Azure Infrastructure as a Service

THE SYSADMIN'S GUIDE

SECOND EDITION BY PAUL SCHNACKENBURG

HORNETSECURITY

ALTARO
Part of HORNETSECURITY group

DOJO

WELCOME

TO THE SECOND EDITION OF THE AZURE IAAS EBOOK...

AND THE ALTARO DOJO!

The DOJO is a dedicated training and educational platform updated every week with high-quality, value-packed content including articles, guides, and tips for M365, Azure and Hyper-V.

Register to the Altaro DOJO now to gain unrestricted access to all content and stay notified when new content is released – it's free to join!

- AUTOMATION
- AZURE
- BACKUP & DR
- CLOUD
- MANAGEMENT
- NETWORKING
- SECURITY
- STORAGE
- WINDOWS SERVER

BECOME A KICK-ASS SYSTEM ADMINISTRATOR – JOIN THE DOJO!

www.altaro.com/dojo

DOJO

THE SYSADMIN'S GUIDE TO AZURE INFRASTRUCTURE AS A SERVICE

2nd Edition by Paul Schnackenburg

PUBLISHED BY HORNETSECURITY / ALTARO

Copyright © 2022 Hornetsecurity

www.hornetsecurity.com/en

Production: Dunya Spiric

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 author. 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 author 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.

If you have any feedback about this book, its content, questions for the author, or any other feedback, please write to dojo@altaro.com.

HORNETSECURITY

Hornetsecurity is a leading email cloud security and backup provider, which secures the digital communication, business continuity, compliance, data and IT infrastructure of companies and organizations of all sizes.

Its award-winning product portfolio covers all important areas of email security, including spam and virus filters, legally compliant archiving and encryption, and protection against CEO fraud and ransomware; as well as backup, replication and recovery.

Its flagship product is the most extensive cloud security solution for Microsoft 365.

BUSINESS 365 TOTAL PROTECTION

With 365 Total Protection Suite , the seamlessly integrated security and compliance suite for Microsoft 365, Hornetsecurity delivers a comprehensive security package specifically for Microsoft 365 customers to protect their email communications and data in the cloud from the latest cyber threats.

FREE TRIAL

Office 365 Backup

Altaro Office 365 Backup enables you to back up and restore all your Microsoft/Office 365 mailboxes and files stored in OneDrive and SharePoint through an online console, on an annual subscription, allowing you to easily manage your backups. Data is backed up to Altaro's Microsoft Azure infrastructure. 24/7 support included.

FREE TRIAL

ABOUT THE AUTHOR

Paul Schnackenburg started in IT when DOS and 286 processors were the cutting edge. And as much as the IT industry has evolved since then, so has Paul's expertise. He teaches virtualization, networking and cloud technologies at a Microsoft IT Academy. He also runs Expert IT Solutions, a small business IT consultancy on the Sunshine Coast in Australia.

Paul is a well-respected technology author and active in the community, writes in-depth technical articles, focused on Microsoft 365, Azure public cloud, Hyper-V, System Center, and private and hybrid cloud technologies. He has MCSE, MCSA and MCT certifications.

Read more articles written by Paul on the Altaro DOJO:

www.altaro.com/dojo/author/paul-schnackenburg/

Or follow his blog:

tellitasitis.com.au

INTRODUCTION

The cloud computing era is well and truly upon us. 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 Pro.

It's a constantly changing environment.

One thing that has changed significantly over the past couple of years is the shift towards making IaaS VMs more like PaaS services. VMs are great but they require a lot of maintenance and care, whereas all the business is really interested in are the applications and data that run inside of them. This explains the popularity of PaaS services such as managed Kubernetes (AKS) and Azure Functions (serverless).

What you'll learn.

In this eBook, we're going to focus on Infrastructure as a Service (IaaS) on Microsoft's Azure platform; learn how to create VMs, size them correctly, and manage storage, networking, and security, along with backup. You'll also learn how to operate groups of VMs, deploy resources based on templates, manage security, and automate your infrastructure. And, if you have VMs in your own datacenter and are looking to migrate to Azure, we'll also teach you that, or how to manage them from the cloud without migrating them there.

If you're new to the cloud (or have experience with Amazon Web Services and/or Google Cloud Platform but not Azure) this book will cover the basics as well as 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 know how to proceed.

You'll benefit most from this book if you follow along with the tutorials, if you don't have access to an Azure subscription you can sign up for a trial here. This will give you 30 days to use $200 USD worth of Azure resources, along with 12 months of free resources. 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). There are also another 25 services that have free tiers "forever".

New to this edition.

If you've read the first edition, this second edition was updated in Dec 2021 and covers new features and updates throughout. All the step-by-step tutorials have been updated. Two new chapters, Automanage (Chapter 11) and Azure Arc (Chapter 12), have been added to bring a lot of automation to IaaS, all lessening the burden on your time.

Let's get started with Azure IaaS!

CONTENTS

About The Author 5

Introduction 6

Chapter 1 – Creating VMs 13

- Creating a VM in the portal 13
- Create a VM using PowerShell 17
- Create a VM using CLI 18
- VM Management 20
- VM Inspector 23
- Windows Server 2022 Datacenter: Azure Edition 23

Chapter 2 – Sizing VMs 25

- VM Series 25
- Virtual machines selector 28
- VM Performance 29

Chapter 3 – Storage 31

- SSD or HDD, Standard, Premium or Ultra 31
- Disk Considerations 33
- Uploading Virtual Disks 35
- File Shares 35
- A Gibibyte vs a Gigabyte 36

Chapter 4 – Networking 37
Keep your vNets close 37
Azure Network Manager 41
Speed 41
Network services 41
Hybrid Networking 43

Chapter 5 – Monitoring & Performance 46
VM Performance 46
Network Monitoring 48
Continuous Cloud Optimization Dashboard 49
Azure in your pocket 49
The Portal 50
Windows Admin Center 51

Chapter 6 – Behind the Scenes – ARM 52
Infrastructure as Code 52
Blueprints 54
Azure Policy 55
Tag – you're it! 56
Naming Standards 56
Management Groups 56
Resource Graph 57
Cloud Adoption Framework 59

Chapter 7 – Many VMs 60
Availability 60
Many VMs 61
Chaos Studio 64
Capacity Reservation 65
Sharing Images 65
Cost management 66

Chapter 8 – Backup & Replication 68
Backup 68
Restore Points 70
Replication 71
Altaro VM Backup 71
Migrate 71

Chapter 9 – Azure AD 73
Identity is the new firewall 73
Managed Identities 75
Azure AD Domain Services 75
Logging in with AAD accounts 76

Chapter 10 – Security 77
Microsoft Defender for Cloud 77
Patching 80
Bastion 80
Azure Key Vault 82
Disk Encryption 83
Role Based Access Control 83
Network Security Groups 84
Azure Firewall 85
Microsoft Sentinel 85
Confidential Computing 86

Chapter 11 – Automanage 87
IaaS vs PaaS 87
It's like Magic 87

Chapter 12 Azure Arc 90
Hybrid hardware 90
Hybrid Software 91
Arc for Servers 93

Chapter 13 – Automation 95
Azure Automation 95
Run Commands 98
VM Applications 98
Azure Lighthouse 99
Azure Advisor 99

Chapter 14 – Beyond IaaS 101
Azure Virtual Desktop 102
Azure SQL 102
Cosmos DB 103
Web applications 103
Azure Kubernetes Service 104
Serverless 104

Conclusion 105

Found This eBook Helpful? 106
Learn More About Azure 106
Explore Other eBooks 107

Secure Your Data 108

CHAPTER 1 – CREATING VMS

In this chapter we're going to look at different ways of creating VMs, using the web-based portal, PowerShell, and the cross-platform command-line interface (CLI). After this first chapter we'll move on to other topics such as the different VM sizes available (Chapter 2), Storage (Chapter 3) and Networking (Chapter 4).

Login at 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 step through the wizard that comes up. First, you must create a Resource Group (RG), call it Azure IaaS. An 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). 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. Learn more

Project details

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

Subscription * : MSDN Platforms

Resource group * : (New) AzureIaaS
Create new

Instance details

Virtual machine name * : AzureIaaS1

Region * : (US) East US

Availability options : No infrastructure redundancy required

Security type : Standard

Image * : Windows Server 2022 Datacenter: Azure Edition - Gen2
See all images | Configure VM generation

Azure Spot instance : ☐

First step to create a VM

Give your VM a name, **AzureIaaSVM1**, pick the East US region, and select the Windows Server 2022 Datacenter: Azure Edition – Gen2 image. The suggested size will most likely be a Standard D series which will be fine for this first walkthrough. Define an administrator account username (note that 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 (for learning purposes), we're going to allow RDP (3389) access from the internet, which is a pretty obvious security no-no. However, we'll be discussing ways to avoid this security headache later 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.

Creating a VM - Management

On the Management step of the wizard enable Azure Security Center and leave all other options as default, do the same on the Advanced step and ditto 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. 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 login. Pro tip – if you're new to Azure you might think that shutting down the VM from within the OS will stop the running cost accruing in Azure – not so, as this shutdown isn't something Azure is aware of. To stop paying for 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

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, it makes sense to use PowerShell, while the 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. Or 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 CloudShell using shell.azure.com, which will give you a full browser experience window or you can click the button (>_) in the top right of the portal, which will give you a smaller shell at the bottom of the browser window.

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

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

```
PS /home/paul> New-AzVm -ResourceGroupName "AzureIaaS" -Name "AzureIaaSVM2" -Location "East US" -virtualNetworkName "AzureIaaSvnet" -Subnet
Name "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: pauls
Password for user pauls: ***************

No Size value has been provided. The VM will be created with the default size Standard_D2s_v3.


ResourceGroupName        : AzureIaaS
Id                       :
/subscriptions/[redacted]resourceGroups/AzureIaaS/providers/Microsoft.Compute/virtualMachines/AzureIaaSVM2
VmId                     : 7c13e527-4a0e-4d8c-9872-b4930229069e
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 : azureiaasvm2-7d6b95.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 and vNet / Subnet as the first one we created. 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 between CLI and PowerShell in the top left of the browser. If you want to run the CLI on your local PC it's available for Windows, macOS, and 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 win2022datacenter --admin-username YourAdminName
--admin-password YourGoodPassword
```

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

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

paul@Azure:~$ az vm create --resource-group AzureIaaS --name AzureIaaSVM3 --image win2022datacenter --admin-username PaulS --admin-password
 GvGgs7NVHnu2kdK-
It is recommended to use parameter "--public-ip-sku Standard" to create new VM with Standard public IP. Please note that the default public
 IP used for VM creation will be changed from Basic to Standard in the future.
{
  "fqdns": "",
  "id": "/subscriptions/[redacted]/resourceGroups/AzureIaaS/providers/Microsoft.Compute/virtualMachines/AzureIaaS
VM3",
  "location": "eastus",
  "macAddress": "00-0D-3A-14-B3-EC",
  "powerState": "VM running",
  "privateIpAddress": "192.168.1.5",
  "publicIpAddress": "20.127.132.215",
  "resourceGroup": "AzureIaaS",
  "zones": ""
}
paul@Azure:~$
```

Creating a VM in the CLI

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 **Deploy a simple Windows VM template**.

Deploy a simple Windows VM

by Brian Moore
Last updated: 12/13/2021

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 an 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.
publicIpName	Name for the Public IP used to access the Virtual Machine.
publicIPAllocationMethod	Allocation method for the Public IP used to access the Virtual Machine.
publicIpSku	SKU for the Public IP used to access the Virtual Machine.
OSVersion	The Windows version for the VM. This will pick a fully patched Gen2 image of this given Windows version.
vmSize	Size of the virtual machine.

Creating a VM from a template.png

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, such as admin username and password, and the name of the VM (**AzureIaaSVM4**). Agree to the terms and conditions and click the Purchase button to deploy your fourth VM.

VM MANAGEMENT

Pick one of the VMs and click on its name. The overview page will show you basic settings. If you click the Networking link in the left-hand menu it'll show you the port rules in the Network Security Group and gives you the option to add additional network interfaces to the VM. 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 NSG rules will apply.

Windows Admin Center, currently in preview, is a free web-based tool that's been available to manage Windows Servers on premises for a few years now and is now available as a blade in the Azure portal. It makes it easy to manage a fleet of Windows IaaS servers in Azure.

The Disks interface lets you add data disks to your VMs, whereas the Size link lets you resize your VM. Note that this will require a restart if it's running so schedule this during non-business hours. The Security link gives you alerts and recommendations but it's better to use Defender for Cloud (Chapter 10) to handle this across all your resources than managing it on an individual VM basis.

Extensions are interesting and allow you to add 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.

The configuration link lets you enable Just-in-time access which protects RDP, SSH or WinRM access to your VMs through those ports being closed normally. When you need to administer the VM, you login 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. 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. If your application has low latency requirements, consider proximity placement groups and perhaps accelerated networking. Host groups are used for scenarios where you have to follow a regulation that prevents you from running VMs alongside VMs from other businesses, so you have a Dedicated Host exclusive to you.

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.

Guest + Host updates help you configure Update management for Windows and Linux server OS regular patching (see chapter 10). It also allows you to see if there is any upcoming planned maintenance for the Hyper-V hosts underneath your VM, giving you about 35 days to pick when the maintenance works for you.

Configuration management is another interesting preview that lets you manage settings inside your VMs OS using Desired State Configuration (DSC) management.

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. 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 boot process use the Serial console for Windows and Linux. If you've forgotten the administrator password you can use Reset password. Connection troubleshoot helps you figure out why you can't connect to the VM if it's caused by NSG rule misconfiguration. 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.

VM INSPECTOR

If the issue is with the OS inside your VM, there's a tool in preview called VM Inspector that collects event logs, configuration, settings and registry keys from Windows and Linux VM's OS disk and outputs them as a zip file to a storage account.

WINDOWS SERVER 2022 DATACENTER: AZURE EDITION

Throughout this book we pick the Windows Server 2022 Datacenter: Azure Edition as it's the first version of Server that unlocks special features when it runs in Azure (or on Azure Stack HCI – chapter 12). It lets you create a "no user action" VPN from Windows 11 and Android to a Windows Server 2022 Datacenter: Azure Edition file share using SMB over QUIC, securely connected over TLS 1.3. This edition also supports hotpatching, the ability to update the OS without having to restart the server (on Server Core only, Server with a UI doesn't yet have it).

NOTE: If you'd like to see SMB over QUIC in action, we have a live demo of it in this webinar.

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 Azure IaaS 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-premise, you're used to being able to choose exactly the number of virtual CPU cores and memory for a new VM, along with (maybe) choosing between different backend storage arrays and their associated speeds.

VM SERIES

In contrast 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. It 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 so is appropriate for test / dev workloads but not production. Each series also comes in versions as the underlying fabric is upgraded, designated by a "**v**" number such as v4. 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.

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 grunt. 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 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 Dasv4 series (running on the AMD EPYC™ 7452 processor) and the Dasv5 (on the EPYC™ 7763v processor).

For workloads requiring a higher ratio of memory to CPU look at the Ev4 and Ev5 (and Easv5 on AMD) 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 Lsv2 series, because you won't want to pay too much for the database software licensing when you pay per core, however, for workloads that require a LOT of memory but fewer cores, look at core constrained VMs.

Next up, If you're doing High Performance compute (clusters of nodes crunching large datasets) look to the HBv3, HC and H series VMs; they come with either 100 or 200 Gbps networking. And 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. Azure offers 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).

Finally, 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 (see more about Confidential Computing in chapter 10).

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 is broken 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).

VIRTUAL MACHINES SELECTOR

If it feels like there are WAY too many choices of VMs, you're not alone. Azure offers a web-based tool, the Virtual machines selector, to help you pick the right VM for the job by answering a series of questions.

Virtual machines selector in action

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 should be 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 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 cautious and have deep pockets) 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's first crack at isolated hosts, the next iteration is 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 (Gen 2). The support for Gen 2 features has been steadily increasing since 2019. It now includes Trusted Launch which builds on

Secure Boot and includes virtual TPM for storing secrets along with Virtualization-based security (VBS). These features enable Hypervisor Code Integrity (HVCI) and Windows Defender Credential Guard which protect against credential theft attacks like Pass-the-Hash (PtH). Trusted Launch also integrates with Microsoft Defender for Cloud (chapter 10).

For the right scenarios, particularly for specific compliance regulations or for very security-sensitive workloads, investigate carefully if Trusted Launch features will fulfill the requirements, or if Confidential Computing (chapter 10) is a better solution.

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 an especially 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) is remote to your VMs and sits 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 hard drive 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. Premium and Standard SSD disks smaller than 512 GiB support credit-based bursting, where it accrues credits when it's not being used at full speed, and then can use those credits to temporarily increase the performance when a spike of disk activity occurs, at no extra costs. Premium SSDs larger than 512 GiB on the other hand offer on-demand bursting which does incur additional charges. If you have IO heavy workloads it pays (literally) to pay attention to disk performance. If you enable on-demand bursting and the disk is using bursting a lot, it will be more cost effective to change the performance tier of the disk instead.

You can use Storage Spaces in Windows and software RAID in Linux to combine multiple data disks for increased performance. Remember in both cases that 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, only for speed. This detailed 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 as different VM sizes have overall limits on the maximum IOPS they will support. Smaller VMs for instance such as a B1s only supports up to 3200 IOPS whereas a D16s_v3 tops out at 25600 IOPS, even if you connect faster disks to them.

DISK CONSIDERATIONS

One difference to consider 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. However, there are so many benefits to managed disks. 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.

VM Images with small OS disks

Each VM is automatically provisioned with a temporary D: drive (/dev/sdb for Linux machines) which is located on the local host 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 learnt 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 changing the drive letters). Since you pay for each size increment, start as small as you can.

Currently in preview is the ability to resize managed disks while the VM is running.

Azure also supports shared disks for guest clustering scenarios. Imagine several VMs running SQL Server, all working from a single, shared, managed disk. You can even have copies of the shared disk be distributed across Availability Zones with ZRS support.

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.

FILE SHARES

The most common workload for a Windows server on-premises is as a file server. So, you might imagine that just lifting and shifting those VMs to Azure is the solution for offering those files to VMs in Azure. A better solution is Azure Files, part of Azure storage. Think of this as a managed file share where you don't have to worry about managing the underlying server. Also, you can use Azure

File Sync to connect your file servers on-premises to Azure and automatically sync older files to the cloud to effectively make your file servers "bottomless".

Azure storage can now also be accessed over Secure File Transfer Protocol (SFTP).

A GIBIBYTE VS A GIGABYTE

When reading Microsoft documentation, you'll come across newer terms to measure size such as Mebibyte (MiB), Gibibyte (GiB) and Tebibyte (TiB) which are 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 are fond of is why your brand new 4 TB drive 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. 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). It can also give you performance metrics for Content Delivery Networks (CDN), file transfers and region-to-region latency.

Closest Datacenters

Region	Average Latency (ms)
Australia Central (Canberra)	101 ms
Australia East (New South Wales)	123 ms
Australia Southeast (Victoria)	130 ms

Latency Test

Geography	Region	Physical Location	Average Latency (ms)
Asia Pacific	Australia Central	Canberra	101 ms
Asia Pacific	Australia East	New South Wales	123 ms
Asia Pacific	Australia Southeast	Victoria	130 ms
Asia Pacific	Central India	Pune	190 ms
Asia Pacific	East Asia	Hong Kong	168 ms
Asia Pacific	Japan East	Tokyo, Saitama	175 ms

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 search for Virtual network (it used to be at the top of the list but now it doesn't even show up). Give it the name **vnet-AzureIaaSVnet** and note how it picks an address space that gives you 65,536 addresses, the maximum amount a vNet can have. 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 **rg-AzureIaaS** (you did delete the RG we created in Chapter 1, right?). Each vNet can be divided into subnets (one called default will be created for you), create one more subnet – call it **snet-Production** with the address space 10.0.1.0/24. Then delete the default subnet.

Creating a Virtual Network

Support for IPv6 is improving in Azure and you can use 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). Only enable Standard DDoS if you really need, it's quite expensive. Leave Service endpoints, BastionHost 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 **snet-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** (see Hybrid networking below).

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 contain workloads. You can easily connect ("peer") vNets together, both in the same region and across regions.

AZURE NETWORK MANAGER

Currently in preview is a new way of managing connectivity and security for vNets at scale. Some Azure customers end up with 100's or 1000's of vNets and managing them individually becomes a big overhead. Azure Virtual Network Manager (AVNM or ANM) lets you manually or dynamically (based on rules) include vNets into network groups. These can span subscriptions and Management groups. Then you can apply connectivity configurations that define how each vNet should be peered with the others (hub-spoke or mesh) and security configurations that add NSG rules *that can't be altered by resource owners*, finally giving the security team centralized control over traffic flow.

SPEED

Azure utilizes Field Programmable Gate Arrays (FPGAs) as network interfaces, offering speeds from 40 Gbps to 100 Gbps. If you need lightning fast VM to VM networking with low latency, make sure you pick the right VM series that supports the speed you need. The FPGAs can also be accessed to perform other work such as Machine Learning.

If you need to figure out the latency between two endpoints, use the right tools.

NETWORK SERVICES

Azure Private Link is the newer way to access PaaS services (Azure Storage and SQL Database for example) over a private endpoint in your virtual network.

This service also enables you to access third party partner services securely and publish your own services to other companies. Not all services fully support Private Link today but it's the best way to not access PaaS services over the public internet. Azure's original solution to this problem, 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. There are subtle differences between the two solutions, but in general Private Link is the preferred option.

If you need to capture all VM network traffic for security inspection or forensics, be aware that the vNet TAP service that was in preview is currently "on hold".

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. There's also DNS private zones which is a managed DNS solution where you have complete control over the records for your vNet(s), without the overhead of running your own DNS servers. Use this article to ensure you design the right DNS solution for your IaaS workloads. On the other hand, if you need public DNS services, consider Azure DNS.

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 have a large, multi-region service the evolution of Traffic Manager is Front Door which provides TLS termination (SSL Offload) and many other features.There's a new Premium version in preview.

If you need load balancing Azure provides one as a 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 (layer 4). For SSL termination or application layer processing (layer 7) 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 with the OWASP based Core rule sets 3.2, 3.1, 3.0 and 2.2.9.

If these last paragraphs were a bit overwhelming and left you wondering – which one should I use – use this article and the flow chart in it to narrow down exactly which one will suit your scenario best.

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 and 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 a 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. If you're adopting Azure Virtual Desktop your on-premises users can now connect to it over ExpressRoute.

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 on the other hand you want your BGP routes that you use on-premises to be propagated into Azure and vice versa, consider using Azure Route Server.

If you have Windows Server 2019 / 2022 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 **vm-IaaSVM5**, 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, **vm-IaaSVM5**). That screen will show you key metrics such as CPU, Network and Disk statistics for the last couple of hours (up to 30 days).

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 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) and then an Action group where you can set up email, SMS, Voice or Azure app Push Notifications (see below) or set up emails that go to a specific Azure RBAC role. You can also enable the common alert schema which brings the alerts across Azure into unison. In the past they all had their own set up and configuration.

Creating a performance alert for a VM

On the Action tab you can configure several Actions to take such as Automation Runbooks, Azure Functions, ITSM (connect to Service Now, System Center Service Manager, Provance and Cherwell), Logic App, Secure Webhook or Event Hub. This provides a comprehensive way to integrate alerts from Azure IaaS into your favorite monitoring platform.

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 setup an alert are actually provided by 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 etc.

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. Also make sure to follow @azurestatus on Twitter. 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.

NETWORK MONITORING

Network Performance Monitor is now retired (you can't create any new tests; existing ones will keep working until 29 February 2024). Instead use Connection Monitor as part of Network Watcher to keep an eye on performance across your hybrid infrastructure. It'll show you loss, latency, response time and bandwidth usage between your different locations and build a topology map to show you how everything is connected. Network Insights is in Monitor and provides a dashboard that shows topology, dependencies, and health for all your network nodes.

CONTINUOUS CLOUD OPTIMIZATION DASHBOARD

An alternate way to visualize your environment at scale is the free Continuous Cloud Optimization Azure Infrastructure Power BI Dashboard which gathers data from your Azure subscription(s) and displays it in a dashboard that you can customize to suit your needs.

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 cursor over a resource, a card appears where you can take actions on it (for a VM, start, stop etc.) and see more information about it. The settings gear (⚙) lets you choose 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. It also lets you set language and region settings, as well as swap between Azure AD tenants and subscriptions.

Portal Settings

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 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).

WINDOWS ADMIN CENTER

As mentioned, you can use Windows Admin Center (WAC) directly in the Azure portal. This web-based UI for managing Windows Servers at scale has gone from strength to strength over the last few years and has a particularly strong hybrid story where you can create Azure VMs, set up backup of on-premises VMs to Azure, configure Azure Site Recovery for Disaster Recovery etc.

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 artefacts) that define your servers, databases, networking, and storage etc. treated just like application code written by developers – Infrastructure as Code. Store it centrally in a code repository (like GitHub) 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 / 2013 fully configured** 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 Java Script 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 CLI. If you've ever done that manually this will give you an indication of 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!).

Since the first edition of this book, there's been a realization at Microsoft that not every IT Pro is comfortable with the complex nature of JSON ARM code. The solution is Bicep (Arm – Bicep – get it?), an intermediate language that lets you write and edit templates easier and then when you deploy them they're transcribed into ARM code that Azure understands. The current 0.4 version is feature comparable to ARM and is supported by Azure support.

Looking beyond ARM and Azure there are several other approaches to Infrastructure as Code, one is Terraform by Hashicorp, which works in Azure, GCP and AWS.

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 assignments (see below) 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 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.

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.

NAMING STANDARDS

If there's one single thing that's most important for you to do after reading this book, it's to define an Azure naming standard for your organization. The importance of spending a few hours nailing down an internal document will save many, many hours down the track as you're trying to figure out why there's a BobServer VM, and a BobServer2 VM when there's no IT person called Bob, or maybe a TestVM in production. Microsoft has a good starting point, and we've been using the standard throughout most of the tutorials in this book.

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 organization 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 company-wide 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 explore 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.

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 **vm-IaaSVM5** and see the separate components, such as a NIC, and disks that make up a VM. Resource Explorer is particularly handy if you've been handed an Azure deployment that's not documented and you're trying to figure out what resources there are and how it's structured.

Resource Explorer

CLOUD ADOPTION FRAMEWORK

Adopting cloud is more than just the technical aspects and Azure has comprehensive guidance in the form of the Cloud Adoption Framework which comes with best practices, documentation, and tools to align business and technology strategies as you move to the cloud.

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 a 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, use Availability Zones (AZs). Each Azure region is (generally speaking) not a single datacenter but several buildings, with independent power, cooling and networking infrastructure providing redundancy for services that are AZ aware. In the 23 regions that are AZ enabled (there were 10 when the first edition eBook was written) 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. There are now two versions of VM Scale Sets, the older version is called Uniform orchestration mode. The new version, called Flexible orchestration ("Flex") is the recommended option going forward, think of it as the best of Availability Sets combined with the best of the old Scale Sets. It supports 1000 VMs compared to 100 in the old model, it supports all Azure VM sizes, you can associate an existing VM with a VMSS and most importantly, you manage the VMs exactly like you manage single VMs. There's no special way to interact with them. Here's a detailed comparison.

Creating a virtual machine scale set

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 **vm-IaaSSS**, pick Windows Server 2022 Datacenter: Azure Edition, put it in the rg-AzureIaaS and select all three zones under AZ. Enter a username and password, and change the VM size to Standard_B2s (less costly than the D series it defaults to). Set the initial instance count to 3 and scaling policy to Custom to see all the different options you have for controlling how many VMs your VMSS will scale up and down to.

Set Scaling Policy for a VM Scale Set

This is the power of the cloud, with just a few clicks you just created a highly-available (HA), load balanced set of three VMs, spread across three datacenters.

Let's look at some of the options that we left at default when we created our VMSS, such as Spot VMs, which takes advantage of the spare capacity in certain 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. New here is the ability to test your application's resiliency by simulating VMs being evicted and also a new API call to try to restore an evicted VM.

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.

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.

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

CHAOS STUDIO

Released in preview late 2021 is Azure Chaos studio. Pioneered by Netflix, Chaos engineering is the concept of having automated tests randomly turning off or introducing latency into your infrastructure / applications to ensure that resiliency to real world issues is really built into your architecture.

It lets you create experiments with many different options such as shutting down VMs or VMSS, adding CPU / memory or disk pressure, DNS failures or killing services.

Chaos Studio experiment designer

Note that specific RBAC permissions are required to create an experiment and resources must be opted in to participate in one, as well as have the right permissions. And there's a big stop button to halt an experiment if it goes wrong.

If you're architecting a medium or large-scale business application in Azure and you want to ensure that all the HA features that we're looking at in this chapter are actually going to work as expected, take Chaos Studio for a spin (it's lots of fun!).

CAPACITY RESERVATION

An interesting facet of cloud computing, elasticity, the ability to have compute capacity "on tap" when you need it, was tested early in the Covid pandemic when certain regions in Azure simply ran out of capacity. A new feature, Capacity Reservation (currently in preview) lets you reserve capacity, perhaps because you know you've got a heavy workload coming up next week (Black Friday) or because you want to ensure that capacity is available in a replication region for disaster recovery.

SHARING IMAGES

As your estate in Azure grows you're eventually going to need to manage images company wide and Azure Compute Gallery (formerly Shared Image Gallery) is the solution for this. It lets you version and group VM images and store them in a HA way in Zone Redundant Storage (ZRS), replicate them between regions and share 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 gallery functionality, just 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 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. Azure reservations has also expanded to many 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 Subscriptions, this'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. Here you can also set alerts on spending and create budgets to manage spending by different 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, **vm-IaaSVM5** (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 **Edit this policy** under the suggested backup policy and set your backup frequency and retention period (up to 99 years for the yearly points), then click Enable Backup.

Create policy

Azure Virtual Machine

Policy name: DailyPolicy-AltaroIaaS

Backup schedule

Frequency *: Daily | Time *: 8:00 PM | Timezone *: (UTC+10:00) Brisbane

Instant Restore

Retain instant recovery snapshot(s) for: 2 Day(s)

Retention range

Retention of daily backup point

At: 8:00 PM | For: 30 Day(s)

Retention of weekly backup point

Not Configured

Retention of monthly backup point

Week Based / Day Based

On *: First | Day *: Sunday | At: 8:00 PM | For: 60 Month(s)

Retention of yearly backup point

Week Based / Day Based

In *: January | On *: First | Day *: Sunday | At: 8:00 PM | For: 10 Year(s)

OK

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 that you can restore individual files and folders, as well as whole VMs. On top of that SQL Server running in a VM is easily protected as well! In terms of deleting backups, several steps are required to ensure that, should a ransomware event occur, the 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. Note that when you do delete backups, they're still kept (14 days) in case you change your mind.

RESTORE POINTS

If you're used to virtualization platforms on-premises you're probably thinking – what about checkpoints? They're not proper backups but they're a handy way to being able to "go back in time" quickly, such as when an OS or application patch proves to be bad. Azure recently announced multi-disk consistent restore points, which expands the existing support for incremental disk snapshots.

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
1	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)
2	ESDC01AD02	Ready For Azure	NotApplicable	Standard_F4s	57.39	17.92	Microsoft Windows Server 2016 (64-bit)	2	4096	0.85	6.85	100
3	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
4	EAAWIN7	Ready For Azure With Conditions	WindowsClientVersionsConditionally Supported	Standard_F4s	57.39	17.92	Microsoft Windows 7 (64-bit)	2	4096	2.95	6.99	100
5	ESDC01AD01	Ready For Azure	NotApplicable	Standard_F4s	57.39	17.92	Microsoft Windows Server 2016 (64-bit)	2	4096	0.95	7.99	100
6	EAASQL01	Ready For Azure	NotApplicable	Standard_DS4_v2	117.33	253.44	Microsoft Windows Server 2016 (64-bit)	4	16384	3.18	6.79	1636
7	ESDC01NS01	Ready For Azure With Conditions	UnendorsedLinuxDistributions	Standard_F4s_v2	45.25	4.8	Oracle Solaris 10 (64-bit)	2	2048	53.89	6.65	20
8	ESDC01FP01	Ready For Azure	NotApplicable	Standard_F16s	229.58	271.36	Microsoft Windows Server 2016 (64-bit)	4	8192	2.18	10.92	2248
9	ESDC01CTXDC01	Ready For Azure	NotApplicable	Standard_DS3_v2	59	17.92	Microsoft Windows Server 2012 (64-bit)	2	8192	4.24	18.23	100
10												

Azure Migrate Assessment Report

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. It gives you the full power of VMware together with integration with 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 / 2022. It lets you move file servers from one server to another. Originally positioned as an "help you upgrade" tool to go from earlier Windows Server versions to Windows Server 2019 / 2022, 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 Microsoft 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, part of M365 E3/E5) 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. If you're not going to use PIM, at least make sure every single administrator has to use MFA to sign in to Azure. Preferably every user in your tenant should be required to use MFA. , It stops 99.9% of all identity-based attacks, and consider moving beyond MFA to passwordless.

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 synched to AAD is a real time saver.

Make sure you create at least one, preferably two Global Admin accounts that are exempt from ALL Conditional Access policies and MFA. Give these accounts REALLY long and secure passwords and store them securely. These break glass accounts are only to be used in emergencies if MFA is down in Azure for instance.

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 a 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).

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; 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 synched with your on-premises AD with AAD Connect). If you do decide to put DCs in Azure, make sure you protect them accordingly.

If you'd like to Learn more about Azure AD, we've got a fantastic webinar on the topic here!

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 RDP to Windows (Server 2019+ and Windows 10). For Linux the new solution uses OpenSSH certificate-based authentication. It integrates with AAD Multi Factor Authentication (MFA), Conditional Access and you can use Role Based Access Control (RBAC) to assign permissions to VMs.

CHAPTER 10 – SECURITY

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

MICROSOFT DEFENDER FOR CLOUD

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.

Microsoft Defender for Cloud 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 regulation compliance. The IT buzzword for this is Cloud Security Posture Management (CSPM). 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. The CSPM parts of Defender for Cloud (showing you where your configuration is weak) is free, but when you want to actively protect your workloads (VMs and PaaS services) you enable

Enhanced Security features which incur costs (after a 30 day trial). You should definitely turn on the enhanced security features for any production workloads in Azure, especially as Defender for Cloud can now also show and protect workloads in AWS and GCP.

Defender for Cloud 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, which blocks 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. Allow listing 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 further harden the rules. All three of these security measures apply to both Linux and Windows VMs.

Most importantly, if you enable Enhanced security features for servers (Windows and Linux) you are automatically licensed for Defender for Endpoint. This is Microsoft's full-fledged Endpoint Detection and Response (EDR) and

endpoint protection solution for Windows, Linux, MacOS, iOS and Android. It also offers Threat and Vulnerability management and identifies all installed software and gives you a prioritized list of applications to upgrade to fix vulnerable versions.

Defender for Endpoint Threat and Vulnerability Management dashboard

PATCHING

Software updates is part of Automation (Chapter 13) 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. Set up alerts so you're notified when things are working and when they're not. It also integrates with Microsoft Endpoint Configuration Manager 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, to your VMs.
It 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. New in Bastion is the ability to manage VMs in peered vNets.

To create a Bastion, start by going to your vNet (for the vm-IaaSVM5) and create a new subnet called **AzureBastionSubnet** (must have exactly that name) with at least a /27 space. Do a search in the portal for Bastions and click Create a Bastion. Call it **bas-AzureIaaS**, put it in the rg-AzureIaaS RG and leave all other configurations as default.

Create a Bastion ...

Project details

Subscription * MSDN Platforms

Resource group * rg-AzureIaaS
Create new

Instance details

Name * bas-AzureIaaS

Region * Australia East

Tier * Standard

Instance count * 2

Configure virtual networks

Virtual network * vnet-AzureIaaS
Create new

Subnet * AzureBastionSubnet (10.0.3.0/24)
Manage subnet configuration

Public IP address

Public IP address * Create new / Use existing

Public IP address name * vnet-AzureIaaS-ip

Public IP address SKU Standard

Assignment Dynamic / Static

Review + create | Previous | Next : Tags > | Download a template for automation

Create a Bastion

Creation will take a few minutes, then go to your vm-IaaSVM5 and under Operations select Bastion. Fill in your credentials and click Connect.

A separate browser tab will open and let you login 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 store and 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. Let's Encrypt certificates (free and just as secure 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 a powerful way for you to have control over the keys, but you must store the keys in Azure Key Vault.

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. The 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

NETWORK SECURITY GROUPS

We've mentioned NSGs several times but not explained them. They're a free software firewall solution that can filter traffic into and out of vNets, and between vNets. The vm-IaaSVM5 that we have should have an NSG associated with it. You'll find it under Settings – Networking under the Inbound port rules list. It should be called vm-IaaSVM5-nsg, click on it. On the Overview tab you can see the default rules that are created for both inbound and outbound traffic and under Settings you can add or edit rules, associate the NSG with a NIC (not the best way) or a subnet (easier to manage at scale).

Network Security Group rules

AZURE FIREWALL

Azure Firewall is an automatically scaling PaaS service that provides centralized control and lets you easily build hub and spoke vNet architectures. The best way to manage Azure Firewall (and the only way for the new Azure Firewall Premium) is the unified management console, Firewall Manager that lets you manage all Azure Firewalls in your estate. Coming soon is also the ability to manage DDOS protection and Web Application Firewall in Firewall Manager.

MICROSOFT SENTINEL

This cloud-based Security Information and Events Management (SIEM) cloud based SIEM tool hosted in Azure is a perfect complement to give you security insight into your VMs (and your AAD, Microsoft 365 + 100's of non-Microsoft data sources) in a single console.

CONFIDENTIAL COMPUTING

Back when edition 1 was being written, Azure Confidential Computing was in its infancy, now it's ready for prime time for the right workloads. For a long time, we've been protecting data in flight / on the network using TLS or VPN tunnels. Similarly, we protect data at rest with full disk encryption such as Bitlocker (standard in Azure and should be on for all your mobile devices). But protecting data while it's being processed has been significantly harder to achieve.

In recent years, both Intel and AMD have released CPUs that offer enclaves, parts of the CPU and associated memory that's encrypted and not available to the rest of the OS, only the application written specifically to take advantage of the enclave. This means Microsoft's engineers, your VM administrators or SQL administrators don't have access to this data, even if they otherwise have full control over the VM. Early iterations of these enclaves provided very little memory and thus applications had to be hand crafted to take advantage of the enclave protection.

Recently both AMD and Intel now offer CPUs that can "contain" a whole VM in Confidential Computing. Particularly the new AMD based DCasv5 and ECasv5 VM series lets you lift and shift VMs from on-premises to Azure into Confidential Computing, while the Intel SGX Gen3 CPUs offer 8 vCPUs and 1500x the amount of memory previous enclaves provided. This technology is also available for Azure Kubernetes Services (AKS) worker nodes and built into SQL Server / Azure SQL.

NOTE: for an overall healthy and effective security posture, don't forget to also secure your M365 environments! IaaS in Azure is only part of the puzzle. You're only as strong as your weakest link!

CHAPTER 11 – AUTOMANAGE

The overhead of managing VMs compared to other cloud services can be a challenge, in this chapter we're going to look at a simple way to lessen this burden.

IAAS VS PAAS

One of the reasons that Kubernetes, serverless computing, Azure Functions and all the other PaaS services are so popular is the fact that they (more or less) abstract away the underlying infrastructure and complexity. VMs on the other hand require a lot of "care and feeding" in the form of patching, governance, back up, security, monitoring etc. Most IT Pros don't notice because it's what we've been doing for the last 20 years on-premises. Lifting and shifting VMs to the cloud doesn't fundamentally change how you do IT, apart from no longer having to swap broken HDDs or NICs. If I had to pick the single best improvement in Azure IaaS since the first edition of this eBook, this is it.

IT'S LIKE MAGIC

Azure Automanage is Microsoft's attempt at bringing VMs closer to zero maintenance, both in Azure and for any Arc connected machine (chapter 12). You can think of this as taking Microsoft documentation on best practices for Windows / Linux on Azure and packaging it up so you can apply it without having to read all the docs and then manually configure all the right settings.

Do a search for Automanage and click Enable on existing machine, you'll get three options, Production, Dev/Test and Custom profile.

Enable Automanage

Click on View Azure Best Practices profiles to see what each profile configures. Production configures Monitoring, Backup, Defender for Cloud, Antimalware, Update Management, Change Tracking and Inventory, Guest Configuration, Automation Account, Log Analytics Workspace and Boot Diagnostics. Dev / Test is similar but drops Backup and Monitoring (common for non-production VMs). Note that you can click on the arrow next to each service and see exactly how it's going to be configured.

Azure best practices profile details

Automanage – Azure machine best practices | PREVIEW

Configuration profile

Azure Best Practices - Production

Below is the set of the services that will be enabled and automanaged with this profile. The set of services may vary depending on machine type and OS. Turning on Automanage is free but some managed services may incur charges based on usage. Learn More

Machines Insights Monitoring

Azure Monitor for Machines monitors the performance and health of your machines, including their running processes and dependencies on other resources. Learn More

Backup (Not supported for Azure Arc machines)

Azure Backup provides independent and isolated backups to guard against unintended destruction of the data on your machines. Learn More
Charges are based on the number and size of machines being protected. Learn more about pricing

Backup frequency	Daily at 12:00 PM UTC
Instant restore	Retain instant recovery snapshot(s) for 2 day(s)
Retention range	Retain backup taken everyday at 12:00 PM for 180 day(s)

Azure Security Center (Not supported for Azure Arc machines)

Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud. Learn More
Automanage will configure the subscription where your machine resides to the free-tier offering of Azure Security Center. If your subscription is already onboarded to Azure Security Center, then automanaged will not reconfigure it.

Microsoft Antimalware (Not supported for Linux and Azure Arc machines)

Microsoft Antimalware for Azure Machines is a real-time protection capability that helps identify and remove viruses, spyware, and other malicious software, with configurable alerts when known malicious or unwanted software attempts to install itself or run on your system. Learn More

OK

Automanage Production best practices profile

Not only does Automanage set all these settings for each VM you apply the configuration to, but it also monitors for drift over time. Most importantly, you can use Policy to enforce that it's applied to VMs when they're created. And you can create custom profiles with exactly the settings your organization requires.

Using Automanage itself is free, but if you haven't used Backup for example before, enabling it will incur the normal cost of Backup storage etc. Currently it's only available in 15 regions around the world.

If you have production VMs in Azure (or elsewhere and are using Arc), do yourself a favor and adopt Automanage, it'll make managing your VM fleet much easier.

CHAPTER 12 AZURE ARC

Another interesting thing that's happened since the first edition of this eBook is the release of Azure Arc. Here Microsoft shows their leadership in hybrid cloud, supporting businesses who are all in the cloud, businesses who are just starting their cloud journey and everyone in between. And hybrid is a destination, not a quick stop along the way. In this chapter we'll look at Azure Arc and how you can use it to make Azure your control plane for your resources, no matter where they're actually running.

HYBRID HARDWARE

On the hardware side there's Azure Stack Hub, a rack of 4-16 servers that you buy from a set of OEMs which run "real Azure" code and offer a subset of the services in public Azure. You then put these racks wherever you need them (remote operations, cruise ships etc.) and write ARM templates and applications for it just like you would for public Azure. It's an appliance where you have no access to the underlying hosts, and you pay for what you use. It also runs VMs.

If you'd like more control over the hosts there's Azure Stack HCI, which combines the best of Windows Server, Hyper-V, Storage Spaces Direct into clusters you build or purchase from an OEM. You also pay a subscription fee based on the number of cores in each host, but in return you get all new features such as the ability to run Azure Kubernetes Services (AKS) anywhere, and now in preview

the ability to run Azure Virtual Desktop. Then there's Azure Stack Edge, a set of different appliances that run ML and other processing on data before a subset of the data is uploaded to applications / data lakes in public Azure.

HYBRID SOFTWARE

On the software side there's Azure Arc, a set of features that extend Azure's control plane to VMs, databases and Kubernetes on-premises and in any other cloud.

Arc gives you inventory, management, governance, and security for ALL your machines (connected via Arc) in any location. You can use Arc to deploy Azure VM extensions to monitor, secure and patch servers. For any Cloud Native Computing Foundation (CNCF) Kubernetes cluster you can manage, govern, and secure them using Azure Policy, plus use GitOps to configure the cluster automatically from a Git repository. You can also run Azure data services on any Kubernetes cluster as if it was running in Azure (SQL Managed Instance and Azure Database for PostgreSQL Hyperscale). Arc-enabled machine learning (in preview) uses Kubernetes clusters to train, inference and manage ML models. Open Service Mesh is a way to manage highly dynamic microservice environments; it's now Arc-enabled as well.

Most excitingly however, is the preview of Azure Arc for VMware vSphere. This lets authorized users do self-service VM creation and management (stop, start, restart, resize, adding or updating disks, managing NICs) directly from the Azure portal. It also supports ARM templates to enable DevOps

CI/CD workflows. You can also onboard large vSphere environments into Azure Monitor or Azure Policy at scale, by deploying the Connected Machine agent to each VM. The synchronization between Azure and your vSphere infrastructure is managed through a virtual appliance called an Arc resource bridge.

Arc is an interesting twist to the multi cloud approach. Some businesses choose to deploy some workloads in AWS and some in Azure for example, the thinking being that they won't have a widespread outage simultaneously. There are many challenges with this approach, such as skilling staff to manage multiple platforms and ending up with "lowest common denominator" deployments to ensure portability. But one big challenge, managing multiple clouds in different portals can be a lot easier with Arc – deploy VMs, Kubernetes clusters and databases in AWS, GCP or another cloud but manage them all from Azure.

There's also a marriage between the hardware and software, specifically Azure Stack HCI now automatically Arc enrolls the hosts (from version 21H2) which will also let you easily deploy extensions to VMs. Further, you can create and manage VMs on your on-premises Azure Stack HCI cluster from the Azure portal.

ARC FOR SERVERS

Since we're focusing on VMs, let's dig deeper into what Azure Arc for Servers offers. Arc connected Linux and Windows servers are given a Resource ID and are placed in a Resource Group that you designate. You can now tag each server and you can apply Policy guest configurations (chapter 6) to them, use Defender for Endpoint via Defender for Cloud (chapter 10), connect them to Microsoft Sentinel, use Automation (chapter 13), apply Automanage (chapter 11), use Monitor to keep an eye on them (chapter 5) and install VM extensions.
If you're running SQL Server inside an Arc server, other scenarios light up as well.
Onboarding a server or several to Arc is easy, the Azure Connected Machine agent needs to be installed using a script.

Add servers to Azure Arc

If you want to learn more about all the different ways you can apply Arc, explore Arc Jumpstart, a set of documented, step-by-step tutorials. If you don't have a lab environment, consider Jumpstart Arcbox, a ready-made big VM with child VMs that lets you try out many different scenarios hands on.

It pays to follow Arc if you have any kind of hybrid infrastructure – Arc is spreading to more and more platforms and services.

CHAPTER 13 – AUTOMATION

In this chapter we'll tie the previous chapters together. You've learnt 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 and Bicep to templatize your deployments, back up 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 clouds 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.

Create an Automation Account ...

Basics Advanced Networking Tags Review + Create

Create an Automation Account to hold the Automation runbooks & configuration used for automating operations and management tasks around Azure and non-Azure resources. You could execute cloud jobs in a serverless environment or use hybrid jobs on your compute via Azure Virtual machines or Arc-enabled servers. Learn more

Subscription * MSDN Platforms

Resource group * rg-AzureIaaS
Create new

Instance Details

Automation account name * aa-IaaS

Region * Australia East

Creating an Automation account

Search for Automation in the portal and click on Automation accounts – click Create. Call your account **aa-IaaS**, put it in the rg-AzureIaaS RG, leave System assigned Managed Identity selected, click Create. Once it's been deployed go to it and click Runbooks under Process Automation, then Browse gallery. 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 lets you set up agents on-premises or in other clouds to automate processes there. It's generally easy to automate actions for Azure resources but extending to other environments can be challenging. The new Hybrid Worker Extension works with Arc connected servers (chapter 12) should make this easier. Schedules lets 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.

State Configuration is eventually going to be replaced by guest configuration (currently in preview) which combines the best features of DSC (without the management overhead), State Configuration plus customer feedback.

RUN COMMANDS

Azure has had the ability to run commands from the portal in VMs for some time. Recently the managed Run Command preview was released which lets you deploy them using ARM templates, run them in parallel or sequentially, specify the time out and let scripts run for hours / days and let you pass secrets to them in a secure manner.

VM APPLICATIONS

Currently in preview there's a new way to manage applications for your Azure IaaS Linux and Windows VMs called VM Applications. It uses the Azure Compute Gallery to distribute the applications, globally if you need it. There are some limitations in the preview, only five applications per VM and each installer can't be larger than 1 GB.

AZURE LIGHTHOUSE

If you're enlisting a Managed Service Provider (MSP) to manage your Azure estate for you, make sure they're using Azure Lighthouse. This allows them to publish an offer to you where they get scoped access to a set of resources in your tenant with RBAC permissions so that they can either be readers or contributors (but not owners). Furthermore, you can enforce that they use MFA when managing your resources and you can revoke access at any time.

AZURE ADVISOR

Azure Advisor is a customized (for your deployments) cloud consultant that gives you recommendations across Reliability, 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 14 – BEYOND IAAS

The last 13 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 is 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 vNets, Azure Monitor, AAD, Azure 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 VIRTUAL DESKTOP

This service has grown tremendously over the last couple of years, as many businesses wanted to provide a secure, managed Windows 10 desktop for their staff that they could access from their homes on any device. AVD (formerly Windows Virtual Desktop) has clients for Android, iOS, MacOS and Windows. One of the things you manage as an AVD administrator is the underlying VMs, how many users can fit onto each Windows 10 Multisession host in the pool is controlled by the size of that VM. So, everything you learnt in chapter 2 applies.

AZURE SQL

There are three basic flavors of SQL Server in Azure – you can run it as 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. 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 rapid compute scale up and down. The third option is SQL Managed Instance, which is "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 you're the application you're migrating relies on SQL Server, investigate your options carefully; perhaps managing and 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 read 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 globally versus the latency off writes to the database.

There are other data services that'll help you manage all types of data 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). 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 v2 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

The modern alternative to VMs is 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 micro services-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). If that's too much to manage, but your application is containerized you can use the new Container Apps.

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. Scaling is taken care of for you by the platform whether that's one request per second or thousands, and you only pay for what you use.

CONCLUSION

This book will have given you a good grounding in how to create, manage and run VMs in Azure but this is just a start. In this rapidly changing landscape, it's important to keep up to date with the latest developments. A great way of doing this is with Azure notes, the Azure Podcast, John Savill's technical training videos and the Altaro DOJO.

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 – I wish you success on this journey.

Make sure to delete the rg-AzureIaaS resource group and any other lingering resources so you don't use up your trial credits. If you've performed backups of VMs you might have to jump through some extra hoops to delete them.

We update this eBook regularly. Please provide any feedback or suggestions for topics to include to dojo@altaro.com

FOUND THIS EBOOK HELPFUL?

LEARN MORE ABOUT AZURE

Journey to the Clouds —

Masterclass on Cloud Migration

On-demand webinar

Watch >

Why Azure and not AWS?

Blog article

Read >

Azure Arc-enabled Kubernetes —

What it means for SysAdmins

Blog article

Read >

5 Powerful Ways to Use Azure IaaS

Blog article

Read >

Share this eBook. **Follow Altaro.** **Follow Hornetsecurity.**

EXPLORE OTHER EBOOKS

The Backup Bible

Everything you need to know about planning, deploying and maintaining a secure and reliable backup and disaster recovery strategy.

Download now >

How to Get the Most Out of Windows Admin Center

Windows Admin Center is one of the most important and powerful tools in a system administrator's toolbox. But are you harnessing its full potential?

Download now >

Office 365 / Microsoft 365 — The Essential Companion Guide

Office 365 and Microsoft 365 contain truly powerful applications that can significantly boost productivity in the workplace. However, there's a lot on offer. Use this guide to ensure you get the most out of your investment!

Download now >

Share this eBook. **Follow Altaro.** **Follow Hornetsecurity.**

SECURE YOUR DATA

TRY OUR TOOLS.

ALTARO BACKUP

Solutions for Companies and Organizations

Hyper-V & VMware Backup & Replication

Award-winning virtual machine (VM) backup and replication solution for Hyper-V and VMware environments

Learn more

Microsoft 365/Office 365 Backup

Backup solution for Microsoft 365 mailboxes and files stored in OneDrive and SharePoint, with unlimited storage

Learn more

Windows Server Backup

Physical to virtual (P to V) backup solution to back up physical WIndows servers and restore them to a virtual environment

Learn more

Solutions for Managed Service Providers (MSPs)

Hyper-V & VMware Backup & Replication

Monthly subscription program enabling MSPs to offer Hyper-V, VMware and physical Windows server backup services

Learn more

Microsoft 365/Office 365 Backup

Monthly subscription program enabling MSPs to back up customers' Microsoft 365 mailboxes and OneDrive/SharePoint files

Learn more

EndPoint Backup

Monthly subscription program enabling MSPs to provide backup services for on-premise and roaming Windows desktop and laptop

Learn more

Start your free 30-day trial today

HORNETSECURITY

FACT SHEET

365 TOTAL PROTECTION

Security and compliance management for Microsoft 365

We offer you two comprehensive packages for your company security management developed for Microsoft 365: With 365 Total Protection Business, you get a comprehensive security solution with a wide range of features that ensure your email and data security in Microsoft 365. The Enterprise version covers legally compliant email archiving with advanced features and offers intelligent protection against advanced persistent threats by using AI-based analysis mechanisms.

Protection from:

Targeted attacks on Microsoft 365 accounts

SPECIALLY DEVELOPED FOR MICROSOFT 365 AND SEAMLESSLY INTEGRATED

It couldn't be easier – onboarding within 30 seconds.
In just 3 clicks, the intuitive onboarding process is complete and your Microsoft 365 merges with 365 Total Protection.
365 Total Protection makes sure you get the most out of your Microsoft cloud services.

Fig.: Simple onboarding process in three steps

1. REGISTER **COMPANY DATA**
2. CONNECT **WITH MICROSOFT**
3. SET UP **COMPLETED!**

INTEGRATION OF 365 TOTAL PROTECTION IN THE EMAIL MANAGEMENT SYSTEM

All aspects of security administration are easy to manage with 365 Total Protection – without the need for maintenance or updates. Existing user profiles can be managed or created in mere seconds.

www.hornetsecurity.com | info@hornetsecurity.com

START YOUR 30-DAY TRIAL