VMware vSphere Basics

ESXi 5.0
vCenter Server 5.0

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-000586-00

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

VMware vSphere Basics 5

1 VMware vSphere and Virtualizing the IT Infrastructure 7
- Aspects of Virtualization 7
- VMware vSphere , a Platform for Virtualization and Cloud Infrastructure 10
- VMware vSphere Components and Features 12
- Physical Topology of vSphere Datacenter 14

2 Virtualization Layer: vSphere Datacenter 17
- Virtual Datacenter Architecture 17
  - Hosts, Clusters, and Resource Pools 18
  - VMware vSphere Distributed Services 20
- Network Architecture 23
  - VMware vShield and Network Security 25
- Storage Architecture 26

3 Management Layer: VMware vCenter Server 29
- vCenter Server Core Services 31
- vCenter Server Plug-Ins 31
- vCenter Server Interfaces 32

4 Interface Layer: Accessing the Virtual Infrastructure 33
- vSphere Client and vSphere Web Client 34
  - Using the vSphere Client 34
  - Using the vSphere Web Client 35
- SDKs and Command-Line Interfaces 35
- Direct Virtual Machine Console Access 36

Index 37

VMware vSphere Basics

VMware vSphere Basics provides information about the features and functionality of VMware vSphere®.

This document describes VMware ESXi™, VMware vCenter Server™, and vSphere Clients, which are the virtualization layer, management layer, and interface layer, respectively, of vSphere.

Intended Audience

This information is intended for those who need to familiarize themselves with the components and capabilities of VMware vSphere. This information is for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

VMware vSphere and Virtualizing the IT Infrastructure

1

VMware vSphere uses virtualization to transform datacenters into scalable, aggregated computing infrastructures. A virtual infrastructure presents IT organizations with increased flexibility in how they deliver their services. A virtual infrastructure also serves as the foundation for cloud computing.

Cloud computing is an approach to computing that builds on virtualization's efficient pooling of resources to create an on-demand, elastic, self-managing virtual infrastructure that can be allocated dynamically as a service. Virtualization uncouples applications and information from the complexity of the underlying hardware infrastructure.

Virtualization, in addition to being the underlying technology for cloud computing, enables organizations of all sizes to make improvements in the areas of flexibility and cost containment. For example, with server consolidation, one physical server takes on the work of many servers by incorporating multiple servers as virtual machines. Also, ease of management and effective resource use are products of virtualizing the datacenter. When you virtualize your datacenter, management of the infrastructure becomes easier and you use your available infrastructure resources more effectively. Virtualization enables you to create a dynamic and flexible datacenter, and can reduce operating expenses through automation while also reducing planned and unplanned downtime.

This chapter includes the following topics:

- "Aspects of Virtualization," on page 7
- "VMware vSphere, a Platform for Virtualization and Cloud Infrastructure," on page 10
- "VMware vSphere Components and Features," on page 12
- "Physical Topology of vSphere Datacenter," on page 14

Aspects of Virtualization

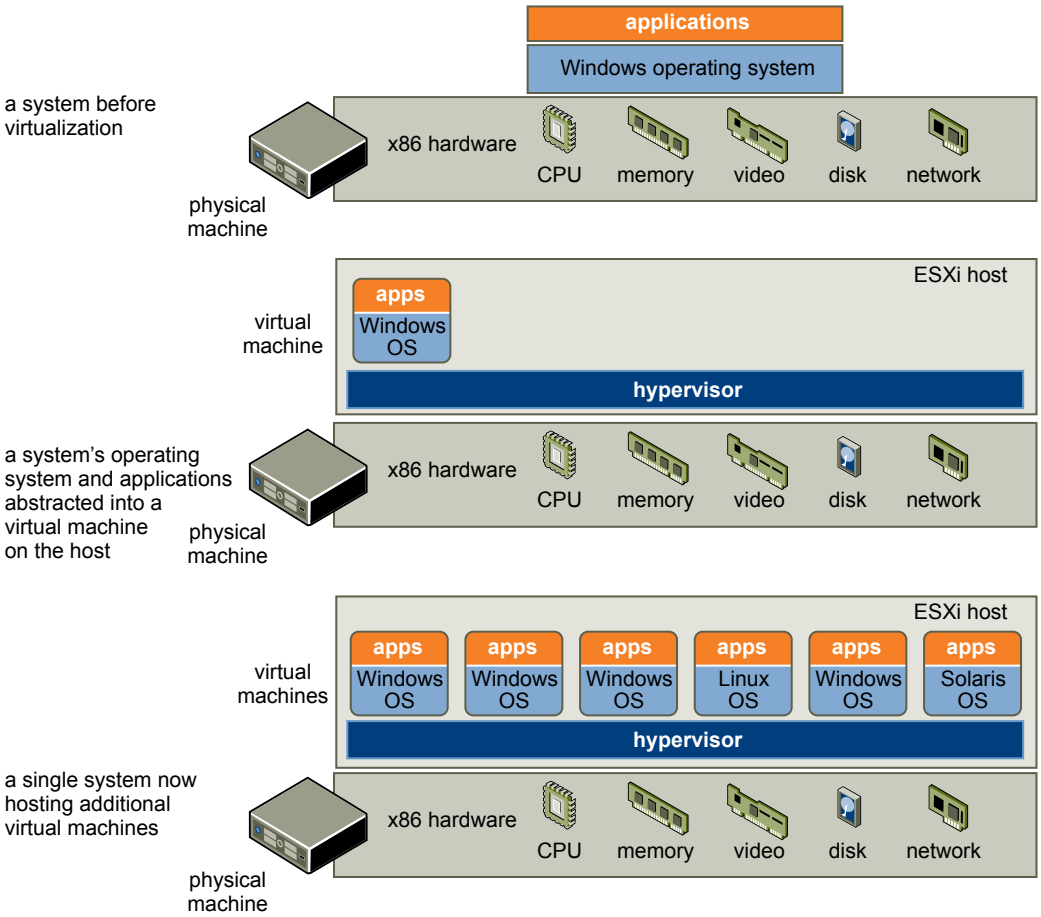
VMware vSphere virtualizes and aggregates the underlying physical hardware resources across multiple systems and provides pools of virtual resources to the datacenter.

Virtualization is a process that breaks the hard connection between the physical hardware and the operating system and applications running on it. After being virtualized in a vSphere virtual machine, the operating system and applications are no longer constrained by the limits imposed by residing on a single physical machine. Virtual equivalents of physical elements such as switches and storage operate within a virtual infrastructure that can span the enterprise.

Virtualizing the Computer

The x86 computer hardware is designed to run a single operating system and a single application, leaving most machines underused. Even with many applications installed, most machines are underused. At the most basic level, virtualizing lets you run multiple virtual machines on a single physical machine, with each virtual machine sharing the resources of that one physical computer across multiple environments. Different virtual machines can run different operating systems and multiple applications, in isolation, side-by-side on the same physical machine.

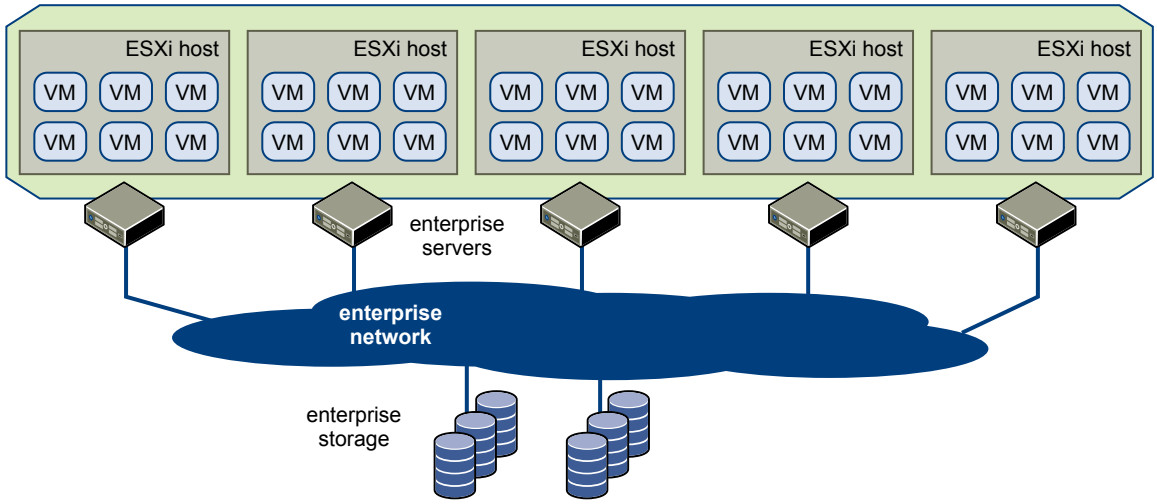
Figure 1-1. Virtualizing the Computer and Adding Virtual Machines



Virtualizing the Infrastructure

In addition to virtualizing a single physical computer, you can build an entire virtual infrastructure with VMware vSphere, scaling across thousands of interconnected physical computers and storage devices. Using virtualization, you can dynamically move resources and processing and allocate hardware resources. You do not need to assign servers, storage, or network bandwidth permanently to each application.

Figure 1-2. The Infrastructure Can Span Many Physical Devices



A virtual infrastructure consists of the following components:

- Bare-metal hypervisors to enable full virtualization of each x86 computer.
- Virtual infrastructure services such as resource management to optimize available resources among virtual machines.
- Automation solutions that provide special capabilities to optimize a particular IT process such as provisioning or disaster recovery.

Cloud Computing

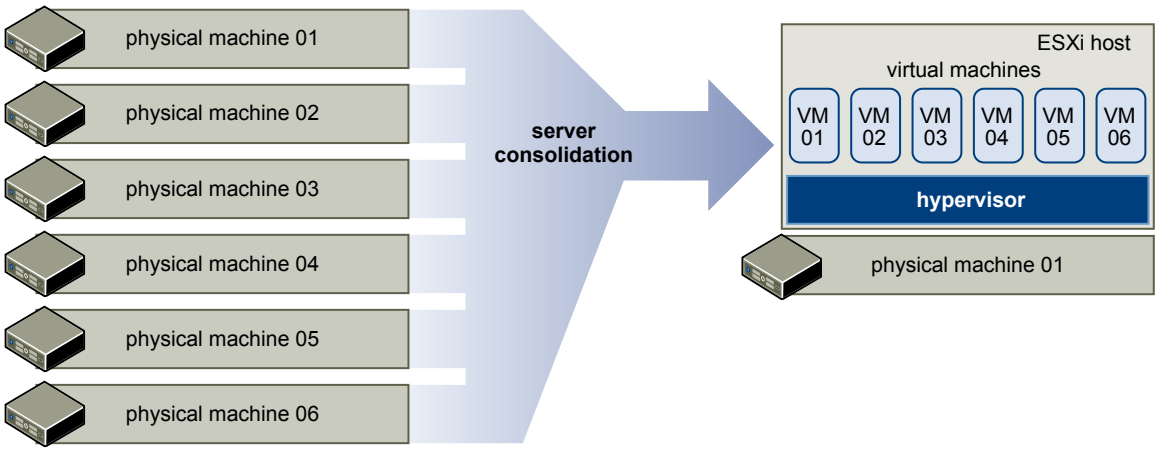
In cloud computing, providers deliver hosted services on demand over the Internet. Cloud computing is similar to utilities like electricity and telephony. The user can consume the level of service needed at any time without being responsible for the production and management of the service.

A virtual infrastructure is the foundation for cloud computing. Cloud computing depends on a scalable and elastic model for delivering IT services, and the model itself depends on virtualization to be workable. VMware vSphere provides that virtualization.

Server Consolidation

Server consolidation through virtualization lets you get more out of your existing servers. It also lets you limit the physical resources that you need to manage, power, store, and buy. You achieve high consolidation ratios by consolidating existing workloads and leveraging remaining servers for the deployment of new applications and solutions.

Figure 1-3. In Server Consolidation, Physical Machines Are Converted to Virtual Machines to Run in a vSphere ESXi Host



Business Continuity

Virtualization enables IT to reduce or even eliminate planned and unplanned downtimes. For example, with vSphere you can migrate virtual machines live to another host and perform maintenance on physical servers anytime, without user or service disruption. Unplanned downtime is reduced by using vSphere features such as High Availability and Fault Tolerance.

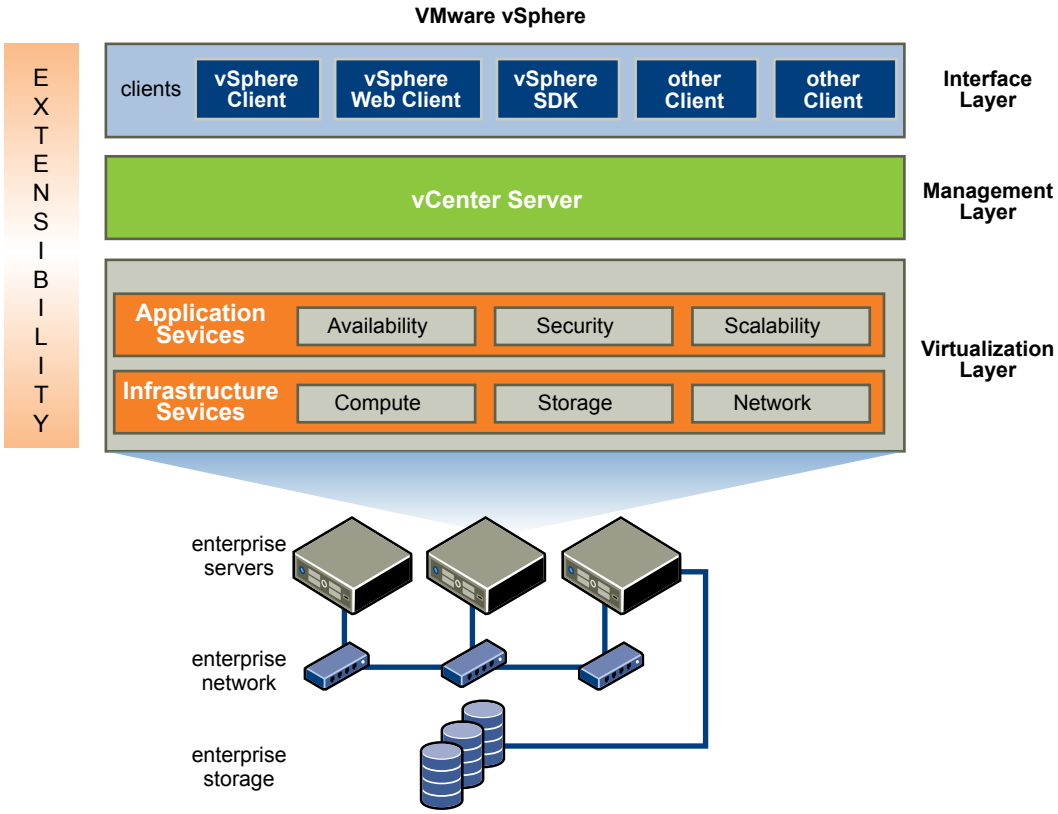
Traditional disaster recovery plans require manual, complex steps to allocate recovery resources, perform bare metal recovery, recover data, and validate that systems are ready for use. VMware vSphere simplifies this environment. Hardware configuration, firmware, operating system, and applications become data stored in a few files on disk. Protecting these files using your backup or replication software means that the entire system is protected. These files can be recovered to any physical computer without requiring changes because virtual machines are hardware-independent.

VMware vSphere , a Platform for Virtualization and Cloud Infrastructure

VMware vSphere manages large collections of infrastructure, such as CPUs, storage, and networking, as a seamless and dynamic operating environment, and also manages the complexity of a datacenter.

The VMware vSphere software stack is composed of the virtualization, management, and interface layers.

Figure 1-4. Relationships Between the Component Layers of VMware vSphere



Virtualization Layer

The virtualization layer of VMware vSphere includes infrastructure services and application services. Infrastructure services such as compute, storage, and network services abstract, aggregate, and allocate hardware or infrastructure resources. Infrastructure services include the following types:

Compute services — Includes the VMware capabilities that abstract away from underlying disparate server resources. Compute services aggregate these resources across many discrete servers and assign them to applications.

Storage services — The set of technologies that enables the most efficient use and management of storage in virtual environments.

Network services — The set of technologies that simplify and enhance networking in virtual environments.

Application services are the set of services provided to ensure availability, security, and scalability for applications. Examples include vSphere High Availability and Fault Tolerance.

Management Layer

VMware vCenter Server is the central point for configuring, provisioning, and managing virtualized IT environments.

Interface Layer

Users can access the VMware vSphere datacenter through GUI clients such as the vSphere Client or the vSphere Web Client. Additionally, users can access the datacenter through client machines that use command-line interfaces and SDKs for automated management.

VMware vSphere Components and Features

An introduction to the components and features of VMware vSphere helps you to understand the parts and how they interact.

VMware vSphere includes the following components and features.

VMware ESXi	A virtualization layer run on physical servers that abstracts processor, memory, storage, and resources into multiple virtual machines.
VMware vCenter Server	The central point for configuring, provisioning, and managing virtualized IT environments. It provides essential datacenter services such as access control, performance monitoring, and alarm management.
VMware vSphere Client	An interface that enables users to connect remotely to vCenter Server or ESXi from any Windows PC.
VMware vSphere Web Client	A Web interface that enables users to connect remotely to vCenter Server from a variety of Web browsers and operating systems.
VMware vSphere SDKs	Feature that provides standard interfaces for VMware and third-party solutions to access VMware vSphere.
vSphere Virtual Machine File System (VMFS)	A high performance cluster file system for ESXi virtual machines.
vSphere Virtual SMP	Enables a single virtual machine to use multiple physical processors simultaneously.
vSphere vMotion	Enables the migration of powered-on virtual machines from one physical server to another with zero down time, continuous service availability, and complete transaction integrity. Migration with vMotion cannot be used to move virtual machines from one datacenter to another.
vSphere Storage vMotion	Enables the migration of virtual machine files from one datastore to another without service interruption. You can place the virtual machine and all its disks in a single location, or select separate locations for the virtual machine configuration file and each virtual disk. The virtual machine remains on the same host during Storage vMotion. Migration with Storage vMotion lets you move the virtual disks or configuration file of a virtual machine to a new datastore while the virtual machine is running. Migration with Storage vMotion enables you to move a virtual machine's storage without any interruption in the availability of the virtual machine.

vSphere High Availability (HA)	A feature that provides high availability for virtual machines. If a server fails, affected virtual machines are restarted on other available servers that have spare capacity.
vSphere Distributed Resource Scheduler (DRS)	Allocates and balances computing capacity dynamically across collections of hardware resources for virtual machines. This feature includes distributed power management (DPM) capabilities that enable a datacenter to significantly reduce its power consumption.
vSphere Storage DRS	Allocates and balances storage capacity and I/O dynamically across collections of datastores. This feature includes management capabilities that minimize the risk of running out of space and the risk of I/O bottlenecks slowing the performance of virtual machines.
vSphere Fault Tolerance	Provides continuous availability by protecting a virtual machine with a copy. When this feature is enabled for a virtual machine, a secondary copy of the original, or primary, virtual machine is created. All actions completed on the primary virtual machine are also applied to the secondary virtual machine. If the primary virtual machine becomes unavailable, the secondary machine becomes immediately active.
vSphere Distributed Switch (VDS)	A virtual switch that can span multiple ESXi hosts, enabling significant reduction of on-going network maintenance activities and increasing network capacity. This increased efficiency enables virtual machines to maintain consistent network configuration as they migrate across multiple hosts.
Host Profiles	A feature that simplifies host configuration management through user-defined configuration policies. The host profile policies capture the blueprint of a known, validated host configuration and use this configuration to configure networking, storage, security, and other settings across multiple hosts. The host profile policies also monitor compliance to standard host configuration settings across the datacenter. Host profiles reduce the manual steps that are involved in configuring a host and can help maintain consistency and correctness across the datacenter. Host profiles are also a component of vSphere Auto Deploy. The concept of an autodeployed host means that vCenter Server owns the entire host configuration and it is captured within a host profile. Certain policies require user input to provide host-specific values. To support Auto Deploy for host profiles, an answer file is created that contains the definitions for those policies.

Physical Topology of vSphere Datacenter

A typical VMware vSphere datacenter consists of basic physical building blocks such as x86 virtualization servers, storage networks and arrays, IP networks, a management server, and desktop clients.

The vSphere datacenter topology includes the following components.

Compute servers

Industry standard x86 servers that run ESXi on the bare metal. ESXi software provides resources for and runs the virtual machines. Each computing server is referred to as a standalone host in the virtual environment. You can group a number of similarly configured x86 servers with connections to the same network and storage subsystems to provide an aggregate set of resources in the virtual environment, called a cluster.

Storage networks and arrays

Fibre Channel SAN arrays, iSCSI SAN arrays, and NAS arrays are widely used storage technologies supported by VMware vSphere to meet different datacenter storage needs. The storage arrays are connected to and shared between groups of servers through storage area networks. This arrangement allows aggregation of the storage resources and provides more flexibility in provisioning them to virtual machines.

IP networks

Each compute server can have multiplephysical network adapters to provide high bandwidth and reliable networking to the entire VMware vSphere datacenter.

vCenter Server

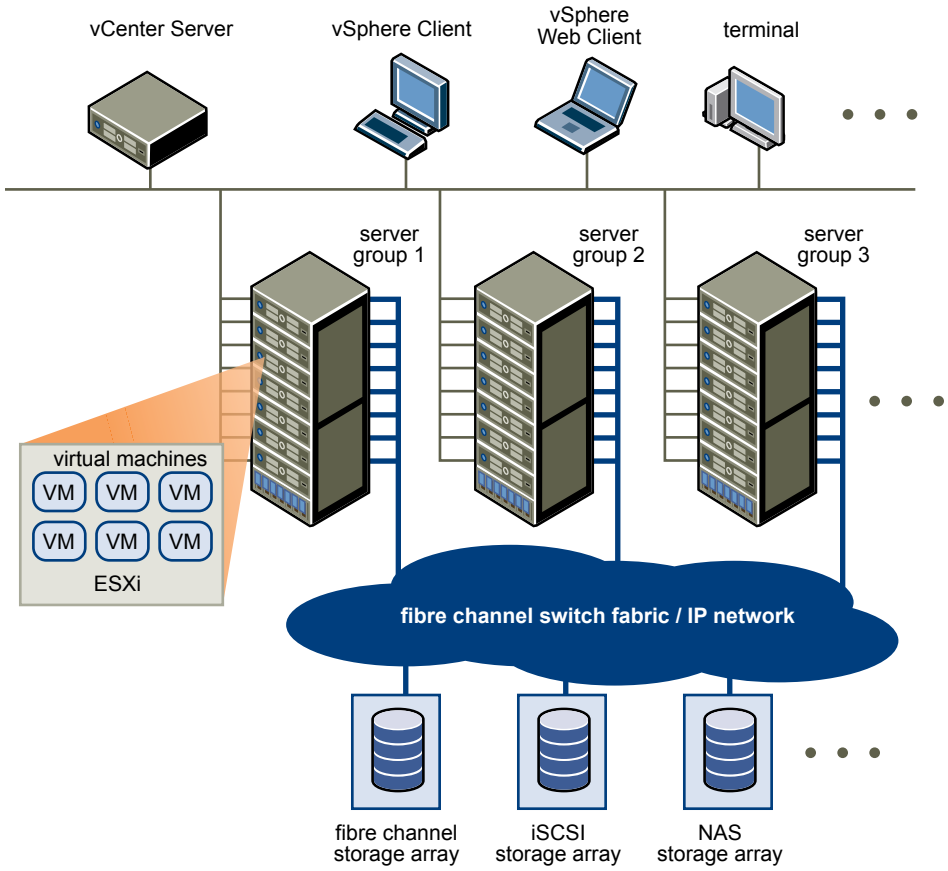
vCenter Server provides a single point of control to the datacenter. It provides essential datacenter services such as access control, performance monitoring, and configuration. It unifies the resources from the individual computing servers to be shared among virtual machines in the entire datacenter. It does this by managing the assignment of virtual machines to the computing servers and the assignment of resources to the virtual machines within a given computing server based on the policies that the system administrator sets.

Computing servers continue to function even in the unlikely event that vCenter Server becomes unreachable (for example, if the network is severed). Servers can be managed separately and continue to run the virtual machines assigned to them based on the resource assignment that was last set. After connection to vCenter Server is restored, it can manage the datacenter as a whole again.

Management clients

VMware vSphere provides several interfaces for datacenter management and virtual machine access. These interfaces include VMware vSphere Client (vSphere Client), vSphere Web Client for access through a web browser, or vSphere Command-Line Interface (vSphere CLI).

Figure 1-5. VMware vSphere Datacenter Physical Topology



Virtualization Layer: vSphere Datacenter

2

The virtualization layer consists of the ESXi hypervisor, which abstracts processor, memory, video, storage, and resources into virtual machines.

The virtualization layer also incorporates application services like Fault Tolerance that ensure availability, security, and scalability.

This chapter includes the following topics:

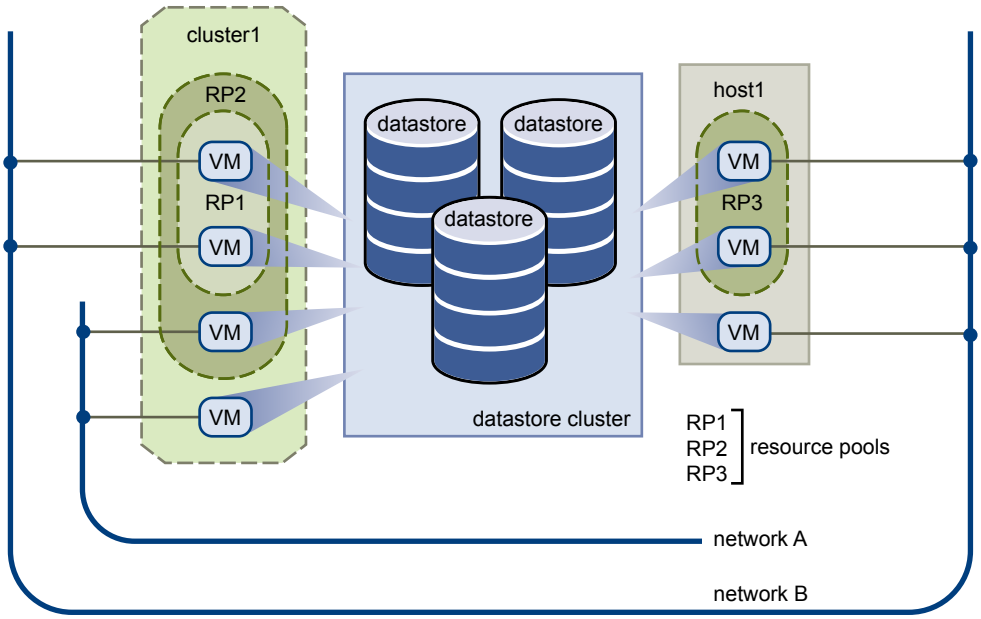
- "Virtual Datacenter Architecture," on page 17
- "Network Architecture," on page 23
- "Storage Architecture," on page 26

Virtual Datacenter Architecture

VMware vSphere virtualizes the entire IT infrastructure including servers, storage, and networks.

VMware vSphere aggregates these resources and presents a uniform set of elements in the virtual environment. With VMware vSphere, you can manage IT resources like a shared utility and dynamically provision resources to different business units and projects.

Figure 2-1. Key Elements in the Virtual Datacenter Architecture



You can use vSphere to view, configure, and manage these key elements. The following is a list of the key elements:

- Computing and memory resources called hosts, clusters, and resource pools
- Storage resources called datastores and datastore clusters
- Networking resources called networks
- Virtual machines

A host is the virtual representation of the computing and memory resources of a physical machine running ESXi. When two or more physical machines are grouped to work and be managed as a whole, the aggregate computing and memory resources form a cluster. Machines can be dynamically added or removed from a cluster. Computing and memory resources from hosts and clusters can be finely partitioned into a hierarchy of resource pools.

Datastores are virtual representations of combinations of underlying physical storage resources in the datacenter. These physical storage resources can come from the following sources:

- Local SCSI, SAS, or SATA disks of the server
- Fibre Channel SAN disk arrays
- iSCSI SAN disk arrays
- Network Attached Storage (NAS) arrays

A datastore cluster is an aggregation of multiple datastores into a single logical, load-balanced pool.

Networks in the virtual environment connect virtual machines to one another and to the physical network outside of the virtual datacenter.

Virtual machines can be assigned to a particular host, cluster or resource pool, and a datastore and datastore cluster when they are created. After they are powered-on, virtual machines consume resources dynamically as the workload increases or give back resources dynamically as the workload decreases.

Provisioning of virtual machines is much faster and easier than physical machines. New virtual machines can be created in seconds. When a virtual machine is provisioned, the appropriate operating system and applications can be installed unaltered on the virtual machine to handle a particular workload as though they were being installed on a physical machine. A virtual machine can be provisioned with the operating system and applications installed and configured.

Resources get provisioned to virtual machines based on the policies that are set by the system administrator who owns the resources. The policies can reserve a set of resources for a particular virtual machine to guarantee its performance. The policies can also prioritize and set a variable portion of the total resources to each virtual machine. A virtual machine is prevented from being powered-on and consuming resources if doing so violates the resource allocation policies. For more information on resource and power management, see the *vSphere Resource Management* documentation.

Hosts, Clusters, and Resource Pools

Hosts, clusters, and resource pools provide flexible and dynamic ways to organize the aggregated computing and memory resources in the virtual environment and link them back to the underlying physical resources.

Because a host represents the aggregate resources of a physical x86 server, if the physical x86 server has four dual-core CPUs running at 4GHz each and 32GB of system memory, the host has 32GHz of computing power and 32GB of memory available for running virtual machines that are assigned to it.

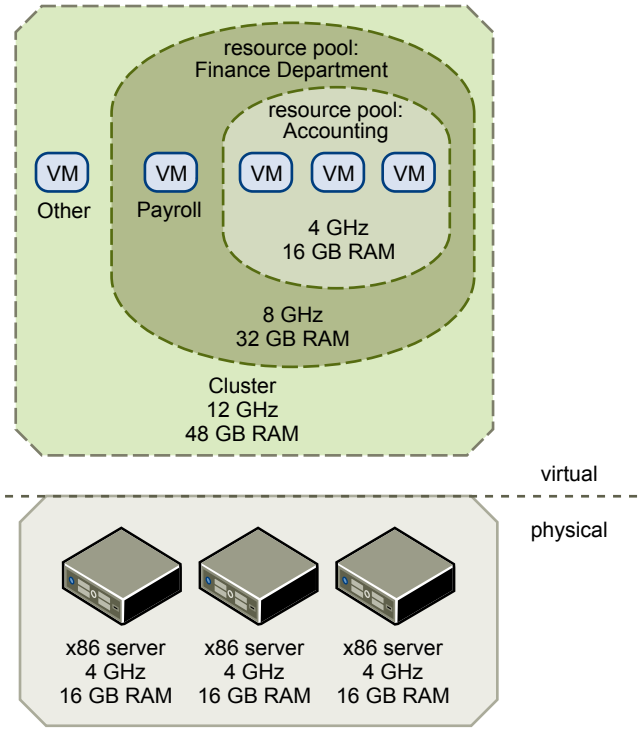
A cluster acts and can be managed as a single entity. It represents the aggregate computing and memory resources of a group of physical x86 servers sharing the same network and storage arrays. For example, if the group contains eight servers with four dual-core CPUs each running at 4GHz and 32GB of memory, the cluster has an aggregate 256GHz of computing power and 256GB of memory available for running virtual machines.

Resource pools are partitions of computing and memory resources from a single host or a cluster. Resource pools can be hierarchical and nested. You can partition any resource pool into smaller resource pools to divide and assign resources to different groups or for different purposes.

Example of Using Resource Pools

Figure 2-2 illustrates the use of resource pools. Three x86 servers with 4GHz computing power and 16GB of memory each are aggregated to form a cluster of 12GHz computing power and 48GB of memory. The Finance Department resource pool reserves 8GHz of computing power and 32GB of memory from the cluster. The remaining 4GHz computing power and 16GB of memory are reserved for the other virtual machine. From the Finance Department resource pool, the smaller, nested Accounting resource pool reserves 4GHz computing power and 16GB of memory in the Finance Department resource pool for the virtual machines from the accounting department. That leaves 4GHz of computing power and 16GB of memory for the virtual machine called Payroll.

Figure 2-2. Hosts, Clusters, and Resource Pools



You can dynamically change resource allocation policies. For example, at year end, the workload on Accounting increases, and which requires an increase in the Accounting resource pool reserve of 4GHz of power to 6GHz. You can make the change to the resource pool dynamically without shutting down the associated virtual machines.

When reserved resources are not being used by a resource pool or a virtual machine, the resources can be shared. In the example, if the 4GHz of resources reserved for the Accounting department are not being used, the Payroll virtual machine can use those gigahertz during its peak time. When Accounting resource demands increase, Payroll dynamically returns them. Resources are reserved for different resource pools, but resources are not wasted if an owner does not use them. This capability helps to maximize resource use while also ensuring that reservations are met and resource policies enforced.

As demonstrated by the example, resource pools can be nested, organized hierarchically, and dynamically reconfigured so that the IT environment matches the company organization. Individual business units can receive dedicated resources while still exploiting from the efficiency of resource pooling.

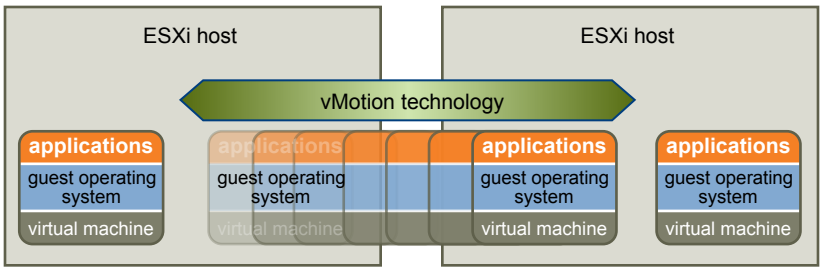
VMware vSphere Distributed Services

vSphere vMotion, vSphere Storage vMotion, vSphere DRS, vSphere Storage DRS, Storage I/O Control, vSphere HA, and Fault Tolerance are distributed services that enable efficient and automated resource management and high availability for virtual machines.

vSphere vMotion

Virtual machines run on and consume resources from ESXi. With vMotion, you can migrate running virtual machines from one physical server to another without service interruption. The effect is a more efficient assignment of resources. With vMotion, resources can be dynamically reallocated to virtual machines across physical servers.

Figure 2-3. Migration with vMotion



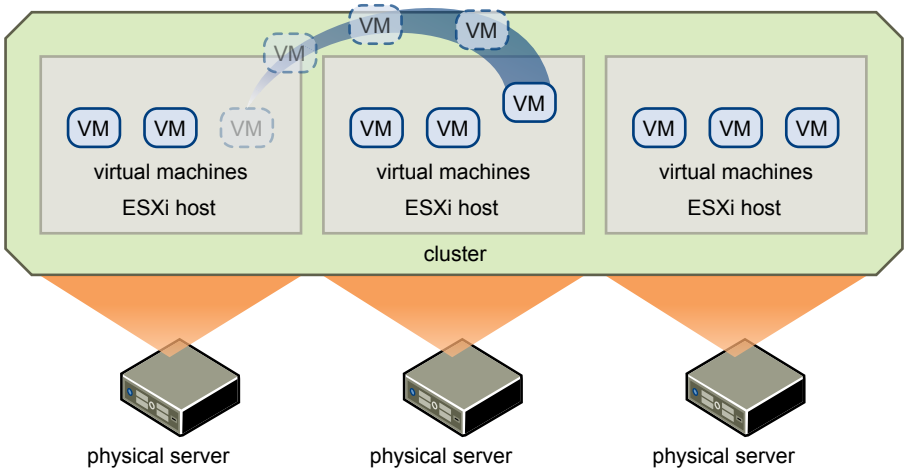
vSphere Storage vMotion

With Storage vMotion, you can migrate virtual machines from one datastore to another datastore without service interruption. This ability allows administrators, for example, to off-load virtual machines from one storage array to another to perform maintenance, reconfigure LUNs, resolve space issues, and upgrade VMFS volumes. Administrators can also use Storage vMotion to optimize the storage environment for improved performance by seamlessly migrating virtual machine disks.

vSphere Distributed Resource Scheduler

vSphere Distributed Resource Scheduler (DRS) helps you manage a cluster of physical hosts as a single compute resource. You can assign a virtual machine to a cluster and DRS finds an appropriate host on which to run the virtual machine. DRS places virtual machines so that the load across the cluster is balanced, and cluster-wide resource allocation policies (for example, reservations, priorities, and limits) are enforced. When a virtual machine is powered on, DRS performs an initial placement of the virtual machine on a host. As cluster conditions change (for example, load and available resources), DRS uses vMotion to migrate virtual machines to other hosts as necessary.

Figure 2-4. vSphere DRS



When you add a new physical server to a cluster, DRS enables virtual machines to immediately take advantage of the new resources because it distributes the running virtual machines.

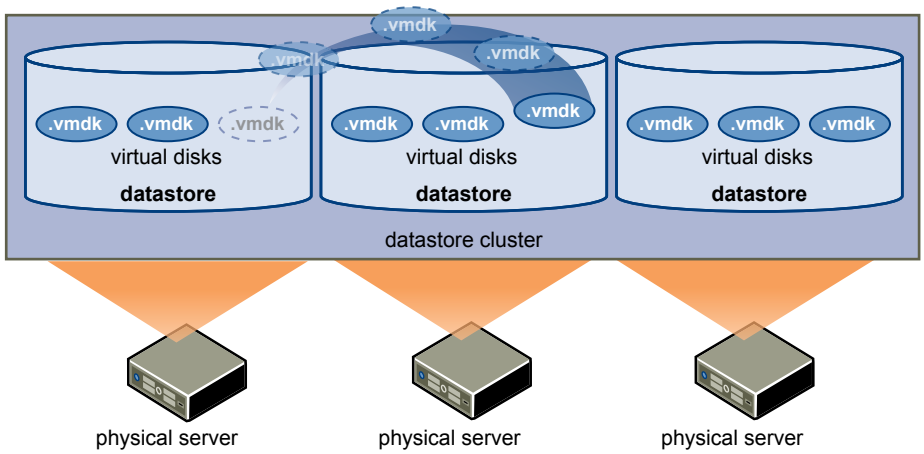
When distributed power management (DPM) is enabled, the system compares cluster-level and host-level capacity to the demands of virtual machines running in the cluster. If the resource demands of the running virtual machines can be met by a subset of hosts in the cluster, DPM migrates the virtual machines to this subset and powers down the hosts that are not needed. When resource demands increase, DPM powers these hosts back on and migrates the virtual machines to them. This dynamic cluster right-sizing that DPM performs reduces the power consumption of the cluster without sacrificing virtual machine performance or availability.

You can configure DRS to perform virtual machine placement, virtual machine migration, and host power actions, or to provide recommendations that the datacenter administrator can assess and manually act on.

vSphere Storage DRS

Storage DRS helps you manage multiple datastores as a single compute resource, called a datastore cluster. A datastore cluster is an aggregation of multiple datastores into a single logical, load-balanced pool. You can treat the datastore cluster as a single flexible storage resource for resource management purposes. In effect, a datastore cluster is the storage equivalent of an ESXi compute cluster. You can dynamically populate datastore clusters with datastores of similar characteristics. You can assign a virtual disk to a datastore cluster and Storage DRS finds an appropriate datastore for it. The load balancer manages initial placement and future migrations based on workload measurements. Storage space balancing and I/O balancing minimize the risk of running out of space and the risk of I/O bottlenecks slowing the performance of virtual machines.

Figure 2-5. Storage DRS



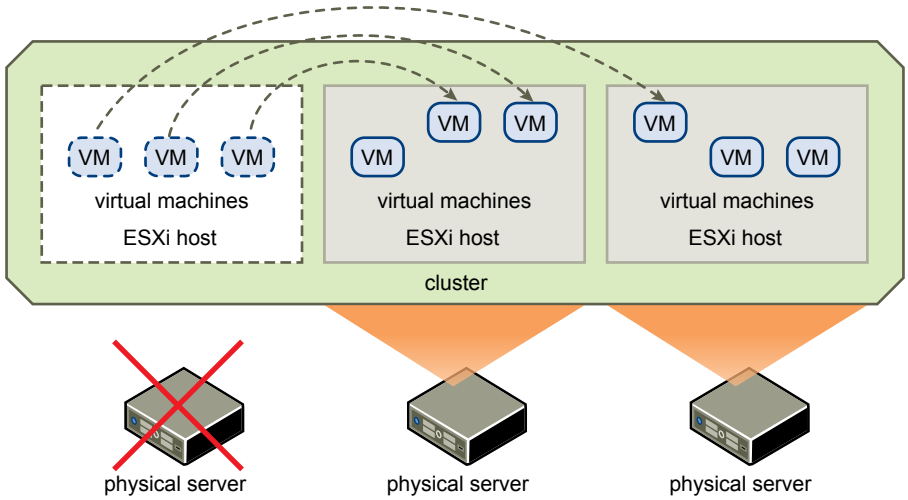
Storage I/O Control congestion management allows cluster-wide storage I/O prioritization. You can control the amount of storage I/O that is allocated to virtual machines during periods of I/O congestion, which ensures that more important virtual machines are preferred over less important virtual machines for I/O resource allocation.

vSphere High Availability

With vSphere HA, virtual machines automatically restart on a different physical server in a cluster if a host fails.

vSphere HA monitors all physical hosts in a cluster and detects host failures. Each physical host maintains a heartbeat with the other hosts in the cluster. Loss of a heartbeat initiates the process of restarting all affected virtual machines on other hosts. vSphere HA admission control ensures that if a host fails, sufficient resources are available in the cluster at all times to restart virtual machines on different physical hosts.

Figure 2-6. vSphere HA



vSphere HA also provides a Virtual Machine Monitoring feature that monitors the status of virtual machines in a vSphere HA cluster. If a virtual machine does not generate heartbeats within a specified time, Virtual Machine Monitoring identifies it as having failed and restarts it. If restarts occur, policies can control the number of restarts. Similarly, you can use the Application Monitoring feature. If the heartbeats for an application are not received for a specified time, Application Monitoring restarts its virtual machine.

vSphere Fault Tolerance

vSphere Fault Tolerance on the ESXi host platform provides continuous availability by protecting the primary virtual machine virtual machine with a secondary virtual machine that runs simultaneously on a separate host. Inputs and events performed on the primary virtual machine are recorded and replayed on the secondary virtual machine, which ensures that the two remain in an identical state. For example, mouse-clicks and keystrokes are recorded on the primary virtual machine and replayed on the secondary virtual machine. Because the secondary virtual machine is running simultaneously with the primary virtual machine, it can take over at any point without service interruption or loss of data.

For more information on vMotion and Storage vMotion, see the *vCenter Server and Host Management* documentation. For more information on DRS, HA, and Fault Tolerance, see the *vSphere Availability* documentation.

Network Architecture

VMware vSphere has a set of virtual networking elements that lets you network the virtual machines in the datacenter like physical machines are networked in a physical environment.

The virtual environment provides networking elements similar to those in the physical environment. They are virtual network interface cards (virtual NICs), vSphere Distributed Switches (VDS), distributed port groups, vSphere Standard Switches (VSS), and port groups.

Each virtual machine has one or more virtual NICs. The guest operating system and application programs communicate with a virtual NIC through either a commonly available device driver or a VMware device driver optimized for the virtual environment. In either case, communication in the guest operating system occurs just as it would with a physical device. Outside the virtual machine, the virtual NIC has its own MAC address and one or more IP addresses. It responds to the standard Ethernet protocol as would a physical NIC. An outside agent does not detect that it is communicating with a virtual machine.

A virtual switch works like a layer 2 physical switch. With vSphere Standard Switch, each server has its own virtual switches. With vSphere Distributed Switch, a single virtual switch spans many servers. On one side of the virtual switch are port groups that connect to virtual machines. On the other side are uplink connections to physical Ethernet adapters on the servers. Virtual machines connect to the physical environment through the physical Ethernet adapters that are connected to the virtual switch uplinks.

A virtual switch can connect its uplinks to more than one physical Ethernet adapter to enable NIC teaming. With NIC teaming, two or more physical adapters can be used to share the traffic load or provide passive failover if a physical adapter hardware fails or a network outage occurs.

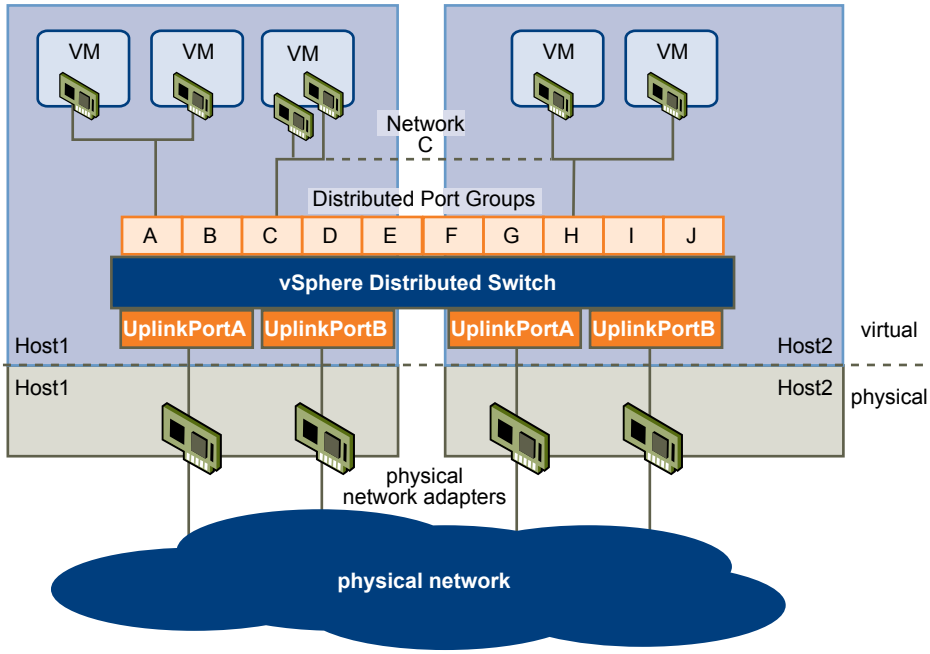
A port group is a unique concept in the virtual environment. A port group is a mechanism for setting policies that govern the network connected to it. For VDS, the groups are called distributed port groups. A virtual switch can have multiple port groups. Instead of connecting to a particular port on the virtual switch, a virtual machine connects its virtual NIC to a port group. Virtual machines that connect to the same port group belong to the same network inside the virtual environment even if they are on different physical servers.

You can configure port groups to enforce policies that provide enhanced networking security, network segmentation, better performance, high availability, and traffic management.

Networking with vSphere Distributed Switches

A vSphere Distributed Switch (VDS) functions as a single virtual switch across all associated hosts. This ability allows virtual machines to maintain consistent network configuration as they migrate across multiple hosts. Each VDS is a network hub that virtual machines can use. A VDS can route traffic internally between virtual machines or link to an external network by connecting to physical Ethernet adapters. Each VDS can also have one or more distributed port groups assigned to it. Distributed port groups aggregate multiple ports under a common configuration and provide a stable anchor point for virtual machines connecting to labeled networks.

Figure 2-7. Relationship Between the Networks with vSphere Distributed Switches Inside and Outside the Virtual Environment



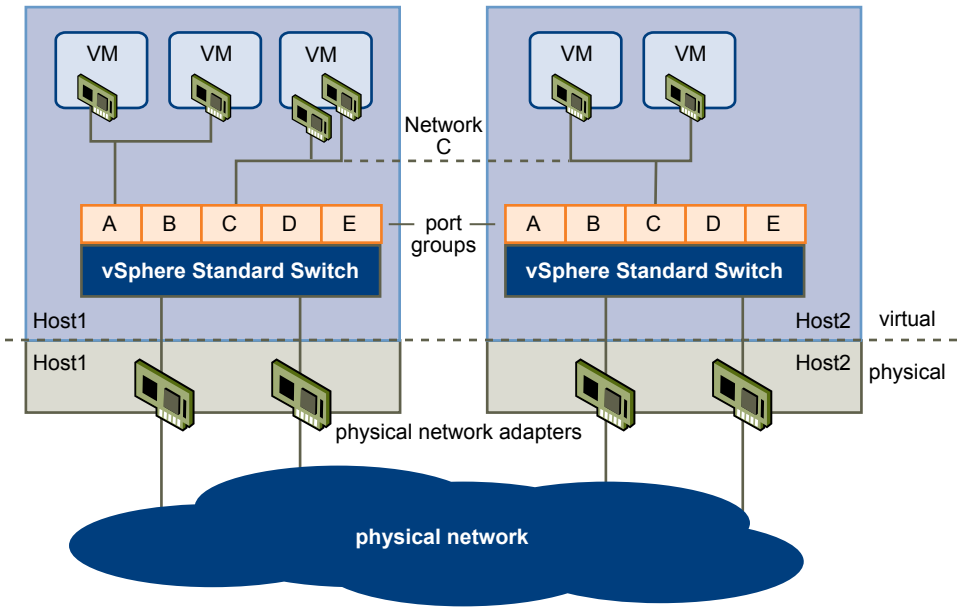
Network resource pools determine the priority that different network traffic types are given on a VDS. When network resource management is enabled, VDS traffic is divided into the following network resource pools: FT traffic, iSCSI traffic, vMotion traffic, management traffic, NFS traffic, and virtual machine traffic. You can control the priority for the traffic from each of these network resource pools by setting the physical adapter shares and host limits for each network resource pool.

The VMware virtual switching layer provides a set of features similar to traditional physical switches, like VLANs, traffic shaping, and monitoring.

Networking with vSphere Standard Switches

With vSphere Standard Switches, each server has its own virtual switch: VSSs handle network traffic at the host level in a vSphere environment. A VSS can route traffic internally between virtual machines and link to external networks.

Figure 2-8. Relationship Between the Networks with vSphere Standard Switches, Inside and Outside the Virtual Environment



See the *vSphere Networking* documentation.

VMware vShield and Network Security

VMware vShield is a suite of security virtual appliances that are built to work with vSphere, protecting virtualized datacenters from attacks and misuse.

VMware vShield is not a component of vSphere, but as a companion to vSphere it provides security for applications and data in the cloud.

The vShield suite includes vShield Zones, vShield Edge, vShield App, and vShield Endpoint.

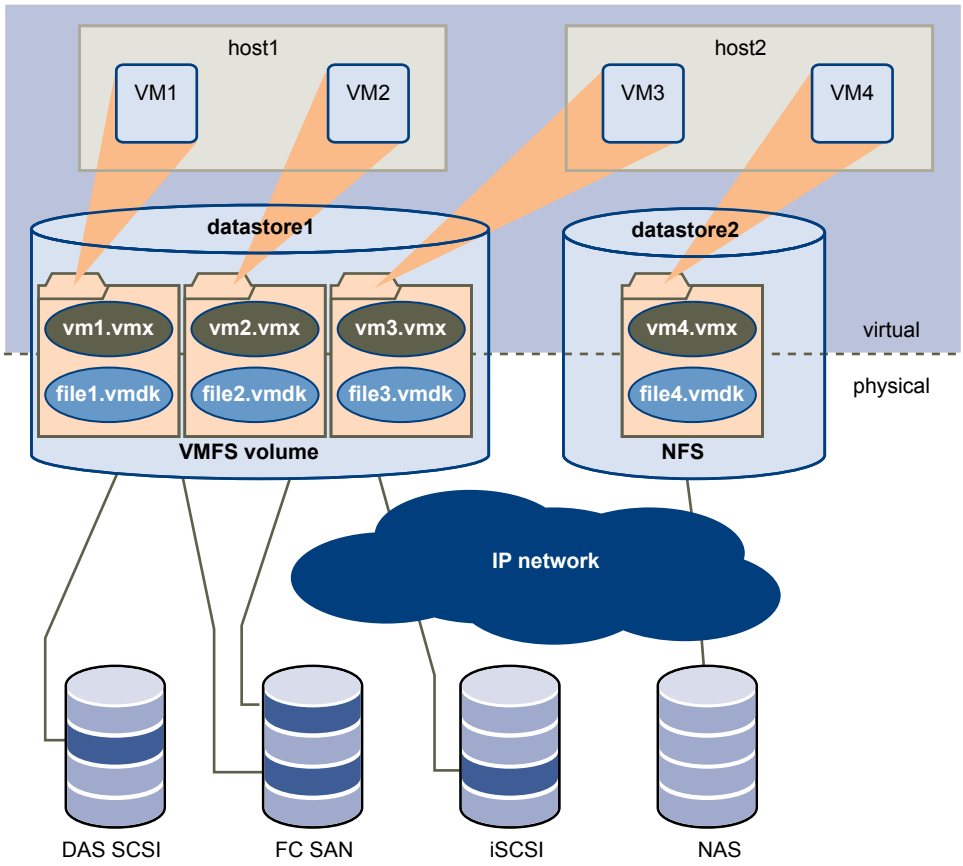
- vShield Zones provides firewall protection for traffic between virtual machines. For each Zones Firewall rule, you can specify the source IP, destination IP, source port, destination port, and service.
- vShield Edge provides network edge security and gateway services to isolate the virtual machines in a port group, distributed port group, or Cisco Nexus 1000V. vShield Edge connects isolated, stub networks to shared, uplink networks by providing common gateway services such as DHCP, VPN, NAT, and load balancing. Common deployments of vShield Edge include in the DMZ, VPN extranets, and multitenant cloud environments where vShield Edge provides perimeter security for virtual datacenters (VDCs).
- vShield App is an interior, virtual-NIC-level firewall that allows you to create access control policies regardless of network topology. vShield App monitors all traffic in and out of an ESXi host, including between virtual machines in the same port group. vShield App includes traffic analysis and container-based policy creation.
- vShield Endpoint delivers an introspection-based antivirus solution. vShield Endpoint uses the hypervisor to scan guest virtual machines from the outside without an agent. vShield Endpoint avoids resource bottlenecks while optimizing memory use.

See the *vShield Administration Guide*.

Storage Architecture

The VMware vSphere storage architecture consists of layers of abstraction that hide the differences and manage the complexity among physical storage subsystems.

Figure 2-9. Storage Architecture



To the applications and guest operating systems inside each virtual machine, the storage subsystem appears as a virtual SCSI controller connected to one or more virtual SCSI disks. These controllers are the only types of SCSI controllers that a virtual machine can see and access. These controllers include BusLogic Parallel, LSI Logic Parallel, LSI Logic SAS, and VMware Paravirtual.

The virtual SCSI disks are provisioned from datastore elements in the datacenter. A datastore is like a storage appliance that delivers storage space for virtual machines across multiple physical hosts. Multiple datastores can be aggregated into a single logical, load-balanced pool called a datastore cluster.

The datastore abstraction is a model that assigns storage space to virtual machines while insulating the guest from the complexity of the underlying physical storage technology. The guest virtual machine is not exposed to Fibre Channel SAN, iSCSI SAN, direct attached storage, and NAS.

Each datastore is a physical VMFS volume on a storage device. NAS datastores are an NFS volume with VMFS characteristics. Datastores can span multiple physical storage subsystems. A single VMFS volume can contain one or more LUNs from a local SCSI disk array on a physical host, a Fibre Channel SAN disk farm, or iSCSI SAN disk farm. New LUNs added to any of the physical storage subsystems are detected and made available to all existing or new datastores. Storage capacity on a previously created datastore can be extended without powering down physical hosts or storage subsystems. If any of the LUNs within a VMFS volume fails or becomes unavailable, only virtual machines that use that LUN are affected. An exception is the LUN that has the first extent of the spanned volume. All other virtual machines with virtual disks residing in other LUNs continue to function as normal.

Each virtual machine is stored as a set of files in a directory in the datastore. The disk storage associated with each virtual guest is a set of files within the guest's directory. You can operate on the guest disk storage as an ordinary file. The disk storage can be copied, moved, or backed up. New virtual disks can be added to a virtual machine without powering it down. In that case, a virtual disk file (`.vmdk`) is created in VMFS to provide new storage for the added virtual disk or an existing virtual disk file is associated with a virtual machine.

VMFS is a clustered file system that leverages shared storage to allow multiple physical hosts to read and write to the same storage simultaneously. VMFS provides on-disk locking to ensure that the same virtual machine is not powered on by multiple servers at the same time. If a physical host fails, the on-disk lock for each virtual machine is released so that virtual machines can be restarted on other physical hosts.

VMFS also features failure consistency and recovery mechanisms, such as distributed journaling, a failure-consistent virtual machine I/O path, and virtual machine state snapshots. These mechanisms can aid quick identification of the cause and recovery from virtual machine, physical host, and storage subsystem failures.

VMFS also supports raw device mapping (RDM). RDM provides a mechanism for a virtual machine to have direct access to a LUN on the physical storage subsystem (Fibre Channel or iSCSI only). RDM supports two typical types of applications:

- SAN snapshot or other layered applications that run in the virtual machines. RDM better enables scalable backup offloading systems using features inherent to the SAN.
- Microsoft Clustering Services (MSCS) spanning physical hosts and using virtual-to-virtual clusters as well as physical-to-virtual clusters. Cluster data and quorum disks must be configured as RDMs rather than files on a shared VMFS.

For more information on storage, see the *vSphere Storage* documentation.

Management Layer: VMware vCenter Server

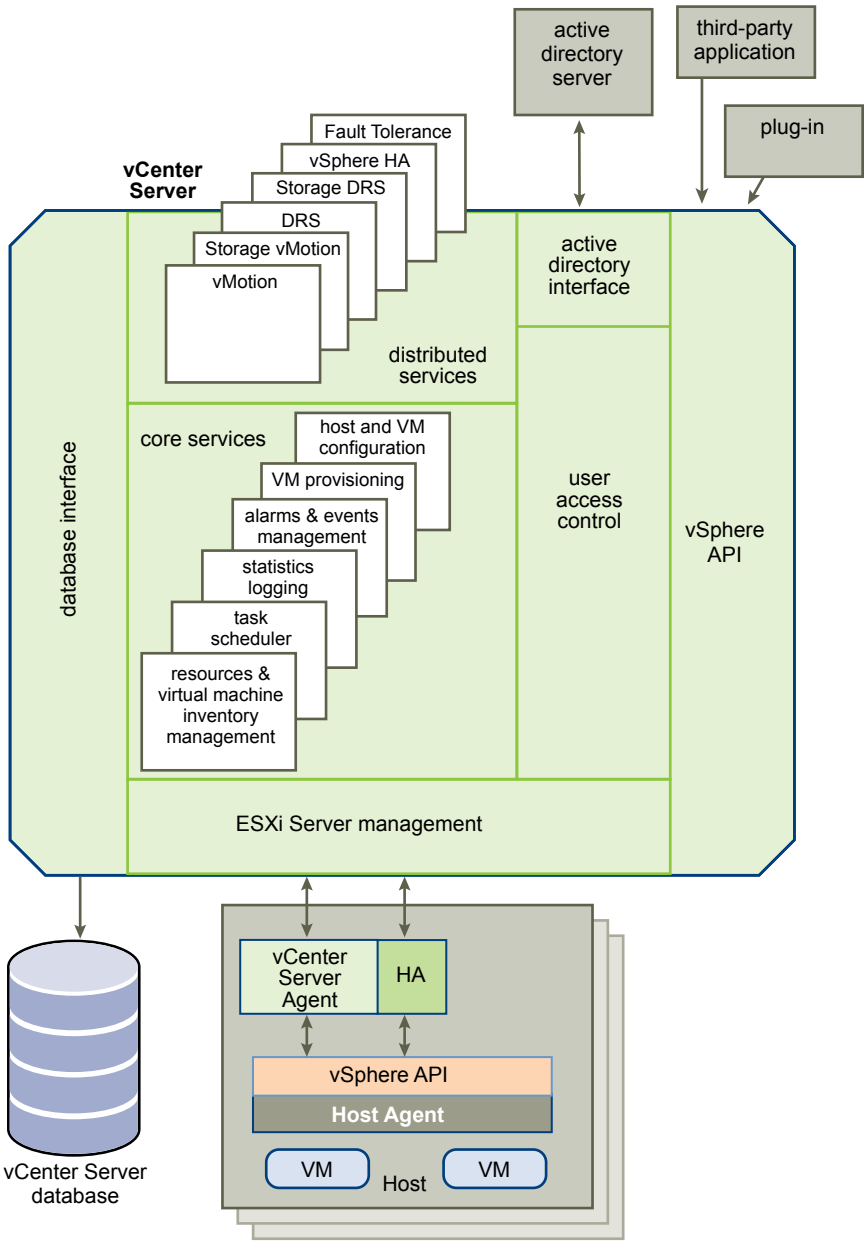
3

VMware vCenter Server provides centralized management for datacenters.

vCenter Server aggregates physical resources from multiple ESXi hosts and presents a central collection of flexible resources for the system administrator to provision to virtual machines in the virtual environment.

vCenter Server components are user access control, core services, distributed services, plug-ins, and various interfaces.

Figure 3-1. vCenter Server Components



The User Access Control component allows the system administrator to create and manage different levels of access to vCenter Server for different classes of users.

For example, a user class might manage and configure the physical virtualization server hardware in the datacenter. Another user class might manage virtual resources within a particular resource pool in the virtual machine cluster.

This chapter includes the following topics:

- "vCenter Server Core Services," on page 31
- "vCenter Server Plug-Ins," on page 31
- "vCenter Server Interfaces," on page 32

vCenter Server Core Services

Core Services are basic management services for a virtual datacenter.

Core Services include the following services:

Virtual machine provisioning	Guides and automates the provisioning of virtual machines and their resources.
Host and VM configuration	Allows the configuration of hosts and virtual machines.
Resources and virtual machine inventory management	Organizes virtual machines and resources in the virtual environment and facilitates their management.
Statistics and logging	Logs and reports on the performance and resource use statistics of datacenter elements, such as virtual machines, hosts, storage, and clusters.
Alarms and event management	Tracks and warns users on potential resource overuse or event conditions. You can set alarms to trigger on events and notify when critical error conditions occur. Alarms are triggered only when they satisfy certain time conditions to minimize the number of false triggers.
Task scheduler	Schedules actions such as vMotion to occur at a given time.
vApp	A vApp has the same basic operation as a virtual machine, but can contain multiple virtual machines or appliances. With vApps, you can perform operations on multitier applications as separate entities (for example, clone, power on and off, and monitor). vApps package and manage those applications.

Multiple vCenter Server systems can be combined into a single connected group. When a vCenter Server system is part of a connected group, you can view and manage the inventories of all vCenter Server systems in that group.

vCenter Server Plug-Ins

vCenter Server plug-ins extend the capabilities of vCenter Server by providing more features and functions.

Some plug-ins are installed as part of the base vCenter Server product.

vCenter Storage Monitoring	Allows you to review information on storage usage and to visually map relationships between all storage entities available in vCenter Server.
vCenter Hardware Status	Uses CIM monitoring to display the hardware status of hosts that vCenter Server manages.
vCenter Service Status	Displays the status of vCenter services.

Some plug-ins are packaged separately from the base product and require separate installation. You can update plug-ins and the base product independently of each other. VMware modules include:

vSphere Update Manager (VUM)	Enables administrators to apply updates and patches across ESXi hosts and all managed virtual machines. Administrators can create user-defined security baselines that represent a set of security standards. Security administrators can compare hosts and virtual machines against these baselines to identify and remediate systems that are not in compliance.
vShield Zones	An application-aware firewall built for vCenter Server integration. vShield Zones inspects client-server communications and communications between virtual machines to provide detailed traffic analytics and application-aware firewall partitioning. vShield Zones is a critical security component for protecting virtualized datacenters from network-based attacks and misuse.
vCenter Orchestrator	A workflow engine that enables you to create and run automated workflows in your vSphere environment. vCenter Orchestrator coordinates workflow tasks across multiple VMware products and third-party management and administration solutions through its open plug-in architecture. vCenter Orchestrator provides a library of workflows that are extensible. You can use any operation available in the vCenter Server API to customize vCenter Orchestrator workflows.
Data Recovery	A disk-based backup and recovery solution that provides complete data protection for virtual machines. Data Recovery is fully integrated with vCenter Server to enable centralized and efficient management of backup jobs and includes data deduplication to minimize disk usage.

vCenter Server Interfaces

vCenter Server interfaces integrate vCenter Server with third party products and applications.

vCenter Server has the following key interfaces:

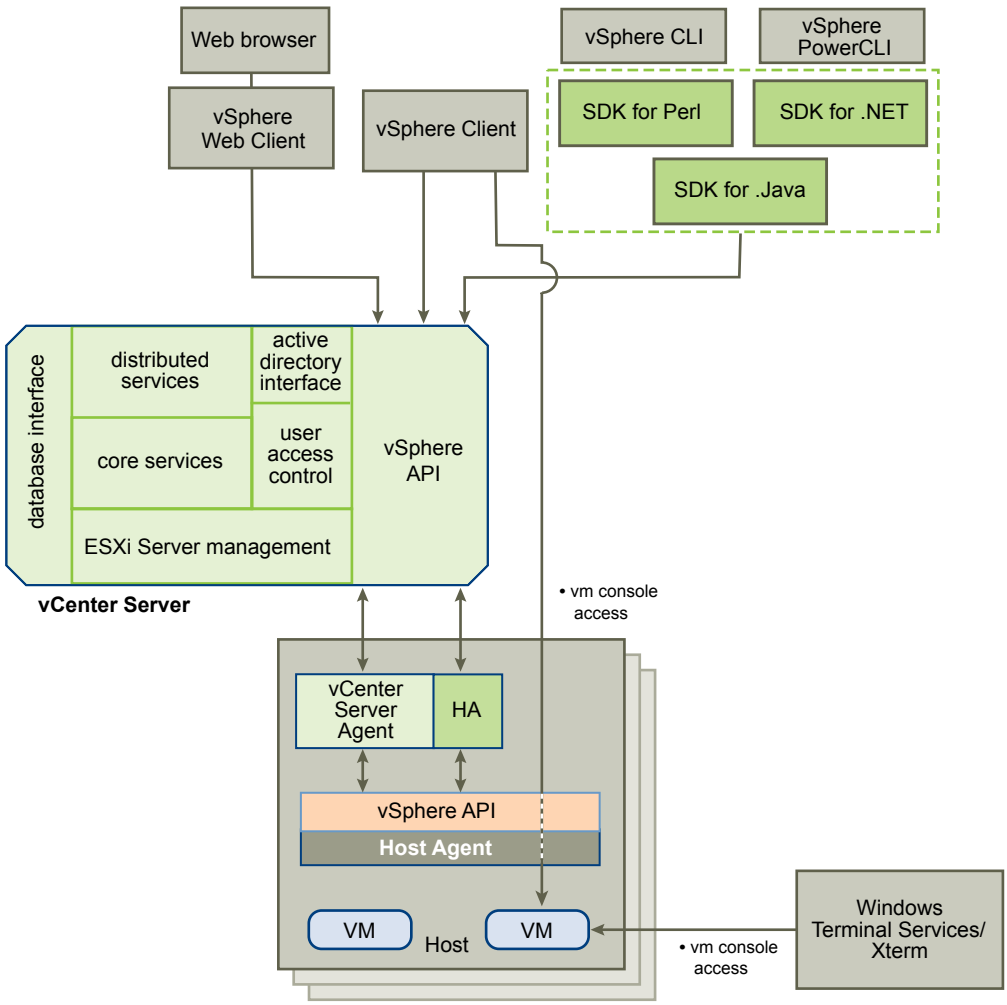
ESXi server management	Interfaces with the vCenter Server agent to manage each physical server in the datacenter.
VMware vSphere API	Interfaces with VMware management clients and third-party solutions.
Active Directory interface	Connects to Active Directory to obtain user access control information.
Database interface	Connects to Oracle, Microsoft SQL Server, or IBM DB2 to store information, such as virtual machine configurations, host configurations, resources and virtual machine inventory, performance statistics, events, alarms, user permissions, and roles.

Interface Layer: Accessing the Virtual Infrastructure

4

Users can access a VMware vSphere datacenter through the vSphere Client, through a Web browser with vSphere Web Client, through a command line interface, or terminal services (such as Windows Terminal Services).

Figure 4-1. VMware vSphere Access and Control



This chapter includes the following topics:

- "vSphere Client and vSphere Web Client," on page 34
- "SDKs and Command-Line Interfaces," on page 35
- "Direct Virtual Machine Console Access," on page 36

vSphere Client and vSphere Web Client

All administrative functions are available through the vSphere Client. A subset of those functions is available through the vSphere Web Client.

Table 4-1. Comparing the Two Clients

vSphere Client	vSphere Web Client
For infrastructure configuration and day-to-day operations.	For day-to-day operations.
■ Locally installed application. ■ Windows operating system only. ■ Can connect to vCenter Server or directly to hosts. ■ Full range of administrative functionality.	■ Web application. ■ Cross platform. ■ Can connect to only vCenter Server. ■ Subset of full functionality, focused on virtual machine deployment and basic monitoring functions. Cannot configure hosts, clusters, networks, datastores, or datastore clusters. ■ Extensible plug-in-based architecture.
Users: Virtual infrastructure administrators for specialized functions.	Users: Virtual infrastructure administrators, help desk, network operations center operators, virtual machine owners.

The vSphere Client uses the VMware API to access vCenter Server. After the user is authenticated, a session starts in vCenter Server, and the user sees the resources and virtual machines that are assigned to the user. For virtual machine console access, the vSphere Client first uses the VMware API to obtain the virtual machine location from vCenter Server. The vSphere Client then connects to the appropriate host and provides access to the virtual machine console.

Users can use the vSphere Web Client to access vCenter Server through a Web browser. The vSphere Web Client uses the VMware API to mediate the communication between the browser and the vCenter Server.

Using the vSphere Client

The vSphere Client is a downloadable interface for administering vCenter Server and ESXi.

The vSphere Client user interface is configured based on the server to which it is connected:

- When the server is a vCenter Server system, the vSphere Client displays all the options available to the vSphere environment, according to the licensing configuration and the user permissions.
- When the server is an ESXi host, the vSphere Client displays only the options appropriate to single host management.

You perform many management tasks from the Inventory view, which consists of a single window containing a menu bar, a navigation bar, a toolbar, a status bar, a panel section, and pop-up menus.

First Time Use

The vSphere Client includes embedded assistance that guides users who are new to virtualization concepts through the steps to set up their virtual infrastructure. This embedded assistance is in-line content presented in the vSphere Client GUI and an online tutorial. You can turn off the assistance for experienced users. You can turn on assistance when new users are introduced to the system.

Using the vSphere Web Client

The vSphere Web Client is a browser-based interface for configuring and administering virtual machines.

When you first log in to the vSphere Web Client, a home page appears with an object navigator pane that you can use to browse for inventory objects. The home page also contains a search box that you can use to run a global search across all applications and objects, a central pane that contains information about a selected object, and a side panel that contains panes for tasks, events, and so on.

You can return to partially finished work by using the Work in Progress pane. In the My Recent Tasks pane, you can see completed tasks, failed tasks, and tasks that are currently running.

SDKs and Command-Line Interfaces

VMware provides features and tools for automating administration tasks.

vSphere includes CLI commands for provisioning, managing, and monitoring hosts and virtual machines. vSphere SDKs provide standard interfaces for VMware and third-party solutions to access vSphere.

vSphere PowerCLI

A command-line scripting tool built on Windows PowerShell that provides cmdlets for managing and automating vSphere.

vSphere PowerCLI provides C# and PowerShell interfaces to VMware vSphere APIs. It includes a number of cmdlets that you can use to perform administration tasks on VMware vSphere components.

Microsoft PowerShell uses the .NET object model and provides administrators with management and automation capabilities.

vSphere SDK for Perl

A client-side Perl framework that provides an interface to the vSphere API. Administrators and developers who are familiar with Perl can use the vSphere SDK for Perl to automate administrative, provisioning, and monitoring tasks in the vSphere environment. The vSphere SDK for Perl includes utility applications.

vSphere CLI (vCLI)

You can use the vSphere CLI command set to run common administration commands against VMware ESXi systems from any machine with network access to those systems. You can run most vSphere CLI commands against a vCenter Server system and target any ESXi system that the vCenter Server system manages. Most administrators run scripts to perform the same task repeatedly or to perform a task on multiple hosts.

vSphere CLI commands run on top of the vSphere SDK for Perl. vSphere CLI is supported on Linux and Windows platforms.

vSphere SDK for .NET

A client-side framework from VMware that simplifies the programming effort associated with the vSphere API and server-side object model. It is a part of VMware vSphere PowerCLI, which provides C# and PowerShell interfaces to vSphere APIs. Using vSphere SDK for .NET you can create, customize, or manage vSphere inventory objects using vSphere APIs calls.

vSphere Web Services SDK

Includes all the components necessary to work with the VMware vSphere API, including WSDL files, sample code, and libraries. The vSphere Web Services SDK facilitates development of client applications that target the VMware vSphere API. With the vSphere Web Services SDK, developers can create client applications to manage, monitor, and maintain VMware vSphere components, as deployed on ESXi and VMware vCenter Server systems.

Direct Virtual Machine Console Access

If the virtual machine is running and the user knows the IP address of the virtual machine, the user can directly access the virtual machine console by using standard tools, such as Windows Terminal Services.

Only physical host administrators in special circumstances should directly access hosts. All relevant functions that can be done on the host can also be done in vCenter Server.

Index

A

Active Directory interface **32**
alarms **31**
APIs, database interface **32**

B

baselines, security **31**

C

CLI **35**
clusters **18**
command-line interface, *See* CLI
components
  fault tolerance **12**
  host profiles **12**
  Storage DRS **12**
  VMware ESXi **12**
  VMware vCenter Server **12**
  VMware vSphere client **12**
  vSphere Distributed Resource Scheduler **12**
  vSphere Distributed Switch **12**
  vSphere High Availability **12**
  vSphere SDKs **12**
  vSphere Storage vMotion **12**
  vSphere Virtual Machine File System **12**
  vSphere vMotion **12**
consolidation **31**

D

database interface **32**
distributed port groups **23**
distributed services
  vSphere DRS **20**
  vSphere HA **20**
  vSphere Storage vMotion **20**
  vSphere vMotion **20**
DRS **12, 20**

E

ESXi, management **32**
ESXi management **32**
event management **31**

F

fault tolerance **12**

H

HA **12, 20**
high availability **20**
host and VM configuration **31**
host profiles **12**
hosts **18**

L

logging **31**

N

network, security **25**
network architecture **23**

P

physical topology
  computing servers **14**
  desktop clients **14**
  IP networks **14**
  storage networks and arrays **14**
  vCenter Server **14**
port group **23**
preface **5**

R

resource pools **18**

S

SDK **12, 35**
security, baselines **31**
server, consolidation **7**
server consolidation **7**
standard switch **23**
statistics **31**
storage architecture **26**
Storage DRS **12, 20**
Storage vMotion **12, 20**

T

task scheduler **31**

V

vApp **31**
vCenter Server
  core services **31**

interfaces **32**
plug-ins **31**
VDS **23**
virtual datacenter, architecture **17**
virtual infrastructure, accessing **33**
virtual machine inventory management **31**
virtual machines
convert **31**
direct access to console **36**
security compliance **31**
virtual NIC **23**
virtualization **7**
VM provisioning **31**
VMFS **12**
vMotion **12, 20**
VMware vCenter Server **29**
VMware vSphere
components **12**
introduction **7, 10**
VMware vSphere API **32**
vShield **25**
vSphere client **12**
vSphere Distributed Switch **12, 23**
vSphere Update Manager **31**

W

web access, vSphere Client **34**
Windows Terminal Services **36**