Windows PowerShell Get-Help on Cmdlet 'New-AzNetworkWatcherFlowLog'

PS:\>Get-HELP New-AzNetworkWatcherFlowLog -Full

WARNING: The names of some imported commands from the module 'Microsoft.Azure.PowerShell.Cmdlets.Network' include unapproved verbs that might make them less discoverable.

To find the commands with unapproved verbs, run the Import-Module command again with the Verbose parameter. For a list of approved verbs, type Get-Verb.

NAME

New-AzNetworkWatcherFlowLog

SYNOPSIS

Create or update a flow log resource for the specified network security group.

SYNTAX

New-AzNetworkWatcherFlowLog [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -Enabled <System.Boolean>

[-EnableRetention <System.Boolean>] -EnableTrafficAnalytics [-Force] [-FormatType <System.String>] [-FormatVersion <System.Nullable`1[System.Int32]>] -Name

<System.String> -NetworkWatcher <Microsoft.Azure.Commands.Network.Models.PSNetworkWatcher> [-RetentionPolicyDays <System.Nullable`1[System.Int32]>] -StorageId

<System.String> [-Tag <System.Collections.Hashtable>] -TargetResourceId <System.String> [-TrafficAnalyticsInterval

<System.Nullable`1[System.Int32]>]
[-TrafficAnalyticsWorkspaceId <System.String>] [-Confirm] [-WhatIf] [<CommonParameters>]

New-AzNetworkWatcherFlowLog [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -Enabled
<System.Boolean>
[-EnableRetention <System.Boolean>] -EnableTrafficAnalytics [-Force] [-FormatType <System.String>] [-FormatVersion
<System.Nullable`1[System.Int32]>] -Name
<System.String> -NetworkWatcherName <System.String> -ResourceGroupName <System.String> [-RetentionPolicyDays
<System.Nullable`1[System.Int32]>] -StorageId
<System.String> [-Tag <System.Collections.Hashtable>] -TargetResourceId <System.String> [-TrafficAnalyticsInterval
<System.Nullable`1[System.Int32]>]
[-TrafficAnalyticsWorkspaceId <System.String>] [-Confirm] [-WhatIf] [<CommonParameters>]

New-AzNetworkWatcherFlowLog [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -Enabled
<System.Boolean>
[-EnableRetention <System.Boolean>] -EnableTrafficAnalytics [-Force] [-FormatType <System.String>] [-FormatVersion
<System.Nullable`1[System.Int32]>] -Location
<System.String> -Name <System.String> [-RetentionPolicyDays <System.Nullable`1[System.Int32]>] -StorageId
<System.String> [-Tag <System.Collections.Hashtable>]
-TargetResourceId <System.String> [-TrafficAnalyticsInterval <System.Nullable`1[System.Int32]>]
[-TrafficAnalyticsWorkspaceId <System.String>] [-Confirm] [-WhatIf]
[<CommonParameters>]

New-AzNetworkWatcherFlowLog [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -Enabled
<System.Boolean>
[-EnableRetention <System.Boolean>] [-Force] [-FormatType <System.String>] [-FormatVersion
<System.Nullable`1[System.Int32]>] -Location <System.String> -Name
<System.String> [-RetentionPolicyDays <System.Nullable`1[System.Int32]>] -StorageId <System.String> [-Tag
<System.Collections.Hashtable>] -TargetResourceId
<System.String> [-Confirm] [-WhatIf] [<CommonParameters>]

New-AzNetworkWatcherFlowLog [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -Enabled <System.Boolean>
[-EnableRetention <System.Boolean>] [-Force] [-FormatType <System.String>] [-FormatVersion <System.Nullable`1[System.Int32]>] -Name <System.String> -NetworkWatcher
<Microsoft.Azure.Commands.Network.Models.PSNetworkWatcher> [-RetentionPolicyDays <System.Nullable`1[System.Int32]>] -StorageId <System.String> [-Tag
<System.Collections.Hashtable>] -TargetResourceId <System.String> [-Confirm] [-WhatIf] [<CommonParameters>]

New-AzNetworkWatcherFlowLog [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -Enabled <System.Boolean>
[-EnableRetention <System.Boolean>] [-Force] [-FormatType <System.String>] [-FormatVersion <System.Nullable`1[System.Int32]>] -Name <System.String>
-NetworkWatcherName <System.String> -ResourceGroupName <System.String> [-RetentionPolicyDays <System.Nullable`1[System.Int32]>] -StorageId <System.String> [-Tag
<System.Collections.Hashtable>] -TargetResourceId <System.String> [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

New-AzNetworkWatcherFlowLog command creates or updates a flow log resource for the specified network security group.

PARAMETERS

-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>

The credentials, account, tenant, and subscription used for communication with Azure.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Enabled <System.Boolean>

Flag to enable/disable flow logging.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-EnableRetention <System.Boolean>

Flag to enable/disable retention.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-EnableTrafficAnalytics <System.Management.Automation.SwitchParameter>

Flag to enable/disable TrafficAnalytics

Required? true

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-Force <System.Management.Automation.SwitchParameter>

Do not ask for confirmation if you want to overwrite a resource

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-FormatType <System.String>

The file type of flow log. The only supported value now is 'JSON'.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-FormatVersion <System.Nullable`1[System.Int32]>

The version (revision) of the flow log.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Location <System.String>

Location of the network watcher.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Name <System.String>

The flow log name.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-NetworkWatcher <Microsoft.Azure.Commands.Network.Models.PSNetworkWatcher>

The network watcher resource.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-NetworkWatcherName <System.String>

The name of network watcher.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ResourceGroupName <System.String>

The name of the network watcher resource group.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RetentionPolicyDays <System.Nullable`1[System.Int32]>

Number of days to retain flow log records.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-StorageId <System.String>

ID of the storage account which is used to store the flow log.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Tag <System.Collections.Hashtable>

A hashtable which represents resource tags.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-TargetResourceId <System.String>

ID of network security group to which flow log will be applied.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-TrafficAnalyticsInterval <System.Nullable`1[System.Int32]>

The interval in minutes which would decide how frequently TA service should do flow analytics.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-TrafficAnalyticsWorkspaceId <System.String>

Resource Id of the attached workspace.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Confirm <System.Management.Automation.SwitchParameter>

Prompts you for confirmation before running the cmdlet.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-WhatIf <System.Management.Automation.SwitchParameter>

Shows what would happen if the cmdlet runs. The cmdlet is not run.

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

Microsoft.Azure.Commands.Network.Models.PSNetworkWatcher

OUTPUTS

Microsoft.Azure.Commands.Network.Models.PSFlowLogResource

NOTES

---------- Example 1 ----------

New-AzNetworkWatcherFlowLog -Location eastus -Name pstest -TargetResourceId

/subscriptions/bbbbbbbb-bbbb-bbbb-bbbb-bbbbbbbbbbbb/resourceGroups/MyFlowLog/providers/Microsoft.Network/network SecurityGroups/MyNSG -StorageId

/subscriptions/bbbbbbbb-bbbb-bbbb-bbbb-bbbbbbbbbbbb/resourceGroups/FlowLogsV2Demo/providers/Microsoft.Storage/storageAccounts/MyStorage -Enabled $true
-EnableRetention $true -RetentionPolicyDays 5 -FormatVersion 2 -EnableTrafficAnalytics -TrafficAnalyticsWorkspaceId

/subscriptions/bbbbbbbb-bbbb-bbbb-bbbb-bbbbbbbbbbbb/resourcegroups/flowlogsv2demo/providers/Microsoft.OperationalInsights/workspaces/MyWorkspace

```
Name                   : pstest
Id                     : /subscriptions/bbbbbbbb-bbbb-bbbb-bbbb-bbbbbbbbbbbb/resourceGroups/NetworkWatcherRG/providers/Microsoft.Network/networkWatchers/NetworkWatcher_eastus/FlowLogs/pstest
Etag                   : W/"f6047360-d797-4ca6-a9ec-28b5aec5c768"
ProvisioningState      : Succeeded
Location               : eastus
TargetResourceId       : /subscriptions/56abfbd6-ec72-4ce9-831f-bc2b6f2c5505/resourceGroups/MyFlowLog/providers/Microsoft.Network/networkSecurityGroups/MyNSG
StorageId              : /subscriptions/56abfbd6-ec72-4ce9-831f-bc2b6f2c5505/resourceGroups/FlowLogsV2Demo/providers/Microsoft.Storage/storageAccounts/MySTorage
Enabled                : True
RetentionPolicy        : {
                         "Days": 5,
                         "Enabled": true
                         }
Format                 : {
                         "Type": "JSON",
                         "Version": 2
                         }
FlowAnalyticsConfiguration : {
                         "networkWatcherFlowAnalyticsConfiguration": {
                           "enabled": true,
```

"workspaceId": "bbbbbbbb-bbbb-bbbb-bbbb-bbbbbbbbbbbb",
"workspaceRegion": "eastus",
"workspaceResourceId": "/subscriptions/bbbbbbbb-bbbb-bbbb-bbbb-bbbbbbbbbbbb/resourcegroups/flowlogsv2demo/providers/Microsoft.OperationalInsights/workspaces/MyWorkspace",
"trafficAnalyticsInterval": 60
}
}

---------- Example 2 ----------

New-AzNetworkWatcherFlowLog -Location eastus -Name pstest -TargetResourceId

/subscriptions/bbbbbbbb-bbbb-bbbb-bbbb-bbbbbbbbbbbb/resourceGroups/MyFlowLog/providers/Microsoft.Network/networkSecurityGroups/MyNSG -StorageId

/subscriptions/bbbbbbbb-bbbb-bbbb-bbbb-bbbbbbbbbbbb/resourceGroups/FlowLogsV2Demo/providers/Microsoft.Storage/storageAccounts/MyStorage -Enabled $false
-EnableTrafficAnalytics:$false

Name : pstest
Id : /subscriptions/bbbbbbbb-bbbb-bbbb-bbbb-bbbbbbbbbbbb/resourceGroups/NetworkWatcherRG/providers/Microsoft.Network/networkWatchers/NetworkWatcher_eastus/FlowLogs/pstest
Etag : W/"f6047360-d797-4ca6-a9ec-28b5aec5c768"
ProvisioningState : Succeeded
Location : eastus
TargetResourceId : /subscriptions/56abfbd6-ec72-4ce9-831f-bc2b6f2c5505/resourceGroups/MyFlowLog/providers/Microsoft.Network/networkSecurityGroups/MyNSG
StorageId : /subscriptions/56abfbd6-ec72-4ce9-831f-bc2b6f2c5505/resourceGroups/FlowLogsV2Demo/providers/Microsoft.Storage/storageAccounts/MySTorage

```
Enabled                 : False
RetentionPolicy         : {
                          "Days": 0,
                          "Enabled": false
                        }
Format                  : {
                          "Type": "JSON",
                          "Version": 1
                        }
FlowAnalyticsConfiguration : {
                          "networkWatcherFlowAnalyticsConfiguration": {
                            "enabled": false,
                            "trafficAnalyticsInterval": 60
                          }
                        }
```

If you want to disable flowLog resource for which TrafficAnalytics is configured, it is necessary to disable TrafficAnalytics as well. It can be done like in the

example 2.

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/az.network/new-aznetworkwatcherflowlog

New-AzNetworkWatcher

Get-AzNetworkWatcher

Remove-AzNetworkWatcher

Get-AzNetworkWatcherNextHop

Get-AzNetworkWatcherSecurityGroupView

Get-AzNetworkWatcherTopology

Start-AzNetworkWatcherResourceTroubleshooting

New-AzNetworkWatcherPacketCapture

New-AzPacketCaptureFilterConfig

Get-AzNetworkWatcherPacketCapture

Remove-AzNetworkWatcherPacketCapture

Stop-AzNetworkWatcherPacketCapture

New-AzNetworkWatcherProtocolConfiguration

Test-AzNetworkWatcherIPFlow

Test-AzNetworkWatcherConnectivity

Stop-AzNetworkWatcherConnectionMonitor

Start-AzNetworkWatcherConnectionMonitor

Set-AzNetworkWatcherConnectionMonitor

Set-AzNetworkWatcherConfigFlowLog

Remove-AzNetworkWatcherConnectionMonitor

New-AzNetworkWatcherConnectionMonitor

Get-AzNetworkWatcherTroubleshootingResult

Get-AzNetworkWatcherReachabilityReport

Get-AzNetworkWatcherReachabilityProvidersList

Get-AzNetworkWatcherFlowLogStatus

Get-AzNetworkWatcherConnectionMonitorReport

Get-AzNetworkWatcherConnectionMonitor

Get-AzNetworkWatcherFlowLog

Set-AzNetworkWatcherFlowLog

Remove-AzNetworkWatcherFlowLog