Networking Virtual Machines

Jon Hall Technical Trainer



Agenda

- Introduction
- New networking features
- Networking virtual machines
 - > Virtual Switch Connections
 - > Port Group Policies
- Networking IP Storage
 - > iSCSI
 - > NAS

A networking Scenario



A Networking Scenario



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

vSwitch – Multiple Physical Adapters (NIC Team)

- 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



Connections



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



Connection Type: VMkernel Port



Connection Type: Virtual Machine Port Group



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

| Connection Type Networking hardware | can be partitioned to accommodate each service requiring connectivity. | |
|--|--|--|
| Connection Type Network Access Connection Settings Summary | Connection Types Virtual Machine Add a labeled network to handle virtual machine network traffic. VMkernel | |

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#

| þ | - Virtual Machine Port Group VM Network | Physical Adapters |
|-------|--|--|
| þ | -Service Console Port Service Console vswif0 : 192.168.31.54 | <u>Q</u> + |
| irtu | al Switch: vSwitch1 | |
| þ | - Virtual Machine Port Group Production | Physical Adapters |
| 'irtu | al Switch: vSwitch2 | |
| Ģ | VMkemel Port VMotion | Physical Adapters • • • • • • • • • • • • • • • • • • • |
| | 10.1.1.4 | |

Policies



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 though the virtual switch
 - Packets are cleared (untagged) as they return to the VM
 - > Little impact on performance



Network Policy: Security

- 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

| vSwitch1 Properties | | | | |
|------------------------|-------------------------|-------------------------|---|--|
| Ports Network Adapters | | | | |
| Configuration | Summary | Port Group Properties — | | |
| vSwitch | 24 Ports | Network Label: | | |
| Production | Virtual Machine | VLAN ID: | | |
| 🛃 Production Prope | rties | | | |
| | 5 | 1 | | |
| General Security | [raffic Shaping NIC] | Teaming | | |
| | | | | |
| Promiscuous Mode: | | | | |
| MAC Address Ch | anges: 🔽 🗖 | Accept | - | |
| Forged Transmits | | Accept | - | |

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



Network Policy: Traffic Shaping (2)

P

- 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

| Switch1 Properties | | | | |
|--|--|--|------------------|--|
| rts Network Adapters | | | | |
| Configuration vSwitch Production General Securi Configuration Configuratio Configuration Configuratio Configuration Configuratio | Summary 24 Ports Virtual Machine roperties ity Traffic Shaping tions a policy defined by the I dwidth: 1 the fill of the fill | NIC Teaming virtual switch, Co2400 | Group Properties | |
| burst bize; | ľ | .02400 | ND | |

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

| peral Security | Traffic Shaping | IC Tear | mina | | |
|---|--|---------|-------------------------|-------------------|--|
| Deline December | | | | | |
| Policy Exceptions | ş ———— | | | | |
| Load Balancing: Route based on the originating virtual port ID | | | | | |
| Network Failover | Detection: | ◄ | Link Status only | • | |
| Notify Switches: | | | Yes | ~ | |
| Rolling Failover: | | | No | v | |
| Failover Order: | | | | | |
| Cverride vSw | itch failover order: | | | | |
| Name | Speed | Netw | orks | Move Up | |
| Active Adapters | | | | | |
| Active Adapte | 35 | | | | |
| Active Adapte | 100 Full | 192.1 | 168.51.1-192.168.51.254 | Move <u>D</u> own | |
| Active Adapte vmnic1 Standby Adapt | ns 100 Full Iters | 192.1 | 168.51.1-192.168.51.254 | Move <u>D</u> own | |
| Active Adapte vmnic1 Standby Adap Unused Adapt | rs 100 Full oters ters | 192.1 | 168.51.1-192.168.51.254 | Move <u>D</u> own | |
| Active Adapte vmnic1 Standby Adap Unused Adapt | rs 100 Full oters ters | 192.1 | 168.51.1-192.168.51.254 | Move <u>D</u> own | |
| Active Adapte vmnic1 Standby Adap Unused Adapt | rs 100 Full oters :ers | 192.1 | 168.51.1-192.168.51.254 | Move <u>D</u> own | |
| Active Adapte vmnic1 Standby Adap Unused Adapt | ars 100 Full Deters ters | 192.1 | 168.51.1-192.168.51.254 | Move <u>D</u> own | |
| Active Adapte vmnic1 Standby Adap Unused Adapt | ars 100 Full beers ters | 192.1 | 168.51.1-192.168.51.254 | Move <u>D</u> own | |
| Active Adapte vmnic1 Standby Adap Unused Adapt — Adapter Details No adapter se | ars 100 Full pters ters | 192.1 | 168.51.1-192.168.51.254 | Move <u>D</u> own | |
| Active Adapte vmnic1 Standby Adap Unused Adapt Unused Adapte Adapter Details No adapter se Driver: | ars 100 Full b ters t ers | 192.1 | 168.51.1-192.168.51.254 | Move <u>D</u> own | |

Load Balancing: vSwitch Port-based (Default)



Load Balancing: Source MAC-based



Load Balancing Method: IP-based



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



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





* Software implementation

Addressing in an iSCSI SAN



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.



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 mru policy only



iSCSI Software and Hardware Initiator

ESX Server 3 provides full support for software initiators

Software Initiator



Hardware Initiator



Set Up Networking For iSCSI Software Initiator

- 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

Security Profile

Firewall

Incoming Connections SSH Server Firewall Properties - 🗆 🛛 CIM Server CIM Secure Serv **Remote Access** EMC AAM Client By default, remote clients are prevented from accessing services on this host, and local clients are prevented from CIM SLP. accessing services on remote hosts. Outgoing Connectid To provide access to a service or client, check the corresponding box. Unless configured otherwise, daemons will VMware License start automatically when any of their ports are opened and stop when all of their ports are closed. VMware Virtuald Telnet Client Label Incoming Ports Outgoing Ports Protocols Daemon 🔺 EMC AAM Client P CIM Secure Server TCP 5989 N/A CIM SLP ~ VMware License Client 27000,27010 TCP N/A Symantec Backup Exec Agent 10000-10200 TCP N/A Virtual Machine I Software iSCSI Client 3260 TCP. N/A Read and write to Symantec NetBackup Agent 13732,13783,1372... TCP N/A FTP Client TCP 21 N/A User Name: ~ EMC AAM Client 2050-5000,8042-8... 2050-5000,8042-8045 TCP, UDP N/A $\mathbf{\nabla}$ Telnet Client 23 TCP N/A FTP Server 21 TCP N/A П NIS Client 111,0-65535 UDP, TCP N/A NTP Client 123 UDP Stopped • • OK. Cancel Help

Configure the iSCSI Software Adapter

iSCSI Alias:

| Storage Adapters | | | | Rescan |
|------------------------|--------------------|-------------------------|--------------------|------------|
| Device | Туре | SAN Identifier | | |
| Smart Array 6i | | | | |
| vmhba1 | Block SCSI | | | |
| QLA2340/2340L | | | | |
| vmhba0 | Fibre Channel SCSI | 21:00:00:e0:8b:89:19:9c | | |
| iSCSI Software Adapter | | | | |
| iSCSI Software Adapter | iSCSI | | | |
| | | | _ | |
| Details | | | | |
| | | | | Properties |
| Model: | | | IP Address: | |
| iSCSI Name: | | | Discovery Methods: | |

VMWORLD 2006

Targets:

Configure Software Initiator: General Properties

Enable the iSCSI initiator

| iSCSI Initiator (vmhba40) Properties |
|--|
| General Dynamic Discovery Static Discovery CHAP Authentication |
| iSCSI Properties |
| iSCSI name: |
| iSCSI alias: |
| Target discovery methods: |
| Software Initiator Properties |
| Status: Disabled |
| Configure |
| General Properties |
| Status Enabled |
| iSCSI Properties iSCSI Name: |
| iSCSI Alias: |
| OK Cancel Help |
| Close Help |

Configure Software Initiator: General Properties (2)

The iSCSI name and alias are automatically filled in after initiator is enabled

| 8 | 🛃 iSCSI Initiator (vmhba40) Properties 📃 🗖 🔀 | | | | | |
|---|--|--|--|--|--|--|
| | General Dynamic Discovery Sta | atic Discovery CHAP Authentication | | | | |
| | -iSCSI Properties | | | | | |
| | iSCSI name: | iqn.1998-01.com.vmware:nitrogen01-5663a5e2 | | | | |
| | iSCSI alias: nitrogen01.priv.vmeduc.com | | | | | |
| | Target discovery methods: | Send Targets | | | | |
| | Software Initiator Properties – | | | | | |
| | Status: | Enabled | | | | |
| | | Configure | | | | |

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

| 🖡 iSCSI Initiator (vmhba40) Properties 📃 🗖 🗙 |
|--|
| General Dynamic Discovery Static Discovery CHAP Authentication |
| Send Targets Obtain information about target devices directly from the following iSCSI servers using the SendTargets commmand. |
| iSCSI Server Status |
| |
| Add Send Targets Server |
| Send Targets iSCSI Server: 192 . 168 . 102 . 241 Port: 3260 |
| Authentication may need to be configured before a session can be established with any discovered targets. |
| OK Cancel Help |
| |
| Add Edit Remove |
| Close Help |

Configure Software Initiator: CHAP Authentication

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

| 🛃 iSCSI Initiato | or (vmhba40) Prope | rties | | | |
|------------------|---|---|-------------|------|--|
| General Dyna | mic Discovery Static D | Discovery CHAP Auther | ntication | | |
| CHAP Authe | ntication | | | | |
| By default, us | e the following credenti | ials for all iSCSI targets: | | | |
| CHAP Name | e: Not speci | ified | Configure | | |
| @ 0 | HAP Authentication | | | | |
| [| Credentials Use the following CH All ISCSI targets are credentials unless of | IAP credentials authenticated using the therwise specified. | ese | | |
| | CHAP Name: 🔽 Use initiator name | | | | |
| | CHAP Secret: | iqn.1998-01.com.vmv 1tsasecr3t | ware:nitrog | | |
| | O Disable CHAP auther | ntication | | | |
| | | OK Cancel | Help | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | Close | Help | |

Discover iSCSI LUNs

Rescan to find new LUNs

| dhiltgen-dev1 VMware Host Agent, e.x | | nce Configuration Users & Groups | Sustem Logs Events | Permission | |
|--------------------------------------|------------------|--------------------------------------|--------------------|-------------|------------|
| Hardware | Storage Adapter | 5 | | | Rescan |
| Storage (SCSI, SAN, and NFS) | Device | | Туре | Target ID | |
| Networking | iSCSI Software / | Adapter | | | |
| Processors | 🎯 vmhba40 | | iSCSI | iqn.1998 | |
| Memory | 53c1030 PCI-X F | usion°MPT Dual Ultra320 SCSI | D Ulacat | | |
| Storage Adapters | Vmhbau | | Parallel SCSI | | |
| Network Adapters | | | | | |
| | | | | | |
| Software | , Details | | | | |
| Licensed Features | vmhba40 | | | | Properties |
| DNS and Routing | Model: | iSCSI Software Adapter | IP Address: | | |
| Virtual Machine Startup/Shutdown | iSCSI Name: | iqn.1998-01.com.vmware.dhiltgen-dev1 | Discovery Method | ls: Send Ta | argets |
| SNMP Agents | ISUSI Alias: | dhiltgen-dev i | l argets: | I | |
| Security Profile | SCSI Target 0 | | | | - |
| Service Console Resources | ISCSI Name: | ign.1992-08.com.netapp:burton | | | |
| Advanced Settings | Target LUNs: | 5 | | F | lide LUNs |
| | Path | Caponical Path Cor | | | |
| | vmbba40:0:0 | vmbba40:0:0 | | | |
| | vmbba40:0:1 | vmhba40:0:1 | TBD_vmbba40:0:1 | | |
| | vmhba40:0:2 | vmhba40:0:2 | TBD_vmhba40:0:2 | | _ |
| | | | | | |

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
 - iqn.yyyy-mm.<domain>.<hostname>:<user defined string>
 - For example: iqn.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

| Internet Service Properties | | | | |
|---|-----------------|-------------|--|--|
| Internet Services | | | | |
| Enable the following services and open their respective | firewall ports: | | | |
| Client | Port Range | Protocols 🔺 | | |
| SSH client | 22 | tcp | | |
| NTP client | 123 | udp | | |
| SSH server | 22 | tep | | |
| 🕑 Software iSCSI Client | 3260 | tcp 🏹 | | |
| FTP server | 21 | tep | | |
| ✓ VirtualCenter Heartbeat | 902 | udp | | |
| VNC server | 5900 | ten 💌 | | |
| | | | | |
| Ok | Cancel | Help | | |

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





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

🗿 Add Storage

Locate Network File System

Which shared folder will be used as a VMware datastore?

| NAS Network File System Ready to Complete | Properties Server: 192.168.56.131 Examples: nas, nas.it.com or 192.168.0.1 Folder /iso Example: /vols/vol0/datastore-001 Mount NES read only |
|---|--|
| | Datastore Name |



_ 0

Configure an NFS Datastore (cont.)

Verify that the NFS datastore has been added

Storage

| Ide | ntification | Device | Capacity | Free Type |
|-----|-------------|------------------|----------|----------------|
| 8 | NFS01 | 192.168.56.131:/ | 7.10 GB | 5.02 GB nfs |
| | storage1 | vmhba0:0:0:3 | 60.25 GB | 59.64 GB vmfs3 |
| | SharedVMs | vmhba1:0:25:1 | 99.75 GB | 99.14 GB vmfs3 |

Details

| NFS01 | | 7.10 GB Capacity |
|---------|----------------|------------------|
| Server: | 192.168.56.131 | 2.08 GB 🔲 Used |
| Folder: | /iso | 5.02 GB 🔲 Free |



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.

