

System Center Data Protection Manager 2010 Management Pack Guide for Operations Manager 2007

Microsoft Corporation

Published: October 2010

Send suggestions and comments about this document to [mpgfeed@microsoft.com](mailto:mpgfeed@microsoft.com?subject=%20DPM%202010%20Management%20Pack%20Guide%20for%20Operations%20Manager%202007,%20published%20October%202010).

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. You bear the risk of using it.

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.

© 2010 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Hyper-V, MS-DOS, SharePoint, Windows, and Windows Server are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Contents

[DPM 2010 Management Pack Guide 5](#_Toc274267834)

[Document Version 5](#_Toc274267835)

[Introduction to the System Center Data Protection Manager 2010 Management Pack 5](#_Toc274267836)

[Downloading the Latest Management Pack and Documentation 5](#_Toc274267837)

[To import a management pack 5](#_Toc274267838)

[Security Considerations 6](#_Toc274267839)

[What's New 6](#_Toc274267840)

[Supported Configurations 7](#_Toc274267841)

[Getting Started 8](#_Toc274267842)

[In This Section 8](#_Toc274267843)

[How to Import the System Center Data Protection 2010 Management Pack 8](#_Toc274267844)

[For ticketing environments 9](#_Toc274267845)

[For non-ticketing environments 9](#_Toc274267846)

[For scaled up environments 10](#_Toc274267847)

[See Also 11](#_Toc274267848)

[Create a New Management Pack for Customizations 11](#_Toc274267849)

[See Also 12](#_Toc274267850)

[Customizing Your Monitors and Rules 12](#_Toc274267851)

[To modify a monitor or rule 13](#_Toc274267852)

[See Also 13](#_Toc274267853)

[Understanding Management Pack Operations 13](#_Toc274267854)

[Management Pack Monitoring Capabilities 14](#_Toc274267855)

[State Monitoring Definitions 15](#_Toc274267856)

[Resolving Alerts Manually 15](#_Toc274267857)

[See Also 15](#_Toc274267858)

[Objects the Management Pack Discovers 15](#_Toc274267859)

[How Health Rolls Up 17](#_Toc274267860)

[Key Monitoring Scenarios 17](#_Toc274267861)

[Alert Rule Group 17](#_Toc274267862)

[Server Rule Group 21](#_Toc274267863)

[Service Discovery Rule Group 22](#_Toc274267864)

[Troubleshooting 22](#_Toc274267865)

# DPM 2010 Management Pack Guide

The System Center Data Protection Manager (DPM) 2010 Management Pack Guide for Operations Manager 2007 explains how to use the DPM Management Pack to monitor the state of data protection and recovery for DPM servers and the computers that they protect, and to monitor key health and performance indicators on DPM servers.

This guide provides an overview of the DPM Management Pack, instructions for deploying the management pack in an existing System Center Operations Manager 2007 R2 environment, and a technical reference to the computer attributes, computer groups, notification groups, and rules that define the behavior of the DPM Management Pack.

## Document Version

This guide is based on the System Center Data Protection Manager 2010 Management Pack.

Revision History

|  |  |
| --- | --- |
| Release Date | Changes |
| October 2010 | Original release of this guide |

# Introduction to the System Center Data Protection Manager 2010 Management Pack

The System Center Data Protection Manager (DPM) 2010 Management Pack Guide explains how to use the DPM 2010 Management Pack to monitor the state of data protection and recovery for DPM servers and the computers that they protect, and to monitor key health and performance indicators on DPM servers.

## Downloading the Latest Management Pack and Documentation

You can find the System Center Data Protection Manager 2010 Management Pack in the [System Center Operations Manager 2007 Catalog](http://go.microsoft.com/fwlink/?LinkId=82105) (http://go.microsoft.com/fwlink/?LinkId=82105).

## To import a management pack

1. Log on to the computer by using an account that is a member of the Operations Manager Administrator's role for the Operations Manager 2007 R2 management group.

2. In the Operations console, click Administration.

Note

When you run the Operations console on a computer that is not a management server, the Connect To Server dialog box opens. In the Server name text box, type the name of the Operations Manager 2007 management server that you want the Operations console to connect to.

3. In the Actions pane, click Import Management Packs, browse to the location of the management pack, and then click Open.

Note

The DPM 2010 Management Pack file name is Microsoft.Windows.SystemCenterDPM2010.mp.

4. In the Import Management Packs dialog box, which displays the management packs that you selected, click Add or Remove to edit the list of management packs to be imported. When you have selected the management packs to import, click Import.

5. After the import process is completed, and the dialog box displays an icon next to each management pack to indicate success or failure of the import, click Close.

## Security Considerations

The Operations Manager agent must run as a local admin account.

# What's New

 The DPM 2010 Management Pack enables you to reduce unnecessary alerts appearing on your console by using service level agreement (SLA)-based alerting and duplicate–error suppression.

Through SLA-based alerting, alerts appear only if a particular job has failed for a certain period.

Through duplicate-error suppression, the management pack suppresses alerts raised as a reaction to a root-cause event. For example, if a DPM protection agent service is unreachable, or a protected computer is not working, and the backup jobs of all data sources are failing, the management pack updates the state of each affected data source without raising a data source-specific alert.

 DPM2010: Recovery point creation failure without alert

 DPM 2010: Recovery point creation failure with precedence

 DPM2010: Replica is inconsistent (3106)

 DPM 2010: Replica inconsistent

 DPM 2010: Synchronization failure without alert

 DPM2010: Synchronization failures (3115)

 If you are using a ticketing system and are using Operations Manager, DPM 2010 Management Pack enables you to use rules instead of the monitors. The rules in the management pack are as follows:

 DPM 2010: Recovery point creation failed, threshold crossed

 DPM 2010: Replica inconsistent with threshold

 DPM 2010: Synchronization failure with threshold

Note

By default, DPM Management Pack enables monitors. If you want to use rules, you must enable them.

 The following alerts are new in this release of the DPM 2010 Management Pack:

 Backup metadata enumeration failed

 Agent ownership required

 Replica allocated and initial replication scheduled

 Share path changed

 Duplicate disks detected

 VHD parent locator fix-up failed

 Virtual machine metadata enumeration failed

 VHD parent locator fix-up canceled

 SharePoint Item Level Catalog failed

 Backup without writer metadata

 Customer Feedback opt-in

 Backup SLA failed

 Hyper-V Recovery Success

 Global DPMDB Database Not Accessible alert notification

 StagingAreaRestore in-progress

 StagingAreaRestore success

 StagingAreaRestore partial success

 StagingAreaRestore failure

 Auto Instance Protection failed

 DPM Online Recovery Point creation failures

 DPM Online Cache volume is missing

 Partial Backup success

 Library devices were disabled

# Supported Configurations

The following table details the supported configurations for the Power Management Pack for Operations Manager 2007.

|  |  |
| --- | --- |
| Configuration | Support |
| Windows Server 2008 R2 | All editions, 32-bit and 64-bit |
| Clustered servers | Supported |
| Agentless monitoring | Not supported |
| Virtual environment | Supported |

# Getting Started

You can install the System Center Data Protection Manager 2010 (DPM) Management Pack from the Administration pane in Microsoft System Center Operations Manager 2007.

Once you have installed the DPM 2010 management pack, you will be able to monitor the status of all the computers protected by DPM 2010.

## In This Section

[How to Import the System Center Data Protection 2010 Management Pack](#za449c74e9e254384a7420fd6814ffb18)

|  |
| --- |
| Describes how to import the DPM 2010 management pack. |

[Create a New Management Pack for Customizations](#zba60d80ac0fa4e8d94022447667e3c64)

|  |
| --- |
| Describes how to create a separate management pack for each sealed management pack that you want to customize. |

# How to Import the System Center Data Protection 2010 Management Pack

For information about how to import a management pack, see [How to Import a Management Pack in Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkId=142351) in the Operations Manager 2007 R2 Operations User's Guide (http://go.microsoft.com/fwlink/?LinkId=142351).

After the DPM 2010 Management Pack is imported, follow these procedures to finish your initial configuration.

1. Create a new management pack.

2. In the new management pack, store overrides and other customizations.

## For ticketing environments

If you are using a ticketing system along with System Center Operations Manager, you must enable rules and disable the monitors so you do not get duplicate alerts. The following table shows you what to enable and what to disable in a ticketing environment.

|  |  |
| --- | --- |
| Alert | Switch |
| DPM 2010: Recovery point creation failed, threshold crossed | Enable |
| DPM 2010: Replica inconsistent with threshold | Enable |
| DPM 2010: Synchronization failure with threshold | Enable |
| DPM 2010: Recovery point creation failure without alert | Enable |
| DPM 2010: Replica inconsistent without alert | Enable |
| DPM 2010: Synchronization failure without alert | Enable |
| DPM 2010: Synchronization failures (3115) | Disable |
| DPM 2010: Recovery point creation failed (3114) | Disable |
| DPM 2010: Replica is inconsistent (3106) | Disable |
| DPM 2010: Synchronization failure with precedence | Disable |
| DPM 2010: Replica inconsistent | Disable |
| DPM 2010: Recovery point creation failure with precedence | Disable |

## For non-ticketing environments

In a non-ticketing environment, if you want every alert in DPM to correspond to a System Center Operations Manager alert, set up your management pack as described in the following table.

|  |  |
| --- | --- |
| Alert | Switch |
| DPM 2010: Synchronization failures (3115) | Enable |
| DPM 2010: Recovery point creation failed (3114) | Enable |
| DPM 2010: Replica is inconsistent (3106) | Enable |

If you want to implement service level agreement (SLA)-based monitoring, set up your management pack as described in the following table.

|  |  |
| --- | --- |
| Alert | Switch |
| DPM 2010: Synchronization failures (3115) | Disable |
| DPM 2010: Recovery point creation failed (3114) | Disable |
| DPM 2010: Replica is inconsistent (3106) | Disable |
| DPM 2010: Synchronization failure with precedence | Enable |
| DPM 2010: Replica inconsistent | Enable |
| DPM 2010: Recovery point creation failure with precedence | Enable |

## For scaled up environments

If you are protecting over 300 data sources on one DPM server, setup your management pack as follows.

On the Operations Manager server

|  |  |
| --- | --- |
| Health Service Handle Count Threshold | 5000 |
| Health Service Private Bytes Threshold | 1GB |
| Monitoring Host Handle Count Threshold | 5000 |
| Monitoring Host Private Bytes Threshold | 1GB |

On the DPM Server

Set the registry key 'HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\HealthService\Parameters\State Queue' to 4096

Set the registry key 'HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\HealthService\Parameters\Management Groups\<MG>\MaximumQueueSizeKb' to 150000

Set the registry key 'HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\HealthService\Parameters\Persistence Version Store Maximum' to 400MB

Tip

Increase it if you see 623 error event when healthservice is reloading config file.

## See Also

[Customizing Your Monitors and Rules](#z70073d753b60411c9b7b870b1af284a3)

[The Entity Health monitor for an Operations Manager 2007 management server displays "Critical" together with a Health Service threshold setting](http://go.microsoft.com/fwlink/?LinkId=201698)

# Create a New Management Pack for Customizations

Most vendor management packs are sealed so that you cannot change any of the original settings in the management pack file. However, you can create customizations, such as overrides or new monitoring objects, and save them to a different management pack. By default, Operations Manager 2007 saves all customizations 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.

Creating a new management pack for storing overrides has the following advantages:

 It simplifies exporting customizations that were created in test environments for your production environment. For example, instead of exporting the Default Management Pack that contains customizations from multiple management packs, you can export just the management pack that contains customizations of a single management pack.

 You can delete the original management pack without first having to delete the Default Management Pack if it does not contain any customizations.

A management pack that contains customizations depends on the original management pack. This dependency requires that you delete the management pack with customizations before you can delete the original management pack. If all your customizations are saved to the Default Management Pack, you must delete the Default Management Pack before you can delete an original management pack.

 It is easier to track and update customizations to individual management packs.

For more information about sealed and unsealed management packs, see [Management Pack Formats](http://go.microsoft.com/fwlink/?LinkId=108355) (http://go.microsoft.com/fwlink/?LinkId=108355). For more information about management pack customizations and the Default Management Pack, see [About Management Packs in Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkId=108356) (http://go.microsoft.com/fwlink/?LinkId=108356).

## See Also

[Customizing Your Monitors and Rules](#z70073d753b60411c9b7b870b1af284a3)

# Customizing Your Monitors and Rules

The DPM 2010 Management Pack provides six SLA-based monitors and three rules. These show up only if a certain job has continuously failed for a certain period. By default, this period is set to 24 hours. You can change the SLA period to suit your needs.

|  |  |
| --- | --- |
| Alert | Description |
| DPM 2010: Synchronization failure with precedence | This monitor suppresses "Recovery point creation failed" alerts if the root cause lies elsewhere. The alert for the root cause is raised separately. |
| DPM2010: Recovery point creation failure without alert | This monitor updates the health state of the data source object if recovery point creation has failed. For example, if a DPM protection agent is unreachable, or a protected computer is not working, and the backup jobs of all data sources are failing, it updates the state of each affected data source without raising a data source-specific alert. |
| DPM 2010: Replica inconsistent | This monitor suppresses "Replica inconsistent" alerts raised when replicated data are inconsistent with their source data if the root cause lies elsewhere. The alert for the root cause is raised separately. |
| DPM 2010: Replica inconsistent without alert | This monitor updates the state of the data source without raising a data source-specific alert if replica is inconsistent. For example, if a protection agent is unreachable, or a protected computer is not working, and the backup jobs of all data sources are failing, it updates the state of each affected data source without raising a data source-specific alert. |
| DPM 2010: Synchronization failure with precedence | This monitor suppresses synchronization failures alerts if the root cause lies elsewhere. The alert for the root cause is raised separately. |
| DPM 2010: Synchronization failure without alert | This monitor updates the health state of the data source object if synchronization failures have occurred. For example, if a protection agent is unreachable, or a protected computer is not working, and the backup jobs of all data sources are failing, it updates the state of each affected data source without raising a data source-specific alert. |
| DPM 2010: Recovery point creation failed, threshold crossed |  |
| DPM 2010: Replica inconsistent with threshold |  |
| DPM 2010: Synchronization failure with threshold |  |

## To modify a monitor or rule

1. Double-click the monitor or rule you want to modify.

2. In the Properties dialog box, on the Configuration tab, click Configure.

3. Note down all the parameter names and values from the Configuration dialog box.

4. Create a new monitor or rule with all the values that exactly match the monitor or rule that you want to change. Parameter 15 has the value 86400, which is one day. You can change this value to change the SLA.

## See Also

[How to Create a Simple Windows Event Unit Monitor in Operations Manager 2007](http://go.microsoft.com/fwlink/?LinkId=196758)

# Understanding Management Pack Operations

By using the DPM Management Pack, an administrator can centrally monitor the state of data protection and recovery for multiple DPM servers and the computers that they protect. The Management Pack also monitors key health and performance indicators on DPM servers.

For DPM servers, the DPM Management Pack monitors the state of DPM database and service health, server performance, and key indicators such as disk availability and configuration changes to volumes protected by DPM. For protected computers, the DPM Management Pack monitors the state of connectivity with DPM, data recovery operations for protected volumes, and replicas and recovery points that are stored on the DPM server.

## Management Pack Monitoring Capabilities

|  |  |
| --- | --- |
| Scenario | Monitored Conditions and Tasks |
| Monitor DPM servers | Are the databases that DPM uses healthy and available for performing protection activities?  Have DPM service failures occurred?  Are CPU usage and memory usage on DPM servers within normal performance ranges?  Can DPM access all disks that have been assigned to the DPM storage pool?  Are permissions for end-user recovery being successfully updated to ensure that only authorized users can retrieve earlier versions of protected data?  Have configuration changes to protected volumes caused potential lapses in protection? |
| Monitor data protection activities on computers protected by DPM | Can DPM connect to DPM protection agents on protected servers to perform protection activities?  Are DPM administrators successfully recovering earlier versions of protected data from the DPM storage pool?  Are initial replicas created successfully when a new protection group is added?  Are all replicas on the DPM server consistent with their data sources on the protected computers?  Are synchronizations and consistency checks for volumes that are protected in DPM failing?  Are scheduled recovery points being created successfully to ensure access to earlier versions of protected data sources? |
| Diagnose and resolve problems on a remote DPM server | Start and stop the DPM service on a remote DPM server.  Ping a DPM server or a protected computer. |

## State Monitoring Definitions

This Management Pack provides state monitoring based on the definitions described in the following table.

Management Pack State Monitoring Definitions

|  |  |
| --- | --- |
| State | Health State |
| Green (Success) | Operations are completing successfully. |
| Green (Informational) | Informational alerts are present that you might want to act on. |
| Yellow (Warning) | Conditions exist that could cause future issues. |
| Red (Critical Error) | A serious problem needs immediate attention. |

## Resolving Alerts Manually

When you resolve an alert manually, the health monitor does not show the updated state automatically. Perform the following steps to update the health monitor.

1. Open the Operations console.

2. Browse to the monitor of the alert you resolved.

3. Click Reset Health State.

## See Also

[Objects the Management Pack Discovers](#zc3ee1acda61248da98615055dc2fe9cf)

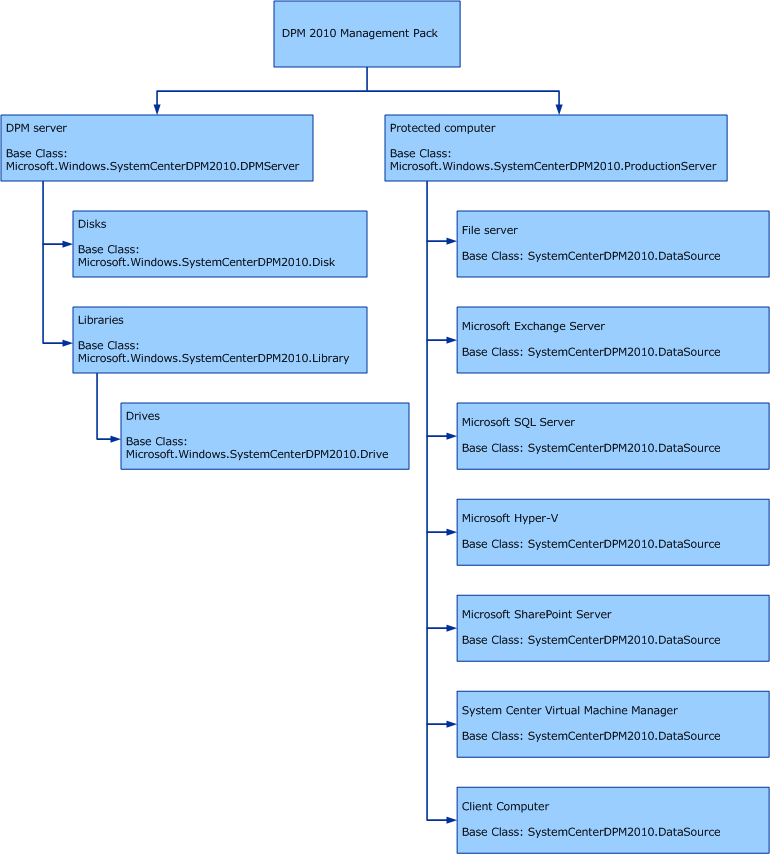
[How Health Rolls Up](#zcbdc2dd66ba544cf8236bee51492faa6)

[Key Monitoring Scenarios](#za7e93bcac1ba4391ab7de16961a9329d)

# Objects the Management Pack Discovers

The DPM 2010 Management Pack discovers the object types described in the following table. Not all of the objects are automatically discovered. Use overrides to discover those that are not discovered automatically.

|  |  |
| --- | --- |
| Category | Object Type |
| DPMServer | DPM server |
| ProductionServer | A computer on which a DPM protection agent is installed |
| Datasources | An entity on the protected computer that DPM protects |
| Disks | Storage space on the DPM server where protected entities are stored |
| Libraries | Tape libraries on a DPM server |
| Drives | Tape drives in a library |



# How Health Rolls Up

The DPM 2010 Management Pack views DPM as a layered structure, where each layer depends on the layers beneath it to be healthy. The top of this structure is the entire DPM environment (known as the Management Group), and the lowest layer includes all of the DPM Agents. When the state of one or more objects in a lower level changes significantly, the state of the objects in the upper levels changes accordingly. This action is called "rolling up health."

A significant change is one where an object changes state from good to bad or vice versa. The upper layers change in response to changes in the lower layer. So if one of the objects in the lower layers changes to a bad state, the objects in the higher layers reflect that change.

In the DPM management pack, the worst condition of a lower object rolls up to the parent instance. Therefore, if a higher-level object has five objects under it and one of them goes bad, the higher-level object shows up as bad.

# Key Monitoring Scenarios

After you import the management pack, wait at least one hour for the management pack to gather data, monitoring data will begin to appear in the Operations Manager 2007 Operations console. In the Monitoring pane, the System Center Data Protection Manager 2010 (DPM) node and child nodes contain views for DPM.

Computer Attributes

The DPM Management Pack collects the following attribute for computers:

 Microsoft System Center Data Protection Manager

DPM Server Groups

The DPM Management Pack includes the following computer group:

 Microsoft System Center Data Protection Manager 2010 Servers

## Alert Rule Group

The rules in the Alert rule group are identical to all the System Center Data Protection Manager (DPM) alerts that might require a user action, so that an administrator can monitor data protection for multiple DPM servers from the Microsoft System Center Operations Manager 2007 Operations console. The Management Pack filters out alerts that do not require user action.

The severity of the alert in DPM determines the severity of the mirrored alert in the Operations Manager Operations console.

 Warning alerts in DPM are warning alerts in Operations Manager.

 Error alerts in DPM are critical errors in Operations Manager.

 Information alerts in DPM are information alerts in Operations Manager.

 An inactive alert in DPM, the alert becomes an inactive alert in Operations Manager and is not displayed.

The product knowledge can be found in the Alert Details of the Operations Manager Operations console. This product provides comprehensive information about each alert, including a summary of the problem, possible causes, resolutions, and additional information sources.

Rules in the Alert Rule Group for DPM

|  |  |  |
| --- | --- | --- |
| Rule | Enabled | Severity |
| Protected Computer |  |  |
| DPM Alert 370: Agent operation failed | Yes | Critical Error |
| DPM Alert 3116: Failed to stop protection | No | Critical Error |
| DPM Alert 3118: Manual replica creation pending | No | Informational |
| DPM Alert 3121: Agent incompatible | Yes | Critical Error |
| DPM Alert 3122: Agent unreachable | Yes | Warning |
| DPM Alert 3123: End user recovery permission update failed | Yes | Warning |
| DPM Alert 3311: Backup to tape failed | Yes | Critical Error |
| DPM Alert 3312: Library catalog build failed | Yes | Warning |
| DPM Server |  |  |
| DPM Alert: DPM server availability | Yes | Critical |
| DPM Alert 369: No agent on cluster node | Yes | Critical Error |
| DPM Alert 24059: Tape encryption certificate expiration | Yes | Warning |
| DPM Alert 3168: Database size threshold reached | Yes | Warning |
| DPM Alert: Memory usage | Yes | Warning |
| DPM Alert: Processor usage | Yes | Warning |
| Data source |  |  |
| DPM Alert 3178: Consolidation of recovery points of replica failed | Yes | Warning |
| DPM Alert 3111: Recovery failure | Yes | Warning |
| DPM Alert 3165: Recovery partial success | Yes | Warning |
| DPM Alert 1689: Partial Backup Success | No | Warning |
| DPM Alert 690: Share Path Changed | No | Warning |
| DPM Alert 3114: Recovery point creation failure | Yes | Critical Error |
| DPM Alert 3114: Recovery point creation failure without alert | No | Warning |
| DPM Alert 3114: Recovery point creation failure with threshold | No | Warning |
| DPM Alert 3163: Replica inconsistent | Yes | Critical Error |
| DPM Alert 3163: Replica inconsistent without alert | No | Warning |
| DPM Alert 3163: Replica inconsistent with threshold | No | Warning |
| DPM Alert 3106: Replica verification in progress | Yes | Critical Error |
| DPM Alert 3115: Synchronization failed | Yes | Warning |
| DPM Alert 3115: Synchronization failed without alert | No | Normal |
| DPM Alert 3115: Synchronization failed with threshold | No | Warning |
| DPM Alert 3161: Volume missing | Yes | Critical Error |
| DPM Alert 3170: Job initialization failure | Yes | Critical Error |
| DPM Alert 3169: Recovery point volume threshold exceeded | Yes | Critical Error |
| DPM Alert 3100: Replica volume threshold exceeded | Yes | Warning |
| DPM Alert 3128: Data corruption detected | Yes | Warning |
| DPM Alert: Data corruption detected during read | Yes | Warning |
| DPM Alert 1556: Staging Area Restore In Progress | No | Warning |
| DPM Alert 1557: Staging Area Restore Complete Success | No | Warning |
| DPM Alert 1558: Staging Area Restore Partial Success | No | Warning |
| Disk |  |  |
| DPM Alert 3120: Disk missing | Yes | Critical Error |
| Library |  |  |
| DPM Alert 3310: Data set copy failed | Yes | Critical Error |
| DPM Alert 3316: Detailed inventory failed | Yes | Critical Error |
| DPM Alert 3305: Free media threshold reached | Yes | Warning |
| DPM Alert 3301: Library not available | Yes | Critical Error |
| DPM Alert 3302: Library not working efficiently | Yes | Warning |
| DPM Alert 3308: Media erase failed | Yes | Critical Error |
| DPM Alert 3309: Media verification failed | Yes | Critical Error |
| DPM Alert 3317: Tape data integrity issues | Yes | Critical Error |
| DPM Alert 3315: Job waiting for tape | Yes | Critical Error |
| Drive |  |  |
| Alert 3303: Drive not functioning | Yes | Critical Error |

## Server Rule Group

The DPM Server rule performs health checks on the System Center Data Protection Manager (DPM) service and monitors database availability. The following table describes the rule in this rule group.

Rules in the Server Rule Group for DPM

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rule | Type | Enabled | Severity | Description |
| DPM Server Not Available | Event | Yes | N/A | This rule generates an event in Operations Manager when the DPM database or service is not available. The DPM Server rule uses this information to generate an alert. As a result of the alert, the state of the DPM server is updated to Red. |

## Service Discovery Rule Group

This rule group contains a single rule, described in the following table, which collects information about managed computers for the System Center Data Protection Manager (DPM) Management Pack.

Rules in the Service Discovery Rule Group for DPM

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rule | Type | Enabled | Severity | Description |
| DPM Server Discovery | Event | Yes | N/A | This rule runs a script that pings all the servers on the network and identified the computers running DPM 2010. |
| DPM Data Discovery | Event | Yes | N/A | This rule runs a script to identify all DPM servers and lists the objects on that server. The objects could be protected computers, data sources, drives, disks, and libraries. |

# Troubleshooting

|  |  |  |
| --- | --- | --- |
| Issues | Cause | Resolution |
| SCOM agent (Health Service) restarts every 15 minutes | The reason for the health service restarting every 15 minutes is the private byte-count and handle-count of the System Center Operations Manager health service crossing the default threshold.  System Center Operations Manager has a monitor that continuously checks for the private byte count and handle count for the health service. The default threshold values are 100 MB private bytes and 2000 handle count. If either parameter crosses the limit, a monitor triggers a recovery action to restart the health service. | Increase the private byte count to 1000 MB and the handle count to 5000. |