

Windows 10 and above Client Management Pack Guide

Microsoft Corporation

Published: March 2022

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

Copyright

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2016 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows Server, and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

Contents

[Introduction to Windows 10 and above Client Management Pack 5](#_Toc439784305)

[Supported Configurations 6](#_Toc439784306)

[Getting Started 6](#_Toc439784307)

[Before You Import the Management Pack 5](#_Toc439784308)

[Files in This Management Pack 6](#_Toc439784309)

[How to Import Windows 10 and above Client Management Pack 7](#_Toc439784310)

[Creating a New Management Pack for Customizations 7](#_Toc439784311)

[Optional Configuration 8](#_Toc439784312)

[Security Considerations 9](#_Toc439784313)

[Low-Privilege Environments 9](#_Toc439784314)

[Computer Groups 10](#_Toc439784315)

[Understanding Management Pack Operations 11](#_Toc439784316)

[Objects That the Management Pack Discovers 11](#_Toc439784317)

[Classes 12](#_Toc439784318)

[Key Monitoring Scenarios 13](#_Toc439784319)

[Putting Monitored Objects into Maintenance Mode 13](#_Toc439784320)

[Appendix 1: Rules and Monitors for Windows 10 and above Client Management Pack 14](#_Toc439784321)

[Rules 14](#_Toc439784322)

[Monitors 21](#_Toc439784323)

[Appendix 2: Reports 2](#_Toc439784324)4

Introduction to Windows 10 and above Client Management Pack

The Windows Client Management Pack provides proactive and reactive monitoring of Windows client computers in your environment. The Windows Client Management Pack monitors client computers that are running Windows 10 and above OS.

The management pack is designed to gather data about client computers, or to monitor specific mission-critical client computers in your organization.

The data gathered by this management pack provides information that can signal an early warning to administrators about issues on client computers that could affect the users of those computers. The reports included in the management pack can help you identify trends or problems with disk utilization, memory health, and various areas of system performance.

Document Version

This guide was written based on the 10.0.0.2 version of the Windows Client Management Pack.

Revision History

| **Release Date** | **Changes** |
| --- | --- |
| May 2017 | In MP Guide, Configuration steps are added for 4 Performance Event Collection Rules which are in Microsoft Windows Client Win10 Aggregate MP |
| January 2016 | Original release of this guide |
| March 2022 | * Windows 10 and above Aggregate MP Fails to Process Root Cause Events issue has been fixed. * The MP has been verified for Windows 10 and above operating systems and branded as version agnostic. |

Changes in Version 10.0.0.2

* Windows 10 and above Aggregate MP Fails to Process Root Cause Events issue has been fixed.
* The MP has been verified for Windows 10 and above operating systems and branded as version agnostic.

Getting the Latest Management Pack and Documentation

You can find the Windows Client Management Pack from [Download Center](https://www.microsoft.com/en-us/download/details.aspx?id=51189)

Supported Configurations

Windows 10 and above Client Management Pack supports monitoring computers that are running Windows 10 and above operating system. System Center Operations Manager 2016 or higher is supported.

Getting Started

This section describes the actions you should take before you import the management pack, any steps you should take after you import the management pack, and information about customizations.

Before You Import the Management Pack

Two types of client monitoring are available in this management pack:

 Aggregate client monitoring for gathering health information on the selected representative clients, and aggregating information for reports that display the trends

 Monitoring of mission-critical business clients

Note

Agentless monitoring is not supported.

Before you import the Windows Client Management Pack, perform the following actions:

 Ensure that Operations Manager 2016 or higher is installed, and then install the agent on every client that you want to monitor.

Files in This Management Pack

To monitor computers that are running a Windows client operating system, you must first download Windows Client Operating System Management Pack from [Download Center](https://www.microsoft.com/en-us/download/details.aspx?id=51189)

The download package includes the following files:

 Microsoft.Windows.Client.Win10.mp

 Microsoft.Windows.Client.Win10.Aggregate.mp

 Microsoft.Windows.Client.Win10.Monitoring.mp

 Microsoft.Windows.Client.Win10.BusinessCritical.xml

 Microsoft.Windows.Client.Library.mp

 EULA.rtf

As a best practice, we recommend that you do not import management pack files that you do not plan to use.

How to Import Windows 10 and above Client Management Pack

Importing Windows 10 and above Client Management Pack

Before importing Windows 10 and above Client Operating System Management Pack, ensure that all dependent libraries are imported, and then import the appropriate client management packs. You can import all of the necessary client management packs at one time.

For information about importing management packs, see [How to Import an Operations Manager Management Pack](http://go.microsoft.com/fwlink/?LinkId=717831) topic (http://go.microsoft.com/fwlink/?LinkId=717831) in Operations Manager Help.

Aggregate Client monitoring gathers health information from Windows 10 and above Client that have a client operating system management pack installed. This type of monitoring provides trending data for representative computers that you select for your purpose and can be used to create reports that display trend information. If you are using this type of client monitoring, no additional setup or configuration is necessary.

If you want to use Business Critical Client monitoring, you must add the computers that are designated as mission-critical to the Business-Critical Client computer group. This group has several overrides that are targeted at the group members. These overrides enable individual monitoring and alerting so that these computers can be monitored in much the same way that a server is monitored. Like server monitoring, each client with this type of monitoring has individual monitors and alerts that an administrator can use to maintain a constant state of operational functionality.

For more information about Aggregate Client monitoring and Business Critical client monitoring, see [Understanding Management Pack Operations](#z545c87e4310f48bfb13d1769fcd57478) section of this guide.

Creating 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. As a best practice, you should instead create a separate management pack for each sealed management pack that you want to customize.

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

 It simplifies the process of exporting customizations that were created in your test and preproduction environments to your production environment. For example, instead of exporting a 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.

 It allows you to delete the original management pack without first having to delete the default management pack. A management pack that contains customizations is dependent on the original management pack. This dependency requires you to delete the management pack with customizations before you can delete the original management pack. If you customized multiple management packs and saved the customizations in the default management pack, then you will lose the customizations for all your management packs.

 It simplifies the process of tracking and updating customizations to individual management packs.

For more information about sealed and unsealed management packs, see [Sealed Management Pack Files](https://technet.microsoft.com/en-US/library/hh457596.aspx) (https://technet.microsoft.com/en-US/library/hh457596.aspx). For more information about management pack customizations and the default management pack, see [Selecting a Management Pack File](https://technet.microsoft.com/en-US/library/hh457560.aspx) (https://technet.microsoft.com/en-US/library/hh457560.aspx).

Optional Configuration

Business Critical monitoring raises aggregated alerts when there is a substantial week-over-week increase in the number of problems detected. You can change the alerting levels for the management pack by overriding the alert rules. For more information and for instructions about how to use overrides, see [How to Override a Rule or Monitor](https://technet.microsoft.com/en-us/library/hh212869.aspx) (https://technet.microsoft.com/en-us/library/hh212869.aspx).

The management pack does not raise alerts for minor degradations in the health of individual computers. To examine the health of individual computers, use the computer’s health explorer.

The reports use aggregations in the reporting server to optimize the reports rendering. For descriptions of the reports contained in this management pack, see [Appendix: Reports](#zf9cb783ab07f48b7a114d562442cbb2f).

In the Windows 10 and above management pack, the items in the following list are disabled by default. You can enable the items for an individual Windows 10 and above computer by adding the computer to All Business Critical Windows 10 and above Client group.

 Performance data collection

 Event collection

 Alerts generated by rules

 Alerts generated by monitors

Security Considerations

If you operate in a low-privilege computing environment, you might have to modify the level of permissions that are assigned to the accounts you use to run management pack rules, monitors, discoveries, recoveries, and diagnostic tasks. These accounts must have minimum permissions for management pack components in order to run properly.

Low-Privilege Environments

Low-privilege Environments and the Agent Action Account

You can use a low-privilege account for the agent action account, although a number of rules and monitors require elevated privileges.

Discoveries and Monitors Configured to Use the Privileged Monitoring Account Run As Profile

The following table lists the object discoveries and monitors that are configured by default to use the Privileged Monitoring Account Run As profile, which defaults to Local System and does not require association with any Run As account or target computer. As a result, no user intervention is required for these object discoveries and monitors that must use a high-privilege account.

Note

You can change the default action account by changing the agent action account associated with Privileged Monitoring Account Run As profile.

If your requirements stipulate that only a low-privilege account should be used in your environment, use overrides to disable the monitor and object discoveries for the appropriate operating systems listed in the table.

For more information and for instructions about how to use overrides, see [How to Override a Rule or Monitor](https://technet.microsoft.com/en-us/library/hh212869.aspx) (https://technet.microsoft.com/en-us/library/hh212869.aspx).

| **Operating System and Monitor Type** | **Discovery or Monitor** |
| --- | --- |
| Windows 10 and above | Discover Windows Physical Disks |
| Windows 10 and above | Discover Windows Logical Disks |
| Windows 10 and above | Logical Disk Availability Health |
| Windows 10 and above | Computer Browser Service Health |
| Windows 10 and above Aggregate Client monitoring | Discover Windows Physical Disk |
| Windows 10 and above Aggregate Client monitoring | Discover Windows Computer |
| Windows 10 and above Aggregate Client monitoring | Discover Operating System |
| Windows 10 and above Aggregate Client monitoring | Discover Windows Logical Disk System Drive |
| Windows 10 and above Aggregate Client monitoring | Discover Windows Logical Disk |
| Windows 10 and above Aggregate Client monitoring | Discover Windows Physical DIMM Disk |
| Windows 10 and above Aggregate Client monitoring | Discover Windows Physical Disk |
| Windows 10 and above Aggregate Client monitoring | Rules that access the event log |
| Windows 10 and above Aggregate Client monitoring | All unit monitors |

Using Roles

In order to use Aggregate Client monitoring to monitor Windows 10 and above Clients in your environment, you must be assigned the Operator role in the Operations Manager. You must be assigned the Administrator role in the Operations Manager in order to use Business Critical Client monitoring. For more information about the types of client monitoring available in the Operations Manager, see [Understanding Management Pack Operations](#z545c87e4310f48bfb13d1769fcd57478) section of this guide.

Computer Groups

When imported, each individual client management pack creates a corresponding computer group. For example, when you install Windows 10 and above Operating Systems Management Pack, a Windows 10 and above computer group is created.

The following groups are defined in this management pack:

 All Business Critical Windows 10 and above Client

Windows 10 and above Client Computer Group

Note

Computer groups are populated by discovery rules that are located in each client management pack. If you receive an error message when you try to view the properties of a computer group, ensure that you installed the management pack that contains the discovery rules for the computer group.

The following table lists the management packs that contains the discovery rules for each computer group.

| **Computer group** | **Management pack** |
| --- | --- |
| All Business Critical Windows 10 and above Client | Microsoft.Windows.Client.Win10.mp |
| Windows 10 and above Client Computer Group | Microsoft.Windows.Client.Win10.mp |

Understanding Management Pack Operations

Two types of client monitoring are available in this management pack: Aggregate Client monitoring and Business Critical Client monitoring. You can implement both types of client monitoring in your network environment.

Aggregate Client monitoring is supported for Windows 10 and above operating systems. Aggregate Client monitoring gathers health information for representative computers that you select, and uses the data to provide trending information in the reports. For example, an administrator might select computers that have a specific hardware configuration in order to receive performance trending data on one component of the hardware configuration. The information gathered through Aggregate Client monitoring is stored in the Operations Manager database and can be used to create reports that display trend information.

Business Critical Client monitoring is the most extensive monitoring available for Windows clients. This type of monitoring gathers health information about designated individual client computers. Like server monitoring, each client with this type of monitoring has individual monitors and alerts that an administrator can use to maintain a constant state of operational functionality. Use this type of monitoring for your mission-critical client computers. Mission-critical client computers are the client computers in your organization that must be available at all times, and must have a reliable and constant connection to the Operations Manager management server.

Objects That the Management Pack Discovers

By default, Windows Client Operating System Management Pack discovers the following objects:

 Operating systems

 Logical disks

 Network adapter

The following objects are not discovered by default, but they can be discovered if the object discoveries are enabled by using overrides.

 Physical disks

 Processor

 Disk partitions

Note

For more information about using overrides, see [How to Override a Rule or Monitor](https://technet.microsoft.com/en-us/library/hh212869.aspx) (https://technet.microsoft.com/en-us/library/hh212869.aspx).

Classes

The following tables describe the classes defined in this management pack.

**Windows 10 and above Client**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Base Class** | **Description** | **ID** |
| All Business Critical Windows 10 and above Client | Microsoft.SystemCenter.ComputerGroup | All Business Critical Windows 10 and above Client OS Computer Systems (alerting enabled) | Microsoft.Windows.Client.Win10.BusinessCriticalClient.ComputerGroup |
| Windows 10 and above Client Computer | Microsoft.Windows.Client.Computer | All instances of computers running Windows 10 and above Client operating system. | Microsoft.Windows.Client.Win10.Computer |
| Windows 10 and above Client Computer Group | Microsoft.SystemCenter.ComputerGroup | A group containing all computers that are running a Windows 10 and above Client version of the Windows operating system. | Microsoft.Windows.Client.Win10.ComputerGroup |
| Windows 10 and above Client Disk Partition | Disk Partition (Client) | All instances of a disk partition on a Windows 10 and above Client operating system. | Microsoft.Windows.Client.Win10.DiskPartition |
| Windows 10 and above Client Logical Disk | Logical Disk (Client) | All instances of a logical disk on a Windows 10 and above Client operating system. | Microsoft.Windows.Client.Win10.LogicalDisk |
| Windows 10 and above Client Network Adapter | Network Adapter (Client) | All instances of a network adapter on a Windows 10 and above Client operating system. | Microsoft.Windows.Client.Win10.NetworkAdapter |
| Windows 10 and above Client Operating System | Microsoft.Windows.Client.OperatingSystem | All instances of Windows 10 and above Client operating system. | Microsoft.Windows.Client.Win10.OperatingSystem |
| Windows 10 and above Client Physical Disk | Physical Disk (Client) | All instances of a physical disk on a Windows 10 and above Client operating system. | Microsoft.Windows.Client.Win10.PhysicalDisk |
| Windows 10 and above Client Processor | Processor (Client) | All instances of a processor on a Windows 10 and above Client operating system. | Microsoft.Windows.Client.Win10.Processor |

**Windows 10 and above Client Aggregate**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Base Class** | **Description** | **ID** |
| Windows 10 and above Client Aggregate Computer | Windows 10 and above Client Computer | A computer running the Microsoft Windows 10 and above operating system | Microsoft.Windows.Client.Win10.Aggregate.Computer |
| Windows 10 and above Client Aggregate Logical Disk | Windows 10 and above Client Logical Disk | A logical volume in a computer running the Microsoft Windows 10 and above operating system | Microsoft.Windows.Client.Win10.Aggregate.LogicalDisk |
| Windows 10 and above Client Aggregate Physical DIMM | Microsoft.Windows.LogicalDevice | A memory DIMM in a computer running the Microsoft Windows 10 and above operating system | Microsoft.Windows.Client.Win10.Aggregate.PhysicalDIMM |
| Windows 10 and above Client Aggregate Physical Disk | Windows 10 and above Client Physical Disk | A hard drive in a computer running the Microsoft Windows 10 and above operating system | Microsoft.Windows.Client.Win10.Aggregate.PhysicalDisk |

Key Monitoring Scenarios

Client Monitoring

The client operating system management packs are designed to monitor issues that occur on clients in your network as a whole, and also on individual mission-critical clients.

Aggregate Client Monitoring

Aggregate Client monitoring gathers and stores information about client computers. It does not monitor individual computers, nor does it generate alerts.

The information gathered through Aggregate Client monitoring is stored in the Operations Manager database. The information includes basic inventory information, such as operating system version, applied service pack, installed updates, and installed hardware.

Business Critical Client Monitoring

Business Critical monitoring is the most comprehensive monitoring available for Windows clients. This is the only type of monitoring that monitors client computers individually, and that can generate alerts.

To implement Business Critical monitoring on a client computer, you must have an agent installed on that client computer, and the correct client management pack imported on the management server. Then, you must manually move the client computer to Business Critical Client computer group. This group is the target of an override that enables all the monitors and alerts that are included in the client operating system management pack, and that are required to closely monitor the health of the client.

Putting Monitored Objects into Maintenance Mode

When a monitored object, such as a computer or distributed application, goes offline for maintenance, the Operations Manager detects that no agent heartbeat is received and, as a result, might generate numerous alerts and notifications. To prevent alerts and notifications, put the monitored object into maintenance mode. In maintenance mode, alerts, notifications, rules, monitors, automatic responses, state changes, and new alerts are suppressed at the agent.

For general instructions on putting a monitored object into maintenance mode, see [Operations Manager Maintenance Mode](https://support.microsoft.com/en-us/kb/2704170) (https://support.microsoft.com/en-us/kb/2704170).

Appendix 1: Rules and Monitors for Windows 10 and above and above Client Management Pack

Rules

**Windows 10 and above Client Monitoring**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Target** | **Category** | **Enabled** |
| Application Incompatibility Rule | Windows 10 and above Client Computer | EventCollection | False |
| Disk Corruption Failed Rule | Windows 10 and above Client Computer | EventCollection | False |
| Disk Corruption File Skipped Rule | Windows 10 and above Client Computer | EventCollection | False |
| Disk Corruption Repair Failed Rule | Windows 10 and above Client Computer | EventCollection | False |
| Disk Corruption Repair Succeeded Need Reboot Rule | Windows 10 and above Client Computer | EventCollection | False |
| Disk Corruption Repair Succeeded No Reboot Rule | Windows 10 and above Client Computer | EventCollection | False |
| Disk Failure Rule | Windows 10 and above Client Computer | EventCollection | False |
| Memory Exhaustion Rule | Windows 10 and above Client Computer | EventCollection | False |
| Memory Failure Detected Rule | Windows 10 and above Client Computer | EventCollection | False |
| Memory Failure Test Cancelled Rule | Windows 10 and above Client Computer | EventCollection | False |
| Memory Failure Test Failed Rule | Windows 10 and above Client Computer | EventCollection | False |
| Logical Disk Average Disk Queue Length | Windows 10 and above Client Logical Disk | PerformanceCollection | False |
| Logical Disk Average Disk Second Per Read | Windows 10 and above Client Logical Disk | PerformanceCollection | False |
| Logical Disk Average Disk Second Per Transfer | Windows 10 and above Client Logical Disk | PerformanceCollection | False |
| Logical Disk Average Disk Second Per Write | Windows 10 and above Client Logical Disk | PerformanceCollection | False |
| Logical Disk Current Disk Queue Length | Windows 10 and above Client Logical Disk | PerformanceCollection | False |
| Logical Disk Bytes Per Second | Windows 10 and above Client Logical Disk | PerformanceCollection | False |
| Logical Disk Reads Second | Windows 10 and above Client Logical Disk | PerformanceCollection | False |
| Logical Disk Writes Per Second | Windows 10 and above Client Logical Disk | PerformanceCollection | False |
| Logical Disk Free Megabytes | Windows 10 and above Client Logical Disk | PerformanceCollection | False |
| % Logical Disk Free Space | Windows 10 and above Client Logical Disk | PerformanceCollection | False |
| Bytes Received Per Sec Collection Mission Critical | Windows 10 and above Client Network Adapter | PerformanceCollection | False |
| Bytes Sent Per Sec Collection Mission Critical | Windows 10 and above Client Network Adapter | PerformanceCollection | False |
| Bytes Total Per Sec Collection MissionCritical | Windows 10 and above Client Network Adapter | PerformanceCollection | False |
| Network Adapter Disconnected | Windows 10 and above Client Network Adapter | EventCollection | False |
| Checking File System Occurred on Startup | Windows 10 and above Client Operating System | EventCollection | False |
| Collection Rule for Windows Clean Restart Events | Windows 10 and above Client Operating System | EventCollection | False |
| Collection Rule for Windows Dirty Shutdown Events | Windows 10 and above Client Operating System | EventCollection | False |
| The Event Log File is Full | Windows 10 and above Client Operating System | EventCollection | False |
| Event Log Full Alert Mission Critical | Windows 10 and above Client Operating System | EventCollection | False |
| A Duplicate IP Address has been Detected on the Network | Windows 10 and above Client Operating System | EventCollection | False |
| IP Address Conflict Alert Mission Critical | Windows 10 and above Client Operating System | EventCollection | False |
| LDM - Can't Read Disk | Windows 10 and above Client Operating System | EventCollection | False |
| LDM Cannot Read Disk Alert Mission Critical | Windows 10 and above Client Operating System | EventCollection | False |
| Memory Available Megabytes | Windows 10 and above Client Operating System | PerformanceCollection | False |
| Memory Page Reads per Second | Windows 10 and above Client Operating System | PerformanceCollection | False |
| Memory Pages per Second | Windows 10 and above Client Operating System | PerformanceCollection | False |
| Memory Page Writes per Second | Windows 10 and above Client Operating System | PerformanceCollection | False |
| Memory % Committed Bytes in Use | Windows 10 and above Client Operating System | PerformanceCollection | False |
| Memory Pool Non-paged Bytes | Windows 10 and above Client Operating System | PerformanceCollection | False |
| Memory Pool Paged Bytes | Windows 10 and above Client Operating System | PerformanceCollection | False |
| NTFS - Delayed Write Lost | Windows 10 and above Client Operating System | EventCollection | False |
| NTFS Delayed Write Lost Alert Mission Critical | Windows 10 and above Client Operating System | EventCollection | False |
| NTFS - File System Corrupt | Windows 10 and above Client Operating System | EventCollection | False |
| NTFS File System Corrupt Alert Mission Critical | Windows 10 and above Client Operating System | EventCollection | False |
| NTFS Quota Threshold Limit Reached Collection | Windows 10 and above Client Operating System | EventCollection | False |
| NTFS Quota Threshold Reached Collection | Windows 10 and above Client Operating System | EventCollection | False |
| Page File Percentage Use | Windows 10 and above Client Operating System | PerformanceCollection | False |
| Performance Counter Data Request TimeOut Alert | Windows 10 and above Client Operating System | EventCollection | False |
| Performance registry corruption | Windows 10 and above Client Operating System | EventCollection | False |
| Performance Registry Corruption Alert | Windows 10 and above Client Operating System | EventCollection | False |
| Collection Rule for Windows Restart Events (restarted from bugcheck) | Windows 10 and above Client Operating System | EventCollection | False |
| Collection Rule for Windows Restarted Events | Windows 10 and above Client Operating System | EventCollection | False |
| The Service has Entered into an Unpredictable State | Windows 10 and above Client Operating System | EventCollection | False |
| Service Entered Unpredictable State Alert | Windows 10 and above Client Operating System | EventCollection | False |
| The Service is Misconfigured | Windows 10 and above Client Operating System | EventCollection | False |
| Service Misconfigured Alert | Windows 10 and above Client Operating System | EventCollection | False |
| The Service or Driver Failed to Start | Windows 10 and above Client Operating System | EventCollection | False |
| Service Or Driver Failed To Start Alert | Windows 10 and above Client Operating System | EventCollection | False |
| Service Or Driver Failed To Start Collection | Windows 10 and above Client Operating System | EventCollection | False |
| The Service Terminated Unexpectedly | Windows 10 and above Client Operating System | EventCollection | False |
| Service Terminated Unexpectedly Alert Mission Critical | Windows 10 and above Client Operating System | EventCollection | False |
| Service Terminated Unexpectedly Collection | Windows 10 and above Client Operating System | EventCollection | False |
| Share Configuration Invalid Alert MissionCritical | Windows 10 and above Client Operating System | EventCollection | False |
| Share Configuration Invalid Collection | Windows 10 and above Client Operating System | EventCollection | False |
| A Software Update Installation Failed | Windows 10 and above Client Operating System | EventCollection | False |
| Software Update Installation Failed Alert MissionCritical | Windows 10 and above Client Operating System | EventCollection | False |
| Software Update Installation Failed Collection | Windows 10 and above Client Operating System | EventCollection | False |
| Collection Rule for Software Updates Installation Events | Windows 10 and above Client Operating System | EventCollection | False |
| Collection Rule for Software Updates Scheduled Installation Events | Windows 10 and above Client Operating System | EventCollection | False |
| System Context Switches per Second | Windows 10 and above Client Operating System | PerformanceCollection | False |
| System Processor Queue Length | Windows 10 and above Client Operating System | PerformanceCollection | False |
| Total Processor % DPC Time | Windows 10 and above Client Operating System | PerformanceCollection | False |
| Total Processor % Interrupt Time | Windows 10 and above Client Operating System | PerformanceCollection | False |
| Processor % Processor Time Total | Windows 10 and above Client Operating System | PerformanceCollection | False |
| Physical Disk Average Disk Queue Length | Windows 10 and above Client Physical Disk | PerformanceCollection | False |
| Physical Disk Average Disk Seconds per Read | Windows 10 and above Client Physical Disk | PerformanceCollection | False |
| Physical Disk Average Disk Seconds per Transfer | Windows 10 and above Client Physical Disk | PerformanceCollection | False |
| Physical Disk Average Disk Seconds per Write | Windows 10 and above Client Physical Disk | PerformanceCollection | False |
| Physical Disk Current Disk Queue Length | Windows 10 and above Client Physical Disk | PerformanceCollection | False |
| Physical Disk Bytes per Second | Windows 10 and above Client Physical Disk | PerformanceCollection | False |
| Physical Disk Reads per Second | Windows 10 and above Client Physical Disk | PerformanceCollection | False |
| Physical Disk Writes per Second | Windows 10 and above Client Physical Disk | PerformanceCollection | False |
| Processor % DPC Time | Windows 10 and above Client Processor | PerformanceCollection | False |
| Processor % Interrupt Time | Windows 10 and above Client Processor | PerformanceCollection | False |
| Processor % Processor Time | Windows 10 and above Client Processor | PerformanceCollection | False |

**Windows 10 and above Client Aggregate**

**Note:** Below 4 performance collection rules are required to configure few steps in SCOM console to avoid module warning events in Operations Manager Event log.

* Windows 10 and above Aggregate Disk Trends Computer
* Windows 10 and above Aggregate Disk Trends Disk
* Windows 10 and above Aggregate Memory Trends RAM
* Windows 10 and above Aggregate Shell Performance Trends

The data source module for these four rules is configured to use the Data Warehouse Action. However, the rules target the Microsoft System Center Data Warehouse class, which isn’t associated in the Run As profile by default. The result is the workflows run with Default Action Account credentials, and that account doesn’t typically have a login for the DW database. Hence below steps to be configure in SCOM console for these 4 rules to work as expected.

1. Open the Operations console, and then click Administration.

2. In the Administrator pane, click Run As Configuration and then expand, click on Profiles

3. Open the **Data Warehouse Account profile**

4. Click the **Run As Accounts** tab.

5. Click Add

6. In the **Run As account** box, select **Data Warehouse Action Account**

7. Click **A selected class, group, or object**.

8. Click Select > Class.

9. Enter “**Microsoft System Center Data Warehouse**” (without quotes) in the “Filter by” box and click Search.

10. Select **Microsoft System Center Data Warehouse** and click OK twice.

11. Click Save.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Target** | **Category** | **Enabled** |
| Windows 10 and above Aggregate Boot Application Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Boot Client Performance Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Boot Device Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Boot Driver Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Boot Policy Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Boot Service Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate COFIRE Fixed NR Collection | Windows 10 and above Client Aggregate Physical Disk | EventCollection | True |
| Windows 10 and above Aggregate COFIRE Fixed R Collection | Windows 10 and above Client Aggregate Physical Disk | EventCollection | True |
| Windows 10 and above Aggregate COFIRE Not Fixed Collection | Windows 10 and above Client Aggregate Physical Disk | EventCollection | True |
| Windows 10 and above Aggregate Collect Client Performance Data | Microsoft.SystemCenter.HealthService | EventCollection | True |
| Windows 10 and above Aggregate Collect Client Performance Root Cause Data | Microsoft.SystemCenter.HealthService | EventCollection | True |
| Windows 10 and above Aggregate Collect Disk Failure Data | Microsoft.SystemCenter.HealthService | EventCollection | True |
| Windows 10 and above Aggregate Collect Memory Failure Data | Microsoft.SystemCenter.HealthService | EventCollection | True |
| Windows 10 and above Aggregate Collect Memory Health Data | Microsoft.SystemCenter.HealthService | EventCollection | True |
| Windows 10 and above Aggregate Collect Shell Performance Data | Microsoft.SystemCenter.HealthService | EventCollection | True |
| Windows 10 and above Aggregate Collect Shell Performance Root Cause Data | Microsoft.SystemCenter.HealthService | EventCollection | True |
| Windows 10 and above Aggregate DFD Collection | Windows 10 and above Client Aggregate Physical Disk | EventCollection | True |
| Windows 10 and above Aggregate Page Corruption Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate RADAR Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Resume Driver Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Resume Hibernate Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Shell Performance Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Shell Performance CPU Root Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Shell Performance Root Disk Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Shell Performance Root Driver Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Shell Performance Root File Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Shell Performance Root Long Driver Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Shell Performance Root Memory Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Shutdown Application Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Shutdown Client Performance Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Shutdown Driver Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Shutdown Service Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Standby Application Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Standby Client Perf Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Standby Driver Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Standby Flush File Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Standby Hibernate Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Standby Service Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate WMD Memory Failed Collection | Windows 10 and above Client Aggregate Computer | EventCollection | True |
| Windows 10 and above Aggregate Disk Trends Computer | Microsoft System Center Data Warehouse | EventCollection | True |
| Windows 10 and above Aggregate Disk Trends Disk | Microsoft System Center Data Warehouse | EventCollection | True |
| Windows 10 and above Aggregate Memory Trends RAM | Microsoft System Center Data Warehouse | EventCollection | True |
| Windows 10 and above Aggregate Shell Performance Trends | Microsoft System Center Data Warehouse | EventCollection | True |

Monitors

**Windows 10 and above Client Monitoring**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Target** | **Category** | **Enabled** |
| Monitor for application incompatibility operational conditions | Windows 10 and above Client Computer | StateCollection | True |
| Monitor for disk corruption failed operational conditions | Windows 10 and above Client Computer | StateCollection | True |
| Monitor for disk corruption file skipped operational conditions | Windows 10 and above Client Computer | StateCollection | True |
| Monitor for disk corruption repair failed operational conditions | Windows 10 and above Client Computer | StateCollection | True |
| Monitor for disk corruption file repair succeeded reboot required operational conditions | Windows 10 and above Client Computer | StateCollection | True |
| Monitor for disk corruption file repair succeeded no reboot required operational conditions | Windows 10 and above Client Computer | StateCollection | True |
| Monitor for disk failure operational conditions. | Windows 10 and above Client Computer | StateCollection | True |
| Monitor for memory exhaustion failure operational conditions | Windows 10 and above Client Computer | StateCollection | True |
| Monitor for memory failure operational conditions | Windows 10 and above Client Computer | StateCollection | True |
| Monitor for memory failure test canceled operational conditions | Windows 10 and above Client Computer | StateCollection | True |
| Monitor for memory failure test failed operational conditions | Windows 10 and above Client Computer | StateCollection | True |
| Logical Disk Availability | Windows 10 and above Client Logical Disk | StateCollection | True |
| Logical Disk - Average Disk Seconds Per Read | Windows 10 and above Client Logical Disk | PerformanceHealth | True |
| Logical Disk - Average Disk Seconds Per Transfer | Windows 10 and above Client Logical Disk | PerformanceHealth | True |
| Logical Disk - Average Disk Seconds Per Write | Windows 10 and above Client Logical Disk | PerformanceHealth | True |
| Logical Disk Free Space | Windows 10 and above Client Logical Disk | PerformanceHealth | True |
| Network Adapter Connection Health | Windows 10 and above Client Network Adapter | StateCollection | False |
| Computer Browser Service Health | Windows 10 and above Client Operating System | StateCollection | True |
| DHCP Client Service Health | Windows 10 and above Client Operating System | StateCollection | True |
| DNS Client Service Health | Windows 10 and above Client Operating System | StateCollection | True |
| Windows Event Log Service Health | Windows 10 and above Client Operating System | StateCollection | True |
| Available Megabytes of Memory | Windows 10 and above Client Operating System | PerformanceHealth | True |
| Percentage of Committed Memory in Use | Windows 10 and above Client Operating System | PerformanceHealth | True |
| Plug and Play Service Health | Windows 10 and above Client Operating System | StateCollection | True |
| RPC Service Health | Windows 10 and above Client Operating System | StateCollection | True |
| Server Service Configuration Health | Windows 10 and above Client Operating System | StateCollection | True |
| Server Service Health | Windows 10 and above Client Operating System | StateCollection | True |
| TCP/IP NetBIOS Service Health | Windows 10 and above Client Operating System | StateCollection | True |
| Total CPU Utilization Percentage | Windows 10 and above Client Operating System | PerformanceHealth | True |
| Total DPC Time Percentage | Windows 10 and above Client Operating System | PerformanceHealth | True |
| Total Percentage Interrupt Time | Windows 10 and above Client Operating System | PerformanceHealth | True |
| Workstation Service Health | Windows 10 and above Client Operating System | StateCollection | True |
| Physical Disk - Average Disk Seconds Per Read | Windows 10 and above Client Physical Disk | PerformanceHealth | True |
| Physical Disk - Average Disk Seconds Per Transfer | Windows 10 and above Client Physical Disk | PerformanceHealth | True |
| Physical Disk - Average Disk Seconds Per Write | Windows 10 and above Client Physical Disk | PerformanceHealth | True |
| CPU Utilization Percentage | Windows 10 and above Client Processor | PerformanceHealth | True |
| CPU DPC Time Percentage | Windows 10 and above Client Processor | PerformanceHealth | True |
| CPU Percentage Interrupt Time | Windows 10 and above Client Processor | PerformanceHealth | True |

**Windows 10 and above Client Aggregate**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Target** | **Category** | **Enabled** |
| Aggregate Page Corruption Monitor | Windows 10 and above Client Aggregate Computer | StateCollection | True |
| Aggregate Frequent Memory Exhaustion Monitor | Windows 10 and above Client Aggregate Computer | StateCollection | True |
| Aggregate Intermittent Memory Exhaustion Monitor | Windows 10 and above Client Aggregate Computer | StateCollection | True |
| Aggregate Shell Performance Monitor | Windows 10 and above Client Aggregate Computer | StateCollection | True |
| Aggregate Windows Memory Diagnostics Monitor | Windows 10 and above Client Aggregate Computer | StateCollection | True |
| Aggregate Memory Failure Monitor | Windows 10 and above Client Aggregate Computer | StateCollection | True |
| Aggregate Corrupted File Recovery Server Monitor | Windows 10 and above Client Aggregate Physical Disk | StateCollection | True |
| Aggregate Repaired Corrupted System File Monitor | Windows 10 and above Client Aggregate Physical Disk | StateCollection | True |
| Aggregate Repaired with Reboot Corrupted System File Monitor | Windows 10 and above Client Aggregate Physical Disk | StateCollection | True |
| Aggregate Irreparable Corrupted System File Monitor | Windows 10 and above Client Aggregate Physical Disk | StateCollection | True |
| Aggregate File System Corruption Monitor | Windows 10 and above Client Aggregate Physical Disk | StateCollection | True |

Appendix 2: Reports

The reports that are provided with this management pack can help you understand trends over specified time periods, such as a week or year. Reporting is an optional component of Operations Manager. See the following tables for a list of reports and a description of each report.

Windows 10 and above Client Operating System Aggregate Reports

The following reports consolidate information retrieved from Windows 10 and above Client computers monitored through this management pack.

| **Report** | **Description** | **Additional Information** |
| --- | --- | --- |
| Windows 10 and above Boot Performance | Provides an overview of boot performance issues encountered by the users of Windows 10 and above Clients. It provides in-depth information about the bottleneck resources that caused slowdown in the system boot process, and pinpoints the various applications and services that used up those particular resources. | Overall Performance: This chart trends the average boot time, breaking it down by computer hardware manufacturer. The number of issues found in any particular computer type is normalized to enable you to compare computer types with each other, and make better purchasing decisions. This chart shows information on the top 10 most problematic computer types. These computer types are identified by looking at the computer types that are consistently having the highest failure ratios over the last three months.  Root Causes: This chart displays the root causes that contributed to boot performance degradation. This charts the average number of times a particular root cause was evidenced in a particular week. Since each computer can have multiple root causes behind its degradation, these root causes together will not sum to the number of boot performance issues evidenced in the enterprise. |
| Windows 10 and above Boot Performance: Degraded Component | Provides detailed information on the individual components contributing to slow booting of Windows 10 and above Clients across the enterprise. The average reported time taken only takes into consideration those boots that were considerably slower due to a particular application or service. The report represents only the boot processes that have degraded. |  |
| Windows 10 and above Disk Failure | Provides detailed information about the set of computers that have impending hard-drive failures and other drive corruption information. This includes data from:   Windows 10 and above Disk Failure Diagnostic, which detects impending hard drive crashes.   Windows 10 and above Corrupted File Recovery Diagnostic, which detects and runs self-healing tasks on corrupted system files. When Windows 10 and above cannot heal itself, this information is displayed. |  |
| Windows 10 and above Disk Health | Provides an overview of the health of disks in Windows 10 and above Clients. It also provides information on disk failures to help pinpoint hardware types and types of computers that are evidencing higher rates of failure. |  |
| Windows 10 and above Disk Space Usage | Lists system volumes ordered by their space usage from the previous day. |  |
| Windows 10 and above Memory Exhaustion Analysis | Lists applications contributing to memory exhaustion in the last three months. |  |
| Windows 10 and above Memory Failure | Provides information about the details of the set of computers that have undergone memory hardware failure. This report helps you ensure that these issues have been investigated and appropriately addressed. The set of failures includes:   Failures in the memory hardware detected by Windows Memory Diagnostics.   Corruption in the memory pages that are allocated to applications. Corruption in the memory pages allocated to applications can cause system and application instability, and is indicative of memory hardware failure. |  |
| Windows 10 and above Memory Health | Overview of memory health in Windows 10 and above Clients: out-of-memory scenarios, time trends, type of computers affected, and a list of computers reporting the worst problems. | Memory Exhaustion chart: shows memory exhaustion over time, and identifies the amount of installed RAM. The data is normalized, and you can view it by computer type. Concentration of memory exhaustion chart: shows the number of memory exhaustion incidents and disruption to users due to low memory conditions. The concentration graph shows the number of computers experiencing memory exhaustion during the past week related the amount of installed RAM. You can view the data by the type of computer.  Application Memory Utilization: charts the applications that used up the memory resources, identifies the average commit charge (amount of memory used by the application) of applications during the time the system is experiencing the low memory conditions. Note that this is not the average memorization utilization of a particular application through its execution lifetime, rather, it is the condition of the application during the periods the computer is reporting a low memory condition. |
| Windows 10 and above Memory Sufficiency | Gives a list of the computers that have suffered low memory conditions. It also details the number of exhaustions that each of these computers have had. |  |
| Windows 10 and above Resume Performance | Provides an overview of the resume performance issues encountered by the users of Windows 10 and above Clients. It provides in-depth information on the bottleneck resources that caused slowdown in the system resume, and pinpoints the various applications and services that used up those particular resources. | Overall Performance: this chart trends the average resume time, breaking it down by computer hardware manufacturer. The number of issues found in any particular computer type is normalized to enable you to compare computer types with each other, and make better purchasing decisions. This chart shows information on the top 10 most problematic computer types. These computer types are identified by looking at the computer types that are consistently having the highest failure ratios over the last three months.  Root Causes: this chart displays the root causes that contributed to resume performance degradation. This charts the average number of times a particular root cause was evidenced in a particular week. Since each computer can have multiple root causes behind its degradation, these root causes together will not sum to the number of resume performance issues evidenced in the enterprise. |
| Windows 10 and above Resume Performance: Degraded Component | Gives detailed information on the individual components contributing to slow resuming of Windows 10 and above Clients from standby across the enterprise. The average reported time taken is not over all resume cycles, but only takes into consideration those boots that were considerably slower due to a particular application/service. Therefore, this is not representative of all resume cycles in the enterprise, just those that have degraded. |  |
| Windows 10 and above Shell Computer | Gives detailed information on the individual components contributing to slow Shell Performance of Windows 10 and above Clients across the enterprise. The report features columns for each of the bottleneck resources that cause system performance degradation. For each computer that has performance degradation, the columns indicate the number of times a particular resource contributed to performance degradation on that computer. |  |
| Windows 10 and above Shell Performance | Provides an overview of the shell performance issues encountered by the users of Windows 10 and above Clients. It provides in-depth information on the bottleneck resources that caused the system to perform poorly, and pinpoints the various applications and services that used up those particular resources. | Overall Performance: this chart trends the frequency of shell performance issues over time, breaking it down by computer hardware manufacturer. The number of issues found in any particular computer type is normalized to enable you to compare computer types with each other, and make better purchasing decisions. This chart shows information on the top 10 most problematic computer types. These computer types are identified by looking at the computer types that are consistently having the highest failure ratios over the last three months.  Root Causes: this chart displays the root causes that contributed to system performance degradation. This charts the average number of times a particular root cause was evidenced in a particular week. Since each computer can have multiple root causes behind its degradation, these root causes together will not sum to the number of performance issues evidenced in the enterprise.  Details on Applications and services behind the root causes: these reports detail the various applications and services that contributed to the exhaustion of resources, which caused the system performance to degrade. |
| Windows 10 and above Shutdown Performance | This report provides an overview of the shutdown performance issues encountered by the users of Windows 10 and above Clients. It provides in-depth information on the bottleneck resources that caused slowdown in the system shutdown, and pinpoints the various applications and services that used up those particular resources. | Overall Performance: This chart trends the average shutdown time, breaking it down by computer hardware manufacturer. The number of issues found in any particular computer type is normalized to enable you to compare computer types with each other, and make better purchasing decisions. This chart shows information on the top ten most problematic computer types. These computer types are identified by looking at the computer types that are consistently having the highest failure ratios over the last three months.  Root Causes: this chart displays the root causes that contributed to shutdown performance degradation. This charts the average number of times a particular root cause was evidenced in a particular week. Since each computer can have multiple root causes behind its degradation, these root causes together will not sum to the number of shutdown performance issues evidenced in the enterprise. |
| Windows 10 and above Shutdown Performance: Degraded Component | Gives detailed information on the individual components contributing to slow shutdowns of Windows 10 and above Clients across the enterprise. The average reported time taken is not over all shutdowns, but only takes into consideration those boots that were considerably slower due to a particular application/service. Therefore, this is not representative of all shutdowns in the enterprise, just those that have degraded. |  |
| Windows 10 and above Standby Performance | Provides an overview of performance issues encountered by Windows 10 and above Clients when entering standby. It provides in-depth information on the bottleneck resources that caused slowdown in the system standby sequence, and pinpoints the various applications and services that used up those particular resources. | Overall Performance: this chart trends the average time to switch to standby mode, breaking it down by computer hardware manufacturer. The number of issues found in any particular computer type is normalized to enable you to compare computer types with each other, and make better purchasing decisions. This chart shows information on the top 10 most problematic computer types. These computer types are identified by looking at the computer types that are consistently having the highest failure ratios over the last three months.  Root Causes: this chart displays the root causes that contributed to standby performance degradation. This charts the average number of times a particular root cause was evidenced in a particular week. Since each computer can have multiple root causes behind its degradation, these root causes together will not sum to the number of standby performance issues seen in the enterprise. |
| Windows 10 and above Standby Performance: Degraded Component | Gives detailed information on the individual components contributing to slow standby cycles of Windows 10 and above Clients across the enterprise. The average reported time taken is not over all standby cycles, but only takes into consideration those standby cycles that were considerably slower due to a particular application/service. Therefore, this is not representative of all standbys in the enterprise, just those that have degraded. |  |

Windows 10 and above Client Operating System Monitoring Reports

The following reports provide performance information about Windows 10 and above Client computers monitored through this management pack.

| **Report** | **Description** |
| --- | --- |
| Logical Disk | Provides information about logical disk performance. |
| Memory | Provides information about memory performance. |
| Network Adapter | Provides information about network adapter performance. |
| Physical Disk | Provides information about physical disk performance. |
| Processor | Provides information about processor performance. |