VMware vSphere VCP 2024 - Data Center Virtualization (VCP-DCV)

Virtualization Basics

Physical Computing

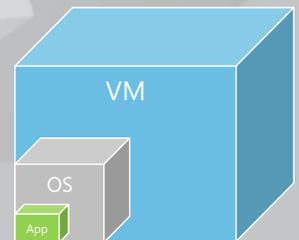| **Physical Environment**	1 server = 1 service Rolling out a service time frame Lack of features Server down, app or service is down

Physical Components

Hardware Server

Physical hardware
Where the OS is installed
CPU, RAM, Storage

Server Operating System

Operating system for serving of services or applications:
        Windows Server 2019
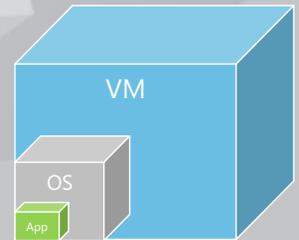   Linux Red Hat

VM

OS

App

The Basics of Virtualization

Virtual Machines- VMs

Self contained hardware-based software
OS is installed inside container
Installed on top of a Hypervisor

Hypervisor

Abstraction layer: Assigns resources to a VM from hardware
Type 1 Baremetal
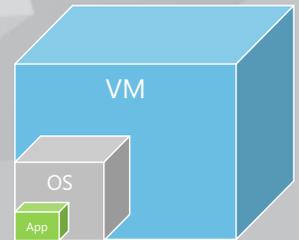Type 2 On top of operating system

VM

OS

App

The Basics of Virtualization

Host

The physical machine, what is traditionally called a server
Where the Hypervisor resides

vCenter Server

Centralized management software
Required for some additional features
NOT required for managing a single host

VM

OS

App

The Basics of Virtualization

Virtual Switches

Host based Networking, Hypervisor configuration
Works like a physical ethernet switch
Detects logically connected VMs

vSphere Distributed Switch

A single switch across multiple hosts
Centrally configured centrally provisioned
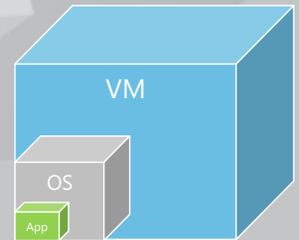vCenter Server configuration
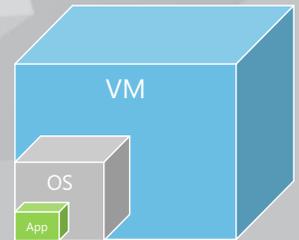
The Basics of Virtualization

Storage

Storage location: SAN, Storage Appliance, Local Storage
Raid Arrays
Where the data resides

vSAN

Amalgamation of storage locations
Multiple hosts local drives turned into SAN
Virtual

VM

OS

App

Traditional Installation
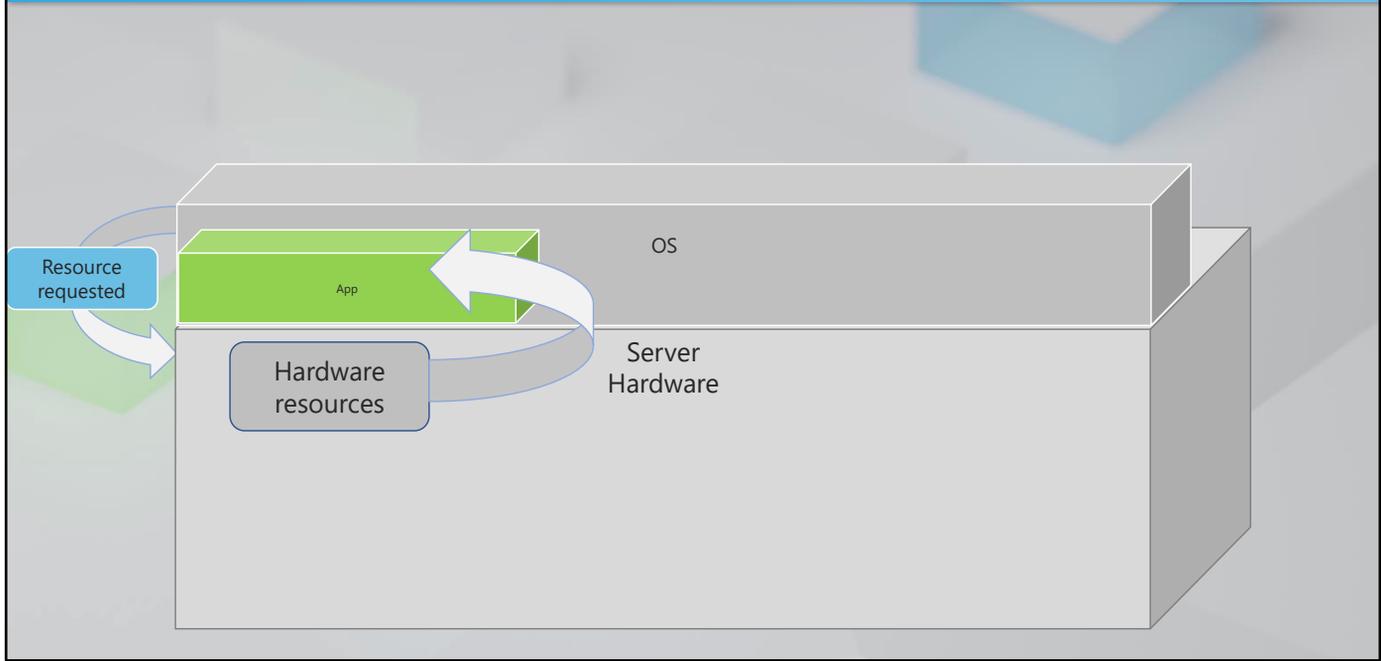
Virtualized Resource Allocation
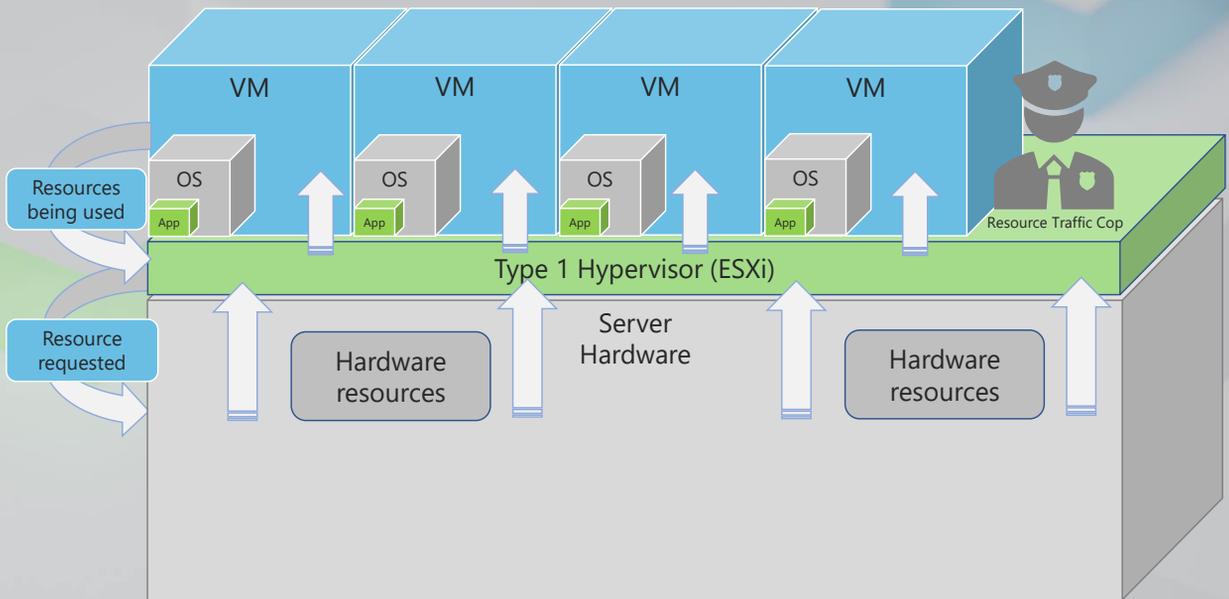
Conclusions

Basic virtualization

Terminology and components

Topology

Data Center Topology
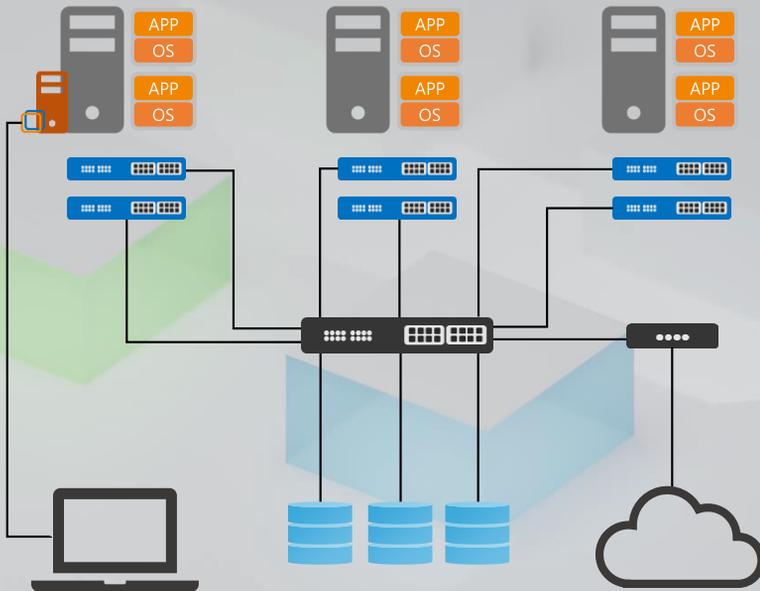
Management Components: vCenter Server

vCenter Server

Host Client

DCUI

Admin

Management Components: Host Client

vCenter Server

Host Client

DCUI

APP
OS
APP
OS

APP
OS
APP
OS

APP
OS
APP
OS

Admin
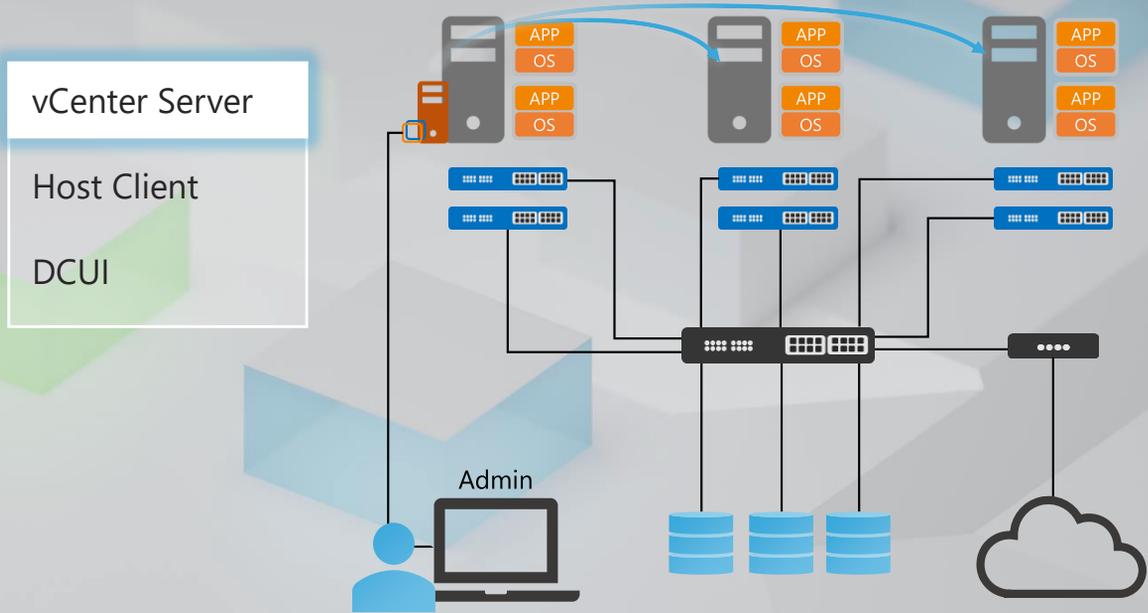
Management Components: DCUI

vCenter Server

Host Client

DCUI

Compute Resources
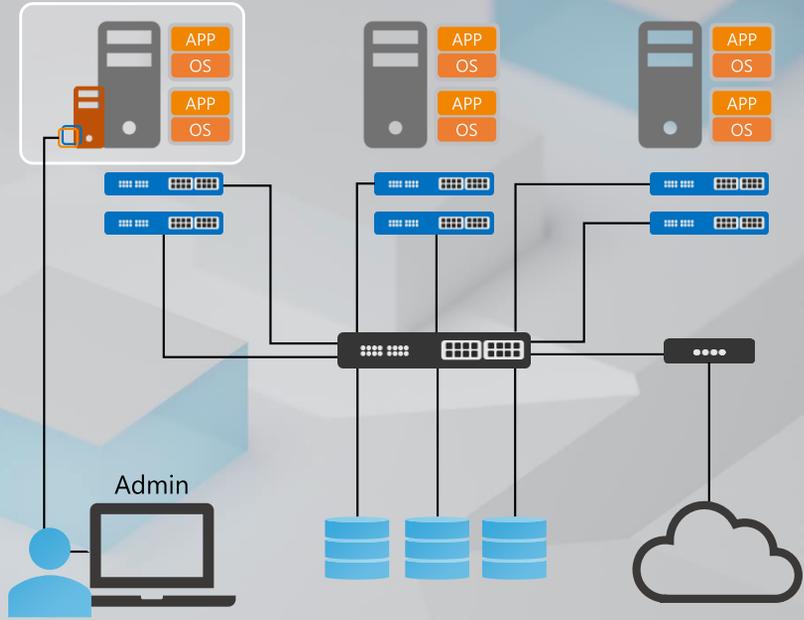
- Hosts
- Clusters
- Resource Pools

APP
OS
APP
OS

APP
OS
APP
OS

APP
OS
APP
OS

Admin

Compute Resources

Hosts

Clusters

Resource Pools

Admin

Compute Resources

Hosts

Clusters

Resource Pools

Admin

Network Components

Physical Networking

Virtual Networking

    Switches

    Switchports

Virtual Networking (NSX)

Distributed vSwitches

APP
OS
APP
OS

APP
OS
APP
OS

APP
OS
APP
OS

Admin

Network Components

Physical Networking

Virtual Networking

    Switches

    Switchports

Virtual Networking (NSX)

Distributed vSwitches

Admin

Network Components

- Physical Networking
- Virtual Networking
  - Switches
  - Switchports
- Virtual Networking (NSX)
- Distributed vSwitches

APP
OS
APP
OS

Storage Components

Physical host HDs

Shared Storage

vSAN

Admin

APP
OS
APP
OS

APP
OS
APP
OS

APP
OS
APP
OS

Storage Components
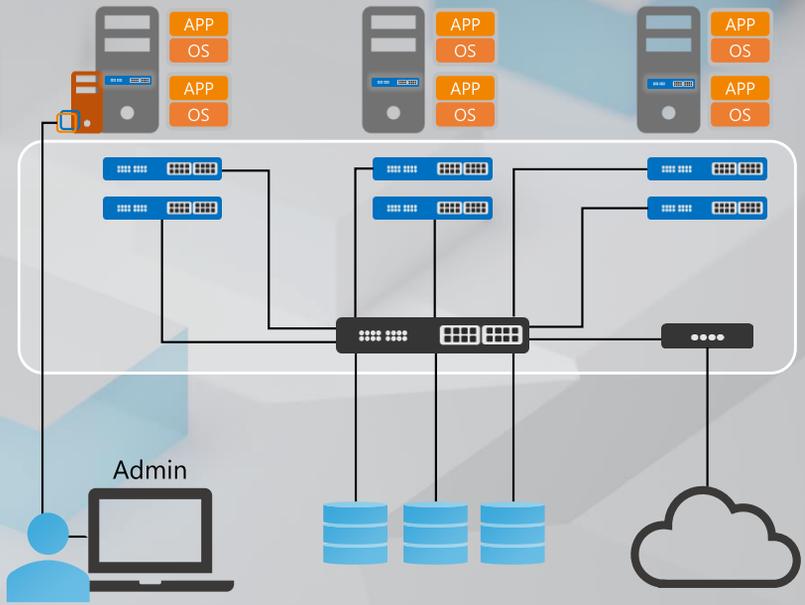
- Physical host HDs
- **Shared Storage**
- vSAN

Storage Components
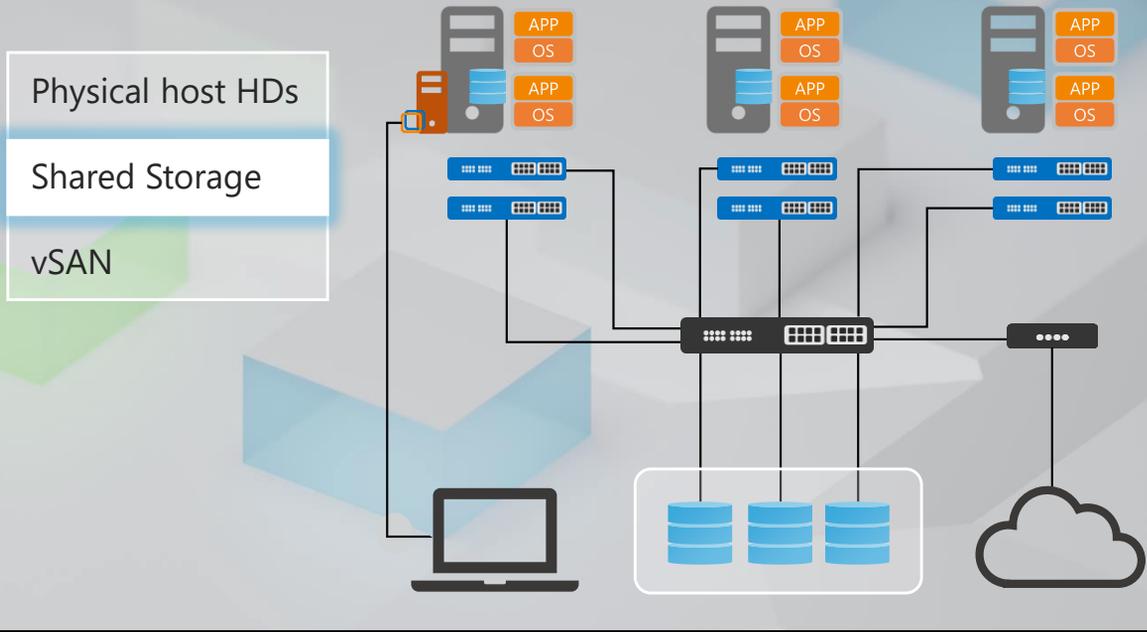
- Physical host HDs
- Shared Storage
- vSAN
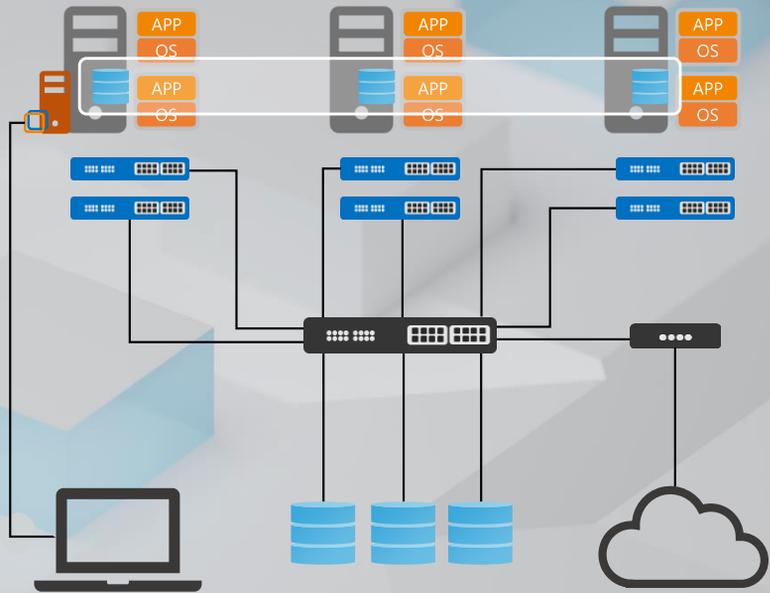
Conclusion

Components

Topology
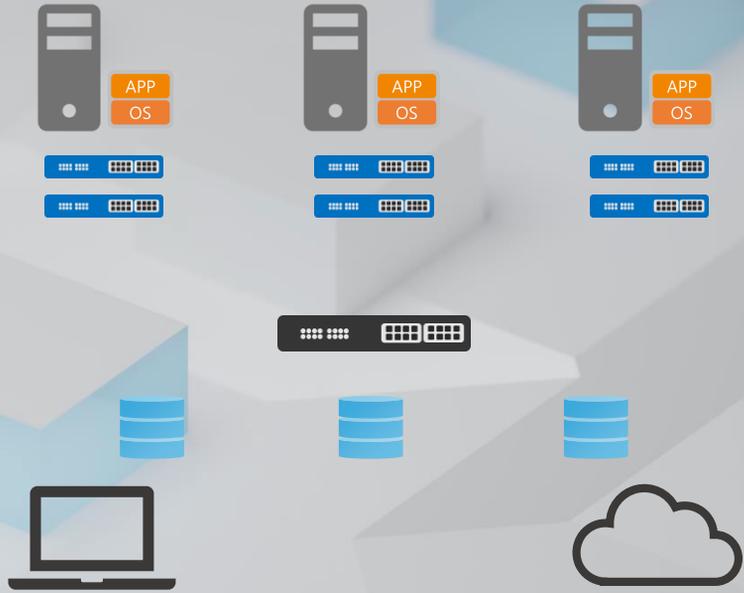
Introduction to vSphere

What is vSphere?

?

Software suite that includes:

ESXi

Management interface

vCenter Server

Management Interfaces

Web Client

vCenter Server

Host Client

DCUI

CLI

DCUI

SSH

Inventory Objects

Inventory Pane

- VMs
- Hosts
- Datacenters
- Clusters
- Resource Pools

Server Plugins

Server Plugins

Ensure support for version you are running

  Local plugins deprecated for v8.0

  Remote plugins recommended

Security concerns

  Some plugins may work but testing is required

Goals of Virtualization

- Hardware independence

- Efficiency

- Flexibility

- Detailed resource allocation

- DR and Business Continuity (uptime)

Advantages and Disadvantages of Virtualization

Advantages

Disadvantages

Advantages and Disadvantages of Virtualization

Advantages

Shared resources

Business Continuity solutions

Flexibility from hardware

No more downtime for maintenance

Disadvantages

Shared resources

Host failure leads to multiple VM failures

Complexity

Advantages and Disadvantages of Virtualization

Advantages

Disadvantages

©2024 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VMware Ecosystem

Horizon

Workspace One

NSX

vSAN

CloudHealth

Carbon Black Cloud/Endpoint

Workstation/ Fuzion

Licensing

Licensing

Features offered are based on licensing

Within the same large version upgrades are free

Is now subscription based

Pricing and Licensing Caps

Per Processor – Licensing

CPUs up to 32 physical cores

No limit to number of VMs

Licenses can be assigned to multiple vSphere hosts

Evaluation Licensing

60 Consecutive days

Not just when you are logged in

All features of the highest product level

Upon expiration:

Disconnected from vCenter Server

Will not be able to power on VMs that are powered off

Features can not be turned on, or if already turned on they may not be altered

Free Licensing (Legacy)

ESXi Free licensing:

    No support from VMware

        Use the community (VMUG, Forums, Etc.)

    No vCenter Server

        Features associated

    API limitations (read only)

    Max : 480 logical CPUs per host

    8 vCPUs max per VM

    RAM and CPU limitations removed in 7.0

[Downloading and licensing vSphere Hypervisor (ESXi 7.x and 8.x) (2107518) (vmware.com)](#)

Standard (Legacy)

vMotion/Storage vMotion

SMP – Multiple Virtual CPUs

Fault tolerance – 2 vCPU

vCenter: HA, Backup, Appliance Migration tool

Virtualization Based Security

Storage Policies

Content Library

Storage APIs

Enterprise Plus (Legacy)

Open Stack Support

Persistent Memory

Host Profiles & Auto Deploy

vMotion (vCenter/Long distance/Cross-Cloud)

Fault Tolerance - 8 vCPU

Virtual Machine Encryption

DRS/DPM

Storage and Network I/O control

Nvidia GRID vGPU

Proactive HA

Accelerated graphics for VMs

Distributed Services Engine

Vendor Device Group

NVIDIA AI-Ready Enterprise Platfm

Trust Authority

On Premises (Legacy)

Standard

- vSphere Hypervisor (ESXi)
- vMotion
- High Availability

Enterprise +

- Tanzu Kubernetes Grid Service
- Distributed Resource Scheduler (DRS)
- Single Root I/O Virtualization (SR-IOV) Support

Cloud Connected

vSphere + Standard

- Cloud Console
- Lifecycle Management Service
- Capacity Visibility Service

vSphere +

- All the features of vSphere+ Standard
- Additional Developer services
- Application performance enhancement features

vCenter Server

Sold separately (except acceleration kit and essentials{Legacy})

	vCenter Server for Essentials	vCenter Server Foundation	vCenter Server Standard
Host #	Up to 3	Up to 4	Unlimited
vSphere licenses	vSphere Essentials and vSphere Essentials Plus	vSphere Standard, vSphere Enterprise Plus and VMware vCloud Suite	vSphere Standard, vSphere Enterprise Plus and vCloud Suite
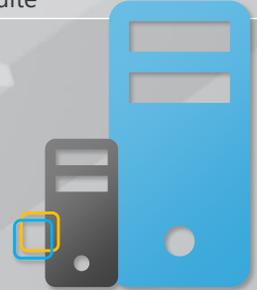
License and Support Price

📅	1-3 Years

🏢	Basic

🏙️	Production

License and Support Price

1-3 Years

Support and Service
Extra $$$

Basic

VMware Basic Support - For Test, Dev and Non-Critical Deployments

Production

VMware Production Support - 24x7 Support for Production Environments

Where are the Licenses at?

In the Evaluation Center
Or
My VMware

What's Different with 8.0

7.0 ➪ 8.0

Distributed Services Engine

vSphere with Tanzu (changes)

Lifecycle Management

AI & ML

Guest OS & Workloads

Resource Management

Security & Compliance

Conclusions

Licensing types

Support contracts

ESXi Installation

ESXi

Review:

ESXi is a bare-metal hypervisor

Acts as a platform for virtual machines

Installed on physical hardware

Controls resource allocation

Requirements for ESXi 8.0

Hosts used to need to meet these requirements:

Category	Requirements
CPU cores	2 (Min)
NX/XD	Enabled for CPU in BIOS
Physical RAM	8 GB Min. / 12GB Rec.
Hardware Virtualization	Enabled
Gigabit / Fast Ethernet Controllers	1+
Installing 8.0 from Boot Disk HDD / SSD (local)	32 GB (Min)
64-bit x86 Processor Support	http://www.vmware.com/resources/compatibility
Platform Support	http://www.vmware.com/resources/compatibility (This link takes you to the hardware compatibility list)

Remote Management Server Models

Model	Firmware
DRAC 9	8.0.30.00
DRAC 7	1.30.30
DRAC6	1.54 , 1.70
DRAC 5	1.0, 1.45, 1.51
DRAC 4	1.75
ILO	1.81, 1.92
ILO 2	1.8
ILO 3	1.28
ILO 4	1.13
ILO 5	2.72
IBM RSA 2	1.03, 1.2

Considerations before Installation

Consider this:

Installation without a local disk or space
can result in degraded ESXi mode

Limited Functionality

Performance Recommendations

Recommendations for performance are similar across 8.0

RAM → 12GB

Management Network and Virtual Machine networks
- Should not be on the same physical network card
- Overtaxes system!

Dedicated GB Ethernet cards
- improve throughput
- Especially to machines with high network traffic

Performance Cont.

Recommendations for performance 8.0

Data and Disks

Data for VMs should be stored on dedicated physical disks

Separate from the ESXi boot image

Virtual Machine File System 6

Installed on first blank local disk

Aligns Starting Sectors

Processors

What is better?

Large Caches

Faster Processors

Log Files Min/Max

Log Files may be:

Automatically Deployed
Set up in a non-default scratch directory
  On VMFS volume

What storage needs to be allocated for Logs?

Log	Max File Size	Min. Disk Space Needed
vSphere HA agent (fdm)	5 MB	50 MB
Virtual Center (vpxa)	5 MB	50 MB
Management Agent (hostd)	10 MB	100 MB

10 Rotations

Prepare to Install!

Step 0: Make sure you have a My VMware account

Step 1: Download the installer for ESXi

https://my.vmware.com/web/vmware/downloads.

Step 2: Check the md5 sum

(Confirms file integrity)

md5 [-c*signature*] [-**l**] [-**n**] [-**u**] [-**v**] [-**d***input_text* | *infile…*]

my **vm**ware·

Register
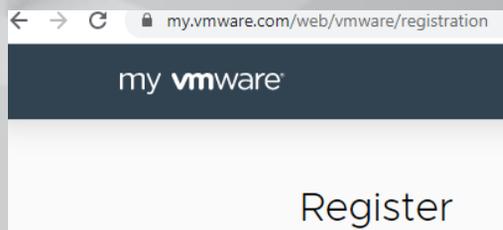
Options for ESXi 8.0 Installation

Interactive Installation

Scripted Installation

Auto-Deploy Installation

Options for ESXi 8.0 Installation

Interactive Installation	For 5 hosts and under
Scripted Installation	Unattended installation Deploy multiple hosts
Auto-Deploy Installation	Available since 5.0 Automatically locates Storage space
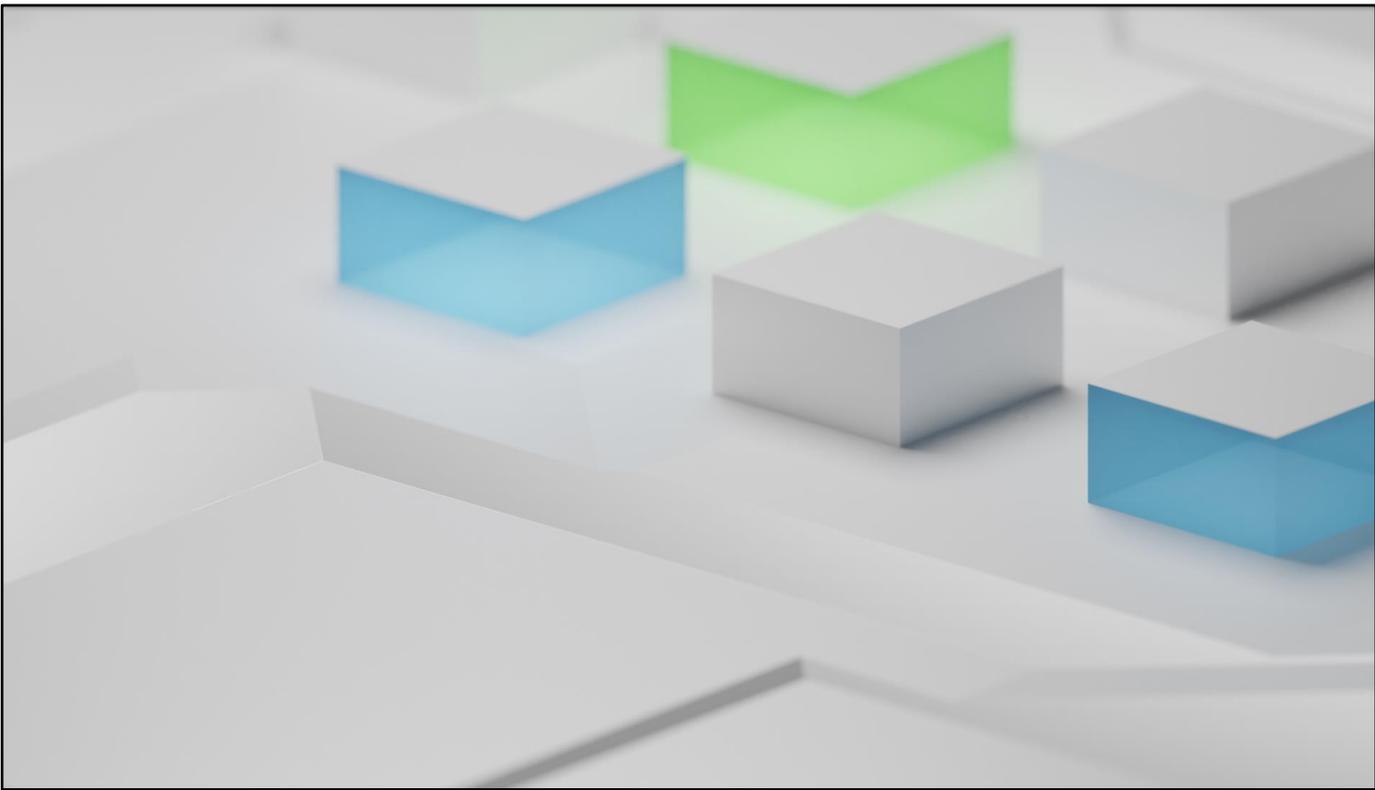
Options for ESXi 8.0 Interactive Installation

For 5 hosts and under

Boot installer from external drive / disk

    CD

    DVD

    USB

    PXE

       On the network

Options for ESXi 8.0 Installation

Utilize Installation Wizard

Boot from External Drive

- Select drive for installation

- If you select SSD you'll wipe the SSD and HDD in the group.

- If you select HDD in a group of more than 2, only the selected is wiped.

- If you select HDD in a group of 2 or less, SSD and HDD are wiped.

Options for ESXi 8.0 Installation

Installation wizard
- Select Keyboard Type
- Enter Root Credentials
- Start Install
- Reboot the host
- Set boot device
  - Same as disk selected previously
- Migrate VMFS data to ESXi host
- 1 ESXi image = 1 ESXi enabled Machine

Scripted Installation

Quickly deploy multiple hosts with ESXi

Scripts

Scripts contain configuration settings

Apply those settings to necessary hosts

Settings can be made unique for each host

Scripted Installation

ks.cfg file

Kickstart file = Installation Script
Can be edited
  Needs:
    Install, Upgrade, or Installorupgrade
    Vmaccepteula
    Rootpw
  Configure:
    Additional drivers
    %POST
    Keyboard
    etc.
  Sample stored at: /etc/vmware/weasel/ks.cfg on host
Stored on:
  FTP, HTTP, HTTPS, NFS shared, USB Flash, or CD/DVD

Scripted Installation

On the installation screen

Quickly! *Shift + O*

```
>ks=nfs://192.168.0.6/storage1/ks.cfg ip = temporaty.ip.address.1 netmask=255.255.255.0
```

^ Points the Installer to the kickstart file

Contains specific configuration settings

Quickly applies those to all desired devices

Or PXE boot:

Create Script (ks.cfg)

PXE Boot Process

Start Install

Auto Deploy ESXi

Quickly provision multiple physical hosts

Allows for specification of:

- Image
- Hosts
- Profiles
- vCenter Server location
    - Makes patches available for ESXi
- Script bundle per host

Completed in vSphere

- ESXi image is loaded directly onto the host's memory
- By vCenter Servers

Auto Deploy Initial Installation Steps

1 Enter the Home tab of vSphere Web Client GUI

2 Select Auto Deploy GUI (int. 6.5)

3 Provision hosts (vCenter Server loads ESXi image on the hosts memory)

4 Configure host with profile that stores ESXi image and configuration on a disk (Optional)

5 Result: Now you have a series of hosts that no longer need vSphere Auto Deploy to provision the hosts.
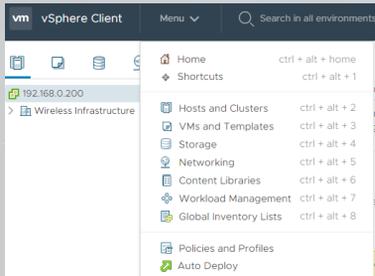
Conclusions

ESXi Installation

Requirements

Installation Options
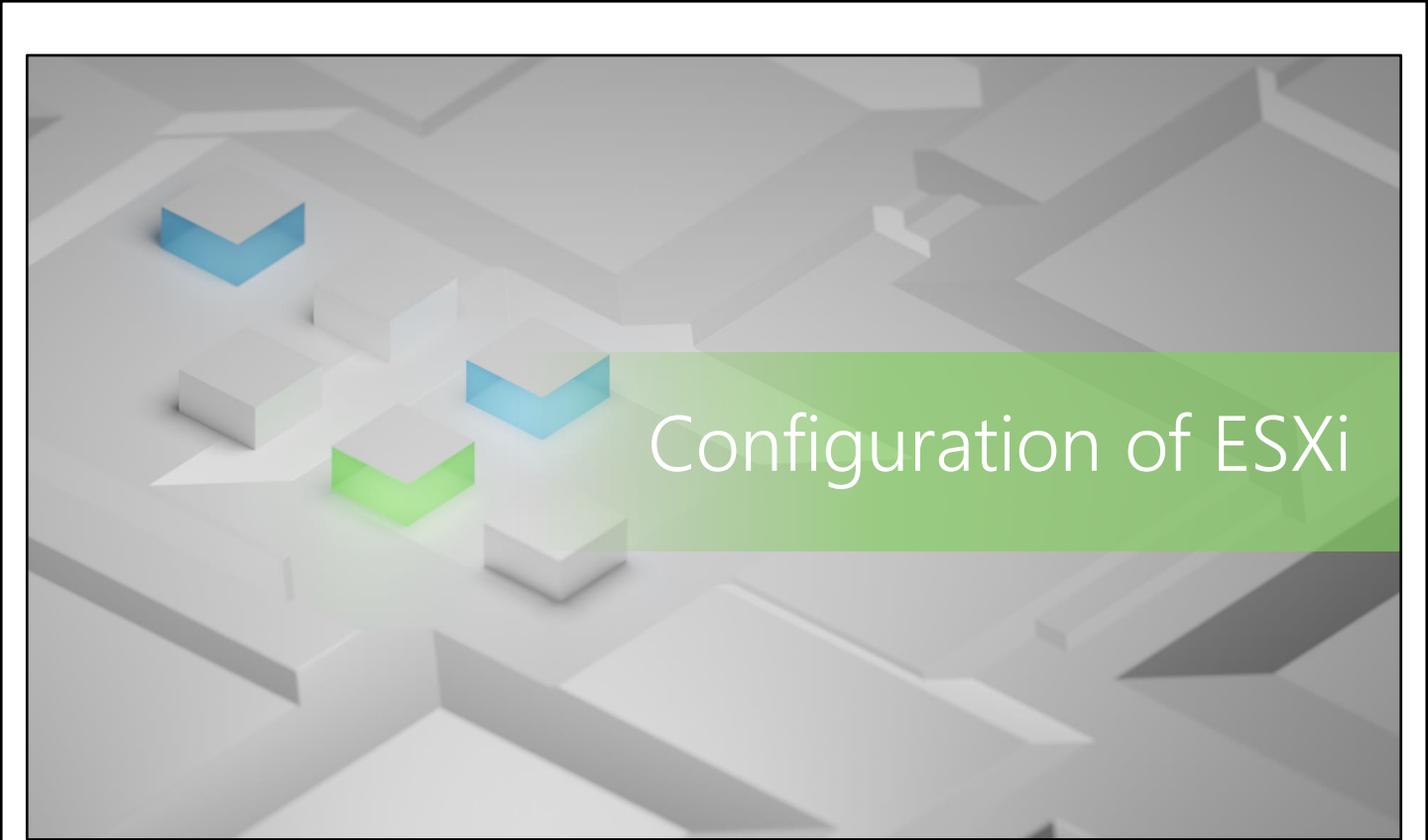
Configuration of ESXi

Configuring ESXi

Initial Configuration

Starts automatically

Configures default:

- System settings
- Network settings
- Storage settings

ESXi Console Interface

Console Interface used for:

Configuration changes

Access control

Troubleshooting

Appears after Autoconfigure completes

Or Accessed via vSphere Client

F2: Configuration changes

Enter: Select Item / Save / Exit

Spacebar: Toggle Value

Common Starting Tasks for Configuration

Configure keyboard

Security Banner

Created in vSphere Client

Appears in console after completion

Direct console redirect to serial (Optional)

Manually in the boot options

In vSphere Client

Common Starting Tasks for Configuration


```
System Customization                    Configure Password
─────────────────────────────          ─────────────────────────────
Configure Password                      Set
Configure Lockdown Mode
                                        To prevent unauthorized access to this system, set the
Configure Management Network            password for the user.
Restart Management Network
Test Management Network
Network Restore Options

Configure Keyboard
Troubleshooting Options

View System Logs

View Support Information

Reset System Configuration




<Enter> Change                                          <Esc> Log Out
```

Remote Management

Options for Remote Management of ESXi hosts

Host Client

http(s)://host-name/ui

http(s)://host-ip-address/ui

vSphere Client

vCenter Server

Creating Credentials for Admins

Root Account

By default, has no password

Configure in Direct Console → Configure password → New password → Enter

Creating Credentials for Admins

Prepare the Network for ESXi

ESXi can have the management IP address entered in either:

vSphere

DHCP based IP address works

DCUI

Can't use DHCP based IP address

DHCP does not provide ESXi with IP address

Check the Network Settings

Check or Change the assigned IP address:

Check:

- DHCP provides ESXi with an IP address
- Check the address in the DCUI
- Use this to connect to host form vSphere Client
- Change
- In DCUI
- Configure Management Network Options
- IP Settings
- IPv4 or IPv6
- Set address
- Enter
- ESC > Y

Configure Management Network

From Configure management network you can change other settings:

- Network Adapters

- VLAN ID

- DNS

  - DNS Configuration

    - Use the following DNS server addresses and hostname

- Custom DNS suffixes
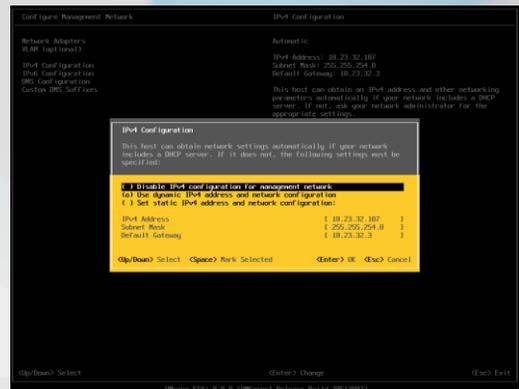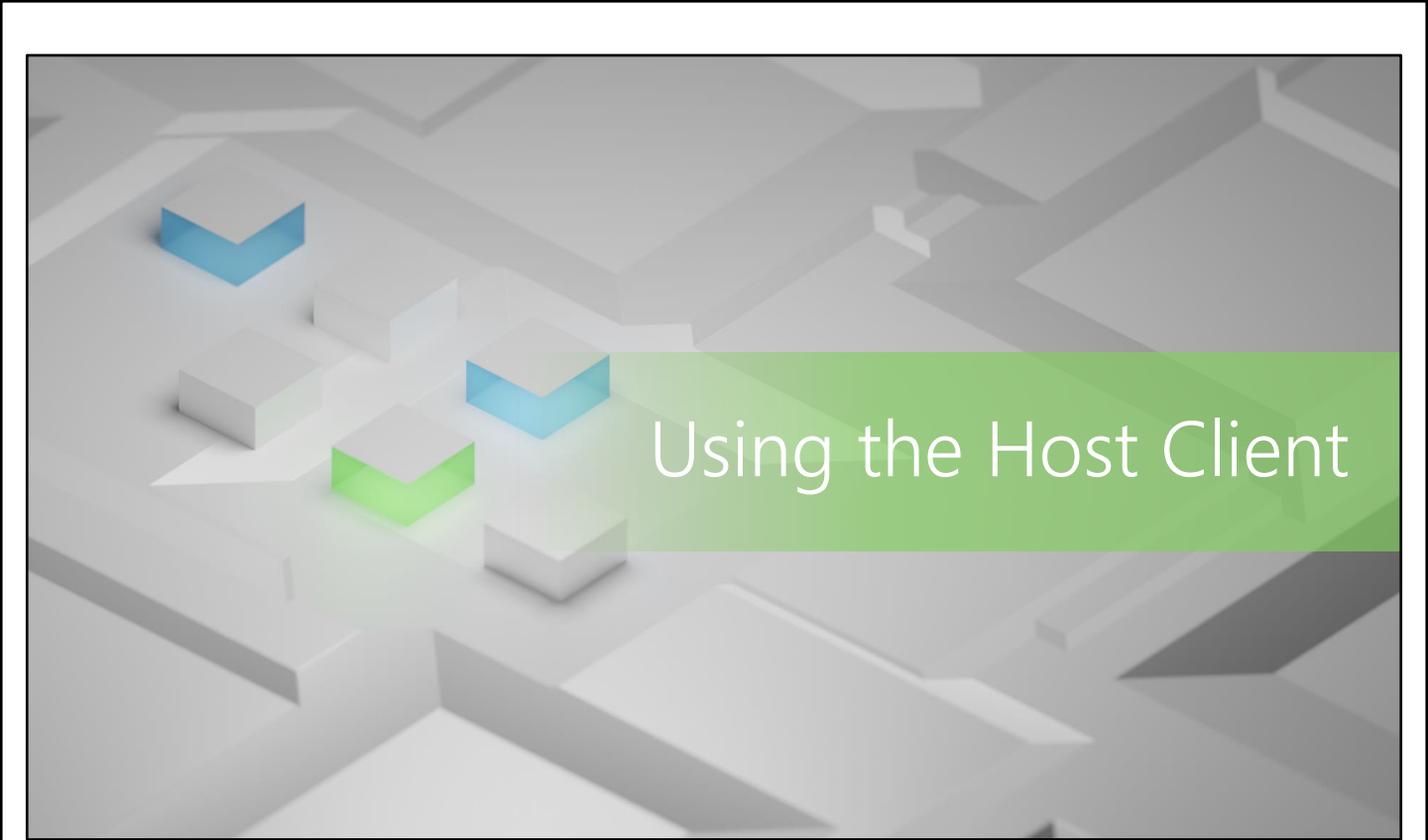
Using the Host Client

VMware Host Client

Used to manage an individual Host

Useful for:

- Troubleshooting

- Administrative tasks

- *Need Admin Privileges*

Access the host:

http://host-ip-address/ui

(DEMO in the OUTLINE)
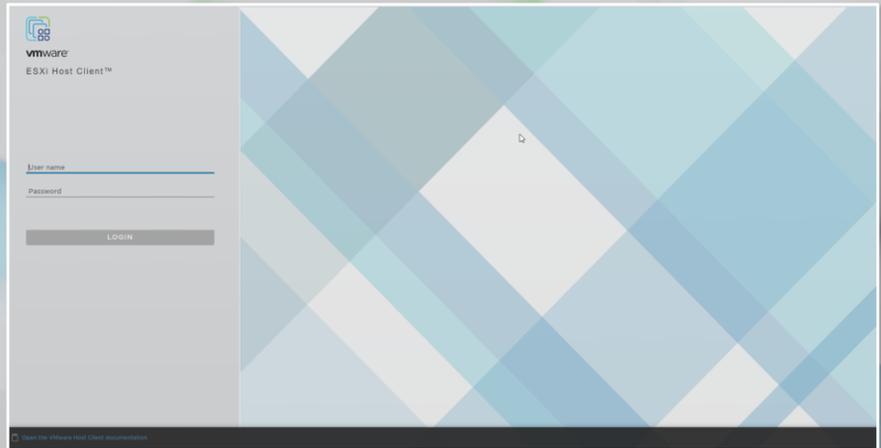
Enable Logging

Logging is critical to monitoring your virtual network

In the vSphere Client:

Find the host you want to enable logging on
Configure
System → Advanced System Settings
Edit
Syslog
Set up desired logging system preferences

Syslog Options
Default Rotate
Default Size
LogDir
LogDirUnique
Log Host

Enable Logging

Post Installation

ESXi is installed

Devices are configured

Network is set up
- Now what?

It's time to manage devices:
- Manage Remotely with:
    - vSphere Client
        - Simple GUI
    - vCenter Server
    - VMware Host Client
        - Connect directly to ESXi host and manage

Manage Hosts and VMs

VMware Host Client

vCenter Server

vSphere Client

Ease of access to console

Launch in a:

- Web based console
- Or
- Remote Console
- If installed

Manage Hosts and VMs

From vSphere you can manage:

- Remote Console
- Virtual Hardware
    - Device Settings
    - Add a new Device
- Permissions
- Datastores Used
- Network Settings
- Current Configurations
    - Policies
    - Alarms
    - User Mappings

Post Installation

It's time to manage storage:

vSphere is an excellent tool for:

Monitoring storage

- Configuring new datacenters
- Managing permissions
- MOTD
- Security Management
- Managing the vSAN
- Health Checks

Post Installation

It's time to manage storage:

Create Datacenters

Configure Datacenters

Capacity

Storage Control

Space Reclamation

Post Installation

It's time to manage storage:

Storage and CPU usage

Post Installation

It's time to manage the network:

Monitor Activity

Manage Permissions

Move your VMs to other networks

Destination network

Which VMs

Complete

Issues with ESXi 8.0

Dell EMC PowerEdge Servers

Upgrading to ESXi 8.0 from earlier versions fails with vmkapi DependencyError

Drivers built with older vmkapi version dependencies

Deprecated form ESXI 8.0

Best Practices – CPU/Power

Monitor CPU usage of hosts

Limit CPU allocation to VMs

Overuse consumes resources

Use more small virtual machines

Scaling out

Use proper power management mode

High performance

Balanced - Default

Low power

Custom

Best Practices - Memory

Memory

Allocate enough memory to ensure performance

Minimize thrashing

Avoid over allocation

Increases overhead unnecessarily

Overhead can't be reclaimed!

Memory management mechanisms

Page sharing

Ballooning

Memory Compression

Swap to host Cache

Regular Host-Level Swapping

Best Practices - Storage

Storage
- vStorage APIs for Array Integration (VAAI)
  - Massive Performance gains in VDI environments
  - Automatically used if SAN supports
  - True for NAS Storage
    - *If vendor specific plug in is present*

Pick a virtual disk mode
- Independent Persistent
  - Best performance
- Independent nonpersistent
  - Redo Logs
- Dependent
  - Snapshots used for disk writes
  - Appended to redo log

Best Practices - Disks

```
                        ┌──────────────┐
                        │  Disk Type   │
                        └──────┬───────┘
              ┌────────────────┴────────────────┐
     ┌────────┴─────────┐              ┌─────────┴────────┐
     │ Thick Provisioned│              │ Thin Provisioned │
     └────────┬─────────┘              └─────────┬────────┘
   ┌──────────┴───────────┐          ┌───────────┴──────────┐
   │ Allocated disk space │          │ Space is allocated and│
   │     at creation      │          │  zeroed on first write│
   └──────────┬───────────┘          └──────────────────────┘
      ┌───────┴────────┐
 ┌────┴─────┐    ┌──────┴──────┐
 │Eager zeroed│   │ Lazy zeroed │
 └────┬─────┘    └──────┬──────┘
┌─────┴──────┐   ┌──────┴──────────────┐
│All space   │   │All space allocated  │
│allocated and│  │at creation, but     │
│zeroed at    │  │zeroing occurs per   │
│time of      │  │block on first write │
│creation     │  └─────────────────────┘
└────────────┘
```

vCenter Server Installation

ESXi
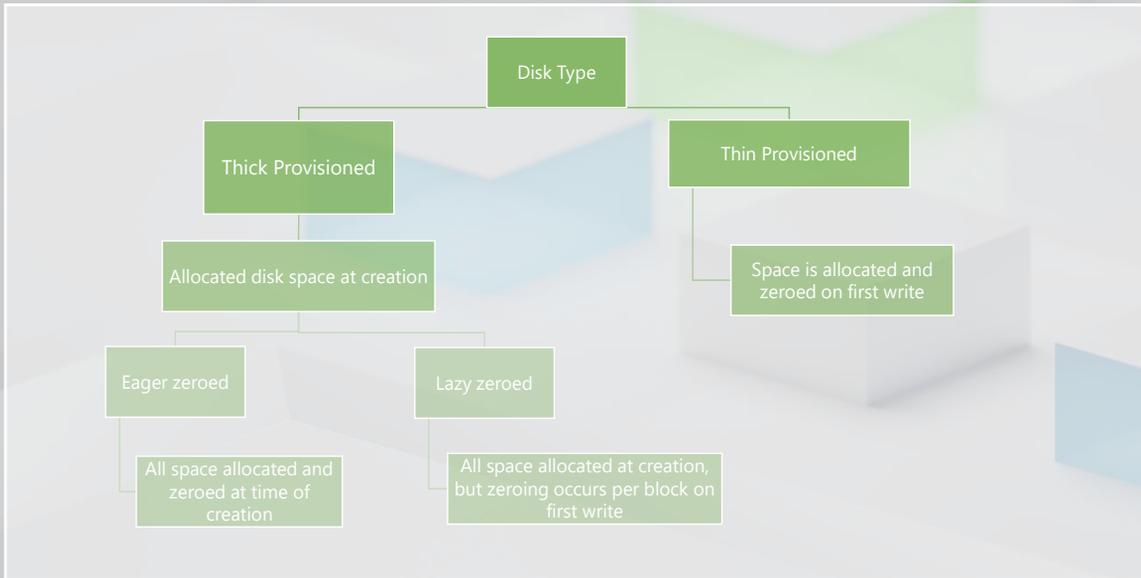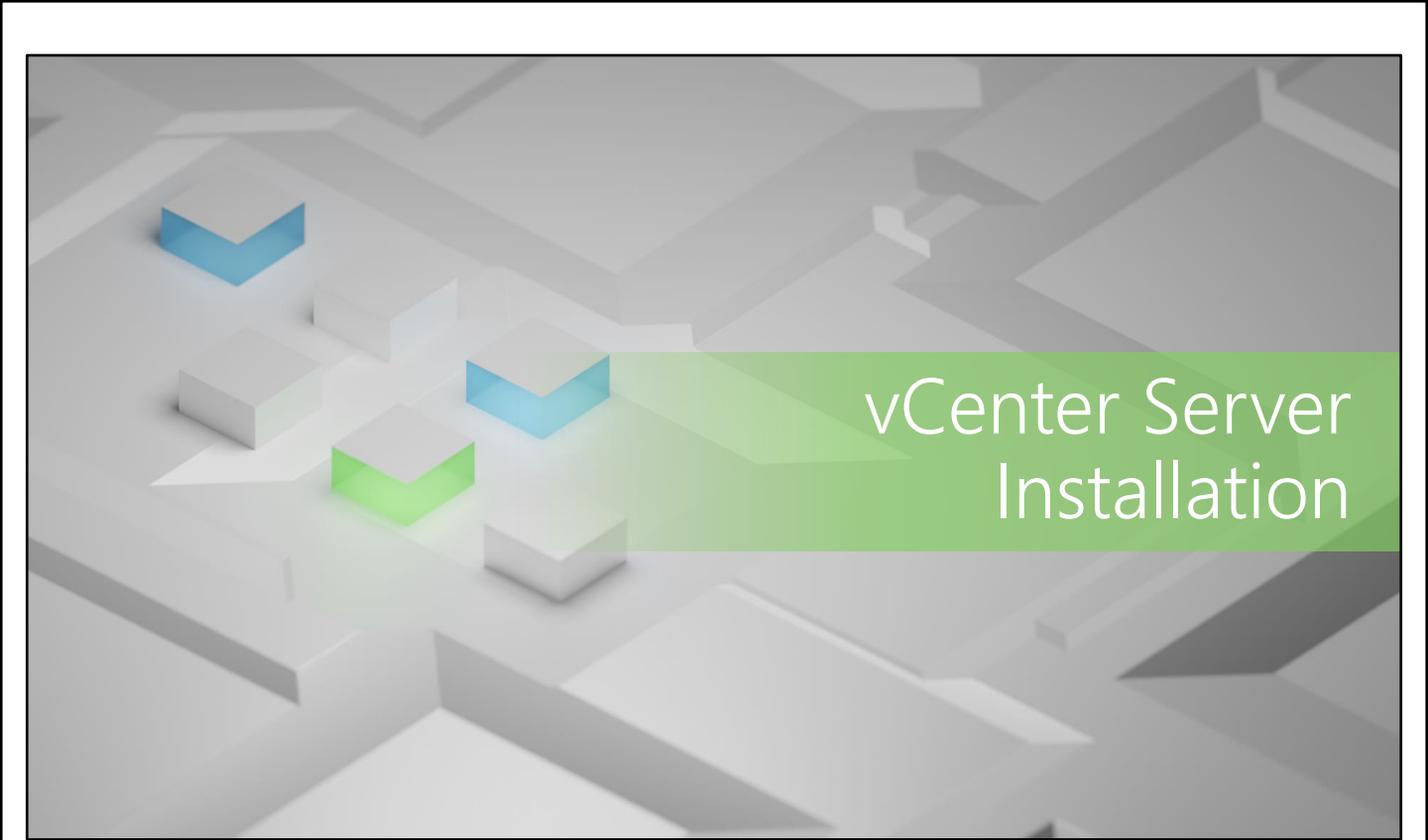
Central Platform for:

Deploying new vCenter Servers
Management
Operations
Provisioning resources
Testing performance
VMs
Hosts

vCenter Server Appliance

Functions:

Authentication

Certificate management

Tags

Licensing

vCenter Server Appliance

vCenter Server Appliance

Pre-Configured VM
- Runs vCenter Server

Includes:
- Photon OS
- Authentication services
  - Via vSphere
- PostgreSQL
- Lifecycle Manager
  - vSphere
  - vCenter
- Supports 64 vCPUs per VM in ESXi

vCenter Server

What's new?
- vCenter Server Appliance
- Only supported in an HTML5 client
- Lifecycle Manager
- No changes in maximums

	8.0
Hosts per Server	2500
Powered on Machines per Server	40000
Registered VMs per Server	45000
Hosts in linked vCenter Servers	15000
Registered VMs in linked vCenter Server	150000

Install vCenter Server

Installation Methods:

GUI deployment
Simpler
OVA Deployment
Appliance Setup

CLI
Silent deployment

Install vCenter Server

GUI installation

https://my.vmware.com/web/vmware/downloads

Mount ISO on host
Run the installer
Example:
    Windows → win32 subdirectory → vcsa-ui-installer
    Run Installer.exe → Mount on desired Device
    Go through Installer Wizard

Install vCenter Server

Installer Wizard

Install vCenter Server

Recommendations for performance

Intro

EULA

Deployment Target

Set up vCenter Server VM

Select Deployment size

Select Datastore

Configure Network Settings

Ready to Complete Stage 1

Install vCenter Server

Intro

EULA

Deployment Target

Set up vCenter Server VM

Select Deployment size

Select Datastore

Configure Network Settings

Ready to Complete Stage 1

1 Introduction

2 End user license agreement

3 vCenter Server deployment target

4 Set up vCenter Server VM

5 Select deployment size

6 Select datastore

7 Configure network settings

8 Ready to complete stage 1

End user license agreement

Read and accept the following license agreement.

VMWARE GENERAL TERMS

Last updated:16 June 2022

By downloading or using an Offering, Customer agrees to be bound by the terms of the Agreement.

1. OFFERINGS.

1.1. **Applicable Terms.** The terms of the Order and these General Terms, including applicable Exhibits and Offering-specific Notes (collectively, the "**Agreement**") govern

☑ I accept the terms of the license agreement.

CANCEL   BACK   NEXT

Install vCenter Server

Intro

EULA

Deployment Target

- IP address of target host
- Port (ex: 443)
- User name
- Password

Set up vCenter Server VM

Select Deployment size

Select Datastore

Configure Network Settings

Ready to Complete Stage 1

Install - Stage 1: Deploy vCenter Server

1 Introduction
2 End user license agreement
3 vCenter Server deployment target
4 Set up vCenter Server VM
5 Select deployment size
6 Select datastore
7 Configure network settings
8 Ready to complete stage 1

vCenter Server deployment target

Specify the vCenter Server deployment target settings. The target is the ESXi host or vCenter Server instance on which the vCenter Server will be deployed.

ESXi host or vCenter Server name: Enter FQDN or IP Address

HTTPS port: 443

User name: root or UserName@DomainName

Password:

Certificate Warning

If an untrusted SSL certificate is installed on 10.23.33.139, secure communication cannot be guaranteed. Depending on your security policy, this issue might not represent a security concern.

The SHA1 thumbprint of the certificate is:

61:33:E9:A4:F0:21:CD:93:42:ED:9F:57:07:F2:D3:FD:69:E9:25:0B

To accept and continue, click Yes

NO   YES

Install vCenter Server

Intro

EULA

Deployment Target

Set up vCenter Server VM

> VM Name
> Root Password (Admin)
> Confirm Root Password

Select Deployment size

Select Datastore

Configure Network Settings

Ready to Complete Stage 1

---

vmw Install - Stage 1: Deploy vCenter Server

1 Introduction

2 End user license agreement

3 vCenter Server deployment target

4 Set up vCenter Server VM

5 Select deployment size

6 Select datastore

7 Configure network settings

8 Ready to complete stage 1

Set up vCenter Server VM

Specify the VM settings for the vCenter Server to be deployed.

VM name	10.23.33.139
Set root password	•••••••••••
Confirm root password	•••••••••••

CANCEL   BACK   NEXT

Install vCenter Server

Intro

EULA

Deployment Target

Set up vCenter Server VM

Select Deployment size

Pick from a drop down

Refer to resource list

Select Datastore

Configure Network Settings

Ready to Complete Stage 1

---

vmw Install - Stage 1: Deploy vCenter Server

1 Introduction

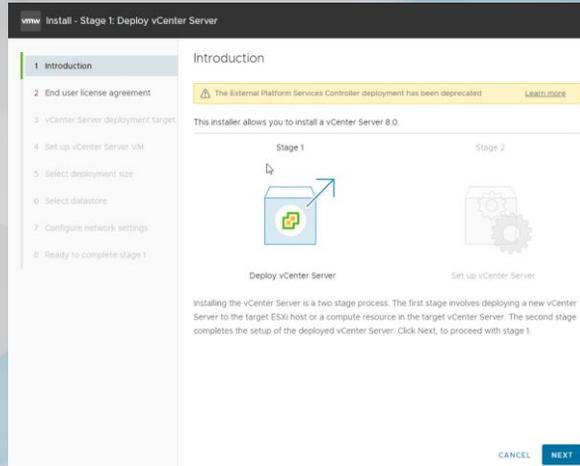2 End user license agreement

3 vCenter Server deployment target

4 Set up vCenter Server VM

5 Select deployment size

6 Select datastore

7 Configure network settings

8 Ready to complete stage 1

Select deployment size

Select the deployment size for this vCenter Server.

For more information on deployment sizes, refer to the vSphere 8.0 documentation.

Deployment size   Tiny

Storage size   Default   ⓘ

Resources required for different deployment sizes

Deployment Size	vCPUs	Memory (GB)	Storage (GB)	Hosts (up to)	VMs (up to)
Tiny	2	14	579	10	100
Small	4	21	694	100	1000
Medium	8	30	908	400	4000
Large	16	39	1358	1000	10000
X-Large	24	58	2283	2000	35000

CANCEL   BACK   NEXT

Install vCenter Server

Intro

EULA

Deployment Target

Set up vCenter Server VM

Select Deployment size

Select Datastore

Existing datastore
or
New vSAN Cluster

Configure Network Settings

Ready to Complete Stage 1

---

vmw Install - Stage 1: Deploy vCenter Server

1 Introduction

2 End user license agreement

3 vCenter Server deployment target

4 Set up vCenter Server VM

5 Select deployment size

6 Select datastore

7 Configure network settings

8 Ready to complete stage 1

Select datastore

Select the storage location for this vCenter Server

○ Install on an existing datastore accessible from the target host

☑ Show only compatible datastores

Name	Type	Capacity	Free	Provisioned	Thin Provisioning
datastore1	VMFS-6	3.51 TB	3.37 TB	148.16 GB	Supported

1 item

☐ Enable Thin Disk Mode ⓘ

○ Install on a new vSAN cluster containing the target host ⓘ

CANCEL   BACK   NEXT

Install vCenter Server

Intro

EULA

Deployment Target

Set up vCenter Server VM

Select Deployment size

Select Datastore

Configure Network Settings

    Which Network
    IP address / Subnet Mask
    DNS Servers (DNS resolve)
    Default Gateway
    Ports

Ready to Complete Stage 1

---

vmw Install - Stage 1: Deploy vCenter Server

1 Introduction
2 End user license agreement
3 vCenter Server deployment target
4 Set up vCenter Server VM
5 Select deployment size
6 Select datastore
7 Configure network settings
8 Ready to complete stage 1

Configure network settings

Configure network settings for this vCenter Server

Network	VM Network
IP version	IPv4
IP assignment	static
FQDN	FQDN (optional)
IP address	
Subnet mask or prefix length	
Default gateway	
DNS servers	Comma separated IP address
Common Ports	
HTTP	80
HTTPS	443

CANCEL BACK NEXT

Install vCenter Server

Intro

EULA

Deployment Target

Set up vCenter Server VM

Select Deployment size

Select Datastore

Configure Network Settings

Ready to Complete Stage 1

Review deployment details
Finish

---

vmw Install - Stage 1: Deploy vCenter Server

1 Introduction

2 End user license agreement

3 vCenter Server deployment target

4 Set up vCenter Server VM

5 Select deployment size

6 Select datastore

7 Configure network settings

8 Ready to complete stage 1

Ready to complete stage 1

Review your settings before starting the vCenter Server deployment.

Deployment Details

Target ESXi host	10.23.33.139
VM name	10.23.33.139
Deployment size	Tiny
Storage size	Default

Datastore Details

Datastore , Disk mode	datastore1 , thick

Network Details

Network	VM Network
IP settings	IPv4 , DHCP
HTTP Port	80
HTTPS Port	443

CANCEL   BACK   FINISH

Install vCenter Server
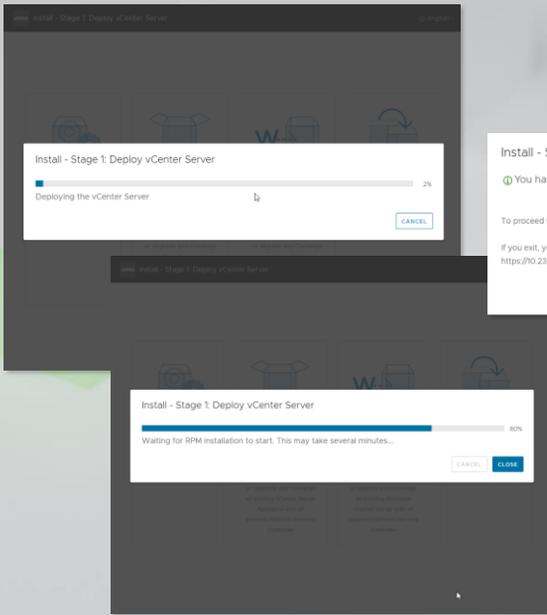
Install vCenter Server Step 2

Intro

vCenter Server Configuration

SSO Configuration

Configure CEIP
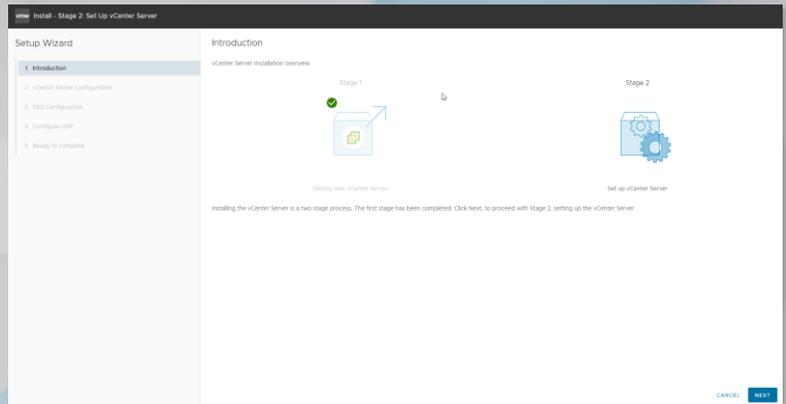
Ready to Complete

Install vCenter Server Step 2

Intro

vCenter Server Configuration

- Determine time sync mode
  - Default to sync with host
- Will you need SSH access?

SSO Configuration

Configure CEIP

Ready to Complete
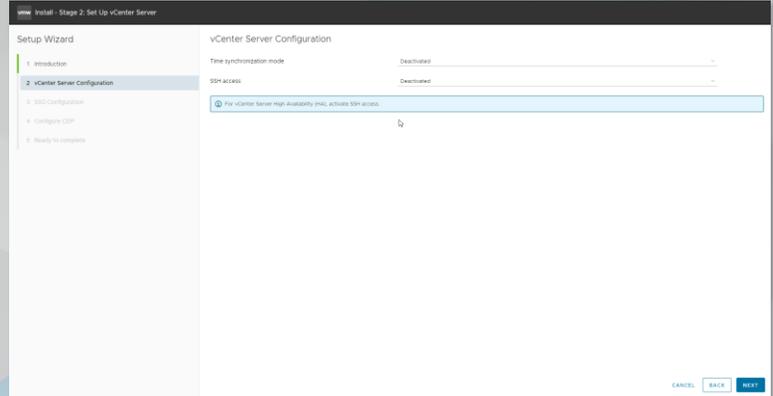
Install vCenter Server Step 2

Intro

vCenter Server Configuration

SSO Configuration

Connects vCenter Servers in a federation
Provide:
    Domain name
    Username
    Password
Or join vCenter Server with existing SSO domains

Configure CEIP

Ready to Complete
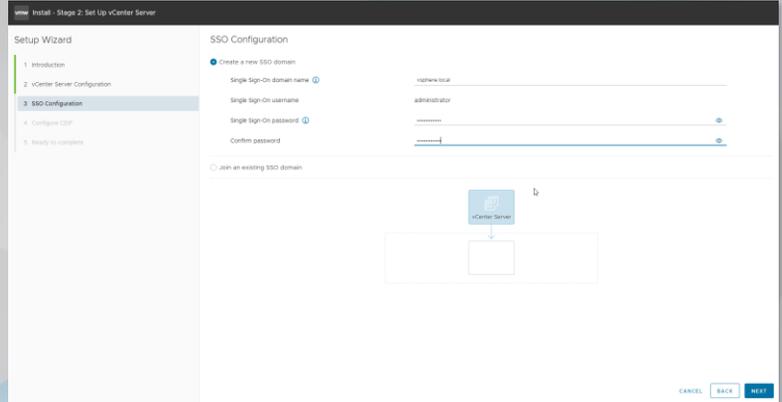
Install vCenter Server Step 2

Intro

vCenter Server Configuration

SSO Configuration

Configure CEIP

(Optional)

Ready to Complete

Install vCenter Server Step 2

Intro

vCenter Server Configuration

SSO Configuration

Configure CEIP

Ready to Complete

Review your setup

Finish

Install vCenter Server Step 2

Intro

vCenter Server Configuration

SSO Configuration

Configure CEIP

Ready to Complete

Review your setup

Finish

Install - Stage 2: Complete

✓ You have successfully setup this vCenter Server

████████████████████████ 100%

Complete

vCenter Server setup has been completed successfully. Click on the link below to get started.
Press close to exit.

Install - Stage 2: Complete

✓ You have successfully setup this vCenter Server.

vCenter Server setup has been completed successfully. Click on the link below to get started. Press close to exit.

vCenter Server Getting Started Page : https://10.23.33.40:443

CLOSE

CLI Installation

When GUI is not an option →

Prepare JSON

Configures similar parameters as GUI
Required before running install

CLI Installation

JSON template:

- **"vc"**
- **"appliance"**
- **"network"**
- **"os"**
- **"sso"**
- Configure parameters in each subsection
- Save in UTF-8 format

Look familiar?

- GUI and CLI configure similar parameters

```
"new_vcsa": {
    "vc": {
        "hostname": "vcsa1.stormlab.com",
        "username": "administrator@local.com",
        "password": "somePassword",
        "deployment_network": "StormwindHQ",
        "datacenter": [
            "OurDataCenter-1"
        ],
        "datastore": "newDATA-3",
        "target": [
            "stormCluster-1"
        ]
    },
    "appliance": {
        "thin_disk_mode": true,
        "deployment_option": "medium",
        "name": "vcsa22"
    },
    "network": {
        "ip_family": "ipv4",
        "mode": "static",
        "system_name": "vcsa22.stormlab.com",
        "ip": "192.168.1.1",
        "prefix": "24",
        "gateway": "192.168.1.254",
        "dns_servers": [
            "192.168.100.5"
        ]
    },
    "os": {
        "password": "osPassword",
        "ntp_servers": "synctime.ntp.org",
        "ssh_enable": true
    },
    "sso": {
        "password": "ssoPassword",
        "domain_name": "vsphere.local"
    }
}
```

CLI Installation

Navigate to:

Windows OS	Linux OS	Mac OS
Vcsa-cli-installer\win32	Vcsa-cli-installer/lin64	Vcsa-cli-installer/mac

Using Windows PowerShell:

```
vcsa-deploy install --accept-eula --acknowledge-ceip path_to_the_json_file
```

Need to check before you deploy?

```
vcsa-deploy install –precheck-only path_to_the_json_file
```

Need to deploy multiple vCenter Servers using various JSON files?

```
vcsa-deploy install --accept-eula --acknowledge-ceip
filepathto/mybatchofJSONs
```

Result:

Exit code : 0

Success!

vCenter Server Management Interface

Access the vCenter Server

In a web browser:

Enter https://ip_address or fqdn_of_vCenter_Server

Submit Credentials

Access the vSphere Client

Locate your Server

VMware® vSphere

example@domain.local

Password

Use Windows session authentication

LOGIN

Access the vCenter Server Management Interface

In a web browser:

Enter https://ip_address or fqdn_of_vCenter_Server:5480

Submit Credentials
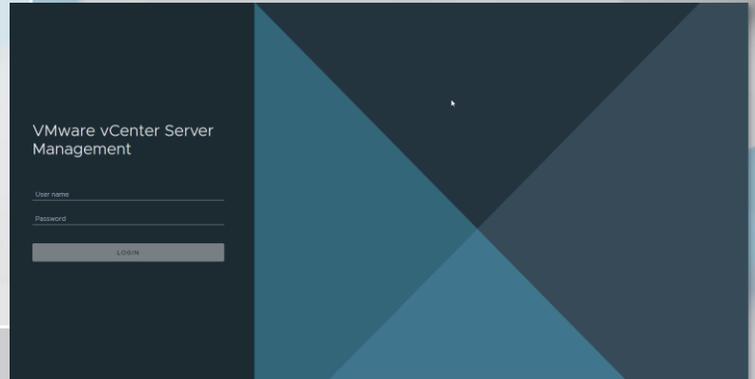
Access the vSphere Client

Locate your Server

VMware vCenter Server
Management

User name

Password

LOGIN

vCenter Server Management Interface

vCenter Server Management Appliance

Monitor usage of:

Memory
Processors
Disk use
Errors
Utilization
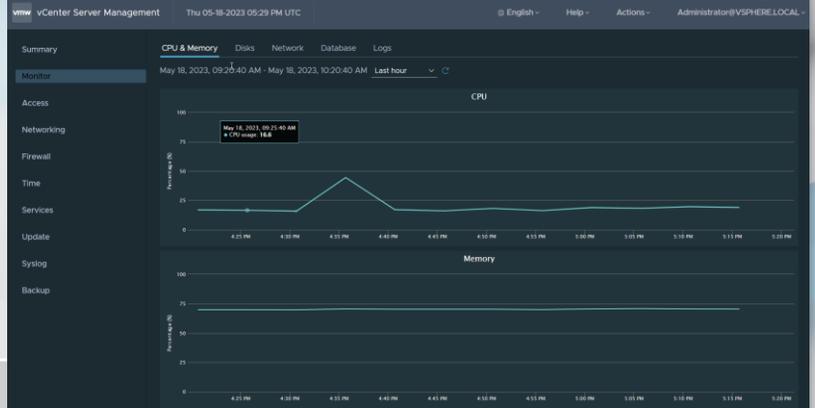
vCenter Server Management Interface

vCenter Server Management Appliance

Access

What is enabled?
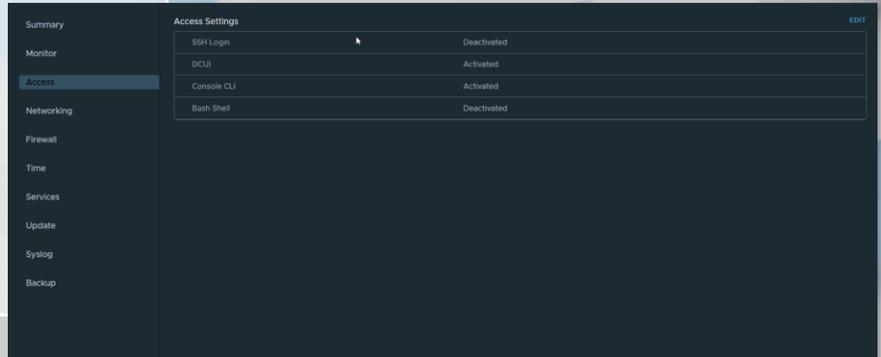
Summary	**Access Settings**	EDIT
Monitor	SSH Login	Deactivated
Access	DCUI	Activated
Networking	Console CLI	Activated
Firewall	Bash Shell	Deactivated
Time		
Services		
Update		
Syslog		
Backup		

vCenter Server Management Interface

vCenter Server Management Appliance

Networking

Edit / Verify
Network
Configurations

vCenter Server Management Interface

vCenter Server Management Appliance

Firewall

Create/ Edit / Delete Firewall Rules
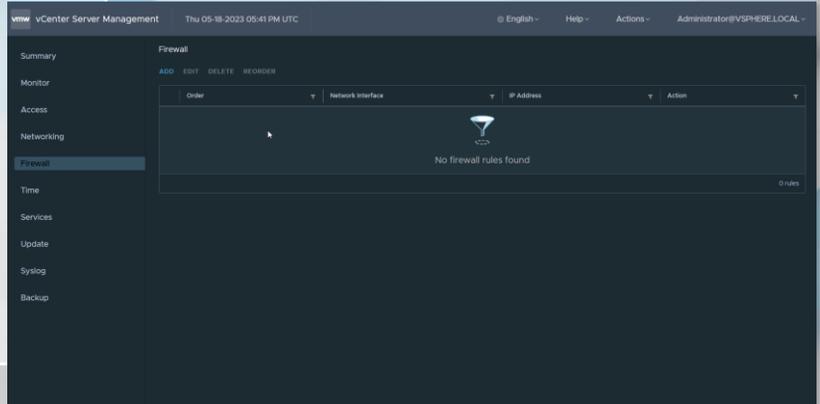
vCenter Server Management Interface

vCenter Server Management Appliance

Time

Edit / Verify the method of time synchronization
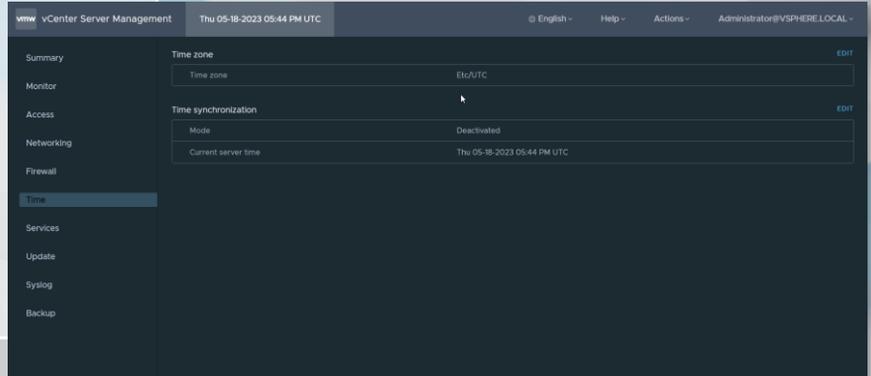
vCenter Server Management Interface

vCenter Server Management Appliance

Services

Start or Stop Services

Restart malfunctioning services

vCenter Server Management Interface

vCenter Server Management Appliance

Update

What version are you running?

Where can updates come from?
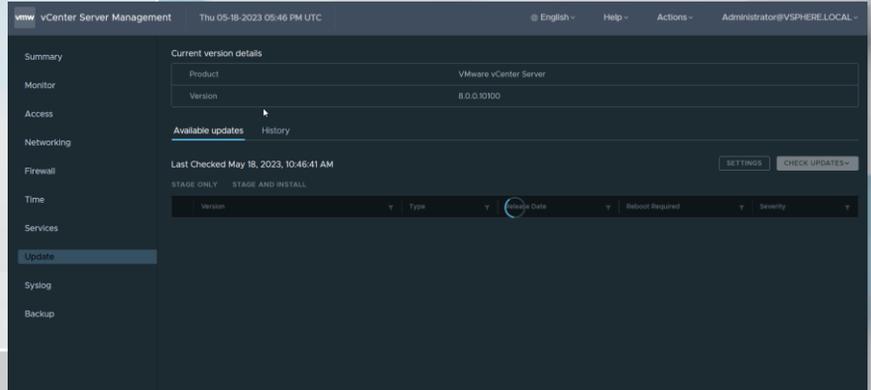
vCenter Server Management Interface

vCenter Server Management Appliance

Syslog

Forward syslog traffic

Remote Syslog Server
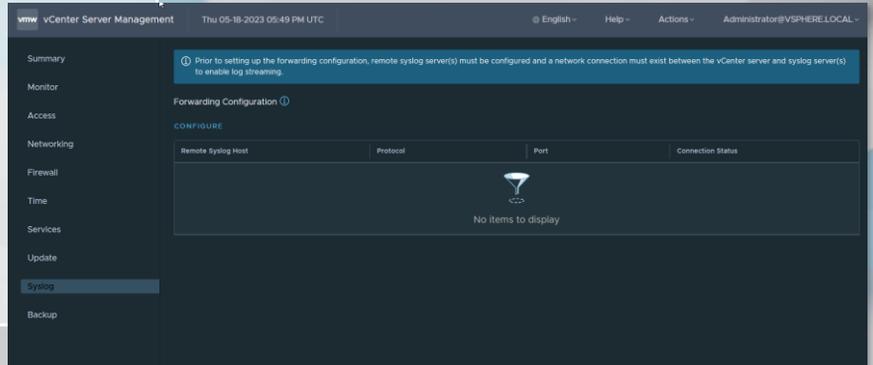
vCenter Server Management Interface

vCenter Server Management Appliance

Backup

- Save in a remote server
- Create a schedule for backups
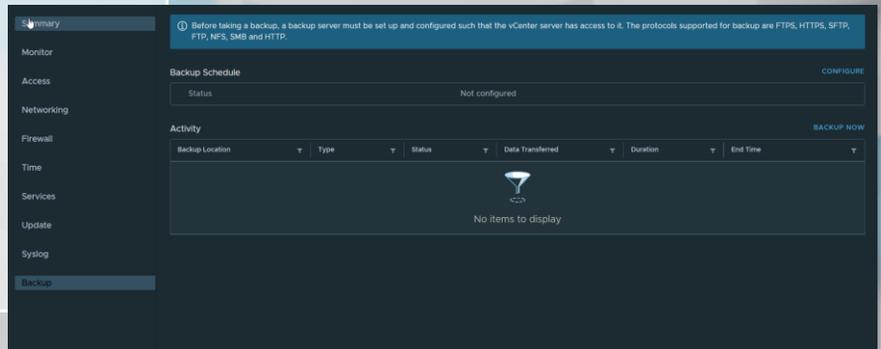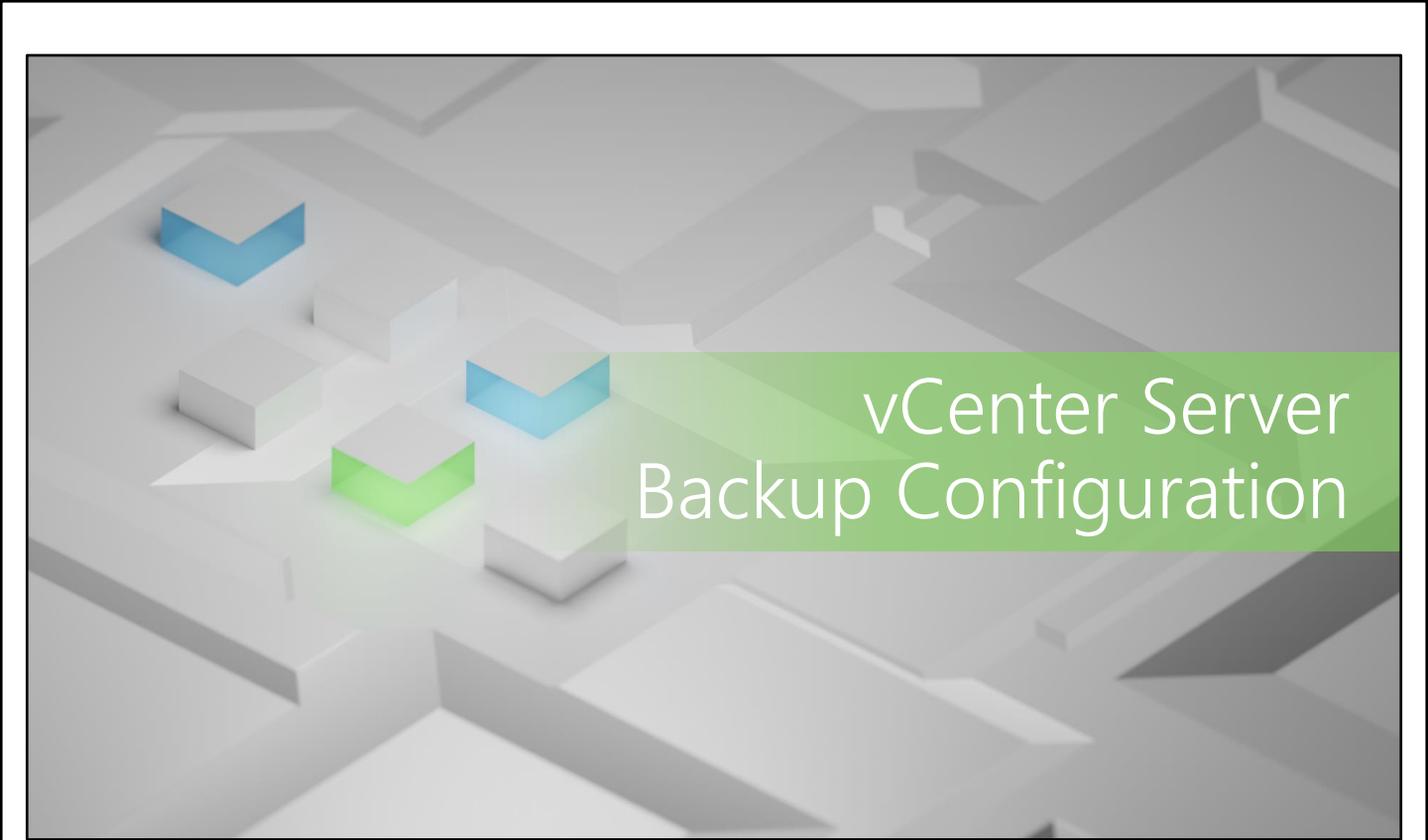
vCenter Server Backup Configuration

Creating a Backup

Backups

File based

Recover vCenter Server virtual environment

Scheduling

Pre-Reqs:

Must have remote storage point via:

HTTPS, HTTP, FTP, FTPS, SFTP, NFS, SMB

Not stored on the vCenter Server

Create Backup Schedule

Backup location *	protocol://server-address<:port-number>/folder/subfolder
Backup server credentials	User name
	Password
Schedule	Daily 11 : 59 P.M. Etc/UTC
Encrypt backup	Encryption Password
	Confirm Password
Number of backups to retain *	● Retain all backups
	○ Retain last 0 backups
Data	☑ Stats, Events, and Tasks
	☑ Inventory and configuration

Total size (compressed)   80 MB

CANCEL   CREATE

Creating a Backup

Creating a Backup
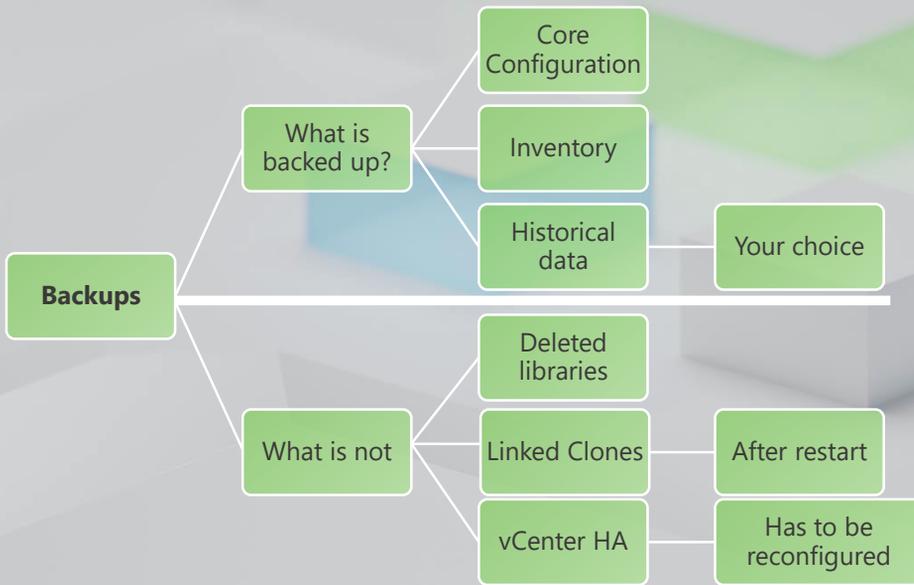
Known Issues

Cross vCenter migration of VM fails with an error

Crossing vCenter vMotion

Moving a VM's storage to different server instance

Linked SDDC vCenter Server instances appear in the on-Prem vSphere client

If a vCenter Cloud gateway is linked to the SDDC

Best Practices
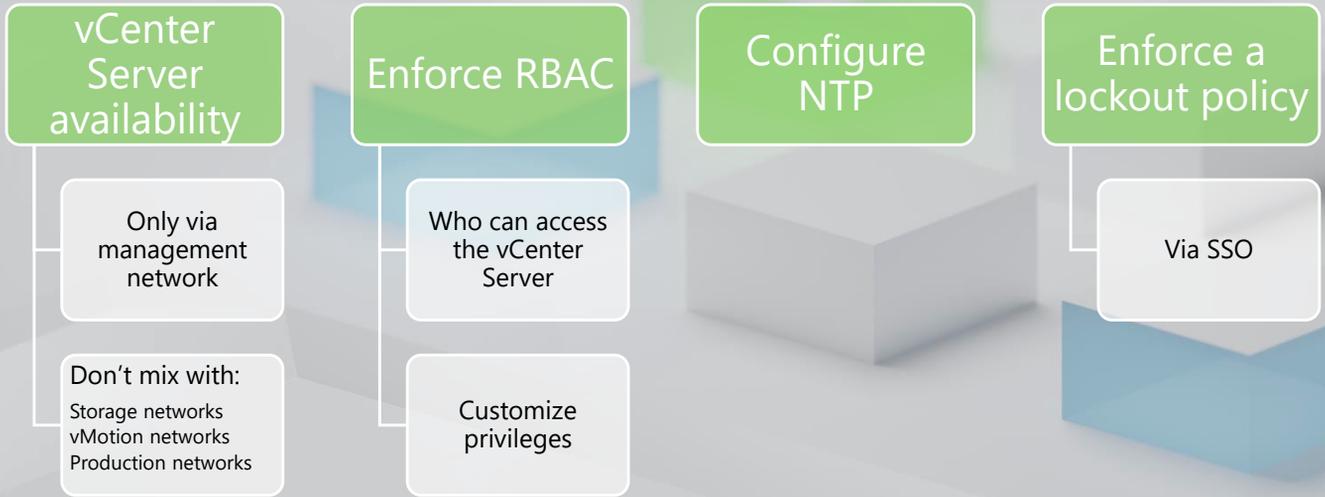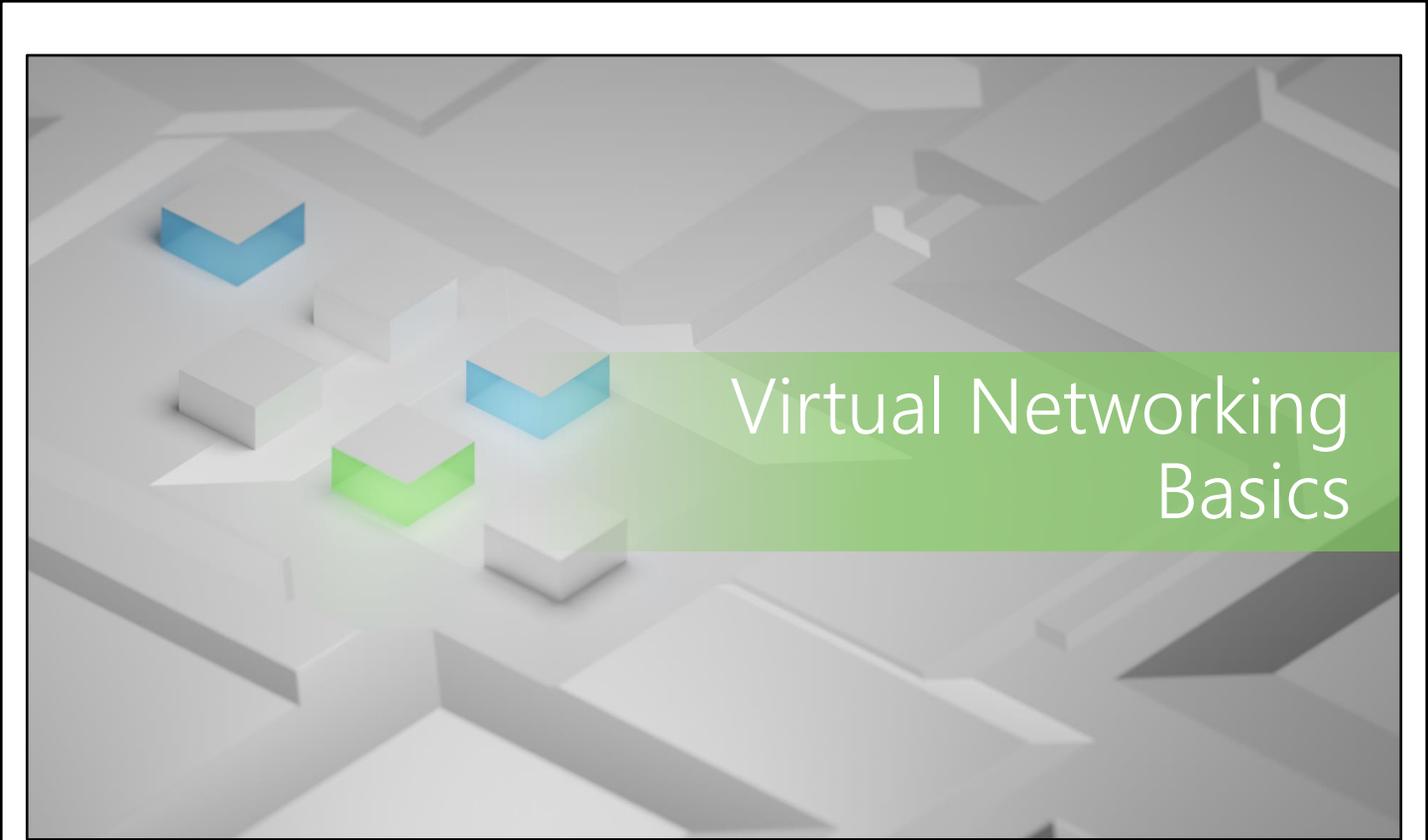
vCenter Server availability
- Only via management network
- Don't mix with:
  Storage networks
  vMotion networks
  Production networks

Enforce RBAC
- Who can access the vCenter Server
- Customize privileges

Configure NTP

Enforce a lockout policy
- Via SSO

Virtual Networking Basics

Key Terms

Virtual Adapters	Connects vSwitch to VM Unique MAC address Layer 2 devices

Virtual Switches	Standard
	    Forwards traffic to connected VMs
	Distributed
	    Centralized management switch
	    Configurations propagate to all attached hosts

Host NIC	Connects physical network to the vSwitch

Basic Architecture of a vSwitch (concept)
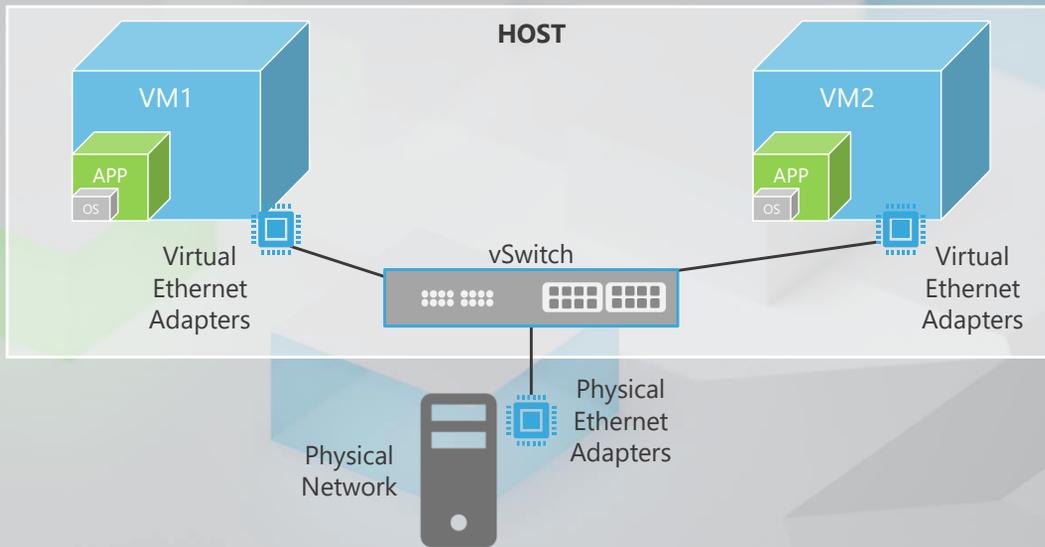
Basic Architecture of a vSwitch (concept)
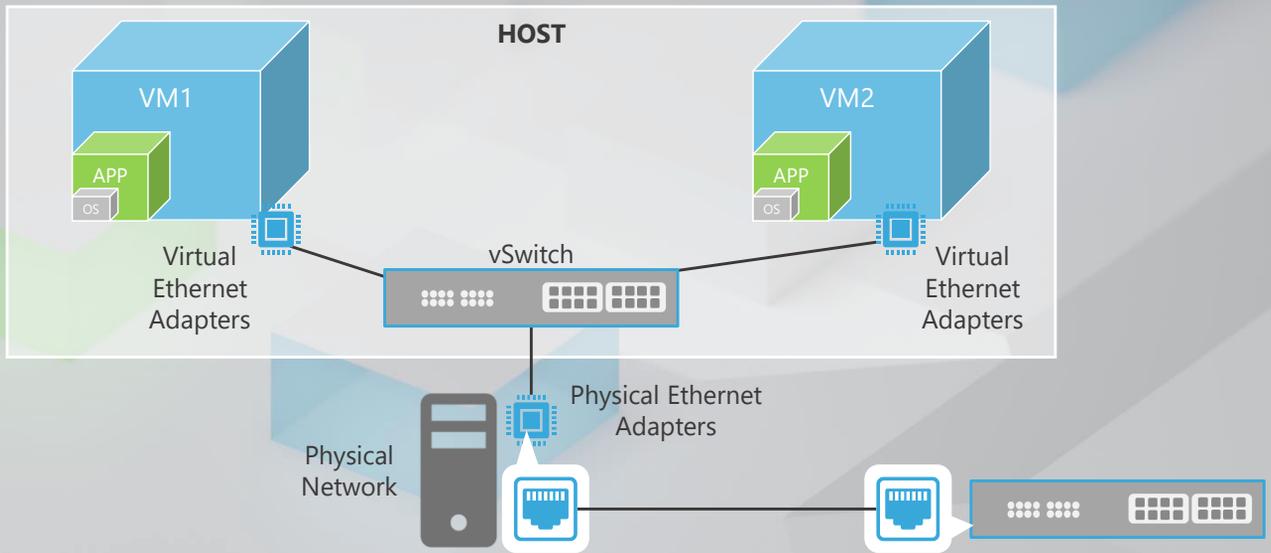
Port Groups

- **Used to connect to standard switches**

- **Sets connection method to the network**

- **Sets VLAN tags and bandwidth**
  - Virtual Local Area Network
  - VLAN allows for network segmenting

- **Switches are associated to port groups**
  - Types of Port Groups:
    - Standard
    - Distributed
    - NSX Distributed

HOST

VM1
VM2
APP
OS
APP
OS

Portgroup

vSwitch

Physical Ethernet Adapters
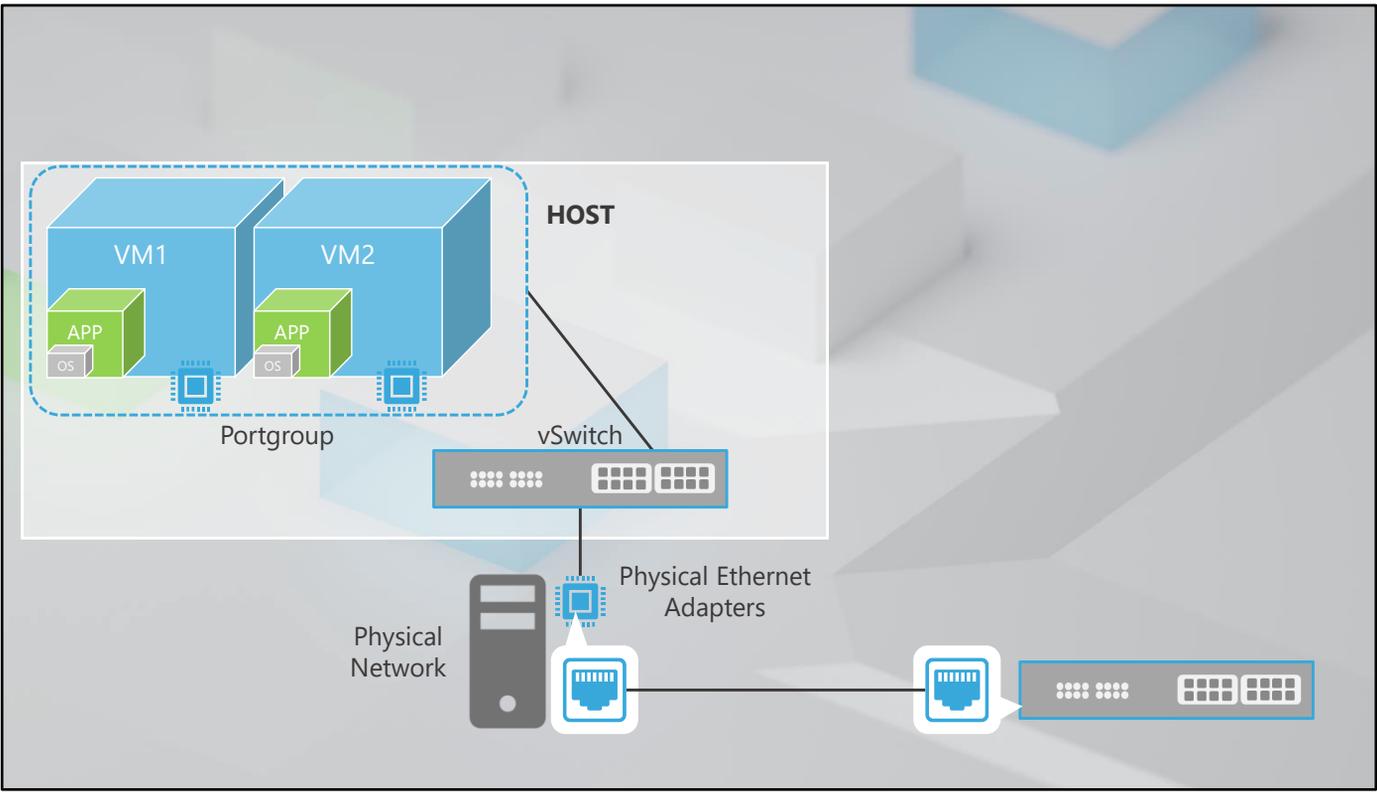
Physical Network

The Virtual Switch

◆ **Local to the host**

The vehicle from portgroups to NIC

Portgroup to physical adapter mappin

◆ **Identify load balancing**

Distributed vSwitch

◆ **vCenter controlled centralized switch**
    Pushed out to hosts

◆ **Very good for large environments**

Basic Architecture of a vSwitch (concept)

Portgroup 2

VM1 VM1

VM Kernel

Portgroup 1

VM1 VM1

vSwitch

VLAN 10
VLAN 20
VLAN 30

Policies can be applied
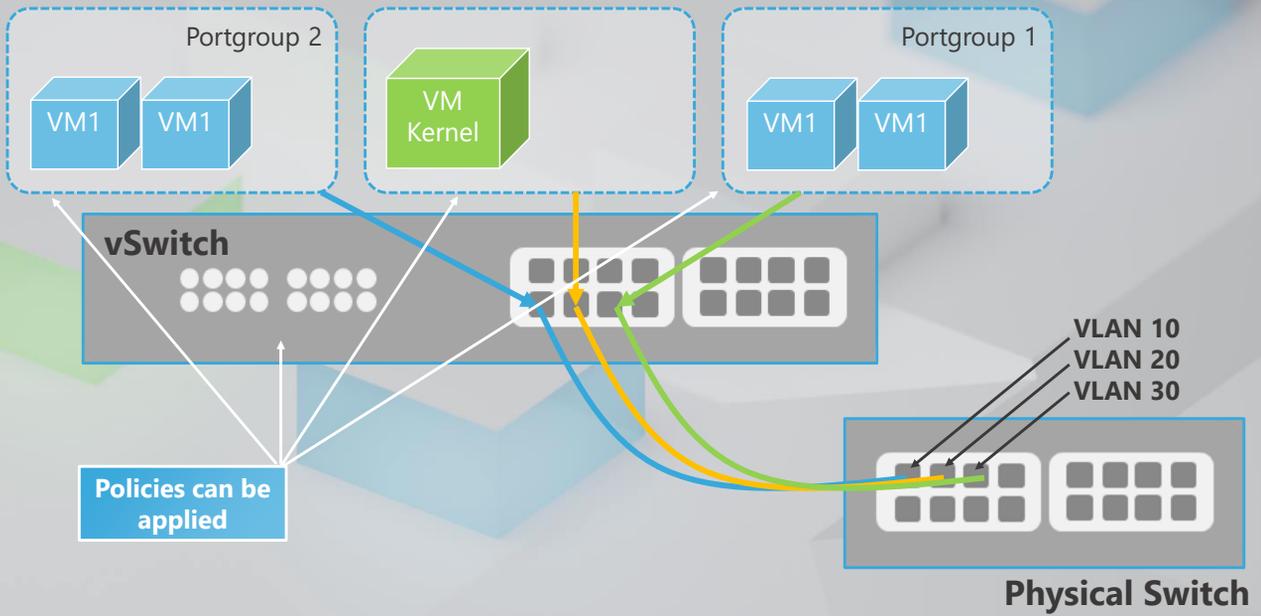
Physical Switch

Conclusions

Virtual Networking Basics

- Virtual adapters
- Virtual switches
  - Intro to distributed switches
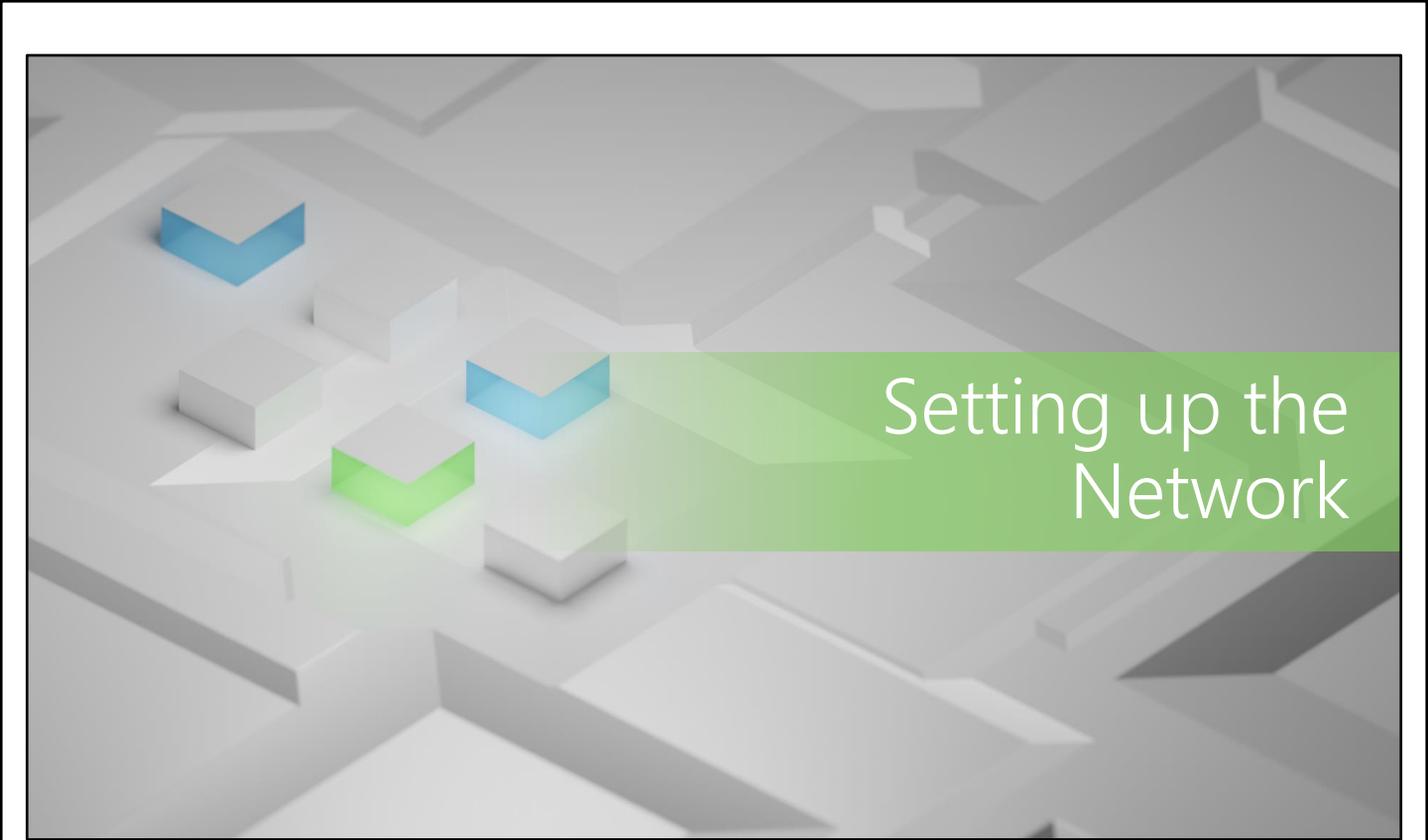
Setting up the Network

Enabling a Physical Adapter

Add Networking

1. Select connection type
2. Select target device
3. **Add physical network adapter**
4. Ready to complete

Add physical network adapter

Assign physical network adapters to the switch.

Select unclaimed (free) adapters on the host and move them to the Active/Standby/Unused adapters of the switch.

MOVE UP   MOVE DOWN

Unclaimed adapters

Active adapters

Standby adapters

Unused adapters

Select a physical network adapter from the list to view its details.

CANCEL   BACK   NEXT

Setting up the Network

Step 1

Create a Physical Adapter

- Select desired host

- Networking → Virtual Switches → Select vSwitch

- Manage Physical Adapters

- Add Adapters with +

- Needed to connect the vSwitch to the On-Premise Network

Creating a vSwitch

Add Networking

1	Select connection type
2	**Select target device**
3	Create a Standard Switch
4	Connection settings
5	Ready to complete

Select target device

Select a target device for the new connection.

○ Select an existing standard switch

● New standard switch

MTU (Bytes)   1500

CANCEL   BACK   NEXT

Setting up the Network

Creating a vSwitch

Select the desired host

Configure → Networking →
Virtual Switches

Add Networking

Creating a Portgroup or VMkernel Adapter

Add Networking

1 Select connection type

2 Select target device

3 Connection settings

4 Ready to complete

Connection settings

Use network labels to identify migration-compatible connections common to two or more hosts.

Network label   VM Network 3

VLAN ID   All (4095) ▾

CANCEL   BACK   **NEXT**

Adding a VM Port Group

◆ **After a switch is added**

◆ **Port groups provide connectivity for VMs to the Switch**

◆ **Add a VM Port Group**

Add Networking

VM Port Group for a Standard Switch

Next

Select a switch

Set a Name and VLAN ID

Review and Finish

Creating a VMkernel Network Adapter

Add Networking

1 Select connection type

2 Select target device

3 **Port properties**

4 IPv4 settings

5 Ready to complete

Port properties
Specify VMkernel port settings.

Network label	VMkernel 2
VLAN ID	None (0)
IP settings	IPv4
MTU	Get MTU from switch 1500
TCP/IP stack	Default

Available services

Enabled services

- ☐ vMotion
- ☐ Provisioning
- ☐ Fault Tolerance logging
- ☐ Management

- ☐ vSphere Replication
- ☐ vSphere Replication NFC
- ☐ vSAN
- ☐ vSphere Backup NFC

- ☐ NVMe over TCP
- ☐ NVMe over RDMA

CANCEL BACK **NEXT**

Adding a VMkernel Network Adapter

◆ **After a switch is added**

◆ **VMKernel Adapters connectivity for vSphere services and features**

◆ **Add a VMkernel Adapter**

Add Networking

VMkernel Network Adapter

Next

Select a switch/ network

Select VLAN/Ipsettings/MTUs/TCP/IP

Services

Next

Review and Finish

Distributed Switch

Created on a Data Center

Administers Network Configuration

Distributed Switch

Created on a Data Center

In the vSphere Client

Built in vCenter Server and connects to hosts

Administers Network Configuration

Manages multiple hosts

Sets their configuration

Centralized management point

Distributed Switch Architecture
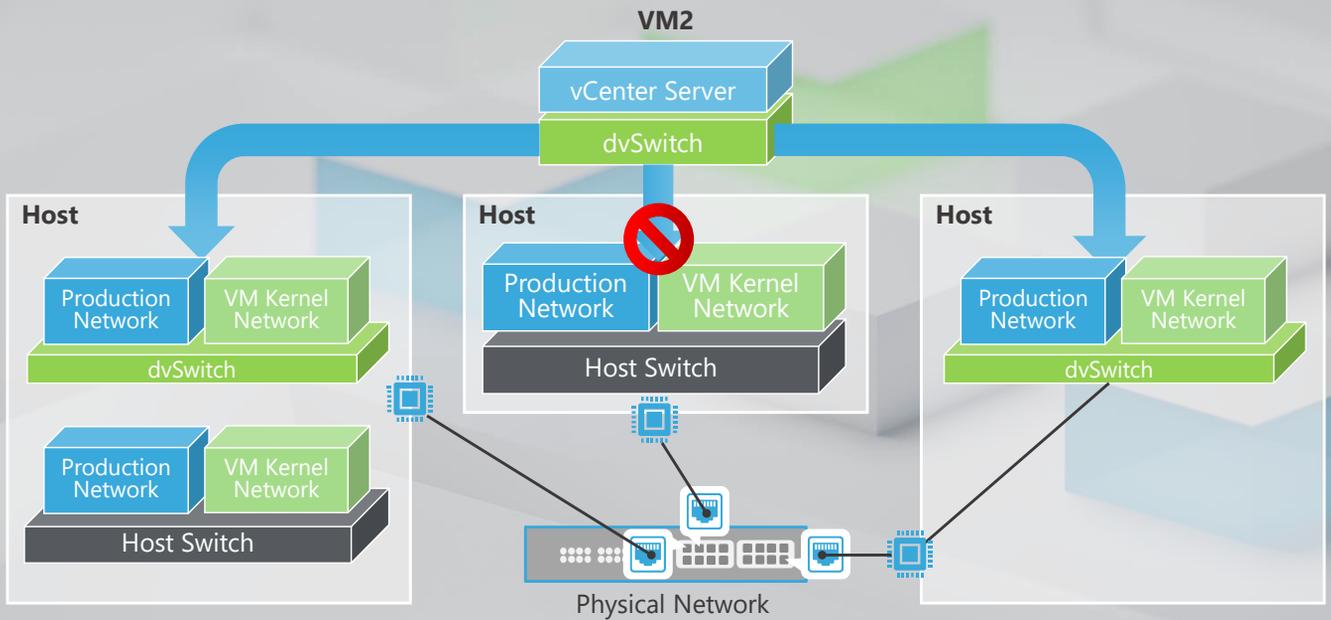
Create a dvSwitch

Add a dvSwitch

Select a datacenter
Distributed Switch →
New Distributed Switch

Configure the dvSwitch

Name the Switch
Set location for dvSwitch

Create a dvSwitch

Versioning

Different versions:
- Compatible to different versions of ESXi
- Have different capabilities

Configure settings

How many ports do you need to connect to hosts?

Enable I/O control if you need to:
- Prioritize traffic
- Based on infrastructure type and deployment needs

Create Default Port Group
- Requires port group name

Add a Distributed Port Group

Locate dvSwitch

Add a distributed port group

Name of the group

Select a dvSwitch

Configure Settings

Set binding

Static binding
> Port to virtual machine assignment on VM connection

Ephemeral
> No binding

Allocate Ports

Elastic
> Maxed port assignments leads to a new set of ports is created

> New group of ports is the same as number of ports originally assigned

Fixed
> Original port count is max that can be assigned

Configure Settings

How many ports do you need

Network Resource Pool

Assigns pool to user-defined network resource pool

VLAN type

None
  Used with external Switch Tagging
VLAN
  Segments the network into broadcast domains (1-4096)
VLAN Trunking
  Set ranges of VLANs to send to the guest OS
Private VLAN

Security for Portgroups

Promiscuous mode

MAC address changes

Forged transmits

Security for Portgroups

Promiscuous mode

Accept - Allows adapters in promiscuous mode to receive frames passed via VM's in a VLAN

Reject – Adapters in promiscuous mode will have their frames rejected by other VMs

MAC address changes

Accept - Guest OS MAC address changes does not affect frame forwarding

Reject – Adapters with guest OS altered MAC addresses will have their frames dropped at the switch

- Lasts until original MAC address is configured

Forged transmits

Accept – All outbound frames are allowed by the switch

Reject – Outbound frames with an altered MAC address are dropped by the vSwitch

Traffic Shaping

Why use traffic shaping?

Protect network from unusual traffic volume.

Control traffic volume for inbound and outbound bandwidth:

Average → Over time

Peak → Max

Burst → Burst Bonus

Note: Each port receives traffic shaping policy individually!

Teaming & Failover

How will the Distributed Port Group handle the following:

Balancing traffic?

Failed adapters?

Recovering from a failure?

Answer = Teaming and Failover

Load Balancing – What is the basis for uplink choice?

Originating Virtual Port

IP hash

Source MAC hash

Physical NIC load

Explicit failover

Failure detection

Link Status
> Adapters link status informs failover

Beacon probing
> NICs are probed to detect if they have failed

(Don't use with IP-hash)

Teaming & Failover

Notify Switches

Yes - Updates lookup tables in the event of a failover

No – No notification

Failback

Yes - Working adapters replace the standby

No – Working adapters can only replace a failed active adapter

Failover order

Set the order for uplinks
Set type of link
Active
    Used as long as it is functioning
Standby
    Used if active links are down
    Not used with IP-hash
Unused

NetFlow & Blocked Ports

NetFlow

Analyze L3 traffic on a dvSwitch

Analysis is sent to the NetFlow Collector

Configured outside of this GUI Console

Here you will either enable or disable the NetFlow you have configured separately!

Block ports

All

None

Verify

◆ **Recent Tasks Bar**

◆ **Check Ports on the Switch**

Conclusions
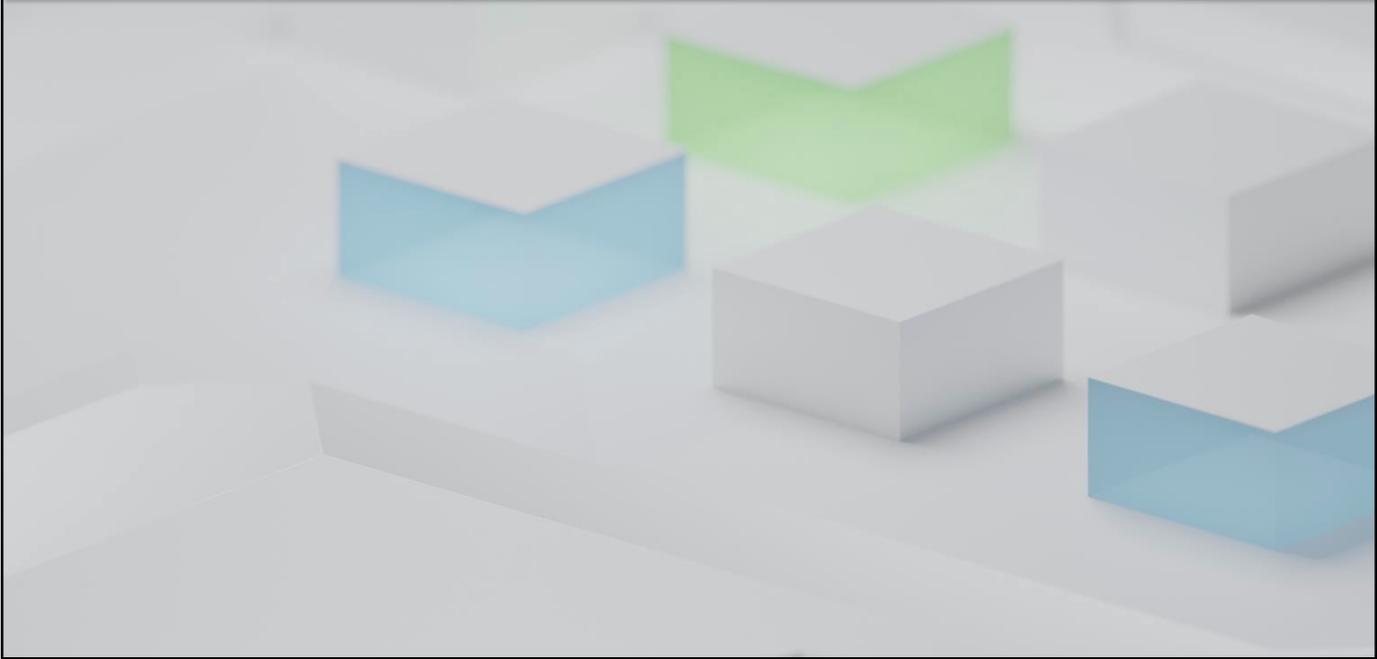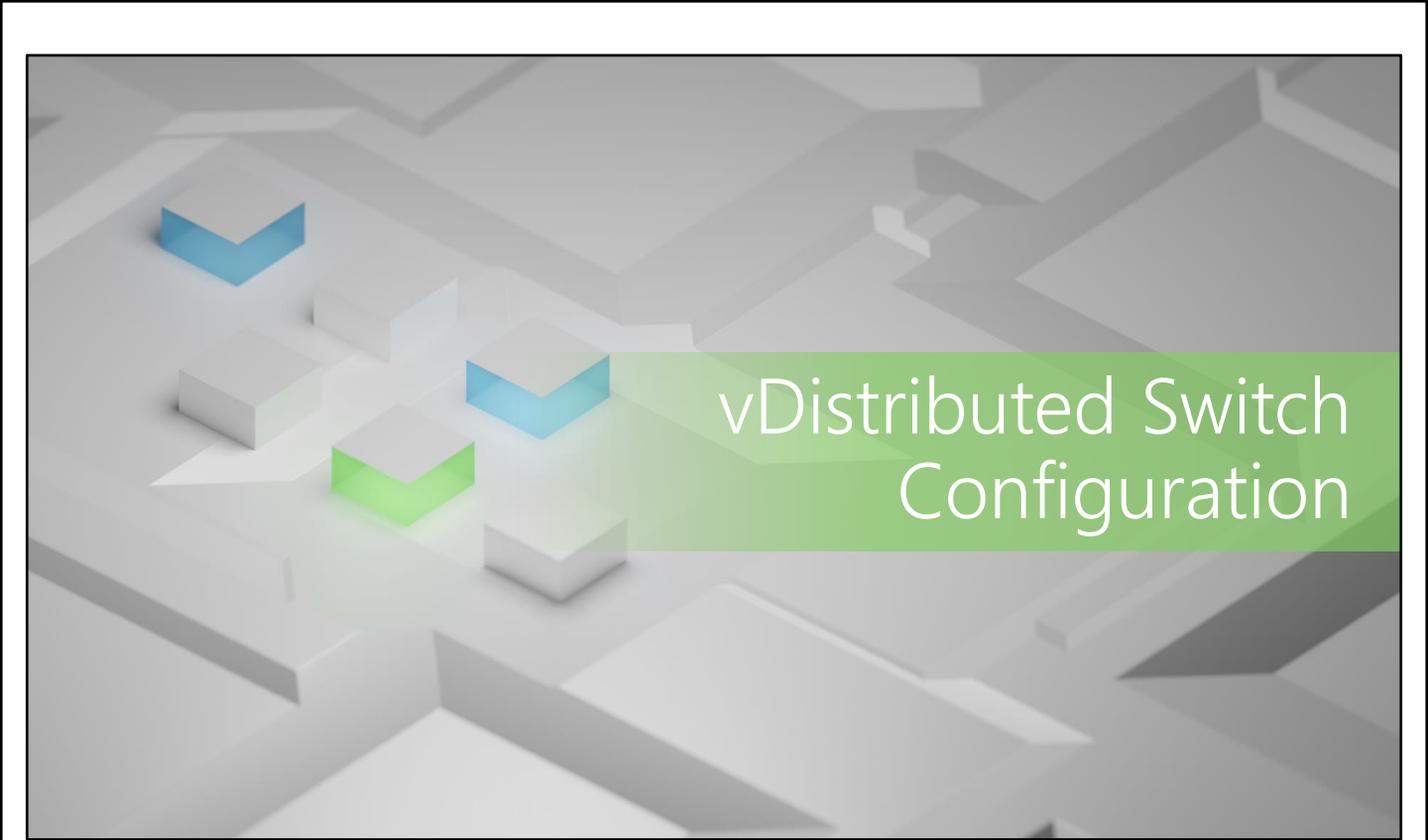
vDistributed Switch Configuration

Adding a Host

Select a NIC

Assign a VMNIC to a host

(Be aware what VMNICs are in use for what!)

Uplinks

Select an uplink number

Assign to the Adapter

Manage Adapters

Assign VMKernel Adapter a Port Group

If not network connectivity can be lost

Or you'll have to migrate them to the dvSwitch

Migrate VMs to dvSwitch

Select VM's that will be assigned to a port group
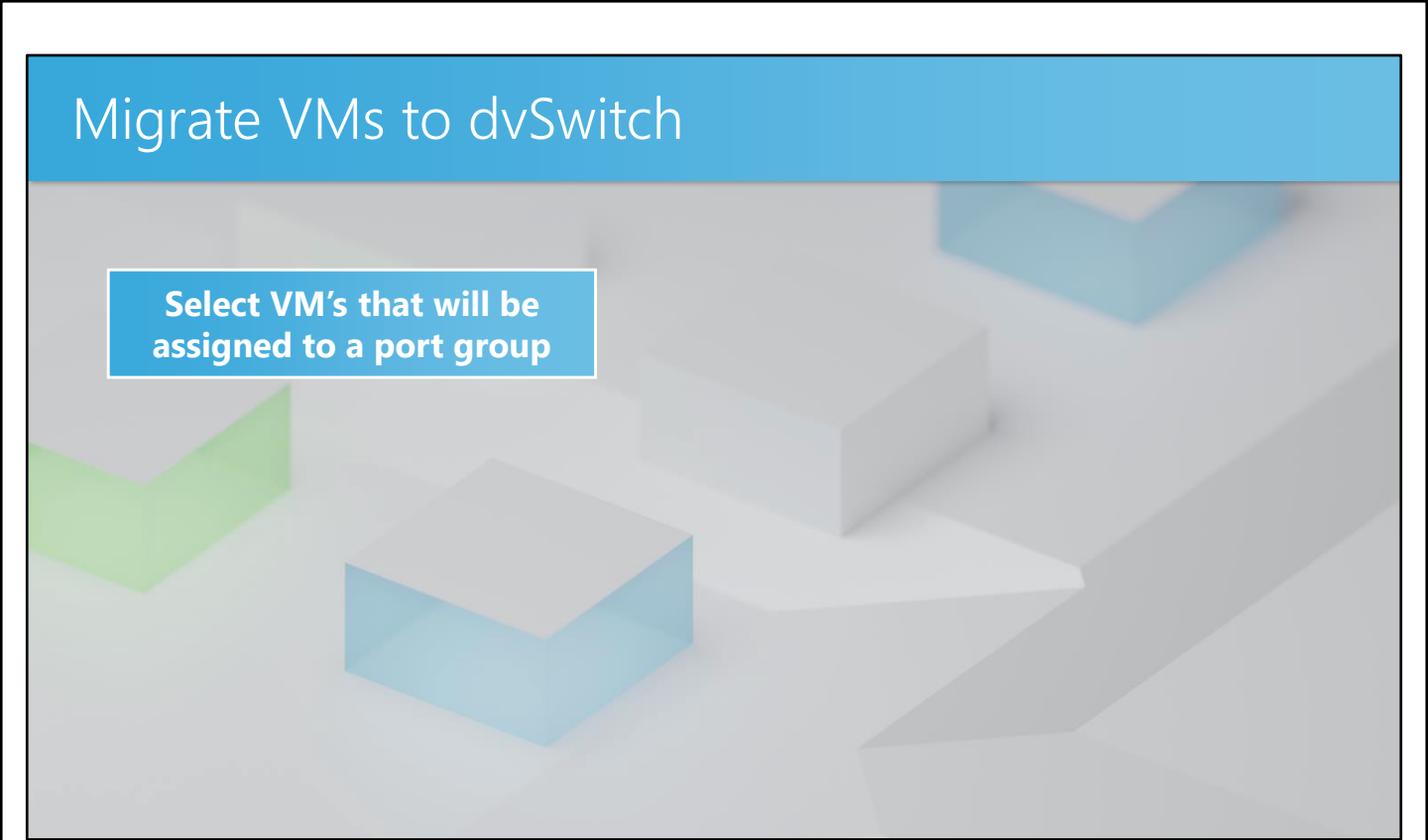
Conclusions
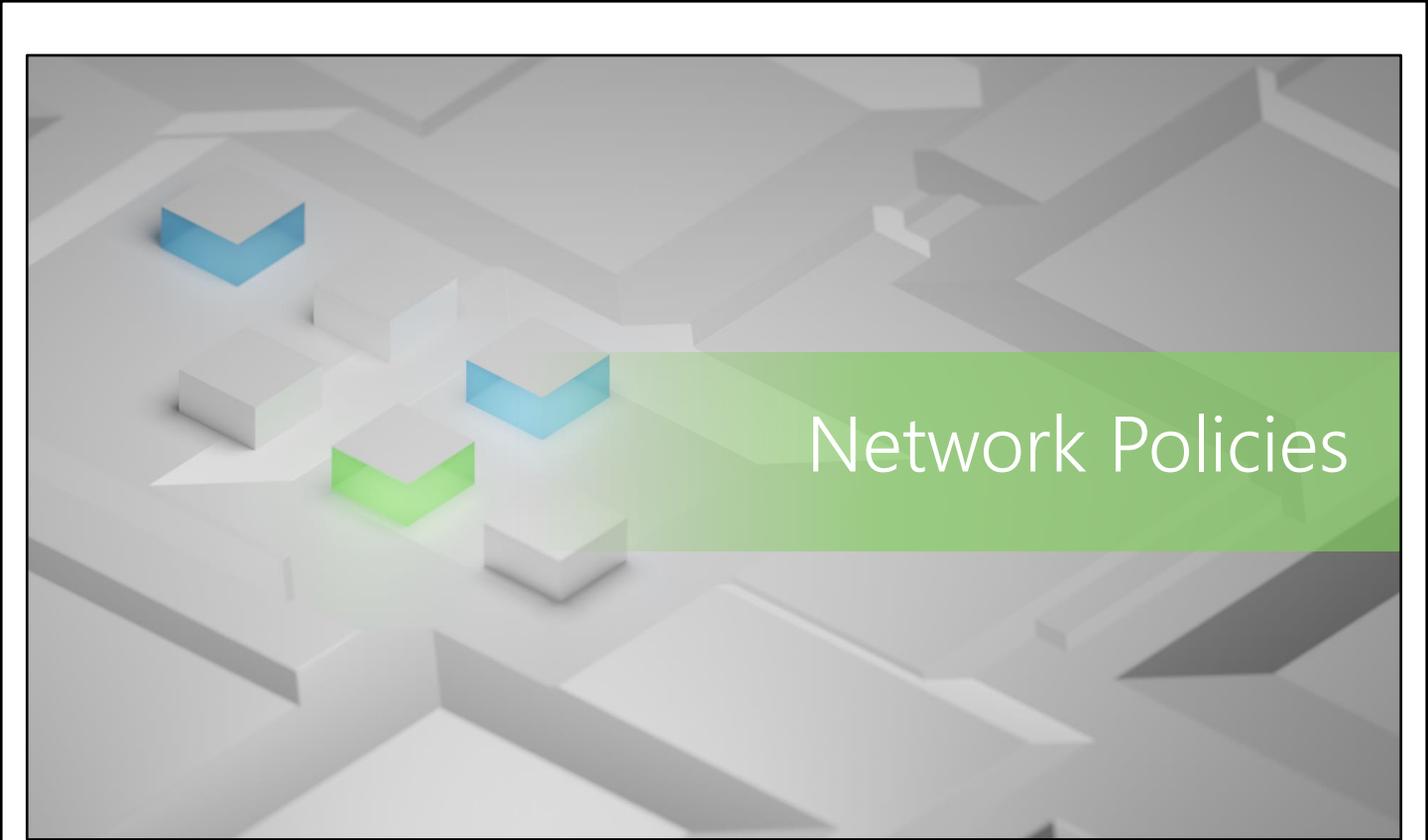
Network Policies

Network Policies

Set policies on Switches

Standard
- Policies applied to:
  - Entire switch
  - Individual port groups

Distributed
- Policies applied to:
  - Port
  - Port Group
  - Uplink Group
  - Uplink Port

Available Policies are different between devices

Network Policies

Network devices can't read your mind

Set network policies to architect your virtual network

Define:

- Connectivity
- VLAN tagging
- Security
- Etc.

Network Policies

Policy Name	Policy Definition	Standard vSwitch Availability	Distributed vSwitch Availability
Teaming and Failover	Arrange NIC failover order. Set Load Balancing policy.	YES	YES
Security	Prevents MAC spoofing & unwarranted port scans.	YES	YES
Traffic Shaping	Shape network bandwidth between links.	YES – Outbound	YES – Inbound & Outbound
VLAN	Configure VLAN tags	YES	YES
Monitoring	NetFlow monitoring on port or port group.	NO	YES
Filtering and Marking	Prevents unwanted traffic. Applies QoS tag to traffic types.	NO	YES
Resource Allocation	Controls bandwidth available to a port or port group.	NO	YES
Port Blocking	Block ports from transmitting or receiving data.	NO	YES

VLAN Policy

VLANs

VLANs treat hosts in the VLAN as part of the same broadcast domain

Not dependent on what network devices they are physically connected to

Network traffic from members of a VLAN is "tagged" with a VLAN ID

- Informs switches on how to handle traffic

VLAN policies define how this will be implemented

VLAN Policy

Applied to a distributed port group or port

- Need to apply VLAN tagging globally?
  - Requires a VLAN policy
- Groups ports into Broadcast Domain

Applied to an Uplink Port Group or Uplink Port

- Apply VLAN tagging policy to all members of uplinks
- Propagate trunk range of VLAN IDs to the physical network adapters

VLAN Policy Distributed Port Group

Implement Policy

Menu → Networking

Select Distributed Port Group → Manage Distributed Port Groups

    VLAN → NEXT

Select Port Groups → Next

    VLAN Type

VLAN Policy Distributed Port Group

VLAN Type

None	VLAN	VLAN Trunking	Private VLAN
No VLAN use	Traffic will be tagged with a VLAN ID Tag can be 1-4094	VLAN Trunking allows traffic on a VLAN to be passed by the vSwitch Traffic can be passed if it's VLAN ID is in a VLAN Trunk Range (Ranges can be separated with commas)	Traffic belongs to a Private VLAN Created on the Distributed Virtual Switch

VLAN Policy Uplink Port Group

Implement Policy

Select dvSwitch

Networking → Uplink Port Groups → VLAN policy

Uplink Port Group

    Pick a group → Edit Settings

    Select VLAN

Uplink Port

    Select Port Group

    Select ports → Edit distributed port settings

    Set VLAN Trunk Range

VLAN Type

None	VLAN	VLAN Trunking	Private VLAN
No VLAN use	Traffic will be tagged with a VLAN ID Tag can be 1-4094	VLAN Trunking allows traffic on a VLAN to be passed by the vSwitch Traffic can be passed if it's VLAN ID is in a VLAN Trunk Range (Ranges can be separated with commas)	Traffic belongs to a Private VLAN Created on the Distributed Virtual Switch

Filtering and Monitoring the Network

Traffic Filtering / Marking

- Mark traffic for QoS handling
- Filter unwanted traffic
- Enable Filtering & Marking

Traffic Filtering / Marking

Mark traffic for QoS handling

Based on Traffic type

Filter unwanted traffic

Based on administratively defined rules
Enhance Security
Rules apply to traffic between the NIC and the Port / Uplink

Enable Filtering & Marking

Distributed Port Group / Uplink port group
    Select dvSwitch → Networks → Select group
    Configure → Settings → Traffic Filtering and Marking
    Click Enable Reorder → Click Enable all traffic rules → OK

Traffic Filtering / Marking

Priority Tags

Designate higher networking requirements for bandwidth
Traffic is classified to designate this

Process

Locate port group
Networks→ Distributed Port Groups or Uplink Port groups
Select group → Configure → Settings → Traffic Filtering and Marking
Add or Select a rule to edit
Traffic Rule Dialog Box
    Set Tag for the traffic

Priority Tags

CoS (Class of Service) Value

Places a priority tag on the traffic
Marks the traffic that matches a rule of a CoS priority tag
L2
Check the box and place a value 0-7

Process

Places a priority tag on the traffic
Marks the traffic that matches a rule of a DSCP priority tag
L3
Check the box and place a value of 0 – 63

Priority Tags

Set rules for filters

Priority Tags

Set rules for filters

Traffic Direction - Inbound vs Outbound Traffic

Set qualifiers

Criteria for traffic to be matched against

Ex:

Data type

Attributes of L2 / L3 traffic

MAC traffic

System traffic

IP traffic

Multicast Filtering

Multicast Filtering

Multicast traffic forwarded
- Based on destination MAC address

Joining a Multicast group
- MAC address propagated via switch
  - MAC address to port mapping is saved
  - Stored in forwarding table

So does the switch make the decision on who joins the group?

No, the Local Multicast Router does.

Switch filters multicast traffic

Related to Multicast Groups
Snooping models

Multicast Filtering

Enable Multicast snooping on a dvSwitch

Introduced in v. 6.5 and later

Networking → Select dvSwitch → Actions → Settings → Edit Settings

Select Advanced → Multicast Filtering Mode → IGMP/MLD Snooping

Set Query Times

Select host

Configure tab → System tab → Advance System Settings → Edit

Adjust **Net.IGMPQueryInterval** Value in seconds

Default interval = 125 Seconds

Multicast Filtering
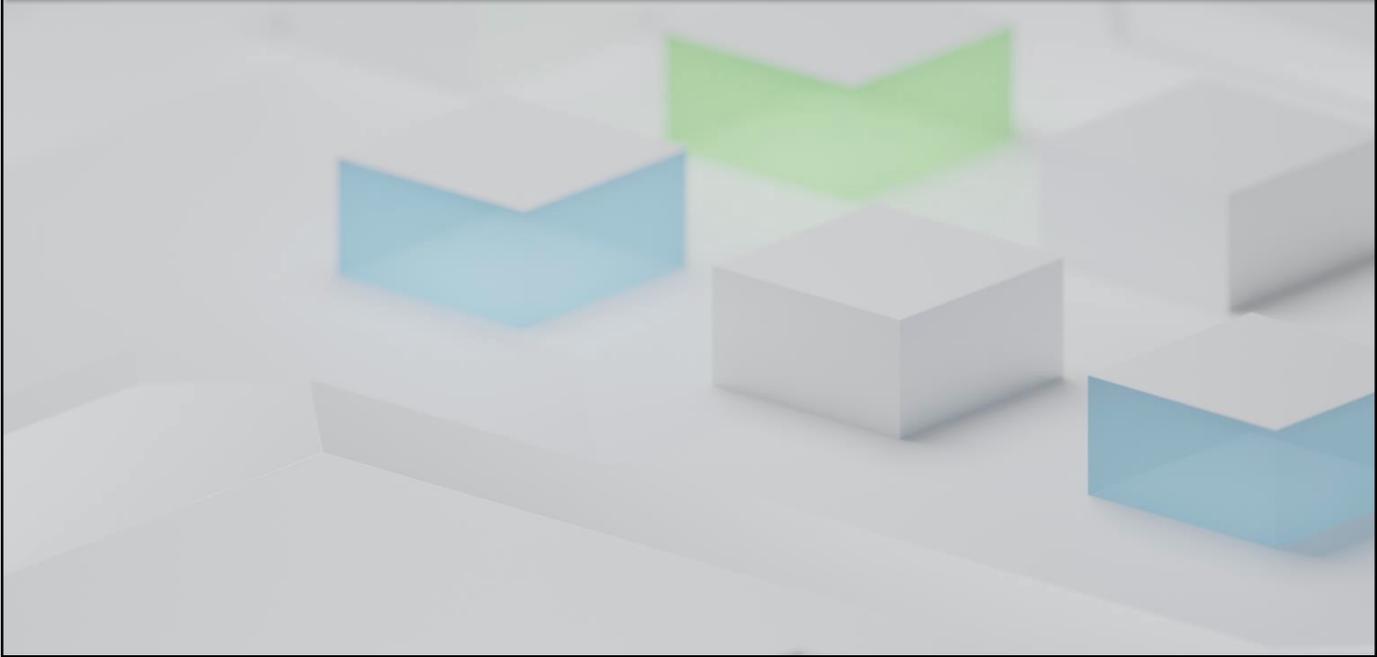
Monitoring

LLDP

Monitoring

LLDP

Displays which switch ports connect to which dvSwitches

View Properties of attached devices

Listen

Advertise

Both

Monitoring

Port-Mirroring

Mirror a copy of traffic
- From one port (or VLAN) to other ports

Other port is a monitoring connection

Used to analyze traffic

Types:
- Distributed
- Remote Mirroring Source
- Remote Mirroring Destination
- Encapsulated Remote Mirroring (L3) Source

Monitor

Health check

Used to determine health of your system

Data is sent to VMware for analysis

vCenter Server needs internet access

You must participate in CEIP

Retest as needed

Ask VMware

KB article describing your issue

Additional Features and Troubleshooting the Network

Traffic Shaping

Shaping Policy

Manipulate rate or capacity of traffic flow

Outbound only on Standard vSwitches / Port Groups

What can you configure?

Status – Enable or Disable

Average Bandwidth

Peak Bandwidth

Burst Size

MAC Address Management

MAC addresses can be set: → **From vCenter Server**
  • Also assign OUIs → **By ESXi host** → **By static configuration**

Assigned by vCenter Server → **You can change the range of addresses** → **Deconflict MAC address assignment**
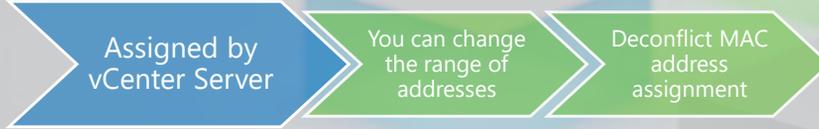
Prefix-Based

Range-Based

PVRDMA

Paravirtual RDMA

A vNIC that supports RDMA

RDMA – Remote Direct Memory Access

Remote memory access from the memory of one device into another

Does not involve OS of either device

vSphere requirements

ESXi v6.5 or later

vCenter Server 6.5 or later

A dvSwitch

Virtual hardware v 13 or later

Linux (64-bit)

Note: PVRDMA automatically enabled on vSphere 7.0

PVRDMA

Note: Remember to Enable Firewall Rule for PVRDMA

Assign PVRDMA adapter to a VM → Select VM and power it off → Actions → Edit Settings → Select Virtual Hardware → Add new device → Network Adapter → Expand Network → Connect VM to distributed port group → Adapter type Menu → Select PVRDMA → Memory Section → Reserve all guest memory (All Locked) → Power on the VM

Run vSphere in IPv6

Why use IPv6?

Large address space (3.4 x 1038 unique IP addresses)

Better for Multicasting

Simpler Routing Mechanism

Enable IPv6 on vSphere Install	Enter the DCUI	Log in	Configure Management Network	Select IPv6 configuration → Enter	Determine IPV6 address necessary for host
					DHCP assignment
					Static Assignment

Run vSphere in IPv6

Return to Configure Management Network Menu → IPv4 Configuration → Enter → Disable IPv4 configuration for management network → Enter → Add hosts to the inventory in vSphere
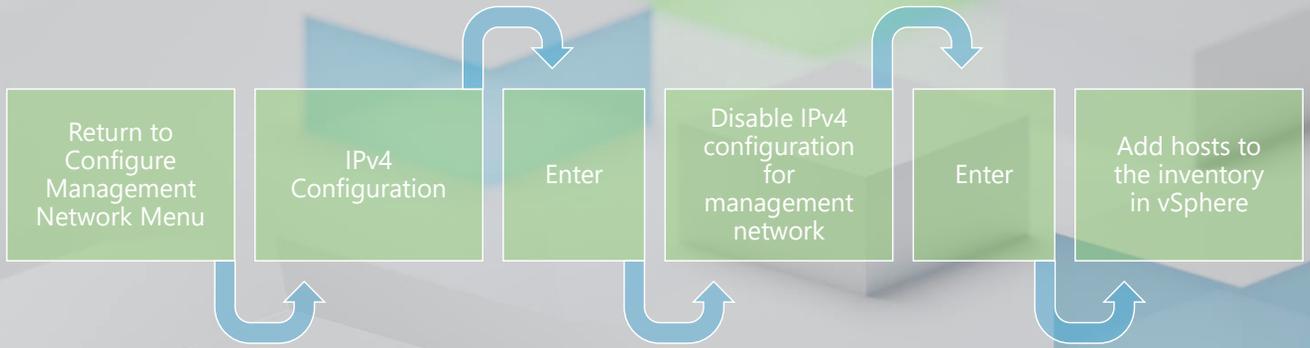
Enable IPv6 on Hosts and vCenter Server

Ex: Allows device to participate in IPv6 network

Connect ESXi host by editing VMkernal adapters

Set method for obtaining IPv6 address
DHCP
Router Advertisement
Statically configured

Known Networking Issues

IPv6 traffic occasionally fails pass through of VMkernal ports using IPSec

Change IP address for VCSA deployed with static IP address

Delay when removing NSX Distributed Virtual Port Group when the logical switch it is attached to is deleted

Known Networking Issues

IPv6 traffic occasionally fails pass through of VMkernal ports using IPSec

Occurs during migration of VMKernal ports

Solution: Remove and then Reapply IPSec after migration

Change IP address for VCSA deployed with static IP address

Requires creation of DNS records in advance

Solution: Create an additional DNS entry with same FQDN and IP address

Delay when removing NSX Distributed Virtual Port Group when the logical switch it is attached to is deleted

Solution: Reconfigure network to lighten load on switch or patience
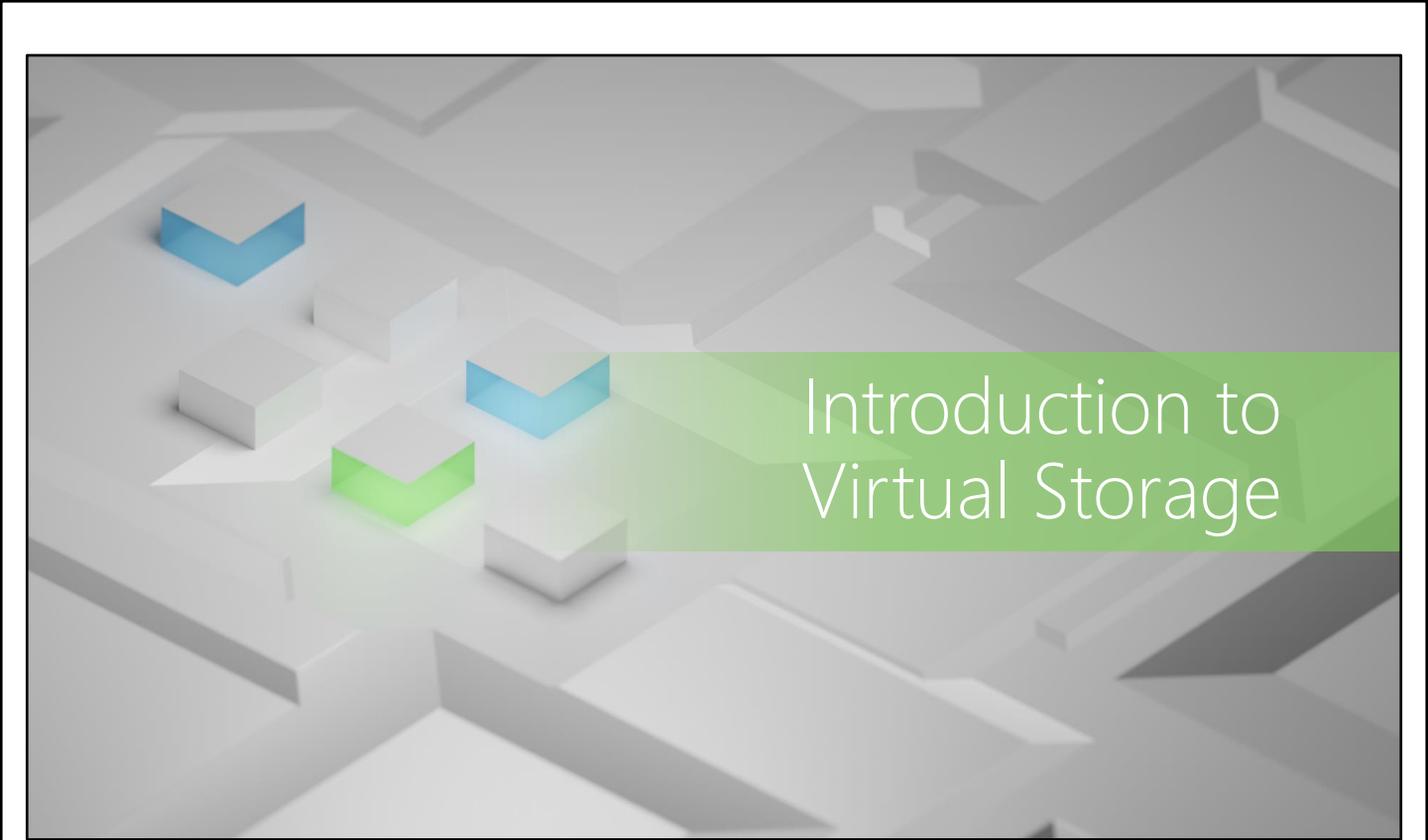
Introduction to Virtual Storage

Storage – Common Terms

TERM	DEFINITION
Local Storage	On premise storage allocated for use by ESXi via Storage Administrator.
SAN (Storage Area Network)	High speed network connecting systems or ESXi hosts to storage systems. Often connected by Fiber Channels. Can be virtualized (vSAN).
iSCSI	An internet-based option for SAN transport. Utilizes ethernet connections.
LUN (Storage Device)	A storage device that is given to a host from block storage systems.
VD (Virtual Disks)	Attached to the VM. Used to store OS, app files, and data. Copying and moving VDs is common when working with VMs.
VMFS	Deployable Datastores. Uses proprietary file system. Stores VMs.
NFS	File Protocol used over TCP/IP. Accesses volume on a NAS server. Can be mounted by ESXi host as datastore.
Raw Device Mapping	Allows guest OS on a VM direct access to a storage device.

Shared Storage Design

| vSAN | Eliminates need for external shared storage
Simplifies configuration |

| How does it work? | Utilize vSAN as shared storage point
    VMs can utilize the combined data storage offered by the vSAN
    Comprised of various Disks in a disk group (SSD, HDD, etc.). |

| Ideal Scenario | vSAN & Disk Group utilize a shared vSAN datastore |

VM
VM
VM
VM

vSAN

Disk Group
SSD
HDD

Data store

Local Storage Design

Local Storage

Disks located in ESXi host

Requires connection to storage

Optional: HBA

External systems

SAS

SATA

Examine the simple local storage design example

ESXi host

VM

SCSI device

VMDK

VMFS
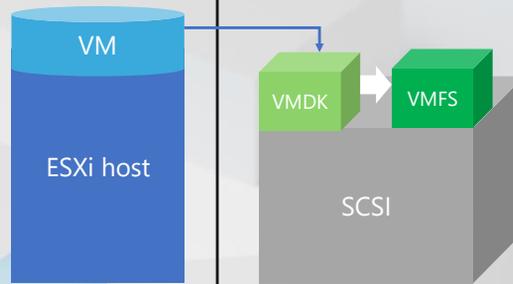
Storage Characteristics

Once block storage is registered with an adapter, we can do some research!

Showing properties of the storage can help us plan and understand our network.

Category	Description
Name	Name assigned by ESXi. Mutable.
Identifier	Universally unique ID
Operational State	Attached or Detached
LUN	Number provided by storage system.
Type	Defines the type of storage device used. (Ex: CD-ROM)
Drive Type	Flash or HDD
Transport	Which transport protocol is in use

Storage Characteristics

Once block storage is registered with an adapter we can do some research!

Showing properties of the storage can help us plan and understand our network.

Category	Description
Capacity	Overall Storage Capacity
Owner	Plug-ins used to manage paths to device
Hardware Acceleration	Capability for storage to enhance VM management ability. Options: Supported/ Not Supported/Unknown
Sector Format	Displays sector format used
Location	Storage path
Partition Format	Scheme used. MBR / GUID / GPT
Partitions	Which primary and logical partitions are used
Multipathing Policing	Policies used to manage paths to storage
Paths	How is storage accessed

Conclusion
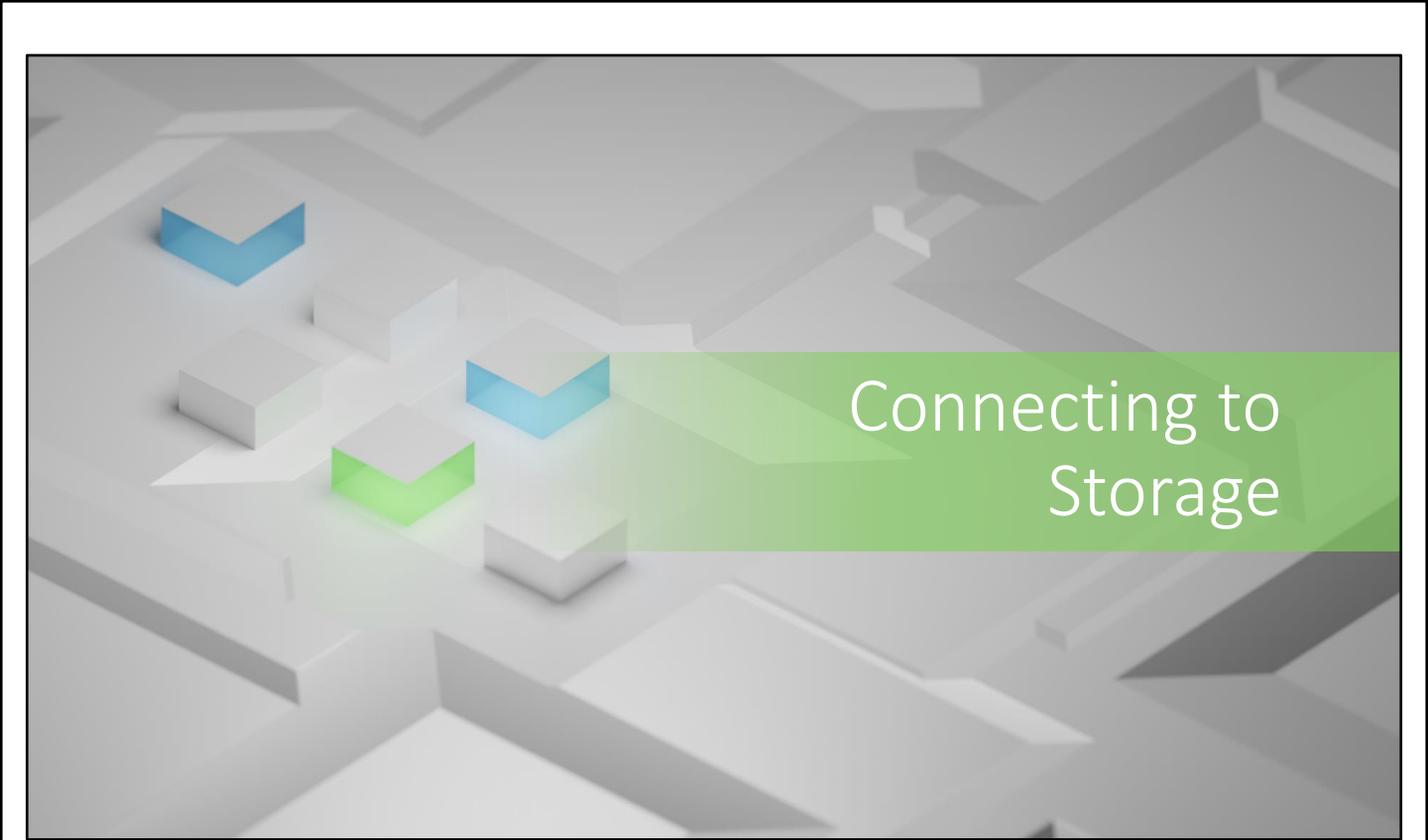
Connecting to Storage

Connecting to Storage

Storage Adapters

- Used to connect ESXi hosts to a storage device
- Require different network considerations
- Require different configuration methods

Adapter types:

- SCSI
- iSCSI
- RAID
- Fiber
- Fiber Channel over Ethernet (FCoE)
- Ethernet

SAN Implementations

Implementation Types

Fiber Channel

FCoE

iSCSI

Background before Setup

SAN Admin tools can't access OS of VMs

    Only monitor

HBA visible to SAN is part of ESXi system

    Not VM

ESXi performs Multipathing

Setting up a SAN

| Setting up a SAN is vendor specific | → | Generally the following is needed: | → | Ensure ESXi host is available on the SAN Storage Array | → | Provide the host with a World Wide Port Name for adapters as port names | → | Record WWPNs for SPs. | → | Create and Assign LUNs | → | Note the IP addresses assigned to Switches and Storage Arrays |

Templates

Pre-requirements for 8.0

Support for SAN system used

1 VMFS volume per LUN

Avoid diagnostic partition on SAN LUN unless needed

RDMs to access raw disks

LUN ID must be consistent when presented to ESXi hosts

Ensure appropriate queue for physical HBA

Note: Windows VMs requires increase of SCSI timeout value to 60

LUN management

Ensure ESXi is compatabile with LUNs

All LUNs need appropriate HBA before connection

LUNs can be shared between hosts

   LUN IDs must be consistent between hosts

For vMotion or DRS

   LUNs for VMs are provisioned to all ESXi hosts

   LUNs need consistent paths with active-passive SAN

Implementing a Fiber Channel SAN

Host Bus Adapter (HBA) management

Vendor mixing HBAs on a host can cause access issues

Matching firmware levels needed

Secure Boot

What is it?

Makes sure that hardware only boots using pre-approved software

Trusted by the manufacturer

VM's can enable / disable secure boot

UEFI Secure boot → All boot software is signed

What do you need for UEFI secure boot?

EFI firmware

Virtual Hardware Version 13 or later

OS support for UEFI Secure Boot

Implementing a Fiber Channel SAN

Implementation Process:

Vendor specific
Here are general steps.

Connect hosts to SAN

Configure HBAs with connected hosts

Ensure hosts have ESXi installed

Spin up VM with guest OS

VM has access to SAN

Booting from Fiber Channel SAN

What does it mean?

Host boot image is stored on a LUN

    In the SAN system

Host will boot from LUN on SAN

Not the local disk

Prepare to Boot:	Configure SAN	Enable Boot adapter in hosts BIOS	Set host to boot from VMware installation source
	Review Setting up a SAN slide	Initiate primitive connection to LUN	

Configure HBA to Boot

Example: Enabling Emulex HBA BIOS

Emulex is an application that provides SAN Management and HBA Support

Step 1: Enabled BootBIOS

Run **lputil**

Firmware Maintenance

Choose the desired adapter

Boot BIOS Maintenance

Enable Boot BIOS

Step 2: Enable BIOS

Host needs to be rebooted

Set adapter parameters

Choose adapter

Configure this adapters parameters

Enable BIOS

Configure HBA to Boot

Example: Enabling Emulex HBA BIOS

Emulex is an application that provides SAN Management and HBA Support

Step 3: Configure boot device

Choose same adapter

Specify location for boot entry

Configure hex for starting LUN

Select boot LUN

Select to boot device by WWPN

Reboot

Step 4: In System BIOS

Place preferred HBA support system (Ex: Emulex) as first in boot controller sequence

Reboot and install on SAN LUN

FCoE

Fiber Channel over Ethernet	Fiber Channel frames are encapsulated into Ethernet Frames		
Requires FCoE adapters	Hardware FCoE Adapters	Software FCoE	(Max 4 per host)
NICs	Partial FCoE offload	No FCoE offload	
Requires Vmkernal Network Adapters for FCoE NICs	Create and assign an adapter that supports FCoE	Assign to the VLAN used for FCoE	
Activate Adapters	Completed in vSphere	Under storage tab	Add Software Adapter icon

FCoE

Activate Adapters → Select Software FCoE Adapter → Choose vmnic

ESXi iSCSI SAN

Using a SAN

- Not everyone can directly connect to a SAN

- Advantageous to access SAN via the internet

- Solution → iSCSI

  - Replaces TCP/IP transport with RDMA transport

Functionality Overview: → iSCSI initiator operates on host → Initiates sessions through encapsulated messages

iSCSI protocol

→ Messages target iSCSI target server

Represents a physical storage system on network

VM

ESXi host

VMDK → VMFS
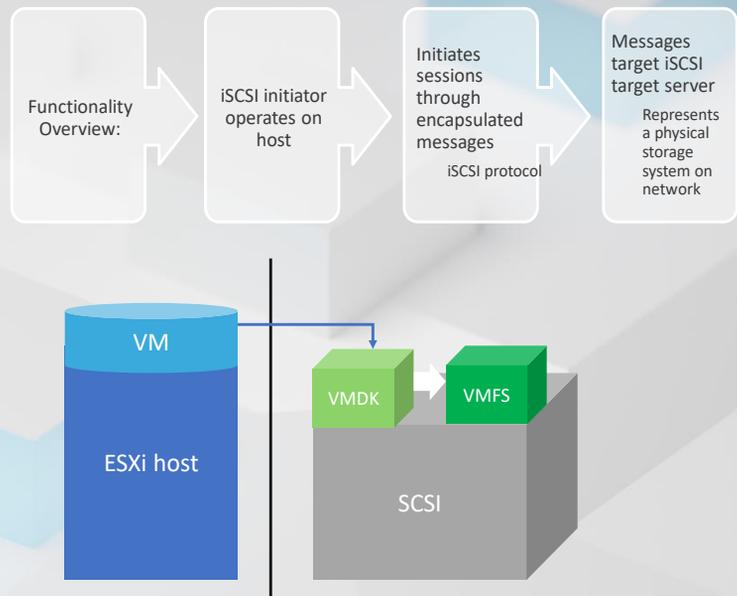
SCSI

Configuring iSCSI

Set up iSCSI storage
- This is vendor specific
- General requirements
  - Configure storage targets
  - Configure diagnostic partitions
    - Local storage
  - Set large enough queue for SCSI controller driver
  - (Windows guest OS needs timeout value of 60)
  - One VMFS datastore per LUN
- No support for:
  - iSCSI tape devices
  - Multipathing for I/O load balancing to single physical LUN
  - Multipathing with 3rd party hardware adapters with software or dependent hardware adapters

Configure iSCSI adapters

Create a datastore on iSCSI storage

Configuring iSCSI

Set up iSCSI storage

Configure iSCSI adapters

Independent Hardware Adapter

No VMKernel Networking required

Software / Dependent Hardware / VMware iSER Adapter

VMKernal Networking required

Create a VMKernal Adapter

Create an iSCSI adapter

Bind it to a iSCSI adapter

Create a datastore on iSCSI storage

Configuring iSCSI

Set up iSCSI storage

Configure iSCSI adapters

Independent Hardware Adapter

No VMKernel Networking required

Software / Dependent Hardware / VMware iSER Adapter

VMKernal Networking required

Create a VMKernal Adapter

Create an iSCSI adapter

Bind it to a iSCSI adapter

Create a datastore on iSCSI storage

Boot from iSCSI SAN

Independent adapter set up – HBA:

Vendor dependent

Here are some general steps

Host image booted using LUN on iSCSI SAN

Now no need to maintain local storage

Enter BIOS screen of host after reboot	Enter HBA configuration menu	Set I/O port	Set IP address / mask for adapter	Set gateway	Set initiator iSCSI name	Set CHAP

Boot from iSCSI SAN

| Set iSCSI Boot Parameters | Provide a target IP and Port for Boot Device settings | Set LUN and iSCSI Name | Set Primary Boot Device | Set iSCSI target Pick LUN ID |

Boot Options

1 VMFS datastore per LUN

Avoid multiple Datastores per LUN

Your SAN and iSCSI deployment will fail

Prepare for this!

Strategies:

Failover Plan

Redundant storage

Redundant connection to storage

Impact Assessments

Review HBA

Slot

Bus speed

iSCSI Best Practices

How are You Monitoring your SAN?

Review where monitored traffic is heading

Changing a LUN ID that is attached to a VMFS data store with running VMs

VMs will fail

RAID groups that contain LUNs of one host should avoid containing LUNs of other hosts

iSCSCI adapter names need to be unique world-wide!

NFS Datastore

Purpose of NFS Datastore →

ESXi host can use storage attached to a network
- *If it has read/write permissions for root account*

Over TCP/IP

Secured with:
- Kerberos
- AUTH_SYS (Default)

What can it store?

- VM files
- ISO images
- Templates
- Etc.

Features supported

- DRS
- HA
- vMotion

When does it work?

When an NFS storage environment has been set up before hand
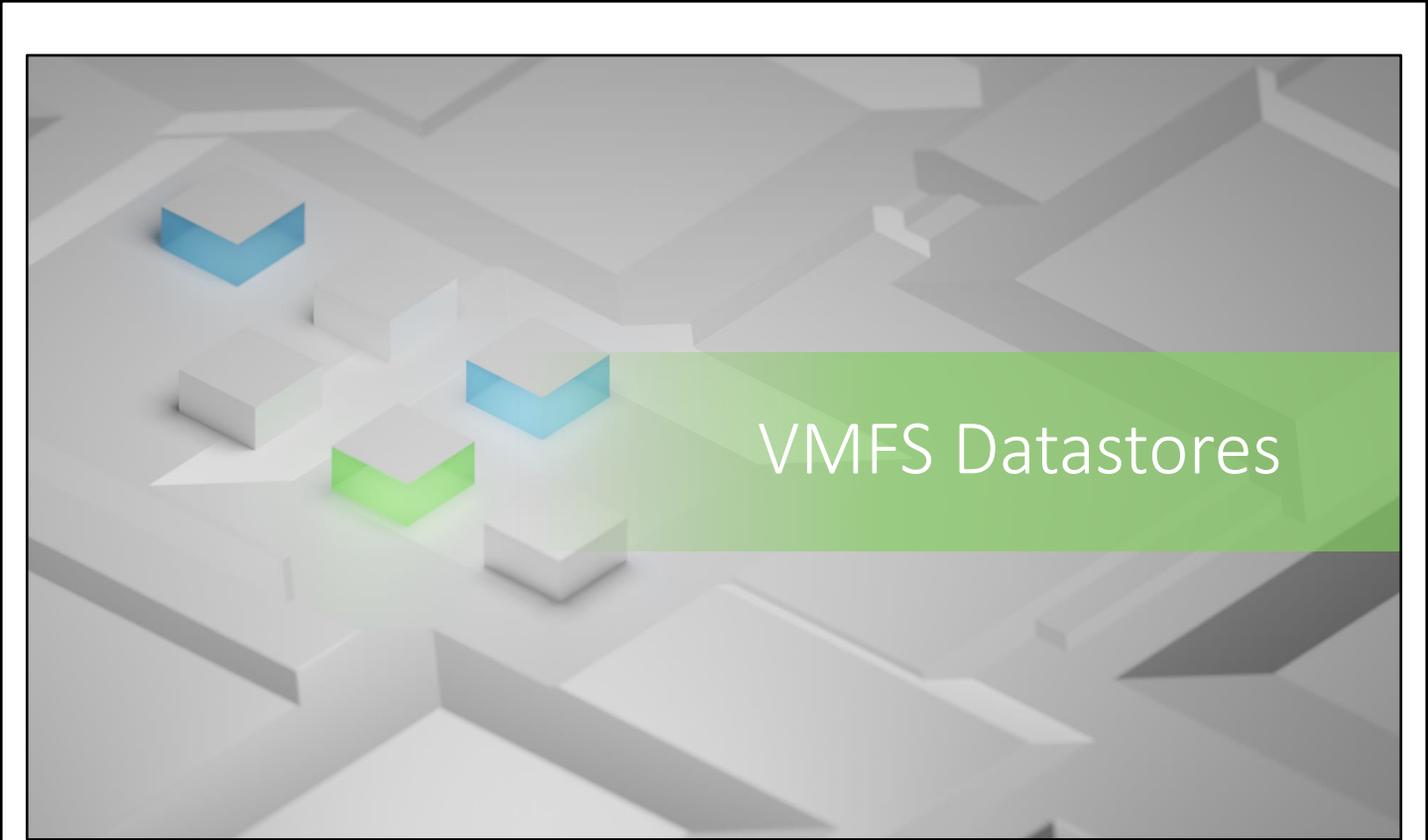
VMFS Datastores

Create a Datastore

> Select a host

> Storage > New Datastore

> Select VMFS

> Name

> Location selection

Which device will be used

Cannot have snapshot values

Create a Datastore

Select a Version
- 6 - Automatic Space Reclamation
- 5 – 2+ TB LUNs

→

Size
- Space allocated
- Block size
- Reclamation parameters

→

How will you partition your datastore
- All available
- Free space
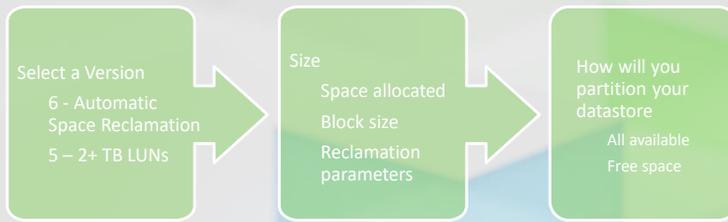
Mount Datastores

Right Click desired datastore → Select Mount Datastore → Select all hosts that can access

Extend Datastores

VMFS Datastores can be extended

No need to power off VMs

Methods:

Expand Datastore
Add an Extent

Select a Datastore

→

Menu > Increase Datastore Capacity

→

Select Device

Expand existing store

Add an extent

→

How will you set up your partition layout?

Depends on what you need

Use free space or use it to expand the datastore

Use all available partitions

→

Configure extent capacity

Min 1.3 Gb

Conclusions
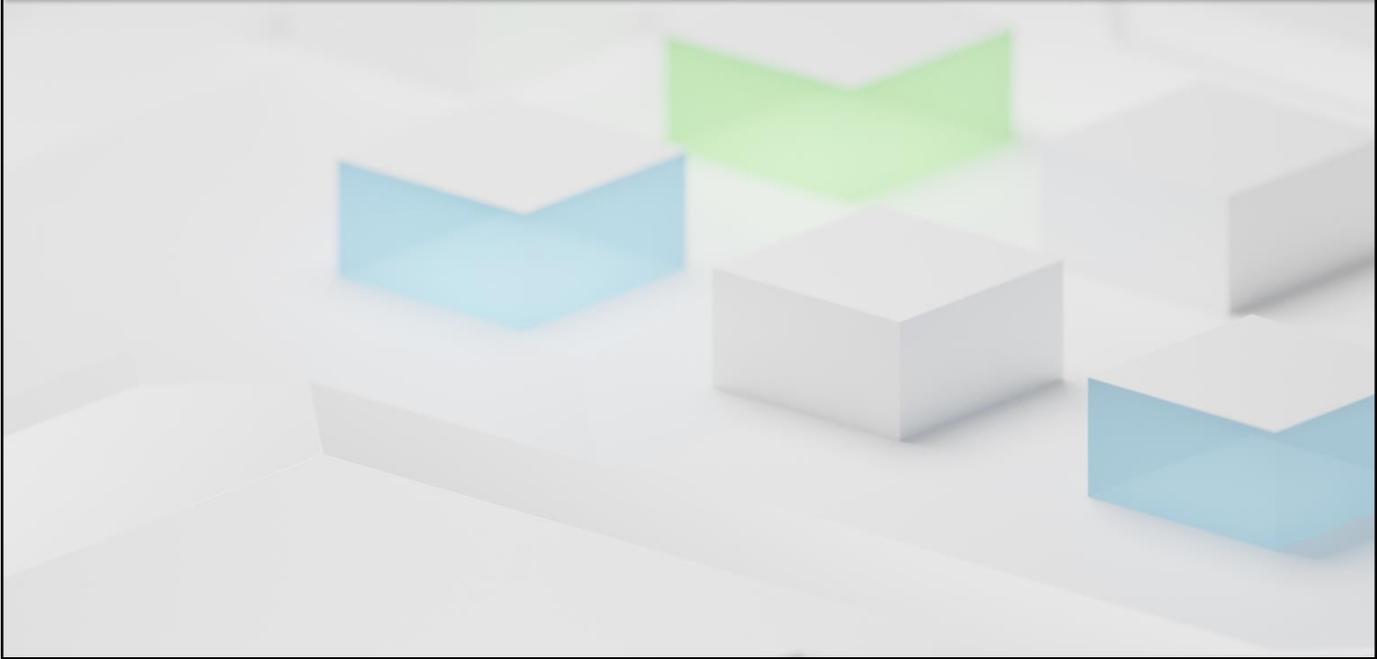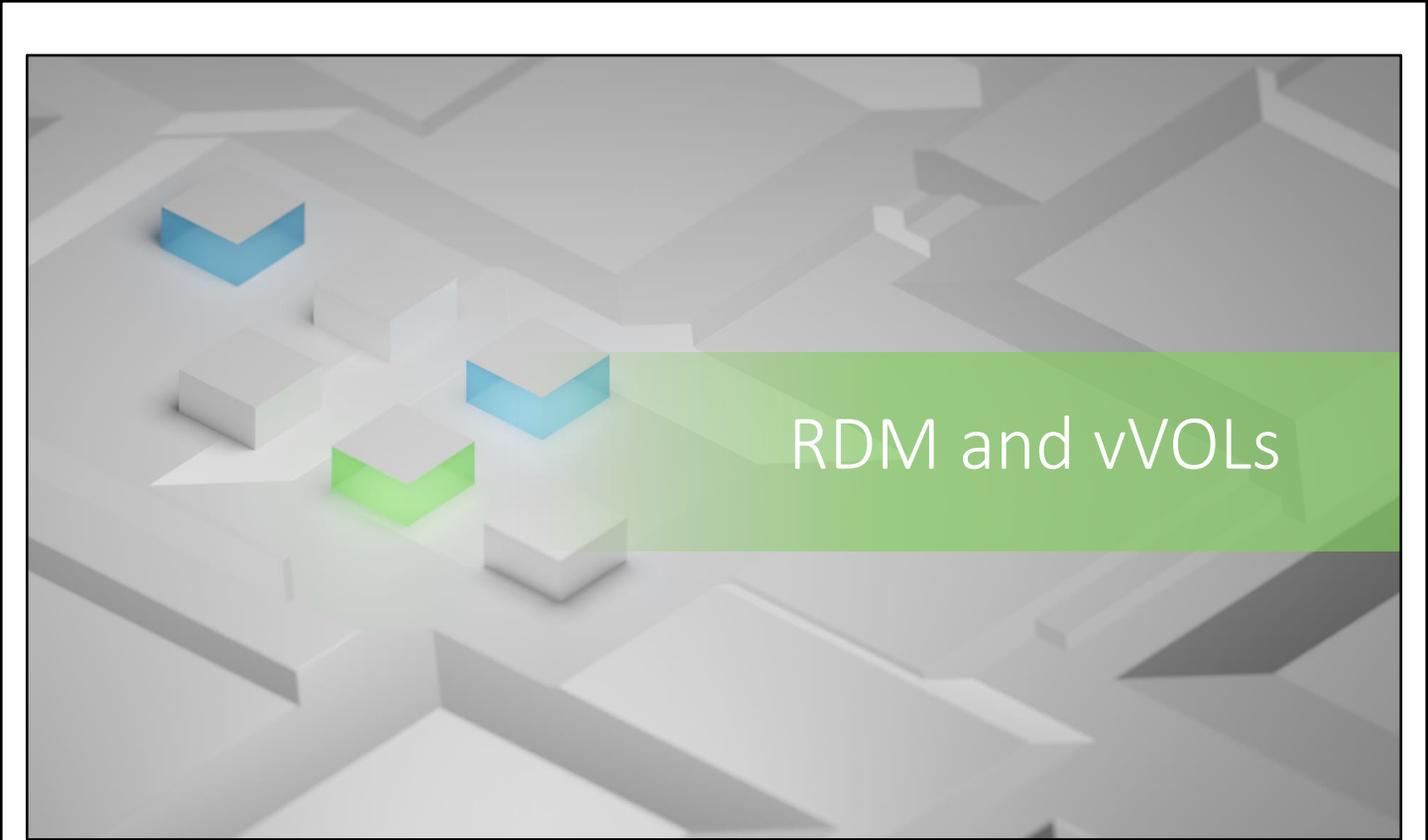
RDM and vVOLs

RDM

Raw Device Mapping	Hybrid solution
Proxy for physical storage	VM reaches out to open a VMFS volume It is directed to a mapping file within Mapping file points to a separate mapped storage device
Provides benefit of Virtual and Physical Storage	Mapping makes LUN in physical device appear to exist in the VMFS Virtual Compatibility Mode Physical Compatibility Mode

vVols

Virtualization of SAN arrays

Optimize storage for a virtual environment

Application focused

Adjusts allocation of storage use by VMs

   Dynamically changes

No file system used

Managed via APIs (VASA)

Arrays are containerized

Services are pushed to the responsibility of the array

vVols Replication

Replication of VMs offloaded to storage network

- Replicate individual objects
- Group objects for replication

Replication is policy based

- Policy defines replication requirements
    - Schedule
    - Frequency
    - RPO
    - Target
    - Secondary site
    - Deletion

vVols Replication

Creating the Replication Policy

In the wizard
Set the server
Datastore specific rules
- Enable rules for vVols storage

vVols rule page

Placement > Add Rule
Ex: Configure IOPS
Tag based rules

Datastore Services

Click tab for replication
Define rules
- Disabled
- Storage policy component
- Custom

Conclusions
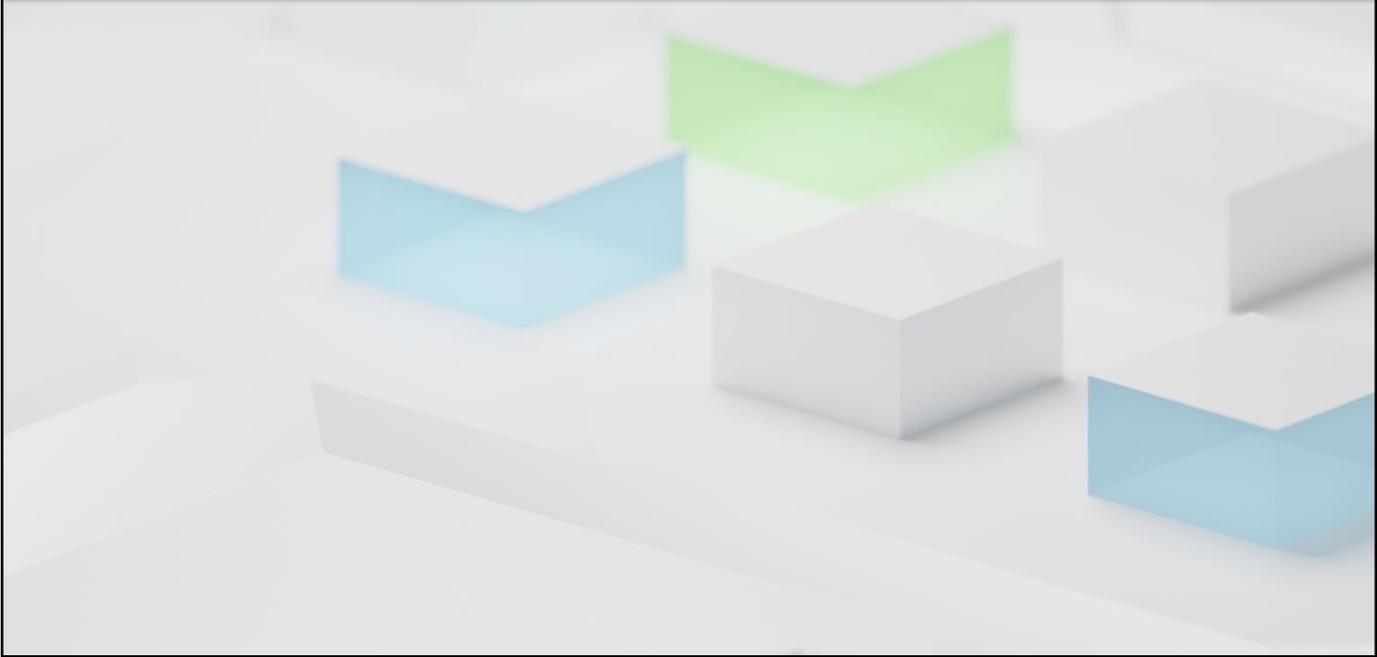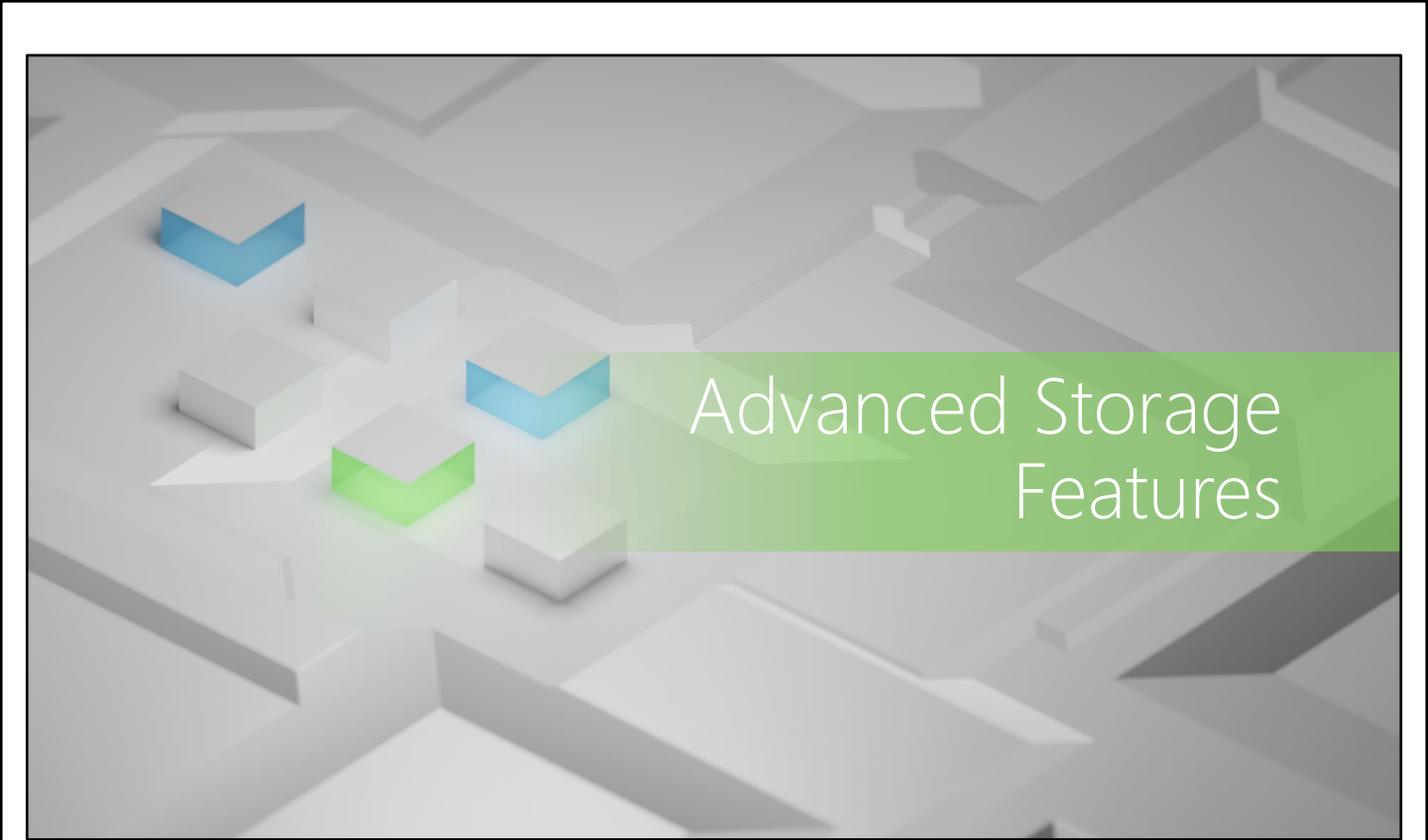
Advanced Storage Features

Data-in-Transit Encryption

| Configure Tab of the Cluster | vSAN | Services | Data-In-Transit > Edit | Enable Data-In-Transit Encryption | Rekey interval | Apply |

Now vSAN data is encrypted independently of data-at-rest with:

AES-256

Forward secrecy

What else is encrypted?

Data hosts > Witness hosts

File service data traffic

VDFS proxy and client

vSAN Storage
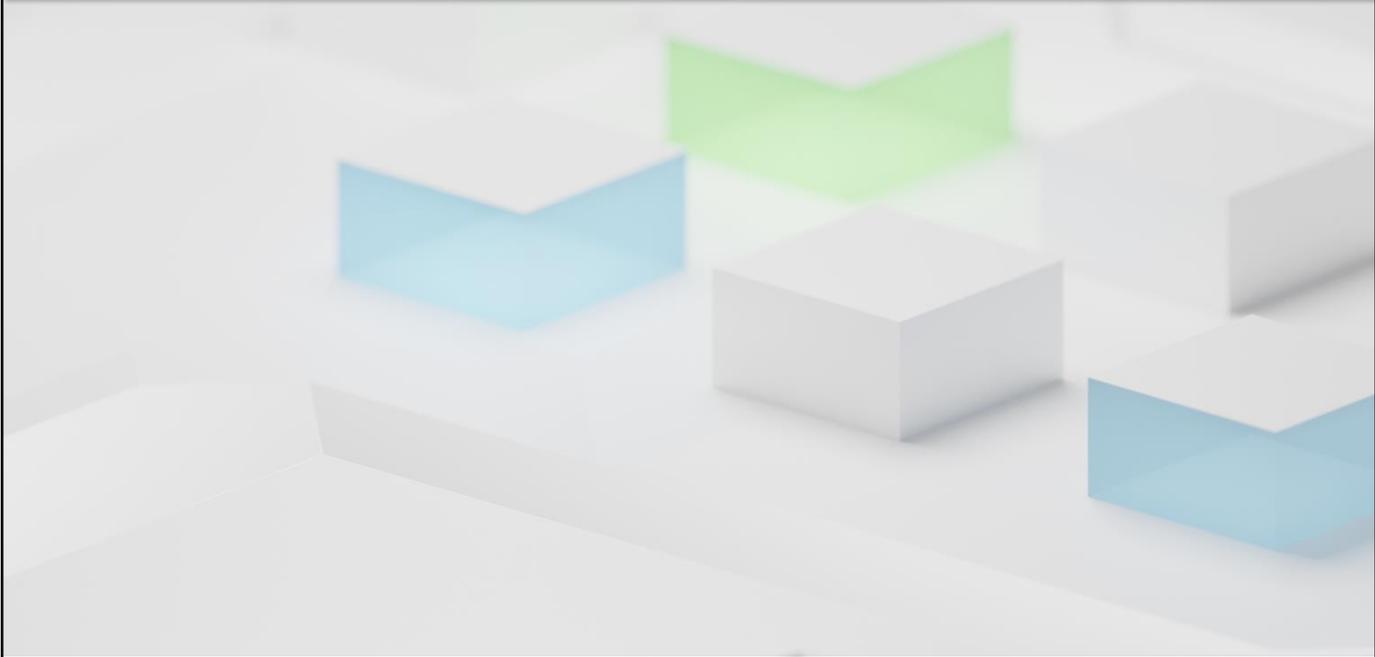
vSAN Storage

Select
Cluster

Configure
tab

Services
→
Encryption

Edit

vSAN Services Page

Enable encryption
Select KMS key
provider
You just made this!

Do you need to
remove residual
before encryption?

Wipe Residual Data

Cluster Upgrade
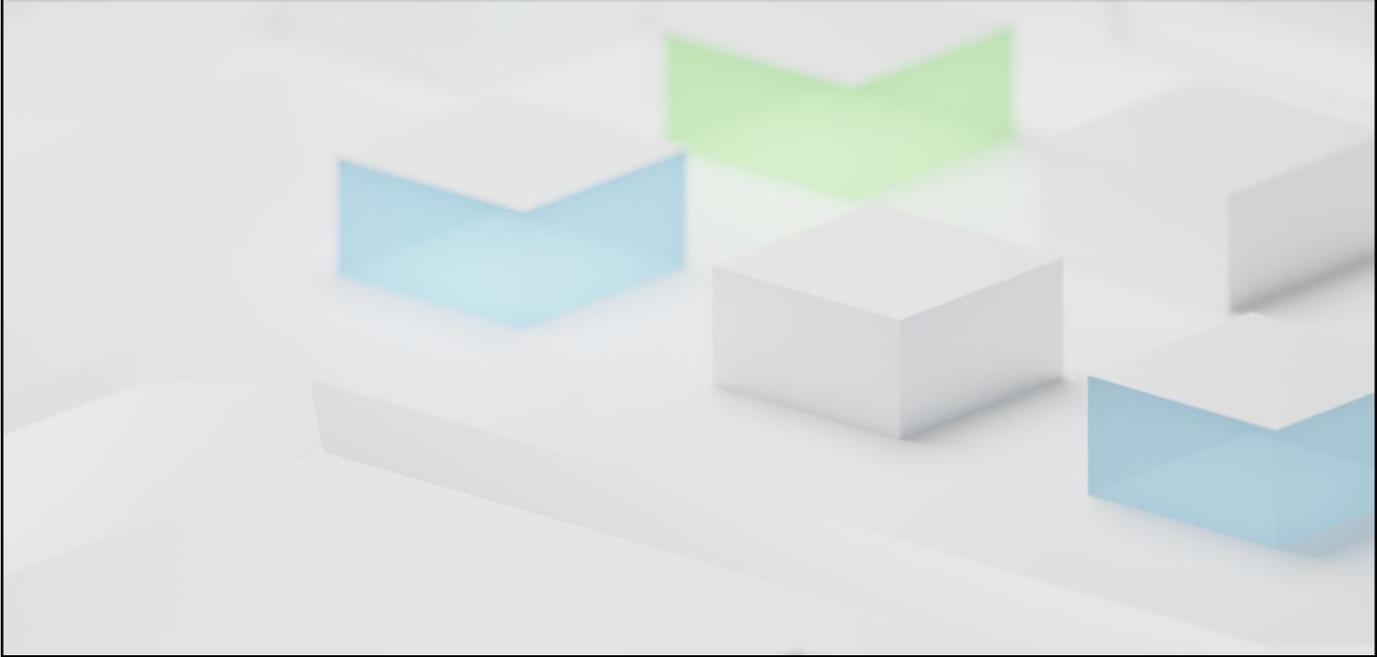
Cluster Upgrade

Process must be completed in order:

Upgrade vCenter Server

Upgrade ESXi hosts

Upgrade vSAN disk format

Hardware needs:

Verify vSAN supports hardware components

> http://www.vmware.com/resources/compatibility/search.php.

Latest vSAN Version

Enough Disk Space

Disk Format

> Capacity
>
> Reduced redundancy

vSAN hosts

> Maintenance mode

VMs

> Backed up

Storage Hardware Acceleration

Summary:

If storage system supports host can offload VM Management tasks to storage systems

Supported by:

- Block storage devices
- iSCSI
- Fiber Channel
- NAS

Hardware Acceleration is used to enhance:

Migrating VMs

Deploying & Cloning VMs

- From templates

Locking VMFS clusters

Provisioning virtual disks

- Thick disks

Fault Tolerance

Vendor Independent

Different vendors may or may not meet the requirements

Check with the vendor!

Thick and Thin Provisioning

Thick

Traditional Storage Method

Storage space is created before it is needed

- Anticipatory

Fixed amount of storage

Space can be left unused

Thin

Flexible storage allocation

- Reactionary

Thin disk only occupies needed storage space

- If it needs half of 40GB it will only occupy 20GB
- It will fill the rest as necessary

Array - Level

Virtual Disk - Level

Create Thin Provisioned VD

1 Create a new VM	2 Customize hardware page	3 New Hard Disk	4 Set necessary disk size	5 Select Thin Provisioning	! Finish
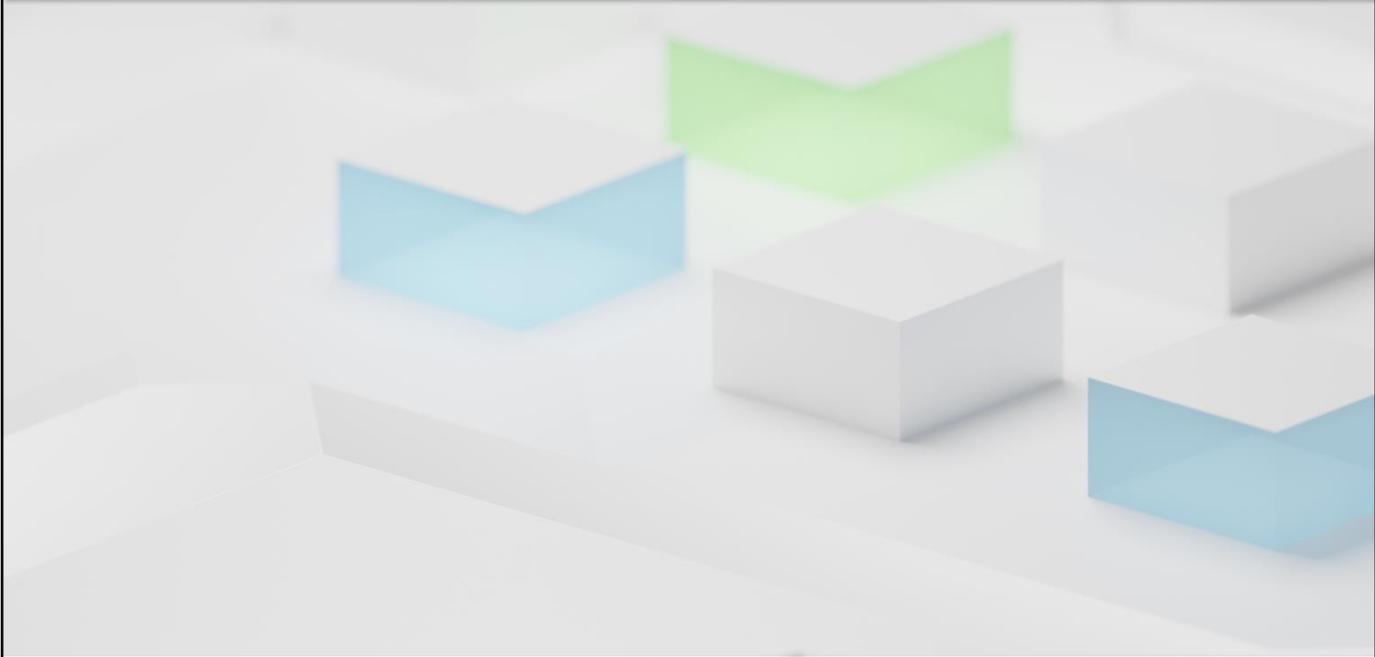
vmkfstools

vmkfstools

Manage VMFS volumes

In cloud shell
Use vmkfstools
- **Create datastore**
- **Manage datastores**
- **Manipulate datastores**

Example:

Create a VMFS Datastore
Vmkfstools –createfs [NAME] –blocksize [PARTITION DEFINITION]
Set the partition
Vmkfstools –spanfs [SPAN PARTITION HEAD PARTITION]

vmkfstools
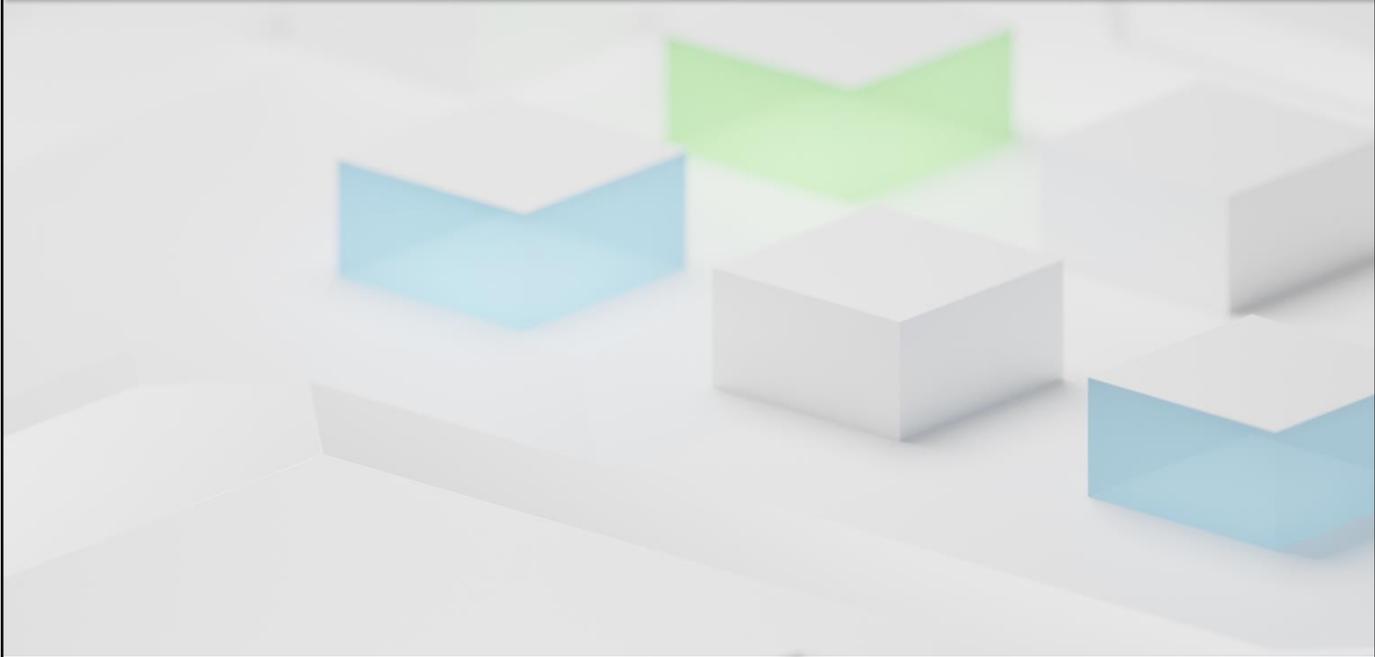
I/O Choices

I/O Filter Type	Description
Replication	All I/O operations are replicated to the target.
Encryption	Encryption tool for VM. Provided by VMware.
Caching	Local flash can be used to cache virtual disk data. Accelerates functionality of the virtual disk. (Requires Virtual Flash Resource)
Storage	Limits levels of storage I/O provided to VMs during periods of high traffic.
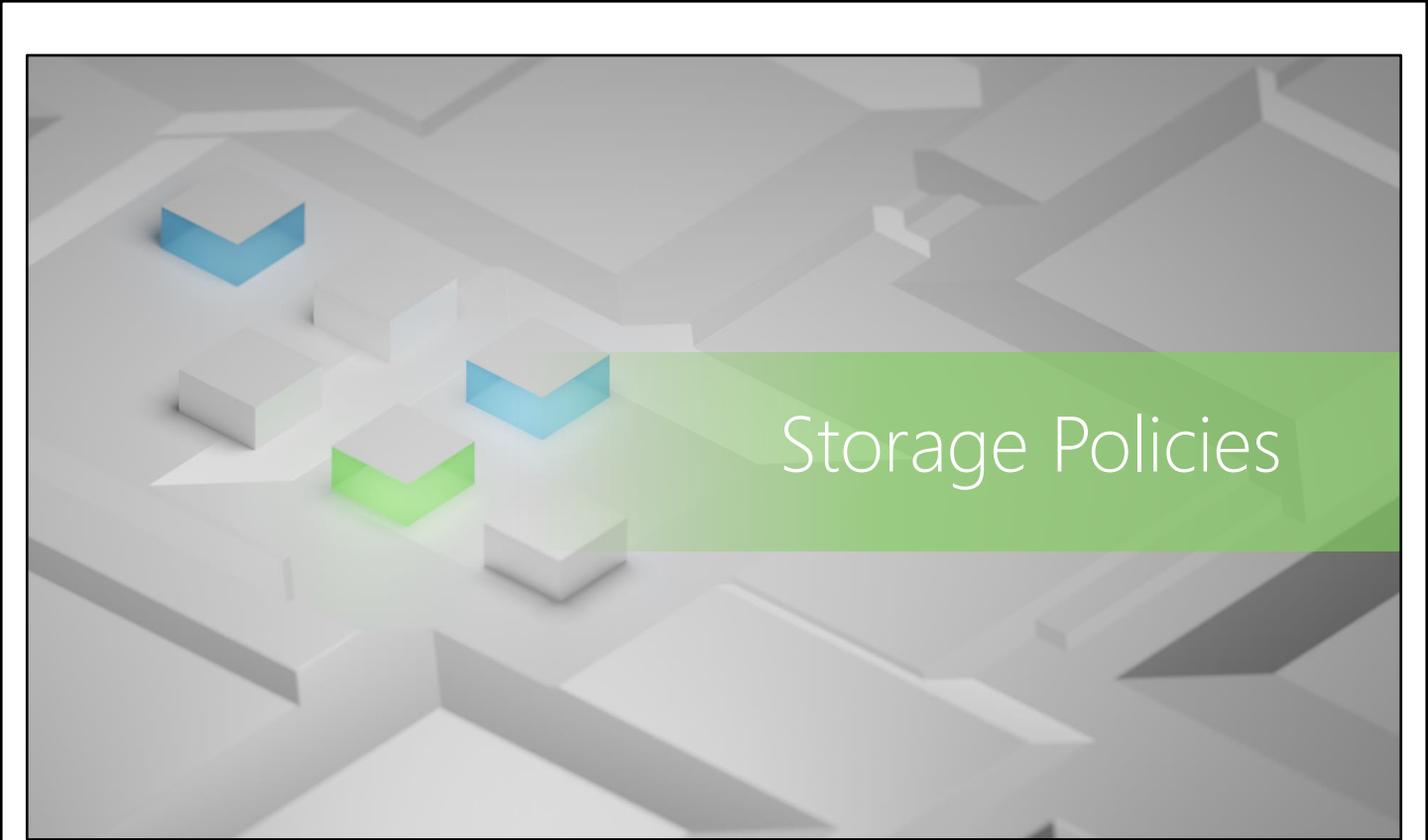
Storage Policies

SPBM – Storage Policy Based Management
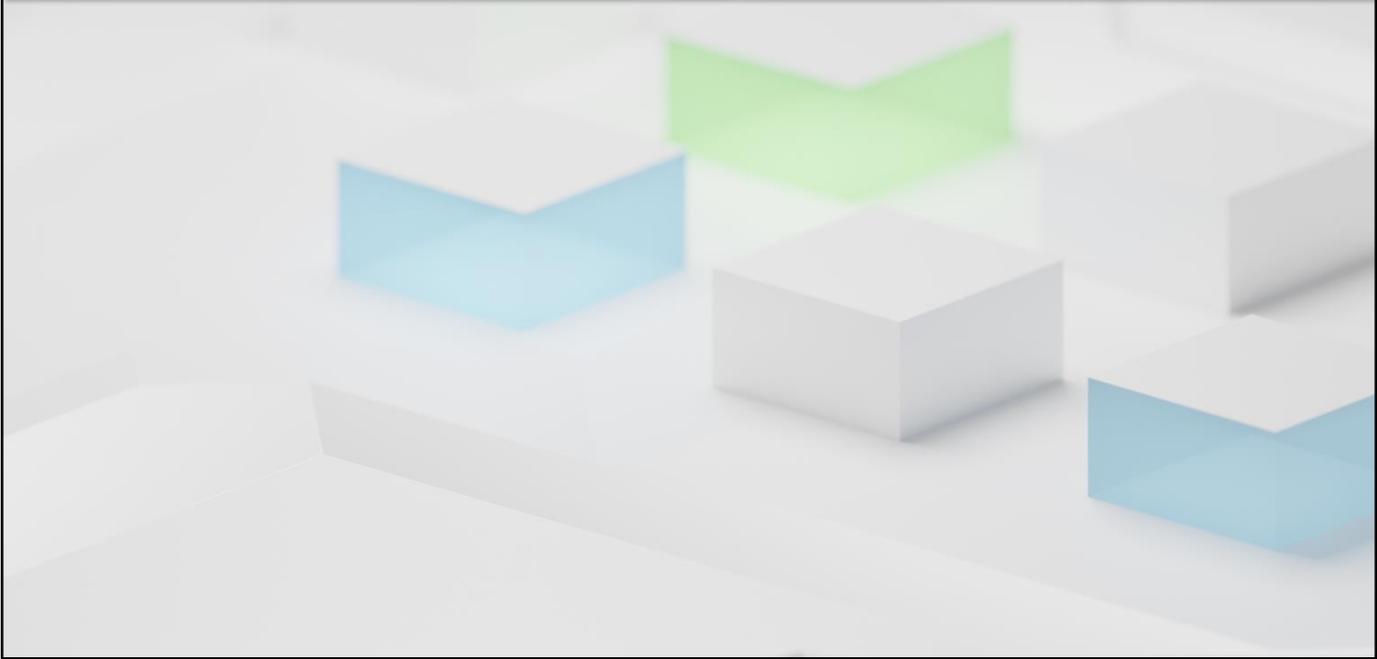
SPBM – Storage Policy Based Management

| Aligns storage with: | Need of Network
Need of Application
Need of VMs |

| Unified Control Panel | Universal framework of integration |

| Controlled via VM Storage Policies | Administrators build policies
Define capabilities of storage array |

| SPBM interprets requirements | Aligns level of storage service with VM service tier
Based on policy defined by the administrator
  Policies assign detailed storage parameters to disks |

SPBM – Storage Policy Based Management
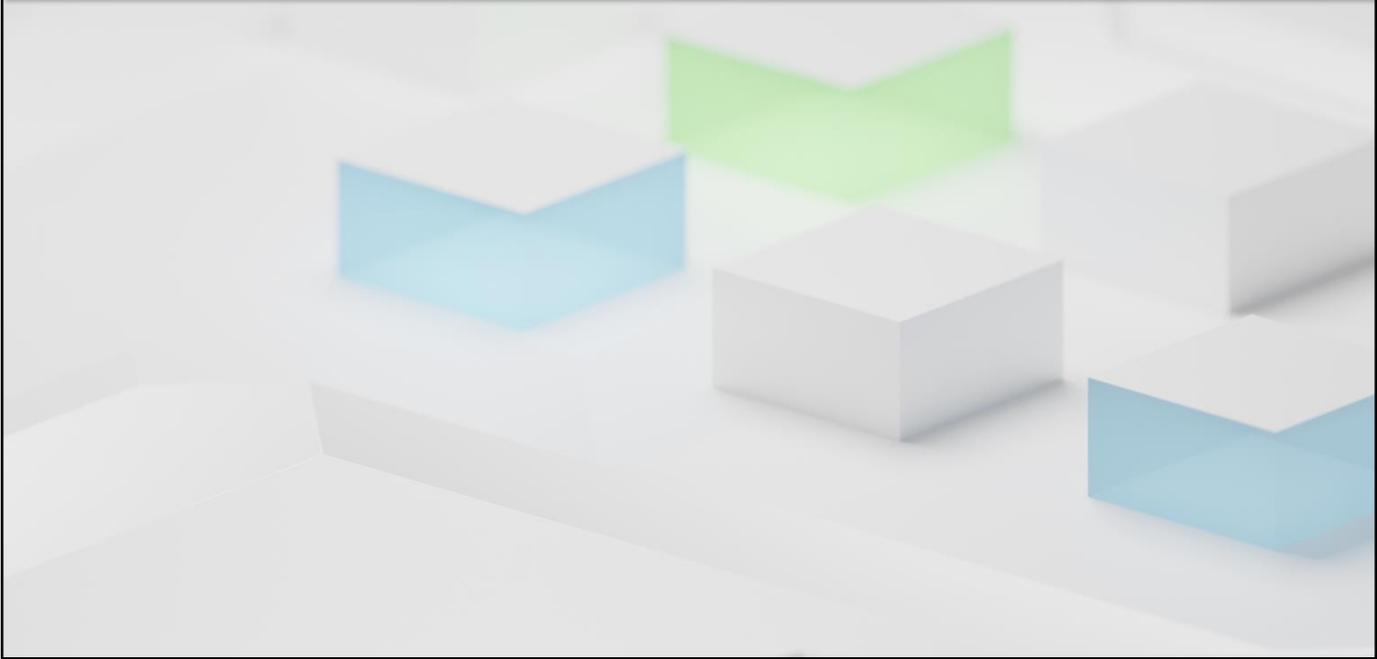
Storage Policy Components

Policies include components

Defines services for VMs

Defined in anticipation of needs

Associated to Storage Policies

Components Define:

Compression

Caching

Encryption

Replication

Type and grade of service

Storage I/O Control

Best Practices:

Components can only have 1 rule set

Is the component reference in VM Storage Policies?

   You can't delete it until it is

1 component per category

   When adding to a policy

Create Components

Create in vSphere	New Storage Policy Component Create	Set unique name amongst components or policies	Set Category Example: Encryption Storage I/O control	Who is providing the service?	Set category parameters Different Categories → Different parameters

Example Component Creation
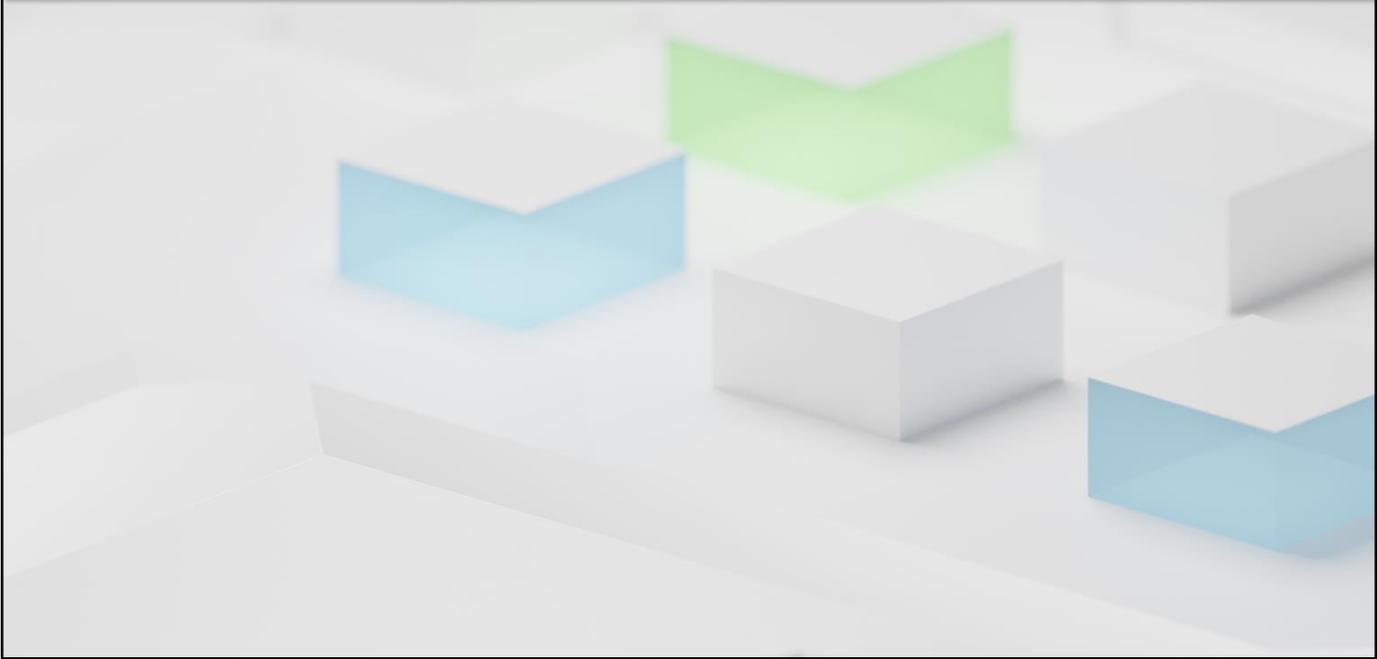
vSAN

vSAN

Software storage solution

Aggregates all attached storage solutions
  In one logical virtual storage area network
Storage Pool used amongst all hosts
Implemented on hypervisor

vSAN Types

Hybrid
  Flash devices used for cache memory
  Magnetic drives used for capacity
All-Flash
  Flash devices used for cache memory and capacity

Managing vSAN

Storage Policies – SPBM
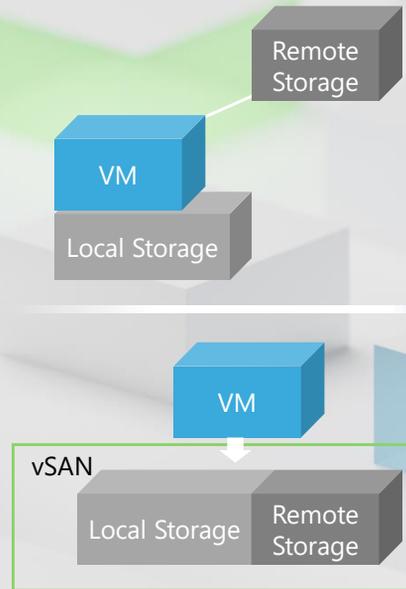
vSAN Key Concepts
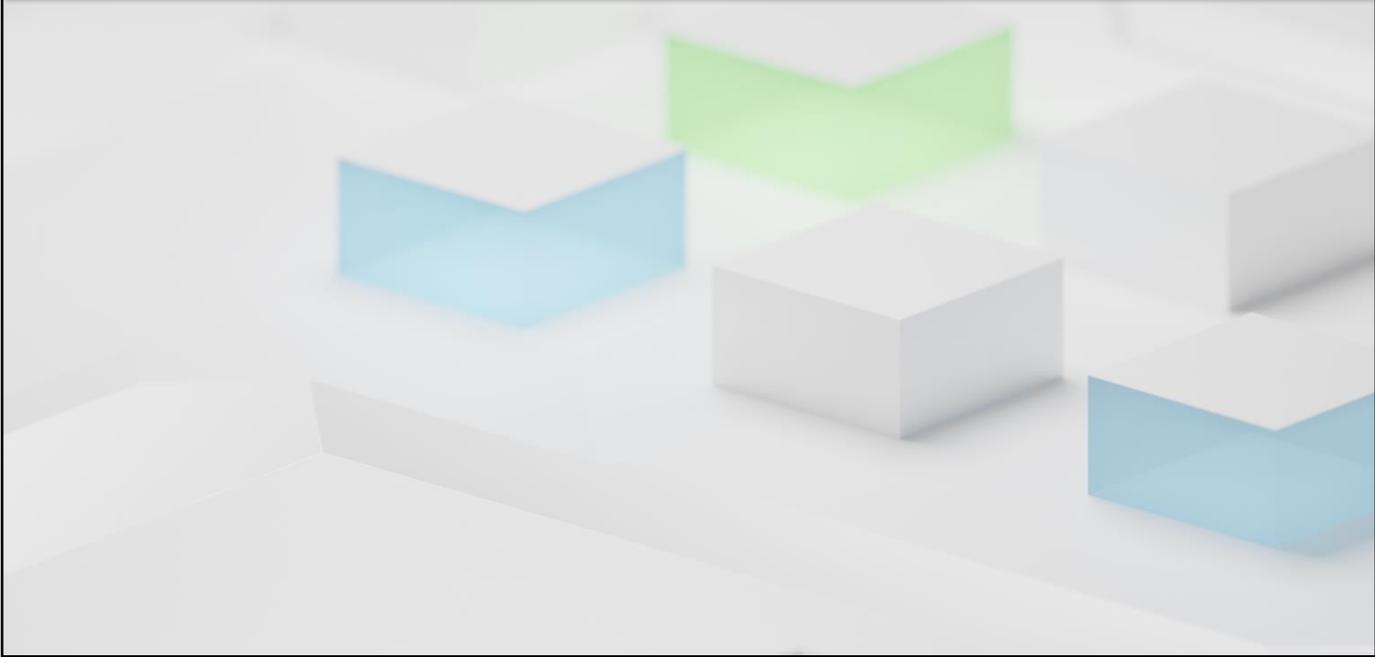
vSAN Key Concepts

Disk Group

Storage used for performing Operations
   Provide functionality to vSAN cluster
Groups of flash and capacity devices

Datastore

00110
01101
01111

When a vSAN cluster is enabled a unique datastore is created
Service level can differ per VM
Characteristics of the Datastore can be altered
      Appear as Capabilities
      Capabilities are referenced in storage policy for VMs

Consumed Capacity

Amount of storage consume by VMs

vSAN Key Concepts
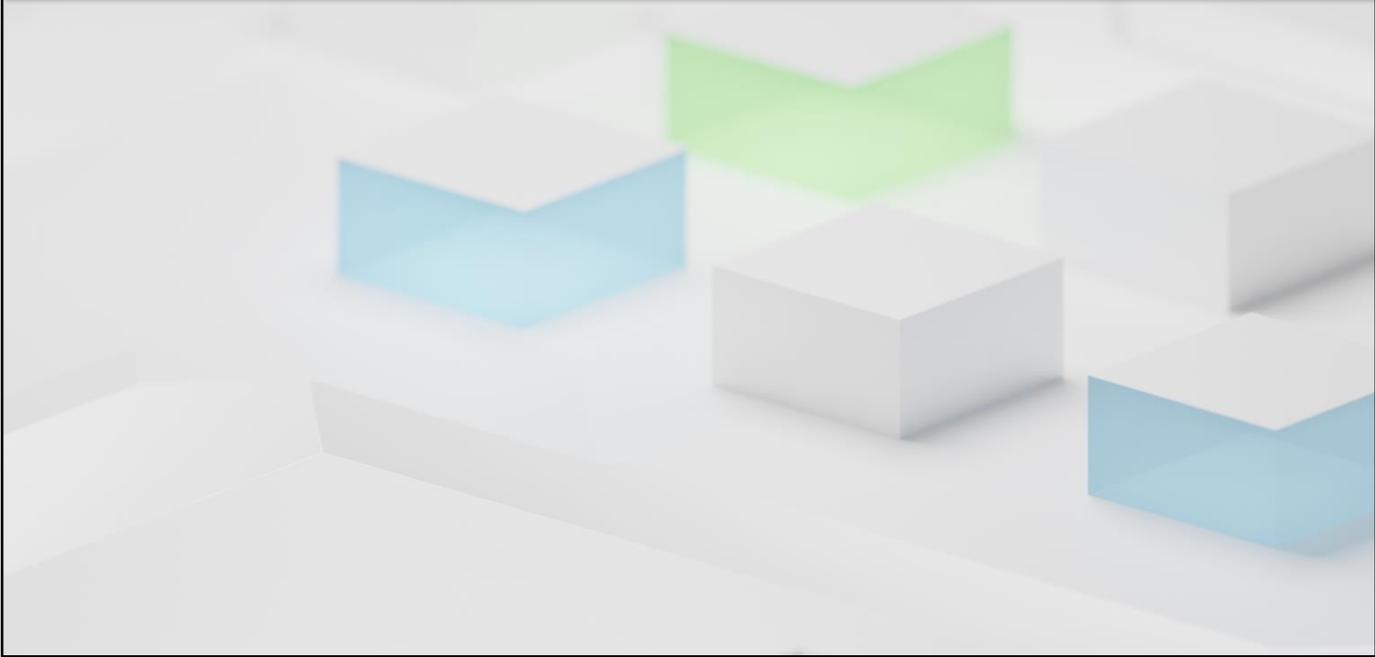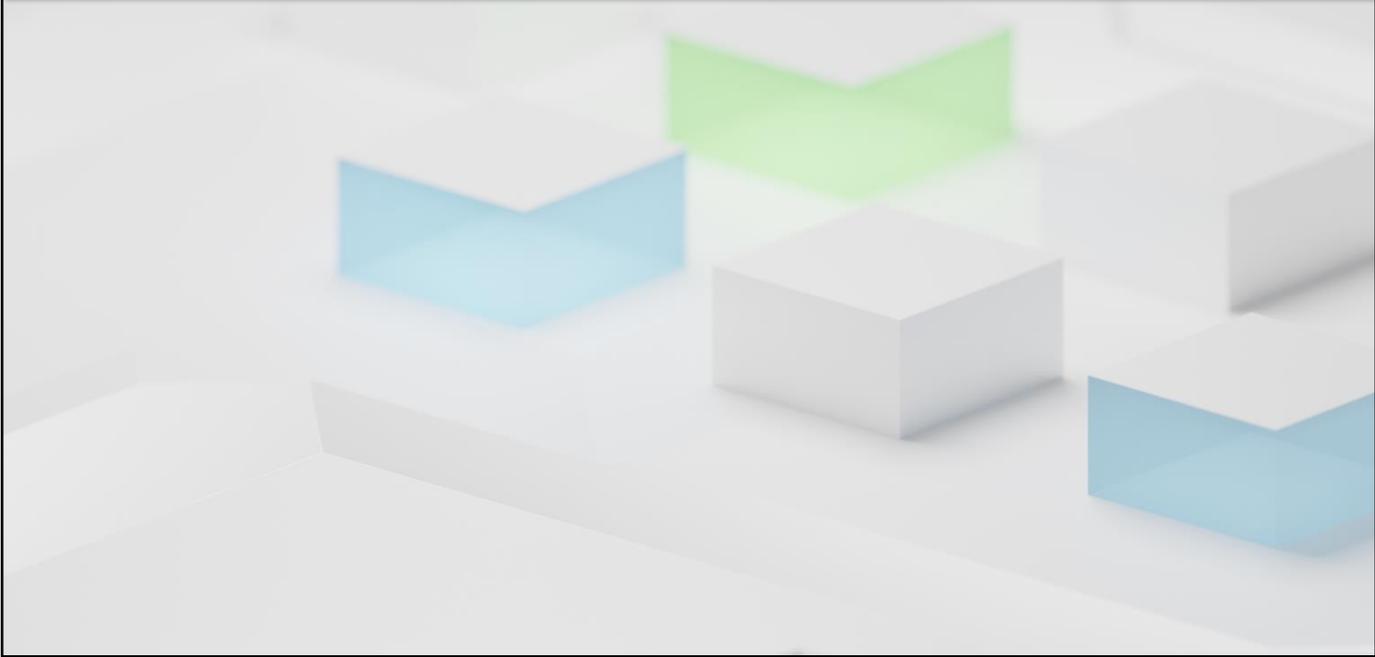
vSAN Key Concepts
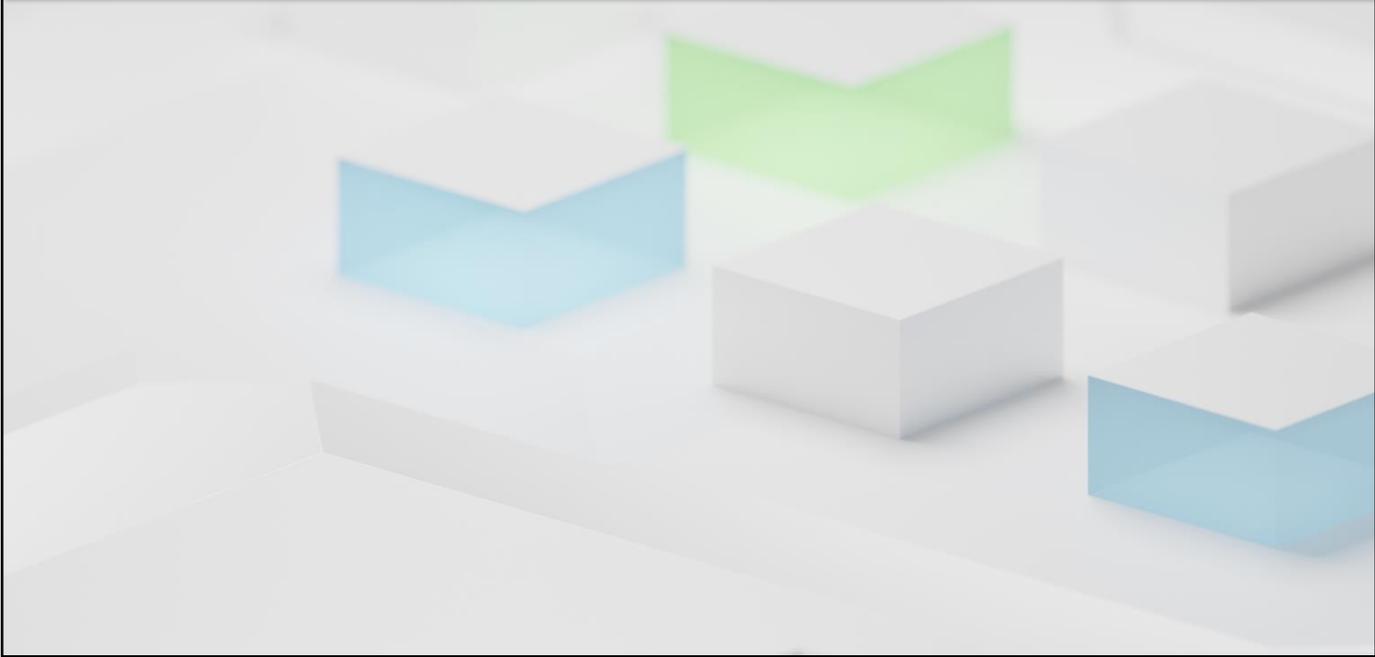
vSAN Key Concepts

vSAN Key Concepts

Object Based Storage

Objects
Components

VM Home Namespace

Home directory
Holds configuration files
.vmx
Logs
vmdks

VMDK

Stores contents of hard drive

Swap Object

Temporary Disk Storage
Created on VM power on

vSAN Key Concepts
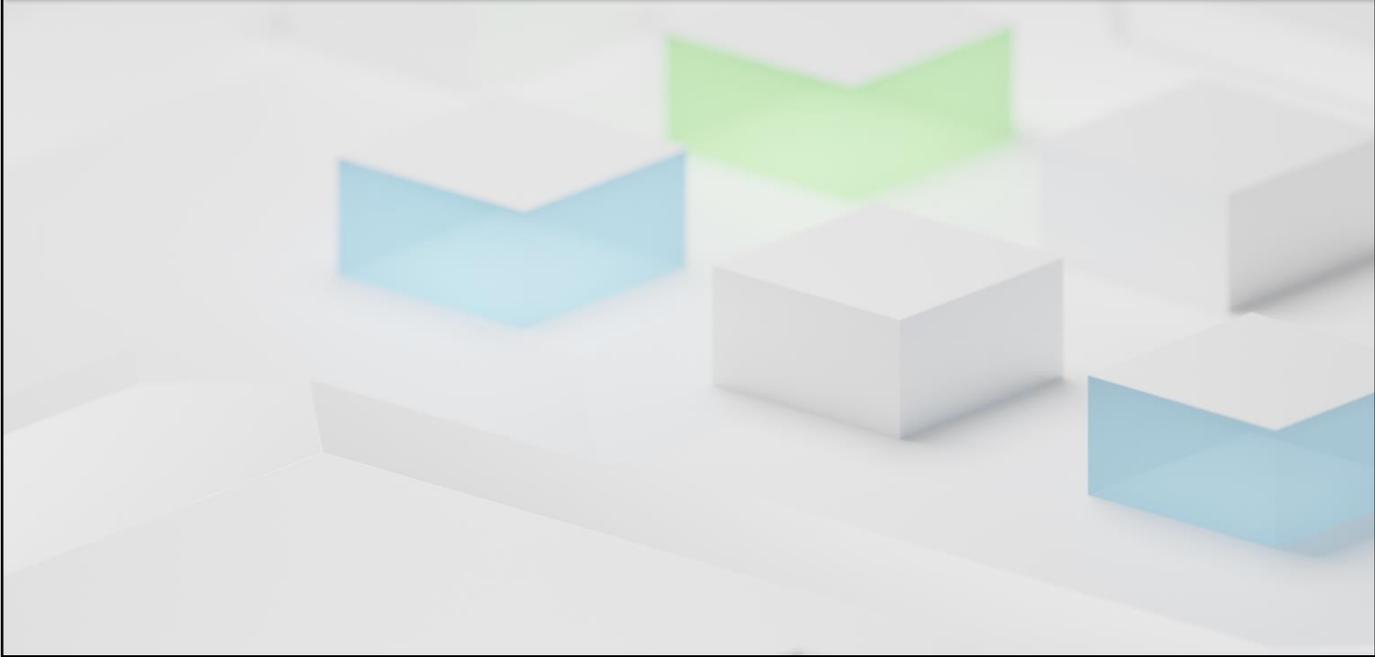
Requirements for a vSAN

Cache

1 SSD or Flash Device

Hybrid Cluster need:

- Flash Caching to cover 10 percent of storage consumed

- On capacity devices

(This does not consider replicas)

VM Data Storage

Hybrid Configuration = 1 Magnetic Disk

All-flash disk group configuration = 1 SSD / Flash device

Requirements for a vSAN

Controllers

- One HBA
- or
- One RAID Controller
  - Passthrough mode
- Don't:
  - Mix controller modes
    - Between vSAN and SAN disks
  - Mix disk groups
  - RAID group

Flash

Is Host Memory < or = 512GB? Is External Device Memory > or = 4 GB?

- Yes = Boot from External USB
- No = Resize core dump partition on host
- or
- Select a disk device with at least 16 GB

vSAN Design
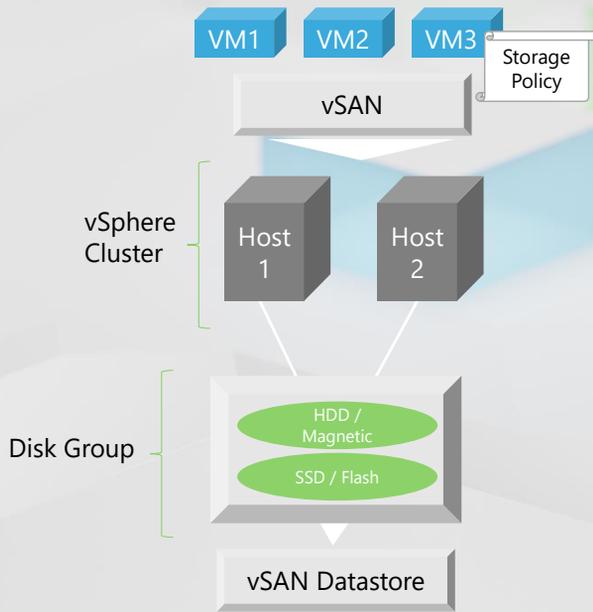
vSAN Design

What to keep in mind:

- Design
- Size
- Capacity

Plan around Expected Consumption

- Calculate Capacity
  - VM Consumption Calculation
  - Datastore Capacity Calculation
  - vSAN Overhead Calculation

Guidelines

- Leave 30% empty space
- Expect and Reserve more Capacity
- Make space for:
  - Home Namespace objects
  - Snapshots
  - Swap files

Primary level of failures to tolerate

- Tolerance Method

Raw Capacity = (# Disk Groups in cluster x Capacity size of devices) – vSAN Overhead

VM Consumption = Number of VMs in the cluster x Expected percentage of consumption per VMDK

Datastore Capacity = Expected Overall Consumption x (PFTT +1)

vSAN Design

PCIe or Flash for: Caching · Capacity

Magnetic Devices: SAS · NL-SAS

Controller Design · Multiple Controllers — Isolate failure · Passthrough mode
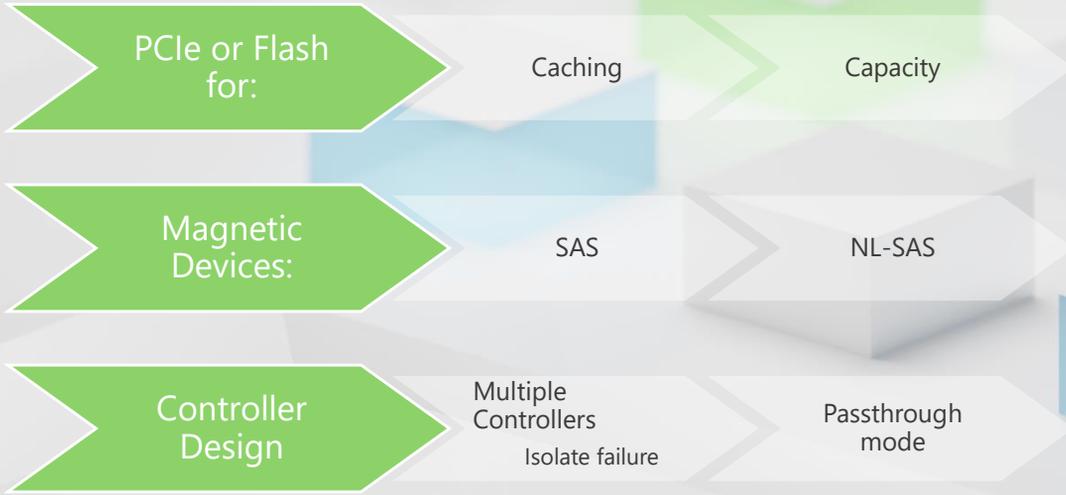
vSAN Design

Consideration for vSAN hosts

Memory
How much Per VM / Host

CPU
Sockets per host
Cores per socket
vCPUs based on VMs
Core to vCPU ratio
Overhead

Host Networking

Ethernet Adapters – Bandwidth

1GbE Minimum

10 GbE for all-flash set ups

vSAN Design

Multiple Disk groups

Pros? Improved performance, failover, and recover time.

Cons? Cost, memory needs, controller increase.

Drive bays

Hot Plugs

Primary Level of Failures to Tolerate (PFTT)

2 x PFTT + 1 = Number of hosts required for cluster

More hosts = Better chance to tolerate host failure

Hosts with Uniform Configurations

      Improves predictability

      Similar maintenance

      Increased performance on hosts that have different types of cache devices

vSAN Design

Network

Failover / Load Balancing

    Route based on Originating Virtual Port

    Route based on IP hash

    Route based on physical Network Adapter Load

After v 6.7 unicast network is sufficient for setting up vSAN

Mark vSAN Traffic

Segment vSAN Traffic with VLANs

Configure Static Routes

    Don't have to rely on ephemeral IP addressing

vSAN Design

Network

Place hosts in the same subnet

Dedicated bandwidth

    1 vs 10 GbE

Configure a port group

    Set policies

    Set VLAN

Ensure Firewall allows vSAN related traffic

Pre- Requirements to Create a vSAN

What do you need?

Min 3 ESXi hosts with Version 7

Hosts need 8 GB memory

Controller is in Passthrough mode or RAID 0

1 Cache & 1 Capacity Storage Source

Hosts need 1 network adapter

May need a Vmkernal Network for vSAN

   Dependent on network

(Demo) Prepare Cluster for vSAN

Verify Compatibility

Ensure Storage is adequate

Provide Memory dependent on vSAN size

Prepare hosts

Update vCenter Server version

Prepared Cluster

Create a vSAN Cluster

Select a Datacenter

New Cluster

Select Name

Activate:
DRS
vSphere HA
vSAN for the cluster

New Cluster appears

Attach additional hosts to the cluster

Edit vSAN Settings

Select Cluster → Configure tab > Services → Edit → Enable:
Deduplication
Compression
Encryption
  Data at rest
  Data in transit

Edit vSAN Settings

Performance Services → **iSCSI Target Services** → **Enable File Service** → **Set the Capacity Reserve**
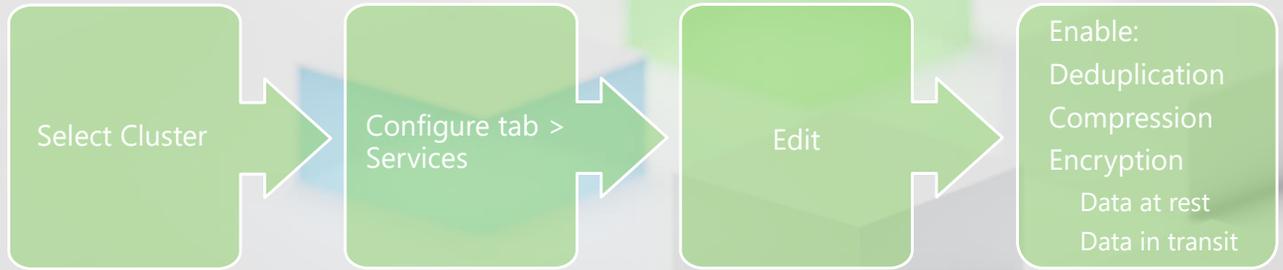
Edit vSAN Settings

Advance Choices:

Object Repair Timer

Read Location

    Stretched clusters

Thin Swap Provisioning

Large Cluster Support

    64 hosts

Automatic Rebalance

View the vSAN

Storage Policies often require you to know characteristics of the vSANs Capabilities

Helps administrators to configure a storage policy for VMs

Navigate to vSAN Datastore	Configure tab	General Tab	Review properties of the vSAN
You just created!			Name Capacity Capabilities Storage Policy vDisk Storage Policy

Upload / Download with vSAN

⬆ Upload ⬆

Files inherit the policy of the datastore they are uploaded to

Process

- Select vSAN Datastore

- Files > Upload Files / Folders

Stream-Optimized format

- Vmdk only

⬇ Download ⬇

Stream-Optimized

- Name_stream.vmdk

- Convertible

Steps:

- Select vSAN Datastore

- Select File Tab

- Download

Expanding the vSAN

Add storage devices	To existing disk groups
Add disk groups	Flash devise for cache Capacity without cache reduces cache to capacity ratio
Add cache and capacity devices to:	I/O controller Host

Add devices to the vSAN

1 Select vSAN cluster

2 Configure tab

3 vSAN Tab

4 Disk Management

5 Disk Group > Add disks

6 Select device to add to
Clear residual data or partition information

! Disk Balance Health Check
Green

vSAN Policies

Define storage needs for VMs

Configured when creating VMs

Provide service levels for VMs

Crated in the VM Storage Policy Wizard

> After enabling rules for vSAN storage

Set Attributes

Availability
   Standard
   Dual Site Mirroring
   None
Failure
   How many failures to what RAID level
   Ex: 2 failures –RAID-1

Advance Policy Rules

> What would the following Advance Rule create →

vSAN Space Efficiency

Reduce space needed for storage

SCSI un-map commands

    Fstrim(8) = Linux Offline Un-maps

    mount –o discard = Linux Inline Un-map

Windows = Default inline NTFS un-maps

Reclaim storage

    Mapped to a nonexistent vSAN object

Methods to improve Space Efficiency

Deduplication / Compression

    Remove duplicate data

    Reduce storage needs with compression

Failure Tolerance Method

    RAID 5

    RAID 6

        Protect data when using less space then RAID 1

vSAN Encryption

Encryption in vSAN

Data in transit
   Dynamically generated symmetric keys
Data at rest encryption
Everything in the datastore is covered
All files are encrypted
   All VMs and their data are encrypted

Encryption performs after processing

Ex: Deduplication

Required Components:

Key Management Server
   Generates and stores keys
vCenter Server System
   Obtains key IDs
   Distributes to ESXi hosts
ESXi hosts

Generates and Stores Key

KMS

Requests Key

vCenter Server

Distributes Keys

ESXi Hosts   ESXi Hosts   ESXi Hosts
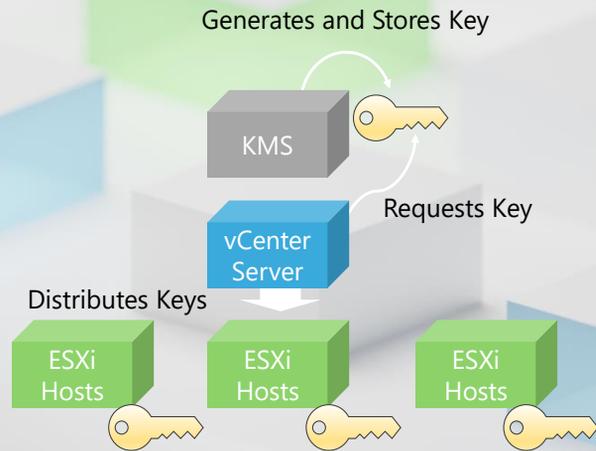
Known Issues vSAN

HA VM failover failure

Disk group removal from host

Migration of VM fails

Solution: Return the disk group

Hosts added to a cluster without a disk group cannot have FSVM deployed on the host.

Hosts need disk groups owned by the vSAN

Solution: Add a disk group to the host

- Assign it to the vSAN

Post recovery VMs lose HA protection

vSAN cluster has hosts with full disks

VMs might lose HA protection

- Due to questions pending

Solution: after recovering from vSAN cluster full scenario

- Reset HA
- Reconfigure HA with new parameters
- Power cycle VMs
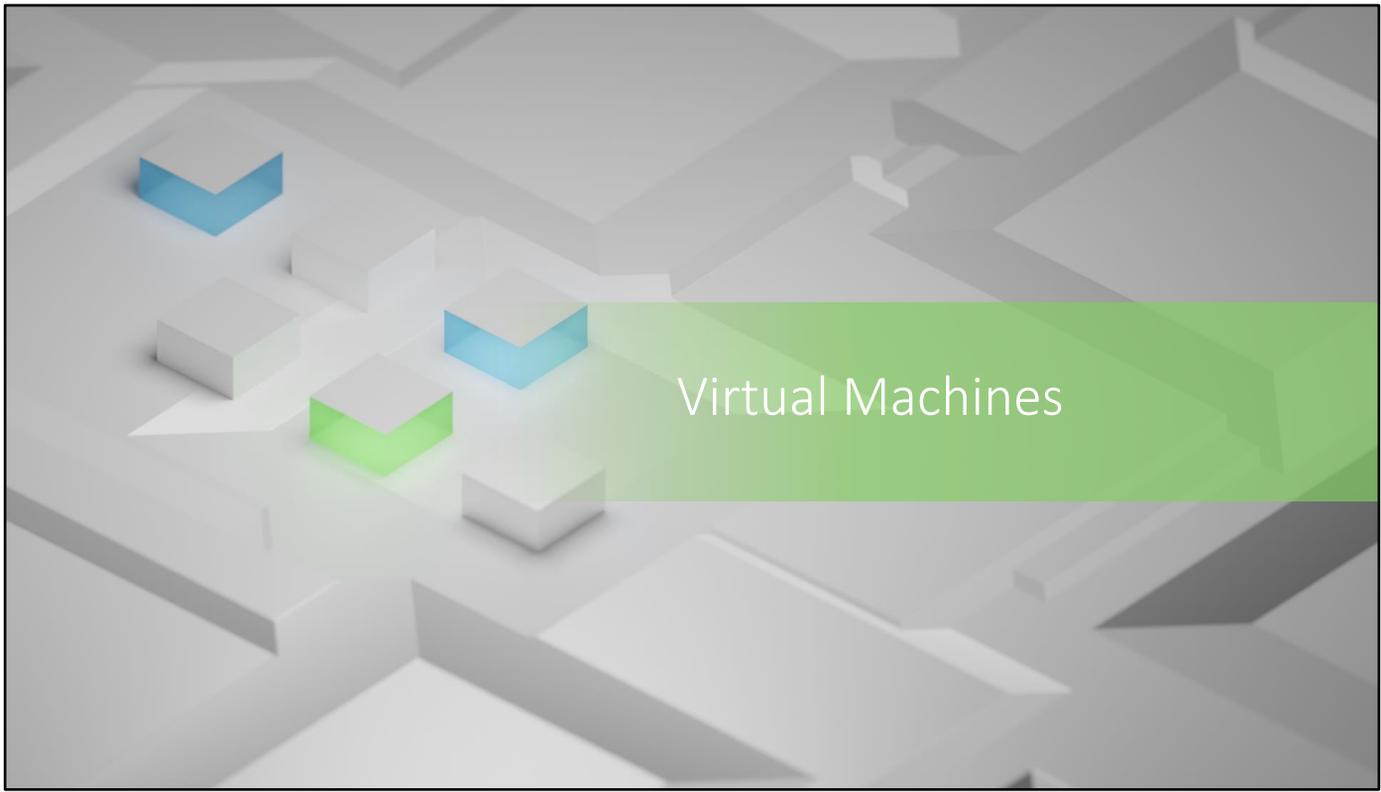
Virtual Machines

What is a VM?

Virtual Machines

Run Operating Systems and Applications

Using software instead of hardware

Can run on the same device

Run on hosts (ESXi)

VMs function separately

Provide application resources

Multiple users

Before Virtual Machines

Historically, devices:

- Ran on one OS
- Dedicated its CPU and Memory to that OS
- Booted replacement OS from BIOS and external drive
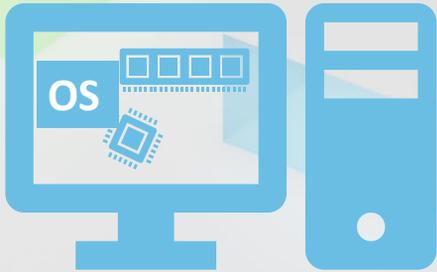
With Virtual Machines

Device can:

Run multiple OSs

CPU and Memory can be dynamically provisioned to support each OS

Rapid Deployments
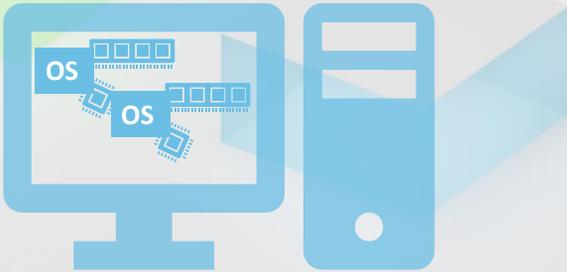
Files

Files determine settings of the VM

    Settings are then configured

        vSphere

        ESXCLI

        Web Services SDK

Files must be stored

Altering these files can lead to errors running your VM

Key Files

File Type	Purpose
.vmx .vmxf	VM Configuration Add. VM Config files
.vmss .vmem	VM suspend file VM paging backup file
.vmdk -flat.vmdk	Virtual Disk Configuration Virtual machine data disk
.nvram	BIOS / EFI Configuration
.vswp	VM Swap Files
.vmsd	Snapshots
.vmsn	Snapshot data File
.log -#.log	Log file Old VM log files
.vmtx	Template for a VM → Replaces .vmx

Guest OS Support

VMware supports guest OSs

An OS that is different then the host OS

During the boot process BIOS or EFI is selected by default

Don't change the firmware after the guest OS is installed

Conclusions
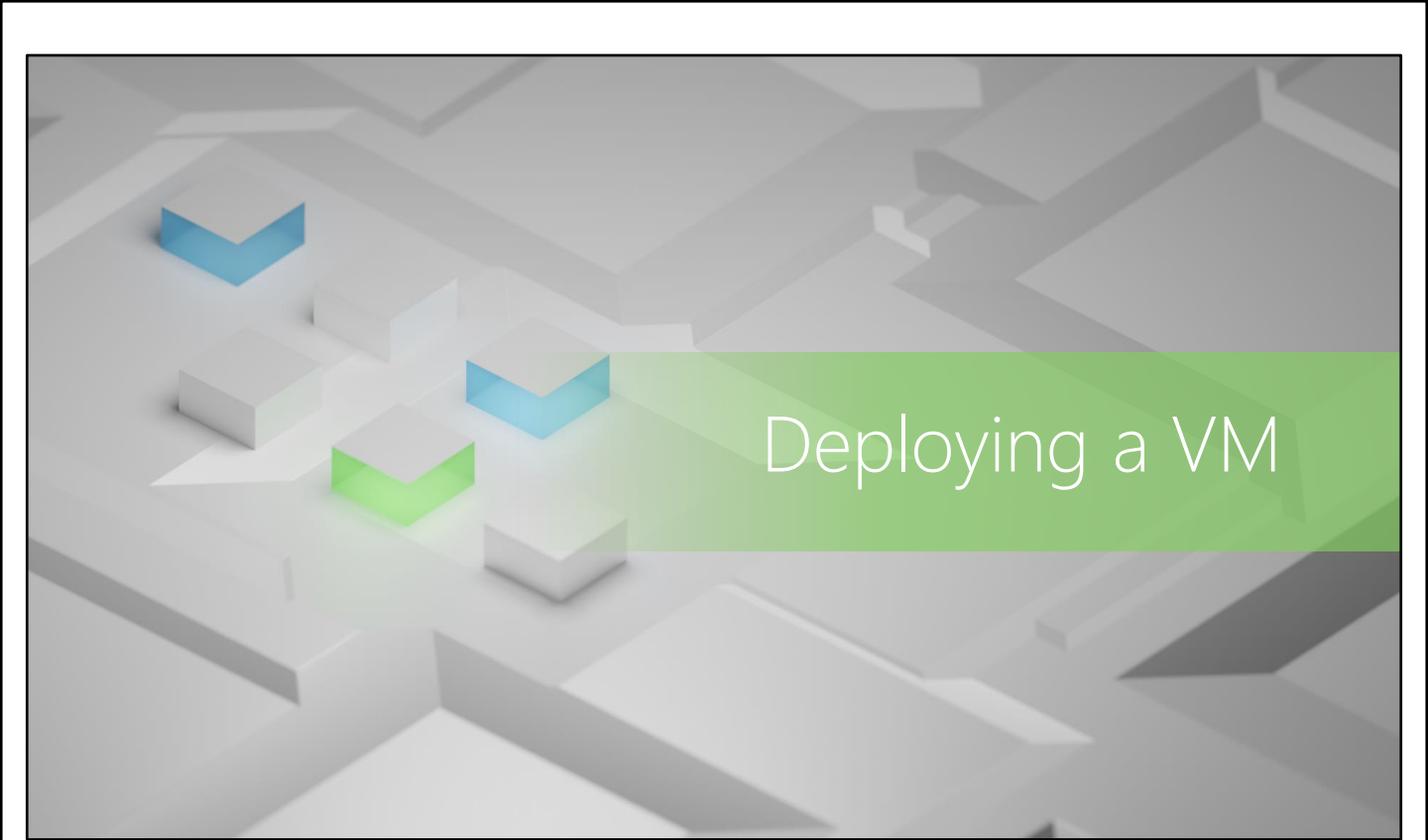
Deploying a VM

Deployment

Various methods of deploying a VM

Create a New VM
- From scratch creation
- Utilize the VM Creation Wizard

Deploy From a Template
- A "golden image"
- Created a VM in the past that meets the needs of many?
- Use that VM as a template to create a new one

Deployment

Various methods of deploying a VM

Cloning a VM

Have a VM that you want a quick exact copy of?

Clone the VM

Instant clone

Clone a template

To a template

To a VM

Templates

A Golden VM

A standard version
Meets the need of users of employees in an environment

VM's are deployed based off the parameters of the template

Alterations can be made, but the template provides a base
Example: Users in a network all need
> Windows 10
> 2.5GB of Memory
> 40 GB of hard disk space

Instead of re-creating this VM from scratch for every user, use the template
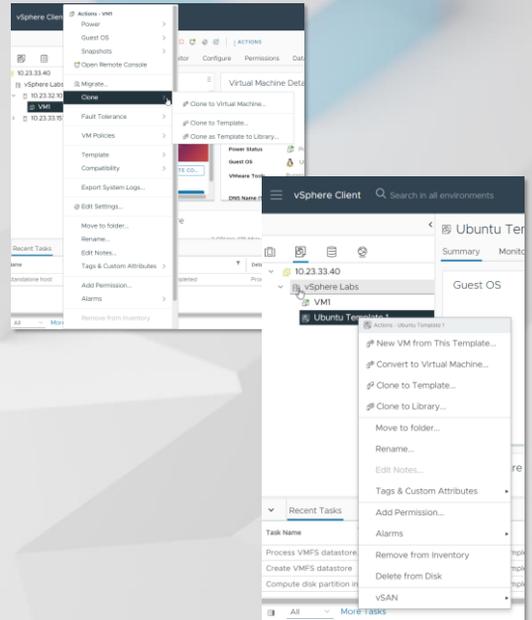
vSphere 8.0 Configuration Limits

Max Virtual CPU's per VM → 768

Max RAM per VM → 24TB

Max SCSI adapters per VM → 4

Max Virtual Disk Size → 62 TB

Max Virtual NICs per VM → 10

Max PMem per VM → 6TB (6128 GB per Machine)

All Configuration Limitations can be found at:
https://configmax.vmware.com/home

Create + Deploying VMs

vSphere used to create and deploy VMs

VM Wizard

    Creates VM + Default Disk

Make a VM

    Navigate to → Hosts and Clusters

    Expand a parent object

        Cluster

        Host

        Pool

    Use **Activities** Drop Down

    Select **New Virtual Machine**
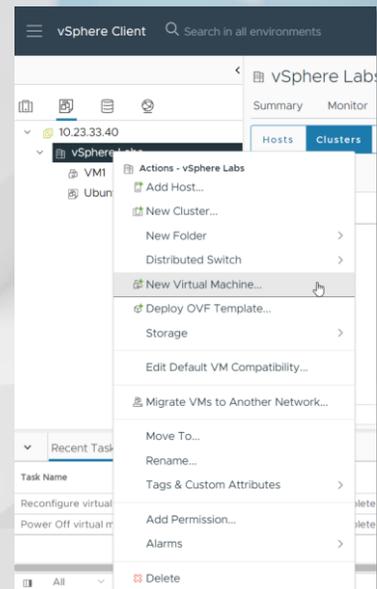
Create + Deploying VMs

Select a Creation Type

Click **Create a New Virtual Machine**
Other options:
- Deploy from a premade template
- Clone a VM
  - To a template
- Clone template on a template
- Convert template to VM

Next

New Virtual Machine

1 Select a creation type	Select a creation type
2 Select a name and folder	How would you like to create a virtual machine?
3 Select a compute resource	
4 Select storage	Create a new virtual machine
5 Select compatibility	Deploy from template
6 Select a guest OS	Clone an existing virtual machine
7 Customize hardware	Clone virtual machine to template
8 Ready to complete	Clone template to template
	Convert template to virtual machine

This option guides you through creating a new virtual machine. You will be able to customize processors, memory, network connections, and storage. You will need to install a guest operating system after creation.

Create + Deploying VMs

Select a name and Folder

    Provide a Name

    Location

    Next

Select compute resource

    Designate where VM will run

    Next

Create + Deploying VMs

Create + Deploying VMs

Select Storage

Standard

PMem > Persistent Memory

Should memory be maintained through a power cycle?

(Optional) Configure Storage Policy

    Examples:

        Large

        Thin

        Stretched

(Optional) Enable Encryption

Storage

Compatibility

ESXi / Workspace Version

Match compatibility selection to the hardware version that is supported
  Select from the dropdown menu
Use the VMware Compatibility Matrix
https://www.vmware.com/resources/compatibility/search.php
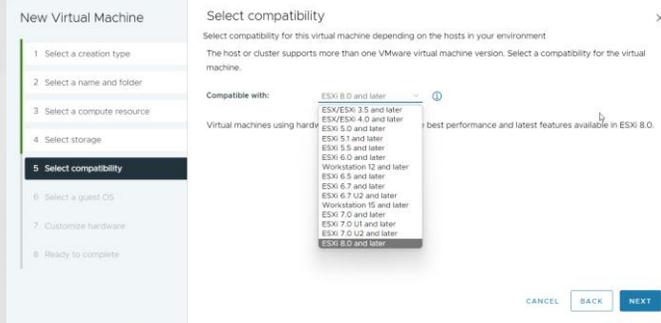
Guest OS

Guest OS Installed on the VM

Wizard will use selection to provide defaults for OS install

Select OS from a dropdown

Family

OS Version
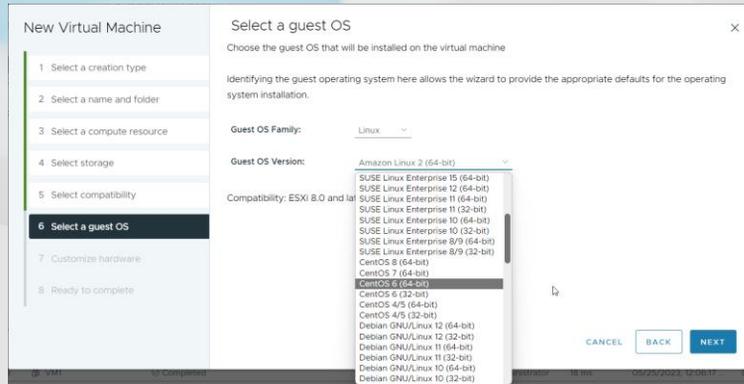
Customize Hardware / Options

Wizard sets default values

You can adjust from a dropdown menu or custom values

Set hardware parameters

Customize Hardware / Options

What can be configured?

Linux Example:

CPU cores

Memory

Hard Disk

SCSI Controller

Network

CD/DVD Drive

Video Card

CPU

Linux Example:

CPU cores
Cores Per socket
Hot plug enable
Reservation
    Min = 0 MHz
    Max = 3593 MHz
Limit
    Min = 0 MHz
    Max = Unlimited
Enable :
    Hardware Virtualization
    Performance Counters
    I/O MMU

CPU Topology	Assigned at power on ⓘ
Reservation	0 MHz ⌄
Limit	Unlimited MHz ⌄
Shares	Normal ⌄ 1000
Hardware virtualization	☐ Expose hardware assisted virtualization to the guest OS
Performance Counters	☐ Enable virtualized CPU performance counters
Scheduling Affinity	_____ ⓘ
I/O MMU	☐ Enabled

CPU Topology (NEW)

Memory

Wizard allows for memory allocation
- Min 256 MB
- Max 6128 GB

Drop downs can edit memory allotted
- Reserve guest memory – Max 21.21 GB
  - Or Reserve all
- Memory Limits
- Shares
  - Low, Normal, High
  - Custom = Min 1 → Max 1,000,000

Memory Hot Plug
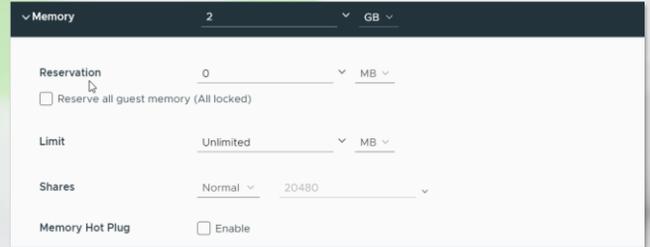
Hard Disk

Size

    Customizable

    (Maximum will be presented)

Storage Policy

    Default

    Encryption

    Large

    Regular

    Etc.

∨ New Hard disk *	16	GB ∨	⋮
Maximum Size	78.34 GB		
VM storage policy	Datastore Default ∨		
Location	Store with the virtual machine ∨		
Disk Provisioning	Thick Provision Lazy Zeroed ∨		
Sharing	Unspecified ∨		
Disk Mode	Dependent ∨		
Virtual Device Node	New SCSI controller ∨	SCSI(0:0) New Hard disk ∨	

Hard Disk

Location of storage
- In the VM
- External Drive

Provisioning
- Thick
  - Eager
  - Lazy
- Thin

New Hard disk *	16	GB ⌄	⋮
Maximum Size	78.34 GB		
VM storage policy	Datastore Default ⌄		
Location	Store with the virtual machine ⌄		
Disk Provisioning	Thick Provision Lazy Zeroed ⌄		
Sharing	Unspecified ⌄		
Disk Mode	Dependent ⌄		
Virtual Device Node	New SCSI controller ⌄	SCSI(0:0) New Hard disk ⌄	

Hard Disk

Sharing
- Unspecified
- No-sharing
- Multi-Writer

Shares

Limit-IOPs

New Hard disk *	16	GB ⌄	⋮

Maximum Size	78.34 GB
VM storage policy	Datastore Default ⌄
Location	Store with the virtual machine ⌄
Disk Provisioning	Thick Provision Lazy Zeroed ⌄
Sharing	Unspecified ⌄
Disk Mode	Dependent ⌄
Virtual Device Node	New SCSI controller ⌄ SCSI(0:0) New Hard disk ⌄

Hard Disk

Disk Mode
- Dependent
- Independent
  - Persistent
  - Disk Configuration remains after power cycle
  - Nonpersistent

Virtual Device Node
- SCSI
- IDE
- SATA

New Hard disk *	16	GB
Maximum Size	228.23 GB	
VM storage policy	Datastore Default	
Location	Store with the virtual machine	
Disk Provisioning	Thick Provision Lazy Zeroed	
Sharing	Unspecified	
Shares	Normal	1000
Limit - IOPs	Unlimited	
Disk Mode	Dependent	
Virtual Device Node	New SCSI controller	SCSI(0:0) New Hard disk

SCSI Controller

SCSI Controller or HBA

Allows small computer system interface device to communicate with the OS

Across a bus

Change Types

Bus Logic Parallel
LSI Logic Parallel
LSI Logic SAS
VMWare Paravirtual

SCSI Bus Sharing

None
Physical
Virtual
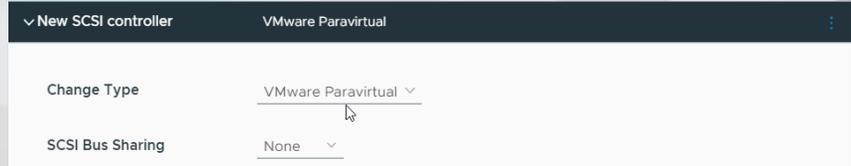
∨ New SCSI controller	VMware Paravirtual	⋮
Change Type	VMware Paravirtual ∨	
SCSI Bus Sharing	None ∨	

Set up the Network

Connect the VM

Will it connect at power on?

Enable

Which adapter type will it use?

Choose from dropdown

VMXNET 3

PCI Passthrough

PVRDMA

MAC address

Static Or automatic
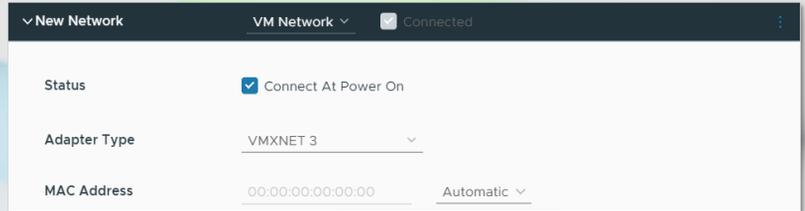
New CD/DVD Drive

Where will the .iso be downloaded from

- Client Device
- Datastore ISO
    - Browse data store for .iso file
- Host Device
- Content Library

Should the device connect at power on?

- Enable

Select a device node

- New SATA Controller

- IDE 0 / 1
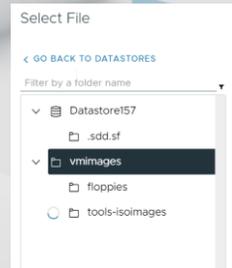
Video Card

How much of the VM Memory will be allocated for video?

1 Start with a display count

2 Set memory dedicated for video

3 Enable 3D support

This requires allocating memory for 3D memory

∨ Video card * ⚠   Specify custom settings ∨

Number of displays   1 ∨

Total video memory   256 _____ ⚠ MB

Total video memory must be between 1.171875 MB and 256 MB.

3D Graphics   ☐ Enable 3D Support

Review Your Awesome VM

New Virtual Machine

1. Select a creation type
2. Select a name and folder
3. Select a compute resource
4. Select storage
5. Select compatibility
6. Select a guest OS
7. Customize hardware
8. **Ready to complete**

Ready to complete

Click Finish to start creation.

Virtual machine name	New Virtual Machine
Folder	vSphere Labs
Host	10.23.33.157
Datastore	Datastore157
Compatibility	ESXi 8.0 and later (VM version 20)
Guest OS name	Amazon Linux 2 (64-bit)
Virtualization Based Security	Disabled
CPUs	2
Memory	2 GB
NICs	1
NIC 1 network	VM Network
NIC 1 type	VMXNET 3
SCSI controller 1	VMware Paravirtual

∨ New hard disk 1

CANCEL   BACK   FINISH

Check your Results

Press the play button in vSphere

Launch the web console

Verify that your OS boots

Go through your OSs boot process
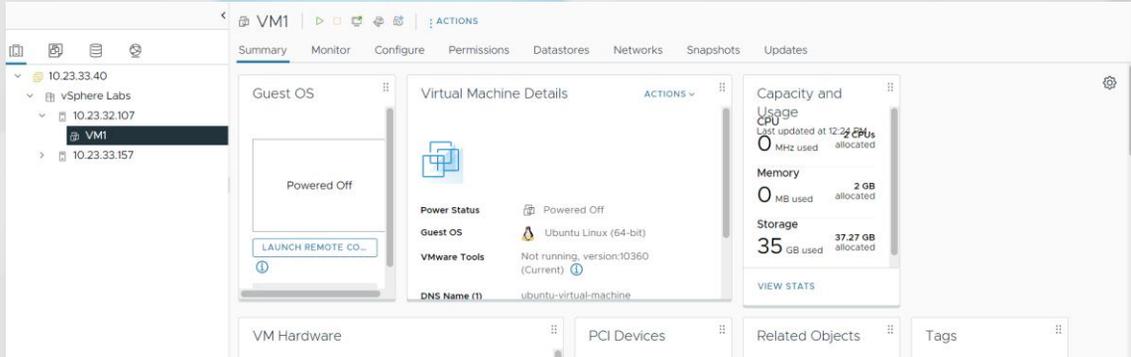
Check your Results

Press the play button in vSphere

Launch the web console

Verify that your OS boots

Go through your OSs boot process
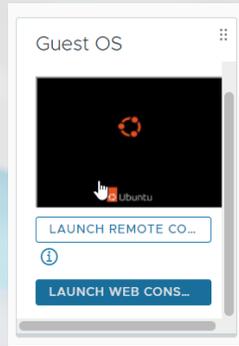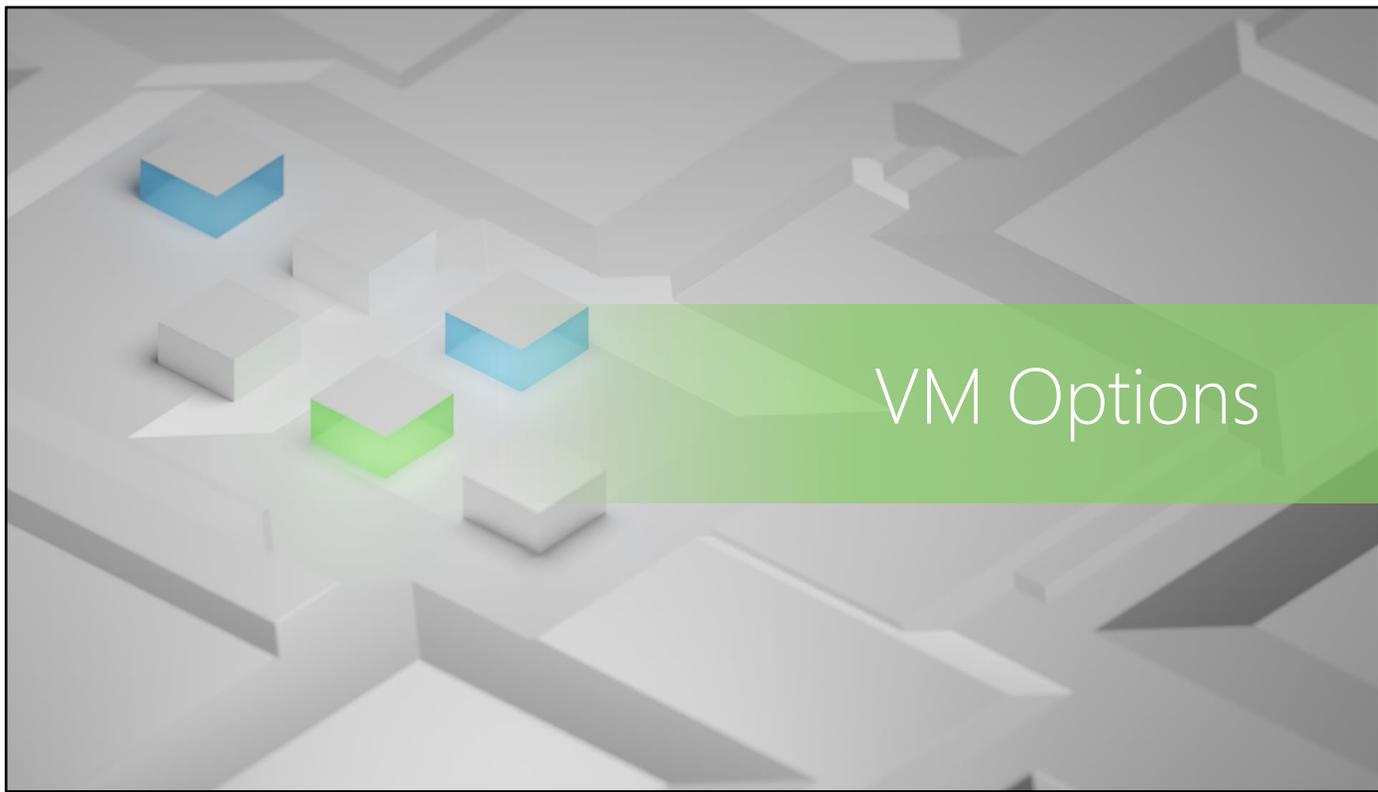
VM Options

Options

Allow user to fine tune the VM

Can be adjusted before and after VM creation

Affects how the VM interacts with its environment

ESXi hosts
Encryption
Power management
Security
Boot Options
NPIV
Datacenters
Clusters
Resource Pools
Etc.
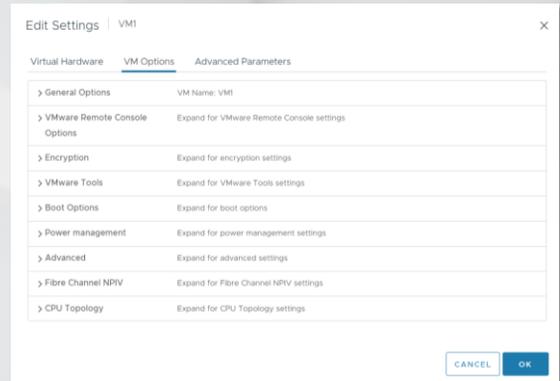
Key Options

General

Name

Location of Files

Location of VM

Encryption Options

Enable or disable

vCenter Server must be trusted

Needs Key Management Server

Encryption for vMotion

Disabled

Opportunistic

Required

Power Management

Manage power usage

Response to Guest OS being put on standby

Suspend

Leave On

Wake on LAN for VM traffic

Select an adapter

VMware Tools

Power Controls

Shut Down vs Power off

Suspend vs Suspend guest

Restart Guest vs Reset

Upgrade VMware Tools

Run scripts

When?

General Options

General Options

VM Name	VM1
VM Config File	[DS107] VM1/VM1.vmx
VM Working Location	[DS107] VM1/
Guest OS Family	Linux
Guest OS Version	Ubuntu Linux (64-bit)

Grey?!

Key Options

General

Name

Location of Files

Location of VM

Encryption Options

Enable or disable

  vCenter Server must be trusted

  Needs Key Management Server

Encryption for vMotion

  Disabled

  Opportunistic

  Required

Power Management

Manage power usage

  Response to Guest OS being put on standby

  Suspend

  Leave On

  Wake on LAN for VM traffic

  Select an adapter

VMware Tools

Power Controls

  Shut Down vs Power off

  Suspend vs Suspend guest

  Restart Guest vs Reset

Upgrade VMware Tools

Run scripts

  When?

Encryption Options

Encryption

Encrypt VM	Datastore Default ⌄
Encrypted vMotion	Opportunistic ⌄ ⓘ
Encrypted FT	Opportunistic ⌄ ⓘ

Disabled
Do not turn on encrypted FT logging.

Opportunistic
Turn on encryption only if both sides are capable, FT VM is allow to move to older version of host that don't support encrypted FT logging.

Required
Choose hosts for FT primary/secondary such that both hosts support encrypted FT logging.

Disabled
Do not use encrypted vMotion, even if available.

Opportunistic
Use encrypted vMotion if source and destination hosts support it, fall back to unencrypted vMotion otherwise. This is the default option.

Required
Allow only encrypted vMotion. If the source or destination host does not support vMotion encryption, do not allow the vMotion to occur.

Key Options

General

Name

Location of Files

Location of VM

Encryption Options

Enable or disable

vCenter Server must be trusted

Needs Key Management Server

Encryption for vMotion

Disabled

Opportunistic

Required

Power Management

Manage power usage

Response to Guest OS being put on standby

Suspend

Leave On

Wake on LAN for VM traffic

Select an adapter

VMware Tools

Power Controls

Shut Down vs Power off

Suspend vs Suspend guest

Restart Guest vs Reset

Upgrade VMware Tools

Run scripts

When?

Power Management

Old

New

Key Options

General

Name

Location of Files

Location of VM

Encryption Options

Enable or disable

vCenter Server must be trusted

Needs Key Management Server

Encryption for vMotion

Disabled

Opportunistic

Required

Power Management

Manage power usage

Response to Guest OS being put on standby

Suspend

Leave On

Wake on LAN for VM traffic

Select an adapter

VMware Tools

Power Controls

Shut Down vs Power off

Suspend vs Suspend guest

Restart Guest vs Reset

Upgrade VMware Tools

Run scripts

When?

VMware Tools

Key Options (Cont.)

Virtualization Based Security (VBS)

Additional security for VM

Latest Windows OS versions

Requires EFI

Can render guest OS unbootable!

Enables IOMMU, hardware virtualization, EFI, and Secure boot on reboot

Boot Options

Firmware type

EFI required if using VBS

BIOS

Boot Delay time

100 millisecond increments

Force EFI setup

Directed to EFI screen

Failed Boot Recovery

Set time to retry

Fibre Channel NPIV

Assign virtual WWN

Normally assigned by:

Host

vCenter Server

LUN access

NPIV

Disable or enable

Generate or Remove WWN

Key Options (Cont.)

Virtualization Based Security (VBS)

Additional security for VM

Latest Windows OS versions

Requires EFI

Can render guest OS unbootable!

Enables IOMMU, hardware virtualization, EFI, and Secure boot on reboot

Boot Options

Firmware type

   EFI required if using VBS

   BIOS

Boot Delay time

   100 millisecond increments

Force EFI setup

   Directed to EFI screen

Failed Boot Recovery

   Set time to retry

Fibre Channel NPIV

Assign virtual WWN

   Normally assigned by:

      Host

      vCenter Server

LUN access

NPIV

   Disable or enable

Generate or Remove WWN

Boot Options

Secure Boot

What is it?

Makes sure that hardware only boots using pre-approved software

Trusted by the manufacturer

VM's can enable / disable secure boot

UEFI Secure boot → All boot software is signed

What do you need for UEFI secure boot?

EFI firmware

Virtual Hardware Version 13 or later

OS support for UEFI Secure Boot

Enable / Disable Secure Boot

1	2	3	4	5	6	7
Navigate to the VM	Select Edit Settings	Select VM Options → Expand Boot Options	Verify firmware is EFI	Check Secure Boot to enable / Un-Check Secure boot to disable	Boot delay / Force EFI/ FBR →OK	Now if an invalid or missing signature is detected, the boot process stops

Boot Options

Firmware	EFI (recommended) ˅
Secure Boot	☐ Enabled
Boot Delay	When powering on or resetting, delay boot order by
	0 milliseconds
Force EFI setup	☐ During the next boot, force entry into the EFI setup screen
Failed Boot Recovery	☐ If the VM fails to find boot device, automatically retry after
	10 seconds

Key Options (Cont.)

Virtualization Based Security (VBS)

Additional security for VM

Latest Windows OS versions

Requires EFI

Can render guest OS unbootable!

Enables IOMMU, hardware virtualization, EFI, and Secure boot on reboot

Boot Options

Firmware type

EFI required if using VBS

BIOS

Boot Delay time

100 millisecond increments

Force EFI setup

Directed to EFI screen

Failed Boot Recovery

Set time to retry

Fibre Channel NPIV

Assign virtual WWN

Normally assigned by:

Host

vCenter Server

LUN access

NPIV

Disable or enable

Generate or Remove WWN

NPIV

Fibre Channel NPIV

Fibre Channel Virtual WWNs Virtual machines running on hosts with Fibre Channel hardware that supports NPIV can be assigned virtual WWNs for advanced features. These WWNs are normally assigned by the host or by vCenter Server.

☑ Temporarily disable NPIV for this virtual machine

No WWNs are currently assigned.

◉ Leave unchanged
◯ Generate new WWNs
◯ Remove WWN assignment

Number of WWNNs: 1 ⌄   Number of WWPNs: 1 ⌄

```
0 Node WWN:
0 Port WWN:
```
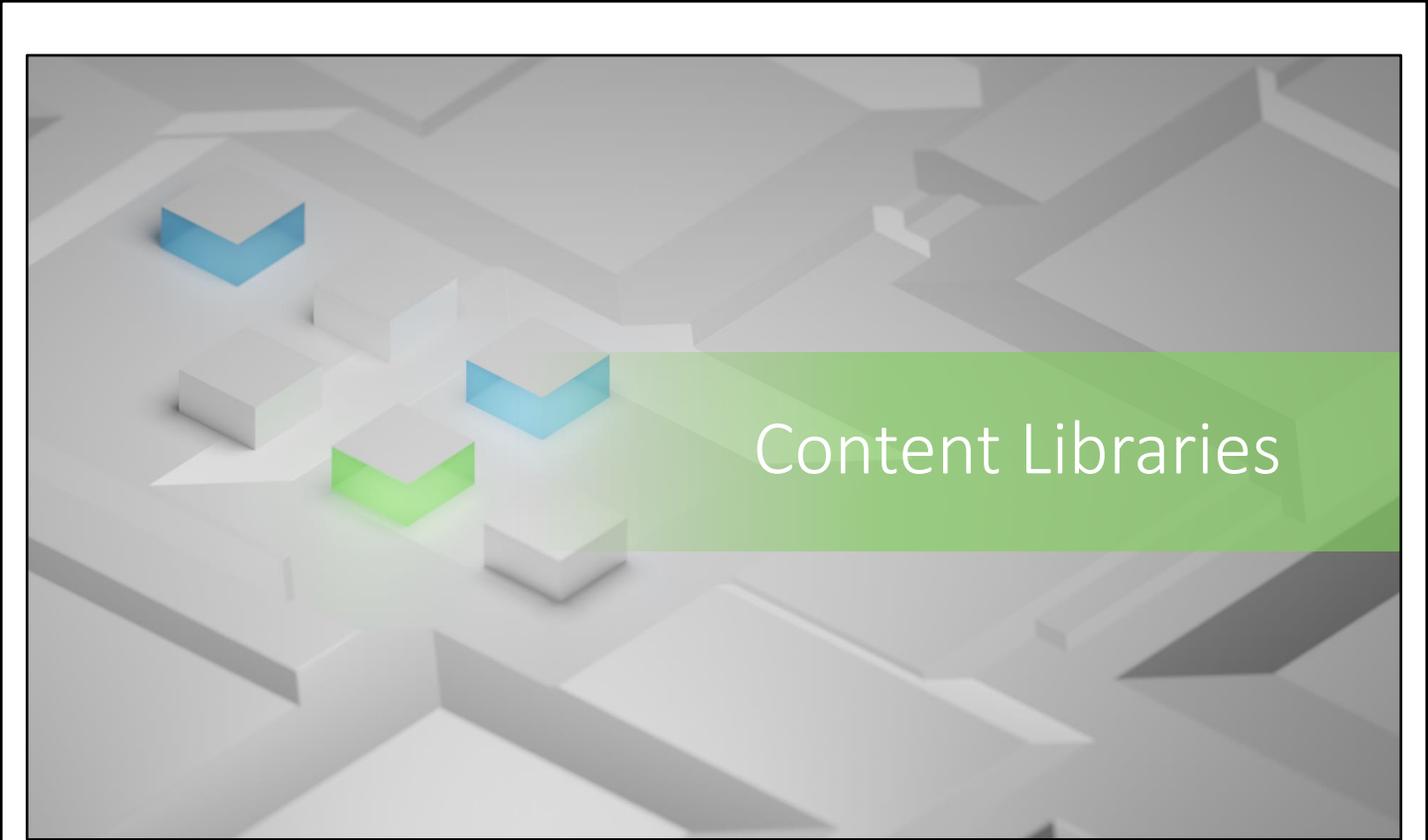
Content Libraries

Content Libraries

What are Content Libraries?

Containers
Store and manage content
Pull up templates, files, iso images, etc.
Share data across vCenter Server

Legacy versions

Only support OVF templates
Now VM templates are supported

Managed by one vCenter Server Instance

Distributed to many

Library Types

Local
Subscribed

vAPP templates

ISO images

VM's

Text Files

Create a Library

1 Menu	2 Content Library	3 Click (+) → New content library	4 Wizard opens	5 Set name	6 Set Server instance	7 Next	8 Select type of library
							Local Publish Authenticate Subscribed

New Content Library

1 Name and location
2 Configure content library
3 Add storage
4 Ready to complete

Name and location

Specify content library name and location.

Name: _____

Notes: _____

vCenter Server: 10.23.33.40 ∨

CANCEL   NEXT

Library Type

Local Content

Only local vCenter Server instance can access

Enable publishing

- Accessible by other vCenter Servers

Enable authentication

- Requires credentials to access content

Subscribed Content

Comes from a published library

Sync with published library

- Up to date content

Subscribing to a content library

What you need:

Subscription URL to the Published Library

Enable authentication (Optional)

Select Download Method

- Immediately
  - Download local copy
- When needed
  - Only downloads metadata for items
  - Saves storage space

Accept SSL certificate thumbprint

Datastore

Add Storage Page

Select datastore
   This is where the library and its content will be located

2 Next

3 Ready to Complete Review

4 Finish

Conclusions
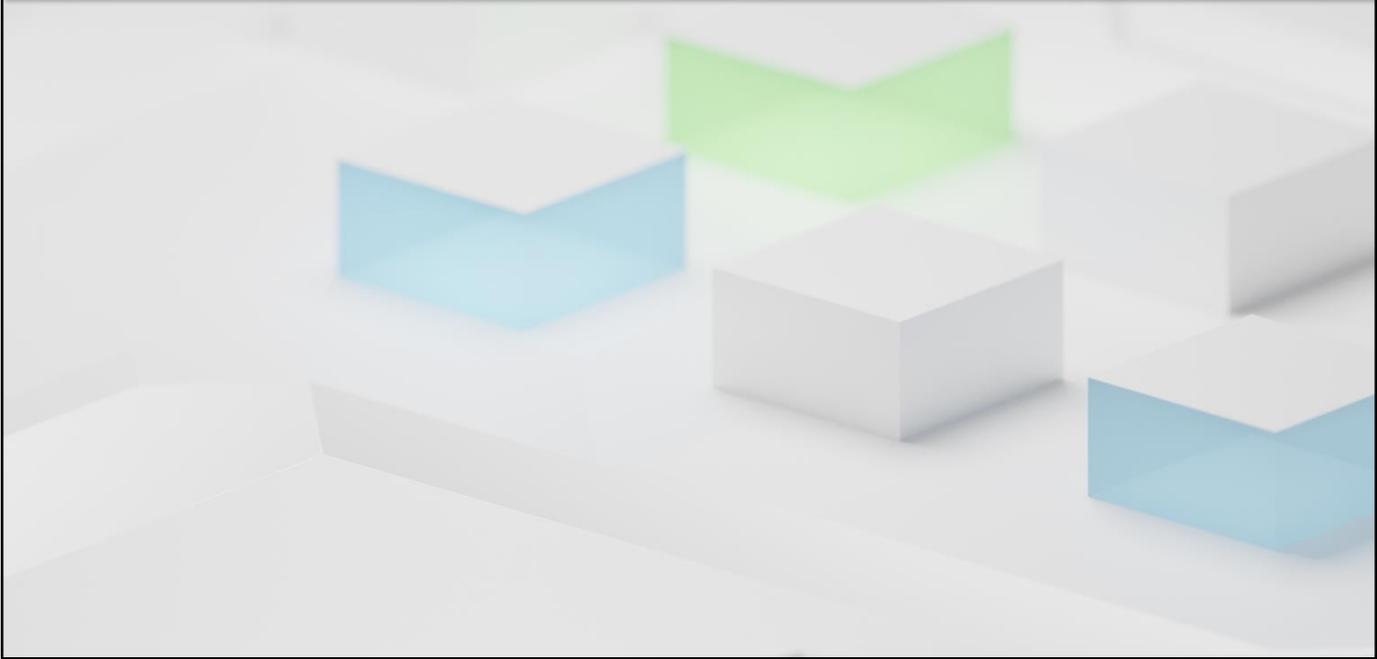
Solutions Manager

Solutions Manager Tabs

Summary

Product name

Descriptions

Vendor websites

Configuration

GUI access

Monitor

Tasks

Events

Configure

Agencies

Issues for selected

Trigger time

VM

Which VMs and Apps utilize the solution

Summary Tab

Solutions Manager Tabs

Summary	Monitor	Configure	VM
Product name	Tasks	Agencies	Which VMs and Apps utilize the solution
Descriptions	Events	Issues for selected	
Vendor websites		Trigger time	
Configuration			
GUI access			

Monitor

Solutions Manager Tabs

Summary

Product name

Descriptions

Vendor websites

Configuration

GUI access

Monitor

Tasks

Events

Configure

Agencies

Issues for selected

Trigger time

VM

Which VMs and Apps utilize the solution

Configure

Solutions Manager Tabs

Summary
Product name

Descriptions

Vendor websites

Configuration

GUI access

Monitor
Tasks

Events

Configure
Agencies

Issues for selected

Trigger time

VM
Which VMs and Apps utilize the solution

Snapshots

VMware Snapshot

Copy of VMDK File

Specific point in time
Not a backup but a changelog

Creates a placeholder disk

Example: **virtual_machine-00000x-delta.vmdk**
Stores data changes since snapshot was created

Helps restore VM

Help identically recreate the VM based on a point in time
After incident or based on network needs

Take a Snapshot

Right click VM

    Snapshots

        Take

            Name the snapshot

            Enable snapshot of VM Memory

        Manage

        Revert

        Consolidate

        Delete
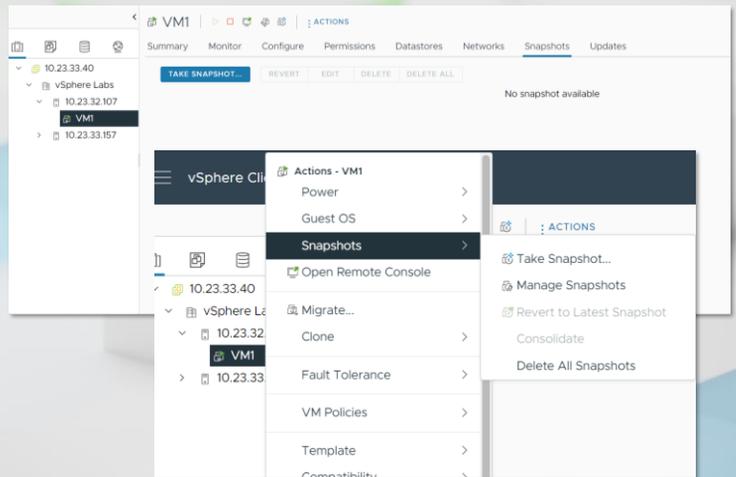
SR-IOV

SR-IOV

Single Root input / Output virtualization
- Isolates PCI express resources
- Single PCI express can be shared in a virtual environment

VMs utilize SR-IOV
- Bypasses VMkernal
- Removes CPU redundancies
  - Traffic is not handled by vSwitch

What is supported
- Physical hosts
- Physical NICs
- PF driver in ESXi
- Guest OS
- VF drive in the guest OS

Check VMware Compatibility Guide

With SR-IOV

| VM | VM |

VMM

ESXi

PCI / IOMMU

VF Adapter w/SR-IOV

Without SR-IOV

| VM | VM |

vSwitch

ESXi

PCI
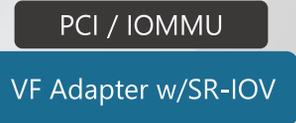
Adapter without /SR-IOV
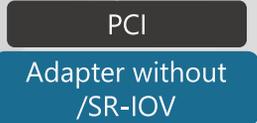
SR-IOV Path

Guest OS requests change on VF → VF forwards request to PF → PF driver checks request → vSwitch verifies request
- Examines request against policy

→ PF Driver configures VF is settings are compliant

Enable SR-IOV

1 vSphere Client

2 Select host

3 Configure → Networking → Physical Adapters

4 Select adapter

5 Select adapter settings

Enable SR-IOV

1 vSphere Client

2 Select host

3 Configure → Networking → Physical Adapters

4 Select adapter

5 Select adapter settings

6 Enable SR-IOV — From drop down

7 Set Number of VFs

8 OK

9 Restart

Enable SR-IOV

Associate a VM with a VF

Allows VM and physical NIC
to exchange data

Must be enabled on host NIC

Process Start:

Select a VM
Power it down
Select Edit Settings

C9800	▶ ■				ACTIONS ⌄
Summary	Monitor	Configure	Per		Actions - C9800

Powered Off

Guest OS: Ot
Li
Compatibility: ES
(V
VMware Tools: No
ve
(G
M

Launch Web Console
Launch Remote Console

DNS Name:
IP Addresses:
Host: 19

VM Hardware

- Power ▶
- Guest OS ▶
- Snapshots ▶
- Open Remote Console
- Migrate...
- Clone ▶
- Fault Tolerance ▶
- VM Policies ▶
- Template ▶
- Compatibility ▶
- Export System Logs...
- Edit Settings...
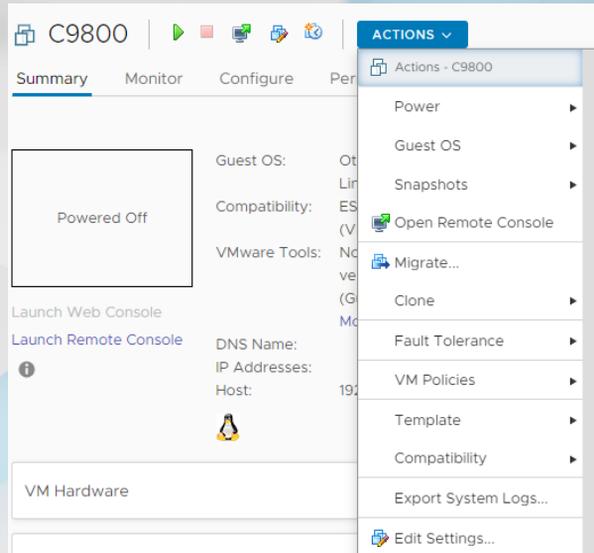
Assign a VF

Select virtual hardware

Open the add new device drop down

Select network adapter

Expand the new network

Connect VM to port group

Select the SR-IOV passthrough adapter type

Physical function drop down

Enable Guest OS MTU change

Select Reserve all guest memory

OK

Power on VM
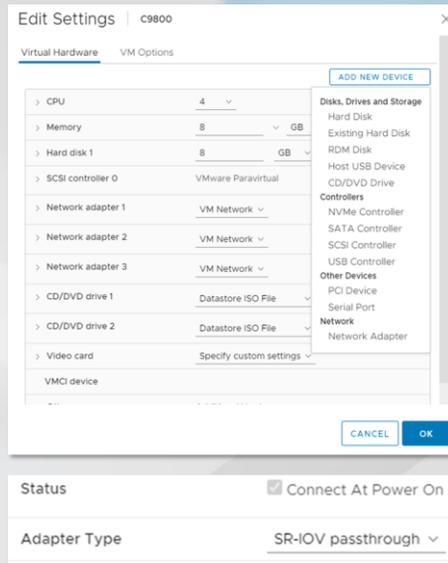
VF options

VM's network features can be altered

Features associated with adapter

What can be adjusted:

MTU size

Security Policy

Set policy for traffic from a VM with a changed MAC address

Global Promiscuous Mode

VLAN tagging mode

VF Modes

Mixed

Physical adapter can perform virtual functions to VMs

Directly handles non SR-IOV VMs

SR-IOV Only

Physical adapter can perform virtual functions to VMs

Cannot handle traffic from non SR-IOV VMs

Non SR-IOV mode

Only handles non SR-IOV VM

No traffic to VF supported VMs

Common Known Issues

Check your VMware tools!

Are your tools not installed?

Are they out of date?

VM Networking devices are not supported

Check compatibility list

A degraded network device can result in downtime

Resource Management / Memory Limits

Consuming to many resources can impact:

- Device Health

- Network Performance

- Ability for end users / remote users to connect

Logging limitations

Logs can be resource intensive

Log files can be used to attack the network

- Don't make yourself vulnerable to DDOS attacks

Only log what you need
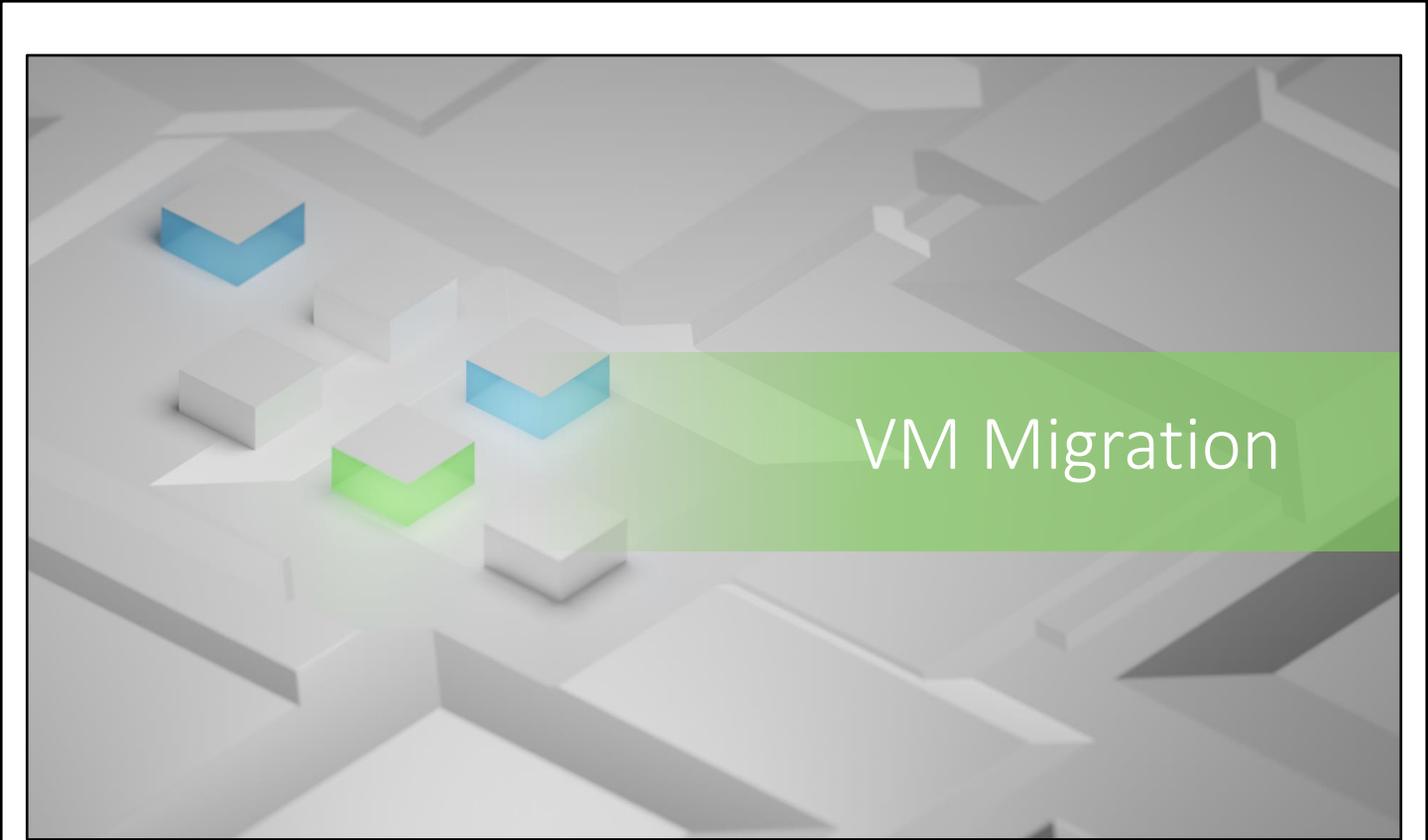
VM Migration

Migrate VMs

Oh no!

Your system has encountered an incident and future downtime is expected

Solution?

Live Migration

vMotion

Zero downtime

Live migration

Takes workload form one server to another

Migrate between:

vSwitches

Clusters

Clouds

Migrate VMs

vMotion Enabled Network

ESXi_01

ESXi_02

VM

VM
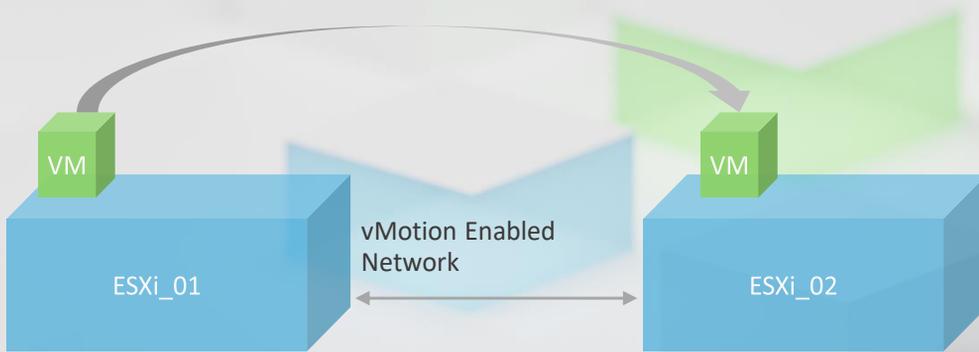
Requires vMotion Enabled Network

Initiated from vCenter Server GUI

DRS → Balance workloads

vMotion Storage
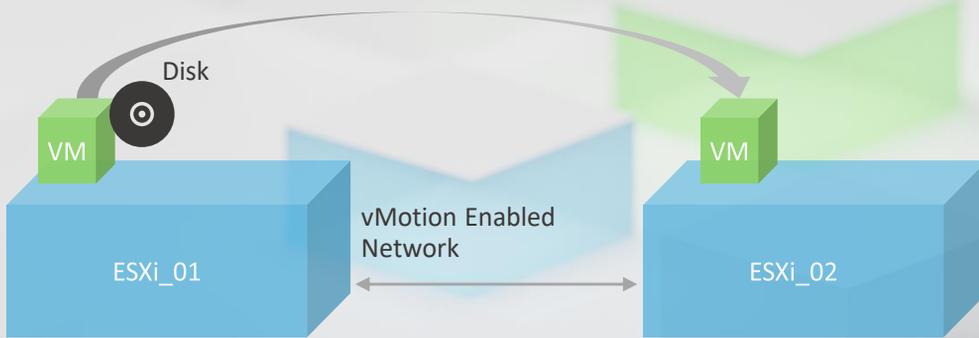
Migrate a VM and disk from Data Store to Data Store(s)

While VM is still running

Demo Configuration of vMotion
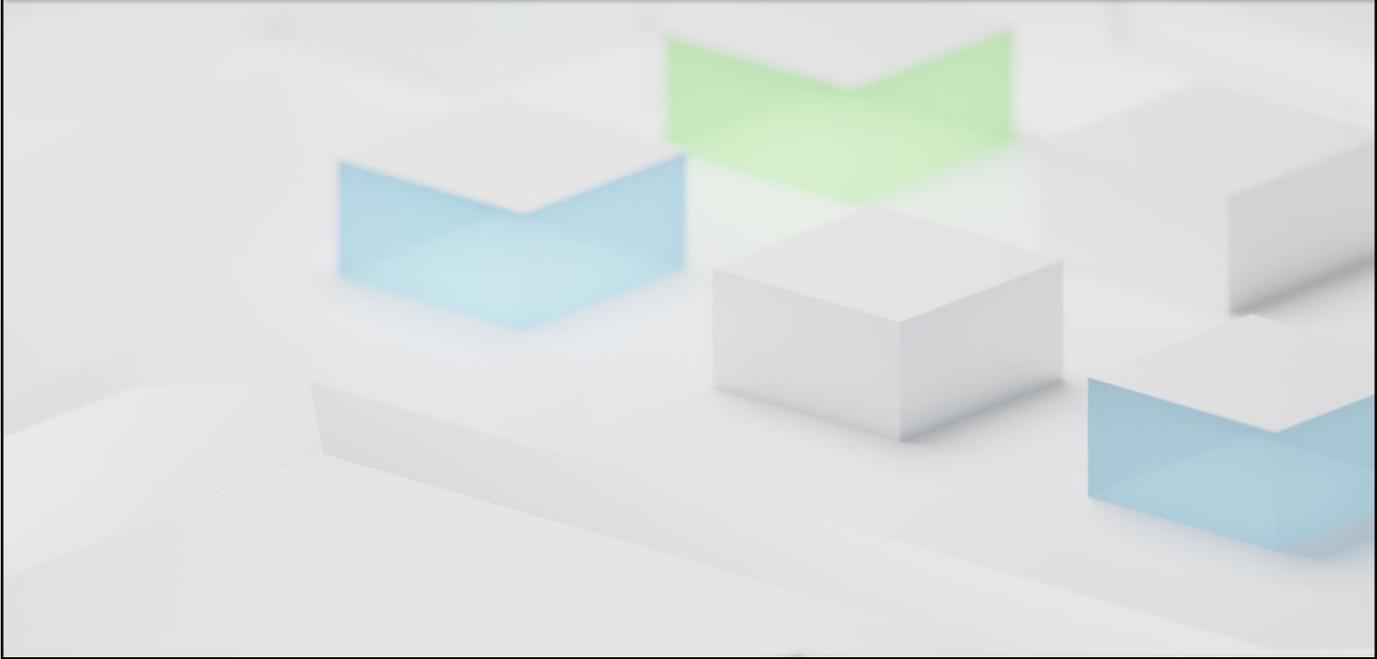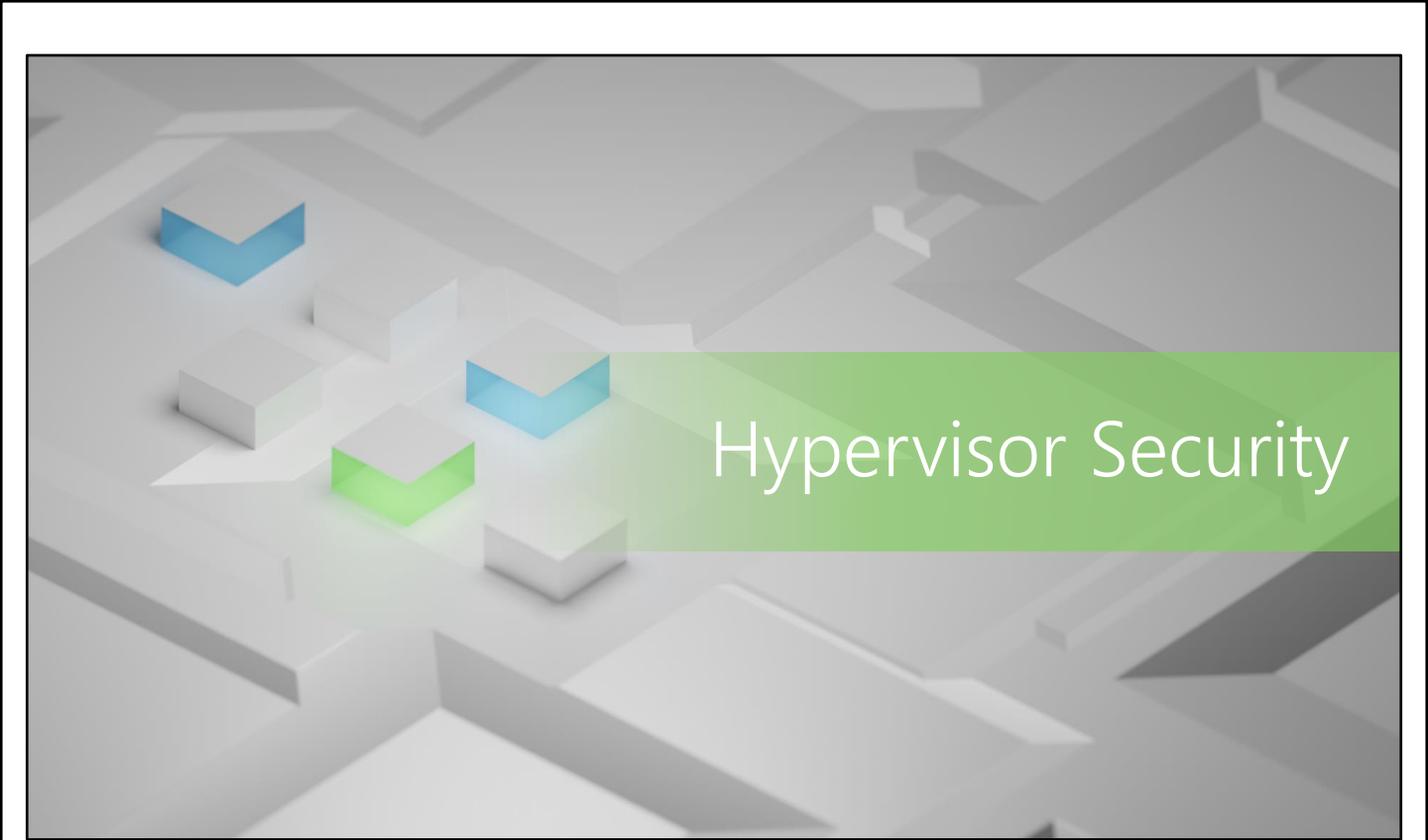
Hypervisor Security

ESXi Hypervisor Security

Limit ESXi access

Shell and SSH disabled by default

Set Timeouts if you enable

Limit permissions

Principle of least privilege

Automate Host Management for consistency

Auto Deploy, Host Profiles

Limit Open ESXi Firewall ports

vSphere client, ESXCLI, PowerCLI

Lockdown Mode

Hosts can only be accessed through vCenter

Strict
DCUI is deactivate

Normal
Only admin accounts have access to DCUI (or specifically assigned)

Service	Normal Mode	Normal Lockdown Mode	Strict Lockdown Mode
vSphere Web Services API	All users, based on permissions	vCenter (vpxuser) Exception Users, based on permissions vCloud Director (vslauser, if available)	vCenter (vpxuser) Exception Users, based on permissions vCloud Director (vslauser, if available)
CIM Providers	Users with administrator privileges on the host	vCenter (vpxuser) Exception Users, based on permissions vCloud Director (vslauser, if available)	vCenter (vpxuser) Exception Users, based on permissions vCloud Director (vslauser, if available)

Service	Normal Mode	Normal Lockdown Mode	Strict Lockdown Mode
Direct Console UI (DCUI)	Users with administrator privileges on the host, and users in the DCUI.Access advanced system setting	Users defined in the DCUI.Access advanced system setting Exception users with administrator privileges on the host	DCUI service is stopped
CIM Providers	Users with administrator privileges on the host	Users defined in the DCUI.Access advanced option Exception users with administrator privileges on the host	Users defined in the DCUI.Access advanced system setting Exception users with administrator privileges on the host

Other ESXi Security Considerations

VIB package integrity

    Acceptance levels

Certificate Management

    Third-party or enterprise certificate authority

Smart Card Authentication

Account lockout

    Default 5 failed attempts, 15 min. timeout

Conclusions

Hypervisor Security

Lockdown mode

Security concerns
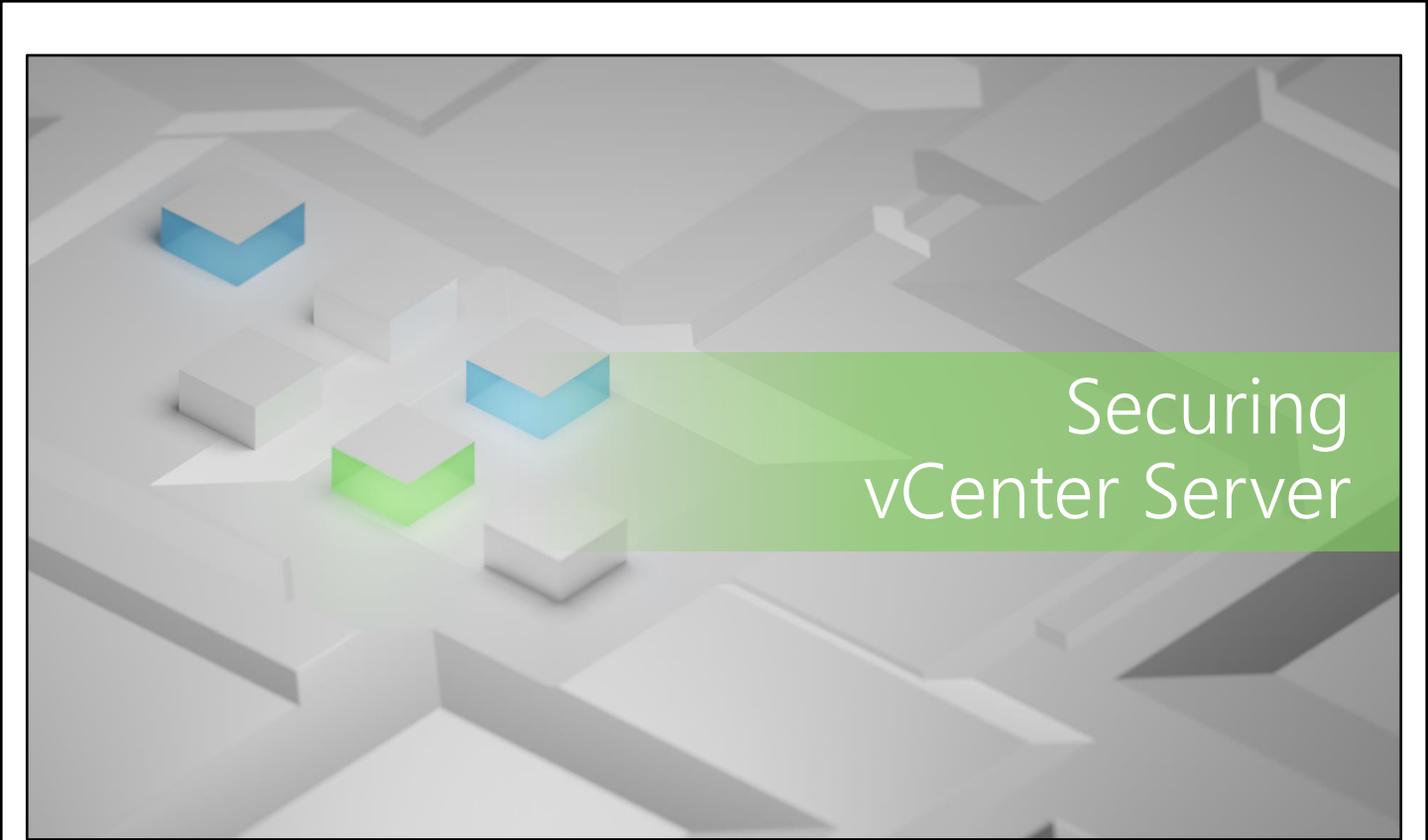
Securing vCenter Server

Default Security Measures

Single Sign-on

Encrypted communication

vCenter communication to vSphere components

Exceptions: DNS, Mail (configuration based), Port 80 (listening)

Hardening vCenter Server Systems

The underlying physical host

Security patches

vSphere certificates

- VMCA by default

Single Sign-on

- Domain (administrator@vsphere.local)
- External identity provider

Role based access control

Setup NTP or PTP

Certificate infrastructure will fail with skew

Important for incident tracking

Logging

Conclusions

Default security measures

Hardening vCenter Server

Securing VMs

General Security Measures for a VM

- Ensure host and vCenter security practices
- Ensure physical security of the host
  - Many of the VM escape vulnerabilities require physical access
- Keep guest OS patched
  - Anti: spyware , malware applications
  - Guest OS best practices and hardening guides
- Minimize VM console use

The Unnecessary

◆ Unused services in the OS
   Ex: file server

◆ Unused physical devices
   Ex: Floppy drives

◆ Unused functionality
   Ex: Display features

Securing your Virtual Network

- Isolate Network Traffic
- Firewalls to close ports
- Enact Network Security Policies
- VM specific network traffic
- VLANs

Securing Connections to Storage

- Isolate Network Traffic
- Firewalls to close ports
- Enact Network Security Policies
- VM specific network traffic
- VLANs

Conclusions

General security for VMs

Unnecessary

Virtual network connection

Storage connection

Single-sign On

vSphere SSO

Performs user authentication

Users must provide credentials to access vCenter Server
Solution users vs. Other Users
VMCA certificate vs. SAML tokens

Administrators

Add identity sources
Set default Identity Source
Manage users in the SSO Domain

vSphere SSO

Adding an SSO User

Addition of internal vsphere.local domain user

How? → Login as a domain admin → Home Page ➔ Administration → Find SSO tab

Select Users and Groups

Users Tab → Set the domain ➔ Add User → Set Credentials (Username can't be changed) → Click Add
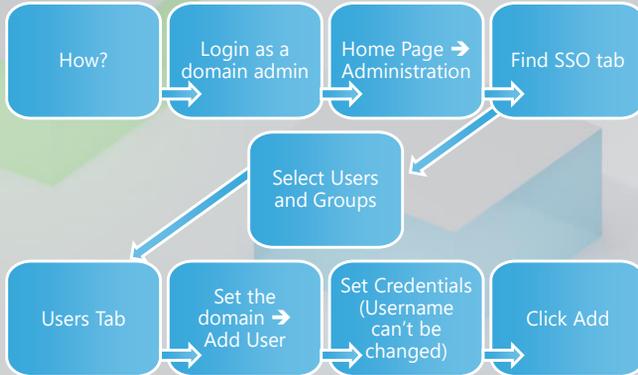
vSphere SSO

Adding an SSO Identity Source

AD over LDAP   Native AD   OpenLDAP

How? → Login as a domain admin → Home Page ➔ Administration → Find SSO tab

Select Configuration → Select the Identity Provider tab
Select Identity Sources
Add → Select the Identity source mode
Set the settings for the source
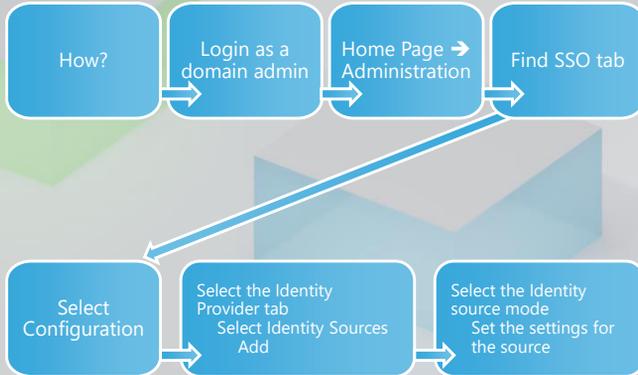
SSO Security Best Practices

SSO can help protect your environment

How can SSO be secured?

NTP

SSO Security Best Practices

SSO can help protect your environment

Forces users to authenticate before manipulating the network

How can SSO be secured?

Keep Password Expiration in mind

- Default lifetime is 90 days
- If a password expires you can't log in

Ensure passwords are changed often

NTP

SSO utilizes time services (NTP)

- Ensure all systems are referencing the same NTP source

Desynchronized time = Inability for SSO and vSphere certificates to be validated

- Intruder Alert!
  - NTP can help track when someone has wrongfully gained network access
  - NTP misconfigurations make legal action, auditing, and investigations difficult

SSO Security Best Practices

SSO

Authentication
Adding a user
Identity sources
Best practices

Certificate
Management

Certificates

Certificates are used to:	CA – Certificate Authority	Certificate Management	VMCA

Encrypt communication between hosts
 	
Sign tokens
 	
Authentication
	Internal – VMware Certificate Authority
	    Preinstalled
	    Default configuration
	External
	    Ex: GoDaddy
		vSphere Client
		
		Certificate Manager Utility
		
		CLIs
		    Dir-cli
		    Certool
		    Vecs-cli
		
		Web-Client
			VMCA default Certificates
			
			Provides all certificates
			
			Lower Overhead
			
			VMCA default Certificates with External SSL Certificates (Hybrid)
			    Replace vCenter Server SSL certificates
			    More Secure

Certificates

Manage Certificates in the vSphere Client

Trusted Root Certificates and SSL Certificate review

Certificate replacement and renewal

Generate and replace CSRs

Review Details of a Certificate

Certificates

Hosts are provisioned with a certificate from the VMCA by default

In auto deploy storage is done within the auto deploy server

If the cert is not available: reboot cycle

Auto deploy as a subordinate of CA

Signed with SSL key

8.0 + custom cert with MAC/BIOS UUID

Managing Certificates

Requires permission

Certificates.Manage Certificates required

ESXi Host name and IP address

Certificate Management with Certificates

Upgrades retain custom certificates

Uploading to the datastore

Certificate must be accepted

Upload fails otherwise

Conclusions

Certificate management

Manage with vSphere client

Security Logging

Enable Logging

Why use logging?	Collect information on events Troubleshooting Security records Legal records

Storage	VM log file = vmware.log Archive log files = vmware-[Sequaential Order Number].log

How to enable: → Select VM ➔ Edit Settings → VM Options tab → Expand Advance Tab → Examine the Setting row → Enable logging → OK

Enable Logging
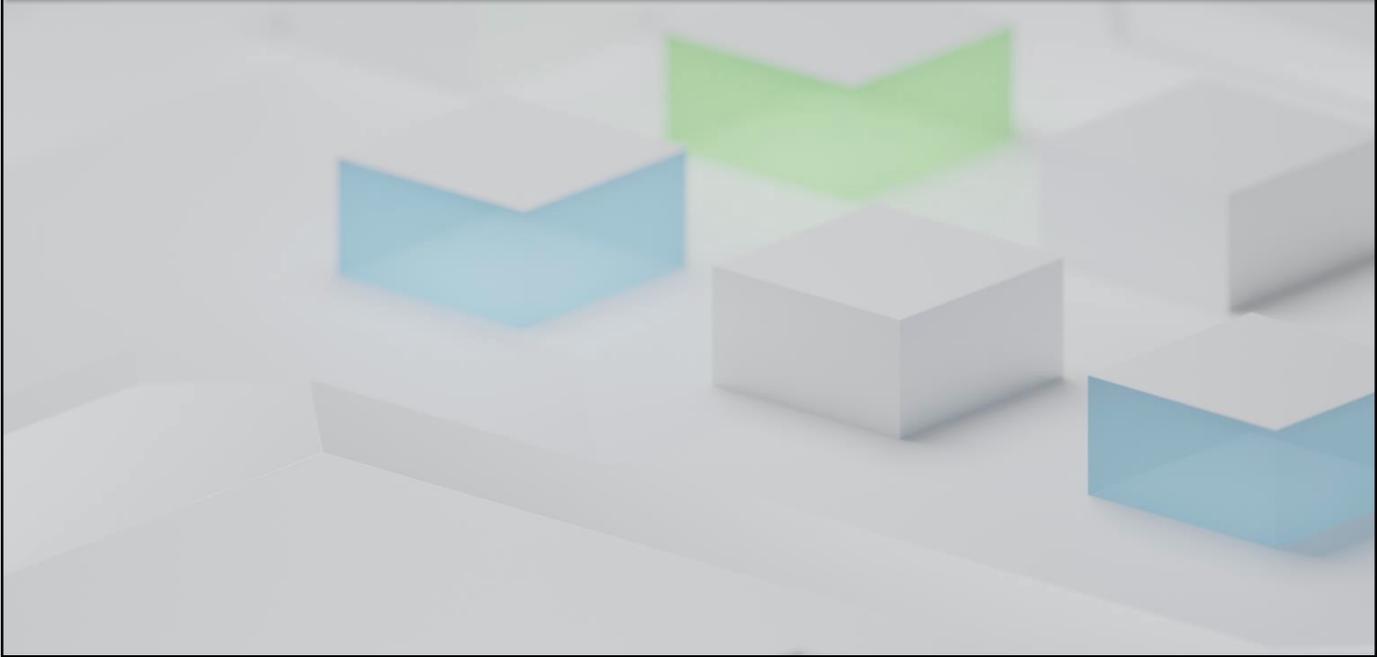
Logging Options

Logging Options

Under the configure tab of the vCenter Server Settings ➔ General ➔ Edit
Logging Settings

None = No logging

Error = Only error logs

Warning = Error ➔ Warning logs

Info = Error ➔ Info logs

Verbose = Error ➔ Verbose logs

Trivia = Error ➔ Trivia logs

Logging Options
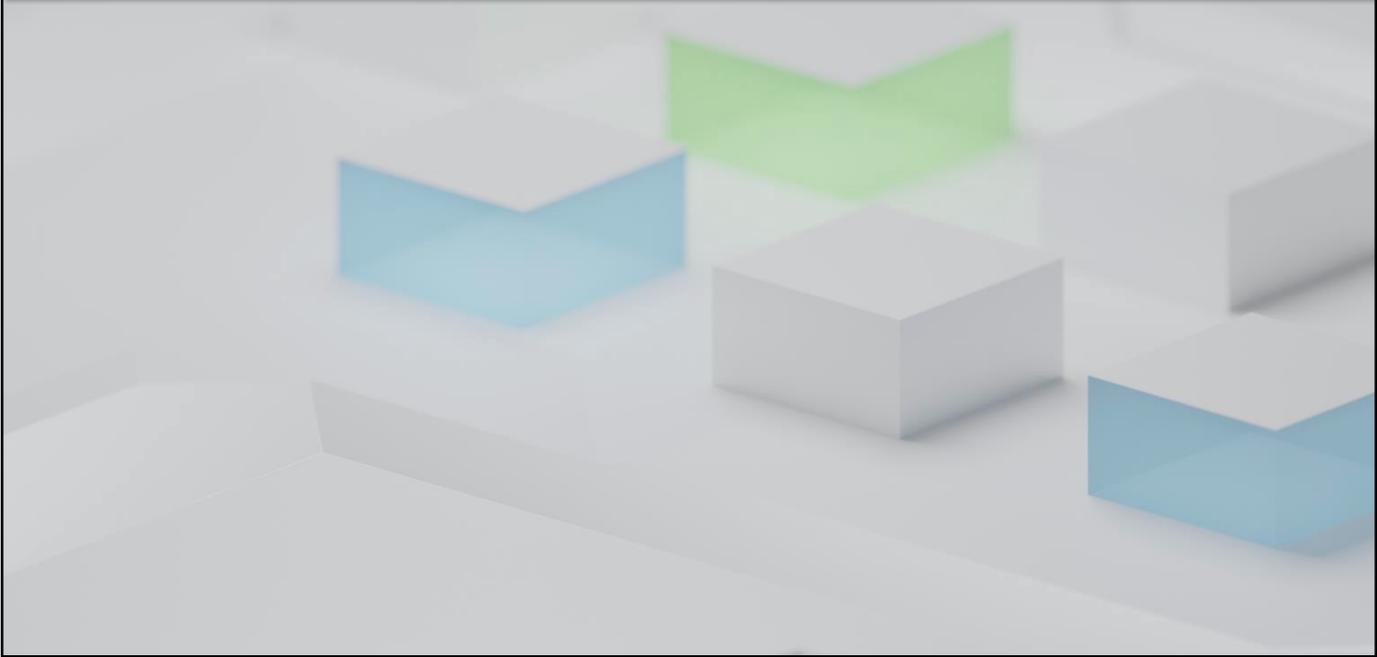
Conclusions

Enable Logging

Logging options

Securing vMotion

Securing vMotion

Migrating encrypted VMs is always encrypted

- Protects CIA triad
- Data in transit is encrypted
    - When the disk is encrypted
- Encrypted migration is supported
    - Across vCenter Server instances

States of Encryption with vMotion

- Required
- Opportunistic
- Disabled

Securing vMotion

Migration Security Requirements

Trust

Securing vMotion

Migration Security Requirements

Source and Destination server share Key Management Server

> KMS cluster name is identical on both

Destination host is actively using encryption mode

Safe mode

Key Change & Storage Policy cannot be altered during migration

Trust

vMotion is supported by Trust authority

> Installed on the destination host
>
> > Attestation

No altering encryption on migration

Hosts need to be trusted to have VMs migrate to them

Enabling Encrypted vMotion

Select a VM → Edit Settings → Click VM Options → Select Encryption → Select a vMotion option from the drop down
Disabled
Opportunistic
Required
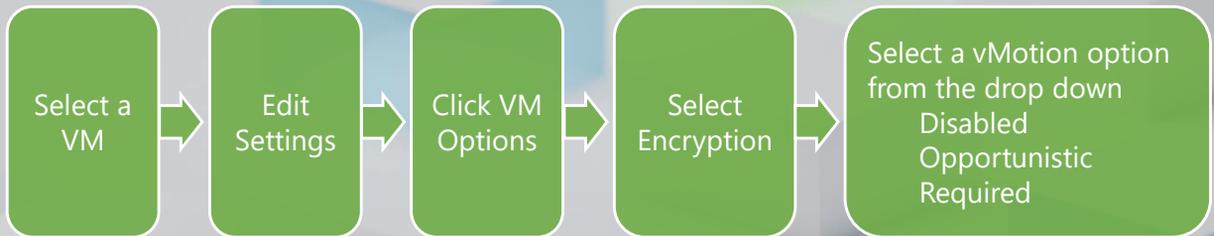
Enabling Encrypted vMotion
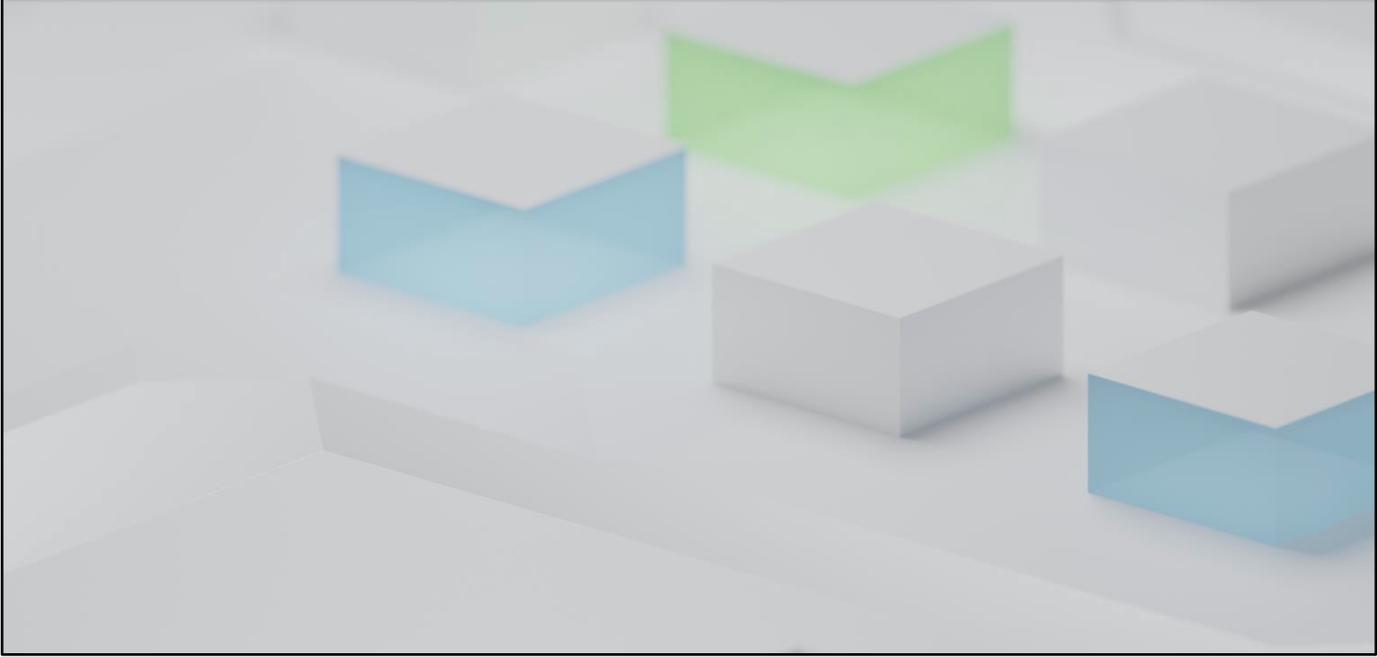
Conclusions

Securing vMotion

Encrypted vMotion
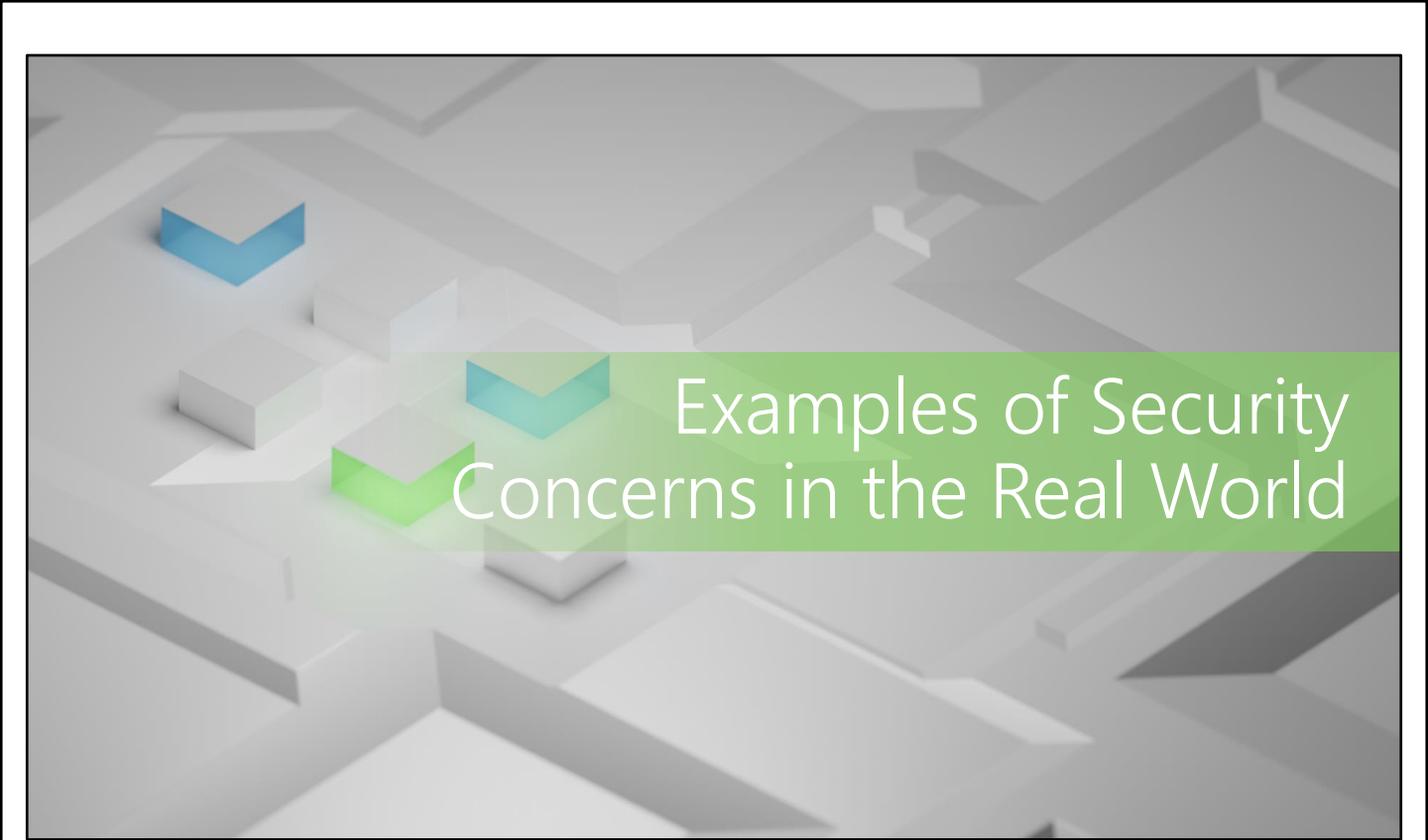
Examples of Security Concerns in the Real World

Examples of Security Issues with VMware

Review Recent Security Vulnerabilities and workarounds

OpenSLP as used in ESXi has a use-after-free issue

Examples of Security Issues with VMware

Review Recent Security Vulnerabilities and workarounds

https://www.vmware.com/security/advisories.html

OpenSLP as used in ESXi has a use-after-free issue

A malicious actor residing in the management network who has access to port 427 on an ESXi machine may be able to trigger remote code execution

Solution: Apply Newest Patch

Examples of Security Issues with VMware

Malicious actors can access VM with 3D graphics enabled

Execute code on hypervisor via a VM

Solution: Apply newest patch

Noticing a pattern?

Security issues often come in the form of being able to access a device

- Then escalate privilege
- To the point of being able to execute code remotely

Often the solution for security issues is updating patches.

Patches aim to fix security vulnerabilities

Conclusions

Examples of security issues with VMware

Introduction to Resource Allocation

Resource Management

Assign resources

Resources are overcommitted

What resources are managed?

Resource Management

Assign resources	From providers to users

Resources are overcommitted	If not regulated
	    Inefficient
	    Can negatively affect your network or services

What resources are managed?	Network resources Storage Power Memory CPU

Resource Management

Who can provide resources?	Hosts Clusters / Pools Datastores
Who takes resources?	Virtual Machines Applications
Why use it?	Avoid committing resources incorrectly Predictability Reduce importance of each VM

Resource Management

Goals:	Efficiency Balancing Ensuring a VM can operate

Conclusions

Advanced Host Management

Host Profiles

Profiles	Contain pre-configured host configurations
	Used for:
	    Template for other hosts / clusters
	    Validation for host configuration compliance
	    Auto-Deploy

What can attach to a profile?	Hosts Clusters
How is a Profile made?	Reference host Make a profile of the reference host Bind new hosts to the profile

Host Profile Use

Using Host Profiles

New installations of similarly configured hosts
Host Profiles can't promise more then the physical device can produce
 If physical device has 3 network adapters, can the host profile configure 4?
Avoid using hosts with wildly different hardware configurations

Large Environment? Multiple vCenter Servers?

Profiles can be exported to multiple vCenter Servers

Maintain consistency

Maintain control of your environment

Compliance Checks

Schedule and Set alarms

Host Profile Use

Recommended Procedures:

Track host-configuration and profile values

Make incremental changes to the Host Profile

Standardize your environment using host profiles

    Reduce variation through consistency

Group hosts with single profiles based on similar hardware

Preferably attach profiles to clusters then individual hosts

Ensure ESXi host capacity is sufficient

    Handle being placed in maintenance mode

Overview of Host Profile

Attaches Profile

Host Profile → Cluster

Attaches Profile

ESXi Host → ♻ *Constantly Check attached entities configurations for deviations*

Creating a Profile
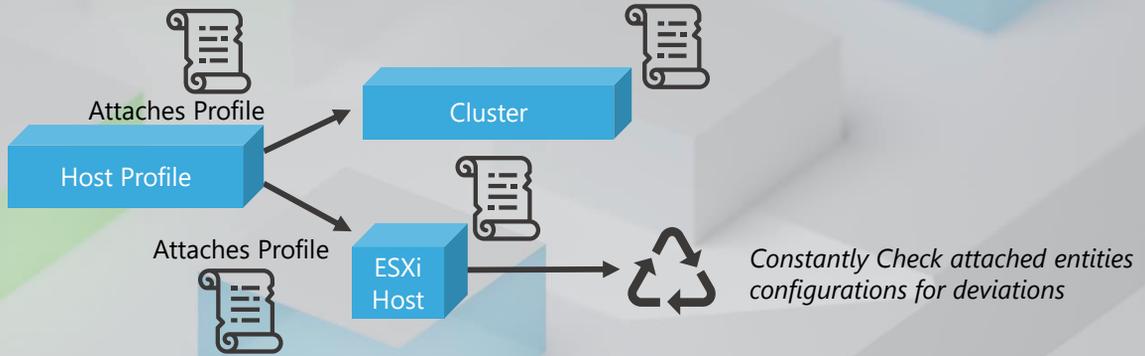
Profiles and Policies Page → Host Profiles → Extract or Import → Select Your reference host (You'll extract this hosts settings) → Name the Profile
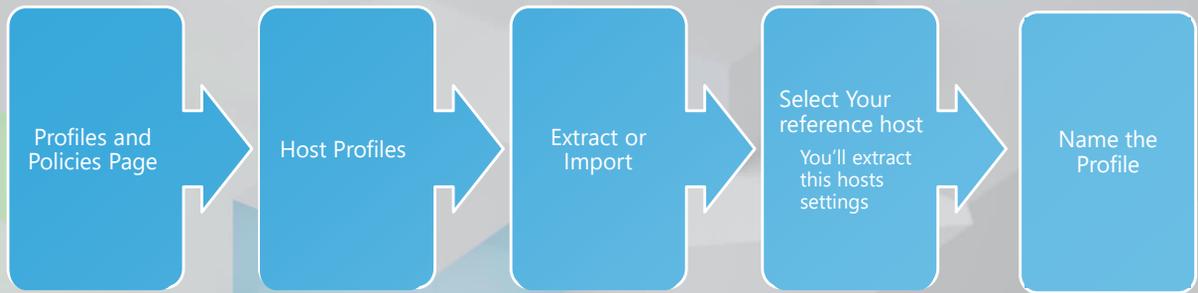
Attaching entities
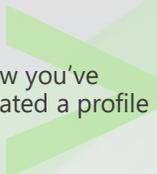
Now you've created a profile

Its time to attach hosts or clusters
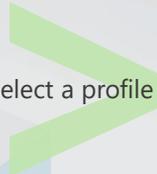
Select a profile

Pick either hosts or clusters to attach to the profile
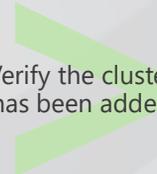
Verify the cluster has been added

Editing the Profile

Aspects of the host profile can be changed

After profile is created
Change policies of specific configuration settings
    Affects how parameters are applied
    Changes affect any device that the profile is attached to
Expand hierarchy to adjust sub profile and alter attributes
No need to memorize all components, just understand

Editing the Profile

Example:

Expanded the network configuration tab

Looking at the configured vSwitch

Edit aspects of the link configuration

    Change the name of the Physical NICs

    Adjust the beacon level

Saving the profile will apply this to associated hosts

Check Compliance

Result of a Compliance Check:

Compliant

Unknown

- No verification possible
- Doesn't mean inconsistency exists

Non-Compliant

- Inconsistency found between profile and host

Real World Tip: Check to see that your host is connected before

Schedule Compliance Checks

Ensures consistency over a period of time

Set for one time or repeated checks

What schedule is best for your environment?

Checks require network resources

- Ensure that your attached hosts are remaining consistent
- Can slow your network

Host Remediation

Scenario:

Non-Compliance result in a Compliance check for a host

Need to bring host "into line"

How?

Remediation:

Resets host parameters to match the host profile

Host Remediation

Process: > Select a host profile > Right click > Remediate > Host May reboot > Pre-Check Remediation. Can the host be remediated? > Reboot necessary hosts > Reboot necessary hosts > Reboot necessary hosts
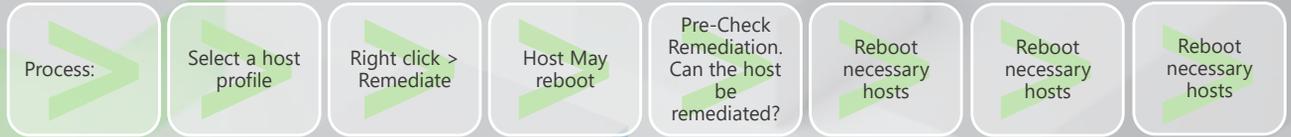
Auto-Deploy

Host Profiles

Can be used to Auto Deploy hosts

Hosts are configured consistently with the profile used

Stateless

Auto-Deployed Hosts can be remediated

Auto-Deploy server

Configures host with image specified by a rule engine

Applies appropriate host profile

Specified in the rule set

After provisioning the auto deployed host is added to the vCenter Server

Duplications

Using Host Profile Duplicates

Copy an existing host profile
Ensure a profile is available
Prepare to move a host profile to a separate vCenter Server

Import / Export Host Profiles

Why import a host profile?

Keep consistency between vCenter Servers
Transferring to a new environment
    Need profiles used in previous clusters
Import .vpf files to be used later as host profiles

Import / Export Host Profiles

Process:　　Select host Profile　　Import Host Profile　　Select the appropriate .vpf file　　Name the new Profile　　OK

Export a Profile

Why export a host profile?

Similar purpose as importing a profile

Need to keep consistency in an expanding environment

Part of the two-step process of importing and exporting host profiles

Propagate profiles in your environment

Creates a .vpf file

Profiles and passwords are not exported

Reapplied after

Configure HBA to Boot

Process: → Select Host Profile → Export Host Profile → Read Warning → Save

Integration

Hosts may need to be rebooted During remediation

- Hosts go into maintenance mode

- Placed before remediation

- Hosts in a fully automated DRS cluster enter maintenance at remediation

Parallel Remediation

- Removed in vSphere 7.0

- Still available: Remediate from flash

Integration

Audit-quality logging

- Enhanced since VMware 6.5
- Provides forensic data on user actions in the environment
- Visibility into operations
- *Who did what?*
- *When did they do it?*
- *Where did they do it?*
- *How did they do it?*

Example:

[VSPHERE.LOCAL\Administrator] [Datacenter] [46196] [Reconfigured X in Datacenter]

Config.hardware.device (4001) deviceInfo.summary:
"Device configured as A" → "Device now configured as B"

Conclusions

Host profiles

Profiles

Duplications

Importing/Exporting a profile

HBA to boot

Integration

High Availability

Business Continuity

VMware can drive down costs	No need to purchase hardware No need to maintain a facility

But it can present some risks	Downtime Lose of direct control

How can we limit negative business impact?	Wield VMware services Ensure minimal negative business impact

Business Continuity

Mitigation Techniques

High Availability	Data Protection	Disaster Recovery
Hardware Backups Software Backups Interoperability Admission Control	Data Protection	Failover Fault Tolerance Preparing network for downtime

Ensuring Business Continuity with:

High Availability

vMotion
Replication
HA

Data Protection

vSphere Data Protection

Disaster Recovery

Operations Management
Recovery Manager
vCloud Suite

HA Clusters

Scenario:

You have 2 hosts

1 host has 2 VM's running on it

The other host has no VMs running on it

That VM is running an application that clients are accessing

How can you protect that process on the VM if the host is showing signs that it may fail soon?

HA Clusters

One Solution:

HA Clusters

Reduces downtime

You don't need to reconfigure the VM on another host

Ensuring Business Continuity with:

ESXi Host 2

HA Cluster

VM 1

ESXi Host 1

VM will Fail

ESXi Host Fails

VM is restarted on another host in the cluster

VM 1

HA Cluster

ESXi Host 2

ESXi Host 1

Active, Passive, Witness Nodes

Active, Passive, and Witness nodes enable a failover solution in HA Clusters

You create an HA Cluster

   It has at least 3 vCenter Server Instances

   Deployed on various ESXi hosts

Deployment includes 3 different node types

Interact with each other to enable HA functionality

Supports resilience to hardware malfunctions

You need all 3 node types

   What are they?

Active, Passive, Witness Nodes

Active node	Runs vCenter Server instance	Has the Public facing IP address	Links to the management interface	Used to interact with Passive and Witness node Over HA network
Passive Node	Starts as a clone of the Active node	Updaters and synchronizes with Active node	Active node fails	Passive node replaces
Witness Node	Starts as a clone of the Active node		Prevents Split-Brain	
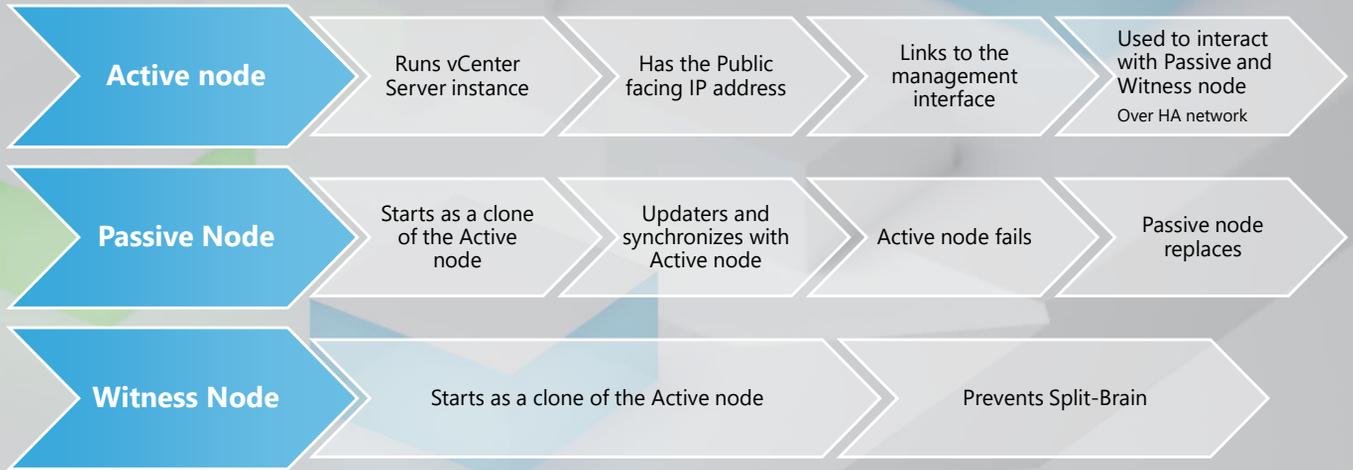
Active, Passive, Witness Nodes
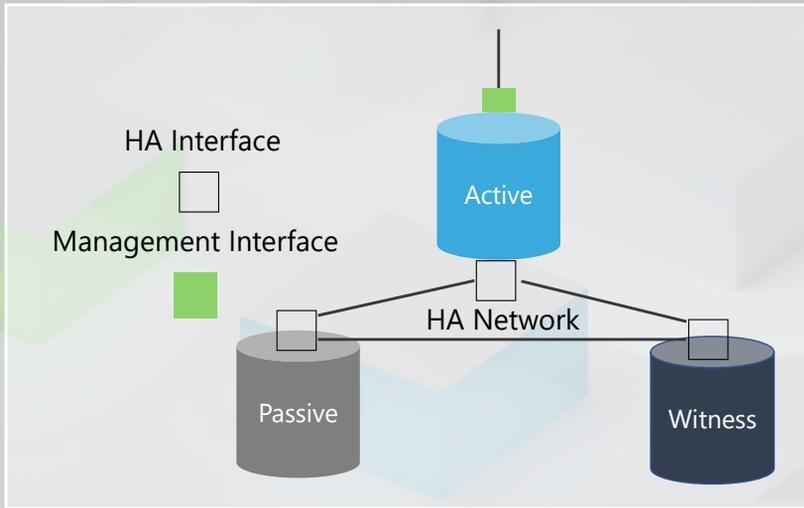
Active, Passive, Witness Nodes

Primary Host

"Manager"

Monitor state of Secondary Hosts

    Determines if Secondary Hosts have failed

    What VMs need to be restarted

        Orchestrates restarts of protected VMs

        Does not include VMs on hosts disconnected from the Host

    What power state is the VM in

Determines who is in the cluster

Interface to vCenter Server

Reports Health of Cluster

Secondary Hosts

Runs VMs

Monitor runtime states

Report updates to primary VM

Admission Control

Are there enough resources to even recover and restart a VM?

Admission Control ensures that

Admission Control Policies protect a certain amount of resources

Cannot be touched by any other processes
Leaves space for:
Restart
Recovery
Processing and Memory Reallocation

Actions that violate Admission Control policies are not allowed

Reduction Threshold → Requires DRS

Admission Control

Resources Reserved:

Often determined as a percentage of resources

- Host
- Cluster

Default Reservation: 0MB / 32MHz CPU

Alternative Models:

Designate which hosts will be used as failover hosts

Slot Policy Admission Control

Interoperability

HA integrates with other services

    HA with vSAN

    HA with DRS

HA with vSAN

It would be helpful if members of an HA cluster could use a shared storage

    Pool all resources

    Pull form all resources as needed

Integrate HA with a vSAN

    Cluster will utilize a shared virtual storage network

    In a cluster with at least 3 ESXi hosts

Interoperability

One Solution:

HA Clusters

Reduces downtime

You don't need to reconfigure the VM on another host

Interoperability

HA with DRS

HA moves VA to different hosts

Process is not balanced automatically

DRS acts as a load balancer for restarted VM hosts

Specify affinity rules in DRS

 Determine how HA applies rule during Failover

New in 7.0 DRS requires vCLS availability

IPv6 & HA

IPv6

 Requires ESXi hosts 6.0 or later

 Consistent IP protocol used in HA Cluster

 vSAN + vSphere HA + IPv6 = NOT Possible

Creating the HA cluster

Min 2 hosts

Common Management network

VMware Tools

VMPC needs ESXi 6.0 or later
No VMCP without APD Timeout

What do you need?

Persistent IP addresses on hosts

VM to Host Compatibility across the board

Support IP protocols

Making the Cluster

Configuring the Cluster

How will the Cluster Respond to failure?

▶ **Host Failure**

Host Isolation

Datastores

PDL

APD

VM Monitoring

Configuring the Cluster

How will the Cluster Respond to failure?

Host Failure

▶ **Host Isolation**

Datastores

    PDL

    APD

VM Monitoring

Configuring the Cluster

How will the Cluster Respond to failure?

Host Failure

Host Isolation

▶ **Datastores**

    PDL

    APD

VM Monitoring

Configuring the Cluster

How will the Cluster Respond to failure?

Host Failure

Host Isolation

▶ **Datastores**

    PDL

    APD

VM Monitoring

Configuring the Cluster

How will the Cluster Respond to failure?

Host Failure

Host Isolation

Datastores

    PDL

    APD

▶ **VM Monitoring**

Configuring Admission Control

Configure:

Max number of host failures cluster can recover from

Failover Capacity defined by:

- Resource Percentage
- Slot Policy
- Dedicated Failover hosts
- Disabled

Set Percentages if needed for:

Host failover capacity

Performance degradation toleration

Selecting a Datastore for Heartbeat

HA monitors host and VM health

Utilizes datastores for hosts monitoring

Datastore Selection

Automatically from a pool of accessible datastores

Selected Datastores

Combination of both solutions

Proactive HA

Automation Level

Quarantine mode vs Maintenance mode
- How will this be determined?

Manual
- vCenter Server Suggests migration

Automated
- VMs migrate to healthy hosts
- Degraded hosts are quarantined

Remediation

How are degraded hosts handled?
- Quarantine mode
- Maintenance Mode
- Mixed

Troubleshooting

| Common issues: | Deployment Errors | Degraded HA Clusters | Active node stops serving client requests |

| Where to start looking for deployment errors: | Network Latency | Routing between nodes is correctly configured | Check health of:
Active Nodes
Passive Nodes
Witness Nodes |
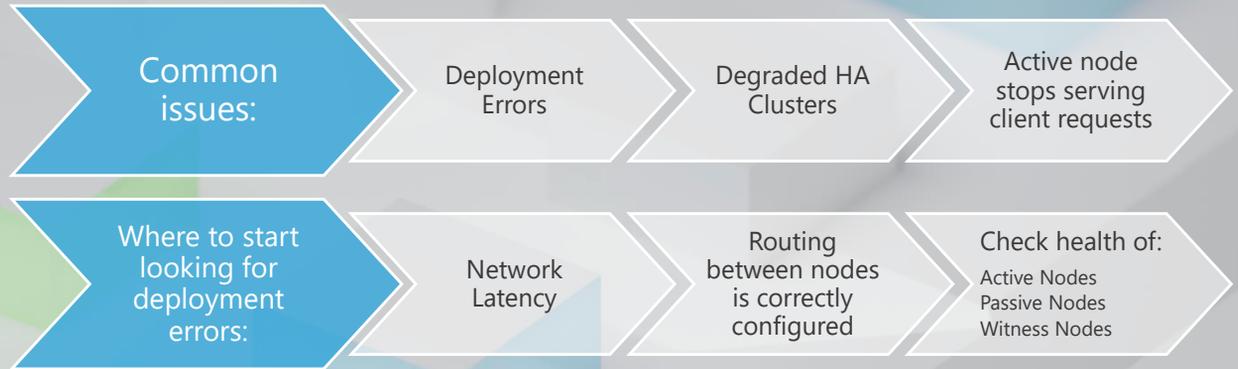
Troubleshooting

Why is my cluster degraded? → Node failure → DB replication failed → Configuration file not copied from active and passive node

What can I do? → Check that you have enough bandwidth → Check that network latency is not more then 10 ms → Check for down hardware or network isolation

Troubleshooting

| Why is my active node not serving client requests? | Isolated | Not connected to Passive or Witness node | Still functions so not replaced |

| What can I do? | Check to see if you can resolve the connectivity issue in the console | Destroy the Active Node in a Bash shell | vcha-destroy –f Now, reboot and reconfigure the cluster |

Fault Tolerance

Fault Tolerance Problem

Scenario:

You have a mission critical VM

Sensitive to failure

How can we protect this "Primary VM"?

> How can we protect the jobs it's running?

Fault Tolerance Problem

Fault Tolerant VMs

Create a duplicate "Secondary VM"

Run on another host

Secondary VM can take over when Primary fails

At anytime

Applications are already running

Data is already stored

Primary and Secondary VMs monitor each other

Maintain fault tolerance

If the secondary replaces the primary a new secondary is made!

When to use Fault Tolerance

Do you have the resources?

Can you afford to have a backup VM?

Enough processing power?

Enough memory?

Use FT if you have:

Failure sensitive applications

i.e. NOT batch processing

HA is not enough of a guarantee

Critical moments during a VM lifecycle may need to be protected

HA is too complicated to configure

Using Fault Tolerance

Enable: → Right Click the Desired VM → Select Fault Tolerance → Turn on Fault Tolerance → Yes → Choose a datastore → Place the Secondary VM config files in the Datastore
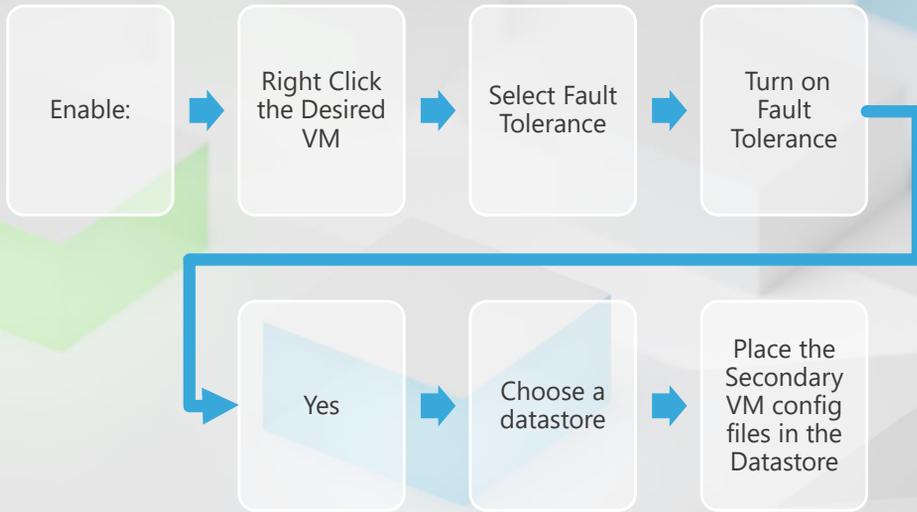
Best Practices for FT

Avoid Secondary VM restarts → Keep CPU frequency consistent → Disable DPM on hosts running FT VMs → Use the time to check consistent DPM setting
Re-enable

Networking → Have specific NICs receive traffic types → 10Gbit NICs → Enable jumbo frames

Best Practices for FT

Clusters

Ensure nodes are compatible	Use common datastore access	Consistent network configurations	Consistent BIOS settings	Check compliance often

Best Practices for FT

ISO storage → Shared storage → Accessible by both primary and secondary VM

vSAN Datastores → Don't mix datastores → Separate your vSAN and FT networks → Store Primary and Secondary VM in separate fault domains in the vSAN
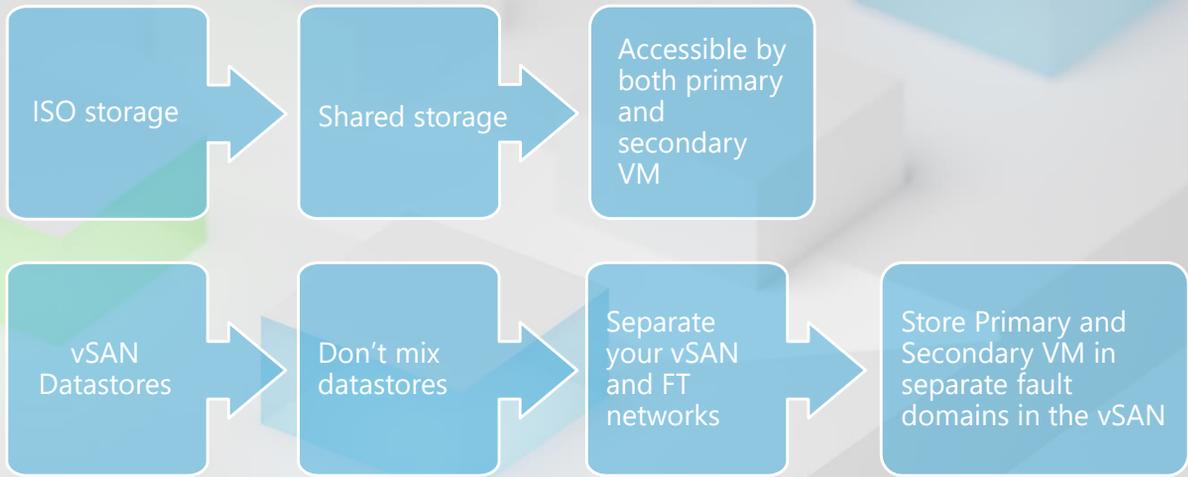
Conclusions

Fault Tolerance

When to use

Best practices

vCSA Upgrade Process

Upgrades

What's getting updated?
?

vCenter Server
ESXi
VMs
VMware tools

What are we upgrading from?
?

v6.5 or v6.7 ➔ v7.0 ➔ v8.0

vCenter Server 6.7
PSC
Operating System

vCenter Server
Appliance

Upgrades

What will you need?

Platform Services Controller

Deployment with a vCenter Server Appliance

Verification that the system meets the minimum requirements for updating

vCenter Server 6.7
PSC
Operating System

vCenter Server
Appliance
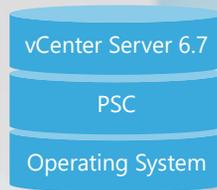
Methods for Updating vCenter Server

GUI installer

Uses an OVA file

You deploy

vCenter Server appliance management GUI

Deployed as OVA file

Configure new appliance

Use source deployment data

CLI installation

Customize CLI templates

Big Picture

Upgrade the vCenter Server Appliance or Migrate → Does equipment meet upgrade requirements → Prepare your network for the upgrade → Upgrade or migrate to the Appliance in the GUI or CLI → Finish post-upgrade jobs
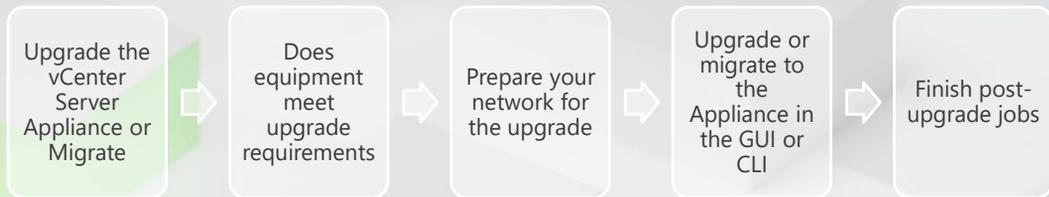
Requirements

Hardware

What appliance environment is right for you?

Environment	Host : VM	vCPU	Memory
Tiny	10 : 100	2	12 GB
Small	100 : 1000	4	19 GB
Medium	400 : 4000	8	28 GB
Large	1000 : 10000	16	37 GB
X-Large	2000 : 35000	24	56 GB

Requirements

Storage

Requirements depend on your environment's storage needs

Environment Type	Default	Large	X-Large
Tiny	415 GB	1490 GB	3245 GB
Small	480 GB	1535 GB	3295 GB
Medium	700 GB	1700 GB	3460 GB
Large	1065 GB	1765 GB	3525 GB
X-Large	1805 GB	1905 GB	3665 GB

Requirements

Software

Installer run in GUI or CLI

Client machine must be running:

Windows

Linux

Mac

OS	Versions	Hardware
Linux	SUSE 15 , Ubuntu 16.04 and 18.04	4 GB RAM, 1CPU 2 Cores 2.3 GHz, 16 GB disk
Windows	8.0, 8.1, 10, 2012 (R2), 2016, 2019	4 GB RAM, 2 CPU 4 cores 2.3 GHz, 32 GB disk
MAC	10.13 – 10.15, High Sierra, Mojave, Catalina	8 GB RAM, 1 CPU 4 cores 2.4 GHz, 150 GB disk

Requirements

- Key Requried Opened Ports
- 22 - SSH
- 53 – DNS Service
- 80 - HTTP
- 88 – AD server
- 389 – LDAP port
- 443 - HTTPS
- 1514 – Syslog Service
- 2014 – RPC port for VMCA API
- 2015 – DNS Management
- 5480 – Appliance Management Interface
- 9443 – vSphere Client HTTPS

Requirements - DNS

vCenter Server Appliance needs:

- An IP address
  - Static or Dynamic
  - DHCP use requires verification that appliance name is updated in DNS
    - Ping it to be sure
- A FQDN
  - Resolved by a DNS server
  - Must be registered to DNS
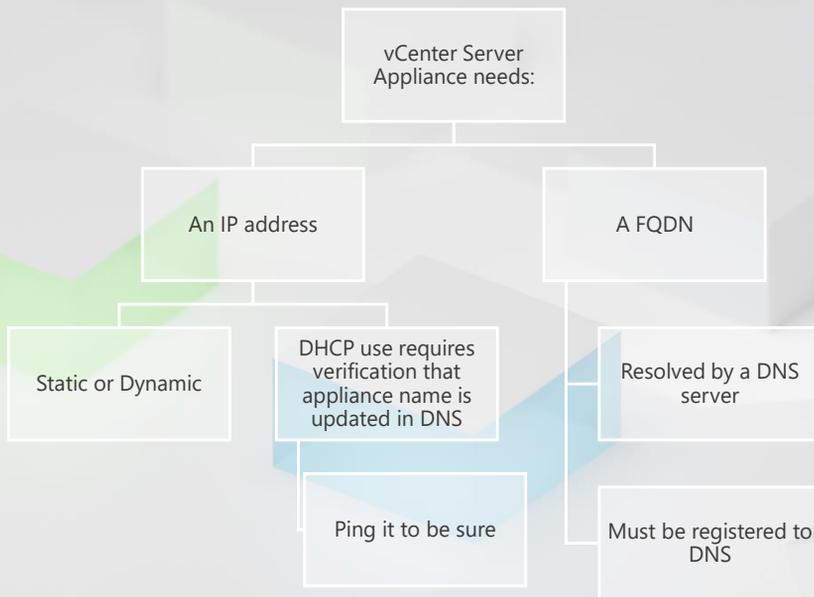
Requirements – DNS

Requires:

Forward and reverse DNS A records

A > IPv4

Verify

nslookup --nosearch --nodename IP address or FQDN

Clock Synchronization

Why is it important to synchronize clocks on machines to vSphere?

SSL Certificate timing

SAML tokens

Both are times sensitive

Discrepancies of time can lead to invalid certificates

This can cause a failure to update

> vmware-fpxd service won't start

Clock Synchronization

Best solution

Synchronize Clocks between physical devices and vCenter Server

Sign into vCenter Server Management Interface → Root user → Select Time → Time zone → Edit → Select a time zone from the drop down → Time synchronization page → Edit

Clock Synchronization
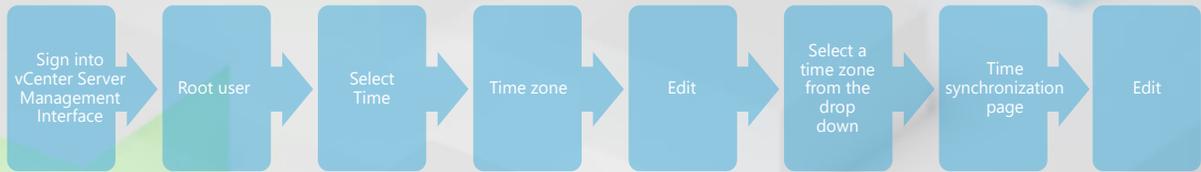
```
                    ┌─────────────────┐
                    │  Select a mode  │
                    └─────────────────┘
            ┌───────────────┼───────────────┐
     ┌──────────┐     ┌──────────┐     ┌──────────┐
     │ Disabled │     │   Host   │     │   NTP    │
     └──────────┘     └──────────┘     └──────────┘
                            │                │
                  ┌─────────────────┐  ┌──────────────────┐
                  │  VMware Tools   │  │  Synchs with an  │
                  │ handles time sync│  │ authoritative NTP│
                  └─────────────────┘  │      server      │
                                       └──────────────────┘
                                       ┌──────────────────┐
                                       │  Requires the    │
                                       │ servers IP address│
                                       │     or FQDN      │
                                       └──────────────────┘
```
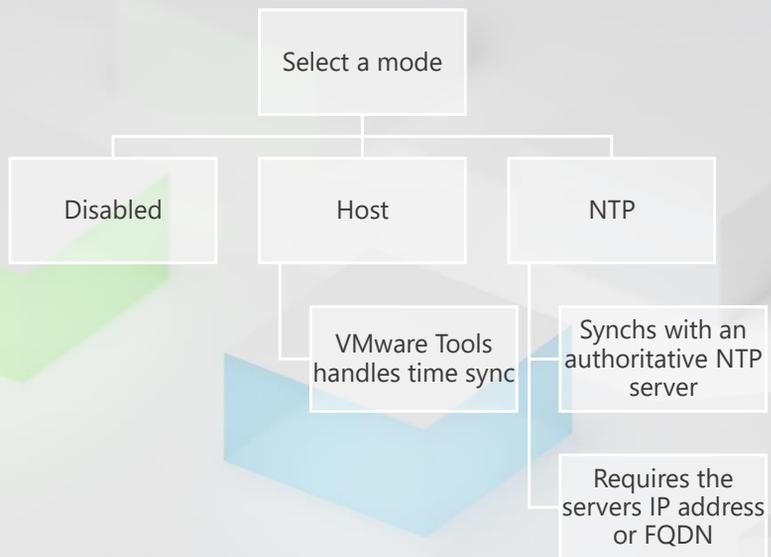
Data Transfer

What is it?

External Databases containing vCenter Server information are embedded to a PostgreSQL database

This is a relational database > Defined schema

Used by version 7.0 of the vCenter Server Appliance

Purpose

Maintains configuration data during the update

Minimized downtime

You don't have to do it all over again!

Maintain historical data

Maintain Metrics data

Data Transfer

Why do it?

Save time reconfiguring the vCenter Server

Save statistics on usage

Maintain metrics

Note:

Once the transfer starts all at once vCenter Server cannot start until finished

All data needs to be embedded to the vCenter Servers Postgre SQL database

Beginning the Update

Download the ISO image	v8.0 https://my.vmware.com/web/vmware/downloads VMware-VCSA-all-*version_number-build_number*.iso
Ensure the ISO received is correct	Verify the MD5 Hash provided
Store the ISO	External hard drive
Mount ISO image	Place on desired machine to be upgraded

Prepare the Host

HA clusters require SSL certificate checking must be enabled

If not HA wont function on updated hosts

Select vCenter Server in vSphere	Configure Settings General Select Edit
SSL settings	Verify that vCenter Server requires verified host SSL certificates

Upgrade using the GUI

Go to your subdirectory and run the installer file

exe
.app
Select Upgrade

2 core steps

OVA Deployment
Appliance Setup

vCenter Server upgrade wizard

Introduction

Explains your options

EULA

Accept if you dare

Connect to Source Appliance

Deployment Target

Target vCenter Server VM

Deployment Size

Select Datastore

Network Settings

Upgrade using the GUI

Introduction

EULA

Connect to Source Appliance

Server appliance
Port
SSO credentials
Host credentials + Port

Deployment Target

Target vCenter Server VM

Deployment Size

Select Datastore

Network Settings

Upgrade using the GUI

Introduction

EULA

Connect to Source Appliance

Deployment Target

Port and Credentials for the target

Target vCenter Server VM

Deployment Size

Select Datastore

Network Settings

Upgrade using the GUI

Introduction

EULA

Connect to Source Appliance

Deployment Target

Target vCenter Server VM

Set target:
      Name
      Root password

Deployment Size

Select Datastore

Network Settings

Upgrade using the GUI

Introduction

EULA

Connect to Source Appliance

Deployment Target

Target vCenter Server VM

Deployment Size

Use the reference chart to pick your model deployment size

Tiny

Medium

Large

Select Datastore

Network Settings

Upgrade using the GUI

- Introduction
- EULA
- Connect to Source Appliance
- Deployment Target
- Target vCenter Server VM
- Deployment Size
- **Select Datastore**
  - Pick a compatible datastore
  - Thin provisioning
- Network Settings

Upgrade using the GUI

Introduction

EULA

Connect to Source Appliance

Deployment Target

Target vCenter Server VM

Deployment Size

Select Datastore

Network Settings

Select a Network
IP settings
    Protocol used
    IP address
    Subnet mask / prefix
Designate a default gateway
Select a DNS server

Upgrade using the GUI

Stage 2

Intro

Connect to source vCenter Server

    Review your configurations you made previously

Select Upgrade data

    What data will be copied to the server?

Configure CEIP

    Join or leave at any time

Complete

    Review

Warning

Source vCenter will shut down

Examine the Pre-Upgrade check results

Upgrade using CLI

Why?
> Allows more control

What you need:
> JSON file
>> Declarative configuration
>> Key : Value Pairs
>
> Path to that JSON file
> Knowledge of JSON syntax

Base argument
> `vcsa-deploy upgrade JSON_file_path`
> Append the argument ass needed
> Ex: `--accept-eula`
> Ex: `--precheck-only`

Post vCenter Server Update

Key components to post update environment:

Verify success

Login to vSphere

Great way to verify success of IP address of FQDN

https://vcenter_server_ip_address_or_fqdn

Shut down the external PSC if used

Removes it from the SSO

Should no longer be referenced by

Enhanced Authentication

Located at the bottom of the vSphere Client login page

Download Enhanced Authentication Plugin

Post vCenter Server Update

Identity Sources / SSO

Attach domains

For use with SSO server

Used for user authentication

7.0 supports federated authentication

vSphere is moving towards token based authentication

What can you use?

AD over LDAP

Integrated windows Authentication

Open LDAP 2.4 and later

Migration

Windows to Appliance

Take a vCenter Server for Windows
Convert to vCenter Server appliance installation
Upgrades as well
v7.0

Requires

Migration assistant
Platform services controller
vCenter Server for Windows

High Level View - Embedded Migration

Run Migration Assistant

vCenter Server

Windows

Migrate

Complete post-migration tasks

vCSA
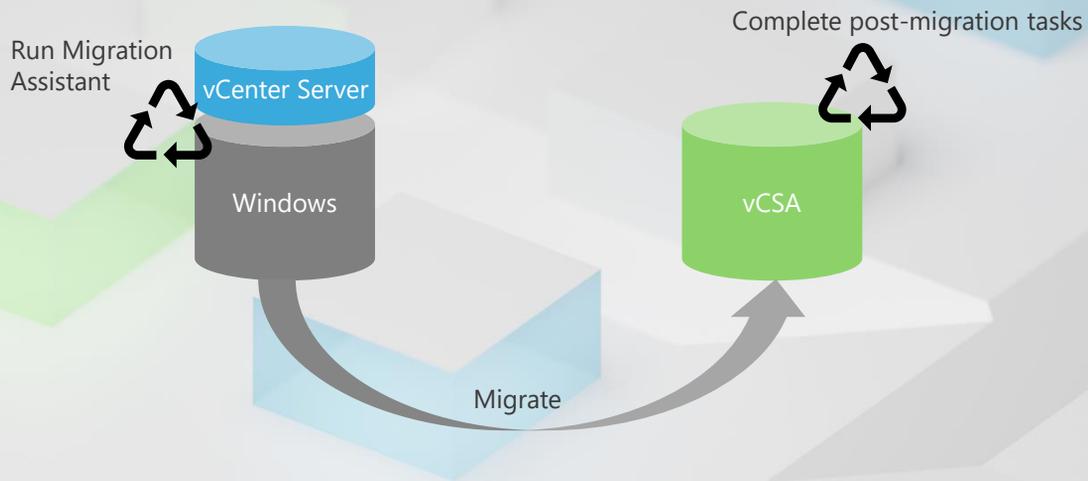
High Level View - External Migration

Migrate

Run Migration
Assistant on PSC

Complete post-migration tasks

Then run Migration
Assistant on
vCenter Server

PCS

vSCA
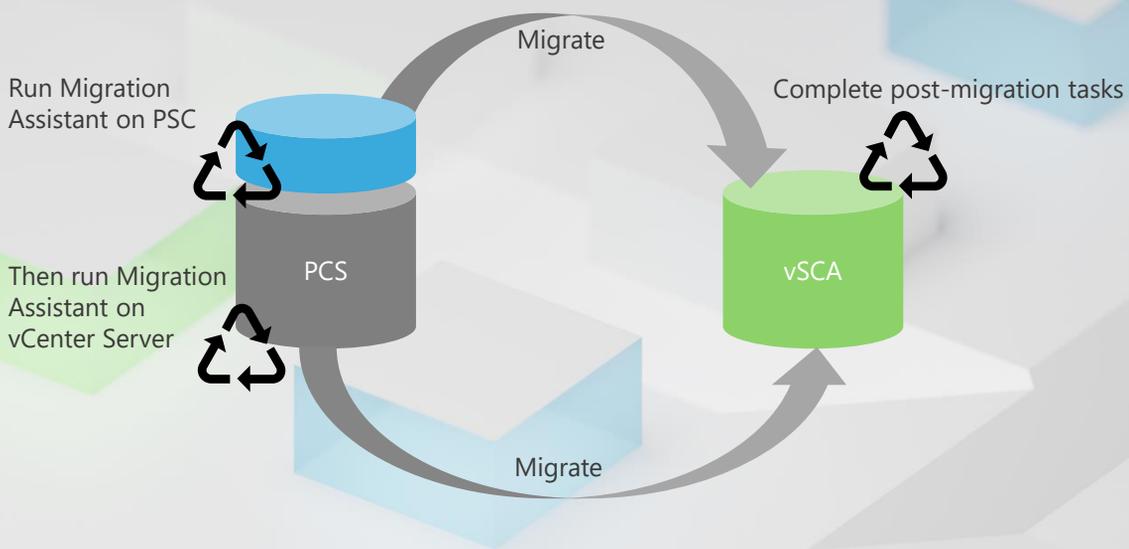
Migrate

Migration System Requirements - Source

Verify permissions of vCenter Server user account:
    Admin group
    Log on as service
    Can replace a process level token
    Act as part of the OS

Non-expired certificates on:
    Platform service controller
    vCenter server

Migration System Requirements - Source

Sync clocks
- NTP server validation
- SSL certificate validity

Service Accounts
- Local account needs read permissions for vCenter Server

System workname
- Cannot be provided by DHCP IP address

Migration System Requirements - Target

Compliance
- Hardware
- Software
- Same as upgrading the appliance

Using a FQDN
- Host machine for vCenter Server appliance and host are on same DNS Server

Synchronize clocks
- Common theme for updating
- Maintains security certificate functionality
- Failure to sync may cause migration failure or prevention
  - Services might not start
  - Due to authentication problems

Migration System Requirements - Target

Roles

Need admin privileges on host

Set Credentials

Storage / Processing

Is there enough storage?
Do you have enough CPUs?
Can storage be accessed?
Answer based on your environment

Migration System Requirements – Network

DNS records

Using a static IP address for temp.
network settings for new appliance?

You need to configure forward and
revers DNS records for that IP address

Using DHCP instead?

ESXi deployment host for new appliance

Must be in same network as host
with previous vCenter Server Appliance

Connected to min. 1 network
associated with a port group

One that accepts MAC
address changes

What to watch out for!

Be careful after the migration

Source vCenter Server will shut down

All solutions installed are unavailable after

Network ID conflict with the target

   Can become a larger issue

Network Adapter

Only one setting migrated to target appliance

Hostname will resolve to one IP address and one network adapter setting

Preparation

Similar to an update

- One key difference
- VMware Migration Assistant

VMware Migration Assistant

- Discovers source deployment type
- Runs pre-checks for you
- Error reporting
  - Mandatory review before migration
- Tells you what to do next
- Run on source server or PSC
- If you use an external update manager running windows
  - Run Migration Assistant on that

Run the Assistant

Installation & Use Cases >	License & Download >	Troubleshooting > & Support	How to Buy >

Download the installer package for the new vCenter Server Appliance

Find the VMware Migration assistant in the directory

Copy that folder onto the source machine

Double Click the .exe fie to access the GUI
Keep the window open until the upgrade / migration is complete

Pre-checks will run
You need to address all issues before migration can begin

Run GUI migration of vCenter server with embedded PSC
After completion

From this point the migration is similar to other migrations and updates

Deploy the OVA

Run it

Select Migrate instead of update

Follow the similar prompts in the wizard

Known Issues

Upgrading vCenter Server can cause an issue with lifecycle manager

Unexpected error!

Solution

Reset Lifecycle Manager database

How?

vCenter Shell

Stop the Lifecyle manager

```
service-control --stop vmware-updatemgr
```
Navigate to the VMware lifecycle (update) manager and reset-db
```
/usr/lib/vmware-updatemgr/bin/updatemgr-utility.py reset-db
rm -rf /storage/updatemgr/patch-store/*
```
Start the manager again
```
service-control --start vmware-updatemgr
```
Re-authenticate and verify fix

Conclusions

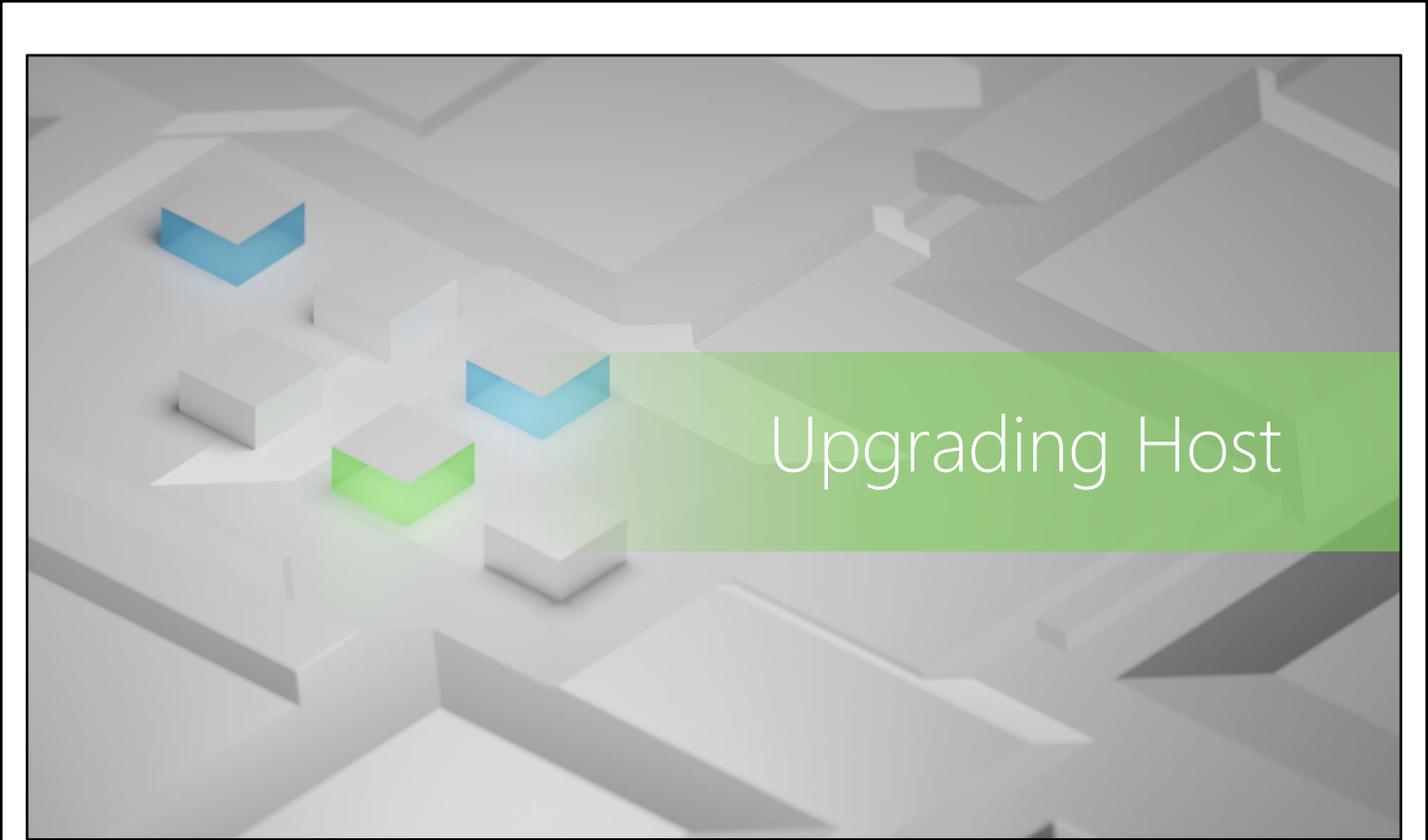## VCSA Upgrade Process

Overview Of Process

Requirements

Post Configuration

Migration

Upgrading Host

Next Step

You've finished updating the vCenter Server	Now it's time to update your ESXi hosts
Updating out of order can lead to:	Data loss Access loss
Methods for interactive updating:	External Disk Scripted upgrade CLI vSphere Lifecycle Manager

Hardware Compatibility

Compatibility Matrix	https://www.vmware.com/resources/compatibility/sim/interop_matrix.php
👍👎	Reference the compatibility matrix Confirms what hardware will work

Key points	Min. 2 CPUs NX/XD bit enabled in bios 4 GB physical RAM Better to have 8 GB Support for hardware virtualization SCSI Disk / non network RAID LUN
🔑	

Storage issues

Not enough disk space on the host?

Provision more as needed before hand

Not enough space for logs locally?

NAS Datastore
NFS Datastore

SAN

Remove fiber channel system before upgrade

Storage issues

Pro-Tips:

Back up everything

VMs & hosts need to power off occasionally during updates

Don't risk losing data

Remote Management Server Models

Server Model	Firmware Version	Java
Dell DRAC 7	1.30.30 (Build 43)	1.7.0_60-b19
Dell DRAC 6	1.54 (Build 15), 1.70 (Build 21)	1.6.0_24
Dell DRAC 5	1.0, 1.45, 1.51	1.6.0_20,1.6.0_203
Dell DRAC 4	1.75	1.6.0_23
HP ILO	1.81, 1.92	1.6.0_22, 1.6.0_23
HP ILO 2	1.8, 1.81	1.6.0_20, 1.6.0_23
HP ILO 3	1.28	1.7.0_60-b19
HP ILO 4	1.13	1.7.0_60-b19
IBM RSA 2	1.03, 1.2	1.6.0_22

ESXi ISO image

Download the installer .ISO image

You can use:

CD

DVD

USB

Network boot

FCoE

I/O Choices

Boot process	Disconnect network storage	Insert external drive	Have BIOS boot from the external drive	Select where you want the upgrade for ESXi	F11	Eject external drive	Reboot host	First boot device should be one used for upgrade
	Not the LUN that has ESXi installation	Restart machine						

Example: Startup Script

Use startup scripts for the installation

In the ESXI installer window
Shift + O → Edit Boot Options

Boot Command

Ks = installation script location + additional
Ex: `ks = http://somefilepath.cfg`
`nameserver = , netmask = , gateway =`

After Installation
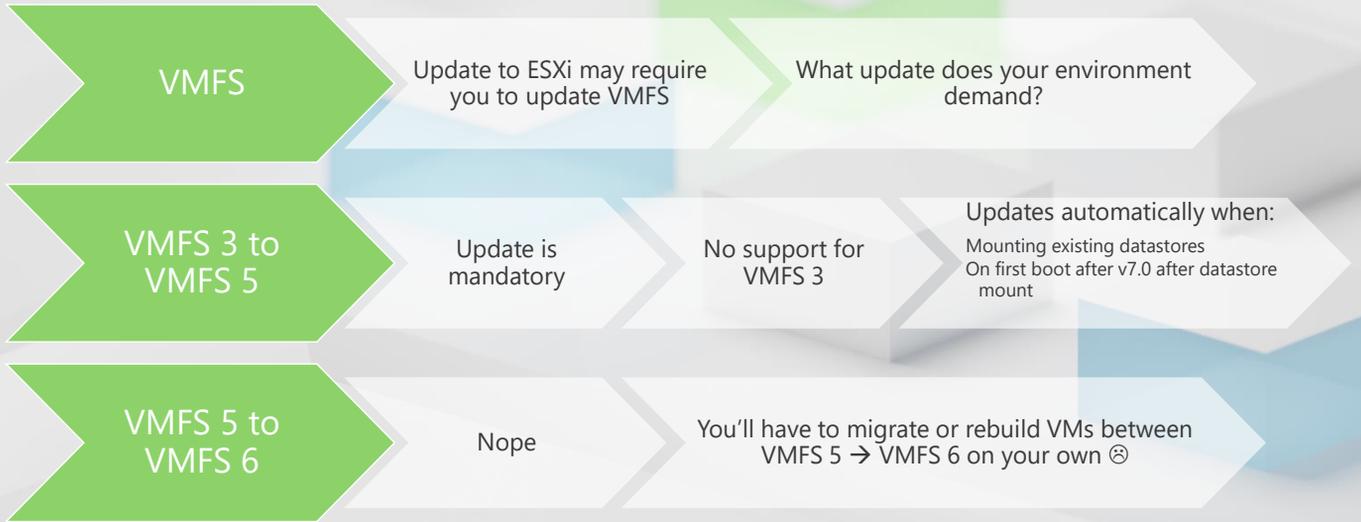
1. View the upgrade logs
2. Reconnect to vCenter Server
3. Host will remain in evaluation mode for 60 days
4. Update licenses as needed
5. Upgrade VMs

Upgrading your Datastore

|		
VMFS	Update to ESXi may require you to update VMFS	What update does your environment demand?
VMFS 3 to VMFS 5	Update is mandatory	No support for VMFS 3	**Updates automatically when:** Mounting existing datastores / On first boot after v7.0 after datastore mount
VMFS 5 to VMFS 6	Nope	You'll have to migrate or rebuild VMs between VMFS 5 → VMFS 6 on your own ☹

Conclusions

Host Upgrade Process

Compatibility

Storage

ISO image

Scripts

Datastore upgrades
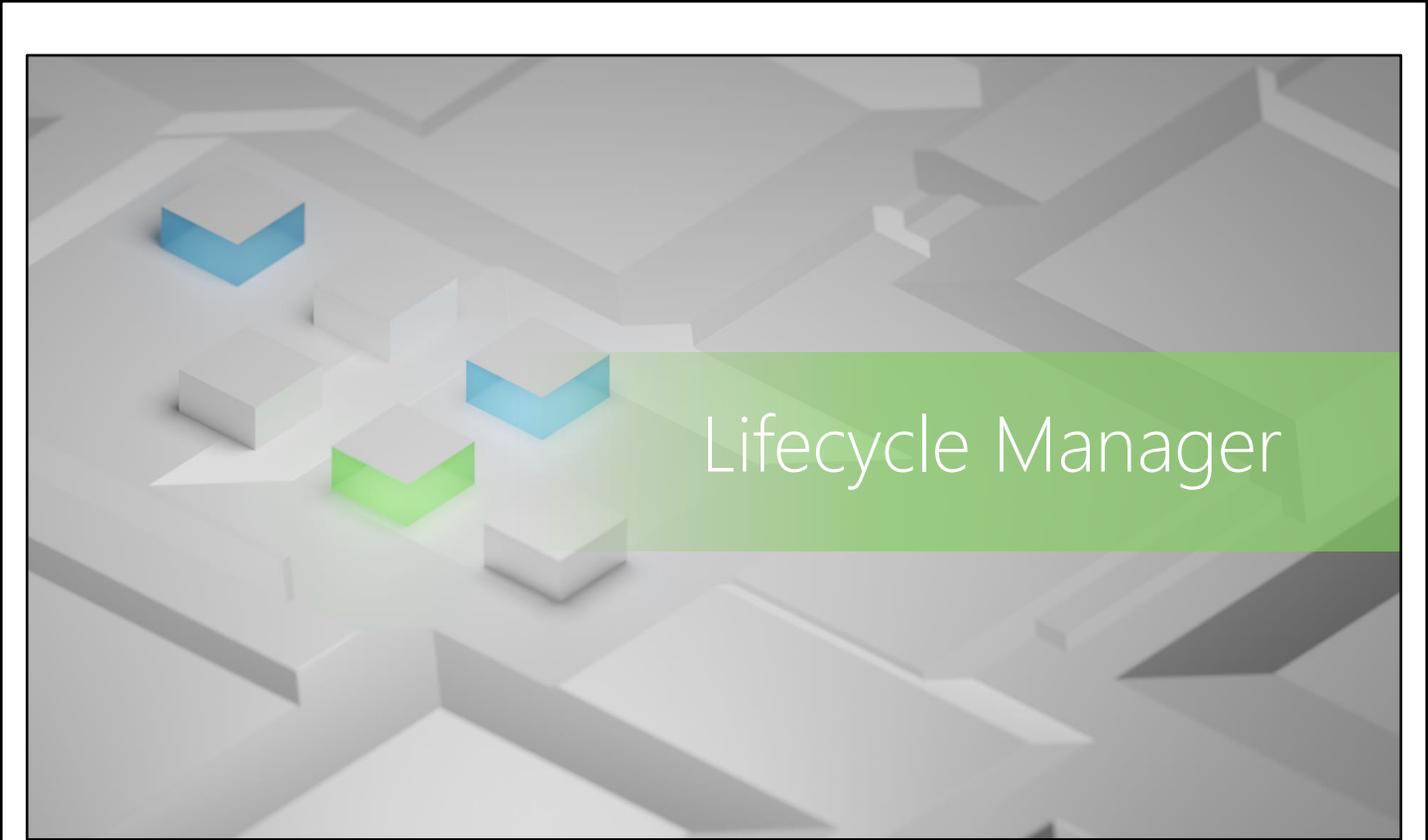
Lifecycle Manager

Lifecycle Manager

How updating used to be:

Manual

Challenging

Time consuming

- Staging patch files
- Install and reboot commands
  - Individually completed

Update Manager

Introduced 2007

Automates these processes

Rebrand:

vLCM – vSphere Lifecycle Manager

Maintains same functionality of Update Manager

Adds new tools

- Manages patching
- Full firmware lifecycle

Lifecycle Manager

Lifecycle Management

Not enough to just update patches
Hardware updates needed to accommodate software updates
Desired state model
Updates server firmware
     Provided by OEMs

Lifecycle Manager Improvements

New Features

Cluster software management

Think declarative configurations

You tell the system where it needs to be

Define a "golden" image

Think of it as documentation

All hosts "check in" with the documentation

Where are they different?

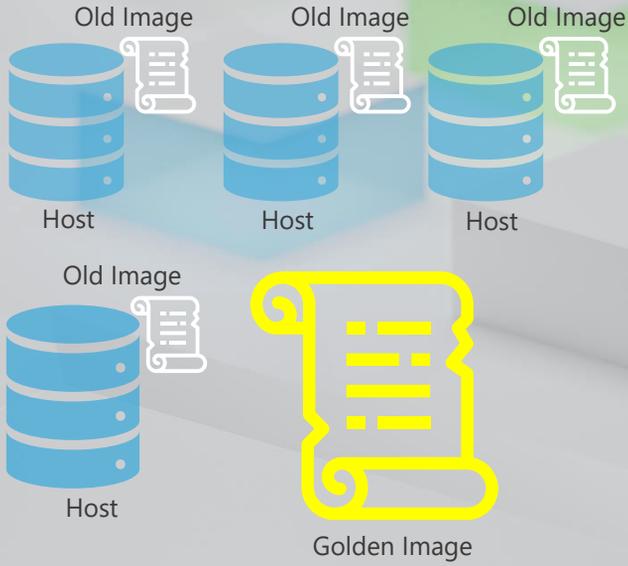Fix themselves until they match the image

Hardware verification

VMware compatibility guide vs. vSAN HCL
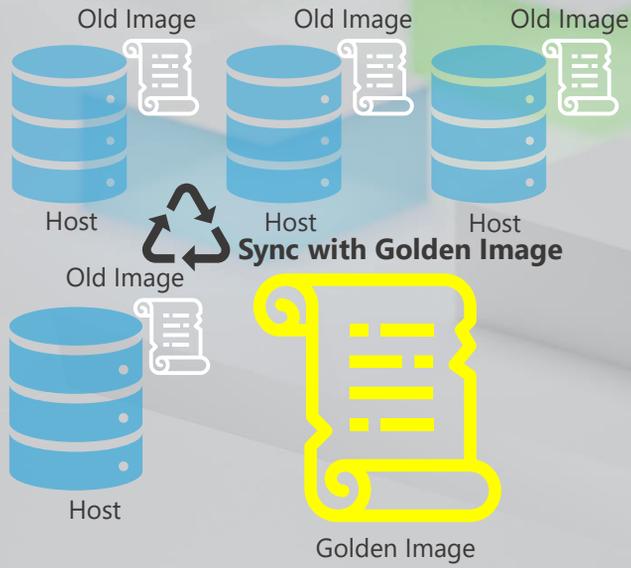
Automated Firmware patches
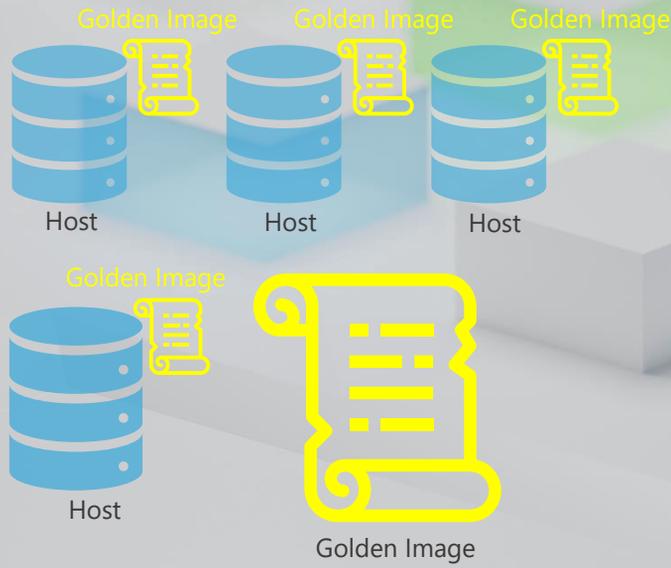
Lifecycle Manager Improvements

Old Image

Host

Old Image

Host

Old Image

Host

Sync with Golden Image

Old Image

Host

Golden Image

Lifecycle Manager Improvements

Using the Lifecycle Manager

Define the "golden" image

Cluster configuration page
Enable ➔ Manage all hosts in the cluster with a single image
Select an ESXi version
Everything else is optional
  Vendor
  Addon

After configuring and saving the cluster:

Cluster compliance is checked against the image
If not compliant
  Lifecycle manager lists these hosts
  Lists why they are not compliant

Using the Lifecycle Manager

Finish Image Set-Up

Image configuration is saved to the cluster

Cluster having an issue?

Remediate cluster to the image again
>   Check remediation impact summary

Exporting an image

JSON
ISO
ZIP

Host Hardware Compatibility

Verify host hardware compatibility
- Compares VCG and vSAN HCL

Run a compatibility check

Sync Updates

Sync with the HCL

Upgrade Suite Lifecycle Manager

Download the upgrade .iso file

Upgrade managed in vRealize Suite
- Lifecycle operations ➜ Settings

System Upgrade
- Select a repository type
- Specify location

Check for upgrade

Select an upgrade

Install upgrades
- .iso file

In vRealize Manger UI
- Settings ➜ System Upgrade

Known Issues

Upgrading vCenter Server can cause an issue with lifecycle manager

Unexpected error!

Solution

Reset Lifecycle Manager database

How?

vCenter Shell

Stop the Lifecyle manager

```
service-control --stop vmware-updatemgr
```
Navigate to the VMware lifecycle (update) manager and reset-db
```
/usr/lib/vmware-updatemgr/bin/updatemgr-utility.py reset-db
rm -rf /storage/updatemgr/patch-store/*
```
Start the manager again
```
service-control --start vmware-updatemgr
```
Re-authenticate and verify fix

Conclusions

Lifecycle Manager

Improvements

Using lifecycle manager

Host compatibility

Known issues