Assignment - Designing a Disaster Recovery Plan

Keegan R. Heaton

University of Advancing Technology

NTS - 366 Cloud Security

Aaron Jones

8/12/2024

1. Disaster Recovery Plan

a. What is a Disaster Recovery Plan and why is it Important?

Disaster recovery planning is critical to keeping businesses safe in case of dangerous events. A disaster recovery plan refers to the lined procedures that an organization ought to follow when recovering from such incidents like natural disasters, cyber attacks, or even system failures.(Yasar et al., 2024) This type of planning becomes very important in the present digital world, where even a minute of downtime can disrupt operations and result in heavy financial losses.

DRP, an acronym for Disaster Recovery Plan, will ensure that business operations are minimized when a disaster causes a disruption. A well-structured plan enables an organization to restore key functions in the fastest possible time so business can continue. This is important because organizations incur heavy losses during such downtimes. As such, fast recovery is essential for protecting every business's bottom line.

Many organizations also have some legal and compliance requirements for a disaster recovery plan. In the event of non-compliance, severe penalties can be incurred, along with damage to their reputation. A good DRP will also help in compliance and, along with that, maintain customer satisfaction through the assurance of the availability of services. Furthermore, the quick restoration of services guarantees little damage to their brand.

Finally, disaster recovery planning is a proactive approach toward the management of risk. In each case, it takes into consideration possible risks and vulnerabilities in order to appropriately prepare an organization for various disruptions. Moving forward, in a fast-changing technological world, advanced data protection and recovery techniques have to be

employed through DRP in order to guarantee operations within the fast paced IT world. Basically, an efficient recovery plan is significant for an organization so they can continue getting customer support. To do so, they must have a respect for data privacy, or they may face the wicked face of the law.

2. Comparative Analysis of Cloud, On-premises, and Hybrid Disaster Recovery Plans

Cloud-based disaster recovery solutions are highly scalable and flexible. They allow an organization to modify the resources assigned as necessary to meet the constantly changing workloads and ensure rapid recovery times. These are cost-effective in the sense that companies can use DRaaS (an acronym for Disaster Recovery as a Service)(CBTS, 2024) and, therefore, pay only for the capacity they used. Also, cloud solutions typically provide geographic redundancy through data replication across multiple regions, very important in maintaining data availability in case of regional disasters. (Gralewski, 2021)

However, cloud-based disaster recovery is complex and requires careful planning to ensure that disaster recovery capabilities are integrated effectively. You also have to plan for Security and compliance. Organizations will need to ensure that cloud providers can meet their specific security and compliance requirements, which prove quite difficult because of the shared responsibility model inherent in cloud services.(Lovett, 2023)

On-premises disaster recovery options will give the organization full control over the Disaster Recovery process and infrastructure. This allows organizations to tailor solutions for their specific needs. This further enhances compliance with data sovereignty laws and

regulations, which might be very crucial in certain cases when dealing with industries that require information to be located within strict geographical locations.

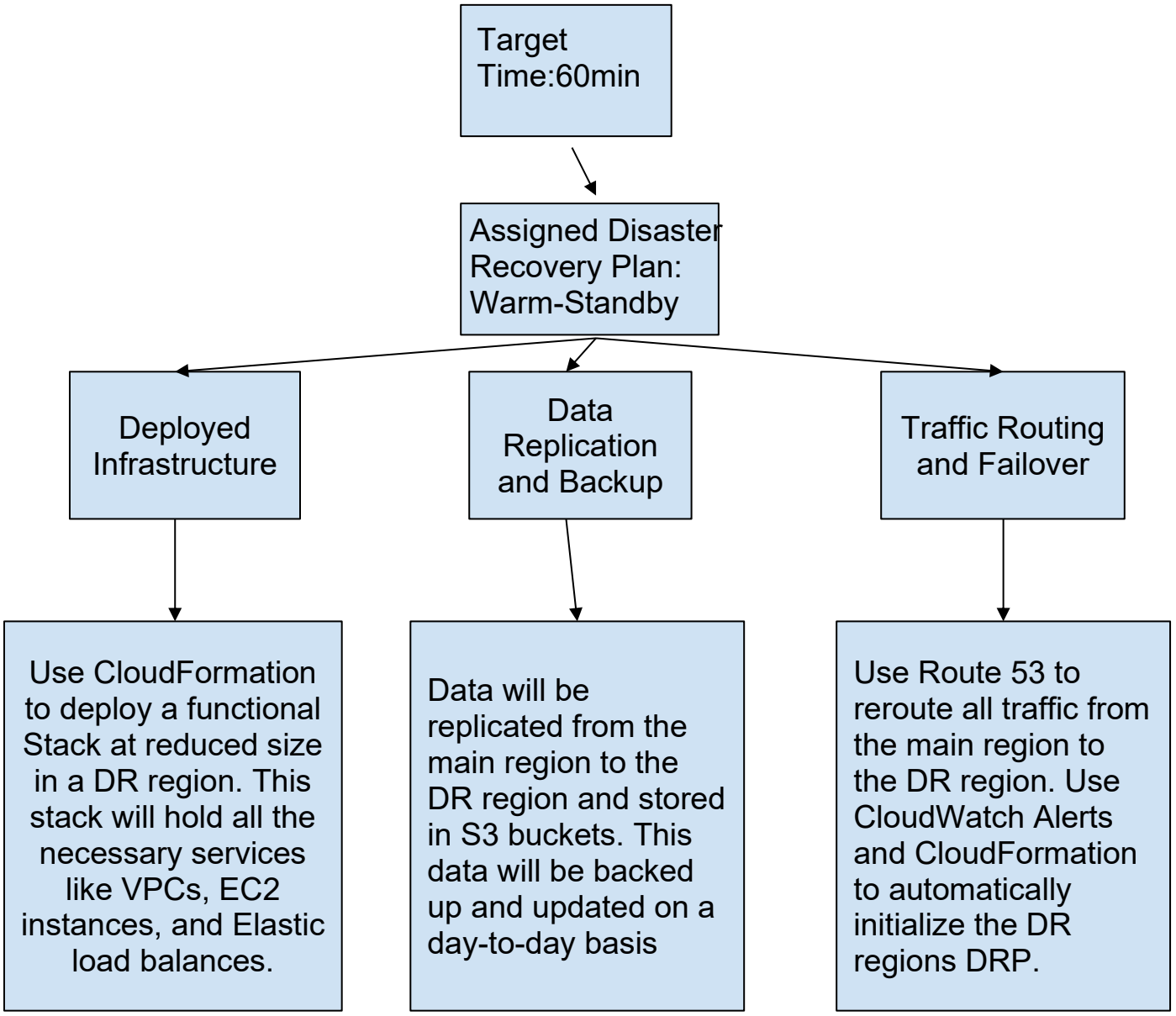
Despite the gains in the use of on-premise disaster recovery solutions, they bear high costs. Notably, organizations have to spend a considerable amount of money on infrastructure and maintenance/testing. Other than that, scaling the infrastructure to meet increased demand takes a lot of time and is super costly, thereby limiting scalability compared to cloud-based alternatives. (CBTS, 2024)

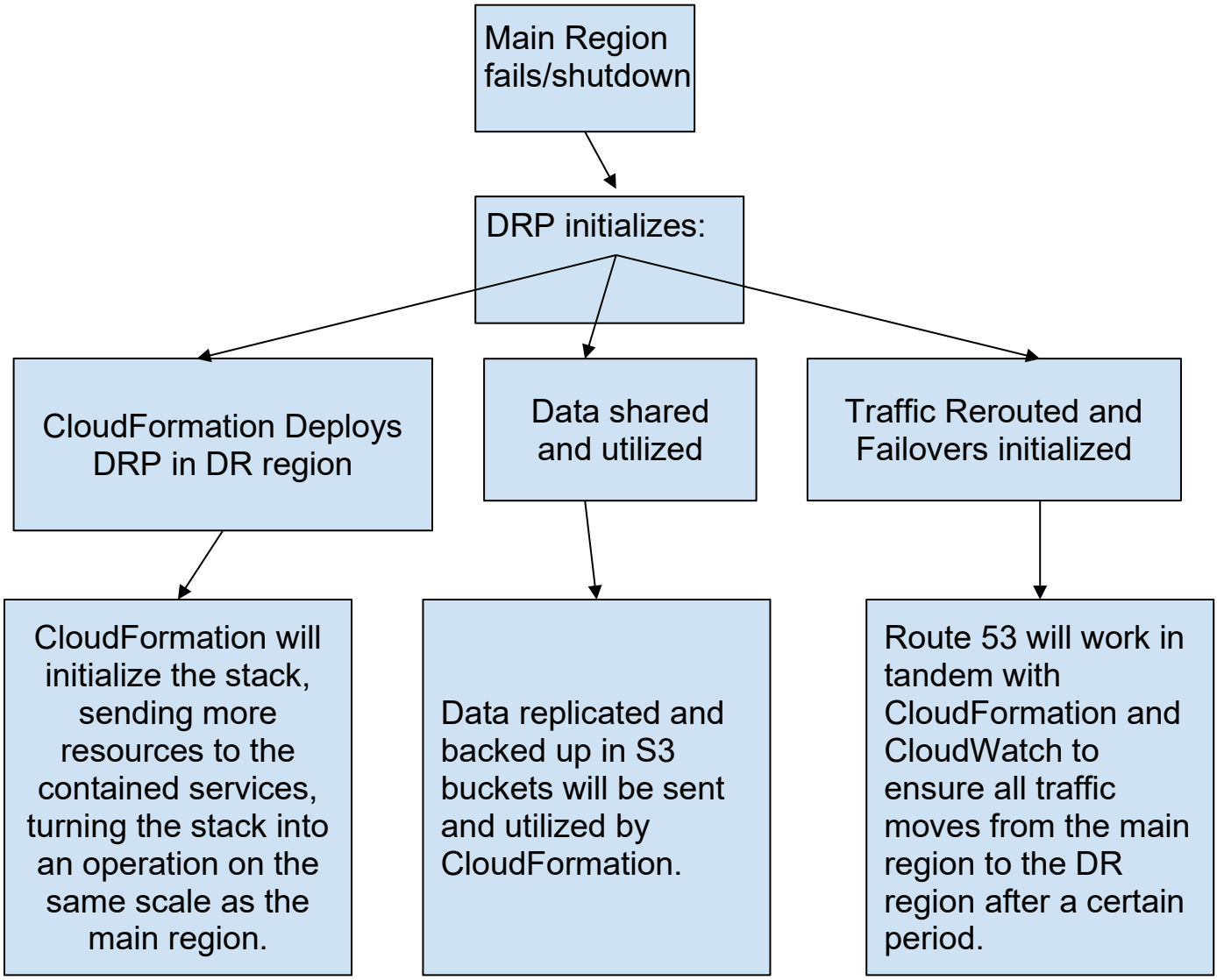
Hybrid disaster recovery solutions bring the best of both worlds. Hybrid combines on-premises and cloud approaches to bring flexibility and scalability of cloud DR and the control of on-premise DR. Furthermore, as these are two types of different resources, hybrid DR offers a far more resilient DR strategy that reduces the risk of failure overall.

However, a Hybrid DR can be complex to manage. It requires far more communication and coordination between on-premises resources and cloud resources. Additionally, Hybrid DR needs more planning in order to have the two integrate seamlessly for automatic failover. Moreover, the security of data across both could be a challenge as ensuring thorough security policies is very difficult.

What brings out the difference between cloud, on-premises, and hybrid disaster recovery solutions are the organizations needs. This goes for cost, control, and the level of complexity an organization would want to put up with. Hybrid solutions provide a well-balanced approach as it applies the strengths of both cloud and on-premises systems in developing a robust, workable disaster recovery strategy.

3. Detailed Security Plan





4. Pros of Warm-Standby

Warm standby DR strategies balance the need for high system availability with cost containment. Some of the key benefits include a lower RTO, since a warm standby system is partially active; hence, it can scale almost immediately to support the traffic in case of a disaster. In addition, this setup provides better readiness and easier testing for recovery processes. Furthermore, organizations are better placed to respond well in case of an incident. Besides, warm standby solutions are designed with advanced data synchronization, which minimizes the

chance of any potential data loss by periodically updating and synchronizing with the primary system and containing that data in S3/RDS storage. (GeeksforGeeks, 2024), (AWS, 2023) Additionally, warm standby systems offer flexibility in deployment, such that organizations can have geographic redundancy across both their main region and DR region. This will reduce the impact of regional disasters and network outages on an organization's operations by allocating resources to different DR regions based on the event. In terms of finances, warm standby DRPs sustain higher operational cost but are less expensive in comparison to a hot standby DRP; essentially a DR that is permanently online. (GeeksforGeeks, 2024)Warm standby is more suitable for mission-critical applications where faster recovery times are required and some reduced performance can be accepted right after the disaster.

References:

AWS. (2023, May 16). Disaster Recovery (DR) Architecture on AWS, Part III: Pilot Light and Warm Standby | Amazon Web Services. Amazon Web Services. https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-iii-pilot-light-and-warm-standby/

CBTS. (2024, January 3). Managed disaster recovery for your cloud, on-premises or hybrid environment | CBTS. https://www.cbts.com/infosheet/managed-disaster-recovery-for-your-cloud-on-premises-or-hybrid-environment/

Cloud4C. (2023, September 4). Implementing Disaster Recovery in Hybrid Cloud Environments. https://www.cloud4c.com/blogs/disaster-recovery-in-hybrid-cloud

GeeksforGeeks. (2024, July 4). Cold Standby vs. Warm Standby - GeeksforGeeks. https://www.geeksforgeeks.org/cold-standby-vs-warm-standby/

Gralewski, P. (2021, March 24). Developing a disaster recovery plan for cloud, on-premises and hybrid data. Commvault - English - United States. https://www.commvault.com/blogs/developing-a-disaster-recovery-plan-for-cloud-on-premises-and-hybrid-data

Lovett, C. (2023, February 16). Disaster Recovery: Cloud vs On-Premises. TierPoint, LLC. https://www.tierpoint.com/blog/disaster-recovery-cloud-vs-on-premise/

MyHalo. (n.d.). What Is the Difference Between Hot, Warm and Cold Disaster Recovery? | myhalo. myhalo | Reduce your carbon footprint. https://myhalo.com.sg/blog/uncategorized/what-is-the-difference-between-hot-warm-and-cold-disaster-recovery-3/

Yasar, K., Brush, K., & Crocetti, P. (2024, April 29). What is a disaster recovery plan (DRP)? | Definition from TechTarget. Disaster Recovery. https://www.techtarget.com/searchdisasterrecovery/definition/disaster-recovery-plan