

Student: Dan Tataru
Student ID: 2125053
Course: Cloud Computing Architecture
Module code: ACCA5025
Lecturer: Koushik Modak

Assessment 2

Virtual machines (VMs) are emulated computer systems that run on top of physical hardware. They utilize resources like virtual hard drives, virtual CPUs, and virtual memory to function as if they were physical machines. VMs are created and managed using hypervisors, which are software or hardware platforms that allow multiple VMs to share a single physical host. In this report, we will discuss the resources associated with VMs, focusing on Azure VMs, and provide an in-depth explanation of virtual networks and network security groups.

1. Resources associated with VMs:

A. Virtual Hard Drives (VHDs):

Virtual Hard Drives (VHDs) are the storage medium for VMs in Azure. They are files stored on the host's physical storage that act as virtual storage devices for the VMs. VHDs have several features:

a. Types of VHDs:

- Fixed-size VHD: These VHDs have a pre-allocated size, which ensures better performance but may lead to wasted storage if the VM doesn't use the entire allocated space.
- Dynamically expanding VHD: These VHDs start small and grow as data is added. This type can help save storage space, but it may have slightly lower performance compared to fixed-size VHDs.

b. Managed Disks:

Azure offers managed disks, which are fully managed VHDs that simplify storage management for VMs. Managed disks provide automatic scaling, high availability, and improved security. They come in various performance tiers, including Standard HDD, Standard SSD, Premium SSD, and Ultra Disk, depending on the IOPS and throughput requirements.

c. Disk Encryption:

Azure Disk Encryption enables users to secure their data at rest using industry-standard encryption methods. Azure integrates with Azure Key Vault to manage keys and secrets used for encryption.

B. Virtual CPUs (vCPUs):

Virtual CPUs (vCPUs) represent the processing power allocated to a VM. They are logical units derived from the physical CPUs of the host machine. Azure offers a wide range of VM sizes with varying vCPU configurations to meet different workload requirements.

a. VM Sizes:

Azure provides various VM sizes, each with a different combination of vCPUs, memory, and storage. They are designed for different workloads, such as general-purpose, compute-optimized, memory-optimized, storage-optimized, and GPU-enabled VMs.

b. CPU Overcommitment:

In some cases, the hypervisor can allow for CPU overcommitment, which means allocating more vCPUs to VMs than there are physical cores available. This can improve resource utilization, but it may also lead to performance degradation if the VMs compete for CPU resources.

C. Virtual Memory:

Virtual memory is the RAM allocated to VMs from the host's physical memory. It allows VMs to run applications and store data as if they were physical machines.

a. Memory-Optimized VMs:

Azure offers memory-optimized VMs, which provide a higher memory-to-vCPU ratio for workloads that require more memory, such as databases and in-memory caching.

b. Memory Ballooning:

Memory ballooning is a technique used by hypervisors to dynamically adjust the memory allocated to VMs based on their needs. It helps improve memory utilization and allows for the overcommitment of memory resources.

D. Virtual Network Interfaces (vNICs):

Virtual Network Interfaces (vNICs) are the virtual representation of a network interface card that connects VMs to the virtual network (vNet). They enable VMs to communicate with other resources within the vNet and beyond.

Create virtual network - Microsoft

ms.portal.azure.com/#create/Microsoft.VirtualNetwork-ARM

Microsoft Azure

Search resources, services, and docs (G+)

[Dashboard](#) > [Virtual networks](#) >

Create virtual network

[Basics](#) [IP Addresses](#) [Security](#) [Tags](#) [Review + create](#)

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [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 *

Contoso

Resource group *

TestRG

[Create new](#)

Instance details

Virtual network name *

VNet

Region ⓘ *

(US) East US

[Deploy to an edge zone](#)

[Review + create](#)

[< Previous](#)

[Next : IP Addresses >](#)

[Download a template for automation](#)

Home

 > [Virtual networks](#) >

Create virtual network

[Basics](#) [IP Addresses](#) [Security](#) [Tags](#) [Review + create](#)

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 10.0.0.0/16).

IPv4 address space

10.0.0.0/16

☐ Add IPv6 address space ⓘ

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained within the virtual network's address space.

[+ Add subnet](#)

[Remove subnet](#)

Subnet name	Subnet address range
☐ default	10.0.0.0/24

ⓘ A NAT gateway is recommended for outbound internet access from subnets. Edit the virtual network to add a NAT gateway.

[Review + create](#)

[< Previous](#)

[Next : Security](#)

[Add](#)

[Cancel](#)

Add subnet

Subnet name *

default

Subnet address range * ⓘ

10.0.0.0/24

(0 Addresses)

NAT GATEWAY

Simplify connectivity to the internet using a network address translation gateway. Outbound connectivity is possible without a load balancer or public IP addresses attached to your virtual machines. [Learn more](#)

NAT gateway

None

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

0 selected

Create virtual network

...

✕

Basics

IP Addresses

Security

Tags

Review + create

BastionHost ⓘ

☐ Disable

☒ Enable

Bastion name *

VNet-Bastion ✓

AzureBastionSubnet address space *

10.0.1.0/26 ✓

10.0.1.0 - 10.0.1.63 (64 addresses)

Public IP address *

(New) VNet-bastion-publicIP ✓

Create new

DDoS Network Protection ⓘ

☒ Disable

☐ Enable

Firewall ⓘ

☒ Disable

☐ Enable

Review + create

< Previous

Next : Tags >

Download a template for automation

Create a virtual machine

...

Basics

Disks

Networking

Management

Monitoring

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 * ⓘ

Contoso

Resource group * ⓘ

TestRG

Create new

Instance details

Virtual machine name * ⓘ

VM1 ✓

Region * ⓘ

(US) East US

Availability options ⓘ

No infrastructure redundancy required

Security type ⓘ

Trusted launch virtual machines

Image * ⓘ

Windows Server 2019 Datacenter - x64 Gen2

See all images | Configure VM generation

VM architecture ⓘ

☐ Arm64

☒ x64

Arm64 is not supported with the selected image.

Run with Azure Spot discount ⓘ

☐

Size * ⓘ

Standard_DS1_v2 - 1 vcpu, 3.5 GiB memory (\$25.55/month)

See all sizes

Administrator account

Username * ⓘ

Azureuser

Password * ⓘ

Confirm password * ⓘ

Create a virtual machine ...

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network *	VNet Create new
Subnet *	default (10.0.0.0/24) Manage subnet configuration
Public IP	None Create new
NIC network security group	☐ None ☒ Basic ☐ Advanced
Public inbound ports *	☒ None ☐ Allow selected ports
Select inbound ports	Select one or more ports

i All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Review + create

< Previous

Next : Management >

**VM1**

Virtual machine

☆

☆

...

Directory: Microsoft

Search

Overview

Activity log

Access control (IAM)

Connect

RDP

SSH

Bastion

Start

E. Additional VM Resources:

a. Extensions:

VM extensions are software components that can be installed on Azure VMs to automate tasks such as configuration management, security, and monitoring.

b. VM Scale Sets:

Azure VM Scale Sets enable the creation of multiple VM instances from a single configuration. They simplify the management and scaling of VMs, allowing them to automatically increase or decrease based on demand.

c. Availability Sets and Zones:

To ensure high availability and fault tolerance, Azure provides availability sets and zones. Availability sets distribute VMs across multiple fault domains (physical hardware) and update domains (planned maintenance) within a single data centre. Availability zones distribute VMs across multiple data centers within a region. This helps protect VMs from hardware failures, network outages, and other potential issues.

d. Backup and Disaster Recovery:

Azure VMs can be backed up using Azure Backup, which creates point-in-time snapshots of VMs and stores them in a geographically separate region. In case of a disaster, VMs can be restored from these backups, ensuring minimal data loss and downtime.

e. Monitoring and Diagnostics:

Azure provides built-in monitoring and diagnostics capabilities for VMs using Azure Monitor. It collects and analyses performance metrics, logs, and other data to help users understand the health, performance, and availability of their VMs. Users can also set up alerts and notifications based on specific conditions.

f. Resource Groups and Tags:

Azure uses resource groups and tags to help users organize and manage their VMs and other resources. Resource groups are logical containers for resources deployed within an Azure subscription, while tags are metadata assigned to resources to categorize them based on user-defined criteria.

6. VM Lifecycle Management:

Managing the lifecycle of VMs in Azure involves several steps, such as provisioning, configuration, monitoring, and decommissioning.

a. Provisioning:

VMs can be provisioned in Azure using the portal, Azure CLI, SDKs, or Infrastructure as Code (IaC) tools like Azure Resource Manager (ARM) templates or Terraform. Users can choose from a variety of images, including marketplace images and custom images, to create VMs with specific configurations.

b. Configuration:

After provisioning, VMs can be configured to meet specific requirements. This includes configuring networking settings, attaching additional storage, installing software and applications, and applying security configurations like NSGs and firewalls.

c. Monitoring:

Once a VM is up and running, it's essential to monitor its performance, availability, and health. Azure Monitor and other third-party monitoring tools can help users keep an eye on their VMs and troubleshoot issues when they arise.

d. Scaling:

Azure VMs can be scaled vertically (by changing the VM size) or horizontally (by increasing the number of VM instances) to meet changing workload demands. VM Scale Sets and auto-scaling capabilities make it easier to manage and automate the scaling process.

e. Maintenance and Patching:

Regular maintenance and patching are necessary to keep VMs secure and up to date. Azure Automation, Update Management, and other tools can help automate the process of applying updates and patches to VMs.

f. Decommissioning:

When a VM is no longer needed, it should be decommissioned to free up resources and avoid unnecessary costs. This includes deleting the VM, its associated storage, and any other related resources.

2. vNets (Virtual Networks) and Network Security Groups:

- vNets are virtual networks in Azure that provide a private, isolated network environment for VMs and other resources. They enable communication between resources within the network and can be connected to on-premises networks using VPN or ExpressRoute.

- Network Security Groups (NSGs) are used to control inbound and outbound traffic to VMs and other resources within a vNet. They act as a virtual firewall, allowing or denying traffic based on rules defined by the user.

Home > Network security groups >

Create network security group

BasicsTagsReview + create

Project details

Subscription *Contoso Subscription

Resource group *myResourceGroup

Create new

Instance details

Name *myNSG

Region *East US

Review + create

< Previous

Next : Tags >

Download a template for automation

Home > Network security groups > myNSG

myNSG | Subnets

Network security group

Search

+ Associate

Search subnets

Name

No results.

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Associate subnet

myNSG

Virtual network ①myVNet

Subnet ①mySubnet

OK

[Home](#) >

Network security groups

Microsoft

+

Create

⚙️

Manage view

↺

Refresh

📄

Export to CSV

🔗

Open query

🏷️

Assign tags

Filter for any field...

Subscription equals **Contoso Subscription**

Resource group equals **all**

Location equals **all**

+

Add filter

No grouping

List view

☐

Name ↑↓

☐

Resource group ↑↓

☐

Location ↑↓

☐

Subscription ↑↓

☐

Flow log ↑↓

☐

myNSG

myResourceGroup

East US

Contoso Subscription

...

myNSG

Network security group

Search

Move

Delete

Refresh

Give feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Monitoring

Help

Essentials

Custom security rules : 0 inbound, 0 outbound

Associated with : 0 subnets, 0 network interfaces

Filter by name

Port == all

Protocol == all

Source == all

Destination == all

Action == all

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
Inbound Security Rules						
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalanc--	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

[Home](#) > [Network security groups](#) > [myNSG](#)

myNSG | Subnets

Network security group

Search

Associate

Search subnets

Name	Address range	Virtual network
mySubnet	10.0.0.0/24	myVNet

Home > Network security groups >

myNSG

Network security group

Search

Move Delete Refresh Give feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Delete network security group

Do you want to delete the network security group 'myNSG'?

Yes No

Subscription (move)
Contoso Subscription

Home > Network security groups > myNSG

myNSG | Inbound security rules

Network security group

Search

Add Hide

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Alerts

Diagnostics settings

Logs

NSG flow logs

Automation

Tasks (preview)

Export template

Help

Effective security rules

Support + Troubleshooting

Network security group

destination, destination, and direction as an a higher priority. Learn more

Filter by name

Port == all

Priority

65000

65001

65500

Add inbound security rule

myNSG

Source

Any

Source port ranges *

*

Destination

Any

Service

Custom

Destination port ranges *

8080

Protocol

Any

TCP

UDP

ICMP

Action

Allow

Deny

Priority *

100

Name *

AllowAnyCustom8080Inbound

Description

Add Cancel

myNSG | Inbound security rules

Network security group

Search

+ Add Hide default rules Refresh Delete Give feedback

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Inbound security rules
- Outbound security rules

Network interfaces

Subnets

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name		Port == all	Protocol == all	Source == all	Destination == all	Action == all
Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action
☐ 300	 RDP-rule	3389	TCP	Any	Any	 Allow
☐ 65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow
☐ 65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any	 Allow
☐ 65500	DenyAllInBound	Any	Any	Any	Any	 Deny

myNSG | Inbound security rules

Network security group

Search

+ Add Hide default rules Refresh

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Inbound security rules
- Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

- Alerts
- Diagnostic settings
- Logs
- NSG flow logs

Automation

- Tasks (preview)
- Export template

Help

- Effective security rules
- Support + Troubleshooting

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule, but you can override them with rules that have a higher priority.

Filter by name	
Port == all	Protocol == all
Priority ↑↓	Name ↑↓
☐ 300	 RDP-rule
☐ 65000	AllowVnetInBou
☐ 65001	AllowAzureLoa
☐ 65500	DenyAllInBou

RDP-rule

myNSG

Source

Any

Source port ranges

*

Destination

Any

Service

RDP

Destination port ranges

3389

Protocol

☐ Any

☒ TCP

☐ UDP

☐ ICMP

Action

☒ Allow

☐ Deny

Priority

300

Name

RDP-rule

Description

Allow RDP

RDP port 3389 is exposed to the Internet. This is only recommended for testing. For production environments, we recommend using a VPN or private connection.

Home > Network security groups > myNSG

myNSG | Inbound security rules

Network security group

Search << + Add Hide default rules Refresh **Delete** Give feedback

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties

Home > Application security groups >

myASG

Application security group

Search << → Move **Delete**

Overview
Activity log
Access control (IAM)
Tags

Settings
Properties

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name

Port == all Protocol == all Source == all Destination == all Action == all

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓
☒ 200	RDP-rule	3389	Tcp	Any
☐ 65000	AllowVnetInBound	Any	Any	VirtualNetwork
☐ 65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer
☐ 65500	DenyAllInBound	Any	Any	Any

Delete the application security group

Are you sure you want to delete the application security group 'myASG'?

Yes No

Subscription ID : abcdef01-2345-6789-0abc-def012345678

Tags ([edit](#)) : [Click here to add tags](#)

3. Use of images in Azure:

VM images in Azure play a crucial role in creating and deploying virtual machines. They serve as templates containing a pre-configured operating system, applications, and settings. By using images, users can quickly deploy VMs with consistent configurations and easily manage their virtual infrastructure.

There are three primary types of images in Azure:

1. Azure Marketplace Images:

Popular app categories

Virtual Machine Images Networking Storage Blockchain
Security Software as a service Databases All categories

Microsoft Azure Marketplace

What is the Marketplace?

The Marketplace is the premier destination for all your software needs - certified and optimized to run on Azure.

- Find solutions you want, from open source container platforms to threat detection to blockchain
- Find apps and services that meet your needs, from open source container platforms to threat detection to blockchain
- Provision end-to-end solutions quickly and reliably

[Learn more](#)

The Azure Marketplace is an online store that offers a wide variety of images created and maintained by Microsoft, third-party vendors, and the community. These images include various operating systems (such as Windows Server, Ubuntu, CentOS, and more), development platforms (like Node.js, .NET, Java, and others), and applications (such as SQL Server, WordPress, Jenkins, etc.).

Benefits of using Azure Marketplace images include:

- a. Quick deployment: Users can quickly deploy VMs with pre-installed software and pre-configured settings, significantly reducing the time and effort required for manual installation and configuration.
- b. Verified and up-to-date: Marketplace images are verified by Microsoft and their respective vendors, ensuring that they are secure, reliable, and up-to-date with the latest patches and updates.
- c. Customization: Users can customize Marketplace images during the deployment process by adding additional applications, configurations, and settings as needed.

2. Custom Images:

Custom images are user-created images based on their specific needs. They can be created from an existing VM, a VHD, or even imported from another environment, such as on-premises or another cloud provider. Custom images enable users to create VMs with a consistent configuration, ensuring that all VMs have the same applications and settings installed.

Benefits of using custom images include:

- a. Consistency: Custom images ensure a consistent configuration across VMs, reducing the risk of errors and inconsistencies caused by manual configuration.
- b. Streamlined deployment: Custom images allow users to deploy VMs with pre-installed applications and settings, eliminating the need for manual configuration after deployment.
- c. Simplified management: Custom images simplify the management of VM configurations, making it easier to maintain and update applications and settings across multiple VMs.

Creating custom images involves several steps:

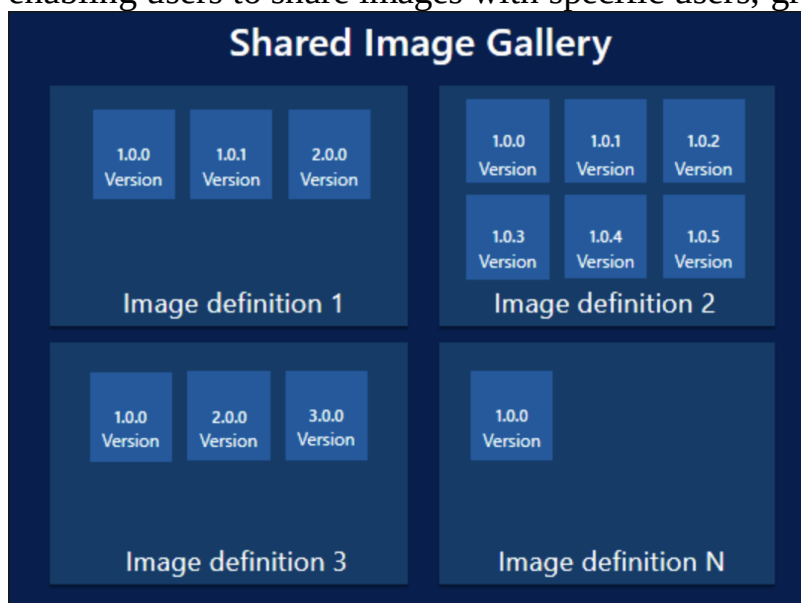
- a. Prepare the source VM: Install the required applications, configurations, and settings on a VM. Sysprep the VM for Windows or use the corresponding tool for Linux to generalize the VM, making it ready for image creation.
- b. Capture the image: Create a VHD from the generalized VM and store it in a storage account or Azure Managed Disks.
- c. Create an image resource: Use the captured VHD to create an image resource in Azure, which can then be used to deploy new VMs.

3. Shared Image Gallery:

Azure Shared Image Gallery is a service that allows users to store, manage, and share images across subscriptions and regions. It simplifies the management of custom images and enables faster deployment of VMs by storing replicas of images in multiple regions.

Benefits of using Shared Image Gallery include:

- a. Global distribution: Users can store and distribute images across multiple Azure regions, ensuring faster deployment and improved performance.
- b. Versioning: Shared Image Gallery supports versioning of images, allowing users to manage and deploy different versions of an image.
- c. Access control: Shared Image Gallery provides granular access control, enabling users to share images with specific users, groups, or subscriptions.



By understanding these VM resources and lifecycle management aspects, users can efficiently manage their VMs in Azure and ensure optimal performance, security, and cost-effectiveness. Combined with the in-depth knowledge of vNets and network security groups, users can create a secure, scalable, and highly available virtual infrastructure in Azure. This report provides an overview of the various resources associated with VMs, how they are created and managed, the role of virtual networks and network security groups, and the use of images in Azure, amounting to a comprehensive understanding of Azure VMs for the user.

References

1. Microsoft Azure. (n.d.). Azure Marketplace. Retrieved from <https://azuremarketplace.microsoft.com/en-GB/>
2. Microsoft Docs. (n.d.). Manage a network security group. Retrieved from <https://learn.microsoft.com/en-us/azure/virtual-network/manage-network-security-group>
3. Microsoft Docs. (n.d.). Quickstart: Create a virtual network using the Azure portal. Retrieved from <https://learn.microsoft.com/en-us/azure/virtual-network/quick-create-portal>
4. Microsoft Docs. (n.d.). Capture a managed image of a generalized VM in Azure. Retrieved from <https://learn.microsoft.com/en-us/azure/virtual-machines/capture-image-resource>
5. Microsoft Azure. (n.d.). Azure Virtual Machines. Retrieved from <https://azure.microsoft.com/en-us/products/virtual-machines/>
6. Microsoft Docs. (n.d.). Create and use a Shared Image Gallery. Retrieved from <https://learn.microsoft.com/en-us/azure/virtual-machines/shared-image-galleries>