FINANCIAL SERVICES

APPLICATION HOSTING ON AWS

LEADING MICROFINANCE INSTITUTION WAS HELPED WITH APPLICATION HOSTING ON AWS ALONG WITH **SECURITY POSTURES WITH PROGRESSIVE'S MANAGED SECURITY SERVICES.**

Start Date – 30th March 2019 **End Date** – 24th April 2019

CLIENT OVERVIEW

The customer is a leading microfinance institution focused on providing micro loans to women customers predominantly in rural regions of India. The company follows a joint liability group (JLG) model of microfinance. The institution provides financial assistance through micro loans such as income generating loans to women engaged in small businesses.

CUSTOMER OBJECTIVE

- Customer was exploring a low CapEx infrastructure hosting and services for their application which serves as Reporting & Services application and Branch Service Application. This application is key to processing and tracking branch-wise business-related service requests.

LANDSCAPE

- This is a .NET based application and the same will be accessed by mobile users and branch users.
- Mobile & Web Applications are public facing whereas Services Application is internal facing.
- Required servers for mobile/web/service application are Windows server.
- Reporting DB and shared DB server are Windows and SQL Server.

SOLUTION APPROACH

PAYG model ensured that CapEx is completely cut down for provisioning this infrastructure.
The UAT server consumption was utilised using automation.
Production infrastructure is hosted in a secure fashion by pacing all servers in private subnet. The Web application is placed behind load balancer thus the IP isn't exposed directly to the internet.
Secure access to infrastructure by administrator is through IPsec tunnel.
S2S VPN connection to be established between on-premise and AWS infrastructure.
Segregation of subnets based on workload.
Internet facing Application Load Balancer to distribute HTTP/HTTPS traffic.
S3 Bucket for storing Angular application code.

OS PLATFORMS

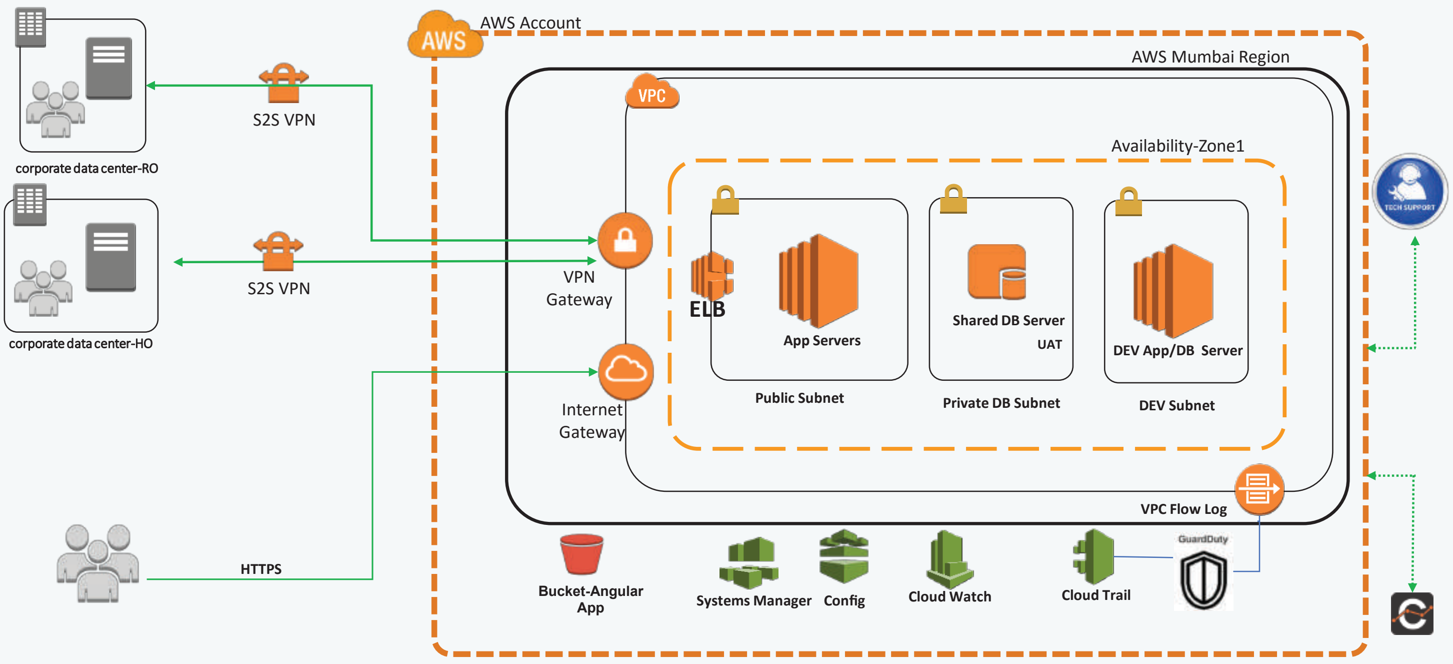
Windows

DESIGN CONSIDERATIONS

All Internet facing applications should be protected by a Web Application Firewall to protect from OWASP Top 10 vulnerabilities.

Database should be hosted on a Multi-AZ deployment model for better performance & availability.

SOLUTION ARCHITECTURE



OPERATIONAL BEST PRACTICES

1. Patching Automation

AWS Systems Manager Patch Manager automates the process of patching managed instances with security-related updates. For Linux-based instances, you can also install patches for non-security updates.

2. Backup & DR

For Backup of EC2 instances, native image based incremental backup will be triggered & which will further be integrated with our in-house auto-backup tool for automatic scheduling & alerting for every successful & unsuccessful backup.

3. Firewall & Security

AWS EC2 Security Groups will act as the firewall to allow the access only from defined IPs in the security rules.

VPC Flow logs have also been proposed (as a future roadmap) which is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC.

4. WAF & Security

It is highly recommended to have a WAF in place for protection of all public facing websites from Top 10 Vulnerability attacks.

AWS Native Service such as GuardDuty has also been proposed with the architecture. GuardDuty is a threat detection service that continuously monitors for malicious or unauthorized behavior to help protect AWS accounts & workloads.

5. Tagging Recommendations

It is highly recommended to tag all AWS Resources.

SERVICES USED

EC2 | VPN GATEWAY | SECURITY GROUPS | CLOUDWATCH | CLOUD TRAIL

SYSTEM MANAGER | AWS CONFIG | VPC FLOW LOGS | GUARD DUTY

OUTCOMES

- Infrastructure size and cost optimization has been achieved as part of MSP Advisory services.
- Customer was able to save 20% of the estimated consumption by enabling the scheduler for the business hours only.
- Application compatibility with the provisioned instance (Windows OS) delivered better user experience.

The customer has opted 24x7 managed service support where Progressive Infotech is offering Proactive Monitoring, support, advisory, and management of the infrastructure. As part of the managed service deliverables, Progressive Infotech is committed in providing better customer experience through Alert Management, Security Controls, Infrastructure & Cost Optimization. Server start/stop has been enabled for the required business hours.