

Guide to System Center Management Pack for Windows Server 2016 and above Operating Systems

**Microsoft Corporation**

Published: November 2021

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.

© 2019 Microsoft Corporation. All rights reserved.

Microsoft and MS-DOS, Windows, Windows Server, and Active Directory are trademarks of the Microsoft group of companies. All other trademarks are the property of their respective owners.

**Contents**

[System Center Management Pack for the Windows Server 2016 and above Operating Systems 5](#_Toc87445776)

[Document Version 5](#_Toc87445777)

[Revision History 5](#_Toc87445778)

[Get the Latest Management Pack and Documentation 7](#_Toc87445779)

[Changes in Version 10.1.0.6 7](#_Toc87445780)

[Changes in Version 10.1.0.5 8](#_Toc87445781)

[Changes in Version 10.1.0.2 8](#_Toc87445782)

[Changes in Version 10.1.0.0 8](#_Toc87445783)

[Changes in Version 10.0.21.0 8](#_Toc87445784)

[Changes in Version 10.0.19.0 9](#_Toc87445785)

[Changes in Version 10.0.17.0 10](#_Toc87445786)

[Changes in Version 10.0.8.0 10](#_Toc87445787)

[Changes in Version 10.0.3.0 12](#_Toc87445788)

[Changes in Version 10.0.2.0 12](#_Toc87445789)

[Changes in Version 10.0.1.0 13](#_Toc87445790)

[Changes in Version 10.0.0.0 13](#_Toc87445791)

[Supported Configurations 13](#_Toc87445792)

[Get Started 14](#_Toc87445793)

[Before You Import the Management Pack 14](#_Toc87445794)

[How to Import the Management Pack 16](#_Toc87445795)

[Create a New Management Pack for Customizations 16](#_Toc87445796)

[Key Monitoring Scenarios 17](#_Toc87445797)

[Availability 17](#_Toc87445798)

[Performance 18](#_Toc87445799)

[Processes and Ports 20](#_Toc87445800)

[Optional Configuration 21](#_Toc87445801)

[Process and Port Monitoring 21](#_Toc87445802)

[Monitor Physical Disks and Disk Partitions 47](#_Toc87445803)

[Monitor Logical and Physical Disks 47](#_Toc87445804)

[Monitor Logical Disk Free Space using the Logical Disk Free Space monitor 48](#_Toc87445805)

[Monitor Logical Disk Free Space using the Disk Free Space (%) Low and Disk Free Space (MB) Low monitors 49](#_Toc87445806)

[Monitor Logical and Physical Disk Performance 50](#_Toc87445807)

[Monitor Processors 50](#_Toc87445808)

[Monitor Memory Utilization 55](#_Toc87445809)

[Security Considerations 56](#_Toc87445810)

[Low-Privilege Environments 56](#_Toc87445811)

[Objects the Management Pack Discovers 58](#_Toc87445812)

[Upgrade an Operating System: How to Prevent Discovery Problems 59](#_Toc87445813)

[Classes 59](#_Toc87445814)

[How Health Rolls Up 60](#_Toc87445815)

[Troubleshooting and Known Issues 64](#_Toc87445816)

[Appendix: Management Pack Objects and Workflows 75](#_Toc87445817)

[(Abstract) Cluster Disk 75](#_Toc87445818)

[(Abstract) Cluster Shared Volume 75](#_Toc87445819)

[[Nano Server] Cluster Disk 75](#_Toc87445820)

[[Nano Server] Cluster Shared Volume 78](#_Toc87445821)

[[Nano Server] Windows Cluster disk monitoring seed 82](#_Toc87445822)

[Cluster Disk 82](#_Toc87445823)

[Cluster Shared Volume 92](#_Toc87445824)

[Health Service 96](#_Toc87445825)

[Operations Manager Standard License 96](#_Toc87445826)

[Virtual Server 97](#_Toc87445827)

[Windows Cluster (disk monitoring) 97](#_Toc87445828)

[Windows Server 98](#_Toc87445829)

[Windows Server 2016 and above Computer 99](#_Toc87445830)

[Windows Server 2016 and above Computer (Core) 99](#_Toc87445831)

[Windows Server 2016 and above Disk Partition 100](#_Toc87445832)

[Windows Server 2016 and above Logical Disk 100](#_Toc87445833)

[Windows Server 2016 and above Logical Processor 116](#_Toc87445834)

[Windows Server 2016 and above Network Adapter 119](#_Toc87445835)

[Windows Server 2016 and above Operating System 125](#_Toc87445836)

[Windows Server 2016 and above Operating System (Core) 159](#_Toc87445837)

[Windows Server 2016 and above Physical Disk 159](#_Toc87445838)

[Windows Server 2016 and above Process Monitoring Seed 169](#_Toc87445839)

[Windows Server 2016 and above Processor 179](#_Toc87445840)

[Windows Server 2016 Computer (Full) 183](#_Toc87445841)

[Windows Server 2016 Operating System (Full) 184](#_Toc87445842)

[Appendix: Rules and Monitors Disabled by Default 184](#_Toc87445843)

# System Center Management Pack for the Windows Server 2016 and above Operating Systems

The System Center Management Pack for Windows Server 2016 and above operating systems consists of the following management packs: Windows Server 2016 and above Operating Systems (Discovery), Windows Server 2016 and above Operating Systems (Monitoring), Windows Server Operating System Library, Windows Server Operating System Reports, Windows Server Cluster Disks Monitoring and Windows Server 2016 and above Process and Port Monitoring. The Microsoft Windows Server management packs monitor the performance, health, and availability of Windows Server 2016 and above operating systems.

By detecting, alerting on, and automatically responding to critical events and performance indicators, management packs reduce resolution times for issues and increase the overall availability and performance of your Windows Server 2016 or and above operating systems, thereby helping to reduce the total cost of ownership.

## Document Version

This guide is composed in terms of 10.1.0.6 version of the Management Pack for Windows Server 2016 and above operating systems.

## Revision History

|  |  |
| --- | --- |
| Release Date | Changes |
| November 2021 | Cluster disk performance collection rules data ingestion issue has been fixed for below Rules in Cluster Shared Volume Monitoring Management Pack   * Collection Rule for Average Disk Seconds Per Read Windows Server Cluster Disk * Collection Rule for Average Disk Seconds Per Write Windows Server Cluster Disk * Collection Rule for Average Disk Seconds Per Transfer Windows Server Cluster Disk |
| April 2021 | * Non-physical NIC’s discovery issue has been fixed in Windows Server 2016 and above Network Adaptor discovery |
| August 2020 | * Fixed Cluster Disk Monitor script time-out Issue * Computer Browser Service Health Monitor disabled by default. |
| April 2019 | * Added Microsoft.Windows.Server.Html5.Dashboard.mp * Updated WMI query exceptions scenarios for OS discovery * Fixed “Process and Port Monitoring” ProcessCmdDim table grooming bugs * Added support Logical Disk Volume Information task for Windows Server 2019 * Added support Display Server Statistics for Windows Server 2019 * Fixed incorrect frequency and threshold values for CPU Percentage Utilization, CPU DPC Time Percentage, CPU Percentage Interrupt Time monitors |
| June 2018 | * Added the “Changes in version 10.0.21.0” topic. * Updated the “Appendix: Management Pack Objects and Workflows” section. * Updated the “Troubleshooting and Known Issues” section. * Updated the “Appendix: Rules and Monitors Disabled by Default” section. |
| April 2018 | * Added the “Changes in version 10.0.19.0” topic. * Updated the “Key Monitoring Scenarios” and “Optional Configuration” sections. * Updated the “Appendix: Management Pack Objects and Workflows” section. * Updated the “Appendix: Rules and Monitors Disabled by Default” section. * Updated the “Troubleshooting and Known Issues” section. * Introduced some structural changes to the guide. |
| February 2018 | * Updated the supported versions of the operating systems (Windows Server 2016 and above) and rebranded the names of the management packs correspondingly. * Added the “Changes in version 10.0.17.0” topic. * Updated the “Optional Configuration” section: Added the “Process and Port Monitoring” section. * Updated the “Supported Configurations” section: added a separate row for Microsoft Windows Server 2016 and above Process and Port Monitoring Management Pack and removed the column about the operating systems’ versions. * Updated the “Troubleshooting and Known issues” section. * Updated the “Files in This Management Pack” section. * Added the “Appendix: Management Pack Objects and Workflows” section. |
| November 2016 | * Added the “Changes in version 10.0.8.0” topic. * Updated the “Troubleshooting and Known Issues” section. * Updated the Revision History. * Updated the “Monitoring Individual Processor Performance” section. * Updated the “Monitoring Physical Disks and Disk Partitions” section. * Added a note to “Monitoring Network Adapter” section. * Updated the “Appendix: Rules and Monitors Disabled by Default” section. * Updated the “Changes in version 10.0.2.0” topic. * Updated the health roll-up diagrams. * Updated the “Files in This Management Pack” section |
| June 2016 | * Added topic “Changes in version 10.0.3.0”. * Updated the Revision History. |
| January 2016 | * Added topic “Changes in version 10.0.2.0”. * Updated the Revision History. |
| December 2015 | * Various versioning and naming changes correlated with “Windows Server Technical Preview” to “Windows Server 2016” Management Pack rebranding. * Added topic “Changes in version 10.0.0.0”. * Updated the Revision History. |
| December 2015 | * Added topic “Changes in version 10.0.1.0”. * Updated the Revision History. |
| August 2015 | The original release of Windows Server Technical Preview Management Pack (version 6.0.7298.0). |

## Get the Latest Management Pack and Documentation

You can find the Management Pack for Windows Server 2016 and above operating systems on the [Download Center](http://go.microsoft.com/fwlink/?LinkId=717060) page.

## Changes in Version 10.1.0.6

Cluster disk performance collection rules data ingestion issue has been fixed for below Rules in Cluster Shared Volume Monitoring Management Pack

* Collection Rule for Average Disk Seconds Per Read Windows Server Cluster Disk
* Collection Rule for Average Disk Seconds Per Write Windows Server Cluster Disk
* Collection Rule for Average Disk Seconds Per Transfer Windows Server Cluster Disk

## Changes in Version 10.1.0.5

* Non-physical NIC’s discovery issue has been fixed in Windows Server 2016 and above Network Adaptor discovery.

## Changes in Version 10.1.0.2

* Fixed Cluster Disk Monitor script time-out Issue
* Computer Browser Service Health Monitor disabled by default.

## Changes in Version 10.1.0.0

* Implemented below Html5 Summary Dashboards
  + Windows Computers Heath
  + Active Alerts - Created In Last 7 Days
  + Operating System Performance
  + Agent Processor Utilization
  + Agent Memory Utilization
  + Disk Queue Length (C:)
  + Cluster Shared Volume Utilization-Average Disk
  + Processor Utilization
  + Available MB in memory
  + Disk % Free Space (C:)
  + Disk Average Sec\Transfer (C:)
  + Network Total Bytes/Sec
  + Network-Percent Bandwidth Used
* Updated WMI query exceptions scenarios for OS discovery
* Fixed “Process and Port Monitoring” ProcessCmdDim table grooming bugs
* Added support Logical Disk Volume Information task for Windows Server 2019
* Added support Display Server Statistics for Windows Server 2019
* Fixed incorrect frequency and threshold values for CPU Percentage Utilization, CPU DPC Time Percentage, CPU Percentage Interrupt Time monitors in Process and Port Monitoring

## Changes in Version 10.0.21.0

* Fixed the Handle Count increase issue.
* Enabled the Debug Level for Port Monitoring Dataset.
* Fixed the incorrect behavior while adding a new server via the [wizard](#_Process_and_Port_2).
* Improved performance for Process and Port Dashboards.
* Fixed bug: the “Time Accuracy Out of Range” monitor is not functioning when OS regional settings are changed.
* Increased the default threshold value from 1 millisecond to 60000 milliseconds for the “Time Accuracy Out of Range” monitor.
* The following monitors are disabled by default and must be enabled manually when necessary:
  + TCPv6 Segments Received Per Second
  + TCPv4 Segments Received Per Second
  + TCPv6 Segments Sent Per Second
  + TCPv6 Segments Retransmitted Per Second
  + TCPv4 Segments Sent Per Second
  + TCPv4 Segments Retransmitted Per Second
  + Time Accuracy Out of Range
* The following rules are disabled by default and must be enabled manually when necessary:
* Collection Rule for Windows Restarted Events
* Collection rule for NTFS Quota Threshold Reached
* Collection Rule for Software Updates Installation Events
* Collection rule for NTFS Quota Threshold Limit Reached
* Collection rule for Service or Driver Failed to Start events
* Collection Rule for Windows Dirty Shutdown Events
* Collection rule for invalid Share Configuration Detected
* Collection Rule for Windows Clean Restart Events
* Collection Rule for Software Updates Scheduled Installation Events
* Collection Rule for Checking the File System Occurred on Startup
* Collection Rule for Unexpected Service Terminations
* Collection rule for Network Adapter was Disconnected from the Network
* Collection Rule for Software Update Installation Failed
* Collection Rule for Windows Restart Events (restarted from bug check)
* TCPv6 Connections Reset
* TCPv4 Segments Received Per Second
* TCPv6 Segments Sent Per Second
* TCPv6 Segments Received Per Second
* TCPv6 Connection Failures
* TCPv6 Connections Established
* TCPv4 Segments Retransmitted Per Second
* TCPv4 Connection Failures
* TCPv4 Connections Established
* TCPv4 Segments Sent Per Second
* TCPv4 Connections Reset
* TCPv6 Segments Retransmitted Per Second

## Changes in Version 10.0.19.0

* Process monitoring is disabled by default: upon a “clean” installation of the management pack, the monitoring is disabled for all existing and newly added monitored servers, except for the case when the monitoring had been configured before via the [wizard](#_Process_and_Port_2) in the previous version of the management pack.
* The following rules are disabled by default:
  + Process Monitoring: Health State Collection
  + Process Monitoring: Process Health State Subscription
  + Process Monitoring: Performance Collection
  + Process Monitoring: Process Performance Metric Subscription
  + Process Monitoring: Network Port State Collection
  + Process Monitoring: Process Network Port Subscription
  + Process Monitoring: High Handle Count
  + Process Monitoring: High Memory Percentage
  + Process Monitoring: High Processor Time Percentage
  + Process Monitoring: Number of Processes Collection
* Elaborated a workaround for the Handle Count increase issue (see details in [Troubleshooting and Known Issues](#_Troubleshooting_and_Known) section).

## Changes in Version 10.0.17.0

* Rebranded the display strings and knowledge base articles according to the supported versions of the operating systems: Microsoft Windows Server 2016 and above.
* Implemented Microsoft Windows Server 2016 and above Process and Port Monitoring management pack.
* Introduced support for Windows Server above operating system.
* Introduced support for SCOM 1801.
* Implemented the “Time Accuracy Out of Range” monitor to track the total time offset of the server.
* Implemented the “Windows Server 2016 Number of Processes Performance Collection Rule” that allows identifying the number of processes on the monitored agent
* Implemented three Windows process alerting rules based on performance metrics. See the [Optional Configuration](#_Optional_Configuration) section.
* Implemented new performance rules for Cluster Disks (see [Cluster Disks](#_Cluster_Disk) section in Appendix: Management Pack Objects and Workflows)
* The following object definitions were added to Windows Server Operating System Library management pack:
  + Added the “Windows Server Process Monitoring Seed” class
  + Added the “Windows Server Computer Hosts Windows Server Process Monitoring Seed” relationship
* Implemented TCP-related performance collection rules and performance unit monitors (see [Key Monitoring Scenarios](#_Key_Monitoring_Scenarios) section).
* Fixed bug: “Performance By System Report” failure when SQL DW Database in German OS.
* Fixed bug: Some discoveries, monitors, rules, and tasks do not work if the WINRM is configured to use https only, or if SPN <http://servername> is set to a user account.
* Fixed the performance issue while running the "Performance by Utilization" report from the Windows Server Operating System report library.

## Changes in Version 10.0.8.0

* Added two new object types (*Windows Server 2016 Computer (Nano)* and *Windows Server 2016 Operation System (Nano)*) and a new group type (*Windows Server 2016 Computer Group (Nano)*). This improvement will help users to differentiate the groups and object types and manage them more accurately.
* Added a new monitor: Windows Server 2016 Storport Miniport Driver Timed Out Monitor; the monitor alerts when the Storport miniport driver times out a request.
* Fixed bug with duplicating Nano Server Cluster Disk and Nano Server Cluster Shared Volumes health discoveries upon MP upgrade. See [Troubleshooting and Known Issues section](#Undiscovery) for details.
* Fixed bug with Windows Server 2016 Operating System BPA Monitor: it did not work.
* Fixed bug with the incorrect discovery of Windows Server Operating System on Windows Server 2016 agentless cluster computers occurring upon management pack upgrade. See [Troubleshooting and Known Issues section](#ImproperDiscoveryKI) for details.
* Fixed bug: Free Space monitors did not work on Nano Server.
* Changed the logic of setting the override threshold values for Free Space (MB and %) monitors: a user can set the threshold values for Error state even within Warning state default thresholds. At that, the Error state will supersede the Warning state according to the set values.
* Fixed localization issue with root report folder in the Report Library.
* Fixed bug: Windows Server 2016 Computer discovery was causing repeated log events (EventID: 10000) due to the improper discovery of non-2016 Windows Server computers.
* Fixed bug: [Nano Server] Cluster Seed Name discovery was causing repeated log events (EventID: 10000) due to the improper discovery of non-Nano objects.
* Due to incompatibility issues in monitoring logic, several Cluster Shared Volumes MP bugs remained in version 10.0.3.0. These are now fixed in the current version (see the complete list of bugs below). To provide compatibility with the previous MP versions, all monitoring logic (structure of classes’ discovery) was reverted to the one present in version 10.0.1.0.
  + Fixed bug: disk free space monitoring issue on Quorum disks in failover clusters; the monitor was displayed as healthy, but actually it did not work and no performance data was collected.
  + Fixed bug: logical disk discovery did not discover logical disk on a non-clustered server with Failover Cluster Feature enabled.
  + Fixed bug: Cluster Shared Volumes were being discovered twice - as a Cluster Shared Volume and as a logical disk; now they are discovered as Cluster Shared Volumes only.
  + Fixed bug (partially): mount points were being discovered twice for cluster disks mounted to a folder - as a cluster disk and as a logical disk. See [Troubleshooting and Known Issues](#MontPoint) section for details.
  + Fixed bug: Cluster Shared Volume objects were being discovered incorrectly when they had more than one partition (applied to discovery and monitoring): only one partition was discovered, while the monitoring data was discovered for all partitions available. The key field is changed, and now partitions are discovered correctly; see [Troubleshooting and Known Issues](#CSV) section for details.
  + Fixed bug: Windows Server 2008 Max Concurrent API Monitor did not work on Windows Server 2008 platform. Now, it is supported on Windows Server platforms starting from Windows Server 2008 R2.
  + Fixed bug: when network resource name was changed in Failover Cluster Management, the previously discovered virtual computer and its objects were displayed for a short time, while new virtual computer and its objects were already discovered.
  + Fixed bug: performance counters for physical CPU (sockets) were collected incorrectly (for separate cores, but not for the physical CPU as a whole).
  + Fixed bug: Windows Server 2016 Operating System BPA monitor was failing with "Command Not Found" exception. Also, see [Troubleshooting and Known Issues](#BPA) section for details on the corresponding task.
  + Fixed bug: View Best Practices Analyzer compliance task was failing with exception: “There has been a Best Practice Analyzer error for Model Id”.
  + Fixed bug: in the Operations Console, “Volume Name” fields for logical disks, mount points, or Cluster Shared Volumes were empty in “Detail View”, while the corresponding data was entered correctly.
  + Fixed bug: Logical Disk Fragmentation Level monitor was not working; it never changed its state from “Healthy”.
  + Fixed bug: Logical Disk Defragmentation task was not working on Nano Server.
  + Fixed bug: If network resource name contained more than 15 symbols, the last symbols of the name was cut off, which was resulting in cluster disks and Cluster Shared Volume discovery issues.
  + Fixed bug: Logical Disk Free Space monitor did not change its state. Now it is fixed and considered as deprecated.
* The Management Pack was checked for compatibility with the latest versions of Windows Server 2016 and updated to support the latest version of Nano Server.
* Added new design for CPU monitoring: physical and logical CPUs are now monitored in a different way.
* Updated Knowledge Base articles and display strings.
* Improved discovery of multiple (10+) physical disks.
* Added compatibility with Nano installation.

## Changes in Version 10.0.3.0

* Several bugs located in Cluster Shared Volumes MP were fixed (see below); error handling migrated to the common recommended scenario. Enabled Quorum monitoring via changing the monitoring logic. The monitoring logic is splitting for Nano Server (with the usage of PowerShell) and all other operating systems.
  + Fixed bug: disk free space monitoring issue on Quorum disks in failover clusters; the monitor was displayed as healthy, but actually it did not work and no performance data was collected.
  + Fixed bug: logical disk discovery did not discover logical disk on a non-clustered server with Failover Cluster Feature enabled.
  + Fixed bug: Cluster Shared Volumes were being discovered twice - as a Cluster Shared Volume and as a logical disk; now they are discovered as Cluster Shared Volumes only.
  + Fixed bug (partially): mount points were being discovered twice for cluster disks mounted to a folder - as a cluster disk and as a logical disk. See [Troubleshooting and Known Issues](#MontPoint) section for details.
  + Fixed bug: Cluster Shared Volume objects were being discovered incorrectly when they had more than one partition (applied to discovery and monitoring): only one partition was discovered, while the monitoring data was discovered for all partitions available. The key field is changed, and now partitions are discovered correctly; see [Troubleshooting and Known Issues](#CSV) section for details.
* Created new overrides for Cluster Shared Volume MP, as long as the old ones did not work.
* Cluster disk monitors alert messages: alert title might be disorienting and was corrected.

## Changes in Version 10.0.2.0

* Updated the Microsoft.Windows.Server.ClusterSharedVolumeMonitoring.ClusterSharedVolume.Monitoring.State monitor alert properties and description. The fix resolved the property replacement failure warning being generated on monitor alert firing.
* Fixed bug: Windows Server Operating System objects were discovered on Agentless Managed virtual cluster computers (Cluster Instances and Cluster Groups).

## Changes in Version 10.0.1.0

* Script code migration to PowerShell for Windows Server 2016 Nano support

## Changes in Version 10.0.0.0

* “Windows Server Technical Preview” to “Windows Server 2016” versioning and naming rebranding changes
* MP used to discover physical CPU, which performance monitor instance name property was not correlated with Windows PerfMon object (expecting instance name in (socket, core) format). That affected related rules and monitors. With this release, MP discovers logical processors, rather than physical, and populates performance monitor instance name in proper format
* Network Adapter performance counters were not collected with the accompanying the event, and not able to resolve counter instance issue posted to the event log; fixed with this release

## Supported Configurations

The management packs provide support for Windows Server 2016 and above operating systems. The following table details the supported configurations for the management packs:

|  |  |  |
| --- | --- | --- |
| **Management Packs** | **SCOM** | **Requirements and Recommendations** |
| * Microsoft Windows Server 2016 and above Discovery * Microsoft Windows Server 2016 and above Monitoring * Microsoft Windows Server Library * Microsoft Windows Server Reports * Microsoft Windows Server Cluster Shared Volume Monitoring | SCOM 2016  SCOM 2019  Note: For other scom versions refer below links | It is highly recommended to use SQL 2012 or later. Recommendations for monitoring large numbers of instances are available in the corresponding [section](#_Monitor_a_Large). |
| * Microsoft Windows Server 2016 and above Process and Port Monitoring | SCOM 2016  SCOM 2019  Note: For other scom versions refer below links | **Installation of Microsoft.Net 4.5 (or higher) Framework is required on agents.**  It is highly recommended to use SQL Server 2016 SP1 in terms of performance improvements.  Recommendations for monitoring large numbers of instances are available in the corresponding [section](#_Monitor_a_Large). |

**Other SCOM versions support for Microsoft Windows Server 2016 and above, refer below links:**

<https://docs.microsoft.com/en-us/previous-versions/system-center/system-center-2012-R2/dn281931(v%3dsc.12)>

<https://docs.microsoft.com/en-us/system-center/scom/system-requirements?view=sc-om-2016#microsoft-monitoring-agent-operating-system>

<https://docs.microsoft.com/en-us/system-center/scom/system-requirements?view=sc-om-1801#microsoft-monitoring-agent-operating-system>

<https://docs.microsoft.com/en-us/system-center/scom/system-requirements?view=sc-om-1807#microsoft-monitoring-agent-operating-system>

<https://docs.microsoft.com/en-us/system-center/scom/system-requirements?view=sc-om-2019#microsoft-monitoring-agent-operating-system>

Support for the operating systems is subject to Microsoft’s overall support lifecycle (<http://go.microsoft.com/fwlink/?Linkid=26134>).

## Get Started

This section provides information about importing the files of System Center Management Pack for Windows Server 2016 and above operating systems.

### Before You Import the Management Pack

Before you import the System Center Management Pack for Windows Server 2016 and above operating systems, mind the following:

* The Management Pack for Windows Server Operating System provides the fundamental monitoring basics for monitoring computers running the Microsoft Windows operating system and Windows-based applications. You should import the Management Pack for Windows Server Operating System **before** using any other management packs such as Microsoft SQL Server, Active Directory Domain Services (AD DS), and Internet Information Services (IIS).
* This management pack includes newer versions of Windows Server Library and Windows Server 2016 and above management pack.
* **You have to import Windows Server OS Library MP (Microsoft.Windows.Server.Library.mp) before importing other Windows Server OS MP files.**

Files in This Management Pack

To monitor Windows Server 2016 and above operating systems by using System Center Operations Manager, you must first download the System Center Management Pack for Windows Server 2016 and above operating systems from the Management Pack Catalog, located at <http://go.microsoft.com/fwlink/?LinkId=82105>. The Management Pack for Windows Server 2016 and above operating systems includes the following files:

|  |  |  |
| --- | --- | --- |
| File | Description | Version |
| Microsoft.Windows.Server.2016.Discovery.mp | Displayed as “Windows Server 2016 and above Operating Systems (Discovery)”.This management pack discovers Windows Server specific classes. This management pack is a prerequisite for Windows Server 2016 and above management pack and is required by other management packs that focus their monitoring on systems running Microsoft Windows Server 2016 and above operating systems specifically. | 10.1.0.3 |
| Microsoft.Windows.Server.2016.Monitoring.mp | Displayed as “Windows Server 2016 and above Operating Systems (Monitoring)“.This management pack defines the rules, monitors, views, tasks, and reports that are used for monitoring Microsoft Windows Server 2016 and above operating systems. | 10.1.0.3 |
| Microsoft.Windows.Server.Library.mp | Displayed as “Windows Server Operating System Library,” this management pack is the library management pack that defines all of the features and components that are common to all versions of the Microsoft Windows Server operating systems. This management pack contains no monitoring configuration and is a prerequisite for all other Microsoft Windows Server operating system management packs. Therefore, this management pack must be imported at the same time or prior to the version-specific management packs. | 10.1.0.3 |
| Microsoft.Windows.Server.ClusterSharedVolumeMonitoring.mp | Displayed as “Windows Server Cluster Disks Monitoring”; this management pack defines the rules, monitors, views, tasks, and reports that are used for monitoring Cluster Shared Volumes on Microsoft Windows Server 2008-2016 and Nano Server operating systems. | 10.1.0.3 |
| Microsoft.Windows.Server.Reports.mp | Displayed as “Windows Server Operating System Reports”; this management pack defines reports on Microsoft Windows Server operating systems. | 10.1.0.3 |
| Microsoft.Windows.Server.2016.ProcessPortMonitoring.mpb | Displayed as “Windows Server 2016 and above Process and Port Monitoring”; this management pack enables the monitoring of Microsoft Windows Server 2016 and above processes and ports. | 10.1.0.3 |

### How to Import the Management Pack

For instructions about importing a management pack, see [How to Import an Operations Manager Management Pack](http://go.microsoft.com/fwlink/?LinkID=98348). The System Center Management Pack for Windows Server 2016 and above operating systems files must be imported together.

Important

While importing the management pack, a security warning from the Operations Manager is displayed because the management pack contains custom write actions that transfer data to the data warehouse.

### 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.

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 pre-production 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 preliminary deletion of 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 all of 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).

## Key Monitoring Scenarios

The System Center Management Pack for Windows Server 2016 and above operating systems is designed to provide monitoring information for computers running Windows Server 2016 (Full and Nano) or Windows Server 2016 and above operating systems (Core). The following section describes some of the most common monitoring scenarios.

### Availability

|  |  |
| --- | --- |
| Operating system and services | The following required services are checked for status (for example, running, not running, or paused):   * Logical Disk Manager * Server * Workstation * Remote Procedure * DHCP Client * Computer Browser * DNS Client * Event Log * Messenger * Plug and Play * TCP/IP NetBIOS Helper * In addition, services and drivers are checked for unstable or unpredictable states, incorrect configuration, failure to start, or unexpected termination. |
| Storage | Logical hard drives are checked for availability, sufficient free space, and integrity of the NTFS partition. |
| Network | Network adapters are checked for connection health, name and IP address conflicts. |

### Performance

|  |  |
| --- | --- |
| Processor | System processor(s) performance is checked system-wide using the following performance indicators:   * CPU Utilization * Percent Interrupt Time * DPC Time   Processors can optionally be monitored on a per-processor basis using the following criteria performance indicators:   * CPU Utilization * Percent Interrupt Time * Percent DPC Time   Performance data is collected for the following processor performance indicators:   * System Processor Queue Length * System Context Switches Per Second * Total Percent Interrupt Time * Total DPC Time * Total CPU Utilization |
| Memory | Memory consisting of physical memory and virtual memory (also known as page files) is monitored using the following performance indicators:   * Available memory (in MB) * Pages per second * Page file percent usage   Performance data is collected for the following memory criteria:   * Percent Committed Bytes In Use * Available MB * Pages per second * Memory Pool Non Paged Bytes (disabled by default) * Memory Pool Paged Bytes (disabled by default) * Page File Percent Usage |
| Logical disk | Logical disks are monitored, and performance data is collected for average disk seconds per reading, disk seconds per write, and disk seconds per transfer.  The “Logical Disk Fragmentation Level” monitor runs a periodic fragmentation check for all logical disks on a given computer running Windows Server 2016 or above operating systems during non-business hours. Use overrides to enable automatic defragmentation or to modify the configuration of non-business hours. |
| Physical disk | Physical disks are monitored, and performance data is collected for average disk seconds per reading, disk seconds per write, and disk seconds per transfer. |
| Network adapter | Network adapters are monitored for the number of bytes received per second, the number of bytes sent per second, and the total bytes per second. In addition, the health state of the network adapter is evaluated and is set to Healthy if connected and Critical if disconnected. |
| Operating system and services | TCP v4/v6 connection and capacity is checked by means of the following performance indicators:   * TCPv4 Connections Established * TCPv4 Connection Failures * TCPv4 Connections Reset * TCPv4 Segments Retransmitted Per Second * TCPv4 Segments Received Per Second * TCPv4 Segments Sent Per Second * TCPv6 Connections Established * TCPv6 Connection Failures * TCPv6 Connections Reset * TCPv6 Segments Retransmitted Per Second * TCPv6 Segments Received Per Second * TCPv6 Segments Sent Per Second |

### Processes and Ports

|  |  |
| --- | --- |
| Processes | The management pack monitors server processes and creates automatic alerts according to the following performance metrics:   * Memory Used (%) * CPU Used (%) * Handles (%) |
| Ports | The management pack collects the data regarding all opened TCP and UDP ports (IPv4 and IPv6) on each server run by Windows Server 2016 or above. At that, the data is collected for all system processes that are currently running. |

**Important**

Monitoring of processes and ports is **disabled by default**. Enable the corresponding workflows only if necessary via the overrides.

**Important**

A Handle Count increase may occur while monitoring processes and ports if a user account with [Debug Programs](https://technet.microsoft.com/en-us/library/cc976527.aspx) privilege is used. To avoid this issue, use a [low-privilege account](#_Low-Privilege_Environments) in “Microsoft Windows Server Process Rules Run As Profile” without [Debug Programs](https://technet.microsoft.com/en-us/library/cc976527.aspx) privilege.

## Optional Configuration

This section contains information about optional configuration changes you can make to the management pack features; for example, you can change the thresholds for monitoring physical and logical disk partitions, processors, and memory. It also contains step-by-step instructions for enabling a number of object discoveries.

**Note:** all entities and monitoring scenarios related to Windows Server 2016 will also work for Windows Server above operating system.

### Process and Port Monitoring

This section is devoted to configuring the Microsoft Windows Server 2016 and above Process and Port Monitoring management pack and its components. The management pack provides the following features:

* Automatic monitoring of all Windows processes and ports
* Selection of particular agents for monitoring
* Detailed visualization of all Windows processes and ports and their current metrics

You can find a detailed information about configuring the management pack in the subsections below.

#### Process and Port Add Monitoring Wizard

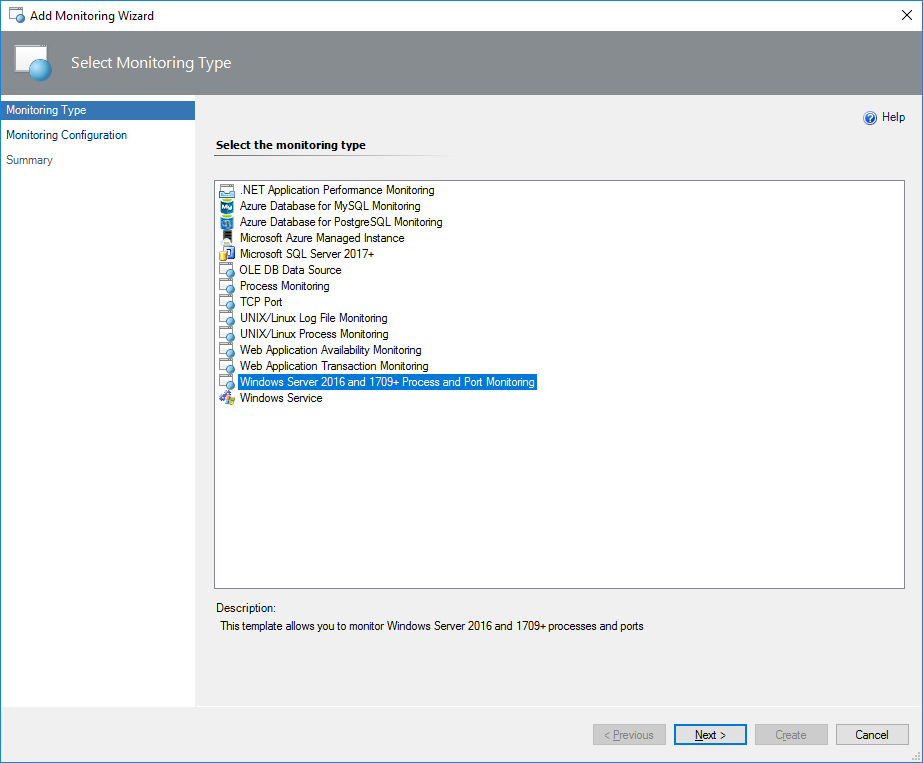
To set up the configuration for processes and ports monitoring and create a monitoring template, **Add Monitoring Wizard** can be used. The wizard has the following steps:

* Monitoring Configuration
* Optional Configuration(available in edit mode only)
* Summary (available upon creation of a template)

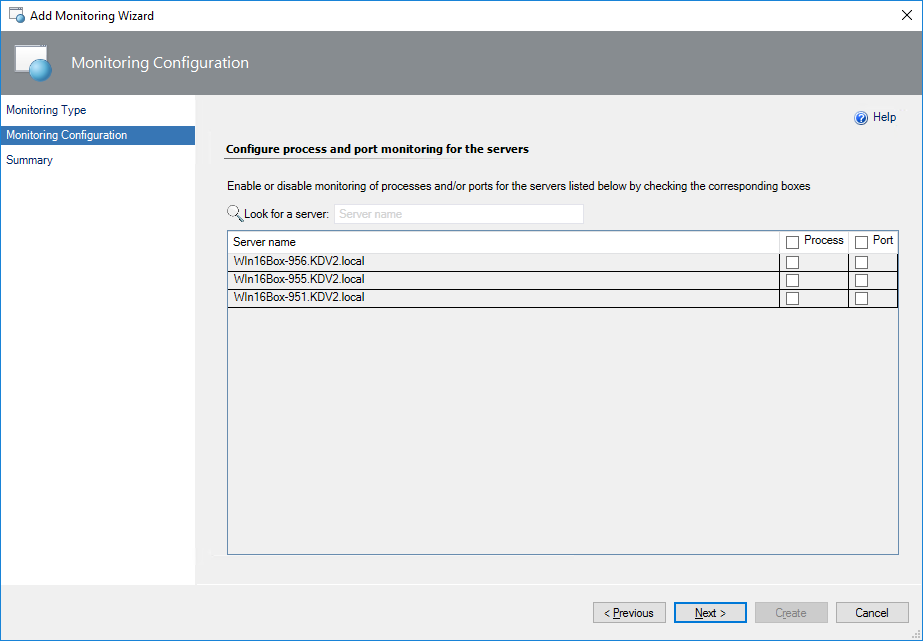
To create a new process and port monitoring template via the wizard, open the Operations Manager console, navigate to **Authoring** | **Management Pack Templates**, right-click **Microsoft Windows Server 2016 and above Process and Port Monitoring** and select **Add Monitoring Wizard…**



In **Monitoring Type** window, select **Microsoft Windows Server 2016 and above Process and Port Monitoring** and click **Next** button.



In **Monitoring Configuration** window, you will see a list of servers available for process and port monitoring. Upon a “clean” installation of the management pack, monitoring of all processes and ports is disabled by default for all existing and newly added monitored servers.



On this page, you can enable or disable monitoring of processes and/or ports for the listed servers by checking the corresponding boxes. You may also look for a specific server by means of the **Look for a server** search box.

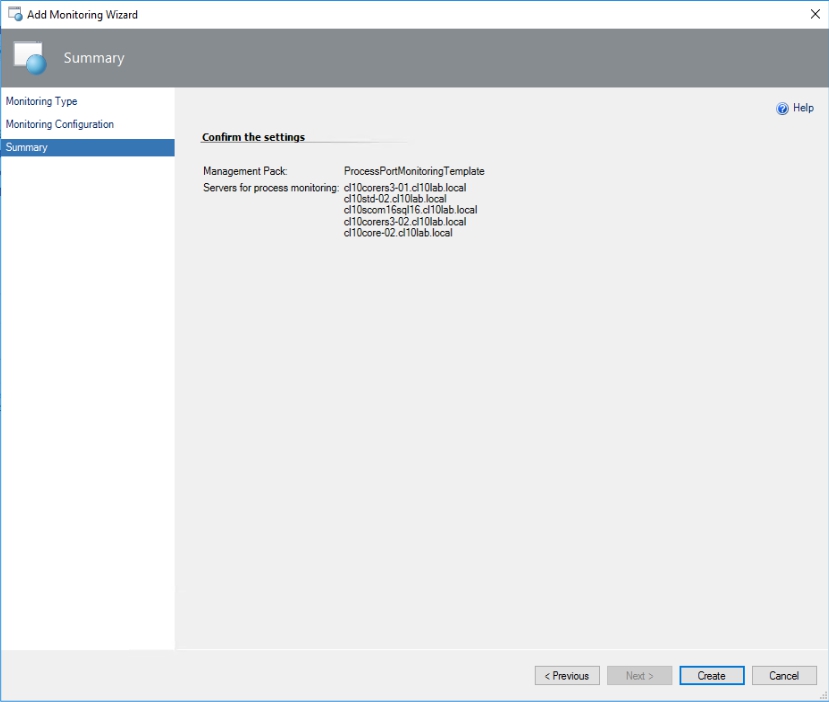
**Note:** In some cases (for example, if a new server is added), it may take up to 20 minutes for the servers to be discovered before they appear in the wizard.   
Previous configurations can be saved within approximately seven days after deletion of the management pack and may be applied upon reinstallation of the management pack within this period.

**Note:** If you change the target type to Windows Server Process Monitoring 2016 and above Seed in the **Discovered Inventory** view of the Operations Manager Console right after the seeds are discovered, you will see that both **Process Monitoring** and **Port Monitoring** columns are blank. At that point, monitoring of all processes is enabled, while monitoring of all ports is disabled by default.

**Important**

**Enabled** property override of the Process Monitoring rules for seed objects has higher priority than the corresponding setting provided in the wizard.

In **Summary** window, you can view your monitoring settings and confirm them by clicking the **Create** button.

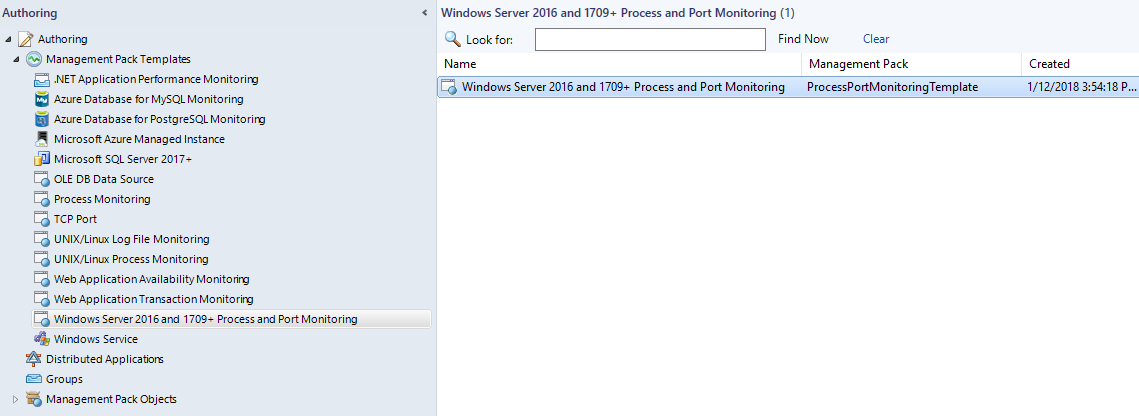


After that, your monitoring template will be successfully created.

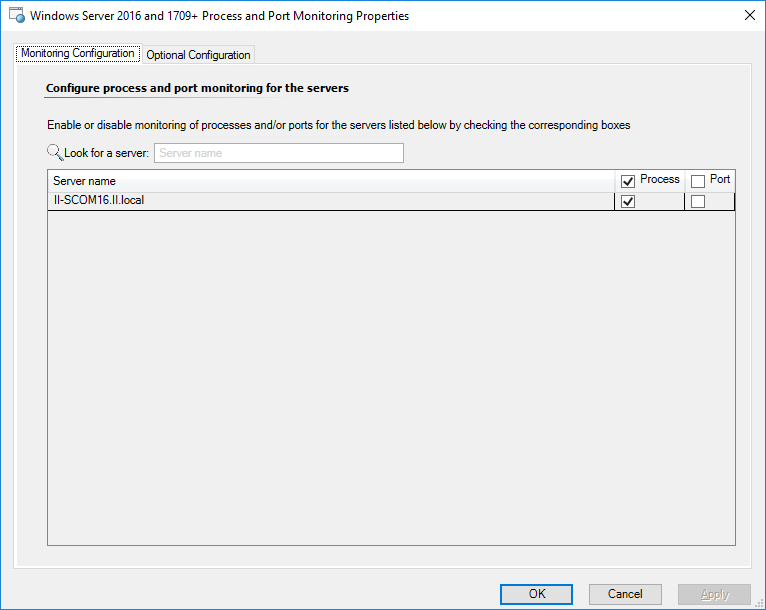
##### Edit Process and Port Monitoring Configuration

By means of the wizard, you may edit the previously created monitoring template. The editing steps are described below.

In the Operations Manager, navigate to **Authoring | Management Pack Templates**, and double-click the monitoring configuration template.



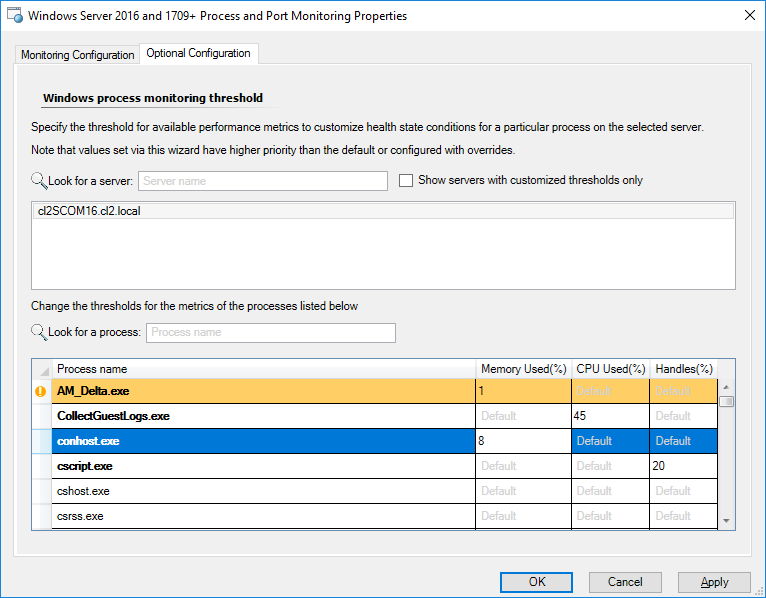
In **Monitoring Configuration** tab, you will see the list of previously configured servers available for process and port monitoring. You may change the monitoring configuration for the listed servers by checking or unchecking the corresponding boxes.



**Important**

**Enabled** property override of the Process Monitoring rules for seed objects has higher priority than the corresponding setting provided in the wizard.

In **Optional Configuration** tab, you can specify a threshold for available performance metrics to customize health state conditions for a particular process on the selected server.



First, select a server from the upper field of the page or look for a specific server by means of the **Look for a server** search box. Then, you can select a process from the table below and specify thresholds for the following performance metrics:

* Memory Used (%)
* CPU Used (%)
* Handles (%)

You may search for a specific process by means of the **Look for a process** search box.

Click the **Apply** button to save the changes and continue configuring the template, or click the **OK** button to save the changes and close the wizard.

**Note:** All settings are saved for some time even after deletion of the management pack. This is also true for the monitoring templates: a monitoring configuration is preserved even after deletion of the corresponding monitoring template.

**Important**

If you change thresholds for any metrics for specific processes, the alerts for that metrics are closed and regenerated for all processes.

#### Data Warehouse Configuration Notes

##### Monitor a Large Environment

Minimal recommended configuration for monitoring 1000+ objects is as follows:

* SCOM 2012 R2 with UR 9
* Window Server 2012 R2 as a server OS
* A dedicated server for the SCOM Operations DB SQL Server
* A dedicated server for the SCOM DW DB SQL Server
* A dedicated SCOM Management server for the Windows Server 2016 and above MP:
* 4 (V)CPU 2.0 GHz
* 8 GB RAM (or more)

A dedicated separate formatted volume with 64K Cluster Size for the SCOM Health State folder.

For all management servers in a management group, it is necessary to update/create the registry settings on the dedicated SCOM Management Server (watcher node) as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| Registry Key | Registry Value | Value in Decimal | Description |
| HKLM\SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\Data Warehouse\REG\_DWORD | Command Timeout Seconds | 1200 | This helps with dataset maintenance, as the default timeout of 10 minutes is often too short. Setting this to a longer value helps reduce the 31552 events you might see with standard database maintenance. See this [article](https://blogs.technet.microsoft.com/kevinholman/2010/08/29/the-31552-event-or-why-is-my-data-warehouse-server-consuming-so-much-cpu/) for more details. |
| SCOM 2012 existing registry value | Not preset (must create "Data Warehouse" key and value). |
| The default value in source code | 300 |
| Deployment Command Timeout Seconds | 86400 | This helps with the deployment of heavy-handed scripts that are applied during version upgrades and cumulative updates. Customers often see blocking on the DW database for creating indexes, and this causes the script not to be able to be deployed in the default of 3 hours. Setting this value to allow one full day to deploy the script resolves most customer issues. Setting this to a longer value helps reduce the 31552 events you might see with standard database maintenance after a version upgrade or UR deployment. This is a very common issue in large environments with very large warehouse databases. |
| SCOM 2012 existing registry value | Not preset (must create "Data Warehouse" key and value). |
| Default value in source code | 10800 seconds (3 hours). |
| HKLM\SYSTEM\CurrentControlSet\services\HealthService\Parameters | Persistence Cache Maximum | 262144 |  |
| Persistence Version Store Maximum | 262144 |
| Persistence Page Hint Cache Size | 262144 |
| Persistence Checkpoint Depth Maximum | 20971520 |

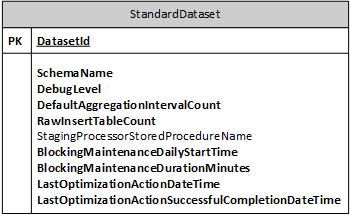
**Note:** It is necessary to restart Microsoft Monitoring agent upon a change of the registry settings.

##### Data Warehouse Dataset Troubleshooting and Customization

The management pack creates custom datasets for process and port monitoring metrics in the Operations Manager Data Warehouse. These datasets are defined in the Operations Manager **StandardDataset** table.

In order to troubleshoot issues, apply grooming and aggregation customizations: look into the Operations Manager Data Warehouse tables that are used by Windows Server 2016 and above Process and Port Monitoring Management Pack.

1. **dbo.StandardDataset** table:



**Configuration notes:**

|  |  |  |
| --- | --- | --- |
| **Column** | **Value** | **Description** |
| DebugLevel | 1 | Set this value for all “ProcessMonitoring” schemas to activate Data Warehouse logging and debugging. |

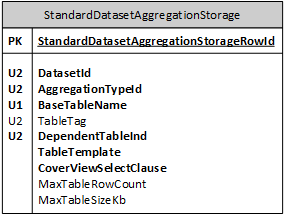
1. **dbo.StandardDatasetAggregation** table:



**Configuration notes:**

|  |  |  |
| --- | --- | --- |
| **Column** | **Value** | **Description** |
| AggregationTypeID | 0 | Corresponds to raw aggregation type. |
| 20 | Aggregate the data once an hour. |
| 30 | Aggregate the data once a day. |
| MaxDataAgeDays | Number of days | The number of days to store the aggregated data for the corresponding stored procedures. |

1. **dbo.StandardDatasetAggregationStorage** table:



**Configuration notes:**

|  |  |
| --- | --- |
| **Column** | **Description** |
| BaseTableName | Contains prefixes for the aggregated data tables. |
| TableTemplate | Contains commands for data tables generation. Aggregation Storage script verifies SQL Server edition. If the edition supports compression, it adds **'WITH (DATA\_COMPRESSION = PAGE)'** and it affects the data migration.  Note that if you want to move a database backup to another server, controlled by a lower SQL Server edition, perhaps you should disable compression on all raw tables due to some older SQL Server editions may not support compression. Check whether your SQL Server supports compression before the backup. Only Enterprise edition supports the backup with compression for SQL Server versions under 2016 SP1. |
| MaxTableRowCount | Contains the maximal number of records within a data table. When the maximal number is reached, a new data table with **BaseTableName** prefix is created. This makes grooming more efficient because old tables that exceeded grooming retention time can be dropped in the database |

Process and Port Monitoring pack includes the following datasets:

* + Process Monitoring: Performance Metric State data warehouse dataset
  + Process Monitoring: Process Health State data warehouse dataset
  + Process Monitoring: Process Network Ports data warehouse dataset

Therefore, it is recommended to override Maintenance Frequency Seconds parameter of Standard Data Warehouse Data Set maintenance rule for these data sets. Set a value slightly greater than the stored procedure run interval, which is 5 minutes (for example, 320 seconds) to prevent issues. It is also recommended to set slightly different frequencies for different data sets so that the rule does not fire simultaneously for all datasets.

To do so, navigate to **Authoring** tab in the Operations Console, navigate to **Authoring -> Management Pack Objects -> Rules** and change scope to **Standard Data Set**. Then you should see Standard Data Warehouse Data Set maintenance rule in the list. Right click on it and select in the context menu **Overrides -> Override the Rule -> For a specific object of class: Standard Data Set**. Select one of the data sets listed above in dialog that appeared and override **Maintenance Frequency Seconds** parameter. Repeat for the other two datasets.

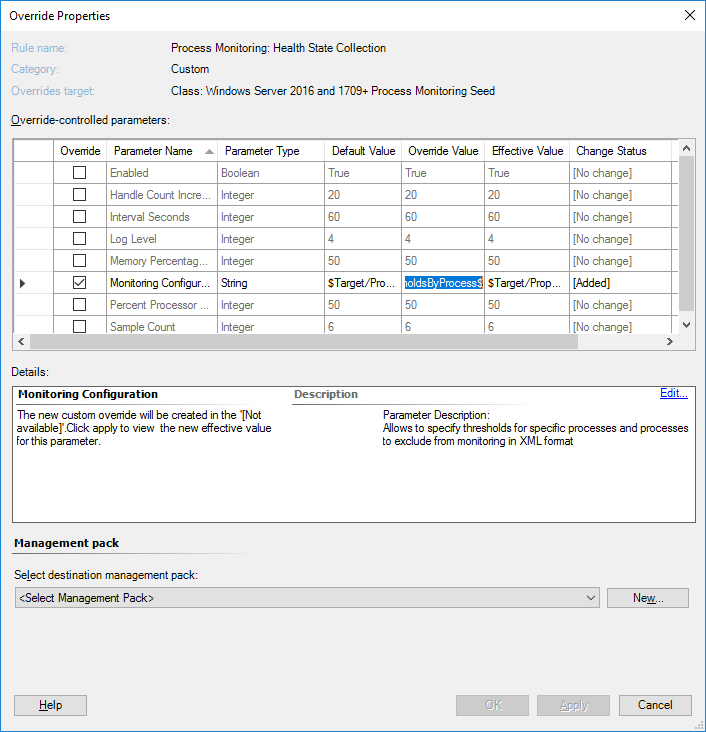
**Recommendation:** In order to improve database performance, add the new files with the same size to the Primary filegroup of SCOM DW database (see [Alter Database Transact-SQL File and Filegroup Options](https://docs.microsoft.com/en-us/sql/t-sql/statements/alter-database-transact-sql-file-and-filegroup-options) article).

#### Common Rules Parameters

##### Change Thresholds for Specific Processes

You can change thresholds for the specific metrics of an exact process via the [Add Monitoring Wizard](#_Process_and_Port_2). If you need to change the thresholds and/or exclude processes from monitoring at the same time, you can override **Monitoring Configuration** parameter of the following rules:

* Handle Count Increases Too Fast Alert Rule
* Processor Time Percentage Too High Alert Rule
* Memory Percentage Too High Alert Rule
* Process Monitoring: Performance Collection
* Process Monitoring: Process Performance Metric Subscription
* Process Monitoring: Health State Collection
* Process Monitoring: Process Health State Subscription
* Process Monitoring: Network Port State Collection
* Process Monitoring: Process Network Port Subscription



For this purpose, you can also use a Monitoring Configuration XML. See an example of the XML below:

***<ProcMonConfig>***

***<Thresholds>***

***<Threshold Name="svchost.exe" Type="Greater">***

***<Cpu>10</Cpu>***

***<Handles>20</Handles>***

***<Mem>23</Mem>***

***</Threshold>***

***</Thresholds>***

***<Exclude>***

***<Process Name="processName.exe" Type="Simple"/>***

***<Process Name="processName.exe" />***

***<Process Name="processName.exe" Type="Regex"/>***

***</Exclude>***

***</ProcMonConfig>***

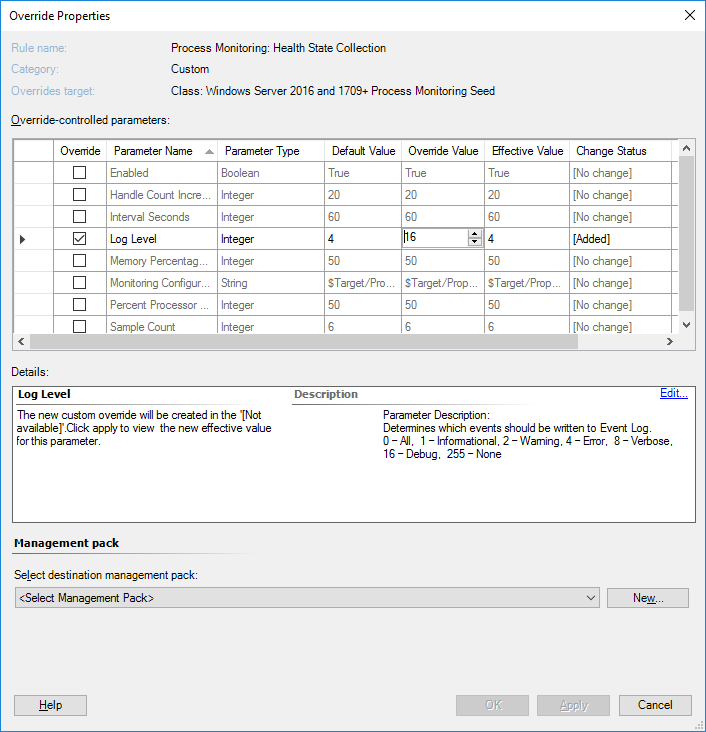
You can find details about the Monitoring Configuration XML nodes below:

* **ProcMonConfig element** – The required single root element
  + **Thresholds element** – The root element of the thresholds section. May contain multiple Threshold child elements.
  + **Threshold element** –Allows specifying overrides for a single process.
    - **Threshold[Name] attribute** – Process thresholds for which metrics are to be overridden.
    - **Threshold[Type] attribute** – Specifies health state calculation condition and can be set to one of the following values: *Greater, GreaterOrEqual, Less, LessOrEqual*.
    - **CPU element** – Value of this element specifies a threshold for *% Processor Time*.
    - **Handles element** – Value of this element specifies a threshold for *% Handle Count Increase*.
    - **Mem element** – Value of this element specifies a threshold for *% Memory*.
  + **Exclude element** – Root element for the process exclude list section. Process exclude list allows excluding specific processes from monitoring.
    - **Process element** – Specifies processes to be excluded from monitoring.
    - **Process[Name] attribute** – Process name or process name regular expression depending on *Type* attribute.
    - **Process[Type] attribute** – Specifies *Name* attribute format and can be set to *Simple* or *Regex*. If *Type* is *Simple*, then *Name* is expected to be a plain string specifying single process. If *Type* is *Regex*, then *Name* is expected to be regular expression so that names of multiple processes may match it. In that case, all those processes whose names match regular expression will be excluded from monitoring.

**Note:** Use this XML template **entirely** (for example, even if you do not need to change the **Thresholds** section).

##### Logging

In order to help troubleshooting issues, the logging has been implemented in the management pack. The rules have an overridable integer **Log Level** parameter that allows controlling the logging.



The log levels are as follows:

|  |  |  |
| --- | --- | --- |
| **Log Level** | **Value** | **Description** |
| All | 0 | All messages are logged. |
| Informational | 1 | Informational messages are logged only; e.g. start or stop of batcher module. |
| Warning | 2 | All information and warning messages are logged. |
| Error | 4 | All information, warning and error messages are logged (error = critical module error). |
| Verbose | 8 | All information, warning and error messages along with messages regarding operations of data collection module are logged. |
| Debug | 16-254 | All information, warning and error messages along with messages regarding operations of data collection module and debug messages are logged. |
| None | 255 | Logging is disabled. |

#### Windows Server Process Alert Rules

Microsoft Windows Server 2016 and above Process and Port Monitoring Management Pack provides several alert rules:

|  |  |
| --- | --- |
| **Rule** | **Description** |
| Process Monitoring: High Handle Count | Analyses the number of handles that a process uses during a specified interval within several samples. |
| Process Monitoring: High Processor Time Percentage | Analyses the processor usage in the percentage that a process uses during a specified interval within several samples. |
| Process Monitoring: High Memory Percentage | Analyses the memory usage in the percentage that a process uses during a specified interval within several samples. |

Based on the corresponding metrics, these rules create alerts when the defined threshold has been exceeded.

To avoid generating excessive alerts, there are minimum thresholds set for each rule.

Default values for minimum thresholds of the rules are as follows:

* 7% for Memory Percentage and Percent Processor Time
* 15% for Handle Count Increase.

**Note**: You cannot set the thresholds lower than the default ones. However, it is possible to change the minimal thresholds by creating registry DWORD (32-bit) values on the appropriate agent under the following registry key:

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\Modules\Global\BaseOSProcessMonitoring***

The used value names are as follows:

* MinimalMemoryPercentageThreshold
* MinimalPercentProcessorTimeThreshold
* MinimalHandleCountIncreaseThreshold

**Note:** It is not recommended to set the interval and sampling values lower than the default ones. The overall interval must be no less than 1 minute. The interval can be set lower if the volume of the database allows doing that.

Important

Alert rules also contain special workflows that activate a process of automatic closing of the outdated alerts. The key elements of these workflows are represented by **Process Name** and **Process PID** values, which are stored in special custom fields (**Custom Field 1** and **Custom Field 2** correspondingly). These fields are used for the closing of the alerts. Do not change these fields in order to avoid incorrect alert closing.

#### Windows Server Process and Port Collection

Process and Port collection is implemented by three pairs of rules. Each rule pair consists of Collection rule that runs on the agents and the corresponding Subscription rule that runs on the Management Server.

Collection rule collects data and sends it to the Management Server. Subscription rule receives data from the agents and writes it to the data warehouse.

Microsoft Windows Server 2016 and above Process and Port Monitoring Management Pack provides the following performance and state collection rules and the corresponding subscription rules:

|  |  |
| --- | --- |
| **Rule** | **Description** |
| Process Monitoring: Performance Collection | Collects process performance metrics. |
| Process Monitoring: Process Performance Metric Subscription | Writes process performance metrics to the data warehouse. |
| Process Monitoring: Health State Collection | Collects process health states. |
| Process Monitoring: Process Health State Subscription | Writes process health states to the data warehouse. |
| Process Monitoring: Network Port State Collection | Collects Network Ports. |
| Process Monitoring: Process Network Port Subscription | Writes Network Port data-to-data warehouse. |

**Note:** If you disable Subscription rule, the data will be collected on the agent side, but will not be written to the data warehouse.

Important

High-privilege **NT AUTHORITY\SYSTEM** account should be configured in SCOM for the **Microsoft Windows Server Process Collection Rules Run As Profile** so that the above-mentioned collection rules receive the data regarding username and command line. If a non-system account is used (even with admin rights), the username and command line fields will remain blank.

**Note:** You may disable process and port monitoring for specific servers: create a group in the Operations Manager console, add the corresponding monitoring seeds to it and override the “Enabled” property of the rules for this group to “False”.

**Note:** Health State Collection rule and Alert rules use separate overrides for the same thresholds.

For example, if you override the threshold for Process Monitoring: High Memory Percentage alert rule and do not override Memory Percentage Threshold for Health State Collection rule, then the alerts for memory percentage may be inconsistent with the corresponding process health state.

##### Process Monitoring Collection Workflows

Process Collection Workflows are Timer Based Workflows, which start regular collection cycle based on the predefined time interval (**60 seconds** by default).

SCOM has limitations on processing large amounts of data items from a rule:

* **128** data Items posting as a non-batch mode
* **1024** data Items posting in batch mode

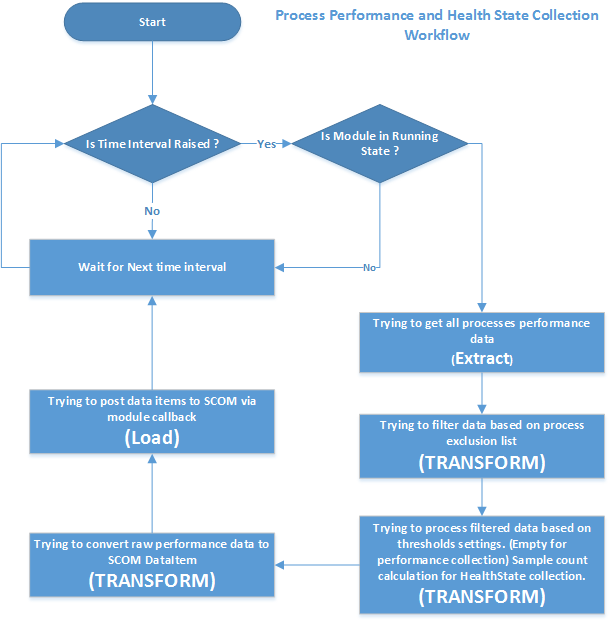
Process collection rules can easily exceed this limit. SCOM will drop such data and generate an error event in the Event Log about too much outstanding data.

To prevent this situation, process monitoring collection rules use a custom timer-based batcher module, which split data to a maximum allowed batch of 1024 data items. Custom batcher implements simple FIFO Queue. This Queue has a hardcoded limit of 1024 batches. It starts dropping data item if the Queue reaches the hard limit (a special event is logged to the console in case of a test application and Operations Manager Event Log in case of MP Build).

A possible loss of data may occur in case of SCOM agent or Health Service stop.

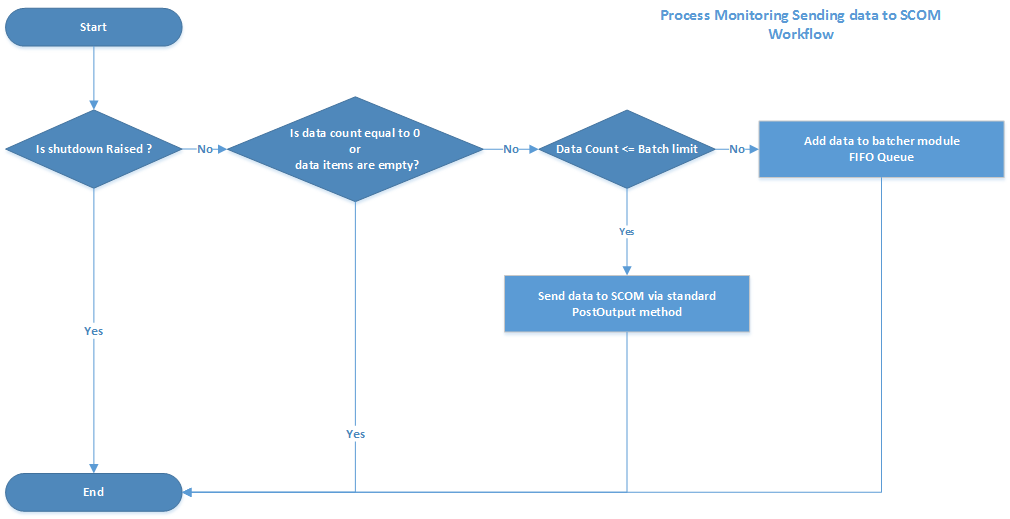
###### Process Monitoring Data Collection Workflow

Process Monitoring Collections for Health State and Performance has the following workflow:



###### Process Monitoring Sending data to SCOM Workflow

This workflow is located in SCOM data source module. It starts with **Process Monitoring Data Collection Workflow**.

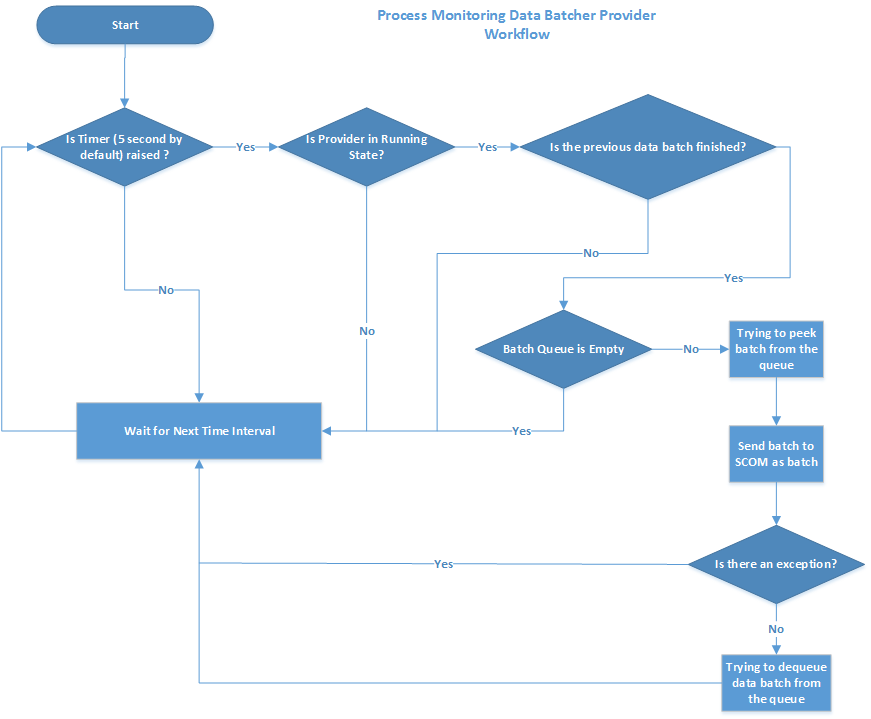


###### Process Monitoring Data Batcher Provider Workflow

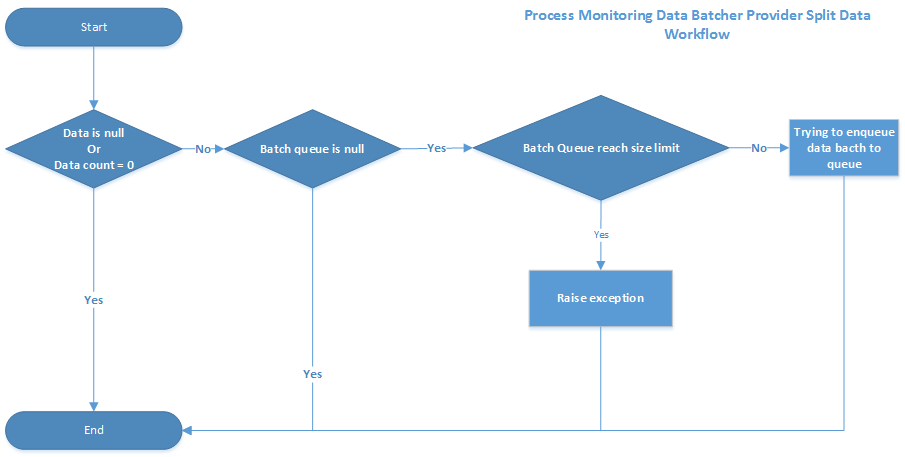
Custom timer based batcher module, which splits data to maximum allowed batch of 1024 data items. Custom batcher implements a simple FIFO Queue. This Queue has a hardcoded limit of 1024 batches. It starts dropping data item if the Queue reaches the hard limit (a special event is logged to the console in case of a test application and Operations Manager Event Log in case of MP Build).

Possible loss of data may exist in case of SCOM agent or Health Service stop.

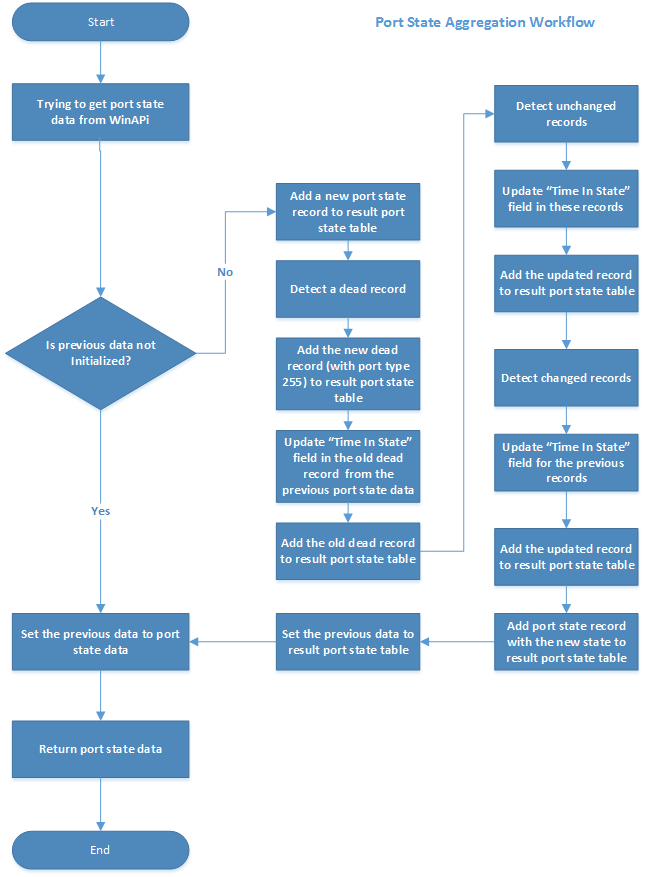
Workflow details:



###### Process Monitoring Data Batcher Provider Split Data Workflow



###### Port State Aggregation Workflow

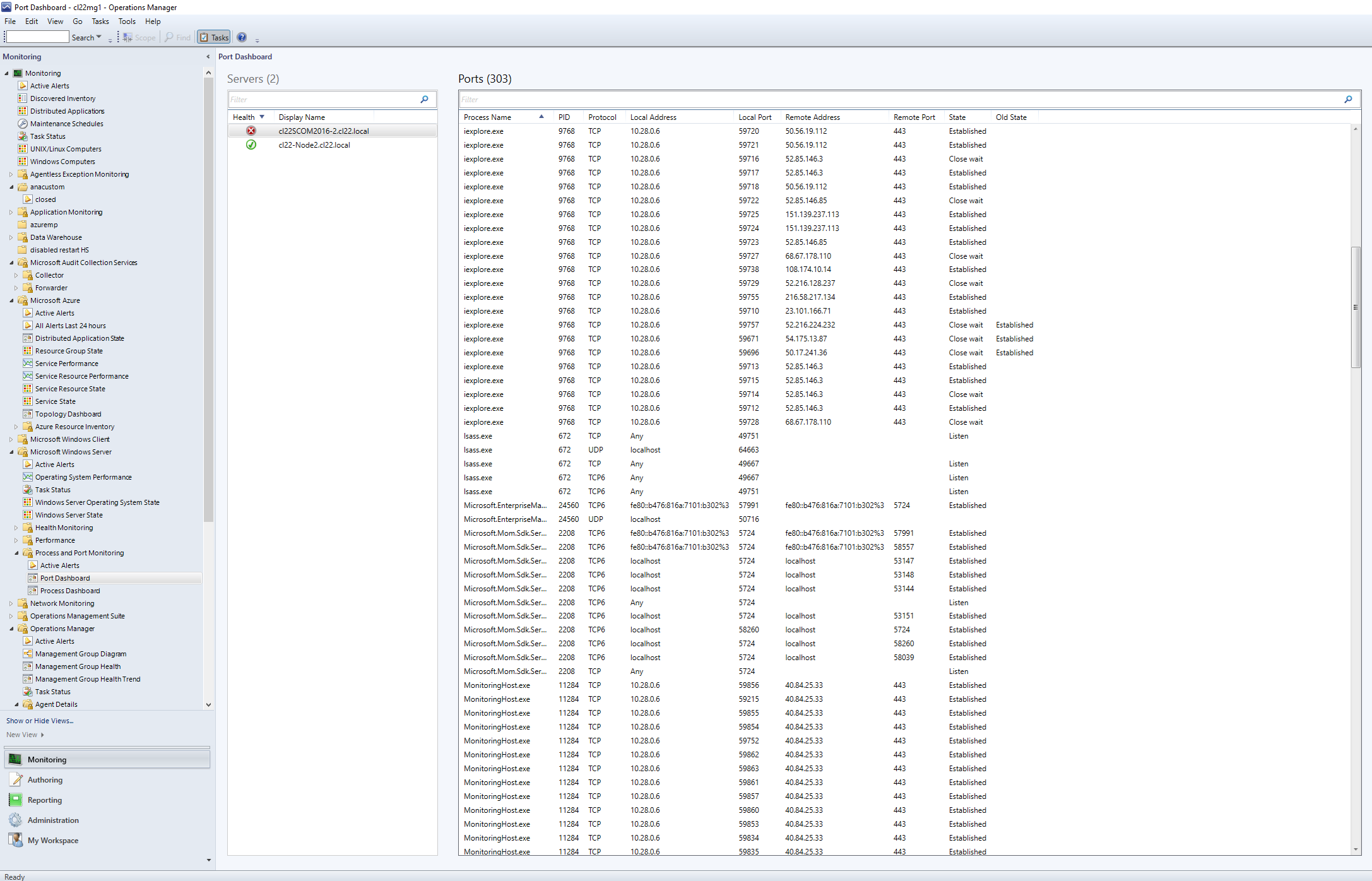


#### Dashboards

The Microsoft Windows Server 2016 and above Process and Port Monitoring management pack includes a set of rich dashboards, which provide detailed information about processes and ports of Windows Server 2016 and above operating systems.

##### Port Dashboard

Port dashboard allows viewing the detailed information regarding the ports currently used by the system processes on each server. The dashboard looks as follows:

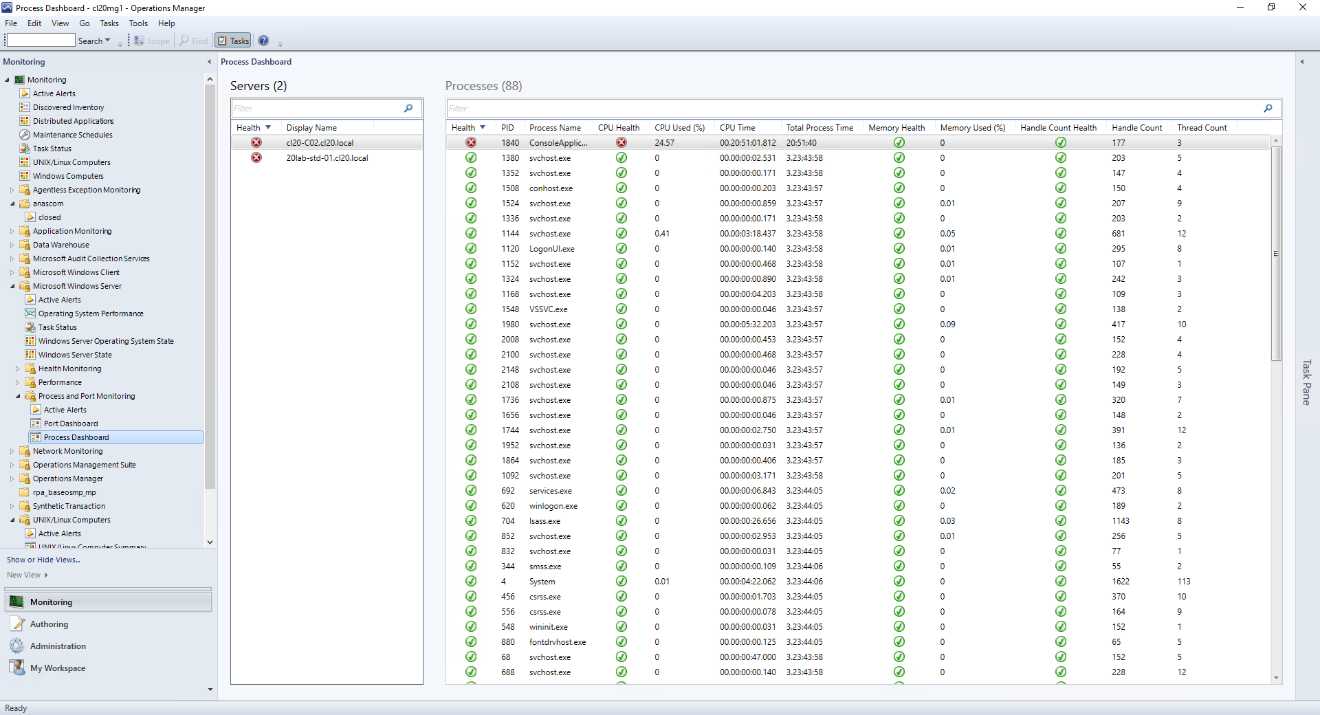


**Note:**

* For TCPv4: if a port is in "Listen" state, the "Remote Port" field of the dashboard is empty.
* For TCPv6: if a port is in "Listen" state, the "Remote Port" of the dashboard is empty. The management pack is not engaged in resolving IP addresses; therefore, the “Local Address” field, in this case, may display any address (0.0.0.0).
* For UDPv4: the "Remote Port" field of the dashboard is empty.
* For UDPv6: the "Remote Port" field of the dashboard is empty. The management pack is not engaged in resolving local addresses; therefore, the “Local Address” field, in this case, may display any address (0.0.0.0).

##### Process Dashboard

Process dashboard allows viewing the processes with their metrics and health states by the servers. The dashboard looks as follows:



For each process, you can view the current values of handle count and thread count along with values and health states regarding the following metrics:

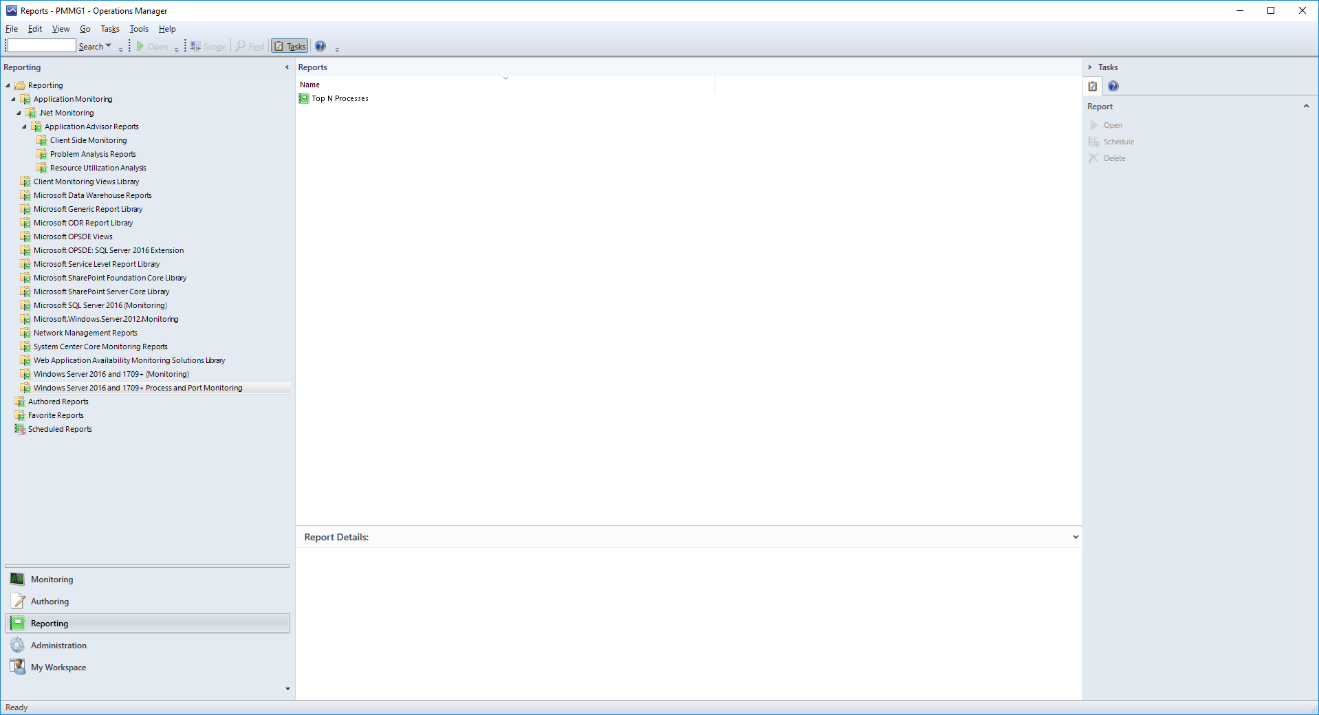
* Memory Used (%)
* CPU Used (%)
* Handle Count

You can also view aggregated (worst of) health state for each process.

**Note:** There is a special System Idle process with PID 0. Health states for metrics of this process do not initialize.

#### Reporting

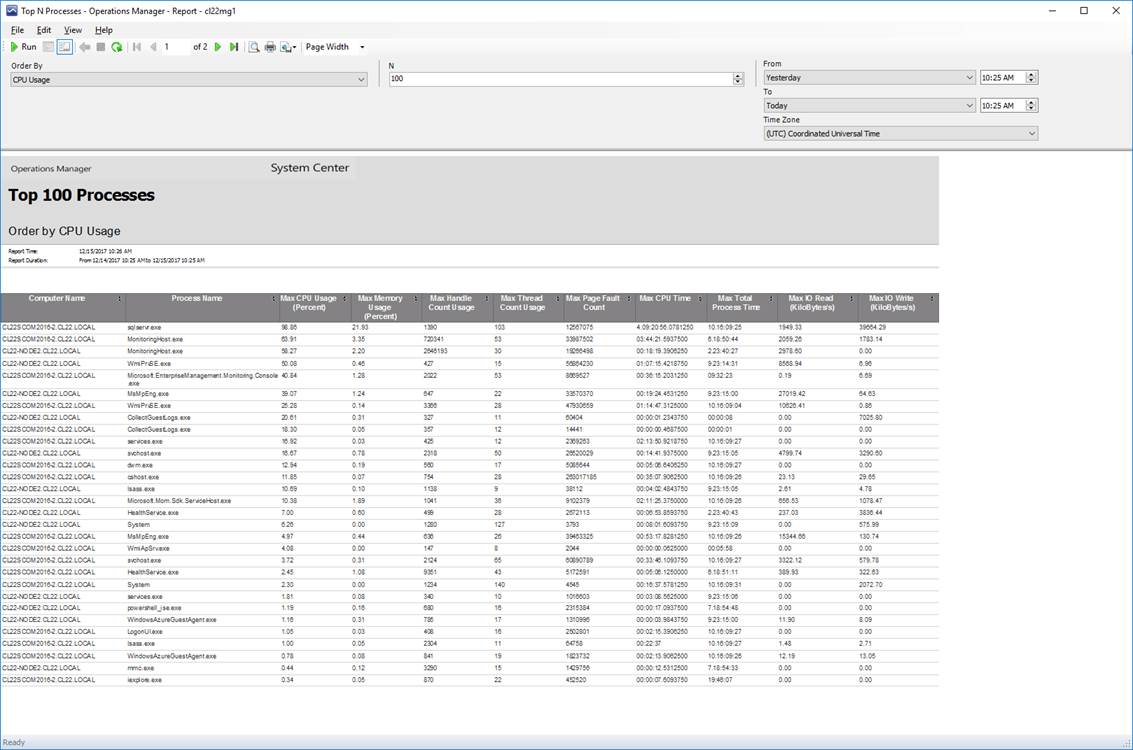
The Microsoft Windows Server 2016 and above Process and Port Monitoring Management Pack introduces the Top N Processes report available in the Reporting section of the management pack in the Operations Manager:



The report generates a table containing a top number (N) of the processes according to the following metrics:

* CPU Usage
* Memory Usage
* Handle Count Usage
* Thread Count
* Page Fault Count
* CPU Time
* Total Process Time
* IO Read (Kilobytes/s)
* IO Write (Kilobytes/s)

The report table contains a list of records gradated according to the selected metric. The number of displayed records and the time interval can be set manually. You can also arrange the displayed records by clicking the corresponding headers of the table.



**Note:** the reporting feature requires Operations Manager Reporting Server to be installed.

### Monitor Physical Disks and Disk Partitions

By default, Windows Server 2016 and above operating systems’ management packs do not discover physical disk partitions, only logical disk partitions. If you want to monitor physical disk drives, you can do so by enabling the Object Discoveries feature for the physical disk objects of Windows Server 2016 and above operating systems. After the object discovery has been enabled, physical disks will be discovered within 24 hours, after which they will become monitored.

### Monitor Logical and Physical Disks

The same set of monitors applies to logical disks, Cluster Shared Volumes, and cluster disks.

|  |  |
| --- | --- |
| Objects | Monitor name |
| Windows Server 2016 and above Logical Disk | Current Disk Queue Length (Logical Disk) |
| Windows Server 2016 and above Logical Disk | File system error or corruption |
| Windows Server 2016 and above Logical Disk | Average Logical Disk Seconds Per Transfer |
| Windows Server 2016 and above Logical Disk | [Deprecated] Logical Disk Free Space (Disabled by Default) |
| Windows Server 2016 and above Logical Disk | Logical Disk Fragmentation Level |
| Windows Server 2016 and above Logical Disk | Logical Disk Percent Idle Time (Disabled by Default) |
| Windows Server 2016 and above Logical Disk | Average Disk Seconds Per Read (Logical Disk) (Disabled by Default) |
| Windows Server 2016 and above Logical Disk | Average Disk Seconds Per Write (Logical Disk) (Disabled by Default) |
| Windows Server 2016 and above Logical Disk | Logical Disk Free Space (MB) Low (Disabled by Default) |
| Windows Server 2016 and above Logical Disk | Logical Disk Free Space (%) Low (Disabled by Default) |
| Windows Server 2016 and above Physical Disk | Current Disk Queue Length (Physical Disk) |
| Windows Server 2016 and above Physical Disk | Average Physical Disk Seconds Per Transfer |
| Windows Server 2016 and above Physical Disk | Physical Disk Percent Idle Time (Disabled by Default) |
| Windows Server 2016 and above Physical Disk | Average Physical Disk Seconds Per Read (Disabled by Default) |
| Windows Server 2016 and above Physical Disk | Average Physical Disk Seconds Per Write (Physical Disk) (Disabled by Default) |

Evaluate the default settings for the following parameters and compare them against your business needs.

### Monitor Logical Disk Free Space using the Logical Disk Free Space monitor

The default health state thresholds for the Logical Disk Free Space monitor are different for the system and non-system logical disk volumes. Error and Warning health states are based on both percentages of free space and on an absolute value, designated in megabytes (MB), of free space, as shown in the following sections.

System Partition

|  |  |  |
| --- | --- | --- |
| Health state | Percentage free space | MB free space |
| Error | 5% | 300 MB |
| Warning | 10% | 500 MB |

Important

For health state to change to Error or Warning, the values for both percentage free space and MB free space must drop below the corresponding threshold.

Non-system Partition

|  |  |  |
| --- | --- | --- |
| Health state | Percent free space | MB free space |
| Error | 5% | 1,000 MB |
| Warning | 10% | 2,000 MB |

Important

For health state to change to Error or Warning, the values for both percentage free space and MB free space must drop below the corresponding threshold.

This monitor is designed to evaluate both percentage free and MB free; the monitor works equally well for disks regardless of their storage capacity. This monitor does not alert on Warning state, only on Error state by default. Use the override to enable alerts in a Warning state.

### Monitor Logical Disk Free Space using the Disk Free Space (%) Low and Disk Free Space (MB) Low monitors

The thresholds used in these monitors are the same as the ones used for the Disk Free Space Monitor. However, you can set the threshold values for Error state even within Warning state default thresholds. At that, the Error state will supersede the Warning state according to the set values.

One reason for using these monitors is the case when you want to receive alerts regarding available MB and % free space separately. Therefore, you should disable the Logical Disk Free Space monitor.

These monitors do not alert on Warning state, only on Error state by default. Use the override to enable alerts on Warning state.

### Monitor Logical and Physical Disk Performance

The following monitors can be used to assess disk performance. By default, Average Disk Seconds Per Transfer is enabled. Average Disk Seconds Per Read and Average Disk Seconds Per Write are not enabled by default.

Average Disk Seconds Per Transfer

Average Disk Seconds Per Transfer monitors the time, in seconds, of the disk transfer. The default threshold value is .04. This monitor collects fifteen samples to compute the threshold. The threshold is met when the value of all fifteen consecutive samples is greater than .04. The health state is considered Healthy when it is below the threshold value and Critical when it is above the threshold. We recommend leaving the threshold at its default value of .04 seconds for an average disk transfer, which is considered acceptable performance.

Average Disk Seconds Per Read and Write

Average Disk Seconds Per Read is the average time, in seconds, to read data from the disk. Average Disk Seconds Per Write is the average time, in seconds, to write data to the disk. The threshold for both these monitors is .04 seconds and a sample is taken every minute. These monitors collect fifteen samples to compute the threshold. The threshold is met when the values of fifteen consecutive samples are greater than .04.

### Monitor Processors

The management pack can monitor individual instances of processors or all instances together. By default, the health of the processors is monitored as a total of all instances. If you are interested in monitoring individual processor instances, you can do so by enabling the Object Discoveries for Windows Server 2016 and above operating systems. After Object Discoveries has been enabled, the processors will be discovered within 24 hours after which they will become monitored, and performance data will be collected.   
Please note that there is no separate performance counter for sockets (processors) in Windows Server. To provide a correct collection of performance data for sockets, a special script is used, which gathers the necessary data from *Win32\_PerfFormattedData\_PerfOS\_Processor* WMI class.

#### Monitor Total Processor Performance

Many rules, tasks, and monitors in the management pack are used for monitoring processor performance. We recommend that you at least monitor the items listed in the following table.

|  |  |
| --- | --- |
| Object | Monitor/rule name |
| Windows Server 2016 and above Operating System | Core Windows Services Rollup |
| Windows Server 2016 and above Operating System | Computer Browser Service Health |
| Windows Server 2016 and above Operating System | DHCP Client Service Health |
| Windows Server 2016 and above Operating System | DNS Client Service Health |
| Windows Server 2016 and above Operating System | Plug and Play Service Health |
| Windows Server 2016 and above Operating System | Memory Pages Per Second |
| Windows Server 2016 and above Operating System | Computer Browser Service Health |
| Windows Server 2016 and above Operating System | Windows Event Log Service Health |
| Windows Server 2016 and above Operating System | Available Megabytes of Memory |
| Windows Server 2016 and above Operating System | Plug and Play Service Health |
| Windows Server 2016 and above Operating System | RCP Service Health |
| Windows Server 2016 and above Operating System | Server Service Health |
| Windows Server 2016 and above Operating System | TCP/IP NetBIOS Service Health |
| Windows Server 2016 and above Operating System | Total CPU Utilization Percentage |
| Windows Server 2016 and above Operating System | Workstation Service Health |
| Windows Server 2016 and above Operating System | Operating System BPA Monitor |
| Windows Server 2016 and above Operating System | Percentage of Committed Memory in Use (Disabled by Default) |
| Windows Server 2016 and above Operating System | Total DPC Time Percentage (Disabled by Default) |
| Windows Server 2016 and above Operating System | Total Percentage Interrupt Time (Disabled by Default) |
| Windows Server 2016 and above Operating System | Max Concurrent API Monitor |

Evaluate the default settings for the following parameters and compare them against your business needs. If your management strategy could benefit from a change in these values, use overrides to make the necessary changes.

Please note that Computer Browser Service Health monitor is not running on Nano Server (the state of the monitor will be always “Healthy”).

Total CPU Utilization Percentage (Monitor)

CPU utilization is the percentage of elapsed time that the processor spends to run a non-idle thread. It is calculated by measuring the duration of the idle thread that is active in the sample interval and subtracting that time from interval duration. CPU utilization is the primary indicator of processor activity, and this monitor displays the average percentage of busy time observed during the sample interval.

CPU queue length is the current length of the system work queue for this CPU.

By default, the threshold for this monitor is a CPU utilization of 95 percent along with a CPU queue length greater than 15 measured once every 2 minutes using five samples to compute the threshold.

Total Processor % Interrupt Time (Collection Rule)

This rule collects the Total Instance of the % Interrupt Time performance counter. By default, a sample is taken every 5 minutes. % Interrupt Time monitors the overall average processor utilization that occurred in Interrupt mode. Only interrupt service routines (ISRs), which are device driver functions run in Interrupt mode. Excessive % Interrupt Time can identify that a device is malfunctioning and serves as a secondary indicator that a device might be contributing to a processor bottleneck.

Processor % Processor Time Total (Collection Rule)

This rule collects the Total Instance of the % Processor Time performance counter. By default, a sample is taken every 5 minutes. % Processor Time is the percentage of time when the processor is not running the idle thread, and it is assumed that the processor is busy on behalf of real work. % Processor Time is the primary indicator of a processor bottleneck. You should be concerned of sustained periods of % Processor Time over 80 to 90 percent.

Total Processor % DPC Time (Collection Rule)

This rule collects the Total Instance of the % DPC Time performance counter. By default, a sample is taken every 5 minutes. % DPC Time monitors the percentage of time that the processor spent in routines known as deferred procedures calls, which are device driver scheduled routes that are called from ISRs. Excessive %DPC Time might be an indication of a hardware or device driver problem.

#### Monitor Individual Processor Performance

The following monitors and rules are enabled when you enable Object Discoveries for processors.

|  |  |
| --- | --- |
| Object | Monitor/rule name |
| Windows Server 2016 and above Processor | Processor % Interrupt Time |
| Windows Server 2016 and above Processor | Processor % Processor Time |
| Windows Server 2016 and above Processor | Processor % DPC Time |
| Windows Server 2016 and above Processor | CPU Percentage Utilization |
| Windows Server 2016 and above Processor | CPU DPC Time Percentage (Disabled by Default) |
| Windows Server 2016 and above Processor | CPU Percentage Interrupt Time (Disabled by Default) |
| Windows Server 2016 and above Logical Processor | Logical Processor % Interrupt Time |
| Windows Server 2016 and above Logical Processor | Logical Processor % Processor Time |
| Windows Server 2016 and above Logical Processor | Logical Processor % DPC Time |
| Windows Server 2016 and above Logical Processor | Logical CPU Percentage Utilization |
| Windows Server 2016 and above Logical Processor | Logical CPU DPC Time Percentage (Disabled by Default) |
| Windows Server 2016 and above Logical Processor | Logical CPU Percentage Interrupt Time (Disabled by Default) |

Processor Information % Interrupt Time (Collection Rule)

This rule collects the Processor of the % Interrupt Time performance counter. By default, a sample is taken every 5 minutes. % Interrupt Time monitors the overall average processor utilization that occurred in Interrupt mode. Only interrupt service routines (ISRs), which are device driver functions run in Interrupt mode. Excessive % Interrupt Time can identify that a device is malfunctioning and serves as a secondary indicator that a device might be contributing to a processor bottleneck.

Processor % Processor Time (Collection Rule)

This rule collects the Processor of the % Processor Time performance counter. By default, a sample is taken every 5 minutes. % Processor Time is the percentage of time when the processor is not running the idle thread and it is assumed that the processor is busy on behalf of real work. % Processor Time is the primary indicator of a processor bottleneck. You should be concerned of sustained periods of % Processor Time over 80 to 90 percent.

Processor Information % DPC Time (Collection Rule)

This rule collects the Processor of the % DPC Time performance counter. By default, a sample is taken every 5 minutes. % DPC Time monitors the percentage of time that the processor spent in routines known as deferred procedures calls, which are device driver scheduled routes called from ISRs. Excessive % DPC Time might be an indication of a hardware or device driver problem.

CPU Utilization Percentage (Monitor)

CPU utilization is the percentage of elapsed time that the processor spends to run a non-idle thread. It is calculated by measuring the duration of the idle thread that is active in the sample interval and subtracting that time from interval duration. CPU utilization is the primary indicator of processor activity, and this monitor displays the average percentage of busy time observed during the sample interval.

CPU queue length is the current length of the server work queue for this CPU.

By default, the threshold for this monitor is CPU utilization of 95 percent measured once every 2 minutes using 5 samples to compute the threshold.

#### Monitor Network Adapter

The performance counters measured from network interfaces are key indicators of network issues.

|  |  |
| --- | --- |
| Windows Server 2016 and above Network Adapter | Percent Bandwidth Used Total |
| Windows Server 2016 and above Network Adapter | Percent Bandwidth Used Read (Disabled by Default) |
| Windows Server 2016 and above Network Adapter | Percent Bandwidth Used Write (Disabled by Default) |
| Windows Server 2016 and above Network Adapter | Network Adapter Connection Health (Disabled by Default) |

Note: only “physical” network adapters with MAC addresses are discovered.

### Monitor Memory Utilization

Sufficient memory is essential for efficient operation of a computer. We recommend that you consider using the following monitor.

|  |  |
| --- | --- |
| Class | Monitor name |
| Windows Server 2016 and above Operating System | Available Megabytes of Memory |

#### Available Megabytes of Memory

Available Megabytes of Memory is the amount of physical memory, in megabytes, immediately available for allocation to a process or for system use. It is equal to the sum of memory assigned to the standby (cached), free, and zero page lists.

The default threshold is 2.5MB, a sample is taken every 2 minutes, and three samples are taken to compute the threshold. This monitor is considered Healthy when available memory is above the threshold and Critical when it is below the threshold.

#### Probe Module: IsFeatureInstalled

The Microsoft.Windows.Server.IsFeatureInstalled.Probe checks whether a specified feature is installed on a computer running the Windows Server 2016 or later server operating system. This module can be used by developers who need to discover features installed.

##### Module

|  |  |
| --- | --- |
| ID | Microsoft.Windows.Server.IsFeatureInstalled.Probe |
| Type | ProbeActionModuleType |
| MP | Microsoft.Windows.Server.Library |
| Run As | System.PrivilegedManagementAccount |
| Accessibility | Public |

##### Input (Configuration)

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Description | Overridable |
| TimeoutSeconds | int | Timeout (seconds) | No |
| TargetComputerName | string | Target computer name | No |
| ServerFeature | string | Server component ID or name.  The possible values of the ServerFeature property correspond to values of the ID or Name property of the WMI class Win32\_ServerFeature (<http://go.microsoft.com/fwlink/?LinkId=119210>). If ServerFeature is a valid integer, then the module will try to search for a particular feature/role by ID first, and then by Name.  Important!  Win32\_ServerFeature::Name does not correspond to a description field provided in the documentation for Win32\_ServerFeature::ID. One way to determine the actual name is to run servermanagercmd.exe -q and find the name in the output. There is also a risk that Win32\_ServerFeature::Name is subject to change without any notice in future operating system versions. | No |

## Security Considerations

This section provides information about using a low-privilege account with the System Center Management Pack for Windows Server 2016 and above operating systems. It also includes information about the computer groups that are added when this management pack is installed.

### Low-Privilege Environments

The Windows Operating System Management Pack uses the agent action account to perform discovery and run rules, tasks, and monitors. The agent action account can run as Local System or as a named account. When running as Local System, the agent action account has all the rights needed to perform discovery and run rules, tasks, and monitors.

Important

Using a low-privilege domain account requires password updating that is consistent with your password expiration policies.

Using a Low-Privilege Account

You can use a low-privilege account for the agent action account; however, a number of rules and monitors require elevated rights. The low-privilege account must meet the following requirements:

 Member of the local users group

 Member of the local Performance Monitor Users group

 Granted Log On Locally rights

Three of the monitors and object discoveries in the Windows Operating System Management Pack require a high-privilege account to perform the functions:

 Mount Point Discovery

 Physical Disk Discovery

 Monitoring the Computer Browser service

In addition, the following tasks require a high-privilege account:

 Top CPU Usage

 Display Active Sessions

 Display Server Statistics

These rules and monitors have been configured to use the Privileged Monitoring Account Run As Profile, which defaults to Local System, and does not require association with any Run As account and the target computer. As a result, no user intervention is required for these rules and monitors that need to use a high-privilege account.

If your requirements stipulate that only a low-privilege account is to be used in your environment, use overrides to disable the three monitors and object discoveries.

Important

High-privilege **NT AUTHORITY\SYSTEM** account should be configured in SCOM for the **Microsoft Windows Server Process Collection Rules Run As Profile** so that the above-mentioned collection rules receive the data regarding username and command line. If a non-system account is used (even with admin rights), the username and command line fields will remain blank.

#### Computer Groups

You can delegate authority to a precise level by using user roles.

The following groups are added when you install the System Center Management Pack for Windows Server 2016 and above operating systems:

|  |  |
| --- | --- |
| Group | Comments |
| Windows Server 2016 and above Computer Group | A group containing all computers that are running Windows Server 2016 or above operating systems. |
| Windows Server 2016 Computer Group (Full) | A group containing all computers that are running a Windows Server 2016 Full version of the Windows operating system |
| Windows Server 2016 and above Computer Group (Core) | A group containing all computers that are running a Windows Server 2016 or above operating systems Core installation type of the Windows operating system. |
| Windows Server 2016 Computer Group (Nano) | A group containing all computers that are running a Windows Server 2016 Nano installation type of the Windows operating system. |
| Windows Server Instances Group | A group containing any instances of the Windows Server classes such as logical disk, physical disk, disk partition network adapter, or processor |

## Objects the Management Pack Discovers

By default, the System Center Management Pack for Windows Server 2016 and above operating systems will discover the following objects:

 Operating systems

 Logical disks

 Cluster Shared Volumes

 Disk partitions containing logical partitions

 Physical disks containing a disk partition

 Network adapter

The following objects are not discovered by default but can be discovered if Object Discoveries is enabled using overrides.

 Physical disks

 Processor

 Disk partitions

* Mount Points

## Upgrade an Operating System: How to Prevent Discovery Problems

Best Practice: Before you upgrade the operating system on a monitored computer, uninstall the Operations Manager agent. After the upgrade, reinstall the Operations Manager agent.

Explanation: The objects that the management pack discovers, such as logical disks, are hosted by a parent class that is not version-specific. When you upgrade the operating system, the order in which discovery occurs can result in duplicate objects being discovered.

If you upgrade a computer without uninstalling the agent first and then discover duplicate objects, uninstall the agent to mark all hosted objects as deleted in the database. Next, reinstall the agent to discover existing applications/objects only.

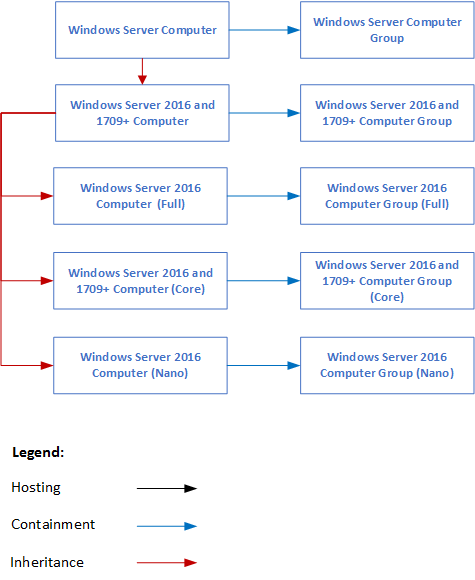
## Classes

The following table describes the available classes:

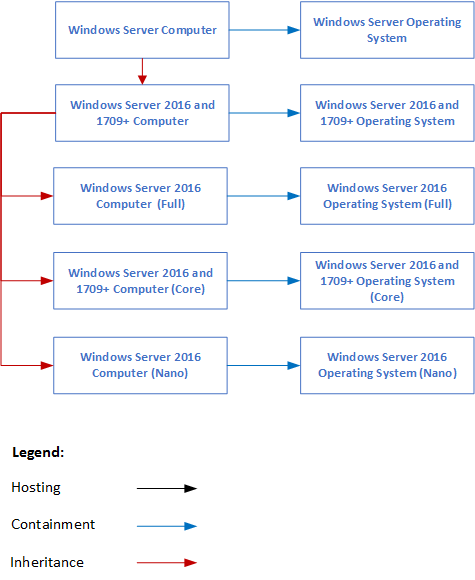
|  |  |
| --- | --- |
| Available Classes | Description |
| Windows Server 2016 and above Computer | All instances of computers running Windows Server 2016 and above operating systems. |
| Windows Server 2016 Computer (Full) | All instances of computers running the Windows Server 2016 Full installation type of the operating system. |
| Windows Server 2016 and above Computer (Core) | All instances of computers running Windows Server 2016 and above operating systems' Core installation type of the operating system. |
| Windows Server 2016 Computer (Nano) | All instances of computers running the Windows Server 2016 Nano installation type of the operating system. |
| Windows Server 2016 and above Operating System | All instances of Windows Server 2016 and above operating systems. |
| Windows Server 2016 Operating System (Full) | All instances of the Windows Server 2016 Full installation type of the operating system. |
| Windows Server 2016 and above Operating System (Core) | All instances of Windows Server 2016 or above operating systems Core installation type of the operating system. |
| Windows Server 2016 Operating System (Nano) | All instances of the Windows Server 2016 Nano installation type of the operating system. |
| Windows Server 2016 and above Computer Group | A group containing all computers that are running Windows Server 2016 or above operating systems. |
| Windows Server 2016 Computer Group (Full) | A group containing all computers that are running a Windows Server 2016 Full version of the Windows operating system. |
| Windows Server 2016 and above Computer Group (Core) | A group containing all computers that are running Windows Server 2016 or above operating systems. |
| Windows Server 2016 Computer Group (Nano) | A group containing all computers that are running a Windows Server 2016 Nano installation type of the Windows operating system. |
| Windows Server 2016 and above Disk Partition | All instances of a disk partition on Windows Server 2016 or above operating systems. |
| Windows Server 2016 and above Logical Disk | All instances of a logical disk on Windows Server 2016 or above operating systems. |
| Windows Server 2016 and above Network Adapter | All instances of a network adapter on Windows Server 2016 or above operating systems. |
| Windows Server 2016 and above Physical Disk | All instances of a physical disk on Windows Server 2016 or above operating systems. |
| Windows Server 2016 and above Processor | All instances of a processor on Windows Server 2016 or above operating systems. |
| Windows Server Process Monitoring Seed | All instances of a Windows Server 2016 Operating System with the exception of Nano Server |

## How Health Rolls Up

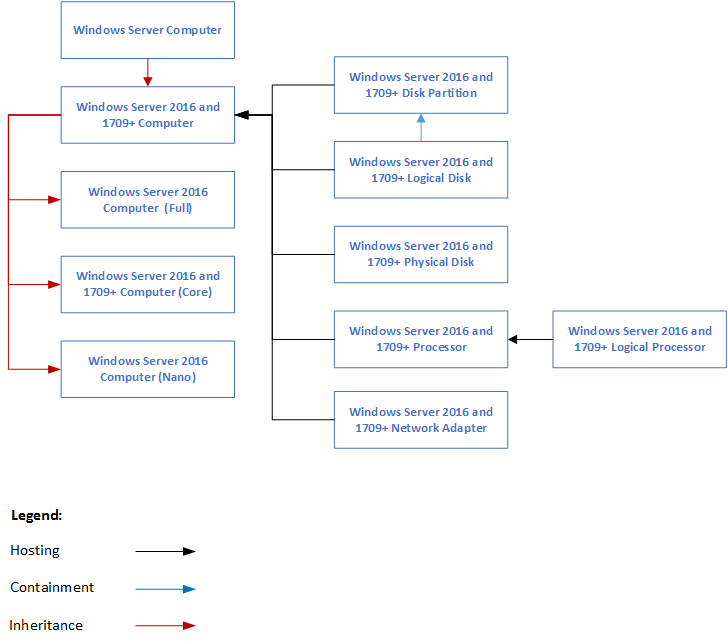
The following diagrams explain how health rolls up within Windows Server 2016 and above operating systems management pack. Health model of this management pack is complicated so it is divided into logical parts.



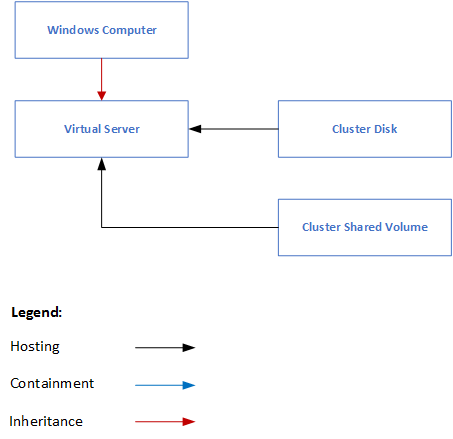
*Diagram 1. Windows Server OS Management Pack Health Rollup 1 of 4*



*Diagram 2. Windows Server OS Management Pack Health Rollup 2 of 4*



*Diagram 3. Windows Server OS Management Pack Health Rollup 3 of 4*



*Diagram 4. Windows Server OS Management Pack Health Rollup 4 of 4*

## Troubleshooting and Known Issues

The following issues have been identified in the System Center Management Pack for Windows Server 2016 and above operating systems.

Known Issue: Disk partitions corresponding to mounted disks are not monitored

Issue: Disk partition discovery is not enabled by default, but when enabled, disk partitions that correspond to mounted disks cannot be monitored properly and will show up as “Not Monitored” in the Operations Console. Management is still provided by way of other means in this management pack, but the disk partition perspective will not work in these instances.

Workaround: There is no workaround currently available.

Known Issue: SUBST drive mappings are not supported by logical disk monitoring

Issue: There is a command-line tool (SUBST.exe) that can be used to associate a path (such as c:\windows\system32) with a drive letter (such as D:\). Because these mappings are exposed in WMI, logical disk monitoring discovers them and attempts to monitor them as such, but will subsequently generate errors.

Workaround: There is no workaround currently available, and this configuration is not supported.

Known Issue: Cluster disks managed by third-party software are not monitored

Issue: If the Cluster disks are managed by a third-party software, and they change the resource type to anything other than “Physical Disk”, these disks will be discovered but we do not provide monitoring for these.

Workaround: There is no workaround currently available. In future, the discovery of these will be also removed.

Known Issue: Some objects may be missing in dashboard view during rediscovering upon the management pack update.

Issue: When the management pack is updated to version 10.0.3.0, some objects (Cluster Disks and Cluster Shared Volumes) may be missing in dashboard view during rediscovering.

Workaround: The objects will appear in dashboard view again after some time (within 24 hours by default). Otherwise, the following discovery rules should be overridden:

* Cluster Name Discovery
* Cluster Shared Volume Discovery
* Cluster Disks Discovery

Known Issue: Cluster disks discovery

Issue: Cluster disks are discovered only for cluster groups that have network name resource.

Workaround: No workaround.

Cluster network name resource state Known Issue.

Issue: When a network name resource is taken offline, the cluster disks related to the same cluster group are displayed, but performance counters are not collected and the discovery does not work.

Workaround: No workaround.

Cluster disks state Known Issue.

**Issue:** When cluster disks are taken offline, they are rediscovered with different names (e.g. \\?\GLOBALROOT\Device\HarddiskX\PartitionY\).

Workaround: No workaround.

Known Issue: Offline Cluster Shared Volume is not displayed in the Operations Manager.

**Issue:** If Cluster Shared Volume is offline, it is not displayed in the Operations Manager console. The issue was fixed for Nano server clusters, but it is still relevant for Server Core and full server version.

Workaround: As soon as Cluster Shared Volume comes online and is discovered, it will be displayed in the Operations Manager again. Please note that discovery is performed on a certain schedule, and rediscovery may take some time.

Known Issue: Cluster Shared Volume State monitor does not work correctly if Cluster Shared Volume goes offline.

**Issue:** If Cluster Shared Volume goes offline for a certain period, Cluster Shared Volume State monitor may work incorrectly (the displayed monitor state may not reflect the actual situation).

Workaround: Wait until Cluster Shared Volume is rediscovered while it is online. Please note that discovery is performed on a certain schedule, and rediscovery may take some time.

Known Issue: Cluster Shared Volume objects will be re-discovered with a new key value upon the management pack upgrade.

Issue: Upon upgrade of the MP to version 10.0.8.0, Cluster Shared Volume objects will be re-discovered with a new key value and will have different names (e.g. CSV\_C:\ClusterStorage\VolumeX instead of CSV).

Workaround: No workaround.

Known Issue: SCOM may stop discovery of clusters and cluster groups.

Issue: SCOM may stop launching discovery on virtual agentless computers that represent clusters and cluster groups. In most cases, the issue arises when cluster groups are moved from one cluster node to another, or network resource name of the cluster group is changed.

Workaround: If possible, move the affected resource to the initial node, or return its initial network resource name. Then, clear the agent’s cache and restart the agent to make the discovery work.

Known Issue: Mount point discovery may work incorrectly.

Issue: In some cases, volume identifier of a cluster disk does not match with volume identifier of a logical disk; therefore, the discovery may work incorrectly: a cluster disk may be discovered as a logical disk. It may be connected with OS operation specifics.

Workaround: No workaround.

Known Issue: "Cluster Disc – Free Space Monitor (MB)” changes its state to “Critical” when the cluster disk is offline.

Issue: When a cluster disk is offline, “Cluster Disc – Free Space Monitor (MB)” changes its state to “Critical”.

Workaround: No workaround.

Known Issue: "Run Chkdsk with Full option" and "Run Chkdsk with Spot Fix option" tasks cannot run.

Issue: On some disks storing system services and applications, "Run Chkdsk with Full option" and "Run Chkdsk with Spot Fix option" tasks may require user action: the tasks cannot run, as long as the selection of “yes” or “no” options is required.

Workaround: No workaround.

Known Issue: "Run Chkntfs" task is not supported on Nano Server.

Issue: "Run Chkntfs" task is not supported on Nano Server; if the user starts the task for Nano Server on Windows Server 2016, a corresponding output message is displayed.

Workaround: No workaround.

Known Issue: Performance metrics are not collected for GUID mount points on Nano Server.

Issue: For GUID mount points on Nano Server, no performance metrics are collected; no monitors are working, except for Free Disk Space monitor.

Workaround: No workaround.

Known Issue: On Windows Server 2016, partitions without mount points and drive letters will not be populated.

Issue: Partitions without mount points and drive letters will not be populated on Windows Server 2016.

Workaround: No workaround.

Known Issue: Performance instance for a physical disk on a cluster node may be generated incorrectly.

Issue: Performance instance for a physical disk on a cluster node may be generated incorrectly if the disk was moved or was offline for some time.

Workaround: No workaround.

Known Issue: Physical Disk-to-Disk Partition Discovery Rule may work incorrectly.

Issue: If both Discover Windows Physical Disks and Discover Windows Disk Partitions discoveries are not enabled simultaneously, Physical Disk to Disk Partition Discovery Rule may work incorrectly.

Workaround: Make sure that both discoveries mentioned above are enabled.

Known Issue: Physical Disk-to-Disk Partition discovery in cluster environment may go wrong.

Issue: As long as clustered resources tend to be occasionally moved from one node to another while the discovery of relations between the resources is run according to a schedule, a certain inconsistency may appear in the discovery results.

Workaround: Make sure that the discovery is run while no resources’ movement is performed.

Known Issue: Logical Disk Fragmentation Level monitor may work incorrectly for some configurations.

Issue: For virtual machines (e.g. Azure), defragmentation data may be sent by operating systems incorrectly (empty data); in this case, Logical Disk Fragmentation Level monitor will always be displayed as healthy.

Workaround: No workaround.

Known Issue: Output for some tasks is returning wrong path value.

Issue: Output for some tasks (Display Server Statistics, Display Workstation Statistics) is returning “\\” instead of the computer name.

Workaround: No workaround.

Known Issue: After repartition, previously discovered Cluster Shared Volume partitions are displayed instead of new ones in the Operations Manager (Windows Server 2016).

Issue: After repartition, previously discovered Cluster Shared Volume partitions are displayed instead of new ones in the Operations Manager, if this Cluster Shared Volume has been repartitioned, but has not been previously formatted. The issue is observed on Windows Server 2016.

Workaround: Format and repartition the Cluster Shared Volume.

Known Issue: View Best Practices Analyzer Compliance Results task does not work on Nano Server.

Issue: On Nano Server, View Best Practices Analyzer Compliance Results task will not work, and the monitor will always be displayed as “Healthy”, as long as Nano Server does not support BPA PowerShell module. Besides, it will not work on Windows Server 2016, if BPA monitor is not enabled for the task.

Workaround: No resolution for Nano Server. On Windows Server 2016, enable BPA monitor if necessary.

Known Issue: Incorrect discovery of Windows Server Operating System on Windows Server 2016 agentless cluster computers may occur upon management pack upgrade.

Issue: Incorrect discovery of Windows Server Operating System on Windows Server 2016 agentless cluster computers may occur upon upgrade from version 10.0.2.0 of the management pack. Previously discovered Windows Server Operating System on Windows Server 2016 agentless cluster computers (Cluster Instances and Cluster Groups) is saved after the update. Logical disks, CPUs, network adapters, disk partitions are discovered repeatedly: for Agentless Managed virtual cluster computers (Cluster Instances and Cluster Groups) and Agent Managed cluster node computers.

Workaround: To remove the improperly discovered entities, perform the following actions: in the Operations Manager, open “**Discovery Inventory**” folder and select “**Change Target Type..**” action in the Tasks pane on the right. As a result, “**Select Items to Target**” dialog menu will be displayed. In this menu, choose “**View all targets**” option, select “**All Management Servers Resource Pool**” and click OK button. After that, run “**Undiscovery of improper Windows cluster objects [2016]**” task from the Tasks pane. Please note that to run this task, you can use either the predefined Run As account or another specific Run As account. Make sure that the Run As account you use is included in the Operations Manager Administrators user role. Therefore, if you prefer to use a specific Run As account (other than the predefined one), do not forget to enter the account credentials in the corresponding fields of the task dialog menu. After that, click Run button. Upon completion of the task, the results will be displayed in the dialog menu. If any artifacts are still present, run the task once again.

Known Issue: Nano Server cluster health discoveries may be duplicated after MP upgrade.

Issue: Nano Server Cluster Disk and Nano Server Cluster Shared Volumes health discoveries may be duplicated after MP upgrade from version 10.0.2.0 to a newer one.

Workaround: Wait until the discovery is completed. If any duplicates are still present, use a special task (**Undiscovery of legacy cluster objects for Nano Server**) to fix the issue. The task is provided to search for new Nano Server cluster objects, and if the objects are found, it gets all the previous Nano Server cluster objects, performs a comparison and removes the older duplicated objects.

Known Issue: Some disk partitions are displayed as “Not monitored”.

Issue: If a disk partition does not have a logical disc, it is displayed as "Not monitored", even if the discovery is enabled.

Workaround: No workaround.

Known Issue: PowerShell script based discoveries fail to run on Nano Agent.

Issue: Any discovery based on a PowerShell script stops working on Nano Agent; at that, a corresponding warning alert is received: "PowerShell Script failed to run".

Workaround: Disable "Agent Initiated Maintenance Mode" rule. To do that, follow these steps:

1. In SCOM console, go to **Authoring -> Rules**.
2. Look for “**Agent Initiated Maintenance Mode**”. Select the rule.
3. Go to overrides: **->** **Override the Rule -> For all Objects of class: Agent**.
4. Set override value to “False”.
5. Click "New" button to create a new management pack.
6. Apply the override.

Known Issue: Nano Agent periodically stops collecting Performance Counters.

Issue: Nano Agent periodically stops collecting Performance Counters; at that, corresponding gaps appear in the graphs.

Workaround: Override the following monitors:

* Health Service Handle Count Threshold
* Health Service Private Bytes Threshold
* Monitoring Host Private Bytes Threshold
* Monitoring Host Handle Count Threshold

Set the threshold value to >= 700 MB.

Known Issue: Network Adapter Connection Health monitor does not work on Nano Server.

Issue: Network Adapter Connection Health monitor looks for the events related to the connection health in the system event log. As long as Nano Server does not create any corresponding events (e.g. regarding media disconnection etc.), the monitor never changes its state (remains always 'Healthy").

Workaround: In order to get the real current state of the monitor, go to Health Explorer, select the monitor and click “Recalculate Health” button.

Known Issue: Performance collection rules of total used, read and write network adapter bandwidth may stop collecting data.

Issue: Performance collection rules of total used, read and write network adapter bandwidth may stop collecting data. It may be caused by possible problem with WMI functionality. The following alerts can be shown:

*System.Management.Automation.CmdletInvocationException: Illegal operation attempted on a registry key that has been marked for deletion.At line:169 char:18*

*+ ... oInstance = Get-CimInstance -ComputerName $sTargetComputer -Namespace ...*

*+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~*

*at System.Management.Automation.Runspaces.PipelineBase.Invoke(IEnumerable input)*

*at Microsoft.EnterpriseManagement.Common.PowerShell.RunspaceController.RunScript[T](String scriptName, String scriptBody, Dictionary`2 parameters, Object[] constructorArgs, IScriptDebug iScriptDebug, Boolean bSerializeOutput)*

*Script Name: Microsoft.Windows.Server.NetworkAdapter.BandwidthUsed.ModuleType.ps1*

Workaround: Run Get-ciminstance Win32\_PerfFormattedData\_Tcpip\_NetworkAdapter command in PowerShell to check if the performance data is collected correctly. If successful, restart Microsoft Monitoring agent. Otherwise, check WMI operation on the agent and resolve all discovered issues.

Known Issue: Cluster Shared Volume NTFS State Monitor does not switch to Critical state.

Issue: Cluster Shared Volume NTFS State Monitor always remains in the Healthy state, even if its real state is critical.

Workaround: No workaround.

Known Issue: Windows Server 2016 Operating System BPA Monitor results may differ from those of the server UI BPA.

Issue: The results of Windows Server 2016 Operating System BPA Monitor may differ from those presented by the server UI Best Practice Analyzer.

Workaround: No workaround.

Known Issue: Active Alerts’ icons are not displayed in the default view.

Issue: When the user cache is cleared, Active Alerts’ icons are not displayed in the default view.

Workaround: Apply “Reset to Default” option via “Personalize view…” menu.

Known Issue: Performance Alerting Rule causes a SCOM error when the threshold and samples values are set too low.

Issue: When the threshold and samples values are set too low for Performance Alert Rule (e.g. for Process Monitoring: High Handle Count Alert Rule samples = 1 and threshold = 50%), it may lead to multiple unclosed alerts and the following SCOM error: “Data was dropped due to too much outstanding data in rule …”)

Workaround: Restart the Health Service to re-enable data synchronization.

Known Issue: Data warehouse stored procedure deadlock.

Issue: You may see the following error in the event log with id 31552:

*Exception 'SqlException': Sql execution failed. Error 777971002, Level 13, State 1, Procedure PerformanceProcessStaging, Line 608, Message: Sql execution failed. Error 1205, Level 13, State 51, Procedure PerformanceProcessStaging, Line 441, Message: Transaction (Process ID 125) was deadlocked on lock resources with another process and has been chosen as the deadlock victim. Rerun the transaction.*

One or several workflows may be affected:

*Workflow name: Microsoft.SystemCenter.DataWarehouse.StandardDataSetMaintenance*

*Instance name: Process Monitoring: Performance Metric  State data warehouse dataset*

*Instance ID: {80F53A0A-1B63-3D68-7C1E-2795469FECA0}*

*Management group: scom16sql16*

Workaround: Increase Standard Data Set Data Warehouse maintenance rule’s Maintenance Frequency Seconds parameter and make it different for the data sets as described in [Troubleshooting and Customization](#_Troubleshooting_and_Customization) section.

Known Issue: Could not find stored procedure ‘sdk.ProcessMonitoring\_Microsoft\_Window\_Server\_GetProcessMetricAndState’.

Issue: When you first import Process and Port Monitoring Pack, you may see the following error in the event log and in Process dashboard:

*An exception was thrown while processing GetDataWarehouseStoredProcedureResult for session ID uuid:949a70e3-b6ac-4bfe-9362-2141fba39c16;id=10.*

*Exception message: The creator of this fault did not specify a Reason.*

*Full Exception: System.ServiceModel.FaultException`1[Microsoft.EnterpriseManagement.Common.UnknownDatabaseException]: The creator of this fault did not specify a Reason. (Fault Detail is equal to Could not find stored procedure 'sdk.ProcessMonitoring\_Microsoft\_Window\_Server\_GetProcessMetricAndState'.).*

The reason for this error is that the data set deployment has not been completed yet.

Workaround: Wait 5-10 minutes until data set deployment is completed.

Known Issue: Could not find stored procedure ‘sdk.ProcessMonitoring\_Microsoft\_Window\_Server\_GetPortState’.

Issue: When you first import Process and Port Monitoring Pack, you may see the following error in the event log and in Port dashboard:

*An exception was thrown while processing GetDataWarehouseStoredProcedureResult for session ID uuid:949a70e3-b6ac-4bfe-9362-2141fba39c16;id=10.*

*Exception message: The creator of this fault did not specify a Reason.*

*Full Exception: System.ServiceModel.FaultException`1[Microsoft.EnterpriseManagement.Common.UnknownDatabaseException]: The creator of this fault did not specify a Reason. (Fault Detail is equal to Could not find stored procedure 'sdk.ProcessMonitoring\_Microsoft\_Window\_Server\_GetPortState'.).*

The reason for this error is that data set deployment have not completed yet.

Workaround: Wait 5-10 minutes until data set deployment is completed.

Known Issue: Processes with long names are not monitored.

Issue: There are certain limits for the key fields in the database. Therefore, processes with names longer than 256 characters will not be monitored. This is also true for usernames: processes run by a user with name exceeding the limit stated above will not be monitored.

Workaround: Avoid using long process and usernames.

Known Issue: Alerts are closed if overrides are applied to the alert rules

Issue: If overrides are applied to the rules stated below, the alerts opened by those rules are closed. Those rules are as follows:

* Process Monitoring: High Handle Count
* Process Monitoring: High Processor Time Percentage
* Process Monitoring: High Memory Percentage

Workaround: No workaround. New alerts will arise within the specified interval if the monitored processes still exceed the conditions set for the alert rules.

Known Issue: Health State of the process is reset if overrides are applied to Health State Collection rule

Issue: If overrides are applied to Process Monitoring: Health State Collection rule, the state of the process is reset on the Process Dashboard.

Workaround: No workaround. Health state of the process will be changed within the specified interval according to the current conditions.

Known Issue: Error 31552 may appear in case of a large dataset

Issue: In case of a large dataset, error with id 31552 may appear in the event log.

Workaround: Increase the Maintenance Frequency Seconds parameter of the Standard Data Warehouse Data Set maintenance rule.

Known Issue: The dashboard may fail with a timeout error while refreshing

Issue: While refreshing, the dashboard may occasionally fail with the "26319" timeout error.

Workaround: Restart the Operations Console; you may also decrease the refresh interval for the dashboard by editing the "PollingInterval" parameter in the following registry key: *HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\Console\CacheParameters*.   
The default value for this parameter is 1 and corresponds to 15 seconds refresh interval. The maximal value is 10 and corresponds to 2 minutes and 30 seconds refresh interval. The zero value switches the automatic refresh off.

Known Issue: The Health Service may be restarted when Handle Count reaches 6000

Issue: In some cases, Handle Count may reach 6000; at that, the Health Service restarts after reaching the default 6000 threshold set for the “Monitoring Host Handle Count Threshold” monitor.

Workaround: To prevent the Health Service restarting, increase the Monitoring Host Handle Count Threshold for the corresponding agent.

Known Issue: The dashboard may display only a part of the processes

Issue: In case of a large number (over 1024) of monitored processes, the dashboard may periodically display only a part of the processes for some time. This happens because the information is loaded parcelwise.

Workaround: Refresh the dashboard.

## Appendix: Management Pack Objects and Workflows

### (Abstract) Cluster Disk

Cluster Disks on failover clusters (Windows Server 2008 and higher). A cluster disk is accessible for all cluster nodes at the same time and managed in an automated FSMO mode.

**(Abstract) Cluster Disk - Aggregate monitors**

**[Nano Server] Cluster Disk - Free Space Rollup Monitor**

This monitor aggregates the free space monitors for cluster disks on Nano Server.

### (Abstract) Cluster Shared Volume

Cluster Shared Volumes on failover clusters (Windows 2008 R2 and higher). A cluster shared volume is accessible for all cluster nodes at the same time and managed in an automated FSMO mode.

**(Abstract) Cluster Shared Volume - Aggregate monitors**

**[Nano Server] Cluster Shared Volume - Free Space Rollup Monitor**

This monitor aggregates the free space monitors for cluster shared volumes on Nano Server.

### [Nano Server] Cluster Disk

Cluster Disks on failover clusters (Nano Server). A cluster disk is accessible for all cluster nodes at the same time and managed in an automated FSMO mode.

**[Nano Server] Cluster Disk - Discoveries**

**[Nano Server] Cluster Disks Discovery**

Discover instances of the cluster disks.

**[Nano Server] Cluster Disk - Unit monitors**

**[Nano Server] Cluster Disk - Free Space Monitor (MB)**

This monitor checks the free space in MB of the targeted cluster disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Error Threshold |  | 100 | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log on Success |  | true | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | | Warning Threshold |  | 500 | |  |
|  |  |  |

**[Nano Server] Cluster Disk - Free Space Monitor (%)**

This monitor checks the free space in % of the targeted cluster disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Error Threshold |  | 5 | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log on Success |  | true | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | | Warning Threshold |  | 10 | |  |
|  |  |  |

**[Nano Server] Cluster Disk - Rules (non-alerting)**

**[Nano Server] Cluster Disk - Free space / MB**

This rule collects the 'Free space / MB' performance counter for a Cluster disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**[Nano Server] Cluster Disk - Total size / MB**

This rule collects the 'Total size / MB' performance counter for a Cluster disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**[Nano Server] Cluster Disk - Free space / %**

This rule collects the 'Free space / %' performance counter for a Cluster disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

### [Nano Server] Cluster Shared Volume

Cluster Shared Volumes on failover clusters (Nano Server). A cluster shared volume is accessible for all cluster nodes at the same time and managed in an automated FSMO mode.

**[Nano Server] Cluster Shared Volume - Discoveries**

**[Nano Server] Cluster Shared Volume Discovery**

Discover instances of the cluster shared volume class hosted on the cluster virtual server representing the cluster on Nano Server. A cluster shared volume is accessible for all cluster nodes at the same time and managed in an automated FSMO mode.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 86400 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**[Nano Server] Cluster Shared Volume - Unit monitors**

**[Nano Server] Cluster Shared Volume - Free Space Monitor (%)**

This monitor checks the free space in % of the targeted cluster shared volume.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Error Threshold |  | 5 | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log on Success |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | | Warning Threshold |  | 10 | |  |
|  |  |  |

**[Nano Server] Cluster Shared Volume - Free Space Monitor (MB)**

This monitor checks the free space in MB of the targeted cluster shared volume.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Error Threshold in MB |  | 100 | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log on Success |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | | Warning Threshold in MB |  | 500 | |  |
|  |  |  |

**[Nano Server] Cluster Shared Volume - NTFS State Monitor**

This monitor checks the state of the file system on the targeted cluster shared volume.

**[Nano Server] Cluster Shared Volume - State Monitor**

This monitor checks the state of the targeted cluster shared volume.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log on Success |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**[Nano Server] Cluster Shared Volume - Rules (non-alerting)**

**[Nano Server] Cluster Shared Volume - Total size / MB**

This rule collects the 'Total size / MB' performance counter for a Cluster Shared Volume.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**[Nano Server] Cluster Shared Volume - Free space / MB**

This rule collects the 'Free space / MB' performance counter for a Cluster Shared Volume.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**[Nano Server] Cluster Shared Volume - Free space / %**

This rule collects the 'Free space / %' performance counter for a Cluster Shared Volume.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

### [Nano Server] Windows Cluster disk monitoring seed

Nano Server Cluster Seed class used by the Nano Server Operating Management Pack to do disk monitoring on Windows Clusters

**[Nano Server] Windows Cluster disk monitoring seed - Discoveries**

**[Nano Server] Cluster Seed Name Discovery**

Discover instances of the cluster name class. This class is hosted on the cluster virtual server representing the cluster. This creates a target running on a single cluster node of a cluster only.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 86400 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

### Cluster Disk

Cluster Disks on failover clusters (Windows Server 2008 and higher). A cluster disk is accessible for all cluster nodes at the same time and managed in an automated FSMO mode.

**Cluster Disk - Discoveries**

**Cluster Disks Discovery**

Discover instances of the cluster disks.

**Cluster Disk - Unit monitors**

**Cluster Disk - Free Space Monitor (MB)**

This monitor checks the free space in MB of the targeted cluster disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Error Threshold |  | 100 | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log on Success |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | | Warning Threshold |  | 500 | |  |
|  |  |  |

**Cluster Disk - Free Space Monitor (%)**

This monitor checks the free space in % of the targeted cluster disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Error Threshold |  | 5 | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log on Success |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | | Warning Threshold |  | 10 | |  |
|  |  |  |

**Cluster Disk - Aggregate monitors**

**Cluster Disk - Free Space Rollup Monitor**

This monitor aggregates the free space monitors for cluster disks.

**Cluster Disk - Rules (alerting)**

**Windows Server NTFS File System Corrupt Rule**

This rule generates alerts base on system events that indicates a NTFS File System Corruption.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | Yes | | Priority | Defines Alert Priority. | 1 | | Severity | Defines Alert Severity. | 1 | |  |
|  |  |  |

**Cluster Disk - Rules (non-alerting)**

**Collection Rule for Total size / MB Windows Server Cluster Disk**

This rule collects the 'Total size / MB' performance counter for a Cluster disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Collection Rule for Split I/O Per Second Windows Server Cluster Disk**

This rule collects the Split I/O Per Second performance counter for a Cluster Disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Collection Rule for Average Disk Seconds Per Read Windows Server Cluster Disk**

This rule collects the Average Disk Seconds Per Read performance counter for a Cluster Disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Collection Rule for Average Disk Seconds Per Transfer Windows Server Cluster Disk**

This rule collects the Average Disk Seconds Per Transfer performance counter for a Cluster Disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Collection Rule for Average Disk Read Queue Length Windows Server Cluster Disk**

This rule collects the Average Disk Read Queue Length performance counter for a Cluster Disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Collection Rule for % Free space Windows Server Cluster Disk**

This rule collects the '% Free space' performance counter for a Cluster disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Collection Rule for Disk Reads Per Second Windows Server Cluster Disk**

This rule collects the 'Disk Reads Per Second' performance counter for a Cluster disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Collection Rule for Disk Read Bytes Per Second Windows Server Cluster Disk**

This rule collects the Disk Read Bytes Per Second performance counter for a Cluster Disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Collection Rule for Average Disk Seconds Per Write Windows Server Cluster Disk**

This rule collects the Average Disk Seconds Per Write performance counter for a Cluster Disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Collection Rule for Free MegaBytes Windows Server Cluster Disk**

This rule collects the 'Free MegaBytes' performance counter for a Cluster disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Collection Rule for Disk Writes Per Second Windows Server Cluster Disk**

This rule collects the Disk Writes Per Second performance counter for a Cluster Disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Collection Rule for Average Disk Write Queue Length Windows Server Cluster Disk**

This rule collects the Average Disk Write Queue Length performance counter for a Cluster Disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Collection Rule for Average Disk Queue Length Windows Server Cluster Disk**

This rule collects the Average Disk Queue Length performance counter for a Cluster Disk

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Collection Rule for % Idle Time Windows Server Cluster Disk**

This rule collects the % Idle Time performance counter for a Cluster disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Collection Rule for Current Disk Queue Length Windows Server Cluster Disk**

This rule collects the Current Disk Queue Length performance counter for a Cluster disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Collection Rule for Disk Write Bytes Per Second Windows Server Cluster Disk**

This rule collects the Disk Write Bytes Per Second performance counter for a Cluster Disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Collection Rule for Disk Bytes Per Second Windows Server Cluster Disk**

This rule collects the Disk Bytes Per Second performance counter for a Cluster Disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

### Cluster Shared Volume

Cluster Shared Volumes on failover clusters (Windows Server 2008 R2 and higher). A cluster shared volume is accessible for all cluster nodes at the same time and managed in an automated FSMO mode.

**Cluster Shared Volume - Discoveries**

**Cluster Shared Volume Discovery**

Discover instances of the cluster shared volume class hosted on the cluster virtual server representing the cluster. A cluster shared volume is accessible for all cluster nodes at the same time and managed in an automated FSMO mode.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Event Log Source |  | ClusterSharedVolumeMonitoring | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 86400 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Cluster Shared Volume - Unit monitors**

**Cluster Shared Volume - NTFS State Monitor**

This monitor checks the state of the file system on the targeted cluster shared volume.

**Cluster Shared Volume - Free Space Monitor (%)**

This monitor checks the free space in % of the targeted cluster shared volume.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Error Threshold |  | 5 | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log on Success |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | | Warning Threshold |  | 10 | |  |
|  |  |  |

**Cluster Shared Volume - Free Space Monitor (MB)**

This monitor checks the free space in MB of the targeted cluster shared volume.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Error Threshold in MB |  | 100 | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log on Success |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | | Warning Threshold in MB |  | 500 | |  |
|  |  |  |

**Cluster Shared Volume - State Monitor**

This monitor checks the state of the targeted cluster shared volume.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log on Success |  | false | | Source |  | ClusterSharedVolumeMonitoring | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Cluster Shared Volume - Aggregate monitors**

**Cluster Shared Volume - Free Space Rollup Monitor**

This monitor aggregates the free space monitors for cluster shared volumes.

**Cluster Shared Volume - Rules (non-alerting)**

**Cluster Shared Volume - Free space / MB**

This rule collects the 'Free space / MB' performance counter for a Cluster Shared Volume.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Event Log Source |  | ClusterSharedVolumeMonitoring | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Cluster Shared Volume - Total size / MB**

This rule collects the 'Total size / MB' performance counter for a Cluster Shared Volume.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Event Log Source |  | ClusterSharedVolumeMonitoring | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Cluster Shared Volume - Free space / %**

This rule collects the 'Free space / %' performance counter for a Cluster Shared Volume.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Event Log Source |  | ClusterSharedVolumeMonitoring | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

### Health Service

This type represents the System Center Health Service.

**Health Service - Rules (non-alerting)**

**Process Monitoring: Process Performance Metric Subscription**

This rule saves Process Performance Metric information to the SCOM data warehouse. To start information collection, make sure that “Process Monitoring: Performance Collection” rule is enabled.

**Process Monitoring: Process Health State Subscription**

This rule saves Process Health State information to the SCOM data warehouse. To start information collection, make sure that “Process Monitoring: Health State Collection” rule is enabled.

**Process Monitoring: Process Network Port Subscription**

This rule saves Process Network Port information to the SCOM data warehouse. To start information collection, make sure that “Process Monitoring: Network Port State Collection” rule is enabled.

### Operations Manager Standard License

This class represents an OpsMgr Standard license.

**Operations Manager Standard License - Discoveries**

**License Discovery for Microsoft Windows Server**

This discovery rule discovers and populates the class named “System Center Operations Manager Standard License"

### Virtual Server

Windows Cluster Virtual Server class

**Virtual Server - Dependency (rollup) monitors**

**Cluster Disk Availability Rollup**

This monitor rolls up the availability state from the cluster disks to the hosting cluster virtual server.

**[Nano Server] Cluster Shared Volumes Availability Rollup**

This monitor rolls up the availability state from the cluster shared volumes to the hosting cluster virtual server on Nano Server.

**Cluster Shared Volumes Availability Rollup**

This monitor rolls up the availability state from the cluster shared volumes to the hosting cluster virtual server.

**[Nano Server] Cluster Disk Availability Rollup**

This monitor rolls up the availability state from the cluster disks to the hosting cluster virtual server on Nano Server.

### Windows Cluster (disk monitoring)

Windows Cluster class used by the Windows Server Operating Management Pack to do disk monitoring on Windows Clusters

**Windows Cluster (disk monitoring) - Discoveries**

**Cluster Seed Name Discovery**

Discover instances of the cluster name class. This class is hosted on the cluster virtual server representing the cluster. This creates a target running on a single cluster node of a cluster only.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Event Log Source |  | ClusterSharedVolumeMonitoring | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 86400 | | Log Successful Event |  | false | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

### Windows Server

Defines the basic properties of computers running Windows Server operating systems

**Windows Server - Aggregate monitors**

**Hardware Availability Aggregate monitor**

This aggregate monitor rolls up the availability health of all hardware hosted on the Windows computer.

**Windows Server - Dependency (rollup) monitors**

**Hardware Performance Rollup**

This monitor rolls up the performance health of all hardware hosted on the Windows computer.

**Operating System Configuration Rollup**

This monitor rolls up the configuration health of the Operating System to the Windows computer.

**Operating System Availability Rollup**

This monitor rolls up the availability health of the Operating System to the Windows computer.

**Operating System Performance Rollup**

This monitor rolls up the performance health of the Operating System to the Windows computer.

**Hardware Availability Rollup**

This monitor rolls up the availability health of all hardware hosted on the Windows computer.

**Windows Server - Console Tasks**

**Computer Management**

Run Computer Management for this computer.

**Remote Desktop (Console)**

Open a remote desktop session to the console on this computer.

**Remote Desktop (Admin)**

Open a remote desktop administration session to this computer.

**Remote Desktop**

Open a remote desktop session to this computer

**Open PowerShell**

Open PowerShell

### Windows Server 2016 and above Computer

All instances of computers running the Windows Server 2016 and above operating systems.

**Windows Server 2016 and above Computer - Discoveries**

**Discover Windows 2016 and above Servers**

This Discovery Rule discovers and populates the Windows Server class named “Windows Server 2016 and above Computer" with instances of computers that are running Windows Server 2016 and above operating systems.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 86400 | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 360 | |  |
|  |  |  |

**Windows Server 2016 and above Computer - Unit monitors**

**Storport Miniport Driver Timed Out Monitor**

The monitor alerts when the Storport miniport driver times out a request

### Windows Server 2016 and above Computer (Core)

All instances of computers running the Windows Server 2016 (Core) and above operating systems.

**Windows Server 2016 and above Computer (Core) - Discoveries**

**Discover Windows 2016 and above Servers**

This Discovery Rule discovers and populates the Windows Server class named “Windows Server 2016 and above Computer" with instances of computers that are running Windows Server 2016 and above operating systems.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 86400 | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 360 | |  |
|  |  |  |

### Windows Server 2016 and above Disk Partition

All instances of a disk partition on Windows Server 2016 and above operating systems.

**Windows Server 2016 and above Disk Partition - Discoveries**

**Discover Windows Disk Partitions**

This rule uses WMI to discover all disk partitions of Windows Server 2016 and above operating systems.

**Windows Server 2016 and above Disk Partition - Dependency (rollup) monitors**

**Logical Disk Availability Rollup**

This monitor rolls up the availability of Logical Disk

**Logical Disk Performance Rollup**

This monitor roles up the performance of Logical Disk

**Windows Server 2016 and above Disk Partition - Console Tasks**

**Start Computer Management Console**

This task starts the Computer Management console.

### Windows Server 2016 and above Logical Disk

All instances of a logical disk on Windows Server 2016 and above operating systems.

**Windows Server 2016 and above Logical Disk - Discoveries**

**Mount Point Discovery Rule**

This Discovery Rule discovers and populates the Windows Server Class named “Windows Server 2016 and above Logical Disk" with instances of Mount Points that are discovered on Windows Server 2016 and above operating systems.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 86520 | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 360 | |  |
|  |  |  |

**Discover Windows Logical Disks**

This Discovery Rule discovers and populates the Windows Server Class named “Windows Server 2016 and above Logical Disk" with instances of Logical Disks (for example C:, D:) that are discovered on Windows Server 2016 and above operating systems. Please note that only Local Disks are detected. Logical Disks that are classified as Removable, Compact Disk, Network Drive, and RAM Disks are excluded.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 86460 | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 360 | |  |
|  |  |  |

**Windows Server 2016 and above Logical Disk - Unit monitors**

**Average Disk Seconds Per Write (Logical Disk)**

Monitor the performance counter LogicalDisk\Avg Disk Sec Per Write

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 60 | | Number of Samples |  | 15 | | Threshold |  | 0.04 | |  |
|  |  |  |

**Average Logical Disk Seconds Per Transfer**

Monitor the performance counter LogicalDisk\Avg Disk Sec Per Transfer

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 60 | | Number of Samples |  | 15 | | Threshold |  | 0.04 | |  |
|  |  |  |

**Average Logical Disk Seconds Per Read**

Monitor the performance counter LogicalDisk\Avg Disk Sec Per Read

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 60 | | Number of Samples |  | 15 | | Threshold |  | 0.04 | |  |
|  |  |  |

**Logical Disk Percent Idle Time**

Monitor the performance counter LogicalDisk\% Idle Time

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Number of Samples |  | 24 | | Threshold |  | 20 | |  |
|  |  |  |

**Logical Disk Free Space (%) Low**

Monitor the percentage of free space remaining on a logical disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Error Threshold for Non-System Drives | Error Threshold for Non-System Drives | 5 | | Error Threshold for System Drives | Error Threshold for System Drives | 5 | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Number of samples | Number of samples the monitor has to be above the threshold before alerting. | 4 | | Warning Threshold for Non-System Drives | Warning Threshold for Non-System Drives | 10 | | Warning Threshold for System Drives | Warning Threshold for System Drives | 10 | |  |
|  |  |  |

**[Deprecated] Logical Disk Free Space**

Monitors the percentage free space and number of free MBytes remaining on a logical disk. Only when both the low percentage free space and low number of free MBytes thresholds are reached, the disk is flagged as having low disk free space.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Error % Threshold for Non-System Drives | Error % Threshold for Non-System Drives | 5 | | Error %Threshold for System Drives | Error % Threshold for System Drives | 5 | | Error Mbytes Threshold for Non-System Drives | Error Mbytes Threshold for Non-System Drives | 1000 | | Error MBytes Threshold for System Drives | Error MBytes Threshold for System Drives | 300 | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Warning % Threshold for Non-System Drives | Warning % Threshold for Non-System Drives | 10 | | Warning % Threshold for System Drives | Warning % Threshold for System Drives | 10 | | Warning MBytes Threshold for System Drives | Warning MBytes Threshold for System Drives | 500 | | Warning threshold in MBytes for the non-system drives | Warning threshold in MBytes for the non system drives. | 2000 | |  |
|  |  |  |

**Current Disk Queue Length (Logical Disk)**

Monitor the performance counter LogicalDisk\Current Disk Queue Length

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Number of Samples |  | 12 | | Threshold |  | 32 | |  |
|  |  |  |

**Logical Disk Free Space Monitor**

Monitors the percentage free space and number of free MBytes remaining on a logical disk. Only when both the low percentage free space and low number of free MBytes thresholds are reached, the disk is flagged as having low disk free space.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Debug Flag | This setting enables the module to log different events at running time | false | | Error % Threshold for Non-System Drives | Error % Threshold for Non-System Drives | 5 | | Error %Threshold for System Drives | Error % Threshold for System Drives | 5 | | Error Mbytes Threshold for Non-System Drives | Error Mbytes Threshold for Non-System Drives | 1000 | | Error MBytes Threshold for System Drives | Error MBytes Threshold for System Drives | 300 | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 3600 | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 360 | | Warning % Threshold for Non-System Drives | Warning % Threshold for Non-System Drives | 10 | | Warning % Threshold for System Drives | Warning % Threshold for System Drives | 10 | | Warning MBytes Threshold for System Drives | Warning MBytes Threshold for System Drives | 500 | | Warning threshold in MBytes for the non-system drives | Warning threshold in MBytes for the non system drives. | 2000 | |  |
|  |  |  |

**Logical Disk Free Space (MB) Low**

Monitor the number of free MBytes remaining on a logical disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Error Threshold for Non-System Drives | Error Threshold for Non-System Drives | 1000 | | Error Threshold for System Drives | Error Threshold for System Drives | 300 | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Number of samples | Number of samples the monitor has to be above the threshold before alerting. | 4 | | Warning Threshold for Non-System Drives | Warning Threshold for Non-System Drives | 2000 | | Warning Threshold for System Drives | Warning Threshold for System Drives | 500 | |  |
|  |  |  |

**File system error or corruption**

Monitors whether the file system has reported an error with the file system or corruption on the logical disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Interval seconds | The recurring interval of time in seconds in which to run the workflow. | 3600 | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Logical Disk Fragmentation Level**

This monitor runs on a periodic basis (Every Saturday at 3 a.m. by default) to check the fragmentation levels of all logical drives. If fragmentation levels are found to be above threshold then by default the state of the monitor will change to "Warning" and an alert will be generated. There is a recovery named "Logical Disk Defragmentation" targeted to this monitor, which is disabled by default. If the recovery is enabled then the state change will automatically kick off a task to defragment the logical drive.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Days Of Week mask | The day(s) that the fragmentation check should be run. The values for the days are Sunday (1), Monday (2), Tuesday (4), Wednesday (8), Thursday (16), Friday (32) and Saturday (64). To specify multiple days, add the values for the days together. For example, for Monday, Wednesday, and Friday, specify 42 (2+8+32). | 64 | | File Percent Fragmentation Threshold | If the "Use OS Recommendation" is set to "False" then this value will be used as the threshold for fragmentation levels. | 10 | | Start time | The time of the day (HH:MM) that the fragmentation check should be run | 03:00 | | Use OS Recommendation | This parameter determines whether the fragmentation level check will use the default threshold determined by the operating system or not. If this parameter is set to "False" then the value from "File Percent Fragmentation Threshold" will be used. | true | |  |
|  |  |  |

**Windows Server 2016 and above Logical Disk - Aggregate monitors**

**Logical Disk - Free Space Rollup Monitor**

This monitor aggregates the free space monitors for cluster disks.

**Windows Server 2016 and above Logical Disk - Rules (alerting)**

**Windows Server 2016 and above NTFS File System Corrupt Rule**

This rule generates alerts base on system events that indicates a NTFS File System Corruption.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | Yes | | Priority | Defines Alert Priority. | 1 | | Severity | Defines Alert Severity. | 1 | |  |
|  |  |  |

**Windows Server 2016 and above Logical Disk - Rules (non-alerting)**

**Logical Disk Free Megabytes Windows Server 2016 and above**

The space in megabytes on the logical disk that is unallocated

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 6 | | Tolerance |  | 10 | |  |
|  |  |  |

**Collection Rule for the Average Disk Queue Length Windows Server 2016 and above**

Collects the performance counter LogicalDisk\Avg Disk Queue Length

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 15 | |  |
|  |  |  |

**Logical Disk Split I/O Per Second Windows Server 2016 and above**

The rate at which I/Os to the disk were split into multiple I/Os.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 6 | | Tolerance |  | 10 | |  |
|  |  |  |

**% Logical Disk Idle Time Windows Server 2016 and above**

The percentage of time during the sample interval that the disk was idle.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 50 | |  |
|  |  |  |

**Average Disk Write Queue Length Windows Server 2016 and above (Logical Disk)**

The average number of write requests that were queued for the selected disk during the sample interval.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 15 | |  |
|  |  |  |

**% Logical Disk Free Space Windows Server 2016 and above**

The percentage of total usable space on the logical disk that is unallocated

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 6 | | Tolerance |  | 10 | |  |
|  |  |  |

**Collection Rule for Disk Writes Per Second Windows Server 2016 and above**

Collects the performance counter LogicalDisk\Disk Writes Per Second

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 10 | |  |
|  |  |  |

**Collection Rule for Average Disk Seconds Per Write Windows Server 2016 and above**

Collects the performance counter LogicalDisk\Avg Disk Sec Per Write

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 0.026 | |  |
|  |  |  |

**Collection Rule for Average Disk Seconds Per Transfer Windows Server 2016 and above**

Collects the performance counter LogicalDisk\Avg Disk Sec Per Transfer

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 0.026 | |  |
|  |  |  |

**Logical Disk Write Bytes Per Second Windows Server 2016 and above**

The rate at which bytes are transferred from the disk during write operations.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 10 | |  |
|  |  |  |

**Collection Rule for Disk Reads Per Second Windows Server 2016 and above**

Collects the performance counter LogicalDisk\Disk Reads Per Second

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 10 | |  |
|  |  |  |

**Disk Read Bytes Per Second Windows Server 2016 and above (Logical Disk)**

The rate at which bytes are transferred from the disk during read operations.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 10 | |  |
|  |  |  |

**Collection rule for Current Disk Queue Length Windows Server 2016 and above**

Collects the performance counter LogicalDisk\Current Disk Queue Length

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 32 | |  |
|  |  |  |

**Average Logical Disk Read Queue Length Windows Server 2016 and above**

The average number of read requests that were queued for the selected disk during the sample interval.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 15 | |  |
|  |  |  |

**Collection Rule for Disk Bytes Per Second Windows Server 2016 and above**

Collects the performance counter LogicalDisk\Disk Bytes Per Second

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 10 | |  |
|  |  |  |

**Collection Rule for Average Disk Seconds Per Read Windows Server 2016 and above**

Collects the performance counter LogicalDisk\Avg Disk Sec Per Read

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 0.026 | |  |
|  |  |  |

**Windows Server 2016 and above Logical Disk - Console Tasks**

**Start Computer Management Console**

This task starts the Computer Management console.

### Windows Server 2016 and above Logical Processor

All instances of a Logical processor on Windows Server 2016 and above operating systems.

**Windows Server 2016 and above Logical Processor - Unit monitors**

**Logical CPU DPC Time Percentage**

Monitors the Percent DPC Time

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | False | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 120 | | Number of Samples |  | 5 | | Threshold |  | 15 | |  |
|  |  |  |

**Logical CPU Percentage Utilization**

Monitors total Logical CPU utilization.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | False | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 120 | | Number of Samples |  | 5 | | Threshold |  | 95 | |  |
|  |  |  |

**Logical CPU Percentage Interrupt Time**

Monitors the Logical CPU Percentage Interrupt Time

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | False | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 120 | | Number of Samples |  | 5 | | Threshold |  | 10 | |  |
|  |  |  |

**Windows Server 2016 and above Logical Processor - Rules (non-alerting)**

**Logical Processor Information % Interrupt Time Windows Server 2016 and above**

Collects the performance counter Processor Information\% Interrupt Time

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 10 | |  |
|  |  |  |

**Logical Processor % Processor Time Windows Server 2016 and above**

Collects the performance counter Processor\% Processor Time

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 5 | |  |
|  |  |  |

**Logical Processor % DPC Time Windows Server 2016 and above**

Collects the performance counter Processor\% DPC Time

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 10 | |  |
|  |  |  |

### Windows Server 2016 and above Network Adapter

All instances of a network adapter on Windows Server 2016 and above operating systems.

**Windows Server 2016 and above Network Adapter - Discoveries**

**Discover Network Adapters (Both Enabled and Disabled)**

This rule uses WMI to discover all network adapters reported by Windows Server 2016 and above operating systems.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Discover Disabled Network Adapters |  | true | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 86760 | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 360 | |  |
|  |  |  |

**Discover Network Adapters (Only Enabled)**

This rule uses WMI to discover all enabled network adapters reported by Windows Server 2016 and above operating systems.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Discover Disabled Network Adapters |  | false | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 86820 | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 360 | |  |
|  |  |  |

**Windows Server 2016 and above Network Adapter - Unit monitors**

**Percent Bandwidth Used Read**

This monitor checks percentage of used network adapter read bandwidth.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Interval seconds | The recurring interval of time in seconds in which to run the workflow. | 300 | | Number of samples | The number of consecutive samples that need to be over the threshold before the monitor will change state. | 12 | | Threshold (percentage) | The threshold (in percentage) over which the monitor will change state. | 60 | |  |
|  |  |  |

**Percent Bandwidth Used Write**

This monitor checks percentage of used network adapter write bandwidth.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Interval seconds | The recurring interval of time in seconds in which to run the workflow. | 300 | | Number of samples | The number of consecutive samples that need to be over the threshold before the monitor will change state. | 12 | | Threshold (percentage) | The threshold (in percentage) over which the monitor will change state. | 60 | |  |
|  |  |  |

**Percent Bandwidth Used Total**

This monitor checks percentage of total used network adapter bandwidth..

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Interval seconds | The recurring interval of time in seconds in which to run the workflow. | 300 | | Number of samples | The number of consecutive samples that need to be over the threshold before the monitor will change state. | 12 | | Threshold (percentage) | The threshold (in percentage) over which the monitor will change state. | 75 | |  |
|  |  |  |

**Network Adapter Connection Health**

Monitors the network adapter connection's health.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Monitor Network Adapter Hardware Malfunction |  | false | | Monitor Network Adapter Media Disconnection |  | false | | Network Adapter Connection Health Monitor Type | This monitor type is used as the basis for the monitor which detects the connection health of network adapters. | true | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Windows Server 2016 and above Network Adapter - Rules (non-alerting)**

**Network Adapter Bytes Sent per Second Windows Server 2016 and above**

Collects the performance counter Network Interface\Bytes Sent/sec

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 25 | |  |
|  |  |  |

**Percent Bandwidth Used Total**

Rule collects Bandwidth Used Total counter for network adapters.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval seconds | How frequently (in seconds) the value should be sampled. | 300 | |  |
|  |  |  |

**Current Bandwidth**

Rule collects Network Interface\Current Bandwidth counter.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 100 | | Tolerance |  | 10 | |  |
|  |  |  |

**Percent Bandwidth Used Write**

Rule collects Bandwidth Used Write counter for network adapters.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval seconds | How frequently (in seconds) the value should be sampled. | 300 | |  |
|  |  |  |

**Output Queue Length**

Rule collects Network Interface\Output Queue Length counter.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 2 | |  |
|  |  |  |

**Network Adapter Bytes Received per Second Windows Server 2016 and above**

Collects the performance counter Network Interface\Bytes Received/sec

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 25 | |  |
|  |  |  |

**Percent Bandwidth Used Read**

Rule collects Bandwidth Used Read counter for network adapters.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval seconds | How frequently (in seconds) the value should be sampled. | 300 | |  |
|  |  |  |

**Network Adapter Bytes Total per Second Windows Server 2016 and above**

Collects the performance counter Network Interface/Bytes Total/sec

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 25 | |  |
|  |  |  |

**Windows Server 2016 and above Network Adapter - Console Tasks**

**Start Computer Management Console**

This task starts the Computer Management console.

### Windows Server 2016 and above Operating System

All instances of the Windows Server 2016 and above operating systems.

**Windows Server 2016 and above Operating System - Discoveries**

**Discover Windows 2016 and above Servers**

This Discovery Rule discovers and populates the Windows Server class named “Windows Server 2016 and above Computer" with instances of computers that are running Windows Server 2016 and above operating systems.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 86400 | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 360 | |  |
|  |  |  |

**Windows Server 2016 and above Operating System - Unit monitors**

**Server Service Health**

Monitors the health of the Windows service for the Server

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Alert only if service startup type is automatic | This may only be set to 'true' or 'false'. If set to 'false', then alerts will be triggered no matter what the startup type is set to. Default is 'true'. |  | |  |
|  |  |  |

**Free System Page Table Entries**

Monitor the performance counter Memory\Free System Page Table Entries

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Number of Samples |  | 6 | | Threshold |  | 5000 | |  |
|  |  |  |

**Total CPU Utilization Percentage**

Monitors the total CPU utilization of this server by correlating the Processor Information\% Processor Time\\_Total and the System\Processor Queue Length performance counters.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | CPU Percentage Utilization Threshold |  | 95 | | CPU Queue Length Threshold |  | 15 | | Interval seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Number of Samples |  | 3 | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**RPC Service Health**

Monitors the health of the Windows service for RPC

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Alert only if service startup type is automatic | This may only be set to 'true' or 'false'. If set to 'false', then alerts will be triggered no matter what the startup type is set to. Default is 'true'. |  | |  |
|  |  |  |

**Workstation Service Health**

Monitors the health of the Workstation service

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Alert only if service startup type is automatic | This may only be set to 'true' or 'false'. If set to 'false', then alerts will be triggered no matter what the startup type is set to. Default is 'true'. |  | |  |
|  |  |  |

**Windows Event Log Service Health**

Monitors the health of the Windows service for the Windows Event Log

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Alert only if service startup type is automatic | This may only be set to 'true' or 'false'. If set to 'false', then alerts will be triggered no matter what the startup type is set to. Default is 'true'. |  | |  |
|  |  |  |

**Total Percentage Interrupt Time**

Monitors the Percentage Interrupt Time

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 120 | | Number of Samples |  | 5 | | Threshold |  | 10 | |  |
|  |  |  |

**TCPv6 Segments Retransmitted Per Second**

Monitors the TCPv6\Segments Retransmitted/sec performance counter.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Number of Samples |  | 12 | | Threshold |  | 10 | |  |
|  |  |  |

**Total DPC Time Percentage**

Monitors the DPC Time Percentage.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 120 | | Number of Samples |  | 5 | | Threshold |  | 95 | |  |
|  |  |  |

**TCPv4 Segments Received Per Second**

Monitors the TCPv4\Segments Received/sec performance counter.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Number of Samples |  | 12 | | Threshold |  | 100 | |  |
|  |  |  |

**Plug and Play Service Health**

Monitors the health of the Windows service for Plug and Play

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Alert only if service startup type is automatic | This may only be set to 'true' or 'false'. If set to 'false', then alerts will be triggered no matter what the startup type is set to. Default is 'true'. |  | |  |
|  |  |  |

**Memory Pages Per Second**

Monitor the performance counter Memory\MemoryPagesPerSecond

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Number of Samples |  | 12 | | Threshold |  | 5000 | |  |
|  |  |  |

**TCPv4 Segments Sent Per Second**

Monitors the TCPv4\Segments Sent/sec performance counter.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Number of Samples |  | 12 | | Threshold |  | 100 | |  |
|  |  |  |

**Reserved**

Reserved

**Max Concurrent API Monitor**

This monitor alerts when Max Concurrent API condition is reached.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Interval seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Synchronization Time | The synchronization time specified by using a 24-hour format. May be omitted. |  | | Threshold Timeouts | Limit to consider in calculation. | 2000 | | Threshold Waiters | Limit to consider in calculation. | 50 | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**TCPv4 Segments Retransmitted Per Second**

Monitors the TCPv4\Segments Retransmitted/sec performance counter.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Number of Samples |  | 12 | | Threshold |  | 10 | |  |
|  |  |  |

**Windows Firewall Service Health**

Monitors the health of the Windows service for the Windows Firewall

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Alert only if service startup type is automatic | This may only be set to 'true' or 'false'. If set to 'false', then alerts will be triggered no matter what the startup type is set to. Default is 'true'. |  | |  |
|  |  |  |

**Time Accuracy Out of Range**

Monitors the total Time Offset of this server

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Interval seconds | The recurring interval of time in seconds in which to run the workflow. | 600 | | Number of Samples |  | 4 | | Threshold in MilliSeconds |  | 60000 | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 120 | |  |
|  |  |  |

**DHCP Client Service Health**

Monitors the health of the Windows service for the DHCP Client

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Alert only if service startup type is automatic | This may only be set to 'true' or 'false'. If set to 'false', then alerts will be triggered no matter what the startup type is set to. Default is 'true'. |  | |  |
|  |  |  |

**Windows Remote Management Service Health**

Monitors the health of the Windows service for the Windows Remote Management

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Alert only if service startup type is automatic | This may only be set to 'true' or 'false'. If set to 'false', then alerts will be triggered no matter what the startup type is set to. Default is 'true'. |  | |  |
|  |  |  |

**TCPv6 Segments Sent Per Second**

Monitors the TCPv6\Segments Sent/sec performance counter.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Number of Samples |  | 12 | | Threshold |  | 100 | |  |
|  |  |  |

**Operating System BPA Monitor**

Monitors compliance of Windows Server 2016 and above operating systems with Best Practices Analyzer rules. As long as Windows Nano Server does not support BPA PowerShell cmdlets, the monitor will always be displayed as "Healthy".

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Interval | Interval in seconds | 86400 | |  |
|  |  |  |

**DNS Client Service Health**

Monitors the health of the Windows service for the DNS Client

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Alert only if service startup type is automatic | This may only be set to 'true' or 'false'. If set to 'false', then alerts will be triggered no matter what the startup type is set to. Default is 'true'. |  | |  |
|  |  |  |

**TCPv6 Segments Received Per Second**

Monitors the TCPv6\Segments Received/sec performance counter.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Number of Samples |  | 12 | | Threshold |  | 100 | |  |
|  |  |  |

**Available Megabytes of Memory**

Monitors the available memory level.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Available Memory Threshold (MBytes) |  | 100 | | Interval seconds | The recurring interval of time in seconds in which to run the workflow. | 900 | | Number of Samples |  | 3 | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Computer Browser Service Health**

Monitors the health of the Windows service for the Computer Browser. Please note that this monitor is not running on Nano Server (the state of the monitor will be always "Healthy").

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Alert only if service startup type is automatic | This may only be set to 'true' or 'false'. If set to 'false', then alerts will be triggered no matter what the startup type is set to. Default is 'true'. |  | |  |
|  |  |  |

**Percentage of Committed Memory in Use**

Monitor the performance counter Memory\% Committed Bytes in Use

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 120 | | Number of Samples |  | 3 | | Threshold |  | 80 | |  |
|  |  |  |

**TCP/IP NetBIOS Service Health**

Monitors the health of the Windows service for TCP/IP NetBIOS

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Alert only if service startup type is automatic | This may only be set to 'true' or 'false'. If set to 'false', then alerts will be triggered no matter what the startup type is set to. Default is 'true'. |  | |  |
|  |  |  |

**Windows Server 2016 and above Operating System - Aggregate monitors**

**Core Windows Services Rollup**

The rollup monitor for all health related to critical Windows services.

**Windows Server 2016 and above Operating System - Rules (alerting)**

**Event Log File is Full**

The event log file is full.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | Yes | | Priority | Defines Alert Priority. | 1 | | Severity | Defines Alert Severity. | 1 | |  |
|  |  |  |

**A Service Terminated Unexpectedly**

An event was collected indicating an unexpected service termination.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | Yes | | Priority | Defines Alert Priority. | 1 | | Severity | Defines Alert Severity. | 1 | |  |
|  |  |  |

**A Share Configuration is Invalid**

A share was detected as having invalid configuration.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | Yes | | Priority | Defines Alert Priority. | 1 | | Severity | Defines Alert Severity. | 1 | |  |
|  |  |  |

**A Service has Entered into an Unpredictable State**

A service has entered an unpredictable state.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | Yes | | Priority | Defines Alert Priority. | 1 | | Severity | Defines Alert Severity. | 2 | |  |
|  |  |  |

**Performance registry corruption**

Corruption was detected in the registry related to performance counters.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | Yes | | Priority | Defines Alert Priority. | 1 | | Severity | Defines Alert Severity. | 1 | |  |
|  |  |  |

**A Software Update Installation Failed**

A failed software update installation was detected.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | Yes | | Priority | Defines Alert Priority. | 1 | | Severity | Defines Alert Severity. | 2 | |  |
|  |  |  |

**A Service is misconfigured**

A service has been detected as misconfigured.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | Yes | | Priority | Defines Alert Priority. | 1 | | Severity | Defines Alert Severity. | 2 | |  |
|  |  |  |

**Too many requests for performance counter data have failed**

Too many requests for performance counter data have timed out and failed.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | Yes | | Priority | Defines Alert Priority. | 1 | | Severity | Defines Alert Severity. | 2 | |  |
|  |  |  |

**Server Service Configuration Health Rule**

Server Service Configuration Health Rule

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | Yes | | Priority | Defines Alert Priority. | 1 | | Severity | Defines Alert Severity. | 1 | |  |
|  |  |  |

**NTFS - File System Corrupt**

NT file system indicates a corrupt file system.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | Yes | | Priority | Defines Alert Priority. | 1 | | Severity | Defines Alert Severity. | 1 | |  |
|  |  |  |

**Duplicate IP Address has been Detected**

A duplicate IP address has been detected on the network

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | Yes | | Priority | Defines Alert Priority. | 1 | | Severity | Defines Alert Severity. | 2 | |  |
|  |  |  |

**A Service or Driver Failed to Start**

An event was detected indicating a service or driver failed to start.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | Yes | | Priority | Defines Alert Priority. | 1 | | Severity | Defines Alert Severity. | 1 | |  |
|  |  |  |

**Disk can not be read**

Logical Disk Manager reports that the disk can not be read

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | Yes | | Priority | Defines Alert Priority. | 1 | | Severity | Defines Alert Severity. | 1 | |  |
|  |  |  |

**NTFS - Delayed Write Lost**

NT file system reports a delayed write was lost.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | Yes | | Priority | Defines Alert Priority. | 1 | | Severity | Defines Alert Severity. | 1 | |  |
|  |  |  |

**Windows Server 2016 and above Operating System - Rules (non-alerting)**

**Pages Input Per Second**

Collects the performance counter Memory\Pages Input/sec

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 6 | | Tolerance |  | 10 | |  |
|  |  |  |

**TCPv4 Connections Established**

This rule collects TCPv4\Connections Established performance counter.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 25 | | Tolerance |  | 10 | |  |
|  |  |  |

**TCPv4 Connections Reset**

The rule collects TCPv4\Connections Reset performance counter.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 25 | | Tolerance |  | 10 | |  |
|  |  |  |

**System Processor Queue Length Windows Server 2016 and above**

Collection rule for the performance counter System\Processor Queue Length.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 10 | |  |
|  |  |  |

**TCPv6 Connection Failures**

The rule collects TCPv6\Connection Failures performance counter.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 25 | | Tolerance |  | 10 | |  |
|  |  |  |

**Cache Data Map Hits Percent**

Collects the performance counter Memory\Data Map Hits %

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 10 | |  |
|  |  |  |

**Memory % Committed Bytes in Use Windows Server 2016 and above**

Collects the performance counter Memory\% Committed Bytes in Use

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 6 | | Tolerance |  | 10 | |  |
|  |  |  |

**Percent Memory Used**

This rule collects data about used physical memory.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval seconds | The recurring interval of time in seconds in which to run the workflow. | 300 | | Number of Samples | Number of Samples | 12 | | Tolerance | Tolerance | 50 | |  |
|  |  |  |

**Free System Page Table Entries**

Collects the performance counter Memory\Free System Page Table Entries

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 6 | | Tolerance |  | 800 | |  |
|  |  |  |

**TCPv4 Connection Failures**

The rule collects TCPv4\Connection Failures performance counter.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 25 | | Tolerance |  | 10 | |  |
|  |  |  |

**Memory Page Reads per Second Windows Server 2016 and above**

Collects the performance counter Memory\Page Reads/Sec.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 250 | |  |
|  |  |  |

**Pool Paged Resident Bytes**

Collects the performance counter Memory\Pool Paged Resident Bytes

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 6 | | Tolerance |  | 10 | |  |
|  |  |  |

**Processor % Processor Time Total Windows Server 2016 and above**

Collects the performance counter Processor\% Processor Time

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 5 | |  |
|  |  |  |

**Pages Output Per Second**

Collects the performance counter Memory\Pages Output/sec

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 6 | | Tolerance |  | 10 | |  |
|  |  |  |

**Memory Available Megabytes Windows Server 2016 and above**

Collects the performance counter Memory\Available MBytes

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 6 | | Tolerance |  | 10 | |  |
|  |  |  |

**TCPv4 Segments Retransmitted Per Second**

The rule collects TCPv4\Segments Retransmitted/sec performance counter.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 100 | | Tolerance |  | 10 | |  |
|  |  |  |

**TCPv4 Segments Sent Per Second**

The rule collects TCPv4\Segments Sent/sec counter.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 100 | | Tolerance |  | 10 | |  |
|  |  |  |

**Memory Pool Non-paged Bytes Windows Server 2016 and above**

Collects the performance counter Memory\Pool Nonpaged Bytes

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 6 | | Tolerance |  | 2000000 | |  |
|  |  |  |

**TCPv4 Segments Received Per Second**

The rule collects TCPv4\Segments Received/sec performance counter.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 100 | | Tolerance |  | 10 | |  |
|  |  |  |

**Memory Pages per Second Windows Server 2016 and above**

Collects the performance counter Memory\Pages Reads/Sec.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 250 | |  |
|  |  |  |

**Committed Bytes**

Collects the performance counter Memory\Committed Bytes

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 6 | | Tolerance |  | 10 | |  |
|  |  |  |

**Memory Pool Paged Bytes Windows Server 2016 and above**

Collects the performance counter Memory\Pool Paged Bytes

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 6 | | Tolerance |  | 2000000 | |  |
|  |  |  |

**Total Processor Information % Interrupt Time Windows Server 2016 and above**

Collects the performance counter Processor Information\% Interrupt Time

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 10 | |  |
|  |  |  |

**TCPv6 Connections Reset**

The rule collects TCPv6\Connections Reset performance counter.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 25 | | Tolerance |  | 10 | |  |
|  |  |  |

**TCPv6 Connections Established**

The rule collects TCPv6\Connections Established performance counter.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 25 | | Tolerance |  | 10 | |  |
|  |  |  |

**Page File Percentage Use Windows Server 2016 and above**

Collection rule for the performance counter Paging File\% Usage

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 6 | | Tolerance |  | 10 | |  |
|  |  |  |

**Cache Bytes**

Collects the performance counter Memory\Cache Bytes

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 6 | | Tolerance |  | 10 | |  |
|  |  |  |

**Total Processor % DPC Time Windows Server 2016 and above**

Collects the performance counter Processor\% DPC Time

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 10 | |  |
|  |  |  |

**Memory Page Writes per Second Windows Server 2016 and above**

Collects the performance counter Memory\Page Writes/Sec.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 250 | |  |
|  |  |  |

**TCPv6 Segments Sent Per Second**

The rule collects TCPv6\Segments Sent/sec performance counter.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 100 | | Tolerance |  | 10 | |  |
|  |  |  |

**TCPv6 Segments Received Per Second**

The rule collects TCPv6\Segments Received/sec performance counter.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 100 | | Tolerance |  | 10 | |  |
|  |  |  |

**System Cache Resident Bytes**

Collects the performance counter Memory\System Cache Resident Bytes

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 6 | | Tolerance |  | 10 | |  |
|  |  |  |

**TCPv6 Segments Retransmitted Per Second**

The rule collects TCPv6\Segments Retransmitted/sec performance counter.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 100 | | Tolerance |  | 10 | |  |
|  |  |  |

**Commit Limit**

Collects the performance counter Memory\Commit limit

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 6 | | Tolerance |  | 10 | |  |
|  |  |  |

**System Context Switches per Second Windows Server 2016 and above**

Collection rule for the performance counter System\Context Switches/sec

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 50 | |  |
|  |  |  |

**Windows Server 2016 and above Operating System - Rules (non-alerting)**

**Collection Rule for Windows Restarted Events**

This rule collects events indicating Windows has restarted

**Collection rule for NTFS Quota Threshold Reached**

An NTFS disk quota threshold was reached.

**Collection Rule for Software Updates Installation Events**

Collection rule for events indicating that new software updates were installed.

**Collection rule for NTFS Quota Threshold Limit Reached**

An NTFS disk quota threshold limit was reached.

**Collection rule for Service or Driver Failed to Start events**

Collection rule for events indicating a service or driver has failed to start.

**Collection Rule for Windows Dirty Shutdown Events**

This rule collects events indicating a dirty Windows shutdown.

**Collection rule for invalid Share Configuration Detected**

Collection rule for events indicating that a share has invalid configuration.

**Collection Rule for Windows Clean Restart Events**

This rule collects the events indicating a clean Windows shutdown.

**Collection Rule for Software Updates Scheduled Installation Events**

Collection rule for events indicating new software updates are scheduled.

**Collection Rule for Checking the File System Occurred on Startup**

This rule collects the events indicates that the system ran a chkdsk on startup

**Collection rule for unexpected service terminations**

Collection rule for events indicating unexpected service terminations.

**Collection rule for Network Adapter was Disconnected from the Network**

Collection rule for events indicating the network adapter was disconnected from the network.

**Collection Rule for Software Update Installation Failed**

Collection rule for events indicating a failed software update installation.

**Collection Rule for Windows Restart Events (restarted from bug check)**

Collection rule for events indicating Windows restarted from bug check

**Windows Server 2016 and above Operating System - Console Tasks**

**Start Computer Management Console**

This task starts the Computer Management console.

### Windows Server 2016 and above Operating System (Core)

All instances of the Windows Server 2016 (Core) and above operating systems.

**Windows Server 2016 and above Operating System (Core) - Discoveries**

**Discover Windows 2016 and above Servers**

This Discovery Rule discovers and populates the Windows Server class named “Windows Server 2016 and above Computer" with instances of computers that are running Windows Server 2016 and above operating systems.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 86400 | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 360 | |  |
|  |  |  |

### Windows Server 2016 and above Physical Disk

All instances of a physical disk on Windows Server 2016 and above operating systems.

**Windows Server 2016 and above Physical Disk - Discoveries**

**Discover Windows Physical Disks**

This rule uses WMI to discover all physical disks of Windows Server 2016 and above operating systems.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 86880 | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 360 | |  |
|  |  |  |

**Windows Server 2016 and above Physical Disk - Unit monitors**

**Average Disk Seconds Per Write (Physical Disk)**

Monitors the disk write latency (average disk seconds per write)

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 60 | | Number of Samples |  | 15 | | Threshold |  | 0.04 | |  |
|  |  |  |

**Average Physical Disk Seconds Per Read**

Monitors the average seconds per read operation to disk.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 60 | | Number of Samples |  | 15 | | Threshold |  | 0.04 | |  |
|  |  |  |

**Physical Disk Percent Idle Time**

Monitor the performance counter PhysicalDisk\% Idle Time

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Number of Samples |  | 24 | | Threshold |  | 20 | |  |
|  |  |  |

**Average Physical Disk Seconds Per Transfer**

Monitors the disk read and write latency (average disk seconds per transfer).

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 60 | | Number of Samples |  | 15 | | Threshold |  | 0.04 | |  |
|  |  |  |

**Current Disk Queue Length (Physical Disk)**

Monitor the performance counter PhysicalDisk\Current Disk Queue Length

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Number of Samples |  | 12 | | Threshold |  | 32 | |  |
|  |  |  |

**Windows Server 2016 and above Physical Disk - Rules (non-alerting)**

**Average Disk Write Queue Length Windows Server 2016 and above (Physical Disk)**

The average number of write requests that were queued for the selected disk during the sample interval.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 15 | |  |
|  |  |  |

**% Physical Disk Idle Time Windows Server 2016 and above**

The percentage of time during the sample interval that the disk was idle.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 50 | |  |
|  |  |  |

**Physical Disk Disk Bytes per Second Windows Server 2016 and above**

Collects the performance counter PhysicalDisk\Disk Bytes/sec.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 10 | |  |
|  |  |  |

**Disk Read Bytes Per Second Windows Server 2016 and above (Physical Disk)**

The rate at which bytes are transferred from the disk during read operations.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 10 | |  |
|  |  |  |

**Physical Disk Average Disk Queue Length Windows Server 2016 and above**

Collects the performance counter PhysicalDisk\Avg. Disk Queue Length

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 15 | |  |
|  |  |  |

**Physical Disk Split I/O Per Second Windows Server 2016 and above**

The rate at which I/Os to the disk were split into multiple I/Os.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 6 | | Tolerance |  | 10 | |  |
|  |  |  |

**Physical Disk Average Disk Seconds per Write Windows Server 2016 and above**

Collects the performance counter PhysicalDisk\Avg. Disk sec/Write.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 0.026 | |  |
|  |  |  |

**Average Physical Disk Read Queue Length Windows Server 2016 and above**

The average number of read requests that were queued for the selected disk during the sample interval.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 15 | |  |
|  |  |  |

**Physical Disk Average Disk Seconds per Transfer Windows Server 2016 and above**

Collects the performance counter PhysicalDisk\Avg. Disk sec/Transfer.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 0.026 | |  |
|  |  |  |

**Physical Disk Reads per Second Windows Server 2016 and above**

Collects the performance counter PhysicalDisk\Disk Reads/sec

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 10 | |  |
|  |  |  |

**Physical Disk Write Bytes Per Second Windows Server 2016 and above**

The rate at which bytes are transferred from the disk during write operations.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 10 | |  |
|  |  |  |

**Physical Disk Average Disk Seconds per Read Windows Server 2016 and above**

Collects the performance counter PhysicalDisk\Avg. Disk sec/Read

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 0.026 | |  |
|  |  |  |

**Physical Disk Current Disk Queue Length Windows Server 2016 and above**

Collects the performance counter PhysicalDisk\Current Disk Queue Length

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 32 | |  |
|  |  |  |

**Physical Disk Writes per Second Windows Server 2016 and above**

Collects the performance counter PhysicalDisk\Disk Writes/sec.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Maximum Sample Separation | Maximum data samples skipped by Optimized Collection when data is within Tolerance | 12 | | Tolerance |  | 10 | |  |
|  |  |  |

**Windows Server 2016 and above Physical Disk - Console Tasks**

**Start Computer Management Console**

This task starts the Computer Management console.

### Windows Server 2016 and above Process Monitoring Seed

Process monitoring seed of Windows Server 2016 and above operating systems.

**Windows Server 2016 and above Process Monitoring Seed - Discoveries**

**Windows Server 2016 Process and Port Monitoring Seed Discovery (Full)**

Discovery of process and port monitoring seed objects of Windows Server 2016 (Full).

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 86400 | |  |
|  |  |  |

**Windows Server 2016 and above Process and Port Monitoring Seed Discovery (Core)**

Discovery of Core process and port monitoring seed objects of Windows Server 2016 and above operating systems.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 86400 | |  |
|  |  |  |

**Windows Server 2016 and above Process Monitoring Seed - Rules (non-alerting)**

**Process Monitoring: Performance Collection**

This rule collects information about the processes' performance metrics.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 60 | | Log Level | Determines which events should be written to Event Log.  0 – All, 1 – Informational, 2 – Warning, 4 – Error, 8 – Verbose,  16 – Debug, 255 – None | 4 | | Monitoring Configuration | Allows to specify processes to exclude from monitoring in XML format | $Target/Property[Type="WindowsServer!Microsoft.Windows.Server.ProcessSeed"]/ThresholdsByProcess$ | |  |
|  |  |  |

**Process Monitoring: High Memory Percentage**

This rule generates an alert when the memory percentage is too high.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 67 | | Log Level | Determines which events should be written to Event Log.  0 – All, 1 – Informational, 2 – Warning, 4 – Error, 8 – Verbose,  16 – Debug, 255 – None | 4 | | Memory Percentage Threshold | Memory Percentage Threshold | 50 | | Monitoring Configuration | Allows to specify thresholds for specific processes and processes to exclude from monitoring in XML format | $Target/Property[Type="WindowsServer!Microsoft.Windows.Server.ProcessSeed"]/ThresholdsByProcess$ | | Sample Count | Sample Count | 6 | |  |
|  |  |  |

**Process Monitoring: Health State Collection**

This rule collects information about the health state of the processes.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Handle Count Increase Threshold | Handle Count Increase Threshold | 20 | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 60 | | Log Level | Determines which events should be written to Event Log.  0 – All, 1 – Informational, 2 – Warning, 4 – Error, 8 – Verbose,  16 – Debug, 255 – None | 4 | | Memory Percentage Threshold | Memory Percentage Threshold | 50 | | Monitoring Configuration | Allows to specify thresholds for specific processes and processes to exclude from monitoring in XML format | $Target/Property[Type="WindowsServer!Microsoft.Windows.Server.ProcessSeed"]/ThresholdsByProcess$ | | Percent Processor Time Threshold | Percent Processor Time Threshold | 50 | | Sample Count | Sample Count | 6 | |  |
|  |  |  |

**Process Monitoring: High Processor Time Percentage**

This rule generates an alert when the percentage of processor time is too high.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 73 | | Log Level | Determines which events should be written to Event Log.  0 – All, 1 – Informational, 2 – Warning, 4 – Error, 8 – Verbose,  16 – Debug, 255 – None | 4 | | Monitoring Configuration | Allows to specify thresholds for specific processes and processes to exclude from monitoring in XML format | $Target/Property[Type="WindowsServer!Microsoft.Windows.Server.ProcessSeed"]/ThresholdsByProcess$ | | Percent Processor Time Threshold | Percent processor time threshold. | 50 | | Sample Count | Sample Count | 6 | |  |
|  |  |  |

**Process Monitoring: High Handle Count**

This rule generates an alert when handle count increases too fast.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Handle Count Increase Threshold | Handle Count Increase Threshold | 20 | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 120 | | Log Level | Determines which events should be written to Event Log.  0 – All, 1 – Informational, 2 – Warning, 4 – Error, 8 – Verbose,  16 – Debug, 255 – None | 4 | | Monitoring Configuration | Allows to specify thresholds for specific processes and processes to exclude from monitoring in XML format | $Target/Property[Type="WindowsServer!Microsoft.Windows.Server.ProcessSeed"]/ThresholdsByProcess$ | | Sample Count | Sample Count | 6 | |  |
|  |  |  |

**Process Monitoring: Network Port State Collection**

This rule collects information about Network Port State.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 60 | | Log Level | Determines which events should be written to Event Log.  0 – All, 1 – Informational, 2 – Warning, 4 – Error, 8 – Verbose,  16 – Debug, 255 – None | 4 | | Monitoring Configuration | Allows to specify thresholds for specific processes and processes to exclude from monitoring in XML format | $Target/Property[Type="WindowsServer!Microsoft.Windows.Server.ProcessSeed"]/ThresholdsByProcess$ | |  |
|  |  |  |

**Windows Server 2016 and above Process Monitoring Seed - Rules (non-alerting)**

**Process Monitoring: Number of Processes Collection**

This rule collects the Number of Processes performance counter for Windows Server 2016 and above operating systems.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 300 | |  |
|  |  |  |

### Windows Server 2016 and above Processor

All instances of a processor on Windows Server 2016 and above operating systems.

**Windows Server 2016 and above Processor - Discoveries**

**Discover Windows CPUs**

This rule uses WMI to discover all processors reported by Windows Server 2016 and above operating systems.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 86640 | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 360 | |  |
|  |  |  |

**Windows Server 2016 and above Processor - Unit monitors**

**CPU DPC Time Percentage**

Monitors the Percent DPC Time

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | False | | Frequency seconds | The recurring interval of time in seconds in which to run the workflow. | 180 | | Number of Samples |  | 5 | | Threshold (percentage) | The threshold (in percentage) over which the monitor will change state. | 10 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**CPU Percentage Interrupt Time**

Monitors the CPU Percentage Interrupt Time

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | False | | Frequency seconds | The recurring interval of time in seconds in which to run the workflow. | 180 | | Number of Samples |  | 5 | | Threshold (percentage) | The threshold (in percentage) over which the monitor will change state. | 10 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**CPU Percentage Utilization**

Monitors total CPU (Processor Information) utilization.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | False | | Frequency seconds | The recurring interval of time in seconds in which to run the workflow. | 180 | | Number of Samples |  | 5 | | Threshold (percentage) | The threshold (in percentage) over which the monitor will change state. | 10 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Windows Server 2016 and above Processor - Aggregate monitors**

**Windows Server 2016 and above Processor Performance Rollup Monitor**

This monitor aggregates the performance monitors for Processor.

**Windows Server 2016 and above Processor - Dependency (rollup) monitors**

**Logical Processors Performance Rollup**

This monitor roles up the performance of Logical Processor

**Windows Server 2016 and above Processor - Rules (non-alerting)**

**Processor Information % DPC Time Windows Server 2016 and above**

Collects the performance counter Processor Information\% DPC Time

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency seconds | The recurring interval of time in seconds in which to run the workflow. | 300 | | Timeout seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Processor Information % Interrupt Time Windows Server 2016 and above**

Collects the performance counter Processor Information\% Interrupt Time

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency seconds | The recurring interval of time in seconds in which to run the workflow. | 300 | | Timeout seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Processor % Processor Time Windows Server 2016 and above**

Collects the performance counter Processor\% Processor Time

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Frequency seconds | The recurring interval of time in seconds in which to run the workflow. | 300 | | Timeout seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

**Windows Server 2016 and above Processor - Console Tasks**

**Start Computer Management Console**

This task starts the Computer Management console.

### Windows Server 2016 Computer (Full)

All instances of computers running the Windows Server 2016 operating system (Full).

**Windows Server 2016 Computer (Full) - Discoveries**

**Discover Windows 2016 and above Servers**

This Discovery Rule discovers and populates the Windows Server class named “Windows Server 2016 and above Computer" with instances of computers that are running Windows Server 2016 and above operating systems.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 86400 | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 360 | |  |
|  |  |  |

### Windows Server 2016 Operating System (Full)

All instances of the Windows Server 2016 operating system (Full).

**Windows Server 2016 Operating System (Full) - Discoveries**

**Discover Windows 2016 and above Servers**

This Discovery Rule discovers and populates the Windows Server class named “Windows Server 2016 and above Computer" with instances of computers that are running Windows Server 2016 and above operating systems.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Interval Seconds | The recurring interval of time in seconds in which to run the workflow. | 86400 | | Timeout Seconds | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 360 | |  |
|  |  |  |

## Appendix: Rules and Monitors Disabled by Default

The following table lists the rules and monitors that are disabled by default.

|  |  |  |
| --- | --- | --- |
| Rule/monitor | Why disabled | When to enable |
| Discover Windows CPUs | This discovery is disabled based on customer feedback. Most of our customers do not monitor Windows CPUs by default. | Enable this discovery rule when CPUs need to be discovered and monitored. |
| Discover Windows Disk Partitions | This discovery is disabled based on customer feedback. Most of our customers do not monitor Windows disk partitions by default. | Enable this discovery rule when Windows disk partitions need to be discovered and monitored. |
| Discover Network Adapters (Both Enabled and Disabled) | There are two different discoveries for network adapters: Discover Network Adapters (Enabled) and Discover Network Adapters (Both Enabled and Disabled). Since they both discover enabled network adapters, both should not be enabled at the same time. | Enable this discovery rule when disabled network adapters need to be discovered. |
| Discover Windows Physical Disks | This discovery is disabled based on customer feedback. Most of our customers do not monitor Windows physical disks by default. | Enable this discovery rule when Windows physical disks need to be discovered and monitored. |
| Mount Point Discovery Rule | This discovery is disabled based on customer feedback. Most of our customers do not monitor Windows mount points by default. | Enable this discovery rule when Windows physical disks need to be discovered and monitored. |
| Windows Server 2016 and above Network Adapter Connection Health | This monitor is disabled based on customer feedback. Most of our customers do not monitor network adapter connection health by default. | Enable this monitor if network adapter connection health monitoring is required. |
| Windows Server 2016 Percent Bandwidth Used Read | This monitor is disabled based on customer feedback. Most of our customers do not monitor percent bandwidth used read performance information on network adapters by default. | Enable this monitor if percent bandwidth used read performance monitoring is required. |
| Windows Server 2016 Percent Bandwidth Used Write | This monitor is disabled based on customer feedback. Most of our customers do not monitor percent bandwidth used write performance information on network adapters by default. | Enable this monitor if percent bandwidth used write performance monitoring is required. |
| Windows Server 2016 Percentage of Committed Memory in Use | This monitor is disabled based on customer feedback. Most of our customers do not monitor the percentage of committed memory in use performance information by default. | Enable this monitor if the percentage of committed memory in use performance monitoring is required. |
| Windows Server 2016 Total DPC Time Percentage | This monitor is disabled based on customer feedback. Most of our customers do not monitor total DPC time percentage performance information by default. | Enable this monitor if total DPC time percentage performance monitoring is required. |
| Windows Server 2016 Total Percentage Interrupt Time | This monitor is disabled based on customer feedback. Most of our customers do not monitor total percentage interrupt time performance information by default. | Enable this monitor if total percentage interrupt time performance monitoring is required. |
| Windows Server 2016 Average Physical Disk Seconds Per Read | This monitor is disabled based on customer feedback. Most of our customers do not monitor average physical disk seconds per read performance information on physical disks by default. | Enable this monitor if average physical disk seconds per read performance monitoring is required. |
| Windows Server 2016 and above Physical Disk Percent Idle Time | This monitor is disabled based on customer feedback. Most of our customers do not monitor physical disk percent idle time performance information on physical disks by default. | Enable this monitor if physical disk percent idle time performance monitoring is required. |
| Windows Server 2016 CPU DPC Time Percentage | This monitor is disabled based on customer feedback. Most of our customers do not monitor Logical CPU DPC time percentage performance information on CPUs by default. | Enable this monitor if CPU DPC time percentage performance monitoring is required. |
| Windows Server 2016 Logical CPU DPC Time Percentage | This monitor is disabled based on customer feedback. Most of our customers do not monitor Logical CPU DPC time percentage performance information on CPUs by default. | Enable this monitor if Logical CPU DPC time percentage performance monitoring is required. |
| Windows Server 2016 CPU Percentage Interrupt Time | This monitor is disabled based on customer feedback. Most of our customers do not monitor CPU percentage interrupt time performance information on CPUs by default. | Enable this monitor if CPU percentage interrupt time performance monitoring is required. |
| Windows Server 2016 Logical CPU Percentage Interrupt Time | This monitor is disabled based on customer feedback. Most of our customers do not monitor Logical CPU percentage interrupt time performance information on CPUs by default. | Enable this monitor if Logical CPU percentage interrupt time performance monitoring is required. |
| Windows Server 2016 Logical CPU Percentage Utilization | This monitor is disabled based on customer feedback. Most of our customers do not monitor Logical CPU percentage utilization performance information on CPUs by default. | Enable this monitor if Logical CPU percentage utilization performance monitoring is required. |
| Collection rule for the Average Disk Queue Length Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the average disk queue length performance information by default. | Enable this collection rule if average disk queue length performance collection is required. |
| Collection rule for Disk Bytes Per Second Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the disk bytes per second performance information by default. | Enable this collection rule if disk bytes per second performance collection is required. |
| Collection rule for Disk Reads Per Second Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the disk reads per second performance information by default. | Enable this collection rule if disk reads per second performance collection is required. |
| Collection rule for Disk Writes Per Second Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the disk writes per second performance information by default. | Enable this collection rule if disk writes per second performance collection is required. |
| Disk Read Bytes Per Second Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the disk read bytes per second performance information on logical disks by default. | Enable this collection rule if disk read bytes per second performance collection is required. |
| Logical Disk Write Bytes Per Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect disk write bytes per second performance information on logical disks by default. | Enable this collection rule if disk writes per second performance collection is required. |
| Average Logical Disk Read Queue Length Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the average logical disk read queue length performance information on logical disks by default. | Enable this collection rule if average logical disk read queue length performance collection is required. |
| Average Disk Write Queue Length Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the average disk write queue length performance information on logical disks by default. | Enable this collection rule if average disk write queue length performance collection is required. |
| Logical Disk Split I/O Per Second Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect split I/O per second performance information on logical disks by default. | Enable this collection rule if split I/O per second performance collection is required. |
| Output Queue Length Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the output queue length performance information on network adapters by default. | Enable this collection rule if the output queue length performance collection is required. |
| Percent Bandwidth Used Read Windows Server 2016 | This collection rule and monitor is disabled based on customer feedback. Most of our customers do not collect the percent bandwidth used read performance information on network adapters by default. | Enable this collection rule or monitor if percent bandwidth used read performance collection or monitoring is required. |
| Percent Bandwidth Used Write Windows Server 2016 | This collection rule and monitor is disabled based on customer feedback. Most of our customers do not collect the percent bandwidth used write performance information on network adapters by default. | Enable this collection rule or monitor if percent bandwidth used write performance collection or monitoring is required. |
| Network Adapter Bytes Received per Second Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the network adapter bytes received per second performance information on network adapters by default. | Enable this collection rule if network adapter bytes received per second performance collection is required. |
| Network Adapter Bytes Sent per Second Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the network adapter bytes sent per second performance information on network adapters by default. | Enable this collection rule if network adapter bytes sent per second performance collection is required. |
| Memory Page Reads per Second Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the memory page reads per second performance information by default. | Enable this collection rule if memory page reads per second performance collection is required. |
| Memory Page Writes per Second Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the memory page writes per second performance information by default. | Enable this collection rule if memory page writes per second performance collection is required. |
| Memory % Committed Bytes in Use Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the memory % committed bytes in use performance information by default. | Enable this collection rule if memory % committed bytes in use performance collection is required. |
| Page File Percentage Use Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the page file percentage use performance information by default. | Enable this collection rule if page file percentage use performance collection is required. |
| A Service or Driver Failed to Start | This alert rule is disabled based on customer feedback. Most of our customers do not alert on a generic failure such as “A Service or Driver Failed to Start” by default. | Enable this alert rule if a generic failure such as “A Service or Driver Failed to Start” monitoring is required. |
| A Service Terminated Unexpectedly | This alert rule is disabled based on customer feedback. Most of our customers do not alert on a generic failure such as “A Service Terminated Unexpectedly” by default. | Enable this alert rule if a generic failure such as “A Service Terminated Unexpectedly” monitoring is required. |
| A Share Configuration is Invalid | This alert rule is disabled based on customer feedback. Most of our customers do not alert on a generic failure such as “A Share Configuration is Invalid” by default. | Enable this alert rule if a generic failure such as “A Share Configuration is Invalid” monitoring is required. |
| A Software Update Installation Failed | This alert rule is disabled based on customer feedback. Most of our customers do not alert on a generic failure such as “A Software Update Installation Failed” by default. | Enable this alert rule if a generic failure such as “A Software Update Installation Failed” monitoring is required. |
| System Context Switches per Second Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect system context switches per second performance information by default. | Enable this collection rule if system context switches per second performance collection is required. |
| Total Processor % DPC Time Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the total processor % DPC time performance information by default. | Enable this collection rule if total processor % DPC time performance collection is required. |
| Total Processor % Interrupt Time Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect total processor % interrupt time performance information by default. | Enable this collection rule if total processor % interrupt time performance collection is required. |
| Cache Bytes | This collection rule is disabled based on customer feedback. Most of our customers do not collect the cache bytes performance information by default. | Enable this collection rule if cache bytes performance collection is required. |
| Committed Bytes | This collection rule is disabled based on customer feedback. Most of our customers do not collect the committed bytes performance information by default. | Enable this collection rule if committed bytes performance collection is required. |
| Pages Output Per Second | This collection rule is disabled based on customer feedback. Most of our customers do not collect the pages output per second performance information by default. | Enable this collection rule if pages output per second performance collection is required. |
| Pages Input Per Second | This collection rule is disabled based on customer feedback. Most of our customers do not collect the pages input per second performance information by default. | Enable this collection rule if pages input per second performance collection is required. |
| Commit Limit | This collection rule is disabled based on customer feedback. Most of our customers do not collect the commit limit performance information by default. | Enable this collection rule if commit limit performance collection is required. |
| Pool Paged Resident Bytes | This collection rule is disabled based on customer feedback. Most of our customers do not collect the pool paged resident bytes performance information by default. | Enable this collection rule if pool paged resident bytes performance collection is required. |
| System Cache Resident Bytes | This collection rule is disabled based on customer feedback. Most of our customers do not collect the system cache resident bytes performance information by default. | Enable this collection rule if system cache resident bytes performance collection is required. |
| Cache Data Map Hits Percent | This collection rule is disabled based on customer feedback. Most of our customers do not collect the cache data map hits percent performance information by default. | Enable this collection rule if cache data map hits percent performance collection is required. |
| Physical Disk Average Disk Queue Length Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the physical disk average disk queue length performance information by default. | Enable this collection rule if physical disk average disk queue length performance collection is required. |
| Physical Disk Average Disk Seconds per Read Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the physical disk average disk seconds per read performance information by default. | Enable this collection rule if physical disk average disk seconds per read performance collection is required. |
| Physical Disk Average Disk Seconds per Write Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the physical disk average disk seconds per write performance information by default. | Enable this collection rule if physical disk average disk seconds per write performance collection is required. |
| Physical Disk Bytes per Second Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the physical disk bytes per second performance information by default. | Enable this collection rule if physical disk bytes per second performance collection is required. |
| Physical Disk Reads per Second Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the physical disk reads per second performance information by default. | Enable this collection rule if physical disk reads per second performance collection is required. |
| Physical Disk Writes per Second Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the physical disk writes per second performance information by default. | Enable this collection rule if physical disk writes per second performance collection is required. |
| % Physical Disk Idle Time Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the % physical disk idle time performance information by default. | Enable this collection rule if % physical disk idle time performance collection is required. |
| Disk Read Bytes Per Second Windows Server 2016 (Physical Disk) | This collection rule is disabled based on customer feedback. Most of our customers do not collect the disk read bytes per second performance information by default. | Enable this collection rule if disk read bytes per second performance collection is required. |
| Physical Disk Write Bytes Per Second Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the physical disk write bytes per second performance information by default. | Enable this collection rule if physical disk write bytes per second performance collection is required. |
| Average Physical Disk Read Queue Length Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the average physical disk read queue length performance information by default. | Enable this collection rule if average physical disk read queue length performance collection is required. |
| Average Disk Write Queue Length Windows Server 2016 (Physical Disk) | This collection rule is disabled based on customer feedback. Most of our customers do not collect the average disk write queue length performance information by default. | Enable this collection rule if average disk write queue length performance collection is required. |
| Physical Disk Split I/O Per Second Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the physical disk split I/O per second performance information by default. | Enable this collection rule if physical disk split I/O per second performance collection is required. |
| Processor Information % DPC Time Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the processor % DPC time performance information by default. | Enable this collection rule if processor % DPC time performance collection is required. |
| Processor Information % Interrupt Time Windows Server 2016 | This collection rule is disabled based on customer feedback. Most of our customers do not collect the processor % interrupt time performance information by default. | Enable this collection rule if processor % interrupt time performance collection is required. |
| Cluster Shared Volume - NTFS State Monitor | This monitor is disabled because the state of the NTFS partition is not typically needed (Dirty State notification). | Enable this monitor if the state of the NTFS file system is required. |
| Cluster Shared Volume - State Monitor | This monitor is disabled because, when enabled, it may cause false negatives during backups of the Cluster Shared Volumes. | Enable this monitor if the availability of the Cluster Shared Volume is necessary (not based on CSV space). |
| Operating System BPA Monitor | This monitor is disabled based on customer feedback. Customers do not want BPA data to be collected on all systems by default. | Enable this monitor if BPA information is necessary. |
| [Deprecated] Logical Disk Free Space Monitor | This monitor is disabled as long as it duplicates the features of Windows Server 2016 and above Logical Disk Free Space Monitor | Enable this monitor only if necessary. |
| Reserved Monitor | This monitor is disabled by default as long as it is reserved. | Enable this monitor only if necessary. |
| Process Monitoring: Health State Collection | This rule is disabled because the process and port monitoring is to be enabled via the [process and port monitoring configuration wizard](#_Edit_Process_and). | Enable this rule only if necessary via the [process and port monitoring configuration wizard](#_Edit_Process_and). |
| Process Monitoring: Process Health State Subscription | This rule is disabled because the process and port monitoring is to be enabled via the [process and port monitoring configuration wizard](#_Edit_Process_and). | Enable this rule only if necessary via the [process and port monitoring configuration wizard](#_Edit_Process_and). |
| Process Monitoring: Performance Collection | This rule is disabled because the process and port monitoring is to be enabled via the [process and port monitoring configuration wizard](#_Edit_Process_and). | Enable this rule only if necessary via the [process and port monitoring configuration wizard](#_Edit_Process_and). |
| Process Monitoring: Process Performance Metric Subscription | This rule is disabled because the process and port monitoring is to be enabled via the [process and port monitoring configuration wizard](#_Edit_Process_and). | Enable this rule only if necessary via the [process and port monitoring configuration wizard](#_Edit_Process_and). |
| Process Monitoring: Network Port State Collection | This rule is disabled because the process and port monitoring is to be enabled via the [process and port monitoring configuration wizard](#_Edit_Process_and). | Enable this rule only if necessary via the [process and port monitoring configuration wizard](#_Edit_Process_and). |
| Process Monitoring: Process Network Port Subscription | This rule is disabled because the process and port monitoring is to be enabled via the [process and port monitoring configuration wizard](#_Edit_Process_and). | Enable this rule only if necessary via the [process and port monitoring configuration wizard](#_Edit_Process_and). |
| Process Monitoring: High Handle Count | This rule is disabled because the process and port monitoring is to be enabled via the [process and port monitoring configuration wizard](#_Edit_Process_and). | Enable this rule only if necessary via the [process and port monitoring configuration wizard](#_Edit_Process_and). |
| Process Monitoring: High Memory Percentage | This rule is disabled because the process and port monitoring is to be enabled via the [process and port monitoring configuration wizard](#_Edit_Process_and). | Enable this rule only if necessary via the [process and port monitoring configuration wizard](#_Edit_Process_and). |
| Process Monitoring: High Processor Time Percentage | This rule is disabled because the process and port monitoring is to be enabled via the [process and port monitoring configuration wizard](#_Edit_Process_and). | Enable this rule only if necessary via the [process and port monitoring configuration wizard](#_Edit_Process_and). |
| Process Monitoring: Number of Processes Collection | This rule is disabled because the process and port monitoring is to be enabled via the [process and port monitoring configuration wizard](#_Edit_Process_and). | Enable this rule only if necessary via the [process and port monitoring configuration wizard](#_Edit_Process_and). |
| Collection Rule for Windows Restarted Events | This collection rule is disabled based on customer feedback. | Enable this rule if the collection is required. |
| Collection rule for NTFS Quota Threshold Reached | This collection rule is disabled based on customer feedback. | Enable this rule if the collection is required. |
| Collection Rule for Software Updates Installation Events | This collection rule is disabled based on customer feedback. | Enable this rule if the collection is required. |
| Collection rule for NTFS Quota Threshold Limit Reached | This collection rule is disabled based on customer feedback. | Enable this rule if the collection is required. |
| Collection rule for Service or Driver Failed to Start events | This collection rule is disabled based on customer feedback. | Enable this rule if the collection is required. |
| Collection Rule for Windows Dirty Shutdown Events | This collection rule is disabled based on customer feedback. | Enable this rule if the collection is required. |
| Collection rule for invalid Share Configuration Detected | This collection rule is disabled based on customer feedback. | Enable this rule if the collection is required. |
| Collection Rule for Windows Clean Restart Events | This collection rule is disabled based on customer feedback. | Enable this rule if the collection is required. |
| Collection Rule for Software Updates Scheduled Installation Events | This collection rule is disabled based on customer feedback. | Enable this rule if the collection is required. |
| Collection Rule for Checking the File System Occurred on Startup | This collection rule is disabled based on customer feedback. | Enable this rule if the collection is required. |
| Collection Rule for Unexpected Service Terminations | This collection rule is disabled based on customer feedback. | Enable this rule if the collection is required. |
| Collection rule for Network Adapter was Disconnected from the Network | This collection rule is disabled based on customer feedback. | Enable this rule if the collection is required. |
| Collection Rule for Software Update Installation Failed | This collection rule is disabled based on customer feedback. | Enable this rule if the collection is required. |
| Collection Rule for Windows Restart Events (restarted from bug check) | This collection rule is disabled based on customer feedback. | Enable this rule if the collection is required. |
| TCPv6 Connections Reset | This rule is disabled based on customer feedback. | Enable this rule when required. |
| TCPv4 Segments Received Per Second | This rule is disabled based on customer feedback. | Enable this rule when required. |
| TCPv6 Segments Sent Per Second | This rule is disabled based on customer feedback. | Enable this rule when required. |
| TCPv6 Segments Received Per Second | This rule is disabled based on customer feedback. | Enable this rule when required. |
| TCPv6 Connection Failures | This rule is disabled based on customer feedback. | Enable this rule when required. |
| TCPv6 Connections Established | This rule is disabled based on customer feedback. | Enable this rule when required. |
| TCPv4 Segments Retransmitted Per Second | This rule is disabled based on customer feedback. | Enable this rule when required. |
| TCPv4 Connection Failures | This rule is disabled based on customer feedback. | Enable this rule when required. |
| TCPv4 Connections Established | This rule is disabled based on customer feedback. | Enable this rule when required. |
| TCPv4 Segments Sent Per Second | This rule is disabled based on customer feedback. | Enable this rule when required. |
| TCPv4 Connections Reset | This rule is disabled based on customer feedback. | Enable this rule when required. |
| TCPv6 Segments Retransmitted Per Second | This rule is disabled based on customer feedback. | Enable this rule when required. |
| TCPv6 Segments Received Per Second | This monitor is disabled based on customer feedback. | Enable this monitor when required. |
| TCPv4 Segments Received Per Second | This monitor is disabled based on customer feedback. | Enable this monitor when required. |
| TCPv6 Segments Sent Per Second | This monitor is disabled based on customer feedback. | Enable this monitor when required. |
| TCPv6 Segments Retransmitted Per Second | This monitor is disabled based on customer feedback. | Enable this monitor when required. |
| TCPv4 Segments Sent Per Second | This monitor is disabled based on customer feedback. | Enable this monitor when required. |
| TCPv4 Segments Retransmitted Per Second | This monitor is disabled based on customer feedback. | Enable this monitor when required. |
| Time Accuracy Out of Range | This monitor is disabled based on customer feedback. | Enable this monitor when required. |