Virtual Network

Overview

The networking provided allows a VM to communicate with other VMs as well as physical machines. Helps with:

- vmotion
- fault tolerance
- ip based storage
- ...

Virtual Switch

Like a physical switch... but virtual.

- works at layer 2 of osi
- Only one virtual switch attached to same physical NIC, but multiple physical NICs to same virtual switch (as with physical nics)
- If we combine physical nics -> load balance, fault tolerance, combine bandwidth

What is the management network

- We configured an IP for this at setup time.
- This is a network over which management traffic flows, not vm traffic
- Why should this be separate?

vNetwork Standard Virtual Switch (vSwitch or VSS)

- configuration done at host level (ESXi)
- vSwitch0 created when install ESXi
  - has a vm port group (VM Network)
  - VM kernel port (Management network)

vNetwork Distributed Virtual Switch (dvSwitch or vDS)

- More functionality
  - Port mirroring
- Can function as a single virtual switch across all ESXi hosts
- Created through vcenter server
Advantages and Disadvantages

- vDs have centralized configuration
- vDS make vmotion easier
- vDS other advanced features
- More expensive licensing
- More complex
- If you lose vcenter server, you can’t manage network

Virtual Switch Ports

- VM Port
  - every vm connects to a particular vm port on the virtual switch. The collection of these ports is a vm port group.
- VMKernel Port
  - Used for management, fault-tolerance, vmotion, accessing storage

Virtual Switch Ports

It is common to separate management and vmotion traffic from the VM traffic.

You could put the vmotion network on a higher capacity physical link.

VLan overview

Allow us to isolate traffic. Or one network and another network.

Trunk port = passes multiple vlans

Basically, your frame is encapsulated in a 802.1q packet. The switch uses this to figure out what broadcast domain you are in.

VLan info

The switch port on the physical switch to which ESXi’s physical NIC is connected must be configured as a static trunk port. Packets from the virtual machine are tagged as they exit the virtual switch and are untagged as they return to the virtual machines. VMware claims that the effect on the performance is minimal.

Network Security Policies

- Security
  - Promiscuous mode - traffic sent to all ports on a vSwitch (useful for wireshark?) default is off.
  - Mac address changes - dont let vm change its Mac
  - Forged Transmits - Dont let vm change its mac
  - Traffic Shaping - controls amt of bandwidth that a vm can transmit.
  - Nic teaming - multiple network adapters for load-balancing and failover.