TABLE OF CONTENTS

PROBLEM STATEMENT

In the ever-evolving realm of contemporary software development, the imperative for streamlined and automated deployment processes becomes increasingly crucial, especially within the intricate settings of Data Center (DC) and Disaster Recovery (DR) scenarios. The pursuit of accelerating release cycles and ensuring robust application reliability encounters formidable challenges arising from manual deployment intricacies, irregularities in infrastructure management, and the constraints of limited visibility.

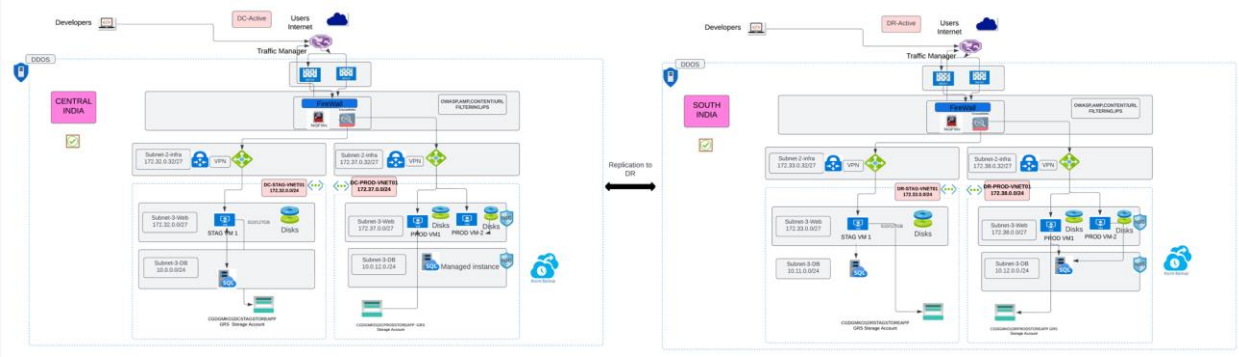
SOLUTION

Minfy has unveiled a comprehensive solution to address the intricacies of modern software development in Data Center (DC) and Disaster Recovery (DR) scenarios. This robust, end-to-end automated deployment workflow leverages key Azure services such as Traffic Manager, Application Gateway, Virtual Network Gateway connections, Virtual Machines (VMs), and Storage Accounts. These elements are strategically orchestrated to enhance fault tolerance, reliability, and security within both staging and production environments. DevSecOps practices are integrated through Azure Policy, Sentinel, Log Analytics Workspace, and Azure Defender for continuous monitoring, advanced threat

protection, and centralized log analysis. Shared dashboards within Azure Monitor provide consolidated views of key metrics and security insights.

- Establish separate Virtual Networks for staging and production environments in both DC and DR. This ensures network isolation and security.
- Deploy VMs within each environment to host your applications. Utilize availability sets or zones to enhance fault tolerance.
- Deploy Azure SQL Database Managed Instances connected with the virtual machines for a fully managed and scalable relational database solution.
- Set up Azure Storage Accounts to store application data. Enable replication between DC and DR for data redundancy.
- Establish secure Virtual Network Gateway connections between DC and DR environments to facilitate seamless data flow with other sites.
- Deploy Azure Application Gateway to manage and optimize the traffic to your applications. Utilize features like Web Application Firewall (WAF) for enhanced security.
- Implement Azure Traffic Managers to distribute incoming traffic across multiple regions (DC and DR) for high availability and fault tolerance.
- Implement Azure Sentinel for intelligent security analytics, threat hunting, and incident response across both environments.
- Implement Azure Monitor to collect telemetry data, providing insights into application performance and health.
- Leverage Azure Policy and Defender for cloud for policy-driven security management and continuous monitoring of security configurations.

ARCHITECTURE



OUTCOME

- By implementing this solution, you can establish a consistent, secure, and automated environment across both Data Center and Disaster Recovery scenarios, incorporating best practices for streamlined deployment processes and infrastructure management. Implementing DevSecOps practices through Azure Sentinel, Azure Defender, and Azure Monitor. Utilizing Azure services like Traffic Manager and Application Gateway for efficient load balancing and traffic management. Comprehensive monitoring with Azure Monitor and Log Analytics Workspace for effective troubleshooting and performance optimization.