

Using Symantec Backup Exec™ with the HP StorageWorks All-in-One Storage System (AiO)



Introduction.....	2
Intelligent backup of iSCSI data directly from the AiO.....	2
Extending AiO intelligent backup to Symantec Backup Exec™.....	3
Creating a backup job.....	4
Creating a restore job.....	7
For more information.....	11

Introduction

Although the HP StorageWorks All-in-One (AiO) storage system includes integrated HP Data Protector Express software, some users may already have standardized on other backup software. With AiO release 1.3 and beyond, it is possible to use pre- and post-scripts generated by AiO with other backup software to protect data hosted in iSCSI virtual disks on the AiO system.

Any backup software product may be easily used to back up system state, system files, and user data stored directly in files and folders on the AiO system. However, the AiO system may also act as an iSCSI target for application data such as Microsoft® Exchange Storage Groups and SQL Server databases. This data is migrated to the AiO system and is stored by the Microsoft iSCSI Software Target in Virtual Hard Disk (.vhd) files. It is not recommended that these files be backed up directly. The .vhd file will be the size of the virtual drive, which will likely be much larger than the actual size used by the files it contains. Furthermore, the application (for example, Microsoft Exchange) would not be involved in the backup, so databases will not be quiesced.

There are three primary ways to protect the data in these .vhd files. First, you can install a backup application on the host server and back up the data from the host server as if it was residing on a local drive. Second, you can back up directly from the AiO using the intelligent integration we have designed into the system. Third, you can use the pre- and post-script mechanism described in this paper to extend this direct backup model to other backup applications.

Intelligent backup of iSCSI data directly from the AiO

The All-in-One Storage Manager (ASM) enables direct backup of the iSCSI .vhd file from the AiO by generating pre- and post-scripts for each application instance that has been migrated to the AiO system. The scripts issue commands supported by an ASM command line interface. Commands in the pre-script create application aware snapshots of iSCSI volumes, and then mounts those snapshots as read-only local volumes on the AiO system, allowing backup software to access the files contained in the .vhd file. The **create snapshot** command is actually executed remotely via the ASM Agent on the application server (for example the Exchange Server), so the application's VSS Writer becomes involved and freezes any data stores and transaction logs for the few seconds that it takes to snapshot each of the involved iSCSI volumes. The resulting snapshot set, containing a snapshot for each involved volume, is then available on the AiO system. After the backup job runs, the post-script issues a command to unmount the local volume(s) and delete the snapshot set.

For a restore job that overwrites the original location, the process is similar. The pre-script will unmount the iSCSI virtual disks from the application server, and mount them locally as writable volumes on the AiO system on the same mount point that was used for backups. When the restore job runs, it will overwrite the files in the virtual disks. The post-script then remounts the virtual disks on the application server. A restore job may also be created to write to an alternate location and, in this case, pre- and post-scripts are not needed.

NOTE: Backing up iSCSI .vhd files directly from the AiO using the process described above has the benefit of significantly reducing backup windows and impact on the application server; however, it does back up data at the volume level. If your data protection strategy calls for more granular recovery (for example, individual Exchange mailboxes) you may choose to accept a larger backup window and back up from your application server using application backup agents.

Extending AiO intelligent backup to Symantec Backup Exec™

When the All-in-One Storage Manager (ASM) wizards are used to configure data protection using the pre-installed Data Protector Express software, all of this work is done on the user's behalf. Other backup software products may be used if they support the concept of a pre- and post-script. Using these products, you may manually configure the backup and restore jobs, and then specify the pre- and post-scripts that ASM generates. The following describes this process using Symantec Backup Exec™ 11d for Windows Servers.

While other backup products have not been tested, it is very likely that the same scripts will work, or you may even modify the generated scripts slightly to achieve the desired result.

Symantec Backup Exec™ may be used in either of two ways with an AiO system:

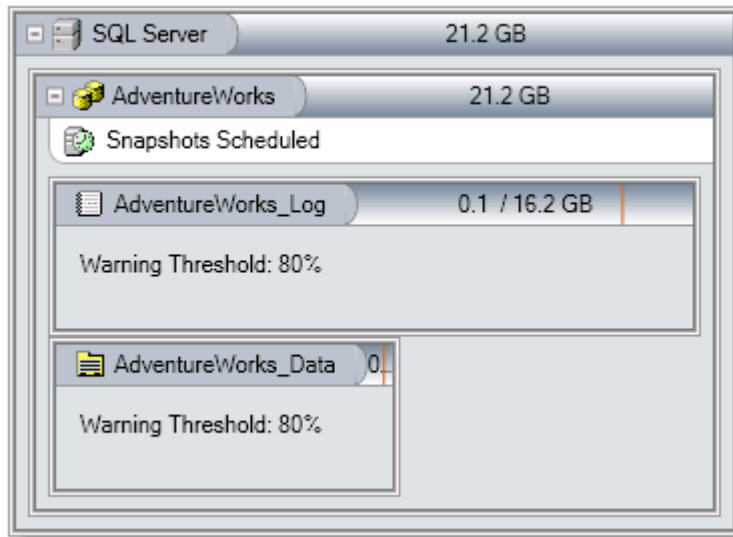
- Install Symantec Backup Exec™ for Windows Servers on the AiO system.

Or

- Install Symantec Backup Exec™ Remote Agent on the AiO system, and publish the AiO hostname or IP address to a Backup Exec™ Media Server on another system.

Creating a backup job

When using the ASM wizards to migrate application data such as Exchange, SQL Server, or a user-defined application to the AiO, do *not* select any Data Protection (except snapshots, if desired) since you will be manually creating your own backup jobs later. When the migration is complete, the application will appear in the application view of the All-in-One Storage Manager, as shown below:



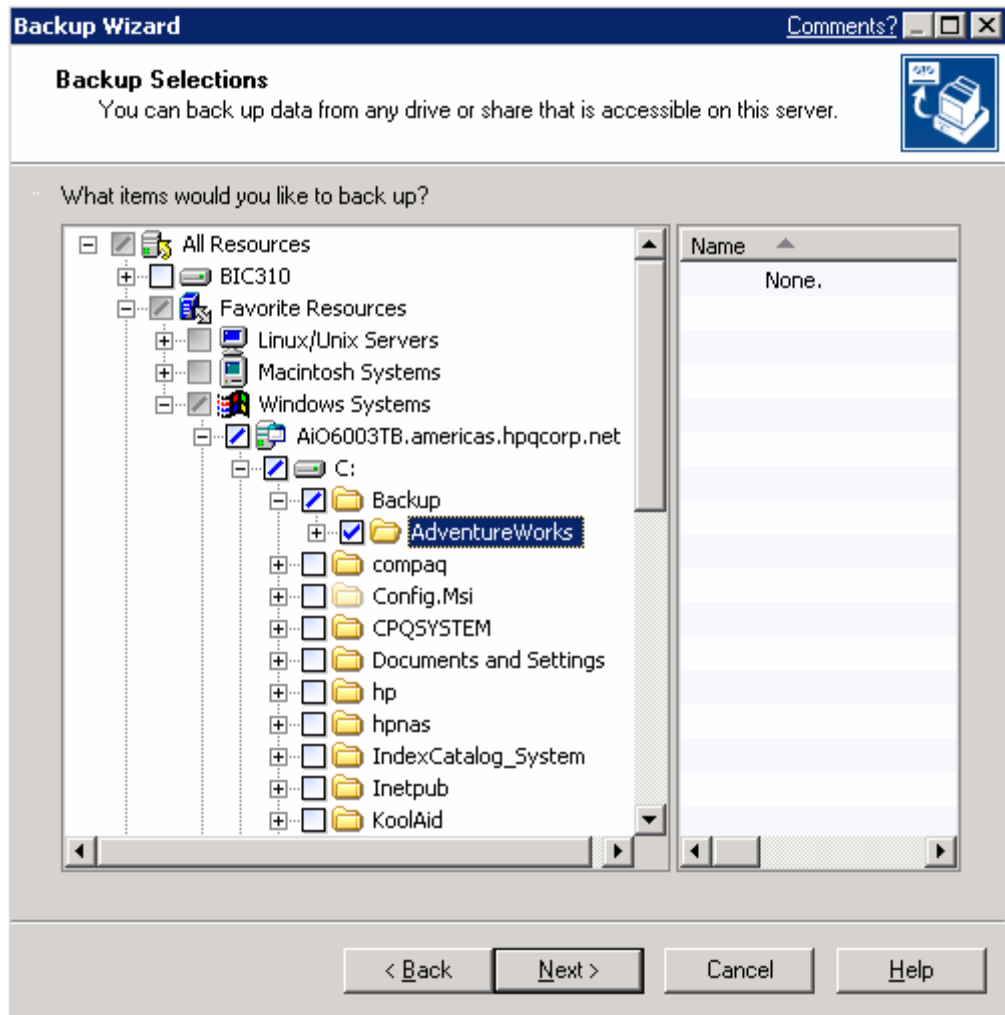
There will also be a directory with the same name as the application under **c:\backup**, for example, **c:\backup\AdventureWorks**.

NOTE: It is recommended that you maintain unique names for the applications migrated to the AiO system. However, it is possible for multiple applications of the same name to be hosted on the AiO system. In this case, the second and subsequent applications of the same name will be given a unique name for backup purposes. This will consist of the application name with a unique number appended. So, for example, the directory described above might be:

c:\backup\AdventureWorks 15645854

To create the backup job using Backup Exec:

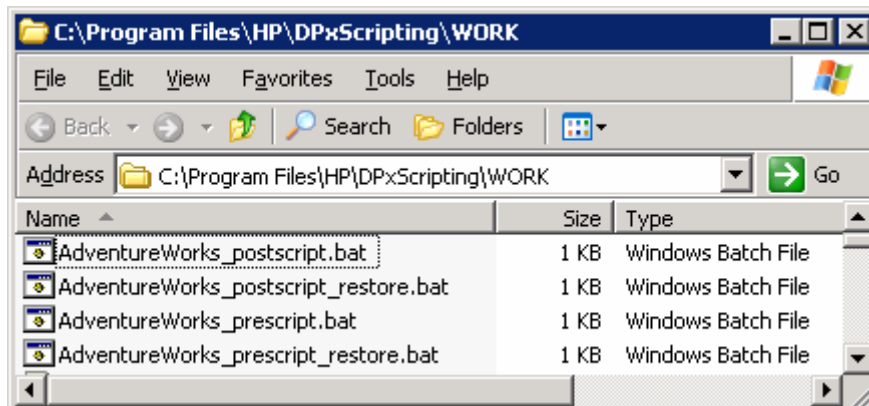
1. Specify this path on the AiO system as the backup selection. Click **Next**.



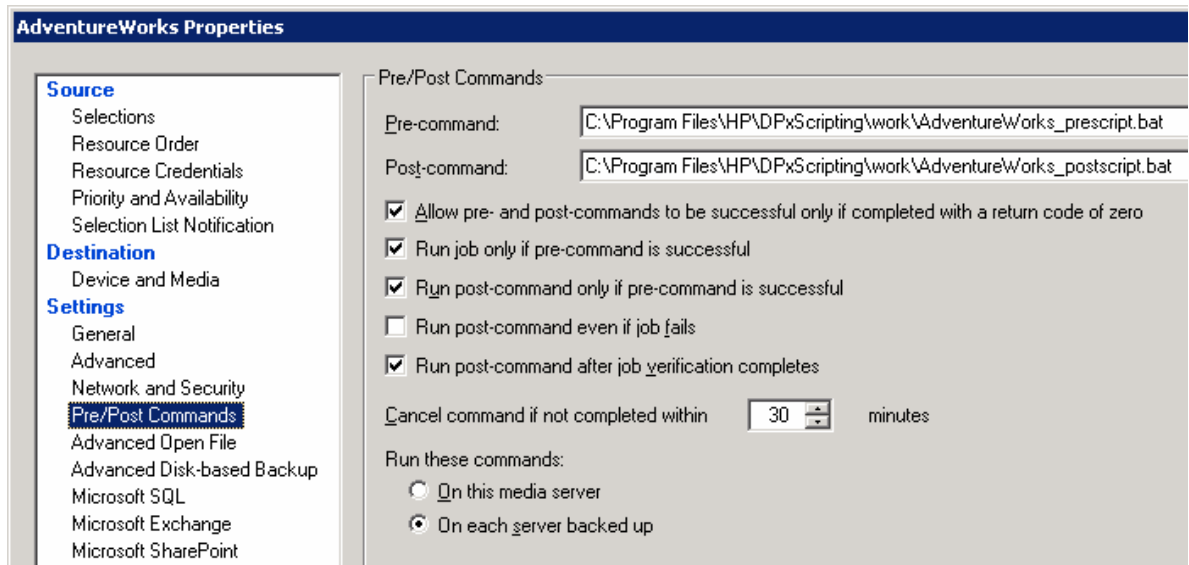
When the application data was migrated, ASM also created backup and restore pre- and post-scripts for the application instance. These scripts will be on the AiO system, at:

C:\Program Files\HP\DPxScripting\work

The following illustration shows the location of the scripts:



- After creating the Backup Exec™ backup job, modify its Pre/Post Commands properties by selecting the appropriate pre- and post-scripts, as shown below. Backup Exec uses the term “Pre/Post Commands” here. The commands may be scripts, such as those generated by ASM.

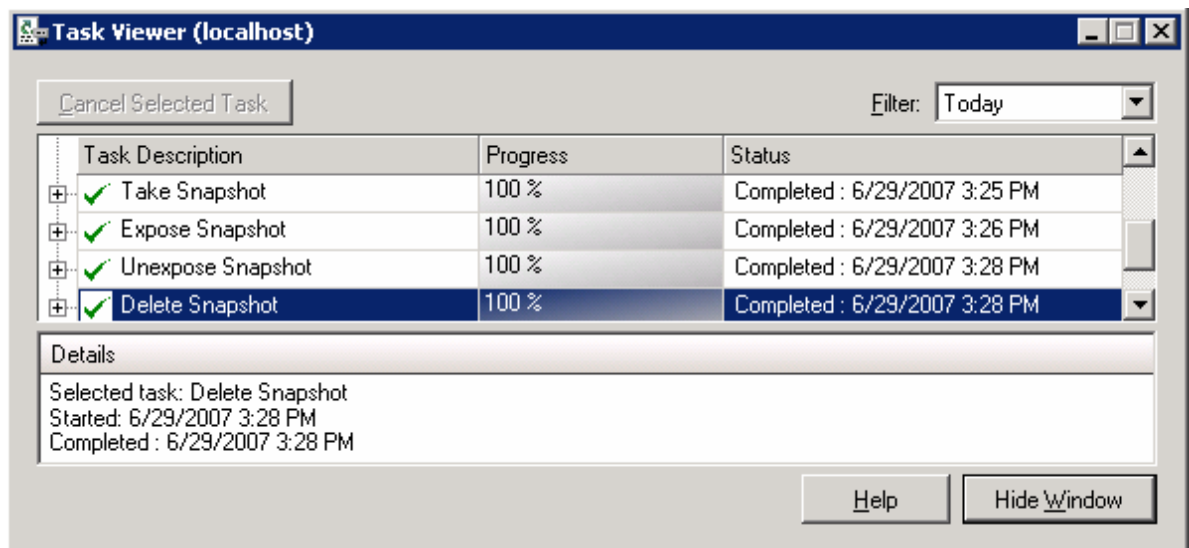


Ensure the following Post-commands are selected:

- Allow pre- and post-commands to be successful only if completed with a return code of zero.
- Run job only if pre-command is successful.
- Run post-command only if pre-command is successful.
- Run post-command after job verification completes.

- Under the Run these commands: option, select On each server backed up.
- Click **Submit**.

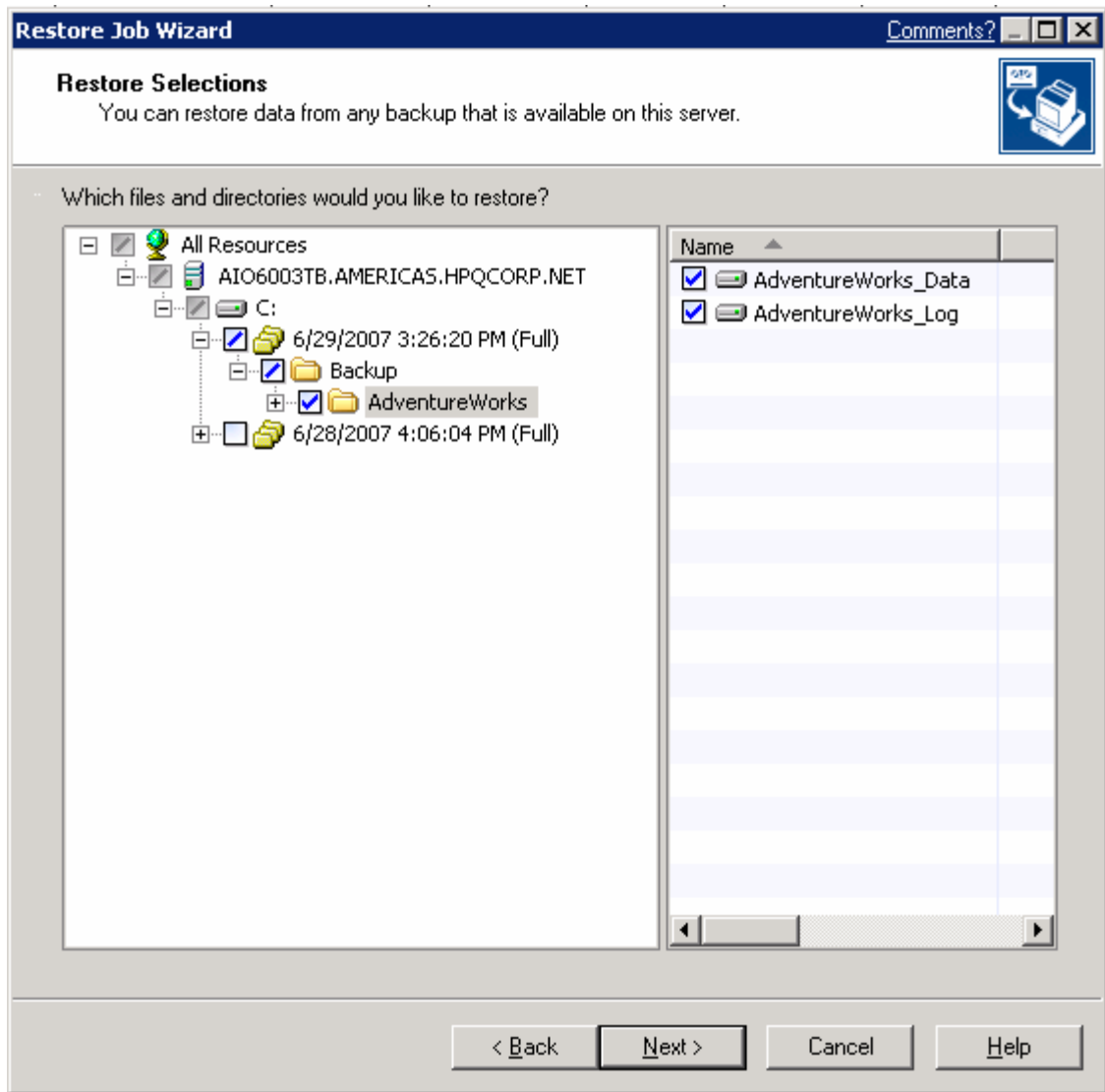
When the backup job runs, tasks appear in the ASM task viewer on the AiO as a result of the commands in the pre- and post-scripts that expose snapshots of the data on the backup path. The snapshots are unmounted and deleted when the backup job completes.



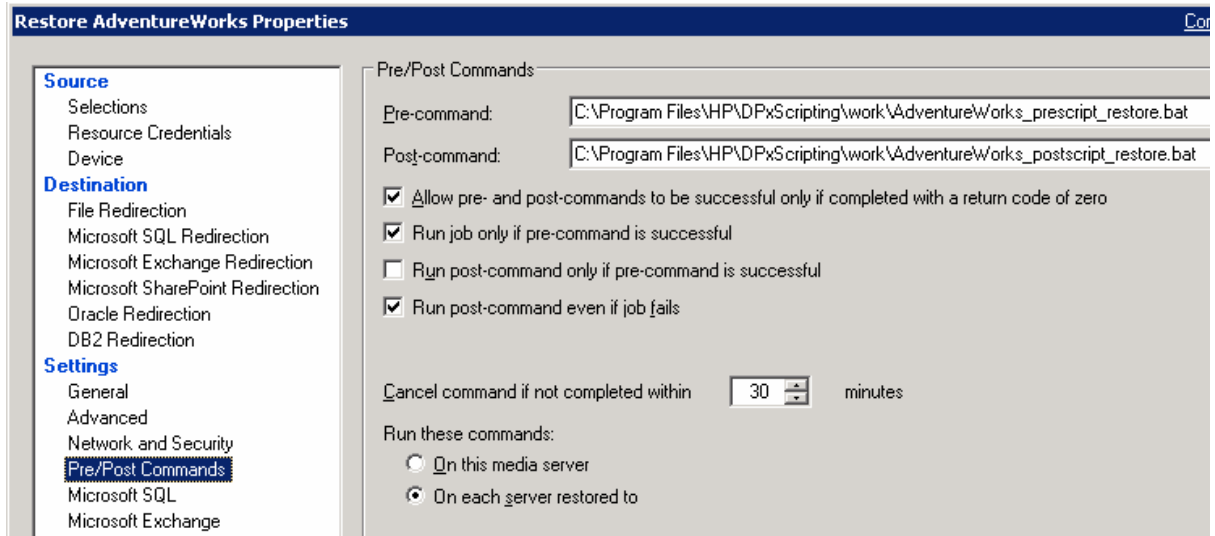
Creating a restore job

To create a restore job with Backup Exec™:

1. Select the desired session and specify the same path used for the original backup job, as shown below:



2. Finish creating the restore job. If you wish to restore the files to an alternate location, pre- and post-scripts are not needed. However, if you wish to overwrite the files in their original location, select pre- and post-scripts, as shown below. Backup Exec uses the term "Pre/Post Commands" here. The commands may be scripts, such as those generated by ASM.

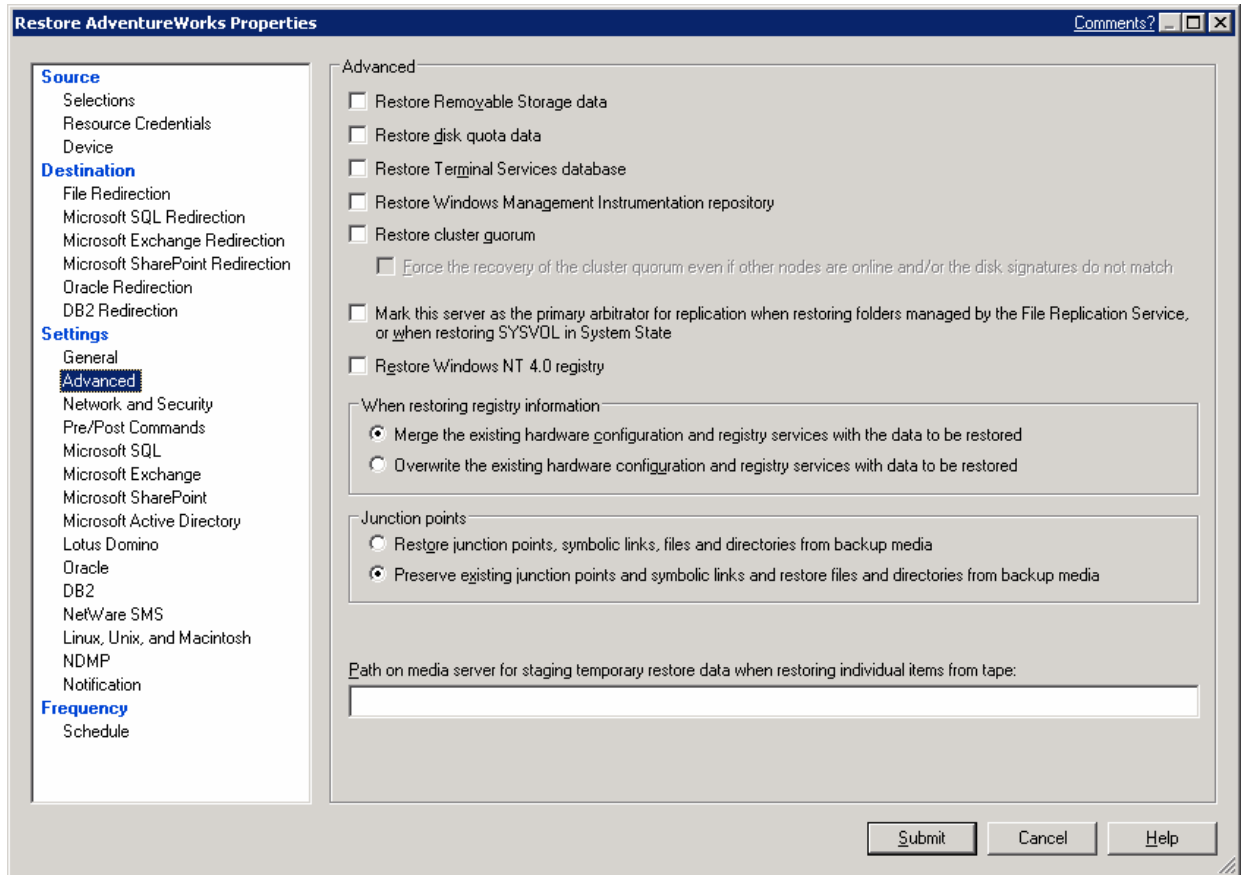


Ensure the following Post-commands are selected:

- Allow pre- and post-commands to be successful only if completed with a return code of zero.
 - Run job only if pre-command is successful.
 - Run post-command even if job fails.
3. Under the Run these commands: option, select On each server restored to.

4. In Advanced, change the setting for Junction points to Preserve existing junction points and symbolic links and restore files and directories from backup media.

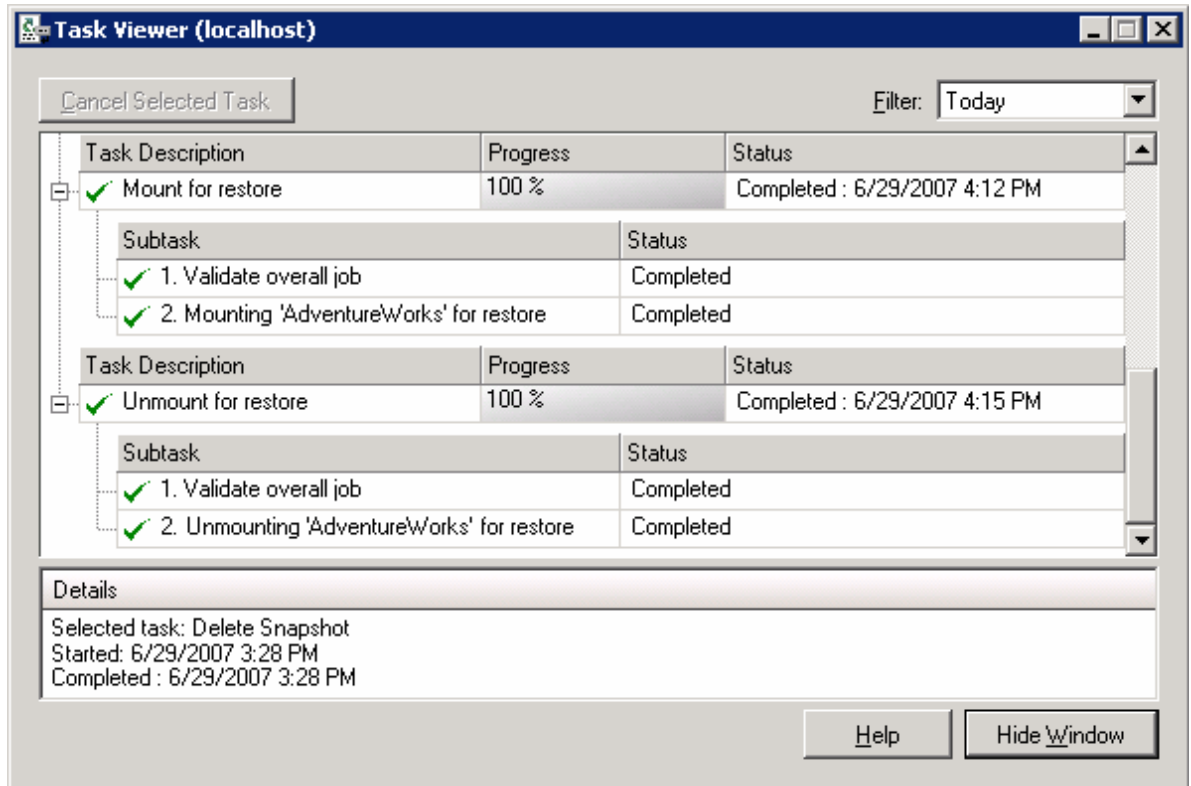
This setting is required in any case, whether the restore is set to overwrite files or not.



WARNING: Before running a restore job that overwrites files in their original location, bring the respective applications offline. For a Microsoft Exchange Storage Group, this means bringing the mail stores and any public stores offline. For a SQL Server database, it means detaching the database. For any user-defined applications, make sure the application is ready for files to be restored.

5. Click **Submit**.

When the restore job runs, the ASM task viewer displays the following tasks as the iSCSI volumes are unmounted from the application server and mounted on the backup path, allowing the backup software to restore files into the volumes.



The volumes are then remounted on the application server, and the application may be restarted (for example, bring mail stores online, attach databases, and so on).

For more information

For more information about HP StorageWorks All-in-One Storage Systems, contact your local HP reseller, or see <http://www.hp.com/go/AiOStorage>.

For more information on other HP StorageWorks products including dedicated NAS, SAN, and data protection products, please visit www.hp.com/go/storage.

For information on Microsoft storage technologies and building blocks, see www.microsoft.com/storage.

© 2007 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Itanium is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

4AA1-4876ENW, September 2007

