HP Data Protector best practices for backing up and restoring Microsoft SharePoint Server 2010

Technical white paper

Table of contents

Introduction

This white paper provides you with example procedures for backing up and restoring Microsoft SharePoint Server 2010, using Data Protector Microsoft SharePoint Server 2007/2010 integration (VDI based integration), Data Protector Microsoft SharePoint Server 2007/2010 VSS based solution (VSS based solution), or both of them.

Follow appropriate example procedure depending on your Microsoft SharePoint Server 2010 environment. However, first you should consider basic security---related aspects to ensure secure operation of Data Protector.

For details of how to configure and use the Data Protector Microsoft SharePoint Server 2007/2010 integration and the Data Protector Microsoft SharePoint Server 2007/2010 VSS based solution, see the *HP Data Protector Integration Guide for Microsoft Applications*. For details of how to use the Data Protector Microsoft SharePoint Server 2007/2010 VSS based solution to back up Microsoft SharePoint Server 2010 data that resides on disk arrays, see the *HP Data Protector Zero Downtime Backup Integration Guide*. For details of how to configure Data Protector security, see the online Help.

Configuring Data Protector Security

Data Protector security has to be planned, tested, and implemented on different security-critical layers to ensure the secure operation of Data Protector. Data Protector Users security is one of the security-critical layers of Data Protector. Each Data Protector user belongs to one user group only. This defines the user's rights.

Data Protector User rights

Data Protector provides three predefined user groups, *admin*, *operator*, and *user*, with specific user rights. The *admin* user group is assigned the strongest user rights which cannot be changed. To configure and use Data Protector for backing up and restoring Microsoft SharePoint Server 2010, the Microsoft SharePoint Server 2007/2010 farm administrator must be added to the Data Protector *admin* or *operator* user group. For details on adding users, creating user groups, and assigning user rights, see online Help.

NOTE
You can separate backup tasks that need to be performed by the Microsoft SharePoint Server farm administrator from those that need to be performed by the Data Protector administrator.

Data Protector Inet service user impersonation

On Windows systems, backup and restore sessions are started by the Data Protector Inet service, which by default runs under the Windows local SYSTEM user account. However, in case of Data Protector Microsoft SharePoint Server 2007/2010 integration, you must specify that sessions are started under the Microsoft SharePoint Server 2007/2010 farm administrator Windows domain user account. For this use the Data Protector user impersonation functionality. You can specify impersonation information by using the Data Protector CLI (by using `omniinetpasswd` or `omnicc` command) or GUI:

- To set up a user account for the Data Protector Inet service user impersonation on one or more specified clients in the farm, by specifying the user name (for example, `SHP farm admin)` and the password (for example, `mysecret`) directly or by saving the user name (for example, user `SHP farm admin` from the domain `HSL`) and the password (for example, `mysecret`) into the specified file, log on to the Cell Manager and from the `Data_Protector_home\bin directory`, run:

  ```
  omnicc -impersonation -add_user -user SHP farm admin@HSL -host Client1-
  host Client2 -host Client3 -passwd mysecret
  ```

  To enable user impersonation on all clients in the cell, specify the `–all` option.

- To add the specified user account from the local Inet configuration, run:

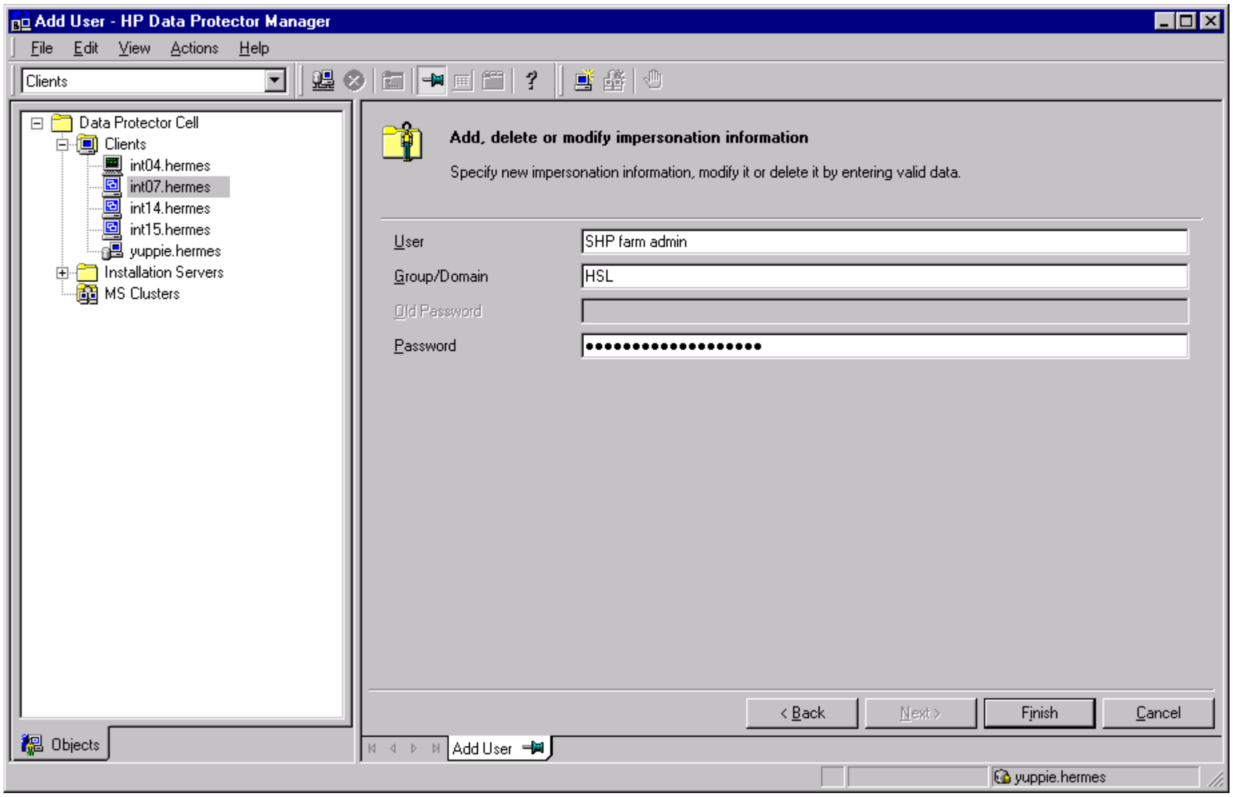
  ```
  omniinetpasswd –add {SHP farm admin@HSL|HSL\...} [Password]
  ```

  Omniinetpasswd prompts for the password if not specified in the command line.

- Open the Data Protector GUI:

1. In the Context List, click Clients.
2. In the Scoping Pane, under Clients, right-click a selected client system and click Add Impersonation.
3. In the Result Area, select the client systems for which you want to configure the Data Protector Inet service user impersonation and follow further steps.

Figure 1: Specifying impersonation information in Data Protector GUI



Add, delete or modify impersonation information

Specify new impersonation information, modify it or delete it by entering valid data.

User	SHP farm admin
Group/Domain	HSL
Old Password	
Password	••••••••••••••••••••

As a result, the Data Protector Inet service will impersonate the Microsoft SharePoint Server 2007/2010 farm administrator Windows domain user account and consequently start the integration agent under that user account although it will run under the Windows local SYSTEM user account.

NOTE
If Microsoft SQL Server systems are configured in a cluster, you must restart the Data Protector Inet service under a Windows domain user account on all cluster nodes. This account does not need to be the Microsoft SharePoint Server 2007/2010 farm administrator, but must be given the following Windows operating system Security Policy privileges:

- Impersonate a client after authentication
- Replace a process level token

To configure the Data Protector Inet service impersonation, firstly configure the Microsoft SharePoint Server 2007/2010 farm administrator Windows domain user account for the Data Protector user impersonation functionality (on all Microsoft SharePoint Server 2007/2010 systems and on all Microsoft SQL Server systems, run the `omniinetpasswd` command. For details, see the *HP Data Protector Zero Downtime Backup Integration Guide*). Secondly, specify the Microsoft SharePoint Server 2007/2010 farm administrator user name in the backup specification or in the restore wizard.

NOTE
You must rerun the `omniinetpasswd` command on all Microsoft SharePoint Server 2007/2010 systems and on all Microsoft SQL Server systems each time your farm administrator password is changed or expired.

For details on the Data Protector Inet service user impersonation, see the online Help index: "user impersonation".

Overview of Data Protector backup solutions for Microsoft SharePoint Server 2010

To back up and restore all Microsoft SharePoint Server 2010 objects, you need to configure and use both, the Data Protector Microsoft SharePoint Server 2007/2010 integration (**VDI based integration**) and the Data Protector Microsoft SharePoint Server 2007/2010 VSS based solution (**VSS based solution**).

The following Data Protector features are available to protect your Microsoft SharePoint Server 2010 data.

Backup and restore features

Granularity of backup and restore

VDI based integration agent can back up and restore the farm configuration, a content database or an individual web application.

VSS based solution agent can only back up and restore an individual database or index.

Scope of protection

VDI based integration agent cannot protect the entire farm (all Microsoft SharePoint Server 2010 system content and services). Backup and restore of search components are not supported.

VSS based solution can protect the entire farm.

Size of backup

VDI based integration agent can perform Full, Incremental and Differential backup.

VSS based solution agent can currently only perform Full backup.

Zero downtime backup (ZDB), instant recovery (IR), and transportable backups

VDI based integration agent cannot perform ZDB, IR, or transportable backups

VSS based solution agent can perform ZDB, IR, and transportable backups

Restore to a new location

VDI based integration agent can perform restore to a new location and recovery

VSS based solution agent cannot perform restore to a new location and recovery

Support for Microsoft FAST Search Server 2010 system

VDI based integration cannot back up and restore FAST Search index files

VSS based solution can back up and restore FAST Search index files

General recommendations

- Back up Web applications using the VDI based integration. It reduces the size of backup and shortens your backup window by enabling you to perform an Incremental backup. Restore to a new location enables a single item recovery.
- Back up service applications using the VSS based solution. It offers you a protection of vital farm services, including Search Service Applications (SSA) and the Secure Store Service.

Data Protector Microsoft SharePoint Server 2010 VSS based solution

Environment description

- A SharePoint farm of arbitrary size.
- You need to back up and restore Microsoft SQL Server databases, Microsoft SharePoint Server 2010 search index files and Microsoft FAST Search Server 2010 search index files. Database granularity suffices your needs. Zero downtime backup (ZDB) and instant recovery (IR) required.
- Use the Data Protector Microsoft SharePoint Server 2007/2010 VSS based solution.

Backup and restore of Microsoft SQL Server databases, Microsoft SharePoint Server 2010 search index files and Microsoft FAST Search Server 2010 search index files

Use the Data Protector Microsoft SharePoint Server 2007/2010 VSS based solution (VSS based solution) to back up and restore Microsoft SharePoint Server 2010 data that is stored in Microsoft SQL Server databases and to back up and restore Microsoft SharePoint Server 2010 and Microsoft FAST Search Server 2010 search index files.

The FAST Search index files can also be backed up incrementally, for all other Microsoft SharePoint Server data only the Full backup type is supported. Also, the VSS based solution enables you to perform zero downtime backup (ZDB) and instant recovery (IR) sessions. If you plan to run these sessions, ensure that the SPSearch and OSearch index files of each SSA, and the FAST Search index files reside on a disk array. Before backup or restore, run the PowerShell commands `SharePoint_VSS_backup.ps1 -help` to display the command usage and `SharePoint_VSS_backup.ps1 -version` to display the command version. Moreover, it is strongly recommended to start the Data Protector PowerShell command `SharePoint_VSS_backup.ps1` from the SharePoint 2010 Management Shell console.

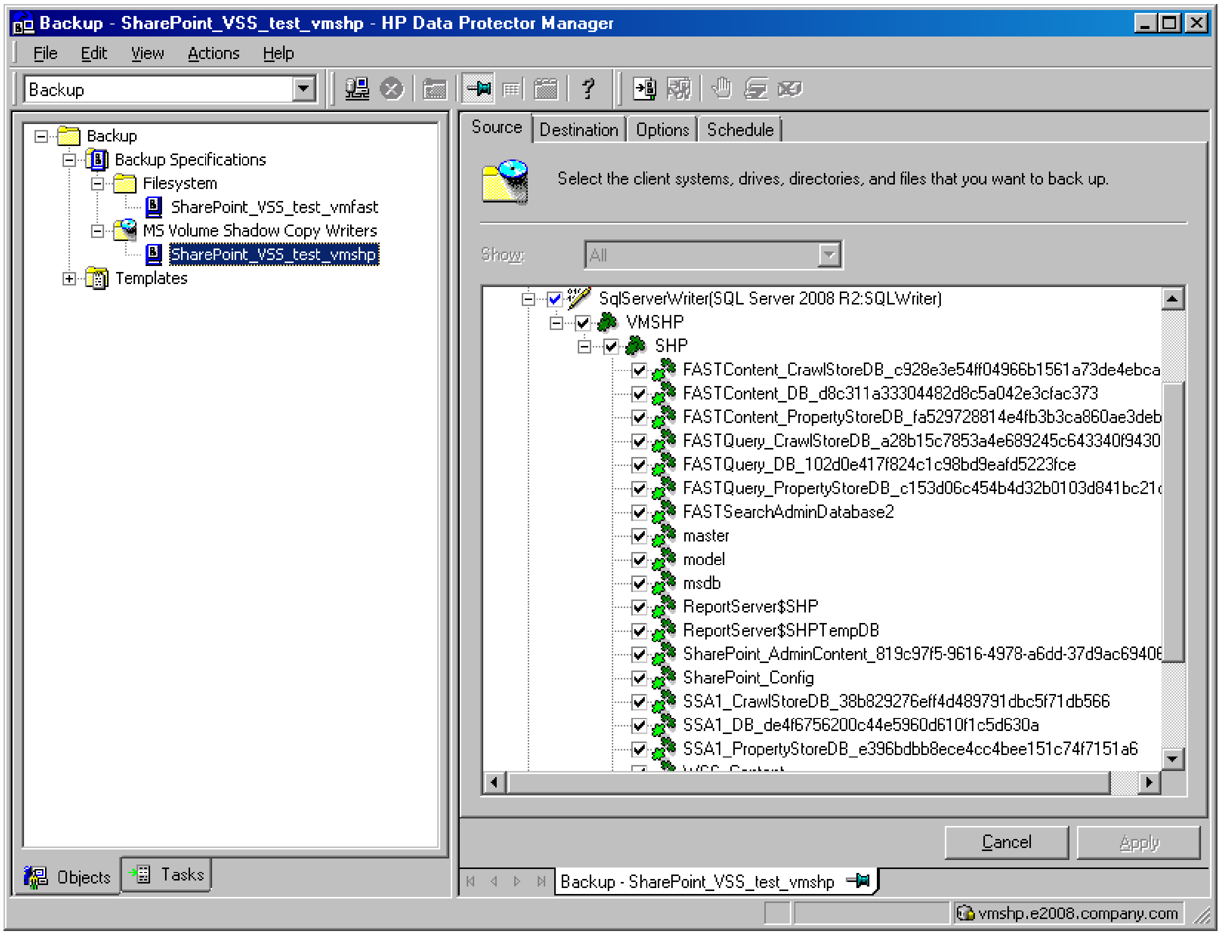
Backup

Create or identify a Windows domain user account that has Windows administrative rights on the Microsoft SharePoint Server system on which you plan to execute the Data Protector commands. This user must also be granted Microsoft SharePoint Server farm administrative rights and must be added to the Data Protector *admin* user group.

The only supported way to create backup specifications and start backup sessions is using the Data Protector PowerShell command `SharePoint_VSS_backup.ps1`. The command needs to be executed on one of the Microsoft SharePoint Server 2010 systems, recommended on the one where the Data Protector Cell Manager is installed. Starting backup sessions using the Data Protector GUI or CLI is not supported. However, you can use the Data Protector GUI to modify backup specifications (for example, to add backup devices).

For a system with the `SharePoint Foundation Database` service enabled, the command creates a backup specification that has the `SqlServerWriter` (Microsoft SQL Server 2005/2008) object selected.

Figure 2: Selection of Microsoft SharePoint Server 2010 databases for backup

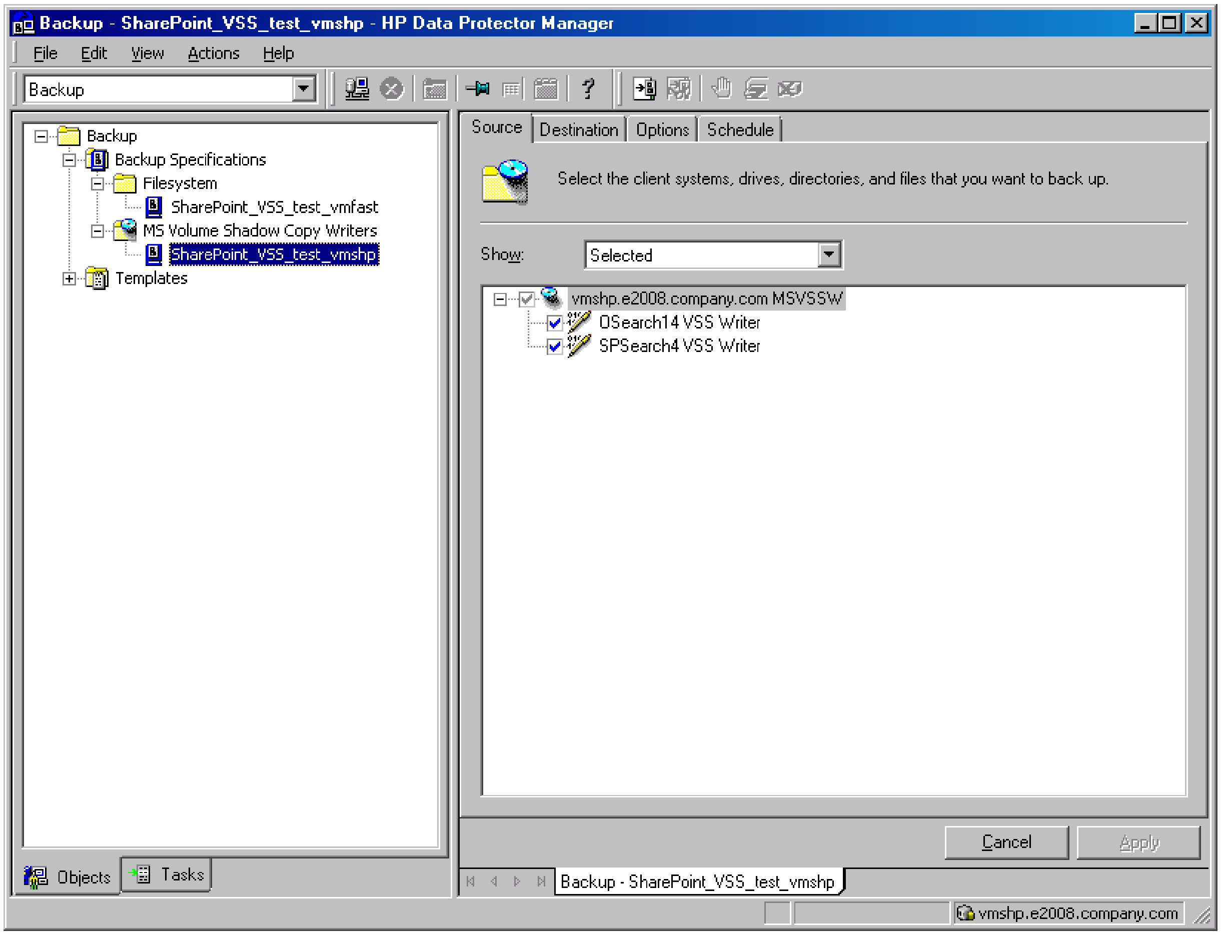

Backup - SharePoint_VSS_test_vmshp - HP Data Protector Manager
File
Edit
View
Actions
Help
Backup
Backup
Backup Specifications
Filesystem
SharePoint_VSS_test_vmfast
MS Volume Shadow Copy Writers
SharePoint_VSS_test_vmshp
Templates
Objects
Tasks
Source
Destination
Options
Schedule
Show:
All
Cancel
Apply
Backup - SharePoint_VSS_test_vmshp
vmshp.e2008.company.com

Select the client systems, drives, directories, and files that you want to back up.

- ☑ SqlServerWriter(SQL Server 2008 R2:SQLWriter)
  - ☑ VMSHP
    - ☑ SHP
      - ☑ FASTContent_CrawlStoreDB_c928e3e54ff04966b1561a73de4ebca
      - ☑ FASTContent_DB_d8c311a33304482d8c5a042e3cfac373
      - ☑ FASTContent_PropertyStoreDB_fa529728814e4fb3b3ca860ae3deb
      - ☑ FASTQuery_CrawlStoreDB_a28b15c7853a4e689245c643340f9430
      - ☑ FASTQuery_DB_102d0e417f824c1c98bd9eafd5223fce
      - ☑ FASTQuery_PropertyStoreDB_c153d06c454b4d32b0103d841bc21
      - ☑ FASTSearchAdminDatabase2
      - ☑ master
      - ☑ model
      - ☑ msdb
      - ☑ ReportServer$SHP
      - ☑ ReportServer$SHPTempDB
      - ☑ SharePoint_AdminContent_819c97f5-9616-4978-a6dd-37d9ac6940
      - ☑ SharePoint_Config
      - ☑ SSA1_CrawlStoreDB_38b829276eff4d489791dbc5f71db566
      - ☑ SSA1_DB_de4f6756200c44e5960d610f1c5d630a
      - ☑ SSA1_PropertyStoreDB_e396bdbb8ece4cc4bee151c74f7151a6

For a system with the `SharePoint Foundation Help Search` and `SharePoint Server Search` services enabled, the command creates a backup specification that has the `SPSearch4 VSS Writer` and `OSearch14 VSS Writer` objects selected.

Figure 3: Selection of Microsoft SharePoint Server 2010 search index files for backup



Backup

- Backup
  - Backup Specifications
    - Filesystem
      - SharePoint_VSS_test_vmfast
    - MS Volume Shadow Copy Writers
      - SharePoint_VSS_test_vmshp
  - Templates

Select the client systems, drives, directories, and files that you want to back up.

Show: Selected

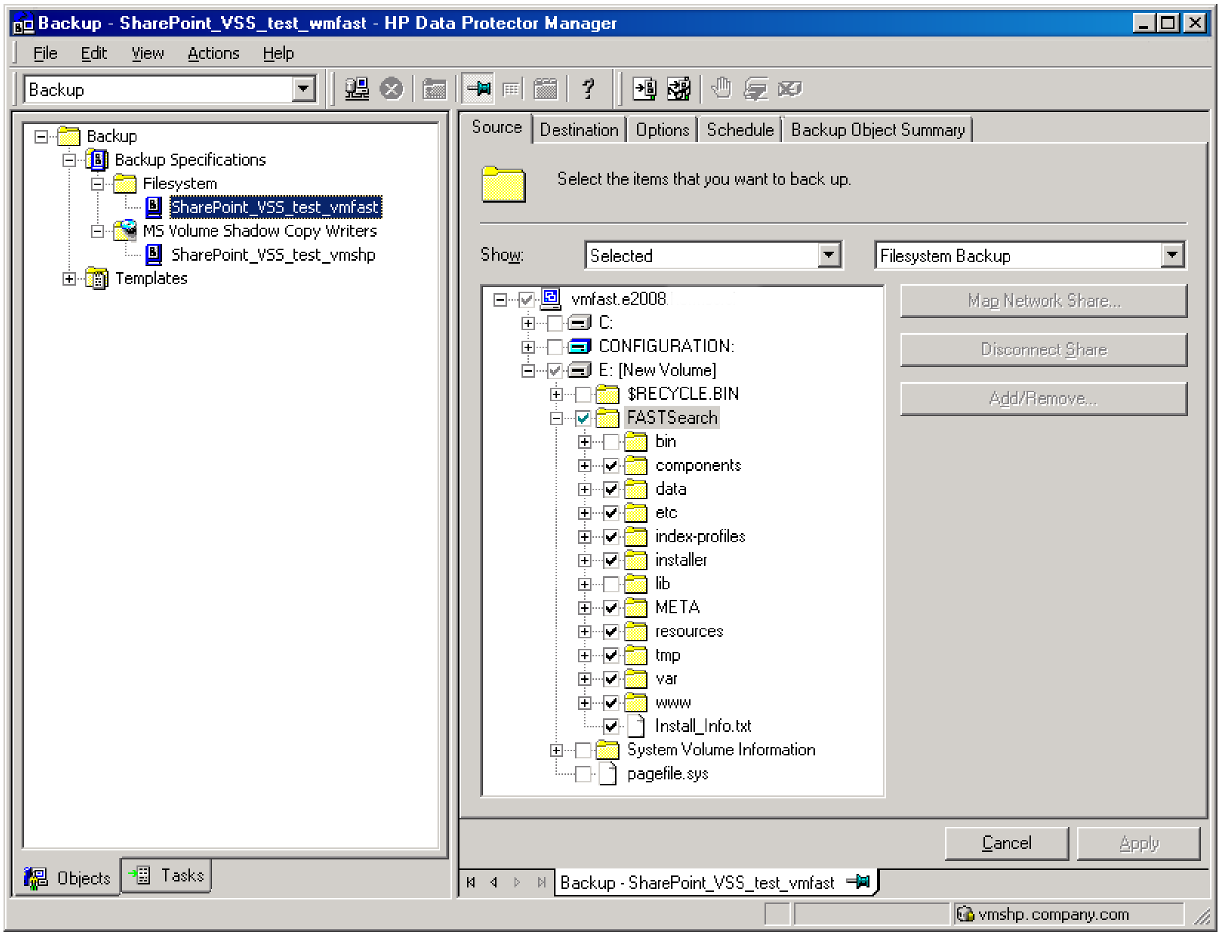
- ☑ vmshp.e2008.company.com MSVSSW
  - ☑ OSearch14 VSS Writer
  - ☑ SPSearch4 VSS Writer

Backup - SharePoint_VSS_test_vmshp

vmshp.e2008.company.com

For a system with the FAST Search Server 2010 service enabled, the command creates a filesystem backup specification (Data Protector filesystem backup with the Use Shadow Copy option selected) that has the FASTSearch home folder selected, excluding bin and lib folders which contain FAST executables.

Figure 4: Selection of FAST Search Server 2010 search index files for backup (filesystem backup with the Use Shadow Copy option selected)



Backup - SharePoint_VSS_test_wmfast - HP Data Protector Manager

Select the items that you want to back up.

Show: Selected

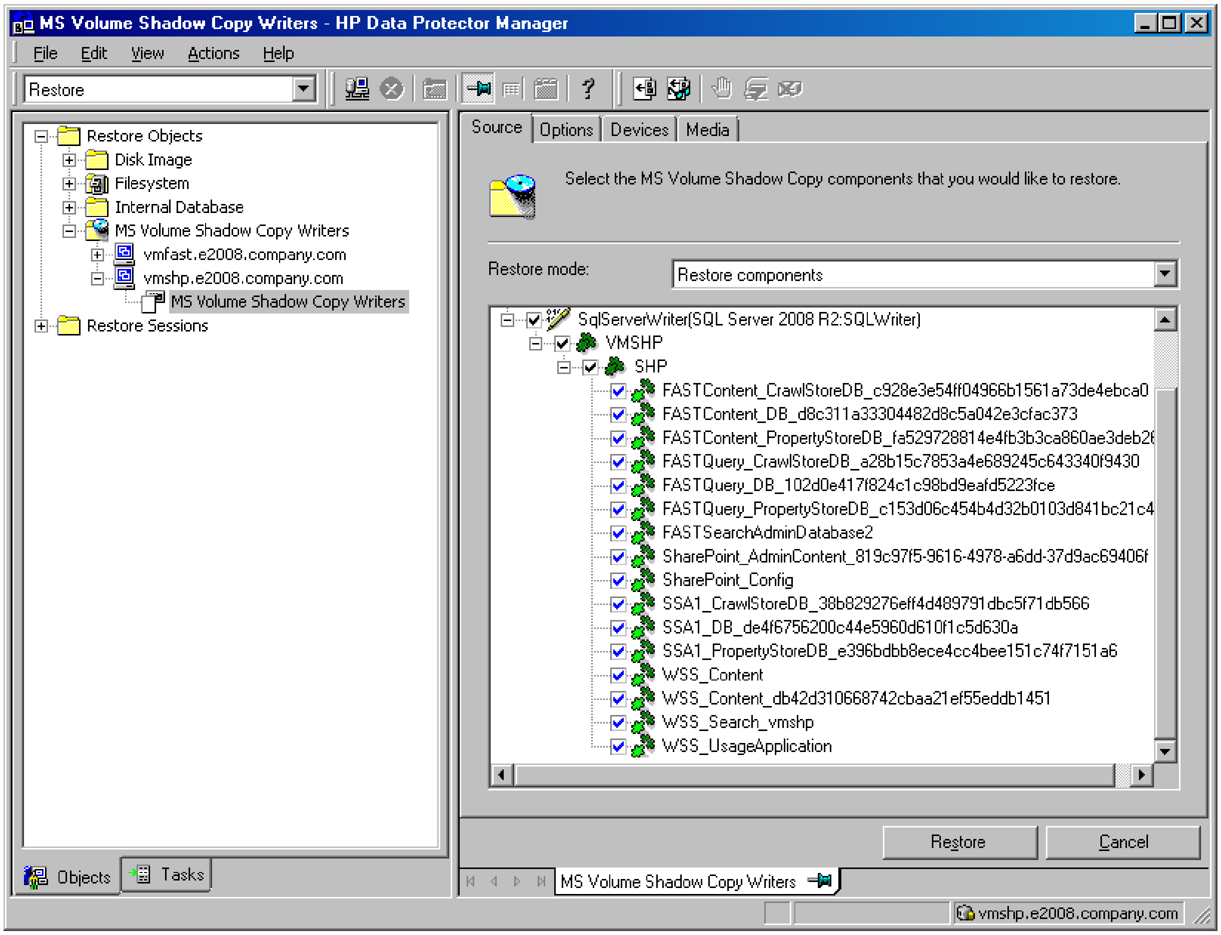
Filesystem Backup

For a system with the `FAST Search Server 2010` service enabled, the command with the –`hardware` option specified creates a VSS backup specification that has the complete `FASTSearch` home folder (including `bin` and `lib`) selected.

Restore

You can restore Microsoft SharePoint Server data using the Data Protector GUI or CLI.

Figure 5: Selection of Microsoft SharePoint Server 2010 databases for restore

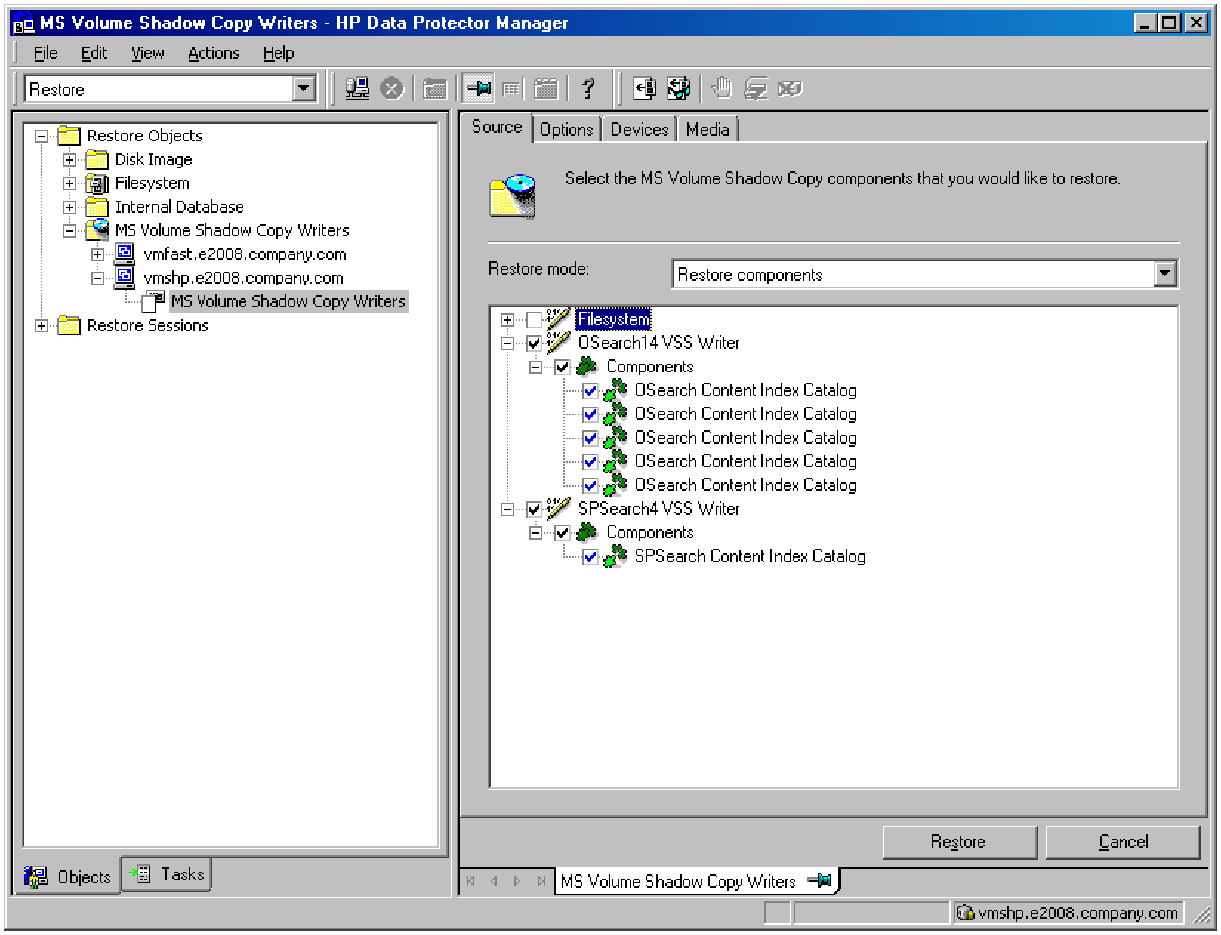


Select the MS Volume Shadow Copy components that you would like to restore.

Restore mode: Restore components

- ☑ SqlServerWriter(SQL Server 2008 R2:SQLWriter)
  - ☑ VMSHP
    - ☑ SHP
      - ☑ FASTContent_CrawlStoreDB_c928e3e54ff04966b1561a73de4ebca0
      - ☑ FASTContent_DB_d8c311a33304482d8c5a042e3cfac373
      - ☑ FASTContent_PropertyStoreDB_fa529728814e4fb3b3ca860ae3deb2
      - ☑ FASTQuery_CrawlStoreDB_a28b15c7853a4e689245c643340f9430
      - ☑ FASTQuery_DB_102d0e417f824c1c98bd9eafd5223fce
      - ☑ FASTQuery_PropertyStoreDB_c153d06c454b4d32b0103d841bc21c4
      - ☑ FASTSearchAdminDatabase2
      - ☑ SharePoint_AdminContent_819c97f5-9616-4978-a6dd-37d9ac69406f
      - ☑ SharePoint_Config
      - ☑ SSA1_CrawlStoreDB_38b829276eff4d489791dbc5f71db566
      - ☑ SSA1_DB_de4f6756200c44e5960d610f1c5d630a
      - ☑ SSA1_PropertyStoreDB_e396bdbb8ece4cc4bee151c74f7151a6
      - ☑ WSS_Content
      - ☑ WSS_Content_db42d310668742cbaa21ef55eddb1451
      - ☑ WSS_Search_vmshp
      - ☑ WSS_UsageApplication

Figure 6: Selection of Microsoft SharePoint Server 2010 search index files for restore



- Restore Objects
  - Disk Image
  - Filesystem
  - Internal Database
  - MS Volume Shadow Copy Writers
    - vmfast.e2008.company.com
    - vmshp.e2008.company.com
      - MS Volume Shadow Copy Writers
- Restore Sessions

Select the MS Volume Shadow Copy components that you would like to restore.

Restore mode: Restore components

- □ Filesystem
- ☑ OSearch14 VSS Writer
  - ☑ Components
    - ☑ OSearch Content Index Catalog
    - ☑ OSearch Content Index Catalog
    - ☑ OSearch Content Index Catalog
    - ☑ OSearch Content Index Catalog
    - ☑ OSearch Content Index Catalog
- ☑ SPSearch4 VSS Writer
  - ☑ Components
    - ☑ SPSearch Content Index Catalog

NOTE

To adhere to your Separation of duties security standards, you can separate tasks as follows:

1. The Microsoft SharePoint Server 2007/2010 farm administrator performs the Data Protector PowerShell command:

   ```
   SharePoint_VSS_backup.ps1 -createonly - dev null-device
   ```

   The farm is discovered. The backup specification is created with a null-device (dummy device) and does not need the Data Protector Save backup specification user right.
   The Microsoft SharePoint Server 2007/2010 farm administrator can see backup devices and can create a backup specification using an existing device.

2. The Data Protector backup administrator modifies the backup specification to use proper devices.

   IMPORTANT:

   If only one device is used to back up a multi-system farm, the corresponding backup sessions cannot run in parallel. This prolongs the time during which the farm is in read-only mode. Specifically, the farm is in read-only mode from the moment when the backup sessions are started up until all VSS snapshots are created. To enable backup sessions to run in parallel, select different or additional devices in each backup specification before the backup is started.

For details of how to modify the devices, see the *HP Data Protector Integration Guide for Microsoft Applications*.

This user does not require the Microsoft SharePoint Server 2007/2010 farm administrator privileges.

3. Using the Windows system scheduler, the Microsoft SharePoint Server 2007/2010 farm administrator runs the Data Protector PowerShell command:

```
Sharepoint_vss_backup.ps1 –backuponly
```

Data Protector Microsoft SharePoint Server 2010 integration (VDI based integration)

Environment description

- A small or medium SharePoint farm
- You need to back up and restore Web applications, associated content databases and the configuration database. No backup of search components needed.
- Use the Data Protector Microsoft SharePoint Server 2010 integration (VDI based integration).

Backup and restore of Web applications and associated content databases

The integration provides Full, Incremental, or Differential online backups of Web applications and associated content databases. Zero downtime backup (ZDB) is not supported with the VDI based integration.

Backup

Specify that a backup session is started under the Microsoft SharePoint Server 2007/2010 farm administrator Windows domain user account. This user account must be configured for the Data Protector user impersonation functionality. To create a backup specification, follow the procedure described in the Data Protector Microsoft SharePoint Server 2007/2010 integration chapter of *the HP Data Protector integration guide for Microsoft applications*.

Restore

When restoring a Web application, you can select the entire Web application or individual content databases. Both can be restored to a new location. For details, see “Restore options” in the Data Protector Microsoft SharePoint Server 2007/2010 integration chapter of the *HP Data Protector integration guide for Microsoft applications*.

NOTE

To adhere to your Separation of duties security standards, you can separate tasks as follows:

1. The Microsoft SharePoint Server 2007/2010 farm administrator must configure the farm administrator user account for the Data Protector user impersonation functionality: on each Microsoft SharePoint Server 2007/2010 system, the farm administrator must run the Omniinet password utility:

   ```
   omniinetpasswd -add User@Domain
   ```

   You will be asked for the password.

2. The Data Protector administrator creates a backup specification with the Microsoft SharePoint Server 2007/2010 farm administrator username and Domain name specified, but without its password. The Data Protector administrator schedules the backup specification and assigns needed devices.
3. The Microsoft SharePoint Server 2007/2010 farm administrator can start the backup specification provided the administrator has been granted the Data Protector Start backup specification user right, but cannot schedule it without the Data Protector Save backup specification user right. As a workaround, the backup specification can be started using the Windows system scheduler:

   ```
   omnib -mssharepoint_list ListName -barmode -full | diff | incr
   ```

Combining Data Protector Microsoft SharePoint Server 2010 VSS based solution and VDI based integration

Environment description

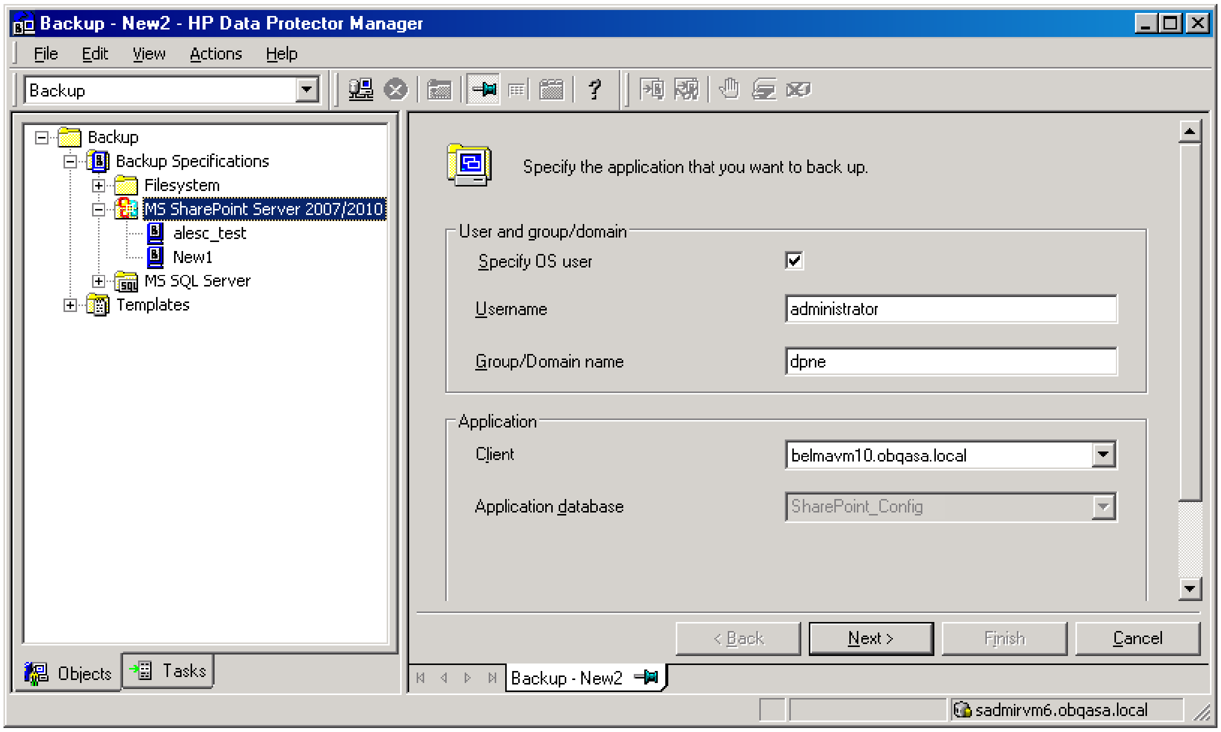
- A SharePoint farm of arbitrary size
- You need to back up the entire Microsoft SharePoint Server 2010 farm. You can run zero downtime backup (ZDB) and instant recovery (IR) sessions. For details, see the *HP Data Protector Zero Downtime Backup Integration Guide.* Also, you can perform disaster recovery (DR). For details, see *HP Data Protector Disaster Recovery Guide.*
- Use a combination of Microsoft SharePoint Server 2010 integration (VDI based integration) and Data Protector Microsoft SharePoint Server 2007/2010 VSS based solution.

Backup and restore of the entire Microsoft SharePoint Server 2010 farm

Backup

- Back up Web applications and associated content databases using the VDI based integration.

Figure 7: Specifying the application that you want to back up



Specify the application that you want to back up.

User and group/domain

Specify OS user ☑

Username: administrator

Group/Domain name: dpne

Application

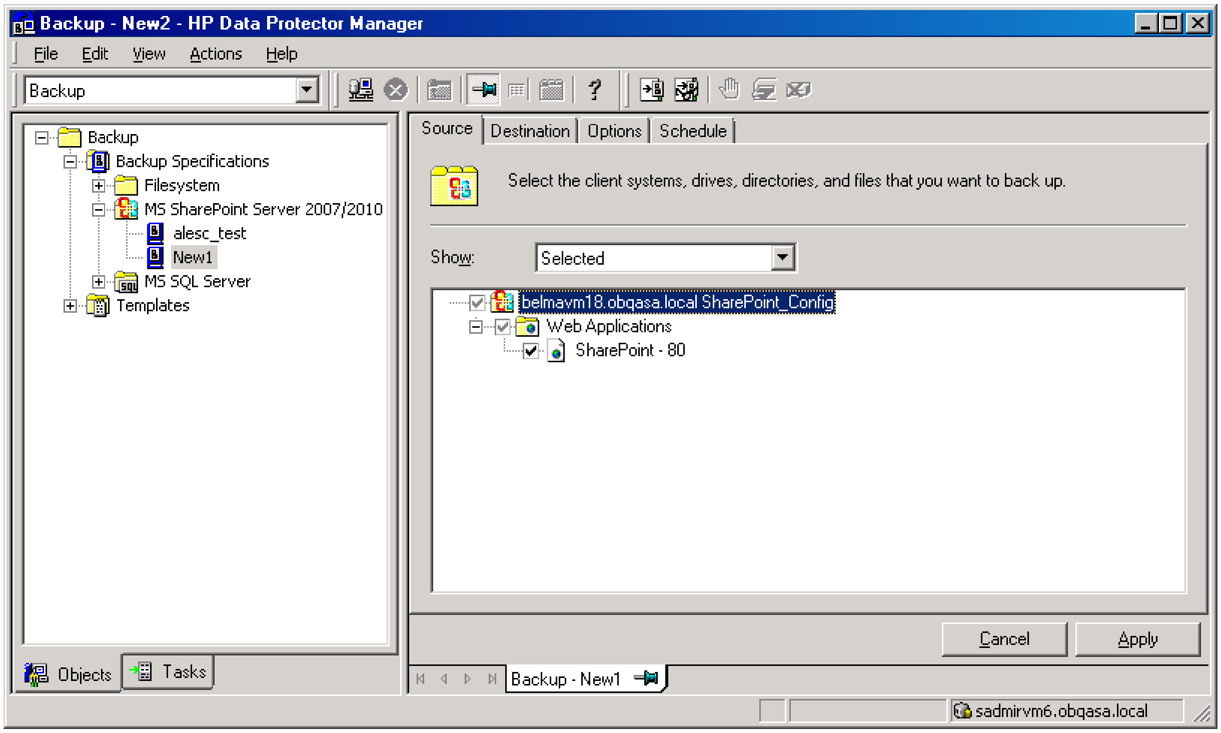
Client: belmavm10.obqasa.local

Application database: SharePoint_Config

IMPORTANT:

The entry point client system needs to be the system on which the Data Protector PowerShell command of the VSS based solution will be started and has the Data Protector Microsoft SharePoint Server 2007/2010 integration agent installed.

Figure 8: Selecting the client systems, drives, directories, and files that you want to back up



Select the client systems, drives, directories, and files that you want to back up.

Show: Selected

- Back up all other components using the VSS based solution:

1. Create VSS based solution backup specifications using the Data Protector PowerShell command, placing it in in the Data Protector `bin` directory on the client with the Data Protector Microsoft SharePoint Server 2007/2010 integration agent installed:

   ```
   \\OmniBack\bin>.\SharePoint_VSS_backup.ps1 -createonly -prefix HYBRID -
    dev FileLib_Writer0
   ```

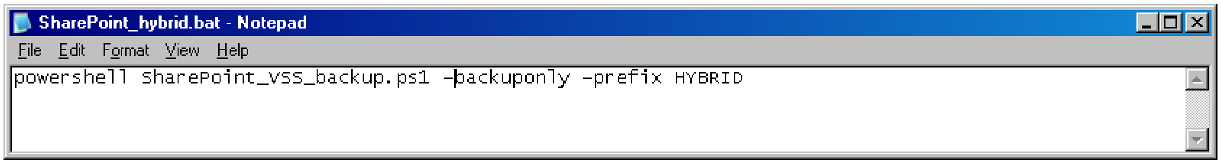
2. Modify VSS based solution backup specifications using the Data Protector GUI:
   - Open the newly created backup specifications and exclude all Web application content databases backed up with the VDI based integration from the VSS based solution backup specifications.
   - Choose the SQL database to be backed up.
   - Edit the device settings. Configure a unique device per each backup specification.

   IMPORTANT:

   The names of the content databases are the same as in the VDI based integration backup specification.

3. Start the VSS backup specifications using the Data Protector PowerShell command on the client with the Data Protector Microsoft SharePoint Server 2007/2010 integration agent installed:
   - Save the Data Protector PowerShell command `SharePoint_VSS_backup.ps1 -backuponly -prefix HYBRID` in the batch file `SharePoint_hybrid.bat`.

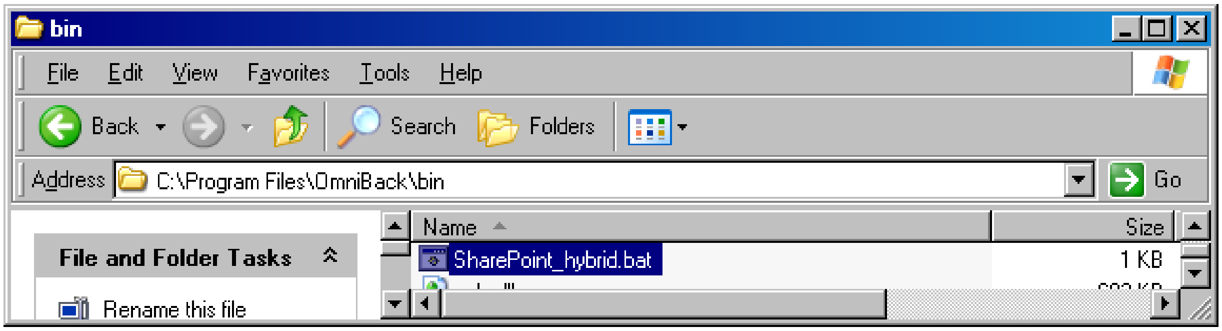
Figure 9: Saving the Data Protector PowerShell command `powershell SharePoint_VSS_backup.ps1 -backuponly -prefix HYBRID` in the batch file `SharePoint_hybrid.bat`.



```
powershell SharePoint_VSS_backup.ps1 -backuponly -prefix HYBRID
```

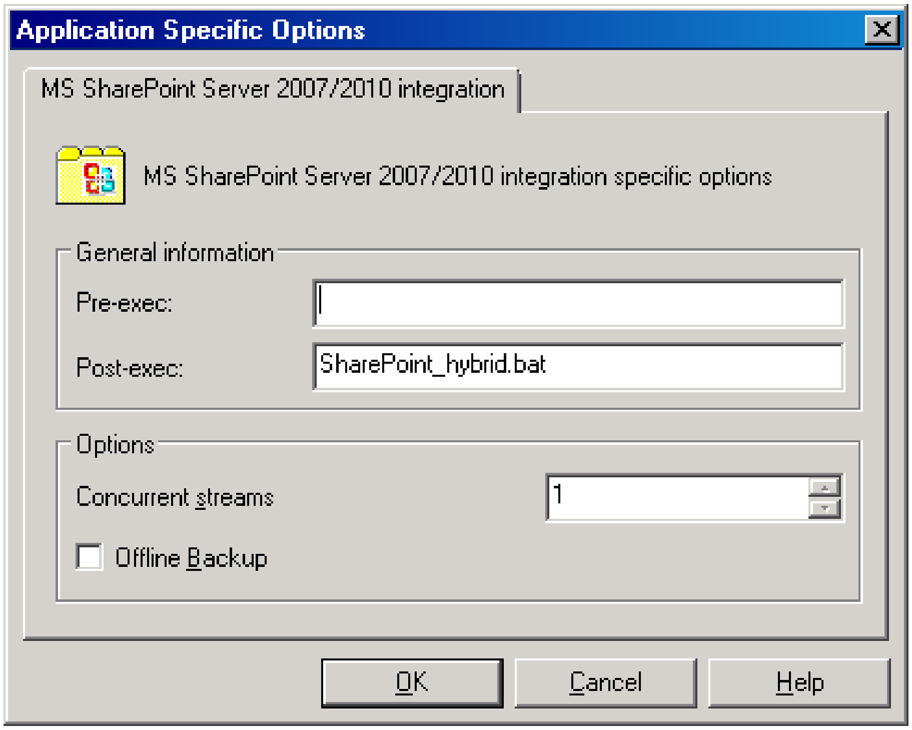
   - Save the batch file `SharePoint_hybrid.bat` in the Data Protector `bin` directory on the entry point client system

Figure 10: Saving the batch file `SharePoint_hybrid.bat` in the Data Protector `bin` directory on the entry point client system



- Specify the Data Protector PowerShell command (saved in the batch file `SharePoint_hybrid.bat`) as the post-exec option in the VDI based integration backup specification

Figure 11: Specifying the Data Protector PowerShell command (saved in the batch file `SharePoint_hybrid.bat`) as the post-exec option in the VDI based integration backup specification


Application Specific Options
MS SharePoint Server 2007/2010 integration
MS SharePoint Server 2007/2010 integration specific options
General information
Options
OK
Cancel
Help

Pre-exec:

Post-exec: SharePoint_hybrid.bat

Concurrent streams: 1

□ Offline Backup

TIP:

If this might be an issue for you to meet your recovery window, use the Windows system scheduler for your backups. See additional instructions in the below NOTE.

IMPORTANT:

If you add a new Web application, a new Microsoft SQL Server system, or you delete a content database, and so on, update the corresponding backup specifications accordingly.

Restore

- Perform a disaster recovery using the VSS based solution. Reinstall the operating system, the Microsoft SharePoint Server 2007/2010 environment and Microsoft SQL Server. Ensure that the new configuration matches the original.
- Perform a restore of Web applications using the VDI based integration. A restore to a new location is possible. For a single item restore (for example, a content database) use the Data Protector Granular Recovery Extension for Microsoft SharePoint Server 2010. For details, see the HP Data Protector Granular Recovery Extension User Guide for Microsoft SharePoint Server.

NOTE
To adhere to your Separation of duties security standards, you can separate tasks as follows:

1. The Data Protector administrator creates the VDI based integration backup specification with the Microsoft SharePoint Server 2007/2010 farm administrator username and Domain name specified, but without its password. Also, the Data Protector administrator schedules the backup specification, assigns needed devices, and adds the Data Protector PowerShell command

   ```
   SharePoint_VSS_backup.ps1 -backuponly
   ```

   as a post-exec option in the VDI based integration backup specification. The -device option is not required.

2. Using the Windows system scheduler, the Microsoft SharePoint Server 2007/2010 farm administrator runs:

   ```
   omnib -mssharepoint_list ListName -barmode -full | diff | incr
   ```

Search service is recoverable without any inconsistency. The crawl fixes any inconsistencies between the content databases and the index.

Troubleshooting

For general Data Protector Microsoft SharePoint Server 2007/2010 integration and the Data Protector Microsoft SharePoint Server 2007/2010 VSS based solution troubleshooting information, see related chapters in the *HP Data Protector integration guide for Microsoft applications*. For ZDB and instant recovery related troubleshooting, see the *HP Data Protector Zero Downtime Backup integration guide*.

For more information

To read more about the Data Protector Microsoft SharePoint Server 2007/2010 integration and the Data Protector Microsoft SharePoint Server 2007/2010 VSS based solution, go to www.hp.com/go/dataprotector

4AA3-4533ENW, Created August 2011