UNIT 10 SEMINAR – DR SOLUTIONS DESIGN AND REVIEW

Vendor lock-in issues and mitigation strategies

Interoperability issues

Design of systems that are incompatible with software developed by other vendors

Implement a Multi-Cloud Strategy.

Portability Issues

The use of proprietary standards or closed architectures that lack interoperability with other applications

Build Portable Applications.

Standardization issue

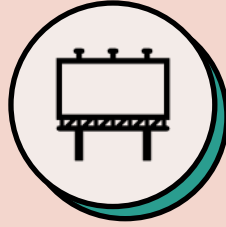Licensing of software under exclusive conditions

Retain Ownership of Data

# Security concerns with the modern cloud and how to mitigate them

Data breaches
Protecting data via encryption; and having a strong, well-tested incident response plan.
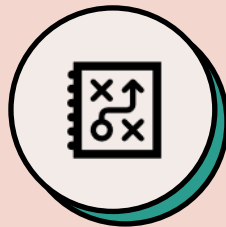
Insufficient identity, credential, access and key management
Two-factor authentication, removing unused credentials and access privileges, and employing central, programmatic key management.
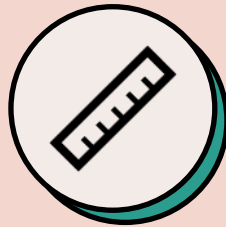
Insecure interfaces and APIs
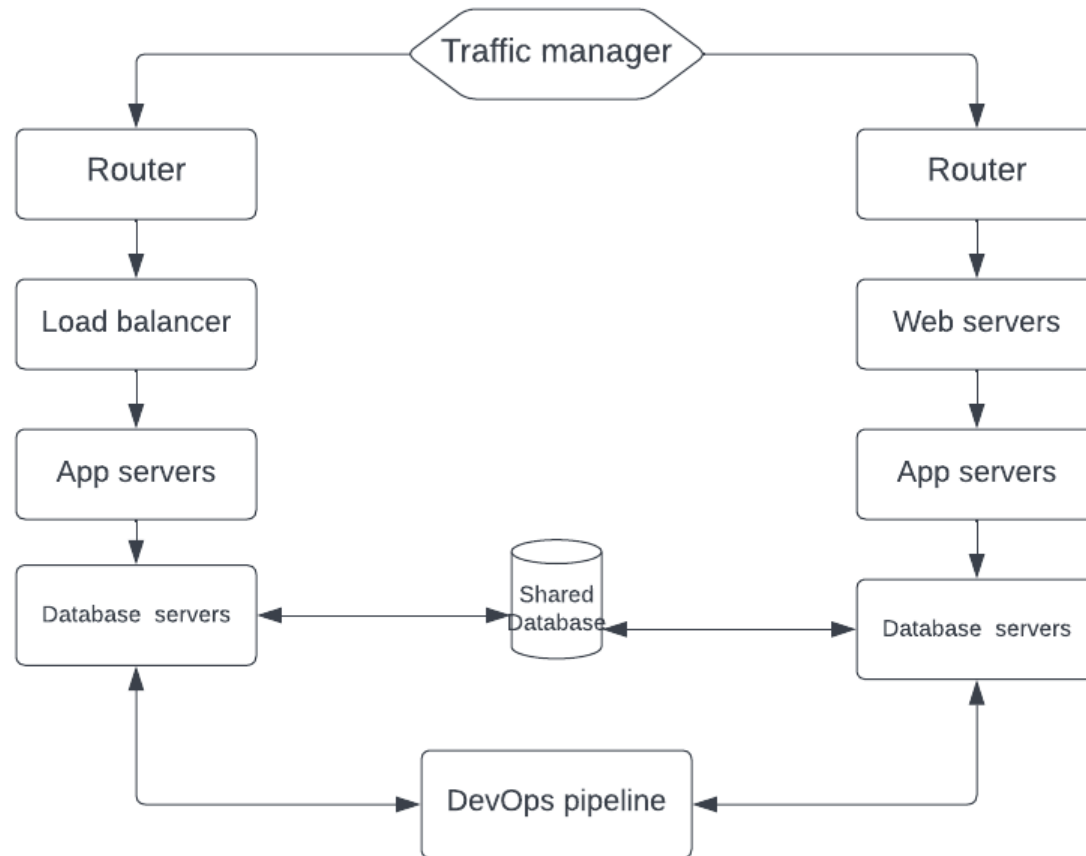Practicing good API hygiene and avoiding API key reuse

Malware infection
Abide by a zero-trust model and implement a threat detection solution.

Insider threats
Conducting security awareness training, fixing misconfigured cloud servers and restricting access to critical systems.
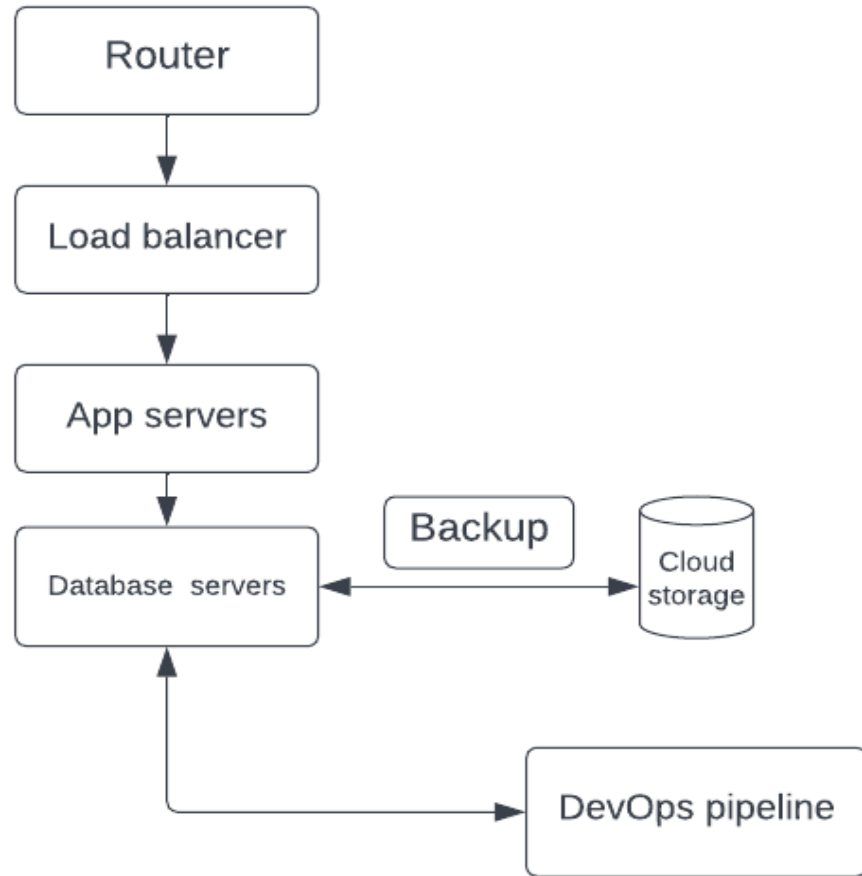
DR SOLUTION

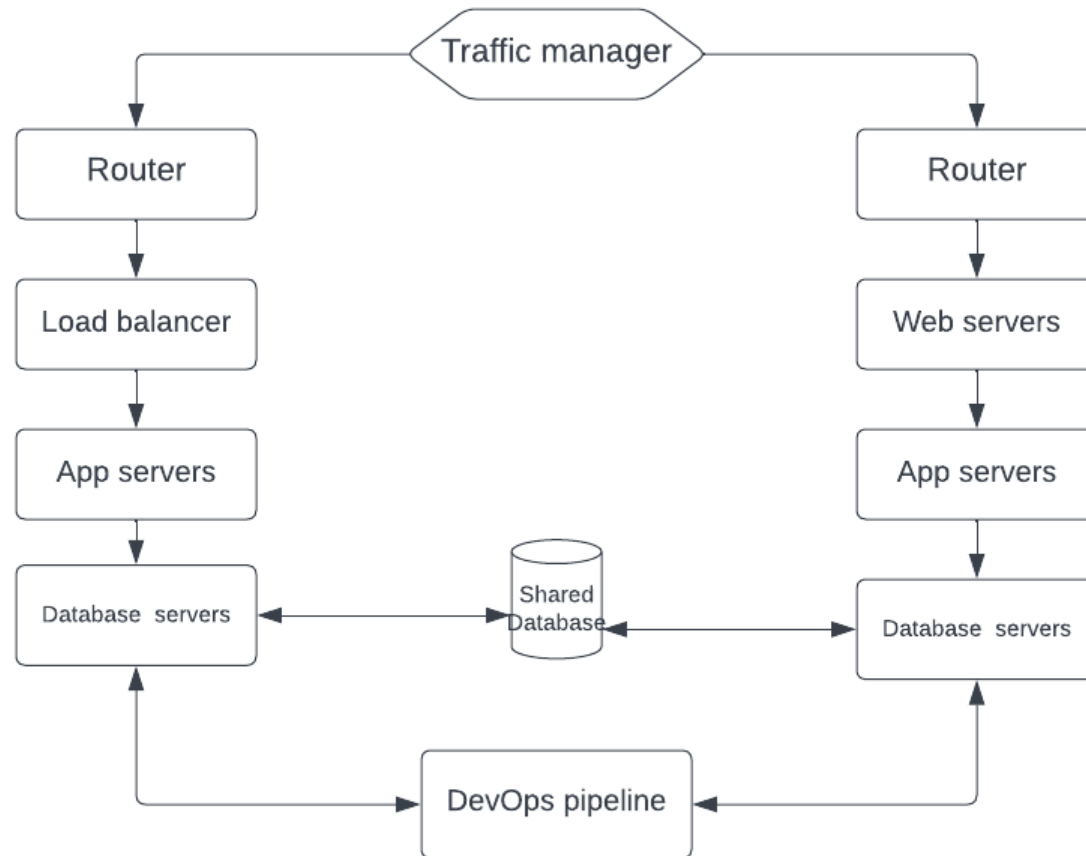RPO = 1 HR

RTO = 8 HR

WARM STANDBY

DR SOLUTION

RPO = 24 HR

RTO = 72 HR

ZONE REDUNDANT STORAGE

DR SOLUTION

RPO = 5 MIN

RTO = 1 HR

HOT STANDBY

References

Morrow et al (2021) Cloud Security Best Practices Derived from Mission Thread Analysis. *Software Engineering Institute*. Available from: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=551466

Opara-Martins et al (2014) Critical Review of Vendor Lock-in and Its Impact on Adoption of Cloud Computing. *Journal of Cloud Computing* Available from: https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-016-0054-z