Minfy-Magnaquest Migration Use Case

Minfy-Magnaquest Migration Use Case

Document Details

Use Case Name	**Minfy Migration – Use Case04**
First Draft	**15th August 2018**
Author	**Prabhakar D**
Reviewed By	**Pradeep Narayanaswamy**

Minfy-Magnaquest Migration Use Case

Scope

This document provides a detailed use case study on data center migrations from Magnaquest – Rackspace cloud data center to AWS Cloud Infrastructure

About Customer

Magnaquest was formed in 1997 by a team of technocrats with a vision to build a company with products and solutions providing extraordinary value to enterprises, fulfilling its role in society with high social responsibility and exemplary corporate governance, and building immense stakeholder value.
Joined and fueled by several enterprising people, the company expanded rapidly and grew from one small office in India to four offices in India, the United States of America, Malaysia and United Arab Emirates (UAE). Presently, we are in the process of setting up our fifth office in Zambia.

Requirement

1. Provide Infra Consulting Services for Migration from Current Cloud Service provider to AWS
2. Environment with High Availability, Cost Reduction and Security
3. To manage their existing as-is infrastructure
4. Provide proactive monitoring & continuous delivery on Managed Shared Services

Current Infrastructure	Provisioned	Usage
Active Directory Server	2 VCPUs /4 GB Hard disk 100/33	100 GB
Web Server 3	4cores/4gb Hard disk 100//172	150 GB
Web Server 5	16cores/48GB RAM Hard disk 100/737/1TB	1.5 TB
Radius Server	2cores/4gb Hard disk 100/104	100 GB
Database Server 4	24cores/48GB 2247GB	2.2 TB
Database Server 3	8cores/24GB hard disk	600 GB
Standby DB server	12cores/24GB hard disk	2.2 TB

Migrated Infrastructure

Current Infrastructure	AWS Instance Type	Volume
Web Server 3	4 VCPUs / 4 GB Hard disk – C5.Large -- Windows	150 GB
Database Server 3	8 VCPUs /24 GB -- m5.2x Large -- RHEL	600 GB
Standby DB server	8 VCPUs /24 GB -- m5.2x Large -- RHEL	600 GB
Open VPN Server	1 CPU/2GB RAM - t2.small	8GB
Load Balancers	ELB	2 Count
Directory Services	Small - Upto 1,00,000 Directory Objects	100 Users
Static Storage	S3	1 TB
Backup	Snapshot	~1.5 TB

Scope of Migration

- Minfy built the setup as per MQ requirements, one VPC for PCI-DSS Compliant and another one for non- compliant
- Database migration was done by Minfy using DMS tool from AWS
- Deployment of SIEM for PCIDSS Compliant VPC to pool all the security logs into SIEM for security analysis

Minfy-Magnaquest Migration Use Case

- Network perimeter security, OS level Patch management, and servers' security (IP based)
- MQ will be responsible for Application Testing, Database testing and application integration to third party
- Support required during the go-live operations by Minfy
- AWS Directory services was used for Application authentication on AWS Infra between On-prim and AWS VPC
- OpenVPN was used with Google authenticator to establish connection between Individual users Devices and AWS VPC
- AWS Site to site VPN connection between Corp DC to AWS VPC
- Documents for PCI/SOC1 Compliance related from AWS during the third party audit by Minfy

Security Best Practices for this Migration

Extend Your Common Security Model

Conventional security and compliance concepts still apply in the cloud. Whether we're talking about existing apps migrating to the cloud or new ones being built there, they must be secured and good practices still apply. You can minimize the time and resources required to achieve this by leveraging the processes and technologies already in place within your organization.

Consolidate Identities

Identity silos expand your attack surface, increase overhead and lead to identity sprawl. Rather than create additional local AWS user accounts and Access Keys, use existing identities (e.g., Active Directory) and enable federated login. Federation enables you to grant an existing user identity within your enterprise directory the appropriate rights to access any AWS service. This avoids identity sprawl, issues with identity duplication and synchronization, and the need to provision and manage yet another identity silo.

Ensure Accountability

Shared privileged accounts (like Amazon ec2_user and Windows administrator accounts) are anonymous. To ensure accountability, it's important that users log in with their individual accounts vs. shared anonymous accounts and elevate privilege as required. Entitlements can be managed centrally from Active Directory, and roles and groups can be easily mapped to AWS roles. All user activities across a hybrid enterprise can then be tied back to unique individual users for 100% accountability. Privileged login sessions should be video recorded and all attempts to log in to AWS portals and Amazon EC2 instances as well as all privilege elevation attempts should be audited and recorded.

Least Privilege Access

When it comes to the AWS Management Console, AWS services, Amazon EC2 instances and access to hosted apps, users should be given the just enough privilege necessary to complete the task at hand. Centrify customers leverage their existing directory infrastructure to manage and audit the roles and rights that give each user the appropriate access at the AWS service level and at the Amazon EC2 Instance level. Any IT user or group from any directory service can be added as a member of a Centrify role, which is then mapped to an AWS role to assign granular rights in the AWS interface.

Audit Everything

Log and monitor authorized and unauthorized user sessions to Amazon EC2 instances. Admins can log in directly with individual accounts, or they can log into the shared password management portal and (if their role allows) log in remotely to an instance using their enterprise credentials. Activities can be audited via session-recording at the proxy or host level, but preferably at the host level to ensure visibility in the event a proxy is bypassed. Centrify Auditing & Reporting, AWS CloudTrails and CloudWatch can be used to help associate all activity to an individual, and for reporting On Privileged Activity and Access Rights.

MFA Everywhere

Highly sensitive actions may require additional user validation, the best practice is to use multi-factor authentication (MFA) everywhere. Even with the appropriate role, users must assure their identities with an out-of-band factor like a push notification to a pre-enrolled mobile device before certain actions can be performed. This can significantly increase

Minfy-Magnaquest Migration Use Case

confidence in identity assurance, preventing attackers using compromised credentials common in the latest cyberattacks. Implement MFA for AWS service management upon login and privilege elevation for Amazon EC2 instances, when checking out vaulted passwords and when accessing enterprise apps.