BUILDING AZURE IAAS-BASED SERVER APPLICATIONS

MODULE OVERVIEW

- HIGH AVAILABILITY
- TEMPLATED INFRASTRUCTURE
- DOMAIN-JOINED VIRTUAL MACHINES

HIGH AVAILABILITY

HIGH AVAILABILITY

- AZURE AVAILABILITY
- AVAILABILITY SETS
- AVAILABILITY ZONES

AZURE AVAILABILITY

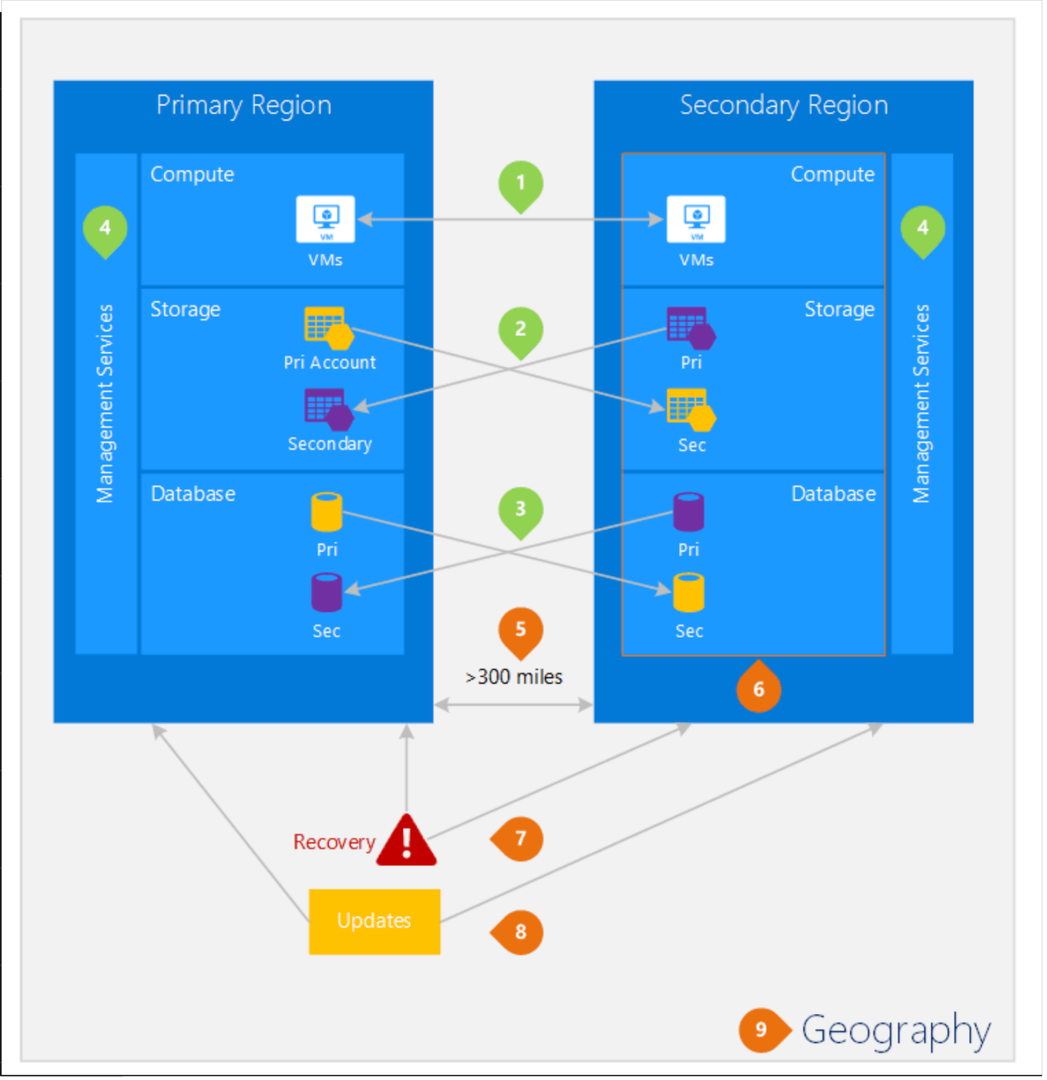
- Most of the resources in Azure has at least **99,9%**, if not stated differently:
https://azure.microsoft.com/pl-pl/support/legal/sla/summary/

- Azure provides money-backed SLAs for IaaS services:
  - Two Instances or more in an Availability Set = **99.95%**
  - Single Instance VM using Premium Storage = **99.9%**
  - Two or more instances in an Availability Zone = **99.99%**

- Decisions should based on cost and availability requirements

AZURE AVAILABILITY – REGIONS AND PAIRS

Geography	Paired regions	
Asia	East Asia	Southeast Asia
Australia	Australia East	Australia Southeast
Australia	Australia Central	Australia Central 2
Brazil	Brazil South 2	South Central US
Canada	Canada Central	Canada East
China	China North	China East
Europe	North Europe	West Europe
France	France Central	France South
Germany	Germany Central	Germany Northeast
India	Central India	South India



AZURE AVAILABILITY

- Most of the resources in Azure has at least **99,9%**, if not stated differently:
https://azure.microsoft.com/pl-pl/support/legal/sla/summary/

- Azure provides money-backed SLAs for IaaS services:
  - Two Instances or more in an Availability Set = **99.95%**
  - Single Instance VM using Premium Storage = **99.9%**
  - Two or more instances in an Availability Zone = **99.99%**

- Decisions should based on cost and availability requirements

AZURE AVAILABILITY – HOW IT WORKS

"**Monthly Uptime Percentage**" for Virtual Machines in Availability Zones is calculated as Maximum Available Minutes less Downtime divided by Maximum Available Minutes in a billing month for a given Microsoft Azure subscription. Monthly Uptime Percentage is represented by the following formula:

Monthly Uptime % = (Maximum Available Minutes – Downtime) / Maximum Available Minutes X 100

The following Service Levels and Service Credits are applicable to Customer's use of Virtual Machines, deployed across two or more Availability Zones in the same region:

MONTHLY UPTIME PERCENTAGE	SERVICE CREDIT
< 99.99%	10%
< 99%	25%
< 95%	100%

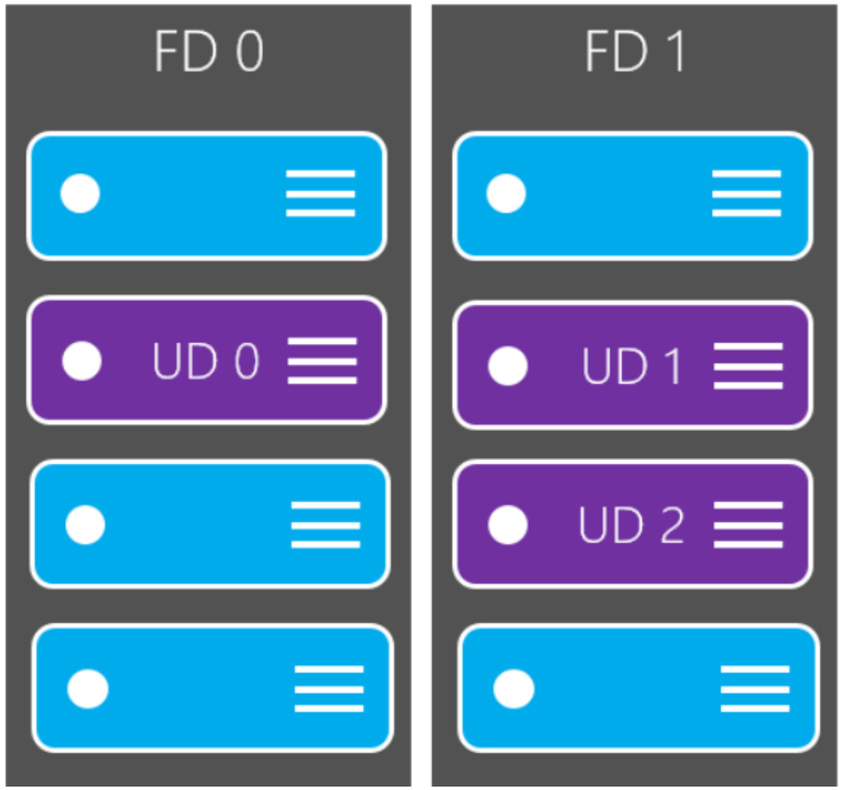
SINGLE VM SLA

- Single instance VM would gain **99.9%** SLA if it complies with:
  - Premium Storage for all Operating System Disks
  - Data Disks

- Any single instance VM without Premium storage receives no SLA

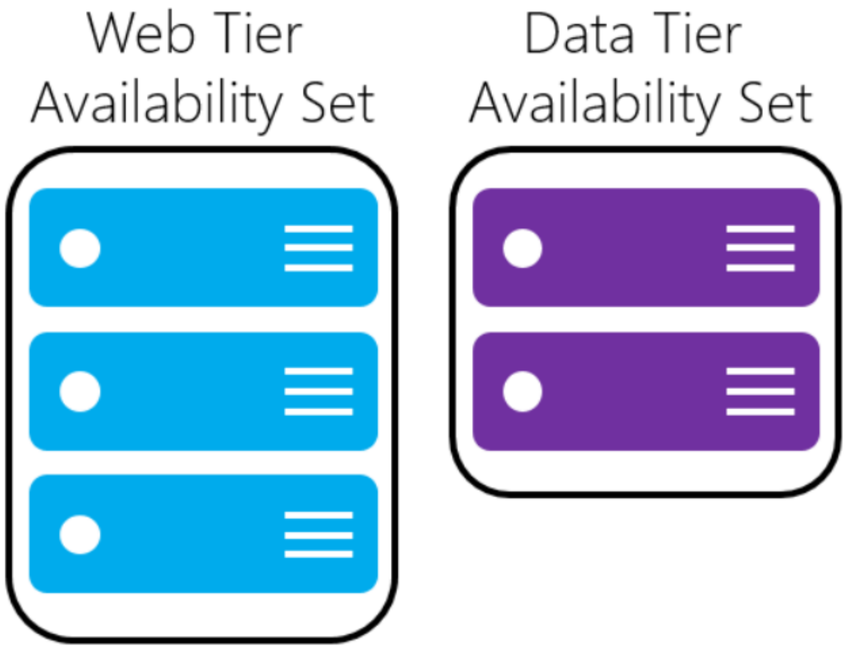
AVAILABILITY SETS

- Availability Sets provide assurance that any multiple instance VM will be available 99.95% of the time
- Availability Sets cater for planned and unplanned maintenance using Update Domains and Fault Domains
- You can have up to 5 Fault Domain.
- **Be careful** – the number can be different between regions, even between pair regions. (CANADA CENTRAL / CANADA EAST). With Azure Site Recovery this becomes super important.

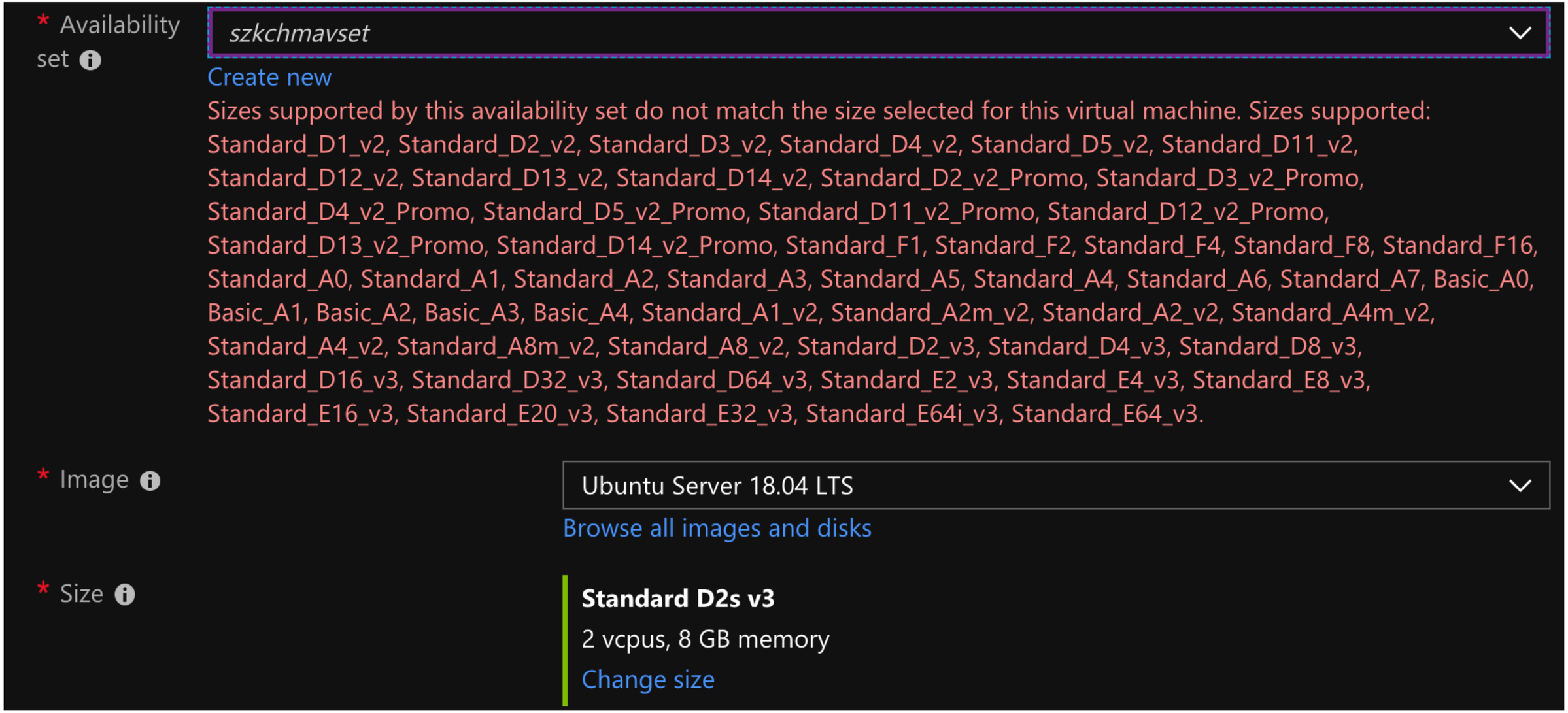


AVAILABILITY SETS

- When planning multiple tier applications use multiple Availability sets, one per tier
- Crucial thing is, you can add the machine to AV SET only during creation time, **afterwards, you have to recreate VM**
- Moreover, you can have machines in the Availability Set only with the same Disk Type. **Either Standard HDD or Premium SSD, you cannot mix them.**



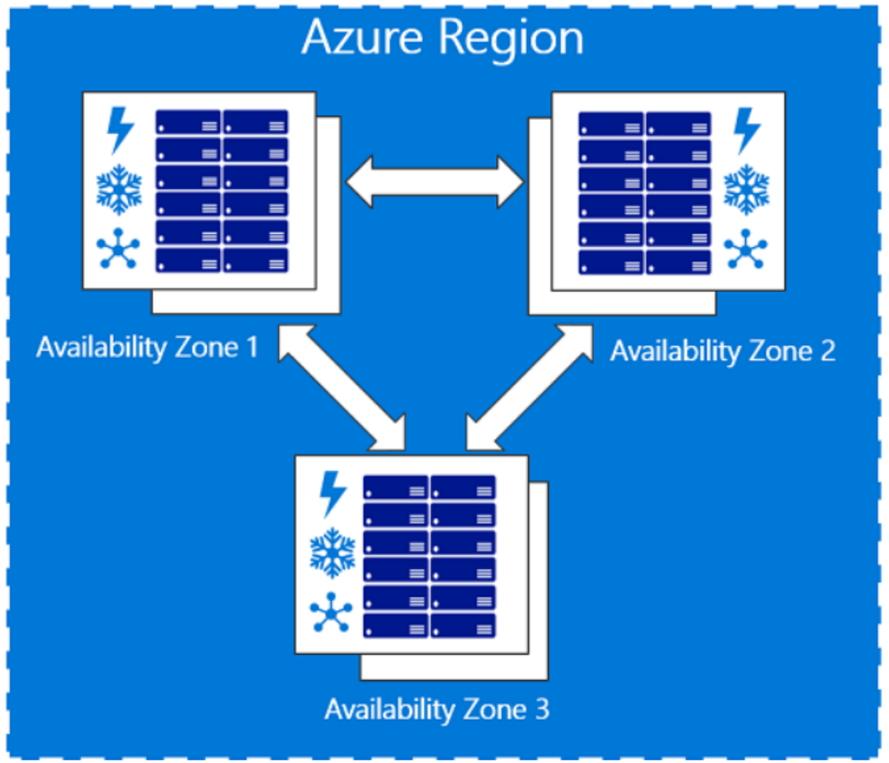
AVAILABILITY SETS – LOOKOUT FOR DISKS TYPE



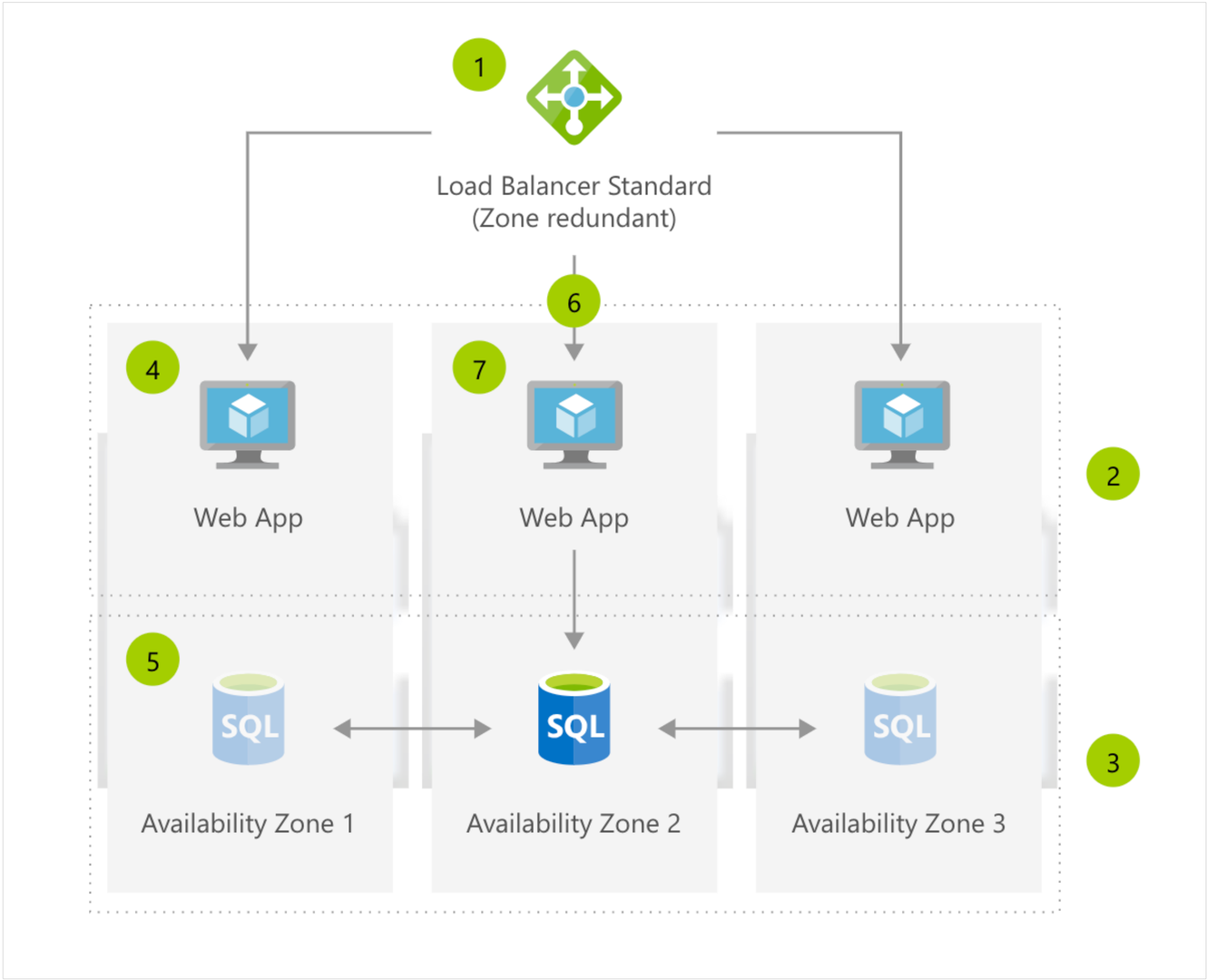
AVAILABILITY ZONES

- Service helps to protect resources from datacenter level failures

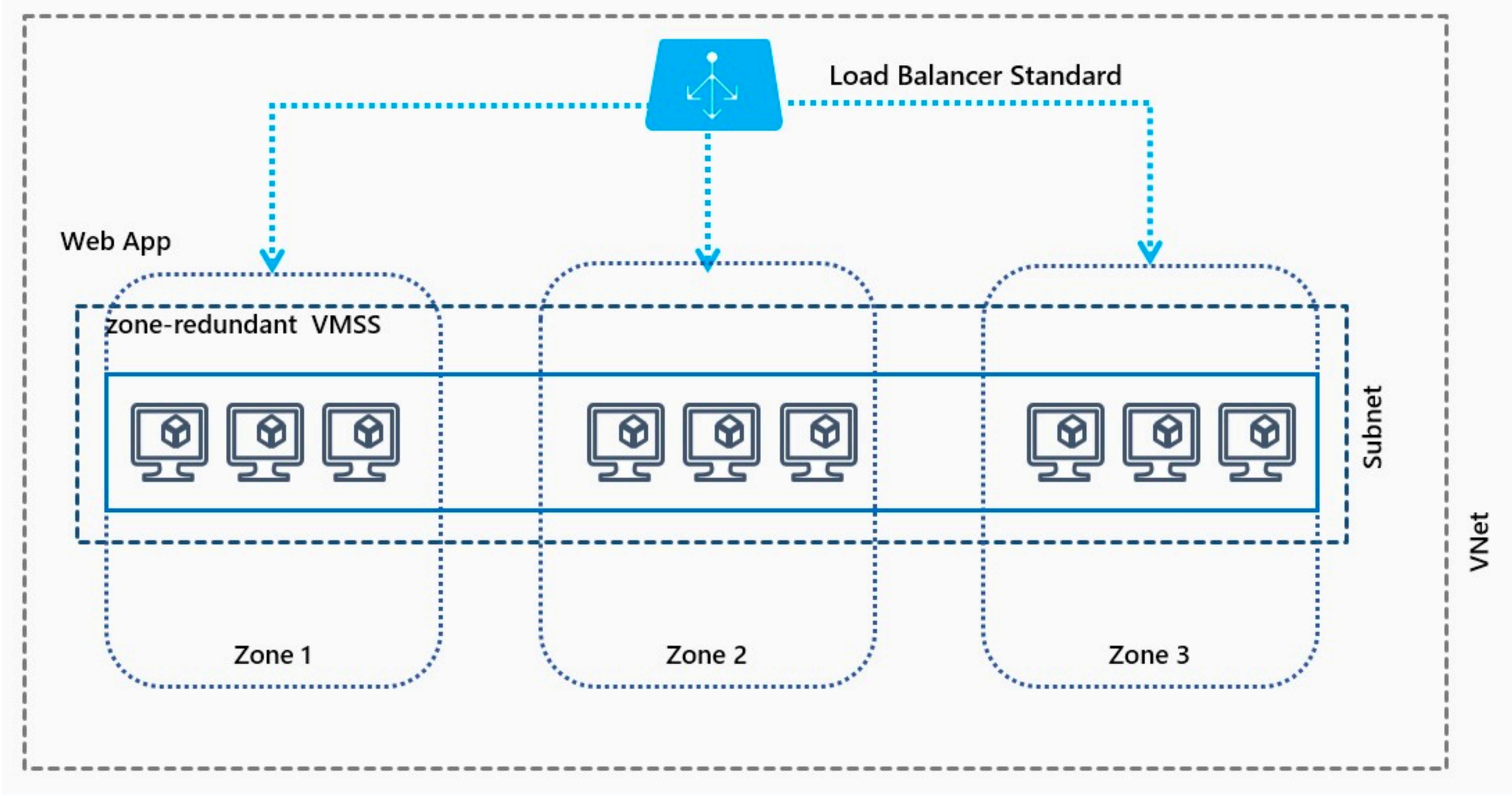
- Provides the ability to place VMs with resilience to the loss of an entire Datacentre building. These are all located within the same Azure region



AVAILABILITY ZONES - ARCHITECTURE

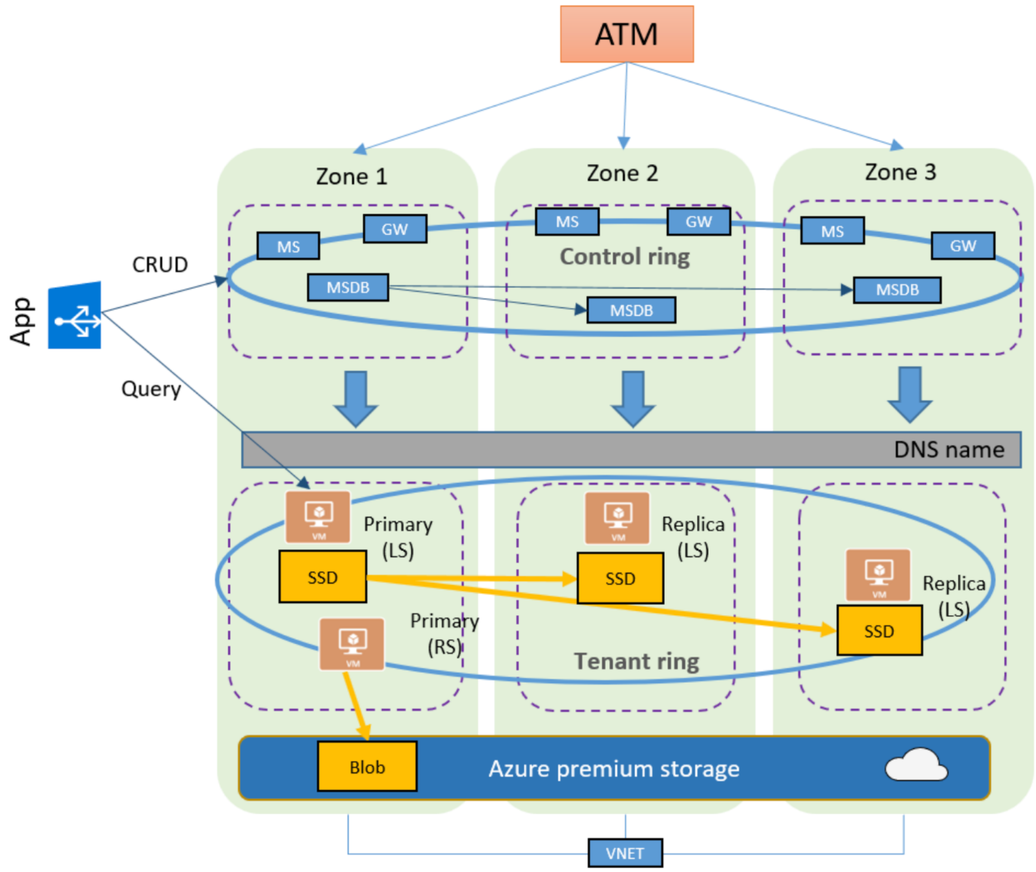


AVAILABILITY ZONES - ARCHITECTURE



AVAILABILITY ZONES – ARCHITECTURE – AZURE SQL

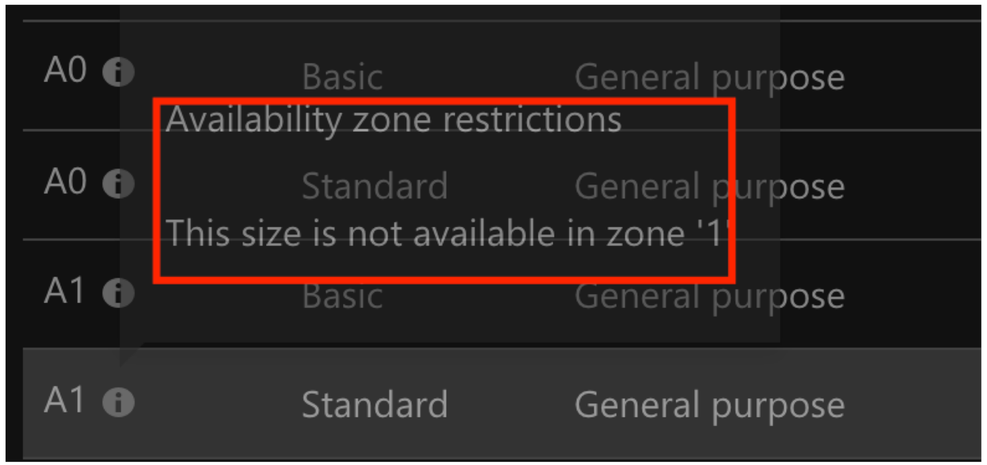
The zone redundant version of the high availability architecture is illustrated by the following diagram:



AVAILABILITY ZONES – BE CAREFUL

Regions that support Availability Zones

- Central US
- East US 2 (Preview)
- France Central
- North Europe
- Southeast Asia (Preview)
- West Europe
- West US 2



Services that support Availability Zones

The Azure services that support Availability Zones are:

- Linux Virtual Machines
- Windows Virtual Machines
- Virtual Machine Scale Sets
- Managed Disks
- Load Balancer
- Public IP address
- Zone-redundant storage
- SQL Database
- Event Hubs
- Service Bus
- VPN Gateway
- ExpressRoute

AVAILABILITY ZONES – BE CAREFUL – PRICING

Availability Zones*

Inbound data transfers

(i.e. data going into VM deployed in an availability zone): **€0.009 per GB**[1]

Outbound data transfers

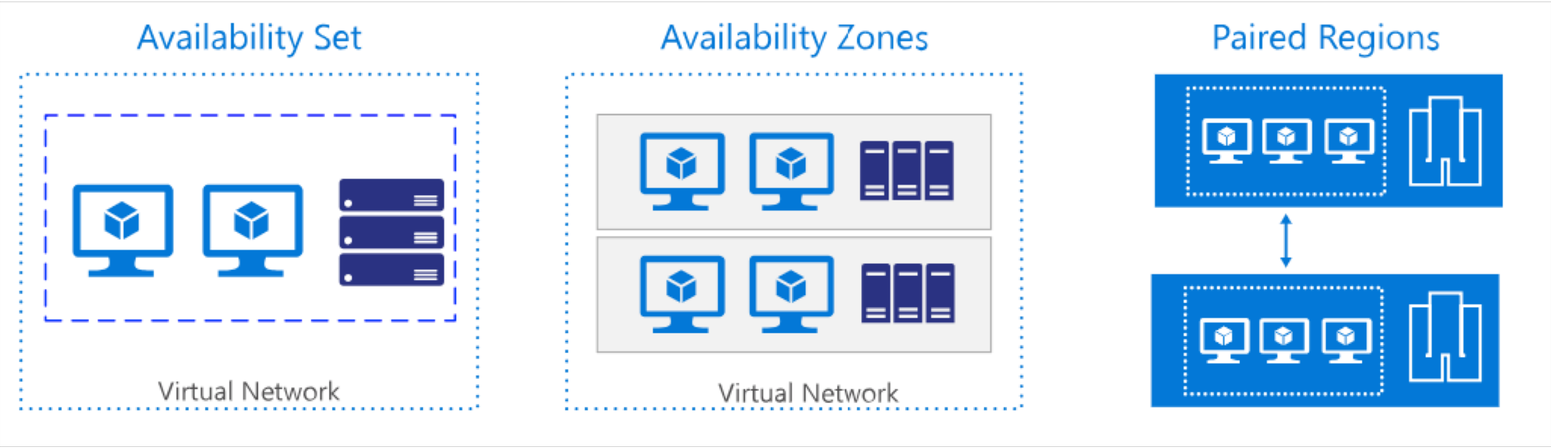
(i.e. data going out of VM deployed in an availability zone): **€0.009 per GB**[1]

*Availability Zone data transfer pricing is only applicable to VNet resources which have been deployed in an Availability Zone by the customer. See FAQs for details.

[1]Availability Zones are generally available. Availability Zone Data Transfer billing will start on 1 February 2019. Usage prior to 1 February 2019 will not be billed.

HIGH AVAILABILITY - DEMO

„DESIGN FOR FAILURE”



	Availability Set	Availability Zone	Paired region
Scope of failure	Rack	Datacenter	Region
Request routing	Load Balancer	Cross-zone Load Balancer	Traffic Manager
Network latency	Very low	Low	Mid to high
Virtual network	VNet	VNet	Cross-region VNet peering

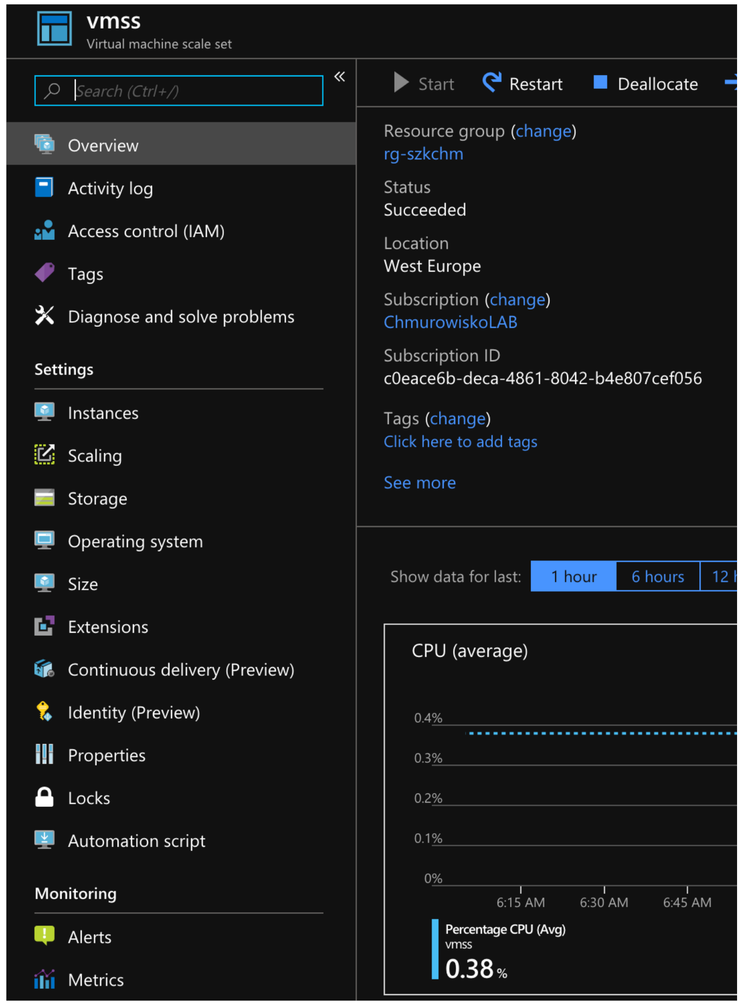
HIGH AVAILABILITY - SUMMARY

- AZURE AVAILABILITY
- AVAILABILITY SETS
- AVAILABILITY ZONES

TEMPLATED INFRASTRUCTURE

VIRTUAL MACHINE SCALE SET

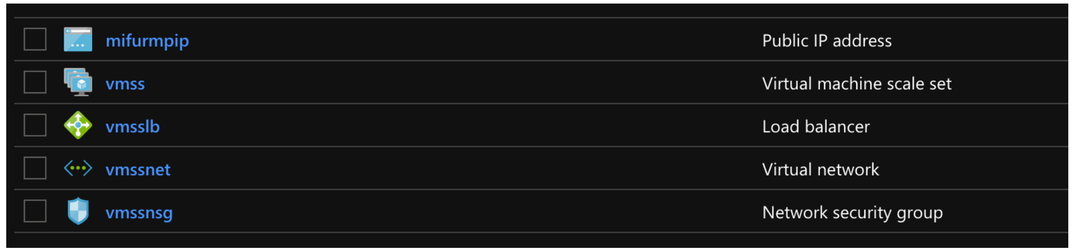
- ARM TEMPLATES ARE THE BEST OPTION TO TEMPLATE THE WHOLE SOLUTION IN AZURE AT THE MOMENT
- IF YOU NEED MASSIVE COMPUTING INSTEAD OF CREATING PLENTY MACHINES IN TEMPLATE YOU CAN USE SCALE SET
- IF YOU NEED:
  - lot’s of resources managed as one
  - require autoscaling
  - simplified networking management (Load Balancer or AppGW managed by Scale Set)
  - simplified CI/CD process for Virtual Machines
- AZURE USE SCALE SET FOR CONTAINERS, WEB FRONT ENDS, SERVICE FABRIC, HD INSIGHTS



VIRTUAL MACHINE SCALE SET

SCALE SETS HAVE A NUMBER OF FEATURES:

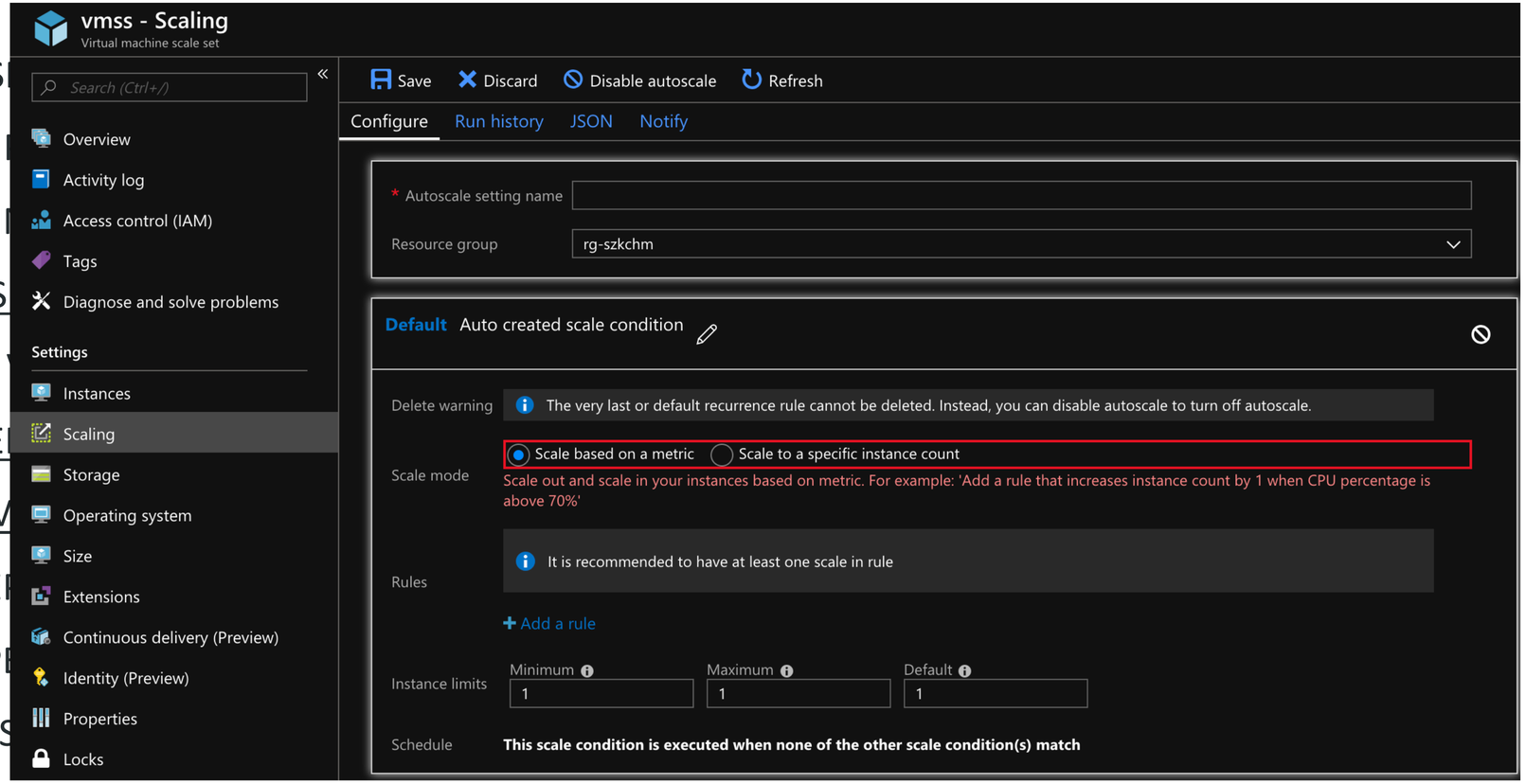
- DEPLOYABLE WITH JSON TEMPLATES JUST LIKE VMS
- CAN USE AZURE AUTO-SCALE
- NO REQUIREMENT TO PRE-PROVISION
- LOAD BALANCER CREATION, APPGW CREATION
- NAT INCLUDED



VIRTUAL MACHINE SCALE SET VS. VM

SCALE SETS:

- ONCE YOU S
  "CAPACITY"
  THAN WRITI
- YOU CAN US
  INDIVIDUAL
- YOU CAN RE
- YOU CAN OV
  QUICKER DE
- YOU CAN SP
  ACROSS VMS



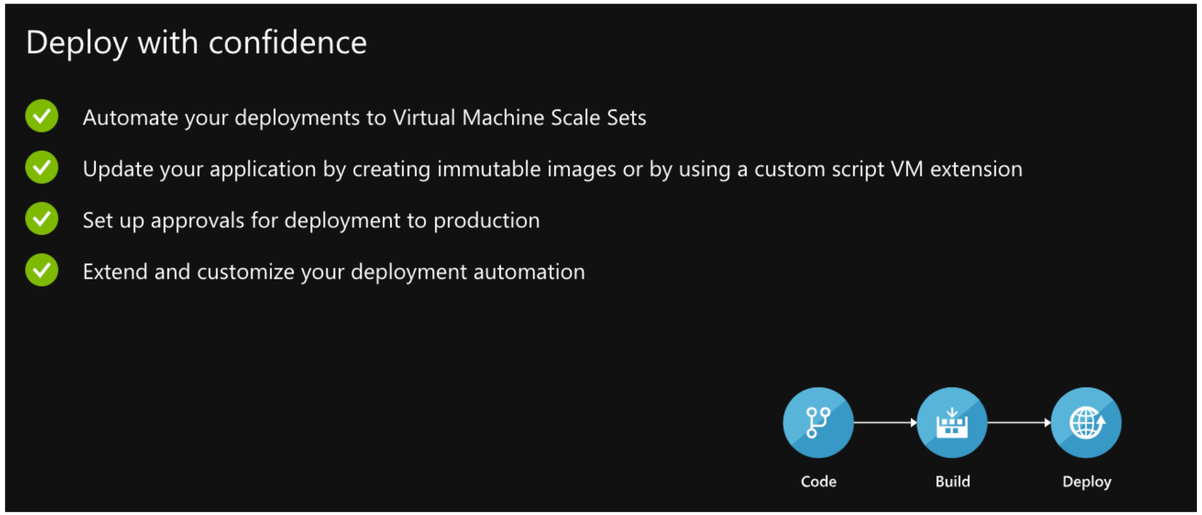
VIRTUAL MACHINE SCALE SET VS. VM

VMS:

- YOU CAN ATTACH DATA DISKS TO SPECIFIC INDIVIDUAL VMS, BUT ATTACHED DATA DISKS ARE CONFIGURED FOR ALL VMS IN A SCALE SET.
- YOU CAN ATTACH NON-EMPTY DATA DISKS TO INDIVIDUAL VMS BUT NOT VMS IN A SCALE SET.
- YOU CAN SNAPSHOT AN INDIVIDUAL VM BUT NOT A VM IN A SCALE SET.
- YOU CAN CAPTURE AN IMAGE FROM AN INDIVIDUAL VM BUT NOT FROM A VM IN A SCALE SET.
- YOU CAN MIGRATE AN INDIVIDUAL VM FROM NATIVE DISKS TO MANAGED DISKS, BUT YOU CANNOT DO THIS FOR VMS IN A SCALE SET.
- YOU CAN ASSIGN IPV6 PUBLIC IP ADDRESSES TO INDIVIDUAL VM NICS BUT CANNOT DO SO FOR VMS IN A SCALE SET. NOTE THAT YOU CAN ASSIGN IPV6 PUBLIC IP ADDRESSES TO LOAD BALANCERS IN FRONT OF EITHER INDIVIDUAL VMS OR SCALE SET VMS.

VIRTUAL MACHINE SCALE SET VS. VM

- CONNECT TO AN INSTANCE OF A VM USING RDP THROUGH THE LOAD BALANCER, YOU CAN CONNECT TO ANY VM
- USE CONTINUOUS DELIVERY TO MAINTAIN AN APPLICATION IN A VMSS WITH AZURE DEVOPS (IN THE PAST: VSTS)
- USING MANAGED DISKS REMOVES STORAGE ACCOUNT CONSIDERATIONS FROM SCALE SET CREATION – NOW YOU CAN SCALE UP TO 1000 VM'S IN SCALE SET



VIRTUAL MACHINE SCALE SET – LARGE DEPLOYMENTS

LARGE SCALE SETS OVER 100 VMS USE PLACEMENT GROUPS – THESE CHANGE LOAD BALANCING AND FAULT DOMAIN CHARACTERISTICS:

- MANAGED DISKS
- MARKETPLACE IMAGES SCALE TO 1,000 VMS
- CUSTOM IMAGES SCALE TO 300 VMS. BE CAREFUL!
- ENSURE AVAILABLE IP ADDRESSES IN SUBNET
- ENSURE YOUR COMPUTE LIMITS ARE HIGH ENOUGH
- FAULT DOMAINS RELATE TO A SINGLE PLACEMENT GROUP

VIRTUAL MACHINE SCALE SET – YOUR OWN IMAGE

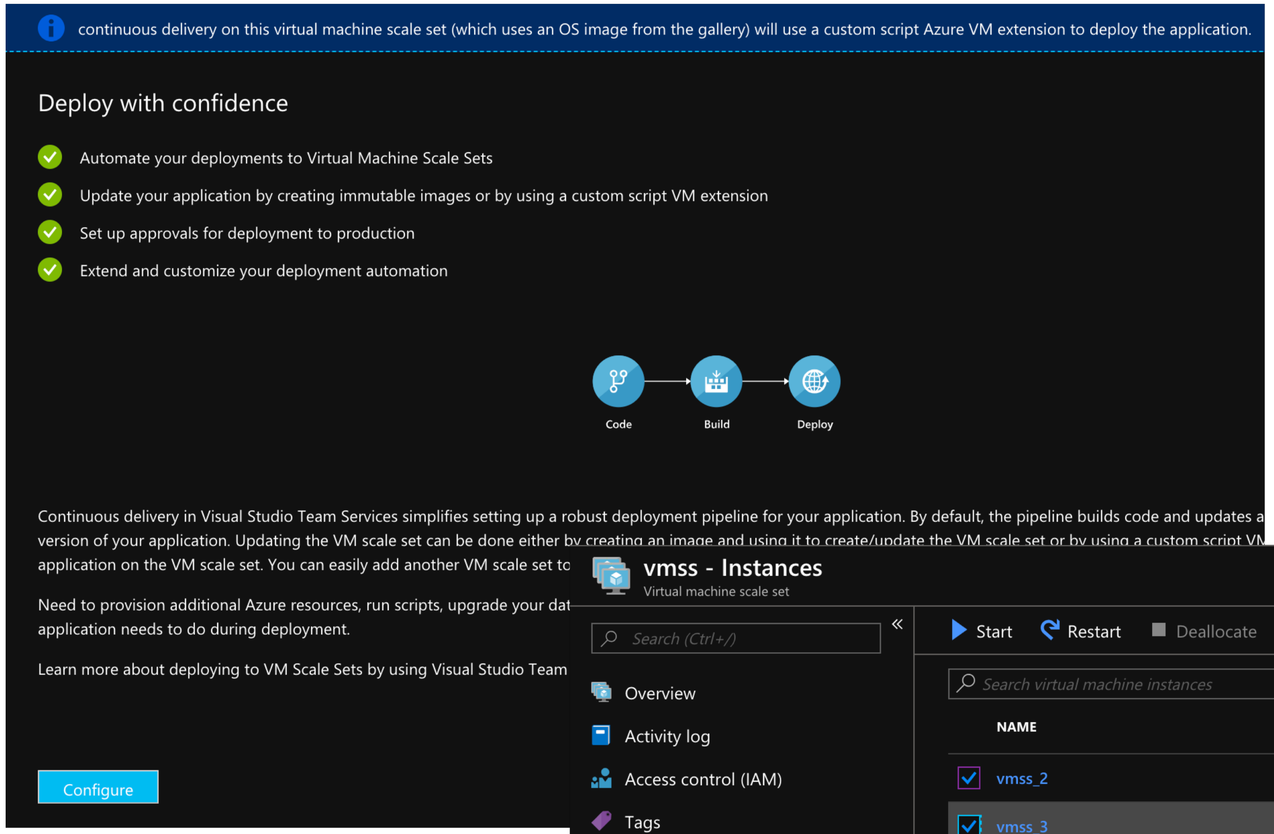
```
michal@Azure:~$ az vm create -n imageVM03 -l westeurope -g imageRG --size Standard_D1 --use-unmanaged-disk --admin-username mifurm --admin-password [redacted] --image UbuntuLTS --storage-sku Standard_LRS
{
  "fqdns": "",
  "id": "/subscriptions/c6484eee-b936-412a-94d6-8dc1b4386bc2/resourceGroups/imageRG/providers/Microsoft.Compute/virtualMachines/imageVM03",
  "location": "westeurope",
  "macAddress": "00-0D-3A-2B-59-14",
  "powerState": "VM running",
  "privateIpAddress": "10.0.0.4",
  "publicIpAddress": "52.166.63.169",
  "resourceGroup": "imageRG",
  "zones": ""
}
michal@Azure:~$ ssh mifurm@52.166.63.169
The authenticity of host '52.166.63.169 (52.166.63.169)' can't be established.
```

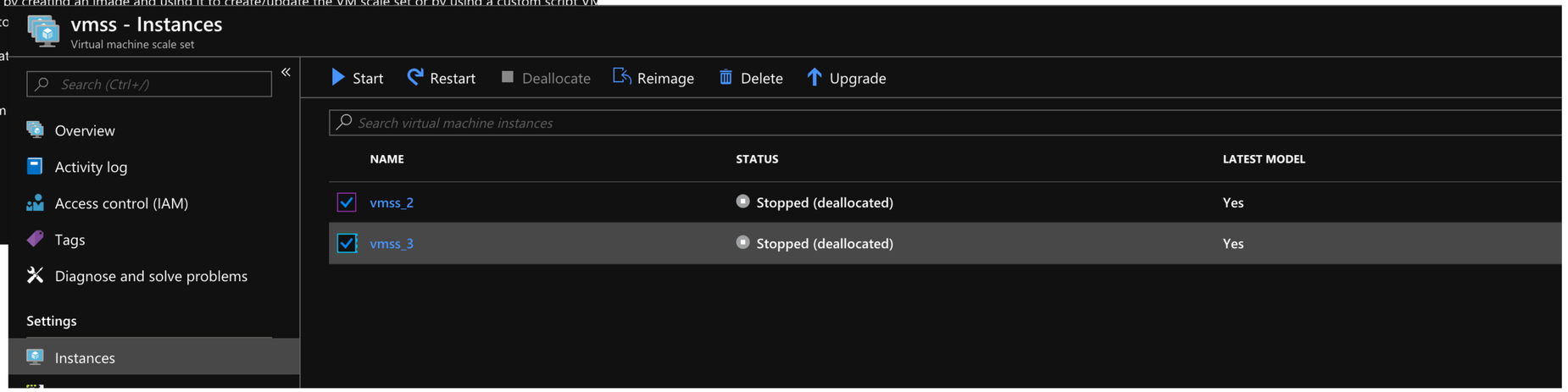
```
mifurm@imageVM03:~$ sudo waagent -deprovision+user -force
WARNING! The waagent service will be stopped.
WARNING! Cached DHCP leases will be deleted.
WARNING! root password will be disabled. You will not be able to login as root.
WARNING! /etc/resolvconf/resolv.conf.d/tail and /etc/resolvconf/resolv.conf.d/original will be deleted.
WARNING! mifurm account and entire home directory will be deleted.
mifurm@imageVM03:~$ exit
logout
Connection to 52.166.63.169 closed.
michal@Azure:~$ az vm deallocate -g imageRG -n imageVM03
{
  "endTime": "2017-10-01T10:52:50.587741+00:00",
  "error": null,
  "name": "c986c1c3-9ebb-4213-ae3b-388c92add7f8",
  "startTime": "2017-10-01T10:51:49.759547+00:00",
  "status": "Succeeded"
}
```

```
michal@Azure:~$ az vm generalize -g imageRG -n imageVM03
```

```
michal@Azure:~$ az vmss create -n chat-vmss-dev -l westeurope -g chat-vmss-dev-rg --use-unmanaged-disk --instance-count 1 --image "htt
pe linux --authentication-type password --admin-username mifurm --admin-password [redacted]
{
  "vmss": {
    "overprovision": true,
    "provisioningState": "Succeeded",
    "singlePlacementGroup": true,
    "uniqueId": "bd8d30a6-2674-49cf-a4e7-4597c39f78f6",
    "upgradePolicy": {
      "automaticOSUpgrade": false,
      "mode": "Manual"
    },
    "virtualMachineProfile": {
      "networkProfile": {
        "networkInterfaceConfigurations": [
          {
            "name": "chatv2f08Nic",
            "properties": {
              "dnsSettings": {
                "dnsServers": []
              },
              "enableAcceleratedNetworking": false,
              "ipConfigurations": [
                {
                  "name": "chatv2f08IPConfig",
                  "properties": {
                    "loadBalancerBackendAddressPools": [
                      {
                        "id": "/subscriptions/c6484eee-b936-412a-94d6-8dc1b4386bc2/resourceGroups/chat-vmss-dev-rg/providers/Microsoft
                        "resourceGroup": "chat-vmss-dev-rg"
                      }
                    ]
```

VIRTUAL MACHINE SCALE SET – YOUR OWN IMAGE





SZKOŁA CHMURY

Chmurowisko

VIRTUAL MACHINE SCALE SET – SUMMARY

- IF YOU ARE STILL USING VMS HAVE A LOOK IF SCALE SET CAN HELP YOU. IN MANY PLACES THEY CAN.
- EASY TO CREATE, UPDATE AND SCALE BUT YOU MUST BE SURE, TO HAVE ALL VMS WITH THE SAME CONFIGURATION
- GREAT FOR WEB FRONT ENDS OR BACKENDS

DOMAIN JOINED VIRTUAL MACHINE

DOMAIN JOINED VIRTUAL MACHINE

- DOMAIN AND IAAS APPLICATIONS
- HYBRID CONNECTIVITY
- AZURE AD DOMAIN SERVICES

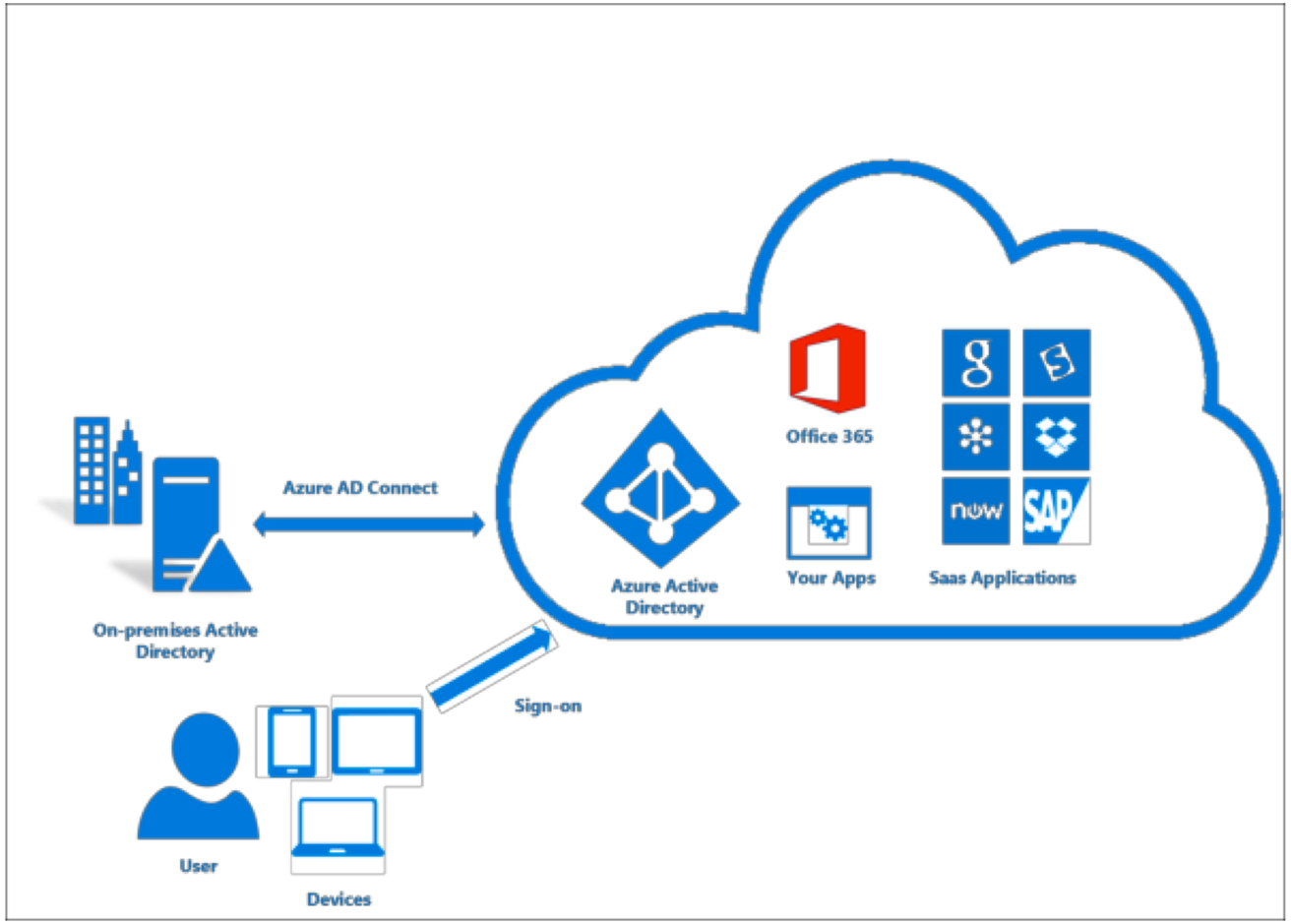
IAAS APPLICATION AND DOMAIN – PLENTY OF OPTIONS

THERE IS NO SIMPLE OPTION – IT STRONGLY DEPENDS ON WHAT REALLY YOU WOULD LIKE TO DO:

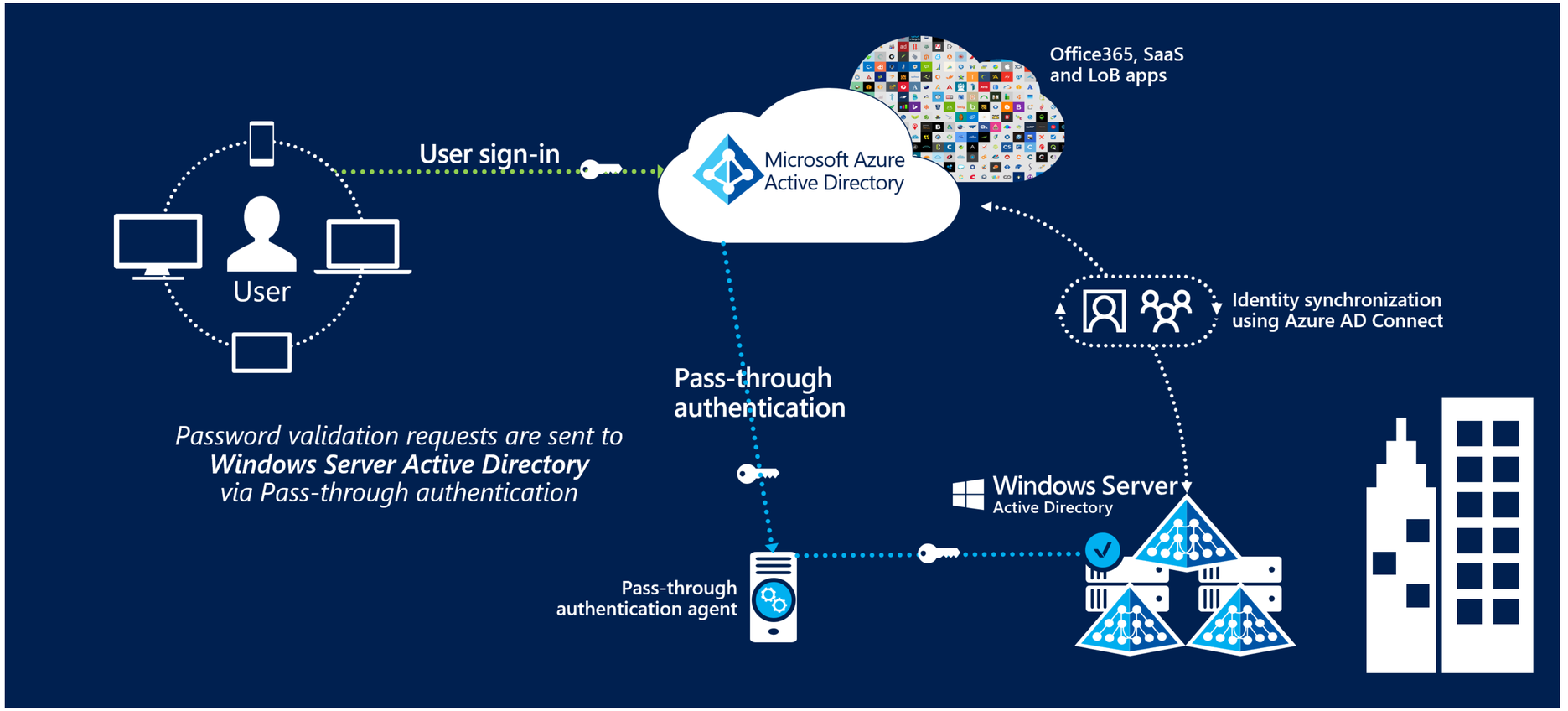
- AZURE ACTIVE DIRECTORY, AAD BUSINES2BUSINESS AND AAD BUSINESS2CONSUMER
- HYBRID ACTIVE DIRECTORY DOMAIN SERVICE AND AZURE AD
- AZURE AD DOMAIN SERVICES

HYBRID CONNECTIVITY

- AZURE AD CONNECT
- ACTIVE DIRECTORY FEDERATION SERVICES – ADFS
- AD CONNECT PASSTHROUGH
- ACTIVE DIRECTORY DOMAIN SERVICES IN AZURE VM



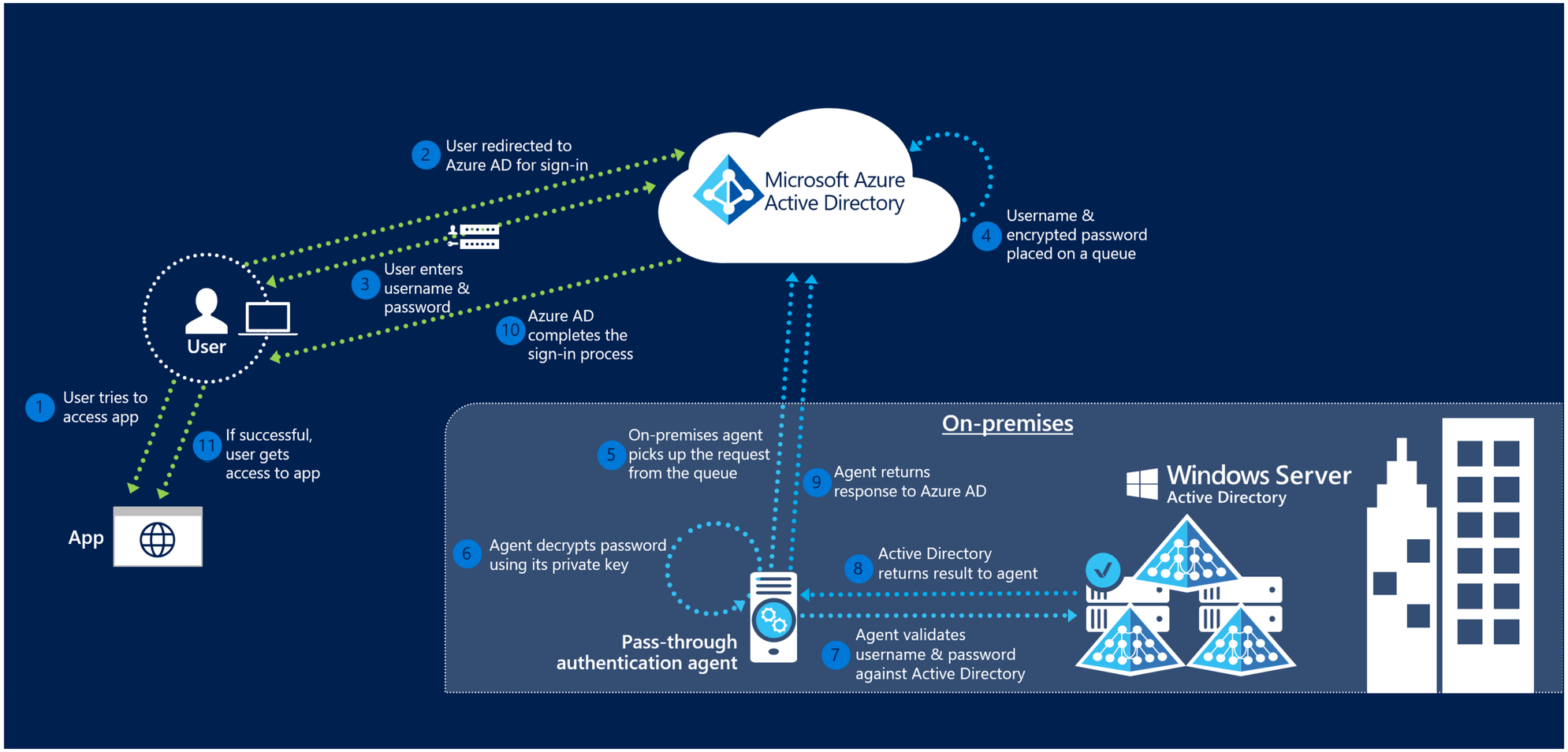
PASSTHROUGH VS ADFS



PASSTHROUGH VS ADFS

- **GREAT UX** – SAME PASSWORD TO SIGN ON-PREM AND CLOUD
- **EASY TO DEPLOY AND MANAGE** – ONE COMPONENT AND AGENT ON-PREM
- **SECURITY** – USER PASSWORDS ARE NEVER STORED IN CLOUD, AGENT MAKES OUTBOUND CONNECTIVITY FROM YOU NETWORK, NO DMZ INVOLVED
- **LOTS OF FEATURES** - WORKS FINE WITH AZURE AD CONDITIONAL ACCESS, MFA AND SECURITY OPTIONS IN AZURE (DETECTING BRUTE FORCE ATTACKS)
- **HIGHLY AVAILABLE** – YOU CAN INSTALL AD CONNECT ON MANY SERVERS

PASSTHROUGH VS ADFS

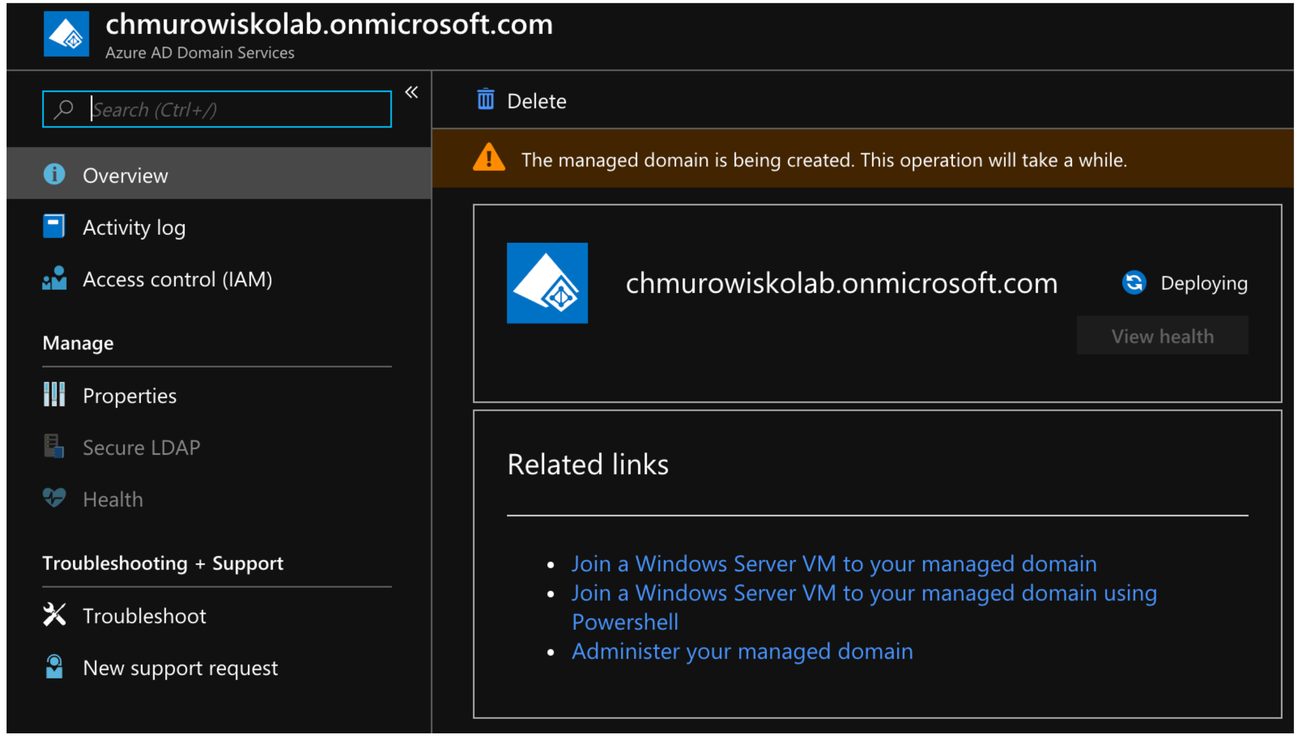


AZURE AD DOMAIN SERVICES

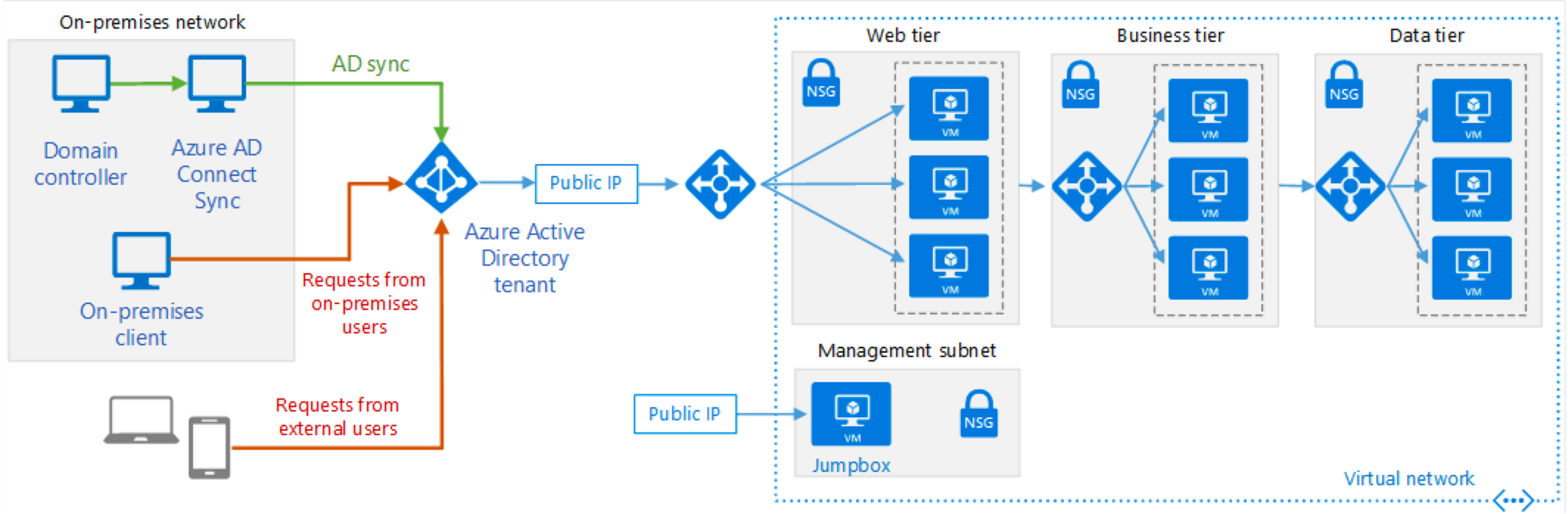
AZURE AD DOMAIN SERVICES INTEGRATES WITH OTHER HYBRID SCENARIOS OR WORKS AS A CLOUD ONLY SOLUTION.

THE BENEFITS ARE:

- **SIMPLICITY** – FEW CLICKS TO SETUP
- **INTEGRATED** – DEEP AZURE AD INTEGRATION
- **COMPATIBLE** – WINDOWS SERVER AD
- **COST-EFFECTIVE** – READY TO USE SERVICE



WHEN TO CHOOSE WHAT? INTEGRATE ON-PREM AD



WHEN TO CHOOSE WHAT?

HTTPS://DOCS.MICROSOFT.COM/EN-GB/AZURE/ARCHITECTURE/REFERENCE-ARCHITECTURES/IDENTITY/

Integrate your on-premises domains with Azure AD

Use Azure Active Directory (Azure AD) to create a domain in Azure and link it to an on-premises AD domain.

The Azure AD directory is not an extension of an on-premises directory. Rather, it's a copy that contains the same objects and identities. Changes made to these items on-premises are copied to Azure AD, but changes made in Azure AD are not replicated back to the on-premises domain.

You can also use Azure AD without using an on-premises directory. In this case, Azure AD acts as the primary source of all identity information, rather than containing data replicated from an on-premises directory.

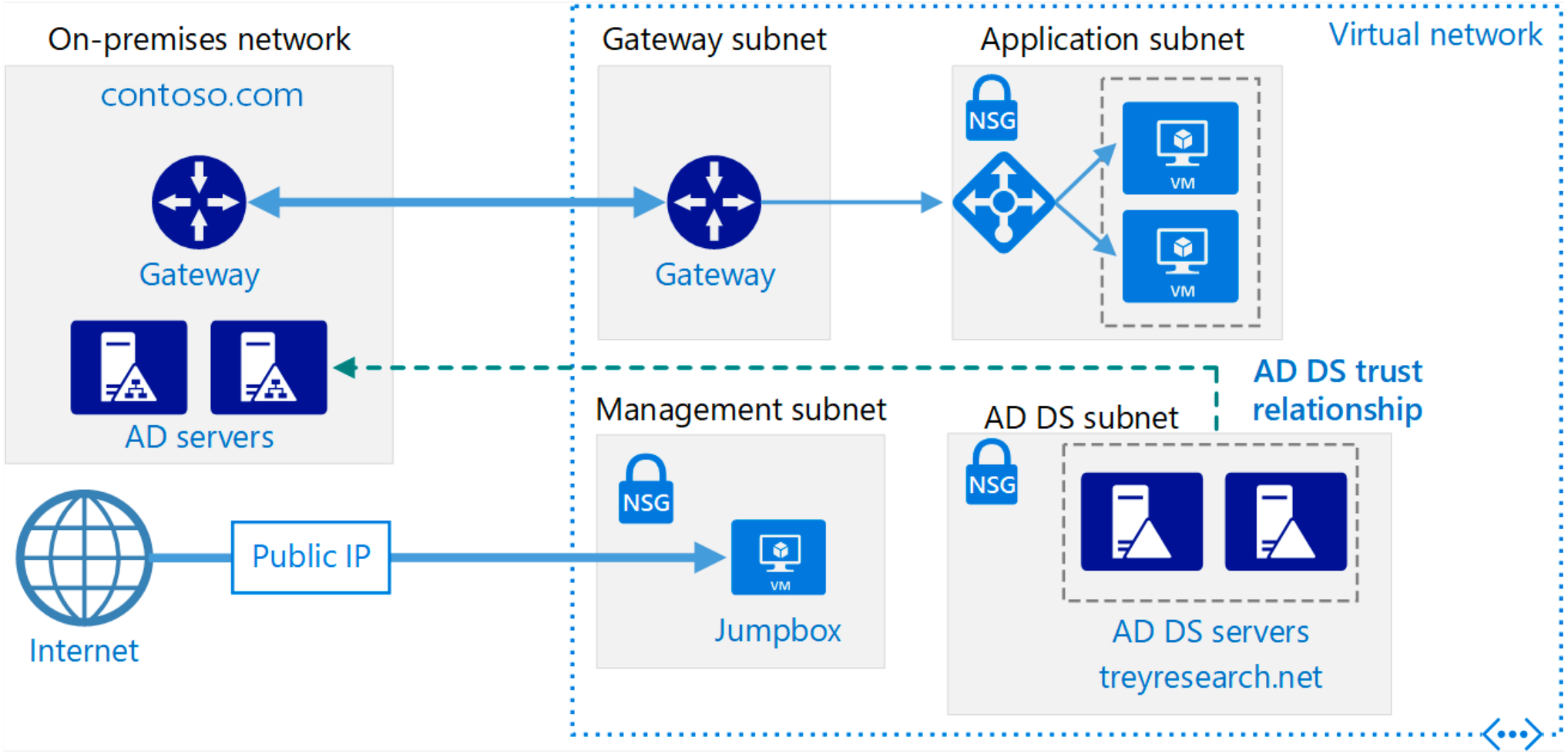
Benefits

- You don't need to maintain an AD infrastructure in the cloud. Azure AD is entirely managed and maintained by Microsoft.
- Azure AD provides the same identity information that is available on-premises.
- Authentication can happen in Azure, reducing the need for external applications and users to contact the on-premises domain.

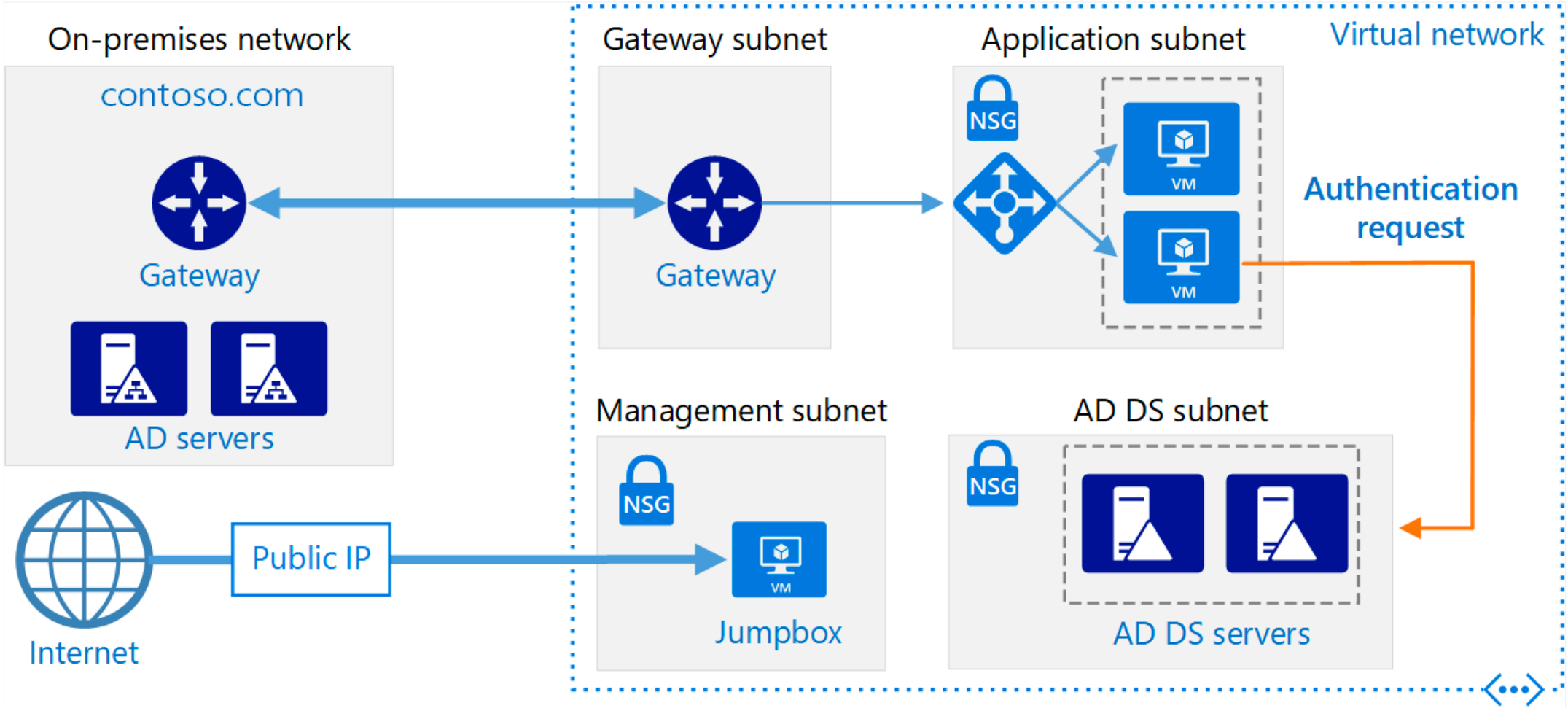
Challenges

- Identity services are limited to users and groups. There is no ability to authenticate service and computer accounts.
- You must configure connectivity with your on-premises domain to keep the Azure AD directory synchronized.
- Applications may need to be rewritten to enable authentication through Azure AD.

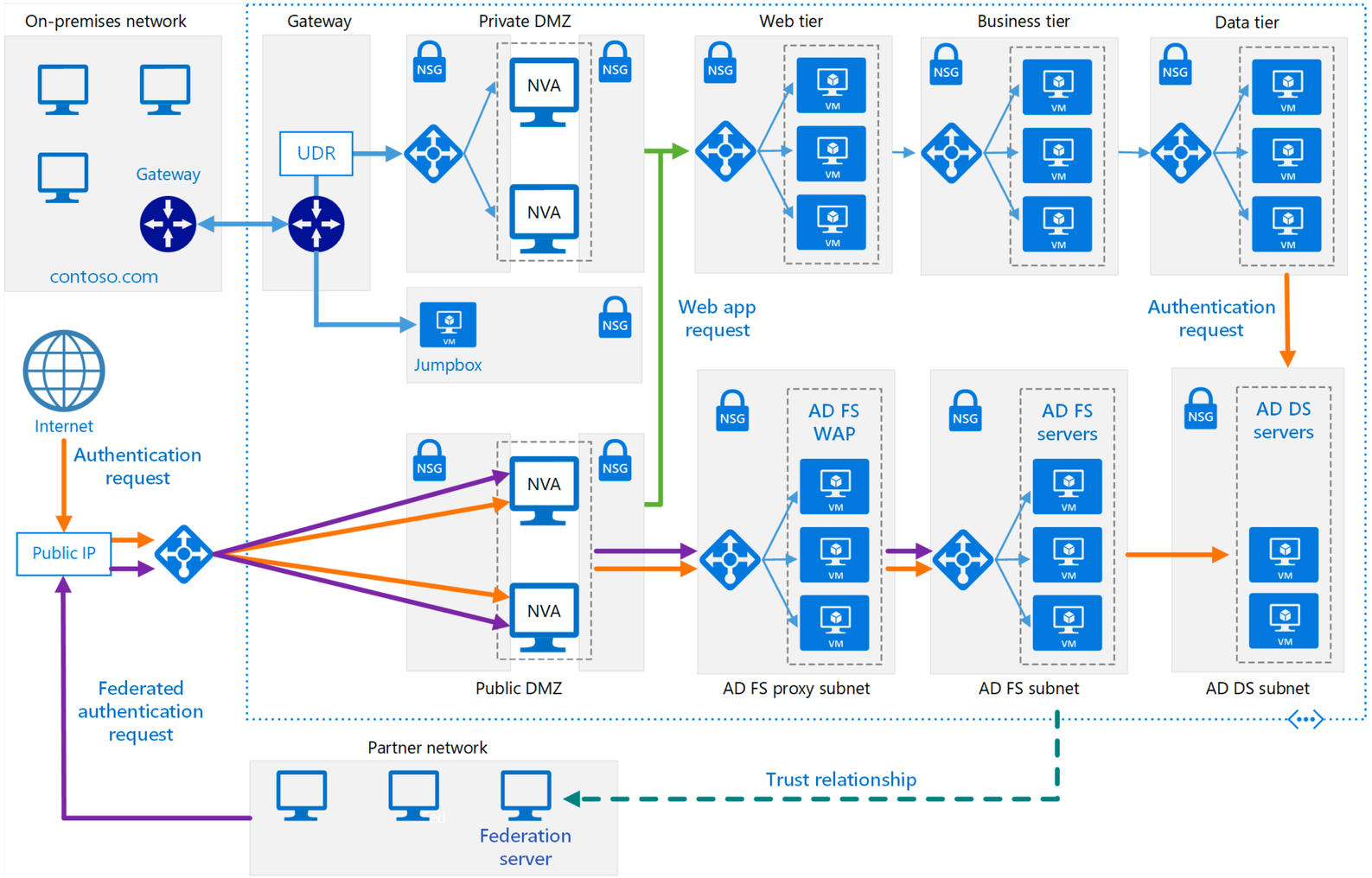
WHEN TO CHOOSE WHAT? EXTEND AD DS TO AZURE



WHEN TO CHOOSE WHAT? CREATE AD DS FOREST IN AZURE



WHEN TO CHOOSE WHAT? EXTEND ADFS TO AZURE



DOMAIN JOINED VIRTUAL MACHINE - SUMMARY

- DOMAIN AND IAAS APPLICATIONS
- HYBRID CONNECTIVITY
- AZURE AD DOMAIN SERVICES