DELL EQUALLOGIC

TECHNICAL SUPPORT INSTRUCTIONAL SERIES

Technical Report	**Document ID:** TR1038
Data Protection Examples Using PS Series Snapshots in a VMWare® Virtual Infrastructure	**Revision**: A02
	Revision Date: August 28, 2009

TECHNICAL REPORT

DATA PROTECTION EXAMPLES USING PS SERIES SNAPSHOTS IN A VMWARE® VIRTUAL INFRASTRUCTURE

ABSTRACT

This tech report demonstrates how using Dell EqualLogic SAN Snapshots can improve data protection in a VMware Virtual Infrastructure environment.

TR1038

V1.0

[May 2008]

PS Series Firmware Version [3.3.1] or later.

Dell Inc.
300 Innovative Way
Suite 301
Nashua, NH 03062
Tel: 603.579.9762
Fax: 603.579.6910

TABLE OF CONTENTS

REVISION INFORMATION

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

Report	Date	Document Revision
1.0	May 2008	Initial Release

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

Vendor	Model	Software Revision
VMware	Virtual Infrastructure	3.x
Dell	EqualLogic PS Series Array	FW 3.3.1

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: https://www.equallogic.com/support/

Vendor	Document Title
Dell	SQL Server Data Protection with Auto-Snapshot Manager
Dell	Deploying Microsoft® SQL Server in an iSCSI SAN
Dell	Deploying Microsoft Windows Server 2003 in an iSCSI SAN
Dell	Microsoft Windows Aligning Disk Sectors for Optimal Performance
Dell	Deploying Microsoft Multipath I/O in an iSCSI SAN
Dell	VMware® ESX Server 3.x Considerations, Configuration and Operation Using an EqualLogic PS Series SAN
Dell	Configuring and Deploying the Dell EqualLogic MPIO DSM in an iSCSI SAN

INTRODUCTION

In today's virtual datacenter, administrators are looking for ways to protect and quickly recover their virtual machines and the data they rely on. Using Dell EqualLogic PS Series volume snapshots, administrators can increase data protection and recovery options. Snapshots can be used throughout the day to augment existing data protection scenarios such as backups. These snapshots can also be automated, executed according to a schedule without burdening the virtual infrastructure. Because VMware encapsulates the virtual machines into files, SAN snapshot technology can be utilized to provide point-in-time copies of these files throughout the day.

This technical report describes examples of using PS Series volume snapshots in virtual environments and recovering the data that resides within them. At the basic level, operating PS Series volume snapshots in a virtual environment can be summarized in four steps:

Step 1. Snap Volume – Use Group Manager UI to create snapshots of the volume

Step 2. Mount Snapshot – Set snapshot online and assign the volume to ESX

Step 3. Recover Data – Move, test, or recover data from snapshot

Step 4. Clean-up – Remove snapshot

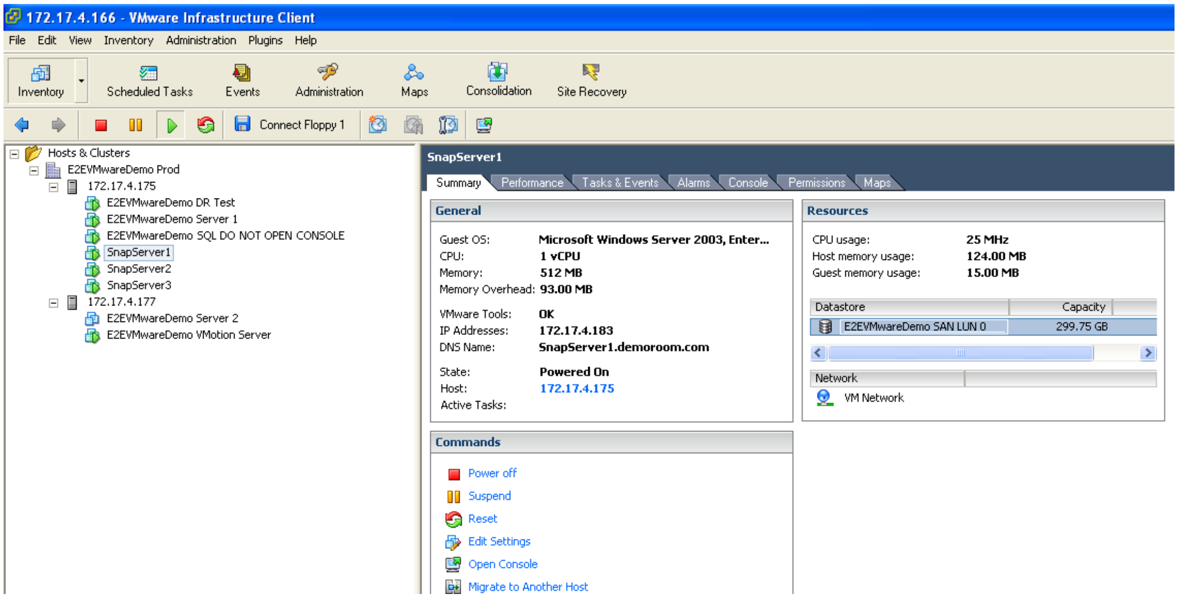
The examples listed in this technical report are not a complete listing of all possible deployments, but provide a framework for using and recovering data from PS Series snapshots within your VMware virtual environment.

EXAMPLE 1: RECOVERING DATA FROM A VIRTUAL DISK (VMDK FILE)

This example demonstrates how to recover data that is stored in a vmdk file that has been protected by a PS Series snapshot. In this example, the virtual machine (VM) is a Windows 2003 Server that resides on a single datastore on the PS Series SAN. The VM has a C:\ drive virtual disk and a D:\ drive virtual disk which both reside on a single VMFS and PS Series volume on the PS Series SAN. During the day, scheduled snapshots of the volume on which this VM resides will be regularly created, enabling recovery of data on the C:\ drive or the D:\ drive at any time. Because of the hardware offload for snapshot operations, the array snapshot does not impact performance of the running VM. Because the vmdk files reside on the same PS Series volume, data I/O consistency is maintained.

Step 1. Snap Volume

First, create a snapshot of the volume on the array on which the VM resides. It is a good practice to name the ESX datastores using the same or similar names as the PS Series volumes to make matching them up easy. In this first example the VM is stored on the datastore **E2EVMwareDemo SAN LUN 0** which matches the **E2EVMwareDemoLUN0** volume on the SAN.



```
Hosts & Clusters
  E2EVMwareDemo Prod
    172.17.4.175
      E2EVMwareDemo DR Test
      E2EVMwareDemo Server 1
      E2EVMwareDemo SQL DO NOT OPEN CONSOLE
      SnapServer1
      SnapServer2
      SnapServer3
    172.17.4.177
      E2EVMwareDemo Server 2
      E2EVMwareDemo VMotion Server
```

SnapServer1

General

Guest OS:	Microsoft Windows Server 2003, Enter...
CPU:	1 vCPU
Memory:	512 MB
Memory Overhead:	93.00 MB
VMware Tools:	OK
IP Addresses:	172.17.4.183
DNS Name:	SnapServer1.demoroom.com
State:	Powered On
Host:	172.17.4.175
Active Tasks:	

Resources

CPU usage:	25 MHz
Host memory usage:	124.00 MB
Guest memory usage:	15.00 MB

Datastore	Capacity
E2EVMwareDemo SAN LUN 0	299.75 GB

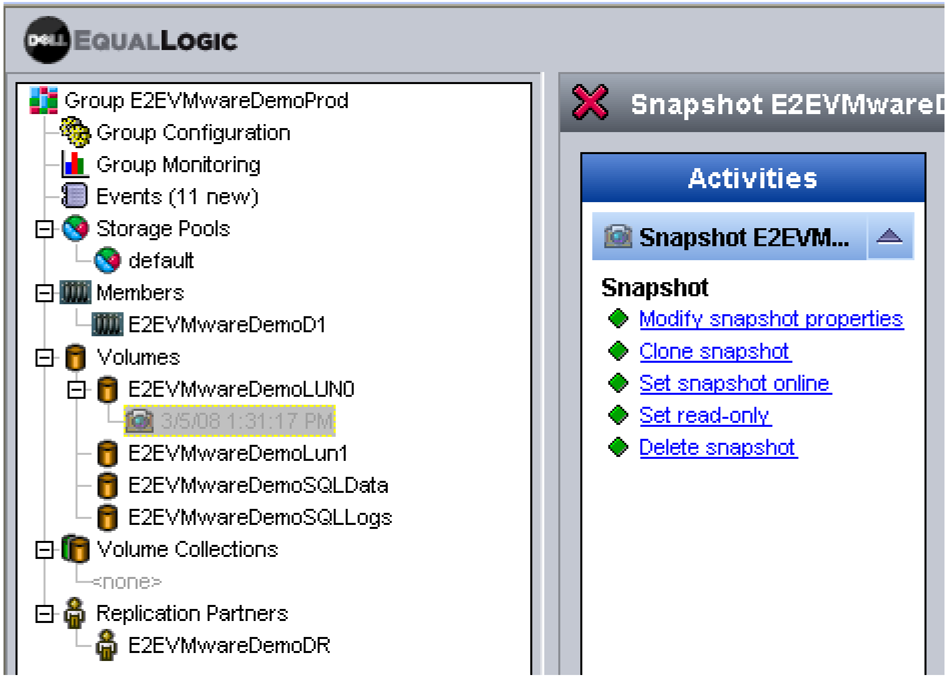
Network
VM Network

Commands

- Power off
- Suspend
- Reset
- Edit Settings
- Open Console
- Migrate to Another Host

- Open the PS Series Group Manager and select the volume that corresponds to the datastore.
- In the activities pane select **Create snapshot now**.
- Give the snapshot a name and click **OK**.

This will put a snapshot under the parent volume. It will be time stamped and appear grayed out to indicate that the volume is not online.



```
Group E2EVMwareDemoProd
  Group Configuration
  Group Monitoring
  Events (11 new)
  Storage Pools
    default
  Members
    E2EVMwareDemoD1
  Volumes
    E2EVMwareDemoLUN0
      3/5/08 1:31:17 PM
    E2EVMwareDemoLun1
    E2EVMwareDemoSQLData
    E2EVMwareDemoSQLLogs
  Volume Collections
    <none>
  Replication Partners
    E2EVMwareDemoDR
```

Snapshot

- Modify snapshot properties
- Clone snapshot
- Set snapshot online
- Set read-only
- Delete snapshot

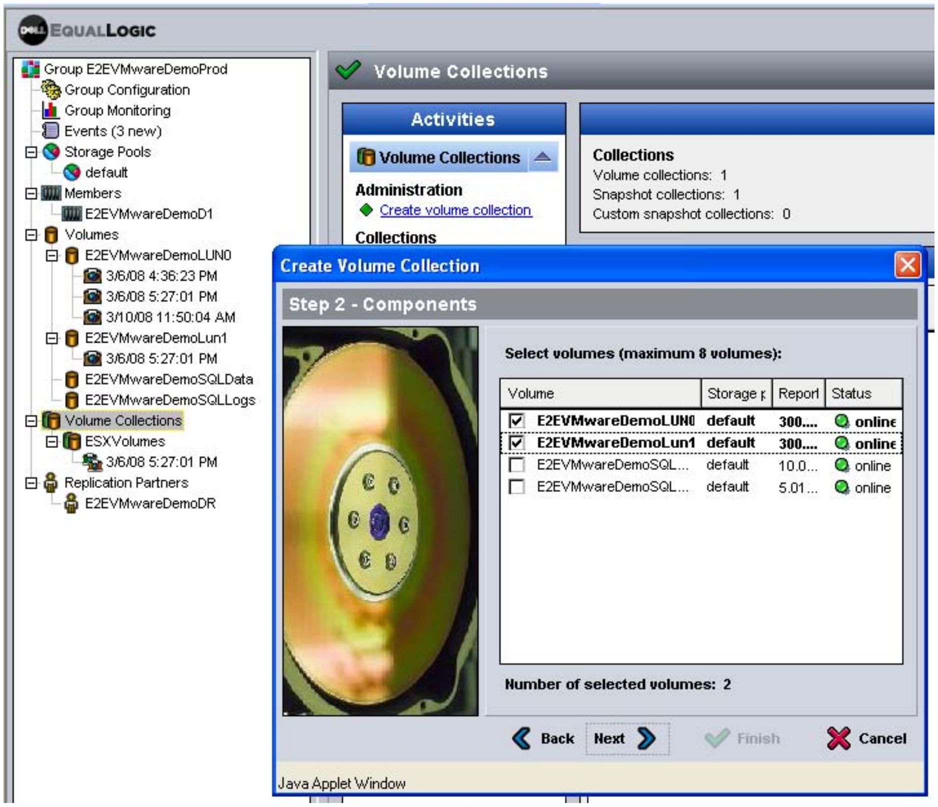
In order to automate the process throughout the day, a snapshot schedule can be created. To create a snapshot schedule select the volume that you want to create the schedule for.

- In the activities panel under Schedules click **Create Schedule**.
- Give the schedule a name, choose Snapshot Schedule, choose how often to run it, click **Enable Schedule,** and click **Next**.
- On the next screen choose how often to run the snapshot, when to run it, and how many copies of the snapshot to keep, and click **Next**.
- Verify all of the settings and click **Finish**. This will enable the schedule.

For more information consult the online help found under **Tools ->** **Online Help** in the Group Manager.

Note that if the VMs span multiple volumes, a PS Series Volume Collection should be used to keep the snapshots of the volumes in sync. A Volume Collection is a group of volumes in the PS Series group that can be snapped at the exact same time to ensure their timestamp integrity.

- To create a Volume Collection, go into the PS Series Group Manager GUI, click on Volume Collections, and in the Activities pane select **Create Volume Collection**.
- Give the collection a name and click **Next**.
- Select the volumes that are to be included in the collection. Click the check box next to each volume and click **Next**.



Collections
Volume collections: 1
Snapshot collections: 1
Custom snapshot collections: 0

Select volumes (maximum 8 volumes):

Volume	Storage p	Report	Status
☑ E2EVMwareDemoLUN0	default	300....	online
☑ E2EVMwareDemoLun1	default	300....	online
☐ E2EVMwareDemoSQL...	default	10.0...	online
☐ E2EVMwareDemoSQL...	default	5.01...	online

Number of selected volumes: 2

Now that there is a Volume Collection, snapshots can be taken manually at the collection level, or a schedule can be set up to snap the entire collection just like an individual volume.

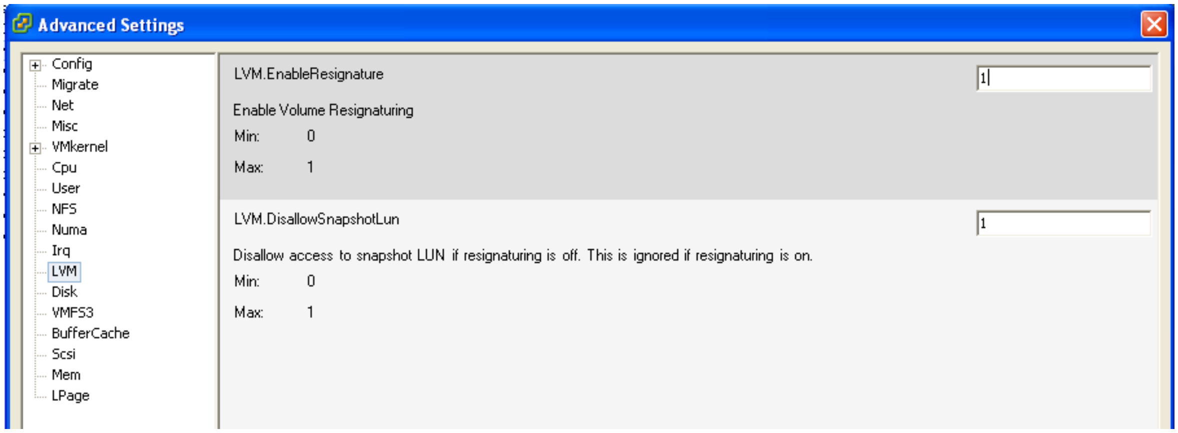
Step 2. Mount Snap

Now that the snapshots have been configured, let's look at a classic case for using them. In this example, a user has a file deleted or corrupted or changed, and you need a previous version of that file. Instead of having to restore from the previous night's tape backup, you can mount one of the snapshots containing the data and copy it back to its original spot.

NOTE: In ESX, you can always add a hard disk to a running virtual machine, but in order to remove a disk the VM must be powered down. This is important to remember when using snapshots for data recovery. If you cannot power down a VM to remove the disk drive, it may be helpful to mount the snapshot to another VM which can be powered off, and copy the file across the network. This way you can recover the files with no impact to the running production VM.

In order to recover files from the D:\ snapshot that was taken earlier, the PS Series snapshot volume will need to be brought online, and ESX rescanned for the new datastore – then the disk can be added to the VM to recover the files. When the snapshot is done, the VM can be powered off, the disk removed from the VM, and the snapshot removed.

- First, bring the snapshot online. In the PS Series GUI select the snapshot you want to mount and in the activities panel under snapshots click **Set Snapshot Online**.
- Now that it is online, you must enable ESX to see the volume. In the Virtual Infrastructure Client (VIC) console first enable LVM to resignature the disk. To do this, on your ESX server click the **Configuration** tab, then **Advanced Settings**.
- Click **LVM** on the left and change the **LVM.EnableResignature** to 1 and click **Ok**.



LVM.EnableResignature 1

Enable Volume Resignaturing

Min: 0

Max: 1

LVM.DisallowSnapshotLun 1

Disallow access to snapshot LUN if resignaturing is off. This is ignored if resignaturing is on.

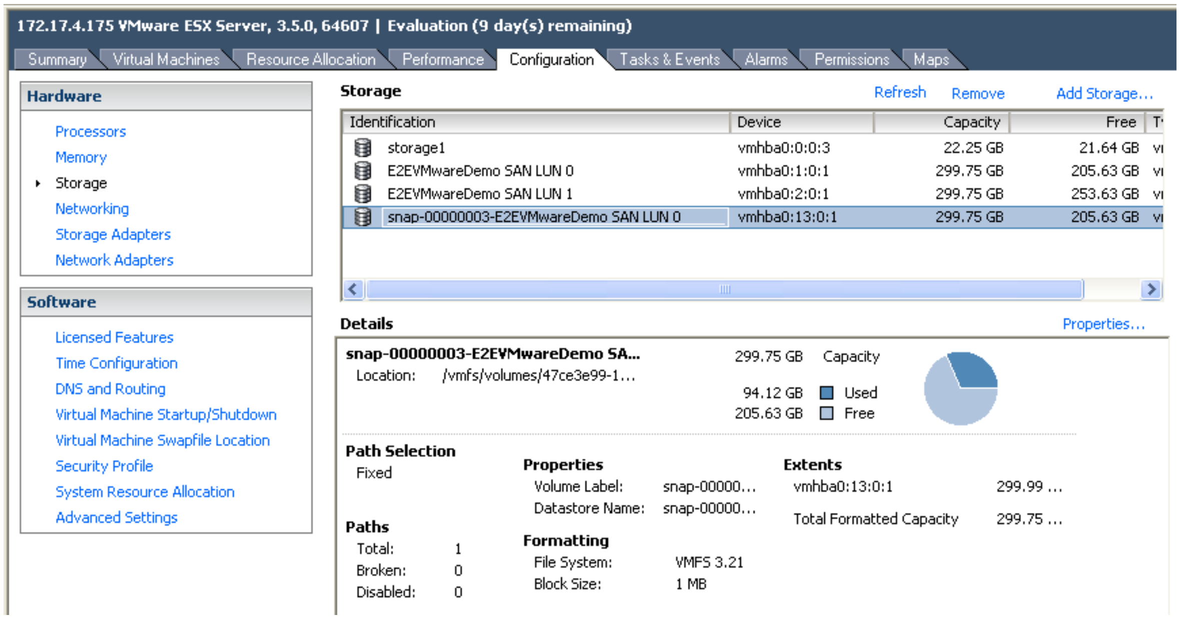
Min: 0

Max: 1

NOTE: It is important to reset this value to 0 after using the snapshots. Failure to do so could cause production datastores to be resignatured, which will result in VMotion, DRS, and HA failing.

- Next, go into the **Configuration** tab and select **Storage Adapters**. Click on **Rescan** and choose to **Scan for New Storage Devices**. Uncheck the box for **Scan for New VMFS Volumes**.
- When this is done, click on **Rescan** and now select **Scan for New VMFS Volumes**. Uncheck the box for **Scan for New Storage Devices**.

- After the rescan click on **Storage** under Hardware. You should see a new datastore with a name that starts with snap-0000xxx-volumename. This is the snapshot volume that was put online.
- Once the PS Series snapshot shows up as a datastore, disable the LVM.EnableResignature option by setting it back to 0 and clicking **Ok**.



172.17.4.175 VMware ESX Server, 3.5.0, 64607 | Evaluation (9 day(s) remaining)

Storage

Identification	Device	Capacity	Free	T
storage1	vmhba0:0:0:3	22.25 GB	21.64 GB	vı
E2EVMwareDemo SAN LUN 0	vmhba0:1:0:1	299.75 GB	205.63 GB	vı
E2EVMwareDemo SAN LUN 1	vmhba0:2:0:1	299.75 GB	253.63 GB	vı
snap-00000003-E2EVMwareDemo SAN LUN 0	vmhba0:13:0:1	299.75 GB	205.63 GB	vı

Details

snap-00000003-E2EVMwareDemo SA...
Location: /vmfs/volumes/47ce3e99-1...

299.75 GB Capacity
94.12 GB ■ Used
205.63 GB □ Free

Path Selection
Fixed

Paths
Total: 1
Broken: 0
Disabled: 0

Properties
Volume Label: snap-00000...
Datastore Name: snap-00000...

Formatting
File System: VMFS 3.21
Block Size: 1 MB

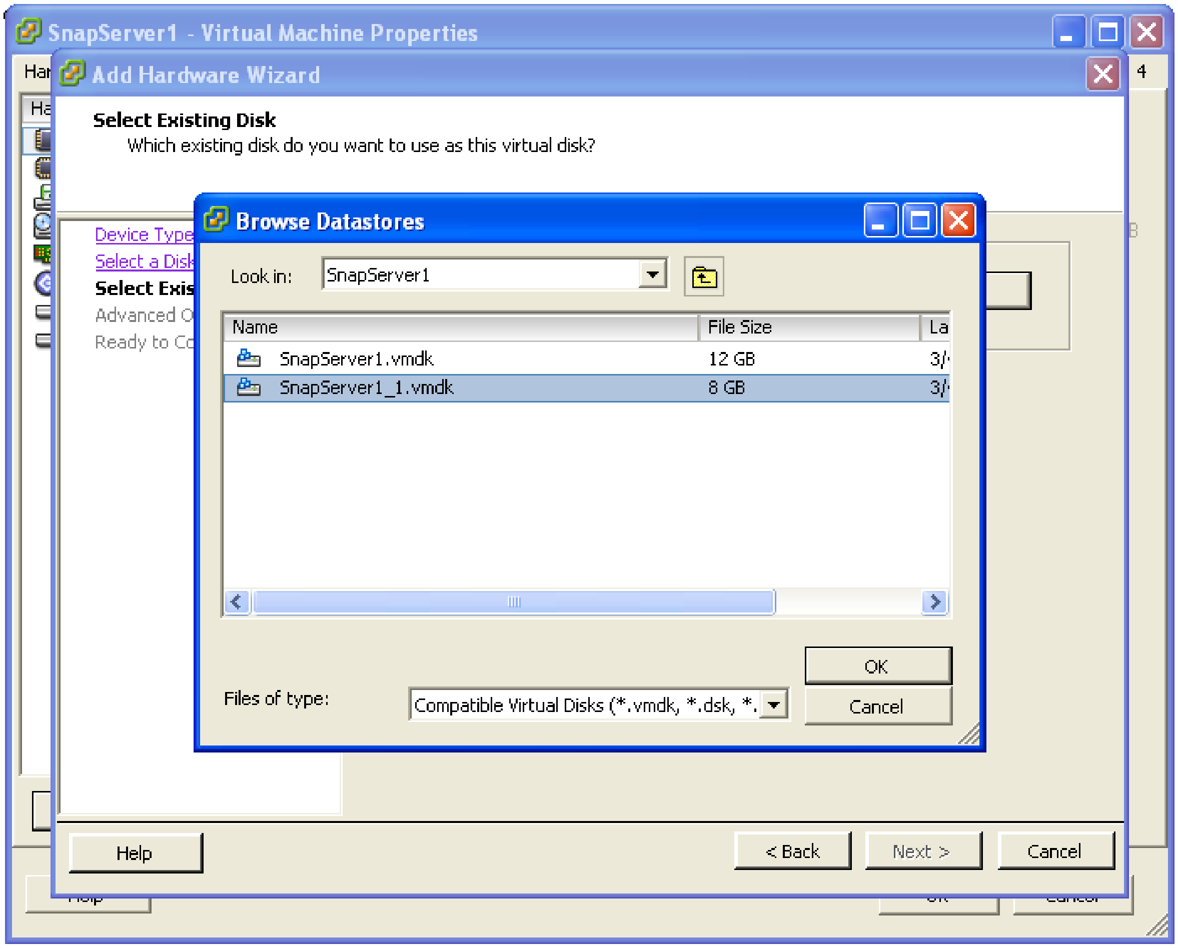
Extents
vmhba0:13:0:1 299.99 ...
Total Formatted Capacity 299.75 ...

If you browse the datastore you will see that it is identical to the original volume at the time the snapshot was taken. You can use this technique for multiple data recoveries.

Step 3. Mount VMDK File to Existing VM

Now that the PS Series snapshot is an available datastore, it must be brought online to the VM to recover the data. To do this, create a new disk for the VM and point it to the disk file that resides on the snapshot.

- In VIC, select the VM to which you are mounting the virtual hard drive to recovering data from and click **Edit Settings**.
- Click **Add** and then select **Hard Disk** and click **Next**.
- On the next screen choose the second option, **Use an existing Virtual Disk**, and click **Next**.
- In the Disk File Path screen click **Browse** and point to the new snapshot datastore volume and the data disk you want to recover. In this example, the original D:\ drive was an 8 GB disk, so that is the one selected from the datastore.



Select Existing Disk

Which existing disk do you want to use as this virtual disk?

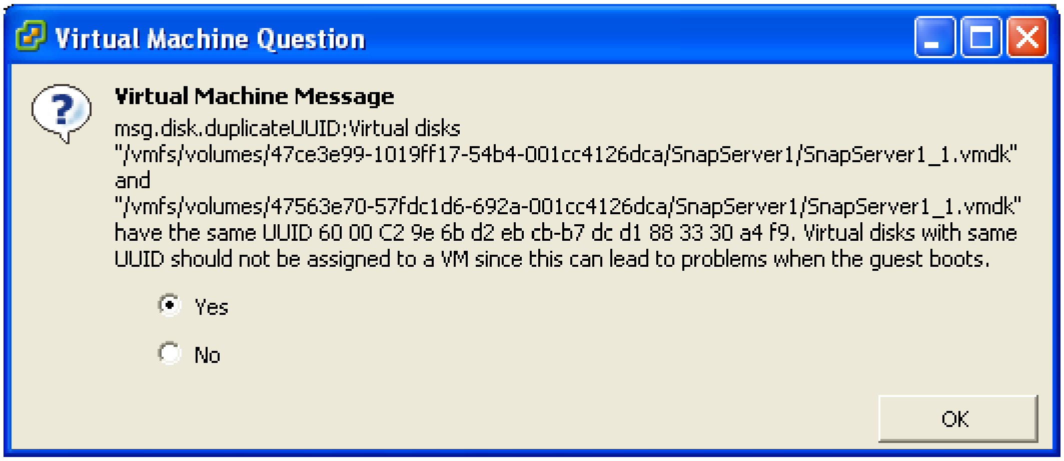
Look in: SnapServer1

Name	File Size	La
SnapServer1.vmdk	12 GB	3/
SnapServer1_1.vmdk	8 GB	3/

Files of type: Compatible Virtual Disks (*.vmdk, *.dsk, *.

- Click **OK** and then **Next**.
- The next screen includes advanced settings that are usually not changed. Click **Next** and then **Finish**.

After reconfiguring the VM, the disk will be available. You will also see an error message that the disk has the same UUID. Continue by selecting **Yes** and then **OK**. Because this is for data recovery only, having the same disk UUID on boot up is not a problem.



Virtual Machine Message

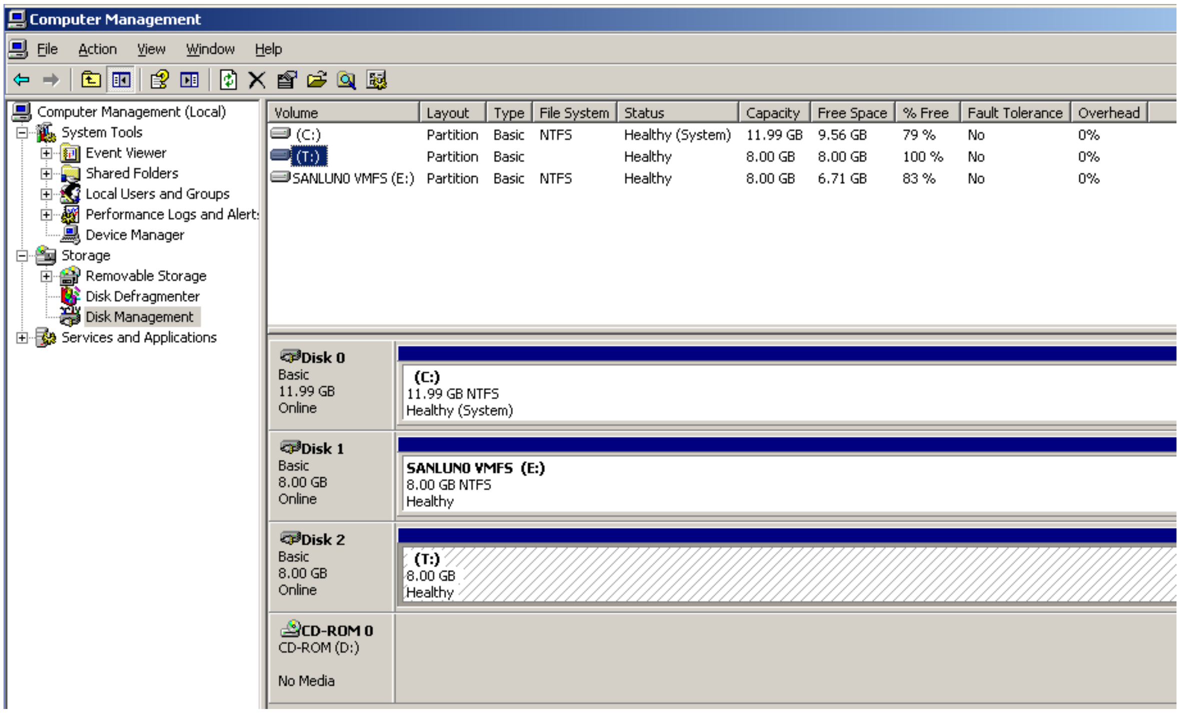
msg.disk.duplicateUUID:Virtual disks "/vmfs/volumes/47ce3e99-1019ff17-54b4-001cc4126dca/SnapServer1/SnapServer1_1.vmdk" and "/vmfs/volumes/47563e70-57fdc1d6-692a-001cc4126dca/SnapServer1/SnapServer1_1.vmdk" have the same UUID 60 00 C2 9e 6b d2 eb cb-b7 dc d1 88 33 30 a4 f9. Virtual disks with same UUID should not be assigned to a VM since this can lead to problems when the guest boots.

● Yes

○ No

Next, open the console or Remote Desktop (RDP) session to the VM. Open the Computer Management console and click on Device Manager. Then right-click the computer name and select **Scan for Hardware Changes**.

When this is done, open Disk Management. You will see the volume that you connected there, but without a drive letter. Once you assign a drive letter the volume can be browsed for data recovery.



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free	Fault Tolerance	Overhead
(C:)	Partition	Basic	NTFS	Healthy (System)	11.99 GB	9.56 GB	79 %	No	0%
(T:)	Partition	Basic		Healthy	8.00 GB	8.00 GB	100 %	No	0%
SANLUN0 VMFS (E:)	Partition	Basic	NTFS	Healthy	8.00 GB	6.71 GB	83 %	No	0%

Disk 0 Basic 11.99 GB Online	**(C:)** 11.99 GB NTFS Healthy (System)
Disk 1 Basic 8.00 GB Online	**SANLUN0 VMFS (E:)** 8.00 GB NTFS Healthy
Disk 2 Basic 8.00 GB Online	**(T:)** 8.00 GB Healthy
CD-ROM 0 CD-ROM (D:) No Media	

Step 4. Cleanup

Once the data has been recovered, the environment must be cleaned up to prevent any error messages on the array and to release the snapshot. In order to remove the disk from the VM it must be powered off.

- Open VIC and select the VM that the disk was added to by clicking **Edit Settings**.
- Select the hard disk that was added and select **Remove** and then **OK**.
- Now that the disk has been removed from the VM it can be removed from Virtual Center. Click on the **Configuration** tab and then select **Storage**.
- Click on the snap-0000xxx-volumename datastore and click **Remove**.

Once this has been removed, it is important to clean up some of the persistent targets that ESX is seeing.

- Click the **Configuration** tab and select **Storage Adapters**.
- Select either the iSCSI Software Adapter or the iSCSI HBA that you are using to connect to the array and click **Properties**.
- Select the **Static Discovery** tab and find the snapshot volume.
- Select the snapshot volume and click **Remove**. Make sure the snapshot volume is not being used by another server for data recovery, as this will remove the connection.

The PS Series snapshot will appear with the iqn name, followed by the volume name, followed by the time stamp. This makes it easy to recognize which volume to remove.

- Once the volume is removed, open the Group Manager GUI and click on the snapshot.
- Under the Activities panel select **Set snapshot offline**.

This will take the snapshot offline. You can then go back into Virtual Center and **Scan for New Storage Devices** to clean up the snapshot LUNs.

EXAMPLE 2: USING SNAPSHOTS TO RECOVER GUEST-ATTACHED ISCSI VOLUMES

This example describes how to combine the VM's guest operating system's native iSCSI software initiator with the Dell EqualLogic PS Series array snapshot to increase overall data protection for the guest's data. There are many opportunities to use the guest operating system iSCSI software initiator, including configurations using VSS integration for Windows NTFS volumes, application consistent snapshots with SQL Server, and MPIO. Therefore, it is important to have a method of protecting these volumes as well. For more information on utilizing the guest iSCSI initiator with VSS tools as well as SQL Server application integration, please refer to the following Technical Reports:

SQL Server Data Protection with Auto-Snapshot Manager
Deploying Microsoft® SQL Server in an iSCSI SAN
Deploying Microsoft Windows Server 2003 in an iSCSI SAN
Microsoft Windows Aligning Disk Sectors for Optimal Performance
Deploying Microsoft Multipath I/O in an iSCSI SAN
Configuring and Deploying the Dell EqualLogic MPIO DSM in an iSCSI SAN

This example uses a Windows 2003 Server running as a VM, with two volumes on the SAN attached via the Microsoft iSCSI initiator with MPIO across two network cards. The concepts in Example 1 apply here, with the changes necessary to make it work from the guest. Again, snapshots can be scheduled throughout the day to add an extra layer of data protection to the volumes.

Step 1. Snap Volume

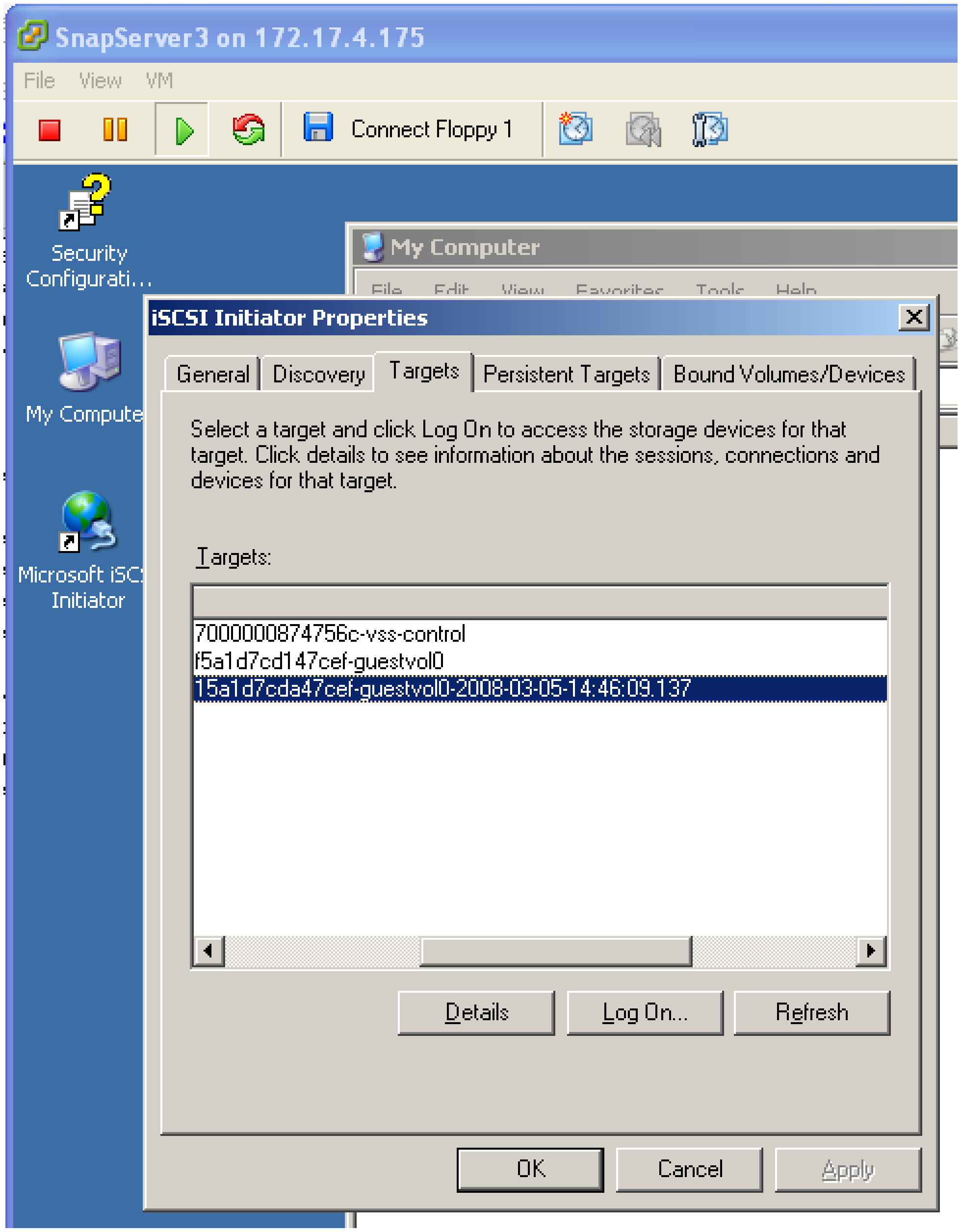
The procedures to snap the volume are the same as in Example 1. A snapshot of the PS Series volume can be taken manually or automatically according to a schedule.

Step 2. Mount Snap and Recover Data

Once a guest-attached iSCSI volume has been snapped you will be working inside that guest OS instead of using Virtual Center, and therefore do not need to enable the LVM.EnableResignature option or Rescan any of the storage adapters. Instead, the guest operating system iSCSI adapter controls will be used to mount the snap and make it available.

- First, within the PS Series GUI, bring the snapshot online. Select the snapshot you want to mount and in the activities panel under snapshots click **Set snapshot online**.
- In this example, because the Microsoft iSCSI Initiator is being used inside the guest, open that tool inside that VM.
- Click on the **Targets** tab and click **Refresh**.

The snapshot will be visible. The PS Series snapshot will appear with the iqn name, followed by the volume name, followed by the time stamp.



Select a target and click Log On to access the storage devices for that target. Click details to see information about the sessions, connections and devices for that target.

Targets:

```
7000000874756c-vss-control
f5a1d7cd147cef-guestvol0
15a1d7cda47cef-guestvol0-2008-03-05-14:46:09.137
```

- Select the snapshot volume and click **Log On**. Since this volume is being used only for data recovery it is not necessary to make it persistent. Multipathing can be enabled if desired.
- Next, open Disk Management. The volume that was just connected will be visible, but without a drive letter. Once you assign a drive letter the volume can be used for data recovery.

This is just one example of how to utilize the PS Series snapshots within the guest operating system. Dell EqualLogic provides the Auto Snapshot Manager tool (part of the Host Integration Tools) to add even more protection, including support for VSS integration within a VM that has volumes connected via the iSCSI initiator. For more information please see the Technical Reports mentioned above.

Step 3. Cleanup

Once the snapshot has been used to recover data, it can be removed from the VM.

- Open the Microsoft iSCSI Initiator and select the snapshot that is connected. Click on **Details**. Click all of the check boxes and select the option to **Log Off**. This will remove the disk from Disk Management.
- Once the volume has been removed, open the PS Series Group Manager GUI and click on the snapshot. In the Activities panel select **Set snapshot offline**. This will take the snapshot offline.

EXAMPLE 3: VM PROTECTION WITH SNAPSHOTS

PS Series snapshots provide not only a method of protecting data within the virtual machine, but also a method of protecting the full VM directory for recovery. Because of the encapsulation of files and the instant point-in-time snapshot ability of the array, this technique can be used to restore a VM that will not boot properly. PS Series volume snapshots can provide point-in-time, I/O consistent copies of each VM on the volume. Using this strategy, multiple snapshots can be taken throughout the day to enable recovery of data or of an entire VM at any point.

This example assumes that a catastrophic event occurred, causing the VM to fail to boot. One hour previously it worked properly, and a snapshot from that hour is available. Instead of rebuilding the server from a template and then restoring from tape, the snapshot and ESX file copy mechanisms can be used to recover the VM files and bring it back online.

Step 1. Snap Volume

Just as in the other examples, a snapshot of the volume that is to be recovered must be available. Follow the directions in Example 1 to create a snapshot or a schedule of snapshots for each volume.

Step 2. Mount Snapshot

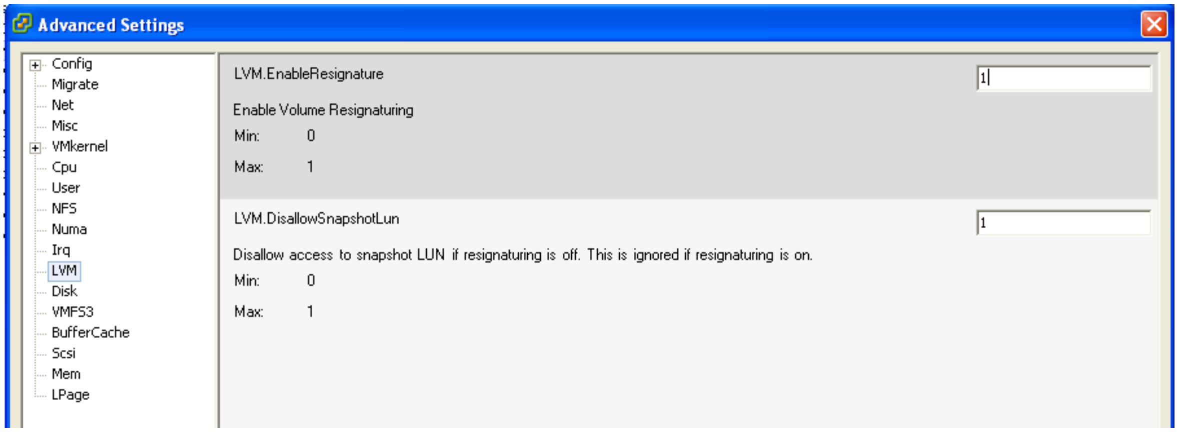
First, bring the snapshot online.

- From within the PS Series GUI select the snapshot you want to mount and in the activities panel under snapshots click **Set snapshot online**.

Note: If there are multiple volumes that were snapped as a part of a volume collection, set each one online by clicking on the collection snapshot and placing each volume snapshot online.

Now that the snapshot is online, enable ESX to see the volume. First, enable LVM to resignature the disk.

- Using VIC, on the ESX server click the **Configuration** tab, then **Advanced Settings**.
- Click **LVM** on the left and change the **LVM.EnableResignature** to 1 and click **Ok**.



LVM.EnableResignature 1

Enable Volume Resignaturing

Min: 0

Max: 1

LVM.DisallowSnapshotLun 1

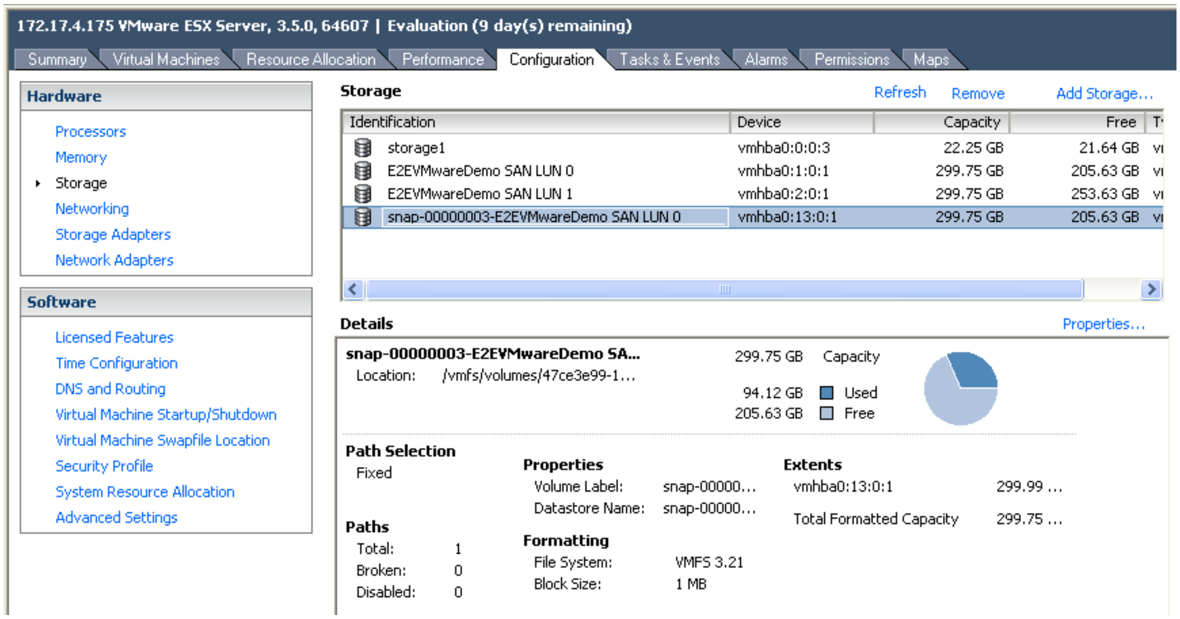
Disallow access to snapshot LUN if resignaturing is off. This is ignored if resignaturing is on.

Min: 0

Max: 1

NOTE: It is important to set this value back to 0 after using the snapshots. Failure to do so could cause production datastores to be resignatured, which will result in VMotion, DRS, and HA failing.

- When this is done, go into the **Configuration** tab and select **Storage Adapters**.
- Click on **Rescan** and choose to **Scan for New Storage Devices**. Uncheck the box for **Scan for New VMFS Volumes**.
- Next, go into the **Configuration** tab and select **Storage Adapters**. Click on **Rescan** and choose to **Scan for New Storage Devices**. Uncheck the box for **Scan for New VMFS Volumes**.
- When this is done, click on **Rescan** and now select **Scan for New VMFS Volumes**. Uncheck the box for **Scan for New Storage Devices**.
- After the rescan click on **Storage** under Hardware. You should see a new datastore with a name that starts with snap-0000xxx-volumename. This is the snapshot volume that was put online.
- Once the PS Series snapshot shows up as a datastore, disable the LVM.EnableResignature option by setting it back to 0 and clicking **Ok**.



Storage

Identification	Device	Capacity	Free	T
storage1	vmhba0:0:0:3	22.25 GB	21.64 GB	vı
E2EVMwareDemo SAN LUN 0	vmhba0:1:0:1	299.75 GB	205.63 GB	vı
E2EVMwareDemo SAN LUN 1	vmhba0:2:0:1	299.75 GB	253.63 GB	vı
snap-00000003-E2EVMwareDemo SAN LUN 0	vmhba0:13:0:1	299.75 GB	205.63 GB	vı

Details

snap-00000003-E2EVMwareDemo SA... 299.75 GB Capacity

Location: /vmfs/volumes/47ce3e99-1...

94.12 GB ■ Used

205.63 GB □ Free

Path Selection

Fixed

Paths

Total: 1

Broken: 0

Disabled: 0

Properties

Volume Label: snap-00000...

Datastore Name: snap-00000...

Formatting

File System: VMFS 3.21

Block Size: 1 MB

Extents

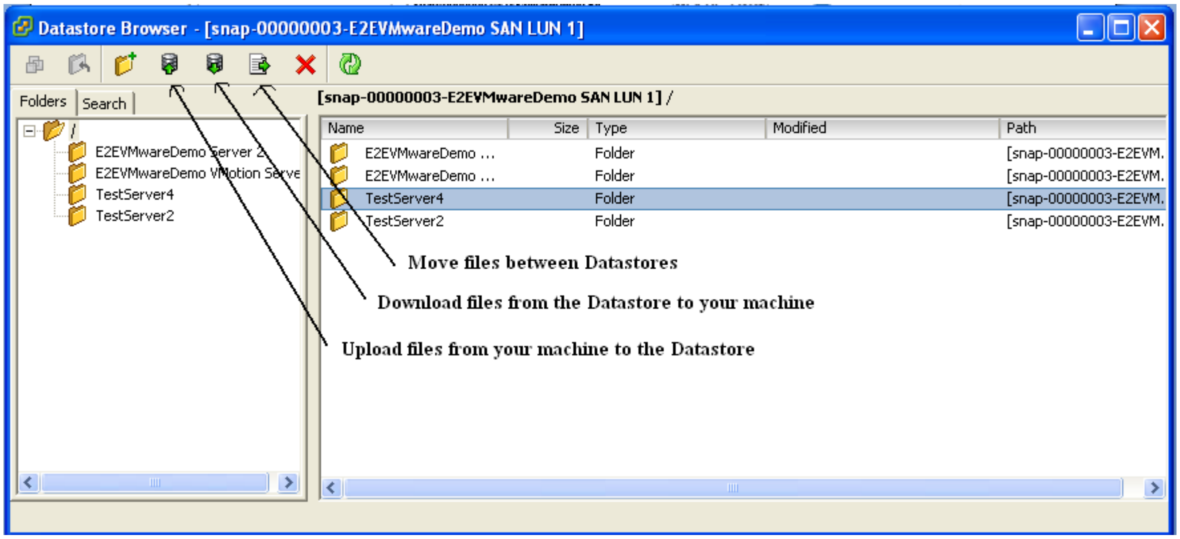
vmhba0:13:0:1 299.99 ...

Total Formatted Capacity 299.75 ...

Step 3. VM Recovery with Data Copy Tools

The next step in restoring this VM is to move the actual data from the snapshot volume to the original datastore. The assumption is that the entire directory structure will be copied, so the original VM must be powered off first.

Now that the snapshot appears under storage, select the snapshot, right-click on it, and select **Browse Datastore**. ESX provides several data copy tool options. You can upload files from your machine to the datastore, download files from the datastore to your machine, and move files from one datastore to another. This is the option that will be used to move the VM from the snapshot to the original datastore.



Datastore Browser - [snap-00000003-E2EVMwareDemo SAN LUN 1]

[snap-00000003-E2EVMwareDemo SAN LUN 1] /

Name	Size	Type	Modified	Path
E2EVMwareDemo ...		Folder		[snap-00000003-E2EVM.
E2EVMwareDemo ...		Folder		[snap-00000003-E2EVM.
TestServer4		Folder		[snap-00000003-E2EVM.
TestServer2		Folder		[snap-00000003-E2EVM.

Move files between Datastores

Download files from the Datastore to your machine

Upload files from your machine to the Datastore

- Click the button to move a file from this datastore to another datastore that Virtual Center can access.
- Select the original VM datastore and then the original file and click **Move**.

This will initiate file movement. The process may take time depending on file size, but it is generally faster than provisioning an entire server. If the server needs to be brought up immediately, follow the procedures in Examples 4 or 5 to bring the VM online; during later downtime, use this process to move the data from the snapshot volume to the original datastore.

Step 4. Cleanup

Once the snapshot VM has been returned to its original datastore, the environment must be cleaned up to prevent any error messages on the array and to release the snapshot.

- Open VIC, select the ESX host, click on the **Configuration** tab, and select **Storage**.
- Click on the snap-0000xxx-volumename datastore and click **Remove**.

Once this has been removed, it is important to clean up some of the persistent targets that ESX is seeing.

- Click the **Configuration** tab and then select **Storage Adapters**.

- Select either the iSCSI Software Adapter or the iSCSI HBA that you are using to connect to the array and click **Properties**.
- Select the **Static Discovery** tab and find the snapshot volume.
- Select the volume and click **Remove**.

The PS Series snapshot will appear with the iqn name, followed by the volume name, followed by the time stamp. This makes it easy to recognize which volume to remove.

- Once the volume has been removed, open the Group Manager GUI and click on the snapshot.
- Under the Activities panel select **Set snapshot offline**. This will take the snapshot offline.

Now, return to the Virtual Center and **Scan for New Storage Devices** to clean up the snapshot LUNs.

EXAMPLE 4: VM RECOVERY RUNNING FROM A SNAPSHOT

At times you may want to run the VM directly from the snapshot volume and not from its original datastore. For example, you may want to test the VM in a test network, or if the original VM becomes unbootable you may want to place the snapshot into production as quickly as possible and move the files during later downtime. The process is very similar to the previous example – mount the snapshot as usual, and then add the snapshot VM to the inventory and boot it. In this example the entire VM resides on one datastore or volume, and the virtual disk drive files are located on the same volume as the configuration file. If you want to bring a VM online using this method but the VM resides on multiple datastores, skip to Example 5 to see the required configuration file changes.

NOTE: When booting a snapshot VM, remember that it is an identical copy of the original VM. If the original VM is currently running, you could cause serious problems because of duplicate names and IP addresses on the network. If the original VM is already on, it is recommended to isolate the snapshot VM to a separate internal-only network for testing.

Step 1. Snap Volume

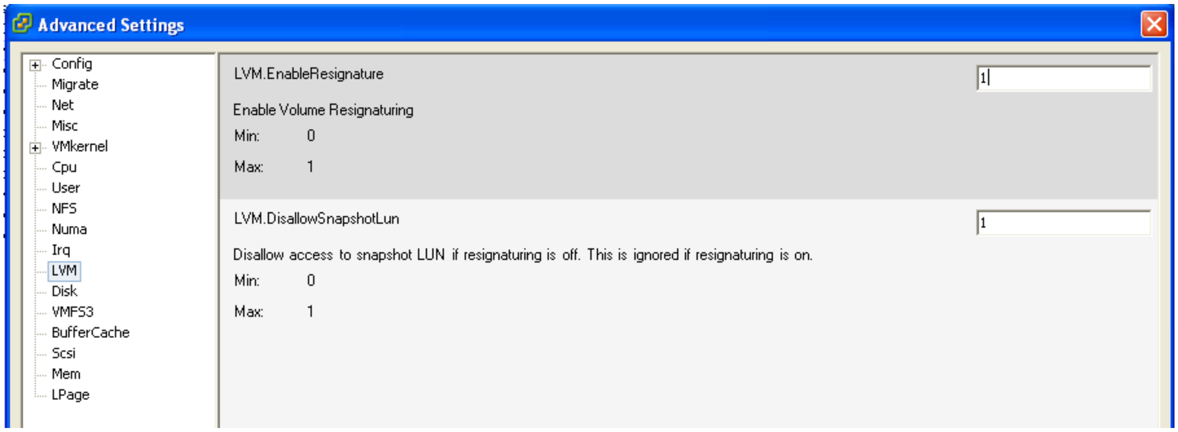
Please refer to Example 1 for the details of creating a PS Series volume snapshot.

Step 2. Mount Snapshot

First, bring the snapshot online. Within the PS Series GUI select the snapshot you want to mount and in the activities panel under snapshots click **Set snapshot online**. If multiple volumes were snapped as a part of a volume collection group, be sure to set each volume snapshot online.

Now that it is online, ESX must be enabled to see the volume snapshot. The first step is to enable LVM to resignature the disk.

- Using VIC, on the ESX host click the **Configuration** tab, then **Advanced Settings**.
- Click **LVM** on the left and change the **LVM.EnableResignature** to 1 and click **Ok**.



LVM.EnableResignature 1

Enable Volume Resignaturing

Min: 0

Max: 1

LVM.DisallowSnapshotLun 1

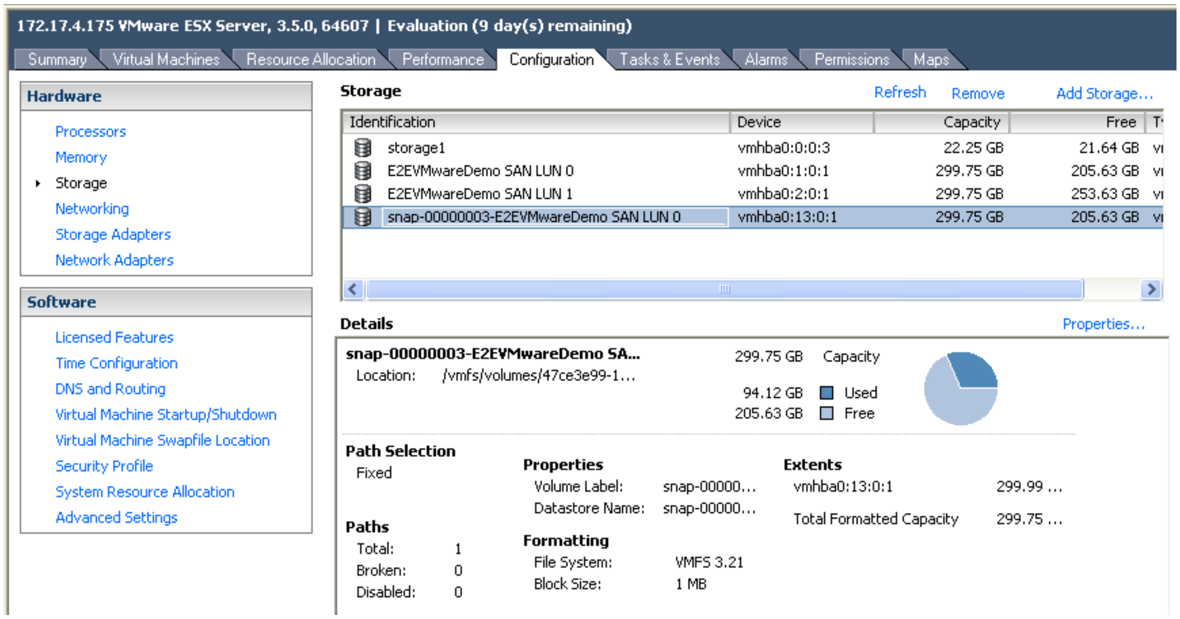
Disallow access to snapshot LUN if resignaturing is off. This is ignored if resignaturing is on.

Min: 0

Max: 1

NOTE: It is important to set this value back to 0 after using the snapshots. Failure to do so could cause production datastores to be resignatured, which will result in VMotion, DRS, and HA failing.

- When this is done, go into the **Configuration** tab and select **Storage Adapters**.
- Click on **Rescan** and choose to **Scan for New Storage Devices**. Uncheck the box for **Scan for New VMFS Volumes**.
- Next, go into the **Configuration** tab and select **Storage Adapters**. Click on **Rescan** and choose to **Scan for New Storage Devices**. Uncheck the box for **Scan for New VMFS Volumes**.
- When this is done, click on **Rescan** and now select **Scan for New VMFS Volumes**. Uncheck the box for **Scan for New Storage Devices**.
- After the rescan click on **Storage** under Hardware. You should see a new datastore with a name that starts with snap-0000xxx-volumename. This is the snapshot volume that was put online.
- Once the PS Series snapshot shows up as a datastore, disable the LVM.EnableResignature option by setting it back to 0 and clicking **Ok**.



Identification	Device	Capacity	Free	T·
storage1	vmhba0:0:0:3	22.25 GB	21.64 GB	vı
E2EVMwareDemo SAN LUN 0	vmhba0:1:0:1	299.75 GB	205.63 GB	vı
E2EVMwareDemo SAN LUN 1	vmhba0:2:0:1	299.75 GB	253.63 GB	vı
snap-00000003-E2EVMwareDemo SAN LUN 0	vmhba0:13:0:1	299.75 GB	205.63 GB	vı

snap-00000003-E2EVMwareDemo SA...
Location: /vmfs/volumes/47ce3e99-1...

299.75 GB Capacity
94.12 GB ■ Used
205.63 GB □ Free

Path Selection
Fixed

Paths
Total: 1
Broken: 0
Disabled: 0

Properties
Volume Label: snap-00000...
Datastore Name: snap-00000...

Formatting
File System: VMFS 3.21
Block Size: 1 MB

Extents
vmhba0:13:0:1 299.99 ...
Total Formatted Capacity 299.75 ...

Step 3. Recover Virtual Machine

Next, register the VM with Virtual Center so that it can be manipulated it as if it were another VM.

- In Virtual Center click on the **Configuration** tab and select **Storage**.
- Right-click on the snapshot volume and choose to **Browse Datastore**. Then open the folder that contains the VM you want to recover.
- Search for the VM configuration file, which ends in .vmx. Right-click that file and select **Add To Inventory**. Enter a new name for the VM, making sure to note that it is a snapshot or recovery.
- Place the VM in the appropriate Datacenter and Pool on the ESX server and click **Finish**.

Once this is done, the new VM will appear in the VM inventory screen in Virtual Center.

The next step differs depending on whether you are just testing the VM or are bringing it into production because the original VM has failed.

- If you are bringing the VM up to test it, first select the VM and click **Edit Settings**. Select the Network Adapters and either disconnect them or connect them to an ***internal*** test network.
- If you are bringing the VM up because the original is no longer available, do not modify the network adapter settings.

Now the VM is part of the inventory and can be powered on as a normal VM. At some point (either because the testing is complete or during downtime for the production VM) you can power down the VM and either delete it from inventory (in the case of a test) or move the files to the permanent datastore by using the procedure demonstrated in Example 3.

Step 4. Cleanup

Once you have used this process to either test the VM or move the snapshot VM back to its original datastore, clean up the environment to prevent any error messages on the array and to release the snapshot.

- Open up Virtual Center and click on the **Configuration** tab and then select **Storage**.
- Click on the snap-0000xxx-volumename datastore and click **Remove**.

Once this has been removed, it is important to clean up some of the persistent targets that ESX is seeing.

- Click the **Configuration** tab and then select **Storage Adapters**.
- Select either the iSCSI Software Adapter or the iSCSI HBA that you are using to connect to the array and click **Properties**.
- Select the **Static Discovery** tab and find the snapshot volume. Select the volume and click **Remove**.

The PS Series snapshot will appear with the iqn name, followed by the volume name, followed by the time stamp. This makes it easy to recognize which volume to remove.

- Once the volume has been removed, open the PS Series Group Manager GUI and click on the snapshot.
- Under the Activities panel select **Set snapshot offline**. This will take the snapshot offline.

You can then go back into Virtual Center and **Scan for New Storage Devices** to clean up the snapshot LUNs.

EXAMPLE 5: RECOVERY OF A VM THAT RESIDES ON MULTIPLE DATASTORES

This final example is a modification of Example 4. The primary difference is that in order to bring a VM online that has virtual disks on multiple datastores; some modifications to the VM configuration file need to be made. Again, you may want to run this VM directly from the snapshot in order to run tests, or perhaps the original VM will not boot and you need it back in production quickly. The process is very similar to the previous example, but before adding the system to inventory, manual changes must be made to the configuration file. This is an advanced step and requires actually editing the .vmx file within the datastore.

NOTE: When booting a snapshot VM, remember that it is an identical copy of the original VM. If the original VM is currently running you could cause serious problems because of duplicate names and IP addresses on the network. If the original VM is already on, it is recommended to isolate the snapshot VM to a separate internal only network for testing.

Step 1. Snap Volumes

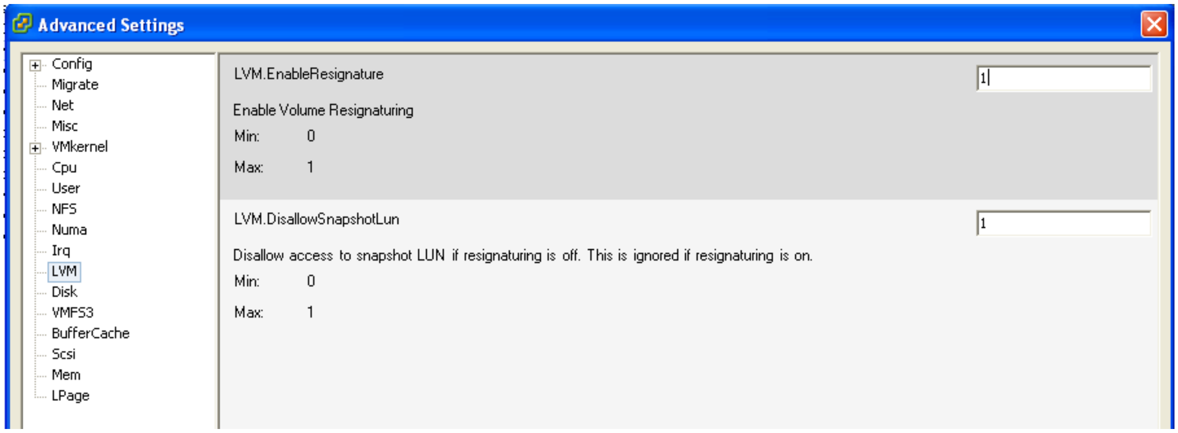
Please refer to Example 1 for detailed information regarding creating a PS Series volume snapshot. Because the VM resides across multiple datastores, use the Volume Collection process (manually or according to a schedule) to snap the entire collection to make sure that the volume snapshots are taken simultaneously.

Step 2. Mount Snapshots

First, bring the snapshots online. From within the PS Series GUI select each of the snapshot volumes you want to mount and in the activities panel under snapshots click **Set snapshot online**.

Now that they are online, ESX must be able see the volume snapshots. To accomplish this, first enable LVM to resignature the disk.

- Within VIC on the ESX server click the **Configuration** tab, then **Advanced Settings**.
- Click **LVM** on the left and change the **LVM.EnableResignature** to 1 and click **Ok**.



LVM.EnableResignature 1

Enable Volume Resignaturing

Min: 0

Max: 1

LVM.DisallowSnapshotLun 1

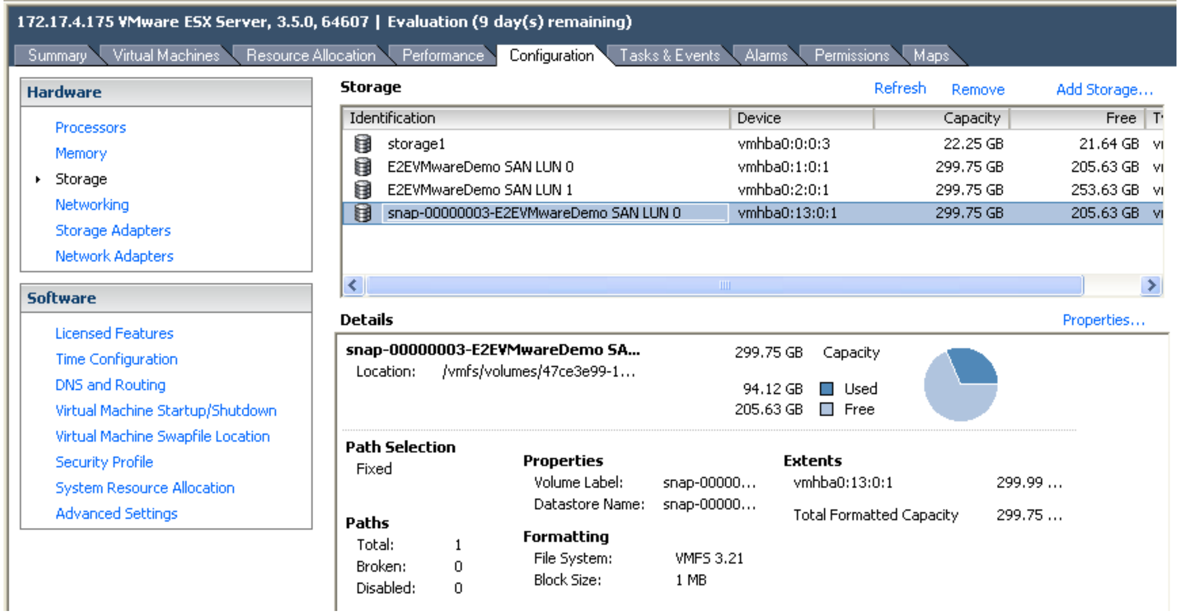
Disallow access to snapshot LUN if resignaturing is off. This is ignored if resignaturing is on.

Min: 0

Max: 1

NOTE: It is important to set this value back to 0 after using the snapshots. Failure to do so could cause production datastores to be resignatured, which will result in VMotion, DRS, and HA failing.

- When this is done, go into the **Configuration** tab and select **Storage Adapters**.
- Click on **Rescan** and choose to **Scan for New Storage Devices**. Uncheck the box for **Scan for New VMFS Volumes**.
- Next, go into the **Configuration** tab and select **Storage Adapters**. Click on **Rescan** and choose to **Scan for New Storage Devices**. Uncheck the box for **Scan for New VMFS Volumes**.
- When this is done, click on **Rescan** and now select **Scan for New VMFS Volumes**. Uncheck the box for **Scan for New Storage Devices**.
- After the rescan click on **Storage** under Hardware. You should see a new datastore with a name that starts with snap-0000xxx-volumename. This is the snapshot volume that was put online.
- Once the PS Series snapshot shows up as a datastore, disable the LVM.EnableResignature option by setting it back to 0 and clicking **Ok**.



Storage

Identification	Device	Capacity	Free	T
storage1	vmhba0:0:0:3	22.25 GB	21.64 GB	v
E2EVMwareDemo SAN LUN 0	vmhba0:1:0:1	299.75 GB	205.63 GB	v
E2EVMwareDemo SAN LUN 1	vmhba0:2:0:1	299.75 GB	253.63 GB	v
snap-00000003-E2EVMwareDemo SAN LUN 0	vmhba0:13:0:1	299.75 GB	205.63 GB	v

Details

snap-00000003-E2EVMwareDemo SA...
Location: /vmfs/volumes/47ce3e99-1...

299.75 GB Capacity
94.12 GB ■ Used
205.63 GB □ Free

Path Selection
Fixed

Paths
Total: 1
Broken: 0
Disabled: 0

Properties
Volume Label: snap-00000...
Datastore Name: snap-00000...

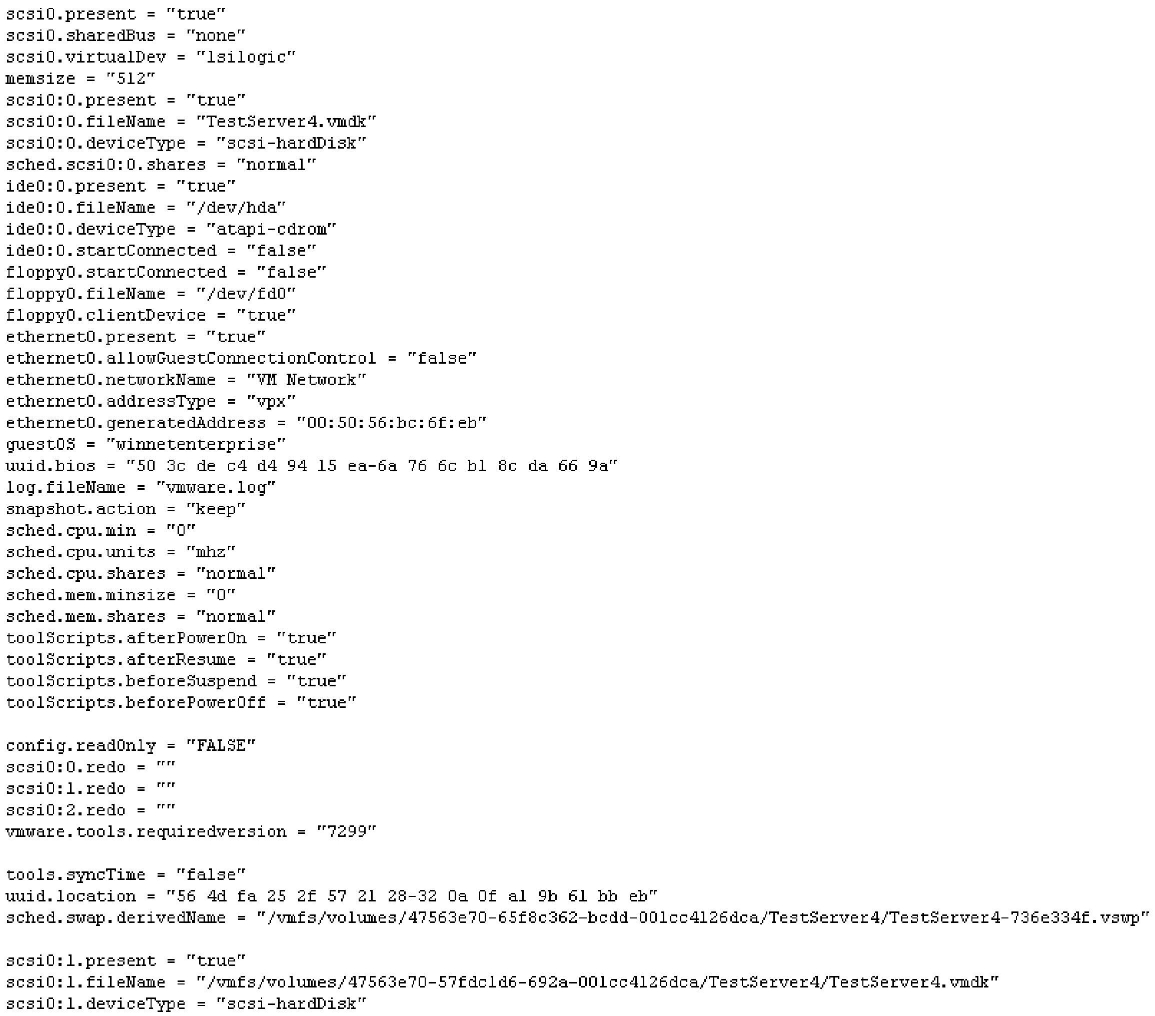
Formatting
File System: VMFS 3.21
Block Size: 1 MB

Extents
vmhba0:13:0:1 299.99 ...
Total Formatted Capacity 299.75 ...

Step 3. Recover Virtual Machine

The next step is to register the snapshot VM with Virtual Center so it can be manipulated it as if it were another VM. It is very important that the changes be made to the .vmx file ***BEFORE*** adding this VM to the inventory. Failure to do so will have the VM communicating with the original volume and not the snapshot volume. This can cause undesired issues. This will include some advanced configuration changes to the .vmx file.

Take a look at the end of the .vmx file in one of the examples. This is a Windows 2003 server that has a virtual disk drive on one datastore, and another virtual disk drive on another datastore. In the .vmx file, the virtual disk drive that is on the same datastore as the configuration file is referenced locally, but the other disk has the reference as a long identifier. This is important to note because this data will be modified.



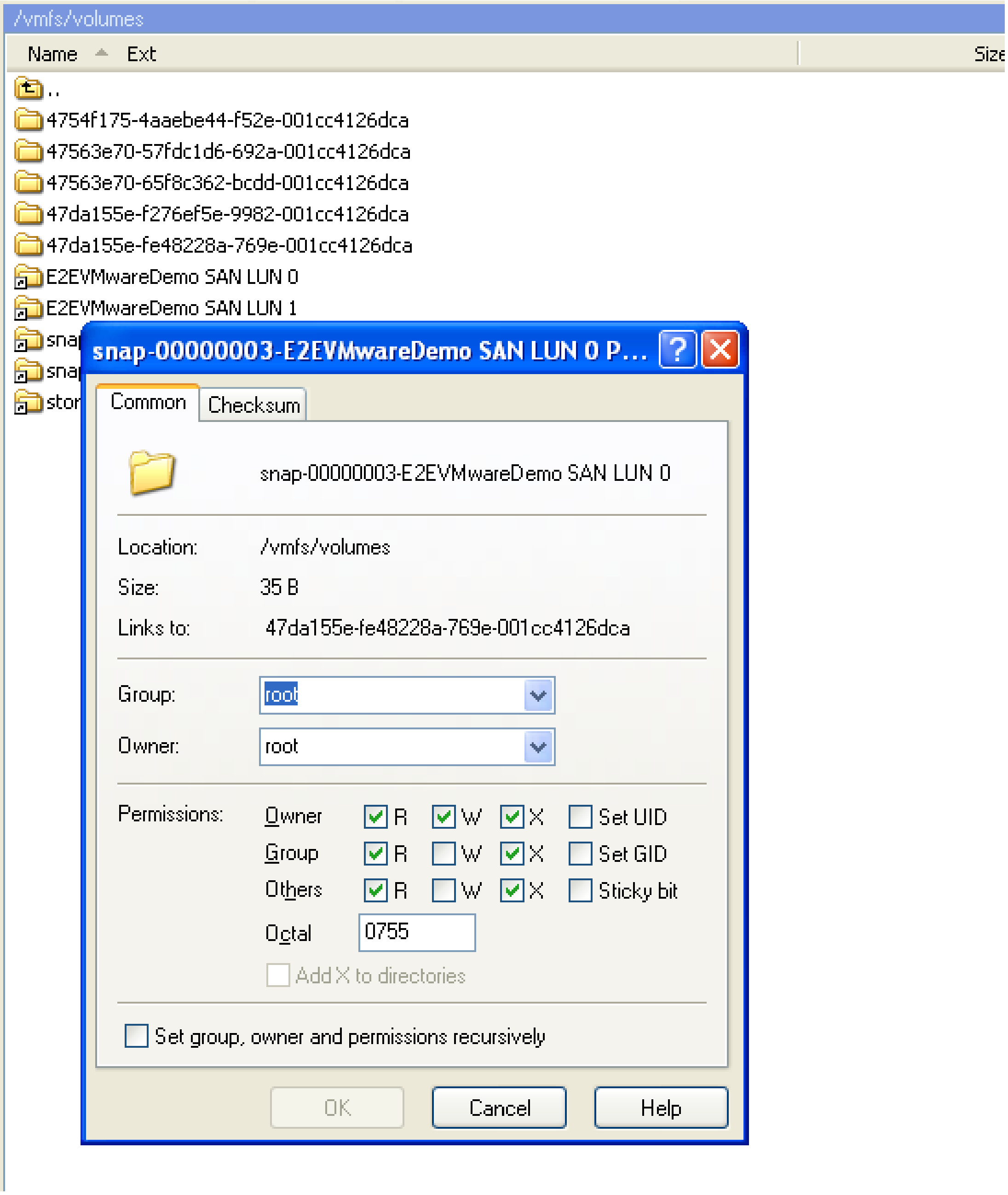
```
scsi0.present = "true"
scsi0.sharedBus = "none"
scsi0.virtualDev = "lsilogic"
memsize = "512"
scsi0:0.present = "true"
scsi0:0.fileName = "TestServer4.vmdk"
scsi0:0.deviceType = "scsi-hardDisk"
sched.scsi0:0.shares = "normal"
ide0:0.present = "true"
ide0:0.fileName = "/dev/hda"
ide0:0.deviceType = "atapi-cdrom"
ide0:0.startConnected = "false"
floppy0.startConnected = "false"
floppy0.fileName = "/dev/fd0"
floppy0.clientDevice = "true"
ethernet0.present = "true"
ethernet0.allowGuestConnectionControl = "false"
ethernet0.networkName = "VM Network"
ethernet0.addressType = "vpx"
ethernet0.generatedAddress = "00:50:56:bc:6f:eb"
guestOS = "winnetenterprise"
uuid.bios = "50 3c de c4 d4 94 15 ea-6a 76 6c b1 8c da 66 9a"
log.fileName = "vmware.log"
snapshot.action = "keep"
sched.cpu.min = "0"
sched.cpu.units = "mhz"
sched.cpu.shares = "normal"
sched.mem.minsize = "0"
sched.mem.shares = "normal"
toolScripts.afterPowerOn = "true"
toolScripts.afterResume = "true"
toolScripts.beforeSuspend = "true"
toolScripts.beforePowerOff = "true"

config.readOnly = "FALSE"
scsi0:0.redo = ""
scsi0:1.redo = ""
scsi0:2.redo = ""
vmware.tools.requiredversion = "7299"

tools.syncTime = "false"
uuid.location = "56 4d fa 25 2f 57 21 28-32 0a 0f a1 9b 61 bb eb"
sched.swap.derivedName = "/vmfs/volumes/47563e70-65f8c362-bcdd-001cc4126dca/TestServer4/TestServer4-736e334f.vswp"

scsi0:1.present = "true"
scsi0:1.fileName = "/vmfs/volumes/47563e70-57fdc1d6-692a-001cc4126dca/TestServer4/TestServer4.vmdk"
scsi0:1.deviceType = "scsi-hardDisk"
```

In this example .vmx file, the scsi0:0.fileName = “TestServer4.vmdk” is the local virtual disk. Note that the scsi0:1.fileName includes a long string that points to the other datastore – this must be changed before the VM can be placed in the inventory. Since this is a snapshot, the .vmx file is identical to the original – it still points to the secondary datastore, and must be altered to point to the secondary snapshot volume. To do this, first find the location of that datastore by opening a Linux console or using a tool such as WinSCP.



/vmfs/volumes

```
..
4754f175-4aaebe44-f52e-001cc4126dca
47563e70-57fdc1d6-692a-001cc4126dca
47563e70-65f8c362-bcdd-001cc4126dca
47da155e-f276ef5e-9982-001cc4126dca
47da155e-fe48228a-769e-001cc4126dca
E2EVMwareDemo SAN LUN 0
E2EVMwareDemo SAN LUN 1
sna
sna
stor
```

snap-00000003-E2EVMwareDemo SAN LUN 0

Location: /vmfs/volumes

Size: 35 B

Links to: 47da155e-fe48228a-769e-001cc4126dca

Group: root

Owner: root

Permissions:

Owner	☑ R	☑ W	☑ X	☐ Set UID
Group	☑ R	☐ W	☑ X	☐ Set GID
Others	☑ R	☐ W	☑ X	☐ Sticky bit

Octal: 0755

☐ Add X to directories

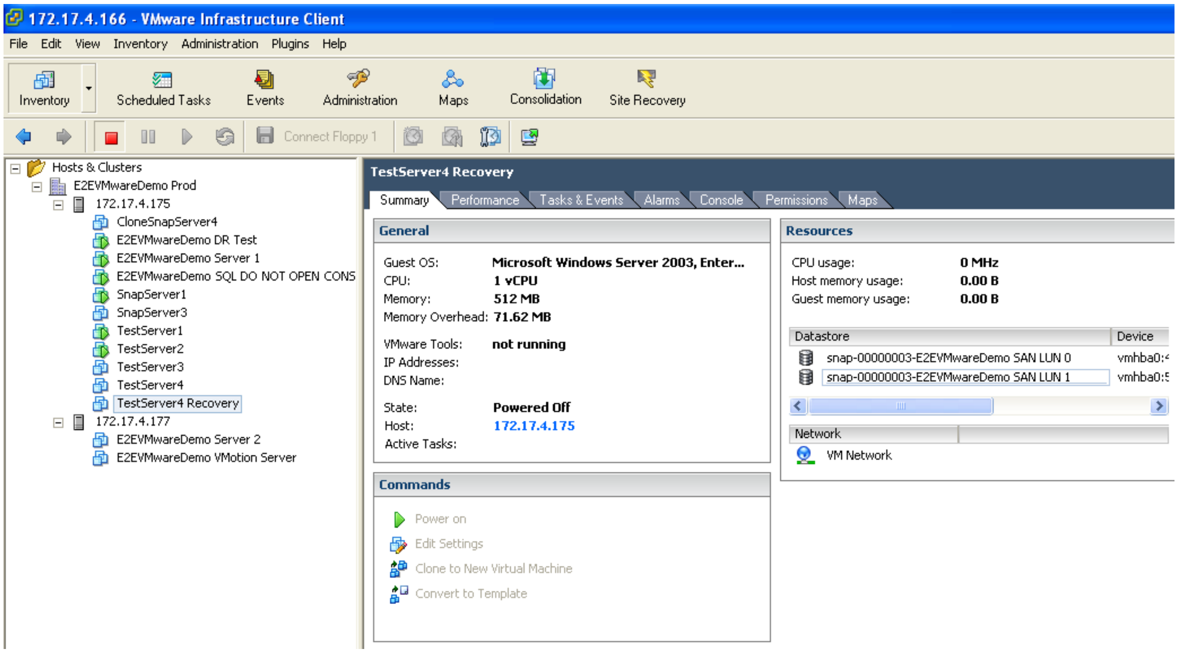
☐ Set group, owner and permissions recursively

As you can see, the snapshot of the secondary datastore points to the folder **47da155e-fe48228a-769e-001cc4126dca**. This identifies what in the original .vmx file must be changed to in order for it to point to the correct snapshot volume. After matching the datastore name with the long identifier, copy this information and change the pointer in the .vmx file. Once the change is made, save the .vmx file and then add the VM to the inventory.

- Right-click on the snapshot volume and choose to **Browse Datastore**. Then open the folder that contains the VM you want to recover.
- Search for the VM configuration file, which ends in .vmx. Right-click that file and select **Add To Inventory**. Enter a new name for the VM, making sure to note that it is a snapshot or recovery.

- Place the VM in the appropriate Farm and Pool on the desired ESX server and click **Finish**.

Once this is done, the new VM will appear in the VM inventory screen in Virtual Center. Notice in the screenshot below that both of the datastores point to the snapshot volumes because of the changes made to the .vmx file. If you do not see this. Do not go any further. Do not power on the VM as the changes were not made correctly and could cause unwanted issues with existing volumes. Remove the VM and edit the .vmx file and re-add it.



Guest OS: Microsoft Windows Server 2003, Enter...
CPU: 1 vCPU
Memory: 512 MB
Memory Overhead: 71.62 MB

VMware Tools: not running
IP Addresses:
DNS Name:

State: Powered Off
Host: 172.17.4.175
Active Tasks:

CPU usage: 0 MHz
Host memory usage: 0.00 B
Guest memory usage: 0.00 B

Datastore	Device
snap-00000003-E2EVMwareDemo SAN LUN 0	vmhba0:4
snap-00000003-E2EVMwareDemo SAN LUN 1	vmhba0:5

Network
VM Network

The next step differs depending on whether you are just testing the VM or are bringing it into production because the original VM failed.

- If you are bringing the VM up to test it, first select the VM and click **Edit Settings**. Select the Network Adapters and either disconnect them or connect them to an ***internal*** test network.

- If you are bringing the VM up because the original is no longer available, do not modify the network adapter settings.

Now the VM is part of the inventory and can be powered on as a normal VM. At some point (either because the testing is complete or during downtime for the production VM) you can power down the VM and either delete it from inventory (in the case of a test) or move the files to the permanent datastore by using the procedure demonstrated in Example 3.

Step 4. Cleanup

Once you have completed this process to either test the VM or move the snapshot VM back to its original datastore, clean up the environment to prevent any error messages on the array and to release the snapshot.

- Open Virtual Center, click on the **Configuration** tab, and select **Storage**.

- Click on the snap-0000xxx-volumename datastore and click **Remove**. Do this for any snap datastores that need to be removed.

Once these are removed, it is important to clean up some of the persistent targets that ESX is seeing.

- Click the **Configuration** tab and then select **Storage Adapters**.
- Select either the iSCSI Software Adapter or the iSCSI HBA that you are using to connect to the array and click **Properties**.
- Select the **Static Discovery** tab and find the snapshot volumes. Select the volumes and click **Remove**.

The PS Series snapshot will appear with the iqn name, followed by the volume name, followed by the time stamp. This makes it easy to recognize which volume to remove.

- Once the volume has been removed, open the PS Series Group Manager GUI and click on the snapshot.
- Under the Activities panel select **Set snapshot offline**. This will take the snapshot offline.

You can then go back into Virtual Center and **Scan for New Storage Devices** to clean up the snapshot LUNs.

SUMMARY

Shared storage in a PS Series SAN enables many of the advanced VMware features such as HA, DRS, and VMotion, but the array's built-in snapshot capability provides another layer of data protection for your virtual infrastructure. Whether you are using it to recover a single user file, run tests against VMs, or recover an entire datastore and every VM on it, the benefits are remarkable. These are just a few examples of ways to add snapshot data protection to your environment and provide an extra layer of safety for your virtual machines and data.

DOCUMENTATION AND CUSTOMER SUPPORT

Visit the Customer Service website, where you can download the latest documentation and firmware. You can also view FAQs, the Knowledge Base, and Technical Reports and submit a service request.

PS Series storage array documentation includes the following:

- *Release Notes*. Provides the latest information about PS Series storage arrays and groups.
- *QuickStart*. Describes how to set up the hardware and start using a PS Series storage array.
- *Group Administration*. Describes how to use the Group Manager GUI to manage a PS Series group. This manual provides comprehensive information about product concepts and procedures.
- *CLI Reference*. Describes how to use the Group Manager command line interface to manage a group and individual arrays.
- *Hardware Maintenance*. Provides information on maintaining the PS Series storage array hardware.

To report a problem or to get access to the resources available on the Customer Support website, go to https://www.equallogic.com/support/ and click LOGIN. If you do not already have an account, you can request one here. Once you are logged in, click Log a Case to report a problem.

To report an urgent issue, please call us at 1-877-887-7337 and speak with a member of the Customer Support team.

If you have any comments or suggestions related to this technical report, please send them to techreports@equallogic.com

Document Control and History Information

Revision	Change Author/Organization	Reason	Approved By/Organization	Date
A02	M. Cynewski / GCSS	ISO Compliance	M. Gauthier / GCSS	August 27, 2009
A01	Unknown	Initial Release	Unknown	May 2008