Windows PowerShell Get-Help on Cmdlet 'Show-NetFirewallRule'

PS:\>Get-HELP Show-NetFirewallRule -Full

NAME

  Show-NetFirewallRule

SYNOPSIS

  Displays all of the existing firewall rules and associated objects in a fully expanded view.

SYNTAX

    Show-NetFirewallRule [-AsJob] [-CimSession <CimSession[]>] [-GPOSession <String>] [-PolicyStore <String>]
[-ThrottleLimit <Int32>] [<CommonParameters>]

DESCRIPTION

  The Show-NetFirewallRule cmdlet displays each of the firewall rules in the policy store, along with the associated objects,
in a clear and formatted list.

  The ActiveStore is a collection of all of the policy stores that apply to the computer, so the majority of rules output from
the following cmdlet are read-only when
  run on a client computer. - `Show-NetFirewallRule -PolicyStore ActiveStore`

PARAMETERS

-AsJob [<SwitchParameter>]

Runs the cmdlet as a background job. Use this parameter to run commands that take a long time to complete.

Required?   false

Position?   named

Default value   False

Accept pipeline input?   False

Accept wildcard characters? false

-CimSession <CimSession[]>

Runs the cmdlet in a remote session or on a remote computer. Enter a computer name or a session object, such as the output of a New-CimSession

(https://go.microsoft.com/fwlink/p/?LinkId=227967)   or

[Get-CimSession](https://go.microsoft.com/fwlink/p/?LinkId=227966)cmdlet. The default is the current session

on the local computer.

Required?   false

Position?   named

Default value   None

Accept pipeline input?   False

Accept wildcard characters? false

-GPOSession <String>

Specifies the network GPO from which to retrieve the rules to be displayed. This parameter is used in the same way as the PolicyStore parameter. When modifying

GPOs in Windows PowerShellr, each change to a GPO requires the entire GPO to be loaded, modified, and saved back. On a busy Domain Controller (DC), this can be a

slow and resource-heavy operation. A GPO Session loads a domain GPO onto the local computer and makes all changes in a batch, before saving the domain GPO back.

This reduces the load on the DC and speeds up the Windows PowerShell cmdlets. To load a GPO Session, use the

Open-NetGPO cmdlet. To save a GPO Session, use the

Save-NetGPO cmdlet.

Required?   false

Position?   named

Default value   None

Accept pipeline input?   False

Accept wildcard characters? false

 -PolicyStore <String>

   Specifies the policy store from which to retrieve the rules to be displayed. A policy store is a container for firewall and IPsec policy. The acceptable values

   for this parameter are:

   - PersistentStore: Sometimes called static rules, this store contains the persistent policy for the local computer. This policy is not from GPOs, and has been

   created manually or programmatically (during application installation) on the computer. Rules created in this store are attached to the ActiveStore and activated

   on the computer immediately. - ActiveStore: This store contains the currently active policy, which is the sum of all policy stores that apply to the computer.

   This is the resultant set of policy (RSOP) for the local computer (the sum of all GPOs that apply to the computer), and the local stores (the PersistentStore, the

   static Windows service hardening (WSH), and the configurable WSH). ---- GPOs are also policy stores. Computer GPOs can be specified as follows. ------

   `-PolicyStore hostname`.

   ---- Active Directory GPOs can be specified as follows.

   ------ `-PolicyStore domain.fqdn.com\GPO_Friendly_Namedomain.fqdn.comGPO_Friendly_Name`.

   ------ Such as the following.

   -------- `-PolicyStore localhost`

-------- `-PolicyStore corp.contoso.com\FirewallPolicy`

---- Active Directory GPOs can be created using the New-GPO cmdlet or the Group Policy Management Console.

- RSOP: This read-only store contains the sum of all GPOs applied to the local computer.

- SystemDefaults: This read-only store contains the default state of firewall rules that ship with Windows Serverr 2012.

- StaticServiceStore: This read-only store contains all the service restrictions that ship with Windows Server 2012.

Optional and product-dependent features are considered part of Windows Server 2012 for the purposes of WFAS. -ConfigurableServiceStore: This read-write store

contains all the service restrictions that are added for third-party services. In addition, network isolation rules that are created for Windows Store application

containers will appear in this policy store. The default value is PersistentStore. The Set-NetFirewallRule cmdlet cannot be used to add an object to a policy

store. An object can only be added to a policy store at creation time with the New-NetFirewallRule or with this cmdlet.

Required?   false
Position?   named
Default value   None
Accept pipeline input?   False
Accept wildcard characters? false

 -ThrottleLimit <Int32>
Specifies the maximum number of concurrent operations that can be established to run the cmdlet. If this parameter is omitted or a value of `0` is entered, then

Windows PowerShellr calculates an optimum throttle limit for the cmdlet based on the number of CIM cmdlets that are running on the computer. The throttle limit

applies only to the current cmdlet, not to the session or to the computer.

Required?   false
Position?   named

Default value   None

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

None

OUTPUTS

Microsoft.Management.Infrastructure.CimInstance#root\StandardCimv2\MSFT_NetConSecRule[]

The `Microsoft.Management.Infrastructure.CimInstance` object is a wrapper class that displays Windows Management

Instrumentation (WMI) objects. The path after the

pound sign (`#`) provides the namespace and class name for the underlying WMI object.

NOTES

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

PS C:\>Show-NetFirewallRule -PolicyStore ActiveStore

This example displays all of the firewall rules currently in the active policy, which is the collection of all of the policy stores

that apply to the computer.

RELATED LINKS

Copy-NetFirewallRule

Disable-NetFirewallRule

Enable-NetFirewallRule

Get-NetFirewallRule

New-NetFirewallRule

Open-NetGPO

Remove-NetFirewallRule

Rename-NetFirewallRule

Save-NetGPO

Set-NetFirewallRule