Windows PowerShell Get-Help on Cmdlet 'Set-AzVMSecurityProfile'

PS:\>Get-HELP Set-AzVMSecurityProfile -Full

NAME

Set-AzVMSecurityProfile

SYNOPSIS

Sets the SecurityType enum for Virtual Machines.

SYNTAX

Set-AzVMSecurityProfile [-VM] <Microsoft.Azure.Commands.Compute.Models.PSVirtualMachine> [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-SecurityType <System.String>] [<CommonParameters>]

DESCRIPTION

The Set-AzVMSecurityProfile cmdlet sets the Security Type of the VM

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

-SecurityType <System.String>

Specifies the SecurityType of the virtual machine. It has to be set to any specified value to enable UefiSettings. By default, UefiSettings will not be enabled

unless this property is set.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-VM <Microsoft.Azure.Commands.Compute.Models.PSVirtualMachine>

The virtual machine profile.

Required? true

Position? 0

Default value None

Accept pipeline input? True (ByPropertyName, ByValue)

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

Microsoft.Azure.Commands.Compute.Models.PSVirtualMachine

Microsoft.Azure.Management.Compute.Models.SecurityTypes

OUTPUTS

Microsoft.Azure.Commands.Compute.Models.PSVirtualMachine

NOTES

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

```
$VM = Get-AzVM -ResourceGroupName "ResourceGroup11" -VMName "ContosoVM07"
$VM = Set-AzVMSecurityProfile -VM $VM -SecurityType "TrustedLaunch"
```

The first command gets the virtual machine named ContosoVM07 by using Get-AzVm . The command stores it in the $VM variable. The second command sets the SecurityType

enum to "TrustedLaunch". Trusted launch requires the creation of new virtual machines. You can't enable trusted launch on existing virtual machines that were

initially created without it.

Example 2: Create a ConfidentialVM Virtual Machine and the Disk encrypted with the VMGuestStateOnly type.

```
$vmSize = "Standard_DC2as_v5";
```

```
$DNSNameLabel = "cvm1" +$ResourceGroupName;
$SubnetAddressPrefix = "10.0.0.0/24";
$VnetAddressPrefix = "10.0.0.0/16";

# Credential setup.
$password = "Password" |ConvertTo-SecureString -AsPlainText -Force;
$securePassword = ConvertTo-SecureString $password -AsPlainText -Force;
$credential = New-Object System.Management.Automation.PSCredential ($user, $securePassword);

$SecurityType = "ConfidentialVM";
$vmDiskSecurityEncryptionType = "VMGuestStateOnly";
$VirtualMachine = New-AzVMConfig -VMName $VMName -VMSize $VMSize;

# Create the Network resources and VM OS setup.
$SingleSubnet = New-AzVirtualNetworkSubnetConfig -Name $SubnetName -AddressPrefix $SubnetAddressPrefix;
   $Vnet = New-AzVirtualNetwork -Name $NetworkName -ResourceGroupName $rgname -Location $LocationName -AddressPrefix $VnetAddressPrefix -Subnet $SingleSubnet;
        $PIP = New-AzPublicIpAddress -Name $PublicIPAddressName -DomainNameLabel $DNSNameLabel -ResourceGroupName $rgname -Location $LocationName -AllocationMethod Dynamic;
$NIC = New-AzNetworkInterface -Name $NICName -ResourceGroupName $rgname -Location $LocationName -SubnetId $Vnet.Subnets[0].Id -PublicIpAddressId $PIP.Id;
   $VirtualMachine = Set-AzVMOperatingSystem -VM $VirtualMachine -Windows -ComputerName $ComputerName -Credential $Credential -ProvisionVMAgent -EnableAutoUpdate;
$VirtualMachine = Add-AzVMNetworkInterface -VM $VirtualMachine -Id $NIC.Id;
   $VirtualMachine = Set-AzVMSourceImage -VM $VirtualMachine -PublisherName 'MicrosoftWindowsServer' -Offer 'windowsserver' -Skus '2022-datacenter-smalldisk-g2' -Version
'latest';
  $VirtualMachine = Set-AzVMOSDisk -VM $VirtualMachine -StorageAccountType "StandardSSD_LRS" -CreateOption "FromImage";

# Set the SecurityType and necessary values on the Uefi settings.
$VirtualMachine = Set-AzVmSecurityProfile -VM $VirtualMachine -SecurityType $SecurityType;
$VirtualMachine = Set-AzVmUefi -VM $VirtualMachine -EnableVtpm $true -EnableSecureBoot $true;
```

```
    # Set the Disk Encryption Type.
      $VirtualMachine = Set-AzVMOSDisk -VM $VirtualMachine -StorageAccountType "StandardSSD_LRS" -CreateOption
"FromImage" -SecurityEncryptionType
    $vmDiskSEcurityEncryptionType;

    $vm = New-AzVM -ResourceGroupName $rgname -Location $LocationName -VM $VirtualMachine;
    $vm = Get-AzVm -ResourceGroupName $rgname -Name $vmname;
    # Verify SecurityType value.
    # $vm.SecurityProfile.SecurityType == "ConfidentialVM";
```

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/az.compute/set-azvmsecurityprofile