Splunk Solution Brief

Highlights

- Virtualize your Splunk implementations in your data center with better performance
- Improve data security with Blanket Encryption
- Increase mobility of Splunk applications within and across DVX enabled data centers
- Improve availability of your critical Splunk infrastructure with faster recovery time objectives
- Protect Splunk data on the DVX without the cost and complexity of additional backup solutions

Splunk with Datrium DVX Hybrid Cloud Platform

The Challenge

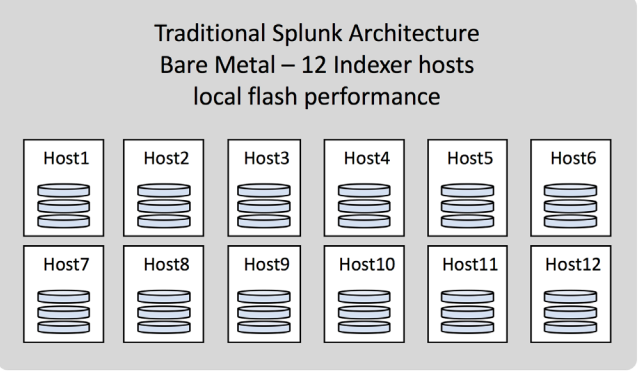
Splunk makes machine data accessible, usable and valuable to everyone in the organization. Splunk turns machine data into answers. Independent of the size or industry, Splunk can help solve your toughest IT, security and business challenges. With Splunk, machine data comes from a myriad of sources and always seems to be increasing as organizations grow or find more creative ways to operate from their infrastructures data.

To build efficient machine data mining solutions you need to architect for data growth and scalability. Building for growth while reducing complexity, improving performance, availability, and increasing data security is one of the bigger challenges facing IT organizations across the board - not just with Splunk.

With the Datrium DVX platform and VMware, organizations can virtualize Splunk deployments with ultimate performance and availability while maintaining focus on the Splunk data and less on the infrastructure to support it. In other words, spend more time with data analytics and less time managing the environment.

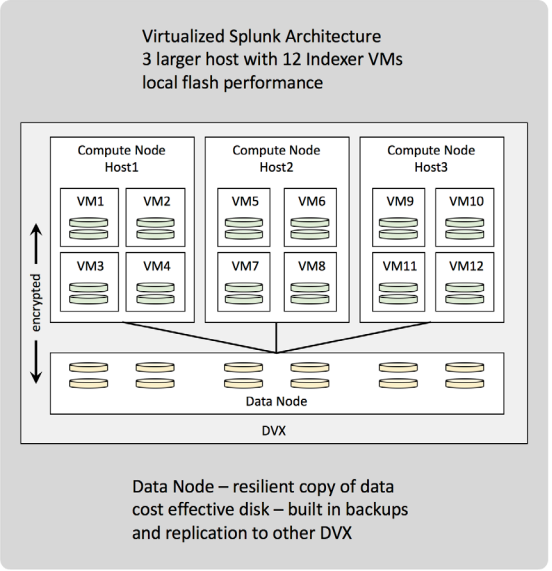
IT organizations that are moving other core IT applications to a virtualized and cloud oriented infrastructure are able to achieve the same benefits for their Splunk workloads. This shift often reduces the potential silos of infrastructure for these core application systems (virtualized) and Splunk resources (bare metal) while simplifying the overall management.

In a typical deployment, as more search or indexing power is required, more hosts are added. For smaller environments this is manageable. Unfortunately, as the workload increases, so does the management of the infrastructure! A typical 12-node Splunk deployment on bare metal hosts might look something like this:



The Solution

To Datrium DVX, Splunk is just another workload that can be easily and efficiently virtualized within fewer, larger and better utilized hardware resources. The key components of a similarly designed virtualized Datrium solution with Splunk might look something like this:



Key Benefits

Performance for index and search at local flash speeds

The Datrium DVX architecture runs the virtualized components (e.g., Splunk Indexer, Search, Forwarder) on local flash on the hypervisor host. Data locality along with flash performance provide ultra low application latencies and linear scalability of the solution. Adding more physical hosts (Compute Nodes) adds more CPU processing power and more storage I/O processing power through the Datrium DVX Hyperdriver software running on the hosts.

With the Datrium DVX architecture it is possible to build Splunk implementations that are capable of ingesting terabytes of data per day while increasing performance and availability as the system grows.

Improve security of sensitive machine data

The Datrium DVX system includes a native built-in encryption capability, Blanket Encryption. Blanket Encryption can easily be enabled across the entire Datrium data management stack with full data services always on (Compression & Deduplication).

From the moment a virtual machine is writing data to the local virtual disk, transferred across the network and at rest in both local flash and on the Data Node, your data is secured with FIPS 140-2 Cryptographic Certification.

Easier deployment of components at scale

When more search or indexing needs arise, additional Splunk virtual machines can be easily deployed into the aggregate environment leveraging denser and higher performing host hardware. Capacity requirements for longer term retention or growing data sets can be handled separately by adding additional Data Nodes or more local flash to the Compute Node hosts. With Datrium, you can consolidate Splunk components onto fewer physical resources and improve overall data center resource density.

With Datrium DVX, the physical hosts (Compute Nodes) can be selected from existing server assets or purchased new to meet the demands of the environment. As long as they are equipped with local flash for the performance copy and run ESXi they can be configured into the DVX system to support more workloads.

Improve availability of critical data with better economics

The Datrium DVX architecture with Split Provisioning between Compute and Data Nodes allows for resiliency protection equivalent to RF3 levels with RF2 implemented across the virtualized index and search node VMs. The shared Data Node provides the increased data availability with Erasure Coding and other beneficial data services like compression and deduplication.

With Built-in backup capabilities through efficient snapshot and replication methods, the critical machine data your organization uses to make operational decisions can be better protected and transferred throughout the organization. Since the data protection copies never leave the DVX system, recovery is as fast as restarting the VM on the most recent snapshot from just minutes ago. The cost of a separate backup system is not required, so the economics of protecting data is dramatically better.

Conclusion

With Datrium DVX, IT organizations can apply the benefits of virtualization to their core Splunk machine data implementations. Leveraging a common, highly efficient, and protected virtualization platform, IT administrators can rest assured that they have the right mix of performance, availability, security, manageability and economics to meet the demanding needs of today's modern data centers.

For More Information

Splunk on DVX: https://www.datrium.com/technology_partners/splunk/

http://www.datrium.com/

http://www.splunk.com/