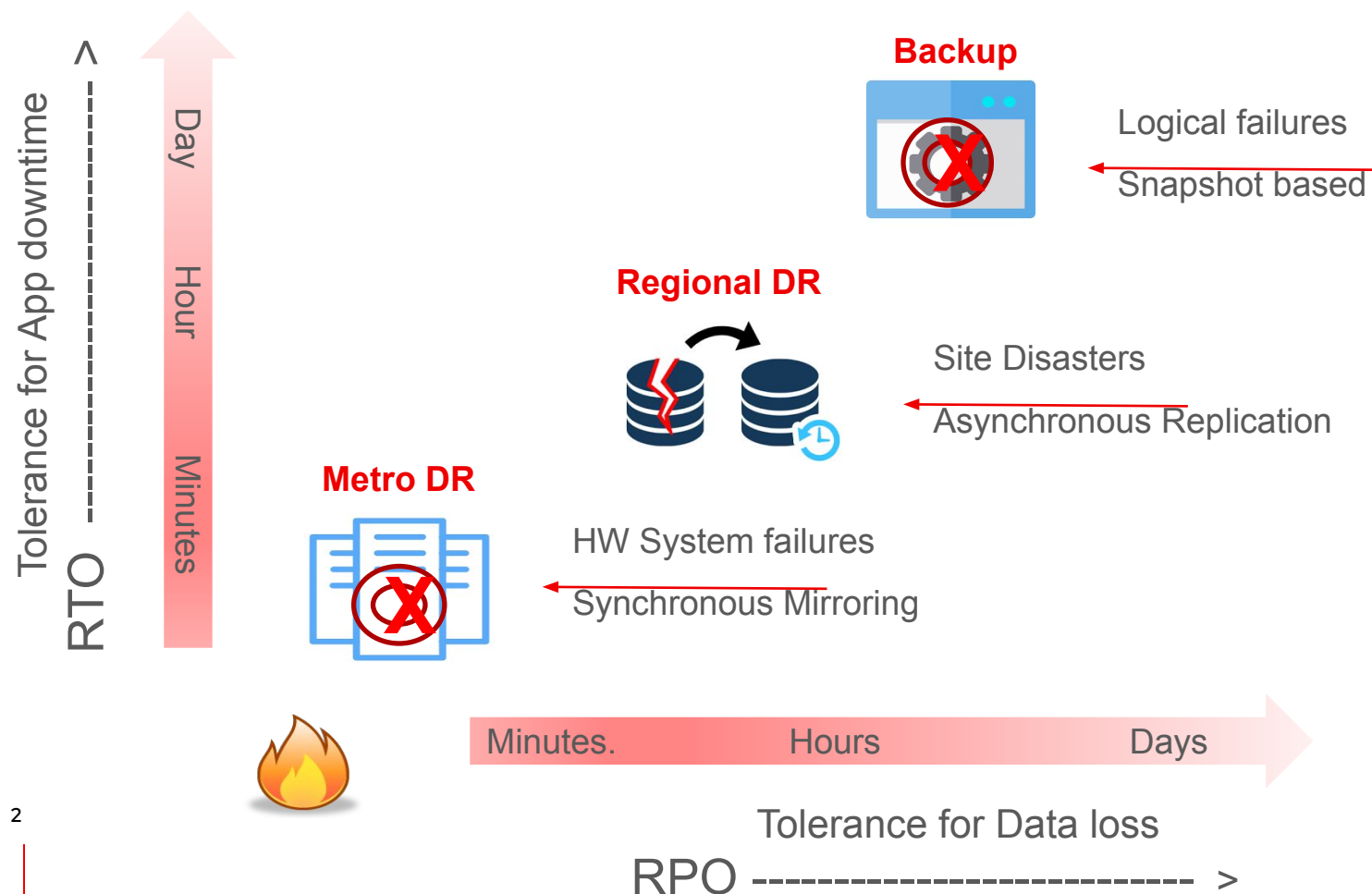




# HA-DR for Stateful Applications on OpenShift

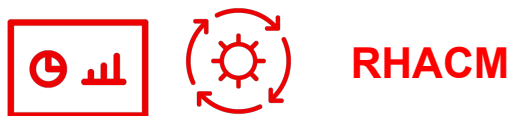
# Resiliency Solutions for different service level objectives



- ▶ Comprehensive protection solutions against wide spectrum of failures
- ▶ Beyond Data Protection --> Full Application protection
- ▶ Resiliency built into the platform – Available to all stateful and stateless applications on OpenShift
- ▶ OCP + ODF + ACM integrated stack lends towards Automated and Simplified Application granular protection

# OCP Integrated, Full Stack DR Protection

Multi-Site  
Multi Cluster  
Manager



- ODR Hub Operator – Orchestrates & Automates DR operations across clusters

Platform



- ODR Cluster Operator – Manages and synchronizes cluster meta data and application data

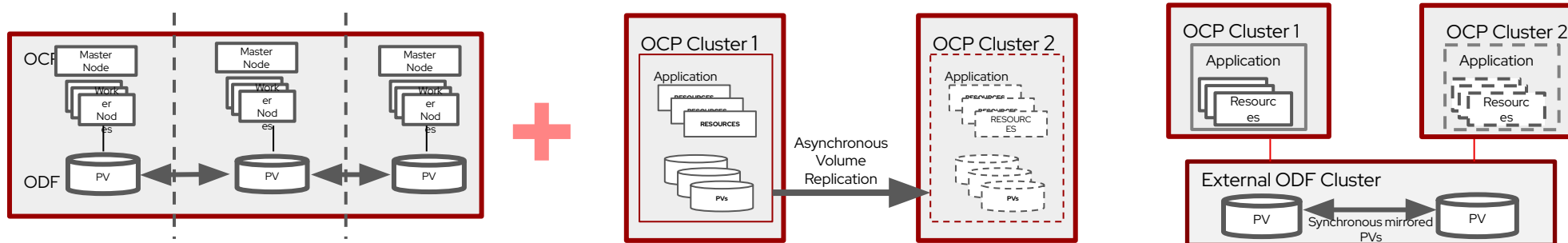
Persistence  
Layer



- Asynchronous replication of Application volumes – or –
- Synchronous Mirroring of Application volumes

- Easy configuration DR across cluster and sites as part of application deployment
- Automated DR Failover and Failback operations reduces RTO
- Manage and Monitor DR across clusters and Apps
- Same consistent DR operations for both Metro-DR and Regional-DR
- Both Application Data and State is protected and used for Application granular protection
- Consistent Data replication or mirroring or both based on infrastructure and desired protection.

# OCP Cluster HA + DR for stateful Applications



## Cluster HA

## Regional-DR

## Metro-DR

Topology	Single OCP+ODF clusters deployed over multiple AZs in a single region	Multi OCP + ODF clusters spread over multiple regions	Multi OCP clusters + single external ODF stretched cluster deployed over low latency networks
RTO (Downtime)	RTO=0 (Continuous)*	RTO = minutes DR Automation from ACM+ODF reduces RTO	RTO = minutes DR Automation from ACM+ODF reduces RTO
RPO (Data loss exposure)	RPO=0 No Data loss due due to Synchronous mirroring of ODF data	RPO > 0; Usually 5 min or higher Depends upon network bandwidth & change rate	RPO=0 No Data loss due due to Synchronous mirroring of ODF data
Infra Requirements	Multi-AZ supported public clouds (vSphere support in OCP 4.10)	All ODF supported platforms No network latency limits	On-prem only (vSphere, bare metal) <10ms network latency between sites

V0000000

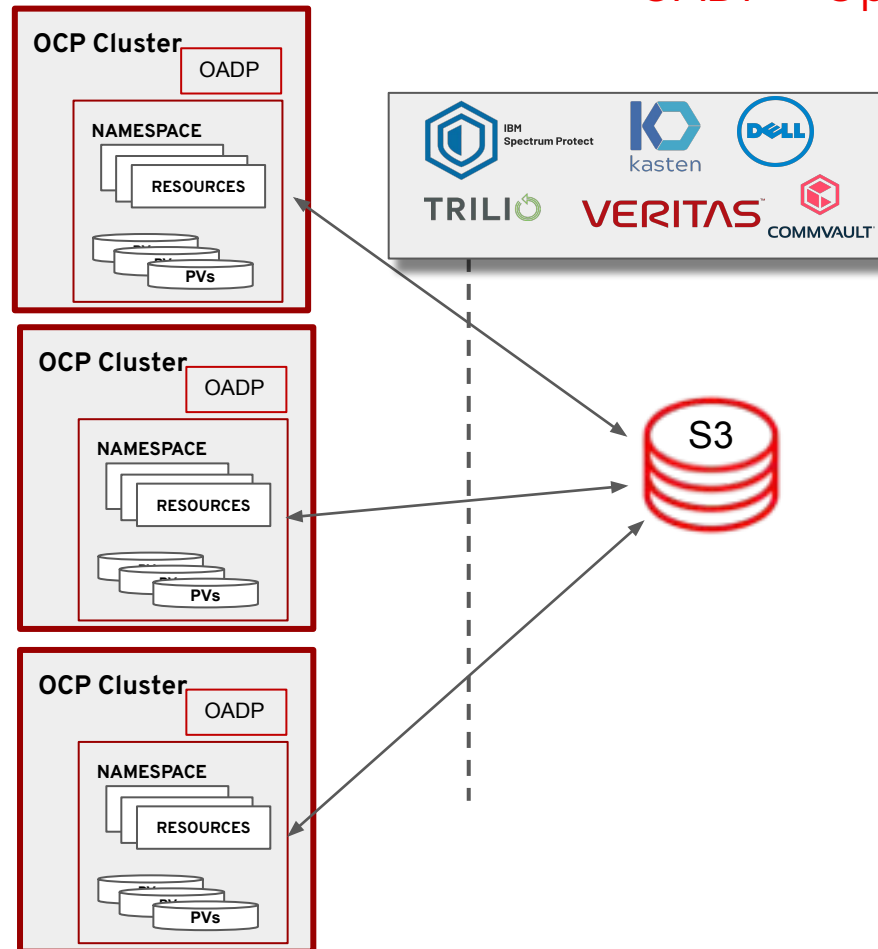


\* Subject to RWO PV limitations

# Solution Overview

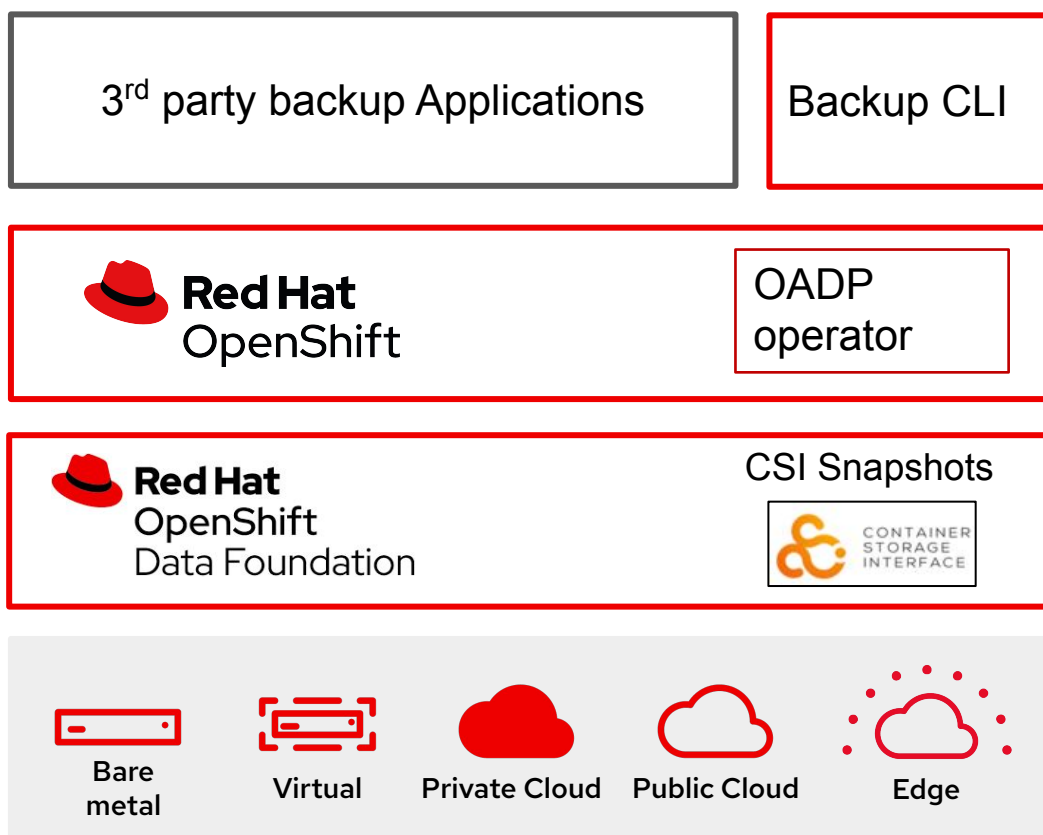
# OpenShift Backup Solution

## OADP – OpenShift API for Data Protection



- ▶ Application granular, cluster consistent backups with OADP
- ▶ OpenShift App backup protection with eco-system of broad Backup Partner ISV partners
- ▶ Snapshots with CSI interface from ODF ensures backups with open standards

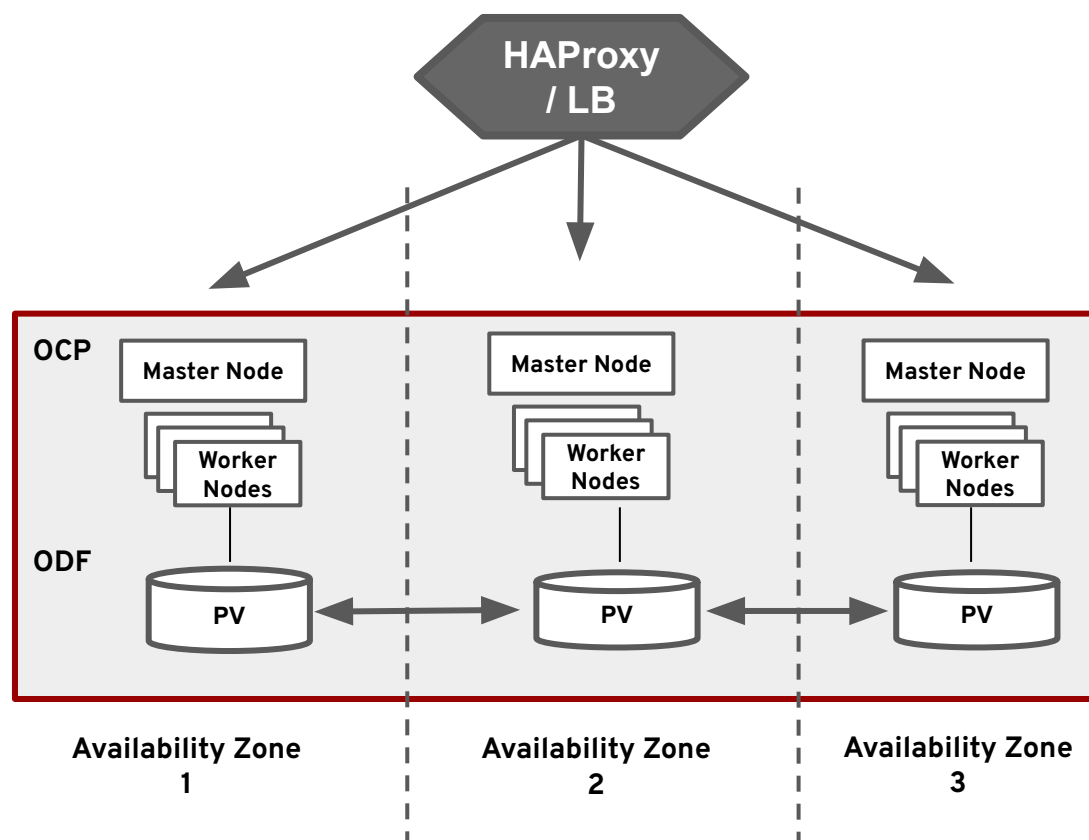
# OCP Application Backup – Key Components



- Third party backup Applications /native CLI
  - Handles Backup policy management, backup scheduling, retention and restore management and data movement
- OADP – OpenShift App Data Protection API
  - Enables namespace or label scoped backups with all ensuing cluster resources and application data (PVs)
  - Ensures OCP version independence and works across storage providers (via plug-ins)
- ODF PV Snapshots via CSI
  - PV/PVC backups of ODF volumes through standard CSI interfaces
  - Can be used with or without OADP

# Application HA

## Multi-Zone spanning Cluster for local HA

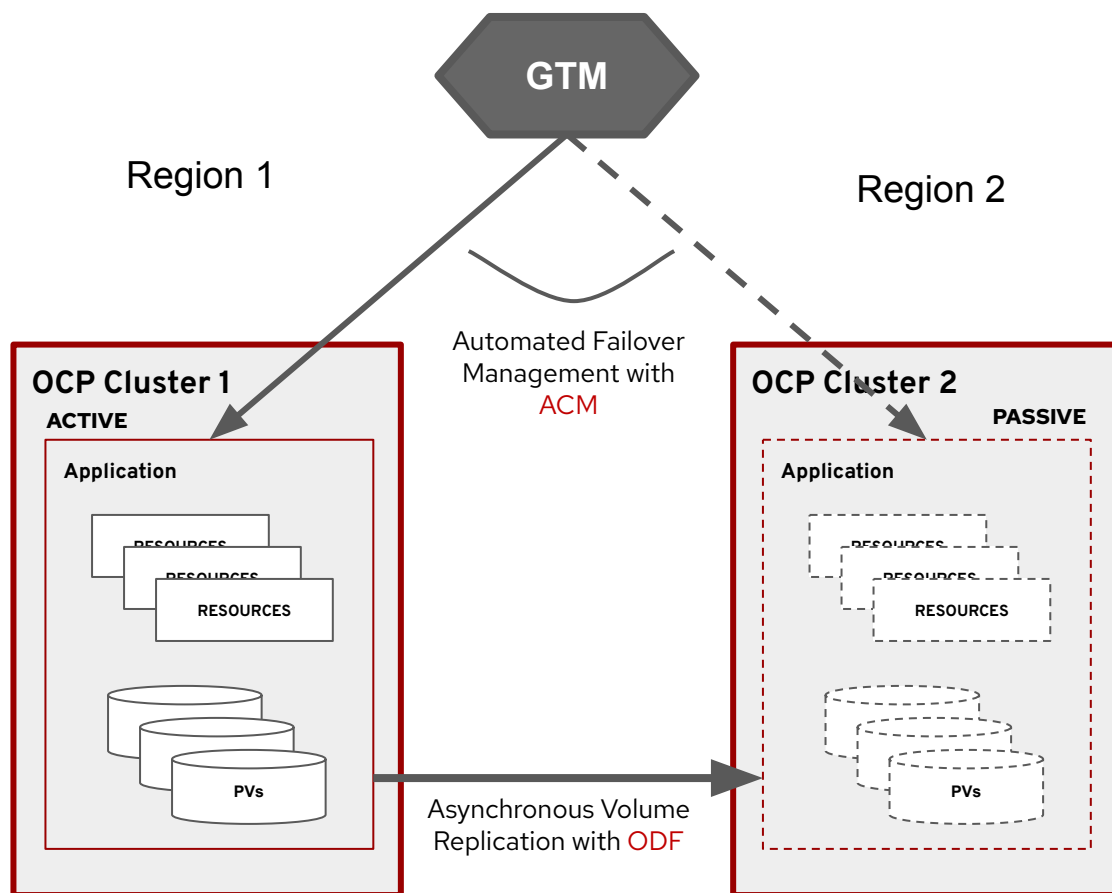


- ▶ HA for Stateful Applications deployed on cluster that is stretched across Availability Zones within a region
- ▶ Installer ensures that resources are deployed across all AZs making the cluster resilient against failures of any single AZ
- ▶ ODF provides synchronous consistent copies in all AZs ensuring no data loss during zone failures
- ▶ Suitable for public cloud platforms with Regions supporting 3 or more AZs
  - Can be deployed on-prem when AZs are connected by networks with <10ms latency



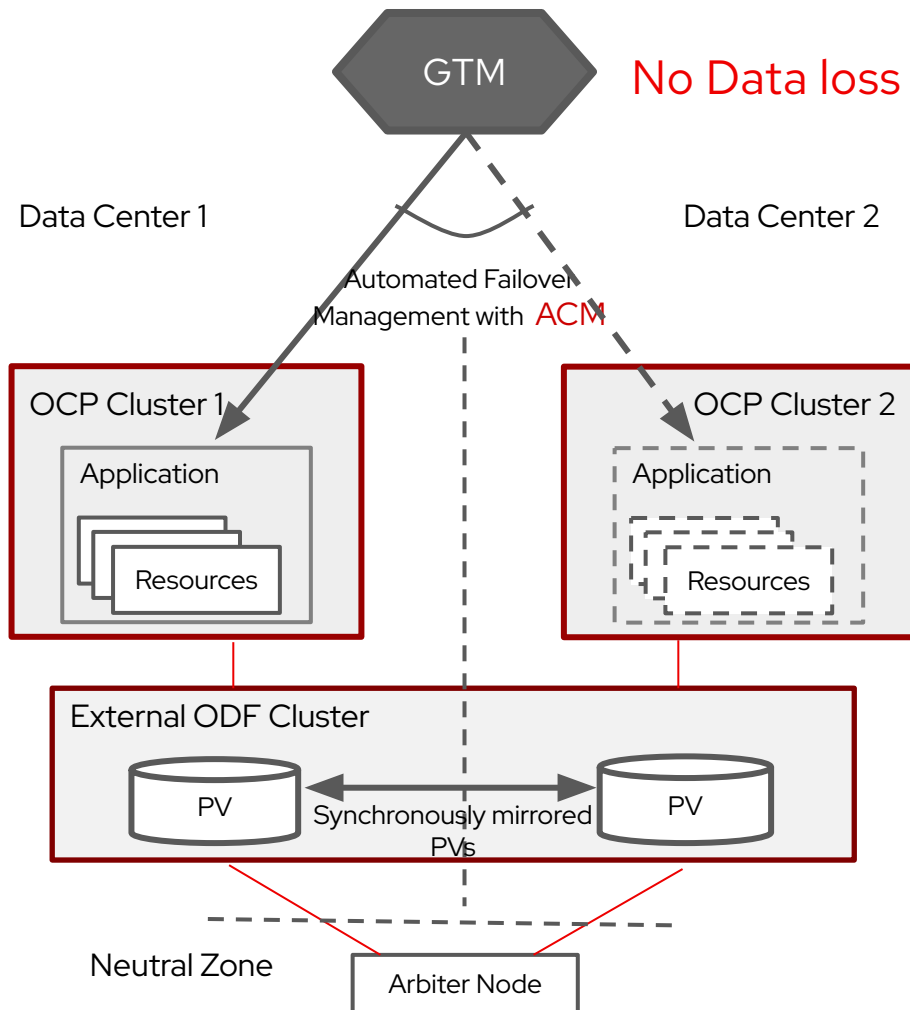
# Regional-DR with Failover Automation

## Protection against Geographic Scale Disasters



- ▶ Asynchronous Volume Replication => low RPO
  - ODF enables cross cluster replication of data volumes with replication intervals as low as 1 min
  - ODF Storage operators synchronizes both App data PVs and Cluster metadata
- ▶ Automated Failover Management => low RTO
  - ACM Multi-Cluster manager enables failover and failback automation at application granularity
- ▶ Both clusters remain active with Apps distributed and protected among them

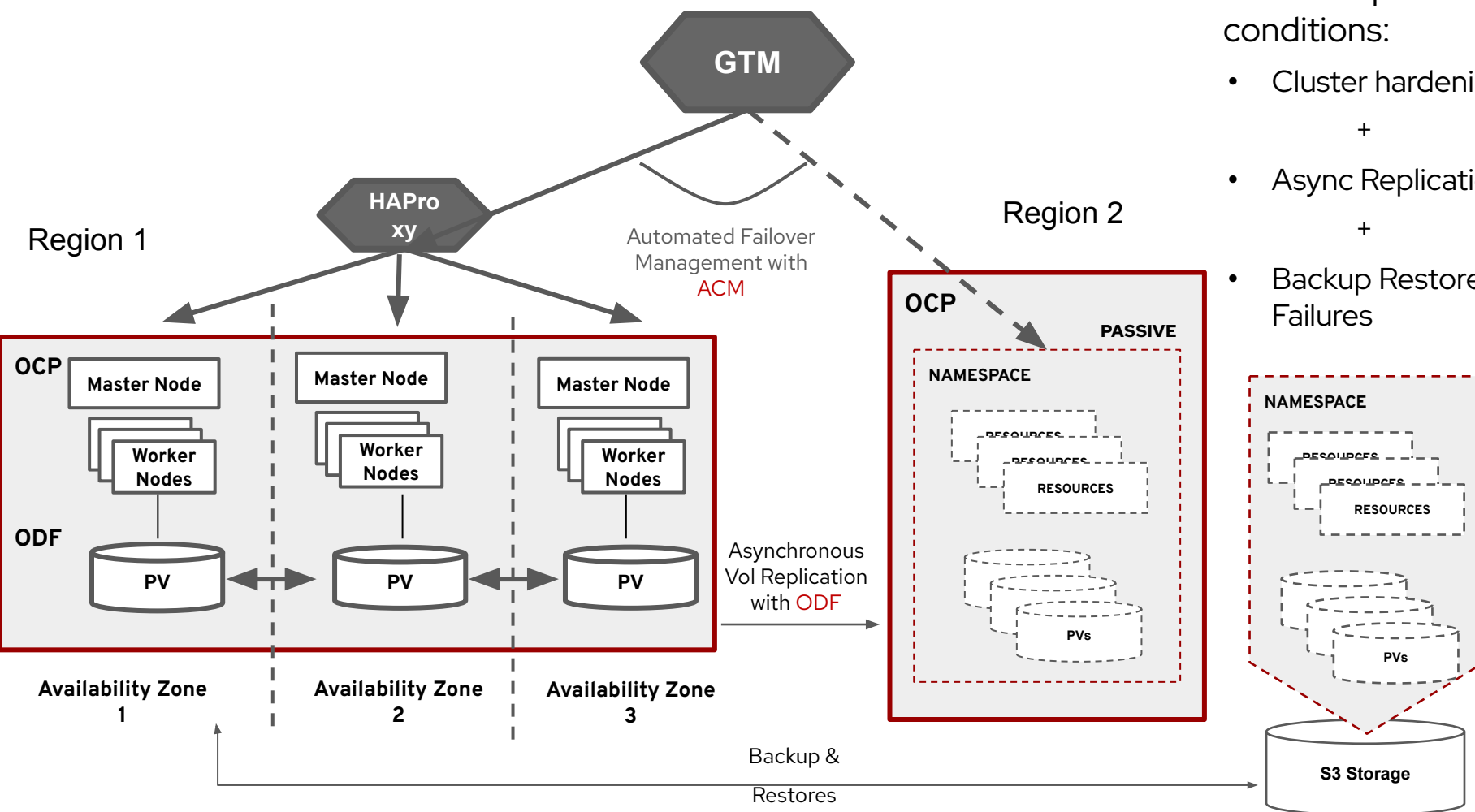
## Metro-DR – Multi Cluster



No Data loss Data Mirroring, across multiple OCP clusters

- Multiple OCP clusters deployed in different AZs provide a complete fault isolated configuration
- External RHCS storage cluster provides persistent synchronous mirrored volumes across multiple OCP clusters enabling zero RPO
- ACM managed automated Application failover across clusters reduces RTO
- Requires Arbiter node in a third site for storage cluster
  - Arbiter node can be deployed over higher latency networks provided by public clouds

# Comprehensive & Flexible Data Protection for the desired SLO (RPO+RTO)



Multi-tier protection against various failure conditions:

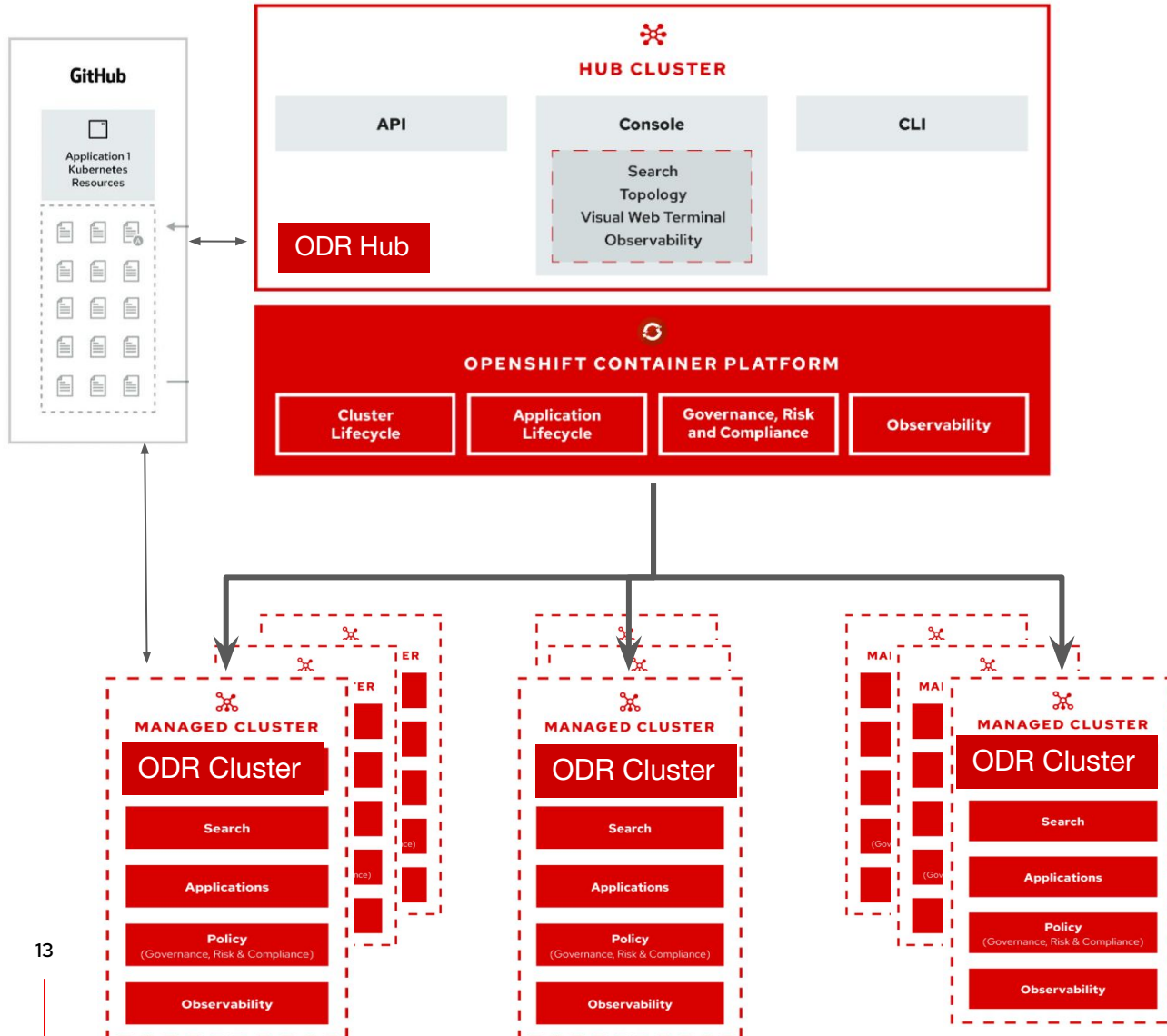
- Cluster hardening with Multi-Zone spanning OCP cluster.
- +
- Async Replication for HW and Data Center Failures
- +
- Backup Restores from Snapshots for Software & Logical Failures

# RH-ACM Based DR Automation

DR Automation reduces  
RTO

# RHACM Managed DR Automation

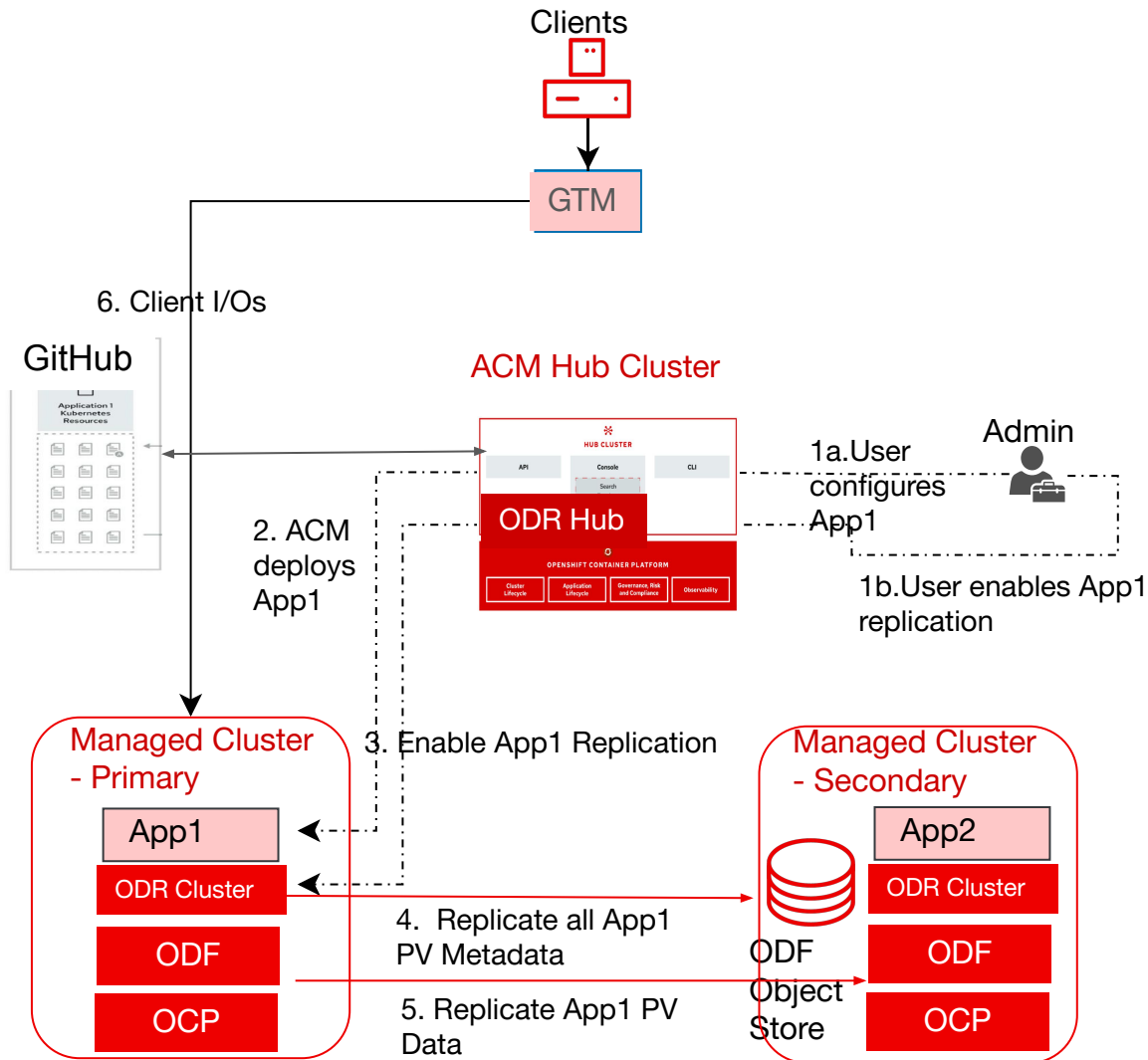
CONFIDENTIAL designator



- ▶ ACM provides DR management and monitoring across multiple clusters.
- ▶ ACM drives placement of DR enabled applications based on capacity and policy
- ▶ DR Orchestration through the centrally managed RH-ACM Hub via ODR Hub operator
- ▶ ODR Cluster Operator on each managed (workload) cluster manages data replication and synchronization
- ▶ ACM Hub cluster is recommended to be placed in a zone neutral to managed clusters

# ODF & ACM enables easy DR Configuration

CONFIDENTIAL designator



- ▶ Ensures both Application state and Data are replicated and protected
  - Uses ODF Object Store to capture App meta data
- ▶ Provide active-active use of both sites, where different applications can be deployed to each site cross replicating to each other
- ▶ Flexibility for replica copy to have different storage configuration than primary

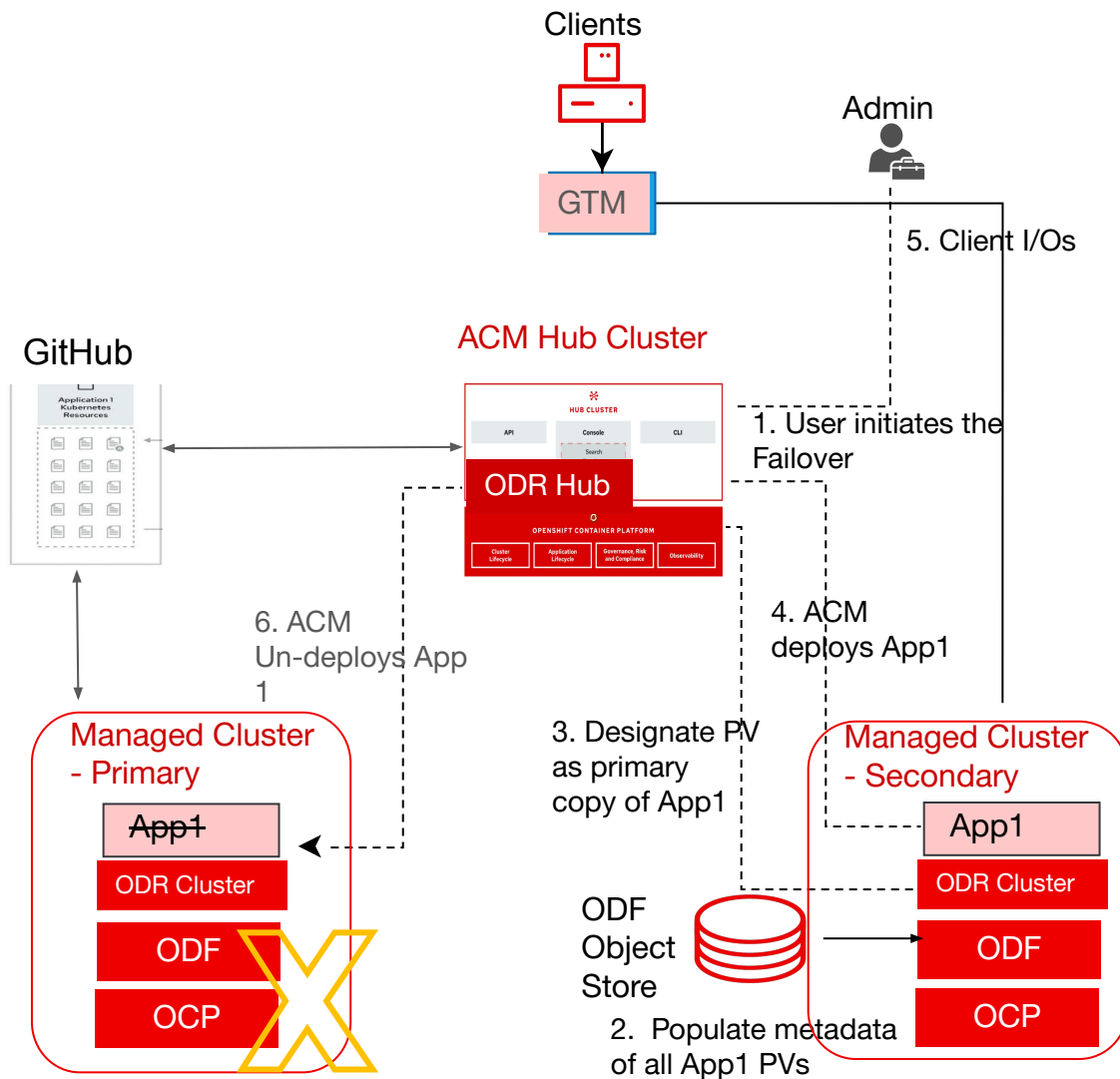
A Centrally deployed ACM Hub managing DR between a pair of Managed clusters deployed at different regions

V0000000



# Automated DR Failover reduces RTO

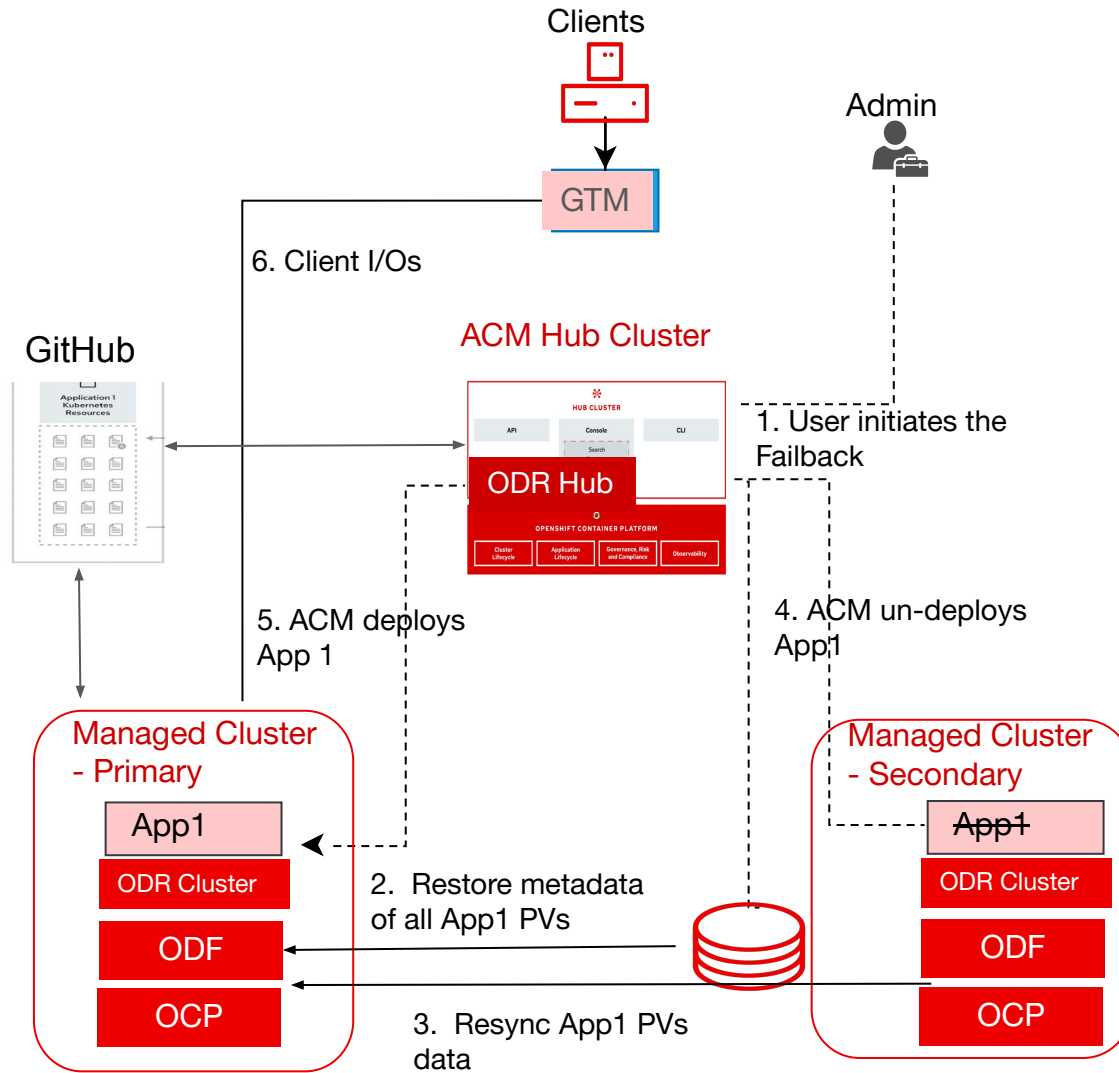
CONFIDENTIAL designator



- ▶ Failover process automation – Increases application availability and reduces user errors
- ▶ Application(s) granular Failovers and Policy based prioritized failovers
- ▶ Failovers are always user initiated and controlled, eliminates un-intended switch and data loss.
- ▶ ODR Hub ensures App metadata is populated before the failover to ensure Apps binds to the right PVs

# DR Failback ensures smooth recovery to Primary

CONFIDENTIAL designator




- ▶ PV Data changes and meta data changes are restored to primary cluster before the fail-back is complete
- ▶ Fail-back operations are user initiated and controlled
- ▶ Workload migrations across hybrid platforms are also enabled with the same process



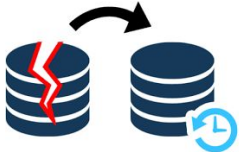
# OpenShift Resiliency Solution Roadmap

CONFIDENTIAL designator


Backup



Regional DR



Metro DR



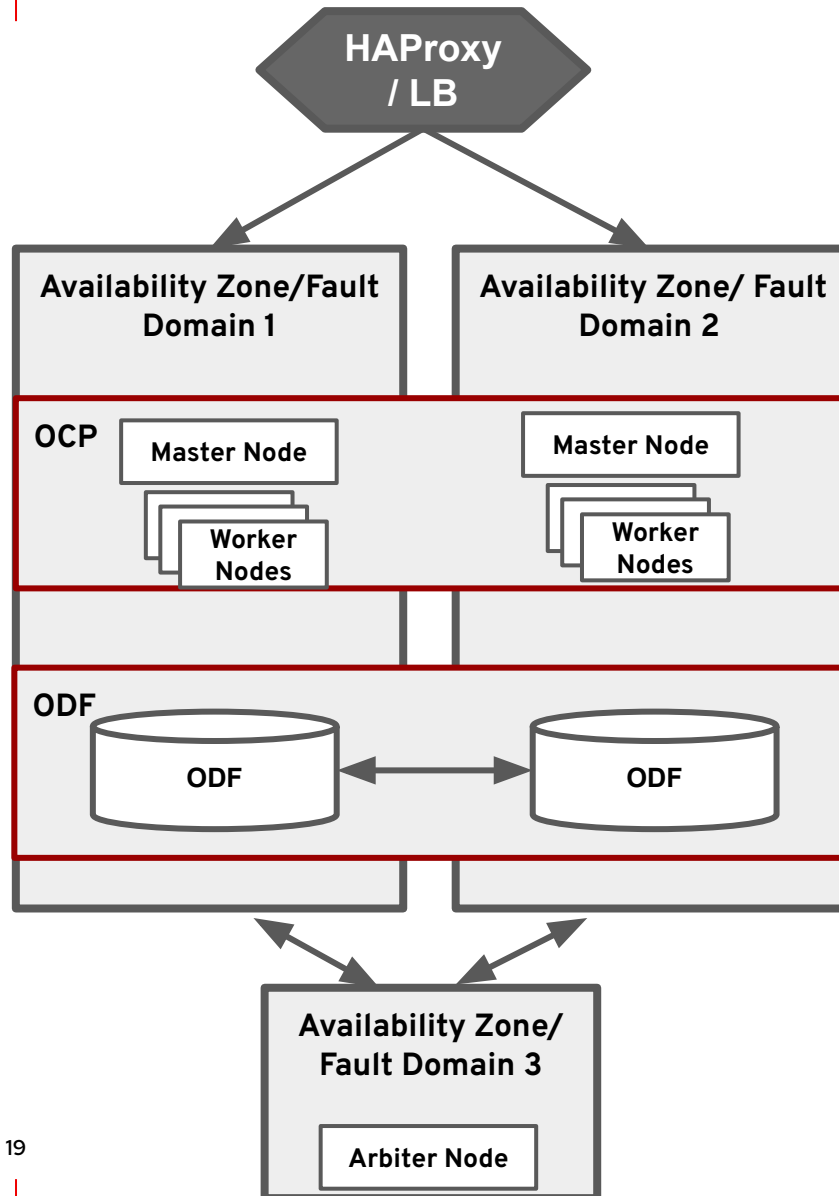
1H 2022	2H 2022
<ul style="list-style-type: none"><li>RedHat OADP Operator (Feb '22)</li></ul>	<ul style="list-style-type: none"><li>Native OCP DP<ul style="list-style-type: none"><li>Differentiated from Partner solutions</li></ul></li></ul>
<ul style="list-style-type: none"><li>Regional DR (GA) - May '22<ul style="list-style-type: none"><li>Block (RBD) only</li><li>Simplified Orchestration</li><li>Resilient ACM Hub</li></ul></li></ul>	
<ul style="list-style-type: none"><li>Metro-DR (GA)<ul style="list-style-type: none"><li>Multi-Cluster, ACM Managed</li></ul></li></ul>	

# Alternate DR Solutions

# Two Zone Stretch Cluster

CONFIDENTIAL designator

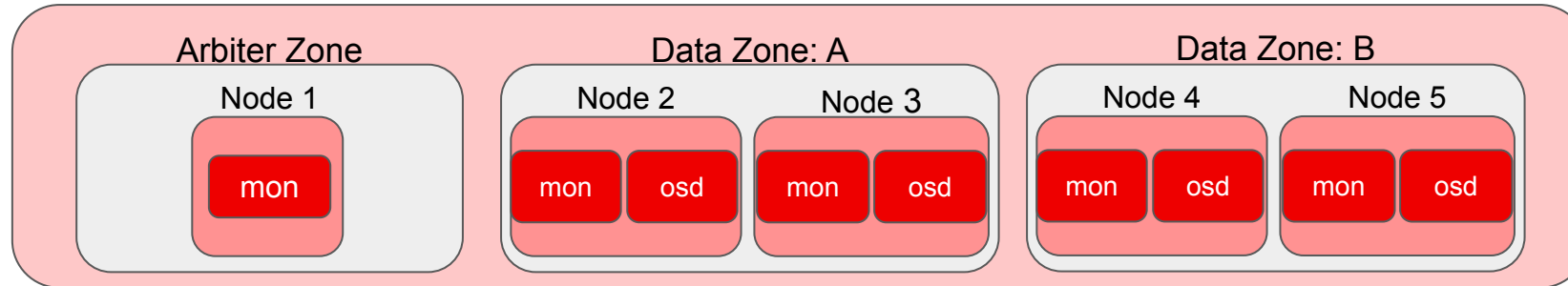
RPO – 0  
RTO – Mins



*No Data loss Data Mirroring, across 2 sites*

- ▶ Stretch OCP-ODF Cluster across 2 AZs
  - Data replicated across 2 AZ/sites connected by low latency networks
- Arbiter for Cluster quorum in a neutral AZ/site
  - Minimal resource requirements for Arbiter node – contains ODF Mon process and OCP Master node
- Failure of any node or resource on one AZ triggers automatic redirection of traffic to its cluster pair.

# Stretch Cluster Configuration



- ▶ Two local copies per data zone for local HA.
  - Requires Replica 4 configuration
- ▶ Two Monitors are required for each data zone
  - A zone is considered down by ODF when all the mons in the zone are unavailable.
- ▶ Rook to detect the topology labels of the nodes set by the user and manages ODF resources accordingly

# Thank you!

 [linkedin.com/company/red-hat](https://linkedin.com/company/red-hat)

 [youtube.com/user/RedHatVideos](https://youtube.com/user/RedHatVideos)

 [facebook.com/redhatinc](https://facebook.com/redhatinc)

 [twitter.com/RedHat](https://twitter.com/RedHat)