Powershell Monitoring Framework

Lightweight Configuration Management Database

Author: Hugh Scott

Version: 1.0

Date: July 5, 2019

# Copyright

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

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

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

© 2018 Microsoft Corporation. All rights reserved.

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

# Version Control

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Changes** | **Comments** |
| 1.0 | 2019/07/05 | Hugh Scott | Original |  |

Table of Contents

[Copyright 2](#_Toc13230957)

[Version Control 3](#_Toc13230958)

[What’s New 5](#_Toc13230959)

[Background 6](#_Toc13230960)

[Setup Requirements and Permissions 6](#_Toc13230961)

[Server Installation Requirements 6](#_Toc13230962)

[Server Permission Requirements and Connectivity 6](#_Toc13230963)

[WMI and PowerShell Permissions 6](#_Toc13230964)

[SQL Server Permissions (Central Repository) 7](#_Toc13230965)

[SQL Server Permissions (Target Servers) 7](#_Toc13230966)

[Connectivity and Port Requirements 7](#_Toc13230967)

[Modules 7](#_Toc13230968)

[Monitor.ps1 7](#_Toc13230969)

[Configuration File 7](#_Toc13230970)

[Parameters 8](#_Toc13230971)

[Process overview for Monitor.ps1 9](#_Toc13230972)

[Sub Modules 9](#_Toc13230973)

[MonitorAdmin.ps1 13](#_Toc13230974)

[Scheduling 13](#_Toc13230975)

[General Notes on the Data Model 14](#_Toc13230976)

[Primary Keys and Unique Keys 14](#_Toc13230977)

[Active, dbAddDate, dbLastUpdate attributes 14](#_Toc13230978)

[Object Creation Time Stamp versus dbAddDate 15](#_Toc13230979)

[Historical Data 15](#_Toc13230980)

[Use of Data for Auditing 15](#_Toc13230981)

[Database Diagram: Computer 17](#_Toc13230982)

[Database Diagram: Database Instance 18](#_Toc13230983)

# What’s New

|  |  |  |
| --- | --- | --- |
| **Date** | **Version** | **Notes** |
| 2019/07/05 | 1.0.2.0 | Removed references to MonitorDomain.ps1 to a separate document. |

# Background

The Powershell Monitoring Framework is a collection of Powershell scripts used to monitor a Microsoft Windows environment, with a focus on Microsoft SQL Server assets. The tool is agentless and uses standard WMI and PowerShell cmdlets for most monitoring activities (there are still a few checks based on registry entries).

The primary purpose of the tool is to provide answers to the following types of questions:

1. How much storage do I have allocated to all of my Windows computers right now?
2. How much storage did I have allocated last year?
3. How many databases do I have, right now?
4. How many databases did I have last year?
5. What Windows applications do I have installed on these computers?
6. What services are running on these computers (or, which computers are running this Service)?
7. What SQL Agent jobs are scheduled in the environment (and which are failing)?

In summary, this tool is designed to measure and monitor your environment at a high level (and often in the aggregate). It’s an attempt to describe your Windows environment as a whole and not just as individual piece parts. It is also an attempt to measure your environment over long periods of time (even years).

***This is NOT a detailed performance monitoring tool.*** It is intended to be lightweight enough to store ***years*** *of data about your environment without consuming entire racks of storage.*

# Setup Requirements and Permissions

## Server Installation Requirements

Operating System:

Windows Server 2012

Windows Server 2012 R2

Windows Server 2016

Powershell Version: 4.0, 5.1

Software Requirements:

Failover Cluster PowerShell Cmdlets

SQL Server Shared Management Objects

## Server Permission Requirements and Connectivity

### WMI and PowerShell Permissions

Currently, the user account performing checks on remote computers needs to be a member of the local administrators group in order for all checks to be performed successfully.

### SQL Server Permissions (Central Repository)

There are predefined roles for each schema used for the checks to be successfully performed. The service account must be a member of the pre-defined roles in order to successfully update the database.

### SQL Server Permissions (Target Servers)

Although not confirmed, it should only be necessary to grant the following rights/privileges for SQL Server checks on remote computers to be performed successfully:

VIEW SERVER STATE

VIEW ANY DEFINITION

VIEW ANY DATABASE

In msdb:

SQLAgentReaderRole

In each database:

Create the user from the Windows login (needs only Public role).

### Connectivity and Port Requirements

Currently, port and network requirements are assessed to be:

ICMP Enabled (Ping)

TCP/UDP Port 135 Microsoft End Point Mapper / RPC Locator

## TCP/UDP Port 137: Netbios name service

## TCP/UDP Port 138: Netbios Datagram service

## TCP/UDP Port 139: Netbios Session service

TCP/UDP Port 445: Microsoft Active Directory, Windows Shares

# Modules

## Monitor.ps1

### Configuration File

Monitor.ps1 (as well as other components) use a single configuration file (app.monitor.config) which contains settings and values in XML format. These include:

*ThrottleLimit:* The number of concurrent checks that may be performed.

AgentName: The default agent name used when sourcing the list of computers to check from the central repository. The default may be overridden by specifying the –AgentName parameter in the monitor.ps1 command line.

ConnectionString: The connection string for the central repository.

### Parameters

#### Checks

An array of strings used to define which checks will be performed during execution of the script. This available values for this parameter are listed; invalid entries will be rejected and cause the script to fail. Current values (and their corresponding checks) are listed here:

| **Abbr** | **Check performed** | **Comment** |
| --- | --- | --- |
| Comp | Check computer system; all |  |
| Os | Check operating system; all |  |
| Disk | Check logical volume, physical disk and partitions; phys only |  |
| DiskSpc | Check logical volume space utilization; phys only |  |
| Clus | Check cluster configuration; all |  |
| CompShr | Check for computer share information; all |  |
| Hotifx | Check for Installed Windows Updates |  |
| InstApp | Check installed applications; phys only |  |
| Net | Check network configuration; phys only |  |
| NLB | Check network load balance configuration; phys only |  |
| Svcs | Check services; phys only |  |
| DiscSQL | Discover installed SQL instances; all |  |
| SQLEng | Check SQL Database Engine; only for discovered instances |  |
| SQLSize | Check SQL Database Size; only for discovered instances |  |
| Olap | Check SQL OLAP Engine; only for discovered instances |  |
| RptSvr | Check SQL Reporting Services; only for discovered instances |  |
| SQLJob | Check SQL Agent Jobs; only for discovered instances |  |
| SQLPerm | Check SQL Permissions; only for discovered instances |  |
| SysEvtLog | Check Windows System Event Log for critical events (WARNING!!!!! This can consume a large amount of space and time); phys only |  |
| AppEvtLog | Check Windows Application Event Log for critical events (WARNING!!!!! This can consume a large amount of space and time); phys only |  |
| WebURL | Test a URL; records response code and response time. |  |

#### Maintenance

An array of strings specifying maintenance to be performed on the database. Current valid values are:

|  |  |  |
| --- | --- | --- |
| **Abbr** | **Maintenance performed** | **Comment** |
| WriteHist | Writes daily summary data to historical tables from Raw tables |  |
| PurgeLog | Deletes entries from the Process Log |  |
| PurgeEvt | Deletes entries from the [cm].[Event] table |  |
| PurgeHist | Deletes historical data from daily summary and raw tables |  |

The retention values for each of these maintenance processes is stored as a varchar value in [dbo].[Config].

#### FileName

The user may specify a file name from which to retrieve computers for checks and validation. This should be a text file and each object to be checked should be entered on a separate line as a fully qualified domain name. For example:

<computer1>.<domain>.<net>

<computer2>.<domain>.<net>

<computer3>.<domain>.<net>

#### AgentName

When using the Central Repository to source the list of computers for checks, this parameter can be used to filter that list. This may be useful if you are monitoring multiple domains (with different credentials) or because the numbers of computers to monitor exceeds the workload capacity for one computer to process all the checks.

#### WhatIf

WhatIf is a switch parameter; if present (-whatif), then the process will simulate the actions indicated without actually performing any work. The console will output the simulated results. This can be useful to verify that the command syntax is correct, or to verify that the list of computers to be checked matches what the administrator is expecting to see (for example, when using multiple agents).

### Process overview for Monitor.ps1

At a high level, the following tasks are performed:

1. A connection is made to the central repository
2. Threading values are configured for parallelization
3. The list of computers to be checked is compiled; if no checks are specified, then this step is skipped.
   1. Each computer is tested for connectivity (ping, port 135)
   2. Each check is performed by spawning a new process (up to the throttle limit specified)
   3. The results are returned and errors/warnings tabulated
4. The list of maintenance tasks is enumerated; if no maintenance tasks are specified, then this step is skipped.

For a more detailed review of the tasks performed during each check, please see the notes below.

### Sub Modules

Each of the following modules is called from the primary module ***Monitor.ps1.*** These modules are NOT intended to be run by themselves.

#### CheckComputer.ps1

This module accesses the CIM\_ComputerSystem class and Win32\_ComputerSystemProduct to update table [cm].[Computer]. This is the base table (or “hardware” layer) of the setup.

Virtual network resources (for example SQL Server Virtual Network Names and MSCS Virtual Network names that are used for clustered resources are identified by a bit flag IsClusteredResource. These are added to the table for referential integrity. They are not physical entities.

Virtual machines are identified with a flag IsVirtual. The logic is embedded in the code. If the manufacturer is VMWare or Microsoft (Hyper-V), then the flag is set to true.

Some thought has been given to moving these entities to the [cm].[OperatingSystem] table and making that table the primary entity for everything except physical resources (disk drives, network adapaters, etc). That may be accomplished in a future release.

#### CheckOperatingSystem.ps1

The module accesses CIM\_OperatingSystem class to update the table [cm].[OperatingSystem].

Clustered resources (virtual network names) are also tracked in this entity. For this reason, it would probably be best to leave clustered entities out of [cm].[Computer] (which is meant to represent physical entities and virtual computer resources). That may be accomplished in a future release.

As part of the OperatingSystem check, the members of the Local Administrators group are enumerated and written to the table [cm].[ComputerGroupMember]. Active directory user accounts/groups may be cross referenced to the [ad].[User] or [ad].[Group] tables.

#### CheckCluster.ps1

This module attempts to discover and describe computers that are members of a Microsoft Failover Cluster. The module attempts to enumerate cluster components using Powershell cmdlets. For this reason, it is necessary to install the Microsoft Failover Cluster components (in Windows 7, these are found in the Add Windows Components after installing Remote Server Administration Tools).

The module attempts to enumerate Cluster Nodes, Cluster Resources, Cluster Groups and the Failover Cluster name. Any resource that is identified as a Network Name is added to the [cm].[Computer] table with the value IsClusterResource set to true.

#### CheckDisk.ps1

This module attempts to enumerate Logical Volumes, Physical Disks, Drive Partitions and the relationships found between Logical Volumes and Physical Disks. In order to describe mounted volumes, the component uses the Win32\_Volume (instead of CIM\_LogicalDisk). Only local drive types (DriveType = 3) are described.

In an effort to reduce complexity and duplication, an effort is made to identify the owner of a clustered disk before adding it to the database.

#### CheckNetwork.ps1

This module uses Win32\_NetworkAdapter and Win32\_NetworkAdapterConfiguration to identify adapters where TCP is enabled.

These entities are related to [cm].[ComputerSystem]. All IP addresses for a Network adapter are enumerated and listed in the IPAddress column.

#### CheckEvents.ps1

This module will attempt to enumerate entries in the specified Windows Event log (currently the System Event log and the Application Event log). The first time that the check is performed for a particular computer, it will retrieve all critical events logged for the past 14 days. After the initial load, the logic of the process is to retrieve only critical events that have occurred since the last critical entry was logged.

**WARNING!!!** This process can be resource intensive and can generate a lot of network traffic (as well as a lot of entries in the [cm].[Event] table.

**NOTE:** Only critical events are collected. Warnings and informational events are ignored.

**NOTE:** In an effort to limit traffic and load, virtual network resources are ignored when collecting events.

#### CheckInstalledApplications.ps1

This module attempts to enumerate entries from the Windows uninstall registry hive. An effort is made to create a “normalized” table of installed applications, along with a linked table showing which computers those applications are installed on.

**NOTE:** Some applications do not use the Windows uninstall registry. Applications such as Oracle have their own install/uninstall routines and therefore will not be discovered as part of this process.

**NOTE:** This process will ***not*** enumerate Windows Updates that have been installed. See the description for *CheckInstalledHotfix.ps1*.

#### CheckInstalledHotfix

This module uses the Powershell cmdlet Get-Hotfix to enumerate the installed hotfixes on a computer. Entries are written to [cm].[WindowsUpdateInstallation]. Similar to the module *CheckInstalledApplications.ps1*, this module maintains a “master” copy of hotfixes in [cm].[WindowsUpdate].

#### CheckServices.ps1

This module enumerates and describes entries from the Win32\_Service class. An attempt was made to use the CIM\_Service class, but it proved to be too slow for practical use.

#### CheckComputerShare.ps1

This module enumerates Shared resources (printers, file shares and administrative shares) for each computer object. The module uses Win32\_Share to list these resources.

#### CheckSQLInstance.ps1

This module attempts to discover installed components of SQL Server (the database engine, Analysis Services and Reporting Services). As yet, SSIS is not included in the discovery routing.

This process is heavily dependent on the Windows Registry to identify installed SQL components and to list out their properties. Due to complications involved in connecting to non-default instances when port 1434 is blocked (or when the SQL Browser is disabled), the process tries to identify non-default ports for the database engine using the entries found in **SuperSocketNetLib\Tcp\IPAll**. This is not always valid.

Alone among the various SQL modules, this module does not use alternate database credentials (thought it can use alternate credentials for OS checks). This module does not actually log in to the database instance at all.

For each of the discovered SQL Classes and instances, an effort is made to determine if the appropriate service for that resource is running.

For Reporting Services, some manual work will need to occur to update the URL for the more detailed Reporting Services process to work.

#### CheckSQLEngine.ps1

This module lists the databases, data files, database properties, server properties and linked servers for the discovered instances on a particular host.

#### CheckSQLJobs.ps1

This module checks the SQL Agent jobs for the discovered instances on a particular host. It does NOT return the detailed list of steps, nor a detailed job history for each job. It is intended to be as fast and lightweight as possible in order to facilitate a quick check (which can therefore be run multiple times).

#### CheckSQLPermissions.ps1

This module enumerates all the logins on a SQL database instance as well as server permissions, database users and database permissions. Object, Server and Database Permissions are all stored in a single table called [cm].[DatabasePermission]. This was an effort to simplify the data solution. A surrogate column was added to define which type of permission is being described.

#### CheckSQLReportingServer.ps1

This module enumerates reports, data sources, data sets, subscriptions and subscription parameters that are related to an instance of SQL Server Reporting Services. Note that the URL for the report server instance must be manually configured by an administrator.

#### CheckSQLAnalysisServer.ps1

This module enumerates the databases and cubes and the server properties for each discovered instance of SQL Analysis Services.

#### CheckSQLDatabaseSize.ps1

This module updates the attributes DataFileSize, DataFileSpaceUsed, LogFileSize and LogFileSpaceUsed for each database in an instance. It also writes an entry into [pm].[DabaseSizeRaw]. The entries in [pm].[DatabaseSizeRaw] are summarized daily into [pm].[DatabaseSizeDaily] as part of the WriteHistory task which is part of the maintenance process.

#### CheckDiskSpace.ps1

This module updates the attribute SpaceUsed in [cm].[LogicalVolume]. In addition, it writes an entry into [pm].[LogicalVolumeSizeDaily]. The entries in [pm].[LogicalVolumeSizeRaw] are summarized daily into [pm].[LogicalVolumeSizeDaily as part of the WriteHistory task which is part of the maintenance process.

#### CheckWebURL.ps1

This module tests a URL for response code and response time. The latest response time and response code are written to [cm].[WebApplicationURL], while a record of each check is written to [pm].[WebApplicationURLResponseRaw]. This check is useful for validating that web services are up and responding to url requests. It is also useful to “warm” .Net services (such as Reporting Services) whose application pools periodically shut down (thus leading to lengthy response times when accessed by end users).

#### CheckNLBCluster.ps1

This module checks for Windows Network Load Balanced clusters, discovers the underlying node(s) and updates the status of the underlying node(s). This module requires installation of Windows Network Load Balance client tools and uses NLB PowerShell cmdlets.

## MonitorAdmin.ps1

# Scheduling

The key to being able to answer these questions effectively is to schedule the various scripts to run at appropriate and predictable intervals. The following tables should serve as a guideline for the frequency with which checks should be performed:

#### WMI and PowerShell based Checks Schedule (Sample)

| **Abbr** | **Frequency** | **Comment** |
| --- | --- | --- |
| Comp | Daily |  |
| Os | Daily |  |
| Disk | Daily |  |
| DiskSpc | Hourly |  |
| Clus | Daily |  |
| CompShr | Daily |  |
| Hotfix | Weekly |  |
| InstApp | Weekly |  |
| Net | Daily |  |
| NLB | Hourly (\*) |  |
| Svcs | Hourly (\*) |  |
| DiscSQL | Daily |  |
| SQLEng | Daily |  |
| SQLSize | Hourly (\*) |  |
| Olap | Daily |  |
| RptSvr | Daily |  |
| SQLJob | Hourly (\*) |  |
| SQLPerm | Weekly |  |
| SysEvtLog | Daily (\*\*) |  |
| AppEvtLog | Daily (\*\*) |  |
| WebURL | Every 10-15 minutes (\*\*\*) |  |

(\*) These checks are designed to be lightweight and fast; they may be run more frequently, but in no case would I attempt to run them more than every ten minutes. Remember! This is not intended to be a real time monitoring system.

(\*\*) The Event Log checks can be very intensive depending on how many entries are in the individual log files. There are better tools for monitoring Windows Event logs, but this functionality can be useful in a pinch.

(\*\*\*) The WebURL check is intended to be very lightweight and fast. In order to serve as a “cache warming” service, it needs to be run frequently enough to prevent application pools from shutting down.

#### Maintenance Tasks

| **Abbr** | **Frequency** | **Comment** |
| --- | --- | --- |
| WriteHist | Daily | Schedule shortly after midnight |
| PurgeLog | Daily | Schedule off hours |
| PurgeEvt | Daily | Schedule off hours |
| PurgeHist | Daily | Schedule off hours |

# General Notes on the Data Model

## Primary Keys and Unique Keys

In most cases, entities have a primary key defined (usually [objectGUID] which is a uniqueidentifier). There should also be a unique index described for each entity to prevent duplicate values from being loaded into the table (for example, dnsHostName is the unique key for [cm].[Computer]. In some cases, the unique index is a compound key (such as [DatabaseInstanceGUID] and [DatabaseName] for [cm].[Database].

In many cases, if the object being described already had a clearly defined GUID value (for example, ID for SQL Agent Job), then I used that value as-is for the [objectGUID] value. This is probably a violation of best practices, but it made sense to me at the time.

## Active, dbAddDate, dbLastUpdate attributes

Each entity contains three common attributes: Active (Boolean), dbAddDate and dbLastUpdate. The state of these three attributes is related to whether an object currently exists, when it was first discovered and when it was last updated.

An entity with an Active attribute of 1 means that -- as of the value in dbLastUpdate – that entity was found to exist in the environment. An entity with an Active attribute of 0 means that that entity was inactivated (as of dbLastUpdate) and ***not found*** during the last check process.

As part of the check process, each routine will first “Inactivate” (set the Active flag to 0) for all objects (of the same object type) belonging to the parent of that object. For example, before enumerating the Logical Volumes on a computer, all existing Logical Volumes, ***for that computer*** are first “Inactivated”. As each volume is then enumerated, the value of the flag is set back to 1.

If a previously discovered object has been removed from a computer (for instance, following the above example, if a Logicial Volume was removed from a computer) then the Active flag (which had been set to 0) will not get set back to 1. Effectively, the application has “discovered” that this object has been delete

In most cases, this process is very fast and the user won’t notice if an object momentarily “goes away”. However, administrators must take care not to schedule reports during mass discovery operations (for example, you should take care not to schedule reports against the database during a period when the disk entities are being updated).

The value of inactivating (versus hard deleting a record) is that we retain the history of the environment from the time that an object was first discovered, even after that object has been retired from the environment. In addition, it can help identify certain Active Directory objects which persist, even though the object has been disabled.

## Object Creation Time Stamp versus dbAddDate

In some cases, entities have their own “Creation time stamp” (such as the Active Directory attribute “whenCreated”). Always keep in mind that the time an object is created does not necessarily correlate with the time that an object is discovered by the application. In cases where these is no creation time stamp attribute, **you must not infer too much information from dbAddDate**. This attribute simply describes when the entity was first added to the database. Only after you have established a set schedule for running the various processes (and have been running it for a while) can you begin to infer things like: “well, the application wasn’t here last week, and it’s here now: therefore it must have been added in the last week.”

Bear in mind that this process/tool was **never intended for real time monitoring.** In most cases, the major checks were only scheduled to be run daily or at most twice daily.

## Historical Data

Certain exceptions exist: the *CheckDiskSpace.ps1* and *CheckDatabaseSize.ps1* scripts do NOT inactivate objects. They simply check the sizes of known entities and update the Raw data tables so that a history of these statistics can be maintained.

## Use of Data for Auditing

It’s important to point out another key limitation of this application: **although this tool can be useful for auditing the current state of your environment, it is not a proper auditing solution.** The tool lacks the necessary transactional component(s) -- not to mention the necessary security controls -- to be used in an auditing role. Nevertheless, it can be used to quickly answer questions such as:

1. What permissions do my SQL Server users have and what permissions did they have last month?
2. Who was a member of this Active Directory group last month (and are they still a member today)?
3. How do the permissions in SQL production compare with those in my other environments?

# Database Diagram: Computer



# Database Diagram: Database Instance

