v4.1 | September 2022 | TN-2038

TECH NOTE

Nutanix AHV Virtualization

NUTANIX
YOUR ENTERPRISE CLOUD

Copyright

Contents

1. Executive Summary 5
Document Version History 5

2. AHV 7

3. Integrated Management Capabilities 8
Cluster Management 8
Virtual Machine Management 12

4. Performance and Scale 22
AHV Turbo 22
vNUMA 22
RDMA 23
Memory Overcommit 23
Virtual Trusted Platform Module 24

5. GPU Support 25
GPU Passthrough 25
vGPU 25
vGPU Live Migration 27

6. Security 28
Security Development Life Cycle 28
Security Baseline and Self-Healing 28
Audits 29
Credential Guard 29
Flow Virtual Networking 29
Flow Network Security 30

7. Conclusion 32

8. Appendix 33

References....33

About Nutanix....34

List of Figures....35

1. Executive Summary

Nutanix natively converges compute and storage into a single appliance you can deploy in minutes to run any application out of the box. The Nutanix solution offers powerful virtualization capabilities—including core virtual machine (VM) operations, live migration, VM high availability, and virtual network management—as fully integrated features of the infrastructure stack rather than standalone products that require separate deployment and management.

The native Nutanix hypervisor, AHV, represents a fresh approach to virtualization that brings substantial benefits to enterprise IT administrators by simplifying every step of the infrastructure life cycle, from buying and deploying to managing, scaling, and supporting.

Document Version History

Version Number	Published	Notes
1.0	January 2022	Original publication.
1.1	July 2016	Updated platform information.
1.2	December 2016	Updated for AOS 5.0.
1.3	May 2017	Updated for AOS 5.1.
2.0	December 2017	Updated for AOS 5.5.
2.1	March 2019	Updated for AOS 5.10 and updated Nutanix overview.
2.2	January 2020	Updated Nutanix overview and the AHV section.
3.0	June 2020	Updated terminology throughout.

Version Number	Published	Notes
4.0	January 2022	Updated for AOS 6.1: Updated Live Migration, Backup APIs, and vGPU sections, and added VM Templates, OVA Import and Export, Metro Availability, Memory Overcommit, vGPU Live Migration, Credential Guard, Flow Network Visualization, and Flow Microsegmentation sections.
4.1	September 2022	Updated for AOS 6.5.1: Added the Virtual Trusted Platform Module section.

2. AHV

We built AHV on a proven open-source CentOS KVM foundation and extended KVM's base functionality to include features such as high availability (HA) and live migration. AHV comes preinstalled on Nutanix appliances and you can configure it in minutes to deploy applications.

There are three main components in AHV:

KVM-kmod

KVM kernel module.

Libvirtd

An API, daemon, and management tool for managing KVM and QEMU. Communication between AHV and KVM and QEMU occurs through libvirtd.

Qemu-KVM

A machine emulator and virtualization tool that runs in user space for every VM (domain). AHV uses it for hardware-assisted virtualization, and VMs run as hardware virtual machines (HVMs).

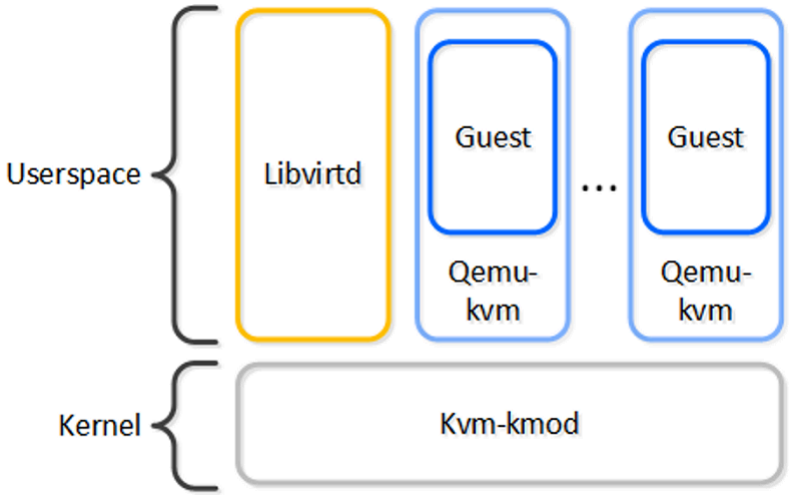

Figure 1: AHV Components

3. Integrated Management Capabilities

You can manage the Nutanix platform from a single pane of glass with Nutanix Prism. Prism provides integrated capabilities for cluster management and VM management that are available from the Prism graphical user interface (GUI), command line interface (CLI), PowerShell, and REST API.

Cluster Management

Managing clusters on AHV focuses on creating, updating, deleting, and monitoring cluster resources. These resources include hosts, storage, and networks.

Host Profiles

Prism provides a central location for administrators to update host settings like virtual networking and high availability across all nodes in an AHV cluster. Controlling configuration at the cluster level eliminates the need for manual compliance checks and reduces the risk of having a cluster that isn't uniformly configured.

Storage Configuration

Nutanix uses a hypervisor-agnostic distributed storage fabric to deliver data services such as storage provisioning, snapshots, clones, and data protection to VMs directly, rather than using the hypervisor's storage stack. On each AHV host, an iSCSI redirector service establishes a highly resilient storage path from each VM to storage across the Nutanix cluster.

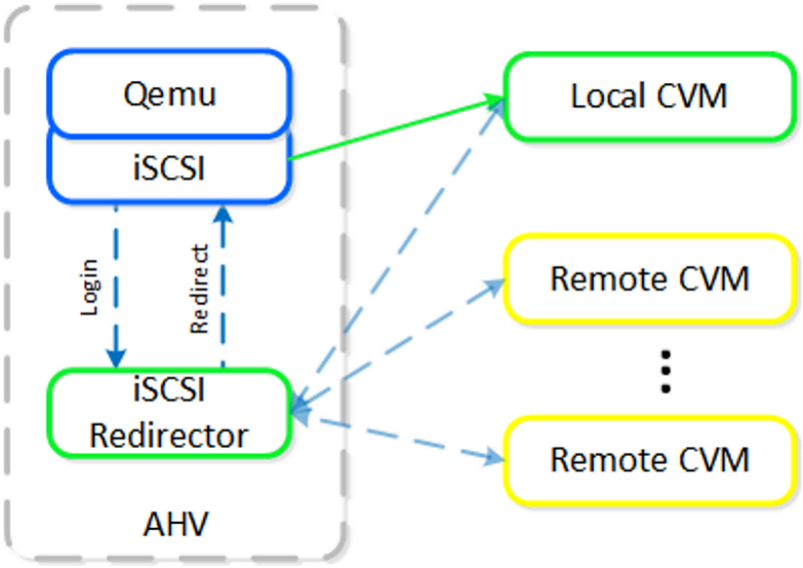

Figure 2: Storage Configuration

Virtual Networking

AHV uses Open vSwitch (OVS) for all VM networking. When you create a new AHV cluster, the system configures the Controller VM (CVM) and management networking paths automatically. Administrators can easily create new VLAN-backed layer 2 networks through Prism. Once you've created a network, you can assign it to existing and newly created VMs.

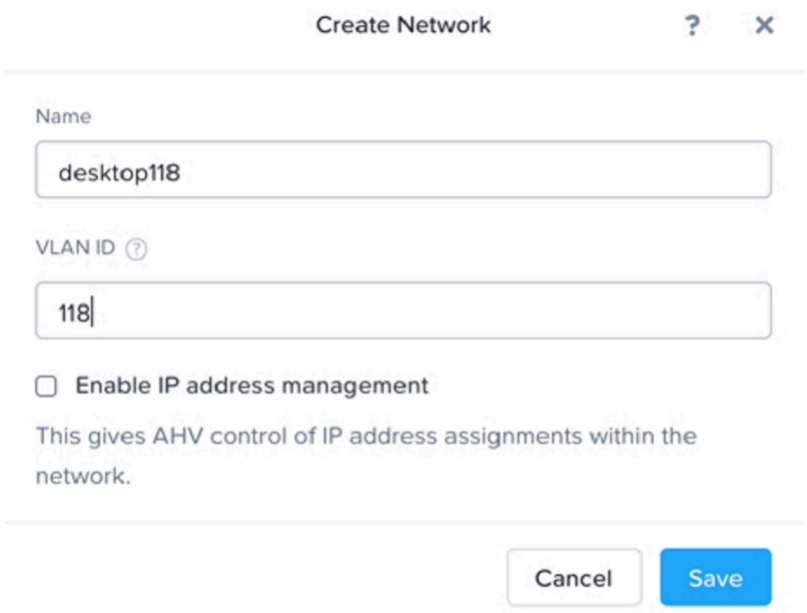

Figure 3: Creating a Network in Prism

Along with streamlining VM network creation, AHV can manage DHCP addresses for each network you create. This functionality allows administrators to configure address pools for each network that they can automatically assign to VMs.

Rolling Upgrades

Nutanix delivers a one-click upgrade process through the Life Cycle Manager (LCM) for all software in the Nutanix platform, including AOS, AHV, firmware, and Nutanix Cluster Check (NCC). Upgrades are nondisruptive and allow the cluster to run continuously while nodes upgrade on a rolling basis in the background, ensuring always-on cluster operation during software maintenance. LCM manages the complexity by understanding the dependencies between products and versions, and only shows upgrade options that are possible for the single or multiple upgrades selected. Nutanix qualifies firmware updates from the manufacturers of the hard or solid-state disk drives in the cluster and makes them available through the same upgrade process.

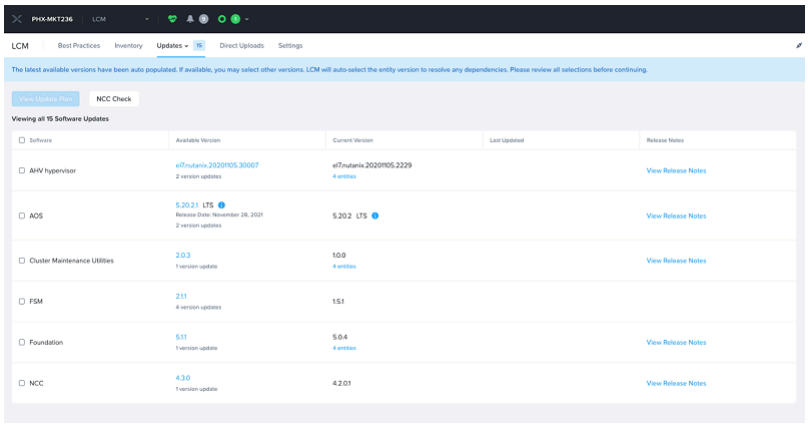

Figure 4: Nutanix LCM Upgrade Process

Host Maintenance Mode

Administrators can place AHV hosts in maintenance mode during upgrades and maintenance-related operations. Maintenance mode live-migrates all VMs running on the node to other nodes in the AHV cluster, and the CVM can safely shut down if required. Once the maintenance process has completed all the steps for the node, it returns the CVM to service and synchronizes with other CVMs in the cluster. Maintenance mode enables graceful host suspension for routine cluster maintenance.

Scaling

The Nutanix solution's scale-out architecture enables incremental, predictable capacity and performance scaling in a Nutanix cluster running any hypervisor, including AHV. Administrators can start with as few as three nodes and scale out theoretically without limits. The system automatically discovers new nodes and makes them available for use. Expanding clusters is as simple as selecting the discovered nodes you want to add and providing network configuration details. Through Prism, administrators can image or update new nodes to match the AHV version of their preexisting nodes for seamless node integration, no matter what version they installed originally.

Virtual Machine Management

VM management on AHV focuses on creating, updating, deleting, protecting the data of, and monitoring VMs and their resources. These cluster services and features are all available through the Prism interface, a distributed management layer that is available on the CVM on every AHV host.

VM Operations

Prism displays a list of all VMs in an AHV cluster along with configuration, resource usage, and performance details on a per-VM basis. Administrators can create VMs and perform many operations on selected VMs, including power on or off, power cycle, reset, shut down, restart, snapshot and clone, migrate, pause, update, delete, and launch a remote console.

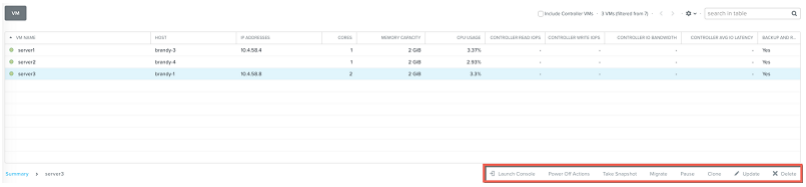

Figure 5: VM Operations in Prism

Image Management

The image management service in AHV is a centralized repository that provides access to virtual media and disk images and the ability to import from external sources. It enables you to store VMs as templates or gold images, which you can then use to create new VMs quickly from a known good base image. The image management service can store the virtual disk files you used to create the VMs or OS installation media as an .iso file that you can mount to provide a fresh OS install experience. Incorporated into Prism, the image management service can import and convert existing virtual disk formats, including .raw, .vhd, .vmdk, .vdi, and .qcow2. The previous virtual hardware settings don't constrain an imported virtual disk, so administrators have the flexibility to fully configure CPU, memory, virtual disks, and network settings when they provision VMs.

VM Templates

AHV has always had the image library, which captured data in a single vDisk so you could clone it easily, but required input from the admin to declare the CPU, memory, and network details. VM templates simplify this concept further. You create AHV VM templates from existing VMs, so they inherit the attributes of the defining VM, such as the CPU, memory, and networking details. You can then configure the template to customize the guest OS on deployment and provide a Windows license key if desired. With VM templates, you can maintain multiple versions of a template, making it easy to apply updates like operating system and application patches without needing to create new templates.

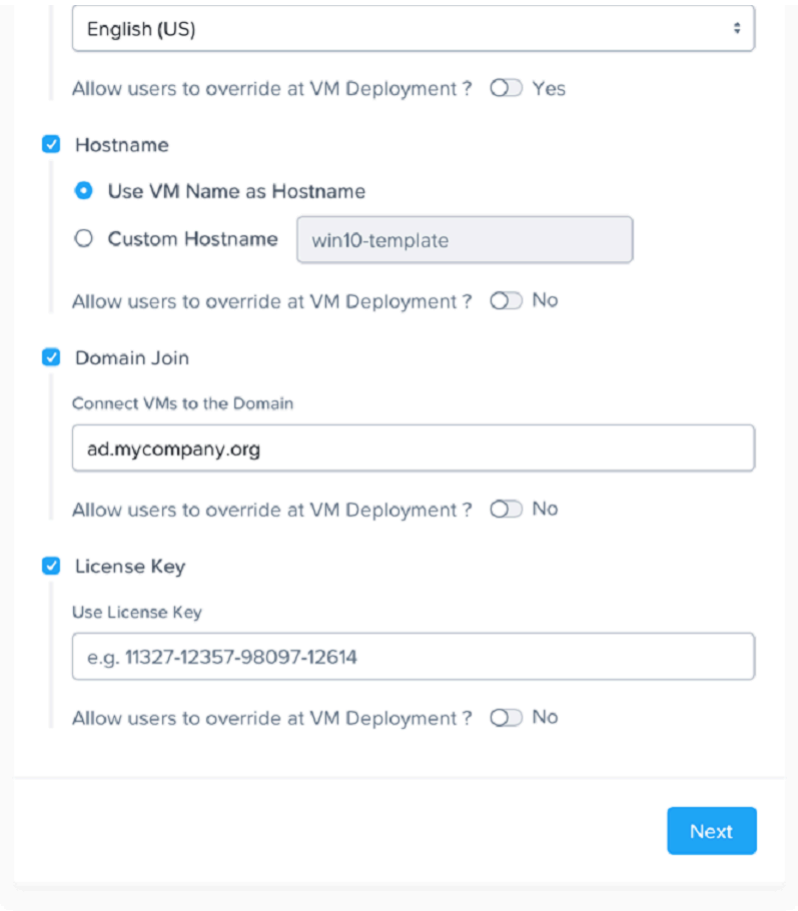

Figure 6: Template Configuration in Prism

OVA Import and Export

There are many situations where you might need to use an Open Virtual Appliance (OVA) file, but the most common are when you deploy virtual appliances (typically from a non-Nutanix vendor) and when you move VMs to a different hypervisor. To help you accomplish these tasks, the OVA import-and-export process is available in Prism Central. This process creates the OVA file, which is a tar archive file created when you convert a VM into an Open Virtualization Format (OVF) package that you can save to your local workstation.

Acropolis Dynamic Scheduling

Acropolis Dynamic Scheduling (ADS) is an automatic function enabled on every AHV cluster to avoid hot spots in cluster nodes. ADS continually monitors CPU, memory, and storage data points to make migration and initial placement decisions for VMs and Nutanix Volumes. Starting with existing statistical data for the cluster, ADS watches for anomalies, honors affinity controls, and only makes move decisions to avoid hot spots. Using machine learning, ADS can adjust move thresholds over time from their initial fixed values to achieve the greatest efficiency without sacrificing performance.

ADS tracks each individual node's CPU and memory usage. When a node's CPU allocation breaches its threshold (currently 85 percent of CVM CPU), Nutanix migrates VMs or Nutanix Volumes off that host as needed to rebalance the workload.

> Note: Migration only occurs when there's contention. If there's skewed usage between nodes (for example, three nodes at 10 percent and one at 50 percent), migration doesn't occur, as it offers no benefit unless there is contention for resources.

Intelligent VM Placement

When you create, restore, or recover VMs, the system assigns them to an AHV host in the cluster based on a recommendation from ADS. This VM placement process also takes into account the AHV cluster's HA configuration, so it doesn't violate any failover host or segment reservations. We explain these HA constructs in the Automated High Availability section.

Affinity and Antiaffinity

With affinity controls, you can govern where VMs run. AHV has two types of affinity controls:

1. VM-host affinity strictly ties a VM to a host or group of hosts, so the VM only runs on that host or group. Affinity is particularly applicable for use cases that involve software licensing or VM appliances. In such cases, you often need to limit the number of hosts an application can run on or bind a VM appliance to a single host.
2. Antiaffinity lets you declare that a given list of VMs shouldn't run on the same hosts. Antiaffinity allows clustered VMs or VMs running a distributed application to run on different hosts, increasing the application's availability and resilience. To prefer VM availability over VM separation, the system overrides this type of rule when a cluster becomes constrained.

Live Migration

Live migration allows the system to move VMs from one host to another while the host is turned on, regardless of whether the administrator or an automatic process initiates the movement. Live migration can occur when you place a host in maintenance mode, which evacuates all VMs. You can also use live migration to migrate VMs to another physical cluster or location or avoid planned interruptions.

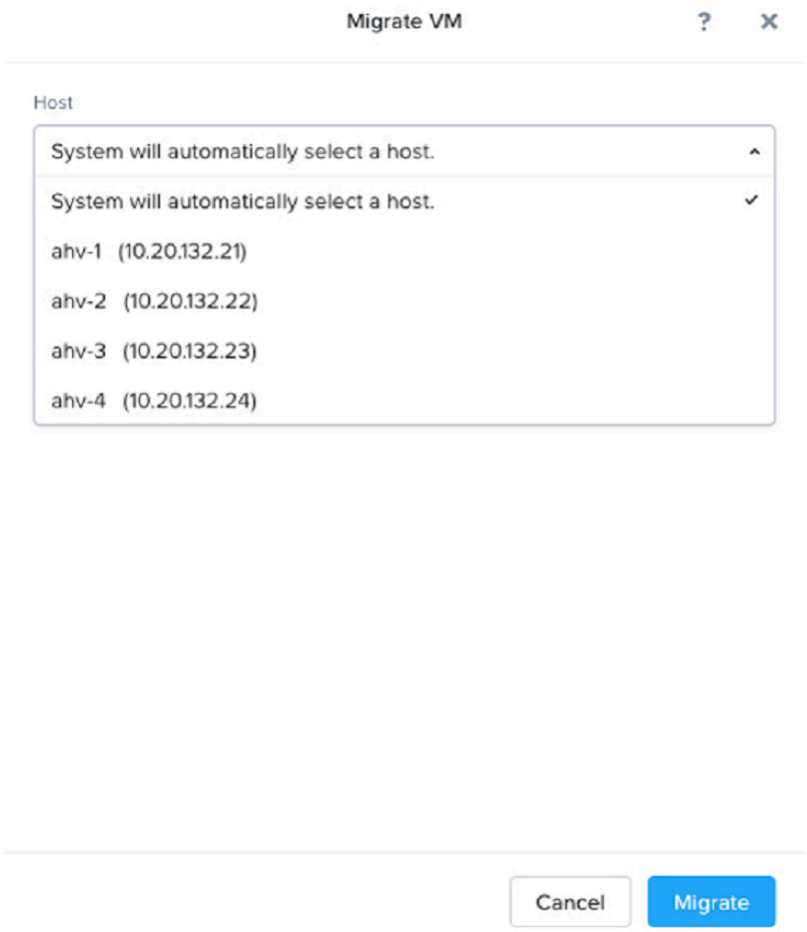

Figure 7: Migrating VMs

Cross-Hypervisor Migration

Nutanix simplifies the process of migrating existing VMs between an ESXi cluster and an AHV cluster using built-in data protection capabilities. You can create one or more protection domains on the source cluster and set the AHV cluster as the target remote cluster. Then, snapshot VMs on the source ESXi cluster and replicate them to the AHV cluster, where you can restore them and bring them online as AHV VMs.

Automated High Availability

AOS offers virtual machine high availability (VMHA) to ensure VM availability in the event of a host or block outage. If a host fails, the VMs previously running on that host restart on healthy nodes throughout the cluster. There are multiple HA configuration options available to account for different cluster scenarios:

- By default, all AHV clusters provide best-effort HA, even when you haven't configured the cluster for HA. Best-effort HA works without reserving any resources and does not enforce admission control, so the capacity may not be sufficient to start all the VMs from the failed host.
- You can also configure an AHV cluster for HA with resource reservation to guarantee that the resources required to restart VMs are always available. To enable guaranteed HA reservations, select the Enable HA Reservation checkbox.

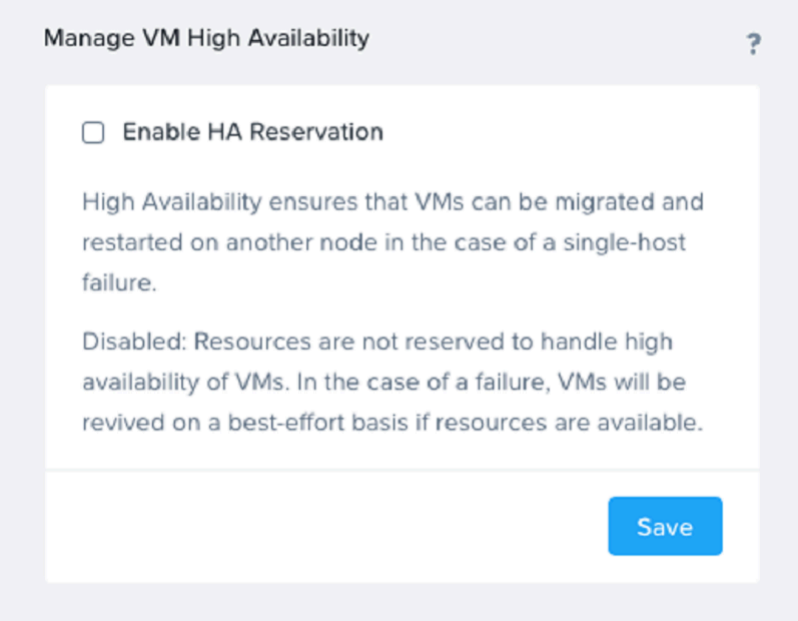

Figure 8: High Availability

The Acropolis Leader CVM restarts the VMs on the healthy hosts and tracks host health by monitoring connections to the libvirt on all cluster hosts. If the Acropolis Leader becomes partitioned or isolated, or if it fails, the healthy portion of the cluster elects a new Acropolis Leader.

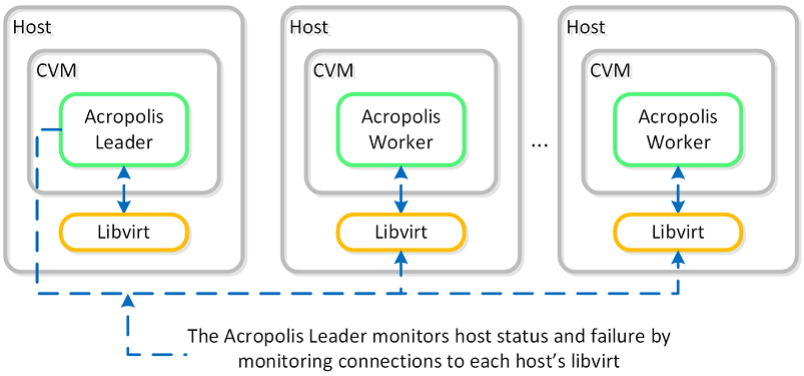

Figure 9: Acropolis Leader Monitoring

Never-Schedulable Nodes

With AHV, you can declare a node as never schedulable when joining it to a cluster. Commonly referred to as storage-only nodes, these never-schedulable nodes enable you to scale the storage performance and capacity of a cluster without expanding the compute resources. Because you configure this setting when you join a node to a cluster, you can't easily undo it without removing the node from the cluster and rejoining it as a regular node. This setting is most helpful when you need to scale storage resources for workloads licensed by compute resources, such as popular database services. By preventing the workload from using the compute resources of these nodes and making the action difficult to undo, we meet the strict licensing requirements of these solutions.

Converged Backup and Disaster Recovery

Nutanix converged backup and disaster recovery services protect your clusters. Nutanix clusters running any hypervisor have access to these features, which safeguard VMs both locally and remotely for use cases ranging from basic file protection to recovery from a complete site outage. To learn more about the built-in backup and disaster recovery capabilities in the Nutanix platform, read the Data Protection and Disaster Recovery tech note.

Metro Availability

Metro Availability creates a global file system namespace across Nutanix clusters and uses synchronous replication. Combining the Nutanix

hyperconverged infrastructure with a continuous availability solution limits downtime and preserves all data, even during a complete site failure. Metro Availability also enables workload mobility for disaster avoidance and planned maintenance scenarios. Administrators can use Metro Availability to extend hypervisor clustering technologies across datacenters. We call this type of configuration a stretched cluster, and it helps to minimize downtime during unplanned outages.

Metro Availability also supports VM migration across sites using technologies like live migration, which means you have zero downtime while transitioning workloads between datacenters. Nutanix has built safeguards into the platform for everything from minor events, such as individual VM deletion, to major ones, including unplanned datacenter failure.

Backup APIs

AHV also publishes a rich set of APIs to support external backup vendors. The AHV backup APIs use changed region tracking to allow backup vendors to back up only the data that has changed since the last backup job for each VM. Changed region tracking also allows backup jobs to skip reading zeros, further reducing backup times and bandwidth consumed.

Nutanix backup APIs allow backup vendors that build integration to perform full, incremental, and differential backups. Changed region tracking is always on in AHV clusters; you don't need to enable it on each VM. Backups can be either crash consistent or application consistent.

Another feature available in the backup APIs is instant recovery, which enables supported backup vendors to instantly recover a VM or vDisk typically on their backup appliance and allow immediate access to its contents. You can use and delete the VM or vDisk or migrate it to a Nutanix volume for permanent storage.

Analytics

Nutanix Prism offers in-depth analytics for every element in the infrastructure stack, including hardware, storage, and VMs. Administrators can use Prism views to monitor these infrastructure stack components, and they can use the Analysis view to get an integrated assessment of cluster resources or to drill down to specific metrics on a given element.

Prism makes detailed VM data available, grouping it into the following categories:

- VM Performance: Multiple charts with CPU- and storage-based reports around resource usage and performance.
- Virtual Disks: In-depth data points that focus on I/O types, I/O metrics, read source, cache hits, working set size, and latency on a per–virtual disk level.
- VM NICs: vNIC configuration summary for a VM.
- VM Snapshots: A list of all snapshots for a VM with the ability to clone or restore from the snapshot or to delete the snapshot.
- VM Tasks: A time-based list of all operational actions performed against the selected VM. Details include task summary, percent complete, start time, duration, and status.
- Console: Administrators can open a pop-up console session or an inline console session for a VM.

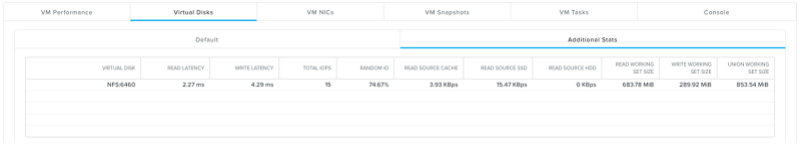

Figure 10: Prism Analytics

The Storage tab provides a direct view into the storage fabric running on an AHV cluster. Administrators can look at detailed storage configurations, capacity usage over time, space efficiency, and performance, as well as a list of alerts and events related to storage.

The Hardware tab gives you a direct view into the Nutanix blocks and nodes that make up a cluster. These reports are available in both a diagram and a table format for easy consumption.

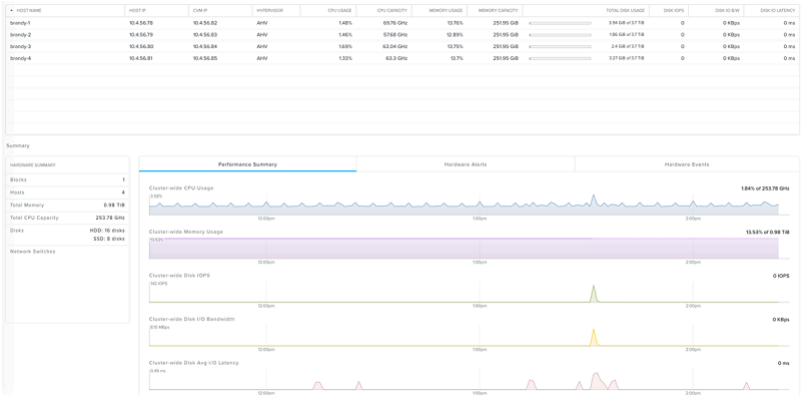

Figure 11: Performance Summary in Prism

The Prism Analysis tab gives administrators the tools they need to explore and understand what is going on in their clusters quickly and to identify steps for remediation as required. You can create custom interactive charts using hundreds of metrics available for elements such as hosts, disks, storage pools, storage containers, VMs, protection domains, remote sites, replication links, clusters, and virtual disks, then correlate trends in the charts with alerts and events in the system. You can also choose specific metrics and elements and set a desired time frame when building reports, so you can focus precisely on the data you're looking for.

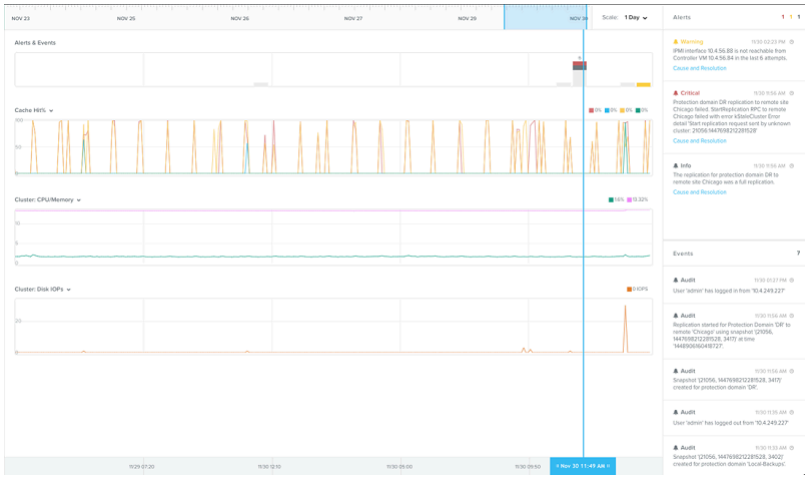

Figure 12: Prism Analysis

4. Performance and Scale

The Nutanix platform optimizes performance at both the AOS and hypervisor levels. The CVMs that represent the control and data planes contain the AOS optimizations that benefit all supported hypervisors. Although we built AHV on a foundation of open-source KVM, we added a significant amount of innovation to make AHV a unique Nutanix offering. The following sections outline a few of the innovations in AHV focused on performance.

AHV Turbo

AHV Turbo represents significant advances to the data path in AHV over the core KVM source code foundation. In the core KVM code, all I/O from a given VM flows through the hosted VM monitor, QEMU. While this architecture can achieve impressive performance, some application workloads require still higher capabilities. AHV Turbo provides a new I/O path that bypasses QEMU and services storage I/O requests, which decreases CPU usage and increases the amount of storage I/O available to VMs.

When using QEMU, all I/O travels through a single queue, which is another issue that can impact performance. The new AHV Turbo design introduces a multiqueue approach to allow data to flow from a VM to storage, resulting in a much higher I/O capacity. The storage queues scale out automatically to match the number of vCPUs configured for a given VM, making even higher performance possible as the workload scales up.

While these improvements demonstrate immediate benefits, they also prepare AHV for future technologies such as NVMe and persistent memory advances that offer dramatically increased I/O capabilities with lower latencies.

vNUMA

Modern Intel server architectures assign memory banks to specific CPU sockets. In this design, one of the memory banks in a server is local to each CPU, so

you see the highest level of performance when accessing memory locally, as opposed to accessing it remotely from a different memory bank. Each CPU and memory pair is a NUMA node. vNUMA is a function that allows a VM's architecture to mirror the NUMA architecture of the underlying physical host.

vNUMA isn't applicable to most workloads, but it can be beneficial to large VMs configured with more vCPUs than there are available physical cores in a single CPU socket. In these scenarios, configure vNUMA nodes to use local memory access efficiently for each CPU to achieve the highest performance results.

RDMA

Remote direct memory access (RDMA) enables a node to write to the memory of a remote node by granting a VM running in the user space access to a NIC directly. This approach avoids TCP and kernel overhead, resulting in CPU savings and performance gains. At this time, AOS RDMA support is reserved for inter-CVM communications and uses the standard RDMA over Converged Ethernet (RoCEv2) protocol on systems configured with RoCE-capable NICs connected to properly configured switches with datacenter bridging (DCB) support.

Memory Overcommit

One of the central benefits of virtualization is the ability to overcommit compute resources, making it possible to provision VMs with more CPUs than are physically present on the server host. Most workloads don't need 100 percent of their assigned CPU all the time, and the hypervisor can dynamically allocate CPU cycles to workloads that need them when they need them.

You can also overcommit memory. The VMs on the host may not use all their allocated memory, and the hypervisor can share that unused memory with other workloads. Memory overcommit enables administrators to provision more VMs per host by combining the unused memory and allocating it to VMs that need it.

AOS 6.1 brings memory overcommit to AHV for environments like test and development that need additional memory and VM density. You define

overcommit on a per-VM basis, so you control whether to share memory between all VMs on a cluster or just a subset.

Virtual Trusted Platform Module

A Trusted Platform Module is a piece of hardware in a server or computer that provides secure storage for keys or credentials. A virtual TPM (vTPM) is an integrated feature in the hypervisor that provides the same functionality but is implemented as software for virtual machines to use. Windows 11 is and likely will remain the primary reason most organizations use a vTPM in their environments, as it's a requirement for running operating system virtually.

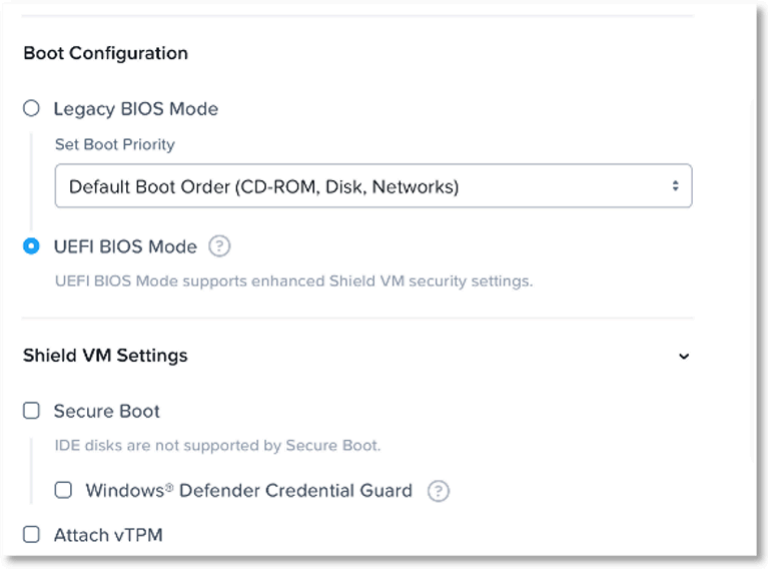

Figure 13: vTPM Assignment

5. GPU Support

A graphics processing unit (GPU) is the hardware or software that displays graphical content to end users. In laptops and desktops, a GPU is either a physical card or built directly into the CPU hardware, while GPU functions in the virtualized world have historically been software driven and consumed additional CPU cycles. With modern operating systems, applications, and 3D tools, more organizations find themselves needing a hardware GPU in the virtual world. You can install physical GPU cards in qualified hosts and present them to guest VMs using passthrough or vGPU mode.

GPU Passthrough

The GPU cards deployed in server nodes for virtualized use cases typically combine multiple GPUs in a single PCI card. With GPU passthrough, AHV can pass a GPU through to a VM, allowing the VM to own that physical device in a 1:1 relationship. Configuring nodes with one or more GPU cards that attach multiple GPUs to a larger number of VMs allows you to consolidate applications and users on each node. AHV currently supports NVIDIA Grid cards for GPU passthrough; refer to our product documentation for the current list of supported devices.

With passthrough, you can also use GPUs for offloading computational workloads—a more specialized situation than the typical graphical use cases. GPU compute scenarios assign one or more GPUs for a VM to use for processing. AHV allows you to assign up to 16 GPU to a single VM, whereas competing hypervisors permit you to assign only 1 GPU per VM.

vGPU

While passthrough is a method that works well for a smaller number of VMs requiring larger amounts of GPU resources, workloads such as VDI often have different requirements. VDI workloads typically have a much larger number of

VMs that need varying amounts of GPU resources based on application types and usage.

Today's NVIDIA Grid GPU cards contain 1–4 GPU on each physical PCI card, and each physical host can support installing one or two cards. This capability allows for up to 8 GPU in each node to meet density requirements driven by VDI workloads. For maximum flexibility, vGPU mode allows you to slice each GPU into smaller segments that you can virtually assign to VMs.

vGPU profiles allow you to assign different levels of resources to VMs, so each of them can use a defined maximum number of displays and quality of resolution. Working within these parameters lets you choose the correct GPU profile to meet your application requirements, and when you also know the type and number of GPU cards in your deployment, you can accurately describe the maximum density possible per host.

In some rare use cases you may need additional GPU resources for demanding workloads. With AHV, you can assign multiple vGPU profiles to a single VM to fulfill the requirements of these workloads.

AHV currently supports NVIDIA Grid cards for vGPU; refer to our product documentation for the current list of supported devices.

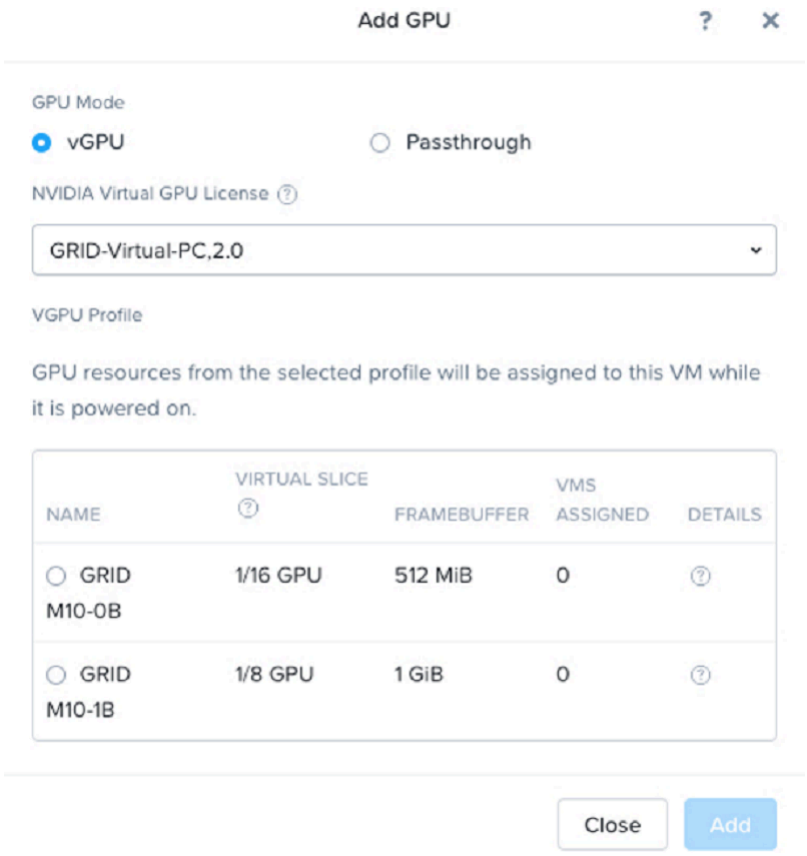

Figure 14: vGPU Profile Assignment

vGPU Live Migration

If you want maintenance operations like upgrades and failure handling to be as efficient as possible, you need the ability to migrate your VMs. With AHV, you can live-migrate VMs with vGPU assignments.

6. Security

The fully integrated Nutanix infrastructure stack eliminates security risks associated with legacy solutions that involve many vendors with a narrow, fragmented view of security. For example, Nutanix designed AHV to be an integral component of the converged infrastructure stack rather than a general-purpose hypervisor. Consequently, to reduce the security surface area, you can turn off many of the services AHV makes unnecessary.

Security Development Life Cycle

To maintain agile and comprehensive security, Nutanix has developed its own Security Development Life Cycle (SecDL), which addresses security at every step of the development process instead of applying it at the end. SecDL integrates security features into the software development process, including automated security testing during development and threat modeling to assess and mitigate customer risk from code changes.

Security Baseline and Self-Healing

Nutanix has developed custom Security Technical Implementation Guides (STIGs), security tools based on well-established National Institute of Standards and Technology (NIST) standards, that administrators can apply to multiple baseline requirements for DoD and PCI-DSS. Unlike general-purpose STIGs that make blanket security recommendations, Nutanix STIGs are specific to the Nutanix platform and therefore more effective. Encoded in a machine-readable format, Nutanix STIGs enable automated validation, ongoing monitoring, and self-remediation, reducing the time required to verify security compliance from weeks or months to days.

You can read more about the Nutanix approach to information security in the Information Security tech note.

Audits

The audits log in Prism provides a comprehensive list of all actions taken by administrators and users against AHV resources. You can easily locate details on who took an action (such as VM creation, deletion, and updates) and when.

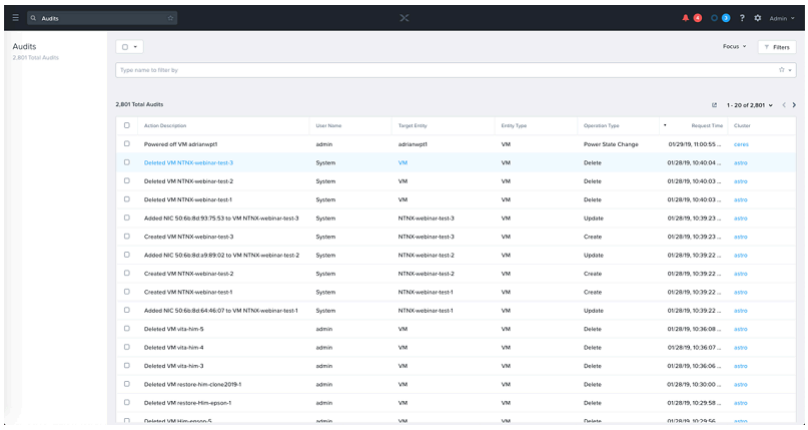

Figure 15: Prism Audits Log

Credential Guard

Credential Guard is an additional virtualization-based security layer for the Local Security Authority Subsystem Service (LSASS) process, which stores credentials for New Technology LAN Manager (NTLM) and Kerberos. Credential Guard isolates the LSASS process in a virtual container that can't be accessed by users and creates a proxy process to communicate with it, protecting the system from further lateral incursion. It's available with Windows 10 Enterprise and Education editions when you use a Hypervisor-Provided Code Integrity (HVCI) driver and a supported hardware BIOS version.

Flow Virtual Networking

Nutanix Flow Virtual Networking is a software-defined network virtualization solution that provides overlay capabilities for on-premises AHV clusters. It deploys networking features like a Virtual Private Cloud (VPC) and Virtual Private Network (VPN) to support flexible app-driven networking that focuses

on VMs and applications instead of virtual LANs and network addresses. With Flow Networking, you get the following benefits:

- A simplified, Prism Central–based workflow that deploys the application-driven network virtualization feature.
- A secure multitenancy solution that enables per-tenant isolation using VPC-based network segmentation and namespace isolation.
- A secure, VPN-based connectivity solution for multiple sites, with automated VPN bundle upgrades.
- NAT-based secure egress to external networks, with IP address retention and policy-based routing.
- Self-serve networking services using REST APIs.
- Enhanced networking features for more effective disaster recovery.

Flow Network Security

Nutanix Flow Network Security protects against new threats designed to spread laterally from one system to another in the same protected datacenter. Because perimeter-based firewalls traditionally only protect the environment from external threats, it can be difficult to repurpose them to protect internal traffic. The problem is compounded by virtualized workloads changing their network configurations and hosts as they start, stop, and migrate frequently. Flow Network Security applies security rules between all applications and VMs in the datacenter, adding internal protection behind your perimeter firewall.

Flow Network Security includes a policy-driven security framework that inspects traffic in the datacenter. Security policies are applied to categories (a logical grouping of VMs) and not to the VMs themselves. Therefore, it doesn't matter how many VMs you have in a category; traffic associated with that category is secured without administrative intervention at any scale.

The framework uses a workload-centric approach instead of a network-centric approach, so it can scrutinize traffic to and from VMs in a datacenter regardless of changes to their network configurations or their locations in the datacenter.

This approach also enables the virtualization team to implement these security policies without having to rely on network security teams.

Prism Central works with Flow Network Security to offer a visualization-based approach to configuring security policies and monitoring the traffic a policy applies to.

7. Conclusion

The Nutanix stack embodies a radically new approach to infrastructure—one that simplifies every step of the life cycle from buying and deploying to managing, scaling, and supporting. The Nutanix solution's web-scale technologies and architecture let you run any workload at any scale. With Nutanix AOS and Nutanix Prism, administrators get powerful virtualization capabilities fully integrated into the converged infrastructure stack and managed from a single pane of glass.

8. Appendix

References

- Data Protection and Disaster Recovery tech note
- Information Security tech note

About Nutanix

Nutanix is a global leader in cloud software and a pioneer in hyperconverged infrastructure solutions, making clouds invisible and freeing customers to focus on their business outcomes. Organizations around the world use Nutanix software to leverage a single platform to manage any app at any location for their hybrid multicloud environments. Learn more at www.nutanix.com or follow us on Twitter @nutanix.

List of Figures

Figure 1: AHV Components....7
Figure 2: Storage Configuration....9
Figure 3: Creating a Network in Prism....10
Figure 4: Nutanix LCM Upgrade Process....11
Figure 5: VM Operations in Prism....12
Figure 6: Template Configuration in Prism....13
Figure 7: Migrating VMs....16
Figure 8: High Availability....17
Figure 9: Acropolis Leader Monitoring....18
Figure 10: Prism Analytics....20
Figure 11: Performance Summary in Prism....21
Figure 12: Prism Analysis....21
Figure 13: vTPM Assignment....24
Figure 14: vGPU Profile Assignment....27
Figure 15: Prism Audits Log....29