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 E-commerce Application of Customer built on .NET v4.5, using database as MSSQL- Standard license included version from the scratch on AWS by following AWS best practices with guidelines for implementation leveraging different AWS Services.

About Customer

Customer is a service oriented e-commerce business which gives you the authority to unleash your shopaholic attitude from home with quality products and world class customer support.

Use Case Description

To Host the Complete E-Commerce Application of Customer on AWS by leveraging the advantages of different AWS Services. 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 resource was 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
- **DB Server:** Windows 2012 R2, MSSQL Standard Edition

AWS Service Stack

- EC2
- VPC
- ELB
- NAT
- Cloud Front
- Cloud Trail
- Cloud Watch
- IAM
- RDS
- ACM
- S3
- Elastic Search
- Lambda
- ASG

Minfy MS Workloads Use Case

AWS Solution Overview

- Servers were launched in the AWS Singapore Region. All access is controlled via Identity and Access Management (IAM) Console of AWS. This also allowed enabling Multi Factor Authentication for secure access
- A secure cluster of servers were launched into a private subnet under a Virtual Private Cloud (VPC). VPC is like a cloud in a cloud and is not accessible to the internet world
- Servers are launched in both the availability Zones (Data Centres in a Region) which serves the purpose of both High Availability and Disaster Management
- All Servers are launched in a Public or Private Subnet. Subnets are used to virtually segregate the servers into various groups. Each subnet is launched under its own subnet range for additional security. Network Access Security List (NACL) is a stateless firewall that provides both inbound and out bound access restriction features
- Servers are launched in an AutoScale unit. AutoScale is an advanced feature of AWS that guarantees that servers scale horizontally in case there is an increase in load
- Each server (or server group) is launched in a security group. Security groups are stateful firewalls where-in we can control the inbound IP and Port access
- An Elastic Load Balancer (ELB) was configured that will connect to servers in both the regions. Load balancer automatically removes unhealthy instances and requests the Auto Scale unit to provide a new pre-configured server with the application installed to it
- AWS RDS database was configured. Since MSSQL Express was being looked for, a server with maximum 1 core CPU has been provisioned. Slave configuration is not available for MSSQL on RDS.RDS performs automated database backup every 24 hours. However, backup scripts can be also configured and triggered at regular intervals to secure data
- ElasticSearch has been recommended for data reads. This ensures high read throughput with less latency and can handle huge load factor. To sync data between MSSQL and ElasticSearch a server with Logstash was installed. Logstash is a data integrator that connects to multiple different sources (incl MSSQL) and move data into ElasticSearch Database
- Servers in the VPC do not have public internet connection. For the servers to access the public internet a NAT Gateway will be provisioned. NAT behaves as a proxy for the servers inside the VPC. Servers will get access to public websites (like FB or G+ for authentication) only through this NAT Gateway
- Since servers are behind a VPC there is no way for the admin/developers to reach them. Therefore a software VPN, OpenVPN was installed on the VPC. Users need to first login to this secure OpenVPN server to ping the servers inside the VPC. This also allows secure and restricted access the client data on the server
- Since servers are behind a VPC there is no way for the admin/developers to reach them. Therefore a software VPN, OpenVPN will be installed on the VPC. Users need to first login to this secure OpenVPN server to ping the servers inside the VPC. This also allows secure and restricted access the client data on the server
- Cookie cutter instance was used to have the master image of the core application. This master image is used to launch servers in the Auto Scaled units
- For global access of resources, CloudFront was configured. Cloudfront will cache only static objects while dynamic data can be served by the host zone

Minfy MS Workloads Use Case

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

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

Minfy MS Workloads Use Case

- **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