



Wasabi Storage Builder® for IP-SAN and Disk-based Backup

Disk-based backup solves many of the problems that plague IT administrators by providing increased performance, reliability, and ease of use relative to traditional backup methods. Microsoft® Data Protection Manager and Wasabi Storage Builder® for IP-SAN delivers a low-cost, yet powerful backup solution that protects critical data, with the flexibility and scalability to meet storage needs now and in the future.

Backup Pain Points

A surprising number of organizations do not have a comprehensive and methodical backup process, leaving them at risk of loss of critical data. The reasons given for not backing up data include the cost of the backup system, difficulty in managing backups (especially if there are multiple servers in the network), and the management resources required to perform and monitor the backups.

Even those organizations that do have a backup process in place face issues on a daily basis. Tape backup, the traditional method for backing up data, presents its own set of problems. Complaints by IT managers about tape backup include the length of time required to perform the backup and restore operations, trouble managing and tracking the backup tapes, and the difficulty of verifying the success of backup and restore operations. If there are multiple servers in a network, the problem of backing up data becomes even more complex.

Disk-based Backup Eases the Pain

It is clear that a faster, efficient, and more reliable method of backing up data is required. Disk-based backup, in which systems use hard disks instead of tape to store the backup data, is quickly becoming the backup method of choice for many IT managers. Disk-based backup solves the problems of those who do not consistently backup because of cost or management factors, as well as the problems associated with backing up to tape.

Disk-based backup delivers:

- **Performance.** Hard disk drives are faster than tapes, decreasing the amount of time it takes to backup and restore data. Just as finding and playing a particular song on an MP3 player is much faster and easier than with a cassette player, finding a particular file or group of files is much quicker with disk-based backup.
- **Reliability.** The hard disks in a disk-based backup system are configured so that no data is lost even if one or more of the individual hard disks fail. If a tape fails, all data on that tape is lost.
- **Scalability.** A disk-based backup system can easily scale as an organization's backup needs grow.

Tape can be a single point of failure, meaning that if a tape fails all of the data on that tape is lost. Disk-based backup provides enhanced data protection by using RAID technology. RAID is an acronym for Redundant Array of Independent (or Inexpensive) Disks. It is a technology that allows for a combination of two or more hard disks to deliver increased fault tolerance and performance compared to what could be achieved with one drive or simply aggregating multiple drives in a JBOD (Just a Bunch of Disks) configuration. Fault tolerance is the ability of the RAID array to withstand the failure of a hard disk drive such that the storage system remains functional and no data is lost. With disks in a RAID

array, even if a hard disk fails the data is still intact and the backup device remains functional.

Disk-based backup also delivers exceptional performance. Recovering data from a disk-based backup is as simple as locating the needed file or files and copying the needed data to the correct location on the production server. Contrast this with file recovery from a tape backup, which entails locating the proper tape and then forwarding or rewinding the tape to the point where the file is located.

Disk-based Backup Using Microsoft® Data Protection Manager

Microsoft Data Protection Manager (DPM) delivers disk-based backup protection for Windows Server 2003 and Server 2000 servers. Microsoft DPM provides near-continuous protection which eliminates the problem of backup windows being too short, or even non-existent. DPM only copies bytes that have been changed since the last backup, minimizing the load on the servers being backed up. The frequency of backups can be scheduled and different schedules can be set for different servers if so desired.

DPM uses the Windows® Server 2003 Volume Shadow Copy Services (VSS) to take point-in-time snapshots of data at specified intervals and replicates those snapshots to the DPM server. This enables recovery of deleted, modified, or corrupted files by rolling back to a previously saved version of the file. If a server or its hard disks fail, a copy of the data still exists on the DPM server.

Data on the DPM server can be backed up to tape for archival purposes. Backing up data from the DPM server rather than the production servers themselves minimizes disruption to the production servers. This eliminates the need to perform tape backups at night or on the weekends, reducing the need for network administrators during off-hours.

DPM monitors its backup jobs to ensure that they complete without error. If an error is detected, DPM has a two-stage error correction process. First, DPM automatically validates the replica against the production server to ensure that the replication is consistent and has occurred as planned. Second, if inconsistencies between a data source and its replica are found during validation, the fix-up activity re-sends the object(s) from the data source to the replica.

DPM further reduces administrative tasks by enabling end users to recover their own files. A user can see previous versions of a file on a DPM-protected share by clicking on the properties of the file. They can then view the older versions and restore the file or copy it to a new file, if desired.

iSCSI Storage

As shown above, IT managers are looking for a backup solution that is cost-effective, easy to manage, has good performance, and is robust and reliable. It would be reasonable to expect the storage component of a disk-based backup solution to have these same attributes, making iSCSI storage a logical choice for a disk-based backup solution.

iSCSI stands for Internet Small Computer System Interface. iSCSI works by sending SCSI data packets over Ethernet. Using standard Ethernet cables, adapters, and switches it is possible to build a low-cost IP-based Storage Area Network (IP-SAN). An IP-SAN uses iSCSI as its data transmission protocol.

IP-SAN storage provides the performance, reliability, and scalability that is required for disk-based backup. It opens up new opportunities for OEMs, Systems Integrators, and VAR's who offer data storage and backup solutions.

IP-SAN storage is:

Cost-effective

An IP-SAN uses standard Ethernet components. It does not require expensive specialized hardware.

Secure

Support for leading RAID controllers keeps data secure and maximizes system uptime.

Easy-to-use

IP-SAN uses TCP/IP, which is widely used and understood.

Scalable

IP-SAN storage targets can be connected to a standard Ethernet switch. If more storage is needed, it is easy to deploy additional iSCSI targets – just plug a new IP-SAN target into the switch.

Flexible

IP-SAN storage can be allocated for use by multiple servers, making more efficient use of disk capacity and making storage management less complex.

Extensible

Using Ethernet and the internet infrastructure, iSCSI storage targets can be located next to a server, in the next room, or even around the world.

Wasabi Storage Builder® for IP-SAN

Wasabi Storage Builder for IP-SAN software enables VAR's, OEMs and systems integrators to transform off-the-shelf computer hardware into a cost-effective IP-SAN (iSCSI) storage for disk-based backup systems. It's a complete turnkey software solution pre-installed on a bootable Compact Flash disk.

Storage Builder for IP-SAN runs on standard hardware components such as Xeon, Pentium 4, and AMD CPU's; Intel, Supermicro, and Tyan motherboards; and 3ware and LSI RAID controllers and lets VAR's, Systems Integrators, and OEM's take advantage of the performance improvements and cost reductions offered by using commodity hardware components.

Storage Builder opens up new windows to the high-growth disk-based backup market with cost-effective IP-SAN storage solutions that provide security, scalability, and flexibility.

Storage Builder for IP-SAN contains all of the software needed to build an IP-SAN target in a reliable Compact Flash Disk-On-Module (DOM). No other software needs to be purchased or installed. This significantly speeds up the installation and assembly process.

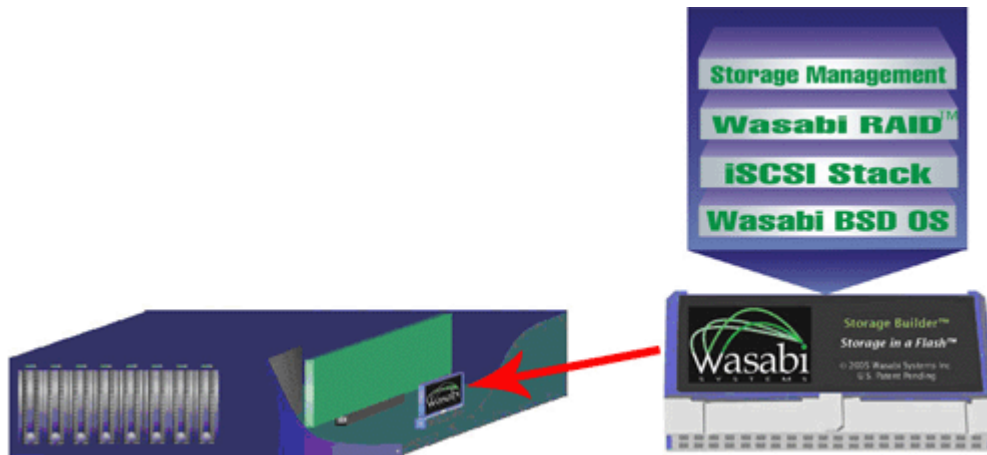


Figure 1: All of the software, including operating system, iSCSI software, and management utility, are pre-installed on a bootable Compact Flash Disk-On-Module (DOM). Just plug the DOM into the IDE port on the motherboard, and it's ready to go.

Storage Builder for iSCSI includes a powerful configuration and management Graphical User Interface (GUI). The Storage Builder GUI runs in a standard web-browser and does not require the installation of any software on the clients (other than the web browser). The GUI can be password-protected to prevent unwanted access.

Once logged into the GUI, all management and configuration tasks can be performed, including network settings, security parameters, and storage configuration and allocation. The Storage Builder GUI even communicates directly with supported RAID controllers so there is no need to use a separate application to perform tasks such as creating, deleting, and rebuilding arrays, checking array status, and setting RAID controller parameters like rebuild/verify rate and cache policy.

E-mail alerts provide immediate notification of logical disk errors or if hard disk S.M.A.R.T. thresholds are exceeded so that problems can quickly be corrected. For supported chassis and motherboard combinations the temperature, power supply and drive status are monitored and fan speed is automatically adjusted to maintain chassis temperatures within specifications.

Storage Builder for IP-SAN is not only a good storage solution for DPM disk-based backup, it is also an excellent storage solution for the servers in the network. The diagram below shows a Storage Builder for IP-SAN being used to store the data for the DPM-protected servers. An additional Storage Builder IP-SAN is being used for the DPM backup data. By consolidating storage the end user will attain improved scalability, more efficient use of disk space, and easier management and maintenance.

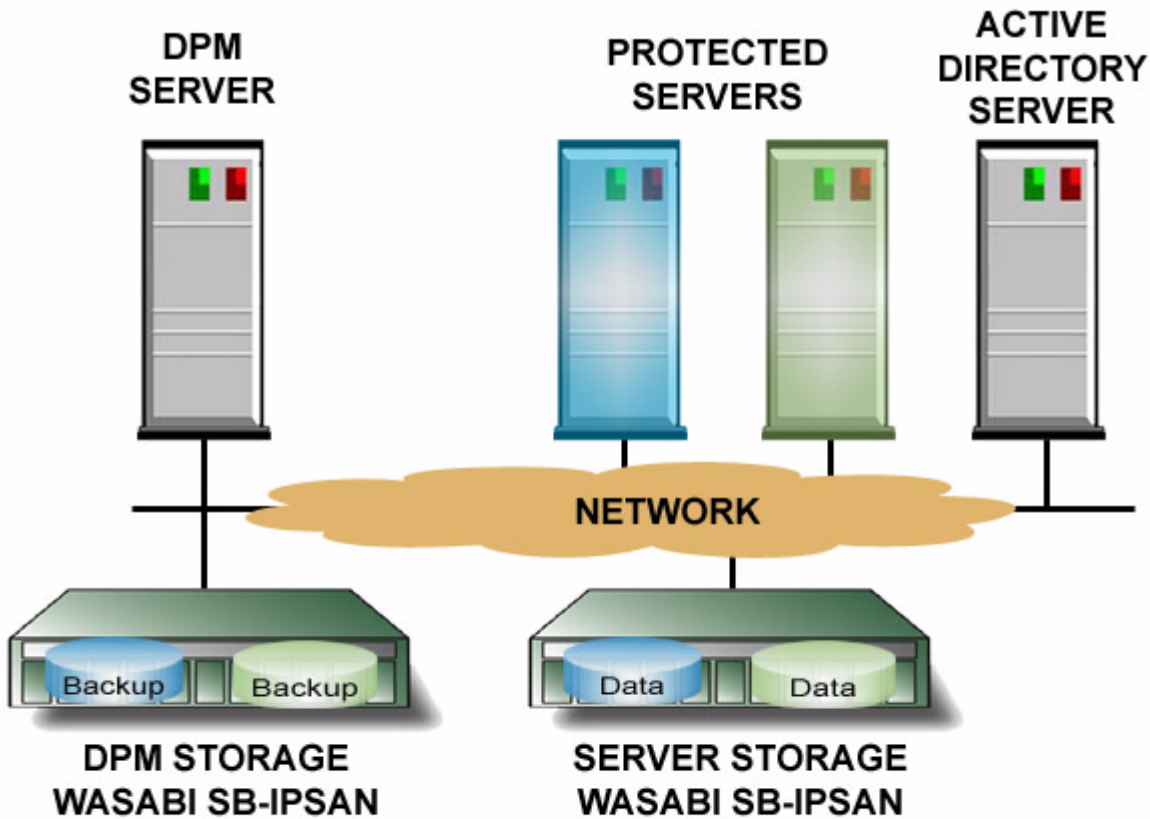


Figure 2: Storage Builder for IP-SAN being used to store the data for the DPM-protected servers.

Using Wasabi Storage Builder for IP-SAN with Microsoft Data Protection Manager

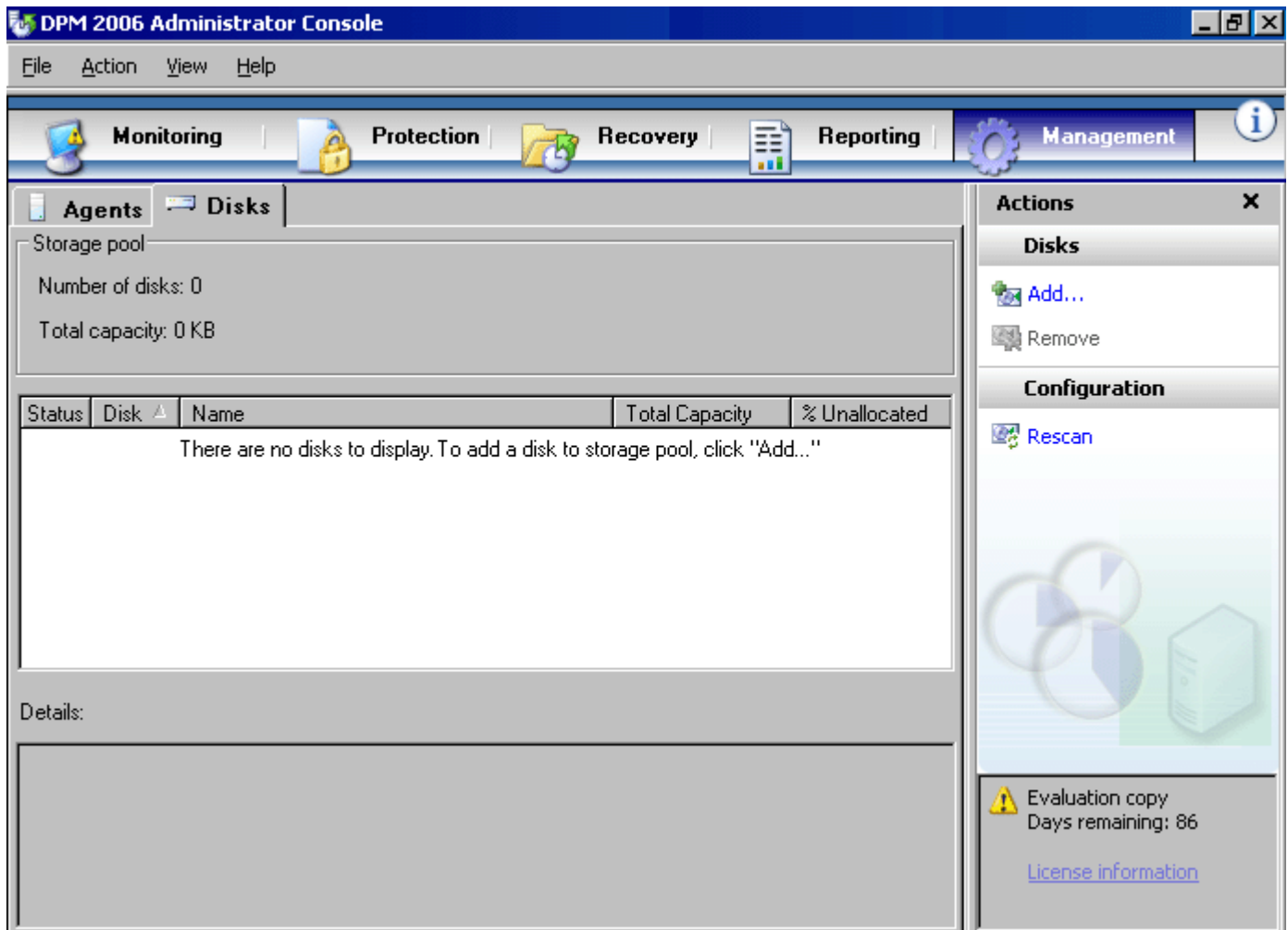
Microsoft Data Protection Manager (DPM), in conjunction with Wasabi Storage Builder for IP-SAN, delivers a disk-based backup system that is fast, reliable, robust, and yet simple to manage and incredibly affordable.

The Data Protection Manager installation assumes that the user has basic familiarity with setup and configuration of Wasabi Storage Builder for IP-SAN, Microsoft Windows Server 2003, and Active Directory.

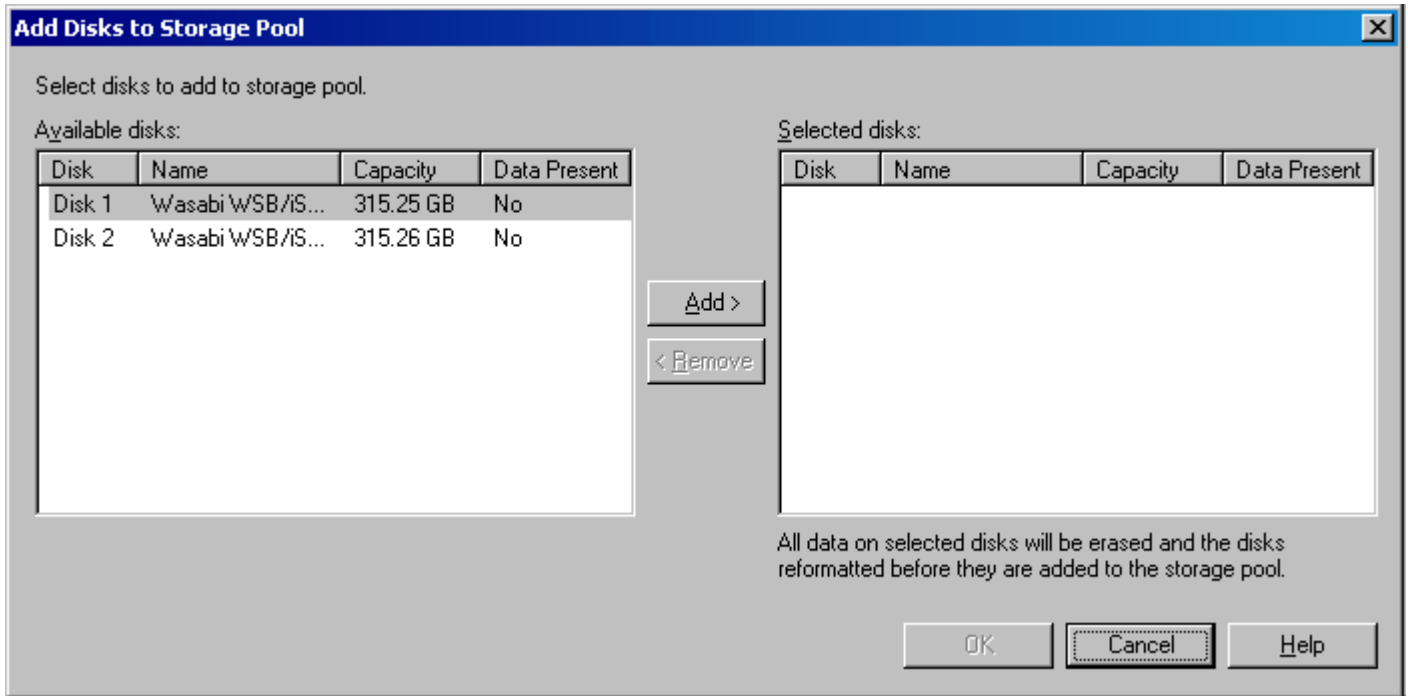
These steps also assume that the DPM software has already been installed, the Storage Builder for IP-SAN system has been configured, and the DPM server is connected to the Storage Builder for IP-SAN target.

DPM Configuration

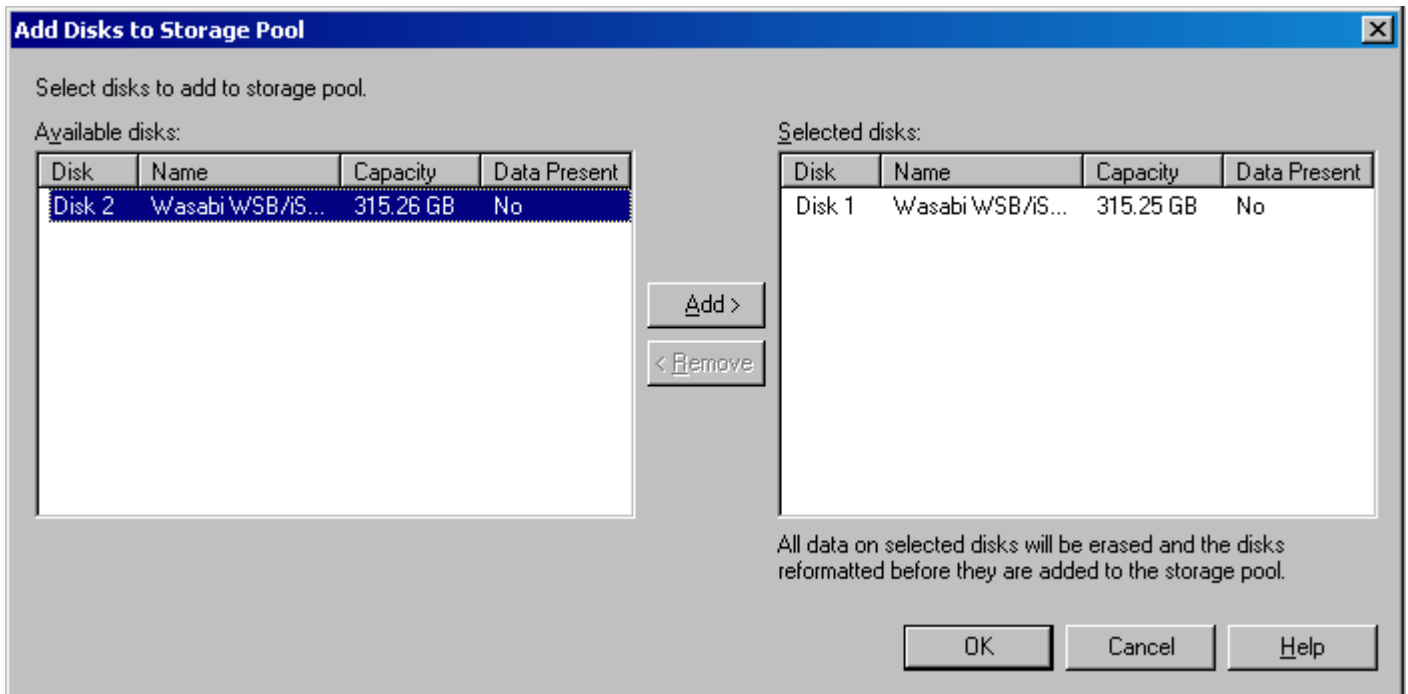
1. Make sure that the DPM server's iSCSI initiator is connected to the Storage Builder target.
2. After installing DPM, start the DPM Administrator Console.



3. Click the **Management** tab
4. Click the **Disks** tab
5. In the **Actions** pane, under Disks, click **Add...**



- Highlight the disk(s) that you want to make available for DPM to use to store backup data and then click the **Add>** button. Do this for all disks that you want to make available for storage.



- When you are finished adding the disk(s) click **OK**. A summary screen displays the disks that have been added.

DPM 2006 Administrator Console

File Action View Help

Monitoring Protection Recovery Reporting Management

Agents **Disks**

Storage pool

Number of disks: 1

Total capacity: 315.25 GB

Allocated for protection: 0 GB

Unallocated: 315.25 GB

Status	Disk	Name	Total Capacity	% Unallocated
✓	Disk 1	Wasabi WSB/iSCSI Multi-Path Disk Device	315.25 GB	100 %

Details:

Name: Wasabi WSB/iSCSI Multi-Path Disk Device
Status: Healthy
Allocated for protection: 0 GB
Unallocated: 315.25 GB
Protected volumes on this disk: None

Actions

Disks

Add... Remove

Configuration

Rescan

- Click on the **Agents** tab. Here the servers which will be backed up with DPM are selected. The DPM agent will be installed to each of the servers selected.

DPM 2006 Administrator Console

File Action View Help

Monitoring Protection Recovery Reporting Management

Agents **Disks**

Agent licenses

Agent licenses purchased: 0 Agent license status: All agent licenses are in use.

Agent licenses in use: 0

Server Name	Agent Status	Agent Updates
There are no servers with agents installed. To install agents, click Install.		

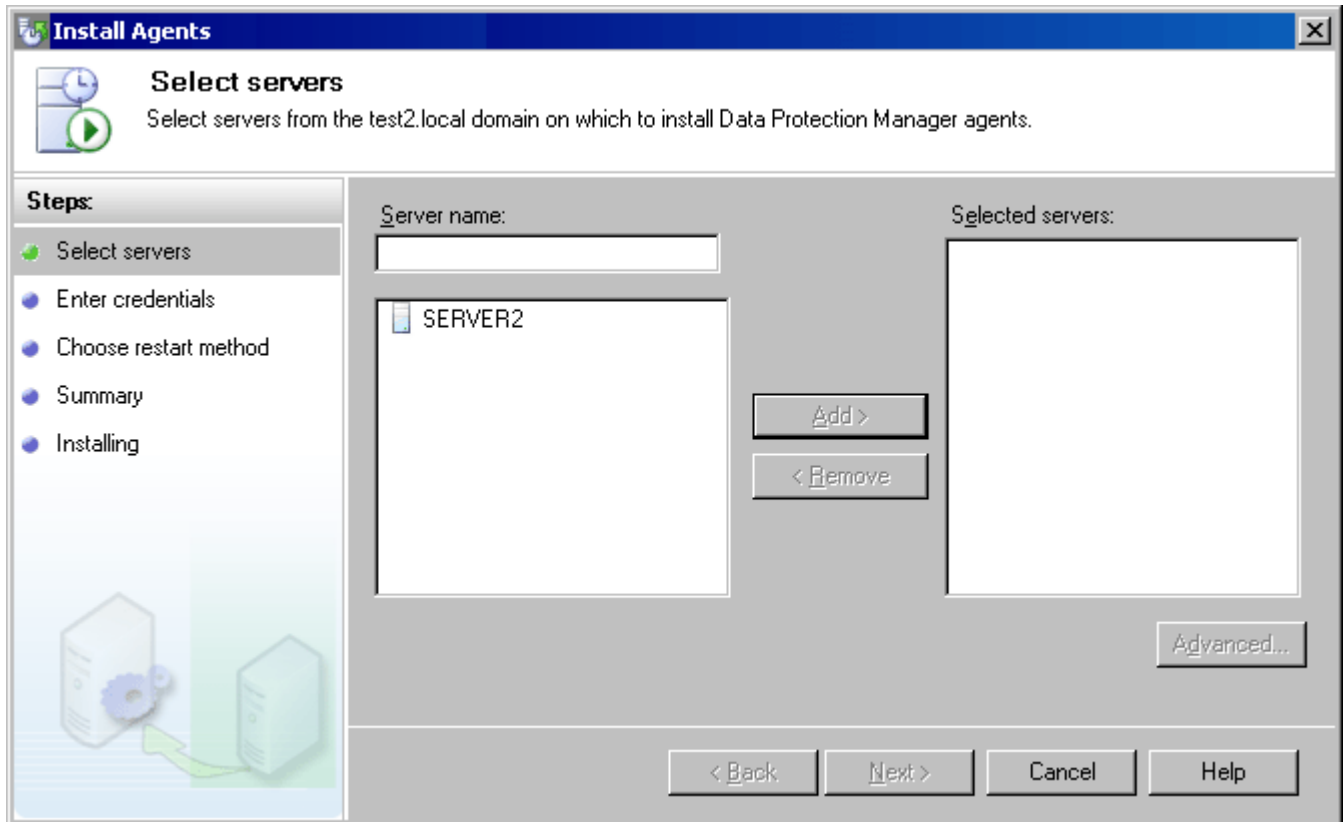
Details:

Actions

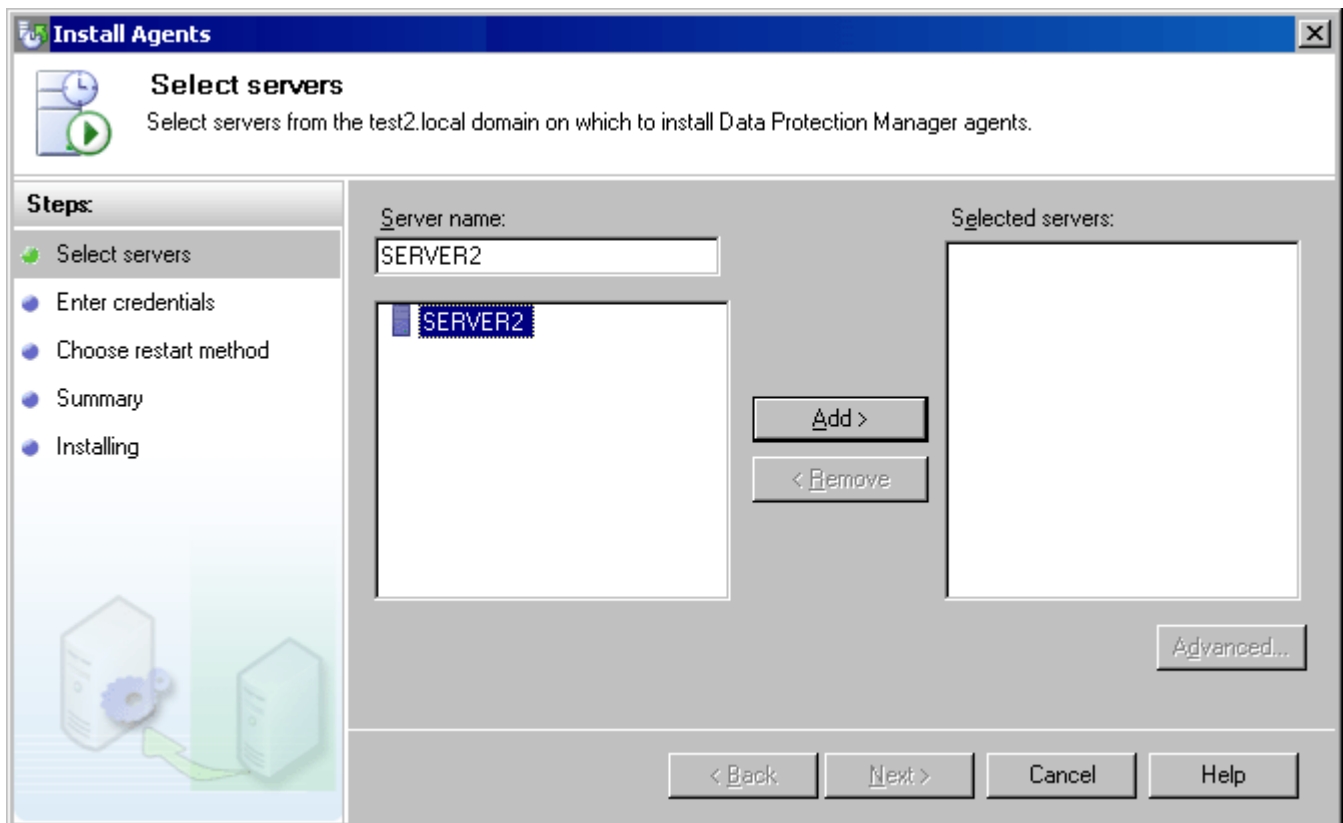
Agents

Install... Update... Uninstall... Refresh information Update agent licenses...

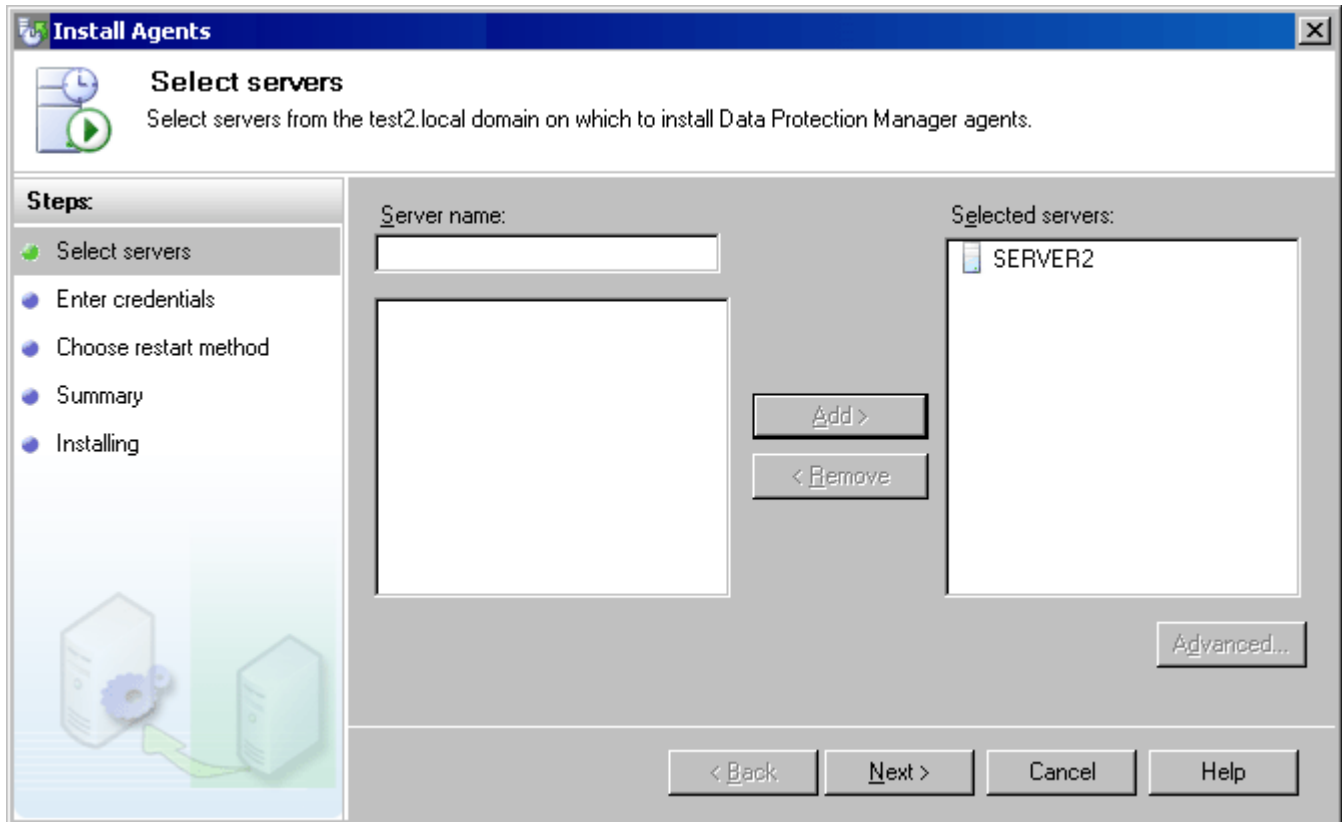
9. In the **Actions** pane, under **Agents**, click **Install...**. A list of all of the servers found in the Active Directory network will be displayed.



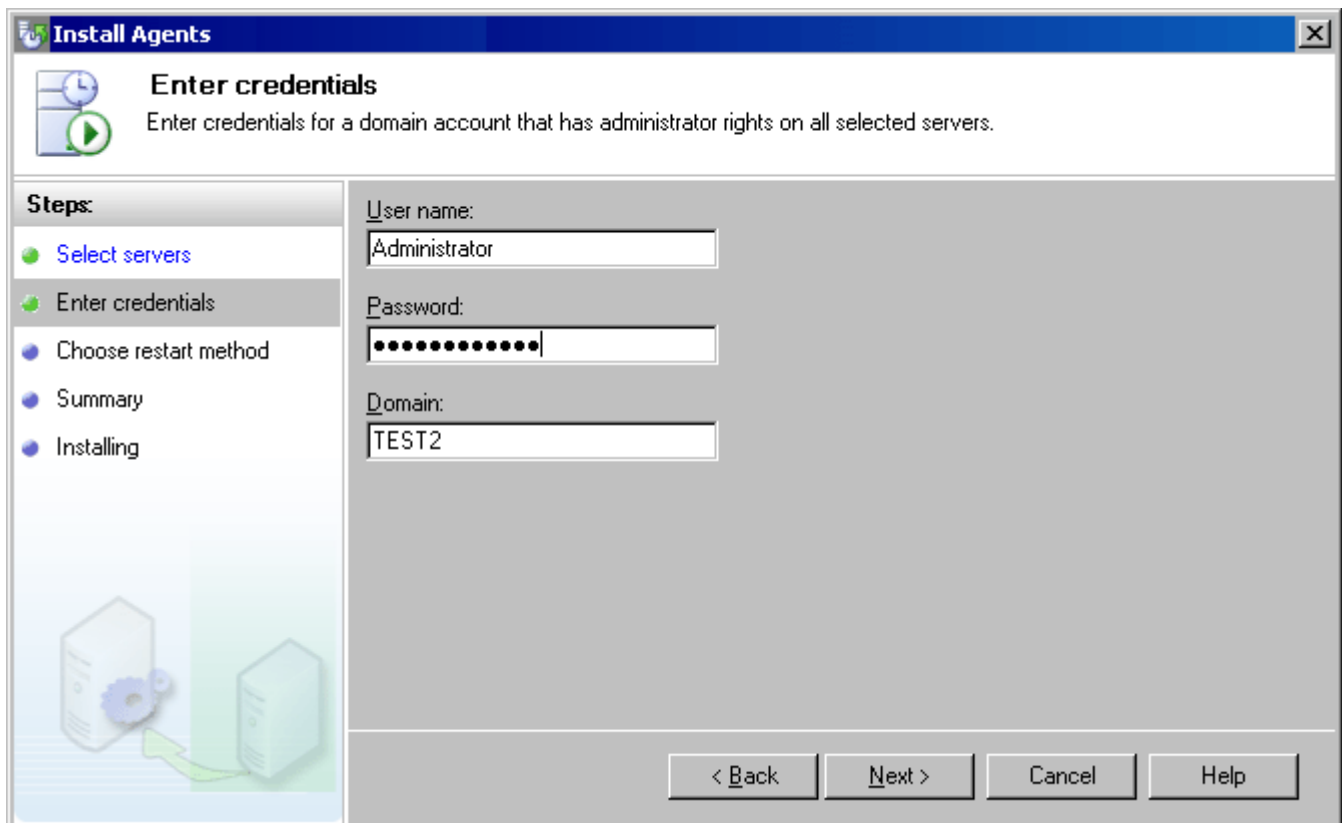
10. Highlight the server(s) which will be backed up with DPM. Click the **Add>** button.



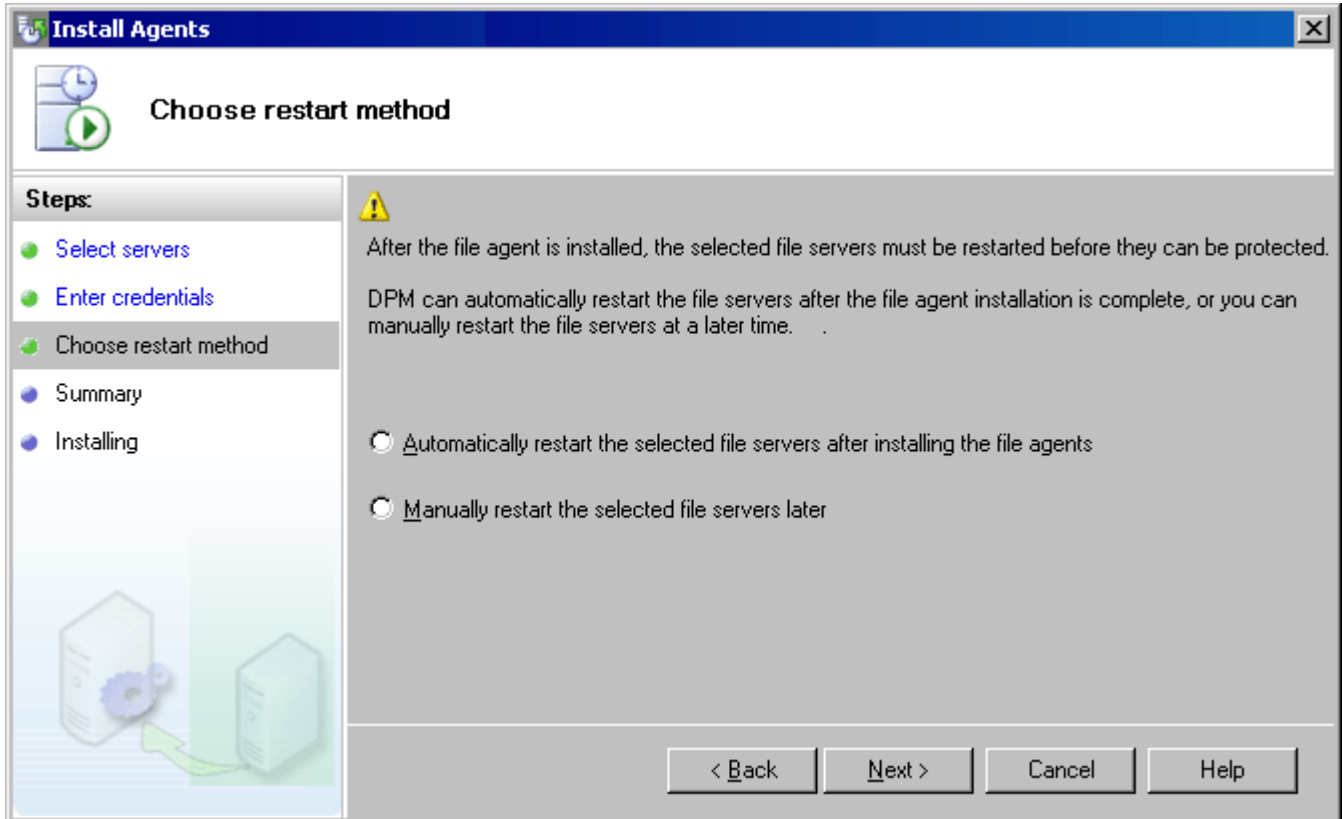
11. You will be presented with a summary screen showing all of the servers for which the DPM agent will be installed. Click the **Next>** button.



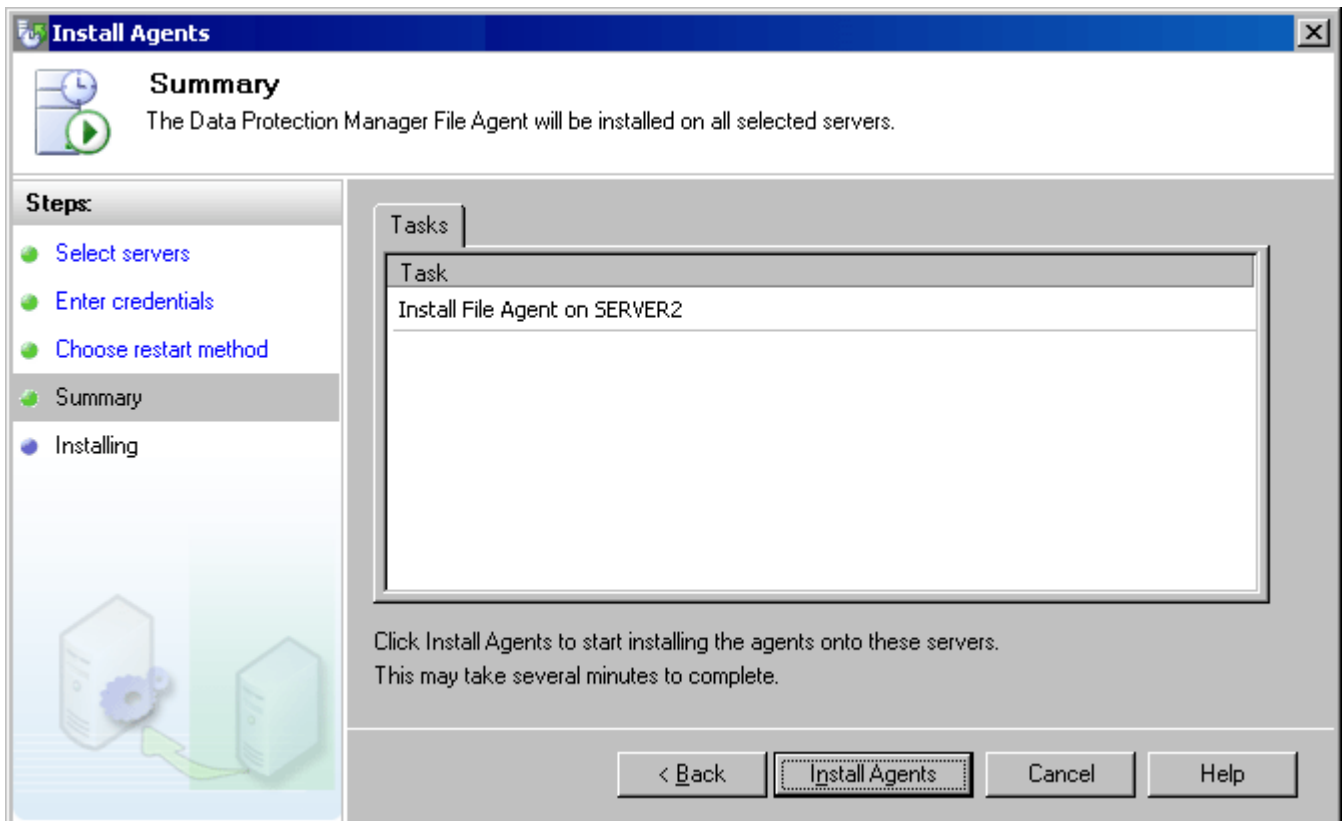
12. Enter a user name and password for an account that has administrative rights on the selected server(s). Click the **Next>** button.



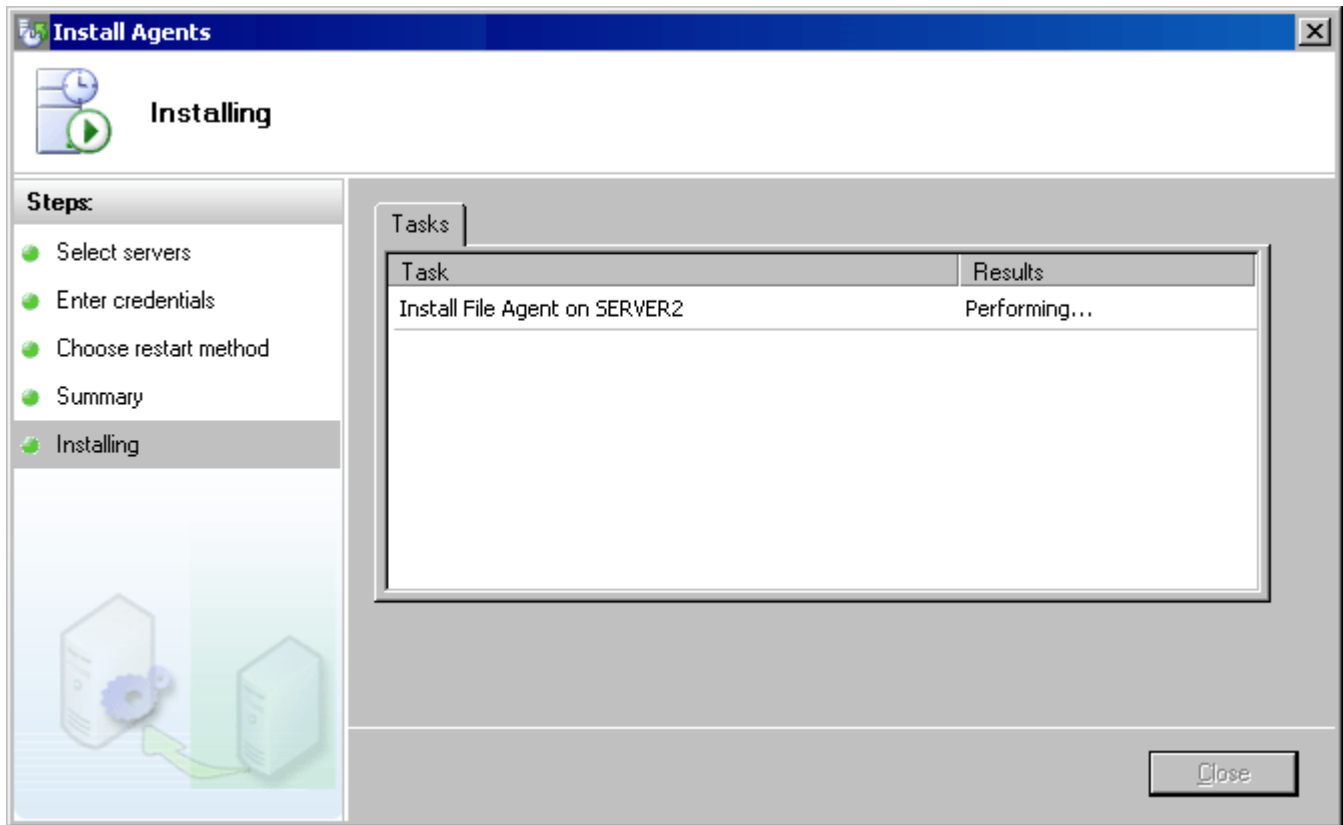
13. Select whether the servers will restart automatically or manually after the DPM has agent has been installed to them. Click the **Next>** button.



14. Click the **Install Agents** button.

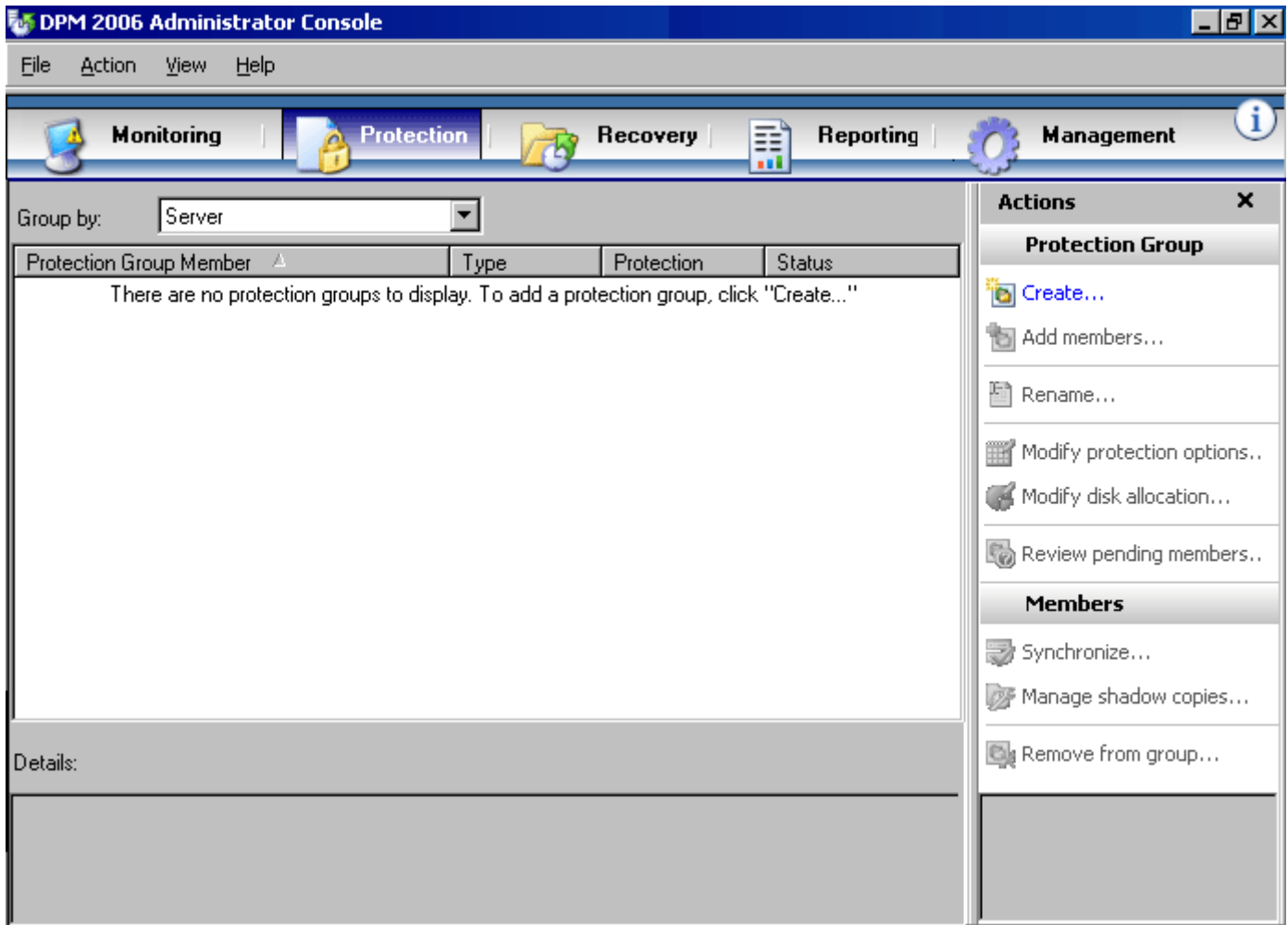


15. The agent will be installed on each of the selected servers. This process may take several minutes.

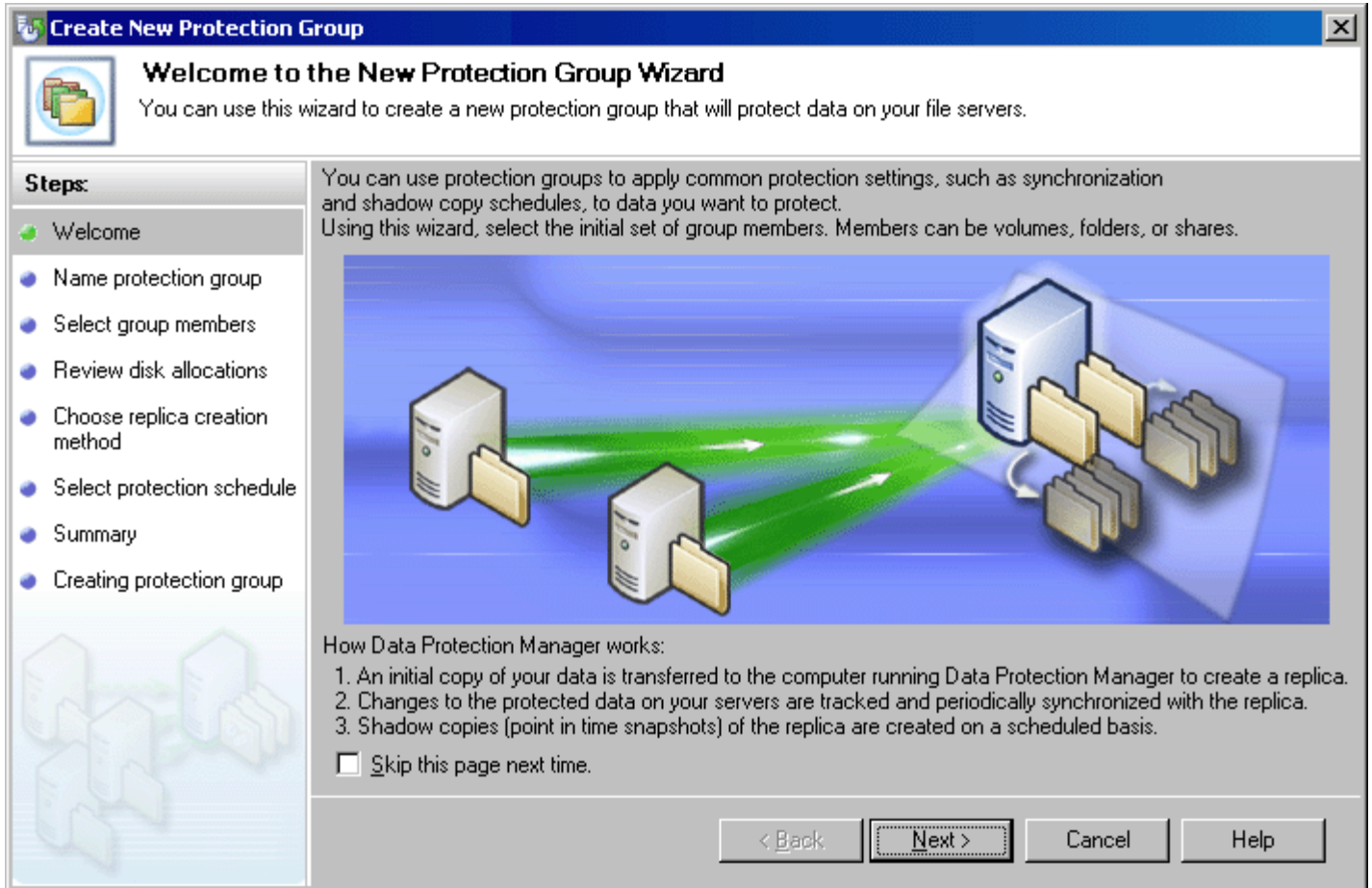


After the DPM agents have been installed one or more protection groups must be created. A protection group is a set of volumes, folders, or shares that you want to protect. You create protection groups to assemble sets of data to which you want to apply the same protection policy.

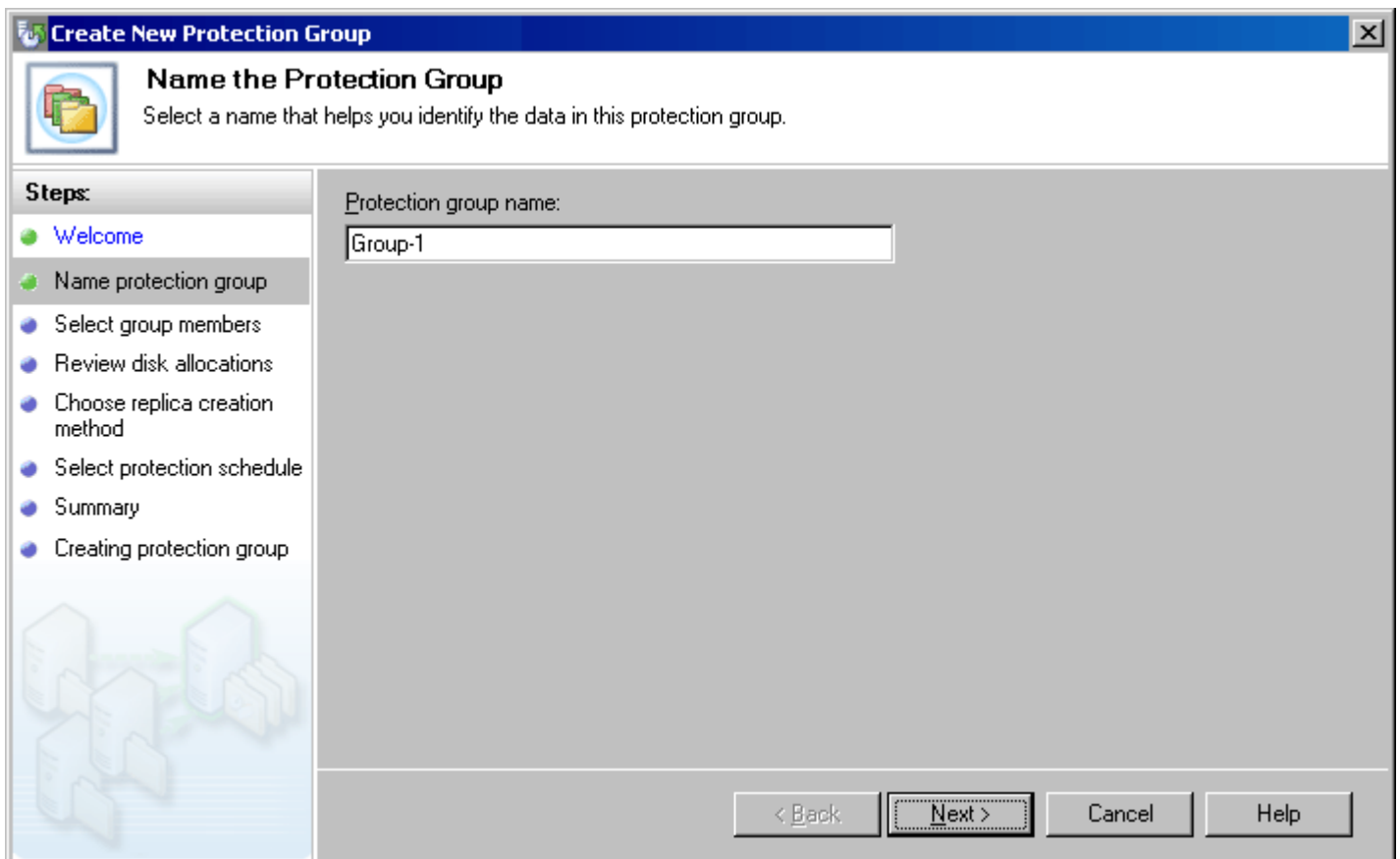
16. Click on the **Protection** tab in the DPM Administrator Console.



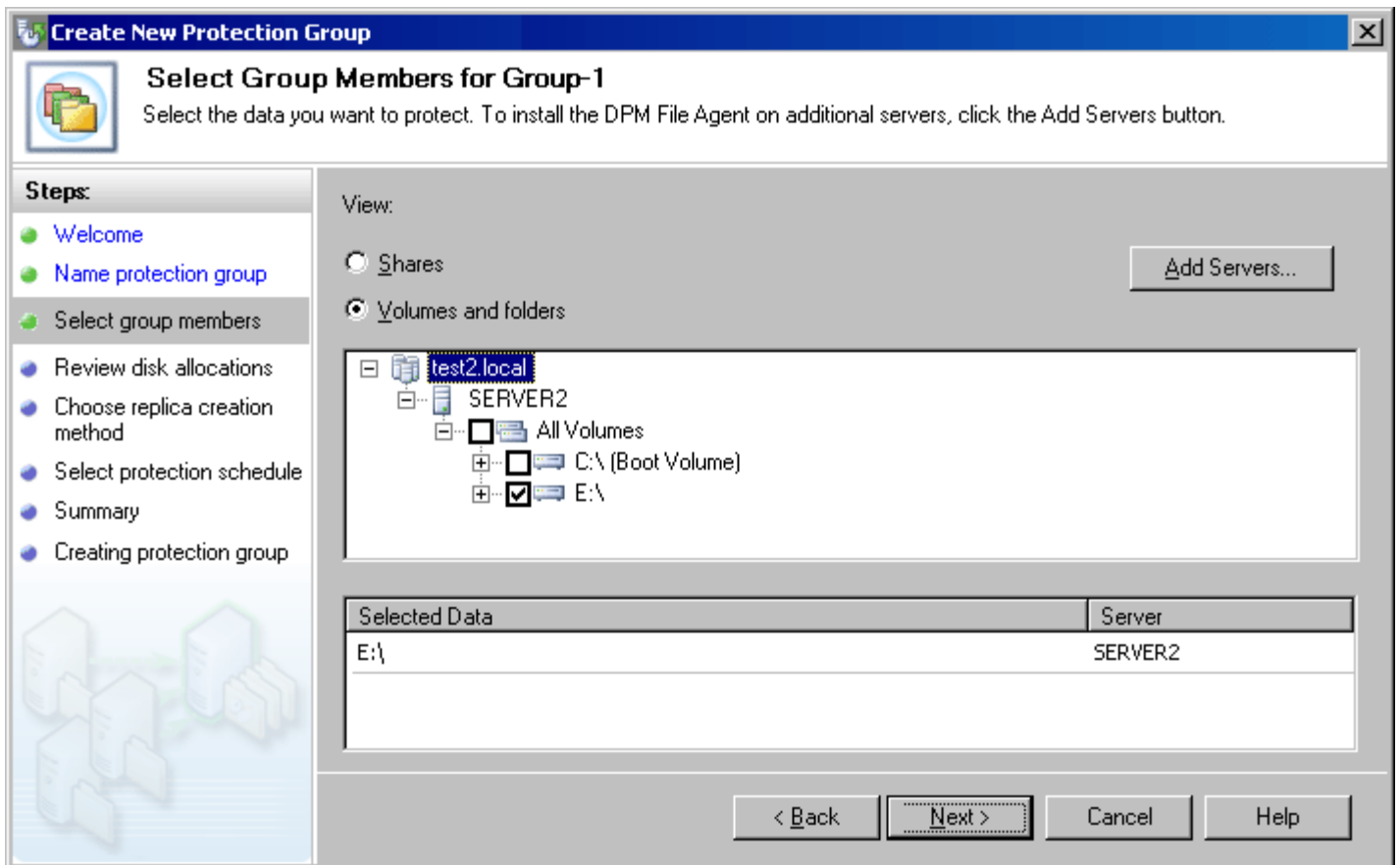
17. In the **Protection Group** section in the **Actions** pane click on **Create...** The Welcome to the New Protection Group Wizard will appear. Click the **Next>** button.



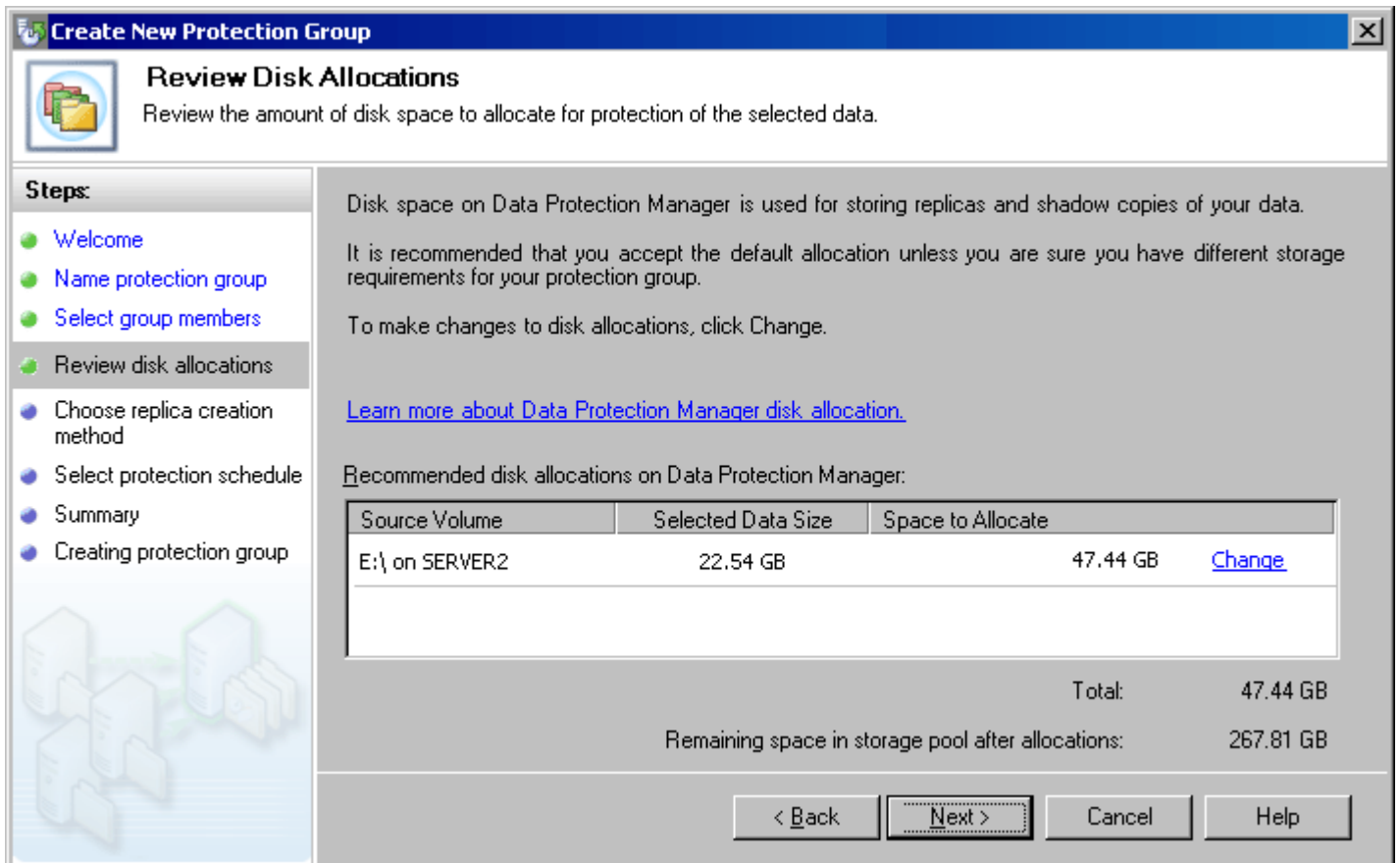
18. Provide a name for the Protection Group. Click the **Next>** button.



19. Select which shares and/or volumes and folders will be backed up. Click the **Next>** button.



20. A summary screen appears. Click the **Next>** button.



21. Select how data will be replicated to the DPM server. Click the **Next>** button.

Create New Protection Group

Choose Replica Creation Method

To protect the data you have selected, you must copy the data to the Data Protection Manager computer.

Steps:

- Welcome
- Name protection group
- Select group members
- Review disk allocations
- Choose replica creation method**
- Select protection schedule
- Summary
- Creating protection group

How do you want to copy the data to the Data Protection Manager computer?

- Let Data Protection Manager replicate the files over the network.**
This option is less labor intensive but it may take several hours or more, depending on your network bandwidth and the size of the data.
- Now**
- Later**
6/19/2007 5:19 PM
- I will transfer the files to Data Protection Manager myself.**
This option requires you to create the replica manually, typically by restoring the data from removable media such as tape. Creating the replica manually can save time if the size of the protected data is large. This option is strongly recommended if you are using DPM in a WAN and your protection group includes more than 5 GB of data. When creating a replica manually, you must preserve the directory structure and file metadata. [Learn more about creating a replica manually](#)

< Back **Next >** Cancel Help

22. Configure the protection schedule. Click the **Next>** button.

Create New Protection Group

Select Protection Schedule

The Data Protection Manager computer maintains a replica of your protected data. Shadow copies (snapshots) of the replica are created according to the schedule specified below.

Steps:

- Welcome
- Name protection group
- Select group members
- Review disk allocations
- Choose replica creation method
- Select protection schedule**
- Summary
- Creating protection group

Protection schedule

Protection frequency:

- Specify schedule
- Nearly-continuous (hourly)**

Create shadow copies at:

8:00 AM
12:00 PM
6:00 PM

Change Times...

To configure options that can improve DPM performance (especially important on a WAN or other slow network) click **Advanced Options...**

Synchronization will occur every hour.

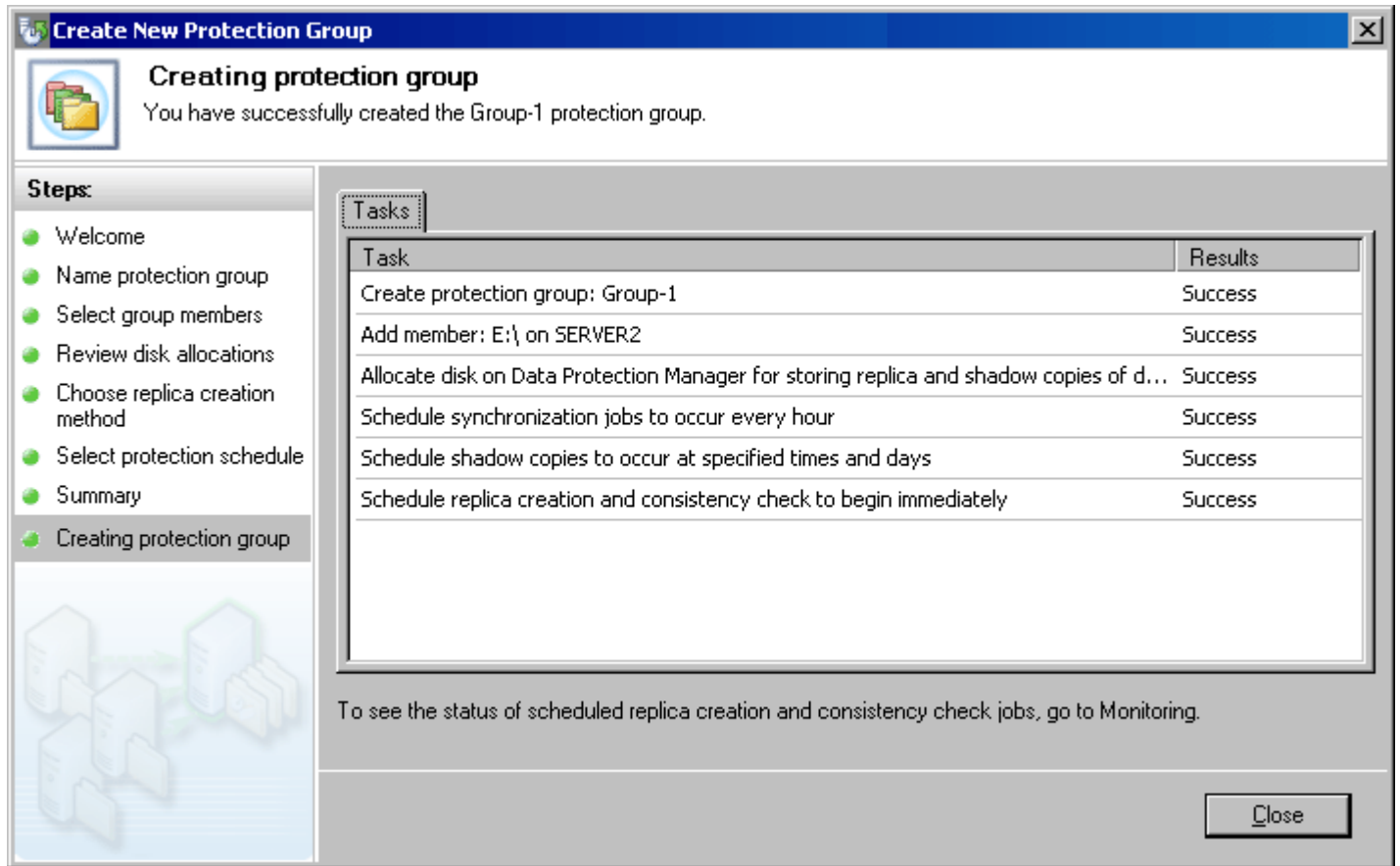
Estimated recovery goals

- Maximum data loss: 1 hour
- Recovery range: 21 days

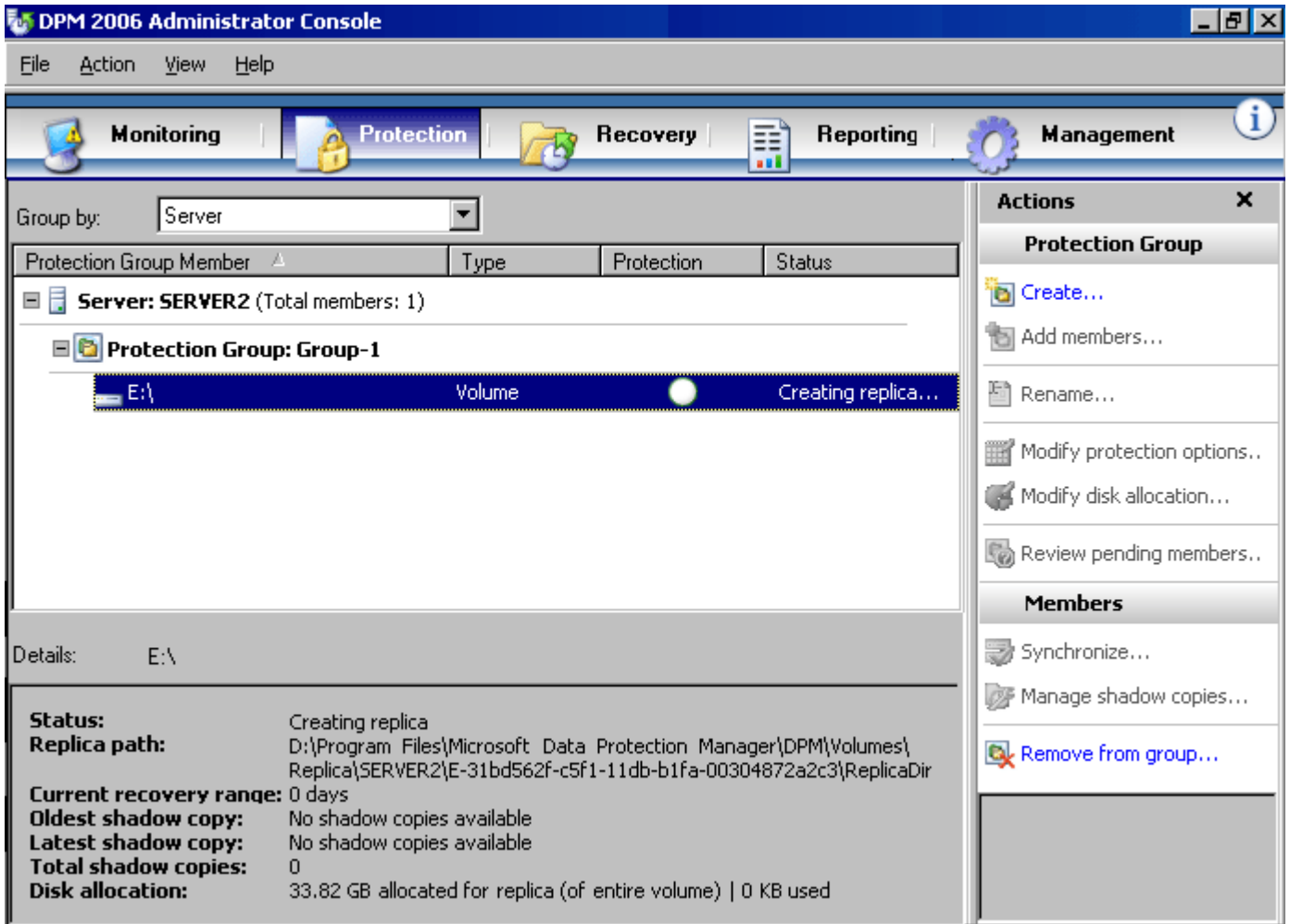
⚠ These recovery goals are estimates and are based on normal operations. Your experience may vary.

< Back **Next >** Cancel Help

23. When finished a summary page will be displayed.



24. If **Let Data Protection Manager replicate the files over the network** was selected in step 21 the data replication will begin.



25. When the replication is complete the status will be displayed as **OK**. Any subsequent changes to data on the protected servers will be replicated to the DPM server according to the protection schedule set in step 22.

DPM 2006 Administrator Console

File Action View Help

Monitoring Protection Recovery Reporting Management

Group by: Server

Protection Group Member	Type	Protection	Status
Server: SERVER2 (Total members: 1)			
Protection Group: Group-1			
E:\	Volume		OK

Details: E:\

Status: OK
Replica path: D:\Program Files\Microsoft Data Protection Manager\DPM\Volumes\Replica\SERVER2\E-31bd562f-c5f1-11db-b1fa-00304872a2c3\ReplicaDir
Current recovery range: 1 day
Oldest shadow copy: 6/19/2007 5:47:25 PM
Latest shadow copy: 6/19/2007 5:47:25 PM
Total shadow copies: 1
Disk allocation: 33.82 GB allocated for replica (of entire volume) | 22.52 GB used

Actions

Protection Group

- Create...
- Add members...
- Rename...
- Modify protection options..
- Modify disk allocation...
- Review pending members..

Members

- Synchronize...
- Manage shadow copies...
- Remove from group...

Summary

The amount of data being created and stored by large and small businesses continues to grow at incredible rates. Best practices dictate that this data should be backed up in case of hardware failure, data corruption, viruses, or any number of other problems that can result in the catastrophic loss of data. Disk-based backup solves many of the problems that plague IT administrators by providing increased performance, reliability, and ease of use relative to traditional backup methods. Together, Wasabi Storage Builder for IP-SAN and Microsoft Data Protection Manager deliver a low-cost, yet powerful disk-based backup solution.

For the VAR/SI/OEM:

- Enables you to provide a high-performance disk-based backup solution for your customers that is secure, scalable, and robust.
- Lowers BOM cost by using standard, off the shelf hardware components.
- Wasabi Storage Builder for IP-SAN minimizes assembly time. All required storage software is pre-installed on the DOM and no additional OS or other software is needed on the storage device.
- Provides the flexibility to hit different capacity and price points.
- Branding option allows you to differentiate as well as further promote your brand.

For the End User:

- Disk-based backup that is specifically targeted to solve your backup issues at a price that is within your budget.
- Backup that is reliable and secure.
- Backup that is simple to configure and easy-to-use, minimizing management costs.
- The backup solution is scalable and will grow as your data storage requirements continue to grow.

The Wasabi Systems Advantage

As important as the product itself is the company behind the product. Wasabi Storage Builder leverages the company's legacy of network operating system leadership. The Wasabi Certified® BSD OS is the same network operating system found in devices such as switches and routers that power the world's networking backbone. Wasabi Storage Builder products leverage years of code development and time-tested network support to deliver a high-performance, fully-optimized networked storage solution.

Wasabi Systems is not just a product vendor; we are your partner. We'll be with you every step of the way to ensure maximum success of your Storage Builder-based IP-SAN storage program. We offer personalized, high-level support, a comprehensive knowledge-base, application notes for using Storage Builder for IP-SAN targets with popular applications, and much more. A training and certification program ensures you'll be able to deliver the highest level of support to your customers. We can help with marketing and sales, with inclusion on the "Where to Buy" section of the Storage Builder web page, sales tools and collateral, presence at trade shows, and we can even accompany you to meetings with key target customers.

Appendix A: Further Information

For more detailed information on Wasabi Storage Builder for IP-SAN and Microsoft Data Protection Manager, please reference the following documents:

“Wasabi Storage Builder® for IP-SAN Data Sheet”

<http://www.wasabisystems.com/docs/StorageBuilderSAN.pdf>

“Wasabi Storage Builder® for IP-SAN Quick Start Guide”

http://www.wasabisystems.com/docs/StorageBuilderSAN_QuickStart.pdf

“Wasabi Storage Builder® for IP-SAN User’s Manual”

http://www.wasabisystems.com/docs/StorageBuilderSAN_UsersManual.pdf

“Microsoft® Data Protection Manager 2006 Product Overview”

<http://www.microsoft.com/systemcenter/dpm/evaluation/overview.aspx>

Microsoft® Data Protection Manager 2006 Documentation: “Data Protection Manager Technical Overview”

<http://www.microsoft.com/systemcenter/dpm/evaluation/whitepaper.aspx>

“Microsoft® System Center Data Protection Manager: Planning and Deployment Guide”

<http://download.microsoft.com/download/2/b/8/2b88a976-7f31-4920-8287-bfd1e4a15fe/PlanningAndDeploymentGuide.doc>

Appendix B: System Requirements

The following section has been excerpted from the Microsoft Data Protection Manager 2006 Documentation: “Data Protection Manager Technical Overview” Copyright © 2005 Microsoft® Corporation. All rights reserved.

A complete installation of DPM includes the Windows Server 2003 operating system with both Internet Information Services (IIS) 6.0 and Service Pack 1 (SP1) or later installed, the DPM application, and the DPM prerequisite software. The prerequisite software, which is included with the DPM product, includes:

- Microsoft® SQL Server™ 2000 (Standard or Enterprise Edition)
- Microsoft® SQL Server™ 2000 Service Pack 3a (SP3a) or later
- Microsoft® SQL Server™ 2000 Reporting Services (Standard or Enterprise Edition)
- Microsoft® SQL Server™ 2000 Reporting Services Service Pack 1 (SP1) or later

These products will be automatically installed on the DPM server if they are not already present. DPM is distributed on a set of four CDs that contain the Standard Editions of SQL Server 2000 and SQL Server 2000 Reporting Services, and include all languages available for DPM.

NOTE Chapter 4 of the DPM Planning and Deployment Guide describes the installation process in more detail.

Server Prerequisites

The DPM server itself must be:

- Running either Windows Server 2003 (Standard or Enterprise Edition) or Windows Storage Server 2003 (Standard or Enterprise Edition) with Service Pack 1 or later installed.
- A member of the same Active Directory domain as the file servers it protects.
- An ordinary single-purpose server; the DPM server must not be an Active Directory domain controller
- Equipped with at least one logical volume (which may be made of multiple physical disks) and at least one additional unused disk.

Servers to be protected by DPM must meet the following requirements:

- The server must be running only one of the following operating systems:
 - Windows Server 2003 with Service Pack 1 or later installed
 - Windows Storage Server 2003 with Service Pack 1 or later installed
 - Windows 2000 Server with both Service Pack 4 and the Windows 2000 Update Rollup installed
- The server must be a member of the same Active Directory domain as the DPM server that protects it.
- DPM can be used to protect stand-alone file servers only. Clustered file servers cannot be protected.
- DPM cannot be used to protect file servers on which case insensitivity for file names has been disabled. For more information on this requirement, see the DPM Planning and Deployment Guide.

Copyright © 2007 Wasabi Systems Inc. All rights reserved. No part of this document may be reproduced, modified, or distributed in any form or by any means without the prior express written consent of Wasabi Systems Inc. Wasabi®, Wasabi Certified®, WasabiRAID®, the Wasabi logo, Storage Builder®, and Flashware® are registered trademarks of Wasabi Systems Inc. NetBSD® is a registered trademark of The NetBSD Foundation. All other brand and product names are trademarks of their respective owners.

