DISASTER RECOVERY WITH IBM CLOUD VIRTUAL SERVERS

PHASE-4

DEVELOPMENT AND FUNCTION OF DISASTER RECOVERY PLAN

TABLE OF CONTENTS

DISASTER RECOVERY WITH CLOUD COMPUTING:

- The term cloud disaster recovery (cloud DR) refers to the strategies and services enterprises apply for the purpose of backing up applications, resources, and data into a cloud environment.
- Cloud DR helps protect corporate resources and ensure business continuity.
- If disaster hits, enterprises can restore data from backed up versions to either on-premise or cloud environments. Another key advantage is the ability to automate many processes and quickly scale according to business requirements and needs.

DISASTER RECOVERY DEVELOPMENT WITH CLOUD COMPUTING:

Increase Backup Frequency: One way to quickly improve RTOs and RPOs is to increase the frequency of backups. While this may not be feasible for every protected asset, consider more aggressive backup schedules for mission-critical data. More frequent backups will reduce your RPO immediately.

Utilize Changed Block Tracking: Accessible via vSphere APIs, Vmware's Changed Block Tracking (CBT) is a feature that aids in performing incremental backups of virtual machines. Backup solutions, including Unitrends, may utilize CBT for any VMs running on ESX/ESXi host.

Embrace Cloud Technology: You should be replicating a copy of your backups to an alternate target. Traditionally, this may have been physical media such as disk or tape. While legacy media still has its place, your RTO will suffer with this strategy since the media must be retrieved, and the data imported and then recovered.

FUNCTION OF DISASTER RECOVERY

Data Backup: Regularly backing up data to the cloud to ensure that critical information is preserved and can be retrieved in case of data loss.

Disaster Recovery Planning: Developing comprehensive disaster recovery plans that outline procedures for data restoration and system recovery.

Testing and Validation: Regularly testing and validating disaster recovery plans to ensure they work effectively when needed.

Rapid Recovery: Ensuring fast recovery times to minimize business disruption during disasters.

Cost Optimization: Balancing the costs of disaster recovery with the criticality of systems and data, and using cloud resources efficiently.

CODE FOR DEVELOPING A PLAN

Developing a disaster recovery plan that includes Recovery Time Objective (RTO) and Recovery Point Objective (RPO) involves creating a structured document outlining how to respond to disasters.

```
RTO = "X hours/days"  # Maximum acceptable downtime
RPO = "Y hours/minutes"  # Maximum data loss tolerance

# Identify Critical Systems and Data
critical_systems = ["SystemA", "SystemB"]
critical_data = ["DataX", "DataY"]
```

```
def response_phase(system) :

def recovery_Phase(system) :
```

```
def testing_and_validation(system):
def communication_plan():
def documentation () :
def reporting():
def monitoring():
def review_and_ updates() :
def employee_training():
def cost_efficiency():
def periodic_testing():
def plan_activation():
```

Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are two of the most important parameters of a disaster recovery or data protection plan. These are objectives that can guide enterprises to choose an optimal cloud backup and disaster recovery plan.

FEATURE ENGINEERING:

Data Source Identification:

Create a feature that identifies the source of the data, such as differentiating between on-premises servers and cloud-based resources.

Data Timestamps:

Extract time-based features from logs, like day of the week, time of day, and special event indicators, to understand when incidents or disasters occur.

Resource Dependency Mapping:

Construct a graph-based feature to map dependencies between critical systems, applications, and services, helping to identify which resources are most critical.

Data Quality Metrics:

Calculate metrics related to data quality, like data completeness, data accuracy, and data consistency. These metrics can help assess the impact of data loss during a disaster.

Resource Utilization Metrics:

Create features related to resource utilization, such as CPU, memory, and storage usage. These can indicate potential resource constraints during disaster recovery.

Log Patterns and Anomalies:

Develop features that capture patterns and anomalies in log data. For example, use techniques like log parsing and log entropy to identify irregularities.

Geographical Information:

If applicable, use location-based features to understand the geographic distribution of resources and the potential impact of regional disasters.

Change Detection:

Identify features that highlight significant changes in resource configurations, code repositories, or application versions. This can help pinpoint potential sources of failure.

Incident History:

Incorporate features related to the history of past incidents, their severity, and the effectiveness of previous disaster recovery efforts.

Security Metrics:

Include features related to security events and vulnerabilities. Understand how security incidents may impact disaster recovery efforts.

SUMMARY OF DISASTER RECOVERY PLAN

In summary, a Disaster Recovery Plan is a vital component of an organization's business continuity strategy. It ensures that critical operations can continue even in the face of adversity, safeguarding the organization's reputation and financial stability.

THANKS!

TEAM MEMBERS:

- **SONA.S**
- **NISHANTHI.M**
- **PRIYADHARSHINI.M**
- **MYTHILY.D**