Guide for System Center Management Packs for Data Protection Manager Reporting, Library, Discovery and Monitoring

Microsoft Corporation

Published: October-2020

Send feedback or suggestions about this document to [mpgfeed@microsoft.com](mailto:mpgfeed@microsoft.com). Please include the management pack guide name with your feedback.

The Operations Manager team encourages you to provide feedback on the management pack by providing a review on the management pack’s page in the [Management Pack Catalog](http://go.microsoft.com/fwlink/?LinkID=82105) (http://go.microsoft.com/fwlink/?LinkID=82105).

Copyright

This document is provided "as-is". Information and views expressed in this document, including URL and other Internet Web site references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious.  No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You may modify this document for your internal, reference purposes.

© 2013 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Bing, BizTalk, Forefront, Hyper-V, Internet Explorer, JScript, SharePoint, Silverlight, SQL Database, SQL Server, Visio, Visual Basic, Visual Studio, Win32, Windows, Windows Azure, Windows Intune, Windows PowerShell, Windows Server, and Windows Vista are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners.

Contents

[Guide for System Center Management Packs for Data Protection Manager Reporting, Library, Discovery and Monitoring 3](#_Toc53995315)

[Document Version 4](#_Toc53995316)

[Revision History 4](#_Toc53995317)

[Management Pack Scope 4](#_Toc53995318)

[Install Instruction 7](#_Toc53995319)

[Files in this Management Pack 7](#_Toc53995320)

[Management Pack Purpose 8](#_Toc53995321)

[Configuring the Management Pack for Data Protection Manager Reporting, Discovery and Monitoring 9](#_Toc53995322)

[Best Practice: Create a Management Pack for Customizations 9](#_Toc53995323)

[Security Configuration 9](#_Toc53995324)

[Tuning Performance Threshold Rules 10](#_Toc53995325)

[Links 10](#_Toc53995326)

[System Center - Operations Manager 10](#_Toc53995327)

[Appendix A: Management Pack Contents 10](#_Toc53995328)

# Guide for System Center Management Packs for Data Protection Manager Reporting, Library, Discovery and Monitoring

This guide was written based on following version of the Management Packs for Data Protection Manager:

* Microsoft.SystemCenter.DataProtectionManager.Library.MP(version 5.0.1401.2)
* Microsoft.SystemCenter.DataProtectionManager.Discovery.MP(version 5.0.1401.2)
* Microsoft.SystemCenter.DataProtectionManager.Reporting.MP(version 5.0.1401.2)

### Document Version

This guide is based on the 5.0.1401.2 version of the DPM Management Pack.

### Revision History

|  |  |
| --- | --- |
| Release Date | Changes |
| October, 2020 (Version 5.0.1401.2) | * Fixed Bugs: Protected data sources, Top backup failure reasons, Storage utilization segment issues |

Supported Configurations

This set of management packs requires System Center Operations Manager.

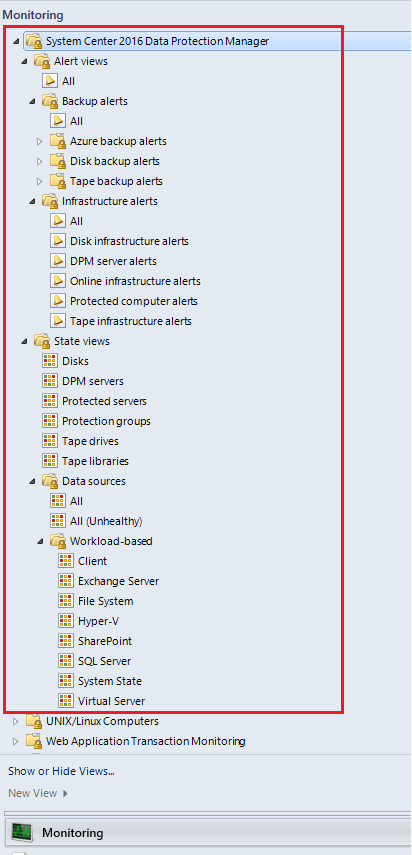
The following table details the supported configurations for the Management Packs for Data Protection Manager:

|  |  |
| --- | --- |
| **Configuration** | **Support** |
| DPM Reporting Management Pack | 5.0.1401.2 |
| DPM Discovery and Monitoring Management Pack | 5.0.1401.2 |
| DPM Library Management Pack | 5.0.1401.2 |
| Clustered servers | Yes |
| Agentless monitoring | No |
| Virtual environment | Yes |

### Management Pack Scope

#### Library, Discover & Monitoring Management Packs

The discovery and library management packs enable you to view, monitor and manage DPM servers, alerts, notifications, and some other monitoring information. For instance, the following menu items appear on the SCOM console after you import the Discovery and Library management packs.



#### Reporting Management Pack

The reporting management pack enables and supports collecting reporting data from all DPM servers deployed on your network. For example, if your domain deployment contains 100 DPM servers, each containing 20 data sources configured into a separate Protection Group (PG), this management pack will enable SCOM to monitor and report data on all 100 x 20 = 2000 data sources.

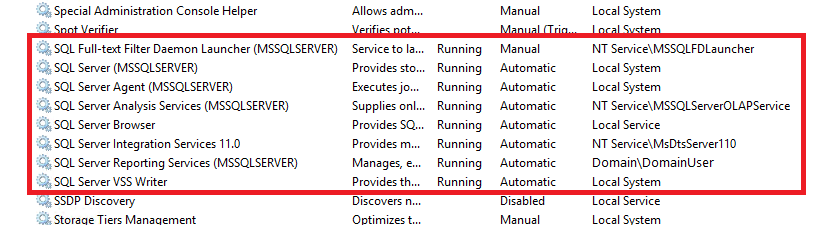
#### Prerequisites

The following requirements must be met to run the discovery, library and reporting management packs:

* SC Data Protection Manager must be installed, up and running on all the DPM servers.
* If you want SLA data in DPM reports, Set SLA Requirements on the DPM Server using the PowerShell command-let :

**Set-DPMProtectionGroupSLA –SLAInHours**

If SLAs are not set on the DPM Servers, you will not get SLA Trends in the Reports.

* SCOM must be up and running.
* SCOM’s Data Warehouse should be up and running. To verify that, ensure that all the SQL Server services with the service name containing the SCOM DB Instance name are up and running. The screenshot depicting the list of running [services](http://technet.microsoft.com/en-us/library/cc772408.aspx) below captures this scenario and your deployment environment must show a similar state before you proceed to install this MP.

### Install Instruction

1. Uninstall any existing DPM MPs.
2. Install [DPM Central Console](http://technet.microsoft.com/en-in/library/jj860391.aspx) version using the guide [here](https://docs.microsoft.com/en-us/system-center/dpm/use-central-console-to-manage-multiple-dpm-servers).
3. Install SCOM Agents using Discovery wizard on all DPM Servers that you want to monitor using central console.
4. Install latest MPs that came with this update
   1. Double click on the msi file that came with this update, accept the license agreement and click on Next.
   2. Select the installation folder and click on Next
   3. Click on Install
   4. It will extract the MP at selected folder
5. In the SCOM Operations Console, right-click the Management Packs entry in the Administration view and Import the following Management Packs using “Add from Disk” option and browsing to the folder selected in Step 4.b

* Microsoft.SystemCenter.DataProtectionManager.Discovery.MP(version 5.0.1401.2)
* Microsoft.SystemCenter.DataProtectionManager.Library.MP(version 5.0.1401.2)
* Microsoft.SystemCenter.DataProtectionManager.Reporting.MP(version 5.0.1401.2)

**Note**: If you get an error while importing the Management Pack try to delete RTM version of Library and Discover & Monitoring MPs(version 5.0.1200.0) and then import the latest Management packs.

### Files in this Management Pack

Import the three management packs as listed below in to your SCOM server following the sequence mentioned in the section “Mandatory Configuration” above.

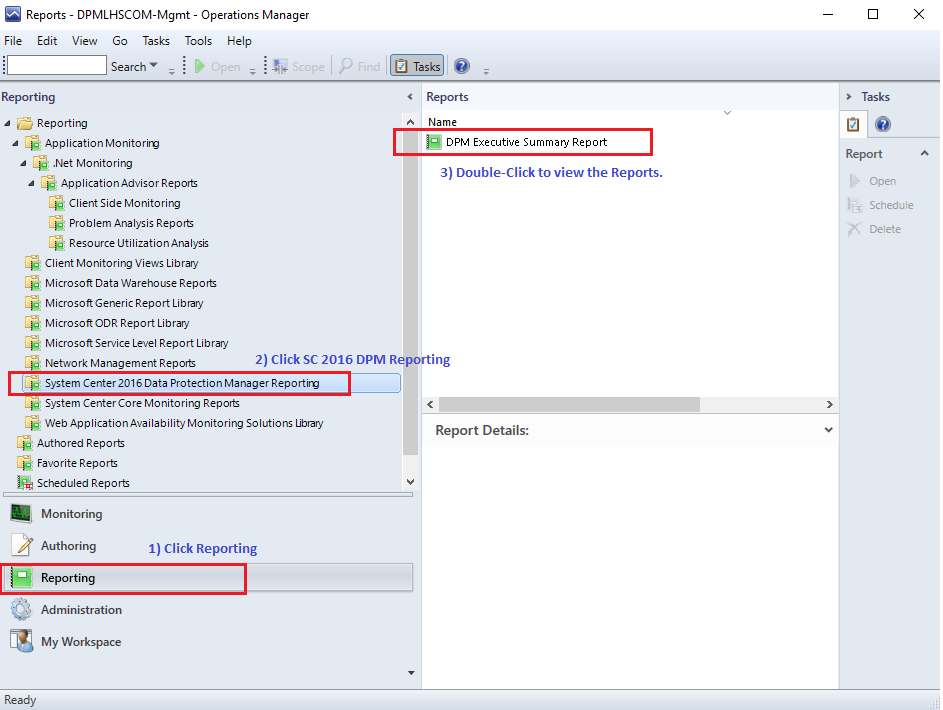
The set of Management Packs for Data Protection Manager Reporting, Discovery and Monitoring includes the following files:

* Microsoft.SystemCenter.DataProtectionManager.Discovery.MP (required) (version *5*.0.1401.2)
* Microsoft.SystemCenter.DataProtectionManager.Library.MP (required) (version *5*.0.1401.2)
* Microsoft.SystemCenter.DataProtectionManager.Reporting.MP (required) (version *5*.0.1401.2)

After importing all management packs, the list of MPs should look something like the following:

Management Pack Purpose

This management pack supports collecting reporting data from all DPM servers deployed on your network. You may write your own code to fetch backup reporting data from the SCOM Data Warehouse views listed in this [Microsoft TechNet article](http://go.microsoft.com/fwlink/?LinkId=525601). For example, if your domain deployment contains 100 DPM servers, each containing 20 data sources configured into a separate Protection Group (PG), this management pack will enable SCOM to monitor and report data on all 100 x 20 = 2000 data sources.



This data will be stored in the SCOM Data Warehouse (DW) and a sample report can be viewed on the SCOM Console by clicking “**Reporting**” on the bottom left pane, then navigating to “**System Center Data Protection Manager Reporting**” and then double-clicking on “**DPM Executive Summary Report**”.

A comprehensive list of the **SCOM Views for DPM Reporting** are given in this [Microsoft TechNet article](http://go.microsoft.com/fwlink/?LinkId=525601) for your quick and easy reference. The sample reports use the same set of tables and views for organizing and displaying reporting data consolidated in to a dashboard format.

In order to view detailed information about any particular aspect of reporting, you may use any tools or programming or scripting language to generate and display detailed reports in a customized format. A sample use case could be - writing a program (using any programming or scripting language of your choice) to download Tape Backup or Cloud Backup and Utilization to an Excel sheet every night at 3AM which the backup administrator can come and analyze the next morning.

### Configuring the Management Pack for Data Protection Manager Reporting, Discovery and Monitoring

This section provides guidance on configuring and tuning this management pack.

 [Best Practice: Create a Management Pack for Customizations](#z2)

 [Security Configuration](#z3)

 [Tuning Performance Threshold Rules](#z4)

### Best Practice: Create a Management Pack for Customizations

By default, Operations Manager saves all customizations such as overrides to the Default Management Pack. As a best practice, you should instead create a separate management pack for each sealed management pack you want to customize.

When you create a management pack for the purpose of storing customized settings for a sealed management pack, it is helpful to base the name of the new management pack on the name of the management pack that it is customizing.

Creating a new management pack for storing customizations of each sealed management pack makes it easier to export the customizations from a test environment to a production environment. It also makes it easier to delete a management pack, because you must delete any dependencies before you can delete a management pack. If customizations for all management packs are saved in the Default Management Pack and you need to delete a single management pack, you must first delete the Default Management Pack, which also deletes customizations to other management packs.

### Security Configuration

DPM Discovery, Library and Reporting MPs contain no “Run As” Profiles.

|  |  |  |
| --- | --- | --- |
| Run As Profile Name | Associated Rules and Monitors | Notes |
|  |  |  |

### Tuning Performance Threshold Rules

DPM Discovery, Library and Reporting MPs do not require Performance Threshold Rules since most of the necessary settings will be configured after the installation of Central Console.

|  |  |
| --- | --- |
| Rule Name | Default Threshold |
|  |  |

### Links

The following links connect you to information about common tasks that are associated with System Center management packs:

### System Center - Operations Manager

* [Management Pack Life Cycle](https://docs.microsoft.com/en-us/system-center/scom/manage-mp-lifecycle)
* [How to Import a Management Pack](https://docs.microsoft.com/system-center/scom/manage-mp-import-remove-delete)
* [Tuning Monitoring by Using Targeting and Overrides](https://docs.microsoft.com/system-center/scom/manage-mp-override-rule-monitor)
* [How to Create a Run As Account](https://docs.microsoft.com/system-center/scom/manage-security-create-runas-link-profile)
* [How to Export a Management Pack](https://docs.microsoft.com/system-center/scom/manage-mp-import-remove-delete)
* [How to Remove a Management Pack](https://docs.microsoft.com/system-center/scom/manage-mp-import-remove-delete)

For questions about Operations Manager and management packs, see the [System Center Operations Manager community forum](http://go.microsoft.com/fwlink/?LinkID=179635).

A useful resource is the [System Center Operations Manager Unleashed blog](http://go.microsoft.com/fwlink/?LinkId=246391), which contains "By Example" posts for specific management packs.

Important

All information and content on non-Microsoft sites is provided by the owner or the users of the website. Microsoft makes no warranties, express, implied, or statutory, as to the information at this website.

### Appendix A: Management Pack Contents

The Management Pack for DPM Reporting discovers the object types described in the following sections. Not all of the objects are automatically discovered. Use overrides to discover those objects that are not discovered automatically.

Discovery Information

DPM Discovery, Library and Reporting MPs contain no Discoveries.

Related Monitors

DPM Discovery, Library and Reporting MPs contain no Monitors.

Note

If you are using connectors, you can disable the monitor and enable its corresponding rule to enable alerts without changing health status.

Related Rules

|  |  |  |  |
| --- | --- | --- | --- |
| Rule | Data source | Notes | Enabled |
| DPM.NetworkPerfRecv.Rule | System.Performance.OptimizedDataProvider | This rule collects Received Bytes performance data and inserts it into the Data warehouse DB. | True |
| DPM.NetworkPerfSend.Rule | System.Performance.OptimizedDataProvider | This rule collects Sent Bytes performance data and inserts it into the Data warehouse DB. | True |
| SCDPM.DiskUtilizationCollection.Rule | Windows!Microsoft.Windows.TimedScript.EventProvider | This rule collects Disk Utilization data and inserts it into the Data warehouse DB. | True |
| SCDPM.BackupJobCollection.Rule | Windows!Microsoft.Windows.TimedScript.EventProvider | This rule collects Backup jobs data and inserts it into the Data warehouse DB. | True |
| SCDPM.DiskManagementCollection.Rule | Windows!Microsoft.Windows.TimedScript.EventProvider | This rule collects Disk Management data and inserts it into the Data warehouse DB. | True |
| SCDPM.RecoveryJobCollection.Rule | Windows!Microsoft.Windows.TimedScript.EventProvider | This rule collects Recovery jobs data and inserts it into the Data warehouse DB. | True |
| SCDPM.SLATrendCollection.Rule | Windows!Microsoft.Windows.TimedScript.EventProvider | This rule collects SLA trend data and inserts it into the Data warehouse DB. | True |
| SCDPM.TapeUtlizationCollection.Rule | Windows!Microsoft.Windows.TimedScript.EventProvider | This rule collects Tape Utilization data and inserts it into the Data warehouse DB. | True |

Note

Disable the rule and enable its corresponding monitor to enable alerts, state changes, and health rollup.