Lab Insight

Cloud Native Application Data Protection: NetApp Astra Control vs. Alternatives

Author: Russ Fellows

March 2022

Evaluator Group

NetApp®

Overview

Cloud native application environments are being used more frequently, not only for development but increasingly used to deploy enterprise applications. According to the most recent survey from the Cloud Native Computing Foundation (CNCF)[1] more than 60% of respondents are running 250 or more container applications in production. Although CNCF respondents are early adopters of container technology, it is clear that cloud native applications are becoming mainstream.

As applications move from development to production, it is imperative to ensure backup and disaster recovery practices are in place to support these applications. Too often, data protection is taken for granted until some type of data loss occurs, often with disastrous implications for the company, IT staff or both.

Strategies and best practices around data protection are often a significant part of engagements with our IT clients. These interactions occur both as a part of strategic engagements, or after a data loss event. With the evolving IT landscape now encompassing on-premises and public cloud resources along with cloud native applications, it is clear that data protection tools are changing, but the need for data protection is only increasing.

Evaluator Group was commissioned to compare the costs associated with using open-source data protection tools to NetApp Astra Control Center to protect container native applications. This was done by installing and operating both open-source data protection tools alongside Astra Control Center in order to protect containerized applications running on multiple Kubernetes / OpenShift clusters.

As a result, our testing measured overall management and ease of use factors that have operational and financial implications, along with other general usability factors. In order to a create a realistic comparison, a multi cluster Kubernetes test environment was utilized which hosted container applications utilizing NetApp storage. Multiple backup targets were evaluated during testing, including on-premises S3 object storage along with AWS S3 storage.

A summary of the cost comparison of Astra Control and open-source tools found:

- NetApp Astra Control Center had between 2X and 3X better TCO (i.e., lower TCO)
  - Note: Cost comparison is based upon an Evaluator Group TCO analysis of OPEX and CAPEX
- Astra Control Center does backups with greater application consistency by using storage snapshots
- Astra Control Center provides a better IT admin experience with a web-access UI, vs. a CLI only
- Astra Control Center automatically scans for new applications and warns of unprotected apps
- Astra Control Center is supported by NetApp, compared to community-based support

[1] CNCF 2020 Container Survey: **www.cncf.io/wp-content/uploads/2020/11/CNCF_Survey_Report_2020.pdf**

Container Data Protection Requirements

One of the primary tasks of IT professionals is protecting application data and minimizing exposure to data loss. Making secure, backup copies is one of the primary data protection methods available to safeguarding applications and data. As previously discussed, operating in either private or public clouds requires protecting applications from a variety of risks including equipment failures, outages or data intrusion and ransomware attacks.

Over time, backup applications have evolved to include a number of highly useful features beyond those available with operating system tools designed to copy data. While backup applications may leverage some of the same underlying technologies, the benefits of using a tool designed to manage data protection for multiple points in time can be significant, both for protecting and recovering data. While the focus is often placed on creating backups, the ability for IT or users to quickly restore applications is the primary consideration. Tools that enable protecting and recovering data quickly is critical.

There are several important features to consider for data protection applications. Below in Table 1 are important requirements along with a comparison between open-source tools and the on-premises NetApp Astra Control Center application tested. Tool capabilities are based upon testing of Velero with Restic as representative of open-source tools and NetApp Astra Control performed by Evaluator Group.

Requirements	Open Source Tools	NetApp Astra Control
Operate in Public & Private Clouds	Yes, custom installs reqd.	Different Offerings
Management Instances	One per Cluster	One per Site
Automatic Scan for New Apps	No, manual scan reqd.	Yes, auto scan for apps
Data Protection Policy Schedules	Requires manual tracking	Policies scheduled via UI
Graphical User Interface	No, CLI per cluster	Yes, multiple K8s clusters
Support any CSI Primary Storage	Yes	Cloud Dependent
Support True Snapshot Copies	No, copy or snapshots	Yes, copy from snapshot
Utilize Multiple Backup Targets	Difficult	Simple
Enterprise Application Support	No, community only	Yes, NetApp Services

Table 1: Comparing Data Protection Features for Cloud Native Application Environments (Source: Evaluator Group)

One of the most important benefits of backup applications is their ability to manage and track resources, including systems or applications that need protection along with backup locations or targets. Typically, management of resources is known as a backup catalog, which tracks the time of backups in addition to

their location. The backup catalog contains meta-data to manage backup sources, targets and importantly the location of each protection point. Enterprise data protection applications are designed to manage resources across multiple locations, and scale to support thousands of resources.

In contrast, backup tools designed to protect specific applications or resources often are not designed around a backup catalog or designed for enterprise scale. While these limitations are not obvious when protecting a few systems or applications, they become increasingly important as the environment scales to hundreds or thousands of applications.

NetApp Astra Control

The vision of NetApp's Astra Control is to provide both a service and software offering that enables customers the ability to protect container applications regardless of where the Kubernetes (K8s) cluster is running, including both public cloud K8s offerings and private cloud clusters.

Astra Control is designed to provide a single point of control for managing multiple data protection across either an on-premises K8s deployment or a public cloud deployment. IT environments operating K8s clusters typically have multiple clusters, with several supporting their production deployments along with additional clusters required for development and testing prior to production. Without a single management point that can be used for an entire site, companies must use an additional protection management point for each cluster, leading to significantly greater complexity, time and expense vs. a consolidated approach like Astra.

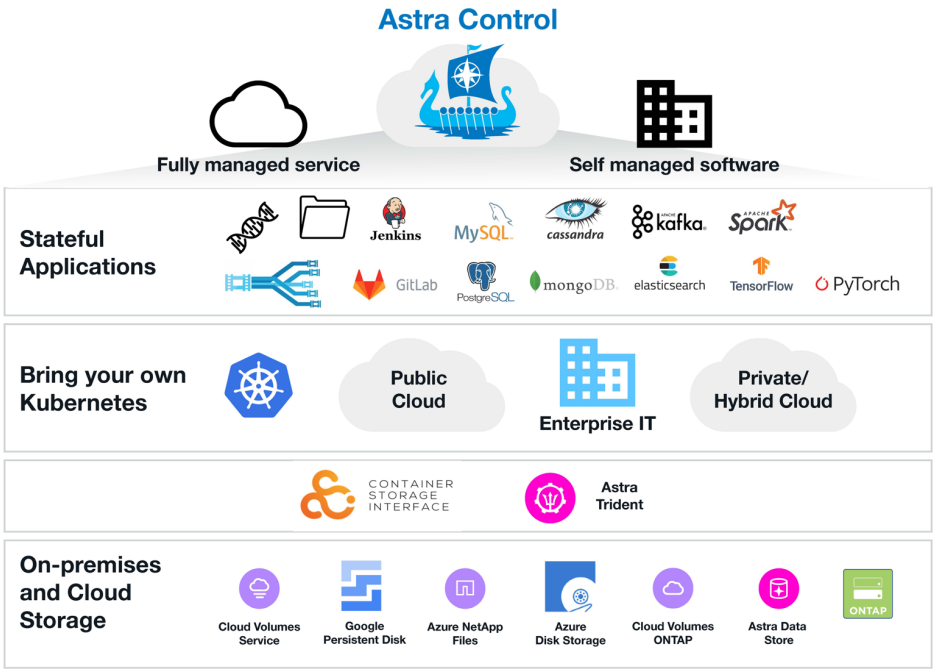

Figure 1: NetApp Astra Control - Overview (Source: NetApp)

Currently, NetApp's Astra Control offerings are bifurcated, with the fully-managed service "Astra Control Service" supporting public cloud environments and the self-managed software "Astra Control Center" product designed for private K8s environments.

This paper focus is on the self-managed Astra Control Center product, which was deployed into an on-premises Kubernetes cluster in order to test data protection of on-premises applications running on K8s clusters.

Comparing Cloud Native Data Protection Options

Evaluator Group was asked to compare open-source tools commonly used for data protection of cloud native applications to NetApp Astra Control. The evaluation created a test environment consisting of an OpenShift Kubernetes cluster on-site with NetApp ONTAP Select storage via the Astra Trident CSI interface to the cluster. As a location for backup copies, both on-premises S3 compatible and AWS public cloud S3 object storage were used as backup targets. Additionally, several cloud native applications were installed to run on the Kubernetes cluster along with both NetApp Astra Control and open-source backup tools Velero and Restic. An overview of the test environment is provided below in Figure 2.

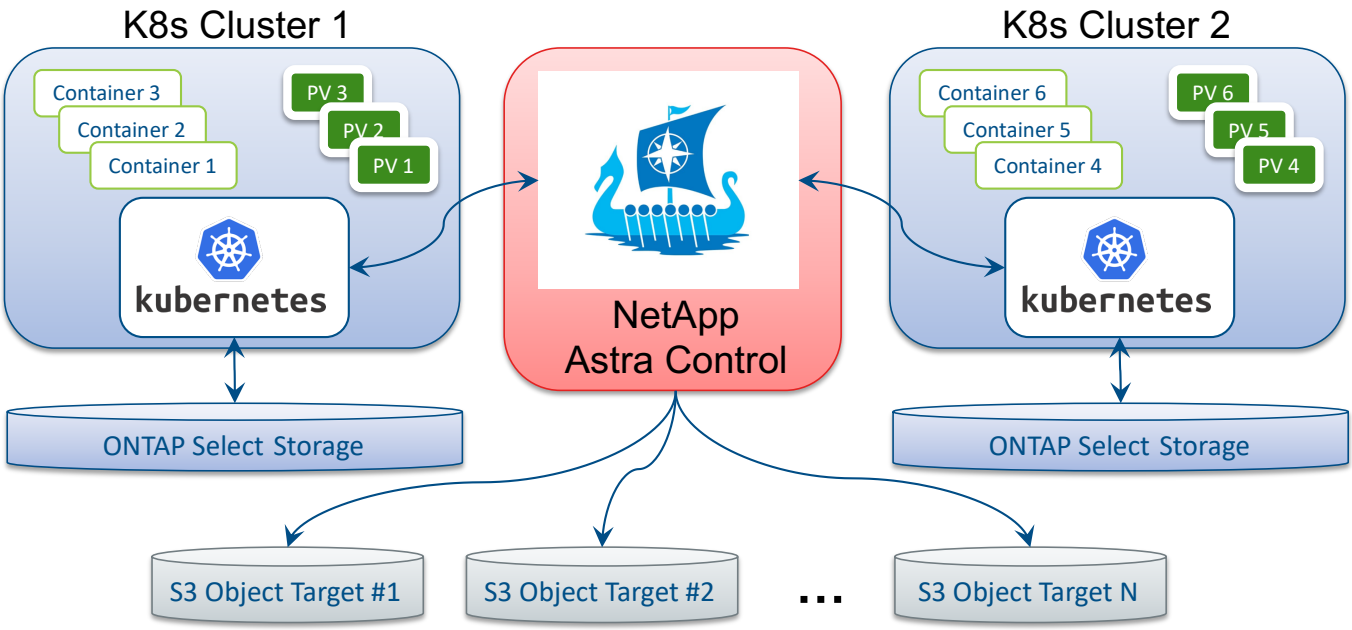

Figure 2: Test Environment - NetApp Astra Control vs. Open-source Tools (Source: Evaluator Group)

The primary focus of testing was to ascertain the relative costs of each option. Costs were driven by two components, the amount of administrative time required to use each tool for data protection and restoration tasks, commonly known as operational or OPEX costs. Additionally, the cost of acquiring or licensing the tools for use were also included, which are also known as capital costs, or CAPEX.

Financial Comparison

In order to construct a valid financial comparison, it was first necessary to establish the following parameters:

- Typical administrative tasks required to protect container apps (may vary by tool)
- Number of times tasks are performed per month (may vary by tool)
- Amount of time required to perform each task (does vary by tool)

With these aspects understood, data protection tasks were performed, and the amount of time required was recorded using both open-source tools and using NetApp Astra Control. The amount of time spent on data protection tasks is dependent upon the size of the environment. Evaluator Group's financial model is driven by several parameters, including the number of Kubernetes nodes per cluster, the number of clusters and the total number of applications in the cluster. Each of these aspects has implications for the amount of time required to manage and protect applications in the specified model.

Astra Control Center required less administrative time compared to open-source tools in every scenario we examined. The cost differences are driven primarily by the decreased time and complexity managing data protection with Astra Control compared to open-source tools.

> ***Evaluator Group Comments: We found Astra Control provides significant cost savings compared to using open-source tools, with typical savings ranging from 2X up to 3X. This is due to the ability to manage data protection far more efficiently, reducing IT administrative time and thereby lowering total costs.***

There were several important findings from our testing and financial analysis when comparing a supported product such as NetApp Astra Control with open-source tools.

- Without formal support, problems and issues that arise with open-source tools may take significantly longer to resolve
- With open-source tools, internal resources and time must be dedicated to supporting, researching and resolving problems
- Evaluator Group's TCO model included additional IT admin time when using open-source tools, which may be seen as an additional cost in the pie chart of the financial model shown below.

During testing we encountered issues when attempting to setup both Astra Control and the open-source tools. However, we were able to utilize NetApp resources to quickly resolve issues with Astra Control but were relegated to internet searches in order to find possible resolutions for the open-source tools. This experience is typical and reinforces the value of supported products, and additional costs of open-source tools.

The five-year cost differences are significant as shown in Figure 3.

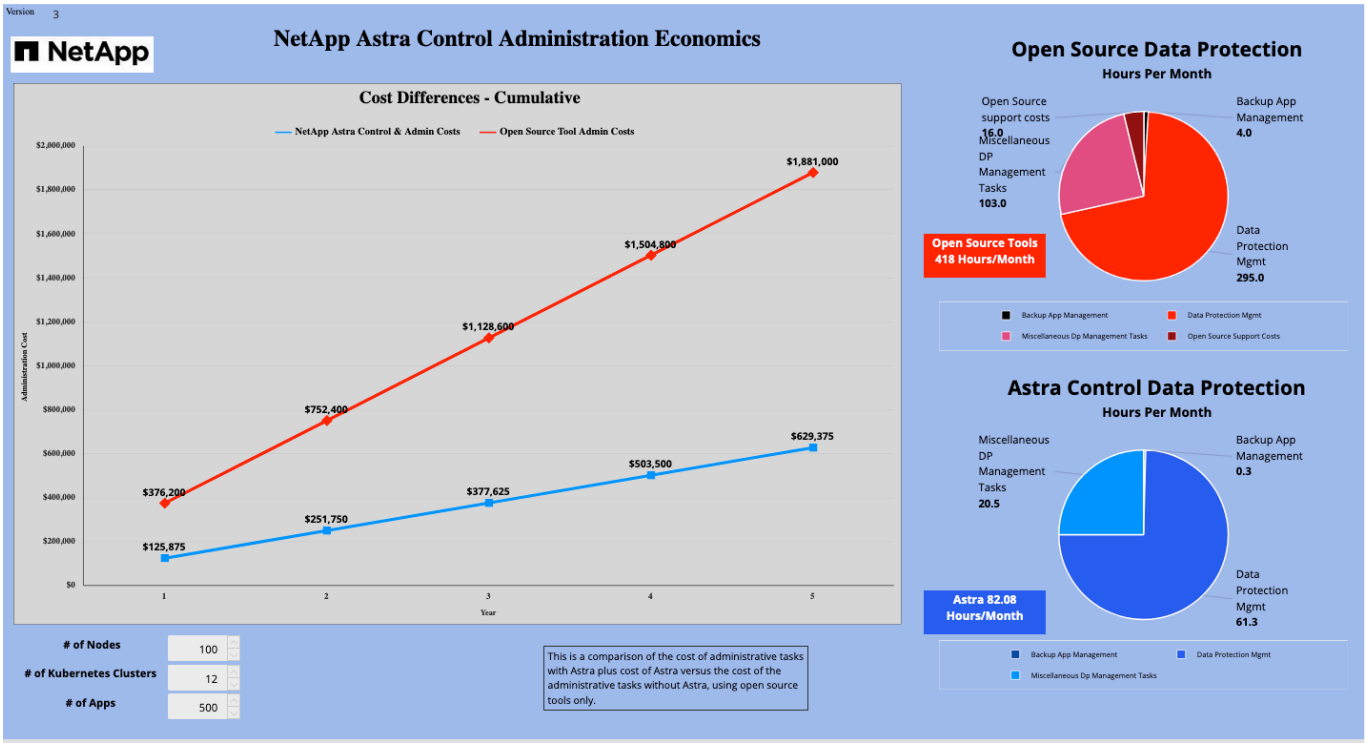

Figure 3: Evaluator Group TCO Comparison – Astra CC vs. Open-source Tools (Source: Evaluator Group)

As the environment grows in size and complexity, the costs diverge significantly with open-source tools requiring substantially more administrative time per cluster. By comparison, Astra Control required only a small amount of time in order to manage additional clusters. As shown in Figure 3 is the comparison of an environment that may be seen in a small enterprise, consisting of 12 K8s clusters with a total of 100 nodes and 500 applications.

Financial Cost Model

In evaluating financial costs, we included only aspects that are easily measured and quantifiable. As previously stated, the financial model derives costs primarily from the amount of administrative time required to complete tasks in a given environment size, using either open-source or Astra Control Center.

Additionally, the cost of licensing and support was included, which differed as follows:

- Open-source tools have no licensing costs, but support requires IT admin time for problem research, posting to web sites as well as finding How-To or Wiki guides
- NetApp Astra Control Center has license charges, which also includes enterprise support and well documented interoperability matrix that is tested by NetApp

Using this model, an almost infinite number of “environments” could be made. A comparison of three different environment sizes is shown in Table 2.

5 Year Cost Comparison (Operational Costs + Licensing)	Open-source Tools (Velero + Restic)	NetApp Astra Control Center	Astra Advantage
Size A: 2 Clusters – 60 Apps	$364,050	$192,375	1.9X Lower
Size B 5 Clusters – 225 Apps	$832,500	$354,000	2.4X Lower
Size C : 12 Clusters – 500 Apps	$1,881,000	$629,375	3.0X Lower

Table 2: Financial Comparison - NetApp Astra Control vs. Open-source Tools (Source: Evaluator Group)

Additional details of the financial model are provided in the Appendix.

Financial Costs NOT Included

As with any analysis, it is critical to decide what should be included, and what should be excluded. We did not include costs associated with data loss, disaster or attacks a company may experience.

> ***Evaluator Group Comments: In many instances, costs from data loss or downtime can far outweigh the cost of implementing an appropriate data protection strategy. This financial analysis did not include these costs due to the wide range based upon industry and company size.***

Our financial comparison was not designed as a full total cost of ownership analysis, as several potential costs were excluded.

A partial list of some of the "soft" costs consciously excluded from our model include:

- Loss of proprietary or customer data
- Loss of credit or PII (personally identifiable information)
- Lost Revenue Opportunity
- Legal or Regulatory penalties
- Ransomware costs, either to recover or rebuild data
- Salary differences between IT admins and Dev/Ops engineers

Usability Comparison

Although the analysis was primarily focused on financial aspects, ease of use along with overall usability and applicability to solving data protection challenges were also evaluated. Broadly, product use-case analysis is often separated between initial setup and on-going, or long-term use. The initial setup and installation can provide a sense for how easy a product is to use, but due to the limited nature of these tasks initial setup typically plays only a minor role in determining on-going management complexity while using the product.

Evaluator Group Comments: Overall, we found that Astra Control was significantly more efficient with each additional K8s cluster protected. The open-source tools tested for data protection incurred additional time and overhead with each additional K8s cluster. In contrast, Astra Control imposed almost no additional time or complexity requirements in order to protect additional clusters.

Another component of ease-of use is the question of "who" is required to perform tasks. During application design and development, a "Dev/Ops" engineer typically assists with the administration, including management of Kubernetes and other IT resources. As container applications move into production, "Dev/Ops" engineers may have limited availability with IT staff often given the responsibility for managing and protecting production applications. Moreover, tools that may be managed via a web-UI and using more IT friendly concepts can often help facilitate successfully managing and protecting container applications operating in K8s environments.

Evaluator Group Comments: With limited availability, the expense of Kubernetes Dev/Ops personnel can be significantly greater than traditional IT administrators. Moreover, empowering IT staff the ability to leverage their skills in order to protect new container-based applications and services can benefit many organizations.

Product Installation & Setup

As part of our testing, we setup multiple clusters, and installed Astra Control Center along with Velero plus Restic for protecting all of the K8s clusters. We quickly learned that Velero and Restic must be installed into each cluster being protected, potentially using different parameters depending upon cluster and resource differences. In contrast, Astra Control Center required only a centralized installation in order to protect all of the K8s clusters we used during testing.

On-Going Management Tasks

Our financial model focused on tasks performed repeatedly, which account for the greatest potential time and administrative expenses. Ease-of use aspects were indirectly captured since they correlate to administrative time. Specifically comparing the tools' complexity and ease of use, there were significant differences between the open-source tools (Velero / Restic) and Astra Control Center.

Some of the differences between tools for ongoing management tasks include:

- Velero/Restic required using a CLI vs. a graphical, Web UI for Astra Control Center
- Some CLI options for Velero/Restic, depending upon cluster configuration
- Well documented REST API for managing Astra Control Center
- Velero/Restic requires application management on a per cluster basis
- Astra Control enables management across multiple clusters
- Ability to create data protection policies and schedule using single management UI

One of the most important differences between using Velero and Astra Control were the amount of time and effort required as the Kubernetes environment grows. When using Velero/Restic, each K8s cluster is managed independently. Thus, any updates, policies or schedules created in one cluster must be repeated for every cluster under management. For small environments this may be acceptable; however, as the size of the K8s environment grows, the open-source tools quickly become inefficient, and require significantly more time, effort and cost to manage.

In contrast, having a single point of management across multiple clusters with Astra, along with the ability to see and manage application protection from a single UI provides significant TCO benefits, even for environments with as few as two clusters.

> ***Evaluator Group Comments: We found that Astra Control provided increasingly better efficiency than open-source tools as the environment grew in size. With a single graphical UI for managing data protection policies across all clusters, vs. the need to manage each individual Kubernetes cluster's protection provides significant TCO advantages for Astra Control.***

Problem Resolution

Nearly every product can encounter issues or challenges when used in a customer's unique environment. The availability and quality of product support often means the difference between either relying on a product, or avoiding it due to the inability to rely upon a tool when needed. One of the primary differences between open-source tools and commercial tools is the availability of product support.

During the testing of Velero and Restic, we encountered several configuration issues and errors. The only "support" was to search help-forums and posts from other users. Issues required posting to online forums, with no defined timeline or promise of resolution. Unless a known solution exists, IT admins are forced to find work arounds or solutions on their own in many cases when using "free" products.

> ***Evaluator Group Comments: The use of freely available tools for production environments typically means the need to dedicate internal IT staff to researching and resolving problems. In many cases, "free" has far greater cost than purchasing a commercially licensed product with support.***

Final Thoughts

Protecting enterprise applications is an important aspect of IT operations, regardless of how those applications are deployed, or where they are operating. With the rise of public cloud computing, many early adopters believed that because of the lower risk of equipment failures occurring in public clouds, they did not need to backup or protect applications in the same way as they had with on-premises applications.

However, as companies use of clouds has matured, so too has their realization that protecting applications in public clouds is every bit as important as it is to protect applications onsite. Additionally, with the increase of ransomware and other nefarious data breaches, companies now understand that creating backup copies of applications is required to guard against all types of disasters, including system breaches and ransomware attacks.

> ***Evaluator Group Comments: Applications data protection continues to be of strategic consideration for any type of application, regardless of where or how it is deployed. Virtualized or in a container deployed in a private or public cloud, applications require protection from disasters, data breaches and ransomware.***

Educated IT consumers understand the importance of creating data protection copies for all types of applications, running across multiple private and public cloud resources. After first deciding to protect applications across a multi-cloud environment, the next decision is choosing the best tools for managing application backups and aiding disaster recovery in the event of a breach or data loss event.

> ***Evaluator Group Comments: NetApp Astra Control Center provides significant ease of use advantages, combined with considerable cost savings compared to using "free" open-source tools. By reducing administrative time, increasing productivity and reducing IT staff from community-support of open-source tools delivers concrete cost savings of 2X to 3X compared to open-source.***

We found that even for smaller environments, the time and cost savings of NetApp Astra Control Center compared to open-source alternatives was nearly 2X. It is increasingly common to first look to freely available tools, as a way to reduce costs. However, the true cost of using inefficient tools results in greater personnel time and costs as the environment grows.

Moreover, it is important to select tools that perform well while helping to increase administrative efficiency for today's hybrid cloud environments running cloud native applications. Based on our financial analysis, along with the significant functional benefits outlined, it is clear that NetApp Astra Control should be a consideration for protecting cloud native application environments.

Appendix

Test Environment

As previously shown on page 4, Figure 1; Evaluator Group setup a test environment consisting of two OpenShift / Kubernetes clusters, along with storage for applications and several S3 compatible backup storage targets.

Hardware Infrastructure

- Two VMware clusters
  - Cluster 1:
    - 4 nodes, Intel E5-2699v4
    - 256 GB DRAM each
    - 2 x 25 Gb/s Mellanox NIC
    - SDS storage: 2 x 375 Optane NVMe + 6 Intel 5510 NVMe
  - Cluster 2:
    - 3 nodes, Intel 6138
    - 384 GB DRAM each
    - 1 x 100 Gb/s Mellanox NIC
    - SDS storage: 2 x 375 Optane NVMe + 6 Intel 5510 NVMe
  - VMware ESXi 7.0U3 with vCenter

Container Infrastructure

- Two Kubernetes clusters, each consisting of:
  - 3- Kubernetes “worker nodes” running as VMs
  - 3-Kubernetes management nodes running as VMs
  - RedHat OpenShift Container Platform 4.6

Primary Storage Infrastructure

- Two instances of NetApp ONTAP Select 9.9 (OTS) Storage
  - Each OTS instance was a single node with 8 TB of capacity

S3 Object Storage Infrastructure

- Target 1: AWS S3 bucket (Public Cloud)
- Target 2: Local S3 compatible bucket (Private cloud, 4-node instance)
- Target 3: Local S3 compatible bucket (Private cloud, 3-node instance)

Time Comparison Details

Comparison of a "Production" environment, with 5 clusters, 45 nodes and 225 applications. Importantly, the amount of IT admin time is significant, 31% for Astra Control vs. 101% for using Velero.

Astra Use for Backup	Percent of Total Time	# Times / Month / Unit	Unit of Measure	What / Unit of Scale	Admin Time / Action (hrs)	Admin hrs / Month	Notes
Backup App Management	**1%**					**0.33**	
Install and Update Backup apps	1%	0.08	Astra instance	1.00	4.00	0.33	Install / Update Astra Control = 4 hours per instance, 1 x per year per instance
Data Protection Mgmt	**75%**					**39.25**	
Discover New or Unprotected Apps	10%	21	Per Catalog	1.00	0.25	5.25	15 minutes per Catalog - Daily (Note: 1 catalog per Astra Instance, multi Clusters)
Schedule App Backups	0.5%	1	Per Catalog	1.00	0.25	0.25	15 minutes per Catalog - Monthly
Track App Backups and Locations	10%	21	Per Catalog	1.00	0.25	5.25	15 minutes per Catalog - Daily
Verify Scheduled Backups Occur	20%	21	Per Catalog	1.00	0.50	10.50	Check each Backup Catalog - Daily (1 catalog / cluster), 30 min / action
Run Ad Hoc App Backups	7%	0.21	1% of Apps	225.00	0.08	3.94	1% of all Apps daily - takes 5 min ea.
Run Data Recovery	22%	0.21	1% of Apps	225.00	0.25	11.81	1% of all Apps daily - takes 15 min ea.
Run Data Migration / Clone	4%	0.04	1% of Apps	225.00	0.25	2.25	1% of all Apps weekly - takes 15 min ea.
Miscellaneous DP Management Tasks	**25%**					**13.08**	
Manage backup targets (capacity, tiers, etc.)	6%	4	Backup Targets	5.00	0.17	3.33	10 minutes per Backup Target - Weekly
Manage backup retention (expire / remove old)	2%	4	Per Catalog	1.00	0.25	1.00	Check each Backup Catalog - Weekly (1 catalog / cluster), 15 min / action
Verify a subset of backups	4%	0.04	1% Ap / wk	225.00	0.25	2.25	1% of all Apps weekly - takes 15 min ea.
Maintain logs of backups and restores	2%	4	Per Catalog	1.00	0.25	1.00	15 minutes per Catalog - Weekly
Review alerts / exceptions and fix issues	7%	21	Per Catalog	1.00	0.17	3.50	10 minutes per Catalog - Daily
Create & review reports on DP success, failures and exclusions	4%	4	Per Catalog	1.00	0.50	2.00	30 minutes per Catalog - Weekly
Total	**100%**					**52.67**	
% of FTE Hours / Month	**%**					**31%**	

Table 3: NetApp Astra Control - Administrative Time (Source: Evaluator Group)

Velero Use for Backup	Percent of Total Time	# Times / Month / Unit	Unit of Measure	What / Unit of Scale	Admin Time / Action (hrs)	Admin hrs / Month	Notes
Backup App Management	**1%**					**1.67**	
Install and Update Backup apps	1%	0.08	Cluster	5.00	4.00	1.67	Install / Update Velero app = 4 hours per instance, 1 x per year per instance
Data Protection Mgmt	**74%**					**124.25**	
Discover New or Unprotected Apps	16%	21	Per Catalog	5.00	0.25	26.25	15 minutes per Catalog - Daily (Note: 1 catalog per Cluster for Velero)
Schedule App Backups	1%	1	Per Catalog	5.00	0.25	1.25	15 minutes per Catalog - Monthly
Track App Backups and Locations	16%	21	Per Catalog	5.00	0.25	26.25	15 minutes per Catalog - Daily
Verify Scheduled Backups Occur	31%	21	Per Catalog	5.00	0.50	52.50	Check each Backup Catalog - Daily (1 catalog / cluster), 30 min / action
Run Ad Hoc App Backups	2%	0.21	1% of Apps	225.00	0.08	3.94	1% of all Apps daily - takes 5 min ea.
Run Data Recovery	7%	0.21	1% of Apps	225.00	0.25	11.81	1% of all Apps daily - takes 15 min ea.
Run Data Migration / Clone	1%	0.04	1% of Apps	225.00	0.25	2.25	1% of all Apps weekly - takes 15 min ea.
Miscellaneous DP Management Tasks	**25%**					**43.08**	
Manage backup targets (capacity, tiers, etc.)	2%	4	Backup Targets	5.00	0.17	3.33	10 minutes per Backup Target - Weekly
Manage backup retention (expire / remove old)	3%	4	Per Catalog	5.00	0.25	5.00	Check each Backup Catalog - Weekly (1 catalog / cluster), 15 min / action
Verify a subset of backups	1%	0.04	1% Ap / wk	225.00	0.25	2.25	1% of all Apps weekly - takes 15 min ea.
Maintain logs of backups and restores	3%	4	Per Catalog	5.00	0.25	5.00	15 minutes per Catalog - Weekly
Review alerts / exceptions and fix issues	10%	21	Per Catalog	5.00	0.17	17.50	10 minutes per Catalog - Daily
Create & review reports on DP success, failures and exclusions	6%	4	Per Catalog	5.00	0.50	10.00	30 minutes per Catalog - Weekly
Total	**100%**					**169.00**	
% of FTE Hours / Month	**%**					**101%**	

Table 4: Open-source Velero + Restic - Administrative Time (Source: Evaluator Group)

Frequency (times / month)	
Daily	21
Weekly	4
Monthly	1
Yearly	0.08

Time in Hours	
5 min	0.08
10 min	0.17
15 min	0.25
30 min	0.50
1 hr	1.00

About Evaluator Group

*Evaluator Group Inc. is dedicated to helping **IT professionals** and vendors create and implement strategies that make the most value of their storage and digital information. Evaluator Group services deliver **in-depth, unbiased analysis** on storage architectures, infrastructures, and management for IT professionals. Since 1997 Evaluator Group has provided services for thousands of end-users and vendor professionals through product and market evaluations, competitive analysis, and **education**. **www.evaluatorgroup.com** Follow us on Twitter @evaluator_group*

This document was developed with NetApp funding. Although the document may utilize publicly available material from various vendors, including NetApp and others, it does not necessarily reflect such vendors' positions on the issues addressed in this document.