10 Seminar Preparation

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. What are some of the main vendor lock-in issues the authors identify? How would you mitigate them?

   Answer : Problems with being "locked in" to a particular vendor can originate from a wide variety of sources, such as technologies, contracts, service level agreements (SLA), and the implementation of vendor-specific technological solutions.

   Following are some mitigation for vendor lock-in :

	Vendor Lock-In Issues	Mitigation
1	Compatibility issues	• Perform proof of concepts with multi-cloud • Choose current technologies and applications
2	Vendor Agreements	• Validate SLA for capacity, availability, and exit • Negotiate the agreements/contracts which favours to company
3	Multi-Cloud approach	• Choose multi-cloud to avoid vendor goes out of business, hardware ceased for government, failures/outages • Keep backups and encryption keys outside the cloud

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

- Self-service portal is both benefit and risk
    - Administrator can provision resources and unattended end up paying
    - Insider advisory can enable unauthorized access

    Solution:

    1. Role based access control with Just in time access (JIT)
    2. Change control
- Lack of security control
    - By default cloud provider don't provide any security control, it the customer responsible to secure the data

    Solution:

    - Tenant level policy, adding firewall log every event and forward to Security information and event management (SIEM) and monitor for any anomaly activity
- Insecure Application programming interface (API)
    - Adversaries can exploit insecure APIs to compromise or steal sensitive and private data

  Solution:

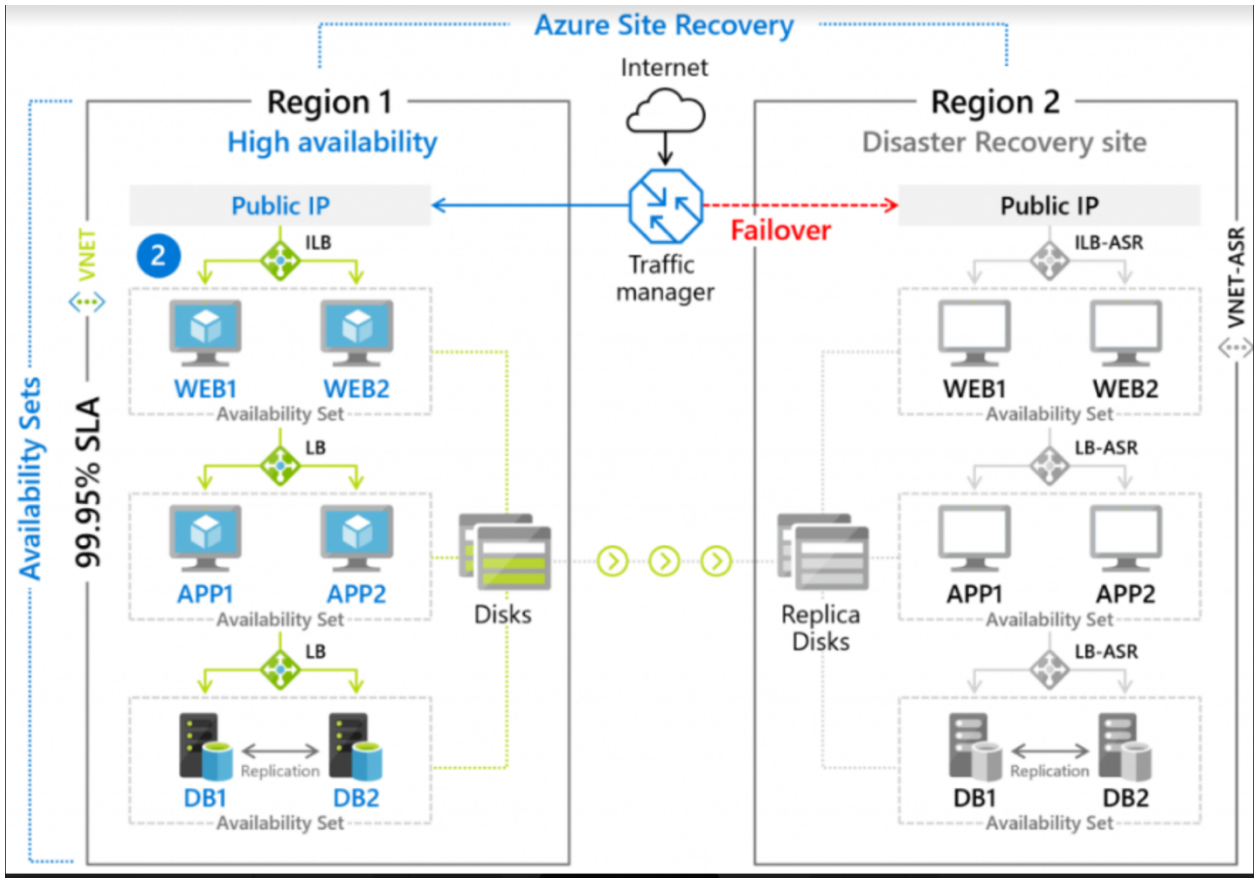
    - Install web application firewall
    - Follow the security best practices while developing the API
    - Ensure the security while using the open-source solution

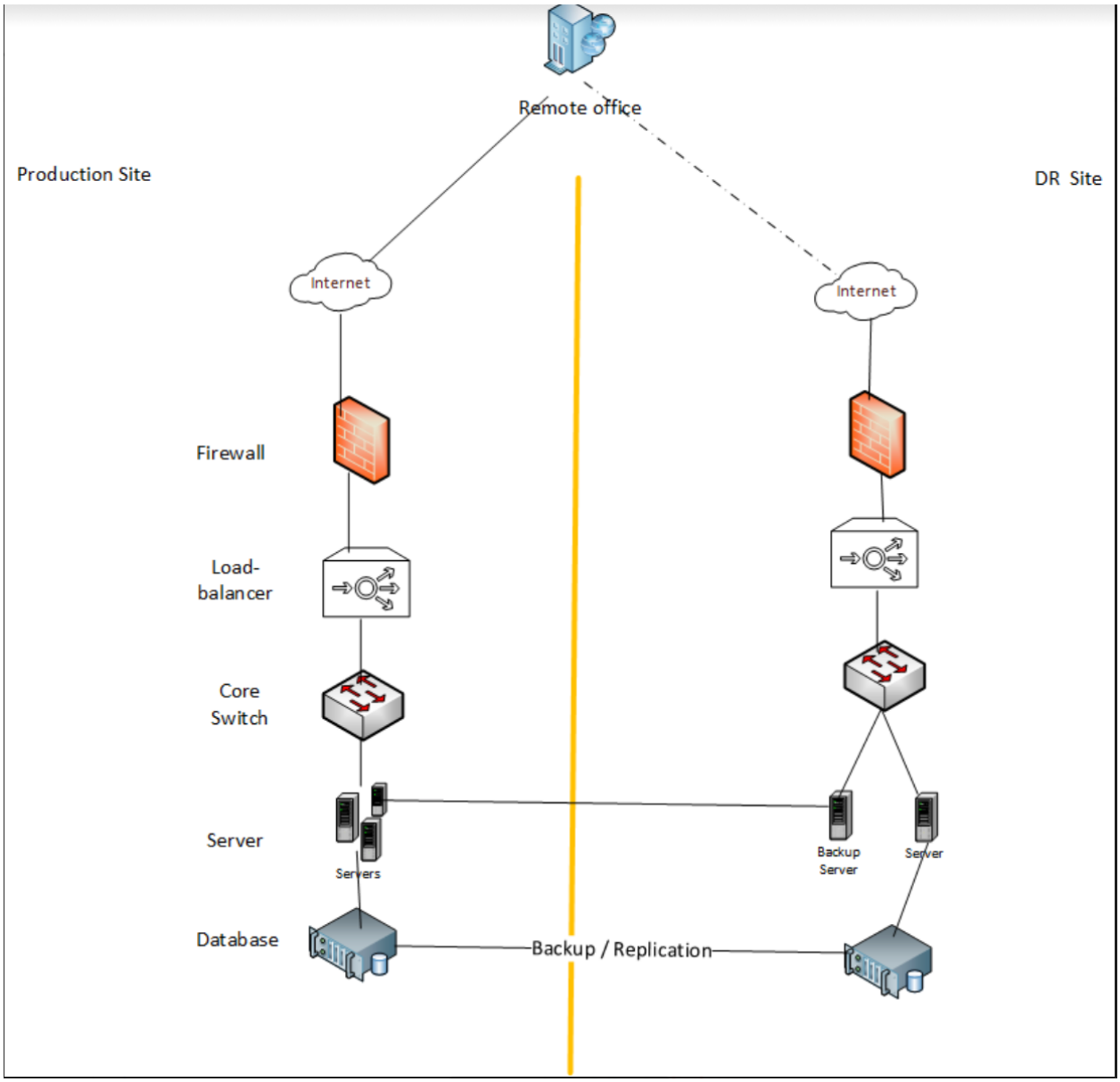
High Level Diagram

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.

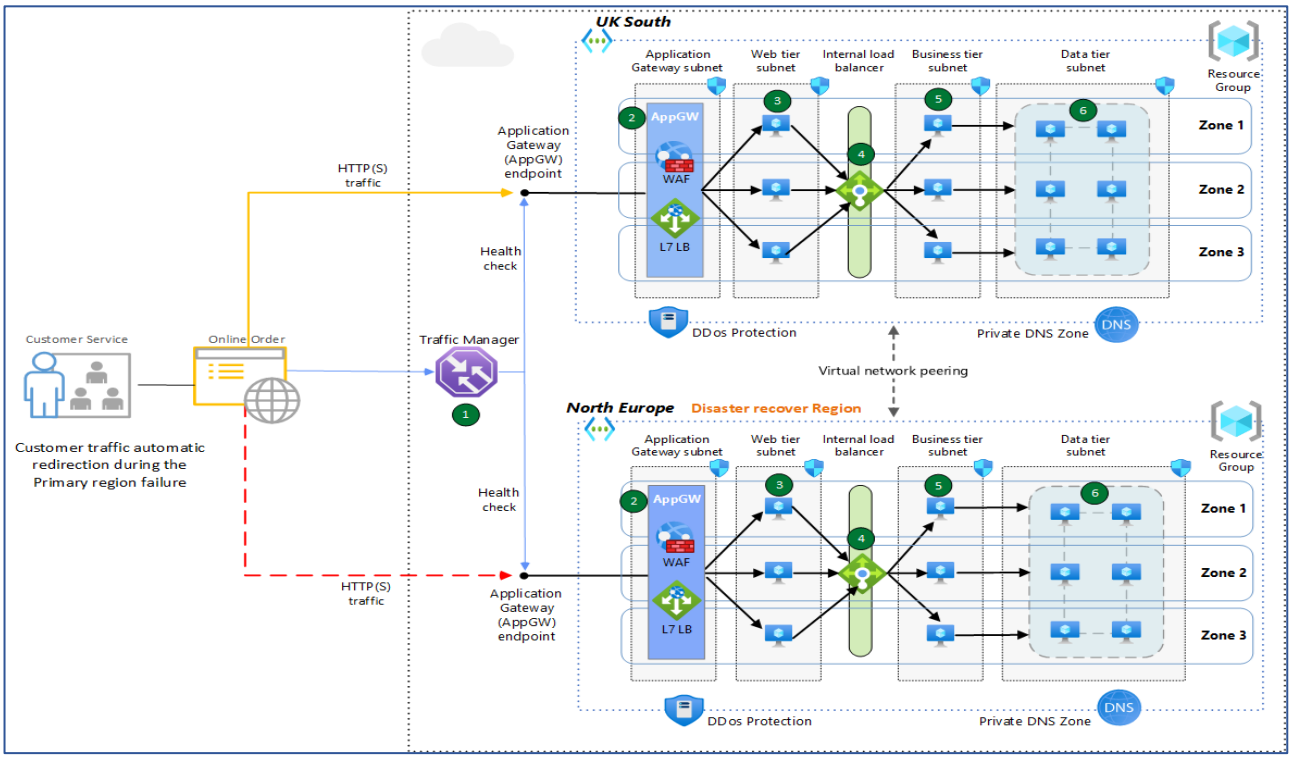
1. RPO= 1 hr; RTO= 8 hrs; high availability (HA) required.

- All servers are running on Primary region, only backups are kept at secondary region
- HA Servers will be installed in production site
- To cover the RPO, database will be replicated using Async method
- All the servers will be installed from the backup


Azure Site Recovery
Internet
Region 1
High availability
Region 2
Disaster Recovery site
Public IP
Public IP
Traffic manager
Failover
VNET
2
ILB
WEB1
WEB2
Availability Set
LB
APP1
APP2
Availability Set
LB
Replication
DB1
DB2
Availability Set
Availability Sets
99.95% SLA
Disks
Replica Disks
ILB-ASR
WEB1
WEB2
Availability Set
LB-ASR
APP1
APP2
Availability Set
LB-ASR
Replication
DB1
DB2
Availability Set
VNET-ASR



- Single server running on the production site
- Backup are pushed to the DR-Site
- Database will be replicated to the dr site
- In case of any failure, the server will be installed from the backup



To cover the RPO of 5 min, database will be synchronous mode and the log files will be written to the database. There will HA pair for every services. So it can address any local failures. Automatic fallback and automatic failure will be achieved with the proposed HLD. User traffic will be automatically redirected based on the service availability. The picture

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