Running CDM Tools on Nutanix

Performance at Scale, and Simplified Management Boost Security

Government Agencies have heightened awareness to protect their systems from ever-evolving cyber-security threats. While security compliance frameworks like FedRAMP and certifications like Common Criteria establish baseline, point-in-time assurance of a defined security posture, agencies must assume that their systems are active targets for intrusions and establish methods to continuously monitor their network and take prescriptive actions to mitigate cyber threats.

In such environments with dynamically evolving sophistication of threats, cyber-security experts look toward adaptive security methods which provide continuous monitoring to detect new issues and anomalies, and real-time mitigation to stop these incidents from causing harm.

In an effort to unify the tools and approaches Federal agencies take with adaptive security, the Department of Homeland Security defined the Continuous Diagnostics and Mitigation (CDM) program to ensure there is consistency and completeness in these efforts.

To be clear, while Nutanix has taken great pains to build in security throughout our products, the intent here is not to offer yet another security tool, but rather to explain why Nutanix is the ideal platform on which to deploy and operate the approved CDM toolsets.

"Nutanix continues to provide innovative solutions to improve IT security across federal government organizations."
– Robert Sanchious,
CEO/Chief of Engineering
SHR Consulting Group

"With multiple people involved in infrastructure deployment, and constant turnover in key positions, blade servers and Fibre Channel SANs add layers of complexity and a very long training time, whereas with Nutanix there isn't much training. That was a big selling point."
– Shawn Stamper,
Lead System Administrator,
Ohio Army National Guard

"HCI provides cost benefits to the Corps that help us continue to be good stewards of taxpayer dollars. It collapses layers for computing, storage and networking, and creates an environment where we can dynamically provide capacity when and where it is needed across the enterprise."
– Lt. Col. Dale Webster
USMC, HQ

HOW NUTANIX BENEFITS CDM DEPLOYMENTS

When introducing new tools into an environment, common worries are compatibility, and the impact to existing operations and IT staff. For security monitoring, it may even be desirable to operate those tools from within their own private cloud to not only minimize disruption, but to also ensure that the tools are not impacting performance of the existing environment. The capacity to monitor and ensure security must not interfere with mission and operational performance.

At the core of Nutanix Enterprise Cloud is our industry-leading Hyperconverged Infrastructure (HCI) platform which integrates compute, storage, virtualization and networking in a full-stack solution that runs nearly any application without modification. With it, CDM capabilities can be incrementally added to an existing network without disruption. The Nutanix scale out software platform supports all application storage requirements for File Services, Bare Metal Apps, Virtualized Workloads, Block based storage requirements, containerized workloads, and object-based storage workloads with one platform – eliminating the need for multiple, disparate, and proprietary storage platforms and Storage Area Networks.

NUTANIX™
YOUR ENTERPRISE CLOUD

FOCUS ON CDM DATA, NOT CDM INFRASTRUCTURE

A Nutanix Enterprise Cloud takes the complexity out of managing infrastructure for CDM tools, allowing security experts to spend more time extracting insight from data. Taking advantage of Nutanix virtualization features, multiple CDM tools can be hosted within a single Nutanix Enterprise Cloud cluster, eliminating server sprawl for systems dedicated to a single workload.

COMPACT POWERHOUSE

In typical IT modernization projects, it is not unusual for customers to realize a 60-80% reduction in datacenter footprint when moving from legacy 3-tier architectures to hyperconverged Nutanix Enterprise Cloud. What this means for a CDM deployment, is that the incremental infrastructure needed to run CDM tools will have minimal impact on existing datacenters. As a 100% software defined solution, Nutanix can be deployed onto commodity hardware, match to existing infrastructure standards, or leverage repurposed hardware already purchased. Fewer racks equate to lower costs, lower power and AC, and fewer elements to manage.

In terms of performance, Nutanix allows applications to:

- 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.

FAST TIME TO VALUE

Nutanix enables full stack private cloud infrastructure to deployed in minutes. Our industry-leading hyperconverged infrastructure foundation can shorten proofs-of-concepts, and deployments. In operation, rolling non-disruptive upgrades with no downtime support continuous innovation and development. Nutanix and CDM tools from providers like Splunk and Palo Alto Networks can be up and running in a few hours, not days.

FUTURE-PROOF CDM INVESTMENTS

Today, CDM deployments are focused on in-house networked assets, but agencies must anticipate incorporating public, private, hybrid, and distributed cloud architectures in their modernization plans. The Nutanix Enterprise Cloud has been designed to facilitate this eventuality. Nutanix Calm, Beam, and Prism Pro give agencies the insight and flexibility to automate and deploy applications where most effective and the governance to monitor security and cost compliance of those applications whether running on-premise on a Nutanix cluster or in a public cloud.

OPERATIONAL AND MANAGEMENT SIMPLICITY

Security experts understand that complexity is a key enabler of cyber vulnerabilities. Nutanix reduces the number of component parts it takes to deploy a complete solution which dramatically reduces complexity, increases automation, eases management, and even simplifies procurement.

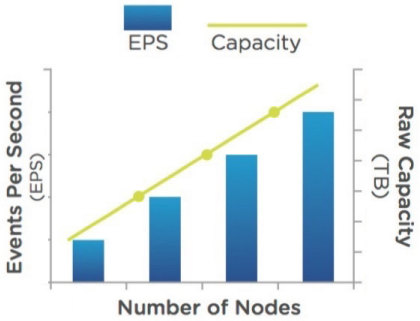
NUTANIX™
YOUR ENTERPRISE CLOUD

Powered by advanced machine learning technology, Nutanix Prism is an end-to-end consumer-grade management interface for virtualized datacenter environments that brings unprecedented simplicity in an uncluttered, yet rich experience and provides an intuitive user interface to simplify and streamline common datacenter workflows.

Technology specialization is minimized with Nutanix, allowing agencies to maximize IT staff activities and functions, minimize license/maintenance costs of third-party applications, and leverage one-click automation.

QUICK SEARCH AND INDEX

Many CDM security applications operate on Big Data which push the performance and scalability limits of traditional infrastructures, requiring good sequential and random performance across large datasets and multiple nodes. Nutanix delivers performance equivalent to bare metal deployments while significantly simplifying infrastructure management for your virtualized big data installations.



PREDICTABLE LINEAR PERFORMANCE AND CAPACITY

CDM deployments may grow rapidly as new data sources are added. 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 CDM deployments can scale without worry. Each additional node delivers predictable performance to support search, indexing, 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.

BUILT-IN VIRTUALIZATION - REDUCES COSTS AND MANAGEMENT

With Nutanix, customers have freedom of choice among common industry virtualization solutions, including Nutanix AHV - a license-free virtualization hypervisor included with the Nutanix Enterprise Cloud OS, Acropolis. With Acropolis and AHV, virtualization is tightly integrated into the Enterprise Cloud OS rather than being layered on as a standalone product that needs to be licensed, deployed and managed separately.

Common tasks such as deploying, cloning and protecting VMs are managed centrally through Nutanix Prism, rather than utilizing disparate products and policies in a piecemeal strategy.

SECURE BY DESIGN

If your mission is to guard the security of your network, the first thing to want to avoid is adding to the problem. The Nutanix Enterprise Cloud platform combines powerful security features, including role-based access control (RBAC), two-factor authentication, application security from VM microsegmentation, and FIPS compliant data at rest encryption, with a Security Development Lifecycle (SecDL) that is integrated into product development.

The Nutanix Enterprise Cloud OS (Acropolis) and Hypervisor (AHV) are pre-STIG'd to NIST 800-53 and DOD/DISA security standards for security hardening, simplifying and accelerating ATO processes. Self-healing security is automated to ensure no configuration drift from the approved baseline. Automated machine-readable reports are generated to demonstrate compliance.

NUTANIX™
YOUR ENTERPRISE CLOUD

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 CDM tools from unplanned downtime.

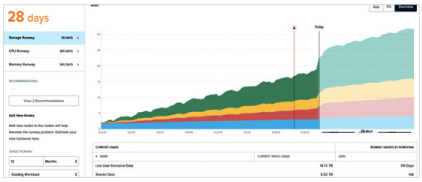
APPROVED PRODUCTS LIST AND RFS PROCESS

Nutanix products are now on the CDM approved products list (APL) . Nutanix sales teams understand the Request for Service (RFS) process and are ready to assist agencies in procuring Nutanix for CDM deployments.

CONCLUSION

With Nutanix, customers can start their CDM deployments small and then scale out the infrastructure as needed to meet data ingest, analysis, and retention requirements. The resilience of Nutanix Enterprise Cloud ensures that the system remains available, ensuring that security monitoring is continuous. Administrators can focus on CDM tools and data, not on the infrastructure.

Nutanix is committed to support IT needs across all levels of government. For more information, please visit www.nutanix.com, or call us toll-free at (855)-NUTANIX.



The Nutanix management capabilities use powerful AI and machine learning to predict when additional capacity may be required

[1] CDM Approved Products List, GSA, June 2019

NUTANIX
YOUR ENTERPRISE CLOUD

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

Nutanix makes infrastructure invisible, elevating IT to focus on the applications and services that power their business. The Nutanix enterprise cloud platform leverages web-scale engineering and consumer-grade design to natively converge compute, virtualization and storage into a resilient, software-defined solution with rich machine intelligence. The result is predictable performance, cloud-like infrastructure consumption, robust security, and seamless application mobility for a broad range of enterprise applications. Learn more at www.nutanix.com or follow us on Twitter@nutanix