

Cap. 2

Introdução à Virtualização

TECNOLOGIAS DE VIRTUALIZAÇÃO
ENGENHARIA INFORMÁTICA
WWW.IPLEIRIA.PT

Cap. 2 - Introdução à Virtualização

- Pré-requisitos e Conceito de Virtualização
- Hypervisor
- Cloud

Pré-requisitos

- Conceitos de hardware
 - Processador
 - Memória
 - Disco
- Conceitos de Redes
- Licenças de Software
- Instalação de servidores

Definição de Virtual

- “Algo que é tão próximo da verdade que, para a maior parte dos propósitos, sua existência pode ser considerada” (Wikipedia)
- “Do latim *virtus* (“força” ou “virtude”), faz referência àquilo que tem a virtude de produzir um efeito apesar de não o produzir verdadeiramente” (Site conceito.de)

Virtualização

- Definição de Virtual
 - Oposto de físico
 - Aquilo que existe apenas na memória de um computador
- O que não é uma máquina virtual é uma máquina física.
- Uma máquina virtual não existe fisicamente, não tem componentes ou hardware que possamos tocar, apenas existe na memória do computador

Analogia

- Jogo de corridas de carros
 - Não existe um carro físico
 - Existe apenas uma simulação por computador de um motor, transmissão, travões, pneus (carro virtual)
- Servidor Virtual
 - Não existem componentes de computador físicos
 - Existe apenas uma simulação por computador de um processador, memória, disco e rede
 - Cumpre os mesmos objetivos tal como um servidor físico



Cap. 2 - Introdução à Virtualização

- Pré-requisitos e Conceito de Virtualização
- **Hypervisor**
- Cloud

Hypervisor

- Hypervisor
 - Uma parte de software, firmware ou hardware que cria e corre máquinas virtuais
- Host
 - Servidor físico que corre o software de hypervisor
 - Um Host pode alojar vários guests
- Guest
 - Máquina virtual alojada pelo hypervisor
 - Não existe fisicamente – apenas existe na memória do hypervisor

Sistemas Operativos

- Host operating system
 - SO do computador físico.
 - Para cada Hypervisor, consultar lista “Supported host OSs”
- Guest operating system
 - SO que corre dentro da VM.
 - Para cada Hypervisor, consultar lista “Supported guest OSs”
 - Embora os Hypervisores suportem outros SOs, selecionam um conjunto de SOs para os quais fazem um conjunto de otimizações, de modo a aproximar-se do desempenho nativo.

Hypervisor

- Tipo 1 – Hypervisor Nativo ou Bare metal ou Embedded.
 - Corre diretamente no hardware do host, funcionando como SO
 - Não há um SO separado do hypervisor
- Tipo 2 – Hosted hypervisor
 - Precisam de um SO separado. Primeiro instala-se um SO e depois instala-se o hypervisor
 - Hypervisor corre como uma aplicação ou um serviço nesse SO.

Hypervisor

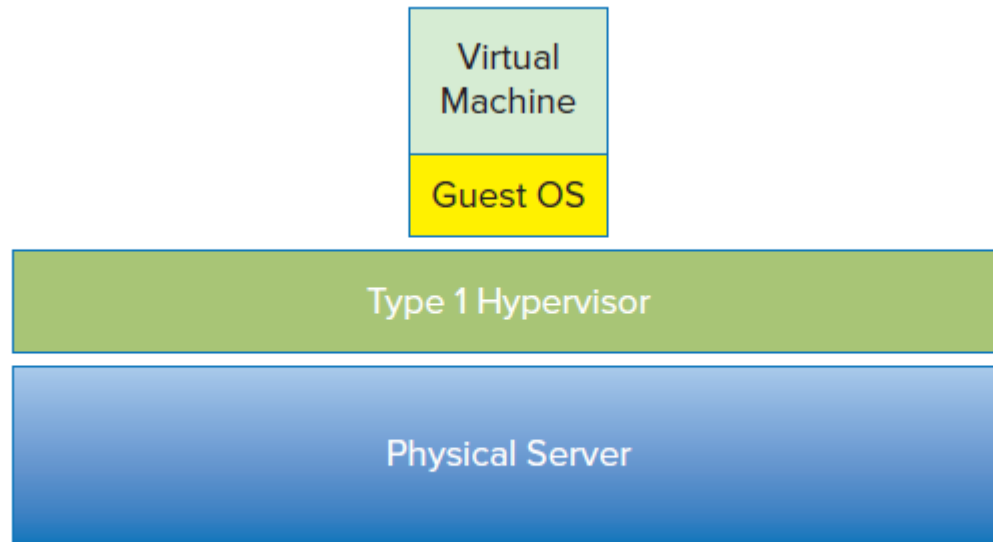


FIGURE 2.3 A Type 1 hypervisor

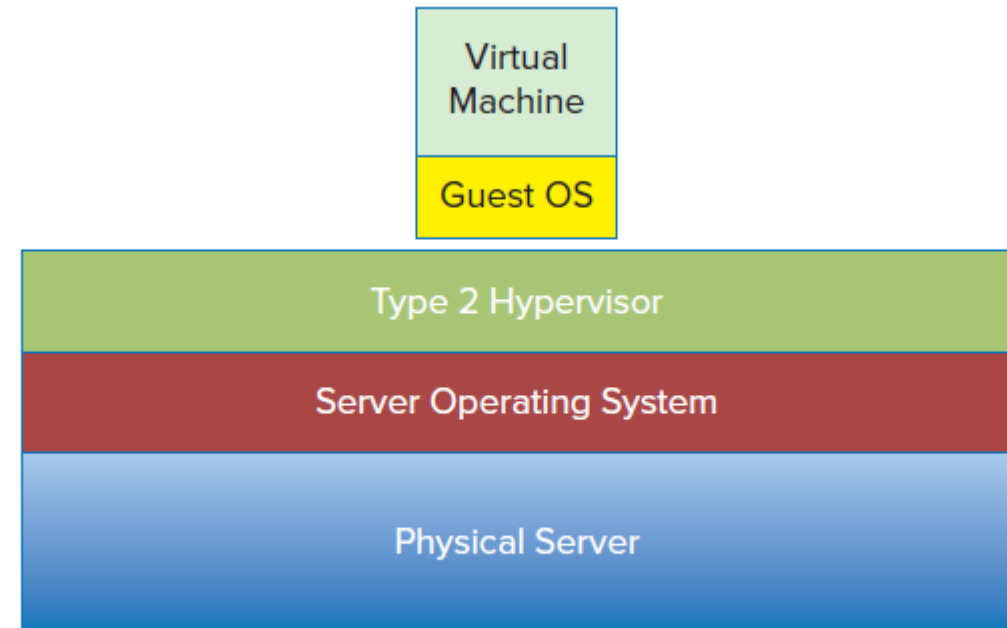


FIGURE 2.5 A Type 2 hypervisor

Cap. 2 - Introdução à Virtualização

- Pré-requisitos e Conceito de Virtualização
- Hypervisor
- **Cloud**

A nuvem - Cloud

- Diferentes fornecedores: diferentes definições
- Em geral:
 - Os fornecedores de Cloud correm software de hypervisor no seu hardware
 - Fornecedores alugam acesso ao hypervisor
 - Cliente pode correr as suas máquinas virtuais ou
 - Cliente pode utilizar máquinas virtuais pré-preparadas

A nuvem - Cloud

- O cliente pode não ter a certeza onde está a correr o seu servidor virtual

[Amazon Web Services - Official Site](#) Traduzir esta página

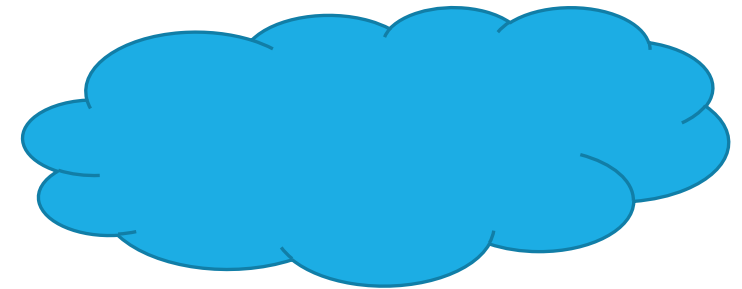
[aws.amazon.com](#) ▼

Amazon Web Services offers reliable, scalable, and inexpensive cloud computing services. Free to join, pay only for what you use.

- Exemplo: Cliente tem um Servidor Amazon.com AWS
 - Amazon tem grandes Data Centers na California, Oregon e Virginia
 - Num determinado momento o servidor virtual pode estar em qualquer um desses Data Centers
 - Mesmo que soubesse qual o Data Center, não saberia em que máquina física estaria a correr

A nuvem - Cloud

- Por essa razão, ao desenhar-se um diagrama de rede, em vez de desenhar o servidor numa localização específica, desenha-se uma nuvem, e utiliza-se o respetivo termo



Nuvem Pública – Nuvem Privada

- A nuvem pública pertence a outra entidade que a aluga mensalmente, existindo muitos clientes diferentes a correr no mesmo conjunto de hardware
- A nuvem privada pertence a quem a utiliza, pelo que apenas existe um cliente a correr numa nuvem privada
- Nuvem híbrida – Combinação de nuvem privada e nuvem pública



Nuvem Híbrida

- Nuvem híbrida – Combinação de nuvem privada e nuvem pública
- Opção cada vez mais Popular
- Exemplo 1: Empresa A utiliza:
 - nuvem privada onde correm as suas máquinas virtuais
 - nuvem pública como plano de backup ou de contingência, para mover para lá as suas máquinas virtuais, no caso da nuvem privada falhar por algum motivo



Nuvem Híbrida

- Exemplo 2: Empresa B de vendas online:
 - que tem um certo movimento durante a maior parte do ano, que a sua nuvem privada pode tratar,
 - mas durante alturas de pico, como o Natal, podem precisar poder de computação extra, podendo combinar com uma nuvem pública, e utilizar ambas as nuvens, privada e pública, durante o pico



Tipos de Serviço Oferecido

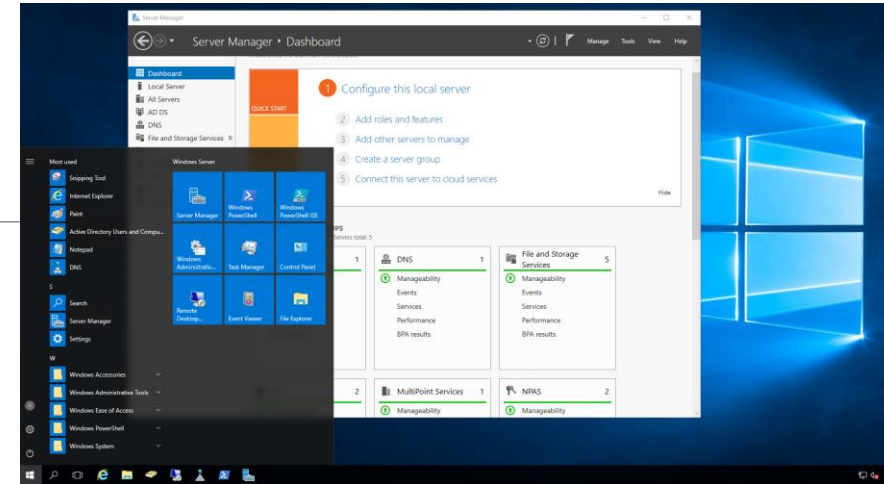
- Os fornecedores de cloud oferecem uma variedade de serviços.
- A maioria dos serviços encaixa-se numa das seguintes categorias:
 - Infrastructure as a service (IaaS)
 - Platform as a service (PaaS)
 - Software as a service (SaaS)

Infrastructure as a service (IaaS)

- O fornecedor de cloud fornece processador, memória e disco virtuais
- O cliente pode utilizar estes recursos como entender:
 - pode instalar máquinas virtuais
 - nessas máquinas pode correr (quase):
 - qualquer SO
 - qualquer software



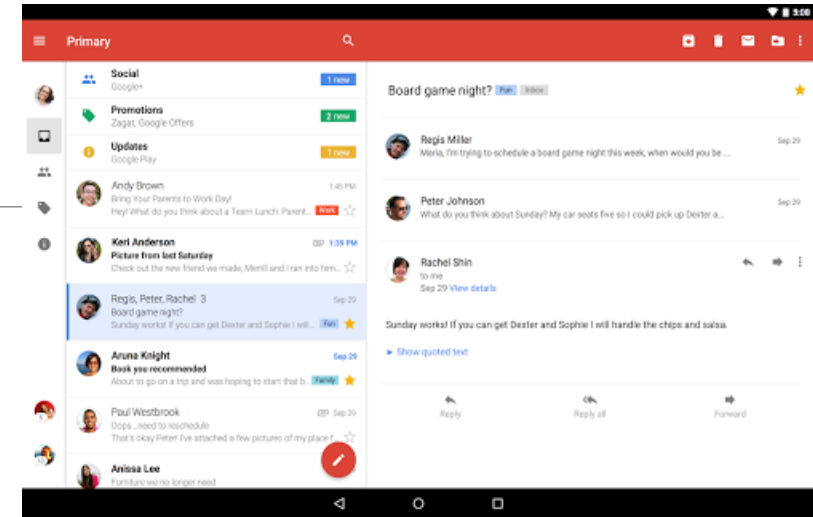
Platform as a service (PaaS)



- O fornecedor de cloud fornece uma plataforma pré-determinada
- SO pré-determinado
- Eventualmente também algum software, como por exemplo um servidor de base de dados e/ou um servidor web
 - Neste exemplo o cliente pode imediatamente começar a criar o seu site web ou carregar dados na BD, sem ter que se preocupar em instalar um SO ou geri-lo.

Software as a service (SaaS)

- O fornecedor de cloud fornece um serviço de software pré-definido e completamente funcional
- O cliente utiliza tal como está
- Tipicamente pouca ou nenhuma manutenção ou gestão pelo cliente
- Exemplo: Quem usa uma conta gmail, está a utilizar um fornecedor de e-mail SaaS. (SaaS e-mail provider), que corre na nuvem google



VMware vSphere ESXi

ESXi – Networking

The screenshot displays the VMware ESXi vSphere Client interface. The top navigation bar shows the user 'root@192.168.15.140' and a search bar. The left-hand 'Navigator' pane shows the hierarchy: Host > Manage > Monitor > Networking > vSwitch0. The main content area is titled 'vSwitch0' and provides details for a Standard vSwitch with 2 port groups and 2 uplinks.

vSwitch0 Details:

vSwitch Details	
MTU	1500
Ports	1536 (1529 available)
Link discovery	Listen / Cisco discovery protocol (CDP)
Attached VMs	0 (0 active)
Beacon interval	1

NIC teaming policy:

NIC teaming policy	
Notify switches	Yes
Policy	Route based on originating port ID
Reverse policy	Yes

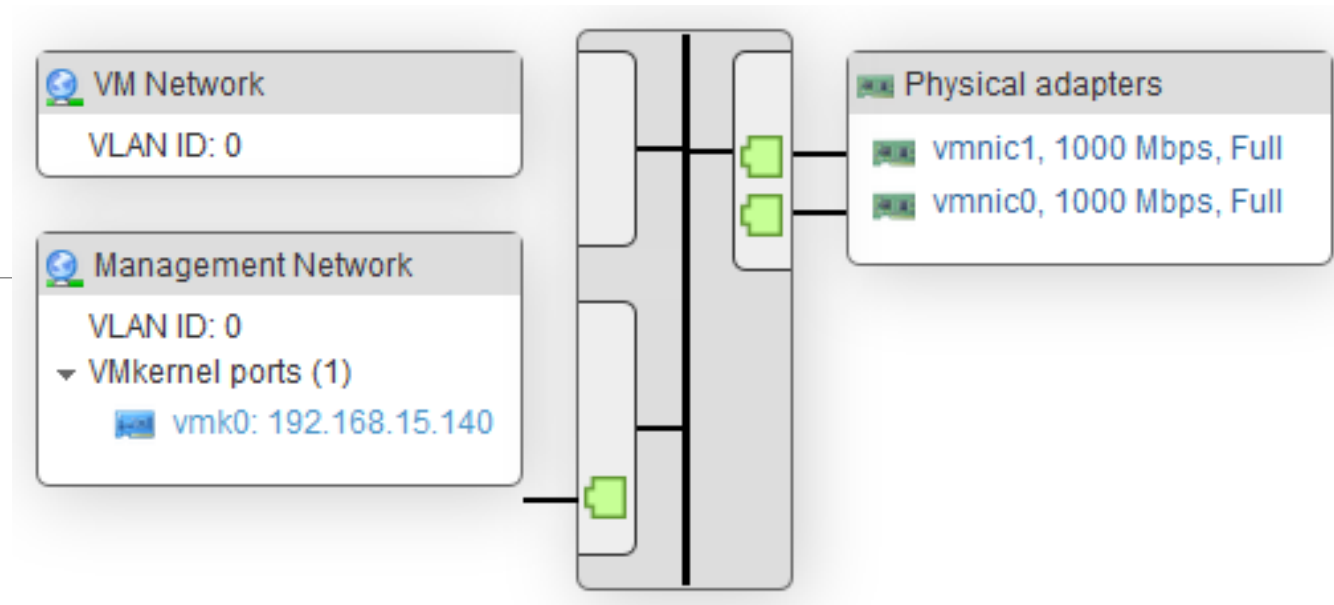
vSwitch topology:

The topology diagram shows the vSwitch connected to two networks: 'VM Network' and 'Management Network', both with VLAN ID: 0. The 'Management Network' is further connected to a 'VMkernel port' named 'vmk0' with IP address 192.168.15.140. On the right, the 'Physical adapters' section shows two adapters: 'vmnic1, 1000 Mbps, Full' and 'vmnic0, 1000 Mbps, Full'.

Recent tasks:

Task	Target	Initiator	Queued	Started	Result	Completed
------	--------	-----------	--------	---------	--------	-----------

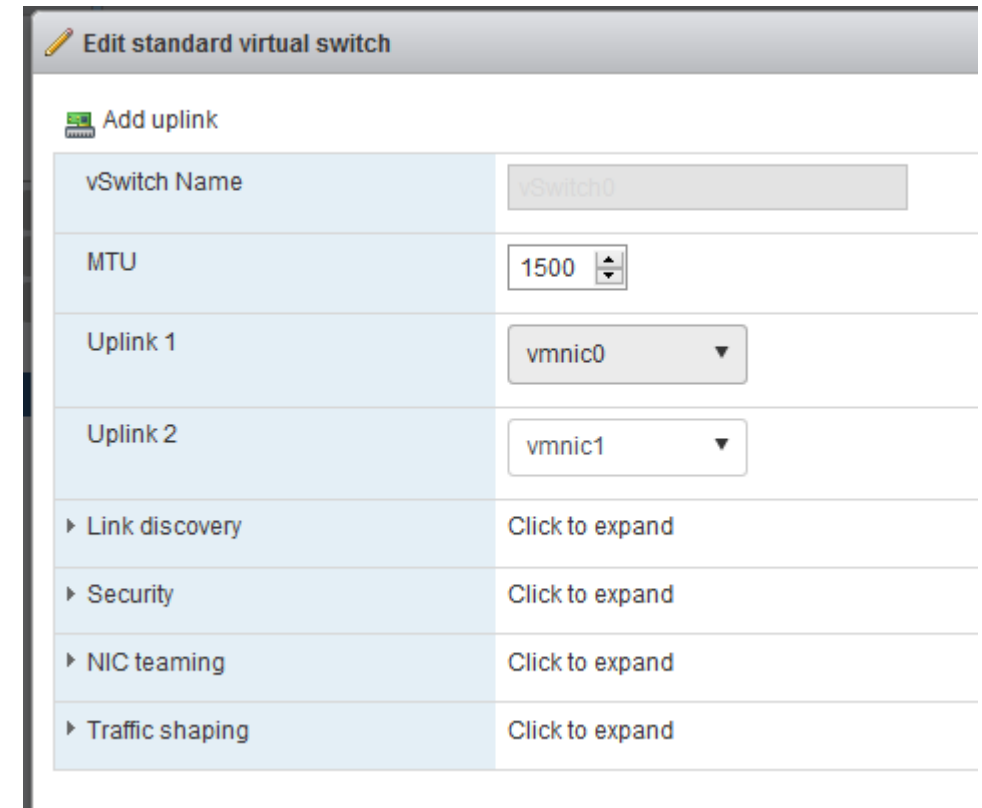
ESXi – Networking




- Physical Adapters. Clicar para ver detalhes das NICs
- As ligações ao vSwitch são feitas através dos Portgroups.
 - No exemplo o vSwitch0 tem 2 portgroups e 2 NICs físicas.
 - Um portgroup para VMs; outro para VMkernels
- As VMkernel NICs são NICs virtuais (com IP) que permitem implementar no host serviços como: Management, Fault tolerance logging, vMotion, ...
 - Por omissão existe a vmk0 apenas com o serviço Management ativo

ESXi – Networking

- Pode configurar-se no vSwitch:
 - MTU (default 1500 B);
 - Link discovery: CDP
 - Security - permitir: modo promíscuo, MAC address changes e Forged transmits
 - Traffic shaping: alocar bandwidth a uma VM
 - Teaming and failover: Load balancing, Network failover detection, Failback



Edit standard virtual switch

 Add uplink

vSwitch Name	vSwitch0
MTU	1500
Uplink 1	vmnic0
Uplink 2	vmnic1
▶ Link discovery	Click to expand
▶ Security	Click to expand
▶ NIC teaming	Click to expand
▶ Traffic shaping	Click to expand

ESXi – Networking

- Depois da configuração de todo o vSwitch, pode ajustar-se a configuração diretamente num determinado portgroup:
 - VLAN:
 - None: tráfego encaminhado sem tag
 - All ou 4095: tag recebida não é alterada
 - Número específico: tráfego é marcado com essa tag
 - Nas restantes opções é possível fazer o “override” às configurações do vSwitch

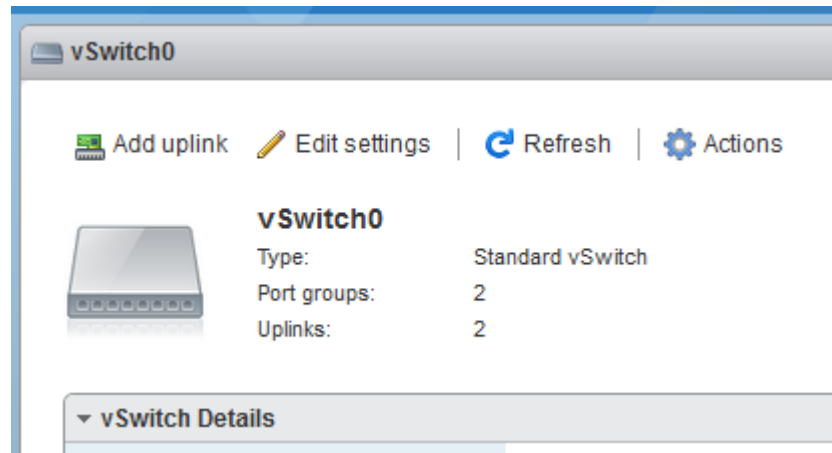
Edit port group - VM Network

Name	VM Network
VLAN ID	
Virtual switch	vSwitch0
Security	
Promiscuous mode	<input type="radio"/> Accept <input type="radio"/> Reject <input checked="" type="radio"/> Inherit from vSwitch
MAC address changes	<input type="radio"/> Accept <input type="radio"/> Reject <input checked="" type="radio"/> Inherit from vSwitch
Forged transmits	<input type="radio"/> Accept <input type="radio"/> Reject <input checked="" type="radio"/> Inherit from vSwitch
▶ NIC teaming	Click to expand
▶ Traffic shaping	Click to expand

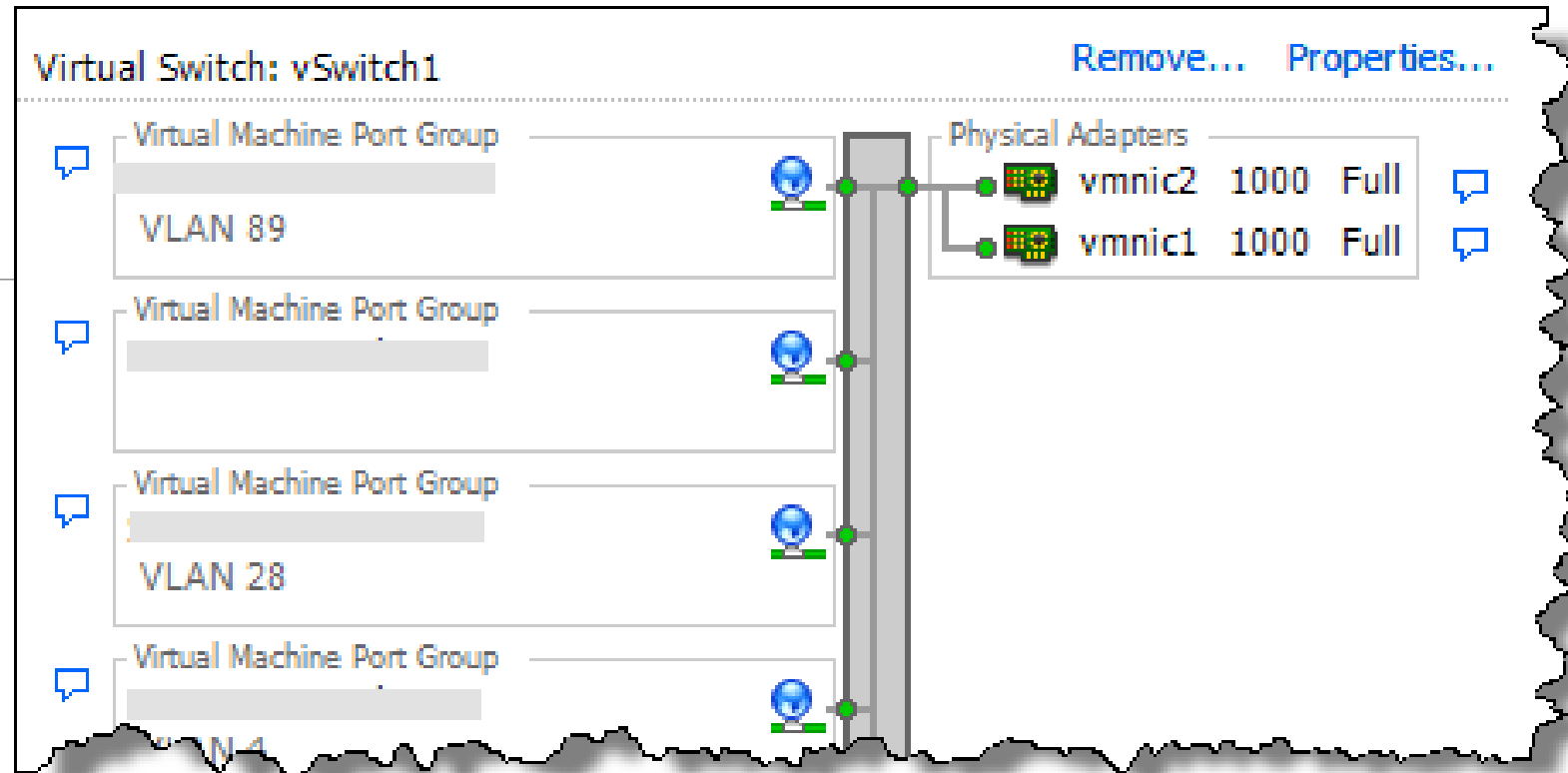
Save Cancel

ESXi – Networking

- É possível adicionar NICs físicas (pré-existentes) ao vSwitch: “Add uplink” ou “Add Physical NIC”

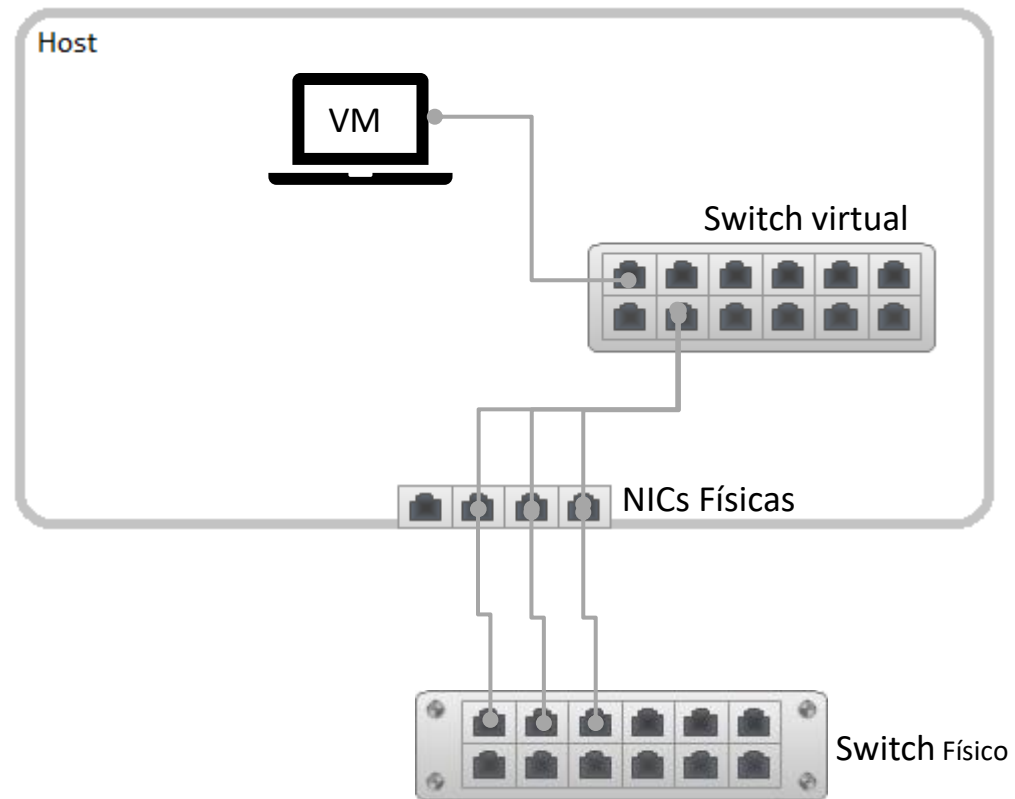


NIC Teaming



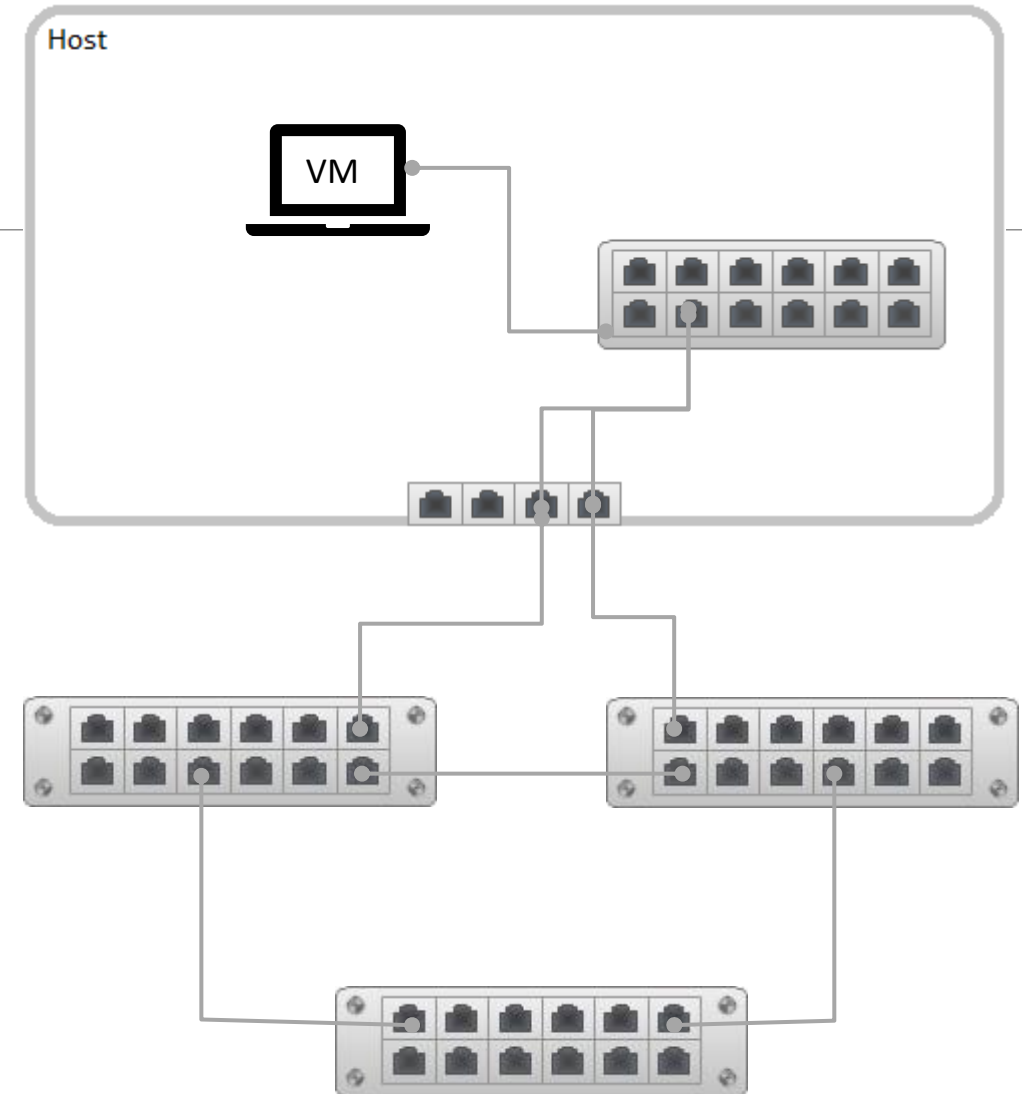
- NIC teaming permite aumentar a capacidade de rede de um switch virtual, e/ou fornecer redundância, incluindo duas ou mais NICs físicas numa equipa (team)

NIC Teaming



NIC Teaming

- Todas as portas no switch físico têm que estar no mesmo domínio de broadcast layer 2



NIC Teaming – Load balancing

- O switch virtual faz o load balancing do tráfego de saída
- O switch físico faz o load balancing do tráfego de entrada

- Métodos de deteção de falha:
 - Link status only
 - Beacon probing

NIC Teaming – Detecção de falha

- Link status only
 - Estado do link fornecido pela NIC:
deteta cabos removidos
e falhas de energia no switch físico
 - Não deteta
porta do switch físico bloqueada pelo STP
ou configurada na VLAN errada

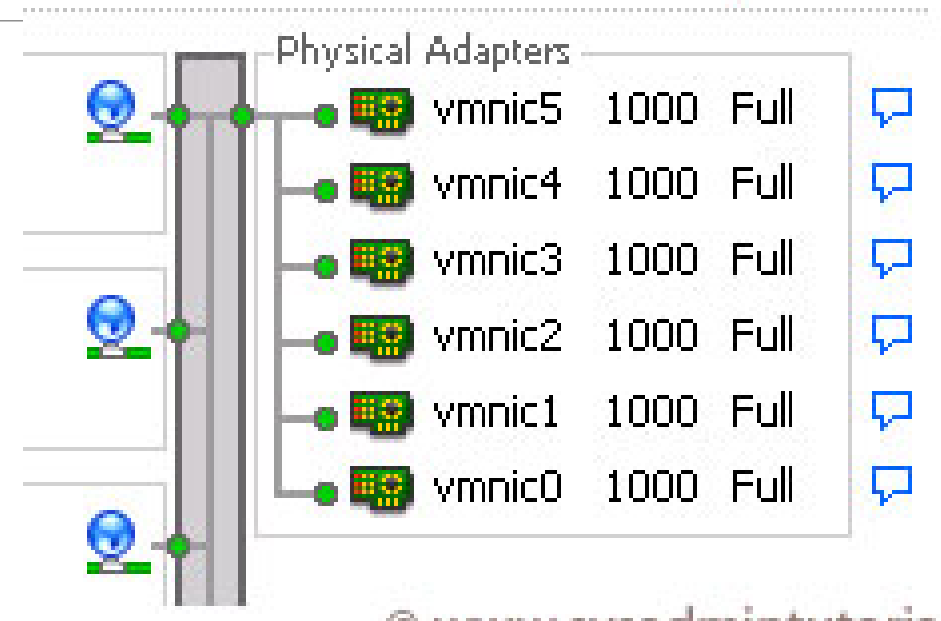


NIC Teaming – Detecção de falha

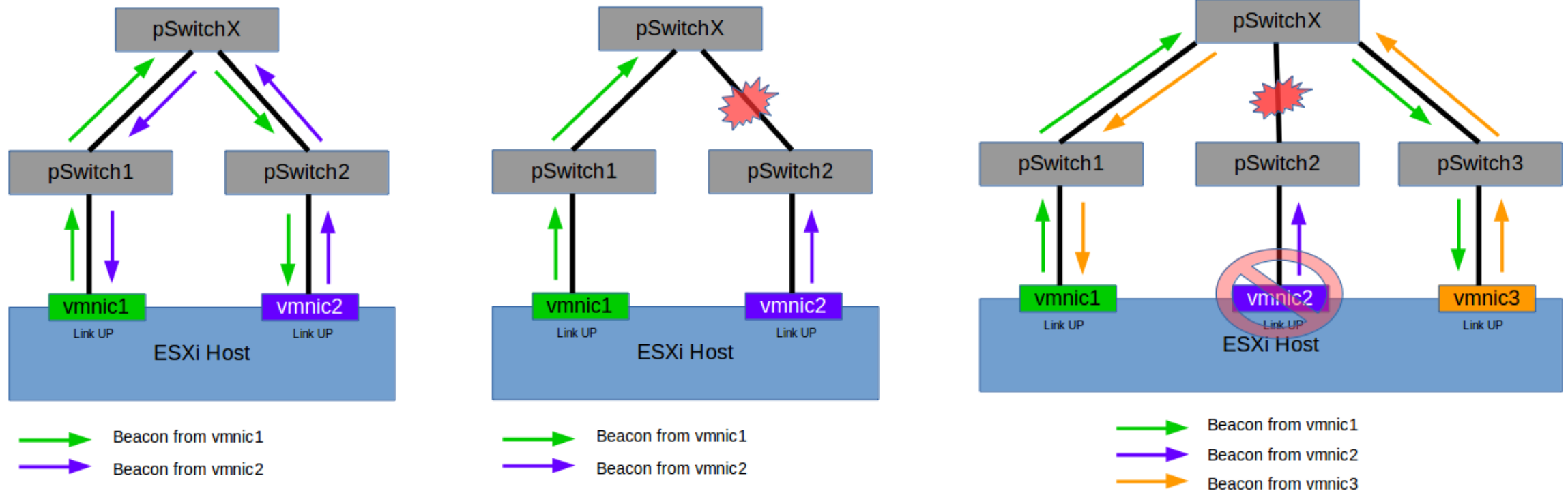
- Beacon probing
 - Envia e escuta frames Ethernet, sondas beacon, através de todas as NICs físicas da equipa (a cada segundo)
 - Muito útil na deteção de falhas do switch físico que não causam um evento link-down

NIC Teaming – Detecção de falha

- Beacon probing
 - Utilizar este método com 3 ou mais NICs.
 - Com apenas 2 NICs o switch não consegue determinar qual a NIC a retirar, pois nenhuma delas recebe beacons, e envia todos os pacotes para ambas as NICs
 - Com n NICs, consegue detetar-se n-2 falhas em NICs



NIC Teaming – Detecção de falha



NIC Teaming – Detecção de falha

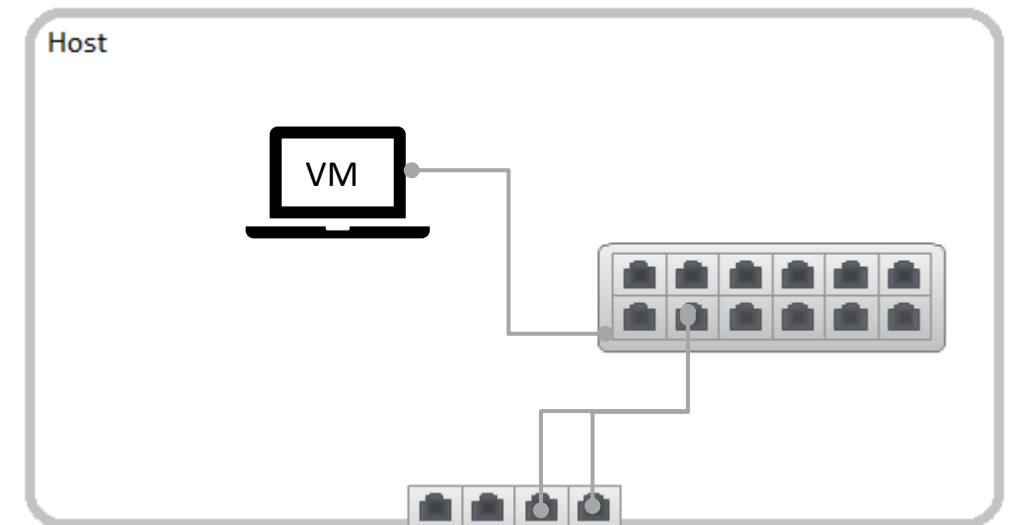
- Otimizações no switch físico nas portas que ligam ao host:
 - Desativar o STP
 - (Cisco) Ativar o modo PortFast para portas de acesso e modo PortFast trunk para interfaces trunk.
Isto pode poupar 30 segundos durante a inicialização do switch físico
 - Desativar a negociação de trunks

NIC Teaming – Load balancing

- Podem configurar-se vários algoritmos de load balancing pelas NICs físicas da equipa (team):
 - Route Based on Originating Virtual Port (default)
 - Route Based on Source MAC Hash
 - Route Based on IP Hash
 - Route Based on Physical NIC Load
 - Use Explicit Failover Order

NIC Teaming – Load balancing

- Route Based on Originating Virtual Port
 - Cada VM tem um Virtual Port ID no switch virtual
 - O switch virtual seleciona uma das NICs para uma VM apenas uma vez
 - Todo o tráfego da VM é enviado por esta NIC



NIC Teaming – Load balancing

(Route Based on Originating Virtual Port)

- Vantagens:
 - Consome poucos recursos
 - Boa distribuição de tráfego se há mais NICs virtuais (várias VMs) que NICs físicas na equipa
 - Não é necessário configurar o switch físico

NIC Teaming – Load balancing

(Route Based on Originating Virtual Port)

- Desvantagens:
 - Pode haver NICs sub-utilizadas (VMs com pouco tráfego)
 - Uma VM fica limitada à largura de banda da NIC física que lhe está atribuída

NIC Teaming – Load balancing

- Route Based on Source MAC Hash
 - Normalmente o mesmo que Route Based on Originating Virtual Port
 - Mas com overhead superior pois o hash é calculado para cada frame
 - A distribuição só difere do anterior se a VM estiver a utilizar mais que um MAC nessa NIC: forged transmits, MAC spoofing

NIC Teaming – Load balancing

X.X.X.Y	X.X.X.Z	
---------	---------	--

- Route Based on IP Hash
 - O switch virtual escolhe a NIC com base no último octeto dos IPs origem e destino do pacote
 - Uma VM pode assim utilizar todas as NICs, resultando num maior throughput potencial, se comunicar com vários IPs destino
 - Mas se comunicar apenas com um IP destino, vai utilizar apenas uma das NICs
 - Obriga a configurar um Etherchannel no switch físico

NIC Teaming – Load balancing

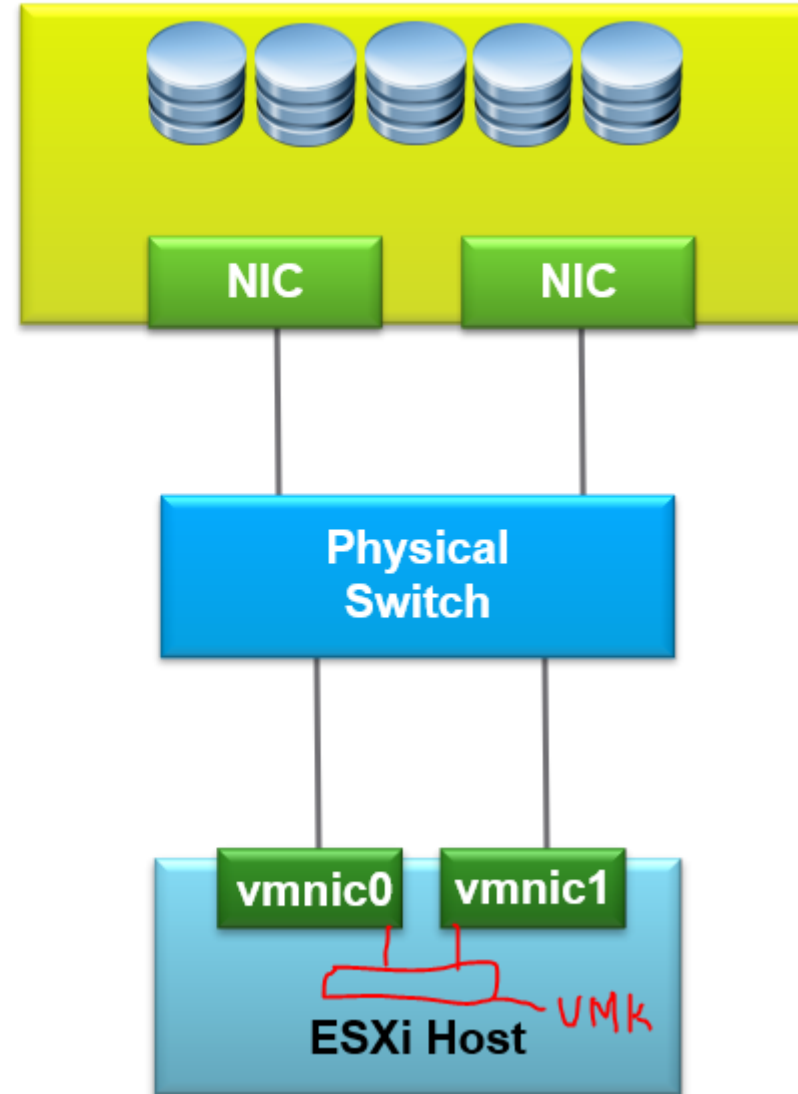
(Route Based on IP Hash)

- Com um Etherchannel, o switch físico regista o MAC da VM nas várias portas e distribui os pacotes por elas
- Sem um Etherchannel, o switch físico altera constantemente o registo na porta do MAC da VM
- Só é suportado Etherchannel estático.
Etherchannel com LACP só é suportado em switchs virtuais distribuídos (vDS).
- Maior consumo de recursos

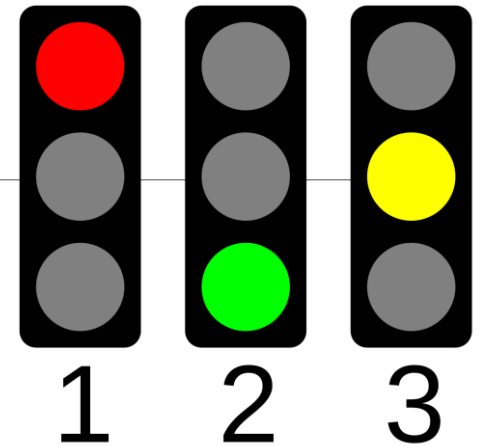
Multipathing and NFS v4.1 Storage

One recommended configuration for NFS version 4.1 multipathing:

- Configure one VMkernel port.
- Use adapters attached to the same physical switch to configure NIC teaming.
- Configure the NFS server with multiple IP addresses:
 - IP addresses can be on the same subnet.
- To better utilize multiple links, configure NIC teams with the IP hash load-balancing policy.



NIC Teaming – Load balancing



- Route Based on Physical NIC Load
 - Só é suportado em switchs virtuais distribuídos (vDS).
 - Método baseado no método Route Based on Originating Virtual Port.
 - Inicialmente é atribuído um uplink da equipa à VM.
 - O vDS testa os uplinks de 30 em 30 segundos, e se a carga (load) excede 75% da utilização, a VM com a maior carga é movida para um uplink diferente

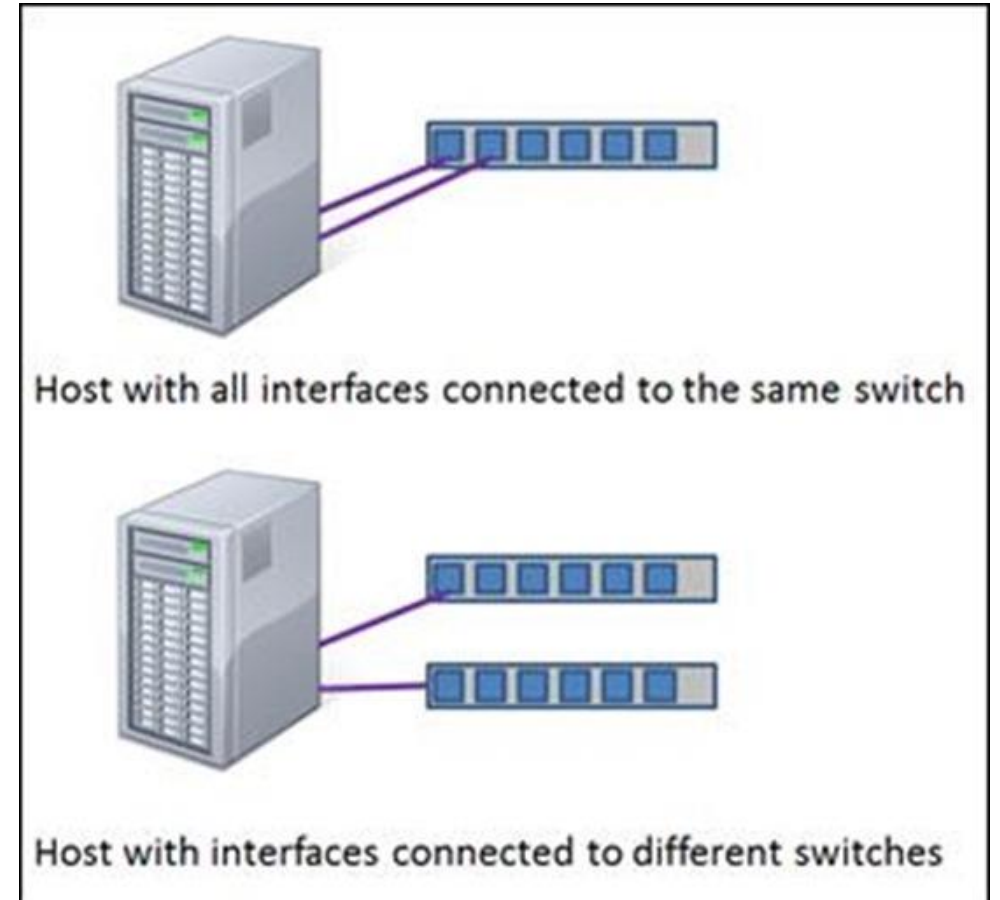
NIC Teaming – Load balancing

(Route Based on Physical NIC Load)

- + Baixo consumo de recursos
- + Não é preciso configurar switch físico
- - A largura de banda disponível para uma VM está limitada pelo uplink que está a utilizar

NIC Teaming – Load balancing

- Use Explicit Failover Order
 - Não faz balanceamento de carga.
 - Utiliza apenas uma NIC

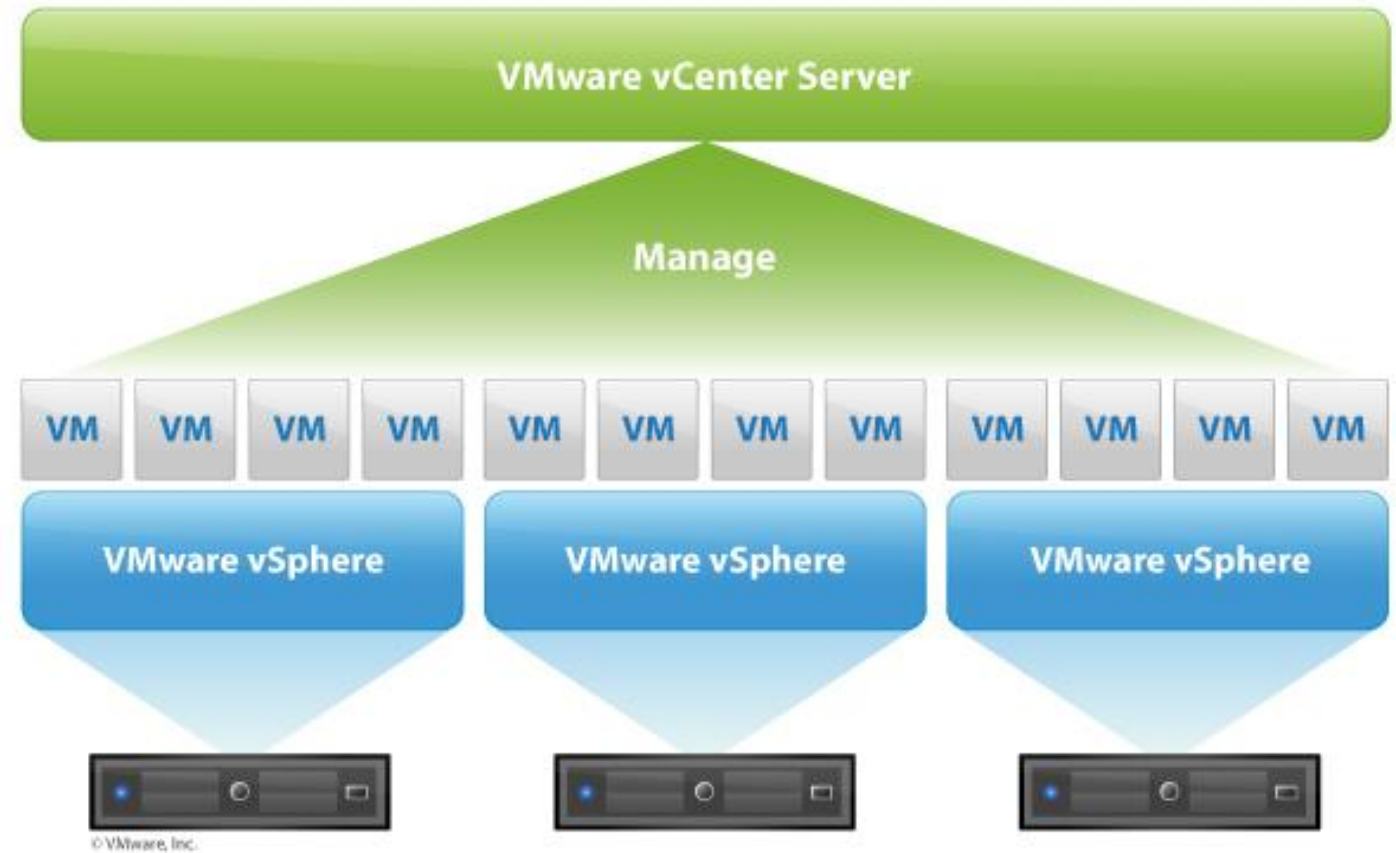


VMware vSphere Distributed Switch -vDS

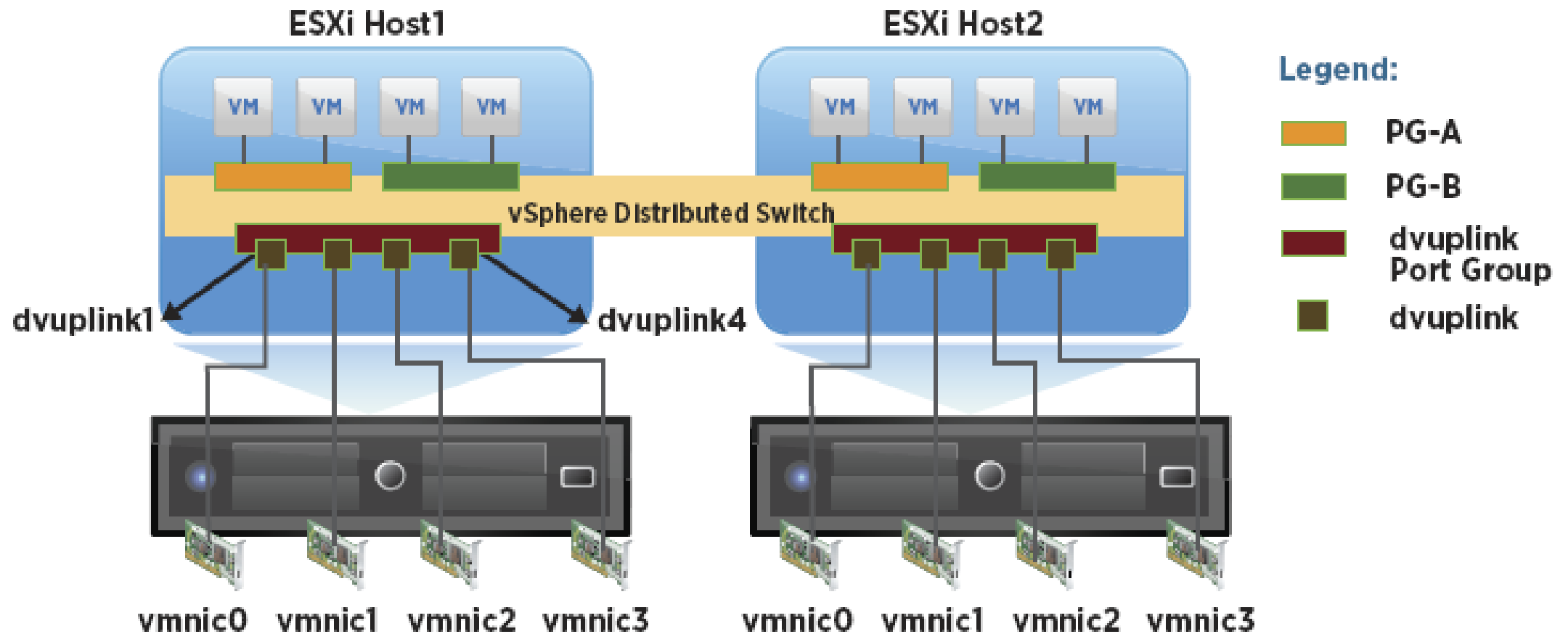
- Um switch distribuído permite que um switch virtual se ligue a múltiplos hosts para gestão centralizada de configurações de rede
- Isto permite às VMs manter configuração de rede consistente nas migrações entre vários hosts
- Ao criar-se o vDS, cada NIC física do host é ligada a um uplink do vDS, podendo configurar-se failover e load balancing.

VMware vSphere Distributed Switch -vDS

- Um vDS configura-se num vCenter Server, sendo a configuração replicada pelos hosts que estão associados com o switch.

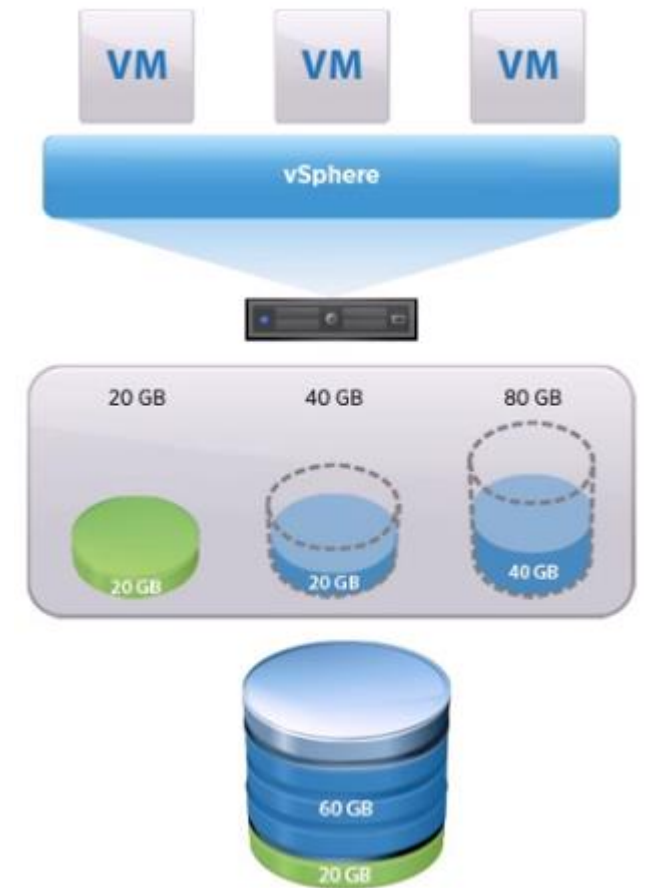


VMware vSphere Distributed Switch -vDS



ESXi – Storage –Thin Provisioning

- O disco thin começa pequeno
- Inicialmente usa apenas o espaço que necessita para as suas operações iniciais
- Se precisa mais espaço, pode crescer até à sua capacidade máxima
- Este é o método mais rápido de provisionamento
- Os blocos de storage são alocados e apagados (reescritos com zeros) no 1º acesso



ESXi – Storage –Thick Provisioning

- O espaço é todo alocado quando o disco é criado
- Duas opções:
 - Thick Provision Lazy Zeroed
 - Thick Provision Eager Zeroed

ESXi – Storage –Thick Provisioning

- Thick Provision Lazy Zeroed
 - Os dados do disco físico não são apagados na criação, sendo apagados na primeira escrita pela VM
 - As VMs não leem dados velhos do dispositivo físico
- Thick Provision Eager Zeroed
 - Os dados velhos do disco físico são apagados quando o disco é criado
 - Este é o processo mais demorado de criação de discos

Converter um servidor físico para servidor virtual (P2V)

- P2V – Physical to Virtual
- A **VMware** tem o **vCenter converter** que converte uma **máquina** física especificamente para uma VM VMware
- A **Microsoft** tem o **Disk2vhd** que converte um **disco** físico para um disco virtual VHD

Converter um servidor físico para servidor virtual (P2V)

- Ambos os produtos anteriores
 - convertem máquinas desligadas e algumas ligadas
 - são gratuitos
- Quase todos os hypervisores têm uma ferramenta P2V que é normalmente grátis
- Isto porque é estratégico para os fabricantes que se convertam máquinas físicas para VMs otimizadas para os seus hypervisores

Converter um servidor físico para servidor virtual (P2V)

- Uma forma de evitar potenciais problemas é desligar a máquina antes de fazer a conversão.
- Outra forma é tentar minimizar a quantidade de fluxo de dados na máquina durante a conversão.
- É normalmente necessário indicar as novas ligações de rede

Converter um servidor físico para servidor virtual (P2V)

- Uma VM vai precisar sempre de drivers um pouco diferentes da máquina física
- A maioria das ferramentas P2V tentará reconhecer os drivers em utilização, e por quais precisam ser substituídos
- Contudo, depois da conversão, por vezes é necessário instalar manualmente alguns drivers

Converter um servidor físico para servidor virtual (P2V)

- É preciso definir quando (cut over) se vai desligar o servidor físico (decommissioning) e substituí-lo pelo servidor virtual
- Minimizar o downtime é um desafio!

Converter um servidor físico para servidor virtual (P2V)

- Uma conversão P2V é uma migração, não um upgrade!
- O objetivo é obter uma VM a correr, da mesma forma que a máquina física estava
- Pode ser tentador corrigir algumas pequenas coisas que estavam menos bem no servidor físico, ao mesmo tempo que se faz a conversão
- Melhor não! Vai complicar o Troubleshooting!

VMware Converter

- O VMware Converter, além da conversão P2V, permite copiar VMs entre hypervisors, com ajustes de hardware e de configurações

VMware Converter - Origem

VM Off	Workstation
	ESXi
	Hyper-V Server
VM On	Windows *1
	Linux *1 *3 *4
	Máquina Local *2

*1 Por ssh; pode ser uma máquina física ou uma VM

*2 Física ou virtual! Correr Converter como administrador

*3 pfSense não dá! Não é linux!

*4 É preciso ter acesso ssh ao user e o user ser capaz de executar comandos sudo sem password

VMware Converter - Opções

- Visualizar descrição da VM origem
- Escolher quais os discos e formato (thick por omissão!)
- Escolher quais as redes onde ligar as NICs
- Escolher versão do hardware destino (incluindo upgrades ou downgrades)
- ...

VMware Converter - Destino

- Workstation (Pro, Player, Fusion) (só com VM desligada)
- ESXi
- (Ao contrário da origem o destino não pode ser Hyper-V nem máquina física, naturalmente)

ESXi – vCenter Server

- O VMware vCenter Server fornece gestão centralizada para datacenters.
- Agrega recursos físicos de vários hosts e apresenta uma coleção central de recursos flexíveis para o administrador poder fornecer às VMs no ambiente virtual.

ESXi – vCenter Server

- O vCenter Server pode ser instalado numa máquina Windows (física ou virtual!)
- Alternativamente a VMware disponibiliza uma Appliance Linux. Esta appliance é uma VM linux pré-configurada, otimizada para correr o vCenter Server e os serviços associados. Esta é a opção recomendada para as versões atuais do vCenter.

ESXi – vCenter Server

- No vCenter Server é possível criar um “Software Defined Datacenter”
- É possível depois adicionar hosts (por nome ou IP) ao Datacenter, indicando o username e password
- É possível escolher para o host o modo Lockdown, ficando o host acessível apenas através do vCenter.

Referências

- Cursos da Academia VMware
- Virtualization Essential Training, Martin Guidry, Lynda.com
- Virtualization Essentials, Matthew Portnoy, Sybex, Wiley
- Site www.virtualbox.org
- Site VMware: www.vmware.com
- Blog vswitchzero.com