Virtual Machine Protection with Dell EqualLogic Virtual Storage Manager v4.0

This Technical Report focuses on the usage of the Dell™ EqualLogic™ Virtual Storage Manager v4.0 to coordinate VMware™ aware snapshots and PS Series SAN snapshots to provide an additional layer of data protection and recovery.

Dell Storage Engineering
March 2014

A Dell Deployment and Configuration Guide

Revisions

Date	Description
March 2014	Initial release

Table of contents

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 v4.0 to create and coordinate hypervisor-aware snapshots for data protection and recovery. Throughout this technical report, examples are given for setting up and configuring snapshots and schedules as well as instructions on data recovery and other advanced options.

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

1 Introduction

VMware virtualization solutions and EqualLogic PS Series SAN storage allow datacenters 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 block level 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 VSM Snapshot.

The Dell Virtual Storage Manager v4 (VSM) is the next generation of VMware vCenter plug-ins that allow 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:

- VSM Datastores: Provides features to provision, expand, delete and monitor EqualLogic datastores.
- VSM Snapshots and Replication: Allow the creation of hypervisor consistent snapshots, clones and replicas for data protection and disaster recovery.
- 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 focuses on VSM Snapshots 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 present and application support from VMware. Administrators are leveraging snapshots on a daily basis to help augment their already existing backup strategies. This can be useful in testing, protection prior to an upgrade, or even as a fast recovery tool for mission critical VMs.

Note: 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" at *http://kb.vmware.com/kb/1015180.*

2 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. Imported as an OFV into vCenter, VSM is available directly through the vCenter Web UI screen. VSM 4.0 will only work with the vCenter Web UI for ESX 5.1 and 5.5 environments.

For installation and configuration of the VSM appliance, refer to *TR1101 EqualLogic Virtual Storage Manager: Installation Considerations and Datastore Management*.

In order for VSM to protect virtual machines residing on datastores, the PS Series group where the datastores reside must be added to the VSM group inventory. VSM 4.0 has support for multiple groups. As long as each group is managed by VSM, they can be included in snapshot operations.

3 Launching VSM for local protection

Once the VSM appliance is installed and running in the environment there will be a new icon labeled **Dell Virtual Storage Manager** in the vCenter Web UI in the **Inventories** section under **Home**.

Throughout this document the term VSM Snapshot refers 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 Web UI. In the Hosts and Clusters view, right clicking on an object in the left pane reveals a new **All Dell VSM Actions** menu with all of the available relevant tasks. These EqualLogic menu options show up throughout the vCenter Web UI whenever a EqualLogic VSM related task can be performed. There are multiple points where the VSM data-protection wizards are accessible. All achieve the same result, and all are based on ease of use and comfort with the tools.

To launch the VSM GUI and manage or monitor snapshots, click on the **Dell Virtual Storage Manager** icon in the **Inventories** section of the **Home** screen.

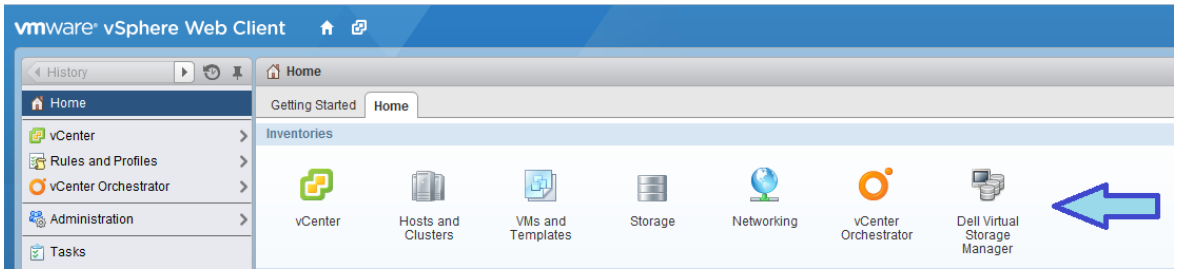


Figure 1 vCenter inventories

Options available from this screen include launching all of the views within VSM; managing and monitoring datastores, snapshots and replicas. This technical report focuses on local virtual machine data protection with snapshots.

4 Protection with VSM snapshots

As discussed in the Introduction, a VSM Snapshot 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 I/O to the virtual machine VMDK files and, if possible, quiesces the application inside the VM. The level of application consistency is based on 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 that the same consistency is obtained 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.

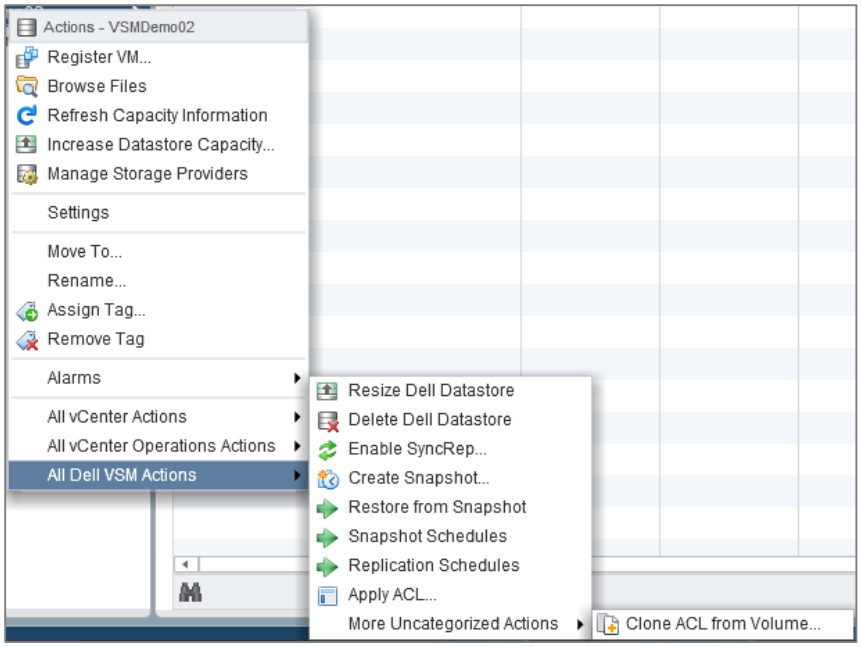
There are multiple ways to launch the Create Snapshot wizard. This flexibility in design allows each of the various features to be launched from a variety of places including objects in Hosts and Clusters view, VMs and Templates view, and Storage view.

The supported objects for a VSM Snapshot are: VM, VM Folder, Datastore, Datastore Folder, and Datastore Cluster.

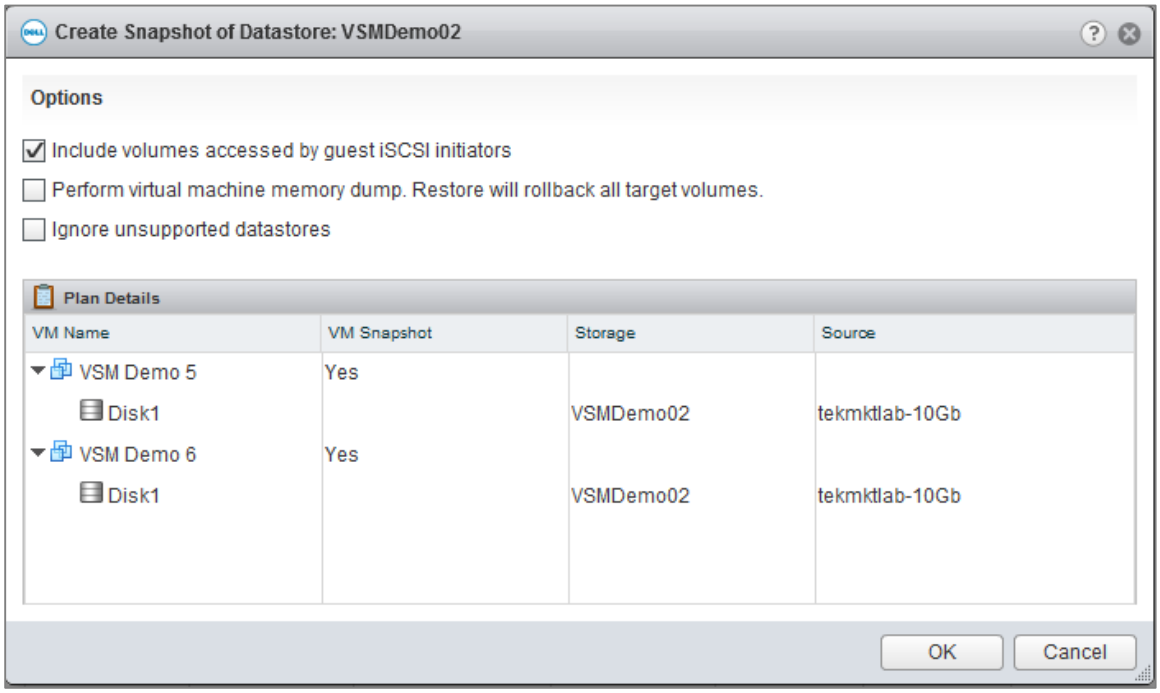
4.1 Creating a snapshot

All of the available actions for a particular object appear in the right click menu of any supported object, **All Del VSM Actions** is listed at the bottom of the menu.

1. Select an object and click **All Dell VSM Actions** > **Create Snapshot t**o take a VSM snapshot.



The **Create Snapshot** wizard is displayed.



The snapshot options displayed are optional parameters that can be selected for the snapshot. These options apply to all VMs included in the Snapshot.

- **Include 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 them in the snapshot. 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 is written to a 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. This problem is especially true if the VM is only being captured a few times a day, making the memory state almost useless. Consider this process and potential impact during the creation of snapshots with virtual machine memory dump option enabled.

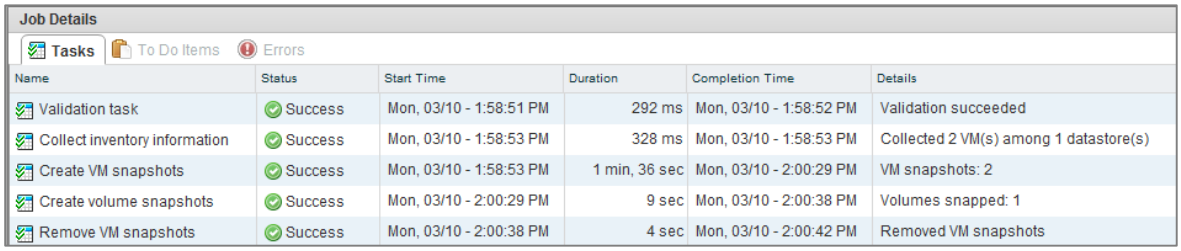
- **Ignore unsupported datastores:** Choose this option to continue the snapshot operation regardless of any unsupported datastores. The job history log will indicate which VMs could potentially be affected. This is important because a VM that spans between supported and unsupported datastores would result in that VM becoming non-recoverable.

- **Plan details:** The Plan details pane lists all of the virtual machines that will be affected by the snapshot. Information such as which group and volume it resides on, as well as any discovered problems, are listed here.

2. Make a selection and click **OK** to create the snapshot.

   During the Snapshot process, each of the VMs are placed into VMware snapshot mode, quiescing the virtual machine (if VMtools are installed). Once the VM snapshots are created, VSM coordinates PS Series snapshots for each of the included PS Series volumes. When the PS Series snapshots are completed, VSM deletes the VMware snapshots associated with the snapshot. This does not delete existing VMware snapshots on the VMs, just the ones created for the snapshot.

3. The job details log lists all of the steps taken and the results.



Inside the Group Manager GUI, the associated PS Series volumes have a new snapshot created and the description reads, "Created by Auto-Snapshot Manager/VMware Edition".

5 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 enables protecting folders of virtual machines and folders of datastores to allow scaling and adding protected objects without constantly having to adjust 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 snapshot. VSM queries to see which VMs are in the folder, which PS Series volumes the VMs reside on, and then takes a snapshot of the entire set. This keeps web server farms consistent or file servers coordinated in their protection.

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

These VM folders, datastore folders, and even datastore clusters can be selected as the object of a snapshot. More importantly, protection schemes can be scheduled around them.

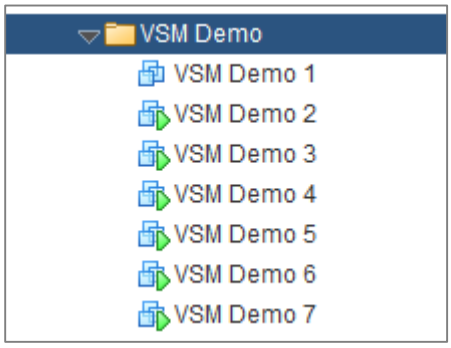


Figure 2 Example of folders in vCenter for protection

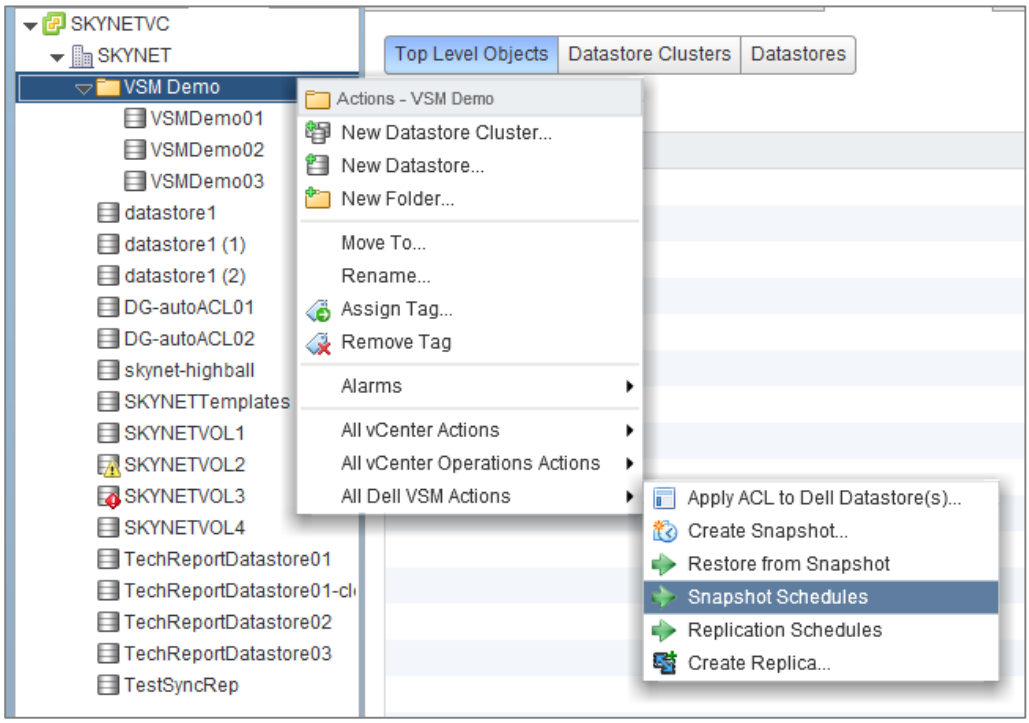
6 Automating protection with schedules

Individual snapshots 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 snapshot taken can also have a schedule created to automate the process. VMs, folders, datastores and datastore folders, and datastore clusters can be scheduled for snapshots.

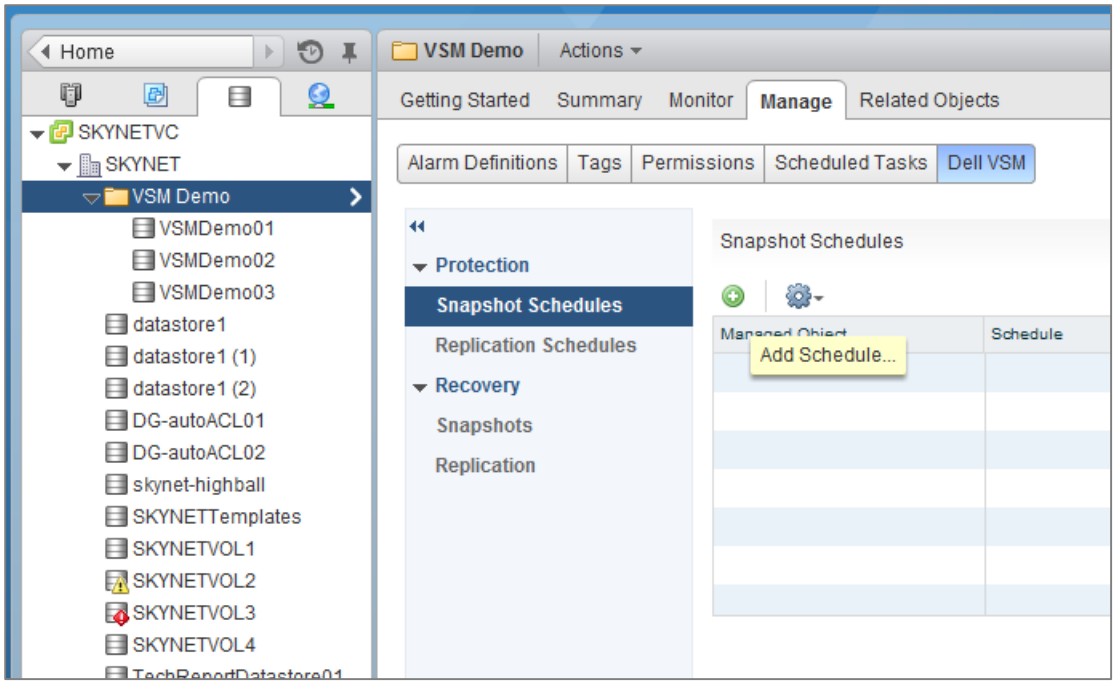
Schedules allow tiering of protection levels for VMs. The administrator can have different schedules for different folders or different datastores, depending on the needs of those VMs. When a new VM is created, it can fall under a certain tier of protection and the administrator doesn't have to adjust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

Creating a snapshot schedule is done in the same way that a standard snapshot is created. Two methods for completing this task are:

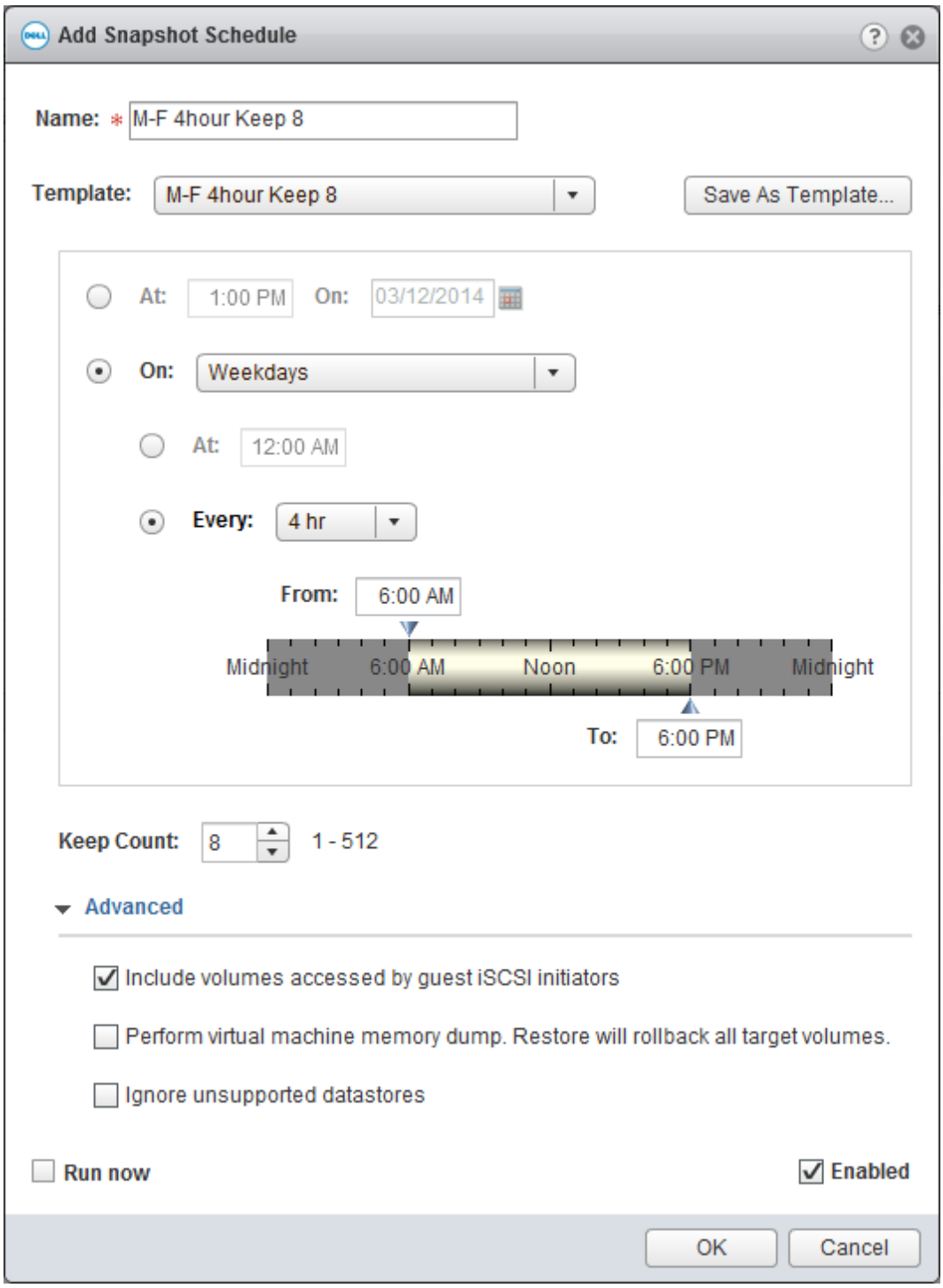
- Right click on an object and then click **All Dell VSM Actions** > **Snapshot Schedules**.
- Click on the object, click the **Manage** tab, and then the **Dell VSM** tab. Under **Snapshot Schedules** click the green + symbol to add a new schedule and launch the **Add Snapshot Schedule** wizard.



Either method displays the Snapshot Schedules for that particular object.


Home
VSM Demo
Actions
Getting Started
Summary
Monitor
Manage
Related Objects
SKYNETVC
SKYNET
VSM Demo
VSMDemo01
VSMDemo02
VSMDemo03
datastore1
datastore1 (1)
datastore1 (2)
DG-autoACL01
DG-autoACL02
skynet-highball
SKYNETTemplates
SKYNETVOL1
SKYNETVOL2
SKYNETVOL3
SKYNETVOL4
Alarm Definitions
Tags
Permissions
Scheduled Tasks
Dell VSM
Protection
Snapshot Schedules
Replication Schedules
Recovery
Snapshots
Replication
Snapshot Schedules
Schedule
Add Schedule...

6.1 Add Snapshot Schedule wizard



1. First give the snapshot schedule a meaningful name.

VSM automatically populates the **Name** field with the object description, but you can change this if you plan on applying it to other objects.

2. If having the same schedule applied to mulitple types of objects is planned, save it as a template and then apply that later to any other object.

   Templates are a useful tool for managing different types of schedules. VSM comes with a few example templates: Business Hours every hour, Weekly Snapshot, and Gold 2hr. These can be modified or used as examples for creating new protection schemes.

3. In this example, protection is established for the datastore folder, VSM Demo, that contains the three datastores (VSMDemo01, VSMDemo02, and VSMDemo03). A four hour schedule that keeps the past 8 copies is created, and it runs from 6am to 6pm. This means a snapshot is received at 6am, 10am, 2pm, and 6pm and then kept for two days. for the schedule is repeated Monday through Friday.

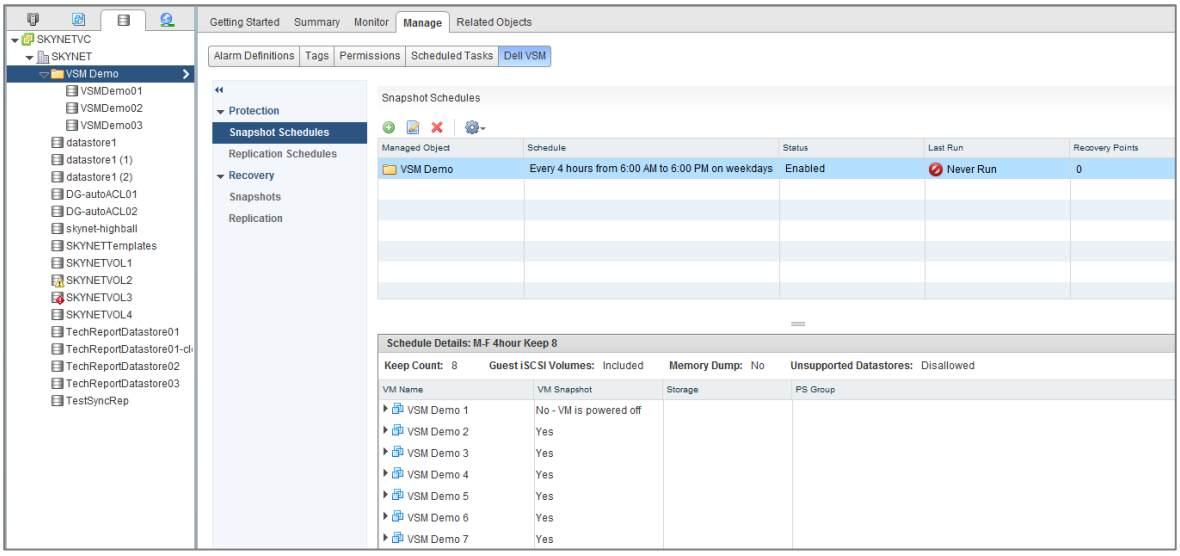
   With the power of schedules, multiple layers of point in time protection for various objects can be created. The great thing about using the schedule on the datastore folder is that any new VM provisioned to those datastores automatically inherits the protection from the schedule without administrator intervention.

   In the advanced options, administrators get the same options for a standard snapshot.

4. The schedule is ready to run and can also be enabled or disabled.
5. Make a selection, and then click **OK**.

   This places the schedule in the list under **Snapshot Schedules**.

6. At this time, more schedules can be applied to this object. In addition, the number of times the snapshot schedule has been run and the objects inside it can be displayed.



Note: With EqualLogic PS Series Firmware version 6.x, snapshot borrowing on the volume can be enabled to allow borrowing unused snapshot space from another volume or from the free pool space. This allows the retention policy to be met in the event that the volume does not have sufficient snapshot reserve. For more information on snapshot borrowing, refer to tech report, TR1084: EqualLogic PS Series Architecture: Snapshot Space Borrowing Overview.

6.2 Overlapping datastore schedules

It is important to have an understanding of what VSM is doing in the background during these schedules. Otherwise, overlapping datastore schedules could occur preventing the data protection scheme from being achieved. Every object that has a snapshot is first put into VMware snapshot mode and then the underlying datastore volume on the PS Series SAN is snapped.

In this scenario, imagine that there is a folder with a VM in a two-hour reoccurring snapshot. Elsewhere in the cluster, another folder with a VM is in a six-hour reoccurring snapshot. The second VM resides on the same datastore volume as the first VM. This causes the PS Series SAN to create multiple snapshots of the same volume, but snapshots of the first VM only happen during its schedule. While the second snapshot is occurring on the same datastore volume, VSM is not placing the first VM in VMware snapshot mode. Therefore, the snapshot of the second folder is not usable as a consistent restore point for the VM in the first folder. The solution to this problem is to either place both VM folders in a higher-level folder, or move the folder of VMs to a different or new datastore. Because of this, proper VM placement for protection strategies is important.

Luckily, when looking at objects in the **Snapshot Schedules** pane, if one is a part of a higher-level snapshot schedule, an alert is displayed.

7 Managing and monitoring snapshots

VSM includes a variety of tools to use for managing the snapshots. The Recovery section lists the snapshot schedules and all of the snapshots of an object. Snapshots can be deleted individually or as a whole. Objects are also displayed as part of a particular snapshot, which is useful for recovery purposes.

Another benefit to VSM is the ability to see the recently performed tasks. Completed snapshots and scheduled operations are displayed, along with any errors. For detailed information, click **Jobs** in the VSM window. Select a snapshot to list all of the tasks associated with running that job.

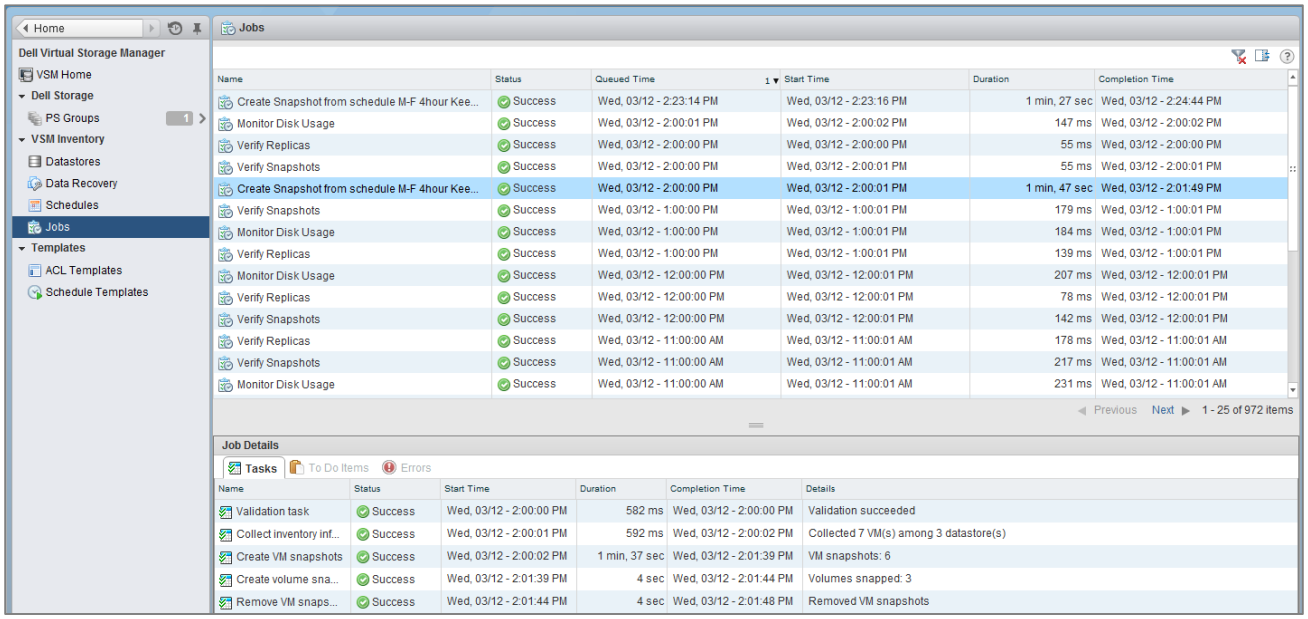


Figure 3 VSM task list

8 Recovering with snapshots

The reasons for recovering virtual machines can be many: A bad patch or software build, corrupt file or virtual machine, or even a file that was deleted by accident. Creating snapshots on a standard schedule adds time specific recovery points of the virtual environment to a traditional backup schedule in case data needs to be restored. By utilizing the snapshots in addition to the traditional backup schemes, administrators gain a shorter recovery time objective. The act of deploying a new virtual machine, patching it, installing the applications, backing up the agent, and then recovering data results in the loss of hours or even days of work. Instead, snapshots can be utilized to rapidly roll a virtual machine back to a good point in time and work can continue with minimal disruption.

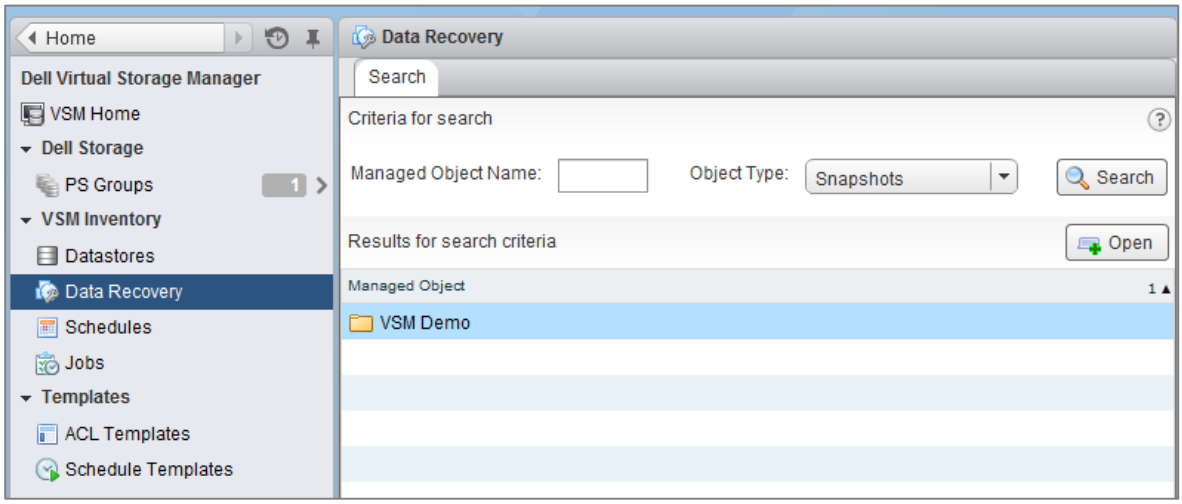
VSM has two different ways to start the process of recovery: From the **Data Recovery** option in the main VSM menu, or from the object itself.

8.1 Data Recovery Menu

The Data Recovery option is useful for viewing all of the available snapshots or replicas in one place. This screen also provides the ability to search for an object that may not exist in the environment but exists in a snapshot.

1. From the main VSM menu, click **Data Recovery**.
2. In the main pane, search for an object or search for all of a certain type of object.
3. Click **Search** to find the object to recover.

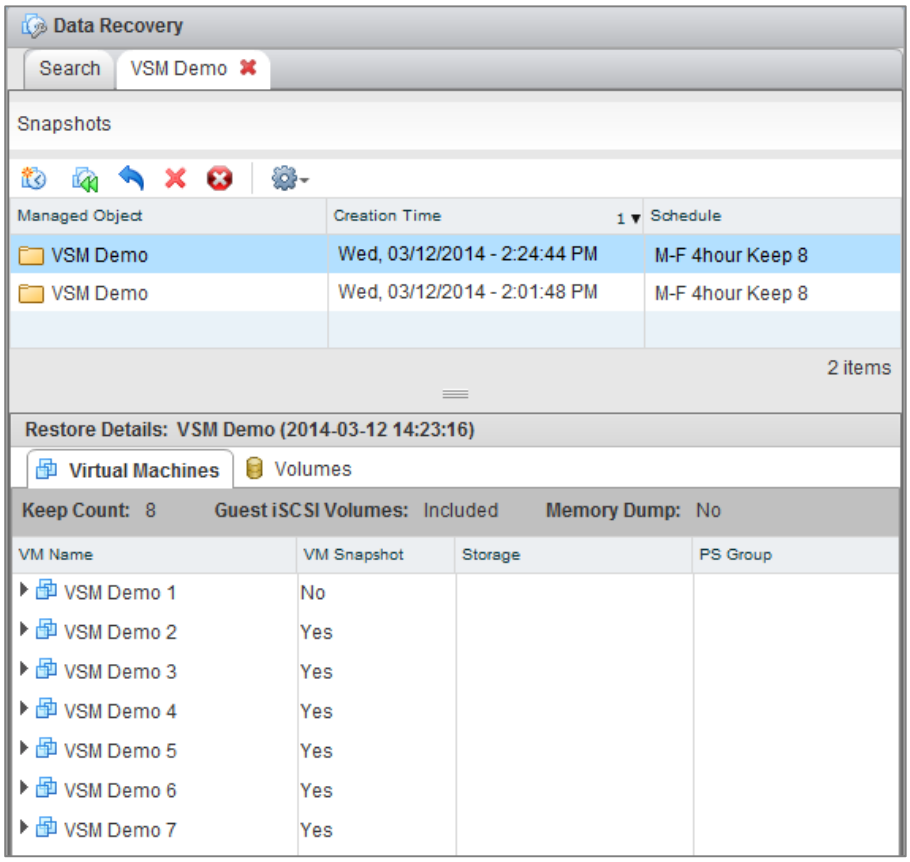
   It does not matter if the object has a single snapshot or dozens, a single object is displayed.



4. Double click an object to open a new tab in the **Data Recovery** pane.

   This will list all of the snapshots for that particular object.

5. Select each snapshot in the lower pane to list all of the virtual machines, volumes and groups that are part of the snapshot.



6. Choose an action to perform on the selected snapshot.

   Create Snapshot: An additional way to create a one time snapshot on this object.

   Selective Restore: Use VSM to restore an individual VM or just a few VMs that are contained inside the snapshot without impacting other VMs.

   Rollback Restore: Revert everything in the snapshot to the point in time that the snapshot was taken. This affects every VM and every volume in the snapshot.

   Delete: Delete the highlighted snapshot.

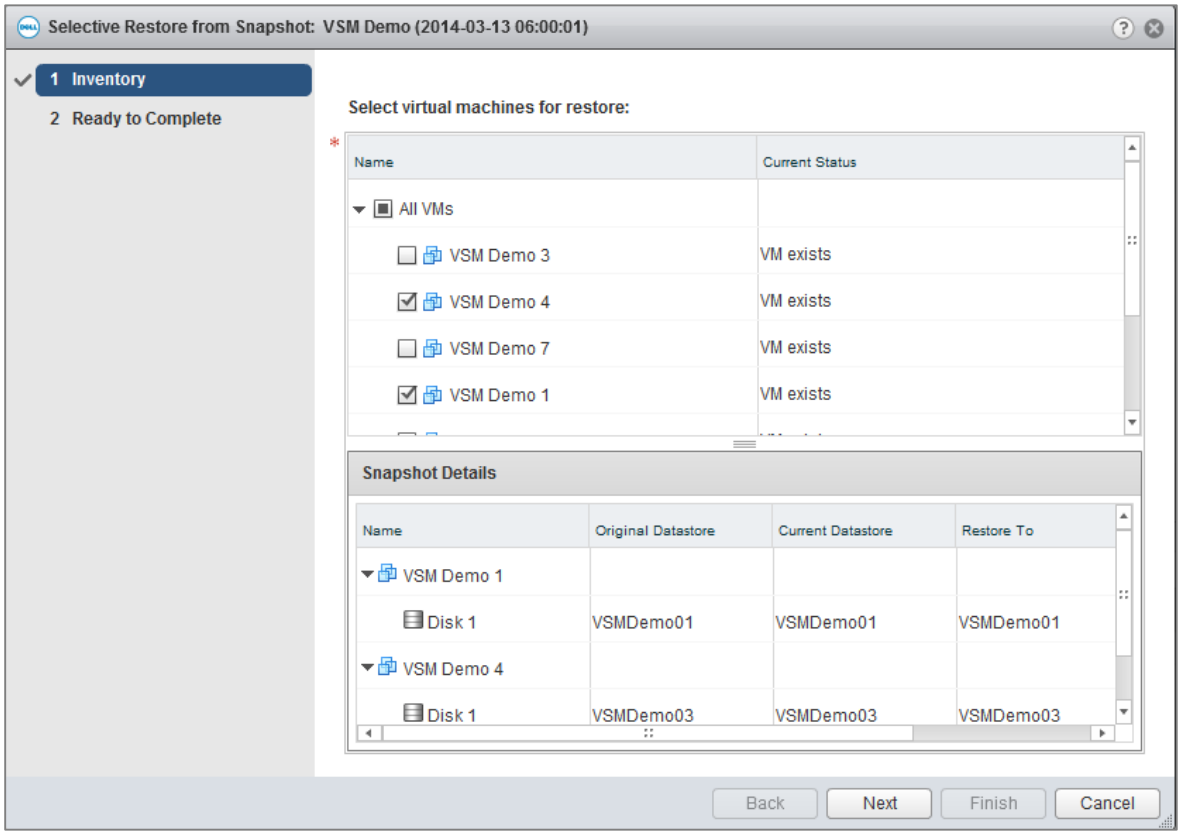
   Delete All Snapshots: Delete all of the snapshots for this object.

In both cases of a restore, the VMware snapshot is reverted and deleted for all of the VMs affected to bring the VM back to the exact state it was in when the Snapshot was created.

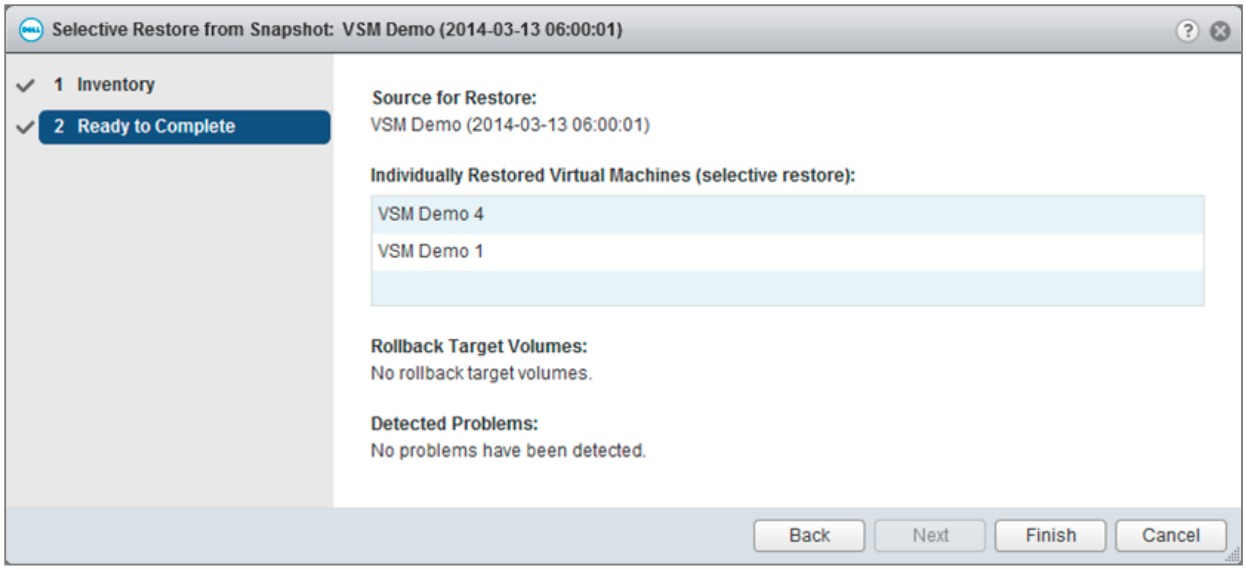
8.2 Selective restore

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

1. To perform a selective restore of any number of VMs in the snapshot, select the snapshot timestamp to recover and click the selective restore icon in the menu bar.
2. **Select Inventory**: Check the VMs to recover. The **Current Status** displays whether the VM has been deleted or still exists.
3. Click **Next** to continue.



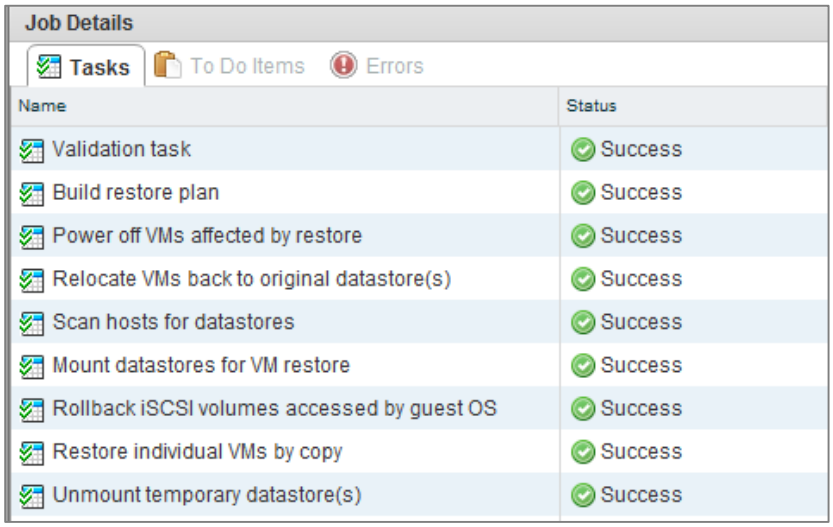
4. **Ready to Complete:** Verify the VMs that are being restored and correct any detected problems.
5. Click **Finish** to start the restore process.



Monitor the restore task in the VSM **Jobs** pane. It may be necessary to occasionally refresh the vCenter web UI.

VSM performs the following steps:

1. Powers off the VMs that are being restored.
2. Creates clones of the datastore volumes named VSM-temp-*****.
3. Rescans the ESX cluster and registers the cloned volumes.
4. Deletes the VMs that are being restored.
5. Copies the VMs from the clone volume to the original datastore.
6. Registers and reverts the VM to the snapshot state.
7. Cleans up the clones and environment.



8.3 Rollback restore

Note: This method rolls back the entire datastore, and affects all VMs on the datastore including new VMs that might not be part of an older Snapshot. VSM provides a warning of these impacts if they exist.

When all of the information in a snapshot needs to be rolled back to the point when it was created, use rollback restore. This reverts every single object in the snapshot including every VM and every volume.

1. Select the point in time to recover from and click the **Rollback Restore** icon in the menu bar.
2. **Inventory:** After the restore is complete, the Job Results lists additional user intervention needed as well as any information or warnings.

9 Creating clones from snapshots

Creating clones in any environment is useful for a number of reasons. Clones allow quick deployment for multiple sets of virtual machines to test configurations and they create identical environments. VSM has the capability to not only clone running virtual machine environments but also to create clones from previous snapshots. This allows the administrator to bring online copies of virtual machines from a prior point in time. This can be helpful for troubleshooting or a side-by-side comparison of machines.

Another use of clones is the ability to test new software without impacting existing production machines. An administrator typically takes a snapshot of a set of virtual machines and then upgrades the software. If this results in an outage or the software is incompatible, the administrator can roll back to a known good snapshot. However, this can be disruptive as the environment is 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 bring a clone of the virtual environment online, isolate it from the production environment, and then run the upgrades and testing on the cloned environment. This way, if anything negative occurs, at no point is the production environment impacted.

Clones can also be used to create identical environments for testing and development. When combined with the PS Series thin clone feature, clones 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 and test environments. For 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* at http://en.community.dell.com/dell-groups/dtcmedia/m/mediagallery/19861241.aspx.

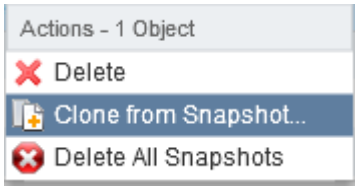
It is very important to note that no matter what the reason is for utilizing clones, they are an exact match of the existing virtual machine. This means that the hostname, the IP address, and the application namespace is identical. It is therefore vital that whenever a cloned virtual environment is brought 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 that have data drives spanning multiple datastore volumes are supported by snapshots. However, during a clone operation these virtual machines have the additional drive registration still points to the original volumes. This causes conflicts without some manual configuration steps. As a best practice, keep all of the data of the VMs that need to be cloned on a single datastore volume to avoid any potential issues.

To create a clone from a snapshot:

1. Open the VSM GUI and go to the object snapshots.

   You can also search in the Data Recovery area of VSM and double click the object. Select a snapshot to clone, right click it and select **Clone from Snapshot**.



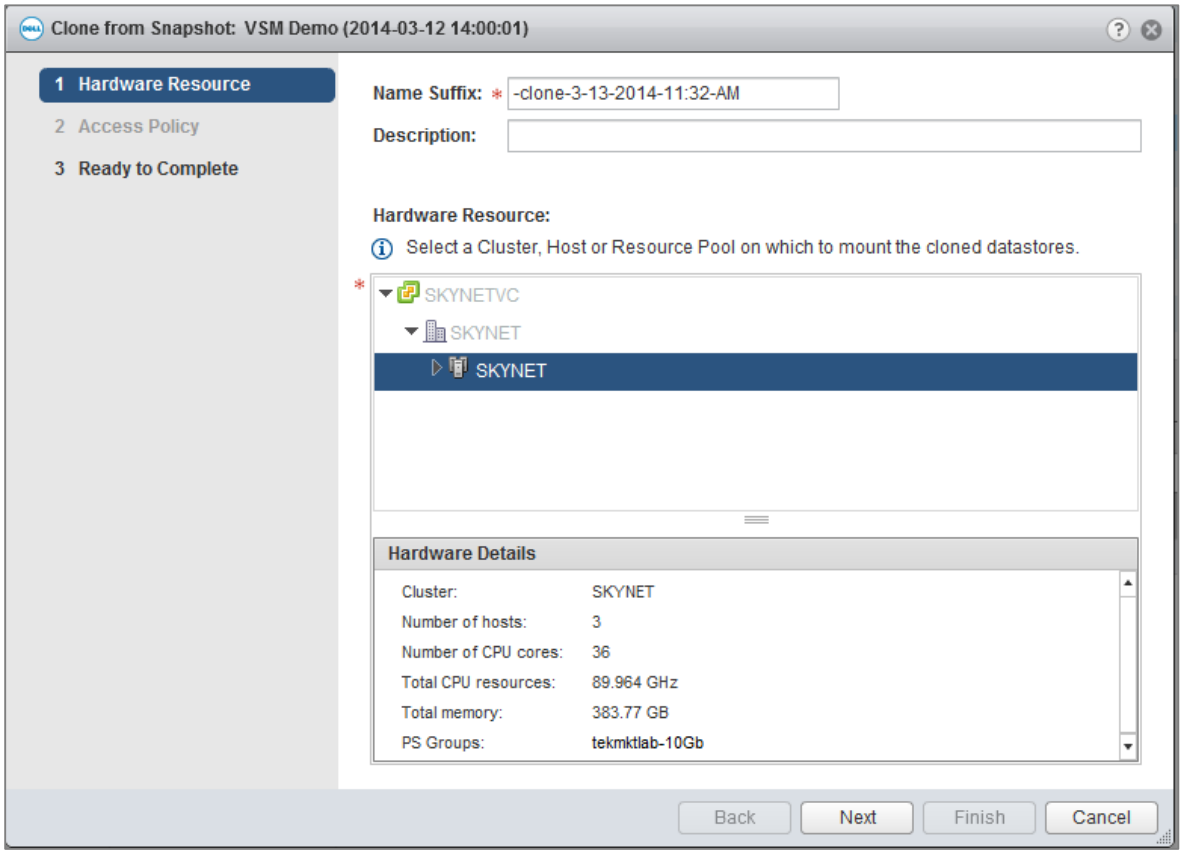
Hardware Resource: VSM needs to create a name suffix for every volume that it clones for the restore. This is needed so that no two datastores can have the same name and provides a way to differentiate between the original datastore and the cloned datastore.

2. By default VSM appends *-clone- date/time of Snapshot*. A description can be entered and the deployment hardware resource selected.

   This enables cloning from a production cluster and mounting to a test and development cluster in the same vSphere farm.

3. Select the hardware resource and click **Next**.

Note: This clones the entire Snapshot and consumes space for the datastore volumes that are part of the snapshot.

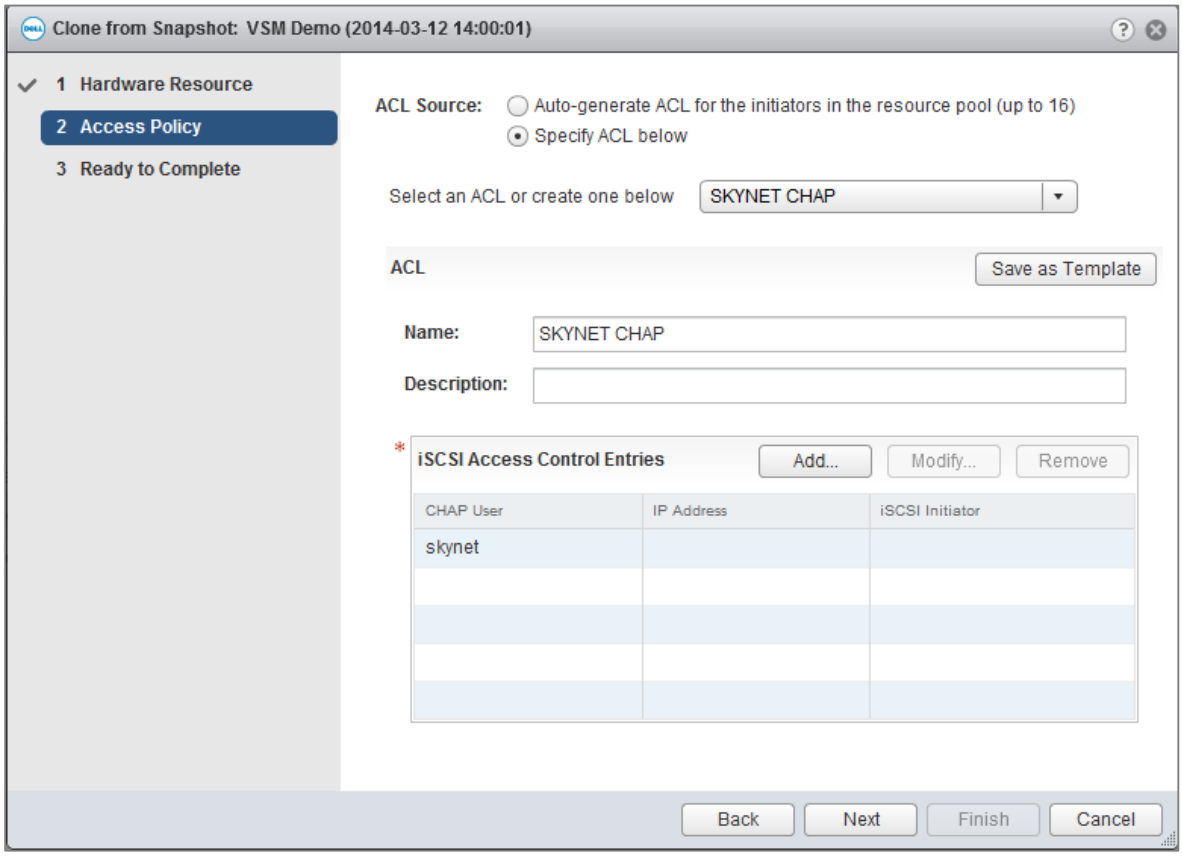


Access Policy: The next step in the process is to choose the access policy for the new cloned volumes.

4. Selecting **Auto-generate** creates ACLs from the hosts that are in the selected cluster. You can choose to specify a new or existing ACL policy.

   For information about ACL policies in VSM see *TR1101 EqualLogic Virtual Storage Manager: Installation Considerations and Datastore Management*.

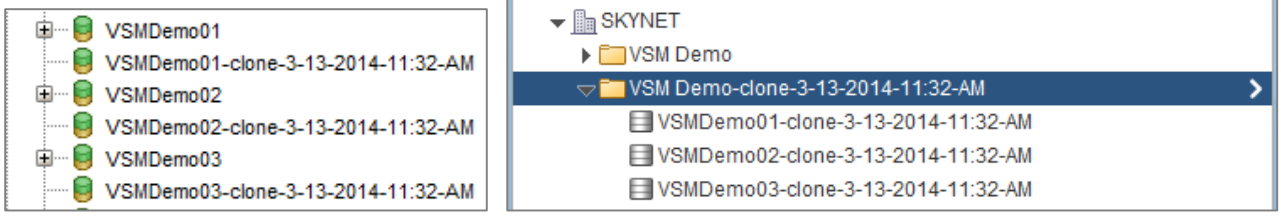
5. Complete your selections and click **Next**.



6. **Ready to Complete**: Verify the options are correct and click **Finish**.

During this time, VSM coordinates with the PS Series SAN and creates volume clones of all the snapshots that are part of the VSM Snapshot. Once the volumes are cloned, VSM tells vCenter to rescan and bring these new cloned volumes into the environment in a datastore folder.

The new cloned volumes are displayed inside the PS Series Group Manager GUI as well as the new datastore volumes inside vCenter.



VSM will not register or power on the VMs so that the original VM environment is protected. Once the cloning is complete, you can browse the datastore, register the VMs, isolate them and power them on.

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

10 Advanced cloning in selective data recovery

There are times when data restoration needs to be more granular than at the level of the individual datastore or individual virtual machine. The idea behind selective data recovery is creating clones, bringing the information online and then attaching the data drive of the VM from the snapshot back to the original VM. Using clones for this is prefered over bringing a snapshot online. By taking a clone of the Snapshot, the original PS Series snapshot data is not modified. If the original PS Series snapshot is online, the data integrity for recovery could be changed (or deleted) by accident.

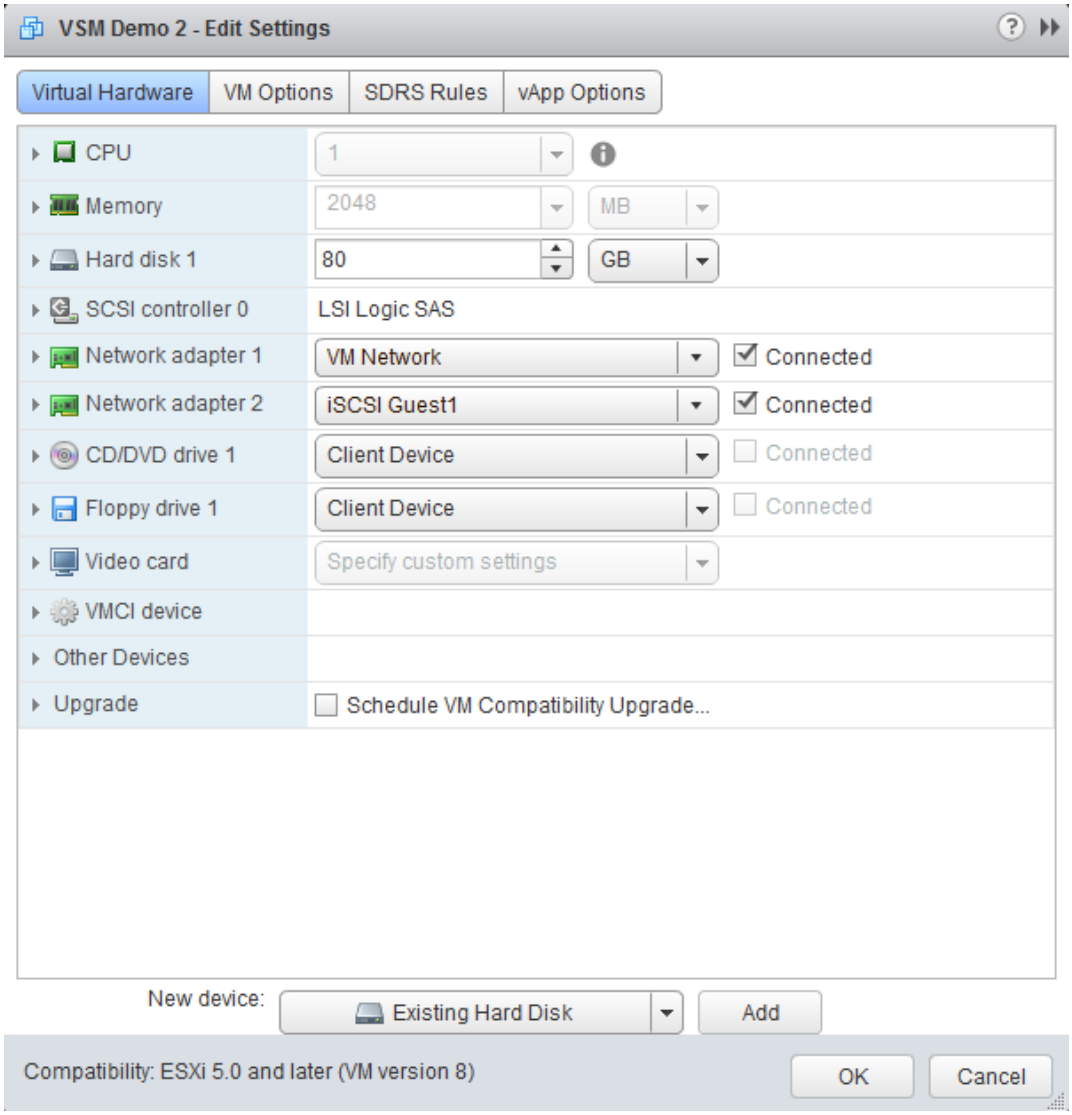
There are multiple options for selective data recovery, but they all revolve around mounting a point-in-time version of the data disk to a VM (usually the original). In order for this to work, the VM OS must support the ability to hot add data disks. The other option is to have a temporary or standby 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 similar to creating a clone but with some additional steps.

1. Find the snapshot containing the data that needs to be recovered. Right click and choose to **Clone from Snapshot**.

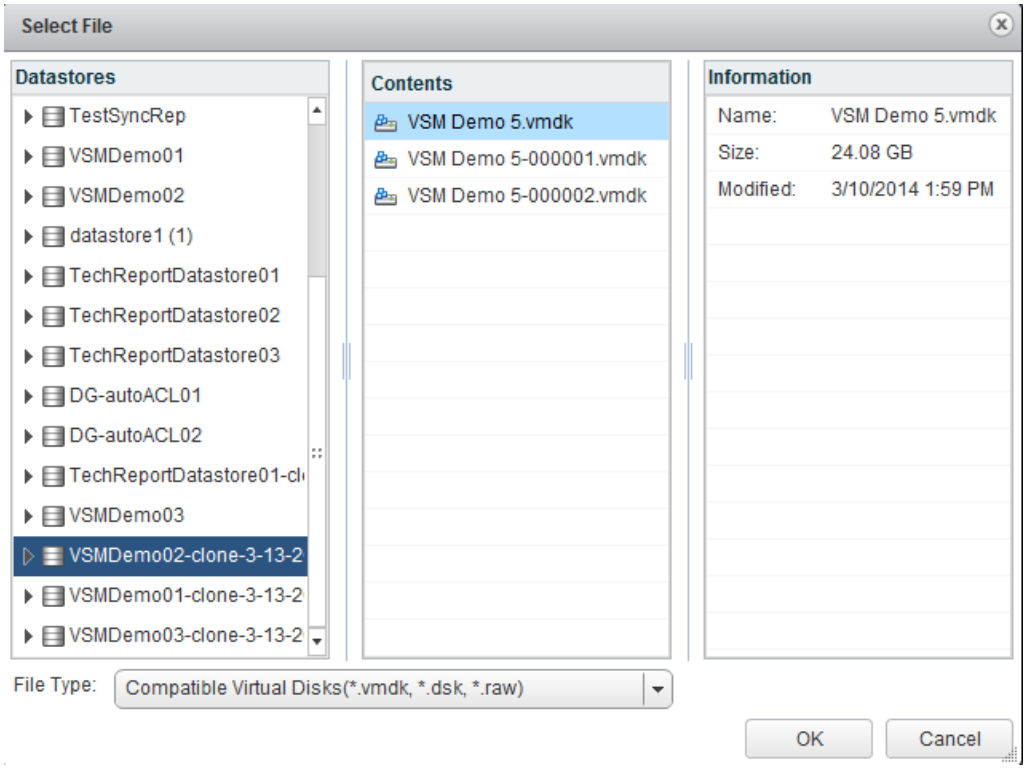
Note: Even if you are trying to restore just one file, the Smart Clone operation could cause multiple datastores to be cloned and mounted. These will need to be deleted using Datastore Manager when the process is finished.

2. Follow the same process as creating a clone from a snapshot. Once the cloned datastores are scanned and found, the data drive can be attached to the VM or recover VM for file restoration.
3. Right click on the VM receiving the recovery data disk and click **Edit Settings**.
4. Click the new device drop down menu, choose **New Existing Hard Disk**, and click **Add**.



The next step is to add an existing hard disk to the VM pointing to the cloned datastore.

5. Find the vmdk file with the data in the folder to recover and click **OK**. Click **OK** again to commit the change.



6. 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, open up disk management first.

7. Place the disk online and a drive letter is assigned to it.
8. Browse the assigned drive letter to see that it is the version of the original data drive from the point in time that the snapshot was taken.
9. 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.

Clean up the environment once the files have been recovered.

1. Remove the added hard disk by editing the VM settings and removing it.

   If the VM or recovery VM does not support hot add/remove the VM needs to be powered off to remove the hard disk.

2. Use the 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 the iSCSI targets and deletion of PS Series cloned volumes.

11 Multilayered data protection approach and data placement

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

Leveraging all of these tools together requires a new approach to data protection and data placement. The snapshot within the PS Series SAN is 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 data protection scenarios are built, it will be easier to decide which tier a particular VM falls into. Once these tiers are set up and configured by either 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 because 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 Snapshots can also be used in conjunction with a variety of the other EqualLogic host integration tools for more granular protection of the application data within the virtual machine.

12 Summary

The EqualLogic Virtual Storage Manager is a vCenter plug-in that provides a whole suite of tools for managing and protecting virtualized environments. By leveraging VSM Snapshots 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.

13 Technical support and customer service

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

13.1 Dell online services

You can learn about Dell products and services using:

- http://www.dell.com or the URL specified in any Dell product information.
- The local menu or click the link that specifies your country or region.

13.2 EqualLogic storage solutions

To learn more about EqualLogic products and new releases being planned, visit the EqualLogic page on Dell TechCenter at: http://delltechcenter.com/page/EqualLogic. This site provides articles, demos, online discussions, technical documentation, and more.

13.3 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 needed.

13.4 Warranty information

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

A Configuration details

This appendix provides additional configuration details used in the development of this paper.

Table 1 Software and firmware

Vendor	Model	Software Revision
Dell	PS Series SAN	6.x and higher
VMware	vCenter/ESX	5.1, 5.5
Dell	Virtual Storage Manager	v4.0

B 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.

The following table lists the documents referred to in this Technical Report.

Vendor	Document Title
Dell	TR1101: EqualLogic Virtual Storage Manager: Installation considerations and datastore management
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

All PS Series Technical Reports are available on Dell TechCenter at: http://en.community.dell.com/techcenter/storage/w/wiki/2660.equallogic-technical-content.aspx.