Introduction

New networking features

Networking virtual machines
  > Virtual Switch Connections
  > Port Group Policies

Networking IP Storage
  > iSCSI
  > NAS
A networking Scenario

Virtual Machines
- VM1 (Production VM)
- VM2 (NAT client)
- VM3 (NAT router)
- Service Console

Physical Switches
- Test LAN (VLAN 101)
- Production LAN (VLAN 102)
- IP Storage LAN (VLAN 103)
- Mgmt LAN

NIC speeds:
- 100 Mbps
- 1000 Mbps

IP storage LAN VLAN: 103
A Networking Scenario

Virtual Machines
- VM1: Production VM
- VM2: NAT client
- VM3: NAT router

Physical NICs
- Test LAN: VLAN 101
- Production LAN: VLAN 102
- IP Storage LAN: VLAN 103
- Mgmt LAN

Physical Switches
- 1000 Mbps
- 100 Mbps

VMWorld 2006
vSwitch - No Physical Adapters (Internal Only)

- Each switch is an internal LAN, implemented entirely in software by the VMkernel
- Provides networking for the VMs on a single ESX Server system only
- Zero collisions
- Up to 1016 ports per switch
- Traffic shaping is not supported
vSwitch - One Physical Adapter

- Connects a virtual switch to one specific physical NIC
- Up to 1016 ports available
  > Zero collisions on internal traffic
- Each Virtual NIC will have its own MAC address
- Outbound bandwidth can be controlled with traffic shaping
Combining Internal And External vSwitches

- Virtual switch with one outbound adapter acts as a DMZ
- Back-end applications are secured behind the firewall using internal-only switches
- Can connect to an 802.3ad NIC team
- Up to 1016 ports per switch
  - Zero collisions on internal traffic
- Each Virtual NIC will have its own MAC address
- Improved network performance by network traffic load distribution
- Redundant NIC operation
- Outbound bandwidth can be controlled with traffic shaping
Network Connections

- There are three types of network connections:
  - Service console port – access to ESX Server management network
  - VMkernel port – access to VMotion, iSCSI and/or NFS/NAS networks
  - Virtual machine port group – access to VM networks

- More than one connection type can exist on a single virtual switch, or each connection type can exist on its own virtual switch
Connection Type: Service Console Port

- Virtual NICs
  - VMware
  - VM1
  - VM2
  - VM3

- Physical NICs
  - Production LANs
  - Management LAN
  - Storage/Vmotion LAN

- Service console port defined for this virtual switch

VMWORLD 2006
Connection Type: VMkernel Port

VMkernel port defined for this virtual switch
Connection Type: Virtual Machine Port Group

Virtual NICs

Virtual Switches
VM0 VM1 VM2 VM3

Physical NICs

Production LANs

Storage/Vmotion LAN

Management LAN

Virtual machine port groups defined for these virtual switches
Defining Connections

- A connection type is specified when creating a new virtual switch
- Parameters for the connection are specified during setup
- More connections can be added later

Add Network Wizard

Connection Type
Network Access
Connection Settings
Summary

Connection Types

- **Virtual Machine**
  Add a labeled network to handle virtual machine network traffic.

- **VMkernel**
  The VMkernel TCP/IP stack handles traffic for the following ESX services: VMotion, iSCSI, and NFS.

- **Service Console**
  Add support for host management traffic.
Naming Virtual Switches And Connections

- All virtual switches are known as vSwitch#
- Every port or port group has a network label
- Service console ports are known as vSwif#
Network Policies

- There are four network policies:
  - VLAN
  - Security
  - Traffic shaping
  - NIC teaming

- Policies are defined
  - At the virtual switch level
    - Default policies for all the ports on the virtual switch
  - At the port or port group level
    - Effective policies: Policies defined at this level override the default policies set at the virtual switch level
Network Policy: VLANs

- Virtual LANs (VLANs) allow the creation of multiple logical LANs within or across physical network segments
- VLANs free network administrators from the limitations of physical network configuration
- VLANs provide several important benefits
  - Improved security: the switch only presents frames to those stations in the right VLANs
  - Improved performance: each VLAN is its own broadcast domain
  - Lower cost: less hardware required for multiple LANs
- ESX Server includes support for IEEE 802.1Q VLAN Tagging
Network Policy: VLANs (2)

- Virtual switch tagging
  - Packets leaving a VM are tagged as they pass through the virtual switch
  - Packets are cleared (untagged) as they return to the VM
  - Little impact on performance
Administrators can configure Layer 2 Ethernet security options at the virtual switch and at the port groups.

There are three security policy exceptions:

- Promiscuous Mode
- MAC Address Changes
- Forged Transmits
Network Policy: Traffic Shaping

- Network traffic shaping is a mechanism for controlling a VM’s outbound network bandwidth.
- Average rate, peak rate, and burst size are configurable.

\[ \text{Burst size} = \text{bandwidth} \times \text{time} \]
Network Policy: Traffic Shaping (2)

- Disabled by default
- Can be enabled for the entire virtual switch
  - Port group settings override the switch settings
- Shaping parameters apply to each virtual NIC in the virtual switch
Network Policy: NIC Teaming

- NIC Teaming settings:
  - Load Balancing
  - Network Failure Detection
  - Notify Switches
  - Rolling Failover
  - Failover Order

- Port group settings are similar to the virtual switch settings
  - Except port group failover order can override vSwitch failover order

Port group settings are similar to the virtual switch settings. Except port group failover order can override vSwitch failover order.
Load Balancing: vSwitch Port-based (Default)

Virtual NICs

VM0

VM1

VM2

VM3

Virtual Switch

VM ports

uplink ports

Teamed physical NICs
Load Balancing Method: IP-based

ESX Server

VM

NIC

VM

Router

Internet

Client

Client

Client
Detecting And Handling Network Failure

- Network failure is detected by the VMkernel, which monitors the following:
  - Link state only
  - Link state + beaconing
- Switches can be notified whenever:
  - There is a failover event
  - A new virtual NIC is connected to the virtual switch
  - Updates switch tables and minimizes failover latency
- Failover is implemented by the VMkernel based upon configurable parameters
  - Failover order: Explicit list of preferred links (uses highest-priority link which is up)
    - Maintains load balancing configuration
    - Good if using a lower bandwidth standby NIC
  - Rolling failover -- preferred uplink list sorted by uptime
Multiple Policies Applied To A Single Team

- Different port groups within a vSwitch can implement different networking policies
  - This includes NIC teaming policies
- Example: different active/standby NICs for different port groups of a switch using NIC teaming

![Diagram of VM ports and uplink ports with active and standby NICs configured differently for each group.](image)
IP Storage
What is iSCSI?

- A SCSI transport protocol, enabling access to storage devices over standard TCP/IP networks
  - Maps SCSI block-oriented storage over TCP/IP
  - Similar to mapping SCSI over Fibre Channel
- “Initiators”, such as an iSCSI HBA in an ESX Server, send SCSI commands to “targets”, located in iSCSI storage systems
How is iSCSI Used With ESX Server?

- Boot ESX Server from iSCSI storage
  - Using hardware initiator only
- Create a VMFS on an iSCSI LUN
  - To hold VM State, ISO images, and templates
- Allows VM access to a raw iSCSI LUN
- Allows VMotion migration of a VM whose disk resides on an iSCSI LUN
Components of an iSCSI SAN

- iSCSI Storage System
- Physical hard disks
- LUNs (Logical Unit Numbers)
- SP (Storage Processor)
- TCP/IP Network
- Servers with iSCSI initiators

Targets

- Disk Array
- SP
- IP Network

Initiators

- HBA
- ESX Server
- Initiator* (Software implementation)
Addressing in an iSCSI SAN

*iSCSI target name*
iqn.1992-08.com.netapp:stor1

*iSCSI alias*
stor1

*IP address*
192.168.36.101

*iSCSI initiator name*
iqn.1998-01.com.vmware:train1

*iSCSI alias*
train1

*IP address*
192.168.36.88
How iSCSI LUNs Are Discovered

- Two discovery methods are supported:
  - Static Configuration
  - SendTargets

- iSCSI device returns its target info as well as any additional target info that it knows about.

iSCSI target 192.168.36.101:3260
Multipathing With iSCSI

- SendTargets advertises multiple routes
  - It reports different IP addresses to allow different paths to the iSCSI LUNs
- Routing done via IP network
- For the software initiator
  - Counts as one network interface
  - NIC teaming and multiple SPs allow for multiple paths
- Currently supported via mrupolicy only
ESX Server 3 provides full support for software initiators

**Software Initiator**

- VMkernel
- iSCSI initiator
- TCP/IP
- NIC driver
- NIC e.g. Broadcom 5700

**Hardware Initiator**

- VMkernel
- iSCSI HBA driver
- iSCSI initiator
- TCP/IP (TCP Offload Engine)

VMWORLD 2006
Both Service Console and VMkernel need to access the iSCSI storage (software initiator uses `vmkiscsid`, a daemon that runs in the service console)

Two ways to do this:

1. Have Service Console port and VMkernel port share a virtual switch and be in the same subnet

2. Have routing in place so both the Service Console port and VMkernel port can access the storage
Enable the Software iSCSI Client

Remote Access

By default, remote clients are prevented from accessing services on this host, and local clients are prevented from accessing services on remote hosts.

To provide access to a service or client, check the corresponding box. Unless configured otherwise, daemons will start automatically when any of their ports are opened and stop when all of their ports are closed.
# Configure the iSCSI Software Adapter

## Storage Adapters

<table>
<thead>
<tr>
<th>Device</th>
<th>Type</th>
<th>SAN Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Array 6i</td>
<td>Block SCSI</td>
<td></td>
</tr>
<tr>
<td>QLA2340/2340L</td>
<td>Fibre Channel SCSI</td>
<td>21:00:00:e0:8b:89:19:9c</td>
</tr>
<tr>
<td>iSCSI Software Adapter</td>
<td>iSCSI</td>
<td></td>
</tr>
</tbody>
</table>

## Details

- **Model:**
- **iSCSI Name:**
- **iSCSI Alias:**

- **IP Address:**
- **Discovery Methods:**
- **Targets:**
Enable the iSCSI initiator
Configure Software Initiator: General Properties (2)

- The iSCSI name and alias are automatically filled in after initiator is enabled.
Configure Software Initiator: Dynamic Discovery

- In the Dynamic Discovery tab, enter the IP address of each target server for initiator to establish a discovery session.
- All available targets returned by the target server show up in the Static Discovery tab.
Configure Software Initiator: CHAP Authentication

- By default, CHAP is disabled
- Enable CHAP and enter CHAP name and secret
Discover iSCSI LUNs

Rescan to find new LUNs

Storage Adapters

Device: vmhba40
Type: iSCSI
Target ID: ign.1998...

S3c1030 PCI-X Fusion MPT Dual Ultra320 SCSI

vmhba0
Parallel SCSI

Details

vmhba40
Model: iSCSI Software Adapter
iSCSI Name: ign.1998-01.com.vmware.dhiltgen-dev1
iSCSI Alias: dhiltgen-dev1
IP Address: Send Targets
Discovery Methods: Targets: 1

SCSI Target 0
iSCSI Name: ign.1992-08.com.netapp.burton
iSCSI Alias: 
Target LUNs: 5

<table>
<thead>
<tr>
<th>Path</th>
<th>Canonical Path</th>
<th>Capacity</th>
<th>LUN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmhba40:0:0</td>
<td>vmhba40:0:0</td>
<td>TBD</td>
<td>vmhba40:0:0</td>
</tr>
<tr>
<td>vmhba40:0:1</td>
<td>vmhba40:0:1</td>
<td>TBD</td>
<td>vmhba40:0:1</td>
</tr>
<tr>
<td>vmhba40:0:2</td>
<td>vmhba40:0:2</td>
<td>TBD</td>
<td>vmhba40:0:2</td>
</tr>
</tbody>
</table>

vmworld 2006
iSCSI Tips and Tricks

- Do not use software iSCSI initiators in virtual machines
- Set console OS firewall to allow iSCSI port traffic if using software initiator
- Default iqn names incompatible with some targets – use this format
  - iqnn.yyyy-mm.<domain>.<hostname>:<user defined string>
  - For example: iqnn.2006-03.esxtest.vmware.com:esx3a-0a97886a.
- Can use QLogic SANsurfer for QLA4010 setup
  - Install on COS with:
    - `sh ./iSCSI_SANsurfer_4_01_00_linux_x86.bin -i silent -D SILENT_INSTALL_SET="QMSJ_LA"
  - Start iqlremote in COS, connect from remote UI application
What is NAS and NFS?

What is NAS?
- Network-Attached Storage
- Storage shared over the network at a filesystem level

Why use NAS?
- A low-cost, moderate-performance option
- Less infrastructure investment required than with Fibre Channel

There are two key NAS protocols:
- NFS (the “Network File System”)
- SMB (Windows networking, also known as “CIFS”)

Major NAS appliances support both NFS and SMB
- Notably those from Network Appliance and EMC

Server operating systems also support both
How is NAS Used With ESX Server?

- The VMkernel only supports NFS
  - More specifically NFS version 3, carried over TCP
- NFS volumes are treated just like VMFS volumes in Fibre Channel or iSCSI storage
  - Any can hold VMs’ running virtual disks
  - Any can hold ISO images
  - Any can hold VM templates
- Virtual machines with virtual disks on NAS storage can be VMotioned, subject to the usual constraints
  - Compatible CPUs
  - All needed networks and storage must be visible at destination
NFS Components

- NAS device or a server with storage
- ESX Server with NIC mapped to virtual switch
- IP Network
- VMkernel port defined on virtual switch
- Directory to share with the ESX Server over the network
Addressing and Access Control With NFS

/etc/exports

/iso 192.168.81.0/24 (rw,no_root_squash,sync)

192.168.81.72
VMkernel port configured with IP address
Before You Begin Using NAS/NFS

- Create a VMkernel port on a virtual switch

You must define a new IP address for NAS use, different from the Service Console’s IP address
Configure an NFS Datastore

- Describe the NFS share

![Configure NFS Datastore](image)
Configure an NFS Datastore (cont.)

- Verify that the NFS datastore has been added

<table>
<thead>
<tr>
<th>Storage</th>
<th>Device</th>
<th>Capacity</th>
<th>Free</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFS01</td>
<td>192.168.56.131:/...</td>
<td>7.10 GB</td>
<td>5.02 GB</td>
<td>nfs</td>
</tr>
<tr>
<td>storage1</td>
<td>vmhba0:0:0:0:3</td>
<td>60.25 GB</td>
<td>59.64 GB</td>
<td>vmfs3</td>
</tr>
<tr>
<td>SharedVMs</td>
<td>vmhba1:0:25:1</td>
<td>99.75 GB</td>
<td>99.14 GB</td>
<td>vmfs3</td>
</tr>
</tbody>
</table>

**Details**

- **NFS01**
  - Server: 192.168.56.131
  - Folder: /iso

- Capacity: 7.10 GB
  - Used: 2.08 GB
  - Free: 5.02 GB

VMWORLD 2006
Questions
Some or all of the features in this document may be representative of feature areas under development. Feature commitments must not be included in contracts, purchase orders, or sales agreements of any kind. Technical feasibility and market demand will affect final delivery.