BEST PRACTICES GUIDE

Nimble Storage Best Practices for CommVault Simpana*

Efficient Nimble Storage snapshots managed by CommVault Simpana IntelliSnap - Enables aggressive data protection for critical applications

*For Nimble Storage OS 2.1 or higher with CommVault Simpana 10 SP7 or higher

Table of Contents

Introduction

Nimble Storage snapshots are based on highly efficient *redirect-on-write* technology and take advantage of universal compression, ensuring that snapshots consume minimal storage space. The ability to take and store months of frequent application consistent snapshots drastically reduces the overhead incurred with traditional backup data movement as data is no longer read from storage by an application server, transported over a network to a backup server, and subsequently written to backup storage. The net result is faster backup, recovery, and disaster recovery preparedness at a reduced total cost of ownership when compared to legacy solutions.

Nimble OS version 1.2 and CommVault Simpana 9.0 R2 SP6 introduced integrated support for Nimble Storage snapshots with IntelliSnap. Nimble Storage OS versions 2.1 and higher with Simpana 10 SP7A and higher enhances integration, enabling users to fully leverage advanced application awareness and automation available in the combined solution. CommVault triggers Nimble Storage snapshots under direct control of Simpana schedule policies. Replication to a downstream Nimble Storage partner array can be automated within a Nimble volume collection schedule such that it occurs at the completion of a successful IntelliSnap backup. Downstream replica snapshots can be restored manually, or can be cloned into volumes and used to perform disaster recovery testing without impacting production workload. "Backup Copy" functionality, the policy based ability to copy IntelliSnap created snapshots from a local Nimble Storage array to external storage media, is also performed under the direct control of Simpana.

The integrated solution provides significant benefits that deliver tangible business value:

- Use Simpana schedule policies to automatically protect supported applications with IntelliSnap and the Nimble Storage snap engine.
- IntelliSnap created Nimble Storage snapshots on the local Nimble Storage array are indexed and cataloged by Simpana enabling search and browse for rapid, targeted recovery.
- Intellisnap created Nimble Storage snapshots can be replicated to a downstream Nimble array under the control of Nimble volume collection schedules. These can then be used to either manually recover or clone snapshot volumes.
- Selectively copy IntelliSnap created Nimble Storage snapshots from a local Nimble Storage array to external media such as tape with Simpana backup copy jobs.
- Browse and recover from IntelliSnap created Nimble Storage snapshots on the local Nimble Storage array via the familiar Simpana user interface.
- Monitor and track backup, restore, and copy job progress using the Simpana Comcell console job controller.
- Use Simpana to generate comprehensive reports.

Target Audience

Simpana administrators, storage architects, and Nimble Storage administrators are encouraged to read this document. The recommendations set out to assist in deploying a supported, successful, and reliable solution.

Strategy & Objectives

The goals of a data protection solution should be focused on data recovery requirements. Service levels for data recovery may include a variety of factors:

- **RPO (Recovery Point Objective):** Generally accepted as the amount of data that can be lost when the most recent backup is recovered.
- **RTO (Recovery Time Objective):** Generally accepted as the amount of time between the instant where an outage occurs to the point where production workload is resumed. Business critical data is likely to have a short recovery time objective, whereas less critical data may have a longer recovery time objective.
- **DR (Disaster Recovery):** A number of scenarios that may include the ability to recover data at a remote location.

It is the responsibility of the user to understand the RPO, RTO, and DR requirements for a given deployment. Subsequent content in this document serves to assist in achieving those objectives.

Recovery Points & Recovery Time

Simpana IntelliSnap backups of a Nimble Storage volume collection represent points in time to which the volume collection can be recovered. The frequency at which IntelliSnap subclient backups are executed will define the maximum duration between backups. The maximum elapsed time between backups is in effect the maximum recovery point for the subclient. Planning the frequency of IntelliSnap backups so that they align with the recovery point objectives of a given subclient is recommended.

Nimble Storage Snapshots

Simpana IntelliSnap subclient backups utilize the Nimble Storage snap engine to create snapshots local to the Nimble Storage array on which the target volume collection resides. Nimble Storage snapshots can be used to effectively reduce recovery point objectives, reduce the storage load that occurs with traditional disk or tape backups, while also reducing the recovery time objective.

Traditional Backup to Disk/Tape

RPO = 1 Hour

RTO = 24 Hours

System/Storage Impact = Heavy

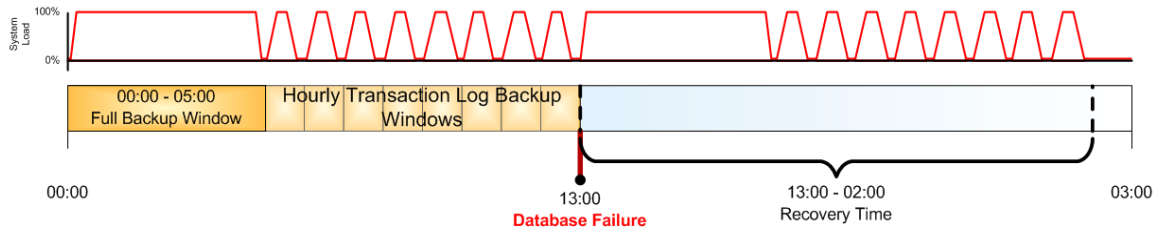

Figure 1 – Traditional Backup and Recovery

Depicted in figure 1 is a traditional MS SQL Server backup strategy. A long full backup window followed by regular transaction log backups impacts both the storage subsystem and database server by placing a load on them while backups are being performed. Recovery time can be substantial as both the most recent full backup and subsequent transaction log backups need to be recovered from traditional backup media, disk or tape.

Nimble Storage Snapshot Backup

RPO = 15 Minutes

RTO = 1 Minute

System/Storage Impact = Minimal

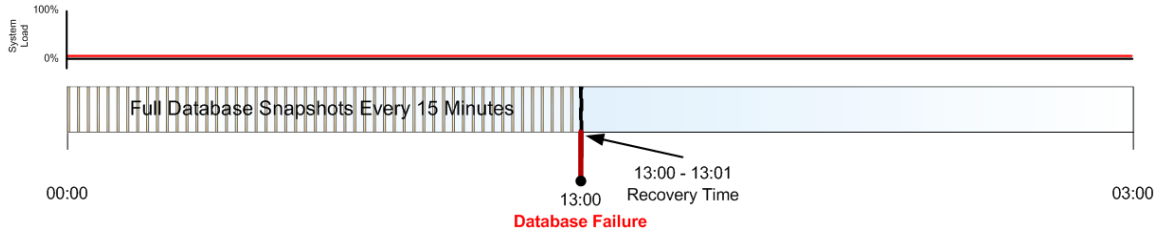

Figure 2 – Nimble Storage Snapshots and Recovery

Depicted in figure 2 are Nimble Storage snapshots managed by CommVault Simpana IntelliSnap taken at 15 minute intervals. Impact to the Nimble Storage array and database server is minimal. Recovery time is drastically reduced, and the entire process is managed using the familiar Simpana user interface.

Terminology

A brief introduction to terminology that may be new or unfamiliar is covered in this section.

- **Simpana Array Management:** The storage array management interface within Simpana that facilitates adding a Nimble Storage array to the configuration. A collection of configuration parameters including the array name, control host, and user credentials as well as a description are entered to allow Simpana to control Nimble Storage snapshots with IntelliSnap.

- **Nimble Storage Volume Collection:** A group of related volumes that share data protection characteristics such as snapshot and replication schedules. An example volume collection might consist of one Nimble Storage volume used for a Microsoft Exchange database and another volume used for the Exchange logs that must be snapshotted simultaneously to ensure data integrity. Backup scheduling is configured within the volume collection such that it is triggered by CommVault Simpana. Optionally, a replication partner can also be configured enabling the volume collection schedule to replicate snapshots to a downstream Nimble array.
- **Nimble Storage Protection Template:** A set of user defined schedules and retention limits that can be selected for use when creating a volume collection or a standalone volume. An example protection template might be created for use with Simpana, enabling CommVault to trigger backup jobs. In this use case Simpana also manages retention and automates data aging. Additionally, a replication partner can be specified in the template.
- **Nimble Storage Replication Partner:** A pair of Nimble Storage arrays that communicate with each other over a network to enable the recovery of volumes in the unlikely event of a failure. Replication partners are configured to replicate snapshots. Volume collections are easily configured to enable automated replication.
- **Nimble Storage Initiator Group:** A method to limit volume access to only specific initiators is to use an initiator group. Depending on how Simpana is configured, it may be practical to add the initiator of a proxy for backup copy jobs to an existing initiator group.
- **Nimble Storage Performance Policy:** A collection of performance parameters associated with one or more Nimble Storage volumes. Standard policies are available for most data types (Oracle, MS SQL, VMware, etc.) Custom performance policies can also be created for special use cases. For example, the case where a Nimble Storage volume is being configured for use as a Simpana disk library.
- **Nimble Connection Manager (NCM):** Part of the integration between Nimble Storage arrays and Windows or VMware deployments is handled by NCM. NCM manages connections between Windows or ESXi hosts and Nimble Storage arrays. NCM is usually deployed by the storage administrative team and is mentioned for awareness only.
- **Nimble Windows Toolkit (NWT):** Provided in a single installation package, NWT includes a number of valuable tools enabling setup management, connection management, and connection services for a Windows environment. NWT should be installed on Simpana Windows Media Agents configured as proxy hosts that perform indexing and backup copy jobs.
- **Nimble Storage InfoSight:** The Nimble Storage InfoSight portal provides comprehensive information about Nimble Storage arrays, and also serves as an access point for Nimble Storage code and documentation downloads.

Recommendations

In all cases the appropriate compatibility matrices should be referenced before architecting a solution. Validate that supported versions of Nimble Storage Operating System, and CommVault Simpana are being used. Also check all related applications to be sure they are supported with the version of Simpana being used.

- Nimble Storage compatibility matrices are located on the InfoSight portal. After logging into the portal click "Downloads" and then select the appropriate Nimble OS version. In the list of available documents select the item named, "Support Matrix". The "Backup Software Coexistence" section of the document contains information about Simpana and Simpana service pack versions that may be required. Also select the item named, "Release Notes". The release notes document may contain additional information specific to Simpana.

  https://infosight.nimblestorage.com/

- CommVault Simpana documentation is located at:

  http://documentation.CommVault.com/CommVault/v10/article

Naming Conventions

What begins as a proof of concept or series of simple tests may turn into a production deployment. Renaming components of a deployed solution may introduce extra work, complexity, and calls to technical support.

When possible, use nomenclature that has already been standardized within the environment. Array and volume names are typically defined prior to data protection solution deployment. Nimble Storage entities that may require creation and naming are volume collections and protection templates. These items should be named such that they conform to existing conventions while being descriptive with regard to purpose and function. Similarly, Simpana entities such as storage policy copies and disk libraries added as part of a Nimble Storage deployment should also be named such that they conform to existing standards while being descriptive with regard to purpose and function.

Snapshots, Frequency, & Retention

- **The shortest recommended duration between Simpana IntelliSnap snapshots on a single subclient is 15 minutes:** Although Nimble Storage arrays are capable of taking snapshots repetitively at intervals as short as one minute, the recommended minimum interval or frequency is fifteen minutes. The reasoning behind this recommendation is tied to application synchronization, where for instance the Microsoft VSS framework surrounding the Nimble Storage array takes time to freeze and resume input/output, and also the time it takes Simpana to catalog and index backup activity.

- **Simultaneous IntelliSnap backups on many subclients should be avoided:** Instead of scheduling a large number of subclients to initiate backups simultaneously, consider staggering the start time of each subclient by a few minutes when possible. Consider different backup schedules for a collection of ten clients that initiate backups at one through ten minutes after the hour, for example.
- **Co-locating multiple databases on the same Nimble Storage volume collection:** Multiple databases residing on the same Nimble Storage volume collection should have the same retention requirements and be protected by the same Simpana subclient. IntelliSnap snapshots occur at the volume level, and are also aged such that the entire snapshot is deleted at expiration time.
- **Retention planning considerations:** Consider the service level agreement (SLA) for data set recovery and implement a Simpana retention strategy that aligns with it. Correlate SLA requirements into retention requirements for hourly, daily, weekly, monthly, and quarterly backups (for example). Plan to deploy backup copy jobs for datasets with long term retention needs that may be impractical to retain as snapshots, such as those with a 7 year retention requirement. Note that backup copy jobs can be executed using IntelliSnap created snapshots on a local Nimble Storage array.
- **Snapshot Replication:** Nimble Storage snapshots managed by Simpana IntelliSnap backups can be replicated to a second Nimble Storage array. The prerequisites for snapshot replication include the use of a volume collection, configuring a replication partner, and the use of a protection template that specifies the replication destination. Snapshots are replicated under the control of Nimble's volume collection schedules.

Configuration & Deployment

Simpana Array Management

Configure the Nimble Storage array within Simpana using the Array Management tool. Enter the Nimble Storage management IP address for the array name and control host parameters. Be sure to select Nimble Storage as the snap vendor. The description parameter is a user defined label, and typically contains the hostname of the Nimble Storage array. If not already known, the user name and password parameters should be obtained from the storage administration team. The user specified must have a role level of "Power User" or "Administrator" assigned on the Nimble array. The Nimble Storage user name and password are required when configuring the array for integration with Simpana.

Figure 3 – Simpana Array Management

Depicted in figure 3 is the Simpana Array Management tool. A single Nimble Storage array has been added to the configuration.

Nimble Storage Volume Collections

A volume collection should consist of related Nimble Storage volumes such as a Microsoft SQL database and log volume. These volumes share common backup and replication data protection characteristics. Limit the number of volumes associated within a volume collection to only related volumes. For example, related volumes are database and log volumes for a single database server. Single volumes such as a NTFS volume, should be protected separately as a standalone volume.

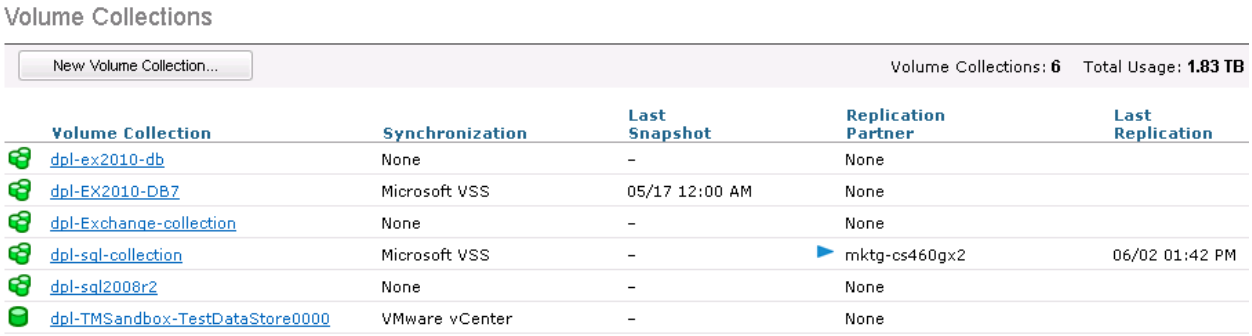

Figure 4 – Nimble Storage Volume Collections

Within a volume collection, application synchronization should be disabled as application consistency in conjunction with Nimble Storage snapshots is orchestrated by Simpana.

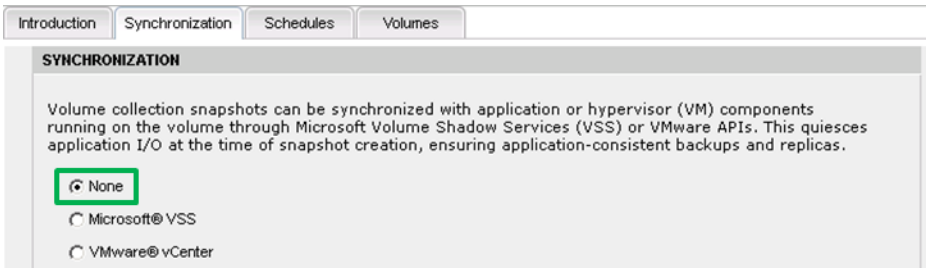

Figure 5 – Volume Collection Synchronization

The volume collection schedule section includes an advanced feature set specific to integration with Simpana. Selecting the advanced menu item, “Snapshot triggered by CommVault”, enables Simpana to

control the scheduling of IntelliSnap backups associated with the volume collection. Additionally, when a replication partner is selected, snapshots will also be automatically replicated.

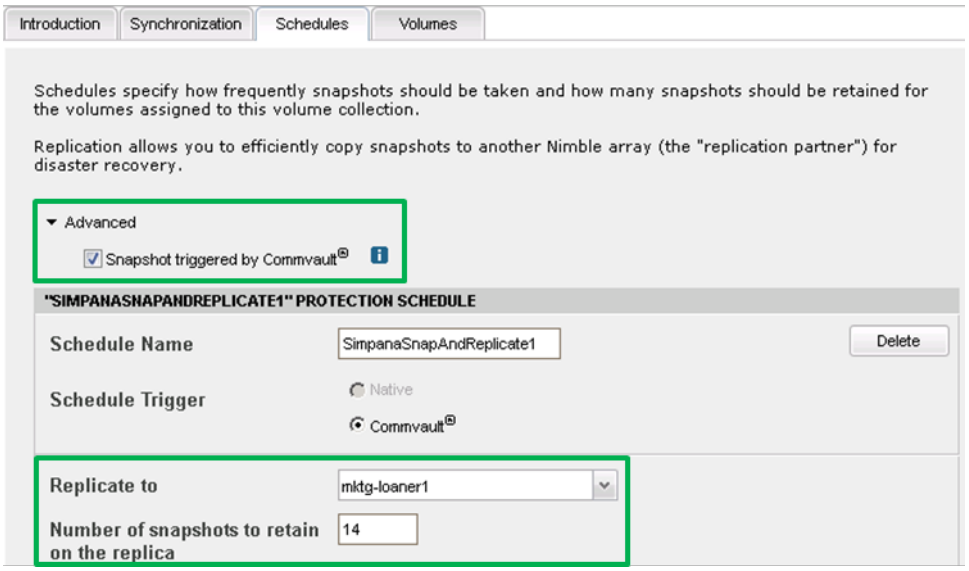

Figure 6 – Volume Collection Schedule

Depicted in figure 6 is the volume collection "Schedules" tab. When selected, the advanced menu item "Snapshot triggered by CommVault" enables Simpana to control the scheduling of IntelliSnap backups associated with the volume collection. Additionally, when a replication partner is selected, snapshots will be automatically replicated.

It is important to understand that while snapshot retention on the local Nimble Storage array is controlled by Simpana, replicated snapshot retention is controlled based on the value entered into the "Number of snapshots to retain on the replica" field. Replicated snapshots that exceed this value cause the oldest replica snapshot to be deleted.

Equally important to understand is that manually created snapshots, snapshots not created by Simpana, can potentially create issues if they are not understood. The first issue is that without Simpana, a manually invoked snapshot has no application synchronization. The synchronization properties of the volume collection have been purposefully configured to a use a value equal to "none" because the intended use case is in conjunction with Simpana. The second potential issue is that manually invoked snapshots that are replicated may displace application consistent snapshots created by Simpana.

Protection Templates

Protection templates can be used to simplify the creation of volume collections with standard configuration parameters. Volume collection synchronization and schedule parameters can be entered once into a protection template and saved for future use with new volume collections. When creating multiple volume collections, it may make sense to re-use common templates for synchronization and

scheduling. Some deployments may require the use of multiple templates. For instance, the following templates could be created for standardized use cases within a given deployment:

- Protection Template 1 enables snapshots triggered by CommVault and replication to a partner retaining some number of snapshots.
- Protection Temple 2 enables snapshots triggered by CommVault without replication.

Replication Partners

Partners are easily configured and provide an opportunity to retain offsite copies of Simpana IntelliSnap backups. Replication partners should be tested when configured to validate connectivity.

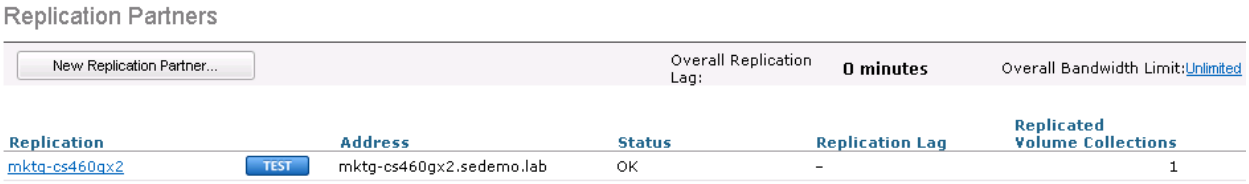

Figure 7 – Replication Partners

Shown in figure 7 is a single replication partner. Note that partner connectivity can be tested with the "TEST" button. Also note that current status, replication lag, and the number of replicated volume collections is displayed.

Note that the replication network is selectable between management or controller IP addresses and data network IP addresses. In either use case the selected network needs to be routable between Nimble Storage arrays.

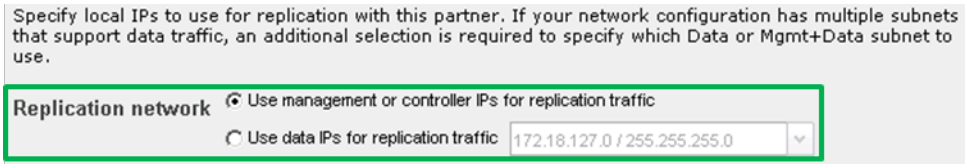

Figure 8 – Replication Network

Simpana Storage Policies

Storage policies define the storage resources used for backups and indices. They also define data aging rules and retention rules for backups. When initially created, a storage policy can accommodate a single instance of a given backup. Duplicate copies can be configured such that the storage policy can manage the creation, aging, and retention of multiple copies of a given backup.

Storage policies intended for use with IntelliSnap should be configured to consist of at least two backup copies. The copy that gets created by default when initially configuring a new storage policy will typically

use a disk or tape library selected by the user as a location to store indices. A new snapshot copy should be added to the storage policy to accommodate IntelliSnap backups.

Within the context of Simpana, each copy of a backup has a precedence value and a copy name. Precedence refers to the order in which the copy was created. Copy name is a user assigned string that can be used to identify (for instance) the location of the copy. An example of a storage policy intended for use with IntelliSnap might consist of copy precendence 1 with a copy name equal to "NimbleSnapshotCopy" and copy precedence 2 with a copy name equal to "TapeCopy".

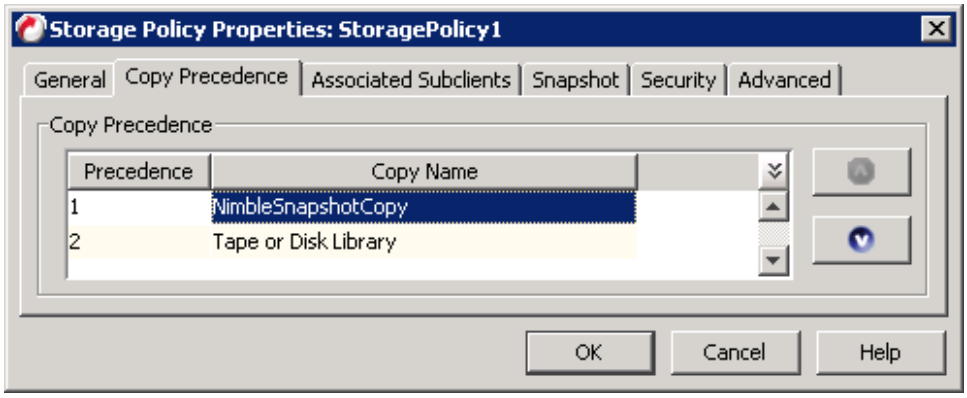

Figure 9 – Storage Policy Copy Precedence

Shown in figure 9 is the copy precedence for a storage policy. The copy names have been modified to best reflect the storage location. Copy precedence 1 represents snapshots residing on a Nimble Storage array. Copy precedence 2 represents a storage location for duplicate copies of Nimble Storage array snapshots on a tape or disk library.

Backup Copy

Creating copies or duplicates of snapshot based backups is popular for a number of reasons:

- Reason 1, in the unlikely event of an outage, application data and snapshot based backup data are not available. Having an external copy of the backup data increases an organizations ability to recover from this type of interruption.
- Reason 2, some storage vendors utilize inefficient snapshot technology that consumes substantial storage space limiting the time that snapshots can be retained. Having an external copy of backup data assists in managing storage space utilization, allowing snapshots to be deleted sooner. Nimble Storage snapshots are lightweight enough to efficiently last for months.
- Reason 3, some storage vendors cannot efficiently replicate snapshots to serve as an offsite backup copy. Having an external copy of backup data facilitates a “putting tapes on trucks” disaster recovery methodology. Nimble Storage replication leverages highly-efficient data compression technology and only transmits block-level changes which greatly reduces bandwidth requirements when compared to other storage vendors.

Backup copies sourced from IntelliSnap created snapshots on the local Nimble Storage array are expensive in terms of reading data from the storage array, moving the data through a media agent, and writing the data out to external storage media. Storage processing power, I/O operations, SAN or network traffic, and the cost of external storage media contribute to the overall expense.

This expense is can be mitigated with storage policy job selection rules. Consider creating fewer duplicate copies of backups. Consider retaining a higher number of copy precedence 1 backups (Nimble Storage array snapshots), replicating more copy precedence 1 backups, while creating a drastically reduced quantity of copy precedence 2 (external backup media) backups.

Backup copy should be enabled if the creation of duplicate backup copies is required. Storage policy job selection rules provide the ability to selectively choose which snapshots are copied to external media.

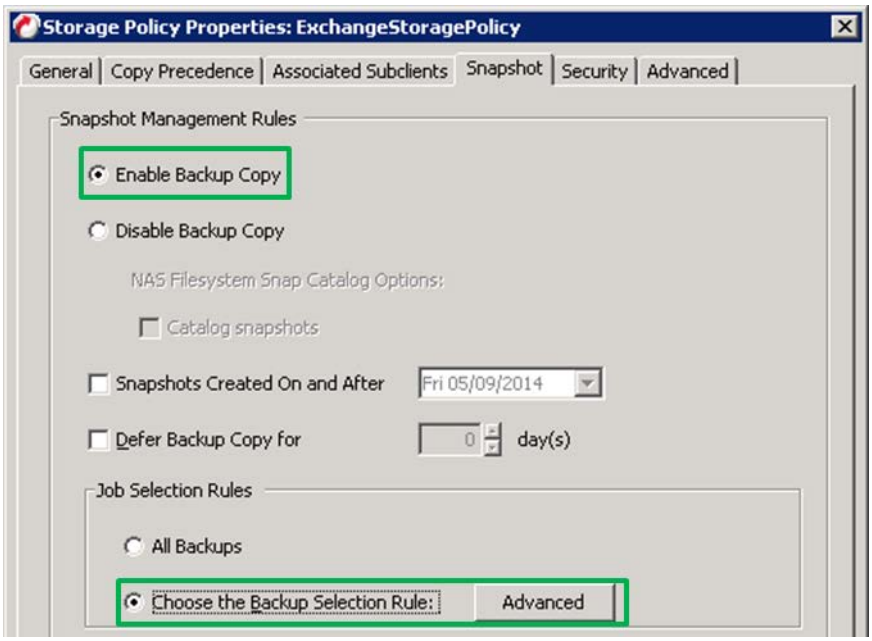

Figure 10 – Storage Policy Snapshot Management Rules

Shown in figure 10 are the snapshot management rules for a storage policy. Backup copy should be enabled if the creation of duplicate backup copies is required. Advanced job selection rules provide the ability to select which backups are copied at a granular level.

The backup selection rule dialog, invoked by clicking the “Advanced” button within storage policy snapshot management rules, facilitates selecting a subset of backups for duplication.

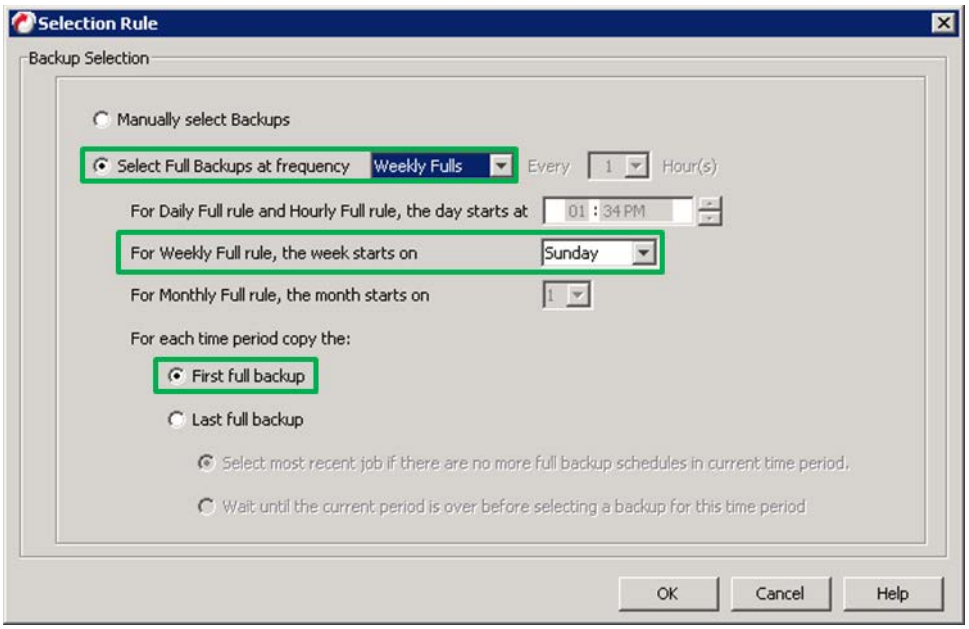

Figure 11 – Selecting Backups for Duplication

Shown in figure 11 are backup selection rules for storage policy backup copies. The example selection rule reduces the quantity of backup copies created by only selecting weekly full backups for copy creation. Sunday has been selected as the day on which the week starts, and for each period the first full backup will be used to source creation of a duplicate copy.

Similar to the way that multiple storage policies may be required to enact different retention periods for different data types, different storage policies can also be created to impose unique backup copy rules for different data types.

Proxy for Backup Copy

Backup copy operations read the contents of a volume collection snapshot, transfer the data through a media agent, and write the data out to backup media. In cases where the media agent managing the IntelliSnap snapshot is not the media agent hosting the backup media (tape, disk, etc.) a network hop between media agents becomes part of the backup copy data path. This extra hop can be eliminated by using a proxy for backup copy operations. Also eliminated is application host resource usage as the backup copy operation is effectively performed off-host.

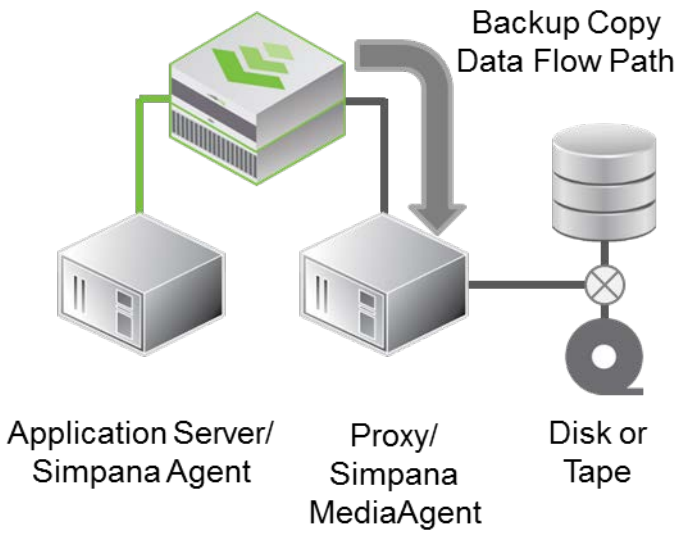

Figure 12 – Proxy for Backup Copy

Shown in figure 12 is a representation of the data path used for a proxy backup copy operation. The use of a proxy eliminates the network hop between application server and external backup media while also eliminating resource usage on the application server.

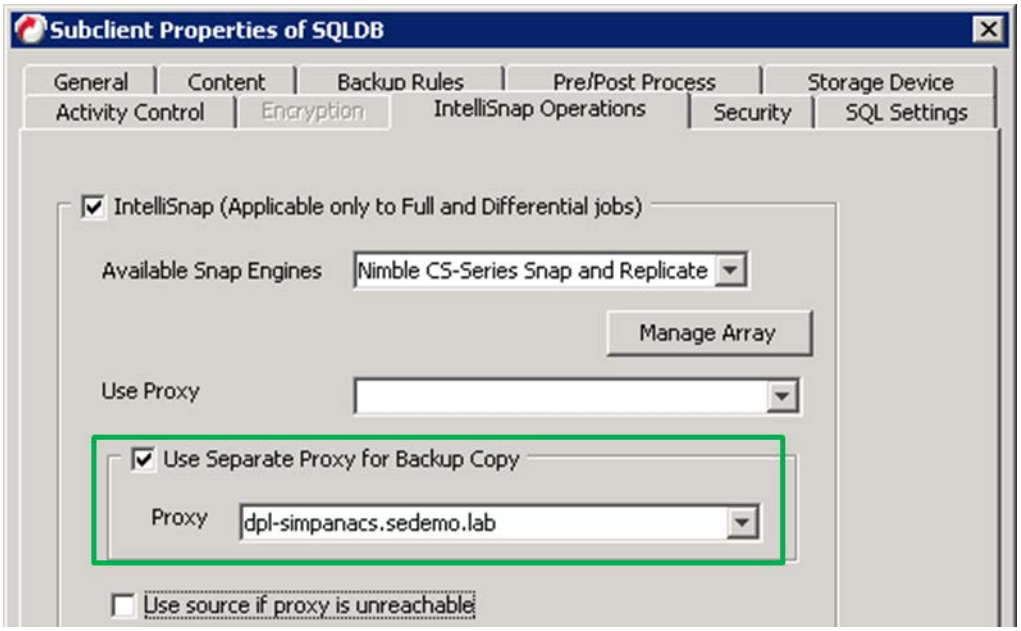

Figure 13 – Proxy for Backup Copy

Shown in figure 13 is the IntelliSnap Operations tab of a subclient. A proxy has been selected for backup copy operations.

In addition to configuring Simpana for backup copy proxy usage, the Nimble Storage volume collection member volumes require modification to their access privileges. The Simpana proxy host needs to have unrestricted snapshot access rights on all volumes within the volume collection.

Figure 14 – Access Privileges for Proxy Host

Shown in figure 14 are access permissions for a member of a volume collection. A Simpana backup copy proxy media agent needs to be granted unrestricted access to snapshots on all member volumes within a volume collection. Note that the "Allow multiple initiator access" checkbox also needs to be checked.

Snap Copy – Data Aging & Retention

Snap copy data aging should be enabled as it allows data from the copy to be deleted when the retention rules have been met. The Simpana data aging process deletes old snapshots that no longer need to be retained.

Retention criteria can be specified in a number of ways to accommodate virtually any retention strategy. As discussed previously in the Backup Copy section of this document, maximizing the use of snapshots and minimizing the use of copies is highly desirable.

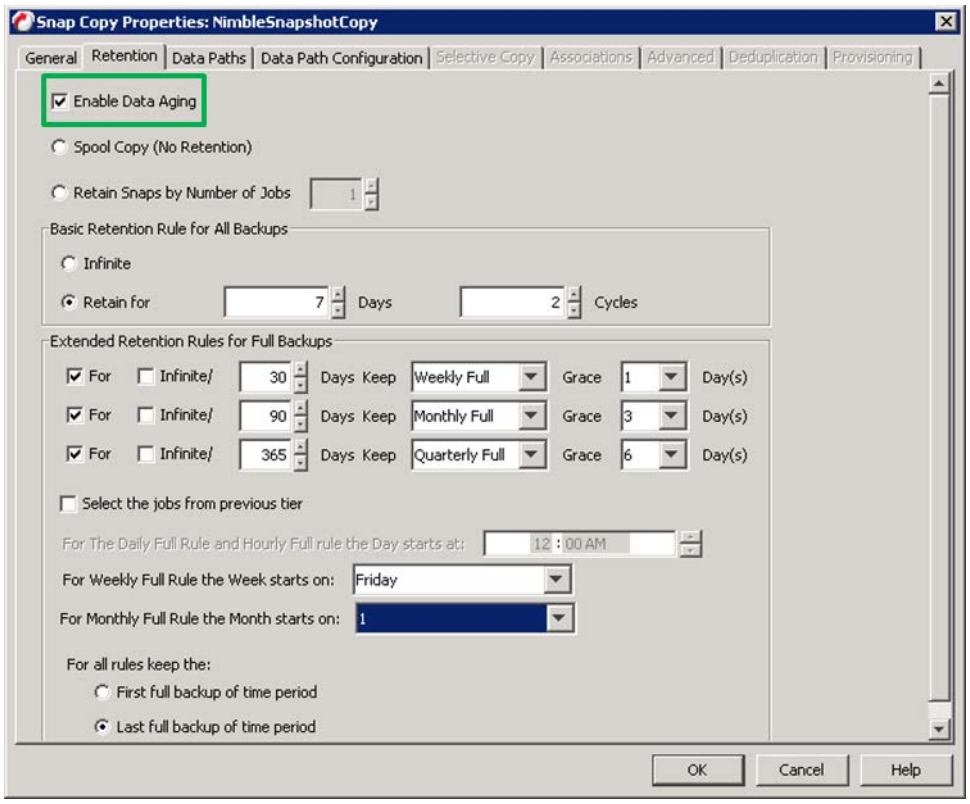

Figure 15 – Snap Copy Retention

Shown in figure 15 is an example Snap Copy Retention strategy. Enabling data aging is recommended. Basic and extended retention rules can be configured to retain snapshots based on business requirements.

Simpana Client & Subclient Properties

Enabling IntelliSnap at the client level is required in order to configure IntelliSnap parameters at the subclient level. From the client properties dialog window, click the “Advanced” button. Within the advanced client properties dialog window the “Enable IntelliSnap” box needs to be checked.

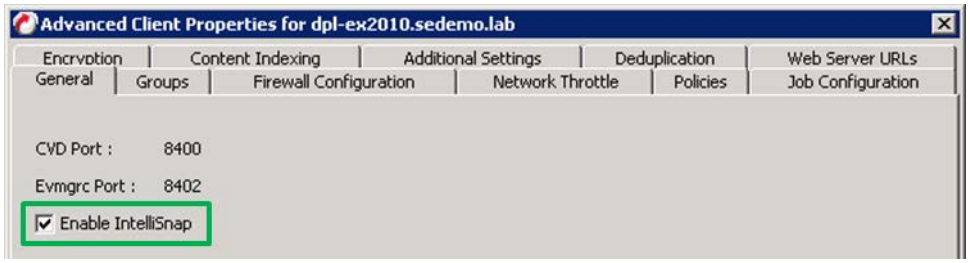

Figure 16 – Advanced Client – Enable IntelliSnap

At the subclient level, Intellisnap should be enabled and the “Nimble CS-Series Snap and Replicate” snap engine should be selected. Selecting this snap engine is applicable to the use case where Nimble

Storage array snapshots will be taken on the local array and replicated to a destination array, as well as the use case where snapshots will be taken without replication.

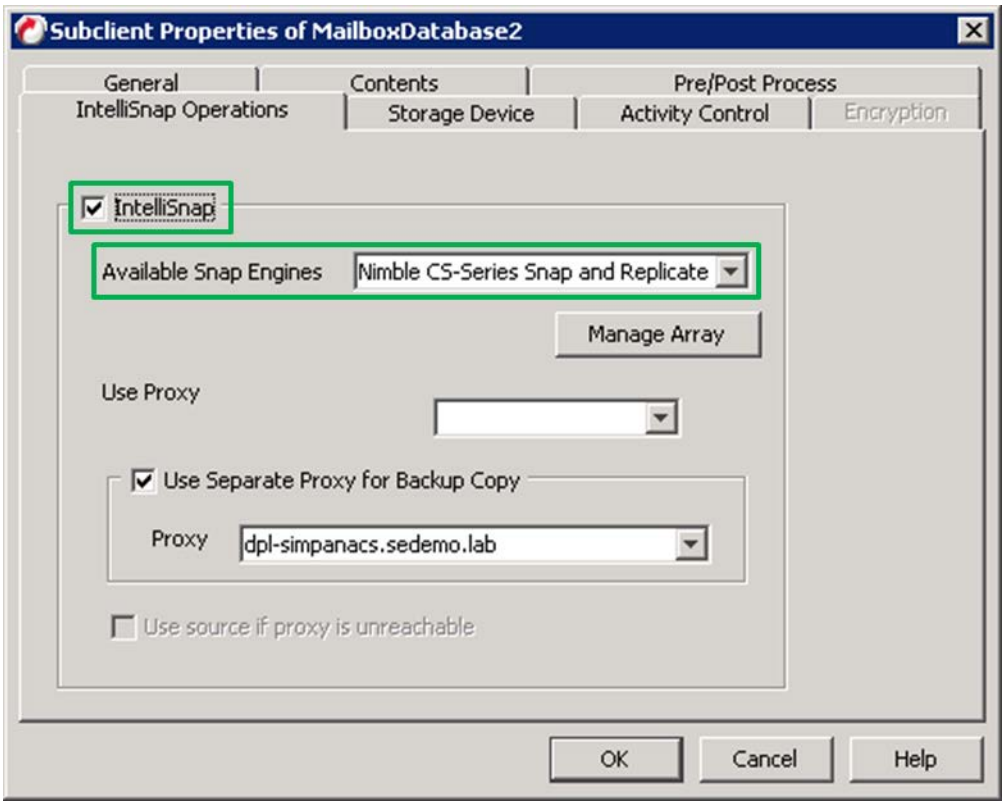

Figure 17 – IntelliSnap Operations

Shown in graphic 17 is the IntelliSnap Operations dialog window for a subclient. IntelliSnap must be enabled by checking the IntelliSnap checkbox, and the "Nimble CS-Series Snap and Replicate" snap engine should be selected from the pull down menu.

Optionally, the backup copy proxy host can also be set at this time if desired.

The subclient properties storage device also needs to be configured. It is important to select a storage policy that has been configured with a snapshot copy.

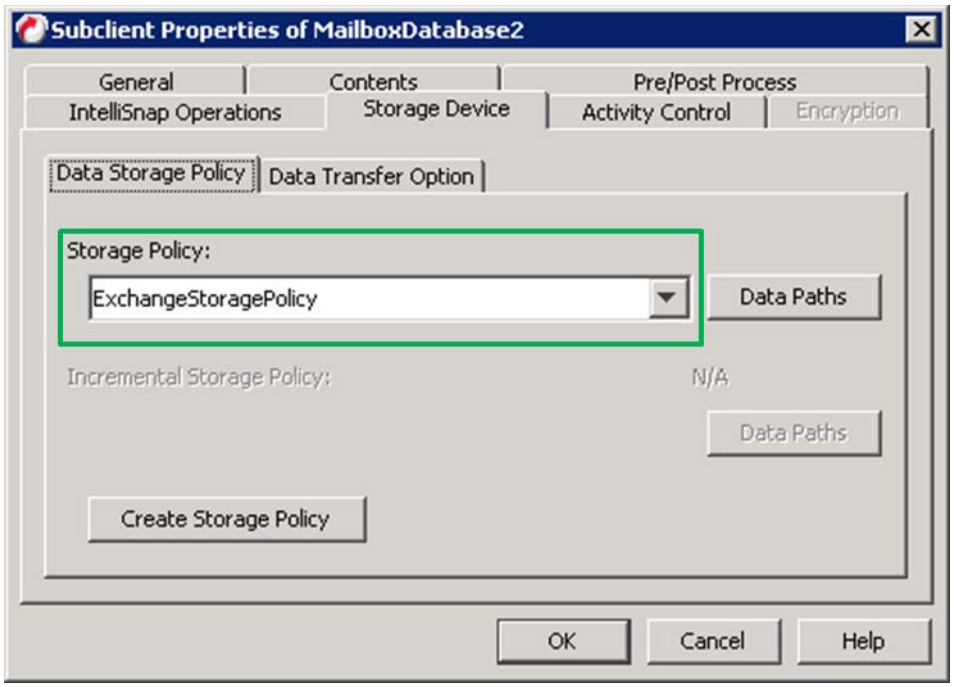

Figure 18 – Subclient Storage Device

Shown in figure 18 is the storage device data storage policy for a subclient. It is important to select a storage policy that has been configured with a snapshot copy.

Recovery

Listing Snapshots

Snapshots can be viewed from within Simpana in two ways. The first method is to right click a client iData Agent and then select “All Tasks > List Snaps” from the pop-up menu. This provides a list of all IntelliSnap snapshots for a specific agent on a specific client. The second method is to use the array management user interface, select a Nimble Storage array, and the click the “List Snaps” button. This provides a list of all IntelliSnap snapshots on the selected array.

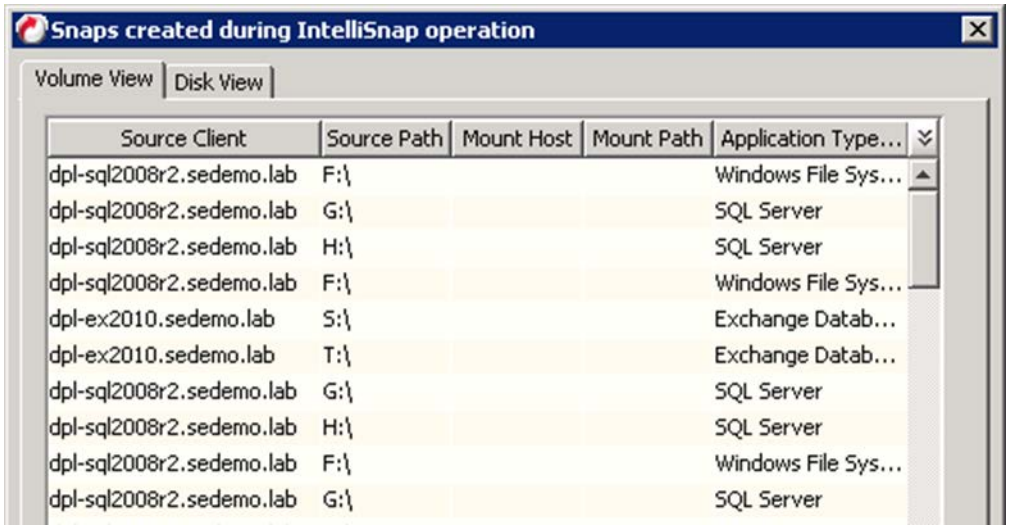

Figure 19 – IntelliSnap Snapshots on a Nimble Storage Array

From the Nimble Storage web user interface, snapshots can be viewed by selecting a particular volume or volume collection, and then clicking on the snapshot tab.

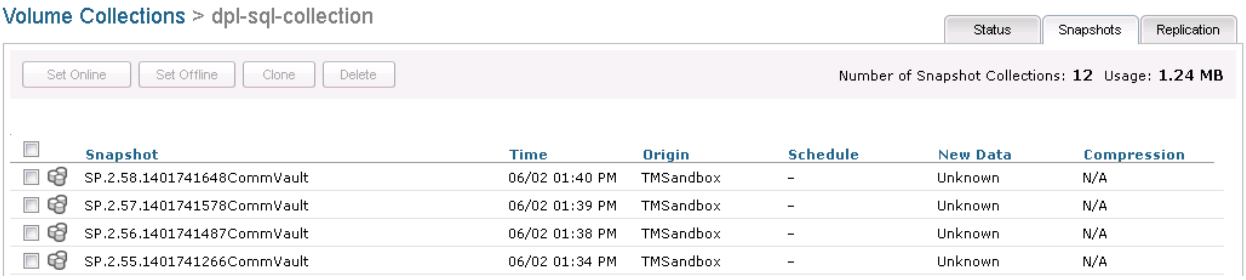

Figure 20 – Snapshots in a Nimble Storage Volume Collection

Local Recovery with Simpana

Right clicking the desired iData Agent for a given client, select “All Tasks > Browse and Restore” from the pop-up menu. View backup content and then select the content to be recovered. The workflow is similar to any Simpana recovery operation. Depending on the iData Agent type, there may be an advanced option available to use the hardware revert capability.

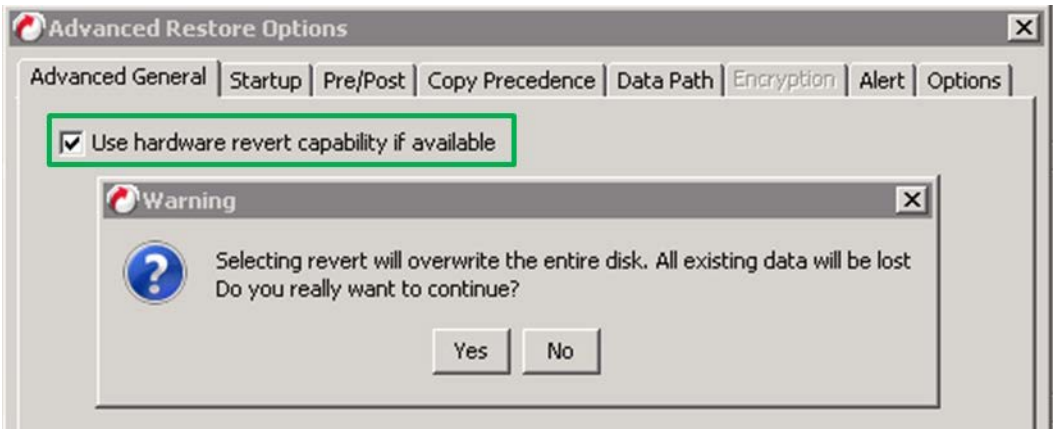

Figure 21 – Simpana Advanced Restore Option – Hardware Revert

Shown in figure 21 is the Simpana advanced restore option hardware revert. Selecting this option brings the entire Nimble Storage volume collection back to the point in time when the snapshot was created.

Hardware revert should be used only when it is necessary to recover an entire volume collection as all data on the volumes will revert back to the time the snapshot was taken. In some use cases, hardware revert may execute faster than a conventional recovery. Instead of copying backup data from a snapshot back into the active file system, hardware revert restores Nimble Storage volumes at the array level without data movement. Hardware revert would be significantly faster in cases where a single large database was being recovered, for example.

Non-Application Aware Recovery

The ability to perform recovery without application awareness is covered here for awareness but is not recommend in practice. Listing snapshots, and right clicking a single snapshot displays a pop-up menu with the option to use the hardware revert capability of the Nimble Storage array. Exercise caution if deciding to use this functionality as it can corrupt a running application.

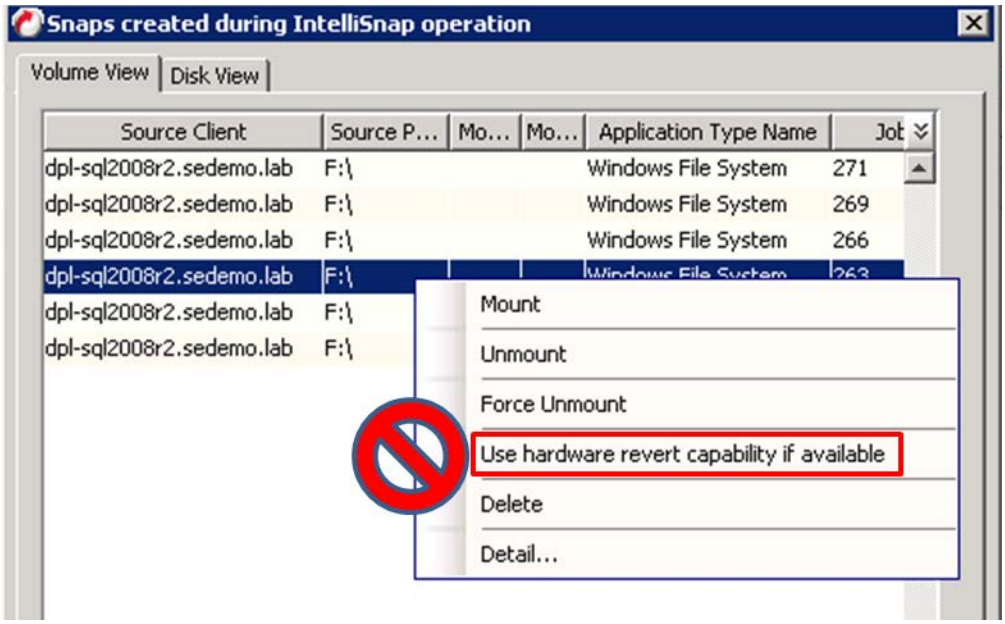

Figure 22 – Non-Application Aware Recovery

Shown in figure 22 is the ability to perform a non-application aware recovery using the hardware revert capability of the Nimble Storage array. Using this capability is not recommended as it may corrupt a running application.

Using Replicated Snapshots for Recovery

IntelliSnap created snapshots are application consistent and reside on the local Nimble Storage array in native file system format. When these snapshots are replicated with Nimble volume collection schedules they will retain the same application consistency and native file system formatting. Unlike backups that may have been written in ANSI, TAR, MTF, or CPIO format, using replicated IntelliSnap created snapshots to recover data or conduct recovery testing is simple and easy.

A short series of steps are executed to enable recovery from replicated volume collection snapshots:

- A volume collection snapshot is cloned to create one or more volumes.
- The cloned volumes are edited to allow access from the desired initiator group and placed online.
- The volumes are discovered by and connected to the desired host.

Once online, the data contained within the snapshot is available for use. Data on the cloned volumes can be used in R/W mode or copied to another location.

Cloned volumes provide an excellent vehicle for disaster recovery testing without impacting production workload. Cloned volumes consume no additional array disk space at creation time. During testing, the content of volume collection snapshots are not altered, the original backup content remains pristine. At the completion of testing, cloned volumes can disconnected from the host, taken offline, and deleted.

The following example details the use of replicated snapshots for MS SQL data recovery. Recovery techniques for other data types will vary, but the underlying principles are the same.

Recovery Example: MS SQL Database Recovery

Replicated volume collection snapshots represent points in time to which a given database can be recovered. Decide which snapshot best meets the recovery objective and then clone the volume collection snapshot. This will create cloned volumes for both the database and log volumes. Edit the cloned volumes to allow access by the initiator group associated with the MS SQL Server host and then set them online. Discover and connect the cloned volumes on the MS SQL Server host. Set the disks online using the Windows Server Manager Disk Management user interface. Copy the correct MDF and LDF files to the desired file system path. (Note: An alternative approach where the cloned volumes are used in R/W mode is also possible but may require the use of the "DiskPart" utility to clear the "Read-only" volume attribute. This eliminates the need to copy MDF and LDF files to an alternate location.) Attach the database using the MS SQL Server Management Studio.

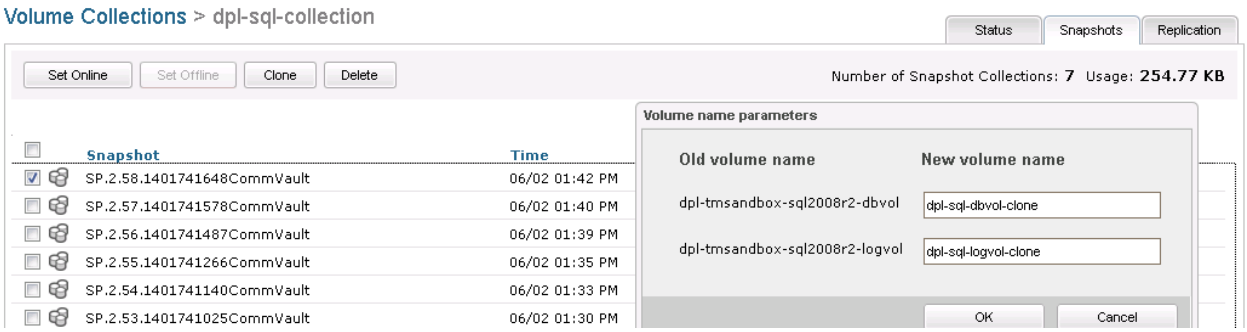

Figure 23 – Cloning a Volume Collection

Shown in figure 23 is a replicated Simpana IntelliSnap volume collection snapshot selected for cloning.

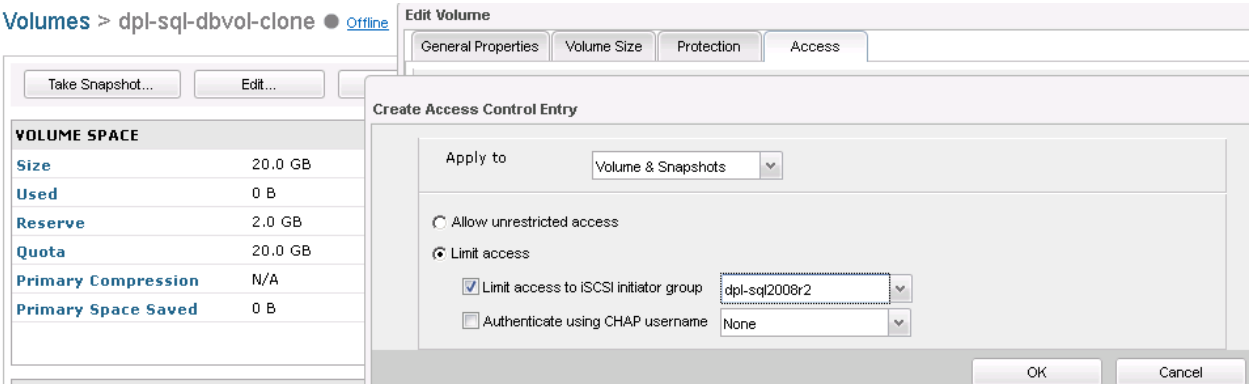

Figure 24 – Editing Volume Access

Shown in figure 24 is the initiator group of a MS SQL Server being added as an access control entry. This action should be performed for both the database and log volumes.

Figure 25 – Set Volume Online

Shown in figure 25 is the "Set Online" button. The cloned database and log volumes should both be set online.

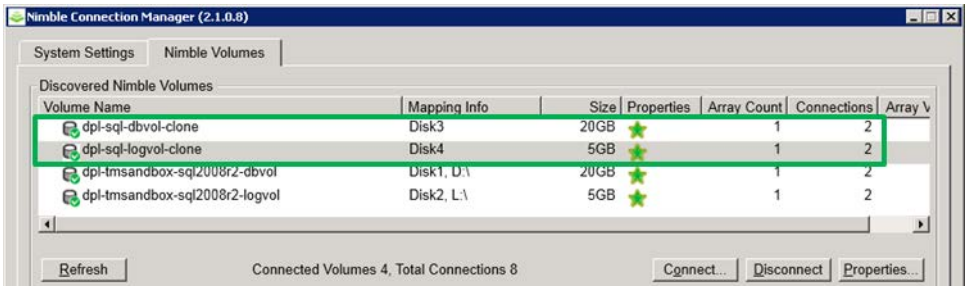

Figure 26 – Nimble Connection Manager

Shown in figure 26 are the cloned database and log volumes after being discovered and connected.

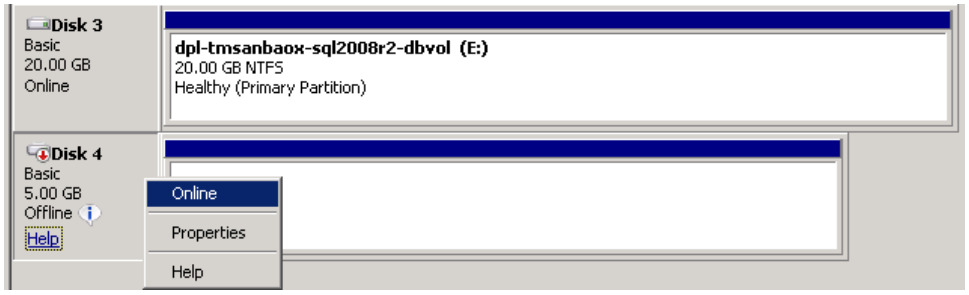

Figure 27 – Windows Server Manager – Disk Management

Shown in figure 27 are disks 3 and 4 representing the MS SQL database and log volumes. Both disks need to be set online.

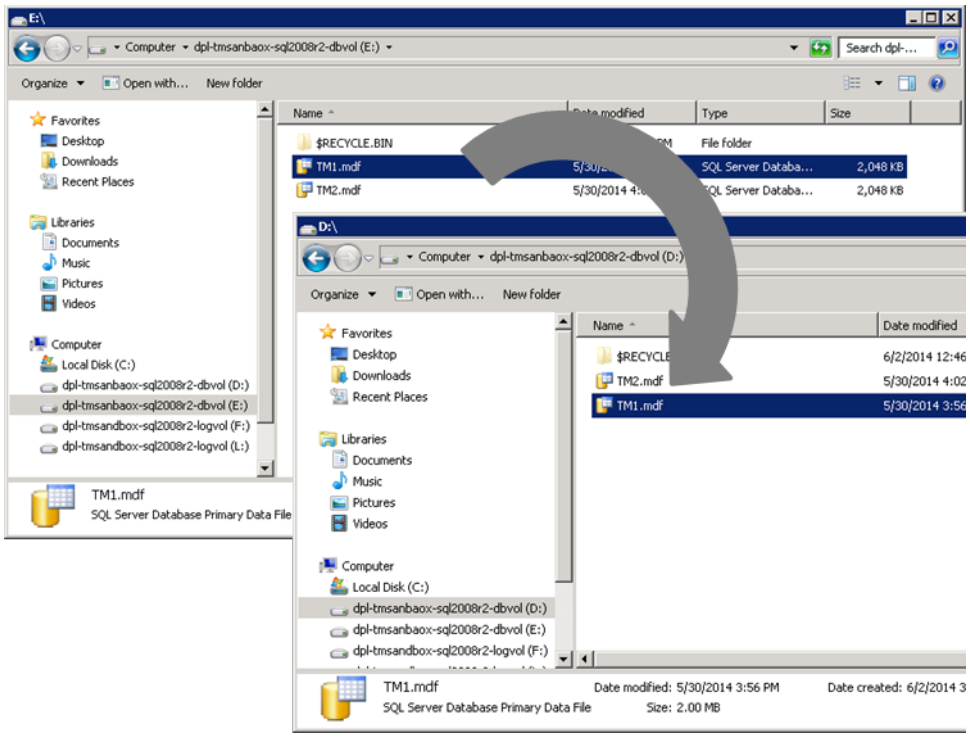

Figure 28 – Copy MDF & LDF Files

Depicted in figure 28 is a copy operation where a MS SQL database file has been copied from a cloned volume to the desired file system path. This operation needs to be performed for both the MDF and LDF files for each database being recovered. An alternative approach where the cloned volumes are used in R/W mode is also possible but may require the use of the "DiskPart" utility to clear the "Read-only" volume attribute. This eliminates the need to copy MDF and LDF files to an alternate location.

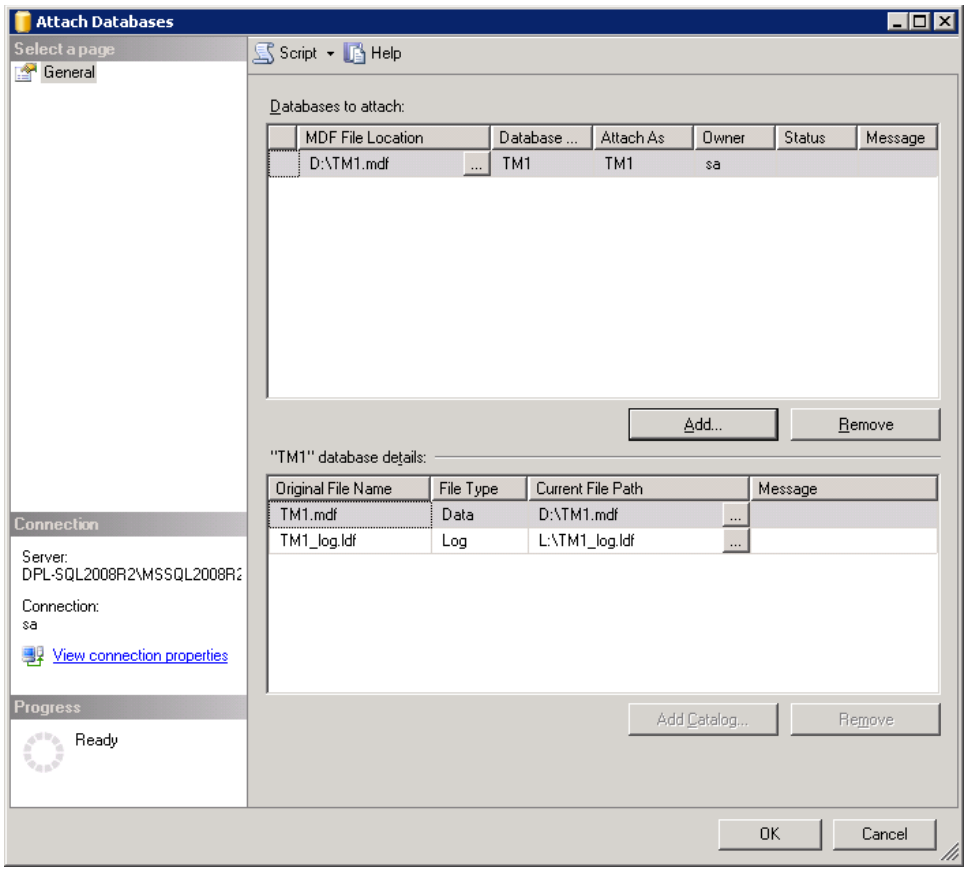

Figure 29 – Attach Database

Shown in figure 29 are the MDF and LDF files copied from the cloned volumes being attached as a database. Note that the "Attach As" field can be altered to attach the recovered database using a different name.

Appendix A: Nimble Storage as a Simpana Disk Library

While the primary focus of this document is Nimble Storage array integration with Simpana IntelliSnap, there may be cases where utilizing a Nimble Storage volume as a Simpana disk library is desirable. This section provides guidelines for configuring the Nimble Storage volume, performance policy, Simpana Media Agent host, and Simpana disk library.

Nimble Storage Performance Policy

Performance policies align the performance requirements of a given application with the performance characteristics of a target Nimble Storage volume. Options to set the storage block size, compression, caching, and "quota exceeded behavior" parameters on a Nimble Storage volume should be configured for use as a Simpana disk library.

In the example provided below, storage block size has been configured to 32 KB, the same value will be configured for the Simpana storage policy copy block size. Compression has been enabled in this example because Simpana subclient software compression has been disabled. Caching is not enabled because backup streams written to the disk library will only be read from disk in the event of a restore request. The space management parameter, "Quota Exceeded Behavior", has been set to "Non-Writeable" instead of offline so that restore requests can be fulfilled even if the volume quota is exceeded.

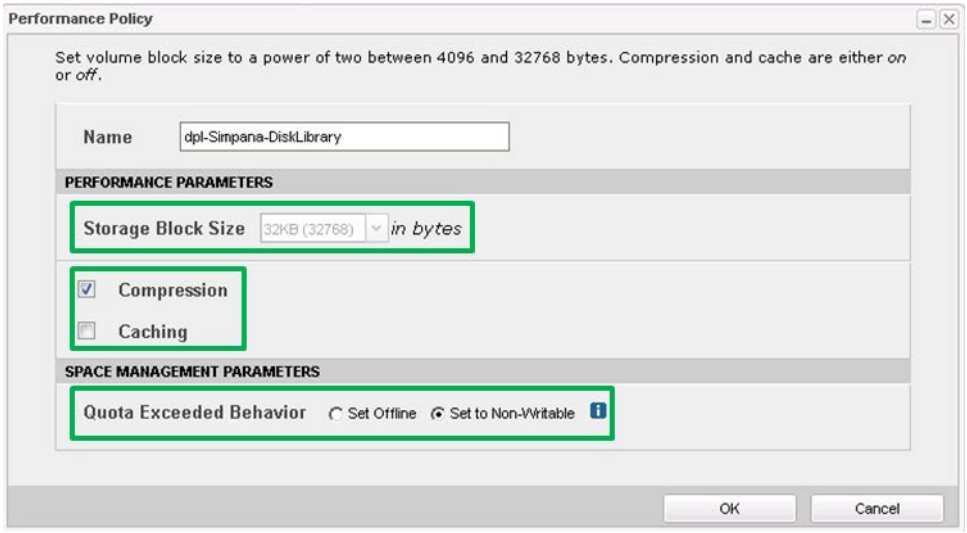

Figure 30 – Nimble Storage Performance Policy

Shown in figure 30 is an example Nimble Storage performance policy. The storage block size, compression, caching, and space management parameters have been set to best align with the intended usage of the volume.

Nimble Storage Initiator Group

The Nimble Storage volume created for use as a Simpana disk library should only be accessed by the specific initiator within the designated Simpana media agent. An initiator group containing only the initiator of the media agent should be configured.

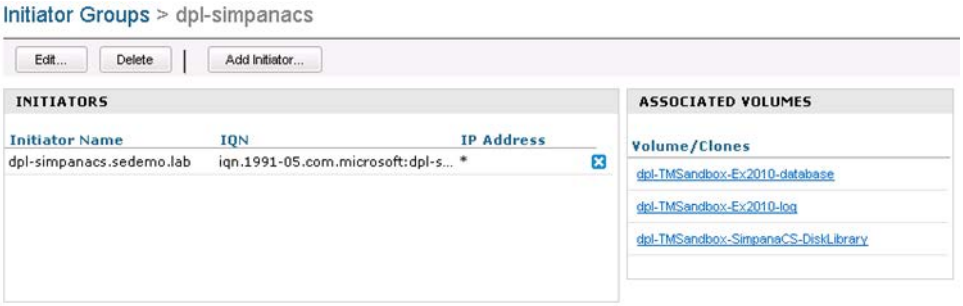

Figure 31 – Nimble Storage Initiator Group

Shown in figure 31 is an initiator group containing only the initiator of the Simpana media agent that will use a target Nimble Storage volume as a Simpana disk library. Note that the initiator group has additional volumes associated with it in order for the media agent to act as a proxy during backup copy operations.

Nimble Storage Volume

The volume created for use as a Simpana disk library should be configured to use the performance policy that was created specifically for use with disk libraries. Volume reserve space should be configured to account for compression (if compression is enabled in the performance policy). Compression typically reaches a 50% ratio, and volume reserve should be configured with a maximum value of 50% of total volume size to avoid reserving array space that may never actually be used.

Volume protection should be set to a value of “None”. This produces “Not Protected” status. This status is appropriate as the volume is being used as a disk library.

Simpana Media Agent

Connecting the Nimble Storage volume to a media agent requires a supported host initiator and operating system for the version of Nimble OS being used. Consult the “Nimble Storage Support Matrix” for the version of Nimble OS being used to assure a supported configuration is being deployed. Nimble Storage compatibility matrices are available on the Nimble Storage InfoSight web portal.

In the example provided, the Simpana media agent is running Microsoft Windows 2008R2 updated with appropriate Microsoft patches and hotfixes. The Nimble Windows Toolkit, available for download from the Nimble Storage InfoSight web portal, includes Nimble Connection Manager software. The Nimble Connection Manager should be configured to discover the Nimble Storage array based on the initiator name of the array.

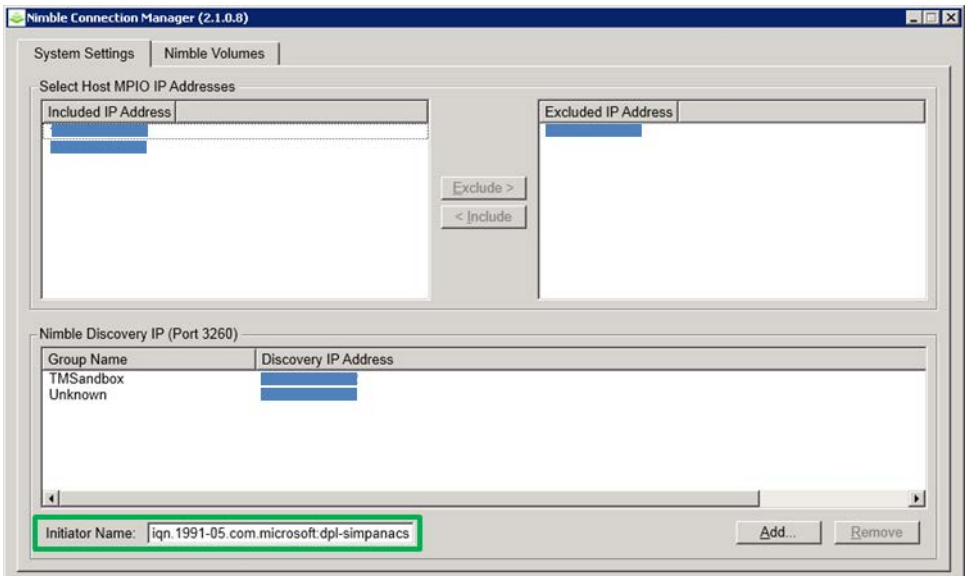

Figure 32 – Nimble Connection Manager - System Settings

Shown in figure 32 is the Nimble Connection Manager configured to discover volumes on the Nimble Storage array containing a volume to be used as a Simpana disk library.

The “Nimble Volumes” tab of the Nimble Connection Manager with the volume that will be used as a Simpana disk library:

Figure 33 – Nimble Connection Manager - Nimble Volumes

Note that the connected volume should be configured to connect on startup.

Figure 34 – Connect on Startup Property

At this point the Windows Server Manager can be used to initialize, format, and assign a drive letter to the volume.

Simpana Disk Library

The Simpana Library and Drive Configuration user interface should be used to configure the new volume as a library. The data path for storage policy copies using the new disk library should be configured to use a block size of 32 KB.

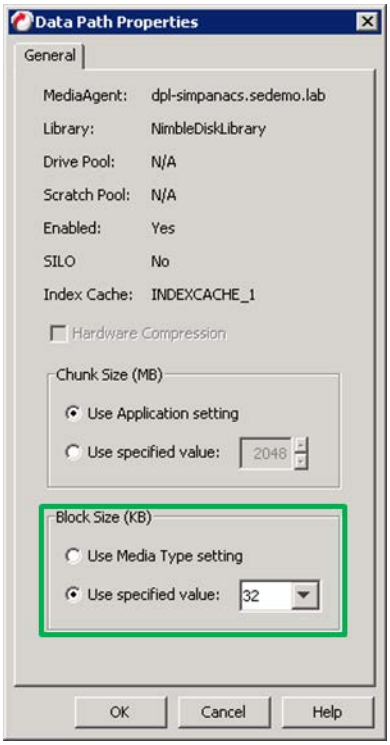

Figure 35 – Data Path Properties

Shown in figure 35 is the data path properties dialog for a storage policy copy that uses the disk library. The block size should be configured to correspond to the block size set within the Nimble Storage performance policy used for the volume.

Nimble Storage, Inc.
211 River Oaks Parkway, San Jose, CA 95134
Tel: 877-364-6253; 408-432-9600 | www.nimblestorage.com | info@nimblestorage.com

© 2014 Nimble Storage, Inc. Nimble Storage, the Nimble Storage logo, InfoSight, CASL, SmartStack, and NimbleConnect are trademarks or registered trademarks of Nimble Storage, Inc. All other trademarks are the property of their respective owners. BPG-SIM-0914