Minfy MS Workloads Use Case

Minfy MS Workloads Use Case

Contents

Scope 3
About Customer 3
Use Case Description 3
Technical Stack 3
AWS Solution 4
Security 4
Benefits 5

Minfy MS Workloads Use Case

Scope

This document provides a detailed use case study on Hosting GSP Application built on .NET v4.5, using database as MySQL Aurora from the scratch on AWS by following AWS best practices.

About Customer

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

Use Case Description

To start with, we hosted the complete infrastructure on AWS by leveraging the advantages of different AWS Services on the UAT Environment. Proceeding further, Sandbox & then Production Setup was done on AWS. Complete Architecture was designed referring to the AWS best Practices in each and every layer. Each Application stack was segregated by smaller network segments called subnets in the Virtual Private Cloud. Each resources were properly tagged and Security best practices driven audit is performed on regular basis to eradicate any flaws.

Technical Stack

Technology Stack

- **Web Server:** Windows 2012 R2, .NET v4.5
- **AD Server:** Windows 2012 R2
- **DB As a Service (RDS) :** MySQL Aurora Engine

AWS Service Stack

- EC2
- VPC
- ELB
- NAT
- ROUTE53
- Cloudfront
- Cloud Trail
- Cloud Watch
- IAM
- RDS
- ACM
- Direct Connect
- EMR
- Lambda
- ASG
- Cloud Formation
- WAF
- Kinesis
- S3
- KMS

Minfy MS Workloads Use Case

AWS Solution

- Segregated each Application Stack into Different sub network classification within a VPC called Subnets
- Concluded the instance types to be used on each environment
- Created Network Layout Diagram
- Created Architecture Diagram
- Setup Direct Connect with GSP
- Setup Client2Site VPN to access AWS VPC with MFA for management
- Configured Cisco CSR Router prior direct connect from VPC for the Application Connectivity
- Addressed dependencies like local firewall and internet blockage to establish connectivity via VPN with AWS
- Configured Lambda Function within the VPC with Specific Subnets
- Configured IDS/IPS Solution on all the servers
- Configured Squid proxy server post ELB for the Application response
- 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
- Configured Kinesis Stream
- Imported Custom SSL certificate to AWS-ACM to be further used on Cloud Front, ELB level
- WAF implemented having CloudFront as origin with rate based Rule
- S3 Endpoint Configured from VPC to have any S3 to & fro transactions

Security

CoudTrail 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

Minfy MS Workloads Use Case

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
- 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