NETAPP TECHNICAL REPORT

SnapMirror® for Open Systems : Windows Standalone Server Full System Replication and Recovery into ESX

Ran Pergamin, NetApp
TR-3627
# TABLE OF CONTENTS

1 INTRODUCTION .................................................................................................................. 3
2 ASSUMPTIONS ..................................................................................................................... 3
3 SNAPMIRROR FOR OPEN SYSTEMS OVERVIEW .............................................................. 3
4 OVERVIEW OF SYSTEM REPLICATION (PHYSICAL TO VIRTUAL) .......................... 4
5 PREPARING THE ENVIRONMENT FOR REPLICATION .................................................. 5
   5.1 PREPARING THE VMWARE GUESTS .............................................................................. 6
   5.2 INSTALLING SNAPMIRROR FOR OPEN SYSTEMS SOFTWARE ..................................... 7
6 INITIATING REPLICATION FROM PHYSICAL TO THE VM ........................................... 7
7 SYSTEM DISK AND DATA RECOVERY IN VM ............................................................... 9
   7.1 CREATING FLEXCLONE COPIES OR LUN CLONES (OPTIONAL) .............................. 9
   7.2 RECOVERING REPLICAỘED FILE SYSTEMS ............................................................... 9
   7.3 RECOVERING REPLICAŐED VOLUME IN A RECOVERY VM ......................................... 11
   7.4 STARTING RECOVERY SERVER ................................................................................... 13
8 CONCLUSION ....................................................................................................................... 16

APPENDIX A 16
   ADD VMWARE SCSI DRIVER ON PHYSICAL SERVER ...................................................... 16

APPENDIX B 20
   ADDING THE VMWARE SCSI DRIVER DURING RECOVERY PROCESS .......................... 20

APPENDIX C 26
   USING CLONES FOR RECOVERY ...................................................................................... 26
   CREATING CLONES IN SNAPMIRROR FOR OPEN SYSTEMS ........................................... 26
   MAPPING FLEXCLONE COPIES IN SNAPMIRROR FOR OPEN SYSTEMS (OPTIONAL) ......... 27
   ADDITIONAL REFERENCES .............................................................................................. 27
   ACKNOWLEDGEMENTS ................................................................................................. 29
   DISCLAIMER .................................................................................................................... 29
1 INTRODUCTION

Full system backup and recovery in Windows® environments has traditionally been a process involving several steps. These processes could include:

- Keeping and refreshing multiple build images of Windows servers (including patches, service packs, application updates, and additional software)
- Restoring the correct server image for a particular application (for example, Exchange, SQL Server™, Oracle®, and so on)
- Installing applications to the restored server image and recovering user data
- Updating active directory information for recovered server

With the combined technology of NetApp and VMware there is now a better alternative: continuous data replication of Windows systems (including both system and data drives).

NetApp offers data replication software, SnapMirror® for Open Systems™, (was known as ReplicatorX until recently) which enables full system, continuous data replication. Also, NetApp® FlexClone® provides space-efficient read/write point-in-time copies of the replicated data for enhanced recovery options and other use cases such as development and testing.

VMware® ESX Server 3.0 enables easy recovery of the replicated Windows system and data drives regardless of the physical hardware of the original server.

The steps outlined in this technical report can be applied to several use cases very useful to core IT operations such as:

- Disaster recovery
- Nondisruptive data migration from physical to virtual servers (physical to virtual)

2 ASSUMPTIONS

Although some basic SnapMirror for Open Systems concepts and instructions are included in this document, it is assumed that the customer has a working understanding of SnapMirror for Open Systems as well as VMware ESX Server 3.0.

Because SnapMirror for Open Systems works on existing infrastructure (network, storage, operating system) in the customer’s environment, it is assumed that the following pre-implementation steps have already been completed:

- Capacity planning: Necessary to make sure that the proper infrastructure is in place to support data replication in the test or production environment.
- Compatibility matrix: Environment has been cross checked against the current SnapMirror for Open Systems compatibility matrix at http://now.netapp.com/NOW/knowledge/docs/oio/guides/tdps/tdps_interoperability_guide.pdf.

3 SNAPMIRROR FOR OPEN SYSTEMS OVERVIEW

SnapMirror for Open Systems is enterprise-class software for data replication, recovery, and continuous data sharing across the range of locations, platforms, and storage systems. SnapMirror for Open Systems can be used by customers for disaster recovery (DR), data migration of any block-based data (SAN, iSCSI,
internal IDE, SCSI, SATA, and so on) and for non disruptive replication of data to support cloning for production support applications like development and testing.

With SnapMirror for Open Systems, customers can near-synchronously replicate block data over any distance, across heterogeneous infrastructures, without the operational disruption incurred through traditional alternatives. Customers can then rapidly recover an up-to-the-second image of data that is 100% consistent.

SnapMirror for Open Systems does replication at the volume level (C:\, D:\, E:\, and so on), which eliminates complexity and guarantees data consistency regardless of the open files, system locks, or application locks, which are problematic for file-system-based replication and backup products.

Advanced features include:

- Real-time asynchronous data replication
- Compression and data reduction
- Advanced consistency algorithms
- Central reporting and configuration
- Easy-to-use scalable GUI
- FlexClone and LUN clone integration with NetApp storage for efficient point-in-time copies
- Historical and real-time reporting including RPO, network bandwidth, and data to replicate
- Support for Windows, UNIX®, and Linux® operating systems

As a software solution, SnapMirror for Open Systems provides maximum flexibility for customers to configure data replication according to particular business needs.

4 OVERVIEW OF SYSTEM REPLICATION (PHYSICAL TO VIRTUAL)

This TR will illustrate the details of replicating from a Windows 2003 physical server to a VMware ESX Server 3.0 infrastructure. The recovery method allows a choice on when and where the VMSCSI driver (required to boot the physical machine) is loaded. This can be preinstalled on the physical machine or loaded into the recovered boot image at recovery time. Both these options are detailed in this TR.

Preinstalling the driver is the simpler solution for recovery. However, this will have a redundant driver installed on the primary machine, which might affect boot up times. Details of the installation process for this driver are included in Appendix A. Installing the driver into the recovery image will require additional steps in the recovery process but will require no changes to the production machine. Details of this installation procedure are included in Appendix B.

This document will refer to the following servers:

- **Physical server**: Physical server we will replicate to a virtual machine. To replicate data, including the system partition, the SnapMirror for Open Systems Replication Client will be installed. Storage replicated from the physical server can be any block storage (SAN, iSCSI, internal IDE, SCSI, SATA, and so on).
- **Target VM**: Virtual machine that will act as a replication target and run the SnapMirror for Open Systems target server software (SnapMirror for Open Systems Replication Server). Although NetApp storage is not required, it does add point-in-time copies of the replicated data through FlexClone and LUN clones. Clones can be created directly from the SnapMirror for Open Systems GUI.
- Recovery VM: Virtual machine that will receive the replicated data from the target VM and boot up as the physical server.
- Management VM: Virtual machine that runs the management software for SnapMirror for Open Systems. This software can optionally be run on the target VM in some cases.

Figure 1 Physical-to-virtual configuration.

At a high level, the steps to complete the physical-to-virtual conversion using SnapMirror for Open Systems are:

1. Install SnapMirror for Open Systems software on servers.
2. (option 1) Install VMware SCSI driver on the physical server.
3. Replicate all drives (C:\, D:\, and so on) from the physical server to the target VM.
4. Freeze replication.
5. Create clone (optional).
6. Recover drives using SnapMirror for Open Systems utilities on the target VM.
7. (option 2) Insert the VMSCSI driver into the recovered boot image.
8. Remove drives from target VM (or map clones and leave replication in session).
9. Add drives to recovery server.
10. Boot physical server in recovery VM.

The details and options of this process are explained in detail in the following sections.

5 PREPARING THE ENVIRONMENT FOR REPLICATION

For purposes of illustration, we will replicate a physical server running Windows 2003 Enterprise Edition to a Windows guest operating system on a VMware ESX Server.

Decide the method of installing the VMSCSI driver. This driver is required to allow the replicated Windows system volume to boot within a VMware environment. If the correct driver is not installed in the Windows registry, the server will not boot in VMware and will result in a blue screen crash with error code 7B.

Appendix A details the process for installing the driver on the production machine, which will be replicated and will boot within the VMware environment without further changes.

Appendix B details the process for inserting the VMSCSI driver during the recovery process.

Consideration must also be given to the replication integrity and recovery methods. It is possible to directly use the target volume as the recovery volume. However, this will destroy the replication integrity, and a full synchronization must be performed for replication to be reestablished. The SnapMirror for Open Systems differential compare procedure can be used for this and can be quicker than a full online synchronization. A
better option is to clone the volume using NetApp FlexClone. This will allow replication to continue without disruption while allowing recovery of the server. This process is discussed in Appendix C.

5.1 PREPARING THE VMWARE GUESTS

In this example, three VMware guest operating systems will be used.

**Target VM:** This will be a Windows guest operating system that will have the NRS software installed. Also, target volumes must be available for replication. SnapMirror for Open Systems replicates data at the volume level, so there must be volumes of equal or greater size on the target VM. Additionally, space is required for replication logging. Refer to the SnapMirror for Open Systems planning and Installation guide to size the log volumes.

When attaching disk storage to the target VM, you can use one of the following:

- Virtual disk from an ESX VMFS (data store)
- A raw device mapped (RDM) VMware volume
- Disk connected with the iSCSI software initiator from Microsoft installed on the target VM

The choice of connectivity method depends on the target storage configuration and performance requirements. This discussion is outside the scope of this document. Refer to VMware documentation and product specialists to assist in making the choice.

Make sure you create the target partitions as NTFS partitions. The target partitions to host the copy of the system volume should be created as basic primary partitions.

All of these options will allow you to recover and incorporate point-in-time copies (discussed in Appendix C).

**Figure 2**

**Recovery VM:** This server can be created when the replicated volumes are available for recovery. In the example above, the recovery VM will boot from the replicated system drive (currently the y:\ drive) on the target VM. The replicated system volume will be allocated as “disk 0” on the recovery server and will become the C drive on boot.

**Management VM:** SnapMirror for Open Systems configuration, monitoring, and control are all centrally managed from the SnapMirror for Open Systems Management Server. This is a software module that can optionally be installed on the recovery VM instead of a dedicated server.
5.2 INSTALLING SNAPSHOTMIRROR FOR OPEN SYSTEMS SOFTWARE


Installation in the above example:

Physical server: Install the SnapMirror for Open Systems Replication Client module. This is a small-footprint module that pushes write updates to the target over TCP/IP in real time at near 0 RPO.

Target VM: Install the SnapMirror for Open Systems Replication Server module. This will receive incoming write updates from the physical server and maintain a consistent/recoverable image of the data volumes being replicated.

Management VM: Install the SnapMirror for Open Systems Management Server module. This will give administrators a central point for managing all replication. This includes configuration, monitoring, creating point-in-time copies, and historical reporting. This software module can be installed to the recovery VM optionally for data migration and other applications.

6 INITIATING REPLICATION FROM PHYSICAL TO THE VM

2. If Java™ has not been installed on the machine, a Java install window will appear. Install Java.
3. Assign replication log volumes on the recovery server. These logs are specific to SnapMirror for Open Systems and are typically 10% of the disk capacity being replicated.
4. Next, create a bitmap. The bitmap might be a separate raw (no NTFS format) partition or a file in Windows 2003 Server. The bitmap is critical for monitoring updates, so place it on redundant local disk if possible.
5. Create a site by right clicking the management server in the left panel and choosing Add Site
6. Right click the raw site, then add the SnapMirror for Open Systems Replication Client → SnapMirror for Open Systems Replication Server (physical server → target VM).
7. Note that the Windows system disk on the SnapMirror for Open Systems Replication Client is not discovered with the “detect disks” option. The system disk must be added manually using the “add volume” option or by changing the .ini parameters to include the system disk discovery for “detect disks.”
8. Select the GUI view and drag the volumes that contain the Windows system disk and any data volumes required to recover the complete server.

Important note: System and data drives might require perfect write-order fidelity for seamless application recovery. If this is the case, all volumes should be configured in a SnapMirror for Open Systems consistency group called a session. The graphic below represents all volumes in a single session (Session1). All volumes have the exact same recovery point.

Once initial synchronization is complete for all volumes in the session, you will see the real-time RPO (in this case, the target drives are one second behind the primary).
Figure 3
7 SYSTEM DISK AND DATA RECOVERY IN VM

To recover replicated data or make a point-in-time copy, you must issue the Freeze command to SnapMirror for Open Systems. Freeze will bring all volumes to the nearest point of consistency and stop applying updates.

![Figure 4](image)

One replication has achieved a frozen state; the volume is ready for recovery.

7.1 CREATING FLEXCLONE COPIES OR LUN CLONES (OPTIONAL)

Point-in-time copies can be created if the storage on the target VMware ESX infrastructure is NetApp FAS storage. Clones can be used for the following uses without disrupting replication:

- Development/test/QA
- Backup
- Data mining

It is a best practice to create point-in-time copies when recovering servers and coexisting with a disaster recovery solution. With FlexClone copies/LUN clones, this can be accomplished directly from the SnapMirror for Open Systems GUI and be nondisruptive to ongoing replication. See Appendix C for details on using FlexClone copies/LUN clones and the integration with the SnapMirror for Open Systems GUI.

7.2 RECOVERING REPLICATED FILE SYSTEMS

Be sure the volume replicas (or optional clones) are available to the target VM (SnapMirror for Open Systems Replication Server). If directly using the target volumes, then the replication should be deactivated at this stage.

The procedure below assumes that clones are being used. Note that the cloned volume can be attached to the SnapMirror for Open Systems Replication Server for the recovery steps or to a helper server. In either case, the following actions are system administration activities or are completed outside the SnapMirror for Open Systems GUI.

Data recovery is a three-step process:

1. Run the disksignature utility on the cloned volume.
2. Mark the partition as active (only if it is a system partition) in disk manager.
3. Check the boot.ini settings.

The disksignature will mount the partition, and let Windows identify it as NTFS partitions.

To run disksignature, go to → console of the target VM (SnapMirror for Open Systems Replication Server).
Open Windows Command Prompt (cmd). From the command line, change directories to binary folder of the NRC:

In this directory, execute `disksignature tv=x:\ fixall=1`.

Figure 5

In this example, `x:\` is the drive containing the clone of the physical server system partition. Note that this volume is not visible in the SnapMirror for Open Systems GUI. Successful output of this command should look like this:

```
C:\WINNT\disksignature tv=x:\ fixall=1
Trying to open m\ <\\\\Volume(d15dca06-9516-1dd-8608-80000294d0f7)>
Exclusively lock for volume device was acquired.
Detecting physical device for volume...
Physical device 4 was detected to contain the requested volume.
Disk \\physicalDrive was opened successfully.
Detected MBR disk
Disk head count is 255
Disk Sectors per track value is 63
Changing the entire content of sector 0

New signature is: NTFS
Changing hidden sector offset from 63(C3h) to 63(C3h)
Changing "Number of head" field inside partition boot sector from 255 to 255
Changing "Sector Per Track" field inside partition boot sector from 63 to 63
Fixing MBR after shuffle operation.
Partition number for the volume is 1
Current MBR FS ID is 7
Changing MBR FS ID from 7 to 7

Conversion successful for m:\
```

Operations performed during disksignature processing:
- Volume relative offset field was set to 63
- Volume "Number of Heads" was set to 255
- Volume "Sector Per Track" was set to 63
- Volume was successfully shuffled and re-written to volume device.
- MBR was changed to indicate partition now have NTFS.

```
```C:\WINNT

Figure 6 - Running DiskSignature

Note that this screenshot shows the Disksignature command for volume M.
Replicated system partitions also are required to be marked as ACTIVE in disk manager.

***Failure to mark the system partition as ACTIVE will result in a volume that fails to boot. Since x:\ is a replicated system partition, this is a required step for that volume.

Open Windows Disk Manager; right click → System Drive Replica Partition (x:\).
Select → Mark as Active.

Recover all other data drives with the disksignature process above but do not set data drives as active partitions. Only the system partition should be marked as active.

Check the boot.ini file on the replicated system drive.

The boot.ini file must be configured to boot from Partition 1 on disk 0; see the example below. Some server manufacturers include a recovery partition as partition 1 and set the server to boot from partition 2. Servers that boot from the SAN might also have additional information that could affect the boot process in VMware.

Example of Boot.ini correctly set up:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS=“Windows Server 2003, Enterprise” /fastdetect
```

7.3 RECOVERING REPLICATED VOLUME IN A RECOVERY VM

Within the VMware infrastructure client, go to the target VM. You cannot remove drives from a VM unless the VM is shut down, so you are required to shut down the target VM and power it off to move the drives (using clones avoids this temporary interruption to the replication target).

A best practice is to use iSCSI to attach the clones to the target (SnapMirror for Open Systems Replication Server) server. With iSCSI it is possible to attach and remove volumes from a Windows server without requiring a reboot.

Be sure not to delete the drives used by other replication sessions or the system drive of the target VM. Also, do not delete the drives from the data store as they will be moved to the recovery VM. It is important to note the VMFS and location of the VMDK files. You will need this information when adding the drives to the recovery VM.
Once the drives have been removed from the target VM, they can be added to the recovery VM.

Create the recovery VM or use one that was already created. Follow the wizards in ESX Server to create a VM for recovery.

On the recovery VM, edit settings. Add each virtual disk or RDM you want to recover. You will need to locate each VMDK file on the data store you want to recover.

In Edit Settings → Add → Hard Disk.

Use an existing virtual disk.

Figure 9

Locate the disk on the (VMFS) data store and choose next.

If the drive you are adding is the system disk, make sure that the SCSI ID is 0,0 as below:

Figure 10
If the option to install the VMSCSI driver at recovery time has been chosen, go to Appendix B and follow the procedure using VMware converter.

Add all other data drives to the recovery VM.

Once the drives are added, make sure that the storage adapter is a BusLogic (LSI will be selected by default). Note that you should only change this option if you preinstalled the VMSCSI driver on the production machine. Do not change this option if you chose the option to install the VMSCSI driver at recovery time using a VMware converter.

![Figure 11](image)

**Note: The VMware driver is a BusLogic driver. This is required to boot within VMware. If LSI Logic (default) is selected here, it will result in a Windows blue screen until the appropriate adapter is selected.**

**7.4 STARTING RECOVERY SERVER**

In the VMware virtual infrastructure client, select the recovery VM from the list of servers.

Start Server.

If the drives moved to the recovery VM were virtual drives originally created with the LSI Logic driver, you will get an informational warning that the drive was created with the LSI Logic driver and might not boot with BusLogic. Remember, the BusLogic driver loaded on the system partition. so select Yes to continue and use the BusLogic driver for each virtual drive.
Windows should boot normally. You might get the following message once bootup is complete. This will happen if you froze the replication with the production machine running. You will not get the message if the production was shut down correctly before freezing the replication and starting the recovery process.

Complete the information and continue booting.

It is a best practice to install the VM tools as part of the recovery process. This will allow the video, keyboard, mouse, and NIC drivers to be set to the VMware specific drivers, rather than the generic Windows drivers.

Your physical server is now running in a VMware guest operating system.

Note: If the physical server is still running, there might be active directory conflicts. You can solve these by renaming the recovery server and adding it to the active directory. There should not be an IP conflict.
because the physical server did not have a virtual NIC and therefore no IP configuration. The virtual NIC will use DHCP by default and grab the next available address.
8 CONCLUSION

SnapMirror for Open Systems provides a nondisruptive method of replicating all data from a physical server (including system disk) to a VMWare virtual machine. Important use cases for IT include:

- Migration from physical machines to virtual machines (physical to virtual)
- Disaster recovery to VMWare infrastructures
- Provisioning of development and Q/A testing environments
- Eliminate process for patches and service packs on recovery servers
- Optional multiple point-in-time copies of all server data which are read/writable and industry leading for performance and efficiency

Using SnapMirror for Open Systems with VMWare ESX Server 3.0 provides a unique solution for physical to virtual:

- Continuous replication of all block storage devices with guaranteed consistency across all files, applications, and operating system data
- Any server hardware or disk storage device support
- No disruption to production servers during the continuous replication process

Details described in this technical report are specific to physical server to virtual machine replication using SnapMirror for Open Systems. For more information regarding SnapMirror for Open Systems installation, refer to the additional resources section of this document in Appendix C.

APPENDIX A

ADD VMWARE SCSI DRIVER ON PHYSICAL SERVER

The first step that is required for a physical server to be recovered in a VMWare guest is installing the VMWare SCSI driver. Note: A server must have the VMWare SCSI driver installed in order to boot in a guest operating system.

To install the VMWare driver manually to the physical server:

Open Control Panel on the physical server console and choose → Add/Remove Hardware Devices.
Select → Next> on the Welcome screen.
Next you will be asked if the hardware is connected. Select → Yes.

Figure 15

Scroll to the bottom of the Installed hardware list and choose → Add a new hardware device.
Figure 16

Select → Install the Hardware that I manually select from a list [Advanced].

Figure 17
Select ➔ Show All Devices.

Figure 18

Browse to the location of the VMware SCSI driver and open ➔ VMSCSI.INF file. You can obtain the driver at www.vmware.com.

Figure 19

Select ➔ VMware SCSI Controller.

Figure 20

Upon completion, you will see the VMware SCSI controller cannot start. This is perfectly normal (you are not currently running the server in a VM). The driver will not be used until the system is loaded in a VM guest operating system.
In Windows device manager, you will see the controller listed.

Figure 21
APPENDIX B

ADDING THE VMWARE SCSI DRIVER DURING RECOVERY PROCESS
The VMware product VMware Converter is used to insert the VMSCSI driver into the replicated boot volume to make it bootable within a VMware environment.

The following procedure is carried out with VMware Virtual Infrastructure client version 2.0.1 and VMware Converter version 3.0.2u1. There might be differences between the screenshots and instructions below if you use different versions in your recovery environment.

Install the VMware Converter utility on either the SnapMirror for Open Systems Replication Server server or another helper server.

Create the recovery virtual server and attach the replicated boot volume (or clone of the volume) as disk 0.

Start the VMware Converter utility:

![Figure 22 Select Configure Machine from the top menu.](image-url)
Figure 23 - Follow the wizard to complete the process

Figure 24 - Select ESX Server or VirtualCenter virtual machine
Log in to the ESX Server or VirtualCenter server where the recovery server is located using a login with the correct credentials to allow VMware Converter to run.
Select the recovery server where you want to install the VMSCSI driver. You will already have attached the replicated boot volume (or clone) to this virtual machine.

The VMware converter process starts to run, first determining that there is a valid operating system on the disk.

---

**Figure 27**

The VMware converter process starts to run, first determining that there is a valid operating system on the disk.

---

**Figure 28**

Your virtual machine will be reconfigured so that it is usable. In addition, you can also enhance and/or customize your virtual machine.

- Install VMware Tools
- Customize the identity of the virtual machine

You can change the hostname, configure the network settings, etc.
Select Install VMware Tools. This is the main process to install the VMware SCSI driver.

It is possible to select Customize the identity of the virtual machine. This option allows the name of the server and IP address to be changed before booting. This option is useful but is outside the scope of this TR document.

![Figure 29](image)

Select Finish to complete the task. Note that no customization was selected.

![Figure 30](image)
The converter application proceeds to install. Progress is shown on the screen. Conversion logs are generated and should be reviewed if there are any errors.

At this stage the recovery server is bootable. All the necessary changes have been made to the replicated boot volume to make it bootable. Return to the main document to continue with the recovery process. Note that the recovery server will automatically reboot to complete the postinstall tasks as the drivers are added to the Windows registry.
APPENDIX C

USING CLONES FOR RECOVERY

If the storage device used by the target VM and ESX Server is NetApp, you can greatly enhance the overall solution with FlexClone copies and LUN clones. Before creating clones from the SnapMirror for Open Systems GUI, you must first:

- Associate the target VM to NetApp storage
- Associate volumes (drive letters or mountpoints) on the target VM to the correct LUNs

One more note on associations. When associating the target VM to the NetApp storage, you must specify the initiator attached to the storage. There are two options here:

Target VM drives are on VMFS:
1. Use the ESX Server FC or iSCSI initiator for the SnapMirror for Open Systems Replication Server.
2. Clones will be mapped back to ESX, and the VMFS will appear as a Snapshot™ copy of the data stores on that LUN automatically. The Snapshot copy will contain the VMDK files to add to the recovery server.

Target VM drives are connected with the Windows iSCSI initiator:
1. Specify the software iSCSI initiator of the guest operating system for the SnapMirror for Open Systems Replication Server.
2. Map the LUN back to ESX and pass it to the recovery VM as an RDM.

CREATING CLONES IN SNAPMIRROR FOR OPEN SYSTEMS

Open the SnapMirror for Open Systems GUI and right click the session.
Under the Session tab, select → Clone Session.

This will open the clone session dialog box. All volumes associated to NetApp LUNs and volumes can be selected for cloning.

![Session: Clone Session](image)

Figure 31
Once cloning is complete, you can unfreeze and continue to replicate data while testing the point-in-time clone.

**MAPPING FLEXCLONE COPIES IN SNAPMIRROR FOR OPEN SYSTEMS (OPTIONAL)**

Mapping to map the FlexClone copy, open the SnapMirror for Open Systems GUI and right click the target VM volumes. In the menu, select → Query Clones under the NetApp tab.

![Figure 32](image)

From this menu in the SnapMirror for Open Systems GUI, you can split, rename, and destroy all clones created on the NetApp storage.

Also, this menu provides the ability to map each clone to an initiator group (FC or iSCSI) created on the NetApp storage. The initiator group should map to the appropriate VMware ESX Server or guest operating system as described in section 8.1.

After rescanning the HBA on the ESX Server, you should see the available LUNs representing the replicated clones.
If the Windows iSCSI initiator was used, simply rescan disk in disk manager.

Once clone drives are mapped back to the target VM, use the recover process described in section 6.3. If the cloned LUN was a VMFS, then you will recover the VMDK drives from a data store preceded by snap. If it is an RDM, it will be passed directly from the ESX Server to the recovery VM after the recovery procedure outlined in section 6.3 is complete on the target VM.

ADDITIONAL REFERENCES

**NetApp**

SnapMirror for Open Systems Software  

SnapMirror for Open Systems Documentation  

SnapMirror for Open Systems Compatibility Matrix  
ACKNOWLEDGEMENTS
The author would like to thank the following individuals for their contribution in this technical report:

- NetApp, Inc.
- SnapMirror for Open Systems Development Team
- Richard Corrigan (for all his valuable input)

DISCLAIMER
Each environment has its own specific set of requirements, and no guarantees can be given that the results presented in this report will work as expected on other platforms. This paper should assist in the research and troubleshooting that might be required in a particular case and serve as a checklist of items to be aware of. Please forward any errors, omissions, differences, new discoveries, and comments about this paper to ran.pergamin@netapp.com.