

Data Protection for Microsoft SharePoint Portal Server 2003

VERITAS Backup Exec™ 10 for Windows Servers

Agent for Microsoft SharePoint Portal Server

Applicable for Windows Sharepoint Portal Server Environments
For Use with Backup Exec 10 *for Windows Servers* and Microsoft
Windows Server 2003

TABLE OF CONTENTS

Executive Summary	3
Product Highlights	3
How it works	4
Conceptual Overview	4
Data-Protection Planning	5
Backup Exec 10 Configuration.....	5
Backup Exec 10 Media Server	5
Backup Exec 10 Media Sets.....	5
Backup Exec 10 Remote Agent.....	5
Configuring Intelligent Disaster Recovery for Targeted Servers	6
Reusing Selection Lists, Policies, and Jobs	6
Monitoring and Reporting	6
Backing Up And Restoring SharePoint Configuration And Content Databases	9
Backing Up The Databases	9
Single Sign-On Services Database.....	10
Legacy SharePoint Portal Server 2001 Agent	10
Restoring From A Backup	11
Database Server	11
Performing A Redirected Restore	11
Restoring To The Same Database Server.....	11
Disaster Recovery	11
Single Sign-on Services Database	13
Summary	13

EXECUTIVE SUMMARY

SharePoint Portal Server (SPS) 2003 offers a second-generation document management, project collaboration and intranet site management tool with improved scalability and flexibility 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.

This white paper provides a detailed review of how to fully protect SharePoint Portal Server version 2003 and Windows SharePoint Services on the Windows Server 2003 platform using Backup Exec 10 *for Windows Servers* version and the optional Backup Exec SPS agent.

The release of SharePoint Portal Server 2003 and Windows SharePoint Services has dramatically changed the product's architecture, requiring new methods for presenting the data to the user as well as for 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 how you back up this data but how the user goes about selecting backup and restore methods without having to know the details about the server's or server farms' configuration.

KEY BENEFITS

- Supports Microsoft SharePoint Portal Server 2003 and Serer Farm
- Fully automated
- Simplifies and ensures that all the necessary components of SharePoint Portal Server 2003 are fully protected and available for restoration and complete disaster recovery

PRODUCT HIGHLIGHTS

The new Backup Exec SharePoint Portal Server agent automates the many steps required to fully protect your SPS environment. The methods involved in protecting SharePoint Portal Server 2003 require the use of the Backup Exec Media Server and the SPS agent, which includes the necessary remote agent for a single server or small server-farm configuration.

This agent supports backup and restore of SQL databases, document libraries, index databases, and some additional metadata. The SPS 2003 agent lets administrators scale a single-server SharePoint Portal Environment to large server farm environments. The use of server farms lets an administrator break out the various components of a SPS configuration to many servers in an enterprise. (Each server is a component of a server farm.) The SPS agent also lets administrators browse the farm independent from the rest of the servers in the enterprise.

HOW IT WORKS

CONCEPTUAL OVERVIEW

A SPS 2003 deployment contains one or more servers and/or server farms within an Active Directory (AD) domain. SPS 2003 consists of the following minimum components: one instance of Microsoft MSDE or SQL server, a Web store, an index database, a search service, a job service, a configuration database, a site database, a profile database, and optional SPS 2001 legacy document libraries.

To clarify various SPS 2003 configurations, note these baseline configurations for establishing common terminology:

Standard farm deployments

- **Single server configuration:** Single server hosting all SharePoint components, including either MSDE or SQL database
- **Small server farm:** All SPS components on a single server except for the SQL database, which has been installed on a separate server
- **Medium server farm:** One or more front-end Web servers with the search component enabled. One or more index management and job servers. One or more servers running a SQL database.
- **Large server farm:** Two or more front-end Web servers. Two or more search servers. One or more index servers, one of which is the job server. One or more SQL database servers.

DATA-PROTECTION PLANNING

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 use adequate data-protection tools for reliable disaster recovery, scalability, and ease of use. Without the proper data protection strategy, an organization places its documents and data at risk — the environment has no defined data-protection schemes, 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. This white paper answers this simple, yet crucial question. It also presents 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 its environment. Additionally, when determining specific SharePoint Portal Server 2003 data protection needs, organizations must consider these questions:

- Will backup processes be performed while SharePoint Portal Server 2003 is on-line or off-line?
- 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?

BACKUP EXEC 10 CONFIGURATION

Backup Exec 10 Media Server

Before you can begin implementing your SharePoint Portal Server 2003 data-protection plan, you must have installed and configured a Backup Exec 10 media server. Installation and configuration instructions are available in the VERITAS Backup Exec 10 for Windows Servers Administrator's Guide. The media server must have the following options licensed:

- Intelligent Disaster Recovery (if part of plan)
- Backup Exec Agent for Microsoft SharePoint Portal Server

Backup Exec 10 Media Sets

After you have a media server available, depending on your media management scheme, you may want to define one or more media sets for the SharePoint Portal Server 2003 servers at your site. A media set is a group of media, most likely a set of tapes or backup-to-disk folders, to which backup jobs are saved. The media set controls the overwrite protection period, which is how long that data is retained before being eligible to be overwritten, and the append period, which is how long that data can be appended to media. Defining a media set lets you customize backup-job retention policies and makes it easier to view SharePoint Portal Server backup entries in the Backup Exec media catalog, since entries are grouped by media set.

Backup Exec 10 Remote Agent

Before you can create jobs, you must install the Backup Exec 10 Remote Agent for Windows Server on each SharePoint Portal Server 2003 server that will be backed up.

Configuring Intelligent Disaster Recovery for Targeted Servers

If your data-protection plan includes the Intelligent Disaster Recovery (IDR) option for any of the servers, make sure to create an IDR bootable recovery image for each one and burn it to a CD. Before creating a server's recovery image and boot CD, you must perform an initial full system backup of the server, including all volumes, system state, and a full SPS backup using the Backup Exec Agent for Microsoft SharePoint Portal Server 2003 to include SQL2000 or Microsoft Desktop Engine (MSDE) instances. Please refer to the VERITAS Backup Exec 10 for Windows Servers Administrator's Guide for detailed instructions on how to configure and maintain IDR recovery data.

Reusing Selection Lists, Policies, and Jobs

Selection lists, policies, and jobs can be copied from one Backup Exec 10 media server to another. Follow these steps to do so (the procedure to move policies and jobs is similar):

1. Launch the Backup Exec 10 Administration application.
2. Open the **Job Setup** window.
3. Right-click the selection list you want to copy to another media server.
4. Select **Copy...**
5. In the **Copy Selection List** popup window, select **Copy to other media servers**, and then click **Add**.
6. Enter the destination media server name and logon account information in the **Add Server** popup window, and click **OK** when done.
7. Repeat for any other destination media servers.
8. Click **OK** to start the copy.

Monitoring and Reporting

Regular monitoring of backup jobs is an important task for backup administrators. If backups of a SharePoint Portal Server 2003 server fail for any reason, it will not be possible to restore that server to its most recent state. For this reason, the SharePoint Portal Server administrator should also monitor the backup status.

Backup Exec 10 offers a management pack for use with the Microsoft Operations Manager (MOM) at no additional cost. The MOM management pack monitors the health and availability of Backup Exec for Windows Servers software. By detecting, alerting about, and automatically responding to critical conditions, the management pack helps identify, correct, and prevent possible service outages. The management pack is available for download at <http://seer.support.veritas.com/docs/272197.htm>.

Backup Exec 10 also includes more than 40 reports that show detailed information about protected servers, media, and devices. When generating most of the reports, you can specify settings that serve as filter parameters or a time range for the data that you want to include in the report. This makes it possible to create a report that includes the set of SharePoint Portal Server 2003 servers. You can run and view a new report immediately, or you can create a job that saves the report data in the job history. You can also view general properties for each report.

Backup Exec 10 can schedule a report to run at a specified time or on a recurring schedule, and it can distribute reports through email notifications. This makes it possible to run scheduled reports that supply the data-protection status of a set of SharePoint Portal Server 2003 servers, as well to distribute the reports to all members of the organization responsible for the maintenance of these servers.

Reports are generated using Crystal Reports and can be viewed and printed in an HTML file format. If Backup Exec detects that Adobe® Reader is available, it displays reports in the Adobe Portable Document Format (PDF). The free Adobe Reader software is available at <http://www.adobe.com/acrobat>.

Below is a list of Backup Exec 10 reports that will help backup and SharePoint Portal Server administrators effectively monitor the data-protection status of a set of SharePoint Portal Server 2003 servers:

- Backup Job Success Rate – shows the success rate of success for jobs run on a set of selected servers.
- Backup Resource Success Rate – shows the success rate of success for each resource on set of selected servers.

- Backup Set Details by Resource – shows detailed information for each resource backed up on a set of selected servers.
- Backup Sets by Media Set – shows detailed information about all backup sets on selected media sets.
- Failed Backup Jobs – lists failed jobs for a set of selected servers, over a user-definable time period.
- Media Set – lists all the media used for a user-selectable group of media sets.
- Overnight Summary – provides an easy-to-view list of all backups within the last 24 hours for a set of selected servers.
- Policy Jobs by Resource Summary – shows details about each resource backed up in a user-defined period using policy-defined jobs, for a set of selected servers.
- Policy Jobs Summary – shows all the jobs derived from selected policies in a specified time range.
- Policy Protected Resources – shows a list of resources, and the policy and templates assigned to them, for a set of selected servers.
- Problem Files – shows a list of files that Backup Exec had a problem backing up, by resource, for a set of selected servers.
- Resource Backup Policy Performance – shows the success rate of policy-derived jobs for a user-defined time period, on a set of selected servers.
- Resource Risk Assessment – provides a list of resources for which the most recent backup failed, for a set of selected servers.
- Restore Set Details by Resource – shows detailed restore information by resource, in a user-defined time period, and for a set of selected servers.

To view or schedule reports, open the Backup Exec 10 administration application, and click the **Reports** tab. Right-click a listed report to see its run and scheduling options.

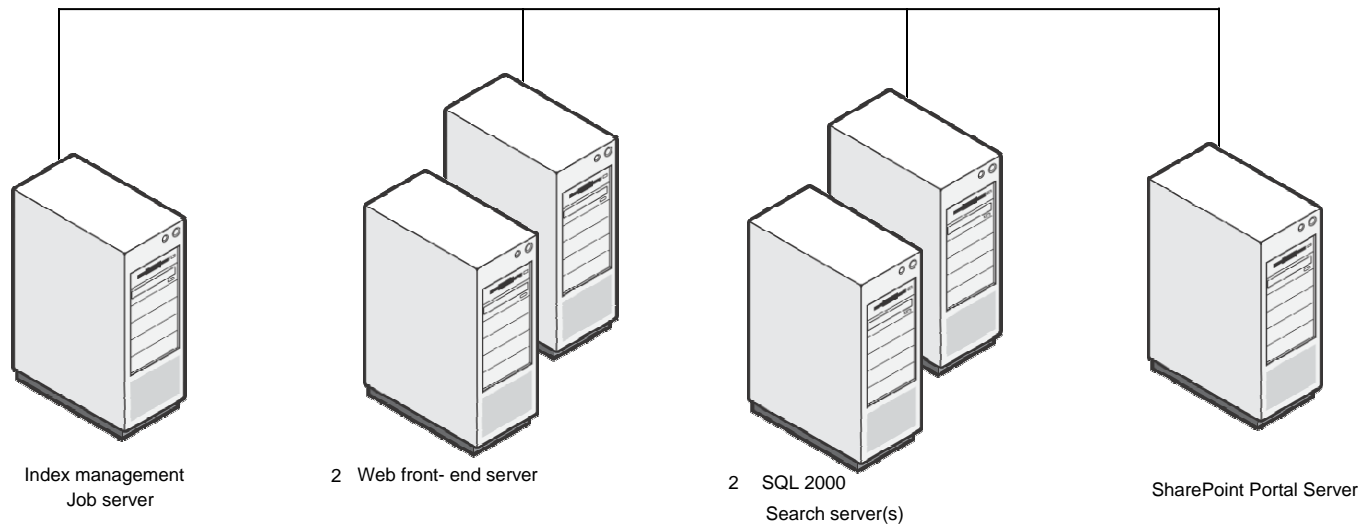
LICENSING OF BACKUP EXEC IN THE SPS ENVIRONMENT

The SPS agent consists of the following components: One component to protect a single SQL database instance and one remote agent for Windows servers (CAL) that is installed on the stand-alone SPS server.

In its simplest form, SPS 2003 is installed on a single server. The SPS server consists of the SharePoint application and an MSDE or SQL 2000 database running on Microsoft Windows Server 2003. The Backup Exec SPS agent includes all the necessary components to protect this configuration.

A typical small server farm consists of two servers: a server running SPS 2003 on Windows Server 2003 and a second server running SQL Server 2000 on Windows Server 2000 or Windows Server 2003. A single Backup Exec SPS license and a remote agent for Windows servers (CAL) are required to protect this small server farm configuration.

A medium or large server farm consists of a minimum of the following components: one SPS 2003 server on Windows Server 2003, one or more SQL servers running on Windows server 2000 or 2003, one or more Web servers, one or more job servers, and one or more search servers. To fully protect these large server farm configurations, you need one SPS 2003 agent, an SQL server agent for each additional SQL server, and a remote agent for each additional server beyond the initial SPS server.



In the example above, the following licenses are required:

- One SPS server agent
- One additional SQL database agent for the second SQL database instance
- Five additional Remote Agents *for Windows Servers*

Note: In cases where you have multiple SPS farms sharing a single SQL database, each farm requires a separate SharePoint license.

BACKUPS AND RESTORES: MSDE VERSUS SQL

In smaller SharePoint configurations, administrators may select to use the default MSDE database in place of the more capable, full SQL database. If the database is MSDE, the default recovery model is Simple, which allows only database and differential backups. If the database is SQL Server 2000, the default recovery model is Full, which allows 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.

BACKING UP THE COMPLETE SHAREPOINT PORTAL SERVER ENVIRONMENT

If the local server has SharePoint components installed, from the local selections node in the file selection view select the node called Microsoft SharePoint Resources. This node will display the list of the SharePoint components installed on this machine. The node will display all of the components in the farm, not just the components installed on the local machine. However, only the local components can be selected from this node. If the SharePoint configuration includes remote selections, a new Microsoft SharePoint Server Farms node will be added to the remote selections node. You can add these nodes manually or automatically. To add these nodes manually, select **Add Server Farms** in the context menu. To add nodes automatically, browse to a front-end Web server that participates in a server farm. You can automatically select the entire server farm to back up the entire set of servers and components for your environment.

BACKING UP AND RESTORING SHAREPOINT 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 database(s). If you want to individually restore 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 SPS 2003 Server as part of a full backup. If you have a server farm configuration, the Backup Exec SharePoint Portal agent contacts the front-end Web server. The Web server is running a process that queries all the database(s) (and/or servers) and collects the necessary data for backup. Since the front-end Web servers collect information from all the SharePoint Servers in the farm configuration, best practices dictate that administrators leverage the Intelligent Disaster Recovery (IDR) option on the Web servers to be able to rebuild these servers in the event of a catastrophic failure of the Web servers.

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.

The following components are interrelated and must be backed up together in a Microsoft Office SharePoint Portal Server 2003 environment so that the database will be in synch. The following examples use Team Portal as the portal name:

The site and profile databases must always be backed up together. For example, the following databases must be backed up together.

- TeamPort1_PROF
- TeamPort1_SITE
- To backup a SharePoint portal site, the Site, Profile, and Server databases must be backed up. For example, the following databases must be backed up:
 - TeamPort1_PROF
 - TeamPort1_SITE
 - TeamPort1_SERV

Note: The site database must exist or be restored prior to a backup of a Profile database. The site and profile databases must always be backed up together.

- If you backup the configuration database, you must ensure that the profile, site, and server databases were all backed up at the same time. If all databases are restored, 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
- If each of these components is on a separate server, each of these components will have its own backup set. Best practices for restore would be to select all sets in one job and bring all databases on-line after the restore job is completed for all databases rather than bringing each database on-line after the individual database restore is complete. See the Backup Exec administrators guide for details on how to configure your database restore to not automatically start up on completion of the restore.

IMPORTANT: Proceed with caution. Restoring these individual databases will only be useful if the configuration on the farm has changed, such as server names, between the time of the backup and the restore. 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.

SINGLE SIGN-ON SERVICES DATABASE

If the Microsoft SharePoint Portal Farm uses Single Sign-On Services, that database as well as the Manage encryption key must be backed up. The database can be automatically backed up using the SPS 2003 agent; the manage encryption key is automatically backed up by the SPS 2003 agent. The Single Sign-On Services database is given the name SSO by default.

LEGACY SHAREPOINT PORTAL SERVER 2001 AGENT

The new Backup Exec 10 SharePoint Portal Server agent will protect instances of SPS 2001 in conjunction with SPS 2003, the old SPS 2001 agent will no longer be required.

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 the following section, “Performing a Redirected Restore”) or restore to the same server from which the data was backed up (see “Restoring to the Same Database Server” later in this document).

PERFORMING A REDIRECTED RESTORE

When you perform a redirected restore to the same server, you must rename the databases. (You can rename only one database at a time.) After this is completed, the data is restored; however, the servers must 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 the Backing Exec 10 admin guide.

RESTORING TO THE SAME DATABASE SERVER

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

DISASTER RECOVERY

Recovery scenarios include the recovery of an MSDE or Microsoft SQL Server 2000 database that has become corrupted, the recovery or replacement of a single hard drive or server, or recovery of multiple servers following a site disaster. Recovery of a database or single server is straightforward, but recovery following a site-wide disaster is more complex.

RESTORE SCENARIO 1

Single-Server MSDE configuration

1. Perform IDR of the server (restore critical volumes/resources and reboot).
2. Restore remaining SQL databases for SQL instances.
3. Change SPS “StandAlone” registry value (this is required to ‘disconnect’ from Config DB via SPS Admin pages).
 1. Open Regedit and navigate to: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SharePoint Portal Server].
 2. Find the value called “StandAlone” and change the data from “1” to “0.”
4. Disconnect from the Config DB via the SharePoint Admin pages.

Note: You should be able to change the “StandAlone” registry value back to “1” at this point.
5. Delete all suspect databases in SQL Enterprise Manager. Note: Because MSDE doesn’t include Enterprise Manager, you either need to install it or delete the suspect DB’s via the command line.
6. Delete Index/Search GUID folders (content usually removed by SPS when disconnecting from Config DB).
7. From WSS, unextend Virtual servers (remove SharePoint from virtual servers).
8. Re-create Config DB with the same name in the same location.
9. Configure the topology as it was before.
10. Set Content Database Server and Component Settings Database Server to allow databases on a different instance.
11. Select and restore all portal databases.
12. Select and restore Single Sig-On Server database (if applicable).

13. Select and restore Doc Library Store (if applicable).

RESTORE SCENARIO 2

Single-Server SQL 2000 configuration

1. Perform IDR of the server (restore critical volumes/resources and reboot).
2. Restore remaining SQL databases for SQL instances.
3. Disconnect from the Config DB via the SharePoint Admin pages.
4. Delete all suspect DB's in SQL Enterprise Manager.
5. Delete Index/Search GUID folders (content usually removed by SPS when disconnecting from Config DB).
6. From WSS, unextend Virtual servers (remove SharePoint from virtual servers).
7. Re-create Config DB with the same name in the same location.
8. Configure the topology as it was before.
9. Set Content Database Server and Component Settings Database Server to allow databases on a different instance.
10. Select and restore all portal databases.
11. Select and restore Single Sign-On Services database (if applicable).
12. Select and restore Doc Library Store (if applicable).

RESTORE SCENARIO 3

Individual Servers of a SPS Server Farm (Small, Medium, or Large)

Search Server (Large)

1. Perform IDR of the server (restore critical volumes/resources and reboot).
2. Because nothing SPS-specific is backed up from the Search servers in this case, no further action is required (other than to restart the PS [Portal Server] Search service).

Index Server/Job Server (Medium or Large)

1. Perform IDR of the server (restore critical volumes/resources and reboot).
2. Delete the Index GUID folders (this may or may not be required, depending on configuration).
3. Select and restore all index databases associated with this index server.

Web Server (Medium or Large)

1. Perform IDR of the server (restore critical volumes/resources and reboot).
2. Because nothing SPS-specific is backed up from the Web servers in this case, no further action is required.

Doc Library Server (All)

1. Perform IDR of the server (restore critical volumes/resources and reboot).
2. Select and restore the Document Library Store for the farm.

SQL Server (All)

1. Perform IDR of the server (restore critical volumes/resources and reboot).
2. Restore remaining SQL databases for SQL instances.
3. Disconnect from the Config DB from all Web servers, index servers, and search servers via the SPS Admin pages.
4. Delete all suspect databases in SQL Enterprise Manager.
5. Delete GUID folders from both index servers and search servers (content is usually removed by SPS when disconnecting from Config DB).
6. From WSS, unextend virtual servers (remove SharePoint from Virtual servers) from each Web server.
7. From one of the servers, re-create Config DB with the same name in the same location.

8. Set Content Database Server and Component Settings Database Server to allow DB's on different instance.
9. Connect to new Config DB from remaining Web, index, and search servers.
10. Configure the topology as it was before.
11. Select and restore all portal and team databases (except for index databases). At this point, the restore will fail with "An error occurred while connecting the restored databases to the Microsoft SharePoint Portal Farm. The portal was not restored." errors even though all portal and team databases are restored to their correct locations.
12. Select and restore the Config DB. Note: Reconnect from Web, index, and search servers if needed.
13. Extend and map all virtual servers to existing sites on all the Web servers.
14. Select and restore index databases for all sites. At this point, the restore will fail with "Unable to Lock the SharePoint Portal Farm." errors. Sometimes both index servers produce the error for each index database, and sometimes only one of the index servers produces this error for each index database.
15. Resubmit the index-database restore job. This should complete successfully.
16. Select and restore the Single Sign-On Services database (if applicable).

SINGLE SIGN-ON SERVICES DATABASE

If the Microsoft SharePoint Portal Farm uses Single Sign-On Services, that database as well as the Manage encryption key must be restored. The database and encryption key can be restored using the Agent for SPS Server. 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.

SUMMARY

The Backup Exec 10 *for Windows Servers* offers industry-leading support of Microsoft Office SharePoint Portal Server 2003. The Backup Exec Agent for SharePoint Portal Server 2003 supports SharePoint Portal Server 2003 and 2001 configurations. The agent lets you restore individual servers or an entire SharePoint Portal Server farm. In addition, individual components and database can be restored in select configurations.

VERITAS Software Corporation
Corporate Headquarters
350 Ellis Street
Mountain View, CA 94043
650-527-8000 or 866-837-4827

For additional information about VERITAS Software, its products, or the location of an office near you, please call our corporate headquarters or visit our Web site at www.veritas.com.