CA ARCserve® Backup for Windows

Agent for Microsoft Data Protection Manager Guide

r12

CA Product References

This documentation set references the following CA products:

- Advantage™ Ingres®
- BrightStor® ARCserve® Backup for Laptops and Desktops
- BrightStor® CA-1® Tape Management
- BrightStor® CA-Dynam®/B Backup for VM
- BrightStor® CA-Dynam®/TLMS Tape Management
- BrightStor® CA-Vtape™ Virtual Tape System
- BrightStor® Enterprise Backup
- BrightStor® High Availability
- BrightStor® Storage Resource Manager
- BrightStor® VM:Tape®
- CA ARCserve® Backup Agent for Novell Open Enterprise Server for Linux
- CA ARCserve® Backup Agent for Open Files on NetWare
- CA ARCserve® Backup Agent for Open Files on Windows
- CA ARCserve® Backup Client Agent for FreeBSD
- CA ARCserve® Backup Client Agent for Linux
- CA ARCserve® Backup Client Agent for Mainframe Linux
- CA ARCserve® Backup Client Agent for NetWare
- CA ARCserve® Backup Client Agent for UNIX
- CA ARCserve® Backup Client Agent for Windows
- CA ARCserve® Backup Enterprise Option for AS/400
- CA ARCserve® Backup Enterprise Option for Open VMS
- CA ARCserve® Backup for Windows
- CA ARCserve® Backup for Windows Agent for IBM Informix
- CA ARCserve® Backup for Windows Agent for Lotus Domino
- CA ARCserve® Backup for Windows Agent for Microsoft Data Protection Manager
- CA ARCserve® Backup for Windows Agent for Microsoft Exchange
- CA ARCserve® Backup for Windows Agent for Microsoft SharePoint

- CA ARCserve® Backup for Windows Agent for Microsoft SQL Server
- CA ARCserve® Backup for Windows Agent for Oracle
- CA ARCserve® Backup for Windows Agent for Sybase
- CA ARCserve® Backup for Windows Agent for VMware
- CA ARCserve® Backup for Windows Disaster Recovery Option
- CA ARCserve® Backup for Windows Disk to Disk to Tape Option
- CA ARCserve® Backup for Windows Enterprise Module
- CA ARCserve® Backup for Windows Enterprise Option for IBM 3494
- CA ARCserve® Backup for Windows Enterprise Option for SAP R/3 for Oracle
- CA ARCserve® Backup for Windows Enterprise Option for StorageTek ACSLS
- CA ARCserve® Backup for Windows Image Option
- CA ARCserve® Backup for Windows Microsoft Volume Shadow Copy Service
- CA ARCserve® Backup for Windows NDMP NAS Option
- CA ARCserve® Backup for Windows Serverless Backup Option
- CA ARCserve® Backup for Windows Storage Area Network (SAN) Option
- CA ARCserve® Backup for Windows Tape Library Option
- CA XOsoft™ Assured Recovery™
- CA XOsoft™
- Common Services™
- eTrust® Antivirus
- eTrust® Firewall
- Unicenter® Network and Systems Management
- Unicenter® Software Delivery
- Unicenter® VM:Operator®

Contact Technical Support

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at http://ca.com/support.

Contents

Chapter 1: Introducing the Agent

CA ARCserve Backup is a comprehensive, distributed storage solution for applications, databases, distributed servers, and file systems. It provides backup and restore capabilities for databases, business-critical applications, and network clients.

Among the agents that CA ARCserve Backup offers is the CA ARCserve Backup Agent for Microsoft Data Protection Manager (DPM). Microsoft Data Protection Manager is an integrated component of the Microsoft Windows Server System that provides data recovery with near-continuous data protection.

DPM enables disk-based data protection and recovery using Volume Shadow Copy Services to provide backup and recovery functions. DPM protects its own production servers while CA ARCserve Backup backs up the DPM database and replicas, protects the DPM server, adds long term archiving capabilities, protection for applications, and bare metal disaster recovery.

Note: DPM refers to DPM 2006 wherever applicable, throughout the guide.

This section contains the following topics:

Benefits of Using the Agent

The CA ARCserve Backup for DPM provides a comprehensive data protection solution, working with the Data Protection Manager to provide the following benefits:

DPM Server Protection

The DPM server can protect the data on many remote server systems. If the DPM server fails, the data on these remote servers is lost and cannot be recovered from the DPM server. CA ARCserve Backup protects the DPM server itself and, after a failure of the DPM server, you can recover the DPM server with the data backed up by CA ARCserve Backup.

DPM Replica Protection

The DPM server collects file system data from DPM protected servers and stores this data on disks. Because you can only store a limited number of versions of files on the DPM server, CA ARCserve Backup allows you to move this data from the DPM server to disk arrays or tape libraries and make it available for restore to the DPM server or directly to the DPM file agent system.

Long Term Archiving

The agent provides the ability to archive data on tapes for disaster recovery and regulatory compliance. The agent can move data protected by DPM to tapes, archiving disks, or Virtual Tape Libraries (VTL) storage systems. CA ARCserve Backup encryption ensures that the data on the tapes cannot be misused even if the tapes are accessed inappropriately.

Bare Metal Disaster Recovery

The agent provides fast and efficient file recovery. However, in the event of a total server crash, the server must be reconfigured and reinstalled before DPM can restore files, increasing recovery time significantly. Using the CA ARCserve Backup Disaster Recovery Option with the Agent for Microsoft DPM, you can reduce recovery time after DPM server failure.

Direct Recovery of Archived Files

The agent provides improved restore time for files residing on the DPM server, allowing fast recovery of files archived to tape when restoring them to the DPM server or the originating DPM protected server.

How the Agent Works

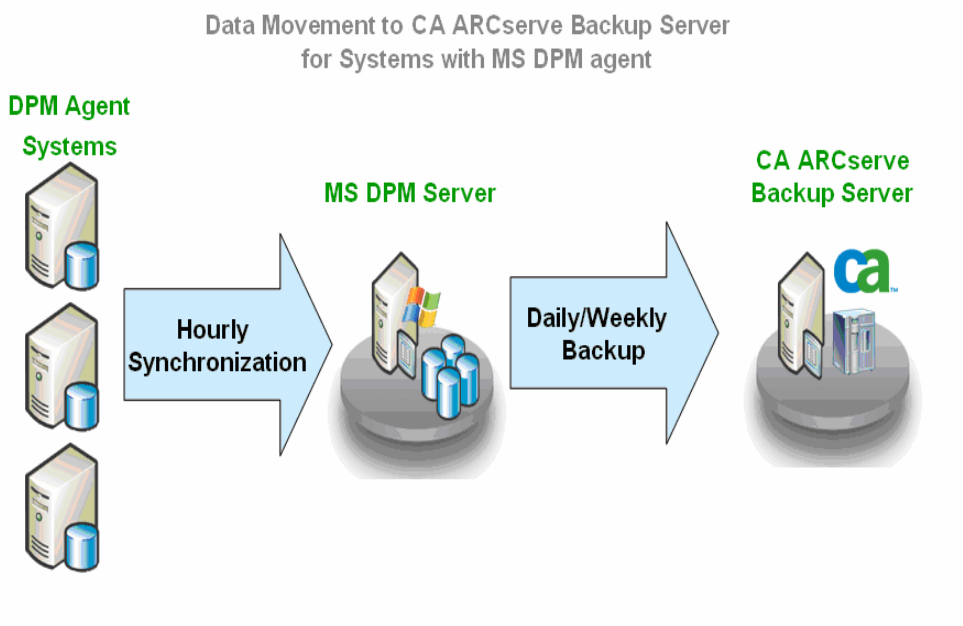
The agent protects Microsoft Data Protection Manager databases and replicas by backing them up to the CA ARCserve Backup server.

The agent performs the following tasks:

- Browses and selects the items for backup
- Runs backup jobs
- Writes data to backup media
- Stores necessary information in the CA ARCserve Backup database
- Browses and selects items for restore
- Executes restore jobs
- Retrieves data from the backup media and restores it to disk

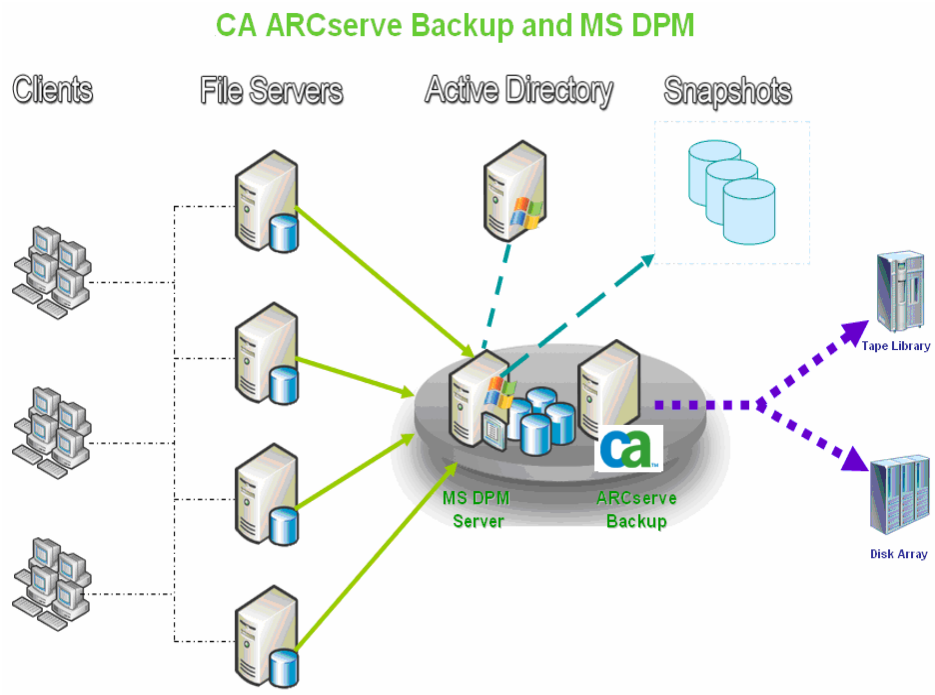
The Agent for DPM integrates with the DPM server to deliver data protection, long term archiving capabilities, protection for applications, and feature rich disaster recovery capabilities. Using the Microsoft Volume Shadow Copy Service (VSS) infrastructure, the agent takes snapshots of the DPM server, including the DPM database and replicas, and then backs up the snapshots to tape or disk devices. You back up your data from the replicas on the DPM server rather than from the live data on the DPM protected servers. Because you back up from a read-only snapshot of the data, you can run backup jobs at any time without affecting the performance of DPM protected servers. With CA ARCserve Backup and the agent, you can restore DPM-archived data directly from your archive media to your DPM protected server without involving the DPM server.

The data flow between CA ARCserve Backup, the agent and DPM is illustrated in the following figure:



Architecture

CA ARCserve Backup can be installed on the same system as the DPM server to back up DPM data and configuration information locally or can be installed remotely to back up multiple DPM servers over the network. Remote backup performance can be affected if the DPM server has a very large amount of data, because network bandwidth may limit the transfer of data to the backup server. With local backup, the tape drive or virtual tape library (VTL) on which the data is archived is directly connected to the DPM server. If the DPM server and CA ARCserve Backup are installed in the same system, DPM data can be moved directly to tape from the disk, bypassing the network.



Components

The CA ARCserve Backup DPM data protection solution contains the following components:

CA ARCserve Backup

Protects mission-critical database applications and systems using application agents and the Client Agent for Windows, by backing up to disk arrays, tape libraries and VTLs.

CA ARCserve Backup Agent for Microsoft DPM

This protection agent, installed on the server running Microsoft DPM, is used by CA ARCserve Backup to protect Microsoft DPM.

CA ARCserve Backup Client Agent for Windows

Backs up system state information and performs bare metal recovery of the server and restores files directly from the backup server to the DPM protected server. Because Microsoft DPM agents cannot back up system state configuration information, Microsoft DPM backups can not be used for bare metal recovery. These functionalities work even if the DPM server is offline, so, if the DPM server crashes, you can restore file system data directly from the CA ARCserve Backup server.

Note: One or more of the above components can be on the same server.

Service Roles

For a DPM backup to be successful, the following entities must work together and with VSS to prepare and perform the backup:

- Requestors
- Providers
- Writers
- Components

Requestors

The Requestor is a piece of software (typically a backup application) responsible for the following tasks:

- Initiating the request for a DPM backup
- Processing the backup instructions from the Writers, including which files should be included for backup when a component is selected and the methods that should be used to back up and restore those files
- Backing up the shadow copy data to media
- Signaling the completion of the backup by deleting the shadow copy data from the disk

CA ARCserve Backup is designed to function as the Requestor in DPM backups.

Providers

The Provider is responsible for managing the volumes involved in the shadow copy backup, as well as for creating the shadow copy. The Provider interfaces with the shadow copy creation capabilities that are either part of the operating system (software-based) or on the disk array (hardware-based).

Hardware disk array vendors can supply their own Providers to interface with the VSS framework, and direct where and how to create the shadow copies.

There are two types of Providers - software-based and hardware-based.

- Software-based Providers are typically implemented as a DLL and a filter to manage storage. The shadow copies are created by the software. Shadow copies created with this type of Provider include a point-in-time view of the original volume as it existed before the shadow copy, and the subsequent snapshots of only the changed data.
- Hardware-based Providers are implemented at the hardware level and work with a hardware controller or storage adapter. Shadow copies are created by a storage appliance, host adapter, or RAID device outside the operating system. Shadow copies created with a hardware-based Provider are of an entire volume (a full copy), and are typically mirrored views of the original volume. Additionally, if a transportable shadow copy is created, it can be imported onto other servers within the same system.

Writers

A Writer is part of a VSS-aware application or service that participates in a backup in the following ways:

- Works with VSS to prepare the application or service's data to be frozen
- Suspends writes to the original volume while the shadow copy is created
- Supplies a list of Components to include in the backup (and the restore) to VSS and the Requestor

To ensure that the data used to create the shadow copy is internally consistent, VSS informs the applications or services that control the files included in the backup to freeze. When an application or service is frozen, the state of the files under its control is consistent. It is the responsibility of the Writer to let VSS know when an application or service's files are in a consistent state.

To ensure that this state does not change during the creation of a shadow copy, the Writers suspend the ability of the application or service to make changes to the volume serving as the source of the shadow copy. The application or service Writer ensures the consistency of its data at the time of the creation of the shadow copy. Work can continue as usual on the original volume, but no changes are actually made to the data until after the shadow copy has been created.

A Writer is also responsible for supplying a list of Components to VSS and to the Requestor in the form of a writer metadata document. A writer metadata document is an XML file produced by a Writer that contains instructions for the Requestor, such as which Components are to be backed up, the backup and restore methods to be used, and a list of any files that should be excluded from the backup.

Note: CA ARCserve Backup does not support Writers under Windows XP. This is because some of the necessary Writer support in Windows Server 2003 is not included in the Windows XP operating system.

Components

A Component is a group of files treated as a single unit by the Writers. The files that make up a Component are grouped together because they are mutually dependent on one another. For example, in a database, each file serves an important function in the context of the database as a whole, but on its own, a single file from a database has no use. By grouping all of these essential files into a Component, you ensure that all the data needed to successfully back up an application and its related files is backed up and can be restored later. If any of the files comprising a Component are inaccessible when the shadow copy is being created, the backup of the Component will fail.

Contact Technical Support

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at http://ca.com/support.

Chapter 2: Installing the Agent

This chapter provides information to help you install the Agent for Microsoft Data Protection Manager on Windows platforms. The information in this chapter assumes you are familiar with the characteristics and requirements of Windows Server 2003 and Microsoft Data Protection Manager 2006 in general, and with the administrator responsibilities in particular.

When the agent is installed, you can begin your first backup of Microsoft DPM. No further configuration is necessary to use the agent to back up and restore Microsoft DPM.

This section contains the following topics:

Prerequisites

Before you install the Agent for Microsoft Data Protection Manager, verify that you meet following prerequisites:

- Your system configuration meets the minimum requirements needed to install the agent.

  For a list of these requirements, see the readme file.

- You have administrator privileges or the proper authority to install software on the machine on which you are installing the agent.

  Note: Contact your CA ARCserve Backup administrator to obtain the proper rights if you do not have them.

- You have installed the Server and Manager for this release of CA ARCserve Backup for Windows on the backup host.

  Note: You must install the agent on the same host as the Data Protection Manager that you want to back up.

- You have the login name and password of the machine on which you are installing the agent.

Licensing

To use the agent, you must enter the license for the agent on the backup server you want to use to protect the Data Protection Manager. The backup server verifies that the agent is licensed.

For more information about licensing, see the *Implementation Guide*.

Installation Considerations

You must install the CA ARCserve Backup Client Agent for Windows and CA ARCserve Backup Agent for Microsoft DPM on the same machine as Microsoft DPM.

You can install CA ARCserve Backup for Windows on the same machine as Microsoft DPM or on another machine.

Agent Installation

Install the agent on each Data Protection Manager server you want CA ARCserve Backup to back up.

The agent follows the standard installation procedure for the system components, agents, and options of CA ARCserve Backup. For the detailed steps in this procedure, see the *Implementation Guide*.

Chapter 3: Using the Agent

This chapter provides information about the procedures and options you can use to back up or restore your data using the CA ARCserve Backup Agent for Microsoft DPM. For an overall description of backup features, see the *Administration Guide*.

This section contains the following topics:

Backup Operations

You must have CA ARCserve Backup for Microsoft DPM installed on a machine that has either the CA ARCserve Backup Server component or the CA ARCserve Backup Client Agent for Windows to back up Microsoft DPM data.

Backup Options

When you select a DPM server for backup, standard CA ARCserve Backup options are available.

Add Remotely-Installed DPM Server

To add the remotely-installed DPM server to CA ARCserve Backup as a backup source

1. On the Backup Manager Source tab, right-click Windows Systems in the displayed tree.
2. Select Add Machine/Object from the pop-up menu.

   The Add Agent dialog appears.
3. Enter the host name and IP address of your DPM server. If you do not have an IP address, click the Use Computer Name Resolution box.
4. Click Add.

   The server is registered with CA ARCserve Backup.

Back Up DPM Data

To protect your Microsoft DPM, you can back up Microsoft System Center Data Protection Manager 2006 Writers. Alternatively, you can back up only the DPM database or the DPM replica.

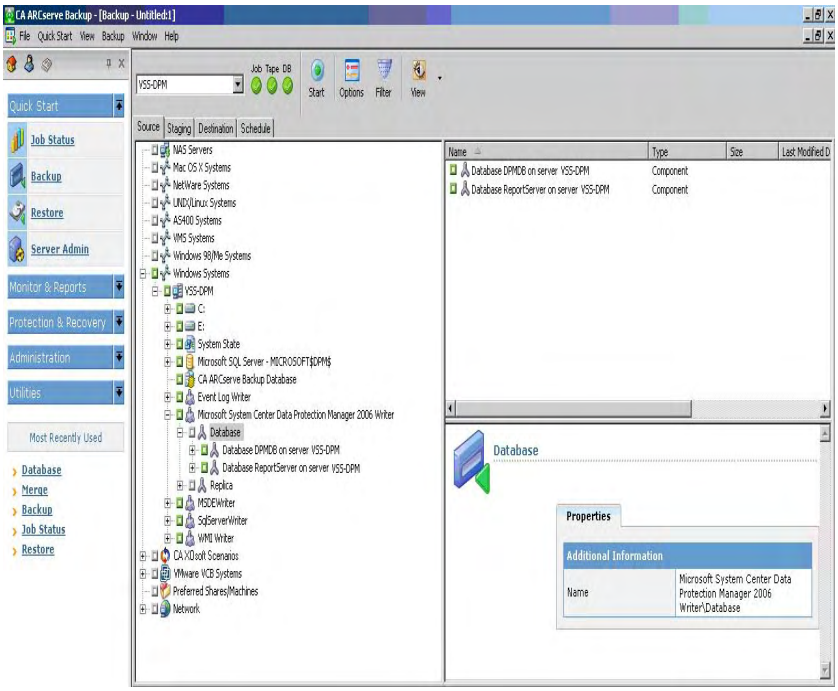
Select a Microsoft System Center Data Protection Manager 2006 Writer, DPM database or DPM replica from the tree on the Source tab of the Backup Manager to protect Microsoft DPM data. DPM replica backup operations back up data at the file or directory level.

Back Up DPM Databases

To back up a DPM database

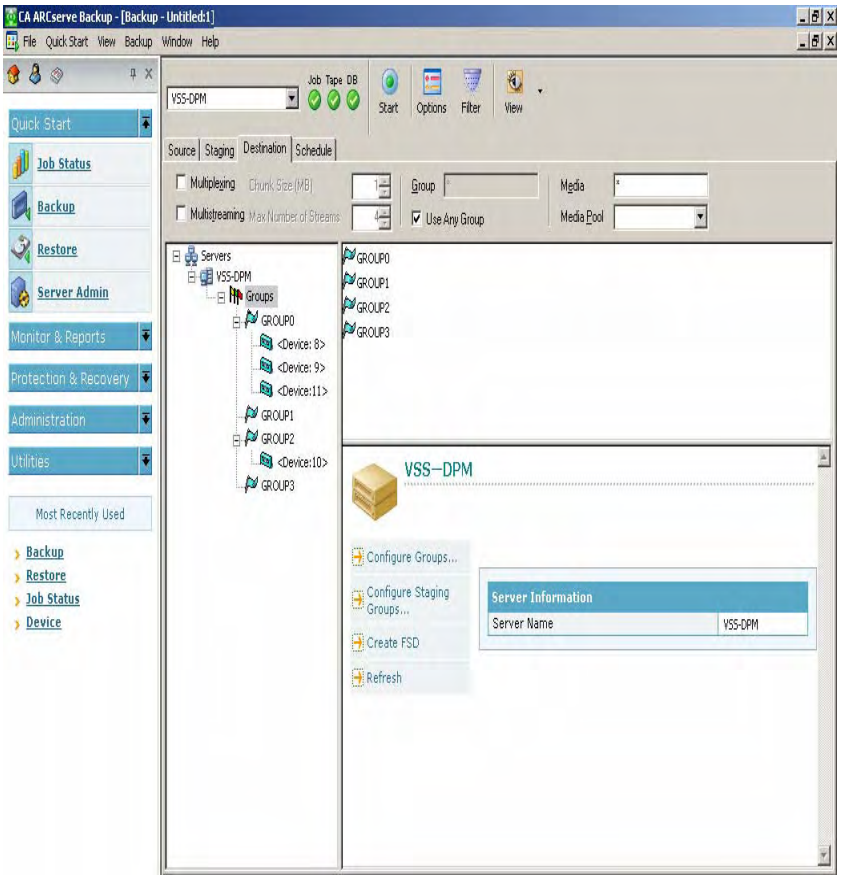
1. Expand Microsoft System Center Data Protection Manager 2006 Writer on the Backup Manager Source tab.

   The available databases appear.



2. Click the appropriate green box next to the DPM database you want to back up.

3. Select the target device for your backup job on the Destination tab.

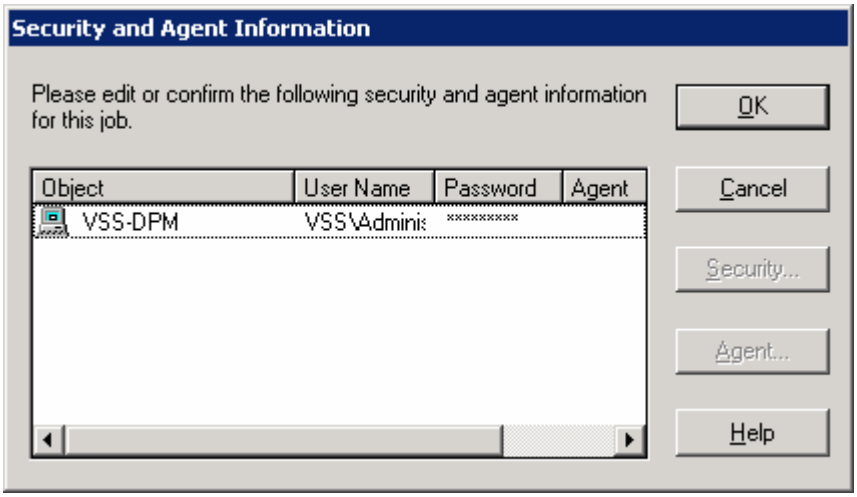


4. Select the appropriate method from the Repeat Method drop-down list on the Schedule tab.

   Note: Incremental and Differential Backup Methods are not supported for backing up DPM Writers. Backup jobs are always Full Backup.

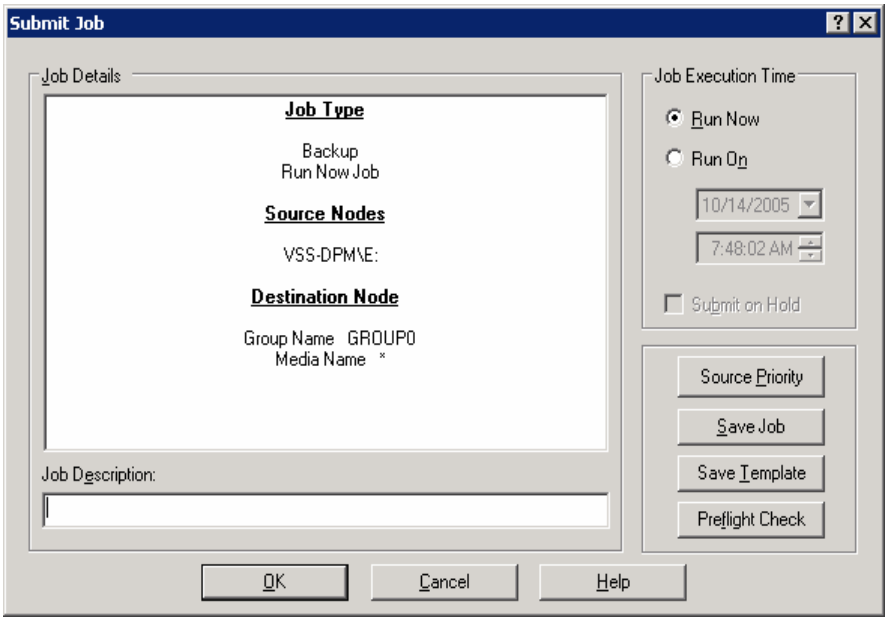
5. Click Start.

   The Security and Agent Information dialog appears.



6. Edit or confirm the information in the Security and Agent Information dialog and click OK.

   The Submit Job dialog appears.



7. Select the appropriate Job Execution Type. You can select one of the following:
   - **Run Now:** The backup job starts immediately
   - **Run On:** Enter the date and time to start the backup job
8. Click OK.

   You can monitor the job's progress using the Job Status Manager.

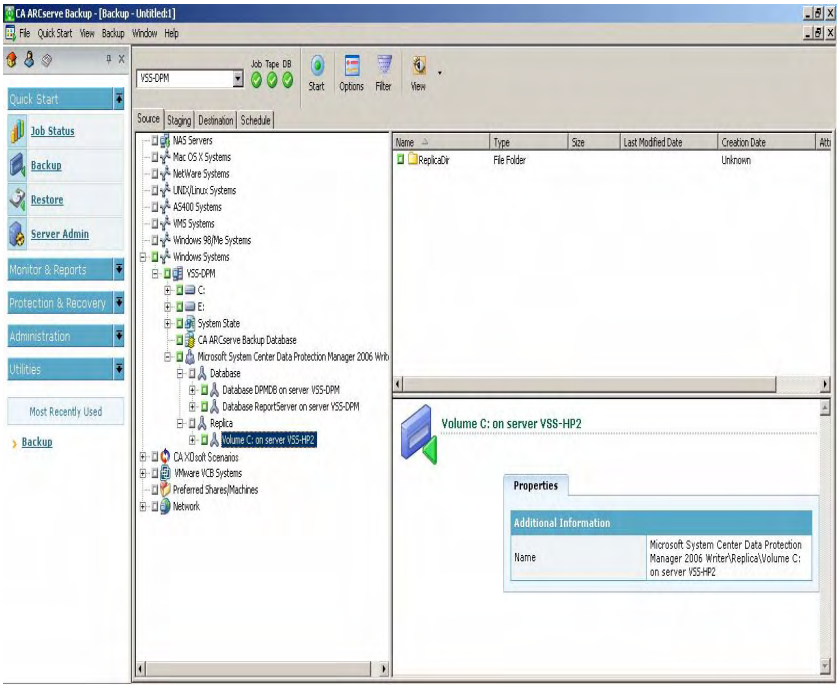
   Note: For more information about the Job Status Manager, see the *Administration Guide*.

Back Up DPM Replicas

To back up a DPM replica

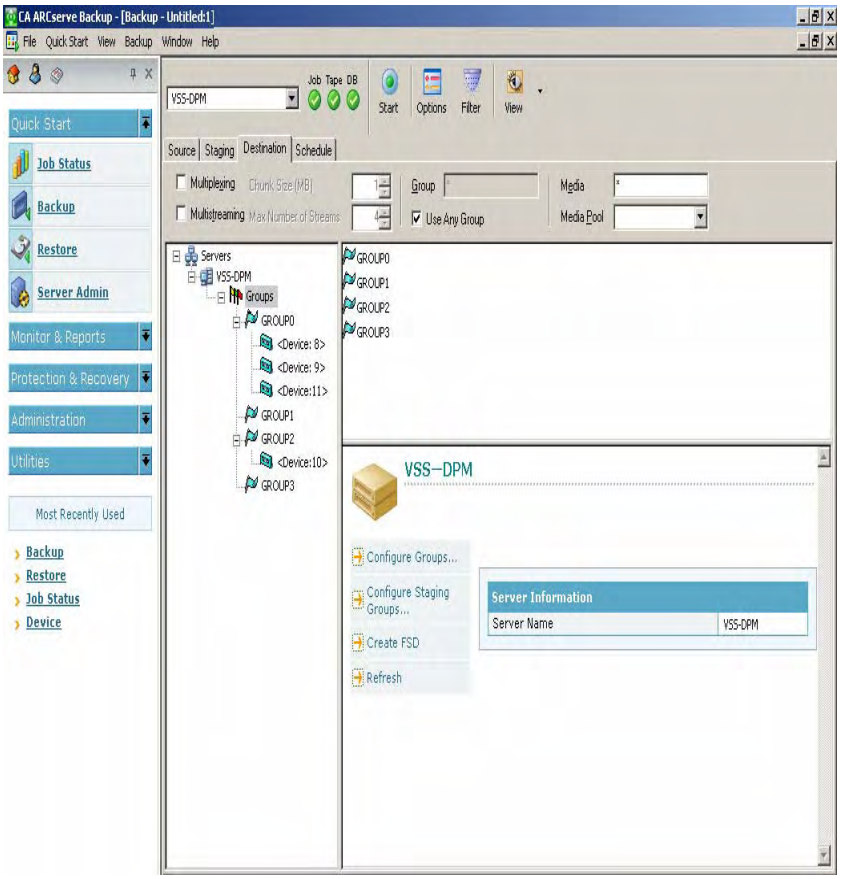
1. Expand the Microsoft System Center Data Protection Manager 2006 Writer on the Backup Manager Source tab.

   The replicas on the DPM server appear. You can back up individual files and folders or entire replicas.



2. Select the files, folders, or replica to back up.

3. Select the target device for your backup job on the Destination tab.

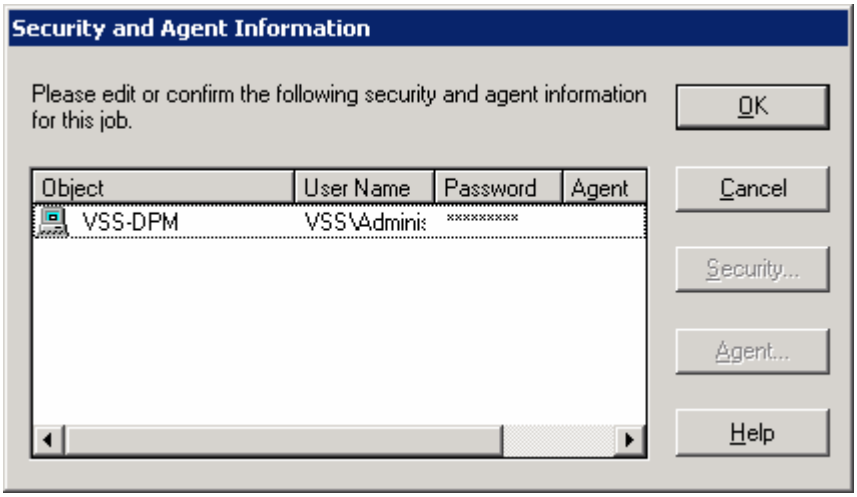


4. Select the appropriate method from the Repeat Method drop-down list on the Schedule tab.

   Note: Incremental and Differential Backup Methods are not supported for backing up the DPM Writer. Backup jobs are always Full Backup.

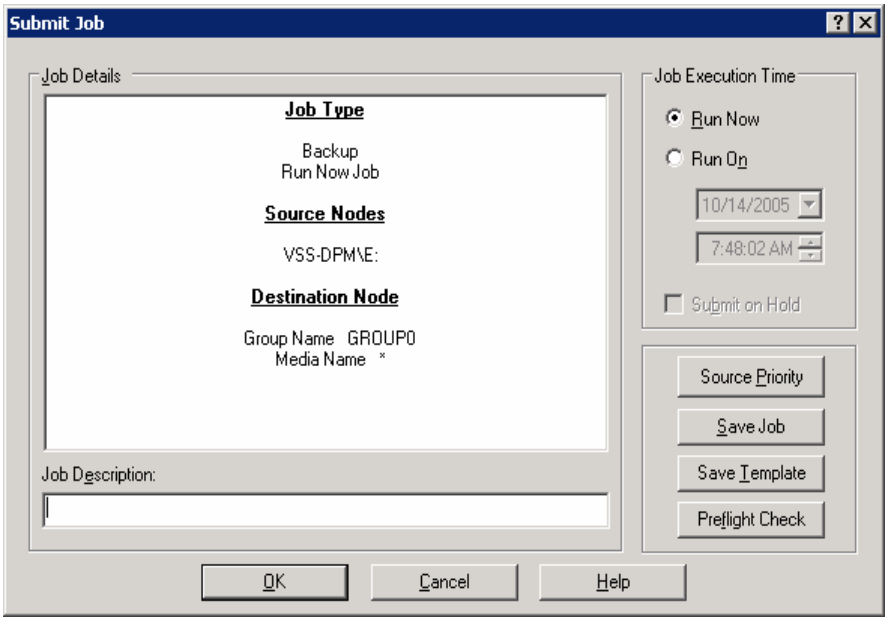
5. Click Start.

   The Security and Agent Information dialog appears.



6. Edit or confirm the information in the Security and Agent Information dialog and click OK.

   The Submit Job dialog appears.



7. Select the appropriate Job Execution Type. You can select one of the following:
   - **Run Now:** The backup job starts immediately
   - **Run On:** Enter the date and time to start the backup job
8. Click OK.

   You can monitor the job's progress using the Job Status Manager.

   Note: For more information about the Job Status Manager, see the *Administration Guide*.

Restore Operations

You can restore data to its original location, a location on DPM server, or to a location on a remote machine.

Restore Methods

The restore methods for the agent are available in a drop-down list on the Source tab of the Restore Manager. When a DPM server is selected for restore, the available methods are:

- **Restore By Tree**—The Restore By Tree method lets you select objects for restore jobs based on the source machine from which the data was backed up. If you select this method, you cannot restore the entire contents of the server as a whole but instead must select all subordinate objects individually. Use this method when you do not know which media contains the data you need but you have a general idea of what you need to restore and which machine it came from. It is the default method for the Restore Manager.
- **Restore By Session**—The Restore By Session method displays a list of all media used in backups and the files contained on them. This method lets you select objects for restore jobs based on backup sessions.

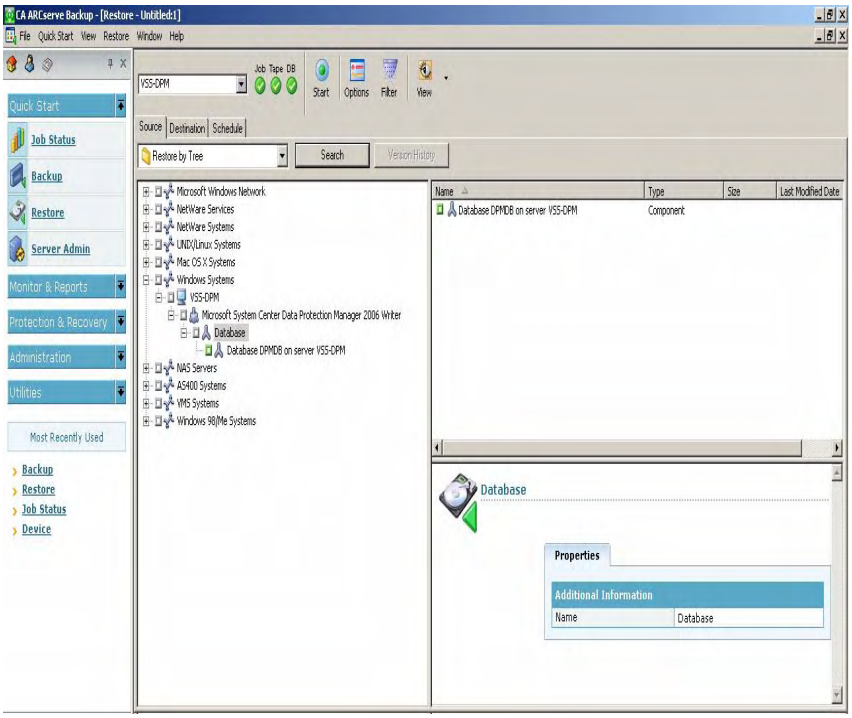
Restore Using the Restore by Tree Method

To restore using the Restore by Tree method

1. Select the Restore by Tree method on the Restore Manager Source tab.

2. Expand the computer from which the DPM Writer was backed up in the navigation tree.

   The DPM Writer components available for restore are displayed.

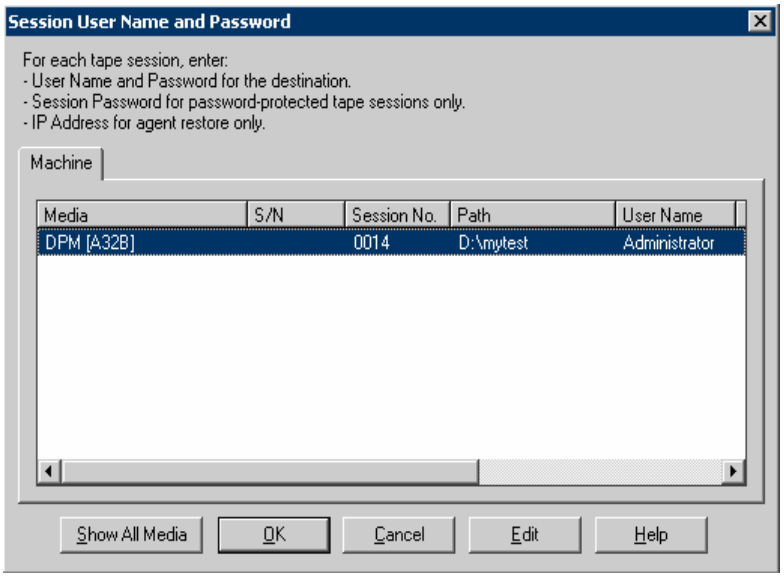


3. Click the appropriate green box next to the DPM Writer component you want to restore.

4. Select the target path for your restore job on the Destination tab.

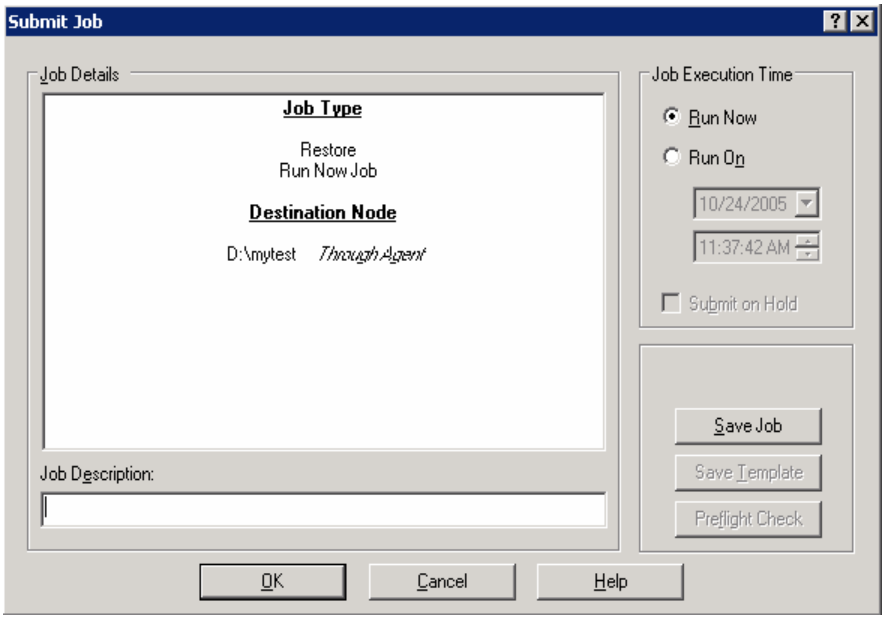
5. Click Start.

   The Session User Name and Password dialog appears.



6. Edit or confirm the information in the Session User Name and Password dialog and click OK.

   The Submit Job dialog appears.



7. Select the appropriate Job Execution Type. You can select one of the following:
   - **Run Now:** The restore job starts immediately
   - **Run On:** Enter the date and time to start the restore job
8. Click OK.

   You can monitor the job's progress using the Job Status Manager.

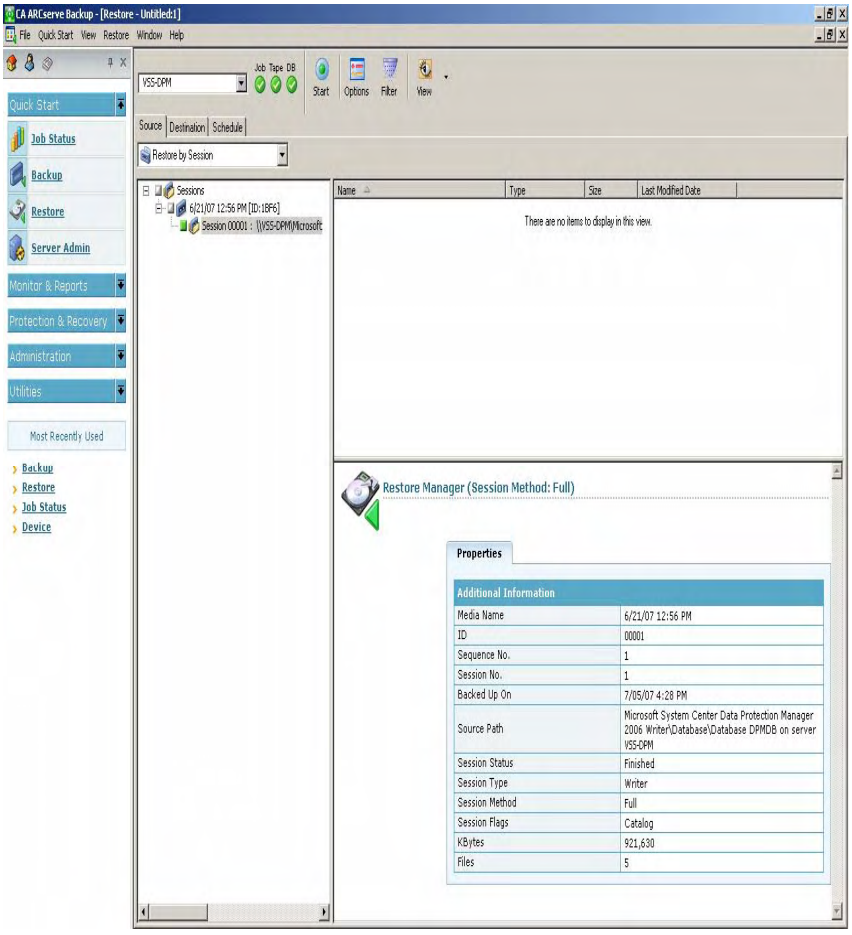
   Note: For more information about the Job Status Manager, see the *Administration Guide*.

Restore Using the Restore by Session Method

To restore using the Restore by Session method

1. Select the Restore by Session method on the Restore Manager Source tab.

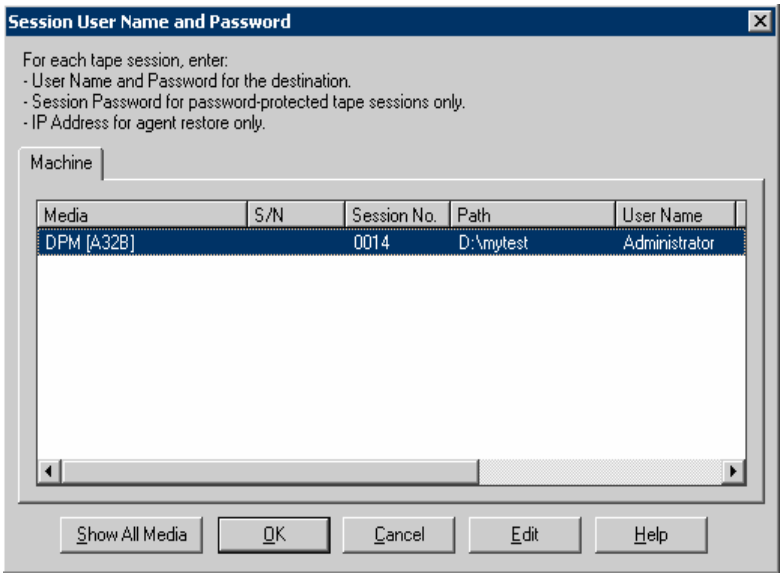
   A list of sessions you have backed up with CA ARCserve Backup are displayed.



2. Click the appropriate green box next to the session you want to restore.

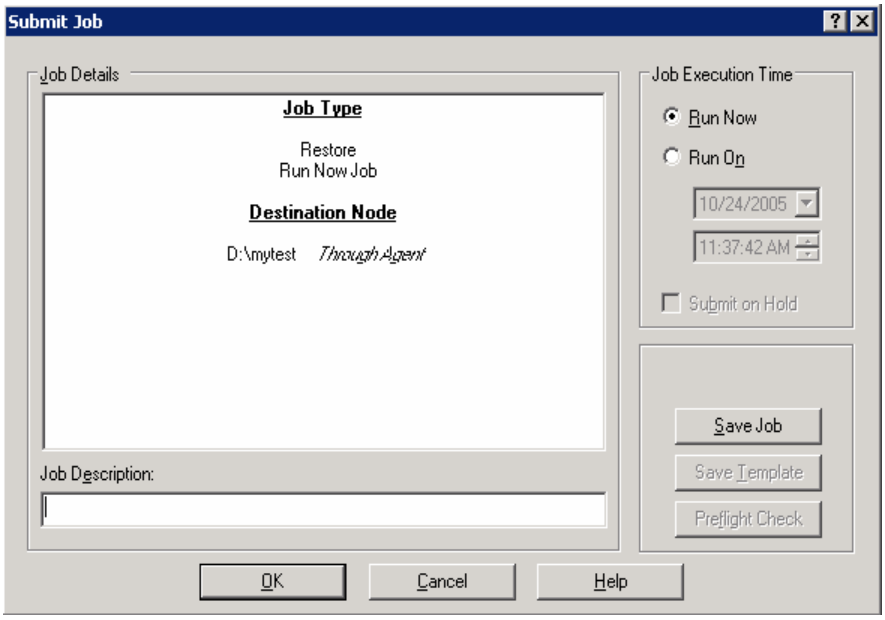
3. Select the target path for your restore on the Destination tab.
4. Click Start.

   The Session User Name and Password dialog appears.



5. Edit or confirm the information in the Session User Name and Password dialog and click OK.

   The Submit Job dialog appears.



6. Select the appropriate Job Execution Type. You can select one of the following:
   - **Run Now:** The restore job starts immediately
   - **Run On:** Enter the date and time to start the restore job
7. Click OK.

   You can monitor the job's progress using the Job Status Manager.

   Note: For more information about the Job Status Manager, see the *Administration Guide*.

Recovery Scenarios

The following types of data loss can affect your DPM data:

- Loss of individual files
- Loss of a DPM protected server
- Loss of the DPM server
- Loss of DPM and DPM protected servers
- Loss of the CA ARCserve Backup Server

The following section discusses each type of failure and how to recover from it.

Individual File Loss

The loss of individual files or volumes protected by DPM servers can happen in the following ways:

- Loss of files or volumes from the DPM server
- Loss of files or volumes archived to the CA ARCserve Backup server

Loss of Files From the DPM Server

If you have lost files from the DPM server, you can recover these files from the DPM server (you must have DPM administrator rights or be an end-user with end-user recovery enabled). Use Windows Explorer or Microsoft Office 2003 to access the DPM shadow copies from your workstations and recover point-in-time copies of the files.

See the *Microsoft Data Protection Manager Planning and Deployment Guide* for more information.

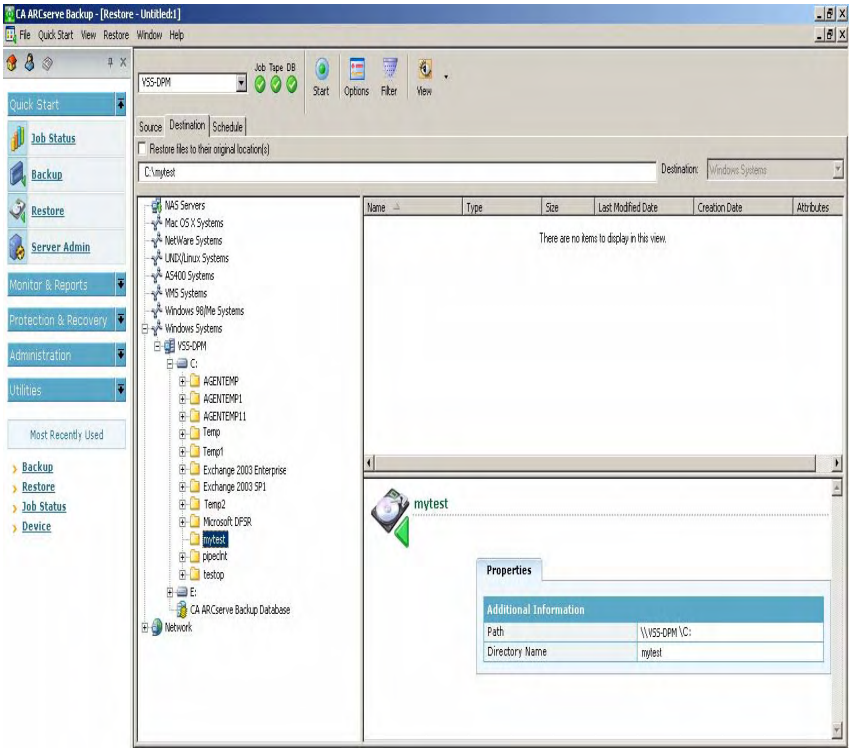
Loss of Files Moved to the CA ARCserve Backup Server

If you have lost files previously moved from your DPM server to the CA ARCserve Backup server, you can recover these files by restoring the files and moving them back to your DPM protected server with the Client Agent for Windows.

Recover From CA ARCserve Backup Server

To recover DPM-protected data from a CA ARCserve Backup server

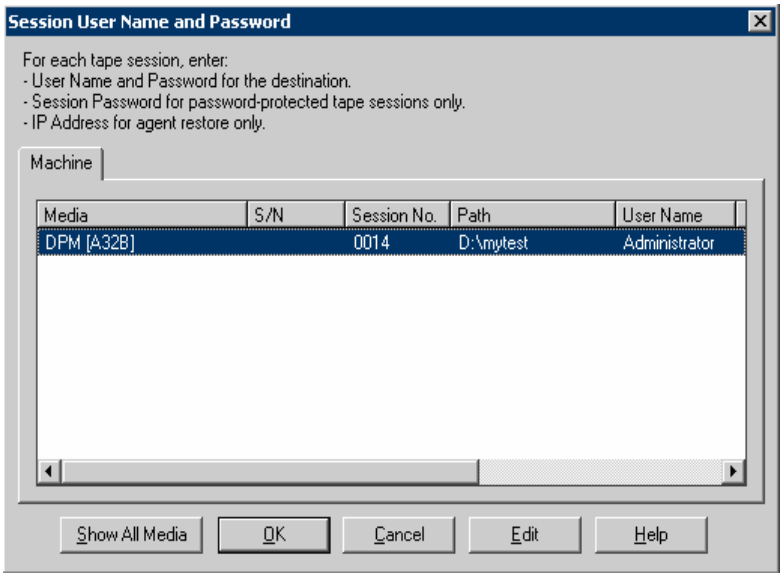
1. Log on to the administrative CA ARCserve Backup workstation as an administrative user.
2. Ensure that the volume you want to restore to is present.
3. Launch the Restore Manager.
4. Select the Restore by Tree method or Restore by Session method on the Restore Manager Source tab.
5. Click the appropriate green box next to the DPM Writer component you want to restore.
6. Clear the Restore files to their original location(s) check box, and specify the target path for your restore job on the Destination tab.



7. Select the appropriate Repeat Method on the Schedule tab.

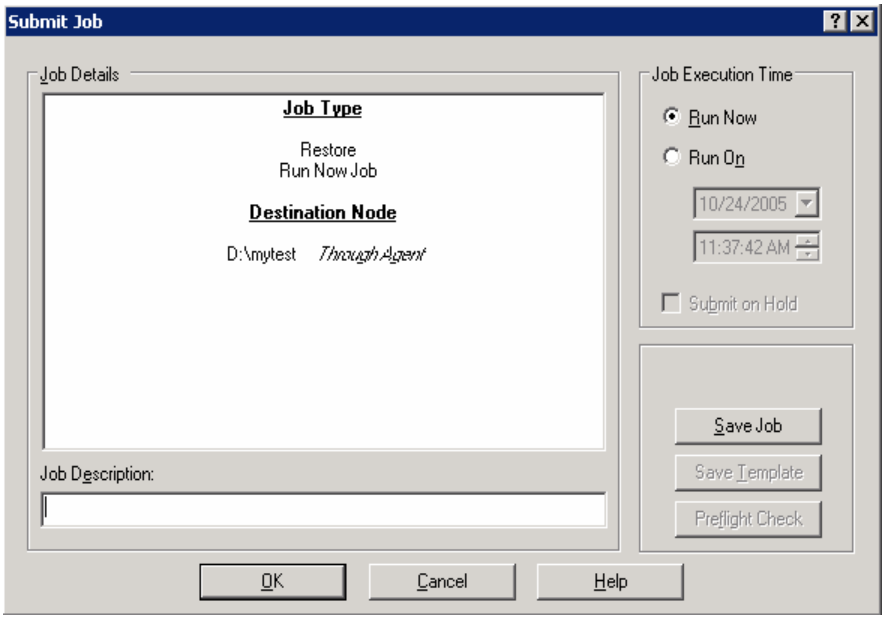
8. Click Start.

   The Session User Name and Password dialog appears.



9. Edit or confirm the information in the Session User Name and Password dialog and click OK.

   The Submit Job dialog appears.



10. Select the appropriate Job Execution Type. You can select one of the following:
    - **Run Now:** The restore job starts immediately
    - **Run On:** Enter the date and time to start the restore job
11. Click OK.

    You can monitor the job's progress using the Job Status Manager.

    Note: For more information about the Job Status Manager, see the *Administration Guide*.
12. Launch Windows Explorer, browse to the location to which you restored the files, and drag and drop the restored files to the DPM protected server.

Server Data Loss

To protect your servers from disaster, you must have installed the CA ARCserve Backup Disaster Recovery Option on the CA ARCserve Backup server, created the necessary media before a disaster occurs, and performed a full backup. We strongly recommend that you create a disaster recovery plan.

To recover successfully after a disaster, you must create disaster preparation materials before the disaster strikes. If you do not prepare these materials, you cannot recover your systems. For more information about the Disaster Recovery Option, see the *Disaster Recovery Option Guide*.

Create a Disaster Recovery Plan

As part of your disaster recovery preparations, you should develop a disaster recovery plan.

To create and test your plan, perform the following actions:

- Create a set of disaster preparation materials to be kept off site. Follow the instructions in the subsequent sections of this guide to complete this step.
- Set up a test server with a similar configuration to your original server.
- Simulate a recovery on your test server by following the disaster recovery instructions in this guide.

DPM Protected Server Loss

If you lose a DPM protected server, you must rebuild it. If you have installed the CA ARCserve Backup Client Agent for Windows and the Disaster Recovery Option on the server and have performed a full file system backup, the disaster recovery process is simple.

You can perform a disaster recovery using the CA ARCserve Backup Disaster Recovery Option by booting from recovery media and providing a disk with critical server configuration information that can be created from the CA ARCserve Backup Manager.

The restore process restores the system and boot volumes and brings the system to the state it was in when the full backup was performed.

If the system did not have the Client Agent for Windows or a full backup, it must be manually rebuilt to its previous configuration, the Microsoft DPM file agent must be installed, and the files in the DPM server must then be restored.

For more information on disaster recovery, see the *Administration Guide* and the *Disaster Recovery Option Guide*.

DPM Server Loss

Restoring the DPM server after a loss of data is similar to recovering a DPM protected server. The key difference is that you must restore the DPM databases and DPM replicas from the CA ARCserve Backup server after you have restored the operating system on the DPM server.

For more information about the Disaster Recovery Option, see the *Disaster Recovery Option Guide*.

Recover DPM Servers

To recover a DPM server using CA ARCserve Backup, the Agent for DPM, and the Disaster Recovery Option

1. Recover the operating system of DPM server using the Disaster Recovery Option.

   For information about the disaster recovery process, see the *Disaster Recovery Option Guide*.

2. Restart the system and verify that the operating system and critical system data have been restored.

3. Uninstall Microsoft Data Protection Manager 2006 using Add or Remove Programs and choose either the Remove Data or Retain Data option in the Uninstall Options dialog.

   When the uninstallation process finishes, click Close.

4. Uninstall the following DPM prerequisite software using Add or Remove Programs. You must uninstall these programs in the following sequence:

   a. SQL Server 2000 Reporting Services

   b. Internet Information Services (IIS)

   c. Microsoft SQL Server 2000 (MICROSOFTDPM)

5. Reboot your computer after all of the programs have been uninstalled.

6. Reinstall Microsoft DPM.

   Ensure that the DPM Writer service is started. Check the status of the service using Windows Administrative Tools\Services.

7. Launch the CA ARCserve Backup Manager and follow the standard restore procedures to restore the Microsoft DPM Database DPMDB and Database ReportServer to their original locations.

8. Execute the following command from C:\Program Files\Microsoft Data Protection Manager\DPM\bin\ from a DOS prompt:

   ```
   DpmSync -Sync
   ```

   If your DPM Server is not installed in its default location, check the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\Setup\DatabasePath to determine the installation path.

   Note: If your DPM Server is monitored in Microsoft Operations Manager 2005 (MOM), after you restore the DPM database, you must synchronize the alerts in MOM with those on the DPM Server. For more information, see the Data Protection Manager 2006 Management Pack Guide on the Microsoft TechNet site MOM 2005 Management Pack Guides (http://go.microsoft.com/fwlink/?linkid=50206 http://go.microsoft.com/fwlink/?linkid=50206).

9. Launch the DPM Administrator Console and add the disks to the storage pool.

   Note: You need not perform this step if your operating system has the access to the disks that were originally allocated for DPM.

10. Launch CA ARCserve Backup Manager, and follow the standard restore procedures to restore the DPM replicas to their original locations.

11. From the DPM Administrator, perform Verification with Consistency Check on each replica after recovering all of your protected resources.

    For information about these procedures, see the *Microsoft DPM* documentation.

DPM and DPM Protected Servers Loss

If you suffer wide-scale data loss, you lose your DPM server and one or more DPM protected servers at the same time. Use one of the following options under such circumstances:

- Recover your DPM server first and use it to stage the recovery of your DPM protected servers.
- Recover one or more DPM protected servers directly and restore the DPM server when the critical servers are back online.

Recover the DPM Server First

Recovering the DPM server first is a slower process. You must first recover multiple replicas to the DPM server and then restore the data to the DPM protected servers.

The main advantage of this option is that it ensures the protection of your DPM protected servers as soon as they are brought back online. However, this method requires that you have all of your usual disk storage capacity for the DPM server. In the event of a wide-scale outage, you may not have spare disk resources on hand. In addition, if you have a large number of servers to rebuild, the process may be slowed.

Recover the DPM Protected Server First

Recovering at least some of DPM protected servers first is quicker than recovering the DPM server first. CA ARCserve Backup offers built-in integration with DPM, to help you easily restore your production data from tape directly through the Client Agent for Windows running on the DPM protected server without requiring the DPM server to be running. This response time is often critical when you have mission-critical servers and data to be restored.

CA ARCserve Backup Server Loss

Recovering from CA ARCserve Backup server loss is similar to recovering from DPM protected server loss.

To recover your backup server automatically perform the following actions before a server failure:

- Install the CA ARCserve Backup Disaster Recovery Option on the server.
- Configure an alternate location for storing Disaster Recovery information when you setup your server.
- Perform regular full backups of the backup server.

  Note: For more information on performing regular full backups, see the *Disaster Recovery Option Guide*.

Reports

CA ARCserve Backup provides several types of reports. You can access these reports from the CA ARCserve Backup Report Manager. The Report Manager provides several functions to help manage both reports and logs. For more information about reports, see the *Administration Guide*.

Glossary

bare metal recovery

Bare metal recovery is the process of recovering data or rebuilding a computer after a catastrophic failure.

DPM Writer

DPM Writer is a Windows service that ensures its data is quiescent and stable-suitable for shadow copy and backup. It also collaborates with restores by unlocking files when possible and indicating alternate locations when necessary.

Microsoft Data Protection Manager 2006

Microsoft Data Protection Manager is a server software application that provides Windows NTFS file system based backup and recovery.

Microsoft Windows Server System

Microsoft Windows Server System is a portfolio of integrated server software products that provides the infrastructure for IT operations, application development and integration, security, and collaboration.

replica

Replica is the container that hosts the protected volumes or share folders of the DPM protected servers. Each replica represents a share folder or volume of a DPM protected server.

Virtual Tape Library (VTL)

VTL is a storage system that includes a disk, a processor, and software to emulate tape or a tape library.

Volume Shadow Copy Service (VSS)

VSS provides the backup infrastructure for Microsoft Windows Server 2003 and Microsoft Windows XP operating systems, and a mechanism for creating consistent point-in-time copies of data (shadow copies). Applications can continue to write data to the disk volume during the shadow copy creation process, eliminating the need to perform backups before or after business hours. Additionally, a volume copy backup lets you perform file restores, minimizing administrative overhead for basic restore operations.

Index