Comprehensive Disaster Recovery Strategies for Production Support: Ensuring Business Continuity in Digital Environments

Sai Santosh Goud Bandari
Morrisville, NC, United States

Tata Consultancy Services Limited
Eamil :bandari.santhosh007@gmail.com

Yashasvi Makin
Seattle, WA, United States
Eamil :yashasvimakin@gmail.com

Abstract:

In today's real world, production environment plays a curtail role in the industries and business operations. Mainly, an organization depends on complex IT architecture, which potentially leads to failures such as cyberattacks and human errors, so this disaster recovery (DR) helps to maintain a continuous effort to the business to handle these kinds of issues more effectively to minimize the downtime and ensure trust of the business community. In this paper we are going to discuss the disaster recovery in detail with an example with an architecture diagram and explain the production support activity in a step-by-step process, offering the best supporting activity in the disaster recovery process.

One aspect of DR is backup and restoration, which helps businesses avoid financial losses and handle reputational damage to the organization. Modern DR has evolved with backup and restoration by modern techniques and automatic restoration mainly that can help us to maintain the downtime and automated incident response. Incident response is the game changer of the DR environment that we need to configure in Splunk, Dynatrace, or APPD monitoring tools to get alerts through mail or to phone, which can help in issue detection and also take action as soon as possible to get a quick resolution in the DR environment.

In conclusion, the production environment produces major strategies every year or every quarter with simplified techniques to restore and apply to get the DR activity to complete successfully at a certain point. Continuous efforts for the business help them to mitigate the issues and strategies against the emerging threats and technological changes, which helps business downtime and ensures the business continues to support and the business community to support the digital assets against the potential landscape environments.

Keywords: cyberattacks, disaster recovery (DR), backup and restoration, automated incident response, Splunk, Dynatrace, digital assets.

1. Introduction:

In today's world, with increasing interconnectivity in the digital landscape, we use DR activity to maintain resilience in production environments. Where production issues can be many types, such as cyberattacks, human errors, technical failures [1]. This robust DR environment helps us to give continuous support to the business environment and minimize the intensity of the issue. In the source of the paper, we are going to discuss how we can triage and mitigate the issue with the short period of time, which can adapt the modern techniques to handle them to reduce the financial loss to minimize the downtime and also regulatory penalties. By implementing the advanced monitoring techniques using the monitoring tools like Splunk to set the threshold and to get the alerting system [2], we help ourselves to prepare for the potential issue identification and to respond within the time to reduce issue intensity.

2. Disaster Recovery Framework:

In a DR environment, risk assessment and business analysis are the fundamental steps for evaluating the DR frameworks. Whereas business impact analysis (BIA) plays a major role in system downtime and data loss. The key perspective of the process is recovery time objective and recovery point objective, which helps us guide and develop appropriate development strategies [3].

In DR, business impact analysis plays a major role in which it analyzes operational and financial consequences, whereas BIA helps your organization to estimate the criticality of the issue and estimates the revenue loss; mostly, it prioritizes the recovery time and assists the organization with reputation damage.

It is the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO) that shape DR strategies. RTO is the longest downtime that can happen before a big problem arises, and RPO is the smallest amount of time that data can be lost before it becomes a problem. Some of the recovery options that can be chosen are hot, warm, and cold sites, cloud-based failover systems, and real-time data replication strategies [4].

By using BIA strategies in the DR, we can ensure the organization's operations can develop robust data integrity and minimize the downtime from unexpected events and help the business to grow. This helps DR procedures in future enhancements and effectiveness.

3. Recovery & Validation Procedures:

Now we are discussing the failover steps in the DR environment in the operational flow, which ensures data integrity and system availability. The following table summarizes the key activities and responsibilities, for which we can check the comments in the below table.

Recovery & Validation Procedures (Failover to DR)		
Recovery Activity	Team Name	Comments
Setup Citrix DR icon for testers to use	Virtualization Support	XEX DR Icon will appear on Citrix
Put in request to put all XEX jobs on hold	Job Scheduling Team	We will now hold all the jobs running on the DR cluster
Take backup of Prod DB (Informix)	INFORMIX Support	We need to take back up for the XEX Informix DB
Stop the Claims Adjudicator	Job Scheduling Team	
Put Informix DB in Single User mode	INFORMIX Support	
Take down Citrix Production Server (XEX GUI)	Virtualization Support	SERV1, SERV2, SERV3 these servers need to be validated
Switch Informix DB to secondary	Informix Support	Validate axm100 server

Explaining the Step-by-step explanation below:

3.1: Setup Citrix DR icon for test:

Team Responsible: Virtualization Support

Objective: Ensure that testers and production support team can access the DR environment [5].

- A Citrix DR icon will be available on the Citrix network.
- This Citrix icon helps to verify the accessibility of the application UI and system responsiveness. A Citrix DR icon will be available on the Citrix network.

3.2: Put XEX app jobs on hold:

Team Responsible: Coordinate with job scheduling team.

Objective: It helps us to prevent interference between Production and Disaster recovery environment.

- A rods request is placed in service now to hold the scheduling jobs in XEX application.
- Production support team will hold the jobs in device now, which helps us to ensure no transaction lost or duplicate.

3.3. Take Backup of Production DB:

Team Responsible: Informix Support

Objective: taking back the latest database before failover.

- The full backup XEX DB is taken from production.
- This ensures the safety without data loss that can roll back when its required.

3.4. Stop the Claims Adjudication

Team Responsible: The production support team needs to coordinate with the job scheduling team.

Objective: Stop the new claims to avoid anomalies or inconsistencies.

- This Claims Adjudication process helps us to prevent transaction conflicts.
- This step helps us to keep claims data consistent during the transaction.

3.5. Put the Informix database in single-user mode.

Team Responsible: The production support team needs to coordinate with the Informix support team.

Objective: Stop or restrict access to the database during failover.

- This feature enables the database to be in single-user mode, allowing the disaster recovery team to interact.
- This helps us to prevent unauthorized changes that corrupt the data during migration.

3.6. Take Down Citrix Production Server:

Team Responsible: The production support team needs to coordinate with the virtualization support.

Objective: This operation shuts down the primary production Citrix environment to initiate failover

- Now we need to bring down all the prod services SERV1, SERV2, and SERV3.
- This feature helps us to redirect the users to the DR environment.

3.7. Switch the Informix database to secondary.

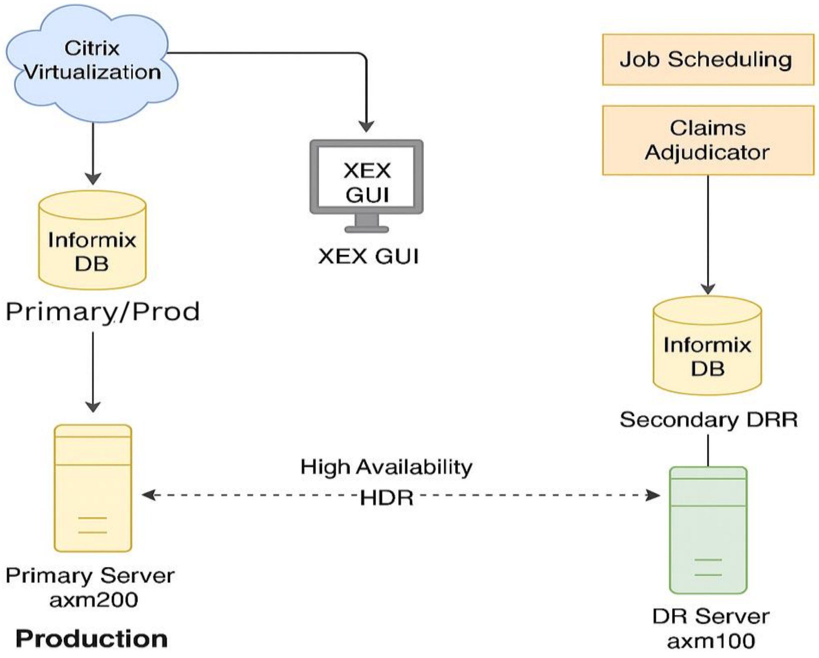
Team Responsible: The production support team needs to coordinate with the Informix support.

Objective: Activate the disaster recovery to handle operations.

- The secondary Informix DB server name, avm100sefrver, is switched to primary mode.
- The result completes the failover process and allows normal operations in the Dr environment.

4. Architecture Diagram Representation:

The following diagram represents the Architecture XEX application, an Informic DB failover system, where the primary DB replicates with the secondary DB (axm100) using HDR. During the DR failover, job scheduling and Citrix virtualization switch to the DR environment to ensure business continuity.



5. Post-Failover Validation & Testing:

After successfully changing it to the DR environment, we need to validate the application and test it to ensure the data integrity is maintained according to the business objective operations without any disturbance [6]. The following are a few validations that we need to perform.

5.1. User Access Testing:

Objective*:* To see whether they can access the DR environment or not.

- All authorized users must be able to log in to the Citrix DR environment.
- Conduct all types of functional testing to check necessary actions.
- Validate SSO multifactor authentication while connecting with the DR environment [7].
- Check login issues. Check if session policies are properly applied or not.

5.2. Database Integrity Check:

Objective: Ensure that the data has been flowing accurately to the DR environment without any loss.

- Perform the data comparison between production and DR databases to verify the record consistency.
- If any records are missing, check the missing records using checksum validation [8].
- Validate all the foreign key constraints and indexes, etc.

5.3 Performance Monitoring:

Objective: Evaluate system stability, any latencies, and speed resource utilization in DR.

- Monitor CPU usage using Dynatrace and APPD, which helps to check each and every server in detail to check the process flows [9], etc.
- Conduct the load testing to check user activities and measure the response times.
- Implement real-time monitoring tools to track application health and generate alerts [10].

6.Case Study:

In a digitally evolving connected healthcare system, any production interruption can lead to significant financial, operational, and reputational harm. The XEX healthcare application, important for managing claims adjudication, sensitive patient and billing data. A failover simulation was to assess the Disaster Recovery (DR) plan and minimal Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

6.1 Result Analysis:

A full failover was completed under supervised conditions. Key metrics before and after DR strategy implementation are outlined below:

Metric	**Pre-DR Simulation**	**Post-DR Simulation**
Downtime (RTO)	180 minutes	30 minutes
Data Loss (RPO)	4 hours	< 1 hour
Transaction Consistency	Inconsistent	Fully retained
Alerting Response Time	Manual (delayed)	Automated (via Splunk)
User Redirection	Manual	Auto-switch via Citrix DR icon

7.Conclusion:

Digital infrastructures are quite important for companies nowadays, so they need a meticulously orchestrated disaster recovery (DR) strategy to maintain their operations. This paper has discussed the significance of DR for production support and presented a thorough framework including risk assessment, failover tactics, database integrity checks, and performance monitoring and identification of possible hazards. reducing failover risks, and ensuring system stability and consistency during disaster recovery efforts. Advanced monitoring technologies such as Splunk, Dynatrace, and AppD help us to identify the potential threats before they come in, meaning for automation incident response systems, they therefore minimize the risk of failover and ensure system stability and system consistency during DR activity.

References:

[1] J. Smith and A. Kumar, *Disaster Recovery Planning for IT Systems: A Business Continuity Approach*, IEEE Transactions on Information Security, vol. 18, no. 3, pp. 45-56, 2023. [2] M. Johnson and T. Brown, "Enhancing IT Resilience with AI-Based Monitoring Tools," *Proceedings of the International Conference on Cloud Security*, pp. 120-130, 2022. [3] TechTarget, "What is Business Impact Analysis (BIA)?," 2024. [Online]. Available: https://www.techtarget.com/searchstorage/definition/business-impact-analysis.

[4] A. Alhazmi and Y. Malaiya, “Evaluating disaster recovery strategies for IT infrastructures,” *Proceedings of the 2006 IEEE International Conference on Systems, Man and Cybernetics*, Taipei, Taiwan, 2006, pp. 2515–2520.

[5] M. K. Soni and R. K. Gupta, **Disaster Recovery Planning for IT Infrastructure: Strategies and Best Practices**. New York, NY, USA: Wiley, 2022, pp. 45-60.

[6] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, “Disaster recovery techniques for cloud computing,” *Proceedings of the 2010 IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC)*, Shenzhen, China, 2010, pp. 343-348.

[7] N. Gruschka and M. Jensen, “Attack surfaces: A taxonomy for attacks on cloud services,” *Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing (CLOUD)*, Miami, FL, USA, 2010, pp. 276-279.

[8] R. C. Merkle, “A digital signature based on a conventional encryption function,” *Proceedings of the 1987 Conference on the Theory and Application of Cryptographic Techniques (CRYPTO)*, Santa Barbara, CA, USA, 1987, pp. 369-378.

[9] P. Barford and M. Crovella, “Generating representative Web workloads for network and server performance evaluation,” Proceedings of the 1998 ACM SIGMETRICS Conference on Measurement and Modeling of Computer Systems, Madison, WI, USA, 1998, pp. 151-160.

[10] M. Mao and M. Humphrey, “A Performance Study on the VM Startup Time in the Cloud,” in 2012 IEEE Fifth International Conference on Cloud Computing, Honolulu, HI, USA, 2012, pp. 423–430. DOI: 10.1109/CLOUD.2012.103.