Minfy-Vara Migration Use Case

Minfy-Vara Migration Use Case

Document Details

Use Case Name	**Minfy Migration - Use Case01**
First Draft	**30 Jul 2018**
Author	**Amrendra Kumar**
Reviewed By	**Pradeep Narayanaswamy**

Minfy-Vara Migration Use Case

Contents

Minfy-Vara Migration Use Case

Scope

This document provides a detailed use case study on migration using lift and shift of applications from on premise to AWS and re-engineering of AWS infrastructure by following AWS best practices with guidelines for implementation.

About Customer

Vara United is a global software solution and services company with over 3500 resources that provide a comprehensive range of services catering to the Banking, Financial Services and Insurance (BFSI) segment. Vara's agile and collaborative approach in developing customized and revolutionary solutions help our customers derive maximum profits from their business.

Vara United is a part of the grand lineage of Kanoria Foundation. The Foundation's ethos, to 'Work With Devotion' represents our guiding philosophy – to work with diligence and passion, and our practice – to have strong corporate citizenship. It reflects the constant churning of ideas and hard work, which are essential to succeed and the passion necessary to implement them with a focus on results.

At Vara United, we provide diverse solutions catering to the BFSI Industry which includes Business Process Outsourcing (BPO), Application Services and Infrastructure Management services (IMS). Vara United as a new entity is steadily advancing towards large scale implementation of mission critical solutions.

Use Case Description

Vara United is a software development and hosting company and developing their product with the stack of php, javaScript, MySql and Postgresql and front end technologies. The production server was on premise which needed to be migrated on AWS environment.

To lift and shift the environment from on-premise to AWS, we have followed below activities,

- Review & Assess existing infrastructure components
- Access to AWS Console
- Provisioning of AWS infrastructure components
- Migrating infrastructure components and websites
- Cut over to AWS

Primary & Supporting Actors

- ***Actors from MinfyTech: Sandeep & Amrendra***
- ***Actors from Client: Mukesh***

Pre & Post Conditions

- ***Pre-implementation state***
  42 websites were hosted in an individual IBM on premise server. Frequently, websites used to go down because of space constraint. Since databases were also in the same standalone server, that led to performance issues.

- ***Post-implementation state***
  Performance has enhanced post migration by choosing required instance type. Databases moved to RDS for high performance. All websites moved to EC2 Instance and DNS pointed to new AWS server. New licence procured for migrated cPanel.

Minfy-Vara Migration Use Case

Trigger/Challenge

1. Single standalone server consists of 42 websites using cPanel
2. Less storage availability
3. Procuring new cPanel licences
4. Redirecting subdomains to different websites as all websites are into same EC2 instance

Implementation

- **Preliminary preparations –** DC end sanity check has been done. During this process entire on premise environment was identified that include application stack, file level architecture and current web services running on DC end.
- **Proposed architecture –** Based on preliminary preparation, we have proposed the architecture based on the AWS environment.
- **Access to AWS Console - IAM User –** After approval of proposed architecture, AWS credential was received will all necessary IAM user and permissions.
- **Provisioning of AWS infrastructure components -** Based on proposed architecture, AWS infrastructure was provisioned.
- **Migrating infrastructure components and websites –** Migration was completed using cPanel migration tool which is suggested by the Customer.
- **Review migrated components –** Once websites are migrated sanity check was done.
- **Cut over to AWS –** After approval of sanity check, final cut over done from on premise to AWS.
- **DNS routing to new AWS server –** DNS routing was done to new AWS Server.

Security with Migration

Tighten CloudTrail security configurations

- Enable CloudTrail across all geographic regions and AWS services to prevent activity monitoring gaps.
- Turn on CloudTrail log file validation so that any changes made to the log file itself after it has been delivered to the S3 bucket is trackable to ensure log file integrity.
- Enable access logging for CloudTrail S3 bucket so that you can track access requests and identify potentially unauthorized or unwarranted access attempts.
- Turn on multifactor authentication (MFA) to delete CloudTrail S3 buckets, and encrypt all CloudTrail log files in flight and at rest.

Followed Identity and Access Management (IAM) best practices

- When creating IAM policies, ensure that they're attached to groups or roles rather than individual users to minimize the risk of an individual user getting excessive and unnecessary permissions or privileges by accident.
- Provision access to a resource using IAM roles instead of providing an individual set of credentials for access to ensure that misplaced or compromised credentials don't lead to unauthorized access to the resource.
- Ensure IAM users are given minimal access privileges to AWS resources that still allows them to fulfill their job responsibilities.
- As a last line of defence against a compromised account, ensure all IAM users have multifactor authentication activated for their individual accounts, and limit the number of IAM users with administrative privileges.
- Rotate IAM access keys regularly and standardize on a selected number of days for password expiration to ensure that data cannot be accessed with a potential lost or stolen key.

Minfy-Vara Migration Use Case

- Enforce a strong password policy requiring minimum of 14 characters containing at least one number, one upper case letter, and one symbol. Apply a password reset policy that prevents users from using a password they may have used in their last 24 password resets.

Follow security best practices when using AWS database and data storage services

- Ensure that no S3 Buckets are publicly readable/writeable unless required by the business.
- Encrypt data stored in EBS as an added layer of security.
- Encrypt Amazon RDS as an added layer of security.
- Restrict access to RDS instances to decrease the risk of malicious activities such as brute force attacks, SQL injections, or DoS attacks.

Custom applications security best practices

- Inventory and categorize all existing custom applications deployed in AWS
- Involve IT security teams throughout the application development lifecycle
- Grant the fewest privileges possible for application users
- Enforce a single set of data loss prevention policies

Benefits

Cost Savings: A Cloud Hosted Desktop provides you with scalable computing power, while minimizing IT requirements and physical data storage, providing you with significant savings.

Security: Perhaps the weakest link in the initial days of cloud adoption was security concerns. But today, more people have begun to realize these concerns are misguided. Cloud IT service providers actually provide higher levels of security and data integrity. Why? Because they make huge investments in the resources and technology, along with a skilled team of IT experts and engineers smaller businesses just can’t afford to do on their own.

Connectivity & Accessibility: Keep users connected no matter where they work with anytime, anywhere access. Users may access files anytime, anywhere, using any device. That means no more risk of files being stored on any computer.

Reduced Risk of Data Loss: Even more security for users by backing-up data offsite – decreasing the potential for hackers, viruses, ransomware, and other cybersecurity problems. Let’s repeat that again, more security. (Read: 3 Tips to Prevent Data Loss).
Faster Deployment: Cloud-based services can be deployed within just an hour or a few days rather than the weeks, months or years it can take to strategically plan, buy, build and implement an internal IT infrastructure with internal personnel.

Increased Collaboration: Cloud computing enables employees situated in various locations to collaborate easily. By providing simultaneous syncing, working and sharing documents and records in real time, cloud computing helps increase the collaboration and efficiency of employees.

Improved Efficiency: After migrating to the cloud, you no longer need to worry about power requirements, space considerations, expensive computer hardware, or software updates. You get to keep your entire company focused on generating revenue and relationships, not on IT.