Full credit is given to the above companies including the OS that this PDF file was generated!

PowerShell Get-Help on command 'Get-MpPerformanceReport'

PS C:\Users\wahid> Get-Help Get-MpPerformanceReport

NAME

Get-MpPerformanceReport

SYNOPSIS

This cmdlet reports the file paths, file extensions, and processes that cause the highest impact to Microsoft Defender Antivirus scans.

SYNTAX

Get-MpPerformanceReport [-Path] <String> [-TopFiles <Int32>] [-TopScansPerFile <Int32>] [-TopProcessesPerFile <Int32>] [-TopScansPerProcessPerFile <Int32>] [-TopPaths <Int32>] [-TopPathsDepth <Int32>] [-TopScansPerPath <Int32>] [-TopFilesPerPath <Int32>] [-TopScansPerFilePerPath <Int32>] [-TopExtensionsPerPath <Int32>] [-TopScansPerExtensionPerPath <Int32>] [-TopProcessesPerPath <Int32>] [-TopScansPerProcessPerPath <Int32>] [-TopExtensions <Int32>] [-TopScansPerExtension <Int32>] [-TopPathsPerExtension <Int32>] [-TopScansPerPathPerExtension <Int32>] [-TopFilesPerExtension <Int32>] [-TopScansPerFilePerExtension <Int32>] [-TopProcessesPerExtension <Int32>] [-TopScansPerProcessPerExtension <Int32>] [-TopProcesses <Int32>] [-TopScansPerProcess <Int32>] [-TopFilesPerProcess <Int32>] [-TopScansPerFilePerProcess <Int32>] [-TopExtensionsPerProcess

<Int32>] [-TopScansPerExtensionPerProcess <Int32>] [-TopPathsPerProcess <Int32>] [-TopScansPerPathPerProcess <Int32>] [-TopScans <Int32>] [-MinDuration <String>] [-MinStartTime <DateTime>] [-MinEndTime <DateTime>] [-MaxStartTime <DateTime>] [-MaxEndTime <DateTime>] [-Overview] [-Raw] [<CommonParameters>]

DESCRIPTION

This cmdlet analyzes a previously collected Microsoft Defender Antivirus performance recording and reports the file paths, file extensions and processes that cause the highest impact to Microsoft Defender Antivirus scans.

The performance analyzer provides insight into problematic files that could cause performance degradation of Microsoft Defender Antivirus. This tool is provided "AS IS", and is not intended to provide suggestions on exclusions. Exclusions can reduce the level of protection on your endpoints. Exclusions, if any, should be defined with caution.

PARAMETERS

-Path <String>

Specifies the location of Microsoft Defender Antivirus performance recording to analyze.

-TopFiles <Int32>

Requests a top files report and specifies how many top files to output, sorted by "Duration".

-TopScansPerFile <Int32>

Specifies how many top scans to output for each top file, sorted by "Duration".

-TopProcessesPerFile <Int32>

Specifies how many top processes to output for each top file, sorted by "Duration".

-TopScansPerProcessPerFile <Int32>

Specifies how many top scans to output for each top process for each top file, sorted by "Duration".

-TopPaths <Int32>

Requests a top paths report and specifies how many top entries to output, sorted by "Duration". This is called recursively for each directory entry. Scans are grouped hierarchically per folder and sorted by "Duration".

-TopPathsDepth <Int32>

Specifies the maxmimum depth (path-wise) that will be used to grop scans when $TopPaths is used.

-TopScansPerPath <Int32>

Specifies how many top scans to output for each top path, sorted by "Duration".

-TopFilesPerPath <Int32>

Specifies how many top files to output for each top path, sorted by "Duration".

-TopScansPerFilePerPath <Int32>

Specifies how many top scans to output for each top file for each top path, sorted by "Duration".

-TopExtensionsPerPath <Int32>

Specifies how many top extensions to output for each top path, sorted by "Duration".

-TopScansPerExtensionPerPath <Int32>

Specifies how many top scans to output for each top extension for each top path, sorted by "Duration".

-TopProcessesPerPath <Int32>

Specifies how many top processes to output for each top path, sorted by "Duration".

-TopScansPerProcessPerPath <Int32>

Specifies how many top scans to output for each top process for each top path, sorted by "Duration".

-TopExtensions <Int32>

Requests a top extensions report and specifies how many top extensions to output, sorted by "Duration".

-TopScansPerExtension <Int32>

Specifies how many top scans to output for each top extension, sorted by "Duration".

-TopPathsPerExtension <Int32>

Specifies how many top paths to output for each top extension, sorted by "Duration".

-TopScansPerPathPerExtension <Int32>

Specifies how many top scans to output for each top path for each top extension, sorted by "Duration".

-TopFilesPerExtension <Int32>

Specifies how many top files to output for each top extension, sorted by "Duration".

-TopScansPerFilePerExtension <Int32>

Specifies how many top scans to output for each top file for each top

extension, sorted by "Duration".

-TopProcessesPerExtension <Int32>

Specifies how many top processes to output for each top extension, sorted by "Duration".

-TopScansPerProcessPerExtension <Int32>

Specifies how many top scans to output for each top process for each top extension, sorted by "Duration".

-TopProcesses <Int32>

Requests a top processes report and specifies how many top processes to output, sorted by "Duration".

-TopScansPerProcess <Int32>

Specifies how many top scans to output for each top process in the Top Processes report, sorted by "Duration".

-TopFilesPerProcess <Int32>

Specifies how many top files to output for each top process, sorted by "Duration".

-TopScansPerFilePerProcess <Int32>

Specifies how many top scans to output for each top file for each top process, sorted by "Duration".

-TopExtensionsPerProcess <Int32>

Specifies how many top extensions to output for each top process, sorted by "Duration".

-TopScansPerExtensionPerProcess <Int32>

Specifies how many top scans to output for each top extension for each top process, sorted by "Duration".

-TopPathsPerProcess <Int32>

Specifies how many top paths to output for each top process, sorted by "Duration".

-TopScansPerPathPerProcess <Int32>

Specifies how many top scans to output for each top path for each top process, sorted by "Duration".

-TopScans <Int32>

Requests a top scans report and specifies how many top scans to output, sorted by "Duration".

-MinDuration <String>

Specifies the minimum duration of any scans or total scan durations of files, extensions and processes included in the report.
Accepts values like '0.1234567sec' or '0.1234ms' or '0.1us' or a valid TimeSpan.

-MinStartTime <DateTime>

Specifies the minimum start time of scans included in the report. Accepts a valid DateTime.

-MinEndTime <DateTime>

Specifies the minimum end time of scans included in the report. Accepts a valid DateTime.

-MaxStartTime <DateTime>

Specifies the maximum start time of scans included in the report. Accepts a valid DateTime.

-MaxEndTime <DateTime>

Specifies the maximum end time of scans included in the report. Accepts a

valid DateTime.

-Overview [<SwitchParameter>]

Adds an overview or summary of the scans captured in the trace to the regular output.

-Raw [<SwitchParameter>]

Specifies that the output should be machine readable and readily convertible to serialization formats like JSON.

- Collections and elements are not be formatted.
- TimeSpan values are represented as number of 100-nanosecond intervals.
- DateTime values are represented as number of 100-nanosecond intervals since January 1, 1601 (UTC).

<CommonParameters>

This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer, PipelineVariable, and OutVariable. For more information, see about_CommonParameters (https:/go.microsoft.com/fwlink/?LinkID=113216).

---------- EXAMPLE 1 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopFiles:10 -TopExtensions:10 -TopProcesses:10 -TopScans:10

---------- EXAMPLE 2 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopFiles:10

-TopExtensions:10 -TopProcesses:10 -TopScans:10 -Raw | ConvertTo-Json

---------- EXAMPLE 3 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopScans:10

---------- EXAMPLE 4 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopFiles:10

---------- EXAMPLE 5 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopFiles:10
-TopScansPerFile:3

---------- EXAMPLE 6 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopFiles:10
-TopProcessesPerFile:3

---------- EXAMPLE 7 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopFiles:10
-TopProcessesPerFile:3 -TopScansPerProcessPerFile:3

---------- EXAMPLE 8 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopPaths:10

---------- EXAMPLE 9 ----------

```
PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopPaths:10
-TopPathsDepth:3
```

---------- EXAMPLE 10 ----------

```
PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopPaths:10
-TopPathsDepth:3 -TopScansPerPath:3
```

---------- EXAMPLE 11 ----------

```
PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopPaths:10
-TopScansPerPath:3
```

---------- EXAMPLE 12 ----------

```
PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopPaths:10
-TopPathsDepth:3 -TopFilesPerPath:3
```

---------- EXAMPLE 13 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopPaths:10
-TopFilesPerPath:3

---------- EXAMPLE 14 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopPaths:10
-TopPathsDepth:3 -TopFilesPerPath:3 -TopScansPerFilePerPath:3

---------- EXAMPLE 15 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopPaths:10
-TopFilesPerPath:3 -TopScansPerFilePerPath:3

---------- EXAMPLE 16 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopPaths:10
-TopPathsDepth:3 -TopExtensionsPerPath:3

---------- EXAMPLE 17 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopPaths:10
-TopExtensionsPerPath:3

---------- EXAMPLE 18 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopPaths:10
-TopPathsDepth:3 -TopExtensionsPerPath:3 -TopScansPerExtensionPerPath:3

---------- EXAMPLE 19 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopPaths:10
-TopExtensionsPerPath:3 -TopScansPerExtensionPerPath:3

---------- EXAMPLE 20 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopPaths:10
-TopPathsDepth:3 -TopProcessesPerPath:3

---------- EXAMPLE 21 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopPaths:10
-TopProcessesPerPath:3

---------- EXAMPLE 22 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopPaths:10
-TopPathsDepth:3 -TopProcessesPerPath:3 -TopScansPerProcessPerPath:3

---------- EXAMPLE 23 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopPaths:10

-TopProcessesPerPath:3 -TopScansPerProcessPerPath:3

---------- EXAMPLE 24 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopExtensions:10

---------- EXAMPLE 25 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopExtensions:10

-TopScansPerExtension:3

---------- EXAMPLE 26 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopExtensions:10
-TopPathsPerExtension:3

---------- EXAMPLE 27 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopExtensions:10
-TopPathsPerExtension:3 -TopPathsDepth:3

---------- EXAMPLE 28 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopExtensions:10
-TopPathsPerExtension:3 -TopPathsDepth:3 -TopScansPerPathPerExtension:3

---------- EXAMPLE 29 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopExtensions:10
-TopPathsPerExtension:3 -TopScansPerPathPerExtension:3

---------- EXAMPLE 30 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopExtensions:10
-TopFilesPerExtension:3

---------- EXAMPLE 31 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopExtensions:10
-TopFilesPerExtension:3 -TopScansPerFilePerExtension:3

---------- EXAMPLE 32 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopExtensions:10
-TopProcessesPerExtension:3

---------- EXAMPLE 33 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopExtensions:10
-TopProcessesPerExtension:3 -TopScansPerProcessPerExtension:3

---------- EXAMPLE 34 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopProcesses:10

---------- EXAMPLE 35 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopProcesses:10
-TopScansPerProcess:3

---------- EXAMPLE 36 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopProcesses:10
-TopExtensionsPerProcess:3

---------- EXAMPLE 37 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopProcesses:10
-TopExtensionsPerProcess:3 -TopScansPerExtensionPerProcess:3

---------- EXAMPLE 38 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopProcesses:10
-TopFilesPerProcess:3

---------- EXAMPLE 39 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopProcesses:10
-TopFilesPerProcess:3 -TopScansPerFilePerProcess:3

---------- EXAMPLE 40 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopProcesses:10
-TopPathsPerProcess:3

---------- EXAMPLE 41 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopProcesses:10
-TopPathsPerProcess:3 -TopPathsDepth:3

---------- EXAMPLE 42 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopProcesses:10
-TopPathsPerProcess:3 -TopPathsDepth:3 -TopScansPerPathPerProcess:3

---------- EXAMPLE 43 ----------

PS C:\>Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopProcesses:10
-TopPathsPerProcess:3 -TopScansPerPathPerProcess:3

---------- EXAMPLE 44 ----------

PS C:\># Find top 10 scans with longest durations that both start and end
between MinStartTime and MaxEndTime:

Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopScans:10
-MinStartTime:"5/14/2022 7:01:11 AM" -MaxEndTime:"5/14/2022 7:01:41 AM"

---------- EXAMPLE 45 ----------

PS C:\># Find top 10 scans with longest durations between MinEndTime and
MaxStartTime, possibly partially overlapping this period

Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopScans:10

-MinEndTime:"5/14/2022 7:01:11 AM" -MaxStartTime:"5/14/2022 7:01:41 AM"

---------- EXAMPLE 46 ----------

PS C:\># Find top 10 scans with longest durations between MinStartTime and MaxStartTime, possibly partially overlapping this period

Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopScans:10 -MinStartTime:"5/14/2022 7:01:11 AM" -MaxStartTime:"5/14/2022 7:01:41 AM"

---------- EXAMPLE 47 ----------

PS C:\># Find top 10 scans with longest durations that start at MinStartTime or later:

Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopScans:10 -MinStartTime:"5/14/2022 7:01:11 AM"

---------- EXAMPLE 48 ----------

PS C:\># Find top 10 scans with longest durations that start before or at MaxStartTime:

Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopScans:10

-MaxStartTime:"5/14/2022 7:01:11 AM"

---------- EXAMPLE 49 ----------

PS C:\># Find top 10 scans with longest durations that end at MinEndTime or later:

Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopScans:10 -MinEndTime:"5/14/2022 7:01:11 AM"

---------- EXAMPLE 50 ----------

PS C:\># Find top 10 scans with longest durations that end before or at MaxEndTime:

Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopScans:10 -MaxEndTime:"5/14/2022 7:01:11 AM"

---------- EXAMPLE 51 ----------

PS C:\># Find top 10 scans with longest durations, impacting the current interval, that did not start or end between MaxStartTime and MinEndTime.

Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopScans:10

-MaxStartTime:"5/14/2022 7:01:11 AM" -MinEndTime:"5/14/2022 7:01:41 AM"

---------- EXAMPLE 52 ----------

PS C:\># Find top 10 scans with longest durations, impacting the current interval, that started between MinStartTime and MaxStartTime, and ended later than MinEndTime.

Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopScans:10 -MinStartTime:"5/14/2022 7:00:00 AM" -MaxStartTime:"5/14/2022 7:01:11 AM" -MinEndTime:"5/14/2022 7:01:41 AM"

---------- EXAMPLE 53 ----------

PS C:\># Find top 10 scans with longest durations, impacting the current interval, that started before MaxStartTime, and ended between MinEndTime and MaxEndTime.

Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopScans:10 -MaxStartTime:"5/14/2022 7:01:11 AM" -MinEndTime:"5/14/2022 7:01:41 AM" -MaxEndTime:"5/14/2022 7:02:00 AM"

---------- EXAMPLE 54 ----------

PS C:\># Find top 10 scans with longest durations, impacting the current interval, that started between MinStartTime and MaxStartTime, and ended between MinEndTime and MaxEndTime.

```
Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopScans:10
-MinStartTime:"5/14/2022 7:00:00 AM" -MaxStartTime:"5/14/2022 7:01:11 AM"
-MinEndTime:"5/14/2022 7:01:41 AM" -MaxEndTime:"5/14/2022 7:02:00 AM"
```

---------- EXAMPLE 55 ----------

PS C:\># Find top 10 scans with longest durations that both start and end between MinStartTime and MaxEndTime, using DateTime as raw numbers in FILETIME format, e.g. from -Raw report format:

```
Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopScans:10
-MinStartTime:([DateTime]::FromFileTime(132969744714304340))
-MaxEndTime:([DateTime]::FromFileTime(132969745000971033))
```

---------- EXAMPLE 56 ----------

PS C:\># Find top 10 scans with longest durations between MinEndTime and MaxStartTime, possibly partially overlapping this period, using DateTime as raw numbers in FILETIME format, e.g. from -Raw report format:

```
Get-MpPerformanceReport -Path:.\Defender-scans.etl -TopScans:10
-MinEndTime:([DateTime]::FromFileTime(132969744714304340))
-MaxStartTime:([DateTime]::FromFileTime(132969745000971033))
```

---------- EXAMPLE 57 ----------

PS C:\># Display a summary or overview of the scans captured in the trace, in
addition to the information displayed regularly through other arguments.
Output is influenced by time interval arguments MinStartTime and MaxEndTime.

Get-MpPerformanceReport -Path:.\Defender-scans.etl [other arguments] -Overview

REMARKS

To see the examples, type: "get-help Get-MpPerformanceReport -examples".
For more information, type: "get-help Get-MpPerformanceReport -detailed".
For technical information, type: "get-help Get-MpPerformanceReport -full".