CASE STUDY

TECH mahindra

Build a Secure, Scalable, Multi-Customer Isolated Environment on AWS

Overview

Enterprises are driving the cloud transformation journey by deploying applications on the cloud and offering services to their customers. Healthcare enterprises have strict compliance requirements to be adhered to requiring isolated hosting environments and other compliance requirements to be complied to. TechM enabled one of the healthcare enterprises to successfully host the application environment on AWS cloud achieving automation, simplicity, isolation, self-management, modern zero-downtime deployment system.

Client Background and Challenges

The client is one of the innovative healthcare technology companies that enables clinicians to make right decisions for the patients through their platform. The challenges we faced were as following:

- Multiple customer isolation and adherence to compliance: The customer wanted multiple isolated environments for their different customers adhering to strict healthcare compliance requirements
- Automation: The customer wanted an automation enabled system that can bring up the infra for the new customer in few hours
- Interconnect several multiple environments: The customer wanted a simpler internetworking amongst different environments adhering to strict guardrails
- Self-managed with minimal manual intervention: The customer's expectation was once the infra is setup, the system management for patching and other maintenance is purely automation driven and least manual intervention
- Lack of expertise: The customer did not have a team with strong cloud implementation experience and thus expected us to bring in best practices

Our Approach and Solution

Considering the customer requirement for multiple isolated environments for different customers and keeping in mind the need for additional accounts as the customer grows, our objective was to ensure cloud setup and governance are simple and less time-consuming. Hence, we implemented an AWS Control tower-based multi account landing zone.

The following organizational unit (OU)structure was implemented:

- **Core OU - AWS master account, log archive account, audit account**
- **Shared Services OU - Network account, automation account, devOps account**
- **Application OU - for application development, test, and quality assurance (QA)**
- **Customer OU - Customer related production, non-production, user acceptance testing (UAT) accounts**

Network Architecture

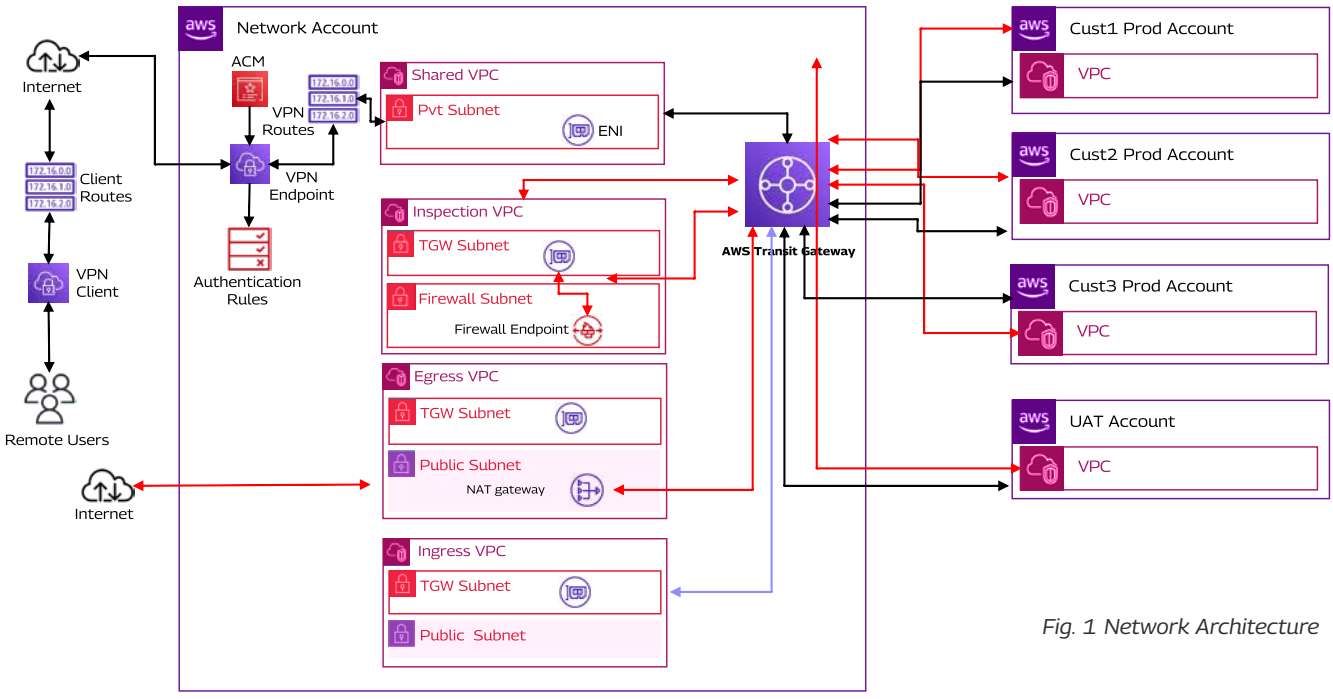

Fig. 1 Network Architecture

The network architecture is designed around AWS Transit gateway being the core of the architecture and is as shown in Fig. 1 above.

AWS Transit gateway simplifies the routing across different networks, and easy to manage - the enabling and restricting of traffic to / from different networks; in addition to easy scaling of the service as the number of accounts increase. Network account part of shared services OU hosts the transit gateway and is used to manage the route table for traffic. The network account has below virtual private cloud (VPCs)

- **Common VPN VPC** - to enable secure VPN connection to access AWS resources
- **Egress VPC** - Outbound internet traffic for AWS resources from all accounts
- **Ingress VPC** - Inbound internet traffic for AWS resources from all accounts
- **Inspection VPC** - Monitor all the traffic to / from all AWS resources. This hosts firewall endpoint within a separate firewall subnet. The VPC route tables are configured to route the traffic through network firewall.

Automation of infra provisioning using IaC and service catalog

Service catalog / products in combination with cloud formation templates are used to provision the infrastructure. This approach makes it easy for security and governance.

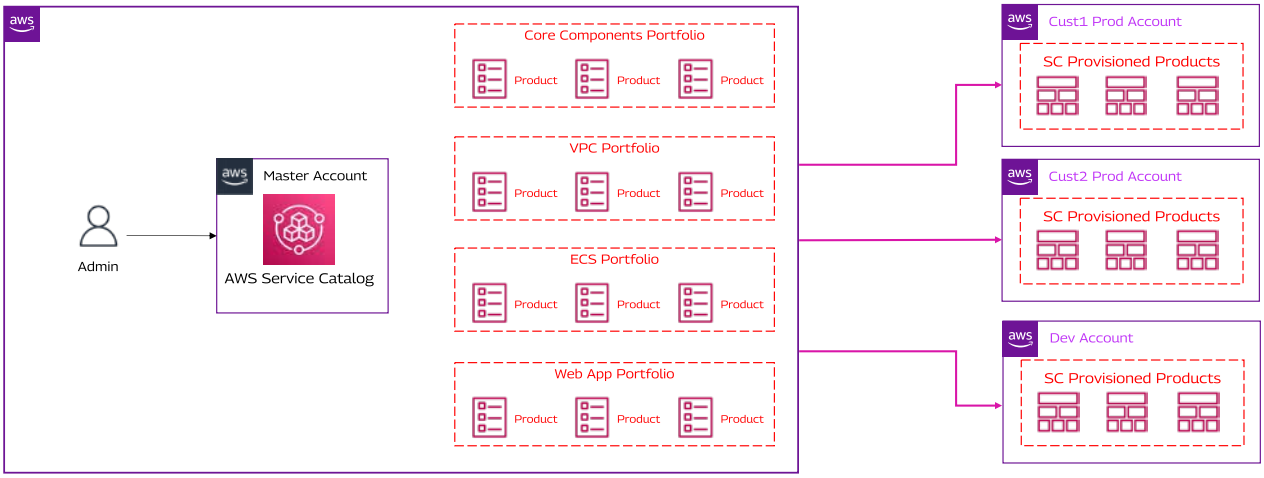

Fig. 2 Multi-account Hub and Spoke AWS Service Catalog architecture

AWS Fargate based ECS

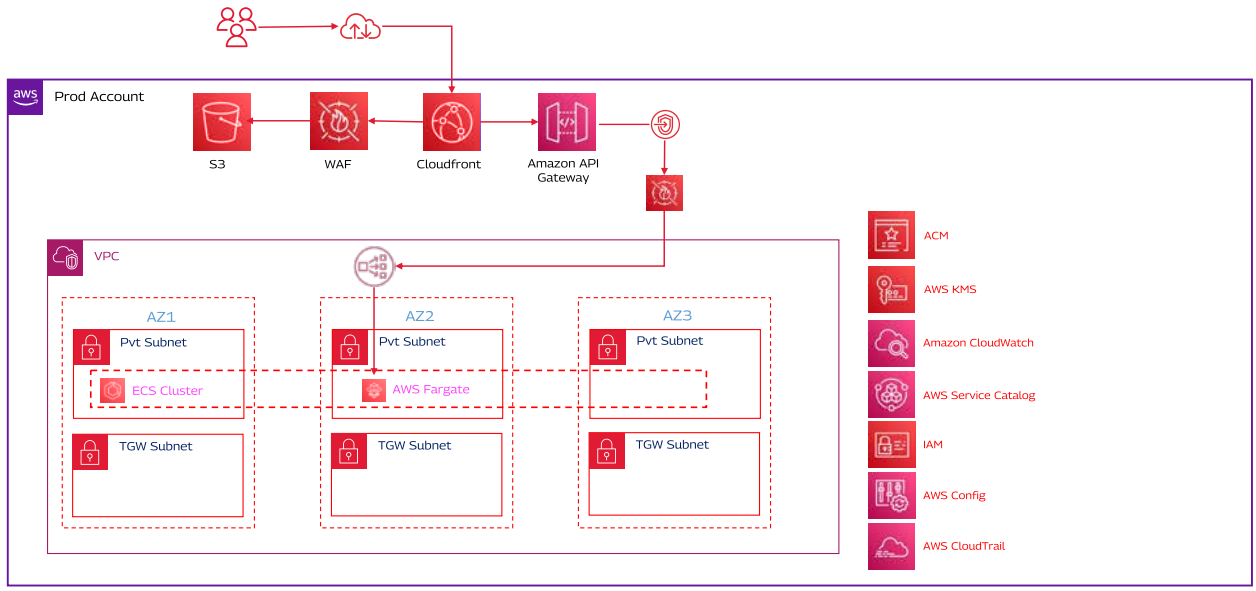

Fig. 3 AWS Fargate based ECS Infra diagram

An AWS Fargate based ECS cluster hosts the microservices application environment hosted on the AWS infra isolated for each of the customer thus adhering to compliance. This infra is provisioned using IAC and AWS Service Catalog / Product portfolio that are available in self service mode.

Business and Community Impact

- Reduction of deployment cycle and service creation time from days to minutes
- Implement a common self-service deployment pattern that is standardized across the organization, incorporating best practices, and in line with compliance and security standards
- Shared service platform to automatically include security and operational best practices into every customer deployment
- Reduced operational overhead, cost, and risk associated
- Includes a standardized approach for monitoring to ease troubleshooting of issues
- Fast, efficient, and standard deployment process - lead time optimization
- Increased productivity, reduced operational cost, and Improved user satisfaction
- Reduced IT expense; improved bottom line
- Reduced downtime; flexible to demand load - Reduction in expense, improvement in client experience
- Standardized process catering to compliance and security requirements
- Ease in governance resulted in more focus on business opportunities
- Improved performance and user experience by minimizing downtime and service degradation with proactive incident detection

For more information, please write to: **CloudNXTMarketing@TechMahindra.com**

TECH mahindra

www.youtube.com/user/techmahindra09
www.facebook.com/techmahindra
www.twitter.com/tech_mahindra
www.linkedin.com/company/tech-mahindra
www.techmahindra.com
top.marketing@techmahindra.com