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

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

SYNOPSIS

Creates a new network configuration diagnostic profile object. This object is used to restrict the network configuration during a diagnostic session using the

specified criteria.

SYNTAX

New-AzNetworkWatcherNetworkConfigurationDiagnosticProfile [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>]

-Destination <System.String> -DestinationPort <System.String> -Direction <System.String> -Protocol <System.String> -Source <System.String> [<CommonParameters>]

DESCRIPTION

The New-AzNetworkWatcherNetworkConfigurationDiagnosticProfile cmdlet creates a new diagnostic profile object. This object is used to restrict the network

configuration during a network configuration diagnostic session using the specified criteria.

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

-Destination <System.String>

Traffic destination. Accepted values are: '*', IP Address/CIDR, Service Tag.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-DestinationPort <System.String>

Traffic destination port. Accepted values are '*', port (for example, 3389) and port range (for example, 80-100).

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-Direction <System.String>

The direction of the traffic. Accepted values are 'Inbound' and 'Outbound'

Required? true

Position? named

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-Protocol <System.String>

Protocol to be verified on. Accepted values are '*', TCP, UDP.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-Source <System.String>

Traffic source. Accepted values are '*', IP Address/CIDR, Service Tag.

Required? true

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.PSNetworkConfigurationDiagnosticProfile

NOTES

Keywords: azure, azurerm, arm, resource, management, manager, network, networking, watcher, diagnostic, profile

Example 1: Invoke network configuration diagnostic session for VM and specified network profile

$profile = New-AzNetworkWatcherNetworkConfigurationDiagnosticProfile -Direction Inbound -Protocol Tcp -Source 10.1.1.4 -Destination * -DestinationPort 50

Invoke-AzNetworkWatcherNetworkConfigurationDiagnostic -Location eastus -TargetResourceId /subscriptions/61cc8a98-a8be-4bfe-a04e-0b461f93fe35/resourceGroups/NwRgEastUS/providers/Microsoft.Compute/virtualMachines/vm1 -Profile $profile

Results : [

{
"Profile": {
"Direction": "Inbound",
"Protocol": "Tcp",
"Source": "10.1.1.4",
"Destination": "*",
"DestinationPort": "50"

```
    },
    "NetworkSecurityGroupResult": {
      "SecurityRuleAccessResult": "Allow",
      "EvaluatedNetworkSecurityGroups": [
        {
          "NetworkSecurityGroupId": "/subscriptions/61cc8a98-a8be-4bfe-a04e-0b461f93fe35/resourceGroups/clean
upservice/providers/Microsoft.Network/networkSecurityGroups/rg-cleanupservice-nsg1",
          "MatchedRule": {
            "RuleName": "UserRule_Cleanuptool-Allow-4001",
            "Action": "Allow"
          },
          "RulesEvaluationResult": [
            {
              "Name": "UserRule_Cleanuptool-Allow-100",
              "ProtocolMatched": true,
              "SourceMatched": false,
              "SourcePortMatched": true,
              "DestinationMatched": true,
              "DestinationPortMatched": false
            },
```


RELATED LINKS

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

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