Microsoft

AZ-800T00A
Administer Windows Server Hybrid Core Infrastructure

Agenda AZ-800

1 Deploy and manage identity infrastructure – Windows Server
2 Deploy and manage identity infrastructure – Hybrid

3 Administering Windows Server Hybrid Core Infrastructure – Windows Server ✓
4 Administering Windows Server Hybrid Core Infrastructure – Hybrid ✓

5 Manage virtualization and containers – Windows Server
6 Manage virtualization and containers – Hybrid

7 Implement and manage networking infrastructure – Windows Server
8 Implement and manage networking Infrastructure – Hybrid

9 Configure storage and file services – Windows Server
10 Configure storage and file services – Hybrid

PS
WAC
ARC ?

Hyper-V
IaaS
PaaS
CaaS
Serverless Compute
Azure Func
Logic App
SaaS

Manage virtualization and containers in a hybrid environment *(Hyper-V virtualization in Windows Server)*

- Configure and manage Hyper-V
- Configure and manage Hyper-V virtual machines
- Securing virtualization in Windows Server
- Run containers on Windows Server
- Orchestrate containers on Windows Server using Kubernetes
- Lab 05 – Implementing and configuring virtualization in Windows Server

Configure and manage Hyper-V

Learning Objectives – Configure and manage Hyper-V

- Overview of Hyper-V
- Overview of Hyper-V Manager
- Best practices for configuring Hyper-V hosts
- Hyper-V networking
- Overview of nested virtualization
- Enhanced Session Mode
- GPU partitioning (GPU-P)
- Hyper-V integration services
- Learning recap

Define Hyper-V (1/2)

Docker Container

Hardware virtualization layer

OS Linux Linux

- Native hypervisor that provides hardware virtualization capabilities

A role in Windows Server

Docker D

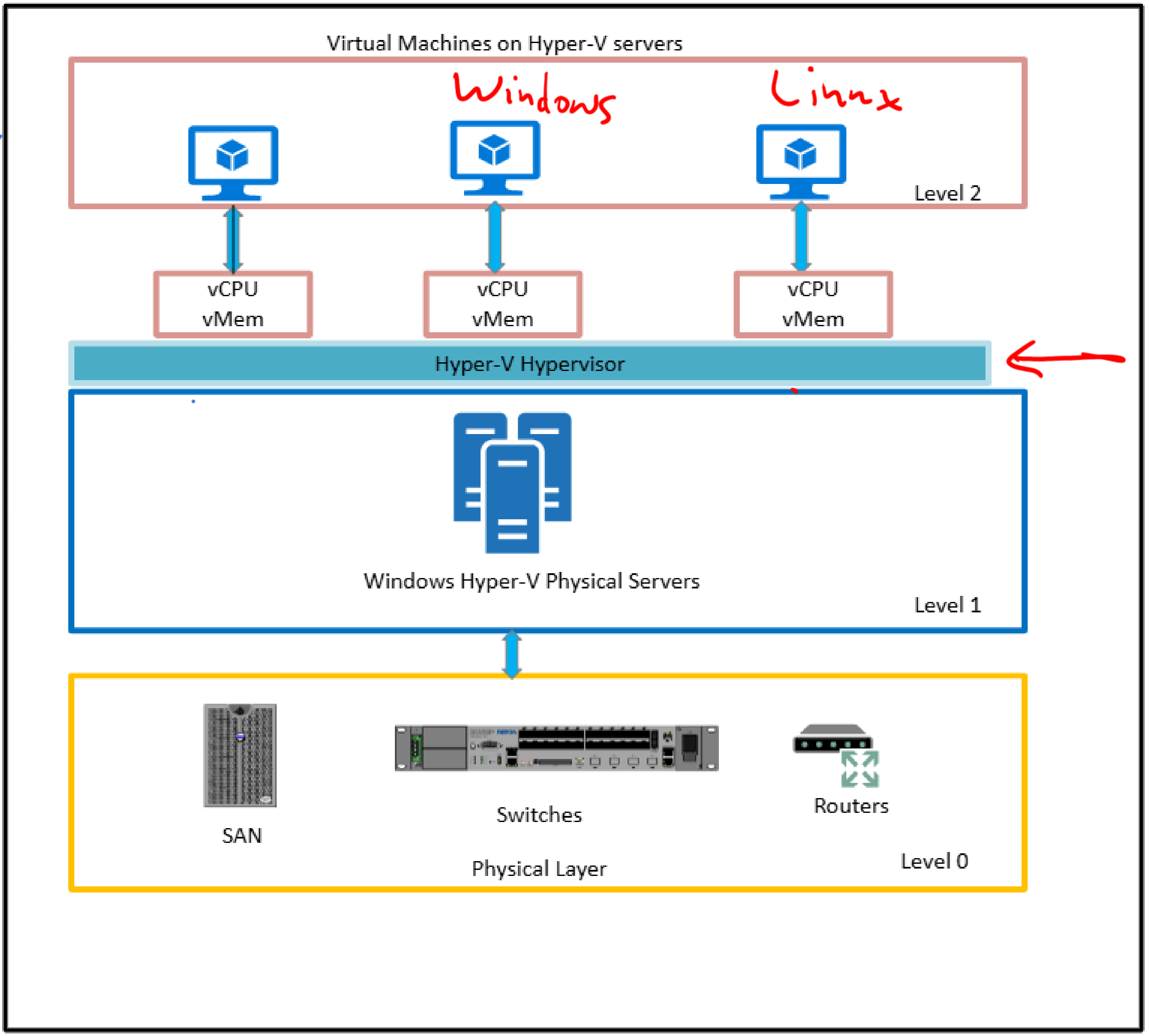
- Supports Windows 10 and 11 as an optional feature

Shared Linux Kernel

Allows creation of multiple VMs on same hardware

Provides an isolated space for each VM to run its own operating system (OS)

On-premises Hyper-V



Define Hyper-V (2/2)

Xen

- **Supports many types of guest operating systems including:**
  - CentOS, Red Hat Enterprise Linux, Debian, Oracle Linux, SUSE, and Ubuntu
  - Several Windows Server and Windows client OSs
  - FreeBSD
- **System requirements:**
  - A 64-bit processor with second-level address translation (SLAT)
  - A processor with VM Monitor Mode extensions
  - Sufficient memory
  - Intel Virtualization Technology (Intel VT) or Advanced Micro Devices (AMD) Virtualization (AMD-V) enabled
  - Hardware-enforced Data Execution Prevention (DEP) enabled (Intel Execute Disable (XD) bit, AMD No Execute (NX) bit)
- **Installation Methods:**
  - Server Manager
  - **Install-WindowsFeature** PowerShell cmdlet

SC - VMM

Define Hyper-V Manager

Hyper-V Manager:

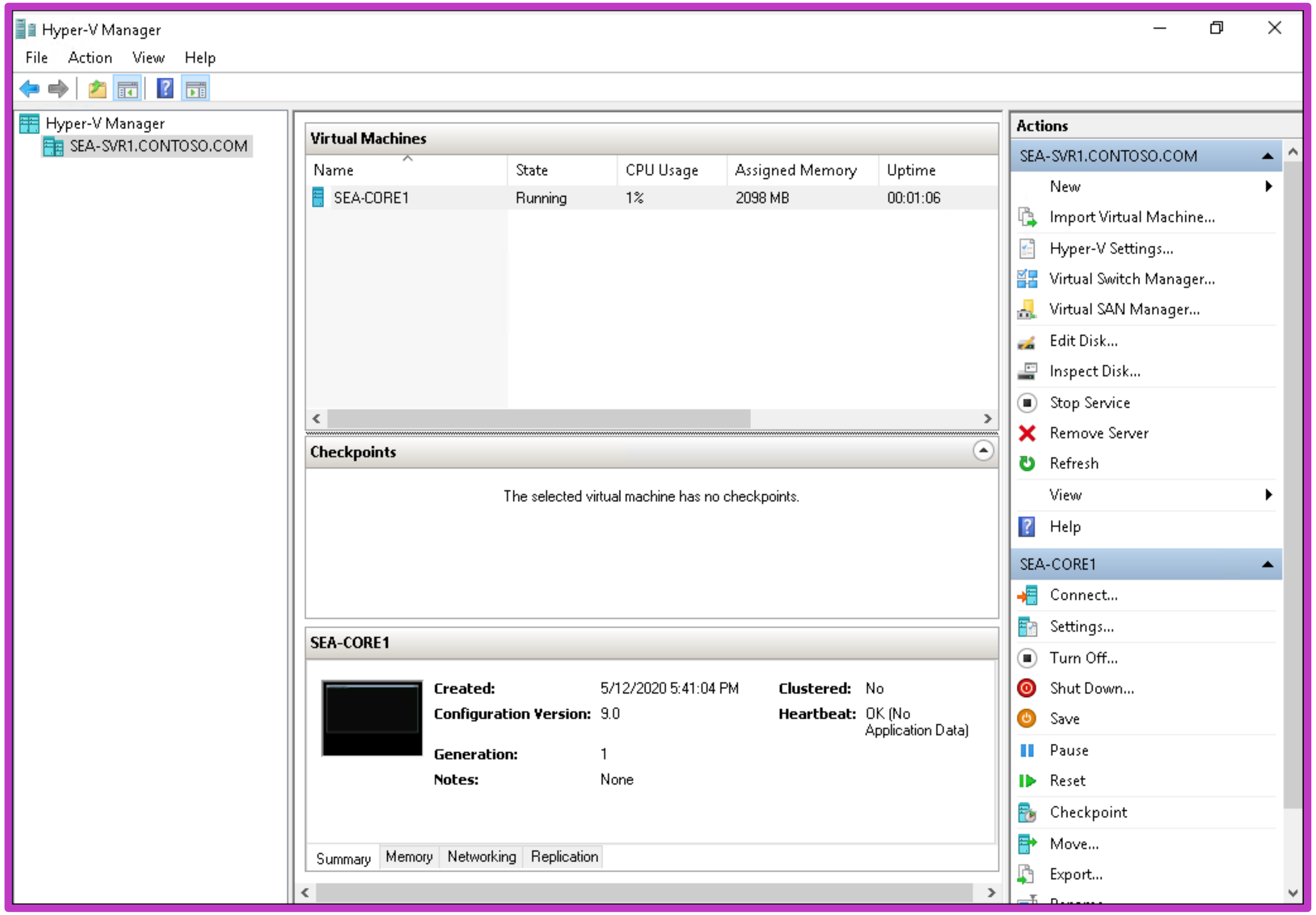
- graphical Interface to manage Hyper-V infrastructure

Supports:

- Previous versions
- Web Services (WS)-Management protocol
- Alternate credential support

Other management tools include:

- Windows PowerShell
- PowerShell Direct
- Windows Admin Center
- SSH Direct *(connect to Linux VMs)*

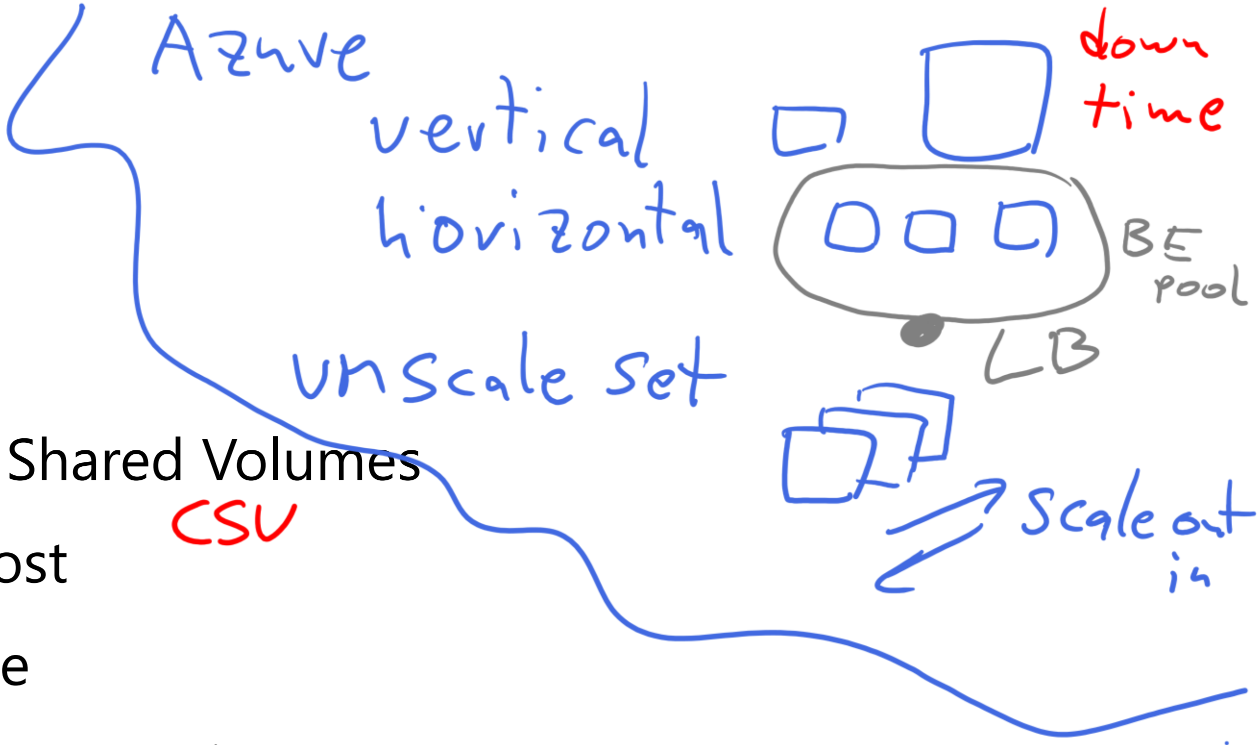


Name	State	CPU Usage	Assigned Memory	Uptime
SEA-CORE1	Running	1%	2098 MB	00:01:06

The selected virtual machine has no checkpoints.

Created: 5/12/2020 5:41:04 PM
Configuration Version: 9.0
Generation: 1
Notes: None
Clustered: No
Heartbeat: OK (No Application Data)

Hyper-V best practices



- Sufficient hardware to run virtual machines
- Deploy VMs on separate disks or Clustered Shared Volumes

CSV

- Avoid installing other server roles on the Host
- Use Server Core to reduce the attack surface
- Run the Best Practices Analyzer and resource metering
- Manage Hyper-V with Remote Server Administrative Tools (RSAT)
- Enable Enhanced Session Mode on the server *(optional)*

Hyper-V networking

Azure
Virtual Network
subnet

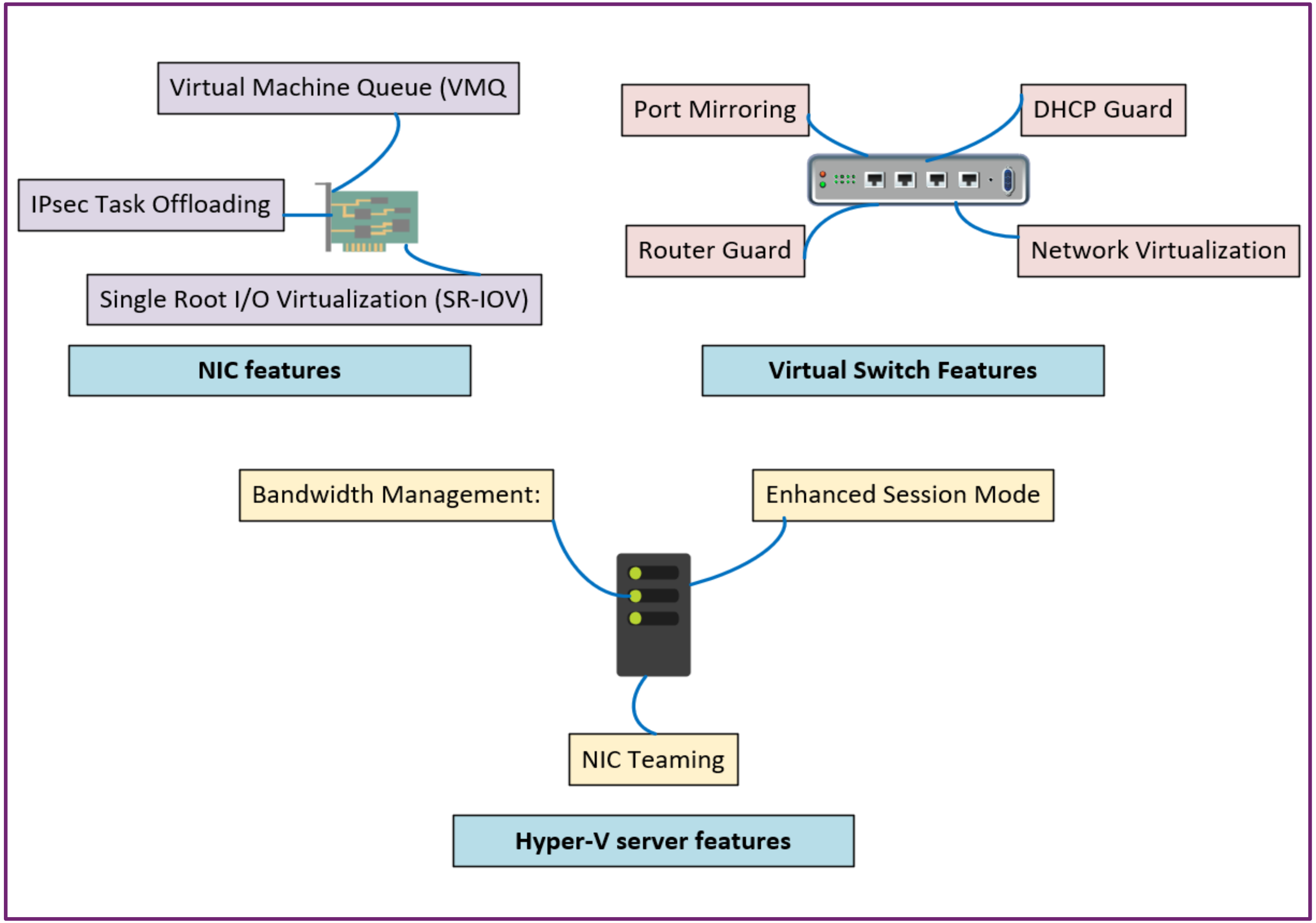
Hyper-V supports the following virtual network adapter types:

- Legacy network adapter *(Generation 1 only)*
- Synthetic network adapter *(supports Generation 1 and Generation 2)*

Hyper-V supports three types of virtual switches:

Virtual switch type	Description
External	Used to map a network to a specific network adapter or network adapter team. Provides external access outside of the host machine.
Internal	Used to communicate between the virtual machines on a host server and to communicate between the virtual machines and the host itself.
Private	Used to only communicate between virtual machines on a Hyper-V host.

Hyper-V network features



Virtual Machine Queue (VMQ

IPsec Task Offloading

Single Root I/O Virtualization (SR-IOV)

NIC features

Port Mirroring

DHCP Guard

Router Guard

Network Virtualization

Virtual Switch Features

Bandwidth Management:

Enhanced Session Mode

NIC Teaming

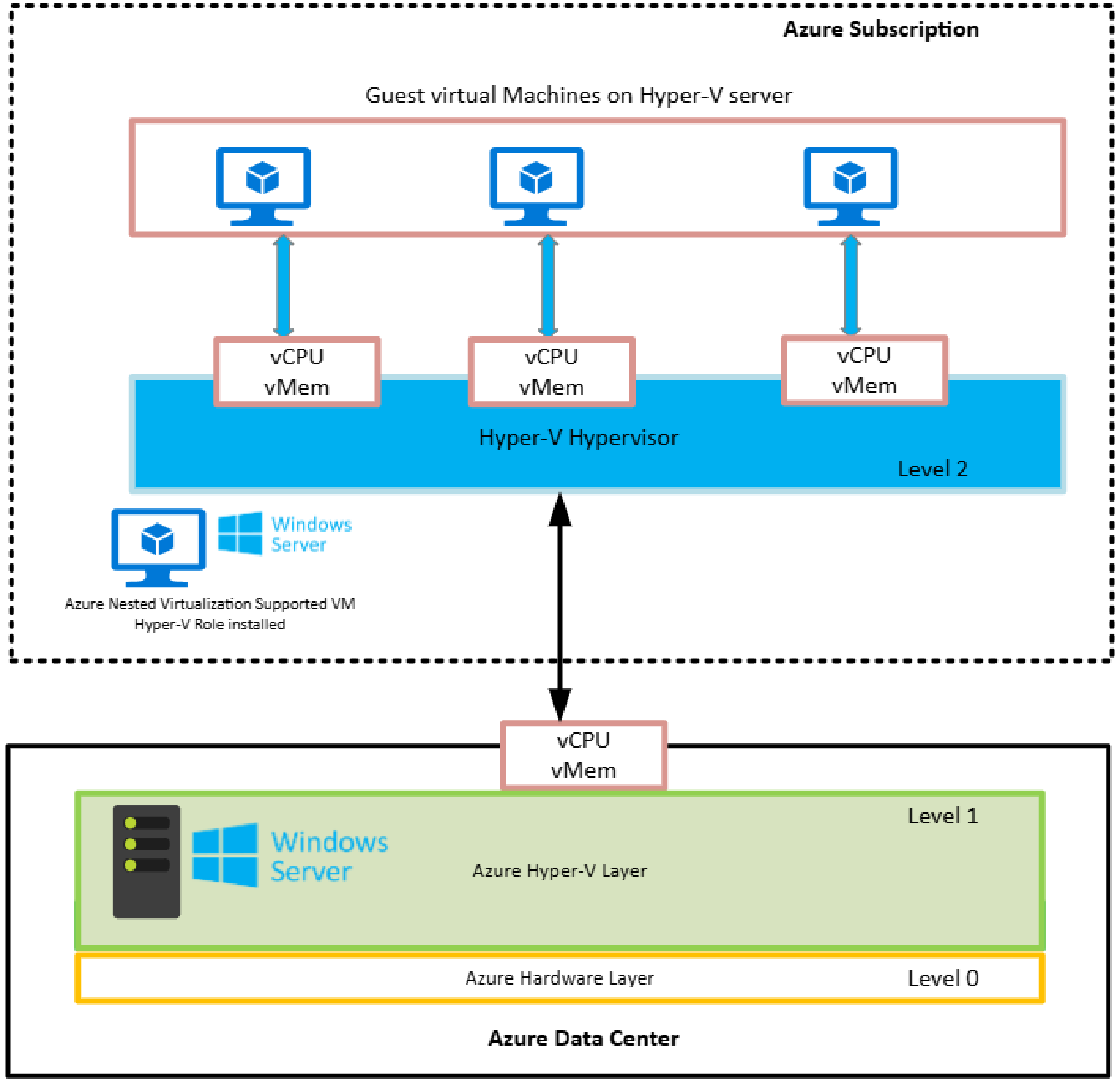
Hyper-V server features

Hyper-V nested virtualization

Hyper-V feature you can use to install and run Hyper-V inside a guest VM

Enables a guest VM to be a Hyper-V host, able to then host other guest VMs

Useful for implementing virtual test and development environments



*To create Nested Virtualization, make sure Azure VM SKU meets the Nested Virtualization requirements.

Enable nested virtualization

Requirements

- Hyper-V Host and the Guest VM must be Windows Server 2016 or later
- Enough Memory
- VM configuration of 8.0 or greater
- Intel processor with VT-x and EPT technology
- AMD EPYC/Ryzen processor or later

Networking options

MAC address spoofing

NAT networking

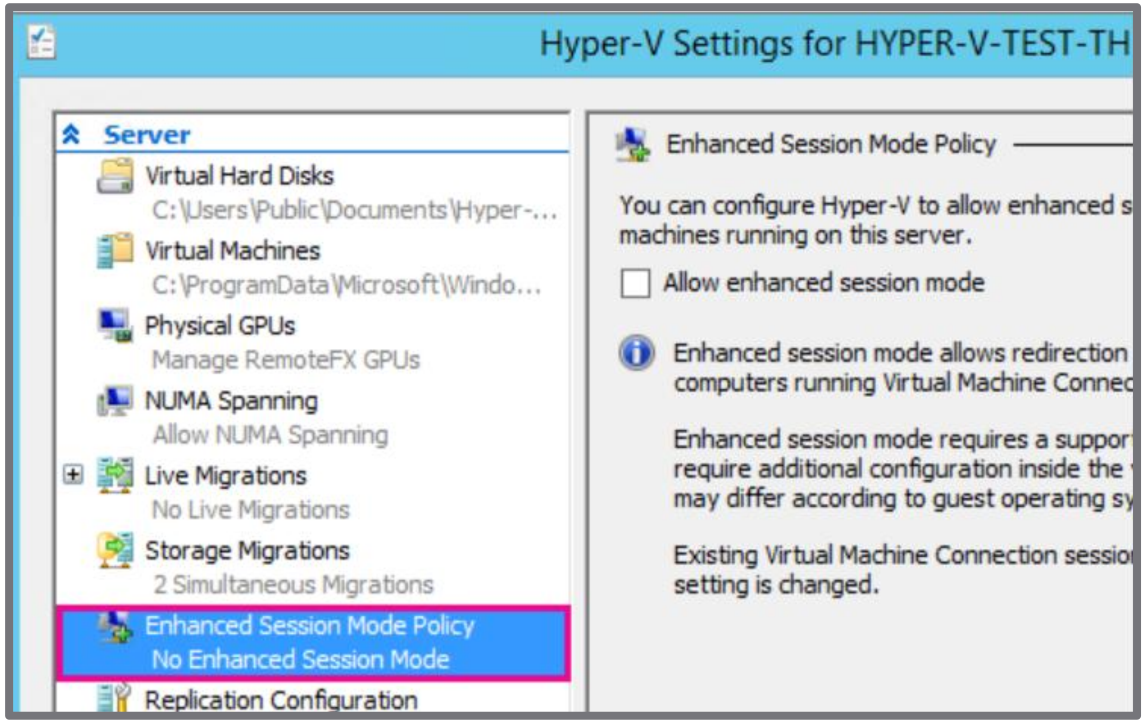
```
# Configure nested virtualization
Set-VMProcessor -VMName “SEA-SVR1”
–ExposeVirtualizationExtensions $true

# Disable nested virtualization
Set-VMProcessor -VMName “SEA-SVR1”
–ExposeVirtualizationExtensions $false
```

Enable Enhanced Session mode

Enhanced Session Mode enables local device redirection and dynamic display resizing

You connect through an RDP session

1. Connect to the computer hosting the virtual machine.
2. Select the host's computer name In Hyper-V Manager.
3. Select **Hyper-V settings**.
4. Under **Server**, select **Enhanced Session Mode Policy**.
5. Select the **Allow enhanced session mode** check box.
6. Under **User**, select **Enhanced session mode**.
7. Select the **Allow enhanced session mode** check box.
8. Click **Ok**.



Hyper-V Settings for HYPER-V-TEST-TH

Server
- Virtual Hard Disks
  C:\Users\Public\Documents\Hyper-...
- Virtual Machines
  C:\ProgramData\Microsoft\Windo...
- Physical GPUs
  Manage RemoteFX GPUs
- NUMA Spanning
  Allow NUMA Spanning
- Live Migrations
  No Live Migrations
- Storage Migrations
  2 Simultaneous Migrations
- Enhanced Session Mode Policy
  No Enhanced Session Mode
- Replication Configuration

Enhanced Session Mode Policy

You can configure Hyper-V to allow enhanced s
machines running on this server.

□ Allow enhanced session mode

Enhanced session mode allows redirection
computers running Virtual Machine Connec

Enhanced session mode requires a suppor
require additional configuration inside the
may differ according to guest operating sy

Existing Virtual Machine Connection sessio
setting is changed.

GPU partitioning (GPU-P)

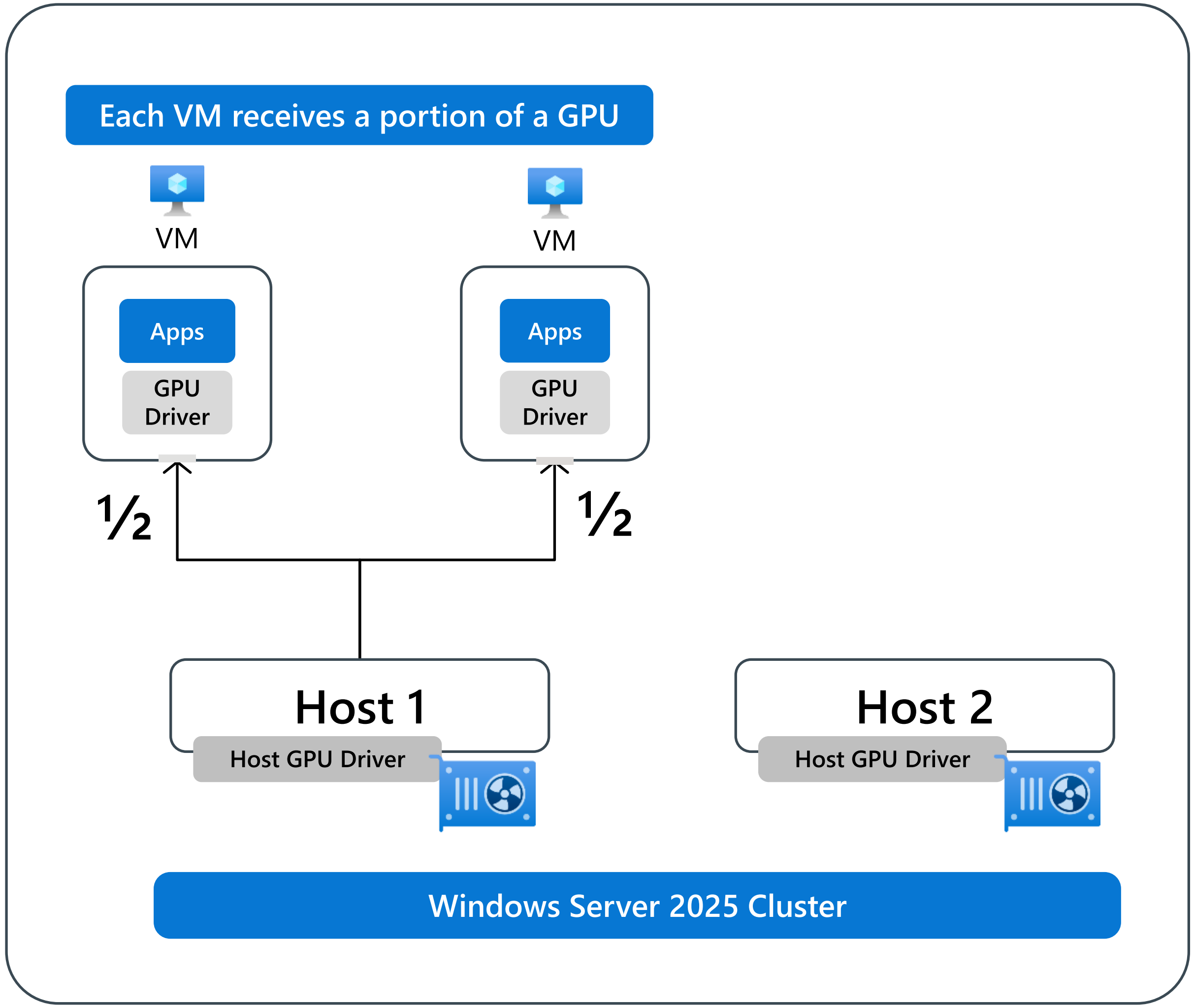
Share a GPU across multiple VMs

- Create GPU partitions
- Assign each partition to a VM that supports
  a set of users (multi-session)
- Manage using PowerShell or WAC

Use cases for GPU-P

- VDI applications
- ML inference applications

Support for live migration and failover clustering



Overview of Hyper-V integration services

Integration services allow virtual machine to communicate with the Hyper-V host

Name	Description
Hyper-V Heartbeat Service	Reports that the VM is running correctly.
Hyper-V Guest Shutdown Service	Allows the host to trigger VMs shutdown.
Hyper-V Time Synchronization Service ✓	Synchronizes the VM's clock with the host computer's clock.
Hyper-V Data Exchange Service (KVP)	Exchanges basic metadata between VM and host.
Hyper-V Volume Shadow Copy Requestor	Allows VSS Service to back up VM without shutting it down.
Hyper-V Guest Service Interface	Interface for host to copy files to/from VM.
Hyper-V PowerShell Direct Service	Manage VM with PowerShell without network connection.

Learning recap – Configure and manage Hyper-V

Knowledge Check

Microsoft Learn Modules (docs.microsoft.com/Learn)

Configure and Manage Hyper-V

Configure and manage Hyper-V virtual machines

Learning Objectives – Configure and manage Hyper-V VMs

- VM Settings and configuration
- VM storage
- Virtual hard disk formats and types
- Manage VM states and checkpoints
- Import and export VMs
- Configure Discrete Device Assignment
- Learning recap

vhd
2TB
4TB

vhdx
64 TB

VM configuration and Generation versions

VM configuration version identifies:

- Compatibility of the VM components with the version of Hyper-V installed on the host machine
- Windows Server 2025 host machines support configuration versions 8.0 through 12.0 or greater
- To update a configuration version, use the following command:
  - ***Update-VMVersion <vmname>***

Generation 1 VMs:

- Support 32 and 64-bit operating systems
- Only support boot volumes a maximum of 2 TB
- Supports legacy BIOS

Generation 2 VMs:

- Support only 64-bit operating systems
- Support secure boot and shielded VMs
- Support boot volumes a maximum of 64 TB
- Supports Unified Extensible Firmware Interface (UEFI)

VM settings

VM settings are grouped into two main areas:

- Hardware
- Management

Available hardware components depend on the generation version of the VM

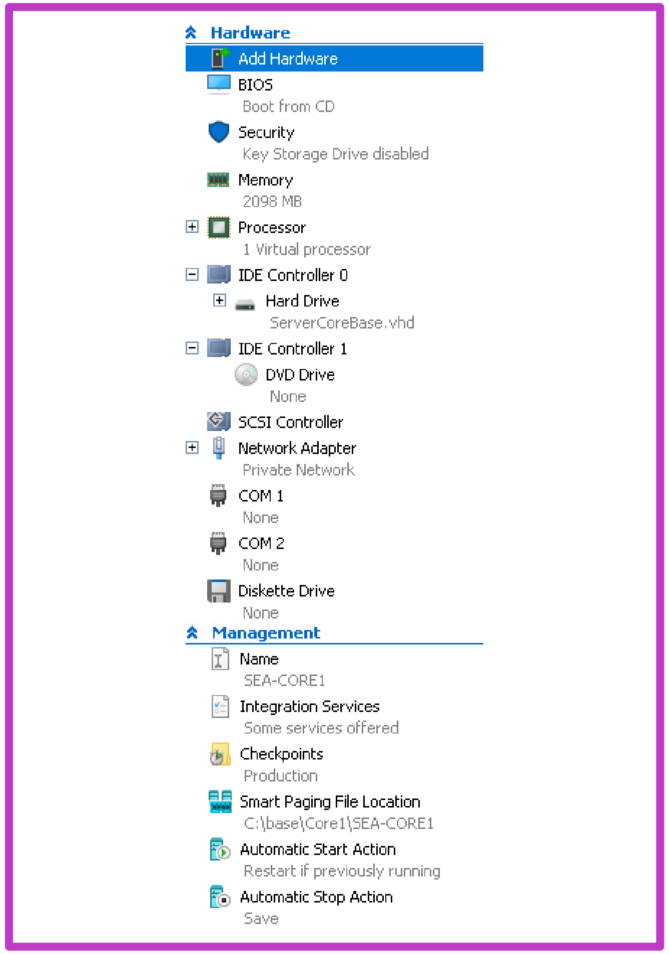
Generation 2

- UEFI, Secure Boot, vTPM, and Enhanced Session Mode

Generation 1

- Designed for legacy hardware configurations that use a traditional BIOS

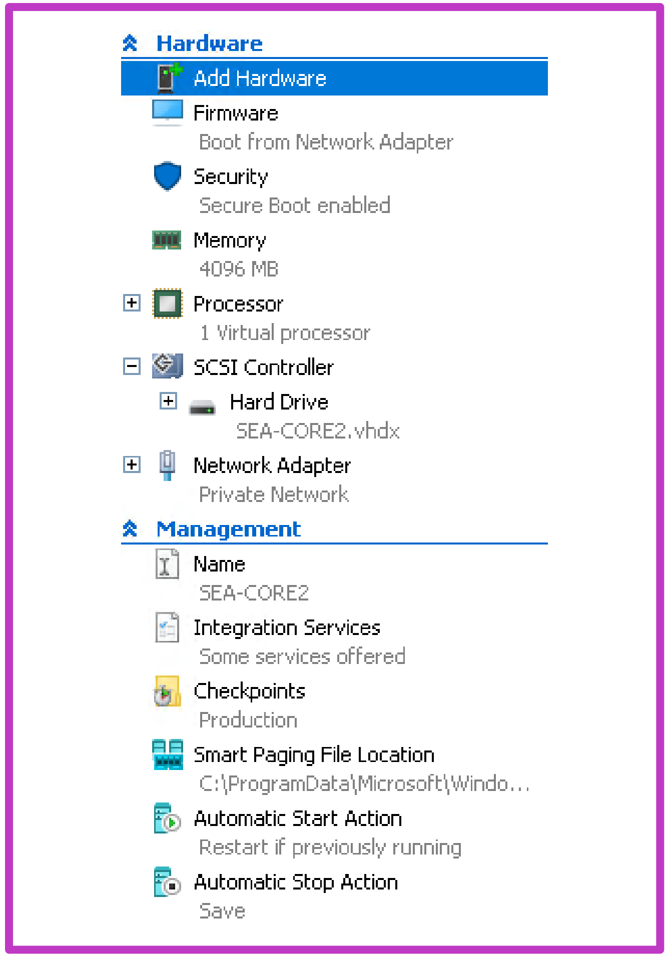
Generation 1 settings



Hardware
- Add Hardware
- BIOS
  Boot from CD
- Security
  Key Storage Drive disabled
- Memory
  2098 MB
- Processor
  1 Virtual processor
- IDE Controller 0
  - Hard Drive
    ServerCoreBase.vhd
- IDE Controller 1
  - DVD Drive
    None
- SCSI Controller
- Network Adapter
  Private Network
- COM 1
  None
- COM 2
  None
- Diskette Drive
  None

Management
- Name
  SEA-CORE1
- Integration Services
  Some services offered
- Checkpoints
  Production
- Smart Paging File Location
  C:\base\Core1\SEA-CORE1
- Automatic Start Action
  Restart if previously running
- Automatic Stop Action
  Save

Generation 2 settings



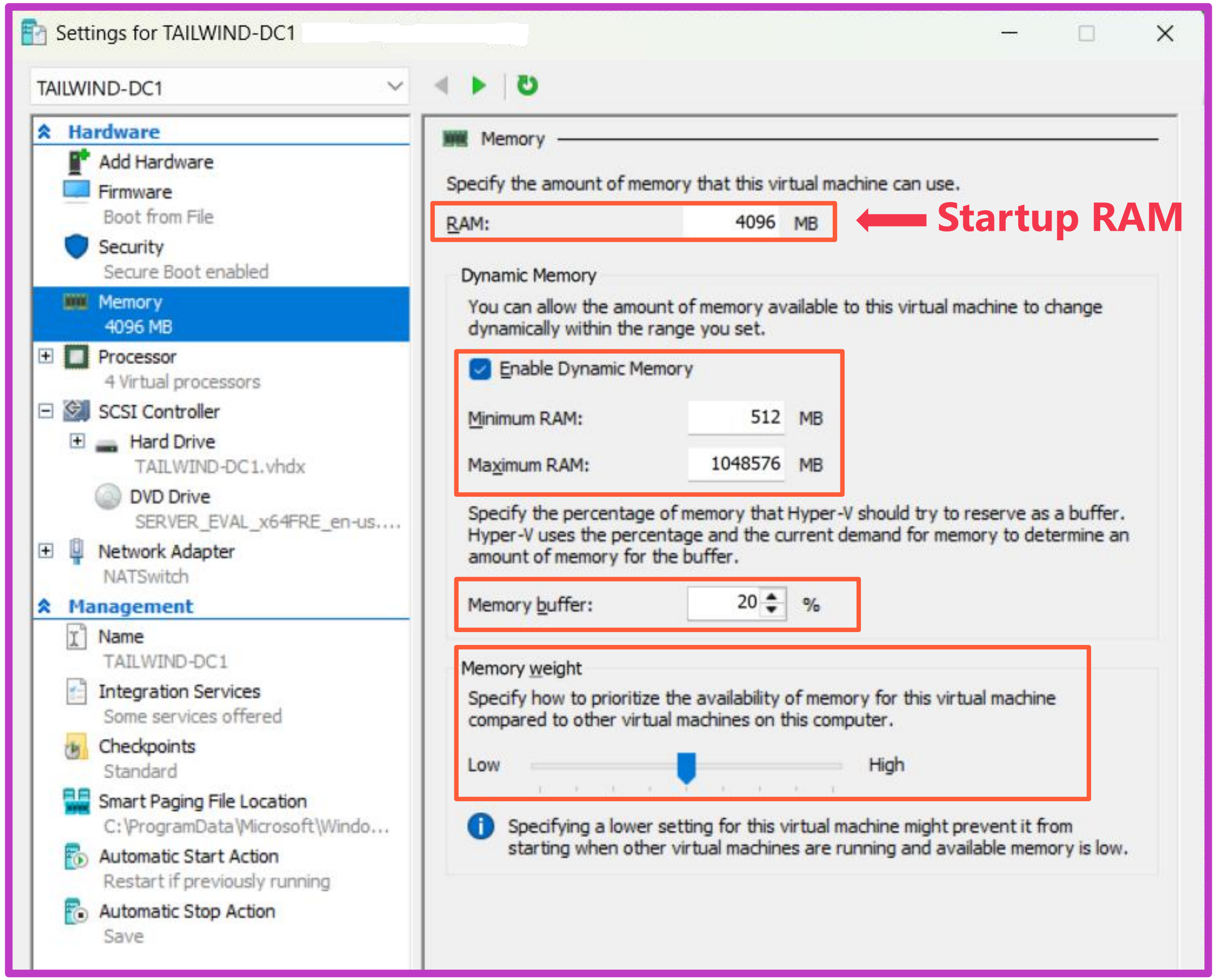
Hardware
- Add Hardware
- Firmware
  Boot from Network Adapter
- Security
  Secure Boot enabled
- Memory
  4096 MB
- Processor
  1 Virtual processor
- SCSI Controller
  - Hard Drive
    SEA-CORE2.vhdx
- Network Adapter
  Private Network

Management
- Name
  SEA-CORE2
- Integration Services
  Some services offered
- Checkpoints
  Production
- Smart Paging File Location
  C:\ProgramData\Microsoft\Windo...
- Automatic Start Action
  Restart if previously running
- Automatic Stop Action
  Save

Configure Dynamic Memory for Hyper-V virtual machines

Enable dynamic memory

- Minimum RAM is the amount of memory allocated at startup or upgrade
- Minimum RAM value – at least 32 MB and cannot exceed the startup memory value
- Maximum RAM value cannot be lower than startup memory.
- Default setting for Maximum RAM = 1TB
- Memory Buffer ensures VM has additional memory available to handle unexpected spikes in memory demand
- Memory weight distributes memory among multiple VMs



Memory

Specify the amount of memory that this virtual machine can use.

RAM: 4096 MB

Dynamic Memory

You can allow the amount of memory available to this virtual machine to change dynamically within the range you set.

☑ Enable Dynamic Memory

Minimum RAM: 512 MB

Maximum RAM: 1048576 MB

Specify the percentage of memory that Hyper-V should try to reserve as a buffer. Hyper-V uses the percentage and the current demand for memory to determine an amount of memory for the buffer.

Memory buffer: 20 %

Memory weight

Specify how to prioritize the availability of memory for this virtual machine compared to other virtual machines on this computer.

Low — High

Specifying a lower setting for this virtual machine might prevent it from starting when other virtual machines are running and available memory is low.

Hyper-V Storage considerations

Consider the following factors when planning storage for virtual hard disks

- High-performance connection to storage
- Redundant storage
- High-performance storage
- Adequate growth space

Supported storage types include

- Fibre channel connections
- Server Message Block (SMB) 3.0 file shares

Virtual hard disk (1/2)

Virtual hard disk formats include

VHD

- Up to 2040 GB in size
- Typically used to support older Hyper-V versions

VHDX

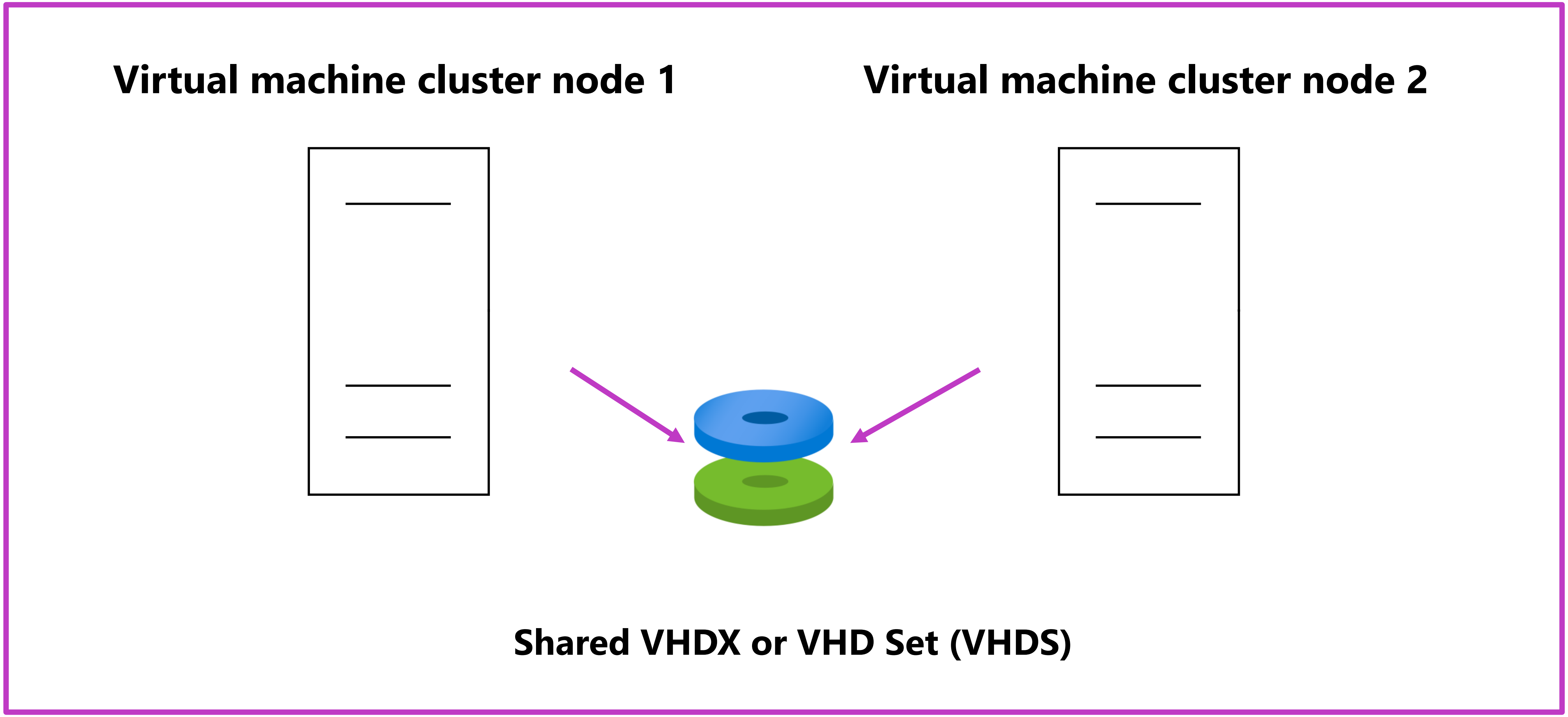
- Up to 64 TB in size
- Recovery from corruption issues
- Supports larger block size resulting in increased performance

Virtual hard disk (2/2)

Azure : Fixed only

Type of disc	Description
Fixed	Allocates all of the hard disk space immediately
Dynamic	The disk only uses the amount of space that needs to be allocated, and it grows as necessary
Differencing	Associated with another virtual hard disk in a parent-child configuration. Any changes made to the differencing disk does not affect the parent disk.
Pass through	Allows the virtual machine to connect directly to an Internet Small Computer Systems Interface (iSCSI) (logical unit number) LUN or a physical disk attached on the host machine

Shared VHDX and VHD Set files



Virtual machine cluster node 1
Virtual machine cluster node 2
Shared VHDX or VHD Set (VHDS)

Manage VM states and checkpoints

A VM can be in one of the following states:

- Off
- Starting
- Running
- Paused
- Saved

Checkpoints:

- Allows you to take a snapshot of a virtual machine at a specific point in time
- Two types of checkpoints
  - Production checkpoints
  - Standard checkpoints
- Maximum of 50 checkpoints per virtual machine allowed

Import and export VMs

When importing a VM you have three options:

- Register the virtual machine in-place (use the existing unique ID)
- Restore the virtual machine (use the existing unique ID)
- Copy the virtual machine (create a new unique ID)

Export options:

- Export a specific checkpoint
- Export a virtual machine with all checkpoints

Configure Discrete Device Assignment (1/2)

Access physical PCIe hardware directly from within a virtual machine through DDA

Example: Virtual machine needs to use a specific graphics adapter, separate from that used by the host

1. Configure the VM for Discrete Device Assignment
2. Dismount the device from the host partition
3. Assign the device to the guest VM

Configure Discrete Device Assignment (2/2)

Deploying devices using Discrete Device Assignment requires some planning.

- ☑ Supported virtual machines and guest operating systems
- ☑ System requirements
- ☑ Device requirements
- ☑ Device driver
- ☑ VM limitations
- ☑ Security
- ☑ PCIe location path
- ☑ MMIO space
- ☑ Machine profile script

Learning recap – Configuring VMs

Knowledge Check

Microsoft Learn Modules (docs.microsoft.com/Learn)

Configure and manage Hyper-V virtual machines

Securing virtualization in Windows Server

Learning Objectives – Securing virtualization in Windows Server

- Guarded fabric
- Attestation modes for guarded fabric
- Host Guardian Service
- Types of protected VMs in a guarded fabric
- General process for creating shielded VMs
- Process for powering on shielded VMs
- Learning recap

Guarded fabric (1/2)

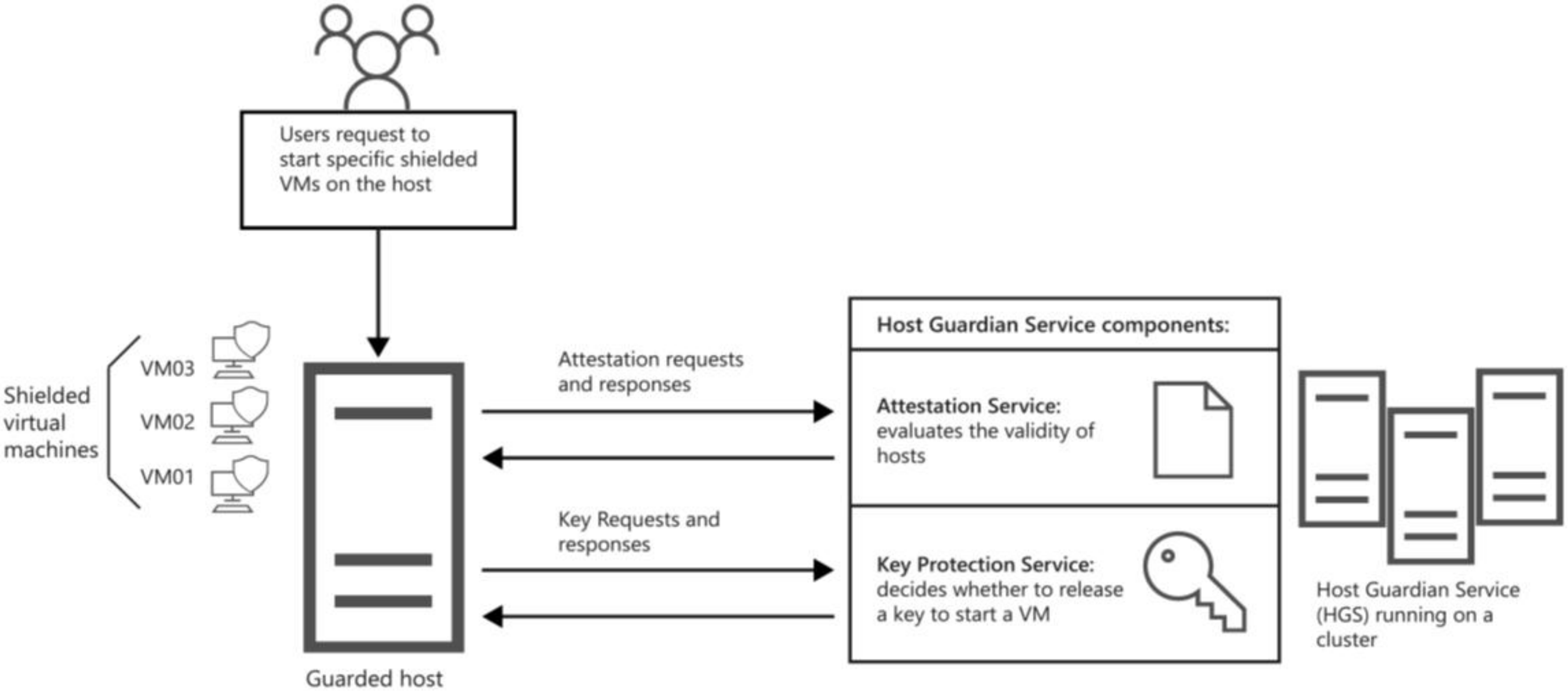
A security solution used to protect virtual machines against:

- Inspection
- Theft
- Tampering from either malware or malicious intent

Security benefits of a guarded fabric include:

- Secure and authorized Hyper-V hosts
- Verification that a host is in a heathy state
- Providing a secure method to release keys to healthy hosts

Guarded fabric (2/2)



Users request to start specific shielded VMs on the host

Host Guardian Service components:

Attestation Service: evaluates the validity of hosts

Key Protection Service: decides whether to release a key to start a VM

Shielded virtual machines
VM03
VM02
VM01
Guarded host
Attestation requests and responses
Key Requests and responses
Host Guardian Service (HGS) running on a cluster

Attestation modes for guarded fabric

Guarded fabric *attestation* is the process of evaluating and validating the Hyper-V host

Attestation mode	Description
Trusted Platform Module (TPM)-trusted attestation	• Hardware-based attestation method offering the strongest protection but does require a more complex configuration and higher host hardware requirements • Requirements include TPM 2.0 and UEFI 2.3.1 with Secure Boot enabled • A guarded Hyper-V host is approved and validated based upon its TPM identity, Measured Boot sequence, and code integrity policies
Host key attestation	• Based upon asymmetric key pairs • Used when existing Hyper-V host machines do not support TPM 2.0 • A guarded Hyper-V host is approved and validated based upon possession of the key

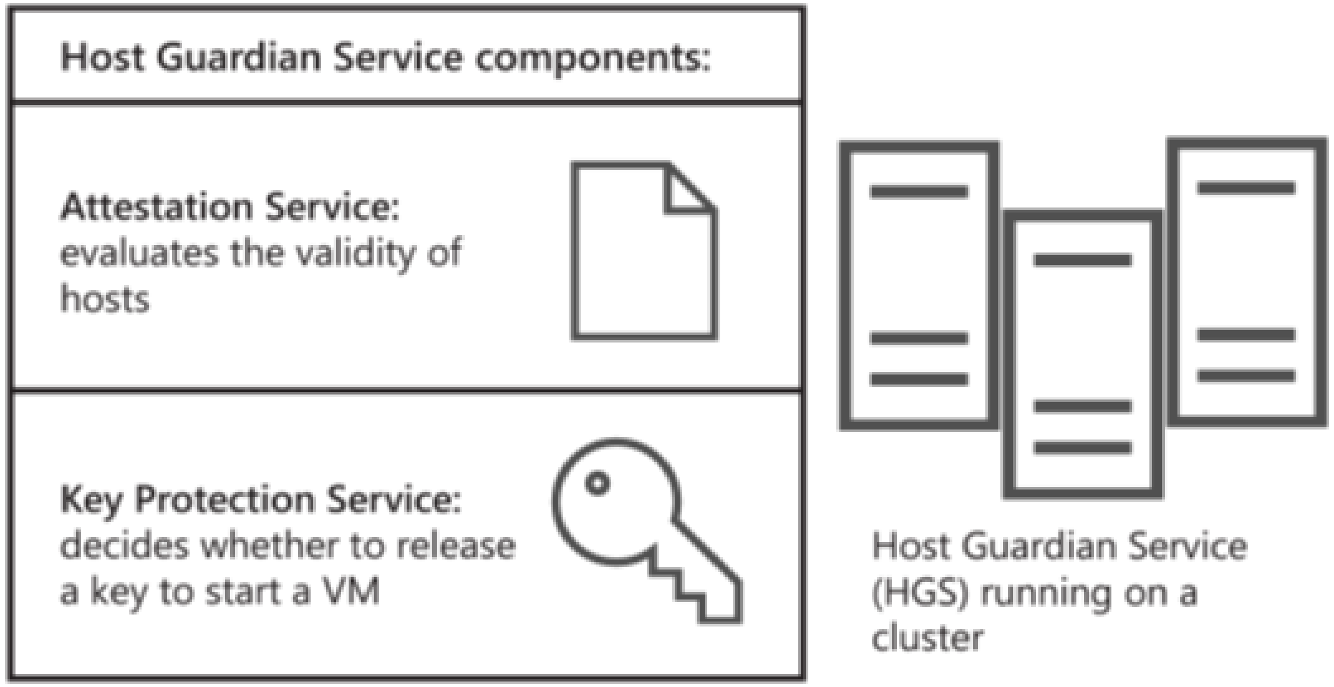
Host Guardian Service

Host Guardian Service includes:

- Attestation service
- Key Protection Service (KPS)

Helps to ensure:

- Protected VMs contain BitLocker encrypted disks
- Shielded VMs are deployed from trusted template disks and images
- Passwords and other secrets are protected when a shielded VM is created
- Control of where the shielded VM can be started



Host Guardian Service components:

Attestation Service: evaluates the validity of hosts

Key Protection Service: decides whether to release a key to start a VM

Host Guardian Service (HGS) running on a cluster

Types of protected VMs in a guarded fabric

Capability	Encryption-supported	Shielded
Secure boot	Yes, required but configurable	Yes, required and enforced
Virtual TPM	Yes, required but configurable	Yes, required and enforced
Encrypt VM state and live migration traffic	Yes, required but configurable	Yes, required and enforced
Integration components	Configurable by fabric admin	Certain components blocked such as PowerShell Direct (enabled in Windows Server v1803), and data exchange

Types of protected VMs in a guarded fabric (*cont.*)

Capability	**Encryption-supported**	**Shielded**
Virtual machine connection, HID devices (keyboard, mouse)	On, cannot be disabled	Enabled for hosts starting at Windows Server v1803; Disabled on earlier hosts
COM/Serial ports	Supported	Disabled (cannot be enabled)
Attach a debugger to the VM process	Supported	Disabled (cannot be enabled)

General process for creating shielded VMs

1. Create a shielded VM template disk

- VHDX disk type
- Globally Unique Identifiers (GUID) partition table
- 2 partitions
- NTFS file system
- BitLocker encrypted
- Shielded Template Disk Creation Wizard

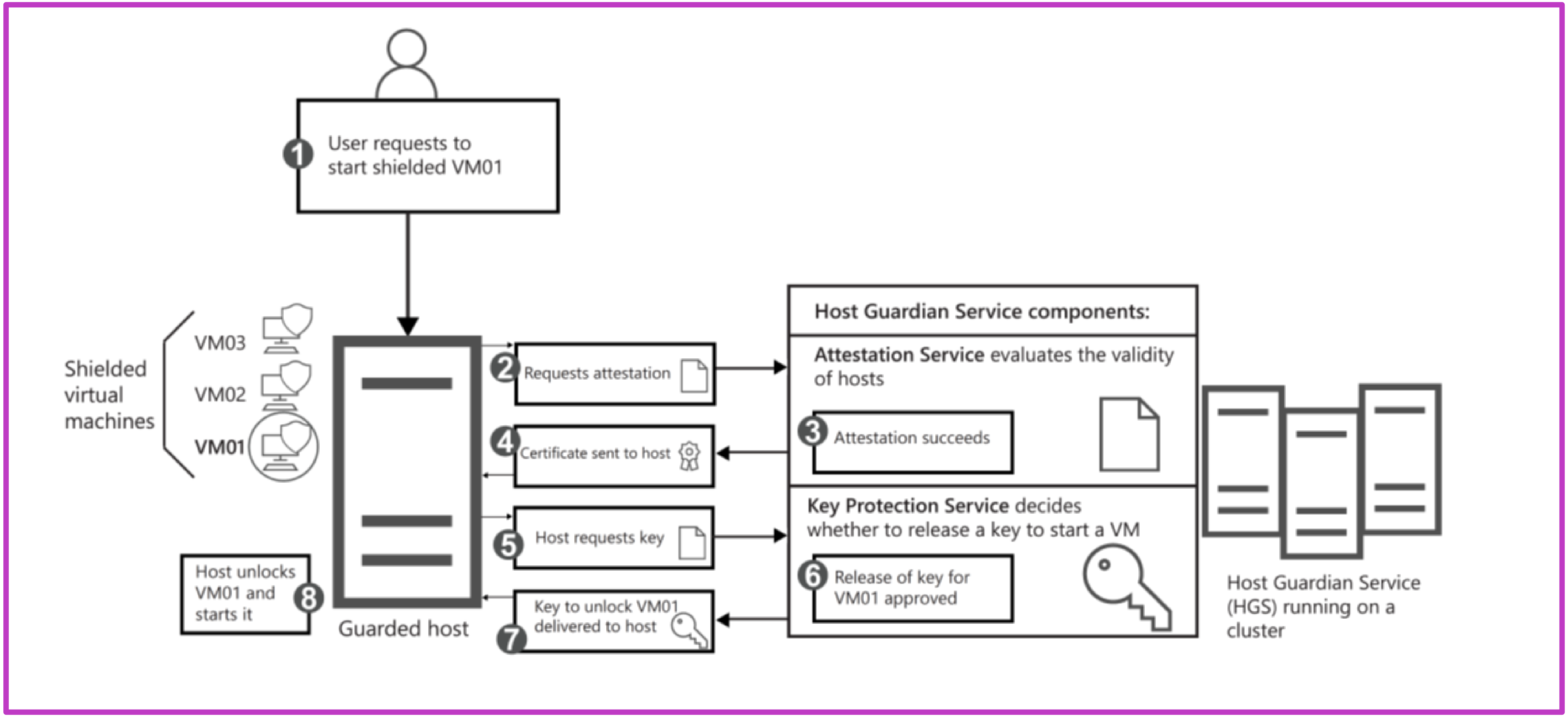
2. Create a shielded data file

- Also called a provisioning data file (PKD)
- Shielding Data File Wizard

3. Deploy a shielded VM

- Deploy using:
  - System Center Virtual Machine Manager (SCVMM)
  - PowerShell

Process for powering on shielded VMs


1 User requests to start shielded VM01
Shielded virtual machines
VM03
VM02
VM01
Guarded host
2 Requests attestation
4 Certificate sent to host
5 Host requests key
7 Key to unlock VM01 delivered to host
Host unlocks VM01 and starts it 8
Host Guardian Service components:
Attestation Service evaluates the validity of hosts
3 Attestation succeeds
Key Protection Service decides whether to release a key to start a VM
6 Release of key for VM01 approved
Host Guardian Service (HGS) running on a cluster

Learning recap – Securing virtualization in Windows Server

Knowledge Check

Microsoft Learn Modules (docs.microsoft.com/Learn)

Secure Hyper-V workloads

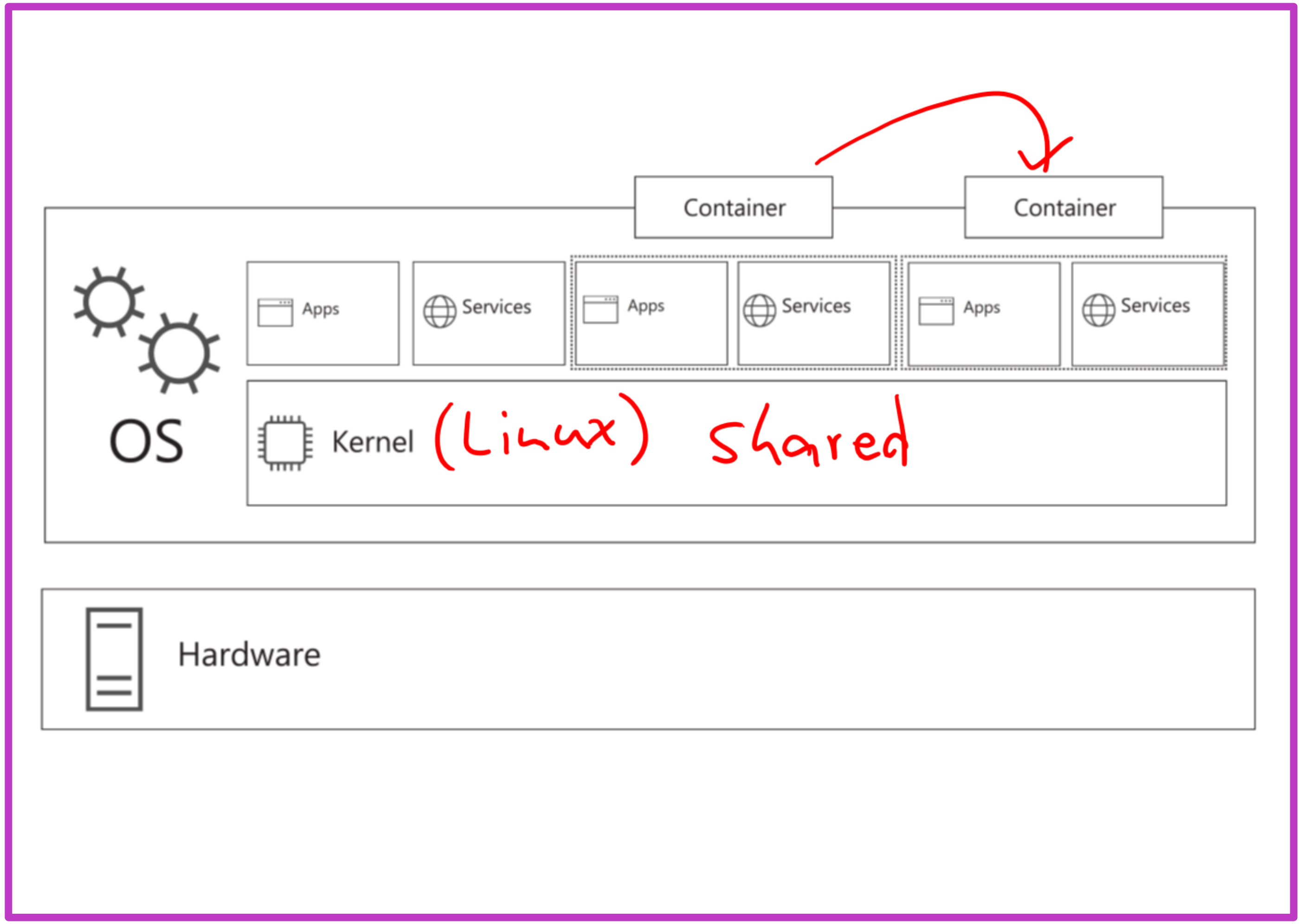
Run containers on Windows Server

Learning Objectives – Run containers on Windows Server

- Define containers
- Containers vs. virtual machines
- Container isolation modes
- Manage containers using Docker
- Download container base images
- Run a Windows container
- Manage containers using Windows Admin Center
- Demonstration: Deploy containers by using Docker
- Learning recap

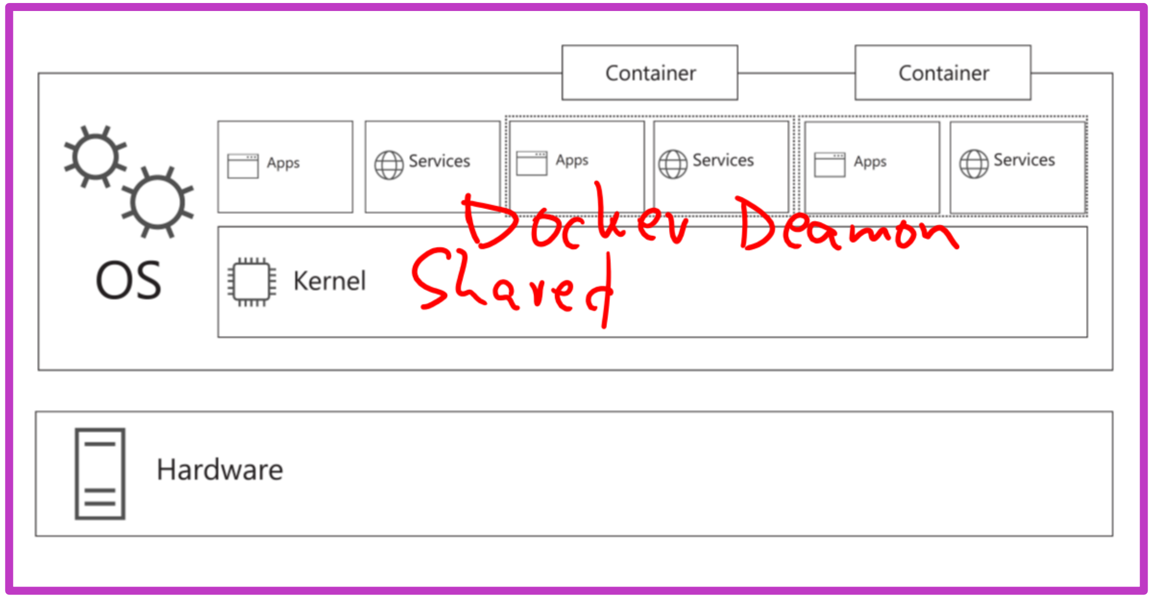
Define Containers

- Package of an application along with all its dependencies
- Lightweight development and runtime environment for applications
- Benefits of using containers:
  - Ability to run anywhere; local workstation, servers, or provisioned in the cloud
  - Isolation ✓
  - Increased efficiency
  - A consistent development environment

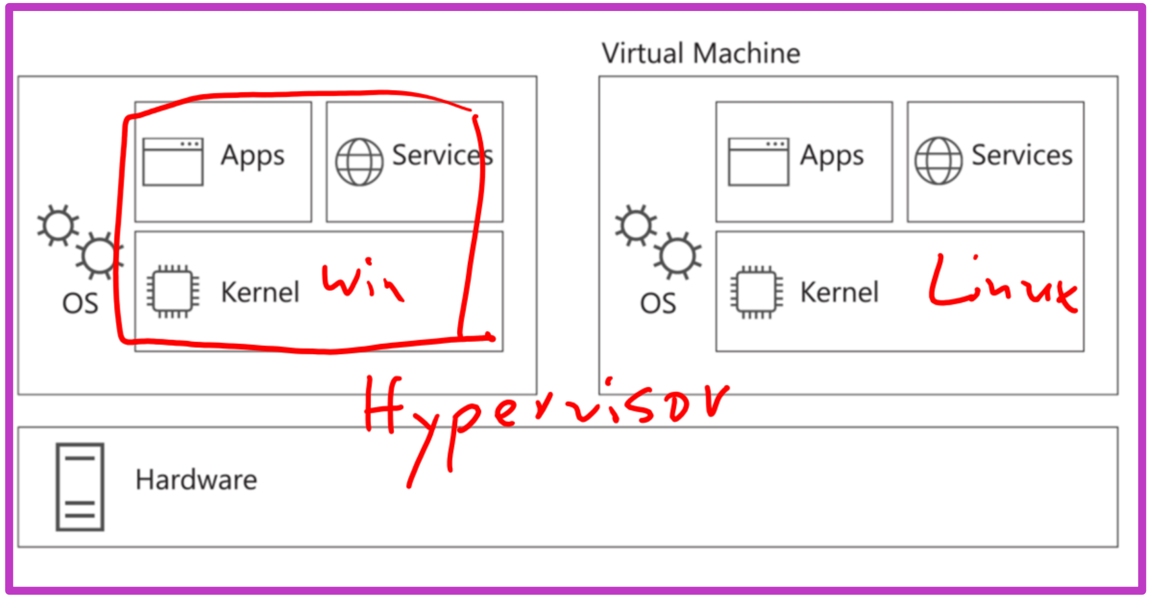


Containers vs. Virtual Machines

Containers



Virtual Machines



Container isolation modes

Process isolation:

- "Traditional" isolation mode
- Containers share the same kernel with each other and the host
- Each container has its own user mode
- Does not provide security-enhanced isolation
- Uses the following switch when starting a container using Docker:
  - **Isolation=process**

zusätzliche SLAT

Hyper-V isolation:

- Each container runs inside of a highly optimized virtual machine
- Each container gains its own kernel and an enhanced level of stability and security
- Also provides hardware-level isolation between each container and the host
- Uses the following switch when starting a container using Docker:
  - **Isolation=process** ?

Manage containers using Docker (1/2)

Docker container:

- Application wrapped in a complete file system including:
  - Code
  - Runtime
  - System tools
  - Supporting files for the app
- Based upon open standards to run on all major operating systems
- Supports any runtime environment or infrastructure; on-premises or in the cloud

Docker container platform includes:

- Docker Engine
  - Runs on Linux, MacOS, or Windows-based operating systems
- Docker client
  - Command line interface to integrate with the engine
  - Runs command to build and manage Docker containers

Docker Desktop

Manage containers using Docker (2/2)

Install one of the following container runtimes on Windows Server:

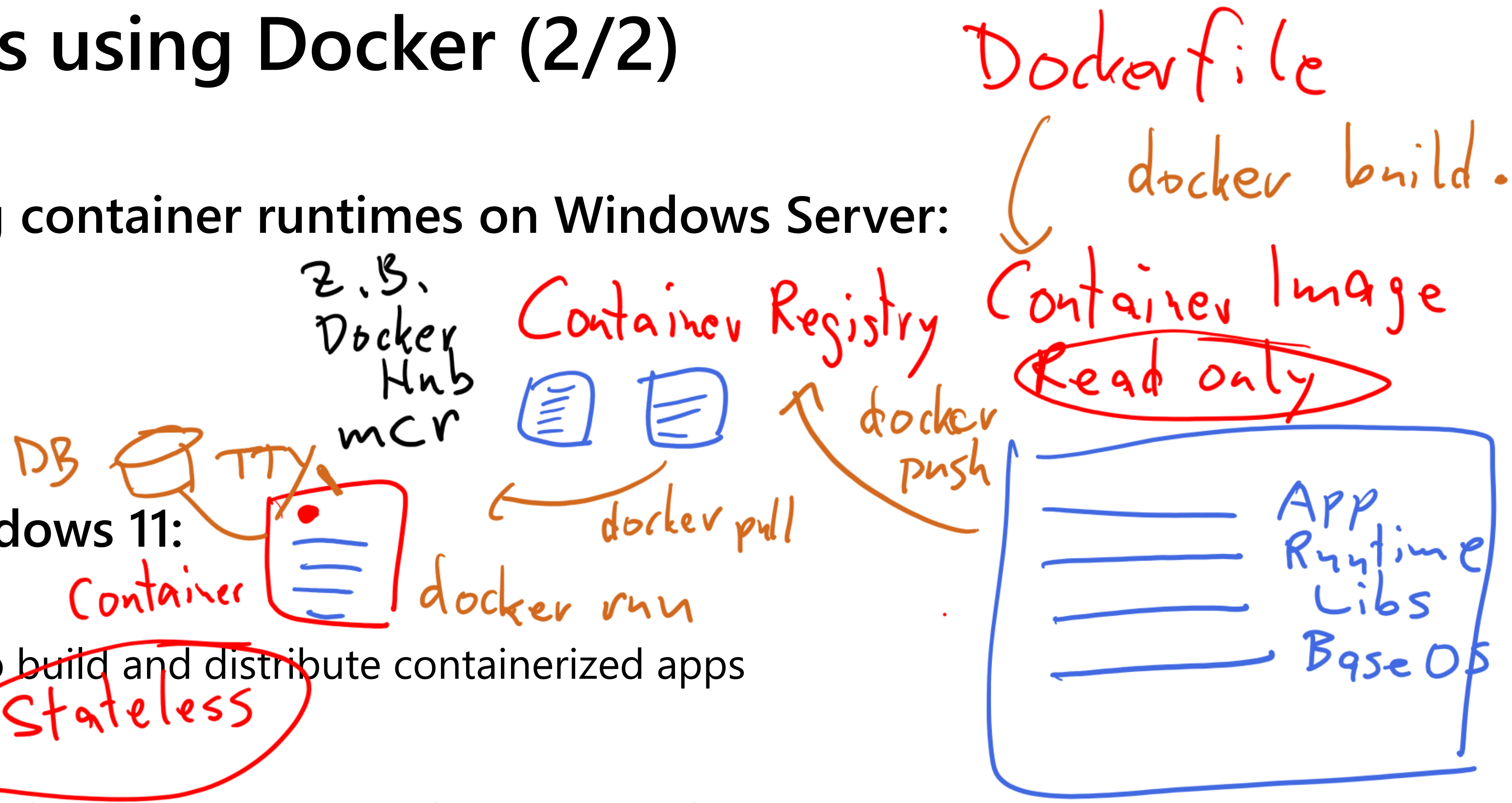
- Docker CE/Moby
- Mirantis Container Runtime
- Containerd

To support Docker on Windows 11:

- Install the Docker Desktop
  - Provides a toolset used to build and distribute containerized apps

Docker Hub

- A web-based library server used to register, store, and manage Docker images
- A community resource with access to over 100,000 shared container images



Base OS Windows
Nano
600 MB

Kubernetes Brendan Burns

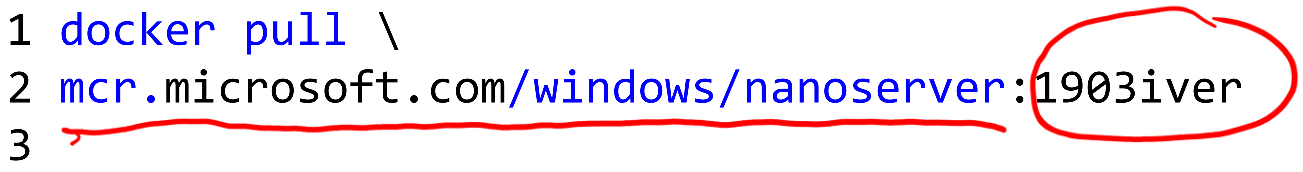
Container images

Container base image:

- Provides a foundational layer of operating system services for a container
- Includes user mode operating system files to support apps
- Includes runtime files and dependencies required by the app
- Use the Docker *pull* command to download images

Four primary container images are available:

- **Nano Server** – support for the .NET Core APIs
- **Window Server Core** – subset of Windows Server APIs and support for traditional .NET framework apps
- **Windows Server** – Slightly smaller than the Windows image, it has full Windows API support and allows more server features
- **Windows** – Includes the full Windows API set



```
docker pull \
mcr.microsoft.com/windows/nanoserver:1903iver

```

Run a Windows container

Methods used to create, manage, and run containers include:

- Automation using a Dockerfile text file and the docker build process
- Manually using Docker commands, as shown in these examples:

Command	Description
docker images	Lists the installed images on your container host
docker run	Creates a container by using a container image
docker commit	Commits the changes you made to a container to a new container image
docker stop	Stops a running container
docker rm	Removes an existing container
docker build	Uses a Dockerfile to automate container image creation

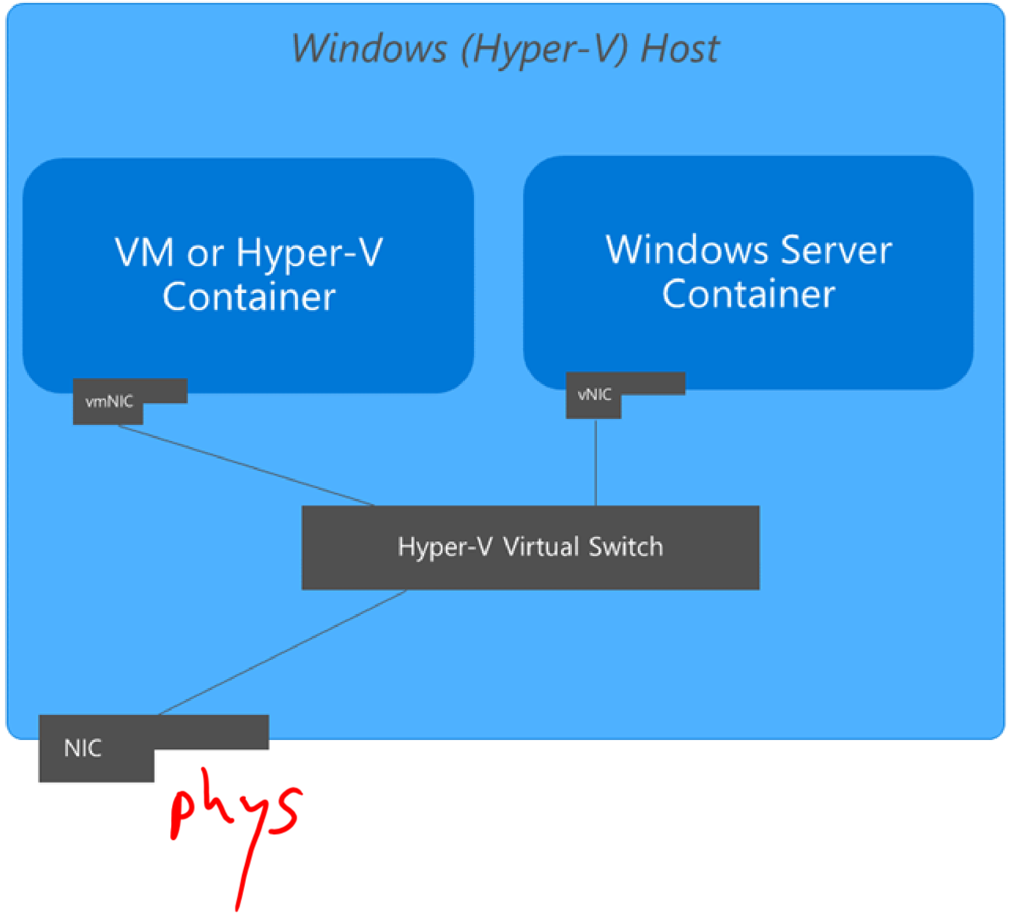
Container networking architecture

Windows supports five different networking drivers or modes

Choose depending on your physical network infrastructure and single- vs. multi-host networking requirements

Docker networking works in conjunction with Hyper-V switches and Windows Firewall to create the network environment

The 'NAT' network is the default network for containers running on Windows



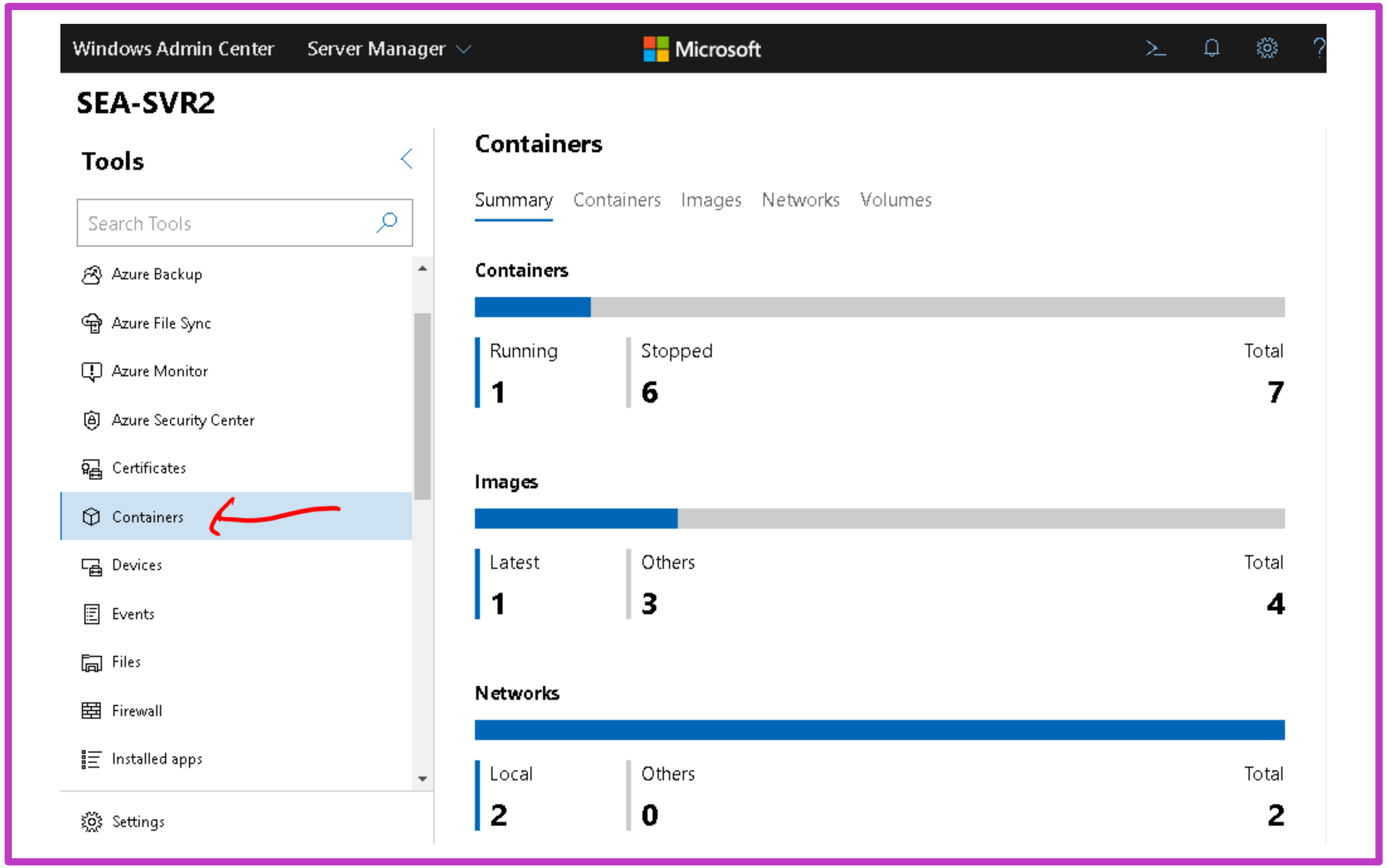
Manage containers using Windows Admin Center

Windows Admin Center:

Browser-based GUI used to manage Windows servers, clusters, and hyper-converged infrastructure

Requires the Containers extension:

- Summary
- Containers
- Images
- Networks
- Volumes



SEA-SVR2

Containers

Containers

Running	Stopped	Total
1	6	7

Images

Latest	Others	Total
1	3	4

Networks

Local	Others	Total
2	0	2

Manage containers using Docker

To install Docker on Windows Server:

1. Install the Docker-Microsoft PackageManagement Provider:
   Install-Module -Name DockerMsftProvider –Repository PSGallery -Force

2. Install the latest version of Docker:
   Install-Package -Name docker -ProviderName DockerMsftProvider

   Docker core platform includes Docker Engine and Docker Client.

Learning recap – Containers in Windows Server

Knowledge Check

Microsoft Learn Modules (docs.microsoft.com/Learn)

Run containers in Windows Server

Orchestrate containers on Windows Server using Kubernetes

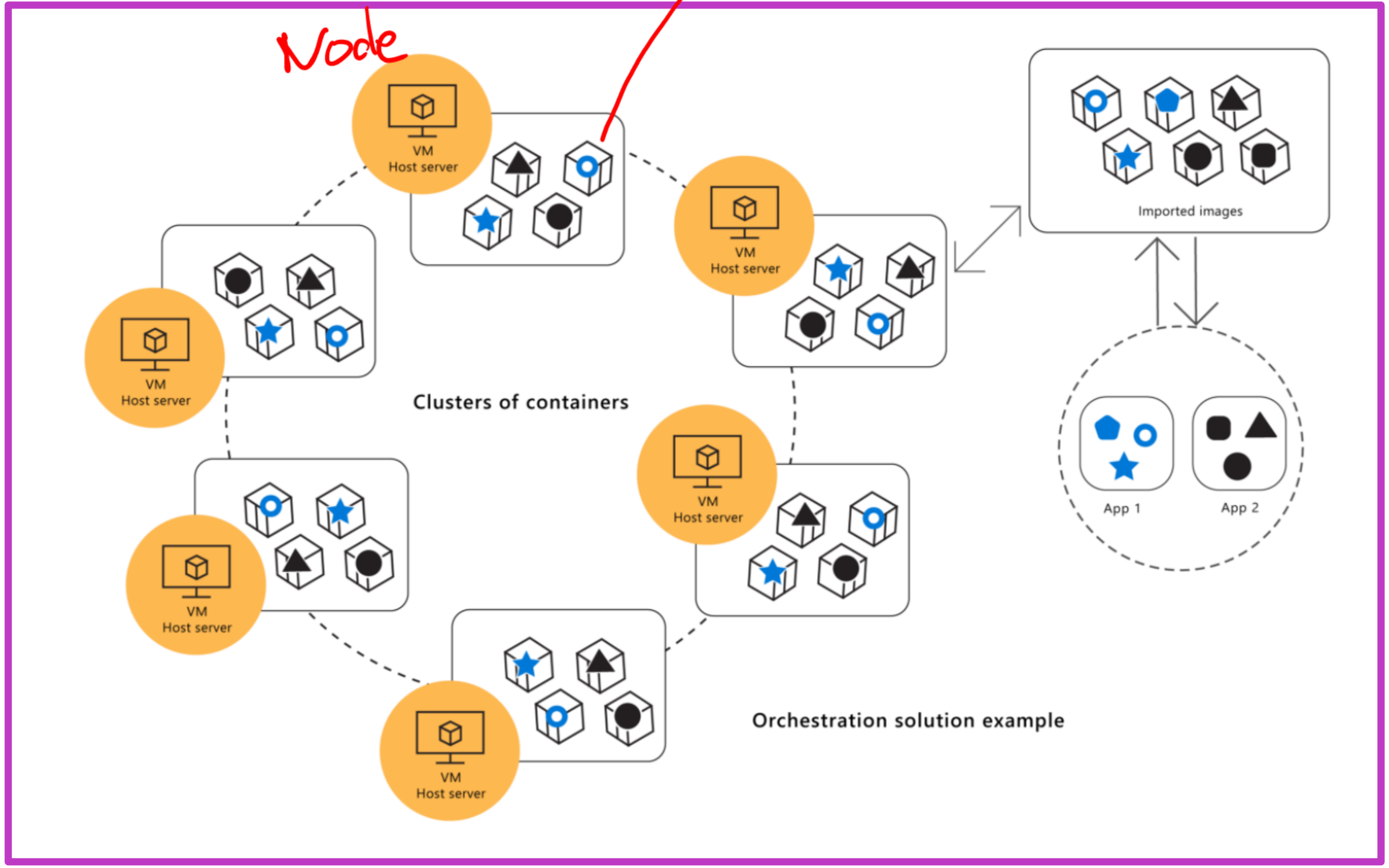
Learning Objectives – Orchestrate containers on Windows Server using Kubernetes

- Describe container orchestration
- Describe Kubernetes
- Describe how to create a Kubernetes cluster
- Describe Azure Arc
- Learning recap

Pod = 1 oder mehrere Container

Define Container Orchestration (1/2)

- Orchestrator to automate and manage large numbers of containers
- Control how the containers interact with one another



Orchestration solution example

Define Container Orchestration (2/2)

Container orchestration involves the following tasks:

- Scheduling
- Affinity/Anti-affinity
- Health monitoring
- Failover
- Scaling
- Networking
- Service discovery
- Coordinated application upgrades

Types of Orchestration Tools:

- Kubernetes
- Docker Swarm
- Apache Mesos

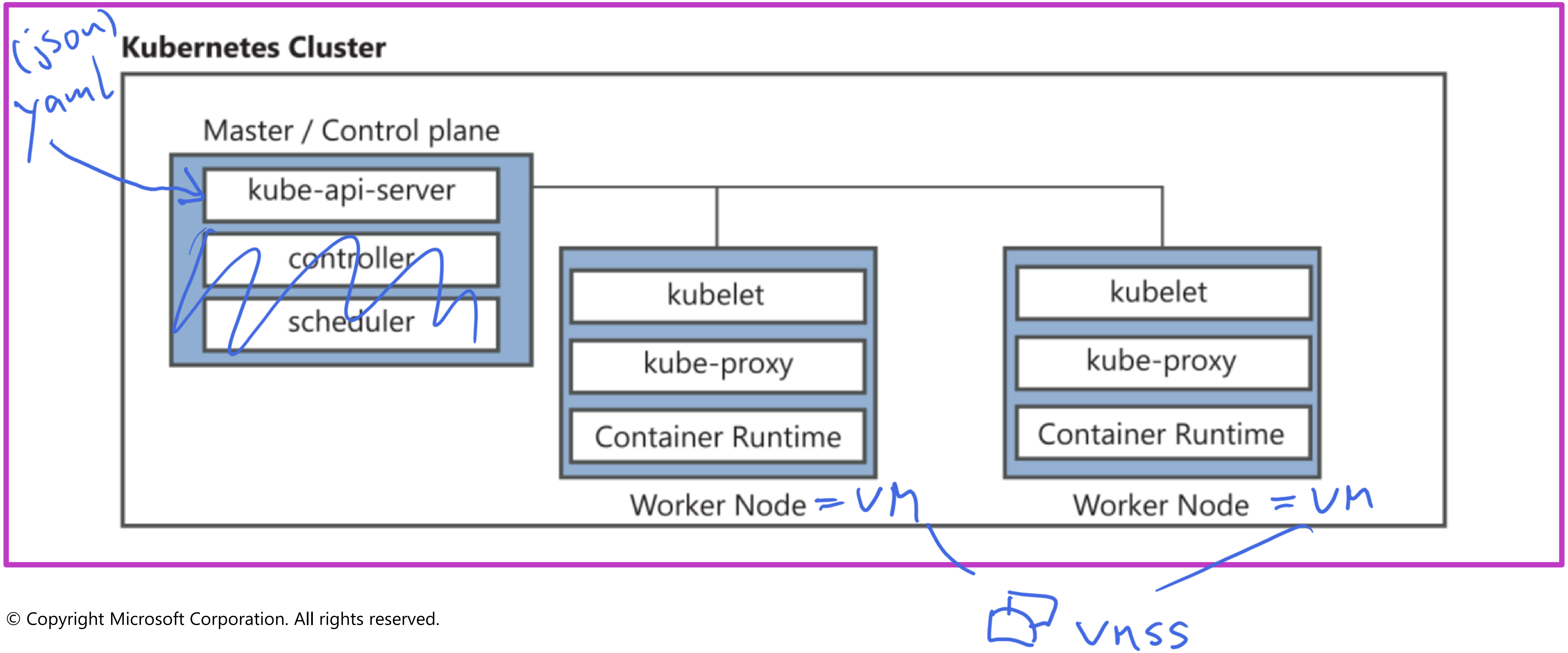
K8S

Kubernetes

Azuer AKS

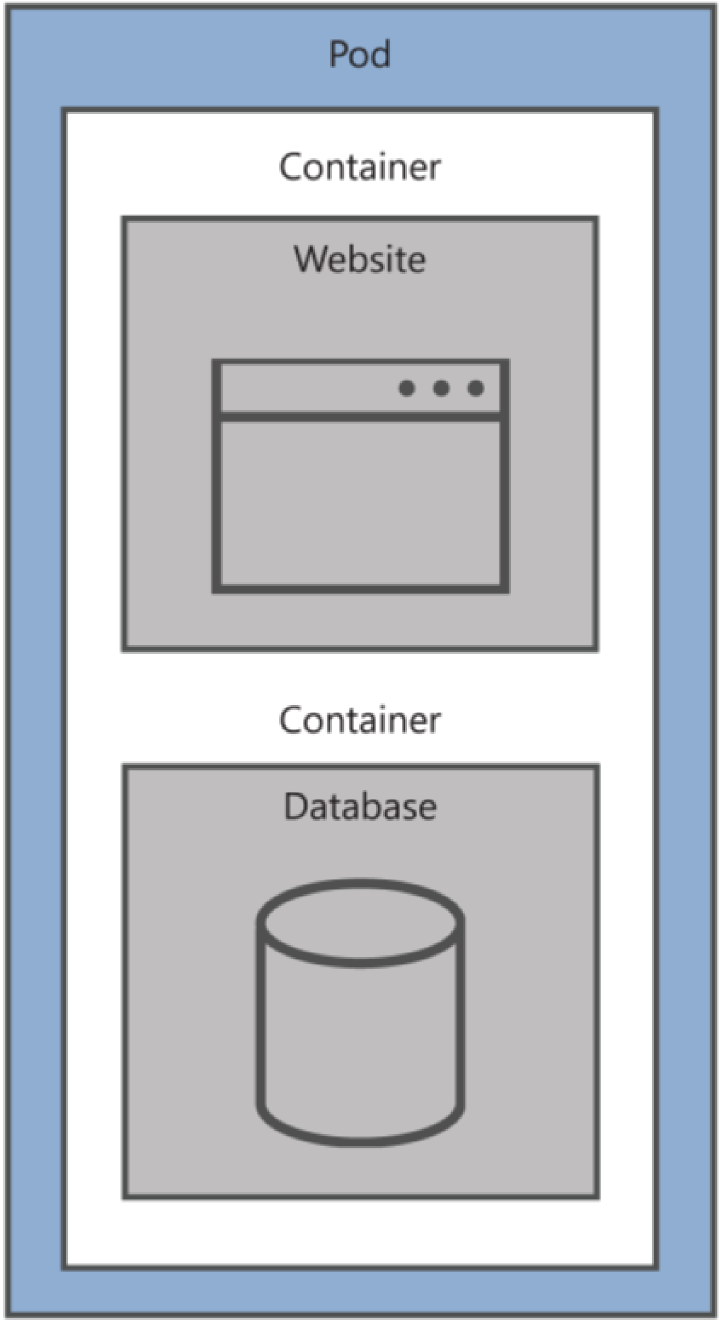
Define Kubernetes (1/2)

Based upon cluster technology where a centralized Master/Control plane is responsible for scheduling and managing components located on multiple nodes within the cluster



Define Kubernetes (2/2)

- Kubernetes Pods:
  - A workload consisting of one or more containers disbursed throughout multiple worker nodes within the cluster
- Includes information about the shared storage, network configuration, and specification on how to run its packaged containers
- Defined as Pod Templates ≈ yaml



Deploy Kubernetes resources

1. **Create a Kubernetes master**
   - Linux operating system
   - *Kubeadm* used to initialize the master and manage cluster nodes

2. **Configure network solution**
   - Used to create routable cluster subnets
   - Linux CNI plugin
   - Flannel, ToR, OvS, OVN

3. **Join worker nodes**
   - Windows Server
   - Linux

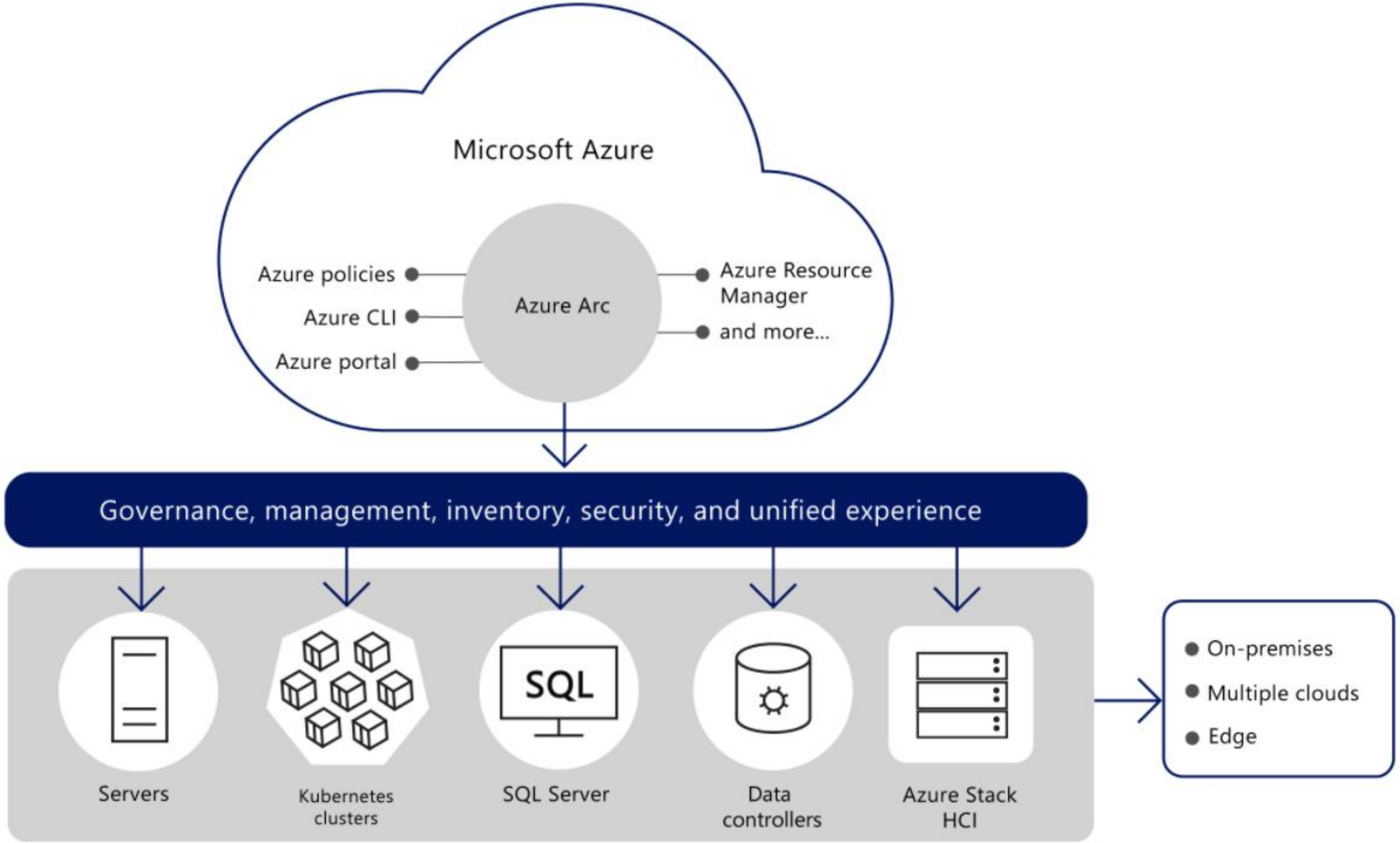
4. **Manage Kubernetes resources**
   - Kubectl used to deploy and manage Kubernetes pods

Cloud services such Azure Kubernetes Service (AKS) reduce many of the challenges of manually configuring Kubernetes clusters by providing a hosted Kubernetes environment

Define Azure Arc (1/2)

- Simplifies the management of complex and distributed environments.
- Extends Azure management to on-premises infrastructure, multiple clouds (including third-party clouds), and edge environments.
- Manage and configure Windows servers, Linux servers, VMware vCenter servers, and Kubernetes clusters that are hosted outside of Azure.
- Manage your IT resources with tools such as Azure Resource Manager, Azure Cloud Shell, the Azure portal, and Azure Policy.
- Extend your organization's DevOps practices, Azure security policies and Azure data services to on-premises, multiple cloud, and edge environments.
- Specific services available in Azure Arc include:
  - Servers
  - Kubernetes clusters
  - Microsoft SQL Server
  - Data controllers
  - Azure Stack HCI

Define Azure Arc (2/2)



Azure Arc-enabled Kubernetes (1/2)

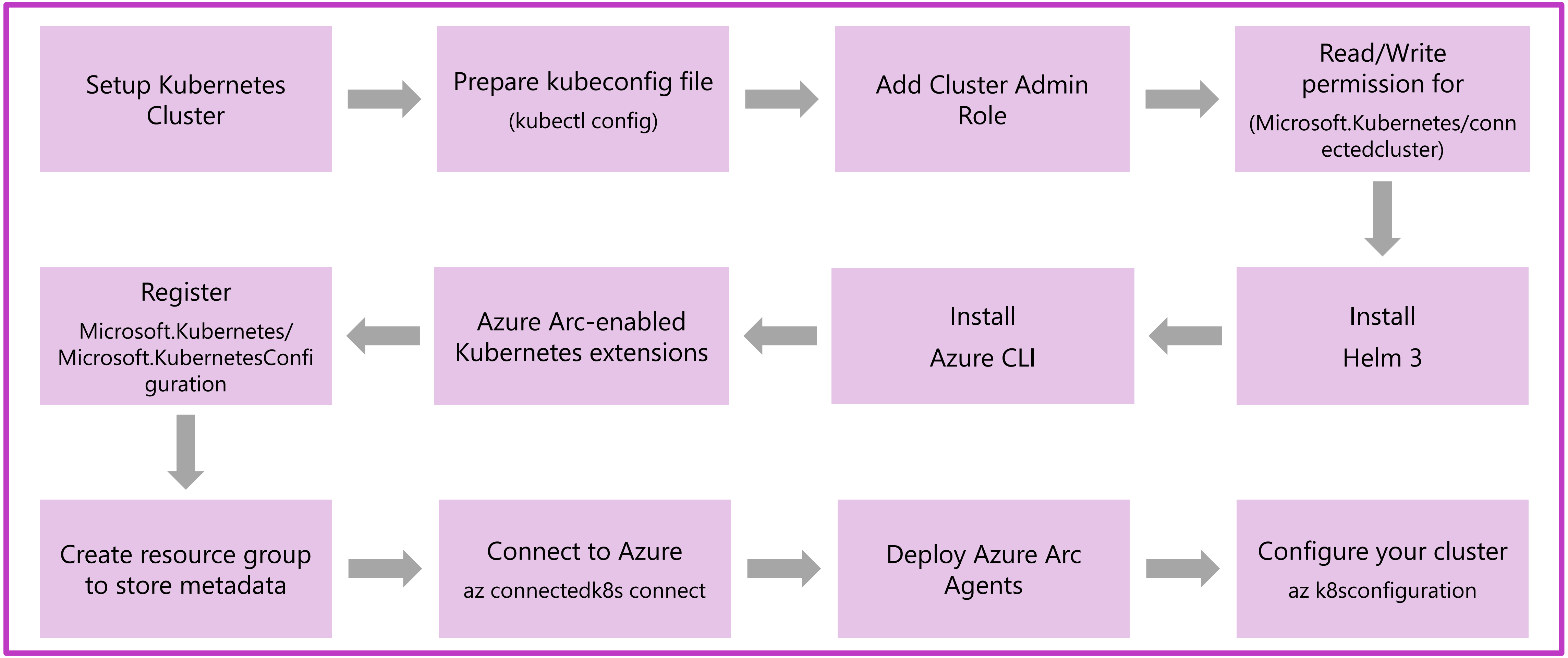
- Connects your Kubernetes clusters with Azure
- Can control your cluster configurations and workloads at scale from files that are stored in your Git repositories.
- Brings an extensive range of Azure features to your Kubernetes clusters
- With Azure Arc-enabled Kubernetes, clusters benefit from Azure management services such as:
  - Azure portal
  - Azure Resource Graph
  - Azure Policy
  - Azure Monitor

Azure Arc-enabled Kubernetes (2/2)

Azure Arc enabled Kubernetes has the following agents:

Kubernetes agents (operators)	**Description**
`deployment.apps/config-agent`	Watches a connected cluster's source control configuration and updates its compliance state.
`deployment.apps/controller-manager`	Orchestrates interactions between Azure Arc components.
`deployment.apps/metrics-agent`	Collects Azure Arc performance metrics.
`deployment.apps/cluster-metadata-operator`	Gathers cluster metadata such as cluster version, node count, and Azure Arc agent version.
`deployment.apps/resource-sync-agent`	Synchronizes cluster metadata to Azure.
`deployment.apps/clusteridentityoperator`	Maintains the managed service identity (MSI) certificate for communicating with Azure.
`deployment.apps/flux-logs-agent`	Collects source control configuration logs.

Connect an Azure Arc-enabled Kubernetes cluster to Azure-Arc



Setup Kubernetes Cluster

Prepare kubeconfig file

(kubectl config)

Add Cluster Admin Role

Read/Write permission for

(Microsoft.Kubernetes/connectedcluster)

Install

Helm 3

Install

Azure CLI

Azure Arc-enabled Kubernetes extensions

Register

Microsoft.Kubernetes/ Microsoft.KubernetesConfiguration

Create resource group to store metadata

Connect to Azure

az connectedk8s connect

Deploy Azure Arc Agents

Configure your cluster

az k8sconfiguration

Learning recap – Overview of Kubernetes

Knowledge Check

Microsoft Learn Modules (docs.microsoft.com/Learn)

Orchestrate containers on Windows Server using Kubernetes

Lab 05 – Implementing and configuring virtualization in Windows Server

Lab 05: Implementing and configuring virtualization in Windows Server

Lab scenario

As part of Contoso's plans to expand virtualization, you will perform a proof of concept to validate using Hyper-V to manage Contoso's virtual machine environment. You will also work with the DevOps team to evaluate using Windows Server containers and managing them in Windows Admin Center.

Objectives

- Create and configure VMs
- Install and configure containers

End of presentation