NUTANIX
YOUR ENTERPRISE CLOUD

Commvault with Nutanix

Nutanix Best Practices

Version 3.0 • November 2020 • BP-2045

Copyright

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

Contents

1. Executive Summary

The Nutanix enterprise cloud is a highly resilient converged compute and storage system that adapts web-scale architecture to benefit all kinds of organizations. This document makes recommendations for optimizing and scaling Commvault with Nutanix on both Nutanix AHV and VMware vSphere. It also covers the option of using Nutanix Objects as an additional backup target. In this guide, we show the elasticity of the platform and provide configuration information on the scale-out capabilities of both Commvault and Nutanix.

Combining Commvault with Nutanix AHV and the Nutanix operating system (AOS) enables an end-to-end complete backup solution for large-scale deployments with minimal configuration. The ESXi solution with Commvault's network block device (NBD) backup mode allows customers to back up large-scale Nutanix deployments easily with the most reliable transport method available today. Both solutions let customers choose between using either virtual or physical Commvault servers, depending on their requirements and available hardware.

2. Introduction

2.1. Audience

This best practices guide is part of the Nutanix Solutions Library. We wrote it for IT administrators and architects who want to understand the data protection and disaster recovery features built into the Nutanix enterprise cloud. Consumers of this guide should have basic familiarity with Nutanix software.

2.2. Purpose

This document covers the high-level best practices for Commvault and Nutanix, focusing on an optimized disk-to-disk backup architecture. We include a best practices checklist to help you make sure you've implemented all the applicable guidance.

2.3. Synergistic Technologies

Commvault's distributed and scale-out design strongly complements the web-scale Nutanix solution and its data locality technology. The Commvault on Nutanix solution uses the strengths of both products to provide network-efficient backups to meet recovery point objective (RPO) and recovery time objective (RTO) requirements. The framework is flexible enough to use either 100 percent virtualized Commvault components or a combination of virtual and physical components, based on the user's requirements and the hardware they have available.

Table 1: Document Version History

Version Number	Published	Notes
1.0	April 2016	Original publication.
1.1	July 2016	Updated IntelliSnap Plus Backup Copy section and Best Practices Checklist with disaster recovery-related best practices.
1.2	April 2017	Updated platform overview and added IntelliSnap with Replication section.

Version Number	Published	Notes
1.3	March 2018	Updated platform overview.
2.0	May 2019	Updated Nutanix overview and added AHV and Nutanix Objects support.
2.1	August 2019	Updated product naming.
2.2	June 2020	Updated Nutanix overview and performance tuning guidance.
3.0	November 2020	Updated transport mode definitions, Commvault sizing guidelines, and networking recommendations.

3. Nutanix Enterprise Cloud Overview

Nutanix delivers a web-scale, hyperconverged infrastructure solution purpose-built for virtualization and both containerized and private cloud environments. This solution brings the scale, resilience, and economic benefits of web-scale architecture to the enterprise through the Nutanix enterprise cloud platform, which combines the core HCI product families—Nutanix AOS and Nutanix Prism management—along with other software products that automate, secure, and back up cost-optimized infrastructure.

Available attributes of the Nutanix enterprise cloud OS stack include:

- Optimized for storage and compute resources.
- Machine learning to plan for and adapt to changing conditions automatically.
- Intrinsic security features and functions for data protection and cyberthreat defense.
- Self-healing to tolerate and adjust to component failures.
- API-based automation and rich analytics.
- Simplified one-click upgrades and software life cycle management.
- Native file services for user and application data.
- Native backup and disaster recovery solutions.
- Powerful and feature-rich virtualization.
- Flexible virtual networking for visualization, automation, and security.
- Cloud automation and life cycle management.

Nutanix provides services and can be broken down into three main components: an HCI-based distributed storage fabric, management and operational intelligence from Prism, and AHV virtualization. Nutanix Prism furnishes one-click infrastructure management for virtual environments running on AOS. AOS is hypervisor agnostic, supporting two third-party hypervisors—VMware ESXi and Microsoft Hyper-V—in addition to the native Nutanix hypervisor, AHV.

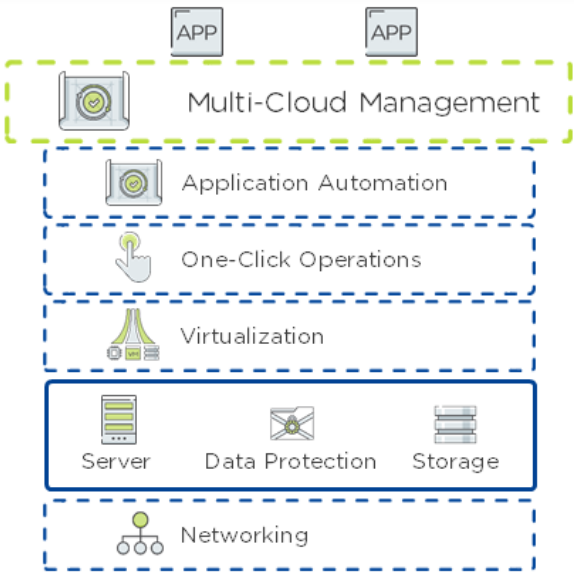

Figure 1: Nutanix Enterprise Cloud OS Stack

3.1. Nutanix HCI Architecture

Nutanix does not rely on traditional SAN or network-attached storage (NAS) or expensive storage network interconnects. It combines highly dense storage and server compute (CPU and RAM) into a single platform building block. Each building block delivers a unified, scale-out, shared-nothing architecture with no single points of failure.

The Nutanix solution requires no SAN constructs, such as LUNs, RAID groups, or expensive storage switches. All storage management is VM-centric, and I/O is optimized at the VM virtual disk level. The software solution runs on nodes from a variety of manufacturers that are either entirely solid-state storage with NVMe for optimal performance or a hybrid combination of SSD and HDD storage that provides a combination of performance and additional capacity. The storage fabric automatically tiers data across the cluster to different classes of storage devices using intelligent data placement algorithms. For best performance, algorithms make sure the most frequently used data is available in memory or in flash on the node local to the VM.

To learn more about the Nutanix enterprise cloud software, please visit the Nutanix Bible and Nutanix.com.

4. Solution Overview

Performing backups in a VMware environment requires that several components interact and that you use VMware vStorage APIs for Data Protection (VADP). In a Nutanix AHV environment, the virtualized VMs must have Nutanix Guest Tools (NGT). Commvault fully supports AHV, so you don't need to install anything else. The Nutanix solution can take advantage of the Commvault scale-out proxy architecture by using multiple virtual Commvault proxies or one or more physical proxies. Physical proxies offload the CPU workload from the Nutanix cluster. The following sections describe the components involved in the backup process.

4.1. Component Overview

The next two tables highlight the different components and virtualization or guest OS–related technologies for the joint solution.

The following table explains the backup components.

Table 2: Backup Components

Nutanix AHV	The native Nutanix hypervisor included with the operating system (AOS) that delivers enterprise-ready virtualized solutions for the multicloud world.
Nutanix Controller VM (CVM)	The CVM runs the Nutanix distributed storage fabric and serves all I/O operations for the hypervisor and all VMs running on that host. The CVM pools and exports storage to the hypervisor as an NFS datastore.
Nutanix Objects	The Nutanix S3-compatible object storage solution that environments can use as a backup target. Objects is currently only supported on AHV.
CommServe	CommServe is the Commvault command and control center. It contains the Microsoft SQL database that stores the CommCell group members, settings, and other metadata. Because CommServe uses a distributed, two-tiered indexing system for tracking managed data, it controls the size of the metadata database. CommServe manages administrative functions, communicating with agents and MediaAgents to initiate data protection, management, and recovery operations.

MediaAgent	The MediaAgent is the data transmission server. It provides high-performance data movement and manages data storage. CommServe coordinates MediaAgent tasks. For scalability, there can be more than one MediaAgent in a CommCell. You can install the MediaAgent software in physical, virtual, and clustered environments.
Virtual Server Agent (VSA)	The VSA provides a unified protection and recovery vehicle for all VM data.

The following table explains the backup technologies.

Table 3: Backup Technologies

VMware vSphere Storage APIs – Data Protection	VMware vSphere Storage APIs – Data Protection is the most recent version of the data protection framework VMware introduced with vSphere 4.0. It lets you perform centralized, highly efficient, and LAN-free VM backups. For more information, see VMware KB article 1021175 (link in appendix).
Nutanix AHV Changed Block Tracking (CBT)	Nutanix AHV CBT enhances the backup performance of Nutanix AHV virtual disks. When Nutanix AHV CBT for IntelliSnap is enabled, the system uses a REST API to detect the changed meta-data regions of the virtual disks by comparing snapshots. This feature can reduce the read operations required for full backups.
VMware Changed Block Tracking (CBT)	CBT is a feature that tracks VM disk sectors that have changed. VMware vSphere Storage APIs – Data Protection uses CBT to generate effective incremental VM backups. It allows Commvault to back up only changed data blocks, greatly increasing backup performance and reducing network bandwidth. The system performs read operations locally, eliminating the load on the network and other Nutanix nodes.
Microsoft VSS	Microsoft VSS is the built-in framework for application-consistent backups. VSS lets you create a consistent snapshot of application data, such as Microsoft Exchange, SQL, Active Directory, or the NTFS file system. Commvault can use VSS to ensure application-consistent backups for VSS-aware applications.

4.2. Commvault Component Sizing

Sizing Commvault servers depends on the number of Nutanix nodes, the total number of virtual machines, and the estimated size of the backup repository. To take advantage of data locality, we recommend running Virtual Server Agent (VSA) servers on each Nutanix node hosting VMs.

Commvault dynamically distributes VMs for backup across available VSA proxies, both at the beginning of the backup job and while the backup is running. When a backup operation starts, the first VSA proxy listed for the VSA instance acts as a coordinator, controlling traffic for backups across all proxies. Dynamic distribution improves performance, enhances scalability, and ensures fault tolerance for backup operations.

Review the material at the links below for more details:

- Minimum requirements for the Commvault package
- Minimum requirements for the CommServe server
- Commvault Media Agent requirements
- Commvault scaling recommendations

4.3. Deployment Models

As shown in the following figure, Commvault supports the backup repository with a variety of potential targets, including a secondary Nutanix or Nutanix Mine cluster, existing physical servers, NAS, or dedicated backup appliances. You can use either Nutanix default storage or Nutanix Objects as a backup target.

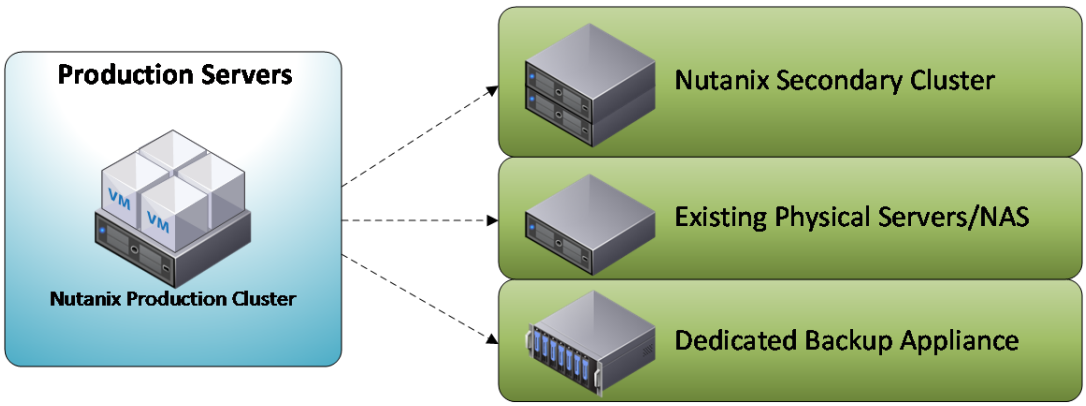

Figure 2: Commvault Repository Options

There are three options when forming the Nutanix secondary cluster as the backup target:

1. Create a Nutanix cluster to store the backed-up data and run other VMs. Depending on your performance and availability requirements, the additional, non-Commvault workload running in the cluster can be development, test, or production.
2. Create a Nutanix cluster to store only the CommServe, MediaAgent, and backed-up data. Nutanix recommends this approach for brownfield Nutanix environments.
3. Use a cluster of Nutanix Mine appliances powered by Commvault for simplified deployment and scalability. Nutanix recommends this approach for greenfield Nutanix environments.

In all the preceding options, you can deploy the Nutanix cluster either as an independent Nutanix storage target or as an object storage target using Nutanix Objects. The following sections provide guidance for two scenarios:

1. A 100 percent virtualized solution on Nutanix, with the option to use Nutanix Objects.
2. Using a physical backup or proxy server.

When using ESXi, Commvault and Nutanix recommend using network block device (NBD) mode instead of hot-add mode. NBD mode enables large-scale environments to perform more reliable backups with a simpler configuration. Additionally, once you factor in the time it takes to mount or unmount disks using hot-add, the difference in performance is negligible. For more information regarding transport modes, review Commvault documentation.

In NBD mode, CommServe connects to the ESXi management network VMkernel port and transfers backup data to the proxy. The network performance does not depend on the VMware switch type, but rather on the speed of the NIC that the ESXi management traffic uses. For the best performance, Nutanix recommends using the Nutanix dual 10 Gbps or faster NIC interfaces.

If the ESXi management interfaces use the 1 Gbps NICs, the backup speed is limited to 60–80 MBps per ESXi host. Using the fastest NICs boosts network speed; additionally, Commvault global source-side deduplication transfers truly unique blocks only, which can reduce overall network requirements by up to 90 percent.

When using AHV, application-consistent mode is the default. If the system cannot perform an application-consistent backup, it attempts a crash-consistent backup. Commvault uses NGT to perform backups at the file system and application levels and hot-add for the transport mode.

4.4. Virtualized Commvault on Nutanix

The following figure shows an entirely virtualized Commvault solution on Nutanix. In this solution each Nutanix compute node (a node that can run VMs) runs a VSA that uses data locality to reduce network congestion and improve read performance from the local flash. All VM data is read using network mode over the 10 Gbps NICs. The solution uses CBT to reduce read operations to only new blocks of data.

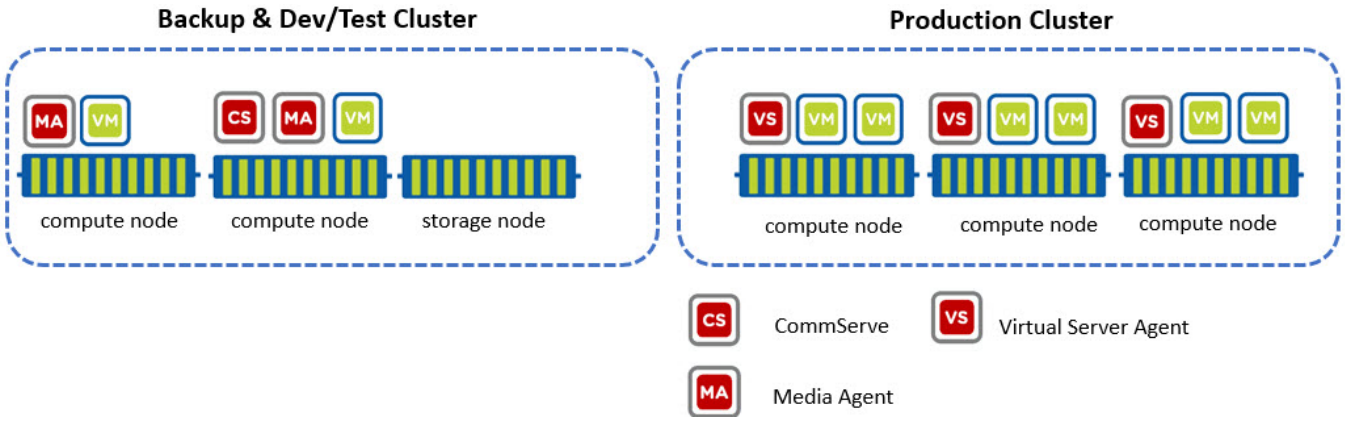

Figure 3: Virtualized Commvault Deployment Model

In this solution, the CommServe has a VSA installed as well, and you can set it up to restore VMs for testing on the target backup cluster. Every node in this case has a VM running the VSA to read from the local performance tier. You can add storage in the form of Nutanix storage-only nodes to increase backup capacity and provide longer retention periods. The storage-only nodes are AHV-based, so they don't require any additional vSphere licensing to expand your environment. You can use multiple MediaAgents on the backup cluster to drive additional throughput if you need it. In general, though, use one MediaAgent per vSphere cluster.

For indexing files, we recommend using the default Commvault live browse feature, which dynamically indexes the VM disk at the time of recovery. This indexing approach saves time during backup because you don't have to index the files in the guest VM. The tradeoff for indexing on the restore is that it takes a few more minutes to mount the VM and open the disk to browse the contents than it does to look at a prebuilt index. One great benefit of both indexing options is that there is no need for any agents—not even temporary ones—which means fewer headaches administering VMs.

When you configure a storage policy with deduplication, the system generates signatures for the data blocks during backups, compares them, and then stores them in the deduplication database (DDB). Commvault constantly monitors the performance of the DDB, and if performance degradation occurs, Commvault alerts you and advises you to move the DDB to faster storage. You can seal the DDB if you run into performance issues. The sealing process closes the existing DDB and starts a new DDB. When the new database starts, the next instance of each data block processed creates a new signature tracking entry and the data block writes to the disk again as a new initial baseline.

You may be able to boost the performance of overallocated SSD tiers by using VM Flash Mode, but enabling VM Flash Mode must be based on a Nutanix Support recommendation.

When you deploy an entirely virtualized solution on Nutanix, place the components in a secondary Nutanix cluster. This placement provides maximum protection from a complete

Nutanix production cluster failure and allows you to scale out the backup repository independent of the production VMs. A secondary Nutanix cluster is also an ideal solution if your organization has multiple remote locations that need to replicate to a centralized DR repository.

4.5. Virtualized Commvault with Nutanix Objects

From the AOS 5.11 release onward, Nutanix also offers an S3-compatible object store called Objects for use with AHV. Because Commvault supports most S3-compatible object stores as backup targets, using Nutanix Objects is simple, seamless, and transparent. All the deployment guidelines described in the previous section, Virtualized Commvault on Nutanix, still apply for Nutanix Objects. The only difference is that you must deploy the target storage resource as an Amazon S3 cloud storage library as shown in the following figure. Once you have added Nutanix Objects as part of Commvault's storage resources, you can use that store as a backup target.

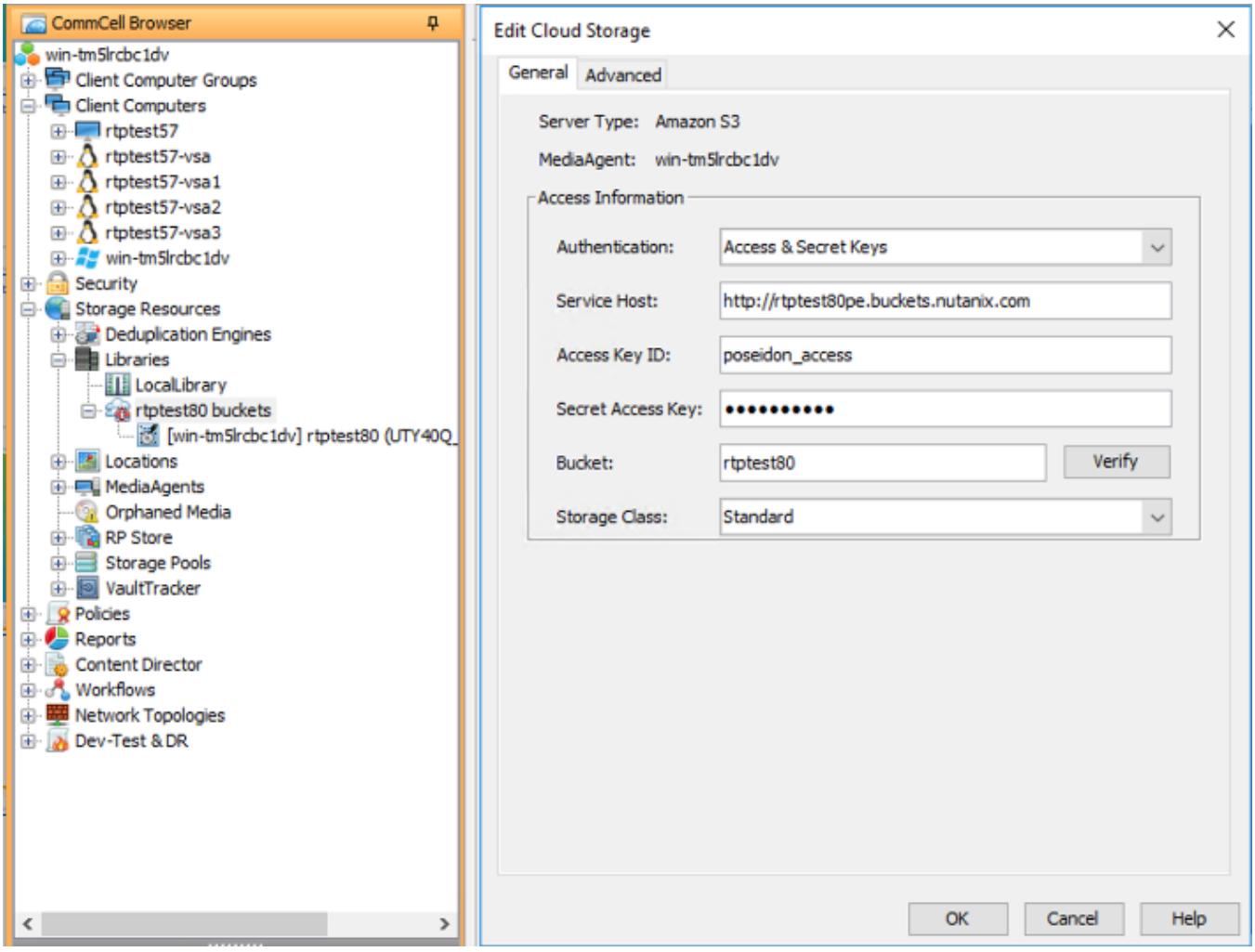

Figure 4: Virtualized Commvault Deployment Model with Nutanix Objects

4.6. Physical Commvault Server

As an alternative to deploying a virtualized Commvault solution, the following figure shows a possible topology for a physical Commvault configuration. In this example, we colocated all Commvault roles (CommServe, VSA, MediaAlert) on a single server. You can use this topology when you need to use tape backup, which requires a physical backup server. Refer to Commvault documentation for supported physical deployment models.

The physical server should meet the minimum Commvault sizing requirements, based on the number of VMs you're backing up and how many concurrent jobs you're running. Larger

environments may require multiple MediaAgent servers to meet backup window or storage capacity requirements.

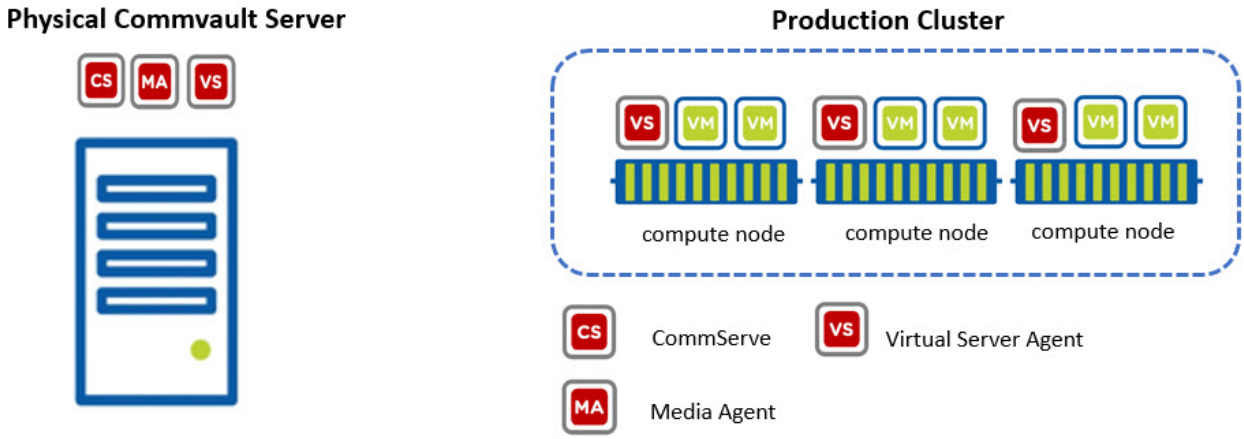

Figure 5: Physical Commvault Server Topology

4.7. Network

As recommended earlier, each Nutanix node should have the management interface configured to use 10 Gbps or faster NICs. This setting enables optimal backup performance, versus using the 1 Gbps NICs. The physical Commvault server should also have dual 10 Gbps or faster NICs and connect to the same layer 2 network as the management network.

4.7. Using AHV

When using Nutanix AHV, network uplinks are configured in active-backup mode by default, with a single active adapter. For active-active uplinks, refer to the AHV Networking best practices guide to configure load balancing on AHV.

4.7. Using vSphere

When using ESXi, Nutanix recommends using vSphere vNetwork Distributed Switches (VDS) and the network resource pool feature to prevent backup traffic from using most of the bandwidth available during a resource contention situation. Follow the recommended VDS configuration in the VMware vSphere Networking best practices guide.

If your Nutanix environment uses vSphere's standard vSwitch for traffic, you probably don't need to separate traffic with active-standby on 10 Gbps or faster NICs, but separation can be a valuable option in 1 Gbps environments.

If you see resource contention, we suggest:

- ESXi + CVM with vmnic0 active and vmnic1 standby.

- MediaAgent and vMotion with vmnic0 active and vmnic1 standby.
- All other VMs with vmnic0 + vmnic1 active-active.
- DRS rules to keep network-heavy VMs apart.

4.8. Performance Tuning

To optimize backup performance, follow the guidance in the CommCell Performance Tuning section in Commvault's documentation. We highlight some of the most important areas involved in using Commvault with Nutanix in the following subsections.

Virtual Server Agents

A Virtual Server Agent (VSA) can be installed on physical or virtual machines. In virtualized solutions such as a Nutanix cluster, VSAs are installed on Nutanix nodes. For best performance, install at least one VSA per Nutanix node to avoid serialization and create independent parallel backups. Because Nutanix provides a scalable and distributed architecture, it is better to distribute VSAs across the nodes for scalability than to place multiple VSAs on one node.
You can install multiple VSAs across Nutanix nodes from the Client Computers section of the CommCell Browser, as shown in the following figure.

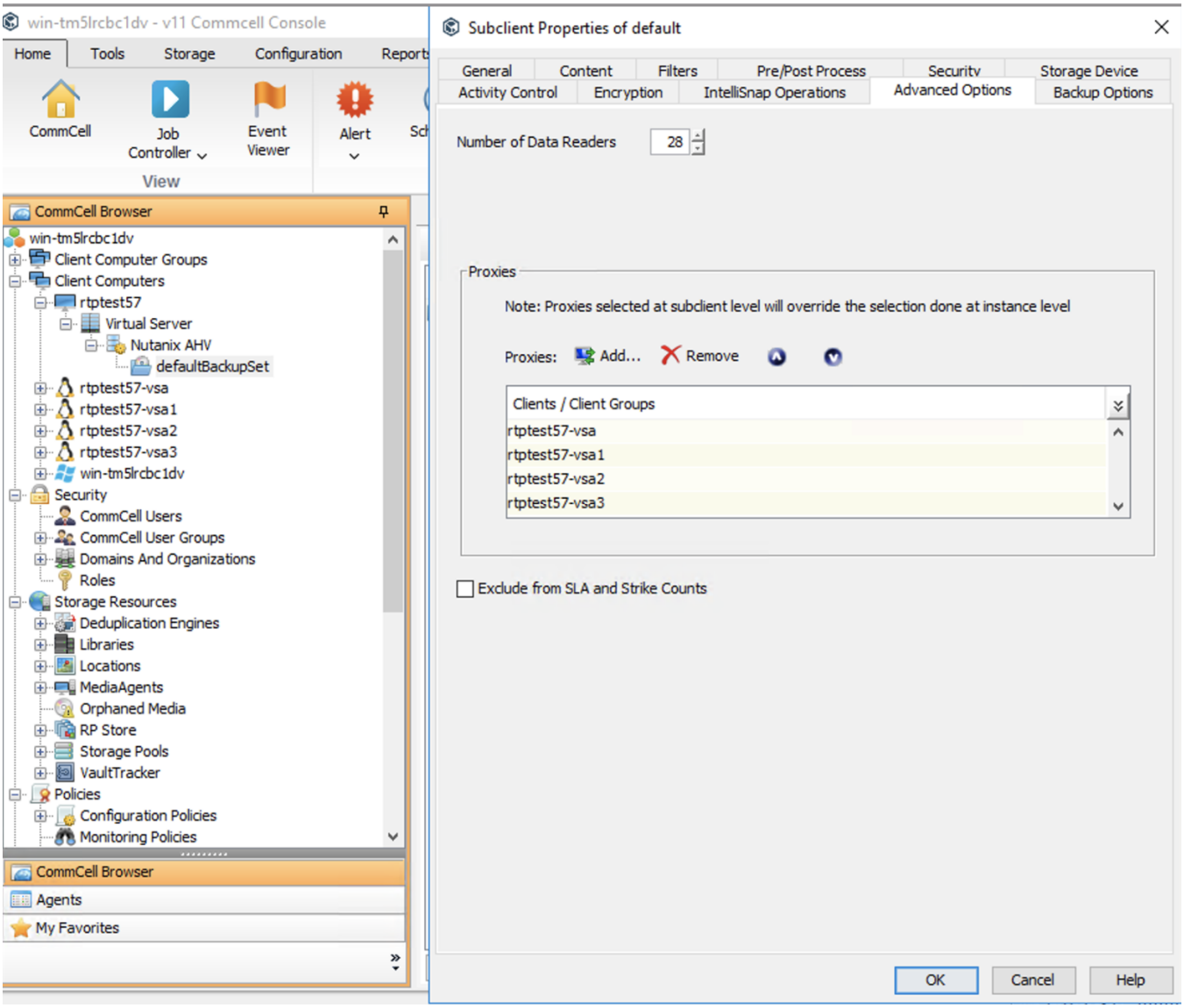

Figure 6: Multiple Virtual Server Agents

Data Readers

Data readers enable parallel read operations when data is backing up. Configuring enough data readers to match the number of disks on the cluster can improve the client's backup performance. For example, if you have one VM with seven disks on each node in a four-node Nutanix source cluster (with one VSA per node), you need 28 data readers to maximize parallel operations. Although it is not a requirement to have one data reader per disk, this allocation can start parallel backup operations across all the disks. If you can't reach the maximum number,

try to have enough data readers to avoid performance bottlenecks due to serialized operations. Configure data readers as part of the Client Computers backup set, as shown in the previous figure. You can also configure data readers as part of setting up VSAs, as shown in the Network Agents and Application Read Size section. Refer to Commvault documentation or contact Commvault Support for more information on data readers.

Network Agents and Application Read Size

To improve network bandwidth during backups, you can tune the number of network agents and the application read size as part of the VSA advanced subclient properties in CommCell. Configure multiple network agents (at least two or four, depending on the environment) to establish multiple data pipes. Similarly, increase the application read size to 4 MB. The following figure shows a sample configuration. For more information on application read size, refer to Commvault documentation.

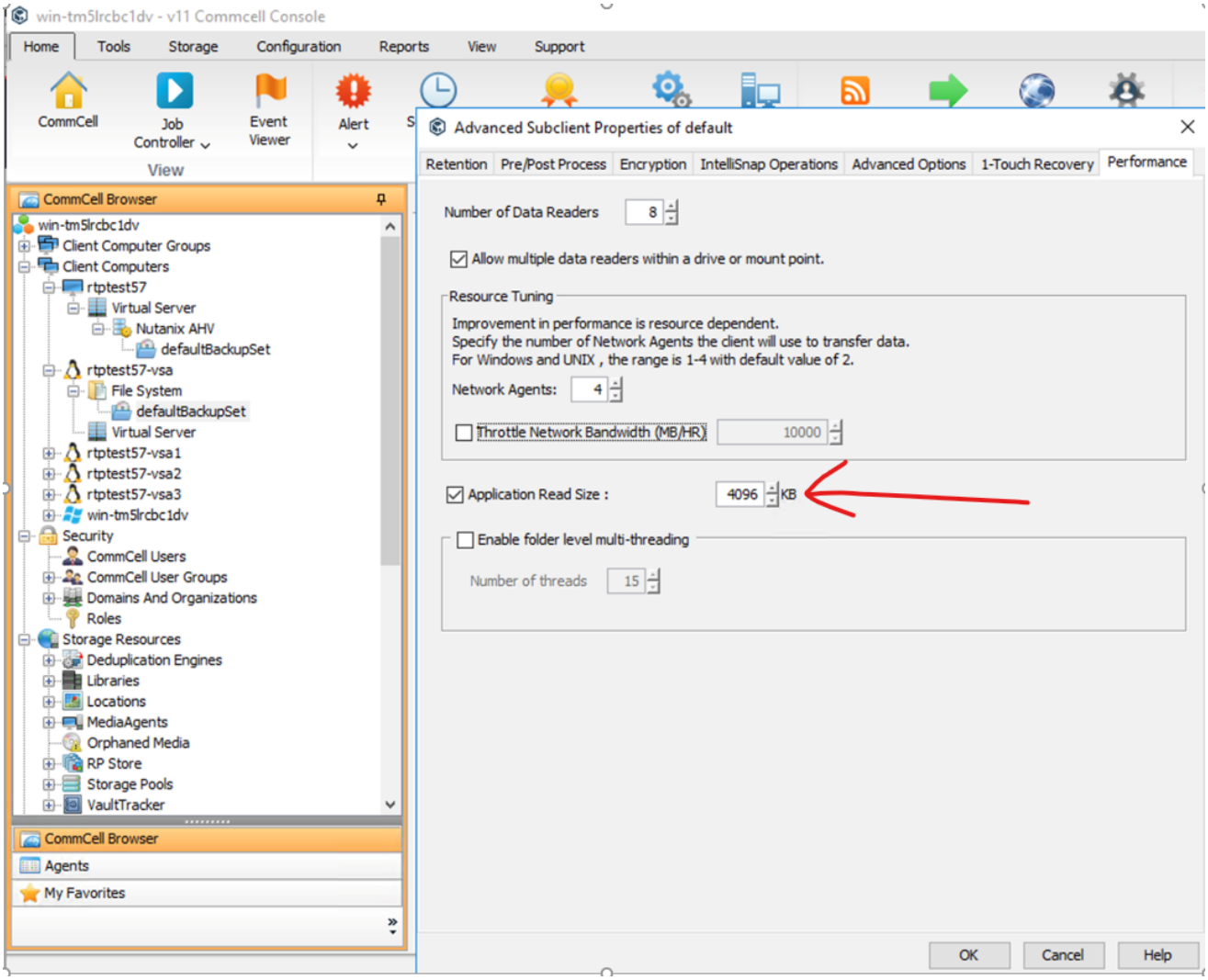

Figure 7: VSA Advanced Subclient Properties

Device Streams

Storage policy device streams are logical channels that enable client data to reach the backup target. Commvault recommends that you set the number of device streams equal to the number of drives or writers for all libraries defined in the storage policy. In other words, the number of device streams should equal the number of data readers.

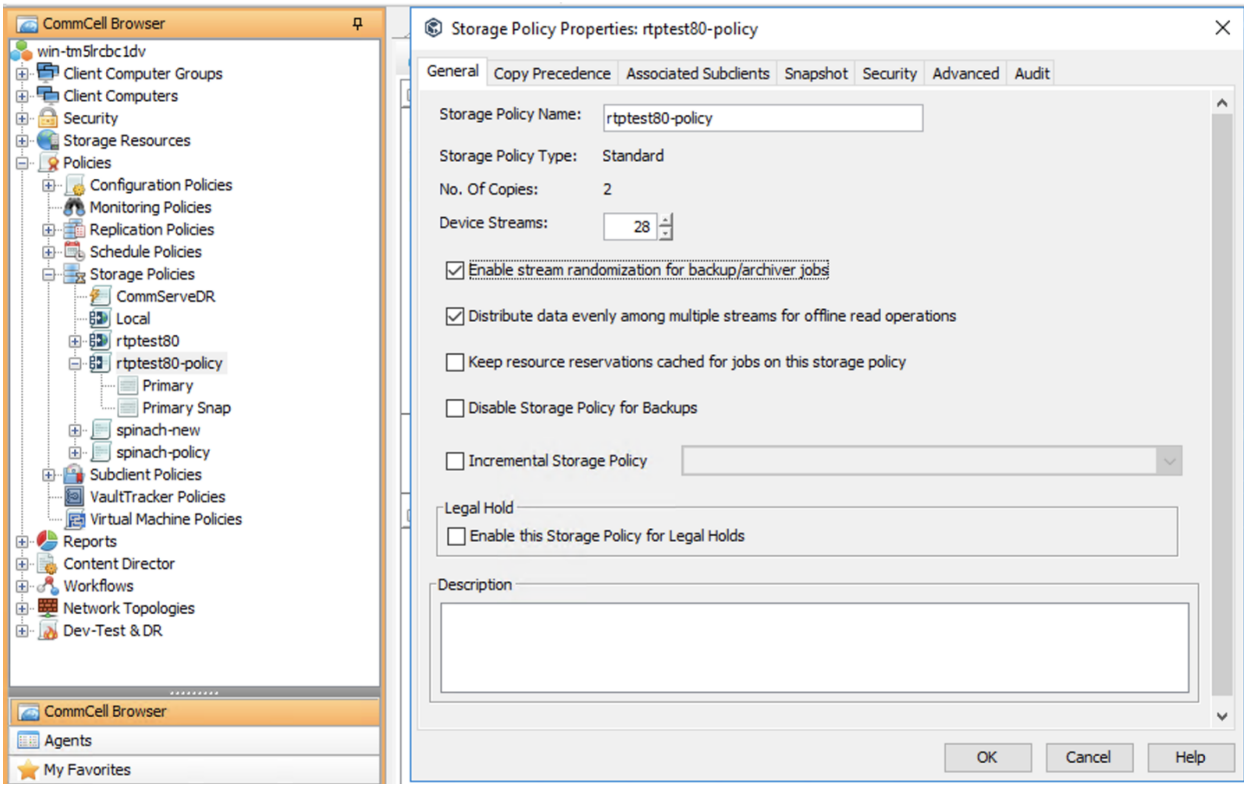

Figure 8: Device Streams in Storage Policy Properties

Chunk Size

A chunk is the unit of data that the Commvault MediaAgent uses when storing data. Before tuning this parameter, determine whether the chunk size is appropriate for the backup target storage media. Every storage media may require a different chunk size, depending on its underlying storage architecture. The following figure presents a sample configuration for tuning this setting. For more information about chunk size, review Commvault documentation. To configure appropriate chunk size for your environment or specific application, contact Commvault Support.

Note: This setting is a global configuration. If you have other storage configured with Commvault, changing the chunk size can interfere with deduplication and compression and may even incur data loss. Consult with your other storage providers before changing the chunk size.

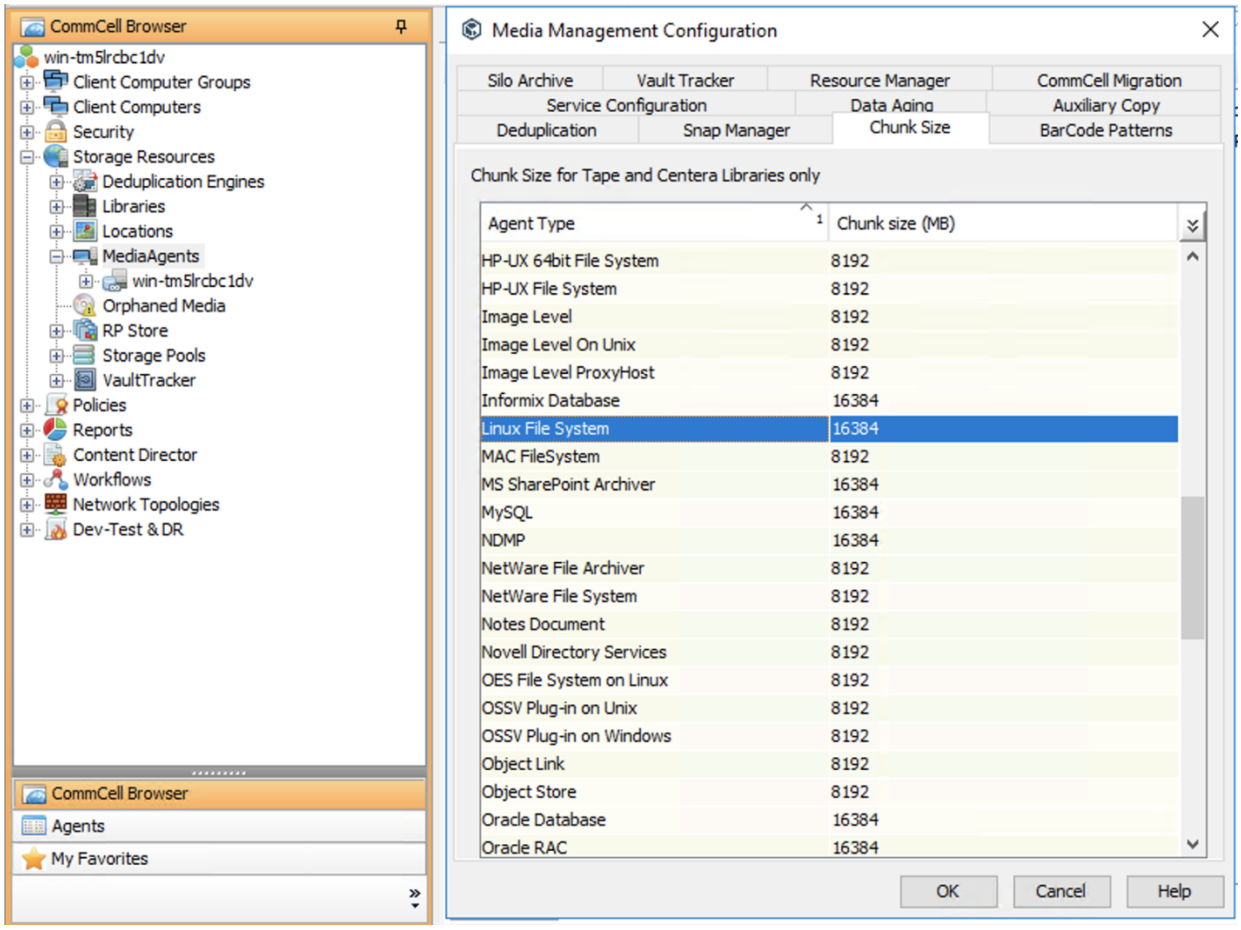

Figure 9: Chunk Size in Media Management Configuration

Commvault Client Compression and Deduplication

Compression and deduplication can deliver significant storage savings. When using Commvault with Nutanix, you can enable compression and deduplication at multiple points in the solution:

- VSA (client)
- MediaAgent
- Backup target

Decisions regarding where to enable compression or deduplication depend on the individual deployment.

When the client computers and MediaAgent are in separate locations or use a virtualized setup that requires data to go through a WAN, enable both data reduction features on the client side during client backup set configuration, as shown in the following figure. This configuration

provides significant network usage savings, because the data has already been compressed and deduplicated before it crosses the network.

If the source and target backup set are on a high-speed LAN and if network usage is not an issue, Nutanix recommends enabling these data reduction features on the backup target storage. This option reduces resource requirements for the VSAs and the MediaAgents. The backup target storage device processes the data to achieve the possible space savings, then archives it. Both Nutanix virtualized storage and Objects support storage compression and deduplication savings. You can enable Nutanix data reduction features on a per-container basis.

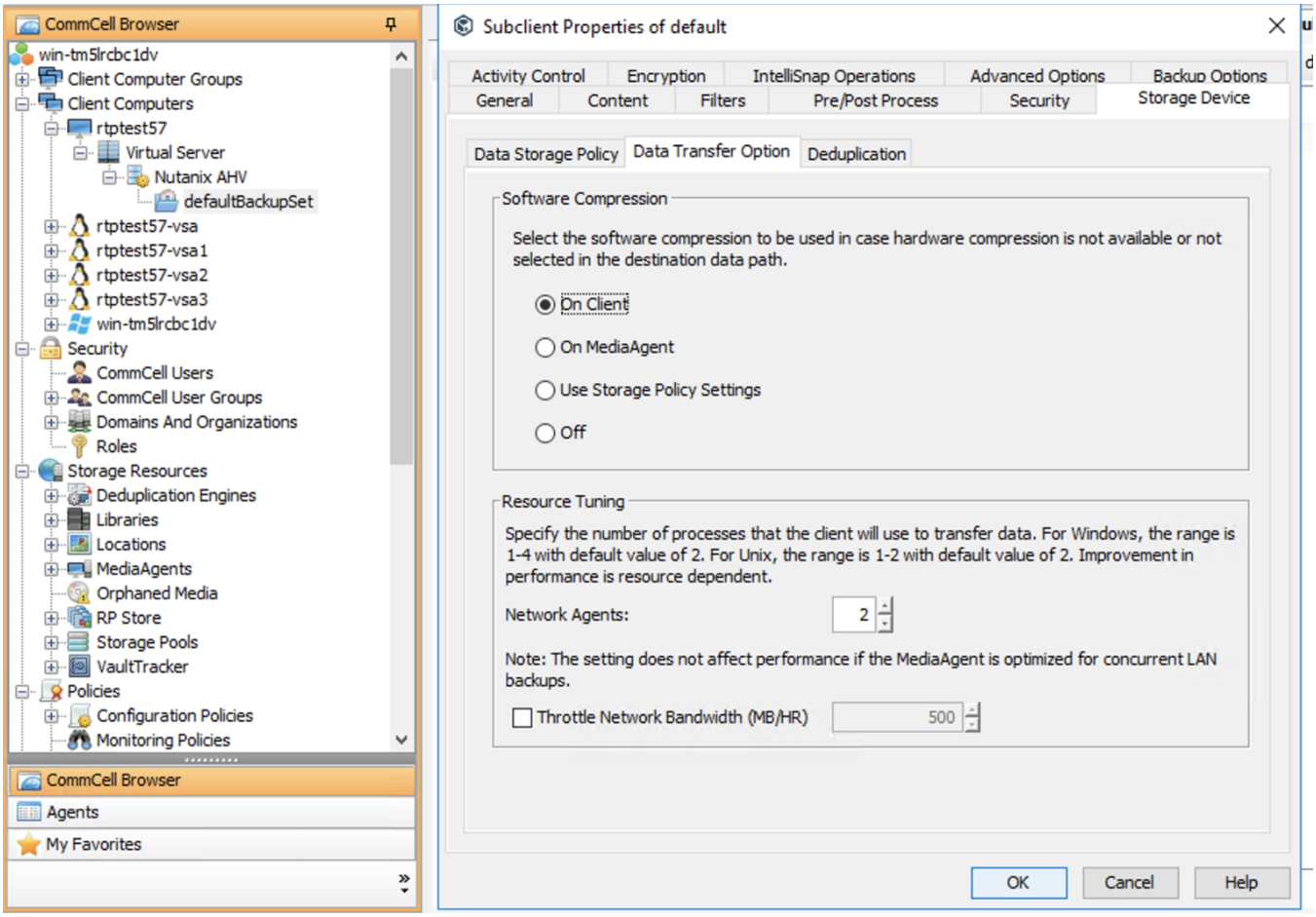

Figure 10: Enabling Software Compression on Client

4.9. Backup Method

This section covers the two backup methods available when using Commvault and Nutanix.

Streaming

Streaming allows you to create point-in-time application-consistent snapshots of VMs using CBT. When you use streaming, AOS is not part of the backup; streaming leverages the Nutanix AHV or VMware ESXi hypervisor. Each node must have a VSA proxy installed and configured for streaming backups.

Note: With VMware ESXi, Nutanix recommends using NBD mode for backups, as hot-add or NAS streaming mode may cause performance issues.

IntelliSnap

IntelliSnap allows you to create a point-in-time, application-consistent snapshot of backup data on the Nutanix distributed storage fabric. The backup administrator doesn't need to log on to Prism to provide this functionality. This approach allows near-instantaneous snapshot mounts for data access.

IntelliSnap offers significant advantages for protecting critical VMs:

- Point-in-time snapshots are taken in a fraction of the time needed for traditional streaming backups.
- Because backups using snapshots require applications to be quiesced for a very short period of time, the time needed to reconcile the production VM with transactions that occur during the backup is also minimized.
- The system can take snapshots as often as necessary, providing multiple daily recovery points for high-transaction VMs.
- You can recover critical VMs and restore them to service quickly.
- You can restore full VMs or files and folders from snapshots or backup copies.
- You can back up snapshots to disk through a proxy (backup copy), limiting the impact of backups on production VM resources.
- Based on policies, the system automatically catalogues and indexes snapshots for restores and backup copies.
- For incremental backups, the system only writes changes to the backup media.

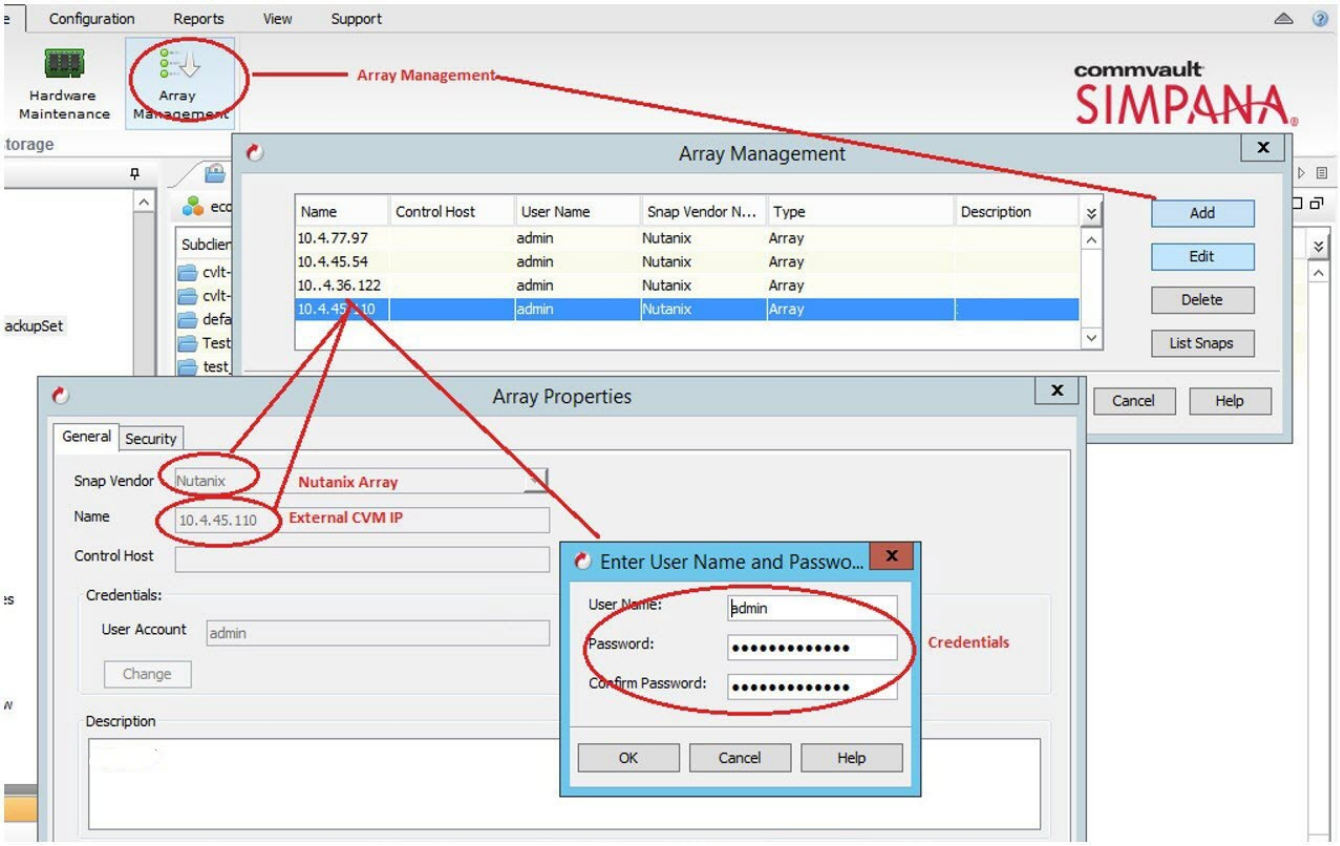

Figure 11: Setting Up IntelliSnap with an External CVM Address

Transport Modes

Commvault support two transport modes for Nutanix AHV:

- Hot-add transport mode (default).
- Network-attached storage (NAS) transport mode.

For more information on these Commvault transport modes for Nutanix AHV, refer to Commvault documentation.

For VMware with Nutanix, we recommend using NBD only if you can't use IntelliSnap. For more information on NBD scenarios, refer to Commvault documentation.

Additional information:

- IntelliSnap-powered asynchronous backup for Nutanix with VMware (VDDK) and Commvault
- IntelliSnap-powered synchronous backup for Nutanix with VMware (VDDK) and Commvault
- Commvault DASH

4.10. Backup Types and Schedules

IntelliSnap Plus Backup Copy

You can use IntelliSnap snapshots to back up and protect large, critical, and high-transaction VMs. Snapshots support application-consistent backups for applications such as Oracle, SQL Server, SharePoint, and Exchange. Hardware snapshots provide multiple persistent recovery points per day for critical VMs, enabling full VM recovery as well as granular file and folder-level recovery, while minimizing the load on production VMs and infrastructure.

You can configure multiple readers on the Commvault job to quiesce multiple VMs simultaneously and create or delete software snapshots faster, reducing the overall IntelliSnap job time. This configuration minimizes the redo log time for large VMs, protecting larger datastores and VMs.

Benefits

- Low impact on production systems.
- Multiple recovery points per day.
- Fast recovery copy.
- Reduced backup workload due to using a proxy server to create the daily backup copy.

Considerations

- Consult Commvault documentation about enabling synthetic full backups (described in the next section) with IntelliSnap if needed.
- When using ESXi, you must specify an ESXi proxy to mount a hardware snapshot for backup copy operations. An ESXi proxy can use a snapshot as the source for secondary VADP backups, allowing you to copy data from a snapshot to alternative storage, such as local storage, SAN, NAS, tape, or cloud targets, for longer-term retention. This method allows you to offload the backup operation to a storage snapshot rather than to the live production system.
- Snapshot reserve requires additional storage.
- IntelliSnap may impact other production systems using the same storage. You can manage this impact by scheduling the backup copy outside peak hours.
- IntelliSnap snapshots the entire container where the protected VMs reside.
- When using IntelliSnap snapshots for DR, you need to use the Nutanix command line interface (nCLI) on the remote site to restore snapshots in case of disaster.

- If using Metro Availability or synchronous replication and Commvault together, do not use IntelliSnap.
- Do not take more than one snapshot per container every hour.
- If the VMs restored for the backup copy job are thick-provisioned, they consume that provisioned space for the duration of the backup window.
- Keep IntelliSnap VMs on their own separate container.
- Create separate backup jobs (subclients) for different classes of VMs, where the VMs in each class have the same protection requirements and backup methods. Specifically, create separate subclients for:
  - # Regular streaming backups.
  - # IntelliSnap backups with backup copy.
- Avoid having multiple subclients that address the same datastore, so that backups for different subclients do not have to take multiple hardware snapshots of the same datastore during IntelliSnap backups.
- Use the latest service pack from Commvault.

We recommend taking a full copy every week, if you can meet your backup window; this recommendation depends on the size of the environment. If you have trouble meeting your backup window, you can create separate schedules to spread out the full copy.

> **Note:** With ESXi, when you add ESX hosts to vCenter, make sure that the format of the ESX host name matches the host name format in vCenter.

For example:

- If the host name format is short name, use short name to add the host to vCenter.
- If the host name format is FQDN, use FQDN to add the host to vCenter.
- If the host name is an IP address, use the same IP address to add the host to vCenter.

Synthetic Full Backups

Synthetic full backups consolidate the data from the latest full or synthetic full backup with any subsequent incremental backups to collapse the backup cycle. This approach allows you to run an incremental forever strategy (more on this strategy below), which consolidates incremental backups to create a new full backup. Because synthetic full backups do not back up data from the source machine, this operation imposes no load on the production system.

When using Commvault deduplication, you can create synthetic full backups in an accelerated mode to significantly reduce the copy duration. This accelerated mode, called a DASH full backup, reads only backup metadata and manages the signature references and index data

in the backup storage. For more information about synthetic full backups, refer to Commvault documentation.

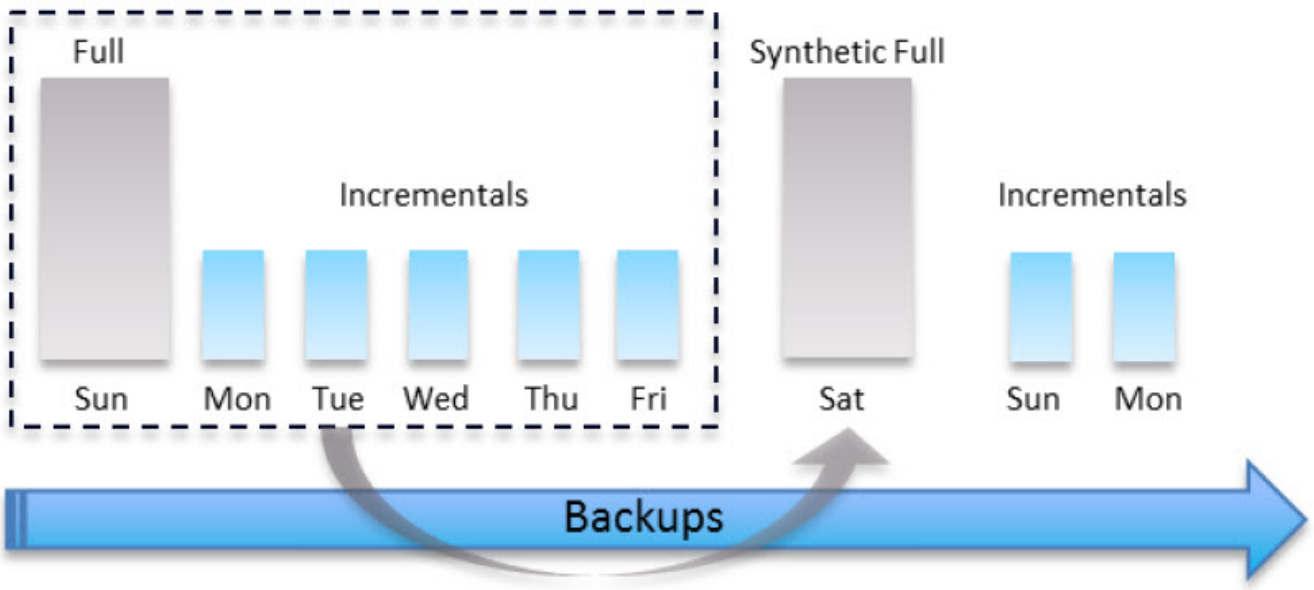

Figure 12: DASH Full Backups

Incremental Forever Approach

For most virtual protection jobs on Commvault with Nutanix, we recommend using an incremental forever approach, where DASH full backups are scheduled periodically, for low-transaction workloads. In incremental backups, CBT helps quickly identify the data blocks on the VM that have changed since the last backup. When combining CBT with Commvault deduplication and compression, the amount of data and load on the virtual machines during incremental backups is minimal, resulting in the fastest and most efficient backup.

IntelliSnap with Replication

Although you cannot use Metro Availability with IntelliSnap, you can still use Nutanix asynchronous replication with the protection domains that Commvault automatically creates. In this scenario, all the IntelliSnap best practices still apply, along with these two additional tips:

- Limit the VMs on any one container to 50 (or 3,200 files), because the process replicates the entire container.
- Offset the replication from the Commvault backup schedule by at least one hour.

To replicate the production domain created by IntelliSnap:

- Set up either another physical cluster or the cloud as your remote site.

- Use Prism to set a schedule. The production domain name adds a random number as a suffix for the name of the container where your VMs reside. For example, if your VMs are on a container called **servers**, the protection domain could be named **servers_1490719768532**.

Restoring the protection domain restores the entire container. You must use the nCLI to restore the container on the remote site. To recover your VMs on the remote side:

- Log on to the nCLI on your remote cluster.
- Find the snapshot you want to restore. The protection domain name includes the name of the container where your VMs reside. Use this command to obtain the snap-id:

```
ncli> pd list-snapshots name=servers_1490719768532
```

- Use the snap-id to restore the snapshot:

```
ncli> pd restore-snapshot snap-id=main:18242901 name=servers_1490719768532 prefix=/
restorevstore
```

- In the command above, we use the prefix in case the container is already active. If the container is not active, you can remove the prefix from the command. The command above adds files from the snapshot to your container, so be sure to go back and remove any unneeded files or VMs when running the restoration against an active container.
- Once you have restored the files, you can move the appropriate datastore onto the path where the primary configuration file for the VM resides (<name_of_VM>.vmx). Right-click on the file to add it to the inventory.

5. Best Practices Checklist

- Use a Nutanix cluster external Data Services IP address when using IntelliSnap.
- Install a VSA on every Nutanix compute node.
- Install the MediaAgent software on all the VSA proxies.
- Install CommServe and MediaAgent on a secondary Nutanix cluster to separate backup and production infrastructure to protect against failure.
- Follow Commvault's sizing guidelines.
- Create a virtual server client proxy group for easier management.
- When using IntelliSnap, colocate the MediaAgent software with the VSA.
- With ESXi, when you add ESX hosts to vCenter, make sure that the format of the ESX host name matches the host name format in vCenter. For example:
  - If the host name format is short name, use short name to add the host to vCenter.
  - If the host name format is FQDN, use FQDN to add the host to vCenter.
  - If the host name is an IP address, use the same IP address to add the host to vCenter.
- With ESXi, use NBD as the transport mode whenever possible.
- With ESXi, configure the management network interfaces to use the 10 Gbps or faster NICs if available.
- With ESXi, follow current Nutanix vSphere networking recommendations.
- Ensure sufficient SSD space is available for the whole deduplication database when running MediaAgents as VMs for storage.
- Set up a seal schedule for the deduplication database by following Commvault's documented process.
- If you're using a Nutanix cluster as target storage, place MediaAgents and disk libraries on a separate secondary cluster.
- Use DASH full backups and the incremental forever approach for low-transaction VMs.
- Use IntelliSnap for high-transaction, high-SLA VMs.
- Don't take more than one snapshot per container every hour.
- Thin-provision IntelliSnap VMs so they don't consume additional space on restore.
- Keep IntelliSnap VMs on their own separate container.

- Limit VMs to 50 (or 3,200 files) on each IntelliSnap-protected container.
- Follow the protection domain limits as documented in Data Protection and Recovery with Prism Element.
- Make sure to apply the latest service packs and hotfixes from Commvault before deployment.
- When using Nutanix replication with IntelliSnap, offset the replication by at least one hour from the Commvault backup schedule.

5.1. Application Backup Recommendations

- In the following list, we provide links to Commvault's guidance for widely used database applications. A backup agent must be installed in the VM running the application. For application-specific best practice recommendations, consult the relevant official documentation.
- MS SQL Server
- MySQL
- Oracle
- PostgreSQL

5.2. Cross-Hypervisor Restore

- To restore VMs from a different hypervisor or cloud provider to AHV using Commvault, refer to Commvault's conversion guide.

6. Conclusion

Nutanix and Commvault provide granular data protection to meet the required recovery point objectives across a range of deployment models. As your application requirements change and your cluster grows, you can scale simply and quickly, with one-click node addition and no downtime. The Nutanix and Commvault solution offers the reliability and flexibility necessary to fulfill your enterprise's backup and recovery needs. The best practices we offer in this document ensure that you safeguard your applications with minimal impact on your production workloads.

Appendix

References

1. Commvault Product Documentation
2. Commvault Nutanix AHV Documentation
3. Commvault with Nutanix and VMware Documentation
4. Commvault Performance Tuning Documentation
5. Hardware Specifications for the CommServe Server
6. Hardware Specifications for Virtual Server Agent
7. Hardware Specifications for MediaAgent
8. VMware vSphere Networking on Nutanix
9. VMware vSphere Storage APIs – Data Protection
10. Nutanix AHV Networking

About Nutanix

Nutanix makes infrastructure invisible, elevating IT to focus on the applications and services that power their business. The Nutanix enterprise cloud software 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.

About Commvault

Commvault's data protection and information management solutions provide mid- and enterprise-level organizations worldwide with a significantly better way to get value from their data. All of the applications in Commvault's end-to-end data protection and information management solutions offer flexible deployment options and are built from the ground up, on the same platform. As a result, they talk to each other, work with each other, and look like each other. Commvault can help companies protect, access, and use all of their data, anywhere and anytime, turning data into a powerful strategic asset. Get control with secure enterprise file sharing and anytime, anywhere data access at www.commvault.com.

List of Figures

List of Tables