DISASTER RECOVERY

Client Requirements

- The online shop needs to be available 24/7/365
- with a less than 1 minute changeover window should DR need to be invoked.
- the business cannot afford to lose more than 1 minute of data.
- Recommend the platform that should be chosen to host the solution and to provide advice on vendor lock-in.

Business Continuity (BC) planning is, as its name suggests, mostly concerned with plans and approaches that can be deployed to allow a business to continue to run in the event of a major disaster or incident – such as a fire, flood, cyberattack or a global pandemic.

The BC plan deals with plans and procedures to ensure that the business and its staff can continue to operate in as close to normal a way as possible.

Disaster Recovery (DR)

Disaster recovery, on the other hand, is more concerned with ensuring that the IT infrastructure that supports the business and staff is available when the BC is invoked – as such it is part of the overall BC plan.

There are two factors in particular that drive the DR plan and design:

- The Recovery Time Objective (RTO)
- The Recovery Point Objective (RPO)

DR solutions can vary in scope and complexity by a vast amount – anything from a basic backup tape to a full hot standby system can constitute a DR solution – which is chosen is driven by the RTO, RPO and of course the cost requirements. From the client requirement specified above, it can be deduced that the RTO is 1 minute and the RPO is not more than 1 minute.

The ISO 22301 standard for Business Continuity recommends that a business:

- Undergoes a risk assessment;
- Undergoes a business impact analysis;
- Selects a BC strategy;
- Creates and implement policies and procedures;
- Performs regular tests to ensure that the strategy is appropriate and;
- Ensures that plans operate as expected.

Adhering to the standard gives customers trust and confidence in a company, knowing that it has plans in place to deal with emergency situations and that it will be able to continue to do business even if a disaster should occur.

A Disaster Recovery plan is an integral part of any BC plan and can be analyzed thus:

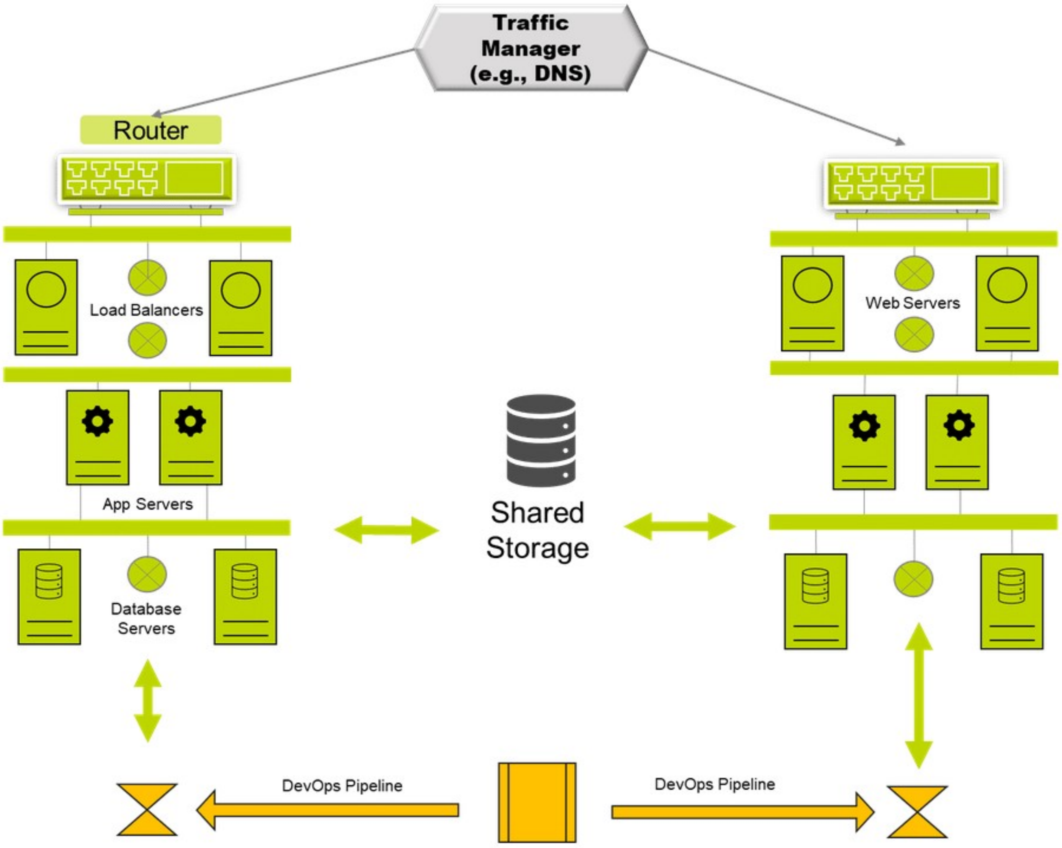

Fig: Active-Active Disaster Recovery Solution Model

DR Strategy

The figure above employs an active-active solution, which suggests that there should be two systems running concurrently - ideally in different regions (or one on premise and one in the cloud). There should be a traffic manager [TM] managing the front end traffic and monitoring both systems to detect if either fails and automatically switch over to the second without disruption to the user. Code will be deployed to both sites simultaneously – although there is an option to use a blue-green deployment strategy where all users are switched over to one site to test the new code, while the second site is held at the older version in case there are user errors with the new code.

Databases should be configured as AOAG groups or use CosmosDB in multi-master mode. Any other data should be copied synchronously between sites. Ideally applications should be deployed in stateless containers and all user-state managed via the database.

The downside of this approach is cost in that the business will be paying for two full systems, and potentially only using one. However if applications are configured to be stateless there is no reason why both sites cannot be used simultaneously – the TM can easily allocate users to both systems on a round robin basis.

The system is highly recoverable due to the fact that both sites run identical systems and if one site fails all users can be switched to the other.

The table below analyzes the efficiency of the active – active approach as a suitable DR strategy for the system under review:

CATEGORY	PROS	CONS	CAVEATS
Availability	Active-active provides immediate, tested always on service.	Cost of additional environments.	Applications must be designed to be active-active ready.
Recoverability	Synchronous copies means fast, highly recoverable service.	Recoverability by definition in paired region.	Need additional solution to cope with data corruption - sync copies will just copy corruption.
Resilience	Always on solution means that every component is replicated and always available - may reduce cost by not duplicating within region.	May require switch over to alt region.	Loss of a region will affect resilience; doesn't solve corruption issue.
Data Corruption	Small replication delays may help address corruption risks.	Replication delays means data loss and higher RPO.	Needs careful tuning to mitigate corruption and avoid data loss.
Regions	Single vendor may make replication and switching easier.	Vendor errors may affect ALL regions - DR will not help.	Consider multi-vendor solution - more complex, possibly higher cost.

Disaster Recovery (DR) Solution can be summarized as follows:

1. Data Backup and Replication:
   - Based on the client’s requirement, the system should implement real-time data backup and replication to ensure that no more than 1 minute of data is lost. This can be achieved by using technologies like continuous data protection (CDP) or synchronous data replication.
   - Cloudification over on-premise data handling; using multiple suppliers to eliminate data lock-in, design lock-in, and faults from having a single supplier. Subscribing to multiple suppliers also ensures reliability
2. Geographically Redundant Data Centers:
   - All applications and data used will be hosted in geographically redundant data centers to minimize the risk of a disaster affecting both locations simultaneously.
3. Load Balancers and Failover:
   - Utilize load balancers and automatic failover mechanisms to ensure high availability. This will help in achieving the less than 1-minute changeover window if DR needs to be invoked.
4. Regular Testing:

    - Regular testing of the Disaster Recovery plan will be done to ensure it functions as expected. Both planned and unplanned tests will be carried out to assess the readiness of the system.

5. Data Encryption:

   The system will also Implement strong data encryption and security measures to protect sensitive information during data replication and storage.

6. Off-Site Backups:
    - So as to safeguard data in case of a major disaster that affects the primary and secondary data centers, we can take advantage of off-site backups.

Platform Selection:

When choosing a platform to host the DR solution, the following factors should be considered:

1. Cloud Service Providers:
    - Cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP) should be explored. These providers offer extensive infrastructure and DR services.
2. Hybrid Approach:
    - A hybrid approach can also be considered by utilizing a combination of on-premises infrastructure and cloud services. This provides flexibility and redundancy.
3. Data Center Providers:
    - If cloud services (which are preferred) are not suitable or in line with budgetary plans, data center providers that offer colocation services, which allow you to host your own infrastructure in their facilities can be explored.
4. Service Level Agreements (SLAs):
    - It is also important to evaluate the SLAs provided by potential platform providers, to ensure they meet the 24/7/365 availability and less than 1-minute changeover window requirements.

Addressing Vendor Lock-In:

Vendor lock-in can be a concern when using third-party platforms. To mitigate this risk:

1. Multi-Cloud Strategy:
    - The recovery system should adopt a multi-cloud strategy, spreading the data services and applications across multiple cloud providers. This reduces dependence on a single vendor and ensures reliability.
2. Standardized Interfaces:
    - The system should ensure that all applications and services use standardized interfaces and APIs. This makes it easier to migrate between platforms if necessary.

3. Data Portability:
    - Keep data portability in mind. This is to ensure data can be easily transferred from one platform to another.
4. Vendor-Neutral Tools:
    - Where possible, vendor-neutral management and orchestration tools should be used, to maintain flexibility in managing services and resources.
5. Regular Evaluation:
    - So as to keep up with current market competition, it is important to periodically evaluate the performance and cost-effectiveness of your chosen platform to determine if a change is needed.

REFERENCES

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.

Alhazmi, O. & Malaiya, Y. (2013) Evaluating Disaster Recovery Plans using the Cloud. *2013 Proceedings Annual Reliability and Maintainability Symposium* (RAMS) 1(1): 1-6

Andrade, E., Nogueira, B., Matos, R., Callou, G. & Maciel, P. (2017) Availability modeling and analysis of a disaster-recovery-as-a-service solution. *Computing*, 99(10), pp.929–954

Olson, D.L. & Desheng D.W (2020) *Enterprise risk management models*. Berlin, Germany: Springer.