R SYSTEMS

CLOUD MIGRATION

CASE STUDY:

Digital Modernization

Migrating Legacy Apps to AWS Cloud

A US-Based **PERSONAL FINANCE SOLUTIONS LEADER**

Improved Security & Reduced Operational Costs

Using a **Scalable AWS Cloud-Based App**

www.rsystems.com

Client Overview

The client is a US-based personal finance solution provider, helping their customers to plan, invest, navigate their financial goals through financial decisions. They provide simple & ethical solutions on their online platform to assist customers to partake in the benefits of financial planning. With their robust systems and efficient processing team, they strive to deliver a steadfast & highly responsive experience to their customers.

Problem Statement

With growing business demand, the client was supposed to resolve the financial queries of the customers within the provided timeline & SLA. But due to legacy based infrastructure and apps, client couldn't do so. The client needed to keep an active directory server at their corporate office with least manageability by IT team. Considering a financial firm, it was expected to secure the accessibility of emails and financial data. From corporate network and allowed remote network only, authorized systems and employees should be able to access the applications & connect with minimum latency.

R Systems was engaged to migrate on-prem applications to AWS which specifically required identifying incompatibilities & re-architecting few of those applications as per FSI compliance.

Challenges Faced

R Systems developed a highly available, adaptable, stable and secure solution for the client who had an active directory & MS Exchange-based authorization, authentication and communication architecture and expected to modernize it for real-time communication and team collaboration. They had financial apps and needed to identify incompatibilities & re-architect those apps to run on Windows-based EC2 workloads in AWS and be securely accessible from other locations as well. Since it belongs to financial domain, ensuring the security of the solution was vital. Our team considered all these requirements while designing the solution.

Why AWS?

Amazon Web Services is a pioneer in providing leading technology services. Various AWS capabilities were utilized to achieve desired outcomes:

- Used AWS managed directory service for directory aware workloads & its integration with RDS-MSSQL, Workspaces and WorkDocs
- Configured Microsoft Windows OS editions for running .NET applications & financial software (QuickBook app)
- Employed Systems Manager to regularly patch the Windows EC2 Workloads
- Ensured near Disaster Recovery (DR) deployment with multiple availability zones
- Enhanced security with IAM, Inspector
- Used CloudWatch for service monitoring and SNS for real-time notifications
- Implemented logging services like CloudTrail for audit
- Developed a well-architected framework for resilient and secure architecture

R Systems' Solution

Delivered cloud-based solution using various AWS services e.g. EC2, AWS managed Microsoft AD, Workspaces, and Inspector, etc. to securely connect every employee and end-user with application during off-hours as well.

Deployment Highlights:

- Re-architected legacy applications to run on AWS
- Integrated on premises Active Directory to AWS by using AWS managed Microsoft AD service
- Migrated on premises exchanged based email solution to Office365 with MS Teams for better collaboration among employees
- Secured Office365 applications from corporate office & AWS network only
- Utilized AWS Workspace service based on WIN 10, to access internal apps securely from outside the office
- Configured .NET applications on MS Windows EC2 instances in Multi-AZ environment
- Used Relational Database Service (RDS) MS-SQL server in Multi-AZ config for scalable DB operations
- Leveraged Autoscaling groups to reduce operational complexity of running and managing apps
- Configured required services, such as IAM, Application Load Balancer, WorkDocs, Route 53, SNS, etc.
- Implemented SSO for accessing Office365 apps from on premise systems

Third Party Tools Used:

- Trend Micro endpoint protection
- Zabbix monitoring tool
- Office365

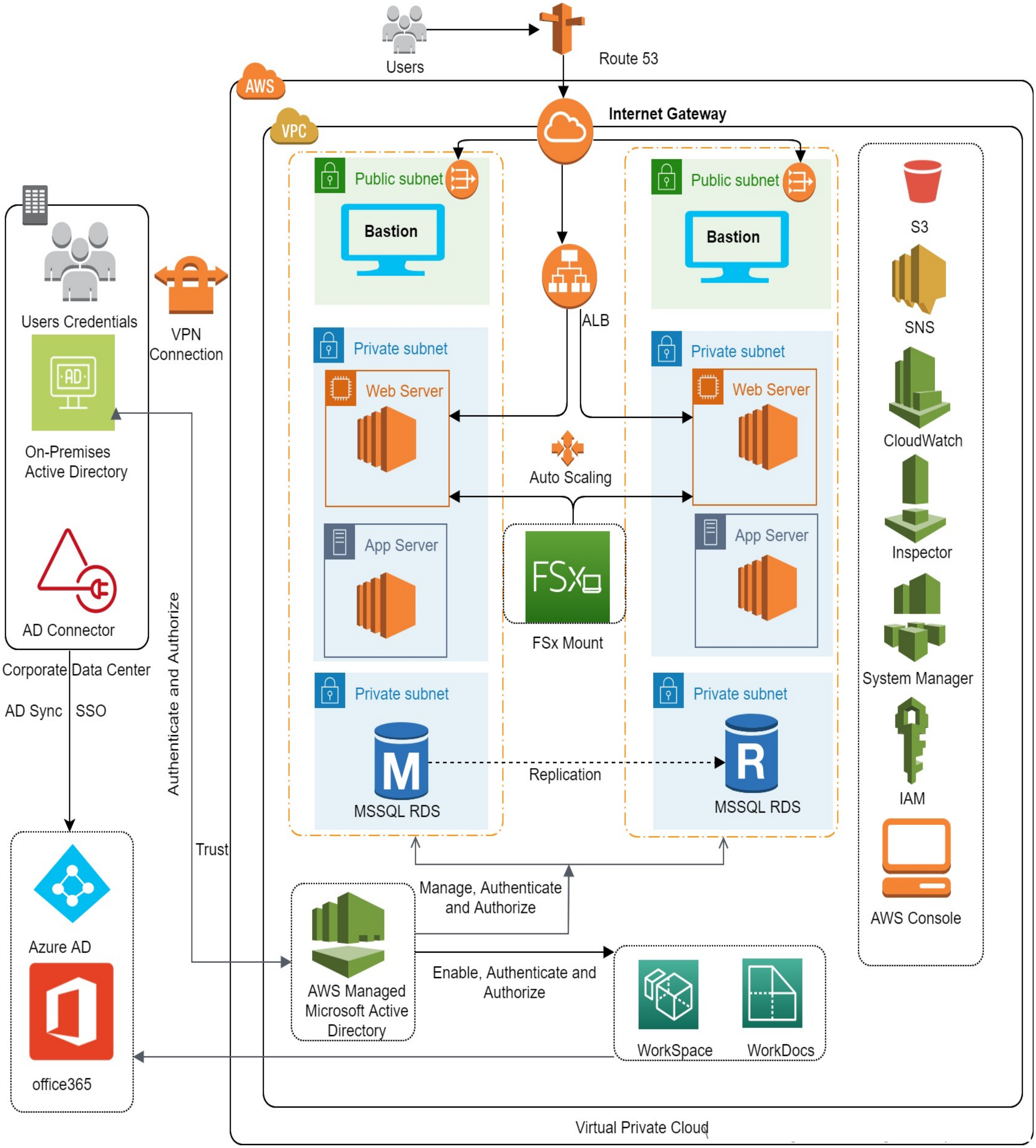
OS & Database:

S. No.	Operating System	Database
1	Windows 2019 Datacenter Edition	RDS MSSQL 2017 Enterprise Edition

AWS Technologies Deployed:

- **RDS MS-SQL:** To manage SQL Database
- **EC2:** To create virtual server in the cloud
- **Systems Manager:** To manage OS patching of Windows-based EC2 instances
- **AWS Managed MS AD:** To manage AD-aware workloads
- **AWS Workspaces:** To provide access to internal secure app to employee from outside office network
- **AWS WorkDocs:** To secure content creation, storage, and collaboration
- **FSx for Windows:** To share file for Windows workloads
- **AWS Inspector:** To improve security and compliance
- **ACM (Certificate Manager):** To easily provision, manage & deploy SSL certificates
- **CloudWatch:** To monitor resources & applications
- **ALB:** To distribute traffic to servers in multiple AZs
- **Autoscaling:** To manage server count as per traffic
- **SNS:** To manage message topics

Architectural Diagram



Operational Excellence

Monitoring tools like AWS CloudWatch & Zabbix were used to generate actionable alerts which were responded by IT team. CloudWatch dashboard was created for IT team to monitor the real-time status of AWS resources. AWS Systems Manager was used to ensure that all Windows based workloads were regularly patched in the defined maintenance window.

Security

- Ensured complete security inside/outside the AWS perimeter & at multiple layers
- Enabled SSO to allow users to access AWS console & resources through their AD credentials. Multi-factor authentication (MFA) was made compulsory
- Whitelisted NAT gateway elastic and on-prem IPs in Office365 to allow traffic from specific IP addresses
- Used AD trusts to connect AWS Managed Microsoft AD to on premises AD. This means users can access AD-aware & AWS applications with their on-premises AD credentials, without needing to synchronize users, groups, or passwords
- Enabled MFA, and disabled programmatic access for root accounts
- Configured separate subnets for each layer (Web, Application, Database) for network-level isolation
- Configured apps on EC2 instances to use IAM roles
- Deployed security groups and NACLs with least permissive rules
- Used App Load Balancer to route the traffic to private subnet's servers over multi-availability zones of AWS for higher availability, and achieve near DR deployment
- Configured VPC flow logs to monitor the incoming/outgoing traffic at ENI level. Logs were stored in S3 bucket for 90 days and then archived to Glacier using life cycle policies
- Implemented CloudTrail to record the API activity of AWS services and logs stored in S3 bucket for audit
- Enabled Amazon S3 server-side encryption (AES-256) to encrypt data at rest
- Encrypted EBS volumes using KMS to safeguard the data in transit
- Configured hardened bastion hosts to access EC2 servers in private subnets
- Maximized security with antivirus protection using Trend Micro endpoint protection
- Configured VPN to secure the traffic coming from Corporate Datacenter to AWS
- Used hardened OS AMIs as per CIS standards

Reliability

R Systems deployed its solution in one AWS region, via AWS Well-Architected Framework, using two Availability Zones (AZs) to ensure availability of all apps.

AWS Life Cycle was configured to take periodic backups of the tagged EBS volumes. Thus, ensuring availability of snapshots of EBS volumes for recovery.

AWS managed database service was used to deploy MS-SQL 2017 server in Multi-AZ architecture to ensure high availability of database. Both primary & secondary database remained in sync & automated backups were configured to minimize RPO & RTO.

Cost Optimization

- Configured Autoscaling to automatically reduce the server count across all layers (Web, Application) based on incoming traffic
- Reduced operational costs by using managed services, such as RDS, AWS directory service
- Selected C5 family instances and purchased 1-year RI (reserved instance) to reduce bills

Project Outcomes & Success Metrics

- Integrated on-prem active directory & exchanged based workload to Amazon cloud & Office365
- Provided virtual desktops using AWS workspaces
- Ensured secure content creation, storage and collaboration using Workdocs
- Provided high availability systems with negligible downtimes
- Utilized Autoscaling to handle traffic
- Used Multi-AZ architecture, automated backups as disaster recovery feature
- Leveraged CloudTrail to simplify audit process
- Secured solution using IAM, Inspector, EBS volume encryption, etc.
- Enhanced accountability of providers & individuals
- Reduced complexity of business processes

About R Systems

R Systems is an AWS Advanced Consulting partner & Microsoft Gold partner. We are a global digital transformation leader that provides AI-driven solutions to clients across industries, through a broad range of technology & AI/analytics services. We continue to empower organizations for over 27 years, with 16 delivery centers, 25+ offices worldwide and a workforce of 2750+ professionals.