

Unit 10 Seminar Preparation

Seminar 5: DR Solutions Design and Review

Please carry out this activity before joining the seminar this week. Your answers will be discussed during the seminar.

Activity

Part A

Read Opara-Martins et al (2014) and Morrow et al (2021) and answer the following questions:

1. What are some of the main vendor lock-in issues the authors identify? How would you mitigate them?
2. What are some of the security concerns with the modern cloud? How can these be mitigated?

Part B

Create a high-level diagram of a DR solution for each of the following requirements. They should be created in PowerPoint, and you should include a basic description of each design. **Be prepared to share and discuss your designs in this week's seminar.**

1. RPO= 1 hr; RTO= 8 hrs; high availability (HA) required.
2. RPO= 24 hrs; RTO = 72 hrs; HA NOT required.
3. RPO= 5 mins; RTO= 1 hr; HA required.

Add your answers to your e-portfolio and be prepared to discuss them at the seminar this week.

Part A

1. Opara-Martins et al (2014):

- Main vendor lock-in issues:
 - “having data locked in to one cloud provider
 - data breach and cyber attack
 - costly data migration or data conversion
 - failure to provide agreed service/meet service needs
 - lack of integration between various cloud networks
 - unexpected application re-engineering or business process change
 - processing incompatibility and conflicts causing disruption of service
 - inability to easily move data and applications in/out of cloud environment” (8)

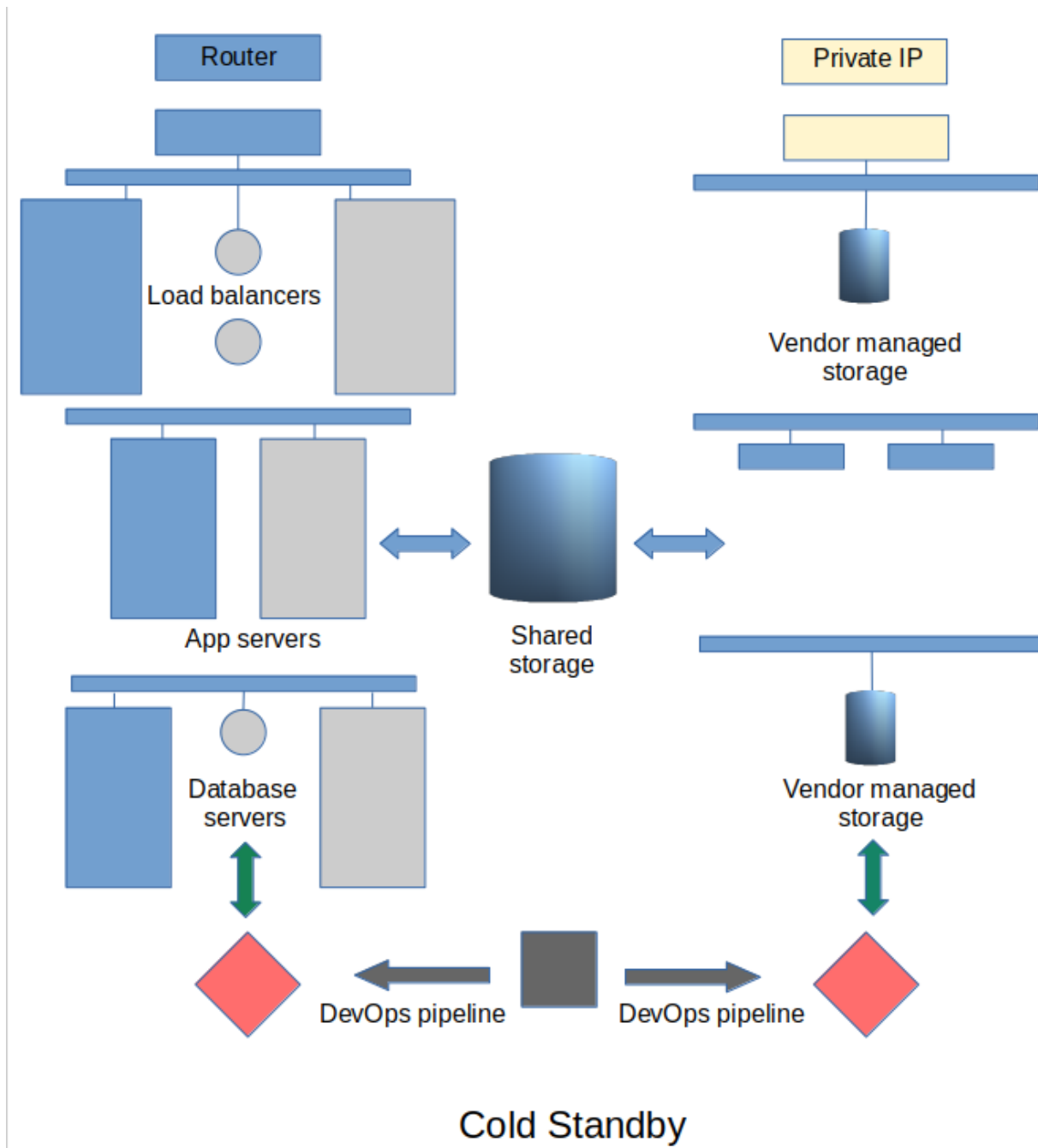
- Mitigations can include:
 - “using standard software components with industry proven interfaces
 - ensure application architectures and IT operations procedures that are not unique to a specific vendor platform
 - consideration for the use of open and published technologies (standardisation)
 - practice and conduct due diligence when hiring cloud providers
 - well-informed decision before selecting vendors and/or signing the cloud services contract
 - build perceived lock-in risks to initial risk assessment and mitigate by choosing a vendor with limited risks
 - involve legal terms and security professional when negotiating cloud providers contract terms and SLA
 - an open environment of continuous competition between providers in cloud services market” (10)

2. Morrow et al (2021):

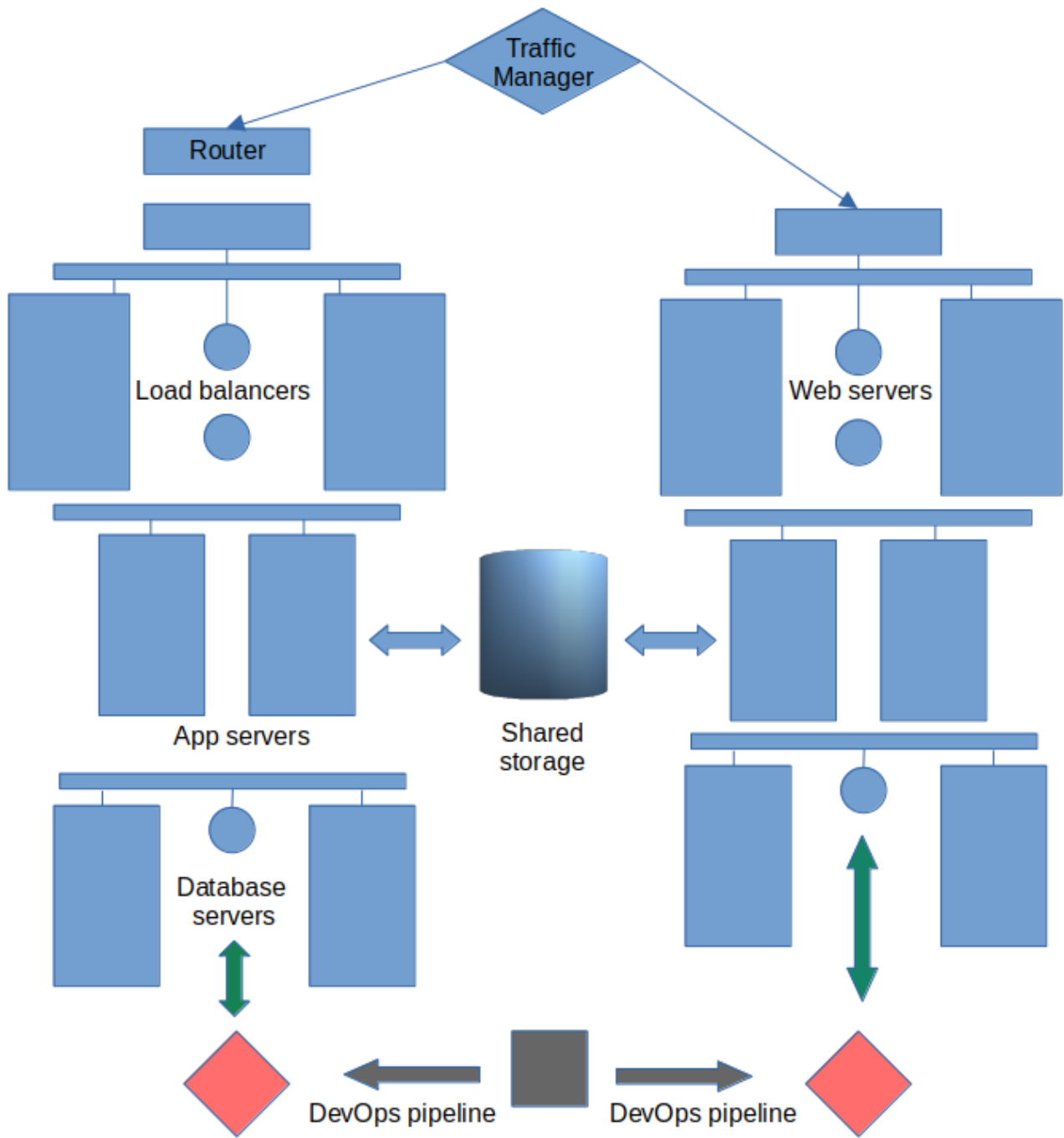
- Security concerns with the modern cloud can include:
 - unsecured storage services
 - AWS Simple Storage service
 - Compromised Sysadmin credentials
 - Deloitte email compromise
 - Accidental data loss
 - Amazon Elastic Block Storage (EBS) - .07%
 - Data and System Damage
 - Code Spaces – AWS privileged user credential compromised
 - Data breach
 - OneLogin – AWS keys
 - Ransomware
 - Using Cloud backups
 - Supply Chain attacks
 - SolarWinds – on-premise attack

Part B

1. RPO= 1 hr; RTO= 8 hrs; high availability (HA) required.



3. RPO= 5 mins; RTO= 1 hr; HA required.



Active-Active Standby

Resources:

Morrow, T., LaPiana, V., Faatz, D., Hueca, A. & Richmond, N. (2021) *Cloud Security Best Practices Derived from Mission Thread Analysis*. Carnegie-Mellon Univ Pittsburgh PA.

Opara-Martins, J., Sahandi, R., & Tian, F. (2014) Critical review of vendor lock-in and its impact on adoption of cloud computing. *In International Conference on Information Society (i-Society 2014)* (pp. 92-97). IEEE.