

Data Protection for Microsoft SharePoint Portal Server 2003

**APPLICABLE FOR WINDOWS
SHAREPOINT SERVICES AND
SHAREPOINT PORTAL SERVER
ENVIRONMENTS**

FOR USE WITH BACKUP EXEC *FOR
WINDOW SERVERS* 9.0 & 9.1 AND
MICROSOFT WINDOWS SERVER
2003

TABLE OF CONTENTS

Introduction 3

Data Protection Considerations..... 3

Solution Highlights..... 4

Microsoft Office SharePoint Portal Server 2003 4

 Backup Exec Agent For Microsoft SQL Server..... 5

 Snapshot Backups And Restores 5

 Legacy SharePoint Portal Server 2001 Agent..... 7

Backing Up And Restoring Configuration And Content Databases 7

 Backing Up The Databases 7

 Single Sign-On Services Database..... 8

 Backing Up Legacy SharePoint Portal 2001 Web Stores..... 11

Restoring From A Backup 11

 Database Server 11

 Performing A Redirected Restore 11

 Restoring To The Same Database Server..... 13

 Single Sign-on Services Database 16

 Adding Servers Back To The Farm..... 19

Microsoft Windows SharePoint Services 2.0 19

 Backing Up The Databases 19

 Snapshot Backups And Restores 20

 Database Server 22

 Performing A Redirected Restore 22

 Restoring To The Same Database Server..... 24

 Adding Servers Back To The Farm..... 24

Risks..... 24

Summary 25

INTRODUCTION

The proliferation of corporate documentation, project collaboration and the dependence on Intranet sites led to the development of Microsoft's SharePoint Portal Server 2001. Now, with the release of the second-generation product, SharePoint Portal Server 2003, Microsoft has improved the scalability and flexibility of their document management and collaboration application for Windows servers. It facilitates easy organization, sharing, retrieval and publishing of information over corporate Intranets and seamlessly integrates with Microsoft Office and web development tools.

The focus of this white paper is to provide a detailed review of how to fully protect SharePoint Portal Server version 2003 and Windows SharePoint Services on the Windows Server 2003 platform in conjunction with Backup Exec *for Windows Servers* versions 9.0 and 9.1 utilizing the optional Backup Exec SQL agent in cooperation with other backup features.

The release of SharePoint Portal Server 2003 and Windows SharePoint Services has dramatically changed the product architecture requiring new methods for presenting the data to the user as well as backing up this data. This format is not only different from the previous version of SharePoint but also introduces many complexities in supporting data that is passed freely between servers. The exchange of information between servers in the farm will not only change the way to back up this data but how the data from multiple servers will be presented to a user such that the user can easily select backup and restore methods without having to know the details about their server or the server farms' configuration.

DATA PROTECTION CONSIDERATIONS

Without the proper tools and processes in place, the time-consuming tasks of collaborating, publishing and controlling access to documents within an organization could easily result in data being lost, overwritten, duplicated or misplaced. While SharePoint Portal Server 2003 solves these and other problems, it does not employ the adequate data protection tools that offer reliable disaster recovery, scalability and ease-of-use. Without the proper data protection strategy, an organization is placing its documents and data at risk by deploying and populating SharePoint Portal Server 2003 in an environment where data protection schemes have not been determined and backup and recovery processes have not been defined. It is crucial that organizations research, evaluate and deploy a complete data protection solution for SharePoint Portal Server 2003.

As organizations deploy SharePoint Portal Server 2003, the common question of "*How to effectively protect valuable data stored within SharePoint Portal Server 2003*" will arise. Through the course of this white paper, VERITAS Software will answer this simple, yet crucial question as well as discuss various tools, processes and strategies available to back up, restore and duplicate SharePoint Portal 2003 servers. Each organization must decide, based on size, infrastructure and type of SharePoint Portal Server 2003 deployment, what combination of these tools best fits their environment. Additionally, when determining specific SharePoint Portal Server 2003 data protection needs, organizations need to consider these questions:

- Will backup processes be performed while SharePoint Portal Server 2003 is online or offline?
- Will backup processes be performed from a central location or distributed among multiple servers?
- Will backups be stored on tape media or disk volumes?
- Will backup processes be performed individually or combined with VERITAS File System™ software and other protected resource backups such as Exchange, SQL or Domino?
- How frequently should a backup of SharePoint Portal Server 2003 be performed?
- How can a corrupted or accidentally deleted file be recovered?
- How is protecting a SharePoint Portal 2003 server farm different from a single server installation?
- What tools exist to help automate and simplify SharePoint Portal Server 2003 data protection?
- What steps are involved for quickly and reliably recovering from catastrophic data loss?

SOLUTION HIGHLIGHTS

A series of steps must be executed concurrently with the implementation of Backup Exec *for Windows Servers*, to fully support SharePoint Portal Server 2003. The methods involved in protecting SharePoint Portal Server 2003 will require the use of the Backup Exec Agent for Microsoft SQL Server. We will also clarify the differences between Windows SharePoint Services and SharePoint Portal Server.

This paper is limited to Backup Exec 9.0 and 9.1 and will not be applicable with any future release of Backup Exec. A new Backup Exec Agent for SharePoint Portal Server 2003 is planned for the next release of Backup Exec *for Windows Servers*. Fully automated, this new agent will simplify and ensure that all the necessary components of SharePoint Portal Server 2003 are fully protected and available for restoration and complete disaster recovery.

MICROSOFT OFFICE SHAREPOINT PORTAL SERVER 2003

The typical installation of Microsoft Office SharePoint Portal Server 2003 consists of a Microsoft SQL Server and WEB servers that share data freely, and optionally a Microsoft SharePoint Portal 2001. This data has three forms:

1. Databases
 - Configuration
 - Site
 - Sever (Index)
 - Profile
2. SharePoint Portal Server Web Store
3. Microsoft SharePoint Search

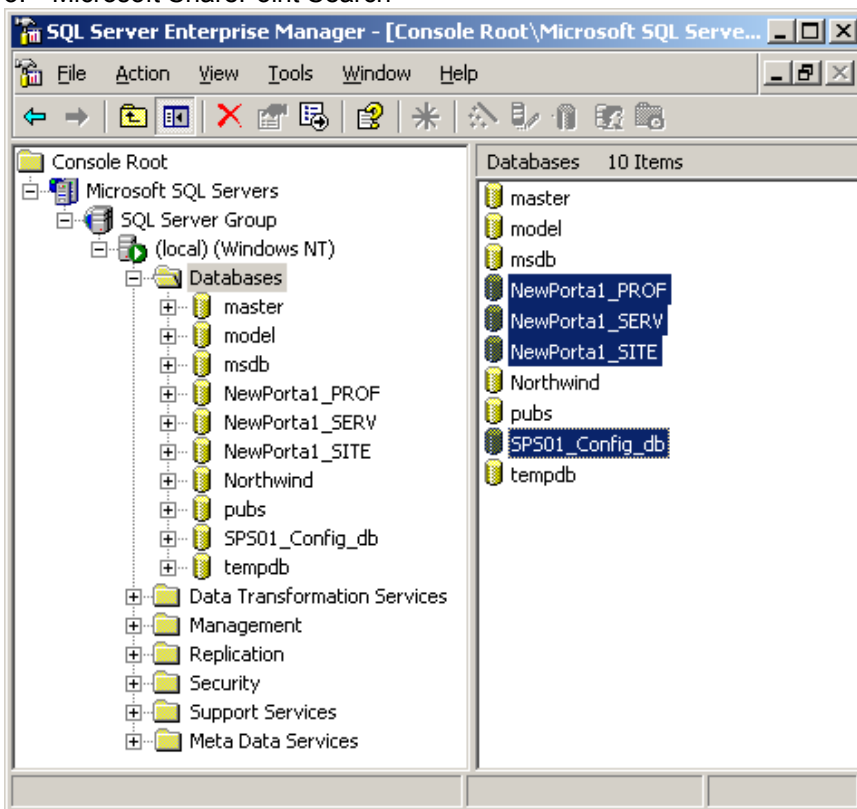


Figure 1: SharePoint Portal Server 2003 database in SQL server.

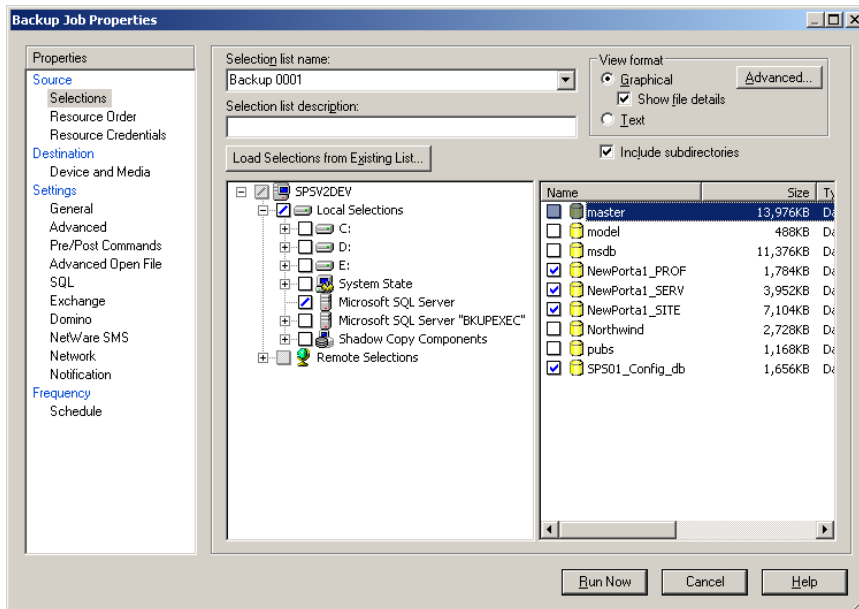


Figure 2: SharePoint Portal Server 2003 databases view in Backup Exec

The SharePoint Portal Server 2003 databases can be protected using the current version of the Backup Exec Agent for SQL Server and this white paper. SharePoint Portal Server 2001 can be protected by the current version of the Backup Exec for Windows Servers SharePoint Portal 2001 Agent.

BACKUP EXEC AGENT FOR MICROSOFT SQL SERVER

The current versions of the Backup Exec 9.0 or 9.1 Agent for SQL Server support several backup and restore methods such as database, differential and log, which can be applied to the SharePoint instance run in Microsoft Office SharePoint Portal Server 2003 implementations.

If the SQL database is MSDE, then the default recovery model is “simple” which allows for database and differential backups only. If the SQL database is on a SQL server 2000 the default recovery model is “Full” which allows for database, differential, and log based backups. If you select log-based backups, you must also select the database configuration for the recovery model setting when applying the various backup methods. This ensures that you will successfully back up the data. This setting can be configured for MSDE or SQL Server 2000 if you have access to Microsoft SQL Server Enterprise Manager.

Note: The SQL server must be configured properly before using this method for transactional backups and restores. This method is supported if Microsoft Office SharePoint Portal Server 2003 is configured with Transaction Log backups.

SNAPSHOT BACKUPS AND RESTORES

Microsoft’s Windows SharePoint Services is available in Windows Server 2003. Since the Windows SharePoint Services data is stored in a SQL instance called SHAREPOINT, as well as SharePoint Portal Server, the Windows SharePoint Services SQL data is protected by the Writer instance of SHAREPOINT in the Backup Exec Shadow Copy Components file system. Therefore, Backup Exec for Windows Servers has the ability to perform snapshot backup and restores of Windows SharePoint Services. This is only if the user does a typical install. If the user does a server farm installation, it could be on any SQL Server.

Although a SQL Agent license is not required to use the SQL Server Writer to protect Windows SharePoint Services on Windows Server 2003, protection is limited to full backup and restores. The individual components can be selected, but other methods of backing up data such as differential or transaction logs are not available.

For more information, see “About the Backup Exec Shadow Copy Components File system” in the VERITAS Backup Exec *for Windows Servers Administrator’s Guide*.

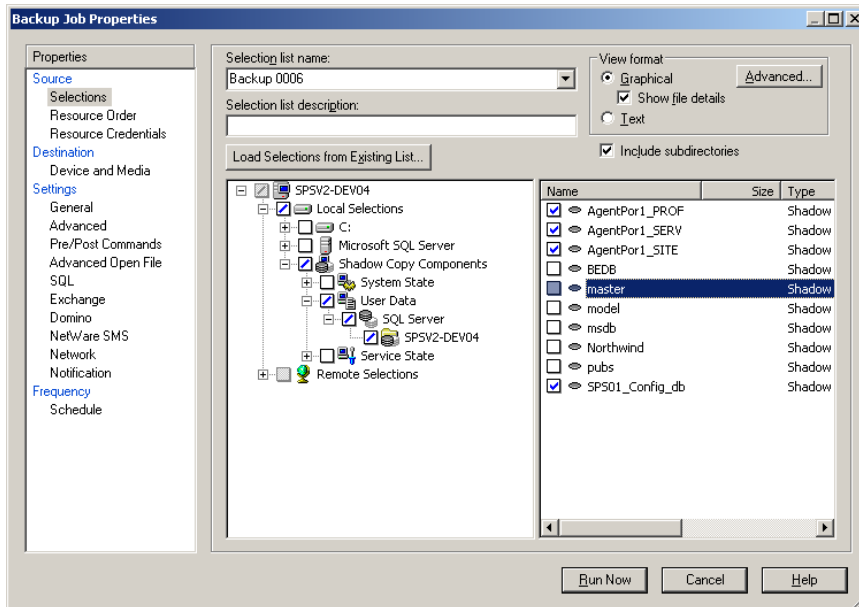


Figure 3: SharePoint Portal Server 2003 database under Shadow copy components for backups.

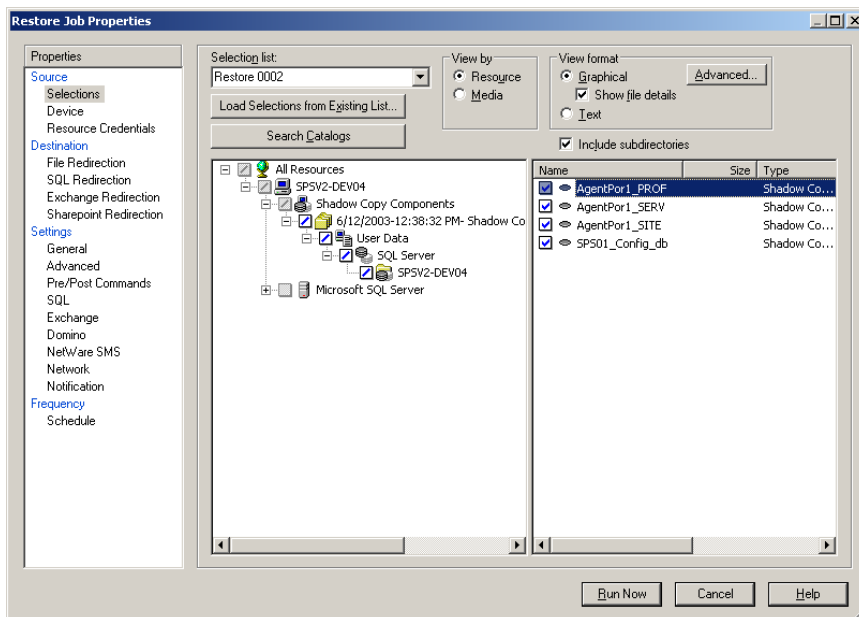


Figure 4: SharePoint Portal Server 2003 database under Shadow copy components for Restore.

LEGACY SHAREPOINT PORTAL SERVER 2001 AGENT

Because of changes in Microsoft Office SharePoint Portal Server 2003, the SharePoint Agent shipped with Backup Exec *for Windows Servers* 9.0 and 9.1 is not able to protect the server farm's data. However, the SharePoint Agent 2001 can be used to back up legacy document stores. These stores are supported by Microsoft Office SharePoint Portal Server 2003 for backwards compatibility. The SharePoint Portal 2001 stores can then be protected using the Backup Exec *for Windows Servers* 9.0 and 9.1 agents. The backup support for the SharePoint Agent 2001 is only for SharePoint Portal 2001 stores, not any store updated or migrated to Microsoft Office SharePoint Portal Server 2003. For more information about SharePoint Portal Server 2001 agent, see "VERITAS Backup Exec - Agent for Microsoft SharePoint Portal Server" in the VERITAS Backup Exec *for Windows Servers* Administrator's Guide.

BACKING UP AND RESTORING CONFIGURATION AND CONTENT DATABASES

In Microsoft Office SharePoint Portal Server 2003, all server and site configuration information is stored in the configuration database, and all site content is stored in content databases. If you want to back up all the Microsoft Office SharePoint Portal Server 2003 information on your server or server farm, you must back up these databases with the Backup Exec Agent for SQL Server.

BACKING UP THE DATABASES

The databases for Microsoft Office SharePoint Portal Server 2003 are usually created in either the default instance or a SharePoint specific instance. The database names are usually the first eight characters of the portal name with no spaces, an increment value, and concatenated with _PROF, _SITE, or _SERV. For example, a database named *Portal Name* is *PortalNaX_YYYY* where *PortalNa* is the first eight characters of the portal name, *X* is a number that is incremented if the first eight characters are the same, and *Y* is the type of database created.

For example, the Team Portal name will have the following databases created:

```
TeamPort1_PROF
TeamPort1_SITE
TeamPort1_SERV
```

The configuration database name is determined after the Microsoft Office SharePoint Portal Server 2003 is installed; the default is SPS01_Config_db. For more information, see your system administrator or SharePoint documentation.

Follow these steps when you back up Microsoft Office SharePoint Portal Server 2003 so that the database will be in sync. The following examples use Team Portal as the portal name.

- The Site and Profile database must be backed up and restored together.

For example, the following databases must be backed up together.

```
TeamPort1_PROF
TeamPort1_SITE
```

- To back up and restore a site, the Site, Profile, and Server databases must be backed up and restored.

For example, the following databases must be backed up and restored.

```
TeamPort1_PROF
TeamPort1_SITE
TeamPort1_SERV
```

- The Site database must exist or be restored prior to back up or restore of a Profile database. For example, the following databases must be backed up and restored.
TeamPort1_PROF
TeamPort1_SITE
- If all databases are restored, then the Microsoft Office SharePoint Portal Server 2003 server or farm will be restored to same state that it was in when it was backed up. This is due to the restore of the configuration database. However, problems may result if the configuration database is restored individually without the other databases. If configuration information is lost, the Microsoft Office SharePoint Portal Server 2003 farm or server may be compromised which may result in data loss. To ensure that the Microsoft Office SharePoint Portal Server 2003 server or farm can be restored in its entirety, you must include the configuration database when you back up all the databases.

For example, the following databases must be backed up to ensure a complete restore of the configuration database.

TeamPort1_PROF
TeamPort1_SITE
TeamPort1_SERV
SPS01_Config_db

IMPORTANT: This is a potential pitfall. Restoring this way will only be of use if nothing else on the farm has changed such as server names. The configuration database holds all of the topology information. If you restore the configuration database and the topology changed then it will not be valid anymore. In that case you would be better off creating a new configuration database and restructuring the topology.

You can use the Backup Exec *for Windows Servers* Agent for SQL Server to back up these databases. Ensure that you back up both the configuration database and all of the content databases used by Windows SharePoint Services. For more information about the SQL Agent, see “VERITAS Backup Exec - Agent for Microsoft SQL Server” in the VERITAS Backup Exec *for Windows Servers* Administrator’s Guide.

SINGLE SIGN-ON SERVICES DATABASE

If the Microsoft SharePoint Portal Farm uses Single Sign-On Services then that database as well as the Manage encryption key must be backed up. The database can be backed up using the SQL agent. The manage encryption key must be backed up through the SharePoint Portal Server Central Administrator page.

The Single Sign-On services database is given the name SSO by default. The database is backed up using the Agent for SQL Server.

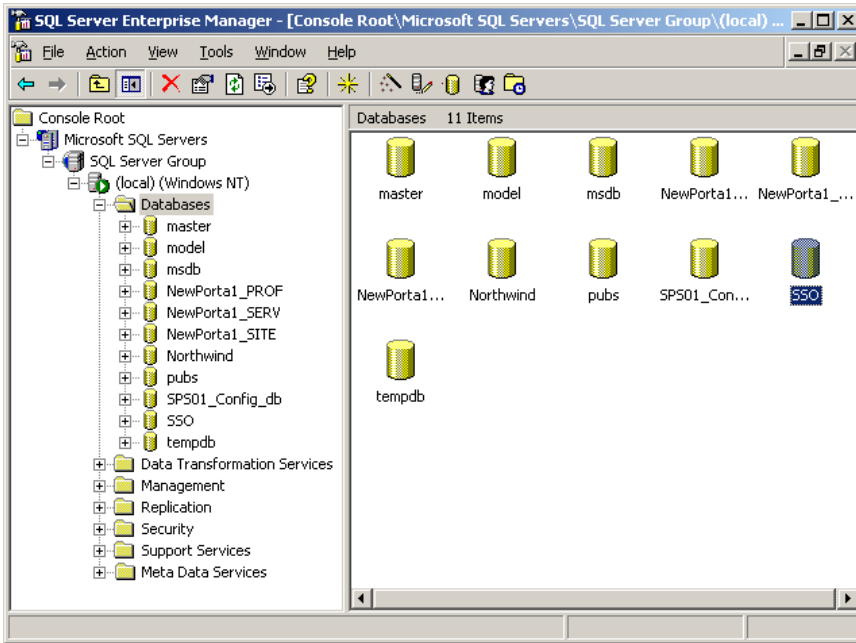


Figure 5: Single Sign-On services database in Microsoft SQL Server Enterprise Manager.

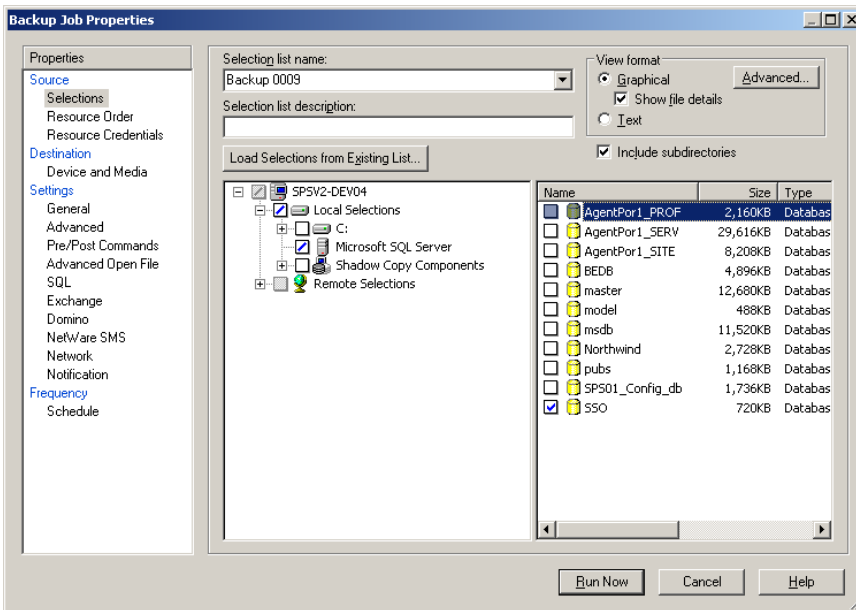


Figure 6: Single Sign-On database in Backup Exec.

The database can also be backed up with Shadow Copy Components.

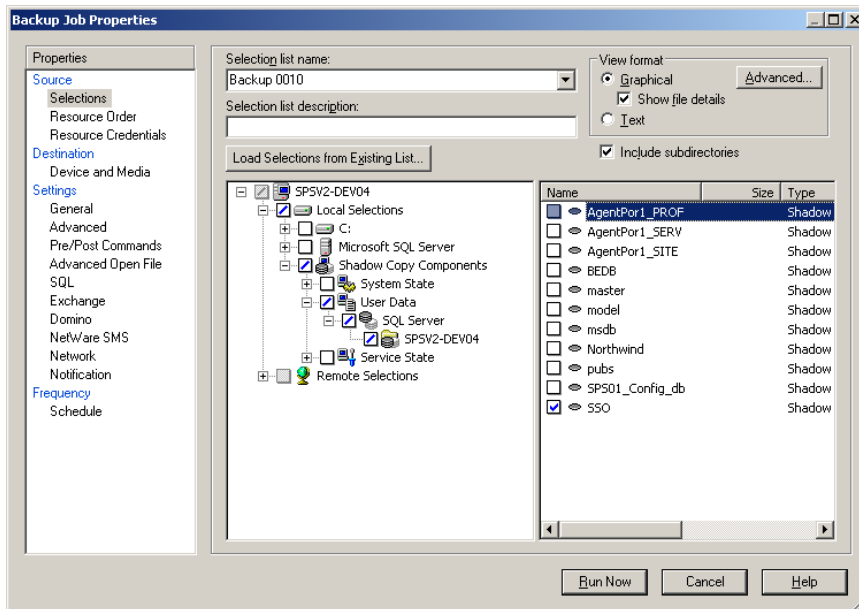


Figure 7: Single Sign-On database in Backup Exec using Shadow Copy Components.

To back up the Manage encryption key you must go to the **SharePoint Portal Server Central Administration** page and click on **Manage Settings for Single Sign-On**. Once the Manage Settings for Single Sign-On page opens, select the **Manage Encryption Key** link, a page will be displayed that allows the user to perform operations on the encryption key.

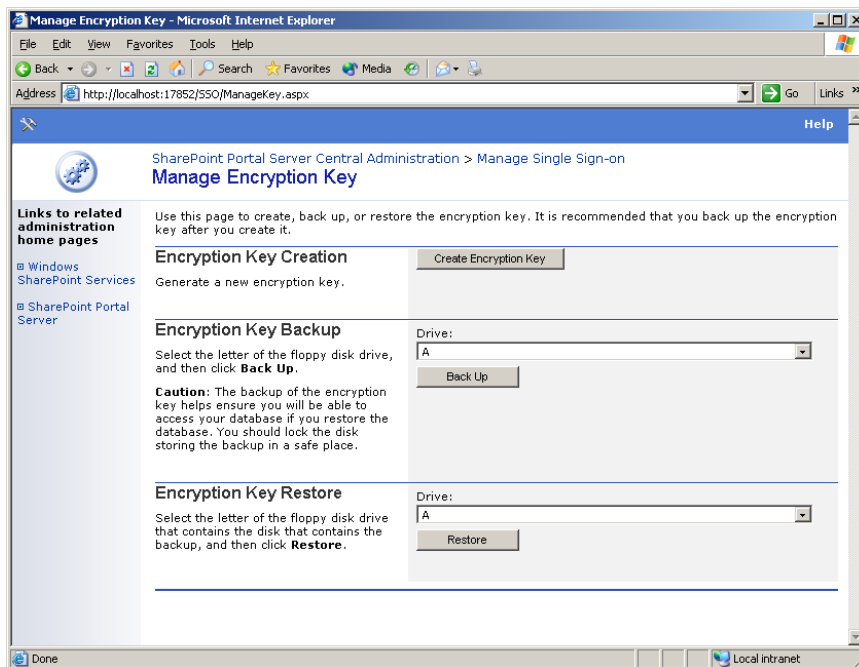


Figure 8: Encryption Key management in SharePoint Portal Server Central Administration.

On this page you will be able to select the place to store the Manage encryption key that goes with that Single Sign-On services database.

With the database backed up and the Manage encryption key saved, the data is now protected.

BACKING UP LEGACY SHAREPOINT PORTAL 2001 WEB STORES

Use the Agent for SharePoint Portal Server 2001 to ensure back up of legacy SharePoint Portal 2001 Web Stores. For more information about the Agent for SharePoint Portal Server 2001, see “VERITAS Backup Exec - Agent for Microsoft SharePoint Portal Server” in the VERITAS Backup Exec *for Windows Servers Administrator’s Guide*.

RESTORING FROM A BACKUP

DATABASE SERVER

There are two ways that you can restore the SQL database server components. You can redirect the databases to another SQL server (see “Performing a Redirected Restore”) or restore to the same server from which the data was backed up (see “Restoring to the Same Database Server”).

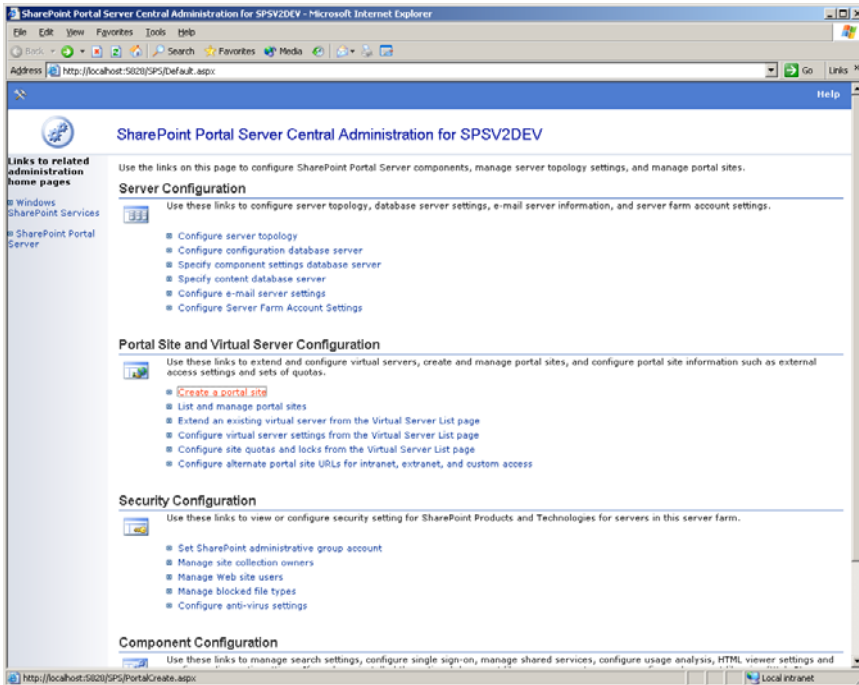
PERFORMING A REDIRECTED RESTORE

When you perform a redirected restore to the same server, you must rename the databases. You can only rename one database at a time. After this is completed, the data is restored; however, the servers need to be reconnected.

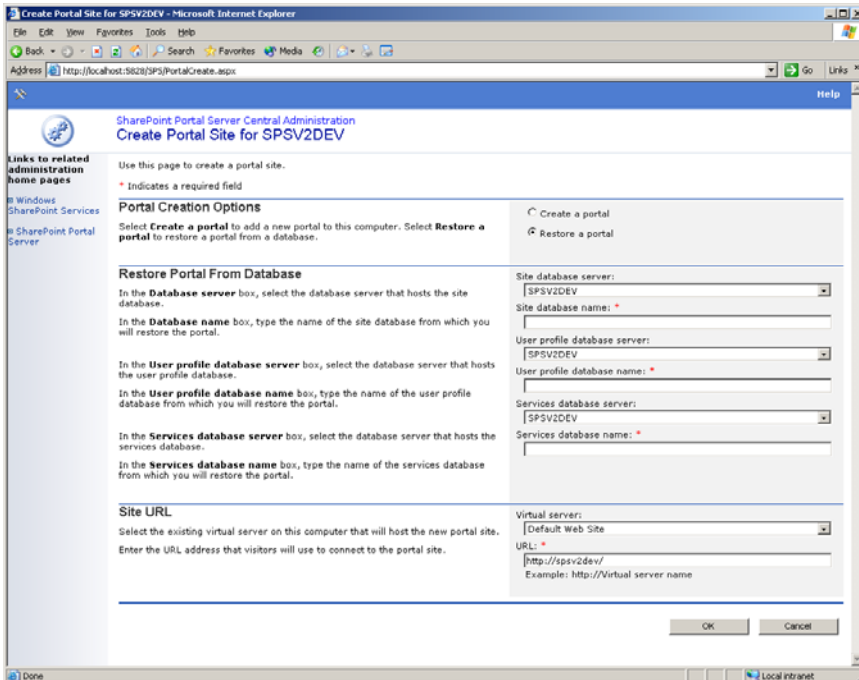
Depending on the role of the server, you must ensure that the server detects that a restore of the data was performed and the local cache on the server is refreshed. For more information about adding individual servers to the farm, see “Backing Up and Restoring Servers on the Server Farm” in the Microsoft Office SharePoint Portal Server 2003 Administrator’s Guide.

If a restore of the portal is required after the database has been restored, perform the following steps from the new Microsoft SharePoint Portal Server 2003 server.

1. Go to SharePoint Portal Server Central Administration page.
2. Click **Create a portal site**.



3. Select Restore a Portal.



- Add the database names to the edit controls.
- Complete the rest of the required information and click **OK**.
- Follow the instructions for the following pages.

RESTORING TO THE SAME DATABASE SERVER

Running regular backup jobs of your servers and sites enable you to restore them in case there is a failure. Perform the following steps to restore a server or server farm from a database backup.

1. From your server or the web front-end servers in your server farm, create the virtual servers to host your web site content in Internet Information Services (IIS).
2. Using the Agent for SQL Server, restore the databases from the backups.

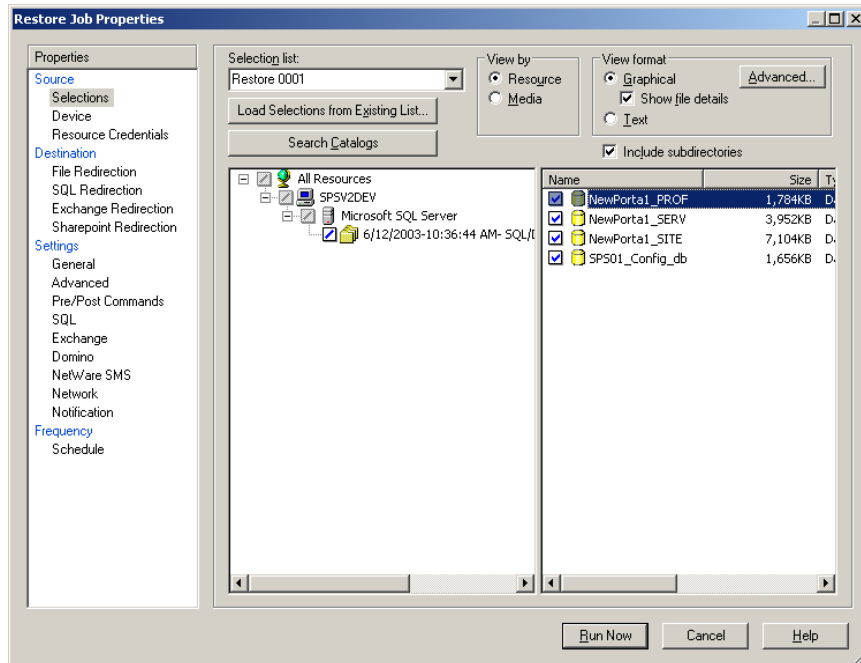


Figure 9: Microsoft Office SharePoint Portal Server 2003 database to be restored

3. In IIS, create the application pools for the content virtual servers. Use original accounts for the application pools and these pools must be members of the Security Administrators and Database Creators roles in SQL Server.
4. From your server or the web front-end servers in your server farm, install Microsoft Office SharePoint Portal Server 2003 and connect to the restore configuration database. When Microsoft Office SharePoint Portal Server 2003 is installed and you connect to an existing configuration database, the included and excluded paths for your server or server farm are automatically recreated.

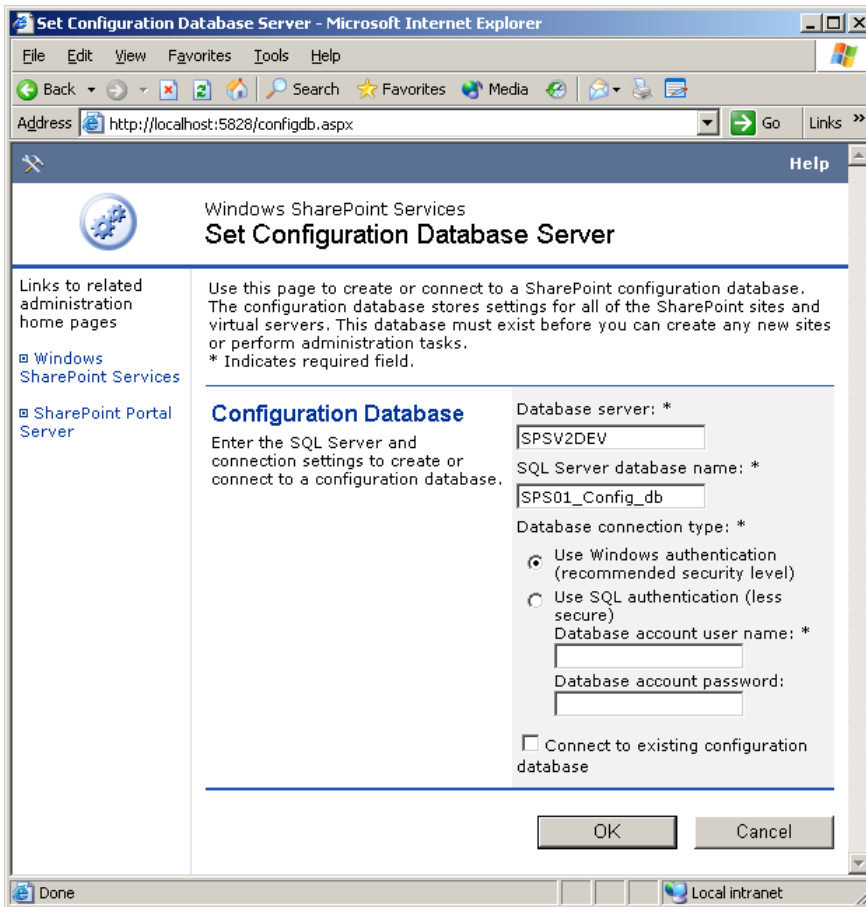


Figure 10: Microsoft Office SharePoint Portal Server 2003 Set Configuration Database Server Page.

5. From the SharePoint Central Administration page, select **Set default content database server** to set the default content database server to the restored database server.

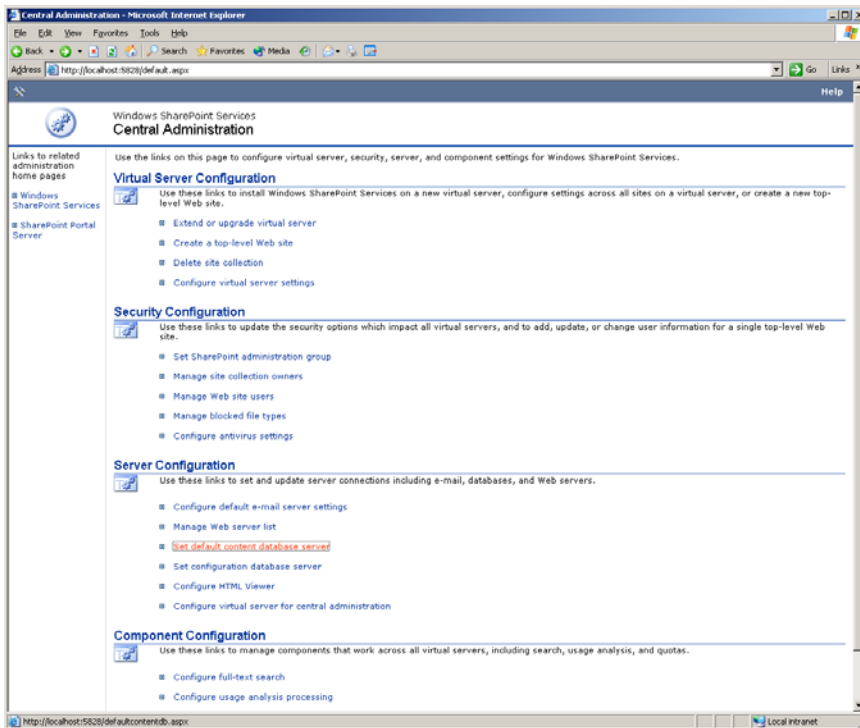


Figure 11: SharePoint Central Administration Page.

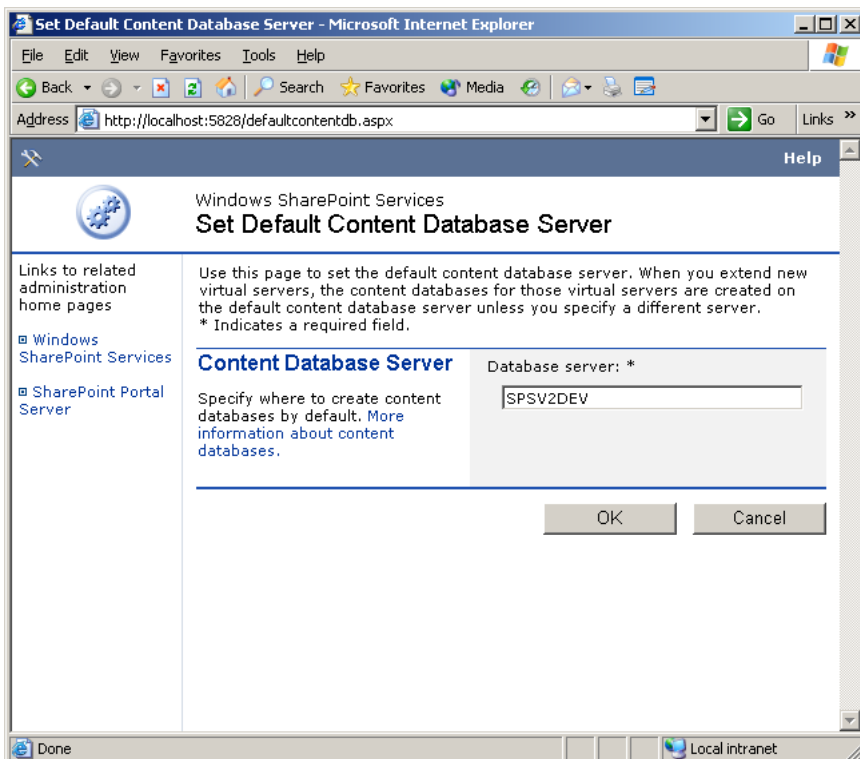


Figure 12: Set default content database server page.

- From the **Extend Virtual Server** page, select **Extend and map to another virtual server** to extend each virtual server. This option enables you to connect a new virtual server to a restore content database. Repeat this step for each new virtual server.

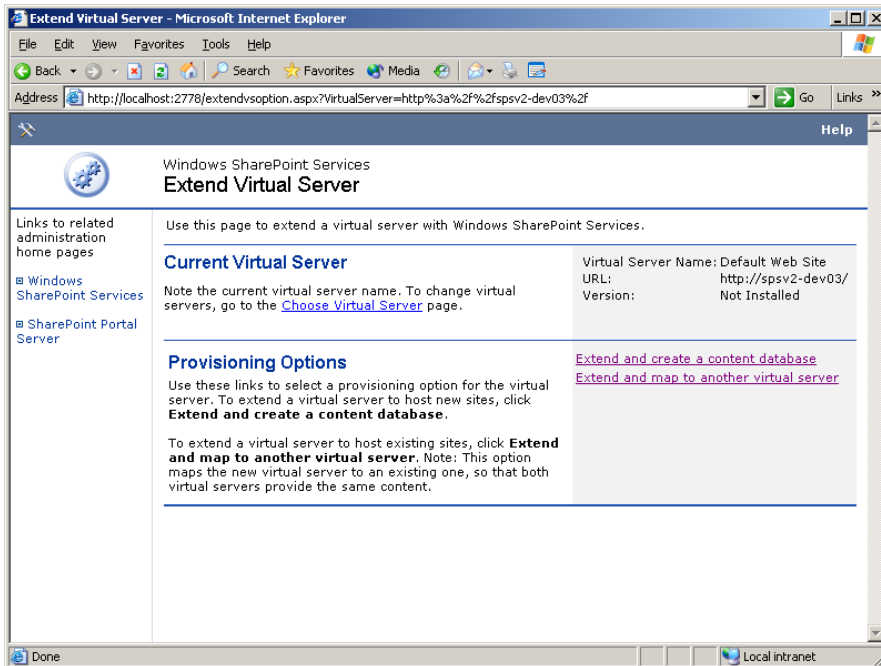


Figure 13: Extend and map to another virtual server.

- Use the **Manage Content Databases** page in SharePoint Central Administration to add additional content databases that have been restored to a virtual server. Repeat this step for each virtual server.

By reconnecting the content databases to the virtual servers, the web sites contained in the list of included paths for the virtual server are restored for those content databases.

SINGLE SIGN-ON SERVICES DATABASE

If the Microsoft SharePoint Portal Farm uses Single Sign-On Services then that database as well as the Manage encryption key must be restored. The database can be restored using the Agent for SQL Server. The manage encryption key must be backed up through the SharePoint Portal Server Central Administrator page.

The Single Sign-On services database is given the name SSO by default. The name can be configured at Single Sign-On services setup time. The database is backed up using the Agent for SQL Server.

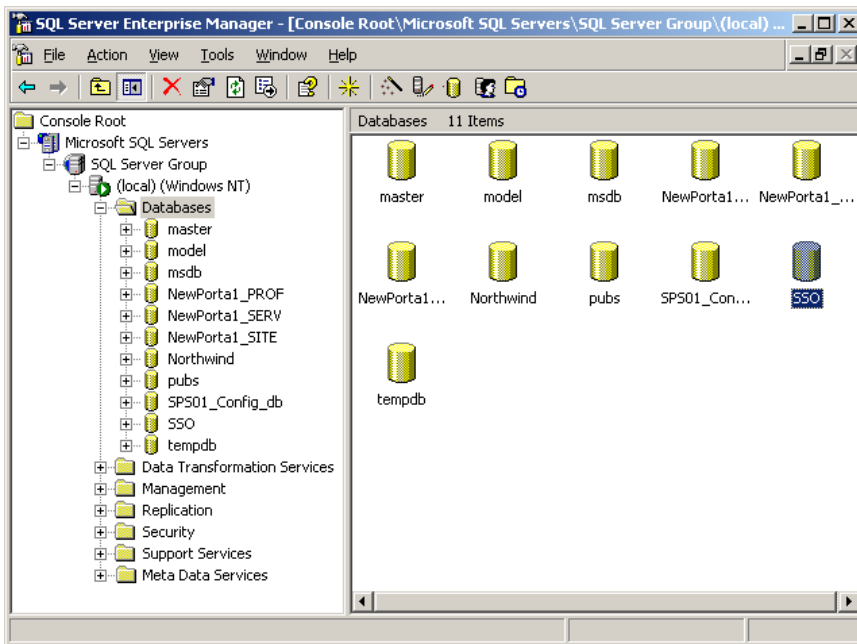


Figure 14: Single Sign-On services database in Microsoft SQL Server Enterprise Manager.

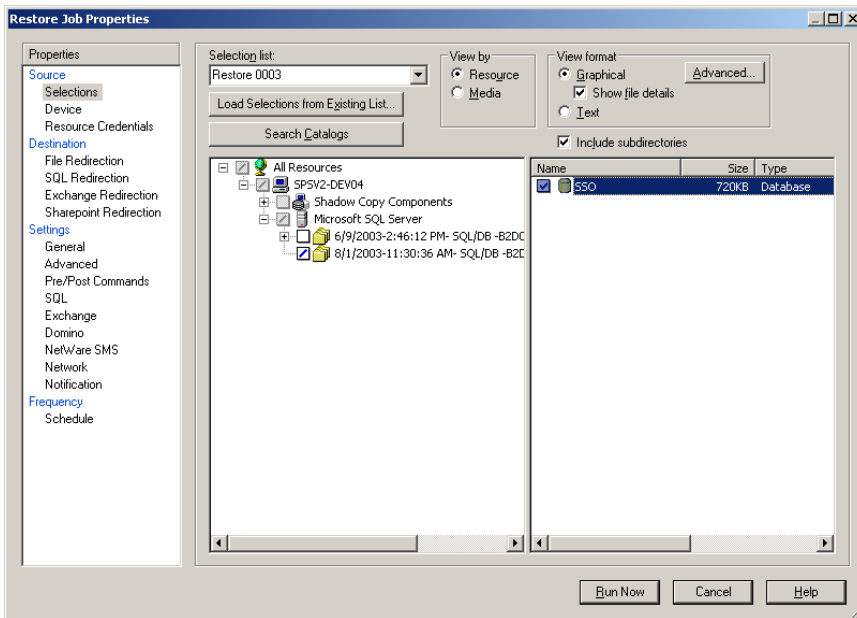


Figure 15: Restore view of Single Sign-On database in Backup Exec.

The database can be restored using Shadow Copy Components if the Single Sign-On database was backed up using that method.

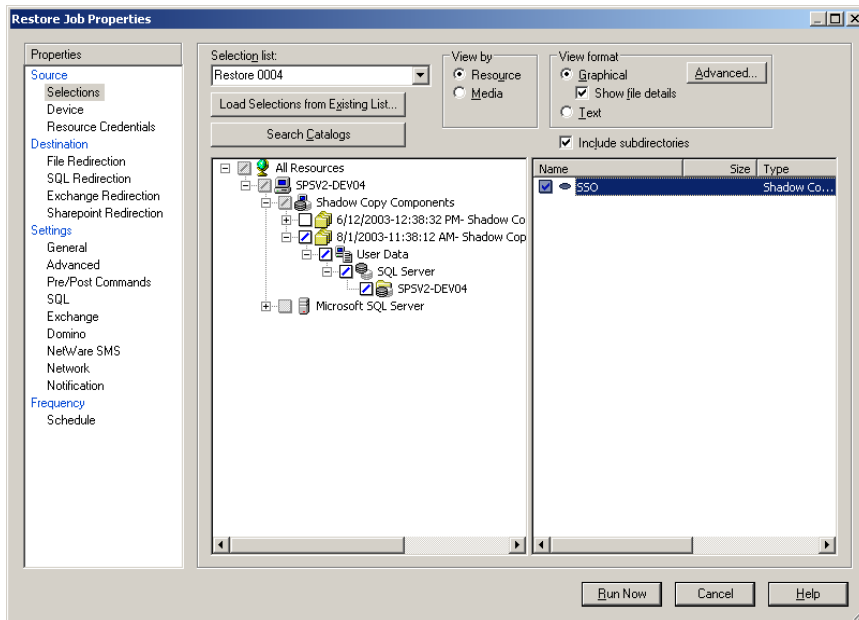


Figure 16: Restore view of Single Sign-On database in Backup Exec under Shadow Copy Components.

To restore the Manage encryption key you must go to the **SharePoint Portal Server Central Administration** page and click on **Manage Settings for Single Sign-On**. Once the Manage Settings for Single Sign-On page opens select the **Manage Encryption Key** link, a page will be displayed that allows the user to perform operations on the encryption key.

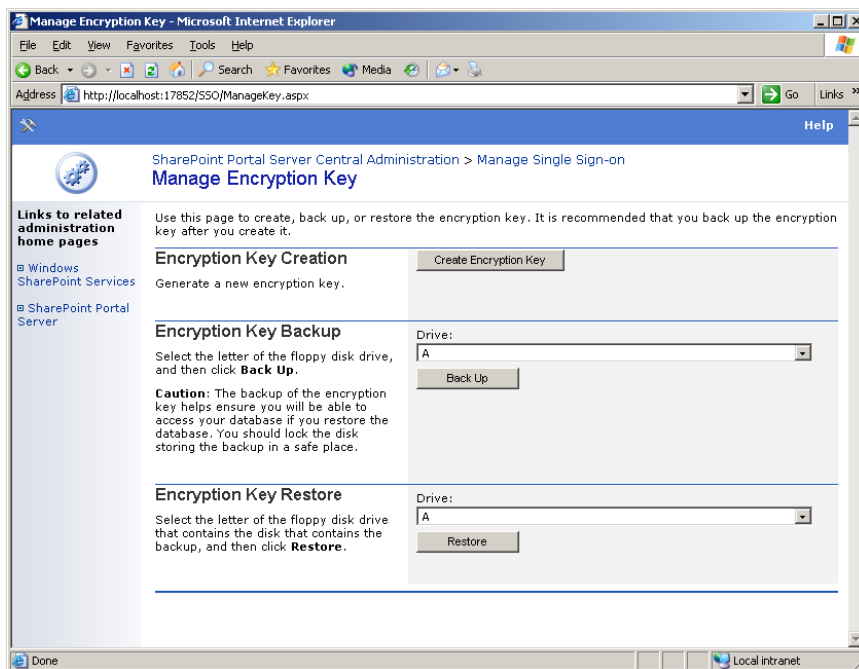


Figure 17: Encryption Key management in SharePoint Portal Server Central Administration.

On this page you will be able to select the place to restore the Manage encryption key that goes with the Single Sign-On services database.

With the Single Sign-On database and the Manage encryption key restore the Single Sign-On services will be functional.

ADDING SERVERS BACK TO THE FARM

In the event a server becomes corrupted, the servers can be added back to the farm with or without the same name. If disaster recovery preparation has been completed on the server and there is a complete backup of the server, the compromised sever can be recovered and the SharePoint farm will not need any additional reconfiguration. If the server is new, restore the database and add the server back to the farm. For more information about adding individual servers to the farm, see “Backing Up and Restoring Servers on the Server Farm” in the Microsoft Office SharePoint Portal Server 2003 Administrator’s Guide documentation.

When you have completed these steps, the restore job is complete. All sites included in your backup should be functioning again with the complete site content, users, and settings.

MICROSOFT WINDOWS SHAREPOINT SERVICES 2.0

In Microsoft Windows SharePoint Services 2.0, all server and site configuration information is stored in the configuration database, and all site content is stored in content databases. If you want to back up all the Microsoft Windows SharePoint Services 2.0 information on your server or server farm, you must back up these databases with the Agent for SQL Server.

BACKING UP THE DATABASES

The databases for Microsoft Windows SharePoint Services 2.0 are usually created in either the default instance or a SharePoint specific instance. The database name is usually STS_ followed by the server name and an underscore and increment value.

For example, a server named *Test* will have the following database name:

STS_Test_1

The configuration database is named when you install Microsoft Windows SharePoint Services 2.0. For more information, see the Microsoft Windows SharePoint Services 2.0 Administrator’s Guide. The default is STS_Config.

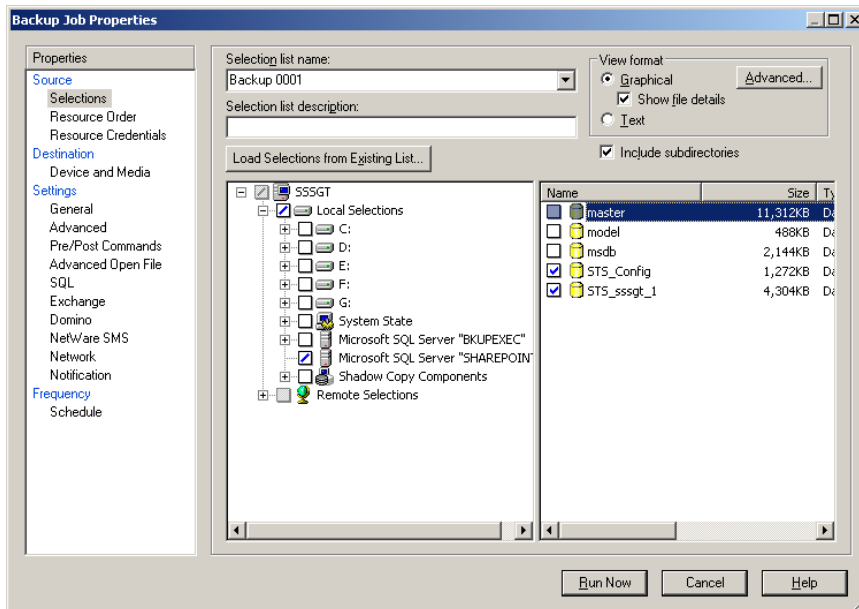


Figure 18: Microsoft Windows SharePoint Services 2.0 databases.

You must use the SQL Agent to back up these databases. Ensure that you back up both the configuration database and all of the content databases used by Microsoft Windows SharePoint Services 2.0. For more information about backing up databases with the SQL Agent, see the VERITAS Backup Exec for Windows Servers Administrator's Guide.

If the SQL database is MSDE then the default recovery model is "simple". This setting in MSDE only allows for database and differential backups. If the SQL database is on a SQL server 2000 the default recovery model is "Full". This setting in SQL Server 2000 allows for database, differential, and log based backups. If log based backups are selected, you must select the database configuration for the recovery model setting when applying the various backup methods to ensure a successful backup of the data. You can configure these settings in MSDE or SQL server 2000 if you have access to Microsoft SQL Server Enterprise Manager.

Note: The SQL server must be to be configured properly before using this method for transactional backups and restores. This method is supported if SharePoint Version 2 is configured with Transaction Log backups.

SNAPSHOT BACKUPS AND RESTORES

Microsoft's Windows SharePoint Services will be available in Windows Server 2003. Since the Windows SharePoint Services data is stored in a SQL instance called SHAREPOINT, as well as SharePoint Portal Server, the Windows SharePoint Services SQL data is protected by the Writer instance of SHAREPOINT in the Backup Exec Shadow Copy Components file system. Therefore, Backup Exec for Windows Servers has the ability to perform snapshot backup and restores of Windows SharePoint Services.

Although a SQL Agent license is not required to use the SQL Server Writer to protect Windows SharePoint Services on Windows Server 2003, protection is limited to full backup and restores. The individual components can be selected, but other methods of backing up data such as differential or transaction logs are not offered.

For more information, see “About the Backup Exec Shadow Copy Components File system” in the VERITAS Backup Exec for Windows Servers Administrator’s Guide.

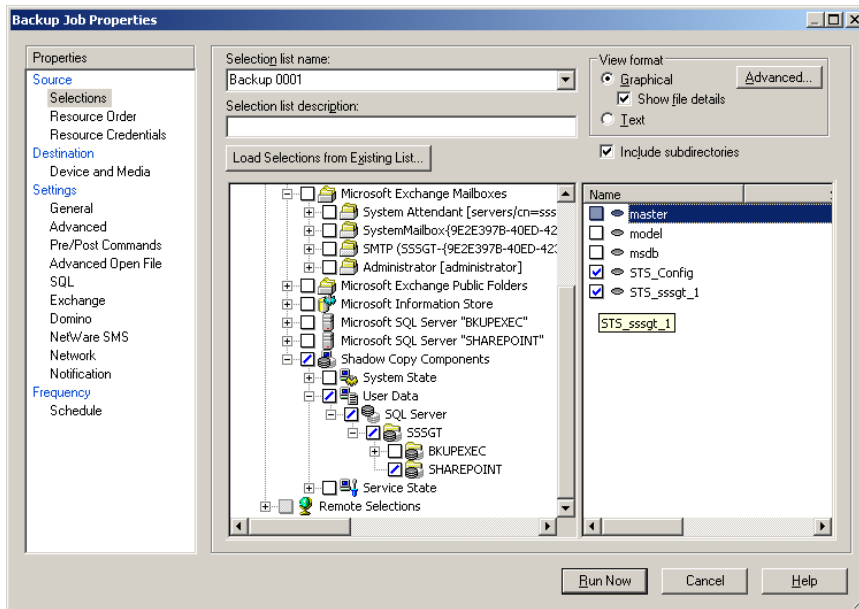


Figure 19: SharePoint database under Shadow copy components for backups.

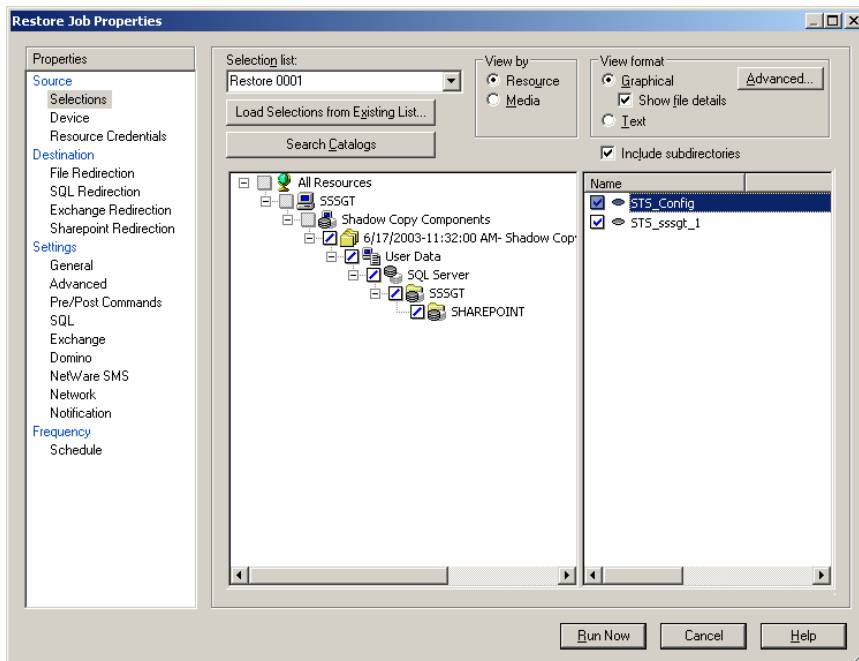


Figure 20: SharePoint database under Shadow copy components for Restore.

DATABASE SERVER

There are two ways that you can restore the SQL database server components. You can redirect the databases to another SQL server (see “Performing a Redirected Restore”) or restore to the same server from which the data was backed up (see “Restoring to the Same Database Server”).

PERFORMING A REDIRECTED RESTORE

When you perform a redirected restore to the same server, you must rename the databases. You can only rename one database at a time. After this is completed, the data is restored; however, the servers need to be reconnected.

Depending on the role of the server, you must ensure that the server detects that a restore of the data was performed and the local cache on the server is refreshed. For more information about the proper way to add individual servers to the farm, see “Backing Up and Restoring Servers on the Server Farm” in the Microsoft Office SharePoint Portal Server 2003 Administrator’s Guide.

To restore a web server after you restore the database, perform the following from the new Microsoft Windows SharePoint Services 2.0 server.

1. Restore the database.

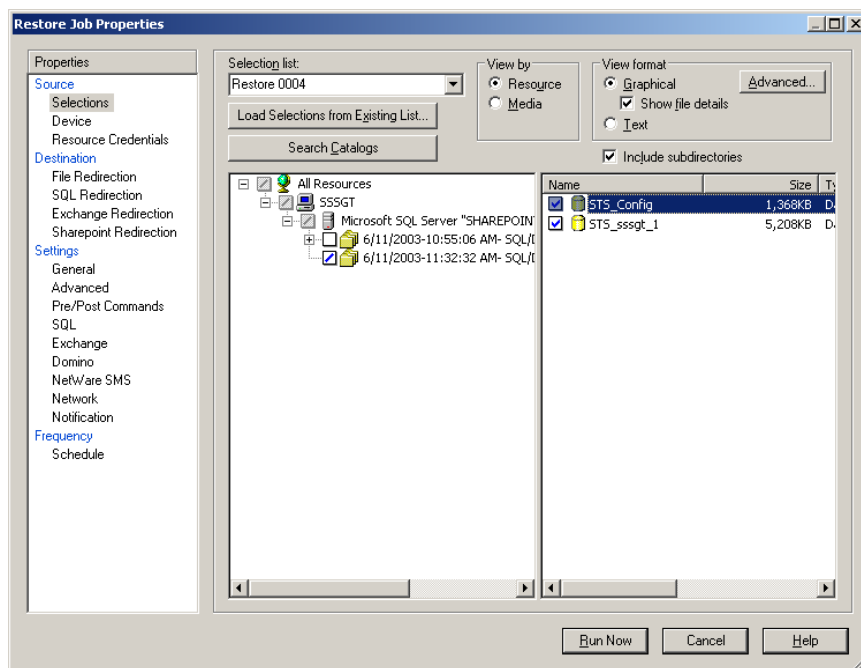


Figure 21: Microsoft Windows SharePoint Services 2.0 databases in Backup Exec for Windows Servers.

2. Navigate to the SharePoint Central Administration Page.

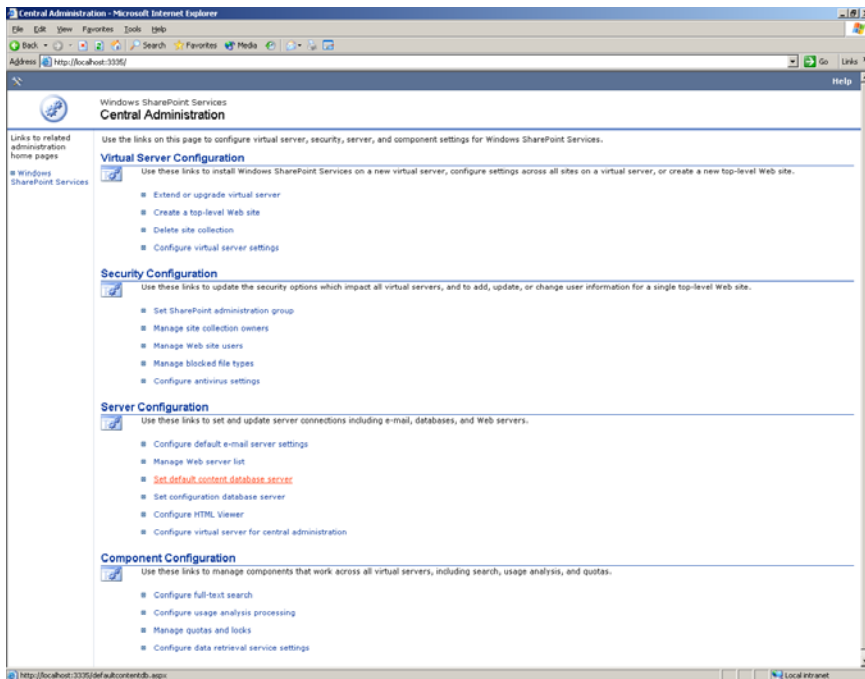


Figure 22: Microsoft Windows SharePoint Services 2.0 Central Administration Page.

3. Select **Set Configuration Database Server**.

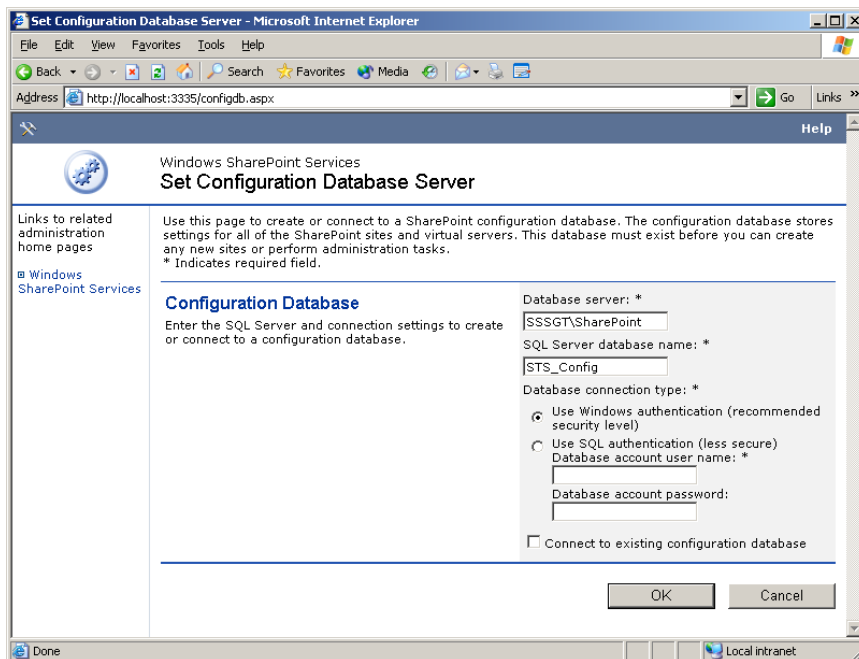


Figure 23: Microsoft Windows SharePoint Services 2.0 Set Configuration Database Server Page.

4. Select **Set Default Content Database Server**.

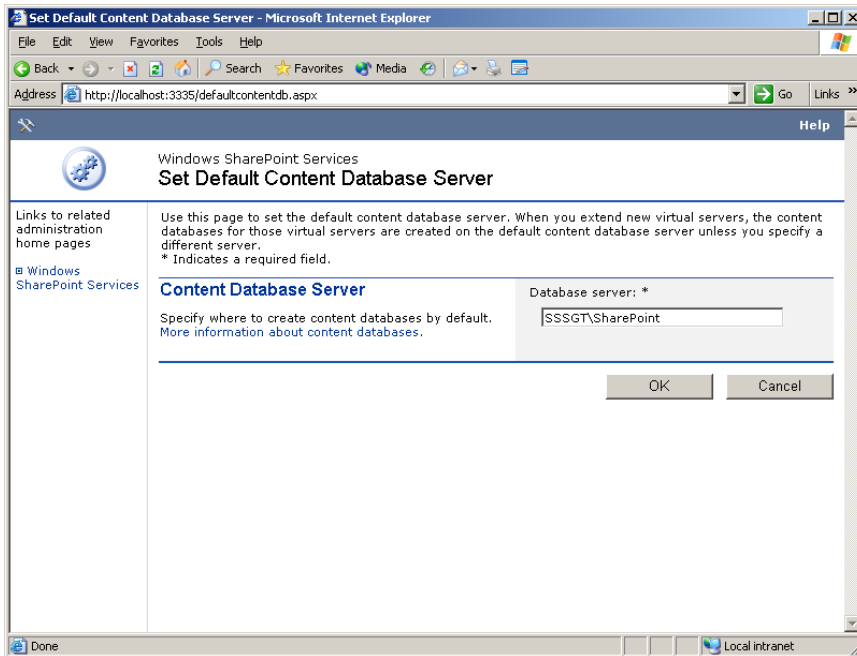


Figure 24: Microsoft Windows SharePoint Services 2.0 Set Default Content Database Server Page.

5. Open the site and navigate to the restored site.

RESTORING TO THE SAME DATABASE SERVER

To restore a server or server farm from a database backup, restore the databases and reconnect the content databases to the virtual servers. The web sites contained in the list of included paths for the virtual server are restored for those content databases.

ADDING SERVERS BACK TO THE FARM

In the event a server becomes corrupted, the servers can be added back to the farm with or without the same name. If disaster recovery preparation has been completed on the server and there is a complete backup of the server, the compromised sever can be recovered and the SharePoint farm will not need any additional reconfiguration. If the server is new, restore the database and add the server back to the farm. For more information about adding individual servers to the farm, see “Backing Up and Restoring Servers on the Server Farm” in the Microsoft Office SharePoint Portal Server 2003 Administrator’s Guide documentation.

When you have completed these steps, the restore is complete and all sites included in the backup job should be functioning again with the complete site content, users, and settings.

RISKS

Restoring multiple databases during the SQL redirection process is possible if you restore all the databases to a separate SQL server. If you restore to the same SQL server using redirection, each of the databases must be renamed and restored individually using Backup Exec.

There is also the possibility of the index information from search server being lost. This lost data may occur if the Microsoft SharePoint database is not backed up; however, the information is rebuilt after a period of time.

There is no current support for document level backups for SharePoint Portal Server Version 2 using the Backup Exec *for Windows Servers* version 9.0 and 9.1 Agent for SharePoint Portal Server 2001. The SharePoint database instance that displays in the selections is for the database backups only, if a current license for the Agent for SQL Server has been provided. If Snapshot options are available in Windows Server 2003, the Snapshot provider only supports SharePoint Team Servers and has limited backup and restore options. These limited options are based on the Snapshot provider implementation and not on the options available in Backup Exec. To obtain the most functionality, it is recommended that a license for SQL Agent be purchased, and then the procedures in this document followed.

SUMMARY

The Backup Exec *for Windows Servers* version 9.0 and 9.1 does not directly support Microsoft Office SharePoint Portal Server 2003. The Backup Exec Agent for SharePoint Portal Server 2001 only supports SharePoint Portal Server 2001. However, leveraging the Backup Exec Agent for SQL Server and the Advanced Open File option in conjunction with the recommended procedures for protecting the SharePoint Portal Server 2003 and SharePoint Services configurations will fully protect your Microsoft Office SharePoint environment. The Agent for SQL Server protects the data in the farm and enables you to back up and restore the data. Future releases of Backup Exec *for Windows Servers*, will support the SharePoint Portal Server 2003 implementation directly, and will automate the procedures outlined in this document.