Minfy MS Workloads Use Case

Minfy MS Workloads Use Case

Contents

Minfy MS Workloads Use Case

Scope

This document provides a detailed use case study on Hosting GST Application built on .NET v4.5, using database as MSSQL Standard Edition, version 13.0.4474.0. from the scratch on AWS by following AWS best practices with guidelines for implementation.

About Customer

Customer is one of the largest professional services firm in the world.

Use Case Description

To Host the complete GST infrastructure on AWS by leveraging the Advantages of different AWS Services it has been started with the Development Environment. Proceeding further QA, UAT, Pre-Production & Production Setup along with the training was also been done completely on AWS. Complete Architecture were designed referring to the AWS best Practices in each and every layer. Each Environment were segregated by the distinct Virtual Private Cloud. Environment wise resources properly tagged and Security best practices driven Audit is performed on regular basis to eradicate the Flaws. The Public Facing JIRA Portal were also hosted for this Application on AWS on a different Virtual Private Cloud.

Technical Stack

Technology Stack

- **Web Server:** Windows 2012 R2, .NET v4.5
- **AD Server:** Windows 2012 R2
- **DB Server:** Windows 2016, SQL Standard License included version 13.0.4474.0
- **DB As a Service (RDS) :** SQL Server Standard Edition 13.00.4422.0.v1 Engine

AWS Service Stack

- EC2
- VPC
- ELB
- NAT
- ROUTE53
- Cloudfront
- Cloud Trail
- Cloud Watch
- IAM
- RDS
- ACM etc.

Minfy MS Workloads Use Case

AWS Solution Walkthrough

- Segregated different Environments as well as their Application Stack into Different VPC
- Concluded the instance types to be used each environment
- Created Network Layout Diagram
- Created Architecture Diagram
- Setup Client2Site VPN to access AWS VPC with MFA for management
- Addressed dependencies like local firewall and internet blockage to establish connectivity via VPN with AWS
- Configured AWS CLI with specified IAM Access Key pair given to use File Upload utility
- Configured IDS/IPS Solution on all the servers
- Configured Cloud Endure in each Client DB for DR mechanism to maintain snapshots in real time
- Setup DNS name mapping against C-Name of the provided AWS resources like Cloud Front or ELB as per the Environment
- Configured Primary & Secondary Domain Controller with the Client Domain Name shared. And Setup all the instances as a part of it, segregated Environment wise
- Configured ADFS Primary and Secondary for access federation, Environment Wise
- Imported Custom SSL certificate to AWS-ACM to be further used on Cloud Front, ELB level
- WAF implemented having CloudFront as origin
- S3 Endpoint Configured from VPC to have any s3 to & fro transactions

Security

CloudTrail Security Configurations

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

Identity and Access Management (IAM) Best Practices

- When creating IAM policies, we ensured that they're attached to groups or roles rather than individual users to minimize the risk of an individual getting excessive and unnecessary permissions or privileges by accident
- Provisioned 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
- Ensured IAM users are given minimal access privileges to AWS resources that still allows them to fulfil their job responsibilities
- As a last line of defence against a compromised account, ensured all IAM users have multifactor authentication activated for their individual accounts, and limit the number of IAM users with administrative privileges
- Rotated IAM access keys regularly and standardized on a selected number of days for password expiration to ensure that data cannot be accessed with a potential lost or stolen key
- Enforced a strong password policy requiring minimum of 14 characters containing at least one number, one upper case letter, and one symbol. Applied a password reset policy that prevents users from using a password they may have used in their last 24 password resets

AWS Database and Data Storage Services

- Ensured that no S3 Buckets are publicly readable/writeable unless required by the business
- Encrypted data stored in EBS as an added layer of security

Minfy MS Workloads Use Case

- Encrypted 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 D-Dos attacks

Custom Applications

- Maintained inventory and categorized all existing custom applications deployed on AWS
- Involved IT security teams throughout the application development lifecycle
- Granted minimal privileges possible for application users
- Enforced 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
- **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