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

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

SYNOPSIS

Creates a DDoS protection plan.

SYNTAX

New-AzDdosProtectionPlan [-AsJob] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -Location <System.String> -Name <System.String> -ResourceGroupName <System.String> [-Tag <System.Collections.Hashtable>] [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The New-AzDdosProtectionPlan cmdlet creates a DDoS protection plan.

PARAMETERS

-AsJob <System.Management.Automation.SwitchParameter>

Run cmdlet in the background

Required? false

Position? named

Default value False

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

-Location <System.String>

Specifies the location of the DDoS protection plan to be created.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-Name <System.String>

Specifies the name of the DDoS protection plan to be created.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ResourceGroupName <System.String>

Specifies the resource group of the DDoS protection plan to be created.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-Tag <System.Collections.Hashtable>

A hashtable which represents resource tags.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

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

System.Collections.Hashtable

OUTPUTS

Microsoft.Azure.Commands.Network.Models.PSDdosProtectionPlan

NOTES

Example 1: Create and associate a DDoS protection plan with a new virtual network

```
$ddosProtectionPlan = New-AzDdosProtectionPlan -ResourceGroupName ResourceGroupName -Name DdosProtectionPlanName -Location "West US"
$subnet = New-AzVirtualNetworkSubnetConfig -Name SubnetName -AddressPrefix 10.0.1.0/24
$vnet = New-AzVirtualNetwork -Name VnetName -ResourceGroupName ResourceGroupName -Location "West US" -AddressPrefix 10.0.0.0/16 -DnsServer 8.8.8.8 -Subnet $subnet
-EnableDdoSProtection -DdosProtectionPlanId $ddosProtectionPlan.Id
```

First, we create a new DDoS Protection plan with the New-AzDdosProtectionPlan command. Then, we create a new virtual network with New-AzVirtualNetwork and we specify
the ID of the newly created plan in the parameter DdosProtectionPlanId . In this case, since we are associating the virtual network with a plan, we can also specify
the parameter EnableDdoSProtection .

Example 2: Create and associate a DDoS protection plan with an existing virtual network

```
$ddosProtectionPlan = New-AzDdosProtectionPlan -ResourceGroupName ResourceGroupName -Name DdosProtectionPlanName -Location "West US"
$vnet = Get-AzVirtualNetwork -Name VnetName -ResourceGroupName ResourceGroupName
$vnet.DdosProtectionPlan = New-Object Microsoft.Azure.Commands.Network.Models.PSResourceId
$vnet.DdosProtectionPlan.Id = $ddosProtectionPlan.Id
$vnet.EnableDdosProtection = $true
$vnet | Set-AzVirtualNetwork

Name : VnetName
ResourceGroupName : ResourceGroupName
Location : westus
Id : /subscriptions/d1dbd366-9871-45ac-84b7-fb318152a9e0/resourceGroups/ResourceGroupName/providers/Microsoft.Network/virtualNetworks/VnetName
Etag : W/"fbf41754-3c13-43fd-bb5b-fcc37d5e1cbb"
```

```
ResourceGuid          : fcb7bc1e-ee0d-4005-b3f1-feda76e3756c
ProvisioningState     : Succeeded
Tags                  :
AddressSpace          : {
                        "AddressPrefixes": [
                          "10.0.0.0/16"
                        ]
                        }
DhcpOptions           : {
                        "DnsServers": [
                          "8.8.8.8"
                        ]
                        }
Subnets               : [
                        {
                          "Name": "SubnetName",
                          "Etag": "W/\"fbf41754-3c13-43fd-bb5b-fcc37d5e1cbb\"",
                          "Id":

"/subscriptions/d1dbd366-9871-45ac-84b7-fb318152a9e0/resourceGroups/ResourceGroupName/providers/Microsoft.Netwo
rk/virtualNetworks/VnetName/subnets/SubnetName",
                          "AddressPrefix": "10.0.1.0/24",
                          "IpConfigurations": [],
                          "ResourceNavigationLinks": [],
                          "ServiceEndpoints": [],
                          "ProvisioningState": "Succeeded"
                        }
                        ]
VirtualNetworkPeerings : []
EnableDdosProtection   : true
DdosProtectionPlan     : {
                        "Id":
```

"/subscriptions/d1dbd366-9871-45ac-84b7-fb318152a9e0/resourceGroups/ResourceGroupName/providers/Microsoft.Network/ddosProtectionPlans/DdosProtectionPlanName"

}

EnableVmProtection : false

First, we create a new DDoS Protection plan with the New-AzDdosProtectionPlan command. Second, we get the most updated version of the virtual network we want to

associate with the plan. We update the property DdosProtectionPlan with a PSResourceId object containing a reference to the ID of the newly created plan. In this

case, if we associate the virtual network with a DDoS protection plan, we can also set the flag EnableDdosProtection to true. Finally, we persist the new state by

piping the local variable into Set-AzVirtualNetwork .

RELATED LINKS

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

Get-AzDdosProtectionPlan

Remove-AzDdosProtectionPlan

New-AzVirtualNetwork

Set-AzVirtualNetwork

Get-AzVirtualNetwork