



3

All monitoring and reporting of activity related to replication is handled through the Zerto Virtual Manager interface – in 1 place, as opposed to SRM monitoring done in several different places.

All protection configuration is done from the Zerto Virtual Manager interface, instead of through vCenter in various places – compared to SRM using vSphere Replication.

No array-based replication requirements for Zerto. The solution is both storage AND hypervisor agnostic and can also protect across different versions of hypervisor.

2

1

Zerto Virtual Manager

vSphere Web Client

Business Stakeholder/Engineering

Start Phase 3

Create VPG for each protection group, or per VM (based on preference and priority)



Pre-Requisites

- ZVM installed on each site.
- vCenter or hosts in each site identified for use.
- WAN connectivity established between sites, including any required firewall rules
- ZVM Sites paired
- VRA deployed to each host in protected and recovery cluster(s)/host(s).
- > 5Mb/s WAN connectivity

- Set replication priority
- Select VM(s)
- Define boot order
- Select recovery destination options (host, datastore, journal history, target RPO alert, WAN Compression)
- Define networks for testing and recovery
- Set IP Address options (recovery and testing)
- Configure offsite backup if needed.

Monitor and report on protection status, RTO, RPO, issues/errors/alerts.

Disaster?

No

Run routine recovery testing as scheduled.

END

Failover to Recovery Site

Re-protect

Start Phase 2

- Create Folder to house Zerto VRAs and ZVM
- Exclude ZVM and ALL VRAs from VADP backups due to corruption caused by snapshots. (Exclude by folder)
- Create recovery folder structure in recovery site
- Create test/recovery networks if new.

Move to Phase 3

Design support procedures and issue mitigation process as related to replication

Problems?

Yes

Move to Phase 2

- Identify application(s) and dependencies
- Identify workloads to protect
- Determine validate availability for required resources for VRAs in the cluster to protect
- Determine recovery host(s) or cluster(s)
- Determine recovery datastore requirements
- Determine what network to recover to
- Determine what network to test on (should be isolated)
- Define recovery test plan, dependencies, and frequency
- Design disaster recovery plan
- Determine RTO/RPO
- WAN-sizing based on change rates to determine initial replication time estimates
- Design monitoring, reporting, and alerting plan for replication jobs.

Identify need for Replication & Protection Service

START HERE