
## *Windows PowerShell Get-Help on Cmdlet 'Add-AzServiceFabricManagedClusterNetworkSecurityRule'*

***PS:\>Get-HELP Add-AzServiceFabricManagedClusterNetworkSecurityRule -Full***

NAME

Add-AzServiceFabricManagedClusterNetworkSecurityRule

SYNOPSIS

Add network security rule to cluster resource.

SYNTAX

Add-AzServiceFabricManagedClusterNetworkSecurityRule [-ResourceGroupName] <System.String> [-ClusterName] <System.String> -Access {Allow | Deny} [-AsJob]

[-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Description <System.String>] -DestinationAddressPrefix

<System.String[]> -DestinationPortRange <System.String[]> -Direction {Inbound | Outbound} -Name <System.String> -Priority <System.Int32> -Protocol {https | http | udp

| tcp | esp | icmp | ah | any} -SourceAddressPrefix <System.String[]> -SourcePortRange <System.String[]> [-Confirm] [-WhatIf] [<CommonParameters>]

Add-AzServiceFabricManagedClusterNetworkSecurityRule [-InputObject] <Microsoft.Azure.Commands.ServiceFabric.Models.PSManagedCluster> -Access {Allow | Deny} [-AsJob]

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

[-Description <System.String>] -DestinationAddressPrefix

<System.String[]> -DestinationPortRange <System.String[]> -Direction {Inbound | Outbound} -Name <System.String> -Priority <System.Int32> -Protocol {https | http | udp

| tcp | esp | icmp | ah | any} -SourceAddressPrefix <System.String[]> -SourcePortRange <System.String[]> [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

Add network security rule to cluster resource. This will add network security rule with specified properties

PARAMETERS

-Access <Microsoft.Azure.Commands.ServiceFabric.Models.NetworkSecurityAccess>

Gets or sets the network traffic is allowed or denied. Possible values include: Allow, Deny

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-AsJob <System.Management.Automation.SwitchParameter>

Run cmdlet in the background and return a Job to track progress

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-ClusterName <System.String>

Specify the name of the cluster.

Required? true

Position? 1

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-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

-Description <System.String>

Gets or sets network security rule description

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-DestinationAddressPrefix <System.String[]>

Gets or sets the destination address prefixes. CIDR or destination IP ranges

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-DestinationPortRange <System.String[]>

Gets or sets the destination port ranges

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Direction <Microsoft.Azure.Commands.ServiceFabric.Models.NetworkSecurityDirection>

Gets or sets network security rule direction. Possible values include: Inbound, Outbound

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-InputObject <Microsoft.Azure.Commands.ServiceFabric.Models.PSManagedCluster>

Managed cluster resource

Required? true

Position? 0

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-Name <System.String>

Network Security Rule name

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Priority <System.Int32>

Gets or sets the priority of the rule. The value can be in the range 1000 to 3000. Values outside this range are reserved for Service Fabric ManagerCluster

Resource Provider. The priority number must be unique for each rule in the collection. The lower the priority number, the higher the priority of the rule

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Protocol <Microsoft.Azure.Commands.ServiceFabric.Models.NetworkSecurityProtocol>

Gets or sets network protocol this rule applies to. Possible values include: http, https, tcp, udp, icmp, ah, esp, any

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ResourceGroupName <System.String>

Specify the name of the resource group.

Required? true

Position? 0

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-SourceAddressPrefix <System.String[]>

Gets or sets the CIDR or source IP ranges

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SourcePortRange <System.String[]>

Run cmdlet in the background and return a Job to track progress

Required? true

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

System.String

OUTPUTS

Microsoft.Azure.Commands.ServiceFabric.Models.PSManagedCluster

NOTES

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

```
$resourceGroupName = "sfmcps-test-rg"
$clusterName = "sfmcps-test-cluster"
$NSRName = "testSecRule1"
$sourcePortRanges = "1-1000"
$destinationPortRanges = "1-65535"
$destinationAddressPrefixes = "194.69.104.0/25", "194.69.119.64/26", "167.220.249.128/26", "255.255.255.255/32"
$sourceAddressPrefixes = "167.220.242.0/27", "167.220.0.0/23", "131.107.132.16/28", "167.220.81.128/26"
```

$cluster = Add-AzServiceFabricManagedClusterNetworkSecurityRule -ResourceGroupName $resourceGroupName -ClusterName $clusterName `

-Name $NSRName -Access Allow -Direction Outbound -Protocol tcp -Priority 1200 -SourcePortRange $sourcePortRange -DestinationPortRange $destinationPortRanges

-DestinationAddressPrefix $destinationAddressPrefixes -SourceAddressPrefix $sourceAddressPrefixes -Verbose

This command will add network security rule with properties above.

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

$resourceGroupName = "sfmcps-test-rg"

$clusterName = "sfmcps-test-cluster"

$NSRName = "testSecRule2"

$sourcePortRanges = "1-1000"

$destinationPortRanges = "1-65535"

$destinationAddressPrefixes = "194.69.104.0/25", "194.69.119.64/26", "167.220.249.128/26", "255.255.255.255/32"

$sourceAddressPrefixes = "167.220.242.0/27", "167.220.0.0/23", "131.107.132.16/28", "167.220.81.128/26"

$cluster = Add-AzServiceFabricManagedClusterNetworkSecurityRule -ResourceGroupName $resourceGroupName -ClusterName $clusterName `

-Name $NSRName -Access Deny -Direction Outbound -Protocol udp -Priority 1300 -SourcePortRange $sourcePortRange -DestinationPortRange $destinationPortRanges

-DestinationAddressPrefix $destinationAddressPrefixes -SourceAddressPrefix $sourceAddressPrefixes -Verbose

Similar to Example1 with different properties.

---------- Example 3 ----------

$resourceGroupName = "sfmcps-test-rg"

$clusterName = "sfmcps-test-cluster"

```
$NSRName = "testSecRule3"
$description = "test network security rule"
$sourcePortRanges = "1-1000"
$destinationPortRanges = "1-65535"
$destinationAddressPrefixes = "194.69.104.0/25", "194.69.119.64/26", "167.220.249.128/26", "255.255.255.255/32"
$sourceAddressPrefixes = "167.220.242.0/27", "167.220.0.0/23", "131.107.132.16/28", "167.220.81.128/26"

$cluster = $clusterFromGet | Add-AzServiceFabricManagedClusterNetworkSecurityRule `
        -Name $NSRName -Access Allow -Description $description -Direction Outbound -Protocol tcp -Priority 1400
-SourcePortRange $sourcePortRanges
        -DestinationPortRange $destinationPortRanges -DestinationAddressPrefix $destinationAddressPrefixes
-SourceAddressPrefix $sourceAddressPrefixes -Verbose
```

This command will add a network security rule using cluster object with piping.

RELATED LINKS

Online Version:

https://learn.microsoft.com/powershell/module/az.servicefabric/add-azservicefabricmanagedclusternetworksecurityrule