

Waiting Room :



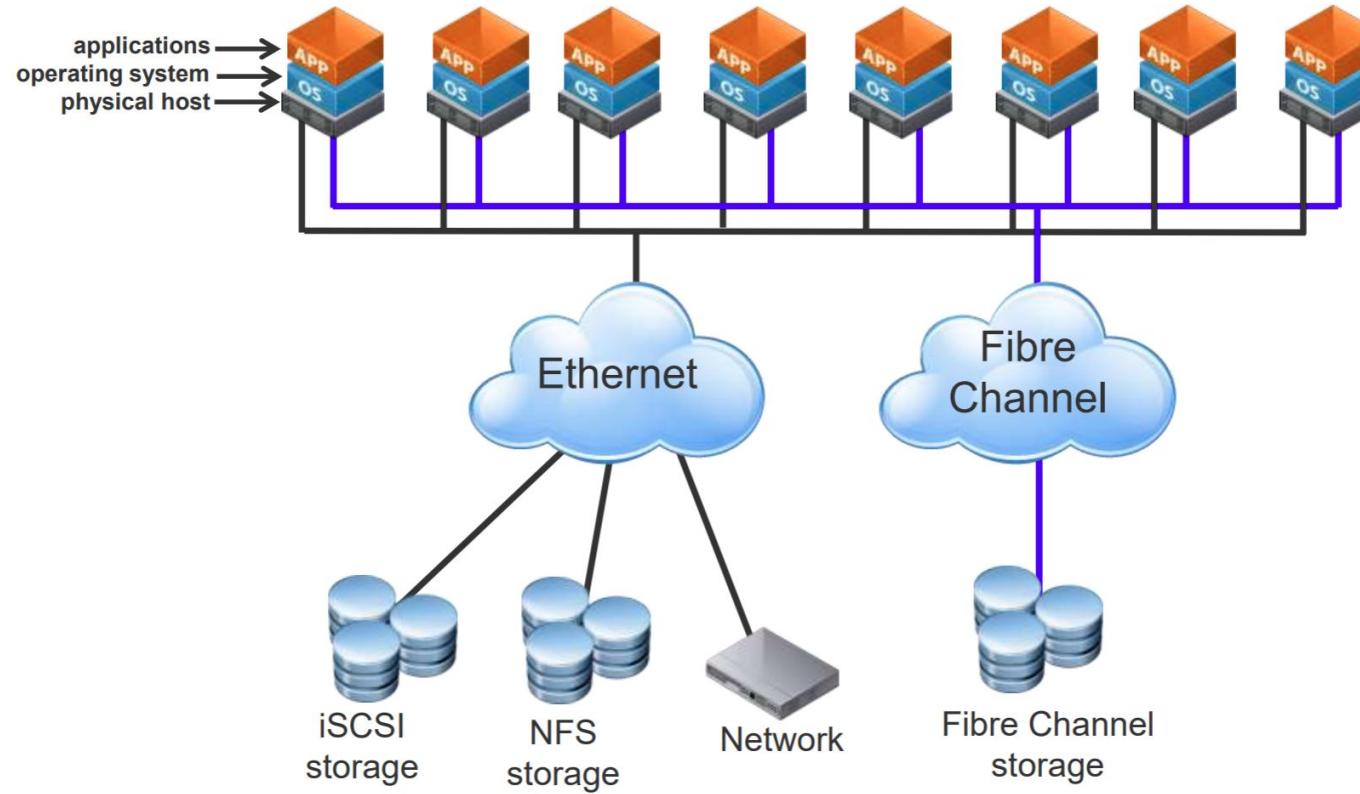
Introduction to VMware vsphere software tools

Module 5

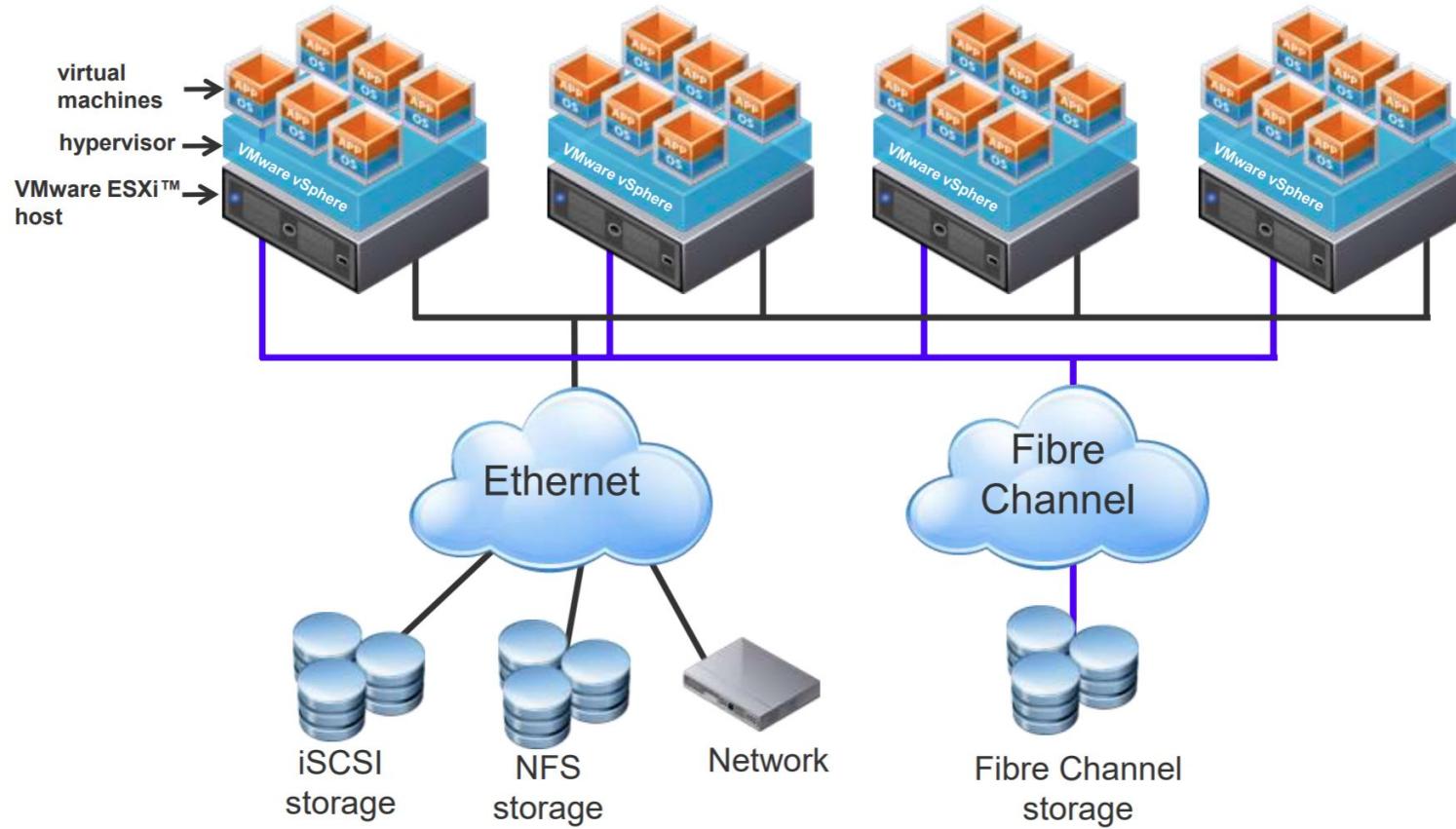
Importance

Virtualization technology has revolutionized the computer industry by lowering capital and operational costs, providing higher service availability, and providing new data protection mechanisms. This module introduces core virtualization concepts and VMware vSphere®.

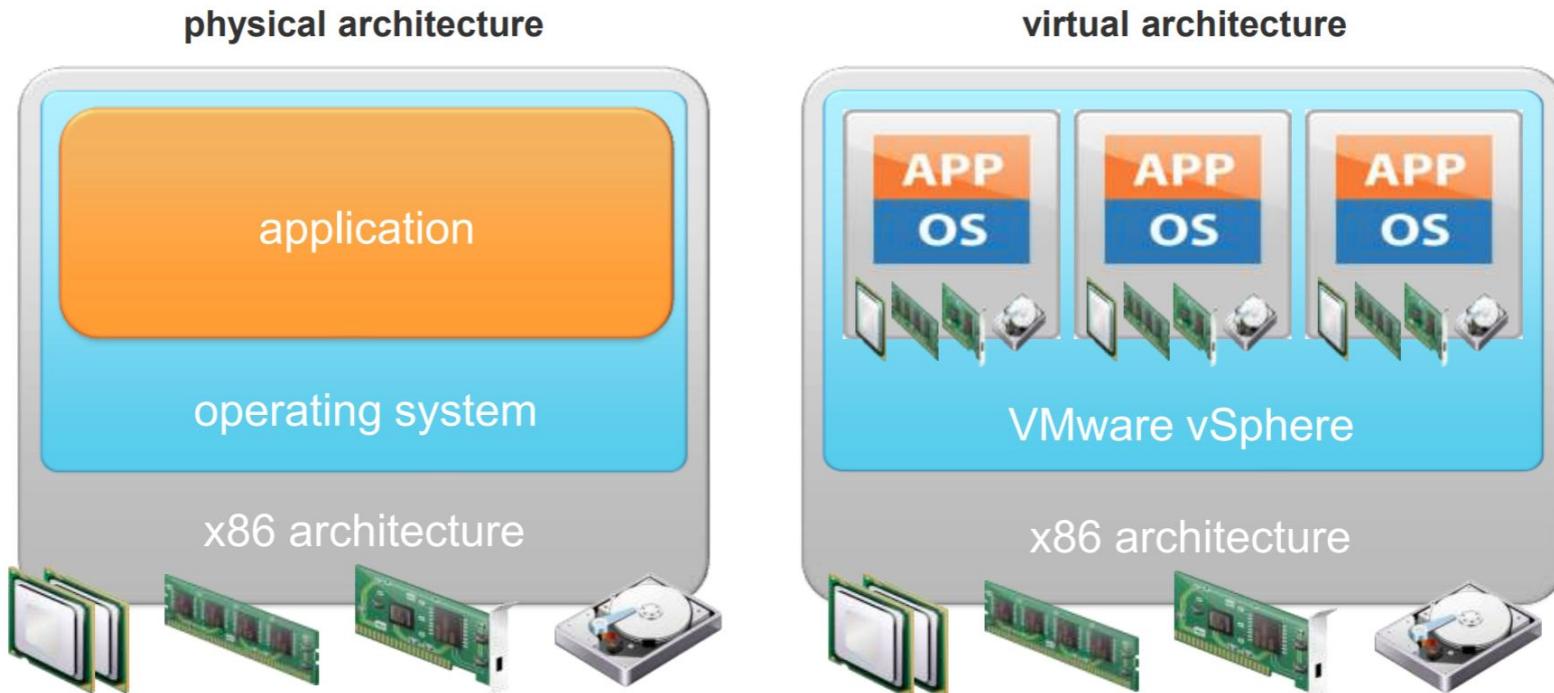
Physical Infrastructure



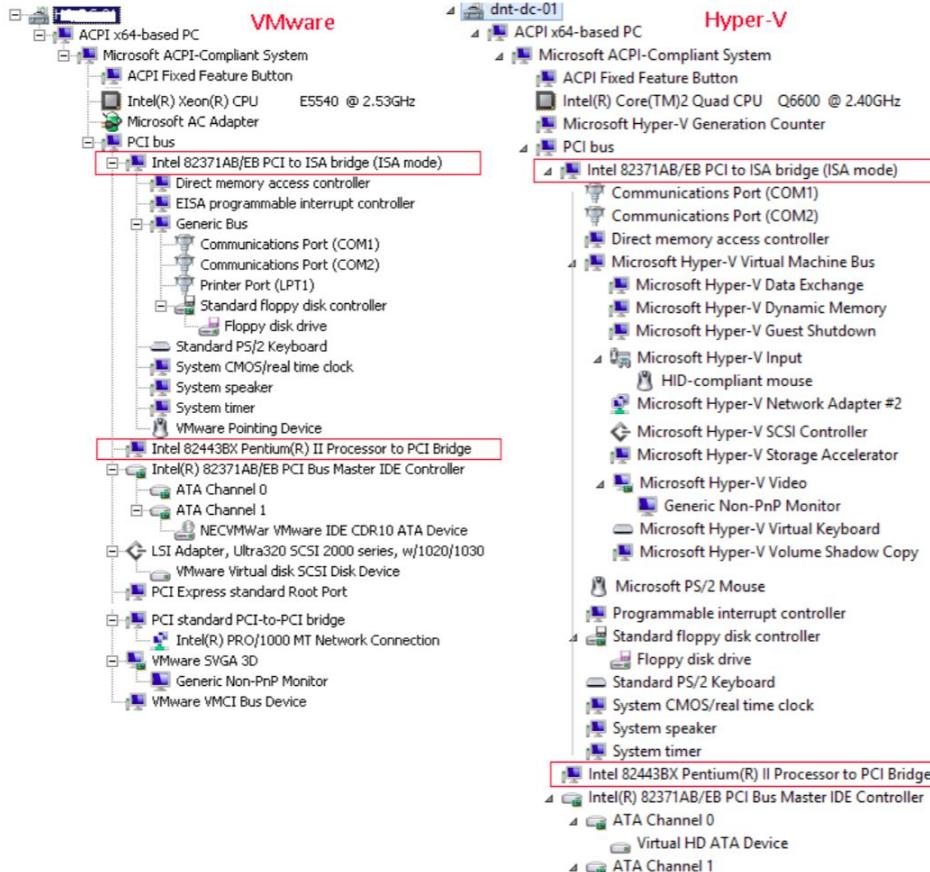
Virtual Infrastructure



Physical Versus Virtual Architecture



Hypervisor device emulation



Why Use Virtual Machines?

Physical machine

Difficult to move or copy
Bound to a specific set of hardware components
Often has a short life cycle
Requires personal contact to upgrade hardware



Virtual machine

Easy to move and copy:

- Encapsulated into files
- Independent of physical hardware

Easy to manage:

- Isolated from other virtual machines
- Insulated from hardware changes

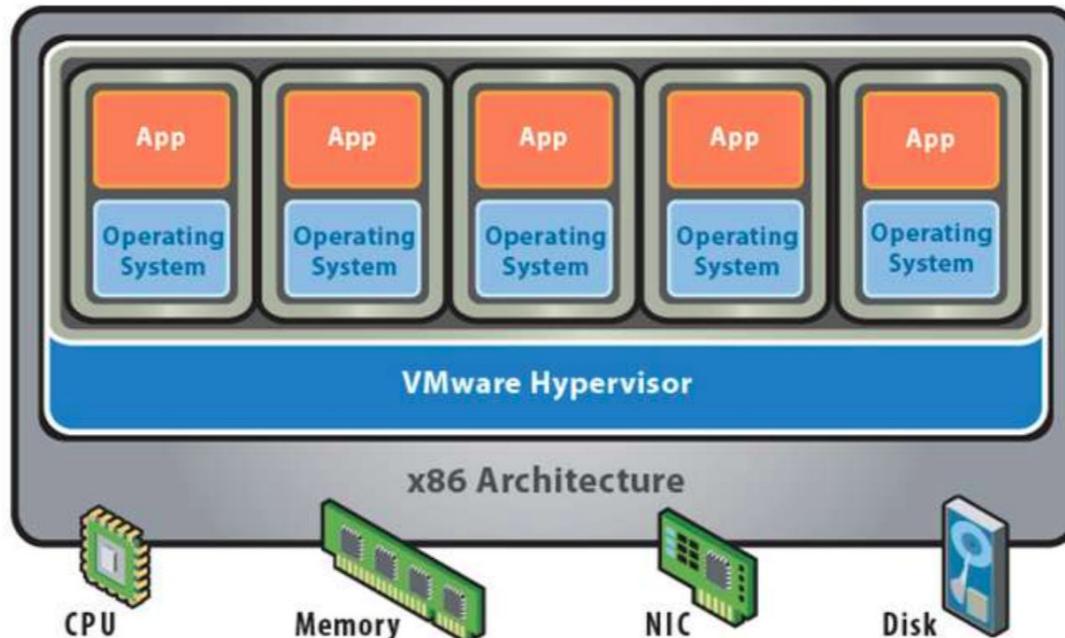
Provides the ability to support legacy applications

Allows servers to be consolidated



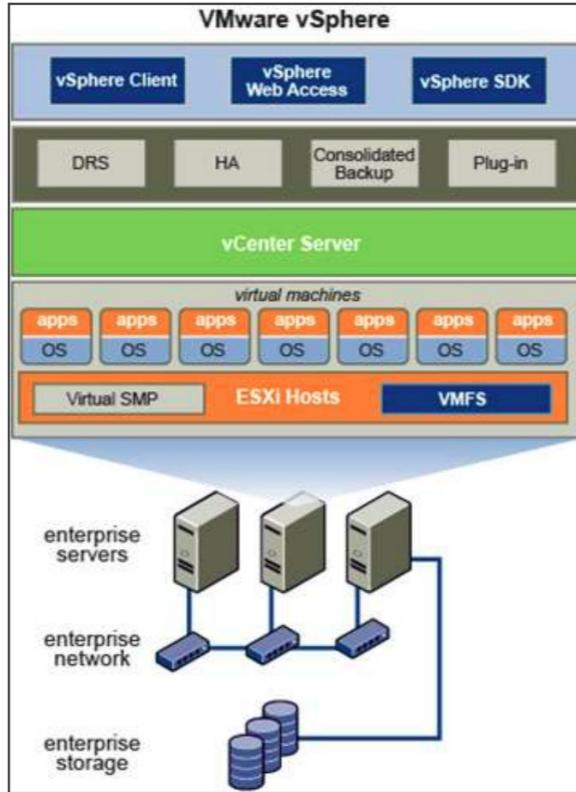
Virtualization Using a Bare-Metal Hypervisor

A bare-metal hypervisor system does not require an operating system. The hypervisor *is* the operating system.



ESXi uses a hypervisor architecture.

What Is VMware vSphere?

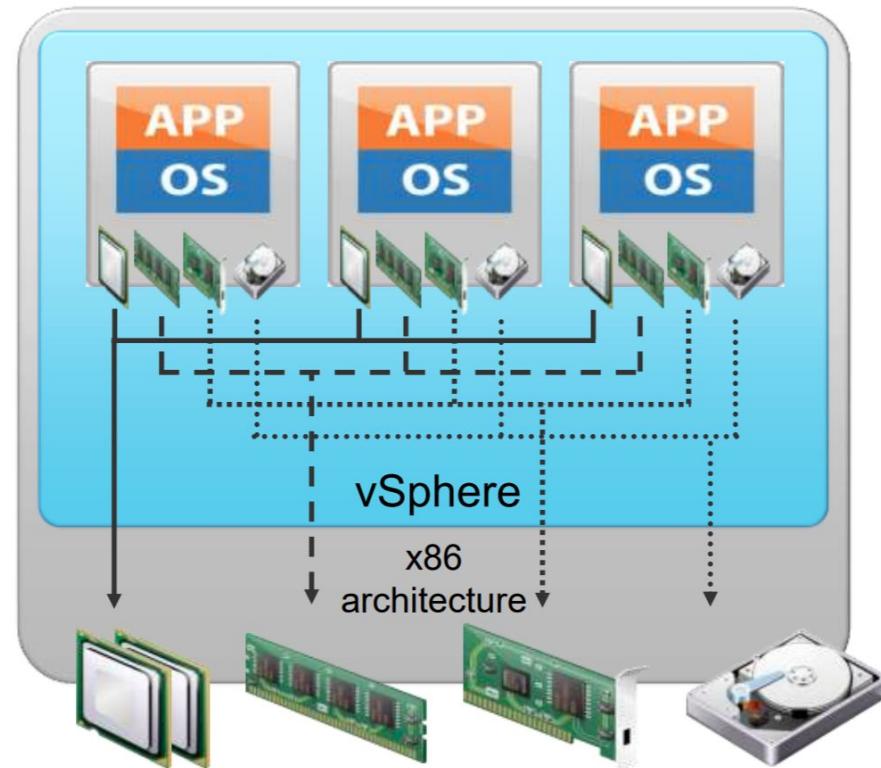


An infrastructure virtualization suite that provides virtualization, management, resource optimization, application availability, and operational automation capabilities

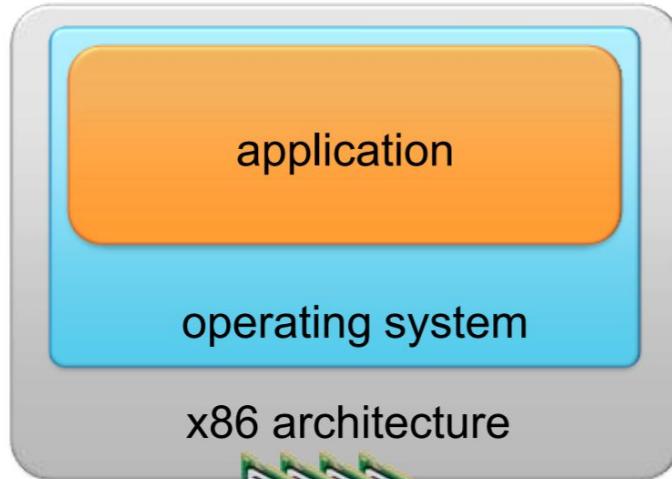
It consists of the following components:

- VMware ESXi
- VMware vCenter Server™
- VMware vSphere® Client™
- VMware vSphere® VMFS
- VMware vSphere® Virtual Symmetric Multiprocessing

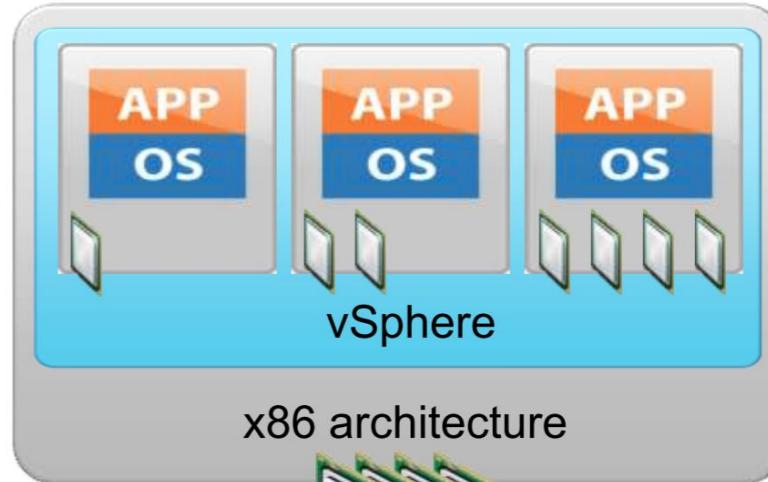
Resource Sharing



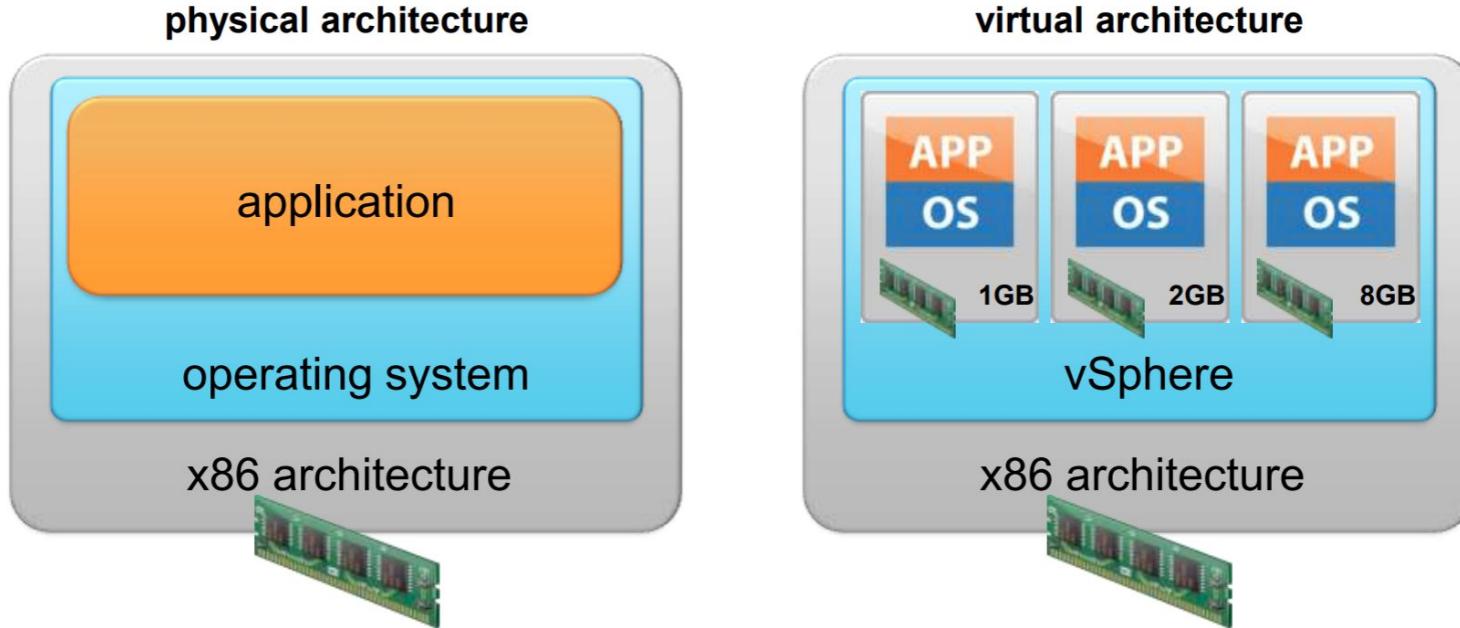
physical architecture



virtual architecture



Physical and Virtualized Host Memory Usage



About Virtual Machines



A virtual machine is a software computer that, like a physical computer, runs an operating system and applications.

Virtual Machine



Virtual Machine Components

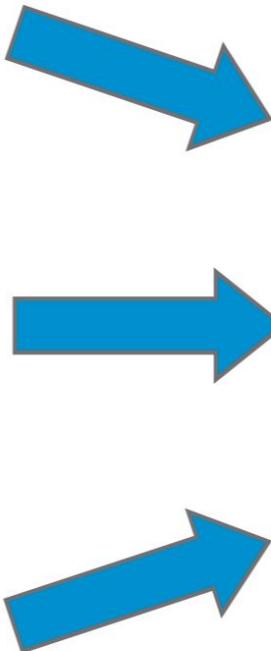
- Operating system
- VMware Tools™
- Virtual resources such as:
 - CPU and memory
 - Network adapters
 - Disk controllers
 - Parallel and serial ports

Encapsulation

VEPSUN



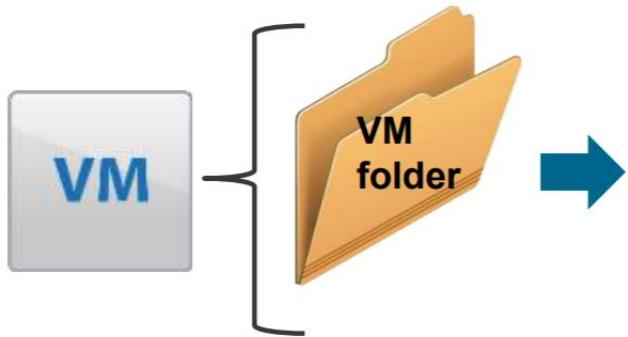
Virtual machine files are stored in directories on a VMFS or NFS datastore.



Datastore: VMFS or NFS

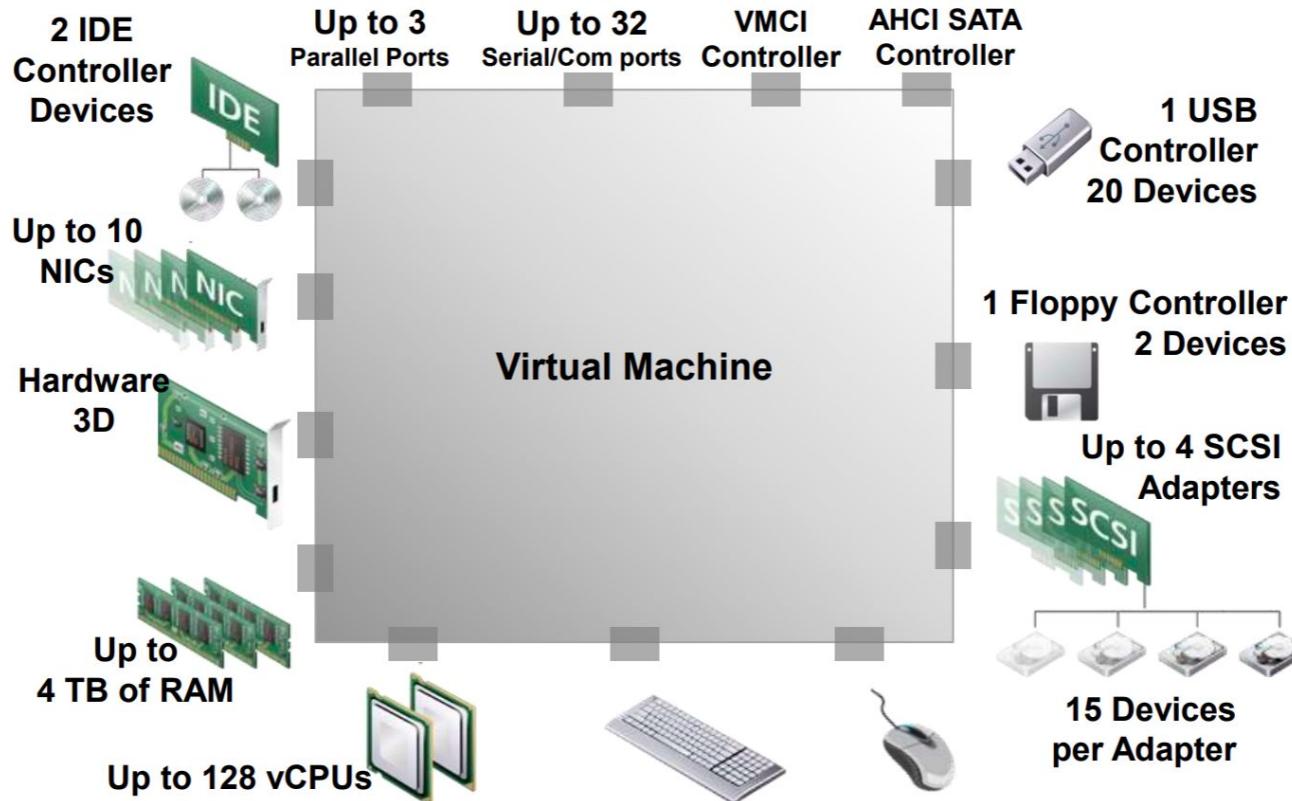
About Virtual Machine Files

A virtual machine consists of a set of related files.



Configuration file	<code>VM_name.vmx</code>
Swap files	<code>VM_name.vswp</code> <code>vmx-VM_name.vswp</code>
BIOS file	<code>VM_name.nvram</code>
Log files	<code>vmware.log</code>
Template file	<code>VM_name.vmtx</code>
Raw device map file	<code>VM_name-rdm.vmdk</code>
Disk descriptor file	<code>VM_name.vmdk</code>
Disk data file	<code>VM_name-flat.vmdk</code>
Suspend state file	<code>VM_name.vmss</code>
Snapshot data file	<code>VM_name.vmsd</code>
Snapshot state file	<code>VM_name.vmsn</code>
Snapshot disk file	<code>VM_name-delta.vmdk</code>

About Virtual Machine Virtual Hardware



A virtual machine must have a vCPU and virtual memory. The addition of other virtual devices makes the virtual machine more useful.

CD/DVD drive:

- Connect to CD, DVD, or ISO image.

USB 3.0:

- Smart-card readers

Floppy drive:

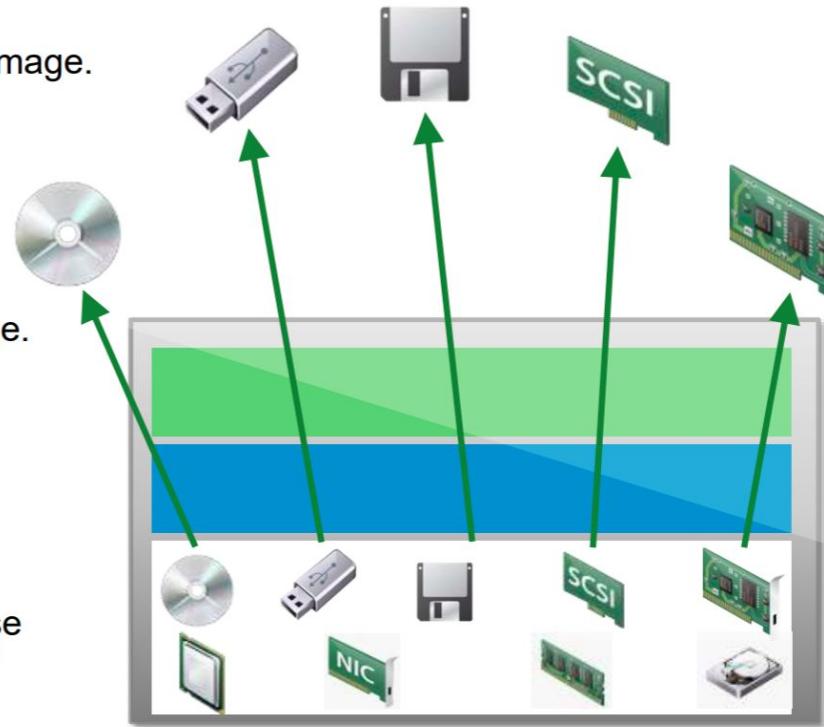
- Connect a virtual machine to a floppy drive or a floppy image.

Generic SCSI devices:

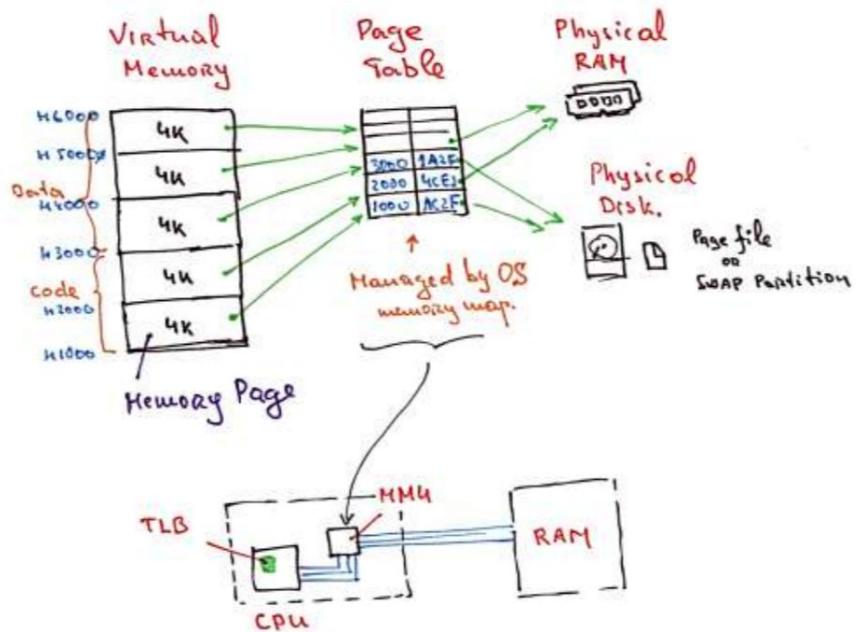
- A virtual machine can be connected to additional SCSI adapters.

vGPUs:

- Enable a virtual machine to use GPUs on the physical host for high-computation activities.

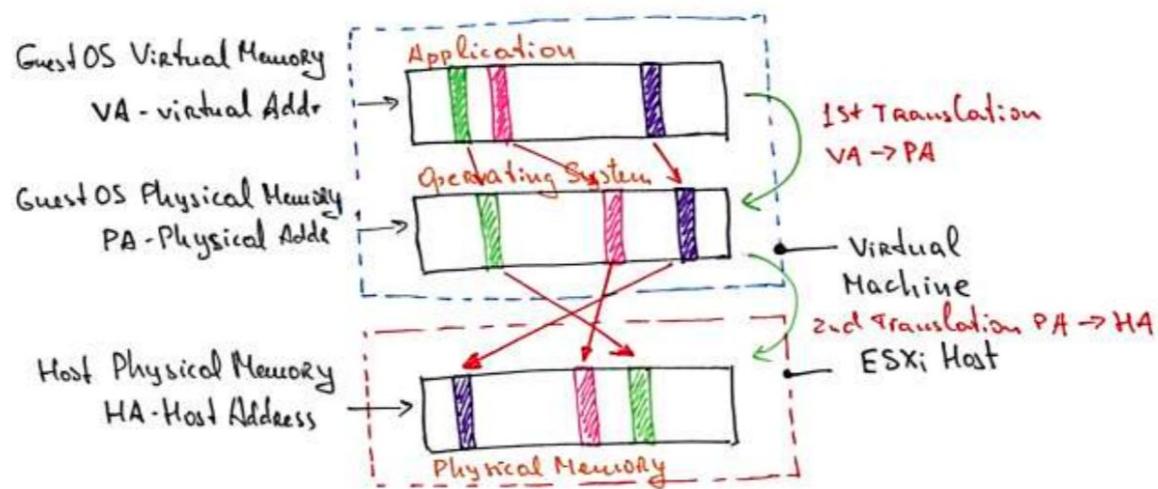


Virtual Memory Concept



MMU - Memory Management Unit
TLB - Translation Lookaside Buffer (MMU Cache)

Hypervisor Memory Virtualization

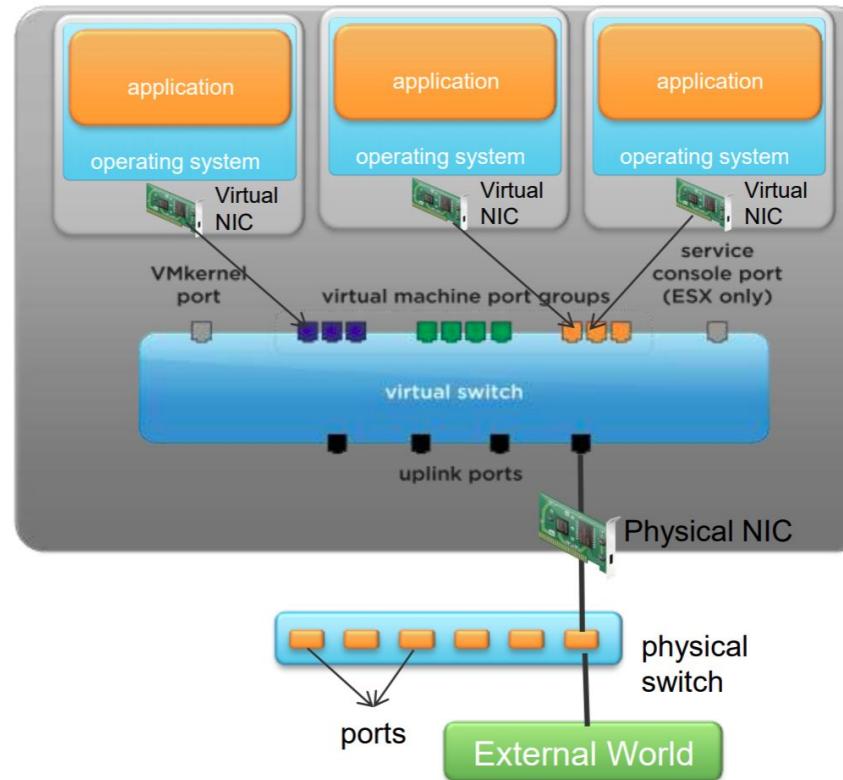


What Is a Virtual Network? What Is a Virtual Switch?

A virtual network provides the networking for hosts and virtual machines that use virtual switches.

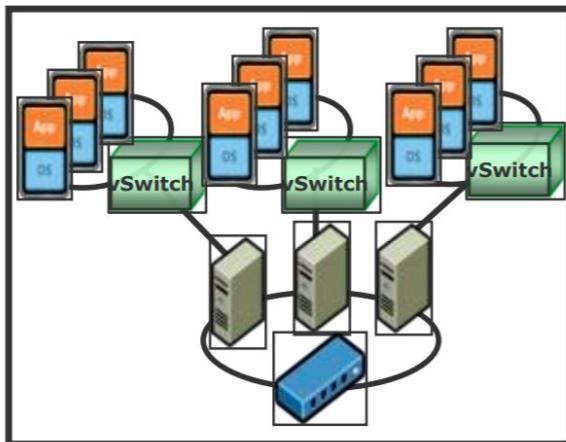
A virtual switch:

- Directs network traffic between virtual machines and links to external networks.
- Combines the bandwidth of multiple network adapters and balances traffic among them. It can also handle physical network interface card (NIC) failover.
- Models a physical Ethernet switch:
 - A virtual machine's NIC can connect to a port.
 - Each uplink adapter uses one port.

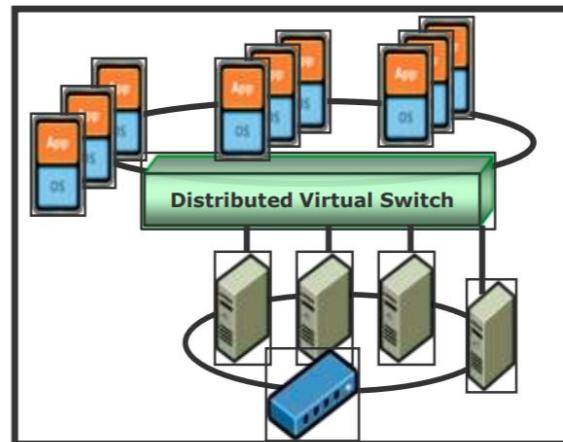


Benefits of distributed switches over standard switches:

- Simplify datacenter administration
- Provide support for private VLANs, Port mirroring, Netflow, Network I/O Control
- Enable networking statistics and policies to migrate with virtual machines during a migration using VMware vMotion™
- Provide for customization and third-party development



standard switches



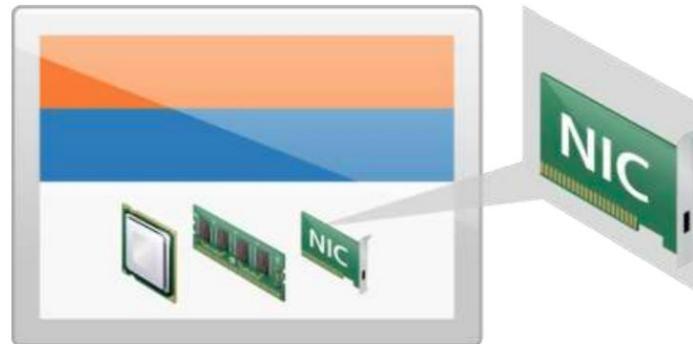
distributed switches

About Network Adapters

When you configure a virtual machine, you can add network adapters (NICs) and specify the adapter type. Whenever possible, select VMXNET3.

Supported network adapter types:

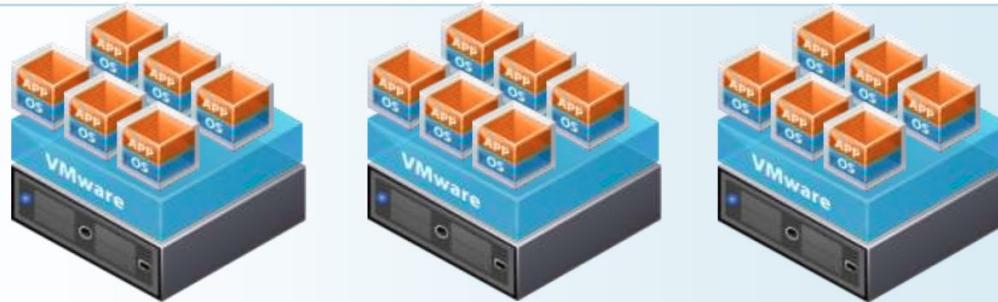
- Flexible: Can function as either a Vlance or VMXNET adapter.
- E1000-E1000E: High-performance adapter available for only some guest operating systems.
- VMXNET, VMXNET2, and VMXNET3 are VMware drivers that are available only with VMware Tools.
- SR-IOV passthrough: The virtual machine and the physical adapter exchange data without using the VMkernel as an intermediary.
 - Limited guest operating system support



virtual machine

vSphere Storage Choices

ESXi hosts



datastore
types

VMware vSphere VMFS

NFS



File
system

storage
technology

Direct
Attached

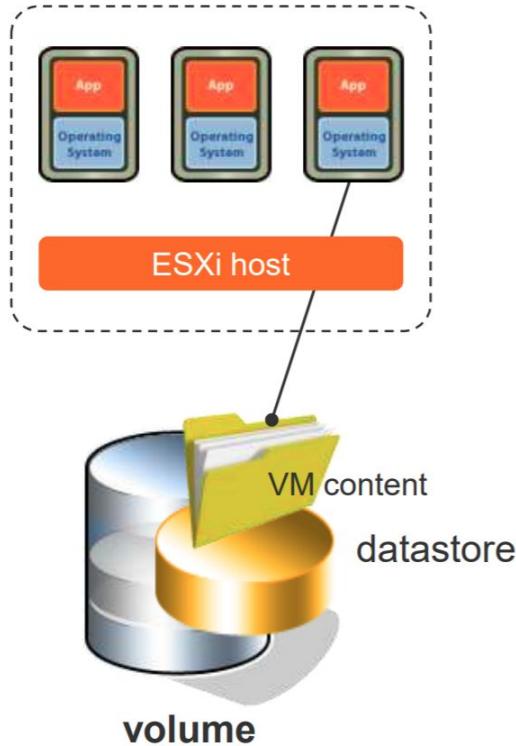
Fibre
Channel

FCoE

iSCSI

NAS

VMFS and NFS Datastores



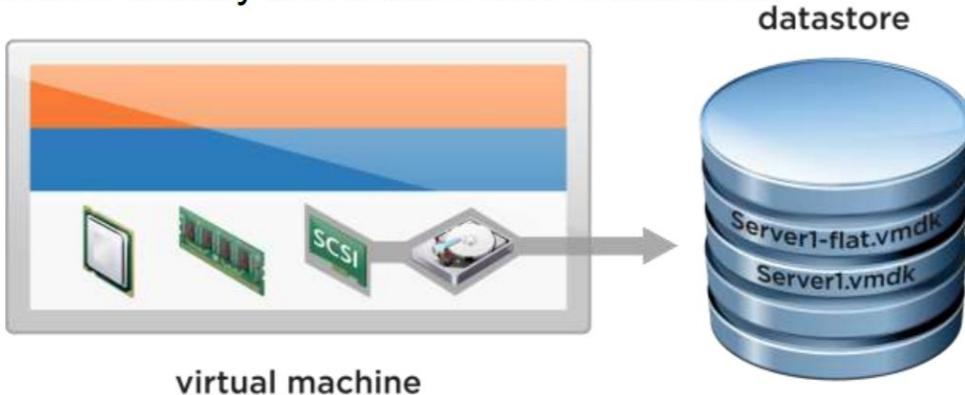
A datastore is a logical storage unit, which can use disk space on one physical device or one disk partition, or span several physical devices.

Types of datastores:

- VMFS
- Network File System (NFS)

Datastores are used to hold virtual machines, templates, and ISO images.

A virtual machine usually has at least one virtual disk.



Sample virtual disk definition:

Virtual disk size:	8 GB
Datastore:	MyVMFS
Virtual disk node:	0:0
Virtual storage adapter:	LSI Logic SAS
Virtual disk files:	Server1.vmdk and Server1-flat.vmdk
Default disk mode:	Snapshots allowed
Optional disk mode:	Independent: Persistent or Nonpersistent
Disk provisioning policy:	Thick Provision Lazy Zeroed, Thick Provision Eager Zeroed, or Thin Provision

About Thin-Provisioned Virtual Disks

Thin provisioning enables virtual machines to use storage space as needed:

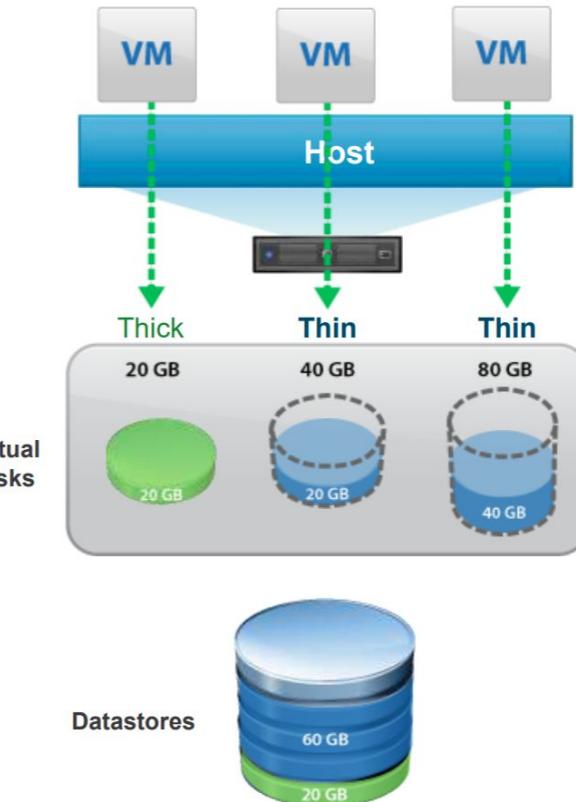
- Thin-provisioned virtual machine disks consume only the capacity needed to hold the current files.
- A virtual machine sees the full allocated disk size at all times.

You can mix thick and thin formats.

Full reporting and alerts help manage allocations and capacity.

More efficient use of storage:

- Virtual disk allocation: 140 GB
- Available datastore capacity: 100 GB
- Used storage capacity: 80 GB



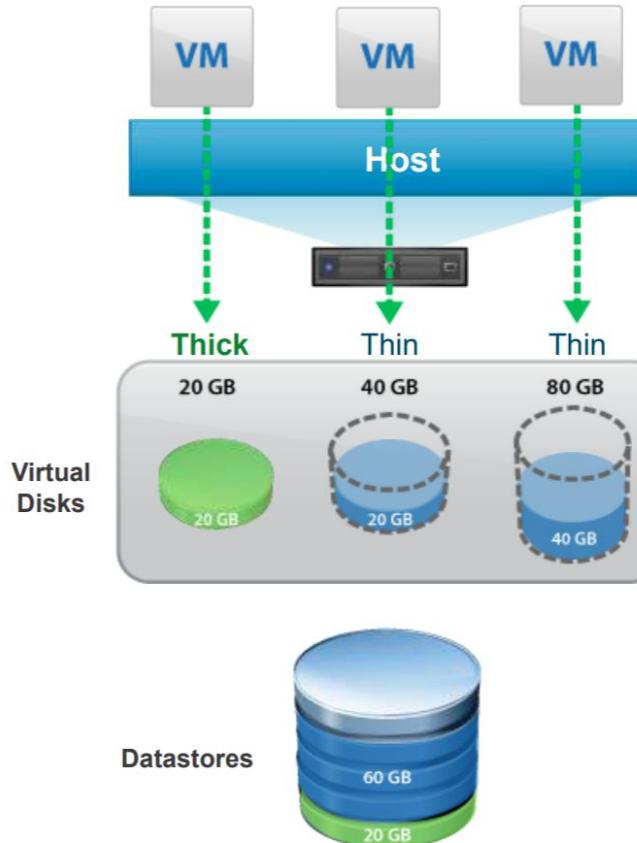
About Thick-Provisioned Virtual Disks

Thick provisioning uses all the defined disk space at the creation of the virtual disk:

- Virtual machine disks consume all the capacity, as defined at creation, regardless of the amount of data in the guest operating system file system.

Eager zeroed or lazy zeroed:

- Every block in an eager zeroed thick-provisioned disk is prefilled with a zero.
- Every block in a lazy zeroed thick-provisioned disk is filled with a zero when data is written to the block.

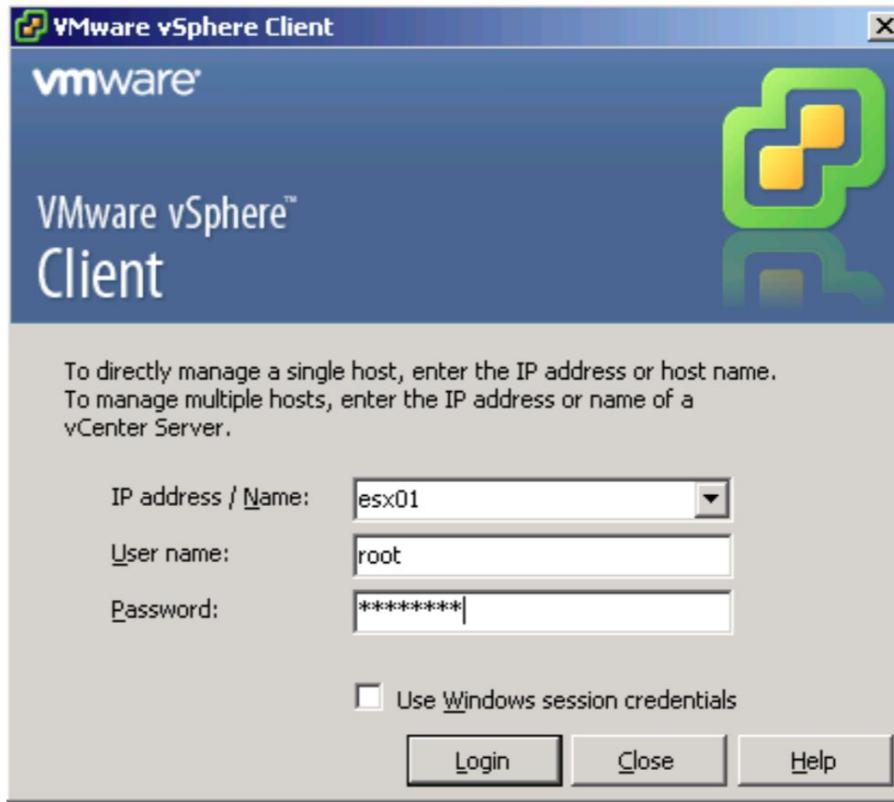


Management Made Easy

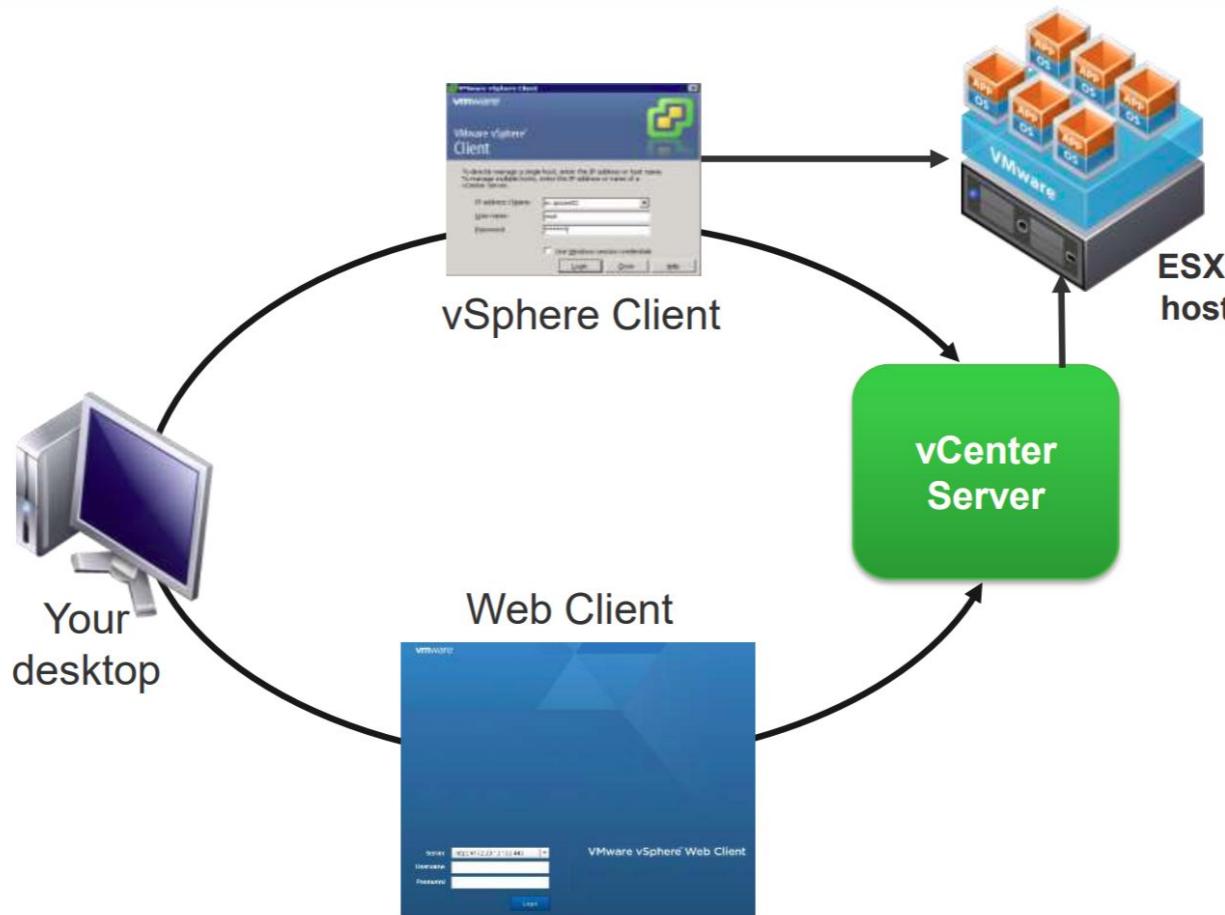
The vSphere Client allows you to centrally manage your vSphere environment.

At the login screen, enter:

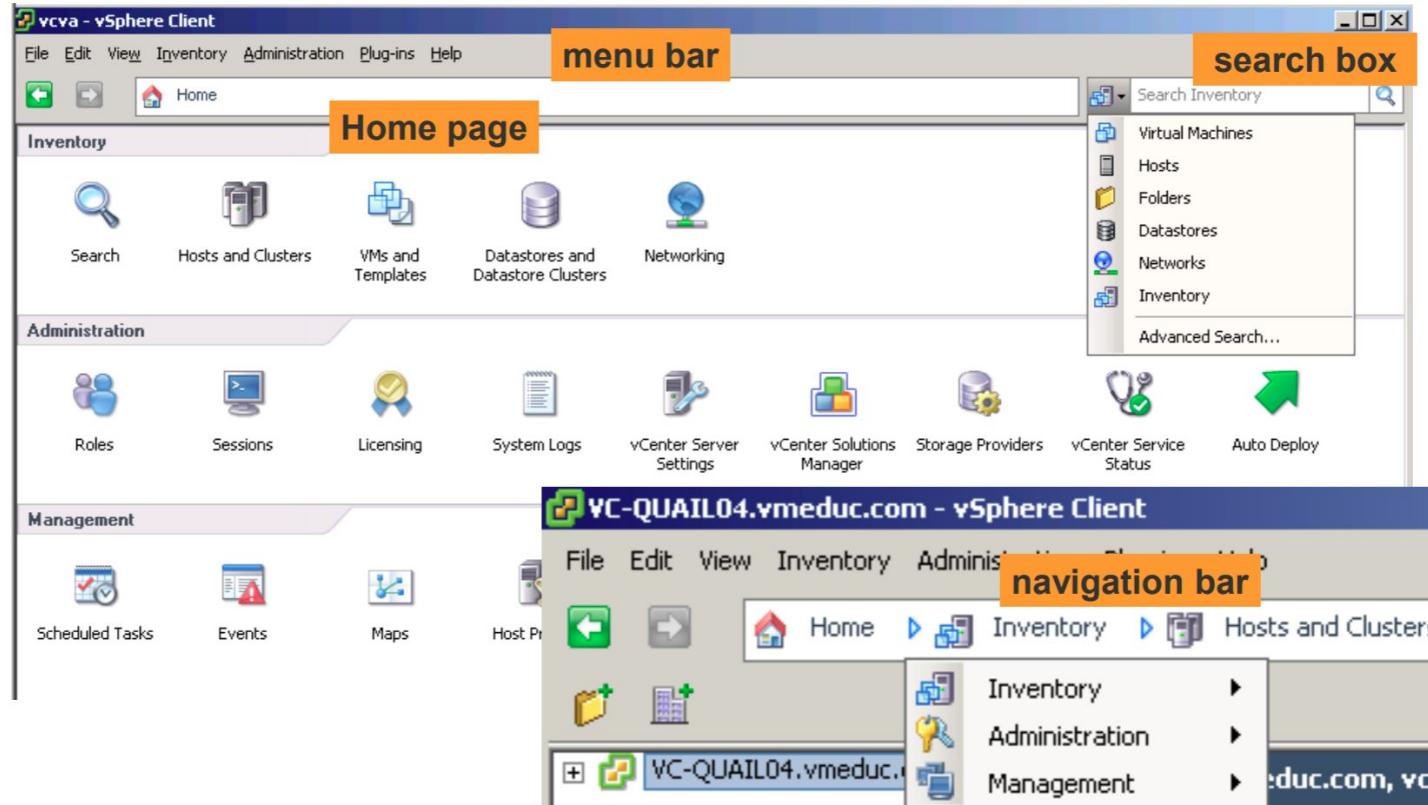
- Host name or IP address of the vCenter Server system
- Windows user and password



User Interfaces



Navigating the vSphere Client



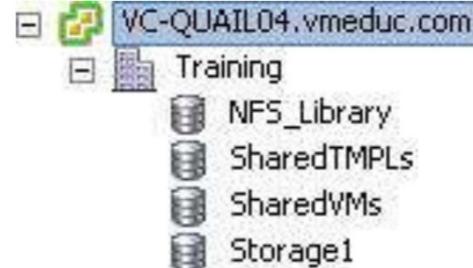
Viewing vCenter Server Inventory

The vCenter Server inventory panels organize objects into a hierarchy.

Hosts and Clusters



Datastores



VMs and Templates

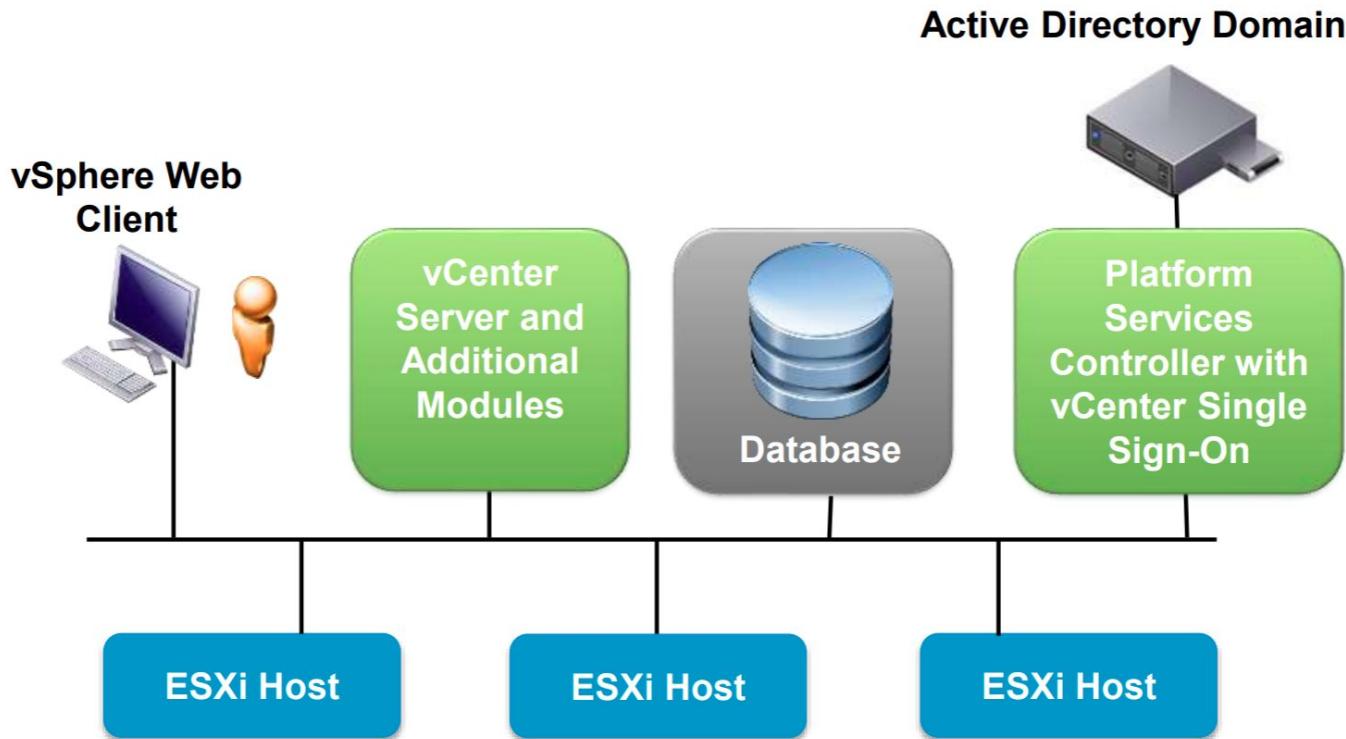


Networks



vCenter Server Architecture

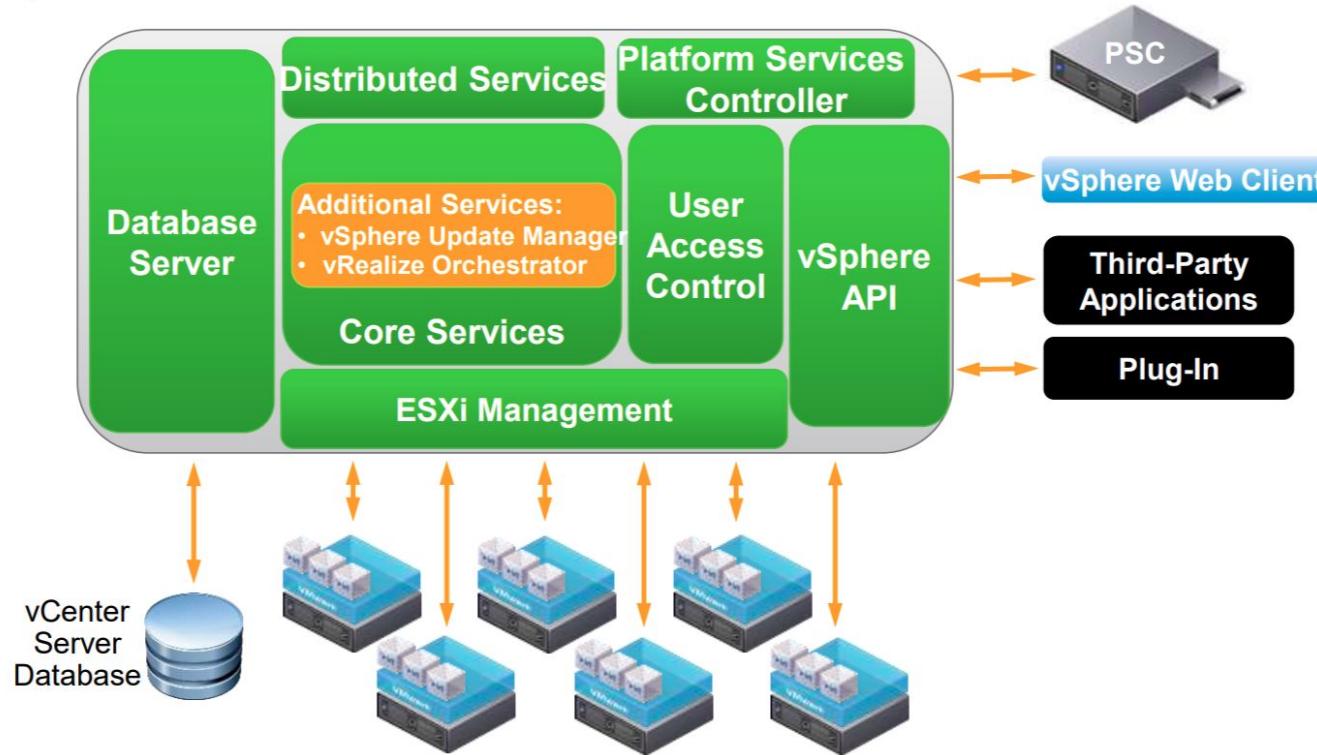
The diagram shows the supporting components for vCenter Server.



Additional vCenter Server Services and Interfaces



vCenter Server has additional services and interfaces that provide important functions.



Platform Service Controller

Briefing the concept of Single sign on -----

Overview

Platform Services Controller (PSC) is a component of the VMware Cloud Infrastructure Suite. PSC deals with identity management for administrators and applications that interact with the vSphere platform.

Key Features and Advantages:

- PSC 6.0 remains a multi-master model, as was introduced in vSphere 5.5 in the form of vCenter Single Sign-On.

What is single sign on ?? and How
does single sign-on work?

What is single sign-on?

Single sign-on (SSO) is an authentication method that enables users to securely authenticate with **multiple applications and websites by using just one set of credentials.**

How does SSO [Single - sign -on] work?

SSO works based upon a trust relationship set up between an application, known as the service provider, and an identity provider, like **OneLogin**. This trust relationship is often based upon a certificate that is exchanged between the identity provider and the service provider.

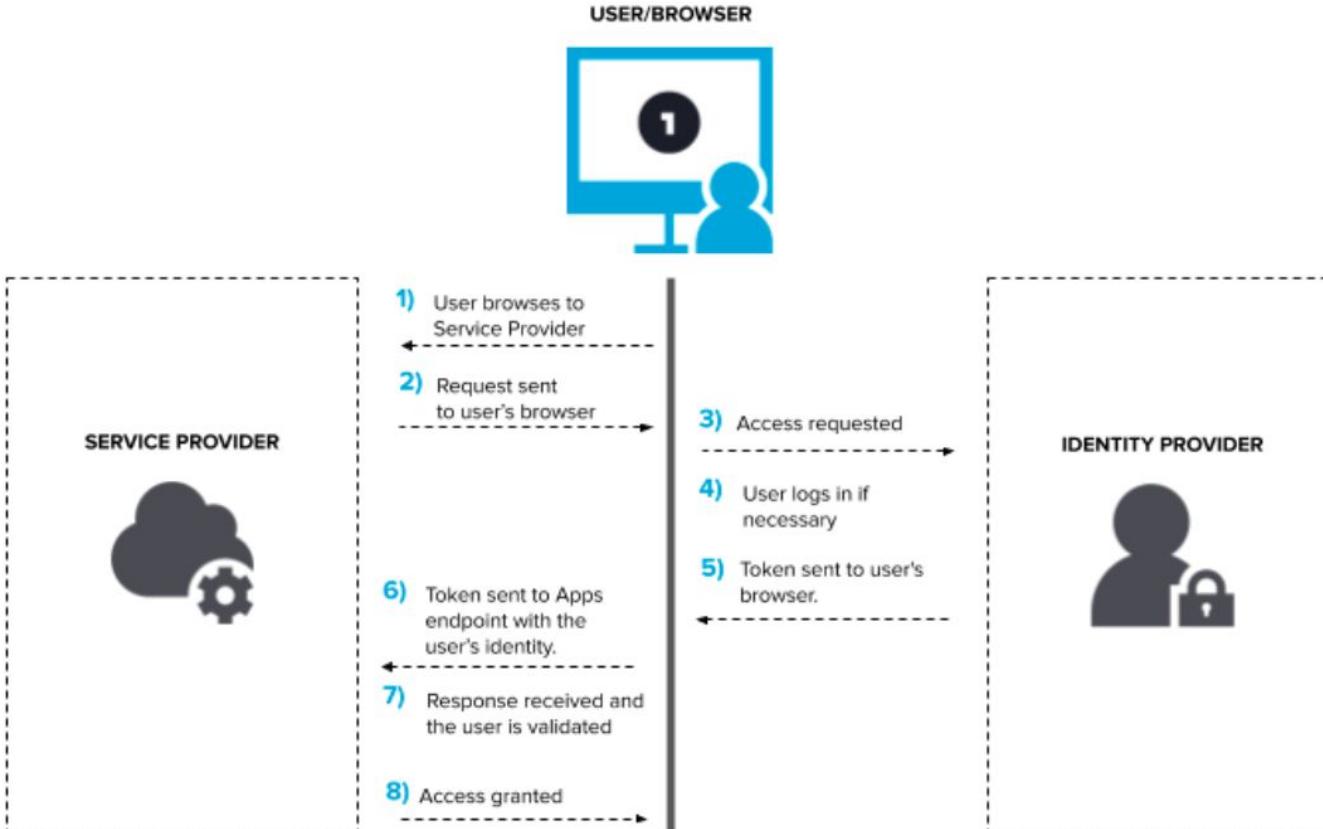
This certificate can be used to sign identity information that is being sent from the identity provider to the service provider so that the service provider knows it is coming from a **trusted source**.

In SSO, this identity data takes the form of tokens which contain identifying bits of information about the user like a user's email address or a username.

SSO - Single sign on Workflow

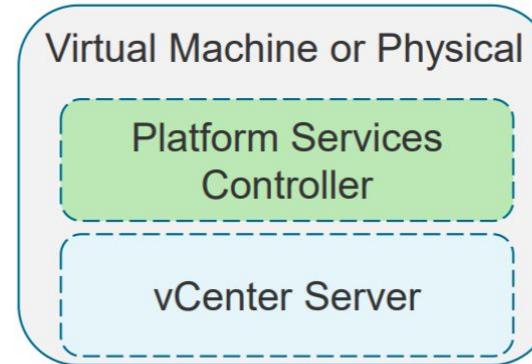
The login flow usually looks like this:

1. A user browses to the application or website they want access to, aka, the Service Provider.
2. The Service Provider sends a token that contains some information about the user, like their email address, to the [SSO system, aka, the Identity Provider](#), as part of a request to authenticate the user.
3. The Identity Provider first checks to see whether the user has already been authenticated, in which case it will grant the user access to the Service Provider application and skip to step 5.
4. If the user hasn't logged in, they will be prompted to do so by providing the credentials required by the Identity Provider. This could simply be a username and password or it might include some other form of authentication like a One-Time Password (OTP).
5. Once the Identity Provider validates the credentials provided, it will send a token back to the Service Provider confirming a successful authentication.
6. This token is passed through the user's browser to the Service Provider.
7. The token that is received by the Service Provider is validated according to the trust relationship that was set up between the Service Provider and the Identity Provider during the initial configuration.
8. The user is granted access to the Service Provider.



vCenter Server includes the Platform Services Controller:

- The Platform Services Controller includes a set of common infrastructure services:
 - VMware vCenter™ Single Sign-On™
 - VMware License Server
 - Lookup Service
 - Certificate Authority
 - Certificate Store
 - VMware Directory Services
- Other features are installed under the vCenter Server component.
- You can install vCenter Server and the Platform Services Controller on the same or different machines.

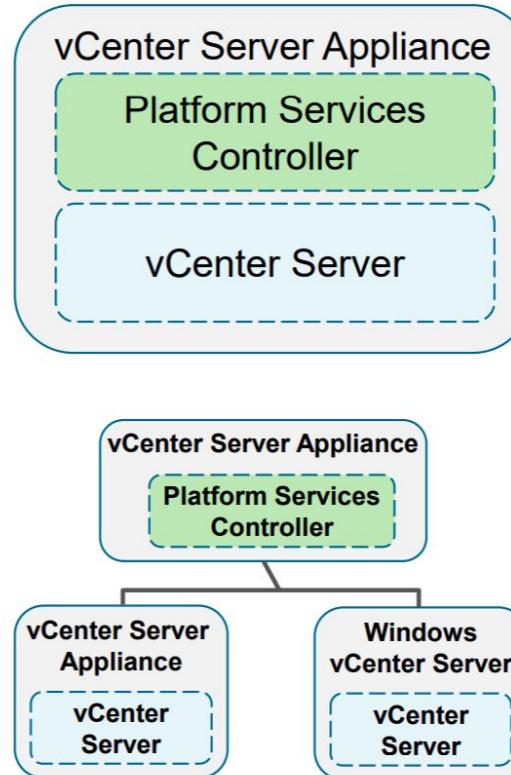


vCenter Server Appliance Basics

VEPSUN

vCenter Server Appliance is functionally equivalent to vCenter Server installed on a Windows server:

- vCenter Server Appliance can be configured with an embedded Platform Services Controller.
- vCenter Server Appliance can be configured as a distributed vCenter Server instance with an external Platform Services Controller.
- You can combine vCenter Server Appliance instances and vCenter Server systems installed on Windows servers in the same architecture.
- vCenter Server Appliance supports Linked Mode.



VMware Vsphere Tool : Configuration Maximums

Source Link : <https://drive.google.com/file/d/1T3o3DmCmhF8nmPRrzxZdkSrl2STNMERO/view?usp=sharing>

Virtual Machine Maximum [configuration] Table

Item	Maximum
Compute	
Virtual CPUs per virtual machine (Virtual SMP)	64
Memory	
RAM per virtual machine	1TB
Virtual machine swap file size	1TB ¹
Storage Virtual Adapters and Devices	
Virtual SCSI adapters per virtual machine	4
Virtual SCSI targets per virtual SCSI adapter	15 ²
Virtual SCSI targets per virtual machine	60
Virtual Disks per virtual machine (PVSCSI)	60
Virtual disk size	62TB
IDE controllers per virtual machine	1 ³
IDE devices per virtual machine	4 ⁴
Floppy controllers per virtual machine	1

Item	Maximum
Floppy devices per virtual machine	2^5
Virtual SATA adapters per virtual machine	4
Virtual SATA devices per virtual SATA adapter	30^4
Networking Virtual Devices	
Virtual NICs per virtual machine	10^6
Virtual Peripheral Ports	
USB host controllers per virtual machine	1^7
USB devices connected to a virtual machine	20^8
Parallel ports per virtual machine	3
Serial ports per virtual machine	4
Miscellaneous	
Concurrent remote console connections to a virtual machine	40
Graphics video device	
Video memory per virtual machine	512MB

Esxi Host [Esxi Compute Resource] Maximum Table

Item	Maximum
Host CPU maximums	
Logical CPUs per host	320
NUMA Nodes per host	16
Virtual machine maximums	
Virtual machines per host	512
Virtual CPUs per host	4096

Item	Maximum
Virtual CPUs per core	32 ¹

Fault Tolerance maximums

Virtual disks	16
Virtual CPUs per virtual machine	1
RAM per FT VM	64GB
Virtual machines per host	4

Memory Maximum

Item	Maximum
RAM per host	4 ¹ TB
Number of swap files	1 per virtual machine
1. Up to 6TB is supported for ESXi 5.5 Update 2 and later.	

Storage Maximum

Item	Maximum
Virtual Disks	
Virtual Disks per Host	2048
iSCSI Physical	
LUNs per server	256
Qlogic 1Gb iSCSI HBA initiator ports per server	4
Broadcom 1Gb iSCSI HBA initiator ports per server	4
Broadcom 10Gb iSCSI HBA initiator ports per server	4
NICs that can be associated or port bound with the software iSCSI stack per server	8
Number of total paths on a server	1024
Number of paths to a LUN (software iSCSI and hardware iSCSI)	8
Qlogic iSCSI: dynamic targets per adapter port	64
Qlogic iSCSI: static targets per adapter port	62
Broadcom 1Gb iSCSI HBA targets per adapter port	64 ¹
Broadcom 10Gb iSCSI HBA targets per adapter port	128

Item	Maximum
LUN size	64TB
LUN ID	255
Number of paths to a LUN	32
Number of total paths on a server	1024
Number of HBAs of any type	8
HBA ports	16
Targets per HBA	256
FCoE	
Software FCoE adapters	4
Common VMFS	
Volume size	64TB ⁵
Volumes per host	256
Hosts per volume	64
Powered on virtual machines per VMFS volume	2048

VMFS3

Raw device mapping size (virtual and physical)	2TB minus 512 bytes
Block size	8MB
File size (1MB block size)	256GB
File size (2MB block size)	512GB
File size (4MB block size)	1TB
File size (8MB block size)	2TB minus 512 bytes
Files per volume	Approximately 30,720

VMFS5

Raw Device Mapping size (virtual compatibility)	62TB
Raw Device Mapping size (physical compatibility)	64TB
Block size	1MB ³
File size	62TB
Files per volume	Approximately 130,690

Networking Maximums

Item	Maximum
Physical NICs	
e1000e 1Gb Ethernet ports (Intel PCI-e)	24
igb 1Gb Ethernet ports (Intel)	16
tg3 1Gb Ethernet ports (Broadcom)	32
bnx2 1Gb Ethernet ports (Broadcom)	16
nx_nic 10Gb Ethernet ports (NetXen)	8
be2net 10Gb Ethernet ports (Serverengines)	8
ixgbe 10Gb Ethernet ports (Intel)	8
bnx2x 10Gb Ethernet ports (Broadcom)	8

Virtual Switch Maximums

vSphere Standard and Distributed Switch

Total virtual network switch ports per host (VDS and VSS ports)	4096
Maximum active ports per host (VDS and VSS)	1016
Virtual network switch creation ports per standard switch	4088
Port groups per standard switch	512
Static/Dynamic port groups per distributed switch	6500
Ephemeral port groups per distributed switch	1016
Ports per distributed switch	60000
Distributed virtual network switch ports per vCenter	60000
Static/dynamic port groups per vCenter	10000
Ephemeral port groups per vCenter	1016
Distributed switches per vCenter	128
Distributed switches per host	16
VSS portgroups per host	1000

Cluster Maximums

Item	Maximum
Cluster (all clusters including HA and DRS)	
Hosts per cluster	32
Virtual machines per cluster	4000
Virtual machines per host	512
Powered-on virtual machine config files per datastore in an HA cluster ¹	2048
Resource Pool	
Resource pools per host	1600
Children per resource pool	1024
Resource pool tree depth	8 ²
Resource pools per cluster	1600

1. This limit does not apply to virtual disks. A virtual machine enabled with Fault Tolerance counts as two virtual machines.
2. Additional 4 resource pools are used by system internals.

Vcenter Maximums

vCenter Server Scalability

Hosts per vCenter Server	1000
Powered-on virtual machines per vCenter Server	10000
Registered virtual machines per vCenter Server	15000
Linked vCenter Servers	10
Hosts in linked vCenter Servers	3000
Powered-on virtual machines in linked vCenter Servers	30000
Registered virtual machines in linked vCenter Servers	50000
Concurrent vSphere Client connections to vCenter Server	100
Concurrent vSphere Web Clients connections to vCenter Server	180
Number of host per datacenter	500
MAC addresses per vCenter Server (using default VMware OUI)	65536

User Interface

USB devices connected per vSphere Client	20
--	----

Case study - Collaboration of AWS with VMware

Customers want a hybrid cloud strategy

83%

of workloads are
virtualized today (IDC)

60%

of large enterprises
run VMs in the
public cloud (IDC)

65%

of organizations have
a hybrid cloud
strategy today (IDC *)

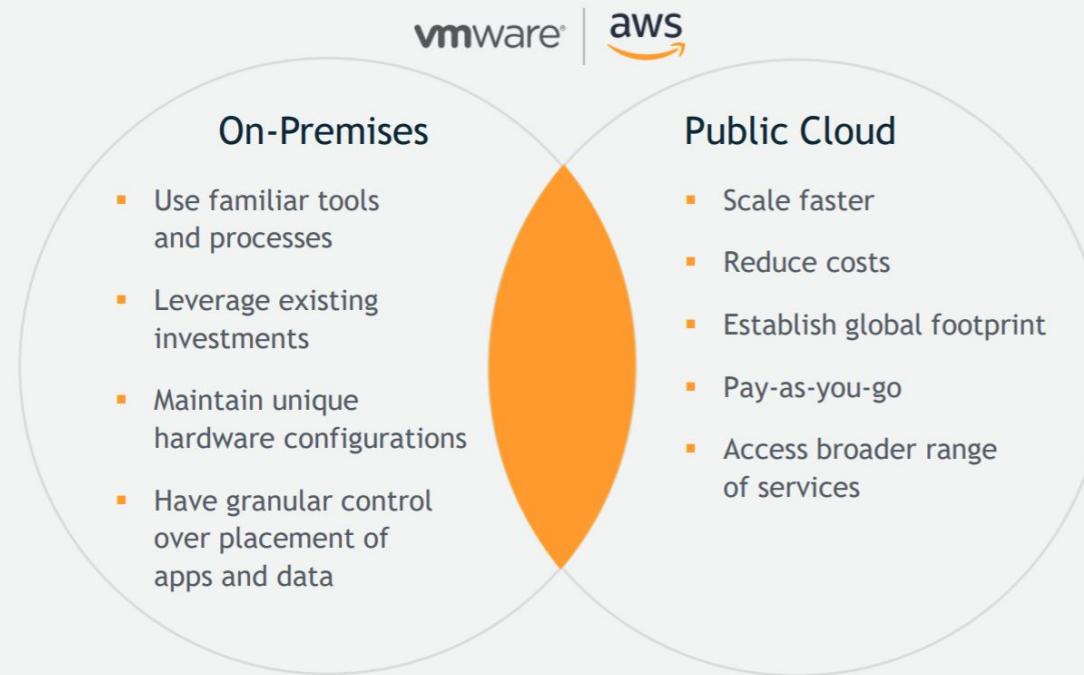
IDC Infographic Video: "Public Cloud for Data Extension and Replacement".
Gary Chen. July 2016. Available on Youtube

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved



Customers are seeking an integrated and hybrid approach

For some customers, hybrid is the preferred operating model



As customers move to the cloud, they are looking for ways to get the best of both worlds without buying new hardware.

A truly compelling and differentiated solution



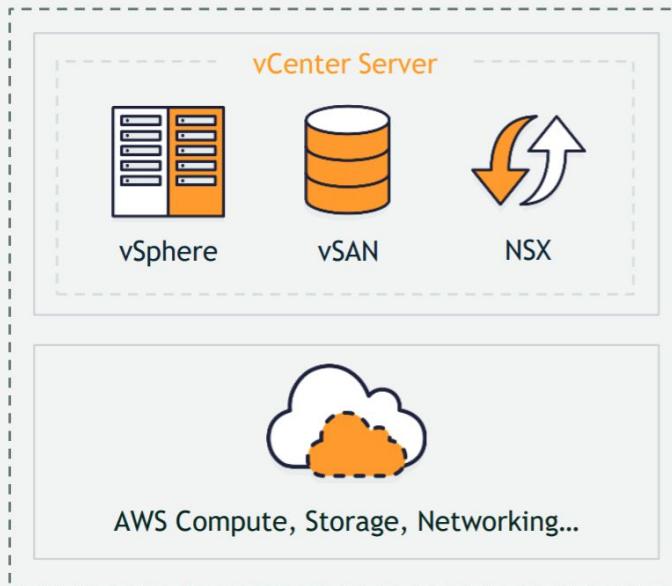
- Leading compute, storage, and network virtualization capabilities
- Support for broad range of workloads
- Standard for the enterprise DC



- Flexible consumption economics
- Broadest set of cloud services
- Global scale and reach

VMware Cloud on AWS = VMware software + AWS infrastructure

VMware Cloud on AWS



VMware Cloud on AWS

$$\begin{array}{c} = \\ \text{VMware Software} \\ + \\ \text{AWS Infrastructure} \end{array}$$

Key Characteristics

- VMware's compute, storage, networking and security delivered as a cloud service
- VMware capabilities and cloud infrastructure sold as a combined VMware offering
- Unit of purchase is physical host with VMware software
- Minimum purchase of 4 hosts
- Add increments of 1 host

What is VMware Cloud on AWS

Software Defined Data Center

vSphere



NSX

vSAN

ESXi

AWS Global Infrastructure

On-Demand, VMware Software
Defined Datacenter Delivered
as a Cloud Service

Latest Software

vCenter Server, ESXi, NSX, vSAN,
Managed by VMware

Dynamic Capacity

DRS/HA Compute Cluster (Intel x86)
VSAN Storage Cluster (NVMe Flash)
NSX Network Virtualization (ENA)

What is VMware Cloud on AWS

Software Defined Data Center

vSphere

NSX

vSAN

ESXi



AWS Global Infrastructure

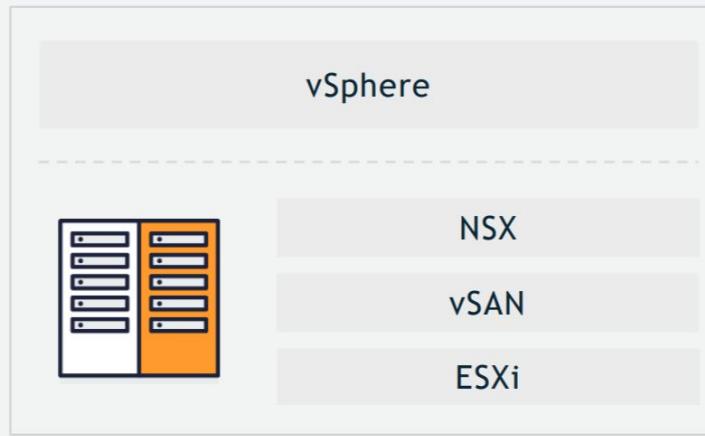
Compute

- Bare Metal
- I3.16XL Equivalent
- 36 Cores/72 vCPUs
- 512GiB Memory15TiB*
- NVMe All-Flash Storage
- 25Gb ENA



What is VMware Cloud on AWS

Software Defined Data Center

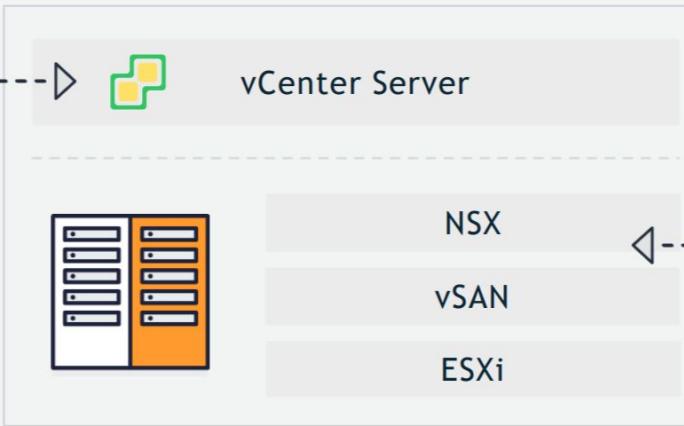
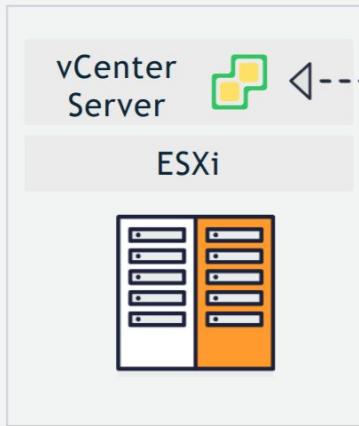


AWS Services

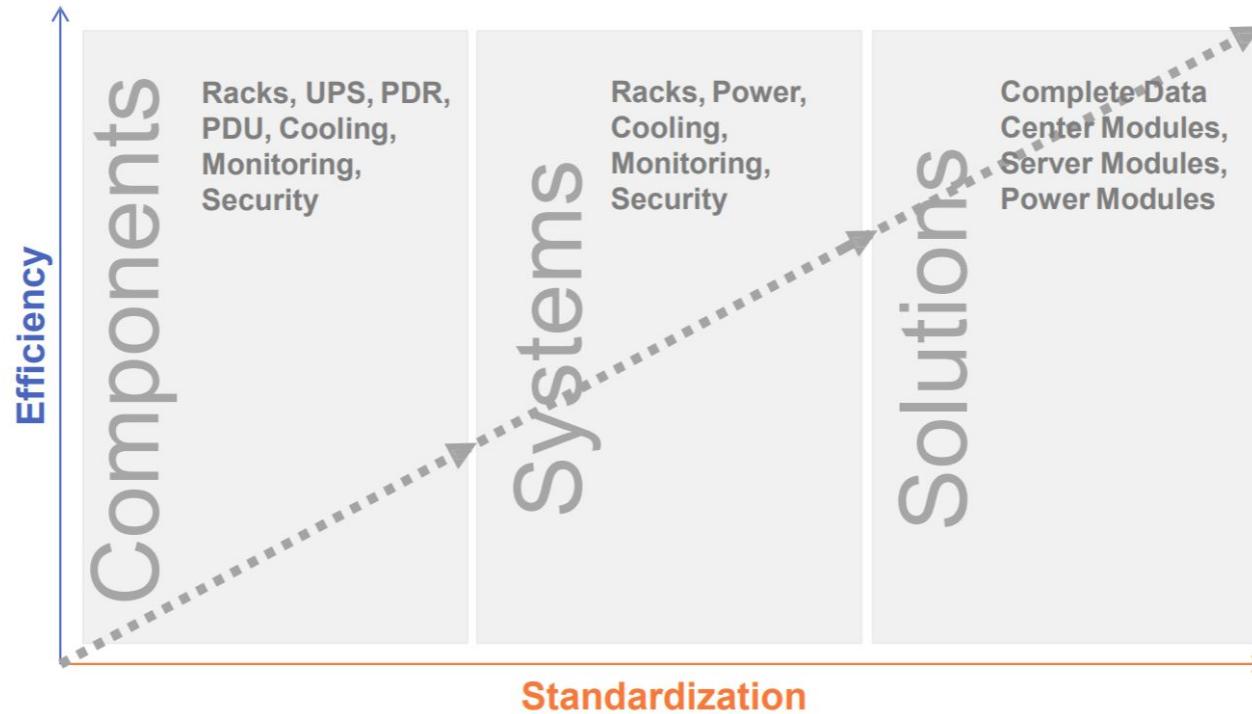


What is VMware Cloud on AWS

Customer Data Center Software Defined Data Center



AWS Global Infrastructure



Customer requirement → increase efficiency in design and operation

What are the drivers for Cloud?

Accelerate new business solutions to improve time to value

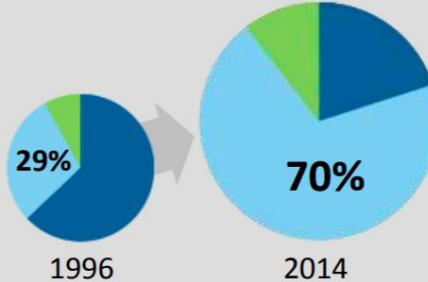


34% of new IT Projects

deploy late

Improve IT efficiency to lower costs

- New server spending
- Power & cooling costs
- Server mgmt & admin costs



70% of IT

operating costs in 2014 will be for
management and administration

Simplify cloud transformations for agility and cost effectiveness



90% plan to implement cloud

by 2017

Concept of Port Mirroring, Netflow and LACP [Link Aggregation Control Protocol]

Introduction to Port Mirroring Concept

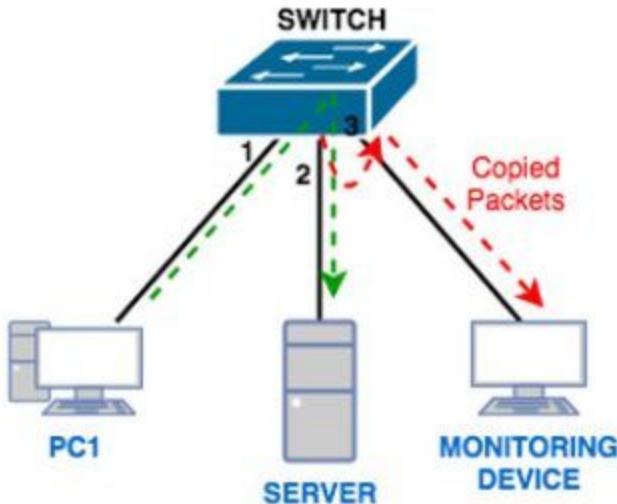
Port mirroring and analyzers send network traffic to devices running analyzer applications. A port mirror copies Layer 3 IP traffic to an interface.

An analyzer copies bridged (Layer 2) packets to an interface. Mirrored traffic can be sourced from single or multiple interfaces.

You can use a device attached to a mirror output interface running an analyzer application to perform tasks such as monitoring compliance, enforcing policies, detecting intrusions, monitoring network performance, correlating events, and other problems on the network.

Port Mirroring

Definition & How-to Configure Lab!



Reference examples of Port Mirroring

Passive Monitoring Access

Access means having visibility to packets.

100% visibility includes packet fragments and Layer 1 and 2 errors.

Passive means without affecting traffic.

- No latency
- No IP Address
- No packets added, dropped, or manipulated
- No link failure

Traffic can be collected from wired networks in the following ways:

- Hubs
- SPAN ports
- In-line Devices
- Taps

SPAN Ports

Switched Port Analyzer (SPAN) Ports, also referred to as “port mirroring” and “port monitoring,” present combined traffic from multiple switch ports.

Advantages:

- Easy access to network traffic because a single NIC on the sensor can connect to a single SPAN port on the switch
- SPAN ports can combine traffic from a variety of switch ports

Disadvantages:

- Switch configuration requires time and resources and can introduce errors resulting in missed traffic
- Under heavy loads, SPAN ports may not see all traffic
- SPAN ports only supply traffic passing through a single switch. Seeing traffic on other devices requires a different approach
- Filters out Layer 1 and 2 errors

Port Mirroring on Vsphere Switch

Reference video Link : <https://youtu.be/RUS1mUw9JaE>

DSwitch1 Actions ▾

Summary Monitor Manage Related Objects

Settings Alarm Definitions Tags Permissions Network Protocol Profiles Ports Resource Allocation

(default filter)

Topology Properties LACP Private VLAN NetFlow Port mirroring Health check

MGMT VLAN ID: 20 VMkernel Ports (3) Virtual Machines (0)

Span VLAN ID: -- Virtual Machines (1)

Storage VLAN ID: 24 VMkernel Ports (3) Virtual Machines (0)

VMNet1 VLAN ID: 30 Virtual Machines (2)

vMotion VLAN ID: 21 VMkernel Ports (3) Virtual Machines (0)

DSwitch1-DVUplinks-41

- Uplink 1 (3 NIC Adapters)
- Uplink 2 (3 NIC Adapters)
- Uplink 3 (3 NIC Adapters)
- Uplink 4 (3 NIC Adapters)

Recent Tasks

All Running Failed

- ✓ Reconfigure vSphere Distribute
- ✓ Reconfigure vSphere Distribute
- ✓ Reconfigure vSphere Distribute
- ✓ Reconfigure Distributed Port Gr
- VMNet2

My Tasks More Tasks

Work In Progress

Alarms

All (0) New (0) Acknowle...

DSwitch1-DVUplinks-41

- Uplink 1 (3 NIC Adapters)
- Uplink 2 (3 NIC Adapters)
- Uplink 3 (3 NIC Adapters)
- Uplink 4 (3 NIC Adapters)

Netflow fundamentals

What is NetFlow?

NetFlow is a network protocol for collecting IP traffic information and monitoring network flow. By analyzing NetFlow data, you can get a picture of network traffic flow and volume.

NetFlow is a one-way technology, so when the server responds to the initial client request, the process works in reverse and creates a new flow record. Using a NetFlow monitoring solution can allow you to monitor and analyze these flow records more efficiently and effectively for traffic within the network.

Datacenter

DSwitch

- Hosts 0
- Virtual Machines 0
- Distributed Port Groups 1
- Uplink Port Groups 1

DSwitch Actions ▾

Getting Started Summary Monitor Manage Related Objects

Settings Alarm Definitions Tags Permissions Network Protocol Profiles Ports Resource Allocation

(default filter)

Topology

Properties LACP Private VLAN NetFlow Port mirroring Health check

DPortGroup
VLAN ID: – Virtual Machines (0)

DSwitch-DVUplinks-29

- Uplink 1 (0 NIC Adapters)
- Uplink 2 (0 NIC Adapters)
- Uplink 3 (0 NIC Adapters)
- Uplink 4 (0 NIC Adapters)

LACP [Link Aggregation Control
Protocol]

Overview of Link Aggregation

What is Link Aggregation?

Link aggregation is the practice of bundling individual links on a network to promote better performance outcomes.

#LACP will be supported by VMware Tools :

[LACP Teaming and Failover Configuration for Distributed Port Groups](#)

To handle the network traffic of distributed port groups by using a LAG, you assign physical NICs to the LAG ports and set the LAG as active in the teaming and failover order of distributed port groups.

LACP supported on Virtual Distributed
Switch

