FINAL PROJECT DOCUMENTATION

DISASTER RECOVERY USING IBM CLOUD VIRTUAL SERVERS

DESCRIPTION:

Disaster recovery (DR) consists of IT technologies and best practices designed to prevent or minimize data loss and business disruption resulting from catastrophic events—everything from equipment failures and localized power outages to cyber attacks, civil emergencies, criminal or military attacks, and natural disasters.

OBJECTIVE:

Disaster recovery planning involves strategizing, planning, deploying appropriate technology, and continuous testing. Maintaining backups of your data is a critical component of disaster recovery planning, but a backup and recovery process alone does not constitute a full disaster recovery plan.

Disaster recovery also involves ensuring that adequate storage and compute is available to maintain robust failover and failback procedures. *Failover* is the process of offloading workloads to backup systems so that production processes and end-user experiences are disrupted as little as possible. *Failback* involves switching back to the original primary systems.

GOALS:

- To minimize interruptions to the normal operations.
- To limit the extent of disruption and damage.
- To minimize the economic impact of the interruption.
- To establish alternative means of operation in advance.
- To train personnel with emergency procedures.
- To provide for smooth and rapid restoration of service.

RECOVERY STRATEGIES:

Cloud-based disaster recovery strategies:

Cloud-based vendors offer Disaster recovery as a service (DRaaS), which are essentially “hot sites” for IT disaster recovery hosted in the cloud. DRaaS leverages the cloud to provide fully configured recovery sites that mirror the applications in the local data center. This allows users a more immediate response, allowing them the ability to recover critical applications in the cloud, keeping them ready for use at the time of a disaster.

Vendors can host and manage applications, data security services, and data streams, enabling access to information via web browser at the primary business site or other sites. These vendors can typically enhance cybersecurity because their ongoing monitoring for outages offers data filtering and detection of malware threats. If the vendor detects an outage at the client site, they hold all client data automatically until the system is restored. In this sense, the cloud is essential to security planning and disaster recovery.

STEPS IN RECOVERY STRATEGIES:

STEP 1: With each approach to DR, you should consider the recovery characteristics of the solution

STEP 2: Systems with multiple capabilities

STEP 3: Automation-based approach to recovering data

STEP 4: Real time VM replication

STEP 5: The backup version of a virtual machine

STEP 6: A stimulation exercise

TESTING PROCEDURES:

Disaster recovery testing is the process to ensure that an organization can restore data and applications and continue operations after an interruption of its services, critical IT failure or complete disruption. It is necessary to document this process and review it from time to time with their clients. It will ensure that you know how to save your client in the event of any fail. Keep reading to learn more about disaster recovery testing scenarios and disaster recovery testing best practices.

FINAL PROJECT DOCUMENTATION

DISASTER RECOVERY USING IBM CLOUD VIRTUAL SERVERS

https://www.techtarget.com/searchdisasterrecovery/definition/disaster-recovery-DR-test

Disaster prevention radio and the telemetry system:

A telemetry system is used to monitor various disaster situations such as earthquakes, volcanos, floods, and environment as well as to operate DRR facilities on a real-time basis. A disaster prevention radio system in aims at sharing disaster information with local residents.

Disaster resilient materials:

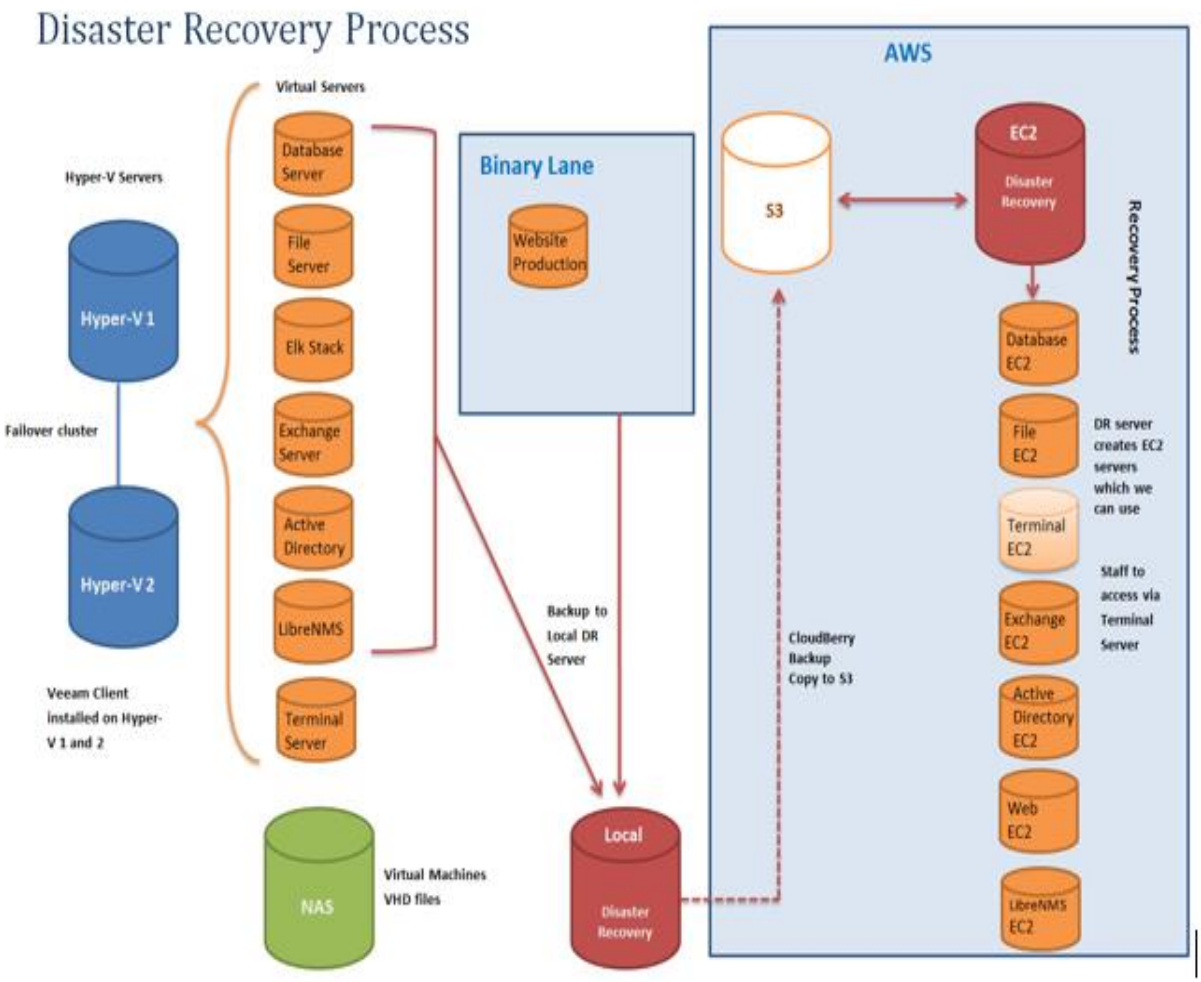
Various materials have been developed to mitigate damages caused by disasters. Waterproof materials are used for temporal measures to protect assets from flooding, while embankments, floodgates, and other structural measures are permanent solutions.

To manage fires it is most effective to finish interior decoration of walls and ceilings of buildings with fireproof materials that are hardly ignited with ordinary fire source or do not ignite.

Hazard mapping:

Hazard maps provide graphic information on the risks of disasters such as earthquakes, floods, landslides, tsunamis, and volcanic eruptions. They serve as a basis to formulate relevant policies and countermeasures of disaster risk

reduction. In addition, Japanese hazard maps include other information on evacuation routes, shelters, and response resources.



FINAL PROJECT DOCUMENTATION

DISASTER RECOVERY USING IBM CLOUD VIRTUAL SERVERS

Risk Assessment:

The first step in creating a DRP is to identify potential risks and vulnerabilities that could disrupt business operations. This includes natural disasters, cyberattacks, equipment failures, and more.

River engineering:

Every country has developed technologies for flood prevention and water resource management according to natural, topographical, and hydrological conditions. However, indigenous technology often has the limitation of the scientific basis. When Japan was established following the Meiji Revolution in the late 19th century, the country introduced western technology in river engineering for preventing floods and developing water resources. Other countries, such as Mexico and China, also started introducing river engineering from western countries, with the Japanese assistance.

Data Backup and Redundancy:

Regularly backup essential data and systems, both on-site and off-site. Utilize redundancy and failover mechanisms to ensure data and services remain accessible during disruptions.

Communication Plan:

Establish communication channels to keep employees, stakeholders, and customers informed during and after a disaster. Clear lines of communication are essential for coordination and trust.

FINAL PROJECT DOCUMENTATION

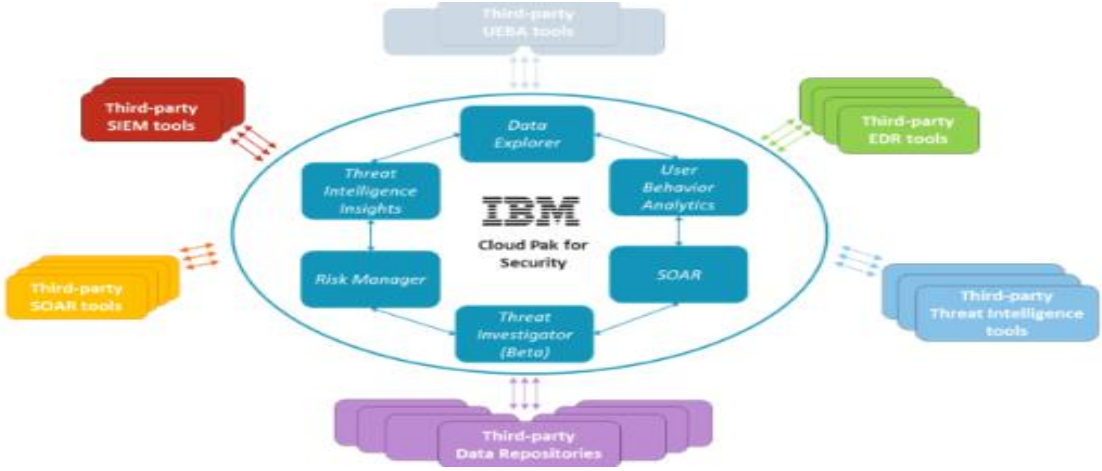
DISASTER RECOVERY USING IBM CLOUD VIRTUAL SERVERS

Architectures of disaster recovery with IBM:

https://www.ibm.com/cloud/architecture/architectures/resilience-active-active-standby

https://www.ibm.com/cloud/architecture/architectures/resilience-active-standby

https://www.ibm.com/cloud/architecture/architectures/resilience-active-active-passive



FINAL PROJECT DOCUMENTATION

DISASTER RECOVERY USING IBM CLOUD VIRTUAL SERVERS

Technology associated:

https://www.ibm.com/cloud/architecture/content/course/advanced-networking-for-vpc

IBM Cloud service:

https://cloud.ibm.com/docs/overview

https://cloud.ibm.com/docs?tab=all-docs

FINAL PROJECT DOCUMENTATION

DISASTER RECOVERY USING IBM CLOUD VIRTUAL SERVERS

Conclusion:

The digitalization journey is accompanied by new architectural models and technologies, such as microservices, containers, and exponential technologies in general. While they provide new opportunities to drive business through IT, they also bring new challenges to non-functional requirements and to resiliency. When new challenges arise, new solutions technologies are developed.
A solution for resiliency depends on SLAs to be met that in turn influence the technology and the topology that is selected for a solution architecture.

COLLEGE : NANDHA COLLEGE OF TECHNOLOGY

TEAM MEMBERS:

P.ADAIKAMMAI (Team leader)

M.SOWMIYA

E.KIRUTHIKA

U.VAISHNAVI

M.GOWTHAMI.

FINAL PROJECT DOCUMENTATION

DISASTER RECOVERY USING IBM CLOUD VIRTUAL SERVERS