Professional Expertise Distilled

Microsoft Data Protection Manager 2010

A practical step-by-step guide to planning deployment, installation, configuration, and troubleshooting of Data Protection Manager 2010

Steve Buchanan

[PACKT] PUBLISHING enterprise professional expertise distilled

Microsoft Data Protection Manager 2010

A practical step-by-step guide to planning deployment, installation, configuration, and troubleshooting of Data Protection Manager 2010

Steve Buchanan

[PACKT] PUBLISHING enterprise professional expertise distilled

BIRMINGHAM - MUMBAI

Microsoft Data Protection Manager 2010

First published: May 2011

Production Reference: 1180511

Published by Packt Publishing Ltd.
32 Lincoln Road
Olton
Birmingham, B27 6PA, UK.

ISBN 978-1-849682-02-2

www.packtpub.com

Cover Image by Dan Anderson (dan@CAndersonAssociates.com)

Credits

Author
Steve Buchanan

Reviewers
David Allen
Islam Gomaa
Robert Hedblom

Acquisition Editor
Kerry George

Development Editor
Alina Lewis

Technical Editor
Vanjeet D'souza

Project Coordinator
Vishal Bodwani

Proofreader
Lisa Brady

Indexer
Rekha Nair

Production Coordinator
Arvindkumar Gupta

Cover Work
Arvindkumar Gupta

About the Author

Steve Buchanan is an Information Technology professional with over 11 years of experience in systems administration of server and desktop environments. For many years Steve has worked with backup solutions and disaster recovery.

Steve has an Associate of Arts degree as a Network Support Specialist and a Bachelor of Science degree in Information Technology. He holds the following certifications: A +, Linux +, MCSA, MCTS: (Hyper-V, SharePoint 2007, Exchange 2007, Vista).

Steve currently is an IT Manager. He enjoys sharing his adventures and ideas about system administration through his blog at `http://www.buchatech.com`. Steve is married and is a proud father of three boys.

Acknowledgement

First and foremost I want to give thanks to God for blessing me with the opportunity to write this book and work with a great group of people. Without God none of this would be possible. I want to thank my wife Ayasha and three sons Malcolm, Jalen and Sean. My Dad, Mom, my brothers David, and Anthony, my cousin John, and everyone else in my family. I also want to thank everyone that has supported the idea of me writing a book: Pastor Tim Jackson, Zach Osiowhemu, Cesar Duran, Ngozika Okoye, Mike Foye, and Luke Grindahl.

I also want to give a big thanks to the Microsoft System Center and DPM MVPs that were involved with this project. Thanks to Islam Gomaa for connecting me with the right people during this project and writing that piece on Opalis and DPM on such short notice. Thanks to Robert Hedblom for all your helpful insight in your reviews and positive feedback. Thanks to David Allen for your helpful feedback and contributing that piece on using Operations Manager with DPM. You guys were all a huge help and this project would not have gone as smoothly as it did without you.

I want to thank the team at Packt for working with me throughout the production of this book. Thanks to Kerry George and Alina Lewis for being patient with me and all my questions as a first time author. Thanks to Vishal Bodwani for helping me stay on track and be on time. Thanks to the rest of the team over at Packt.

Being around Microsoft MVPs and authors is inspirational and I want to thank Bill English, Todd Bleeker, and Brian Alderman for inspiring me to write. Working for Mindsharp has been a great experience. I also want to thank Ben Curry for inspiring me to write as well and for being a mentor.

Thank you to Gary Broadwater and Ken Galvin of Quest Software, Brendan Carr of Iron Mountain, Geralyn Miller and David Langdon of i365 and the rest of the vendors that gave me demos and answered all my questions about their products. Also a big thanks to Yegor Startsev and the entire DPM community!

About the Reviewers

David Allen has worked in the IT industry for over ten years, starting as a first line support analyst and working up to his current role as a Principal Consultant for Infront Consulting Group. David actively consults to large organizations helping them architect, implement, configure and customize System Center technologies integrating them into their business processes. David has spoken on System Center topics at industry events such as MMS and TechEd. David enjoys developing training material on the applications that he consults on and regularly delivers this training around the world for large enterprise customers. David is currently an Operations Manager MVP and has been for the last 3 years, and actively posts at `http://www.scdpmonline.org`. David is also a co-author of the System Center Opalis 6.3 book which is due for release in mid-2011.

Islam Gomaa is a Data Protection Manager MVP from Ottawa, Canada, specializing in System Center Products, disaster recovery and system infrastructures running on the Microsoft server technology stack. Islam brings over 12 years of expertise in helping organizations align their business goals using Microsoft technology and deploying Microsoft-based solutions for the private and public sector. He is also a member of the Windows Springboard Technical Expert Panel [STEP] for Windows 7 and Server 2008 R2 having delivered STEP presentations as an evangelist in Ottawa, Edmonton and Calgary. Islam authored some webcasts on Data Protection Manager 2007 and 2010 including 300 level "Protecting Applications with DPM2007" and 400 level "DPM and Opalis Automation for Disaster Recovery". Islam presented at TechDays 2010 in Winnipeg Canada and he is always invited to present for both OWSUG in Ottawa and MITPRO in Montreal.

Islam has a B.Sc. in computer science from Montreal University, and holds several Microsoft technical designations, and he is an active member of the IT community.

Islam is currently an IT Manager. He enjoys sharing his adventures and ideas about system administration through his blog at `http://owsug.ca/blogs/islamGomaa` and `http://www.IslamGomaa.com`. Islam is married and a proud father of his boy Yassine.

Robert Hedblom is a MVP for DPM and Senior Security Consultant who works at the Office IT-Partner Borås in Sweden. During his years as a focused DPM specialist and senior security consultant he gathered in-depth knowledge about DPM and the function of the technology. Robert Hedblom has written the official DPM 2010 training program for Cornerstone in Sweden and also tech DPM at Cornerstone. Robert is often seen as a speaker at Microsoft events and other technically focused conferences. Robert also runs the DPM blog *Robert and DPM* (`http://robertanddpm.blogspot.com`).

I would like to say thank you for the opportunity to work with Steve Buchanan who did a great job with this book.

---

www.PacktPub.com

Support files, eBooks, discount offers and more

You might want to visit `www.PacktPub.com` for support files and downloads related to your book.

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at `www.PacktPub.com` and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at `service@packtpub.com` for more details.

At `www.PacktPub.com`, you can also read a collection of free technical articles, sign up for a range of free newsletters and receive exclusive discounts and offers on Packt books and eBooks.

http://PacktLib.PacktPub.com

Do you need instant solutions to your IT questions? PacktLib is Packt's online digital book library. Here, you can access, read and search across Packt's entire library of books.

Why subscribe?

- Fully searchable across every book published by Packt
- Copy and paste, print and bookmark content
- On demand and accessible via web browser

Free access for Packt account holders

If you have an account with Packt at `www.PacktPub.com`, you can use this to access PacktLib today and view nine entirely free books. Simply use your login credentials for immediate access.

Instant updates on new Packt books

Get notified! Find out when new books are published by following `@PacktEnterprise` on Twitter, or the *Packt Enterprise* Facebook page.

This book is dedicated to the memory of my grandfather James A. Buchanan.

Table of Contents

Preface

Microsoft Data Protection Manager (DPM) 2010 is a backup and recovery solution which provides continuous data protection for Windows application and file servers to seamlessly integrated disk, tape, and cloud.

This Data Protection Manager book is a practical, step-by-step tutorial that will show you how to effectively back up your business data using Microsoft Data Protection Manager 2010 and how to plan, deploy, install, configure, and troubleshoot Microsoft Data Protection Manager 2010 as a standalone product. This book will focus on Microsoft best practices as well as the author's own real world experience with Data Protection Manager.

What this book covers

Chapter 1, *DPM Overview* provides an overview of what DPM is, along with what it can do. It discusses the history of DPM, new features to 2010, understanding licensing, and more.

Chapter 2, *Planning For Your Backup Needs* shows you how to develop a backup solution strategy.

Chapter 3, *Installation* looks into installing DPM as well as upgrading DPM.

Chapter 4, *Configuration* covers the required and optional configurations needed to get DPM up and running.

Chapter 5, *Administration* looks into DPM administration including the console, reporting, maintenance, and performance.

Chapter 6, *Configuring DPM to Back Up Servers and Clients* will cover topics such as protecting Windows' servers, Windows' clients, protecting clients and servers in untrusted domains or in workgroups, and configuring end-user recovery.

Chapter 7, *Backing Up Critical Applications* looks into backing up critical Microsoft applications such as SharePoint, SQL, Hyper-V, Exchange, and ISA Server 2006.

Chapter 8, *Recovery Options* deals with restoring critical Microsoft applications such as SharePoint, SQL, Hyper-V, Exchange, and ISA Server 2006.

Chapter 9, *Offsite, Cloud Backup and Recovery* covers the options that are available for Data Protection Manager offsite as well as cloud backup, recovery options and also how to configure them.

Chapter 10, *DPM PowerShell* discusses the basics of using PowerShell with DPM along with some useful scripts.

Chapter 11, *Troubleshooting and Resources* covers the basics of DPM troubleshooting as well as the many resources out there for DPM.

What you need for this book

To run the examples mentioned in this book you will need the following software:

- Base build:
  - Windows Server 2008 R2
  - PowerShell
  - Microsoft DPM 2010
- Other software used in the book:
  - Firestreamer
  - Exchange 2007/2010
  - SQL 2005/2008
  - ISA 2006
  - SharePoint 2010
  - Hyper-V
  - CloudRecovery by Iron Mountain
  - EVault for DPM by i365

Who this book is for

If you are a Network Administrator, System Administrator, Backup Administrator, Storage Administrator, or an IT consultant who wants to effectively back up your business data using Microsoft Data Protection Manager 2010, then this book is for you.

A good understanding of operating systems, backup devices and network administration is required. However, knowledge of Data Protection Manager is not necessarily required.

Conventions

In this book, you will find a number of styles of text that distinguish between different kinds of information. Here are some examples of these styles, and an explanation of their meaning.

Code words in text are shown as follows: " Disable the antivirus software real-time monitoring of `csc.exe` and `dpmra.exe`."

Any command-line input or output is written as follows:

```
Get-Command -PSSnapinMicrosoft.DataProtectionManager.PowerShell
```

New terms and **important words** are shown in bold. Words that you see on the screen, in menus or dialog boxes for example, appear in the text like this: "The **Libraries** tab is similar to the **Disk** tab."

Warnings or important notes appear in a box like this.

Tips and tricks appear like this.

Reader feedback

Feedback from our readers is always welcome. Let us know what you think about this book—what you liked or may have disliked. Readers' feedback is important for us to develop titles that you really get the most out of.

To send us general feedback, simply send an e-mail to `feedback@packtpub.com`, and mention the book title via the subject of your message.

If there is a book that you need and would like to see us publish, please send us a note in the **SUGGEST A TITLE** form on `www.packtpub.com` or e-mail `suggest@packtpub.com`.

If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, see our author guide on `www.packtpub.com/authors`.

Customer support

Now that you are the proud owner of a Packt book, we have a number of things to help you to get the most from your purchase.

Errata

Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you find a mistake in one of our books—maybe a mistake in the text or the code—we would be grateful if you would report this to us. By doing so, you can save other readers from frustration and help us improve subsequent versions of this book. If you find any errata, please report them by visiting `http://www.packtpub.com/support`, selecting your book, clicking on the **errata submission form** link, and entering the details of your errata. Once your errata are verified, your submission will be accepted and the errata will be uploaded on our website, or added to any list of existing errata, under the Errata section of that title. Any existing errata can be viewed by selecting your title from `http://www.packtpub.com/support`.

Piracy

Piracy of copyright material on the Internet is an ongoing problem across all media. At Packt, we take the protection of our copyright and licenses very seriously. If you come across any illegal copies of our works, in any form, on the Internet, please provide us with the location address or website name immediately so that we can pursue a remedy.

Please contact us at `copyright@packtpub.com` with a link to the suspected pirated material.

We appreciate your help in protecting our authors, and our ability to bring you valuable content.

Questions

You can contact us at `questions@packtpub.com` if you are having a problem with any aspect of the book, and we will do our best to address it.

1
DPM Overview

Welcome to the first chapter of our journey into the world of data protection through Microsoft Data Protection Manager (DPM). This chapter will provide you with an overview of DPM. After reading this chapter you will understand what DPM is and the basis of what it can and cannot do. We will go through DPM Architecture, pricing of DPM, DPM downfalls, compare DPM to other back up solutions, DPM features as well as features specific to the new 2010 version.

In this chapter, we will cover the following topics:

- What is DPM?
- DPM Architecture
- Cons of DPM
- DPM pricing
- DPM feature set
- New features of DPM 2010
- What makes DPM different from other back up solutions

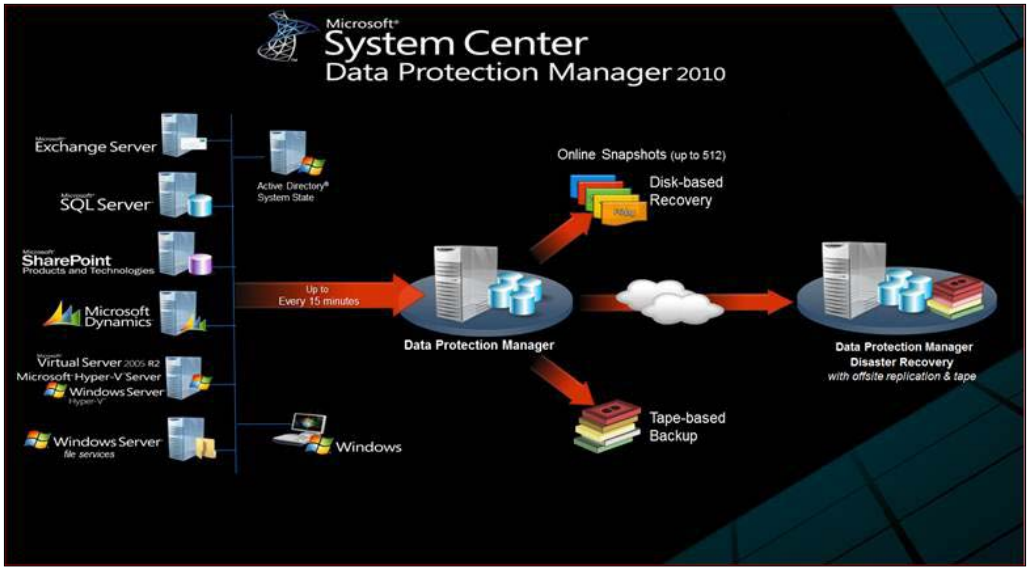
What is DPM?

Data Protection Manager (**DPM**) is a part of the Microsoft System Center product suite. The Microsoft System Center products are recognized as tools that IT professionals use to manage their Microsoft domain environments. DPM fits right into this category of products. DPM is Microsoft's first strategy in the back up and recovery space. DPM is on its third version starting with DPM 2006 released in 2005, then DPM 2007 and now DPM 2010. Data Protection Manager is designed to provide IT professionals with a better, more stable way to manage data back up and recovery and minimize data loss.

DPM is a centralized back up solution for Microsoft domain environments. DPM does not back up non-Microsoft operating systems natively. Backing up non-Microsoft systems can be done through third party solutions that we will cover later in *Chapter 9* (this includes server and client operating systems). DPM utilizes **Microsoft Shadow Copy** technology to perform continuous back ups. It performs these continuous back ups at the block-level to ensure data integrity. DPM creates continuous snapshots of data from protected clients. DPM performs a synchronization of only changed data from protected clients keeping the space requirements low on the drives you are backing up to. For example, if you have 200 GB of data that you are protecting on the protected server, DPM will only synchronize the changed data and this might be a couple hundred MB of data. Sending a couple hundred MB of data over a network versus 200 GB of data helps keep bandwidth usage low allowing DPM to perform back ups more frequently.

DPM can perform these synchronizations as often as every 15 minutes, depending on workload being protected, providing constant protection.

The following is a diagram of what DPM can protect and how it can provide protection in your environment:



The DPM Architecture has many parts to it but is easy to understand. We will go through the various pieces. DPM's index and configuration information is stored in a SQL database. This DPM database can be either local or remote on a new or existing instance of SQL. A SQL 2008 instance is required for the DPM database. DPM 2010 runs on Windows Server 2008 or Windows Server 2008 R2 64 bit architecture. It is recommended by Microsoft that DPM needs to be installed on a server dedicated for DPM only. DPM has several combinations in which it can back up your data which help determine the topologies in which DPM can be set up. A number of things need to be considered such as how long you need to retain data, how quickly you need to recover data and how much data you have to back up.

DPM is capable of Disk-to-disk (D2D), Disk-to-tape (D2T), Disk-to-disk-to-tape (D2D2T), and Disk-to-disk-to-cloud (D2D2C) protection. Back up to disk offers fast restores while back up to disk then to tape offers a way to archive date for long retention. You can also back up straight to tape skipping back up to disk all together and back up to the cloud. Backing up to the cloud offers a way to get critical data offsite without the need to send tapes offsite. DPM was designed to back up data on any disk that is presented to the operating system on the DPM server including internal hard drives, Direct Attached Storage (DAS), tape solutions, Storage Area Network (SAN), iSCSI NAS, and to the cloud.

NOTE: DPM natively cannot back up to external USB hard drives but there is a work around for this which we will cover in *Chapter 7*.

For every operation that DPM performs, there is a PowerShell code that runs underneath. This is good news because that means that anything DPM does from the GUI can be scripted to help automate certain tasks. In fact, some tasks can only be performed in PowerShell. This will be covered in detail in *Chapter 10* It is recommended that you have PowerShell knowledge or start learning it as soon as you can. Microsoft is now creating a good amount of its new applications in PowerShell, some of these being products in the System Center suite.

Cons of DPM

As with every product, DPM does have some disadvantages. Along with all the pros of DPM we need to understand what the cons are as this will help you determine if DPM will fit your needs or not. The last thing you want is to invest in DPM only to find out it won't do what you need it to do.

The cons of DPM are as follows:

- One obvious con is that DPM can only back up Windows based servers and clients natively. DPM can back up Linux if it is running on a Hyper-V virtual machine. You can also get a third-party appliance to back up non-Microsoft workloads such as Linux. This is still a problem if you need to back up MAC, Linux, or anything non-Microsoft in your environment without purchasing another tool to do so. The other problem with running Linux on Hyper-V is that Hyper-V can only run certain Linux distributions. The list of supported Linux distributions can be found here: `http://blogs.technet.com/b/seanearp/archive/2008/06/29/linux-on-hyper-v.aspx`.
- By default DPM uses the local `C:\` drive of a protected server when backing up system state on that protected server. This could cause the drive to fill up on that protected server and we all know that is not a good thing. There is a way to change the drive used to store the system state back up by altering the `PSDataSourceConfig.xml` file on the protected computer.
- DPM cannot back up the server that it is on right out of the box without some further configuration or unless you are backing it up to tape. You can enable DPM to protect itself by running the following command in PowerShell (we will cover more of this in *Chapter 10*):

  ```
  Set-DPMGlobalProperty –AllowLocalDataProtection $true –
  DPMServerName
  ```

  We cover PowerShell in *Chapter 10*. The best option for backing up a DPM server is with another DPM server. We will cover how to back up a primary DPM server with another secondary DPM server in *Chapter 9*.

DPM is an intuitive back up tool built with System Administrators, Messaging Administrators, Database Administrators, SharePoint Administrators, Virtualization Administrators, and developers in mind. Microsoft's goal was to provide anyone in these roles with the power to back up without the complex configurations or the need for extensive training in back up and storage.

DPM is not the be all and end all back up solution if you have non-Microsoft servers and clients in your environment, nor is it perfect. It is however, a top industry leading data protection solution compared to other data protection solutions out there on the market. DPM is a back up/restore/disaster recovery solution that you can depend on for backing up and recovering your data. DPM integrates well with the products it protects such as Exchange, SharePoint, SQL Server, and other Microsoft applications. Last but not least, DPM provides great value for the price as you will see next.

DPM pricing

DPM 2010 pricing can be confusing on the Microsoft site. In the following chart the DPM licensing and pricing has been broken down in a way that is easier to understand. DPM 2010 pricing is as follows:

DPM type	Cost	Description
DPM 2010 Enterprise	$432	This allows you to back up file servers as well as application-specific servers. Some application-specific servers include: SharePoint, SQL 2008, Exchange, and Hyper-V. This license gives you the power to do bare metal restore and is required if you are backing up 2003 and 2003 R2 servers using SRT (System Recovery Tool was a tool used for BMR with DPM 2007. In DPM 2010. SRT is only used for BMR when protecting 2003 servers. DPM 2010 has BMR natively built in for Windows 2008 servers.)
DPM 2010 Standard	$158	This license gives you file level protection as well as system protection such as system state and BMR. With this license you cannot back up application-specific servers such as Exchange or SharePoint.
DPM 2010 Client license	$32	This license is for backing up client computers on your network. This is good for Windows XP, Windows Vista, and Windows 7 only. This does include system state and backing up remote staff computers.

No license is required for the DPM Server in DPM 2010. You can have as many DPM servers as you like as long as the servers being protected are appropriately licensed as per the previous table.

All of the above licenses are considered to be Management Licenses (MLs). MLs are legal rights and have no digital footprint. This means MLs are not installed on the managed device (OSE) or placed in the registry. It is up to the customer to make sure they are in compliance with licensing. DPM 2010 requires ML licenses for each managed device (OSE). OSE stands for Operating System Environment. An OSE covers all OSs running in any environment (physical or virtual). A managed device would be more fitting. A managed device is any server or client that is protected by DPM. However an ML is not required for any managed device that is functioning solely as a network infrastructure device. An example of this would be an ISA server. The ISA server performs network functions such as being a firewall or a load balancing device.

All prices mentioned were applicable at the time of writing this book. For the most current pricing visit: `http://www.microsoft.com/systemcenter/en/us/data-protection-manager/dpm-pricing-licensing.aspx`

DPM feature set

DPM has a robust set of features and capabilities. The following are some of the most valuable ones:

- Disk-based data protection and recovery
- Continuous back up
- Tape-based archiving and back up
- Built in monitoring
- Cloud-based back up and recovery
- Built-in reports and notifications
- Integration with Microsoft System Center Operations Manager
- Windows PowerShell integration for scripting
- Remote administration
- Tight integration with other Microsoft products
- Protection of clustered servers
- Protection of application-specific servers
- Backing up the system state
- Backing up client computers

New features of DPM 2010

Microsoft has done a great job of updating Data Protection Manager 2010 with great new features and some much needed features. There were some issues with Data Protection Manager 2007 that would cause an Administrator to perform routine maintenance on it. Most of these issues have been resolved with Data Protection Manager 2010. The following are the most exciting new features to DPM:

- DPM 2007 to DPM 2010 in-place upgrade
- Auto-Rerun and Auto-CC (Consistency Check) automatically fixes Replica Inconsistent errors
- Auto-Grow will automatically grow volumes as needed
- It allows you to shrink volumes as needed
- Bare metal restore

- A Back up SLA report that can be configured and e-mailed to you daily
- Self-restore service for SQL Database Administrators of SQL back ups
- When backing up SharePoint 2010, no recovery farm is required for item level recoveries for example: recover SharePoint list items, and recovery of items in SharePoint farm using host-headers. This is an improvement to SharePoint that DPM takes advantage of
- Better back up for mobile or disconnected employees (This requires VPN or Direct Access)
- End users of protected clients are able to recover their data. The end users can do this without an Administrator doing anything.
- DPM is Live Migration aware. We already know DPM can protect VMs on Hyper-V. Now DPM will automatically continue protection of a VM even after it has been migrated to a different Hyper-V server. The Hyper-V server has to be a Windows Server 2008 R2 clustered server.
- DPM2DPM4DR (DPM to DPM for Disaster Recovery) allows you to back up your DPM to a second DPM. This feature was available in 2007 and it can now be set up via the GUI. You can also perform chained DPM back up so you could have DPM A, DPM B, and DPM C. Before you could only have a secondary DPM server backing up a primary DPM server.
- With the 2010 release, a single DPM server's scalability has been increased over its previous 2007 release:
    - DPM can handle 80 TB per server
    - DPM can back up up to 100 servers
    - DPM can back up up to 1000 clients
    - DPM can back up up to 2000 SQL databases

As you can see from the previous list there are many enhancements to DPM 2010 that will benefit Administrators as well as end users.

What makes DPM different from other back up solutions

As you will probably know there are many products out there in the data protection market. Here are a few, broken down by paid and free:

Paid	Free
ARCserve Backup	AMANDA
Backup Exec	Bacula
Acronis	rsync
CommVault	BackupPC
Handy Backup	DirSync Pro
Mozy	Cobian Backup

Most of the free products are for Linux platforms and offer limited and/or community support because they are open source. A few of them such as DirSync Pro, AMANDA, and BackupPC will back up MAC OS as well. All of the free products on the list will back up Windows based servers. None of the free products are nearly as good as DPM when comparing features and you will not get the same level of support that you will receive from Microsoft.

One of the most well-known and used product is Symantec's Backup Exec. Some of the differences between DPM and Backup Exec are that DPM is a lot more intuitive and easy to set up and DPM is integrated much better when backing up Microsoft applications servers. The following is a list comparing DPM to other back up solutions on the market. We will only cover three of the paid back up products:

	DPM 2010	**Back up Exec 2010**	**Acronis® Back up & Recovery™ 10 Advanced Server**	**CommVault Simpana**
Cost	$432 for the enterprise license. This price does gives you all the functionality of DPM. This allows you to back up applications such as Exchange, SQL, or SharePoint.	$1,162.66, and does not include agents' licenses. This also does not allow you to back up any applications such as Exchange, SQL, or SharePoint. If you needed to back up an application like SharePoint you would need to pay an extra $1,162.66 for this license.	$1,219.00 for one server license. You would need to buy separate licenses to back up workstations. This does not allow you to back up any applications such as Exchange, SQL, or SharePoint.	$1,503 for a single server for Windows, not including agents' licenses. This also does not allow you to back up any applications such as Exchange, SQL, or SharePoint.
Bare metal restore	Yes	Yes	Yes	No
Linux	No	Yes	Yes	Yes
Remote management	No	Yes	Yes	Yes
Deduplication	No	Yes	Yes	Yes
Continuous back up protection	Yes	Yes	No	Yes
Back up targets	Local disc, DAS, iSCSI NAS, SAN, TAPE, Cloud	Local disc, DAS, SAN, TAPE	Disc, NAS, SAN, Tape, FTP	Local disc, DAS, SAN, TAPE
Server cluster support	Yes	No	No	Yes
VSS integration	Yes	No	Yes	Yes

	DPM 2010	Back up Exec 2010	Acronis® Back up & Recovery™ 10 Advanced Server	CommVault Simpana
Bandwidth throttling	Yes	No	No	Yes
Scripting	Yes	No	Yes	No
Virtualized back up	Yes	Yes	Yes	Yes
Reporting	Yes	Yes	No	No

As you can see from the preceding table, there are many features that are common across all of these back up products and there are some major differences as well. **Acronis** is easy to implement in firewall protected environments. Acronis also lets you take complete images of your servers as none of the other above products do. One of the major differences is cost and this is where DPM takes the prize. All of the mentioned solutions require you to purchase extra licensing to back up workstations. Most of the solutions require you to buy additional licensing to back up specific applications such as SQL, SharePoint, and Exchange. However DPM includes this in its enterprise license and it still costs less than the other back up products.

Something you will notice when you shop for a back up product is that most of the pricing options on the products' websites are complex. This can make it difficult when trying to figure out the pricing of what you need for your environment. Choosing a DPM solution for your workload is relatively simpler. For example, you only pay one price and you are able to back up applications in your network.

The majority of the back up products mentioned earlier have a good amount of training resources and information around to help you get up to speed with them. The only one I found difficult to find training and documentation on was CommVault.

One of the drawbacks of DPM is that it is limited to only backing up Microsoft servers natively. You can protect non-Microsoft computers if it runs as a virtual machine in Hyper-V or with a third party product. All of the other products can back up Linux servers natively without third party add-ons. Many environments contain VMware and not being able to back this up with DPM is a problem. Microsoft has included the capability to manage and monitor non-Microsoft products such as VMware with System Center Operations Manager and System Center Virtual Machine Manager. You would think Microsoft would have included the ability to protect VMware and Linux with DPM. This would be a nice feature to have within DPM. Maybe Microsoft will add protection to non-Microsoft servers that are common today in many environments in the next release of DPM: that way you won't need to purchase a third party product for it.

Summary

From this chapter, you should now have a good understanding of what Data Protection Manager is, its architecture, features, licensing, new features for 2010, its pros, cons, and what makes it different from other data protection products.

In the next chapter we will touch on preparing for your back up strategy and DPM 2010 deployment.

2
Planning For Your Backup Needs

In this chapter we will explore backup and Disaster Recovery (DR) as well as planning for a DPM deployment. You should have an understanding of backup and DR before you can really get into planning your DPM deployment. In the first half of this chapter we will go into detail about what to back up in your environment. Some IT professionals don't really have a good understanding of this and this chapter will point out some best practices regarding this. We will also briefly cover disaster recovery, what it means and how to plan for it.

In the second half of this chapter, we will plan our DPM deployment by digging into how to plan for protection groups and the recovery goals. This is what you need to get ready when making decisions about how many DPM servers your environment will need, where they should be located and whether to use hard drives or tapes, and so on.

We will cover the following topics:

- Why back up?
- Assessing your backup needs
- Disaster Recovery
- Planning DPM deployment

Why back up?

Backups and Disaster Recovery (DR) are critical to a business's survival. Yet backups and DR are often undervalued or simply done wrong, time and time again. Often, senior management do not understand the severity of having a solid backup/DR system and plan in place in the event of hardware failure or catastrophe. Often, senior management will want to know why backup is needed or why it costs' so much. It is up to you as an IT professional to help them understand why. We will explore the different aspects of backup DR planning and what goes into it. You will then be armed and ready to fight for a backup and DR system in your environment.

Getting your backup and DR recovery set up the right way is not rocket science it just takes some forethought and planning. When designing your backup strategy, go into it with the mindset of experiencing the worst possible scenarios. Imagine your business was located in New Orleans when hurricane Katrina hit, or you arrive at work to find out the domain controller has completely failed, or this could be Exchange or the phone server or the accounting server. What would you do? Imagine losing all e-mails, user accounts, financial data, and phone records. This would make for the start of a very bad day.

When dealing with computers always remember that if it can fail someday, it will. That is something you can count on. You can do everything right in regards to maintenance of hardware but remember that hardware will fail. The time when your server hardware does fail is the time that counts. This is the time you will be tested and tried, and for your sake you better have a solid backup and DR plan. First and foremost, it is important to be able to get the data back and that it is good data, second you should be able to do this in a short amount of time so that the business can continue to operate. Now we will go into assessing your backup needs and forming the strategy.

Assessing your backup needs

In this section you will discover what it takes to build a backup plan from the ground up. We will cover this process step-by-step through several topics.

What to back up?

As an IT professional tasked with designing the backup plan you will ask yourself, what should I be backing up? This is a great question and here are some things to get you going. First off, think of what data your company would need to run. This should include things like e-mail, accounting data, HR data, customer information such as CRM data, any type of database data or things specific to what your company does. You really need to know your business and think about what would happen if one of the above scenarios happened or one of these other common causes such as accidental file deletion, application errors and corruption, application patches or upgrades, and of course hardware failure. What data would be needed to keep the business running? This is called business continuity. There is more to business continuity than just data such as the rest of the infrastructure systems but we will cover this briefly later on in the disaster recovery section.

Applications/Data	Why?
E-mail (Exchange itself and user mailboxes)	You need your company's mail and end user e-mail accounts. Don't just back up the mail be sure to back up the mail server settings as well.
Domain Controller (AD and AD user accounts)	This is very important. This server is the meat of your infrastructure. This has all of your domain information, your active directory, user accounts, group policies, DNS, and DHCP. Make sure you have a good backup of this server or you will be in trouble. An example would be having a good Exchange backup but not the Domain Controller. You would not be able to run Exchange without this.
CRM (Customer Data)	This is a no brainer you will need your customer data. Many companies keep this in some sort of CRM system.
Websites (IIS sites and SharePoint)	If you host any internal websites then you will need this. IIS is Microsoft's web server that you use to host your own websites on. SharePoint is a website but it consists of a front end (IIS) and a SQL database. Be sure to back this up. We will cover this in more detail later on.
File Servers (Users data such as mapped drives and so on)	This is another no brainer. If you have user data on mapped drives or shares you will want to back this data up.

Applications/Data	Why?
QuickBooks (Financial Data)	You will need to back this up for sure. You may even be required to archive some of this data such as tax information.
Databases (SQL)	Many applications run databases on the backend. Some of these include SharePoint, CRM, and Office Communication Server. Even DPM has its own database that lives on SQL. These are important, be sure to back them up.
Servers (Operating Systems, System State)	In case you don't know what System State is; this is critical system related components on a computer. You will want to back this up. System State contains the Registry, COM+ Database, Certificate Services, Active Directory, SysVol, and IIS Metabase. Not all servers contain the Active Directory, Certificate Services, or IIS Metabase. What is in system state depends on the server role. You can find more details about system state online.

The other reason to back up may not be for restoration purposes but for retention and archiving. Some industries have compliance needs and will require certain types of data to be retained for a period of time. You may backup data to tape and archive it indefinitely. Such types of data may include HR data, financial records, e-mail, and legal documentation. You can archive to different types of media but often tape is the media of choice for this. Next we will explore the different media types you can chose for your backup and the pros and cons of each.

Which media to use?

Depending on what your environment needs are you will need to choose the right type of backup media to use. Several factors will determine this and also what will work best for you. You will need to match the capacity of the backup media to the amount of storage your data will need. This is important because backups can take up a lot of space. Some of the most common backup media types are covered in the following table. Remember you can combine multiple media types with DPM to get the right solution.

Type	Pro/Con
Disk (SATA, eSATA, USB hard drives)	**Pro**: Low costs for large amounts of storage space. **Con**: Not very mobile for offsite. Disks are often internal to the backup server. If you have an external drive, DPM does not work well with these. DPM does not support the use of USB drives, however using third-party software it is possible to simulate a tape library to DPM which utilizes USB disks. This will be covered later in this book.
Tape (Usually a single tape unit or robotic tape library and tapes that you rotate.)	**Pro**: Good for offsite and archiving. **Cons**: Cost can be high on the units and purchase of tape inventory. Storage limits on tapes. Some administrators will require training on tape systems. There are many tape formats (LTO, DLT, DAT/ DDS, SAIT/AIT, and Travan) the one you choose to use today may not be around tomorrow.
DAS (Direct Attached Storage)	**Pro**: Relatively low cost. Fast back ups with eSATA. **Con**: Not mobile for offsite backup.
SAN (Storage Area Network) and iSCSI NAS	**Pro**: Very fast. These systems use fiber optics. Recommended for enterprise environments with large amounts of data to back up. **Con**: High cost of equipment. You will need to train most administrators on these type of systems. This is not mobile for offsite backup as well.
Cloud (An offsite vendor's data center)	**Pro**: Great alternative to tapes or moving drives offsite. Unlimited backup capacities available. **Con**: Monthly cost required. The more data you have the more you will pay. Cloud storage has high bandwidth usage possibly causing speeds on your network to diminish. Dependant on having internet connectivity.

Overall you need to be aware of how much your organization is willing to spend on media for the backup system. When you choose the media you will use for your backup solution the following should be considered:

- The cost of the media as well as training
- On-going administration
- Maintenance

Capacity planning

Something you need to be concerned with is the amount of storage space your backups will use. Once you know the capacity you need you will be able to better plan your DPM configuration. You also need to know if you need to archive this data as well. If you have large amounts of data and you only have a need for short-term backups then disks are the way to go but if you need to archive, tapes would be more ideal than disks.

Backup and restore time

Now when it comes to backups you need to think about the amount of time it takes to back up and how quickly you can restore data. If someone loses data they will want it restored in a timely fashion. If you have your backups on disk this should be relatively fast to restore data. Now if you have the data on tapes it could take a long time to restore because tapes typically require multiple steps before you can even restore. They need to be mounted, then they need to catalog, then they take time to actually read from the tape to restore. Something else to consider here is when your backups will run. When your backups will run is really determined by the amount of data you back up and the type of backup you perform. Traditionally with backups there are three types of backups you can perform, these are:

- **Full**: This is a complete backup of all the data
- **Incremental**: This backup type contains only files that have changed since the most recent backup being full or incremental
- **Differential**: This backup type is cumulative of all changes made since the last full backup

Full is the slowest backup type because it is getting all data within the backup. Differential will be quicker than Full because it only gets the files that have changed since the last full backup. Incremental takes longer to restore because you need the latest full backup and all incremental backups after the last full. When backing up, Incremental would also be fast as only data that has changed is backed up.

Backup times and speeds are improved with DPM because with DPM backups you perform an Express Full back up the first time and afterwards you only move the block-level changes.

You want your backups to run during the quietest times with regards to network usage and this is typically not during business hours if possible. But if your data takes a really long time to back up it may overlap and end up running during business hours. If your backup has to run during business hours this could impact network performance. One way around this is to utilize a second network that only your backups run on. This is typically seen in larger environments that contain larger amounts of data. The end result should be fast backups and fast restores. When backups are fast and efficient, there is generally less of an impact on the server being protected which keeps both administrators and users of that server happy.

Backup schedule

One of the ways to determine your backup schedule is to calculate the frequency with which your important data changes. DPM can back up as often as every 15 minutes although you may not want to back up all your data this often. Some data may only change once per day or once every couple of days and you could then back that data up as often as it changes. Typical data types that change frequently throughout a business day are file shares, Exchange (e-mail), financial data, and databases. Be sure to schedule your backups when network usage is at its lowest. As covered previously, you could negatively impact network performance if these backups are scheduled during working business hours. Your media will often be a factor in determining your backup schedule. If you use a disk-based backup and you have a lot of storage space you can run backups more often. DPM improves upon bandwidth usage by using the VSS function and takes snapshots of the data. The installed DPM agent wont process the actual data, instead it will process the snapshot data. Because of this it is more viable to make a back up of a production environment during production hours. Even with the bandwidth usage improvements in DPM you still want to be cautious of the network usage that your backup uses depending on your specific workloads.

Local and offsite backup

Now let's talk about local and offsite backups. There are two kinds of backups. One is a local backup that stays within your physical building and the other is an offsite backup that is away from your psychical building. Not all companies will have the resources for offsite backups but it is strongly recommended to have an offsite backup in case a disaster happens to your office destroying your onsite backups. Local backups can be on disk or tape and are stored locally. Offsite backups are disks that have been taken offsite, tapes that have been moved offsite, or moving data to offsite storage using a data transfer mechanism.

Local backups are nice in many ways, an example would be that a user deletes a file in the afternoon that was there that same morning and simply needs to restore the file. With a local backup you can do a fast restore. When a user needs a restore they don't want to hear that a tape or disk needs to be mailed to the office or you have to wait for the download to finish pulling down the backup data. This would take too long and the offsite backups will take some time to retrieve. But what happens if the office burns down taking the disk or tapes with it? You won't have the backup to restore from and will be out of luck. Having an offsite backup would protect you from such a scenario. You would simply have the offsite disk or tapes sent to you or pull down the data from your offsite backup provider. The best backup plans combine local and offsite backup. This gives you the option to restore fast but protects you if something happens to your physical office.

Integrity of backups and testing restore

It is extremely important to check your backups and perform test restores. You do not want to find out that your backups are no good when it is crunch time and someone is depending on you to restore some data. Things can happen such as your media goes bad. Tapes can deteriorate and hard drives die and you want to be prepared if this happens. It is recommended that you verify your backups by running verification after backing up. DPM only supports verification for tape backups and for protection Exchange. Microsoft may add this feature in the future. The best way to test a backup is by doing a restore of it. You can restore over production but this is not recommended. It is recommended that you restore to a different location or maybe a duplicate virtual copy of a production server. You do not want to restore to your production servers and find out the data is bad. It is a good idea to check the backup on an ongoing basis. Make performing test restores a regular habit. The more frequent your back ups are, the more often you want to check the backups. No matter what your backup frequency is, it is recommended that you run a verification and do a restore once a week.

Data privacy and security

In recent years, many new compliance and data retention laws have been introduced in the IT industry. These laws continue to become more complex every year. Your company may or may not be susceptible to all or some of these laws. It is your job to find out what laws pertain to your business. Many times HR and legal departments are a great resource for this. You should also be concerned with security, privacy, and retention of the data you are backing up. Here are a few of the data regulations out there:

Sarbanes-Oxley Act	The Sarbanes-Oxley Act of 2002 (often shortened to SOX) is legislation enacted in response to the high-profile Enron and WorldCom financial scandals to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise. The act is administered by the Securities and Exchange Commission (SEC), which sets deadlines for compliance and publishes rules on requirements. Sarbanes-Oxley is not a set of business practices and does not specify how a business should store records, rather, it defines which records are to be stored and for how long. (Source: `http://searchcio.techtarget.com/definition/Sarbanes-Oxley-Act`)
(HIPPA) Healthcare Insurance Portability and Accountability Act	HIPAA is the United States Health Insurance Portability and Accountability Act of 1996. There are two sections to the Act. HIPAA Title I deals with protecting health insurance coverage for people who lose or change jobs. HIPAA Title II includes an administrative simplification section which deals with the standardization of healthcare-related information systems. In the information technology industries, this section is what most people mean when they refer to HIPAA. HIPAA establishes mandatory regulations that require extensive changes to the way that health providers conduct business. (Source: `http://searchdatamanagement.techtarget.com/definition/HIPAA`)
(PCI) Payment Card Industry Data Security Standard	Payment Card Industry (PCI) compliance is adherence to a set of specific security standards that were developed to protect card information during and after a financial transaction. PCI compliance is required by all card brands. (Source: `http://searchcompliance.techtarget.com/definition/PCI-compliance`)

There is a lot more to data retention, security, privacy, and compliance than what we are able to cover in this book. Be sure to do further research and seek help before diving into this topic further.

Policies and processes

Okay, so now your backup plan is almost complete but you are missing a few things. You need some policies and procedures and lots of documentation. You also need to put some policies in place.

The documentation is a no brainer. There are two things you should document, one is your backup plan before you set up your backup system and second the backup configuration itself should be documented. The backup configuration should consist of things such as what databases are being backed up, what file shares, server system states, and more. It is important to have both of these things documented for yourself in the future and for new members of your IT team. If your backup system itself completely fails you can use this documentation to recreate the backup system. It will also help you know how things are configured and what is and what is not being backed up so you can plan for growth and troubleshooting if a problem arises.

You also need some policies and processes on how things should go. Some of these processes should describe who is responsible for back ups, how and when test restores should be performed. This also defines your data retention polices.

Disaster Recovery

We will not go into a lot of detail regarding Disaster Recovery (DR). We will just cover what Disaster Recovery is because backup is a part of DR. DR is processes and procedures of what you would do in the event of a failure or catastrophe. This includes but extends beyond backup. This covers things such as what you will do if hardware in your infrastructure were to fail, what you would do if certain services fail like DNS, firewalls, email service, database services and more. Backup is a part of it because this is what will contain the data and the configuration data but you will need documentation of settings, hardware replacement plans, clustering and procedures to restore services quickly. These are things you need to consider alongside your backup plan so you can mitigate in the event one occurs.

Planning DPM deployment

In this section we will explore the DPM deployment process. This is broken down in multiple sections to give you an in depth look into each one.

DPM backup and recovery goals

In this sub-section we will look at the different areas in your DPM deployment that need to be planned in order for DPM to fit your specific backup and recovery goals.

Protection Groups

When planning your DPM deployment, the first thing you need to decide on is your protection groups. This goes back to understanding your company's business requirements helping you to recognize why you are backing up and what you need to back up. Protection groups in DPM are a group of servers/data that you are protecting. These protection groups can have different protection and retention options set for each group. Here is an example, you can have your Exchange and SQL servers in one protection group and your print servers in another protection group. Your print servers do not need to be backed up every 15 minutes but your Exchange and SQL servers will definitely need to be backed up every 15 minutes. The application data on Exchange and SQL changes constantly so you need to back this up often. Your print server can be backed up once per day if you want because it does not change often but needs to be protected. You can set the backup frequency differently on each because they are in separate protection groups and hold their own policy settings. Some companies may put all their data and servers that need to be protected in the same protection group and some environments may call for many protection groups. How many protection groups you use is really determined by your particular needs but this is an important piece to have planned out up front.

Backup schedule and retention

Be realistic with your goals when determining your DPM backup system. This goes back to laying out your need for backup and restore times that are acceptable in your company. Also this is where planning your backup schedule comes into play. Do you need to backup data every 30 minutes? If so what data needs this level of backup frequency? What amount of time is acceptable for restores? DPM has a few options here. The options that can be set on a protection group are synchronization frequency, recovery point schedule, and retention range. It is important to know your backup goals, that way when you go to set up protection groups you will know what you will want for these settings. Here is what each of these settings mean:

- **Synchronization frequency**: This is how often DPM will synchronize its data with the data on the protected server. You can set this as often as every 15 minutes.
- **Recovery point schedule**: Is the date and time that protected data is available for recovery. These dates and times are available for you to restore from.
- **Retention range**: This sets the length of time DPM will retain your protected data for

Choosing media for DPM

With DPM you have short-term and long-term protection options. This is true regardless of whether you choose tape or disk. Tapes and disks have different schedule options. Short-term protection options for tapes can be scheduled in a range of 1-12 weeks. You can back up on tape daily, weekly, or bi-weekly. You set this through the retention range. For long-term range protection you can select from 1 week up to 99 years. These are called tape archives. Again this is set by the retention range. With disk-based protection you can choose to back up as often as 15 minutes all the way up to once every 24 hours. You can set the retention range for disk-based protection between 1 and 448 days. For long-term protection you can set the retention range from 1 to 99 years. You can also choose offsite cloud protection as a long-term solution. We will cover offsite cloud protection in *Chapter 9*.

Storage pools

A storage pool is a group of hard disks in the DPM server. These disks are where DPM stores the replicas and recovery points. DPM can use any of the following solutions for its storage pool:

- SAN's iSCSI or a Fiber Channel SAN
- (DAS) Direct Attached Storage
- iSCSI NAS
- Internal hard disks

In this book, I will use an eSATA DAS solution in my examples. You don't need a DAS or SAN though, you can simply purchase some extra disks, insert them into your server and back up to them; DPM supports IDE, SATA, and SCSI. When planning for your storage pool you need to consider capacity requirements which are covered next and the configuration of your disks such as, are you going to use a DAS or SAN? Internal disks or a DAS solution are less expensive compared to a SAN solution however you will get better performance with a SAN.

With a DAS solution you have the option of using a hardware RAID. Note that RAID cannot be a software based RAID it has to be hardware based. You could also use a JBOD (Just a Bunch Of Disks) DAS solution. A JBOD solution will appear as one large disk. A RAID solution can provide improved performance and redundancy. Microsoft recommends that you choose a RAID 5 if you go with a RAID solution; however this will not apply to every deployment. Depending on business requirements, JBOD or RAID 0, RAID 1, RAID 5, or RAID 10 may be more suitable.

Microsoft recommends that you do not use single disks that go over 1.5 TB. DPM can span up to 32 disks so Microsoft recommends using multiple disks for your storage pool configuration.

In DPM you can use a volume over a storage pool. You would need to assign a custom volume to your protection group member indicating that you want to use the volume instead of the storage pool. Almost any volume on a DPM server can be used as a custom volume for a protection group. You cannot use a volume with the operating system or program files on it as a custom volume for DPM. You would use a custom volume if you wanted more control over the storage DPM uses to back up onto.

One of the major differences between a custom volume and a storage pool is that DPM can manage a storage pool but DPM cannot manage a custom volume. You would have to manage a custom volume through windows disk management. Here is an example, if your volume for a protection group member started running out of space you would have to manually increase this. If you are using a storage pool and it is running out of space, DPM can automatically increase the space to the amount needed if it is available. On protection groups you cannot change from a storage pool to a custom volume or the other way around once it has been set. This is something you need to consider when planning to use or not use storage pools. It is recommended that you use storage pools unless there is a strong reason not to because you will have better management through DPM with a storage pool.

For offsite purposes, you can use tapes, DPM2DPM, or offsite cloud solutions. Tapes are a good option but can be costly as you may have to pay for storage and transportation of the tapes as well as the hardware and media. An offsite cloud is newer, so this is a good option with little upfront investment. It requires monthly fees and a robust bandwidth connection to sync data with the offsite vendor.

To use a tape library with DPM it has to be SAN, iSCSI, or SCSI attached. You need to consider the amount of tape backup jobs with the size of protected data. Also there are many types of tape options. You can have a library that loads the tapes automatically for you or a manual loader where a human has to swap tapes in a manual loader but this is prone to human error. To calculate the amount of tape storage required, multiply the backup frequency by the retention range. DPM has a default tape labeling scheme, if you want your own custom scheme you will need to plan this ahead of time. This is the default DPM tape label format: (`DPM - <ProtectionGroupName> - long-term tape <number>`). We will cover offsite backup in more detail in *Chapter 9*.

Capacity planning

DPM capacity requirements depend on the size of the protected data, retention range, recovery point size, and expected future data growth. The retention range is the number of days that recovery points are stored for your protected data. Microsoft recommends making your DPM storage pools two to three times the size of the protected data. This recommendation is based on a retention range of ten working days excluding weekends. A retention range of ten working days would give you a recovery range of two weeks in the event of data loss. The longer the retention range you choose, the lower the amount of possible recovery points you have.

With a retention range of eight days you would be able to have eight recovery points each day. If you chose a retention range of ten days you could have six recovery points per day.

NOTE: This only pertains to file backups as there is a VSS limit of 64 recovery points. For application protection, there are 512 recovery points available.

No matter what you chose for your initial storage size you want to use a solution that is easily scalable in the event you need to add more storage.

Other considerations

Remember to plan for integrity of backups and restore testing, data privacy, policies and processes when planning your DPM deployment. Use the previous information to assist in planning these as these topics are more general then specific to DPM.

DPM server configuration

In this sub-section we will look at the different DPM configuration options.

How many DPM servers?

You may be wondering how many DPM servers you need in your environment. There really is no secret to the amount of DPM servers you will need. The beauty of DPM is that a single DPM server will cover the needs of most small businesses. Of course if you are in an enterprise shop you may need more than one DPM server for your needs. When deciding how many DPM servers you will implement, you will need to consider the following things:

- Firstly, how much can a single DPM server handle? DPM can protect up to 80 TB of data, 100 servers, 1000 clients, and 2000 SQL databases.
- The next thing to look at is whether you will be backing up across a forest with multiple domains and with no trust relationship; you will then need a DPM server placed in each domain. DPM 2010 can also protect computers in untrusted domains using NTLM authentication and data can be further secured with the use of IPSec. Will you be backing up remote locations in one domain that is across a WAN? If so, you may want the DPM servers at your remote location.
- You also want to consider the performance of each DPM based on what you plan to back up. If you are backing up 150 data sources across 50 servers and 75 clients you will want 10 TB of space on a local disk. If you are protecting the same amount of data, servers, and clients with multiple DPM servers you would only need about 6 TB of space on a local disk across DPM servers. As you can see, the more DPM servers you deploy the lower the requirements of resources you will need on each DPM server.

DPM has a snapshot limit per server and this applies regardless of the storage pool size. A single DPM server can only store up to 9,000 disk-based snapshots. This includes snapshots that you chose to retain even after stopping the protection of a server, client, or data source. If you know that you will need to retain more than 9,000 snapshots then you will want to implement another DPM server. These are the things you should consider when planning how many DPM servers you will need.

Location of DPM servers

DPM must be deployed in a Windows 2003 or Windows 2008 Active Directory services domain. This is a requirement for DPM to function properly and there is no way around this. It is recommended that you deploy it in a Windows 2008 Active Directory services domain. DPM can back up in a forest. The forest must have a two-way trust relationship between domains setup in order for DPM to work across it. This must be in Windows 2008 server forest mode. DPM can back up across domains in a forest without a trust relationship if you utilize NTLM authentication between DPM and the protected server.

The last thing to consider when locating your DPM server(s), is bandwidth between itself and the clients that it will protect. The minimum network bandwidth DPM can operate on over a WAN is 512 Kbps.

You should not have to worry about bandwidth between the DPM and the protected clients in the same location, as DPM can operate on most LANs nowadays because they are fast enough to handle the traffic.

DPM SQL instance

DPM contains a SQL database as part of its architecture. This SQL database contains all of the DPM settings and the configuration information. DPM 2007 could use an instance on SQL server 2005 for its database. It is important to note that DPM 2010 requires an instance on SQL server 2008 SP1, Standard or Enterprise Edition. When you install DPM you have the option to use a SQL instance that DPM will install locally on the same server as DPM. This local instance runs on top of SQL Server 2008 Standard Edition. DPM uses a special version that was built specifically for it and is a full SQL server that does not require a license.

You will also get the option to place the DPM database on a remote SQL 2008 instance. This would be a SQL 2008 server that is separate from the DPM server. You would need a full SQL server license on the remote SQL server. DPM requires that your remote SQL instance should have the SQL Server Database Engine and Reporting Services components installed.

DPM security

DPM can be a serious security risk if it is compromised. Think about all the data running through your DPM server, e-mail, HR data, financial data, and customer data. If someone were to get their hands on any of this data that could mean big problems for you. DPM functions on a high-privileged level in the network. One of the easy ways to compromise a DPM server is to start installing unnecessary software and changing the default security settings. These are things you do not want to do. The best action is to keep the default DPM security architecture. During your installation of DPM you will want to accept all security defaults and if you run your DPM database on a remote SQL instance, do not run the instance as the local system and do not modify SQL Server 2008 settings, Internet Information Services (IIS) settings, DCOM settings, or settings of local users and groups that are created during the DPM installation. DPMs security architecture is built upon the security features of Windows Server 2008, Active Directory Domain Services, SQL Server 2008, and SQL Server Reporting Services. DPM will configure the settings it needs in those areas during the installation.

The other part of DPM security is to know about user privileges needed to install and operate DPM. In small IT environments that have a couple of administrators that wear many hats this won't matter as the administrators will typically all have the full access they need to install and operate DPM. Here are the different types of access you will need to install DPM and for performing certain tasks in DPM:

- To install DPM you need an administrator account on the DPM server
- To enable end-user recovery on the DPM server, you need an administrator account on the DPM server
- To access the DPM Administrator Console, you need to be an administrator on the DPM server
- To install DPM Recovery Point client software on a client computer, you need an administrator account on the client computer
- To recover SharePoint data, you need to be a SharePoint farm administrator and this same account needs to be an administrator account on the front-end server that the DPM protection agent is on
- To access previous versions of protected data from a client, you need a user account with access to the protected share

Before you install DPM you need to add its server to your Active Directory domain. When enabling end-user recovery in DPM, several tasks need to be done in your Active Directory domain. These tasks include:

- Extending Active Directory Domain Services schema to enable end-user recovery
- Create a container and grant permission to it in Active Directory for end-user recovery

For these you will need a domain administrator account and schema administrator privileges in the domain. End-user recovery is covered in greater detail in *Chapter 6*.

Antivirus on DPM server

DPM will work just fine with most antivirus solutions but there are some issues to look out for. The last thing you want is for your antivirus to affect your DPM server's performance. You need to watch how you handle real-time virus monitoring and infected files. Disable real-time monitoring of DPMs `DPMRA.exe` process. Also disable real-time scanning of the `csc.exe` process. The `DPMRA.exe` process is located in `Microsoft Data Protection Manager\DPM\bin`. The `csc.exe` process is located in `Windows\Microsoft.net\Framework\v2.0.50727`. If you do not disable monitoring of the `DPMRA.exe` process then `DPMRA.exe` will eventually slow down your DPM server because the antivirus will scan all the files whenever DPM adds changes to its replicas. If the `csc.exe` process is scanned by the real-time scanner, the DPM admin console could potentially slow down. The `csc.exe` process is the C# complier and emits files when generating XML messages. If these files are scanned you will end up taking a performance hit.

Replicas and recovery points can easily be corrupted by antivirus software. If your antivirus software is set to clean or quarantine infected files this can corrupt the replica and recovery point data. Cleaning and quarantining causes the antivirus to modify files with changes that DPM cannot detect.

When DPM synchronizes replica data and this data has been changed by something other than DPM, the data will get corrupted. This may corrupt the recovery points as well as render recovery of this data impossible.

There is a simple solution to this problem. Set up your antivirus software to delete infected files instead of cleaning and quarantining them. There is one problem that the antivirus deleting infected files can cause. It causes replicas to become inconsistent. You will have to either manually run a consistency check to fix this or DPM 2010 can be configured to autorun a consistency check if a data source becomes inconsistent.

Firewall ports

Protecting computers behind a firewall with DPM is a topic in many forums. To protect firewalled servers or clients you need to open up ports for communication between the DPM server, domain controllers on your network, and the protected computers.

You will want to make sure the Windows 2008 server firewall on the server that you are going to install DPM on is configured for DPM traffic. If the firewall is enabled during the DPM installation the setup will correctly configure the firewall for communication between DPM and the protected clients. If the server's firewall is not enabled during the set up you will need to manually configure the firewall after installation. The following is a chart of firewall ports used by DPM:

Protocol	Port	Details
DCOM	135/TCP Dynamic	The DPM control protocol uses DCOM. DPM issues commands to the protection agent by invoking DCOM calls on the agent. The protection agent responds by invoking DCOM calls on the DPM server. TCP port 135 is the DCE endpoint resolution point used by DCOM. By default, DCOM assigns ports dynamically from the TCP port range of 1024 through to 65535. However, you can configure this range by using Component Services. For more information, see **Using Distributed COM with Firewalls** (`http://go.microsoft.com/fwlink/?LinkId=46088`). Note that for DPM-Agent communication you must open the upper ports 1024-65535. To open the ports, perform the following steps: • In IIS 7.0 Manager, in the **Connections** pane, click the server-level node in the tree • Double-click the **FTP Firewall Support** icon in the list of features • Enter a range of values for the **Data Channel Port Range** • After you enter the port range for your FTP service, in the **Actions** pane, click **Apply** to save your configuration settings
TCP	5718/TCP 5719/TCP	The DPM data channel is based on TCP. Both DPM and the protected computer initiate connections to enable DPM operations such as synchronization and recovery. DPM communicates with the agent coordinator on port 5718 and with the protection agent on port 5719.
DNS	53/UDP	Used between DPM and the domain controller, and between the protected computer and the domain controller, for host name resolution.
Kerberos	88/UDP 88/TCP	Used between DPM and the domain controller, and between the protected computer and the domain controller, for authentication of the connection endpoint.
LDAP	389/TCP 389/UDP	Used between DPM and the domain controller for queries.

Protocol	Port	Details
NetBIOS	137/UDP 138/UDP 139/TCP 445/TCP	Used between DPM and the protected computer, between DPM and the domain controller, and between the protected computer and the domain controller, for miscellaneous operations. Used for SMB directly hosted on TCP/IP for DPM functions.

(Source: DPM deployment and planning guide 2010)

There tends to be a lot of posts regarding what ports to open on client firewalls to install the DPM agent. The note from the previous chart addresses these issues by opening ports 1024-65535 on the computer you want to protect. After you open those ports, the agent should be able to install through the firewall. The other option is to disable the Windows firewall on the clients' computers you will be protecting. Note that disabling the Windows firewall on the computers you want to protect is a security risk.

End-user recovery requirements

DPM is capable of end-user recovery. This is great for administrators and end-users alike. It gives power to end-users if they need to recover some data they have lost. The end-users can only recover data that is within folders. When planning your DPM deployment you should consider what data will be end-user recoverable so you can specify this in DPM.

If you have shares on your servers that use shadow copies you can remove this and get the space back that these shadow copies were using. With end-user recovery you don't need to have shadow copies. End-user recovery essentially does the same thing. It allows users to recover previous versions of their data. Later, in *Chapter 8* we will cover how to set up end-user recovery in DPM.

Summary

Backups and Disaster Recovery (DR) are critical to a business's survival. This chapter covered the ins and outs of making a backup plan and outlines what you need to know when planning your DPM deployment. An ideal backup plan must address what to back up, the right media to use, scheduling of back ups, the procedures that should be in place to ensure integrity of the backups, security, and privacy. Different areas in your DPM deployment need to be planned in order for DPM to fit your specific backup and recovery goals. Backup and recovery goals encompass protection groups, different media to support DPM, storage pools, and storage capacity plans. To configure the DPM server you must determine how many DPM servers to deploy, where to locate them, choose the right SQL instance, DPM security, how DPM works with firewalls, and end-user recovery.

In the next chapter we will walk you through the entire process of installing DPM.

3
Installation

The DPM installation as well as the upgrade process is pretty straightforward. The areas where the DPM installation can get tricky are prerequisites, hardware and software requirements, as well as making sure your operating system is properly updated and patched. All of these things need to be met or completed before you can start the DPM installation. With the DPM upgrade you will face some of the same issues as with the installation such as what are the prerequisites? is your operating system patched? and is DPM 2007 fully patched and ready for the upgrade? This chapter will walk you through each step of the DPM installation process during the first half and the DPM 2007 to DPM 2010 upgrade in the second half. After reading this chapter you should know what to look for when working through the prerequisites and requirements. The goal is to ensure that your install or upgrade goes smoothly.

In this chapter we shall cover the following topics:

- Installing DPM
- Installing Single Instance Store (SIS)
- Installing DPM (on a local or remote SQL instance)
- Migrating from DPM 2007 to DPM 2010

Prerequisites

In this section we will jump right into the prerequisites for DPM and how to install them as well as the two different ways to install DPM. We will also go through the DPM 2007 to DPM 2010 upgrade process.

We will first visit the hardware and software requirements, and a pre-install that is needed before you are able to actually install DPM 2010.

Hardware requirements

DPM 2010 requires a processor of 1 GHz (dual-core or faster), 4 GB of RAM or higher, the page file should be set to 1.5 or 2 times the amount of RAM on the computer. The DPM disk space requirements are as follows:

- DPM installation location needs 3 GB free
- Database file drive needs 900 MB free
- System drive needs 1 GB free
- Disk space for protected data should be 2.5 to 3 times the size of the protected data

DPM also needs to be on a dedicated, single purpose computer.

Software requirements

DPM has requirements of both the operating system as well as software that needs to be on the server before DPM can be installed. Let's take a look at what these requirements are.

Operating system

DPM 2007 can be installed on both a 32-bit and an x64-bit operating systems. However, DPM 2010 is only supported on an x64-bit operating systems. DPM can be installed on a Windows Server 2008 and Windows Server 2008 R2. It is recommended that you install DPM 2010 on Windows Server 2008 R2.

DPM can be deployed in a Windows Server 2008, Windows Server 2008 R2, or Windows Server 2003 Active Directory domain. Be sure to launch the Windows update and completely patch the server before you start the DPM installation, no matter what operating system you decide to use. If you end up using Windows 2008 Server for your DPM deployment you will need to install some hotfixes before you start the DPM installation. The hotfixes are as follows:

- FIX: You are prompted to format the volume when a formatted volume is mounted on a NTFS folder that is located on a computer that is running Windows Server 2008 or Windows Vista (KB971254) (`http://go.microsoft.com/fwlink/?LinkId=184109`).
- Dynamic disks are marked as "Invalid" on a computer that is running Windows Server 2008 or Windows Vista. When you bring the disks online, take the disks offline, or restart the computer if Data Protection Manager is installed (KB962975) (`http://go.microsoft.com/fwlink/?LinkId=185942`).

- An application or service that uses a file system filter driver may experience function failure on a computer that is running Windows Vista, Windows Server 2003, or Windows Server 2008 (KB975759) (`http://go.microsoft.com/fwlink/?LinkId=185943`).

Software

By default, DPM will install any software prerequisites automatically if it is not enabled or installed. Sometimes these software prerequisites might fail during the DPM setup. If they do, you can install these manually.

Visit this site for detailed information on installing the software prerequisites:
`http://technet.microsoft.com/en-us/library/ff399781.aspx`

The following is a list of the software that DPM requires before it can be installed:

- Microsoft .NET Framework 3.5 with Service Pack 1 (SP1)
- Microsoft Visual C++ 2008 Redistributable
- Windows PowerShell 2.0
- Windows Installer 4.5 or later versions
- Windows Single Instance Store (SIS)
- Microsoft Application Error Reporting

NOTE: It is recommended that you manually install Single Instance Store on your server before you even begin the DPM 2010 installation. We shall see a step by step installation along with a detailed explanation of Single Instance Store.

User privilege requirement

The server that you plan to install DPM on must be joined to a domain before you install the DPM software. In order to join the server to the domain you need to have at least domain administrative privileges. You also need to have administrative privileges on the local server to install the DPM software.

Restrictions

DPM has to be installed on a dedicated server. It is best to make sure that DPM is the only server role running on the server you use for it. You will run into issues if you try to install DPM on a server with other roles on it. The following are the restrictions you need to pay attention to when installing DPM:

- DPM should not be installed on a domain controller (not recommended)
- DPM cannot be installed on an Exchange server
- DPM cannot be installed on a server with System Center Operations Manager installed on it
- The server you install on cannot be a node in a cluster

There is one exception—you can install DPM on a domain controller and make it work but this is not supported by Microsoft.

Single Instance Store

Before you install DPM on your server, it is important to install a technology called Single Instance Store (SIS). SIS will ensure you get the maximum performance out of your disk space and reduce bandwidth needs on DPM.

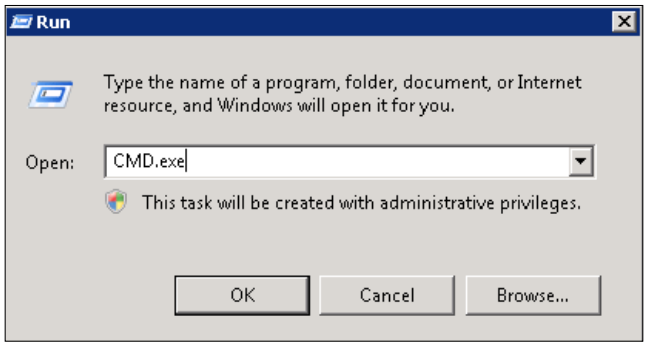
SIS is a technology that keeps the overhead of handling duplicate files low. This is often referred to as **de-duplication**. SIS is used to eliminate data duplication by storing only one copy of files on backup storage media. SIS is used in storage, mail, and backup solutions such as DPM. SIS helps to lower the costs of bandwidth when copying data across a network as well as needed storage space.

Microsoft has used a single installation store in Exchange since version 4.0. SIS searches a hard disk and identifies duplicate files. SIS then saves only one copy of the files to a central location such as a DPM storage pool. SIS will then replace other copies of the files with pointers that direct you to the copy of the files the SIS repository already has stored.

Installing Single Instance Store (SIS)

The following procedure walks you through the steps required to install SIS:

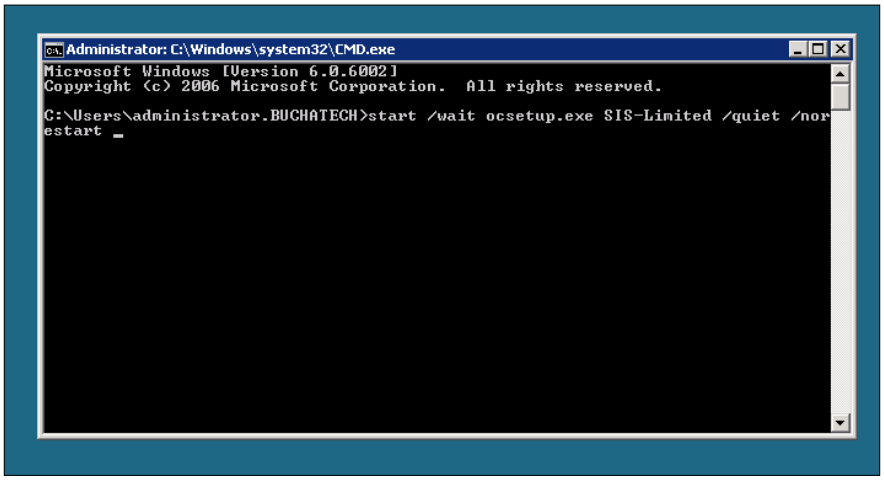
1. Click **Start** and then click **Run.**
2. In the **Run** dialog box, type **CMD.exe** and press **OK**:



3. At the command prompt type the following:

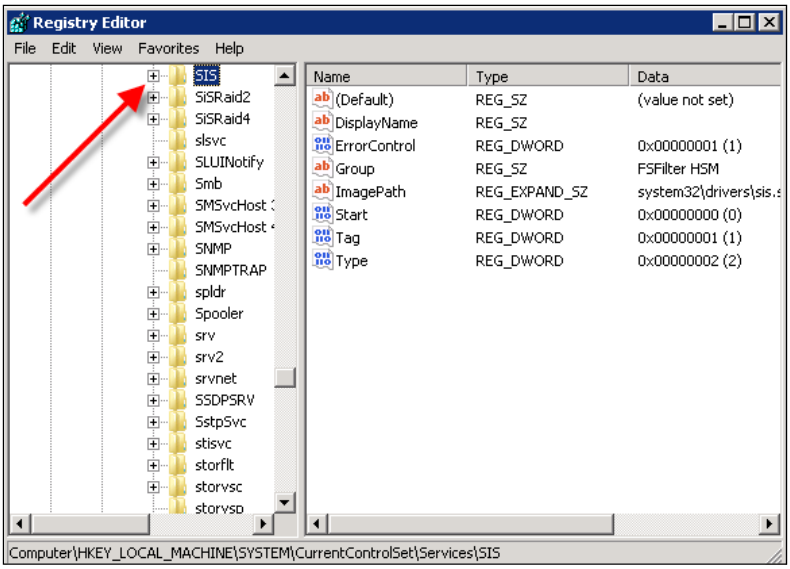
   ```
   start /wait ocsetup.exe SIS-Limited /quiet /norestart
   ```

   And then press **Enter**.



4. **Restart** the server.
5. To ensure the installation of SIS went okay, check for the existence of the SIS registry key.
6. Click **Start**, then click **Run.**
7. In the **Run** dialog box, type `regedit` and press **OK**.

8. Navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SIS`:



If the **SIS** key is shown (as in the screenshot) in the registry it would mean that Single Instance Store (SIS) is installed properly and you can be sure to get the maximum performance out of your disk space on the DPM server.

Installing DPM

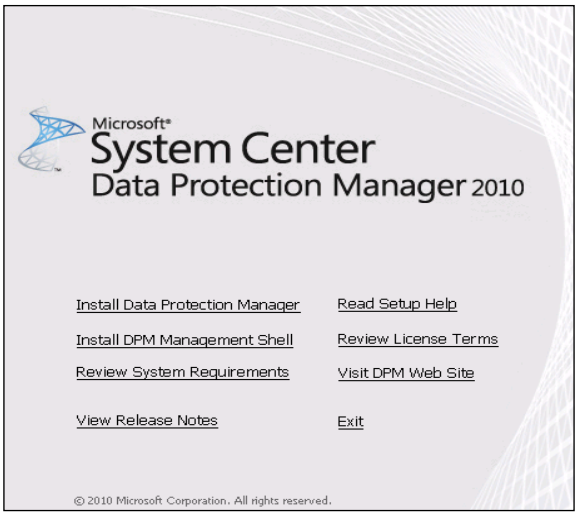
Now we move on to the actual installation of DPM. This section is divided into two parts:

- Installing DPM on a local SQL instance
- Installing DPM on a remote SQL instance

Installing DPM using a local instance of SQL Server 2008

To begin your installation of DPM using a local instance of SQL Server 2008, you will need to complete the following steps:

1. Launch the DPM 2010 installer from the disk and select the **Review System Requirements option**.



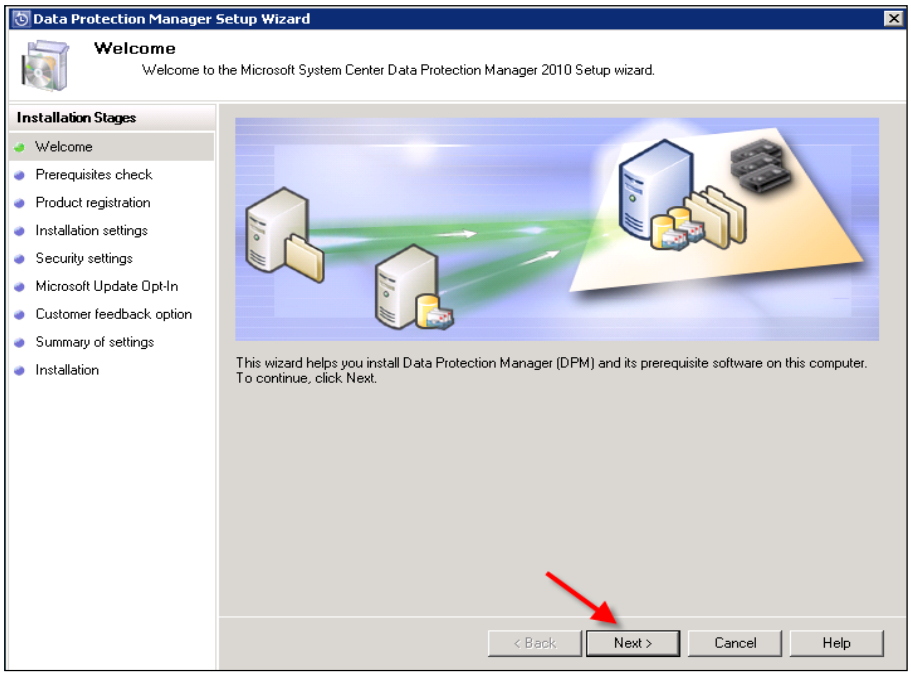
2. This will bring you to a technet site where you can learn more about DPMs requirements. The following is the URL to this site:

   `http://technet.microsoft.com/en-us/library/ff399554.aspx`

NOTE: You do not need to install DPM Management Shell because it will be installed with DPM.

3. Close the web browser when you are finished.
4. Go back to the splash launch screen. Click on **Install Data Protection Manager** this time.
5. On the next screen accept the licensing terms.
6. A window will pop up and copy the temporary setup files for the DPM installation.

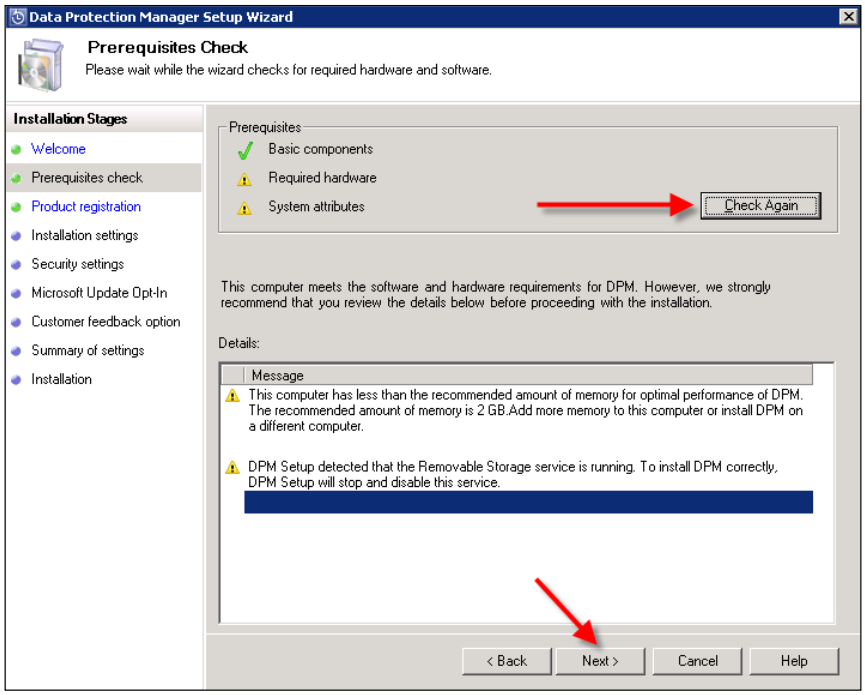
7. Click **Next** on the **Data Protection Manager Setup Wizard Welcome** screen.



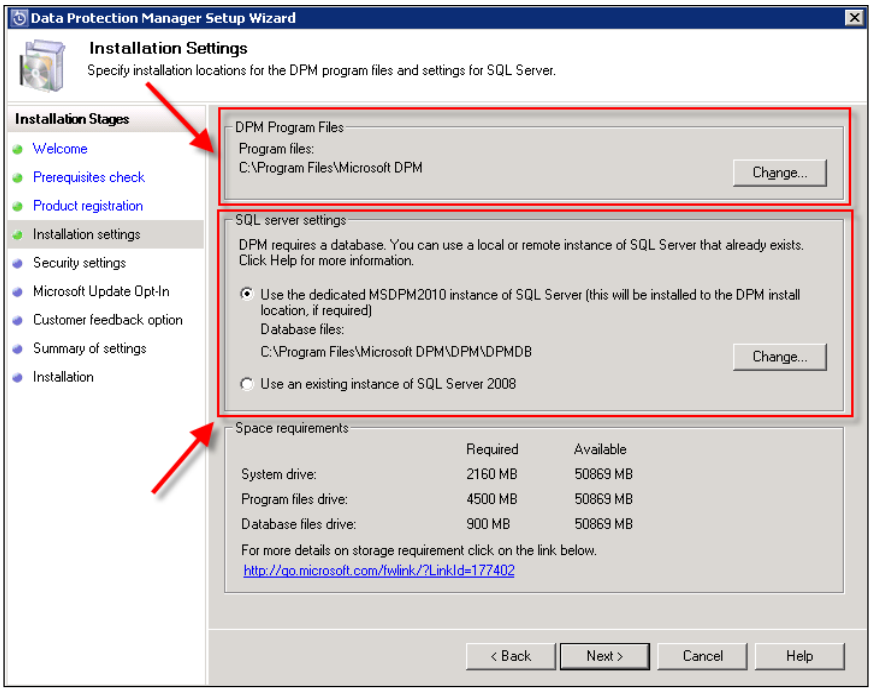
8. This next screen runs the prerequisite check on the server you are attempting to install DPM on. If there are any issues with this server the **Prerequisite check** will let you know and you will need to fix them before the installation will allow you to continue. After you have fixed the issues that arose, you will need to click **Check Again** before the installation will let you click **Next**.

[**NOTE**: The DPM installation stops the Removable Storage service, before it will continue installing DPM 2010.]

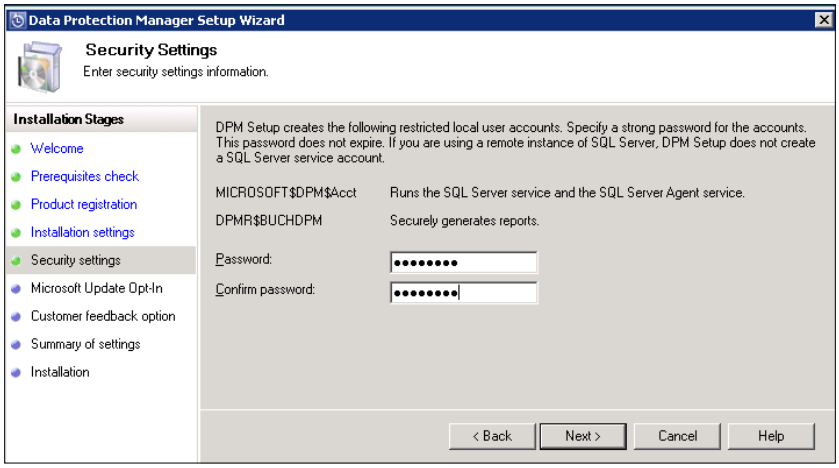
Click **Next** to continue with the installation.



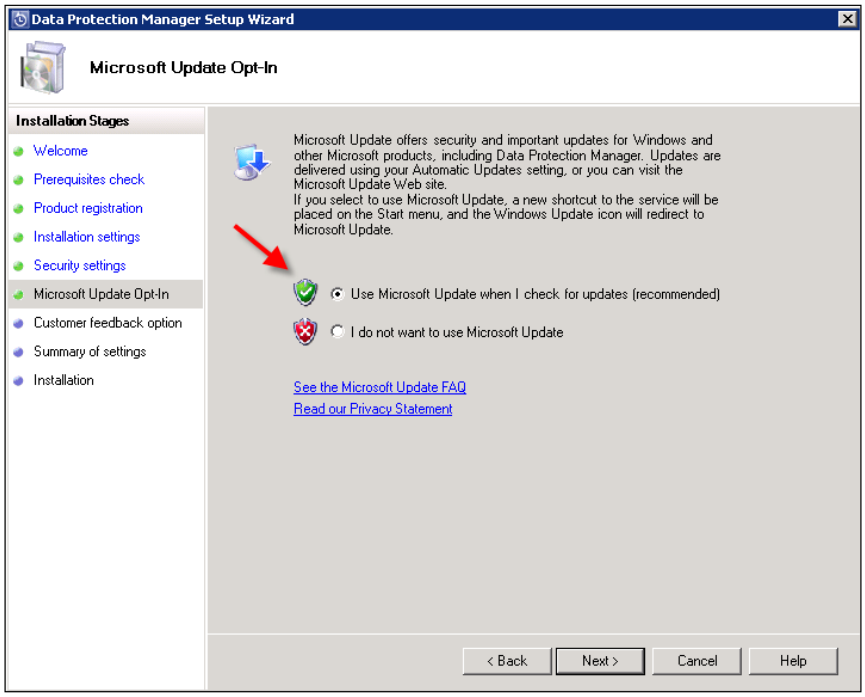
9. On the **Product registration** screen, enter your username, company name, product key, and the number of licenses that you have purchased. Then click **Next**.
10. The **Installation settings** screen lists your installation directories as well as the type of SQL instance and gives you the option to choose a local dedicated SQL instance or a remote SQL instance as well as your DPM installation path. Once you have confirmed your installation settings click **Next.**



11. On the **Security settings** screen, input a password. When you install a local SQL instance, DPM creates a local account that is used for the SQL Server and SQL Agent services.



12. Click **Next**, then on the **Microsoft Update Opt-In** screen choose **Use Microsoft Update when I check for updates** and click **Next**:



13. On the next screen choose one of the two options and click **Next**.
14. Review your installation settings and click **Install**.
15. The next screen gives you the status of the SQL installation and the DPM installation as it progresses along.
16. Once the installation is complete click **Close**.

That's it; Data Protection Manager 2010 is installed. In the next chapter we will dig into the configuration of DPM. Below you will see how to install DPM using a remote SQL instance.

Installing DPM using a remote instance of SQL Server 2008

Before you begin your installation of DPM on a remote SQL instance, there are a few tasks you need to ensure are complete on your remote SQL Server first. These tasks are:

- Before you install DPM, you must install a new, dedicated instance of SQL Server 2008 SP1
- When you install the SQL Server, keep the default failure audit settings, enable password policy checking, and assign a strong password to the SA account
- Install SQL Database engine and SQL Reporting Services components only
- Make sure the remote SQL 2008 server has SP1 installed. This must also be Standard or Enterprise Edition
- Make sure the account that you log onto the DPM server with is a domain user and that this account is a member of the local administrators group on the server that the remote SQL instance is on and the SQL Server sysadmin fixed server role on the computer running the remote instance of SQL Server
- On the remote SQL Server, enable the **Named Pipes** protocol for the instance that you are going to install the DPM database on
- In order for DPM to access the SQL Server through its firewall, configure an incoming exception for `sqlservr.exe` for the instance that you are going to place the DPM database on to allow port 80 on TCP protocol

NOTE: If you are installing SQL Server on Windows Server 2008 R2, a compatibility warning might appear. Select **Run program**, and then proceed with the SQL Server 2008 installation. For more information see the following link:

`http://technet.microsoft.com/en-us/library/ff399303.aspx`

By completing the above tasks your remote SQL Server should be prepared for your DPM database. Now let's get to the installation:

1. Launch the DPM 2010 installer.

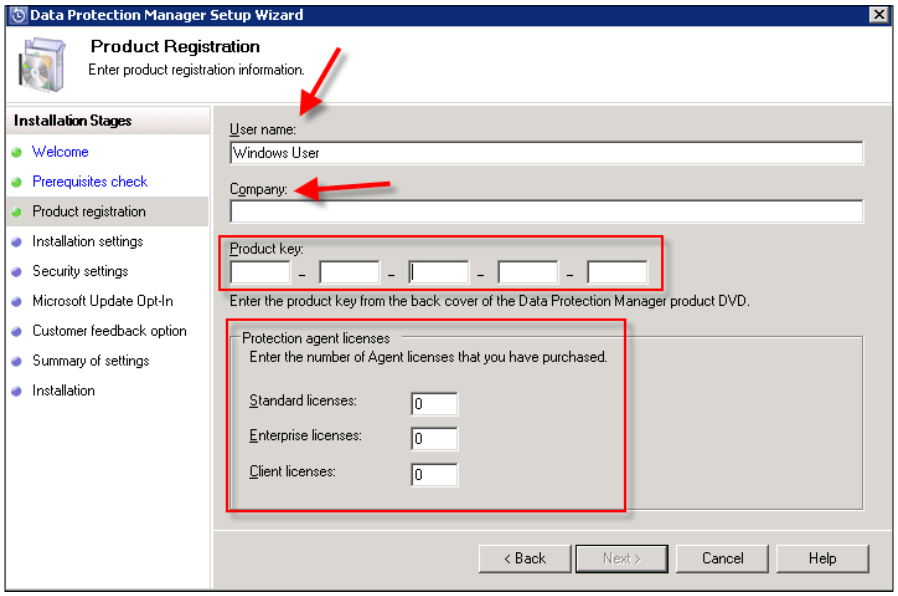
NOTE: You do not need to install the DPM Management Shell because it will be installed with DPM.

2. Click on **Install Data Protection Manager**.

3. On the next screen accept the licensing terms.
4. A window will pop up and copy the temporary setup files for the DPM installation.
5. Click **Next** on the **Welcome** screen.
6. This next screen runs the Prerequisite check on the server you are attempting to install DPM on. If there are any issues with this server the Prerequisite check will let you know and you will need to fix them before the installation will allow you to continue. After you have fixed the issues that came up you will need to click **Check Again** before the installation will let you click **Next.**

[**NOTE**: The DPM installation stops the Removable Storage service, before it continues with installing DPM 2010.]

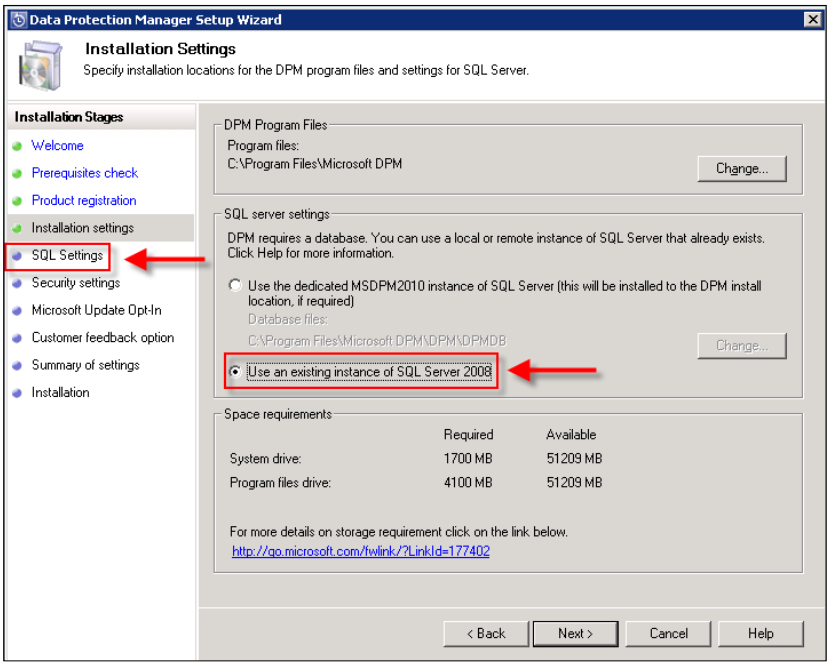
7. Click **Next** to continue with the installation.
8. On the **Product registration** screen, enter your username, company name, product key, and the number of licenses that you have purchased then click **Next**:



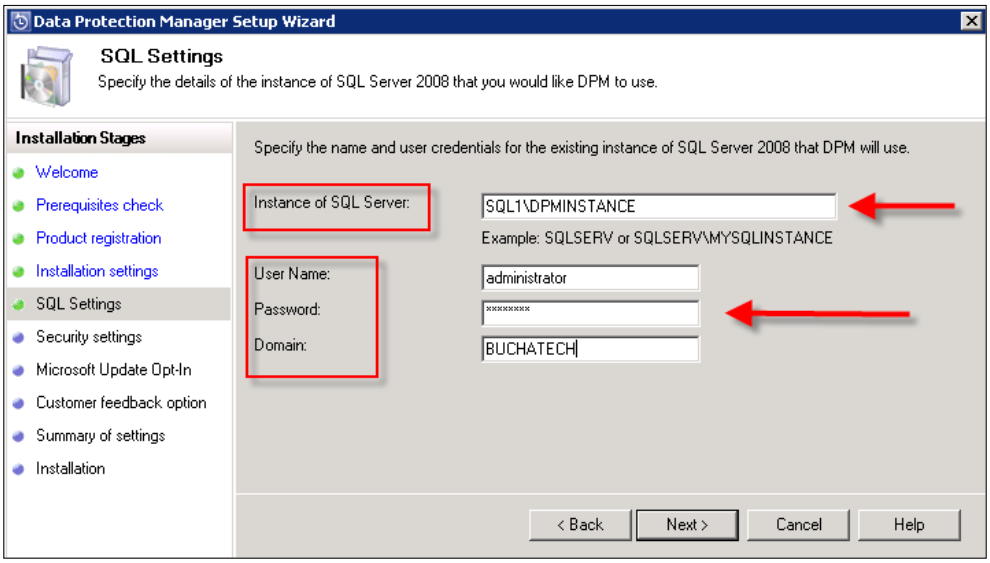
9. The **Installation settings** screen lists your installation directories as well as the type of SQL instance and gives you the option to choose a local dedicated SQL instance or a remote SQL instance as well as your DPM installation path.

NOTE: This time you need to select an existing instance. You will notice on the left-hand side it does not list the **SQL Settings**. When you click **Next** you will need to enter the settings for the remote SQL instance.

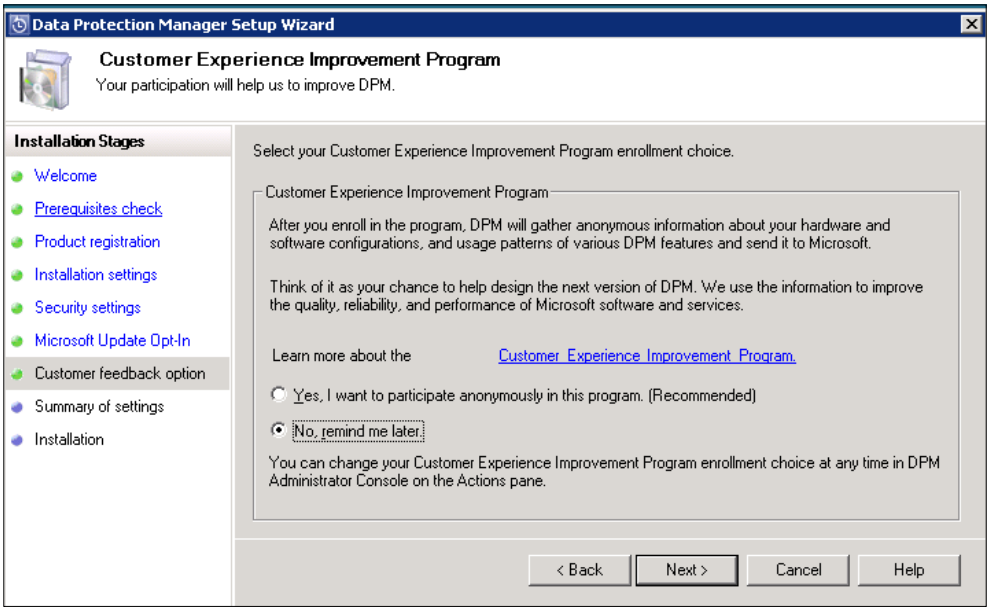
10. Once you have confirmed your installation settings click **Next.**



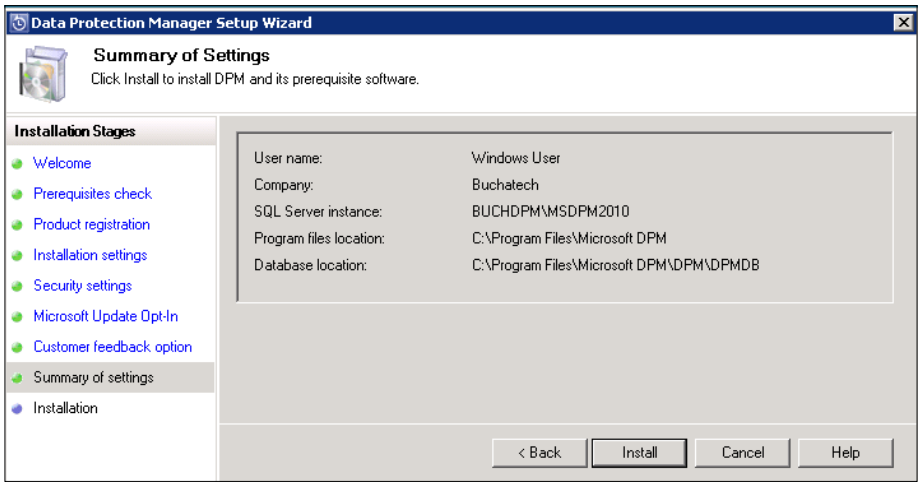
11. Fill in your existing SQL instance along with credentials in the **SQL Settings** screen and click **Next.**



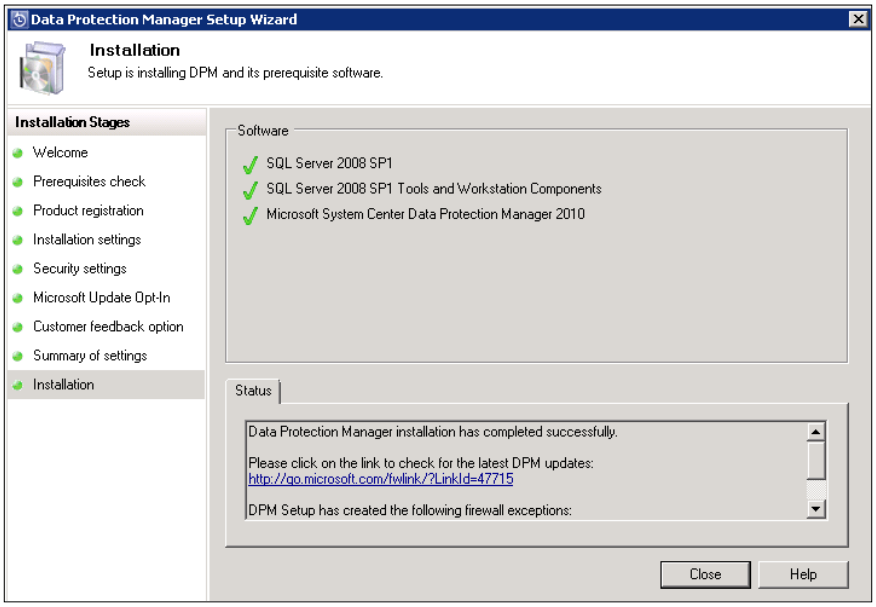
12. Enter a password for DPM in the **Security settings** and click **Next**.
13. Then on the **Microsoft Update Opt-In** screen, choose **Use Microsoft Update when I check for updates** and click **Next.**
14. On the next screen, choose one of the two options and click **Next.**



15. Review your installation settings and click **Install.**



16. The next screen gives you the status of the SQL installation and the DPM installation as it progresses along.
17. On the next screen click **Close:**



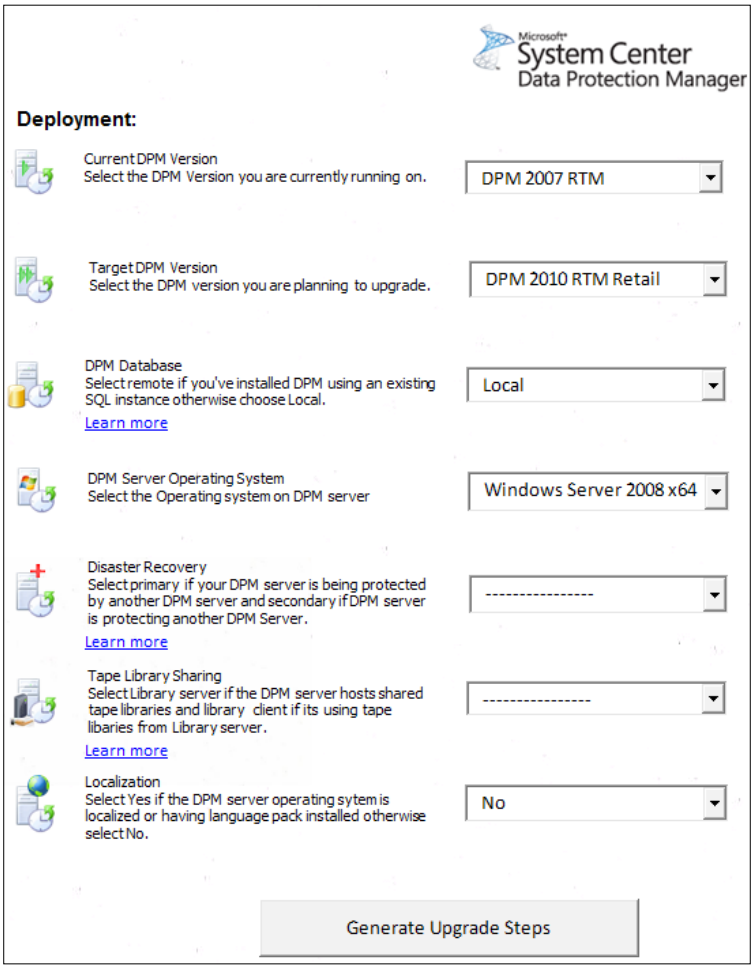
Data Protection Manager 2010 is now installed.

Migrating from DPM 2007 to DPM 2010

Microsoft has released an **upgrade adviser tool** for upgrading from DPM 2007 to DPM 2010. You will need to run this to see if your current DPM 2007 is ready for the upgrade. This is a tool that asks you a series of questions and it will give you the recommended steps to take in order to upgrade your DPM from 2007 to 2010. This tool is an excel file and can be downloaded at the following site:

`http://blogs.technet.com/b/dpm/archive/2010/02/26/upgrade-advisor-for-dpm-2010-now-available.aspx`

Here are what the questions are and what the tool looks like:



Here are the steps that the tool recommends after answering the series of questions:

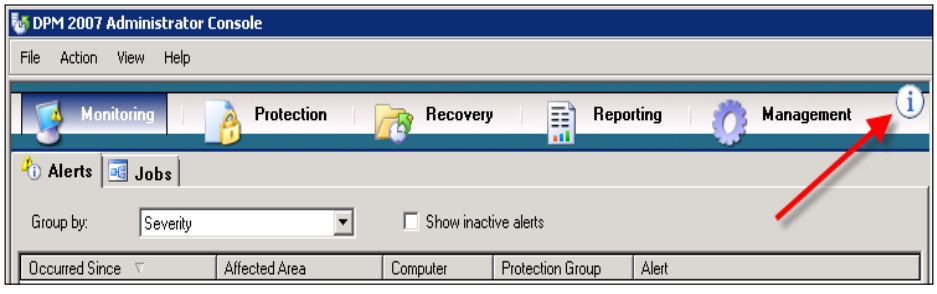
1. Upgrade to DPM 2007 SP1 (`http://support.microsoft.com/kb/959605`) (mandatory) and install the latest rollup package (`http://support.microsoft.com/kb/979970`) (optional).
2. Close the DPM administrator console and DPM Management Shell if opened.
3. Launch the DPM 2010 RTM retail setup and proceed by clicking on **Install** DPM.
4. Complete the installation wizard and restart the computer to complete the upgrade.
5. Upgrade agents on production servers.

NOTE: If rollup KB976542 (version 2.0.8861.0) or the latter is installed, you can upgrade the agent from the DPM Administrator Console. If this rollup is not installed, you should upgrade the agents manually by running the `DPMAgentInstaller`.

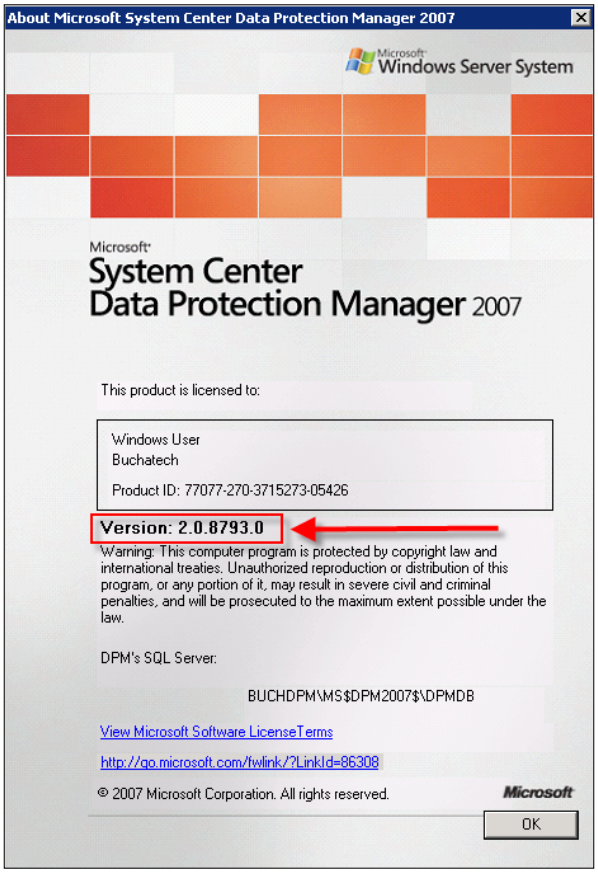
6. Run a consistency check for all the protected datasources.
7. Uninstall DPM 2007 SQL instance (optional) if there are no issues after the upgrade. However, if you're looking to downgrade then DPM 2007 DPMDB is required.

Depending on the state of your current DPM and the server it is installed on you may need to do some pre-work. You need to make sure your server, DPM, and SQL are fully patched and up-to-date before you can upgrade. You will need to check the following requirements and recommendations on your current DPM 2007 server before you can run the upgrade:

1. You need to make sure your DPM 2007 server is service pack 1.
2. To check your DPM service pack level, open the DPM administrator console and click on the icon in the upper-right hand corner, as shown:



3. On the DPM 2007 information page, check the version number is the same as in the following image. If this version number is 2.0.5820.0 or higher then service pack 1 is installed.



4. Install all of the latest hotfixes for DPM 2007 SP1. To get the latest updates and hotfixes for DPM go to:

   `http://go.microsoft.com/fwlink/?LinkId=188865`

5. Make sure your DPM 2007 server is installed on Windows Server 2008 or Windows Server 2008 R2, either needs to be 64 bit.
6. Make sure the disk on which DPM 2007 is installed and you plan to run the upgrade on has a minimum of 3 GB of free space.
7. It is highly recommended that you back up your current DPM database (DPMDB) on external media. If you don't know how to do this you can refer to *Chapter 10* for a walkthrough.

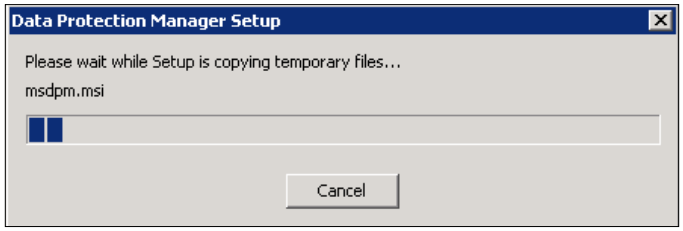
8. If you are using a local dedicated SQL instance, don't worry, the DPM upgrade process will install SQL 2008 and place the new database here. If you are using a remote SQL instance on SQL 2005 it is recommended that you do a fresh install of SQL 2008. This can be SQL Standard or Enterprise editions. You will then point the DPM 2010 upgrade installation to this remote SQL instance.

Upgrade process

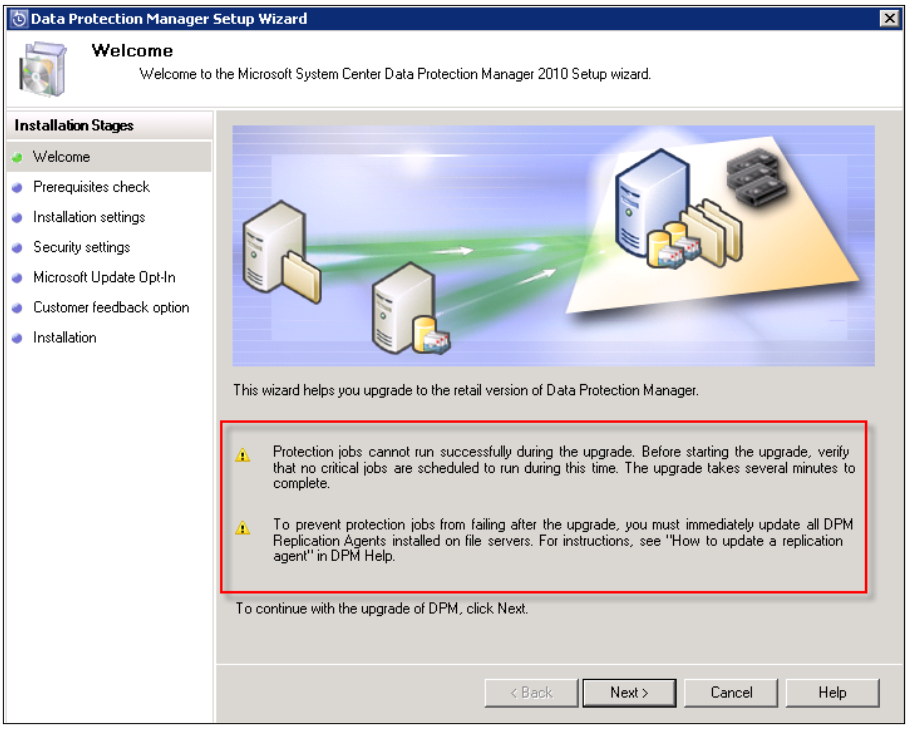
Now, let's get into the upgrade process itself. This will be a step by step guide to completing the installation. The upgrade installation is somewhat similar to the DPM 2010 installation. You will need to complete the following steps:

1. Launch the DPM 2010 installer.
2. Click on **Install Data Protection Manager**:

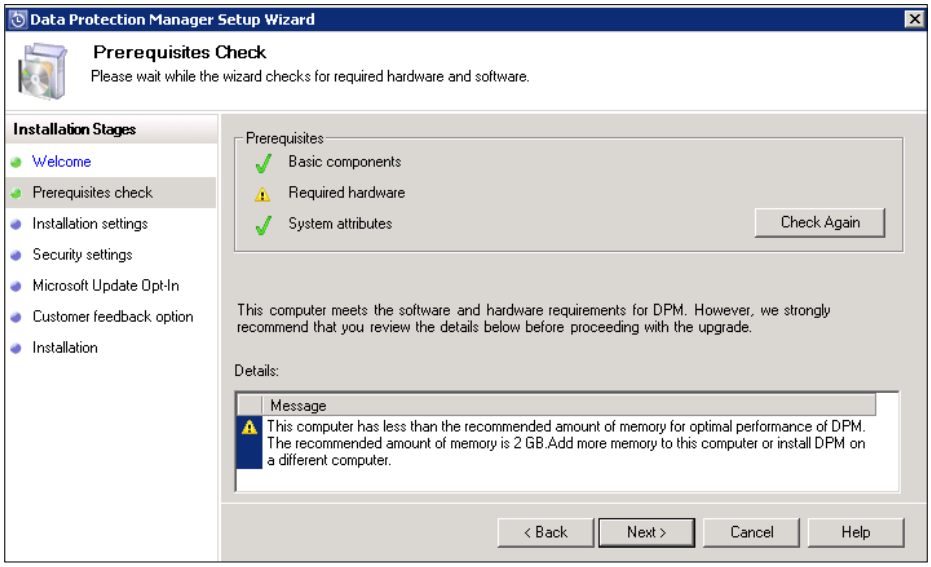
3. Accept the licensing terms and click **OK**. DPM will copy the setup files just like the regular installation does:



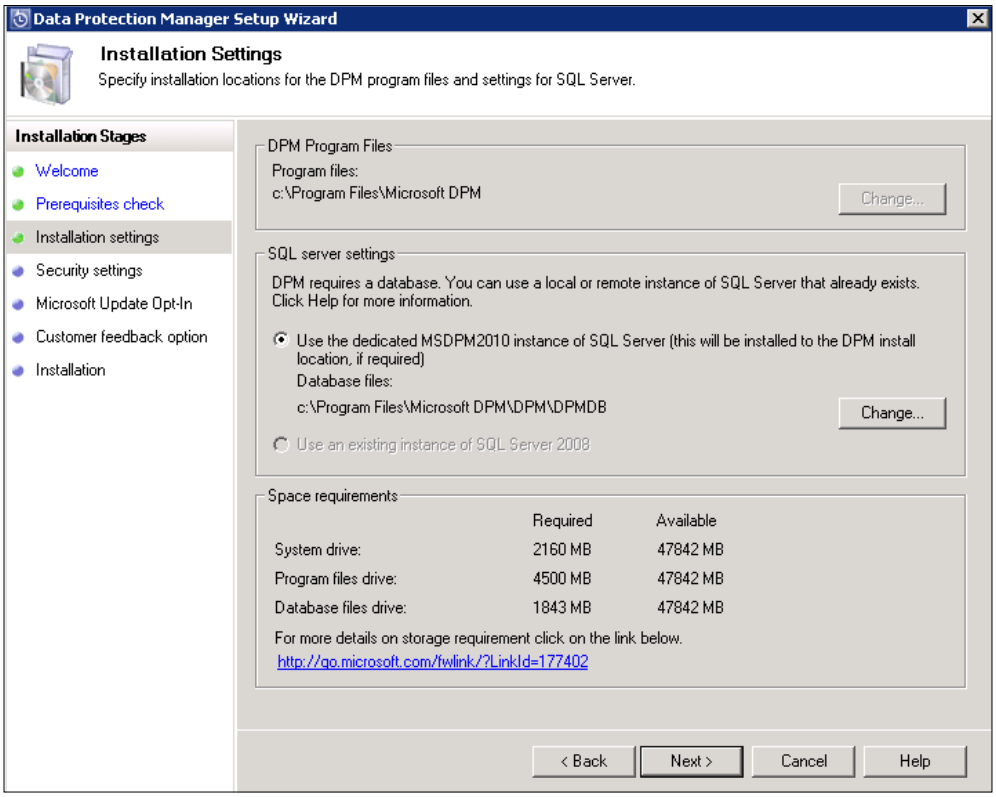
4. The **Welcome** screen reminds you that all protection jobs need to be stopped during the upgrade process. You also need to update the DPM agents right after the upgrade on your protected servers.



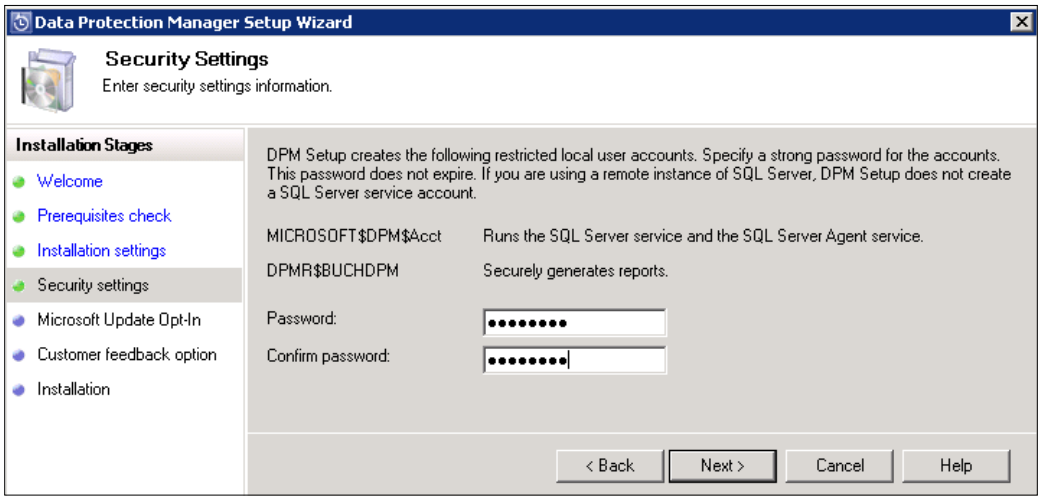
5. Click **Next** to go to the next screen.
6. The installation then checks all the prerequisites.



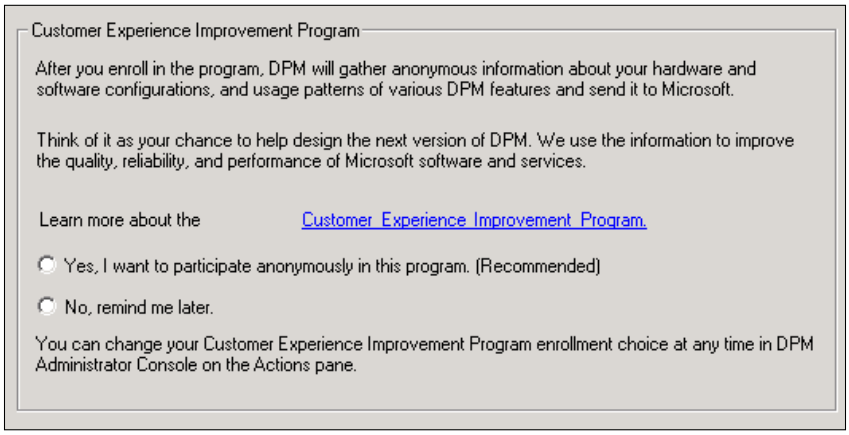
7. Take care of any issues that the installation finds then click **Check Again**. Once everything is okay click **Next**.
8. The next screen is the DPM installation path and choice of SQL instance. You can chose a local dedicated or a remote SQL instance. Make your selections and click **Next**.



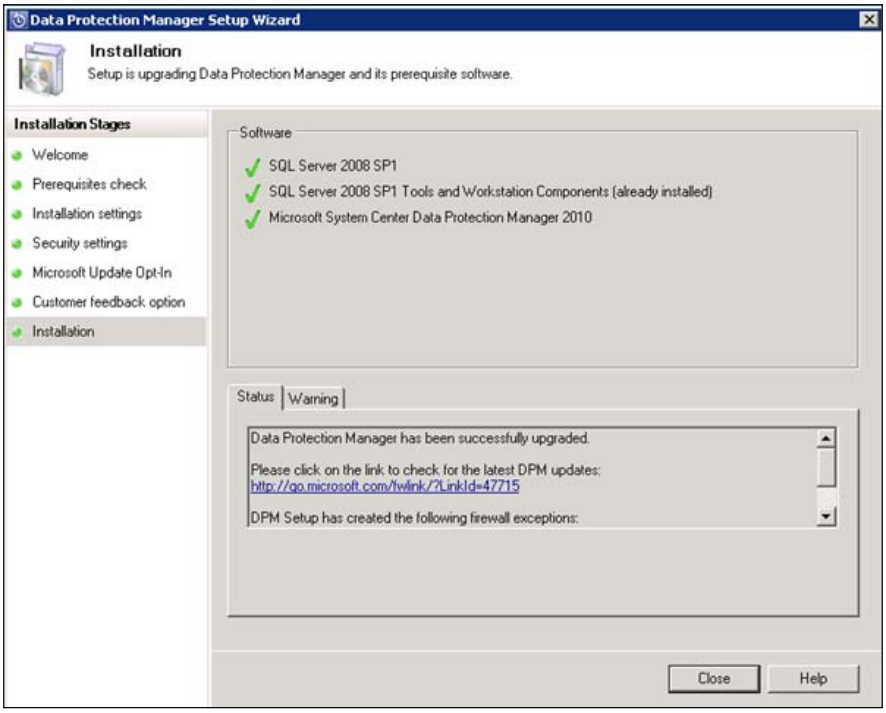
9. If you selected a local SQL instance then fill in a password and click **Next**. If you chose remote SQL instances then input your SQL Server settings and click **Next**. If you need instructions on this please refer to *Installing DPM using a remote instance* of SQL Server 2008 earlier in this chapter.



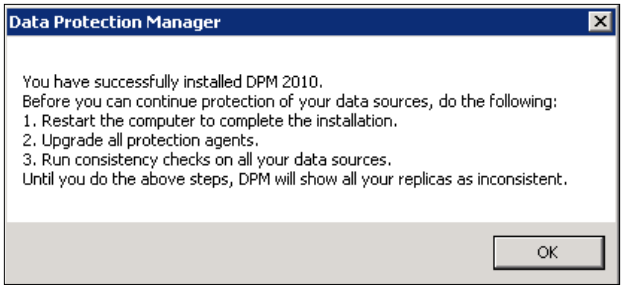
10. Choose to use Microsoft updates and click **Next**. Select whether you want to send Microsoft feedback or not and click the **Upgrade** button to start the DPM upgrade.



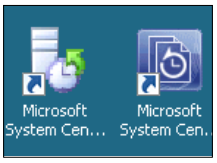
11. If you see the following screen with all check marks, it means that the upgrade went smooth. Click **Close** to complete it.



12. A window will pop up reminding you to reboot your server and to update the DPM agents on all of your protected servers:



13. You will now see DPM 2007 and DPM 2010 icons on your desktop:



14. Once you reboot, DPM 2007 will be completely removed.

The post-upgrade process

After successfully upgrading to DPM 2010, there are some tasks you need to complete to get the rest of your servers functioning properly with DPM 2010. These tasks are:

- Upgrade all of the protection agents on protected servers. Upgrading the agents will not require a restart of the protected computer.
- Once you upgrade the DPM server and the agents on the protected computers, all of your protected data will go into an inconsistent state. You will need to perform a consistency check on all of the protected data after the agents have been upgraded.

Upgrading a protection agent

The following are the steps to perform an agent upgrade by running the `DPMAgentInstaller.exe`:

- In the root directory on your DPM 2010 disc, locate the agent's folder, and then copy these two files: `DPMAgentInstaller_x64.exe` and `DPMAgentInstaller_x86.exe` to a share on your network or an external drive.
- Now log on to your protected servers and either put in your external drive or navigate to your network share where you put the DPM agent installation files in. Now run the appropriate `DPMAgentInstaller.exe` file. You will either have a 32-bit or a 64-bit server.

Summary

In this chapter, we first looked into the prerequisites for installing DPM 2010; what is needed before you can install DPM 2010 and the aspects that need be checked and taken care of pre-install. This can be done using a local or remote SQL instance. We then moved on to migrating from DPM 2007 to DPM 2010 using the Upgrade Adviser tool.

Just like any other server role there is specific administration and routine maintenance that needs to be done to keep DPM up and running. In the next chapter you will learn what these administration and maintenance tasks are.

4
Configuration

In this chapter we are going to learn how to configure DPM after its installation. There are some optional DPM configurations and there are some required DPM configurations—we will cover both. The required DPM configurations are needed for DPM to function. The optional DPM configurations can be useful for you in your environment. We will cover these optional configurations so you can determine what you want to use or don't want to use.

We will configure the following:

- Required:
  - Adding disks to the storage pool
  - Configuring tape libraries
  - Configuring the WSS Writer service
- Optional:
  - Auto Discovery
  - Throttle
  - Setting up an SMTP server
  - Configuring alert notifications
  - Publishing DPM alerts
  - Configuring DPM Management Shell
  - Configuring DPM for End-user Recovery

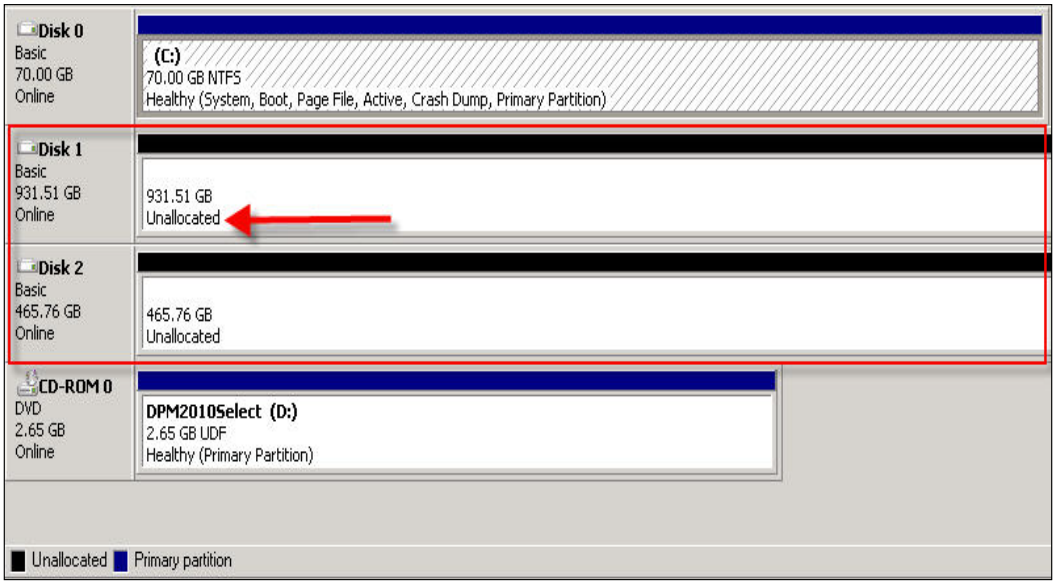
Required configurations

First of all, we will cover the required DPM configuration tasks. Remember these are required for DPM to function. The following topics are guides on how to set up these configurations.

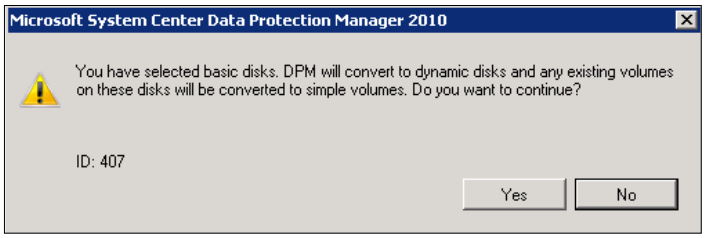
Adding disks to the storage pool

You cannot start protecting any data without a disk to store the backup data on. The first step that should be taken is configuring a disk(s) in your storage pool in DPM. Once you do this you can begin protecting servers and clients. There are a couple of things you need to do to your disk(s) before DPM will allow you to add them to a storage pool.

The disk(s) cannot be formatted or have a drive letter. Basically you should not be able to see the disk in Windows Explorer like other disks. The disk(s) need to remain unformatted. The following screenshot is an example of what your disk(s) should look like in Windows Disk Management.



NOTE: You will notice the disks in the image are basic disks. DPM requires the disks that you will use with it to be dynamic disks. If you try to add a disk(s) to a storage pool, DPM will prompt you to convert the disk to a dynamic disk. You can see this in the following image:



DPM does not support USB disks without a work around. The work around to use USB disks with DPM is a third-party software called **Firestreamer** made by a software company named **Cristalink.** We will cover how to use this software under *Configuring tape libraries* in the next section.

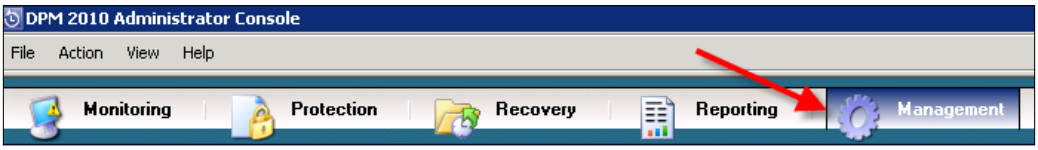
To add a disk(s) to your storage pool follow these steps:

1. Open up the DPM 2010 Administrator Console.

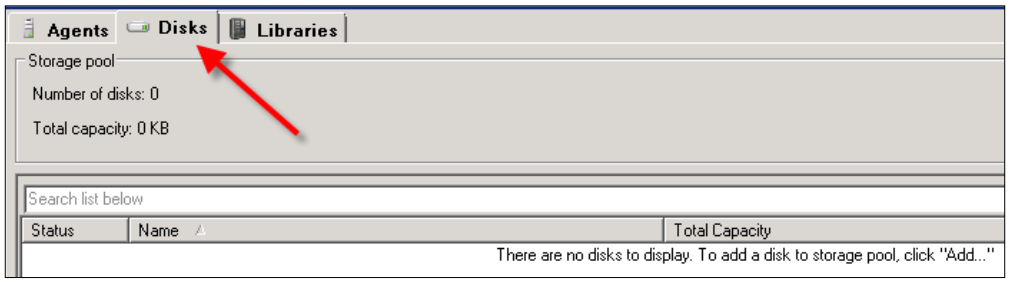
NOTE: To open the DPM Administrator Console first log onto the DPM server. Double-click the **Microsoft System Center Data Protection Manager 2010** icon on the desktop:

Alternatively you can go to the **Start** menu, select **All Programs**. Navigate to the **Microsoft System Center Data Protection Manager** folder and click **Microsoft System Center Data Protection Manager**.

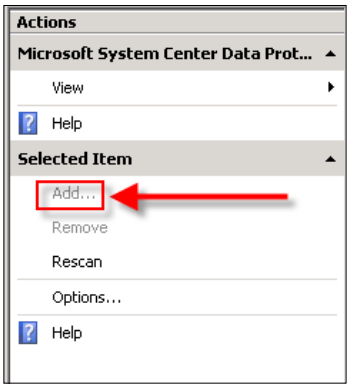
2. On the navigation bar in the Administrator Console click on **Management**:



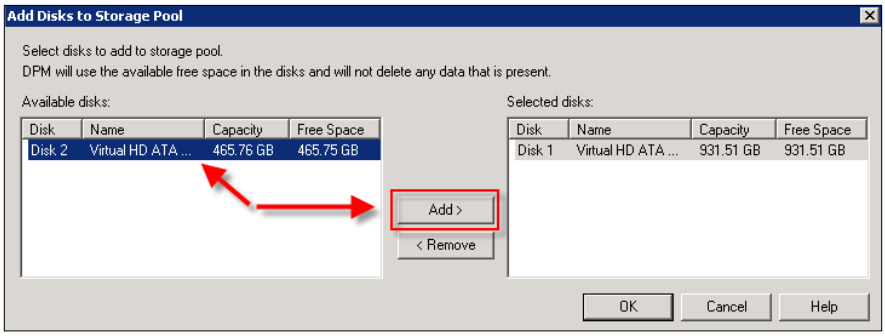
Click on the **Disks** tab:



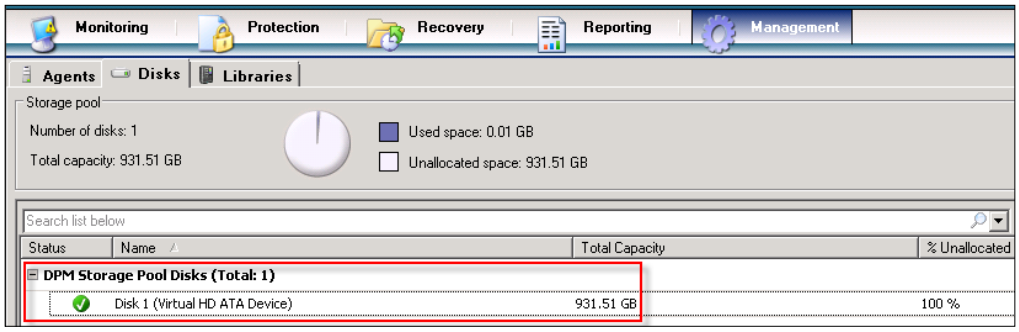
3. On the right-hand side under **Actions** click on **Add**:



4. An **Add Disks to Storage Pool** window will pop up.
5. Choose the disk(s) you want to add on the left-hand side under **Available disks**.
6. Once the disk you want is highlighted, click **Add** and the disk will be moved to the right-hand side:



7. Click **OK**. Now you will be able to see the disk you added is a part of your storage pool:



Configuring tape libraries

DPM was designed primarily to be a disk-to-disk data protection solution with backing up to tape as an alternative option. The functionality is in DPM to back up directly to tape or back up to disk first, then to tape. DPM can back up to a stand-alone tape unit or a tape library.

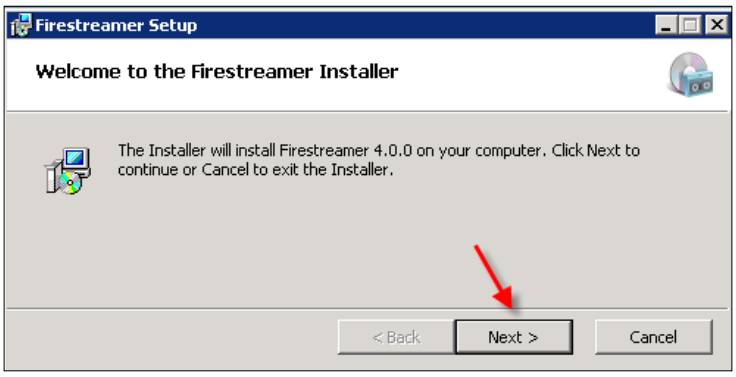
The stand-alone tape unit or tape library you will use must be attached to your DPM server. The library can be attached via a SAN (fiber) or direct SCSI. In this book we will use a stand-alone tape unit. This stand-alone tape unit is actually an external USB drive. We will learn how to use an external USB drive with DPM through a software called **Firestreamer**. To install Firestreamer on your DPM server follow these steps:

1. Download Firestreamer from the following site:

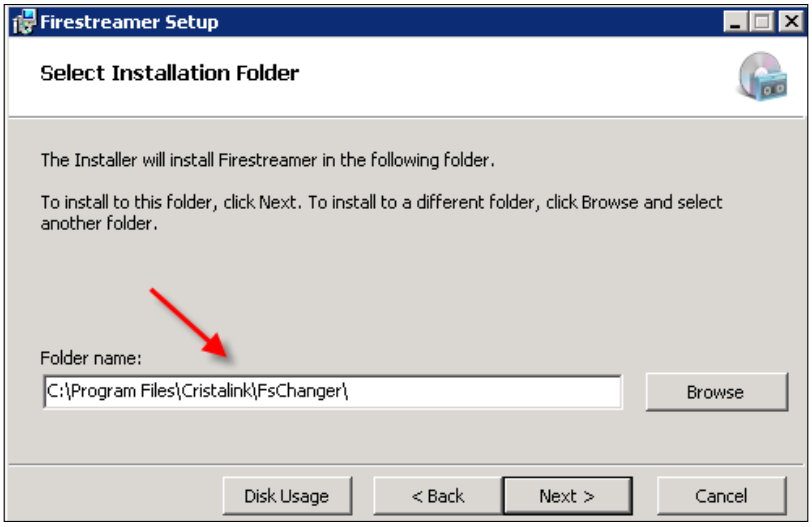
   `http://www.cristalink.com/fs/download.aspx`

NOTE: This is a 30-day trial. When it expires it will be in read-only mode so you won't be able to back up anymore to your external USB drives through DPM. You will need to purchase the software if you plan to use external USB drives.

2. Launch the Firestreamer installer.
3. Click **Next** on the welcome screen to start the installation:

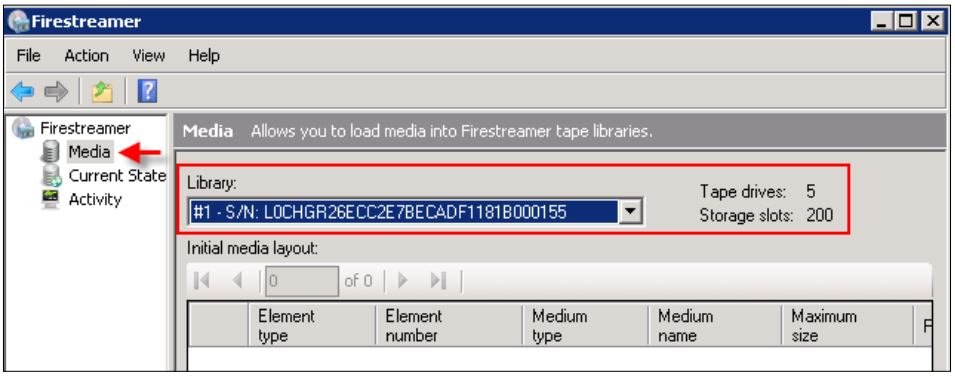


4. Accept the license agreement.
5. You can change the Firestreamer installation folder if you want to, or accept the default and click **Next** to start the installation:

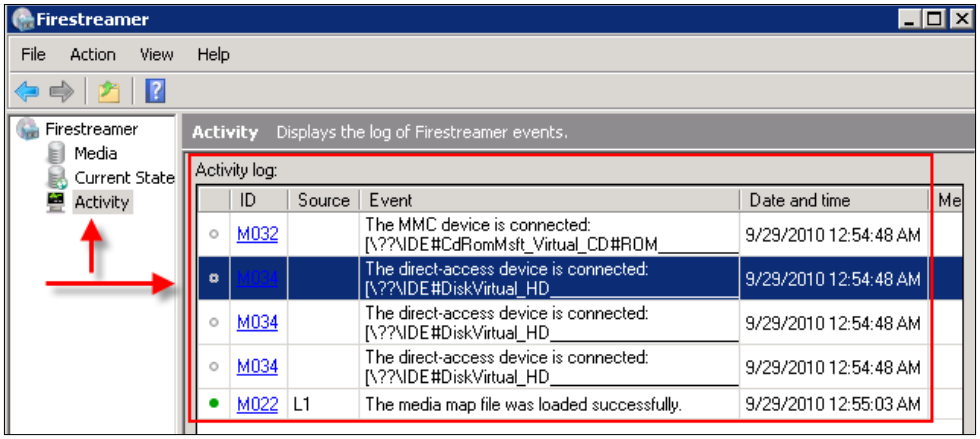


6. You will see the Firestreamer installation progress.
7. Once the installation is complete click on **Finish.**
8. Now launch Firestreamer by double-clicking the **Firestreamer** icon on the desktop:

9. On the left-hand side click on **Media.** You will see your USB external drive listed and the number of tape drives:



10. You can also click on **Activity** on the left-hand side to see when your USB drive is connected and disconnected. This can help in troubleshooting to know if Firestreamer detects your USB drive or not:



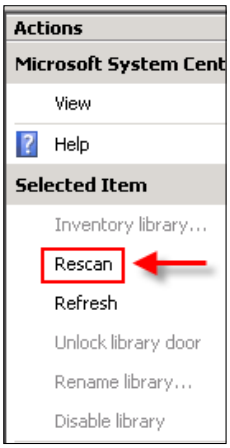
11. Now that Firestreamer is installed we will look at adding a tape library in DPM.

> **NOTE**: In this example we use a virtual hard drive instead of an external USB drive. The process would be exactly the same using an external USB drive.

Next, we will need to configure the tape libraries. In order to do so, follow these steps:

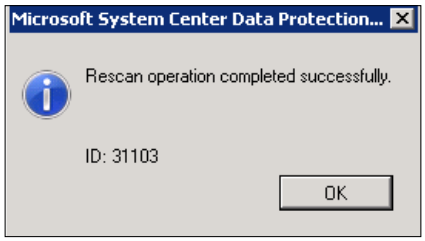
1. Open the DPM Administrator Console and click on **Management.**
2. Click **Libraries**:

3. On the right-hand side under the **Actions** pane click **Rescan**:

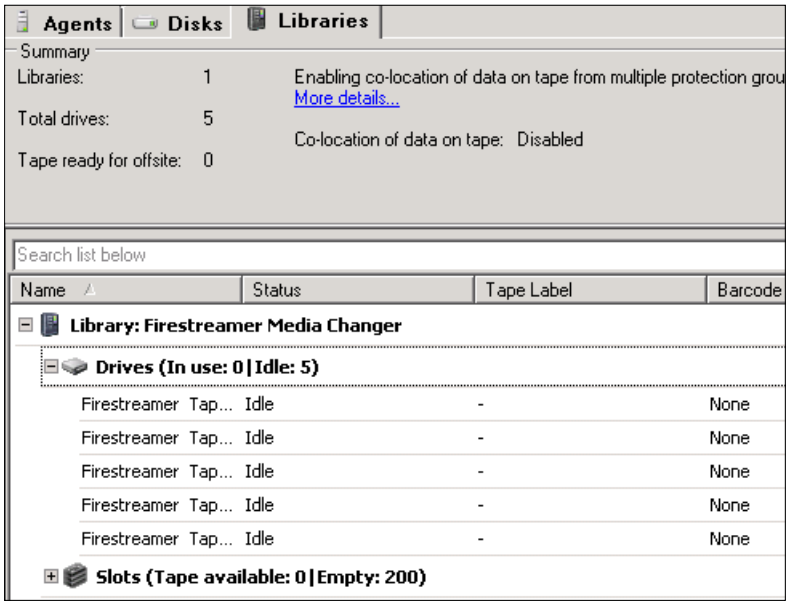


4. You will receive a popup message. Click **Yes** on it.

5. The scan process will begin. When the scan completes click **OK**:



6. Verify that Firestreamer is listed as a tape library with five tape drives and 200 slots:



That's all you need to do to add a tape library to DPM. Now you can begin backing up to your tape unit or tape library.

NOTE: We used Firestreamer in this example. If you had a tape unit or tape library it would list the brand name of your tape unit or tape library instead of Firestreamer.

The WSS Writer service

Configuring the WSS Writer is only required if you have a SharePoint deployment in your environment that you need to protect. Technically this configuration task is optional as you don't need it if you are not using SharePoint, however Microsoft lists it as a required task hence the reason this is listed in this book under required tasks. Before you can protect SharePoint farms in your environment you have to start and configure the WSS Writer service. We will cover backing up SharePoint in *Chapter 7* and you will learn how to configure the WSS Writer service at that point.

Optional configurations

Now let's talk about the optional DPM configuration tasks. Remember these are not required for DPM to function but many of them you will find useful for your specific needs. The following are guides on how to set up these configurations.

Auto Discovery

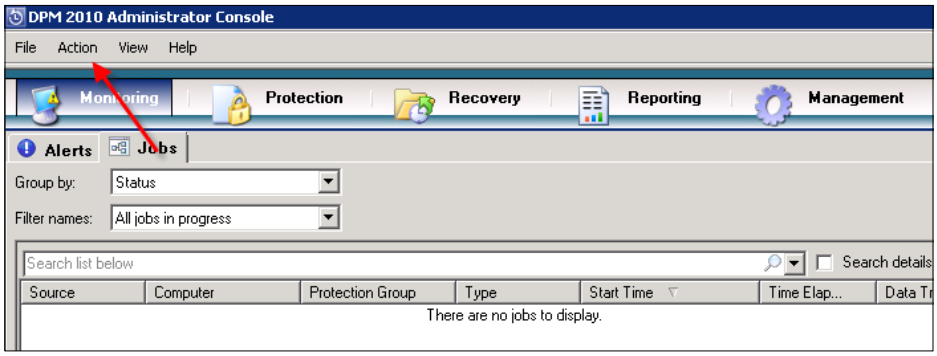
In DPM there is a function called **Auto Discovery**. Auto Discovery searches for computer additions and removals in Active Directory so a list of computers to which a DPM agent can be installed may be produced. Auto Discover does not auto install or remove agents, it simply compiles a list of computers that a DPM administrator can install an agent on. DPM communicates with the nearest domain controller through active directory LDAP queries. DPM will send a small request to Active Directory and it will respond with an update on what computers have been added and removed. These queries are small and will not hurt the network bandwidth.

This process is limited to the domain that DPM is joined to so you cannot auto discover computers across forests. By default DPM will run this process at 1 a.m. every day. We will learn how to change this time. The next time you open the DPM Protection Agent Installation wizard or go to create a new protection group for clients, DPM will list new computers that it has discovered and will not show computers that have been removed.

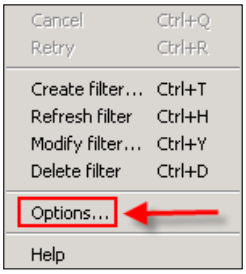
Changing the Auto Discovery time

You may want to change the default Auto Discovery time to a time that works better for you in your environment. Here are the steps on how to do this:

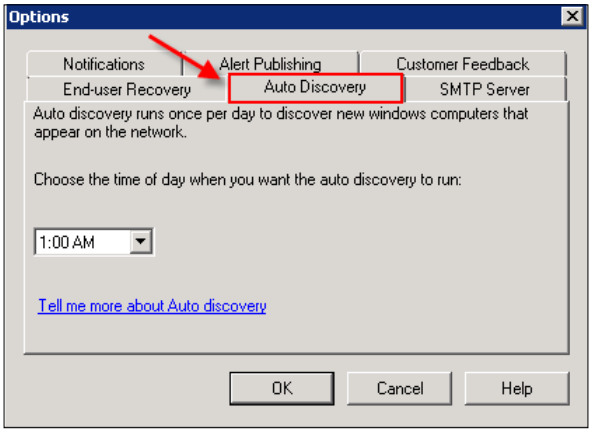
1. Open the DPM Administrator Console.



2. Go to the **Action** menu and click **Options**:



3. On the **Options** window click on the **Auto Discovery** tab:



4. Change the time of day that you want Auto Discovery to run, then click **OK** when done.

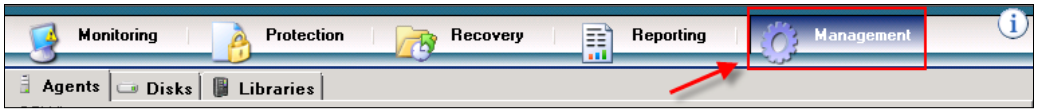
The Auto Discovery process also tracks changes on the protected servers when it runs the scheduled scan. If there are changes discovered during this process DPM will create an alert in the alert area of the Administrator Console.

Throttle

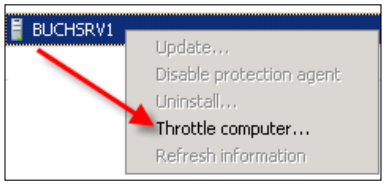
Throttling in DPM can be used to limit the bandwidth that DPM will use when synchronizing protected data. This is how you can ensure DPM does not use up too much of your network's bandwidth.

To configure throttling follow these steps:

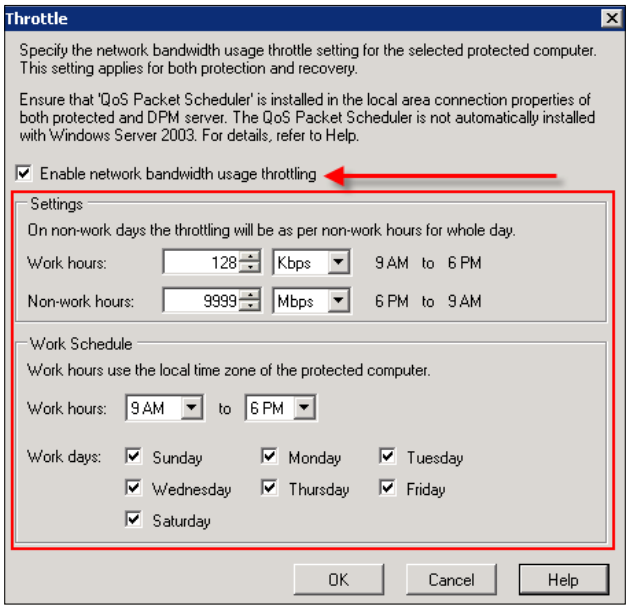
1. Open the DPM Administrator Console.
2. Click on **Management** on the navigation bar:



3. Click the **Agent Sub** tab on the left-hand side, and then highlight the computer for which you want to configure network bandwidth usage throttling.



4. Right-click on the computer you have selected and click **Throttle computer**.
5. In the **Throttle** dialog box, check **Enable network bandwidth usage throttling**:



NOTE: In the image you can set different throttling settings based on the days and the time of day. They are split into work days and non-work days. They are also split between working hours and non-working hours. This is good because you can cut back on the bandwidth DPM is allowed during business hours and days when there is heavy bandwidth use, and give DPM more bandwidth during off-peak days and hours.

6. Set the amount of bandwidth you want to allow for DPM use and then click **OK**.

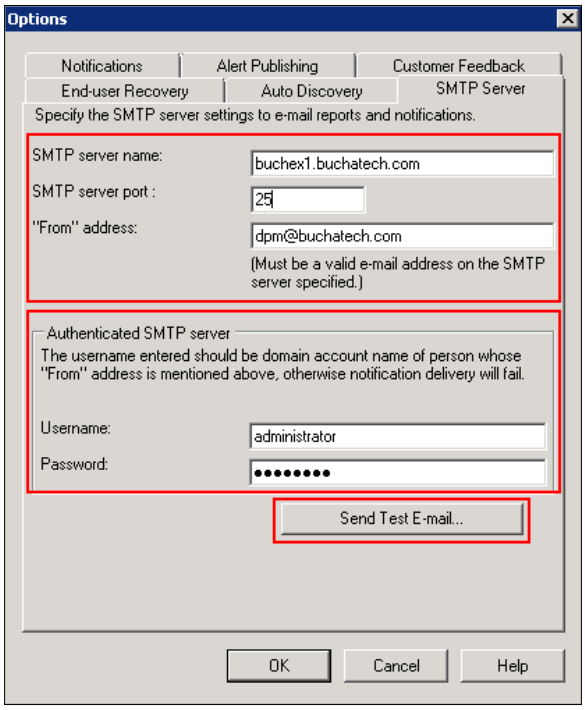
Setting up an SMTP server

This is not really about setting up an SMTP server. Microsoft refers to it that way in all the DPM documentation out there. What you really do in this section is learn how to configure DPM to use an existing SMTP server to send out e-mail for things like notifications and alerts. Typically this SMTP server will be an Exchange server or another type of e-mail server in your environment.

Configuring DPM to use your SMTP server

The following are the steps to configure SMTP settings within DPM:

1. Open the DPM Administrator Console.
2. Go to the **Action** menu and click **Options**.
3. Click on the **SMTP Server** tab:



4. Enter your SMTP server (in this book we use Exchange as our SMP server), SMTP port 25 (port 25 is default for SMTP but can differ). Enter the e-mail account reports and the notifications will appear to come from when they are e-mailed to you, and last enter an account that has access to the from e-mail account.
5. Now click on **Send Test E-mail.** A window will pop up asking you to enter the e-mail account the e-mail will be sent to.

6. A new window will pop up and tell you whether the test failed or was successful. Click **OK**.

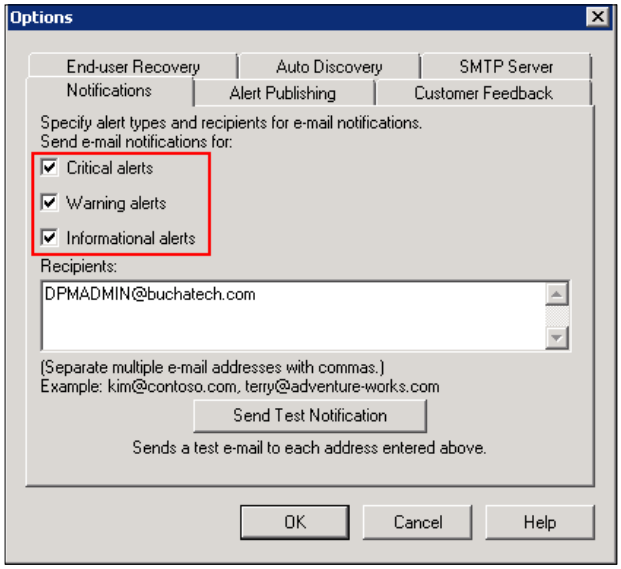
This is an example of the e-mail you will receive:

> *Receipt of this message confirms that the SMTP server settings for Data Protection Manager enable delivery of reports and notifications by e-mail. To change the SMTP settings, in the DPM Administrator Console, on the Action menu, choose Options. Then update the options on the SMTP Server tab.*

Configuring alert notifications

It is important to receive alert notifications to know if your DPM server has a problem. The following are the steps on how to configure alerts:

1. Open the DPM Administrator Console.
2. Go to the **Action** menu and click **Options**.
3. Click on the **Notifications** tab:



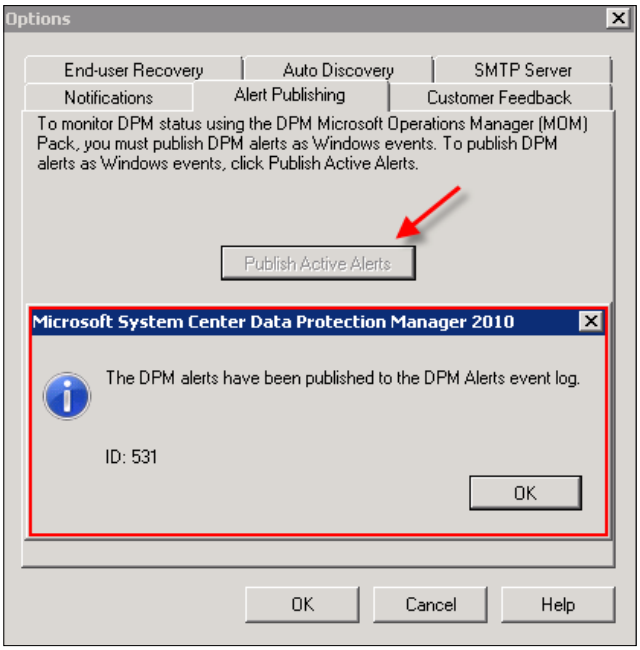
Here you can select the type of alert(s) you want to receive. For example, you can chose to get **critical** and **warning** alerts only. This would not give you informational alerts, only events that can turn into a more serious issue and actual errors. Once you select the type of alert you want to receive you will need to enter an e-mail address that should receive the alerts. This can be a single e-mail address, or several. Be sure to click on **Send Test Notification** to ensure the e-mail is working.

Publishing DPM alerts

By default DPM alerts are not published to the local server's Event Viewer. In order for **System Center Operations Manager** or **System Center Essentials** to pick up DPM alerts for monitoring these need to be published in Event Viewer.

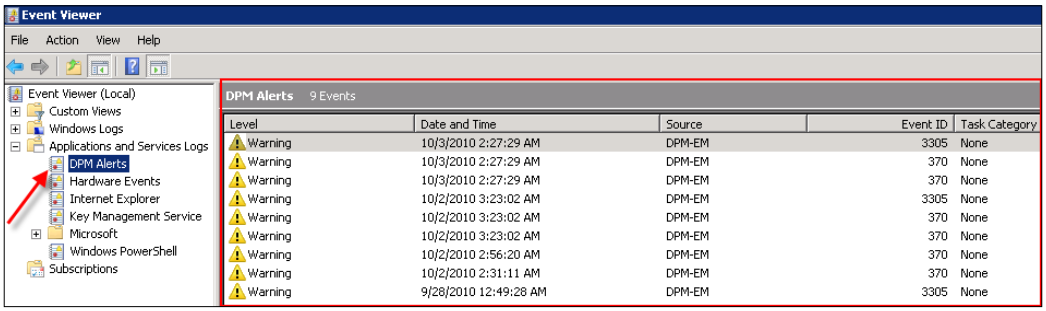
To publish DPM alerts follow these steps:

1. Open the DPM Administrator Console.
2. Go to the **Action** menu and click **Options**.
3. Click on the **Alert Publishing** tab.
4. Click **Publish Active Alerts**:



Now you can go to Event Viewer and see DPM specific alerts. To open DPM alerts in Event Viewer follow these steps:

1. Click on **Start**.
2. Click on **Administrative Tools**.
3. Click on **Event Viewer**.
4. Expand **Applications and Services Logs**.
5. Click on **DPM Alerts** (The DPM Alerts will show up in the right-hand window pane.)



To monitor DPM from SCOM (System Center Operations Manager) or SCE (System Center Essentials) you need to download a management pack on your system center server and the System Center agent needs to be installed on the DPM server. The management pack can be downloaded from the following site along with documentation:

`http://www.microsoft.com/downloads/en/details.aspx?FamilyID=32077d99-618f-43d0-843d-4ba4f8019f84`

Configuring DPM Management Shell

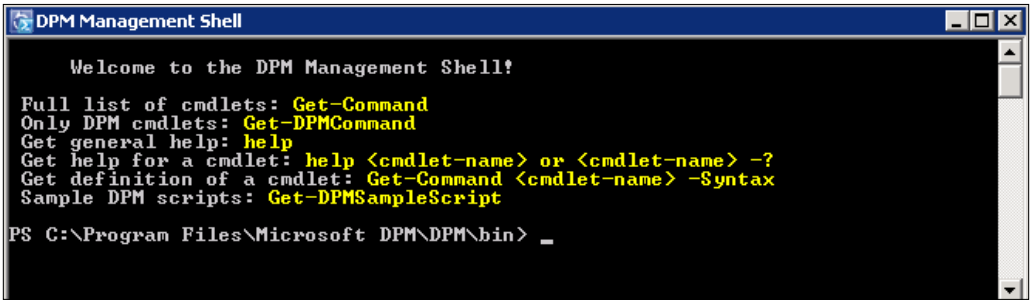
By default when you install DPM, the DPM Management Shell will be installed along with the DPM Administrator Console on your DPM server. If for some reason the DPM Management Shell is not installed you can always install it later on. It can also be installed on other computers beside the DPM server. This gives administrators the ability to manage DPM via command shell remotely. DPM Management Shell can be installed on other servers or client computers such as Windows XP, Windows Vista, and Windows 7. It is based on Windows PowerShell and contains PowerShell commands that are unique to DPM. These DPM PowerShell commands are scriptable, so administrative tasks that can be performed from the DPM Administrator Console can be performed automatically. We will cover DPM Management Shell and its commands in greater detail in *Chapter 10*.

Installing the DPM Management Shell

The following are the steps for installing DPM Management Shell just in case it was not installed when you installed your DPM server:

1. To install the DPM Management Shell on your computer, insert your DPM 2010 installation media. The DPM Setup wizard should launch automatically. If it does not then open the medium and click `Setup.exe` in the root folder to launch the installer.
2. On the DPM 2010 splash screen, click **Install DPM Management Shell**.
3. After DPM Management Shell is installed you will see the following icon on your desktop for it:

4. Click on the icon to launch the shell. This is what the shell looks like:



Configuring DPM for End-user Recovery

In this section we will learn how to get DPM ready for End-user Recovery. We will go through the steps it takes to configure the steps on the DPM server end. Enabling End-user Recovery consists of three configurations. DPM needs to be enabled for End-user Recovery, Active Directory needs to be configured, and the Shadow Copy client software needs to be installed on your end-users' computers. These need to be configured in this order:

1. Active Directory.
2. DPM.
3. Shadow Copy software.

Once the three configurations are completed, end-users can begin independently recovering previous versions of their data. When users recover their own data they are actually pulling recovery points of their data from the DPM server.

We will cover the DPM shadow copy client software in more detail when we cover End-user Recovery later in *Chapter 6*. There are a couple of things we will note here:

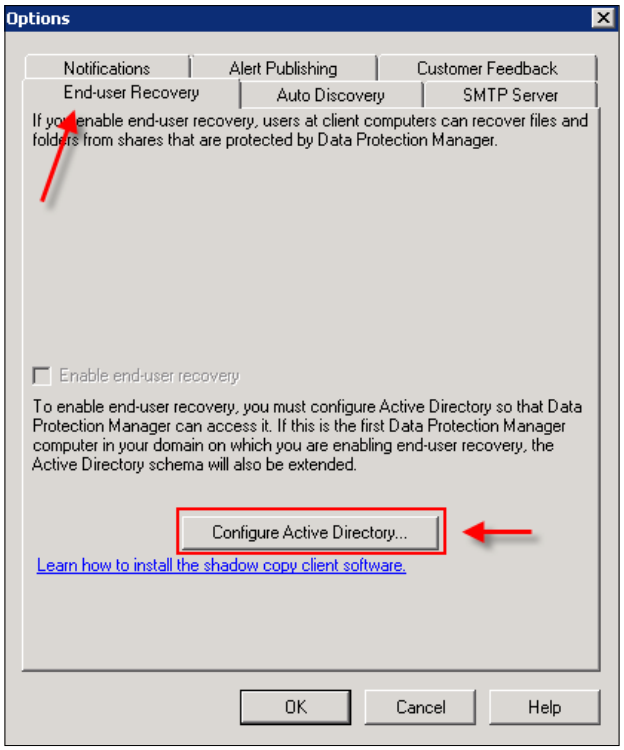
- The DPM shadow copy must be installed on all end-user computers that will be protected.
- If your client computers contain the Shadow Copy software already it must be updated to support DPM. The Shadow Copy client software is supported on Windows XP SP2 and later, as well as Server 2003 and later. If your environment consists of Windows Vista or Windows 7 clients you do not need to install the shadow client software on these computers.
- Active Directory must be configured before DPM will let you enable End-user Recovery. When you configure Active Directory what you are actually doing is extending the Active Directory schema for DPM. The Active Directory schema only needs to be extended once per DPM server you install in your environment. For example, if you have three DPM servers you will need to extend Active Directory schema a total of three times—once for each DPM server.

Configuring Active Directory and enabling End-user Recovery in DPM

Here are the step-by-step instructions to configure Active Directory and enable End-user Recovery for DPM. There are two sets of steps—one for configuring AD automatically and one for configuring AD manually:

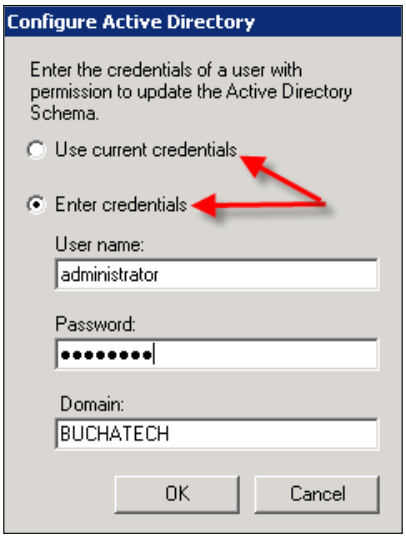
1. Log on to the DPM server with a domain account that has domain administrator and schema administrator privileges.
2. Open the DPM Administrator Console.
3. Go to the **Action** menu and click **Options.**

4. Click on the **End-user Recovery**:



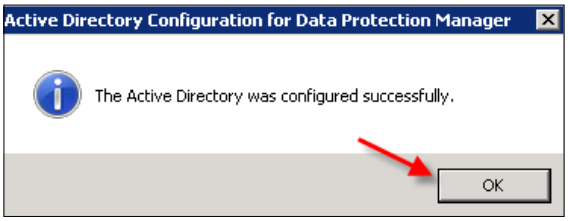
NOTE: You will notice the **Enable end-user recovery** box is grayed out so you cannot check it.

5. Click on the **Configure Active Directory** button.
6. Select **Use current credentials** or select **Enter credentials** and enter an account that has domain administrator and schema administrator privileges:

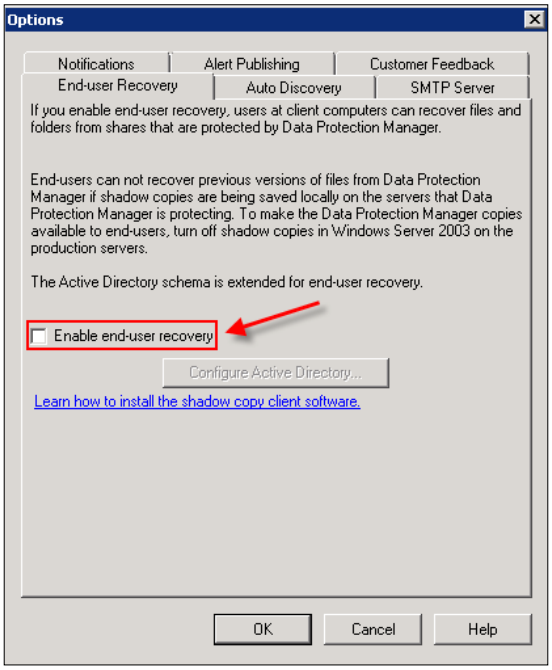


7. An informational alert will pop up letting you know your Active Directory is about to be extended. Click **Yes** to continue:

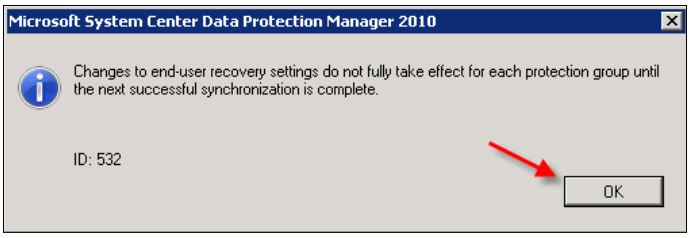
8. Another informational alert will pop up letting you know the update may take some time. Click **OK** to continue.
9. Once the configurations are complete, another window will pop up letting you know that the Active Directory was successfully updated. Click **OK**.



10. You will then go back to the DPM options window on the **End-user Recovery** tab. Notice the **Enable end-user recovery** checkbox is now available to be checked:

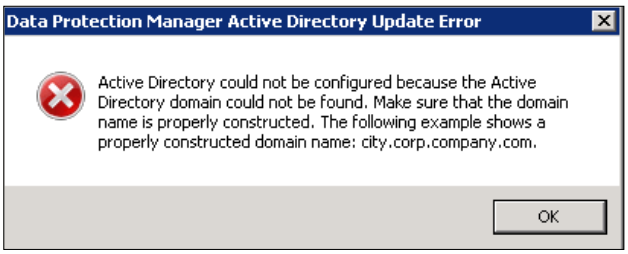


11. Check **Enable end-user recovery** and click **OK**.
12. Another window will pop up warning you that the changes do not take effect until after the next successful sync of your protection groups. Click **OK**:



Now your DPM is configured for End-user Recovery.

NOTE: The following error may pop up if your account does not have the proper permissions or the domain controller cannot be contacted:



If this error comes up, click **OK** and you will need to manually extend the Active Directory schema. The next series of steps will guide you through manually extending the Active Directory schema on the domain controller.

Manually prepare Active Directory for DPM

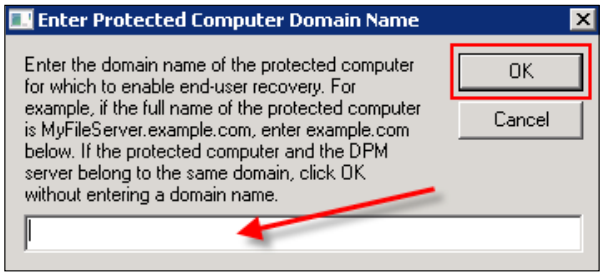
Here are the steps to manually configure Active Directory and enable End-user Recovery for DPM:

1. Log on to your domain controller.
2. Click **Start** and type in the path to your `DPM` folder on your DPM server `\\DPMSERVERNAME\c$\Program Files\Microsoft DPM\DPM\End User Recovery\`.
3. Double-click on `DPMADSchemaExtension.exe`.
4. An informational alert will pop up letting you know your Active Directory is about to be extended for DPM End-user Recovery. Click **Yes** to continue:

5. Enter your domain name in the **Enter Data Protection Manager Server Name** window and click **OK**:

NOTE: This is the dialog box that you want to enter the domain name on. This should only be the domain name. For example do not enter `BUCHDPM.BUCHATECH.com` only enter `BUCHATECH.com`.

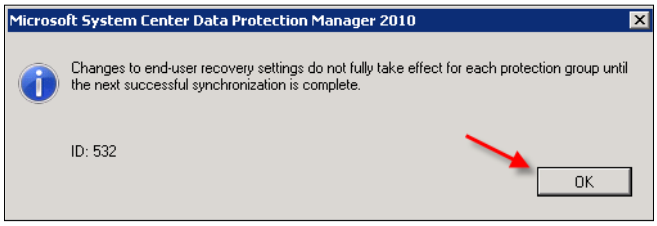
6. Leave the next field blank and click **OK**:



NOTE: You can leave this field blank as long as the DPM server and the domain controller are in the same domain. If you are on a separate domain you will need to enter the domain name that the protected servers reside on. For example, only enter `BUCHATECH.com`.

7. Another informational alert will pop up letting you know that the update may take some time. Click **OK** to continue. The window goes away and you won't see anything for a moment. All of a sudden a new window will pop up to notify that the Active Directory was successfully configured.
8. Now go back to the DPM server and open the DPM Administrator Console.
9. Go to the **Action** menu and click **Options**.
10. Click on the **End-user Recovery**.

11. You will notice the **Enable end-user recovery** checkbox is now available to be checked. Check **Enable end-user recovery** and click **OK.**



Now your DPM is configured for End-user Recovery. As stated before we will cover End-user Recovery in greater detail later in *Chapter 6*.

Summary

In this chapter we covered the areas you need to configure to get DPM up and running. This was broken down into required and optional tasks. These tasks included configuring disks in the storage pool, tape libraries, the Auto Discovery process, configuring SMTP, and configuring alerts. In the next chapter we will dig into more DPM terms the DPM Administrator Console and how to administer DPM.

5
Administration

You have made it this far getting the DPM application installed and your DPM server configured. This chapter aims to provide you with an overview as well as guidance on the day to day administration and management of DPM. We will cover important tasks that you need to know and understand to maintain your DPM server.

After you're done reading this chapter you will be able to identify the different areas of the Administrator Console, how to run reports, how to tweak DPM to get the best performance, common terms, and DPM's file structure and processes.

In this chapter, we will cover these specific areas:

- DPM structure
- DPM Administrator Console
- DPM general maintenance
- DPM reporting
- Managing DPM performance

DPM structure

In this section we will look at the DPM file structure in order to have a better understanding of where DPM stores its components. We will also look at important processes that DPM runs and what they are used for. There will be some hints and tips that you should know about that will be useful when administering DPM.

DPM file locations

It is important to know not only how DPM operates, but also to know the structure that is underneath the application. Understanding the structure of where the DPM components are will help you with administering and troubleshooting DPM if the need arises. The following are some important locations:

- The DPM database backups are stored in the following location. Also when you make backup shadow copies for the replicas these will be stored in this directory. You would make backup show copies of your replicas if you were archiving them using a third-party backup solution:

  `C:\Program Files\Microsoft DPM\DPM\Volumes\ShadowCopy\Database Backups`

- The following directory is where DPM is installed:

  `C:\Program Files\Microsoft DPM\`

- The following directory contains PowerShell scripts that come with DPM. There are many scripts that can be used for performing common DPM tasks. We will cover these scripts and PowerShell in greater detail in *Chapter 10*.

  `C:\Program Files\Microsoft DPM\DPM\bin`

- The following folder contains the database and files for SQL reporting services:

  `C:\Program Files\Microsoft DPM\SQL`

- The following directory contains the SQL DPM database. MDF and LDF files:

  `C:\Program Files\Microsoft DPM\DPM\DPMDB`

- The following directory stores shadow copy volumes that are recovery points for a data source. These essentially are the changed blocks of VSS (Volume Shadow Copy Service) (Shadow Copy).

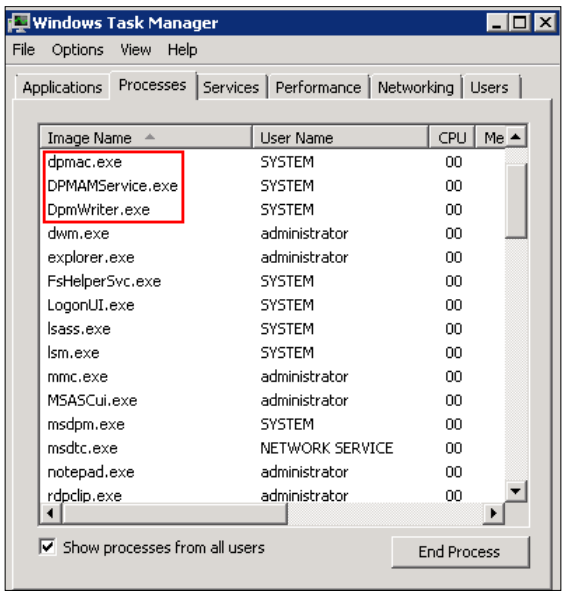
  `C:\Program Files\Microsoft DPM\DPM\Volumes\DiffArea`

- The following folder contains mounted replica volumes. Mounted replica volumes are essentially pointers for every protected data object that points to the partition in a DPM storage pool. Think of these mounted replica points as a map from DPM to the protected data on the hard drives where the actual protected data lives.

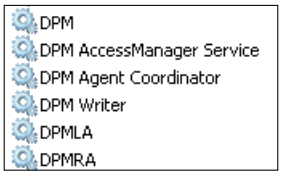
  `C:\Program Files\Microsoft DPM\DPM\Volumes\Replica`

DPM processes

We are now going to explore DPM processes. The executable files for these are all located in `C:\Program Files\Microsoft DPM\DPM\bin`. You can view these processes in Windows Task Manager and they show up in Windows Services as well:



The following screenshot shows the DPM services as they appear in Windows Services:



We will look at what each of these processes are and what they do. We will also look at the processes that have an impact on the performance of your DPM server. The processes are as follows:

- `DPMAMService.exe`: In Windows Services this is listed as the **DPM AccessManager Service**. This manages access to DPM.
- `DpmWriter.exe`: This is a service as well, so you will see it on the services list. This service is used for archiving. It manages the backup shadow copies or replicas, backups of report databases, as well as DPM backups.

- `Msdpm.exe`: The **DPM** service is the core component of DPM. The DPM service manages all core DPM operations, including replica creation, synchronization, and recovery point creation. This service implements and manages synchronization and shadow copy creation for protected file servers.
- `DPMLA.exe`: This is the **DPM Library Agent Service**.
- `DPMRA.exe`: This is the **DPM Replication Agent**. It helps to back up and recover file and application data to DPM.
- `Dpmac.exe`: This is known as the **DPM Agent Coordinator Service**. This manages the installations, uninstallations, and upgrades of DPM protection agents on remote computers that you need to protect.

DPM processes that impact DPM performance

The **Msdpm.exe**, **MsDpmProtectionAgent.exe**, **MicrosoftDPMAcct.exe**, and **mmc.exe** processes take a toll on DPM performance. `mmc.exe` is a standard Windows service. "MMC" stands for **Microsoft Management Console** application and is used to display various management plug-ins. Not all but a good amount of Microsoft server applications run in the MMC such as Exchange, ISA, IIS, System Center, and the Microsoft Server Manager. The DPM Administrator Console runs in an MMC as well. `mmc.exe` can cause high memory usage. The best way to ensure that this process does not overload your memory is to close the DPM Administrator Console when not using it.

`MsDpmProtectionAgent.exe` is the DPM Protection Agent service and affects both CPU and memory usage when DPM jobs and consistency checks are run. There is nothing you can do to get the usage down for this service. You just need to be aware of this and try not to schedule any other resource intensive applications such as antivirus scans at the same time as DPM jobs or consistency checks.

`Mspdpm.exe` is a service that runs synchronization and shadow copy creations as stated previously. Like `MsDpmProtectionAgent.exe`, `Mspdpm.exe` also affects CPU and memory usage when running synchronizations and shadow copies. Like `MsDpmProtectionAgent.exe` there is nothing you can do to the `Mspdpm.exe` service to reduce memory and CPU usage. Just make sure to keep the system clear of resource intensive applications when the `Mspdpm.exe` is running jobs. If you are running a local SQL instance for your DPM deployment you will notice a `Microsoft$DPM$Acct.exe` process. The SQL Server and SQL Agent services use a `Microsoft$DPM$Acct` account. This normally runs on a high level. This service reserves part of your system's memory for cache. If the system memory goes low, the `Microsoft$DPM$Acct.exe` process will let go of the memory cache it has reserved.

Important DPM terms

In this section you will learn some important terms used commonly in DPM. You will need to understand these terms as you begin to administer DPM on a regular basis. You can read the full list of terms at this site:

`http://technet.microsoft.com/en-us/library/bb795543.aspx`

We group the terms in a way that each group relates to an area of DPM. The following are some important terms:

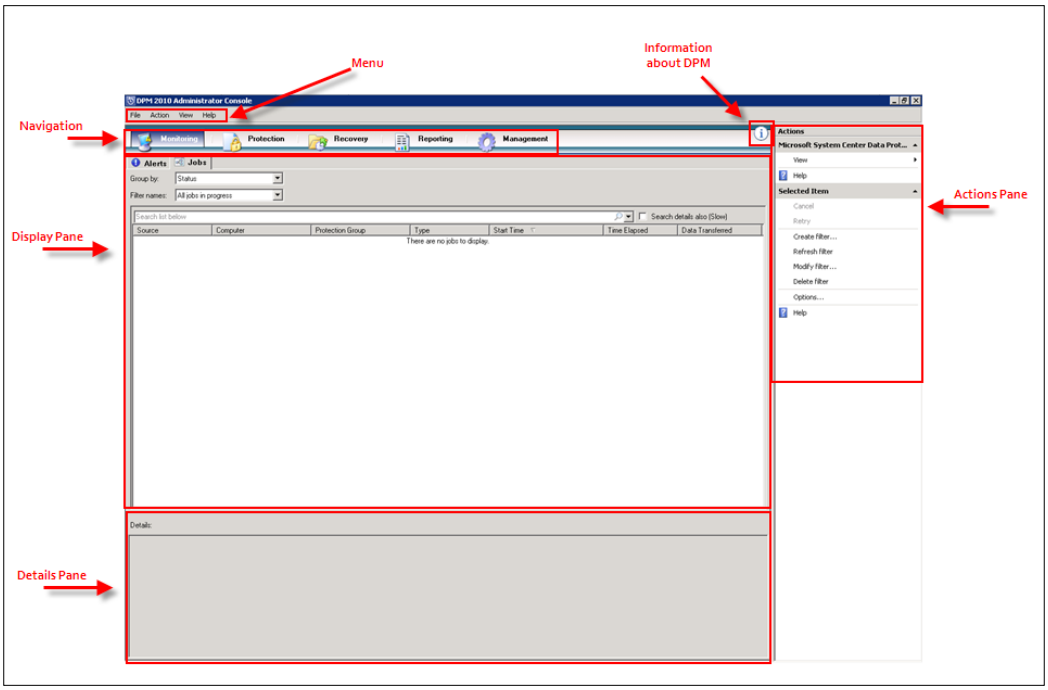
- **Bare metal recovery**: This is a restore technique that allows one to restore a complete system onto bare metal, without any requirements, to the previous hardware. This allows restoring to dissimilar hardware.
- **Change journal**: A feature that tracks changes to NTFS (New Technology File System) volumes, including additions, deletions, and modifications. The change journal exists on the volume as a sparse file. Sparse files are used to make disk space usage more efficient in NTFS. A sparse file allocates disk space only when it is needed. This allows files to be created even when there is insufficient space on a hard drive. These files contain zeroes instead of disk blocks.
- **Consistency check**: The process by which DPM checks for and corrects inconsistencies between a protected data source and its replica. A consistency check is only performed when normal mechanisms for recording changes to protected data, and for applying those changes to replicas, have been interrupted.
- **Express full backup**: A synchronization operation in which the protection agent transfers a snapshot of all the blocks that have changed since the previous express full backup (or initial replica creation, for the first express full backup).
- **Shadow copy**: A point-in-time copy of files and folders that is stored on the DPM server. Shadow copies are sometimes referred to as **snapshots**.
- **Shadow copy client software**: Client software that enables an end-user to independently recover data by retrieving a shadow copy.

- **Replica**: A complete copy of the protected data on a single volume, database, or storage group. Each member of a protection group is associated with a replica on the DPM server.
- **Replica creation**: The process by which a full copy of data sources, selected for inclusion in a protection group, is transferred to the DPM storage pool. The replica can be created over the network from data on the protected computer or from a tape backup system. Replica creation is an initialization process that is performed for each data source when the data source is added to a protection group.
- **Replica volume**: A volume on the DPM server that contains the replica for a protected data source.
- **Custom volume**: A volume that is not in the DPM storage pool and is specified to store the replica and recovery points for a protection group member.
- **Dismount**: To remove a removable tape or disc from a drive.
- **DPM Alerts log**: A log that stores DPM alerts as Windows events so that the alerts can be displayed in **Microsoft System Center Operations Manager (SCOM)**.
- **DPMDB.mdf**: The filename of the DPM database, the SQL Server database that stores DPM settings and configuration information.
- **DPMDBReaders group**: A group, created during DPM installation, that contains all accounts that have read-only access to the DPM database. The DPMReport account is a member of this group.
- **DPMReport account**: The account that the Web and NT services of SQL Server Reporting Services use to access the DPM database. This account is created when an administrator configures DPM reporting.
- **MICROSOFTDPM**: The name that the DPM setup assigns to the SQL Server instance used by DPM.
- **Microsoft$DPMWriter$ account**: The low-privilege account under which DPM runs the DPM Writer service. This account is created during the DPM installation.

- **MSDPMTrustedMachines group**: A group that contains the domain accounts for computers that are authorized to communicate with the DPM server. DPM uses this group to ensure that only computers that have the DPM protection agent installed from a specific DPM server can respond to calls from that server.
- **Protection configuration**: The collection of settings that is common to a protection group; specifically, the protection group name, disk allocations, replica creation method, and on-the-wire compression.
- **Protection group**: A collection of data sources that share the same protection configuration.
- **Protection group member**: A data source within a protection group.
- **Protected computer**: A computer that contains data sources that are protection group members.
- **Synchronization**: The process by which DPM transfers changes from the protected computer to the DPM server, and applies the changes to the replica of the protected volume.
- **Recovery goals**: The retention range, data loss tolerance, and frequency of recovery points for protected data.
- **Recovery collection**: The aggregate of all recovery jobs associated with a single recovery operation.
- **Recovery point**: The date and time of a previous version of a data source that is available for recovery from media that is managed by DPM.
- **Report database**: The SQL Server database that stores DPM reporting information (`ReportServer.mdf`).
- **ReportServer.mdf**: In DPM, the filename for the report database—a SQL Server database that stores reporting information.
- **Retention range**: Duration of time for which the data should be available for recovery.

DPM Administrator Console

In this section you will learn about the DPM Administrator Console, its layout, task areas, and functions in them. The DPM administrator interface gives you one place to access all DPM areas and functions. The DPM Administrator Console is the central tool that is used to manage the application. Knowing the DPM Administrator Console will assist you down the road when administering DPM.



Menu

The menu bar is an important part of the DPM Console and contains the following menus: **File**, **Action**, **View**, and **Help**. Now let's look at each of these four menus.

File

The **File** menu is similar to the one you would see in your standard MMC interface. The **File** menu contains **Options** and **Exit**. Selecting **Options** will allow you to run a disk clean-up of stored console changes. Selecting **Exit** from the **File** menu is one way of closing the DPM Console.

Action

The items in the **Action** option on the menu bar can also be found on the right-hand side in the **Actions Pane**. In *Chapter 4* we used the **Action** item to perform many tasks such as configuring notifications, and Auto Discovery. Those tasks as well as other tasks such as end-user recovery can all be found under **Options** item and are system wide. The **Help** item gives you a help file for DPM and MMC itself.

View

The **View** menu has a link to the DPM community website (`http://technet.microsoft.com/en-us/library/ff399133.aspx`) and gives you another way to get to the task areas.

Help

Here you will find help on DPM and on the MMC itself. You will also find a link to Microsoft's Tech Center website. The About Microsoft Data Protection Manager does not contain this version.

Navigation

The **Navigation** section contains five task areas. These areas are **Monitoring**, **Protection**, **Recovery**, **Reporting**, and **Management**. Let's break each area down in more detail so you can better understand what their functions are.

Monitoring

The **Monitoring** task area contains two tabs: **Alerts** and **Jobs.**

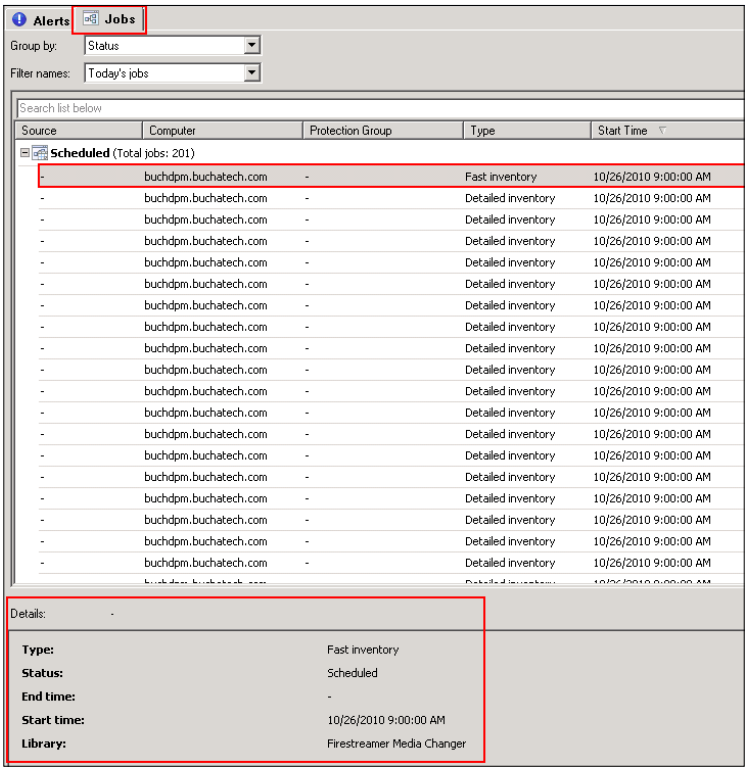
Alerts

The **Alerts** tab shows informational alerts, warnings, and errors. You have the option to show inactive or active alerts and you can group these messages in several ways by severity, protection groups, or computers. You can also choose to get notifications via e-mail when certain types of alerts occur. You learned the steps to configure e-mail notifications in *Chapter 4*. There are four types of alert levels. They are: Current problems (critical alerts), Potential problems (warning alerts), Important activity (informational alerts), and Recommended actions.

On the **Alerts** tab you have the option to manually mark an alert as inactive. You can do this by right-clicking on the alert and choosing **Inactivate alert**. Doing this will make the alert inactive and mark the protected object as **OK**. Marking an alert as inactive is a bad practice and should not be done unless absolutely necessary. This will make the error or warning go away without actually fixing the problem. By default when you fix an error or warning, the alert will automatically become inactive and the protection object will be marked as **OK**.

Jobs

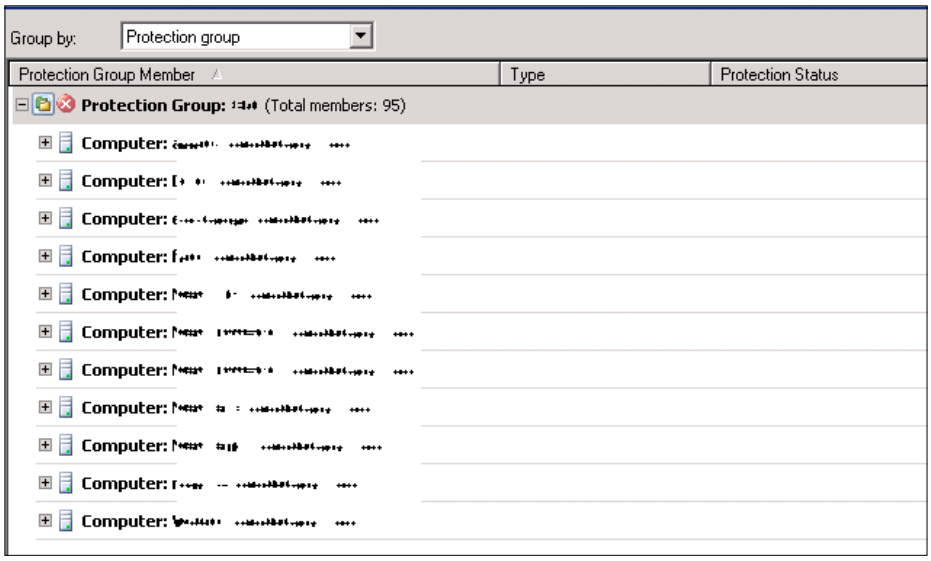
The **Jobs** task area contains all the information on your DPM jobs. This includes jobs that are currently in progress, failed jobs, scheduled jobs that will run in the future, and past jobs that were successful or failed. Within the jobs tab you can also see what jobs are running or scheduled for protected computer(s), protection group(s), how long past jobs ran for, and resources that were used for the job. On the jobs tab you can right-click on any running or scheduled job and chose cancel to stop the job from running. If a job fails and you want to know why it failed, you can click on that job and in the **Details** screen you will see more information about why this job failed. You can also filter the list of jobs that are displayed. You can filter on these various options: job status, job, protection group, or computer.



Protection

This area is used to manage your protection groups. Protection groups are protected computers that are grouped together. This area gives you a view of all your protection groups at once. You can expand each protection group to see its protection members. We will cover creating a protection group in *Chapter 6* as we start protection of a file server. You use this area to create protection groups, rename them, adjust protection group schedules, and adjust disk allocation sizes.

You can also run manual synchronizations and consistency checks from here. This is helpful if a protection member becomes inconsistent.

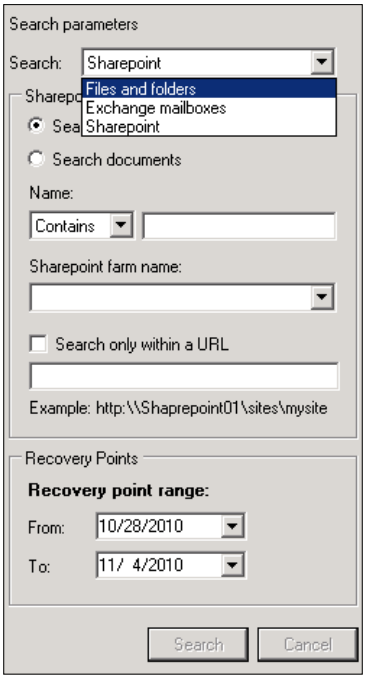


Recovery

The **Recovery** area is the place you go to get your data back. You have two options here:

- The first one is to browse through based on protection groups and the day and time you want to recover from. You can drill down to the folder and file level. We will cover recovering data from DPM later in *Chapter 8*.

- The second option you have is to search for data you want to recover. This comes in handy if a user wants some data back and he or she knows the name of the data but not what server it was on. This option enables you to search for the data without knowing the server it was on. You have several parameters you can set to help narrow down your searches. You will see in the following image the parameters you are able to set:



Reporting

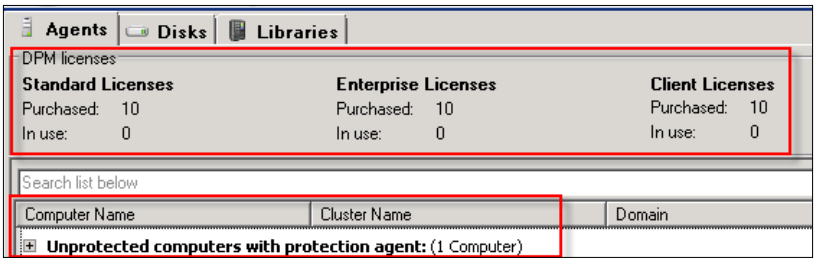
The **Reporting** task area is pretty straightforward. You use this area to manage Reporting Services settings, generate schedules, and view your DPM reports. We will cover how to do report tasks later in this chapter.

NOTE: Once you start protecting data it still takes up to at least 24 hours before you can get reports from DPM that contain data. DPM needs time to populate data for the reports.

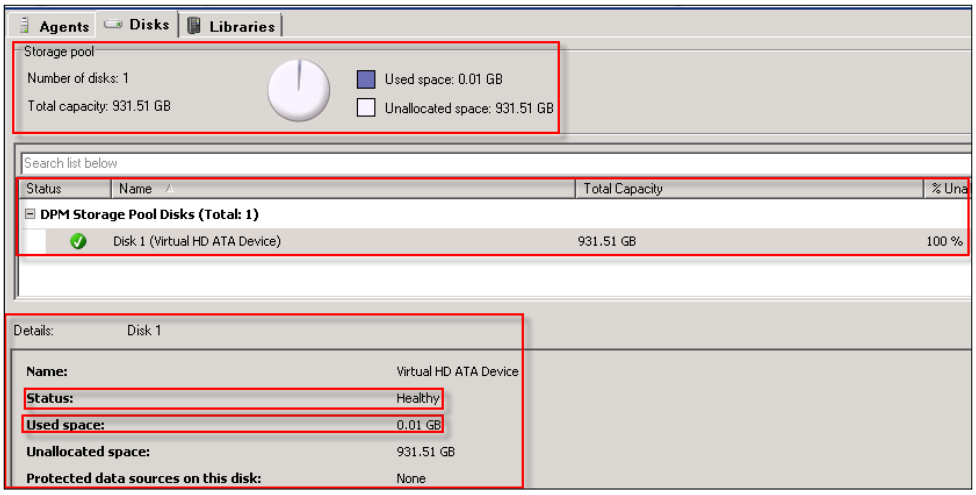
Management

The **Management** area is where you manage storage pools, tape libraries, and your protection agents. This is where you can add or remove protection agents, disks to your storage pool, and tapes or tape libraries.

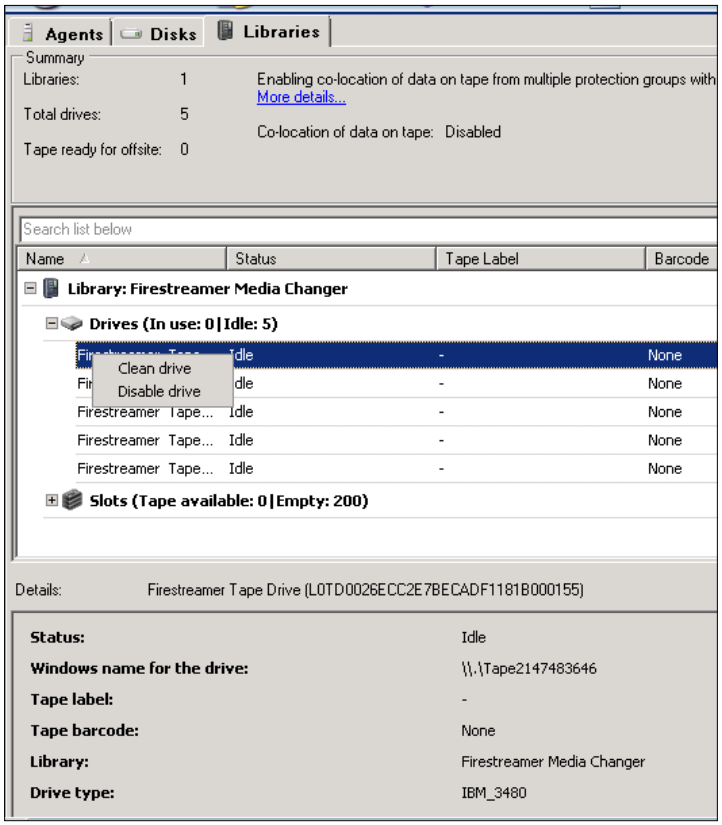
You have three tabs in **Management**. These three tabs are **Agents**, **Disks**, and **Libraries**. Under the **Agents** tab you can install and remove agents on computers that you want to protect. On the **Agents** tab you can also see a list of computers that you are currently protecting. On this **Agents** tab you will also notice that you can see what type and how many DPM licenses you currently have. Note that this information is only as accurate as the person entering the license information:



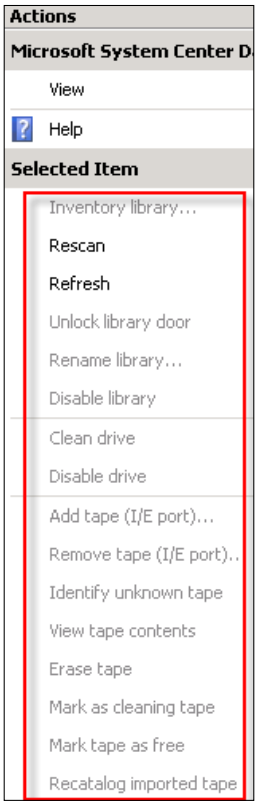
On the **Disks** tab you can add and remove disks from your DPM storage pool. You can also see what disks are currently added and how much of the disks are used up. When you click on a disk in the display pane, more information is shown in the **Details** pane about the disk such as state of health and what data is being protected on a particular disk. This is very helpful when trying to figure out what data is on what disk in your DPM storage pool.



The **Libraries** tab is similar to the **Disk** tab in what it shows you and what you can do, except this is for tapes. This allows you to see tape libraries or single tape units. It lets you see what tapes are available and allows you to rescan the tapes. You can also clean drives and disable them by right-clicking on one of them.



Keep an eye on the options on the **Action** pane on the right side of the window when in the **Libraries** tab. There are many options for managing your tape library or tape unit.

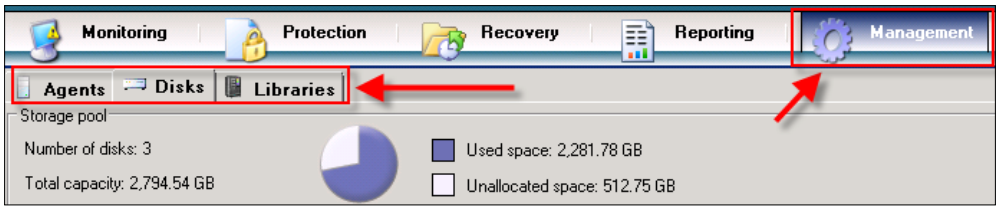


Display pane

The display pane shows you information that pertains to the task area you are currently in. For example, if you are in the **Protection** area you will see protection groups and the data you can restore from. If you are in the **Reporting** area you will see the different reports that you can work with. Each task area may look different in the display pane. For example, the **Recovery** tab will only have two tabs while the **Management** tab will have several tabs to choose from in the display pane.

The following image shows the **Recovery** tab:

This image shows the **Management** tab:

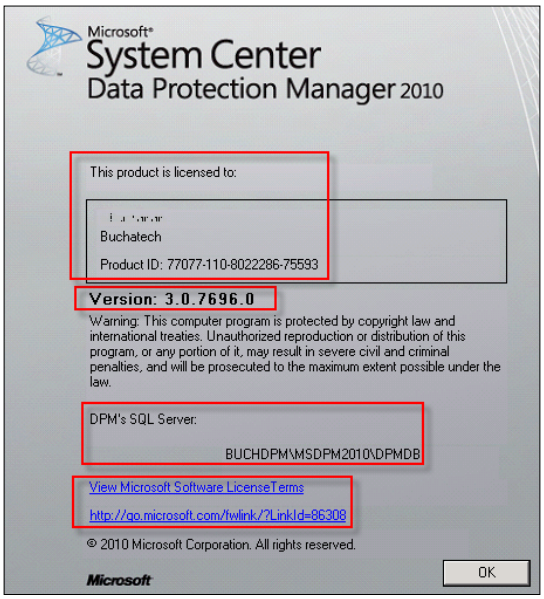


Details pane

The **Details** pane ties into the display pane. When you select an item in the display pane, details about the selected object will show up in the details pane. For example, if you were in the **Protection** area and selected a protection group in the display pane, detailed information such as the status, properties and other important information will show in the **Details** pane.

Information icon

When you click on the information icon you will get a popup that gives you the product ID, DPM version, the SQL instance that the DPM database is on, as well as a link to Microsoft Software License Terms and to the System Center Data Protection Manager Community website.



Actions pane

The **Action** pane gives you certain tasks you can do that relate to the current task area you have selected. For example, if you were in the **Reporting** area you will notice on the **Actions** pane you have the options to select **View** or **Schedule**. This will change with every task area. Basically it is another way of doing things with the task areas in DPM.

DPM general maintenance

There are many things that will come up when maintaining a DPM server. We will cover some best practices in regards to maintenance.

Restarting the DPM server

When the time comes for you to restart your DPM server, you should check a few things first to make sure you don't cause any issues with DPM. You should check the monitoring task area in DPM for jobs that are running and take note of scheduled jobs.

You don't want to restart the DPM server if a scheduled job is about to kick off during the restart time. If there is a shadow copy creation or replica creation job that is scheduled to start you will want to postpone your restart until after these jobs finish. If a restart happens during the shadow copy creation or replica creation you will need to perform manual tasks to correct these jobs. You will need to run a synchronization with a consistency check for the replica creation and run a synchronization and create a shadow copy for the create shadow copies job. The best practice is to not restart your DPM server often and if you need to, be sure no DPM related tasks are running or scheduled.

Running antivirus on a DPM server

We first discussed running antivirus software on a DPM server in *Chapter 2*. Let's touch on this briefly again here as it is important to understand that this can cause DPM to perform poorly if not set up correctly.

Disable the antivirus software real-time monitoring of `csc.exe` and `dpmra.exe` on your DPM server. The reasons why we want to disable scanning of these two processes are covered in more detail in *Chapter 2*, so refer to it if you want more information on these processes. Additionally the antivirus to add is the antivirus software scanning of the `\XSD` and `\Temp\MTA` directories should also be disabled. Doing this will prevent file conflicts between DPM and antivirus programs.

The last thing to remember when it comes to antivirus software on your DPM server, is to always set your antivirus software to delete infected files rather than cleaning or quarantining them. Deleting infected files will ensure that DPM does not throw errors for corrupted data. If you would like more information on this please refer back to *Chapter 2*.

Disk Defragmenter and Check Disk

Do not run Disk Defragmenter on any disks that are members of a DPM storage pool. Defragmenting a disk in a DPM storage pool could cause shadow copies to be lost. You would not want to run Check Disk either. Running Check Disk on DPM recovery point and replica volumes will cause the volumes to dismount and cause loss of recovery points. Also Disk Cleanup is not available to disks or volumes in DPM storage pools. DPM typically does its own management of disks and there are some manual operations you can perform to clean up your DPM disks. The manual tasks are done via PowerShell and we will cover this later in *Chapter 10*.

Windows update on a DPM server

As we know in system administration, it is important to keep our servers patched and updated. The same is true for your DPM server. The best practice is to use Windows updates for your DPM updates. These updates will be applied along with your standard server OS updates. This will save you time applying the DPM updates at the same time. There is one exception to receiving all your updates for DPM through Windows updates. The exception is when you need to install full DPM service packs. DPM service packs should typically be downloaded and installed separately. These typically contain several patches and fixes. You will want to fully understand the effects this may have on your DPM server.

Moving DPM to a different SQL instance

It is always the best practice to decide on where you are going to store the DPM database before your DPM installation. You need to choose between using a local or remote SQL instance. However the need may arise to move your DPM database to another SQL instance. Moving the DPM SQL database is possible. You need to use the **DpmSync** tool to perform this task. The following steps show how to move a DPM database to a different SQL instance:

1. First, stop the DPM to ensure no DPM jobs are running. You can ensure this by stopping the DPM service (`Msdpm.exe`) on your DPM server.

2. Perform a standard SQL back up of the DPM database through SQL Management studio. You want a full backup and should end up with a `.bak` file when done.
3. Uninstall the DPM application and choose **retain data** during the uninstallation process.
4. Restart your DPM server.
5. Install DPM again and choose the SQL instance you want to install the DPM database on. Remember if you are moving away from a remote SQL instance to a local SQL instance, SQL server will be installed on the DPM server.
6. When the installation is finished, stop the DPM again by stopping the DPM service (`Msdpm.exe`).
7. Now you need to use the `DpmSync` tool to restore the DPM database that you backed up. You also need to synchronize the DPM database backup after it is restored.
8. Run this command to restore the DPM database:

```
DpmSync -RestoreDb -DbLocYOURBACKUPPATH:\DPMDB.bak.
```

9. Run this command to synchronize the DPM database:

```
DpmSync -RestoreDb -DbLoc location -INSTANCENAME SEVERNAME\
INSTANCENAME
```

Adding disks to the storage pool

For more information on adding disks to your DPM storage pool refer to *Chapter 4*.

Removing and replacing a disk in the storage pool

To replace a disk in a DPM storage pool you need to perform the following steps:

1. Locate the disks/volumes that contain the replicas.
2. Remove the protected data from the DPM.
3. Now go to the **Management** task area and then select the **Disks** tab.

4. Chose the disk you need to remove, right-click on this and select **Remove**.

5. Remove the physical disk and install the new physical disk.
6. Once the new disk is installed go back to DPM Management and add the new disk to your storage pool. If you need the steps for this again please refer to *Chapter 4*.

NOTE: Neither moving a DPM to a new domain nor renaming a DPM server should ever be done; this is not supported by Microsoft.

DPM reporting

Reporting is important when it comes to back ups. It is useful to know how your backup environment is doing because back ups are critical to business continuity. We are going to look at DPM reporting in this section.

Monitoring with reports and alert notifications

The purpose of DPM reporting is to provide backup administrators with a way to pull reports on a DPM server. This helps an administrator know the health of their DPM environment.

DPM has both new and historical reporting. New reports are current reports that you can pull on the fly. Historical reports are reports that are scheduled to run at a later time. DPM reports are generated by SQL Reporting Services. SQL Reporting Services is also the tool that collects the data for the reports. This is why SQL reporting is required as a part of the DPM installation. There are several types of DPM reports that you can view to gain an understanding of what's going on with your DPM environment.

The following is a list of the DPM report types and what they are used for:

- **Disk utilization report**: This provides an overview of your disk capacity, allocation, and usage of disk space in the DPM storage pool.

- **Recovery report**: This report type contains the history of all recoveries that were initiated by an administrator. This displays the time it has taken for restores to complete and the average size of the recoveries over a period of time.
- **Recovery point status report**: This is the report you would use to see if you are meeting your backup SLAs. This report is generated on the currently selected data sources.
- **Status report**: The status report basically gives you an overview of your backup and overall recovery health for the entire system. It gives you the total number of successes and failures for all recovery points for a specified period. It also gives you the status of disk-based and tape-based recovery points.
- **Tape management report**: This report is for tape libraries only. This will assist you in tape rotation. It lets you know which libraries are below the free tape threshold.
- **Tape utilization report**: This report will give you an overview of your tape utilization. The idea is to use this report to help in planning for capacity and growth. This report can help when making decisions about adding more tapes or not and when this is needed.

Displaying reports in DPM

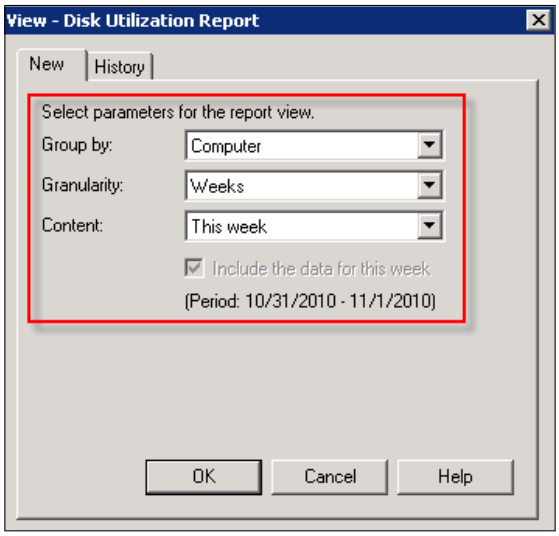
All DPM reports can be displayed in Internet Explorer. You can then print the report from Internet Explorer. Here is how you open up a report:

NOTE: In your environment a need may arise for custom DPM reports that contain data that you cannot get from the default reports in DPM. You can create custom reports in DPM using SQL Reporting Services and the DPM data directly from the SQL database. I have detailed out this process step-by-step on my blog. You can view the article here:

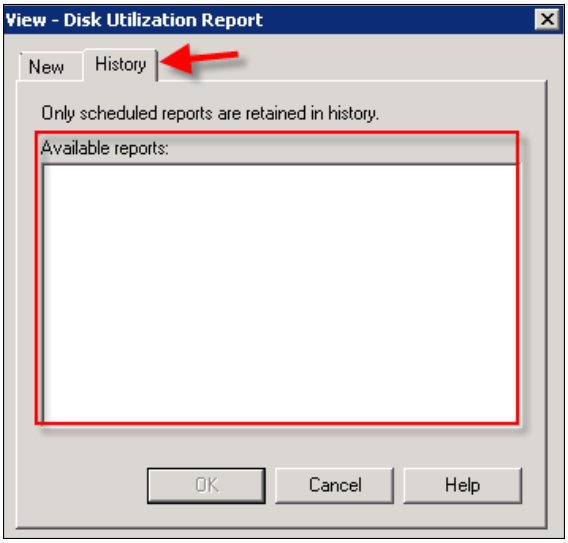
`http://www.buchatech.com/2011/01/building-custom-reports-in-dpm/`

1. Go to the DPM Administrator Console and click on **Reporting**. This will bring you to the reporting area.
2. Either double-click, or right-click and select **View** on the report you want to see.

3. A window will popup on the new report tab. Here you can group by protected computers or protection groups. You then have the option to select a unit of time (Week, Month, Quarter, or Year). The last option you have is to select the time period for the report under the content field.



4. Click **OK** and your report will be generated and displayed in Internet Explorer.



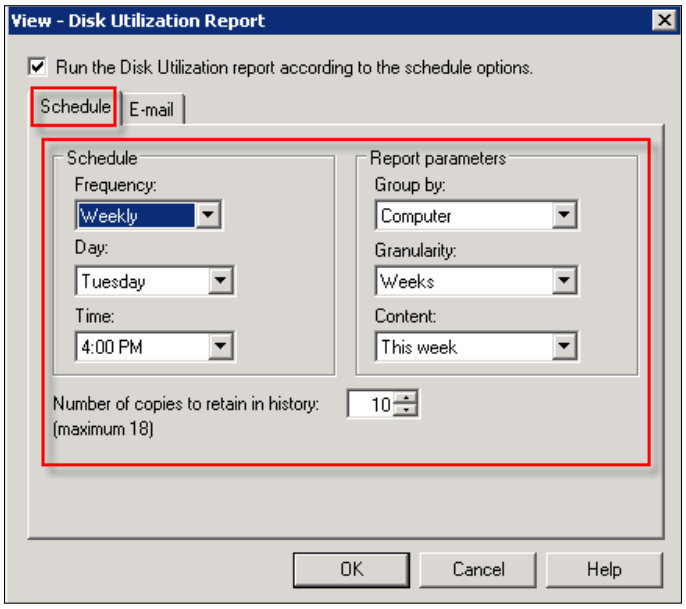
Notice when you selected to view the report it had an option to select a historical report by clicking on the **History** tab.

On this tab only DPM reports that have been scheduled will be displayed.

Now let's look at how to schedule a report and generate a report notification in DPM. To schedule reports follow these steps:

1. From the DPM Administrator Console click on **Reporting**. This will bring you to the reporting area.
2. Right-click on the type of report you want to schedule and select **Schedule** from the listed options.
3. Now, set your **Schedule**, **Report parameters**, and the amount of copies DPM is to retain.

NOTE: You can only retain up to 18 copies of a scheduled report. These retained reports can be accessed at a later time.



4. Once you are done, click on the **E-mail** tab. This is where you set the recipients you want to be e-mailed every time the report is generated.
5. You can choose the report format that will be e-mailed to you to be in HTML, PDF, or Excel. Click **OK** when you are done to set the schedule.

Managing DPM performance

Here we are going to walk through the different things you can modify to improve the performance of DPM and also things to look out for that could degrade DPM performance.

The pagefile on DPM

The pagefile is important for DPM and the servers it protects. If the pagefile is set up incorrectly it can have a bad effect in your DPM deployment.

On the DPM server you want to set the system pagefile size to 1.5 times the amount of RAM in the server. You then want to increase the pagefile size to 0.2% the size of your recovery volumes combined. If your DPM has 2 GB of RAM you will set the pagefile size to 3.5 GB. That meets the 1.5 times rule. To meet the increase 0.2% rule on a recovery volume total 4 TB size combination, your pagefile would need to be increased by another 8 GB. Make sure you have enough hard drive space on your main drives hard drive. On your protected servers you will want to set their pagefile sizes to two times the amount of RAM in the server. DPM needs this to properly back them up.

To set your pagefile size follow these steps:

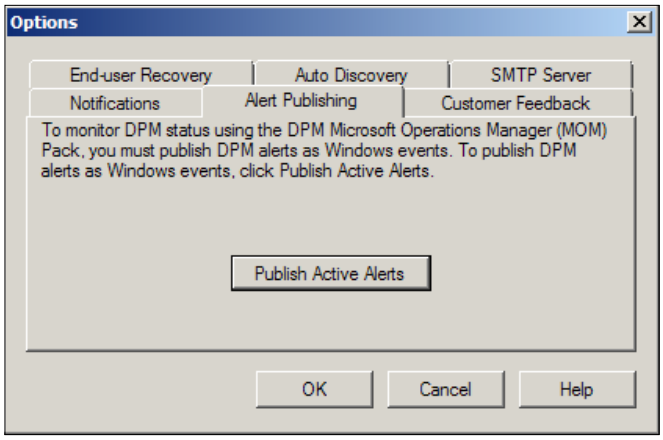
1. From the windows **Run** box or command prompt, type **SystemPropertiesAdvanced.exe**, and you will be directed to the **Advanced System Settings** on the **Advanced** tab.
2. Go ahead and click the **Settings** button under the **Performance** section. Here is where you can set your Windows pagefile.

DPM performance monitors

You can use the built in Windows performance monitor for monitoring you're DPM server, or you can use the DPM management pack in System Center Operations Manager (SCOM) to monitor DPM. SCOM is another product in the System Center suite of products and is the perfect tool to use for monitoring DPM servers. SCOM monitors the health status of DPM. It will alert the backup administrator if there is any health alerts. The alerts also provide potential fixes to problems. Although DPM does have its own monitoring and reporting mechanisms, these are on a per DPM server basis, whereas using SCOM provides central monitoring solution.

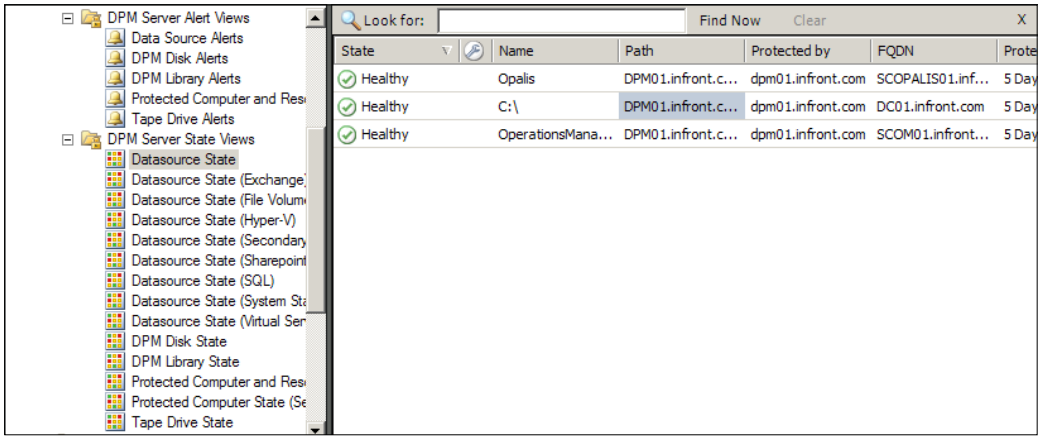
To enable monitoring of DPM in SCOM, the DPM management pack is required, and this can be obtained at `http://www.microsoft.com/downloads/en/details.aspx?FamilyID=32077d99-618f-43d0-843d-4ba4f8019f84&displaylang=en`. Once this management pack is imported into SCOM and an agent has been deployed to the DPM servers, all the DPM servers will be discovered. SCOM will automatically start monitoring the DPM servers after they have been discovered. However, a number of DPM monitors rely on events being published to the DPM Alerts log on the DPM servers. This is not enabled by default, but can easily be switched on within the DPM Administrator Console by following the steps below:

1. Open the DPM Administrator Console and select **Management**.
2. From the **Actions** menu, select **Options**.
3. Select the **Alert Publishing** tab and click **Publish Active Alerts**.



With the management pack imported in SCOM and alerts published in DPM, monitoring in SCOM is now enabled.

The DPM management pack provides monitoring of the DPM server, the storage, the tape library, and all of the data sources being protected. Using the state views provided, it is easy to view the current state of all DPM servers and the current state of all data sources being protected. The following figure shows the datasource state view:



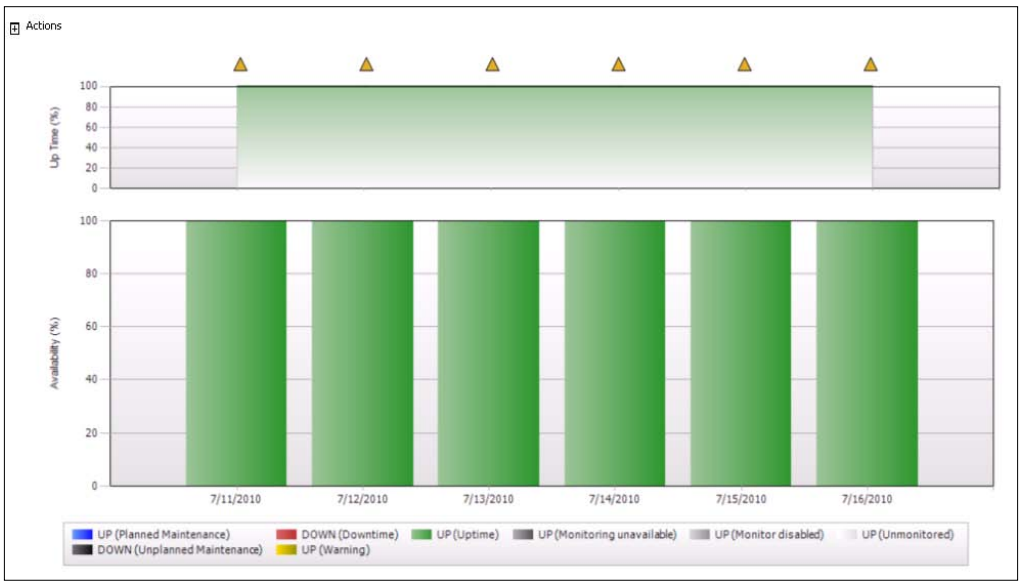
Contained in this datasource state view are all the datasource objects from all the DPM servers being monitored. The state of each datasource is determined by a number of monitors that run against each object. There are over 31 monitors that run for each object to make sure that the protection being provided by DPM is accurately reflected in SCOM. There are also state views for the DPM server, DPM Disk State, Tape Drive State, and Protected Computer.

Also included in the management pack are a number of alert views. These views are useful as they will display alerts for all monitored DPM servers. To further assist with managing DPM servers from SCOM, there are a number of tasks that can be performed. These include the following:

- Creating a recovery point
- Running a consistency check
- Running Synchronization
- Starting the DPM Service
- Stopping the DPM Service
- Pinging the DPM server

These tasks can be used to assist in both troubleshooting and resolving a DPM issue without the need to connect to a DPM server. All these tasks are very useful if you are managing more than one DPM server.

There are no reports included with the DPM management pack; however the Generic Report Library provided with SCOM can be used to produce reports based on the state data being collected. Every datasource is represented as a monitored object in SCOM, and every monitored object has a state. This means that a generic availability report can be run against these objects to provide a report on how successful DPM protection has been. This is extremely useful if there is more than one DPM server as a separate report does not need to be run at each DPM server. The following figure shows an example of an availability report for DPM datasources:



The DPM management pack may also be configured for SLA-based or Ticket System-based monitoring. Re-configuring this management pack for these is not covered in this book; however more information is available at:

`http://blogs.technet.com/b/jonathanalmquist/archive/2010/10/21/data-protection-manager-2010-management-pack-just-released-things-you-need-to-know.aspx`

Performance counters

There are several performance counters you can monitor using the standard Windows Performance Monitor. This comes with every version of Windows. To open the Windows Performance tool:

1. Click **Start**.
2. Go to **Administrative Tools**.
3. Next click on **Performance**.

For information on how to create and monitor objects go to: `http://go.microsoft.com/fwlink/?LinkId=47881`. The objects you will want to monitor on your DPM server(s) are as follows.

Processor usage

If your processor usage stays above 95% for long periods of time this means your processor is overworked and there is some issue.

Some potential issues could be that DPM jobs are synchronizing at the same time and they are processor intensive. Make sure you DPM processor is equipped to handle the workloads. Compression on the wire for DPM has been enabled on protection members. This improves network performance but can increase processor usage.

Disk queue length

If you have more than 80 requests for long periods of time this is typically over six minutes. A potential cause is again that multiple DPM jobs running can cause high disk usage. Be sure the disks you are using in DPM can handle the current workloads.

Memory usage

If your available memory is low—less than 50 MB—this is a big problem. Potential issues could be that other applications on the DPM server are using large amounts of memory, or multiple DPM jobs are running that use large amounts of memory. Make sure you meet the 4 GB minimum DPM memory requirements. Remember it is recommended that you have at least 8 GB of RAM for your DPM server. The full list of hardware requirements can be found here:

`http://technet.microsoft.com/en-us/library/ff399280.aspx`

Ways to improve performance

Make sure you meet DPM hardware requirements for memory, processor, and hard drive types. It is recommended to go above the DPM requirements when choosing hardware. Also do not run unnecessary applications on your DPM server. Remember that DPM is to be run on a stand-alone server and should not have other Windows server roles running on it. Another way you can improve performance of your DPM server is to make changes to the DPM server workload. You can additionally change the synchronization and consistency checks so that they occur during off-peak hours and the start times are staggered so they do not start at the same time. Configure network bandwidth throttling of your protection groups. Enable on-the-wire compression. If you are running a local SQL instance move the DPM database to a remote SQL instance.

Summary

This chapter covered topics related to administration and management of DPM. By now you should have understood the DPM file structure, the processes involved and how they affect DPM performance. The DPM Administrator Console is the central tool that is used to manage applications. DPM has both new and historical reporting. It helps you monitor the system with reports and alert notifications. You can use the built-in Windows performance monitor to monitor your DPM server, or even use the DPM management pack in System Center Operations Manager to monitor DPM. Through *Chapter 6* you will begin to learn how to protect servers and clients.

6

Configuring DPM to Back Up Servers and Clients

Configuring DPM to back up your servers is important because this is how you protect data objects such as hard drive volumes, files, folders, and shares. Another important item that can be included in a server backup is the system state. It is also important to know how to back up clients through DPM so that you are getting all of your user data.

In the first half of this chapter we will find out how to back up Windows' servers. This chapter will not cover backing up specific applications such as Exchange or SharePoint. Backing up applications will be covered in *Chapter 7*. This chapter will focus on the back up of standard Windows' servers.

Protecting Windows' servers will cover topics such as backing up files, shares, and the entire hard drive of a server, as well as backing up System State. We will walk through the process of installing the DPM agent on servers, creating Protection Groups, and protecting servers in untrusted domains or workgroups. In the second half of this chapter we will cover backing up clients with DPM.

We will break up the content into two specific topics. These topics are:

- Configuring DPM backup on servers
    - Requirements for a server before DPM can protect it
    - Installing DPM agent on servers
    - Creating a Protection Group and adding a server to it
    - Backing up files, shares, or the entire hard drive of a server
    - How system state backups work through DPM and how to configure this
    - How to protect servers in untrusted domains or in workgroups

- Configuring DPM backup on clients
    - What is the DPM client?
    - Installing the DPM client

Configuring DPM backup on servers

There are certain requirements that a server must fulfill before DPM can protect it. The operating systems that are supported include Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2. Core, Standard, Enterprise, and Datacenter editions of Windows Server 2003/2008/R2 are all supported. Another requirement is that any protected volumes must be formatted as NTFS. DPM uses the Volume Shadow Copy Service to create a snapshot of the protected data and this needs at least 1 GB free space on the protected volume.

The pagefile should be set to 0.2 percent the size of all recovery point volumes combined, this is in addition to the recommended size of 1.5 times the amount of memory in the server. When the pagefile is not set correctly this can cause protected data on DPM to become inconsistent. You also need to make sure the servers you want to protect have certain Windows Updates applied. These updates are:

Operating System	Update
Windows Server 2003	Service Pack 2 Windows Server 2003 of Knowledge Base article 940349 `http://go.microsoft.com/fwlink/?LinkId=186465` Hotfix from Knowledge Base article 975759 `http://go.microsoft.com/fwlink/?LinkId=185943`
Windows Server 2008	Hotfix from Knowledge Base article 977381. `http://go.microsoft.com/fwlink/?LinkId=186472` Hotfix from Knowledge Base article 975759 `http://go.microsoft.com/fwlink/?LinkId=185943`
Windows Server 2008 R2	Hotfix described in Knowledge Base article 977381. `http://go.microsoft.com/fwlink/?LinkId=186472`

NOTE: All of these updates and hotfixes are required for protecting file servers. Application specific servers such as Exchange or SharePoint will require different updates and hotfixes and we will cover this in *Chapter 7* when we discuss each application.

Meeting all the requirements for protecting a server with DPM does not mean that a computer is protected. You still need to install the DPM agent on the protected computer. The DPM protection agent is software that needs to be installed on any computer you want to protect. Once a computer has the agent installed it will then show up in the DPM Management task area. The protected computer can be added to a Protection Group only after the agent is installed. DPM uses the agent to communicate with the protected computer. Each agent is exclusive to one DPM server. For example, if you had two DPM servers called DPM1 and DPM2, the computers that had the agent installed from DPM1 could not be protected by or communicate with DPM2. The computer would only be able to be protected by and communicate with DPM1.

The agent allows DPM to access shares, volumes, and folders on the computer you are protecting. The agent also records changes of the protected data in a change journal. The journal is a hidden file on the protected volume. The changes in the journal on the protected computer are then transferred to the DPM server by the agent. Once DPM knows about these changes it will then synchronize the changes of the protected data with a replica of the protected data on the DPM server.

DPM 2010 offers more agent installation options over DPM 2007. In DPM 2010 you can Install, or Attach an agent. You would choose the attach agent option for computers that are behind a firewall that the DPM server cannot get through, if the protected server already has the DPM agent installed. Attaching the agent simply adds the protected computer to the DPM server but does not install the agent on the protected server. The agent can be installed before or after attaching to the DPM server.

When you choose to attach an agent over installing the agent you must manually install the agent on the protected server. When installing the agent manually, you can install on computers in the same domain as the DPM server and on computers in an untrusted domain or workgroup. In DPM 2007 the only option you have is to install the DPM agent and only on computers that are in the same domain as the DPM server.

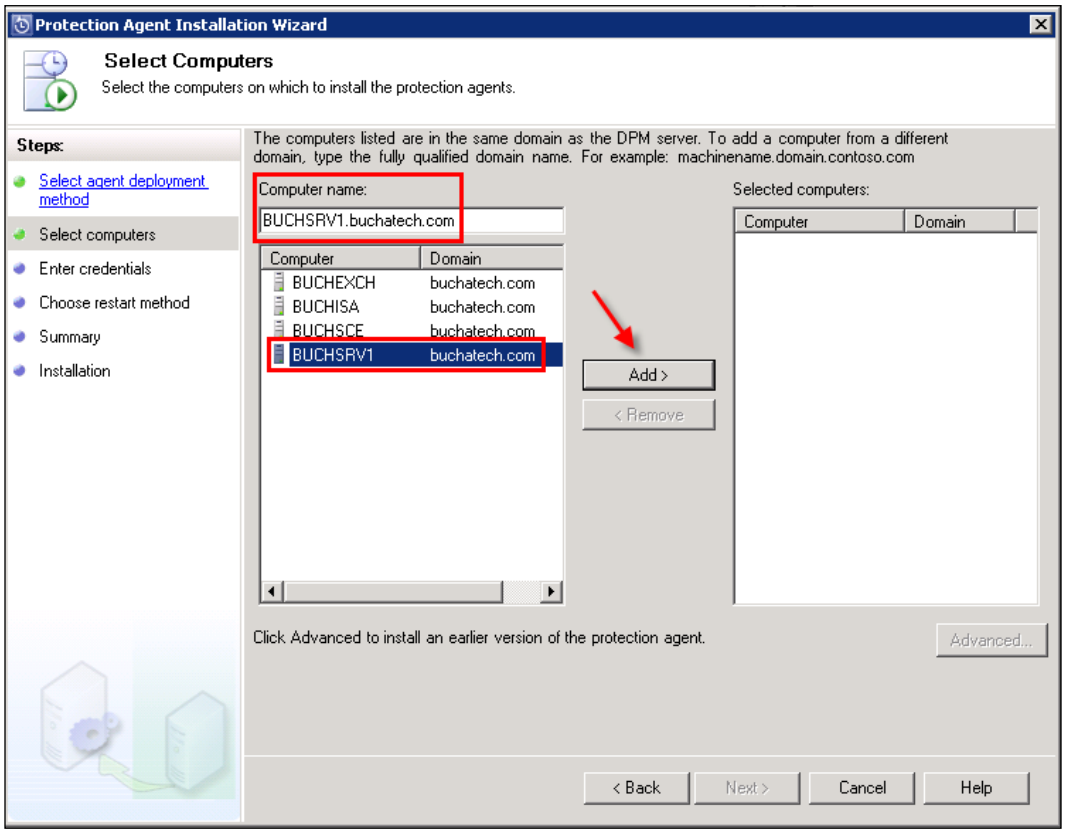
Let's walk through installing the DPM agent on a server using both Install and Attach.

Installing the DPM agent

In this example we will run through the typical way of installing the DPM agent:

1. Open the DPM Administrator Console.
2. Click the **Management** tab on the navigation bar.
3. Now click on the **Agents** tab.
4. On the **Actions** pane, click **Install**.

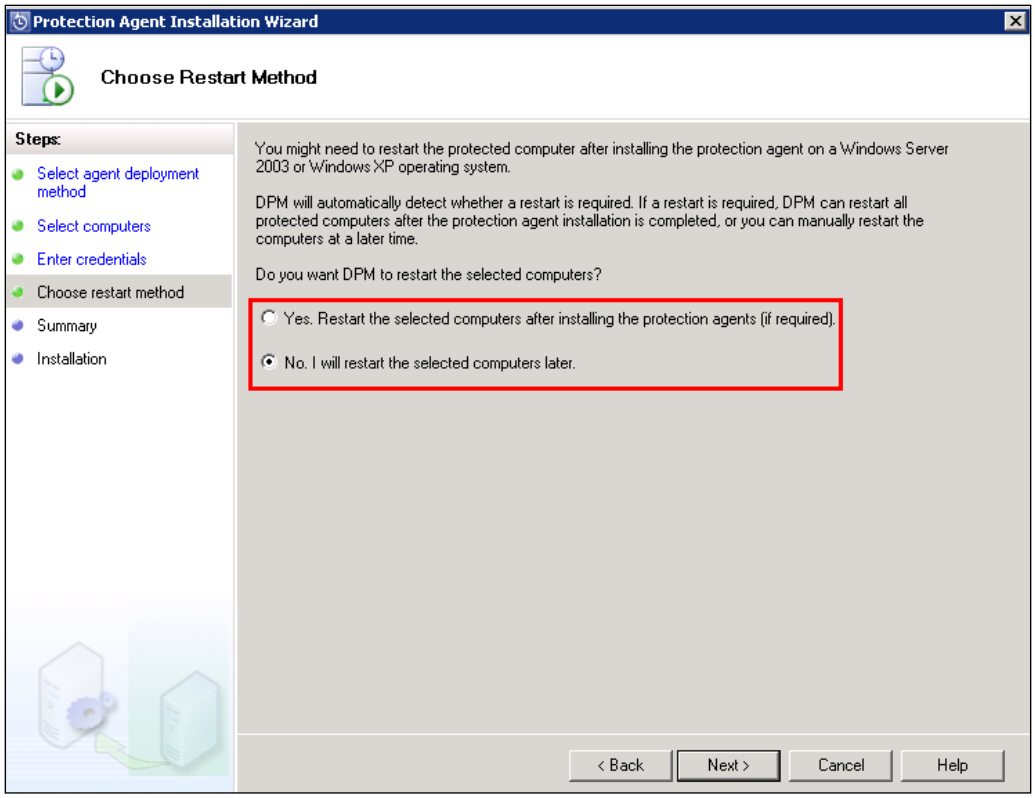
5. Now the **Protection Agent Install Wizard** will pop open. Choose **Install** agents and click **Next**.
6. On the next screen, select the computer you want to protect then click **Add**. This will move the computer to the **Selected computers** area. Click **Next** to continue.



7. Enter the credentials for the domain. The account that you need to specify in the next window needs to have administrative rights on the computer you are going to protect. Click **Next** to continue.

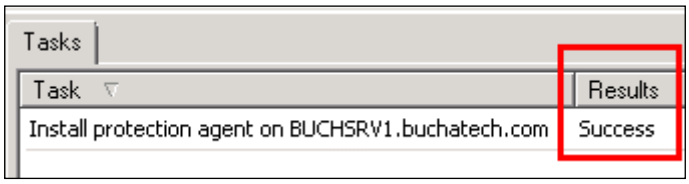
8. On the next screen you have the option to have DPM automatically restart the computer you are going to protect or to manually restart it. For this example we will choose to manually restart. Click **Next** to continue.

NOTE: The DPM 2010 agent doesn't require you to restart the machine; restart is mandatory only in the case of an upgrade from 2007 to 2010.

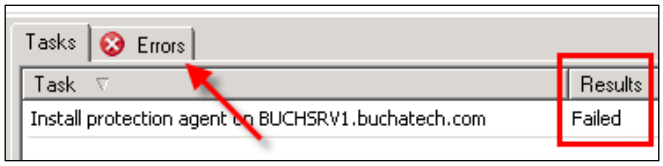


9. On the next screen click **Install** to continue with the DPM agent installation.

10. You will then receive a status screen. This will show you the progress of the DPM agent installation.
11. The status will show **Success** in the **Results** field if the installation succeeded and **Failed** if there is a problem with the installation.



12. To see more information on the errors if the installation failed click on the **Errors** tab in the window.

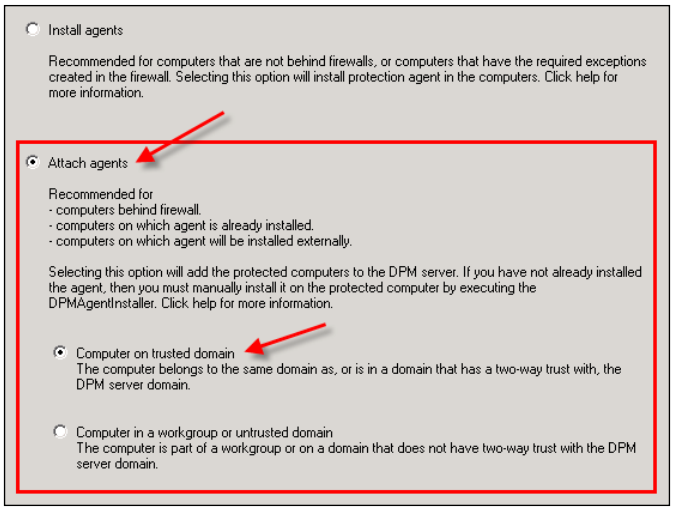


13. Click **Close** when it is finished.

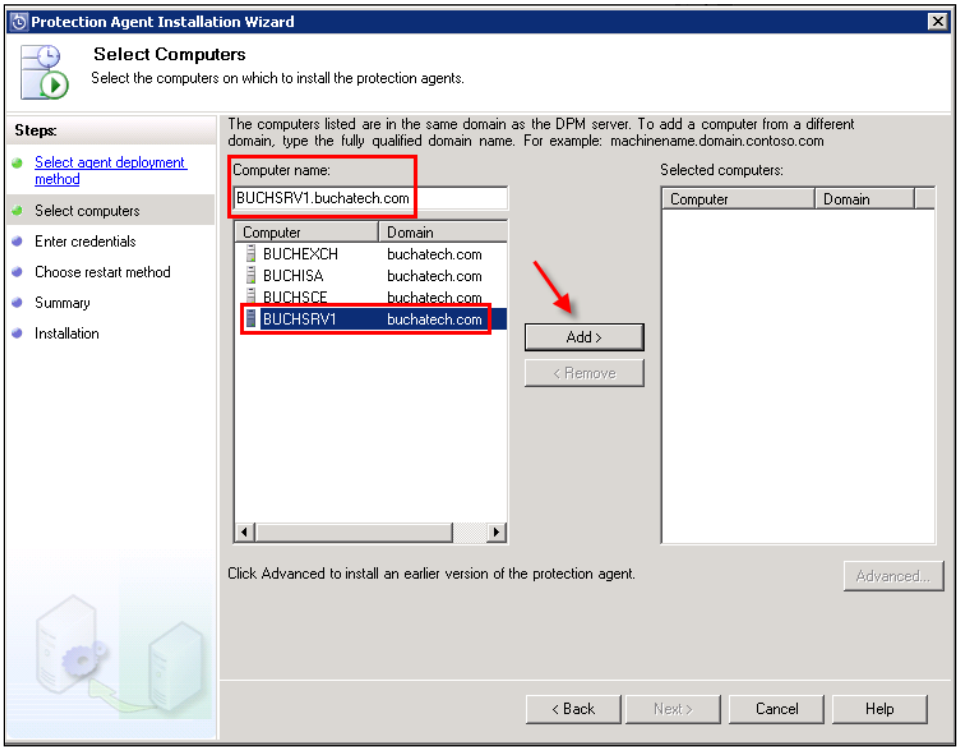
Installing the DPM agent manually

In this example we will run through the manual way of installing the DPM agent using the **Attach** option. This will walk you through installing the wizard on DPM and then through installing the agent manually on the computer you want to protect:

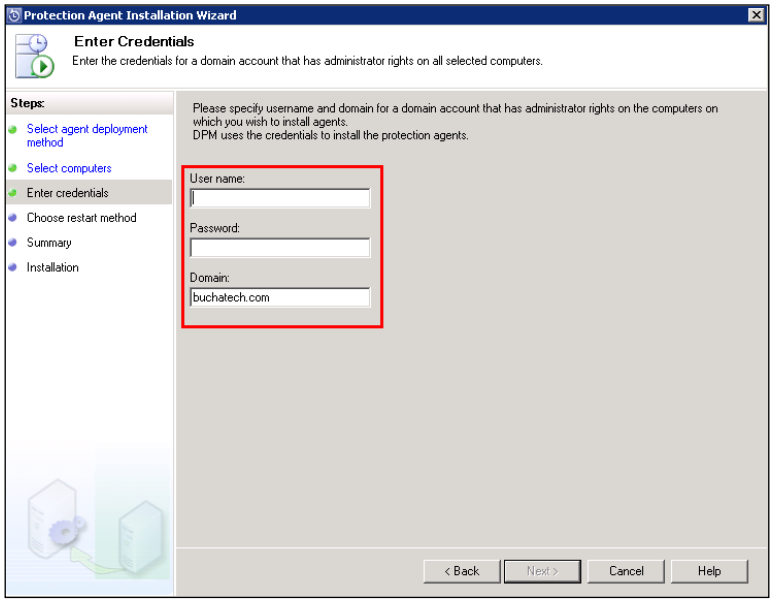
1. Open the DPM Administrator Console.
2. Click the **Management** tab on the navigation bar.
3. Now click on the **Agents** tab.
4. On the **Actions** pane, click **Install**.
5. Now the **Protection Agent Install Wizard** should pop up. Choose **Attach agents**.
6. Choose **Computer on trusted domain** and click **Next**.



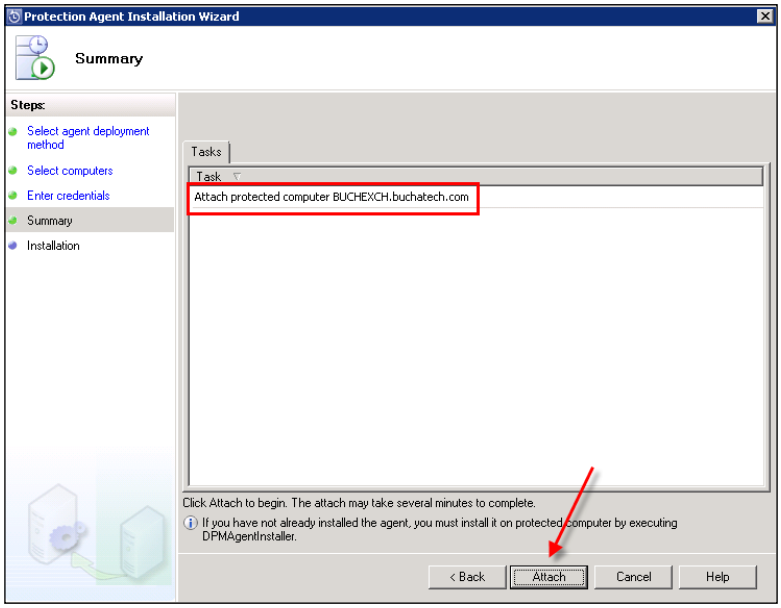
7. On the next screen select the computer you want to protect then click Add. This will move the computer to the **Selected computers** area. Click **Next** to continue.



8. Enter the credentials for the domain. The account that is used here needs to have administrative rights on the computer you are going to protect.
   Click **Next** to continue.



9. On the next screen click **Attach** to continue with the DPM agent installation.



Now you need to install the agent on the computer you want to protect. Here are the steps to do this:

1. Locate the `3.0.7696.0` folder on your DPM server here:

   `%systemroot%\Program Files\Microsoft DPM\DPM\ProtectionAgents\RA\`

2. The `3.0.7696.0` folder will have two folders, `i386` and `amd64` in it. If you are installing on a 64 bit server use the installer from the `amd64` folder otherwise use the `i386` folder.

3. Copy this folder to the local `%systemroot%` drive on the server you want to protect. The best thing to do is to create a folder that will hold the DPM agent installation files on the server that need to be protected in order to make the installation easy. You can name it `DPMagentinstall` for example `c:\DPMagentinstall`.

4. Open a command prompt on the server you are going to protect. If this is Windows 2008 Server be sure to open the command prompt with elevated privileges.

5. For 32 bit computers, type:

   `cd c:\DPMagentinstall\DPMAgentInstaller_x86.exe <DPMServerFQDN>`

6. For 64 bit computers, type:

   `cd c:\DPMagentinstall\DPMAgentInstaller_x64.exe <DPMserverFQDN>`

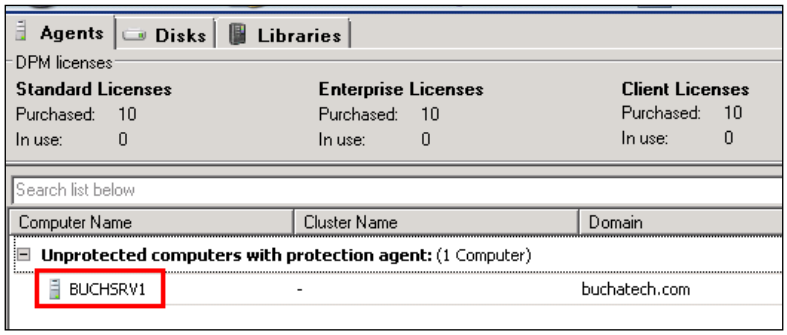
   For example: `DPMAgentInstaller_x86.exe DPM01.mydomain.com`

It will then let you know that your server requires a restart if it was successful.

If the protected computer was attached in DPM before the agent installer on the protected computer, the computer will then already be in the DPM Console. If the protected computer was not attached in DPM beforehand then attach the computer in the DPM Administrator Console or simply run the following commands in PowerShell on the DPM server:

```
Attach-ProductionServer.ps1YOURDPMSERVERNAME SERVERNAMEYOUWANTTOPROTECT
YOURUSERNAME YOURPASSWORD THEDOMAINNAME
```

Running the above command will bring the agent into DPM Administrator Console so you can now see it.



As an alternative you could also simply type `.\Attach-ProductionServer.ps1` in DPM PowerShell then hit *Enter* and it will prompt you for all the following information step-by-step:

- DPMServer
- PSName
- UserName
- Password
- Domain

Creating Protection Groups

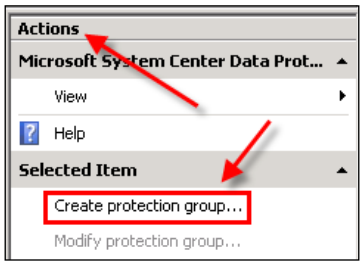
After you install the DPM agent on a server you want to protect, it still needs to be added to a Protection Group. Protection Groups are a collection of data sources that share a common configuration for protecting them. Protection Groups are policies for groups of protected computers. An example of common configuration would be one Protection Group synchronizes every 30 minutes while another synchronizes every hour. You may want to place SQL databases in the Protection Group that synchronizes every 15 minutes rather than the Protection Group that synchronizes every hour because the data changes more often and you want DPM to back this up frequently. The data sources within a Protection Group are considered members of that Protection Group. These are called Protected Members.

The members are data sources of protected computers. Some examples of data sources are volumes, shares, Exchange storage groups/DAGs, SQL databases, and Hyper-V virtual hard drives. When you want to protect a server you would add it to a Protection Group and then it will be backed up by DPM.

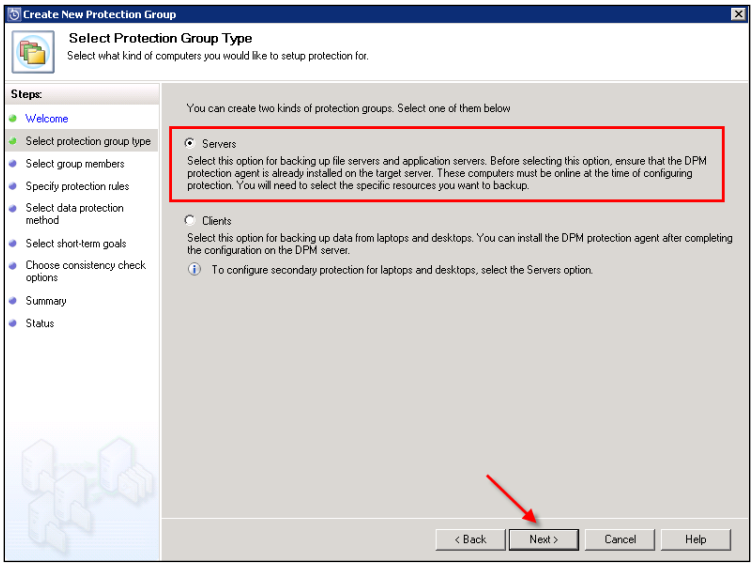
Once your protected computer is added to a Protection Group DPM will then begin backing up your data. Here is the process of creating a Protection Group and how to add a server to it.

A common type of data that is backed up in every environment are files, folders, and basic data on hard drives. Backing up this type of data through DPM is straightforward; when you add the server to a Protection Group you can select the files, shares, or entire volumes as a part of the back up. Here is how you create a Protection Group and choose the data you want to back up:

1. Open the DPM Administrator Console.
2. Click the Protection tab on the navigation bar.
3. In the **Actions** pane click on **Create protection group**:

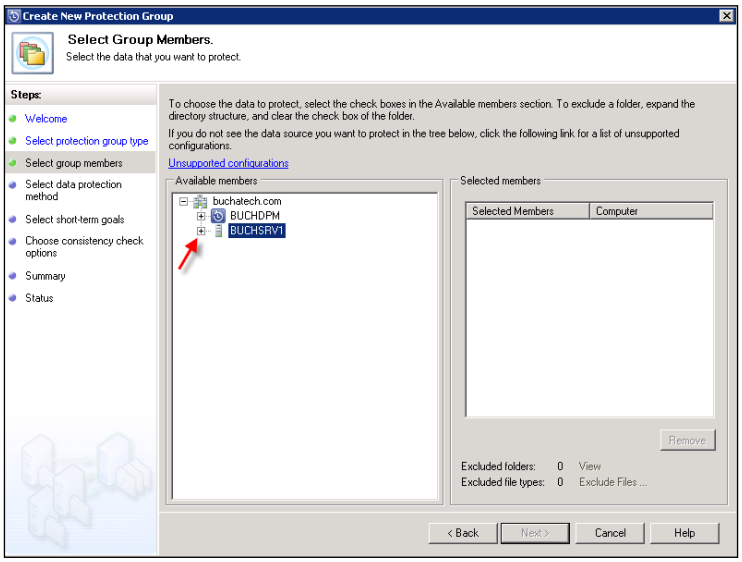


4. Click **Next** on the **Welcome** page.
5. Select **Servers** for this **Protection Group Type** and click **Next**.

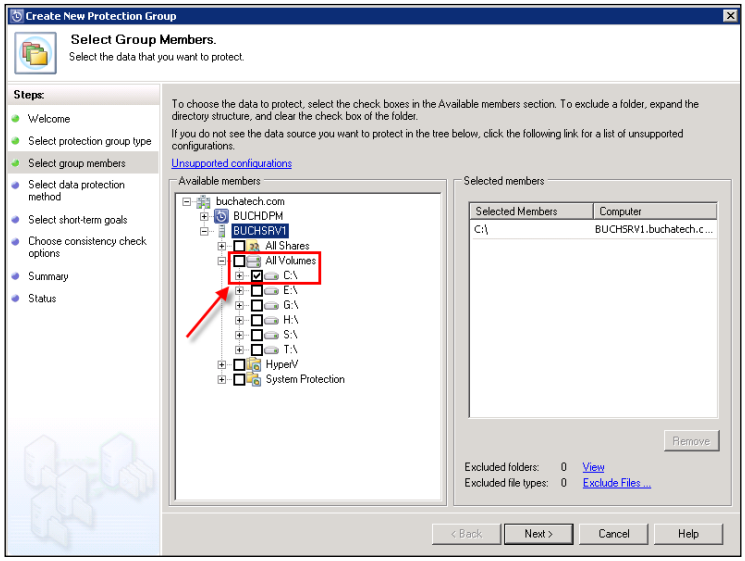


6. Expand the server you want to protect by clicking the + next to it.

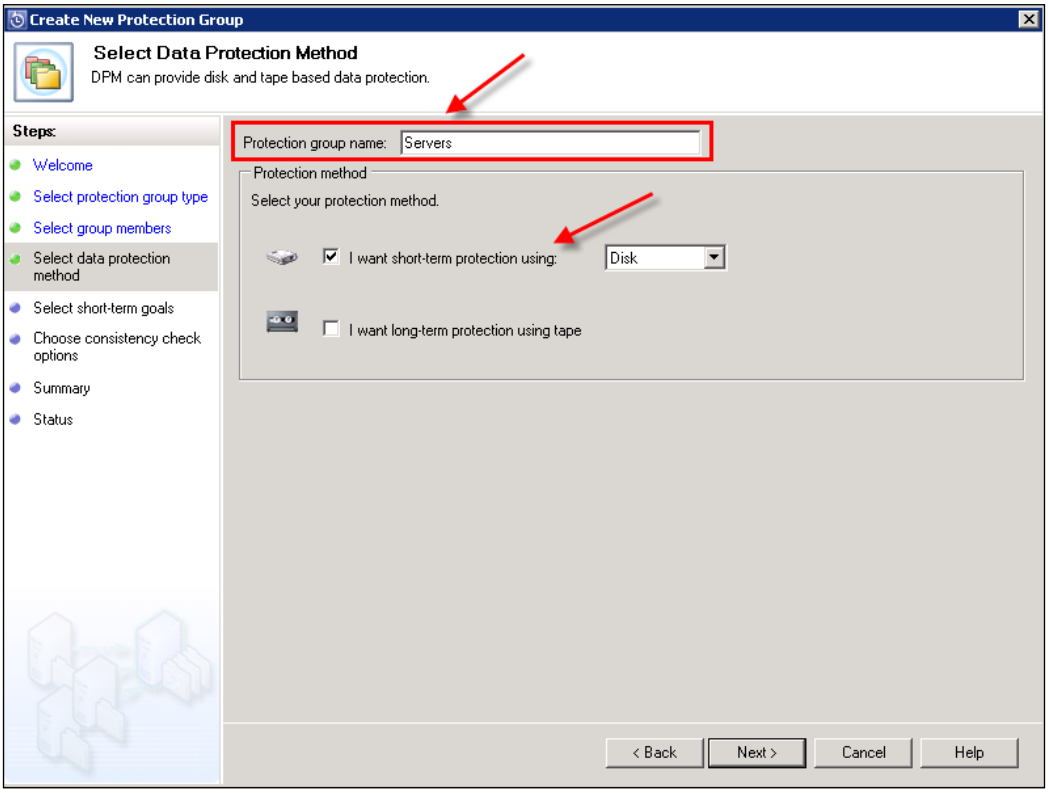
> **NOTE**: Be patient after you expand the server you want to protect. This may take some time while the VSS service is being queried on the target computer.



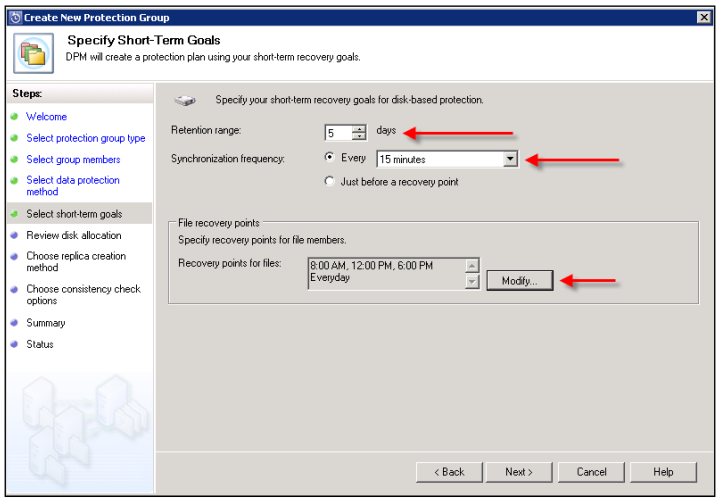
7. Expand the data object you want to protect by clicking the + next to it.



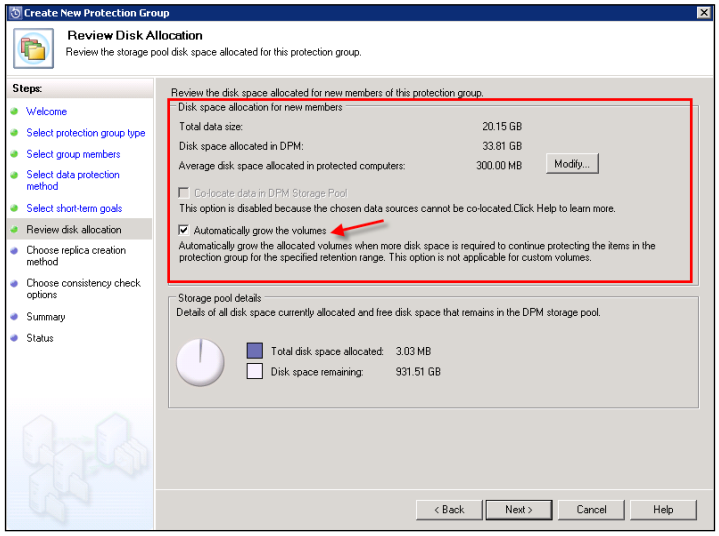
8. Place check marks next to the data you want to protect by clicking in the open boxes next to the data object. Here we are going to select the **C:** drive under **All Volumes**. Click **Next**.
9. Now give your Protection Group a name. Select disk or tape protection. In this example we chose disk only. Click **Next**.



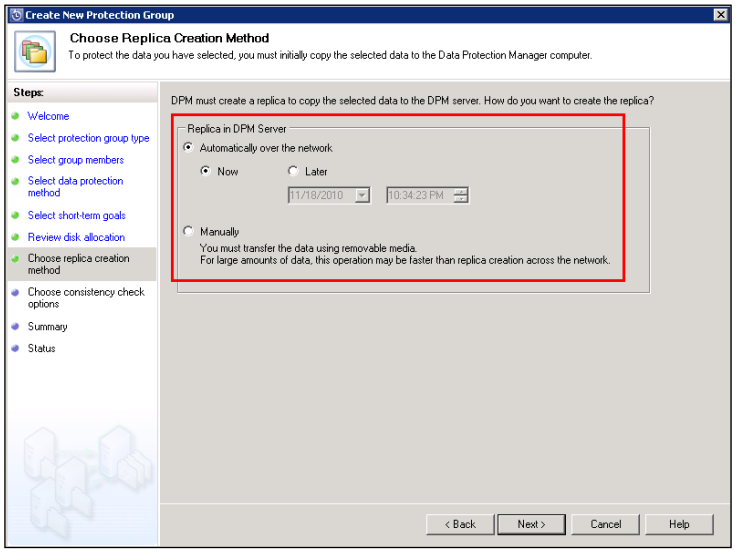
10. Next, choose how long you want to retain your data, how often you want to synchronize your data and the recovery point creation schedule. You can set the recovery point schedule by clicking on the **Modify** button. Once you have all your settings in place click **Next**.



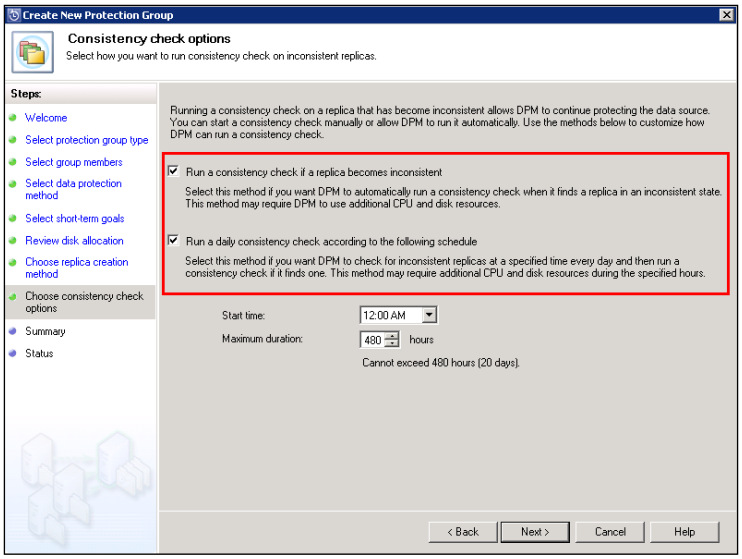
11. Review your disk space allocation. This screen shows you an estimate of how much space this protected data will use from your disk pool. You also have the option to set the automatic growth feature. This tells DPM to grow the space allocation in your storage pool as the protected data grows. In DPM 2007 you had to do this manually. Click **Next** to continue.



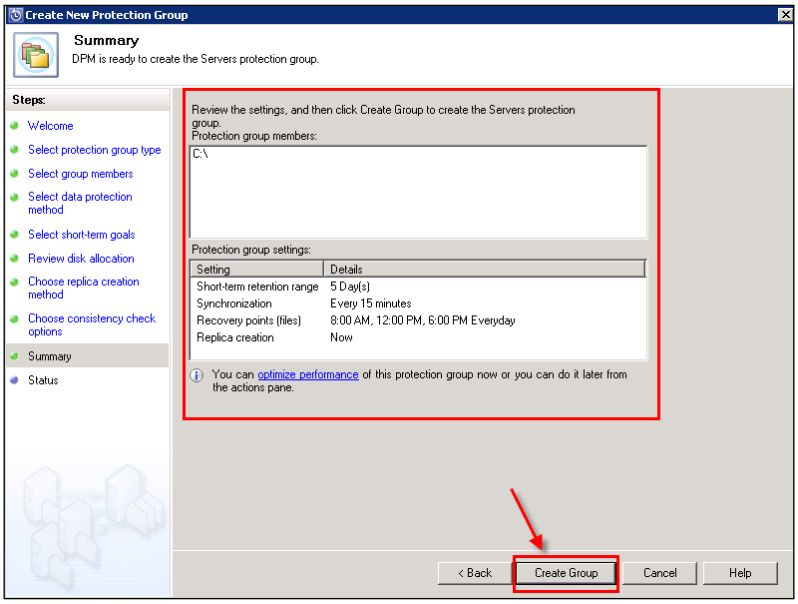
12. On this screen you can create a replica of the protected data now or later at a specified date and time. You also have the option of creating the replica manually using removable media. This is used for large amounts of data or protected servers that are unreachable over the network at the current time. Click **Next** to continue.



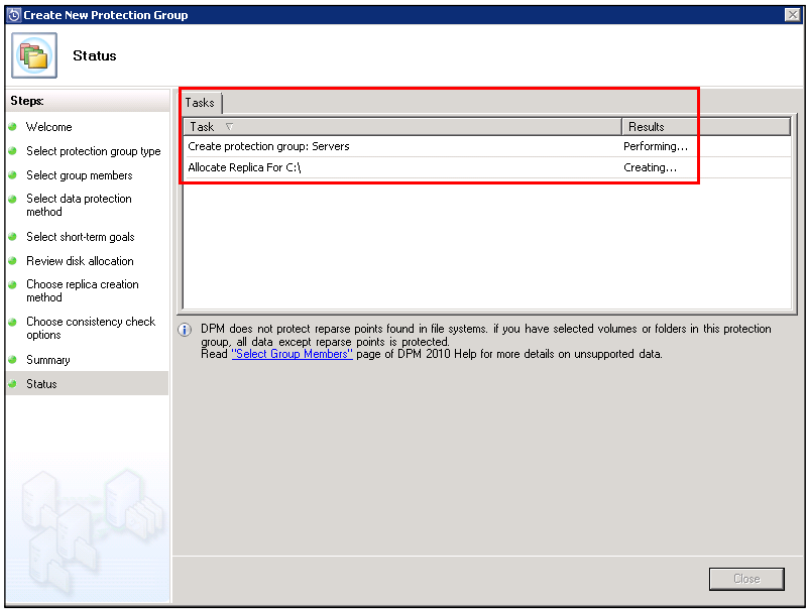
13. Check mark to automatically run a consistency check and it is recommended that you run this automatically daily. Click **Next** to continue.



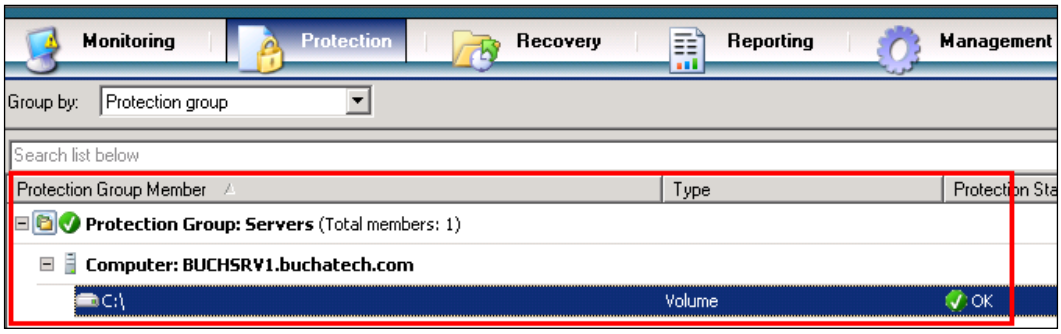
14. This screen gives you a summary of the Protection Group you are about to create. Click **Create Group**.



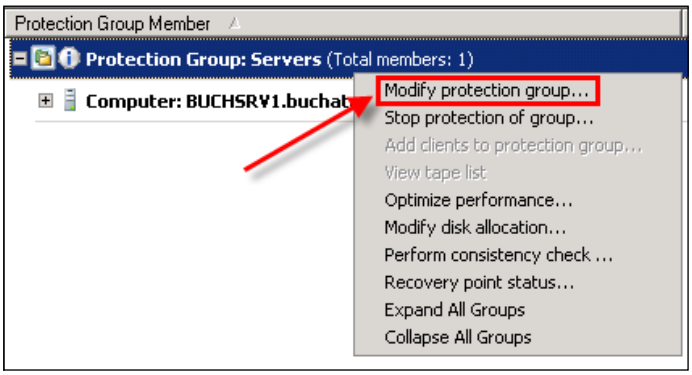
15. The next screen shows you the status of the group creation and will display **Success** or **Fail** when done. Click **Close** when it is done.



16. Now under the **Protection** tab on the management menu you will see your new Protection Group and the servers you are protecting:



17. If you want to add more servers just right-click on the Protection Group and choose **Modify Protection Group**.



So that is how you create a **Protection Group**, add a **Protected Member** to it and back up data.

Backing up System State

System State is a backup of critical system related components. The System State can be used to restore a system after a crash. The System State contains the following:

- Registry
- COM+ Class Registration database
- System files that are under Windows File Protection

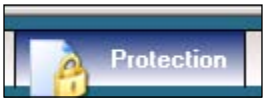
- Active Directory (if the server is a domain controller)
- SysVol (if the server is a domain controller)
- Certificate Services (if the server is running Certificate Services)
- IIS Metabase

The System State backup only backs up system components. System State does not contain any data from hard drives or application specific data such as Exchange, SharePoint, or SQL data. It is recommended that you back up the hard drives and any application specific files that will be needed in the event of a failure. If you want to back up specific applications you will need to refer to your application documentation on backup. For more information on System State refer to:

`http://technet.microsoft.com/en-us/library/cc785306(WS.10).aspx`

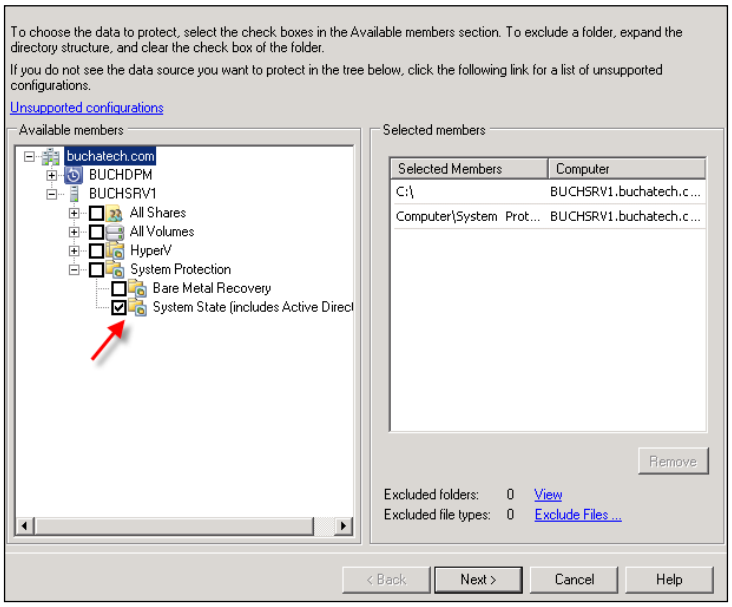
In order for DPM to back up System State on a Windows 2008 server the WSB (Windows Server Backup) feature needs to be installed on that Windows server. System State has grown significantly in size in Windows 2008 server. It is common for the System State backup to be double digit Gigabytes in size or larger. Be sure to have enough free space on the drive that will store the System State backup. We are going to use our existing Protection Group for the following example. These steps will show you how to modify an existing Protection Group and how you back up System State in DPM:

1. Open the DPM Administrator Console.
2. Click the **Protection** tab on the navigation bar:

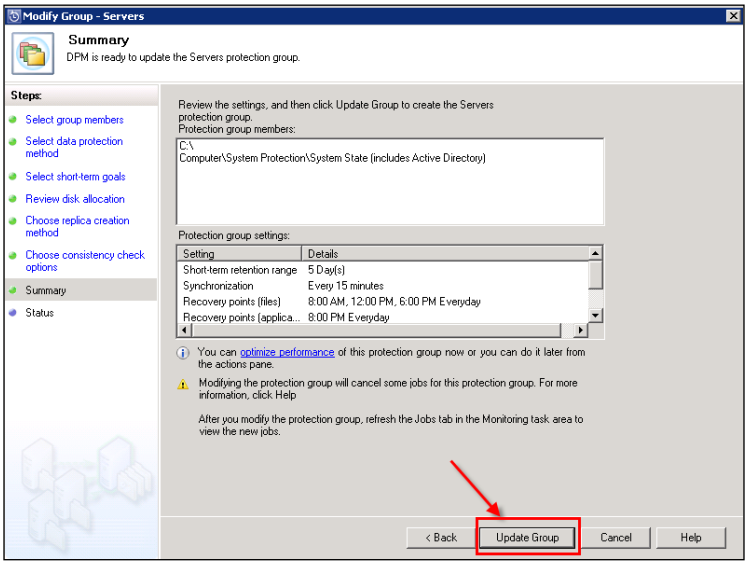


3. Right-click on the Protection Group and choose **Modify Protection Group**.
4. Expand the **+** next to the server you want to back up the System State on.
5. Expand the **+** next to **System Protection**.

6. Put a check mark in the box next to **System State** and click **Next**.



7. You will then click **Next** on the following five screens that you have already configured when you set up the Protection Group.
8. On the final screen, click on **Update Group** and the System State backup will be added to this Protected Member:



Protecting computers in workgroups and untrusted domains

In DPM 2010 you are able to back up computers that are in workgroups or in untrusted domains. This includes backing up file servers, Hyper-V, SQL, and Exchange in non-trusted domains. Backing up SharePoint in untrusted domains is not supported.

NOTE: DCOM needs to be enabled on the protected server. If this is not enabled you may receive the "incorrect password" error when trying to attach the protected computer of a workgroup or untrusted domain.

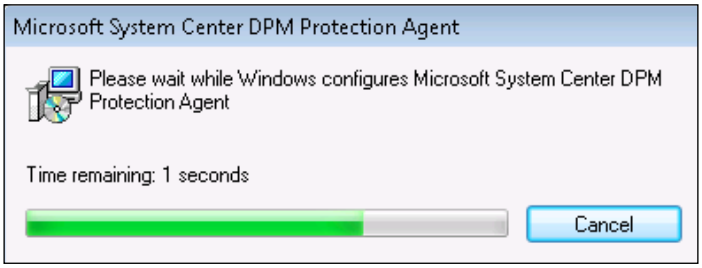
The way to protect computers in untrusted domains or workgroups is by using a local user account from the computer you are protecting. This is NTLM authentication that is between DPM and the protected computer using the local user account from the protected computer. These credentials are to be supplied during the installation of the DPM agent. The agent has to be installed using the attach option in the DPM Agent Installation Wizard and then has to be manually installed on the computer you plan to protect. Any updates that are needed for the agent in the future will have to be manually applied.

There are two parts to protecting a computer that is in a workgroup or untrusted domain. The first part is installing the DPM agent on the computer that needs to be protected. The second part is to attach the agent in DPM. Here are the steps to back up a computer in a workgroup or untrusted domain:

1. From the computer you will be protecting, access the DPM server over the network and copy the folder with the Agent installer in it down to the local machine. Use this path:

   `\\DPMSERVERNAME\Program Files\Microsoft DPM\DPM\ProtectionAgents\RA\3.0\3.0.7696.0\i386`

2. Then from the local folder on the protected computer run `dpmra.msi` to install the agent.



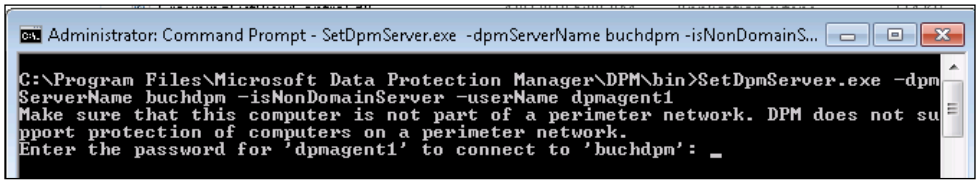
3. Open a command prompt (make sure you have elevated privileges) change directory to `C:\Program Files\Microsoft Data Protection Manager\DPM\bin` then run the following:

   `SetDpmServer.exe -dpmServerName<serverName> -isNonDomainServer-userName<userName>`

   Example:

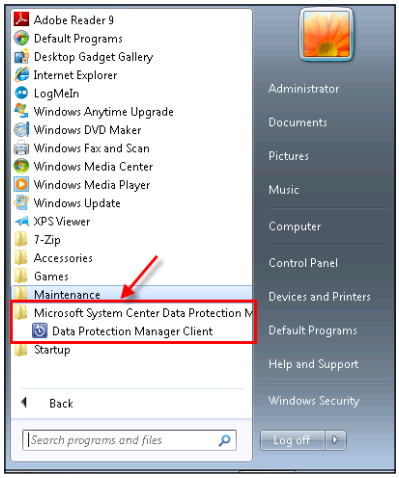
   `SetDpmServer.exe -dpmServerNamebuchdpm -isNonDomainServer -userName dpmagent1`

4. You will be prompted to enter a password. Enter a password and press the enter key. It will then ask you to confirm the password by typing it in a second time:



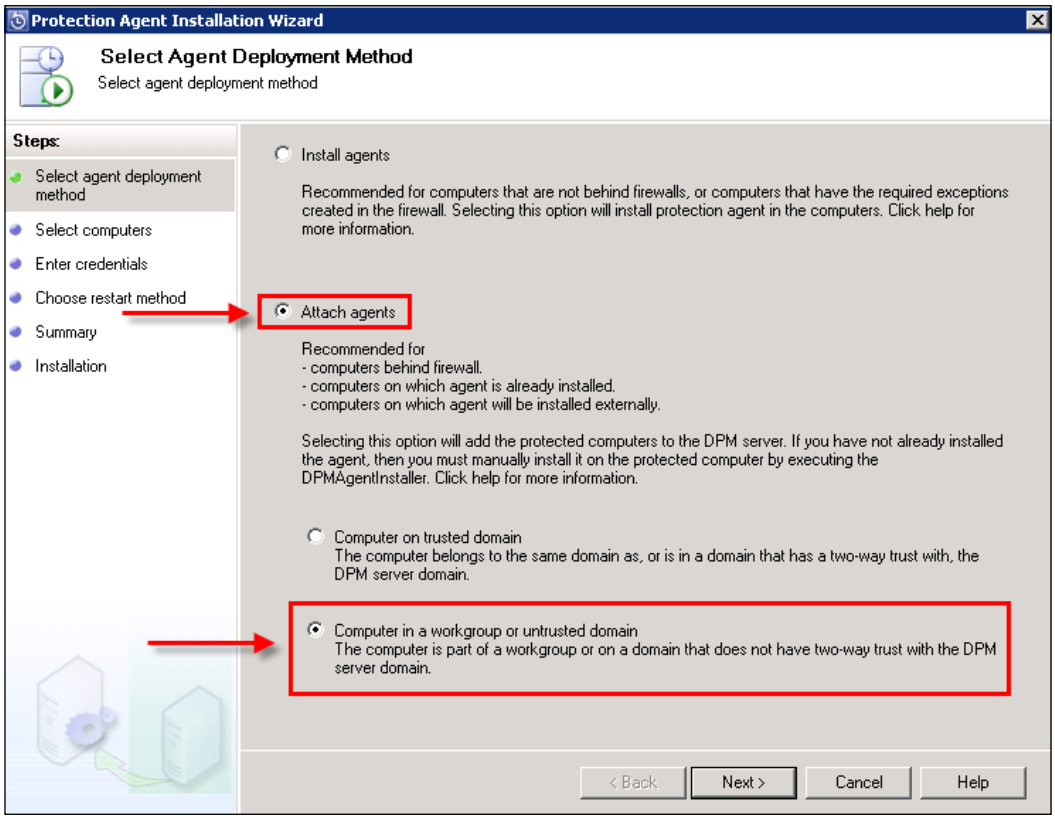
5. Hit *Enter* and the `SetDpmServer.exe` will finish configuration:

You will then see the DPM client installed and connected to the DPM server in the **Start** menu.

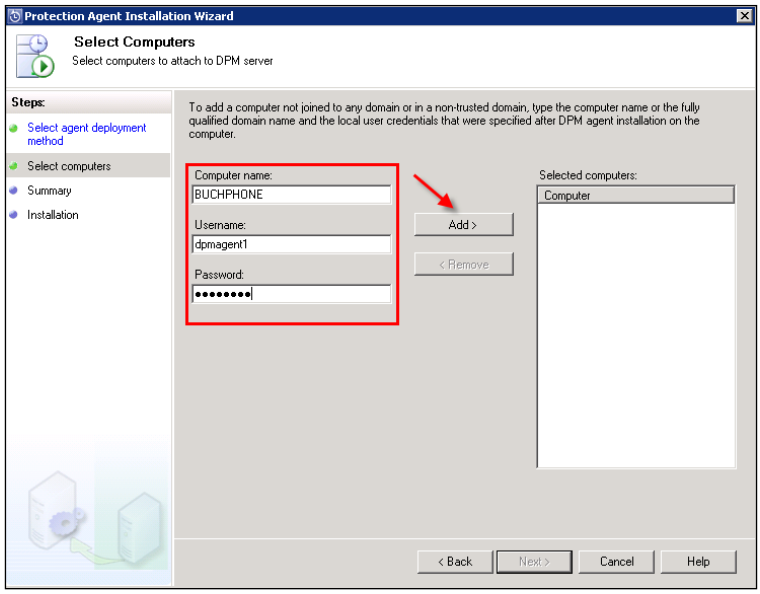


The next step is to go back to the DPM server and attach the agent to the protected computer. To do this follows these steps:

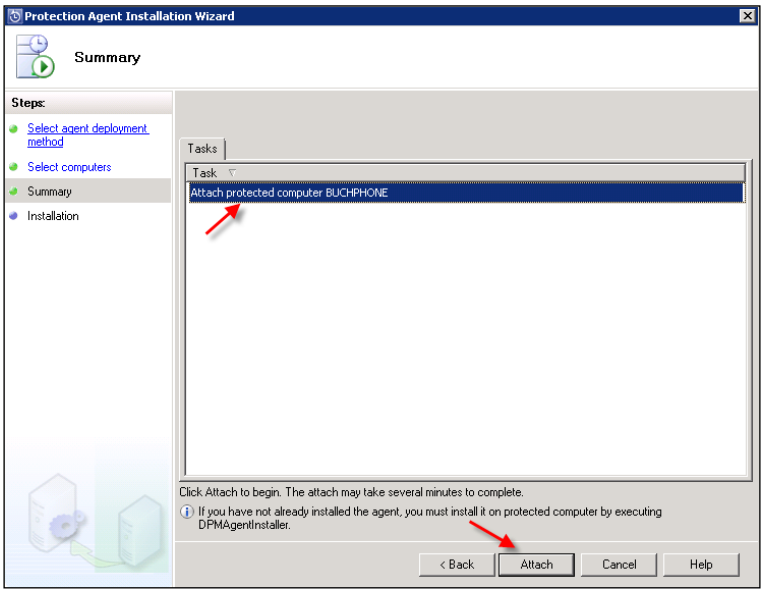
1. Go to the DPM server and open the DPM Administrator Console.
2. Click the **Management** tab on the navigation bar.
3. Now click on the **Agents** tab.
4. On the **Actions** pane, click **Install**.
5. Now the **Protection Agent Install Wizard** should pop up. Choose **Attach agents**, and select **Computer in a workgroup or untrusted domain** then click **Next**:



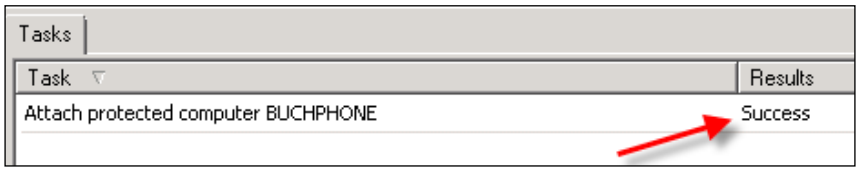
6. Add the computer name of the computer you want to protect and add the account that you used when you ran the `SetDpmServer.exe` configuration on the protected computer. Click **Add** to move the computer to the **Selected computers** box. Click **Next** to continue.



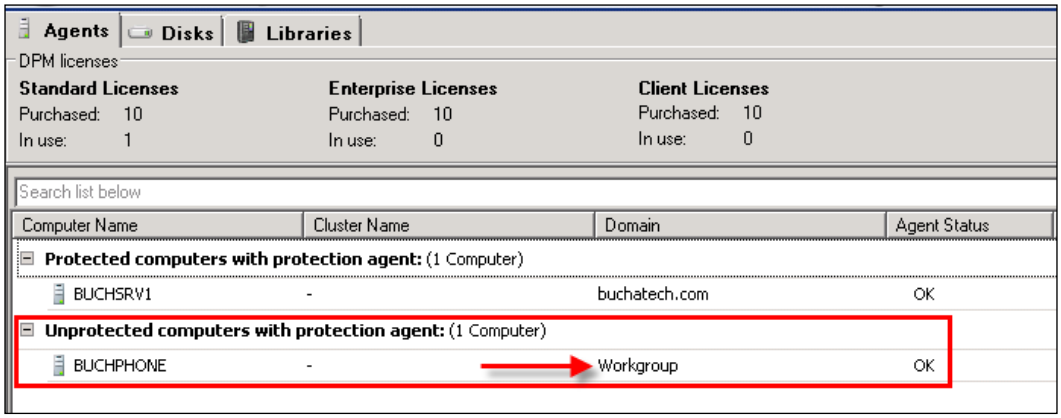
7. Click **Attach** to begin the agent installation:



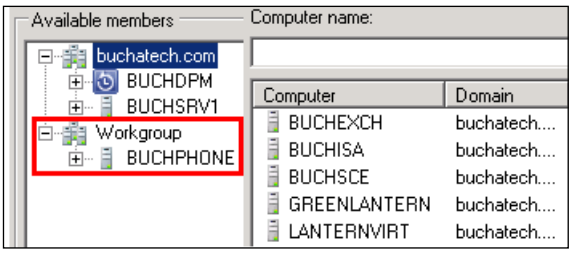
8. Once it is finished you will see a status of **Success** or **Failed**.



That is all you needed to do to start protecting a computer in a workgroup or untrusted domain. You will notice now that in the DPM Administration Console the newly added computer shows up with a domain field of workgroup. You can now add data sources from this computer to a Protection Group.



NOTE: When you add workgroup or untrusted domain computers to a Protection Group you must choose a Protection Group Type of Servers. Workgroup and untrusted domain computers will not show up in the Protection Group Type Clients and therefore you will not be able to protect their data.



Configuring DPM backup on clients

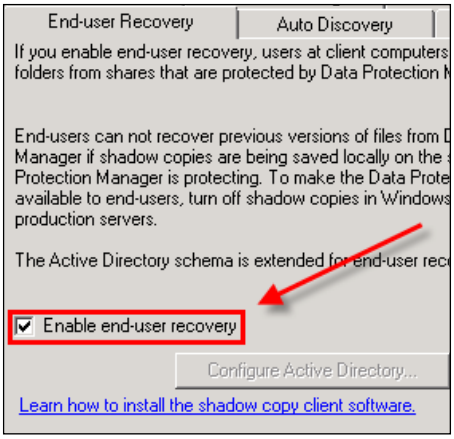
DPM 2010 has improved the client backup management and experience. Client back up consists of backing up desktops and laptops. The backup has even been improved for remote clients that are not connected to the network very often. As a DPM administrator you can configure the client and control what is backed up. You also have the option of letting the end-users control their own backup.

The DPM client utilizes the Previous Versions feature that is seen in Windows Vista and Windows 7. DPM creates a local copy of protected data and a remote copy on the DPM server. DPM can protect client computers that are either 32 or 64 bit. The following are the operating systems that are supported by DPM:

- Windows XP SP2 or later
- Windows Vista
- Windows 7

Configuring End-user Recovery

The first step is to make sure End-user Recovery is enabled. To check mark this in the DPM Administrator Console go to the **Action** menu and select **Options**. A check should be in the box next to **Enable end-user recovery**:

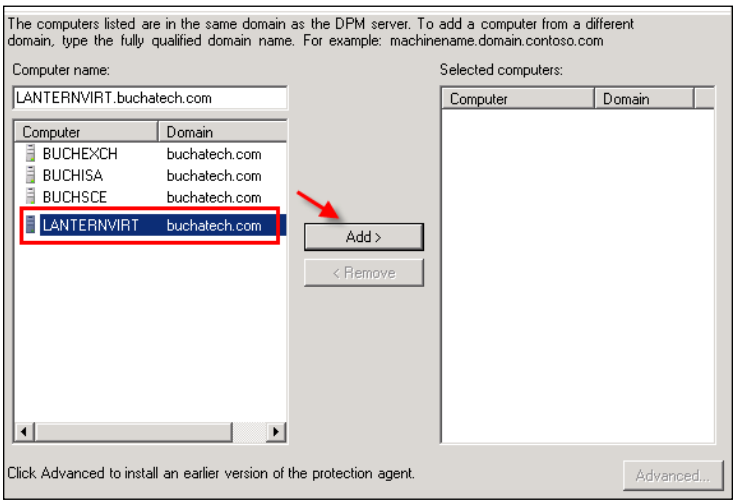


If this box is not checked you will need to configure Active Directory and then check this box. For more information on configuring End-user Recovery refer back to *Chapter 4*.

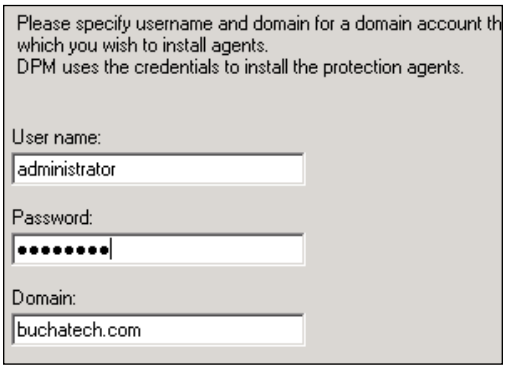
Installing the DPM client

Now let's look at the steps for installing the DPM client on a client computer:

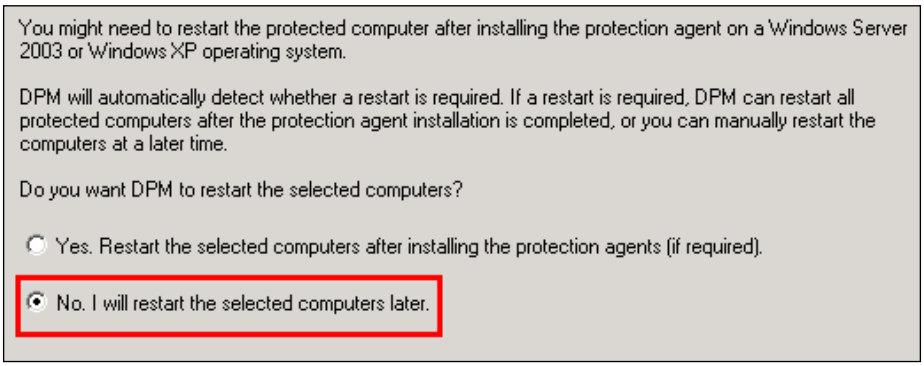
1. Go to the DPM server and open the DPM Administrator Console.
2. Click the **Management** tab on the navigation bar.
3. Now click on the **Agents** tab.
4. On the **Actions pane**, click **Install**.
5. Now the **Protection Agent Install Wizard** should pop up. Choose **Install agents** then click **Next**.
6. Select the computer you want to protect from the list and click **Add**. Click **Next** to continue.



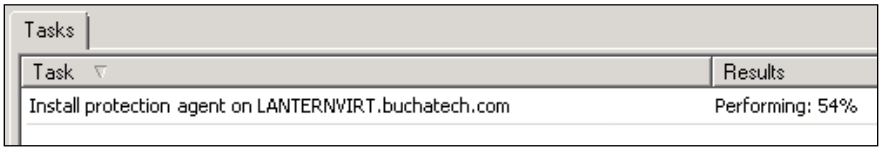
7. Enter a domain account and click **Next**.



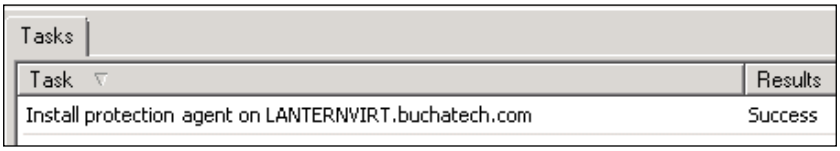
8. Choose to restart manually later and click **Next**.



9. Click **Install** to start the actual installation.



10. You will see a **Success** or **Failure** status when the installation is complete:

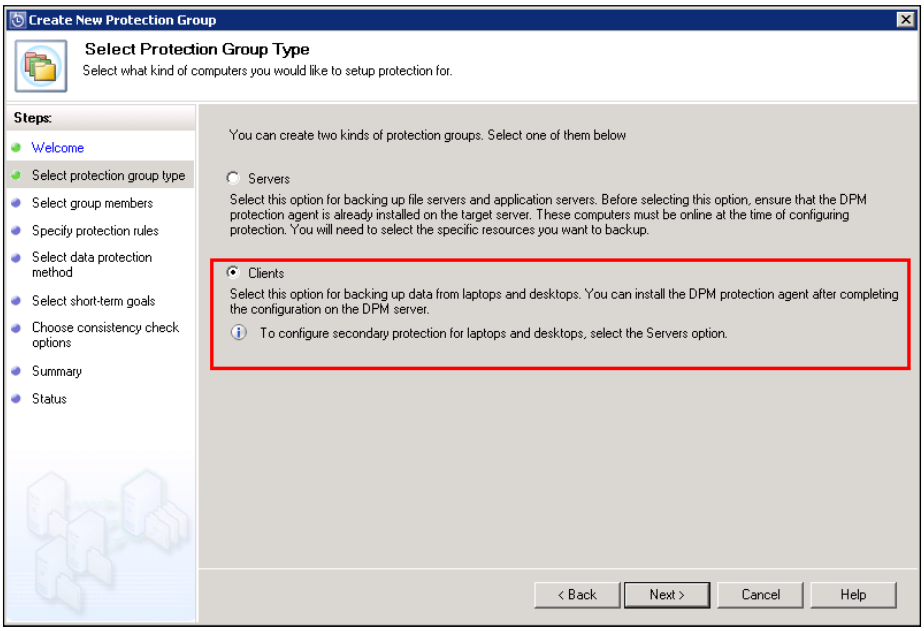


Configuring clients in Protection Groups

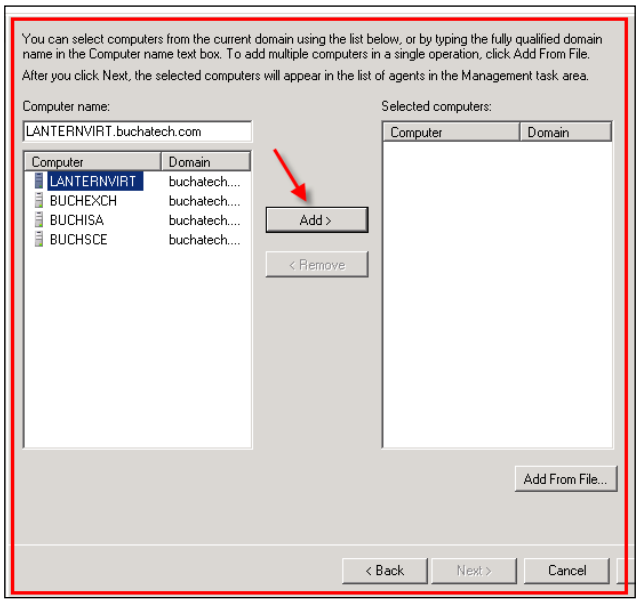
The client needs to be added to a Protection Group now. There are features that we will look at as we configure the client in the Protection Group. Here are the steps for adding a client to a new Protection Group:

1. Click the **Management** tab on the navigation bar.
2. Click **Create Protection Group** in the **Actions** menu.
3. Click **Next** on the welcome screen.

4. Select **Clients** and click **Next**.

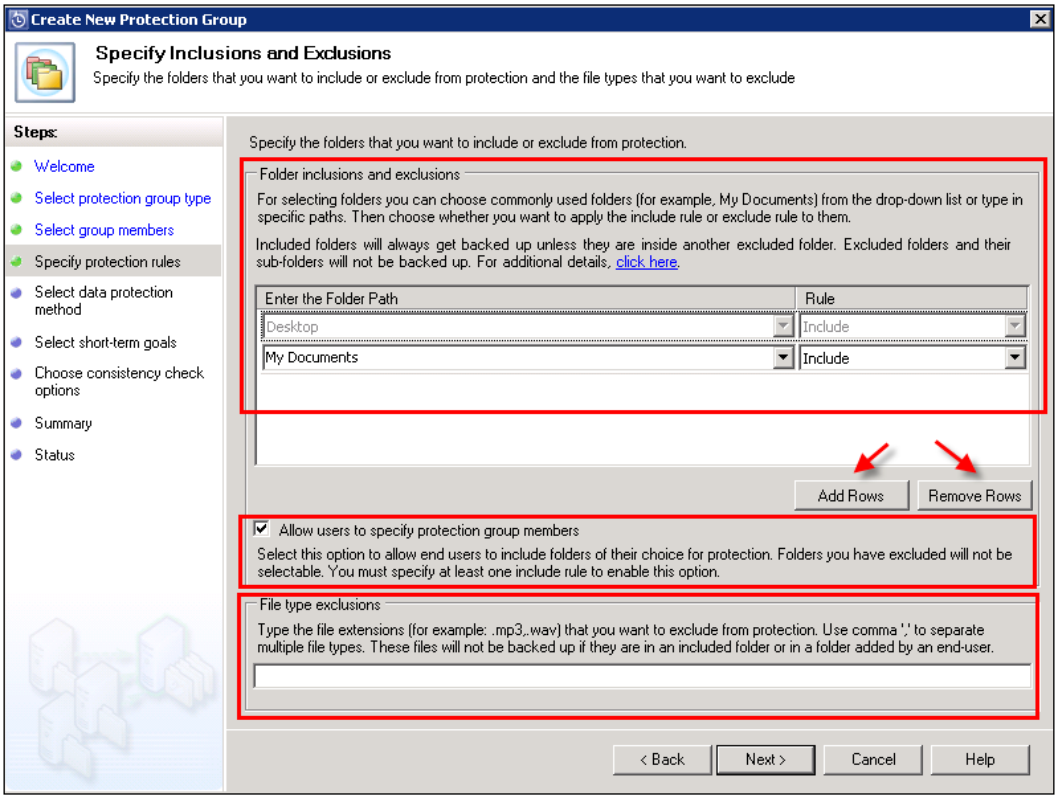


5. Select the client computer you installed the agent on and click **Add** then click **Next**.



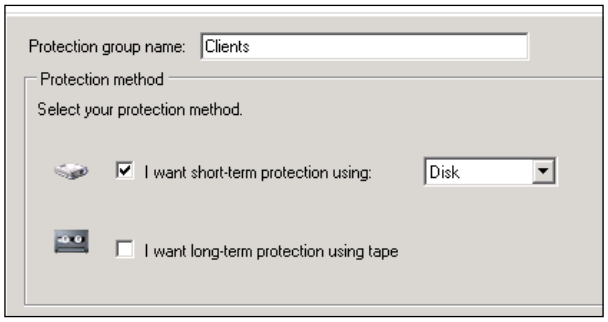
6. On the next screen you can set rules for the client backup. You can choose data on the client computer to include or exclude. You can add rules by clicking on **Add Rows**. You can delete rules by clicking on **Remove Rows**.

In this example we will include the **Desktop** and **My Documents** folder. There is an option here to exclude file types from the backup. One useful feature is to allow the end-users to choose other folders they want to be included in the backup. You can give this permission to the end-users by checking **Allow users to specify protection group members**. Once you have your entire configuration set click **Next**.

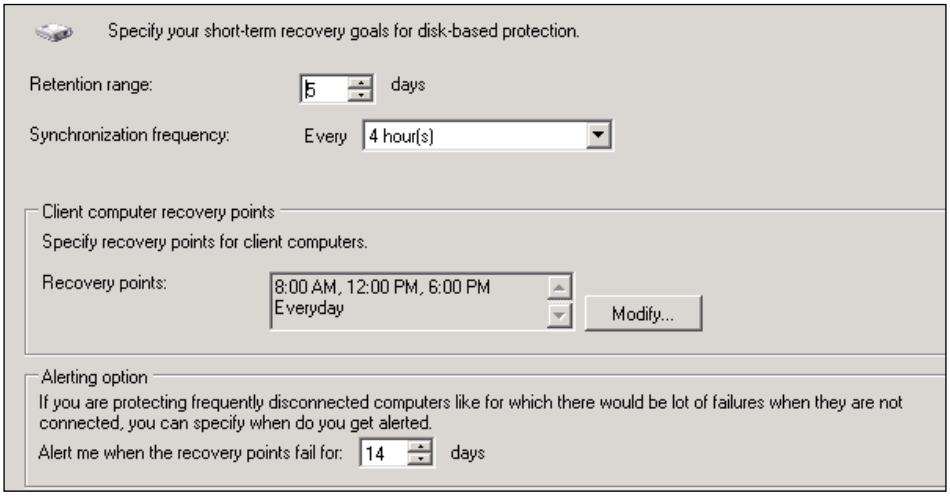


This should be displayed after the diagram featured below:

1. Name your Protection Group. Click **Next**:

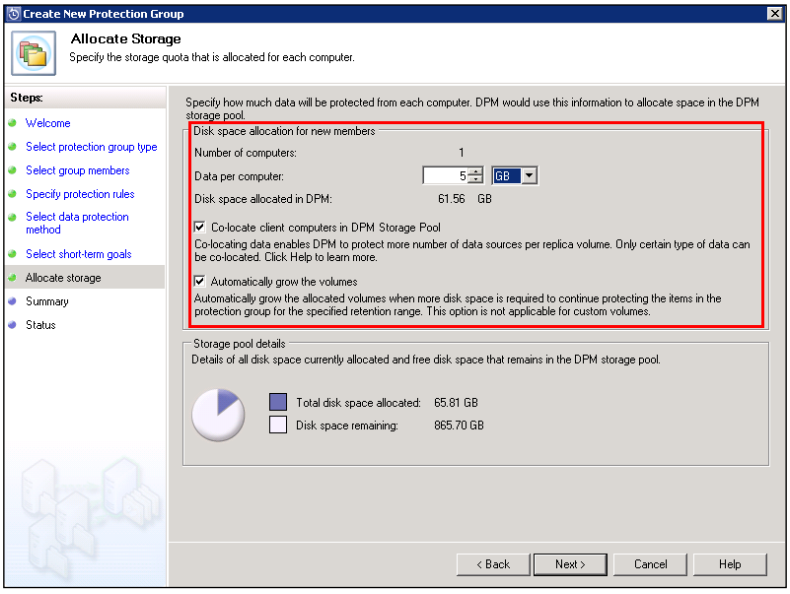


2. Set your **Retention range**, **Synchronization frequency**, and **Recovery points** schedule. Click **Next** to continue:

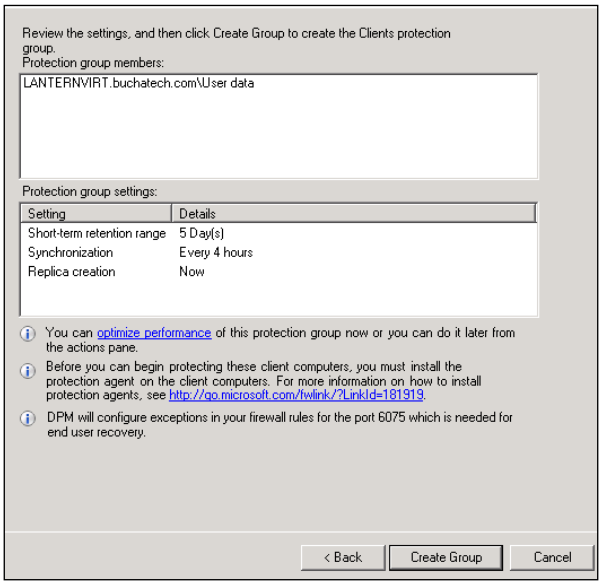


NOTE: If a client misses the Synchronization time; the clients sync won't restart upon connection to the network that DPM is on. It will try to sync again at the scheduled time in the protection policy. This is the amount of days set on the **Alerting option**. You can launch a manual sync from either the DPM client or from the DPM Administrator Console itself. By default DPM sets the **Alerting option** to 14 days before it will alert the end-user that the DPM administrator will get an alert that the sync has not happened.

3. Here you can specify a space limit as to how much data can be backed up on each client. By default it limits it to 5 GB of space. Choose the other defaults and click **Next**:



4. The next screen is a summary. Click **Create Group** to finish creating the Protection Group for your clients:



Summary

In this chapter we covered some very important details of configuring DPM. As a DPM administrator it is necessary to understand how to install the DPM agent and add protected computers to Protection Groups. Protection Groups are a collection of data sources that share a common configuration for protecting them. This chapter covers details of backing up file servers and System State. The System State can backup only system components. You should also have knowledge of the DPM client and backing up in workgroups and untrusted domains.

In the next chapter we will get into backing up application-specific servers.

7
Backing Up Critical Applications

Every business has critical applications that the business and its users depend on from day to day. These applications need to stay up and keep running and if they go down the time to get them back up has to be fast. These are beyond just file shares and user data. These applications are things like e-mail, customer data, financial data, virtualized servers, inventory systems, websites, and more. Some specific applications are Exchange, CRM, SharePoint, PBX phone systems, and ERP systems such as Dynamics AX 2009 and SAP (if it is running on SQL Server). Many of these applications store their data in databases on Microsoft SQL Server. DPM has the power to back these up and does a really good job of this. Out of the box with an enterprise license, DPM can back up Microsoft SQL databases, Hyper-V virtual machines, Exchange, and SharePoint. Since these applications were developed by Microsoft and DPM was developed by Microsoft, it offers the best integration and backup for them. DPM can back up applications like Microsoft CRM, ISA, PBX, and more. You need to know these applications and which components need to be backed up. For example, to back up CRM you simply need to make sure DPM is backing up the SQL database. If the SQL server that is hosting the CRM database fails you can restore it from DPM to another SQL server and re-point CRM to it in order to get this up and running.

In this chapter, we are going to cover common Microsoft applications that many businesses use today in their environments. The topics include:

- Protecting Exchange with DPM
- Protecting Hyper-V with DPM
- Protecting SharePoint with DPM
- Protecting SQL Server with DPM
- Protecting ISA Server 2006 with DPM

Protecting Exchange with DPM

> *Microsoft Exchange Server is a client/server solution with Exchange being the server side and Outlook being on the client side. Exchange is a messaging and collaborative application. Exchange is widely used in businesses it has about 65% of the market share of all organizations according to Ferris Research.*

`http://www.ferris.com/2008/01/31/email-products-market-shares-versions-deployed-migrations-and-software-cost/`

Exchange consists of e-mail, calendaring, contacts, and tasks. Exchange also includes support for mobile and web-based access. DPM offers tight integration with Exchange. DPM is able to back up Exchange and makes this process easy. We will cover configuring DPM to back up Exchange.

It is recommended that you use a utility called **Eseutil** on DPM when protecting Exchange. Using this utility is recommended because DPM will use the utility to perform consistency checks on the data that is written to disk or tape to make sure it is not corrupt. Using the utility will minimize the load that is put on the Exchange server from the backup; the utility does this by offloading the resources used by Eseutil on the DPM server instead of on the Exchange server. If you do not use this utility you will see this warning when trying to protect Exchange through DPM. This is the warning that you will see:

> *Eseutil consistency check cannot be performed for this protection group, as eseutil.exe is not present on the DPM server.*

Copy the following files from the Exchange server installation folder to `C:\Program Files\Microsoft DPM\DPM\bin\`on the DPM server:

- `Ese.dll`
- `Eseutil.exe`

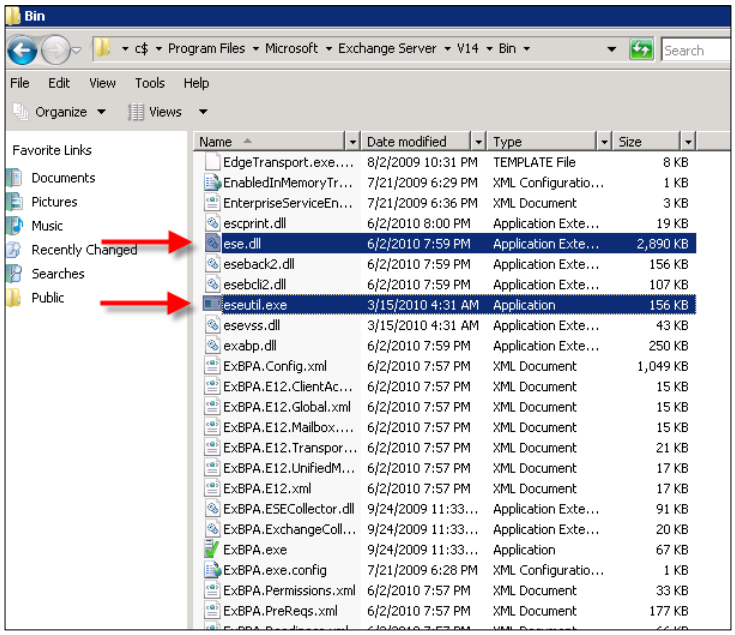
You can also choose not to run the `Eseutil` consistency check for this protection group, by un-checking the **Run Eseutil Consistency check** option. However, this is not recommended because it will not ensure the recoverability of the protected data.

As the warning states using the Eseutil is not required but is recommended. In the following example we will walk through copying the proper files so DPM will use the Eseutil utility. Eseutil is an internal utility that ensures good health of the Exchange stores in 2007 or the DAG databases in 2010. It is used to verify, modify, and repair Exchange stores and databases. DPM uses Eseutil to verify the integrity of Exchange and reports the status of backups back to Exchange after it is done.

NOTE: In the case of protecting Exchange 2003 if the Eseutil for 2003 does not work, you will need to get the Eseutil for 2010. It is backward compatible and you will be able to use this one.

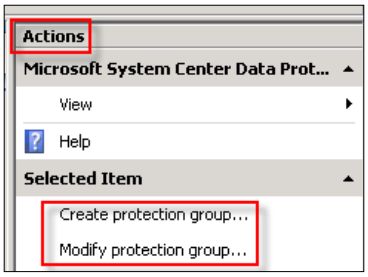
Here are the steps to start protecting your Exchange servers with DPM:

1. On your DPM server navigate to the `\\EXCHANGESERVER\c$\Program Files\Microsoft\Exchange Server\V14\Bin` directory on the Exchange server.
2. Copy the `ese.dll` and `eseutil.dll` files from the Exchange server to the `\\DRIVEEXCHANGEISINSTALLEDON)\Program Files\Microsoft DPM\DPM\bin` folder on your DPM server:



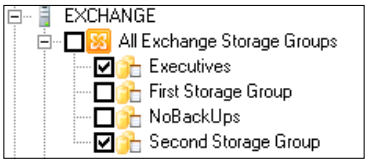
3. Go to the DPM Administrator Console.
4. Click on the **Protection** tab.

5. Click on either **Create protection group** or **Modify protection group** if you already have one created:

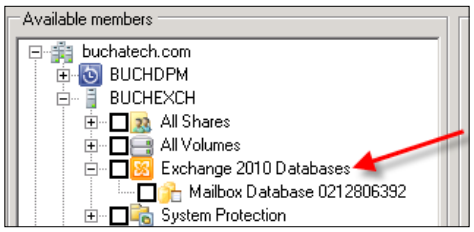


6. Expand the **Exchange** server.
7. Expand the **Exchange 2007 Database** or **Exchange 2010 Database** and select the storage groups or the DAG databases you want to protect.

   Example of Exchange 2007:

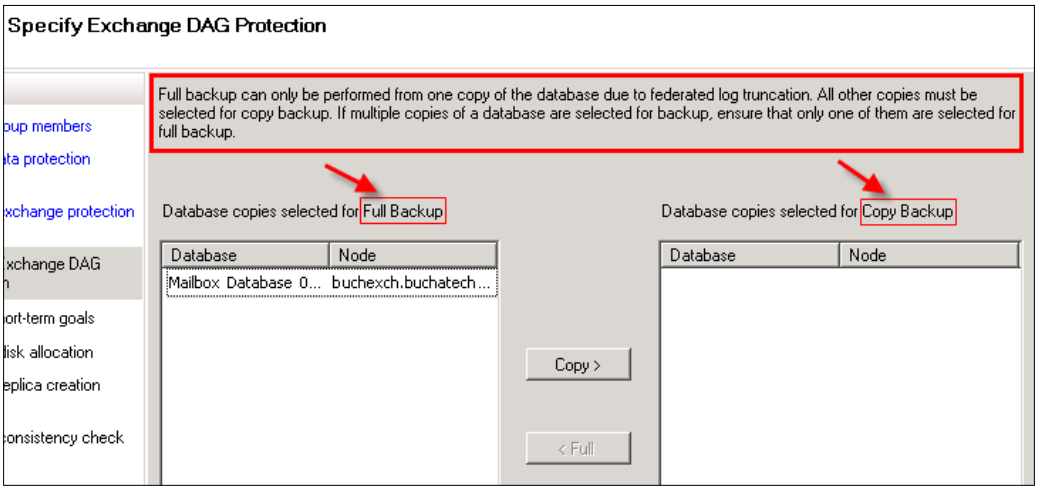


   Example of Exchange 2010:



   Click **Next**.

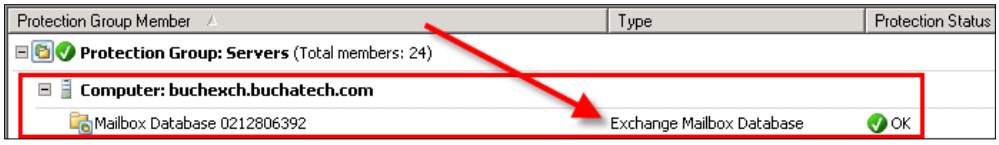
8. If you have multiple Exchange databases move all except one to Copy Backup and click **Next**:



NOTE: DPM can only make a full backup on one Exchange database.

9. Click **Next** on the following four windows.
10. Click **Update Group** or **Create Group** to add Exchange to the protection group.

When it is done you will see a result of **Success** and your Exchange data will now be protected. The following screenshot is an example of what your Exchange data will look like in a protection group when it is protected by DPM:



For more information on backing up Exchange with DPM download this whitepaper:

`http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=be885d26-25e5-41ff-afc8-506414aed960`

Protecting Hyper-V with DPM

In recent years virtualization has exploded in information technology. Many companies today utilize virtualization to cut costs and scale down their environments. Microsoft entered the market with Hyper-V and many businesses began using this as their hypervisor of choice. When DPM was made it was made with the intention to natively backup Hyper-V. This ensures that the back ups of a Hyper-V environment will simply work. DPM is Hyper-V aware out of the box.

DPM supports two methods of protecting Hyper-V. DPM is capable of both host protection with the agent being installed on the Hyper-V host or guest based protection with the agent being installed on the guest virtual machine and both at the same time with the agent being installed on the host and inside the virtual machine. With DPM host based protection the entire virtual hard drive is backed up. This means when you go to restore you have to restore the entire virtual hard drive. With DPM agent based backup the data on the guest virtual machine can be backed up just like a physical server. This includes Microsoft applications that DPM is aware of such as SQL or Exchange. Both are viable options for protection and function well. It is totally left up to preference on what type of backup method you would prefer to use.

DPM offers two backup options for Hyper-V they are:

- **Online backup**: This means that the guest virtual machine is running Hyper-V integration tools and can be backed up without being taken offline. These operating systems support Hyper-V integration tools: Windows Server 2008 R2, Windows Server 2008, and Windows Server 2003. When Hyper-V integration tools are installed on the guest virtual machine DPM uses the VSS service running in the guest virtual machine to perform the back up while the guest virtual machine stays online. This is also known as a VSS request.
- **Offline backup**: This is used for non-Microsoft operating systems and legacy Microsoft operating systems. Examples of non-Microsoft operating systems are Linux or Mac. Legacy Microsoft operating systems are Windows NT 4.0 and Windows Server 2000, Windows 2000, Windows ME, Windows 98/95 and 3.1. In offline backup mode DPM pauses the guest virtual machine for a brief moment while it takes the backup and then brings the guest virtual machine back online. This is the only way you can actually protect Linux or other non-Microsoft operating systems. DPM can store up to 512 shadow copy backups of virtual hard drives.

Both backup options utilize Hyper-V's VSS writer service to back up the VHD's (Virtual Hard Disks) at the block level and will synchronize any changes. This is called Express Full backup.

DPM requires some Windows updates to be applied on your Hyper-V host before DPM can protect the virtual machines on that host. These Windows updates are:

- For Windows Server 2008 (`http://support.microsoft.com/kb/948465`) and (`http://support.microsoft.com/kb/971394`).
- For Windows Server 2008 R2 (`http://support.microsoft.com/kb/975354`).

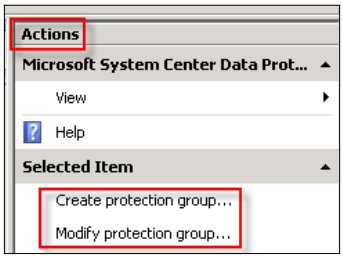
If you do not have these Windows' updates installed when you go to add protection to your virtual machines you will receive the following error:

> *One or more prerequisites for protecting this data source is missing.*
>
> *Ensure that the following prerequisite software is installed on BUCHSRV1.buchatech.com:*
>
> *Windows Server 2008 with*
>
> *Knowledge Base article 948465 (http://support.microsoft.com/kb/948465)*
>
> *AND*
>
> *Knowledge Base article 971394 (http://support.microsoft.com/kb/971394)*
>
> *- OR -*
>
> *Windows Server 2008 R2 with*
>
> *Knowledge Base article 975354 (http://support.microsoft.com/kb/975354)*
>
> *If you have already installed the required prerequisite, refresh the agent status in the management tab and try again.*
>
> *ID: 31313*

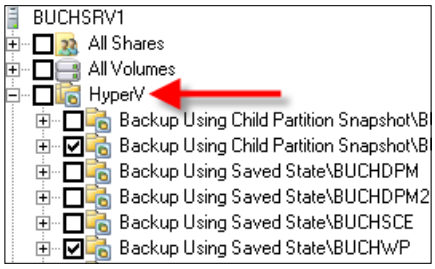
Here are the steps to start protecting your Hyper-V environment:

1. Go to the DPM Administrator Console.
2. Click on the **Protection** tab.

3. Click on either **Create protection group** or **Modify protection group** if you already have one created:



4. Expand the server running the Hyper-V role.
5. Expand **HyperV** and select the virtual machines you want to protect:

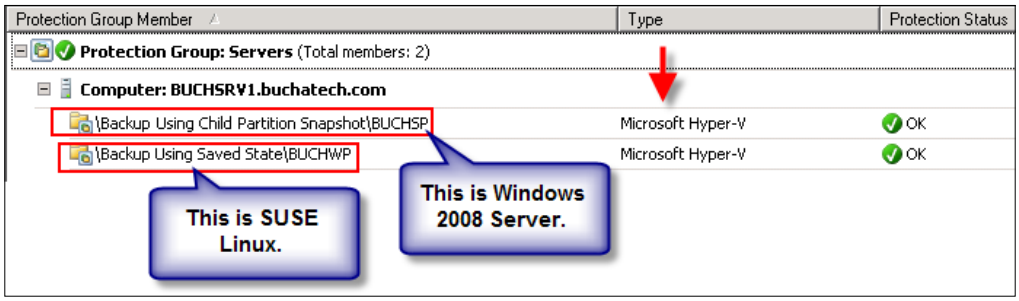


6. Click **Next** on the following five screens.
7. Click **Update Group** or **Create Group** to add Hyper-V to the protection group.

When it is done you will see a result of **Success** and your virtual machines will now be protected.

One way to tell if DPM is using Online or Offline backup is by looking at the Protected Members in your protection group. *If DPM is using the Online backup method the Protection Member will be listed as a Child Partition Snapshot.* This means that the virtual machine is using VSS and it has integration services installed.

If the virtual machine in the Protected Member is showing Saved State it is a Legacy Windows operating system or a non-Microsoft operating system such as Linux. Once again these virtual machines will be paused and then a snapshot will be captured and synched to DPM. DPM will then resume the virtual machine to its current state. There is an example of this in the following screenshot:



Protecting SharePoint with DPM

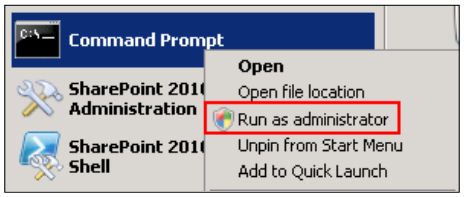
SharePoint is a portal, collaboration, file sharing, web publishing application and more. SharePoint has become a critical business application in many companies today. DPM was built specifically to back up Microsoft workloads, with SharePoint being one of them. Other backup solutions have a more generic approach to backing up specific applications like SharePoint. The majority of these SharePoint backup solutions offer full restores only with no granular recovery of individual items. They are complex to set up and configure, requiring some level of training. However there are some SharePoint backup tools out there in the market that do a good job at backing up SharePoint offering granular restore, easy set up and configuration such as DocAve Backup and Recovery by AvePoint as well as Recovery Manager for SharePoint by Quest. DPM falls into the category of a good backup solution for your SharePoint. DPM is easy to configure for SharePoint backup and with the release of DPM 2010 it can restore down to the item level which you will see in *Chapter 8*. With the release of SharePoint 2010 a recovery farm is no longer required to perform restores, DPM 2010 takes full advantage of this feature so that you can perform a restore without a recovery farm right from DPM to your SharePoint.

DPM uses VSS to back up open and in use files. Other backup solutions do not always utilize VSS as they are built to back up static closed files. DPM backs up the SharePoint server farm, SharePoint sites, document libraries, lists, documents, and other objects. DPM uses byte-level replication and integrity checking. DPM can also back up SharePoint service applications.

Before you can back up SharePoint with DPM the configurations and prerequisites have to be met. We are going to cover these requirements as well as the steps to protect your SharePoint environments.

The following are the steps to start protecting your SharePoint environment:

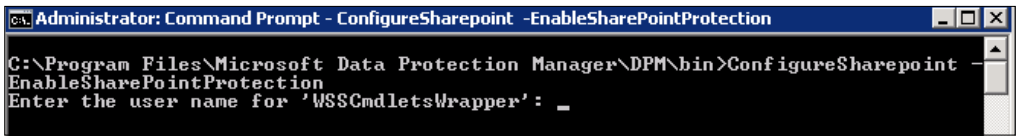
1. On the *SharePoint Web Front End* open up an elevated command prompt.



2. Change the directory to `C:\Program Files\Microsoft Data Protection Manager\DPM\bin`. Use the command:

   `cd C:\Program Files\Microsoft Data Protection Manager\DPM\bin`

3. Type `ConfigureSharepoint -EnableSharePointProtection` and press *Enter*.

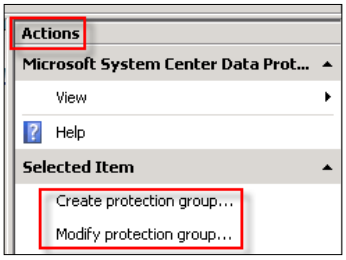


4. Enter the user name and password of a farm administrator account then press *Enter*.

5. When completed, you will see a message verifying that it was completed successfully.

NOTE: If your SharePoint farm administrator password changes you will need to run `ConfigureSharePoint-EnableSharePointProtection` again to update the DPM backup with the proper credentials.

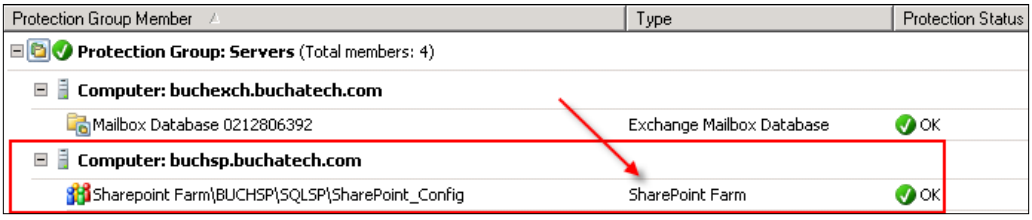
6. Go to the DPM Administrator Console.
7. Click on the **Protection** tab.
8. Click on either **Create protection group** or **Modify protection group** if you already have one created:



9. Expand the server running **SharePoint**.
10. Expand SharePoint and select the SharePoint configuration:

11. Click **Next** on the following five windows, if no further protection group configuration changes are required.
12. Click **Update Group** or **Create Group** to add your SharePoint to the protection group.

You will now be able to see in your Protection group that your SharePoint farm is being backed up. All web applications will be automatically included in this backup. You will be able to restore the entire SharePoint farm, SharePoint sites, document libraries, lists, documents, and other objects. We will cover this in *Chapter 8*. The following screenshot is an example of what your SharePoint data will look like in a protection group when it is protected by DPM:



Protecting SQL Server with DPM

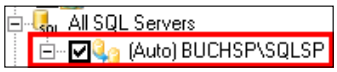
Many companies rely on Microsoft SQL Server to run their business. Whether your company uses it directly or not, chances are one of your critical business applications stores its data in a SQL database. Some examples of applications that store data in SQL are SharePoint and CRM. As you can see backing up SQL is an important task. It is a good thing DPM does a good job of backing up SQL. Unlike other backup systems DPM was designed specifically to back up SQL Server. This makes DPM one of the best backup solutions for SQL. Even though DPM can only back up as often as 15 minutes it still gives an administrator the power to restore to any transaction point.

DPM makes an initial baseline back up of the SQL databases it is backing up. DPM then performs Intelligent Application Protection on SQL in two ways:

- SQL transaction logs are continually synchronized to the DPM server
- The SQL Server VSS Writer service identifies blocks that have changed in the entire database and sends only the updated blocks to DPM

DPM can protect up to 2000 databases per DPM server and can store up to 512 shadow copes of each SQL database. DPM can only protect SQL 2000 SP4, SQL 2005, SQL 2008, and SQL 2008 R2. SQL is the easiest application to back up with DPM because there are no special prerequisites or configurations you have to make on your SQL server. DPM recognizes SQL data right out of the box. As soon as you have your agent installed and go to add your SQL server to a protection group, DPM knows that the server contains SQL data on it.

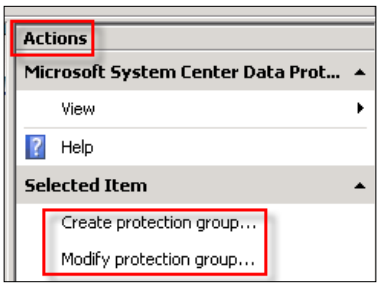
DPM 2010 can protect SQL servers at the instance level. This means that when new databases are created on that instance DPM can automatically start protecting them. To not use this feature select only the databases you want to back up when modifying or creating a new protection group. To use this feature simply select the entire instance when modifying or creating a new protection group. See the following screenshot as it shows selecting a SQL instance:



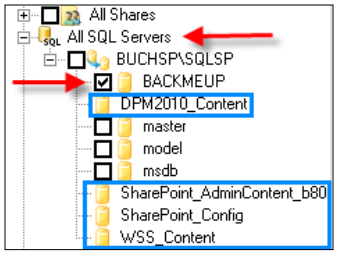
NOTE: When you checked the box next to the SQL instance DPM adds **(Auto)** next to the SQL instance name. This means that the automatic SQL database protection is turned on. The next time a database is added to the instance it will be automatically protected.

Now we are going to cover adding SQL databases from a SQL instance to a protection group in DPM. The following are the steps to start protecting your SQL databases:

1. Go to the DPM Administrator Console.
2. Click on the **Protection** tab.
3. Click on either **Create protection group** or **Modify protection group** if you already have one created:



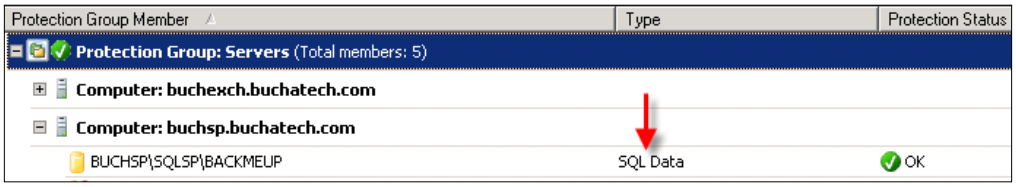
4. Expand your SQL server.
5. Expand **All SQL Servers**.
6. Expand the SQL instances you want to protect data on.
7. Select the SQL databases that you want to protect:



NOTE: In the previous screenshot some of the databases, the ones that are outlined, do not have checkboxes next to them. This is because they are SharePoint databases and are already protected as SharePoint protection members. You do have the option to simply protect SharePoint databases here but you will not have the same benefits DPM 2010 offers by protecting your SharePoint environment as a SharePoint data type in DPM. It is recommend to use the built-in SharePoint protection.

8. Click **Next** for the next five windows if no further protection group configuration changes are required.
9. Click **Update Group** or **Create Group** to add your SQL databases to the protection group.

The following screenshot is an example of what your SQL data will look like in a protection group when it is protected by DPM:



Protecting ISA Server 2006 with DPM

ISA server 2006 is a software based multi-featured and multi-purpose firewall security gateway. ISA can protect against external and internal web-based threats through its firewall and offers advanced protection such as intrusion detection. ISA is used as a remote access tool by publishing applications such as Exchange OWA, SharePoint, and Microsoft CRM. ISA can also provide a VPN service and act as a load balancer. Lastly, ISA can be a web cache server and provide routing to connect multiple sites. ISA is a powerful tool that is used in many businesses. It is another business tool that needs to be backed up.

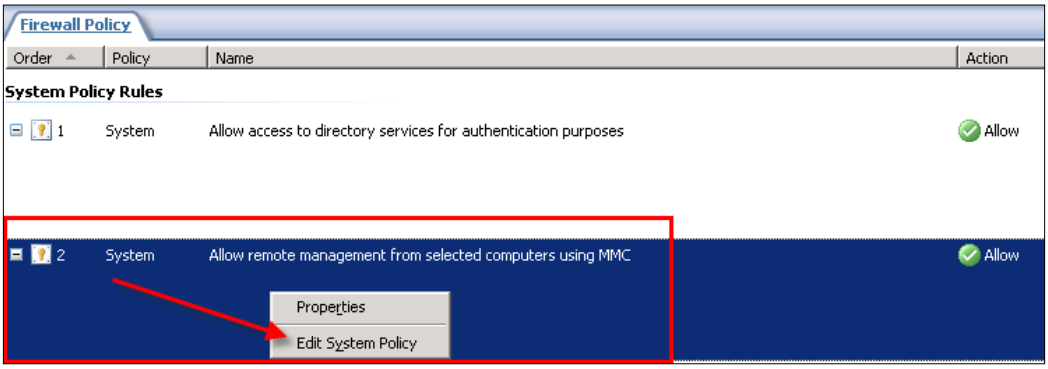
DPM was not designed to natively back up ISA like it has been for all of the previous applications. This is because ISA server configurations do not typically change that often, hence there is no need for intelligent protection of it. ISA is not like SharePoint, Exchange, or SQL that constantly change. Administrators typically schedule or manually back up ISA through its built-in export function. Administrators then copy the XML backup file to a network share that DPM can access and that is how they back up ISA with DPM. Time could be saved by scheduling the ISA exports and if DPM could back up the ISA server configuration directly.

While surfing the internet and seeing many forum posts asking how to properly backup ISA with DPM it was decided to add information on how to do this. We will cover the steps you need to take to allow the DPM agent to be installed and to begin protection your ISA server from DPM. The following are the steps to start protecting your ISA 2006 server.

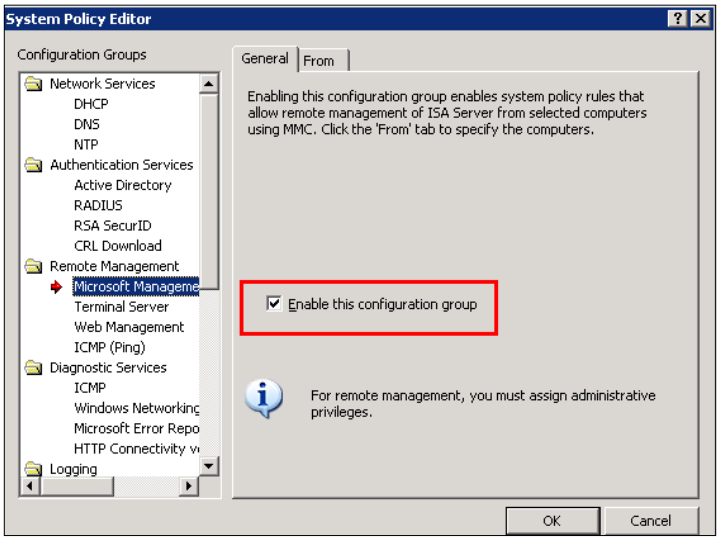
First, you need to configure firewall settings within ISA to allow ISA and DPM to communicate properly. Here are the steps to configure the ISA firewall:

1. Open the **ISA Server Management** MMC.
2. Expand **Arrays**, expand the **ISA Server computer**, and then click **Firewall Policy**.
3. On the **View** menu, click **Show System Policy Rules**:

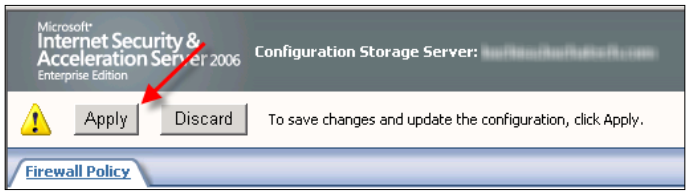
4. Right-click on the **Allow remote management from selected computers using MMC** system policy rule. Select **Edit System Policy**:



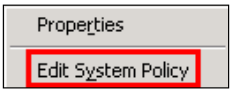
5. In the **System Policy Editor** dialog box, click to clear the enabled check box, and then click **OK**:



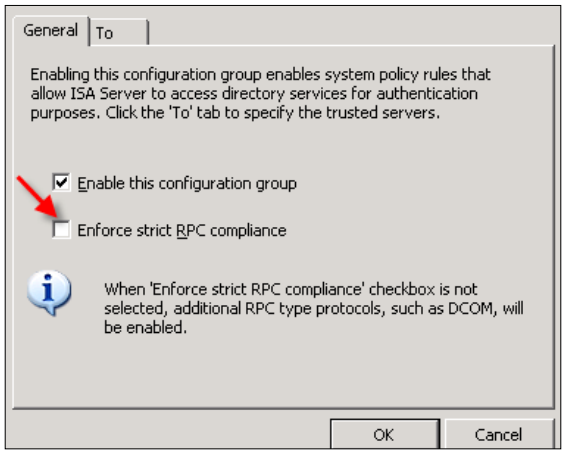
6. Click **Apply** to update the firewall configuration, and then click **OK**:



7. Right-click on the **Allow RPC from ISA server to trusted servers** system policy rule. Select **Edit System Policy**:

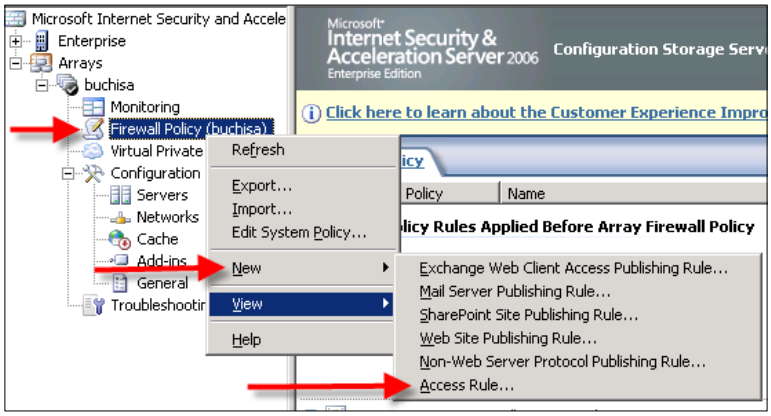


8. In the **System Policy Editor** dialog box, click to clear the **Enforce strict RPC compliance** check box, and then click **OK**:



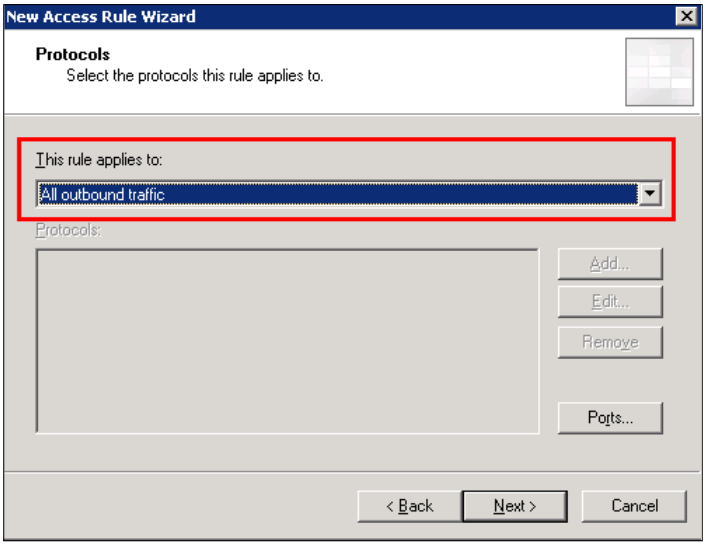
9. Click **Apply** to update the firewall configuration, and then click **OK**.
10. On the **View** menu, untick **Show System Policy Rules**:

11. Right-click on **Firewall Policy**. Select **New**, select **Access Rule**:

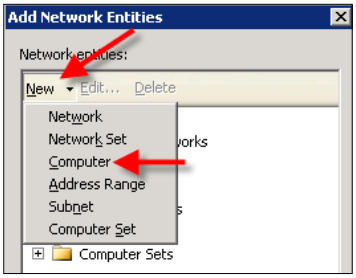


12. In the **New Access Rule Wizard**, type a name in the **Access rule name** box. Click **Next**:

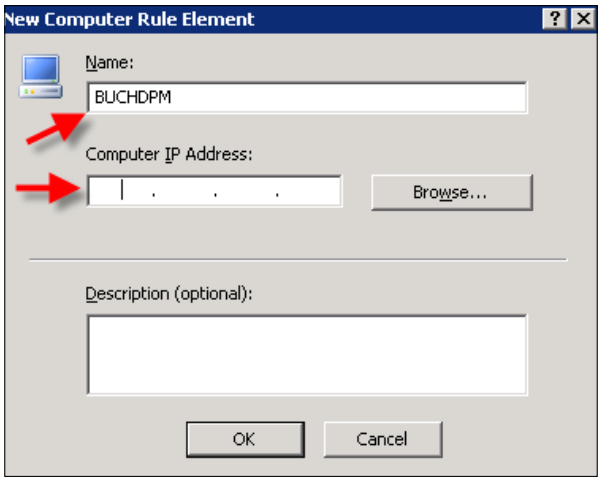
13. Choose **Allow** and then click **Next**.
14. In the **This rule applies to** list select outbound traffic from the drop down and click **Next**:



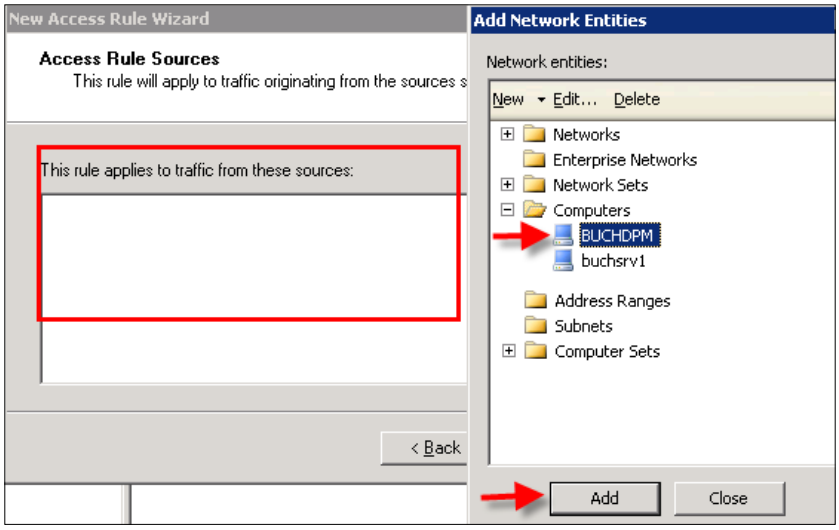
15. On the **Access Rule Sources** page, click **Add**.
16. In the **Add Network Entities** window, click **New**, and select **Computer** from the drop down:



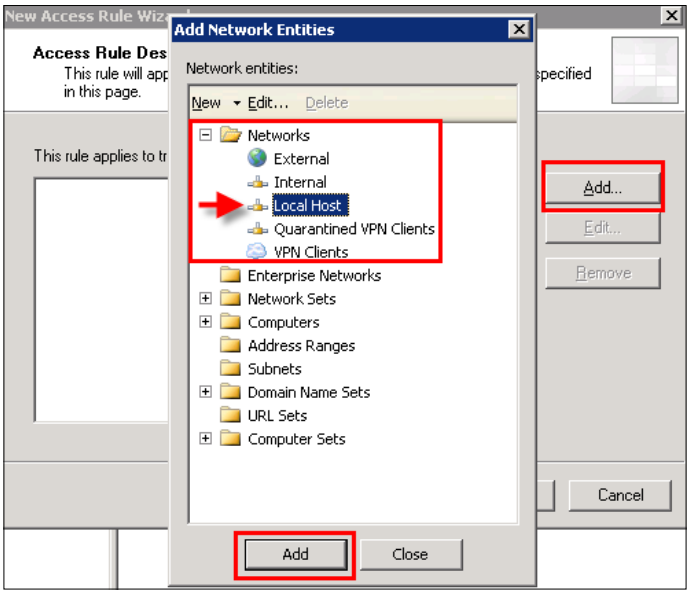
17. Now type the name of your DPM server and type the DPM server's IP Address in the **Computer IP Address** field. Click **OK** when you are done:



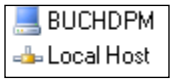
18. You will then see the DPM server listed under the **Computers** folder in the **Add Network Entities** window. Highlight it and click on **Add**. It will then bring the DPM computer into your **Access rule**. Click **Next**.



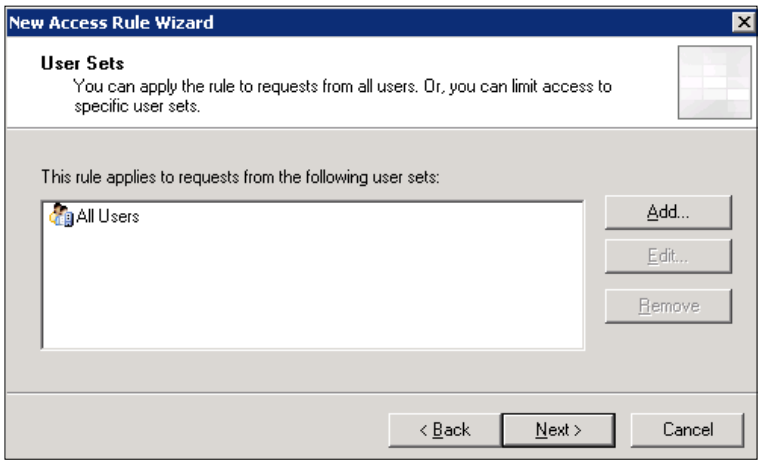
19. In the **Add Rule Destinations** window, click **Add**. The **Add Network Entities** window will come up again. In this window expand **Networks**, select **Local Host**, and click **Add**:



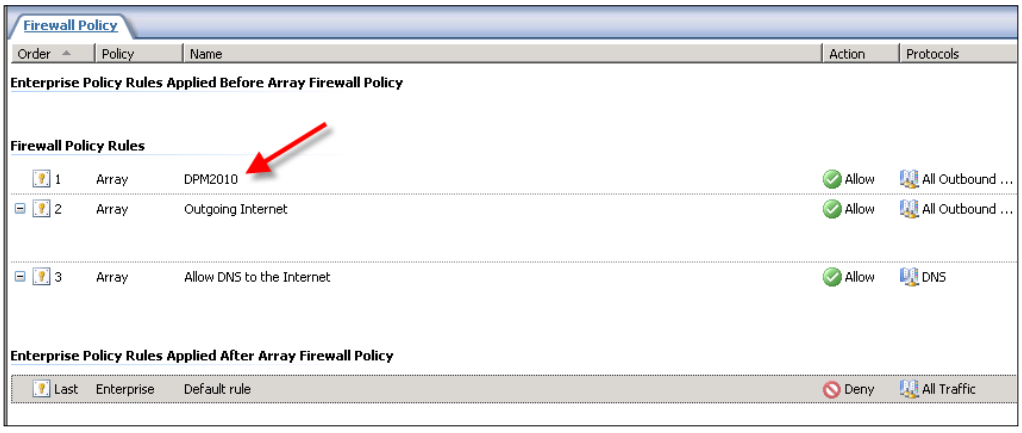
20. Now click **Next**. Your rule should have both the DPM server and local host listed for both incoming and outgoing.



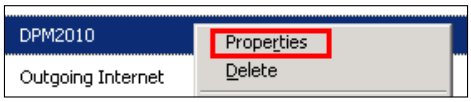
21. Click **Next**, leave the default **All Users** entry in the rule applies to requests from the following user sets box. Click **Next** again.



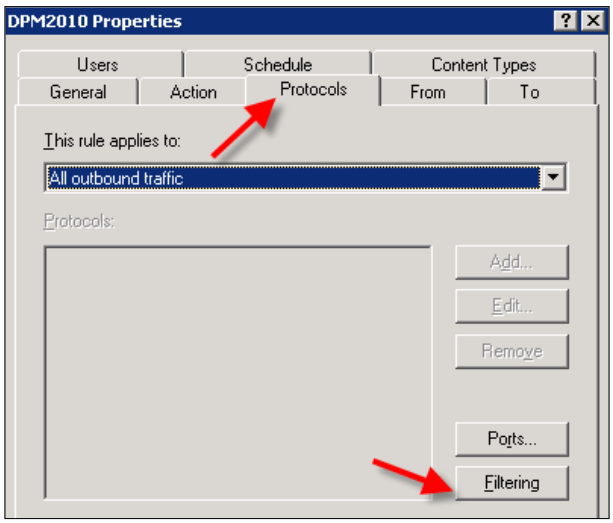
22. Click **Finish** once you complete the **New Access Rule Wizard**.
23. Right click on the new rule (**DPM2010** in this example), and then click **Move Up**.



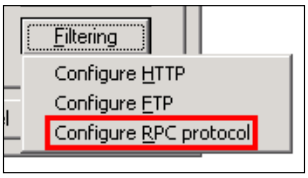
24. Right-click on the new rule, and select **Properties**:



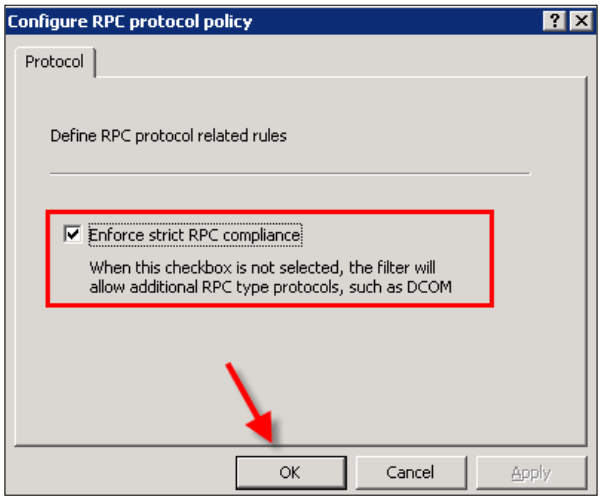
25. In the rule (**DPM2010**) properties dialog box, click the **Protocols** tab and then click **Filtering**:



26. Now select **Configure RPC Protocol**:



27. In the **Configure RPC Protocol policy** dialog box, untick the **Enforce strict RPC compliance** check box, and then click **OK** two times:

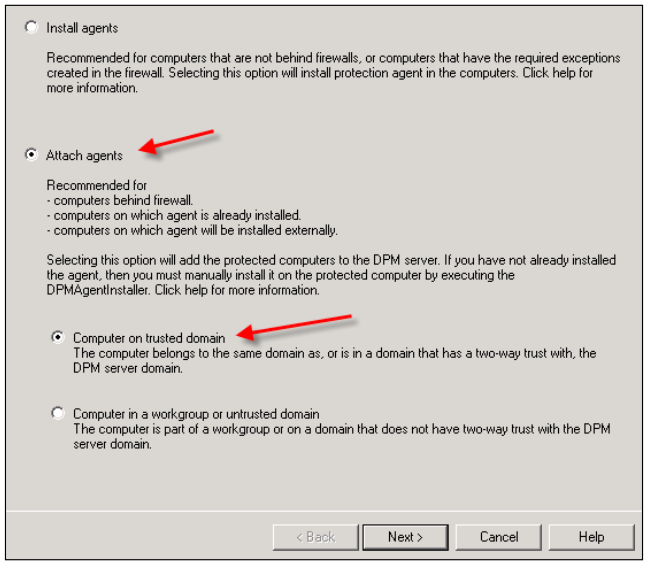


28. Click **Apply** to update the firewall policy, and then click **OK**.

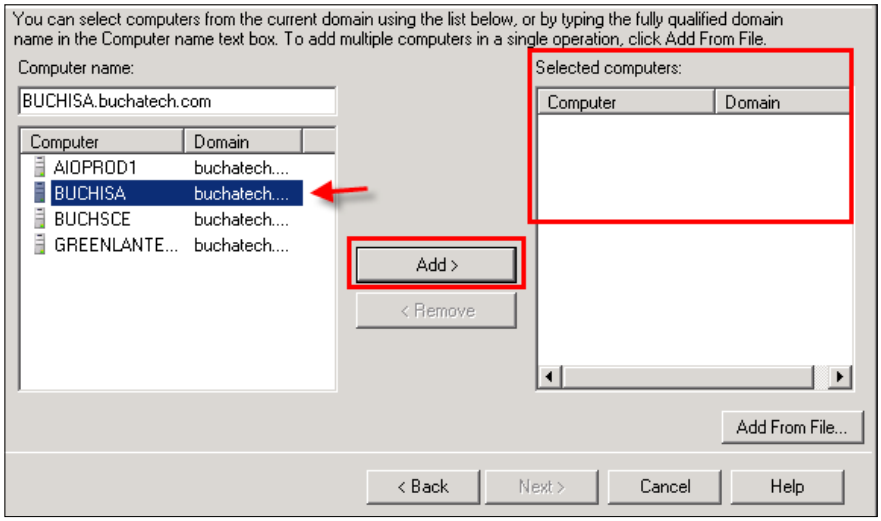
Now you will need to attach the DPM agent for the ISA server. Here are the steps for completing this task:

1. Open the DPM Administrator Console.
2. Click the **Management** tab on the navigation bar.
3. Now click on the **Agents** tab.
4. On the **Actions** pane, click **Install**.

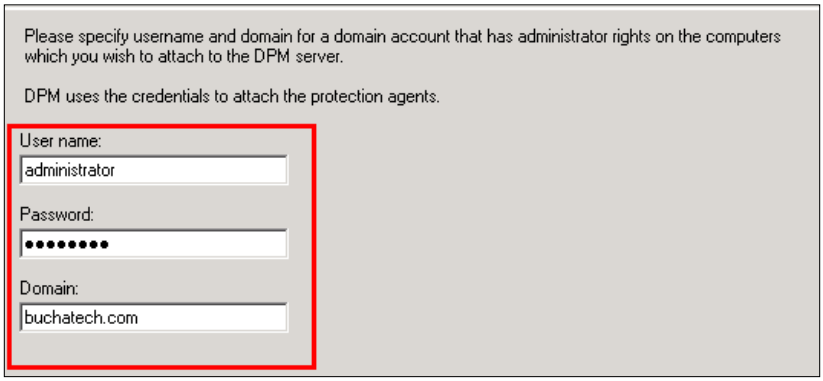
5. Now the **Protection Agent Install Wizard** should pop up. Choose **Attach agents**. Choose **Computer on trusted domain** and click **Next**:



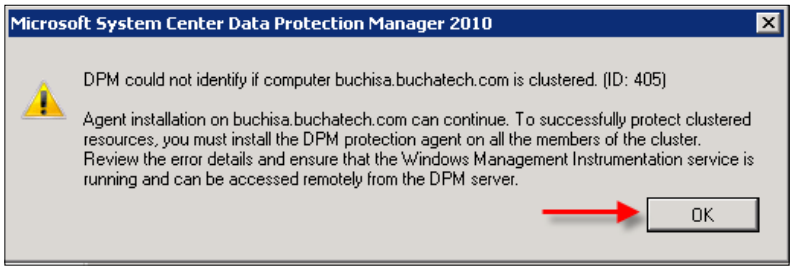
6. Select the ISA server from the list, click **Add**, and then click **Next**.



7. Enter credentials for the domain. The account that is used here needs to have administrative rights on the computer you are going to protect. Click **Next** to continue.



8. You will receive a warning that DPM cannot tell if the ISA server is clustered or not. Click **OK** on this:



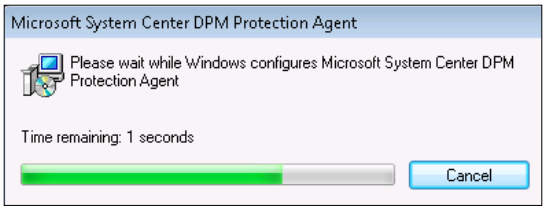
9. On the **Summary** screen click **Attach** to continue.

Now you have to install the agent on the ISA firewall and point the agent to the correct DPM server. Here are the steps to complete this task:

1. From the ISA server you will be protecting, access the DPM server over the network and copy the folder with the Agent installation in it down to the local machine. Use this path:

```
\\DPMSERVERNAME\%systemdrive%\Program Files\Microsoft DPM\DPM\
ProtectionAgents\RA\3.0\3.0.7696.0\i386
```

2. Then from the local folder on the protected computer run `dpmra.msi` to install the agent.



3. Open a command prompt (make sure you have elevated privileges) change directory to `C:\Program Files\Microsoft Data Protection Manager\DPM\bin`. Then run the following: `SetDpmServer.exe -dpmServerName<serverName>userName<userName>`

   For example:

   ```
   SetDpmServer.exe -dpmServerNamebuchdpm
   ```

4. Now restart the ISA server.
5. Once your ISA server comes back up, check Windows services to make sure the **DPMRA** service is set to automatic and start it.

That is it, now you can start protecting your ISA server from DPM.

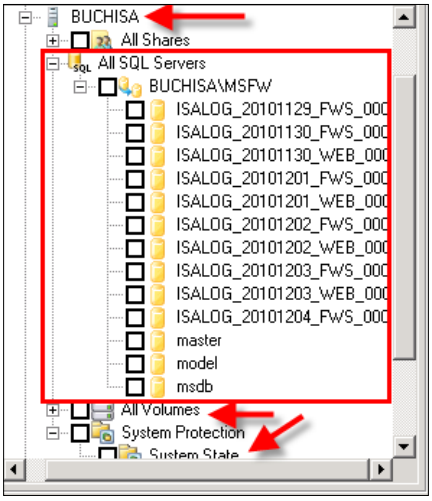
Go back to the DPM Administrator Console on your DPM server and modify your protection group to add ISA. With the ISA backup you can choose to back up certain ISA components depending on your recovery needs. With DPM you can back up the ISA hard drive, ISA logs that are stored in SQL, and ISA's System State. Here is a list of what you should back up depending on your circumstances:

- ISA Configuration Settings (exported through ISA)
- ISA Firewall Settings (exported through ISA)
- ISA Log Files (stored in SQL Databases)
- ISA Install Directory (only needed if you have custom forms for things such as an Outlook Web Access Login screen.)
- ISA Server System State

All of the components are not required except for the ISA settings. The ISA settings contain the settings you will need to get ISA up and running again on a new ISA installation. For more information on backing up ISA 2006 visit:

`http://technet.microsoft.com/en-us/library/bb794757.aspx`

Here is a screenshot of ISA in a protection group. You will notice DPM is able to back up the ISA SQL logs directly, the ISA program files, and the ISA servers System State and DPM can back up the hard drive.



DPM cannot back up the ISA server settings natively. This would need to be scripted and scheduled through Windows Task Scheduler, then placed on the local hard drive. DPM can back up the XML settings exported from there. You can find the ISA server export script at `http://msdn.microsoft.com/en-us/library/ms812627.aspx`. Place this script into a `.vbs` file then set up a scheduled task to run this file. That is how you automate your ISA server settings export.

NOTE: This information on how to back up ISA 2006 with DPM will also work with TMG 2010 (Threat Management Gateway).

Summary

In this chapter we covered protection of Windows application workloads including Exchange, Hyper-V, SharePoint, and SQL Server. Additionally, we covered backing up ISA 2006 which is not natively backed up by DPM. We walked through the steps in order to start protecting all of these critical business applications. This included requirements and configurations that were needed before they could be protected.

In the next chapter we are going to cover the procedures for restoring data in DPM.

8
Recovery Options

In the last two chapters, we looked at backing up servers and applications that are critical today to many businesses. While doing this we also covered how to deploy agents on your standard servers and servers running critical applications. Now that we have covered backing up it is time to now cover restoring data and these critical applications.

It is important to understand what capabilities available and limitations placed in order to restore data and applications in DPM. In this chapter you will get an idea of these. We will first explore recovery options in the DPM Administrator Console as well as recovering files, folders, and shares. Next, you will see how to carry out self service recovery for end-users using the DPM client works. Then we will go into more advanced restores such as BMR (Bare Metal Recovery), and restoring of applications. The applications we will look at restoring are Hyper-V, Exchange, SQL, and SharePoint. You will see the cool features that DPM now offers such as recovering Hyper-V VHDs, or item-level data from within these VHDs, SharePoint item-level restores, and restoring a SQL database to a different instance. This chapter is planned to arm you with the knowledge of what DPM can do in regards to restores, so you can start performing your own restores today. Here are the specific topics we will cover in this chapter:

- General recovery
    - Recovery overview in the DPM Administrator Console
    - Recovering files, folders, shares, and volumes
    - Using self service recovery for end-users through the DPM client
    - Recovering data using System State
- Bare Metal Backup and Recovery
    - What is Bare Metal Backup and Recovery?
    - How to perform a Bare Metal Recovery

- Restoring critical applications with DPM
    - Restoring Exchange mailboxes with DPM
    - Restoring Hyper-V virtual machines with DPM
    - Restoring SharePoint data with DPM
    - Restoring SQL databases with DPM
    - Configuring and using SQL self service recovery for SQL administrators

General recovery

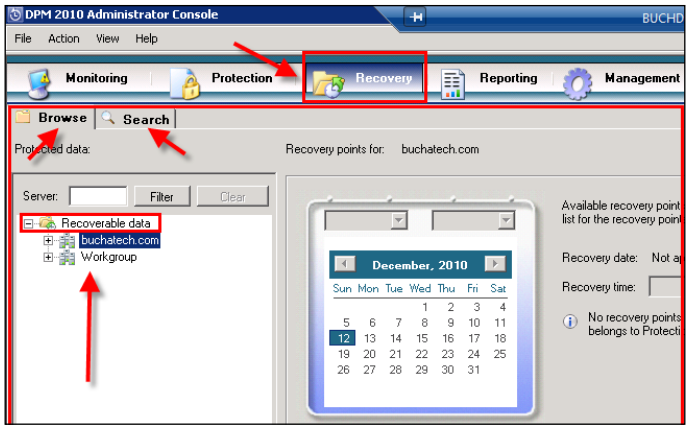
In this section we take a look at the basics of DPM recovery as well as using the DPM client to perform end-user recovery of data.

Recovery overview in the DPM Administrator Console

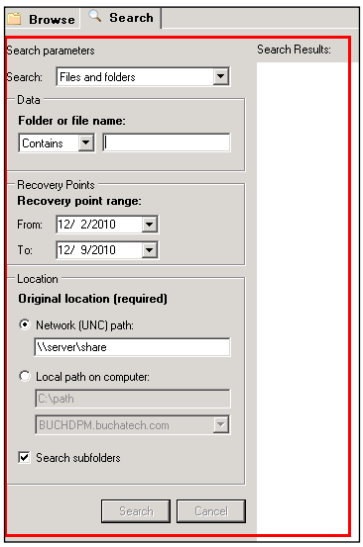
As you know by now DPM creates recovery points of each replica in a protection group. This is when DPM creates a point in time in which you are able to restore data that DPM has protected. DPM makes it possible to quickly and easily recover your protected data. DPM gives you an easy to understand interface and the Recovery Wizard in which to perform the restores. You typically have the option to specify the restore destination to the original location, a file share, or tape. Restoring data for specific applications can offer other restore options which we will cover later in this chapter. DPM gives you the ability to browse or search recovery points for data that is lost. DPM lists the available versions that can be recovered. You can drill down into the protected data to find the specific version that needs to be recovered.

1. To access the DPM recovery section log on to the DPM server.
2. Open the **DPM Administrator Console**; click **Recovery** on the navigation bar.

Here is an example of what the **Recovery** section looks like:



In the preceding screenshot you will notice in the **Recovery** pane that you have two tabs. One tab labeled **Browse** and one labeled **Search**. Notice while on the **Browse** tab the **Recoverable data** folder in the **Protected data** section. This lists all domains and workgroups that contain recoverable data. All the protected computers that you have in your Protection Groups will be listed here. Click on the **Search** tab and you will see that you can enter search parameters such as what type of data you are restoring. The types of data you can restore will depend on what you are protecting. On the server used in this book we have the options to restore files and folders, Exchange mailboxes, and SharePoint data. If you are not protecting SharePoint on your DPM server, SharePoint will not be an option. You also have the option to put in the range that the Recovery Point would have been created in as well as the data's location. This is shown in the following screenshot:



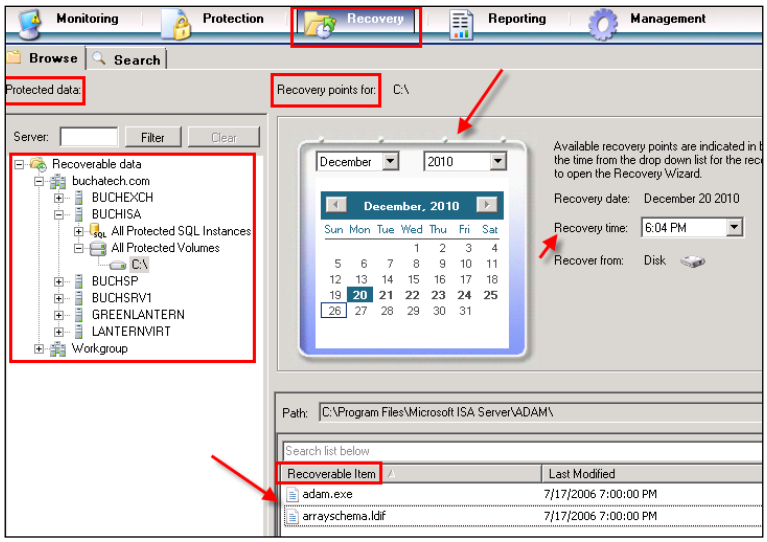
Recovery in the DPM Administrator Console is straightforward, easy to understand and use. We will now go into more detail on recovering data using DPM. You will be able to see the **Recovery Wizard** and different recovery options in action.

Recovering files, folders, shares, and volumes

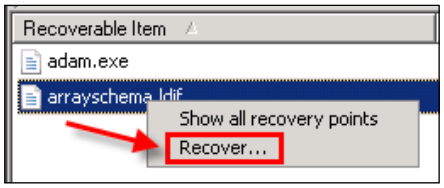
Let's take a look at recovering files, folders, shares, and volumes one step at a time. This type of data will be the most common in your environment. All servers have files, folders, volumes and many have shares. Then client computers have this same data that needs to be protected. The following steps will show how to recover basic data:

1. On your DPM server open the DPM Administrator Console.
2. Click on the **Recovery** tab.
3. Browse or search for the data you want to recover in the **Protected data** section. You can either search for the data or browse for it on the protected server.
4. In the **Results** pane, select the data you want to restore. This can be an entire volume, a share, a folder, or a file.
5. In the **Recovery** section on the calendar, any available recovery points will be indicated in bold. To the right of the calendar will be a drop down box with times that are available for recovery.

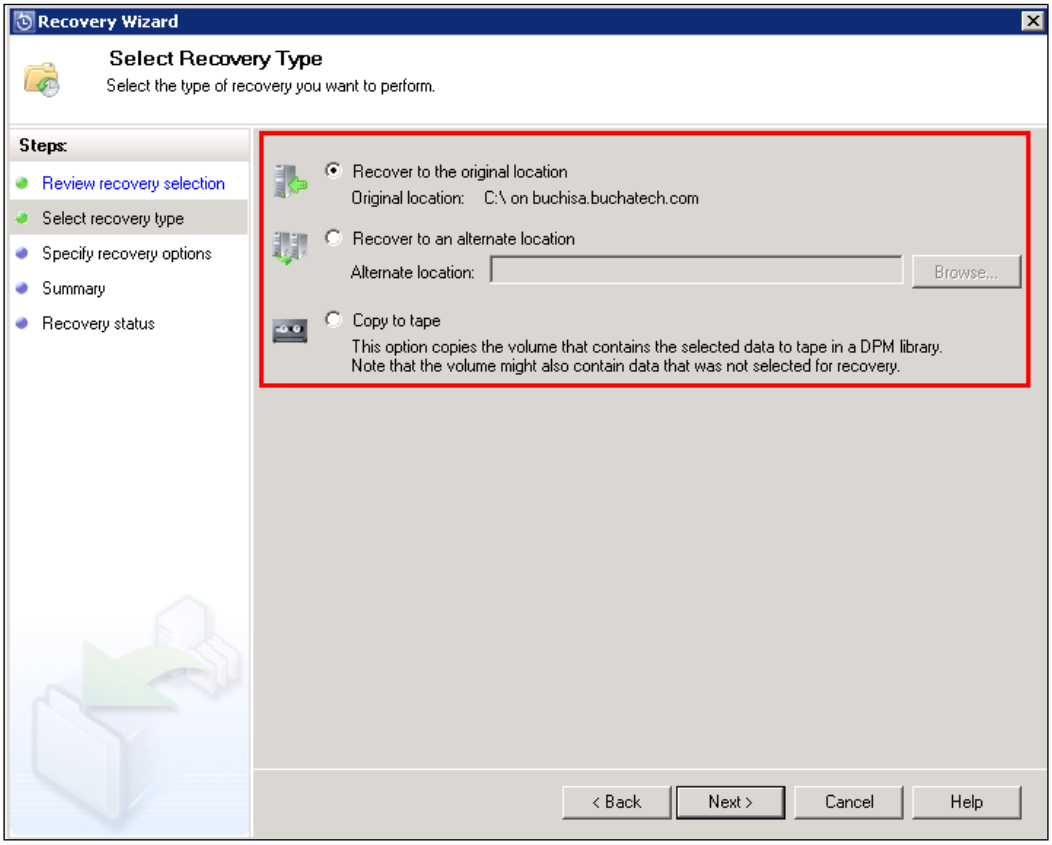
   The **Recoverable item** pane will show the actual items that you can recover such as the volume, shares, folders, or files.



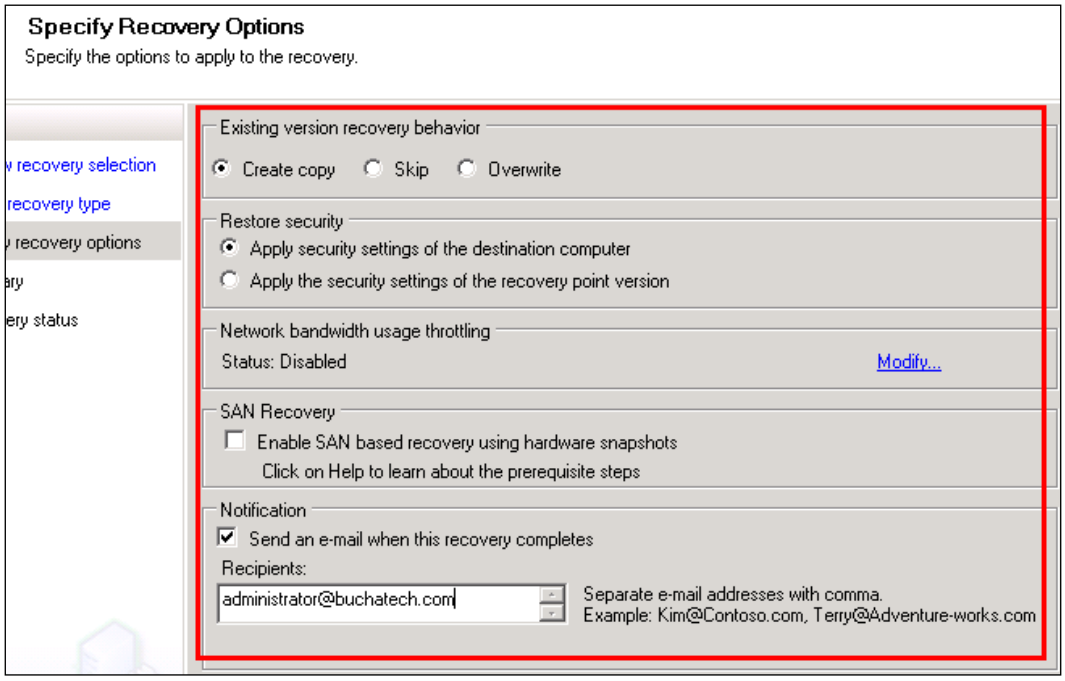
6. When you are ready to start a restore, right-click on the data that you want to restore in the **Recoverable Item** pane and select **Recover**:



7. The DPM **Recovery Wizard** will pop up, make sure your selection is correct then click **Next**.
8. Specify the type of recovery you would like to perform such as to the original location, alternate location, or to tape and then click **Next**:



6. On the next screen you can choose to retain the security settings of the original location, or the new location. At this point you can also choose to add network throttling, SAN recovery, and the behavior in regards to versions. Additionally, you can choose to receive a notification when the restore completes. Click **Next** to continue.



7. On the next screen you have one more chance to review your recovery options. Click **Recover** when ready.

These are all the steps to recover data. These steps will work regardless of whether you are recovering volumes, shares, folders, or files.

Using self service recovery for end-users through the DPM client

DPM client/end-user protection works in two ways. It protects data locally by storing a copy of the data in cache known as shadow copies introduced in Windows Server 2003. The other way is the data is stored on the actual DPM server. This makes it possible to protect clients that are connected to or disconnected from the network. Disconnected clients are typically remote or travelling employees and are required to connect to VPN or Direct Access to sync with the DPM server. As a backup administrator, DPM gives you the ability to let your users restore their own data when needed or to lock it down so that they have to contact you to perform any restores. The benefit in allowing your users to restore their own data is less calls to you. You need two things for client/end-user protection to work properly:

- The first thing is that the end-user recovery needs to be enabled in DPM, this was covered in *Chapter 4*
- The second thing is the DPM client needs to be installed on the protected client computers and this was covered in *Chapter 6*

Once the client is installed, the end-user has the ability to manually synchronize the data on to DPM, recover data from DPM, see what is being protected, and, if the user has the permission, add more content to be backed up.

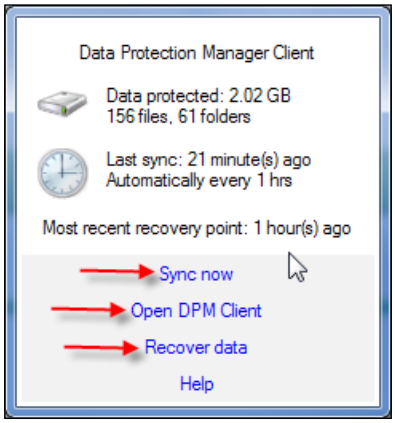
NOTE: Synchronizing is typically done based on a schedule you set in DPM.

The client can be opened on the client computer by doing the following:

1. Clicking on the **Start** button, then **All Programs**.
2. Click on **Microsoft System Center Data Protection Manager 2010** to expand it.
3. Click on the **Data Protection Manager Client** to launch it.

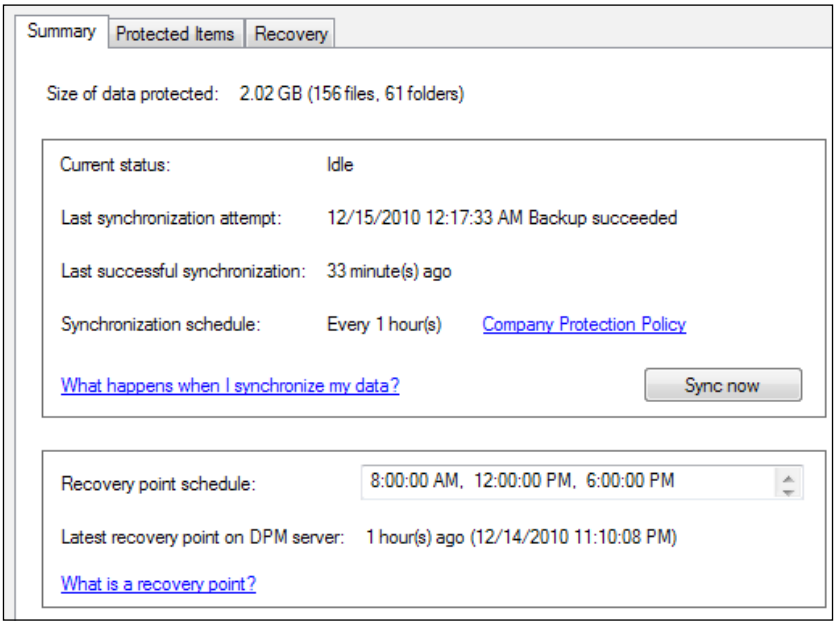
Once you launch the DPM client you will notice a DPM icon in your taskbar on the lower-right hand side of the screen. It will remain here when you close the client so you can reopen it right from here:

You have the option to double-click or right-click on it. If you right-click on it you will see a summary of your protected data, last sync time, and you will have the option to **open DPM client**, **Sync now**, or **Recover Data**:

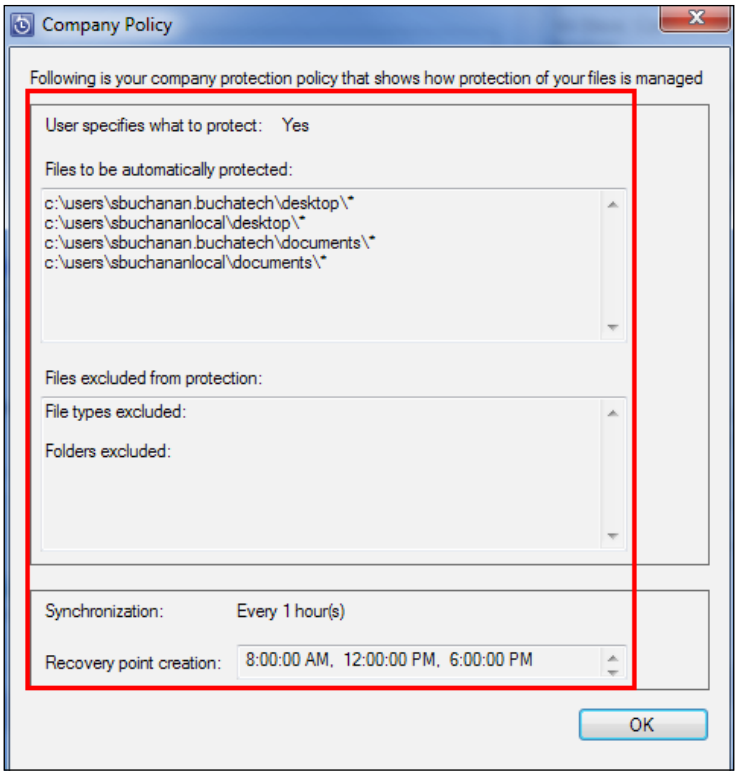


Now let's look at the full client. You have three tabs **Summary**, **Protected Items**, and **Recovery**.

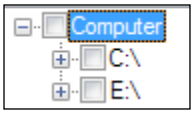
On the **Summary** tab you will see an overview about your protection. This can show you if your client is currently syncing, when the last sync was, if it failed or succeeded along with the schedule for syncing.



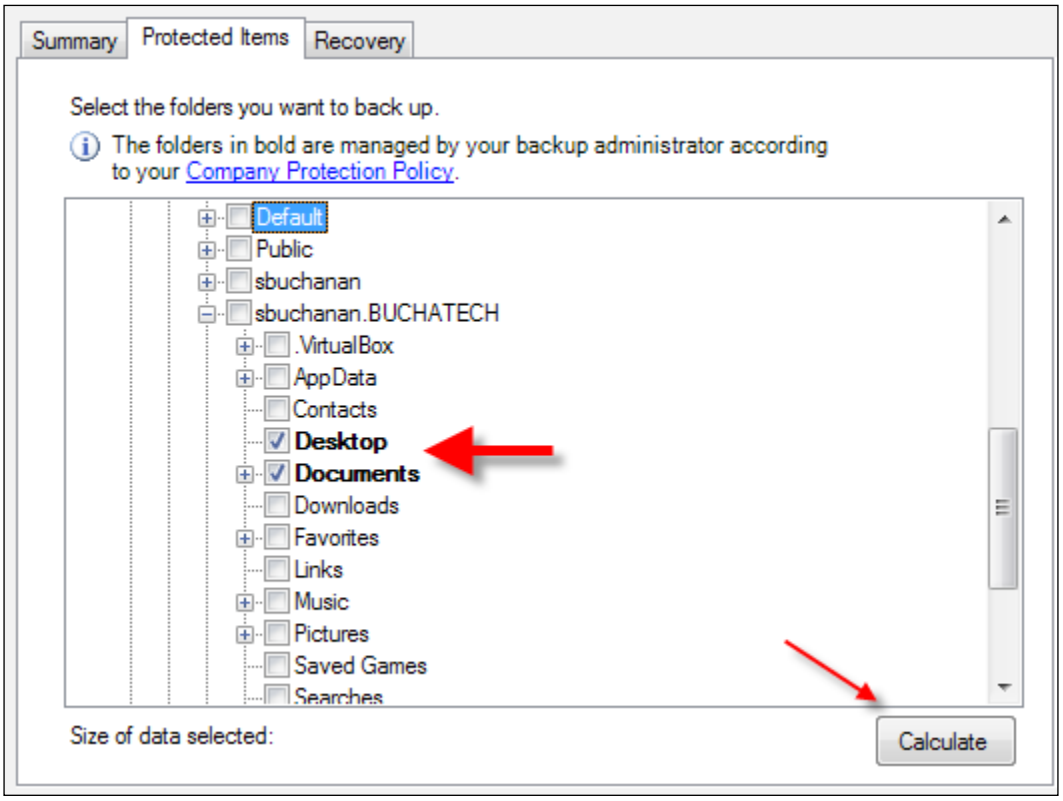
Notice the **Company Protection Policy** link. If you click on that link another window will pop up. This window will show the end-user policy that was set by the backup administrator. It shows what is to be included in the backup, what is excluded, and what the sync times are. The following is a screenshot of what this looks like:



On the **Protected Items** tab you will see a Windows Explorer-like view of the client computers hard drives:

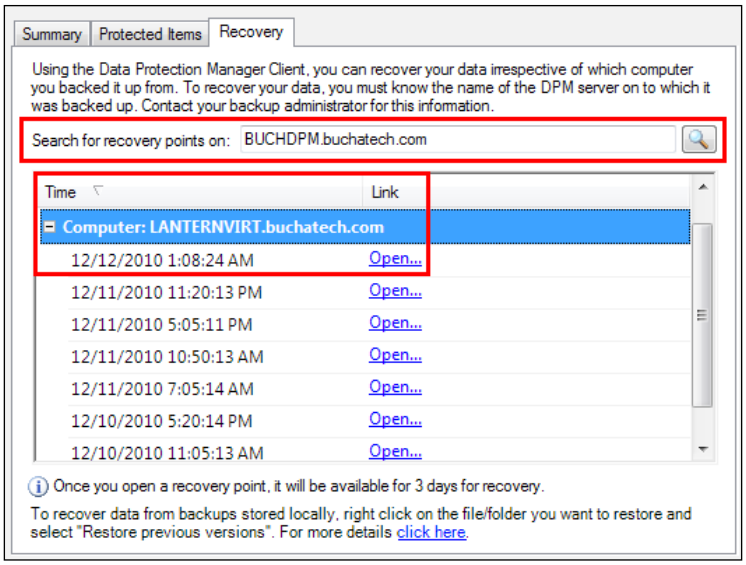


Expand these to see the data that is actually being backed up as per the **Company Protection Policy.** You will see an example of this in the following screenshot:



Also notice the check boxes next to all objects. If you check these boxes, then that data will also be included in the backup. You will only have the ability to check these boxes if the backup administrator has granted permissions to add to the data that is being backed up in the DPM **Company Protection Policy**. There is a **Calculate** button on this tab as well. You can click this after adding data to the backup to see how much the total backup will be including the data that was just added. It will appear next to the text **Size of data selected.**

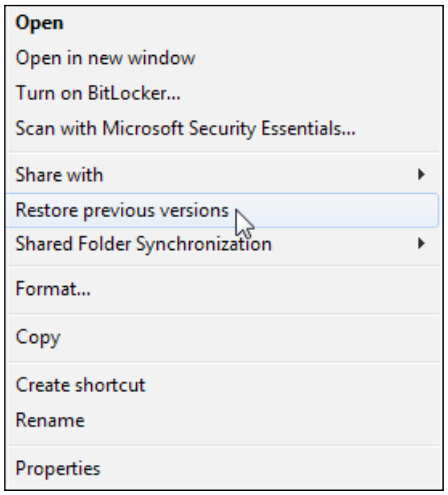
The **Recovery** tab will typically be blank and you will need to search the DPM server for recovery points. Once you find the recovery points the window will be populated with recovery points like in the following screenshot:



You need to know the full name of your DPM server to put this into the **Search for recovery points on** field. The screenshot is showing you what the recovery points on the DPM server look like. Remember there are two ways to get data back if it becomes lost. The first is restoring through Shadow Copies and the second is from a DPM recovery point. Let's walk through the recovery processes now.

To recover data from a Shadow Copy follow these steps:

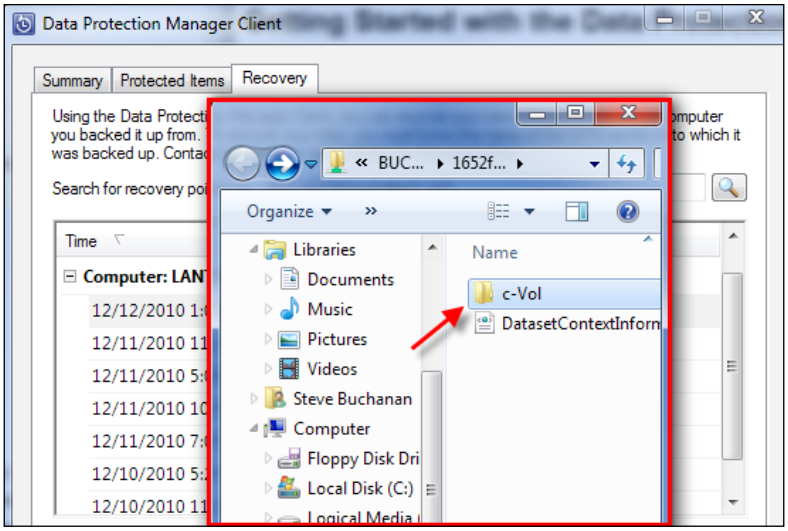
1. Find the file or folder you want to restore and right-click on it then click on **Restore previous versions**:



2. A **Properties** dialog will pop up. You will be on the **Previous Versions** tab. Here will be a list of available previous versions of the file or folder to restore from.
3. Once you verify that this is the data you want, click **Restore**.

To recover data from a DPM recovery point follow these steps:

1. Click **Start**, select **All Programs**.
2. Click on **Microsoft System Center Data Protection Manager 2010** to expand it.
3. Click on the **Data Protection Manager Client** to launch it.
4. In the DPM client window click on the **Recovery** tab.
5. In the **Search for recovery points on** field, type the name of the DPM server that has the recovery points.
6. Click the **Search** button to start searching for the recovery points on the DPM server.
7. All the listed recovery points have a date and time so it should be easy for you to locate the data you need. To access the data in these recovery points from the DPM server, click the **Open** link next to the recovery point you want to recover data from.
8. An explorer window will pop up like in the following screenshot. You can navigate to the data you need. Once you find it simply copy the data from this window to the original location or another location on the local client computer.



NOTE: In order to protect Windows' clients using DPM 2010 please make sure to install the latest QFE of DPM at `http://support.microsoft.com/kb/2465832`. After applying the QFE 2465832, the administrator will need to add a registry key and the non-administrator end-users to the newly added registry key. Adding this key and the non-administrator users to this key will ensure that recovery points are created properly and the end-users will be able to access the recovery points.

- Navigate to: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\Agent\ClientProtectionREG_MULTI_SZ` and add a registry key named: `ClientOwners`
- Then add your end-user(s) to the key in the following format: `YOURDOMAINNAME\USERNAME`
- You can add multiple users by separating the user names with a ",". Here is an example: `YOURDOMAINNAME\USERNAME,YOURDOMAINNAME\USERNAME2`
- After a reboot of the computer and the next recovery point creation your end-user should see the recovery points and will be able to restore.
- That completes the steps to restore end-user data on a client computer through Shadow Copies and from DPM recovery points.

This process would be the same for an end-user that is not on the corporate network. They would follow the same steps while connected to the corporate VPN connection. It may not be as fast over VPN but this depends on the speed of the the VPN and the internet connections involved.

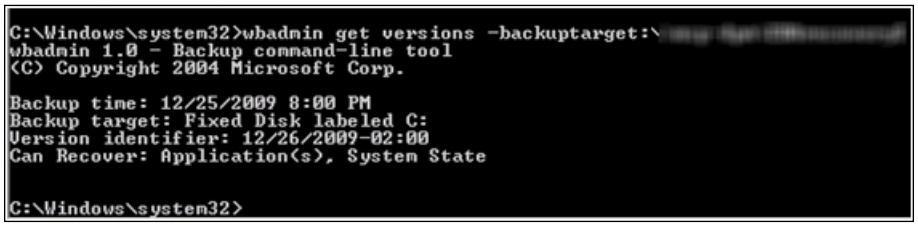
Recovering data using System State

So, you have your Windows Server 2008 servers System State backed up by DPM. Your server crashes and you need to recover. DPM does not give an option to recover to the server only to tape or a network share:

What do you do from here? The answer is you have to actually restore the System State using Microsoft's built in Windows Backup Utility. There is also another catch in that it has to be done via command line using `wbadmin`. Here are the steps to recover a server using Windows 2008 Backup from the command line:

1. In DPM recover the System State for the protected computer that you plan to recover.
2. Copy the System State backup created by DPM to a share on your network or external drive. Be sure to move the `WindowsImageBackup` folder that DPM recovered to the root of your share or external drive. If you do not move this to the root of your share or external drive the `wbadmin` command will not work.
3. Load your server with a fresh OS and get it on the network so you can access the share that stores your System State data. Be sure to install the Windows Backup feature on this server.
4. Now get the version ID of the System State using the following command:

```
wbadmin get versions -backuptarget:\\server\sharename
```



5. Now go ahead and start the System State recovery using the following command:

```
wbadmin START SYSTEMSTATERECOVERY -version:<Version identifier>
-backupTarget:<\\server\sharename> -machine:<SERVERNAME THE
SYSTEMSTATE WAS TAKEN FROM>
```

Bare Metal Backup and Recovery

Imaging a server creates an exact copy of a live machine for a complete backup, this is like taking a picture of that server. This allows you to restore the server back to its current state in the event of total failure. Server imaging provides very comprehensive data protection. In many IT departments today imaging of servers is a common practice because of its reliability and ease of restores. In recent years Bare Metal Backup and Recovery has become a very popular added feature of imaging. Microsoft has its own imaging tools and with DPM has added a solid BMR solution. We are going to discuss BMR in more detail and show you how this is done in DPM.

What is Bare Metal Backup and Recovery?

Bare Metal Recovery is needed in the event of a server disaster. BMR is similar to imaging servers. It can restore the entire system including the operating system, any applications and all the data. BMR typically only protects the operating system drive by default. This means if your server has multiple disks you will need to protect the data on those drives as well. It is also similar to System State in that it contains the components needed to get the operating system. The key difference between imaging a server or having the System State backed up on a server is that BMR can restore like an image but to dissimilar hardware. This means you can take the BMR and restore it on an entirely different hardware platform from the platform the server was originally running on.

This is key for administrators because if your server dies you might have extra hardware around but it is not the same type of hardware. Before BMR if you tried to restore on dissimilar hardware you would get the blue screen of death with errors. That was because of the HAL (Hardware Abstraction Layer) differences between the hardware platforms. Before BMR you would have needed to rely on System State and the restore does not always work; restore is also a time-consuming process. With BMR if your server dies and you have a different piece of hardware you can restore it if the hardware can handle your server.

With the release of Windows Server 2008, Microsoft revamped the Windows Backup application (`wbadmin`). One of the features Microsoft introduced was BMR through the imaging of servers. DPM leverages Windows Backup for BMR, it is only supported on Windows 2008 Server or newer. Unfortunately you are limited to System Recovery Tool (SRT), System State, or third-party imaging tools for protecting your Windows 2003 servers. For more information on SRT visit:

`http://technet.microsoft.com/en-us/library/bb795839.aspx`

BMR does not require a certain amount of space on the protected server. DPM reserves 30 GB of space for the replica in the disk pool on the DPM server.

Getting a BMR of your server is simple. Install the Windows Server Backup role and the DPM agent on the server you want to protect. Go into DPM and click on **Modify** New Protection Group Wizard. Expand **System Protection** on the server you want to protect. BMR will be listed here. Select **BMR** and click **OK** on the wizard.

NOTE: When you select BMR under System Protection, System State will automatically be selected. These are required to be in the same protection group together.

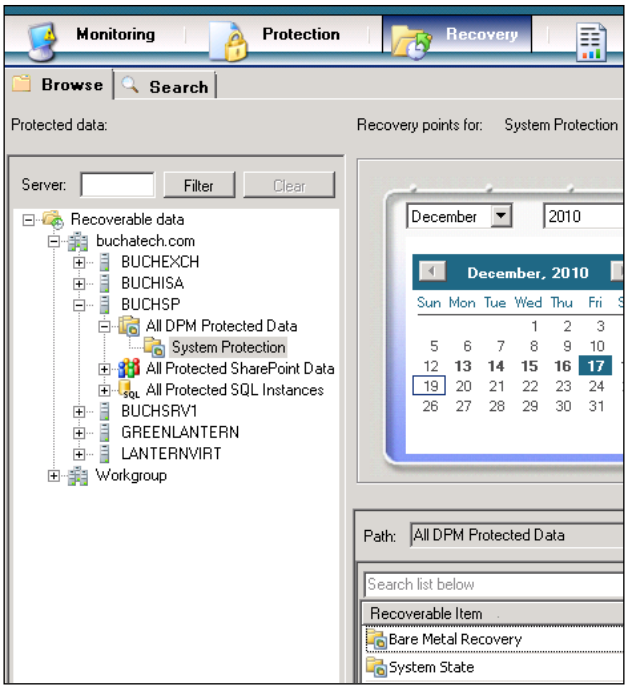
How to perform a Bare Metal Recovery?

Now let's get into the restore process of BMR. This essentially is the same process as restoring an image taken by Windows Backup with a few more steps added. This is a two-step process. The first process is to recover the BMR data in DPM. The second step is to restore the BMR data on your new server hardware.

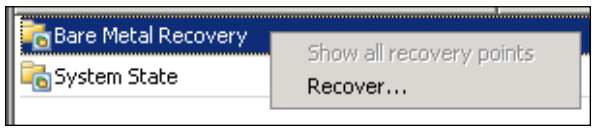
Recovering BMR data in DPM

To recover the BMR data in DPM follow these steps:

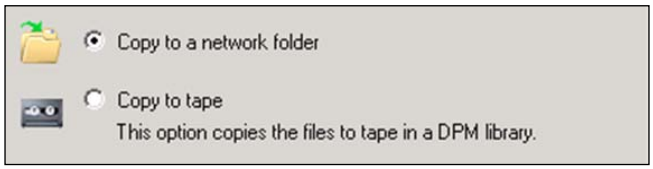
1. Go to the DPM Administrator Console.
2. Navigate to the **Recovery** tab and expand the protected computer, expand **System Protection**, then select **Bare Metal Recovery**.



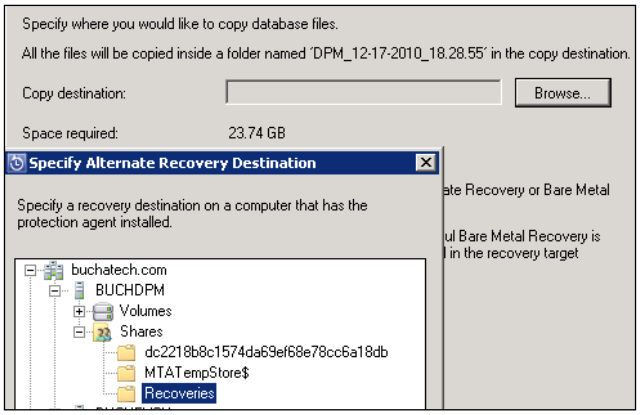
3. Find the date and time you want to recover the system to then right-click on **Bare Metal Recovery** and choose **Recover**:



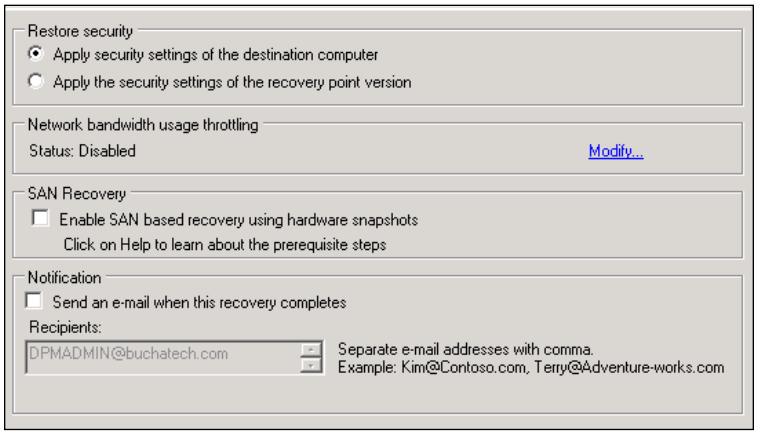
4. Review your selections for the recovery and click **Next**.
5. Recover the BMR data to a network share:



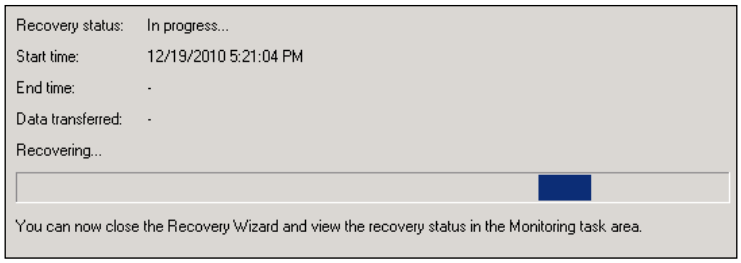
In this example we will recover to the local DPM server and move the data from here.



Choose to keep the existing security settings of the recovering data or the security settings of the share you are recovering the data to. Also you can choose to receive an e-mail once the recovery is complete if you want to.



You will now see a summary of your recovery. Click **Recover** to start the restore. You will then see a progress bar for a while then the restore will complete:

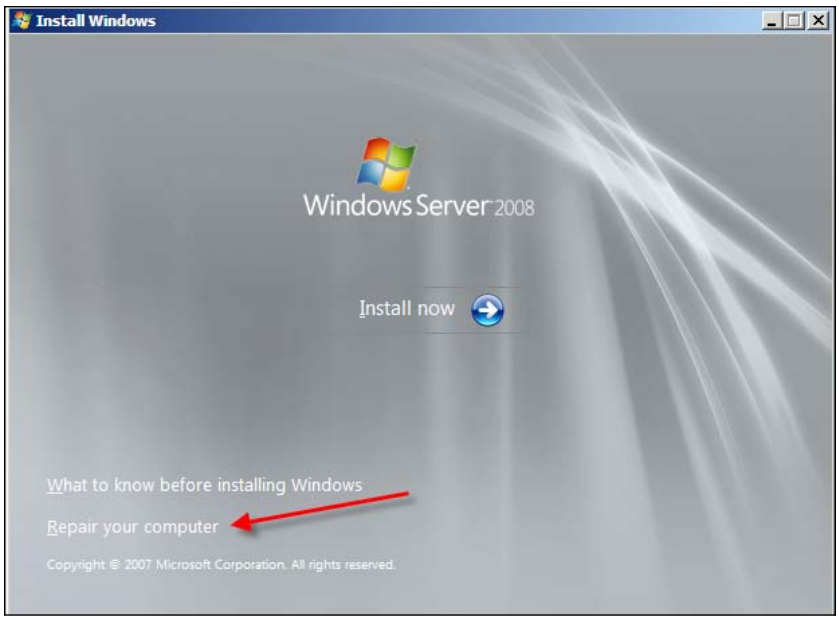


That is it as far as recovering the BMR data goes. Now it can stay where it is or be moved to another form of media.

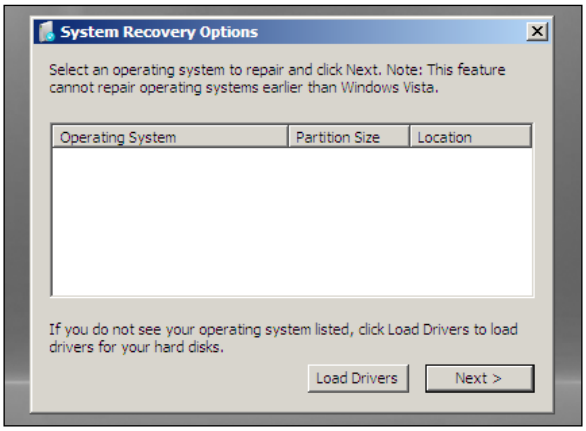
Restoring BMR data on your server

To restore the BMR data on your new server follow these steps:

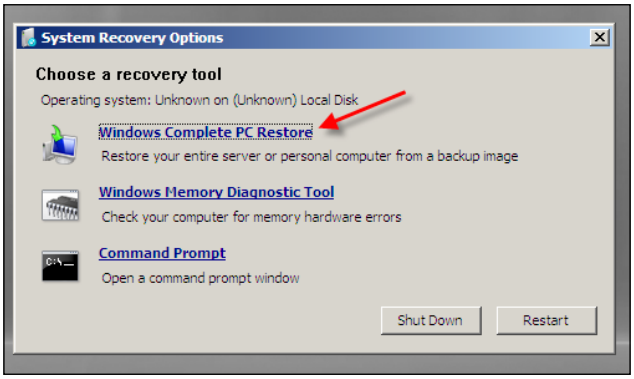
1. Boot your new server using the Windows Server 2008 disc.
2. Select the settings appropriate to you and click **Next**.
3. On the next screen click **Repair your Computer**:



4. On the **System Recovery Options** window load drivers for your hard disk if you need to. If not simply click **Next**:



5. On the next **System Recovery Options** window click on **Windows Complete PC Restore**:



This is the point where you come to a fork in the road and you can do one of two things:

- Restore from a network share
- Restore from a local or external hard drive

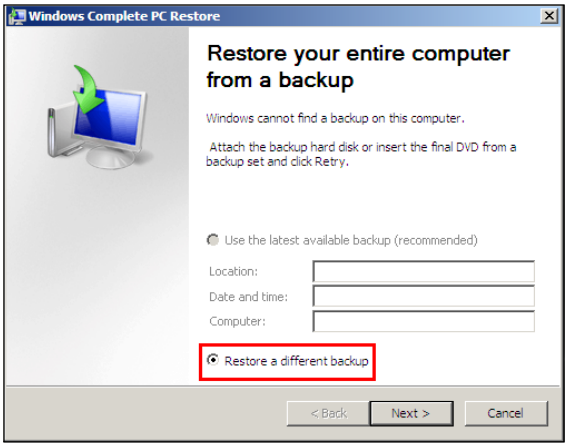
Restoring from a second local hard drive or an external hard drive tends to be the best option. Note that the second local hard drive was stated. This is because you cannot contain the BMR data on the hard drive that you are restoring to because this drive will be formatted and overwritten. Hence you would need to attach a second drive to hold the BMR data.

On this window the restore tool will scan all of the hard drives attached to your system for an available restore image. If it finds backup data this will be listed under the **Use the latest available backup** option. If it does not find it on local drives or attached external drives the option will be grayed out and you cannot use this option. You will then need to select the **Restore a different backup** option. We will first see what it looks like to restore from a network share (Option A), then we will go back to restoring from a local drive (Option B).

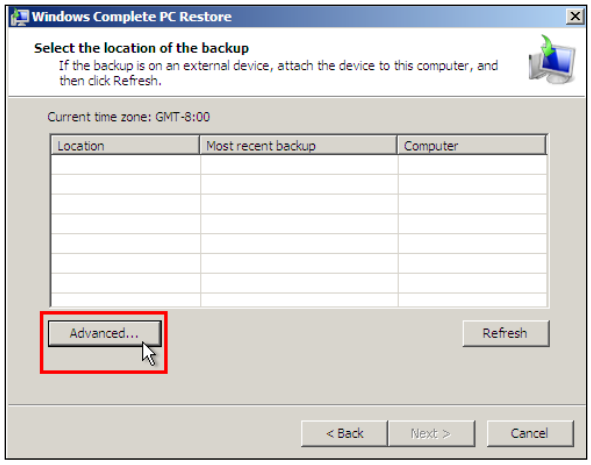
Option A: Restoring from a network share

The following steps will demonstrate how to restore data from a network share:

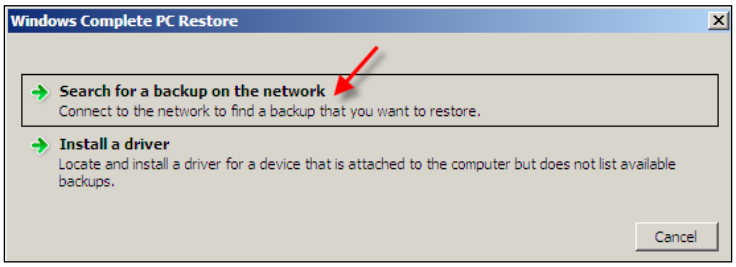
1. Select the **Restore a different backup** option and click **Next**.



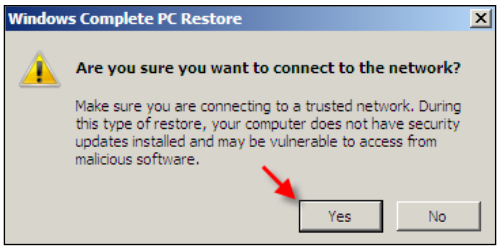
2. Click the **Advanced** button:



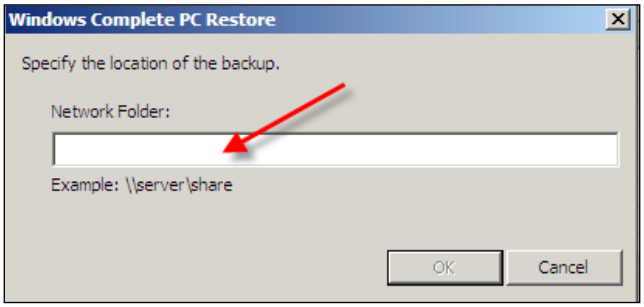
3. Select **Search for backup on the network**:



4. On the dialog box that appears, click **Yes**:



5. Type in the UNC path to the share that contains your Windows Image Backup. Click **OK**:

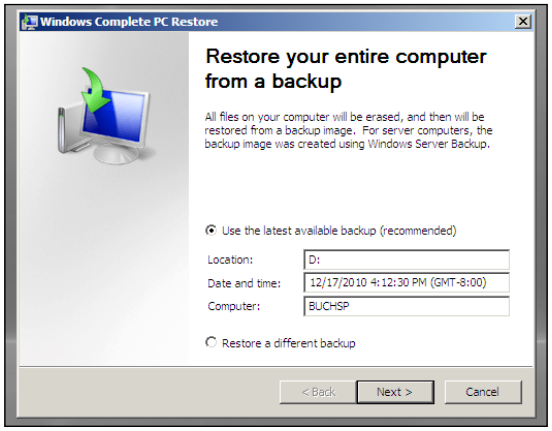


6. Now you will be able to see the recovery images that are available. Select the correct one and click **Next**.

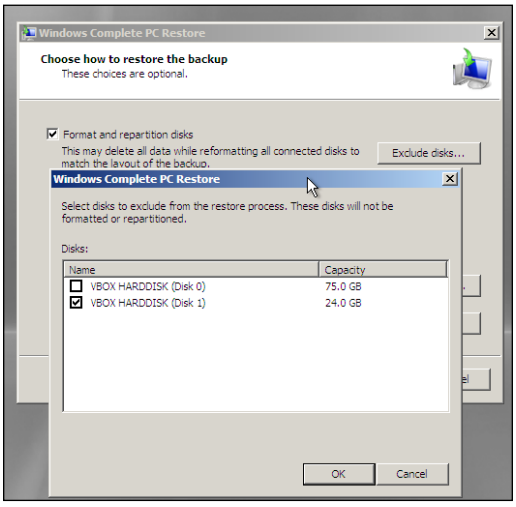
Option B: Restoring from a local hard drive

The following steps will demonstrate how to restore data from a local hard drive:

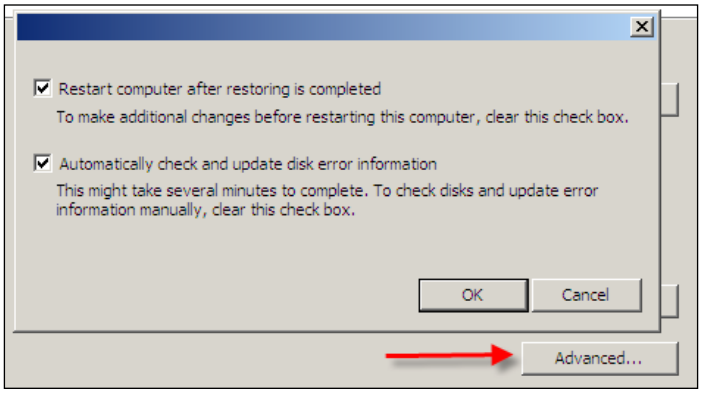
1. Choose **Use the latest available backup** and click **Next**:



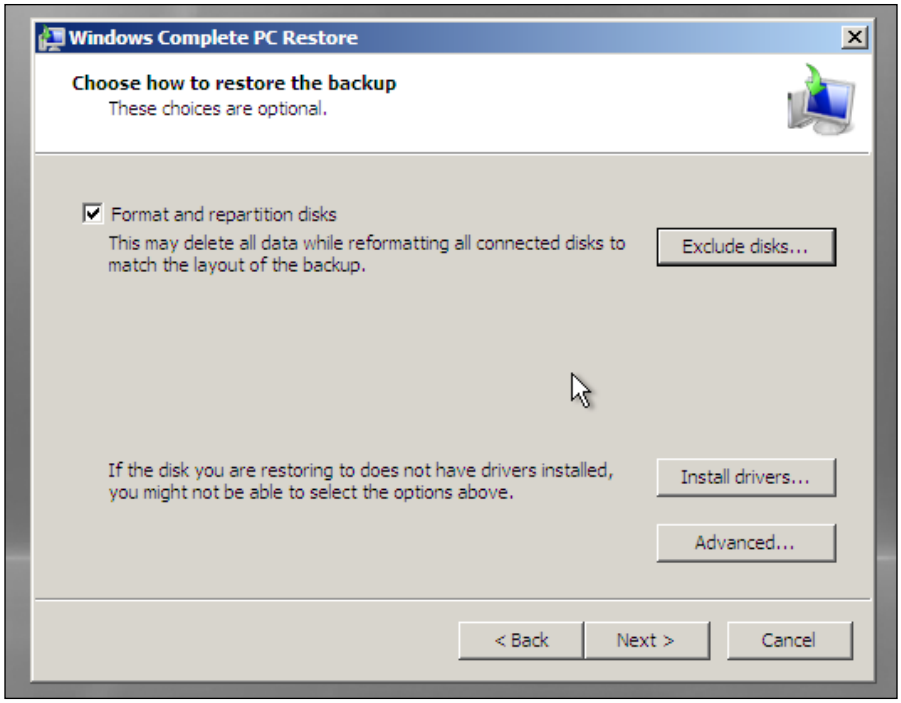
2. On the **Choose how to restore your backup** window, you have several options:
    - You can install any needed drivers for the disk you are restoring by just clicking the **Install Drivers** button.
    - You can exclude disks that don't need to be formatted. This is needed when you are pulling the data from a second local hard drive or external drive. You can exclude drives by clicking on the **Exclude disks** button:



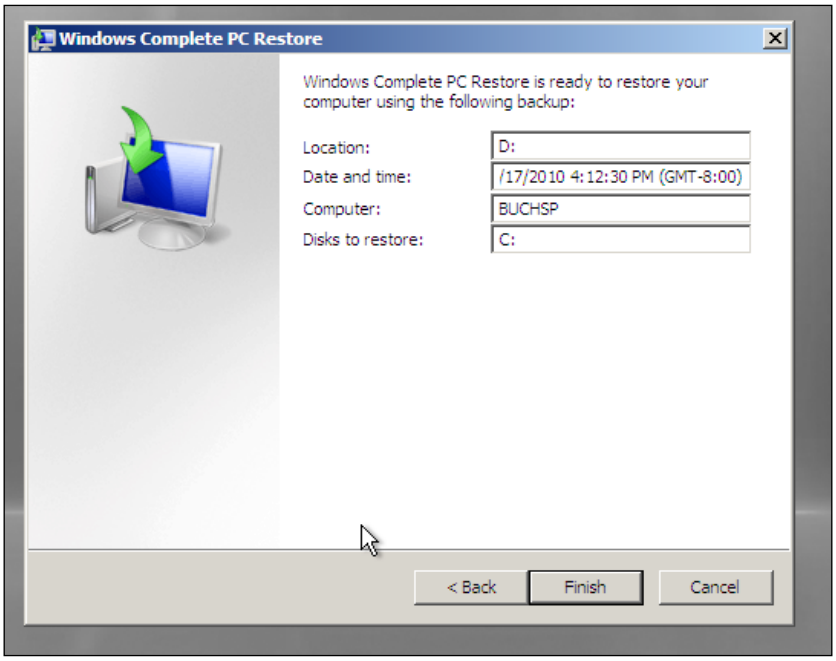
- Click on the **Advanced** button if you want to restart the computer after the restore process and to automatically check and update error information:



3. Once you have added the extra options, click on the **Next** button:



4. On the next screen make sure all your settings are correct. Click **Finish** to start the restore process:



5. The last warning will pop up asking you to confirm you are okay with formatting the hard drive. Click **OK** and the process will begin.

You will see the progress window for a while. Once this is done your server will reboot and come up to a Windows login screen as long as the restore goes well.

We covered restoring standard data such as files and folders and we also covered restoring using BMR. Now let's look at restoring some of the important applications that are relied upon in many companies today.

Restoring critical applications with DPM

In this section we take a look at restoring workloads of your companies' critical applications. DPM does a great job of simplifying the restore process of the critical applications in your environment. This is made possible through well-designed restore wizards and tight integration with Microsoft products. Now let's look at the processes for restoring Exchange, Hyper-V, SharePoint, and SQL.

Restoring Exchange mailboxes with DPM

We are going to look at the processes of restoring mail using DPM 2010 in Exchange 2007 and Exchange 2010. These processes are somewhat complex and can be expensive in terms of storage and performance. Mailbox restores should not be a regular on-going task in most IT departments. If this is the case it is best practice to find out why these restores are common and the deleted mailbox and item retention periods should be increased. End-users should then be trained on how to recover mailboxes within this time frame using their Outlook clients. More information on this can be found here:

`http://office.microsoft.com/en-us/outlook-help/recover-deleted-items-from-any-folder-HA001116528.aspx`

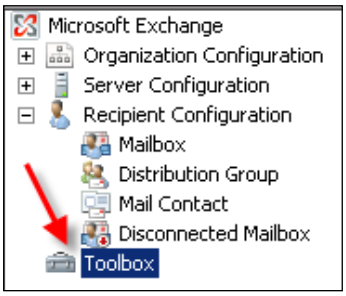
Having a network administrator restore mailboxes should be a last resort in any environment. Now let's look at recovering mail in Exchange 2007 and Exchange 2010 using DPM.

Recovering mail in Exchange 2007

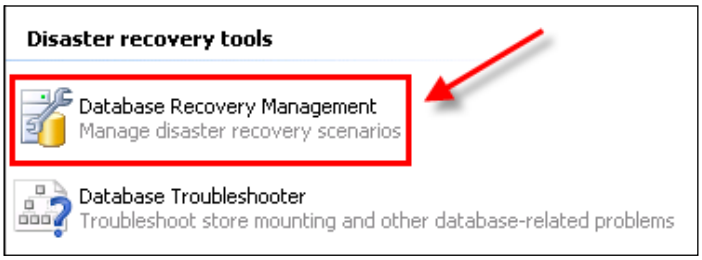
Exchange 2007 uses Storage Groups (SG) to store the mailbox databases were the mailboxes reside. Mail cannot be restored directly to the Storage Groups that are in production. A Recovery Storage Group (RSG) needs to be created and then mailboxes can be restored to the RSG from backups. Administrators are able to extract data from mailboxes that have been restored to an RSG without affecting a production SG. Here are the steps to recover mail in Exchange 2007:

1. Create an RSG on your Exchange 2007 server for the mailbox database that you are going to restore to. Creating this RSG can be done via GUI or PowerShell. In this guide we will show you how to do this via the GUI. In the Exchange 2010 guide we will show you how to do it via PowerShell. Go to **Start**, and then **All Programs**, Expand **Microsoft Exchange Server 2007**, now launch **Exchange Management Console** by clicking on it:

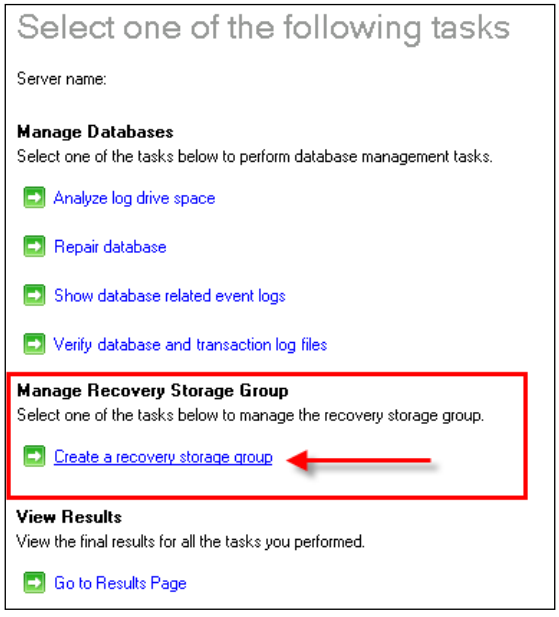
2. Navigate to **Toolbox**:



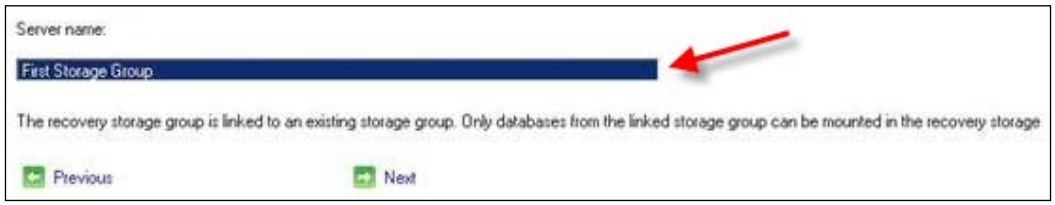
3. Click on **Database Recovery Management** in the right-hand pane:



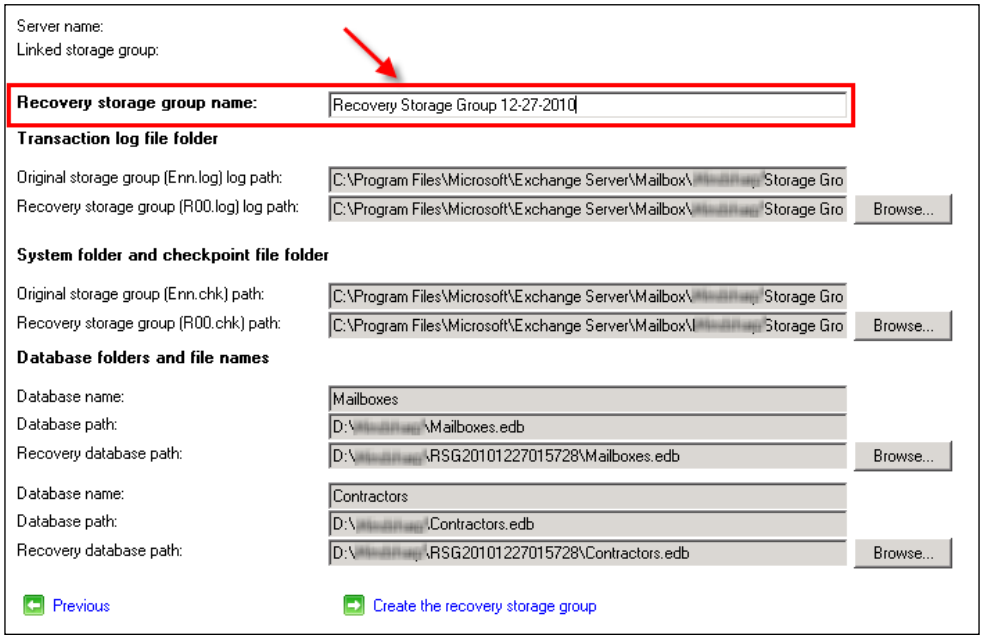
4. Select **Create a recovery Storage Group**:



5. Then link it with the existing group.

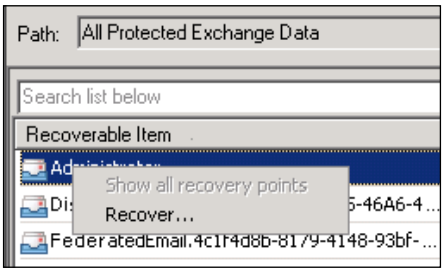


6. Name the RSG and verify the location of the exchange data and logs:

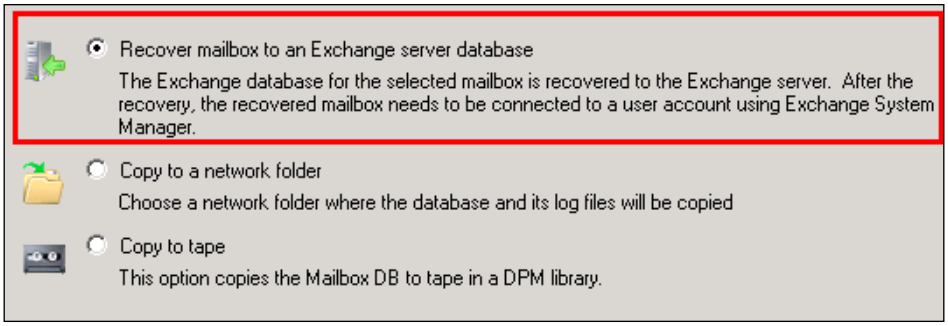


7. Click **Create the recovery storage group**.
8. Go back to the DPM server. Here you will restore the mailbox to the recovery Storage Group you created on the Exchange server. Navigate to the **Recovery** tab and locate the mailbox from the Exchange database that you want to restore:

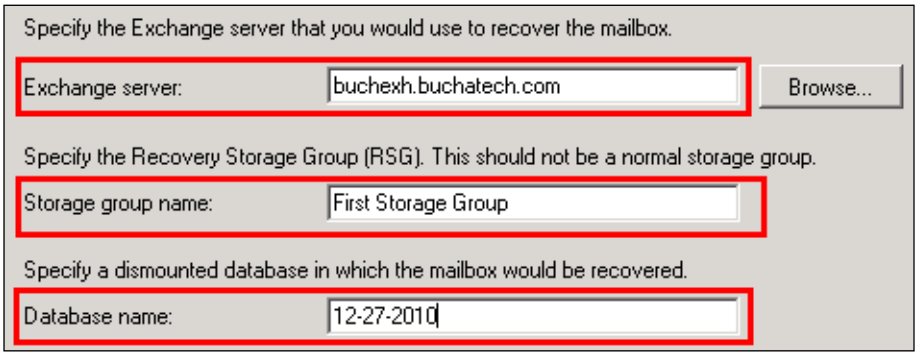
9. Right-click on the mailbox and select **Recover**:



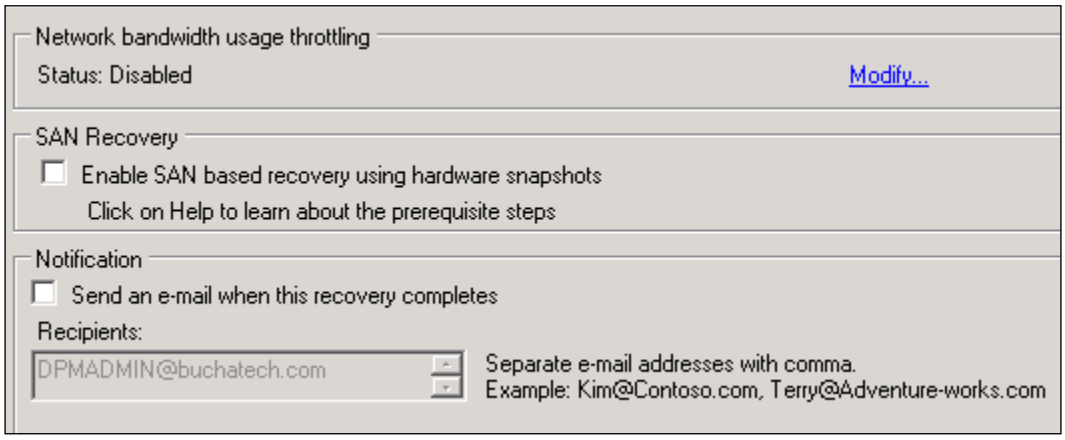
10. Review your selection and click **Next**.
11. Select **Recover mailbox to an Exchange server database**. Click **Next**:



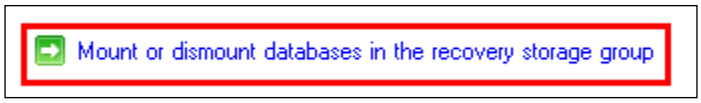
12. Enter your **Exchange server** address, the recovery **Storage group name**, and the **Database name**:



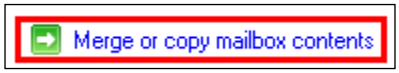
13. Set any extra options you want on this restore job and click **Next**:



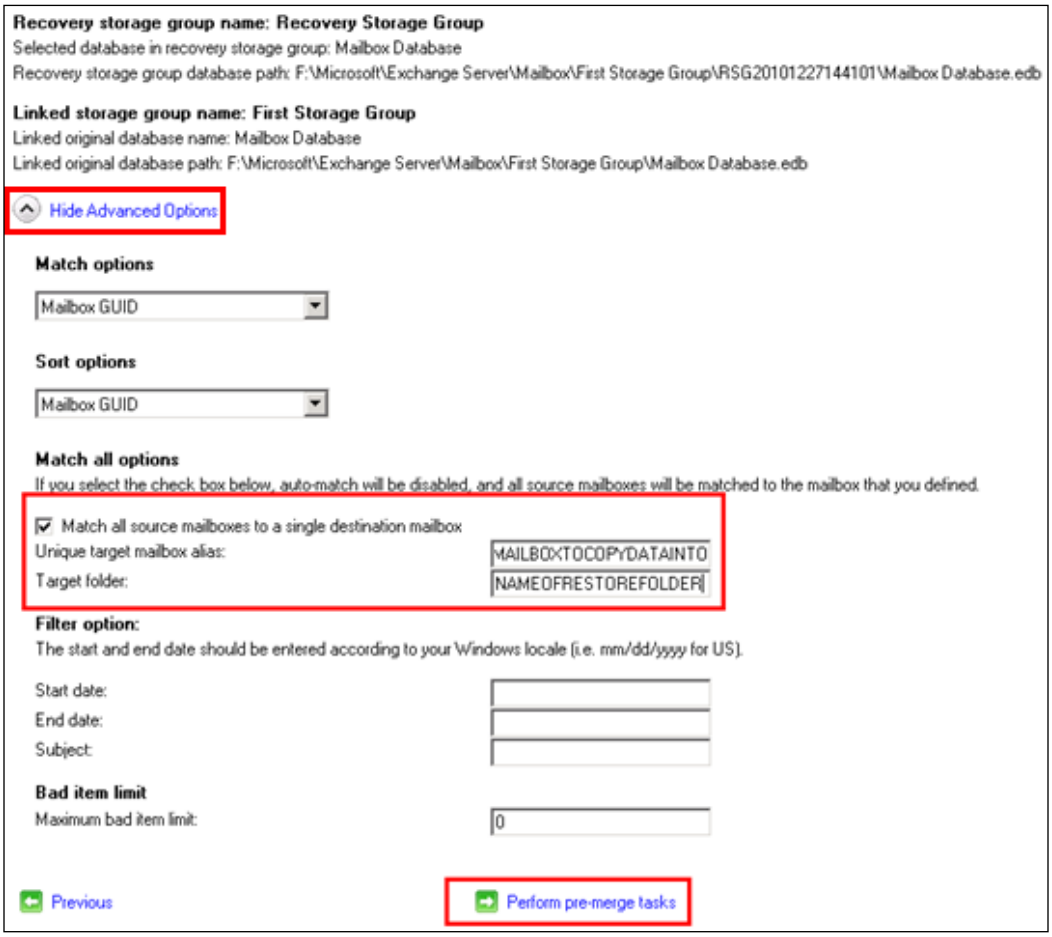
14. Review your restore selections for the last time and click **Recover** when you are ready to start the restore.
15. Go back to your Exchange server.
16. Open the **Exchange Management Console**, open **Toolbox** then go to **Database Recovery Management**.
17. Now mount the mailbox database that you just restored in the RSG:



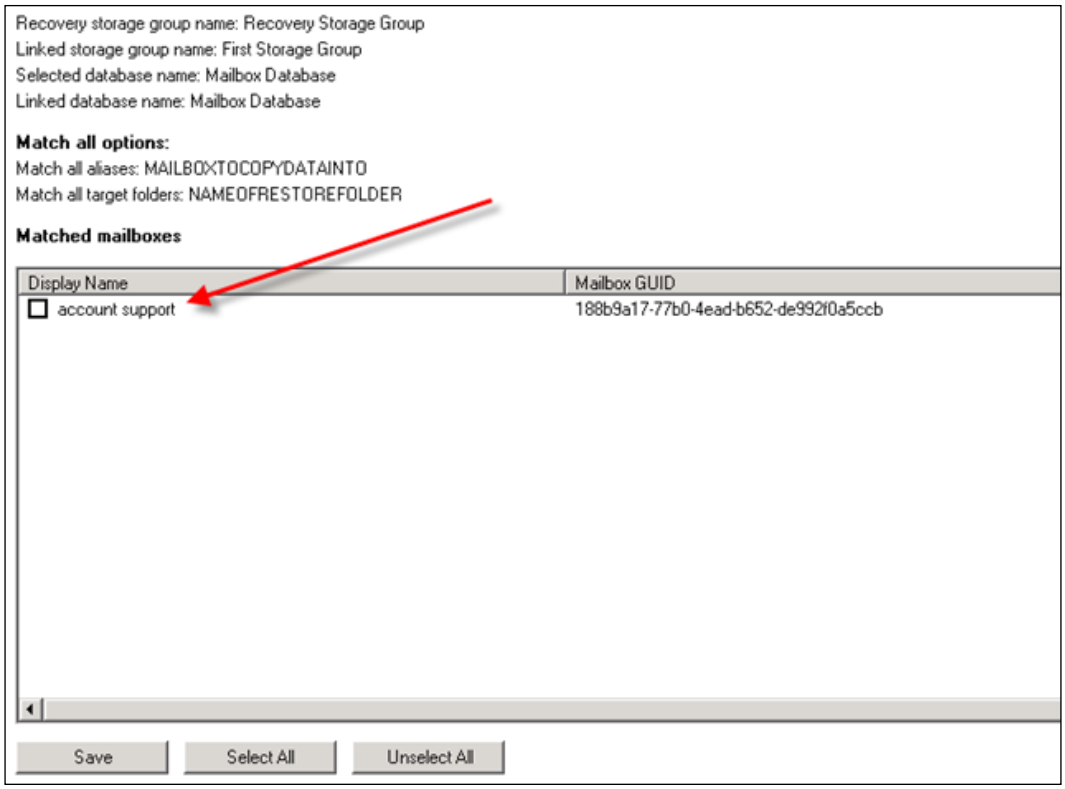
18. After the database is mounted click on **Previous** then select **Merge or copy mailbox contents**:



19. Choose the mailbox database that contains the mailbox you want to restore then click **Gather Merge information**. To restore a single mail item click **Advanced Options**. This will allow you to search for a particular mail using criteria such as date or subject of the e-mail. Leave these fields blank if you want to recover the entire mailbox. To restore mail to a folder in another mailbox fill in the **Unique target mailbox alias** and **Target folder** under the **Match all options** section. Click **Perform pre-merge tasks** to start the recovery.



20. On the next screen select the mailbox that you want to recover or recover mail from and click **Recover**.



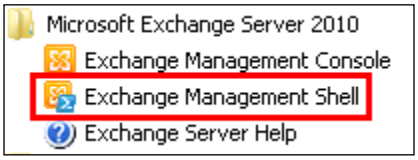
Recovery in Exchange 2010

Recovering mail in Exchange 2010 is similar to restoring mail in Exchange 2007 but differs in a few areas. Exchange 2010 does not use SG's, it uses databases only. Also Exchange 2010 does not have a GUI tool for restoring so these tasks need to be done via command line. In order to recover mail in Exchange 2010 you need to complete some tasks on the Exchange server itself so you need to be familiar with Exchange as some of the tasks for Exchange 2010 are beyond the scope of this book. We will cover the basic steps in Exchange 2010 that are needed for a successful recovery in the steps that will follow. One of the tasks that you need to do is create a Recovery Database (RDB). Creating the RDB is an Exchange task and will need to be complete on the Exchange server. You can learn more about RDB here:

`http://technet.microsoft.com/en-us/library/dd876954.aspx`

You will need to run commands in the **Exchange Management Shell** as many tasks have been removed from the Exchange management GUI interface. Let's get started. To recover Exchange data using DPM follow these steps:

1. Go to your Exchange server and open **Exchange Management Shell**. Click on **Start**, click on **All Programs**, Expand **Microsoft Exchange Server 2010**, Launch the **Exchange Management Shell** by clicking on it:



2. Using Exchange PowerShell, create a recovery database on your Exchange server. Use the following command:

```
New-MailboxDatabase -Recovery -Name NAMEOFYOURRDB -Server
NAMEOFYOUREXCHANGESERVER
```

NOTE: You can remove your RDB from Exchange in case you made a mistake when creating it such as forgetting to set it as a recovery database. Here is the syntax for removing a mailbox database from Exchange:

```
Remove-MailboxDatabase"NAMEOFYOURRDB"
```

3. The recovery database defaults to a **Dismounted** status and will need to be mounted.

   Here is the syntax to mount the database:

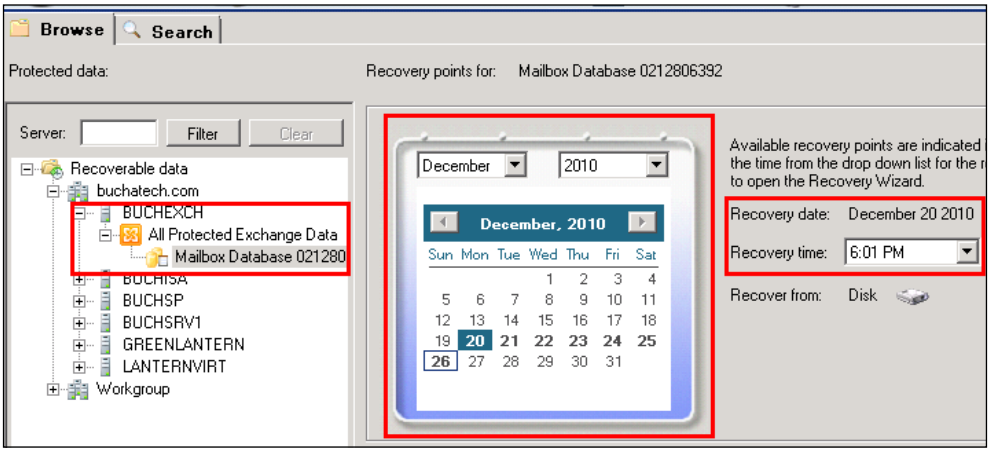
```
Mount-Database -Identity "NAMEOFYOURRDB"
```

   Set the overwrite flag to allow this recovery database to be overwritten. Here is the syntax for this:

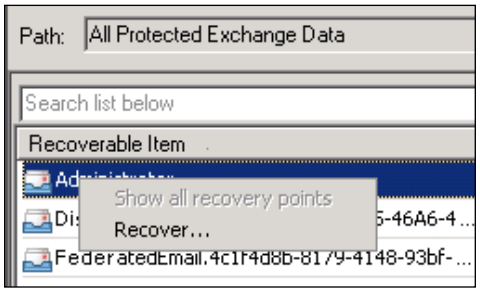
```
set-mailboxdatabase -Identity "NAMEOFYOURRDB" -AllowFileRestore 1
```

NOTE: The overwrite flag will need to be set every time you want to recover from DPM to this RDB.

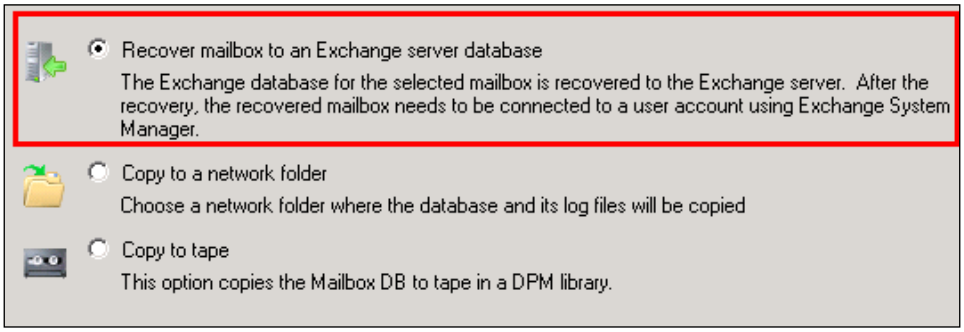
4. Go back to the DPM server. Here you will restore the mailbox to the recovery database you created on the Exchange server. Navigate to the **Recovery** tab and locate the mailbox from the Exchange database that you want to restore:



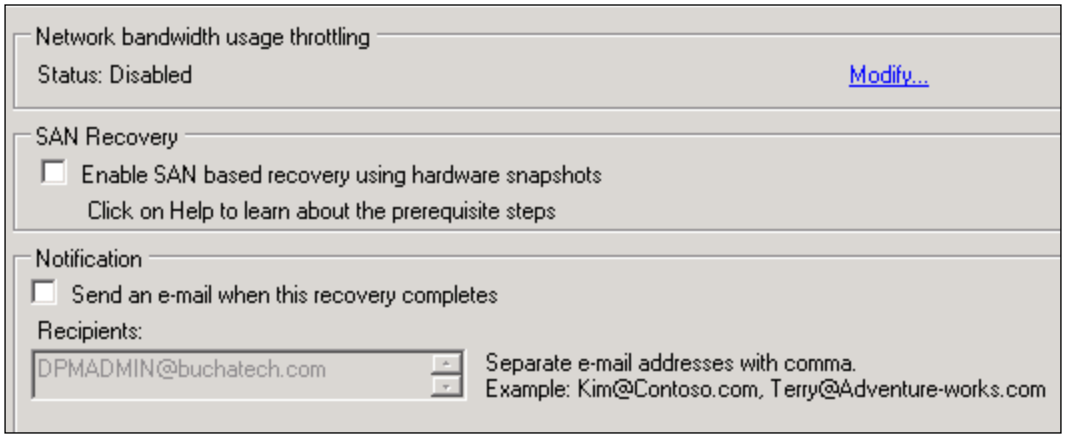
5. Right-click on the mailbox and select **Recover**:



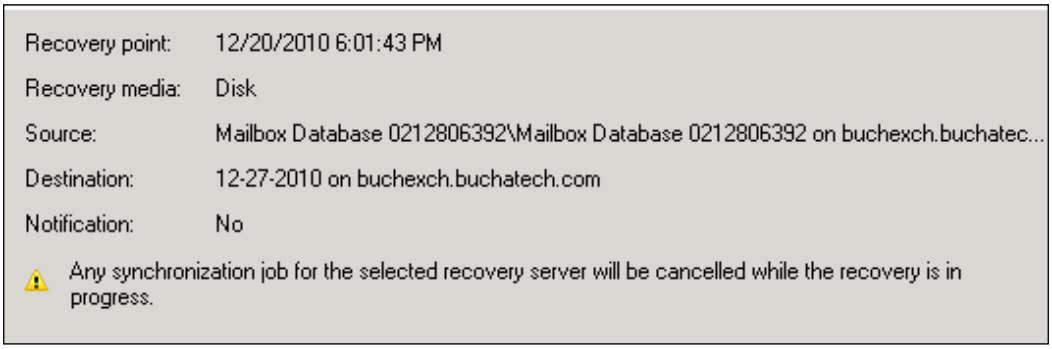
6. Review your selection and click **Next**. Select **Recover mailbox to an Exchange server database**. Click **Next**:



7. Enter your Exchange server address and the recovery database name in the next window. Set any extra options you want on this restore job and click **Next**:



8. Review your restore selections for the last time and click **Recovery** when you are ready to start the restore:



9. Go back to the Exchange server and extract the mailbox from the recovery database that DPM restored to. Then restore the mail to another mailbox of your choice. The following is the syntax used for this command:

```
Restore-mailbox -identity MAILBOXYOUAREGOINGTORESTORETO -recov-
erydatabaseNAMEOFYOURRDB -targetfolder "NAMEOFTHEFOLDERTORE-
STOREMAILTO" -RecoveryMailbox MAILBOXTHATWILLBERESTORED
```

You will be asked to confirm this action; the following message will appear:

Confirm

Are you sure you want to perform this action?

Recovering mailbox content from mailbox 'Administrator' in the recovery database '12-27-2010' to the mailbox for 'Administrator (Administrator@buchatech.com)'.

This operation may take a long time to complete.

[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (default is "Y"):

Now go to Outlook on the mailbox that you restored the mail to and you will see a folder with the name you gave it and the mail inside.

Restoring Hyper-V virtual machines with DPM

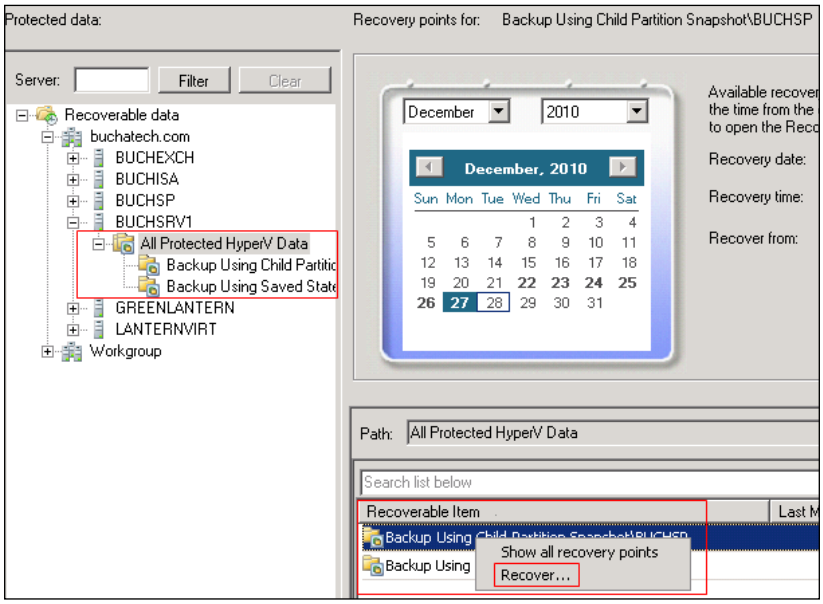
Today many IT departments utilize virtualization and many have chosen Hyper-V as their hypervisor. We covered how DPM protects Hyper-V and how to configure this protection in *Chapter 7*. Now it is time to dig into the restore options we have with Hyper-V in DPM. With DPM you can restore VMs (virtual machines) to an original or an alternate Hyper-V host. DPM captures the metadata of the virtual machine configuration so DPM can restore the VHD and the VM's configuration settings. This gives DPM the power to restore the entire VM on the same Hyper-V host or an alternative one. With DPM you can recover VM VHD's and/or their configuration files to shares and get the restoration of individual files or folders through a feature called ILR (Item-level Recovery). This feature in DPM allows administrators to restore files hosted on a Hyper-V virtual machine to a network share or to a volume on the Hyper-V host server protected by DPM. ILR does not require the restoration of the virtual machine on which the file(s) were originally hosted. When a VM is protected at the guest level the restore process is exactly the same as that of a physical server.

Recovery of a VM to its original location

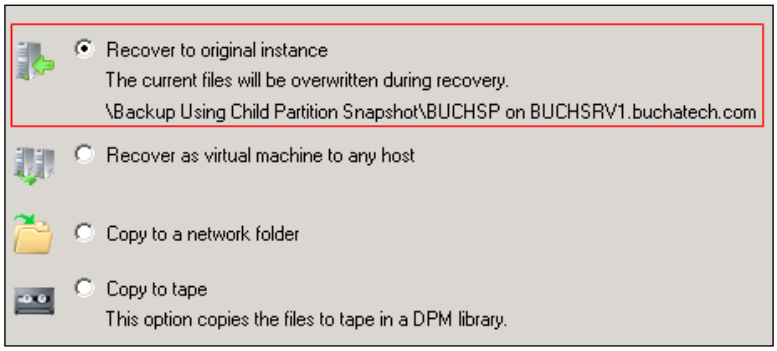
DPM can recover a VM to its original location in the event a VM becomes corrupted at the VHD level or the OS level. This consists of recovering the VHD and the VM's settings as well. This is a straightforward process. Let's look at the steps to recover a VM:

1. Open the **DPM Administrator Console** and click the **Recovery** tab.
2. Under **Protected data** browse to the Hyper-V host that the virtual machine you want to recover is on and expand it.
3. Select **All Protected Hyper-V Data**. Under **Recoverable Item**, the VMs on this Hyper-V host will appear.

4. Right-click on the VM you want to recover under **Recoverable Item** and select **Recover**:

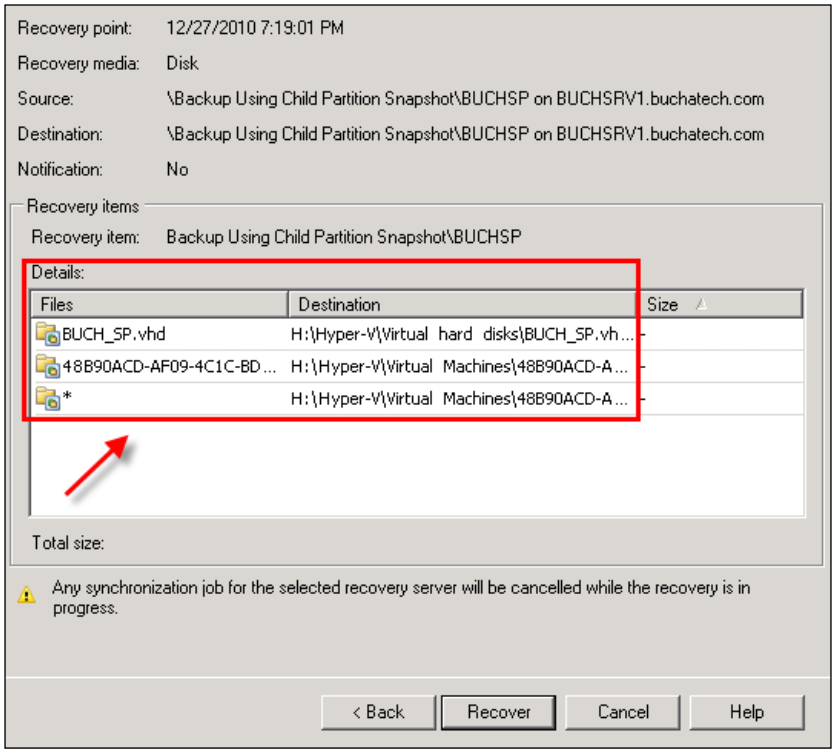


5. Select **Recover to original instance** and then click **OK**:



6. Choose one of the recovery options and click **Next**. Once again you can set the network bandwidth usage throttling, SAN-based recovery, and e-mail notification.

7. You can now review your restore settings. Notice in the screenshot you will see a list of all the VM's data that will be restored. This data contains the VHD and the VM's settings. Once you are done reviewing click **Recover**:

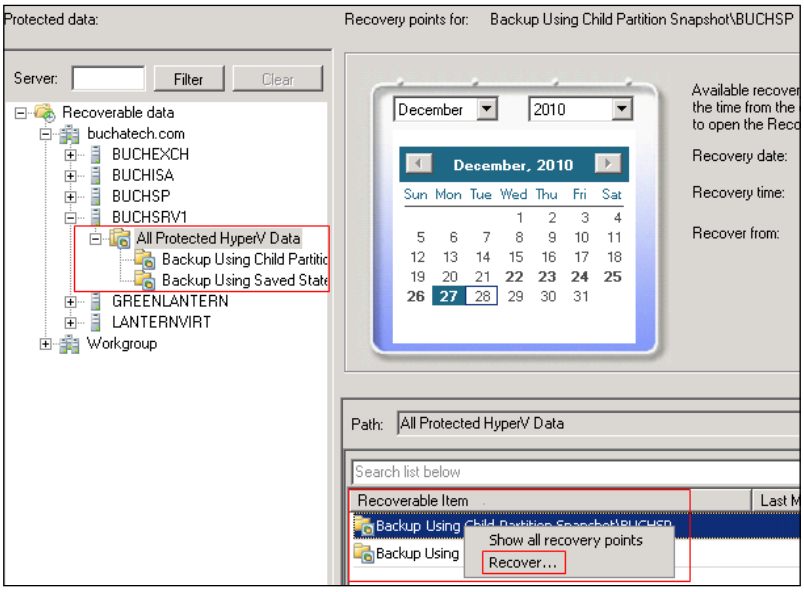


Recovery of a VM to an alternate location

DPM can also recover a VM to an alternate Hyper-V host. These restores can be performed regardless of the alternate server's processor architecture. This is good for administrators as it gives them more flexibility in the use of hardware platforms. This also contains the VHD and Hyper-V settings of the VM. Here are the steps to perform a VM restore to an alternate Hyper-V host:

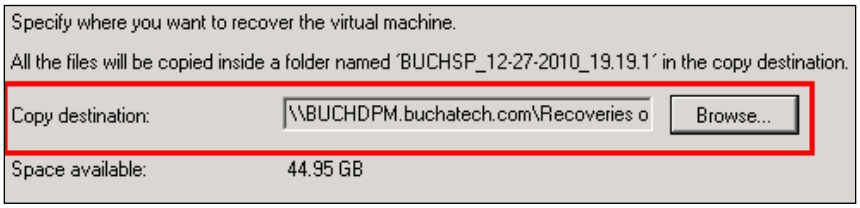
1. Open the **DPM Administrator Console** and click the **Recovery** tab.
2. Under **Protected data** browse to the Hyper-V host that the virtual machine you want to recover is on and expand it.
3. Select **All Protected Hyper-V Data**. Under **Recoverable Item** the VMs on this Hyper-V host will appear.

4. Right-click on the VM you want to recover under **Recoverable Item** and select **Recover**:



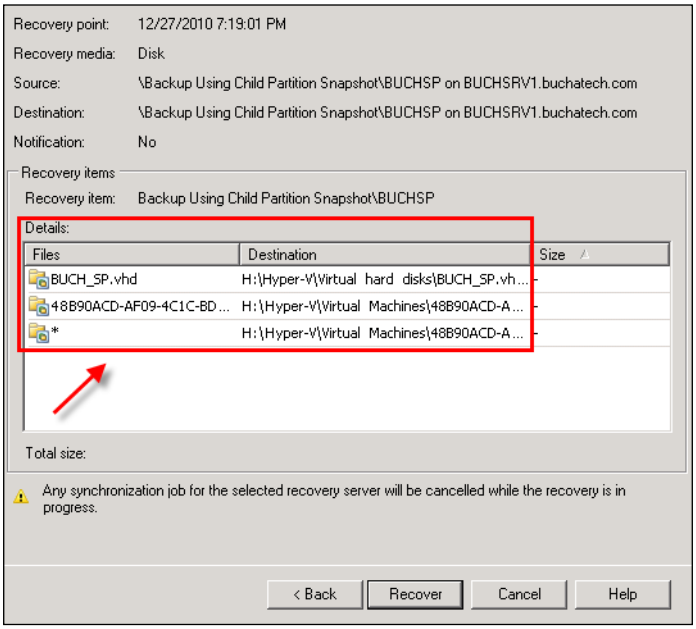
5. Select **Recover as virtual machine to any host** and click **OK**.

6. On this screen you need to specify a destination to recover this VM to. This will recover the virtual machine's VHD and Hyper-V settings to a folder. You will then need to copy this to the new Hyper-V host you want to place this VM on and use the Hyper-V import tool to import this VM onto that host. Click **Next** to continue:



7. Choose one of the recovery options and click **Next**. Once again you can set the network bandwidth usage throttling, SAN-based recovery, and e-mail notification.

8. You can now review your restore settings. Notice in the screenshot you will see a list of all the VM's data that will be restored. This data contains the VHD and the VM's settings. Once you are done reviewing click **Recover**:



Item-level recovery of a Hyper-V VM

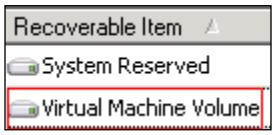
The item-level recovery (ILR) feature in DPM 2010 allows granular recovery of files, folders, and volumes. Recoveries can be done from a host-level backup of a Hyper-V VM. This item-level data can be extracted to shares, or the volume on the DPM server. ILR will work natively if the operating system of the DPM server is Windows Server 2008 R2. If the operating system of the DPM server is Windows Server 2008, the Hyper-V role must be installed in order for ILR to work. When DPM performs an ILR, DPM actually mounts the VM's virtual hard disk and that is how it is able to look inside of it. Windows Server 2008 is not able to mount VHDs but Windows Server 2008 R2 is able to mount VHDs, this is why Windows Server 2008 requires the Hyper-V role. Another point to note is if your DPM server is virtualized on Hyper-V itself, it cannot perform ILR if it is Windows Server 2008. It can perform ILR as a virtualized machine on Hyper-V if it is running Windows Server 2008 R2. Other requirements for successful ILR are: The VM's VHD has to have at least one volume and the guest OS in the VM cannot be on a dynamic disk.

Let's look at how to perform an item-level recovery:

1. Open the **DPM Administrator Console**.

2. Click the **Recovery** tab.
3. Under **Protected data** browse to the Hyper-V host that contains the VM that holds the items that you want to recover. Click on this VM to highlight it.
4. To view the list of files and folders that can be recovered, drill down into the VM by double-clicking the VHD that you want to recover items from:

   Once again drill down by double-clicking **Virtual Machine Volume**. This will bring you into the hard drive structure so you can see the items you want to restore:



5. Select the items (files and folders) that you want to recover. You can select multiple files and/or folders to restore at the same time. Do this by holding down the *Ctrl* key on your keyboard and clicking on the items you want to restore.
6. Once you have the data you want to recover, right-click on the items and select **Recover**. This will launch the recovery wizard.
7. Review your recovery selections then click **Next**.
8. The only option you have is to copy the data to a share on the network. Click **Next** to continue.
9. Review the recovery selections then click on **Recover**.

Restoring SharePoint data with DPM

When SharePoint is protected by DPM you have the ability to restore an entire farm, SharePoint sites, document libraries, lists, documents, and other objects. Restoring of any type of SharePoint data is pretty straightforward. We are going to look at the process of restoring SharePoint data in DPM.

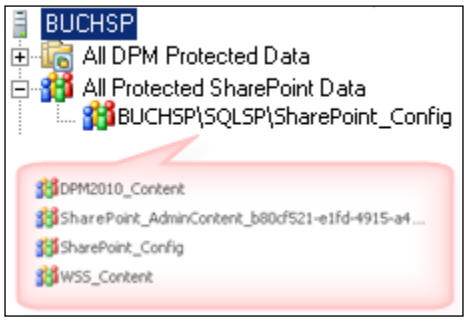
Farm recovery

Backing up an entire farm consists of the configuration, service application, and Central Administration databases. These databases can be backed up individually but this is not supported by Microsoft. If you run into problems restoring this way you will be on your own. Microsoft says restoring individual databases can lead to data corruption in the SharePoint farm. It is best practice to enable SharePoint protection and protect your SharePoint farms this way. In DPM 2010 there no longer is a need for a SharePoint recovery farm when protecting SharePoint 2010. Most SharePoint environments are pretty standard. However some SharePoint environments are not all out of the box and do have customizations. These can be things such as custom settings to the `web.config` file or other settings and files in the SharePoint directories. The best way to protect this information is to back up the System State and the SharePoint directory on the web front end.

NOTE: When protecting SharePoint 2010 no recovery farm is needed, however, when protecting SharePoint 2007 a recovery farm is still required.

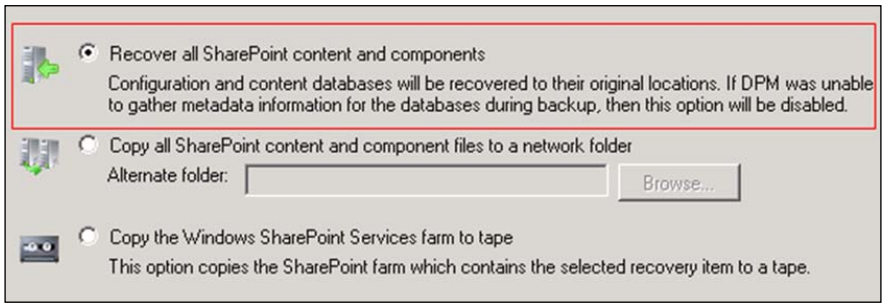
Here are steps to recover a SharePoint farm:

1. Open the **DPM Administrator Console** and click **Recovery**.
2. Browse to **All Protected SharePoint Data** in the **Protected data** pane and select it.
3. In the **Recoverable item** pane, right-click on the **config** database and choose **Recover**. DPM will start the **Recovery Wizard**:

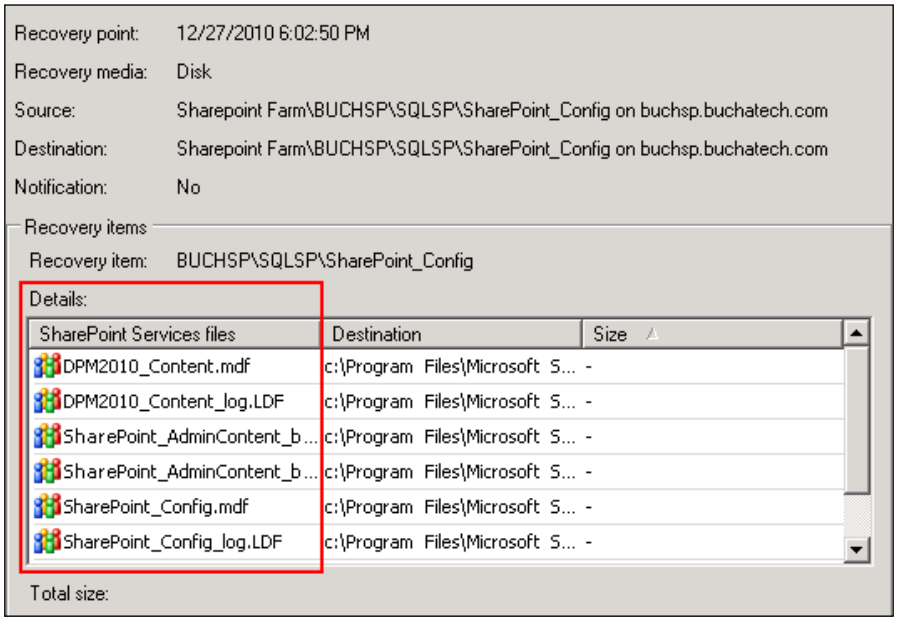


NOTE: Recovering the **config** database will recover the entire farm and all content databases. In DPM all of this data is within the **config** database. If you were to double-click on the **config** database you would see the content, configuration, administrator content, and any search application databases you are protecting.

4. Review your recovery selection, and click **Next**.
5. Specify the type of recovery you would like to perform. Select **Recover all SharePoint content and components** like in the screenshot to recover the entire farm. You can copy to a tape or alternate location but the data will then need to be restored manually later.



6. Choose one of the recovery options and click **Next**. Once again you can set the network bandwidth usage throttling, SAN-based recovery, and e-mail notification.
7. You can now review your restore settings. Notice in the screenshot you will see a list of all databases that will be restored as a part of your farm recovery. Once you are done reviewing click **Recover**.



Recovering sites, documents, and lists

The process of restoring sites, documents, and lists is the same as restoring item-level data which we will cover next. When DPM creates recovery points, it catalog the SharePoint farm. DPM gathers a list of anything in the SharePoint object hierarchy that is stored within a SharePoint content database. All of these items such as sites, documents, and lists then become recoverable. The process for recovering one of these objects is the same process and will be covered under item-level recovery next.

Item-level Recovery

One of the best features of DPM 2010 is the item-level recovery of SharePoint 2010 data. We learned how to enable this type of protection for our SharePoint farms in *Chapter 7*. This item-level recovery is actually utilizing a new feature of SharePoint 2010 called **Unattached Recovery**. An Unattached Recovery can actually be performed in SharePoint 2010 itself without the need for DPM. However without using DPM the process has many more steps and is therefore prone to operational errors. DPM actually locates the recovery point of the content database, restores the entire database, then exports the file from the unattached content database, and re-imports it into the live SharePoint site. Without DPM you would be completing all of those steps on your own. DPM makes this easier and less painful.

During the item-level recovery DPM requires these three things:

- A temporary SQL server instance to restore the content database
- A directory on SQL server to temporarily hold the databases files
- A directory on the web front end to temporarily hold the restored item in `cmp` form

You will be able to input the location of the SQL server and locations for the data in the recovery wizard. This will be demonstrated soon when we walk through the recovery process. The data will be cleaned up automatically by DPM when it is done with the restore process. It is recommended to use a non-production SQL server, and non-production SharePoint farm to store the temporary data. Now let's run step by step through an item-level recovery in DPM, following these steps:

1. Open the **DPM Administrator Console**. Click on **Recovery** in the navigation bar.
2. Under **Protected data** browse to the SharePoint server you want to recover data from.

3. In the **Recoverable item** pane double-click on the content database you want to recover data from:

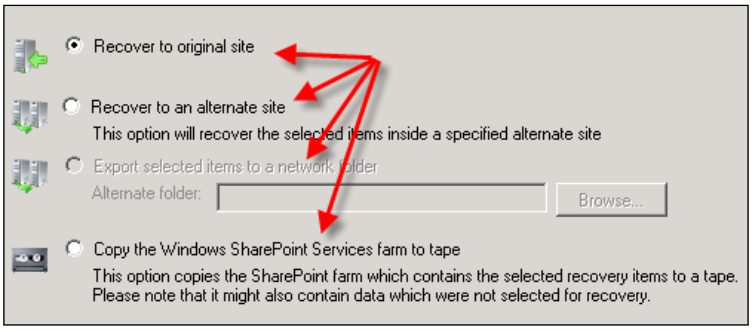
This will drill down further into the database. You will be drilling down into the SharePoint object hierarchy. The hierarchy consists of site collections, sites, lists, and libraries and then objects such as pictures, office documents, and PDFs or list items. In the following screenshot you can see a drill down into a site all the way down to `AllItems.aspx` in the link list. You could recover this item if you needed to. That is the level of granularity that you get with DPM protection of SharePoint:

In the Recoverable item pane you also have the option to navigate up if you need to.

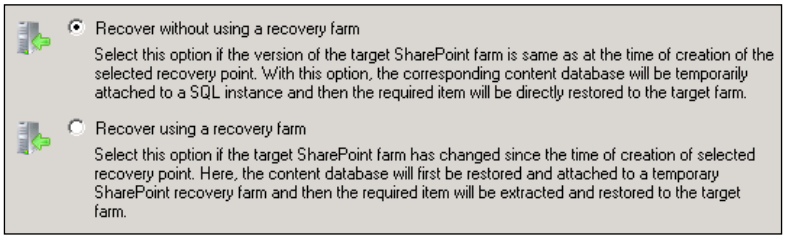
4. Once you found the SharePoint object you want to restore, right-click on it and choose **Recover**:

5. Review your recovery selection, and click **Next**.

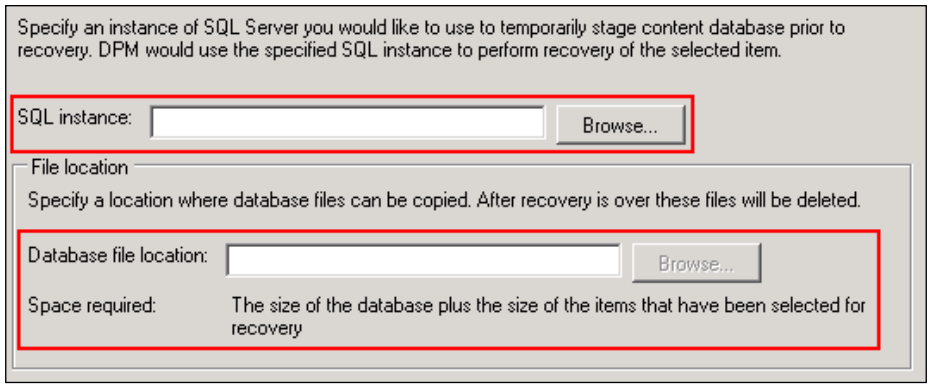
6. Specify the type of recovery you would like to perform. In this example we will select **Recover to original site**. Click **Next** to continue:



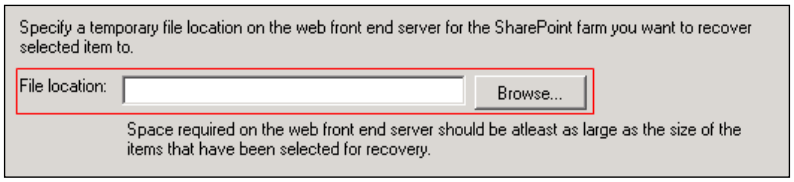
7. Select a recovery process. In this example we are going to **Recover without a recovery farm**:



8. This screen is where you specify temporary locations for the recovery. We covered this at the beginning of the ILR section. You need to specify a SQL instance that DPM can place the database on and a directory that DPM can place the database files in. The database and files will be removed once the restore is completed. Click **Next** to continue.



9. Specify a temporary directory on the SharePoint web front end to store the recovery data:



10. Choose one of the recovery options and click **Next**. Once again you can set the network bandwidth usage throttling, SAN-based recovery, and e-mail notification.
11. Review your recovery settings, and click **Recover**.

That is it. You recovered data in SharePoint using DPM. Remember, these steps will work for recovering any object data in SharePoint except for entire farms.

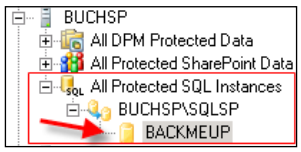
Restoring SQL databases with DPM

DPM backup of SQL databases and restore of SQL data is easy right out of the box with little configuration on your SQL servers. As mentioned before, DPM 2010 can protect SQL databases at the instance level allowing DPM to protect any databases that are added to that instance automatically. The beauty of this is that your databases will be added automatically and the recovery process is pretty straightforward. DPM 2010 also has the ability to let your database administrators perform their own restores. We will cover this as well.

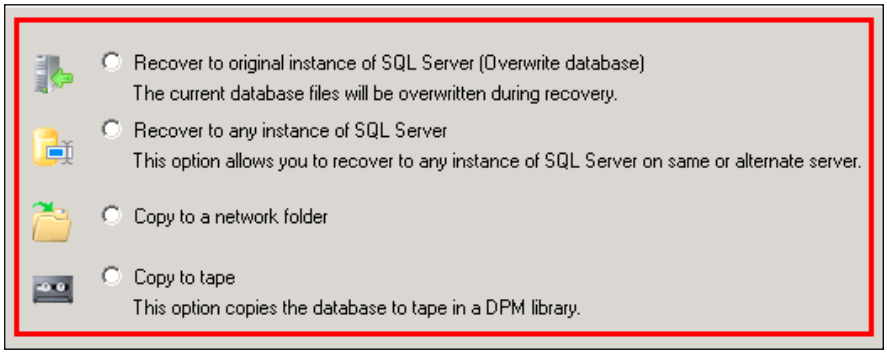
SQL database recovery

As mentioned previously, restoring SQL data in DPM is a simple process. You can restore to the original instance, a different instance, tape, or to a share on the network. This is possible because DPM allows recovery of SQL server databases at the instance level. The following steps will demonstrate how to recover a SQL database:

1. Open the **DPM Administrator Console**. Click on the **Recovery** tab.
2. Under **Protected data** browse the SQL server you want to recover data from. Expand the SQL instance to see all of the protected databases:



3. In the **Recoverable item** pane right-click on the content database you want to recover data from and select **Recover**.
4. The DPM **Recovery Wizard** will pop up, make sure your selection is correct then click **Next**.
5. Specify the type of recovery you would like to perform such as the options that appear in the following screenshot and then click **Next**:



   - If you choose to recover the database to the original SQL instance you will have the option to leave the database as operational or as non-operational. If you choose operational the database will be ready to use as soon as the recovery is completed. If you choose non-operational the database will be restored to the SQL server but it will not be live. Choosing non-operational gives you the opportunity to restore additional transaction logs or perform other tasks on the database if you need to before putting it back into production.
   - If you choose to recover your database to an alternate SQL server instance you will need to browse to the SQL server and specify the location for the `.mdf` and `.ldf` SQL database files. You can also change the name of the the recovered database on the alternate SQL instance during the alternate SQL server instance recovery type.
   - Choosing to recover the database to a network folder or tape is the same process as recovering files, folders, or volumes to a network folder or tape. This will give you the SQL database backup file and you can move it around as you choose from here.
6. On the next screen you can choose to retain the security settings of the original location, or the new location. At this point you can also choose to add network throttling, SAN recovery, and the behavior in regards to versions and to receive a notification when the restore is complete. Click **Next** to continue.

7. On the next screen you have one more chance to review your recovery options. Click **Recover** when ready.

Those are all the steps to recover database from within the DPM Administrator Console.

Configuring and using SQL self service recovery for SQL administrators

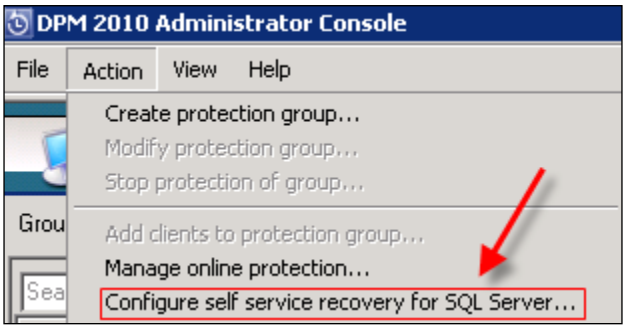
DPM 2010 has another new feature that allows database administrators to restore their own SQL databases. This feature is known as self service recovery for SQL. It is done by creating groups in the Active Directory or specifying users that can restore certain databases and where they can restore them to. Additionally it is easy to configure. We didn't cover this in *Chapter 7*, but we are now going to look at how to set this feature up and how to perform a restore using it.

Setting up self service recovery for SQL

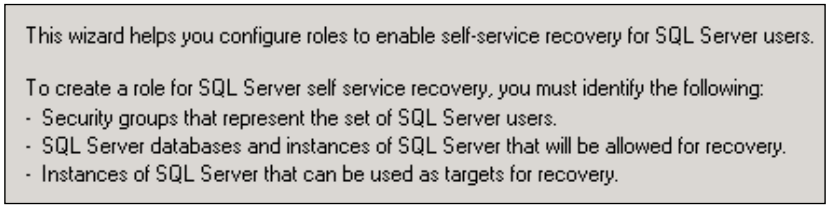
We need to create a role that has the permission to recover databases. Here are the steps to do this:

1. Create a group in the Active Directory. We have one called **SQLDBAS** in this example. Add the user accounts of your database administrators to this group.
2. Go to your DPM server and open the **DPM Administrator Console**. Click on the **Protection** tab:

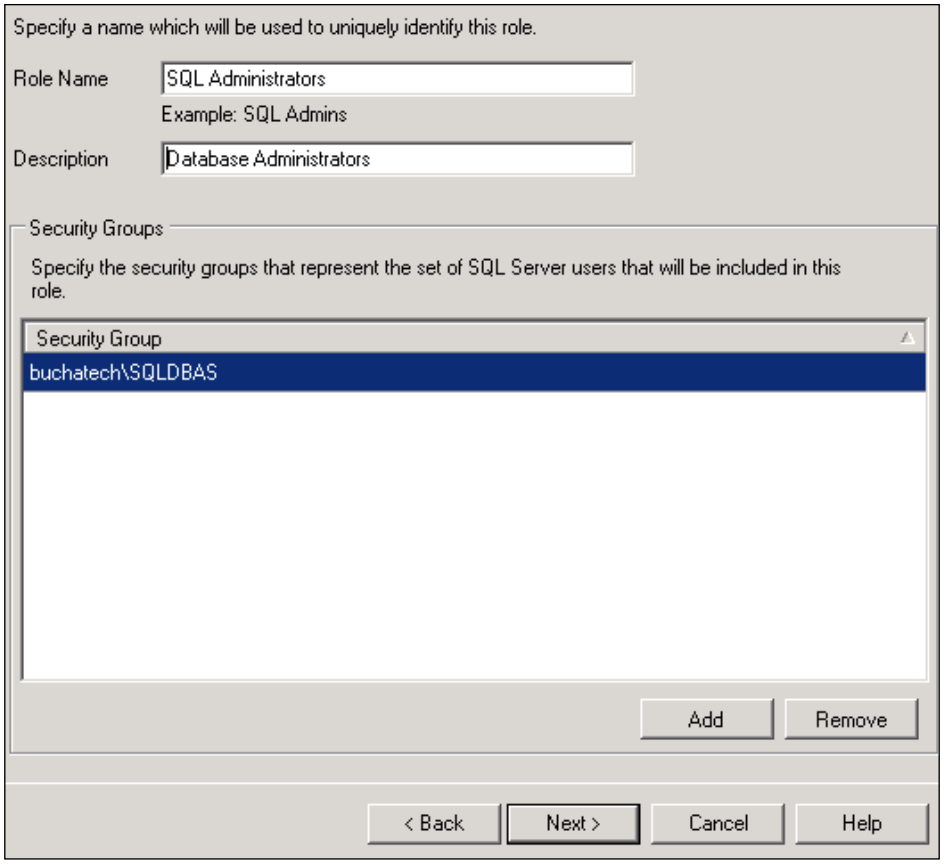
3. Click on **Action** then select **Configure self service recovery for SQL Server**:



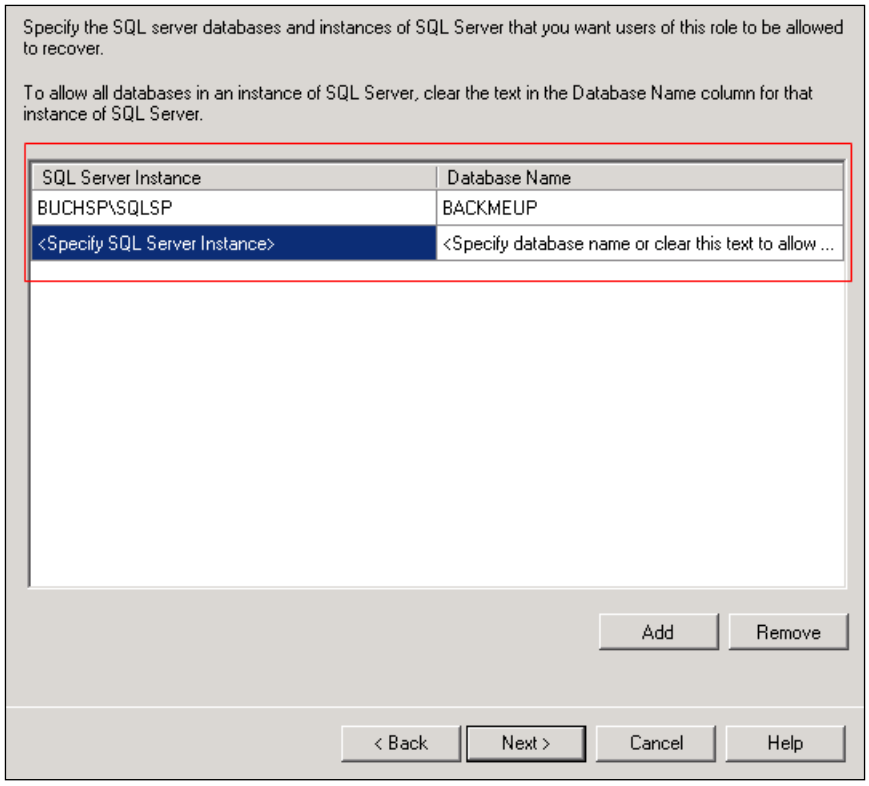
4. The **DPM Self Service Recovery Configuration Tool** for SQL server window will pop up. Click **Create Role**.
5. Click **Next** on the **Create New Role** page.



6. On the **Specify Security Groups** page give your new role a name and a description. Click **Add** and browse through the Active Directory to add the group your database administrators are in. Once the group has been added click **Next**:

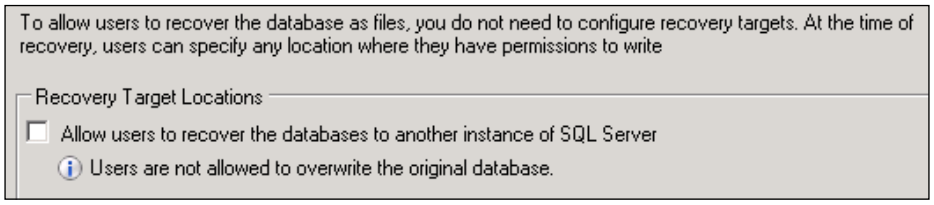


7. On the **Specify Recovery Items** page add the SQL instances and databases that this new role will be allowed to recover:

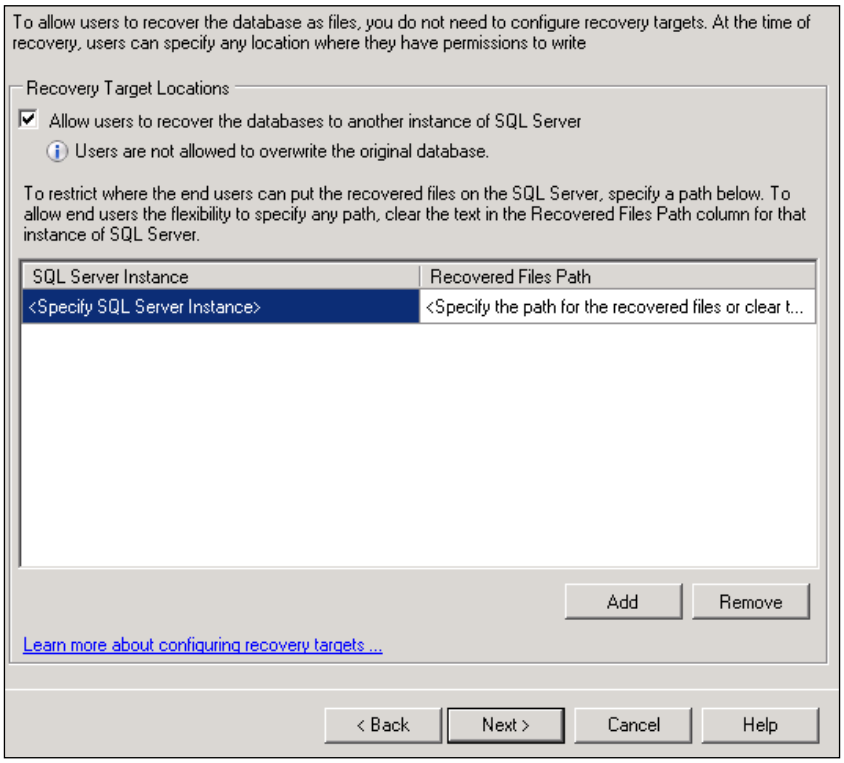


8. On the **Recovery Target Locations** page you can give your database administrator accounts permission to recover databases to other SQL instances. If you give the user this permission a new table will become available where you can specify the instances that users are allowed to recover to. Click **Next** to continue.

   The following screenshot is displayed without the table:



The following screenshot is displayed with the table:



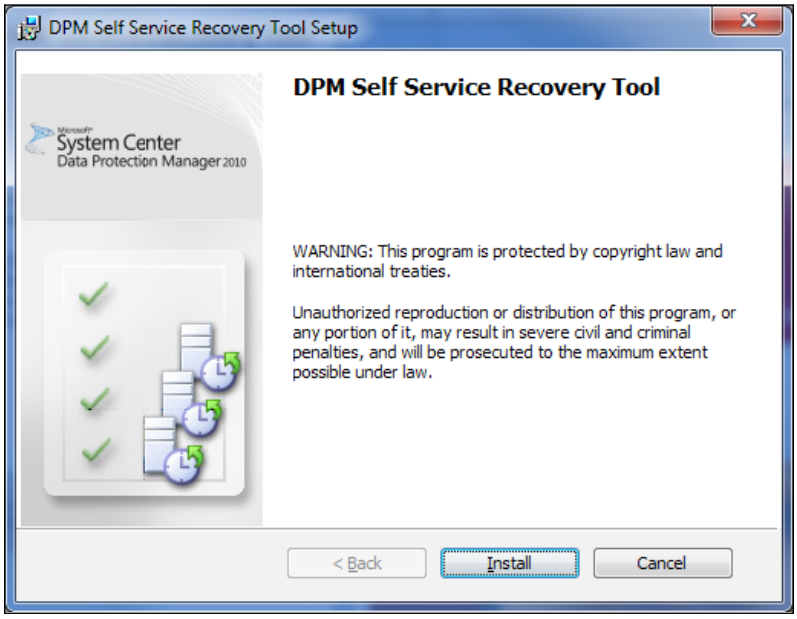
9. Review your settings and click **Finish** when you are done.
10. When it is done a window will pop up and notify you that the configuration has been successfully saved. Click **OK** on this.

Recovering through self service recovery for SQL

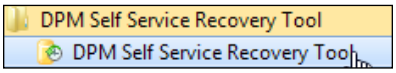
Okay, so we have the role in DPM created and our database administrators have the ability to recover databases on their own. Now we need to give them the interface to perform the recoveries through. This is called the **DPM Self Service Recovery Tool**. This tool does not need to be installed on a SQL server to work. It will run on a server OS or a client OS. This is good because your database administrators can run this tool from their workstations. The following steps show how you set this up on a client machine:

1. Put the DPM 2010 installation disc in your client computer.

2. Launch either `DPMSQLEur_x64.msi` for 64 bit computers or `DPMSQLEur_x86.msi` for 32 bit computers in the `DpmSqlEURInstaller` folder on the DPM 2010 installation disc.

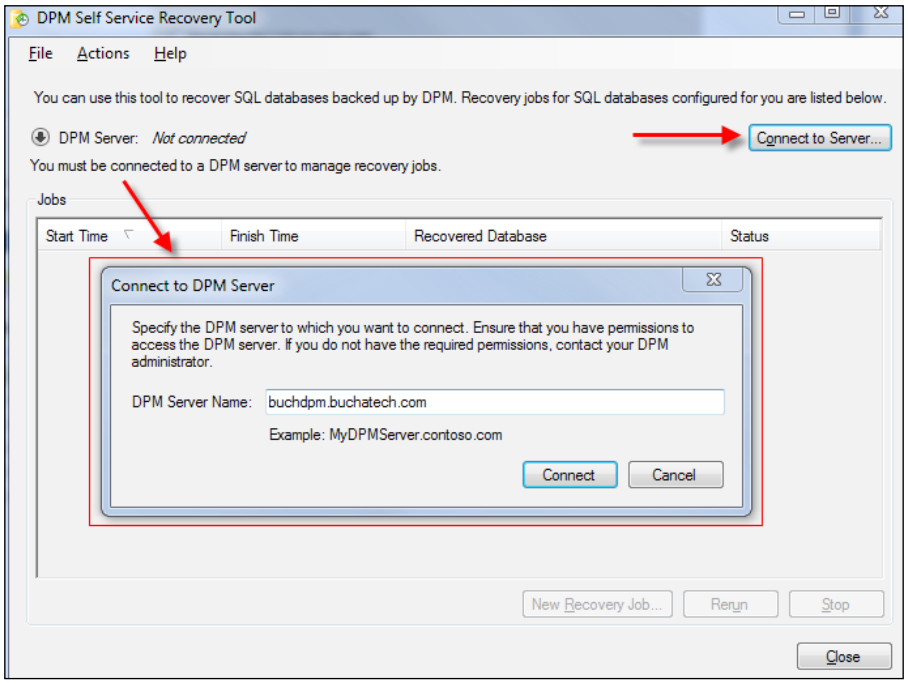


3. On the first screen click **Install**. The tool will then be installed.
4. Click **Finish** when done.
5. Go to **Start** | **All Programs** | **DPM Self Service Recovery Tool** and open the **DPM Self Service Recovery Tool**:

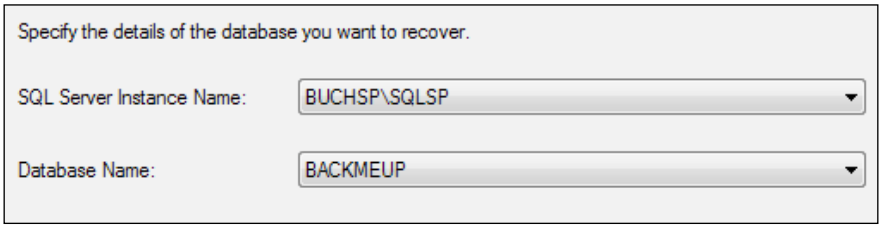


6. Click the **Connect to Server** button inside the tool.

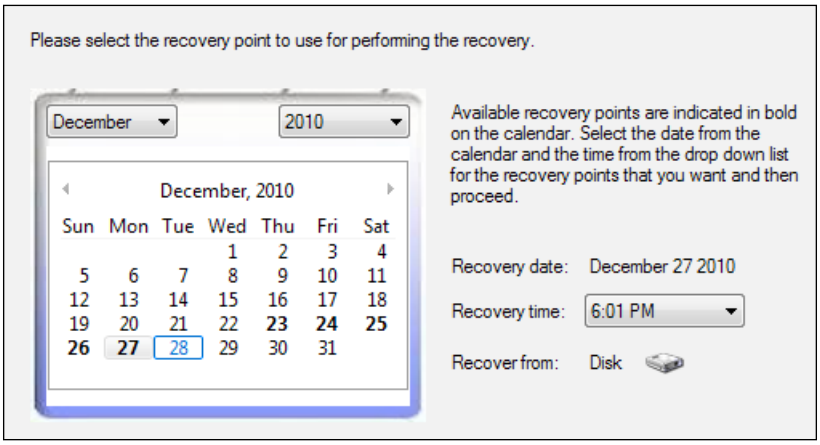
7. Enter your DPM server that is backing up your SQL databases:



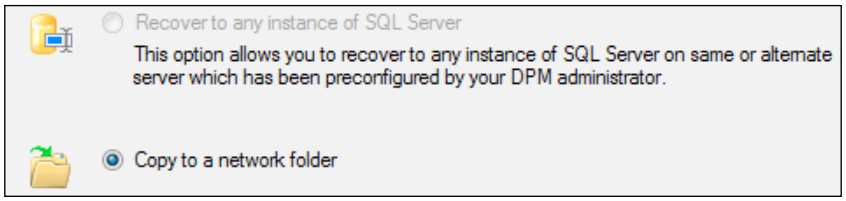
8. After you are connected to the DPM server click on the **New Recovery Job** button to launch the **Recovery Wizard**.
9. On the **Recovery Wizard** screen click **Next**.
10. You will see the available SQL instances and databases that you have permission to recover. Select the database you want to recover in the drop down box and click **Next**.



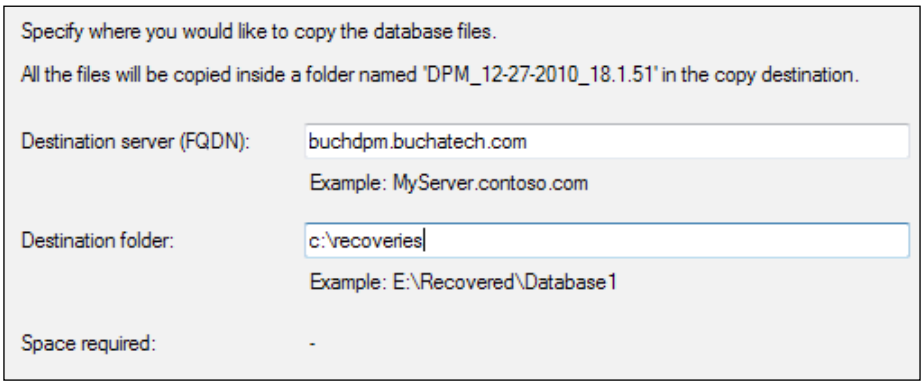
11. On this screen select a date and time of the recovery point. Click **Next** to continue:



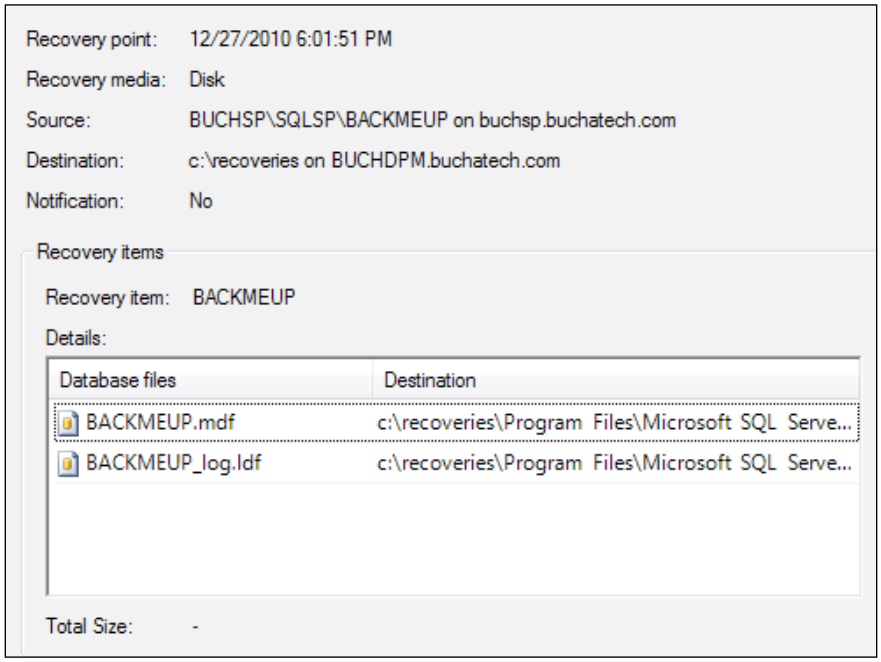
12. Select the **Recover Type** and click **Next**. You have the option to recover to the SQL instance or to a network folder:



13. Set the destination of the recovery. You need to input the name of the server and a directory on that server. Click **Next** to continue:



14. Choose your recovery options and click **Next**.
15. Click **Recover** and the restore will begin.



That's the process for recovering SQL databases using the **DPM Self Service Recovery Tool**. As you can see it is similar to recovering a SQL database in DPM.

Summary

The very purpose of having a backup is to restore critical data. As you can see once again DPM is a powerful tool with several features and capabilities which make an administrator's life easier and offers some of the best protection around.

In this chapter, we covered the basic recovery options in DPM including items such as System State recovery, Bare Metal Recovery, and file/folder recovery. We then dived into more advanced and specific recovery items such as recovering SQL databases, SharePoint data, Exchange mailboxes, and Hyper-V virtual machines.

In the next chapter we will get into offsite backup and protecting your DPM server.

9

Offsite, Cloud, Backup and Recovery

Inexperienced and experienced backup administrators should know that offsite backups are critical to your disaster recovery plan. You never know when a natural disaster such as a flood, earthquake, or a fire could strike. DPM does a great job of providing a solid onsite backup that makes it fast to recover data; but what happens if a natural disaster takes out your office along with your onsite backup? You better have an offsite backup somewhere. With DPM you have several offsite backup options.

With DPM you have several offsite backup options, which will be covered in this chapter. Let's talk about where offsite backup has been and where it is headed. Traditionally, backups have been transported offsite using removable storage media such as tapes or optical storage such as CDs and DVDs. Some companies choose to manage and store their own offsite backups. Other companies choose to have their backups managed and stored by third-party companies that provide offsite backup services. Backup administrators had to either have someone physically take the offsite storage home or to another location. This is a problem because people can easily lose such devices.

As a backup administrator you could pay an offsite provider to transport the tapes or optical storage for you but this could be expensive. These forms of offsite backups also consist of slow data retrieval because someone has to transport the data back to the office.

Fast forward to the age of increased bandwidth speeds and lowered cost of disc storage. Both have introduced two more options to the backup offsite market. These new options copy backups to external hard drives using SCSI, USB, FireWire, and eSATA or send your backup data to an offsite location directly over the Internet. There are benefits to each; some of these are: external hard drives are cheaper than tapes and tape libraries, and offsite backup via the Internet provides faster restores because you can pull the data right back down to your office via the Internet.

The beauty of DPM is that it can utilize any of these options. DPM takes advantage of the newer offsite technologies in the market giving backup administrators multiple offsite options to choose from. DPM is capable of combining these options or using one of the options by itself. For example, DPM can back up to disc then to tape or back up only to tape. In this chapter we are going to cover what your backup offsite options are and how to configure them in DPM.

These are the topics that will be covered in this chapter:

- DPM offsite backup
    - Disk-to-Disk-to-Tape
    - Backing up DPM using a secondary DPM server
    - Backing up DPM using third-party software
- DPM cloud backup
    - Iron Mountain CloudRecovery®
    - i365 EVault

DPM offsite backup

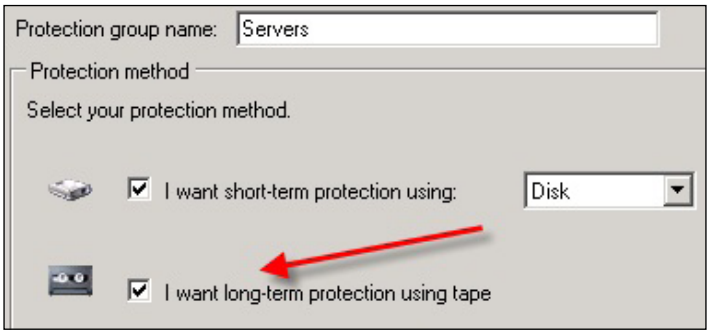
We are going to learn about the three non-cloud offsite solutions for backing up your DPM server. Two of these solutions can be utilized with DPM right out of the box without purchasing other software or services from another vendor. The third solution is actually using other software to back up your DPM server. The solutions are Disk-to-Disk-to-Tape, backing up DPM using a secondary DPM server, and backing up DPM using a third-party software. These solutions also serve as Disaster Recovery for your DPM server. Now let's get into more detail on each of these solutions.

Disk-to-Disk-to-Tape

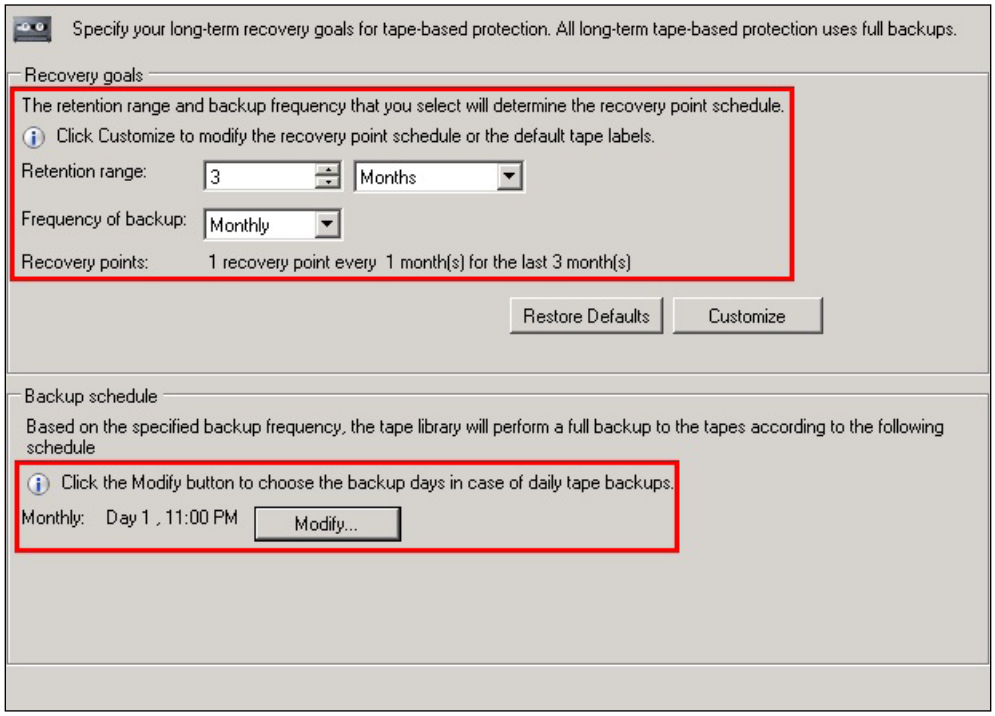
Disk-to-Disk-to-Tape (D2D2T) is an approach of backing up data to disk first and then periodically copying this data to a tape. This is one way you could get the speed of backing up to disk and the ability to store data on tapes offsite. One downfall to this is if you need to restore from tape this process can be lengthy. This backup scheme would be best for archiving data. When data is archived you are not retrieving that data very often therefore you avoid the often slow restores. Of course this decision will be made based on offsite requirements in your backup plan. Now let's look at protecting data using a D2D2T scheme in DPM:

NOTE: You need to make sure your tape, tape library unit, or external drives, that are made to look like tapes by Firestreamer, are already installed on the DPM server and are configured under the **Management** tab in DPM. If you need more information on Firestreamer, revisit *Chapter 4*.

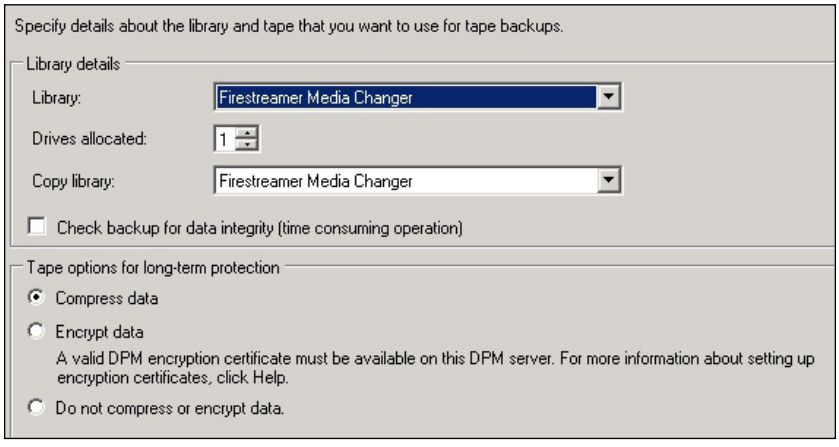
1. Go to your DPM server and open the **DPM Administrator Console**.
2. Click on the **Protection** tab.
3. Either create a Protection Group or modify an existing one.
4. Click **Next** on the **Select Group Members** screen.
5. On the **Select Data Protection Method** screen, put a check mark next to **I want long-term protection using tape**:



6. Click **Next** until you reach the **Select Long-Term Goals** screen. On this screen you need to specify how long you want to retain the data, the frequency of the backup to tape, and the backup days and time. Click **Next** to continue:



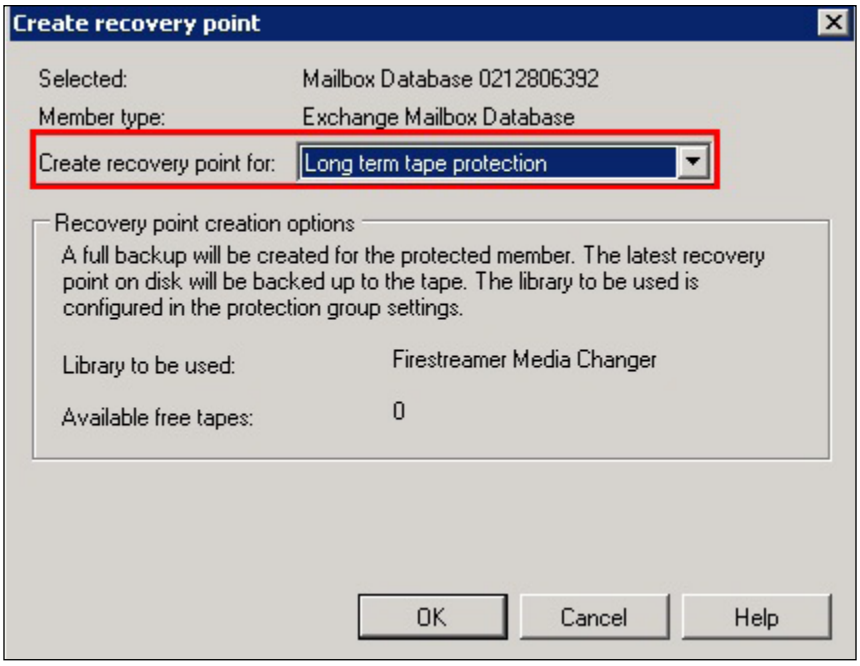
7. On this screen choose your tape or tape library and choose what options to have on the data such as encryption or compression. Click **Next** to continue.



8. When you come to the last screen of the modify/create Protection Group wizard, Click **Update Group** to commit the changes to the Protection Group.

Now your protected data will be copied to tape based on the schedule you specified. You can also perform a manual backup to tape by following these steps:

1. In the DPM Administrator Console, go to the **Protection** tab.
2. Right-click on the **Protected Members data** object and choose **Create Recovery point.**
3. In the **Create recovery point for** drop down list choose **Long term tape protection**. This will create a recovery point on your tape. Click **OK:**



NOTE: DPM can protect its own database natively, only when it is being backed up to tape. To enable DPM to protect its own data you will first need to run a command in PowerShell. This command is `Set-DPMGlobalProperty-AllowLocalDataProtection$true`. You will learn about using PowerShell for DPM in *Chapter 10*.

That wraps up the D2D2T solution. Many environments still have tape hardware, either as a single unit or a tape library, and this gives IT professionals a way to continue using this hardware with DPM.

Backing up DPM using a secondary DPM server

Another option for protecting your DPM server is to back it up with another DPM server. Your main server is known as the primary DPM server and the other DPM server is known as the secondary DPM server. The primary DPM server backs up the protected servers directly. The secondary DPM server protects the databases and the replicas on the primary DPM server. This provides disaster recovery for your DPM solution in the event the primary DPM server fails.

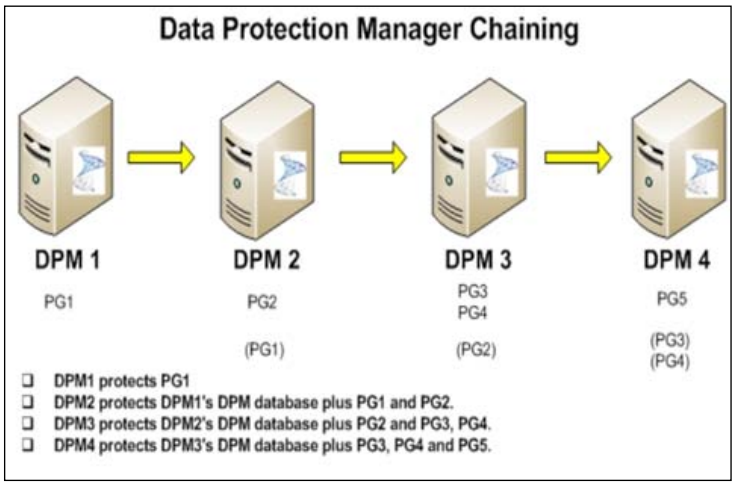
Using this solution will allow you to continue backing up the protected servers that are on the primary DPM server in the event of the primary DPM server failing. You will have the primary server's database and replicas on the secondary server. You can use these to rebuild the primary DPM server moving the backup of the protected servers back to the primary DPM server. It is also possible to switch primary protection to the secondary DPM server and it is possible to restore to the protected computer directly from the secondary DPM server.

NOTE: Something that you should be aware of is two new features in DPM 2010 called **Cyclic protection** and **DPM Chaining**:

- **Cyclic protection**: is good for companies with branch offices. With this type of protection two DPM servers are able to protect each other. For example, let's say you have DPM server A and DPM server B; DPM server A protects everything on DPM server B and DPM server B protects everything on DPM server A. The data from both servers (office locations) will therefore exist due to each other.
- **DPM Chaining**: is literally creating a chain of DPM servers. Each DPM server in the chain protects the next server in the chain. For example, let's say you have DPM1, DPM2, and DPM3 in the chain. DPM1 is a primary DPM server, DPM2 is a secondary DPM server to DPM1 and/or primary DPM server as well, and then DPM3 is a secondary DPM server to DPM2. A secondary DPM server can protect the DPM database of the primary DPM server along with replicas that the primary DPM server protects. Also take note that if a DPM server that protects its own local data such as: DPMDB, C:, System State, and so on that this will break the chain.

Here is a link to more information for setting up DPM chaining: `http://technet.microsoft.com/en-us/library/gg410636.aspx`.

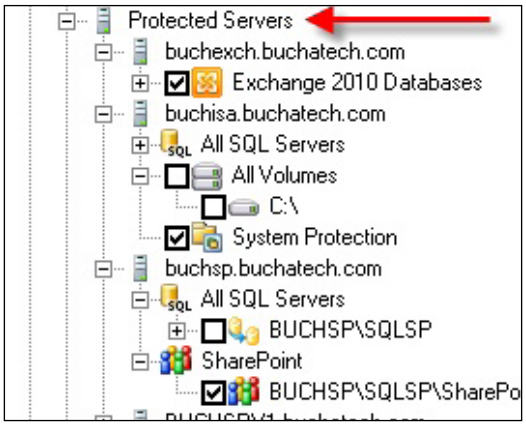
See the following diagram on DPM Chaining:



Protecting DPM with a secondary server can be used as a DR solution for onsite or offsite. To use this solution as an offsite you would simply set up a site to site VPN that the two DPM servers could communicate over. The two DPM servers would also need to be in the same domain or in a fully trusted domain. It is recommended that the secondary DPM server is built on the same site. First, let the data synchronize and then move the secondary DPM server offsite. Here are the steps to enable protection of a primary DPM server on a secondary DPM server:

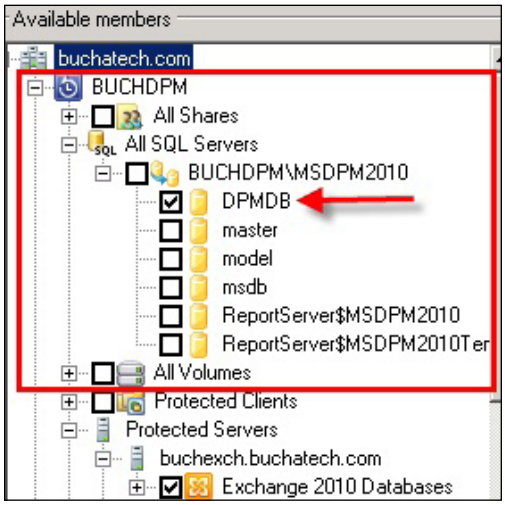
1. From your secondary DPM server install the DPM protection agent on the primary DPM server. (you can find the agent installation process in *Chapter 6*).
2. On your secondary DPM server open the **DPM Administrator Console**.
3. Click on the **Protection** tab.
4. Create a new Protection Group.

Communication needs to be established between the secondary DPM server and the protected servers on the primary DPM server. This is done by selecting those data sources under **Protected Servers**. Note that you will only see **Protected Servers** on this screen when it is a secondary DPM server backing up a primary DPM server.



NOTE: If you are protecting Exchange data on your primary DPM server remember to copy over the `Ese.dll` and Eseutil.exe files from your Exchange server to your secondary DPM server. Also take note that if you are protecting Exchange 2003 you will need the `Ese.dll` and `Eseutil.exe` from Exchange 2010 because they are backwards compatible and they will allow you to protect Exchange 2010, 2007, and 2003.

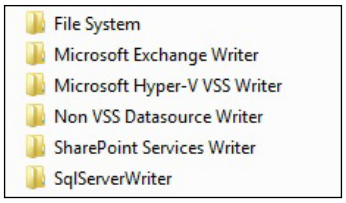
Be sure to back up the primary DPM server's database as well.



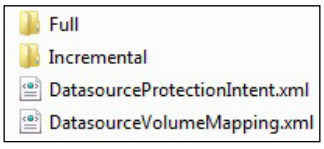
Backing up DPM using third-party software

If you choose to back up DPM using third-party software it is ideal to choose one that supports DPM or VSS. Software that is designed to work with DPM will support the DPM VSS Writer service. If the software does not support DPM but supports VSS, it simply uses the shadow copy service that comes with Windows. Using the VSS service and not the DPM VSS Writer can cause the backup process to become more complex. You can also use third-party backup software that does not support DPM or VSS. In order to use a backup solution that does not support DPM or VSS you need to use a DPM tool called **DPMBackup**. No matter what third-party software you choose to go with, essentially the DPM database and the replicas are the components that need to be backed up. A replica is a complete copy of the protected data. The DPM database stores your DPM settings and configuration information:

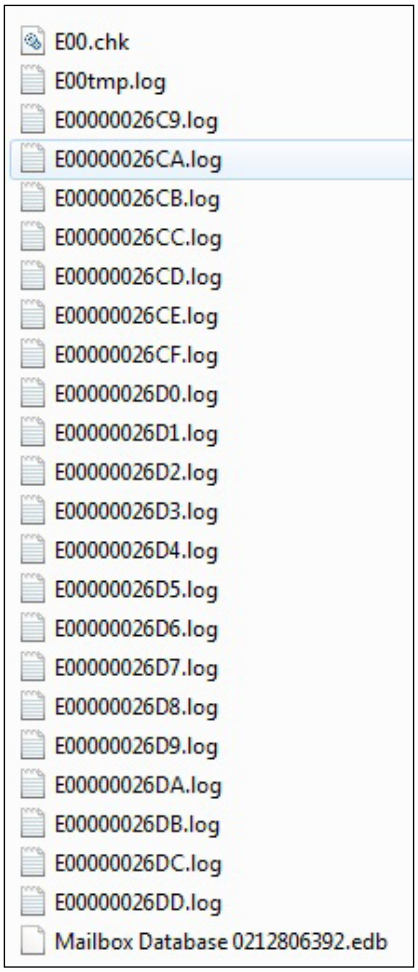
- The DPM database is located on your DPM server at the following location: `%systemdrive%\ProgramFiles\MicrosoftDPM\DPM\DPMDB`. It will be a file called `MSDPM2010.mdf`. In the simplest terms, the DPM database contains a map of where your data is located within the replica structure. You need these two in order to successfully bring a dead DPM server back to life.
- Let's have a look at the replica folder structure so you can see why the DPM database contains a map. Replicas are stored on your DPM server here: `%systemdrive%\ProgramFiles\MicrosoftDPM\DPM\Volumes\Replica`. In the replicas you will see a folder structure similar to the following:



If you drill down into each folder you will see a folder with a very long name beginning with "vol_" and then a series of letters and numbers. Here is an example of the name: `vol_37bbdd6d-38cf-4a1a-97ae-2d4653c31a47`. If you drill down further you will find a folder called `Full` and one called `Incremental`. These contain the actual replicas of the data that you are protecting:



- In this example let's drill down and look at our Exchange database. We will drill down to: `%systemdrive%\Program Files\Microsoft DPM\DPM\Volumes\Replica\MicrosoftExchangeWriter\vol_37bbdd6d-38cf-4a1a-97ae-2d4653c31a47\7caeaadb-3a2b-4223-b89c-d34785170816\Full\C-Vol\ProgramFiles\Microsoft\Exchange Server\V14\Mailbox\MailboxDatabase0212806392`. Now as you will see in the screenshot this contains our actual mailbox database and all the Exchange temp and log files:



In theory you could copy this out to your Exchange server and do a recovery right from this. However the advantages of doing a recovery with DPM is that DPM simplifies the restore process and you can recover individual mailboxes.

If this was SQL we would see `.mdf` and `.ldf` files. If it was Hyper-V you would see `.vhd` files or if it was just word documents that were being protected you would see `.docx` files. We need to see this to get a better understanding of what the replicas are and to see how important it is to back them up along with the DPM database. This is where your actual data resides and where the DPM configuration is. Other items that you can include in your DPM backup are:

- DPM reporting database `ReportServer.mdf`.
- `bin` folder located at: `%systemdrive%\Program Files\Microsoft DPM\DPM\bin`. This may contain custom PowerShell scripts you utilize for DPM.

These items are not required to recover a DPM server. Now let's look at restoring the DPM database and the replicas. This will essentially be the same across any third-party software you choose. In the following examples we will act as if the DPM server failed and you have new hardware that will become your new DPM server. You will need to use a command-line tool called `DpmSync`. It is used to restore the DPM database to a SQL instance and to synchronize the DPM database with the replicas in the storage pool.

Follow these steps to restore a DPM database:

1. Rebuild your server with the OS and prepare your SQL instance if you plan to use a remote one.
2. Install DPM on the replacement hardware.
3. Make a folder to store the DPM database restores in.
4. Recover the DPM database that you have backed up to this folder.
5. Now you must use the `DPMSync` tool to reattach the DPM database. Here is the syntax for this:

   ```
   DpmSync-RestoreDb -DbLocLOCATIONOFYOURBACKEDUPDPMDB-
   InstanceNameNAMEOFSQLINSTANCEYOUWILLUSE
   ```

   When this runs the DPM service will be stopped and then restarted.

Before you can even restore a replica, its status in DPM needs to be set as **manual replica creation pending**. The following steps will show you how to restore DPM replicas:

1. Run `DpmSync-sync` to finish the database restore process and start the replica restore process. Running `DpmSync-sync` will change the replicas status to **manual replica creation pending**.
2. Run `DpmSync-ReallocateReplica` to reformat replicas that are marked as missing and change their status to **manual replica creation pending**. This is actually reallocating disk space from the storage pool for the replicas.

3. Now manually create the replica by using the **Restore to replica** option from a secondary DPM server or run the `RestoreToReplica` command in the DPM Management Shell to restore from tape. Either of these options are how you restore the replica. The **Restore to replica** option will be available in the **Recovery task area** on the secondary DPM server. Choose the data sources you need and go through the restore process. Instead of restoring the data choose **Restore to replica**.

Third-party tool that supports DPM

Ideally you will want to use third-party software that supports DPM natively if you are forced to use a third-party tool for your DPM backup. This will give you a tool that will be intuitive to DPM and minimize the steps it will take to back up and restore DPM.

Follow these steps to back up the database:

1. From the console of the third-party backup program, browse to `%systemdrive%\Program Files\Microsoft DPM\DPM\DPMDB`, and select the DPM database. The filename of the DPM database is `MSDPM2010.mdf`.
2. Select where you will back up your database to.
3. Start the back up and you should end up with a `.bak` file when it is all complete.

Follow these steps to back up the replicas:

1. From the console of the third-party backup program expand the DPM server.
2. Select the data on the protected computers that you want to back up.
3. Select where you want to back up the data to.
4. Start the back up.

Third-party tool that supports only VSS

Okay, so this is the option where your third-party backup supports VSS. You need to make sure that this software does not modify data on the replica volumes. If it does in anyway your backups could easily become corrupt. The safest backup type to use to ensure the data will not be modified is copy.

Follow these steps to back up the database:

1. From the console of the third-party backup program, browse to `%systemdrive%\Program Files\Microsoft DPM\DPM\DPMDB` and select the DPM database. The filename of the DPM database is `MSDPM2010.mdf`.

2. Browse to `%systemdrive%\Program Files\Microsoft DPM\Prerequisites\data\` and select the DPM report database. The filename of the DPM report database is `ReportServer.mdf` on the DPM server.
3. Select where you will back up your database to.
4. Start the back up and you should end up with `.bak` files when it is complete.

Follow these steps to back up the replicas:

1. From the console of the third-party backup program browse to `%systemdrive%\Program Files\Microsoft DPM\DPM\Volumes\Replica\` on the DPM.
2. Select the folders of the protected computers that you want to back up.
3. Select where you want to back up the data to.
4. Start the back up.

Third-party tool that does not support DPM or VSS

DPMBackup must be used when using a third-party backup solution that does not support the DPM Writer service or VSS. It is not recommended to use a third-party backup solution that does not support the DPM Writer service or VSS. This makes backing up your DPM server more complex. **DPMBackup** is a command-line tool that can back up and restore DPM databases and replicas.

This tool creates backups of the DPM database and the DPM reporting database. It creates read-only shadow copies of all the replica volumes on your DPM server. It puts these shadow copies in in the following location on your DPM server: `%systemdrive%\Program Files\MicrosoftDataProtectionManager\DPM\Volumes\ShadowCopy\`. These shadow copies will be organized by server name. Here are the steps for creating the DPM database backup and the replica shadow copies.

Follow these steps to back up the DPM database:

1. From an elevated command prompt run this syntax: `DpmBackup.exe-db`. It will create a `DPMDB.bak` file at the following location: `%systemdrive%\Program Files\Microsoft DPM\DPM\Volumes\ShadowCopy\DatabaseBackups\`.
2. From the console of the third-party backup program, browse to `%systemdrive%\Program Files\Microsoft DPM\DPM\Volumes\ShadowCopy\DatabaseBackups\` and select the `DPMDB.bak` and `ReportServer.bak` databases.
3. Select where you will back up the database to.
4. Start the backup.

NOTE: If your DPM database is hosted on a remote SQL instance you can either back up the DPMDB using a SQL backup tool or you can run this syntax for a DPM database that is on a remote SQL instance: `DpmBackup.exe-db-instanceNameNAMEOFSQLINSTANCEGOESHERE`.

Follow these steps to back up the replicas:

1. From the same command-prompt window run: `DPMBackup.exe-replicas`. This is going to place shadow copies of your protected data here: `%systemdrive%\Program Files\Microsoft DPM\DPM\Volumes\ShadowCopy\`. Remember these will be organized by protected computers.
2. From the console of the third-party backup program browse to `%systemdrive%\Program Files\Microsoft DPM\DPM\Volumes\ShadowCopy\` and select the folders of the protected computer that you want to back up.
3. Select where you want to back up the data to.
4. Start the back up.

Re-establishing protection after recovering the primary DPM server

Many times after you restore a DPM server, the agents for your protected computers will show errors. These will need to be repointed and synced to the newly restored DPM server. To do this:

1. Go to your protected computers.
2. From a command prompt navigate to: `%systemdrive%\Program Files\MicrosoftDataProtectionManager\DPM\bin\`.
3. Run `SetDpmServer.exe-dpmServerName YOURDPMSERVERNAMEGOESHERE`.
4. Go back into DPM and refresh the agent status of your protected computers.

DPM cloud backup

These days you can go to any search engine on the Internet, search for offsite backup and you will get hundreds of results. These results are companies offering offsite backup services. At the time of writing this book there are only two offsite backup providers that support DPM. These companies are Iron Mountain and i365. There are other offsite backup providers out there that can back up DPM but keep in mind that they are not a supported provider. Do not get the term "supported" confused. That term means these companies have partnered with Microsoft and tailored their solution to work with DPM. Microsoft itself does not assume responsibility for the services provided by these two companies.

To find out more about Microsoft cloud backup options go to this link:

`http://www.microsoft.com/systemcenter/en/us/data-protection-manager/dpm-cloud.aspx`.

We are going to cover each of these services in further detail in this chapter.

Now other services can certainly work to back up DPM. The same principles of using third-party software to back up DPM applies here. The offsite backup provider's agent or software will need to be VSS aware and if it is not, then you will need to use the `DpmBackup` tool. With that said there are four general things you want to look for in an offsite backup provider. These are:

- **Free trial**: You want this so you can test the service to ensure it works and meets your needs before you get locked in.
- **A solid reputation of support**: Do your research and read reviews. Make sure the company has a history of good support and that they do what they say they will do.
- **Good reporting and alerts**: You need reports so that you can quickly see that your data backup is actually working. On the same note you want e-mail notifications to be at a minimum; that way you can be contacted right away if a problem with your backup were to arise.
- **Easy to use and reliable solution**: You want easy to configure and easy to use software. You don't want a cloud backup system that requires you to go through training just to use it. You also need a solution that is reliable. The last thing you need is a solution that fails when you need to recover critical data.

Now let's dive into the two current DPM offsite cloud offerings by Iron Mountain and i365.

Iron Mountain CloudRecovery®

Iron Mountain is a company that started out specializing in records management and information destruction. Iron Mountain has now moved into the backup market. Iron Mountain is known for its underground "vaults", one of them being 220 feet underground. This is where it stores records and backups.

Iron Mountain has partnered with Microsoft and offers a service called CloudRecovery that integrates directly with DPM. CloudRecovery can automatically back up your DPM data into the cloud. This service gives an administrator long-term retention, easy restores, and a web portal for administration.

To start off with the service you can go to the following link:

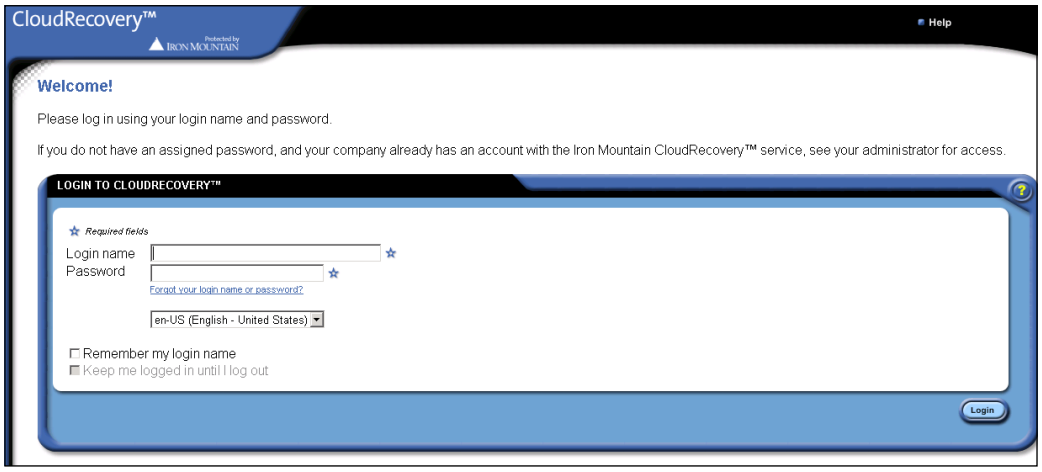
`http://ironmountain.com/forms/cloud/index.asp`

Fill out the form to get in contact with Iron Mountain and they will help you get an account set up. Once you have an account set up you will get a link to the CloudRecovery® web portal. This is where you will do all of your administration on the cloud service and get the agent for your DPM server. Let's look at installing, configuring, and using this service.

Installing the agent

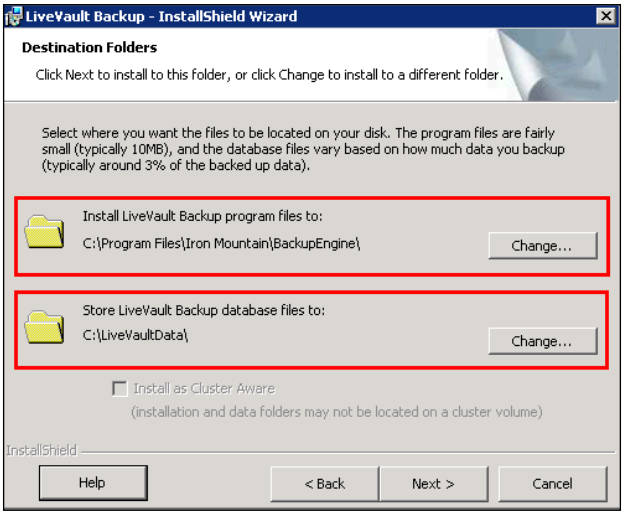
First let's install the CloudRecovery® agent. It is called **LiveVault backup**. Follow these steps to install the agent:

1. Go to the link that was sent to you by Iron Mountain and log in to the web portal. The login screen looks like the following:



2. Click on **DOWNLOADS**. Now select the agent that matches your operating system. Click the **Download** button to download the agent installation kit:

3. Launch the installation wizard by double-clicking on `LVBackupX64Agent_7.15.7466.exe`.
4. Click **Next**.
5. Accept the terms and click **Next**.
6. This screen is for the destination folders. It contains two locations. The first location is where you will install the **LiveVault** application. The Backup database files location stores any changes that are made to the source backup files. This uses snapshot technology to keep track of the changes. This takes up a lot of space, and is usually 5-10% of the total amount of data that is a part of the backup. You want to have at least 150 MB of free disk space for this location. Change these if you need to and click **Next**.

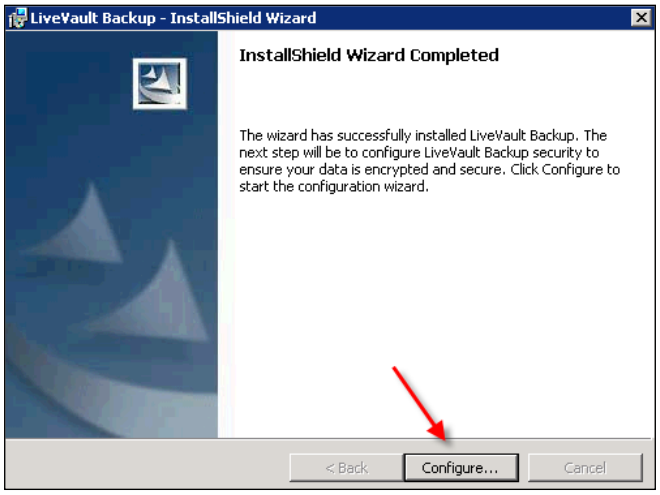


7. Click on **Install** to finish installing the agent kit.

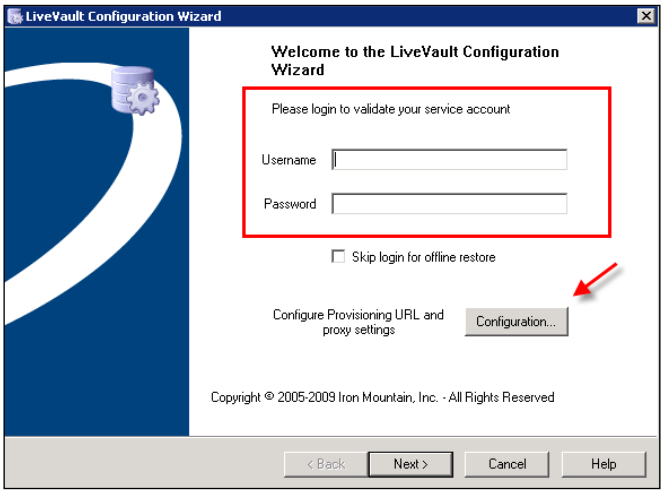
Configuring the agent

The agent has now been successfully installed and now requires configuring:

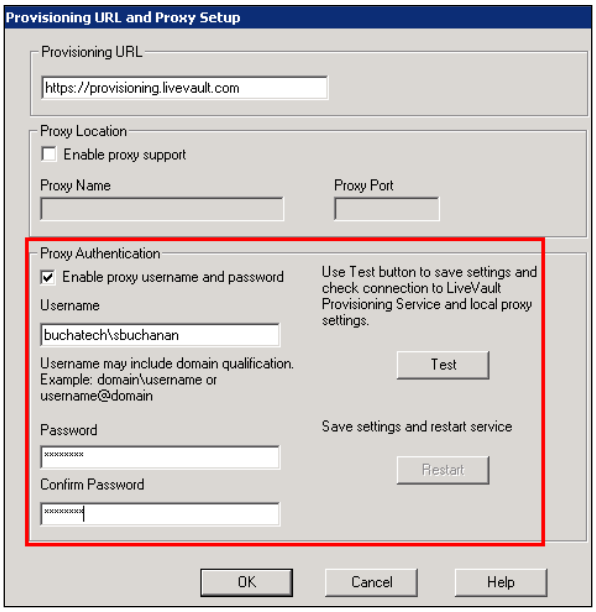
1. Click on **Configure**.



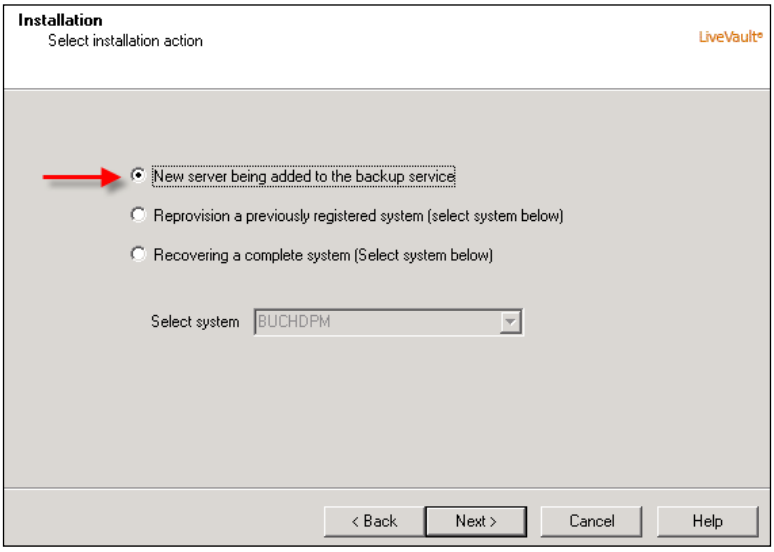
2. Enter the username and password that were given to you by Iron Mountain. These are the same credentials that you used to log into the web portal with. Click on the **Configuration** button next to **Configure Provisioning URL and proxy settings**.



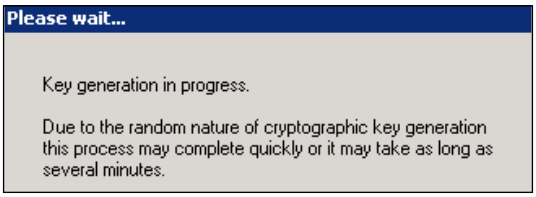
3. You need to input an Active Directory account here that has at least local administrator privileges on the DPM server. This account is used by the CloudRecovery service to connect back to your DPM server when syncing backup data and doing restores.



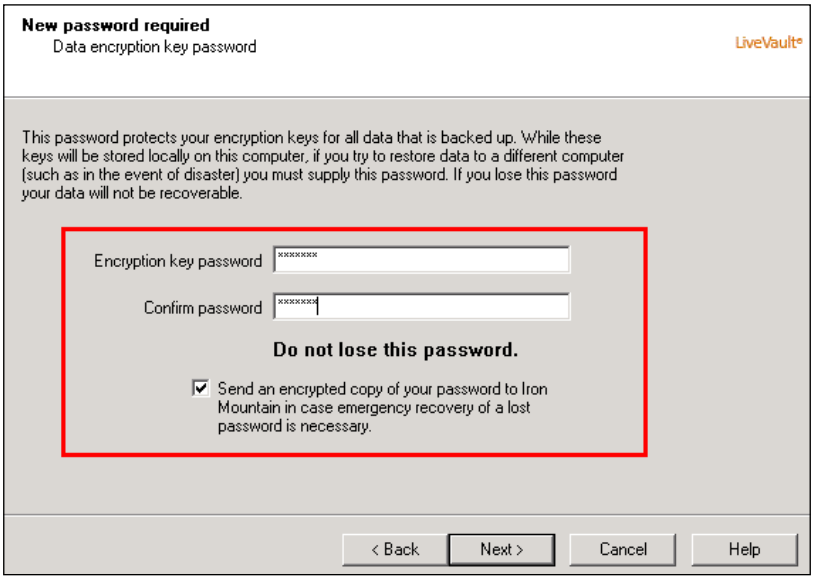
4. Select the appropriate action and click **Next**.



You will see the following status window:

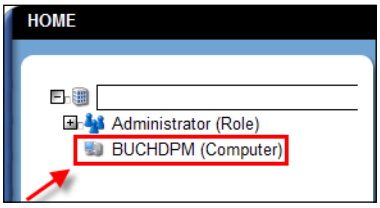


5. You will then need to set a new password to protect the encryption key for this server. There is also an option to send a copy of this key up to Iron Mountain in case you lose it. Click **Next** to continue:



6. Click the **Finish** button to complete the configuration wizard. Restart the DPM server after the installation is complete.

   The next time you log into the web portal you will be able to see the DPM server you just added:



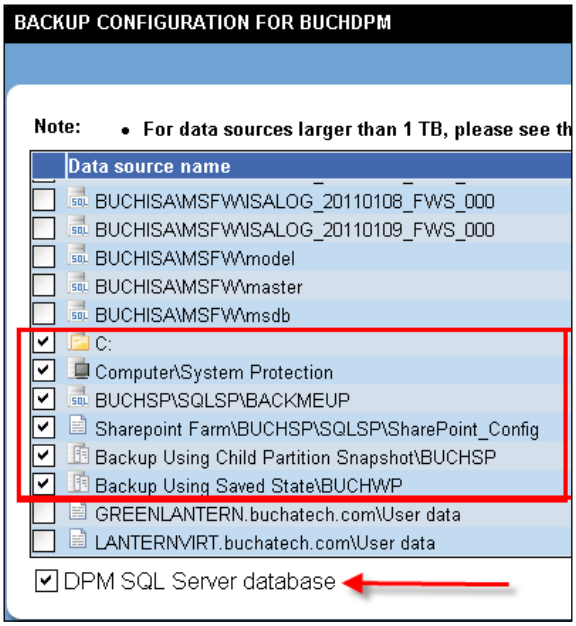
CloudRecovery and adding protected data

Now we need to add protected data to our cloud service and we will also explore the many options in the UI of the web portal:

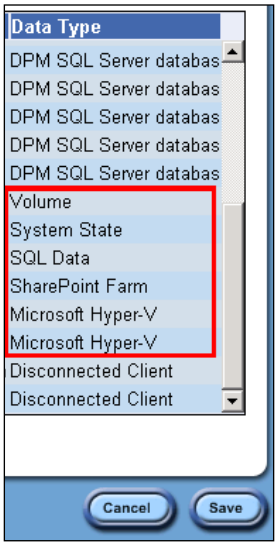
1. Log into the web portal and click on your DPM server.
2. You will then see three tabs. These tabs are:

   - The **Selection** tab allows you to choose the data you want to protect
   - The **Schedule** tab is where you set a date and time to sync your data
   - The **Options** tab is where you set how long you want to retain your data

3. Click on the **Selection** tab.
4. Select the data that you want to protect in the cloud. Your DPM server database will be selected by default:

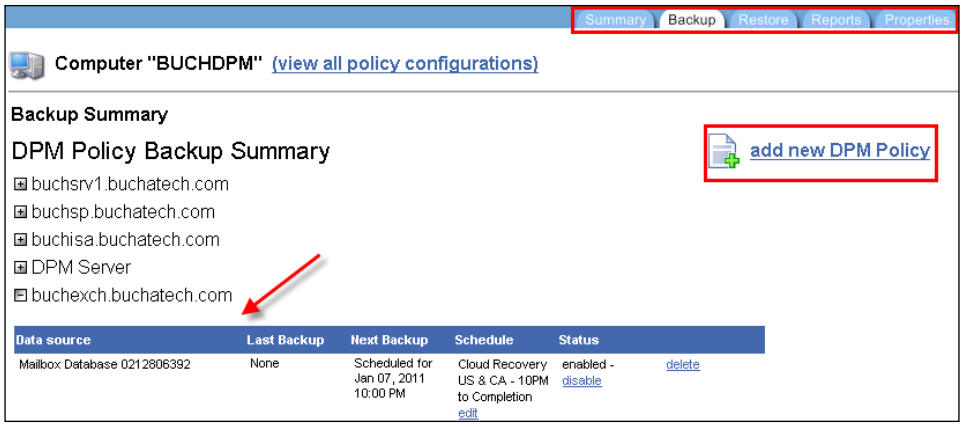


The CloudRecovery service sees the type of data just like DPM. As you can see from the following screenshot it knows when you have data such as SQL, Hyper-V, or SharePoint data.

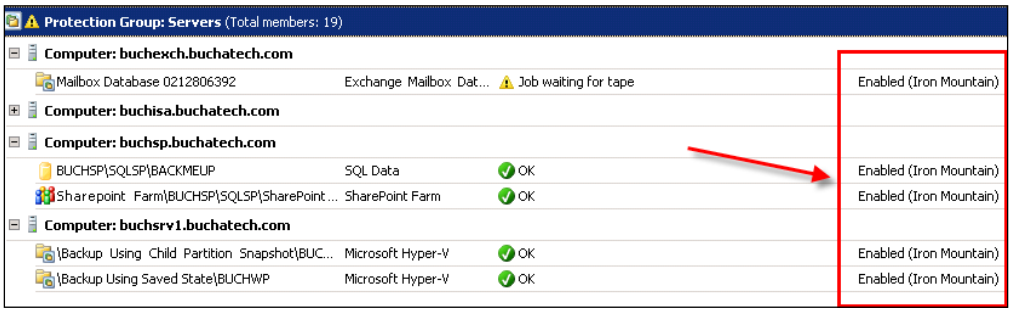


5. Click **Save** when you are done.
6. You will end up back on the main screen. On this screen you will notice many new options. These options are as follows:
    - The **Summary** tab will bring you back to the main screen
    - The **Backup** tab shows you each protected item
    - The **Restore** is where you can perform restores from
    - The **Reports** tab is where you can run reports on your protection so that you know the health of your backups
    - The **Properties** tab shows you detailed information about your DPM server such as the OS, hostname, local IP, and agent version. You can also retrieve your encryption password

    You can enable or disable the protection status, you can delete this data from protection, and you can see information about the protected data.
7. Clicking **add new DPM Policy** will bring you to the **Selection** tab where you can add more data to be protected.
8. Clicking **view all policy configurations** will give you a list of all the protection for your DPM server.



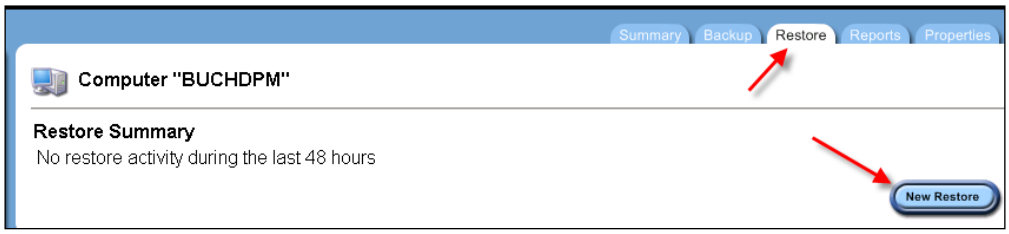
9. You will notice in the DPM Administrator Console that any objects that are protected by Iron Mountain will be listed now. You can see an example of this in the following screenshot:



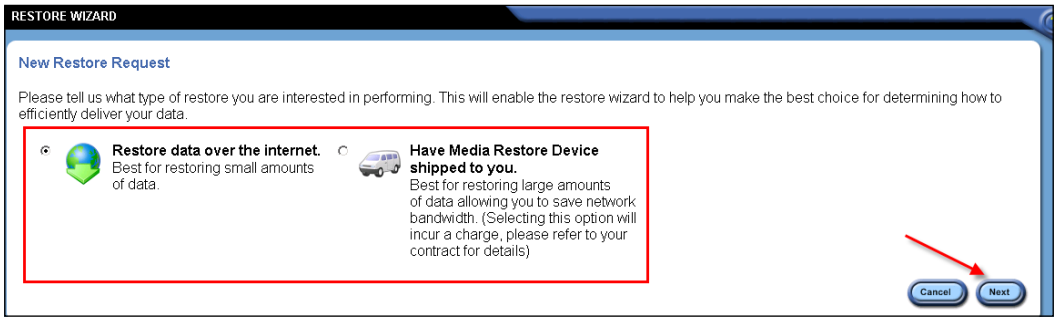
Restoring data from the cloud

With CloudRecovery there are two ways to restore data. You can restore over the Internet or have Iron Mountain ship you the data on a hard drive. There is a fee for shipping the data to you. Let's look at the steps to perform a restore:

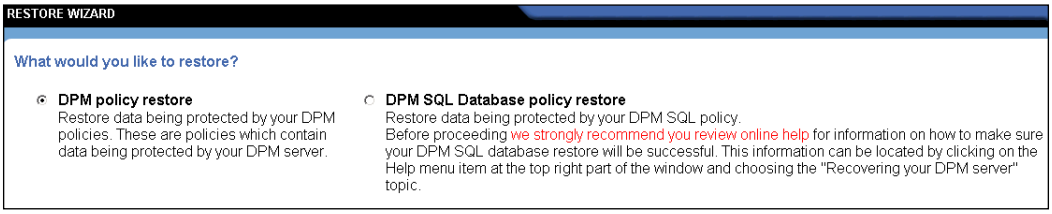
1. Click on the **Restore** tab:



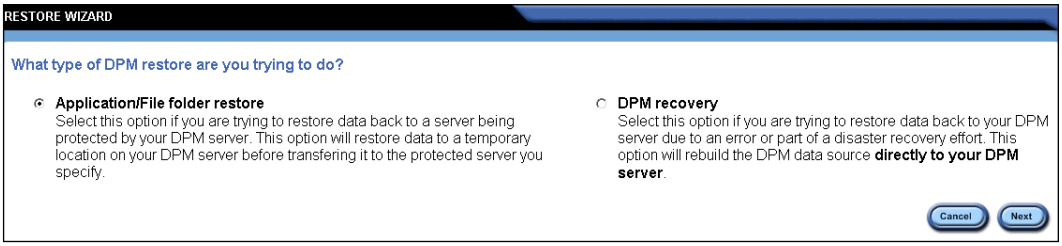
2. Choose to restore the data over the Internet or have it shipped to you. Let's choose the Internet option. Click **Next**:



3. Choose a restore option and click **Next**:
    - **DPM policy restore** means restoring directly back to the DPM server and then the DPM server restores the data back to the protected server
    - **DPM SQL Database policy restore** means restoring the DPM SQL database. This would be used if you're rebuilding your DPM server after a failure.

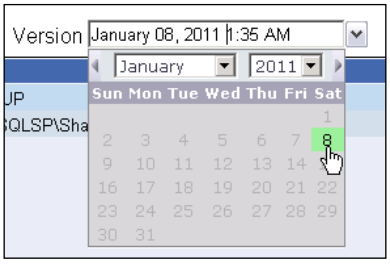


4. Now choose to restore data, an application, or to perform a DPM server recovery. These are self-explanatory. Click **Next** to continue:

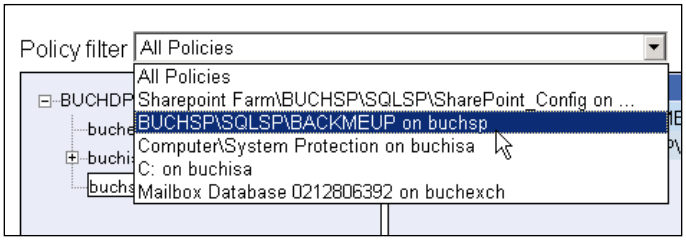


The following screen allows you to name your restore:

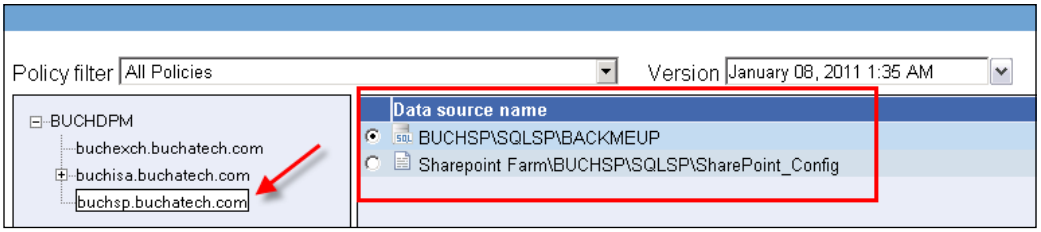
Where it says **Version** select a date to restore from:



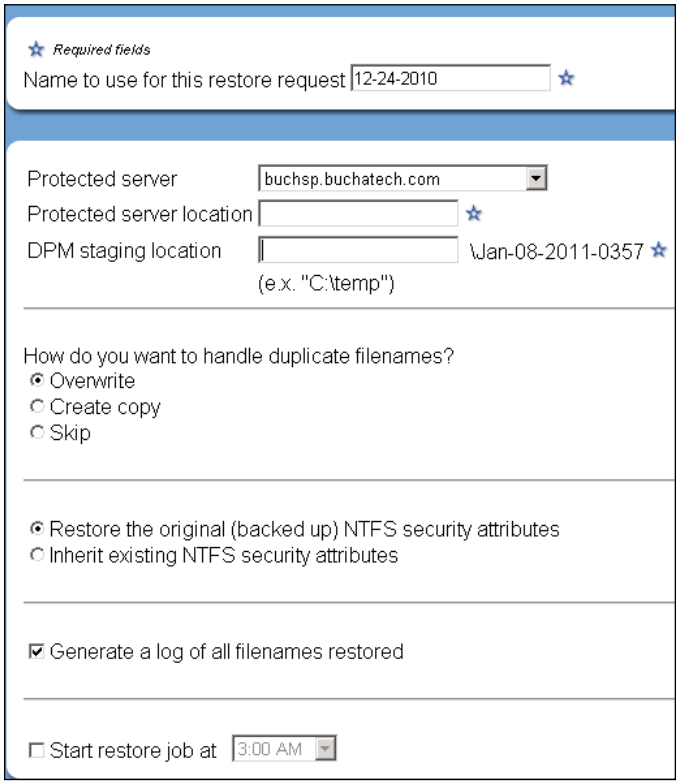
5. Go nextext to **Policy filter**; click the drop down box and select a protection policy to restore from. These are simply groups of data that you are protecting.



6. On the left-hand side of the middle pane click on the protected server you want to restore data from. All protected objects will appear in the center pane to the right. Select the data you want to restore and click **Next** to continue.



7. On this screen select the protected server. Enter the path from the protected server that the data came from into the **Protected server location** field. Enter a temporary folder on the DPM server that the data can move to until it is restored back to the original server. This field is called the **DPM staging location**. Choose what you want to do as far as duplicate data behavior, security attributes, logs, and when to start the restore. Click **Next** to continue.



8. Review your restore job and click **Done** to kick off the restore.

i365 EVault

The next cloud solution is more than just a cloud solution for DPM. It is called **EVault for DPM** often referred to as **EDPM**. EDPM is a solution by i365, a Seagate company. EDPM is a protection solution that combines DPM with EVault to offer protection for non-Windows' platforms. It comes as a physical appliance or a virtual appliance.

The appliance is made by Dell. The nice thing about a pre-configured hardware appliance is that it takes the guesswork out of making sure you get the right hardware for the job. This has already been done by i365 and Dell. The virtual appliance can be in VMware or Hyper-V format. Choosing a virtual appliance gives you the option of specifying your own hardware. EDPM gives IT professionals the ability to protect mixed environments extending protection past Windows' platforms. EDPM can back up Windows, Linux, VMware, Sun Solaris, HP-UX, IBM AIX, Novell NetWare, and Oracle databases.

What is nice about EDPM is that it is completely managed by you with the flexibility of purchasing an appliance as physical or virtual. With this product you have the option to simply back up to this appliance or to back up to the appliance and then push this data out to the i365 cloud for offsite protection. EDPM also comes with built-in deduplication so that you save on storage space. With the use of deduplication your network bandwidth will not take as much of a hit when backing up on and offsite.

EDPM has a full Windows Server 2008 R2 server with EVault and DPM already pre-installed on it. When you deploy the appliance for the first time in your environment you will configure both EDPM and DPM.

You can get an EDPM physical appliance in a 2 TB, 6 TB, or 10 TB configuration with RAID 5.i365 offering optional 24/7 service maintenance contracts for the appliance. The i365 cloud service is an optional monthly contract paid for on a per-gigabyte basis.

We are going to cover installing EDPM, installing a EDPM agent, the EDPM consoles, how to add protection, and perform a recovery. There is a lot more to EDPM than what we will cover in this section and unfortunately we will not be able to cover it all in this book.

EDPM installation

EDPM is ready to go right out of the box after some configuration. The EDPM configuration is a straightforward wizard-driven process. There is however a few things you need to have done before hand to ensure the configurations complete successfully.

The first thing you need to configure is access for EDPM through your firewall. You will need to open up the following ports:

External ports			
Ports	Purpose	Direction	Type
2547 12547	Connects internal appliance storage to i365 (required even if you do not intend to transfer data offsite)	Outbound	TCP
443 444	Appliance software updates	Outbound	TCP
80 443	Allows external users to connect to the EVault Console via HTTP/HTTPS (optional)	Inbound	TCP

NOTE: Only open external inbound ports 80 and 443 if you plan to access your EDPM dashboard from outside of your network.

Internal ports			
Ports	Purpose	Direction	Type
8086 8087	Required for communication between the EVault Console and EVault Agents	Inbound	TCP
2546	Required for EVault Agents	Inbound	TCP
80 443	Allows internal users to connect to the EVault Console	Inbound	TCP
806	Internal appliance storage management	Inbound Outbound	TCP
809	Required for internal appliance storage administration service	Inbound	TCP

Here are the rest of the items you need to have for a successful configuration:

- The Active Directory domain that this server will be joined to. Take note that once the EDPM server is joined to a domain it cannot be changed
- Determine the host name of the EDPM server
- The IP address of the EDPM server cannot change. This can be either a static IP or a permanently reserved IP address

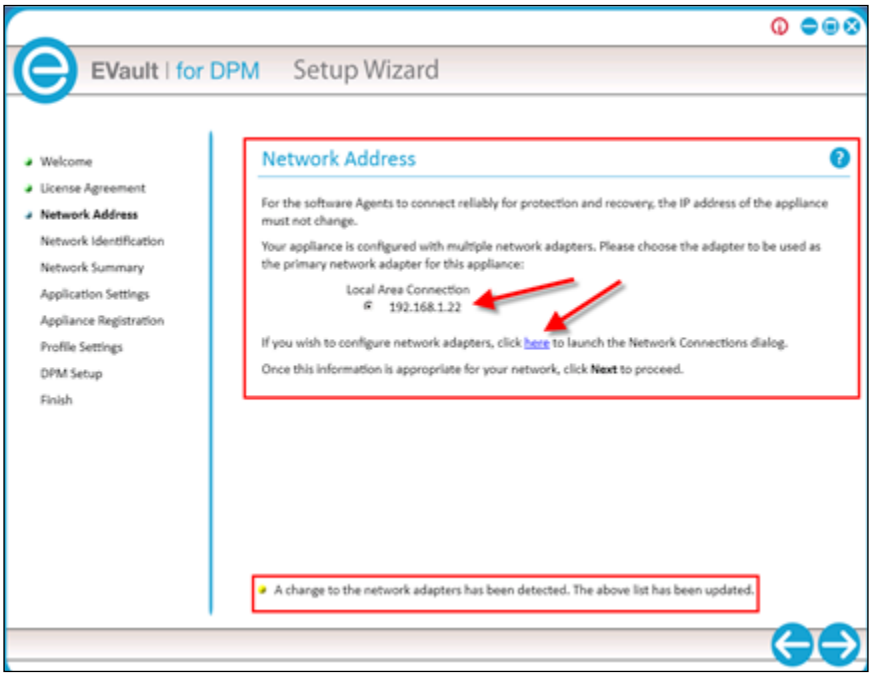
Okay those are all the prerequisites for the configurations. Here is the setup process for EDPM.

The first thing you will need to do when you boot up the appliance is to set a password for the local administrator account. Once you are logged into the server the EDPM wizard will launch automatically. Minimize this and complete these steps right away:

- Assign the server a static IP address
- Rename the computer with the host name you want to give the server and then reboot the server
- Join the server to the domain and then reboot the server

Let the server boot up and login using a domain administrator account. The EDPM wizard will come up shortly. You will see the **Welcome** screen; click the next arrow. Then follow these steps:

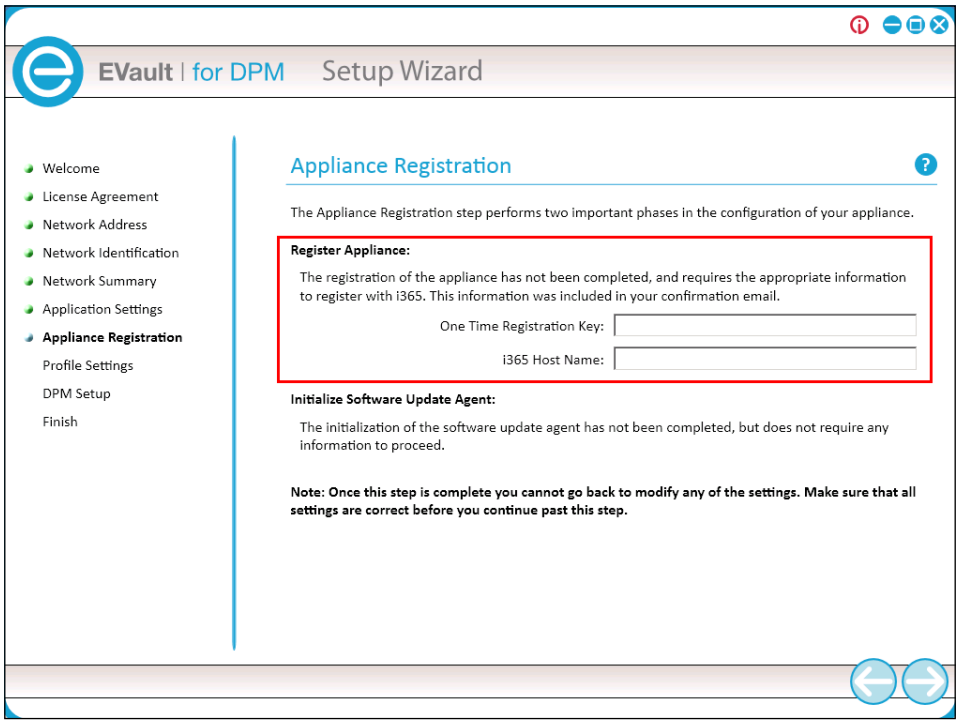
1. Scroll down check the **Accept License Agreement** and click the next arrow.
2. Verify the IP address of your sever. If you need to change the IP address do so now. When done click the next arrow:



NOTE: Your EDPM server should have its host name already set and should already be joined to the domain. If it is not joined to the domain you will get the following error:

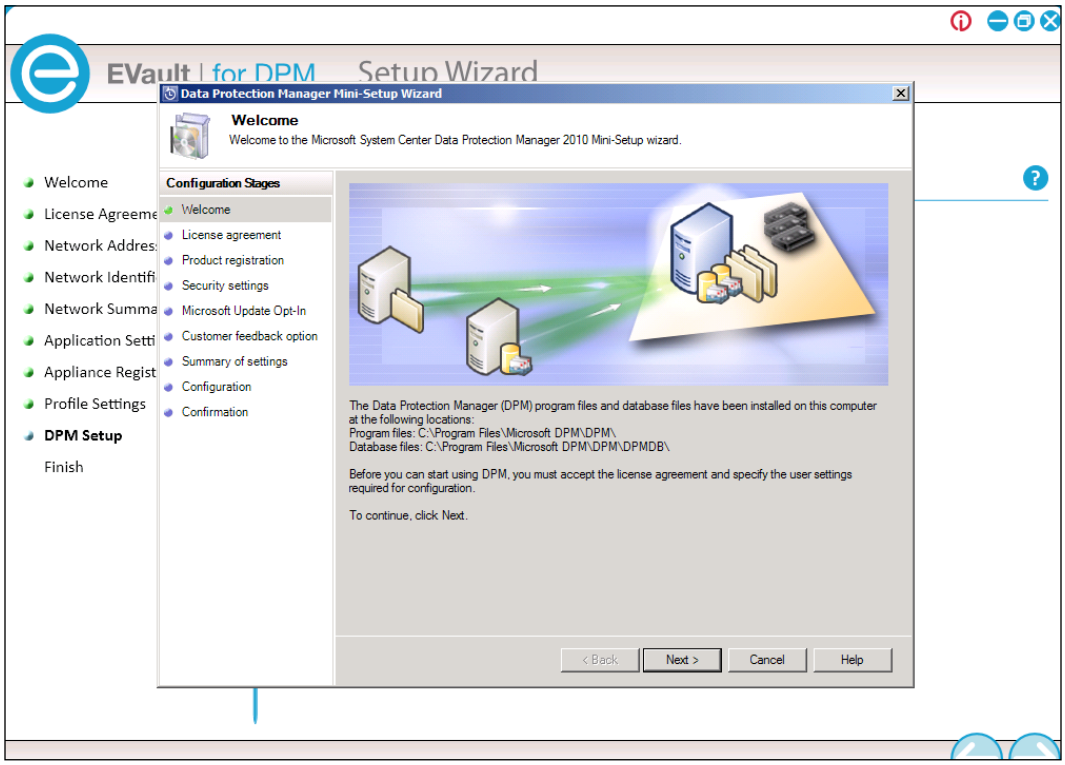
> The wizard cannot continue until the appliance is a member of an Active Directory domain. Please add the appliance to the appropriate domain for your environment.

3. Review your EDPM server's host name and domain then click the next arrow to continue.
4. Review your network summary then click the next arrow.
5. Click the next arrow on the **Application Settings** screen.
6. Now you need to register the appliance with i365. Enter the **One Time Registration Key** (example: XXXXX-XXXXX) and the **i365 Host Name** that was given to you (example: `Vault02.edpm.i365.com`) then click the next arrow.



The profile settings will be configured.

7. Now click the next arrow on the **DPM Setup** screen.
8. DPM has already been pre-installed. A DPM mini-setup will be launched. The mini-setup consists of accepting the Microsoft license terms, entering a username and a company name, setting a SQL Agent Service password, choosing to use or not to use Microsoft updates for DPM, opting in or out of the Microsoft customer experience program, and configuration of all of these settings. Enter the proper information and click **Next** to continue:



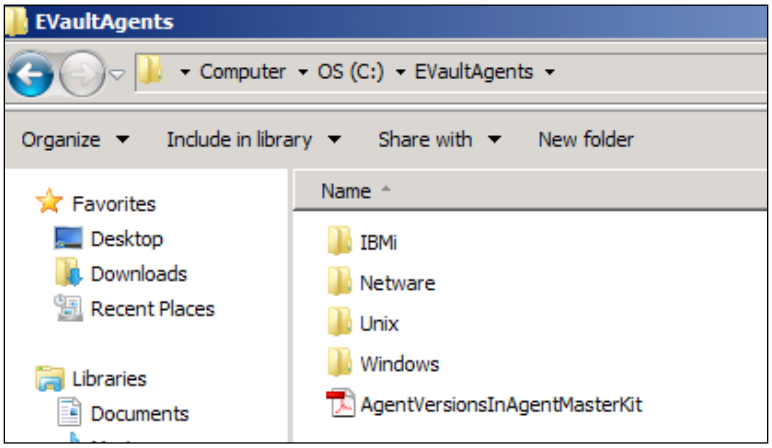
NOTE: You should stop here and go to Windows' Services then restart the WMI service for DPM to properly configure. This part of the install will fail on the appliance if you do not restart this service first.

9. Click **Close** when the DPM mini-setup completes.
10. Once the DPM mini-setup is complete you will go back to the EDPM wizard. Click the next arrow to continue.
11. Click **Finish** to complete the EDPM configuration.

EDPM is now installed. Let's now look at installing a DPM agent.

EDPM agent installation

EDPM has an installer for each platform it supports. The installation files by default are located in `%systemdrive%\EVaultAgents` on the EDPM server. You can also navigate to the agent's directory via the network using this path `\\YOUREDPMSERVERNAME\c$\EVaultAgents`. In the following screenshot you can see the platforms that EDPM has installers for:



Each agent installation folder has a PDF file in it that you can use as a guide for installing and operating the agent. We are going to cover installing the Windows and Linux agent in this section.

Windows

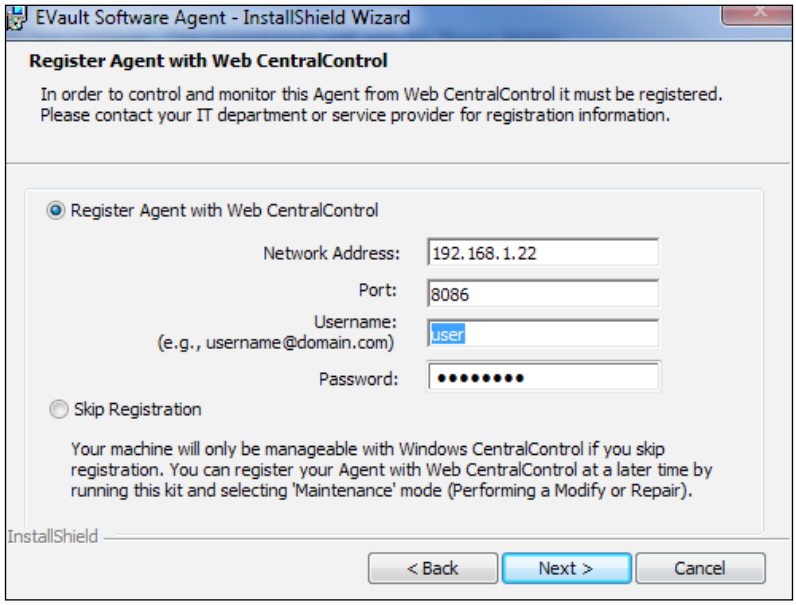
Make sure that you have local administrative privileges before you install the EDPM agent. The Windows agent is located in the `Windows` folder in the `EVaultAgents` folder on the EDPM server. You can navigate to it via this path over the network: `\\YOUREDPMSERVERNAME\c$\EVaultAgents\Windows`. You will need to copy the agent installer over to the computer you are going to protect and then install from there. Here are the steps:

1. Copy over `Agent-Windows.exe` or `Agent-Windows-x64.exe` to a folder on the local computer. Use these for 32 bit and 64 bit computers respectively.
2. Click on the appropriate agent installer to launch the installation.
3. Click **OK** to continue. The installation will be prepared.
4. Click **Next** to continue.
5. Review the release and support notes then click **Next** to continue.

6. Accept the agreement and click **Next** to continue.
7. Select the typical type of installation and click **Next** to continue. You can choose **Custom** if you need to do something such as changing the installation directory.
8. On this screen you need to register your agent with the console. You will be asked for the following items:
    - **Network Address** (this is the IP address of your EDPM server)
    - **Port** (use the default port 8086)
    - **Username** (by default this username is "user")
    - **Password** (by default this is "password")

    Click **Next** to continue.

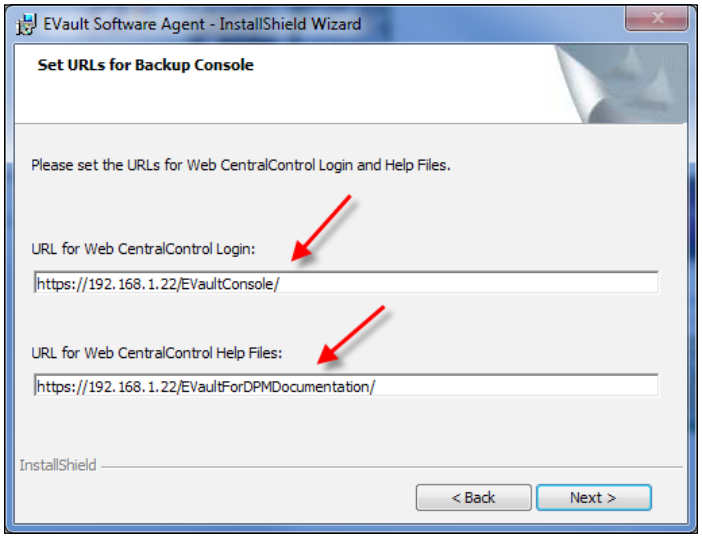
NOTE: If you skip out registering your agent the installation will fail.



NOTE: The **Web CentralControl** is typically for clients that have purchased the standalone backup service from i365. In the case of having a EDPM appliance the **Web CentralControl** is actually your EVault Console.

9. Set the URLs for Web CentralControl Login sites:
    - The URL for Web CentralControl Login is:
      `https://192.168.1.22/EVaultConsole/`
    - The URL for Web CentralControl Help Files is:
      `https://192.168.1.22/EVaultForDPMDocumentation/`

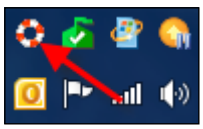
    On your installlation replace "192.168.1.22" with your EDPM servers IP or server name, click **Next** to continue.



10. Click **Install** to begin the installation.
11. The agent will install. The installation will take several minutes to complete. The completed screen will eventually come up. Click **Finish** to complete the installation.

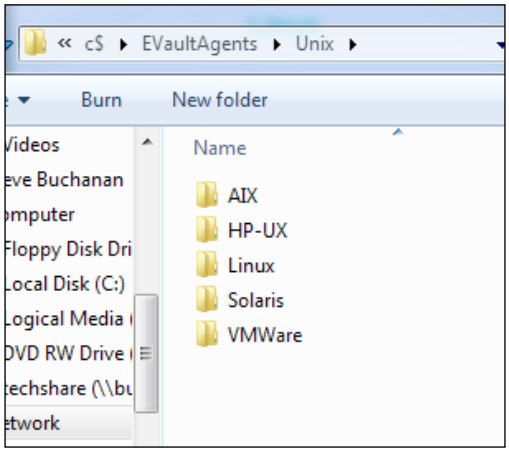
That is it; your EDPM agent will now be installed on your Windows computer.

NOTE: By default the agent is installed here: `C:\ProgramFiles\EVaultSoftware`. You will also have an icon in your system tray labeled **Maestro**. **Maestro** is the EDPM agent and needs to be running for the protection to work. Here is a screenshot of what the Maestro icon looks like:



Linux

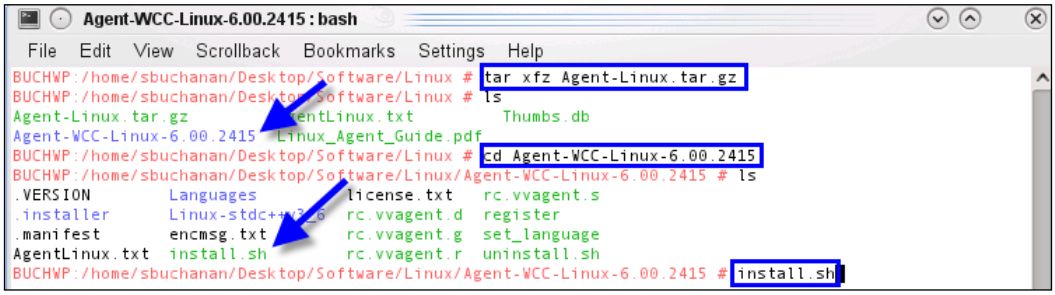
The Linux agent is not located on the root of the `EVaultAgents` folder; it is actually located inside a Unix folder inside of the `EVaultAgents` folder on the EDPM server. Here is the full path for the Linux installer: `%systemdrive%\EVaultAgents\Unix\Linux` on the EDPM server or you can navigate to the agent across the network on this path `\\YOUREDPMSERVERNAME\c$\EVaultAgents\Unix\Linux`. Here is a screenshot of this directory so that you will know what is in this folder:



Be sure to have either **root privileges** on the Linux server or be able to **sudo** for the installation of the agent. The Linux agent is compressed in `.tar` format. Here are the steps to install the EDPM Linux agent:

1. Copy the `Agent-Linux.tar.gz` file from `%systemdrive%\EVaultAgents\Unix\Linux` to the `/tmp` directory on your Linux computer.
2. Now you need to extract the installation files. Do this by running the following commands in a shell:
    - `cd/tmp`
    - `tarxfzAgent-Linux.tar.gz`
    - `cdAgent-Linux`
3. Now you should be able to run the install script. The install script is `install.sh`. You can launch this by typing the following command in a shell: `/tmp/Agent-Linux/install.sh`.

4. This script will prompt you for configuration information about the agent settings. This is similar to the prompts on the Windows agent installation. The Linux agent installation will ask for items such as web registration (address, port number, and authentication), log file name, and language selection for logs and command lines. Here is a screenshot to give you an example of extracting and installing the EDPM Linux agent:



NOTE: In this example we used a directory on the desktop of the Linux computer called `software` to install from.

5. When the installation is finished, a message will appear and the agent daemon will be running on your Linux computer. A Linux daemon is equivalent to a service in Windows. Your EDPM should be live on your Linux computer now.

NOTE: There is an installation log for the EDPM agent installer. The file name is `Install.log` and will be located in: `/usr/local/BUAgent/`. You can use this file for troubleshooting if your EDPM agent fails.

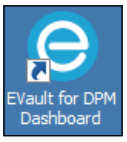
EDPM administration

EVault for DPM has its own dashboard and console. Both the dashboard and console are web-based. With the consoles being web-based they can be accessed from anywhere on your internal network and if you open it up you can access them from outside of the network as well. The dasboard is a central location to monitor the status of your computers and applications that are protected by DPM and EVault. This helps you see what is going on with your entire backup environment. From within the dashboard you can launch either the DPM Administrator Console or the EVault Console.

EDPM Dasboard

The EDPM Dashboard gives you a way to quickly see the status of your DPM and EVault protected computers in one place. You do not use this as an administrative tool it is used as a dashboard and a central place to access DPM and EVault administration consoles.

To launch the EDPM Dasboard click on the EDPM icon on the desktop of the EDPM server. This is what the icon looks like:



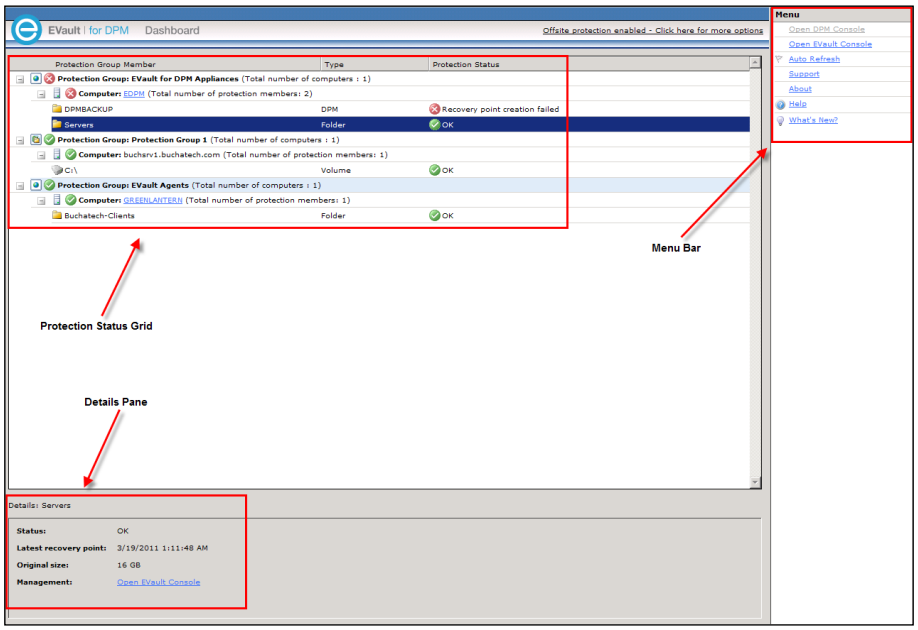
This dashboard is web-based so you could also access this from any web browser on the network by typing this URL into your browser:

```
https://SERVERNAMEORIPADDRESS/EVaultForDPMDashboard
```

An example of the URL would be:

```
https://edpm/EVaultForDPMDashboard
```

The EDPM Dashboard consists of three main parts. The three parts are the **Protection Status Grid**, **Details Pane**, and the **Menu Bar**.



- **Protection Status Grid**: This gives you an overview of the health of your protection groups, status of the agents, computers, and recovery points. It shows you the **Protection Group Member**, the type of data being protected for example, if the data is SQL it will list SQL here or if it is a UNC share it will list UNC files here, and it shows the **Protection Status**. The protection status is much like what you are accustomed to seeing in the DPM Administrator Console under the **Protection** tab. You will see errors, information, and statuses. You can click on any protection members here to see more information in the **Details Pane**.
- **Details Pane**: This is pretty self-explanatory as it shows more information about the selected protection set within the **Protection Status Grid**.
- **Menu Bar**: This is on the right-hand side of the dashboard. This contains links to open the DPM Administrator Console, the EDPM Console, a link to turn **Auto Refresh** on or off so that your dashboard will auto refresh the status of your protection sets, a link to the i365 support portal, the **About** page to see what version of EDPM you are running, and the EVault **Help**.

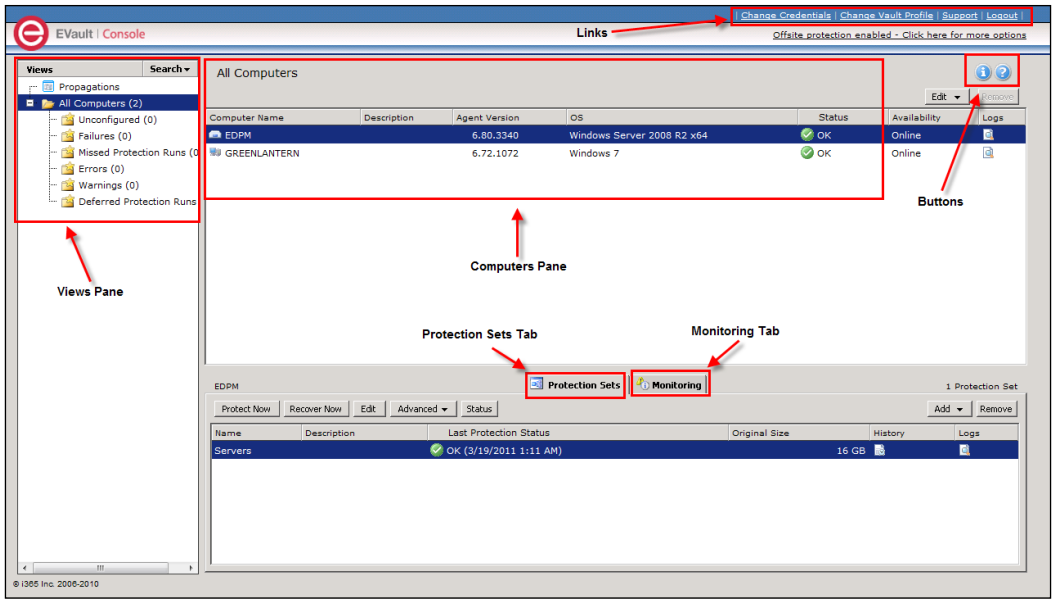
EVault Console

EVault is a separate application from DPM so it has its own console. EVault is the application that protects your non-Windows' workloads. From within the EVault Console you can configure, monitor, and manage all of your protection and recovery tasks. This console gives you management access to the protection of any server that has the EDPM agent installed. This is the console you would typically find your non-Windows' servers in such as Linux, and VMware. This console has a look and feel much like the DPM Administrator Console so it will not take you long to get up to speed and start using it.

The EVault Console is also a web-based interface so you could access this from any web browser on the network by typing this URL into your browser:

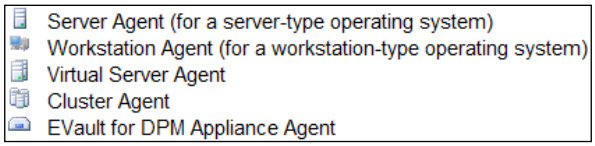
```
https://SERVERNAMEORIP/EVaultConsole
```

Here is a screenshot of the console:



The EVault Console consists of multiple components to help you manage your protection. These components are:

- **Views Pane**: This pane gives you a summary of the protection status of your systems and anything that may require your attention. It lists computers in different categories that you can click on to just see the computers that fit that criterion. The categories are: **Unconfigured Computers**, **Computers with Failures**, **Missed Protection Runs**, **Errors**, **Warnings**, and with **Deferred Protection Runs.**
- **Computers Pane**: This pane is where you see the computers that you are protecting. You can see the **Computer Name**, **Agent Version**, the OS that is running on the computer, the protection status, its online or offline availability, and you can click on the logs icon next to the protected computer to view logs about it. One thing you will notice in the **Computers Pane** is that your computers that are protected have different icons depending on what they are. Here is a list of all the types of icons and what they stand for:



In the **Computers Pane** you also have an **Edit** menu that allows you to access:

- **Agent Settings**: This is where you would change advanced agent settings such as retention and notification settings. More about these settings can be found in the EDPM documentation.
- **Vault Settings**: This is where you can access the Vault Address, Account, User Name, and Password if you need to change them or add/remove additional vaults.

- **Configure Cluster Virtual Servers**
  - **Propagate Agent Settings**: EVault has a feature that lets you copy settings from one EVault agent to another existing agent. This is handy if you need similar agent settings across multiple servers. You could propagate to speed up deployment of the agents. This is where you can adjust these settings. More information about the agent propagation process can be found in the EDPM documentation.
- The **Remove** button will remove a computer from EVault and will no longer be protected.
- **Protection Sets**: This is one of the more important areas in the console because this is where you configure protection sets as well as vault communications. Essentially you set up your backups and perform recoveries here. We will cover setting up protection and performing a recovery in the next section. That will cover the majority of what you will do in this tab. You can learn more about this tab in the EDPM documentation.
- **Monitoring**: This is where you can monitor the progress of protection, set protection and recovery jobs.
- **Links**: You will notice the following links:
  - **Change Credentials**: This is where you can change the username and password that the agents use to register with the console. We covered this in the agent installation.
  - **Change Vault Profile**: This is where you can change your vault information or add more vaults.
  - **Support**: This is a link to i365's support page.
  - **Logout**: Clicking this link will log you out of the console.
- **Buttons**: The following buttons are available:
  - **Information**: This will show you what the version of your console is.
  - **Help**: Clicking the help button will launch online help.

That covers the overview of the EDPM Dashboard and the EVault Console. Both are useful tools for monitoring and managing your protection. You will find more information about the consoles in the EDPM documentation that we were unable to cover in this book.

Vault

The Vault is a storage space/center in i365's data center. When you purchase the EDPM appliance you will be given a group of settings from i365. These settings are:

- Vault Address
- Account
- User
- Password

These are the settings you use to connect from your appliance to the i365 cloud. You should have been asked for these settings during the initial configuration of EDPM. If you need to change these settings you can access them here, at your EVault Console:

```
https://localhost/EVaultConsole
```

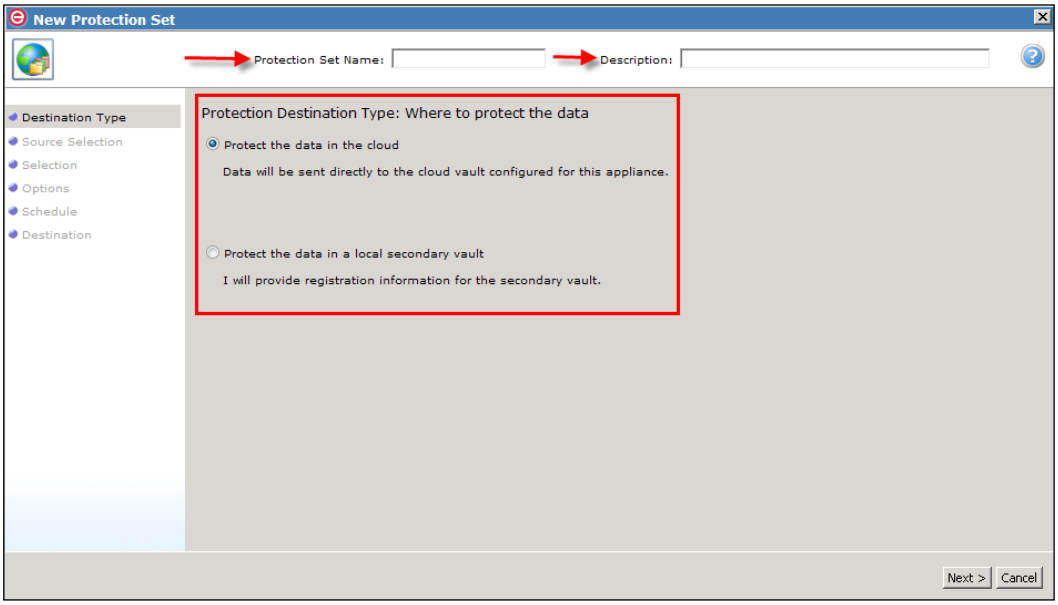
Toward the top of the console, click on **Change Vault Profile**. Here is where you can change existing Vault profiles.

Adding a Protection Set

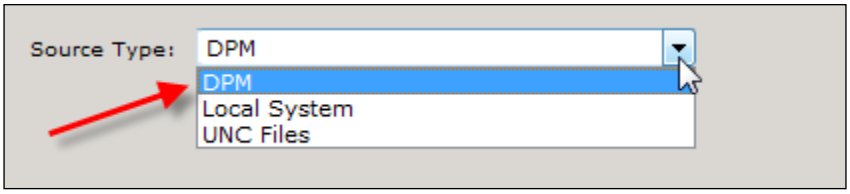
A **Protection Set** in EVault contains the settings of each set of data that you are protecting. This includes items such as what the data is, when does it get backed up and if it is encrypted or not. There are more to **Protection Sets** than that and we will cover them and how to create and configure a protection set below:

1. Go to your EVault Console `https://localhost/EVaultConsole`.
2. In the computer's pane, select the computer that you want to create a protection set for.
3. In the protection set pane, click the **Add** button and choose **Protection Set**. The **New Protection Set** wizard will pop up.

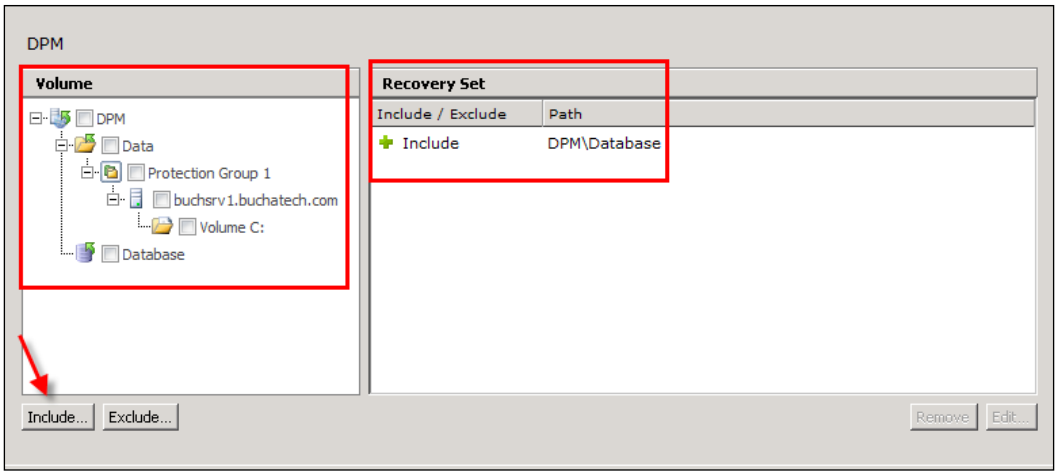
4. Give your protection set a name and add a description if you want one. Select to either protect your data in the cloud or in the local vault. Click **Next** to continue.



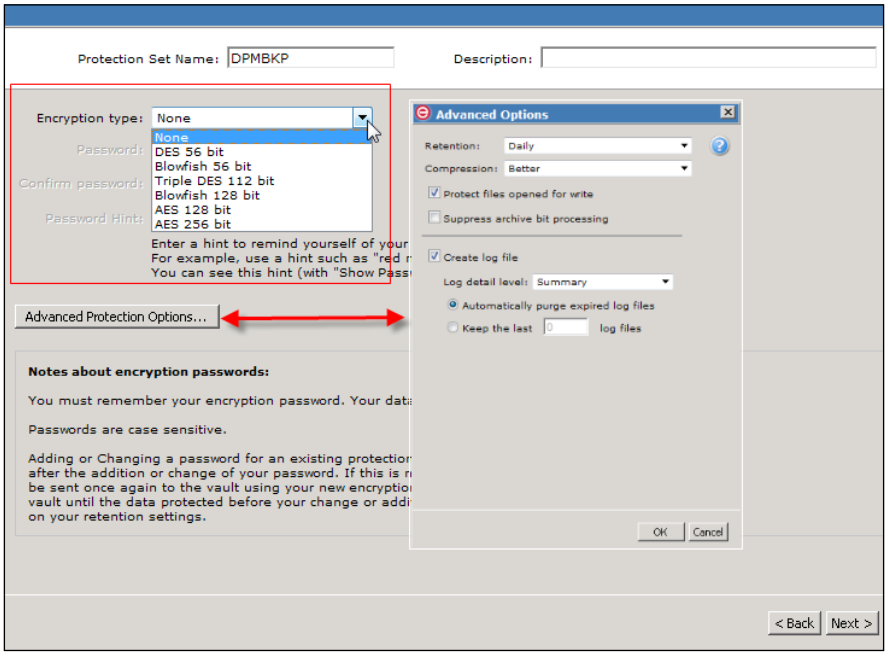
5. Now you need to select the type of data you plan to protect. This will change depending on the computer you are protecting. For example, if the computer you selected was a database server database would be one of the types you could choose. Click **Next** to continue. The following screenshot shows the selection of DPM as the source type:



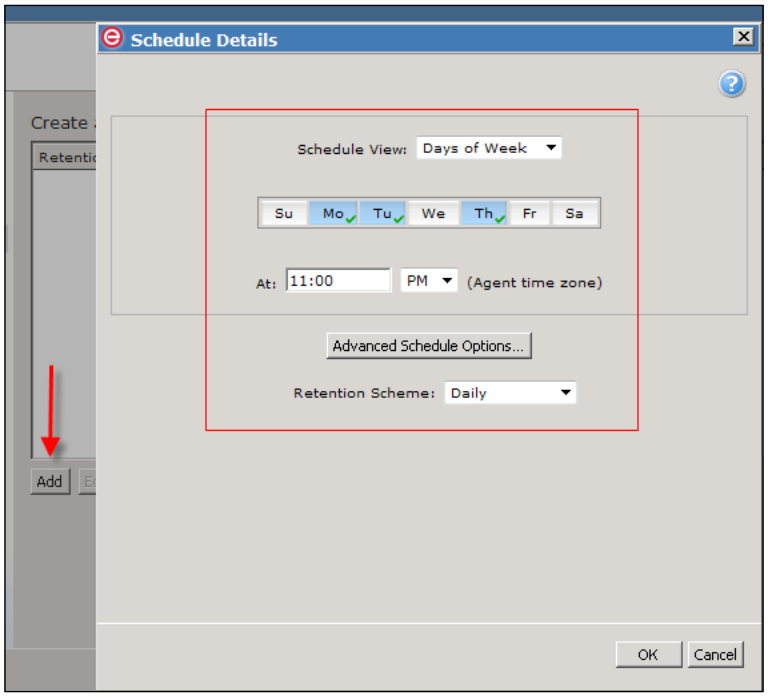
6. The **Selection** screen is where you choose the data that will be protected. In our example we chose to protect the DPM database. Select data that needs to be protected, click the **Include** button and then click **Next** to continue.



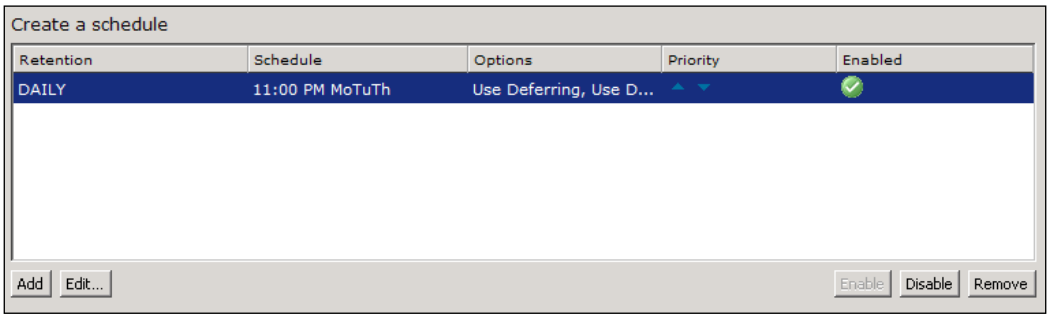
7. The **Options** screen is where you can set encryption for your data. You can choose the **encryption type** and set a password for the encryption. You can also set a number of **Advanced Options**. These include retention, compression, protection of open files for write, suppressing the archive bit, log file levels and how long to store the logs. Once you have set all the options you want click **Next** to continue. The following screenshot shows you the **Options** and **Advanced Options** screen:



8. Click the **Add** button to bring up the **Schedule Details** window. This is where you select the days and time that you want your data to be protected:



9. After you select the date and time click **OK**. This will bring you back to the main **Schedule** screen. You will see the schedule that you just made on the main schedule screen.



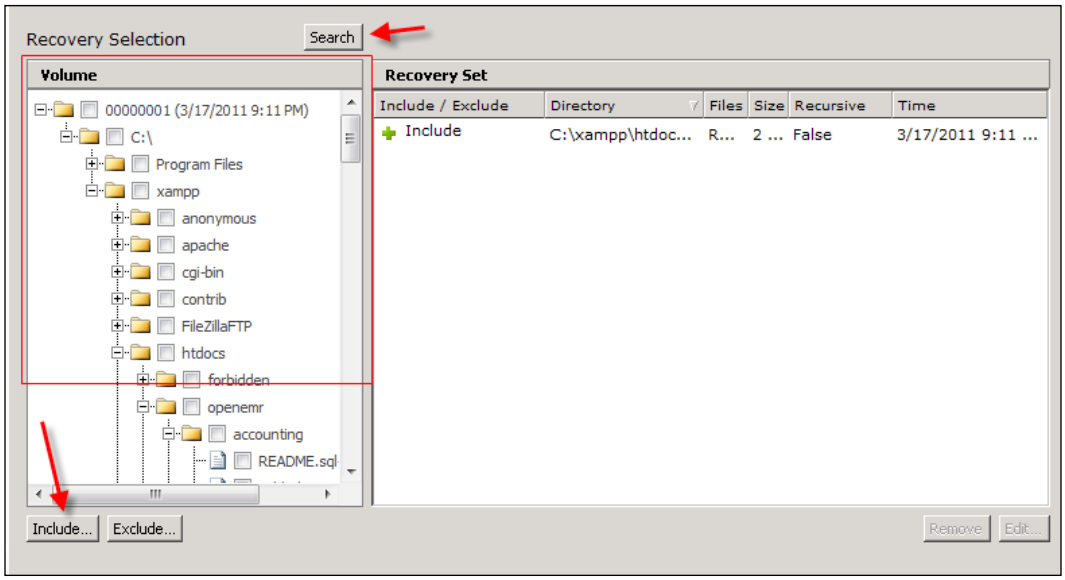
9. Click **Finish** to complete the new Protection Set.

You will now see the protection set you just created listed on the **Protection Sets** tab and it will run the next time that it is scheduled to run.

Recovery

We just learned how to create a protection set, now let's dive into performing a recovery from the EVault Console:

1. Go to your EVault Console: `https://localhost/EVaultConsole`.
2. In the Computers pane select the computer that you want to recover data from.
3. In the **Protection set** tab highlight the date of the recovery point and then click the **Recover Now** button. The **Recovery wizard** will pop up.
4. Select to recover from the **Vault** or a **directory on disk**. The Vault is referring to the cloud. Ensure the right recovery point date and time is showing in the recovery point drop down box. Click **Next** to continue.
5. On the **Recovery Selection** expand the recovery point until you find the data you want to recover. You can also do a search for the data you want to recover by clicking the **Search** button. Once you locate the data you want put a check next to it and click the **Include** button.



6. On the **Options** screen you can choose to recover the data to its **original location** or to an **alternate location**. You can also choose how this recovery will handle an overwrite operation if there are existing files in the location you are recovering to. The **Advanced Recovery Options** button will give you a set of options for handling logging for this recovery, the ability to use all bandwidth or to let EVault throttle bandwidth on this recovery, something called Streams (Streams refers to the properties of the data such as security settings), and the ability to overwrite locked files for example, if there is an existing set of files that you are trying to recover and they are locked by the operating system or services.
7. Once you are done setting the options you need to click **Recover Now** to perform the recovery.

That is an overview of EVault for DPM. It is a really good product and a useful extension onto the DPM platform. The product has a lot of power and an entire book could probably be written about it as we were able to only cover some of the capabilities of the product in this book. EDPM comes with a robust set of documentation to help you get up to speed about the product if you decide to purchase it.

Summary

This chapter covered details on backing up your DPM server. We first covered offsite backup and then cloud backup options. Three of the non-offsite back up solutions included the Disk-to Disk-to-Tape, backing up DPM with secondary DPM server, and backing up DPM with third-party software options. There are currently two vendors that offer cloud backup. By now you should have a better understanding of what cloud and offsite backups you can do as well as how to get this set up.

In the next chapter we are going to dive into DPM PowerShell.

10
DPM PowerShell

In this chapter we are going to dive into PowerShell for DPM. You will learn a brief history of PowerShell and the basics about it. We are not going to cover advanced PowerShell or go too in-depth. We are going to cover how to utilize PowerShell to perform functions and tasks for your DPM server. You will also get an overview on Opalis and DPM. There are lots of resources online if you want to learn more about PowerShell in general. Simply go to a search engine and search with Learn PowerShell.

Here are the topics that will be covered in this chapter:

- PowerShell
    - Background of command-line and scripting in Windows
    - Basics of PowerShell
- DPM Management Shell
    - Overview of DMS
    - DMS cmdlets
    - DPM tasks and functions from the shell
    - DPM scripts
- Overview of Opalis

PowerShell

PowerShell is a command-line shell built on top of Microsoft's .Net framework and C# scripting language. A shell is different from a command-line tool like `cmd.exe` in that a shell is object-orientated. We are going to learn how PowerShell came about, what it is used for and some basics about using it.

Background of command line and scripting in Windows

Microsoft operating systems and applications have historically been managed from a GUI. In recent years this has started to change with the introduction of PowerShell. In the past, PowerShell, Microsoft operating systems, and applications all came with command-line tools. These tools are `command.com` or `cmd.exe`. These tools supported some basic commands and scripts that were made using batch files. Batch files are simply executable text files that contain a series of commands. IT professionals would use batch files to automate routine tasks. These tools are limited and IT professionals have had to resort back to the available GUI tools.

Microsoft has attempted to provide better command-line tools over the years. These attempts have been Windows Script Host and `cscript.exe`. The Windows Script Host tool allowed administrators to use other scripting languages such as JScript and VBScript but those script languages are geared more towards programmers. `cscript.exe` is a command-line version of Windows Script Host that can be used to launch existing scripts. While these tools have been good improvements and are a step forward in regards to command-line tools in Windows environments, they were not the answer. The first PowerShell was released in 2006. PowerShell v2.0 was then released in 2008. Today PowerShell is an integral part of many Microsoft applications and operating systems. Certain tasks that need to be performed in applications can only be done from PowerShell and not the GUI. That is one of the reasons, as an IT Professional, it is extremely important to take the time to learn PowerShell. Not only does it come standard with Microsoft operating systems but it is a part of Microsoft's applications. DPM is one of these many applications that have PowerShell integrated into it. PowerShell is included not only with DPM but with these other Microsoft applications on the following chart:

Application	Version
Exchange Server	2007/2010
Windows Server	2008
Microsoft SQL Server	2008
System Center Operations Manager	2007
System Center Virtual Machine Manager	2007
System Center Data Protection Manager	2007/2010
System Center Essentials	2010
Windows Compute Cluster Server	2007
Internet Information Services	7.0
Windows 7 Troubleshooting Center	6.1
Microsoft Deployment Toolkit	2010

As you can see Microsoft is serious about making PowerShell a part of all of their products. It makes sense to invest time into learning PowerShell.

Basics of PowerShell

We are going to look at the basics of PowerShell before we get into using PowerShell with DPM.

Cmdlets

In PowerShell commands are no longer called commands. They are referred to as **cmdlets** (pronounced command-lets). Cmdlets consist of two parts connected by a hyphen. These two parts are a verb and a noun like this "verb-noun". An example of this would be `Get-Command`. The verb is an action that will be performed and the noun is an object on which the verb will be performed. So let's break down `Get-Command` for a better understanding. `Get` is going to retrieve something; but what is it going to retrieve? `Command` is what `Get` is going to retrieve. `Get` gathers a list of commands that are in the shell and outputs this information to the screen. To sum this up PowerShell has a lot of verbs and those verbs can be combined with any object in that shell to perform tasks at the command-line. You have the standard PowerShell that comes with Windows and then you have shells that come with other Microsoft products such as Exchange. The shell with Exchange will contain more Exchange-specific objects that the standard Windows PowerShell will not contain. Even though each product has its own set of objects, the verbs have the same concept behind them making it easy to start using them if you are already familiar with PowerShell. Once you grasp the basic concept of cmdlets it will help you better understand the power they hold.

NOTE: In addition to cmdlets PowerShell can run all the commands you can run in Windows using `command.com` and `cmd.exe`.

Help

There are several ways to get help with PowerShell, one is online at `http://technet.microsoft.com/en-us/library/bb978526.aspx`. Another source of help with PowerShell is the **PowerShell Getting Started** documentation that is installed along with PowerShell, and the **Help cmdlet**. All of this information is essentially the same. It is just displayed differently in each location for preference of the user. For online help visit the previously mentioned URL. To access the **Getting Started** documentation on the system go to **Start | All Programs | Windows PowerShell**, and then click **Getting Started**. To use the Help cmdlet type `Get-Help` into a PowerShell window. As a new PowerShell user you should become familiar with how to use the Help cmdlet.

Variables

A variable is used to hold data. Variables store information that will be used later within a script. An example would be storing the path to a file that needs to be referenced later in a script. Variables contain objects, text strings, and integers.

Pipeline

Pipeline also known as Piping is not new. Piping has been in the Unix shell for a long time. The part that is new to Windows is the ability to pipe objects together and this is arguably one of the best features of Windows PowerShell. Piping is taking the output of one cmdlet and passing it into the next cmdlet as input. The Piping character is "|".

An example of piping cmdlets together is running the `Get-Command` cmdlet and piping it to the `Sort-Object` cmdlet. This allows you to get a list of PowerShell commands and then sort them for easy reading. The syntax would be `Get-Command | Sort-Object`.

Tab

Another nice feature of PowerShell is Tab Completion of cmdlets. The way it works is when you type a part of a common cmdlet you can hit the *Tab* key on your keyboard and PowerShell will complete the rest of the cmdlet for you. An example would be if you typed `Get-C` and hit *Tab*, PowerShell will scroll through a list of all commands that begin with `Get-C` such as `Get-Command`. For this example, let's say you were looking for the `Get-Command` cmdlet, you would type `Get-C` and then keep pressing the *Tab* key until "Command" is appended to `Get-C` on the screen. It helps you put cmdlets into the shell faster.

NOTE: This is a basic overview of PowerShell. A complete guide to PowerShell is beyond the scope of this book. You can find more information about PowerShell on these sites:

`http://technet.microsoft.com/en-us/library/ee221100.aspx` (Microsoft tutorial on PowerShell)

`http://en.wikipedia.org/wiki/Windows_PowerShell` (Detailed overview of PowerShell)

`http://ss64.com/ps/` (A list of PowerShell commands)

DPM Management Shell

When you install DPM 2010 it includes a scripting shell called **DPM Management Shell** also known as **DMS**. DMS is built on Windows PowerShell. IT professionals familiar with PowerShell will be able to easily learn DMS. DMS is an administrative-focused tool for DPM administrators. DPM administrators can use DMS to perform many of the same functions that can be performed from the DPM Administrator Console as well as some tasks that can only be performed from the shell.

A DPM administrator can use DMS to perform the same tasks in the areas of protection, recovery, library and disk management. In fact when you perform the tasks in the same areas in the DPM Administrator Console it is executing DMS cmdlets. This means an administrator will get the same experience regardless of using the UI or the shell. The other benefit of having DPM built this way is that third-party vendors can easily develop tools to extend DPM's functionality through PowerShell. A DPM administrator can even install DMS on other machines and control DPM servers remotely through DMS. DMS can be installed on other servers or client machines.

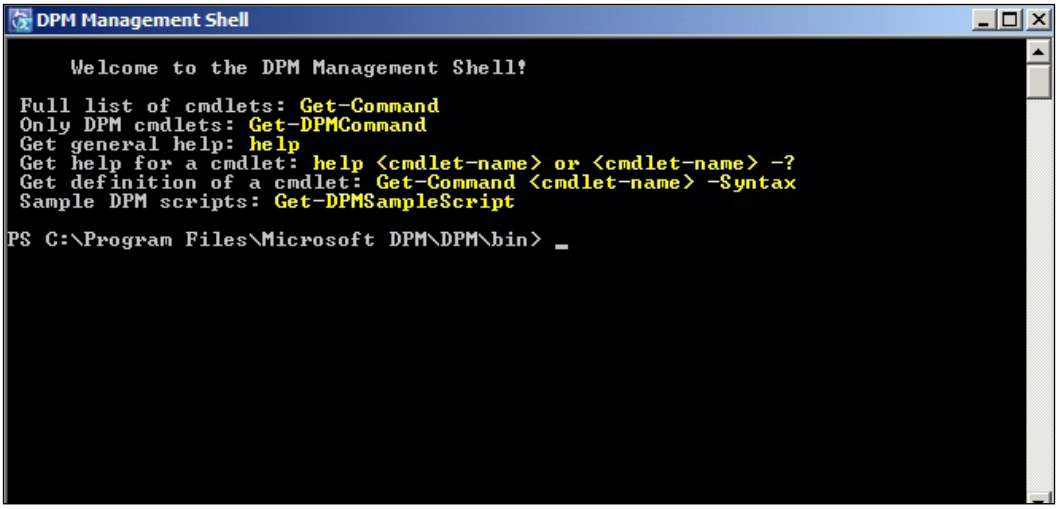
In this section you are going to learn about the DPM Management Shell and learn some DPM cmdlets that can run from the shell as well as DPM scripts that are available.

NOTE: The Data Protection Management shell for DPM 2010 is not supported on 32 bit computers.

Overview of DMS

Let's start by opening DMS. If you have the DMS icon on your desktop, double-click on it to open it. The other way to open DMS is to click on the **Start** | **All Programs** | **Microsoft Data Protection Manager 2010** | **DPM Management Shell**.

DMS will look and operate a little different than the standard PowerShell window that comes with Windows. This is what the console looks like:



The DMS is different because it contains DPM-specific cmdlets that you could not run from a standard PowerShell console. When you open the DMS console it defaults to the DPM `bin` directory. The shell defaults to this directory because this is where the cmdlets and scripts reside. This is the directory you will work out of. Under the **Welcome to the DPM Management Shell!** you will see a list of cmdlets that you can run and that will help you get started with the DMS console. Most of these are self-explanatory but here is more information about each of them:

- `Get-Command`: This will give you a full list of cmdlets available. It prints the list on the screen.

- `Get-DPMCommand`: This does the same as `Get-Command`, printing a list of cmdlets on the screen, but this cmdlet will list DPM cmdlets only. `Get-Command` includes standard PowerShell cmdlets as well.
- `Help`: This command will will provide you with general help about PowerShell. You can run `help<cmdlet-name>` or `<cmdlet-name> -?` to get help about specific cmdlets.
- `Get-DPMSampleScript`: This cmdlet will give you a list of available DPM scripts. These scripts are in the DPM `bin` directory.

DMS cmdlets

Here is a condensed list of useful DMS cmdlets that can be used as an easy reference when administering DPM from the shell. You can also generate this list with the full amount of information such as longer descriptions and parameters for each cmdlet. To do this, simply go to the DMS shell and run the following syntax:

```
Get-Command -PSSnapinMicrosoft.DataProtectionManager.PowerShell | Get-Help -detailed > DPMHelpTopicsSortedNounVerb.txt
```

This will pipe the command and help cmdlets together and output the data to a text file that can then be printed out. You can also find a list of these commands here:

`http://technet.microsoft.com/en-us/library/ff631926.aspx`

Cmdlet	Description	Syntax
`Add-BackupNetworkAddress`	Specifies a backup network for the server to use.	`Add-BackupNetworkAddress [-DPMServerName] [-Address] [-SequenceNumber]`
`Get-BackupNetworkAddress`	Returns a backup network specified for the server.	`Get-BackupNetworkAddress [-DPMServerName]`
`Remove-BackupNetworkAddress`	Stops the DPM server from trying to use the specified network.	`Remove-BackupNetworkAddress [-DPMServerName] [-Address]`
`Connect-DPMServer`	Opens a connection to a DPM server.	`Connect-DPMServer [-DPMServerName] <String> [-Async Operation<AsyncOperation>]`
`Disconnect-DPMServer`	Closes and releases all objects for a DPM connection session.	`Disconnect-DPMServer [[-DPMServerName]]`
`Get-ProductionCluster`	Returns a list of all clusters on which the DPM agent is installed.	`Get-ProductionCluster [-DPMServerName]`

Cmdlet	Description	Syntax
Get-ProductionServer	Returns the list of servers that have the DPM Protection Agent installed on them.	`Get-ProductionServer [-DPMServerName]`
Get-ProductionVirtualName	Returns the virtual names for a cluster.	`Get-ProductionVirtualName [-ProductionCluster] [-Async] [-Handler] [-Tag]`
Start-SwitchProtection	Switches protection of a data source between the primary DPM server and the disaster recovery server.	`Start-SwitchProtection [-ProtectionGroup] -Datasource [-Async]`
Add-DPMDisk	Adds a new disk to the storage pool	`Add-DPMDisk [-DPMDisk]`
Get-DPMDisk	Returns a list of disks found in the last rescan on a DPM server.	`Get-DPMDisk [-DPMServerName]`
Get-DPMVolume	Returns a list of volumes on the DPM server.	`Get-DPMVolume [-DPMServerName]`
Remove-DPMDisk	Removes a disk from the storage pool.	`Remove-DPMDisk [-DPMDisk]`
Start-DPMDiskRescan	Scans for new disks or disks where configuration has changed.	`Start-DPMDiskRescan [-DPMServerName]`
Add-Tape	Adds a tape to a DPM library.	`Add-Tape [-DPMLibrary] [-Async] [-JobStateChangedEventHandler]`
Disable-DPMLibrary	Disables the specified library.	`Disable-DPMLibrary [-DPMLibrary] [-Confirm] [-PassThru]`
Disable-TapeDrive	Disables the specified tape drives in the library.	`Disable-TapeDrive [-TapeDrive] [-Confirm] [-PassThru]`
Enable-DPMLibrary	Enables the specified library.	`Enable-DPMLibrary [-DPMLibrary] [-PassThru]`
Enable-TapeDrive	Enables the specified tape drives in the library.	`Enable-TapeDrive [-TapeDrive] [-PassThru]`
Get-DatasetStatus	Returns the dataset state of the archive tape.	`Get-DatasetStatus [-Tape]`
Get-DPMLibrary	Returns the list of libraries attached to the DPM server and their status.	`Get-DPMLibrary [-DPMServerName]`

Cmdlet	Description	Syntax
Get-HeadlessDataset	Returns any incomplete dataset on the archive tape.	`Get-HeadlessDataset [-Tape]`
Get-MaintenanceJobStartTime	Returns the start time of the maintenance job.	`Get-MaintenanceJobStartTime [-MaintenanceJob] [-DPMServerName]`
Get-Tape	Returns a list of tapes in the library across drives and slots.	`Get-Tape [-DPMLibrary]`
Get-TapeDrive	Returns a list of drives in a library on a DPM server.	`Get-TapeDrive [-DPMLibrary]`
Get-TapeSlot	Returns the list of slots in the library.	`Get-TapeSlot [-DPMLibrary]`
Lock-DPMLibraryDoor	Locks the door of the specified library.	`Lock-DPMLibraryDoor [-DPMLibrary] [-Async] [-DoorAccessJobStateChangeEventHandler]`
Lock-DPMLibraryIEPort	Locks and loads the media present in the IE port.	`Lock-DPMLibraryIEPort [-DPMLibrary] [-Async] [-JobStateChangedEventHandler]`
Remove-Tape	Removes a tape from a DPM library.	`Remove-Tape [-Tape] [-DPMLibrary] [-Async] [-Confirm] [-JobStateChangedEventHandler]`
Rename-DPMLibrary	Renames the specified library.	`Rename-DPMLibrary [-DPMLibrary] [-NewName] [-PassThru]`
Set-MaintenanceJobStartTime	Sets or removes the start time of a maintenance job.	`Set-MaintenanceJobStartTime [[-StartTime]] [-MaintenanceJob] [-DPMServerName]`
Set-Tape	Marks the specified tape as Archive, Cleaner, Free, or Not Free.	`Set-Tape [-Tape] -NotFree [-PassThru]`
Start-DPMLibraryInventory	Starts an inventory of the tape in the specified library.	`Start-DPMLibraryInventory [-DPMLibrary] -DetailedInventory [-JobStateChangedEventHandler] [-Tape]`
Start-DPMLibraryRescan	Starts a rescan job in the background to identify new libraries or ones that have changed.	`Start-DPMLibraryRescan [-DPMServerName] -RefreshOnly [-JobStateChangedEvent Handler]`
Start-OnlineRecatalog	Returns a detailed list of data on a tape.	`Start-OnlineRecatalog [-RecoveryPoint] [-JobStateChangedEventHandler] [-RecoveryPointLocation]`

Cmdlet	Description	Syntax
Start-TapeDriveCleaning	Starts a clean tape drive job.	`Start-TapeDriveCleaning [-TapeDrive] [-JobStateChangedEventHandler]`
Start-TapeErase	Starts a tape erase job.	`Start-TapeErase [-Tape] [-JobStateChangedEventHandler]`
Start-TapeRecatalog	Returns information about the data on a tape.	`Start-TapeRecatalog [-Tape] [-JobStateChangedEventHandler]`
Test-DPMTapeData	Verifies the data set for a recovery point.	`Test-DPMTapeData [-RecoveryPoint] [-JobStateChangedEventHandler]`
Unlock-DPMLibraryDoor	Unlocks the door of the specified library.	`Unlock-DPMLibraryDoor [[-Timeout]] [-DPMLibrary] [-Async] [-Confirm] [-DoorAccessJobState ChangeEventHandler]`
Unlock-DPMLibraryIEPort	Unlocks the IE port for the specified library.	`Unlock-DPMLibraryIEPort [-DPMLibrary] [-Async] [-JobStateChangedEventHandler]`
New-RecoveryNotification	Builds the notification object used for recovery.	`New-RecoveryNotification [-NotificationIdList] [-NotificationType]`
Set-PerformanceOptimization	Enables setting or removing of on-wire compression of data.	`Set-PerformanceOptimization [-ProtectionGroup] -EnableCompression [-PassThru]`
Add-ChildDatasource	Adds data source or child data source to a protection group.	`Add-ChildDatasource [-ProtectionGroup] [-ChildDatasource] [[-Online]] [-PassThru]`
Get-ChildDatasource	Returns a backup network specified for the server.	`Get-ChildDatasource [-ChildDatasource] [[-ProtectionGroup]] [-Async] [-Inquire] [-Tag]`
Get-Datasource	Retrieves the list of protected and unprotected data in a computer or protection group	`Get-Datasource [-ProtectionGroup]`
Get-DatasourceProtectionOption	Returns the protection options for all data sources of the specified data source type in a protection group.	`Get-DatasourceProtectionOption [-ProtectionGroup]`
Get-ModifiableProtectionGroup	Retrieves a protection group in an editable mode.	`Get-ModifiableProtectionGroup [-ProtectionGroup]`

Cmdlet	Description	Syntax
Get-PolicyObjective	Returns the protection policy for a protection group.	`Get-PolicyObjective [-ProtectionGroup] -LongTerm`
Get-PolicySchedule	Returns the schedule for various protection jobs like synchronization, recovery point creation (shadow copy), and tape backups.	`Get-PolicySchedule [-ProtectionGroup]`
Get-ProtectionGroup	Retrieves the list of protection groups on the DPM server.	`Get-ProtectionGroup [-DPMServerName] [-Async]`
Get-ProtectionJobStartTime	Returns the start time of a protection job.	`Get-ProtectionJobStartTime [-JobType] [-ProtectionGroup]`
Get-ReplicaCreationMethod	Retrieves the replica creation method that is specified for a protection group.	`Get-ReplicaCreationMethod [-ProtectionGroup] [-OnlineReplica]`
New-ProtectionGroup	Creates a new protection group on the DPM server.	`New-ProtectionGroup [-DPMServerName]`
Remove-ChildDatasource	Removes a data source or child data source from a protection group.	`Remove-ChildDatasource [-ProtectionGroup] [-ChildDatasource] [-KeepDiskData] [-KeepOnlineData] [-KeepTapeData] [-PassThru]`
Rename-ProtectionGroup	Renames an existing protection group on the DPM server.	`Rename-ProtectionGroup [-ProtectionGroup] [-NewName] [-PassThru]`
Set-DatasourceProtectionOption	Sets the protection options for the specified data source.	`Set-DatasourceProtectionOption`
Set-PolicyObjective	Sets the policy objective for a protection group.	`Set-PolicyObjective`
Set-PolicySchedule	Sets the schedule for various protection jobs like synchronization, recovery point creation (shadow copy), and tape backups.	`Set-PolicySchedule`
Set-ProtectionGroup	Saves all the actions performed on the protection group on the DPM server.	`Set-ProtectionGroup [-ProtectionGroup] [-Async] [-TranslateDSList]`

Cmdlet	Description	Syntax
Set-ProtectionJobStartTime	Sets or changes the start time of a protection job.	`Set-ProtectionJobStartTime [-JobType] [-ProtectionGroup]`
Set-ProtectionType	Allows you to specify the protection type to be used with the protection group.	`Set-ProtectionType [-ProtectionGroup] [-LongTerm [<Enum>]] [-PassThru] [-ShortTerm]`
Get-DatasourceDiskAllocation	Retrieves the amount of disk space that is allocated to the protected data.	`Get-DatasourceDiskAllocation [-Datasource] [-Async] [-CalculateShrinkThresholds] [-CalculateSize] [-PrimaryDpmServer] [-Tag]`
Set-DatasourceDiskAllocation	Modifies disk allocation for the protected data.	`Get-DatasourceDiskAllocation [-Datasource] [-Async] [-CalculateShrinkThresholds] [-CalculateSize] [-PrimaryDpmServer] [-Tag]`
Set-ReplicaCreationMethod	Sets the replica creation method for disk-based protection.	`Set-ReplicaCreationMethod [-ProtectionGroup] "when" [-OnlineReplica] [-PassThru]`
Start-DatasourceConsistencyCheck	Performs a consistency check on a data source.	`Start-DatasourceConsistencyCheck [-ProtectionGroup]`
Get-TapeBackupOption	Returns the library, drive and other backup or archive options for a protection group.	`Get-TapeBackupOption [-ProtectionGroup]`
Set-TapeBackupOption	Sets the tape backup and library options for a protection group.	`Set-TapeBackupOption [-ProtectionGroup]`
Get-RecoverableItem	Returns a list of recoverable items in a recovery point.	`Get-RecoverableItem`
Get-RecoveryPoint	Returns all available recovery points for a data source.	`Get-RecoveryPoint [-Datasource] or [-Tape] [-Async]`
Get-RecoveryPointLocation	Returns the location of a recovery point.	`Get-RecoveryPointLocation [-RecoveryPoint]`
New-RecoveryOption	Allows setting of recovery options for various servers.	`New-RecoveryOption`
New-RecoveryPoint	Creates a new recovery point for the data source.	`New-RecoveryPoint [-Datasource]`

Cmdlet	Description	Syntax
New-SearchOption	Builds an object with the search options to search for a particular string within the set of specified recovery points.	New-SearchOption [-ToRecoveryPoint] [-SearchString] [-SearchType] [-SearchDetail] [-FromRecoveryPoint] [-Location] [-Recursive]
Recover-RecoverableItem	Recovers a version of the data source to a target location.	Recover-RecoverableItem [-RecoveryOption] [[-RecoverableItem]] [-JobStateChangedEventHandler] [-RecoveryNotification] [-RecoveryPointLocation]
Copy-DPMTapeData	Copies the data from a tape for a given recovery point.	Copy-DPMTapeData [-RecoveryPoint]
Remove-DatasourceReplica	Removes an inactive replica	Remove-DatasourceReplica [-Datasource]
Remove-RecoveryPoint	Removes a recovery point from tape or disk.	Remove-RecoveryPoint [-RecoveryPoint] [-Confirm] [-ForceDeletion]

DPM tasks and functions from the shell

DPM tasks can be performed in the shell using cmdlets. The syntax for some of these cmdlets can be somewhat complex when you start adding parameters and other switches. In this section we are going to cover common tasks that can be performed from DMS and dive deeper into how to use them.

Library

DPM is geared more towards disk protection but it still offers tape protection and you can complete certain tape and library tasks from DMS. These include:

- `Enable-TapeDrive` enables a specified tape drive in the library. Parameters for this cmdlet are:
    - `-TapeDrive`: This specifies the tape drive to use.
    - `-PassThru`: The `-PassThru` parameter can be used with many commands in DPM to return a related object in cases where there is no default output. Using the `-PassThru` parameter allows such cmdlets to be part of a pipeline.

Example of syntax:

```
Enable-TapeDrive -TapeDrive $TapeDrive
```

- `Add-Tape` will add a tape to a DPM library. Parameters for this cmdlet are:
  - `-DPMLibrary`: A DPM library object.
  - `-Async`: This allows the user to indicate that the cmdlet should run asynchronously. This is useful with cmdlets that take a long time to complete. The control returns to the user immediately after the operation starts. The progress of the operation is communicated to the user periodically. This is useful when building a GUI using cmdlets. It is not used when working with the DPM Management Shell.
  - `-JobStateChangedEventHandler`: This is used along with the `-Async` parameter so that the user can be informed of the status of the operation. This is useful when building a GUI using cmdlets. It is not used when working with the DPM Management Shell.

  Example of syntax:

  ```
  Add-Tape -DPMLibrary $DPMLib
  ```

- `Enable-DPMLibrary` enables a specified library. Parameters for this cmdlet are:
  - `-DPMLibrary`: A DPM library object.
  - `-PassThru`: Using the `-PassThru` parameter allows such cmdlets to be part of a pipeline.

  Example of syntax:

  ```
  Enable-DPMLibrary -DPMlibrary "LIBRARYNAME"
  ```

- `Add-DPMDisk` can be used to add a new drive to the DPM storage pool. Parameters for this cmdlet are:
  - `-DPMLibrary`: A DPM library object.
  - `-PassThru`: Using the `-PassThru` parameter allows such cmdlets to be part of a pipeline.

  Example of syntax:

  ```
  Add-DPMDisk -DPMDisk $DPMDisk
  ```

- `Disable-DPMLibrary` disables a specified library. Parameters for this cmdlet are:
  - `-DPMLibrary`: A DPM library object.

- `-Confirm`: Asks the user to confirm the action.
- `-PassThru`: Using the `-PassThru` parameter allows such cmdlets to be part of a pipeline.

Example of syntax:

```
Disable-DPMLibrary -DPMLibrary $DPMLib
```

Disk management

Disk management functions can be done easily enough through the DPM Administrator Console. You also have the option to perform disk management tasks through DMS as well:

- `Add-DPMDisk` can be used to add a new drive to the DPM storage pool. Parameters for this cmdlet are:
  - `-DPMDisk`: A disk that is part of a storage pool.

  Example of syntax:

  ```
  Add-DPMDisk -DPMDisk $DPMDisk
  ```

- `Remove-DPMDisk` can be used to remove a drive from the DPM storage pool. Parameters for this cmdlet are:
  - `-DPMDisk`: A disk that is part of a storage pool.

  Example of syntax:

  ```
  Remove-DPMDisk -DPMDisk $DPMDisk
  ```

Protection

The cmdlets in this section relate to the **Protection** area in the DPM Console:

- `Get-ProtectionGroup` retrieves a full list of the protection groups on your DPM server. This cmdlet does not make the protection group modifiable; you must use the `Get-ProtectionGroup` with the `Get-ModifiableProtectionGroup` cmdlet to modify protection groups.

  Parameters for this cmdlet are:
  - `-DPMServerName`: The name of a DPM server.
  - `-Async`: This allows the user to indicate that the cmdlet should run asynchronously. This is useful with cmdlets that take a long time to complete. The control returns to the user immediately after the operation starts. The progress of the operation is communicated to the user periodically. This is useful when building a GUI using cmdlets. It is not used when working with the DPM Management Shell.

Example of syntax:

```
Get-ProtectionGroup -DPMServerName "DPMSERVERNAME"
```

- `New-ProtectionGroup` creates a new protection group on the specified DPM server. Parameters for this cmdlet are:
    - `-DPMServerName`: The name of a DPM server.
    - `-Name:` The name of a protection group.

  Example of syntax:

```
New-ProtectionGroup -DPMServerName "buchdpm" -Name "New Protection Group"
```

- `Rename-ProtectionGroup` renames an existing protection group with a new name. Parameters for this cmdlet are:
    - `-ProtectionGroup`: The name of a protection group.
    - `-NewName`: The new name for an object.
    - `-PassThru`: Using the `-PassThru` parameter allows such cmdlets to be part of a pipeline.

  Example of syntax:

```
Rename-ProtectionGroup -ProtectionGroup $mpg -NewName'NEWPGNAME'
```

- `Set-ProtectionGroup` commits actions that have been performed on a protection group on the DPM server. Actions performed on a protection group through the DPM Management Shell on a DPM server exist only in memory until this command is run. Parameters for this cmdlet are:
    - `-ProtectionGroup`: The name of a protection group.
    - `-Async`: Allows the user to indicate that the cmdlet should run asynchronously.
    - `-TranslateDSList`: A list of data sources that need to be force translated. This helps to regenerate jobs.

  Example of syntax:

```
Set-ProtectionGroup-ProtectionGroup "NAMEOFAPROTECTIONGROUP"
```

Recovery

There are many cmdlets and ways you can work with recoveries in DPM through the shell. The following are some of them:

- `Get-RecoveryPoint` returns a list of all available recovery points for a specified data source. They are use to see what data on certain dates and times can be recovered. Parameters for this cmdlet are:
    - `-Datasource`: A Windows file system share or volume, Microsoft SQL Server database, Microsoft Exchange storage group, Microsoft SharePoint farm, Microsoft Virtual Machine, DPM database, or system state that is a member of a protection group.
    - `-Tape`: Indicates a tape object.
    - `-Async`: This allows the user to indicate that the cmdlet should run asynchronously.

  Example of syntax:

  ```
  Get-RecoveryPoint -Datasource $ds
  ```

- `Get-RecoverableItem` will output a list of recoverable items in a recovery point. Parameters for this cmdlet are:
    - `-BrowseType`: Indicates whether to browse only the parent nodes or to browse the child nodes as well. The valid values are `Parent` and `Child`.
    - `-SearchOption`: Sets the search options as defined in `New-SearchOption`.
    - `-Datasource`: A Windows file system share or volume, Microsoft SQL Server database, Microsoft Exchange storage group, Microsoft SharePoint farm, Microsoft Virtual Machine, DPM database, or system state that is a member of a protection group.
    - `-RecoverableItem`: A child item within a recovery point that can be recovered. For example: a Windows file system share or volume, Microsoft SQL database, Microsoft Exchange storage group, Microsoft SharePoint, Microsoft Virtual Machine, Microsoft DPM database, system state, or a recovery point.
    - `-RecoveryPointForShares`: The recovery point to use.
    - `-Async`: This allows the user to indicate that the cmdlet should run asynchronously.

- `-Tag`: Helps distinguish the replies to each asynchronous call made by a cmdlet. This is useful when building a GUI using cmdlets. It is not used when working with the DPM Management Shell.

Example of syntax:

```
Get-RecoverableItem -RecoverableItem $rp -BrowseType child
```

- `Remove-RecoveryPoint` can remove recovery points from tape or disk. Parameters for this cmdlet are:
  - `-RecoveryPoint`: The recovery point to use.
  - `-Confirm`: Asks the user to confirm the action.
  - `-ForceDeletion`: Indicates that the data source will be pruned even if a backup job is currently running.

Example of syntax:

```
Remove-RecoveryPoint -RecoveryPoint $rp
```

Backup network

DPM has the ability to choose a network card that all backup traffic travels across. This is helpful if you have a separate network that is dedicated to backup only. If you need to keep backup traffic off your main production network this is a cmdlet you should be familiar with. Selecting the network to back up to is a task that cannot be performed by using DPM Administrator Console. The following cmdlets are available:

- `Add-BackupNetworkAddress` specifies a backup network for the server to use. Parameters for this cmdlet are:
  - `-DPMServerName`: The name of a DPM server.
  - `-Address`: The IP address or subnet mask of the network.
  - `-SequenceNumber`: Specifies the priority of the address for use as backup.

Example of syntax:

```
Add-BackupNetworkAddress -DpmServername Buchdpm -Address
192.168.2.10/24 6 -SequenceNumber 1
```

- `Remove-BackupNetworkAddress` stops a DPM server from trying to use a specified network for backup. Parameters for this cmdlet are:
  - `-DPMServerName`: The name of a DPM server.
  - `-Address`: The IP address or subnet mask of the network.

Example of syntax:

```
Remove- BackupNetworkAddress -DpmServername Buchdpm -Address
192.168.2.10/24
```

- `Get-BackupNetworkAddress` will list the backup network that is specified for the current DPM server. Parameters for this cmdlet are:
    - `-DPMServerName`: The name of a DPM server.

  Example of syntax:

  ```
  Get-BackupNetworkAddress -DpmServername buchdpm
  ```

Other

There are other DMS cmdlets that don't fall under the traditional management areas of DPM. These are typically tasks that cannot be performed from the DPM Administrator Console:

- `Connect-DPMServer` connects you to a DPM server in the same domain or a different domain. Parameters for this cmdlet are:
    - `-DPMServerName`: The name of a DPM server.
    - `-AsyncOperation`: Used for synchronization purposes.

  Example of syntax:

  ```
  Connect-DPMServer buchdpm.buchatech.com
  ```

- `Disconnect-DPMServer` closes and releases all objects for a DPM connection session. Parameters for this cmdlet are:
    - `-DPMServerName`: The name of a DPM server

  Example of syntax:

  ```
  Disconnect-DPMServer -DPMServerName "buchdpm"
  ```

- `Start-ProductionServerSwitchProtection` is used to switch protection on a data source between a primary DPM server and a secondary DPM server. This cmdlet is important because if your primary DPM server were to fail running this would change the protection of that data to the secondary DPM server. Now let's say you had the protection switched to the secondary DPM server and you just got the primary DPM back online now the protection needs to be moved back. Use this cmdlet to move that protection back to the primary DPM server. This is another task that cannot be performed from the DPM Administrator Console. Parameters for this cmdlet are:
    - `-ProtectionType`: Indicates the type of protection.

- `-UserName`: The user account to use.
- `-Password`: Password for the user account. Do not pass this value through the command-line. Run the command and wait to be prompted for the password.
- `-DomainName`: The domain to which the user account belongs.
- `-ProductionServer`: A server that has a DPM agent installed on it.

Example of syntax:

```
Start-ProductionServerSwitchProtection -ProtectionTypeprimary -
UserName administrator -Password12345 -DomainName buchatech.com -
ProductionServerbuchdpm
```

- `Set-PerformanceOptimization` cmdlet can enable and disable on-wire compression of data when it goes across the network from your DPM server. This can be useful when you are running into network performance issues. Parameters for this cmdlet are:
  - `-ProtectionGroup`: The name of a protection group.
  - `-DisableCompression`: Indicates that on-wire compression of data must be disabled.
  - `-EnableCompression`: Indicates that throttling must be enabled.
  - `-PassThru`: Using the `-PassThru` parameter allows such cmdlets to be part of a pipeline.

  Example of syntax:

```
Set-PerformanceOptimization -ProtectionGroup $pg1
-EnableCompression
```

DPM scripts

As you may know with most command-line tools you can write scripts to automate tasks. DMS is no exception to this. In fact, one of the major purposes of PowerShell is to give IT professionals a powerful scripting tool. By default DPM comes preloaded with some scripts. As stated previously, you can type `Get-DPMSampleScript` in DMS and this will give you a list of the available DPM scripts. These scripts are located in the DPM `%systemdrive%\Program Files\Microsoft DPM\DPM\bin\` directory and here is what they are along with an explanation of what they do:

- `Attach-NonDomainServer.ps1`: This script can be used to add a workgroup server to a Protection Group on a DPM server after installing the DPM agent manually.

- `Attach-ProductionServer.ps1`: This script is used to add a protected server to DPM after you have installed the DPM agent on the protected server manually. After running this script your protected server will be listed in the DPM Administrator Console.
- `AutoProtectInstances.ps1`: If a SQL instance has auto-protection turned on and is having errors, this script can be run as an attempt to automatically repair the errors.
- `delete-shadowcopy.ps1`: This script is used to delete shadow copies manually.
- `DpmCliInitScript.ps1`: This is a DPM initilization Script that can be used if DMS has problems hanging while exiting.
- `Enable-ExchangeSCRProtection.ps1`: This script is used to enable protection of an Exchange 2007 SCR server. SCR is a high availability feature introduced in Exchange 2007, it stands for standby continuous replication. SCR is beyond the scope of this book.
- `Get-ExchangeSCRProtection.ps1`: This script will list what Exchange servers are enabled protection for SCR protection on by your DPM server.
- `Disable-ExchangeSCRProtection.ps1`: This script is used to disable protection on an Exchange 2007 SCR server.
- `Migrate-DataSource.ps1`: This is used to migrate protected computer volumes in the event a disk is corrupt.
- `MigrateDatasourceDataFromDPM.ps1`: This is used to migrate entire DPM volumes.
- `pruneshadowcopiesDpm2010.ps1`: This will look to see what recovery points are out of retention range and remove them from the DPM storage pool.
- `Remove-ProductionServer.ps1`: Use this to manually remove a protected computer from DPM.
- `Update-NonDomainServerInfo.ps1`: This script will allow you to update the password of an agent on a non-domain computer that is being protected by DPM.
- `Update-ServerInfo.ps1`: This script is used to continue protection after rebuilding a DPM server.

Notice they all have the extension `.ps1`. That is how you can tell which files in the DPM `bin` directory are DMS script files. You can edit these scripts by opening them in Windows Notepad or another text editor of your choice. If you need to modify one of these scripts before using it, it is recommended that you copy it and then use the script copy. You can run any of these scripts from the DMS. Any of these files ending with an extension of .ps1 can be run from PowerShell. Some of these scripts are used by DPM and you wouldn't want to cause issues by modifying the default scripts. These scripts are only a few of many DPM scripts you can find online. IT professionals will sometimes write their own DPM scripts and share them. You can find more DPM scripts here at Microsoft's TechNet Script Center Repository: `http://gallery.technet.microsoft.com/scriptcenter/site/search?f%5B0%5D.Type=RootCategory&f%5B0%5D.Value=systems&f%5B0%5D.Text=System%20Center&f%5B1%5D.Type=SubCategory&f%5B1%5D.Value=protection&f%5B1%5D.Text=Data%20Protection%20Manager%202007` and on System Center Central at `http://www.systemcentercentral.com/Default.aspx?tabid=143&IndexID=76863`.

Some of the types of scripts you will find in these repositories are:

- Get registry settings across multiple boxes to fix System State errors
- Find 100 GB of unused space in DPM 2010
- DPM Disk Allocated
- Get Protection Group Details
- Force Mark Tape As Free
- Export DPM Recovery points

NOTE: The majority of DPM scripts you will find online are for DPM 2007 but will work with DPM 2010. It is always recommended that you test a script on a test DPM server before running it on production.

Running pre-backup and post-backup scripts in DPM

On the DPM server there is a way to configure DPM to run scripts before and after DPM backup jobs. This is handy if you need to do something either pre or post backup such as starting or stopping a service or clearing an archive bit (which DPM cannot do). To do this you need to place your script on the protected computers local drive and change a DPM configuration file that is also located on the protected computer. The script can be in PowerShell or VBS. The file that needs to be changed is called ScriptingConfig.xml and will be located here: `%systemdrive%\Program Files\Microsoft DPM\DPM\Scripting`. DPM checks the `ScriptingConfig.xml` file before and after running backup jobs. The `ScriptingConfig.xml` file will look like this:

```
<?xml version="1.0" encoding="utf-8"?>
<ScriptConfigurationxmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns="http://schemas.microsoft.com/2003/dls/ScriptingConfig.xsd">
</ScriptConfiguration>
```

You will need to add the following lines to the file:

- `DataSourceName`: This property denotes the name of the protected data source.
- `PreBackupScript`: This script will run the pre-backup script. This is a script that you have to specify in the `ScriptingConfig.xml` file.
- `Postbackupscript`: This script will run the post-backup script. This is a script that you have to specify in the `ScriptingConfig.xml` file.
- `TimeOut`: This denotes how many minutes before the script should time out.

Once you have added the lines with the proper information the file will look like this:

```
<?xml version="1.0" encoding="utf-8" ?>
<ScriptConfigurationxmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="http://
schemas.microsoft.com/2003/dls/ScriptingConfig.xsd">
<DatasourceScriptConfigDataSourceName="E:">
<PreBackupScript>"PATHTOVBSSCRIPTORCMDFILE"</PreBackupScript>
<PostBackupScript>"PATHTOVBSSCRIPTORCMDFILE"<PostBackupScript />
<TimeOut>30</TimeOut>
</DatasourceScriptConfig>
</ScriptConfiguration>
```

NOTE: There is no way to monitor if the pre-backup and post-backup scripts ran successfully or not on the DPM server. However it is possible to monitor the pre- and post-backup scripts to see if they were successful using System Center Operations Manager. This is beyond the scope of this book.

That sums up the basics of scripts in DPM. Refer to the previously mentioned links for updated information on DPM scripts.

Overview of Opalis

Now you know that you can automate most of your DPM backup jobs and tasks using PowerShell , but the problem is that you might not be up to speed yet with PowerShell or you don't have time to write the scripts, don't panic there is a solution. This solution is Opalis.

Early last year Microsoft acquired Toronto-based Opalis Software, a maker of datacenter management software.

Opalis is an automation tool for orchestrating IT and datacenter operations. Opalis enables IT professionals with the ability to automate best practices through workflows. Best practices such as the ones found in Microsoft Operations Framework (MOF) and Information Technology Infrastructure Library (ITIL). Opalis workflow processes coordinate other systems such as System Center Operations Manager, System Center Configuration Manager, System Center Virtual Machine Manager and System Center Data Protection Manager as well as other management tools such as HP iLO, IBM Tivoli Enterprise Console, and VMware vSphere to automate tasks– Tasks such as incident response, change management, compliance and even DPM protection tasks.

Through its workflow designer, Opalis automatically shares data and initiates tasks in System Center Operations Manager, System Center Configuration Manager, System Center Service Manager, Virtual Machine Manager, Active Directory and third-party tools. Opalis workflow automates IT infrastructure tasks, while System Center Service Manager workflow provides automation of human workflow.

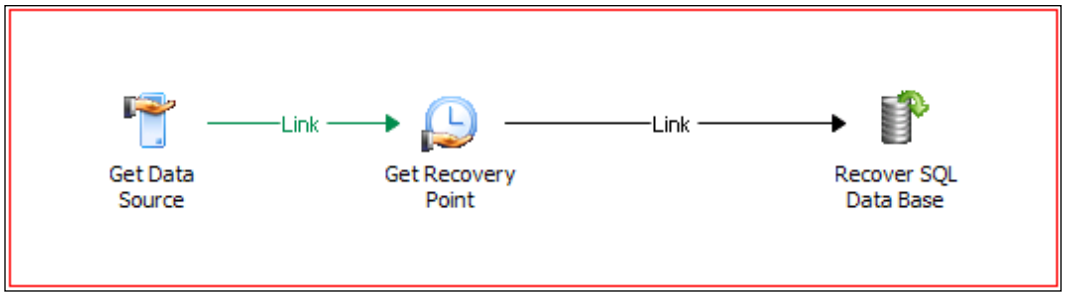
Opalis is composed of the following:

- **Client**: The Opalis Integration Server Client enables you to build, deploy, and maintain your policies.

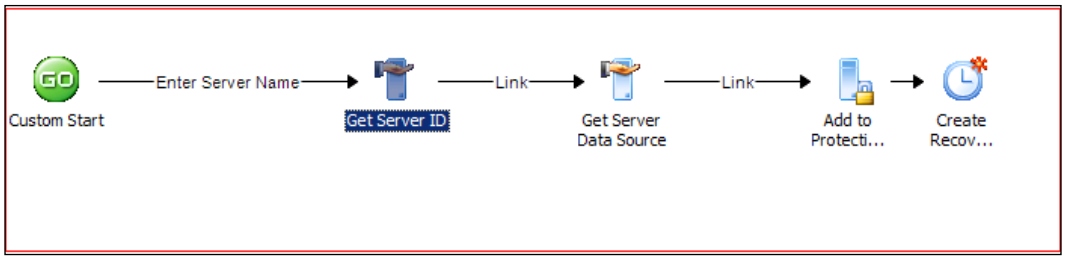
- **Operator Console**: The Operator Console enables you to see which Policies are currently running, view their real-time status, and start or stop them from a browser console interface.
- **Policy Testing Console**: The tool used by administrators to test Policies that are developed in the Client before they are deployed.
- **Action Server**: The engine that executes Policies. Action Servers have failover mechanisms that ensure performance and stability.
- **Self-Monitoring**: This service monitors for Policies that have not started and sends an event if one is detected.
- **Management Server**: The central manager of Clients, Action Servers, Policies, the Policy Testing Console, and the Self-Monitoring functionality. The Management Server deploys Opalis Integration Server Integration Packs to Action Servers and Clients, deploys Policies to Action Servers, and acts as a communication link between the Clients, the Action Servers, and the Datastore.
- **Deployment Manager**: This tool enables you to view your entire Opalis Integration Server infrastructure and deploy Action Servers, Clients, Integration Packs, and Hotfixes from one place.

Microsoft has created an integration pack for most of the system center products including DPM that allows you to automate most of the tasks and jobs.

Imagine that you have a requirement to automate a daily restore for your production database, so your development team can start testing on a fresh data-base on a daily basis. With Opalis you can create a Policy (workflow) from three steps to accomplish the task



Not limited to a database recovery, you can automate the protection process of your server deployment. With Opalis you can create a workflow that automatically protects a server, without having to create and modify a protection group or to add the server to the protection group, and so on.



That was an overview of Opalis and a couple of examples of how it can coordinate with DPM to automate tasks. Opalis is a powerful addition to DPM as well as other System Center products to help you automate your environment without being a PowerShell expert.

Summary

Today PowerShell is an important part of many Microsoft products including Data Protection Manager. We will see Microsoft continue to build future releases of DPM around PowerShell like they have done with their other products. In this chapter you were given a glimpse into the world of PowerShell and how it relates to DPM. We covered the basics of PowerShell, the Data Protection Manager Shell, an overview of Opalis as well as the cmdlets and capabilities of using PowerShell to perform DPM tasks. In the next and final chapter we will look at troubleshooting DPM problems and resources for DPM.

11
Troubleshooting and Resources

You have made it to the last chapter of this book about Data Protection Manager. The ultimate goal is for you to have a deeper understanding of DPM as a whole and to arm you to begin administration of DPM.

In any network environment, problems will arise with many of the applications on them. DPM 2010 is no exception to this. As an IT professional it is your responsibility to tackle these problems as they come up in your network environment. In this chapter we set out to cover basic DPM troubleshooting steps as well as common problems you might run into.

When I started working with DPM 2007 there was virtually no documentation about DPM apart from the Microsoft documentation. The resources on DPM 2007 were also minimal at best. This proved to be difficult when implementing and during the beginning stages of administering DPM 2007. Today there are more resources, documentation, and blogs by IT professionals on DPM 2010. Microsoft has even created a dedicated area of TechNet forums for DPM. Through this chapter you should gain information on the best resources, documentation, and tools that are out there to guide you along the DPM path.

Here are the topics that will be covered in this chapter:

- Troubleshooting DPM
    - Overview of DPM troubleshooting
    - Troubleshooting DPM installation issues
    - Troubleshooting agent installation issues
    - Troubleshooting protected server issues
    - Troubleshooting DPM client issues

- DPM resources
    - Documentation
    - List of DPM error codes
    - List of DPM releases
    - Forums
    - Blogs
    - Communities
    - Training
    - Other Tools

Troubleshooting DPM

DPM has been installed, configured to protect your environment, things are running smoothly, and then all of a sudden DPM crashes. As a DPM administrator you need to know how to troubleshoot problems with DPM deployment. Let's start off with basic DPM troubleshooting. This can be used as a guide when problems come up.

Overview of DPM troubleshooting

Whenever you run into an issue with DPM there is some general information you should gather. Most of this information you will already know but I am going to list all of it as this information should be the first step towards troubleshooting your DPM issue:

- What is the build number of your DPM? To get this information open the DPM Administrator Console and click the circled "i" next to the **Management** tab.
- What operating system is your DPM server running on and is it fully patched?
- Are there any other applications running on your DPM server? Remember that DPM should be running on a dedicated server.
- Is your DPM patched?
- Document or track when the problem first started happening.
- Were there any changes made to DPM or to the protected computer before the issues started?
- Is it only one protected data source having the issue or are there any other protected data sources having the same issue?

- Are errors specific to a data type such as SharePoint, Exchange, and Hyper-V? If the error occurs on one data type there might be a problem with the specific application that is being protected.
- When the error occurs are there other services running such as antivirus or a third-party backup used to back up DPM?
- Can the error be reproduced using specific steps?

Other general items to look at when troubleshooting DPM issues are:

- Check to make sure the following services are running:
    - **DPM Service**
    - **DPM Access Manager Service**
    - **DPM Agent Coordinator**
    - **DPM Writer**
    - **DPMLA** (if you are using tape or tape library)
    - **DPMRA**
    - **SQLAgent$MICROSOFT$DPM$** (SQL Agent)
    - **MSSQL$MICROSOFT$DPM$** (SQL Server)
    - **Virtual Disk Service** (VDS)
    - **Volume Shadow Copy** (VSS)

    To check these services go to the DPM server, open **Administrative Tools**, and then open **Services**. If the services are not running start them and make sure they are set to **Automatic** under the **Start-up** type. This applies to a DPM server running a local instance of SQL. If your DPM is running a remote instance of SQL check the SQL services on the remote SQL server and the DPM services on the local DPM server. All of these services should be set to start up automatically.
- Check the VSS writer state on the protected computer that is giving you issues. You can do this by running `vssadmin list writers` in a command window with elevated privileges on the protected computer. You want the state to be stable and to not have any errors listed. Here is an example of what the results should look like:

```
Writer name: 'VSS Metadata Store Writer'
Writer Id: {75dfb225-e2e4-4d39-9ac9-ffaff65ddf06}
Writer Instance Id: {088e7a7d-09a8-4cc6-a609-ad90e75ddc93}
State: [1] Stable
Last error: No error
```

If you do encounter any errors the first step is to search `http://support.microsoft.com` for more information on the error. If you cannot resolve it there you may need to contact Microsoft support.

- Make sure your DPM server and the protected computer with the error can communicate. From the DPM server ping the protected computers. On the protected computer ping the DPM server. Here is an example of the ping command:

```
C:\>ping buchdpm

Pinging BUCHDPM.buchatech.com [192.168.1.17] with 32 bytes of
data:
Reply from 192.168.1.17: bytes=32 time=26ms TTL=128
Reply from 192.168.1.17: bytes=32 time=5ms TTL=128
Reply from 192.168.1.17: bytes=32 time=2ms TTL=128
Reply from 192.168.1.17: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.17:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 26ms, Average = 8ms
```

  Doing this will help you verify that the name resolution (DNS) is working. Without name resolution the DPM server and protected computer would not be able to communicate.

- Check the **DPM Monitoring** tab for alerts and errors. The information on this tab will tell you what the issue is, it will give you an error ID that you can look up on TechNet (the link to this site is coming up in the resources section), and it will sometimes give you potential fixes to whatever issues are occurring. This is especially helpful when you have issues with protected computers.
- Check the event logs on the DPM server and the protected computer around the time when the job failed. This can help you identify issues with the operating system, other system issues, or application-specific issues. You can check this in the **Windows Event Viewer** under: **Event Viewer | Applications and Services | DPM Alerts**.

- If you are getting "Access Denied" errors when DPM is performing a task that involves communication with a protected computer such as synchronizing; this issue could be caused by one of two things:
    - The system time on the DPM server and the protected computer are not synced with the same time server. (The domain controller in a network is typically the time server.)
    - It could be the DPM server does not have access to the Distributed COM Users group on the protected computer. This group also needs to have Distributed COM (DCOM) Launch and Access permissions on the protected computer.

To verify the DPM server's membership to the Distributed COM Users group on the protected computer follow these steps:

1. Go to the **Start** menu, click on **Administrative Tools** | **Computer Management** | **System Tools** | **Local Users and Groups** | **Groups**.
2. In the **Details** pane, double-click the **Distributed COM Users group**.
3. Verify that the computer account for the DPM server is a member of this group.

To verify the group has DCOM Launch and Access permission on the protected computer follow these steps:

1. In **Administrative Tools**, open **Component Services**.
2. Expand **Component Services** | **Computers**, right-click **My Computer**, and then click **Properties**.
3. On the **COM Security** tab, under **Access Permissions**, click **Edit Limits**.
4. Verify that the **Distributed COM Users group** is allowed both **Local Access** and **Remote Access** permissions.
5. On the **COM Security tab**, under **Launch and Activation Permissions**, click **Edit Limits**.
6. Verify that the **Distributed COM Users groups** is allowed the following permissions:
    - Local Launch
    - Remote Launch
    - Local Activation
    - Remote Activation

(Steps taken from: `http://technet.microsoft.com/en-us/library/ff399749.aspx`.)

- Check the DPM log files. These are located in: `%systemdrive%\Program Files\Microsoft DPM\DPM\Temp` and they end with `.errlog` and `.Crash`. These can be opened with a text editor such as Notepad. These are the columns of information you will see in the `.errlog` files:

  ```
  ProcessId     ThreadId      Date   Time   ComponentCode
  FileName(FileLine)  This   TaskId Level  TraceMessage
  ```

  The `.Crash` files do not have headings for the columns but they are in human readable format.

Troubleshooting DPM installation issues

The DPM installation is pretty straightforward. We covered this in *Chapter 3*.

In the majority of cases, DPM will install without any issues as long as the hardware and software prerequisites are met. These prerequisites were also covered in *Chapter 3*. You could also run into issues while installing DPM on a remote SQL instance. Here are some of the common problems you may run into and what to do to get past them:

Problem	Resolution
DPM installation fails on local SQL installer	If SQL is installed on the current server already; uninstall it and let SQL be installed with DPM
You cannot install to a remote SQL instance because it is not recognizing the name	Make sure you have the remote SQL instance name in the correct format. It should be the servers name and then the instance name like this: `<SQLSERVERNAME>\<NAMEOFTHESQLINSTANCE>`
Error 810 or ID: 4315. The trust relationship between this workstation and the primary domain failed	Make sure that your DPM server can communicate with the domain controller. A good test is to ping the domain controller from the DPM server
Error 812. Configuration of reports failed	If you have SharePoint Services and SQL Reporting Services installed on the same application pool in IIS you will see this error. In order for both SQL Reporting Services and SharePoint to run on the same server you will need to make some configurations to SharePoint and IIS. The configuration changes you need to make can be found here: `http://msdn.microsoft.com/en-us/library/Aa179370`

Problem	Resolution
DPM is unable to configure the Windows Server account because the password you entered does not meet the Group Policy requirements	Make sure that your password meets the Group Policy password requirements
Setup cannot query the WMI service	Make sure the WMI services is enabled and started on the DPM server

Troubleshooting agent installation issues

Installing agents seem to be problematic at first, until you fully understand the process. For example, instead of trying to install the DPM agent on a server that you know has a deeply secured firewall, it makes sense to just attach the agent and manually install it on the protected server. The majority of issues I have seen with DPM agents are caused by communications. It is important for the DPM server and the protected client to be able to communicate. In my experience, running the `SetDPMServer` command on the agent computer resolves lots of issues. You would also want to check the firewall on the computer you need to protect. Make sure that the firewall is configured properly. This should cut off communication issues to the DPM server. Here are some of the common errors I have typically seen:

Problem	Resolution
Error 300: The agent operation failed because it could not communicate with the specified server	This is typically resolved by making sure the firewall is configured properly and that the RPC Server service can be contacted. Make sure DNS is functioning; your time settings may be off on either the protected computer or the DPM server; the Remote Registry service is not running on the DPM server, and the TCP/IP NetBIOS Helper service is not running on the DPM server
Error 306: Agent installation failed because the specified server already has a different version of the protection agent installed	Uninstall any already installed DPM agents from the protected computer. Remove the agent from the DPM server then add it again. Re-install the DPM agent on the protected computer

Troubleshooting protected server issues

Protected servers can be problematic because they have so many different purposes, with some of them running specific applications. Some Microsoft applications such as Exchange, SharePoint, and Hyper-V can have issues and those issues will cause protection to fail. The majority of the issues that you would see with applications like Exchange, and SharePoint can be avoided by making sure you have the prerequisites for them on the protected servers. For example, there is a `.dll` and `.exe` file that you need for DPM to be able to back up Exchange and for SharePoint you need to configure protection for it by running some commands on the SharePoint web front end. These topics were covered in *Chapter 7*. Here are some other common problems you may run into:

Problem	Resolution
DPM cannot communicate with the protected servers agent	Make sure the firewall is still set up correctly. Also make sure the agent on the protected server is set to the correct DPM server by using the `SetDPMServer` command
Recovery point time and synchronization time do not match	Recovery point time reflects the time that the data was last changed. So if the recovery point is created at a later time than the actual data was changed, DPM will show the time stamp of when the data was changed. There is no fix as this is intended behavior
Replicas are marked as inconsistent	Perform a manual consistency check on the protected data
Unable to connect to Active Directory error	Make sure the DPM server can communicate with the domain controller. Make sure your DPM server is still a member of the domain. Make sure your DPM server has the proper rights to the Active Directory. Enter the Active Directory on the domain controller and expand the domain, then expand the system, and then right-click on `MS-ShareMapConfiguration`, choose **Properties** and make sure the DPM server is listed on the **Security** tab
Volume is Missing error	Check the disk management tab in DPM to see if any of the drives are showing errors. Check disk management to see if any disks in the storage pool have errors. Resolve any errors with the disk. You may need to run manual consistency checks on the data once the disk issues are resolved

Troubleshooting DPM client issues

The best way to avoid major issues with client protection is to make sure that the firewall is configured properly inside the network and over the WAN. Also your clients communicate back to DPM via VPN when offsite so it is good practice to make sure your VPN service is healthy. On the client computer make sure these services are started:

- DPM Client Service
- DPMRA

Here are a few other issues to watch out for:

Problem	Resolution
Backups of client computers connected to a corporate network through VPN gives a status error on the client GUI RPC server unavailable error. Or cannot communicate with the DPM server.	Ensure the firewall is allowing DPM traffic through. I have a blog on how to allow traffic for DPM through ISA 2006 or TMG 2010: `http://www.buchatech.com/2011/02/allow-dpm-traffic-through-isa-2006-tmg-2010/`. If you have a different firewall, the ports still need to be configured properly. Refer to my blog for information on the ports that need to be added.

The best and most comprehensive resources for troubleshooting DPM issues are the DPM 2010 Troubleshooting Guide, the DPM error code list, and TechNet DPM forums. The links for all of these will be in the next section. The TechNet DPM forums is the best resource for troubleshooting because it will have issues that others have run into and fixes for those issues.

DPM resources

When I started working with DPM 2007 there were little or no resources out there. This has changed as there are more and more resources for Data Protection Manager popping up all the time. Microsoft has even added dedicated forums to DPM on TechNet, there are DPM MVPs now and more and more IT professionals are blogging about DPM. Here is a compiled list of the DPM resources out there for you. These are online so they are updated on a regular basis.

Documentation

The majority of DPM documentation out there is by Microsoft. The next best resource for documentation on DPM are blogs. You will see a list of DPM blogs later but here is a list of useful DPM documentation:

- Planning a System Center Data Protection Manager 2010 Deployment

  `http://www.microsoft.com/downloads/en/details.aspx?FamilyID=277DB8F2-DBD9-456A-A99D-8FB6F47F3203`

- Deploying System Center Data Protection Manager 2010

  `http://www.microsoft.com/downloads/en/details.aspx?FamilyID=4EA389EF-7626-48AC-BAC2-66EF4173F167`

- Data Protection Manager Tested Hardware

  `http://technet.microsoft.com/en-us/systemcenter/dm/cc678583.aspx`

- Data Protection Manager 2010 Operations Guide

  `http://www.microsoft.com/downloads/en/details.aspx?FamilyID=58ED28C3-252A-452B-B6E1-992BD56CEDE0`

- Data Protection Manager 2010 Troubleshooting Guide

  `http://www.microsoft.com/downloads/en/details.aspx?FamilyID=ed702ecc-0469-455c-9337-a0a7f14a3cf3`

- How to protect Hyper-V with DPM 2010 whitepaper

  `http://www.microsoft.com/downloads/en/details.aspx?FamilyID=C9D141CF-C839-4728-AF52-928F61BEBDCA`

- How to protect SQL Server with DPM 2010 whitepaper

  `http://www.microsoft.com/downloads/en/details.aspx?displaylang=en&FamilyID=d003dd4e-3c4a-4766-9749-61c846993dd8`

- How to protect SharePoint with DPM 2010 whitepaper

  `http://www.microsoft.com/downloads/en/details.aspx?FamilyID=6BD8CFF3-6E9A-49C4-A35C-51824F476DC2`

- How to protect Exchange with DPM 2010 whitepaper

  `http://www.microsoft.com/downloads/en/details.aspx?FamilyID=BE885D26-25E5-41FF-AFC8-506414AED960`

- How to protect Windows Clients with Microsoft System Center Data Protection Manager 2010

  `http://www.microsoft.com/downloads/en/details.aspx?displaylang=en&FamilyID=243b1535-8e21-4691-907d-4181cc9288a9`

Here are some other books out there where you can get more information on DPM:

- **Mastering System Center Data Protection Manager 2007** by Devin L. Ganger and Ryan Femling (*Sybex, Inc*).
- **Microsoft® System Center Enterprise Suite Unleashed**, by Chris Amaris, Tyson Kopczynski, Alec Minty, and Rand Morimoto (*Sams Technical Publishing*). This is a book about the entire System Center suite. It covers DPM but it is limited in what it could cover as it is all contained in *Chapter 10*.
- **Data Protection for Virtual Data Centers** by Jason Buffington, DPM product manager at Microsoft (*Sybex, Inc*). This book covers DPM in *Chapter 12*. It is a must-have book for any IT professional that deals with data protection and disaster recovery. This book would be a nice addition to have and a good read after finishing the DPM book you are currently reading.

List of DPM error codes

This list of error codes are maintained on TechNet by Microsoft. This list is helpful because a lot of the error codes you will run into will be on this list. It lists each error code and a possible fix:

`http://technet.microsoft.com/en-us/library/ff399290.aspx`

List of DPM releases

The following resource contains DPM version and Service Pack information all the way back to DPM 2007. Santhosh Sivarajan does a great job of keeping this list updated:

`http://portal.sivarajan.com/2009/12/dpm-2007-hotfix-and-service-pack.html`

Forums

There are plenty of forums online now dedicated to DPM with a good amount of other technical forums that have a dedicated section to DPM. Here is a list of DPM forums with lots of activity:

- Microsoft System Center forum:

  `http://social.technet.microsoft.com/Forums/en/category/dpm`
- SCDPM Online:

  `http://www.scdpmonline.org/forum.aspx`

- System Center Central:

  `http://www.systemcentercentral.com/tabid/60/tag/Forums+Data_Protection_Mgr/Default.aspx`

- myITforum.com:

  `http://www.myitforum.com/forums/System-Center-Data-Protection-Manager-f146.aspx`

- Mombu:

  `http://www.mombu.com/microsoft/f-data-protection-manager-348/?s=eaf3cce2b3790082f4a1a08acde5eee0]`

Blogs

As DPM continues to expand into more and more network environments new blogs seem to keep popping up documenting different experiences with DPM. Today if you do an internet search on Data Protection Manager several pages of the results will contain links to DPM blogs. However there are a few blog sites out there dedicated specifically to DPM or blogs that are regularly updated with DPM content and here is a list of them:

- I apologize for the shameless plug here. This is my blog `www.buchatech.com` and the section dedicated to Data Protection Manager is `http://www.buchatech.com/category/microsoft/data_protection_manager/`. Be sure to check my blog frequently for updates as I document my adventures with DPM.
- This is Jeff Buffington's blog. He is the DPM Product Manager at Microsoft:

  `http://blogs.technet.com/b/jbuff/`

- This is the Data Protection Manager product team at Microsoft's blog:

  `http://blogs.technet.com/b/dpm/`

- Microsoft DPM MVP Robert Hedblom's blog:

  `http://robertanddpm.blogspot.com/`

- Microsoft DPM MVP Islam Gomaa's blog:

  `http://owsug.ca/blogs/IslamGomaa/`

- Microsoft DPM MVP Fatih Karaalioglu's blog:

  `http://www.fakaonline.com/`

- Microsoft DPM MVP Mike Resseler's blog:

  `http://scug.be/blogs/scdpm`

- Microsoft System Center MVP David Allen's blog:

  `http://wmug.co.uk/blogs/aquilaweb/default.aspx`

- A DPM blog by Matthijs Vreeken:

  `http://scdpm.blogspot.com/`

- A DPM blog by Yegor Startsev:

  `http://ystartsev.wordpress.com`

- A System Center blog by Anders Bengtsson. He posts a lot of good information about DPM on a regular basis:

  `http://contoso.se/blog/?cat=34`

Communities

There are several community and resource websites out there for DPM, here are a few:

- The Microsoft DPM community portal:

  `http://technet.microsoft.com/en-US/systemcenter/dm/default.aspx`

- DPM Twitter page:

  `http://twitter.com/SCDPM`

- This site is a community of all things System Center including DPM:

  `http://www.systemcentercentral.com`

- This link is for TechNet Virtual labs on System Center. These are great tools for learning DPM in a test environment before you go and deploy it in a real production environment:

  `http://technet.microsoft.com/en-us/virtuallabs/bb539977`

- SCDPM Online is an online resource for DPM. It is run by Microsoft System Center MVP David Allen. It is complete with Articles, scripts, downloads, and forums for DPM:

  `http://www.scdpmonline.org/`

- An eight-step learning plan by Microsoft with links to resources. This learning plan is intended to help an IT professional get on a plan and stay on a plan to learn DPM from start to finish:

  `http://learning.microsoft.com/manager/LearningPlanV2.aspx?resourceId=62c7c178-71e4-4f95-9390-101c7e2ead84&clang=en-US&cats=d4e8e42c-3d5a-4a6e-915d-d99556a49bd7`

Training

There are some training options out there in the market if you want to get some formal instruction on DPM. Here is a list of a few options:

- DPM MVP Robert Hedblom actually works as a trainer on DPM for a company called Cornerstone in Sweden. Robert wrote the courseware for this class. I am sure this is an awesome course as it was created and is taught by Robert who also happens to be an MVP:

  `http://www.cornerstone.se/Web/Templates/CoursePage.aspx?id=2513&course=COUR20090525100914006378O4&epslanguage=SV`

- There is a three-day course by Source Solutions based out of the US. This course is hands-on and it will give you the tools to be able to implement and operate Microsoft System Center Data Protection Manager 2010:

  `http://www.sourcesolutionsco.com/current-courses/dpm/`

- Here is another three-day course on DPM based in the UK from Sovereign Computer Training & Technologies Ltd.:

  `http://www.sovereigntraining.co.uk/DPM2010_training_course.htm`

- Trainsignal has computer-based training available on DPM. This is cheaper than a class and you can do it at your own pace:

  `http://www.trainsignal.com/System-Center-Data-Protection-Manager-2010-Training.aspx`

- Here is CBT training on DPM on CBT Planet:

  `http://www.cbtplanet.com/microsoft-system-center-data-protection-manager-training-courses.htm`

Other Tools

Here is a list of free tools and some commercial add-on tools that you can download to help you with DPM:

- There is a tool called **DPM 2010 Setup Pre-Requisite Checker Tool**. This tool can be run on a server you plan to install DPM on to check and install all prerequisites that DPM 2010 needs. Here is the link to download it:

  `http://www.microsoft.com/downloads/en/details.aspx?FamilyID=6bfe19b9-1302-4dbb-a202-c20159d67057`

- If you have System Center Operations Manager or System Center Essentials in your environment you can use the **System Center Data Protection Manager 2010 Monitoring Management Pack** to monitor your DPM health. Not only does this monitor the health of your DPM it will alert you and give you suggestions to fix the errors it detects. This can be downloaded here:

```
http://www.microsoft.com/downloads/en/details.
aspx?FamilyID=32077d99-618f-43d0-843d-
4ba4f8019f84&displaylang=en
```

- Microsoft has released **DPM 2010 storage calculators**. These can help you calculate the size you will need for your DPM storage pool. Here is the link to download these:

  ```
  http://www.microsoft.com/downloads/en/details.
  aspx?FamilyID=c136c66c-bd4a-4fb1-8088-
  f610cd02dc51&displaylang=en
  ```

- The **Hyper-V Auto-Protection DPM 2010 PowerShell Script** allows you to turn on auto protection for protected Hyper-V servers. This script will make it so that if a new virtual machine turns up on the Hyper-V server it will automatically be added to the protection group on DPM. You can find the script here:

  ```
  http://www.microsoft.com/downloads/en/details.
  aspx?FamilyID=46d51b5a-5827-43f6-84f5-
  ce33f4a8e6c3&displaylang=en
  ```

- A Microsoft consultant named Ruud Baars has a useful repository of packages for DPM. These are PowerShell scripts that have been put together to help with certain tasks in DPM. They are available for download at this link:

  ```
  http://cid-b03306b628ab886f.office.live.com/browse.aspx/.Public
  ```

  Most of these tools have documentation with them but some do not. Here are a few from that list:

  - **DPMTapeUtil** combines several existing tape related scripts into one script tool to administer tapes through DPM. Here is the DPM product team's blog post on it: `http://blogs.technet.com/b/dpm/archive/2010/07/09/the-search-for-dpm-tape-utilities-stops-here.aspx`. It comes complete with a full user guide.
  - **DPM3Psync** will create shadow copies of the DPM replicas and will mount them on to a simple path so they can be accessed easily. This tool can help when using third-party backups to protect your DPM.
  - **DPMvolumeSizing** can assist you in preparing for large-scale deployments of protected data. These can include such applications as Exchange, SharePoint, SQL and Hyper-V. The instructions are for DPM 2007 but this will work for DPM 2010 as well.

- **DPMslastatus** is very useful because it can pull a report from multiple DPM servers about their recovery point statuses. This can help if you need to meet an SLA and need status reporting on more than one DPM server. This tool can even be scheduled to e-mail the reports to a DPM administrator or anyone else.

Here are some commercial tools that are add-ons to DPM. I have not used all of them but wanted to include them in this book for your reference:

- **BitWackr** is a tool made by a company named Exar. BitWackr adds true deduplication capability to DPM. It can reduce data stored by DPM up to 90% by combining deduplication with compression. BitWackr uses hardware acceleration for the deduplication process with zero impact on the processor of your DPM server. BitWackr also adds encryption to your DPM backups. You can learn more about this product here:

  `http://www.exar.com/common/content/default.aspx?id=7490`

  There are products from BridgeSTOR available that use the BitWacker technology, find them here:

  `http://www.bridgestor.com/products/dpm/146-aos-for-dpm.html`

- **Quest Management Xtensions (QMX)** is a tool made by Quest Software that enables your DPM to protect heterogeneous environments reaching into non-Windows' platforms. QMX can protect the following:
  - CiscoRouters/Switches
  - IBM AIX
  - HP-UX
  - Debian Linux
  - Fedora Linux
  - RedHat Linux
  - SuSe Linux
  - Ubuntu Linux
  - Solaris

  There are two key points that set QMX apart from the other products and that extends DPM into non-Windows environments:
  - The first is that QMX is software that you can place on your existing DPM server without the need to buy additional hardware

    - The second is that QMX allows DPM to reach into your Cisco networking equipment. As an administrator you know how critical your Cisco configuration data is. It makes for a very bad day if one of your critical Cisco routers/switches goes down and you lose the protocols, objects, rules, filters, ACLs, and so on. This software lets the administrator be sure that all of this critical configuration data is easily accessible to recover in the event of a catastrophe.

  You can learn more about this product here:

  `http://www.quest.com/system-center/backup-recovery.aspx`

- **EVault for DPM (EDPM)** is a tool made by i365 a Seagate company. EDPM is an appliance that enables your DPM to protect heterogeneous environments reaching into non-Windows' platforms. EDPM can also send your protected data to the i365 cloud. We covered EDPM more in-depth in *Chapter 10*. EDPM can protect the following:
    - Linux (Red Hat and SUSE)
    - VMware®
    - Sun Solaris
    - HP-UX
    - IBM AIX
    - IBM i (formerly OS/400)
    - Novell NetWare
    - Oracle databases

  You can learn more about this product here:

  `http://www.i365.com/products/data-backup-software/microsoft-backup-recovery/index.html`

- **CloudRecovery** is an off-site cloud solution by Iron Mountain. It allows administrators to automatically send their data to Iron Mountain's secure cloud for short- and long-term storage. We covered this product in greater detail back in *Chapter 10*. You can learn more about this product here:

  `http://ironmountain.com/forms/cloud/index.asp`

- **dBeamer!DPM** is a tool for DPM that is made by a company called Instavia Software. They specialize in instant data delivery software. dBeamer!DPM allows DPM administrators instant access to DPM data while it is restoring or even if the DPM service is offline. It also allows the data to be modified and used while the data is still being recovered. For example, a database can be attached live on a SQL instance and the service is instantly restored while the data is still being recovered. You can download a demo of this tool here:

  `https://www.instavia.com/istv/lib/download/download.php`

- **Firestreamer** is a virtual tape library. It is made by a company named Cristalink. This software enables you to use non-tape storage such as disk drives as tapes with DPM. This is helpful when you need to use some of the tape features in DPM but you do not have a tape library. We covered Firestreamer in *Chapter 4*. A demo of Firestreamer can be downloaded here:

  `http://www.cristalink.com/downloads.aspx`

Summary

As you can see there are a lot of resources and tools out there for DPM. It is a good thing most of them are free. In the future DPM will continue to grow to become an even bigger and better data protection product as it has already progressed nicely from version 2006, and 2007 up to a more stable product in the 2010 version. I am very excited about the upcoming DPM version 2012. I believe this release will be feature-packed and have many improvements over version 2010. In this chapter we talked about some troubleshooting procedures in DPM and looked at the many DPM resources that are out there.

Index

Symbols

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Thank you for buying

Microsoft Data Protection Manager 2010

About Packt Publishing

Packt, pronounced 'packed', published its first book "Mastering phpMyAdmin for Effective MySQL Management" in April 2004 and subsequently continued to specialize in publishing highly focused books on specific technologies and solutions.

Our books and publications share the experiences of your fellow IT professionals in adapting and customizing today's systems, applications, and frameworks. Our solution based books give you the knowledge and power to customize the software and technologies you're using to get the job done. Packt books are more specific and less general than the IT books you have seen in the past. Our unique business model allows us to bring you more focused information, giving you more of what you need to know, and less of what you don't.

Packt is a modern, yet unique publishing company, which focuses on producing quality, cutting-edge books for communities of developers, administrators, and newbies alike. For more information, please visit our website: `www.packtpub.com`.

About Packt Enterprise

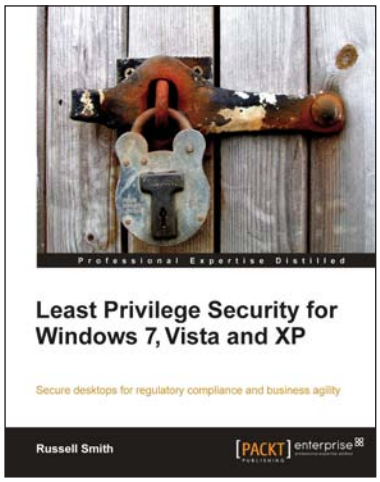
In 2010, Packt launched two new brands, Packt Enterprise and Packt Open Source, in order to continue its focus on specialization. This book is part of the Packt Enterprise brand, home to books published on enterprise software – software created by major vendors, including (but not limited to) IBM, Microsoft and Oracle, often for use in other corporations. Its titles will offer information relevant to a range of users of this software, including administrators, developers, architects, and end users.

Writing for Packt

We welcome all inquiries from people who are interested in authoring. Book proposals should be sent to author@packtpub.com. If your book idea is still at an early stage and you would like to discuss it first before writing a formal book proposal, contact us; one of our commissioning editors will get in touch with you.

We're not just looking for published authors; if you have strong technical skills but no writing experience, our experienced editors can help you develop a writing career, or simply get some additional reward for your expertise.

[PACKT] enterprise
professional expertise distilled
PUBLISHING



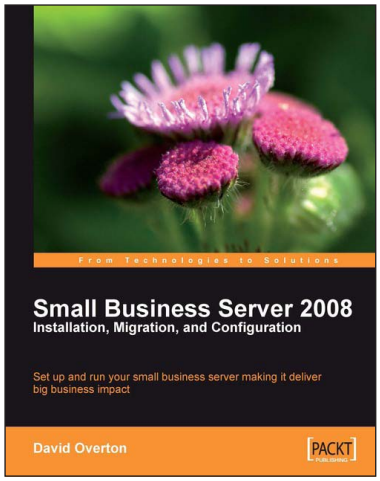
Least Privilege Security for Windows 7, Vista and XP

ISBN: 978-1-849680-04-2 Paperback: 464 pages

Secure desktops for regulatory compliance and business agility

1. Implement Least Privilege Security in Windows 7, Vista and XP to prevent unwanted system changes
2. Achieve a seamless user experience with the different components and compatibility features of Windows and Active Directory
3. Mitigate the problems and limitations many users may face when running legacy applications

---



Small Business Server 2008 – Installation, Migration, and Configuration

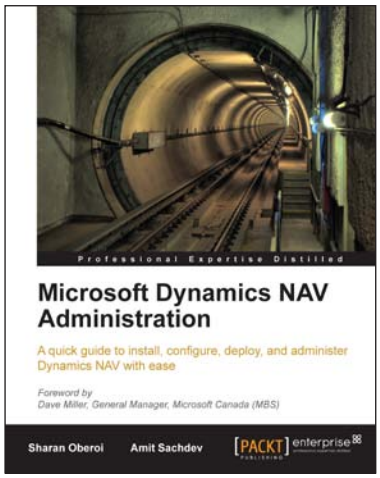
ISBN: 978-1-847196-30-9 Paperback: 408 pages

Set up and run your small business server making it deliver big business impact

1. Step-by-step guidance through the installation and configuration process with numerous pictures
2. Successfully install SBS 2008 into your business, either as a new installation or by migrating from SBS 2003
3. Configure hosted web sites for public and secure information exchange using Office Live for Small Business and Office Live Workspaces

Please check **www.PacktPub.com** for information on our titles

[PACKT] enterprise
professional expertise distilled
PUBLISHING



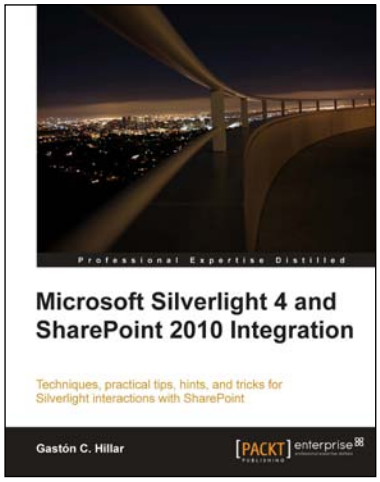
Microsoft Dynamics NAV Administration

ISBN: 978-1-847198-76-1 Paperback: 190 pages

A quick guide to install, configure, deploy, and administer Dynamics NAV with ease

1. Install, configure, deploy and administer Dynamics NAV with ease
2. Install Dynamics NAV Classic Client (Dynamics NAV C/SIDE), Dynamics NAV Role Tailored Client (RTC), and Dynamics NAV Classic Database Server on your computer to manage enterprise data
3. Connect Dynamics NAV clients to the Database Server in the earlier versions and also the latest Dynamics NAV 2009 version

---



Microsoft Silverlight 4 and SharePoint 2010 Integration

ISBN: 978-1-849680-06-6 Paperback: 336 pages

Techniques, practical tips, hints, and tricks for Silverlight interactions with SharePoint

1. Develop Silverlight RIAs that interact with SharePoint 2010 data and services
2. Explore the diverse alternatives for hosting a Silverlight RIA in a SharePoint 2010 Page
3. Work with the new SharePoint Silverlight Client Object Model to interact with elements in a SharePoint Site
4. Use Visual Studio 2010's new features to debug Silverlight RIAs that interact with SharePoint 2010

Please check **www.PacktPub.com** for information on our titles