QSAN Official Document

Achieve DR Solution in VMware with Snapshot Consistency

Application Note

July 2022

ANNOUNCEMENT

Copyright

QSAN believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

Trademarks

- QSAN, the QSAN logo, QSAN.com, XCubeFAS, XCubeSAN, XCubeNXT, XCubeNAS, XCubeDAS, XEVO, SANOS, and QSM are trademarks or registered trademarks of QSAN Technology, Inc.
- Microsoft, Windows, Windows Server, and Hyper-V are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.
- Linux is a trademark of Linus Torvalds in the United States and/or other countries.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Mac and OS X are trademarks of Apple Inc., registered in the U.S. and other countries.
- Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
- VMware, ESXi, and vSphere are registered trademarks or trademarks of VMware, Inc. in the United States and/or other countries.
- Citrix and Xen are registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries.
- Other trademarks and trade names used in this document to refer to either the entities claiming the marks and names or their products are the property of their respective owners.

TABLE OF CONTENTS

FIGURES

NOTICES

Information contained in this document has been reviewed for accuracy. But it could include typographical errors or technical inaccuracies. Changes are made to the document periodically. These changes will be incorporated in new editions of the publication. QSAN may make improvements or changes in the products. All features, functionality, and product specifications are subject to change without prior notice or obligation. All statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

PREFACE

Executive Summary

This document provides technical guidance for setting up DR (Disaster Recovery) solution in VMware environment and making sure that the replicated data will be consistent with special script implemented in ESXi server, and it leads XCubeFAS, XCubeSAN, XCubeNXT, and XCubeNAS products being able to achieve real DR with snapshot consistency, it is no longer necessary to install any agent in the environment before achieving this.

Audience

This document is applicable for QSAN customers and partners who are interested in learning about DR solution on VMware. It assumes the reader is familiar with QSAN products and has general IT experience, including knowledge as a system or network administrator. If there is any question, please refer to the user manuals of products, or contact QSAN support for further assistance.

Technical Support

Do you have any questions or need help trouble-shooting a problem? Please contact QSAN Support, we will reply to you as soon as possible.

- Via the Web: https://www.qsan.com/technical_support
- Via Telephone: +886-2-77206355
- (Service hours: 09:30 - 18:00, Monday - Friday, UTC+8)
- Via Skype Chat, Skype ID: qsan.support
- (Service hours: 09:30 - 02:00, Monday - Friday, UTC+8, Summer time: 09:30 - 01:00)
- Via Email: support@qsan.com

Information, Tip, and Caution

This document uses the following symbols to draw attention to important safety and operational information.

INFORMATION

INFORMATION provides useful knowledge, definition, or terminology for reference.

TIP

TIP provides helpful suggestions for performing tasks more effectively.

CAUTION

CAUTION indicates that failure to take a specified action could result in damage to the system.

1. INTRODUCTION

In virtualization environments, the ever-increasing data production and demand continue to grow, resulting in an increasing demand for stable backups of virtual machines. This document introduces the concept of DR (Disaster Recovery) and provides technical guidance for setting up a DR solution in the VMware environment.

1.1. Disaster Recovery

DR (Disaster Recovery) is about preventing total failure of mission critical business systems and to recover within minimum time and impact. Preventing data loss requires a continuous data protection method. This includes preparation for and recovery from events of human error, software and hardware failure, network down, internal or external power failure and all other events. To beat this challenge, IT managers must plan for redundancy of one or more backup systems at different locations. This involves constant or periodically data duplication to infrastructures at different sites to ensure business continuity from constant availability.

Figure 1-1 Top Reasons for Disaster Recovery

1.2. Challenge

Today, backup is considered to be one of the most important parts of implementing a data center environment. Backing up data in a single location is no longer sufficient to prevent

disasters. IT managers may need to prepare another copy of important data at a remote site. Disaster recovery solution becomes the best choice. Virtualization environments may have their own DR applications, but they are usually more expensive. Storage vendors support the same backup function locally at no additional charge, but the headache here is the cached data stored in the server memory.

For those Brand A suppliers, this is not a problem, because they have implemented an additional tool installed in the environment to support the function of requesting the server to queue its I/O when taking a snapshot on the storage side, even if shooting It is the complete image of the data written after the snapshot is completed. Without this feature, the copied data will be inconsistent, but the effort to install the agent is another matter.

This document will help you set up the environment, and the results are as above, but you don't need to install any agent in the environment before that. This can be easily achieved through simple scripts and snapshot copies stored in QSAN.

2. DISASTER RECOVERY SOLUTION IN VMWARE

In this chapter, we provide detailed operations for configuring the DR solution in the VMware environment, and ensure that the replicated data is consistent with the special script implemented in the ESXi server. The procedure is as follows.

1. The prerequisite is to set up an ESXi server.
2. Configure a remote replication task to backup VM files.
3. Create a script in the ESXi server to rotate the snapshots.
4. Roll back replication task for disaster drills.

You can implement this DR solution in XCubeFAS, XCubeSAN, XCubeNAS, and XCubeNAS series products. These series of products are separated in step 2 and step 4, and there are different setting methods.

2.1. Setup ESXi server

The environment prepared here is an ESXi 6.5 server, installed with a 10G HBA card, directly connected to QSAN storage, and ensure that the ESXi server is managed by vCenter.

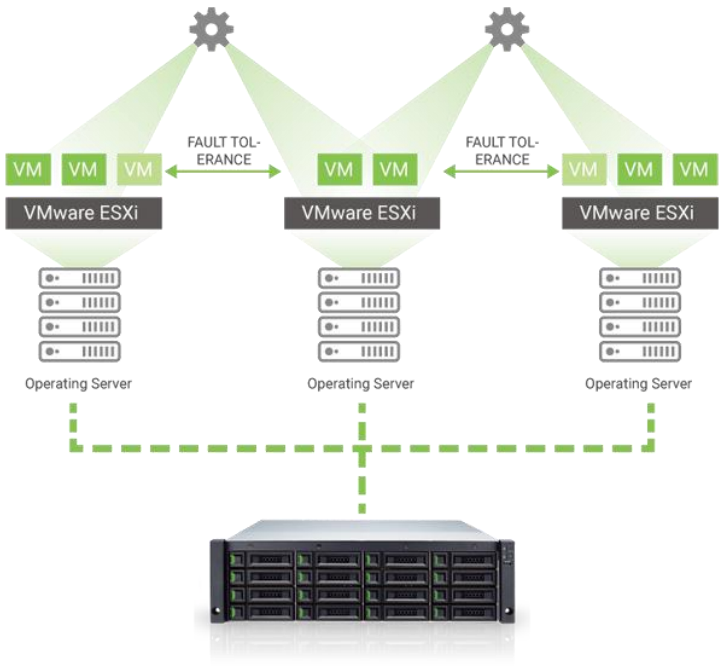

Figure 2-1 ESXi Server Architecture

2.2. Configure Remote Replication

To configure a remote replication task, you need to set up two QSAN storage systems, and the available space of the target unit must be greater or equal to the source unit. Otherwise, the snapshot replica function may fail due to insufficient storage space. Although the setting method is different, the following sections describe the configuration separately.

2.2.1. XEVO Configuration

Prepare two XCubeFAS storage systems named FAS-a and FAS-b. The following is the procedure.

1. Connect one of 10G ports from FAS-a to FAS-b.
2. In FAS-a, create a pool and a volume. And then set the snapshot space to make the snapshot replica function work normally.
3. In FAS-a, mount the created volume to the prepared ESXi server.
4. Create a VM (Virtual Machine) based on the mounted Datastore in the ESXi server.
5. In FAS-b, repeat steps 2 above to create the same or larger volume size as FAS-a. You may also need to set up snapshot space. Or you may skip this step if you use auto replication to configure the remote replication task.
6. In FAS-a, select the **Protection** tab to create a remote replication task to the replica volume in FAS-b.

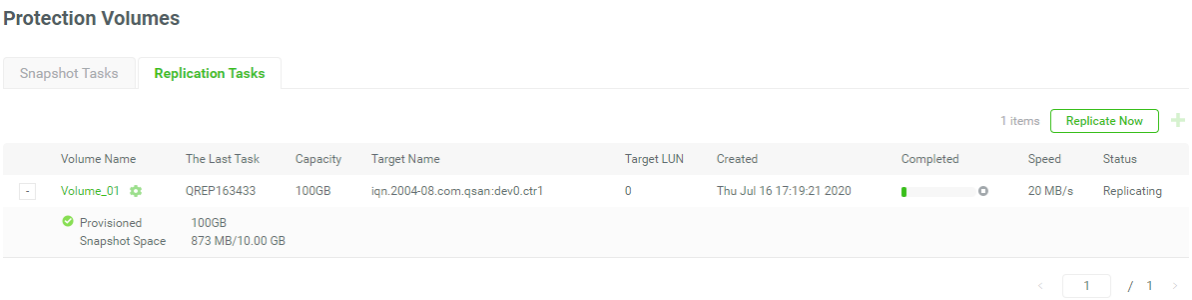

Figure 2-2 Configure a Replication Task

7. Open the console of the VM in the ESXi server, and periodically put some files (such as robocopy utility) to continuously increase the data.

INFORMATION

Robocopy, for "Robust File Copy", is a command-line directory and/or file replication command for Microsoft Windows. Please see Robocopy in Wikipedia.

8. Create scheduled snapshots in this VM from the vCenter UI, in this example, we take 5 snapshots.

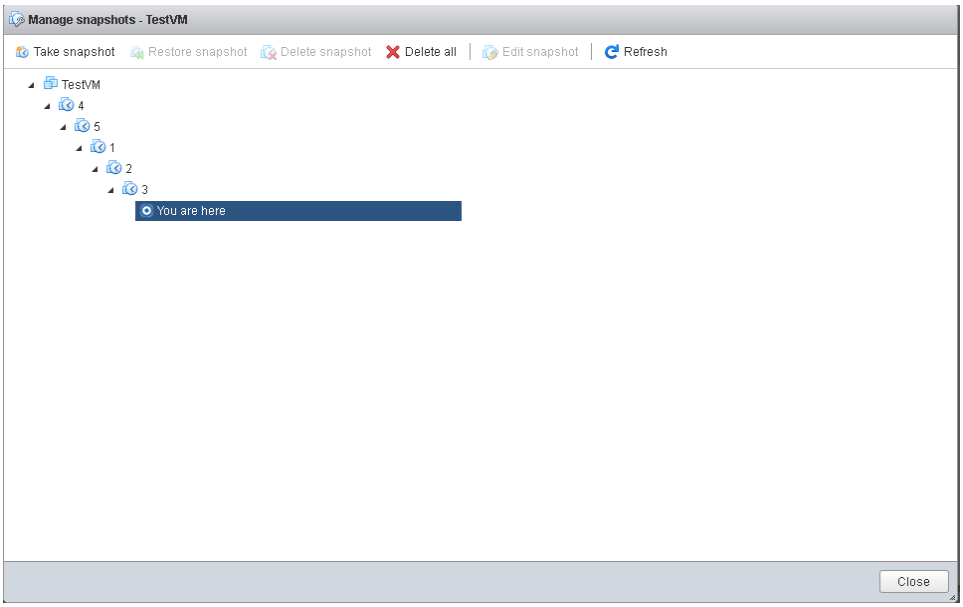

Figure 2-3 Create a Scheduled Snapshot in the VM

9. The preparation work is over here.

INFORMATION

For more detailed information on configuring remote replication, please refer to section 7.2, Configure Protection Groups in the XEVO Software Manual.

2.2.2. SANOS Configuration

Prepare two XCubeSAN storage systems named SAN-a and SAN-b. The following is the procedure.

1. Connect one of 10G ports from SAN-a to SAN-b.
2. In SAN-a, create a pool and a volume. And then set the snapshot space to make the snapshot replica function work normally.
3. In SAN-a, mount the created volume to the prepared ESXi server.
4. Create a VM (Virtual Machine) based on the mounted Datastore in the ESXi server.
5. In SAN-b, repeat steps 2 above to create the same volume size or larger as SAN-a. You may also need to set up snapshot space.
6. In SAN-a, select the **Remote Replication** function submenu to create a remote replication task to the replica volume in SAN-b.

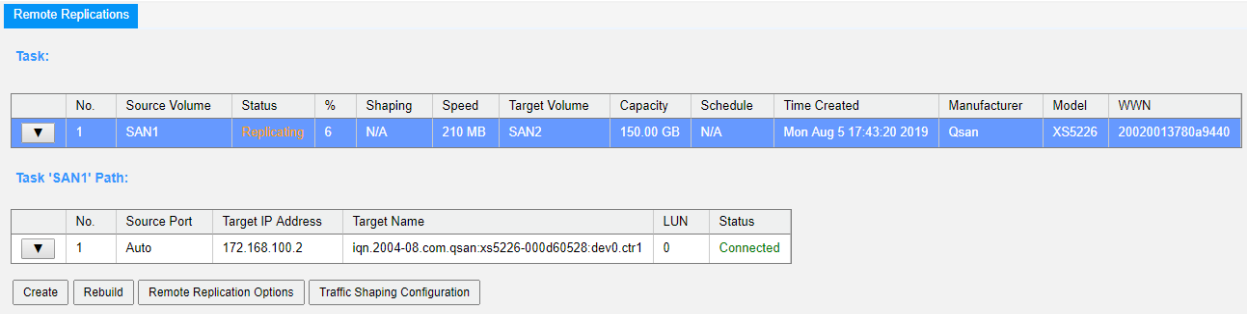

Figure 2-4 Configure a Replication Task

7. Open the console of the VM in the ESXi server, and periodically put some files (such as robocopy utility) to continuously increase the data.

INFORMATION

Robocopy, for "Robust File Copy", is a command-line directory and/or file replication command for Microsoft Windows. Please see Robocopy in Wikipedia.

---

8. Create scheduled snapshots in this VM from the vCenter UI, in this example, we take 5 snapshots.

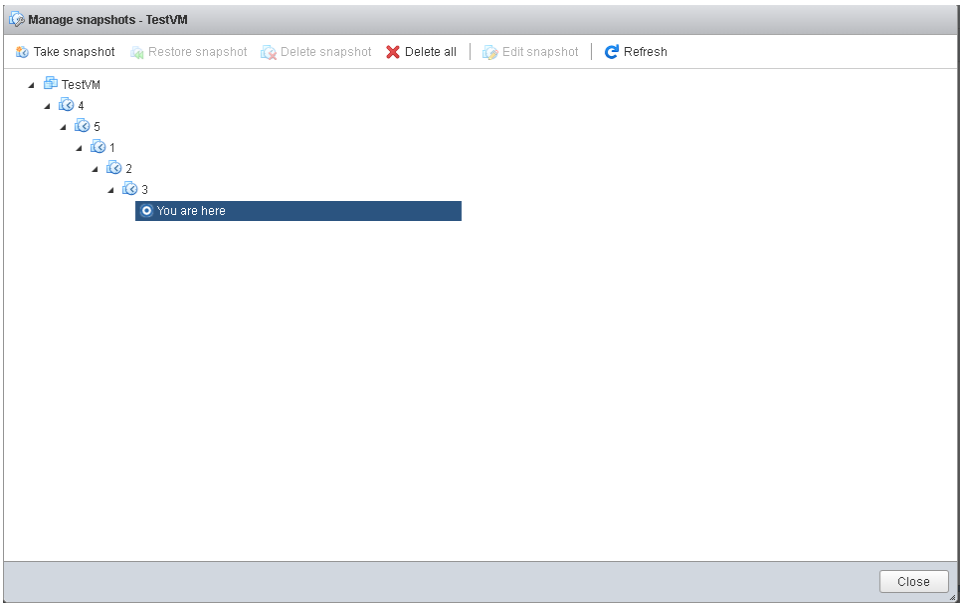

Figure 2-5 Create a Scheduled Snapshot in the VM

9. The preparation work is over here.

INFORMATION

For more detailed information on configuring remote replication, please refer to section 12.3, Managing Remote Replications in the SANOS Software Manual.

2.2.3. QSM Configuration

Prepare two XCubeNXT or XCubeNAS storage systems named NAS-a and NAS-b. The following is the procedure.

1. Connect one of 10G ports from NAS-a to NAS-b.
2. In NAS-a, create a volume and a shared folder.
3. Access NFS shared folders to assign RW permissions to all connected hosts.

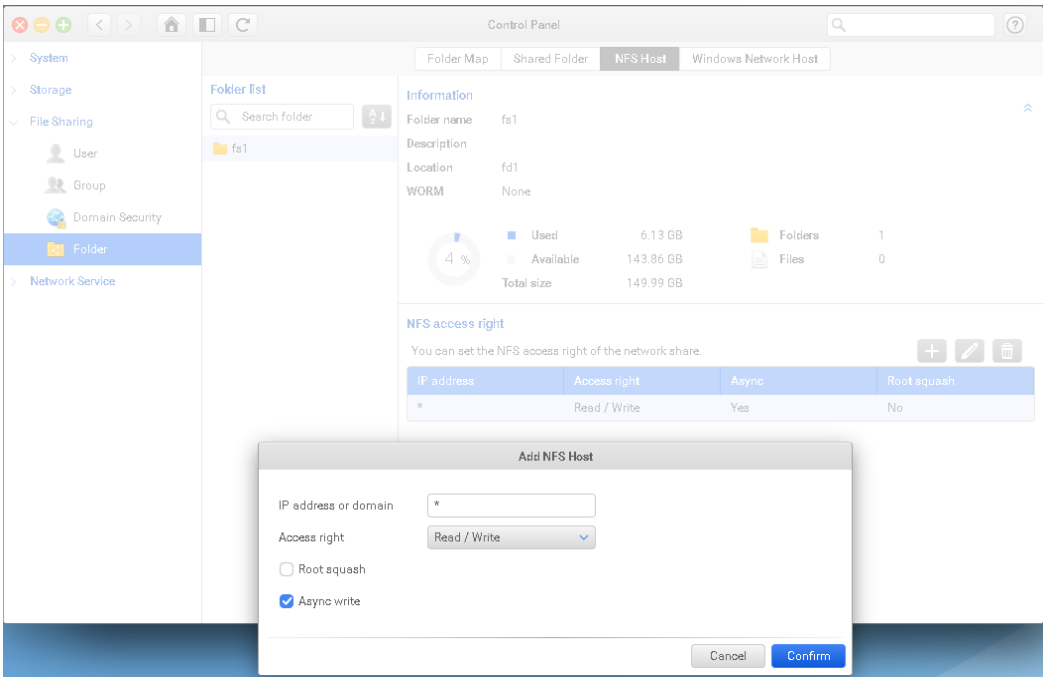

Figure 2-6 Access NFS shared folders

4. In NAS-b, create a volume the same size or larger as the volume in NAS-a.
5. In NAS-a, mount the created shared folder to the prepared ESXi server.
6. Create a VM (Virtual Machine) based on the mounted Datastore in the ESXi server.
7. In NAS-a, select the **Backup Manager** function submenu to create a snapshot reaplica task to the volume in NAS-b.
8. Open the console of the VM in the ESXi server, and periodically put some files (such as robocopy utility) to continuously increase the data.

INFORMATION

Robocopy, for "Robust File Copy", is a command-line directory and/or file replication command for Microsoft Windows. Please see Robocopy in Wikipedia.

---

9. Create scheduled snapshots in this VM from the vCenter UI, in this example, we take 5 snapshots

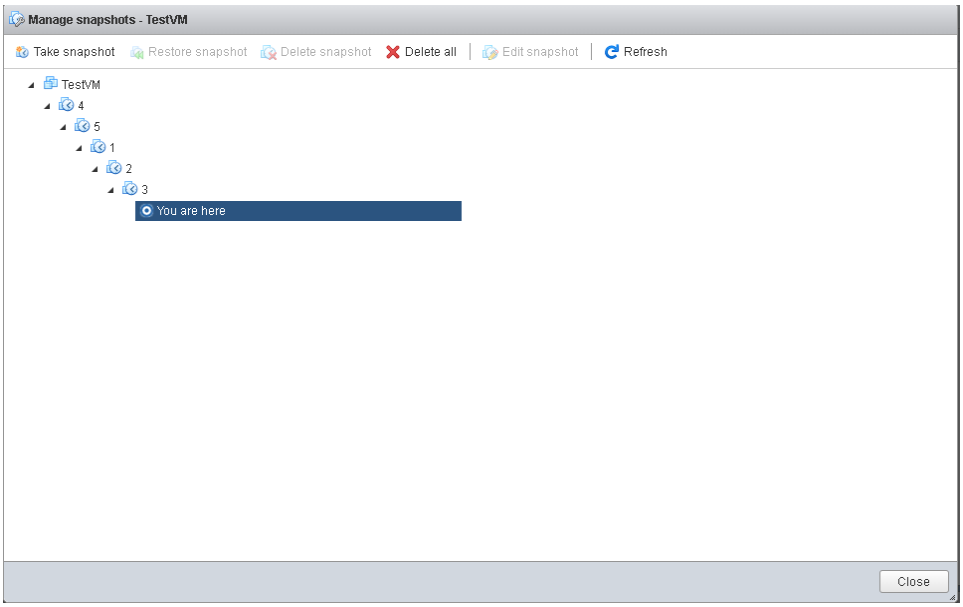

Figure 2-7 Create a Scheduled Snapshot in the VM

10. The preparation work is over here.

INFORMATION

For more detailed information on configuring remote replication, please refer to section 4.2, Remote Backup in the QSM Software Manual.

2.3. Create a Script in ESXi server

According to the above operations, we first take a snapshot in the VM from the ESXi server itself, and then replicate the .VMDK file along with the taken snapshots to the remote site. After mounting the volume at the remote site, registering and rolling back the snapshot taken, everything will be consistent with this method.

However, VMware does not automatically delete or rotate snapshots, so it retains a large number of snapshot images, which can cause poor performance for a long time. The script we provide here is to specify a fixed quantity of snapshots. ESXi servers can maintain rotation to

prevent too many snapshots from affecting virtual machine performance. Take SAN-a as an example below. FAS and NAS are the same.

1. Create a “Crontabs” folder in the Datastore mounted from SAN-a.
2. Upload the following script “SnapshotAutoDelete.sh” to the “Crontabs” folder.

```
# cat SnapshotAutoDelete.sh

#!/bin/sh

LOG_PATH="/var/log/Schedule_Snapshot.log"
[ -f "$LOG_PATH" ] && rm $LOG_PATH;

QTY=2 # Reserved quantity
for i in `vim-cmd vmsvc/getallvms 2>/dev/null | awk '{print $1}' | grep -e "[0-9]"`
# Grab all Vmid on esxi
do
    SNAPSHOT_COUNT=`vim-cmd vmsvc/snapshot.get $i | egrep -- '--\|-CHILD|^\|-ROOT'
| wc -l`
    GuestName=$(vim-cmd vmsvc/get.summary $i | grep name | awk '{ print $3 }' | cut
-d \" -f 2)
    if [ $SNAPSHOT_COUNT -gt $QTY ]; then  # If the number of snapshots is greater
than the number of reservations
        DELETE_COUNT=$(($SNAPSHOT_COUNT-$QTY))
        OLD_SNAPSHOT_ID=`vim-cmd vmsvc/snapshot.get $i | grep Id | head -
$DELETE_COUNT | awk -F: '{print $2}'`
        for n in $OLD_SNAPSHOT_ID
        do
            vim-cmd vmsvc/snapshot.remove $i $n; ret=$?
                sleep 30s
                    if [ $ret -eq 0 ];then
                        echo "$(date "+%F %T") : $GuestName snapshot $n Delete
Success.." >> $LOG_PATH # Output to log path after deletion
                    else
                        echo "$(date "+%F %T") : $GuestName snapshot $n Delete
FAILED.." >> $LOG_PATH
                    fi
        done
    else
        echo "$(date "+%F %T") : $GuestName snapshot not found." >> $LOG_PATH
    fi
done
```

3. Change the permission of the script to 777, from the SSH session of ESXi server.

```
[root@local:~] cd vmfs/volumes/SAN1/Crontabs/
[root@local:/vmfs/volumes/5d445d0a-fae8654e-a676-001b21d4d680/Crontabs] chmod 777 SnapshotAutoDelete.sh
[root@local:/vmfs/volumes/5d445d0a-fae8654e-a676-001b21d4d680/Crontabs] ls -al
total 1152
drwxr-xr-x    1 root     root        73728 Aug  2 16:38 .
drwxr-xr-t    1 root     root        73728 Aug  2 16:38 ..
-rwxrwxrwx    1 root     root         1088 Aug  2 18:52 SnapshotAutoDelete.sh
[root@local:/vmfs/volumes/5d445d0a-fae8654e-a676-001b21d4d680/Crontabs]
```

4. Locate the Datastore via the following command in the SSH session.

```
# esxcli storage filesystem list
```

```
[root@local:~] esxcli storage filesystem list
Mount Point                                  Volume Name  UUID                                 Mounted  Type      Size          Free
-------------------------------------------  -----------  -----------------------------------  -------  ------  ------------  ------------
/vmfs/volumes/5bc3fd0f-f996289d-ba94-001018edee60  datastore1   5bc3fd0f-f996289d-ba94-001018edee60    true  VMFS-6  492042190848  442177159168
/vmfs/volumes/5d445d0a-fae8654e-a676-001b21d4d680  SAN1         5d445d0a-fae8654e-a676-001b21d4d680    true  VMFS-6  160792838144  88226136064
/vmfs/volumes/5ceb8d20-96976e3b-25ef-08606e151c65                5ceb8d20-96976e3b-25ef-08606e151c65    true  vfat       299712512     80486400
/vmfs/volumes/9bfaa77a-a157614d-7923-8cc7a16bcdea                9bfaa77a-a157614d-7923-8cc7a16bcdea    true  vfat       261853184    261844992
/vmfs/volumes/3d40c777-b5b2f4fb-b003-5dfeca8c4b86                3d40c777-b5b2f4fb-b003-5dfeca8c4b86    true  vfat       261853184    113819648
/vmfs/volumes/5ceb8d28-4a26e650-7a8a-08606e151c65                5ceb8d28-4a26e650-7a8a-08606e151c65    true  vfat      4293591040   4264230912
[root@local:~]
```

5. Use the following command to add a cron job to execute the script at 23:30 every day. You can specify the time point according to your environment. This point in time should be earlier than the periodic snapshot task created by vCenter. Or you can edit this file directly.

```
# echo "30    23    *    *    *    sh /vmfs/volumes/5d445d0a-fae8654e-a676-
00lb2ld4d680/Crontabs/SnapshotAutoDelete.sh" >> /var/spool/cron/crontabs/root
```

INFORMATION

The YELLOW' word above is the UUID of the Datastore, please check yours with the above command.

---

6. Since the configuration will be cleared after the ESXi server restarts, you need to add the above commands to permanently save the configuration. Edit the local cron job file (/etc/rc.local.d/local.sh) of the ESXi server and add the following commands at the end of the configuration file.

```
# vi /etc/rc.local.d/local.sh

...
/bin/echo "30    23    *    *    *    sh /vmfs/volumes/5d445d0a-fae8654e-a676-
00lb2ld4d680/Crontabs/SnapshotAutoDelete.sh" >>/var/spool/cron/crontabs/root
/bin/kill $(cat /var/run/crond.pid)
/usr/lib/vmware/busybox/bin/busybox crond
```

7. Check the quantity of retained snapshots from the ESXi UI and confirm that the snapshots have been retained as the latest two.

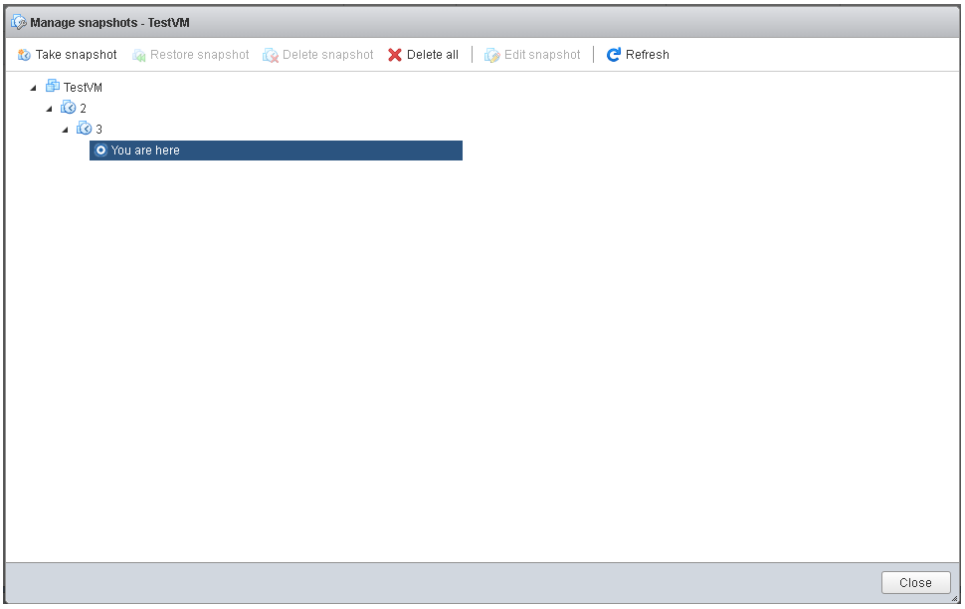

Figure 2-8 List the Snapshots in the VM

8. Use the following command to check the log.

```
# cat /var/log/Schedule_Snapshot.log
```

```
[root@local:~] cat /var/log/Schedule_Snapshot.log
2019-08-05 11:30:38 : 2012R2-SAN1 snapshot 1 Delete Success..
2019-08-05 11:31:12 : 2012R2-SAN1 snapshot 2 Delete Success..
2019-08-05 11:32:10 : 2012R2-SAN1 snapshot 3 Delete Success..
[root@local:~]
```

9. The ESXi server configuration is complete.

2.4. Disaster Drill

We provide disaster drills to prove the effectiveness of backups. Similarly, the setting method is different; the following sections describe the configuration separately.

2.4.1. XEVO Configuration

Continue the previous section, two XCubeFAS storage systems named FAS-a and FAS-b. The following is the procedure.

1. In FAS-a, select the **Protection** tab to find the remote replication task.

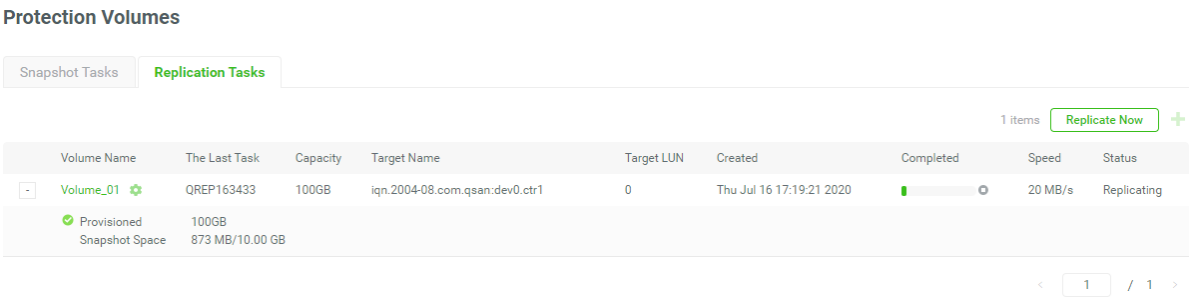

Figure 2-9 Remote Replication Task

2. You may need to umount the original Datastore (of FAS-a) from the ESXi server to simulate a disaster on FAN-a.
3. In FAS-b, select the **Protection** tab to expose the replicated snapshot as a writable volume, and its exposed snapshot capacity is greater than 0 (GB) by default. This is called the writable snapshot function.

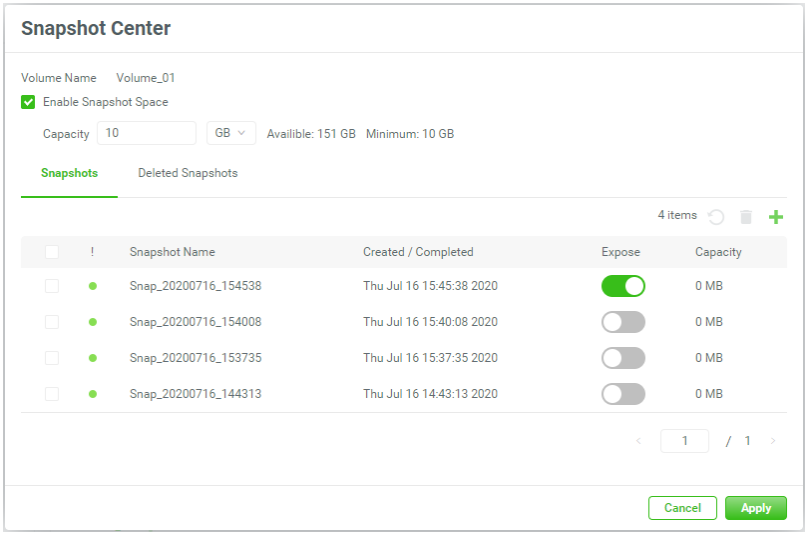

Figure 2-10 Expose the Snapshot

4. Map the volume as a LUN with read-write permission, and the access the vCenter UI (of the ESXi server) to mount the exposed snapshot volume to be a Datastore.
5. During the process of mounting the Datastore, the ESXi system will ask you to assign a New Signature or use an Existing signature. Please choose to use an Existing signature.
6. Right click on the Datastore, you will be able to see the VM replicated from FAS-a, then you can register this VM and try to boot up after the snapshot on the VM is rolled back.

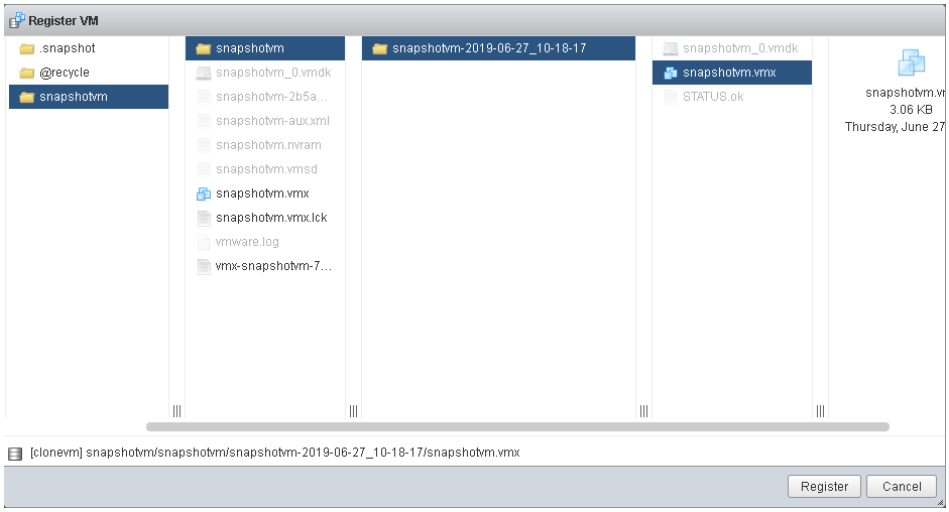

Figure 2-11 Snapshot is rolled back

TIP

It is necessary to roll back the snapshot of the VM because the .VMDK file may be inconsistent due to the data cached by the ESXi server. Please roll back the last snapshot before powering on the VM to ensure that the VM can be successfully booted up.

---

7. Done.

2.4.2. SANOS Configuration

Continue the previous section, two XCubeSAN storage systems named SAN-a and SAN-b. The following is the procedure.

1. In SAN-a, select the **Remote Replication** function submenu to find the remote replication task.

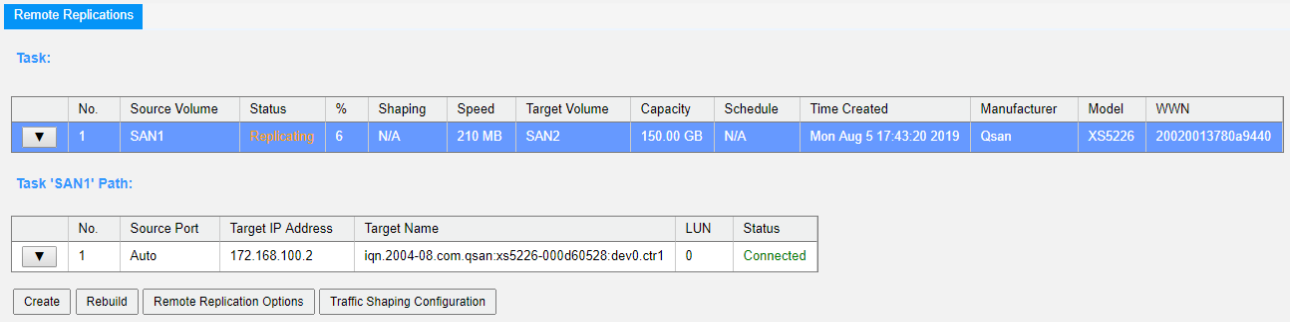

Figure 2-12 Remote Replication Task

2. You may need to umount the original Datastore (of SAN-a) from the ESXi server to simulate a disaster on SAN-a.
3. In SAN-b, select the **Remote Replication** function submenu to expose the replicated snapshot as a writable volume, and its exposed snapshot capacity is set to be greater than 0 (GB). This is called the writable snapshot function.

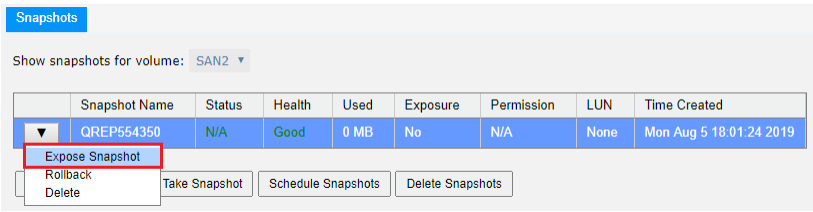

Figure 2-13 Expose the Snapshot

4. Map the volume as a LUN with read-write permission, and the access the vCenter UI (of the ESXi server) to mount the exposed snapshot volume to be a Datastore.
5. During the process of mounting the Datastore, the ESXi system will ask you to assign a New Signature or use an Existing signature. Please choose to use an Existing signature.
6. Right click on the Datastore, you will be able to see the VM replicated from FAS-a, then you can register this VM and try to boot up after the snapshot on the VM is rolled back.

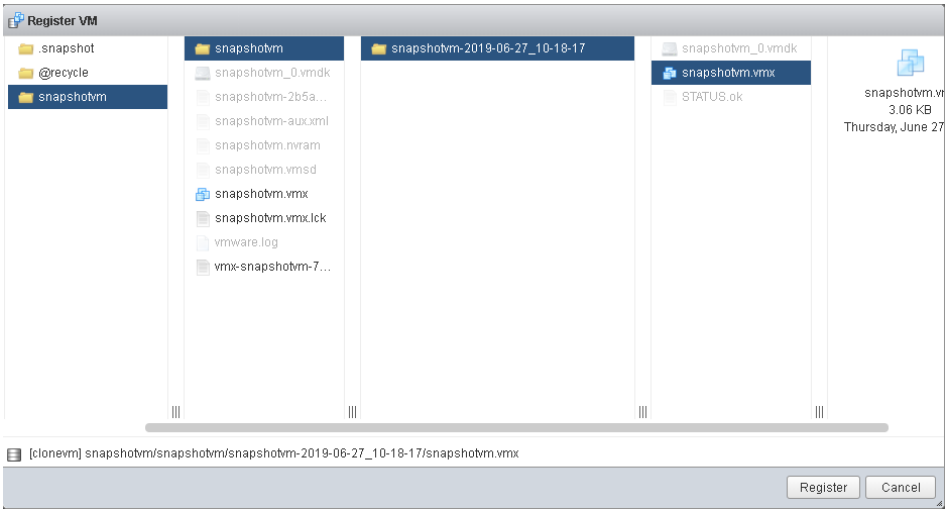

Figure 2-14 Snapshot is rolled back

TIP

It is necessary to roll back the snapshot of the VM because the .VMDK file may be inconsistent due to the data cached by the ESXi server. Please roll back the last snapshot before powering on the VM to ensure that the VM can be successfully booted up.

7. Done.

2.4.3. QSM Configuration

Continue the previous section, two XCubeNXT or XCubeNAS storage systems named NAS-a and NAS-b. The following is the procedure.

1. In NAS-a, select the **Backup Manager** function submenu to find the created snapshot replica task.

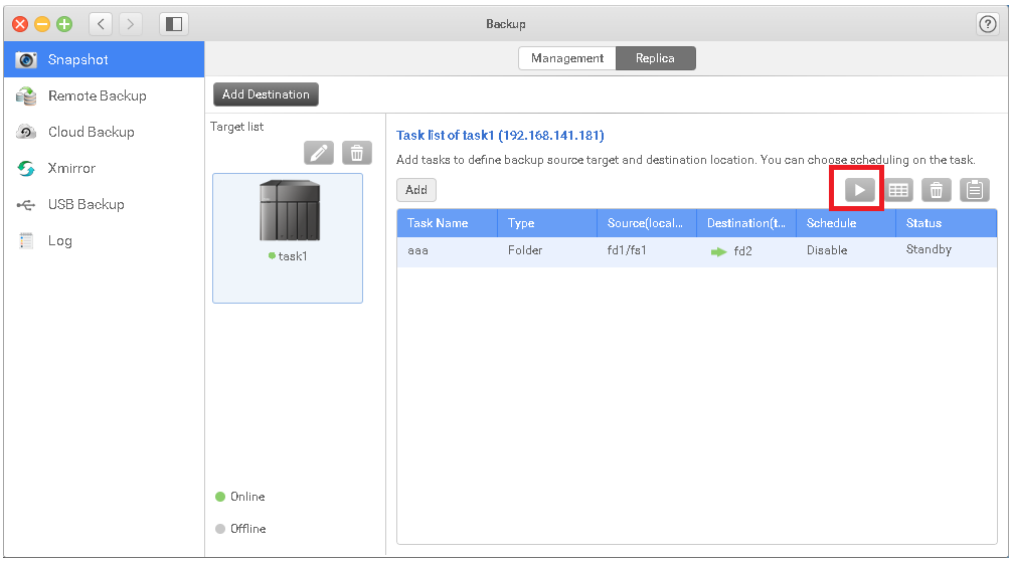

Figure 2-15 Replica Task

2. In NAS-b, select the **Backup Manager** function submenu, and clone the replicated snapshot into the volume.

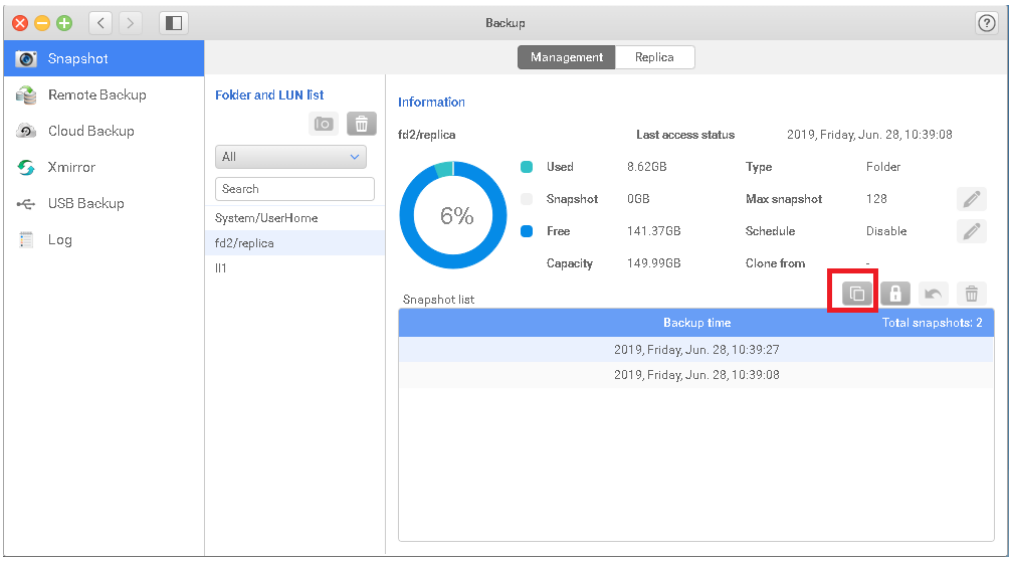

Figure 2-16 Clone the Replicated Snapshot

3. After the clone is completed, change the permission from RO to RW in shared folder page.

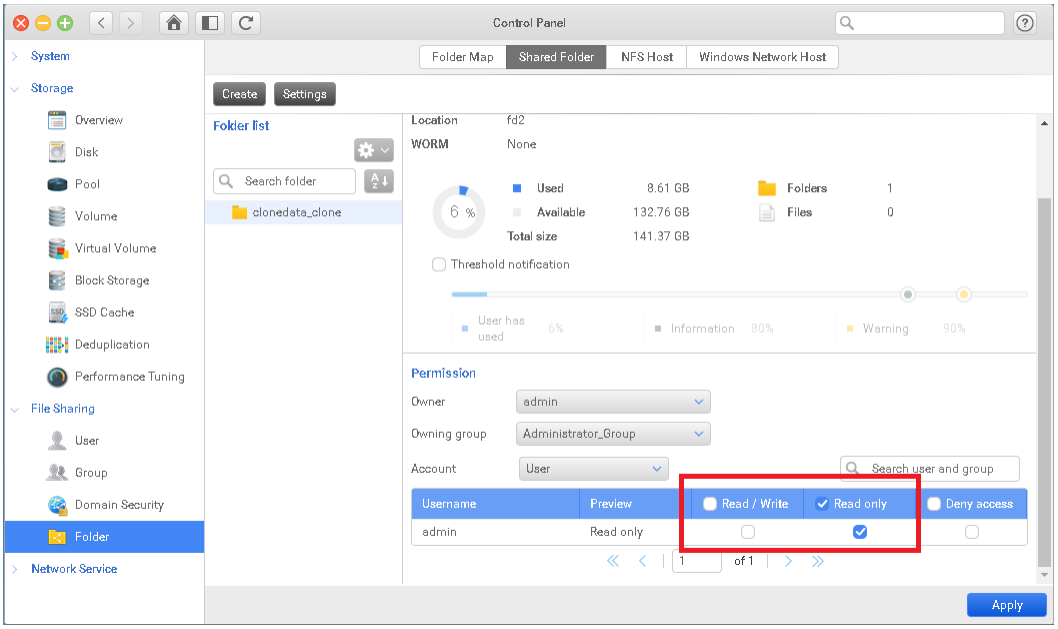

Figure 2-17 Change the shared folder

4. Assign the folder with RW permission to the NFS protocol, just like we did in NAS-a.

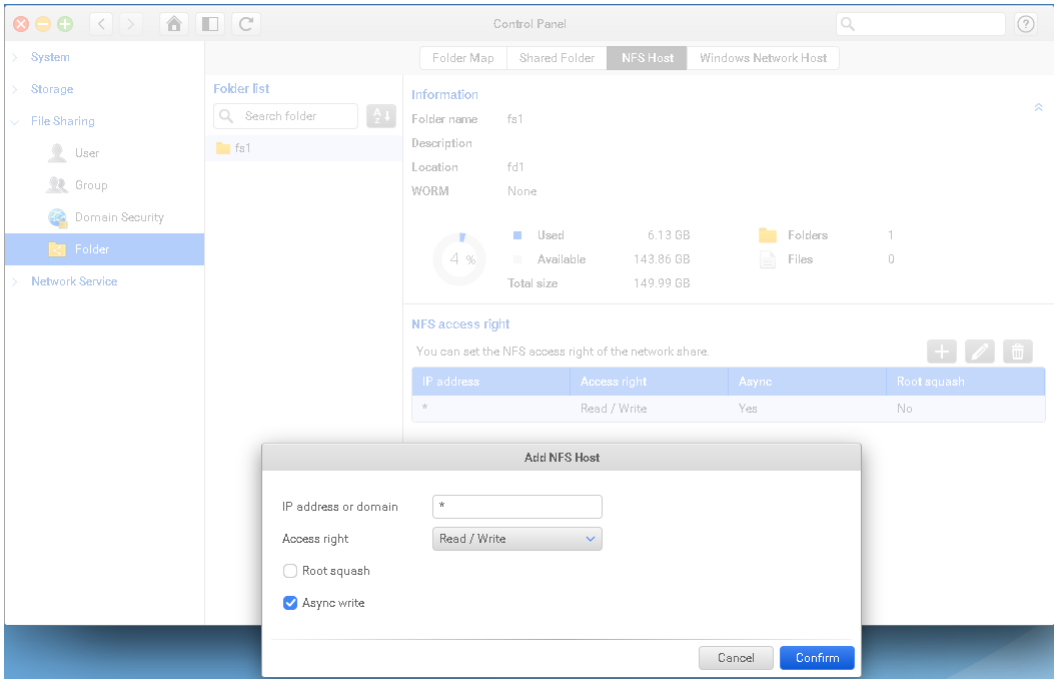

Figure 2-18 Assign the NFS folder

5. In NAS-b, go to ESXi server, mount the NFS shared folder as a Datastore..

6. Right click on the Datastore, you will be able to see the VM replicated from NAS-a, then you can register this VM and try to boot up after the snapshot on the VM is rolled back.

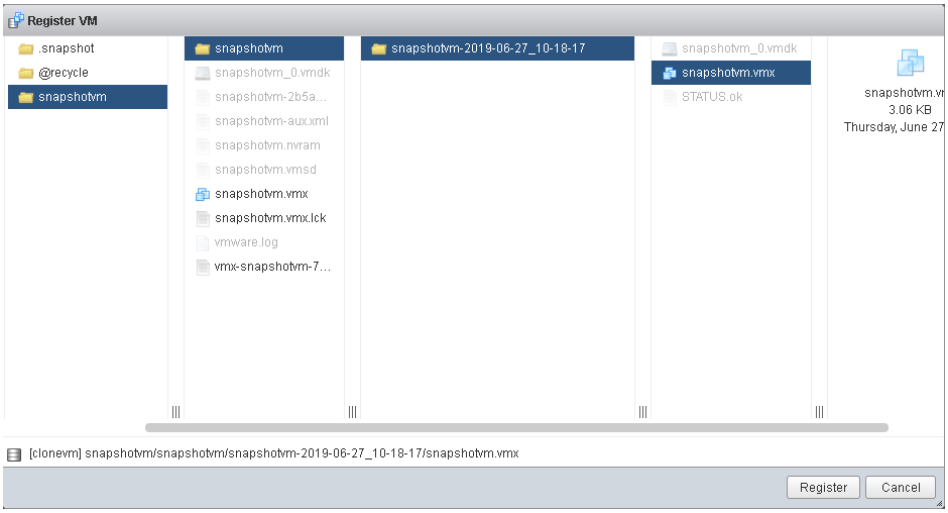

Figure 2-19 Snapshot is rolled back

TIP

It is necessary to roll back the snapshot of the VM because the .VMDK file may be inconsistent due to the data cached by the ESXi server. Please roll back the last snapshot before powering on the VM to ensure that the VM can be successfully booted up.

---

7. Done.

3. CONCLUSION

This document discusses continuous backup solutions and disaster drills in a VMware environment. Configuring a data protection solution helps prevent unexpected situations. In addition, this is a cost-effective method and does not require any agent to be installed in the environment. The solution we provide can be easily implemented with the simple script and snapshot copies stored in QSAN storage.

4. APPENDIX

4.1. Apply To

- XEVO firmware 2.0.0 and later
- SANOS firmware 2.0.0 and later
- QSM firmware 3.3.0 and later

4.2. Reference

Software Manuals

- XEVO Software Manual
- SANOS Software Manual
- QSM Software Manual

White Paper

- QReplica 3.0 White Paper