

# Splunk on Nutanix



Splunk Enterprise is the leading software platform for unleashing the power of machine data gathered from IT infrastructure and equipment of all types.

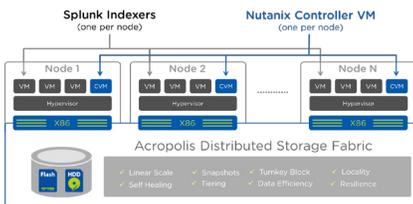
With the amount of machine data seeming to increase without bound, the job of the Splunk architect has become a challenge. Reducing complexity, improving data security, and eliminating bottlenecks are top priorities. Traditional IT infrastructure is ill-suited to address the needs of growing Splunk installations.

## FOCUS ON SPLUNK DATA, NOT SPLUNK INFRASTRUCTURE

A Nutanix Enterprise Cloud takes the complexity out of managing infrastructure for Splunk, allowing Splunk experts to spend more time extracting insight from data.

**Virtualization with a difference.** Nutanix allows Splunk to take full advantage of server virtualization without the limitations of other solutions.

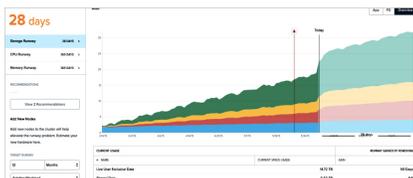
- **DSF.** With the Nutanix Distributed Storage Fabric, Splunk indexers access data locally. Splunk data is automatically stored on the right media—SSD for hot data, HDD for cold— and the resources allocated to each indexer can be changed effortlessly.
- **Life cycle management.** Nutanix continuously monitors data access patterns and places data in the most appropriate location, complementing the Splunk life cycle.
- **AHV.** Acropolis Hypervisor is a next-generation hypervisor that accelerates deployment and simplifies management. It is included at no extra cost with Nutanix purchases, eliminating virtualization licensing costs.



**Self-healing infrastructure.** A Nutanix enterprise cloud is resilient by design. If a drive or node fails, workloads are automatically restarted and full resiliency is restored quickly without operator intervention, protecting Splunk from unplanned downtime.

**Built-in availability.** Data protection, DR, and high availability are integral to the Nutanix environment, delivering higher Splunk availability with less time and effort.

**One-click management.** With Nutanix Prism, Splunk administrators easily monitor and manage all infrastructure used by Splunk, gaining full visibility of storage, CPU, and memory runway. One-click software, hypervisor, and firmware upgrades and one-click problem remediation take the pain out of day-to-day operations.



## ELIMINATE BOTTLENECKS

Splunk deployments grow rapidly as new data sources are added. Start small and scale out without worrying about the bottlenecks that occur with traditional architectures:

- **Ingest terabytes of data per day.** A compact 4-node, 2U cluster provides sequential throughput of 3 GB/s or more
- **Process millions of events per second.** A 4-node cluster can process 500,000 events per second
- **Scale incrementally.** Start small and grow linearly by adding nodes

Traditional storage systems can experience significant I/O bottlenecks, particularly in virtual environments. By ensuring data is accessed locally by all Splunk indexes, DSF eliminates the “I/O Blender” effect that can plague conventional infrastructure.

Administrators can scale existing Nutanix clusters or deploy new clusters in minutes with less concern for storage and network bottlenecks. A Nutanix enterprise cloud provides linear scaling, so Splunk deployments can scale without worry. Each additional node delivers predictable performance to support Splunk search heads, indexers, and other shared workloads. Because of its distributed architecture, a Nutanix enterprise cloud prevents one workload from starving another, allowing the infrastructure to be shared if desired.

## INCREASE SECURITY WITHOUT ADDING SILOS

To ensure the security of sensitive data, many Splunk architects find they have no choice but to deploy dedicated infrastructure for Splunk.

Nutanix combines features such as two-factor authentication and data-at-rest encryption with a security development lifecycle. Nutanix systems are certified across a broad set of evaluation programs to ensure compliance with the strictest standards.

Security features include:

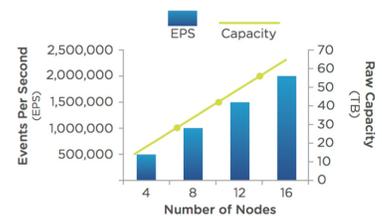
- Security-first engineering that ensures the stack is secure and any vulnerabilities are immediately addressed
- Integrated, self-healing security baseline for storage and AHV

Splunk can be deployed securely on a Nutanix cluster with other workloads, avoiding the need for a separate silo of infrastructure.

For those who wish to deploy separate infrastructure for Splunk, Nutanix Prism Central makes it possible to monitor and manage the infrastructure deployed for Splunk along with other Nutanix clusters. Larger organizations can deploy multiple clusters globally to support Splunk and manage them all from a single Prism Central console.



T. 855.NUTANIX (855.688.2649) | F. 408.916.4039  
info@nutanix.com | www.nutanix.com | @nutanix



Nutanix delivers invisible infrastructure for next-generation enterprise computing, elevating IT to focus on the applications and services that power their business. The company's software-driven Xtreme Computing Platform natively converges compute, virtualization and storage into a single solution to drive simplicity in the datacenter. Using Nutanix, customers benefit from predictable performance, linear scalability and cloud-like infrastructure consumption. Learn more at [www.nutanix.com](http://www.nutanix.com) or follow us on [Twitter@nutanix](https://twitter.com/nutanix).

©2016 Nutanix, Inc. All rights reserved.  
Nutanix is a trademark of Nutanix, Inc., registered in the United States and other countries. All other brand names mentioned herein are for identification purposes only and may be the trademarks of their respective holder(s).