CASE STUDY

AWS-based Implementation and Support of Native Microservices and Data Warehouse Platform

Overview

The customer wanted to rearchitect a monolithic customer information management (CIM) platform into an microservices architecture solution using AWS native services and host a non-native data warehouse solution on AWS. Some of the key business requirements were:

- Isolated environment for microservices and data warehouse solution
- Connect multiple locations - on-prem, Snowflake over HTTPS with ease using secure VPN, direct connect, and HTTPS over the internet
- To setup end to end (E2E) DevOps pipeline that is fast, reliable, and highly secure and achieve faster time to market for every new feature release / upgrades / bug fixes.
- Fully automated deployment process for development environment and follow an approval process for other environments.
- Cost optimization by optimally using AWS resources
- Simplify operations by utilizing with Jira service desk.

Client Background and Challenge

The customer is a new generation telco company with approximately 20k employees, serving millions of customers across the world empowering people, companies , and societies to stay in touch with everything that matters 24 hours in a day, 7 days in a week and 365 days in a year. The customer wanted an experienced partner who could foresee the problems and implement a solution that is scalable, reliable, and secure, keeping future expansion in mind.

Our Approach and Solution

- Defined loosely coupled architecture with microservices to reduce the blast radius and provided the ability to scale each component independently.
- Transit gateway being core of inter and intra network communication
- Amazon Elastic Container Service (ECS) Fargate solution for microservices
- Site to site VPN connection from on-prem to AWS for microservices
- Direct connect connection from on-prem to AWS for data warehouse
- Compliance and security are addressed at scale using the AWS best practices and recommendations incorporated with AWS identity and access management (IAM) and parameter store, a capability of AWS systems manager.

AWS Services Consumed

- AWS ECS
- AWS Fargate
- AWS Transit Gateway
- AWS WAF
- AWS IAM
- Amazon API Gateway
- AWS Aurora
- AWS Cloud Trail
- AWS Cloud Watch
- AWS Site to Site VPN
- AWS Direct Connect
- AWS S3
- AWS ECR
- AWS Load Balancer
- (ALB / NLB)
- Route 53
- AWS Certificate Manager
- AWS KMS
- AWS Code Build, Code Pipeline, Code Commit

Multi Account Structure

- Multi-account strategy based on workload type and environment type was implemented to isolate the environments and workloads
- Account details: 2 Prod, 2 Non-prod, 1 Sandbox

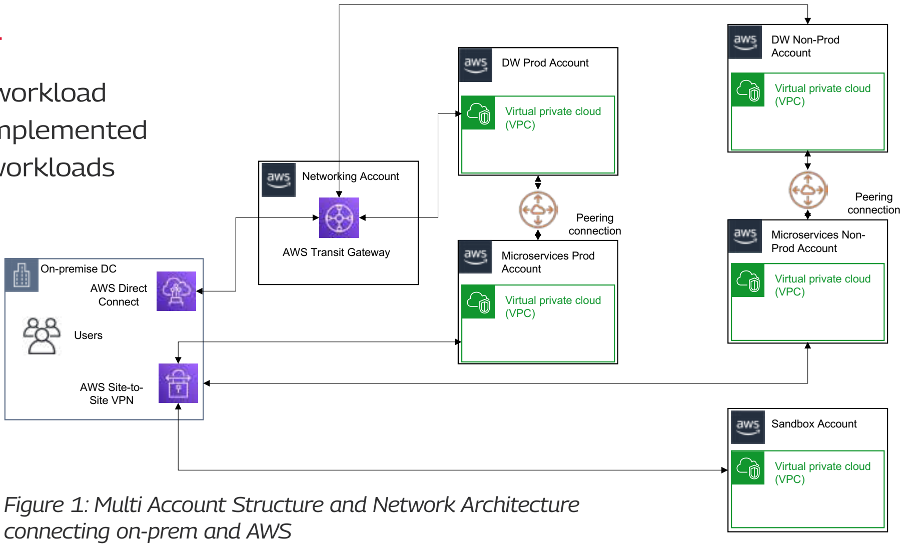
DW Non-Prod Account
Virtual private cloud (VPC)
DW Prod Account
Virtual private cloud (VPC)
Networking Account
AWS Transit Gateway
Peering connection
Peering connection
Microservices Prod Account
Virtual private cloud (VPC)
Microservices Non-Prod Account
Virtual private cloud (VPC)
On-premise DC
AWS Direct Connect
Users
AWS Site-to-Site VPN
Sandbox Account
Virtual private cloud (VPC)

Figure 1: Multi Account Structure and Network Architecture connecting on-prem and AWS

Below diagram shows the Application infrastructure of AWS ECS Fargate based microservices solution.

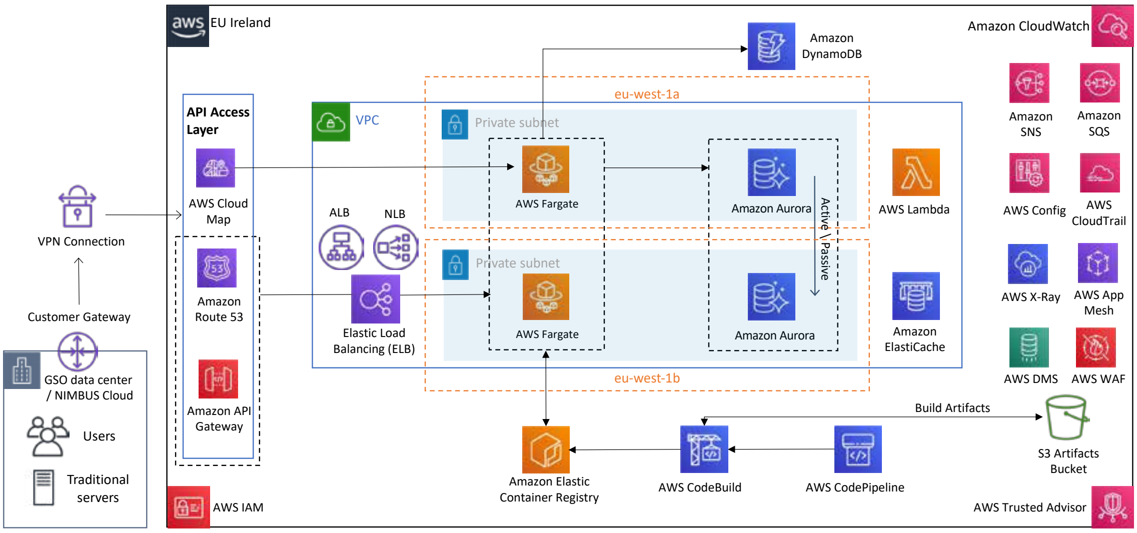

Figure 2: Microservices architecture for Fargate based ECS cluster

Below diagram shows the application infrastructure of datawarehouse solution.

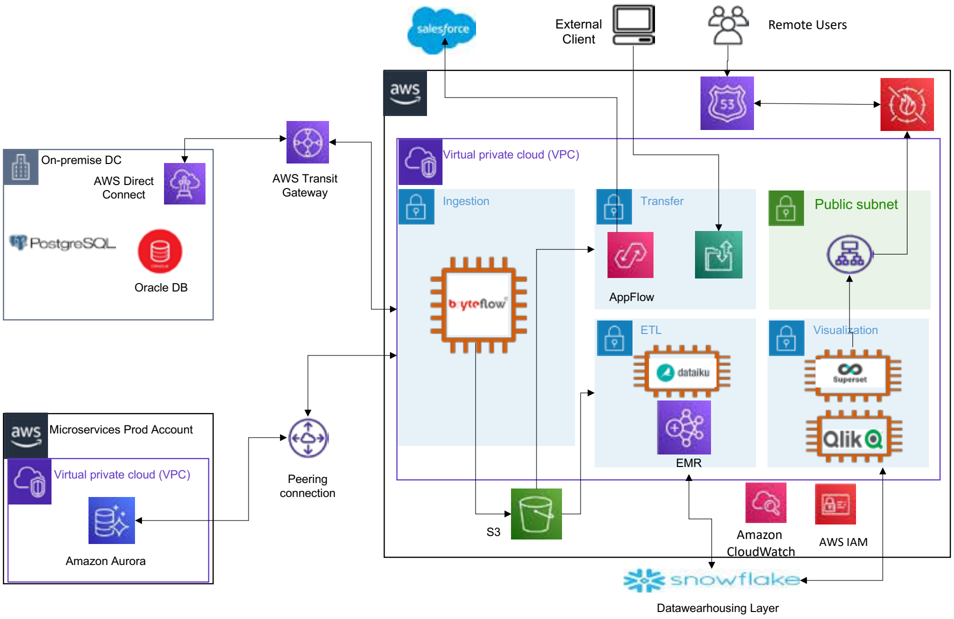

Figure 3: Architecture of Datawarehouse Solution

Cloud Ops Overview

Governance

- AWS CloudTrail is enabled to track the activities of the account users, logs are encrypted and stored to a separate AWS account in Amazon Simple Storage Service (S3) bucket. Any resource level changes are monitored based on AWS API activity and an alarm will be triggered that provides notification.
- Customer's AWS account has AWS configuration enabled and rules are configured with regular check against the desired state.

Security and Access Management

- Using AWS Key Management Service (KMS) services like Amazon Elastic Block Store (EBS), Amazon Relational Database Service (RDS) are encrypted. Amazon S3 buckets are encrypted using server-side encryption
- Transport layer security (TLS)/ secure socket layer (SSL) is used to encrypt data in transit

- In addition to security groups, public load balancer is protected using AWS Web Application Firewall (WAF)
- AWS Secrets Manager and Parameter Store are leveraged to store credentials and secrets like RDS credentials, API keys, etc.
- Amazon Inspector service to assesses for exposure, vulnerabilities, and deviations from best practices.
- AWS access is enabled through federation using customer's active directory (AD) via single sign-on process.
- IAM role is used to control access between AWS Fargate service to other services.

Operations Management

- AWS Systems manager is used to keep all the Amazon EC2 instances up to date and for patching process regularly.
- Leveraged Terraform for infra provisioning automation and AWS code pipeline to orchestrate release and deployment process in customer's organization.
- Jira is leveraged as a ticketing tool where all the tickets related to AWS issues are assigned and acted upon by the TechM AWS operations team based on the priority set.

Monitoring and Observability

- Amazon CloudWatch is used to collect and analyze outputs such as logs, metrics, and traces. This insight allows operations teams to quickly detect, investigate, and remediate problems.
- Sentry is used for application monitoring and error tracking; it provides real-time insight into production deployments with information to reproduce and fix crashes.
- AWS X-Ray is used for distributed tracing.
- VPC flow logs are enabled to monitor the traffic flow.

Business and Community Impact

- Better understanding of application health and network health due to regular monitoring
- Best possible experience for end users.
- Detect problems quickly, investigate efficiently, and remediate as soon as possible to minimize disruption for customers
- Automated mundane and repetitive tasks
- Fully automated release and deployment process
- Secure, scalable, and cost-efficient environment
- Improved performance
- Zero downtime, highly available (HA), and cost-effective solution

About Tech Mahindra

Tech Mahindra is an AWS Premier Consulting Partner and Managed Service Provider. We help customers to secure their digital transformation journey by, addressing all their cloud security needs by protecting their cloud environment, providing unified visibility, and ensuring compliance.

TECH
mahindra

Copyright © Tech Mahindra 2023. All Rights Reserved.

Disclaimer. Brand names, logos and trademarks used herein remain the property of their respective owners.