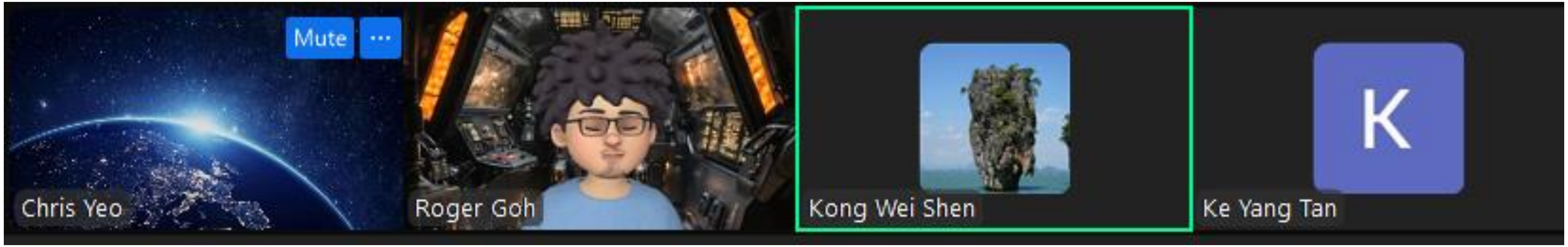
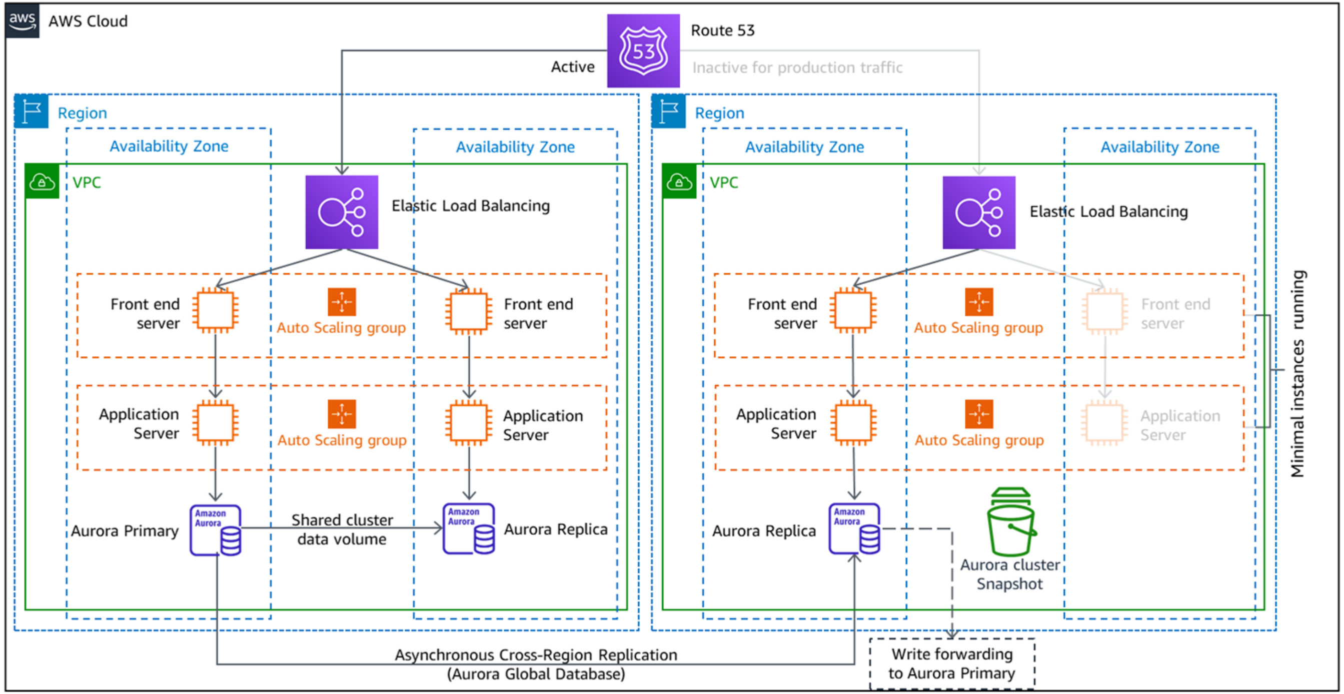
Assignment 2.1

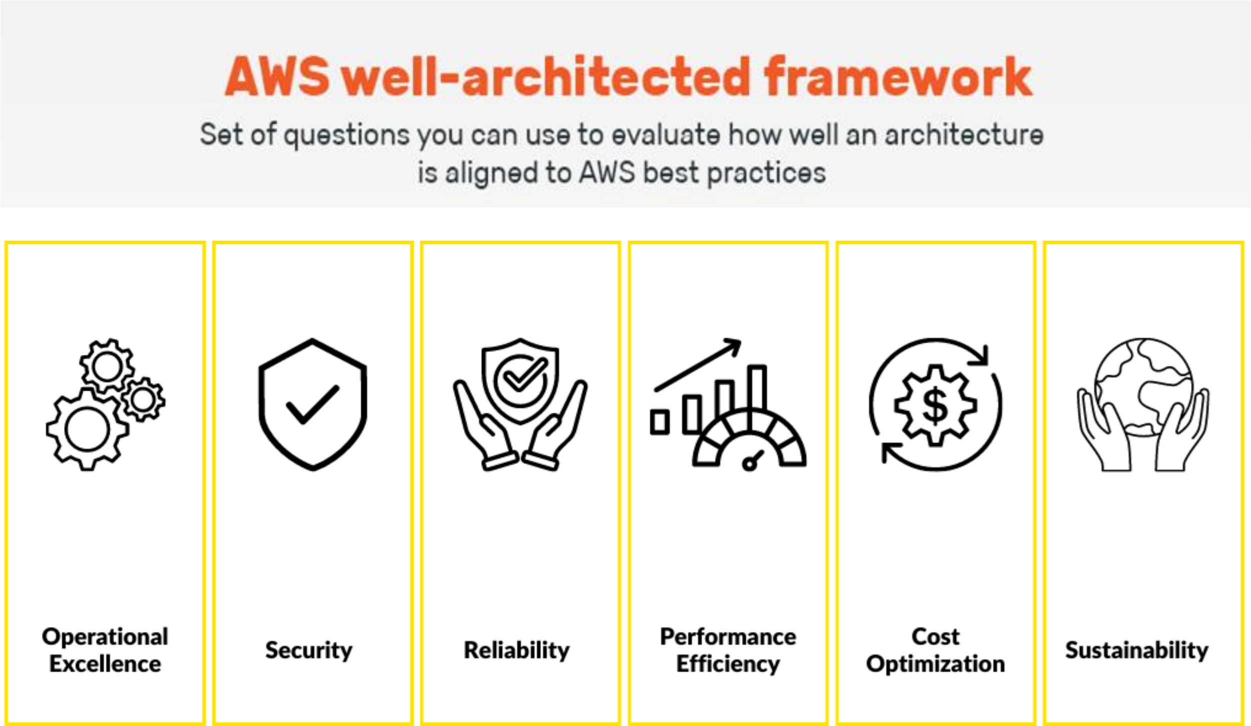
Group 3



Discuss how the principles apply



Overview



AWS well-architected framework

Set of questions you can use to evaluate how well an architecture is aligned to AWS best practices

- Operational Excellence
- Security
- Reliability
- Performance Efficiency
- Cost Optimization
- Sustainability

Security:

- Not Implement a strong identity foundation:
    a. No private and public subnet segregation
    b. No security group
    c. Database server not in private subnet.
- Enable traceability
    a. Missing traceability tools
- Apply security at all layers
    a. Missing IAM
    b. Missing firewall
    c. No security group
- Protect data in transit and at rest
    a. Aurora-encrypted database clusters use the AES-256 encryption algorithm
- Automate security best practices
    a. implement AWS CloudTrail
    b. Deploy AWS shield
- Keep people away from data
    a. Private-public segregation; DB should be in private subnet
    b. Data segregate from application server by using Aurora Database server.
- Prepare for security events
    a. Have multiple AZ, RZ | Somewhat ready

Some additional security considerations for each component:

Front-End Server

- **Web Application Firewall (WAF)**: Deploy a WAF to protect against common web exploits and vulnerabilities.
- **SSL/TLS Encryption**: Ensure that all web traffic is encrypted with SSL/TLS certificates.
- **DDoS Protection**: Utilize AWS Shield for protection against Distributed Denial of Service (DDoS) attacks.

Application Server

- **IAM Roles**: Ensure that application servers use IAM roles with the minimum necessary permissions.
- **Patch Management**: Regularly update and patch your application servers to protect against vulnerabilities.
- **Network Security**: Implement security groups to restrict access to the application servers only from trusted sources.

Aurora DB

- **Encryption**: Ensure that your Aurora DB instances and snapshots are encrypted.
- **Database Auditing**: Enable database auditing to monitor and log database activities.
- **Backup and Recovery**: Regularly back up your database and test your recovery process.

General Recommendations

- **Security Monitoring**: Use AWS CloudWatch and CloudTrail to monitor for suspicious activities.
- **Incident Response Plan**: Develop and regularly update an incident response plan.
- **Compliance Checks**: Use AWS Config to continuously assess, audit, and evaluate the configurations of your AWS resources.

Reliability

- Automatically recover from failure
  a. Multiple AZ, multiple region AZ implemented - enabled HA
- Test recovery procedures
  a. Failover mechanism like Route 53 that failover routing to different region.
  b. Test Application Failover
  c. For RDS, ensure automatic failover between availability zones works by forcing a failover using the AWS Management Console or CLI.
  d. Implement Elastic Load Balancer (ELB) Health Checks to confirm unhealthy instances are removed and traffic is redirected to healthy ones.
- Scale horizontally to increase aggregate workload availability
  a. Auto-scaling groups implemented
- Stop guessing capacity
  a. ASG implemented | Does not need to manually provision resources
  b. Implement CloudWatch to monitor change in demand
- Manage change in automation
  a. Implement AWS CloudTrail
  b. Implement AWS Change Manager