How CTX used AWS Well-Architected to save infrastructure cost by 70%

Customer: One of the largest digital asset trading companies

Summary

Cyberdyne Tech Exchange (CTX) is one of the largest digital asset exchange companies who publish and trade-in asset-backed security tokens like artwork, real estate, diamonds, etc. This trading is carried out by qualified issuers and investors through their newly developed applications which they plan to migrate to AWS cloud. The deployed applications must provision for high availability and scalability, automation and security along with a well-architected framework.

About the customer

CTX is one of the largest digital asset exchange companies where qualified issuers and investors publish and trade asset-backed security tokens. These security tokens are backed by curated investment-grade assets such as artwork, diamonds, real estate and equity securities.

Their platform offers a complete suite of services that include primary issuance, trading and settlement as well as custody services.

Global institutional investors trade 24/7 on their trading architecture that is powered by Nasdaq's matching and market surveillance (SMARTS) engines. Clients have the assurance that they are trading on an institutional-grade platform with fair and transparent price discovery.

Problem Statement

CTX intends to deploy their newly developed application to AWS. The deployed application should adhere to the following:

- Highly Available & Scalable environment
- AWS Well-Architected Framework
- MAS & PDPA compliance
- Automated Infrastructure Provisioning
- Automated Application deployment

Proposed Solution

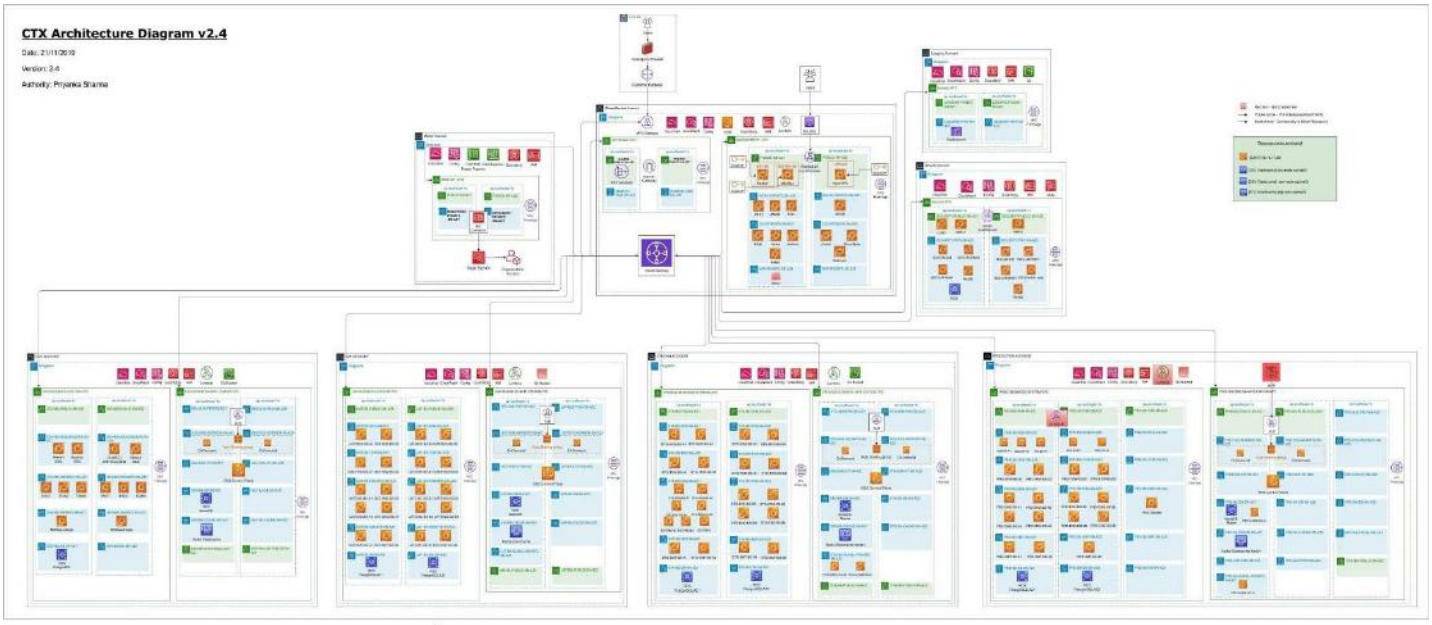
Architecture Description

- The AWS accounts are provisioned based on the landing zone concept, with a centralized logging account, security account, shared service account and separate accounts for different applications.
- Master Account hosts AWS organization Cost, SCP for member accounts and consolidated billing.
- Shared service account hosts all common services like Transit Gateway, ECR, Jenkins, Bastion Route 53 etc.
- Security Account hosts GuardDuty master and all other accounts will be added as members.
- All security services like IPS & IDS, Cyberark and other future security-related services will be deployed in Security accounts.
- Centralized Logging Account host all logs like VPC flow logs, ELB logs, CloudTrail, Cloudwatch and Elasticsearch streaming live application logs from all member accounts.
- DEV Account / UAT Account / Staging Account / Production Account is provisioned to host the application.
- All the infrastructure provisioning happens through CloudFormation Template. [VPC, EC2, EKS, S3, RDS, TGW, TGW connections]
- CTX has two major applications - Business System[BS] and Business Application[BA].
- BS & BA are provisioned in separate VPCs for all the environments.
- BS is a monolithic application and the applications are deployed on EC2 instances.
- BA is a service layer and talks to BS systems through API. BA deployed in the EKS cluster.
- Around 20 microservices are deployed in the EKS cluster.
- ALB ingress controller has been deployed along with AWS WAF for the application communication from External users to microservices.
- The application deployment lifecycle is completely automated using JenkinsFile.
- PostgreSQL RDS is used as a Database.
- CloudWatch service will be used for monitoring and SNS will be used to notify the users in case of alarms, metrics crossing thresholds etc.
- All snapshot backups will be regularly taken and automated based on best practices.

Security & Logging

- AWS SSO is created and appropriate IAM accounts have been formed with least permissible access provided to the accounts.
- MFA has been enabled on both root and IAM accounts.
- Except for bastion, all servers will be placed in private subnets.
- Security groups are used to control traffic at the VM level. Only the required ports will be opened, and access allowed from required IP addresses.
- Network Access Control Lists (NACLs) are used to control traffic at the subnet level.
- CloudTrail has been enabled to capture all the API activities occurring in the account.
- VPC flow logs enabled to capture all network traffic.

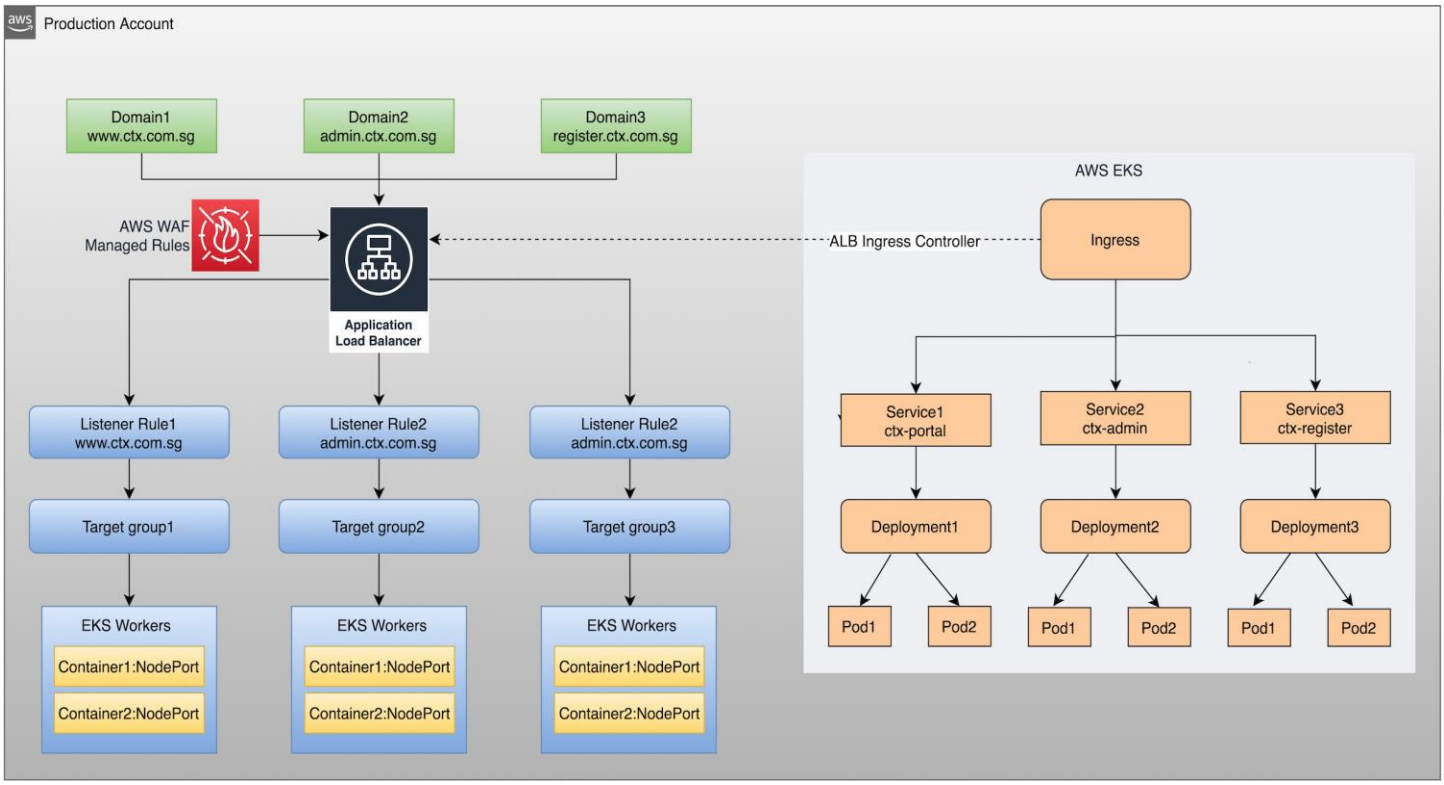
- AWS Guard Duty enabled for threat detection and identifying malicious activities in the account like account compromise.
- AWS Config enabled, and all the AWS recommended config rules are created.
- All servers will be encrypted using KMS. KMS keys are stored in Security accounts and admin access to keys are restricted only to Security Admins.



AWS WAF

- WAF is mandatory for Compliance requirements[MAS].
- AWS WAF has been used as a Web Application Firewall for the external-facing applications.
- WAF Managed rules are created to mitigate top 10 OWASP's web application vulnerabilities.
- AWS CloudFormation has been created to deploy the WAF rules in all the required environments.
- The following rules are created using the CloudFormation template.
    - Generic-detect-admin-access
    - Generic-detect-bad-auth-tokens
    - Generic-detect-blacklisted-ips
    - Generic-detect-php-insecure
    - Generic-detect-rfi-lfi-traversal
    - Generic-detect-ssi
    - Generic-enforce-csrf
    - Generic-mitigate-sqli
    - Generic-mitigate-xss
    - Generic-restrict-sizes
- Web ACL logging has been enabled to capture information about all incoming requests.

- AWS Cloudwatch has been used to monitor and alert based on WAF rules.
- AWS WAF has been integrated with ALB. ALB has been provisioned by ALB ingress controller which is deployed in EKS cluster.



Benefits

- Successfully provisioned the entire application in AWS using CloudFormation with all the necessary security measures as per MAS compliance specifications.
- Spot instances are used for scalable instances. This saves AWS infrastructure cost by 60% to 70%.
- Application deployment is completely automated using Jenkins.
- The highly secured environment has been provisioned with the help of AWS services like AWS WAF, Guard Duty and other third-party solutions like Trend Micro Deep Security Manager.

Cloud platform

AWS.

Technologies/Services used

EC2, RDS, S3, EKS, ECR, TGW, Guard Duty, Route53, ALB, AWS WAF, IAM, KMS.