Contents

[Glossry: 2](#_Toc52389807)

[Choose an Azure compute service for your application 2](#_Toc52389808)

[Virtual Machine 3](#_Toc52389809)

[VM Naming Convention 3](#_Toc52389810)

[Availability Sets 3](#_Toc52389811)

[Availability Zone 6](#_Toc52389812)

[Availability zone vs Availability set 7](#_Toc52389813)

[Scale sets 8](#_Toc52389814)

[Azure Scale set vs Azure Availability Zone 10](#_Toc52389815)

[AutoScale 10](#_Toc52389816)

[Disks 13](#_Toc52389817)

[Managed and Unmanaged Disks 14](#_Toc52389818)

[Features of Managed Disks 14](#_Toc52389819)

[Disk roles 16](#_Toc52389820)

[OS Disk 16](#_Toc52389821)

[Data Disk 16](#_Toc52389822)

[Temp Disk 17](#_Toc52389823)

[Disk Types and attach process 17](#_Toc52389824)

[Azure Disk Encryption 17](#_Toc52389825)

[Terminology 17](#_Toc52389826)

[VM Requirement for Encryption 18](#_Toc52389827)

[Azure Backup 19](#_Toc52389828)

[implement Azure Backup for VMs 19](#_Toc52389829)

[VM Cli 19](#_Toc52389830)

[VM Power Shell 19](#_Toc52389831)

[NetworkWatcherRG 19](#_Toc52389832)

[Tasks : 19](#_Toc52389833)

[Add disks 19](#_Toc52389834)

[Add NIC Card/network interfaces 19](#_Toc52389835)

[FAQ 20](#_Toc52389836)

[Azure VM sizes with no local temporary disk 20](#_Toc52389837)

# Glossry:

**SKU** : Stock Keeping Units ( Various types or options available)

**Region** : A set of datacenters deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network.

**Geography** : An area of the world containing at least one Azure region. Geographies define a discrete market that preserve data residency and compliance boundaries. Geographies allow customers with specific data-residency and compliance needs to keep their data and applications close. Geographies are fault-tolerant to withstand complete region failure through their connection to our dedicated high-capacity networking infrastructure.

**Availability Zone**: Unique physical locations within a region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking.

**Recommended region**: A region that provides the broadest range of service capabilities and is designed to support Availability Zones now, or in the future. These are designated in the Azure portal as Recommended.

**Alternate (other) region**: A region that extends Azure's footprint within a data residency boundary where a recommended region also exists. Alternate regions help to optimize latency and provide a second region for disaster recovery needs. They are not designed to support Availability Zones (although Azure conducts regular assessment of these regions to determine if they should become recommended regions). These are designated in the Azure portal as Other.

**Foundational service**: A core Azure service that is available in all regions when the region is generally available.

**Mainstream service**: An Azure service that is available in all recommended regions within 12 months of the region/service general availability or demand-driven availability in alternate regions.

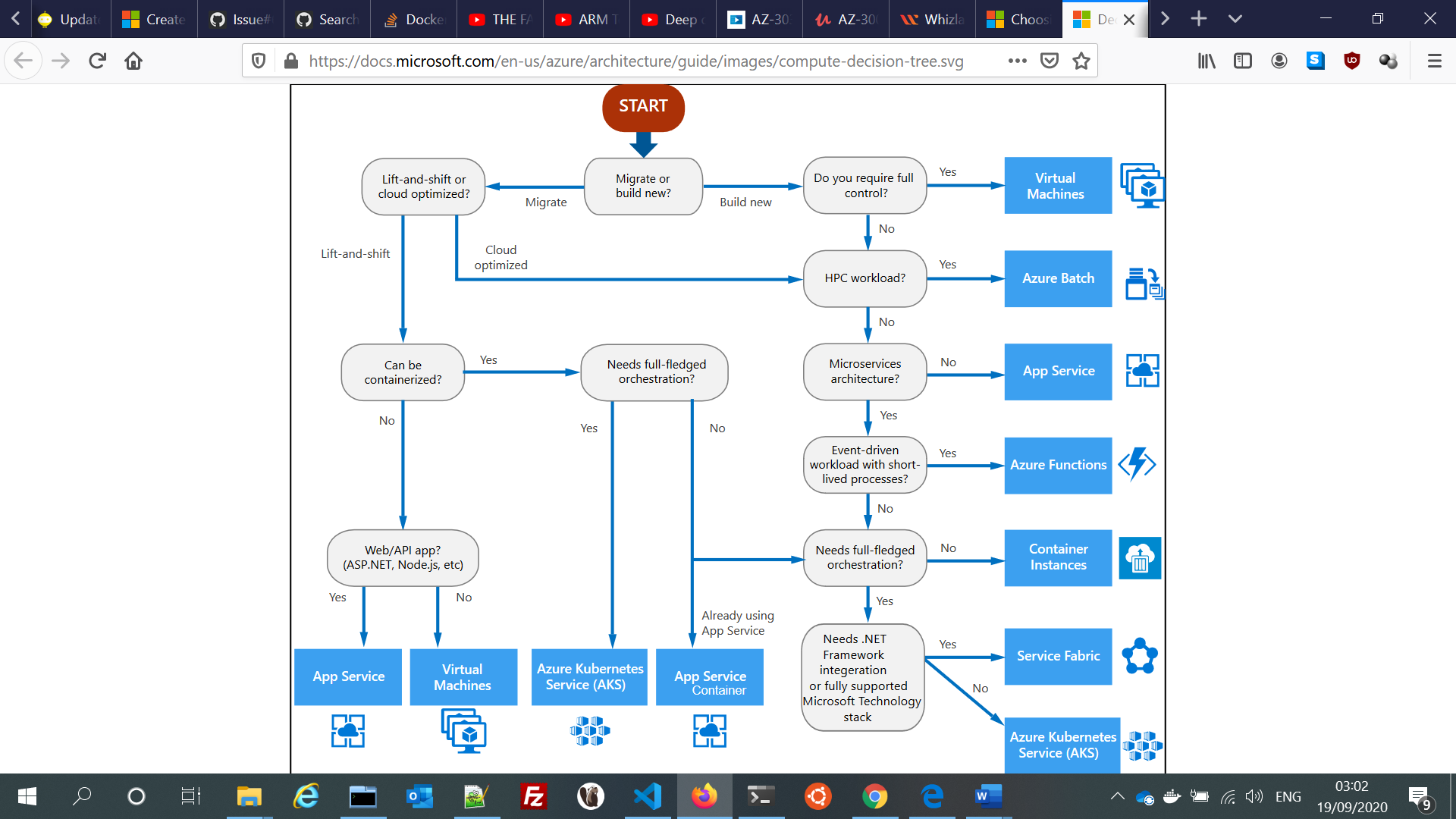
**Specialized service**: An Azure service that is demand-driven availability across regions backed by customized/specialized hardware.

**Regional service**: An Azure service that is deployed regionally and enables the customer to specify the region into which the service will be deployed. For a complete list, see Products available by region.

**Non-regional service**: An Azure service for which there is no dependency on a specific Azure region. Non-regional services are deployed to two or more regions and if there is a regional failure, the instance of the service in another region continues servicing customers. For a complete list, see Products available by region.

# Choose an Azure compute service for your application

<https://docs.microsoft.com/en-us/azure/architecture/guide/technology-choices/compute-decision-tree>



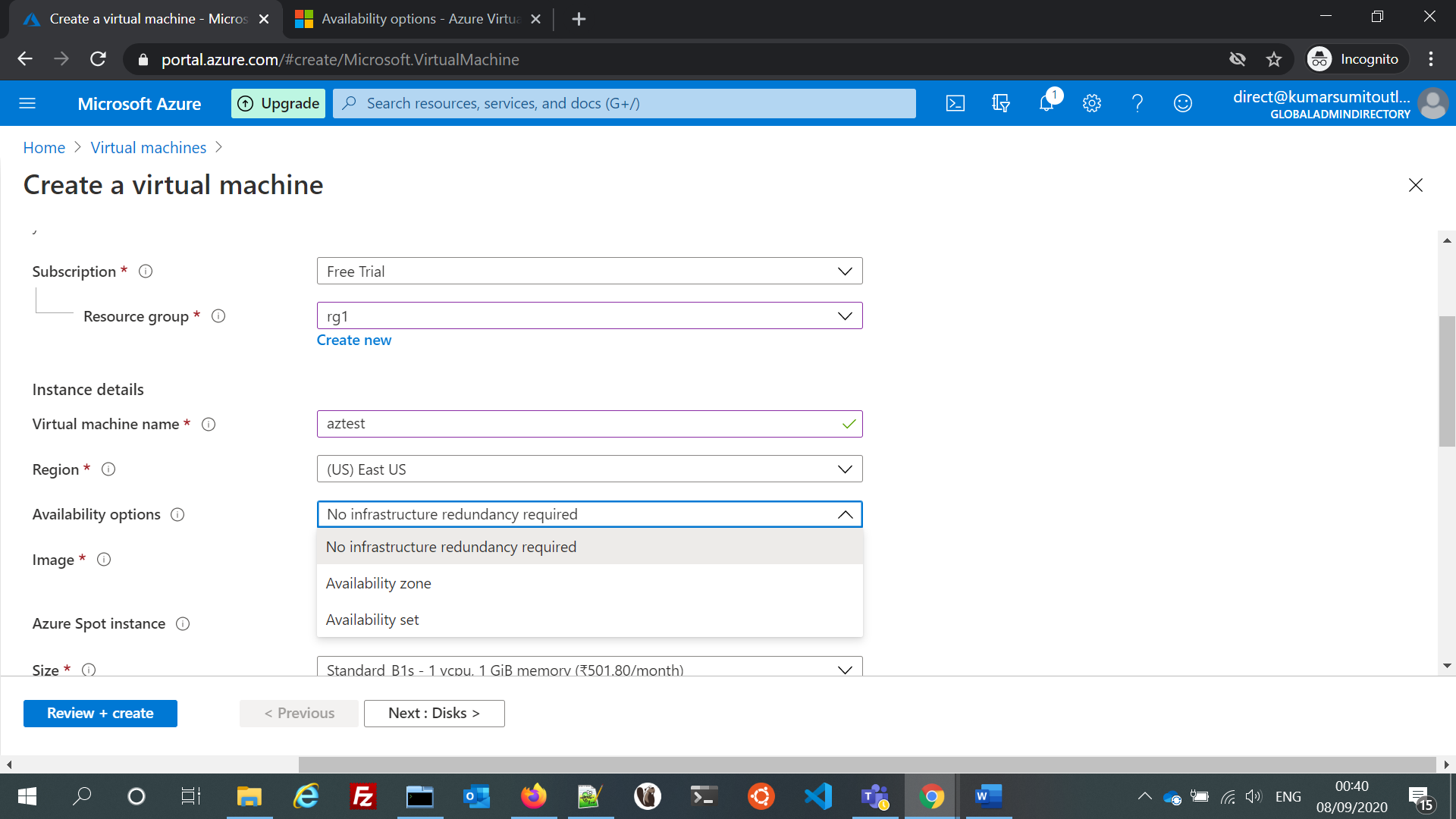
# Virtual Machine

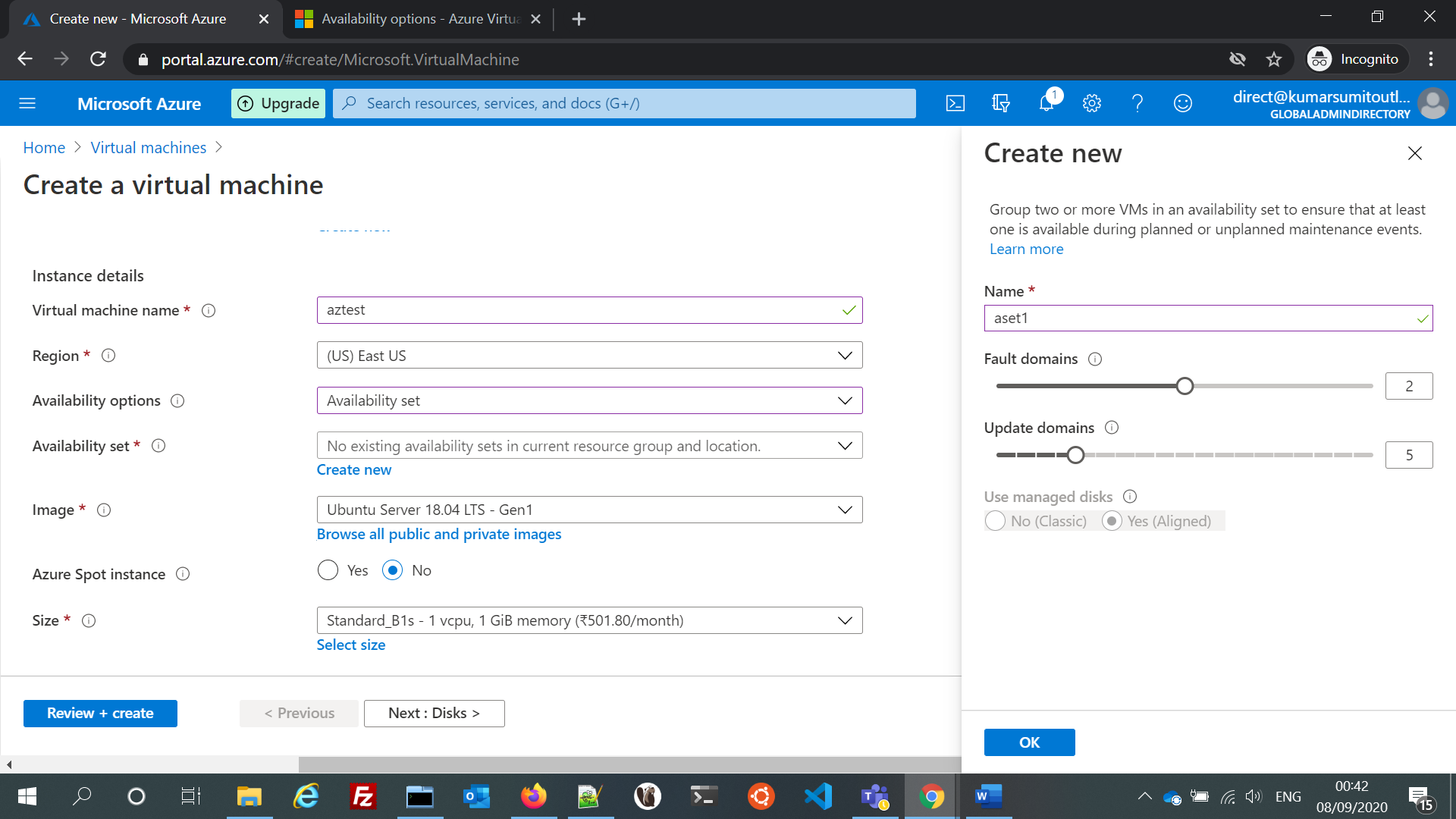
## VM Naming Convention

<https://docs.microsoft.com/en-us/azure/virtual-machines/vm-naming-conventions>

## Availability Sets

Running a VM with one or more replicated copies on separate hardware **within the same Availability Zone**, providing resiliency against machine failure.



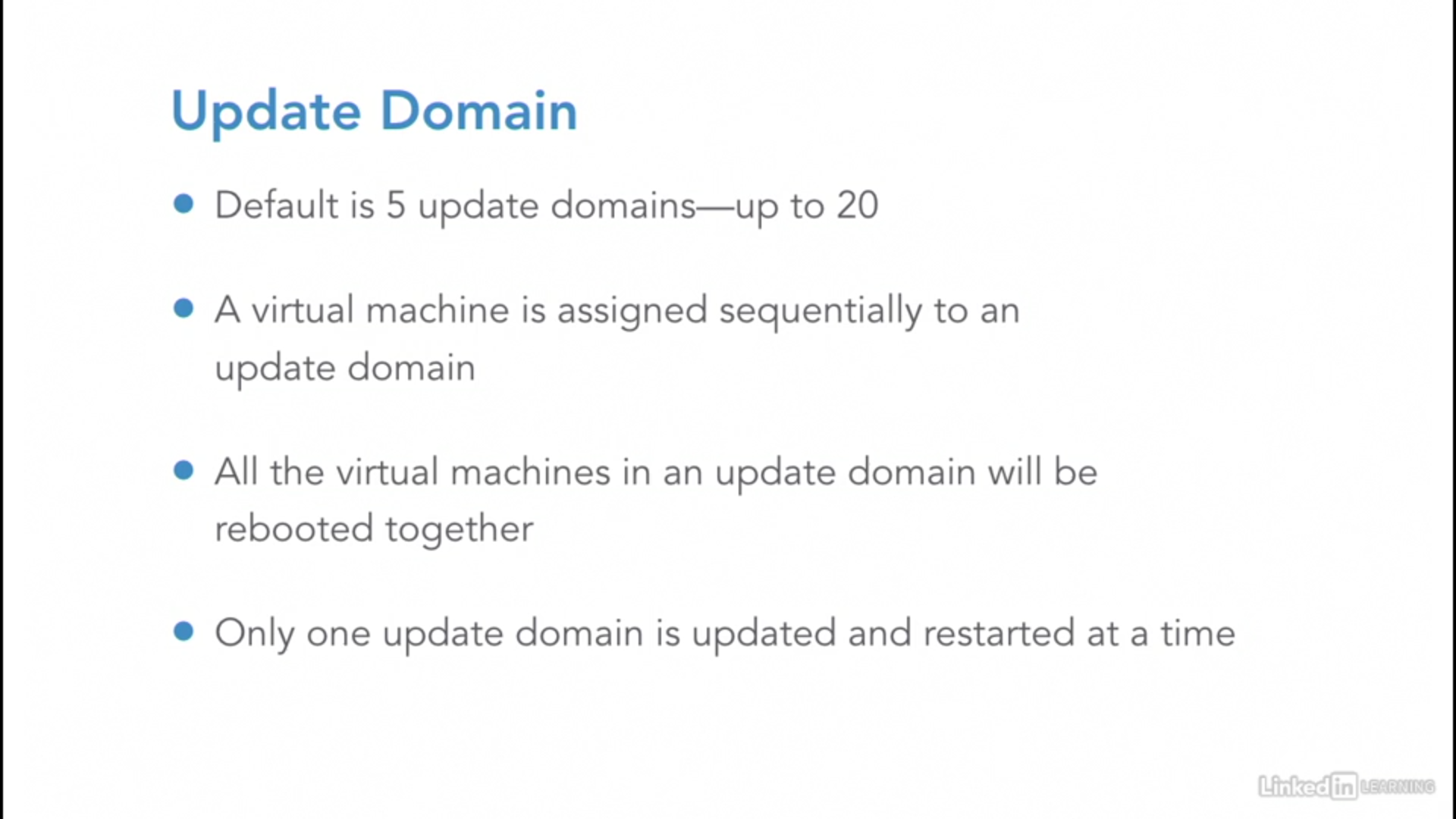


**Integration with availability sets**

Managed disks are integrated with availability sets to ensure that the disks of VMs in an availability set are sufficiently isolated from each other to avoid a single point of failure. Disks are automatically placed in different storage scale units (stamps). If a stamp fails due to hardware or software failure, only the VM instances with disks on those stamps fail. For example, let's say you have an application running on five VMs, and the VMs are in an Availability Set. The disks for those VMs won't all be stored in the same stamp, so if one stamp goes down, the other instances of the application continue to run.

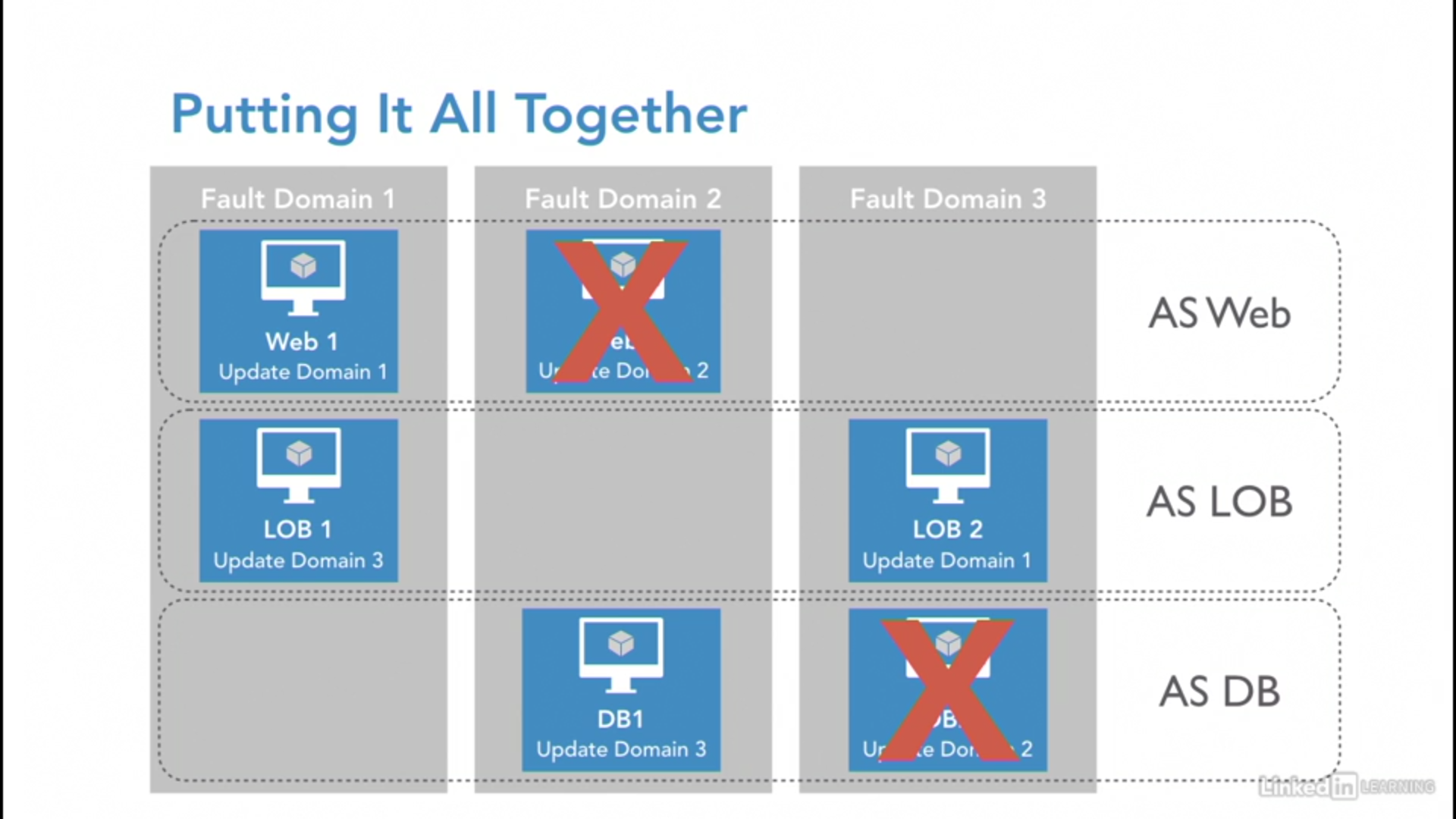
**Integration with Availability Zones**

Managed disks support Availability Zones, which is a high-availability offering that protects your applications from datacenter failures. Availability Zones are unique physical locations within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. To ensure resiliency, there's a minimum of three separate zones in all enabled regions. With Availability Zones, Azure offers industry best 99.99% VM uptime SLA.



**Fault domain** share a common power source and physical network switch.

Virtual machines in the same **update domain** will be restarted together during planned maintenance. Azure never restarts more than one update domain at a time.



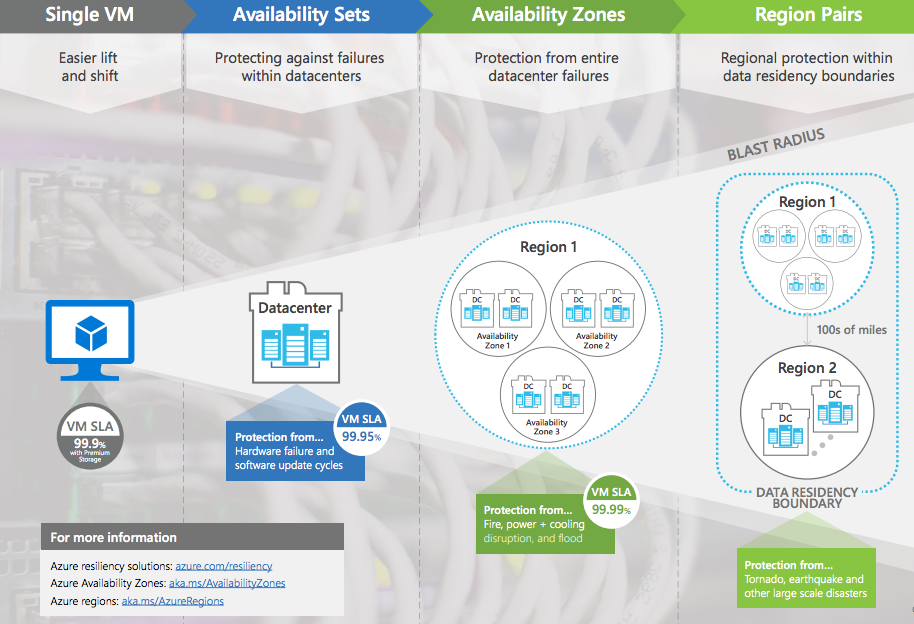
Note:

* **In Availability Set you get to choose Fault Domains and update domains.**

## Availability Zone

<https://docs.microsoft.com/en-us/azure/availability-zones/az-overview>

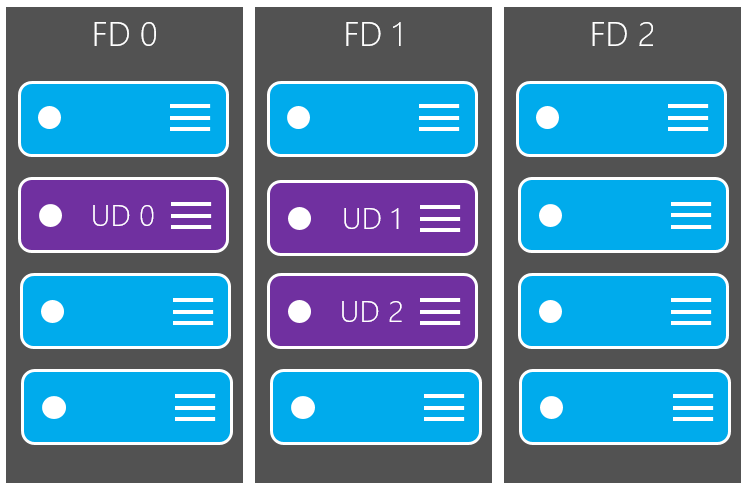
Availability Zones are unique physical locations within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. To ensure resiliency, there's a minimum of three separate zones in all enabled regions. The physical separation of Availability Zones within a region protects applications and data from datacenter failures. Zone-redundant services replicate your applications and data across Availability Zones to protect from single-points-of-failure.



An Availability Zone in an Azure region is a combination of a **fault domain** and **an update domain**.  For example, if you create three or more VMs across three zones in an Azure region, your VMs are effectively distributed across three fault domains and three update domains.

**Fault domains define the group of virtual machines that share a common power source and network switch.**

**The order of update domains being rebooted may not proceed sequentially during planned maintenance, but only one update domain is rebooted at a time.**



<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/manage-availability>

There are two categories of Availability Zones:

* **Zonal Services** (Add the resource to a specific zone, for example VMs, Managed Disks, IP Addresses )
* **Zone-redundant services** (Automatic replication across zones is enabled for SQL Database, zone-redundant storage)

### Availability zone vs Availability set

<https://social.technet.microsoft.com/wiki/contents/articles/51828.azure-vms-availability-sets-and-availability-zones.aspx>

|  |  |
| --- | --- |
| Availability set | Availability zone |
| A group with two or more virtual machines in the same Data Center is called Availability Set | A group with two or more virtual machines in the **same Zone (more than one Data Center)** is called Availability Zone |
| We can configure an Availability Set ONLY when we deploy a New Virtual Machine, we can't add an existing Virtual Machine to an Availability Set. |  |
| Protect from Hardware failures within data centers | Protect from entire data center failure |
| SLA 99.95% | SLA 99.99% |

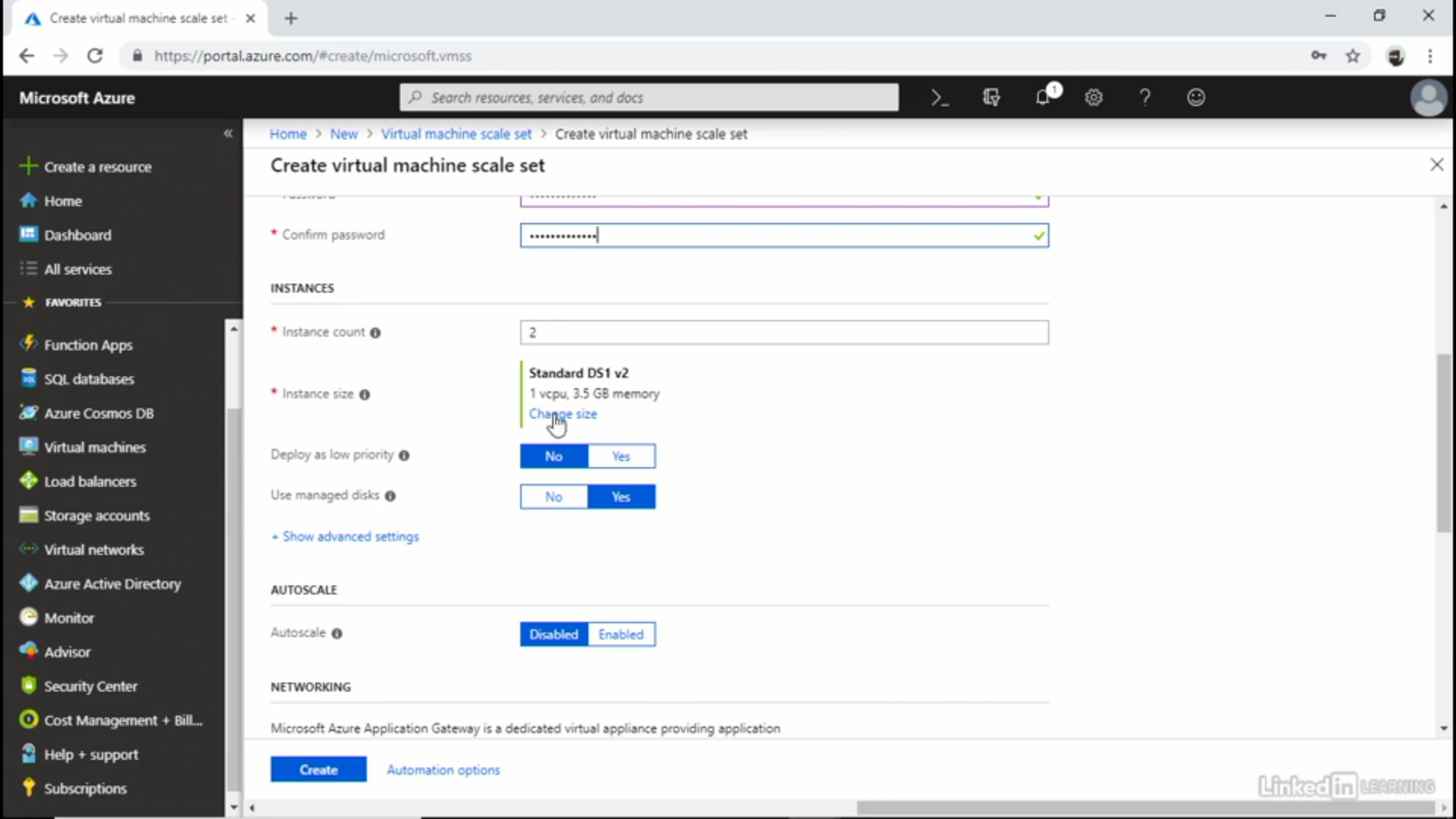
## Scale sets

<https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/overview>

They are basically auto scaled VM machine groups which scale up and down depending upon CPU usage.

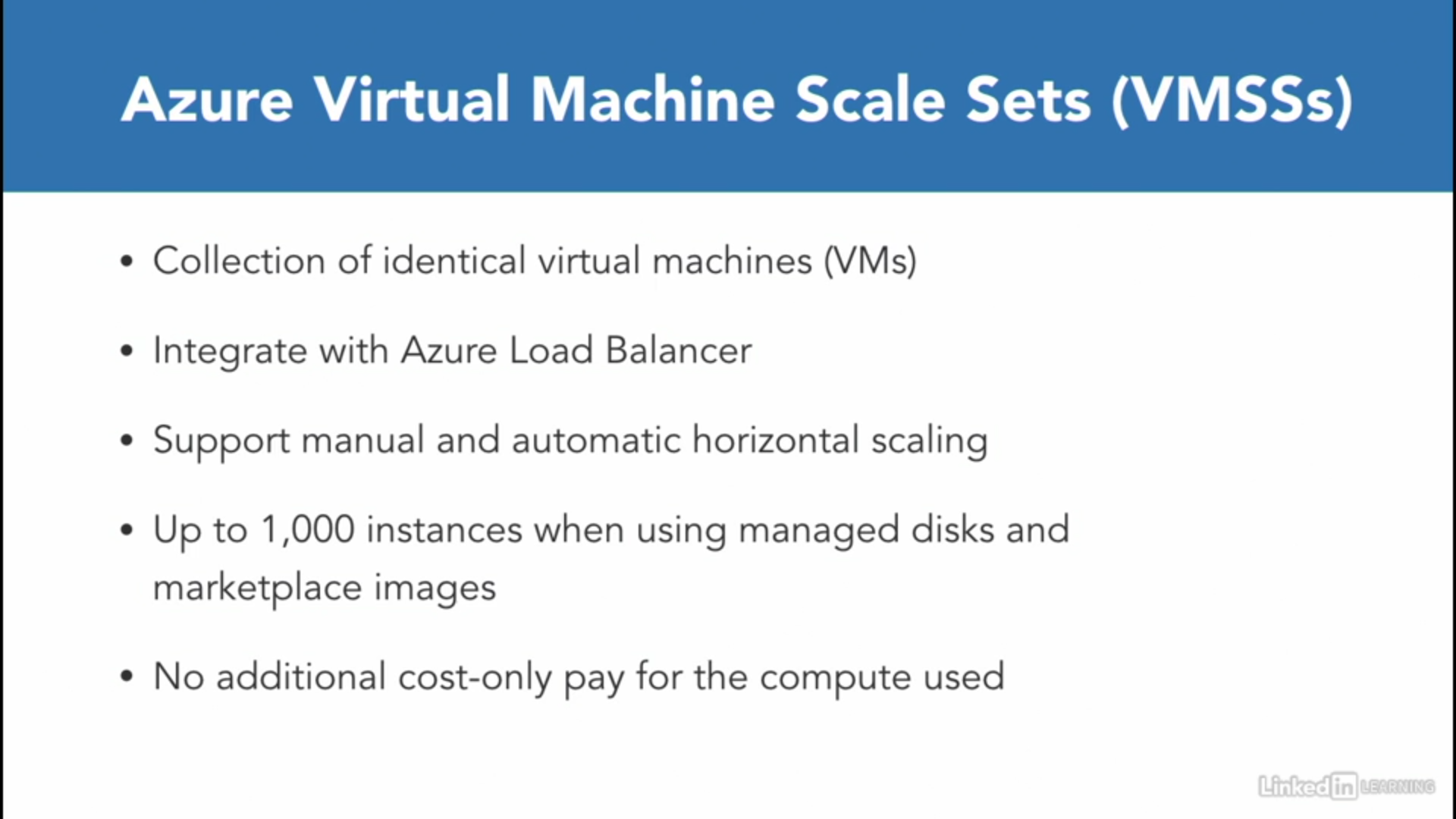
Azure virtual machine scale sets provide the management capabilities for applications that run across many VMs, [automatic scaling of resources](https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-autoscale-overview), and load balancing of traffic.

You can deploy VMs in a VM Scale Set (VMSS). VMSS lets you create and manage a group of identical, load-balanced VMs, and dynamically add or remove VMs from the set. If you set up your VMSS with availability sets, you have the option to deploy a single set per Availability Zone, and load balance traffic across zones.



| **Scenario** | **Manual group of VMs** | **Virtual machine scale set** |
| --- | --- | --- |
| Add additional VM instances | Manual process to create, configure, and ensure compliance | Automatically create from central configuration |
| Traffic balancing and distribution | Manual process to create and configure Azure load balancer or Application Gateway | Can automatically create and integrate with Azure load balancer or Application Gateway |
| High availability and redundancy | Manually create Availability Set or distribute and track VMs across Availability Zones | Automatic distribution of VM instances across Availability Zones or Availability Sets |
| Scaling of VMs | Manual monitoring and Azure Automation | Autoscale based on host metrics, in-guest metrics, Application Insights, or schedule |

There is no additional cost to scale sets. You only pay for the underlying compute resources such as the VM instances, load balancer, or Managed Disk storage. The management and automation features, such as autoscale and redundancy, incur no additional charges over the use of VMs.



### Azure Scale set vs Azure Availability Zone



<https://tutorialsdojo.com/azure-scale-set-vs-availability-set/>

To sum up use availability set when load is predictable or want redundancy and scale set when load is unpredictable.

## AutoScale

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/autoscale-overview>

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/autoscale-common-scale-patterns>

Off and on

Unpredictable by CPU

Adding Resources

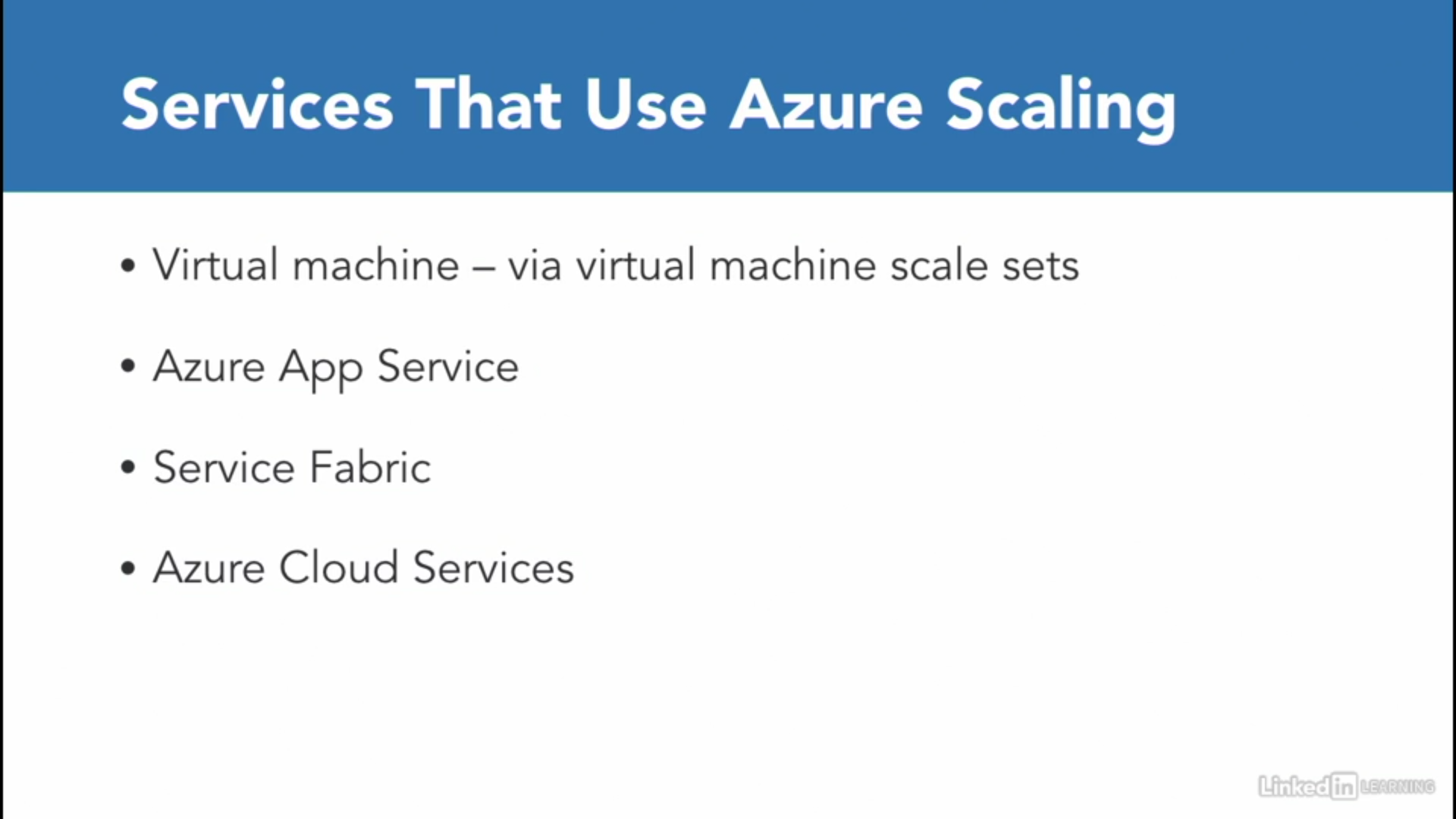
Predictable

Adding resources is correct as you can scale this solution manually.

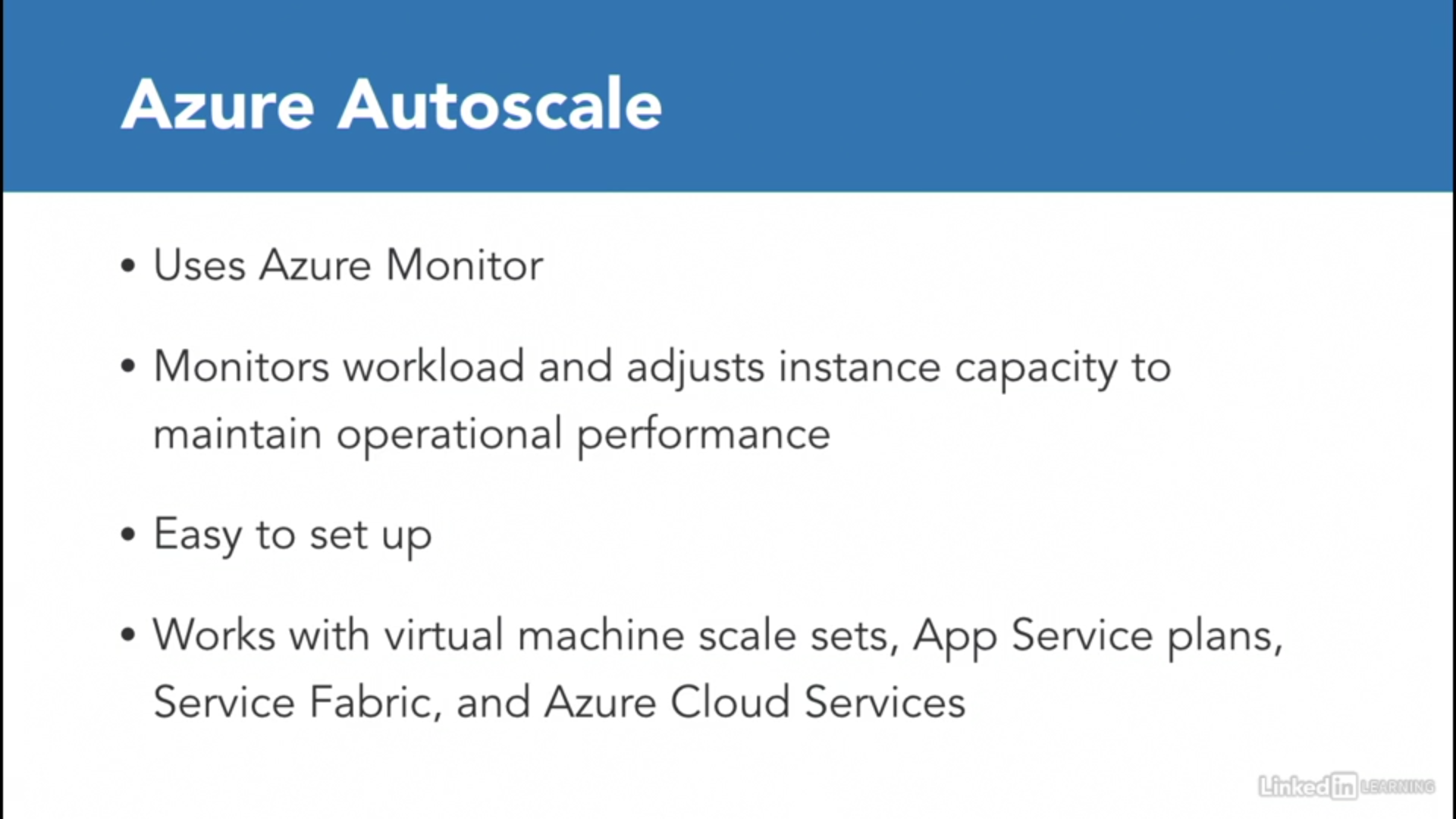
Off and On autoscaling will not suffice as this solution is already working full time at a high capacity, shutting it down will not improve anything.

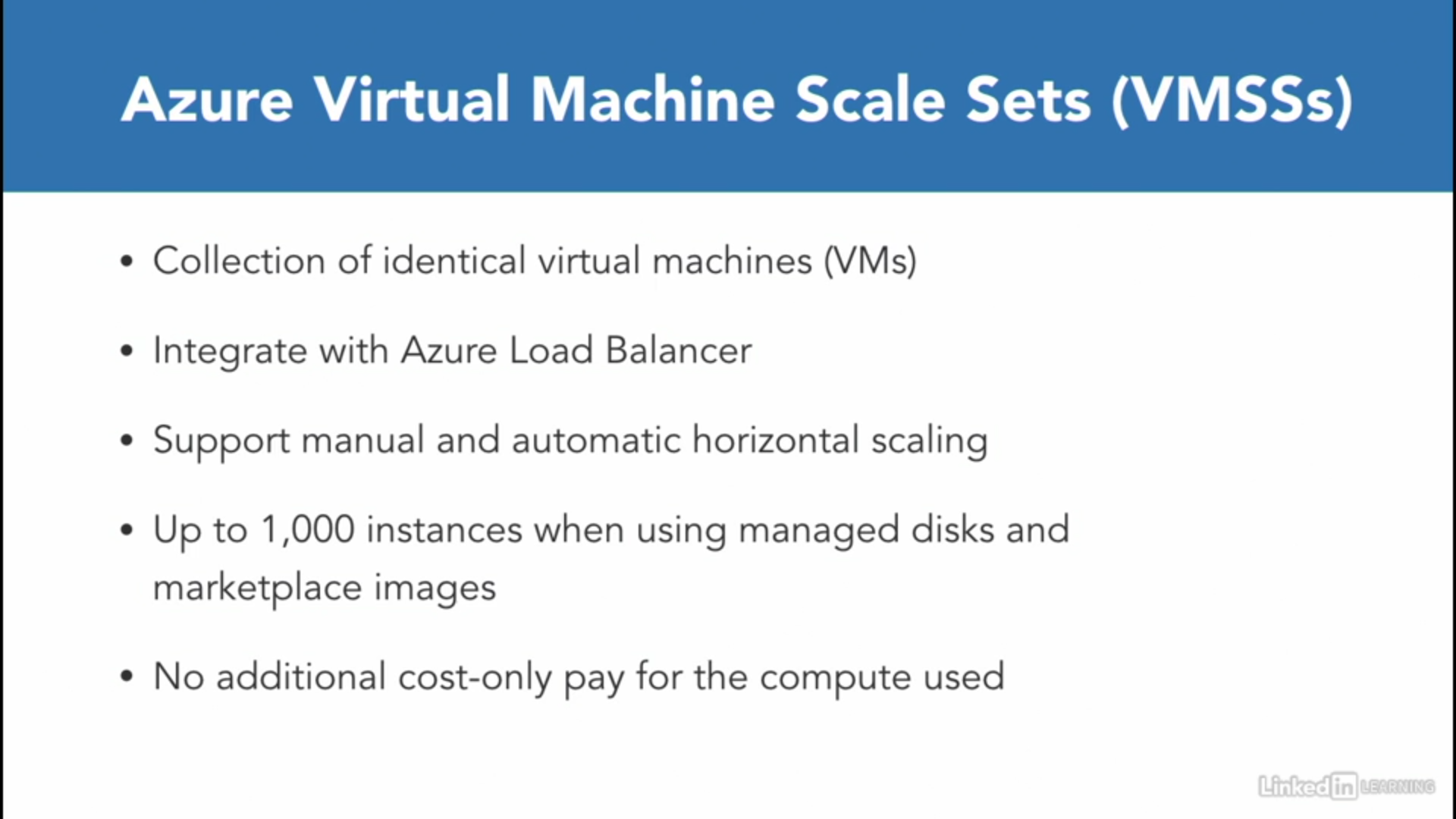
Unpredictable autoscaling will not suffice as this pattern is used for example when the CPU threshold is above 95% for 5 minutes and you did not predict it, however, the current load is consistently running around 70-90%.

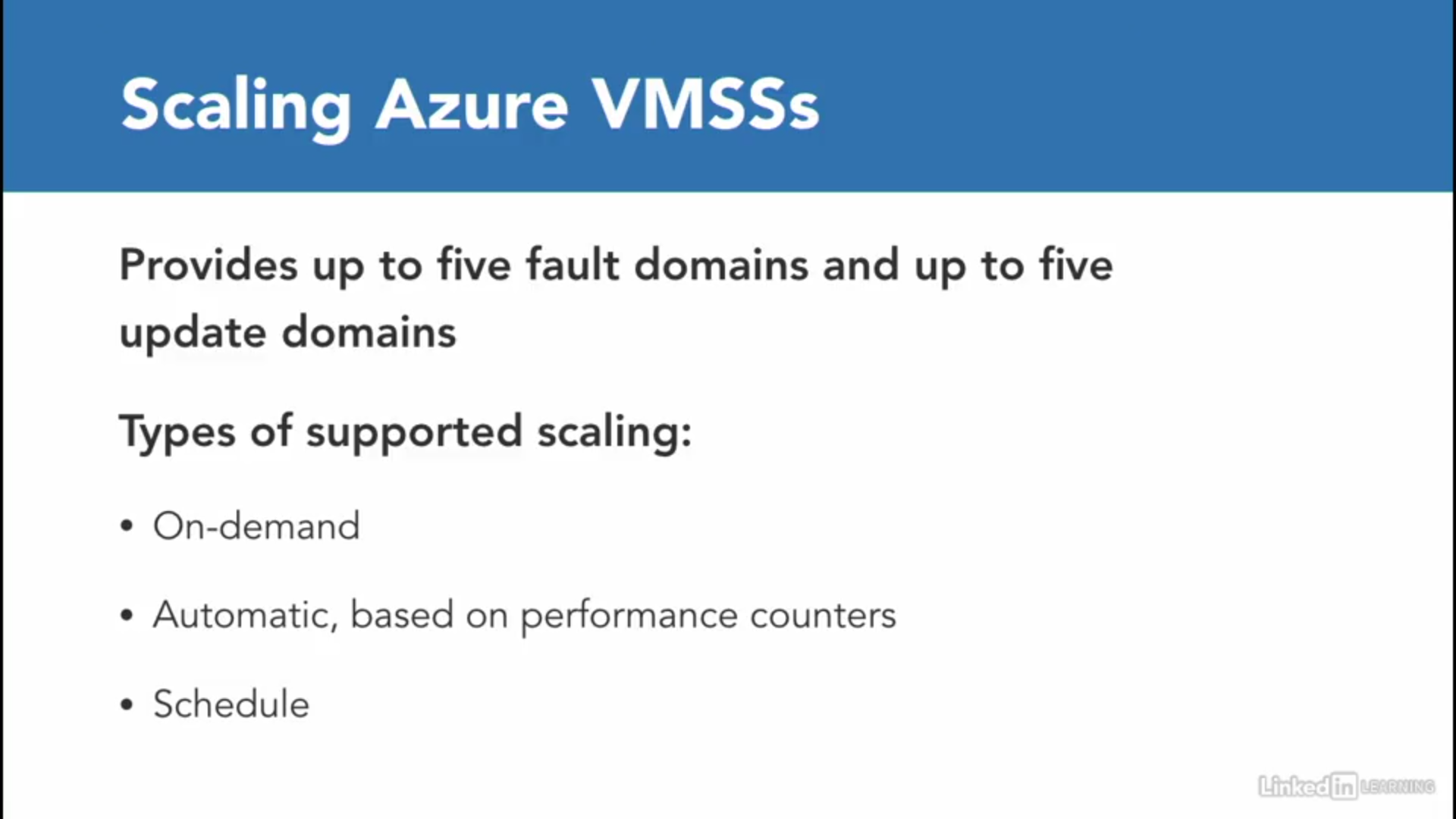
Predictable autoscaling will not suffice as this is primarily used when you know or suspect when resources will be maxed out, however in this scenario resources are already maxed out and needs immediate attention











## Disks

### Managed and Unmanaged Disks

<https://www.youtube.com/watch?v=oQVVsEy1ciQ>

|  |  |  |
| --- | --- | --- |
| Features | Managed Disks | Unmanaged Disks |
| Management | Is an ARM (Azure Resource Manager) object (resource) | Is not an ARM resource, but a file (.vhd) residing on an Azure Storage Account. The latter is an ARM object |
| Size | The managed disks sizes are fixed (and can be resized). Which means that you cannot choose a custom size. You will need to pick up from a list. | You can choose the disk size during the provisioning (and can be resized) when using Standard Storage. |
| Performance | A managed disk has a predictable performance, with standard HDD (Upto 2000 IOPS), with Standard SSD storage (Upto 6000 IOPS), Premium SSD storage (Upto 20000 IOPS), Ultra Disk offering (Upto 160,000 IOPS)  \*IOPS depends on the size of the disk. | Only premium storage disks have a predictable performance (depends on the disk). Standard storage has a predictable performance (500 IOPS) unless they are impacted by the Storage Account performance limits (A maximum of 40 disks per standard storage account is recommended, otherwise disks can be throttled). |
| Availability | When placing Azure Virtual Machines using managed disks under an Availability Set, disks are placed on different fault domains in order to achieve the better SLA (The Availability Set SLA is only for compute) | When placing Azure Virtual Machines using unmanaged disks under an Availability Set, there is no guarantee that the disks are placed on different fault domains, even if they are on different Storage Accounts. |

## Features of Managed Disks

<https://docs.microsoft.com/en-us/azure/virtual-machines/managed-disks-overview>

1. Integration with availability sets

Managed disks are integrated with availability sets to ensure that the disks of VMs in an availability set are sufficiently isolated from each other to avoid a single point of failure. Disks are automatically placed in different storage scale units (stamps).

1. Integration with Availability Zones

Managed disks support Availability Zones, which is a high-availability offering that protects your applications from datacentre failures. To ensure resiliency, there's a minimum of three separate zones in all enabled regions.

1. Granular access control

You can use Azure role-based access control (Azure RBAC) to assign specific permissions for a managed disk to one or more users.

1. Upload your vhd

Direct upload makes it easy to transfer your vhd to an Azure managed disk. Previously, you had to follow a more involved process that included staging your data in a storage account.

1. Encryption

Managed disks offer two different kinds of encryption. The first is Server Side Encryption (SSE), which is performed by the storage service. The second one is Azure Disk Encryption (ADE), which you can enable on the OS and data disks for your VMs.

**Server-side encryption**: Server-side encryption is enabled by default for all managed disks, snapshots, and images, in all the regions where managed disks are available. (Temporary disks, on the other hand, are not encrypted by server-side encryption unless you enable encryption at host; see Disk Roles: temporary disks). You can either allow Azure to manage your keys for you, these are platform-managed keys, or you can manage the keys yourself, these are customer-managed keys.

**Azure Disk Encryption**: Azure Disk Encryption allows you to encrypt the OS and Data disks used by an IaaS Virtual Machine. This encryption includes managed disks. For Windows, the drives are encrypted using industry-standard **BitLocker** encryption technology. For Linux, the disks are encrypted using the **DM-Crypt** technology. The encryption process is integrated with Azure Key Vault to allow you to control and manage the disk encryption keys.

1. Managed disk snapshots

A managed disk snapshot is a read-only crash-consistent full copy of a managed disk that is stored as a standard managed disk by default

Snapshots are billed based on the used size. For example, if you create a snapshot of a managed disk with provisioned capacity of 64 GiB and actual used data size of 10 GiB, that snapshot is billed only for the used data size of 10 GiB. You can see the used size of your snapshots by looking at the Azure usage report.

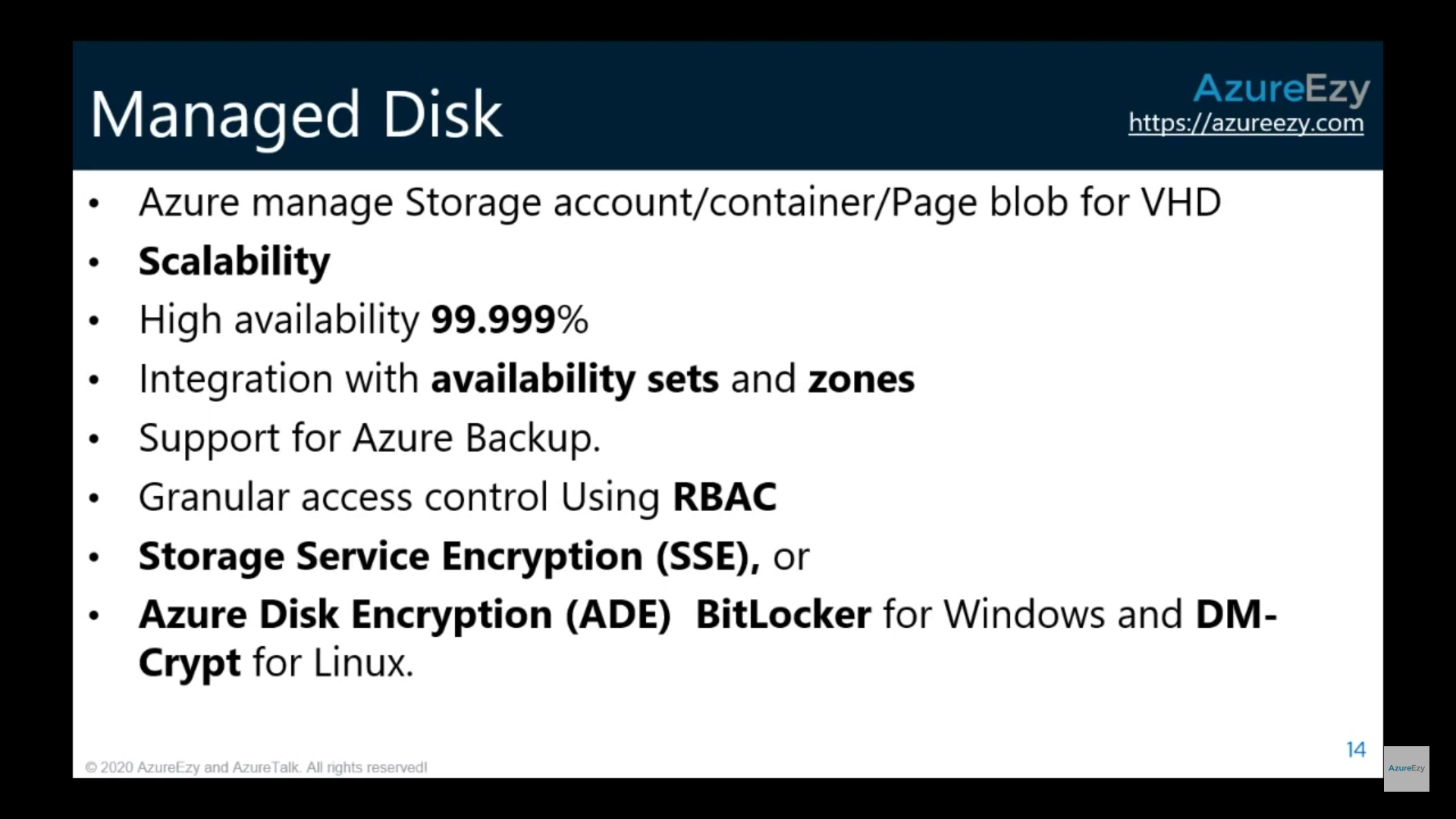
1. Images

Managed disks also support creating a managed custom image. You can create an image from your custom VHD in a storage account or directly from a generalized (sysprepped) VM. This process captures a single image. This image contains all managed disks associated with a VM, including both the OS and data disks. This managed custom image enables creating hundreds of VMs using your custom image without the need to copy or manage any storage accounts.

With managed disks, you can take an image of a generalized VM that has been deallocated. This image includes all of the disks attached to the VM. You can use this image to create a VM, and it includes all of the disks.

A snapshot is a copy of a disk at the point in time the snapshot is taken**. It applies only to one disk**. If you have a VM that has one disk (the OS disk), you can take a snapshot or an image of it and create a VM from either the snapshot or the image.

**A snapshot doesn't have awareness of any disk except the one it contains.**



## Disk roles

There are three main disk roles in Azure: the data disk, the OS disk, and the temporary disk. These roles map to disks that are attached to your virtual machine.



### OS Disk

Every virtual machine has one attached operating system disk. That OS disk has a pre-installed OS, which was selected when the VM was created. This disk contains the boot volume.

This disk has a maximum capacity of 4,095 GiB.

### Data Disk

A data disk is a managed disk that's attached to a virtual machine to store application data, or other data you need to keep. Data disks are registered as SCSI drives and are labeled with a letter that you choose. Each data disk has a maximum capacity of 32,767 gibibytes (GiB). The size of the virtual machine determines how many data disks you can attach to it and the type of storage you can use to host the disks.

### Temp Disk

Most VMs contain a temporary disk, which is not a managed disk. The temporary disk provides short-term storage for applications and processes, and is intended to only store data such as page or swap files. Data on the temporary disk may be lost during a maintenance event or when you redeploy a VM. During a successful standard reboot of the VM, data on the temporary disk will persist. For more information about VMs without temporary disks, see Azure VM sizes with no local temporary disk.

On Azure Linux VMs, the temporary disk is typically /dev/sdb and on Windows VMs the temporary disk is D: by default. The temporary disk is not encrypted by server side encryption unless you enable encryption at host.

## Disk Types and attach process

<https://docs.microsoft.com/en-us/azure/virtual-machines/disks-types>

how to attach a disk in linux

<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/attach-disk-portal>

<https://docs.microsoft.com/en-in/learn/modules/create-linux-virtual-machine-in-azure/>

# Azure Disk Encryption

### Terminology

| **Terminology** | **Definition** |
| --- | --- |
| Azure Key Vault | Key Vault is a cryptographic, key management service that's based on Federal Information Processing Standards (FIPS) validated hardware security modules. These standards help to safeguard your cryptographic keys and sensitive secrets. For more information, see the [Azure Key Vault](https://azure.microsoft.com/services/key-vault/) documentation and [Creating and configuring a key vault for Azure Disk Encryption](https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-key-vault). |
| DM-Crypt | [DM-Crypt](https://gitlab.com/cryptsetup/cryptsetup/wikis/DMCrypt) is the Linux-based, transparent disk-encryption subsystem that's used to enable disk encryption on Linux VMs. |
| Key encryption key (KEK) | The asymmetric key (RSA 2048) that you can use to protect or wrap the secret. You can provide a hardware security module (HSM)-protected key or software-protected key. For more information, see the [Azure Key Vault](https://azure.microsoft.com/services/key-vault/) documentation and [Creating and configuring a key vault for Azure Disk Encryption](https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-key-vault). |

<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-overview>

Azure Disk Encryption is not available on [Basic, A-series VMs](https://azure.microsoft.com/pricing/details/virtual-machines/series/), or on virtual machines that do not meet these minimum memory requirements:

| Supported VMs | |
| --- | --- |
| **Virtual machine** | **Minimum memory requirement** |
| Linux VMs when only encrypting data volumes | 2 GB |
| Linux VMs when encrypting both data and OS volumes, and where the root (/) file system usage is 4GB or less | 8 GB |
| Linux VMs when encrypting both data and OS volumes, and where the root (/) file system usage is greater than 4GB | **The root file system usage \* 2. For instance, a 16 GB of root file system usage requires at least 32GB of RAM** |

Once the OS disk encryption process is complete on Linux virtual machines, the VM can be configured to run with less memory.

| **Publisher** | **Offer** | **SKU** | **URN** | **Volume type supported for encryption** |
| --- | --- | --- | --- | --- |
| Canonical | Ubuntu | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:latest | OS and data disk |
| RedHat | RHEL 7.8 | 7.8 | RedHat:RHEL:7.8:latest | OS and data disk (see note below) |
| OpenLogic | CentOS 7.7 | 7.7 | OpenLogic:CentOS:7.7:latest | OS and data disk |
| SUSE | openSUSE 42.3 | 42.3 | SUSE:openSUSE-Leap:42.3:latest | Data disk only |
| SUSE | SLES 12-SP4 | 12-SP4 | SUSE:SLES:12-SP4:latest | Data disk only |

### VM Requirement for Encryption

Azure Disk Encryption requires the **dm-crypt and vfat modules** to be present on the system.

Before enabling encryption, the data disks to be encrypted must be properly listed in /etc/fstab.

If the /etc/fstab file doesn't mount the drive properly before enabling encryption, Azure Disk Encryption won't be able to mount it properly.

Before starting encryption, be sure to stop all services and processes that could be writing to mounted data disks and disable them, so that they do not restart automatically after a reboot. These could keep files open on these partitions, preventing the encryption procedure to remount them, causing failure of the encryption.

## Azure Backup

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-introduction>

<https://www.youtube.com/watch?v=NpAc1XFdkJM>

### implement Azure Backup for VMs

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-arm-vms-prepare>

Create your backup service vault in the same region where your VMs are.

# VM Cli

<https://docs.microsoft.com/en-us/cli/azure/vm?view=azure-cli-latest>

# VM Power Shell

### NetworkWatcherRG

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-create>

# Tasks :

## Add disks

## Add NIC Card/network interfaces

# FAQ

<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/faq>

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/faq>

## Azure VM sizes with no local temporary disk

1. Can I resize a VM size that has a local temp disk to a VM size with no local temp disk?

No. The only combinations allowed for resizing are:

1. VM (with local temp disk) -> VM (with local temp disk); and
2. VM (with no local temp disk) -> VM (with no local temp disk).
3. Do these VM sizes support both Linux and Windows Operating Systems (OS)?

Yes.

1. Will this break my custom scripts, custom images or OS images that have scratch files or page files on a local temp disk?

If the custom OS image points to the local temp disk, the image might not work correctly with this diskless size.