

Operations Manager 2007 and Data Protection Manager in collaboration

This document is a first look at System Center Data Protection Manager, how to use the product to backup Operations Manager, and Operations Manager to monitor Data Protection Manager.

Author:

Anders Bengtsson, Microsoft MVP - MOM

<http://www.contoso.se>

Joseph Ryan Bittman, Microsoft MVP - DPM

<http://cactidevelopers.resdev.net/Product%20Guides/Headlines.aspx>

Reviewers:

Stefan Olsson, MCSA: Messaging

Pete Zerger, MVP - MOM

July 2007

Version 2.0

Some Rights Reserved: You are free to use and reference this document and it's, so long as, when republishing you properly credit the author and provide a link back to the published source.

Contents

Introduction	3
What to Backup.....	3
IIS Metabase.....	3
How to Backup Metabase	3
Root Management Server	4
How to backup the root management server encryption key	4
Operations Manager Database	4
Operations Manager Data Warehouse Database	5
Reporting Database	5
ACS Database	5
Master Database	5
MSDB Database	5
Management Packs	5
Files.....	6
Schedule Tasks within Operations Manager 2007	6
Background Information about Data Protection Manager.....	6
How-to backup SQL databases with Data Protection Manager.....	7
How-to Backup Files and Directories with Data Protection Manager.....	9
Monitoring System Center Data Protection Manager.....	11
Links to Related Information.....	12
Feedback.....	12

Introduction

In this guide you will learn how to backup your Operations Manager 2007 management group using Data Protection Manager. Data Protection Manager is a member of the System Center suite.

This guide is based on System Center Operations Manager 2007 and System Center Data Protection Manager beta 2. Most likely there will be modification in the product before RTM version. This guide will not cover restore of your management group.

What to Backup

There are a number of components to backup in a management group. Which component to backup depends on your environment, for example not all environments includes custom reports and audit collection servers. The following components need to be backed up within Operations Manager 2007, depending on the environment:

- Metabase
- Root Management Server
- Operations Manager Database
- Operations Manager Data warehouse Database
- Reporting Database
- ACS Database
- Master Database
- MSDB Database
- Management Packs
- Files

IIS Metabase

The metabase is xml file stores configuration information on IIS settings. You should backup the metabase once after installation and then after every major modification. This is done on the machine running the web console and on the machine running reporting services.

How to Backup Metabase

You can setup a protection group within DPM to backup your metabase too, as the metabase is part of the system state. This is also the most reliable backup of the metabase. You can setup the protection group in the same way as with SQL, but instead of SQL, choose system state in the wizard.

This will show you how to do a backup with the IIS console

1. From the start menu start the **Internet Information Services (IIS) Manager**
2. In Internet Information Services (IIS) Manager, **right-click** your **server name** and choose **All Tasks** and **Backup/Restore Configuration**
3. In the Configuration Backup/Restore window, click **Create Backup...**
4. In the Configuration Backup window, **input a backup name** and click **OK**

5. In the Configuration Backup/Restore window, click **Close**
6. In Internet Information Services (IIS) Manager, open the **File menu** and choose **Exit** from the drop down menu

The default location of the backup file will be C:\WINDOWS\system32\inetsrv\MetaBack.

Root Management Server

The root management server is the first management server in your management group. This server includes a number of roles. If this machine goes down, agent less machines can't be monitored and gateway servers cannot send data from agents. Also you can't connect with a console to your management group. The management root server also includes an encryption key that includes all run-as account information.

How to backup the root management server encryption key

1. **Copy SecureStorageBackup.exe** from the installation CD (\SupportTools) to the Ops Mgr installation directory (default C:\Program Files\System Center Operations Manager 2007\)
2. From the start menu open a **command prompt**
3. At the command prompt, change directory to the installation directory, with default settings, input **cd C:\program files\system center operations manager 2007** and click **enter**
4. At the command prompt, input **SecureStorageBackup.exe Backup C:\BackupOfKey.bin**
5. At the command prompt, when prompted, **input a password**

Make sure take notice of the password you used. To use Data Protection Manager to back up this file, synchronization must occur at least every week due to DPM's architecture. If you don't want this file sitting on the file system, look into DPM 'pre-scripting' the SecureStorageBackup command to create the file before the DPM backup job, and then 'post-scripting' to delete the file off the operating system. As specified in the note about synchronizations below in the How-to backup files section, make sure you ensure a recovery point is created after the synchronization grabs this key file before it is noticed to be deleted at the next synchronization.

Operations Manager Database

Your operations manager database contains all settings, agent information, management packs, all customizations, operations data and all other information and data that operations manager requires to operate. If this database is lost without a backup, you will have to rebuild your entire management group.

When you are working with operations manager there are read and write operations in this database at all times. This means the data is constantly updating, therefore you must backup this database more often.

In Microsoft Operations Manager (MOM) 2005 this database is named OnePoint. In operations manager 2007 you can choose any name during the setup. Default database name is OperationsManager. You should backup this database on a daily basis.

Operations Manager Data Warehouse Database

The Data Warehouse database stores all historic data used by your reports. Data is transferred from your operations manager database to your reporting database continuously, not as in MOM 2005 where it was transferred only one time every 24-hour period. This should be remembered when planning the backup schedule. If you lose this database you will not get access to any historic data. This data is an important component for performance tracking, cost planning and analyses.

The data warehouse database uses simple recovery mode with default settings. This means there is no idea backing up log files, instead make complete database file backup. Default database name is OperationsManagerDW. You should do a full backup of this database every month and an incremental backup every week. The backup schedule must fulfill your organization requirements.

Reporting Database

The Reporting server database stores all report definitions, report metadata, cached reports and snapshots. If you lose this database and don't have a backup you can re-import all reports, but cached reports will be lost. You should backup this database after modification of reports or adding new reports.

ACS Database

The ACS database stores all security events collected from your agents. This database is continuously updated, as new events are written. It is important to backup this database often as it will be used in forensic work if anything happens on your machines. Default database name is OperationsManagerAC.

If you lose this database you will not have access to any security related information collected with your ACS policy, and you will not be able to collect any event either. You should do a full backup of this database every month and an incremental backup every week.

Master Database

The Master database is a system database within SQL Server. This database stores all system-level information, for example logon accounts and file locations. You should backup this database once after installation of operation, and then after every major modification.

MSDB Database

The MSDB database is a system database within SQL Server. This database stores agent related data, for example schedule jobs. Operation Manager 2007 is depending on a number of scheduled tasks and therefore it is important to backup this database too. You should backup this database once after installation of operation, and then after every major modification.

Management Packs

Management packs contain all information how an application or device should be monitored. Sealed management packs can't be changed; instead all changes are stored in new management packs. According to best practices you should have a management pack for customization for every sealed

management pack, for example if you have Exchange MP you should have an exchange customization management pack too. You should backup your custom management packs after every modification.

Files

If you are running gateway servers or agents with certificates, it is important to back them up. If you have developed custom reports you must backup them too, custom reports are stored in rdl-files. You should backup your custom management packs after every modification.

Schedule Tasks within Operations Manager 2007

There are a number of maintenance jobs running within an Operations Manager 2007 management group. Operations Manager 2007 maintenance jobs are visible within the Ops Mgr console, if you look under Rules in the Authoring part of the console you can see these jobs as system rules. You should plan your backup jobs so they do not interrupt with a maintenance job.

Task name	Default schedule	Note
Discovery Data Grooming	Every day at 02:00	System rule that grooms discovery data
Partition and Grooming	Every day at 00:00	Partition and delete old data from the Operations Manager database
Detect and fix object space	Every 30 minute	Detects and fixes object space inconsistencies in the operational database.
Alert Auto Resolved Execute All Properties	Every day at 04:00	Auto resolves alerts after a pre-defined time

Background Information about Data Protection Manager

DPM's protection architecture specifies that change information is kept track of and transferred to the DPM server, using a 'protection agent'. This agent is installed through the Management area of DPM administrator console or locally on the production server and then 'attached' to the appropriate DPM server using a commandlet through the DPM Management Shell.

To begin protection, you must create a Protection Group (PG). A PG contains the information necessary for protecting data, including what servers, what files/applications and the frequency of backups. After creation, a 'replica' is created on the DPM server. A replica, as the name implies, is an exact copy of the data on the production server. This initial complete transfer of information can be sent automatically over the network by DPM, or manually yourself through a variety of storage mediums. Synchronizations (incremental backups) and express full backups are then performed to pull any new changes, and sacrificing specifics for general understanding, update the replica.

'Recovery points' are created against the replica, for a specific point-in-time version of the data, which are the versions which can be recovered. Incremental and express full backups, as well as the recovery point creations, are scheduled according to the Protection Group settings specified. Depending on the type of data and intricacies involved, recovery points may be created automatically during certain types of jobs.

All this data from the production server is stored in two places, the replica area and recovery point area. These areas are physically located on the DPM server disks in the 'DPM Storage Pool' or specified during PG creation on specific empty partitions in accordance to the Custom Volumes feature. This guide assumes the Storage Pool is used, and assumes you have previously added a disk to the pool. Adding disks and installing agents are beyond the scope of this guide (although these events are assumed to have already occurred), although both procedures are very intuitive and done through the Management area of the user interface.

Note: adding a disk to the Storage Pool erases all data on it and its usage can only be used for DPM. See DPM documentation for further information.

How-to backup SQL databases with Data Protection Manager

This section assumes you have previously installed a protection agent on the SQL server and have added disk storage to the DPM storage pool. Feel free to customize the following steps to your environment, which will be necessary in a majority of steps. Databases with similar protection schedule needs should be grouped together among multiple protection groups to tailor to their protection frequency needs. The following steps will show how to protect the Master and MSDB in the same protection group, as they have similar needs set forth earlier in the guide. To begin,

1. From the start menu start the **DPM Administrator Console**
2. In DPM Administrator Console: click **Protection**
3. In DPM Administrator Console - Protection: click "**Create protection group...**"
4. At the Create New Protection Group Wizard - *Welcome*: click **Next**
5. At the Create New Protection Group Wizard - *Select group members*: Expand your **domain**, expand your **database server**, expand **All SQL Servers**, expand the **SQL server instance**, select the **Master** and **MSDB** databases. Click **Next**

Note: A message complaining about SQL server prerequisites not met may appear. If so, please check and make sure the SQL VSS writer service is running and SP1 is installed.

6. At the Create New Protection Group Wizard - *Select data protection method*: Specify a self-explanatory **Protection Group name**, select **short term protection using Disk**, click **Next**

7. At the Create New Protection Group Wizard - *Select short-term objectives*: Specify a retention range then click **Modify** and input settings for express full backup. Click **OK** and then click **Next**

Note: Incremental backups can only be performed if the SQL database is set as full recovery mode. Otherwise, recovery points are created using full express backups which are more intensive on server resources and can only be performed every 30 minutes, compared to every 15 minutes with incremental backup jobs. This guide assumes simple recovery mode. Please see Data Protection Manager product documentation for further details.

As the guide previously mentions, the Master and MSDB databases don't have high frequency backup requirements. Modify the schedule as you feel appropriate. An example might be once a week during off-peak hours such as Sunday at 2 AM. The least frequent possible is once a week. The retention range specifies how many days to keep before being deleted. The max eldest you may keep is 64 days old (not including days the replica was inconsistent). See DPM product documentation for further information about scheduling jobs to meet your needs.

8. At the Create New Protection Group Wizard - *Review disk allocation*: Click **Modify**

On this page, you get to make sure there is enough storage allocated to the replica and recovery point areas. In addition to the current live data's sizing needs, make sure to provide enough to cover future expected growth.

Note: If you cannot dedicate a whole disk to the storage pool, look into documentation about the Custom Volumes feature. To use Custom Volumes, select this option from the drop down list on the current page and specify your custom-created partitions for each replica and recovery point area. Pay close attention to partition sizing, as any future change needs will have to be done by you through Disk Management, and may require the re-creation of the Protection Group.

Review the default allocated space and adjust accordingly, click **OK**, then **Next**.

9. At the Create New Protection Group Wizard - *Choose Replica Creation Method*: Choose **Automatic** and **Now**.

Initially, an exact copy of the data on the production server needs to be transferred to the DPM server. This can either be done by DPM now or at a later date, or manually by you copying the data to another storage medium and transferring it to the DPM server. You may wish to transfer manually if you are concerned with the amount of network stress needed or to quicken the transfer in some cases. Click the Help button for info on how to manually transfer the replica. Click **Next**

10. At the Create New Protection Group Wizard - *Summary*: **Review** your settings and going back pages to make corrections. Then click **Create Group** to begin the creation of the PG and automatic start of the replica creation if chosen.
11. Click **Close** after watching the progress – finish monitoring the replica creation through the Protection and Monitoring areas of the user interface. Verify that the results are **successes**.

Tasks	
Task	Results
Create protection group: DEV. Master and MSDB db	Success
Allocate Replica For CO-OPSMGR-GRP2\msdb	Success
Allocate Replica For CO-OPSMGR-GRP2\master	Success

How-to Backup Files and Directories with Data Protection Manager

This section assumes you have previously installed a protection agent on the file server and have added disk storage to the DPM storage pool. Feel free to customize the following steps to your environment, which will be necessary in a majority of steps. File servers with similar protection schedule needs should be grouped together among protection groups to tailor to their protection frequency needs. The following steps will show how to directories. To begin,

1. From the start menu start the **DPM Administrator Console**
2. In DPM Administrator Console: click **Protection**
3. In DPM Administrator Console - Protection: click "**Create protection group...**"
4. At the Create New Protection Group Wizard - *Welcome*: click **Next**
5. At the Create New Protection Group Wizard - *Select group members*: Expand your **domain**, expand your **file server**, expand **All Volumes**, expand the **drive**, and select the **folders** to protect, such as "C:\windows\system32\inetrv\metaback\" for IIS. Click **Next**.

Note: Depending on whether the folder is expanded or collapsed, checking a parent folder does not necessarily mean the children will be checked. Verify children are checked as expected. Check DPM documentation for more information on how events such as a new folder created under a protected folder are handled.

Also, if a message comes up about protecting files from a system volume, you can ignore it. It is warning you that by protecting an entire volume you won't be protecting all that is necessary to recovery system state in a disaster.

6. On Create New Protection Group Wizard - *Select data protection method*: Specify a self-explanatory **Protection Group name**, select **short term protection using Disk**, click **Next**

7. At the Create New Protection Group Wizard - *Select short-term objectives*: Carefully specify a **retention range** and **synchronization schedule**.

Unlike with types of application data, synchronizations on files do not automatically create recovery points. The synchronizations are applied to the replica. The data versions available for recovery are only the recovery points created according to the schedule or manually by the administrator against the current replica. Also, unlike with application data, there is a maximum limit of 64 recovery points – then oldest points are deleted as new ones are created.

To clarify, synchronizations can occur on a schedule such as every 15 minutes. This does not necessarily mean you will achieve a maximum of 15 minute data loss! Synchronizations do not create recovery points which are the versions available for recovery. For example, if a user had a file and this file existed during a previous synchronization, and the file got deleted, the file's ability to be restored is determined by a number of factors. If a recovery point was created which contained the file, then this recovery point can be restored from, and the file is easily restored. If a recovery point has not been created but the file is in existent in the current DPM replica's copy, an administrator can manually create a recovery point of the replica at any time through the UI console, and the file can then be restored.

Here is an example of the types of scenarios you have to watch out for: *If* the file had been captured in the previous synchronization with no recovery point yet (so the file is in the replica), the file gets deleted, and another synchronization takes place before a recovery point, then this new synchronization will notice the file no longer exists and will delete it from the replica. Since there is no longer a copy of the file on the production server, DPM replica, or DPM recovery points, then file is lost. **Note:** if a DPM-to-DPM disaster recovery scenario is implemented, the DPM server backing up the normally used DPM server might have a copy of the replica from the time the file existed in the first DPM server's replica. See documentation for more information and limitations of the DPM-to-DPM scenario.

8. On the same page, *Select short-term objectives*, click **Modify** to specify a recovery point schedule. As mentioned above, the recovery point schedule needs careful consideration in relation to the synchronization schedule. **Close** the modify window and then click **Next**.

Note: The retention range value specified previously will limit the number of recovery point creations scheduled. This is due to the 64 point limit. . . for instance, to ensure a 10 day retention range of backups, there can be no more than 6 recovery points created per day, as this is 60 points over 10 days which is under the 64 max. If you put the retention range lower, such as 5 days, then up to 12 recovery points will be allowed per day. This 64 limitation is mandated by the operating system for End User Recovery functionality which DPM implements.

9. At the Create New Protection Group Wizard - *Review disk allocation*: **Review** this page to make sure there is enough storage allocated to the replica and recovery point areas. In addition to the

current live data's sizing needs, make sure to provide enough to cover future expected growth.

Note: It is very important on PGs containing files, to click **Modify**, and click **Calculate** so that DPM can accurately determine the current size of the data to be protected. Without calculating, DPM's recommended values can be off *significantly*.

10. Perform the steps in the above note. Click **Modify** and then **Calculate** for all entries shown. **Close** the window and click **Next**.

Note: If you cannot dedicate a whole disk to the storage pool, look into documentation about the Custom Volumes feature. To use Custom Volumes, select this option from the drop down list on the current page and specify your custom-created partitions for each replica and recovery point area. Pay close attention to partition sizing, as any future change needs will have to be done by you through Disk Management, and may require the re-creation of the Protection Group.

11. At the Create New Protection Group Wizard - *Choose Replica Creation Method*: Choose **Automatic** and **Now**.

Initially, an exact copy of the data on the production server needs to be transferred to the DPM server. This can either be done by DPM now or at a later date, or manually by you copying the data to another storage medium and transferring it to the DPM server. You may wish to transfer manually if you are concerned with the amount of network stress needed or to quicken the transfer in some cases. Click the Help button for info on how to manually transfer the replica. Click **Next**

12. At the Create New Protection Group Wizard - *Summary*: **Review** your settings and going back pages to make corrections. Then click **Create Group** to begin the creation of the PG and automatic start of the replica creation if chosen.

13. Click **Close** after watching the progress – finish monitoring the replica creation through the Protection and Monitoring areas of the user interface. Verify that the results are **successes**.

Monitoring System Center Data Protection Manager

Data Protection Manager includes a couple of functions to monitor the system. You can setup SMTP notification to get an e-mail when anything happens. You can also read the logs and look in the administrator console. These functions are very suitable for large organizations.

The best way to monitor your Data Protection Manager is with Microsoft Operations Manager (MOM) or Microsoft System Center Operations Manager (Ops Mgr). With Operations Manager and the data protection manager management pack you get a central system to verify the health of all your server

protection. This can make troubleshooting much easier. With Operations Manager you can also generate reports about your server protection. An administrator can also generate custom reports for purposes such as auditing by writing custom SQL Reporting Services queries against the DPM server database.

Links to Related Information

Operations Manager 2007 Backup and Recovery Guide

http://download.microsoft.com/download/7/4/d/74deff5e-449f-4a6b-91dd-ffbc117869a2/OpsMgr2007_Backup.doc

System Center Data Protection Manager 2007

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

Feedback

Please send your comments and suggestions to anders@contoso.se