
Microsoft Office Project Server 2003 Disaster Recovery Guide

Online Books

Microsoft

Microsoft® Office servers

Microsoft Office Project Server 2003 Disaster Recovery Guide



Enterprise Project Management Solution

Copyright

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2003 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows NT, Windows Server, and SharePoint are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Published: October 19, 2003

Updated: January 30, 2004; August 13, 2004

Applies To: Microsoft Office Project Server 2003, Microsoft Office Project Professional 2003, Microsoft Office Project Web Access 2003

Author: Mike Plumley

Editors: Kerry Landen; Laura Graham

Reviewed By: Project Product Development

Table of Contents

Introduction	1
Introduction	1
Microsoft Office Project Server 2003 Online Books Series.....	1
What Will You Learn from This Book?.....	2
Who Should Read This Book?	3
Revision History.....	3
Chapter 1	4
Overview of Disaster Recovery	4
Chapter 2	6
Identifying Fault Tolerance Strategies	6
Minimizing Single Points of Failure	6
Using Standby Servers.....	7
Using Standby Database Servers	7
Using Log Shipping	7
Using Clustering	7
Using Failover Clusters	8
Using Load-Balanced Clusters	9
Using RAID Configurations.....	10
Using Power Backup	10
Chapter 3	12
Establishing Recoverability	12
Creating Database Backups.....	13
Transaction Log Backups	13
Hard Disk Space Considerations	13
Using Hardware Standards.....	14
Maintaining Hardware Records.....	14
Maintaining Software Records.....	15
Planning Hardware Contingencies.....	15
Providing Training and Documentation	16

Chapter 4	17
Planning a Disaster Recovery Solution	17
Managing Risk	17
Determining Cost of Availability	18
Determining Acceptable Downtime	19
Determining Return on Investment	20
Chapter 5	21
Backing Up Your Deployment	21
Managing Media	21
Backing Up Computers in Your Deployment	22
Disk Imaging	22
Backing Up the Enterprise Global Template and Enterprise Resource Pool	23
Backing Up a Single Database.....	23
Setting the Recovery Model	23
Backing Up the Database.....	24
Backing Up Multiple Databases.....	24
Setting the Recovery Model	24
Marking the Transaction Logs.....	25
Creating a Table for Log Marking.....	26
Using Stored Procedures to Mark the Logs.....	26
Backing Up the Databases.....	28
Automating Transaction Log Marking.....	28
Backing Up MSDE and WMSDE Deployments	31
Chapter 6	32
Recovering Your Deployment	32
Basic Recovery Steps	32
Recovering a Computer Running SQL Server 2000	33
Recovering to the Point of Failure	33
Recovering to an Earlier Point in Time	33
Recovering a Single-Database Deployment.....	34
Recovering a Multiple-Database Deployment.....	34
Recovering a Computer Running Analysis Services.....	35
Recovering a Computer Running Windows SharePoint Services.....	35
Installing Windows SharePoint Services	35
Configuring the Administrative Virtual Server	36
Setting the Configuration Database Server	38
Extending the Virtual Server.....	40
Creating a Windows SharePoint Services Administrator	40
Updating Project Web Access Settings.....	41

Recovering a Computer Running Project Server 2003.....	41
Appendix A	46
Additional Resources	46
Microsoft Office Project Server 2003 Online Books Series.....	46
Project Server–Related Web Sites.....	47
Appendix B	48
Project Server Recovery Tools.....	48
Restore Single Project Tool	48
Running the Restore Single Project Tool.....	49
Configuring the Windows SharePoint Services Database	50
Copying the Windows SharePoint Services Site.....	52

Introduction

System administrators must protect their networks from both data loss and system downtime. The *Microsoft Office Project Server 2003 Disaster Recovery Guide* provides guidelines for developing a disaster prevention and recovery strategy for computers running Microsoft® Office Project Server 2003.

This guide is written for administrators who have experience with backing up and restoring complex systems, and for system architects and planners who need to determine the best and most cost effective disaster prevention and recovery strategy for a Project Server deployment.

Send us your feedback. Please let us know what you think about the quality of this content. If this text does not meet your needs, let us know how we can improve it. If this text was helpful to you, let us know how it helped.

<mailto:proidocs@microsoft.com?subject=Feedback: Microsoft Office Project Server 2003 Disaster Recovery Guide>

Microsoft Office Project Server 2003 Online Books Series

The Microsoft Office Project Server 2003 Online Books series documents the Microsoft Office Enterprise Project Management (EPM) Solution and provides a detailed reference for all phases of deploying Project Server, including planning, installation, configuration, and administration. Each book is designed to stand alone and can be referred to on an as-needed basis. You can also read these books in the order listed below for a complete guide to deploying Project Server 2003:

- *Microsoft Office Project Server 2003 Solution Planning Guide*
<http://go.microsoft.com/fwlink/?LinkId=33654>
- *Microsoft Office Project Server 2003 Configuration Planning Guide*
<http://go.microsoft.com/fwlink/?LinkID=20235>
- *Microsoft Office Project Server 2003 Disaster Recovery Guide*
<http://go.microsoft.com/fwlink/?LinkID=20234>
- *Microsoft Office Project Server 2003 Installation Guide*
<http://go.microsoft.com/fwlink/?LinkID=20233>

This includes the following resources:

- *Microsoft Office Project Server 2003 Installation Guide: Single Server Deployment*

- *Microsoft Office Project Server 2003 Installation Guide: Small Scale Deployment*
- *Microsoft Office Project Server 2003 Installation Guide: Medium Scale Deployment*
- *Microsoft Office Project Server 2003 Application Configuration Guide*
<http://go.microsoft.com/fwlink/?LinkID=20237>
- *Microsoft Office Project Server 2003 Administrator's Guide*
<http://go.microsoft.com/fwlink/?LinkID=20236>
- *Microsoft Office Project Server 2003 Security Group Guide*
<http://go.microsoft.com/fwlink/?LinkId=33554>

This includes the following resources:

- *Microsoft Office Project Server 2003 Portfolio Managers Guide*
- *Microsoft Office Project Server 2003 Project Managers Guide*
- *Microsoft Office Project Server 2003 Resource Managers Guide*
- *Microsoft Office Project Server 2003 Team Leads Guide*
- *Microsoft Office Project Server 2003 Team Members Guide*
- *Microsoft Office Project Server 2003 Executives Guide*

A key part of deploying Project Server 2003 and the EPM Solution it provides is proper planning. These books will help your organization plan for deployment by explaining Project Server 2003 in detail, highlighting the questions you should ask throughout the planning phase, and providing a reference for the requirements during each phase of deployment. These books are not intended to be a substitute for proper planning within your organization as to what your EPM Solution should be. The Microsoft Office Project Server 2003 Online Books series will help you succeed in deploying your organization's project management solution.

What Will You Learn from This Book?

This guide describes availability options and backup and recovery techniques for a Project Server deployment. The guide covers the following topics:

- Fault tolerance and recoverability, and why they are important considerations when planning disaster recovery for your Project Server deployment.
- How to back up your Project Server and Microsoft Windows® SharePoint® Services data.
- How to recover your deployment after a system failure or disaster.

Use the information presented in the first four chapters in this guide to help you determine an optimum availability and recoverability plan for your Project Server deployment. Then, using the information presented in Chapter 5, **Backing Up Your Deployment** and

Chapter 6, **Recovering Your Deployment**, you can develop a backup and recovery plan that meets the needs of your organization.

Who Should Read This Book?

This guide is designed to benefit the following professionals:

IT Administrators

Those individuals who are responsible for installing Project Server 2003 and its related components.

Database Administrators

Those individuals who are responsible for database maintenance, including backup and recovery.

Deployment Planners

Those individuals who plan Project Server deployments in your organization.

Important It is recommended that the users who complete the procedures for backup and recovery in this book have experience with Microsoft SQL Server™ database administration.

Revision History

The following table provides the revision history for this document.

Date	Revision
October 2003	<ul style="list-style-type: none">● Initial Publication.
January 2004	<ul style="list-style-type: none">● Added Appendix B, Project Server Recovery Tools.
August 2004	<ul style="list-style-type: none">● Minor updates to text for consistency and clarity.

1

Overview of Disaster Recovery

In recent times, organizations have dramatically increased their reliance on computer-based data storage. As a result, it is important for information technology (IT) workers to reduce costs to organizations by maintaining critical applications and preventing unnecessary system downtime.

System administrators must protect their networks from both data loss and system downtime. This involves both routine procedures performed on an ongoing basis and nonroutine steps taken to prevent or recover from unexpected downtime.

Some of the potential causes of system downtime include:

- Hard disk subsystem failure
- Power failure
- Systems software failure
- Accidental or malicious use of deletion or modification commands
- Destructive viruses
- Natural disasters
- Theft or sabotage

This guide is designed to help you develop a disaster recovery plan for your Microsoft® Office Project Server 2003 deployment. In addition to reading this guide, it is important to have the following elements of a disaster recovery plan in place:

- A plan to acquire replacement hardware
- A communication plan
- A list of people to be contacted in the event of a disaster
- Instructions for contacting the people involved in the response to the disaster
- Information about who owns the administration of the plan

An effective disaster recovery plan ensures that you can quickly recover your data if it is lost. Be sure to develop your backup and restore strategies with appropriate resources and personnel, and test them.

A disaster recovery plan should ensure that all your systems and data can be restored to normal operation quickly in the event of a natural disaster (such as a fire) or a technical disaster (such as a two-disk failure in a RAID-5 array). When you create a disaster recovery plan, you identify all of the actions that must occur in response to a catastrophic event.

Thoroughly test your backup and recovery plan before deploying Project Server 2003 in a production environment. When testing, look for vulnerable areas by simulating as many possible failure scenarios as you can. It is recommended that you verify your disaster recovery plan by simulating the occurrence of a catastrophic event.

When planning your disaster recovery strategy, consider the following questions:

- To what medium will you send the backup (tape or disk)?
- Will you do the backups manually or schedule them to be done automatically?
- If backups are automated, how will you verify that they successfully occurred?
- How will you ensure that the backups are usable?
- How long will you save the backups before reusing the medium?
- Assuming failure, how much time will it take to restore from the most recent backup? Is that an acceptable amount of downtime?
- Where will you store the backups, and do the appropriate people have access to them?
- If the responsible system administrator is unavailable, is there someone else who knows the proper passwords and procedures to perform backups and, if necessary, to restore the system?

As part of any disaster recovery plan, it is recommended that you do the following:

- Use Microsoft Windows® Event Viewer on a daily basis to check both the system log and application log on your production servers for any errors or warnings.
- Always maintain an up-to-date Windows Emergency Repair disk or Automated System Recovery (ASR) set for each server in your deployment. See Windows Help for more information.
- Ensure that all your servers are protected with adequate antivirus software. Keep the software up-to-date with the latest virus signature files. Use the automatic update feature of your antivirus application to keep the virus signatures current.

2

Identifying Fault Tolerance Strategies

Fault tolerance refers to the ability of a system to continue to function when part of the system fails. To create a fault-tolerant system, use preventive measures to minimize the possibility of a system failure and to minimize the impact of any disaster.

You can use the following strategies to improve the fault tolerance of your Microsoft® Office Project Server 2003 deployment:

- Minimizing single points of failure
- Using standby servers
- Using clustering
- Using RAID configurations
- Using power backup

This chapter provides more information about each of these strategies. You can apply these strategies individually or in combination. Because each strategy has a cost associated with it, it is important to examine the cost/benefit ratio for each before applying it in your organization.

Minimizing Single Points of Failure

You can provide some fault tolerance for your Project Server deployment by deploying additional hardware configurations that duplicate the hardware configuration of your organization. In this way, if one path of data input/output (I/O), or the physical hardware components of a server (such as computer, network, and storage area network components) fail, the system is not affected. The hardware that you use to minimize the single points of failure varies according to what components you want to make redundant. Hardware vendors typically include duplicate hardware as part of their storage solution.

Using Standby Servers

A standby server is a second server that can be brought online if a primary production server fails. The same software components that are installed on the primary server are installed on the standby server. Using a standby server allows users to continue working with Project Server data if the primary server becomes unavailable.

A standby server can also be used when a primary server is unavailable due to scheduled maintenance. For example, if you must take the primary server offline for a hardware or software upgrade, you can use the standby server until the primary server is brought back online.

The most important factor to consider when using standby servers is that the hardware, software updates, and firmware updates on a standby server must be identical to those of the primary server that the standby server is designed to replace.

Using Standby Database Servers

If the standby server is a database server, it must contain a copy of the databases on the primary server. If the primary server goes offline and the standby server is brought online, when the primary server becomes available again, any changes to the copies of the database that are located on the standby server must be copied back to the primary server.

Otherwise, those changes are lost. When users start using the primary server again, the databases on the primary server should be backed up and copied to the standby server.

Periodically, transaction log backups from the databases on the primary server are applied on the standby server to ensure that the standby server remains synchronized with the primary server. If the primary server fails, or even if just a single database fails, the databases on the standby server are made available to user processes. Any user processes that cannot access the primary server must use the standby server instead.

Using Log Shipping

With Microsoft SQL Server™ 2000 Enterprise Edition, you can use log shipping to feed transaction logs from one database to another continuously. Continually backing up the transaction logs from a source database and then copying and restoring the logs to a destination database keeps the destination database synchronized with the source database. Log shipping provides an automated method of maintaining a standby server.

Using Clustering

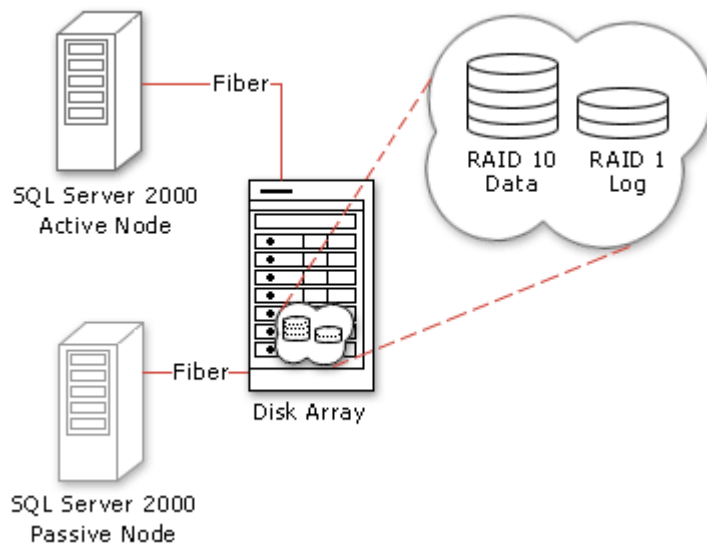
Clustering can protect your system against an application or operating system failure, whereas a fault-tolerant standby server cannot. You can also perform many tasks on

clustered computers without taking them offline, including upgrading an application or operating system or installing a service pack or update. You can only perform upgrades on standby servers by taking the hardware offline.

Server clusters are designed to keep applications available, rather than to protect data. To protect against viruses, corruption, and other threats to data, you need solid data protection and recovery plans. Cluster technology cannot protect against failures caused by viruses, software corruption, or human error.

Using Failover Clusters

Failover clusters are designed for stateful applications. Stateful applications have long-running in-memory state, or they have large, frequently updated data states.



Failover cluster.

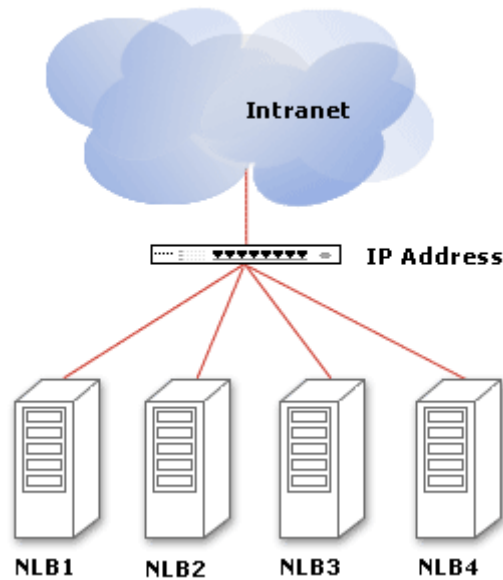
Failover clusters provide high availability by allowing the failover of resources. Failover clusters also maintain client connections to applications and services.

In failover clusters, nodes share access to data. Nodes can be either active or passive, and the configuration of each node depends on the operating mode (active or passive) and how you configure failover in the cluster. A server that is designated to handle failover must be sized to handle the workload of the failed node in addition to its own workload.

In Project Server deployments, you can use failover clustering with SQL Server 2000. You can also use failover clustering with the Views Processing and Session Manager services in a distributed deployment.

Using Load-Balanced Clusters

You can use Network Load Balancing (NLB) in Microsoft® Windows® 2000 Server and Microsoft Windows Server™ 2003 to create load-balanced clusters. Load-balanced clusters are intended for stateless applications. Stateless applications do not have long-running in-memory state. A stateless application treats each client request as an independent operation, and, therefore, it can load-balance each request independently.



A load-balanced cluster.

Load-balanced clusters are groups of identical, typically cloned computers that are used to enhance the availability of Web servers, Microsoft Internet Security and Acceleration (ISA) servers (for proxy and firewall servers), and other applications that receive Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) traffic. Because cluster nodes are usually identical clones of each other and can therefore operate independently, all nodes in a cluster are active.

You can scale load-balanced clusters by adding servers as demand on the cluster increases. Each node runs a copy of the Internet Protocol (IP)-based application or service that requires load balancing and stores all the data necessary for the application or service to run on local drives.

In Project Server deployments, you can use NLB with the Project Server Front-End service and Microsoft Windows® SharePoint® Services.

Note For more information about load balancing, see the *Microsoft Office Project Server 2003 Configuration Planning Guide* (<http://go.microsoft.com/fwlink/?LinkID=20235>).

Using RAID Configurations

By using a redundant array of independent disks (RAID), you can increase the fault tolerance of your Project Server deployment. RAID stores identical data on multiple disks for redundancy, improved performance, and increased mean time between failures (MTBF). In a RAID configuration, part of the physical storage capacity contains redundant information about data stored on the hard disks. The redundant information is either parity information (in the case of a RAID-5 volume), or a complete, separate copy of the data (in the case of a mirrored volume). The redundant information enables data regeneration if one of the disks or the access path fails, or if a sector on the disk cannot be read.

To ensure that computers running Project Server 2003 continue to function properly in the event of a single-disk failure, you can use RAID disk mirroring or disk striping with parity on the hard disks within your Project Server deployment. Disk mirroring and disk striping with parity creates redundant data for the data on your hard disks.

Using RAID configurations does not prevent damaged files or other file errors. For this reason, do not use RAID configurations as a substitute for keeping current backups of important data on your servers.

To implement a RAID configuration, you must use a special set of hard disks designed only for use with RAID configurations.

Because transaction log files and database files are critical to the operation of computers running Project Server 2003, you can keep the transaction log files and database files on separate physical drives. You can also use RAID disk mirroring or disk striping with parity to prevent the loss of a single physical hard disk from causing a failure in your Project Server database.

Note For more information about disk mirroring and disk striping with parity, see the Windows Server 2003 Help and Support Center.

Using Power Backup

Using an uninterruptible power supply (UPS) and battery backup to increase fault tolerance in your Project Server deployment is necessary for servers that contain critical data, especially in large server deployments. UPS and battery backup provide protection against power surges and short power losses that can cause damage to your servers and the data they contain. For large data centers or critical applications, consider a large-scale UPS

system and a backup generator to maintain power to the UPS, air conditioning, and other critical systems during long outages.

3

Establishing Recoverability

Recoverability from a failure refers to the ability to restore your deployment to the point at which the failure occurred. The ability to recover quickly from a system failure or disaster depends not only on having current backups of your data, but also on having a predefined plan for recovering that data on new hardware.

This chapter covers the primary elements for which you must plan for fast and efficient recovery in the event of a system failure or disaster, including:

- **Creating database backups** Database and transaction log backups are vital to the recoverability of your deployment.
- **Using hardware standards** Using set standards for hardware improves the maintainability and recoverability of your deployment.
- **Maintaining hardware records** Keeping good records of your hardware configurations and hardware parts suppliers helps make both routine maintenance and disaster recovery more efficient.
- **Maintaining software records** Software configuration records can assist with regular maintenance tasks, as well as with disaster recovery.
- **Planning hardware contingencies** Having a hardware contingency plan can help minimize downtime costs by allowing you to replace hardware quickly in the event of a failure.
- **Providing training and documentation** Proper documentation of your systems and training of your staff is vital for allowing you to recover from a system failure or disaster in the least possible amount of time.

Each of these elements must be part of your backup and recovery plan to ensure your ability to restore your deployment in the event of a system failure or disaster.

Creating Database Backups

Microsoft® Office Project Server 2003 data and Microsoft Windows® SharePoint® Services data is stored in Microsoft SQL Server™ 2000 databases. To protect your data against loss, you must create database backups by using the tools provided with SQL Server 2000. Database backups contain a complete record of all the data in your database at the time the backup completes. Database backups can be used in combination with transaction log backups to restore your Project Server and Windows SharePoint Services data to the point of failure or to an earlier point in time.

Transaction Log Backups

The transaction log is a serial record of all modifications that have occurred in a database as well as the transaction that performed each modification. The transaction log records the start of each transaction. It records the changes to the data and enough information to undo the modifications (if necessary later) made during each transaction. The log grows continuously as logged operations occur in the database.

Transaction log backups enable you to recover the database to an earlier point in time (for example, prior to entering unwanted data), or to the point of a failure. In addition to database backups, transaction log backups must be part of your recovery strategy.

Because most Project Server deployments maintain data in two or more related databases, you may also need to use marked transactions to ensure synchronization during restore operations.

Note For more information about transaction log backups, see Chapter 5, **Backing Up Your Deployment** in the *Microsoft Office Project Server 2003 Disaster Recovery Guide*.

Hard Disk Space Considerations

You must have enough space on your hard disk to restore both the database and the log files on the computers running Project Server 2003. You might have a backup that is too large to restore to its original location. For example, a Normal backup performed once per week plus six days of Differential backups might require more disk space during a restore than your server has available.

Also, you should never let your database drive become more than half full. Although a database drive that is less than half full results in unused disk space, it can still reduce extended server downtime for the following reasons:

- You can restore databases faster than you can when a drive is full (especially if the file system is fragmented).

- You can back up a copy of the databases to the same physical disk before you restore them, which enables you to attempt to repair the databases if a problem occurs during the restore process (for example, if the existing backup contains errors).

Using Hardware Standards

Adopt one standard for hardware, and apply it as much as possible. Use the same kinds of components, such as network cards, disk controllers, and graphics cards, on all of your computers. Use this standard computer profile for all applications, even if it is more than you need for some applications. The only modifications that you should make to the hardware are to the amount of memory, the number of CPUs, and the hard disk configurations.

Hardware standards provide the following advantages to your organization:

- Having only one platform reduces the amount of testing needed.
- When applying driver updates or application software updates, you only need to perform one test before deploying the updates to all of your computers.
- Because only one type of system must be supported, support personnel require less training.
- You do not need to keep as many spare parts on location, which reduces costs to the organization.

Keep spare and replacement parts on-site, and include spare equipment in any hardware budget. The number of spare parts that you keep on location varies according to the configuration and failure conditions that users and operations personnel can tolerate.

Some parts, such as memory and CPU, are easy to find years after the original parts are acquired. Other parts, such as hard disks, are often difficult to locate after only a few years. For parts that may be hard to find, and where exact matches must be used, plan to buy spares when you buy the equipment. Consider using service companies or contracts with a vendor to delegate the responsibility, or keep one or two of each of the critical components in a central location.

Maintaining Hardware Records

To limit the amount of time you spend troubleshooting hardware configuration problems during a disaster recovery, maintain current hardware configuration records, including:

- A list of all hardware vendor contact information, including phone numbers, e-mail addresses, and Web pages for online support.
- A list of the hardware in each server, with firmware update versions and hardware driver versions (this hardware information can be found in Windows Device Manager).

- A list of the Basic Input/Output System (BIOS) information, interrupt request (IRQ) settings, hard disk configuration information, and jumper settings on the hardware for your server.

Important Maintain a copy of this information off-site in case your facilities are damaged and you need to recover your systems in a new location.

Maintaining Software Records

To limit the amount of time you spend troubleshooting software-related problems during a disaster recovery, maintain current software records, including:

- A list of your software vendor contact information, including phone numbers, e-mail addresses, and Web pages for online support.
- A chronological list of all software upgrades (such as service packs) and software patches that are installed on your servers. By keeping this list, you can install the software updates in the same order in which they were installed originally.
- A record of the configuration for each server, including:
 - Server name.
 - Administrative group name to which the server belongs.
 - Hard disk configuration information, including a list of each hard disk partition with the volume names and sizes of the partitions as well as a summary of what is installed on each partition.
 - List of any static Internet Protocol (IP) addresses, subnet masks, and default gateways used by the server.
 - A record of the cluster configuration information, if your topology includes clusters. To back up this information, use the Microsoft Cluster Tool (Clustool.exe) included in the *Microsoft Windows 2000 Server Resource Kit* (<http://go.microsoft.com/fwlink/?LinkId=33124>).
 - Any customizations you made to the server, such as Project Web Access customizations.

Important Maintain a copy of this information off-site in case your facilities are damaged and you need to recover your systems in a new location.

Planning Hardware Contingencies

To minimize downtime costs, including losses in sales and productivity, keep replacement hardware immediately available for your production servers. Types of replacement hardware to consider having immediately available include alternate backup servers,

network adapters, video and hard disk controller cards, routers, cables, hard disks, motherboards, and power supplies.

Providing Training and Documentation

Ensure that administrators, operators, and support staff within your organization have access to various training opportunities and documentation regarding disaster recovery issues.

If one or more of your servers experiences problems, the subsequent downtime can be costly. However, if you invest in good training courses and up-to-date technical manuals for your server administrators, operators, and support staff, your organization will be prepared, and downtime will decrease.

You can also perform occasional disaster recovery simulations in separate, non-production domains. These simulations familiarize administrators, operators, and support staff with recovery procedures, as well as indicate any deficiencies in your backup and restore strategies. Update your documentation with any new procedures or practices you develop during these simulations.

4

Planning a Disaster Recovery Solution

It is important to understand how backup and recovery of your Microsoft® Office Project Server 2003 deployment fits in with the needs of your organization and the other software applications that you deploy.

The technologies that you use for fault tolerance and recoverability varies according to the needs of your organization. You must weigh the cost of downtime against the cost of recovery. You should also account for the ease with which lost data can be replaced in a variety of failure scenarios, and the cost of lost goodwill with customers and other organizations caused by system downtime.

Planning a disaster recovery solution involves the following steps:

- Managing risk
- Determining cost of availability
- Determining acceptable downtime
- Determining return on investment

This chapter describes provides information about each of these steps.

Managing Risk

Risk management involves engaging in a broad range of activities to identify, control, and mitigate risks. IT planners should use risk management to identify vulnerabilities so that appropriate controls can be put in place to either prevent disasters from happening or to limit the effects of a disaster.

A risk assessment for your Project Server deployment should identify system vulnerabilities, threat, and current controls and attempt to determine the risk based on the likelihood and the impact of a threat.

When assessing risk for your disaster recovery strategy, consider the following:

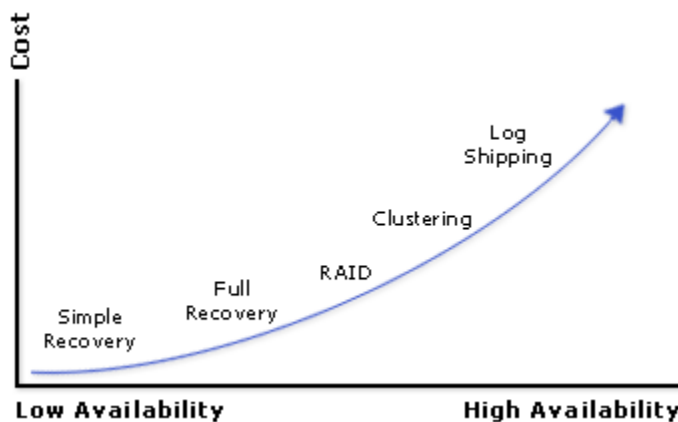
- Cost
- Allowable outage time
- Security
- Integration with larger, organization-level contingency plans

When planning a highly available Project Server environment, consider all available alternatives and measure the risk of failure for each alternative. Evaluate the costs of each alternative against its risk factors and the impact of downtime to your organization.

After you evaluate risks versus costs, and after you design and deploy your system, your IT staff will require guidelines and plans of action in case a system failure does occur.

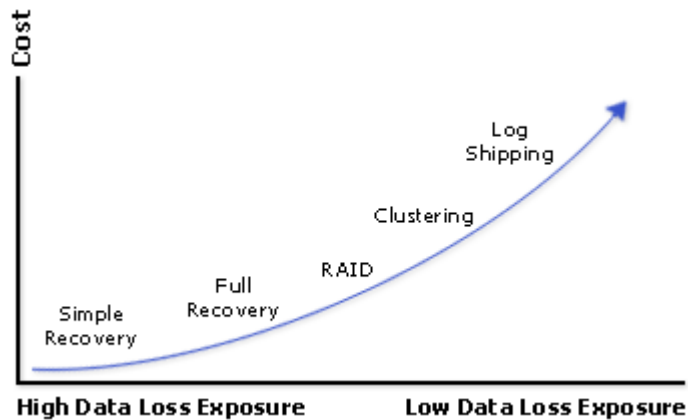
Determining Cost of Availability

When you implement more sophisticated options to improve the availability of your Project Server deployment, costs can rise dramatically.



Cost vs. availability.

Using clustering technologies, log shipping, standby servers, or even standby data centers will improve availability and also lessen data loss exposure. However, in a small deployment or a deployment in which data can be recreated easily, data loss exposure may not be a critical consideration. For larger deployments that use more complex Project Server features, recreating lost data can be time-consuming and costly. The risk of data loss in such a case can justify investing in technologies for high availability.



Cost vs. data loss exposure.

To develop a successful disaster recovery plan, you must understand when your data needs to be accessible and the potential impact of data loss on your business. Answering the following questions can help you determine your availability requirements and sensitivity to data loss:

- What are your availability requirements? What portion of each day must Project Server be online?
- What is the financial cost of downtime to your business?
- If you experience media failure, such as a failing disk, what is the acceptable downtime?
- In case of a disaster, such as the loss of a server in a fire, what is the acceptable downtime of your Project Server deployment?
- How important is it to never lose changes to your data?
- How easy would it be to re-create lost data?
- Does your organization employ system or database administrators?
- Who will be responsible for performing backup and recovery operations, and how will they be trained?

You can determine technical and financial tradeoffs for your availability solution based on your answers to these questions.

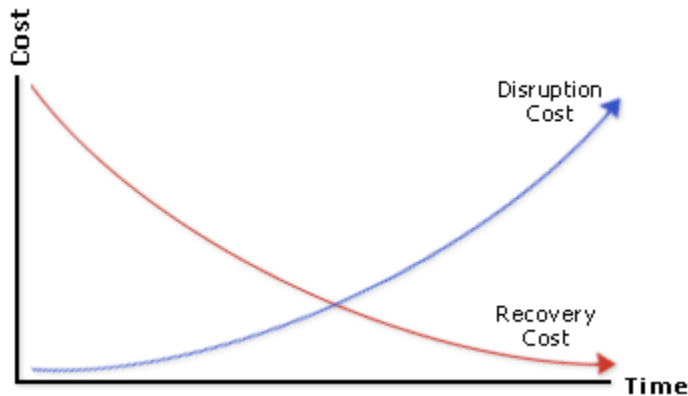
Determining Acceptable Downtime

You can measure the costs of replacing lost hardware easily. However, it is more difficult to assess the total cost of downtime that occurs when a computer running Project Server experiences a failure. Excessive downtime can result in many business losses, including the loss of sales, loss of customer goodwill, loss of productivity, loss of competitiveness,

missed contractual obligations, and increased costs resulting from the need to make up these losses. Therefore, you and your management team should agree in advance on what the acceptable amount of downtime is for a computer running Project Server 2003 in your organization. This agreement is called a service level agreement. After you establish a service level agreement, you can determine the Project Server deployment and server configurations that best meet the requirements for that agreement.

Determining Return on Investment

Creating a highly available Project Server deployment might require a combination of new or costly hardware solutions, additional staff, and support staff for non-peak hours. As you determine how important it is to maintain availability in your Project Server environment, consider whether the added availability is worth the cost.



Disruption cost and recovery cost crossover.

Analyze the effects of an outage over time to identify the maximum allowable time that users of a resource can be denied service before the outage prevents or inhibits the performance of an essential function. Also analyze the effects of the outage across related resources and dependent systems to identify any cascading effects that may occur as a disrupted system affects other processes that rely on it.

The point at which the cost of a disruption and the cost of recovery meet represents the amount of investment that your organization should make in a disaster recovery solution.

5

Backing Up Your Deployment

Microsoft® Office Project Server 2003 data and Microsoft Windows® SharePoint® Services data is stored in Microsoft SQL Server™ 2000 databases. Backing up these SQL Server databases is a key aspect of protecting your Project Server deployment against loss.

When you deploy Project Server 2003, keep a record of the accounts that you create, and computer names, passwords, and setup options that you choose. Keep this information in a safe place. Always keep a copy of all recovery materials, documents, and database and transaction log backups at an offsite location.

Important Perform a trial data restoration periodically to verify that your files are properly backed up. A trial restoration can uncover hardware problems that do not show up with software verifications.

This chapter describes the various methods that you can use to back up your Project Server deployment, including backup media, backing up computers and single and multiple databases, and backing up MSDE and WMSDE deployments.

Managing Media

When you back up and restore a database, you must back up the data onto media (for example, tapes and disks). Your backup plan should include provisions for managing media, such as:

- A tracking and management plan for storing and recycling backup sets.
- A schedule for overwriting backup media.
- In a multi-server environment, a decision to use either centralized or distributed backups.
- A means of tracking the useful life of media.

- A procedure to minimize the effects of the loss of a backup set or backup media (for example, a tape).
- A decision to store backup sets onsite or offsite, and an analysis of how this will affect recovery time.

To safeguard against a catastrophic event (such as a fire or earthquake), keep duplicates of your server backups in a different location from the location of the servers. This will protect you against the loss of critical data. As a best practice, keep three copies of the backup media, and keep at least one copy offsite in a properly controlled environment.

Backing Up Computers in Your Deployment

Because Project Server and Windows SharePoint Services data is stored in SQL Server databases, it is not necessary to back up the computers on which Project Server and Windows SharePoint Services are installed. In the event of a media failure or disaster involving those computers, reinstalling Project Server 2003 or Windows SharePoint Services provides a cleaner and more reliable alternative to restoring from a backup.

Disk imaging is one method that you can use to back up your computers. It is also important to back up the Enterprise Global Template and Enterprise Resource Pool that your organization uses.

Disk Imaging

You can use disk imaging to back up the computers in your Project Server deployment to help reduce recovery time in the event of a system failure or disaster. When using disk imaging, be sure to shut down your Project Server deployment before creating any disk images.

Important Restoring a disk image can cause problems if you are restoring to a different hardware configuration than the original system.

Use the following guidelines when using disk imaging to back up your Project Server deployment.

Computers Running Project Server Services, Analysis Services, or Windows SharePoint Services

When your Project Server deployment is shut down, create a disk image of the computer. Update the image each time you make a change to the system, such as the application of a service pack. You can then restore this image after a failure.

Computers Running SQL Server 2000

You can use disk imaging to back up computers running SQL Server 2000, but only the SQL Server installation itself can be backed up in this manner. Do not attempt to back up SQL Server data by using disk imaging technologies; you cannot apply log file backups and roll forward to the point of failure after recovering from a disk image backup. To back up your SQL Server data, use SQL Server 2000 database and transaction log backups.

Disk Images Shared Between Computers

Do not share disk images between computers. Create a unique disk image for each computer in your deployment. Sharing disk images between computers can result in problems with services running on those computers when you restore the image.

Backing Up the Enterprise Global Template and Enterprise Resource Pool

It is recommended that you periodically check out the Enterprise Global Template and Enterprise Resource Pool and save them offline. These backups can later be used to restore Enterprise Global Template and Enterprise Resource Pool information.

Backing Up a Single Database

Use the backup procedures in this section if you have deployed Project Server in a single database and are not using Windows SharePoint Services.

Important The procedures in this section apply only to deployments that use Project Server 2003 alone in a single-database configuration. If you are using Windows SharePoint Services with your Project Server deployment, or if you have partitioned your Project Server database onto multiple database servers, see the topic **Backing Up Multiple Databases** in Chapter 5, **Backing Up Your Deployment** of the *Microsoft Office Project Server 2003 Disaster Recovery Guide*.

Setting the Recovery Model

Set the recovery model for each of the databases in your deployment in the following ways:

- **Project Server database: Full Recovery** A daily full backup of the Project Server database is recommended.

Note It is recommended that you move your Project Server databases to fault-tolerant storage.

- **MsdB: Simple Recovery** This database contains the backup and restore history for all of your databases. You will need this information when recovering your Project Server deployment. A daily backup of the Msdb database is recommended.

Note It is recommended that you move the Msdb database to fault-tolerant storage.

- **Master: Simple Recovery** This database contains SQL Server 2000 security and configuration information. A daily backup of the Master database is recommended.

Backing Up the Database

It is recommended that you create a full backup of your Project Server database as often as required according to the backup policies of your organization, or at a frequency that enables you to recover Project Server data while minimizing data loss. For example, if your organization requires that timesheets be submitted and approved weekly, you can perform a weekly backup after that process is complete to ensure that you always have a record of completed work cycles.

► To back up your Project Server deployment

1. Back up the Project Server database.

Note It is recommended that you also back up the Master and Msdb databases after you back up the Project Server database.

2. Back up the transaction log throughout the day.

Backing Up Multiple Databases

When Project Server data is stored in two or more related databases, it is necessary to use marked transactions in the transaction logs of each database to facilitate recovery. If you are using Windows SharePoint Services as part of your Project Server deployment, or if you have partitioned your Project Server database, follow the guidelines in this section when backing up your deployment.

Important By default, the network access settings of the Microsoft Distributed Transaction Coordinator (MSDTC) are disabled on new installations of SQL Server 2000 on computers running Microsoft Windows Server™ 2003. If the databases in your deployment are located on more than one computer and you are using Windows Server 2003, follow the procedure in Microsoft Knowledge Base Article 329332 (<http://go.microsoft.com/fwlink/?LinkId=19685>) to make sure your MSDTC settings are correct. After you complete the procedure, restart your computer.

Setting the Recovery Model

Set the recovery model for each of the databases in your deployment as follows:

- **Project Server database: Full Recovery** Both point-of-failure recovery and recovery to earlier points in time require full backups and transaction log backups of your Project Server databases.

Note It is recommended that you move your Project Server databases to fault-tolerant storage.

- **Windows SharePoint Services Content database: Full Recovery** This database contains the documents, issues, and risks data for your Project Server deployment. Both point-of-failure recovery and recovery to earlier points in time require full backups and transaction log backups of your Windows SharePoint Services database.

Note It is recommended that you move your Windows SharePoint Services Content database to fault-tolerant storage.

- **Windows SharePoint Services Configuration database: Simple Recovery** This database contains configuration and site mapping information for your server computer, the virtual servers on your server computer, and servers in a server farm. Back up this database whenever you make changes to your Windows SharePoint Services configuration.
- **Msdb: Simple Recovery** This database contains the backup and restore history as well as the log marking history for all of your databases. You will need this information when recovering your Project Server deployment. A daily backup of the Msdb database is recommended.

Note It is recommended that you move the Msdb database to fault-tolerant storage.

- **Master: Simple Recovery** This database contains SQL Server 2000 security and configuration information. A daily backup of the Master database is recommended.

Marking the Transaction Logs

A marked transaction is a transaction that is given a name. By applying marked transactions to all the databases in your deployment simultaneously, you create a consistent point in all databases to which you can recover.

Related database recovery does not allow recovery to an arbitrary point in time. Recovery of related databases to any time earlier than the point of failure can only be accomplished by recovering to a marked transaction.

To mark transactions across related databases, place distributed marks across all databases before backing up the log in any database. This ensures that all log backups have a mark that will appear in all databases and allows synchronization during restore.

To recover related databases to a point in time prior to the point of failure, you must have the following:

- A full database backup of each database

- Subsequent transaction log backups of each database containing a distributed named mark

Important The transaction log backup for each database must contain identical distributed named marks.

Creating a Table for Log Marking

To mark the transaction log, you must execute a transaction against a table in the database. To do this, you can create a table specifically for use with log marking. This will allow you to mark your transaction logs without altering any of your Project Server or Windows SharePoint Services data.

This table will not contain any actual data. Its only purpose is to allow you to run a transaction against the database without changing any other data.

To add a table for use with log marking to your database, use SQL Server Query Analyzer to execute a script such as the following:

```
USE <database>

CREATE TABLE LogMarks
(
    logmark tinyint
)
GO

INSERT INTO LogMarks (logmark) VALUES (1)
GO
```

Run this script for each database that you will be backing up as part of your Project Server recovery plan. This includes your Windows SharePoint Services Content database, your main Project Server database, and any partitioned Project Server databases.

Using Stored Procedures to Mark the Logs

The easiest way to implement log marking in related databases is to create a stored procedure in each database that will create the marked transaction. A master stored procedure can then be created that runs each of the individual stored procedures simultaneously, causing the log marks to be synchronized.

In each SQL Server database in your deployment, add a stored procedure such as the following:

```
CREATE PROCEDURE sp_SetMark
@name nvarchar (128)
AS
BEGIN TRANSACTION @name WITH MARK
UPDATE <database>.dbo.LogMarks SET logmark = 1
COMMIT TRANSACTION
GO
```

This stored procedure creates a named mark in the transaction log for that database. To allow for synchronized recovery, create a stored procedure on one of the databases in your deployment similar to the following:

```
CREATE PROCEDURE sp_MarkAll
@name nvarchar (128)
AS
BEGIN TRANSACTION
EXEC spring.ProjectServer.dbo.sp_SetMark @name
EXEC bleecker.ProjectServerViews.dbo.sp_SetMark @name
EXEC astor.WSSConfigDB.dbo.sp_SetMark @name
EXEC astor.STS_astor_1.dbo.sp_SetMark @name
COMMIT TRANSACTION
GO
```

This stored procedure runs the **sp_SetMark** stored procedures on each of the databases in your deployment. This example assumes you have three computers running SQL Server in your deployment: the server Spring, containing the Project Server database; the server Bleecker, containing the Project Server View tables; and the server Astor, containing the Windows SharePoint Services Content and Configuration databases. When you run this stored procedure, it creates identical synchronized marks in the transaction logs on each of these databases. You can then recover each database to this mark in the future.

Note When using nested marked transactions such as those shown in the preceding example, SQL Server 2000 issues the warning “WITH MARK option only applies to the first BEGIN TRAN WITH MARK. The option is ignored.” This is not an error message; however, it can appear in event logs and can cause SQL Server Agent jobs to report as failed. To verify that your transaction logs are being properly marked, check the **logmarkhistory** table in the Msdb database.

Backing Up the Databases

It is recommended that you create a full backup of each Project Server and Windows SharePoint Services database each day.

► **To back up your Project Server deployment**

1. Back up each database in your deployment.

Note It is recommended that you also back up the Master and Msdb databases after you back up the other databases in your deployment.

2. Before backing up the transaction log, run a marked transaction that spans each database. (For example, execute the `sp_MarkAll` stored procedure. For more information about running a marked transaction that spans a database, see the topic **Using Stored Procedures to Mark the Logs** in Chapter 5, **Backing Up Your Deployment** of the *Microsoft Office Project Server 2003 Disaster Recovery Guide*.)
3. Back up the transaction log on each database.
4. Continue to back up the transaction log throughout the day.

Note You may want to mark the transaction logs at regular intervals. You can automate this process. For more information about automating transaction log marking, see the topic **Automating Transaction Log Marking** in Chapter 5, **Backing Up Your Deployment** in the *Microsoft Office Project Server 2003 Disaster Recovery Guide*.

Be sure to keep the full database backups and transaction log backups together; you will need both to restore all databases to a point of mutual consistency.

Important If you keep database backups for long periods of time, such as monthly or quarterly backups, you must also keep the transaction log backups immediately following the database backup. If you do not keep transaction log backups containing distributed marked transactions for each database in your deployment, you will not be able to restore your deployment to a consistent state.

Automating Transaction Log Marking

For much greater versatility in recovering your Project Server deployment, consider creating a SQL Server Agent job that executes a distributed marked transaction on all the databases in your deployment on a regular schedule.

If your databases are located on more than one instance of SQL Server, you will need to create administrator accounts on each instance of SQL Server that have identical user names and passwords, and configure SQL Server Agent to connect by using those accounts. You can use your system administrator account for this purpose if the passwords are the same for each instance of SQL Server.

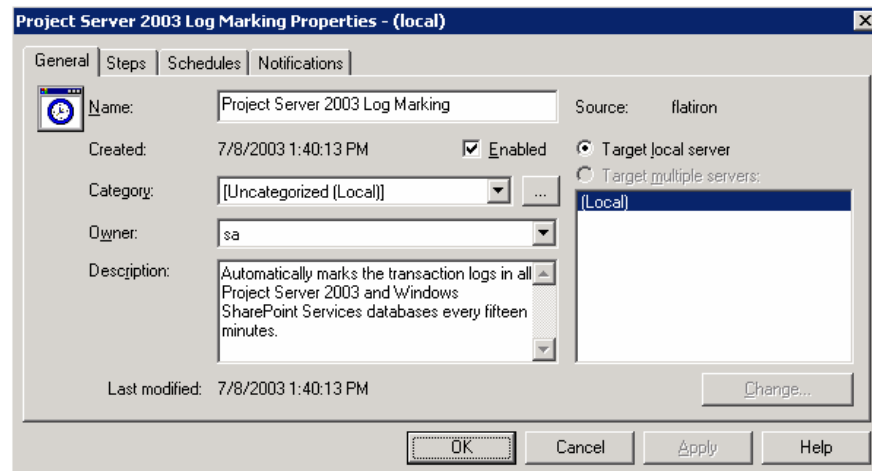
Note To configure SQL Server Agent connection settings, in Enterprise Manager, right-click **SQL Server Agent**, click **Properties**, and then specify the connection information on the **Connection** tab.

► **To schedule transaction log marking with SQL Server Agent**

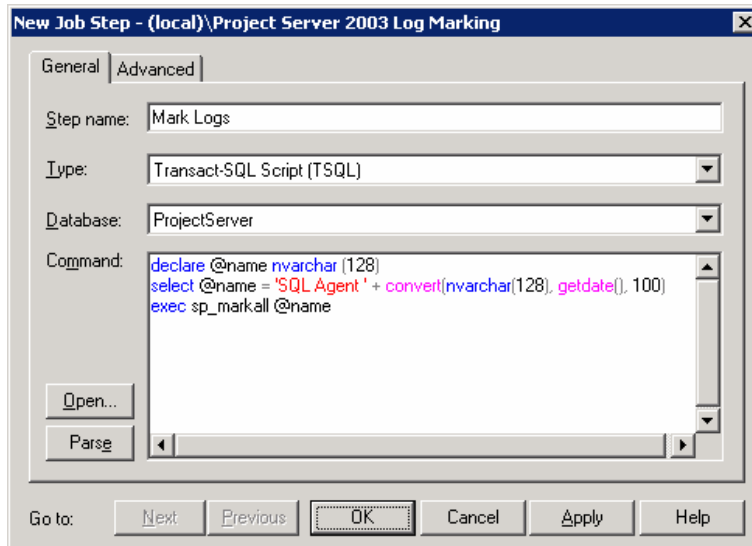
1. Open SQL Server Enterprise Manager.
2. Expand the server group, and then expand the server on which the master stored procedure for marking the transaction logs is located.

Note For more information about running a marked transaction that spans a database, see the **sp_MarkAll** stored procedure in the topic **Using Stored Procedures to Mark the Logs** in Chapter 5, **Backing Up Your Deployment** of the *Microsoft Office Project Server 2003 Disaster Recovery Guide*.

3. Expand **Management**, and then expand **SQL Server Agent**.
4. Right-click **Jobs**, and then click **New Job**.
5. On the **General** tab, type a name for the job in the **Name** box, choose a category from the **Category** list, and then type a description in the **Description** box.



6. On the **Steps** tab, click **New**.
7. In the **New Job Step** dialog box, type a name for the step in the **Step name** box, select **Transact-SQL Script (TSQL)** from the **Type** list, and then select the appropriate database from the **Database** list.



In the **Command** box, type the Transact-SQL statement that you want to use to mark the transaction logs. A statement such as the following can be used to create a unique name for the transaction log mark each time the job runs:

```
declare @name nvarchar (128)  
select @name = 'SQL Agent ' + convert(nvarchar(128), getdate(),  
100)  
exec sp_markall @name
```

8. In the **New Job Step** dialog box, click **OK**.
9. On the **Schedules** tab, click **New Schedule**.
10. In the **New Job Schedule** dialog box, type a name for the schedule in the **Name** box, and then click **Change**.
11. In the **Edit Recurring Job Schedule** dialog box, choose the schedule parameters you want to use with this job, and then click **OK**.

The screenshot shows a dialog box titled "Edit Recurring Job Schedule - (local)". The "Job name" is "Project Server 2003 Log Marking". Under the "Occurs" section, "Daily" is selected. The "Daily" frequency is set to "Every 1 day(s)". Under the "Daily frequency" section, "Occurs every:" is selected with a value of "15" and "Minute(s)". The "Starting at" time is "12:00:00 AM" and the "Ending at" time is "11:59:59 PM". Under the "Duration" section, "Start date:" is "7/ 8/2003" and "No end date" is selected. At the bottom are "OK", "Cancel", and "Help" buttons.

Note The more frequently you mark the transaction logs, the more versatile your recovery options. However, the server incurs some load from running the marked transactions.

12. In the **New Job Schedule** dialog box, click **OK**, and then on the **Schedules** tab, click **OK** to save the job.

Backing Up MSDE and WMSDE Deployments

If you are using Microsoft SQL Server 2000 Desktop Engine (Windows) (WMSDE) for your database server, you must manage your backup and restore processes by using the Osql tool. For more information about using the Osql tool to manage your MSDE databases, see Microsoft Knowledge Base article 325003 (<http://go.microsoft.com/fwlink/?LinkId=19688>).

If you are using Microsoft SQL Server 2000 Desktop Engine (Windows) (WMSDE) for your Windows SharePoint Services data or if you are using any combination of MSDE and SQL Server 2000 for different databases in your deployment, it is not possible to synchronize your databases during restore by using marked transactions. If you are using a combination of different database servers, you must shut down your Project Server deployment while you back up your databases if you want to be able to restore them to a point prior to the point of failure.

6

Recovering Your Deployment

This chapter covers the steps to take to recover your Microsoft® Office Project Server 2003 deployment from a system failure or disaster. Following any system failure or disaster, start with the basic recovery steps, then follow the steps for recovering specific parts of your Project Server 2003 deployment.

Basic Recovery Steps

Follow these basic recovery steps when recovering from a system failure or disaster.

► **To recover from a system failure or disaster**

1. Be sure your Project Server 2003 deployment is offline.

Note You can bring your deployment offline by stopping Internet Information Services (IIS) on the computer running the Project Server Front-End service and the computer running Microsoft Windows® SharePoint® Services.

2. Acquire suitable replacement hardware.
3. Reinstall Microsoft Windows and any required services packs and hotfixes.
4. Verify appropriate domain and network functionality.
5. If you are replacing an entire server, be sure to give it the same name as the original server.

Note If you are recovering more than one computer in your deployment, complete this procedure for each computer.

When you are finished replacing hardware and installing the operating system, proceed with recovering specific parts of your Project Server deployment.

Recovering a Computer Running SQL Server 2000

Follow these steps when recovering a computer running Microsoft SQL Server™ 2000.

► **To recover a computer running SQL Server**

1. Follow the procedure **To recover from a system failure or disaster** in the topic **Basic Recovery Steps** in Chapter 6, **Recovering Your Deployment** of the *Microsoft Office Project Server 2003 Disaster Recovery Guide*.
2. If necessary, install SQL Server 2000 and apply any appropriate service packs and hotfixes.

You can recover a computer running SQL Server 2000 to the point of failure or to an earlier point in time.

Recovering to the Point of Failure

To recover your database to the point of failure, you must be able to back up the currently active transaction log. If you cannot back up the currently active transaction log due to media failure or other problems, you have to recover the database to an earlier point in time.

Note For information about recovering the database to an earlier point in time, see the topic **Recovering to an Earlier Point In Time** in Chapter 6, **Recovering Your Deployment** of the *Microsoft Office Project Server 2003 Disaster Recovery Guide*.

► **To recover to the point of failure**

1. Back up the currently active transaction log.
2. Restore your backups of the Master and Msdb databases.
3. Restore the most recent full database backup.
4. Restore any differential database backups that were created since the most recent full backup.
5. Restore transaction log backups up to and including the log you backed up in step 1.
6. Recover the database.

Recovering to an Earlier Point in Time

If you are unable to back up the currently active transaction log after a system failure or disaster, recover the database to an earlier point in time. The procedures for this vary according to whether you are recovering a single-database deployment or a multiple-database deployment.

Recovering a Single-Database Deployment

If your Project Server deployment consists of a single Project Server database, you are not using Windows SharePoint Services, and you have not partitioned your database, you can recover to any specific point in time if you have transaction log backups that cover that time.

► **To recover to a specific point in time**

1. Restore your backups of the Master and Msdb databases.
2. Restore the most recent full database backup without recovering the database.
3. Restore any differential database backups that were created since the most recent full backup without recovering the database.
4. Apply each transaction log backup in the same sequence in which it was created.
5. Recover the database at the specified point in time within a transaction log backup.

Note For more information about recovering a database to a specific point in time, see the topic **Recovering to a Point In Time** in the Microsoft SQL Server Documentation on MSDN (<http://go.microsoft.com/fwlink/?LinkId=19690>).

Recovering a Multiple-Database Deployment

If your Project Server deployment includes Windows SharePoint Services, or if you have partitioned your Project Server database and you want to recover your database to a point prior to the point of failure, you must use marked transactions.

You must restore each database in your deployment to the same marked transaction. This includes your Project Server database and any partitioned databases, as well as your Windows SharePoint Services configuration database and content database.

► **To recover to a marked transaction**

1. Restore your backups of the Master and Msdb databases.
2. Restore the most recent full database backup.
3. Restore any differential database backups that were created since the most recent full backup.
4. Recover the database at the specified marked transaction within a transaction log backup. You must use the Transact-SQL **RESTORE LOG** statement and the **WITH STOPATMARK='mark_name'** clause to restore to a named mark.

Note For more information about recovering a database to a marked transaction, see the topic **Recovering to a Named Transaction** in *SQL Server 2000 Books Online*, or on the Microsoft Web site (<http://go.microsoft.com/fwlink/?LinkId=19691>).

5. Repeat steps 2 through 4 for each database in your deployment, recovering each to the same named mark.

Recovering a Computer Running Analysis Services

Follow these steps when recovering a computer running Analysis Services.

► **To recover a computer running Analysis Services**

1. Follow the procedure **To recover from a system failure or disaster** in the topic **Basic Recovery Steps** in Chapter 6, **Recovering Your Deployment** of the *Microsoft Office Project Server 2003 Disaster Recovery Guide*.
2. Install Analysis Services.
3. Recreate the user you were using for the online analytical processing (OLAP) administrator and add that user to the OLAP Administrators group.

Note If you create a new user, you must run the Project Server COM+ Settings tool (PSCOMPlus.exe) on the computer running the Project Server Front-End service and the View Processing service and specify the new user as the Analysis Services (OLAP) Access Identity.

4. Migrate the Analysis Services repository to a SQL Server database. If you are migrating the repository to the same database you used previously, drop and recreate the database to clear out any old data.
5. Rebuild the OLAP cube.

Recovering a Computer Running Windows SharePoint Services

Follow these steps to reinstall Windows SharePoint Services and connect to your existing database.

► **To recover a computer running Windows SharePoint Services**

1. Follow the procedure **To recover from a system failure or disaster** in the topic **Basic Recovery Steps** in Chapter 6, **Recovering Your Deployment** of the *Microsoft Office Project Server 2003 Disaster Recovery Guide*.
2. Recreate the account you used for the Windows SharePoint Services administrator in your original deployment.

Installing Windows SharePoint Services

Windows SharePoint Services is available only as a download from the Microsoft Web site. Follow this procedure to install Windows SharePoint Services.

► **To install Windows SharePoint Services**

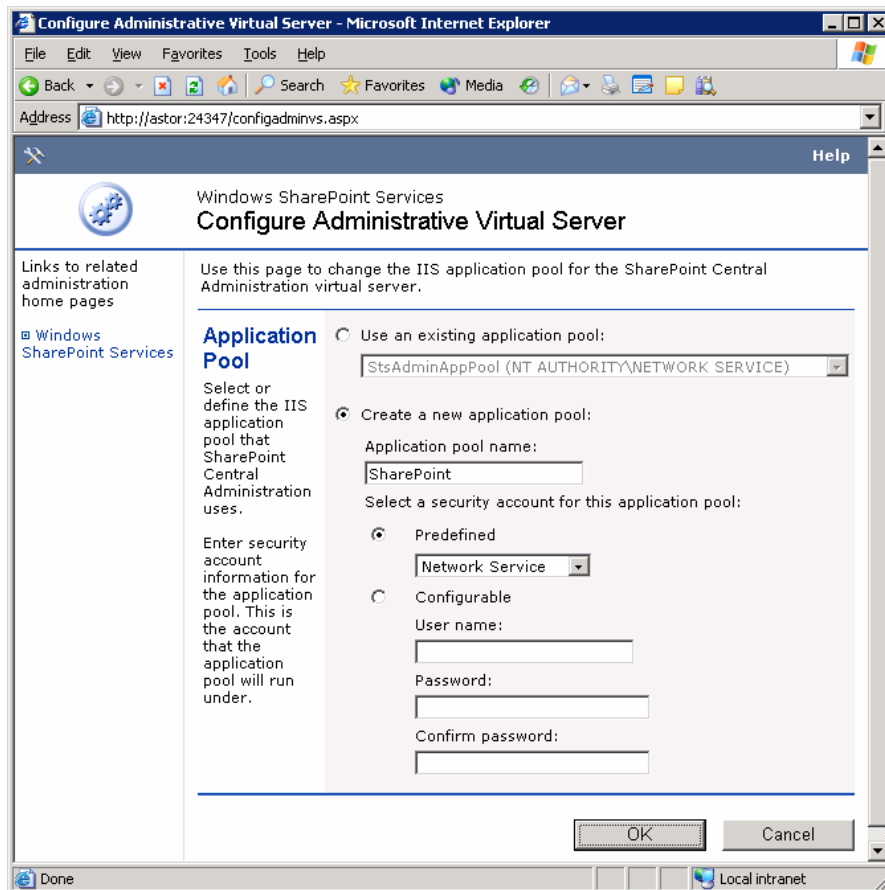
1. Go to Windows Update on the Microsoft Web site (<http://go.microsoft.com/fwlink/?LinkId=19686>).
2. In the left pane, expand **Pick updates to install**, and then click **Windows Server 2003 Family**.

3. Under **Recommended Updates**, click **Add** for the Windows SharePoint Services download.
4. Click **Review and install updates** to start the Windows SharePoint Services Setup program.
5. In the **End-User License Agreement (EULA)** dialog box, review the terms, select the **I accept the terms in the License Agreement** check box, and then click **Next**.
6. In the **Type of Installation** dialog box, select the **Server Farm** option, and then click **Next**.
7. In the **Summary** dialog box, verify that only Windows SharePoint Services will be installed, and then click **Install**.

Setup runs and installs Windows SharePoint Services. When Setup completes, a browser launches, and the **Configure Administrative Virtual Server** page is displayed.

Configuring the Administrative Virtual Server

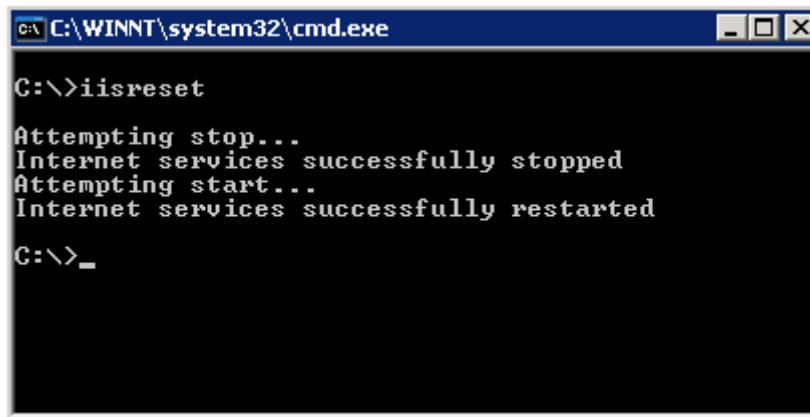
After the setup process is complete, you can configure your administrative virtual server, specifying an application pool to use for the virtual server processes.



The Configure Administrative Virtual Server page.

► **To configure the administrative virtual server**

1. On the Configure Administrative Virtual Server page, click **Create a new application pool**, and keep the default application pool in the list.
2. In the **Application pool name** box, type a name for the application pool.
3. Click **Predefined**, and then choose **Network Service** from the list.
4. Click **OK**.
The Application Pool Changed page appears.
5. On your Windows desktop, click **Start**, click **Run**, and then in the **Open** box, type **cmd** and click **OK**.
6. At the command prompt, type **iisreset**, and then press ENTER.

A screenshot of a Windows command prompt window. The title bar reads "C:\WINNT\system32\cmd.exe". The command prompt shows the following text:

```
C:\>iisreset  
Attempting stop...  
Internet services successfully stopped  
Attempting start...  
Internet services successfully restarted  
C:\>_
```

7. When Internet Information Services (IIS) restarts, close the command prompt window and return to your browser.
8. On the Application Pool Changed page, click **OK**.

Setting the Configuration Database Server

Use the Set Configuration Database Server page to connect your new Windows SharePoint Services installation to an existing configuration database.

Set Configuration Database Server - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media

Address http://astor:24347/configdb.aspx

Windows SharePoint Services
Set Configuration Database Server

Links to related administration home pages

- Windows SharePoint Services

Use this page to create or connect to a SharePoint configuration database. The configuration database stores settings for all of the SharePoint sites and virtual servers. This database must exist before you can create any new sites or perform administration tasks.
* Indicates required field.

Configuration Database

Enter the SQL Server and connection settings to create or connect to a configuration database.

Database server: *
flatiron

SQL Server database name: *
WSSConfigDB

Database connection type: *

- Use Windows authentication (recommended security level)
- Use SQL authentication (less secure)

Database account user name: *
Database account password:

Connect to existing configuration database

Active Directory Account Creation

Specify whether to use existing accounts for users, or whether to automatically create accounts for users in the active directory.

Specify the domain and organizational unit in which user accounts will be created. Make sure that the configuration user has permissions to create users in the active directory.

- Users already have domain accounts. Do not create active directory accounts.
- Automatically create active directory accounts for users of this site.

Active Directory Domain:

Done Local intranet

The Set Configuration Database Server page.

- ▶ **To set the configuration database server**
 1. In the **Database server** box, type the name of the instance of SQL Server 2000 to which you want to connect.
 2. In the **SQL Server database name** box, type the name of the existing configuration database.
 3. Under **Database connection type**, click **Use Windows authentication (recommended security level)**.
 4. Select the **Connect to existing configuration database** check box.
 5. Click **OK**.

Extending the Virtual Server

After you set up the connection to SQL Server 2000, you can extend your virtual servers to use Windows SharePoint Services.

► **To extend the virtual server**

1. On the **Central Administration** page, click **Extend and map to another virtual server**.
2. On the **Virtual Server List** page, click **Default Web Site**.
3. On the **Extend and Map to Another Virtual Server** page, click the **Create a new application pool** option.
4. In the **Application pool name** box, type a name for the application pool.
5. Select the **Predefined** option, and then choose **Network Service** from the list.
6. Click **OK**.

Creating a Windows SharePoint Services Administrator

To enable Project Server to access Windows SharePoint Services, you must create a Windows SharePoint Services administrator on the computer running Windows SharePoint Services. To do this, add the account you originally used for this purpose to the Administrators group on the computer running Windows SharePoint Services.

Note If you are restoring Windows SharePoint Service to an existing Project Server deployment and you want to use a different account for your Windows SharePoint administrator, you must run PSCOMPlus.exe on the computer running Project Server 2003 to update that computer with the new account information. For more information about running PSCOMPlus.exe, see the topic **Project Server COM+ Settings Tool** in Appendix B, **Project Server Installation Tools** of the *Microsoft Office Project Server 2003 Installation Guide*.

► **To create a Windows SharePoint Services administrator**

1. On the computer running Windows SharePoint Services, open Computer Management.
2. In the console tree, click **Groups**.
3. Right-click **Administrators**, and then click **Properties**.
4. Click **Add**.
5. In the **Enter the object names to select** box, type the name of the Windows account that you want to add to the group, and then click **OK**.
6. Click **OK**.

Updating Project Web Access Settings

When you reinstall Windows SharePoint Services, a new port is chosen for the SharePoint Central Administration page. You must update the SharePoint Central Administration Uniform Resource Locator (URL) in Microsoft Office Project Web Access 2003 with the new information.

► **To update Project Web Access settings**

1. Log on to Project Web Access as an administrator.
2. Click the **Admin** tab.
3. In the side pane under **Actions**, click **Manage Windows SharePoint Services**.
4. In the **SharePoint Central Administration URL** box, type the server name and port number for the Windows SharePoint Services Central Administration page.
5. Click **Save Changes**.

Recovering a Computer Running Project Server 2003

When you are recovering a computer running one or more of the Project Server services, you must run the Project Server Setup program. Use the documentation you created when you originally deployed Project Server 2003 to guide you when recovering.

Note For detailed information about running the Project Server Setup program, see the *Microsoft Office Project Server 2003 Installation Guide* (<http://go.microsoft.com/fwlink/?LinkId=20233>).

► **To recover a computer running the Session Manager service**

1. Follow the procedure **To recover from a system failure or disaster** in the topic **Basic Recovery Steps** in Chapter 6, **Recovering Your Deployment** of the *Microsoft Office Project Server 2003 Disaster Recovery Guide*.
2. Install the Project Server Session Manager service.
3. If you installed the Session Manager service on a computer that has a different name than the original server, uninstall and then reinstall the Project Server Front-End service and specify the new computer name on the **Enter the Session Manager server name** page of the Project Server Setup wizard.

► **To recover a computer running the View Processing service**

1. Follow the procedure **To recover from a system failure or disaster** in the topic **Basic Recovery Steps** in Chapter 6, **Recovering Your Deployment** of the *Microsoft Office Project Server 2003 Disaster Recovery Guide*.
2. Install the Project Server View Processing service.
3. If you are using Analysis Services:
 - a. Install the Analysis Services Decision Support Objects.

- b. Create an account with the same user name and password as the OLAP administrator on the computer running Analysis Services.
- c. Add the new account to the OLAP Administrators group on the computer running the View Processing service.
4. If you installed the View Processing service on a computer that has a different name than the original server, uninstall and then reinstall the Project Server Front-End service and specify the new computer name on the **Enter the View Processing server information** page of the Project Server Setup wizard.

► **To recover a computer running the Front-End service**

1. Follow the procedure **To recover from a system failure or disaster** in the topic **Basic Recovery Steps** in Chapter 6, **Recovering Your Deployment** of the *Microsoft Office Project Server 2003 Disaster Recovery Guide*.
2. Run the Project Server Setup program.
3. On the **Connect to a Web Server Running Microsoft Windows SharePoint Services** page, choose the **Enter this information later** option.

Important You must choose the **Enter this information later** option; if you do not, the site address URLs for the published projects will be deleted.

4. Complete the Project Server Setup process.
5. Reconnect to the server running Windows SharePoint Services by using Project Web Access.

► **To recover a computer running all services**

1. Follow the procedure **To recover from a system failure or disaster** in the topic **Basic Recovery Steps** in Chapter 6, **Recovering Your Deployment** of the *Microsoft Office Project Server 2003 Disaster Recovery Guide*.
2. Run the Project Server Setup program.
3. On the **Choose the services you want to install on this server** page, choose to install all services. (This is the default.)
4. On the **Enter database server information** page, select the **Connect to another existing database** option, and then enter the information for your existing Project Server database.
5. On the **Connect to a Web Server Running Microsoft Windows SharePoint Services** page, choose the **Enter this information later** option.

Important You must choose the **Enter this information later** option; if you do not, the site address URLs for the published projects will be deleted.

6. Complete the Project Server Setup process.

7. Reconnect to the server running Windows SharePoint Services by using Project Web Access.

Appendices



Microsoft Office
Project

Enterprise Project Management Solution

A

Additional Resources

If you want to learn more about Microsoft® Office Project Server 2003, Microsoft Office Project Web Access 2003, and Microsoft Office Project Professional 2003, or how to use these three applications as part of your organization's Microsoft Office Enterprise Project Management (EPM) Solution, please refer to the following online books, planning and training guides, and Web sites.

Microsoft Office Project Server 2003 Online Books Series

- *Microsoft Office Project Server 2003 Solution Planning Guide*
<http://go.microsoft.com/fwlink/?LinkId=33654>
- *Microsoft Office Project Server 2003 Configuration Planning Guide*
<http://go.microsoft.com/fwlink/?LinkId=20235>
- *Microsoft Office Project Server 2003 Disaster Recovery Guide*
<http://go.microsoft.com/fwlink/?LinkId=20234>
- *Microsoft Office Project Server 2003 Installation Guide*
<http://go.microsoft.com/fwlink/?LinkId=20233>

This includes the following resources:

- *Microsoft Office Project Server 2003 Installation Guide: Single Server Deployment*
- *Microsoft Office Project Server 2003 Installation Guide: Small Scale Deployment*
- *Microsoft Office Project Server 2003 Installation Guide: Medium Scale Deployment*
- *Microsoft Office Project Server 2003 Application Configuration Guide*
<http://go.microsoft.com/fwlink/?LinkId=20237>
- *Microsoft Office Project Server 2003 Administrator's Guide*

<http://go.microsoft.com/fwlink/?LinkID=20236>

- *Microsoft Office Project Server 2003 Security Group Guide*

<http://go.microsoft.com/fwlink/?LinkID=33554>

This includes the following resources:

- *Microsoft Office Project Server 2003 Portfolio Managers Guide*
- *Microsoft Office Project Server 2003 Project Managers Guide*
- *Microsoft Office Project Server 2003 Resource Managers Guide*
- *Microsoft Office Project Server 2003 Team Leads Guide*
- *Microsoft Office Project Server 2003 Team Members Guide*
- *Microsoft Office Project Server 2003 Executives Guide*

Project Server–Related Web Sites

The following Web sites are also available:

- Microsoft Office Project Server 2003 Software Development Kit
<http://go.microsoft.com/fwlink/?LinkID=20238>
- Microsoft Office Online: <http://www.office.microsoft.com>

Send us your feedback. Please let us know what you think about the quality of this content. If this text does not meet your needs, let us know how we can improve it. If this text was helpful to you, let us know how it helped.

<mailto:proidocs@microsoft.com?subject=Feedback: Microsoft Office Project Server 2003 Disaster Recovery Guide>

B

Project Server Recovery Tools

This appendix describes tools that are available to administrators of Microsoft® Office Project Server 2003. These tools can be used in day-to-day post-deployment operations.

Restore Single Project Tool

You can restore a single project to an earlier state by using the Restore Single Project tool (RestoreP.exe). To use RestoreP.exe, you must restore a backup of the Project Server database under a different name to the same server on which your main Project Server database is located. You can then use RestoreP.exe to copy an earlier version of a particular project to your production database.

Note RestoreP.exe will not work with a Microsoft Project Server 2002 database.

If you are using Microsoft Windows® SharePoint® Services as part of your Project Server deployment, you must restore a backup of Windows SharePoint Services to a point consistent with that of your Project Server backup, and then use the Windows SharePoint Services Site Migration tool (WSSMigr.exe) to back up an individual site and restore it to your production database.

To successfully restore a project, you need the following:

- Database backups for each database in your deployment. If you have more than one database in your deployment (for example, Project Server and Windows SharePoint Services), you must also have transaction log backups that contain named marks.

Note For more information about creating database backups, see Chapter 5, **Backing Up Your Deployment**, in the *Microsoft Office Project Server 2003 Disaster Recovery Guide*.

- Sufficient hard disk space to restore the database backups on your production computers.

► **To restore a single project**

1. Download the file RestoreP.exe from the Microsoft Download Center: (<http://go.microsoft.com/fwlink/?LinkId=21137>).

Important The version of RestoreP.exe included on the Project Server 2003 CD has been superseded by the version available from the Microsoft Download Center. Use the version from the Microsoft Download Center.

2. Run RestoreP.exe.
3. Back up your existing deployment by using the methods described in Chapter 5, **Backing Up Your Deployment**, in the *Microsoft Office Project Server 2003 Disaster Recovery Guide*.
4. Restore the databases containing the project you want to restore. You must restore these databases under a different name on the same servers than your production databases. If you are restoring multiple databases, you must recover to a marked transaction. For more information, see Chapter 6, **Recovering Your Deployment**, in the *Microsoft Office Project Server 2003 Disaster Recovery Guide*.
5. On the computer containing the main Project Server database, run RestoreP.exe.
6. On the computer running Windows SharePoint Services, configure your restored Windows SharePoint Services database to run on a virtual server. For more information, see the topic **Configuring the Windows SharePoint Services Database** in Appendix B, **Project Server Recovery Tools**, in the *Microsoft Office Project Server 2003 Disaster Recovery Guide*.
7. Move the desired Windows SharePoint Services site to your production database by using the procedure in the topic **Copying the Windows SharePoint Services Site** in Appendix B, **Project Server Recovery Tools**, in the *Microsoft Office Project Server 2003 Disaster Recovery Guide*.

When you have restored the project and verified the functionality, you can remove the restored databases and the Windows SharePoint Services virtual server.

Running the Restore Single Project Tool

RestoreP.exe restores a single project from a Microsoft Project Server database. Before you can use RestoreP.exe, you must add a stored procedure to the Project Server database that you will be restoring to.

► **To add the single project restore stored procedure**

1. Open Microsoft SQL Server™ Query Analyzer.

2. Execute the RestoreP.sql script on the database on which you want to restore the project.

The MSP_RESTORE_PROJECT stored procedure is added to the database.

After you run the RestoreP.sql script, you can run RestoreP.exe. RestoreP.exe uses the following syntax:

```
restorep.exe -s server_name [-u user_name -p user_password | -e] -f
source_db_name -d dest_db_name -i proj_id -n projname [-y]
```

RestoreP.exe uses the following command-line parameters:

Parameter	Description
-s	SQL Server name (both databases must reside in the same server)
-u	User name (must have write permissions on both databases)
-p	User password
-e	Use trusted connection
-f	Source database (located where the backed up project is)
-d	Destination database (the database to which the project should be restored)
-i	Project ID of the project to restore
-n	Project name
-y	Force copying of project data; minimal validation performed

Configuring the Windows SharePoint Services Database

Because the Windows SharePoint Services Stsadm.exe tool cannot access data directly from a SQL Server database, you must connect the restored Windows SharePoint Services database to a virtual server. Follow the procedures in this topic to configure the Windows SharePoint Services database that you restored.

► To create a new virtual server

1. On the **Start** menu, click **Run**.
2. In the **Open** box, type **Inetmgr** and then click **OK**.
The Internet Information Services Manager starts.
3. In the left pane, expand the tree until you see the **Web Sites** folder.

4. Click the **Web Sites** folder and on the **Action** menu, click **New**, and then click **Web Site**.
5. In the Web Site Creation Wizard, click **Next**.
6. On the **Web Site Description** page, type a description (for example, SharePoint Restored Database), and then click **Next**.
7. On the **IP Address and Port Settings** page, change the TCP port to a value such as 4444, and then click **Next**. This number must be unique. Do not use 80 or any other port you have previously defined for a Web site.
8. On the **Web Site Home Directory** page, click **Browse**. On the drive on which Microsoft Windows is installed, find and select the Inetpub folder.
9. Click **Make New Folder**. Type **Restore**, and then click **OK**.
10. Click **Next**.
11. On the **Web Site Access Permissions** page, click **Next**.
12. Click **Finish**.
13. Close IIS Manager.

► **To give application pool ID permissions on the new database**

1. Open SQL Server 2000 Enterprise Manager.
2. In the tree view, expand the tree to open the **Security** folder, and then click **Logins**.
3. In the right pane, double-click **NT Authority\Network Service**.

Note If the login does not exist, you must add the account as a login. To do this, right-click **Logins**, and then select **New Login**.

4. Click the **Database Access** tab.
5. Select the check box next to the SharePoint database you restored previously.

Note Do not change the access settings for any of the other databases.

6. Select **db_owner** for the database role, and then click **OK**.
7. Close SQL Server Enterprise Manager.

► **To extend the Windows SharePoint Services site and add the restored database**

1. On the **Start** menu, point to **Administrative Tools**, and then click **SharePoint Central Administration**.
2. Click **Configure Virtual Server Settings**.
3. On the Virtual Server List page, click the virtual server that you created (for example, SharePoint Sample Database).
4. On the Extend Virtual Server page, click **Extend and create a content database**.

5. In the **Application Pool** section, in the **Application pool name** box, type a name for the application pool (for example, **WSSRestoreAppPool**).
6. Click **Predefined**, and choose **Network Service** from the list.
7. In the **Site Owner** section, type a domain and user name in the **User Name** box. This account must have access to this computer.
8. In the **E-Mail** box, type an e-mail address for the site owner, and click **OK**.
9. On the **Virtual Server Successfully Extended** page, click **OK**.
10. Under **Virtual Server Management**, click **Manage content databases**.
11. Under **Content Databases**, click **Add a content database**.
12. Under **Database Information**, select the **Specify database server settings** option, and then type the name of the restored Windows SharePoint Services database in the **Database name** box.
13. Type a user name and password to use to access the database.
14. Enter values in the **Number of sites before a warning event is generated** and **Maximum number of sites that can be created in this database** boxes, such as 1000 and 1500.
15. Click **OK**.

Copying the Windows SharePoint Services Site

The Windows SharePoint Services database that you restored contains the site associated with the project you are restoring. To copy that site from the restored database to your production Windows SharePoint Services database, use WSSMigr.exe to back it up to a file. You can then restore that backup to your production database.

► To copy the Windows SharePoint Services Site

1. Back up the site associated with the project you are restoring. Use WSSMgr.exe with the following syntax:

```
WSSMigr.exe -bo -w http://<SharePointRestoreServer>/sites -f
c:\<BackupFolder>
-i <ProjectID>
-dbserver <SQLServer>
-dbname <ProjectServerDB>
```

where *BackupFolder* is the folder in which the backup file should be created, *SharePointRestoreServer* is the Windows SharePoint Services server on which the site you want to restore is located, *ProjectID* is the ID of the project you are restoring, *SQLServer* is the database server, and *ProjectServerDB* is the Project Server database containing the project you are restoring.

2. Restore the site you just backed up to your production database. Use WSSMgr.exe with the following syntax:

```
WSSMigr.exe -ro -w http://<SharePointProductionServer>/sites -f  
c:\ <BackupFolder>
```

where *SharePointProductionServer* is the Windows SharePoint Services server on which you are restoring the project, and *BackupFolder* is the folder you specified when you created the backup.