Cloud Migration for a Retail E-commerce Company

Xuanyu Zhu

CSCL 1000

2025.Feb.28

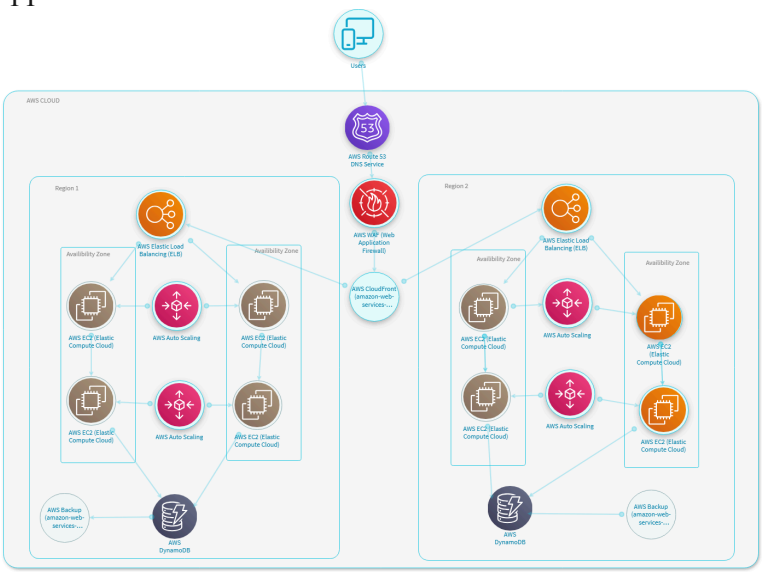
Current infrastructure
L-Mate's on-premises setup is prone to significant scalability, performance, maintenance, cost-effectiveness, and disaster recovery issues. The absence of quick scaling of computing capabilities leads to website slowness, downtime, and missed sales, especially during traffic surges. Performance bottlenecks mean poor user experience, lower conversions, and loss of brand reputation.

Ongoing hardware maintenance and software updates consume IT resources, reducing productivity and taking attention away from innovation. High capital and operating costs strain the budget, further limiting expenditure on business growth. Inadequate disaster recovery processes increase the risk of data loss and extended downtime and threaten business survival.

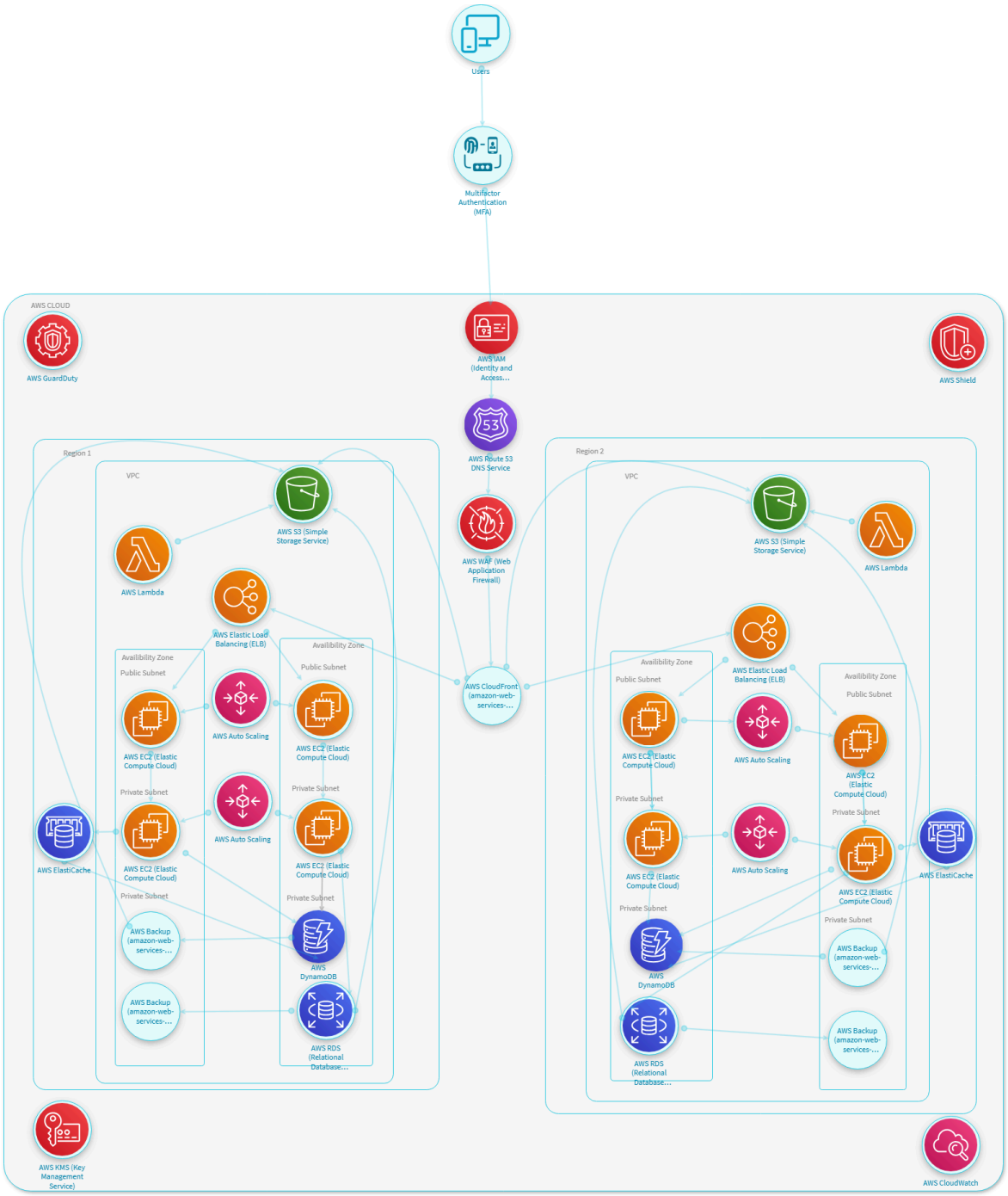
A cost-effective, yet scalable and dependable solution is required to ensure long-term sustainability and competitiveness.

AWS Cloud Diagram:
Accordingly, we improved its infrastructure and integrated cloud computing, making the entire system keep its original function but enjoy faster, more secure, and more cost-saving development, deployment, and maintenance.

This is an architecture diagram of a multi-region AWS design constructed for high availability, scalability, and resiliency. At the top, Amazon Route 53 supplies DNS routing, directing traffic to each region. Within each region, traffic is directed initially through a front-end Elastic Load Balancer (ELB), which load-balances requests across several Availability Zones of Amazon EC2 instances managed by AWS Auto Scaling groups. These Auto Scaling groups automatically add or remove EC2 instances in response to demand, sustaining consistent performance. Amazon DynamoDB offers fast, scalable storage for data in both regions, and Amazon S3 (Static Site Hosting) is also available to host static content. AWS Backup services are also present to provide reliable backup and restore capability. By placing resources across multiple regions and Availability Zones, this pattern reduces the likelihood of downtime and creates a strong foundation for hosting highly available applications.



However, we realized that there are many recommendations worth implementing, such as AWS IAM (Identity and Access Management) and AWS GuardDuty. We recalled what we learned in class about MFA, so we added some components to make a more complete architecture diagram.



So our newest AWS architecture for scalability and high availability. At the top, Users access through AWS Route 53 (DNS Service) for domain resolution, then AWS WAF (Web Application Firewall) to filter out malicious traffic. Traffic then passes through Region 1 and Region 2, each with Basic Elastic Load Balancing (ELB) to spread incoming requests across

multiple Availability Zones with Amazon EC2 instances. These use examples leverage AWS Auto Scaling to automatically adjust capacity in real time as required for optimum performance and cost savings. ElastiCache further provides in-memory storage and forward for enhanced data access acceleration, and Amazon DynamoDB is a NoSQL database for high-throughput, low-latency storage. Both regions feature AWS Backup for automating protection and recovery of data. With the inclusion of multi-region deployment, load balancer, and auto scaling, this architecture allows for consistent performance as well as against traffic spikes or regional crashes.

Based on the threat report and risk summary, we can still see some mainly recommendations that can be improved. The following paragraph will introduce all of them.

First of all, users are open to a wide range of vulnerabilities including exploiting weak authentication and authorization controls, clickjacking to get them click on hidden elements, third-party dependency vulnerabilities which can be used for tampering, and cross-site scripting (XSS) attacks that could result in stealing information or session hijacking. To address these threats, one should employ effective authentication mechanisms like turning on MFA and implementing the least privilege principle for role and user permissions, utilize frame-busting scripts in conjunction with X-Frame-Options and a good Content Security Policy (CSP) to defend against spoofing, update third-party components automatically through automated dependency scanning tools on a regular basis, and use strict input validation and output encoding to thwart XSS attacks.

Secondly, AWS Backup is also exposed to several threats: misconfigured backup plans can cause denial-of-service situations, inconsistent data tagging of backup resources increases the risk of data exposure, unencrypted cross-region backup copies risk data interception, backup operations are vulnerable to data corruption, and unauthorized deletion of backup vault is vulnerable. To prevent these risks, organizations must audit and test backup configurations regularly, employ standardized tagging across all resources, encrypt all cross-region backups with KMS keys, employ continuous integrity checks during the backup, and enable AWS Backup Vault Lock to prevent accidental deletion.

Thirdly, EC2 instances have risks like data loss or exposure via unencrypted EBS volumes or poor isolation of operating system and data storage, network misconfigurations exposing instances to external attacks, resource mismanagement leading to service disruption, poor failover and recovery mechanisms leading to prolonged downtime, and poor access controls leading to unauthorized modifications. To avoid such risks, encrypting EBS volumes and isolating OS and data storage, network setting configuration in a proper manner with secure security groups and ACLs and maintaining systems up to date, optimal use of resources using metadata, tagging, and Trusted Advisor, and hosting instances on more than one Availability Zones using Auto Scaling, proper failover designs and periodic recovery process testing, and enforcing strong access controls using identity federation and least privilege security group rules should be followed.

Finally, MFA products are vulnerable to risks such as potential denial-of-service attacks that crash authentication, session hijacking even when MFA is enabled, social engineering attacks that trick users into divulging MFA credentials, and weak fallback mechanisms that can allow MFA bypass. To mitigate these threats, design MFA systems for high availability and redundancy, secure sessions with aggressive timeouts and real-time session monitoring, enhance user training to make users more aware of social engineering attacks, and

supplement MFA fallback processes with additional verification steps and robust anomaly detection.

Finally, we will make some other threats like AWS CloudWatch resilient through higher high availability, robust encryption, strict access controls, and regular auditing so that timely anomaly detection is possible and sensitive monitoring information is safe. Lambda functions should be tested and audited from time to time so that misconfigurations leading to data exposure or unauthorized access are prevented. GuardDuty should never be disabled and correctly configured at all times to ingest complete log data, with security findings verified in a timely fashion to avoid lateral attacks. For AWS KMS, key deletion protection must be enabled, strict access controls implemented, key operations secured with encryption, and regular audits conducted to avoid permanent data loss and key compromise. CloudFront distributions need to enforce origin access controls, demand HTTPS (auto-redirecting from HTTP to HTTPS), and use versioning with signed cookies and URLs to guarantee that unauthorized content manipulation or data mining is averted. Lastly, ELB must be secured by establishing AWS WAF and network ACLs to limit incoming requests, having tight security group rules, using interface endpoints for secure access to VPC, and encrypting all the communications with Perfect Forward Secrecy enabled and applying authentication schemes on ALB listeners where they are needed.