



PS Series Best Practices

Deploying CommVault® Galaxy™ 6.1.0 ProxyHost iDataAgent using PS Series Groups with Auto-Snapshot Manager 2.0

Abstract

This Technical Report describes how to configure the ProxyHost iDataAgent to support Transportable hardware-based VSS snapshots while backing up NTFS volumes using CommVault Galaxy 6.1.0 with PS Series group storage and the EqualLogic Auto-Snapshot Manager V2.0 for Windows VSS hardware provider.

Copyright © 2006 EqualLogic, Inc.

April 2006

EqualLogic is a registered trademark of EqualLogic, Inc.

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

Possession, use, or copying of the documentation or the software described in this publication is authorized only under the license agreement specified herein.

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

PS Series Firmware Version 2.3.5 or later.

Table of Contents

| | |
|--|----|
| Technical Report and Software Revision Information..... | iv |
| Introduction..... | 1 |
| VSS Hardware Provider Process..... | 1 |
| Deploying ProxyHost and Auto-Snapshot Manager..... | 3 |
| PS Series Groups within CommVault Environments | 3 |
| Production Host Requirements | 3 |
| Backup Host Requirements..... | 4 |
| ProxyHost – Auto-Snapshot Manager Configuration Steps | 5 |
| Production Host..... | 6 |
| Backup Host..... | 11 |
| Create a New ProxyHost Subclient..... | 13 |
| Create a ProxyHost VSS Transportable Shadow Copy | 17 |
| Summary | 17 |
| Appendix: CommVault Recommendations: Transportable Shadow Considerations | 18 |
| Registry Key Attributes | 18 |

Technical Report and Software Revision Information

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

| Technical Report Revision | Date | Change |
|----------------------------------|-------------|------------------|
| 1.0 | 03/20/2006 | Initial release. |

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

| Vendor | Model | Software Revision |
|---------------|---|--|
| CommVault | CommVault Galaxy iDataAgent™ for Quick Recovery | Release 6.1.0 |
| CommVault | CommVault Galaxy iDataAgent™ for ProxyHost | Release 6.1.0 |
| CommVault | CommVault Galaxy iDataAgent™ for File System | Release 6.1.0 |
| CommVault | CommVault Galaxy Quick Recovery Enabler for VSS | Release 6.1.0 |
| CommVault | CommVault QiNetix – Service Pack 1 | 6.1.0B50_SP1 (02/2006) |
| Microsoft® | Windows Server™ 2003 Enterprise Edition | 2003 SP1 |
| Microsoft® | Windows Server™ 2003 Enterprise Edition R2 | |
| Microsoft | iSCSI Software Initiator | Version 2.01 |
| QLogic™ | QLA4010 iSCSI HBA | BIOS: 1.11 Firmware: 03.00.00.04 Rom Loader: 2.0.0.0 |
| QLogic | ESX 3.0 Service Console (Linux Redhat) Driver | 3.10 |
| QLogic | SANsurfer Manager | 4.01.00 |
| QLogic | SCSIport Miniport Driver | 2.1.0.3 |
| QLogic | STORport Miniport Driver* | 2.1.0.8 |

Introduction

The EqualLogic Auto-Snapshot Manager (also denoted as the VSS hardware provider within this document) enables the CommVault Galaxy ProxyHost iDataAgent to request the creation and backup of volume shadow copies without imposing a load on the production server. This is accomplished through the volume shadow copy *transportable* attribute. This feature permits a backup application installed on a system independent of the shadow copy source to mount, or import the shadow and perform backup operations of this NTFS file system.

The CommVault ProxyHost iDataAgent works in harmony with the Auto-Snapshot Manager installed on the production and backup servers to request new shadows. The iDataAgent, in conjunction with the VSS hardware provider, automatically connects to these shadow volumes creating imports on the backup host to backup the imported volumes, and then completes the process by deleting the shadow volumes. This feature greatly reduces the overhead and LAN bandwidth consumed when performing remote backups of local shadow volumes on the production host.

When enabling VSS functionality for use with the CommVault QiNetix iDataAgents, the system will use the default Microsoft software provider to create the shadow copies. However when a hardware provider has been installed such as the EqualLogic Auto-Snapshot Manager, this will become the default provider for storage on the SAN. The Microsoft Software Shadow Copy provider then uses the VSS hardware provider to create non-transportable hardware-based shadow copies. The VSS hardware provider will have a higher precedence than the Microsoft Software Shadow Copy provider and so QR Volume creation with the Shadow Copy Provider will fail.

There is another VSS factor to consider when deployed with the CommVault QiNetix iDataAgents. If there are multiple hardware providers residing on the same production and backup servers, note that not all hardware providers will support the same volumes. For example, the EqualLogic provider will only support disks on the PS Series Array; the HDS provider will only support HDS disks, etc. VSS determines if it supports the volume to be snapped.

The ProxyHost iDataAgent is the backup and restore vehicle for Windows based NTFS applications/file systems that reside in a system which supports a snapshot engine. Note that both the production and backup server must be running the same operating system. The ProxyHost iDataAgent is installed on the production host only. Detailed configuration instructions are provided in a later section of this report.

VSS Hardware Provider Process

The ProxyHost iDataAgent can be implemented in conjunction with the VSS Enabler to conduct backup operations using a VSS Hardware Provider (PS Series Array and Auto-Snapshot Manager). The ProxyHost iDataAgent uses the volume shadow copy to back up large amounts of data without using production host resources. Figure 1 shows a sample ProxyHost configuration in a VSS Hardware Snapshot Provider environment.

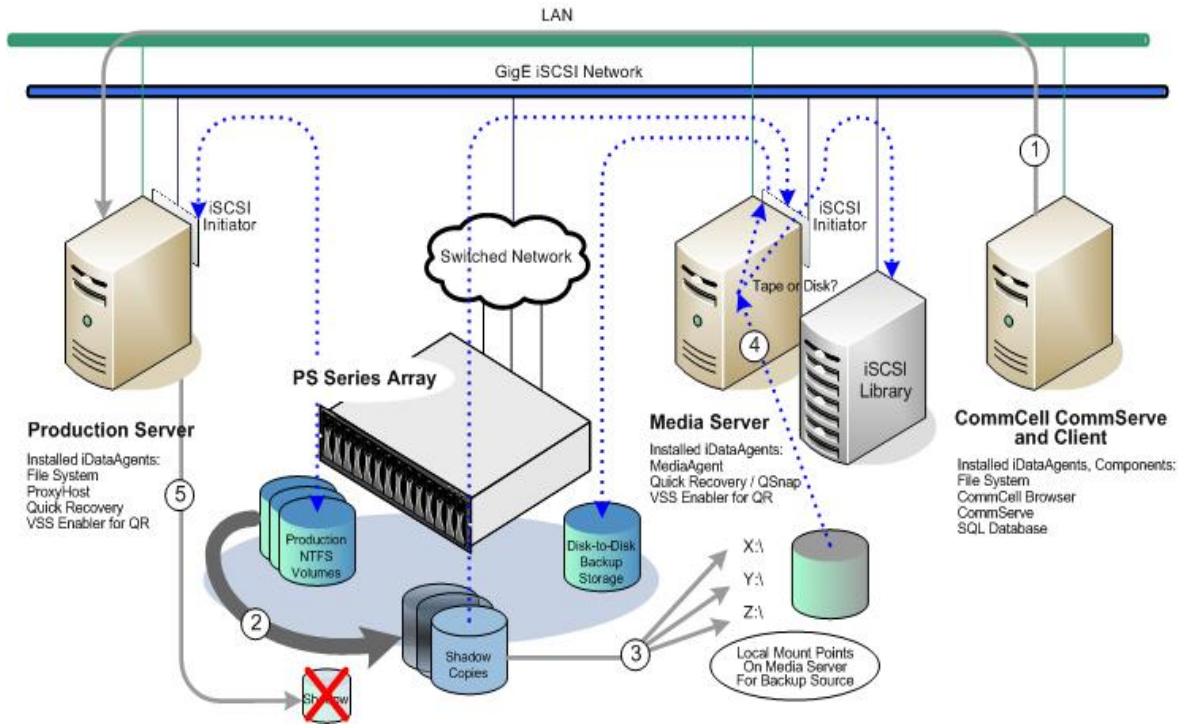


Figure 1: ProxyHost in a VSS Environment.

Snapshots of the data stored on the production host volumes are created by the VSS Hardware Provider; this snapshot is referred to as a *shadow*. The shadow is imported to the Backup Host, and ProxyHost begins the backup. When the backup completes, the shadow is deleted using a post backup script.

The ProxyHost *iDataAgent* is installed on the production host only. The same File System *iDataAgent* is installed on both the production host and the backup host. In addition, the VSS Enabler is installed on the production host and backup host.

During a ProxyHost backup, the following sequence of events takes place:

1. The CommServe controller instructs the ProxyHost *iDataAgent* residing on the production host to initiate a backup operation.
2. The *PreScan* script located on the production host executes the required *vssnapshot* commands that create the transportable shadow copy(s).
3. The transportable shadow copies are then imported onto the backup server, (connected via the local iSCSI initiator), by way of NTFS mount points.
4. The point-in-time shadow copy available via a mount point is then backed up on the backup server with the data being written to either tape or disk storage.
5. When the backup process has completed the *PostBackup* script located on the production host executes the required *vssnapshot* commands to delete the shadow copy(s). Because the backup does not occur on the production host, resources on the production host are not affected by the backup operation.

Deploying ProxyHost and Auto-Snapshot Manager

The CommVault Quick Recovery *iDataAgent* is required when configuring the ProxyHost *iDataAgent* along with the EqualLogic Auto-Snapshot Manager in order to support transportable snapshots of NTFS file systems. Quick Recovery point-in-time snapshots, recovery, and application volume protection are not supported with the Auto-Snapshot Manager and the Quick Recovery *iDataAgent* through a generic enabler at this time. This report covers only the ProxyHost *iDataAgent* deployment and protection of flat file NTFS volumes only.

PS Series Groups within CommVault Environments

For an overview of PS Series Group requirements and Best Practice procedures for deployment within a CommVault Galaxy 6.1.0 environment refer to the Technical Report, *Deploying CommVault Galaxy Backup & Recover Release 6.1.0 and Auto-Snapshot Manager 2.0*, available on the EqualLogic Customer Support website.

Production Host Requirements

The production host is also referred to as the “source” or “primary host path” in reference to the transportable shadow volume direction or location. This server is connected to one or more EqualLogic iSCSI NTFS volumes and will be protected by the backup host. Servers to be used for this purpose must meet the following requirements:

- Microsoft Windows Server 2003 R2 or the Windows Server 2003 family of operating systems with SP1 and hotfix KB891957
 - CommVault Galaxy 6.1.0 ProxyHost *iDataAgent*
 - CommVault Galaxy 6.1.0 VSS Enabler
- Note:** When the Galaxy VSS Enabler is selected during install, the Quick Recovery *iDataAgent*, the QSnap *iDataAgent*, and the Windows Server 2003 File System *iDataAgent* are automatically selected. The QSnap *iDataAgent* can be deselected for this application.
- CommVault Galaxy 6.1.0 File System *iDataAgent*
 - CommVault Galaxy 6.1.0 Quick Recovery *iDataAgent*
 - CommVault QiNetix Galaxy Service Pack 1 updates (02/06 or later)
 - Industry-standard iSCSI initiator, either:
 - Microsoft iSCSI Software Initiator Version 2.01 or later
 - iSCSI host bus adapter (HBA) initiator plus the service portion of the Microsoft iSCSI Software Initiator Version 2.01 or later (for VSS support).

For installation information, consult the initiator vendor documentation.

- Auto-Snapshot Manager for Windows Version 2.0 or later (VSS hardware provider). The Auto-Snapshot Manager for Windows is installed with the EqualLogic Host Integration Tools for Windows 2.0.

For operating system, iSCSI initiator, and other requirements, see the Auto-Snapshot Manager Installation and Administration manual. The production host must be configured to have access to the VSS control volume provided on the PS Series Group in order for the provider to function properly.

Beginning with version 2.0 of the Auto-Snapshot Manager this access is controlled via CHAP. Use the Remote Setup Wizard provided within the Host Integration Tools for Windows 2.0 available on the EqualLogic Customer Support website to configure the backup host to access the SAN.

- Available storage capacity on the PS Series Group for creation of each volume to be used for data storage on the production host.
 - Access control configured for each volume.
 - Persistently connect the backup host to the volume(s).
 - If you want to use multipath I/O, set up redundant paths between servers and storage. See the EqualLogic Technical Report *Using Multipath I/O for Windows* on the EqualLogic Support Site for information.
 - Initialize the volume(s) as basic disk(s).
 - For the best performance, align disk sectors. See the Technical Report, *Aligning Disk Sectors for Optimal Performance*, on the EqualLogic Customer Support website for more information.
 - Format the new disk(s).
- Consult the Network Connection Guidelines Technical Report on the EqualLogic Customer Support website for information about improving network performance between PS Series storage arrays and servers.

Backup Host Requirements

The backup host is also referred to as the “import host” or “destination” in reference to the transportable shadow volume direction or location. When used with the ProxyHost *iDataAgent* the backup host serves as the platform on which the VSS shadow copies taken of the production hosts data volumes are imported, (connected to via the iSCSI initiator), and made available via NTFS mount points. Servers to be used for this purpose must meet the following requirements:

- Microsoft Windows Server 2003 R2 or the Windows Server 2003 family of operating systems with SP1 and hotfix KB891957
- CommVault Galaxy 6.1.0 VSS Enabler

Note: When the Galaxy VSS Enabler is selected during install, the Quick Recovery *iDataAgent*, the QSnap *iDataAgent*, and the Windows Server 2003 File System *iDataAgent* are automatically selected. The QSnap *iDataAgent* can be deselected for this application.
- CommVault Galaxy 6.1.0 File System *iDataAgent*
- CommVault Galaxy 6.1.0 Quick Recovery *iDataAgent*
- CommVault QiNetix Galaxy Service Pack 1 updates (02/06 or later)
- Industry-standard iSCSI initiator, either:
 - Microsoft iSCSI Software Initiator Version 2.01 or later
 - iSCSI host bus adapter (HBA) initiator plus the service portion of the Microsoft iSCSI Software Initiator Version 2.01 or later (for VSS support).

For installation information, consult the initiator vendor documentation.

- Auto-Snapshot Manager for Windows Version 2.0 or later (VSS hardware provider). For operating system, iSCSI initiator, and other requirements, see the Auto-Snapshot Manager Installation and Administration manual. The backup host must be configured to have access to the VSS control volume provided on the PS Series Group in order for the provider to function properly.

Beginning with version 2.0 of the Auto-Snapshot Manager this access is controlled via CHAP. Use the Remote Setup Wizard provided within the Host Integration Tools for Windows 2.0 available on the EqualLogic Customer Support website to configure the backup host to access the SAN.

- Available drive letters for each transportable shadow copy volume to be imported during backups. These drive letters are temporary and defined within the source-destination mapping file located on the production host described in more detail in a later section of this report.

Note: If the backup host will also be used as a MediaAgent, (backup data source), and disk-to-disk backups will be performed then the additional requirements apply:

- CommVault Galaxy 6.1.0 MediaAgent
- CommVault QiNetix Galaxy Service Pack 1 updates (02/06 or later) after the base MediaAgent has been installed on the backup host.
- For each backup volume reserved for disk-to-disk backup media:
 - Available storage capacity on the PS Series Group for creation of each volume.
 - Access control configured for each volume.
 - Persistently connect the backup host to the volume(s).
 - If you want to use multipath I/O, set up redundant paths between servers and storage. See the EqualLogic Technical Report *Using Multipath I/O for Windows* on the EqualLogic Support Site for information.
 - Initialize the volume(s) as basic disk(s).
 - For the best performance, align disk sectors. See the Technical Report, *Aligning Disk Sectors for Optimal Performance*, on the EqualLogic Customer Support website for more information.
 - Format the new disk(s).
 - Configure the backup application to use the new disk for a backup-to-disk device.
- Consult the Network Connection Guidelines Technical Report on the EqualLogic Customer Support website for information about improving network performance between PS Series storage arrays and servers.

ProxyHost – Auto-Snapshot Manager Configuration Steps

The activities involved to configure the proper operation of the ProxyHost *iDataAgent* and the Auto-Snapshot Manager are covered within this section as a list of steps to be completed on production host, the backup host, and within the CommVault CommCell/CommServe Console.

1. If the server that is planned for use as the production host does not contain an iSCSI initiator begin the setup process by obtaining and installing the Microsoft iSCSI initiator or an iSCSI HBA. To prepare this Technical Report the QLogic QLA4010 HBA was used for the initiator function, and the Microsoft iSCSI service was installed to support VSS. Consult the instructions provided by the vendor to install, configure, and operate the iSCSI initiator selected for the production host.
2. If the production host has yet to be connected to a PS Series Group member and volumes have not been created see the PS Series *QuickStart* or *Group Administration* manual for detailed information about setting up PS Series storage array hardware and creating a PS Series group (SAN) with the array as the first group member.
3. You can use the Group Manager GUI or CLI to create production host volumes and access control records that restrict production host access to volumes and backup host access to the volumes snapshots. To start the GUI, enter the group IP address in a Web browser and log in to the default grpadmin account.
4. In the Activities panel, click **Create Volume**. A dialog box will open, as shown in Figure 3. Specify the name for the volume(s) required and the volume size. You must also reserve space for snapshots that will be created for these volumes during backup operations. The Space Utilization table in the dialog box shows the current group space statistics and statistics with the new volume size and snapshot space.
5. Click **Next** to create an access control record that will allow the production host access to the volume. You can specify an IP address, iSCSI initiator name, CHAP user name, or any combination of the three. The production host must match all the requirements in one record in order to access the volume or snapshot.
6. You must also include access to the volume's snapshot by the backup server. This is accomplished by adding a new volume access control record for the backup server and deselecting the volume checkbox so that the backup server has access only to the snapshot. See Figure 2.

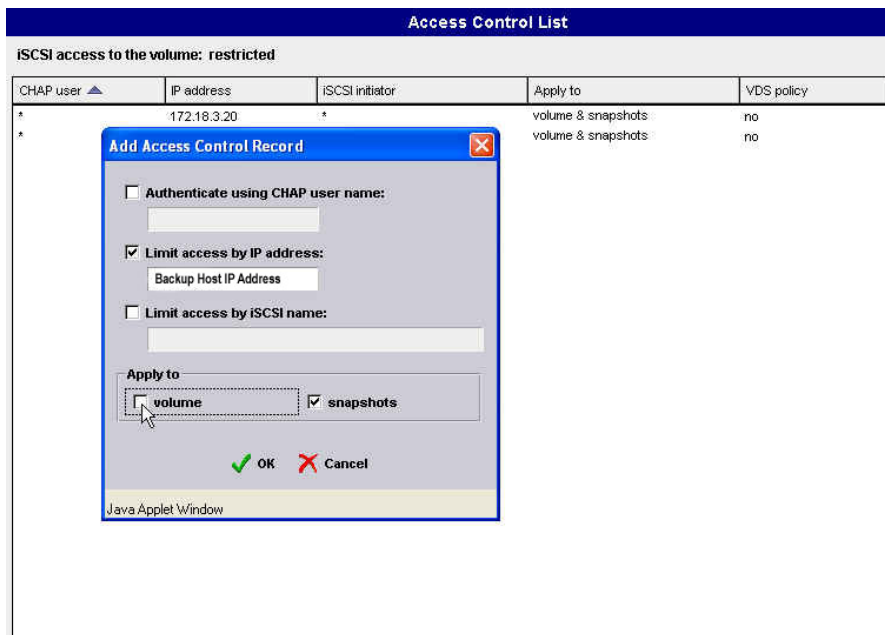
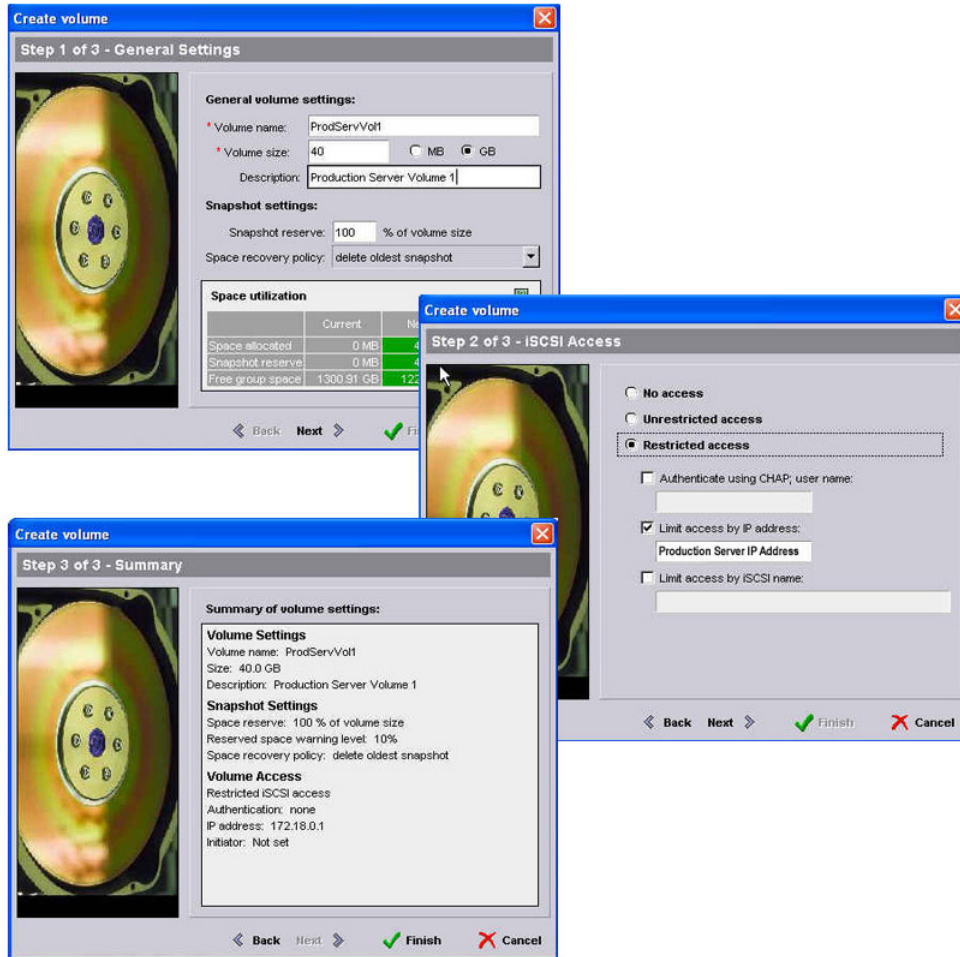


Figure 2: Setting up an Access Control Record.

7. Once the new volumes have been created on production host and backup server access has been setup for existing PS Series Group volumes it is time to install the Auto-Snapshot Manager. This will enable the VSS hardware provider functionality for the production host.
8. Follow the instructions provided within the EqualLogic Auto-Snapshot Manager Installation and Administration Guide. The Host Integration Tools 2.0 for Windows setup utility will be used to install these components. After the installation process has been completed, use the VSS requestor included with the Auto-Snapshot Manager to verify volume shadow copies of the base volumes connected to the production host can be created and imported.
9. The production host volumes have been prepared and the VSS hardware provider is available and functioning properly. Follow the instructions provided within the CommVault QiNetix Galaxy documentation to install the ProxyHost *iDataAgent*, the VSS Enabler, and the Quick Recovery Agent on the production host. When the VSS Enabler is selected the QR Agent, QSnap, and *iDA* for Windows 2003 are all automatically selected. The QSnap option is not necessary for ProxyHost VSS support and can be deselected. Figure 3 shows an example of how the CommVault Installer should look once the ProxyHost installation has been completed.

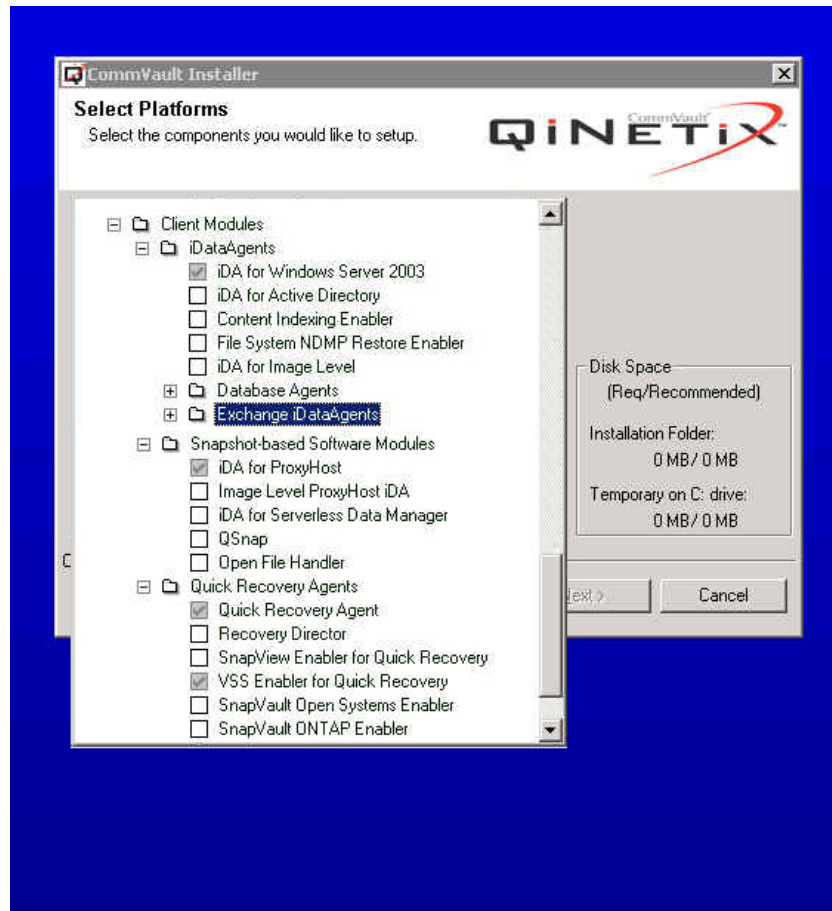


Figure 3: After the ProxyHost is installed.

10. This step involves adding 2 new values to the production host registry. Exercise care when making these changes.

10.1. Locate the QREnabler key in the following registry path:

HKEY_LOCAL_MACHINE\SOFTWARE\CommVault Systems\Galaxy\Platform Information\ControlSet00#(<ProductionServerName>\QREnabler

(Figure 4.) Within the QREnabler Key **add** a new nTRANSPORTABLE DWORD value and set it to 0x1.

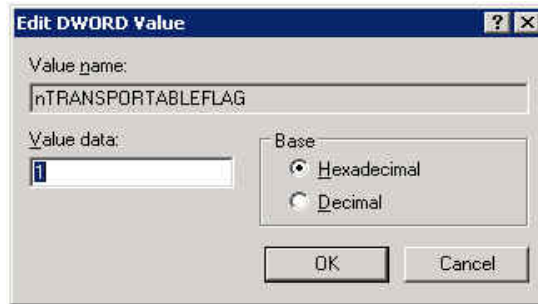


Figure 4: Adding a Registry Key.

10.2. Locate the QREnabler key in the following registry path:

HKEY_LOCAL_MACHINE\SOFTWARE\CommVault Systems\Galaxy\Platform Information\ControlSet00#(<ProductionServerName>\QREnabler

(Figure 5). Within the QREnabler Key add a new SLOCALBCDBASEPATH String value and set it to the path to which the BCD files will be created during the volume shadow copy process. The BCD files are persistent binary files that provide linkage between the shadow copy volumes created on the production host and the import process on the backup host. This directory will be created automatically by ProxyHost.

Note: Please refer to the final section of this report for further description of the CommVault registry keys.

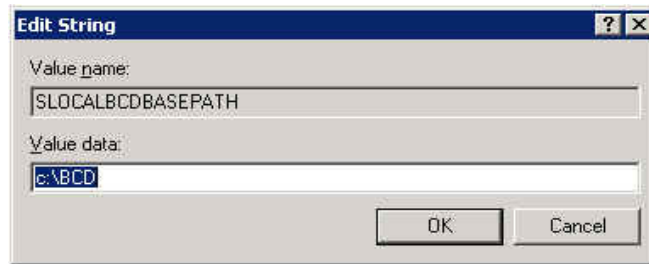


Figure 5: Entering the BCD file path.

11. In order to communicate what production host volumes are to be used for volume shadow copy creation and to what drive letter on the backup host they will be mounted, a snapshot list initialization file is required containing this mapping information. This file is also known as the source-destination mapping file.

The source-destination mapping file can reside on either the production host or the backup host. The production host is also the location for the PreScan and PostBackup scripts so it is recommended that this file also be placed on the production server. This Technical Report uses “c:\commvault_ini\snap.ini” as the filename and path; this information must be specified in the PreScan and PostBackup scripts discussed in the next step. See an example of the source-destination mapping file on the following page.

```
[SNAPVOLUMELIST]
COUNT=N
SRCVOL_N=<mount point>:
DESTVOL_N=<mount point>:
```

Where:

| | |
|--------------------------|---|
| [SNAPVOLUMELIST] | All source-destination .ini files should start with this header. |
| COUNT=N | Where N is the number of production volumes you want to snap. |
| SRCVOL_N=<mount point>: | The source volume mount point, where N equals the number identifying the source/destination pair starting at 0. |
| DESTVOL_N=<mount point>: | The destination mount point, where N equals with a number identifying the source/destination pair starting at 0. (Free drive letter on the backup host). |

For example, suppose you have two production host volumes (F: and G:). You must specify a count of two volumes, and specify a backup host mount point for each source as follows:

```
[SNAPVOLUMELIST]
COUNT=2
SRCVOL_0=E:
DESTVOL_0=Y:
SRCVOL_1=F:
DESTVOL_1=Z:
```

-Drive letters Y: and Z: were chosen because these letters are usually available and are not used by other devices.

- The PreScan and PostBackup scripts are called by the backup application to manage the actual volume shadow copy creation and deletion. The scripts also specify the names and roles of the production and backup hosts. More information on these scripts can be found in the CommVault QiNetix Resource Pack in the following directory:

\Windows\SnapTools\Template Scripts\VSS Hardware Provider

This Technical Report uses “c:\commvault_scripts\” as the path for the PreScan and PostBackup scripts. This location will be used when setting up a Subclient under the ProxyHost iDataAgent. Use the following example as a guide when creating these two scripts.

PreScan.bat: (appeng01 = production host / appeng07 = backup host)

```
"C:\Program Files\CommVault Systems\Galaxy\base\"vsssnapshot.exe multisnap C:\commvault_in\snap.ini -vm
appeng01.appeng.com
"C:\Program Files\CommVault Systems\Galaxy\base\"vsssnapshot.exe vss import -i C:\commvault_in\snap.ini -S
appeng07.appeng.com -vm appeng01.appeng.com
```

Postbackup.bat:

```
"C:\Program Files\CommVault Systems\Galaxy\base\"vsssnapshot.exe unsnap -i C:\commvault_in\snap.ini -S
appeng07.appeng.com -vm appeng01.appeng.com
```

This completes the configuration steps for the production host, proceed to the Backup Host configuration in the next section.

The flexibility of the CommVault QiNetix Galaxy product permits the backup host to be configured as a dedicated server managing only the shadow volume copy import and mount activity, redirecting the backup data to another server acting as the MediaAgent. The backup host role can also be combined with a MediaAgent, or a MediaAgent and a CommServe Console. Choose the best configuration for your data center requirements and use the following guidelines to deploy the backup host ProxyHost *iDataAgent*.

Regardless of the current CommVault configuration required to manage the backup host functionality, there are only four basic steps required to prepare the environment to support the ProxyHost *iDataAgent*:

1. If the server that is planned for use as the backup host does not contain an iSCSI initiator begin the setup process by obtaining and installing the Microsoft iSCSI initiator or an iSCSI HBA. To prepare this Technical Report the QLogic QLA4010 HBA was used for the initiator function, and the Microsoft iSCSI service was installed to support VSS. Consult the instructions provided by the vendor to install, configure, and operate the iSCSI initiator selected for the backup host.
2. Install the VSS hardware provider. Follow the instructions provided within the EqualLogic Auto-Snapshot Manager Installation and Administration Guide. The Host Integration Tools 2.0 for Windows setup utility will be used to install these components. Be sure to select the Remote Setup Wizard at the end of the Host Integration Tools installation in order to add the PS Series Group containing the production host volumes. If this server has existing connections to PS Series volumes use the VSS requestor included with the Auto-Snapshot Manager to verify volume shadow copies of the base volumes connected to the backup host can be created and imported. If this is a backup host function install only, (no local iSCSI base volumes required), create a temporary volume and connect to it for verification of correct VSS functionality. See the production server configuration instructions for details on how to create PS Series volumes if required.
3. Follow the instructions provided within the CommVault QiNetix Galaxy documentation to install the VSS Enabler, and the Quick Recovery Agent on backup host. When the VSS Enabler is selected the QR Agent, QSnap, and *iDA* for Windows 2003 are all automatically selected. The QSnap option is not necessary for ProxyHost VSS support and can be deselected. Figure 6 shows an example of how the CommVault Installer should look once the VSS Enabler installation has been completed.

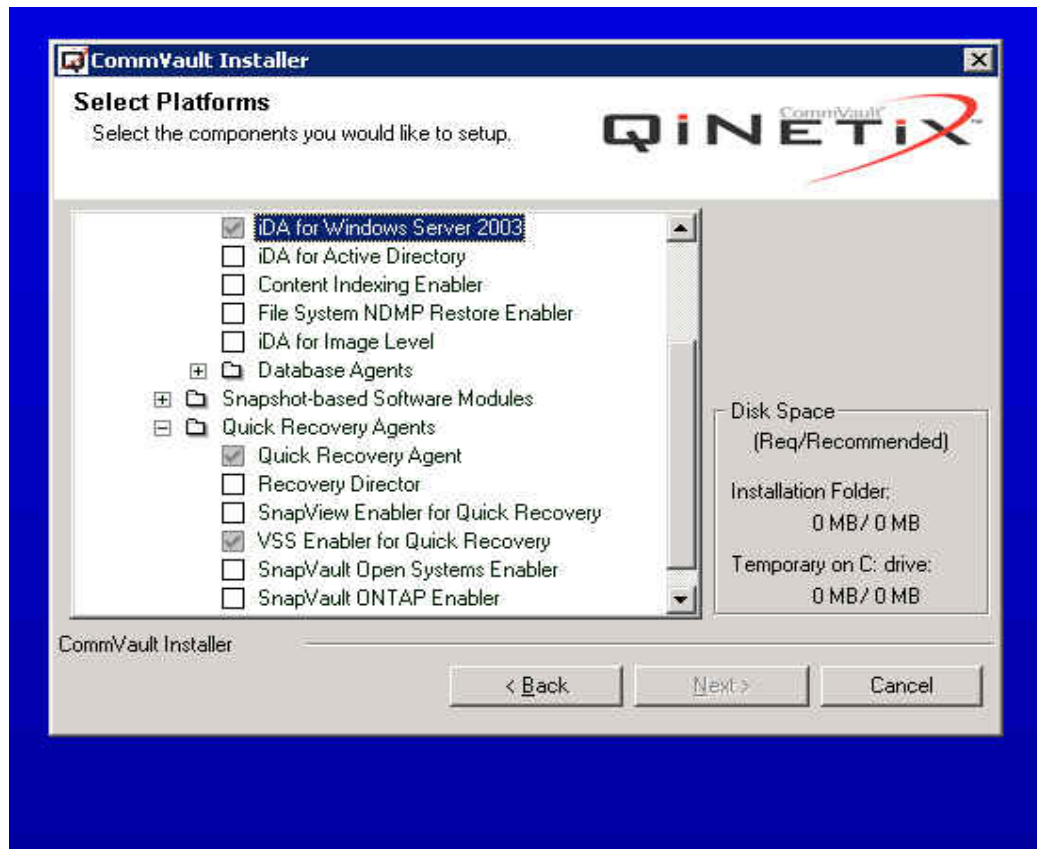


Figure 6: CommVault Installer after VSS Enabler installation.

4. The fourth and final step involved in configuring the backup host is to add a new value to the backup host registry. Exercise care when making this change.
 - a. Locate the QREnabler key in the following registry path:

HKEY_LOCAL_MACHINE\SOFTWARE\CommVault Systems\Galaxy\Platform Information\ControlSet00#(<ProductionServerName>\QREnabler

(Figure 7). Within the QREnabler Key **add** a new nTRANSPORTABLE DWORD value and set it to 0x1.

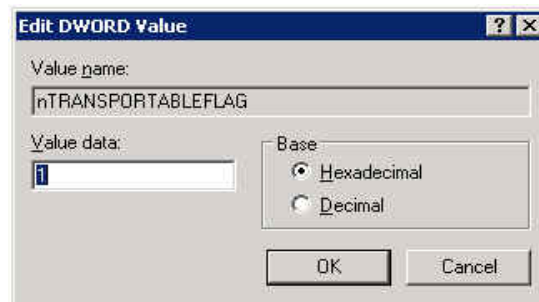


Figure 7: Adding and setting the nTRANSPORTABLE DWORD.

Note: If the backup host role is being added to an existing MediAgent environment and additional disk-to-disk backup storage resources are required, it may be necessary to add additional PS Series Group volumes to the backup host. If this is the case review the steps in

configuring the production server detailing the creation and preparation of PS Series Group volumes.

This completes the configuration steps for the backup host.

Create a New ProxyHost Subclient

After the production and backup hosts have been configured for ProxyHost iDataAgent support the last configuration task involves creating a new Subclient to control the production host backup with volume shadow copy activities.

1. **Do not** create a Subclient while the parent node or any sibling Subclient has a data protection or archive operation currently running on it.
2. Using the CommCell Browser begin the ProxyHost Subclient creation process by selecting the production host from the list of Client Computers. Highlight and right click the ProxyHost iDataAgent, select “New Subclient” from the “All Tasks” option. Choose a new Subclient name within the dialog box as shown in Figure 8.

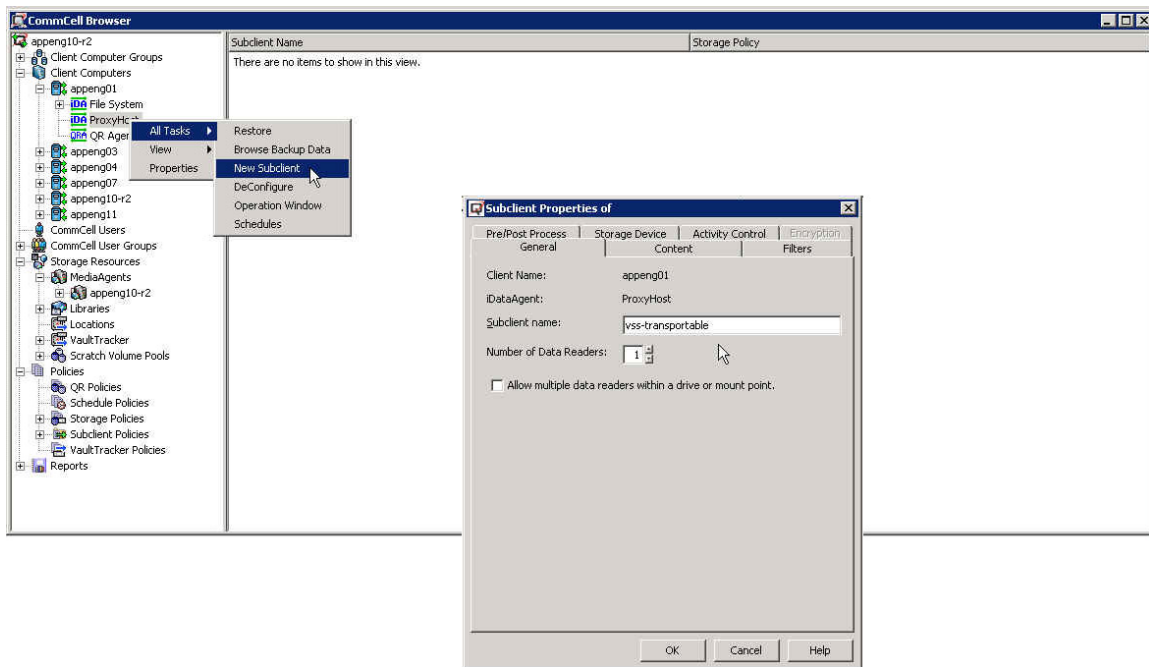


Figure 8: Set a new Subclient name.

3. Select a storage policy for the ProxHost Subclient from the list of previously configured tape or disk-to-disk policies (Figure 9).

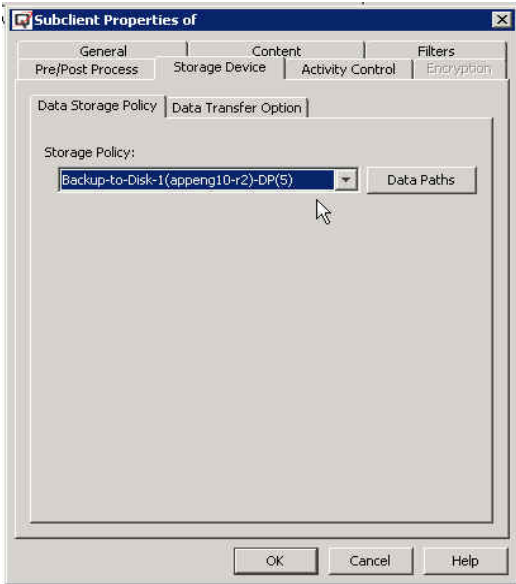


Figure 9: Selecting a storage policy.

4. Select the Content:(volumes) and path of the production host base volume(s) that will be shadowed and backed up by the backup host. The Backup Host BCV¹ Path: can not be located as easily from the Browse option as is the Content: section. This path like the source-destination mapping file described within the production host configuration section references the mount point to be used on the backup server. The same unused drive letters specified in the mapping file can also be used for the root path. See Figure 10 for an example.

¹ (BCV) Business Continuance Volume

A mirror-image of an active production volume; obtained through split-mirror technology, a BCV can be created and used without affecting the production volume.

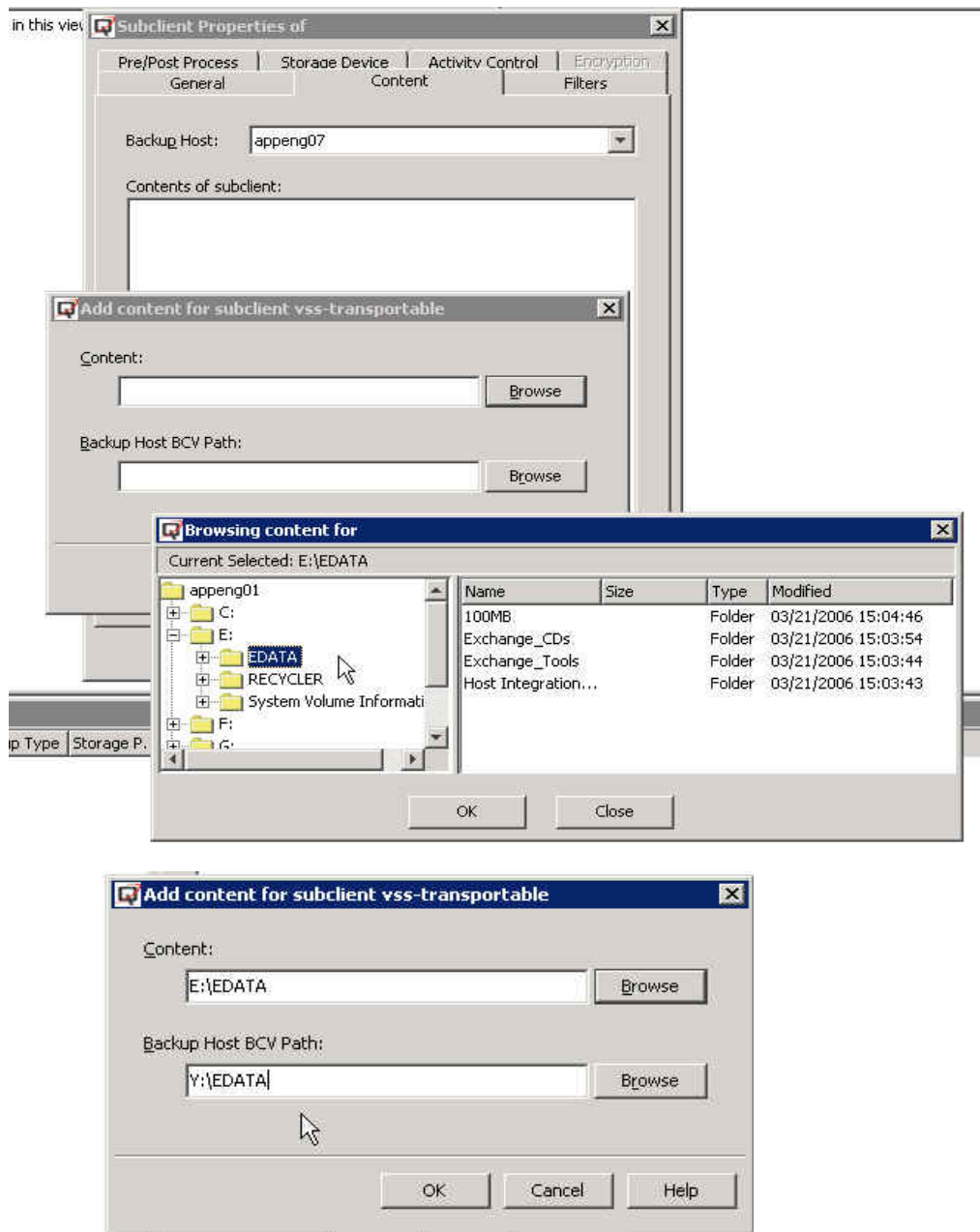


Figure 10: Working with unused drive letters.

5. Pre/Post Process setup. In step five the prescan and postbackup scripts are specified along with their locations. Use the Browse option to point to these batch files that were created during the production host configuration. If these files reside on the production server be sure to select "On Primary Host". See Figure 11 for an example.

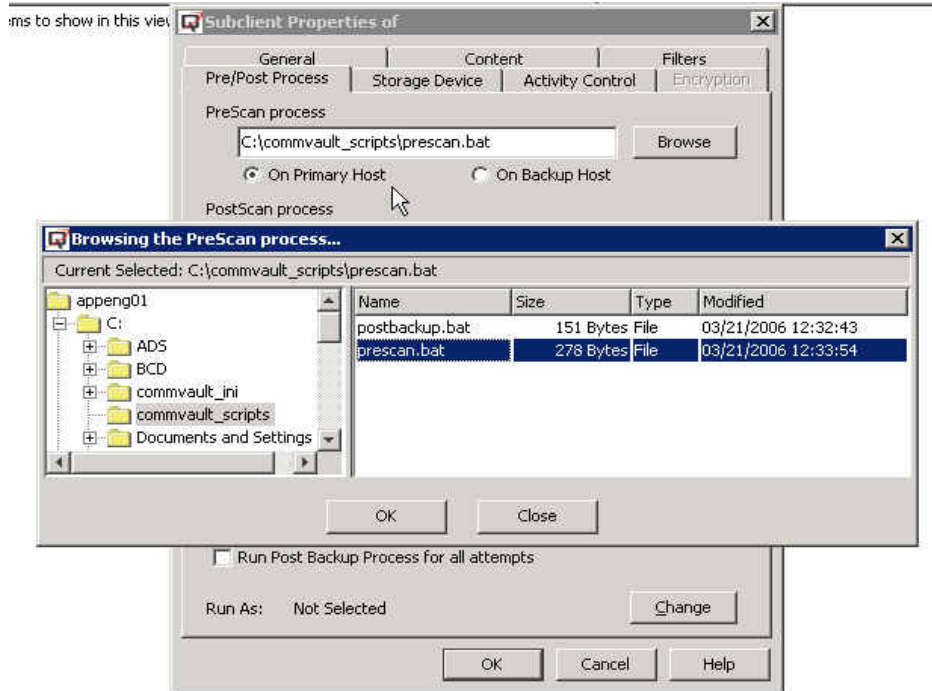


Figure 11: Pointing to prescan and postbackup scripts.

6. The final step to configure the ProxyHost Subclient is to select the account that has access to the prescan and postbackup scripts; the default uses the local system account. Click the “Change” button and select the local system account or choose another account with access rights to the scripts (Figure 12).



Figure 12: Specify access through the Local System Account.

Create a ProxyHost VSS Transportable Shadow Copy

Use the following procedure to create a VSS transportable shadow copy with the ProxyHost *iDataAgent*:

1. Using the CommCell Browser begin the ProxyHost Subclient backup operation by selecting the production host from the list of Client Computers. Next select the ProxyHost *iDataAgent*, and then the Subclient name. Highlight and right click the Subclient and select the Backup option. A new dialog box will open as shown in Figure 13.

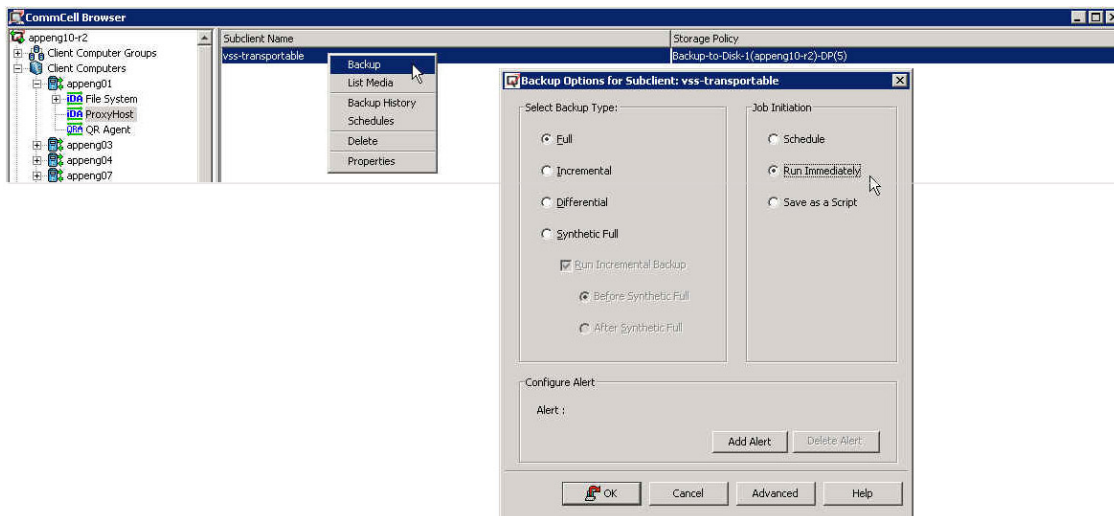


Figure 13: Setting snapshot backup options.

2. From the Backup Options for Subclient dialog box select the backup “Type” and “Job Initiation”. The example in Figure 13 initiates a full backup and runs it immediately.
3. Use the CommCell Browser Job Controller and EventViewer to monitor the progress of the shadow copy and backup process.

Summary

The combination of the EqualLogic Auto-Snapshot Manger hardware VSS capability in conjunction with CommVault Galaxy ProxyHost *iDataAgent* provides a reliable backup solution. The transportable shadow copy feature enables a method to create consistent point-in-time backup images nearly transparent to the operation of the server that is being protected.

Appendix: CommVault Recommendations: Transportable Shadow Considerations

Before creating VSS Hardware Shadows, review the following information:

- VSS hardware providers create snapshots at the volume level, not the partition level. It is recommended that each volume have only one partition.
- Transportable shadows can only be deleted after they have been imported. If you attempt to delete a transportable shadow that has not been imported, it will be automatically imported to the default import host before deletion.
- **ProxyHost**
 - You cannot create multiple VSS shadows of a source volume in a single Source-Destination mapping file. Even if you specify different destination mount points, any subsequent shadows of the same source will overwrite the shadow created before it. You can, however, use a different Source-Destination mapping file to create another shadow of the source volume to a different mount point.

Registry Key Attributes

| | |
|----------------------------------|--|
| Location | HKEY_LOCAL_MACHINE\SOFTWARE\CommVault Systems\Galaxy\Platform Information\ControlSet00#(<VirtualMachineName>\ |
| Key | QREnabler (standard) |
| Value | nTRANSPORTABLEFLAG (optional) |
| Value Type (Windows only) | DWORD |
| Valid Range | 0 - All VSS Hardware Shadows will not be transportable. 1 - All VSS Hardware Shadows will be transportable. |
| Created in | The source and destination hosts for the VSS hardware shadow. |
| Description | This key specifies whether all shadows created will be transportable. |
| Applies To | ProxyHost for Windows |

| | |
|----------------------------------|---|
| Location | HKEY_LOCAL_MACHINE\SOFTWARE\CommVault Systems\Galaxy\Platform Information\ControlSet00#(<VirtualMachineName>\ |
| Key | QREabler (standard) |
| Value | SLOCALBCDBASEPATH (optional) |
| Value Type (Windows only) | String |
| Valid Range | Set to the path to which the BCD files will be saved (e.g., c:\bcd). |
| Created in | The source host for the VSS hardware shadow. |
| Description | This key specifies where the BCD files will be saved. |
| Applies To | ProxyHost for Windows |

| | |
|----------------------------------|---|
| Location | HKEY_LOCAL_MACHINE\SOFTWARE\CommVault Systems\Galaxy\Platform Information\ControlSet00#(<VirtualMachineName>\ |
| Key | QREabler (standard) |
| Value | NUsePlexMode (optional) |
| Value Type (Windows only) | DWORD |
| Valid Range | 0 - Create Shadows. 1 - Create Clones. |
| Created in | The source and destination hosts for the VSS hardware shadows/clones. |
| Description | This key specifies whether shadows or clones will be created. |
| Applies To | ProxyHost for Windows |