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?

   Some of the main vendor lock-in issues range from cost, being time consuming, lack of standards among the vendors, incompatible technology between the vendor and the organisation. Data stored with cloud vendors may be stored in their own format.

2. What are some of the security concerns with the modern cloud? How can these be mitigated?

   If the data is on premise or on the cloud the security concerns are still the same. There is always a concern for Data Breaches, insider threats, lack of staff training, password or security policy, Insecure API's or misconfigurations.

   To mitigate these threats a regular review would be required with the vendor and the organisation to ensure

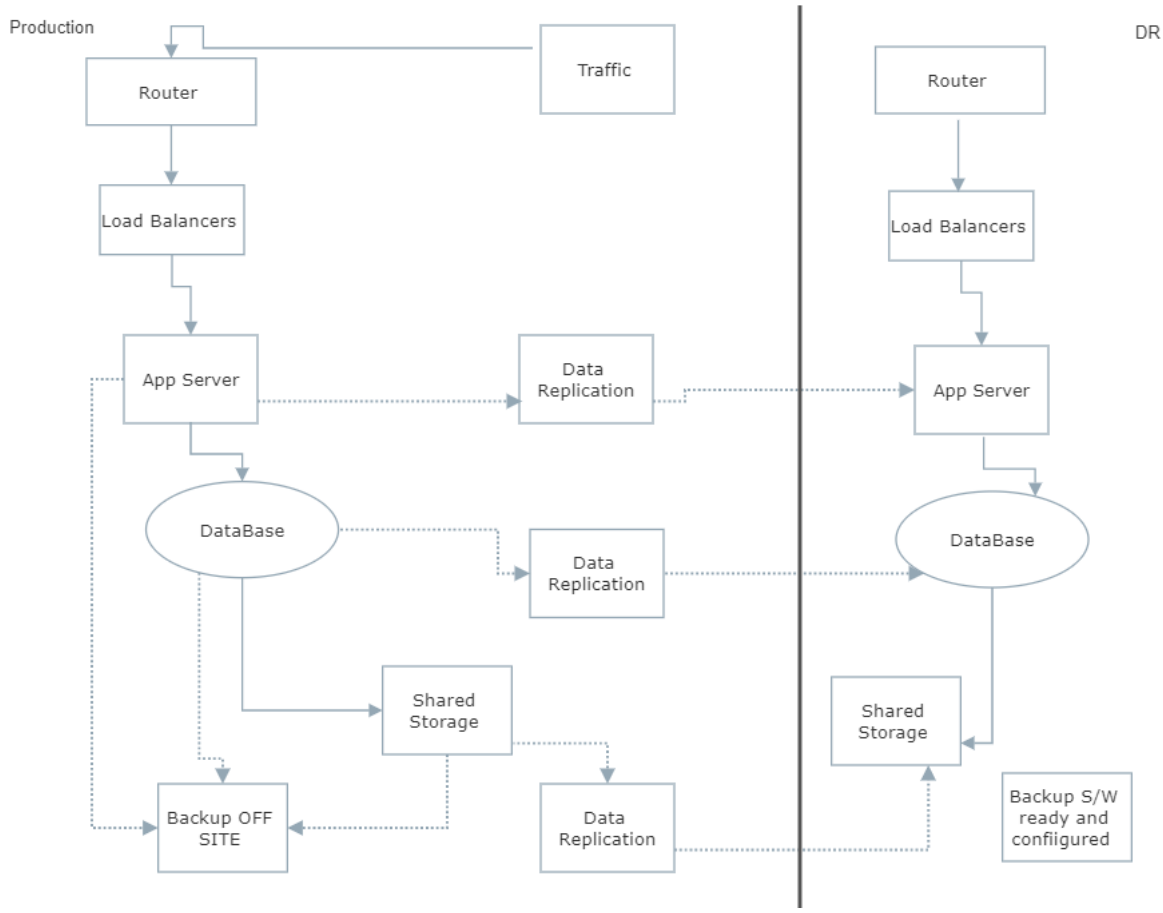
   - Password policy is in place
   - Access controls are in place on who can see and modify the data
   - Ensure both parties have staff training on security.
   - Ensure Organisation are restricted from where and how they can log into the cloud
   - Ensure the vendor has configuration in place that only allows certain two factor authentication is place
   - Ensure that all default password are changed.
   - Ensure logging is in place and reviewd
   - Intrusion detection are in place and both parties are alerted

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.**

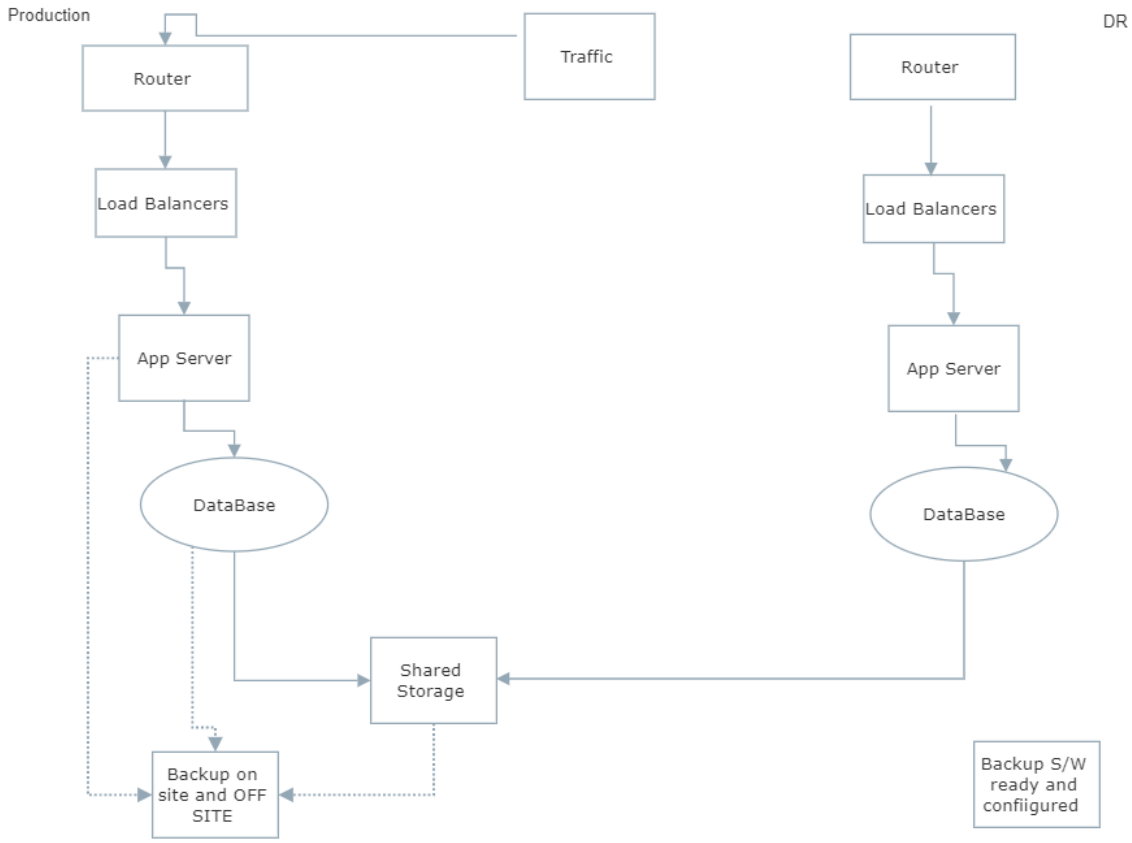
1. RPO= 1 hr; RTO= 8 hrs; high availability (HA) required.

The Diagram below shows an environment where the system is running in Production only and Disaster Recovery site is set up and ready to be activated in case of a Disaster. This is to ensure we meet the SLA of Recovery Point Objective of 1 hour. We have ensured that each component has a backup in case of any hardware issue, in which case DR can be activated if RTO SLA is to be breached. All the data has real time replication back to a stand by servers and also ensure the data is kept on tape and is sent off site. This is to ensure that two copies of the backup are available. Full back up will be performed on the weekend, Incremental back up during the week.



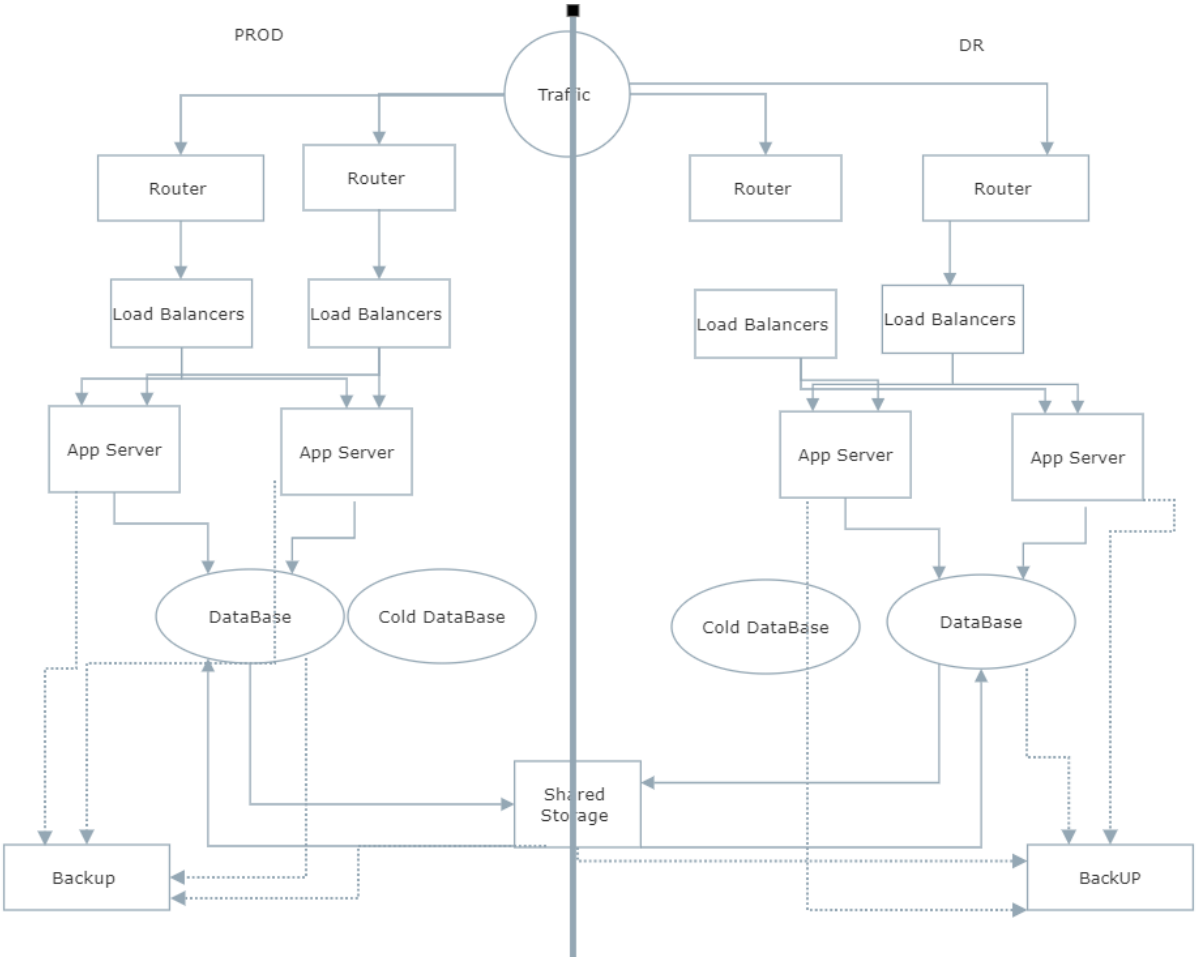
2. RPO= 24 hrs; RTO = 72 hrs; HA NOT required.

The Diagram below shows an environment where the system is running only in Production. Disaster Recovery has been set up but is in standby mode. The dotted lines represent backups being performed, we have ensured that each component has a data backup and there are two copies one kept on- site and one kept offsite. The backups performed will be a full back up over the weekend and incremental backups during the week. The offsite location would have be located a distance of 20 miles from both sites.



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

The Diagram below shows an environment where the system is running in both Production and Disaster Recovery. This is to ensure we meet the SLA of Recovery Point Objective of 5 minutes. We have ensured that each component has a backup in case of any hardware issue. The Database has replication back to a stand by Database in a different Datacentre in case we have issues. The dotted lines represent backups being performed, which will follow a full back up over the weekend and incremental backups during the week, This ensure the data is kept in two separate locations if we need to ever restore.


PROD
DR
Traffic
Router
Router
Router
Router
Load Balancers
Load Balancers
Load Balancers
Load Balancers
App Server
App Server
App Server
App Server
DataBase
Cold DataBase
Cold DataBase
DataBase
Shared Storage
Backup
BackUP