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

PS:\>Get-HELP Remove-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

Remove-AzDdosProtectionPlan

SYNOPSIS

Removes a DDoS protection plan.

SYNTAX

Remove-AzDdosProtectionPlan [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -Name <System.String>

[-PassThru] -ResourceGroupName <System.String> [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The Remove-AzDdosProtectionPlan cmdlet removes a DDoS protection plan.

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

-Name <System.String>

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

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-PassThru <System.Management.Automation.SwitchParameter>

Returns an object representing the item with which you are working. By default, this cmdlet does not generate any output.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-ResourceGroupName <System.String>

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

Required? true

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

OUTPUTS

System.Boolean

NOTES

------- Example 1: Remove an empty DDoS protection plan -------

Remove-AzDdosProtectionPlan -ResourceGroupName ResourceGroupName -Name DdosProtectionPlan

In this case, we remove a DDoS protection plan as specified.

Example 2: Remove a DDoS protection plan associated with a virtual network

$vnet = Get-AzVirtualNetwork -Name VnetName -ResourceGroupName ResourceGroupName

$vnet.DdosProtectionPlan = $null

$vnet.EnableDdosProtection = $false

$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/"65947351-747e-4686-aa8b-c40da58f6c8b"
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/\"65947351-747e-4686-aa8b-c40da58f6c8b\"",
                        "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   : false
DdosProtectionPlan     : null
EnableVmProtection     : false
```

Remove-AzDdosProtectionPlan -ResourceGroupName ResourceGroupName -Name DdosProtectionPlan

DDoS protection plans cannot be deleted if they are associated with a virtual network. So the first step is to disassociate both objects. Here, we get the most

updated version of the virtual network associated with the plan, and we set the property DdosProtectionPlan to an empty value and the flag EnableDdosProtection (this

flag cannot be true without a plan). Then, we persist the new state by piping the local variable into Set-AzVirtualNetwork . At this point, the plan is no longer

associated with the virtual network. If this is the last one associated with the plan, we can remove the DDoS protection plan by using the command

Remove-AzDdosProtectionPlan.

RELATED LINKS

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

New-AzDdosProtectionPlan

Get-AzDdosProtectionPlan

New-AzVirtualNetwork

Set-AzVirtualNetwork

Get-AzVirtualNetwork