Seminar preparation unit 10 Practical Applications and Issues in DR Implementations

Workshop Activity

Read Sutton (2021) and Popov, Lyon and Hollcroft (2022).

In this unit we shall:

- Discuss the impact of RPO and RTO values on DR solutions.
- Examine some typical system solutions to meet the various standby requirements.
- Describe the limitations of the proposed solutions.

On completion of this unit you will be able to:

- Design a solution that will meet a set of RPO and RTO requirements.
- Describe the advantages and disadvantages of DRaaS.
- Discuss the challenges with vendor lock-in, resilience and (network) security.

General:

- RPO (Recovery Point Objective): How much data loss is tolerable (measured in time).
- RTO (Recovery Time Objective): How quickly systems must be back online after disruption

Non- critical system	**Low criticality system**	**Medium criticality system**	**Highly critical system**
Target RTO > 48hr Target RPO > 24hr.	Target RTO > 12hr Target RPO > 1hr.	Target RTO > 6hr Target RPO > 15 mins	Target RTO < 1hr Target RPO < 1m.
Backup restore	Cold Standby	Active-passive / warm standby systems	Active – active solution / hot standby
Simple backup and restore solution, non-automated	Backups to tape/disk/cloud	More frequent incremental backups or asynchronous replication	Real-time replication, clustering, or synchronous mirroring.
	Cost: low.	Cost: moderate.	Cost: high.

DR Solution	Description
Cold Standby (Cold site)	• An empty or minimally equipped site (building, power, networking, maybe basic hardware). • Organisation must bring in servers, restore data from backups, and configure systems. • **RPO/RTO: High** (long recovery times, significant data loss possible). • Cheapest option. • Suitable for non-critical systems where downtime is tolerable.
Warm Standby (Warm site)	• A partially prepared site with some hardware and systems pre-installed. • Systems require some setup, data restoration, and configuration before going live. • **RPO/RTO: Medium** (moderate downtime and data loss). • More expensive than cold, less than hot. • Suitable for systems that are important but not absolutely critical.
Hot Standby (Hot site)	• A fully equipped, real-time mirrored system that can take over almost immediately. • Automated failover, minimal human intervention. • **RPO/RTO: Low to near zero** (almost no downtime or data loss). • Most expensive, requires real-time replication and constant maintenance. • Mission-critical systems where downtime or data loss is unacceptable (e.g., healthcare, banking).
Cloud-Based DR (DRaaS – Disaster Recovery as a Service)	• Recovery solutions hosted in the cloud, often using virtualisation. • Failover to cloud infrastructure, with backups or live replication. • **RPO/RTO: Varies** (can be configured from near-zero to longer times depending on service level). • Flexible costs. Pay-as-you-go, often cheaper than running a hot site in-house. • Especially for SMEs.
Hybrid Cloud (Private + public mix)	• A combination of private cloud (on-premises or dedicated) and public cloud resources, often chosen for reasons of compliance (e.g. data residency) and cost optimisation. • Critical data and applications may be hosted in a private cloud for security and compliance and non-critical workloads to the public cloud for scalability and cost savings. In a disaster, workloads can fail over between the two environments. • **RPO/RTO: Flexible.** often slightly higher than pure hot standby because synchronisation across environments adds complexity, but can be configured for low values.

	• **Cost:** Moderate to high. More expensive than single-cloud solutions (managing two infrastructures), but potentially cheaper than a full hot site.
	• **Impact of RTO/RPO:**
	  ○ **Low RPO/RTO:** Requires advanced orchestration, automated replication across both environments, and real-time failover (similar to hot standby costs/complexity).
	  ○ **Higher RPO/RTO:** Hybrid setup can prioritise critical systems for rapid recovery in the private cloud while allowing less critical systems to be restored more slowly from the public cloud.
	• For organisations with regulatory obligations but who also want the scalability and resilience of cloud for non-sensitive workloads.

	RPO	**RTO**	**Comment**
Lower values	Less data loss, requiring real-time replication and frequent backups.	Faster recovery solutions, typically involving hot standby systems and automated failover mechanisms	Lower RPO/RTO values → faster recovery, less data loss → higher cost and complexity.
Higher values	More acceptable data loss, allowing less frequent backups or manual restoration.	Slower recovery solutions, typically involving cold standby or manual failover approaches.	Higher RPO/RTO values: slower recovery and more acceptable data loss, leading to lower cost and simpler recovery solutions (e.g. cold standby, manual failover).

Advantages DRaas	**Disadvantages DRaas**
• Pay-as-you-go or subscription pricing models are cheaper than maintaining a physical hot site. • Resources can be scaled up/down on demand. • Faster deployment. Cloud-based failover reduces setup time compared with on-premises DR. • Cloud recovery environments can be accessed remotely from anywhere. • Many DRaaS platforms offer automated failover and recovery orchestration, reducing downtime. • Easier and cheaper to test	• Recovery depends heavily on internet bandwidth and latency. • long-term subscription fees may exceed the cost of in-house DR for large enterprises. • Shared responsibility: still need to ensure correct configuration, monitoring, and compliance • Regulatory issues: Sensitive data may be restricted from leaving certain jurisdictions • Complexity of integration with other applications • Vendor Lock-in

Challenges with vendor lock-in, resilience and (network) security

Vendor lock-in:

- Many DRaaS providers use proprietary formats, APIs, or configurations.
- Moving workloads to a new provider can be expensive and time-consuming.
- Limits flexibility and can trap organisations in suboptimal contracts.
- Solution: hybrid cloud models reduce dependency on one provider.

Resilience:

- if the provider suffers a disruption or failure, access may be lost to backup/recovery service
- Solution: hybrid cloud models reduce dependency on one provider.

Network Security:

- DRaaS relies on continuous data replication over the internet or private networks. Risk of data interception, misconfiguration, or insufficient encryption.
- Solution: Use of strong encryption in transit and at rest, secure VPNs or private links for replication, Network monitoring and regular penetration testing.

Sutton (2021):

- Organisations must align their recovery strategy with their risk appetite; higher resilience and shorter recovery objectives dramatically increase costs.
- Each increment of higher availability raises cost disproportionately
- Standby Solutions: Cold, warm, and hot standby as core DR options, ranging from low-cost/slow recovery to high-cost/instant failover.
- Information risk management is inseparable from business continuity.
- Disaster recovery should not be treated in isolation but as part of wider information risk and continuity planning.

Popov, Lyon and Hollcroft (2022):

- DR and continuity strategies should be grounded in risk assessment, hazard analysis, and business impact analysis (BIA).
- Recovery measures (e.g. RPO/RTO) must be as low as reasonably practicable (ALARP). Recovery objectives must be proportionate to business risk tolerance and available resources.
- Disaster Recovery (DR) and Business Continuity (BC) should not be handled in an ad-hoc way. Organisations should follow recognised international standards and frameworks (e.g. ISO 22301, NFPA 1600) to ensure structured, auditable approaches.

Shared ideas:

Both Sutton and Popov et al. emphasise that RPO and RTO (even if not named directly by Popov, Lyon and Hollcroft) are business decisions. They must balance:

- Criticality of systems

- Acceptable risk exposure
- Cost and complexity of solutions

References

Popov, G., (2022) *Risk assessment : a practical guide to assessing operational risks*. Second edition. Hoboken, New Jersey: Wiley.

Sutton, D. (2021) *Information risk management : a practitioner's guide*. 2nd ed. England: BCS Learning & Development Limited.