



# The SysAdmin's Guide to **Azure Infrastructure as a Service**

By Paul Schnackenburg

**ALTARO**

# TABLE OF CONTENTS

<b>INTRODUCTION .....</b>	<b>3</b>
<b>CHAPTER 1 – CREATING VMs .....</b>	<b>5</b>
Creating a VM in the portal .....	5
Create a VM using PowerShell .....	8
Create a VM using CLI.....	9
Create a VM from a template .....	10
<b>CHAPTER 2 – SIZING VMs .....</b>	<b>13</b>
VM Series .....	13
VM Performance .....	15
<b>CHAPTER 3 – STORAGE .....</b>	<b>16</b>
SSD or HDD, Standard, Premium or Ultra .....	16
Disk Considerations .....	17
Uploading Virtual Disks.....	18
A Gibibyte vs. a Gigabyte.....	18
<b>CHAPTER 4 – NETWORKING .....</b>	<b>19</b>
Keep your vNets close .....	19
Network services.....	21
Hybrid Networking.....	22

<b>CHAPTER 5 – MONITORING &amp; PERFORMANCE .....</b>	<b>23</b>
VM Performance .....	23
Network Monitoring.....	25
Azure in your pocket.....	25
The Portal.....	25
Windows Admin Center.....	27
 <b>CHAPTER 6 – BEHIND THE SCENES – ARM .....</b>	 <b>28</b>
Infrastructure as Code.....	28
Blueprints.....	29
Azure Policy.....	29
Tag – you’re it! .....	29
Management Groups .....	30
Resource Graph .....	30
 <b>CHAPTER 7 – MANY VMs .....</b>	 <b>32</b>
Availability .....	32
Many VMs.....	32
Sharing Images.....	34
Cost management.....	34
 <b>CHAPTER 8 – BACKUP &amp; REPLICATION .....</b>	 <b>36</b>
Backup.....	36
Replication .....	37
Altaro VM Backup .....	37
Migrate.....	37

<b>CHAPTER 9 – AZURE AD .....</b>	<b>39</b>
Identity is the new firewall .....	39
Managed Identities .....	40
Azure AD Domain Services .....	40
Logging in with AAD accounts .....	40
<b>CHAPTER 10 – SECURITY .....</b>	<b>41</b>
Azure Security Center .....	41
Patching.....	41
Bastion.....	41
Azure Key Vault.....	43
Disk Encryption .....	43
Role-Based Access Control .....	43
Azure Firewall .....	44
<b>CHAPTER 11 – AUTOMATION.....</b>	<b>45</b>
Azure Automation .....	45
Azure Advisor .....	46
<b>CHAPTER 12 – BEYOND IAAS.....</b>	<b>48</b>
Azure SQL .....	48
Cosmos DB .....	48
Web applications.....	48
Azure Kubernetes Service .....	49
Serverless.....	49
<b>GOING FORWARD .....</b>	<b>50</b>
<b>ABOUT PAUL SCHNAKENBURG .....</b>	<b>50</b>
<b>ABOUT ALTARO.....</b>	<b>50</b>

# INTRODUCTION

The cloud computing era is well and truly upon us, and knowing how to take advantage of the benefits of this computing paradigm while maintaining security, manageability, and cost control are vital skills for any IT professional in 2020 and beyond. And its importance is only getting greater.

In this eBook, we're going to focus on Infrastructure as a Service (IaaS) on Microsoft's Azure platform - learning how to create VMs, size them correctly, manage storage, networking, and security, along with backup best practices. You'll also learn how to operate groups of VMs, deploy resources based on templates, managing security and automate your infrastructure. If you currently have VMs in your own datacenter and are looking to migrate to Azure, we'll also teach you that.

If you're new to the cloud (or have experience with AWS/GCP but not Azure), this book will cover the basics as well as more advanced skills. Given how fast things change in the cloud, we'll cover the why (as well as the how) so that as features and interfaces are updated, you'll have the theoretical knowledge to effectively adapt and know how to proceed.

You'll benefit most from this book if you actively follow along with the tutorials. We will be going through terms and definitions as we go – learning by doing has always been my preferred way of education. If you don't have access to an Azure subscription, you can [sign up for a free trial with Microsoft](#). This will give you 30 days

to use \$200 USD worth of Azure resources, along with 12 months of [free resources](#).

Note that most of these “12 months” services aren’t related to IaaS VMs (apart from a few SSD based virtual disks and a small VM that you can run for 750 hours a month) so be sure to get everything covered on the IaaS side before your trial expires.

There are also another 25 services that have free tiers “forever”.

Now you know what’s in store, let’s get started!

# CHAPTER 1 – CREATING VMS

In this chapter, we're going to look at different ways of creating VMs, using the web-based portal ([portal.azure.com](https://portal.azure.com)), PowerShell, and the cross-platform CLI. We're not going to focus on the different VM sizes available (that's [Chapter 2](#)), Storage ([Chapter 3](#)), and Networking ([Chapter 4](#)).

If you're following along as we go (recommended), start by logging in at [portal.azure.com](https://portal.azure.com).

## CREATING A VM IN THE PORTAL

Click the plus sign – create a resource and click on Compute. Select Virtual Machine; let's go through the wizard that comes up.

First, you must create a Resource Group (RG), call it **AzureIaaS**.

A RG is a logical grouping of resources that you want to manage as a unit.

For instance, a production application RG could contain two VMs running a web front end, a load balancer, and a backend SQL database (both PaaS services). Additionally, you can assign permissions ([Chapter 10](#)) for the management of that RG using Role-Based Access Control (RBAC).

## Create a virtual machine

**Basics** Disks Networking Management Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image.

Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.

Looking for classic VMs? [Create VM from Azure Marketplace](#)

### Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ	<input type="text" value="MSDN Platforms"/>
Resource group * ⓘ	<input type="text" value="Azurelaas"/>

[Create new](#)

### Instance details

Virtual machine name * ⓘ	<input type="text" value="AzurelaaS1"/>
Region * ⓘ	<input type="text" value="(US) East US"/>
Availability options ⓘ	<input type="text" value="No infrastructure redundancy required"/>
Image * ⓘ	<input type="text" value="Windows Server 2019 Datacenter"/>
Size * ⓘ	<div><b>Standard DS1 v2</b> 1 vcpu, 3.5 GiB memory <a href="#">Change size</a></div>
Administrator account	
Username * ⓘ	<input type="text" value="Paul"/>

First step to create a VM

Give your VM a name, **AzurelaaSVM1**, pick the East US region, and select the Windows Server 2019 Datacenter image.

Note: The suggested size will most likely be a Standard D series, which will be fine for this first walkthrough.

Define an administrator account username (you can't use Admin and similar account names) and a password at least 12 characters (123 max) with three out of four – lowercase, uppercase, number, and special characters.

For this first VM, we're going to allow RDP (3389) access from the internet.

Ways to avoid this security headache are covered in [Chapter 10](#).

For OS disk type, pick Premium SSD and don't add any data disks.

Because we haven't set up any networking prior to creating this VM, Azure will suggest creating a new Virtual Network (Vnet), a new subnet, and a new Public IP, along with a Network Security Group (NSG) with the RDP port open.

### Create a virtual machine

---

Monitoring

Boot diagnostics ⓘ  
☒ On ☐ Off

OS guest diagnostics ⓘ  
☐ On ☒ Off

Diagnostics storage account \* ⓘ  

(new) azureiaasdiag

Create new

Identity

System assigned managed identity ⓘ  
☐ On ☒ Off

Azure Active Directory

Login with AAD credentials (Preview) ⓘ  
☐ On ☒ Off

Auto-shutdown

Enable auto-shutdown ⓘ  
☒ On ☐ Off

Shutdown time ⓘ  

7:00:00 PM

Time zone ⓘ  

(UTC) Coordinated Universal Time

Notification before shutdown ⓘ  
☒ On ☐ Off

Email \* ⓘ  

paulschnack@hotmail.com

Review + create

< Previous

Next : Advanced >

Creating a VM - Management

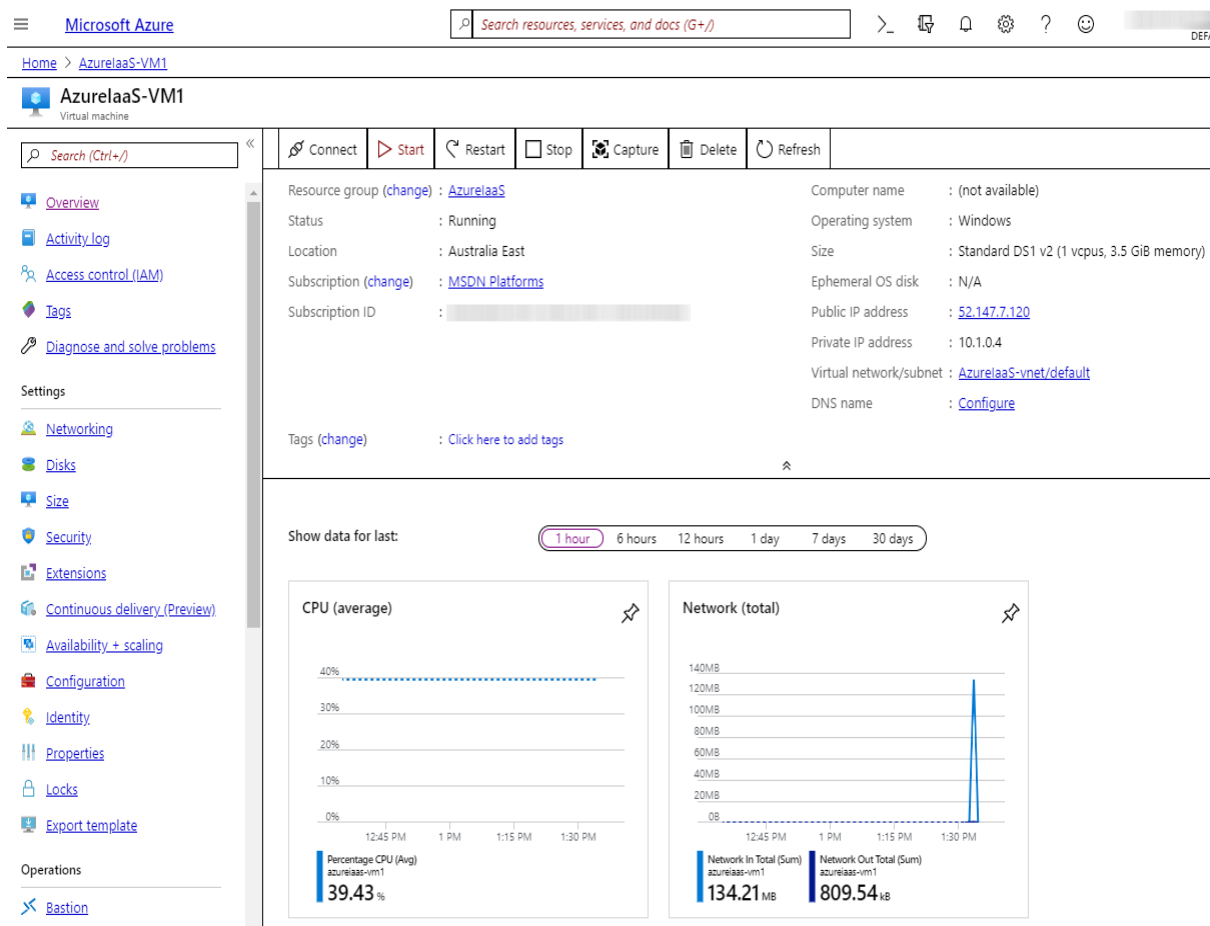
On the Management step of the wizard, leave all options as default and the same on the Advanced step (including leaving VM generation as Gen 1) as well as for Tags.

On the review screen, click the Create button.

A notification will appear under the bell ( 🔔 ) in the top right, and if you click on it, it'll show you the deployment progress, and once it's deployed, the notification will change and let you click "Go to Resource".

The Overview page for your VM will show its status and configured settings, along with performance statistics for CPU, Network, and Disk. When you click the Connect button, it'll download an RDP file that lets you connect to your VM and log in.

**Pro tip** – if you're new to Azure, you might think that shutting down the VM from within the OS will stop the cost accruing in Azure – not so, as this shutdown isn't something Azure is aware of. To stop paying for the running of the VM, click the Stop button in the portal, which will change the state (once it's shut down) to Stopped (Deallocated).



VM Overview screen

How about from the CLI? Azure has two command-line interfaces – PowerShell and the cross-platform CLI. Which one to use is mostly up to you. If you're a Windows person and comfortable with PowerShell, using that makes sense. Whereas the Azure CLI is BASH based and makes sense for a Linux user.

## CREATE A VM USING POWERSHELL

Time to create a second VM, this time [using PowerShell](#). There are two ways of running PowerShell against Azure; you can download the appropriate modules and [install them on your local PC](#). Alternatively, you can use CloudShell which is PowerShell or the CLI (see below), running in a browser, that already has the required

modules installed. You can get to the cloud shell using [shell.azure.com](https://shell.azure.com), or you can click the button ( > ) in the top right of the portal.

To create a new VM in the same RG (resource group) that we created the first VM in type in the following, all on one line:

```
New-AzVm -ResourceGroupName "AzureIaaS" -Name "AzureIaaSVM2" -
Location "East US" -virtualNetworkName "AzureIaaSvmnet2" -
SubnetName "default" -SecurityGroupName "AzureIaaS-VM1-nsg" -
PublicIpAddressName "AzureIaaSVM2ip" -OpenPorts 3389
```

```
PS Azure:\> New-AzVm -ResourceGroupName "AzureIaaS" -Name "AzureIaaSVM2" -Location "East US" -virtualNetworkName "AzureIaaSvmnet2" -
SubnetName "default" -SecurityGroupName "AzureIaaS-VM1-nsg" -PublicIpAddressName "AzureIaaSVM2ip" -OpenPorts 3389

cmdlet New-AzVM at command pipeline position 1
Supply values for the following parameters:
Credential
User: Paul
Password for user Paul: *****

ResourceGroupName      : AzureIaaS
Id                     : /subscriptions/ /resourceGroups/AzureIaaS/providers/Microsoft.Compute
e/virtualMachines/AzureIaaSVM2
VmId                   : f9f0e2bc-c18d-4f21-b91f-41d196d941e2
Name                   : AzureIaaSVM2
Type                   : Microsoft.Compute/virtualMachines
Location               : eastus
Tags                   : {}
HardwareProfile         : {VmSize}
NetworkProfile          : {NetworkInterfaces}
OSProfile               : {ComputerName, AdminUsername, WindowsConfiguration, Secrets, AllowExtensionOperations,
RequireGuestProvisionSignal}
ProvisioningState       : Succeeded
StorageProfile          : {ImageReference, OsDisk, DataDisks}
FullyQualifiedDomainName : azureiaasvm2-3c3710.East US.cloudapp.azure.com
```

### Creating a VM with PowerShell

It'll ask you for credentials for the new VM and then proceed to deploy it for you.

We've put this VM in the same RG as the first one we created but in a separate VNet (Virtual Network).

Once the deployment has completed, go back to the Azure portal to make sure that the VM shows up in your RG.

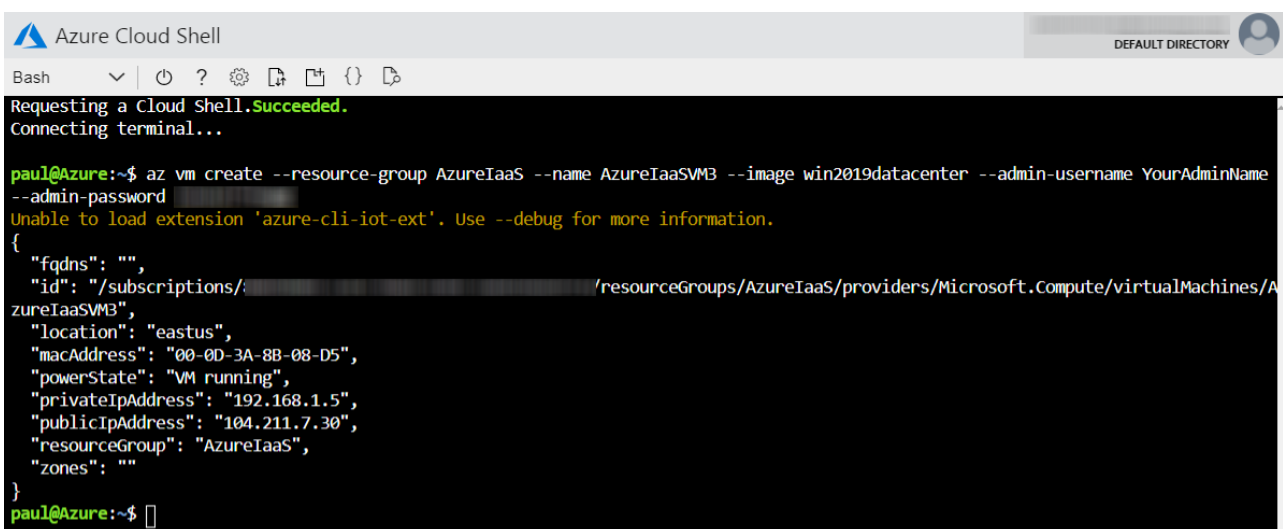
## CREATE A VM USING CLI

One nice thing about CloudShell is that you can simply swap to between CLI and PowerShell in the top left of the browser. If you want to [run the CLI on your local PC](#), it is available for Windows, macOS, Linux. You can even run it in a Docker container.

Swap to Bash (CLI) and [type in the following](#) on one line to create our third VM:

```
az vm create --resource-group AzureIaaS --name AzureIaaSVM3 --  
image win2019datacenter --admin-username YourAdminName --admin-  
password YourGoodPassword
```

Check again in the portal to make sure that the new VM shows up in your RG.



```
Azure Cloud Shell
Bash
Requesting a Cloud Shell.Succeeded.
Connecting terminal...

paul@Azure:~$ az vm create --resource-group AzureIaaS --name AzureIaaSVM3 --image win2019datacenter --admin-username YourAdminName --admin-password YourGoodPassword
Unable to load extension 'azure-cli-iot-ext'. Use --debug for more information.
{
  "fqdns": "",
  "id": "/subscriptions/.../resourceGroups/AzureIaaS/providers/Microsoft.Compute/virtualMachines/AzureIaaSVM3",
  "location": "eastus",
  "macAddress": "00-0D-3A-8B-08-D5",
  "powerState": "VM running",
  "privateIpAddress": "192.168.1.5",
  "publicIpAddress": "104.211.7.30",
  "resourceGroup": "AzureIaaS",
  "zones": ""
}
paul@Azure:~$
```

Creating a VM with the CLI

# CREATE A VM FROM A TEMPLATE

The previous methods are useful for creating VMs on an ad-hoc basis or perhaps using scripts, but realistically, once you move production workloads to Azure and you want to have repeatability, ARM templates are your friend. We'll cover these in detail in [Chapter 6](#), but let's create a VM from a template to whet your appetite.

Head over to [Azure QuickStart Templates](#), and scroll to see some of the different templates.

Clicking on See all lets you filter based on the resource type, pick Microsoft. Compute and then click on the **Deploy a simple Windows VM template**.

Templates / Deploy a simple Windows VM

## Deploy a simple Windows VM



by Brian Moore

Last updated: 10/31/2019

Deploy to Azure >

Browse on GitHub >

This template allows you to deploy a simple Windows VM using a few different options for the Windows version, using the latest patched version. This will deploy a A2 size VM in the resource group location and return the FQDN of the VM.

This Azure Resource Manager template was created by a member of the community and not by Microsoft. Each Resource Manager template is licensed to you under a license agreement by its owner, not Microsoft. Microsoft is not responsible for Resource Manager templates provided and licensed by community members and does not screen for security, compatibility, or performance. Community Resource Manager templates are not supported under any Microsoft support program or service, and are made available AS IS without warranty of any kind.

### Parameters

PARAMETER NAME	DESCRIPTION
adminUsername	Username for the Virtual Machine.
adminPassword	Password for the Virtual Machine.
dnsLabelPrefix	Unique DNS Name for the Public IP used to access the Virtual Machine.
windowsOSVersion	The Windows version for the VM. This will pick a fully patched image of this given Windows version.
vmSize	Size of the virtual machine.
location	Location for all resources.

Creating a VM from a template

Click the Deploy to Azure button, which will take you to the portal where you enter the same information as when you created the other VMs earlier. This includes things such as admin username and password, the name of the VM (**AzureIaaSVM4**) etc.

Agree to the terms and conditions and click the Purchase button to deploy your fourth VM.

## VM MANAGEMENT

There is a lot of information at your fingertips when it comes to VM management in the Azure portal. Let's take a look at some of the main sections.

Pick one of the VMs and click on its name. This brings up the overview page for that VM. The overview page will show you basic settings.

## NETWORKING

If you then click the Networking link in the left-hand menu, it'll show you the port rules in the Network Security Group and give you the option to add additional network interfaces to the VM.

## APPLICATION SECURITY GROUPS

You can also configure [Application security groups \(ASG\)](#), which is a way to group VMs together under logical names ("DB", "FrontEnd", etc.) and then build your NSG security rules using these names instead of IP addresses. When you then need to add another VM to one of the tiers, simply add it to the ASG, and the right firewall rules will apply.

## DISKS AND RESIZING

The Disks interface lets you add data disks to your VMs, and the size link lets you resize your VM.

**NOTE:** that disk resizing will require a restart if it's running, so schedule this during non-business hours.

## SECURITY

The Security link gives you alerts and recommendations but it's better to use Security Center ([Chapter 10](#)) to handle this across all your resources than managing it on an individual VM basis.

## EXTENSIONS

Extensions are also interesting and allow you to add additional functionality to your VMs such as backup, security, anti-malware, management and monitoring solutions, both from Microsoft and third parties. **The ones I would recommend as a baseline are Azure Performance Diagnostics, Application Insights (depending on the application in your VM), and either Microsoft Antimalware or your preferred third-party AV solution.**

## CONFIGURATION

The configuration link lets you enable [Just-in-time access](#) which protects RDP, SSH or WinRM access to your VMs by keeping those ports closed on a regular basis and when you need to administer the VM you log in to the Azure portal, perform Multi-Factor Authentication (MFA) to prove that it's really you and then it opens the required port for three hours.

## SOFTWARE ASSURANCE

If you have Software Assurance for your Windows (or SQL Server) licenses, you can use [Hybrid Benefit](#) to lower the cost of your Azure VMs.

## LOW LATENCY CONSIDERATIONS

If your application has low latency requirements, consider [proximity placement groups](#) and perhaps [accelerated networking](#).

## HOST GROUPS

Host groups are used for scenarios where you have to follow an industry regulation that prevents you from running VMs alongside VMs from other businesses so you can pay for a [Dedicated Host](#) exclusive to you.

## PREVENTING CHANGES

Any resource type (not just VMs) can have a lock applied to them, either preventing configuration changes (Read-only) or deletion (Delete), and the lock can only be removed by someone with the required permissions.

## RESOURCE HEALTH

[Resource health](#) tells you if there are any Azure issues currently with the fabric where your VM runs and provides a history of any platform issues for the past four weeks.

## BOOT DIAGNOSTICS

The Boot diagnostics link shows you screenshots of the system in situations where you can't access the VM and the Serial log shows you the output of the boot process (most useful for Linux VMs). If you'd like to interact with the boot process, use the Serial console for [Windows](#) and [Linux](#).

## RESETTING ADMIN PASSWORDS

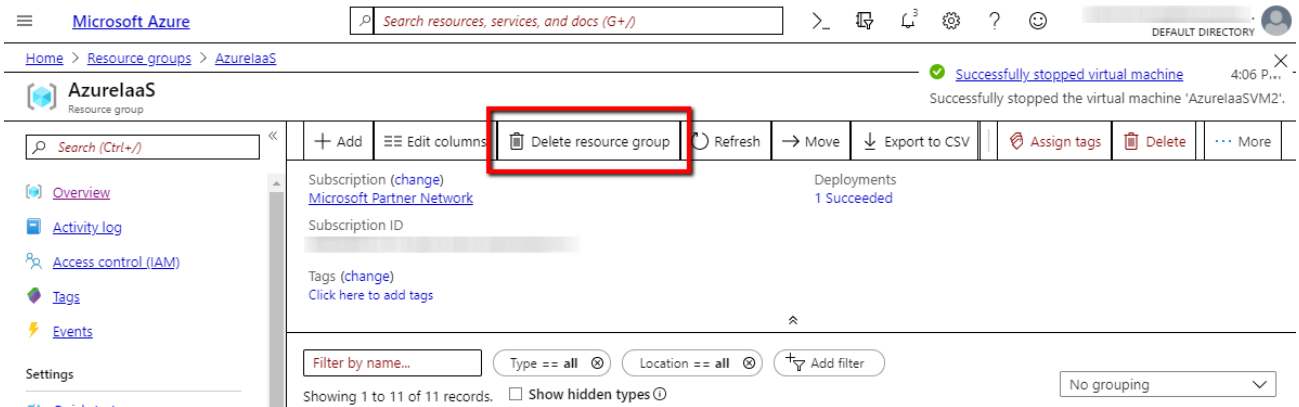
If you've forgotten the administrator password you can use Reset password.

## CONNECTIVITY TROUBLESHOOTING

Connection troubleshooting helps you figure out why you can't connect to the VM if it's caused by NSG rule misconfiguration.

## PERFORMANCE TROUBLESHOOTING

If you've got performance issues with your VMs, you can run [Performance diagnostics](#), preferably before you open a [new support request](#) with Microsoft regarding the issue.



Delete the whole resource group

Before we proceed to [Chapter 2](#), let's make sure you don't use up all your free credit on these VMs, simply by deleting the entire RG. Click on the hamburger menu in the top left of the portal, select Resource groups, and click on the AzurelaaS RG, you should see your VMs and associated resources listed. Click the Delete resource group button and confirm that you want to delete it.

# CHAPTER 2 – SIZING VMs

In this chapter, we're going to look at how you pick the VM family and size for your workload. If you use virtualization on-premises, you should be used to choosing the exact number of virtual CPU cores and memory for a new VM, along with (maybe) choosing between different backend storage arrays and their associated speeds. Now we will go through this process in Azure IaaS.

## VM SERIES

In Azure, you must pick from the [T-shirt sizes on offer](#) and you have to know which family to select; there are quite a few to choose from.

The decision making process should start with your workload – you need to know what performance characteristics the application requires and what type of deployment it is, development, test, QA or production. As you pay per minute, it's vital that you don't let your developers pick whatever they want (we'll cover Azure policy in [Chapter 6](#), which you can use to keep people within your guardrails).

The first distinction is between the Basic and Standard Tier. The former doesn't support SSD storage or high availability features and is appropriate for test/dev workloads but not production.

Each VM series also comes in versions as the underlying fabric in each Azure datacenter is upgraded by Microsoft. These are designated by a v number such as v4.

**NOTE:** you'll often find deals on the previous versions as the new ones are rolled out.

The “**s**” in a VM size indicates that the VM can use Premium Storage (SSD based) and an “**m**” shows you that its memory-optimized, with a higher ratio of memory to CPU while “**r**” is for [Remote Direct Memory Access \(RDMA\)](#), ultrafast, low latency networking between VMs. An “**a**” in a VM name indicates that the underlying Hyper-V host runs on AMD processors instead of Intel CPUs, and an “**i**” shows you that it's an isolated VM (see below).

## GENERAL PURPOSE VMS IN AZURE

For your general-purpose workloads, look at the [A, B, or D series](#) VMs. The Av2 series is good for smaller VMs and test and dev workloads that don't need a lot of power. The [B series](#), on the other hand, is appropriate for bursty workloads that don't use a lot of CPU, except for short periods of time. Your VM will accrue CPU credits when it's running but the processor isn't taxed, which it then uses said credits when the VM uses the CPU heavily. When your accrued credits run out the CPU will be throttled back. The B series is a bit of a hidden secret (it's considerably more cost-effective than the D series), as many server workloads don't use the CPU very heavily most of the time. For production workloads, the D series is the go-to workhorse, including the [recently released](#) Dasv4 series (running on the AMD EPYC™ 7452 processor).

## SPECIALIZED VMS

- For workloads requiring a higher ratio of memory to CPU, look at the [Ev3, Ev4 series and the Mv2 series](#).
- For workloads requiring higher CPU to memory ratio look at the [Fsv2 series](#),
- If you need very fast storage (Big Data, SQL and NoSQL databases), look at the [Lv2 series](#).
- For workloads that require a LOT of memory but fewer cores because you don't want to pay too much for the database software licensing when you pay per core look at [core constrained VMs](#).
- If you're doing High Performance compute (clusters of nodes crunching large datasets), look to the [HB, HC, and H](#) series VMs, they come with either 100 or 200 Gbps networking.
- If you need graphics performance, look to the [various N series](#), which offer GPUs, either for remote desktop access to graphical workstation applications or Machine Learning (ML) workloads. Recently Azure started previewing the NVv4 series that provides partitioned GPUs, where you can have access to a portion of a GPU, all the way from 2 GB to the full 16 GB (from an AMD RADEON INSTINCT™ MI25).
- The DC series gives you [encrypted hardware enclaves](#) where you can run your own code and no-one except you will have access to the data as it's being processed.

Now let's look at individual VM sizes and the naming standard. This is a list of Dsv3 VMs and their associated stats:

Size	vCPU	Memory: GiB	Temp storage (SSD) GiB	Max data disks	Max cached and temp storage throughput: IOPS / MBps (cache size in GiB)	Max uncached disk throughput: IOPS / MBps	Max NICs / Expected network bandwidth (Mbps)
Standard_D2s_v3	2	8	16	4	4000 / 32 (50)	3200 / 48	2 / 1000
Standard_D4s_v3	4	16	32	8	8000 / 64 (100)	6400 / 96	2 / 2000
Standard_D8s_v3	8	32	64	16	16000 / 128 (200)	12800 / 192	4 / 4000
Standard_D16s_v3	16	64	128	32	32000 / 256 (400)	25600 / 384	8 / 8000
Standard_D32s_v3	32	128	256	32	64000 / 512 (800)	51200 / 768	8 / 16000
Standard_D48s_v3	48	192	384	32	96000 / 768 (1200)	76800 / 1152	8 / 24000
Standard_D64s_v3	64	256	512	32	128000 / 1024 (1600)	80000 / 1200	8 / 30000

### Standard Dsv3 VM sizes

Here's how it breaks down, a [Standard\\_D32s\\_v3 VM](#) has 32 vCPU (1x to the number in the name), 128 GiB of memory (4x), supports up to 32 data disks (1x), is a Standard VM size (not Basic) and comes from the third version of the D series. On the other hand, a [memory-optimized VM](#) such as the Standard\_E32s\_v3 also has 32 vCPU (1x) but 256 GiB of memory (8x), whereas the [compute-optimized](#) Standard\_F32s\_v2 also has 32 vCPU (1x) but only 64 GiB of memory (2x).

## VM PERFORMANCE

If you find that your VM isn't using all its resources and you need to size it down or alternatively that it doesn't have enough and needs more, and you need to make it bigger, you can easily [resize it](#). It'll be restarted (so schedule a maintenance window accordingly), and if the size you're looking to move to isn't available in the hardware cluster where it's currently running, the VM needs to be stopped and deallocated first.

To be able to compare VM sizes, each VM gives an [Azure compute unit \(ACU\)](#) value where a Standard\_A1 is 100, and thus you can compare how much faster each VM series is to this baseline. If real-world figures are more your cup of tea, look at the [SPECint 2006](#) benchmarks that Microsoft has run [across all VM sizes](#).

If you have regulations that state that your workloads can't live on shared infrastructure (or you're REALLY paranoid and have deep pockets), as mentioned previously, there are [a few VM sizes](#) that guarantee that yours is the only VM on that host. You'll then use [nested virtualization](#) to carve up that VM for each of the VMs you need to run on your isolated host. These VM sizes were Microsoft first crack at isolated hosts, in-preview is the next iteration, [Dedicated host](#). This takes away the responsibility to manage the nested virtualization, you simply [pick the VM sizes you need](#), and they're deployed on your host. It also lets you manage OS patching and other platform needs.

If you've got experience with Hyper-V, you know that a few versions ago, we got a new VM type, Generation 2. While Gen 2 VMs are now available in Azure (for select VM sizes and OSs) be aware that features such as Secure Boot, Shielded VM, vTPM,

Virtualization-based security VBS and the VHDX file format are still not available in Azure (although in some cases there are equivalent technologies that make more sense than these on-premises focused features). Also, note that Site Recovery and Disk Encryption are also not supported on Gen 2 (yet).

# CHAPTER 3 – STORAGE

In this chapter, we're going to look at the different types of disks you can pick for your VMs and why this is a very important step for the overall performance of your servers.

## SSD OR HDD, STANDARD, PREMIUM OR ULTRA

Most IT pros are aware of the difference that fast storage can make for server workloads, but it's much harder to quantify than memory and processor requirements. “Database server x requires 64 GB of RAM + 4 x 2 GHz+” processor cores is very common, less common is “requires 500 IOPS per GB of database data stored”. Overall, both on-premises and in the cloud, storage Input Output Operations Per Second (IOPS), throughput in MB/s and latency make the most difference to the performance of server workloads.

When we created our first VMs in [Chapter 1](#), we had different options for the OS disk. The same options are available for additional data disks you attach to your VMs as well. All disk storage (except for Ultra, see below) are remote to your VMs and sit in a storage stamp, which introduces some latency between the Hyper-V host that runs your VM and its associated disks.

The [first choice](#) is between HDD and SSD storage, where hard drive (as you might guess) is the most cost-effective, but the slowest and only comes in a [Standard flavor](#). The speed varies with the size of the provisioned disk but starts at 500 IOPS per disk.

SSD based storage, on the other hand, comes both in Standard SSD (500 IOPS per disk between 128 GB and 4TB in size but with more even performance than HDD based storage) and [Premium SSD](#). The latter varies in IOPS; a 128 GB disk has 500 IOPS, a 256 GB disk has 1100 and a 32 TB disk comes in at 20,000 IOPS.

**NOTE:** that disks smaller than 512 GiB support [bursting](#), where it accrues credits when it's not being used at full speed and then can use those credits to increase the performance when a spike of IO occurs temporarily.

Also worth noting is that you can use Storage Spaces in Windows and software RAID in Linux to combine multiple data disks for increased performance. Remember, in both cases, you're not configuring for redundancy / data protection (unlike what you'd do on-premises) as that's taken care of by the underlying storage fabric. You're only configuring for speed. [This long article](#) covers how to configure storage for high performance in Azure and [this one](#) covers most questions you may have.

Ultra disk is a newer option for very high-performance needs and goes up to 160,000 IOPS and 2000 MB/s per disk. Another benefit is that you can change the performance characteristics of the disk while it's running so if you have a reporting server for instance that crunches end of month reports from a large database for two days every month, schedule an Azure Automation job to dial up the performance for those two days and then bring it back to a normal (and less costly) level for the rest of the time.

Be aware as you work out the disk throughput, latency, and IOPS requirements for your workload that different VM sizes have overall limits on the maximum IOPS they will support. Smaller VMs, for instance, such as a B1s, only support up to 3200 IOPS, whereas D16s\_v3 tops out at 25600 IOPS, even if you connect faster disks to them.

## DISK CONSIDERATIONS

One difference to take into account between [managed](#) and Standard (but not Premium) unmanaged disks is that the former charges you for the entire size of the disk, whether you're using all of it or not, whereas the latter only charges you for disk space actually used. There are so many benefits to managed disks, however, and you can offset the cost premium by using smaller disks for the OS drive using the [smalldisk] templates that give you a 30 GB OS drive instead of 127 GB.

The screenshot shows the Microsoft Azure Marketplace page for Windows Server. The page header includes the Microsoft Azure logo and navigation links: Home > New > Marketplace > Windows Server. The main heading is "Windows Server" by Microsoft. Below this, there's a "Select a software plan" section with a search bar and a "Create" button. A list of software plans is displayed, each starting with "[smalldisk]". The plans include Windows Server 2008 R2 SP1, Windows Server 2012 Datacenter, Windows Server 2012 R2 Datacenter, Windows Server 2016 Datacenter, Windows Server 2016 Datacenter - Server Core, Windows Server 2019 Datacenter, Windows Server 2019 Datacenter Server Core, Windows Server 2019 Datacenter Server Core with Containers, Windows Server 2019 Datacenter with Containers, Windows Server, version 1803 with Containers, Windows Server, version 1809 with Containers, and Windows Server, version 1903 with Containers. On the left side, there's an "Overview" tab and a list of features: Unique hybrid, Advanced mul, Faster innovat, and Unprecedented. Below this, there's an "Available Images" section with a description of Windows Server 2019 and a "Latest: Windows Ser" section with a list of features: Server with De, Server Core or, and Containers op.

Each VM is automatically provisioned with a temporary D: drive (/dev/sdb for Linux machines) which is located on the localhost on SSD drives (for most VM series), but this drive should only be used for truly disposable data ([TempDB in SQL server](#) in certain scenarios).

Also, consider your [options for caching](#) on VM disks– Azure hosts provide a read or a read/write cache for both OS and data disks – depending on your workload, enabling caching can improve performance.

One tip that I’ve learned the hard way is to not oversize your premium disks – you can increase their size later but not shrink them (apart from copying all the data to a new drive and then change the drive letters) and since you pay for each size increment, start as small as you can.

## UPLOADING VIRTUAL DISKS

We’ll cover migrating VMs at scale in Chapter 8, but you can actually [upload a VHD file to Azure](#) and create a VM from it. You can even upload a VHD directly as a [managed disk](#).

## A GIBIBYTE VS. A GIGABYTE

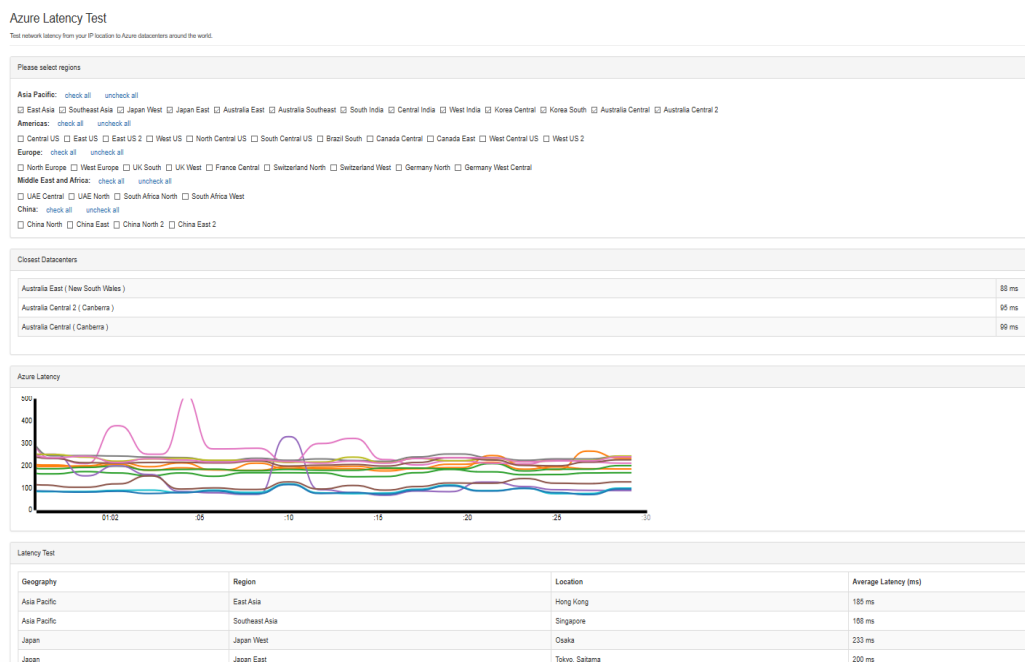
When reading Microsoft documentation you’ll come across newer terms to measure sizes such as Mebibyte (MiB), Gibibyte (GiB) and Tebibyte (TiB) which are actually the proper calculation of 1024 bytes (not 1000), so 1 Kilobyte is 1000 bytes, while one Kibibyte is 1024 bytes and so forth. This “rounding off” that hard drive manufacturers, in particular, are fond of is why your brand new 4 TB drive actually only fits 3,725 GB instead of the full 4000 GB you’d expect.

# CHAPTER 4 – NETWORKING

In this chapter, we'll look at a better way of setting up your VMs in Azure by laying the foundation of a well-designed network first. After all, if you were setting up a new branch office, you'd make sure cabling, switches and routers were in place before deploying workloads, and Azure is no different.

## KEEP YOUR VNETS CLOSE

The best way to pick the region in Azure to host your workloads is to keep them close to your datacenter or customers – use [Azure Latency Test](#) from AzureSpeed.com. This free service is not affiliated with Microsoft but very useful (and [open-sourced on GitHub](#)) and can also give you performance metrics for CDN, file transfers, and region to region latency.



Azure Speed latency test

Once you know which region provides the lowest latency, login to the portal and click the Create a resource button.

Select Networking in the left-hand menu and the very first option should be [Virtual network](#).

Give it the name **AzureIaaSvnet** and note how it picks an address space that gives you 65,536 addresses, the maximum amount a vNet can have.

**NOTE:** If you're ever planning to connect your on-premises network to Azure, make **absolutely sure** that you're picking an address space for your vNets that doesn't overlap with your on-premises address ranges.

Create a new RG called **AzureIaaS** (you did delete the RG we created in Chapter 1, right?). Each vNet can be divided into subnets and you need at least one subnet – call it **Production** with the default address space.

## Create virtual network □ ×

Name \*

AzureIaaSvnet

Address space \* ⓘ

10.1.0.0/16

10.1.0.0 - 10.1.255.255 (65536 addresses)

☐ Add an IPv6 address space ⓘ

Subscription \*

MSDN Platforms

Resource group \*

(New) AzureIaaS

[Create new](#)

Location \*

(Asia Pacific) Australia East

Subnet

Name \*

Production

Address range \* ⓘ

10.1.0.0/24

10.1.0.0 - 10.1.0.255 (256 addresses)

DDoS protection ⓘ

☒ Basic ☐ Standard

Service endpoints ⓘ

**Disabled** Enabled

Firewall ⓘ

**Disabled** Enabled

Create

[Automation options](#)

Creating a Virtual Network

The support for IPv6 is improving in Azure, and you can [enable \(preview\) support](#) for it if you need it.

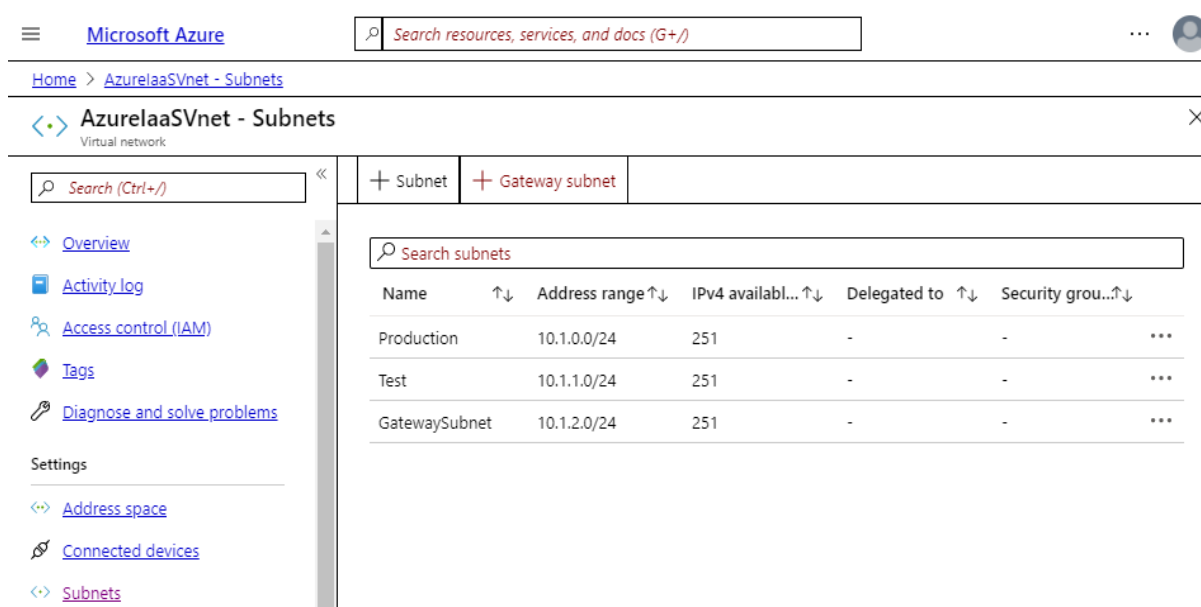
Leave [DDoS protection](#) at Basic (the same overall protection that all resources get in Azure from the daily DDoS attacks). Standard gives protection for your specific workloads with access to engineers if you're under a DDoS attack and specific reporting, along with cost protection (if you incur network charges due to the attack they'll be refunded by Azure).

Leave Service endpoints and Firewall disabled and click Create.

Go to your new network and click on the Subnets button on the left and click the +Subnet button to add another called **Test** with the default space.

**Note** that three addresses are reserved for Azure and each subnet provides 251 addresses for you to use.

While we're here, you should create a Gateway subnet as well. It'll automatically be named **GatewaySubnet**.



Microsoft Azure

Search resources, services, and docs (G+)

Home > AzureIaaSvnet - Subnets

AzureIaaSvnet - Subnets

Virtual network

Search (Ctrl+/)

+ Subnet + Gateway subnet

Search subnets

Name	Address range	IPv4 availabl...	Delegated to	Security grou...
Production	10.1.0.0/24	251	-	-
Test	10.1.1.0/24	251	-	-
GatewaySubnet	10.1.2.0/24	251	-	-

Subnets in your vNet

In this tutorial, we're only creating a single vNet but in larger deployments, you'll likely have several, perhaps in the popular [hub and spoke model](#) where a central vNet contains shared services (AD DCs, DNS, Firewall and VPN connectivity to on-premises) and spoke networks contains workloads. You can [easily connect \("peer"\) vNets together](#), both in the same region and across regions.

## NETWORK SERVICES

[Service endpoints](#) are a way to add named PaaS services in Azure (AAD, KeyVault, SQL, Storage, and Web apps, etc.) to your vNets / subnets to control traffic so that it doesn't have to pass over the internet. You can even control endpoints with [policies](#). If you need to capture all VM network traffic for security inspection or forensics, the [vNet TAP](#) service is in preview.

Azure will automatically assign IP addresses to your VMs (DHCP with infinite lease times), don't ever try to assign a specific address to a VM from within the OS itself. If a VM needs a specific IP address in your vNet, use the portal to [assign one](#). If, on the other hand, you need a fixed public IP address, perhaps to publish an application to the internet through DNS, you can [reserve those](#).

By default every vNet will use Azure provided DNS name resolution but depending on your workloads you may want to point VMs to your own DNS servers (if you're running DCs in Azure for instance) or if you're using a Site to Site (S2S) VPN, back to your on-premises DNS servers. This is configured in the left-hand menu under DNS servers. You can also use PaaS services for both [public](#) and [private DNS](#) services.

If you have many VMs in different regions and you need to redirect traffic from different geographies to the closest resource, consider using [Traffic Manager](#), a global DNS-based traffic load balancer. The endpoints that Traffic Manager points to do not have to be VMs in Azure, they can be on-premises or in other clouds as well.

If you need [load balancing](#), [Azure provides one as PaaS](#). It can be used as an internal Load Balancer (in front of several backend database servers, for instance) or as a public Load Balancer for internet traffic.

For SSL termination or application layer processing, look at [Application Gateway](#) instead, it can also be combined with Azure's [Web application firewall \(WAF\)](#), which will protect your websites from common attacks (either the [OWASP 2.2.9 or 3.1 ruleset](#)).

If you need both TLS termination and global DNS load balancing in one service, consider the [Front Door service](#) as it offers both and combines it with IPv6, HTTP/2, URL rewrite, OWASP rules and smart health probes for managing a planet-sized application.

## HYBRID NETWORKING

For many businesses having VMs running in isolation in Azure is not enough – connecting the cloud to your on-premises locations to facilitate hybrid services is required. For ad-hoc connectivity from individual computers, you can use Point to Site (P2S) VPN connectivity but for more permanent linking, you need to look at either [Site to Site \(S2S\)](#) VPN or ExpressRoute.

The former requires a [VPN router in your datacenter](#), a [VPN gateway](#) (that's why we created the Gateway subnet earlier), and [a connection](#) in Azure. The largest VPN gateway SKUs go all the way up to 10 Gbps speeds (provided your internet connectivity can keep up, of course) but S2S VPN is still going over the internet with the corresponding issues around security, latency and performance variability.

[ExpressRoute](#), on the other hand, provides a private link between your datacenter(s) and Azure and comes in speeds from 50 Mbps to 10 Gbps ([ExpressRoute Direct](#) goes all the way up to 100 Gbps). There are three connectivity models, [CloudExchange Co-location](#), [Point-to-point Ethernet Connection](#), and [Any-to-any \(IPVPN\) Connection](#). You can also use an ExpressRoute connection in one region to reach other regions over Azure's backbone (with the [Premium SKU](#)).

If you have ExpressRoute, you can have failover to an S2S VPN for even higher availability, and if you have multiple S2S and ExpressRoute connections in different locations, you can use [Virtual WAN](#) to connect these locations over Azure's backbone.

For scenarios where your existing on-premises workloads can't have their IP addresses changed as you migrate them to the cloud, you can [extend your IP address range into a vNet](#).

If you have Windows Server 2019 deployed outside of Azure, you can use the [Azure Network Adapter](#) to easily deploy a P2S VPN to connect each individual server to your vNet – handy for branch office scenarios, for instance.

To prepare for the next chapter, create a small VM in your new vNet using the steps in Chapter 1, call it **laaSVM5**, we're going to use it for monitoring and performance.

# CHAPTER 5 – MONITORING & PERFORMANCE

This chapter will show you how to monitor your VMs performance and their networking, along with tips on how to set up alerts to let you know when things aren't working correctly.

## VM PERFORMANCE

The first place to go if you get reports that a VM is misbehaving is the overview for that VM (in our case, **laaSVM5** created at the end of the last chapter). The overview screen will show you CPU, Network, and Disk statistics for the last couple of hours.

To dig deeper, head to the Metrics blade under the Monitoring heading where you can pick performance metrics to measure.

Click the Add metric button to keep adding additional measurements to track down your issue.

You can change the time span in the top right and change the chart type as well as pin your final layout to your dashboard.

Furthermore, you can create an alert rule based on a specific condition (CPU greater than 75% for more than 5 minutes as an example) or you can use the new [Dynamic thresholds](#) which are built on Machine Learning to spot behavior that's abnormal, rather than you having to figure out exactly which numbers are unusual for your

workload. Either way, you then define an Action group where you can set up email, SMS, Voice or Azure app Push Notifications as well as triggering Automation Runbooks, Functions, LogicApp, integrating with your helpdesk system (Service Now, System Center Service Manager, Provance and Cherwell) or a Webhook.

[relaaS4 - Metrics](#) > [Create rule](#) > [Add action group](#)

### Add action group

Action group name \* ⓘ

AltaroNotify ✓

Short name \* ⓘ

AltaroNotify ✓

Subscription \* ⓘ

MSDN Platforms ▼

Resource group \* ⓘ

Azurelaas ▼

Actions

Action Name *	Action Type *
Email ✓	Email/SMS/Push/Voice ▼
Unique name for the action	Select an action type ▼

[Privacy Statement](#)  
[Pricing](#)

Have a consistent format in emails, notifications and other endpoints irrespective details. [Learn more](#)

### Email/SMS/Push/Voice

Add or edit an Email/SMS/Push/Voice action

☒ Email

Email \*

✓

☐ SMS (Carrier charges may apply)

Country code \*

1 ▼

Phone number \*

1234567890

☐ Azure app Push Notifications

Azure account email \* ⓘ

email@example.com

☐ Voice

Country code \*

1 ▼

Phone number \*

1234567890

Enable the common alert schema. [Learn more](#)

Yes

No

OK

## Creating a performance alert for a VM

The monitoring we just covered is provided by the host infrastructure, if you'd like deeper information from within the guest OS, click [Diagnostics settings](#) and enable guest-level monitoring through a VM extension.

If your application supports it (.NET, .NET Core, Node.js, Mobile or web app) you can use [Application Insights](#) to provide information from within your own code.

All the steps we did to configure metrics and to set up an alert are actually provided by [Azure Monitor](#), the umbrella term for monitoring not just a single VM but your entire Azure estate. If you click the hamburger menu and click Monitor in the list, you can start monitoring across VMs, storage accounts, containers, and Cosmos DB with more coming.

Apart from monitoring your own resources, it pays to keep an eye on the Azure platform itself. You can get to [Service Health](#) from the hamburger menu (look for the broken blue heart). This lets you pick the subscriptions, resources, services and regions that matter to you to see if there are any issues with Azure itself.

You can also [set up an alert](#) to let you know if there are any service health issues. From a VM, you can click on Resource health under the Support heading; this will give you an indication if there's anything in Azure affecting the VM as well a list of past health events. You can also set up [alerts for these](#).

For best practices around the overall management of VMs in Azure, see [this excellent article](#).

## NETWORK MONITORING

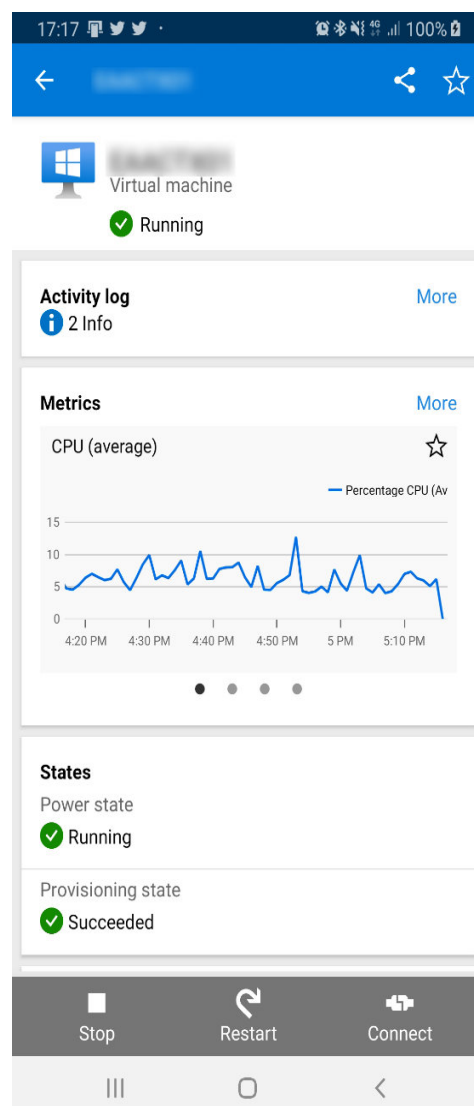
You can use [Network Performance Monitor](#) to keep an eye on performance across your hybrid infrastructure. It relies on the Log Analytics agent being installed on nodes in Azure and on-premises and installing the solution in Azure Monitor. It'll show you loss, latency, response time, and bandwidth usage between your different locations and builds a topology map to show you how everything is connected.

[Network Insights](#) is in preview in Azure Monitor and provides a dashboard that shows topology, dependencies and health for all your network nodes.

Finally, [Service Connectivity Monitor](#) can check on your websites, SaaS and PaaS applications and your SQL databases.

## AZURE IN YOUR POCKET

A great way to keep an eye on your Azure deployments is the free Azure App for iOS and Android. It shows you the health and status of your deployments (including alerts), lets you stop and start VMs and even run PowerShell / CLI against your Azure resources.



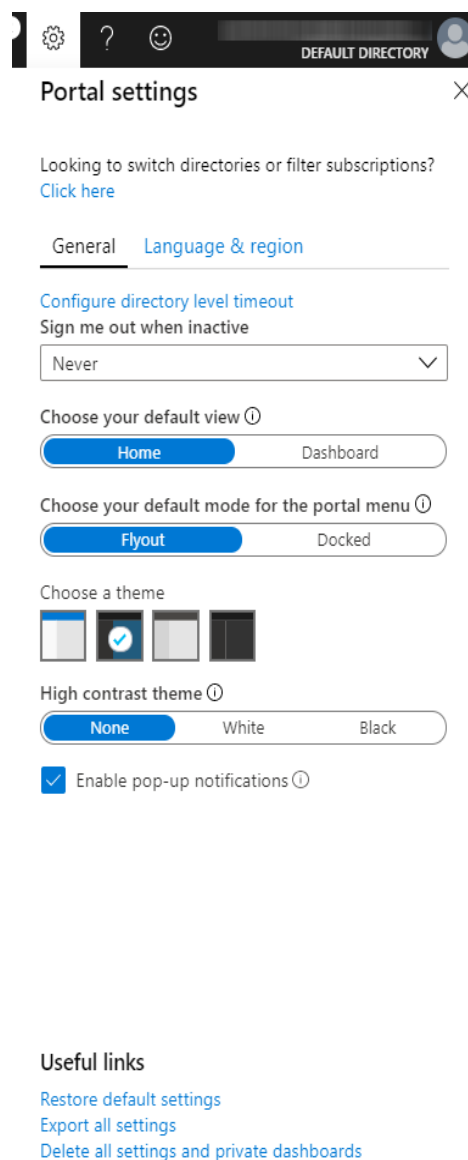
Azure App on Android

# THE PORTAL

There are a few good habits to adopt to get the most out of the Azure portal.

If you hover your mouse over a resource, a card appears where you can either create it or again hover over “view” to see more information, links to training on that resource type, and offers for you.

The settings gear (⚙️) lets you chose whether to open the portal on a dashboard or the home view, whether the left-hand portal menu should be docked or hidden (under the hamburger menu), pick a theme (including dark theme!) and high contrast settings.



The screenshot shows the 'Portal settings' dialog box in the Azure Portal. At the top, there's a header bar with a settings gear icon, a question mark, a smiley face, and a 'DEFAULT DIRECTORY' label with a user profile icon. Below the header, the title 'Portal settings' is followed by a close button (X). The main content area has a link 'Looking to switch directories or filter subscriptions? Click here' and two tabs: 'General' (selected) and 'Language & region'. Under the 'General' tab, there's a link 'Configure directory level timeout', a section 'Sign me out when inactive' with a dropdown menu set to 'Never', a section 'Choose your default view' with radio buttons for 'Home' (selected) and 'Dashboard', a section 'Choose your default mode for the portal menu' with radio buttons for 'Flyout' (selected) and 'Docked', a section 'Choose a theme' with four color swatches (light gray, dark gray, blue, and black), a section 'High contrast theme' with radio buttons for 'None' (selected), 'White', and 'Black', and a checkbox 'Enable pop-up notifications' which is checked. At the bottom, there's a 'Useful links' section with three links: 'Restore default settings', 'Export all settings', and 'Delete all settings and private dashboards'.

Portal settings

Looking to switch directories or filter subscriptions?  
[Click here](#)

General Language & region

[Configure directory level timeout](#)

Sign me out when inactive

Never

Choose your default view

Home Dashboard

Choose your default mode for the portal menu

Flyout Docked

Choose a theme

High contrast theme

None White Black

☒ Enable pop-up notifications

Useful links

[Restore default settings](#)

[Export all settings](#)

[Delete all settings and private dashboards](#)

If you have multiple accounts / subscriptions, you can swap between them by clicking on your name in the top right.

To get to the search bar to find deployed resources or new services that you may want to use, click G+.

If you want to live on the edge and see what's coming for the portal, go to [preview.portal.azure.com](https://preview.portal.azure.com) to see the latest things Microsoft is trying out for the UI.

You can also create custom dashboards; click on the hamburger and pick Dashboard, here you can edit the layout and add resources, share the dashboard with others and enable full screen (think large-screen displays in your NOC).

The screenshot displays the Microsoft Azure portal interface. At the top, there's a navigation bar with the 'Microsoft Azure' logo, a search bar labeled 'Search resources, services, and docs (G+)', and user account information. Below the navigation bar, a toolbar contains icons for dashboard management. The main area features a custom dashboard with several tiles: 'AzureIaaS4' (Virtual machine, Stopped), 'AzureIaaS4-nsg' (Network security group), 'AzureIaaS4Bastion' (Bastion), 'IaaSVM5' (Virtual machine, Stopped), 'vault247' (Recovery Services vault), and a 'Security metric' tile showing a score of 353 out of 710. Performance tiles for CPU and network usage are also present. On the right, a 'Sharing + access control' sidebar is open, showing options to publish the dashboard, set a name ('AzureIaaS'), select a subscription ('Microsoft Partner Network'), and choose a location ('Central US'). A 'Publish' button is at the bottom of the sidebar.

Custom Dashboard being shared

# WINDOWS ADMIN CENTER

If you've missed the news around [Windows Admin Center \(WAC\)](#), it's a free, web-based interface for managing Windows Server, and it's got several tie-ins with Azure. You can enable the new [Azure Arc](#) service for on-premises servers, integrate with Azure Security Center (Chapter 10) and Azure Monitor. You can even create Azure VMs from within [WAC](#).

If you want to learn more about this management tool, check out our free eBook [How to get the Most Out of Windows Admin Center](#).

# CHAPTER 6 – BEHIND THE SCENES – ARM

In this chapter, we'll introduce you to [Azure Resource Manager \(ARM\)](#), the control plane of Azure, and what it means for your IaaS deployments.

## INFRASTRUCTURE AS CODE

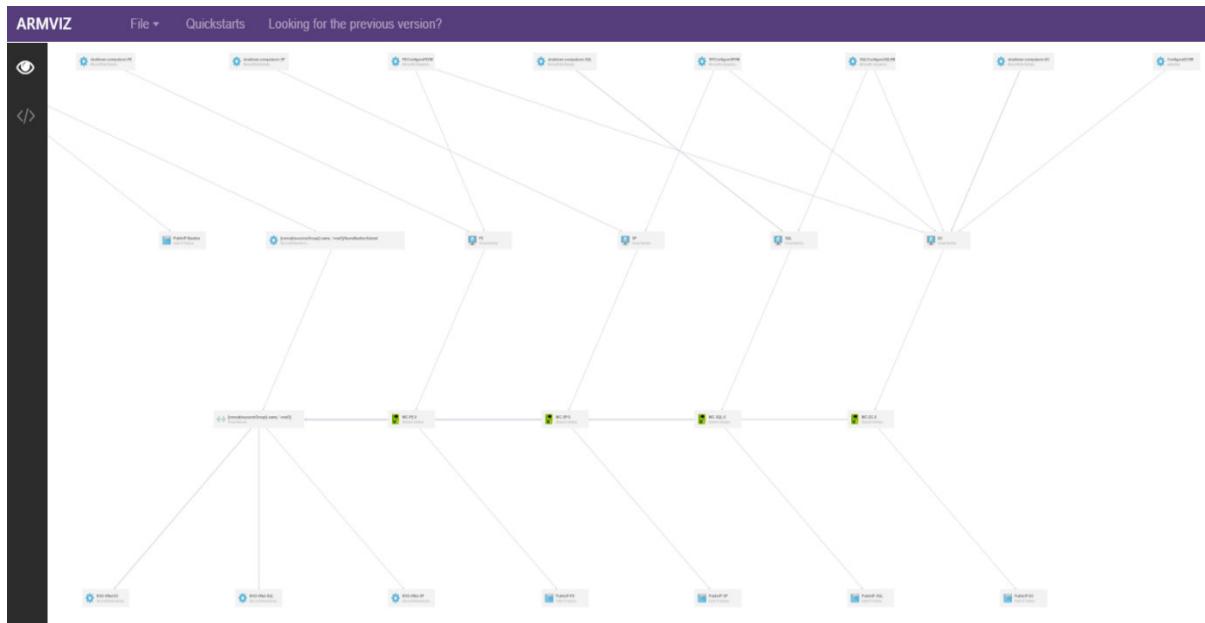
A concept that's slowly permeating IT departments is the idea of having the code (templates and artifacts) that define your servers, databases, networking and storage etc. treated just like application code written by developers. You then store it centrally in a code repository (like git) with version control and deploy new environments in a predictable manner. [ARM templates](#) facilitate this approach, as does [Azure DevOps](#).

To see how you could use templates to achieve this repeatability nirvana, head over to Quickstart templates again and click on the Microsoft.Compute link on the left.

Do a search for SharePoint and click on the **SharePoint 2019, 2016 and 2013 configured with ADFS** template.

Click on the Browse on GitHub button to see the files associated with the template as well the Visualize button, which gives you either a diagram of the resources in the deployment and their relationship or a code view of the template.

When you click on a resource in the diagram, you're taken to the part of the template that defines that part of the deployment.



Four VM SharePoint ARM template

Scroll through, and you'll see that the JavaScript Object Notation (JSON) layout is quite easy to understand. Start at the top where you'll see bits about what Schema version is used and then the definition of several parameters. Together with a parameters file, you could deploy an entire SharePoint farm with a single line of PowerShell or Azure CLI. If you've ever done that manually, you will now likely understand the power of ARM and infrastructure as code.

A thorough deep dive on the ARM language is beyond the scope of this book but take [this free course](#).

ARM takes care of deploying all the VMs and associated infrastructure, but when it comes to configuring the OS inside those VMs, look to [Desired State Configuration \(DSC\) from PowerShell](#). For editing ARM templates (and DSC), [Visual Studio Code](#) with the [right extensions](#) is my favorite tool (and it's free!).

Looking beyond ARM and Azure, there are several other approaches to infrastructure as code. One is [Terraform by Hashicorp](#). It works for Azure, GCP and AWS. Another [recent addition by Microsoft](#) is support for [Pulumi](#) which uses JavaScript, TypeScript or Python to [describe cloud infrastructure](#).

## BLUEPRINTS

If your business is in a regulated industry, you should consider applying [Blueprints](#), a superset on top of ARM templates that adds support for Roles and Policy (see below) assignments to create entire environments. Unlike ARM templates (which you can store anywhere you want), Blueprints are stored in Cosmos DB and are replicated to several regions and they maintain a link back to the deployment so you can upgrade deployments simply by upgrading the template. Microsoft also provides many Blueprints [aligned with regulations](#) such as ISO 27001, NIST SP 800-53, and PCI-DSS and others.

## AZURE POLICY

This is probably one of the most underused and most powerful “hidden” features of Azure. As a subscription owner, you can define policies that restrict [what size VMs \(and other resources\)](#) your IT staff can create, in which regions they can create them as well as require them to add tags (see below) when they create them for example.

After resources have been deployed, you can audit their state to see if they have disk encryption enabled or backup is configured, for instance, along with many other policies. And if the resources don't conform to a policy they can be automatically remediated. You can combine several policies into [an initiative](#) that can be applied as a unit to achieve an overall governance goal.

The screenshot shows the 'Policy - Definitions' page in the Microsoft Azure portal. The left sidebar contains navigation links: Overview, Getting started, Join Preview, Compliance, Remediation, Authoring (Assignments, Definitions), and Related Services (Blueprints (preview), Resource Graph, User privacy). The main content area has tabs for '+ Initiative definition', '+ Policy definition', and 'Refresh'. Below these are filters for Scope (2 selected), Definition type (Policy), Type (Built-in), Category (1 categories), and a Search bar. A table lists 12 policies, all of which are 'Policy' type and 'Compute' category. The policies are related to virtual machines, including disaster recovery, managed disks, migration, antimalware, disk encryption, OS patching, diagnostic logs, and VM extensions.

Name	Definition type	Type	Category	Search
Audit virtual machines without disaster recovery configured	Policy	Built-in	1 categories	Filter by name or id...
Audit VMs that do not use managed disks	Policy	Built-in	1 categories	Filter by name or id...
Virtual machines should be migrated to new Azure Resource Manager resources	Policy	Built-in	1 categories	Filter by name or id...
Deploy default Microsoft IaaS Antimalware extension for Windows Server	Policy	Built-in	1 categories	Filter by name or id...
Unattached disks should be encrypted	Policy	Built-in	1 categories	Filter by name or id...
Require automatic OS image patching on Virtual Machine Scale Sets	Policy	Built-in	1 categories	Filter by name or id...
Diagnostic logs in Virtual Machine Scale Sets should be enabled	Policy	Built-in	1 categories	Filter by name or id...
Microsoft IaaS Antimalware extension should be deployed on Windows servers	Policy	Built-in	1 categories	Filter by name or id...
Only approved VM extensions should be installed	Policy	Built-in	1 categories	Filter by name or id...
Microsoft Antimalware for Azure should be configured to automatically update protection signatures	Policy	Built-in	1 categories	Filter by name or id...
Allowed virtual machine SKUs	Policy	Built-in	1 categories	Filter by name or id...

List of VM specific Azure Policies

## TAG – YOU'RE IT!

[Each deployed resource](#) in Azure can have up to [50 tags applied to it](#) (used to be 15) which are simple name-value pairs; examples are; **Environment** (Dev, Test, QA, Production), **Owner**, **Cost Center** (which will show up in your bill from Azure) and **Department**. And you can use Azure Policy to enforce the use of tags for your resources, creating a well-governed cloud estate instead of a wild west mess.

For even better management, spend some time with your teams to work out a naming convention for all resources. Here's a good [starting point](#).

# MANAGEMENT GROUPS

A big puzzle piece for a large, well-governed Azure deployment is [Management Groups \(MG\)](#), these are a way to group many different subscriptions and their associated RGs under one organizational umbrella. Once you have enabled the first root MG (takes up to 15 minutes), you can create further MGs to mimic your company structure and then apply Azure Policy and RBAC permissions at each level. So, if you need a companywide policy, apply it at the root MG, policies that should apply only to European resources are applied at that MG level and so forth.

Management Groups and associated subscriptions

# RESOURCE GRAPH

The final piece of ARM and governance is [Azure Resource Graph](#), which lets you query and explores already deployed resources to filter, group, and sort to figure out what is out there and assess the impact of applying Azure policy in large deployments. The best way to try it out is to have some resources deployed and then do a portal search for resource graph queries – try out [some of the samples](#).

Microsoft Azure

Home > Resource Graph queries > Azure Resource Graph Explorer

Azure Resource Graph Explorer

Query 1 X Query 2 X

```

1 Resources
2 | project name, location, type
3 | where type =~ 'Microsoft.Compute/virtualMachines'
4 | order by name desc

```

Results Charts Messages

Download as CSV Pin to dashboard

name	location	type
AzureIaaS4	australiaeast	microsoft.compute/virtualmachines

See details

## Resource Graph Query

You can also use Resource Explorer to drill down in a graphical way to see what's deployed, test it out with **IaaSVM5** and see the separate components such as a NIC and disks that make up a VM.

Microsoft Azure

Home > Resource Explorer

Resource Explorer

Search...

Resources (Response Time 165ms)

/subscriptions/aba3adde-9e7e-426a-a57b-7af31875b54/resourceGroups/AzureIaaS/resources?api-version=2014-04-01-preview

```

1 {
2   "value": [
3     {
4       "id": "/subscriptions/aba3adde-9e7e-426a-a57b-7af31875b54/resourceGroups/AzureIaaS/providers/Microsoft.Compute/disk1_57c6eb9ef82d4d95bda050d4a26c4ea2",
5       "name": "AzureIaaS4_disk1_57c6eb9ef82d4d95bda050d4a26c4ea2",
6       "type": "Microsoft.Compute/disk1_57c6eb9ef82d4d95bda050d4a26c4ea2",
7       "sku": {
8         "name": "Premium_LRS",
9         "tier": "Premium"
10      },
11      "location": "australiaeast"
12     },
13     {
14       "id": "/subscriptions/aba3adde-9e7e-426a-a57b-7af31875b54/resourceGroups/AzureIaaS/providers/Microsoft.Compute/virtualMachines",
15       "name": "AzureIaaS4",
16       "type": "Microsoft.Compute/virtualMachines",
17       "location": "australiaeast"
18     },
19     {
20       "id": "/subscriptions/aba3adde-9e7e-426a-a57b-7af31875b54/resourceGroups/AzureIaaS/providers/Microsoft.Compute/virtualMachines/extensions",
21       "name": "AzureIaaS4/LinuxDiagnostic",
22       "type": "Microsoft.Compute/virtualMachines/extensions",
23       "location": "australiaeast"
24     },
25     {
26       "id": "/subscriptions/aba3adde-9e7e-426a-a57b-7af31875b54/resourceGroups/AzureIaaS/providers/Microsoft.DevTestLab/schedules",
27       "name": "shutdown-computevm-AzureIaaS4",
28       "type": "Microsoft.DevTestLab/schedules",
29       "location": "australiaeast"
30     },
31     {
32       "id": "/subscriptions/aba3adde-9e7e-426a-a57b-7af31875b54/resourceGroups/AzureIaaS/providers/microsoft.insights/actiongroups",
33       "name": "AltaroNotify",
34       "type": "Microsoft.insights/actiongroups"
35     }
36   ]
37 }

```

## Resource Explorer

# CHAPTER 7 – MANY VMs

This chapter looks at deploying groups of VMs and managing availability, scale-out / in and cost management for Azure.

## AVAILABILITY

A single VM running on Premium SSD disks (OS and data disks) receives [a financially backed 99.9% SLA](#) from Azure. If you want better uptime, look at [Availability Sets \(AS\)](#).

As an example, say you have two Domain Controllers for your on-premises domain running in Azure (linked back to on-premises with an S2S VPN). If you put them in an AS, Azure will automatically distribute them in separate fault domains (racks/servers/storage units/network switches), giving you a 99.95% SLA.

If you need [even better VM availability](#), look at [Availability Zones \(AZs\)](#). Each Azure region is (generally speaking) not a single datacenter but several buildings designed with independent power, cooling, and networking infrastructure, providing redundancy for services that are AZ aware. In the [10 regions that are AZ enabled](#) you can choose to deploy resources to numbered AZs (1-3). Note that you can't rely on this numbering to be consistent across subscriptions, Zone 1 in one subscription may not refer to the same datacentre in another subscription. If you spread VM instances across zones, they get a 99.99% SLA.

## MANY VMS

If you need an “elastic pool” of VMs that can be scaled out or in based on demand, [VM Scale Sets \(VMSS\)](#) are your friend, they’re also AZ aware. Let’s test this out now.

Login to the portal and press G+/ to activate the search box and type “VM Scale” and pick Virtual machine scale sets in the results.

Click Create virtual machine scale set, and call the VMSS **laaSVMS**, pick Windows Server 2016 Datacenter, put it in the AzureIaaS RG, and select all three zones under AZ.

Enter a username and password, set the instance count to 3, and change the VM size to B1ms (less costly than the D series it defaults to).

Enable Autoscale and leave the defaults for scale-out and scale in.

For Networking pick Load balancer (you can use either a load balancer or the Application Gateway depending on your workload– see chapter 4),

call the Public IP address **laaSVMS** and pick **laasvmss** for the beginning bit of the DNS name (note that this has to be unique across the internet so that name may already be taken, just add some characters).

Pick your vNet and open port 3389 for RDP, leave all other settings at default and click Create.

This is the power of the cloud. With just a few clicks, you just created an HA, load-balanced set of three VMs spread across three datacenters.

### Create virtual machine scale set

[Preview the new create experience →](#)

---

**BASICS**

Virtual machine scale set name \*  ✓

Operating system disk image \* ⓘ  ✓  
[Browse all public and private images](#)

Subscription \*  ✓

Resource group \*  ✓  
[Create new](#)

Location \*  ✓

Availability zone ⓘ  ✓

Username \* ⓘ  ✓

Password \*  ✓

Confirm password \*  ✓

---

**INSTANCES**

Instance count \* ⓘ  ✓

Instance size \* ⓘ **Standard B1ms**  
 1 vcpu, 2 GiB memory  
[Change size](#)

Deploy as low priority (preview) ⓘ ☒ No ☐ Yes

---

[Automation options](#)

## Create a VM Scale Set

Let's look at some of the options that we left at default, such as [low priority](#) VMs, which takes advantage of spare capacity in Azure regions. You pay a lot less for these VMs (they have no SLA) but they can be turned off at any time, so are only appropriate for stateless workloads or applications where you're continually storing data for the applications outside of the VMSS.

You can combine low priority with [Ephemeral OS disks](#), which are stored on the local Hyper-V hosts in Azure and thus provide lower latency and faster deployment times, again suitable for stateless workloads.

Name	Status	Protection policy	Latest model
<input type="checkbox"/> IaaSVMSS_2	Running		Yes
<input type="checkbox"/> IaaSVMSS_5	Running		Yes
<input type="checkbox"/> IaaSVMSS_6	Running		Yes

## Nodes in a VM Scale Set

Once your VMSS is deployed, you can click on the Scaling option to manually scale up the number of nodes – note that the maximum is 1000; **you don't want to do that with the limited dollars in an Azure trial.**

**Note** that you can also configure additional scale-out rules instead of just the default CPU rule that we set during the creation of the VMSS.

Choose how to scale your resource

**Manual scale** (Selected)  
Maintain a fixed instance count

**Custom autoscale**  
Scale on any schedule, based on any metrics

Manual scale

Override condition

Instance count: 393

## Scaling out a VM scale set

**IMPORTANT:** To make sure you don't use up your free credits – make sure to go to Home in the portal, click on All resources, and delete **IaaSVMSS** so you don't continue paying for the scale set.

## SHARING IMAGES

As your estate in Azure grows, you're eventually going to need to manage images company-wide and [Shared Image Gallery \(SIG\)](#) is the solution for this. It lets you version and group VM images and stores them in an HA-enabled way in Zone Redundant Storage (ZRS) by replicating them between regions and sharing them across subscriptions and between AAD tenants. A VM image can be just the OS disk or all disks, including data disks. There is no extra cost for the SIG functionality, only the storage cost.

## COST MANAGEMENT

One of the great challenges in moving to the cloud for many organizations is managing cost. Most CFOs will be more than happy to move from a Capital Expenditure (CAPEX) to an Operational Expenditure (OPEX) model, but they will want to know HOW big that monthly bill is going to be.

If you're early in your cloud migration journey, start with the [TCO Calculator](#) that lets you compare your on-premises workload costs against Azure costs.

Another great option, which we'll cover more in detail in Chapter 8, is [Azure Migrate](#), which helps evaluate your VMware, Hyper-V and physical server workloads on-premises. It provides you with reports detailing the equivalent VM sizes to use in Azure (based on actual performance data, not the size your VMs are on-premises) and monthly costs.

[Reserved Instances \(RI\)](#) are another option where you pay per month for a certain collection of VM capacity that you've committed to for one or three years, providing you a substantial discount. You can also scale VMs up and down in size within the overall capacity you've reserved. Note that RI works best for VMs that are on 24/7, if you turn them off during non-business hours, RI may not be cost-effective. RI was also recently expanded [to services other than VMs](#), such as storage, Premium SSD disks and databases.

For a quick overview of your spend click on the hamburger menu and then on Subscriptions, that'll show you a donut graph of your current spend in this billing month on various resources. For more in-depth analysis head to [Cost Management + Billing](#) where you can slice and dice your costs for various billing periods and resources, it's also had some [recent updates](#). Here you can also set alerts on spending and create budgets to manage spending by department for instance.

# CHAPTER 8 – BACKUP & REPLICATION

In this chapter, we're going to deal with another common misconception about the cloud. We'll focus on backup, replication and Disaster Recovery (DR). We'll also look at migrating VMs to Azure and how you can continue to run your VMs on VMware, even when they're in Azure.

## BACKUP

The myth that “since it's in the cloud, I don't need to back it up” is persistent, but nothing could be further from the truth. First, you may be subject to regulations that require you to keep backups of production applications and data for several years. Beyond that, you need backups of your VMs to protect yourself against user mistakes (deleting or overwriting the wrong file or clicking the wrong button), admin mistakes (“oh, I thought that was the test VM that you wanted me to delete”), data corruption or ransomware encrypting all your data files.

At this stage, you should have a single VM, **laaSVM5** (you did remember to delete the scale set – didn't you?) open it in the portal and click on the Backup link under Operations. It'll suggest creating a Recovery Services vault to store your backups, click **Create (or edit) a new policy**, and set your backup frequency and retention period (up to 99 years for the yearly points), then click Enable Backup.

## Backup policy



The changes will apply to all the existing and new recovery points. Existing recovery points will be affected and now retained as per the modified retention range.

### Backup schedule

Frequency \* Time \* Timezone \*

Daily 9:30 PM (UTC+10:00) Brisbane

### Retention range

☒ Retention of daily backup point.

At \* For

9:30 PM 180 Day(s)

☐ Retention of weekly backup point.

Not Configured

☐ Retention of monthly backup point.

Not Configured

☒ Retention of yearly backup point.

Week Based Day Based

In \* On \* Day \* At \* For

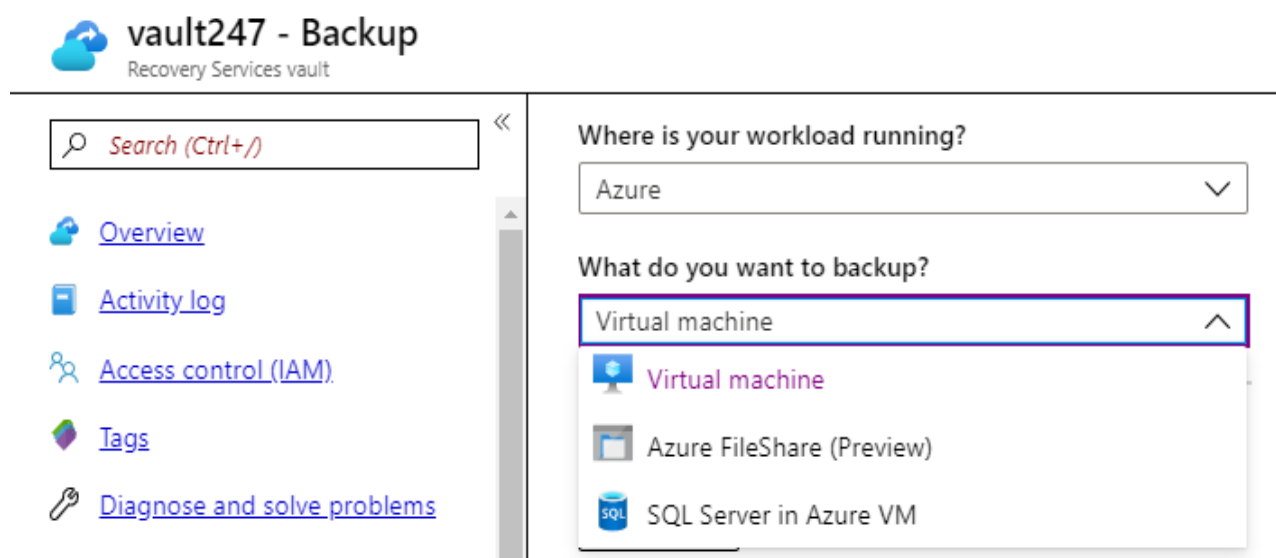
January First Sunday 9:30 PM 99 Year(s)

## Backup Policy Configuration

When you have production VMs [take a holistic approach](#), go to the search bar and type in Backup.

Click on Recovery Services Vaults and click on the name of your vault, select Backup in the left-hand menu.

Here you can pick what to backup and where it's running. Once you click Backup, pick your policy, and then you'd select all VMs that require protection (instead of having to do it on each individual one). You can also use [Azure Policy](#) to enforce the configuration of backup on VMs.



Configuring Backup from a Vault

Note that [Backup](#) works for both Windows and Linux VMs and you can restore [individual files](#) and folders as well as [whole VMs](#), [SQL Server in a VM is easily protected](#), and [that deleting backups](#) require several steps to ensure that attacker who is encrypting your files can't easily get rid of your backups to leave you with no choice but to pay the ransom. And when you do [delete backups](#), they're still kept (14 days) in case you change your mind.

**Note:** This provides basic protection for your Azure virtual machines.

If you require over and above this level of functionality, you'll need to go to a third-party backup provider.

## REPLICATION

For complete protection, you should use [Site Recovery](#) to replicate business-critical VMs from one region to another, in case a whole region has an outage (it [has happened](#)). Note that you'll need to create another vault in a separate region from the VM and then [replicate the VM](#) to that region.

## ALTARO VM BACKUP

To protect your on-premises VMs (VMware and Hyper-V), you can use [Altaro VM Backup](#), which easily [replicates VMs to Azure storage](#). You can then restore the protected VMs to the original host or an alternate host or if it's a major disaster, you can [restore the VMs to Azure](#) instead.

## MIGRATE

[Azure Migrate](#) is a collection of tools to identify your on-premises workloads ([VMware](#), [Hyper-V](#), and [physical servers](#)), their dependencies, their performance requirements, and any blocking issues for running them in Azure in reports that use to assess your expected costs for a “lift and shift migration.” It'll also help you with the actual migration of servers to Azure. Migrate also integrates with a number of [third-party services](#) for assessments and migrations.

	A	B	C	D	E	F	G	I	J	K	L	M
	Machine	Azure VM readiness	Azure readiness details	Recommended size	Compute monthly cost USD	Storage monthly cost USD	Operating system	Cores	Memory(MB)	CPU usage(%)	Memory usage(%)	Storage(GB)
1	ESDC01AD02	Ready For Azure	NotApplicable	Standard_F4s	57.39	17.92	Microsoft Windows Server 2016 (64-bit)	2	4096	0.85	6.85	100
2	EAACTX01	Ready For Azure	NotApplicable	Standard_D16s_v3	219.58	34.56	Microsoft Windows Server 2016 (64-bit)	8	32768	45.43	29.79	200
3	EAAWIN7	Ready For Azure With Conditions	WindowsClientVersionsConditionallySupported	Standard_F4s	57.39	17.92	Microsoft Windows 7 (64-bit)	2	4096	2.95	6.99	100
4	ESDC01AD01	Ready For Azure	NotApplicable	Standard_F4s	57.39	17.92	Microsoft Windows Server 2016 (64-bit)	2	4096	0.95	7.99	100
5	EAAQLO1	Ready For Azure	NotApplicable	Standard_DS4_v2	117.33	253.44	Microsoft Windows Server 2016 (64-bit)	4	16384	3.18	6.79	1636
6	ESDC01NS01	Ready For Azure	UnendorsedLinuxDistributions	Standard_F4s_v2	45.25	4.8	Oracle Solaris 10 (64-bit)	2	2048	53.89	6.65	20
7	ESDC01FP01	Ready For Azure	NotApplicable	Standard_F16s	229.58	271.36	Microsoft Windows Server 2016 (64-bit)	4	8192	2.18	10.92	2248
8	ESDC01CTXD01	Ready For Azure	NotApplicable	Standard_DS3_v2	59	17.92	Microsoft Windows Server 2012 (64-bit)	2	8192	4.24	18.23	100
9												
10												

If you don't want to convert your VMware VMs to run on Azure and would prefer to keep using VCenter and other VMware tools to manage your VMs look at [Azure VMware Solution by CloudSimple](#). It gives you the full power of VMware combined with the integration of PaaS services in Azure.

Another service you can use as part of your migration to the cloud is the [Storage Migration Service](#) built into Windows Server 2019. It lets you move file servers from one server to another, originally positioned as a “help you upgrade” tool to go from earlier Windows Server versions to Windows Server 2019 but you can use it to migrate (and upgrade them simultaneously) file servers from on-premises to Azure without actually moving the file servers themselves.

# CHAPTER 9 – AZURE AD

In this chapter, we'll look at Azure Active Directory (AAD) and how you can integrate identity with VMs as well as Azure AD Domain Services, a service that makes it easy to host your AD domain in Azure.

## IDENTITY IS THE NEW FIREWALL

Typing Active into the search bar and click AAD will take you to your default directory, created with your trial subscription (if you're not using a trial subscription, tread lightly here as you could interfere with production AAD operations).

Clicking Roles and administrators on the left introduces you to the built-in [Administrative roles in AAD](#). Note that many of these are there because AAD isn't just the directory for your users in Azure, it's also the directory for Office 365.

In a production deployment, you'd use these roles to assign users the permissions they need to do their work (and no more). If you have AAD Premium P1 or P2 (paid versions of AAD), you can create custom admin roles as well as use [Privileged Identity Management \(PIM\)](#) to turn administrative users into "eligible" accounts where they have to request an elevation to be able to perform administrative tasks and they're only granted the role for a short amount of time.

**Default Directory - Roles and administrators**  
Azure Active Directory

Search (Ctrl+/)

[+ New custom role](#)
[Refresh](#)
[Got feedback?](#)

To create custom roles, your organization needs Azure AD Premium P1 or P2. Start a free trial. →

**Your Role:** Global administrator

**Administrative roles**  
Administrative roles can be used to grant access to Azure AD and other Microsoft services. [Learn more](#)

Search:  Type:

Role	Description	Type
Application administrator	Can create and manage all aspects of app registrations and enterprise apps.	Built-in
Application developer	Can create application registrations independent of the 'Users can register a...	Built-in
Authentication administrator	Has access to view, set, and reset authentication method information for any...	Built-in
Azure DevOps administrator	Can manage Azure DevOps organization policy and settings.	Built-in
Azure Information Protection admini	Can manage all aspects of the Azure Information Protection product.	Built-in
B2C IEF Keyset administrator	Can manage secrets for federation and encryption in the Identity Experience ...	Built-in
B2C IEF Policy administrator	Can create and manage trust framework policies in the Identity Experience Fr...	Built-in
B2C user flow administrator	Can create and manage all aspects of user flows.	Built-in
B2C user flow attribute administrator	Can create and manage the attribute schema available to all user flows.	Built-in
Billing administrator	Can perform common billing related tasks like updating payment information.	Built-in
Cloud application administrator	Can create and manage all aspects of app registrations and enterprise apps ...	Built-in
Cloud device administrator	Full access to manage devices in Azure AD.	Built-in
Compliance administrator	Can read and manage compliance configuration and reports in Azure AD an...	Built-in
Compliance data administrator	Can create and manage compliance content.	Built-in
Conditional Access administrator	Can manage conditional access capabilities.	Built-in
Customer LockBox access approver	Can approve Microsoft support requests to access customer organizational d...	Built-in

## Azure AD Administrative Roles

[Application proxy](#) lets you publish on-premises applications to remote users, negating the need for VPNs. [Azure AD Connect](#) is the umbilical cord back to your on-premises AD and definitely something you should use for your hybrid cloud: creating / changing and deleting accounts in a single place (AD) and have them automatically synced to AAD is a real time saver.

There's [a lot more to AAD](#) that's beyond the scope of this book.

## MANAGED IDENTITIES

An age-old problem for applications is where to store the credentials for accessing services. Ideally, they should never be on the developer's PC, nor checked into source control. In Azure, this is accomplished with the free service [managed identities](#). This puts a service principal into AAD that's used, for instance, when an application in your VM needs to [access Azure SQL](#) (database PaaS service) or [storage](#), obviating the need to store credentials in the application or the VM. There are two types: System-assigned and User-assigned. The former is created as part of resources and shares its lifecycle and is used only by that resource. The latter, in contrast, is created separately and can be shared among multiple resources (several VMs accessing the same Data Lake, for instance). There's [a free course](#) to learn more.

## AZURE AD DOMAIN SERVICES

If you're migrating older applications that rely on Kerberos, NTLM, and AD authentication to the cloud, you may have to spin up one or more DCs in VMs in the cloud (make sure you don't put the AD database on the temporary D: drive). This is a bit of management overhead, and you have to keep them running, back them up, patch and protect them against malware etc.

[AAD Domain Services](#) is an alternative – a PaaS domain service that Microsoft manages and patches that integrates with your AAD tenant (which in turn is synced with your on-premises AD with AAD Connect). You can create two types of forests, a User forest or a [Resource forest](#), depending on your business needs.

## LOGGING IN WITH AAD ACCOUNTS

If you have one or two test VMs in the cloud, logging in with a local admin account works, but as your estate grows, better solutions are needed. You can use your AAD account to login to both [Windows](#) and [Linux](#) VMs through a VM extension. It integrates with AAD Multi-Factor Authentication (MFA), Conditional Access, and you can use Role-Based Access Control (RBAC) to assign permissions to VMs. This service is currently in preview.

# CHAPTER 10 – SECURITY

This chapter looks at Azure Security Center (ASC), patching Linux and Windows VM, Bastion, Just-In-Time VM access, Disk Encryption, Key Vault, Firewall, and other services – all designed to improve your security posture in the cloud.

## AZURE SECURITY CENTER

It's important to remember that security in a public cloud is a shared responsibility. Some things are taken off your plate compared to on-premises such as physical security, disk destruction at the end of a server's lifetime, etc. However, the applications in your VMs and the OS in those VMs are your responsibility, both to manage and protect.

[Azure Security Center \(ASC\)](#) helps you with [these challenges](#) – it's your one-stop-shop for understanding the security posture of your workloads (whether [on-premises](#), in Azure or in other clouds), threat protection, and regulatory compliance. It uses the same concept as Microsoft 365 – [Secure Score](#) to “gamify” security-related actions you take by assigning them a score tracking the improvement in your overall score over time.

ASC will draw a Network map to show the topology of your workloads and how they're connected to spot potential avenues for bad guys, and it'll give you recommendations based on your applications on how to improve security.

Features you can audit to see if they're on, and enable if they're not, include just-in-time access, blocking access to RDP / WinRM for Windows servers and SSH for Linux until you unlock it for a period of three hours from the portal when you need to administer the VM. [Adaptive application controls](#) uses Machine Learning (ML) to build an allow list of applications running in your VMs. Whitelisting applications like this is notoriously difficult on end-user machines as they change so frequently, whereas servers generally have stable workloads and lend themselves to making sure only known software can run (you can also alert rather than block other executables). [File Integrity Monitoring](#) tracks changes to file and registry entries, while Adaptive Network Hardening monitors your network flows and NSG rules to identify opportunities to harden the rules further. All three of these security measures apply to both Linux and Windows VMs. ASC comes in a [free flavor and a Standard SKU](#) with additional features.

## PATCHING

[Update Management](#) is part of Automation (Chapter 11) and lets you manage OS updates for both [Windows](#) and [Linux](#). You can run assessments to identify what patches your machines are missing, pick what classifications to deploy and patch VMs to bring them in line with your baseline. It also [integrates with System Center Configuration Manager \(SCCM\)](#) if you're using that.

## BASTION

An alternative to leaving RDP/SSH ports open to the internet (a really bad idea) and just-in-time VM access (better, though a bit clunky) is [Azure Bastion](#). It provides [SSH](#) and [RDP](#) access directly from [within the Azure portal](#), on your VMs and is even better

than a jump box (a single VM that is open to the on-premises management PCs) that many IT departments have adopted, because it requires no open management ports and it's a managed PaaS service instead of a VM that you have to manage. The [cost is 19 cents per hour](#) (about \$ 140/month) with outbound data charges once you go over 5 GB in a month.

To create a Bastion, start by going to your vNet (for the IaaSVM5) and create a new subnet called **AzureBastionSubnet** with at least a /27 space.

Do a search in the portal for Bastion and click Create a Bastion. Call it **AzureIaaS Bastion**, put it in the AzureIaaS RG and leave all other configurations as default.

Create a bastion

---

[Basics](#) [Tags](#) [Review + create](#)

---

Bastion allows web based RDP access to your vnet VM. [Learn more.](#)

**Project details**

Subscription \*

Resource group \*   
[Create new](#)

**Instance details**

Name \*

Region \*

**Configure virtual networks**

Virtual network \*   
[Create new](#)

☒ To associate a virtual network with a Bastion, it must contain a subnet with name AzureBastionSubnet with prefix of at least /27.

Subnet \*   
[Manage subnet configuration](#)

**Public IP address**

Public IP address \* ☒ Create new ☐ Use existing

Public IP address name \*

Public IP address SKU

Assignment \* ☐ Dynamic ☒ Static

---

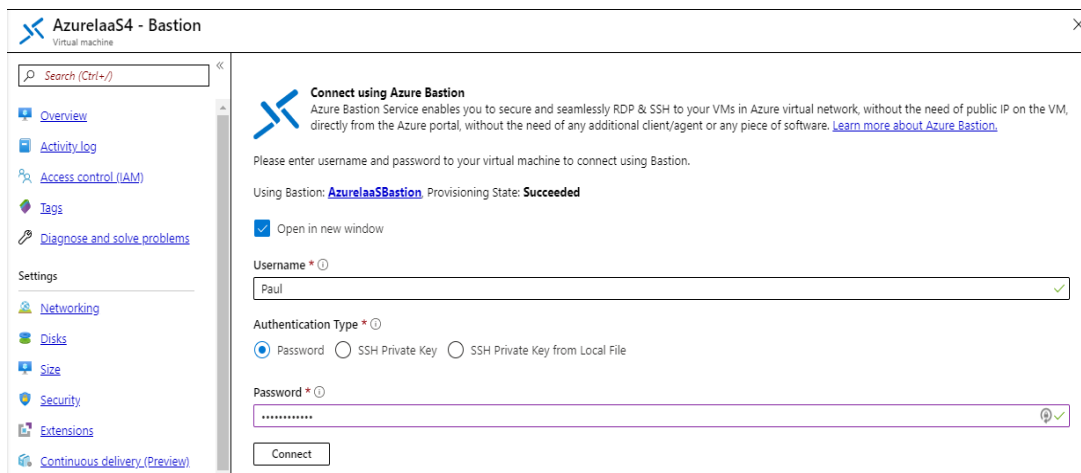
[Review + create](#) [Previous](#) [Next : Tags >](#) [Download a template for automation](#)

Create a Bastion

The creation will take a few minutes, then go to your IaaSVM5 and under Operations select Bastion.

Fill in your credentials and click Connect.

A separate browser tab will open and let you log in to the VM.



Connect to a VM using Bastion

## AZURE KEY VAULT

There's one place in Azure to securely store your tokens, passwords, certificates, API keys, encryption keys, and the like, and that's [Key Vault](#). Backed either by Hardware Security Modules (HSM) with the [Premium SKU](#) or software (Standard SKU), Key Vault lets you securely access secrets from [Windows](#) and [Linux](#) VMs. It also manages certificates and integrates with third-party Certificate Authorities (CAs) DigiCert and GlobalSign so that you can use KeyVault to generate new certificates and automatically renew existing ones. [Letsencrypt](#) certificates (free and just as good as the ones from commercial CAs) are available for [Azure Kubernetes Service \(AKS\)](#) with Application Gateway.

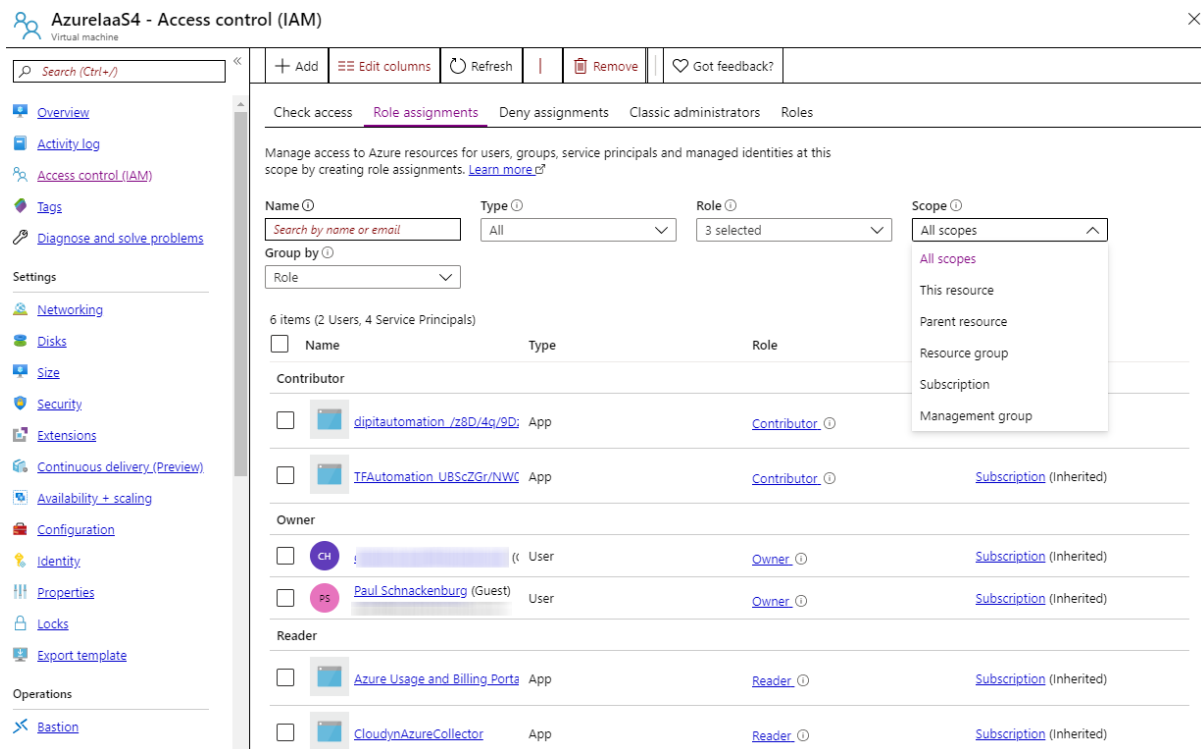
## DISK ENCRYPTION

One good way to protect your VMs in the cloud is to encrypt their disks. [Windows VMs use Bitlocker](#), [Linux uses DM-Crypt](#). Note that the first version of disk encryption stored the keys in AAD, the current version uses Key Vault. Take care when [backing up and restoring](#) encrypted VMs. [Server-side encryption with customer-managed keys](#) is currently in preview.

## ROLE-BASED ACCESS CONTROL

AAD was introduced in the last chapter. Here we'll look at the common Azure roles you'll want to apply to different people who are managing your VMs.

The basic RBAC principle is that there are three levels: Owner, Contributor and Reader. The first can make any change as well as assign permissions, whereas Contributor can make any change (including deleting) to a resource but not change its permissions, and Reader can see the configuration but not make any changes. These permissions can then be applied at a resource level (not a good idea, too hard to manage), RG level, Subscription level and Management Group level (all commonly used). VMs have other roles, such as VM Administrator Login and VM Administrator User Login, that are used when logging in with AAD credentials.



Assigning permissions to a VM

## AZURE FIREWALL

In chapter 1, we looked at NSGs and while they're a good software firewall, they are hard to manage at scale. Previously your only option was a third-party Network Virtual Appliance (NVA) firewall with the associated management of VMs etc.

[Azure Firewall](#) is an automatically scaling PaaS service that provides centralized control and lets you easily build hub and spoke vNet architectures. Recently Microsoft unveiled a unified management console, [Firewall Manager](#), for multiple deployments in different regions.

# CHAPTER 11 – AUTOMATION

In this chapter, we'll tie the previous chapters together. You've learned how to deploy single VMs and groups of VMs, how to lay the foundation with networking and picking the right storage for VMs, selecting the right type of VM, how to monitor them, using ARM to templatize your deployments, backup and protect your VMs data, use AAD for identity wisely, and how to implement the right security controls to protect them.

Here we're going to round out the IaaS story with Automation and Azure Advisor recommendations, which will give you the foundation to manage Azure IaaS VMs like an expert.

## AZURE AUTOMATION

[Azure Automation](#) gives you cloud-based configuration and automation across your on-premises, Azure, and [other cloud](#) resources. It lets you orchestrate processes using graphical, Python, or PowerShell [runbooks](#), collect inventory and track changes and configure desired state, and as we saw in the last chapter, manage your OS updates.

Add Automation Account

Name \* ⓘ

Subscription \*

Resource group \*

[Create new](#)

Location \*

Create Azure Run As account \* ⓘ  
☒ Yes ☐ No

*i*
This will create Azure Run As account in the Automation account which are useful for authenticating with Azure to manage Azure resources from Automation runbooks. Note that the creation of Azure Run As account may affect the security of the subscription. [Learn more](#)

*i*
[Learn more about Automation pricing.](#)

Create

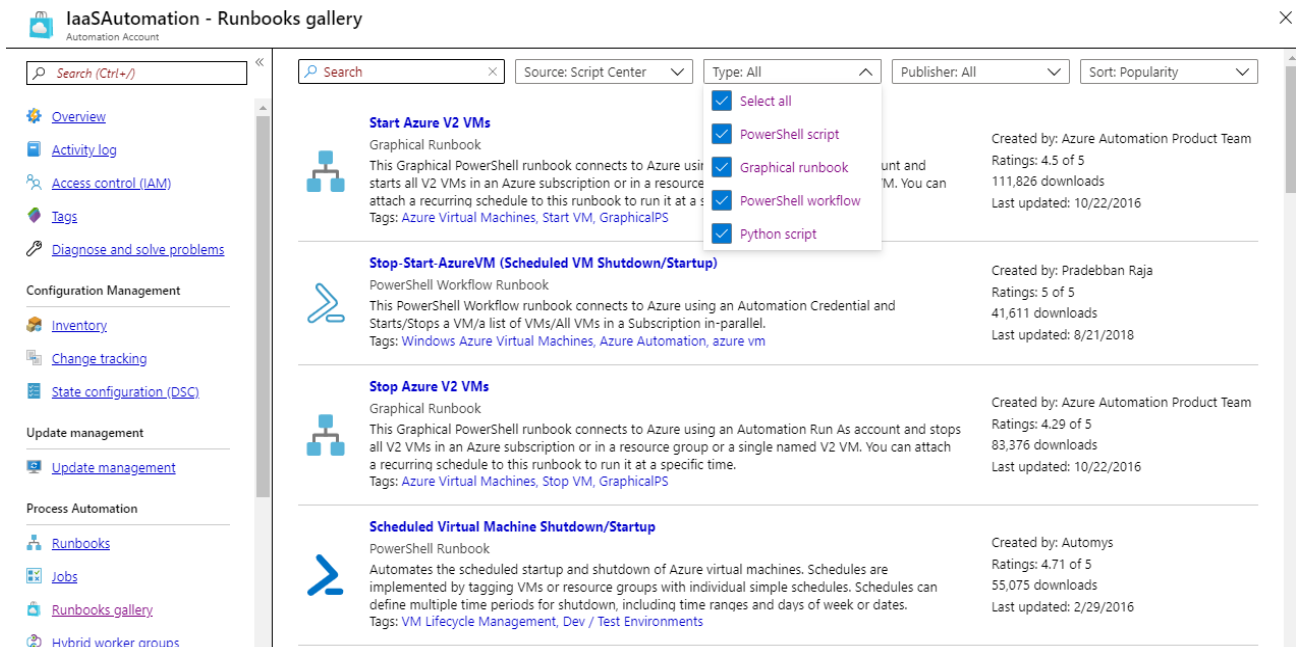
## Creating an Automation account

Search for Automation in the portal and click on Automation accounts – click Create.

Call your account IaaSAutomation, put it in the AzureIaaS RG, and leave the [Run As account](#) as Yes, click Create.

Once it's been deployed, go to it and click [Runbooks gallery](#) under Process Automation.

Here you can see a list of ready-made runbooks that you can customize. You can also filter based on the [type of runbook](#). You'll find runbooks to start and stop VMs (by tags if you'd like), find and delete orphaned disks, resize VMs and collect backup reports as examples.



## Automation Runbook Gallery

[Hybrid worker groups](#) let you set up agents on-premises or in other clouds to automate processes there.

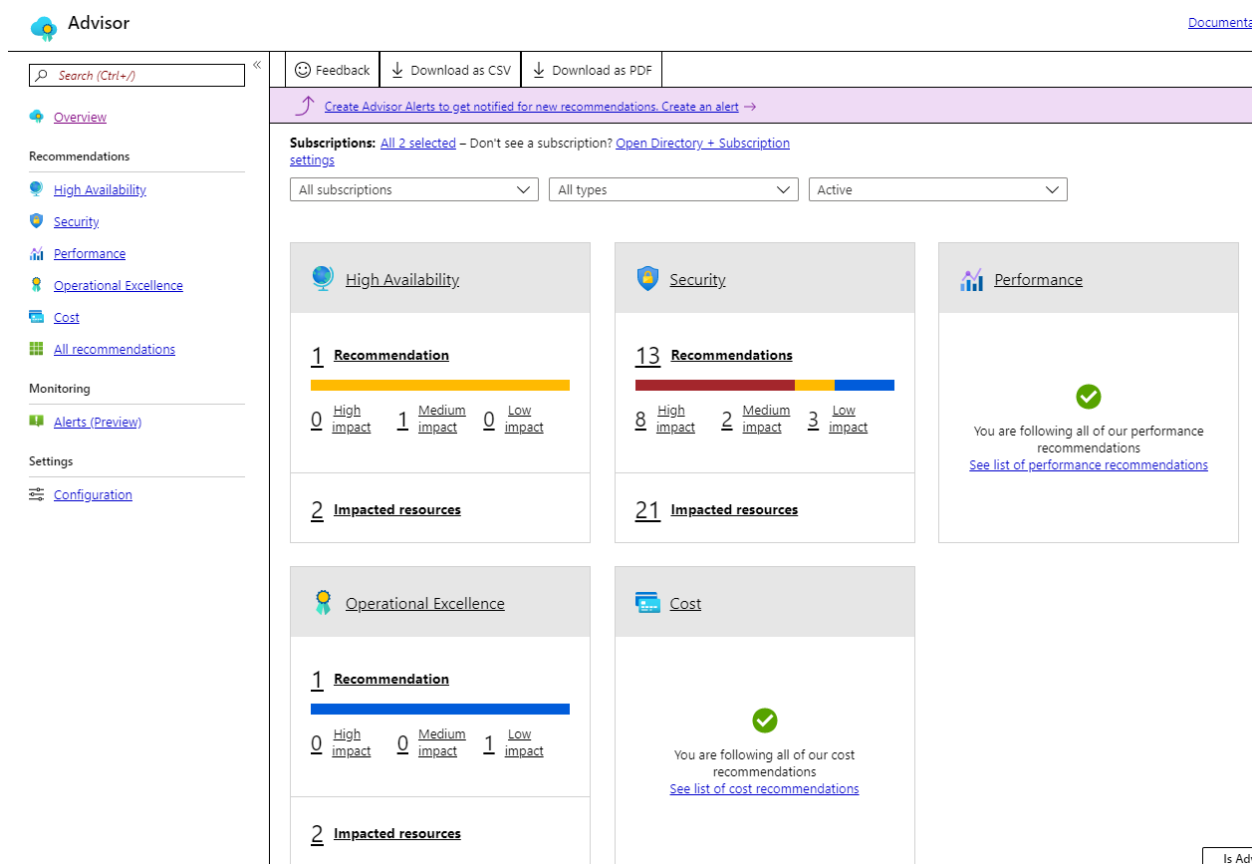
Schedules let you define custom timetables that you can then use for your runbooks, and [Credentials](#) lets you enter various secrets that can be used in Runbooks without revealing the passwords.

[Change Tracking and Inventory](#) keeps track of changes to files, registry entries, services, and Linux daemons in VMs to help you catch operational issues.

[State Configuration](#), on the other hand, uses PowerShell Desired State Configuration (DSC) to assign configurations to target nodes. If you're used to DSC, there's a built-in pull server that you don't have to manage, and Automation stores all your configurations, resources, and target node information across both Linux and Windows.

## AZURE ADVISOR

[Azure Advisor](#) is a customized (for your deployments) cloud consultant that gives you recommendations across [High Availability](#), [Security](#), [Performance](#), [Cost](#), and [Operational Excellence](#). Click on Advisor in the hamburger menu on the left, it's always there and doesn't need to be deployed.



Advisor dashboard

As a human cloud consultant, my advice is – take the recommendations from Advisor with a pinch of salt. Sometimes they're very useful and alert you to something you might have missed or a configuration that another administrator implemented with less than ideal results. But Azure changes very quickly, and sometimes the recommendations are misleading or incorrect. To stop having to remember to go to the Advisor blade, you can [set up alerts](#) to notify you of recommendations.

# CHAPTER 12 – BEYOND IAAS

The last 11 chapters have all focused on running and managing VMs in Azure – IaaS. This is comfortable territory for most IT Pros. After all, we've been virtualizing workloads on-premises for a long time and the paradigm is familiar. It also helps with lift-and-shift migrations to the cloud.

But Azure is SO much more than just IaaS and in fact, started as a PaaS platform (unlike AWS, which started as an IaaS platform). In this chapter, we're giving you a taste of what's beyond the familiar walls of the IaaS castle that you can apply to your business requirements. The main benefits you get from complementing IaaS with PaaS and SaaS services are cost-effectiveness (for example, Azure SQL is considerably more cost-effective than running your own SQL database in a VM and that's before you count the labor cost of managing yet another VM) and agility.

In fact, this book has already taught you many PaaS / SaaS services that help you run your VMs such as Azure Backup, vNets, Monitor, AAD, Bastion, NSGs / Firewall, and ASC as well as Automation. This chapter will show you a few more services that you can use to complement the applications in your VMs.

## AZURE SQL

There are [three basic flavors of SQL Server in Azure](#) – you can run it your own VM, which gives you full control but considerable management overhead (although Azure [helps with Backup](#) and [hybrid licensing](#)). Or you can use [Azure SQL Database](#), a fully managed platform where you don't have to worry about the VMs or backup at the [cost of some SQL compatibility](#). The scale is not an issue with the [Hyperscale SKU](#) which lets you go up to 100 TB databases with lightning-fast backups and restores, read-only replicas, and rapidly compute scale up and down. The third option is [SQL Managed Instance](#), which is a “real” SQL server running in VMs, but they're managed by Microsoft, with near 100% compatibility with your existing SQL Servers that you're migrating to Azure. So, if your application that you're migrating relies on SQL Server, investigate your options carefully, perhaps paying for that large VM to run 24/7 isn't the best option.

## COSMOS DB

If you need a global database that can have both reads and write replicas deployed in multiple regions with a mouse click and that can “talk” several different languages, [Cosmos DB](#) is your friend. It's got APIs for [SQL](#), [MongoDB](#), [Cassandra](#), [Tables](#), or [Gremlin](#). There are five options for [consistency levels](#); the tradeoff between how up to date each copy of the database is global versus the latency of writes to the database.

There are other data services such as [Data Explorer](#) (real-time analysis), [HDInsight](#) (Hadoop clusters as a service), [Data Lake](#) (combining file storage semantics with

Big data), [Stream Analytics](#) (process high volumes of fast streaming data), [Databricks](#) (Apache Spark-based analytics), [Synapse Analytics](#) (combining enterprise data warehouse with Big data analytics) and [Data Factory](#) (extract-transform-load, ETL as a service) that'll help you manage all types of data. Besides SQL and Cosmos, Azure has managed offerings of [MySQL](#), [PostgreSQL](#) and [MariaDB](#).

## WEB APPLICATIONS

If you have websites running on Apache or IIS, [App Service](#) is a good alternative to migrate to instead of running your own web server VMs. If you need an isolated environment look at [App Service Environment](#), and if your application publishes an interface, use [API Management](#). Additional web related services include [Content Delivery Networks \(CDN\)](#), [Media Services](#) for streaming video, and AI-powered [Cognitive Search](#).

## AZURE KUBERNETES SERVICE

You may have heard of an alternative to VMs, Containers. Unlike a VM which emulates a whole server with a motherboard, ports, virtual CPUs and memory, etc., a container is simply a “copy” of a running OS in a separate namespace. Linux pioneered containers and Windows has two flavors, including the more secure and isolated Hyper-V container flavor that Azure uses. If you're looking to write new applications for the cloud era, using containers and a microservices-based architecture is the way to go. The challenge of deploying and managing hundreds (or thousands) of containers across a cluster is solved by [Azure Kubernetes Service \(AKS\)](#).

# SERVERLESS

A flavor of PaaS services that's grown tremendously over the last few years is [serverless computing](#). A bit of a misnomer because of course there are servers underneath, [Azure Functions](#) lets you upload your code and have it trigger based on a schedule, or an event and scaling is taken care of for you by the platform whether that's one request per second or thousands and you only pay for exactly what you use.

# GOING FORWARD

This book has hopefully given you a good grounding in how to create, manage, and run VMs in Azure, and we trust you've found it useful. **Don't forget to delete the AzureIaaS RG so you don't waste your free credits.**

Learning the technical steps for creating VMs and associated services is a great first step for understanding Azure – beyond this is the fundamental change in how to “do IT” that comes with truly adopting a cloud mindset and DevOps (and DevSecOps) that's awaiting you and your team. We've already documented a wide range of resources in this eBook to make sure you never stop learning about Azure, however, if you want to receive helpful weekly content including best practices and tips on maximizing your Azure experience, [sign up to the Altaro Dojo newsletter](#).

I wish you success on your Azure journey!

# ABOUT THE AUTHOR



**Paul Schnackenburg** started in IT when DOS and 286 processors were the cutting edge. He works part time as an IT teacher at a Microsoft IT Academy. He also runs Expert IT Solutions, a small business IT consultancy on the Sunshine Coast, Australia. Paul writes in-depth technical articles, focused on Hyper-V, System Center, private and hybrid cloud and Office 365 and Azure public cloud technologies. He has MCSE, MCSA, MCT certifications. He can be reached at [paul@expertitsolutions.com.au](mailto:paul@expertitsolutions.com.au), follow his blog at TellITasITis, <http://tellitasitis.com.au>.

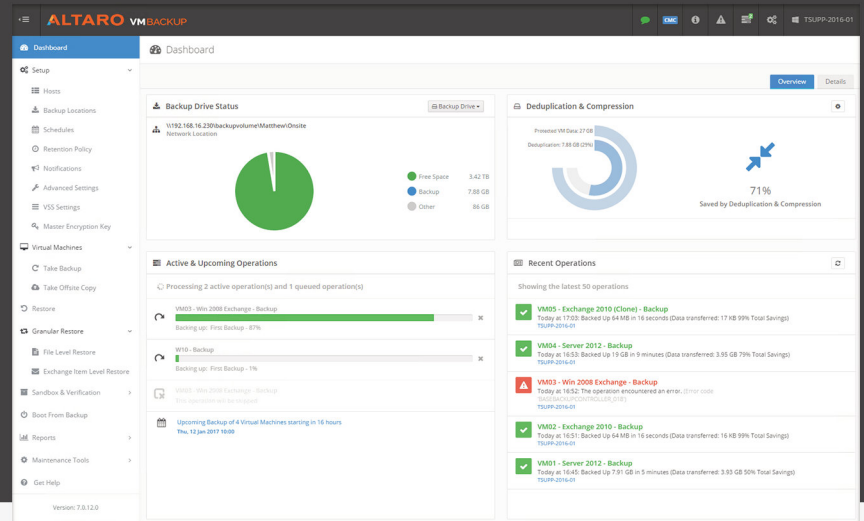
# Altaro VM Backup - Trusted by over 50,000 SMBs

Altaro VM Backup for VMware & Hyper-V is hassle-free and affordable virtual machine backup solution. Start your free trial today!

- ✓ Hassle-free and effective
- ✓ Unbeatable Value
- ✓ Outstanding Support

The free trial enables you to backup unlimited VMs for 30 days. Afterwards, you can continue to use the free version to backup 2 VMs per host, forever – our way of assisting micro businesses.

**Download your  
30-day trial**

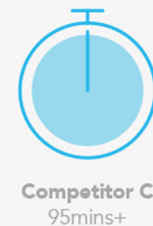
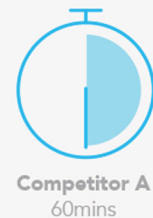
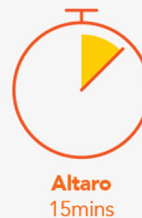


## Up and running quickly, without the need for complex configurations!

With Altaro VM Backup, you can install and run your first virtual machine (VM) backup in less than 15 minutes. Get up and running quickly, without the need for complex configurations or software dependencies.

Altaro VM Backup is designed to give you the power you need, without the hassle and steep learning curve.

- **Easy to use, intuitive UI** - making it easy to implement a rock solid backup strategy
- **Managing and configuring backup/restore jobs across multiple hosts has never been simpler**
- **Full control & scalability** - Monitor and manage all your Hyper-V and VMware hosts from a single console

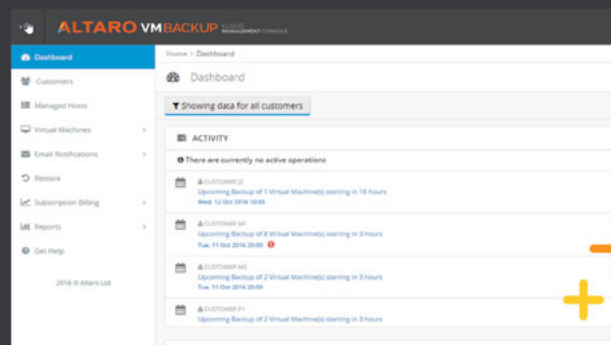


Virtual machine backup software packed with powerful features for **VMware** and **Hyper-V**.

**View features**

# ALTARO VM BACKUP for MSPs

**Altaro VM Backup for MSPs** is a subscription program that allows you to monitor and manage all your customers' virtual machine backups via a central online console.



## Multi-tenant

Monitor and manage all your customers through a single online console



## Real-time status update

View live operation activity and backup results as they occur



## Unbeatable value

Pay only \$5 per VM per month – the most accessible price in the industry



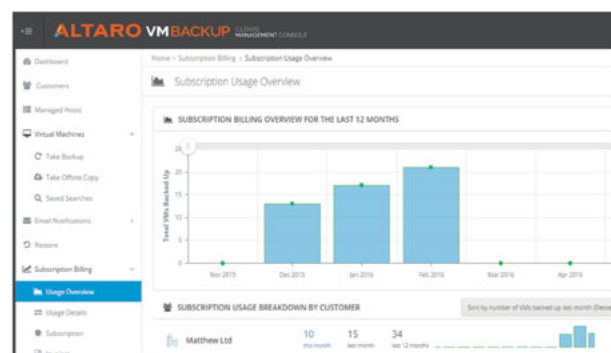
## Low commitment

Minimum of only 10VMs per month; You may stop at any time

Through the Altaro VM Backup for MSPs subscription program you can roll out the latest and most feature rich editions of Altaro VM Backup across all your customers with no upfront fees through a monthly subscription. All monitored and managed centrally through a ground breaking Cloud Management Console (CMC), making life easy and hassle-free.

## Benefits of the Altaro VM Backup for MSPs subscription program:

- **No upfront costs**
- **Pay based on usage** - Pay per VM per month, which means you pay only for what you use
- **Recurring revenue** - Charge your customers a **monthly recurring fee**
- **Central multi-tenant management** - Monitor and manage all your customer installations through a single online management console
- **'Best Support in the IT industry'** - 23 second average call pick up, LIVE chat, speak directly with an expert, no tier 1 agents or gatekeepers



Sign up for your 30-day trial  
[www.altaro.com/msp/](http://www.altaro.com/msp/)

## ABOUT ALTARO

Altaro Software is a fast-growing developer of easy-to-use backup solutions which backs up and restores both Hyper-V and VMware-based virtual machines, built specifically for MSPs and SMBs customers with up to 50 host servers. Altaro take pride in their software and their excellent level of personal customer service and support, and it shows. Founded in 2009, Altaro already services over 40,000 satisfied customers worldwide and are a Gold Microsoft Partner for Application Development and Technology Alliance VMware Partner.

### FOLLOW ALTARO

Like this eBook? **There's more!**



**HYPER-V**  
**D O J O**

[Subscribe to our Hyper-V blog](#) and receive best practices, tips, optimization guides and more!



**DOJO FORUMS** by **ALTARO**

Take your training to the next level on the Altaro Forums! Browse topics, read answers and contribute to this growing community of IT professionals.

[Check out the Altaro Dojo Forums](#)

**Follow Altaro at:**



### SHARE THIS RESOURCE!

Liked the eBook? **Share it now on:**



PUBLISHED BY ALTARO SOFTWARE

<http://www.altaro.com>

Copyright © 2020 by Altaro Software

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means without the prior written permission of the publisher or authors.

## WARNING AND DISCLAIMER

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

## FEEDBACK INFORMATION

We'd like to hear from you! If you have any comments about how we could improve the quality of this book, please don't hesitate to contact us by visiting [www.altaro.com](http://www.altaro.com) or sending an email to our Customer Service representative Sam Perry: [sam@altarosoftware.com](mailto:sam@altarosoftware.com)