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

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

SYNOPSIS

Creates a collection of Firewall application rules.

SYNTAX

New-AzFirewallApplicationRuleCollection -ActionType {Allow | Deny} [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -Name <System.String> -Priority <System.UInt32> -Rule <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallApplicationRule[]> [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The New-AzFirewallApplicationRuleCollection cmdlet creates a collection of Firewall Application Rules.

PARAMETERS

-ActionType <System.String>

The action of the rule collection

Required? true

Position? named

Default value None

Accept pipeline input? False

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

-Name <System.String>

Specifies the name of this application rule. The name must be unique inside a rule collection.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Priority <System.UInt32>

Specifies the priority of this rule. Priority is a number between 100 and 65000. The smaller the number, the bigger the

priority.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Rule <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallApplicationRule[]>

Specifies the list of rules to be grouped under this collection.

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

None

OUTPUTS

Microsoft.Azure.Commands.Network.Models.PSAzureFirewallApplicationRuleCollection

NOTES

--------- Example 1: Create a collection with one rule ---------

$rule1 = New-AzFirewallApplicationRule -Name "httpsRule" -Protocol "https:443" -TargetFqdn "*" -SourceAddress "10.0.0.0"

New-AzFirewallApplicationRuleCollection -Name "MyAppRuleCollection" -Priority 1000 -Rule $rule1 -ActionType "Allow"

This example creates a collection with one rule. All traffic that matches the conditions identified in $rule1 will be allowed. The first rule is for all HTTPS traffic

on port 443 from 10.0.0.0. If there is another application rule collection with higher priority (smaller number) which also matches traffic identified in $rule1, the

action of the rule collection with higher priority will take in effect instead.

---------- Example 2: Add a rule to a rule collection ----------

```
$rule1 = New-AzFirewallApplicationRule -Name R1 -Protocol "http:80","https:443" -TargetFqdn "*google.com", "*microsoft.com" -SourceAddress "10.0.0.0"
$ruleCollection = New-AzFirewallApplicationRuleCollection -Name "MyAppRuleCollection" -Priority 100 -Rule $rule1 -ActionType "Allow"

$rule2 = New-AzFirewallApplicationRule -Name R2 -Protocol "http:80","https:443" -TargetFqdn "*google.com", "*microsoft.com"
$ruleCollection.AddRule($rule2)
```

This example creates a new application rule collection with one rule and then adds a second rule to the rule collection using method AddRule on the rule collection

object. Each rule name in a given rule collection must have a unique name and is case insensitive.

--------- Example 3: Get a rule from a rule collection ---------

```
$rule1 = New-AzFirewallApplicationRule -Name R1 -Protocol "http:80","https:443" -TargetFqdn "*google.com", "*microsoft.com" -SourceAddress "10.0.0.0"
$ruleCollection = New-AzFirewallApplicationRuleCollection -Name "MyAppRuleCollection" -Priority 100 -Rule $rule1 -ActionType "Allow"
$getRule=$ruleCollection.GetRuleByName("r1")
```

This example creates a new application rule collection with one rule and then gets the rule by name, calling method GetRuleByName on the rule collection object. The

rule name for method GetRuleByName is case-insensitive.

------- Example 4: Remove a rule from a rule collection -------

```
$rule1 = New-AzFirewallApplicationRule -Name R1 -Protocol "http:80","https:443" -TargetFqdn "*google.com", "*microsoft.com" -SourceAddress "10.0.0.0"
$rule2 = New-AzFirewallApplicationRule -Name R2 -Protocol "http:80","https:443" -TargetFqdn "*google.com", "*microsoft.com"
$ruleCollection = New-AzFirewallApplicationRuleCollection -Name "MyAppRuleCollection" -Priority 100 -Rule $rule1, $rule1 -ActionType "Allow"
$ruleCollection.RemoveRuleByName("r1")
```

This example creates a new application rule collection with two rules and then removes the first rule from the rule collection by calling method RemoveRuleByName on

the rule collection object. The rule name for method RemoveRuleByName is case-insensitive.

RELATED LINKS

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

New-AzFirewallApplicationRule

New-AzFirewall

Get-AzFirewall