TECHNICAL PAPER

Veeam Backup & Replication with Nimble Storage

Document Revision

Date	Revision	Description (author)
11/26/2014	1. 0	Draft release (Bill Roth)
12/23/2014	1.1	Draft update (Bill Roth)
2/20/2015	2.0	Draft update (Bill Roth)
2/20/2015	2.2	Published version 1(Bill Roth)

Table of Contents

List of Figures

Introduction

Audience

Veeam Backup & Replication administrators and Nimble Storage administrators are encouraged to read this document. The recommendations and usage scenarios presented set out to create an understanding of how to take advantage of Nimble Storage capabilities when deployed as part of a Veeam Backup & Replication solution.

Assumptions

- General knowledge of and familiarity with the Nimble Storage user interface and basic setup tasks
- Experience with and knowledge of Veeam Backup & Replication

Limitations and Other Considerations

Descriptions and examples provided in this document are constrained to Nimble Storage software versions 2.1.2 and higher with iSCSI network connectivity. Veeam Backup & Replication descriptions and examples are based on version 8.

Overview

The deployment of Nimble Storage in conjunction with Veeam Backup & Replication falls into two general categories; 1) Taking advantage of Veeam Backup & Replication to protect data stored on a Nimble Storage array, and 2) Taking advantage of Nimble Storage when used within Veeam Backup & Replication as backup infrastructure components.

Nimble Storage is widely deployed as storage for VMware in the form of datastores. Leveraging Veeam Backup & Replication as the vehicle to orchestrate protection and recovery of these datastores includes the ability to use different virtual disk transport methods. Configuring LAN, SAN, and HotAdd transport modes with Nimble Storage is detailed to assist in meeting data protection requirements.

Veeam Backup & Replication is widely deployed and includes backup infrastructure components that enable both basic and advanced functionality. Nimble Storage can be used as a backup repository, the location used to store backup files. Nimble Storage can also be used as vPower NFS root folder storage, playing a high performance role in Veeam SureBackup, and Instant VM Recovery. Additionally, Nimble Storage is the logical choice for use as a Veeam virtual lab datastore, where redo logs are temporarily stored while virtual machines run from read-only backup files.

Subsequent sections of this paper take a deeper look into these use case categories.

Protecting VMware Datastores on Nimble Storage

By definition a VMware datastore is a storage location for virtual machine files. When the datastore resides on a Nimble Storage array, it consists of a Nimble volume presented to one or more ESXi hosts and has been formatted as a VMFS (Virtual Machine File System) volume. Veeam Backup & Replication can be configured to protect the datastore via three supported virtual disk transport methods: LAN, SAN, and HotAdd.

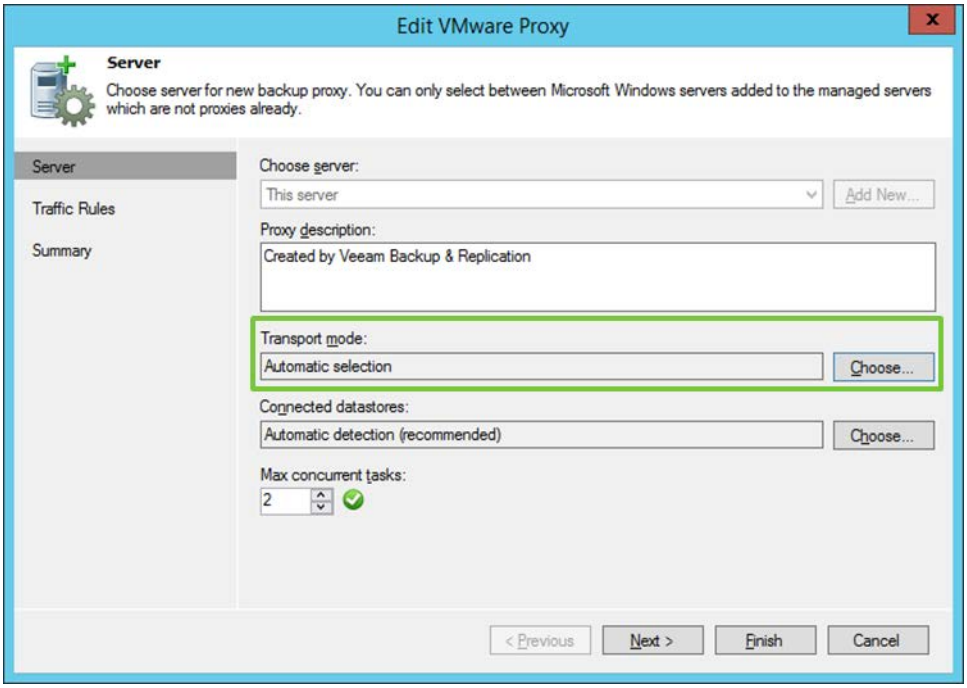

Figure 1: Automatic Transport Selection

By default Veeam Backup & Replication will use automatic backup proxy transport selection, where the backup proxy and connected VMFS datastore are analyzed to determine the most efficient transport mode that can be used. The default mode can be altered by editing the properties of the backup proxy.

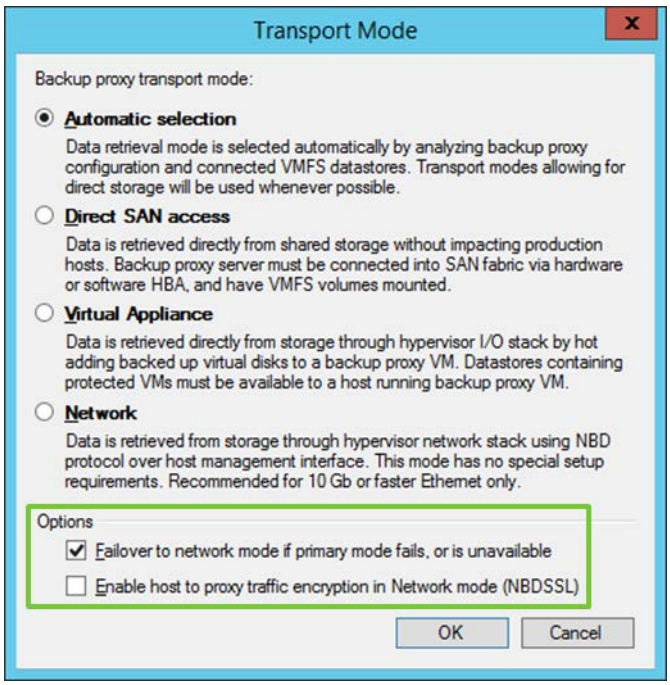

Figure 2: Transport Mode Selection

The transport mode can be modified to use a specific transport:

- Direct SAN access mode to use the SAN transport
- Virtual Appliance mode to use the HotAdd transport
- Network to use the LAN (NBD) transport

There are also two optional parameters that can be altered. The first is “Failover to network mode if primary mode fails or is unavailable”. This option is enabled by default. The second optional parameter enables NBDSSL when the LAN transport is used.

LAN (NBD) Transport

Within Veeam Backup & Replication, this transport mode is referred to as “Network” transport mode. LAN transport for data access uses NBD (Network Block Device) or NBDSSL (Encrypted Network Block Device) to move data over a TCP/IP connection. By default this transport mode is used when no other transport mode is available or when it is explicitly selected. It is generally considered to be the least efficient transport mode.

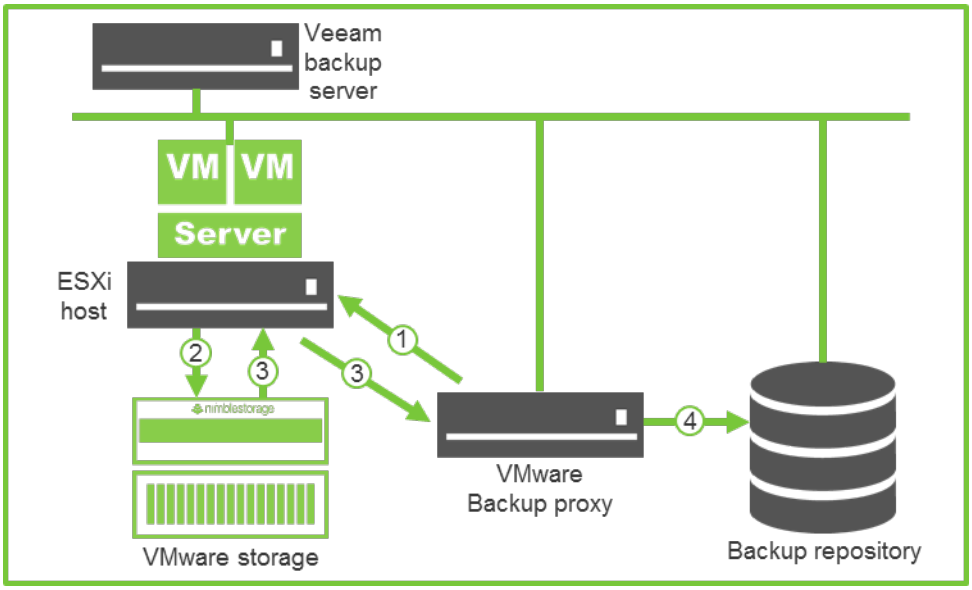

Figure 3: LAN Transport

The data retrieval flow for a LAN transport backup can be summarized in four different steps:

- In step 1 the backup proxy sends a request to the ESXi host to locate the necessary VM on the datastore
- In step 2 the ESXi host locates the VM on storage
- In step 3 VM data blocks are copied from storage and sent to the backup proxy over the LAN
- In step 4 the backup proxy sends the data to the backup repository

On the Nimble array, no changes or alterations are required to support the LAN transport mode. The ESXi host or hosts accessing the datastore volume already have access permission.

SAN Transport

Within Veeam Backup & Replication, this transport mode is referred to as “Direct SAN access” transport mode. SAN transport mode reads data directly from the SAN or iSCSI LUN where a virtual disk resides. It is generally considered to be the most efficient transport mode as no data is transferred through the production ESXi host.

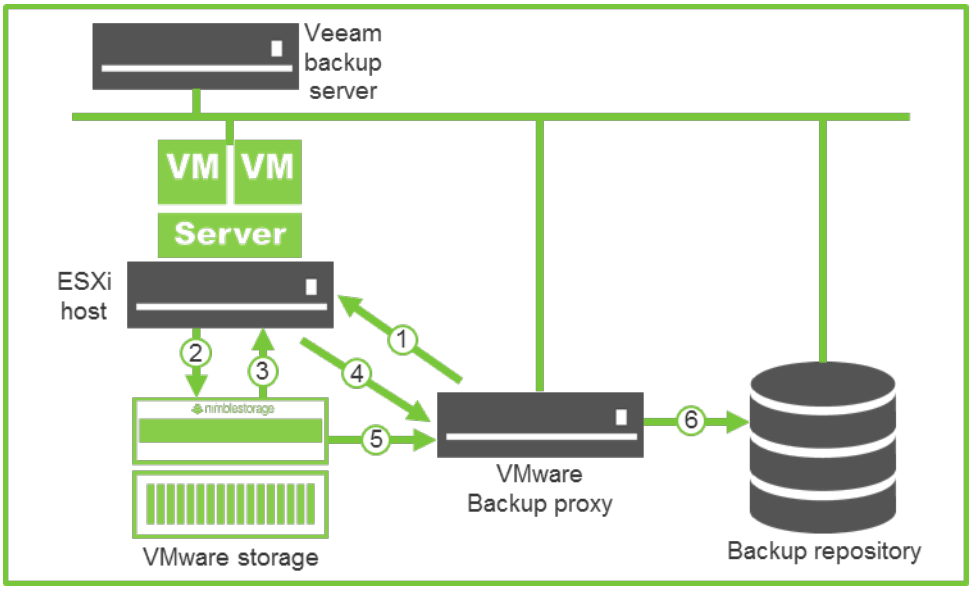

Figure 4: SAN Transport

The data retrieval flow for a SAN transport backup can be summarized in six different steps:

- In step 1 the backup proxy sends a request to the ESXi host to locate the necessary VM on the datastore
- In step 2 the ESXi host locates the VM on storage
- In step 3 the ESXi host retrieves metadata about the layout of VM disks on the storage
- In step 4 the ESXi host sends metadata to the backup proxy
- In step 5 the backup proxy uses metadata to copy VM data blocks directly from storage via the SAN
- In step 6 the backup proxy processes copied data blocks and sends them to the backup repository

Enabling SAN transport mode backups requires a minor configuration change on the Nimble Storage array. Datastore volume access permission changes are necessary. This change grants volume level access to one or more Veeam Backup & Replication proxy servers.

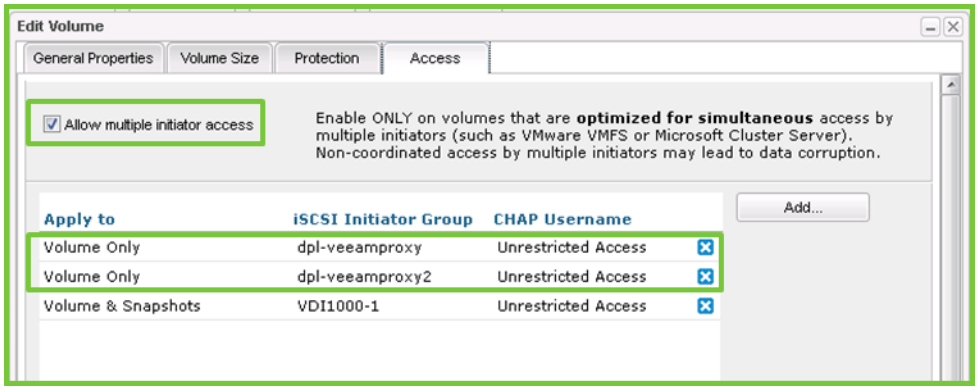

Figure 5: Nimble Volume Access

The Nimble array volume used as a VMware datastore should be edited to add access permission for one or more Veeam Backup & Replication proxy servers. This change makes it possible for the backup

proxy server(s) to copy VM data blocks directly from storage over a SAN connection, bypassing the production ESXi server during the retrieval process. Note that the “Allow multiple initiator access” property also needs to be enabled. See “Appendix 1” in this document for additional information about initiator groups.

On each Veeam Backup & Replication proxy server that may be used to perform SAN transport mode retrieval, the VMware datastore volume needs to be connected.

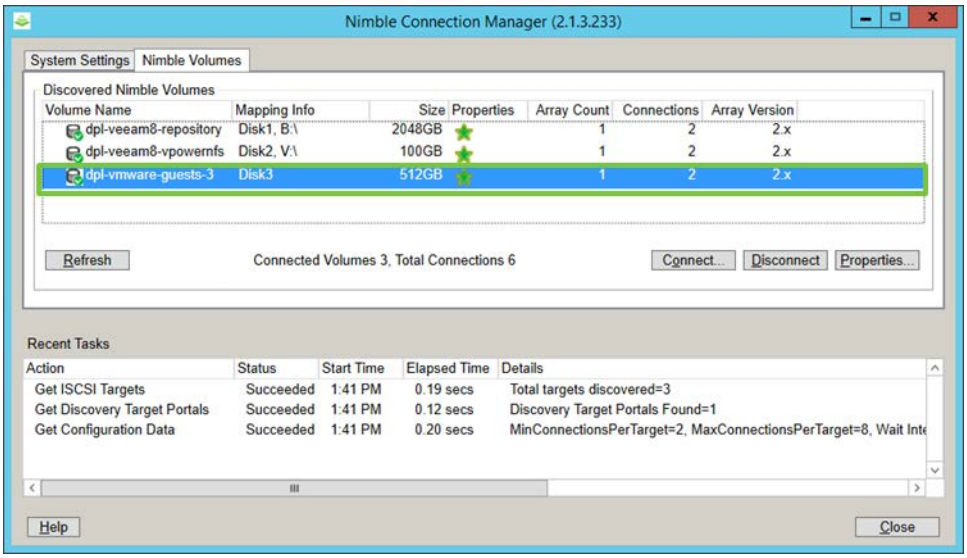

Figure 6: Nimble Connection Manager - Nimble Volumes

Use the Nimble Connection Manager to discover and connect the VMware datastore volume. During the connect process accept the default “Connect on startup” property. See “Appendix 2” in this document for additional information about the Nimble Connection Manager.

Note that a Windows drive letter should not be assigned to the volume.

HotAdd Transport

Within Veeam Backup & Replication, this transport mode is referred to as “Virtual Appliance” transport mode. This transport mode reads data directly from storage through the hypervisor I/O stack by hot adding a virtual disk to the backup proxy VM guest.

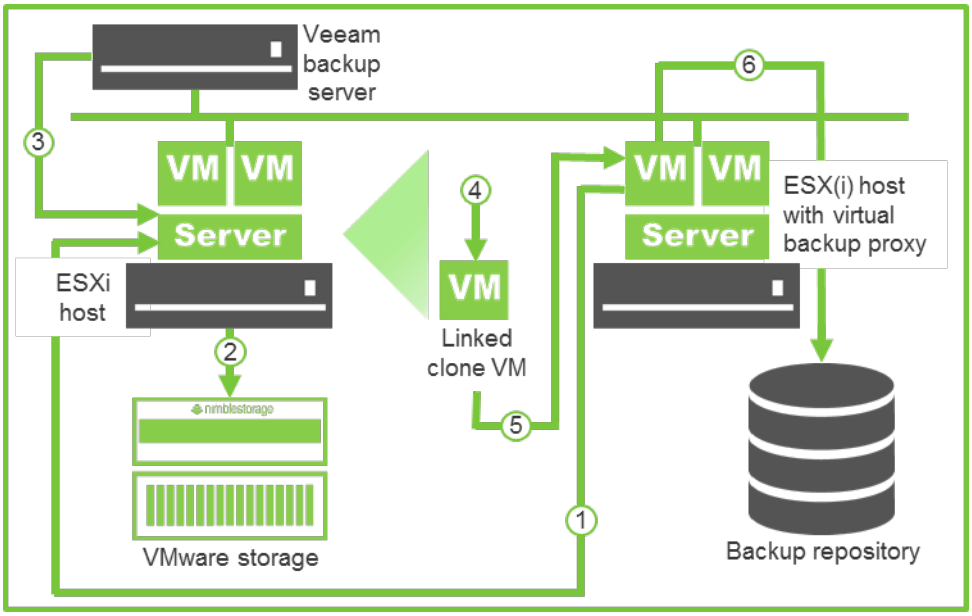

Figure 7: HotAdd Transport

The data retrieval flow for a HotAdd transport backup can be summarized in six different steps:

- In step 1 the backup proxy sends a request to the ESXi host to locate the necessary VM on the datastore
- In step 2 the ESXi host locates the VM
- In step 3 Veeam Backup & Replication triggers VMware vSphere to create a VM snapshot
- In step 4 VMware vSphere creates a linked clone VM from the VM snapshot
- In step 5 disks of the linked clone VM are hot-added to the backup proxy VM
- In step 6 Veeam Backup & Replication reads data directly from disks attached to the backup proxy VM through the ESXi I/O stack

On the Nimble array, no changes or alterations are required to support the HotAdd transport mode. The ESXi host or hosts accessing the datastore volume already have access permission.

Backup Repositories on Nimble Storage

This section examines the use of a Nimble Storage volume deployed as a Veeam backup repository. A backup repository is a storage location used by Veeam Backup & Replication jobs to store backup files.

Create a Nimble Storage Volume for use as a Backup Repository

Create a new volume on the Nimble Storage array. From the user interface select “Manage > Volumes” and then click the “New Volume” button.

Figure 8: New Volume

Name the volume and then select a performance policy. The Nimble volume should be configured to use the optimal performance policy based on the host platform that will mount the volume, in this example that's the server backing the repository.

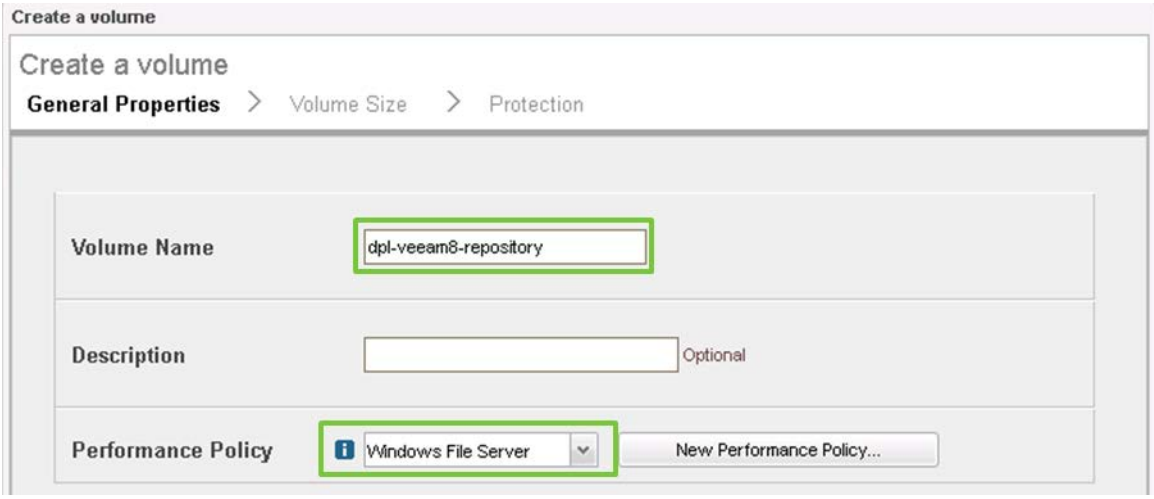

Figure 9: General Properties

This example uses a Veeam proxy server running on Microsoft Windows Server 2012 R2 that will function as the server backing the repository. The Nimble volume performance policy has been set to "Windows File Server", the recommended setting for this use case. Note that a customized performance policy can be created and used instead of a preconfigured performance policy.

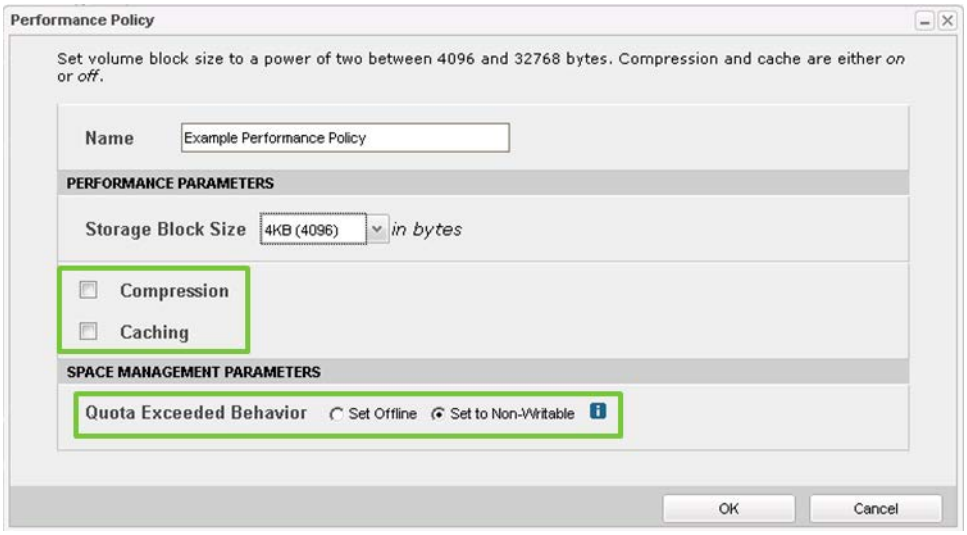

Figure 10: Custom Performance Policy

Creating a new performance policy provides the ability to explicitly set values for both compression and caching.

Native Nimble Storage compression does not impact array performance and should be enabled in most use cases. Veeam compression may affect the duration of backups. The use of Nimble Storage compression may negate any need to enable Veeam compression. This may assist in eliminating any backup proxy CPU utilization associated with Veeam compression.

On Nimble Storage sequential writes are not cached, and backups typically generate a sequential write workload. Disabling caching within the performance policy is not expected to provide any benefit. Additionally, a customized performance policy also allows setting the volume "Quota Exceeded Behavior". Selecting "Set to Non-Writable" is preferred over the "Set Offline" behavior as it will allow restores to be executed in the event that the volume space quota has been exceeded.

On the access control section add the initiator group that contains the iSCSI initiator IQN of the server backing the repository. See "Appendix 1" in this document for additional information about initiator groups.

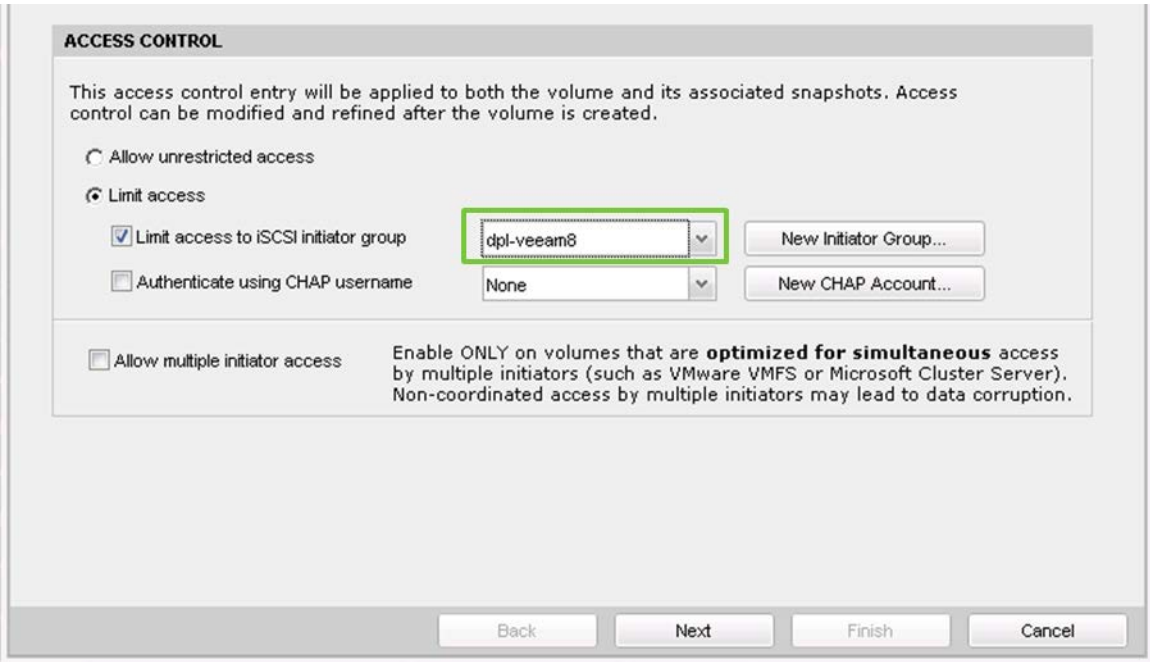

Figure 11: Access Control

The iSCSI initiator group correlating to the Veeam Backup & Replication proxy server backing the repository has been added to the volume. Click the "Next" button to continue.

Backup repository volume size is configured in the "Volume Size" section. Select a volume size that meets or exceeds anticipated usage requirements.

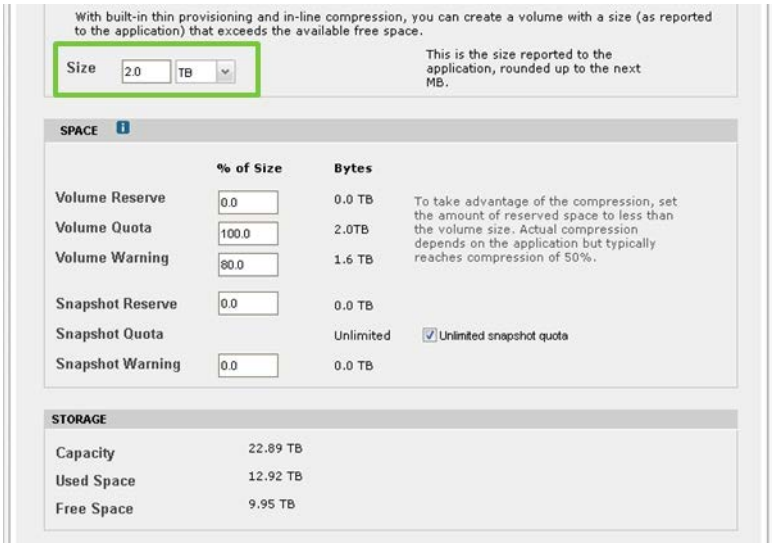

Figure 12: Volume Size

In this example a volume size of 2 TB has been specified. The "Volume Reserve" property has been left at its default value of 0%. Thin provisioning the Nimble Storage volume minimizes the chance of wasted

space in cases where compression or Veeam Backup & Replication deduplication results in the use of less space than was originally allocated.

In the protection section select “None”.

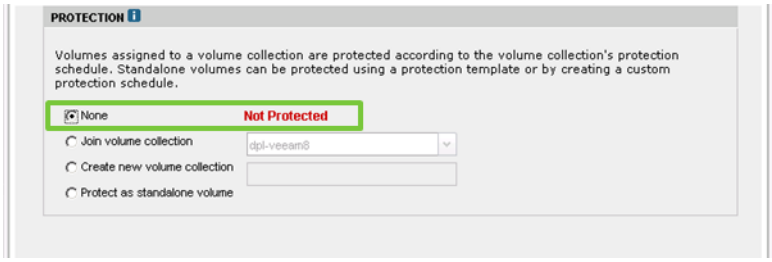

Figure 13: Volume Protection

A volume protection property equal to “None” indicates that the Nimble Protection Manager, a feature that provides native data protection for Nimble Storage array volumes, will not be used on this volume. Click the “Finish” button to complete the volume creation process.

On the server backing the repository launch the Nimble Connection Manager to discover and connect the volume that will be used for the repository. See “Appendix 2” in this document for additional information about the Nimble Connection Manager.

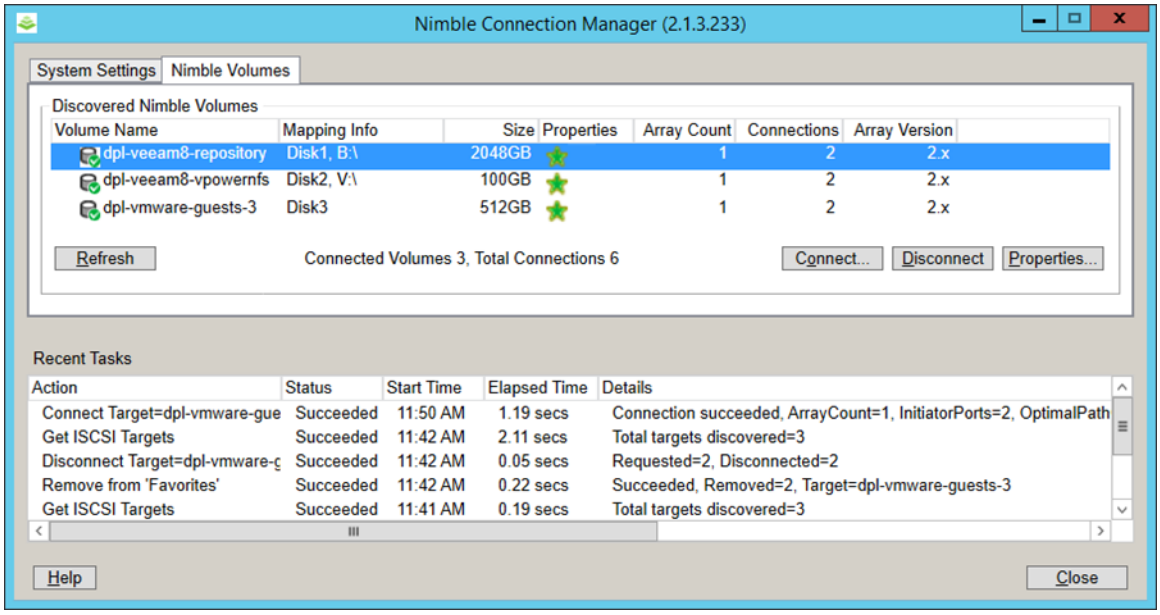

Figure 14: Nimble Volumes

In this example the volume named “dpl-veeam8-repository” has been connected. The connected volume has also been assigned a drive letter, “B:\”, using Windows Server Manager.

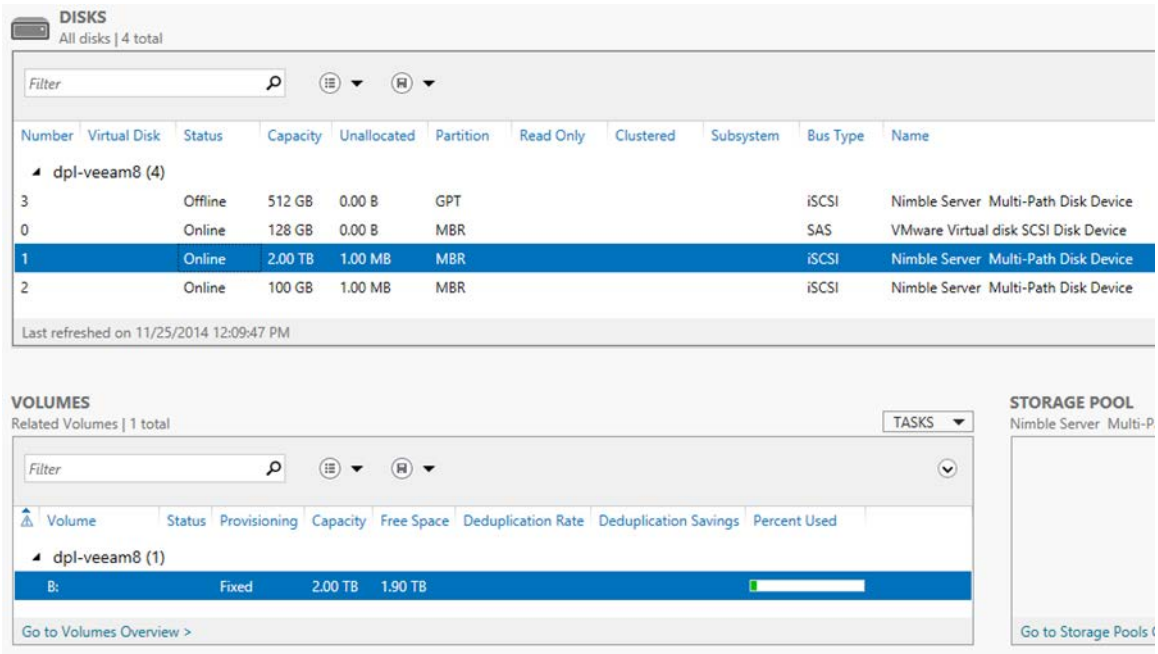

Figure 15: Server Manager – Disks

Note that an additional 100 GB Nimble volume has already been connected for use a vPower NFS root folder. The use of this volume will be detailed later, at the point where it is configured within the backup repository.

Add a Veeam Backup Repository

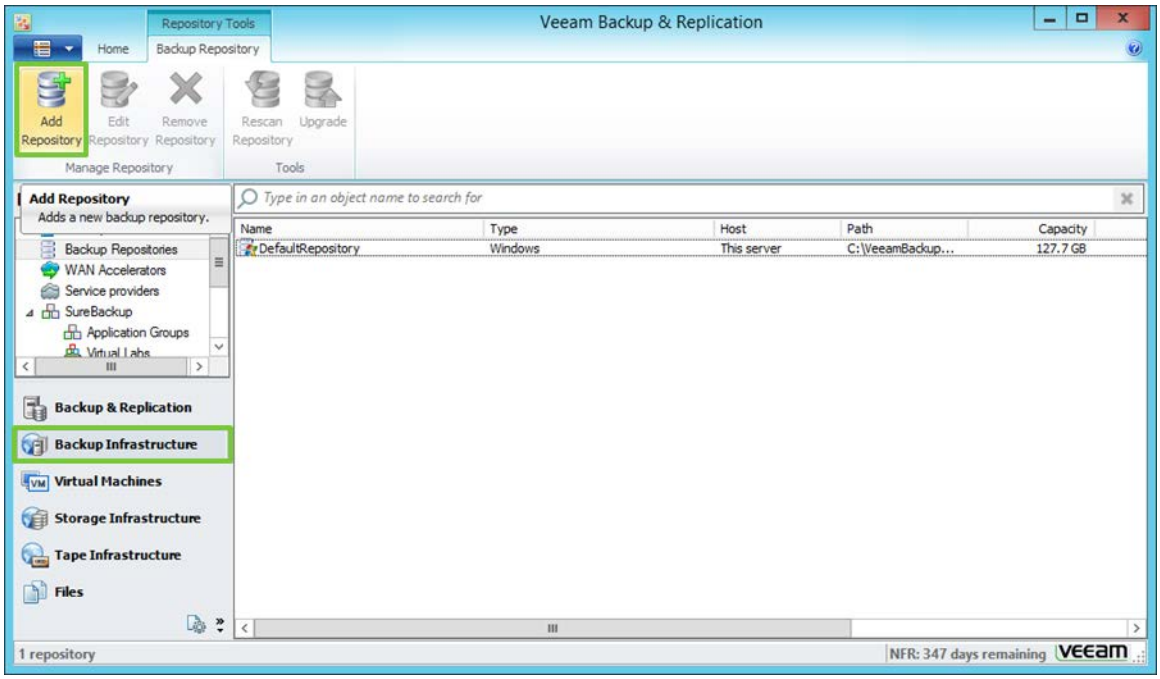

Figure 16: Veeam Backup & Replication

Within the Veeam Backup & Replication user interface select “Backup Infrastructure” and then click on the “Add Repository” icon.

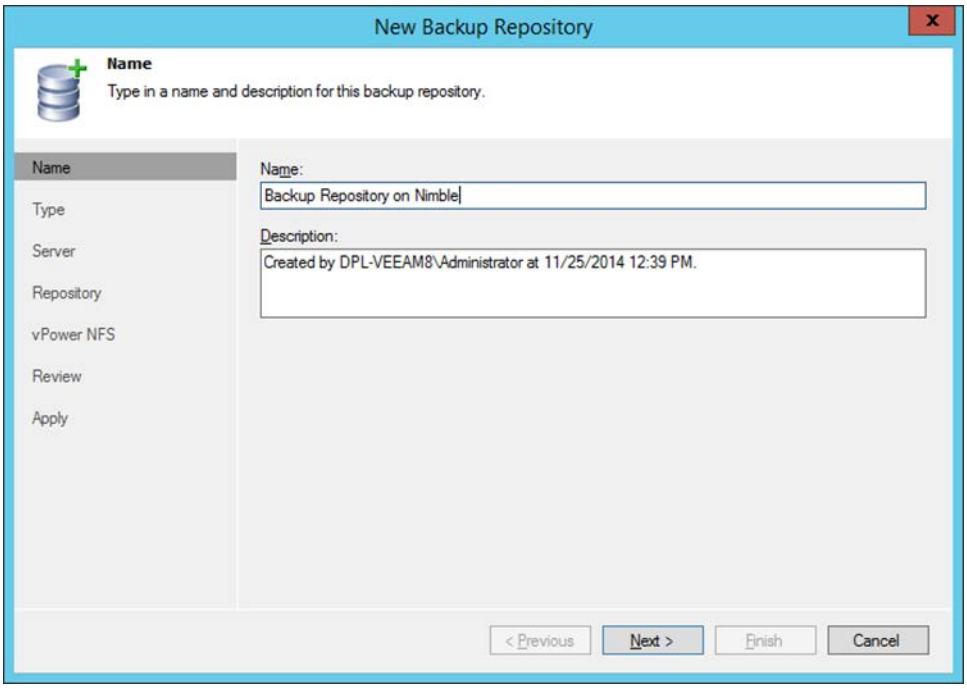

Figure 17: New Backup Repository - Name

Name the new backup repository and then click the “Next” button. In this example the repository has been named “Backup Repository on Nimble”.

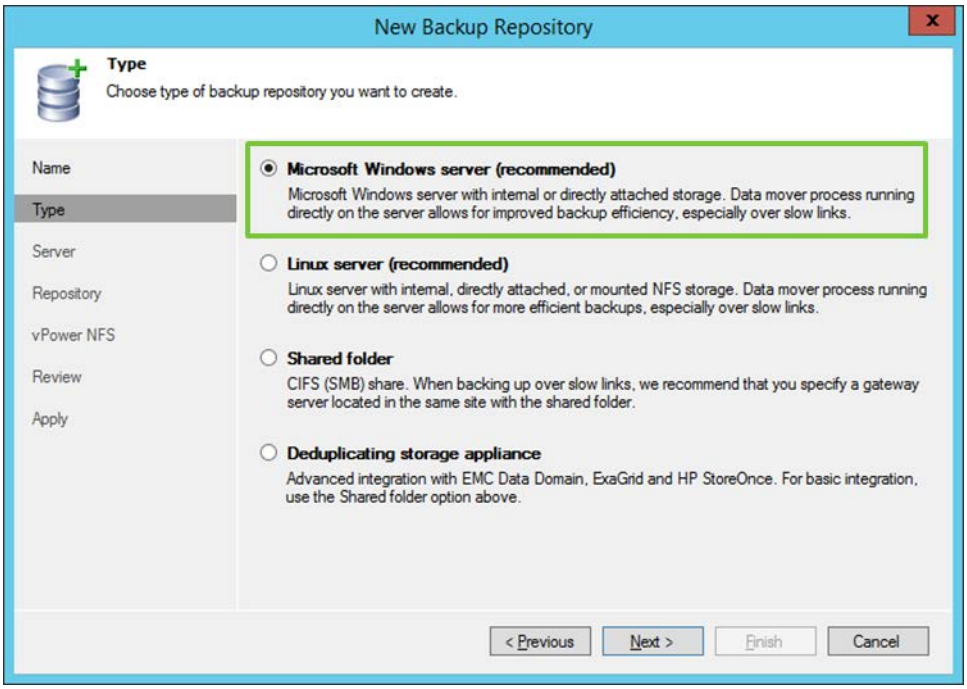

Figure 18: Backup Repository - Type

Select the backup repository type and then click the “Next” button. In this example “Microsoft Windows server” has been selected.

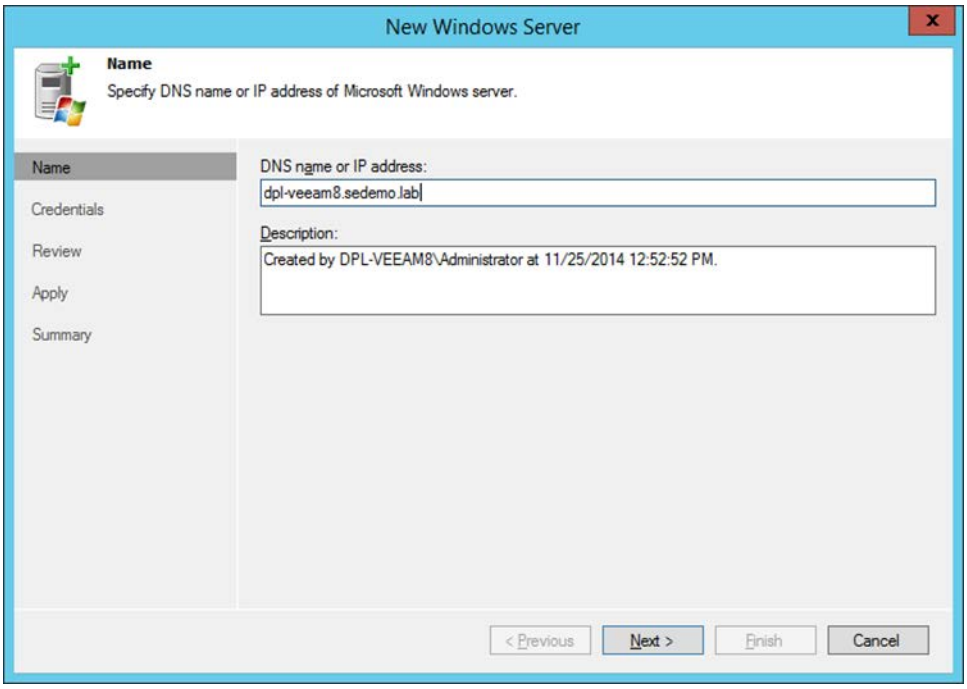

Figure 19: New Windows Server

Specify the DNS name or IP address of the server and then click the “Next” button. In this example a server named, “dpl-veeam8.sedemo.lab” has been specified.

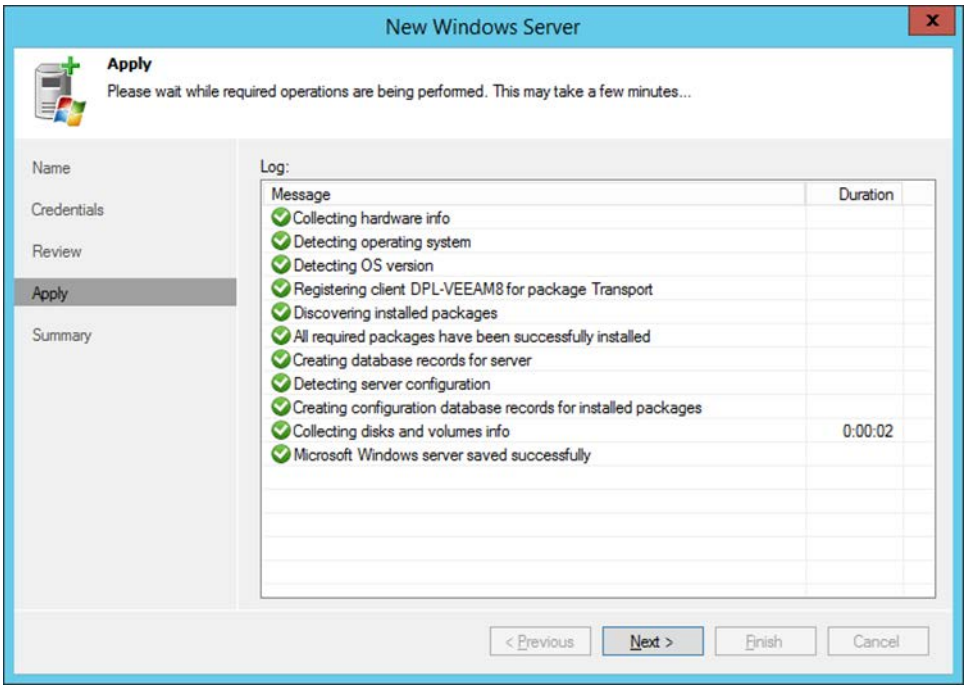

Figure 20: New Windows Server - Apply

Click the “Next” button to continue.

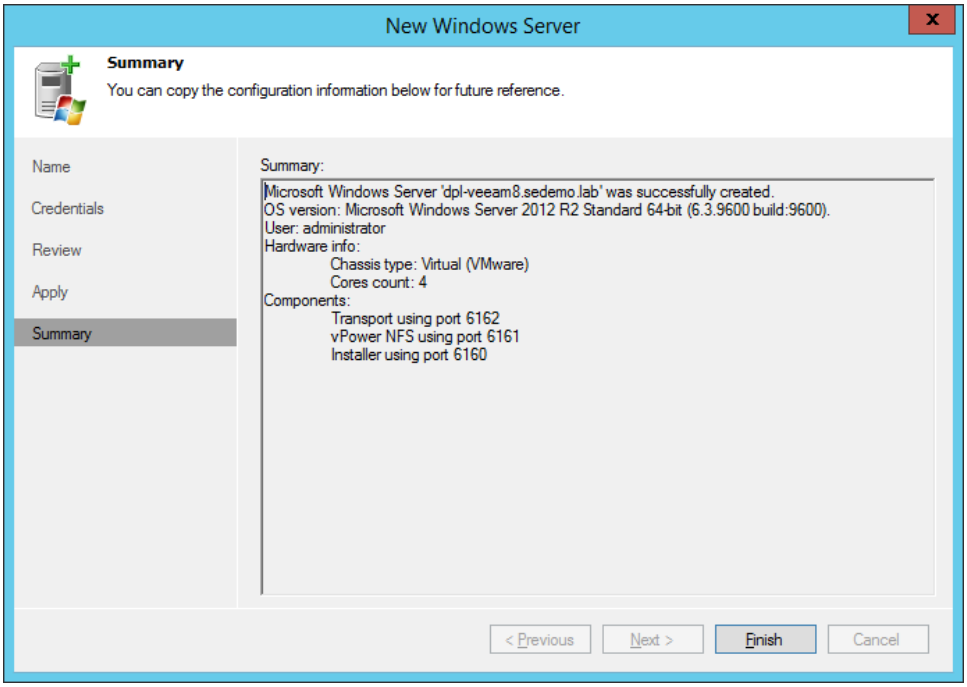

Figure 21: New Windows Server - Summary

Click the “Finish” button to continue.

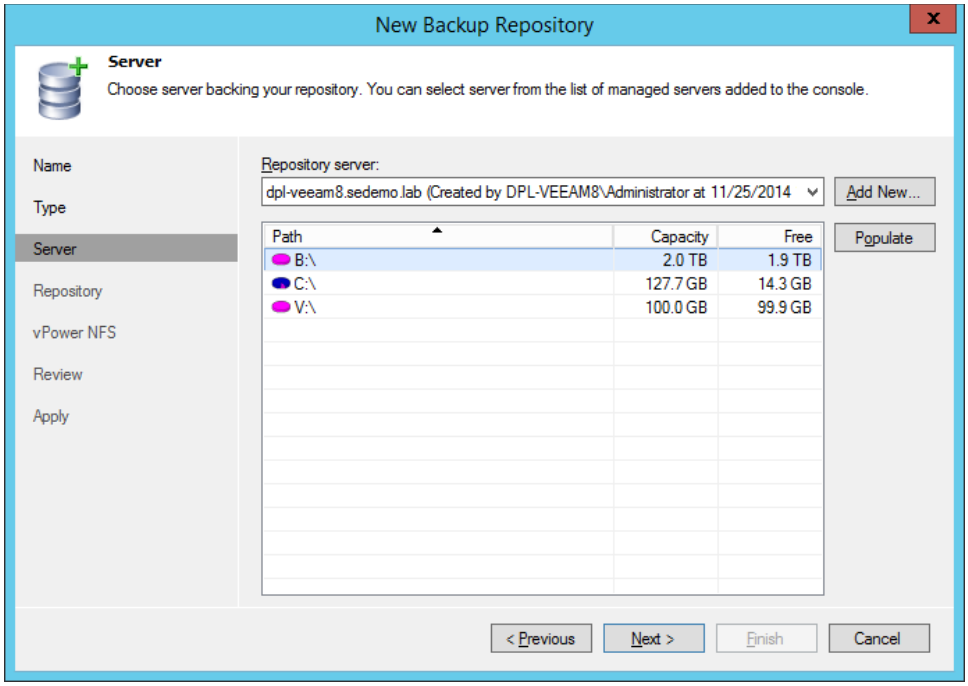

Figure 22: New Backup Repository - Server

At this point in the process the server backing the repository has been configured. Clicking the “Populate” button will display available file system paths on the server. Click the “Next” button to continue.

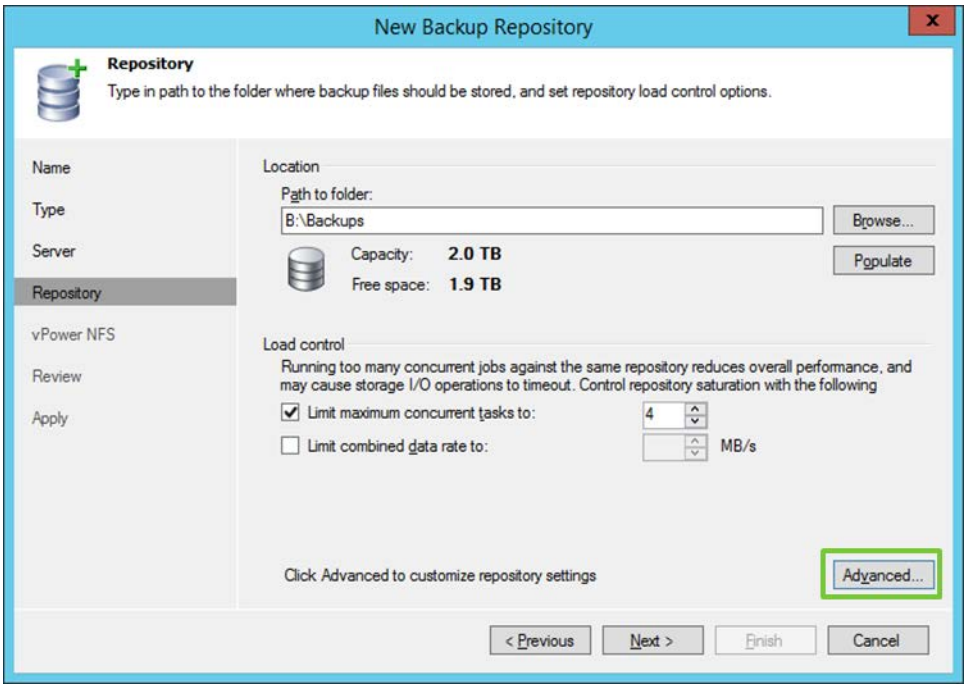

Figure 23: New Backup Repository Path

Make sure the correct “Path to folder” has been specified. In this example the “B:\Backups” path has been set. Clicking the “Populate” button will display the capacity and free space available on the specified path. Click the “Advanced” button to display the “Storage Compatibility Settings” dialog window.

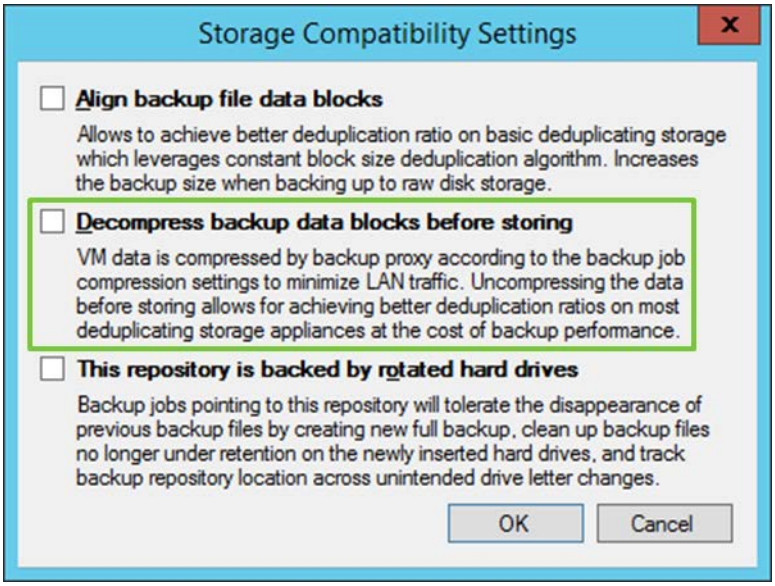

Figure 24: Storage Compatibility Settings

Consider enabling the “Decompress backup data blocks before storing” if the Nimble Storage volume used for the repository is using a performance policy that includes compression. Click the “OK” button and then click the “Next” button on the “New Backup Repository Path” dialog window to continue.

Getting Backups offsite with Veeam and Nimble Storage

Using Nimble Storage as a backup repository for Veeam Backup provides the best possible performance of Veeam backup, restore, and backup verification jobs. However, a comprehensive data protection strategy includes the creation of additional copies of backups that can be retained offsite. Nimble Storage in conjunction with Veeam Backup provides several options to retain backups in additional locations or on other media types. Examples of these include:

- Nimble Volume Collection Replication – Protect Veeam Backup repositories by replicating them to a downstream Nimble Storage array. Nimble volume collection replication provides efficient replication by only transferring changed blocks.
- Veeam Backup copy jobs with WAN Acceleration – Protect Veeam Backups by copying them to another Nimble Storage array through WAN accelerators to minimize replication network bandwidth utilization.
- Veeam tape copy jobs – Copy Veeam backups to tape for offsite archiving.
- Veeam Cloud Connect – Use a Veeam Cloud Connect partner to copy backups to offsite hosted backup repositories.

vPower NFS on Nimble Storage

Because the repository is backed by a Windows server, it can also be configured to function as a vPower NFS server. This provides ESXi hosts with transparent access to backed up VM images stored on the repository, and enables valuable features such as “SureBackup” and “Instant VM Recovery”.

Create a second Nimble Storage volume for use as the vPower NFS root folder. Add the initiator group of the server backing the new repository to the access tab of the volume. Use the Nimble Connection Manager to connect the volume to the host, and then assign a drive letter using the Windows Server Manager.

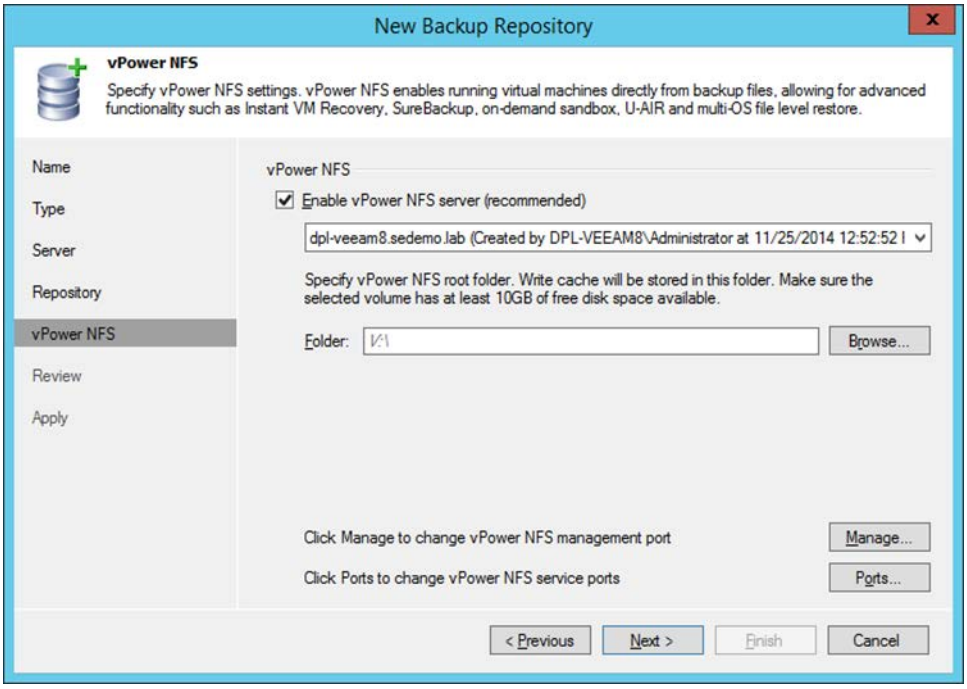

Figure 25: New Backup Repository – vPower NFS

Ensure vPower NFS is enabled. In this example the vPower NFS root folder has been specified as file system path “V:\”.

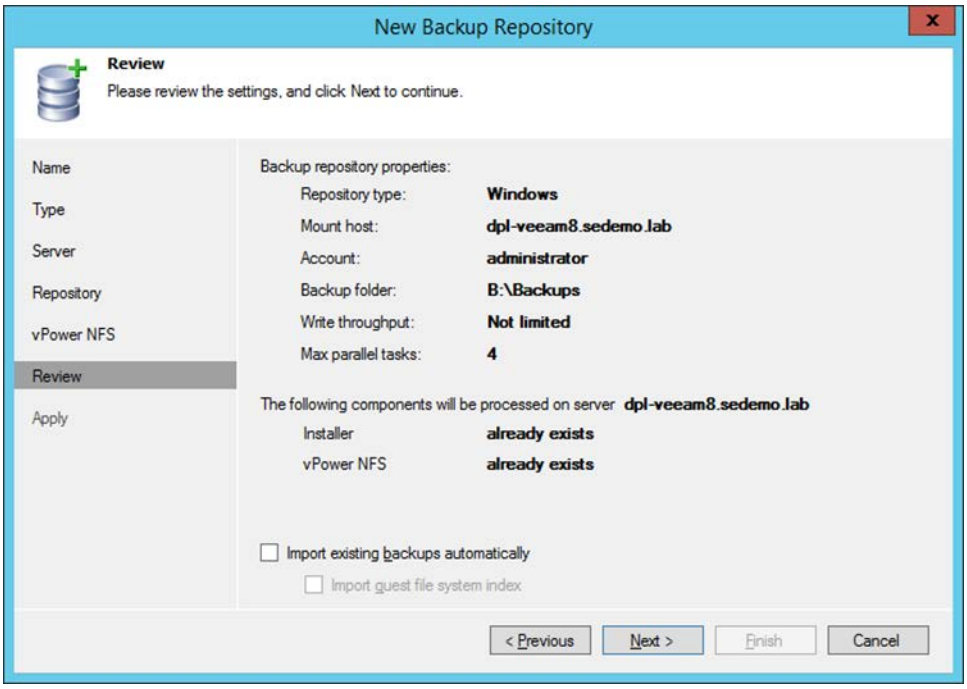

Figure 26: New Backup Repository – Review

Review the settings and then click the “Next” button to continue.

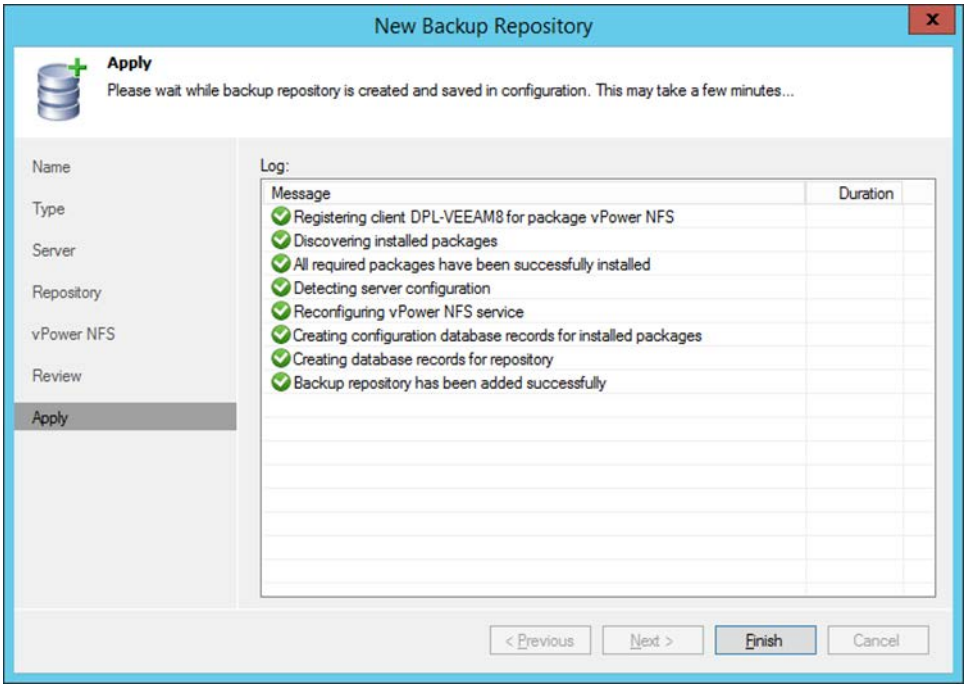

Figure 27: New Backup Repository – Apply

Click the “Finish” button. At this point the new backup repository has been configured using a Nimble Storage volume. In addition, a second Nimble Storage volume has been configured for use as a vPower NFS root folder. The backup repository is now available for selection from within a backup job.

Virtual Lab Datastore on Nimble Storage

Veeam Backup & Replication “SureBackup” recovery verification provides an automated method to verify recovery of backed up VMs. One component of this testing methodology is a virtual lab datastore. This section takes a look at using a Nimble Storage volume as a virtual lab datastore for use with “SureBackup”.

Create a Nimble Volume for use as a Datastore

From the Nimble Storage user interface select “Manage > Volumes” and then click the “New Volume” button.

Figure 28: New Volume

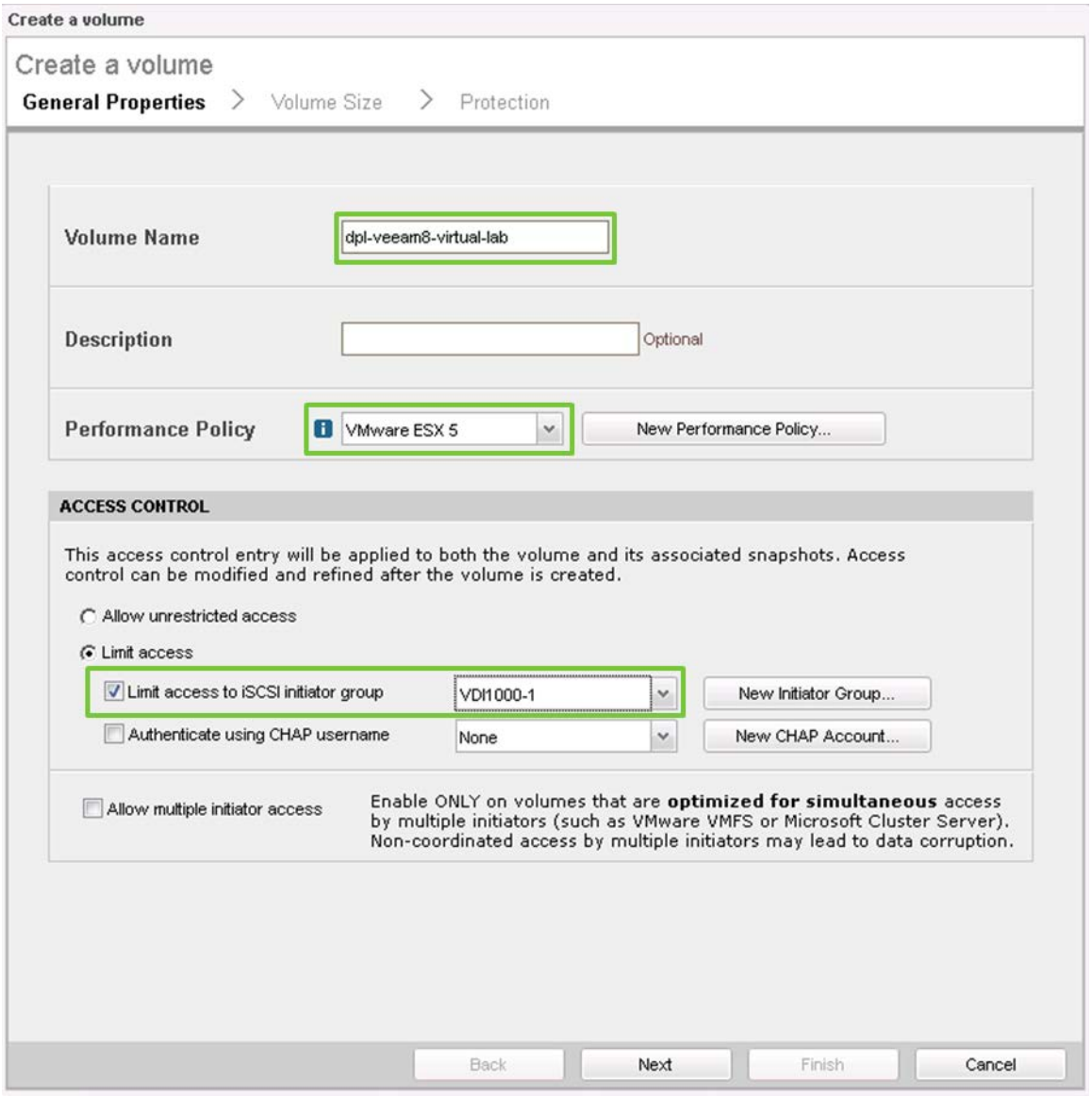

Figure 29: New Volume – General Properties

Name the new volume, and select the appropriate VMware ESX performance policy. Configure the access control parameters to allow access to the ESXi hosts that will need to use the virtual lab. Click the "Next" button to continue.

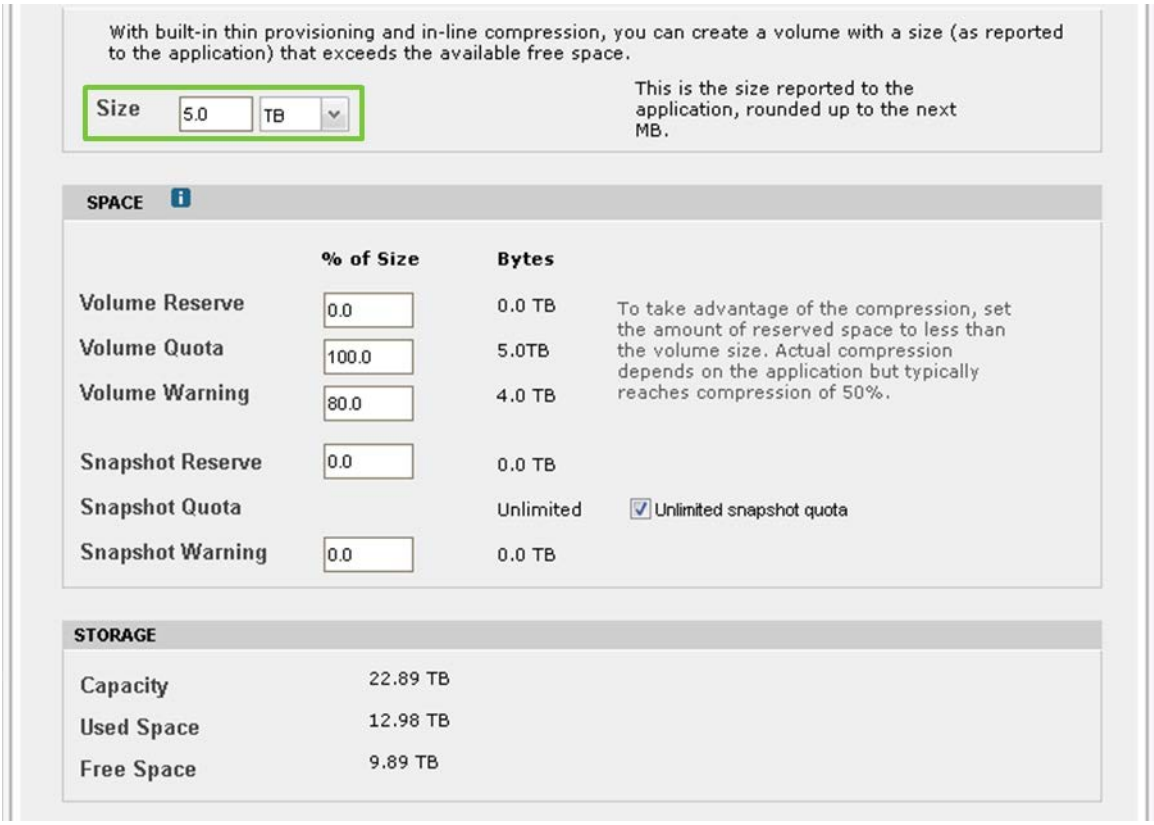

Figure 30: Volume Size

Virtual lab volume size is configured in the “Volume Size” section. Select a volume size that meets or exceeds anticipated usage requirements. In this example a volume size of 5 TB has been specified. The “Volume Reserve” property has been left at its default value of 0%. Thin provisioning the Nimble Storage volume minimizes the chance of wasted space.

In the protection section select “None”.

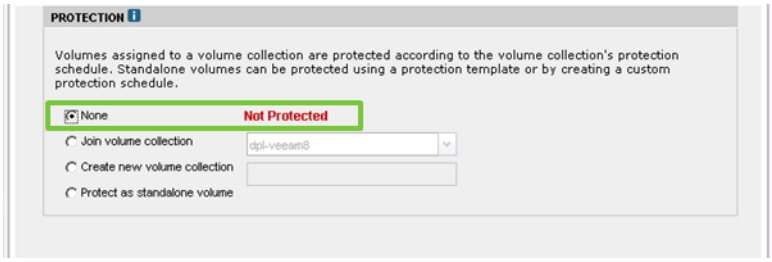

Figure 31: Volume Protection

Click the “Finish” button to complete the volume creation process.

Within VMware vSphere, rescan for new storage devices and then add storage. Add the “Disk/LUN” that correlates to the new volume just created. Format the new datastore.

Create a Veeam Virtual Lab

Within the Veeam Backup & Replication user interface, click “Backup Infrastructure”, expand the “SureBackup” tree, and the right click “Virtual Labs”.

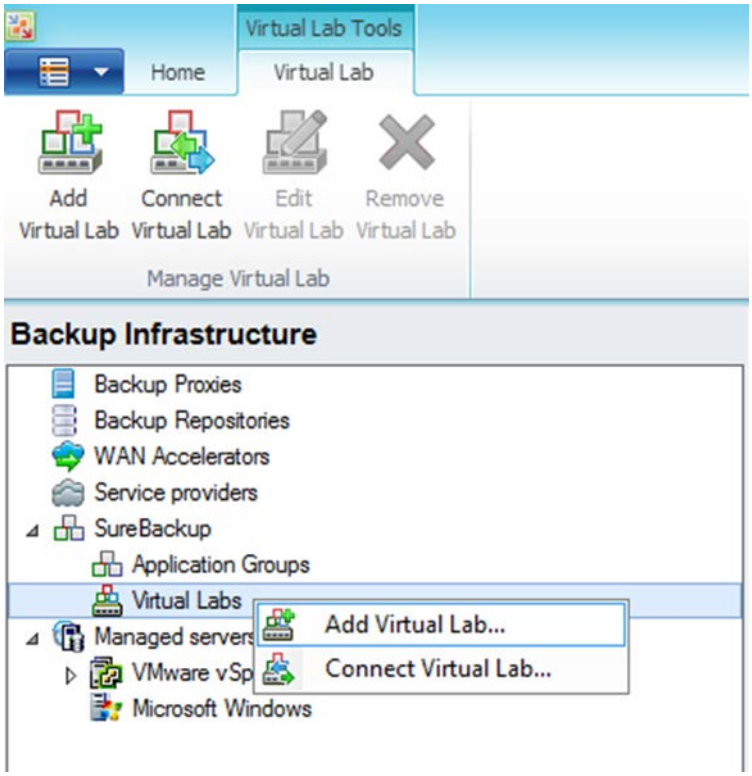

Figure 32: Add Virtual Lab

Click the “Add Virtual Lab” menu item to continue. Alternatively, clicking the “Add Virtual Lab” icon will also facilitate creation of a new virtual lab.

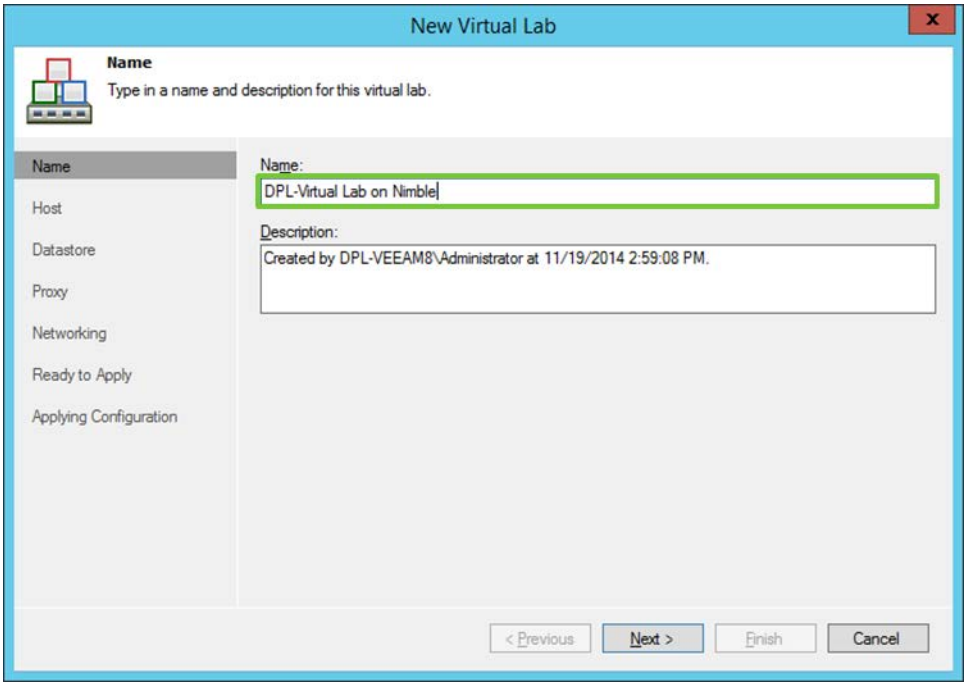

Figure 33: New Virtual Lab - Name

Name the new virtual lab and then click “Next” to continue. In this example the new virtual lab has been named, “DPL-Virtual Lab on Nimble”.

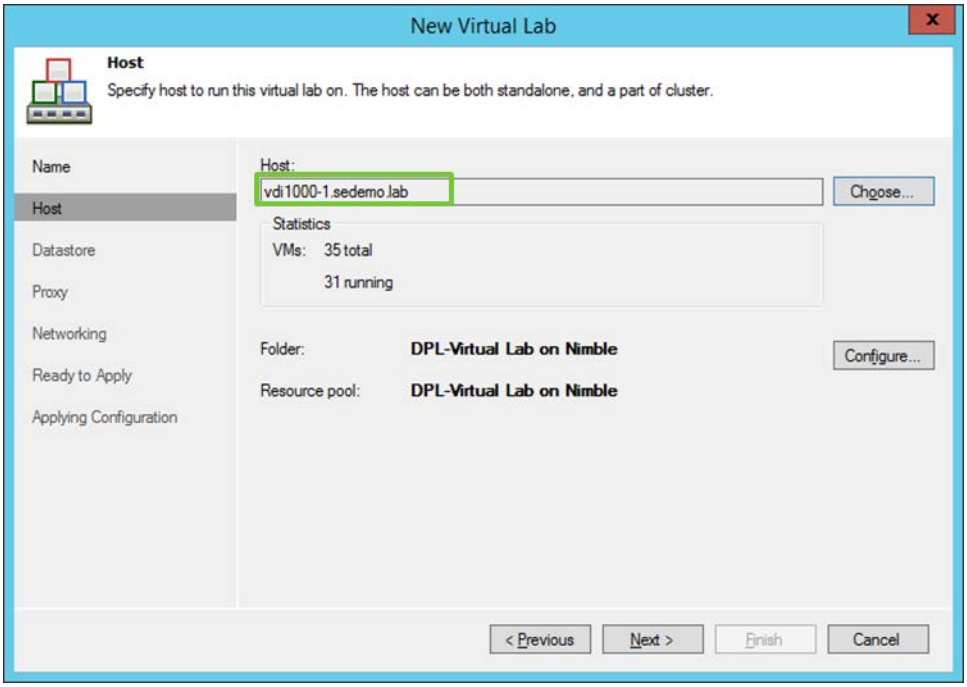

Figure 34: New Virtual Lab – Host

Choose the ESXi host or cluster that will run the virtual lab. Click the “Next” button to continue.

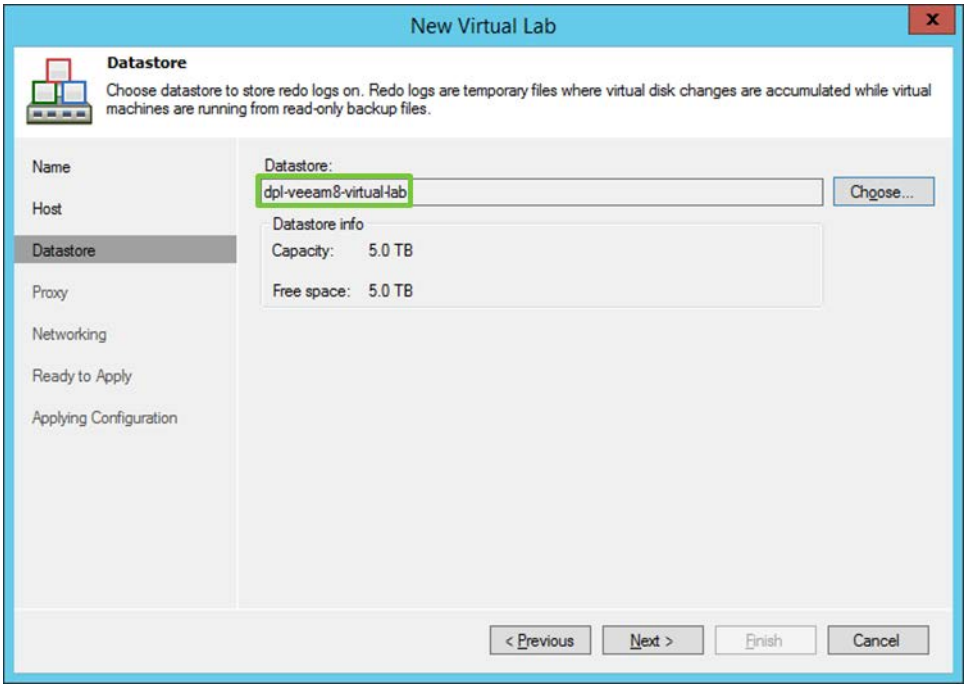

Figure 35: New Virtual Lab - Datastore

Select the datastore that will be used for the virtual lab. This is the volume/datastore created earlier in this section. In this example the “dpl-veeam8-virtual-lab” datastore has been selected. Click the “Next” button to continue.

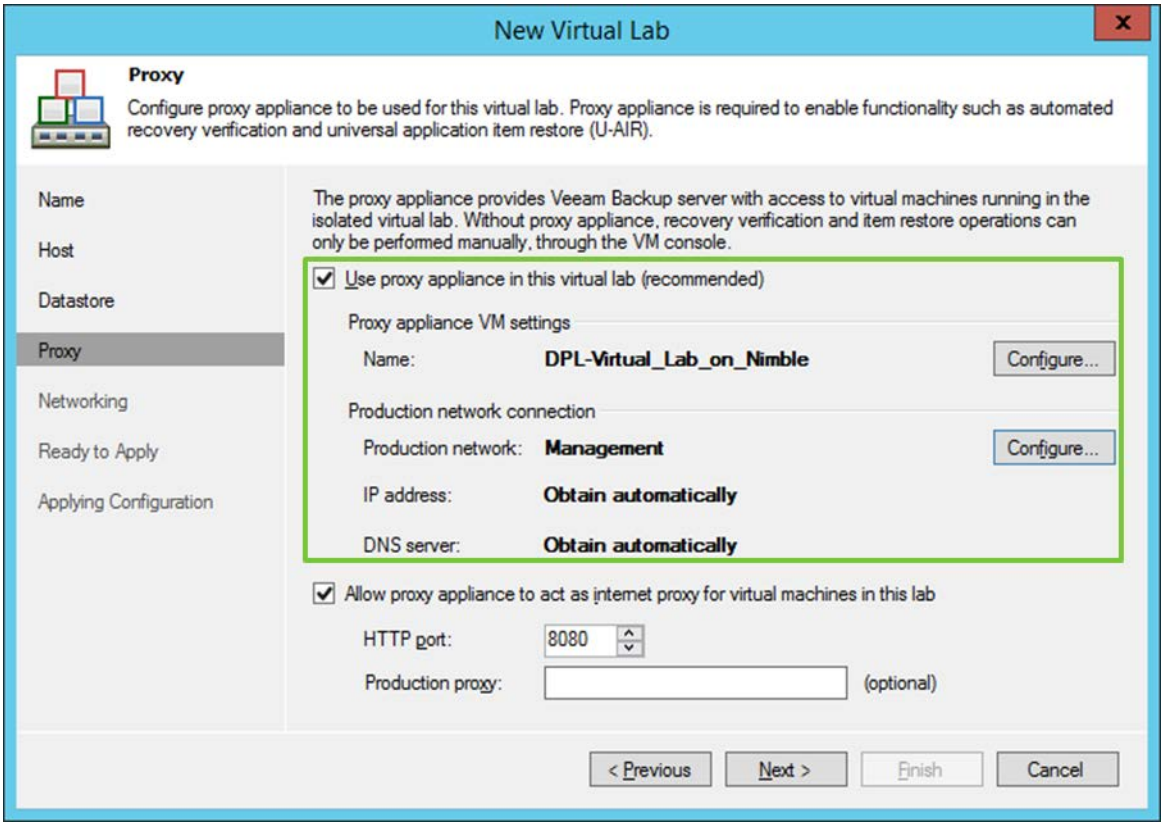

Figure 36: New Virtual Lab – Proxy

Configure the proxy appliance for the new virtual lab. Click the “Next” button to continue.

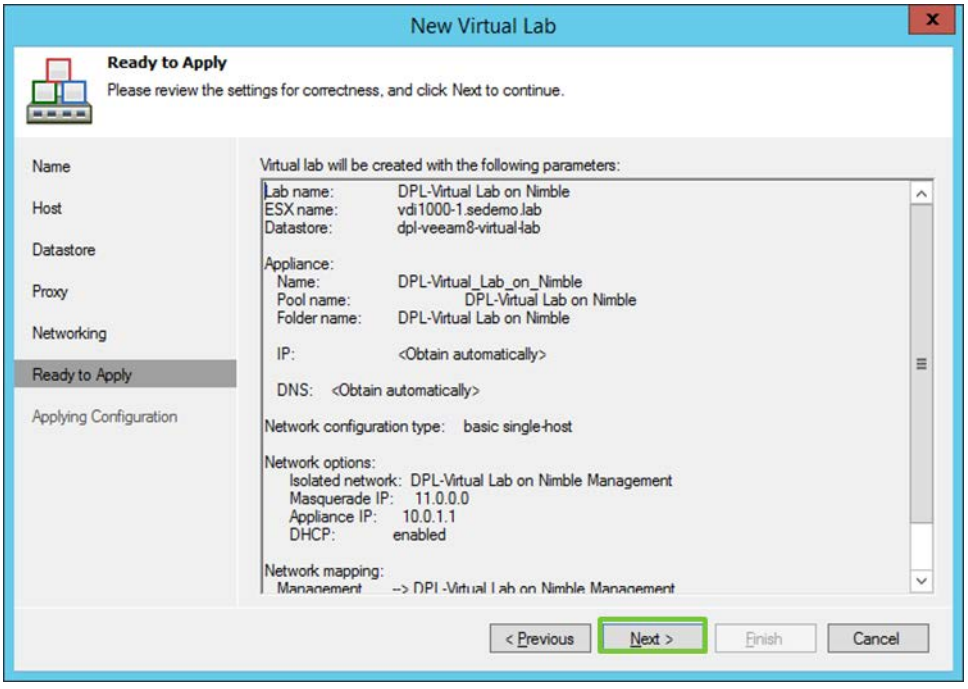

Figure 37: New Virtual Lab – Apply

Review the settings and then click the “Next” button.

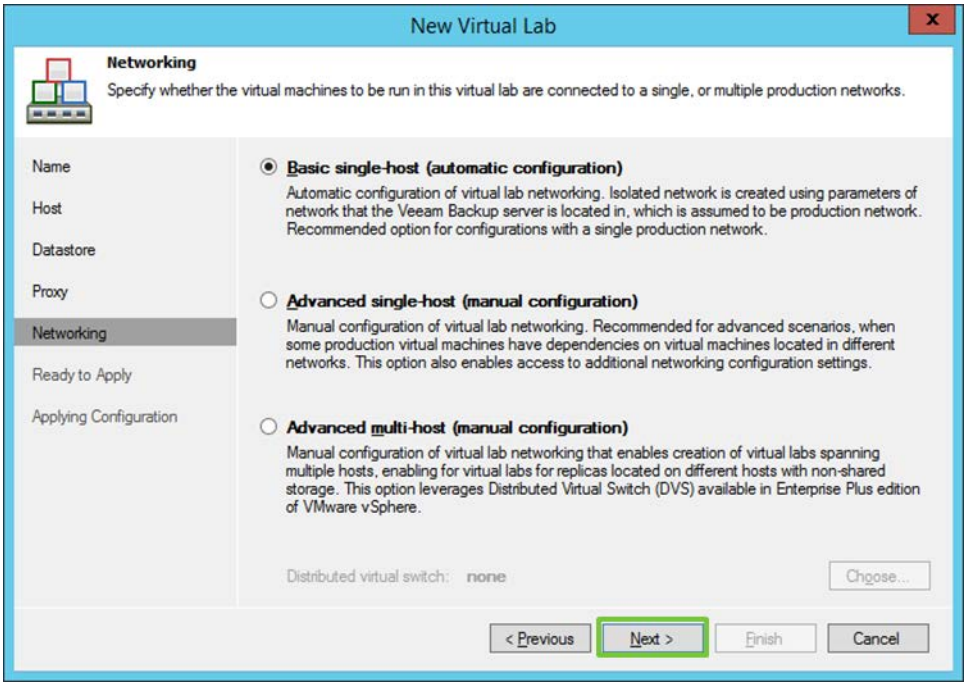

Figure 38: New Virtual Lab – Networking

Select the desired network settings for the virtual lab and then click the “Next” button.

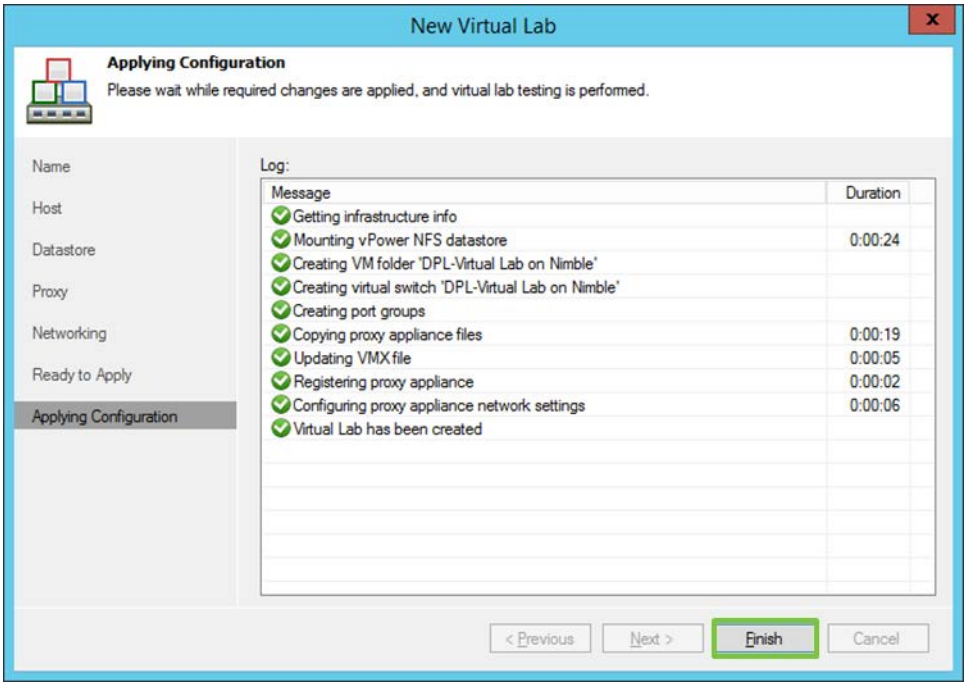

Figure 39: New Virtual Lab – Apply Configuration

Click the “Finish” button to complete creation on the new virtual lab.

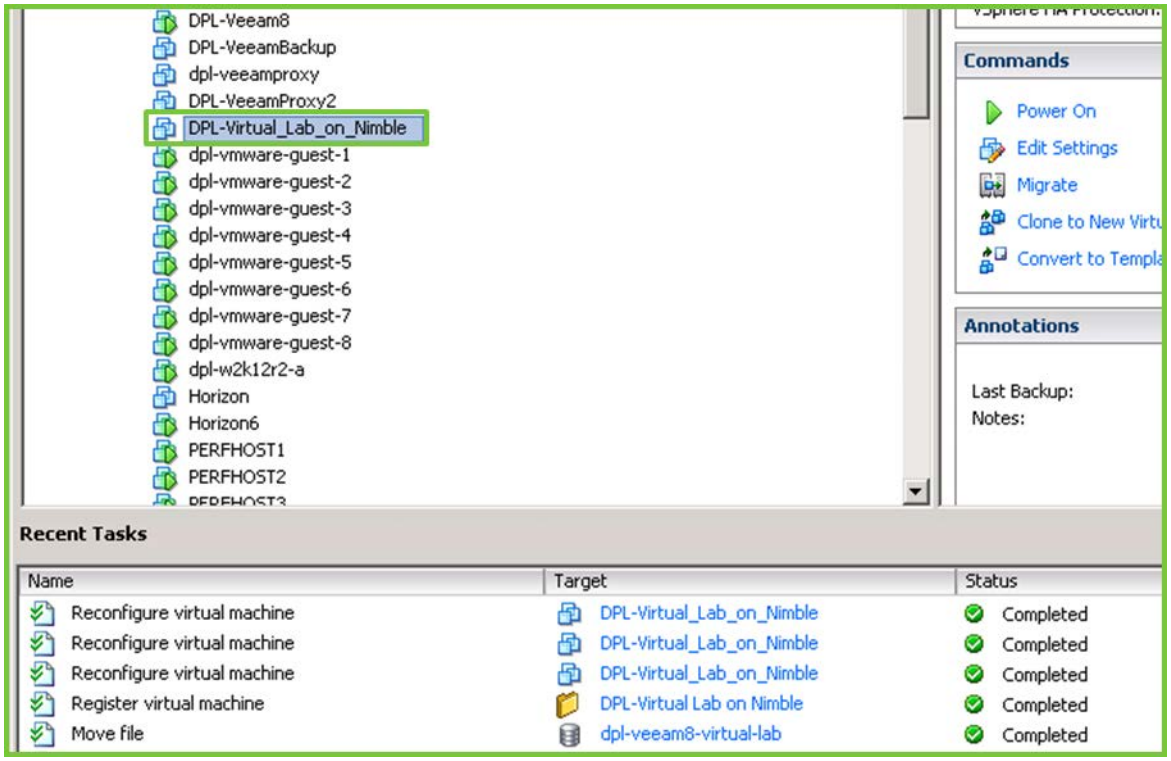

Figure 40: Virtual Lab as vSphere Inventory

At this stage the virtual lab will appear in vSphere as inventory. The virtual lab is now ready to use. An “Application Group” and “SureBackup” job are required to use the virtual lab.

Summary

When protecting VMware datastores hosted on a Nimble Storage array, Veeam Backup & Replication provides a robust feature set enabling a variety of data protection strategies. This includes the ability to leverage the most efficient transport mode based on the configuration of the backup infrastructure.

High performance Nimble Storage arrays can be deployed as part of a Veeam Backup & Replication infrastructure. Backup repositories, vPower NFS root folders, and virtual labs hosted on Nimble volumes assist in creating a fast and reliable data protection solution.

Appendix 1 – Initiator Group

Initiator groups provide a convenient way to limit volume access to only the specific iSCSI initiators that are members of the group.

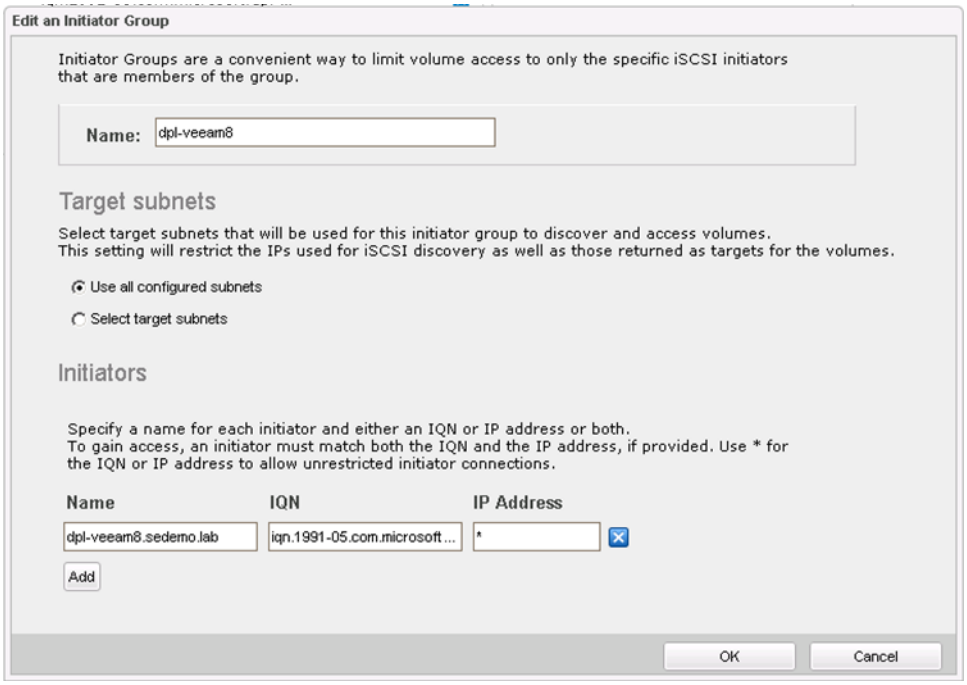

Figure 41: Edit an Initiator Group

The example used here is for a Veeam Backup & Replication proxy server that also backs a repository. The name of the host server and the IQN of the host server have been added to the initiator group.

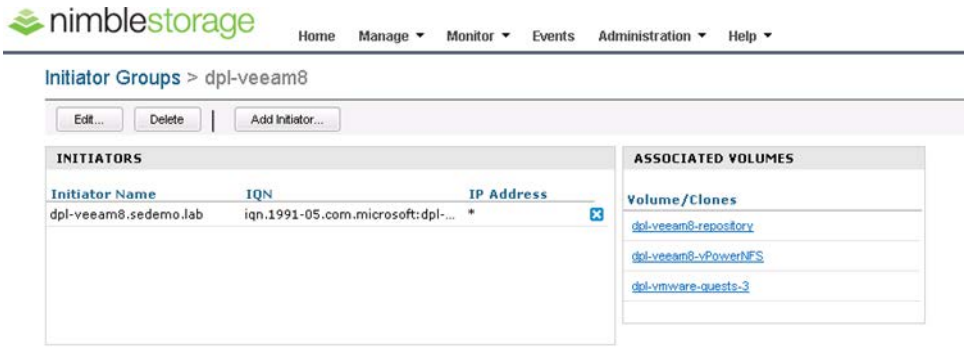

Figure 42: Initiator Group

When viewing an initiator group a list of associated volumes is displayed. In this example a Veeam Backup & Replication host has been granted access to three different volumes.

Appendix 2 – Nimble Connection Manager

The Nimble Connection Manager is designed to simplify making and maintaining iSCSI connections between a Windows host and Nimble Storage array volumes. The Nimble Connection Manager is available after successful installation of the Nimble Windows Toolkit, which can be downloaded from the Nimble Storage InfoSight portal.

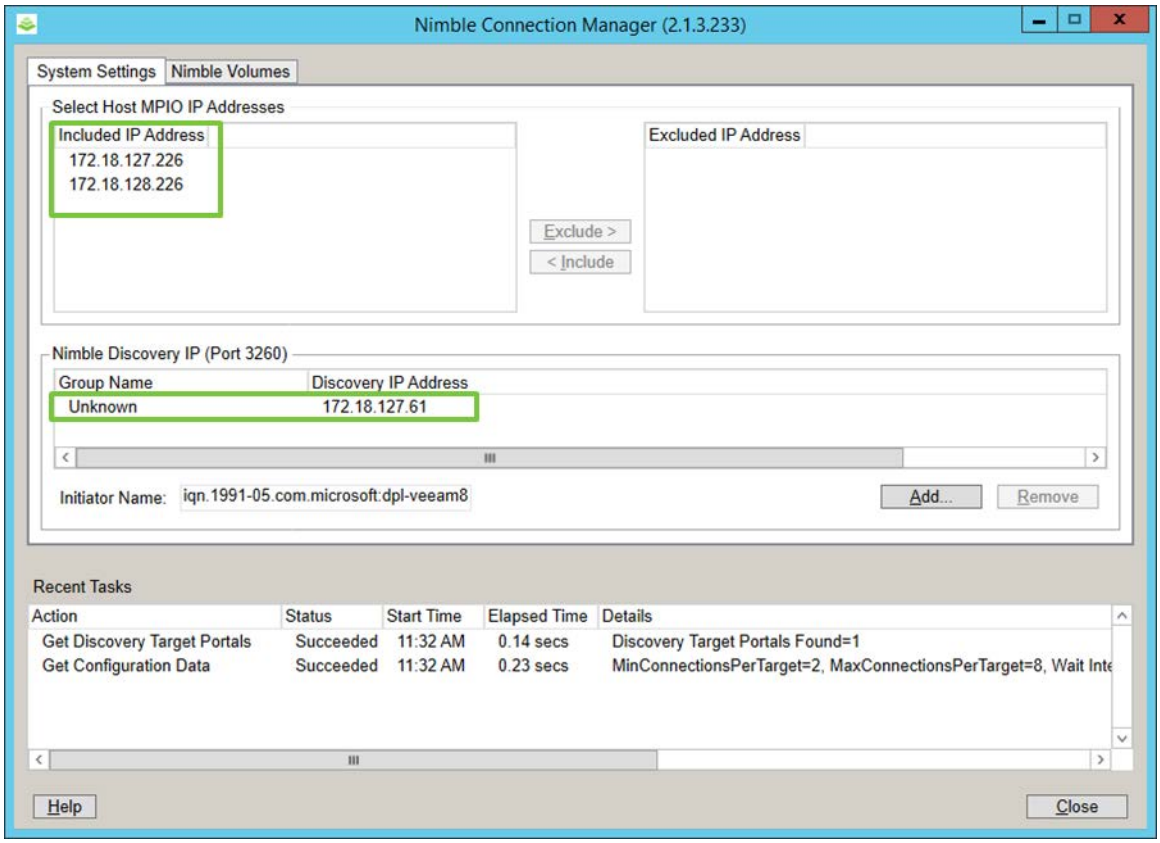

Figure 43: Nimble Connection Manager - System Settings

The “System Settings” tab on the Nimble Connection Manager is configured to discover volumes on one or more Nimble Storage arrays. The Nimble discovery IP address of each array is added by clicking the “Add” button.

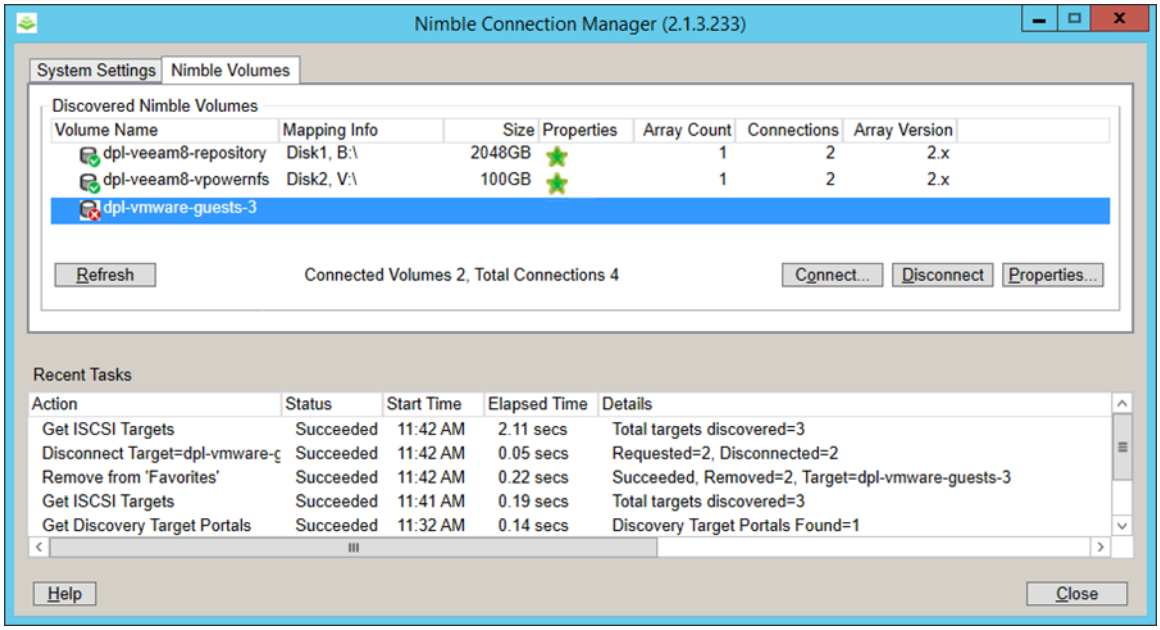

Figure 44: Nimble Connection Manager - Nimble Volumes

New volumes are discovered by clicking the “Refresh” button. Discovered volumes can be connected by first clicking the newly discovered volume, and then clicking the “Connect” button. At connection time, a “Connect to Target” dialog window will provide the option to automatically connect the volume on startup.

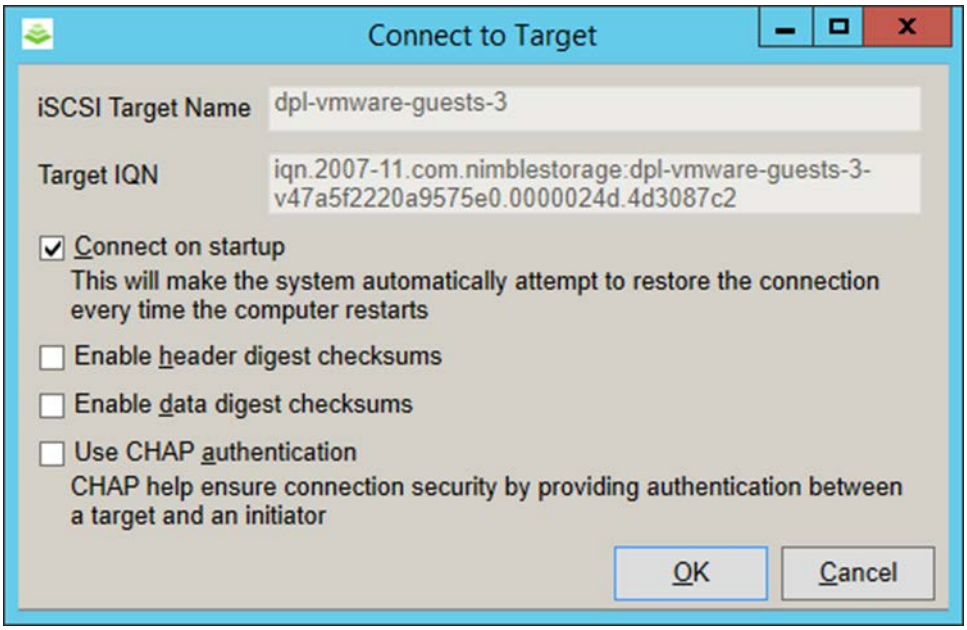

Figure 45: Connect to Target

Accepting the default “Connect on startup” parameter will cause the system to automatically attempt to restore the connection every time the computer restarts.

Appendix 3 - NPM with Veeam Backup & Replication

NPM (Nimble Protection Manager) is included with Nimble Storage arrays and provides the ability to create application consistent snapshot backups using VMware vCenter synchronization as well as Microsoft VSS synchronization. The co-mingling of NPM snapshots with Veeam Backup & Replication backups is possible. From a high level perspective NPM & Veeam both deliver tangible benefits.

- Veeam Backup & Replication for VMware:
  - Enables granular restore
  - Enables automated tape based copies of backups
  - Enables the use of VMware Instant Recovery
  - Enables “SureBackup” and the use of virtual labs
- Nimble Protection Manager vCenter synchronized snapshots:
  - Enables aggressive data protection with frequent snapshots
  - Enables the use of efficient Nimble replication

On the surface the solutions appear to be complimentary, and when scheduling is properly coordinated NPM and Veeam Backup & Replication can be used together to fulfill business objectives. However there are known issues that may occur when both data protection solutions attempt to protect the same guest at approximately the same time.

Avoid Overlapping Usage

When both data protection solutions issue simultaneous or near-simultaneous requests for vCenter snapshots of the same guest, errors may occur. These errors will typically manifest themselves as failed snapshots. On the Nimble side of the equation users may experience messages such as, “failed to create vCenter snapshot”. Veeam Backup & Replication may report errors that include, “failed to prepare guest for backup”. Windows application events on the guest may indicate that VSS errors, or VMware tools errors have occurred. In all known cases these errors can be avoided by assuring that requests for vCenter snapshots do not overlap.

Another challenge overlapping schedules can create occurs in cases where a Veeam Backup & Replication temporary snapshot exists and NPM requests a snapshot of the same guest. In effect, the Veeam snapshot may be captured within the NPM snapshot.

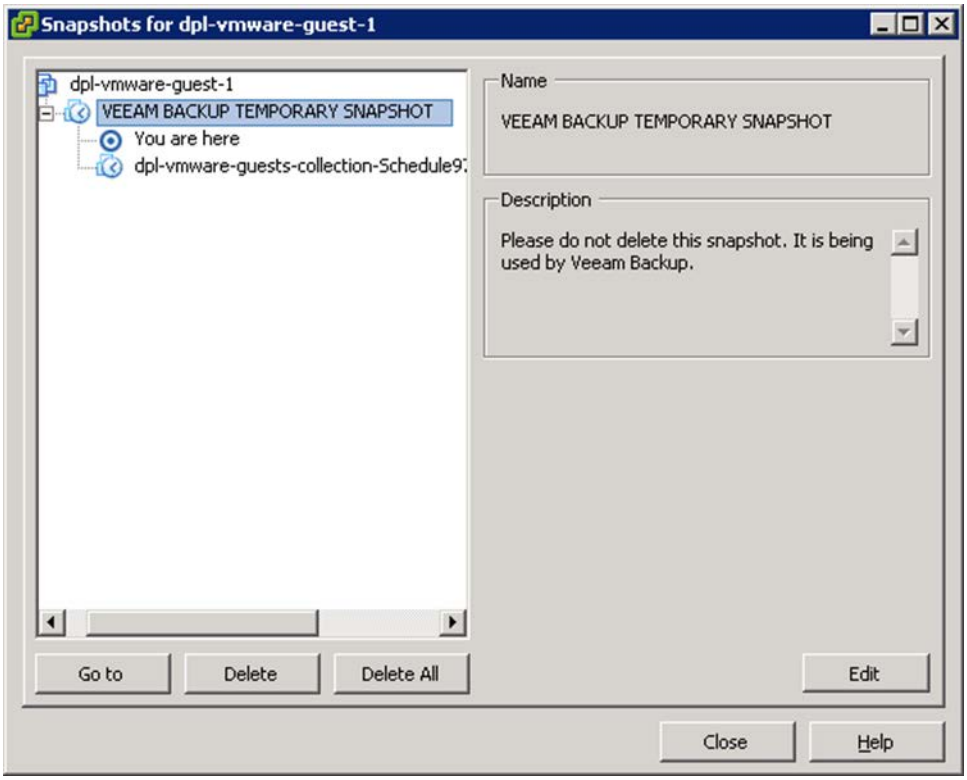

Figure 46: Overlapping vCenter Snapshots

In this scenario both backups may complete successfully. However, if the NPM snapshot is recovered it may contain an orphaned Veeam Backup & Replication snapshot. Orphaned snapshots need to be removed manually, creating additional administrative overhead.

Another side effect that may occur when performing backups with both NPM and Veeam Backup & Replication occurs when a Nimble snapshot is recovered that predates the most recent Veeam backup. In this scenario the next Veeam backup may request changed blocks referencing a point in time that doesn't yet exist on the recovered virtual disks. The backup will complete but it may post a warning message indicating that CBT (Changed Block Tracking) cannot be used.

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