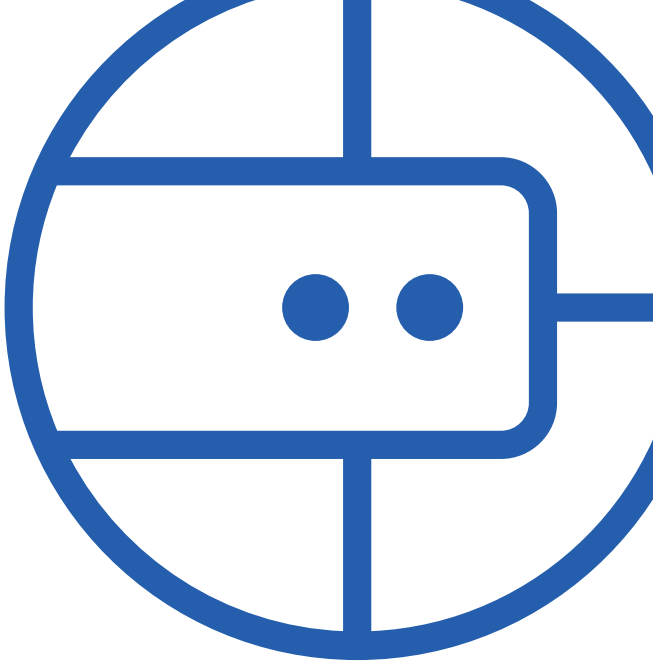
SOPHOS

Security made simple.



Sophos Central

Server Protection in Microsoft Azure

Document date: April 2017

Contents

Overview 3

1 Windows servers: Example workflows for creating and configuring images 4

1.1 Deploy a VM with the Sophos Server Protection Agent when launched 4

1.2 Creating an image from a VM with the Sophos Server Protection Agent 4

1.3 Deploying a new VM from an image 5

2 Linux servers: Example workflows for creating and configuring images 6

2.1 Deploying a VM with the Sophos Server Protection Agent when launched 6

2.2 Creating an image and template from a VM with the Sophos Server Protection Agent 7

2.3 Deploying a new VM from an image and template 7

3 Sophos XG Firewall on Microsoft Azure 8

4 Appendix: Scripts 8

Technical support 11

Legal notices 12

Overview

Sophos provides the ability to manage the security of server images in Microsoft Azure with your Sophos Central account.

You need a Sophos Central Server Protection license.
This guide tells you how to do the following on Windows or Linux servers:

- Deploy VMs with Sophos Server Protection Agent when launched.
- Create an image with Sophos Server Protection Agent.
- Deploy a new VM with a Sophos agent from an image.

Notes:

- Microsoft Azure AD is not supported.
- The Sophos Server Protection Agent can be installed on existing Azure VMs by following the guidance in the following article: Knowledge Base Article 119265: How to deploy the Sophos Central software
- Details of the domains and ports required for communication between the Sophos Server Protection Agent and the Sophos Central Admin console can be found in the following article: Knowledge Base Article 121936: How to configure firewalls for the Sophos agent

1. Windows servers: Example workflows for creating and configuring images

This section provides examples of how to create and configure your Azure images with the Sophos Server Protection Agent.

Prerequisites:

- Knowledge of Microsoft Azure (how to deploy VMs, create VM prerequisites such as virtual networks and subnets, run Azure command lines, etc.).
- Download the Windows Server installer from Sophos Central under the **Protect Devices** section.

Note: Sophos Update Cache and **Server Lockdown** can only be installed after initial deployment. They cannot be installed as part of an image.

1.1 Deploy a VM with the Sophos Server Protection Agent from launch

How to deploy a Windows VM with Sophos Server Protection Agent using an Extension in the Azure portal:

Prerequisites:

1. Create the VM in the Azure portal as normal, adding the Custom Script Extension.
2. Add the script shown in Deploying a VM with the Sophos Server Protection Agent from launch.

Note: The script will need renaming from _ps1.txt to .ps1

3. In the arguments box, put in the link to the Sophos Windows installer.
4. Start the VM.

1.2 Creating an image from a VM with the Sophos Server Protection Agent

How to create an image for a Windows VM using Azure PowerShell:

Step 1: Generalize the VM

1. To avoid duplicating servers in Sophos Central, complete the steps in the following article: Knowledge Base Article 120560: How to install Sophos Central Endpoint on a gold image avoiding duplicate identities
2. Run sysprep on the VM using the command-line or GUI options to generalize and shutdown.
3. Run the following commands:
   - Stop-AzureRmVm -ResourceGroupName resource-group-name -Name vm-name –Force
   - Set-AzureRmVm -ResourceGroupName resource-group-name -Name vm-name –Generalized

Step 2: Create an image from the generalized VM

1. Run the following command:
   - Save-AzureRmVMImage -ResourceGroupName *resource-group-name* -VMName *vm-name* - DestinationContainerName *image-container-name* -VHDNamePrefix *vhd-prefix-name*

Note: This will create a VHD image that is stored as a blob in the blob container associated with the storage account for the VM.

1.3 Deploying a new VM from an image

How to deploy a VM from an image using an Azure PowerShell script:

Modify the script shown in Deploying a new VM from an image script to change the customization variables, then run it.

Note: The script will need renaming from _ps1.txt to .ps1

2. Linux servers: Example workflows for creating and configuring images

This section provides examples of how to create and configure your Azure images with the Sophos Server Protection Agent.

Prerequisites:

- Knowledge of Microsoft Azure (how to deploy VMs, create VM prerequisites such as virtual networks and subnets, run Azure command lines, etc.)
- Copy the download link to the Linux Server installer within Sophos Central, under the **Protect Devices** section, by right click on the Linux Server installer link, select Properties, then copy the URL.

2.1 Deploying a VM with the Sophos Server Protection Agent when launched

How to deploy a Linux VM with the Sophos Server Protection Agent using Azure CLI:

In the following scripts replace the <LinkToInstaller> with the link to the correct Server Installer taken from Sophos Central as part of the prerequisites:

Step 1: Run SophosInstall.sh

On kernels that are supported for multiple options for on-access scanning, such as Ubuntu:

```
#! /bin/bash
wget <LinkToInstaller> -P /tmp/
chmod +x /tmp/SophosInstall.sh
/tmp/SophosInstall.sh
```

On kernels that have limitations for on-access scanning, using yum package manager:

```
#! /bin/bash yum update -y
yum install gcc kernel-headers kernel-devel -y wget <LinkToInstaller> -P /tmp/
chmod +x /tmp/SophosInstall.sh
/tmp/SophosInstall.sh
```

Step 2: Run the azure vm create command

azure vm create --resource-group *resource-group-name* --name *vm-name* --location *region* --os-type Linux --ssh- publickey-file *public-keypair-filename* --image-urn *image-urn* --admin-username *administrator* --nic-name *nic-name*--custom-data *custom-data-filename*

Note:

- The *custom-data-filename* should reference the file created in Step 1.
- This example create command requires a nic-name. If you do not want to use this, an alternative example is to use azure vm quick-create.

2.2 Creating an image and template from a VM with the Sophos Server Protection Agent

This section tells you how to create an image and template for a Linux VM using Azure CLI.

Step 1: Generalize the VM

1. ssh into the VM.
2. Run the command: sudo waagent -deprovision+user
3. Shutdown the VM and release resources: azure vm deallocate --resource-group *resource-group-name* --name *vm-name*
4. Run the command: azure vm generalize --resource-group *resource-group-name* --name *vm-name*

Step 2: Create an image and template from the generalized VM

Run the command:

azure vm capture --resource-group *resource-group-name* --name *vm-name* --vhd-name-prefix *vhd-name-prefix* --template-file-name *template-file-name*

- This example create command requires a nic-name. If you do not want to use this, an alternative example is to use azure vm quick-create.

Note: This will create a VHD image and a JSON template that are stored as blobs in the blob container associated with the storage account for the VM and will store a template file locally.

2.3 Deploying a new VM from an image and template

How to deploy a VM from an image and template using Azure CLI:

Deploy from a local template file:

azure group deployment create --template-file *template-name.json resource-group-name deployment-name*

3. Sophos XG Firewall on Microsoft Azure

In addition to Sophos Server Protection, Sophos also offers a next generation firewall for Azure. Sophos XG Firewall can be selected and launched from within the Microsoft Azure Marketplace. XG Firewall deploys as an all-in-one solution that combines advanced networking, protections such as Intrusion Prevention (IPS) and Web Application Firewalling (WAF), and user and application controls as well. XG Firewall is designed to help you protect your Azure-based workloads against advanced threats.

Synchronized Security is a best of breed security system that enables your defenses to be as coordinated as the attacks they protect against. On Azure, Sophos Server Protection Agent and Sophos XG Firewall work together to bring Synchronized Security to the Azure Cloud.

https://www.sophos.com/en-us/lp/synchronized-security.aspx

https://www.sophos.com/solutions/public-cloud/azure.aspx

4. Appendix: Scripts

Deploying a VM with the Sophos Server Protection Agent from launch

```
$url=$args[0]

$installer = "C:\SophosInstall.exe"

$wc = New-Object System.Net.WebClient

$wc.DownloadFile($url, $installer)

& $installer -q
```

Deploying a new VM from an image

```
# Change the values of these customization variables for a specific deployment:

$prefix = 'MyVM'

# Maximum five char prefix for all resources created (VM, NIC, IP)

$vmSize = 'Standard_DS2_V2'

# Size of VM

$subscriptionId =      '12345678-90ab-cdef-1234-567890abcdef'

# Subscription id

$storageAccountName = 'examplestorage'

# Storage account name for image and new VM's VHD

$sourceImageUri = 'https://examplestorage.blob.core.windows.net/vhds/examplevmimage201702 23155132.vhd' # VM image blob URI

$adminUsername = 'username'

$adminPassword = 'password'

# End of custom variables

# Authenticate against Azure and cache subscription data
Login-AzureRmAccount
```

```
# Switch subscription
Select-AzureRmSubscription -SubscriptionId $subscriptionId

# Get the storage account
$storageAccount = Get-AzureRmStorageAccount | ? StorageAccountName -EQ
$storageAccountName
if(-not $storageAccount) {
    throw “Unable to find storage account ‘$storageAccountName’. Cannot continue.”
}

# Enable verbose output and stop on error
$VerbosePreference = ‘Continue’
$ErrorActionPreference = ‘Stop’

# Some reserved script variables
$resourceGroupName = $storageAccount.ResourceGroupName
$location = $storageAccount.Location
$vmSuffix = Get-Random
$vmName = ‘{0}{1}’ -f $prefix,$vmSuffix
$nicName = ‘{0}{1}-NIC’ -f $prefix, $vmSuffix
$ipName = ‘{0}{1}-IP’ -f $prefix, $vmSuffix
$domName = ‘{0}-{1}’ -f $prefix.ToLower(), $vmSuffix
$vnetName = $vmName

# Create VNET
Write-Verbose ‘Creating Virtual Network...’
$vnetDef = New-AzureRmVirtualNetwork -ResourceGroupName
$resourceGroupName -Location $location -Name $vnetName -AddressPrefix ‘10.0.0.0/16’ Write-Verbose ‘Adding
subnet to Virtual Network’
$vnet = $vnetDef | Add-AzureRmVirtualNetworkSubnetConfig -Name ‘Subnet- 1’ -AddressPrefix ‘10.0.0.0/24’ | Set-
AzureRmVirtualNetwork
```

```
# Create NIC Write-Verbose ‘Creating Public IP...’

$pip = New-AzureRmPublicIpAddress -ResourceGroupName $resourceGroupName -Location $location -Name $ipName
-DomainNameLabel $domName - AllocationMethod Dynamic Write-Verbose ‘Creating NIC’

$nic = New-AzureRmNetworkInterface -ResourceGroupName

$resourceGroupName -Location $location -Name $nicName - PublicIpAddressId $pip.Id -SubnetId $vnet.Subnets[0].Id


# Specify the VM name and size

Write-Verbose ‘Creating VM Config...’

$vm = New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize


# Specify local administrator account and then add the NIC

$cred = New-Object PSCredential $adminUsername, ($adminPassword | ConvertTo-SecureString -AsPlainText -Force) # could
use Get-Credential to get prompted instead

$vm = Set-AzureRmVMOperatingSystem -VM $vm -Windows -ComputerName

$vmName -Credential $cred -ProvisionVMAgent -EnableAutoUpdate # change -Windows to -Linux if deploying a Linux VM

$vm = Add-AzureRmVMNetworkInterface -VM $vm -Id $nic.Id


# Specify the OS disk

$diskName = ‘osdisk’

$osDiskUri = ‘{0}vhds/{1}{2}.vhd’ -f

$storageAccount.PrimaryEndpoints.Blob.ToString(), $vmName.ToLower(),

$diskName

$vm = Set-AzureRmVMOSDisk -VM $vm -Name $diskName -VhdUri $osDiskUri - CreateOption fromImage -SourceImageUri
$sourceImageUri -Windows # change -Windows to -Linux if deploying a Linux VM


Write-Verbose (‘Creating VM {0}...’ -f $vmName)

New-AzureRmVM -ResourceGroupName $resourceGroupName -Location $location

-VM $vm
```

Technical support

You can find technical support for Sophos products in any of these ways:

- Visit the SophosTalk community at http://community.sophos.com/ and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at http://www.sophos.com/support/.
- Download the product documentation at http://www.sophos.com/support/docs/.
- Send an email to support@sophos.com, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

Legal notices

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

SOPHOS