Disaster Recovery with IBM Cloud Virtual Clouds

➢ Recovery options

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

- Failure scenarios: For each type of failure scenarios that could occur, ranging from small scale to very large-scale issues, how do you intend your system to respond?
- Recovery time objective (RTO): In the event of a failure, how quickly do you need to be able to recover to a functioning service? This influences whether you take a cold (infrequent backups), warm (periodic backups), or hot (fully redundant) standby approach to your deployment.
- Recovery point objective (RPO): What is the window of acceptable data loss in the event of a disaster? This calculation helps determine whether you need to implement live replication of data to a DR site (RPO=seconds/minutes), or if a backup approach is suitable (typically RPO=hours/day).

STEP 2: Systems with multiple capabilities

- In systems involving multiple capabilities, the answers to questions about the best recovery options will differ, depending on your judgement of how best to optimize your costs and effort to meet the specific business needs for each capability.
- Cloud Pak for Integration capabilities are typically middleware that provide integration between different systems of record—each of which has its own separate approach to disaster recovery. You must consider how your entire business environment is recovered in the event of a failure, and how disparate capabilities react when differently-timed snapshots of state are restored.

Types of data:

There are two key types of persistent data to consider when implementing your DR process for Cloud Pak for Integration:

Configuration data, which tends to come in two main types:

- Static or infrequently updated configurations that are owned or controlled by the administrator. These are stored in OpenShift objects such as operator subscriptions, custom resources (CRs), ConfigMaps, and secrets.
- Other infrequently changing persistent configuration state applied to a capability after its initial deployment, such as deployed API definitions and application subscriptions in IBM API Connect.

Dynamic runtime data. This is state that changes very frequently (such as every second or every minute), and outside the control of the administrator. This type of data results from an application or external entity's use of the system. Examples include messages being sent from and received by an IBM MQ queue, events sent to a topic in IBM Event Streams, and consumer applications subscribing to invoke APIs in API Connect.

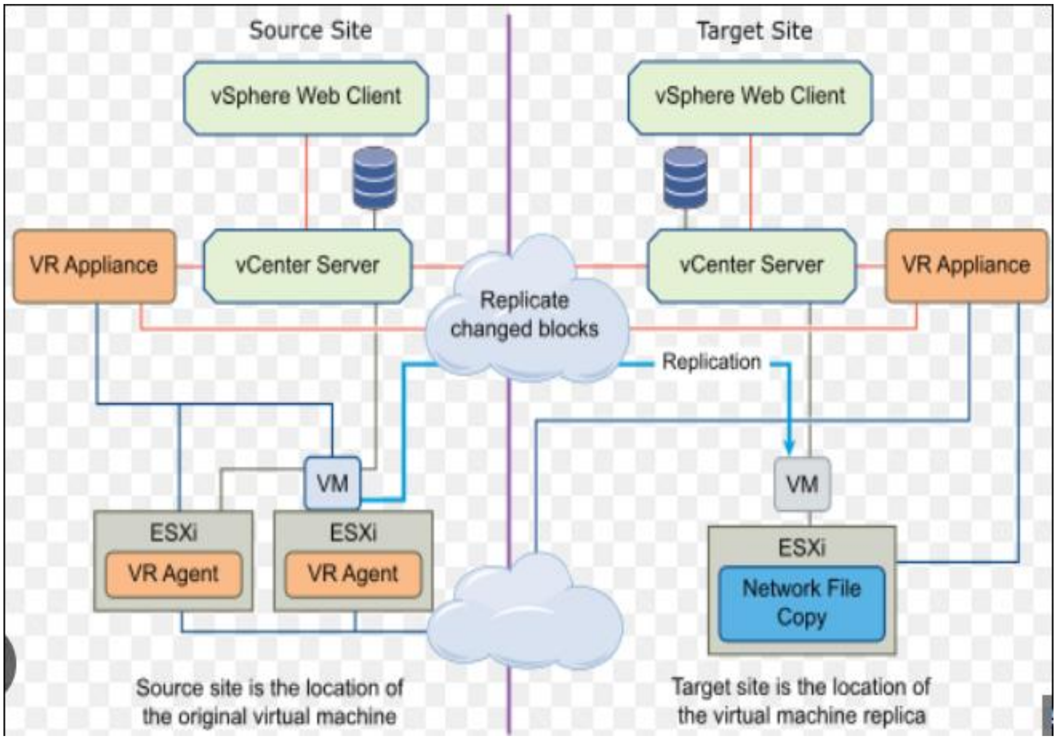
STEP 3: Automation-based approach to recovering data

Using automation techniques in your DR strategy ensures that at any point, you can rerun the deployment pipeline against a new cluster to create an instance with the same configuration state as the original. These techniques include infrastructure as code, CI/CD, and GitOps to manage versioning, and automating the deployment of capability instances from version control. Cloud Pak for Integration can be configured in this way by using your preferred tool, such as OpenShift Pipelines, ArgoCD, Tekton, or an equivalent.

The method you use for restoring dynamic runtime data will vary for each capability to reflect:

- The functional and non-functional characteristics of the runtime environment.
- The business domain in which those capabilities are used.

Virtual machine replication is a process used by information technology (IT) professionals to create backup versions of virtual machines (VMs) The backup can be kept and used to restore the machine in the event that its data is corrupted or lost.



There are two major types of virtual machine replication that provide organizations with various restore points:

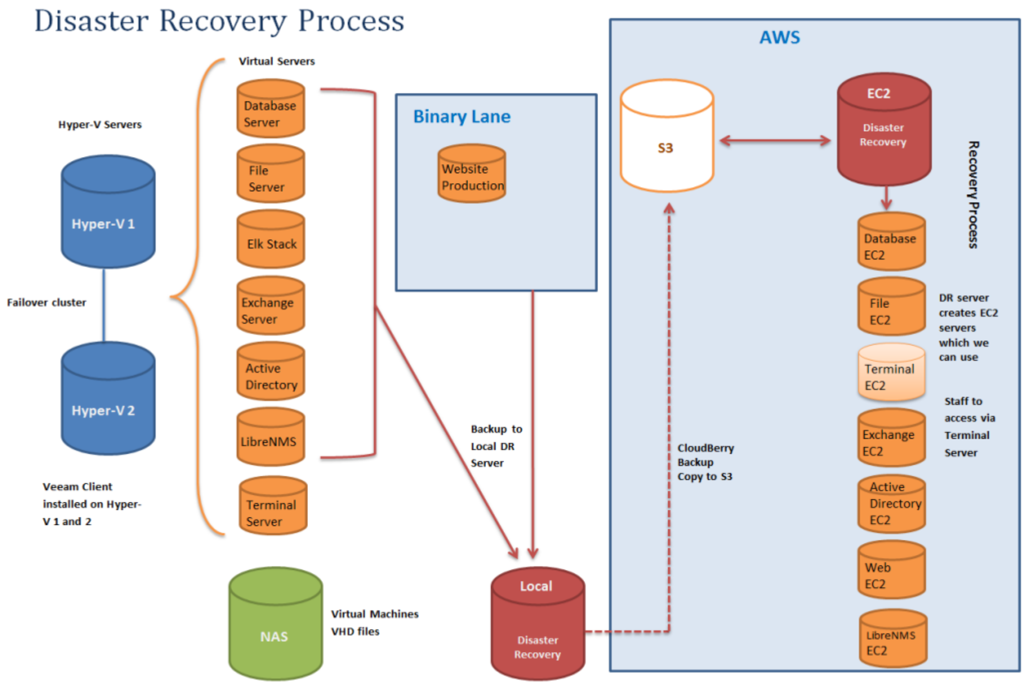
STEP 4:

- Real-time VM replication- Data is copied to the replicated VM as it is being written, giving the most precise backup. However, this requires a large amount of hardware and bandwidth.
- Point-in-time VM replication- This initiates data replication on a scheduled or requested basis.

STEP 5:

The backup version of a virtual machine may be created on the host where the original VM resides, a neighboring local host or a host somewhere remote to the organization. Computer professionals can configure their backup VM with a primary and secondary site.

In order to perform a replication, the primary and secondary sites must meet certain criteria. The primary site needs to provide all of the services available for the virtual machine and the secondary site is a place where those services can be migrated, whether in the same room or a separate remote site location. For added security, it is a good practice to host the secondary site somewhere that would not fall prey to disasters or weather events that could impact the primary site, like a fire or hurricane.



STEP 6:

A Simulation Exercise (SimEx) simulates an emergency situation to which a described or simulated response is made. The purpose of a simulation exercise is to validate and enhance preparedness and response plans, procedures and systems for all hazards and capabilities. WHO defines different types of exercises, including discussion-based table top exercises as well as operations-based exercises such as drills, functional exercises and field/full scale exercises.

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