Windows PowerShell Get-Help on Cmdlet 'Get-SystemDriver'

PS:\>Get-HELP Get-SystemDriver -Full

NAME

Get-SystemDriver

SYNOPSIS

Scans for drivers on the system.

SYNTAX

Get-SystemDriver [-Audit] [-NoScript] [-NoShadowCopy] [-OmitPaths <String[]>] [-PathToCatroot <String>] [-ScanPath <String>] [-ScriptFileNames] [-UserPEs]

[<CommonParameters>]

DESCRIPTION

The Get-SystemDriver cmdlet performs a full system scan for drivers. This cmdlet returns a DriverFile object that contains information for the New-CIPolicyRule and

New-CIPolicy cmdlets. Those cmdlets create rules based on the scanned files. By default, this cmdlet recursively scans C:\ and includes only kernel mode files.

PARAMETERS

-Audit [<SwitchParameter>]

Indicates that this cmdlet searches the Code Integrity Audit log for drivers. It does not perform a full system scan.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-NoScript [<SwitchParameter>]

Indicates that this cmdlet does not scan script files. It searches portable executable files (PE files) only.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-NoShadowCopy [<SwitchParameter>]

Indicates that the Volume Snapshot Service (VSS) does not make a shadow copy of the disk while the scan runs. This parameter could cause an incomplete scan for a

system that is running.

If a scan fails due to VSS errors caused by low disk space on the target drive, this cmdlet prompts you to specify this parameter.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-OmitPaths <String[]>

Specifies an array of paths that this cmdlet omits from the scan. We recommend that you omit C:\Windows.old.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-PathToCatroot <String>

Specifies the path of the CatRoot folder. Specify this parameter to scan a remote or mounted drive.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ScanPath <String>

Specifies the path for this cmdlet to scan. You can specify a local or remote path. If you specify a remote or mounted drive, also specify the PathToCatroot

parameter.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ScriptFileNames [<SwitchParameter>]

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-UserPEs [<SwitchParameter>]

Indicates that this cmdlet includes user mode files in the scan.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

<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).

INPUTS

OUTPUTS

DriverFile

This cmdlet returns a DriverFile object that contains all properties and certificates of a driver that you must have in order to generate a Code Integrity policy

rule.

NOTES

---------- Example 1: Scan a folder for drivers ----------

PS C:\> Get-SystemDriver -ScanPath '.\temp' -UserPEs

FilePath : \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy9\cmdlets\temp\ConfigCI.psd1

FriendlyName : \\?\E:\cmdlets\temp\ConfigCI.psd1

FileName :

Loaded : False

FileVersion :

Hash : 1844B4531711EC9170A9D33277CE1D4FF7626C54

Hash256 : 60311157F6685727F42CC04717FEF6F905EC2A317C3B8381CDD9A79D0B184483

PageHash :

PageHash256 :

UserMode : True

OpusInfos : {}

Signers : {}

FilePath : \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy9\cmdlets\temp\Microsoft.ConfigCI.Commands.dll

FriendlyName : \\?\E:\cmdlets\temp\Microsoft.ConfigCI.Commands.dll

FileName : Microsoft.ConfigCI.Commands.dll

Loaded : False

FileVersion : 10.0.10543.1000

Hash : BE0777F5AF88628D4555A875036648DF1AD19BBE

Hash256 : 6FA5AF724499C338A77FEEAD90F55DDF5F23D081C6DCE8E9DF486E95C6A9B310

PageHash : D41570F2E6E7E6245CF342131D4706C944562B1E

PageHash256 : F714D9784E15B88F56180C8EE2B40C769CC83428954585A1DCF9A260FE967CDD

UserMode : False

OpusInfos : {}

Signers : {}

This command scans the specified folder. The command returns the DriverFile object that is used to make rules.

Provide this object to New-CIPolicyRule to create a rule.

------ Example 2: Scan only PE files and exclude a folder ------

PS C:\> Get-SystemDriver -ScanPath '.\temp\' -UserPEs -OmitPaths '.\temp\ConfigCITestBinaries' -NoScript

FilePath : \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy10\cmdlets\temp\Microsoft.ConfigCI.Commands.dll

FriendlyName : \\?\E:\cmdlets\temp\Microsoft.ConfigCI.Commands.dll

FileName : Microsoft.ConfigCI.Commands.dll

Loaded : False

FileVersion : 10.0.10543.1000

Hash : BE0777F5AF88628D4555A875036648DF1AD19BBE

Hash256 : 6FA5AF724499C338A77FEEAD90F55DDF5F23D081C6DCE8E9DF486E95C6A9B310

PageHash : D41570F2E6E7E6245CF342131D4706C944562B1E

PageHash256 : F714D9784E15B88F56180C8EE2B40C769CC83428954585A1DCF9A260FE967CDD

UserMode : False

OpusInfos : {}

Signers : {}

FilePath : \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy10\cmdlets\temp\Microsoft.ConfigCI.Commands.dll

FriendlyName : \\?\E:\cmdlets\temp\Microsoft.ConfigCI.Commands.dll

FileName : Microsoft.ConfigCI.Commands.dll

Loaded : False

FileVersion : 10.0.10543.1000

Hash : BE0777F5AF88628D4555A875036648DF1AD19BBE

Hash256 : 6FA5AF724499C338A77FEEAD90F55DDF5F23D081C6DCE8E9DF486E95C6A9B310

PageHash : D41570F2E6E7E6245CF342131D4706C944562B1E

PageHash256 : F714D9784E15B88F56180C8EE2B40C769CC83428954585A1DCF9A260FE967CDD

UserMode : True

OpusInfos : {}

Signers : {}

This command scans the specified folder, just like the previous example. This command specifies the OmitPaths parameter to exclude files in the

temp\ConfigCITestBinaries folder. The command specifies the NoScript parameter so that it gets information for only PE files.

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/configci/get-systemdriver?view=windowsserver2022-ps&wt.mc_id=ps-gethelp

New-CIPolicy

New-CIPolicyRule