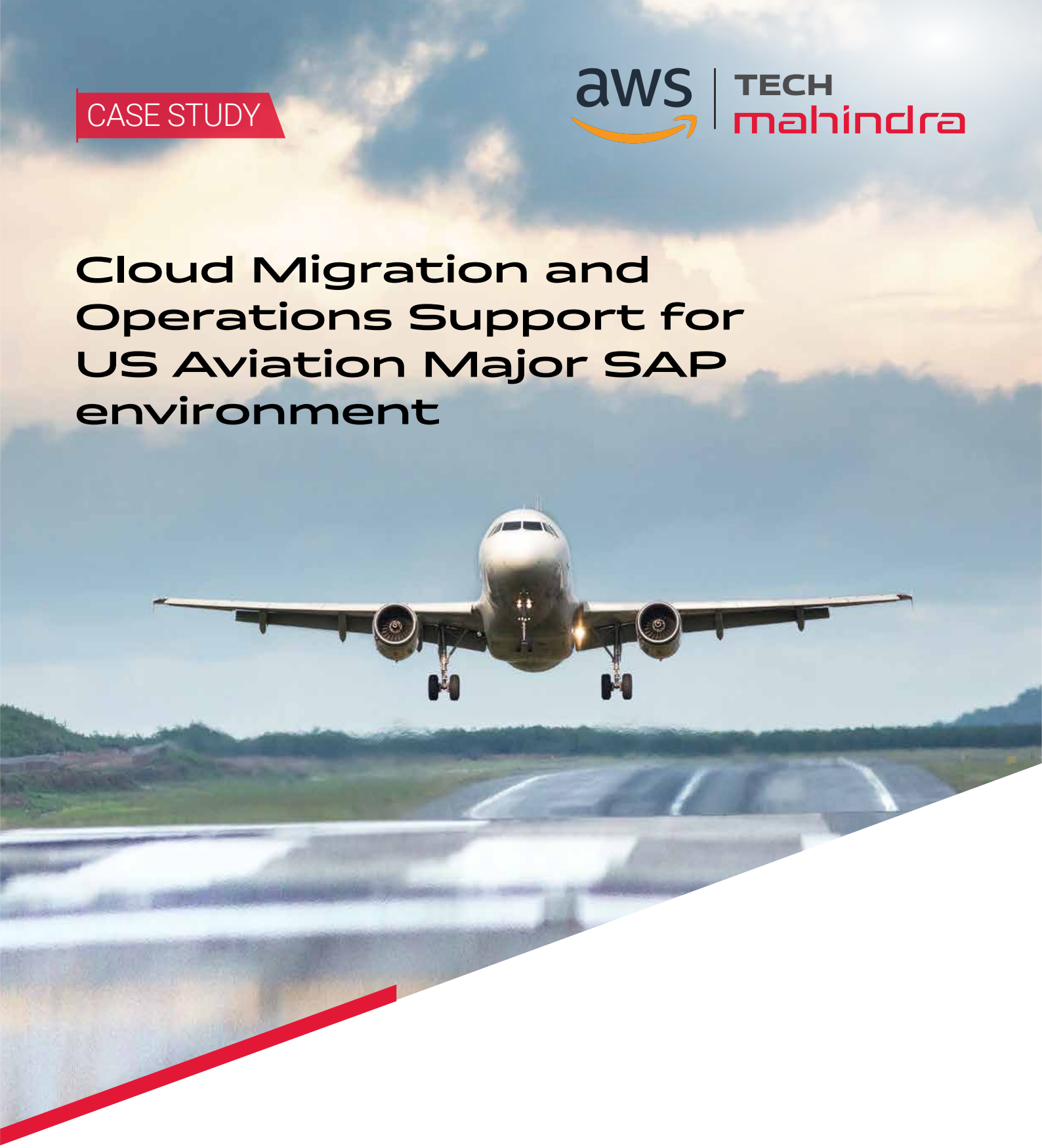
CASE STUDY

Cloud Migration and Operations Support for US Aviation Major SAP environment



Overview

Our client, an aviation major is a world-leading provider of jet and turboprop engines, as well as integrated systems for commercial, military, business, and general aviation aircraft. It has a global service network to support these offerings.

The organization needed to transform their IT infrastructure solution to enhance security, integrity of data, and access control. The customer needed to migrate servers and applications to AWS cloud to increase efficiency, mobility, and improved cost management. High availability and disaster recovery are also the prime requirements. Reactive maintenance, low technician productivity, and lack of full control/access are the few challenges that needed to be tackled for stable environment and seamless operations support.

Client Background and Challenge

SAP ECC 6 is an enterprise resource planning (ERP) solution that helps organizations manage their users, track operations, and perform preventive maintenance leveraging predictive analysis and enterprise-ready features.

The customer was facing issues like no control and visibility of the hardware resources; infra level high availability (HA)/disaster recovery (DR) solution are also not there with the existing datacenter provider. They face complete outage for monthly operating system (OS) patching. Data refresh tasks and infra scaling was expensive and tedious.

With cloud computing becoming the norm in the industry, Tech Mahindra provided migration services to move Customer's SAP instances and the associated systems from current provider to cloud. Understood the system landscapes and performed migrations based on project/ operation needs. Designed and built

subset of systems in a new environment restored from an existing system. Created high level project plan and hyper care plan post go live for the services provided.

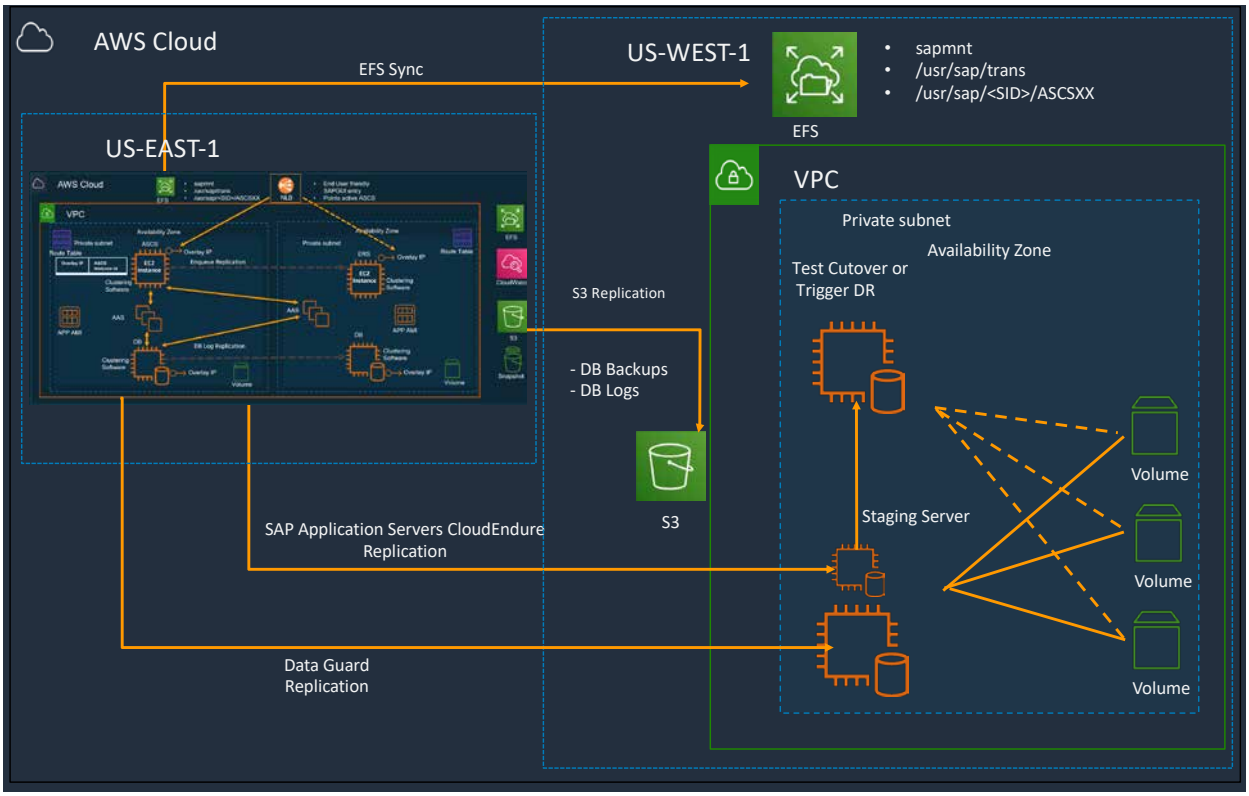
Our Approach and Solution

- Design and plan workloads migration from Virtustream Dell cloud to AWS cloud
- Provisioned AWS VPC accounts for development, quality assurance (QA), production and disaster recovery (DR) environments.
- Defined route tables, subnets CIDR range planning, and VPC transit gateways
- CloudFormation stacks were used to Build Amazon Elastic Compute Cloud (EC2), Amazon Elastic File System (EFS), and network load balancer
- Hardened / customized images of RHEL and OEL images used to build instances
- GP3 Amazon Elastic Block Store (EBS) volumes used for file systems and Amazon Elastic File System (EFS) is used for SAP transport shares
- AWS network load balancers (NLB) configured to connect SAP graphical user interface (GUI) logins
- Network access control list (NACLs) and Security groups (SG) ports implemented to secure SAP apps and database (DB)
- SIOS solution is used for SAP ASCS and ERS central instance high availability
- Oracle Data Guard broker is used for database (DB) production high availability and disaster recovery (DR) solution
- CloudEndure used for SAP CI and ECC application instances in DR scenario
- SAP data mock loads and performance testing done to check system stability
- AWS instances bootstrapping with Chef for configuration management
- AWS Systems Manager (SSM) implemented for monthly patching operating systems
- New relic is used to monitor AWS resources
- Amazon Simple Storage Service (S3) buckets are used for data migration and route 53 is used for site resolutions
- Qualys, Splunk, Crowdstrike installed for security, logs, and endpoint protection
- AWS Backup policies created for volumes snapshots and DB RMAN backups

Multi Account Structure

- Multi-account strategy based on workload type and environment type was implemented to isolate the environments and workloads
- 4 Amazon virtual private cloud (VPCs) for production (2) and non-production (2)
- Each of these VPCs span across two AWS Availability Zones in US-East-1 region for high availability and DR zones in the US-West-1 region.
- Production Accounts:
  - US-EAST-1-Prod
- Non-Production Account:
  - US-EAST-1-Non-Prod
- Production DR Account:
  - US-WEST-1-Prod
- Non-Production DR Account:
  - US-WEST-1-Non-Prod

AWS Architecture



- Architecture meets the customer requirements of high availability and disaster recovery solution
- Primary region with two availability zones (AZs) were built in US-EAST-1 and DR is in US-WEST-1
- CloudFormation templates were used to auto provision AWS Infra with SAP installation
- Pacemaker with overlay IP across different AZs has been configured as HA solution for SAP systems
- AWS Disaster Recovery Solution (DRS)/CloudEndure has been configured for disaster recovery solution
- Oracle data guard has been used at database level for HA and DR
- Oracle Service Bus (OSB) was used for database backups which sends the database backups directly from Oracle to S3. This Backup is replicated to the DR region using the S3 cross region replication (CRR)
- Shared EFS mounts were configured per SID. EFS sync is being used to replicate data across Region for DR

Cloud Operations

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. Amazon CloudWatch events are used to detect and react to changes in the status of Amazon Web Services (AWS) resources. Based on the rules created, CloudWatch events invokes one or more target action like Amazon Simple Notification Service (SNS) notifications, capture event information, take corrective action, initiate events, or take other actions. VPC flow logs are enabled to monitor the traffic flow. New-Relic is used to monitor hardware resources and alert the team for any alarms set.

Governance

AWS CloudTrail is enabled to track the activities of the account users. Any resource level changes are monitored based on AWS API activity. Created cloud formation templates that are used to provision the infrastructure consisting of VPC, two subnets spread across multiple AZs, provision EC2 instances, application load balancer (ALB), NLB and SAP install. AWS Systems Manager (SSM) is used to stop the non-prod servers during non-business hours and on weekends. Simple, repetitive tasks automated, freeing up valuable personnel for more important, complex tasks.

Security and Access Management

Using AWS Key Management Service (KMS) services like Amazon EBS and EFS 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. App specific load balancers were enabled to permit legitimate traffic to hit application servers. AWS Secrets Manager is used to store credentials and secrets like credentials. AWS access is enabled through federation using customer's AD via single sign-on process. IAM role is used to control level of access to AWS resources and services.

Operations Management

AWS systems manager is used to keep all the Amazon EC2 instances up to date and for patching process regularly. Leveraged CloudFormation for Infra Provisioning and SAP installation. ServiceNow 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. Runbooks have been created to improve the incident triage time for repeated and critical issues within AWS.

Business and Community Impact

- 25% reduction in total cost of ownership (TCO) for the customer while improving the RPO and RTO objective by migrating from Virtustream Dell cloud to AWS cloud. The migration was performed in much shorter time and hence reduced downtime and cost to the customer.
- 30% reduced cost on data center spends.
- Achieved near zero downtime for monthly operational maintenance activities.
- Automated OS patch process using AWS SSM, which increased system availability.
- Increased the security positioning of the customer SAP workload by segregating their workload and following the industry standards on securing SAP.
- Aligned customer practice to DevOps by leveraging AWS CloudFormation stacks for provisioning and scale the workloads.
- Increased operational resilience by implementing New Relic monitoring tool.
- Integrated with ServiceNow for incident management enabling faster business turnaround for critical issues.
- Increased the availability of workloads with clustering for HA and Cloud Endure (AWS DRS) for DR.
- Operational efficiency increased with automation of alerts, backup process, and nimble business recovery/restore process in case of disaster.
- Continuous optimization of AWS resources as part of operations excellence.
- Chef is used for configuration management to maintain the infra and application related agents update to date. This has helped in improving risk management, streamlining IT operations and increasing service resiliency.

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