White Paper

Using BrightStor® ARCserve® Backup With Microsoft Data Protection Manager

CA and Microsoft Corporation
September 2005

Abstract

This paper provides guidance on integrating Computer Associates BrightStor ARCserve Backup and Microsoft System Center Data Protection Manager (DPM) for designing an optimum data protection solution. It explains how DPM works and how the customer will benefit from using it in conjunction with BrightStor ARCserve Backup. It gives guidance on issues and configuration questions that storage administrators will encounter in deploying the combined solution. It also addresses common backup and recovery scenarios to assist in disaster recovery planning.

Contents

Introduction

In an increasingly competitive business environment, the access and availability of information is often the differentiator between success and failure. The proliferation of the internet and movement toward on-demand computing has only heightened the need to effectively leverage information assets to increase revenue and profit opportunities. Data is the heart of any organization's information assets.

With all the potential disasters in today's world — fire, flood, theft, hardware failure, human error, virus infection, etc. — every organization needs an effective strategy to protect its critical data. Increasingly innovative disk based data protection strategies are being used to improve operational efficiency and performance of data protection solutions. Taking advantage of reliability and the cost-effectiveness disk technologies, IT administrators can not only reduce cost but also offer protection at a level that was never possible before. A disk-tape combined approach provides a number of benefits when compared to traditional tape only backup methods. For example, faster file and server recovery, faster backup, easier management and better use of network bandwidth.

Microsoft System Center Data Protection Manager (DPM) and Computer Associates BrightStor ARCserve Backup create a complimentary data protection solutions designed to work with each other and leverage the disk based technologies to solve data protection challenges such as meeting backup windows, recovery point and recovery time objectives.

This paper discusses how to optimally deploy DPM and BrightStor ARCserve Backup to meet your data protection requirements.

About Microsoft DPM

Microsoft DPM, the newest member of the Microsoft Windows Server System focuses on disk-based data protection and recovery. DPM works with Microsoft Windows Server operating systems to deliver best-in-class data protection services. DPM uses replication, Volume Shadow Copy services infrastructure and a rich, policy-driven engine to provide businesses of all sizes with better control of their recovery infrastructure, continuous protection, and rapid data recovery at the lowest total cost of ownership.

After DPM servers are installed, you use the DPM Administrator Console to push the DPM agent to each production server and create your protection groups. A protection group is a collection of data resources that share the same protection policy, such as shared folders and disk volumes. You define the data to protect, at which point the DPM agent begins to replicate the designated data to the DPM server according to the policy-defined schedule. The DPM agent tracks the data, replicates only the changed blocks, validates the replica, and corrects errors. By performing incremental replication at the disk block level, DPM can reduce the bandwidth required by your data protection solution.

As DPM fully integrates with VSS, protection policy can define how many shadow copies or snapshots to make available, independently of the replication schedule. IT administrators can then access these snapshots to perform file recoveries as requested. Users can directly access the snapshots and recover files themselves, or recover of files from within Windows Explorer and Microsoft Office 2003 applications.

About BrightStor ARCserve Backup

With an installed base of more than 350,000 users, BrightStor ARCserve Backup is a leader in data protection solution for distributed servers, databases, and applications. Certified by Microsoft on all of their server platforms, BrightStor ARCserve Backup provides reliable, secure and high performance backup and restore with flexible scheduling, easy administration, broad device and platform support. It allows administrators to customize data protection strategies based on business needs, reducing administrative worries and operating cost. It provides integrated *e*Trust® Antivirus scan and cure capabilities, as well as an extremely easy to use interface. The modular design allows administrators to procure and configure BrightStor ARCserve Backup according to their requirements on an as-needed basis. Administrators get the advantage of a solution that grows with their business — they do not have to replace their backup solution as their data protection requirement grows.

BrightStor ARCserve Backup and Microsoft DPM — Better Together

MS DPM and BrightStor ARCserve Backup together provide a comprehensive solution for all of the data protection needs of the enterprise. BrightStor ARCserve Backup adds critical capabilities to MS DPM offering such as:

- **Protection of the DPM Server.** Since DPM server protects the data of many server systems, it is vitally important to protect the DPM server itself. If the DPM server fails, the data on remote servers is unprotected and data lost from remote servers cannot be recovered from the DPM server. BrightStor ARCserve Backup offers protection to the DPM server itself and in case of a failure, the DPM server and the data it is protecting can be recovered very quickly from backups.
- **Protection of DPM Replicas.** DPM server collects file system data from DPM agents and stores them in disks. As disks are of finite capacity, it is only possible to

store a limited number of versions of files in the DPM server. BrightStor ARCserve Backup adds the capability to move the data from the DPM server to disk arrays/tape libraries and make them available for restore, to the DPM server or directly to the DPM agent system.

- **Disaster Recovery and Long-Term Archiving.** Long-term archiving of data in tapes for disaster recovery and regulatory compliance remains a critical data protection need for all companies. Data protected by DPM can be efficiently and securely moved to tapes, archiving disks and virtual tape libraries by BrightStor ARCserve Backup. Encryption technology in BrightStor ARCserve Backup ensures that the data in the tapes can not be misused even if the tapes are lost.
- **Protection of Applications.** DPM offers protection for file servers and BrightStor ARCserve Backup extends this capability to protection of business critical applications such as Microsoft Exchange Server, Microsoft SharePoint Portal and Microsoft SQL Server.
- **Bare Metal Recovery of DPM Server and Production Servers.** Using MS DPM, administrators and end-users can perform fast and efficient file recoveries. However if there is a total server crash, the server has to be reconfigured and reinstalled before DPM can restore files, increasing recovery time significantly. Using BrightStor ARCserve Backup, administrators can reduce recovery time after server failure by performing bare metal recovery.
- **Protection of Platforms Not Supported by DPM.** BrightStor ARCserve Backup extends data protection to servers beyond those supported by DPM such as NAS filers, non-Windows systems etc.
- **Direct Recovery of Archived Files.** BrightStor ARCserve Backup allows fast recovery of files archived to tape by restoring them to the DPM server, the originating server or to any other alternate location.
- **Integrated Anti-Virus Capabilities.** DPM replicated files from the production server to the DPM server whenever they change, even when the changes are initiated by virus attacks or other types of file corruption. It is possible to lose the DPM, both the production server files as well as the DPM replicas, in case of a virus attack. Integrated antivirus capabilities in BrightStor ARCserve Backup protects from such scenarios by checking for viruses as the files are backed up.
- **Integrated Encryption Capabilities.** BrightStor ARCserve Backup can encrypt data as they are moved to tape, preventing unauthorized use of data in tapes, in case they are misplaced.
- **Integrated SRM Capabilities.** SRM capabilities can be added to BrightStor ARCserve Backup to understand the business value of the data being protected and adjust the data protection level accordingly.

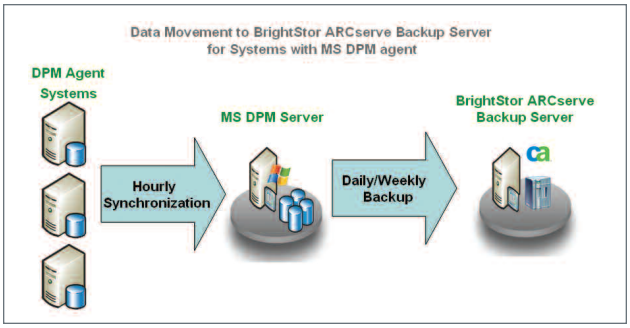

Figure 1. Data Movement to BrightStor ARCserve Backup Server for systems with DPM agent.

Using MS DPM and BrightStor ARCserve Backup

BrightStor ARCserve Backup provides seamless integration with the DPM server to deliver an optimal data protection solution for your company. BrightStor ARCserve Backup not only protects the DPM server, adding long-term archiving capabilities to DPM, but also offers protection for applications and provides feature rich disaster recovery capabilities. Using the Microsoft recommended Volume Shadow-Copy Service (VSS) infrastructure, BrightStor ARCserve Backup takes snapshots of the DPM server, which includes the DPM database and replicas, and then creates a backup of the snapshots on the tape or disk devices. You create backups of your data from the replicas on the DPM server rather than from the live data on the production servers. Since you are backing up from a read-only snapshot of the data, you can do this at any time without affecting your production server performance. Network utilization is reduced as the DPM agent only transfers changed blocks over the network and not the changed files. With BrightStor ARCserve Backup, you can restore DPM-archived data directly from your archive media to your DPM protected server using BrightStor ARCserve Backup without involving the DPM server.

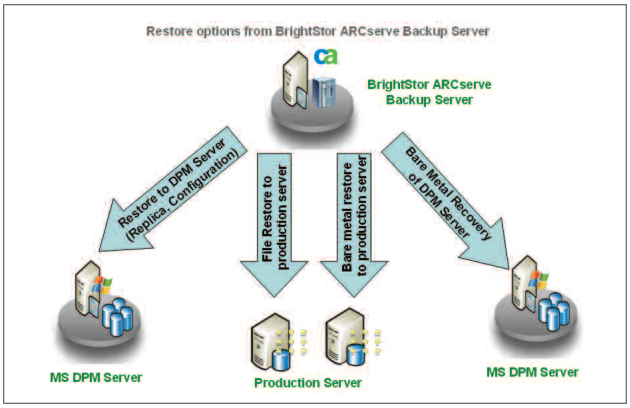

Figure 2. Restore with BrightStor ARCserve Backup.

Planning Deployment of DPM with BrightStor ARCserve Backup

BrightStor ARCserve Backup is a flexible and powerful backup solution. It offers a high degree of scalability and flexibility along with support for multiple operating systems and specialized agents for many applications such as Microsoft Exchange Server and Microsoft SQL Server 2000. By using BrightStor ARCserve Backup with DPM, you can optimize your backup infrastructure, offering a higher level of data protection at a lower total cost of ownership. The figure below demonstrates a common scenario for deploying DPM and BrightStor ARCserve Backup together.

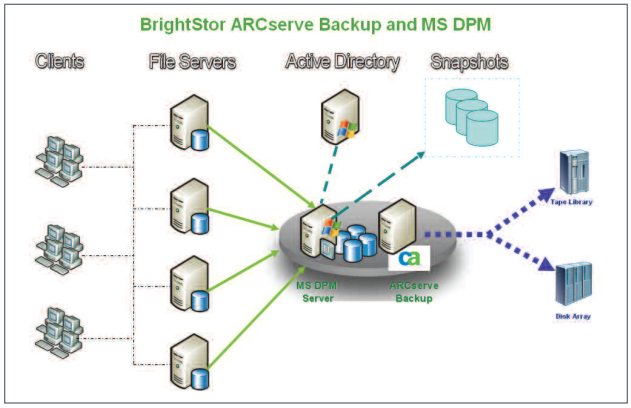

Figure 3. BrightStor ARCserve Backup and MS DPM deployment.

Understanding What You Need

An effective data protection strategy should be guided by business requirements. The first step for planning a data protection solution is to understand what needs to be protected and an estimate of the business value of the application or data that is being protected. With this information you can develop data protection policies that reflect your business needs establishing an intelligent storage management approach for you business.

RPO and RTO. Business value of data and applications should be expressed in terms of Recovery Time Objective (RTO) and Recovery Point Objectives (RPO). The RTO measures how long it is acceptable for an application to be unavailable (measured from short to long). Restoring from offsite tapes can't start until the tape is onsite and this can take hours; recovering from disk may be started immediately and progress quickly. The RPO measures the age of data that is restored (measured from low to high). A worst-case scenario for a disk backed up every day is a RPO of just under 24 hours; this would occur, for example, when a disk fails just prior to the start of the daily backup. Data with highest business value usually has the lowest RPO and shortest RTO. There can be exceptions. For example, regulatory compliance data archives are very high in business value but a long RTO may be acceptable as such data will rarely be required at extremely quick notice.

RTO varies on the nature of failure. It is important to note that different data protection technologies will provide very different RTO depending on the type of failure. DPM offers excellent RTO in case of file level failure. However, in case of a total server crash the RTO is going to be significantly higher as a new server will have to be manually configured before DPM can be used to restore file data. Bare metal recovery solutions such as BrightStor® ARCserve® Backup Disaster Recovery Option can significantly reduce RTO in such scenarios. If there is a need to recover archived files directly to the production server bypassing the DPM server, the presence of the BrightStor ARCserve Backup agent on the production server enables you do so, substantially reducing RTO for archived data. This capability can be invaluable in scenarios where there has been multiple server failures and you want to bring back the revenue generating systems online before recovering the DPM server. Without the agent, the DPM server has to be recovered before the production server is recovered but this may not satisfy the RTO of the data being protected.

Choosing between local or over the network backup of DPM server. BrightStor ARCserve Backup can be installed on the same system as the DPM server and can backup the DPM data and configuration information locally, or can be installed remotely and backup multiple DPM servers over the network. With local backup, the tape drive or virtual tape library (VTL) on which the data is being archived will have to be directly connected to the DPM server. The DPM server should also be capable of handling backup task loads and DPM server loads simultaneously. With remote backup, you gain the flexibility of deployment but if the DPM server has a very large amount of data, network bandwidth may be incapable of transferring all of it to the backup server. If the DPM server and BrightStor ARCserve Backup are installed in the same system, DPM data can be directly moved to tape from the disk, bypassing the network.

Protecting System State. Windows system state consists of critical set of files and configuration settings that are needed for restoring a Windows operating system back to its previous state. Information stored in system state include the Active Directory database, registry files, network settings, security settings, latest patches and other vital files. Thus system state is critical not only for recovering crashed systems using bare metal recovery solutions but also for the ensuring the security of the enterprise. The alternative to using system state backup is to go through the time consuming and manual process of re-configuring a server in case of a failure. DPM cannot protect system state information directly. For protecting system state we recommend you install a BrightStor® ARCserve® Backup Client Agent for Windows and perform regular backups. In case of a system state failure, use the weekly backup to restore the server. In case of file corruption you should use the MS DPM to recover the lost files.

Components of Data Protection Architecture

A BrightStor ARCserve Backup/DPM data protection solution will have the following components which have to be deployed according the RTO/RPO requirements as well as the technical considerations discussed above.

MS DPM Agent. For protecting file server data with minimal data loss and low network bandwidth usage. Offers end-user driven recoveries.

MS DPM Server. DPM server protects the DPM agent systems by storing their data in disk arrays.

BrightStor ARCserve Backup. BrightStor ARCserve Backup server protects and backs up your mission-critical database applications and systems through BrightStor ARCserve Backup application agents and Client Agent for Windows to disk arrays, tape libraries and VTLs.

BrightStor ARCserve Backup Agent for Microsoft DPM. This protection agent should be installed on the server running MS DPM. BrightStor ARCserve Backup Server will be use this agent to protect the DPM server.

BrightStor ARCserve Backup Client Agent for Windows with Open File Technology. BrightStor ARCserve Client Agent for Windows should be installed on the production file servers which need to be recovered promptly from any type of failure. This agent can backup system state information and adds the capability to perform bare metal recovery of the server as well as the capability of restoring files directly from the ARCserve server to the production server. DPM agents can not backup system state configuration information and thus DPM backups can not be used for bare metal recovery. These functionalities work even if the DPM server is offline, implying if the DPM server crashes the restore of file system data and bare metal recovery can be performed directly from the BrightStor ARCserve Backup server. In addition, Open File technology enhances the BrightStor ARCserve Backup Client Agent for Windows by adding the capability to safely backup files opened by applications. With using BrightStor ARCserve Client Agent for VSS, you will be able to take the advantage of the point-in-time backup feature of Microsoft Volume Shadow Copy Service (VSS) that allows open files to be backed up. Applications and large VSS-aware databases can also be backed up ensuring transactional consistency during the backup process.

BrightStor ARCserve Backup Application Agent. Application specific agents for MS Exchange, MS SQL, MS SharePoint and others offers the ability to backup and restore applications when they are online, without interrupting application access.

One or more of the above components can be in the same server.

Sample Deployment

The list below consists of the servers commonly found in a small/medium business environment and shows a typical deployment of BrightStor ARCserve Backup.

Type of Data	Components to Be Deployed
Microsoft Exchange Server This server is the backbone of the company's email communication. Business requirement of very low RPO and RTO from all types of failure. All emails need to be retained for regulatory compliance.	▪ BrightStor® ARCserve® Backup Agent for MS Exchange ▪ BrightStor ARCserve Backup Client Agent for Windows
Microsoft SQL Server Hosts companies client, order processing and HR databases. Business requirement of very low RPO and RTO from all types of failure.	▪ BrightStor® ARCserve® Backup Agent for MS SQL ▪ BrightStor ARCserve Backup Client Agent for Windows
Microsoft SharePoint Server Directly affects employee productivity. Business requirement of very low RTO.	▪ BrightStor® ARCserve® Backup Agent for MS SharePoint Agent ▪ BrightStor ARCserve Backup Client Agent for Windows
Domain Controller and Network Administration Provides network security, and network administration. Business need of low RTO.	▪ MS DPM Agent ▪ BrightStor ARCserve Backup Client Agent for Windows ▪ BrightStor® ARCserve® Backup Agent for Open File
Business Critical File Servers Stores business critical business information. Very low RTO and RPO needs.	▪ MS DPM Agent ▪ BrightStor ARCserve Backup Client Agent for Windows ▪ BrightStor ARCserve Backup Agent for Open File
Servers — Non-Business Critical Stores business information. High recovery time acceptable.	▪ MS DPM Agent
Backup Server with 1 TB disk array and tape drive Server allocated for data protection task.	▪ MS DPM Server ▪ BrightStor ARCserve Backup Server with Disaster Recovery Option ▪ BrightStor ARCserve Backup Agent for MS DPM

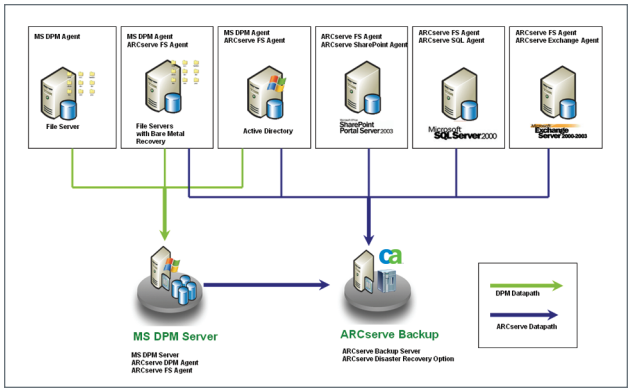

Figure 4. MS DPM and BrightStor ARCserve Backup deployment.

Deploying BrightStor ARCserve Backup and DPM

The following tasks must be performed to deploy DPM and BrightStor ARCserve Backup in your environment:

1. Installation and configuration of MS DPM:
   - Install the DPM server.
   - Allocate storage on the DPM server.
   - Install the DPM agent on production servers.
   - Create and configure protection groups.
   - Start DPM Writer service
2. Install and configure BrightStor ARCserve Backup
   - Install BrightStor ARCserve Backup server, options and Agents.
   - Launch BrightStor ARCserve Backup Manager, and create the backup jobs for Microsoft DPM Writer.
   - Schedule backups and submits the jobs.

For details of the installation process, please consult respective product documentation listed in the reference section at the end of this document.

Deploying DPM

When you are ready to introduce DPM into your production environment, the first task you need to perform is to install the DPM server. This involves installing and configuring DPM. Detailed instruction can be found in the document "Data Protection Manager Planning and Deployment Guide."

Before you begin the deployment process, verify that your deployment meets the following requirements:

DPM Server Requirements

- The domain controllers are running either Windows Server 2003 or Windows 2000 Server.
- Windows 2000 Server domain controllers have Windows 2000 Server Service Pack 3 or later installed and schema updates enabled if end-user recovery will be deployed.
- The domain has the Kerberos V5 authentication protocol enabled. This is the default.
- The server is running either Windows Server 2003, Windows Storage Server 2003 and with Microsoft .NET Framework 1.1 installed. Latest Service Packs must also be applied.
- The server meets the hardware and software requirements for Microsoft SQL Server 2000 Service Pack 4 (see **microsoft.com/sql/default.mspx** for more details).
- The server is a member of the same Active Directory domain as the production servers it will protect, even if the production servers are located across a WAN link. You will need at least one DPM server for every domain in which protected servers reside.
- The server is not a domain controller or an application server.
- The server has at least two disk volumes available:
  - One disk volume is dedicated to the system and DPM installation files.
    - One or more disk volumes are dedicated to the storage pool.
    - The server is configured to use NTFS.
  - The server has a persistent connection to any branch office file servers it protects.

Production Servers Where DPM Clients Will Be Installed

- The server is running Windows Server 2003, Windows Storage Server 2003 or Windows 2000 Server with appropriate service packs and hot fixes.
- The server is a member of the same Active Directory domain as the DPM server that protects it.

- The server is not part of a cluster. Clustered file servers cannot be protected.
- The server has a minimum of 500 megabytes (MB) of free space available on each volume to be protected. This space holds the synchronization log, which must be at least 500 MB.

See Chapter 1 of the *Data Protection Manager Planning and Deployment Guide* for more information on how DPM works and common deployment and recovery scenarios.

Installing the DPM Server

After you have verified that your servers meet the prerequisites for their roles, you can install the DPM software on your DPM server. The installation process will install DPM, SQL Server 2000 with latest patches and hotfixes as well as IIS. At least one DPM server is needed in each Active Directory domain that contains a production server you want to protect. This requirement may be particularly relevant in many branch office deployment scenarios. Although DPM relies on Active Directory for discovery of new servers, it does not require a domain controller to be located on a local network segment.

Allocating Storage on the DPM Server

The next step in deploying DPM is to create the storage pool. The storage pool consists of one or more disk volumes that are used exclusively by DPM to store replicas, shadow copies, and logs. DPM will use the entire volume and reformat it, so ensure that you have no data on the devices you add. You can use three types of disk volume: direct attached storage (DAS), storage area networks (SAN), or Windows-certified iSCSI devices. You can add RAID volumes to your storage pool, but some common RAID configurations such as RAID 5 are less suitable for use with DPM because of the characteristics of their write performance. After installation DPM will scan Active Directory to find file servers to protect. After DPM finds them, you will need to deploy the DPM File Agent on the servers you want protect using DPM.

Creating and Configuring Protection Groups

After the DPM agent has been installed on your production file servers, you can begin to configure DPM and designate which disk volumes and network shares to protect. You do this by defining protection groups, which are collections of data sources that share common usage characteristics and are protected under the same policies. Each protection group consists of three elements:

- The disk allocation reserves space in the storage pool for the log files, replicas, and shadow copies of the data sources in the protection group.
- The replication schedule determines how frequently the DPM agent synchronizes the data source to the DPM server.
- The snapshot schedule determines how often shadow copies are made of the replica data.

Deploying BrightStor ARCserve Backup

Deploying BrightStor ARCserve Backup involves the following steps:

1. Installing and configuring BrightStor ARCserve Backup application and file system agents
2. Installing and configuring BrightStor ARCserve Backup server and options
3. Configuring BrightStor ARCserve Backup to protect DPM — creating jobs and data protection schedule

(Please consult *BrightStor ARCserve Backup for Windows Getting Started Guide* for further details.)

Installing and Configuring BrightStor ARCserve Backup Application and Client Agents

The first step for deploying BrightStor ARCserve Backup is to install the application and file system agents in the production servers to be protected. The installation can be performed locally or remotely using BrightStor® remote deployment technology. The ARCserve Backup Agent for Microsoft DPM should be installed on the DPM server. If the ARCserve Backup server is to be installed on a remote system, ARCserve Backup Client agent should also be installed on the DPM server. Application specific agents should be installed in corresponding servers and configured according to documentation.

Installing and Configuring BrightStor ARCserve Backup Server

If the DPM server is to be backed up over the network, BrightStor ARCserve Backup server can be installed on any server with a tape library or other storage device attached to it. If DPM server is to be backed up locally, ARCserve Backup Server and ARCserve Backup Agent for Microsoft DPM should be installed on the server where Microsoft DPM is installed.

BrightStor ARCserve Backup can be installed on any Windows server system which fulfills the following requirements:

1. It should be running Internet Explorer 6.0 with the latest service packs applied.
2. All storage devices should be connected to the machine.

3. If you are using a fiber or SCSI device, ensure that your BrightStor ARCserve Backup server has a SCSI/Fiber controller or adapter supported by both Windows and BrightStor ARCserve Backup. BrightStor ARCserve Backup can support an unlimited number of installed SCSI controllers.

4. To ensure that your hardware devices are compatible and that BrightStor ARCserve Backup can communicate with your system, obtain the latest Certified Device List from the Computer Associates website.

Configuring BrightStor ARCserve Backup to Protect DPM

The next task is to configure BrightStor ARCserve Backup to protect DPM server, application agents and the Client Agents. Different backup jobs will have to be created for each but only the configuration for jobs protecting the DPM server is discussed here. For details on other type of jobs please consult the BrightStor ARCserve Backup Administrator's Guide.

Data in DPM Server. Before configuring backup jobs for DPM server, it helps to get an understanding of the types of data in the DPM server.

- **DPM Server.** DPM server consists of database with all the configuration information and meta-data used by DPM to protect the DPM environment. Without this information, the DPM server will have to be reconfigured and DPM data re-synchronized from the production servers. This information is protected using the BrightStor ARCserve Backup Agent for Microsoft DPM.

- **DPM Replicas.** DPM replicas are the data collected by DPM agents and sent over to the backup server. Each replica represents a share folder or volume of a DPM protected server. This information is protected using the BrightStor ARCserve Backup Agent for Microsoft DPM.

- **DPM Server System State.** This is information regarding the server hosting DPM. In case this information is lost, a new server has to be provisioned, and DPM installed on it to continue data protection tasks. This is protected through the BrightStor ARCserve Backup Client Agent for Windows.

All the above types of data will need to be protected by BrightStor ARCserve Backup. For those production servers which have DPM agents installed, backup jobs should backup data from the replicas in the DPM server for those systems. This provides the advantages of greatly reduced backup Windows and reduced network traffic.

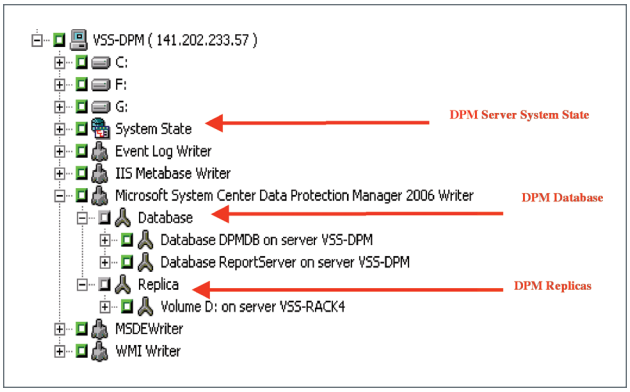

Figure 5. DPM data represented in BrightStor ARCserve Backup manager.

Protecting DPM Replicas. Backup jobs in BrightStor ARCserve Backup should protect the data stored within DPM. You can back up at the server level or select specific shares, volumes, folders, or files on the server, according to your protection strategy. It is recommended to dedicate a media set for each production server; this allows you to quickly and easily restore that server's data in the event a rebuild or restore is needed.

By default DPM will scan the Active Directory once a day to alert you to any changes, such as new servers and volumes. After you know about them, you can then add them into your existing protection groups and create new BrightStor ARCserve Backup jobs for them.

The following steps demonstrate how to create a new volume-level backup job against a DPM server using BrightStor ARCserve Backup:

1. Make sure DPM Writer services is started through Windows Control Panel ->Services.

2. Log on to the administrative workstation as an administrative user, and launch the BrightStor ARCserve Backup Manager.

3. Click Backup from the Quick Start menu at the left of BrightStor ARCserve Backup Manager.

4. In the Backup Source window, expand your Windows 2003 Server which has DPM installed.

5. Expand Microsoft System Center Data Protection Manager 2006 Writer, and select the desired source(s) to backup.

6. Click Destination tab to specify the data should be archived to.

7. Click Schedule tab to schedule when the backup job should start.

8. Click Start button to submit the job.

(Please see the *BrightStor ARCserve Backup Administrator Guide* for more information on configuring the various backup job options.)

Protecting DPM Server. The above process should be followed to protect the DPM databases.

The backup processes involved for DPM server information and BrightStor ARCserve Backup Server are as follows:

1. At the scheduled time, BrightStor ARCserve Backup server contacts the DPM server through the Microsoft Volume Shadow Copy (VSS) Service and requests the creation of a shadow copy of DPM Writer.

2. VSS coordinator then instructs the DPM Writer to prepare the creation of the shadow copy.

3. BrightStor ARCserve Backup server then performs a backup of the shadow copy to either tape of disk device without impacting the DPM server.

4. BrightStor ARCserve Backup server releases the shadow copy after the backup job is done and DPM server deletes the shadow copy.

Protecting DPM Server System State. To protect against loss of the DPM server, you should create an additional backup job that archives the DPM server system state data. This will be used to recover the DPM server itself in case of a failure.

Scheduling Backups

After you have created the backup job in BrightStor ARCserve Backup you need to schedule it to run on a regular basis. Because you are backing up from a shadow copy of the protected data, you no longer need to run your backup jobs in the night. Considering the possible synchronization delay on the replicas, you need to keep your DPM replication schedules in mind when scheduling your backup jobs allowing sufficient amount of time for replication to complete before your backup jobs kick off.

You should run the backup jobs on a regular basis to ensure recoverability in the event the failure of the DPM server. The frequency of your backups depends on the amount of data you are willing to risk. If you must ensure that documents created each day are available for recovery, you should run a backup at least once a day.

Recovery Scenarios

The best data protection system in the world is useless if you cannot successfully restore your data when files are lost. Data loss events can happen at several stages:

- The loss of individual files.
- The loss of a production server.
- The loss of the DPM server.
- The loss of the BrightStor ARCserve Backup server.
- Loss of an entire site that requires rebuilding of multiple servers.

The following section discusses each type of failure scenario and how to recover from them. Please note, loss of file or application data in servers in which DPM agent is not installed is not discussed here. Please consult *BrightStor ARCserve Backup Administrator's Guide* for further information.

Loss of Individual Files

There can be two scenarios of recovering individual files and volumes protected by DPM server. First, the files may be available in the DPM server itself and second, the version of the file needed may have been removed from the DPM server to the BrightStor ARCserve Backup server.

Recovering files from the DPM Server. If the version of the file that needs to be restored is available in the DPM server, the end user or the DPM administrator can recover the files, depending on the configuration of the DPM environment. End-user file recovery is one of the key features of DPM. In case of your data loss events, administrators or users will be able to use Windows Explorer or Office 2003 applications to easily access the DPM shadow copies directly from their workstations and recover point-in-time copies of their files. Please consult Data Protection Manager Planning and Deployment Guide for details.

Recovering files from BrightStor ARCserve Backup server. The process of recovering DPM-protected data from BrightStor ARCserve Backup is extremely simple if there is a BrightStor ARCserve Backup Windows Client Agent for Windows installed in the production server. This process can be followed even if the DPM server is unavailable, allowing business critical servers to be recovered before the DPM server is recovered. The ability to recover business critical servers without going through time consuming DPM server recovery process can be extremely valuable in case of multiple server failures. You need to know which server the desired files were originally on; from there, it is a

straightforward process to recover it to a production server running BrightStor ARCserve Backup Windows Client Agent using the following steps:

1. Log on to the administrative workstation as an administrative user and ensure that the volume you want to restore to is present.
2. Launch the BrightStor ARCserve Backup manager.
3. Click Restore from the Quick Start menu at the left of ARCserve Backup manager, and select either Restore By Tree or Restore By Session to view backup sessions.
4. Select the desired session or expand the session tree to select an individual file or folder.
5. Click Destination tab to specify where the data should be restored.
6. Click Schedule tab to schedule when the backup job should start.
7. Click Start button to submit the job.

Recovering Files from BrightStor ARCserve Backup Server for the Version of the Files That No Longer Exist on the DPM Server and ARCserve Windows Client Agent for Windows is Not Installed on the Production Server

1. Log on to the administrative workstation as an administrative user and launch the BrightStor ARCserve Backup manager.
2. Click Restore from the Quick Start menu at the left of ARCserve Backup manager, and select either Restore By Tree or Restore By Session to view backup sessions.
3. Select the desired session or expand the session tree to select an individual file or folder.
4. Click Destination tab, uncheck "Restore files to their original locations," and specify where the data should be restored on the server where DPM is installed.
5. Click Schedule tab to schedule when the backup job should start.
6. Click Start button to submit the job.
7. Launch Windows Explorer, browse to the location where you just restored the files, and drag & drop the restored files to the production server.

Loss of Production Server

If you lose a production server, you will need to rebuild it. If a BrightStor ARCserve Backup Client Agent for Windows was installed on the server and a full file system backup was performed, the process of performing bare metal recovery is extremely simple. This process can be accomplished entirely using the BrightStor ARCserve Backup Disaster Recovery Option as discussed previously. You initiate a bare metal recovery by booting off a recovery media and providing a floppy with critical server configuration information that can be created from the BrightStor ARCserve Backup manager. The Restore process restores the system and boot volumes and recovers the system to a state when the full backup was performed. If DPM server contains more recent versions of the file than the full backup, these files can be restored to the production server subsequent to the bare metal recovery. In case a system did not have BrightStor ARCserve Backup Client Agent for Windows installed or a full machine backup available, it has to be manually rebuilt to its previous configuration, installed with DPM agent and then the files in the DPM server have to be restored to it.

Please consult *BrightStor ARCserve Backup Administrator's Guide* and *BrightStor ARCserve Backup Agent for Microsoft DPM Guide* for further information on bare metal recovery.

Restoring the DPM Server

Restoring the DPM server after a data loss event is, for the most part, like recovering a production server. The key difference is that after you have restored the operating system, you must restore the DPM databases and replica data from the BrightStor ARCserve Backup server.

The following steps demonstrate how to recover a DPM server using ASR:

1. Perform bare metal recovery of the DPM server using BrightStor ARCserve Backup Disaster Recovery Option, following the steps given above.
2. When the system restarts after the recovery process, verify that the operating system, critical system data, and DPM application files have been restored.
3. Follow standard BrightStor ARCserve Backup restore processes to restore the DPM databases.

4. From a command line, run the *\Program Files\Microsoft Data Protection Manager\2006\bin\DPMSync.exe* utility to move the database and log files to the proper location. This utility also synchronizes the database with the current state of the server.

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

6. Reallocate space in the storage pool for each replica and select how the initial synchronization will happen:
   - If you choose disk-to-disk initialization, the DPM server will synchronize the replica with the current data on the production server. If this is not the latest data, you can follow the preceding file recovery procedure to restore the latest backups from tape. This option can have a large impact on network bandwidth and usage.
   - If you choose media load, DPM will specify the locations on the DPM server system partition you need to restore the data to. Follow standard BrightStor ARCserve Backup recovery processes to retrieve the missing data from your tape backups.

7. After all of your protected resources have been recovered, use the DPM Administrator to perform verification with consistency check on each replica.

Restoring BrightStor ARCserve Backup Server

Recovering from loss of BrightStor ARCserve Backup server is similar to recovering from loss of a production server. Bare metal recovery provided by BrightStor ARCserve Backup Disaster Recovery Option will automatically recover the backup server. However, it is critical to ensure you take the following two steps before a server failure:

1. Install Disaster Recovery (DR) Option on the BrightStor ARCserve Backup server and configure the "alternate location" during setup. Installation of the Disaster Recovery Option ensures you will be able to perform a bare metal recovery of the server. Configuring "alternate location" ensure vital server configuration information is stored in multiple location and is not lost if the backup server crashes.

2. Perform regular full backups of the backup server.

Recovering from Multiple Server Failures

In a case of wide-scale data loss, you could lose your DPM server and one or more production servers at the same time. In this case, you need to decide the order in which you will recover your servers. You have two basic choices: recover your DPM server first and use it to stage recovery of your production servers, or recover one or more production servers directly and restore the DPM server when the critical servers are back online. Both options have their advantages and disadvantages.

Recover the DPM server first. Recovering the DPM server first will probably be a slower process, because you have to recover multiple replicas to the DPM server and then restore the data back to the production servers. This requires you to have all of your usual disk storage capacity for the DPM server; during a wide-scale outage, you may not have the spare disk resources on hand. Another disadvantage to this method is that the DPM server is a bottleneck; this option does not scale well if you have a large number of servers to rebuild. The main advantage of this method is that it ensures that your production servers are once again being protected as soon as they are brought back online.

Recover the production servers first. Recovering at least some of your production servers first will in many circumstances get them up and running more quickly than the other option. Because BrightStor ARCserve Backup offers built-in integration with DPM, you can easily restore your production data from tape directly through BrightStor ARCserve Backup Client Agent for Windows running on the production server without requiring the DPM server to be running. That response time is often critical when you have mission-critical servers and data that need to be restored.

Reference

This document provides an overview of deploying BrightStor ARCserve Backup and MS DPM for protecting your company's data. Following are the sources of information will provide further details needed for an implementation.

- Microsoft Data Protection Manager home page — **microsoft.com/dataprotectionmanager**
- Data Protection Manager Planning and Deployment Guide — **go.microsoft.com/fwlink/?linkid=43087**.
- BrightStor ARCserve Backup Getting Started Guide
- BrightStor ARCserve Backup Administrators Guide
- BrightStor ARCserve Backup Disaster Recovery Option Guide
- BrightStor ARCserve Backup Agent for Microsoft DPM Guide

For the latest information about Windows Server 2003, see the Windows Server 2003 Web site: **microsoft.com/windowsserver2003**.

For the latest information about data management and protection solutions from CA please see: **ca.com/brightstor**.

About CA

CA (NYSE:CA), one of the world's largest management software companies, delivers software and services across operations, security, storage, life cycle and service management to optimize the performance, reliability and efficiency of enterprise IT environments.

For more information, please call 1-877-246-3674 or visit ca.com/brightstor.

Quality System
Quality Endorsed Company
ISO 9001
Lic. 2443

MP292741205