Disaster Recovery for Kubernetes (Files, Containers, or Clusters)

SOLUTIONS BRIEF

Software-Defined Continuity That is Adaptive to The Infrastructure

THE CHALLENGE

Disaster recovery (DR) is a last-resort plan to maintain business continuity, even if a critical piece of infrastructure unexpectedly fails. Unfortunately, because DR workflows are static the conventional approach to DR is prone to errors and rarely tested. Also, DR workflows quickly become obsolete as infrastructure, apps, and data locality changes – an issue especially concerning in Kubernetes environments.

DR solutions do not adapt in real-time; they are only bolt-on point solutions that don't understand the dynamic nature of the infrastructure or the data they are designed to protect. The problem compounds when you add Kubernetes and hybrid cloud to the equation. You must ask yourself the question, "If the worst happens, how certain am I that our DR plan will work?"

THE SOLUTION

Hammerspace takes a data-centric approach to file data in the cloud, serving and managing it independently from the infrastructure. Built for the hybrid multi-cloud, Hammerspace serves data at high-performance to any site across the hybrid multi-cloud. Hammerspace abstracts data from the infrastructure, making it easy to define DR policy objectives through metadata so that recovery can be fully automated across sites at file, application, or site granularity.

To span data management across the hybrid multi-cloud, Hammerspace separates the control plane (metadata) from the data plane (data) reading, writing, and moving data across sites through a Global File System, at file level granularity. Hammerspace metadata servers are present at each site, replicating metadata so that every site has a complete view of all data, with the assistance of machine learning-driven automation to direct resource optimization. When non-local data is accessed, Hammerspace moves data live to where it needs to be, even while actively being read/written. DSX data services are architected to scale-out on-demand so that performance is parallelized to meet application SLAs. Hammerspace key management server (KMS) integration encrypts all

AGILITY, CONTROL & EFFICIENCY

Simplify DR for files, containers, and clusters

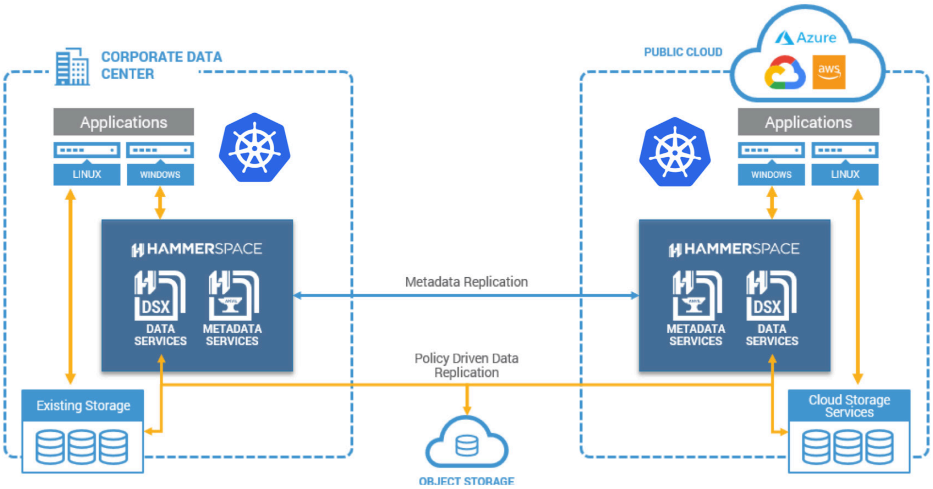
- File, container, or site granular
- Active-active across sites
- Any cloud, any storage
- Define RPO/RTO by application SLA

DR workflows are always current

- Resilient to infrastructure changes and migrations
- Error-free recovery
- Easy, non-disruptive DR testing

DR as a policy, not a point-solution

- Data policies follow the data
- Optimize for global data reduction
- DR is an integrated data management policy



data stored and moved across the cloud; and data is protected by services like snapshots, undelete, and replication to defend against the loss of infrastructure.

AGILITY: SIMPLIFY DR FOR FILES, CONTAINERS, AND CLUSTERS ACROSS THE HYBRID MULTI-CLOUD

Since Hammerspace manages application data through the metadata and as data is being written to the Global File System, data protection policies direct which sites and storage that data gets placed on to defend against disaster. The traditional approach to DR pushes data from storage to the target DR site. Hammerspace takes it a step further, at local sites machine learning intelligently keeps the most important data close to the application to meet performance SLAs with an RPO/RTO defined by the applications themselves. This makes for easy and error-free hybrid cloud DR recovery from any storage to any site, even if apps move or if the infrastructure has changed over time.

CONTROL: DISASTER RECOVERY WORKFLOWS ARE ALWAYS CURRENT

When users access data through the Global File System, metadata-driven policy objectives keep data safe even as infrastructure changes over time. IT can add or remove storage infrastructure; perform data migrations; or implement new compliance or security rules; but with Hammerspace, none of these things will upset your DR workflow. As Hammerspace manages data independently from storage, data management and protection activities like DR are resilient to changes at the infrastructure layer. Hammerspace protects data at every level of granularity from files, to apps, to sites. With policy-driven DR, it is trivial to change your target DR location or to non-disruptively perform DR testing

EFFICIENCY: DISASTER RECOVERY AS A METADATA POLICY OBJECTIVE

With Hammerspace, DR is simply a policy objective applied through the metadata so that data protection and DR policies follow data anywhere across the infrastructure – continuously optimizing data placement across the infrastructure to meet those objectives. With Hammerspace, the Universal Global Namespace enables DR to be active-active across all sites, autonomically copying data to DR targets leveraging global data reduction. No longer should DR be considered a point-solution; it is simply a policy objective managed through metadata like any other data management policy.

ABOUT HAMMERSPACE

Hammerspace is storageless data for hybrid cloud Kubernetes environments. By untethering data from the infrastructure, Hammerspace overcomes data gravity to provide dynamic and efficient hybrid cloud storage as a fully automated, consumption-based resource. Users self-service their persistent data orchestration to enable workload portability from the cloud to the edge.

To learn more, visit us at www.hammerspace.com or on Twitter @Hammerspace_Inc