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

PS:\>Get-HELP New-AzPacketCaptureFilterConfig -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-AzPacketCaptureFilterConfig

SYNOPSIS

Creates a new packet capture filter object.

SYNTAX

New-AzPacketCaptureFilterConfig [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-LocalIPAddress <System.String>] [-LocalPort <System.String>] [-Protocol <System.String>] [-RemoteIPAddress <System.String>] [-RemotePort <System.String>] [<CommonParameters>]

DESCRIPTION

The New-AzPacketCaptureFilterConfig cmdlet creates a new packet capture filter object. This object is used to restrict

the type of packets that are captured during a

packet capture session using the specified criteria. The New-AzNetworkWatcherPacketCapture cmdlet can accept multiple filter objects to enable composable capture

sessions.

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

-LocalIPAddress <System.String>

Specifies the Local IP Address to filter on. Example inputs: "127.0.0.1" for single address entry. "127.0.0.1-127.0.0.255" for range. "127.0.0.1;127.0.0.5;" for

multiple entries.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-LocalPort <System.String>

Specifies the Local IP Address to filter on. Example inputs: "127.0.0.1" for single address entry. "127.0.0.1-127.0.0.255" for range. "127.0.0.1;127.0.0.5;" for

multiple entries.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-Protocol <System.String>

Specifies the Protocol to filter on. Acceptable values "TCP","UDP","Any"

Required? false

Position? named

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-RemoteIPAddress <System.String>

Specifies the remote IP address to filter on. Example inputs: "127.0.0.1" for single address entry. "127.0.0.1-127.0.0.255" for range. "127.0.0.1;127.0.0.5;" for

multiple entries.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-RemotePort <System.String>

Specifies the Remote Port to filter on. Remote port Example inputs: "80" for single port entry. "80-85" for range. "80;443;" for multiple entries.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

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

System.String

OUTPUTS

Microsoft.Azure.Commands.Network.Models.PSPacketCaptureFilter

NOTES

Keywords: azure, azurerm, arm, resource, management, manager, network, networking, watcher, packet, capture, traffic, filter

--- Example 1: Create a Packet Capture with multiple filters ---

$nw = Get-AzResource | Where-Object {$_.ResourceType -eq "Microsoft.Network/networkWatchers" -and $_.Location -eq "WestCentralUS" }

$networkWatcher = Get-AzNetworkWatcher -Name $nw.Name -ResourceGroupName $nw.ResourceGroupName

$storageAccount = Get-AzStorageAccount -ResourceGroupName contosoResourceGroup -Name contosostorage123

$filter1 = New-AzPacketCaptureFilterConfig -Protocol TCP -RemoteIPAddress "1.1.1.1-255.255.255" -LocalIPAddress

"10.0.0.3" -LocalPort "1-65535" -RemotePort "20;80;443"

$filter2 = New-AzPacketCaptureFilterConfig -Protocol UDP

New-AzNetworkWatcherPacketCapture -NetworkWatcher $networkWatcher -TargetVirtualMachineId $vm.Id -PacketCaptureName "PacketCaptureTest" -StorageAccountId

$storageAccount.id -TimeLimitInSeconds 60 -Filter $filter1, $filter2

In this example we create a packet capture named "PacketCaptureTest" with multiple filters and a time limit. Once the session is complete, it will be saved to the

specified storage account. Note: The Azure Network Watcher extension must be installed on the target virtual machine to create packet captures.

RELATED LINKS

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

New-AzNetworkWatcher

Get-AzNetworkWatcher

Remove-AzNetworkWatcher

Get-AzNetworkWatcherNextHop

Get-AzNetworkWatcherSecurityGroupView

Get-AzNetworkWatcherTopology

Start-AzNetworkWatcherResourceTroubleshooting

New-AzNetworkWatcherPacketCapture

New-AzPacketCaptureScopeConfig

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