ijar
ISSN NO. 2320-5407

Journal Homepage: -www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI:10.21474/IJAR01/11542
DOI URL: http://dx.doi.org/10.21474/IJAR01/11542

RESEARCH ARTICLE

DISASTER RECOVERY FOR DATABASE ON CLOUD ENTERPRISE

Maqhbool Jameel Ahmed[1] and Shahina Begum Ahmed[2]

1. Director, Tech Mahindra America's Inc Plano, Texas, United States.
2. Manager, IBM Corporation San Jose, California, United States.

Manuscript Info

Manuscript History
Received: 20 June 2020
Final Accepted: 24 July 2020
Published: August 2020

Key words:-
Data loss, Data Recovery, Cloud Computing, IT Assets, Data Recovery Plan, Business Support, Identity and Access Management, Cloud Database

Abstract

In IT Platforms, data loss and Disaster recovery is a persistent problem which is more crucial in cloud computing. Database on Cloud offers the capability to retain an unlimited number of databases backup virtually. In a Database, there is an additional backup and restore the capacity for Database that enables the retention of many databases, and the requirement of retaining sensitive data is accommodated. IT assets Recovery team handles disruption/ disaster recovery using their skilled expertise and knowledge in information and technology to present a data recovery plan. A considerable amount of research has been published in disaster recovery using cloud computing by researchers in the past few years. However, there is a lack of accurate survey for further analysis of cloud-based disaster recovery and to fill this gap; this study presents a detailed survey of disaster recovery mechanisms and research in the cloud environment.

Introduction:-

Computing is the delivery of services on demand from application to data centers on a pay-for-use basis. Computation using cloud dates back to the 1950s, it has evolved over the years through phases pioneered. Data recovery consists of best practices and IT systems designed to minimize or prevent data loss and disruption of businesses out of a catastrophic event. The loss of data is caused by civil emergencies, natural disasters, equipment failure, power outage, and criminal attacks. Disaster recovery planning involves deploying appropriate technology and continuous testing to maintain backup and ensure adequate storage to maintain robust failover procedures. This study shows the scope of Database and the architectural configuration and implantation of the recovery processes. The study also highlights the Roles and responsibilities of the IT asset recovery team as well as the benefits of implementing the recovery plan.

Objective:-

This study provides a framework for making decisions and executing plans to continue the operations of one or more critical IT assets in response to a catastrophic failure. The execution of the Recovery plan facilitates the continuation of critical business processes and eventual resumption of business operation normally. The extent and nature of the impact may vary, and the assessment of the impact by an IT asset operator determines the invocation of the recovery plan. The plan supports the recovery of IT assets and is verified during IT asset testing and is subject to annual review by Business Processes Owners (BPO).

Corresponding Author:- Maqhbool Jameel
Address:- Director, Tech Mahindra America's Inc Plano, Texas, United States.

The Architecture of Disaster Recovery Configuration: -

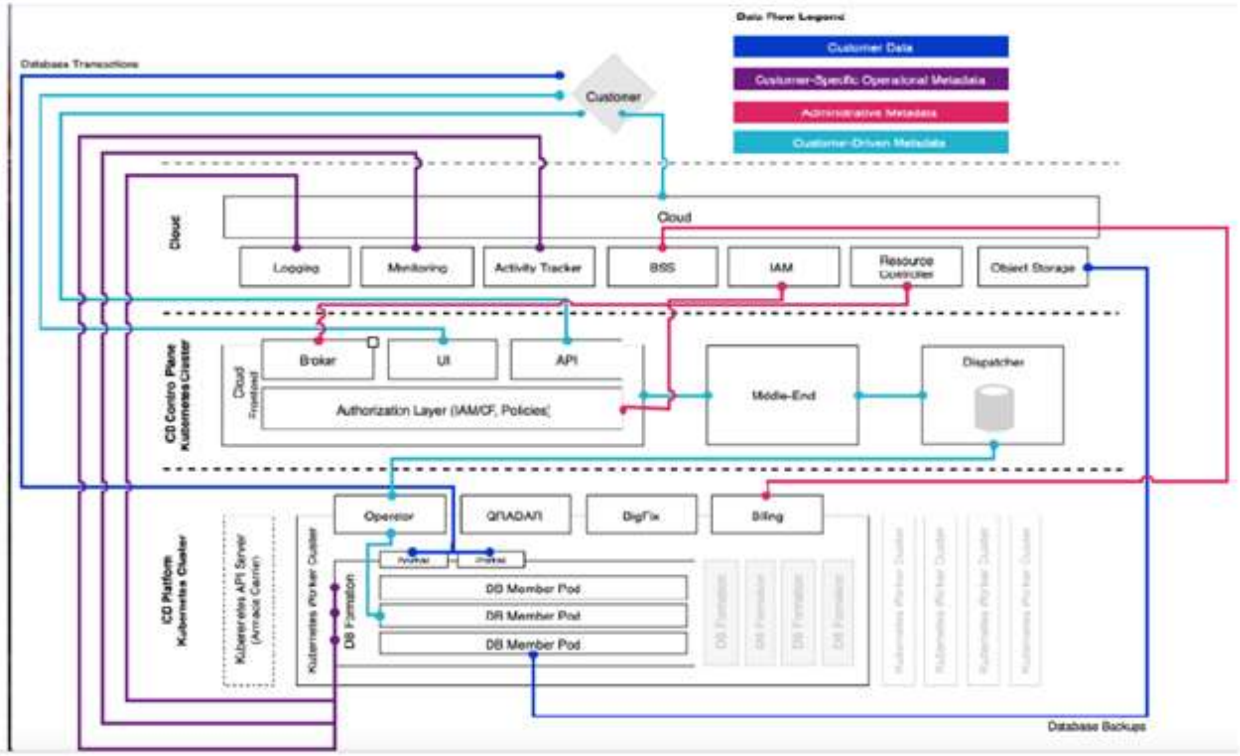

Fig 1:- Disaster Recovery Configuration.

In order to support a wide range of systems on a unified platform, the Cloud Data base(CD) system is implemented in layers. At the heart of the system is a core set of abstractions and processes for managing them; this is typically called the platform. Below these abstractions are the concrete implementations for specific systems. On top of the platform is the control plane, which implements customer and Cloud facing APIs and the third layer is the Cloud is to manage logging, monitoring, tracking and Pricing.

Activity auditing (logging/monitoring) controls provide reasonable assurance that security events are recorded to support threat detection and investigation activities.

Activity Tracker records events, compliant as per standards, triggered by user-initiated activities that change the state of a service in the cloud. Thus a customer can see, manage, and analyze cloud actions.The purpose of Activity Tracker is for the customer to be able to track all user activity in the customer's Cloud account.

Business Support Service(BSS) has to do with pricing and metering, measuring usage of our service tagged to individual client.

Identity and Access management (IAM) enables you to securely authenticate users for platform services and control access to resources consistently across Cloud. A set of Cloud services are enabled to use IAM for access control, and are organized into resource groups within your account so you can give users quick and easy access to more than one resource at a time.

All CD services are regional - not global, and not zonal. CD deploys a single Kubernetes cluster to manage the control plane and one or more "data plane" clusters that host the platform and customer workloads. The control plane cluster is wired up to Cloud and hosts the API, service broker, etc., and is responsible for mapping individual formations to particular data plane clusters. Incidentally the control plane cluster also runs the platform in order to host the databases it needs to operate.When a data plane cluster is "full" a new cluster is deployed to the region to host new formations.

Customer routes for control plane traffic and data plane traffic are distinct. All control plane traffic - scaling instances, backing up formations, etc. - hits the regional control plane endpoints. Data plane traffic does not flow through control plane clusters. Customers are provided with hostname/port pairs dedicated to their formation and traffic flows directly to single-tenant components on the data plane cluster. Where possible all CD Kubernetes clusters are multi-zone CD deployed in a select few single-zone regions.Control plane clusters are fixed-size; data plane clusters are automatically horizontally scaled to meet the needs of the workloads they support.

For Db2onCloud we will leverage Kubernetes to provide the raw compute and memory for the service. Leveraging encryption capabilities of Block storage and COS as opposed to Db2 Native encryption capabilities for Data at REST.

Leveraging operator based deployments instead of a central tool like UCD/ Ansible etc. to control the day to day activities and deployment of customer formations. Network is provided via NodePort services as

The Db2 console providing the user interface features for the service is not specific to each customer and instead operates as a truer web service used by all customers. Monitoring is provided by Sysdig from Prometheus compatible endpoints.

Prometheus is a systems and service monitoring system. It collects metrics from configured targets at given intervals, evaluates rule expressions, displays the results, and can trigger alerts if some condition is observed to be true

Implantation Plan:

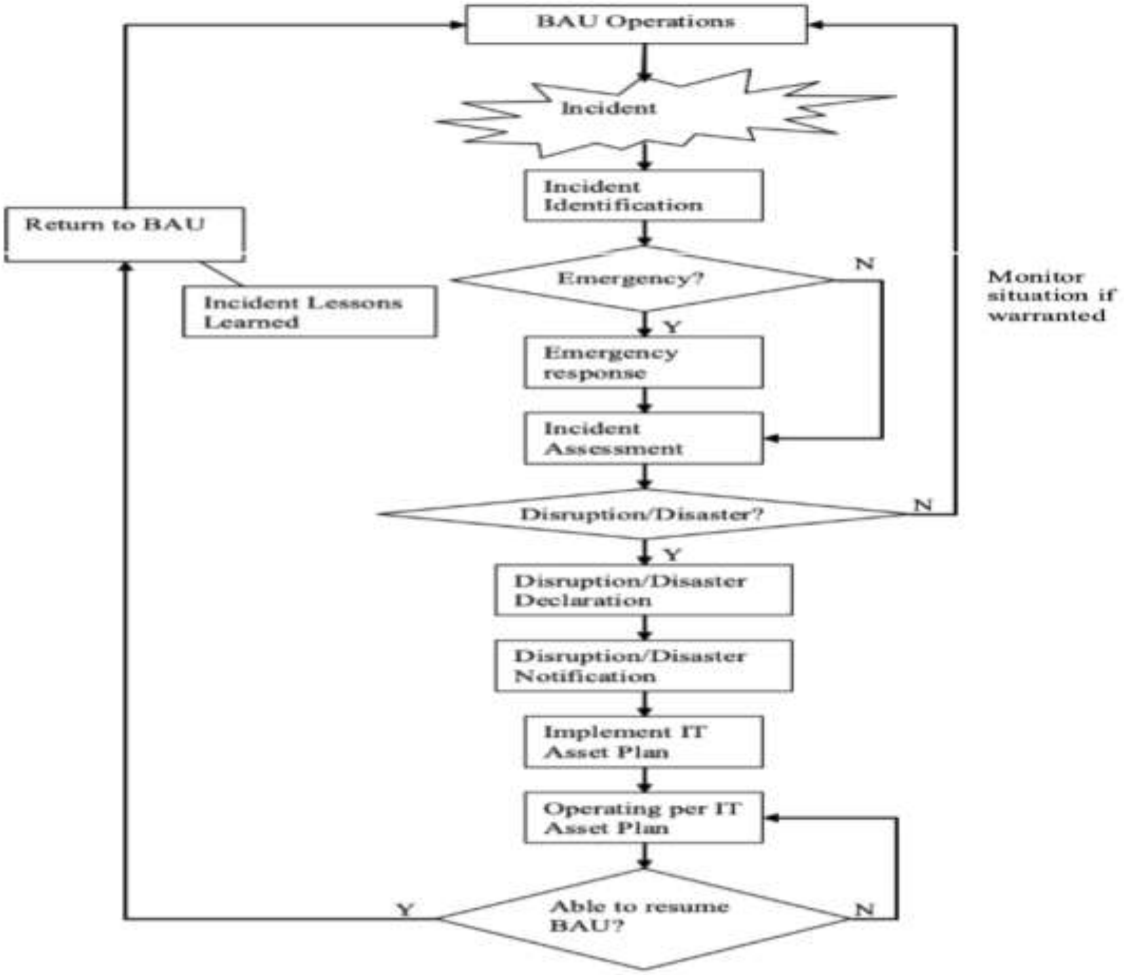

Fig 2:- Stages of Disaster Recovery.

Step 1: Incident Identification:
All disruption does not always begin with an emergency. However, an emergency may or may not become a disaster. An emergency requires Personnel on-site to act since disruption caused by an emergency has a short duration, and after the interruption, an operation may quickly return to normal. The local site security department is the first point of contact, and all personnel should familiarize themselves with procedures on emergency cases. A quick assessment of the situation should be conducted by the first personnel who discovers/ notified about an issue. After the assessment, the person should determine the extent of the impact and take a course of action immediately (Alshammari et al., 2017). In the case of an emergency, local emergency procedures should be followed whereby the notified manager should contact the Asset Recover IT Team lead, which in turn, informs the Recovery team members of potential disruption.

Step 2: Incident Assessment:
The site Crisis Management Team (CMT) assesses the extent of the damage for a disruption affecting the operation at a particular location and decides when the facility is safe for occupation. The recovery and status outlook communication come from CMT members on site. However, not all issues impacting a critical IT asset is addressed by a site CMT first, the recovery team performs assessment determining the impact level and the estimated time for restoration (Saif & Wazir, 2018). The assessment considers the safety of occupants of the building determined by critical function availability like power, internet/intranet, and phone. Once sufficient information has been gathered to make a recommendation, the IT asset Recovery Team Lead receives the report, which is done before the completion of the assessment.

Step 3: Disruption/ Disaster Declaration:
The IT Asset Recovery Team Leader initiates an emergency conference to decide whether to declare a disaster or not and to select a course of action. In making the declaration decision, the IT asset recovery team appraises the severity of the situation based on the findings and recommendations. A judgment exercise is determining the declaration of a disruption/ disaster best cause of action to follows, factors in the variability in the criticality of the processes (Bedoya et al., 2016). If the expected business impact is acceptable, then the appropriate decision is not to declare a disaster or a disruption and select a team to execute selected tasks.

The declaration occurs at any point once the disaster/ disruption has been identified. If the situation indicates relocation of IT assets, resources are mobilized in the declaration to implement the necessary steps. The recovery team lead and management should make the final decision to declare and the course of action to be taken, and the communication made quickly and clearly (Saif & Wazir, 2018). The IT asset Recovery Team, based on the specific impact and current business event, determines the appropriate course of action at the time of the incident.

Step 4: Disaster/Disruption Notification and IT Asset Recovery:
Once a disruption/disaster has been declared, and the directive for the recovery given, all employees of the business Area are contacted soonest possible. The departmental managers then instruct employees on their specific course of action and report to the Recovery Team the status of employees' notification. Key clients, both internal and external, are also notified through the notification manager who has the list of clients and their e-mail addresses (Wang et al., 2016). Key Vendors or suppliers are notified depending on the severity of the disaster through designated personnel by the IT Asset Recovery Team.

There are technical steps to be followed to recover assets, and the steps include: to receive technical recovery requests, validate infrastructure availability and capacity, prepare for recovery, prioritize customer recoveries, Recover Database warehouse on the cloud, perform database recovery, and validate Recovered customer instance.

Step 5: Return to Business as Usual:
While the IT asset using the Recovery Plan is being executed, the affected primary site is monitored, determining the possibility of returning all or part of the affected IT assets to normal operations. The Recovery Team determines the date, time, and plan to revert to the original site once it has been determined that a facility is restored and ready for use (Bedoya et al., 2016). Once the asset has been restored to business as usual operation and lesson learned from the incidence evaluation, there is the closure of the specific disaster.

Dependencies:
For recovery operations, remote network access is a necessity, as restore scenarios rely on Soft layer for data center hosting environment and server functionality. Network connectivity between hosting locations is required for the restoration of multizone functions and backup operations. To completely restore operations on the Database cloud, it requires a series of services: A cloud Kubernetes service backend requires a deployment target to make backup available for restore. Cloud Object Storage provides archival storage for customer database instances without which Database on cloud does not operate. A cloud internet services provide DNS and L7 proxy services for the ICD frontend to enable communication with the control plane (Alshammari et al., 2017). Key-protect provide essential management services for the data volume backing the database and without a functional key Protect configuration of newly provisioned data for encryption is undoable

Assumptions:
It is assumed that Database on cloud enterprise covers multizone deployment and that it is the only deployment option in service currently. There is an assumption of data loss for the period between failure time and last backup since the backup is done every 24 hours. Failover is handled by constant replication and automatic failover within an Multiple Zone region(MZR), which is equivalent to Recovery Period Objective (RPO) and Recovery Time Objective (RTO) from the service perspective. Note database backups are available in geo-replicated backup on cloud object storage (Saif & Wazir, 2018). At the same time, the customers can restore Database backup by themselves since backup restoration is a functional requirement in the last 14 days outside the scope of exercise. It is assumed that Database Cloud service recovery objectives are to provide customers with access to their customer data for restoration and to restore service functionality.

Process and Approach:
The first step is to determine if a declaration of disaster and execution of offering a recovery plan is required and need to ensure the available workforce. To recover from a regional failure, the Database on cloud Enterprise team will stand up a new data plane cluster in a substitute region with the cloud Databases and Restore the backup of Kubernetes from the failed region onto cluster provisioned above. Ensure persistent volumes are attached to all appropriate dedicated formation and update DNS to direct traffic for the failed region's control plane to the restored control in the substitute region (Alshammari et al., 2017). The Disaster Recovery plan and the document is reviewed and updated every end of a year or before to reflect any changes in the offering that impact the existing DR plan. Service operational personnel carry out a full execution test of the Disaster Recovery plan.

Execution Steps Stages:
The Business Processes Owners (BPO) verifies that an invocation of the Disaster Recovery Plan would result in being able to recover and restore services that are required to a level that is foreknown. In the timeframe predetermined, the plan identifies a Recovery Scope for the disaster Determining Disaster Recovery Strategy and performing due diligence on Disaster Recovery. Also, the BPO defines and documents the disaster Recovery Plan, and the Security focal point verifies that the DR plan is regularly tested on an unplanned and planned basis (Saif & Wazir, 2018). The BPO is responsible for declaring a disaster while the security. The focal point is responsible for coordinating recovery activities. In the final stage, the BPO updates the plan on disaster Recovery.

Roles and Responsibilities:
The responsibilities and roles of the IT Asset Recovery team are set out. The responsibilities include assessing the overall performance and effectiveness of the IT Asset recovery process after use. To notify an incident response plan to the IT Asset Recovery teams of a user-impacting plan on the decision whether to declare a disaster and what course of recovery actions to follow. Another role is communicating with all affected personnel and Interfacing with the corporate, site, and business unit executives to obtain resources and authorizations as required (Alshammari et al., 2017). In conjunction with business area executive management, The IT asset Recovery team makes decisions regarding business resumption once recovery activities have completed. The Asset Recovery team, asses' general performance and effectiveness of the recovery process after use and train the management team and recovery personnel about their responsibilities under the plan and how to fulfill them. Besides, The Asset Recovery Team tests the plan annually and reviews the results with the management in determining the risk.

Benefits of Implementing Disaster Recovery:
The organization that uses a Cloud-based Recovery solution is cost-efficient as it takes advantage of the pay-as-you-grow model, which streamlines costs with the complexity and size of IT disaster recovery need. With cloud-based

disaster recovery, organizations can start without significant investment in a secondary site, software, or hardware and are provided with the specialized knowledge needed (Wang et al., 2016). Cloud-based solution for disaster recovery allows non-disruptive and frequent testing of IT disaster recovery effort; thus, it is reliable. Organizations that use Cloud-based solutions are more flexible since they can run the cloud or restore systems and data at any location. It also allows uses to access necessary arrangements remotely and offers consistency and simplified management.

Conclusion:-

Data loss is a threat in computing, and the recovery of the data gives a relief to the IT experts and systems. The nature and extent of disruption vary, and the recovery plans are diverse as assessed and recommended by the IT assessment Team and the management. Minimizing business disruption and negative impact on business the best plan is executed. The implementation plan of Data Recovery involves various steps and stages that are outlined in this study (Wang et al., 2016). Several services are required to complete the restoration operations, the assumptions of Database and the procedures are also spelt out in the study. Besides the benefit that accrues to an organization that uses a cloud-based recovery solution are discussed.

References:-

1. Alshammari, M. M., Alwan, A. A., Nordin, A., & Al-Shaikhli, I. F. (2017, November).
2. Disaster recovery in single-cloud and multi-cloud environments: Issues and challenges. In 2017 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS) (pp. 1-7). IEEE.. Bedoya, H., Cruz, F., Lema, D., & Singkorapoom, S. (2016). External Procedures, Triggers, and User-defined Functions on IBM DB2 for i. IBM Redbooks.
3. Saif, S., & Wazir, S. (2018). Performance Analysis of Big Data and Cloud Computing Techniques: A Survey. Procedia computer science, 132, 118-127.
4. Wang, L., Harper, R. E., Mahindru, R., & Ramasamy, H. V. (2016, June). Disaster Recovery for Cloud-Hosted Enterprise Applications. In 2016 IEEE 9th International Conference on Cloud Computing (CLOUD) (pp. 432-439). IEEE.