Universidade Lusófona de Humanidades e Tecnologias

Licenciatura em Engenharia Informática

Virtualization

Virtualization based on VMware vSphere, Virtual Desktops, Cloud and Remote Access Software

Projecto apresentado como requisito parcial para obtenção de grau Lincenciado em Engenharia Informática

Orientador: Prof. Doutor José Faísca, ULHT

Yassir Haji

October 2012

ACKNOWLEDGEMENTS

This project represents a lot of hours searching, reading and studying. It is the end of a long journey and i hope that it is the beginning of new ones.

Although this project represents the compilation of my own efforts, first i would like to thank my advisor, Professor José Faisca for his invaluable guidance, support and knowledge, and many thanks to everyone that supported me directly or indirectly, specially my friends, teachers and colleagues.

Finally, i would like to specially thank my parents for their understanding, support and patience for my study.

Lisbon, October 2012

ABSTRACT

Virtualization is a technology extensively understood and generally adapted, it has many benefits, allowing a better CPU and Memory utilization, reducing management costs and energy consumption, improving availability and disaster recovery.

Virtualization creates flexible and cost effective IT infrastructures, can be applied to almost all its parts and is a key enabling technology for cloud computing environments.

This study represents a brief overview at server virtualization with VMware vSphere Platform regarding management, high availability and security. Server Virtualization is reshaping datacenters landscape, and companies themselves.

First, we present the technology based on server virtualization, next it is presented the design of the solution based on VMware vSphere following implementation and configuration. It is also demonstrated VMware solutions for cloud and desktop virtualization, followed by different forms of remote accessing servers using open source software.

Keywords: Virtualization, VMware, vSphere, Cloud, Remote Desktop

ABSTRACT

Virtualização é uma tecnologia extensa geralmente percebida e implementada, cujos benefícios são imensos, tais como, a optimização da utilização de recursos como o CPU e a memória, reduzindo os custos de gestão e de energia, melhorando também a disponiblidade e situações de desastre.

A virtualização permite a criação de uma infraestrutura de IT flexível e com custos reduzidos, que por sua vez pode ser aplicada a quase todas as partes da infraestrutura, que por sua vez também é uma chave importante para ambientes de cloud computing.

A virtualização de servidores está a alterar o modo de funcionamento dos datacenter e das próprias empresas.

Este estudo representa um breve sumário sobre a virtualização baseada na plataforma da VMware o vSphere em relação à gestão e à alta disponibilidade.

Primeiramente, apresento a tecnologia, a sua arquitectura e o modo de funcionamento.

Também é demonstrado a tecnologia de Cloud da VMware e de virtualização de desktops, seguido de várias formas de conexão a servidores virtuais utilizando aplicações de acesso remoto open source.

Palavras-chave: Virtualização, VMware, vSphere, Cloud, Remote Desktop

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AD-Active Directory

ADM-V-AMD Virtualization

API-Application Programming Interface

ARP -Address Resolution Protocol

COS-Console Operating System

CPU-Central Processing Unit

DHCP-Dynamic Host Configuration Protocol

DHCP -Dynamic Host Configuration Protocol

DMZ-Demilitarized Zone

DNS-Domain Name System

DNS-Domain Name System

DR -Disaster Recovery

DRS-Distributed Resource Scheduler

ESX-Elastic Sky X

GPO- Group Policy

HA-High Availability

HCL-Hardware Compatibility List

HTTP- Hypertext Transfer Protocol

HTTPS- Hypertext Transfer Protocol Secure

ICMP-Internet Control Message Protocol

Intel VT-Intel Virtualization Technology

LUN-Logical Unit

NAT-Network Address Translation

NTP-Network Time Protocol

OS-Operating System

RAID-Redundant Array of Independent Disks

RAM-Random Access Memory

VCD-vCloud Director

VDI-Virtual Desktop Infrastructure

VLAN-Virtual Local Area Networks

VM-Virtual Machine

VMM-Virtual Machine Monitor

VPN-Virtual Private Network

x86 -Family of instruction set architectures based on the Intel 8086

1. INTRODUCTION

Virtualization refers to abstracting, or masking a physical resource to make it appear different logically to what is physically, it detaches the software environment from its hardware allowing to consolidate multiple servers, networks and storage infrastructure into pools of resources. Dynamically delivering those resources, reliably and securely, to applications on demand. With this approach customers can use building blocks of inexpensive industry-standard servers to build a self-optimizing datacenter and deliver high levels of utilization, availability, automation and flexibility.

Virtualization has become an overall trend in enterprise IT that includes autonomic computing, a scenario in which the IT environment will be able to manage itself based on perceived activity, and utility computing, in which computer processing power is seen as a utility that clients can pay for only as needed. The main objective of virtualization is to centralize administrative tasks while improving scalability and workloads.

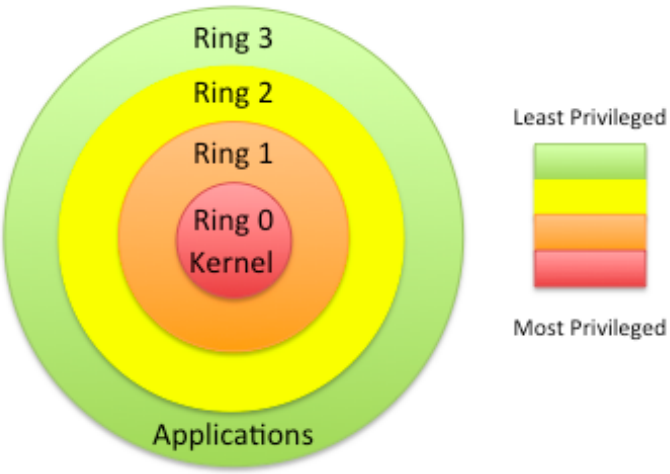
There are three areas of IT where virtualization is making the difference, all of which carry out important tasks in businesses: network virtualization, storage virtualization and server virtualization, it can be considered as if virtualization is the creation of a virtual version of something, such as an operating system, a server, a storage device or network resources.

The term server virtualization is usually used as a synonym for virtual machine technology, as it is a generally used form of server virtualization technology for today based x86 servers.

2. VIRTUALIZATION

Virtualization works by inserting a thin layer of software directly on a host operating system or on the computer hardware, a virtual machine monitor (VMM) or "hypervisor" that allocates hardware resources transparently and dynamically. Multiple operating systems can run at the same time on a single physical computer and share hardware resources between them, by encapsulating an entire machine, including memory, CPU, operating system, scsi devices and network devices, a virtual machine is fully compatible with all standard x86 operating systems, applications, and device drivers.

The x86 processor family has been designed with 4 levels of privilege also called rings. Ring 0 represent the most privileged and the ring 3 represent the least privileged. Ring 0 contains the most critical software which is generally the kernel of the operating system.



With virtualization the hypervisor is installed on ring 0 and has the most privileged level. Also the OS will run at ring 1 because ring 0 is occupied by the hypervisor. To have the OS running on ring 1 without any modification, INTEL and AMD modified the x86 processors.

2.1 Virtual Infrastructure

A virtual infrastructure lets you share your physical resources of multiple machines across your entire infrastructure. A virtual machine lets you share the resources of a single physical computer across multiple virtual machines for maximum efficiency. Resources are shared across multiple virtual machines and applications. Your business needs are the driving force behind dynamically mapping the physical resources of your infrastructure to applications—even as those needs evolve and change. Aggregate your servers along with network and storage into a unified pool of IT resources that can be utilized by the applications when and where they're needed. This resource optimization drives greater flexibility in the organization and results in lower capital and operational costs.

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 and consolidated backup to optimize available resources among virtual machines.
- Automation solutions that provide special capabilities to optimize a particular IT process such as provisioning, availability and/or disaster recovery.

2.2 CPU Virtualization:

There are many challenges to x86 hardware virtualization, as these systems are designed to run on bare-metal hardware as if they totally control the computer hardware.

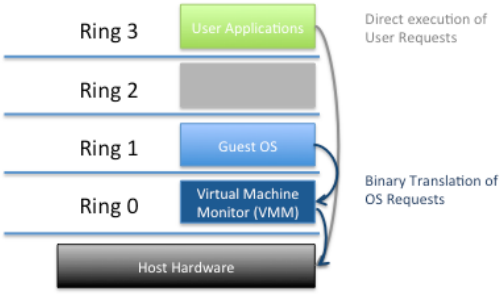
This architecture has four privilege levels, Ring 0, 1, 2, 3. User applications typically usually run on ring 3, the OS must have direct access to the memory and hardware and must execute its privileged instructions on ring 0.

Virtualizing the x86 architecture requires placing a virtualization layer that delivers shared resources under the operating system which is expecting to be in the most privileged Ring 0, to create and manage the virtual machines.

There are three main technologies to virtualize a guest OS:

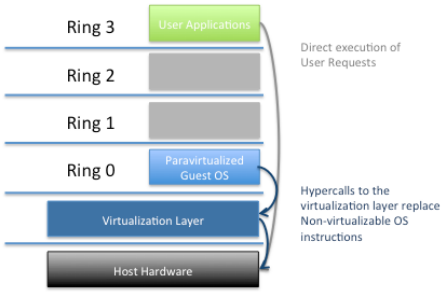
- Full Virtualization using binary translation
- OS assisted virtualization or Paravirtualizarion
- Hardware assisted virtualization

Full virtualization: Almost completes simulation of the actual hardware to allow software, which typically consists of a guest operating system, to run unmodified, also designated by binary translation. With this technology the guest OS is provided with all the services from the physical environment, BIOS, virtual devices, memory etc..

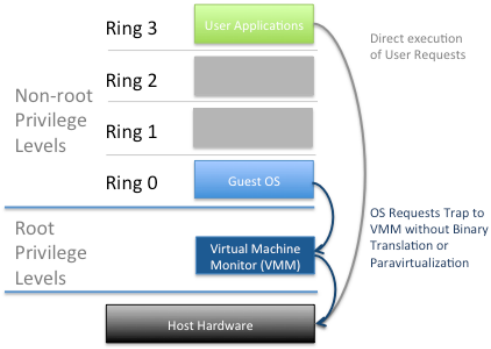


The VMM runs on ring 0 and the guest OS runs on ring 1.

Paravirtualization: A hardware environment is not simulated; however, the guest programs are executed in their own isolated domains, as if they are running on a separate system. Guest programs need to be specifically modified to run in this environment as they are required to translate non-virtualizable instruction with hypercalls, allowing the guest OS to communicate with the hypervisor. This kind of virtualization degrades compatibility and portability of the systems, enhancing its performance.



Hardware-assisted virtualization is a way of improving the efficiency of hardware virtualization. It involves employing specially designed CPUs and hardware components that help improve the performance of a guest environment, allows the guest OS to communicate with the VMM without modifications. The processors trap OS requests that come from ring 1, ring 0 is transformed as ring -1 and ring 1 is a ring 0 where the guest OS can operate removing the need for binary translation and paravirtualization.



2.3 Memory Virtualization

Involves sharing the physical system memory and dynamically allocating it to virtual machines.
Applications see a contiguous address space that is not necessarily tied to the underlying physical memory in the system. The operating system keeps mappings of virtual page numbers to physical page numbers stored in page tables. All modern x86 CPUs include a memory management unit (MMU) and a translation look aside buffer (TLB) to optimize virtual memory performance.
The VMM is responsible for mapping guest physical memory to the actual machine memory, and it uses shadow page tables to accelerate the mappings.

2.4 Device and I/O Virtualization

Required beyond CPU and memory virtualization is device and I/O virtualization. This involves managing the routing of I/O requests between virtual devices and the shared physical hardware.
Software based I/O virtualization and management, in contrast to a direct pass-through to the hardware, enables a rich set of features and simplified management.
The hypervisor virtualizes the physical hardware and presents each virtual machine with a standardized set of virtual devices. These virtual devices effectively emulate well-known hardware and translate the virtual machine requests to the system hardware. This standardization on consistent device drivers also helps with virtual machine standardization and portability across platforms as all virtual machines are configured to run on the same virtual hardware regardless of the actual physical hardware in the system.

2.5 Types of Virtualization

- Software

Operating system-level virtualization, hosting of multiple virtualized environments within a single OS instance

Application virtualization and workspace virtualization, the hosting of individual applications in an environment separated from the underlying OS. Application virtualization is closely associated with the concept of portable applications.

Service virtualization, emulating the behavior of dependent (e.g, third-party, evolving, or not implemented) system components that are needed

to exercise an application under test (AUT) for development or testing purposes. Rather than virtualizing entire components, it virtualizes only specific slices of dependent behavior critical to the execution of development and testing tasks.

- Memory

Memory virtualization, aggregating RAM resources from networked systems into a single memory pool. Giving an application program the impression that it has contiguous working memory, isolating it from the underlying physical memory implementation

- Data

Data virtualization, the presentation of data as an abstract layer, independent of underlying database systems, structures and storage

- Storage

Storage virtualization is the process of completely abstracting logical storage from physical storage, pooling of physical storage from multiple network storage devices into what appears to be a single storage device that is managed from a central console. Storage virtualization is commonly used in storage area networks (SANs). This is also a great way to keep an eye on resources in a business, as you can then see exactly how much you have left at a given time.

- Network

Network Virtualization is when all of the separate resources of a network are combined, allowing the network administrator to share them out amongst the users of the network, it is a method of combining the available resources in a network by splitting up the available bandwidth into channels, each of which is independent from the others, and each of which can be assigned (or reassigned) to a particular server or device in real time. The idea is that virtualization disguises the true complexity of the network by separating it into manageable parts, much like your partitioned hard drive makes it easier to manage your files.

- Hardware Virtualization

Hardware virtualization or platform virtualization refers to the creation of a virtual machine that acts like a real computer with an operating system. Software executed on these virtual machines is separated from the underlying hardware resources. For example, a computer that is running Microsoft Windows may host a virtual machine that looks like a computer

with CentOS Linux operating system; CentOS based software can be run on the virtual machine.

In hardware virtualization, the host machine is the actual machine on which the virtualization takes place, and the guest machine is the virtual machine. The words host and guest are used to distinguish the software that runs on the actual machine from the software that runs on the virtual machine. The software or firmware that creates a virtual machine on the host hardware is called a hypervisor or Virtual Machine Monitor.

Hardware virtualization is not the same as hardware emulation: in hardware emulation, a piece of hardware imitates another, while in hardware virtualization, a hypervisor (a piece of software) imitates a particular piece of computer hardware or the whole computer altogether. Furthermore, a hypervisor is not the same as an emulator; both are computer programs that imitate hardware, but their domain of use in language differs.

2.7 Hypervisors

A bare-metal virtualization hypervisor does not require admins to install a server operating system first. Bare-metal virtualization means the hypervisor has direct access to hardware resources, which results in better performance, scalability and stability. One disadvantage of a bare-metal virtualization hypervisor, however, hardware support is limited, as the hypervisor usually has limited device drivers built into it.

Bare-metal virtualization is well suited for enterprise data centers, because it usually comes with advanced features for resource management, high availability and security. These systems can centrally managed, which is critical if the virtual infrastructure has many hosts. The most popular bare-metal virtualization hypervisors are:

- VMware ESX and ESXi
- Microsoft Hyper-V
- Citrix XenServer

Unlike the bare-metal virtualization hypervisor, a hosted hypervisor requires you to first install an OS. These hypervisors are basically like applications that install on a guest OS. This approach provides better hardware compatibility than bare-metal virtualization, because the OS is responsible for the hardware drivers instead of the hypervisor.

But, as with the bare-metal hypervisor, there are disadvantages. A hosted virtualization hypervisor does not have direct access to hardware and

must go through the OS, which increases resource overhead and can degrade the virtual machine (VM) performance. Also, because there are typically many services and applications running on the host OS, the hypervisor often steals resources from the VMs running on it.

Hosted hypervisors are common for desktops, because they allow you to run multiple Operating Systems. These virtualization hypervisor types are also popular for developers, to maintain application compatibility on modern Operating Systems.

The most popular hosted virtualization hypervisors are:

- Microsoft Virtual PC.
- Oracle VM VirtualBox.
- Parallels Desktop.
- VMware Player, Workstation and Fusion.

3. VMWARE VSPHERE

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

- 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.

- 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 Web Client. Additionally, users can access the datacenter through client machines that use command-line interfaces and SDKs for management.

3.1 VMware Hypervisors

VMware Hypervisor is available in two main types, VMware ESX and VMware ESXi, they are bare metal embedded hypervisors for guest virtual servers that run without requiring an aditional underlying operating system, ESX is being replaced by ESXi, as from version 5, only ESXi is available.

The ESX includes its own kernel, which runs after a Linux kernel, designated as vmkernel bootstraps the hardware, the service resulting is considered to be a microkernel and has three interfaces:

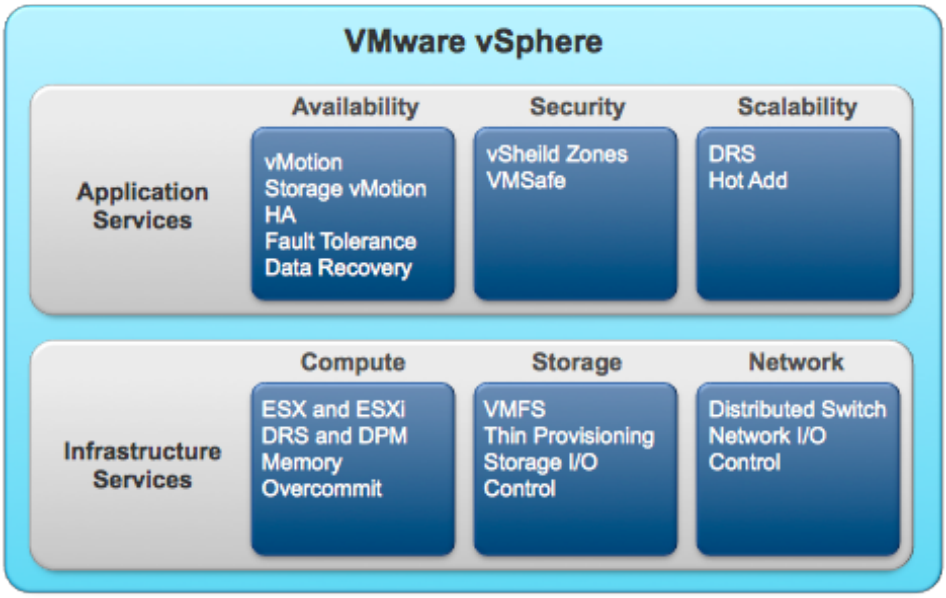
- Hardware
- Guest System
- Console Operating System (service console)

Some of the features of VMware ESXi Server are:

- The ESX architecture uses a service console for management, includes third-party agent installation and script execution. ESXi does not have the ESX service console, it is a smaller footprint version of ESX. ESXi migrates the management functionality from a local command line interface to remote management tools.
- ESXi has an ultra-thin architecture, because its smaller code-base presents a lesser attack area with less code to patch and due to its thinner architecture because of its more compact size and reduced number of components, ESXi needs fewer patches when compared to ESX shortening service windows and reduce security vulnerabilities.
- Security profiles configuration of ESXi have been made simpler, and instead of a full server console it uses a small direct console user interface.

3.2 Features

VMware vSphere includes the following components and features.



Using vCenter it enables some features depending on the licensing model. vCenter provides a centralized point of control to the datacenter, provides essential services such as access control, monitoring and configuration.

In the event where the vCenter becomes unavailable, the ESX hosts can be managed separately and the virtual machines allocated to them continue to run based on the last setting.

I will cover the 3 most important features that distinguish from other virtualization platforms.

vMotion enables the migration of powered on machines between physical servers with zero down time.

Storage vMotion enables the migration of virtual machine files from one datastore to another without interrupting the service. When migrating you can specify the locations for the virtual disks and the virtual machine configuration file.

High availability is obtained with vSphere HA and DRS, HA is a feature that in case of server failure, virtual machines are restarted on another available servers, and DRS auto-balances and allocates computing capacity in the same cluster. In version 5 it is available the Storage DRS, allowing the creation of datastore clusters balancing automatically storage space and i/o load.

3.3 File System

ESX/ESXi servers user VMware VMFS, Virtual Machine File System, it is a high performance cluster filesystem created by VMware. It is used to store virtual machine disk images, including snapshots. On the latest version, VMFS5 the block size is unified at 1MB.

64 ESX Servers can concurrently read and write to the same storage by using per-file lock. It has many features specially the fact that it allows live migration of powered-on virtual machines from a host server to another and by using distributed journaling, it is possible to recover VMs faster and more reliable in a case of a server failure.

Virtual machines files are stored on a datastore, and consists of the following types of files:

Configuration settings:

```
.vmx
.vmxf
```

Virtual Disks:

```
.vmdk
-flat.vmdk
```

Bios or EFI configuration:

```
.nvram
```

Sanpshots:

```
.vmsd
.vmsn
```

Swap:

```
.vswp
```

Suspend File:

```
.vmss
```

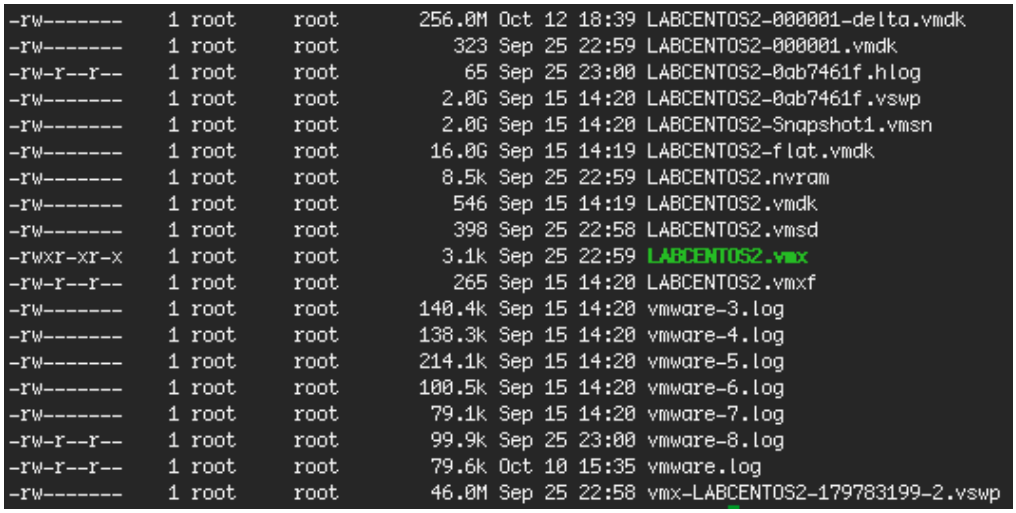
Log:

```
.log
-#.log
```

Example of a VM Directory:

/vmfs/volumes/<DatastoreName>/<VMName>

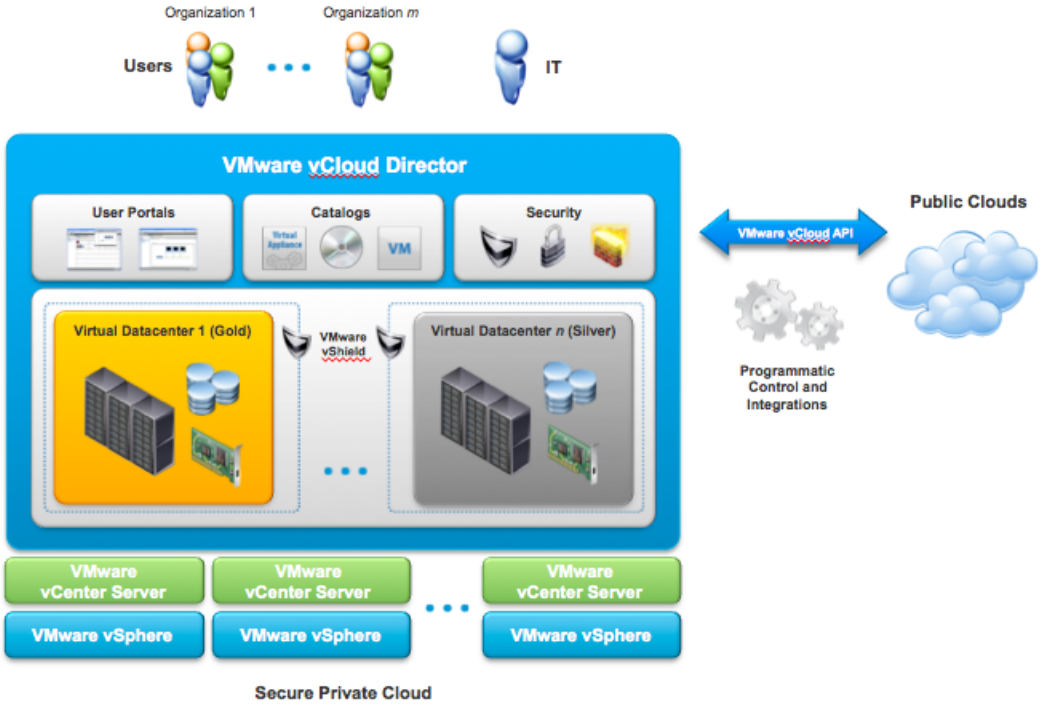
ls -lha /vmfs/volumes/LABCX4960SANVOL01/LABCENTOS2



3.4 vCloud

Infrastructure as a Service is a concept on cloud computing, which can be understood as the delivery of computing resources as a service.

VMware vCloud Director allows delivering infrastructure on demand. Administrators can create multiple types of clouds, hybrid, private and even public clouds by pooling resources to be consumed by users. With this solution it is available the creation of various types of pools, including compute, storage and network each with their custom policies.



As shown in the image above, its full integration with vSphere allows the configuration of multiple vCenters with many types of tiers supporting multi tenant environments.

3.5 Virtual Desktops

The desktop virtualization solution chosen was VMware View 5 as it is built on and integrated with vSphere, taking full advantage of all the features like, vMotion, snapshots and DRS.The advantages over traditional workstations exceed our expectations, provisioning and management are simpler and easier, data is secure on the datacenter and many features can be customized. The main components of this solution are:

View Client - Dedicated terminal (zero/thin client) or a client application running on a normal workstation (Linux/MacOS/Windows or a mobile device)

Display Protocol - View uses two protocols to access the virtual workstations, Microsoft Remote Desktop Protocol (RDP) and PC over IP (PCoIP). Although the RDP protocol is available, it should be used for lower-bandwith connections and for lower-demand situations. PCoIP with View integration supports high resolution, full frame rate 3D graphics and High Definition media, multiple large displays also with full USB peripheral connectivity.

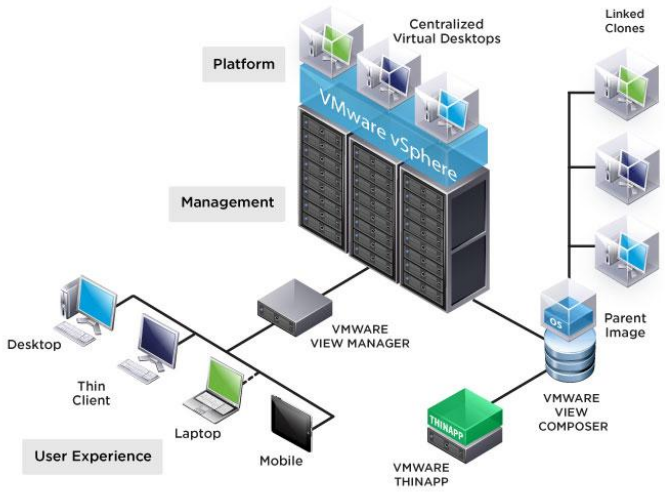
View Connection Server/ View Manager - Management of the VDI infrastructure is centralized here, provisioning and deployment of virtual desktops. It is also the broker for connections to the View virtual desktops.

View Composer - View composer technology enables the use of linked clones, creating gold master images that share a common virtual disk. Using linked clones, administrators can patch and update the master image without interrupting the service provided to the users, such as applications, data or settings.

View Desktop - Can be physical or virtual, a view agent is installed allowing communication with the View Manager and the Client.

ThinApp - Optional solution that encapsulates applications, decoupling from the operating system. Applications after configured can be deployed using the View Manager, without the need of installing they are packed on a single executable file.

Example of a traditional View Infrastructure:



4. INFRASTRUCTURE DESIGN

4.1 Overview

4.1.1 Summary

Logica is a business and technology service company, employing 41,000 people, providing business consulting, systems integration and outsourcing to clients around the world, including many of Europe's largest businesses. Logica creates value for clients by successfully integrating people, business and technology.

As part of a datacenter optimization project, IT was asked to test the new version of the VMware vSphere platform. The test is going to have place on the primary datacenter in Sacavém.

4.1.2 Design Overview

The architecture is independent of hardware specific details. Some specifications of physical design components that were chosen for the design are also provided.

This architecture design can be used to implement the solution using different hardware vendors, so long as the requirements do not change, hardware must be compatible with vSphere 5.

This design includes:

- One physical site (Sacavém)
- Clusters of hosts for load balancing through VMware High Availability/VMware Distributed Resource Scheduler (DRS) for host and guest operating system (virtual machine) failure.
- VMware vCenter Server integrated with Microsoft Active Directory. vCenter Server will leverage the extensive inventory of existing Active Directory users and groups to secure access to vSphere.
- Redundancy in network and storage infrastructure
- System component monitoring with email alerts
- VMware vCenter Update Manager for automating patching of all hosts and VMware Tools

4.2 Storage Design

4.2.1 Requirements

- EMC Clarion CX-4960 (active-active storage array)
- Storage solution must be flexible, highly available, secure, and maintain high performance.

4.2.2 Design Patterns

Storage Load Balancing	
Design Choice	Round-Robin
Justification	Round-Robin as the array supports asynchronous logical unit access (ALUA)

VMFS or RDM	
Design Choice	For most applications, VMware vStorage VMFS virtual disks will be used unless there is a specific need for raw device mapping (RDM). The most common use cases for RDM are, Microsoft clustering, NPIV, or running SAN management software in a virtual machine.
Justification	VMFS is a clustered file system specifically engineered for storing virtual machines. A datastore is like a storage appliance that serves up storage space for virtual disks in the virtual machines.
Impact	To ensure proper disk alignment, datastores were created using the VMware vSphere Client.

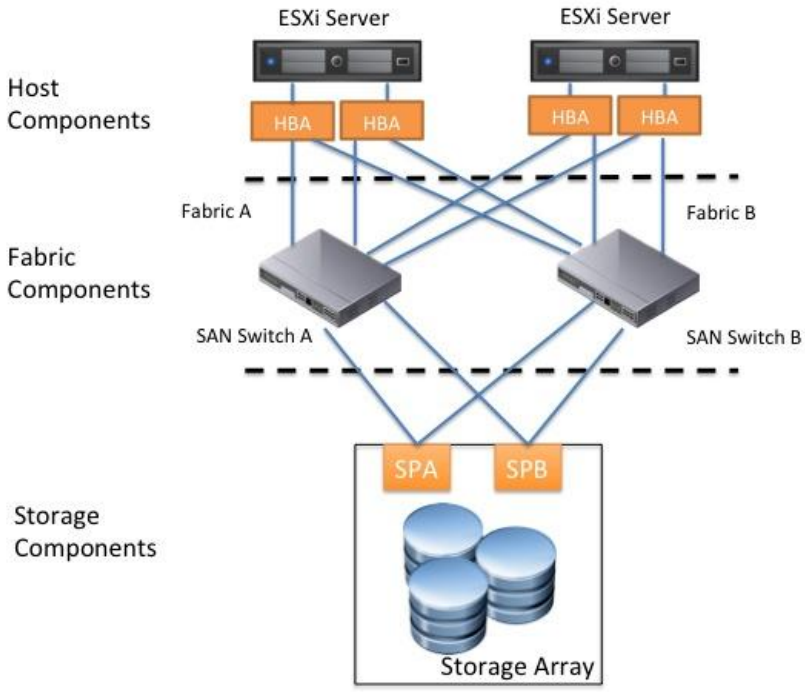
Host Zoning	
Design Choice	Single-initiator zoning will be used. Each host will have two paths to the storage ports across separate fabrics.
Justification	EMC best practices dictate single-initiator zoning, with multiple paths to storage targets across separate fabrics.

LUN Presentation	
Design Choice	LUNs will be masked consistently across all hosts in a cluster
Justification	Having consistent storage presentation ensures that virtual machines can be run on any host in a cluster. This optimizes high availability and DRS while reducing storage troubleshooting. It is important to minimize differences in LUNs visible across hosts within the same cluster or vMotion scope.
Impact	Requires close coordination with the storage team because LUN masking is performed at the array level.

Thin vs Thick Provisioning	
Design Choice	By default unless constrained by specific application or workload requirements, or special circumstances all volumes should be deployed as thick. In this Lab environment we will deploy thin disks except when required.
Justification	The rate of change for a system volume is low, while data volumes tend to have a variable rate of change. Thin provisioning increases time dispended in maintaining datastores.
Impact	Alarms must be configured to alert if approaching an "out of space" condition to provide sufficient time to source and provision additional disk.

4.2.3 Logical Design

Attribute	Specification
Storage type	Fibre Channel
Number of storage processors	multiple (redundant)
Number of FC switches	2(redundant)
Number of ports per host per switch	1
VMFS datastores per LUN	1



4.2.4 Physical Design

Attribute	Specification
Vendor and model	EMC Clarion CX-4960
Type	Active-active
ESXi host multipathing policy	Round-Robin

4.3 Network Design

4.3.1 Requirements

- LAB traffic should be isolated from Workstations traffic
- Virtual networking must be designed and configured for availability, security, and performance.

4.3.2 Design Patterns

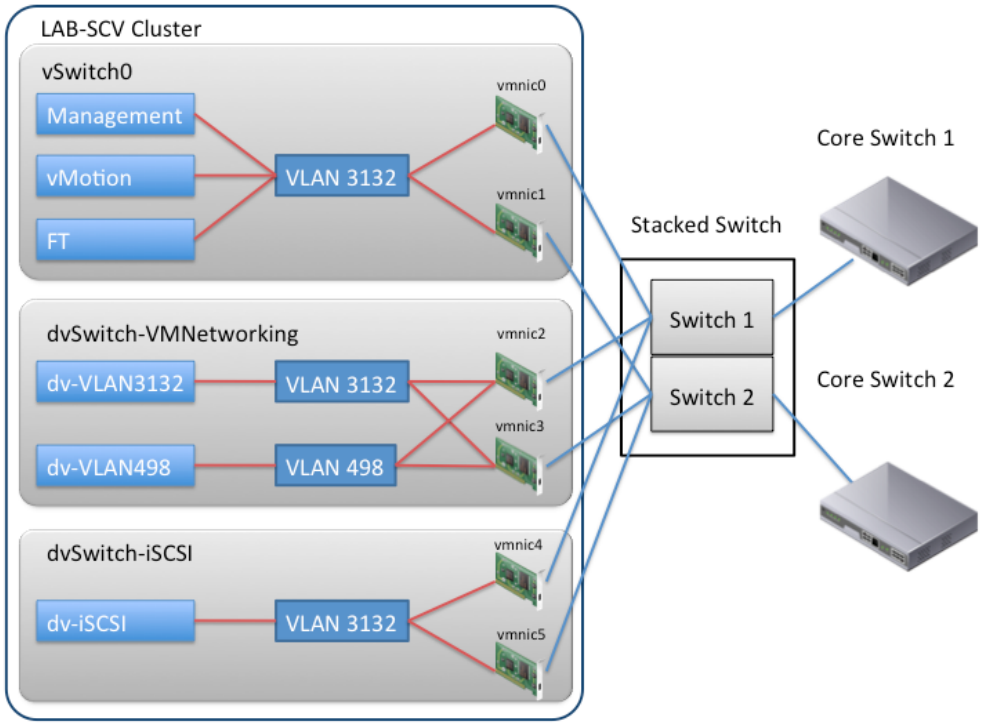
vNetwork Switch	
Design Choice	1 vStandard Switch 1 vDistributed Switch
Justification	Management traffic routed through vStandard Switch for maximum availability and Guests VLANs routed through vDistributed Switch
Impact	Impact Using vDistributed Switch as its configuration depends on the vCenter, if the vCenter becomes unavailable the management on the Switch also is unavailable.

vSwitch VLAN Configuration	
Design Choice	VLANs assigned to Mgmt Network, VM Network, VMotion, and Fault Tolerance.
Justification	Virtual LANs provide isolation and separation of traffic.
Impact	All ESX host facing ports must be configured as trunk ports.

vSwitch Load-Balancing Configuration	
Design Choice	Route based on IP hash
Justification	This method chooses an uplink based on a hash of the source and destination IP address of each packet.

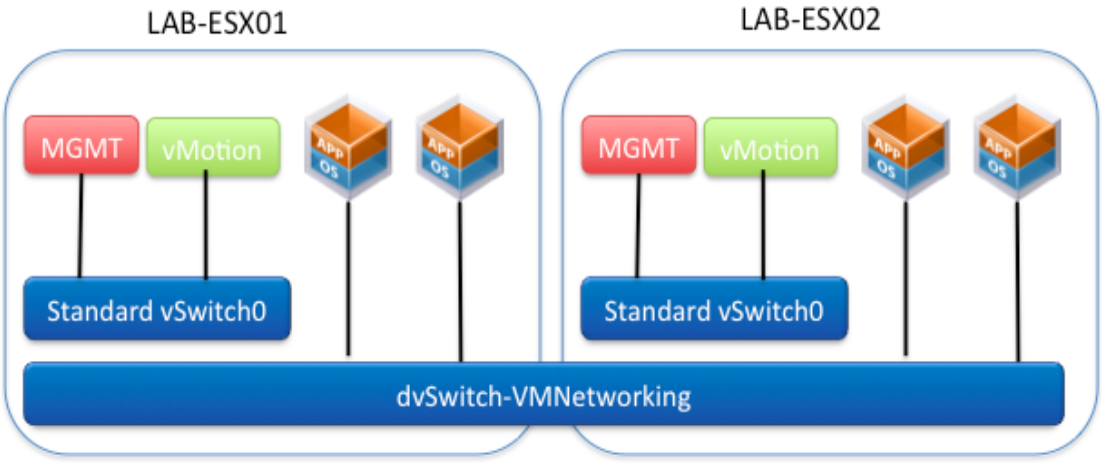
vSwitch Security Settings	
Design Choice	vSwitch default security settings: Forged Transmits: Reject, MAC address changes: Reject, Promiscuous Mode: Reject
Justification	There are no requirements that necessitate the use of any of the vSwitch security settings.
Impact	Setting all options to Reject provides optimal vSwitch security by preventing potentially risky network behavior.

4.3.3 Logical Design

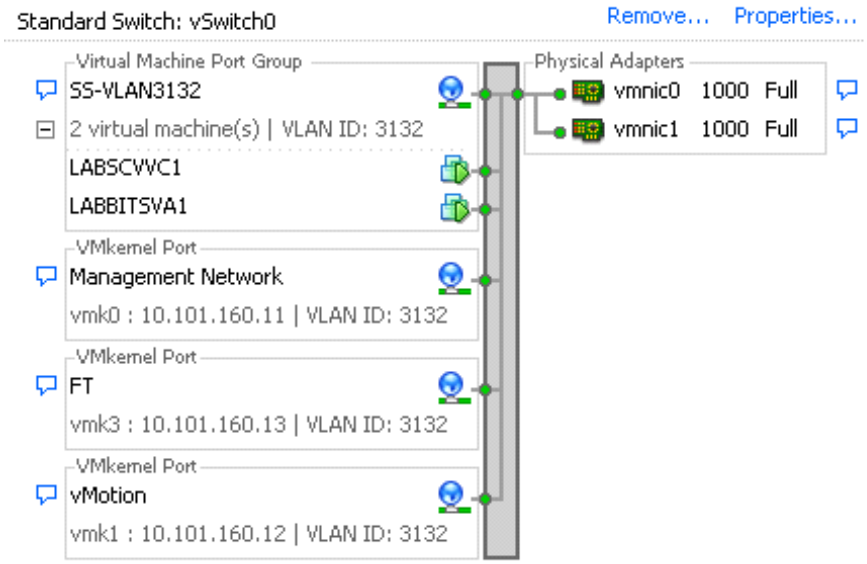


4.3.4 Physical Design

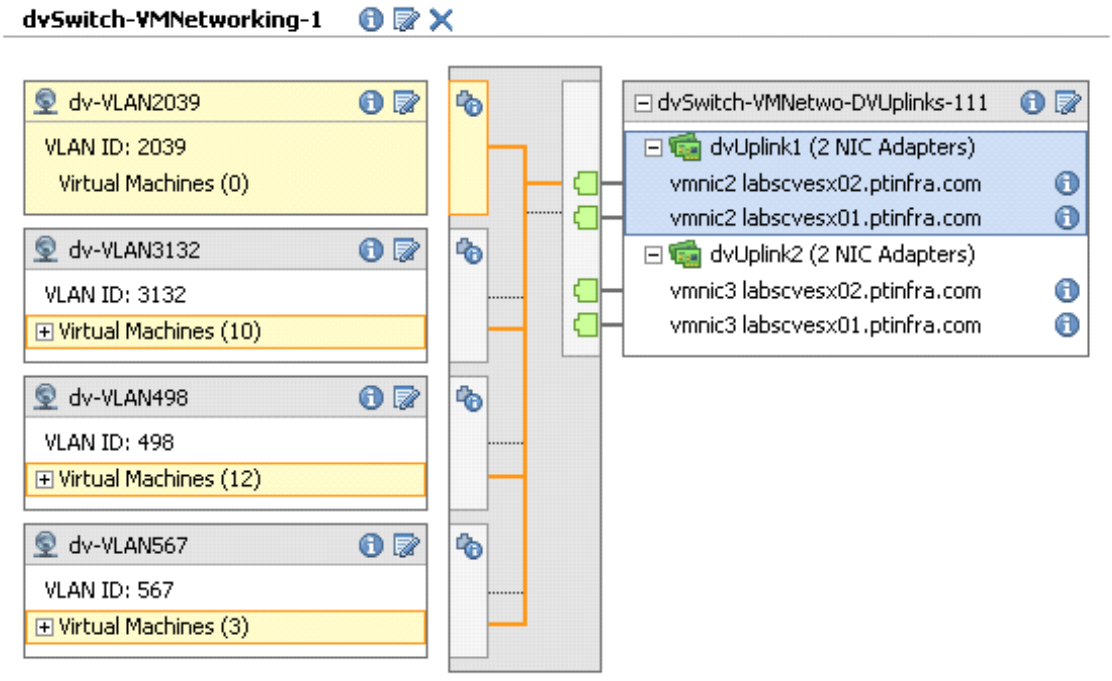
4.3.4.1 Infrastructure overview



4.3.4.2 Standard Virtual Switch - vSwich0



4.3.4.3 Distributed Virtual Switch - dvSwitch-VMNetworking-1



4.4 Host

4.4.1 Design Patterns

Blade or Rack Servers	
Design Choice	Blade servers will be used.
Justification	Blade solution is modular and offers increased processing power in less space.
Impact	Power and cooling requirements for blade chassis must be considered.

4.4.2 Logical Design

Attribute	Specification
Host type and version	ESXi 5.0
Storage	Local for ESX binaries SAN LUN for virtual machines
Number of CPU sockets Number of cores per CPU Total number of cores Processor speed	2 4 8 2.66GHz
Memory	32GB
Number of NIC ports Number of HBA ports	6 4

4.4.3 Physical Design

Attribute	Specification
Vendor and model	HP
Processor type Total CPU sockets Cores per CPU Total number of cores Processor speed	Intel® Xeon® CPU X5355 2 4 8 2.66GHz
Memory	32GB
Onboard NIC vendor and model Onboard NIC ports x speed Number of attached NICs NIC vendor and model Number of ports/NIC x speed Total number of NIC ports	Broadcom Corporation 2 Broadcom Corporation 2 6
Storage HBA vendor and model Storage HBA type Number of HBAs Number of HBA ports Total number of HBA ports	QLogic QMH2462 4Gb FC HBA for HP c-Class BladeSystem FC 2 2 4
Number and type of local drives RAID level Total storage	2 0+1 120GB
System monitoring	HP SIM

4.5 Virtual Machine

4.5.1 Design Patterns

Swap and Operating System Paging File Location	
Design Choice	Virtual machine swap files are placed in the same location as the other virtual machine files (default behavior).
Justification	Keeping files on default datastore is easier to manage. Moving the vmswap files to a different location for performance or replication bandwidth issues requires additional configuration and management processes.
Impact	If future requirements mandate that virtual machine swap files be moved to a separate location, all relevant virtual machines will need to be reconfigured.

4.6. Virtual Datacenter

4.6.1 Requirements

Availability

- Design for maximum availability

Management:

- All components must use corporate authentication (Active Directory)
- Some Systems Administrators are running Mac OS and Ubuntu

Compute:

- All Virtual Machines may reside on the same cluster;
- Verify resource pools usefulness

4.6.2 Design Patterns

vCenter Server Physical or Virtual (VM or Virtual Appliance)	
Design Choice	vCenter Server will be provisioned as a virtual machine.
Justification	The vCenter Server system will be set up as a virtual system on a separate ESX cluster (Management cluster) due to cost and management considerations. This allows ACME Energy to leverage the benefits of VMware infrastructure like vMotion, DRS, and VMware HA. The Virtual Appliance version will not be used, as some of the features (SQL database, vCenter Update Manager, vCenter Linked Mode and vCenter Heartbeat) are not available.
Impact	To improve manageability, the location of the vCenter Server virtual machine should be static. This can be handled by pinning the vCenter Server virtual machine to a specific ESX host or by setting up a separate management cluster.

vCenter Server Database Shared or Dedicated	
Design Choice	Separate instance.
Justification	The SQL server will be used for many products.
Impact	Database management is offloaded to a separate database team.

vCenter Update Manager Location	
Design Choice	VMware Update Manager will be located on the vCenter Server system and requires a separate database instance on an external database system.
Justification	The vCenter System server will be sized appropriately to accommodate only the Update Manager. Only VMware components will be installed on the vCenter System server, to allow for better performance and scalability. The size of the environment required a separate database instance but not a dedicated server VM.
Impact	Co-located with vCenter Server will required to allocate more resource to the vCenter VM but will decrease the management cost as no more management VM is required.

vSphere License Edition	
Design Choice	vSphere Enterprise Plus Edition
Justification	vNetwork distributed switch functionality is required to meet the requirements of the solution. vSphere Enterprise Plus Edition enables features like Host Profiles, vNetwork distributed switch, and third-party multipathing.
Impact	vSphere Enterprise Plus is the most expensive edition. In this environment Licenses were activated from VMware Partner Portal.

4.6.3 Logical Design

Attribute	Specification
vCente Server Version	5.0.1
Physical or virtual system	Virtual
Number of CPUs	4

Processor type	vCPU
Processor speed	2.66GHz
Memory	4GB
Number of NIC and ports	1NIC
Number of disks and disk size(s)	40GB + 10GB
Operating System	Windows Server 2008 SP2 STD

4.6.4 Phyical Design

Attribute	Specification
Vendor and model	VMware virtual hardware 8
Processor type	VMware vCPU
NIC vendor and model Number of ports Network	Vmxnet3 1x GbE LABVLAN
Local disk	N/A

4.7. Management and Monitoring

4.7.1 Design Patterns

Server, Network, SAN Infrastructure Monitoring	
Design Choice	All of the physical systems, including the network and SAN, will continue to be monitored directly by the enterprise monitoring system, which will be configured to incorporate any additional infrastructure required to support this vSphere LAB.
Justification	Leverages existing enterprise monitoring system. Allows for exploration of virtualization-specific offerings in the future.

Impact	Requires integration of vCenter Server and ESX with existing monitoring systems.

vSphere Management	
Design Choice	The vSphere infrastructure will be managed through vMA and VMware vSphere PowerCLI.
Justification	vMA5 is a virtual appliance that is preloaded with a 64-bit Enterprise Linux operating system, VMware Tools, vSphere SDK for Perl, and vSphere CLI.
Impact	Requires compute resources for the vMA. In a production environment vMA should be placed in the management cluster.

Cluster Attribute	Specification
Number of ESXi Hosts	2-3
VMware DRS Configuration	Fully automated
VMware DRS Migration Threshold	3 stars
VMware HA Enable Monitoring	Yes
VMware HA Percentage	25%
VMware HA Admission Control Response	Prevent VMs from being powered on if they violate availability constraints
VMware HA Default VM Restart Priority	N/A
VMware HA Host Isolation Response	Leave VM Powered ON
VMware HA Enable VM Monitoring Sensitivity	Medium

5. REMOTE ACCESS SOFTWARE

There are many types of connecting to servers, in this project i will test some of them. By default there are 2 types, in windows machines we have the Remote Desktop Services proprietary of Microsoft, and for Unix machines we have ssh providing command line access.

Using vSphere it is already available a client, Virtual Machine remote Console (VMRC) that provides direct access to the servers console independently of the operating system. Although this connection seems easier, remote console sessions consume CPU resources in the service console of the ESX Hosts. The VMRC is not optimized and is not designed to be used as a standard technology for remote access. This type of action should only be used for administrative actions where there is no access through the network.

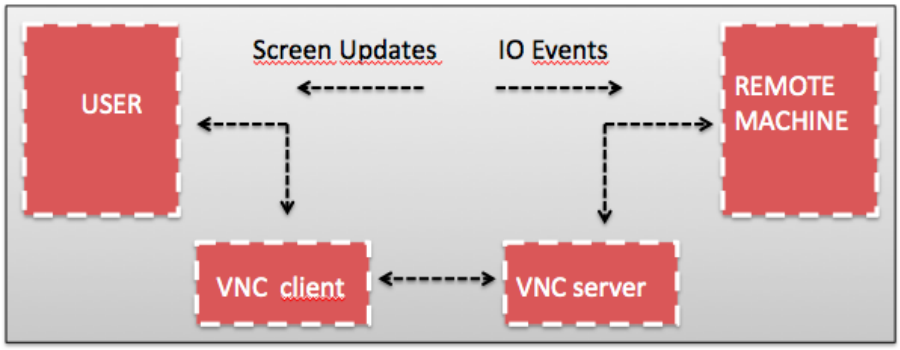
To experiment other types of connections it was chosen open source RDP Clients and one that was cross platform non specific to any operating system, the Virtual Network Computing (VNC), wich is a graphical desktop sharing system that uses the RFB protocol to remotely control another computer. Mouse and keyboard events are transmitted from one computer to another over a network, relaying the graphical screen updates back in the other direction.

RFB ("remote framebuffer") is a simple protocol for remote access to graphical user interfaces. Because it works at the framebuffer level it is applicable to all windowing systems and applications, including X11, Windows and Macintosh.

RFB Client or viewer is the remote endpoint where the user sits (i.e. the display plus keyboard and/or pointer).

RFB Server is the endpoint where changes to the framebuffer originate (i.e. the windowing system and applications.

VNC functions with the simple server-client architecture. VNC server has to run in the remote machine, VNC viewer is launched from where you're going to access it.



Screen updates are captured from video frame buffer by the VNC server and sent to the VNC viewer. Which responds to the server, transmitting the keyboard and mouse events getting back its screen updates.

VNC server:

VNC server waits for the clients connection, authenticates them, do the protocol negotiations and send the frame buffer updates to the clients.

VNC client:

VNC client is the program, which connects to the VNC server, send password for authentication, do protocol negotiations with server, receive the frame buffer updates from server and display it to the user.

RFB Protocol:

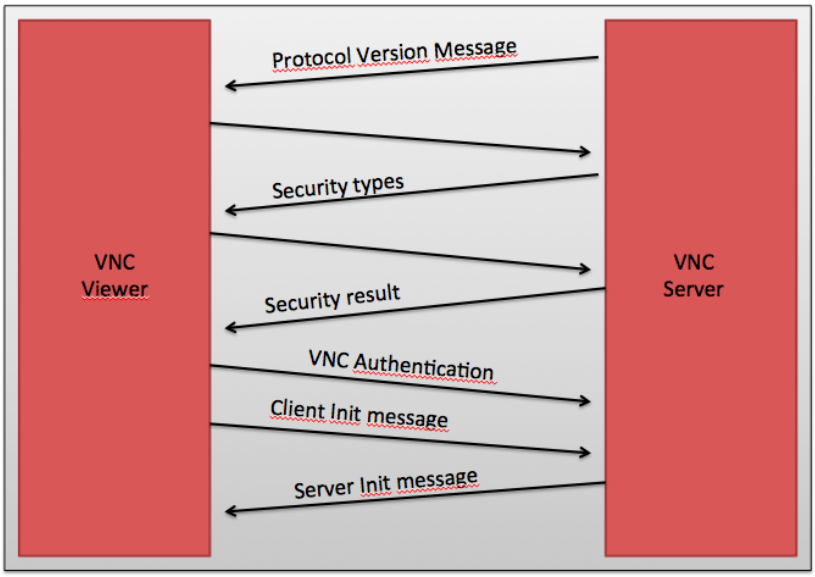
- RFB - Remote Frame Buffer.
- Simple protocol for remote access to graphical user interface.
- Functions at the frame buffer level, working with any windowing system.

How it works:

There are 2 types in protocol messages based on its purposes:

- Display
- Input

Negotiation diagram:



There are many vnc servers, in this project it was tested TigerVNC, although there was a lack of documentation the implementation was simpler and its functionality corresponded to the expectations.

To test remote desktop features, we experimented rdesktop as a client and xrdp as a rdp server, both were executed without problems and the installation was simple.

As an alternative method the ESXi hosts have already by default a VNC Server, to function it needs to configure the firewall of the host and the guest vm configuration file must be edited to allow vnc connections, and its independent of guest os installed in the virtual machine.

From the tests made we obtained the following table:

Software	Server Windows	Client Windows	Server MacOSX	Client MacOSX	Server Linux	Client Linux
MS Remote Desktop	Yes	Yes	No	Yes	No	Yes
xrdp	-	Yes	-	Yes	Yes	Yes
TigerVNC	Yes	Yes	-	Yes	Yes	Yes
rdesktop	Yes	Yes	-	Yes	Yes	Yes
ESXi VNC	Yes	-	Yes	-	Yes	-

6. SETTING THE INFRASTRUCTURE

Installing VMware ESXi 5.0

1. Load ESXi 5 ISO

2. Boot Menu > ESXi 5 - Standard Installer

3. Welcome Screen > Press ENTER

4. End User License Agreement (EULA) > Accept F11

5. Select a Disk > ENTER

6. keyboard layout > Portuguese

10. Configure root password

11. Ignore warning

12. Confirm Install > F11

13. After succefull installation > ENTER to reboot

Configuring ESXi after installation

ESXi 5.0 screen > F2, enter root password

Troubleshooting Options > Enable ESXi Shell and Enable SSH

Restart Management Services

Configure Management Network

Leave VLAN Blank

Set IP Configuration

Set DNS Configuration

Custom DNS Suffixes > Add domain.com

Restart Management Network

Test Network -> Success

If there is no connectivity, configure vSwitch0 NIC teaming with Route based on IP hash because of the configuration in the physical switchs. Run the command:

esxcli network vswitch standard policy failover set -l iphash -v vSwitch0

Install vSphere Client - vi-client

Open url on browser https://<esx-host-ip>

Download vSphere Client

Install

Open vSphere Client

User:root Password:Registered during installation

Configure Networking

Configuration -> Networking

vSwitch0 -> Properties -> Ports

Edit vSwitch

Load Balacing: Route based on IP hash

Network Failover Detection: Link status only

Rest options leave default

Remove VM Network, it is created by default

Ports > Edit Management Network

Insert VLAN ID

Leave only selected Management Traffic

vSwitch0 -> Properties -> Network Adapters

Edit each vmnic

Configured Speed Duplex: Auto negotiate

Add vMotion Network

vSwitch0 -> Properties -> Add

Connection Type - VMKernel

Network Label: vMotion

VLAN ID: Insert VLAN ID

Select: Use this port group for vMotion

Insert IP Configuration

Connect to ESX > ssh root@<ip||hostname>

Run

esxcli network nic list

This command will list the Physical NICs currently installed and loaded on the system and their status.

Enable ports on physical switch each at a time, with the objective of verifying the aggregates on the physical switch.

Add VLAN for VMNetworking

vSwitch0 -> Properties -> Add

Connection Type - VMNetwork

Network Label: SS-VLAN<ID>

VLAN ID: Insert VLAN ID

Select:

vCenter Configuration

Setting VM to host the vCenter Server

Log into ESXi Host with VMware vSphere Client

Right click into the Host > New Virtual Machine > Custom

Name: LABSCVVC1

Storage - Created on the local datastore and afterwards migrated to a standard LUN

Virtual Machine Version: 8

Guest OS: Windows 2008 R2

vCpu: 2 - Mem: 4

Network: 1 VMXNET3 - SS-VLAN<id>

SCISI Controller: LSI Logic SAS; Disk Size: 40GB Thin-Provision

Leave node on (0:0)

Installing Microsoft Windows Server 2008 R2 OS

Load ISO

Options:

Language: English

Time: Europe\Lisbon

Keyboard: Portuguese

Windows Server 2008 R2 Standard (Full Installation)

Accept license agreement

Custom > Disk > Drive Options

New > Apply > Format

Set Administrator password

Login

Guest > Install/Upgrade VMware Tools

Control Panel > Network Connections

Change name of Adapter

Right click > Properties

Uncheck IPv6

Link-Layer *

IPv4 > Properties

Set IP address; subnet; gateway; DNS servers

Run > cmd

Ping gateway to verify network connection

Ping domain

netsh interface tcp set global autotuning=disable

netsh interface tcp set global rss=disable

netsh firewall set opmode disable

Computer > Properties > Change settings

Computer Name > Change

Domain > Enter domain ex: domain.com | Restart Later

Advanced > Performance Settings > Adjust for best performance

Remote > Allow connections from computers running any version of Remote Desktop

Reboot

VMware vCenter Installation

Log into the vCenter with administrator credentials

Load ISO

Autorun Media

Wizard > Install VMware vSphere 5

Select English language > Agree license agreement

Enter user information > Enter license key

Select SQL instance

Select the system account for the vCenter Server service account

Keep default directory

Select Create standalone VMware vCenter Server instance

Keep default ports

Select 1024 MB for JVM memory

Install > After installation is complete restart server

Log into the vCenter with administrator account in vSphere Client

Right-Click on the root of vCenter > New Datacenter > Name: LAB

Right Click on Datacenter (LAB) > New Cluster > Name: LAB-Cluster-1

Configure Cluster with options referred on Design Section

Right-Click Cluster Add Hosts > Allocate all resources

Configuration of the CentOS VM

Why CentOS? CentOS is an Enterprise-class Linux Distribution derived from sources freely provided to the public.

Operating System was installed with default configurations

VMware Tools Installation

On the vSphere Client

Select VM:
Guest -> Install/Upgrade VMware Tools

Create a mount point:

```
mkdir /mnt/cdrom
```

Mount the CDROM:

```
mount /dev/cdrom /mnt/cdrom
```

Copy the Compiler gzip tar file to a temporary local directory:

```
cp /mnt/cdrom/VMwareTools-...tar.gz /tmp/
```

Change to the tmp directory and extract the contents of the tar file into a new directory called vmware-tools-distrib:

```
cd /tmp
tar -zxvf VMwareTools-....tar.gz
```

Change directory to vmware-tools-distrib and run the vmware-install.pl PERL script to install VMware Tools:

```
cd vmware-tools-distrib
./vmware-install.pl
```

Remove VMware Tools installation packages:

```
cd
rm /tmp/VMwareTools-...tar.gz
rm -rf /tmp/vmware-tools-distrib
```

(/usr/bin/vmware-config-tools.pl)

VM->Edit Settings -> CD/DVD drive 1

Remove marks on Device Status

Network Configuration

```
vi /etc/sysconfig/network-scripts/ifcfg-eth0
system-config-network
vi /etc/hosts
```

SSH

```
/sbin/chkconfig --list | grep sshd
sshd              0:off 1:off 2:off 3:off 4:off 5:off 6:off
chkconfig sshd on
/sbin/chkconfig --list | grep sshd
sshd              0:off 1:off 2:on  3:on  4:on  5:on  6:off
```

Proxy

```
vi /etc/profile.d/proxy.sh
export http_proxy=http://proxy:port
export https_proxy=http://proxy:port
export ftp_proxy=http://proxy:port
:wq!
```

Update OS

```
yum clean all
yum update
```

TigerVNC Server - Installation and Configuration

Users:

User	Password	VNC Password
root	centos	
user1	user1	user1vnc
user2	user2	user2vnc

Install TIGERVNC-server

```
yum install tigervnc-server
```

Edit the server configuration

```
vi /etc/sysconfig/vncservers
VNCSERVERS="1:user1 2:user2"
VNCSERVERARGS[1]="-geometry 1024x768"
VNCSERVERARGS[2]="-geometry 640x480"
/sbin/service vncserver restart
```

Starting vncserver at boot

```
chkconfig --list | grep vnc
vncserver         0:off 1:off 2:off 3:off 4:off 5:off 6:off
chkconfig vncserver on
chkconfig --list | grep vnc
vncserver         0:off 1:off 2:on  3:on  4:on  5:on  6:off
```

Set users VNC passwords

login user1

```
su - user1
vncpasswd
```

login user2

```
su - user2
vncpasswd
```

Testing with a vnc client

The default port number is 5900+1 for each user
Example for the second the port will be 5902

```
<ip>:<arg>
```

rdesktop

rdesktop is an open source client for Windows Remote Desktop Services, capable of natively speaking Remote Desktop Protocol (RDP). Currently runs on most UNIX based platforms with the X Window System and is released under the GNU Public Licence (GPL), version 3.

Requirements

```
kernel verison of 2.X or better
XFree86
make
gcc
OpenSSL
X Window System
```

Install requirements

```
yum install make gcc libX11-devel openssl-devel
```

Installation

```
cd /tmp/;
tar -xzvf rdesktop-1.1.0.tar.gz
cd /rdesktop-1.7.1
./configure
make
make install
```

Test RDP from Windows to linux

Applications > System Tools > Terminal

```
rdesktop <server_ip>
```

xrdp

Requirements

```
gcc
make
pam-devel
openssl-devel
vnc-server
```

Install requirements

```
yum install pam-devel
yum install autoconf automake libtool libX11-devel libXfixes-devel
```

Install xrdp

```
tar -zxf xrdp-v0.6.6.tar.gz
mv xrdp-v0.6.6/ /usr/lib64/xrdp-v0.6.6/
cd /usr/lib64/xrdp-v0.6.6/
./bootstrap
./configure
make
make install
```

Run rdp server

```
/etc/xrdp/xrdp.sh start
```

VMware ESXi 5 VNC Server

Connect to virtual machines without installing in each Vitual Machine a vnc server

Configure ESXi Firewall

Create rule on services.xml for tcp ports 5950-5960 inbound and outbound

```
<!-- VNC Firewall Rules—>
 <service id="0033">
   <id>VNC</id>
   <rule id='0000'>
      <direction>outbound</direction>
      <protocol>tcp</protocol>
      <porttype>dst</porttype>
      <port>
        <begin>5950</begin>
        <end>5960</end>
      </port>
    </rule>
    <rule id='0001'>
      <direction>inbound</direction>
      <protocol>tcp</protocol>
      <porttype>dst</porttype>
      <port>
        <begin>5950</begin>
        <end>5960</end>
      </port>
    </rule>
    <enabled>true</enabled>
    <required>false</required>
 </service>
```

2. Set permissions temporarily:

```
chmod 7777 /etc/vmware/firewall/services.xml
```

3. Edit and insert the code above:

```
vi /etc/vmware/firewall/services.xml
```

4. Refresh the ESX firewall:

```
esxcli network firewall refresh
```

```
esxcli network firewall ruleset list ( | grep VNC)
```

Edit VM Settings

VM must be Powered Off

```
vi /vmfs/volumes/<datastore>/<VM>/<VM>.vmx
```

.vmx configurations:

- RemoteDisplay.vnc.enabled = [true|false]
- RemoteDisplay.vnc.port = [port #]
- RemoteDisplay.vnc.password = [optional]

Insert following lines:

```
RemoteDisplay.vnc.enabled = true
RemoteDisplay.vnc.port = 5951
```

Search and identify virtual machines with VNC option configured:

```
cd /vmfs/volumes
grep -rl "RemoteDisplay.vnc.enabled" */*/*vmx
```

7. CONCLUSION AND FUTURE WORK

This project is a result of study work about virtualization based on the vSphere platform, its principal characteristics and utilization.

Virtualization brings many benefits, enabling multiple operating systems to run on the same platform, detaching workloads and data from the physical infrastructure accelerates services delivery, high availability and migrations without interrupting any service.

Independently of the platform of virtualization, costs over management and service delivery are greatly reduced, with server consolidation and ease access to data, as the hosts and the guests can be centrally managed,

While there are many competitors, we can enumerate the main platforms such as Hyper-V and XenServer, but even though they are advancing in virtualization, VMware still has a big advantage over them, specially regarding management and high availability, such as vMotion, Storage vMotion, DRS, HA and hardware Hot Add, which in this case don't need to be provided with the use of third-party applications or with specific configurations from hardware vendors. Many comparisons have been made between virtualization platforms, but this isn't part of this study.

Regarding the QoS of the environment, as the virtual machines run in an isolated mode, each VM will not affect the others although shares can be assigned individually enabling some guests to have more priority than others. This option should not be enabled individually, over the time managing it becomes time consuming and if the underlying infrastructure is well configured there is only the necessity to create limits on the clusters and enabling storage and networking i/o monitorization. The performance of the virtual machine usually degrades with the lack of supervision, an example is when after deploying a service during its life there is a lack of supervision of its resources usage. With this observation its is proposed that after a certain period of time, the system administrators teams involved with the service should analyse if there is an over-commitment or a lack of resources, this could be automatically provided with the use of an automated solution, our investigation resulted in two main products such as vKernel vOPS and VMware vCenter Operation Managent Suite.

Resource scheduling proved to be highly efficient, DRS auto balances virtual machine workloads across the hosts in a cluster, recommending and performing VM migrations. Power management in a cluster is valuable but we consider that its usage should be retained to non productive clusters, because in the event of a ESXi host crash, depending on the number of paths because of the storage infrastructure, the host

availability time could be slower deriving from the paths discovery process during the boot, consequently causing the virtual machines recovery to take even more time but it also depends on the resource usage of the hosts within the cluster.

Desktop management has become more complex to manage and to respond to user requests, end-users want freedom and they want to be flexible in how they access their data and applications.

Desktop virtualization enables administrators to control, manage and maintain compliance. There are many customization methods for the virtual desktop pools, there are three options, terminal services, manual and an automated pool, the last we consider the most important, the usage of View Composer is one of the main features, it uses the linked clone technology, the clones are linked to a full clone of the golden image, referred as a replica allowing for multiple virtual desktops to share the same virtual disks decreasing the storage usage.

If a end-user requires different applications from those within the base image, applications can be virtualized using thin app, which encapsulates registry and application files into a single package, that can be deployed, managed and updated independently from the OS.

Only XenDesktop was investigated as another solution to virtualize desktops, from our investigation we consider that the setup of this solution is more complex than View, but it should be done a more in depth analysis regarding its performance as there are some studies with different use cases where XenDesktop has a better performance.

During the implementation of the View solution, one of the main problems we found was the lack of documentation regarding firewall rules, only third party documents from blogs had most of them, we had to analyze the firewalls to verify what was missing.

As a solution to provide infrastructure as a service, vCloud Director was tested. It enables the pooling of resources and provisioning them as a virtual center, supporting multi-tenant environment. We consider multi-tenancy a delicate subject, depending on the cloud model multitenancy should be analyzed regarding security and flexibility. Considering as a use case a private cloud, tenants could have dedicated resource models for the underlying infrastructure. Though this decreases management flexibility it gives more security to the environment. More investigation should be made regarding automatic methods and billing process for security solutions in the cloud, vCloud Director uses vShield but its firewalls configuration could be complemented with tird-party solutions.

These facts resulted in many hours of exploiting the virtual environment and its features, understanding this made us realize that this is a vast area, and its benefits are indeed undeniable.

Regarding remote desktop software, proprietary software like Windows remote desktop protocol and Apple remote desktop are integrated in their operating systems, comparing to VNC, which is a cross platform software. With VNC a Linux Server can control a Windows Server and vice-versa. Although VNC can be used with almost all operating systems, there is a lack of security in many of its variants, which could cause the data that is transferred to be sniffed, unlike other Remote Desktop software which are already secure. A VNC connection could be protected with the usage of a VPN or a SSH tunnel, further investigation should be made regarding the security of VNC.

Selecting the remote desktop software, depends on the client operating system, we consider that VNC is the most appropriate option when connecting to different operating systems.

8. BIBLIOGRAPHY

VMware Inc. vSphere Installation and Setup- vSphere 5.0 Update 1 URL http://pubs.vmware.com/vsphere-50/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-501-installation-setup-guide.pdf. Retrieved March, 2012.

VMware Inc. vSphere 5 Online Documentation URL http://pubs.vmware.com/vsphere-50/index.jsp. Retrieved March, 2012.

VMware Inc. What's New in vSphere 5.0 URL http://www.vmware.com/support/vsphere5/doc/vsphere-esx-vcenter-server-50-new-features.html. Retrieved March, 2012.

VMware Inc. VMware vSphere Design Workshop, Student Manual, ESXi 5.0 and vCenter 5.0, VMware Education Services 2012.

VMware Inc. VMware vSphere: Install, Configure, Manage, Student Manual - Volume 1, ESXi 5.0 and vCenter 5.0, VMware Education Services 2012.

VMware Inc. VMware vSphere: Install, Configure, Manage, Student Manual - Volume 2, ESXi 5.0 and vCenter 5.0, VMware Education Services 2012.

CentOS 6.2. URL https://www.centos.org/. Retrieved June 2012

TigerVNC. URL http://sourceforge.net/apps/mediawiki/tigervnc/index.php. Retrieved June 2012.

xrdp. URL http://www.xrdp.org/ . Retrieved June 2012.

rdesktop. URL http://www.rdesktop.org/. Retrieved June 2012.

RealVNC. The RFB Protocol URL http://www.realvnc.com/docs/rfbproto.pdf. Retrieved June 2012.

TigerVNC. The RFB Protocol URL http://www.tigervnc.org/cgi-bin/rfbproto. Retrieved June 2012.

Wikipedia. RFB Protocol URL http://en.wikipedia.org/wiki/RFB_protocol. Retrieved June 2012.

Wikipedia. TigerVNC URL http://en.wikipedia.org/wiki/TigerVNC. Retrieved June 2012.

VMWare Inc. Using VNC to connect to VMs URL
http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1246

Virtualization Technology in Green IT with CloudComputing Infrastructure, JOURNAL OF COMPUTING, VOLUME 3, ISSUE 11, NOVEMBER 2011, ISSN 2151-9617

Virtualization Platforms Comparison Matrix. URL
http://www.virtualizationmatrix.com/matrix.php

Virtualization Platforms Comparison . URL
http://blog.danbrinkmann.com/2012/06/12/hyper-v-xenserver-vsphere/

Connections & Ports in ESX & ESXi. URL
http://www.vreference.com/public/ConnectionsPorts-v10Q3.pdf