ESG First Look

Protecting Kubernetes in the Enterprise with Metallic Services from Commvault

Date: January 2021 **Author:** Vinny Choinski, Senior Validation Analyst; and Christophe Bertrand, Senior Analyst

Data Protection Challenges:

85% The percentage of organizations that believe **application consistent backups across multiple containers** is critical or very important.[1]

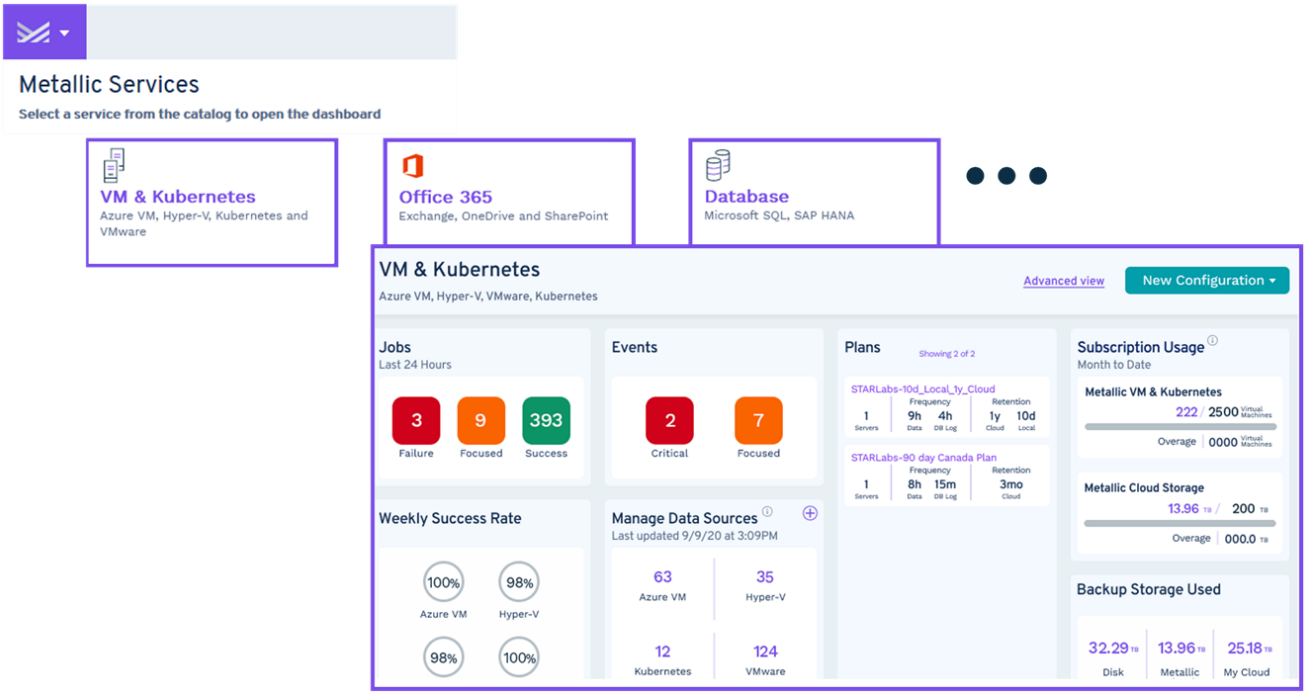
44% The percentage of respondents who identify **managing backup/recovery of container-based applications** in hybrid cloud environments as one of their biggest challenges related to managing backup/disaster recovery for container environments.

Container adoption is accelerating and so too is the requirement to properly protect container environments and the data in them. ESG research indicates that, so far, IT professionals are often just kicking the can down the road. While many organizations recognize the growing importance of containers relative to other vital application platforms, their confidence levels in their ability to protect containerized workloads are lagging.

Metallic for VM & Kubernetes

Metallic is a cloud-based, SaaS-delivered solution that provides fast, easy enterprise-grade data backup and recovery for businesses. It is easy to install and designed to scale as your business grows. The Metallic VM & Kubernetes Backup Service delivers cloud-native protection for your applications as they are virtualized and modernized with container technology. Figure 1 shows how the many different Metallic services are accessed from the main Metallic page and the ecosystem visibility that the intuitive VM & Kubernetes dashboard provides.

Figure 1. Metallic Services Tiles and VM & Kubernetes Dashboard



[1] Source: ESG Master Survey Results, *Data Protection Considerations for Containers*, 2020. All ESG research references in this First Look have been taken from this Master Survey Results set.

The key Metallic for VM & Kubernetes benefits include:

- **BaaS deployment:** Metallic is deployed in minutes as a cloud service, with no backup infrastructure to manage, automatic updates, or flexible subscription model.
- **Hybrid cloud flexibility:** Metallic supports native Kubernetes protection for on-prem, hybrid, and public cloud deployments. It offers multiple options for backup data storage targets, including the flexibility to leverage existing investments in cloud or on-premises storage or to leverage the highly scalable Metallic Cloud Storage. Metallic also supports the Kubernetes Container Storage Interface (CSI) integration.
- **Workload support:** Metallic supports all CNCF-certified distributions, offers native API-SERVER integration, and delivers application-consistent protection.
- **Data protection agility:** Metallic easily protects, recovers, and migrates containerized applications.

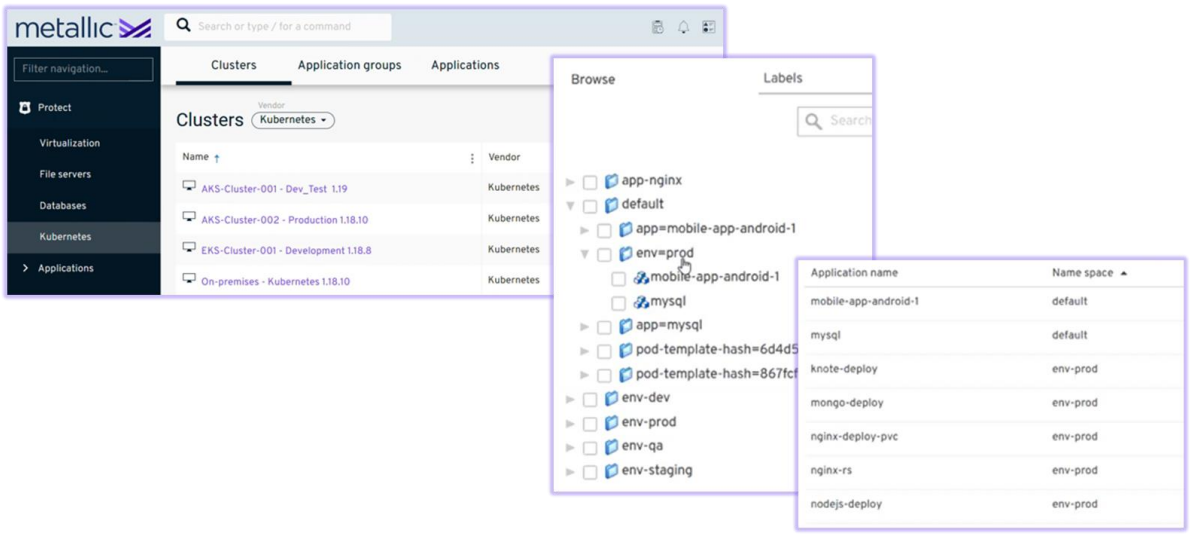
ESG Lab Demo Highlights

ESG performed a detailed evaluation of the Metallic VM & Kubernetes data protection solution by participating in a solution briefing and a detailed hands-on demo hosted by Commvault subject matter experts. The evaluation focused on highlighting the solution's native integration, flexible deployment options, automation and scalability features, and flexible recovery options and capabilities.

Enterprise Class Data Protection Management

As shown in Figure 2, ESG started the evaluation process by clicking on the Kubernetes tab on the left side of the Metallic management interface, which then displays three options (Clusters, Application groups, and Application) at the top of the center management window. Here, under *Clusters*, we saw a summary of the Kubernetes clusters being protected in the demo environment. Metallic for VM & Kubernetes has all the enterprise-class data protection features a data protection professional would expect to help them meet the data protection requirements of the modern enterprise. This includes the ability to create data protection policies with granular selection of containerized applications and objects, retention period, frequency schedules, consistency settings, and the ability to monitor their success rate. When used efficiently, policies help IT align data protection attributes with the lifecycle of containerized applications. For instance, one policy might be specifically designed for production and another for development. The middle of Figure 2 shows how Metallic uses label tags to help automate policy designation at scale. Here we see two applications, an android mobile app and a database app, tagged with the label *env=prod* that can be used for automatic policy assignment.

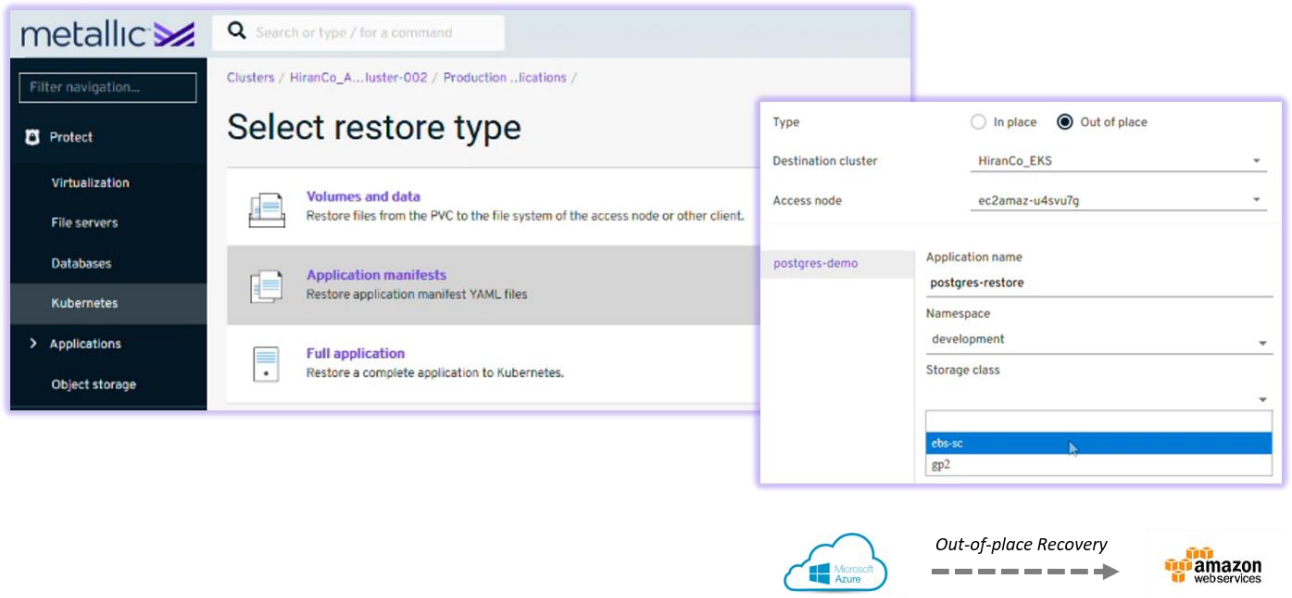
Figure 2. Backup Management Capabilities Overview



On the right side of Figure 2, we see the applications listed by namespace. If tags were not used and policies only leveraged namespace, the two applications would likely miss important backups when they were promoted to production.

Finally, and most importantly, we used Metallic for VM & Kubernetes to restore a Postgres database. As shown in Figure 3, Metallic for VM & Kubernetes has flexible restore capabilities that include Kubernetes volumes and data, application manifests, and full applications. We used the full out-of-place restore option to recover and essentially migrate a Postgres database from Azure to AWS. The process created all the resources on the target platform to run the application, including provisioning the storage and nodes.

Figure 3. Flexible Recovery Operations



First Impressions

Container adoption is accelerating and so too is the requirement to properly protect container environments and the data in them. While many recognize the growing importance of containers relative to other vital application platforms, confidence levels in the ability to protect containerized workloads are lagging. In fact, respondents to an ESG research survey identified managing backup/recovery of container-based application across multiple public cloud services and hybrid clouds as two of their biggest challenges related to managing backup/disaster recovery for container environments.[2]

ESG's first impression is that the Metallic VM & Kubernetes data protection solution from Commvault was designed to natively protect Kubernetes containers at scale whether an organization is protecting hundreds or thousands of containerized applications, or more. Even with scalability in mind, the developers did not leave out features needed to perform enterprise-level data protection. And the recovery scenarios should satisfy both application developers and IT operations teams alike. As part of a broader BaaS portfolio, Metallic lets teams easily extend their data protection from traditional workloads to containers with single pane of glass management.