



This document has been archived and will no longer be maintained or updated. For more information go to the [Storage Solutions Technical Documents page on Dell TechCenter](#) or contact support.

Virtual Machine Protection with Dell EqualLogic Virtual Storage Manager v3.5

Abstract

This Technical Report focuses on the usage of the Dell™ EqualLogic™ Virtual Storage Manager v3.5 to coordinate VMware™ aware snapshots and PS Series SAN snapshots to provide an additional layer of data protection and recovery.

Copyright © 2012 Dell Inc. All Rights Reserved.

EqualLogic is a registered trademark of Dell Inc.

Dell is a trademark of Dell Inc.

All trademarks and registered trademarks mentioned herein are the property of their respective owners.

Information in this document is subject to change without notice.

Dell, Inc. will not be held liable for technical or editorial errors or omissions contained herein. The information in this document is subject to change.

Reproduction in any manner whatsoever without the written permission of Dell is strictly prohibited.

Authored by William Urban

January 2013

Preface

PS Series arrays optimize resources by automating performance and network load balancing. Additionally, PS Series arrays offer all-inclusive array management software, host software, and free firmware updates.

Audience

The information in this guide is intended for VMware vCenter administrators and PS Series SAN administrators.

Related Documentation

For detailed information about PS Series arrays, groups, volumes, array software, and host software, log in to the [Documentation page](#) at the customer support site.

Dell Online Services

You can learn about Dell products and services using this procedure:

1. Visit <http://www.dell.com> or the URL specified in any Dell product information.
2. Use the locale menu or click on the link that specifies your country or region.

Dell EqualLogic Storage Solutions

To learn more about Dell EqualLogic products and new releases being planned, visit the Dell EqualLogic TechCenter site: <http://delltechcenter.com/page/EqualLogic>. Here you can also find articles, demos, online discussions, technical documentation, and more details about the benefits of our product family.

Table of Contents

Revision Information	vi
Executive Summary	1
Introduction.....	1
Installation and Configuration.....	2
Launching VSM for Local Protection.....	2
Protection with Smart Copies	5
Scalability with Folders and Datastores.....	13
Automating Protection with Schedules	14
Managing Smart Copies and Operations	22
Recovering with Smartcopies	26
Creating Smart Clones.....	33
Advanced Cloning - Selective Data Recovery.....	40
Multilayerd Data Protection Approach and Data Placement.....	49
Summary.....	50
Technical Support and Customer Service	51

Revision Information

The following table describes the release history of this Technical Report.

Report	Date	Document Revision
1.0	November 2012	Initial Release for VSM v3.5

The following table shows the software and firmware used for the preparation of this Technical Report.

Vendor	Model	Software Revision
Dell	PS Series SAN	5.2 or higher, 6.x
VMware	vCenter/ESX	4.1, 5.0, 5.1
Dell	Virtual Storage Manager	v3.5

The following table lists the documents referred to in this Technical Report. All PS Series Technical Reports are available on the Customer Support site at: support.dell.com

Vendor	Document Title
Dell	TR1067 EqualLogic Virtual Storage Manager: Installation Considerations and Datastore Manager
Dell	TR1063 Dell EqualLogic PS Series Template Volumes and Thin Clones: How and When to Use them
Dell	TR1084 EqualLogic PS Series Architecture: Snapshot Space Borrowing Overview.
VMware	KB 1015180 Understanding virtual machine snapshots in VMware ESXi and ESX

EXECUTIVE SUMMARY

This technical report is aimed at VMware™ and Dell™ EqualLogic™ PS Series SAN administrators to guide them on the use of the Dell Virtual Storage Manager v3.5 to create and coordinate hypervisor-aware snapshots for data protection and recovery. Throughout this technical report, examples will be given for setting up and configuring snapshots and schedules as well as instructions on data recovery and other advanced options.

INTRODUCTION

In today's datacenter, customers are utilizing VMware™ virtualization solutions and Dell™ EqualLogic™ PS Series SAN storage to consolidate servers and storage for better utilization, efficiency and ease of management. The encapsulation of the virtual machine (VM) into a set of files not only increases the flexibility of data protection but also raises the challenge of managing the protection of all these virtualized assets. VMware provides a snapshot technology within vCenter that can quiesce and help protect these mission critical VMs. Dell has combined the intelligence of native point in time PS Series SAN snapshots with the hypervisor snapshots offered by VMware to provide a scalable and automated data protection package for the virtual environment. This automated coordination is referred to as a SmartCopy.

The Dell Virtual Storage Manager v3.5 (VSM) is the next generation of VMware vCenter plug-ins that allows administrators to coordinate data protection and recovery within their VMware vSphere virtual environment. The Dell VSM is a virtual appliance that is downloaded as part of the all-inclusive Dell EqualLogic software support and can be installed into an existing VMware vCenter environment. VSM contains many features and abilities that help VMware administrators gain better control and functionality over their EqualLogic environment including:

- Datastore Manager - a feature to provision, expand, delete and monitor EqualLogic Datastores
- VSM Smart Copies and Replication - formerly known as Auto-Snapshot Manager/VMware which allows the creation of hypervisor consistent snapshots, clones and replicas for data protection and disaster recovery
- VDI Tool - a feature which coordinates SAN based thin clones to provision space efficient virtual desktops within a VMware View environment
- Dell EqualLogic VASA Provider - a set of API calls that allow vCenter and the EqualLogic SAN to communicate for better storage awareness

This technical report will focus on VSM Smart Copies for local data protection and recovery. This is done by first coordinating with vCenter to place virtual machines into VMware snapshot mode, then coordinating with the SAN to take

space efficient point in time snapshots, and then releasing the VMs from snapshot mode. The benefits allow VSM to combine the hypervisor and application aware snapshots from VMware with the SAN snapshots for a better coordinated data protection plan. VM consistency is determined by a number of factors such as the VMware Tools being present, application support from VMware etc. Administrators are leveraging snapshots on a daily basis to help augment their already existing backup strategies. This can be used to do some testing, protect prior to an upgrade, or even used as a faster recovery tool for mission critical VMs.

For more information on the VMware snapshot process, which is invoked before the datastore volume is snapped at the SAN level refer to VMware KB article 1015180 Understanding virtual machine snapshots in VMware ESXi and ESX. <http://kb.vmware.com/kb/1015180>

INSTALLATION AND CONFIGURATION

VSM is distributed as a virtual appliance that is downloaded from the EqualLogic support portal and is provided license free as part of the all-inclusive software suite of the EqualLogic PS Series SAN. VSM is an OFV imported into vCenter and then is available directly through the vCenter Client application screen.

For installation and configuration of the VSM appliance please refer to *TR1067 EqualLogic Virtual Storage Manager: Installation Considerations and Datastore Manager*.

In order for VSM to be able to protect virtual machines residing on datastores, the PS Series Group that the datastores reside on must be added to the VSM Group inventory. VSM 3.5 now has support for multiple groups. As long as each group is managed by VSM, they can be included in SmartCopy operations.

LAUNCHING VSM FOR LOCAL PROTECTION

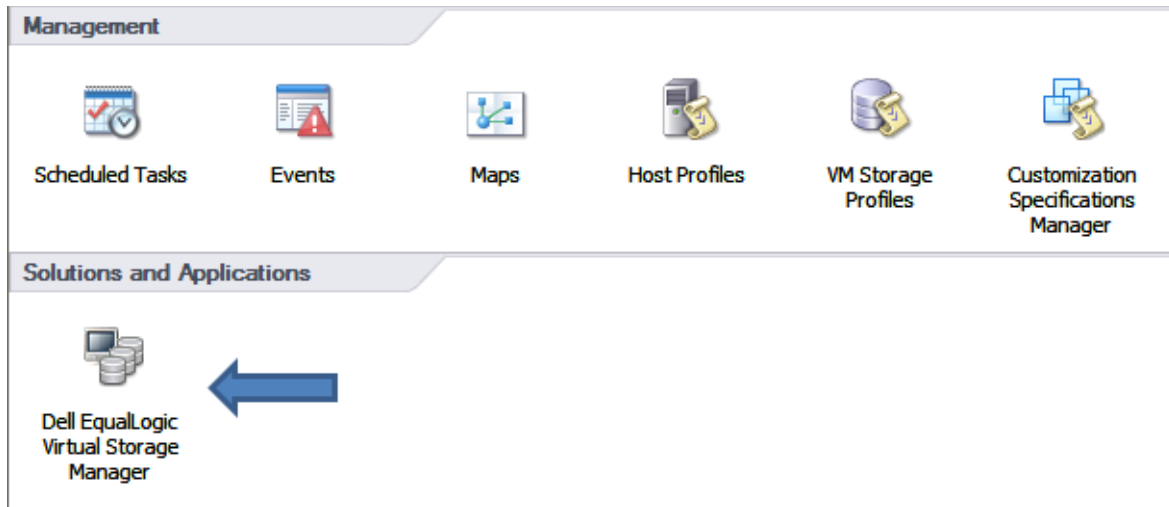
Once the VSM appliance is installed and running in the environment there will be a new icon under the Solutions and Applications area from the Home screen of vCenter.

Throughout this document the terms Auto-Snapshot Manager/VMware, ASM/VE, and Smart Copy all refer to the coordinated protection process of VMware snapshots and PS Series SAN snapshots being used together to create a hypervisor aware array snapshot recovery point.

In addition to launching VSM from the Home screen icon there are newly available options inside the vCenter GUI. From the Hosts and Clusters view by right clicking on an object in the left pane a new EqualLogic option shows up in the context sensitive menu with all of the available relevant tasks. These EqualLogic menu options show up throughout the vCenter GUI whenever a EqualLogic VSM related task can be performed. There are multiple points from which to access the VSM data-protection wizards, depending upon your

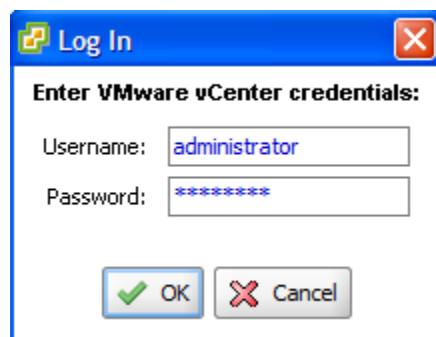
preference for accessing / using / the vCenter Client, all will allow you to achieve the same result, and are all based on ease of use and comfort with the tools.

To launch the VSM GUI to manage and monitor your Smart Copies click on the **Dell EqualLogic Virtual Storage Manager** icon on the Home screen of the vCenter Client under Solutions and Applications.



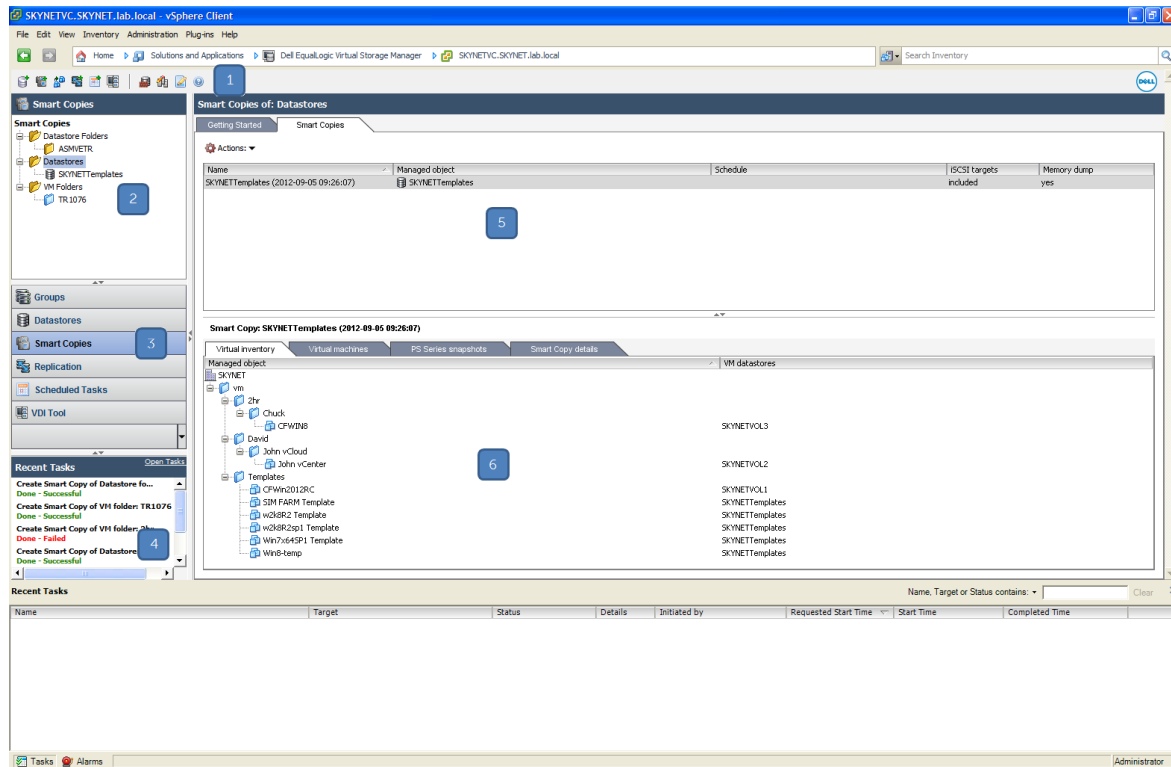
This will launch a login dialogue box. You will need to log into VSM with credentials that have vCenter administrative access.

NOTE: Java is required to be installed on the machine used to launch the VSM GUI.



Once you are logged in you are presented with the VSM Main screen GUI. From this screen you can launch all of the views within VSM; manage and monitor your datastores, Smart Copies, replicas and more. For this technical report we are going to focus on local virtual machine data protection with

Smart Copies. See Table 1 for a description of each of the various panes available to you within the VSM GUI.



1	List of commonly used toolbar shortcut icons.
2	Main object pane for the tool you are using.
3	Tool buttons to launch any of the management tools inside VSM. These can be minimized to small icon buttons.
4	VSM Recent Tasks pane.
5	This information pane area will show more information about the object selected in the object pane, including a Getting Started tab with common functions and a more detailed tab showing context aware information for the object.
6	More detailed information based on the selection highlighted inside the information pane.

Table 1: VSM GUI

Table 2 is a description of each of the toolbar shortcut icons.











Icon	Function
	Provision new Datastore(s)
	Create a Smart Copy
	Create a Smart Clone
	Create a Smart Copy Replica
	Create a scheduled task
	Create a VDI desktop pool
	Manage ACL Policies
	Configure VSM Appliance
	Set user preferences
	Access online help


Table 2: Toolbar Shortcut Icons

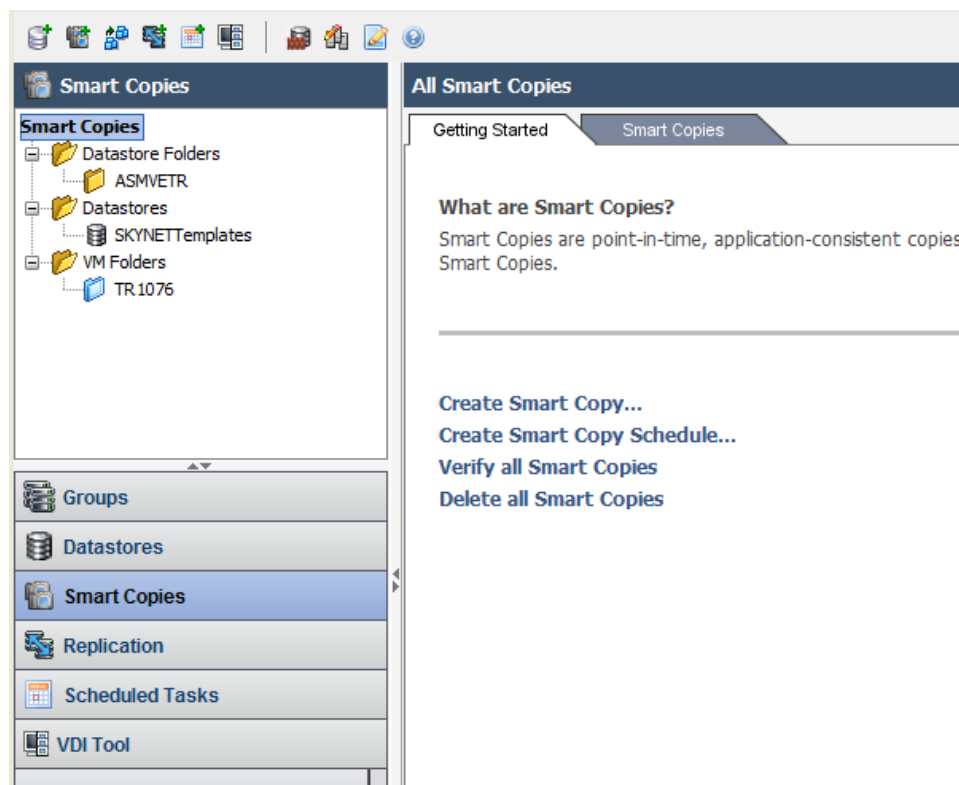
PROTECTION WITH SMART COPIES

As discussed earlier, a Smart Copy is a hypervisor or application aware VMware snapshot combined with a PS Series SAN snapshot. When VMware puts the VM into snapshot mode it quiesces the IO to the virtual machine VMDK files and if possible quiesces the application inside the VM. The level of application consistency is based upon the Operating System of the VM, the VMware Tools, and the application. There are multiple options including the ability to save memory state to disk but once these VMs are quiesced, any new changes to the VM are stored in a separate VMDK. Once the VM is quiesced, VSM coordinates with the SAN to determine which PS Series volume(s) to snapshot. These datastore volumes have a PS series snapshot created on them and then VSM coordinates with vCenter to release the VM snapshot. The benefit to this is you obtain the same consistency without leaving the virtual machine in snapshot mode for an extended period of time which could possibly lead to longer consolidation times for the snapshot and space consumption on the datastore.

There are multiple ways to launch the Create Smart Copy wizard and it really comes down to the user and their preference as they all launch the same set of dialogue wizards. This flexibility in design allows for each of the various Smart Copies, schedules, etc. to be launched from a variety of places.

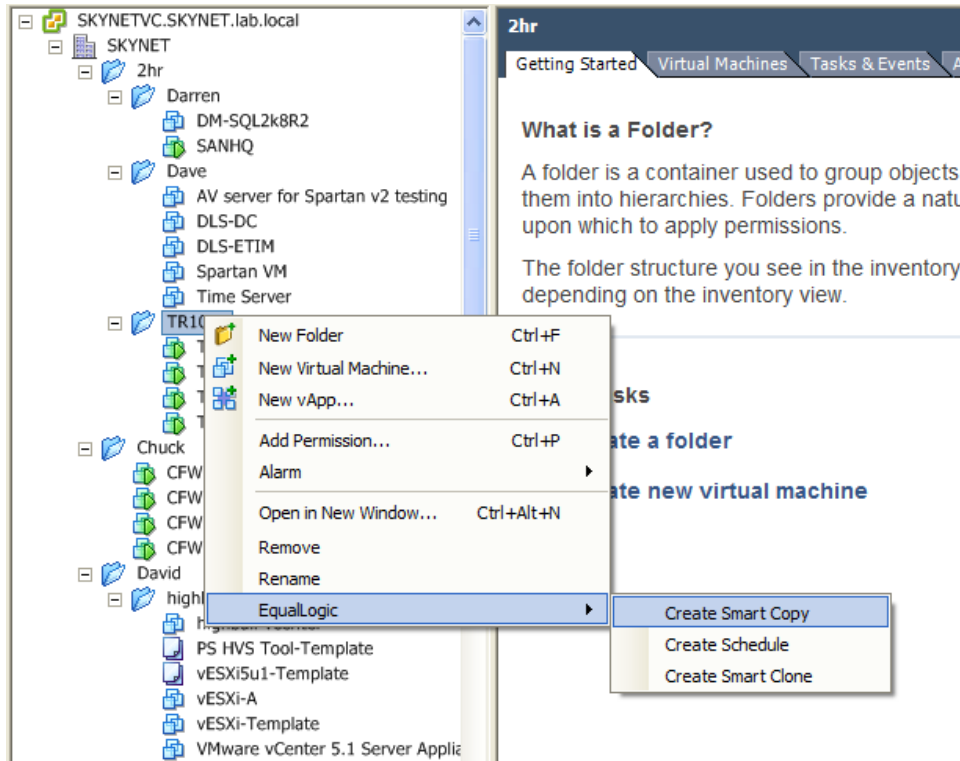
They include:

- From the VSM Main GUI - Click the toolbar shortcut icon for  **Create a Smart Copy**
- From the VSM Main GUI - In the Tool Buttons click **Smart Copies** then under the Getting Started tab click **Create Smart Copy...**

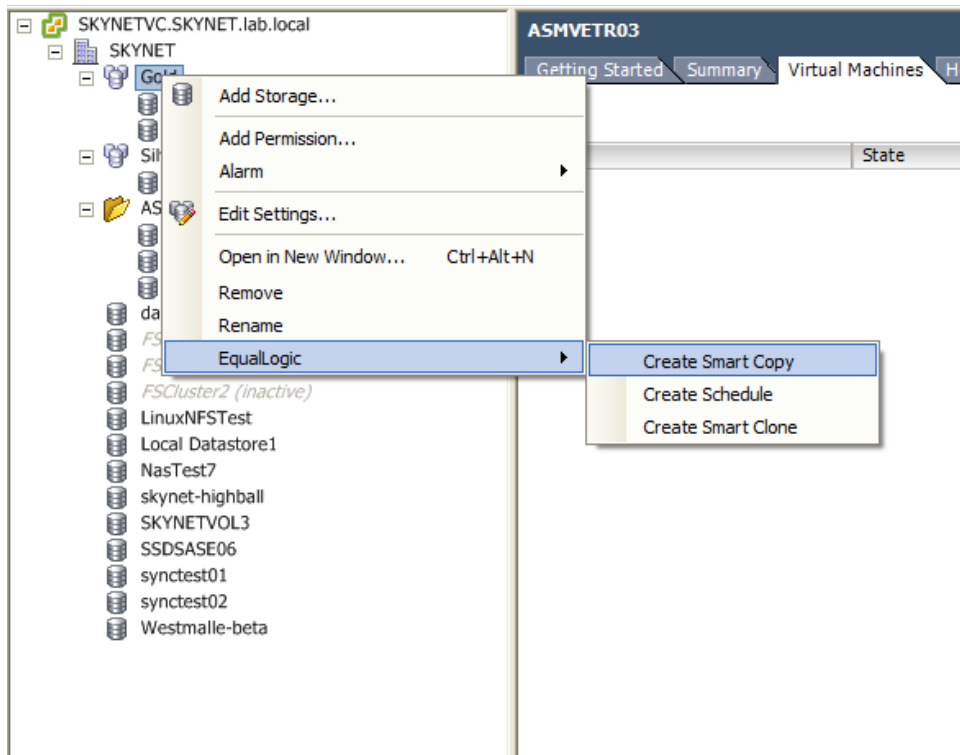


Smart Copy from VSM GUI

- From within vCenter under the Hosts and Clusters view, Datastores and Datastore Clusters view or VMs and Templates view, right click an object, be it a VM, a folder of VMs or a datastore, select EqualLogic -> **Create Smart Copy**



Smart Copy from vCenter UI -> VMs and Templates view



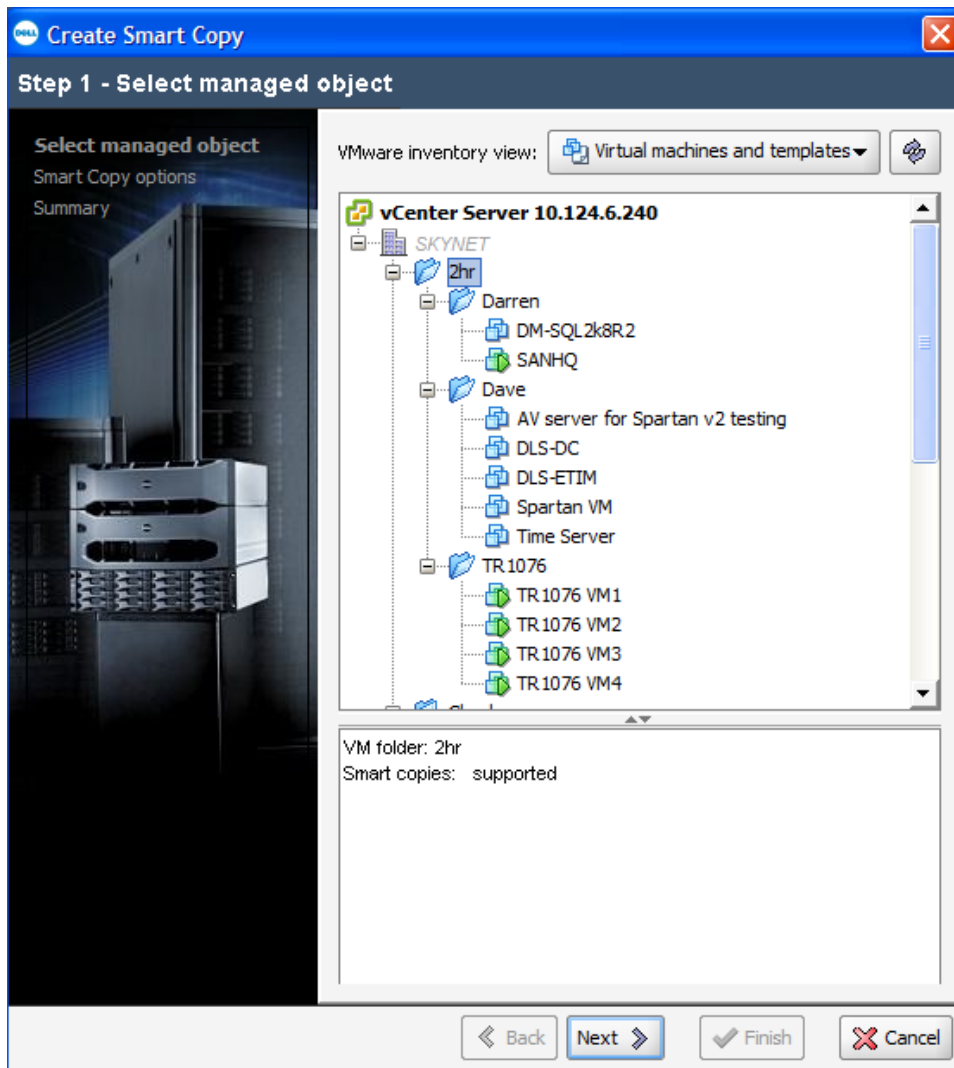
Smart Copy from vCenter UI -> Datastores and Datastore Clusters view

Step 1 - Create Smart Copy

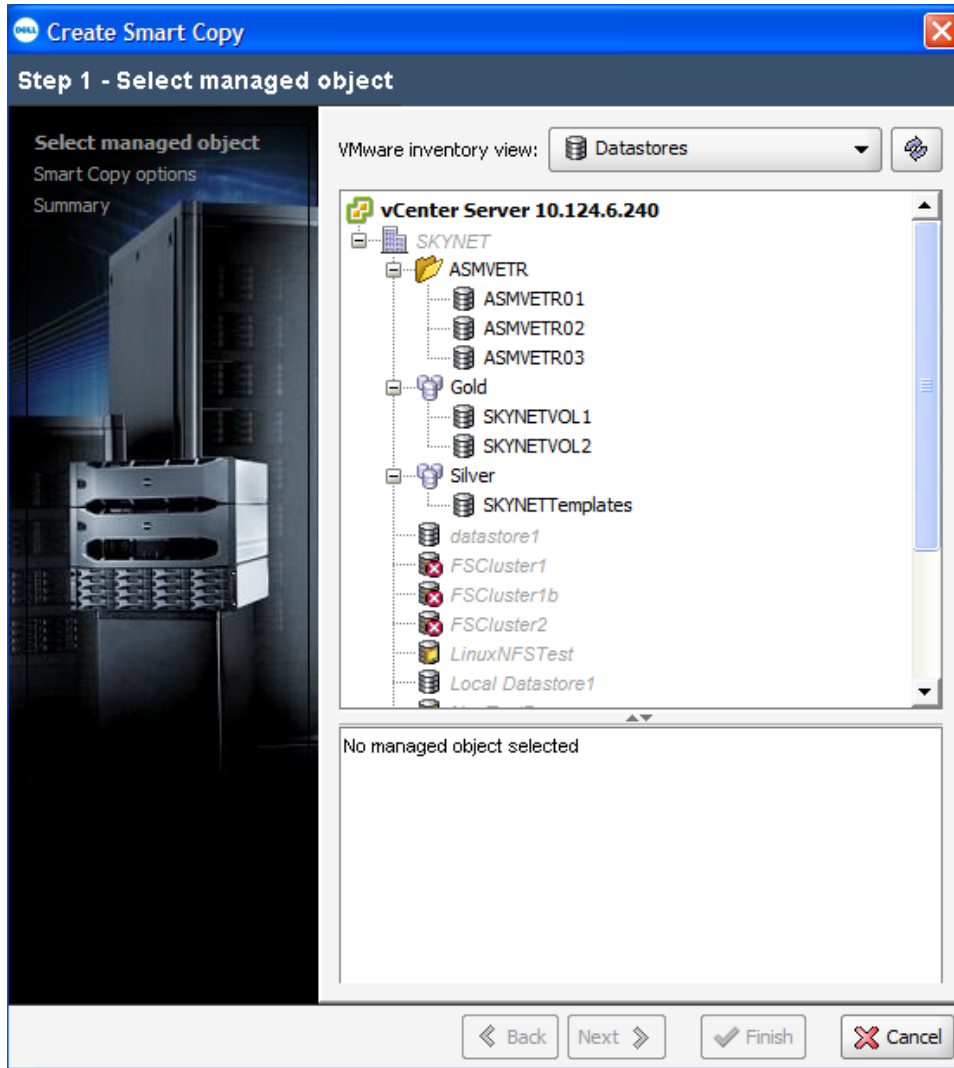
When creating Smart Copies from the VSM Smart Copy interface the first step is to select a managed object. This can be a Virtual Machine or a Virtual Machine folder. The inventory view can be changed to Datastores in which case the managed object can be a Datastore, a Datastore folder or a Datastore cluster.

If launching the Smart Copy Wizard from within vCenter by right clicking an object, that entity will become the managed object for the Smart Copy Wizard and it will skip Step 1 effectively re-numbering the steps explained in this document. (i.e. Step 2 will actually be Step 1 and so forth but the options remain identical)

Make your selection of what object is to be protect with Smart Copy and click **Next**.

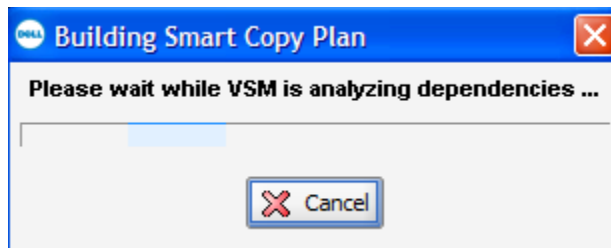


Virtual Machines and Virtual Machine Folder selection



Datastore, Datastore Folder, and Datastore Cluster selection

VSM will analyze the dependencies such as which datastore it lives on, if the VMware Tools are installed, etc and prepare a Smart Copy Plan for review.



Step 2 - Smart Copy Options

There are a variety of configuration choices depending on the needs of the protection scheme for the VMs.

Smart Copy options: These are optional parameters that can be selected for the Smart Copy. These options apply to all VMs included in the Smart Copy.

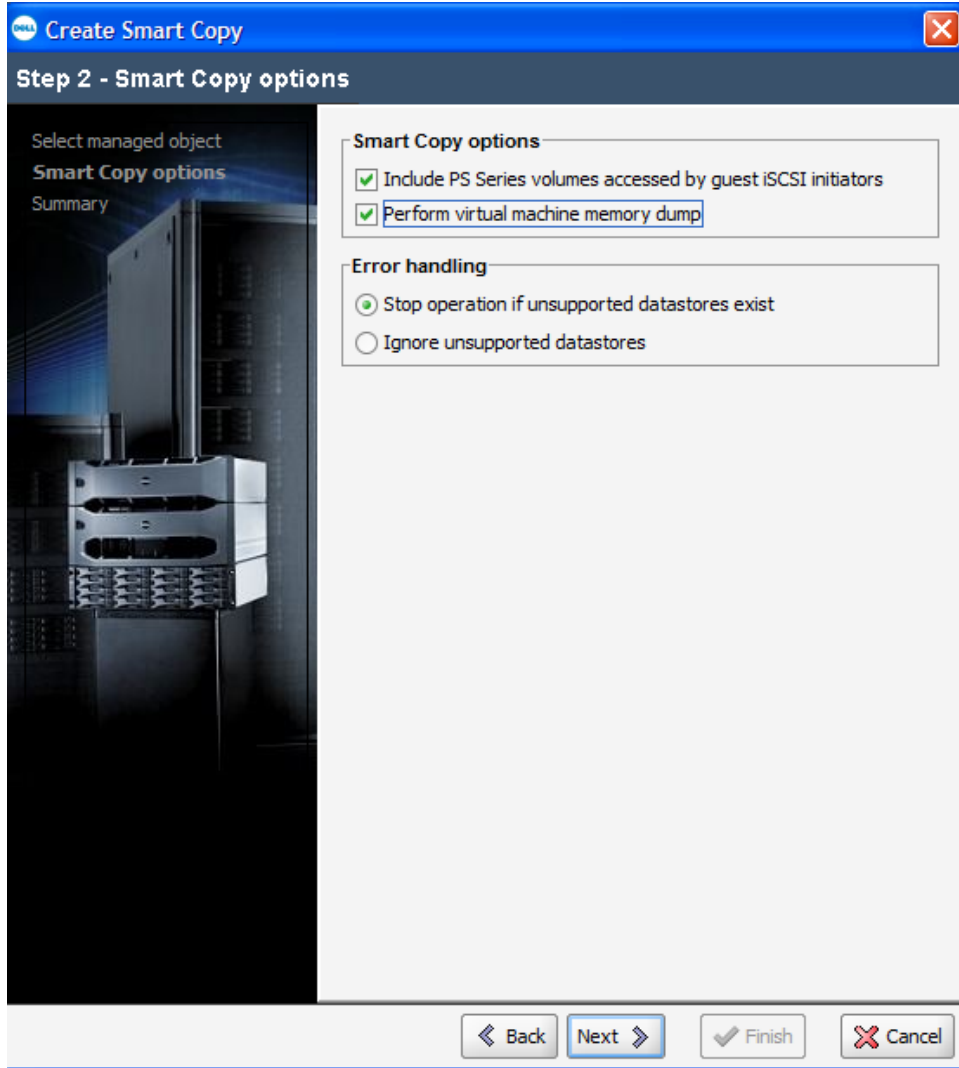
- **Include PS Series volumes accessed by guest iSCSI initiators** - This option requires the VMs to be powered on and the VMware Tools to be installed. If these conditions are met, VSM will query the tools and any connected PS Series iSCSI initiated volumes and include those in the Smart Copy. These volumes must reside on a Group that is also managed by the VSM.
- **Perform virtual machine memory dump** - This option requires the VMs to be powered on and the VMware Tools to be installed. As part of the VMware initiated snapshot, the memory of the virtual machine will be written to disk.

NOTE: The virtual machine is stunned during the memory commit process. Depending on the size of memory and activity, the time it takes to stun the VM could pose a problem for applications and access especially if the VM is only being captured a few times a day making the memory state almost useless. Take this process into account during creation of Smart Copies.

Error Handling: Choose one of the error handling processes.

- **Stop operation if unsupported datastores exist** - Choose this option to have the Smart Copy quit if unsupported datastores exist. This could happen because of a VM mounting an ISO file or VMDK from a local datastore, or a VM spanning across to a datastore that isn't part of a managed PS Series Group.
- **Ignore unsupported datastores** - Choose this option to continue the Smart Copy operation regardless of any unsupported datastores. The job history log will indicate which VMs could potentially be affected. This is important as a VM that spans between supported and unsupported datastores would result in that VM being non-recoverable.

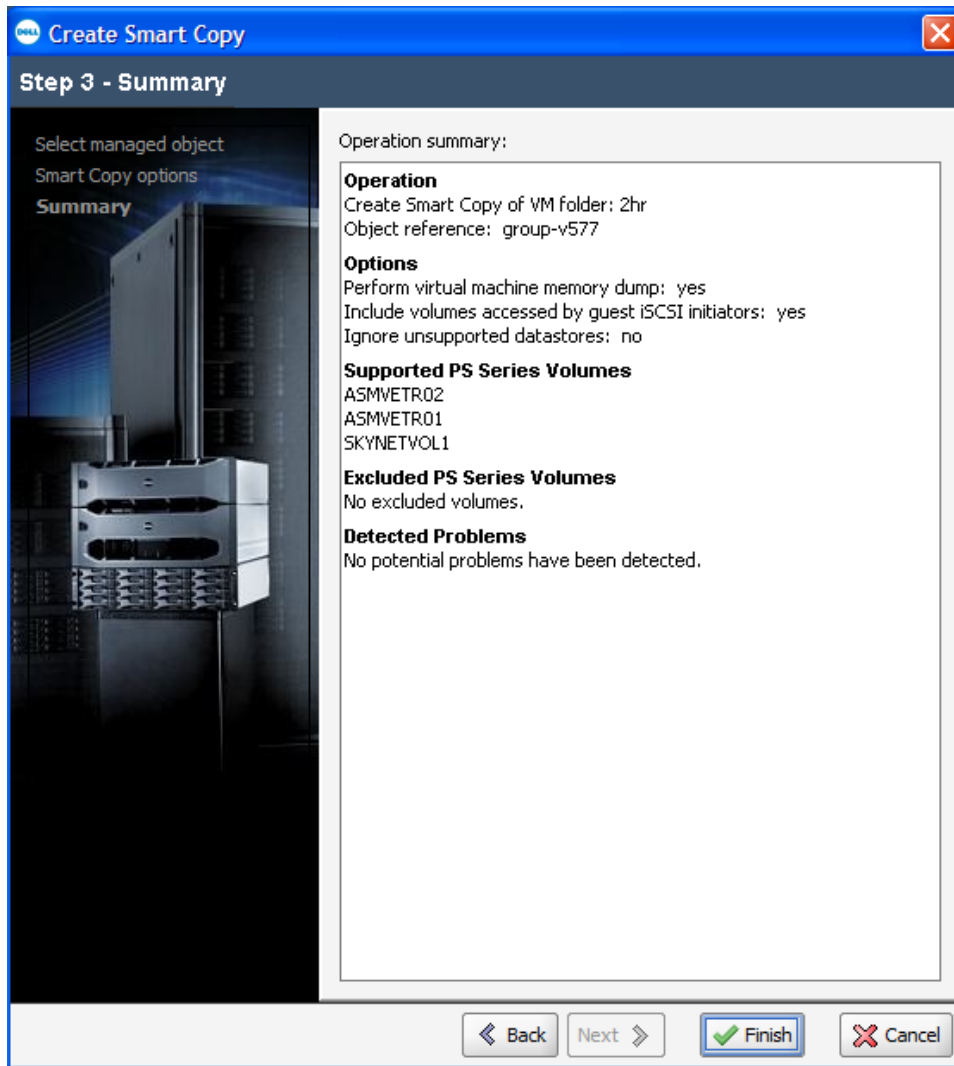
Select the options for the VM and error handling of the Smart Copy and click **Next**.



Step 3 - Summary

A variety of informational pieces are displayed. All of the options previously chosen will be displayed. In addition, all of the affected PS Series Volumes that will be part of the Smart Copy and snapshotted will be listed here. Each volume needs to have snapshot reserve space configured for it. The summary screen will display any detected problems such as unsupported datastores, powered off VMs, no tools installed etc.

Verify the summary and resolve any detected problems. When ready to create the Smart Copy click **Finish**. This will begin the Smart Copy Process.



During the Smart Copy process, each of the VMs will be placed into VMware snapshot mode, quiescing the virtual machine (if VMtools are installed). Once the VM snapshots are created, VSM will coordinate PS Series snapshots for each of the included PS Series Volumes. When the PS Series snapshots are completed, VSM will then delete the VMware snapshots associated with the Smart Copy. This will not delete any existing VMware snapshots on the VMs, just the ones created for the Smart Copy.

You can verify the Smart Copy operation and watch its progress in the VSM Recent Tasks pane. In the vCenter Recent Tasks pane you will see the VM snapshots being created and deleted.

Name	Target	Status
Remove snapshot	TR1076 VM1	Completed
Remove snapshot	SANHQ	Completed
Remove snapshot	TR1076 VM3	Completed
Remove snapshot	TR1076 VM2	Completed
Remove snapshot	TR1076 VM4	Completed
Create virtual machine snapshot	SANHQ	Completed
Create virtual machine snapshot	TR1076 VM2	Completed
Create virtual machine snapshot	TR1076 VM1	Completed
Create virtual machine snapshot	TR1076 VM4	Completed
Create virtual machine snapshot	TR1076 VM3	Completed

vCenter Recent Tasks Pane

Inside the Group Manager GUI the associated PS Series Volumes will have a new snapshot created and the description will read Created by Auto-Snapshot Manager/VMware Edition.

The screenshot shows a tree view of SKYNET volumes on the left and a detailed view of SKYNETVOL2 on the right. The detailed view shows the following information:

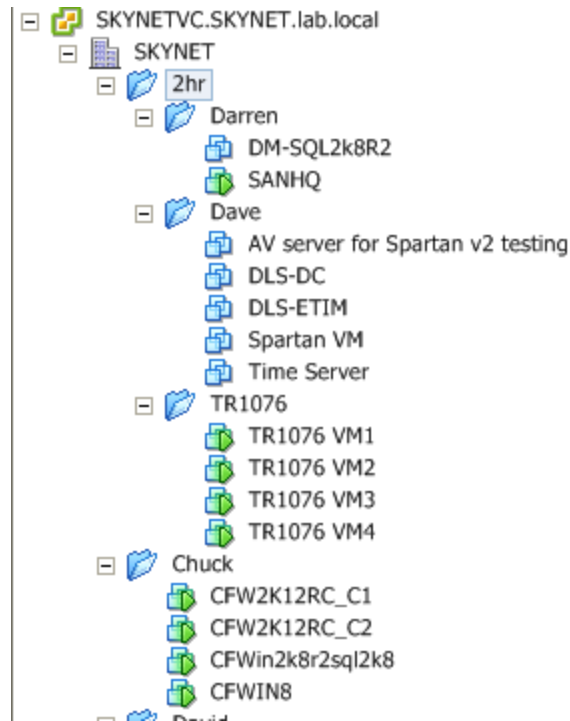
- Status: offline
- iSCSI access: restricted
- Access type: read-only, not shared
- iSCSI connections: 0
- Description: Created by Auto-Snapshot Manager/VMware Edition

Group Manager GUI

SCALABILITY WITH FOLDERS AND DATASTORES

As virtual environments grow it becomes increasingly important to be able to protect these environments. However protecting these growing and changing environments can also be a challenge. VSM allows for the ability to protect folders of virtual machines and folders of datastores to allow the ability to scale and add without constantly having to adjust your protection schemes. By utilizing the folder structure in vCenter Server to organize the VMs based on administrative roles or protection groups, administrators can select an entire folder of VMs or datastores and create a Smart Copy. VSM will query to see which VMs are in the folder, which PS Series volumes the VMs reside on, and take a Smart Copy of the entire set. This allows for keeping web server farms consistent or file servers coordinated in their protection.

This process also allows for VMs to migrate from one Datastore volume to another, either by Storage vMotion or Migration, and still retain their protection strategy as it is assigned at the folder level and includes multiple datastores.




Example of folders in vCenter for Protection

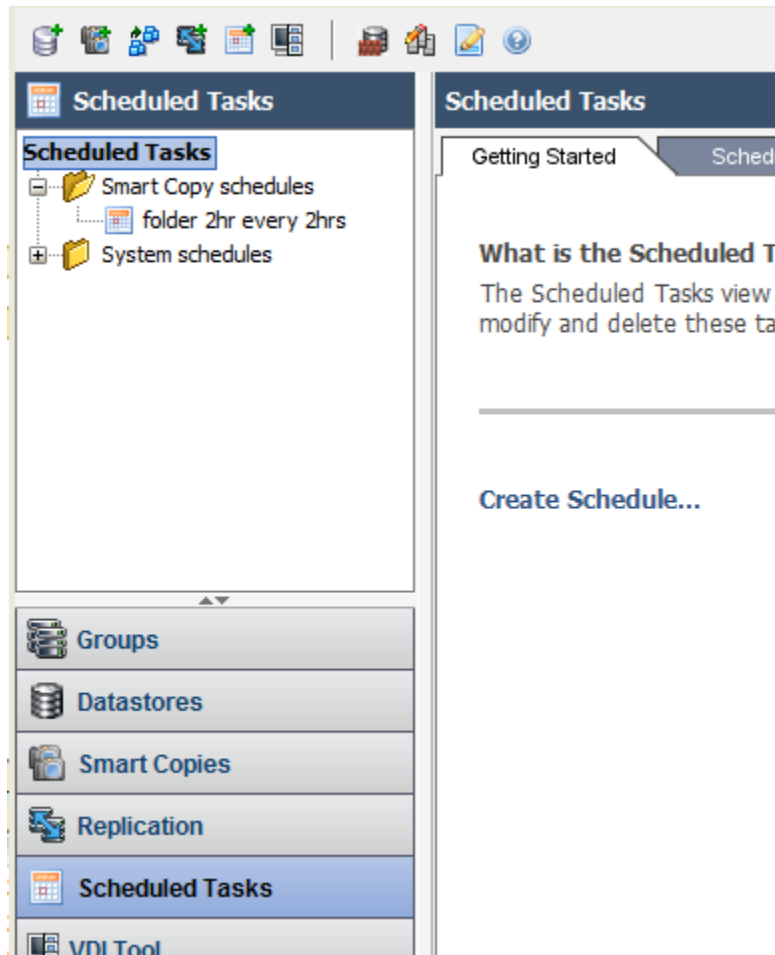
AUTOMATING PROTECTION WITH SCHEDULES

Individual Smart Copies are useful for one off situations such as testing a new patch or software build but the real power from VSM comes from the built-in scheduling function. This provides a layer of protection that allows VMs to meet a better SLA for recoverability. Everything that can have a Smart Copy taken can also have a schedule created to automate the process. VMs, folders, datastores and datastore folders, even datastore clusters can be scheduled for Smart Copies.

Schedules allow for tiering of protection levels for VMs. The administrator can have different schedules for different folders or different VMs, depending on the needs of that VM. When a new VM is created it can fall under a certain tier of protection and the administrator doesn't have to adjust the schedule as it will now inherit the protection scheme of the folder or datastore it resides in.

Creating a Smart Copy Schedule is done in the same way that a standard Smart Copy is created. Like creating a Smart Copy it can be launched a variety of ways.

- From the VSM Main GUI - Click the toolbar shortcut icon for  **Create a Schedule**
- From the VSM Main GUI - In the Tool Buttons click **Scheduled Tasks** then under the Getting Started tab click **Create Schedule...**



Schedule from VSM GUI

- From within vCenter under the Hosts and Clusters view, Datastores and Datastore Clusters view or VMs and Templates view right click an object, select EqualLogic -> **Create Schedule**

As with creating an individual Smart Copy, when creating a Smart Copy Schedule from the VSM Smart Copy interface the first step is to select a managed object. This can be a Virtual Machine or a Virtual Machine folder. The inventory view can be changed to Datastores in which case the managed object can be a Datastore, a Datastore folder or a Datastore cluster.

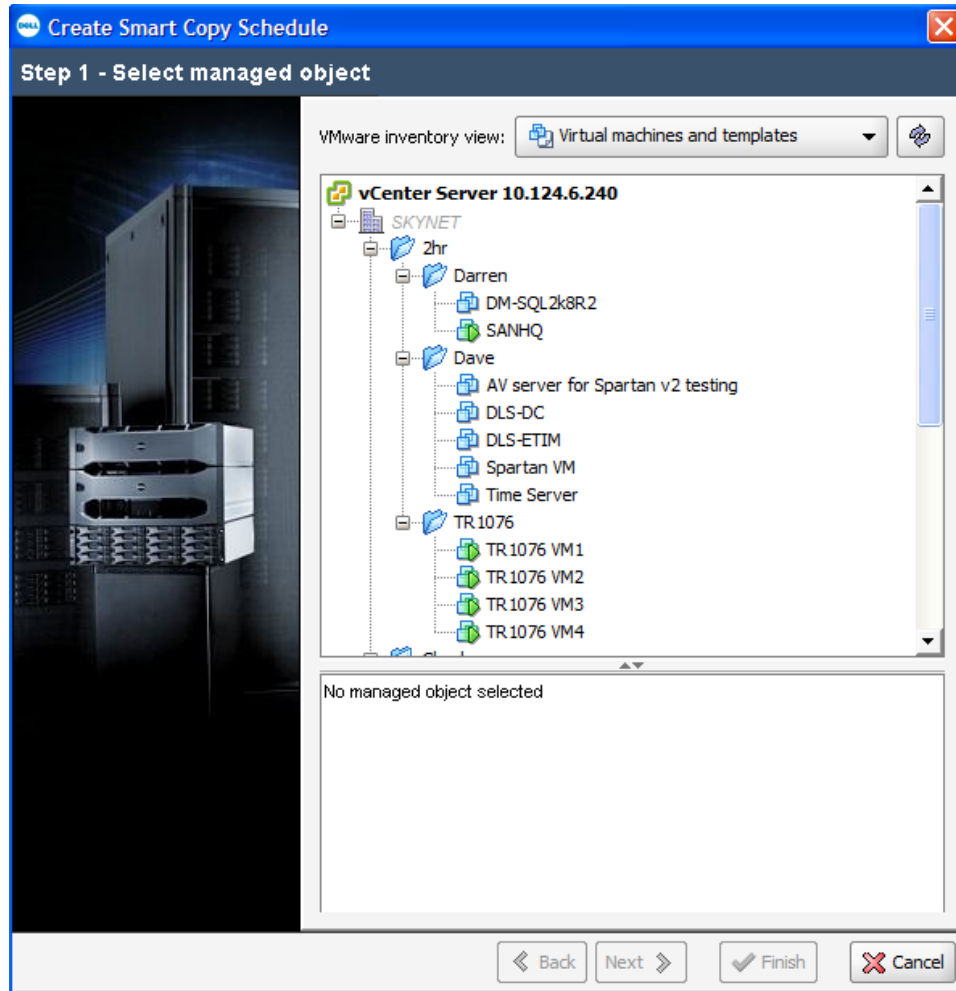
If launching the Smart Copy Schedule Wizard from within vCenter by right clicking an object, that entity will become the managed object for the Smart Copy Wizard and it will skip Step 1 effectively re-numbering the steps explained in this document. (i.e. Step 2 will actually be step 1 and so forth but the options remain identical)

In this example we have a folder named **2hr** that contains multiple VM folders, which in turn contain multiple virtual machines. The plan is to configure a

Smart Copy Schedule that happens every 2 hours and has a keep count, or maximum number of copies, of 10. The additional benefit to this is any new VMs that are created that need the same level of protection only have to be placed inside the 2h folder to inherit that protection, and no changes to the schedule are needed. There are multiple options when choosing your protection schemes.

Step 1 - Select Managed Object

Make your selection of the object in the correct view and click **Next**.



Step 2 - Schedule Type

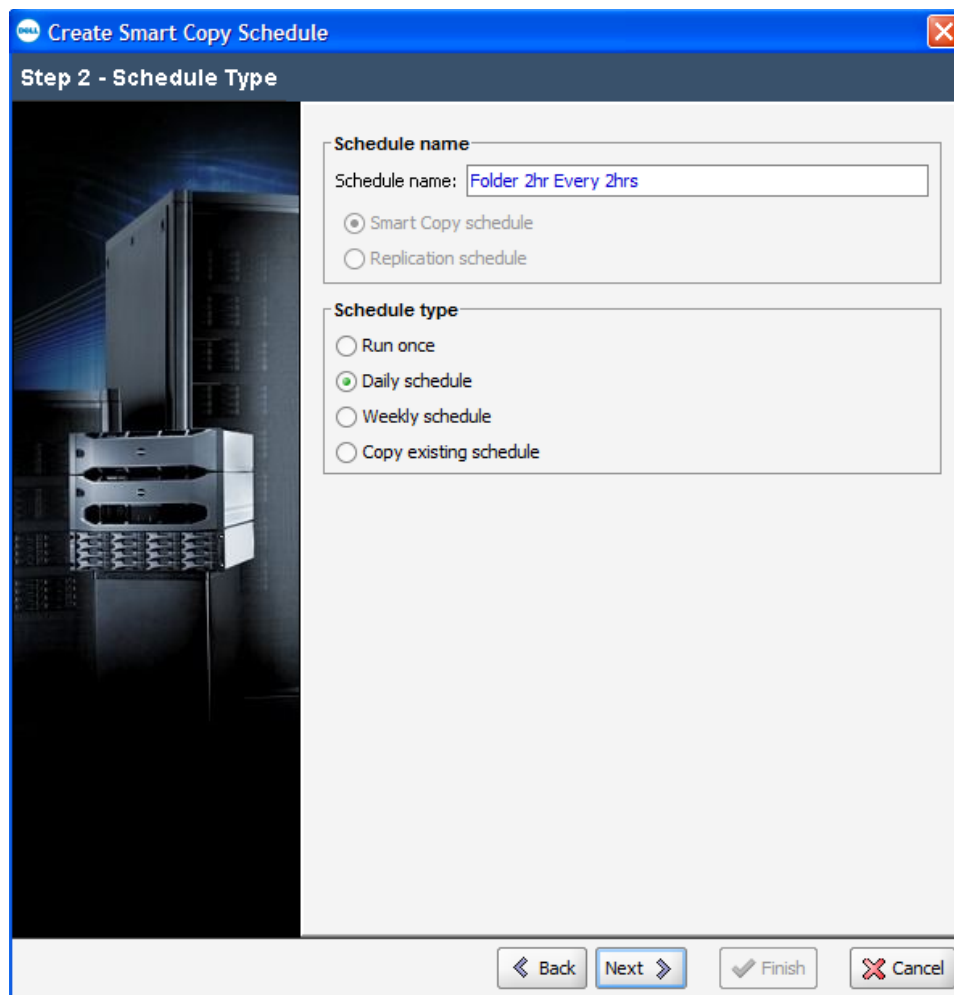
When choosing the Schedule type, there are two options to configure.

Schedule name: Enter a unique schedule name for the schedule. In the example below we chose the VM folder 2hr and named it uniquely *Folder 2hr Every 2hrs*.

Schedule type:

- **Run once** - Run once is used to test a schedule or to set it to run once on a particular date and time in the future.
- **Daily schedule** - Use Daily schedule to configure a schedule that will run every day with options including all days, weekdays only or weekends only.
- **Weekly schedule** - Weekly schedule can be used to configure a schedule that runs only once a week. The days and time for each time it is run can be configured in the wizard.
- **Copy existing schedule** - Copy an existing schedule to repeat it on the new object. The copied schedule can be modified to suit.

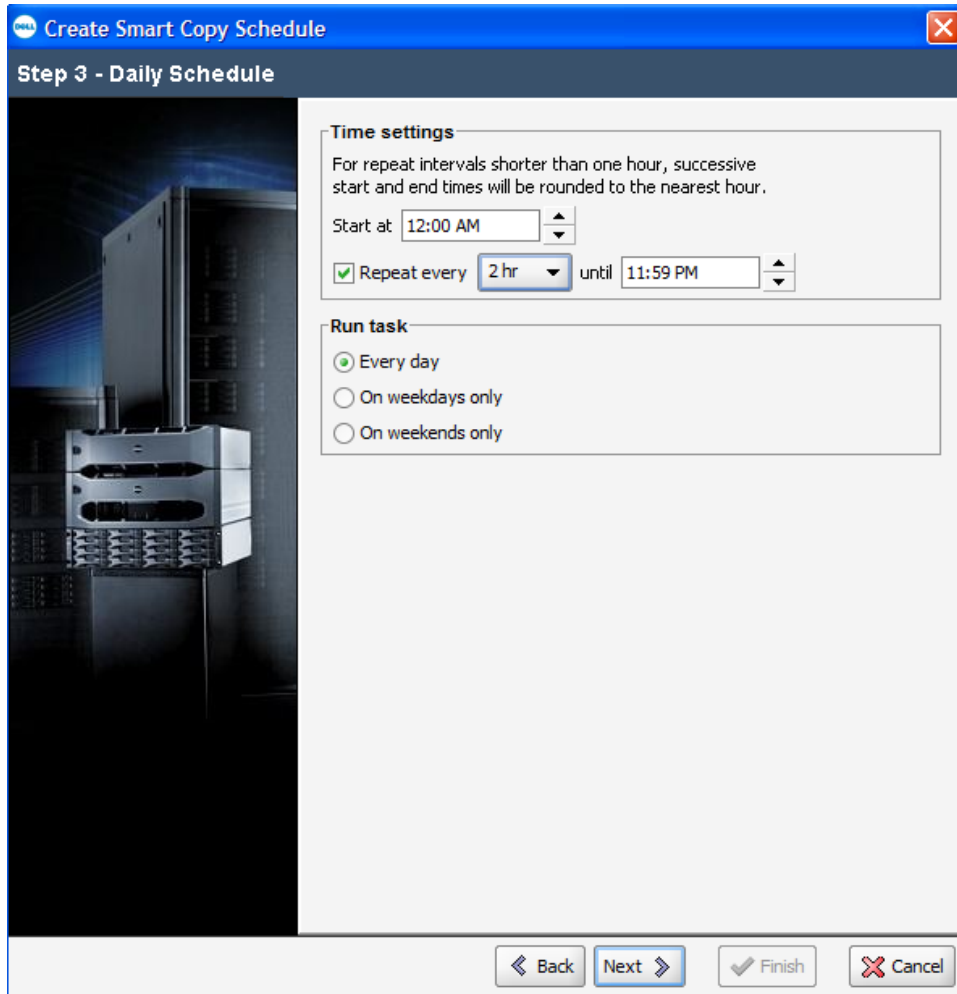
Input the name and type and click **Next**.



Step 3 - Run once/Daily schedule/Weekly schedule

The various options based on the type of schedule will be presented. Choose the date or times as appropriate. In the example below a Daily Schedule was selected so the start time and how often to repeat the schedule, are all options.

Configure all of the relevant options and click **Next** to continue.



Step 4 - Options

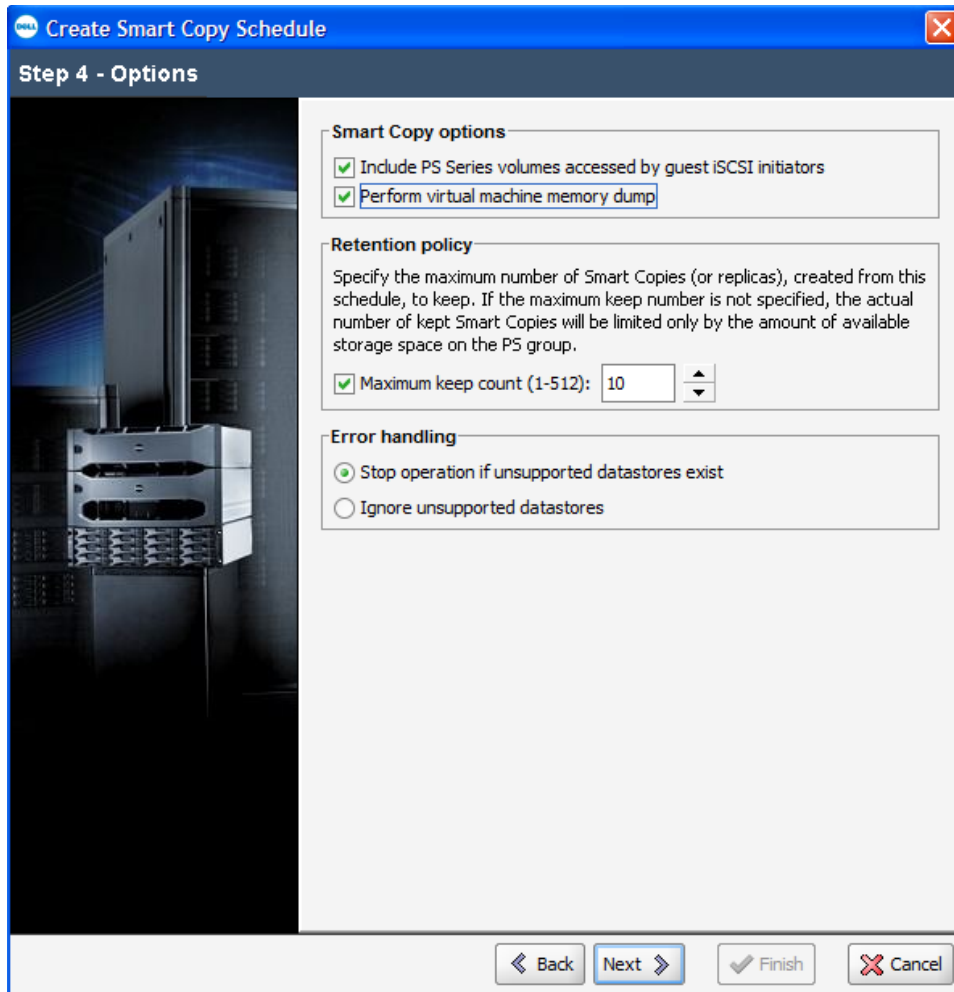
You are presented with the same Smart Copy options to Include PS Series volumes accessed by guest iSCSI initiators and whether or not to perform virtual machine memory dump.

In addition to the Smart Copy options, there is a Retention policy to specify the maximum number of Smart Copies to keep. This will allow for a rolling schedule to keep a particular number of Smart Copies and roll them over when the oldest one expires. There must be sufficient snapshot space available to accommodate all of these Smart Copies.

NOTE: With Dell EqualLogic PS Series Firmware v6.x you can enable snapshot borrowing on the volume to allow for borrowing from unused snapshot space belonging to other volumes or from the free pool space to allow for the retention policy to be met in the event that the volume does not currently have sufficient snapshot reserve to keep all of the keep count Smart Copies. For more information on snapshot borrowing please refer to TR1084 EqualLogic PS Series Architecture: Snapshot Space Borrowing Overview.

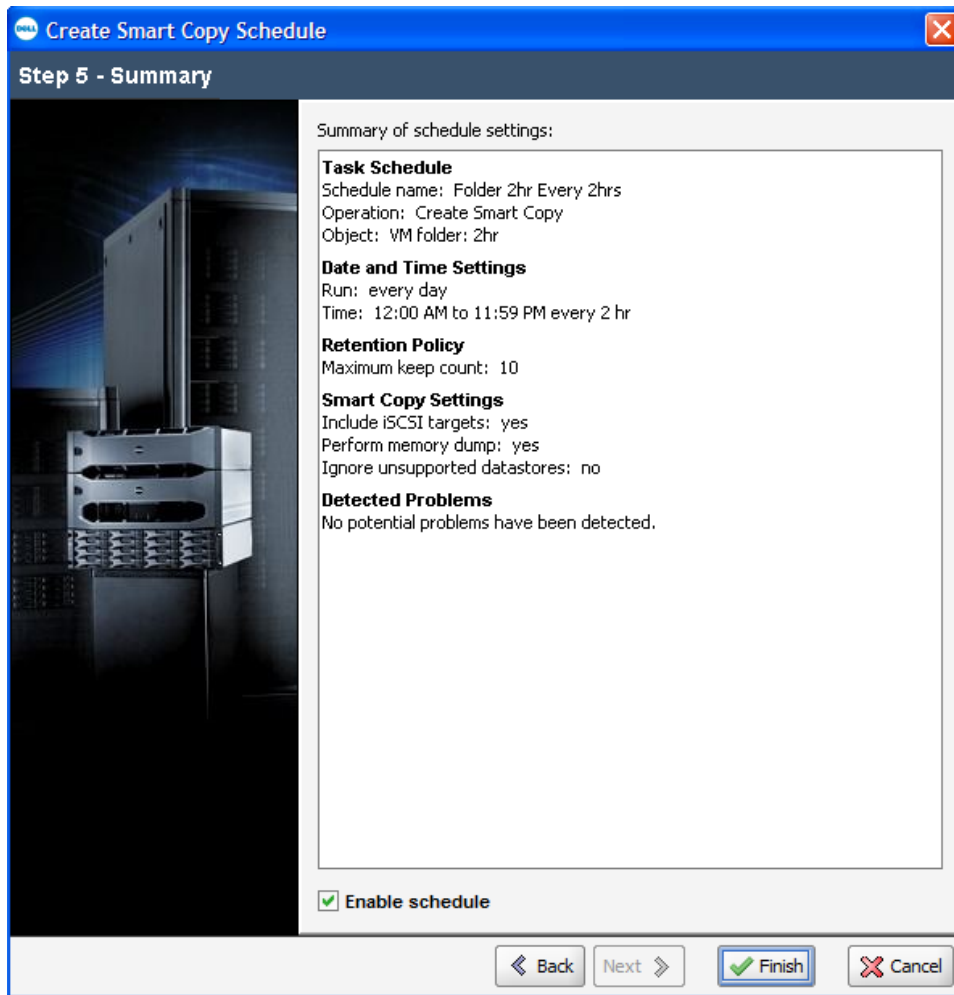
The last option for Error Handling is identical to when taking a stand-alone Smart Copy.

Make your selections and click **Next**.



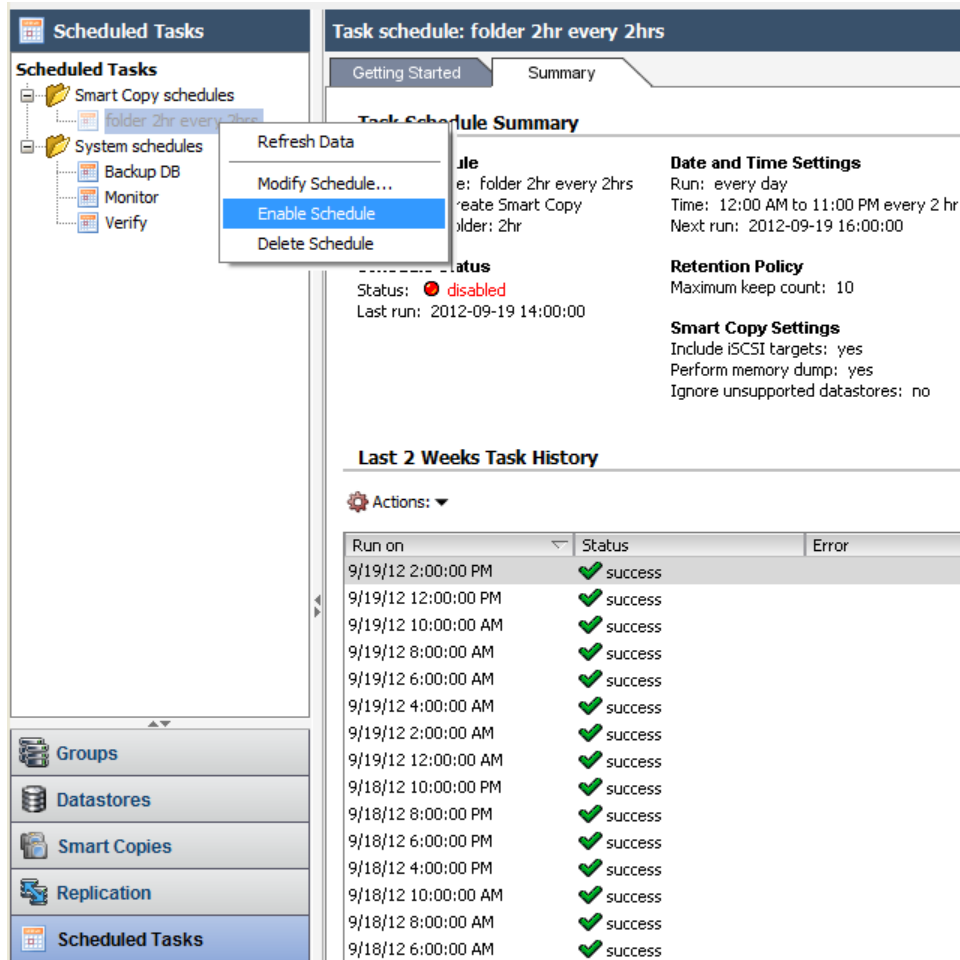
Step 5 - Summary

Verify all of the information in summary pane. During this time you can choose to disable this schedule as well to run at a later time. Once everything is set click **Finish** to complete the Smart Copy Schedule wizard.



Verifying and Modifying Smart Copy Schedules

Once a Smart Copy schedule has been configured you can see it, along with all the other schedules, by clicking the **Scheduled Tasks** tool button in the main VSM home page. Expand Smart Copy schedules and all available schedules will be listed. By right clicking on the schedule you can enable/disable the schedule or make modifications to the schedule. You can also see prior runs and verify whether they were successful or not.



Overlapping Datastore Schedules

It is very important to have an understanding of what VSM is doing in the background during these schedules otherwise you may end up with overlapping datastore schedules and not accomplishing the data protection scheme you are trying to achieve. Every object that is Smart Copied is first put into VMware snapshot mode and then the underlying datastore volume on the PS Series SAN is snapped.

If you have a VM that is part of a folder that is being Smart Copied every 2 hours, and elsewhere in the cluster you have another VM that is part of another folder that is being Smart Copied every 6 hours, however, this VM also resides on the same datastore volume as the first VM, the PS Series SAN will be creating multiple snapshots of the same volume but the consistency of the first VM will only happen during the Smart Copy it is a part of. While the second Smart Copy is snapshotting the same datastore volume, VSM is not placing the first VM in VMware snapshot mode. Therefore, the Smart Copy of the second folder is not usable as a consistent restore point for the VM in the first folder. The solution is to either place both folders of VMs in a higher level folder, or move the folder of

VMs to a different or new datastore. It is because of this, that proper VM placement for protection strategies is important.

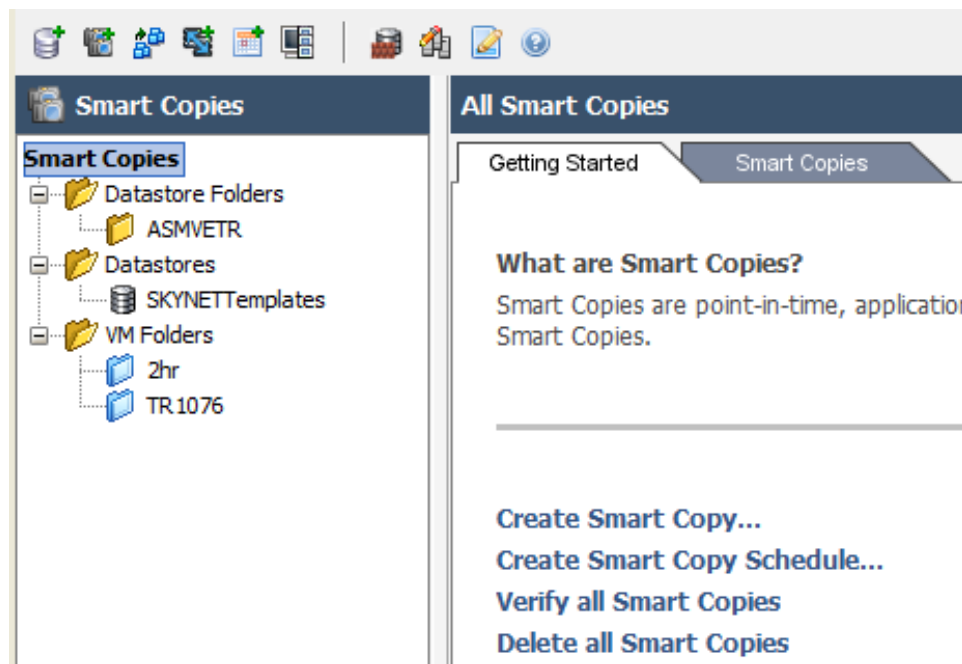
MANAGING SMART COPIES AND OPERATIONS

VSM includes a variety of tools to manage the Smart Copies that are created. From within the Smart Copies Getting Started tab you have the option to **Verify all Smart Copies** or to **Delete all Smart Copies**.

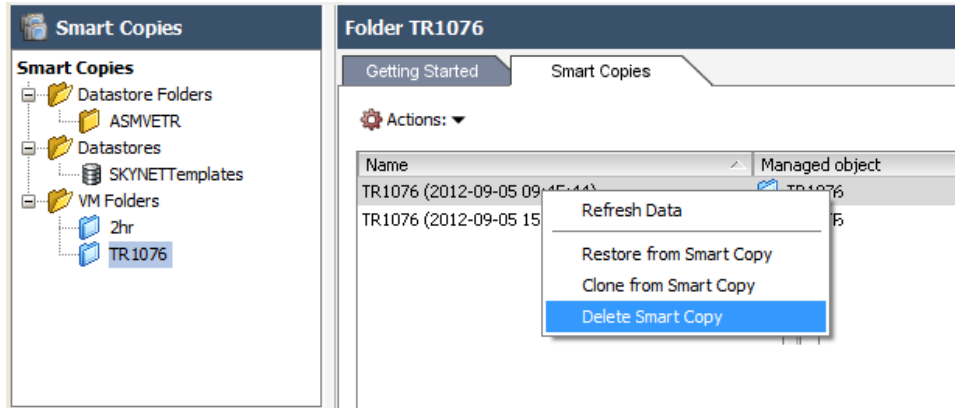
When the verify runs, it will query the VSM database and make sure that the PS Series snapshots still exist that relate to each Smart Copy. There is a scheduled verify task that runs every hour.

Deleting all Smart Copies will delete all existing Smart Copies for all of the objects that have Smart Copies in the database. It will also remove any associated PS Series snapshots. This process cannot be reversed, and therefore should be used with caution

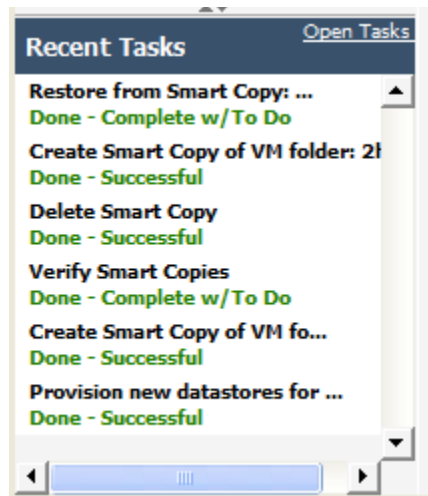
NOTE: Even if an object is selected on the left, Delete all Smart Copies affects all of the Smart Copies in VSM not just the ones associated with the highlighted object.



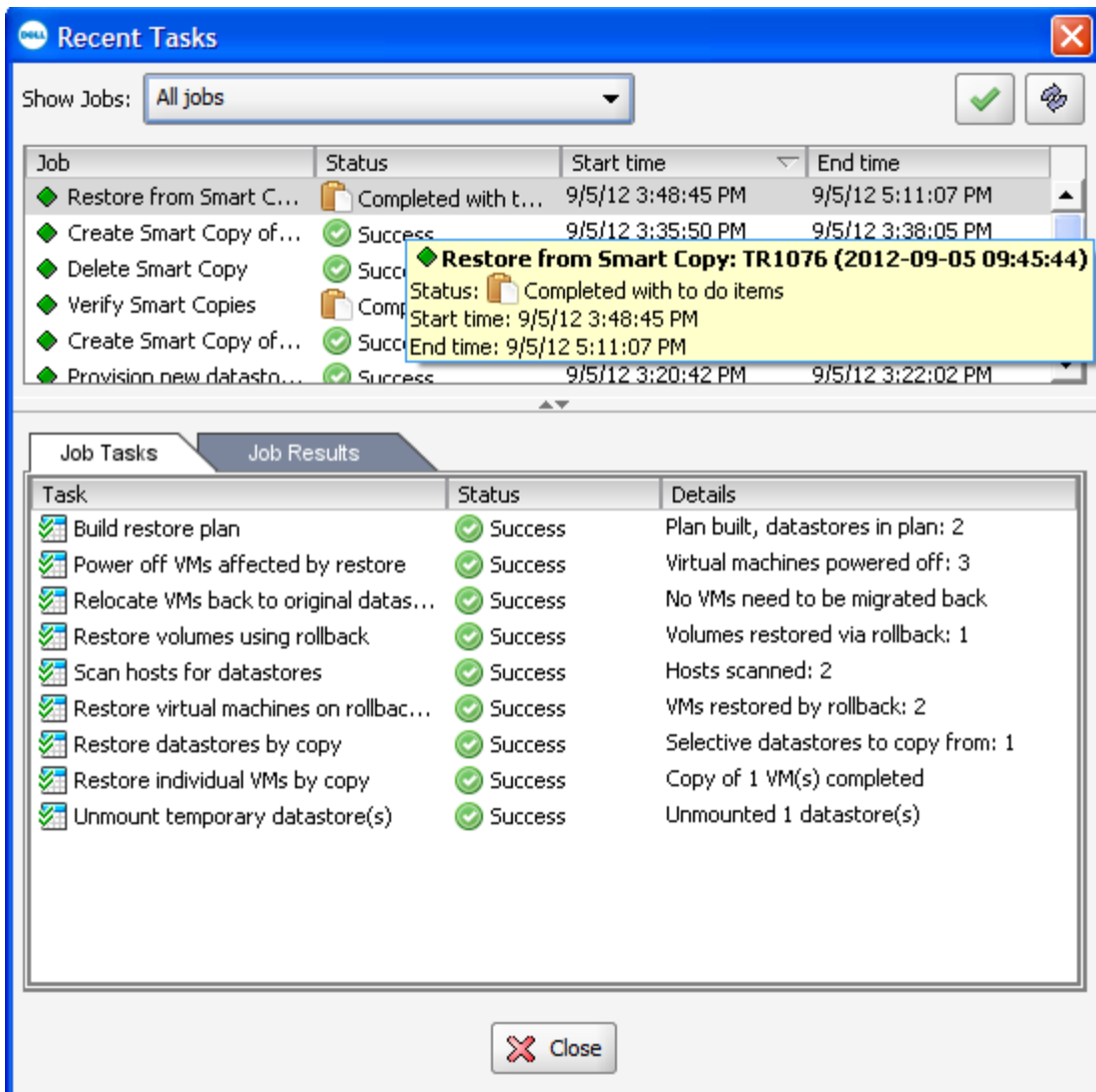
If you wish to delete individual Smart Copies from an object, click the object and under the Smart Copies tab right click on the Smart Copy you wish to delete and click **Delete Smart Copy**.



Another benefit to the VSM is the ability to see the recent tasks that have been performed. You can look through this to see which Smart Copies or scheduled operations have been completed along with any errors. For more detailed information click the **Open Tasks** link.



This will show a list of all of the VSM tasks that have been run along with their status.



By selecting an operation such as a Smart Copy, you can click the Job Results tab to get a better understanding of the operations that were performed as well as if it was successful. In the Job Results tab there will also be any further user interactions that have to be performed listed here.

Recent Tasks

Show Jobs: All jobs

Job	Status	Start time	End time
Restore from Smart C...	Completed with t...	9/5/12 3:48:45 PM	9/5/12 5:11:07 PM
Create Smart Copy of...	Success	9/5/12 3:35:50 PM	9/5/12 3:38:05 PM
Delete Smart Copy	Success	9/5/12 3:29:14 PM	9/5/12 3:29:18 PM
Verify Smart Copies	Completed with t...	9/5/12 3:28:51 PM	9/5/12 3:28:54 PM
Create Smart Copy of...	Success	9/5/12 3:22:02 PM	9/5/12 3:24:11 PM
Provision new databa...	Success	9/5/12 3:20:42 PM	9/5/12 3:22:02 PM

Job Results

- ▶ **Status of restore operation: complete**
- ▼ **Smart Copy Summary (4)**
 - Created: 2012-09-05 09:48:47
 - Schedule: null
 - Memory dump performed: yes
 - iSCSI targets (volumes) accessed by VMs: included
- ▼ **Restored Volumes (1)**
 - iqn.2001-05.com.equallogic:0-8a0906-7b25d4409-7bb92486c7b50461-asmvetr02: ASMVETRO2-2012-09-05-10:17:27.3751.1
- ▼ **Fast Restored Virtual Machines (2)**
 - TR1076 VM4: revert success
 - TR1076 VM3: revert success
- ▼ **Selective Restored Virtual Machines (1)**
 - TR1076 VM1: success
- ▼ **Emergency Snapshots Created (1)**
 - ASMVETRO1: ASMVETRO1-2012-09-05-16:23:30.3768.1
- ▼ **Additional User Actions Required (1)**
 - Verify restore has completed satisfactorily, remove any restore snapshots created by PS Series groups.

Close

RECOVERING WITH SMARTCOPIES

The reasons for to recover virtual machines can be many; bad patch or software build, corrupt file or virtual machine, or even a file that was deleted by accident. Creating Smart Copies on a standard schedule adds additional recovery points of the virtual environment to a traditional backup schedule in case data needs to be restored. By utilizing the Smart Copies in addition to the traditional backup schemes, administrators gain a shorter recovery time objective. Instead of deploying a new virtual machine, patching it, installing the applications and backup agent, and then recovering data from the previous known good backup with the resulting loss of many hours or even days' worth of work, Smart Copies can be utilized to rapidly roll a virtual machine back to a good point-in-time and work can continue with minimal disruption.

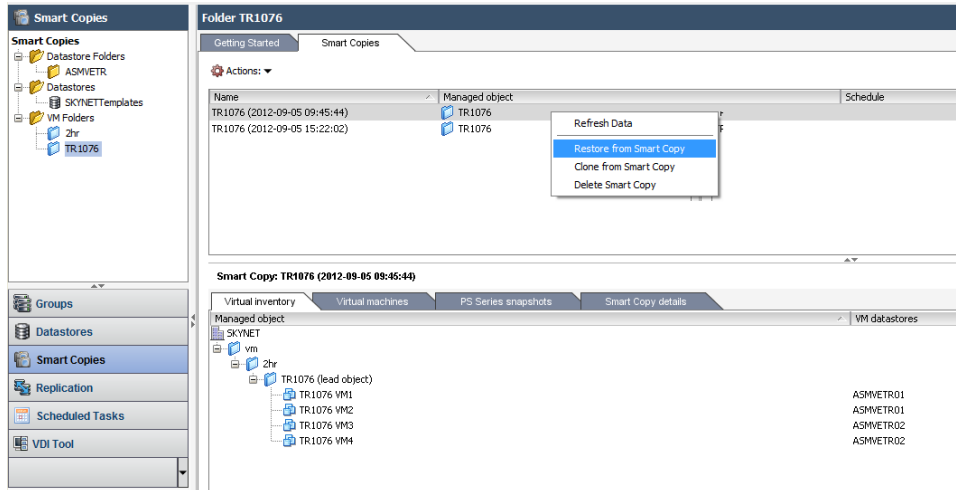
To launch the Smart Copy recovery wizard click on the **Smart Copies** button in the VSM main UI page.

In the left pane you will see all of the Smart Copies that have been created broken down by object. Click a Smart Copy object and then the Smart Copies tab on the right to display all of the available Smart Copies of that object.

For more information, click on a Smart Copy in the left pane. In the bottom pane there are four tabs each with additional information about the selected Smart Copy.

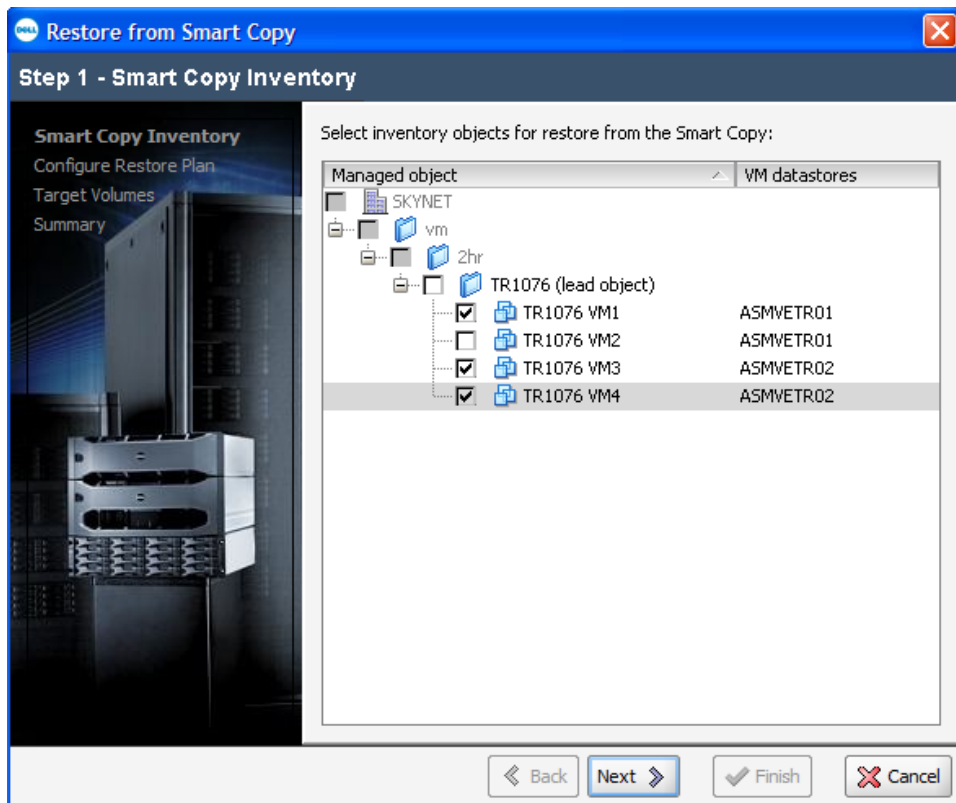
- Virtual inventory - A list of VMware inventory objects that are part of the Smart Copy as well as the datastores they reside on.
- Virtual Machines - A list of the VMs included, whether a VM snapshot was taken, and if it included a memory dump, and finally if the VM was quiesced.
- PS Series Snapshots - A list of the PS Series snapshots and PS Series groups that were part of the Smart Copy.
- Smart Copy details - A summary of details such as, the schedule that created the Smart Copy, the number of virtual machines, and snapshots contained in the Smart Copy

Select the Smart Copy and either click the Actions dropdown or right click on the Smart Copy to be recovered and select **Restore from Smart Copy**.



Step 1 - Smart Copy Inventory

A Smart Copy can contain multiple VMs from multiple datastores. In certain recovery scenarios restoring an entire Smart Copy might be desired but in other recovery scenarios only a select few VMs, or an individual VM, are needed to be recovered. Select the VM or VMs that are to be recovered and click **Next**.



Step 2 - Configure Restore Plan

In Step 2, each of the VMs to be recovered is displayed under their associated datastore. There are two ways to recover VMs.

- Restore by rollback - By selecting Rollback datastore, all of the affected VMs will be powered off and then the entire datastore is reverted to a previous PS Series snapshot. The ESXi servers will rescan the HBAs and then the VMs are refreshed from this point in time.

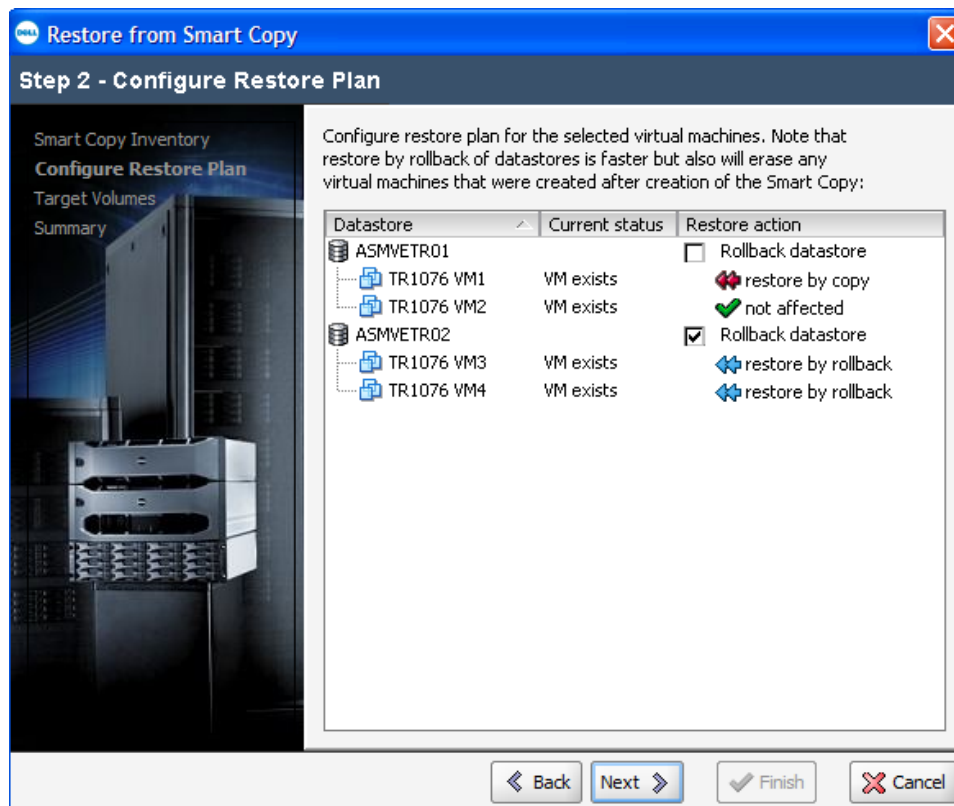
NOTE: The entire datastore will be rolled back, this will affect all VMs on the datastore including new VMs that might not be part of an older Smart Copy. VSM will warn you of these impacts if they exist.

- Restore by copy - By selecting to restore individual machines on a datastore, VSM will first power off the VM. Then VSM will create a clone of the PS Series snapshot, mount it, and copy the VM back to its original location.

NOTE: This process will take longer than a restore by rollback but it does not impact any other VMs on the datastore.

In both cases all the VMs affected will also have their VMware snapshot reverted and deleted to bring the VM back into the exact state it was in when the smart Copy was created.

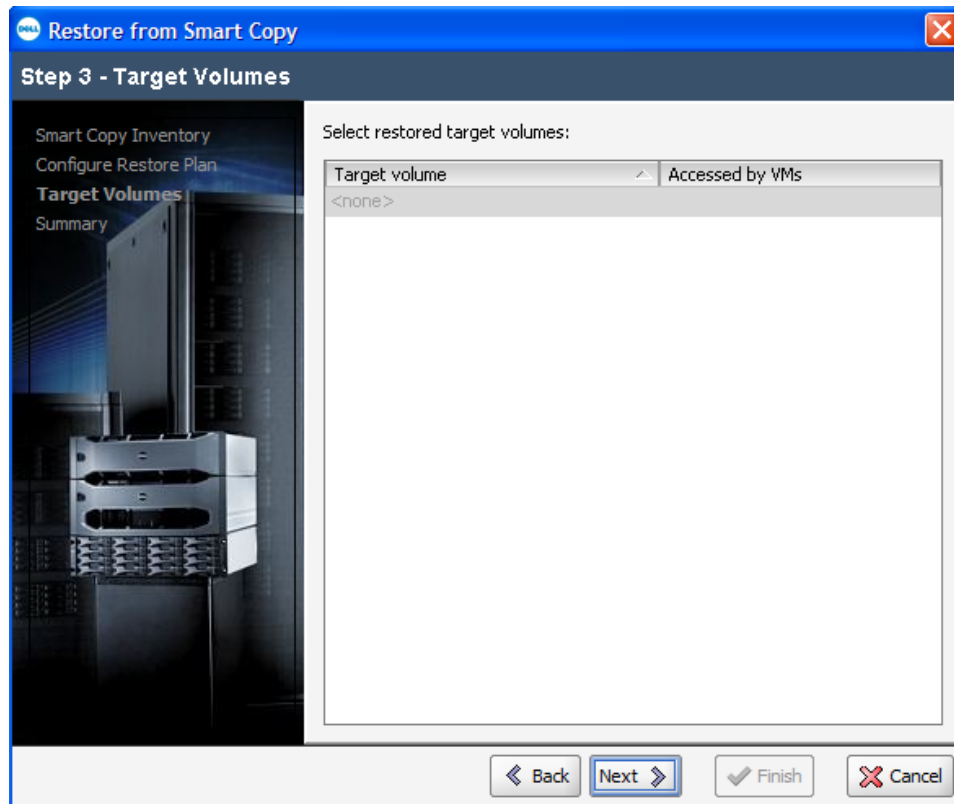
Select the restore action and click **Next**.



Step 3 - Target Volumes

If there are any iSCSI attached volumes as part of the Smart Copy these can also be selected for restoration. The iSCSI volume will be reverted to the PS Series snapshot.

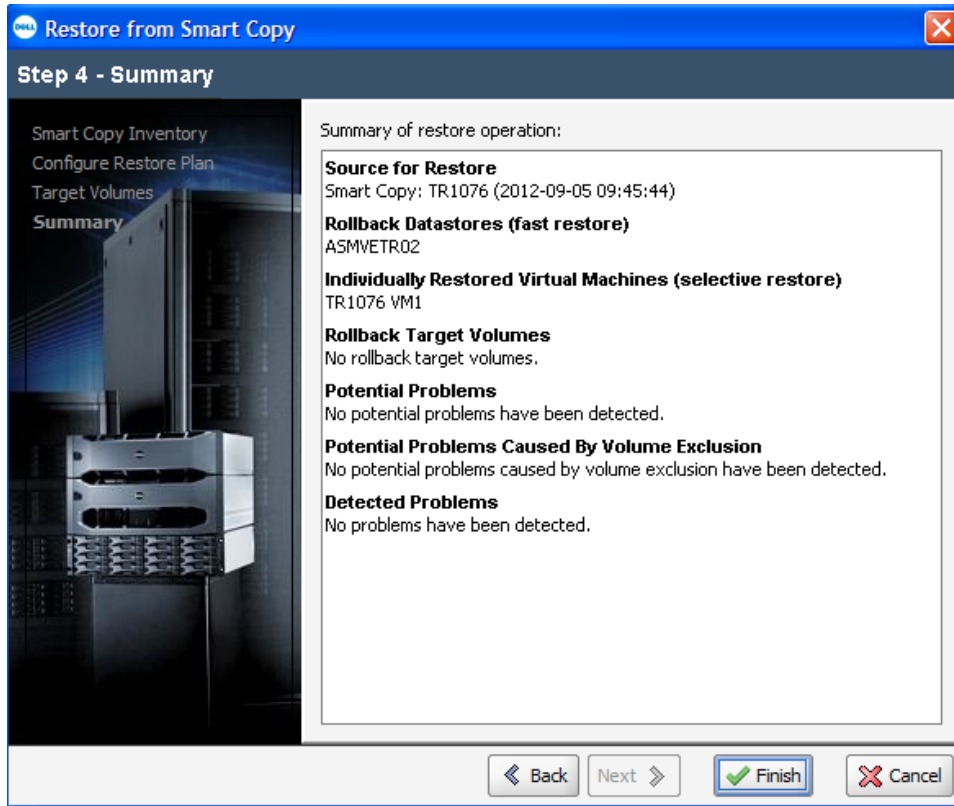
Select any target volumes to recover and click **Next**.



Step 4 - Summary

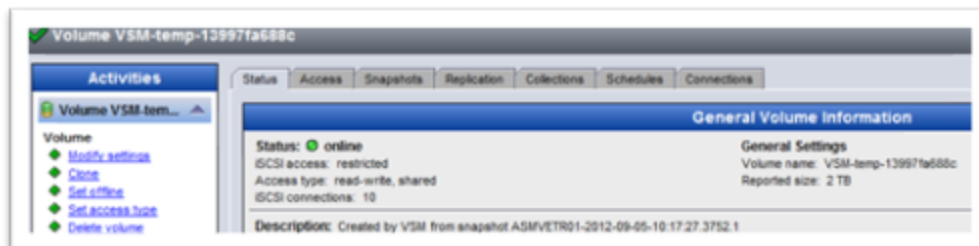
Verify all of the choices. If there are any VMs that are impacted because of a roll back they will be listed here along with any other detected issues.

Click **Finish** to begin the Smart Copy recovery process.











During the restore process you can monitor the progress in the Recent Tasks pane of the VSM GUI. During a restore by copy a new PS Series volume will appear that is the clone of the PS Series snapshot. It will be appended with VSM-temp. When vCenter rescans you will see a new datastore appended with snap- and the name of the base datastore. The volumes will be cleaned up and deleted after the restore by copy is completed.

NOTE: During a restore by rollback, the PS Series SAN will create a temporary snapshot of the volume with Description: "Snapshot from restore". This can be used to recovery from in case the rollback was incorrect or done in error. This snapshot will need to be manually cleaned up from Group Manager GUI after the rollback has been verified completed. This is listed as additional user tasks to complete in the tasks pane.



Example of VSM-Temp PS Series Volume for restore by copy

 SKYNETVOL1	 accessible	tekmtlab-10Gb
 SKYNETVOL2	 accessible	tekmtlab-10Gb
 SKYNETVOL3	 accessible	tekmtlab-10Gb
 snap-6d4becd9-A5MVETRO1	 accessible	tekmtlab-10Gb

Example of snap- datastore for restore by copy

After the restore is complete, you can see in the Job Results any additional user intervention that might need to be taken as well as any information or warnings.

Recent Tasks

Show Jobs: All jobs

Job	Status	Start time	End time
Restore from Smart C...	Completed with t...	9/5/12 3:48:45 PM	9/5/12 5:11:07 PM
Create Smart Copy of...	Success	9/5/12 3:35:50 PM	9/5/12 3:38:05 PM
Delete Smart Copy	Success	9/5/12 3:29:14 PM	9/5/12 3:29:18 PM
Verify Smart Copies	Completed with t...	9/5/12 3:28:51 PM	9/5/12 3:28:54 PM
Create Smart Copy of...	Success	9/5/12 3:22:02 PM	9/5/12 3:24:11 PM
Provision new databa...	Success	9/5/12 3:20:42 PM	9/5/12 3:22:02 PM

Job Tasks | Job Results

▶ ◆ **Status of restore operation: complete**

▼ ◆ **Smart Copy Summary (4)**

- ◆ Created: 2012-09-05 09:48:47
- ◆ Schedule: null
- ◆ Memory dump performed: yes
- ◆ iSCSI targets (volumes) accessed by VMs: included

▼ ◆ **Restored Volumes (1)**

- ◆ iqn.2001-05.com.equallogic:0-8a0906-7b25d4409-7bb92486c7b50461-asmvetr02: ASMVETR02-2012-09-05-10:17:27.3751.1

▼ ◆ **Fast Restored Virtual Machines (2)**

- ◆ TR1076 VM4: revert success
- ◆ TR1076 VM3: revert success

▼ ◆ **Selective Restored Virtual Machines (1)**

- ◆ TR1076 VM1: success

▼ ◆ **Emergency Snapshots Created (1)**

- ◆ ASMVETR01: ASMVETR01-2012-09-05-16:23:30.3768.1

▼ ◆ **Additional User Actions Required (1)**

- ◆ Verify restore has completed satisfactorily, remove any restore snapshots created by PS Series groups.

Close

Example Job Results

CREATING SMART CLONES

Creating clones in any environment can be very useful for a number of reasons. They allow you to quickly deploy multiple sets of virtual machines to either test configurations or create identical environments to use. VSM has the capability to not only clone running virtual machine environments but also create clones from previous Smart Copies. This allows the administrator to bring online copies of virtual machines from a prior point in time. This can be helpful for troubleshooting or side by side comparison of machines.

Another great use of Smart Copy Clones is the ability to test new software without impact to existing production machines. Typically an administrator might take a Smart Copy of a set of virtual machines and then upgrade the software. If this results in an outage or the software is incompatible, the administrator can roll back to a previous known good Smart Copy. However this can be disruptive as the environment will be unavailable during the restore. Creating brand new machines to test the software upgrade very rarely introduces the same issues that might come up with existing software builds. Another option an administrator can do is to bring online a clone of the virtual environment, isolate it from the production environment, and then run the upgrades and testing on the cloned environment. This way should anything negative occur, at no point is the production environment impacted.

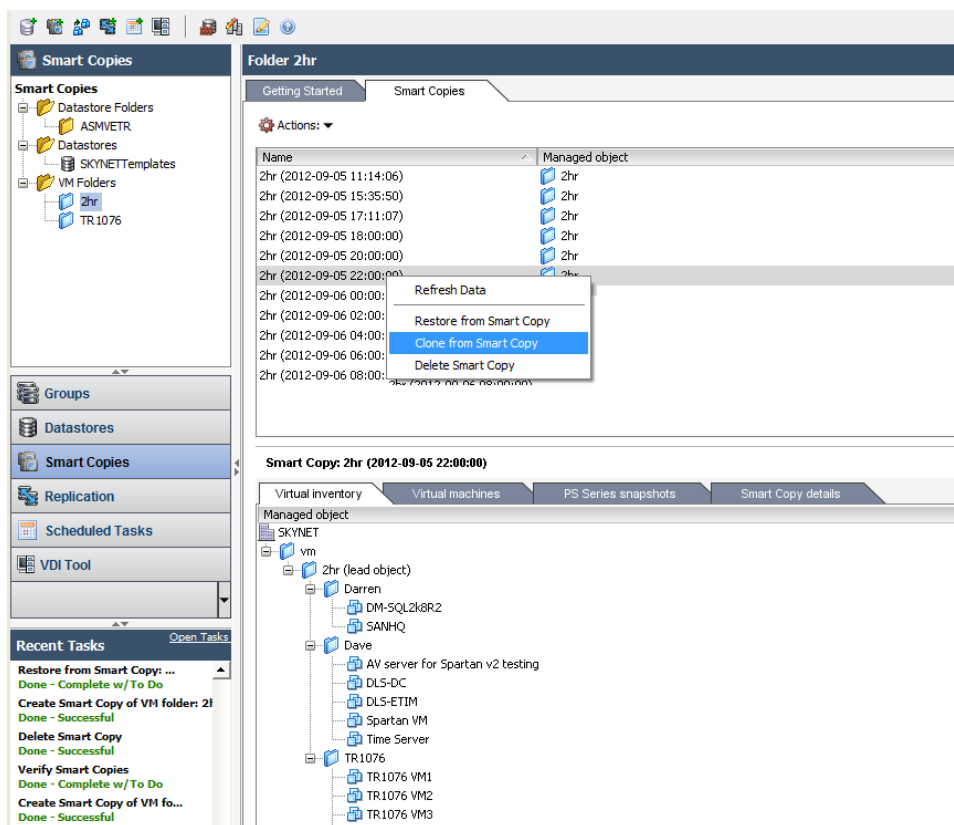
Clones can also be used when creating identical environments for testing and development environments, and when combined with the PS Series thin clone feature, can result in significant space savings. By taking a clone of several virtual machines residing on a datastore volume, the volume can be converted into a thin clone template and several space efficient copies of these VMs can be spun off and given to various developers. For more information on leveraging thin clones in your environment refer to technical report *TR1063 Dell EqualLogic PS Series Template Volumes and Thin Clones: How and When to Use them*.

It is very important to note that no matter what the reason is for utilizing clones, they are an exact match of the existing virtual machine. This means the hostname, the IP address, and the application namespace is identical. It is therefore vital that whenever a cloned virtual environment is brought online it is segmented from the production environment to avoid any conflict. This can be done with isolated virtual switches, networking changes or other methods.

NOTE: Virtual Machines which have drives spanning multiple datastore volumes are supported by Smart Copies. However during a clone operation these virtual machines will have the additional drive registration still pointing to the original volumes. This will cause conflicts without some manual configuration steps. It is recommended that any VMs that are desired to be cloned have all of their data residing on a single datastore volume to avoid any potential issues.

Smart Clones can be created from existing objects in vCenter in the exact same manner as creating a Smart Copy, or more commonly, can be created from previously run Smart Copies.

To create a Smart Clone from an existing Smart Copy open the VSM GUI and click the tool button Smart Copies. Select a Smart Copy object you wish to clone. In the right pane right click on the desired Smart Copy and select **Clone from Smart Copy**.



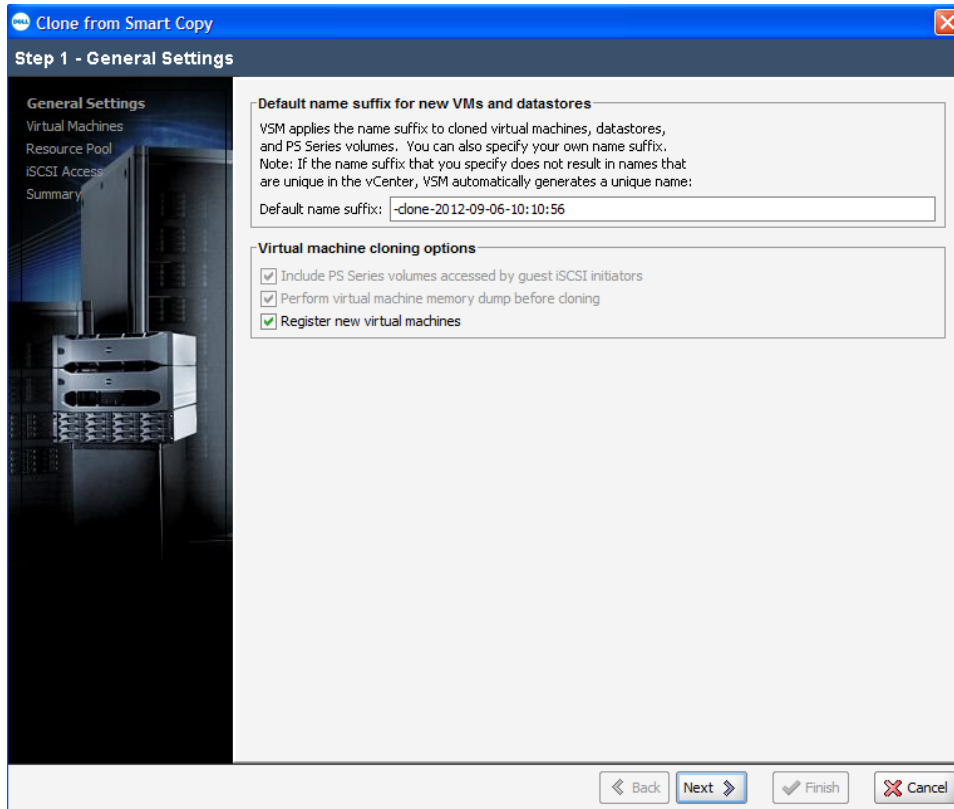
NOTE: The entire Smart Copy will be cloned and consume additional space for all of the datastore volumes that are part of the Smart Copy.

Step 1 - General Settings

The first page of the wizard will allow you to append a name to the datastores that will be cloned. This is needed as no two datastores can have the same name and also allows you to differentiate between the original datastore and the cloned datastore. By default it will append *-clone-date/time of smartcopy*.

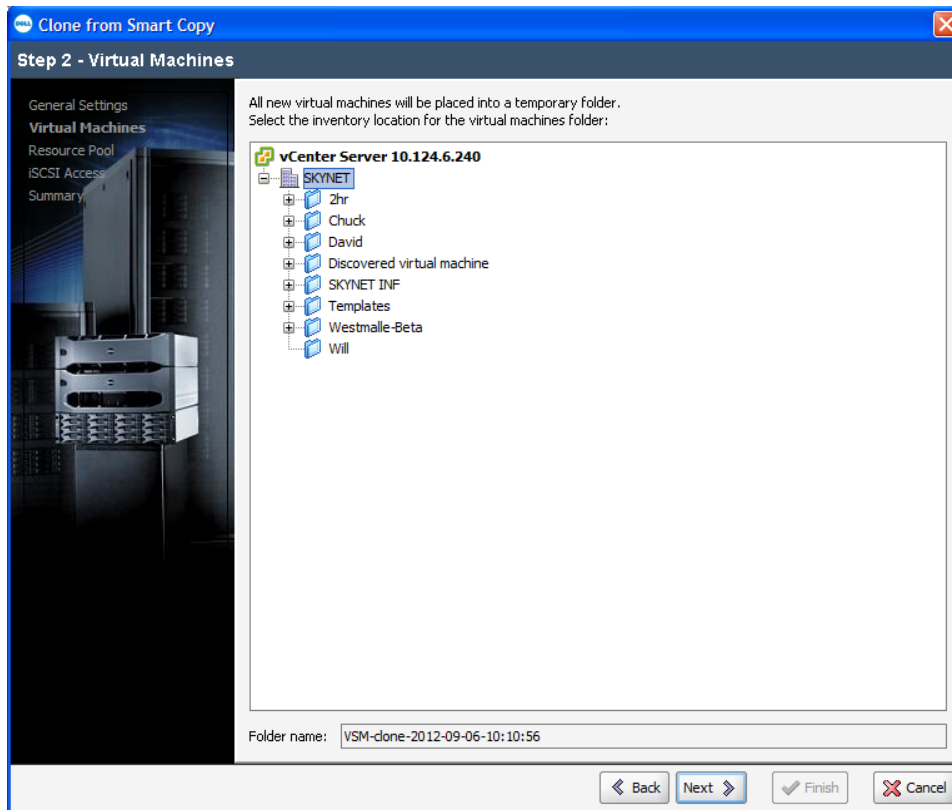
You can also choose to register the new virtual machines or not. This will come into play in the next section on advanced data recovery but generally it makes it easier to allow VSM to automatically register the VMs from the clone.

Make your selection and click **Next**.



Step 2 - Virtual Machines

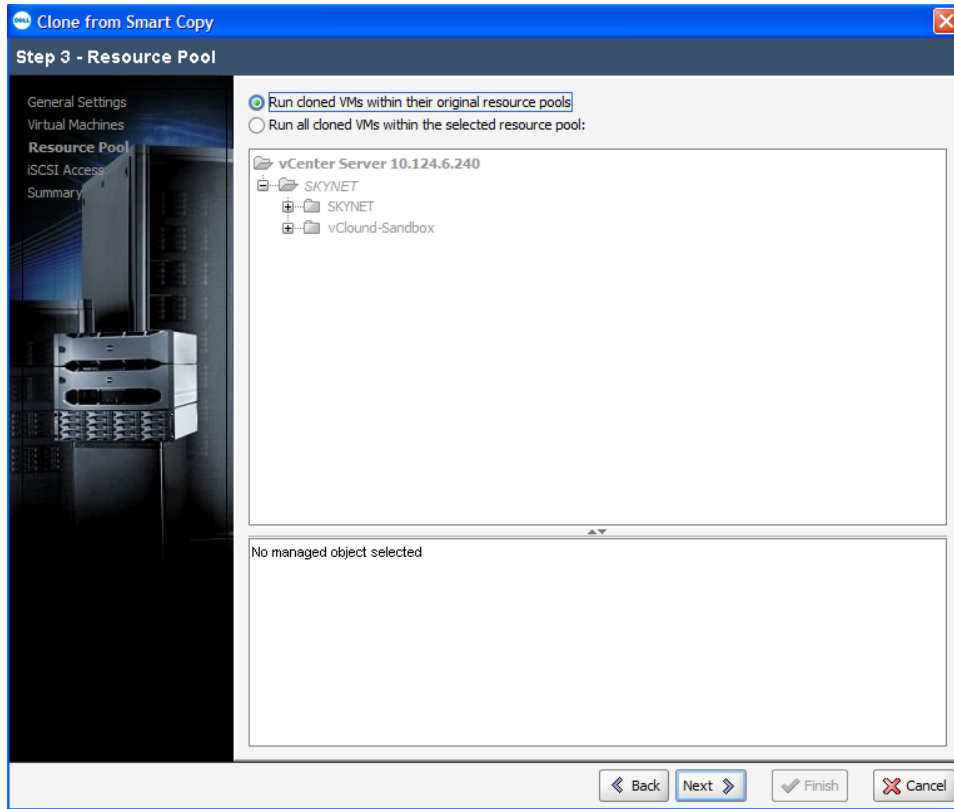
In the next page of the wizard, select the folder location for the newly cloned VMs. They will also have a unique name and timestamp of the Smart Copy. Select the inventory location and click **Next**.



Step 3 - Resource Pool

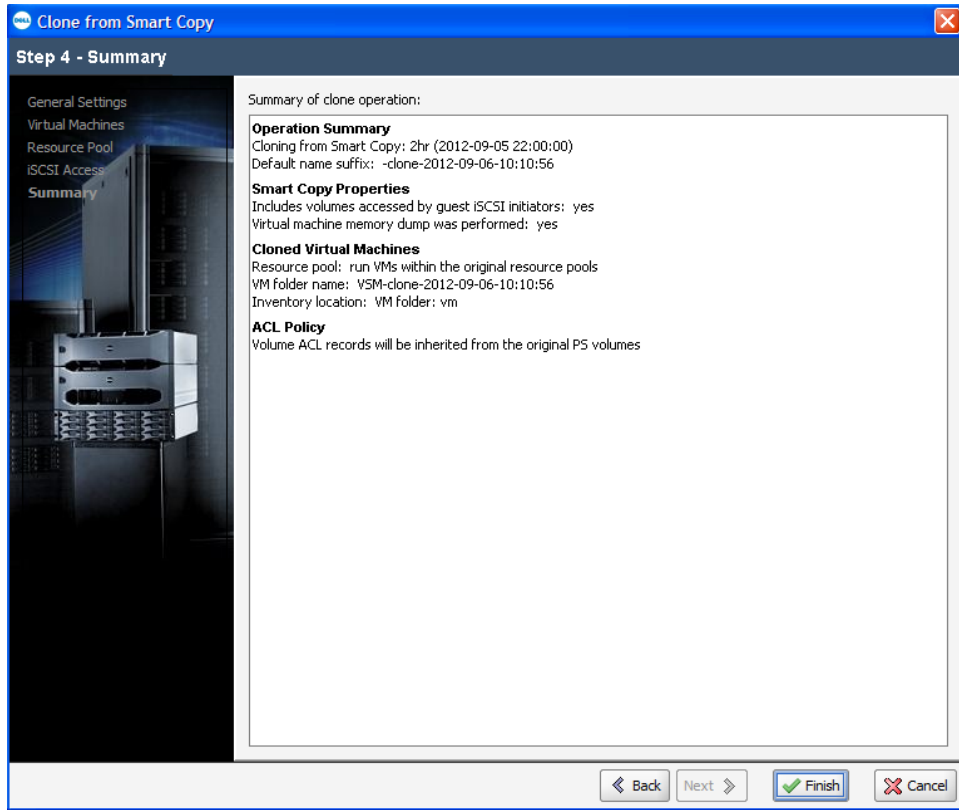
There may be times in which the cloned VMs should run in a different resource pool than the original. In this step you can choose to have the VMs run in the same resource pool as the original VMs, or have them draw their resources from a different resource pool.

Make your selection and click **Next**.



Step 4 - Summary

In the final page of the wizard verify all of the settings and click **Finish** to begin the cloning process.



During this time VSM will coordinate with the PS Series SAN and create volume clones of all of the snapshots that are part of the Smart Copy. Once these volumes are cloned VSM will tell vCenter to rescan and bring these new cloned volumes into the environment. Then depending on if you selected to register the VMs, VSM may register these VMs and assign them to the appropriate resource pool.

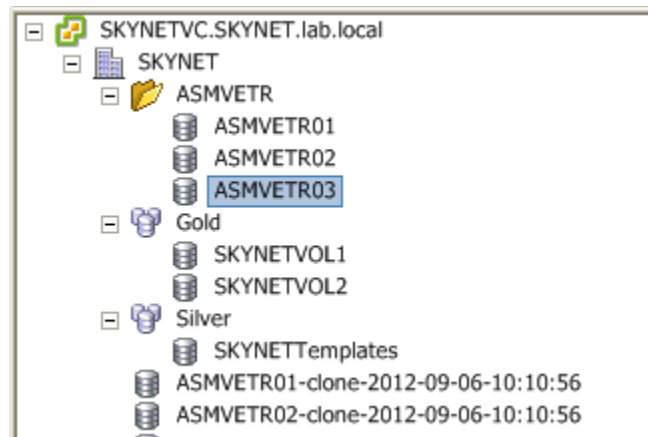
VSM will not power on any VMs. This is to protect the original VM environment. After this time depending on what the use case for the clone is, you can isolate the VMs and power them on.

NOTE: VMs will contain VMware snapshots and possibly memory state from the Smart Copy process. During the process VSM will not revert or delete these snapshots to protect the original VM. These snapshots need to be managed manually once the VMs are isolated.

You will see the new cloned volumes inside the PS Series Group Manager GUI as well as the new datastore volumes inside vCenter.



Cloned volumes inside PS Series Group Manager GUI




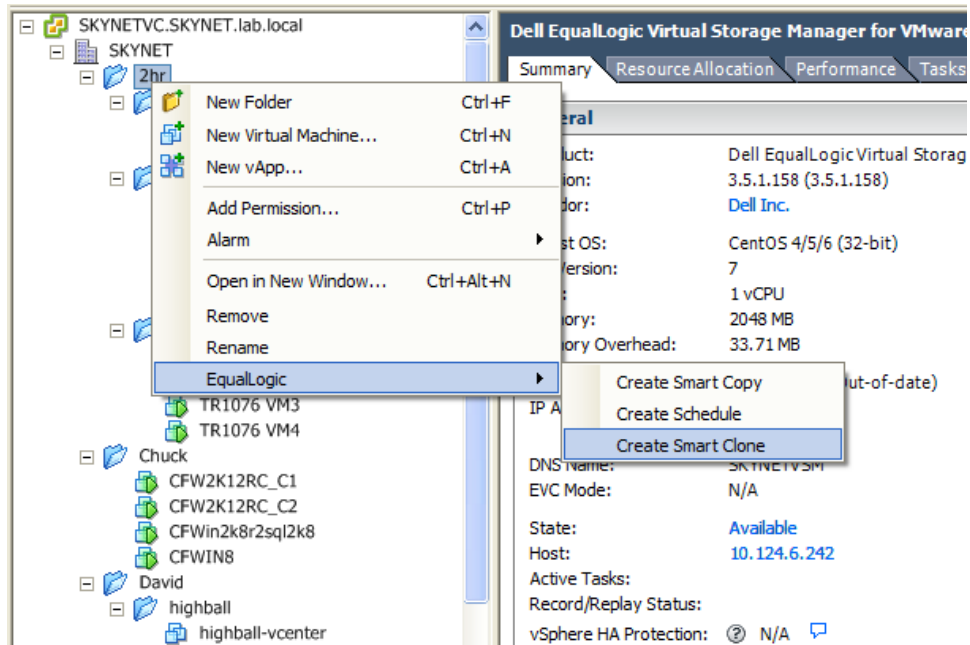
Cloned datastores in vCenter GUI

Smart Clones from vCenter environment

Occasionally you may wish to create a Smart Clone of existing virtual machines and not from a previously taken Smart Copy. The process is similar to taking a Smart Clone.

Just as there are multiple ways to take a Smart Copy there are the same options when taking a Smart Clone.

- From the VSM Main GUI - Click the toolbar shortcut icon for  **Create a Smart Clone**
- From within vCenter under the Hosts and Clusters view, Datastores and Datastore Clusters view or VMs and Templates view right click an object, select EqualLogic -> **Create Smart Clone**



This will launch the Smart Clone wizard but the managed object will need to be selected. If the wizard is launched from the shortcut toolbar button you have the option of selecting the managed object. If Create Smart Clone is launched through the vCenter UI on an object, as shown in the above screenshot, VSM will use that object for the Smart Clone.

From here the steps for creating a Smart Clone of a running environment versus creating one from a previous Smart Copy, as previously documented, are identical.

Monitor the VSM Recent Tasks to see when the Smart Clone is complete. When the Smart Clone has completed additional tasks can then be done such as the isolation of the networks and reverting the VMware snapshot data.

ADVANCED CLONING - SELECTIVE DATA RECOVERY

There are some times when data restoration needs to be more granular than at the individual datastore or even at the individual virtual machine level. The idea behind selective data recovery is creating Smart Clones from existing Smart Copies and bringing this information online and then attaching the data drive of the VM from the Smart Copy back to the original VM. Using clones for this is recommended verses bringing a Smart Copy online. As by taking a clone of the Smart Copy, the original PS Series snapshot data is not modified. If you set online the original PS Series snapshot, the data integrity for recovery could be changed by accident if information on that read/write snapshot is deleted or altered.

There are multiple options for selective data recovery but they all revolve around mounting a point in time version of the data disk to a VM; usually the original VM. In order for this to work the VM's OS must support the ability to

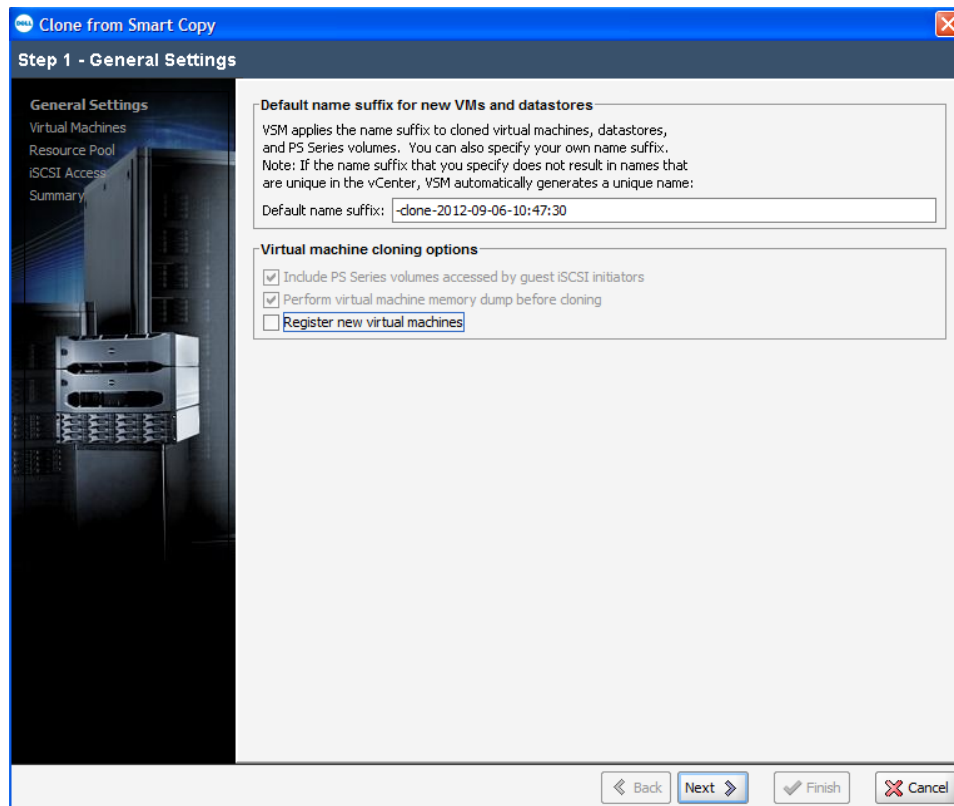
hot add data disks. The other option is to have a temporary or standby recovery VM available that can have data drives mounted to it and then used to find the files to recover and copy them back to the original location.

The process is very similar to creating a Smart Clone but with some additional steps. First find the Smart Copy that contains the data that needs to be recovered. Choose to **Clone from Smart Copy**.

Step 1 - General Settings

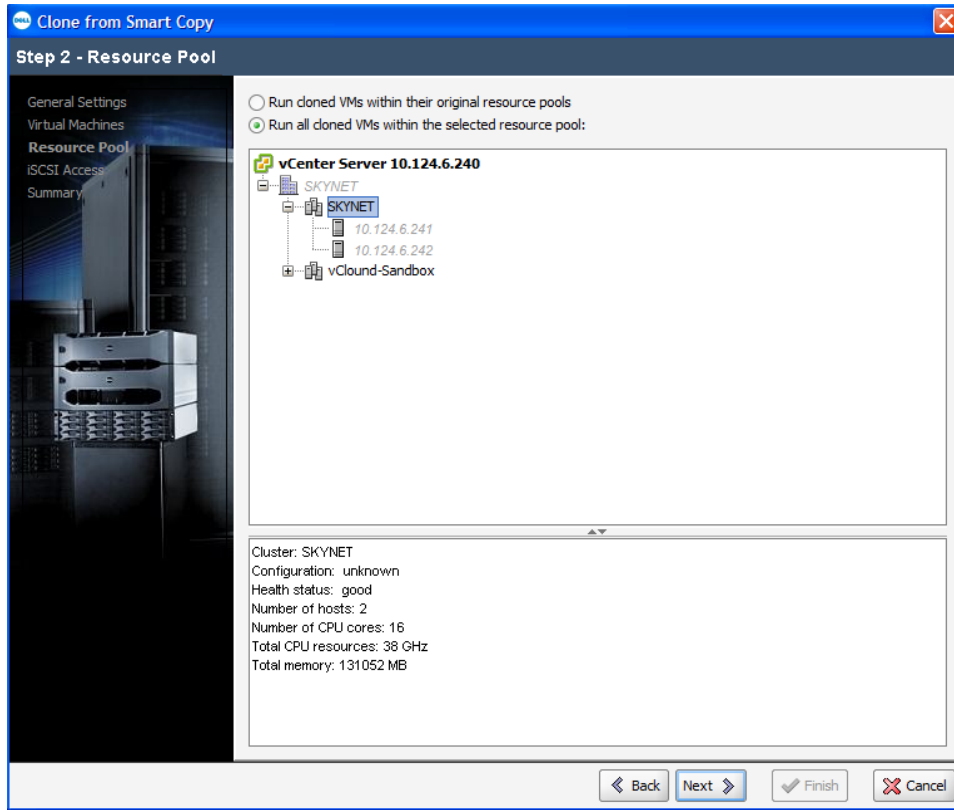
Unlike creating a full clone of a Smart Copy, deselect the option to **Register new virtual machines**. It is not necessary to register the VMs for selective data restoration. Click **Next** to continue.

NOTE: Even if you are trying to restore just one file, the Smart Clone operation could cause multiple datastores to be cloned and mounted. These will need to be deleted using Datastore Manager when the process is finished.



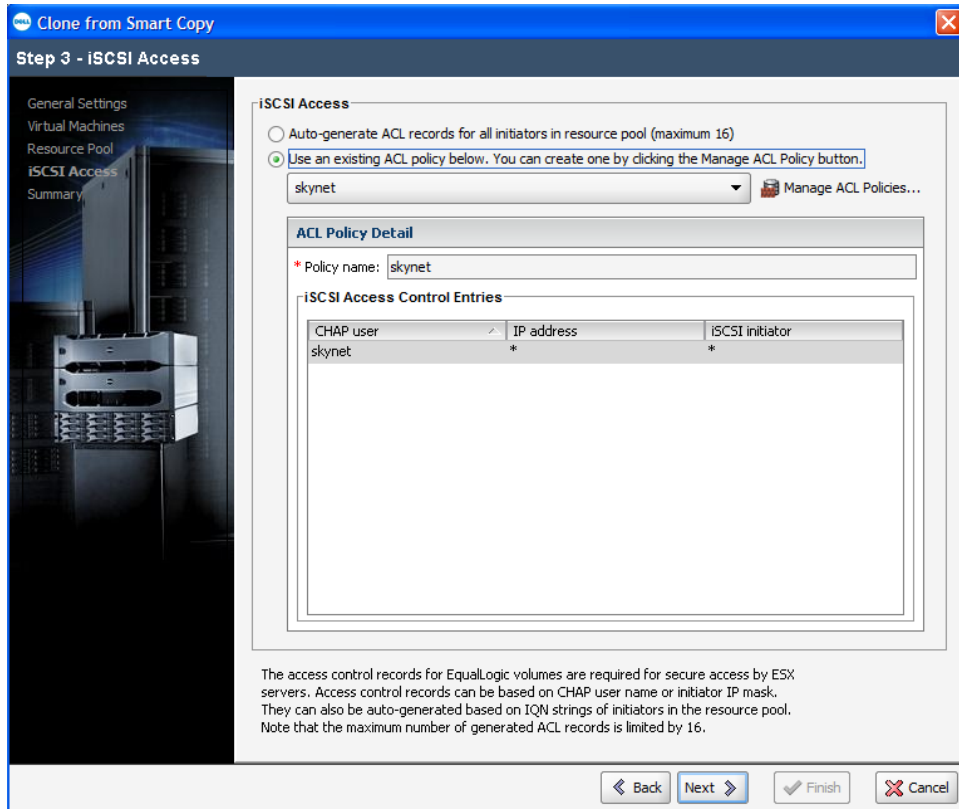
Step 2 - Resource Pool

Select the vCenter cluster to assign the cloned datastores to and click **Next**.



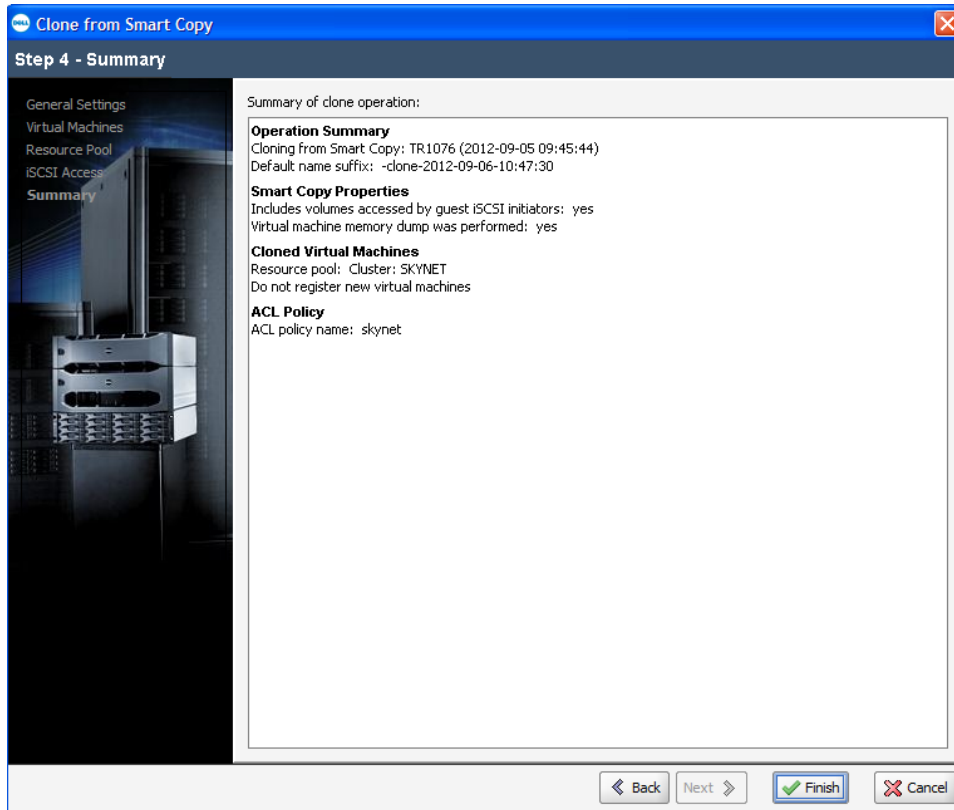
Step 3 - iSCSI Access

Choose to Auto-Generate ACL records or use an ACL policy to assign to the cloned volumes to ensure that the designated cluster can rescan and see the volumes. For more information on creating and using ACL policies see *TR1067 EqualLogic Virtual Storage Manager: Installation Considerations and Datastore Manager*. Select the iSCSI Access and click **Next**.



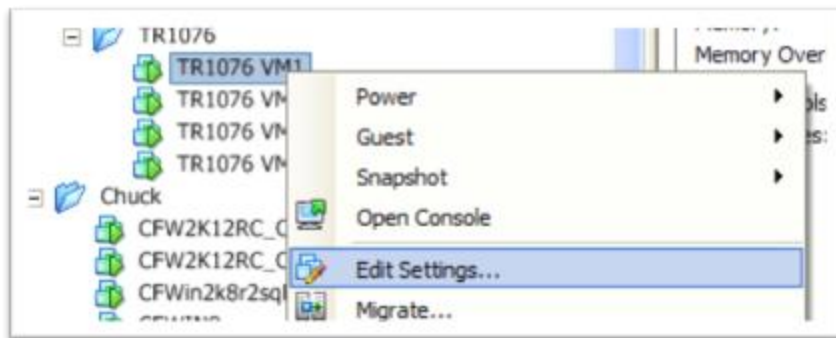
Step 4 - Summary

Verify the clone settings and click **Finish**. This will create clones on the PS Series SAN of all of the datastore volumes associated with the Smart Copy. Then it will rescan the vCenter cluster that was designated.



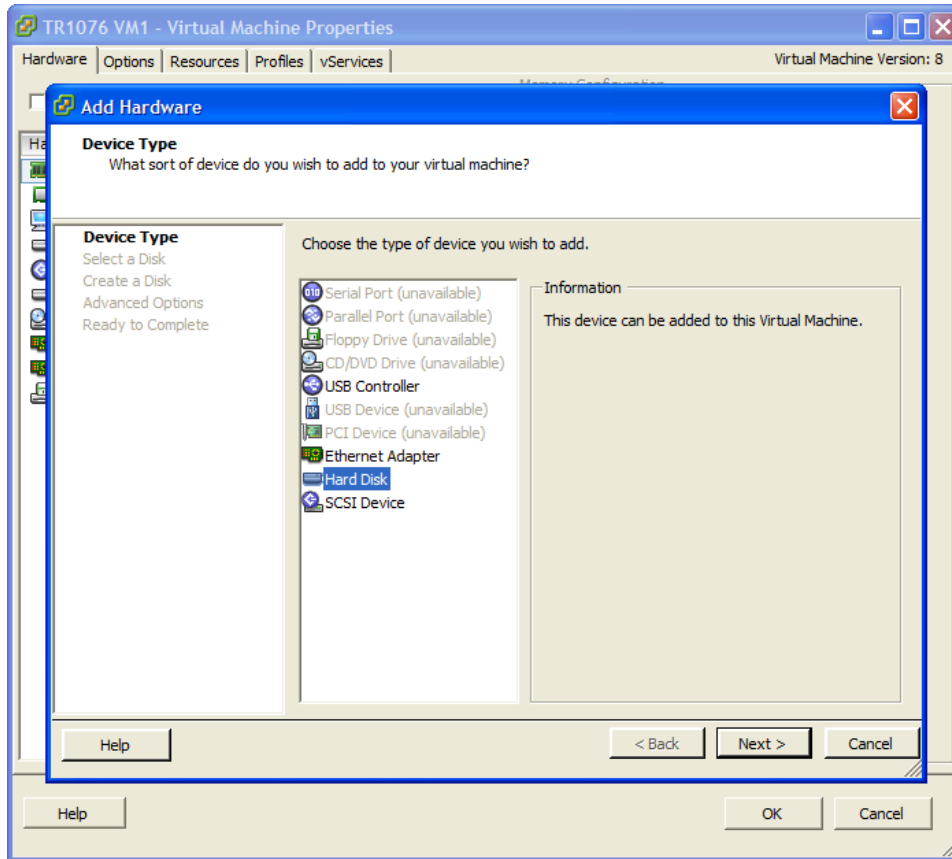
Step 5 - Edit VM

After this is done you can continue with attaching the data drive to the initial VM or recovery VM. Once the datastores have been cloned and are seen by vCenter right click on the VM that will be receiving the recovery data disk and click **Edit Settings**.

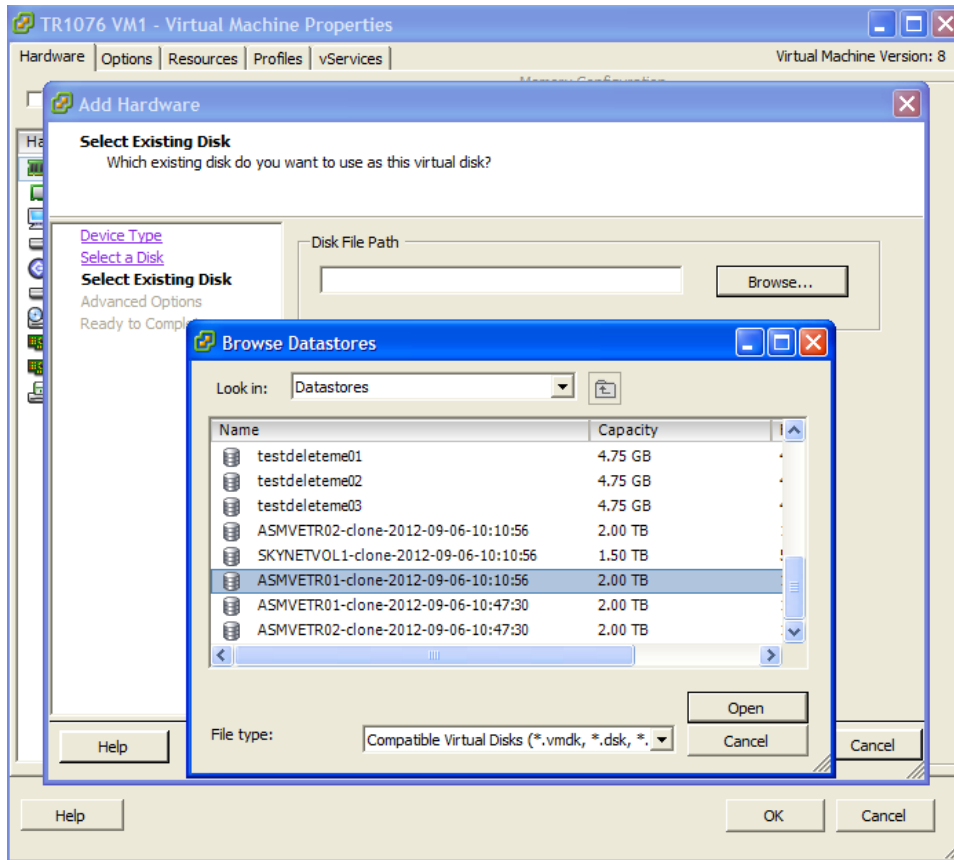


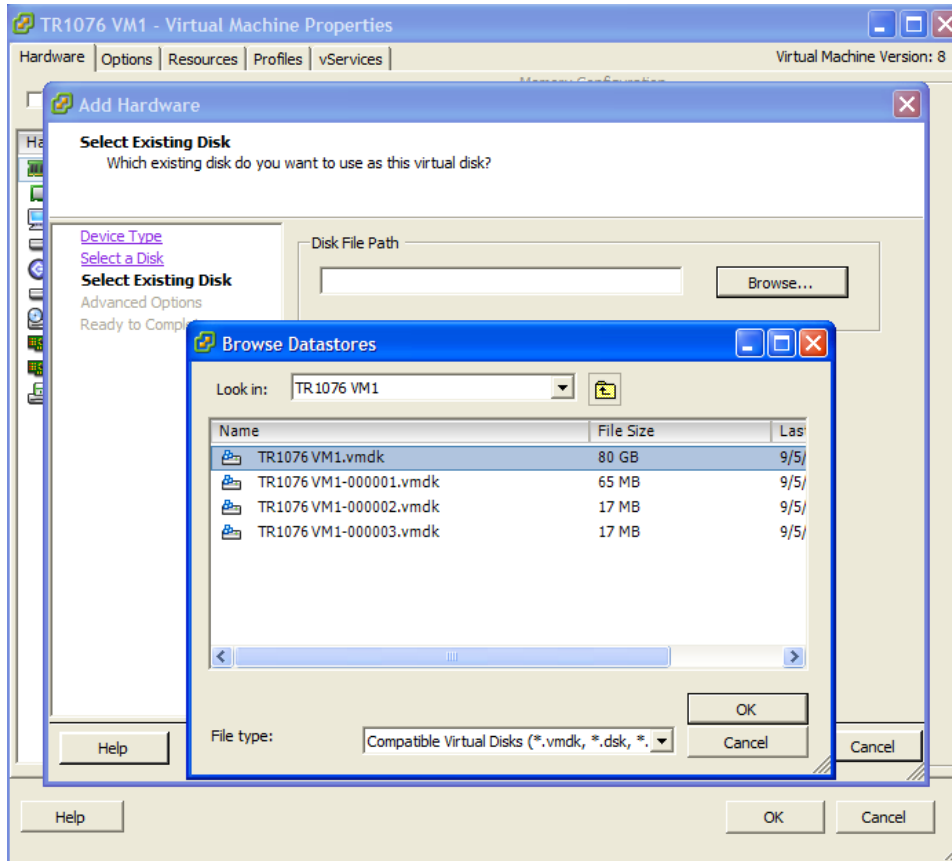
Step 6 - Attach Disk

The next step is to add an existing hard disk to the VM pointing to the snapshot datastore. Click Add Hardware and select Hard Disk and click **Next**.

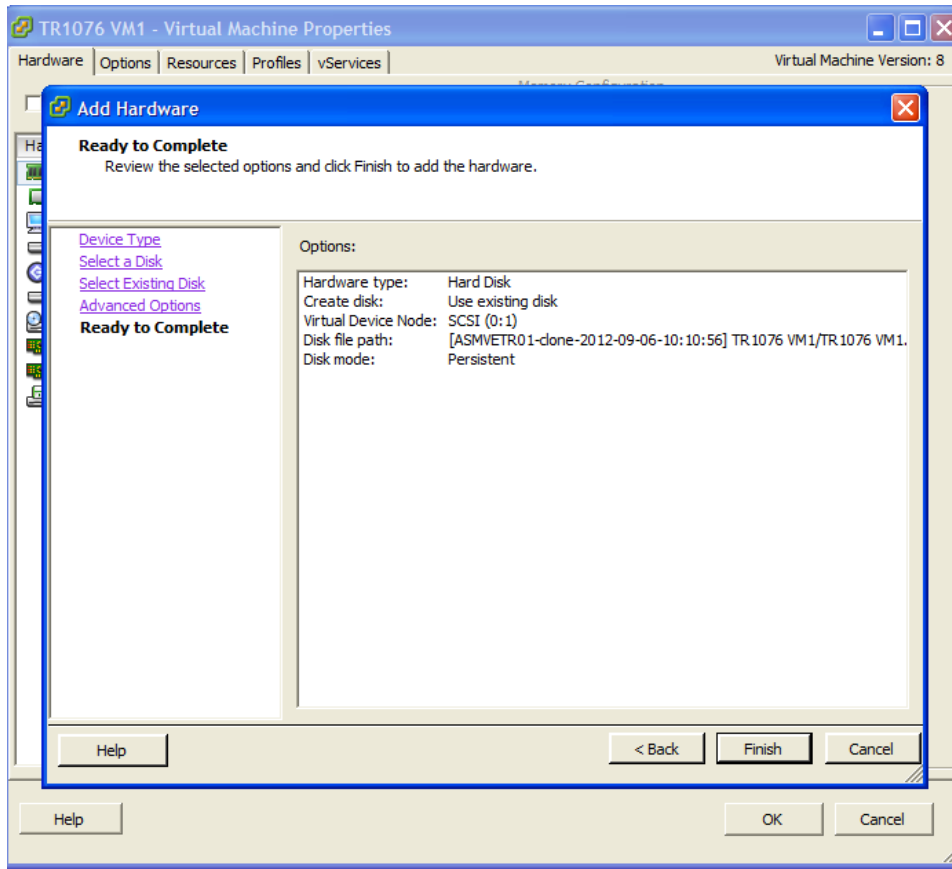


Choose to Use an existing virtual disk and click **Next**. Click **Browse** and browse to the cloned datastore that has the data disk. Select the datastore, and click **Open**. Browse to the Virtual Machine folder and select the data disk .vmdk you wish to attach. Click **Ok**.

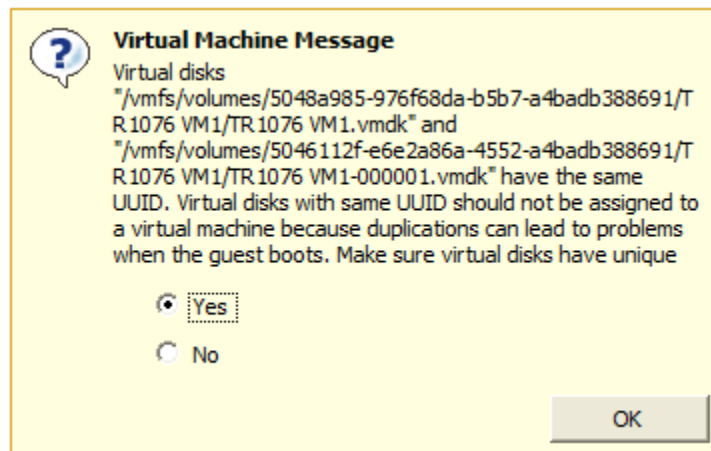




Keep the defaults for the virtual disk and click **Next**. Normally in persistent data drives you would configure a different virtualized SCSI adapter but in a recovery scenario the defaults are sufficient. Verify all the settings and click **Finish**. Click **Ok** to finalize adding the virtual disk to the VM.



NOTE: You might receive a virtual machine message about this disk having the same UUID. During the recovery process this disk will not exist long so you can continue adding it and removing it after the recovery process. If you plan on keeping the recovery volume around for a period of time including a reboot of the recovery VM, choose a new UUID for it.



Step 7 - Recover Data

Once the recovery data disk has been mounted to the VM, utilize the native OS tools to recover the data. For example, in Windows 2008R2, first open up disk management. Online the disk and it will assign a drive letter to that disk. After the drive letter is assigned, browse that drive letter and it will be the version of the original data drive from the point in time that the Smart Copy was taken. Copy or move the files or data that need to be recovered inside the VM. If using a recovery VM move the files back to the original VM via the network or some other process.

Step 8 - Cleanup

Once the files have been recovered there are some steps that need to be taken to clean up the environment.

Remove the hard disk that was added by editing the VM settings and removing it. If the VM or recovery VM does not support hot add/remove the VM will need to be powered off to remove the hard disk.

Use VSM Datastore Manager to delete all of the clone volumes that were created during the recovery process. These clones will be listed in the completed task for the clone. This will ensure proper removal of iSCSI targets and the deletion of PS Series cloned volumes.

MULTILAYERD DATA PROTECTION APPROACH AND DATA PLACEMENT

Dell EqualLogic PS Series SANs are tightly integrated with vSphere through the Virtual Storage Manager and with features such as Smart Copies to provide an additional layer of protection by offering hypervisor-aware snapshots for virtual machines. These tools and techniques are designed to enhance an organization's existing data protection or business continuance strategies and work in conjunction with other solutions such as traditional backup techniques as well as the Dell EqualLogic Auto-Snapshot Manager/Microsoft Edition inside Windows VMs to protect SQL, SharePoint and Exchange data or Auto-Snapshot Manager/Linux Edition to protect Linux data drives.

Leveraging all of these tools together though requires a new approach to data protection and data placement. It is worth noting again that the snapshot within the PS Series SAN is still done at the volume level even if the object in vCenter is a folder or a subset of VMs. This means that to meet the SLA and RTO of a particular set of VMs, they should all reside together in the same protection scheme. During VM deployment another decision needs to be made. Where does this VM go so that it can have the required protection options and service level for recovery? As you build out your data protection scenarios it will be easier to decide which tier a particular VM falls into and then once these tiers are set up and configured either by folders or datastores, VM placement will be easier. In addition to meeting SLAs, VM placement will also have an effect on local PS Series snapshot space. Whenever a VM is moved using migrate or storage vMotion, the SAN keeps track of this movement as it is

seen as new writes. Leveraging Storage DRS (sDRS) or constantly moving VMs from one volume to another could dramatically increase the amount of snapshot space consumed on the SAN to keep track of this movement.

VSM Smart Copies can also be used in conjunction with a variety of the other Dell EqualLogic host integration tools for more granular protection of the application data within the virtual machine.

SUMMARY

The Dell EqualLogic Virtual Storage Manager is a vCenter plug-in that provides a whole suite of tools in managing and protecting virtualized environments. By leveraging VSM Smart Copies for local data protection, environments can augment their existing backup strategies to provide a much finer window of recovery. As businesses are growing their virtual infrastructures, tools like VSM are needed to keep up with the growth and provide manageable recovery points and data protection.

Technical Support and Customer Service

Dell support service is available to answer your questions about PS Series SAN arrays.

Contacting Dell

1. If you have an Express Service Code, have it ready.
The code helps the Dell automated support telephone system direct your call more efficiently.
2. If you are a customer in the United States or Canada in need of technical support, call 1-800-945-3355. If not, go to Step 3.
3. Visit support.equallogic.com.
4. Log in, or click "Create Account" to request a new support account.
5. At the top right, click "Contact Us," and call the phone number or select the link for the type of support you need.

Warranty Information

The MODEL array warranty is included in the shipping box. For information about registering a warranty, visit <http://support.dell.com/EqualLogic>.