

Dibzi Achieved A Safe & Secure Environment By Migrating To AWS Cloud



Introduction

DIZBI is a digital product and services private limited company in Bengaluru, India. Dizbi is the technology arm of PDS Multinational Group, which has an annual turnover of 1.2 billion USD with its presence in 18 nations. Given Dizbi's rich technology experience in developing enterprise frameworks, processes, and excellent resources, it has enabled the digital transformation journey of many enterprises with the philosophy of design thinking and applied thought.

» AWS Services

AWS Workspaces, Directory Service, NAT Gateway, VPN, Config, S3, CloudWatch, CloudTrail, IAM

Business Need

The customer acquired a company known as "Collective Heads." Employees working under Collective Heads were also moved to work under Customer payroll.

While these new users need to work on new projects, the customer wanted to have a safe & secure environment so that data privacy & security rules are intact while these new users are added to the system. They also wanted minimal operational overhead in maintaining the system.

Below are the requirements from the customer:

- » A separate isolated and secure remote workplace solution & avoid users connecting to their on-premises workspaces.

- » When users need to work on development projects, they still need secure access to the applications/data deployed in the customer's own data center.
- » A highly secure and reliable solution that would keep their data safe & secure from any theft or loss.
- » A centralized identity management system is in place to track & manage access smoothly
- » The solution should also serve as a contingency plan for their business continuity in case their premises are not accessible due to some unavoidable reasons.

Solution Approach

Our AWS Certified Solutions Architects conducted detailed workshop sessions with the customer to understand their existing setup, challenges, and requirements. We also captured remote users' licensing and software requirements in the discovery.

The following solution approach was proposed and implemented with best practices and business continuity principles and then migrated their production workload to AWS.

- » AWS Workspaces was proposed as it is a highly reliable managed service with minimal operational overhead.
- » A separate network with a combination of VPC / Subnets was created as per the best practices.
- » All the workspaces were launched in private subnets & endpoints accessible through the Internet.
- » AWS & Customer Data Centre was connected using AWS site-to-site VPN tunnel for establishing connectivity required between AWS Workspaces & On-Prem Data/applications.

- » The workspaces were integrated with a self-managed Active Directory hosted on AWS EC2 for authentication with an AD connector.
- » Workspaces were also hardened according to the requirement of the customer.
- » Office & Anti-Virus packages were provided by the customer & included in the image to launch Workspaces.
- » Installation packages for other agent-based software required were also included in the image.
- » All traffic from the Internet has been routed through the site-to-site VPN tunnel to access the Internet and applications.
- » Restricted policies were applied to prevent any data movement between AWS Workspaces & User-machine.
- » Both web-based and client-based applications were configured as part of this setup.

Reaping Rewards

- » AWS workspaces solve customers' need for business continuity for all users.
- » With this solution, we were able to provide a secure and reliable remote workplace option for the user set separate from the existing setup.
- » AWS VPN connectivity between AWS & On-Prem data center helped AWS workspaces communicate with applications & data residing on-prem with low latency.
- » Data copy restrictions were applied from AWS Workspaces to users' machines to safeguard data from theft & loss.



+91 733 868 6644
 info@rapyder.com
 www.rapyder.com