy regulations, we cannot provide the consultant with access to the entire dataset." "How would you approach this situation securely using S3 functionalities? What specific features would you leverage?"**

**Scenario: you're a Cloud Infrastructure Engineer working for a popular e-commerce platform. Your platform experiences unpredictable traffic surges during peak sales periods and trending product launches. These spikes cause website slowdowns and occasional outages, leading to lost sales and frustrated customers.\*\***

****

**\*\*Your Challenge:\*\***

**Implement a highly available and scalable architecture for the e-commerce platform's website using AWS services. Ensure the website can handle unpredictable traffic spikes while maintaining optimal performance and a seamless user experience. Here's what you, as the Cloud Infrastructure Engineer, would be responsible for:**

**1. Infrastructure Provisioning:**

**- VPC and Subnets: Set up a Virtual Private Cloud (VPC) with multiple public subnets across different Availability Zones for reliability.**

**- Security Groups: Establish security groups to control access to various components like EC2 instances, ALB, and other resources, enhancing VPC security.**

**- IAM Roles: Create IAM roles for EC2 instances to grant specific access permissions to necessary AWS resources, following the principle of least privilege.**

**2. Backend Scalability with Auto Scaling:**

**- Launch EC2 Instances: Deploy EC2 instances in a private subnet to host backend application servers.**

**- Auto Scaling Group Configuration: Configure Auto Scaling Group with EC2 instances to automatically adjust instance numbers based on predefined metrics such as CPU usage or incoming traffic.**

**- Target Group Configuration:\*\* Set up a target group within the ALB to include EC2 instances from the Auto Scaling Group, allowing the ALB to direct traffic to healthy instances.**

**3. Application Load Balancer Integration:\*\***

**- ALB Creation and Configuration: Create an Application Load Balancer (ALB) in a public subnet, configuring health checks to ensure traffic is routed only to healthy backend instances.**

**- Route Table Configuration: Update route tables associated with public subnets to direct website traffic to the ALB's DNS name.**

**4. Additional Considerations:**

**- Database Integration: If a separate database is used, configure security groups and IAM roles for secure communication between application servers and the database.**

**- Content Delivery Network (CDN): Consider implementing a CDN to cache static content and enhance website loading times for users across different locations.**

**- CloudWatch Integration: Set up CloudWatch for monitoring and logging to gain insights into system performance, resource utilization, and application behavior. Configure alarms to notify of any unusual activity or performance issues.**