Teil 2 – Virtuelle Netzwerke im Überblick

Motto von Teil 2:
Gäste flexibel im LAN oder in abgeschotteten Testumgebungen betreiben.

Teil 2 dieser Workshopserie erklärt die Grundlagen virtueller Netzwerke und zeigt die notwendigen Einstellungen, um Gäste ins LAN zu bringen oder isolierte Testumgebungen aufzubauen.

Ziele auf einen Blick:
Vermittlung der Grundlagen virtueller Netzwerke zur praktischen Anwendung:

- Virtuelle Switches und Portgruppen.
- Virtuelle Netzwerkarten in den Gästen.
- Physische Adapter und Uplinks zum LAN.

Hinweis: Weiterführende und ergänzende Dokumentationen enthält das Dokument *VMware Virtual Networking Concepts* und der *ESX Server 3 Configuration Guide* auf den VMware Webseiten:
http://www.vmware.com/support/pubs/vi_pages/vi_pubs_35.html
http://www.vmware.com/files/pdf/virtual_networking_concepts.pdf

Grundlagen und Zusammenhänge virtueller Netzwerkkomponenten auf einen Blick

Die Konfiguration virtueller Netzwerke ist sehr flexibel und reicht vom einfachen Anschluss einer VM ans LAN bis zu komplexen internen virtuellen Netzwerken mit Routern und VLANs.

Virtuelle Netzwerke bestehen aus ähnlichen Komponenten wie Netzwerke in der physischen Welt. Folgende Übersicht verdeutlicht die Prinzipien und Komponenten auf einen Blick:

- ***Virtuelle Switches*** - Virtuelle Switches (vSwitch) bilden das Rückrat der Netzwerkfunktionen auf dem Host. Ein vSwitch funktioniert genau wie ein physischer Layer-2-Switch und verbindet angeschlossene Gäste untereinander, unabhängig vom verwendeten Netzwerkprotokoll der Gäste.

  Virtuelle Switches existieren nur als Software auf einem Host. Verschiedene vSwitches eines Hosts sind untereinander isoliert und bilden getrennte Netzwerke (Broadcast-Domänen).

- ***Ports und Portgruppen*** – ESX Server untergliedert die vSwitches in Portgruppen. Ähnlich wie bei einem physischen Switch lassen sich Portgruppe mit verschiedenen Eigenschaften konfigurieren, etwa mit VLAN IDs oder mit Regeln zur Begrenzungen der Bandbreite.

  Gäste werden immer an Portgruppen angeschlossen, um Kontakt zum vSwitch zu bekommen. Verschiedene Host-Funktionen, etwa die Service

Console, verfügen ebenfalls über Ports an vSwitches.

- ***Virtuelle Netzwerkadapter*** - Eine virtuelle Maschinen kann bis zu vier virtuelle Netzwerkadapter verwenden. Für das Gastsystem erscheinen diese emulierten Adapter wie echte Hardware. Die virtuellen Adapter der Gäste sind an die Portgruppen der virtuellen Switches angeschlossen. Die physischen Adapter des Hosts sind für die Gastsysteme nicht sichtbar.

- ***Isolierte Netzwerke*** - Grundsätzlich erfolgt die Kommunikation der Gäste nur untereinander am gleichen vSwitch. Netzwerkverkehr gelangt weder zu anderen vSwitches am gleichen Host, noch nach draußen ins physische LAN. Unterschiedliche Portgruppen am gleichen vSwitch sind nicht untereinander isoliert, können aber bei Bedarf mittels VLANs getrennt werden.

- ***Uplink ins LAN*** - Jedem vSwitch kann man eine oder mehrere physische Adapter des Hosts zuweisen. Zugewiesene physischen Adapter bilden einen Uplink zu einem physischen Switch und damit eine Brücke ins LAN. Der vSwitch ist nicht mehr isoliert, sondern direkt mit dem physischen Switch verbunden. VMs und physische Rechner können darüber Netzwerkverkehr austauschen.

- ***Router und Firewalls*** – Unterschiedliche vSwitches eines Hosts können intern nur über Router-VMs verbunden werden, da keine Uplink-Funktion zwischen vSwitches existiert. Router-VMs als Firewall schützen sensible virtuelle Maschinen, isolieren Abteilungen voneinander oder bilden eine DMZ. Eine Router-VM benötigt mindestens zwei virtuelle Netzwerkadapter an zwei unterschiedlichen vSwitches. Als Router können beispielsweise Linux-Distributionen oder Microsoft ISA Server im Gast dienen.

- ***Unabhängige Identität der Gäste*** - Jeder Gast hat seine eigene MAC- und IP-Adresse und tritt in den internen Netzwerken des Hosts und auch im LAN als eigenständige Einheit auf. Die MAC-Adressen der physischen Adapter des Hosts treten bei dieser Kommunikation nicht in Erscheinung. ESX Server vergibt jedem Gast automatische ein eindeutige MAC-Adresse beim ersten Start der VM.

- ***Kernel Dienste und Service Cosole*** – Die Service Console des ESX Servers und Dienste des VMkernels, etwa VMotion, iSCSI-Initiator oder NAS-Anbindung, sind ebenfalls über eigene Ports an virtuelle Switches angeschlossen. Damit kommunizieren diese Dienste auf dem gleichen Weg wie die Gäste. Service Console und Kernel Dienste haben eigene IP-Konfigurationen.

  Hinweis: Kernel Dienste und Service Console sollten aus Sicherheits- und Leistungsgründen möglichst andere vSwitches (und damit separate physische Adapter) verwenden, als die Gäste. In der Service Console laufen sicherheitsrelevante Agenten für die Kommunikation mit dem VI Client und Virtual Center und Dienste wie Webserver, SSH oder Zeitsynchronisation.

- ***Redundanz*** - Einem vSwitch können mehrere physische Adapter zugewiesen werden. Fällt einer aus, läuft die Kommunikation über den anderen Adapter weiter. Für die Gäste ist dieses Failover transparent. Idealerweise sind redundante Adapter an unterschiedlichen physischen Switches angeschlossen. Für die einzelnen virtuellen Maschinen genügt dadurch jeweils ein einziger virtueller Adapter, für Redundanz sorgt der vSwitch.

- ***Lastausgleich*** – Für mehrere Gäste am gleichen vSwitch kann Lastausgleich über unterschiedliche physische Adapter erfolgen. Der ausgehende Methode des Lastausgleichs kann am vSwitches mittels NIC Teaming Regeln konfiguriert werden. Für eingehende Lastausgleich ist immer der physische Switch zuständig.

- ***VLANs*** – Sollten im Netzwerk VLANs nach IEEE 802.3q Verwendung finden, kann die Verwaltung vom physischen Switch auf den virtuellen Switch verlagert werden. Dazu muss am physischen Switch ein Trunk-Port den Verkehr aller benötigten VLANs zusammenfassen. Dieser gesammelte Verkehr gelangt über einen physischen Adapter des Hosts zum vSwitch.

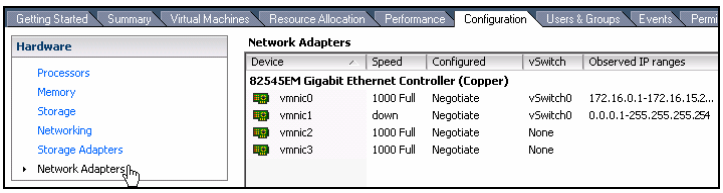
  Am vSwitch lassen sich einzelnen Portgruppen unterschiedliche VLAN-IDs zuweisen. ESX Server verteilt den Netzwerkverkehr anhand dieser IDs an die richtigen Portgruppen und damit an die angeschlossenen VMs. Die VLANs bleiben weiterhin isoliert.

  Die Verwaltung der VLANs am virtuellen Switch spart Netzwerkadapter im Host und macht die VLAN-Verwaltung sehr flexibel und unabhängig vom physischen Switch.

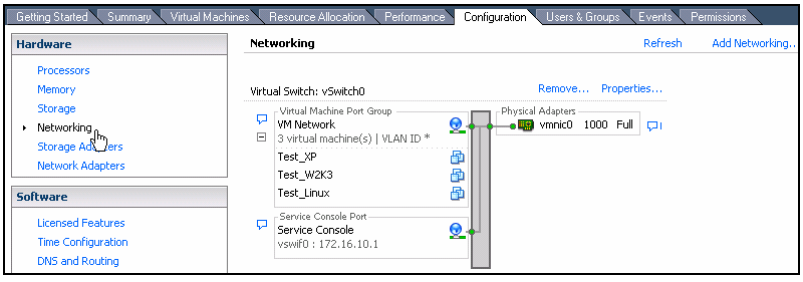
Konfiguration der virtuellen Netzwerke im VI Client

Unter folgenden Menüpunkten im VI Client finden sich alle relevanten Netzwerk-Einstellungen:

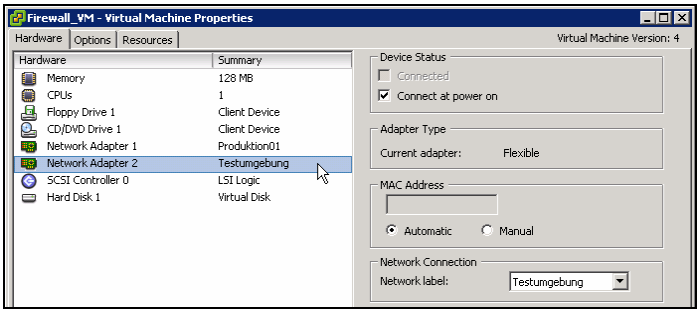
- ***Host > Configuration > Network Adapter*** – Hier sind alle erkannten physischen Netzwerkadapter des Hosts mit ihrem Verbindungsstatus aufgelistet. Einstellungen sind an dieser Stelle nicht möglich.



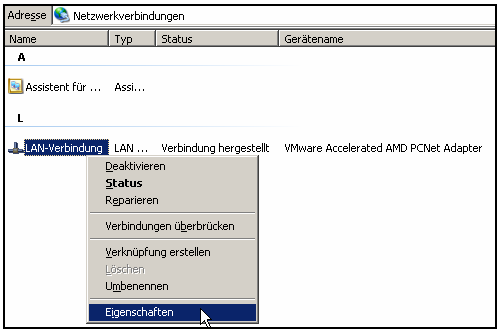
- ***Host > Configuration > Networking*** – Das ist die zentrale Stelle zur Konfiguration von vSwitches, Portgruppen und Uplinks. Die Konfiguration der vSwitches ist der Dreh- und Angelpunkt der Netzwerkkonfiguration.



- ***VM > Edit Settings*** - In der Konfiguration jeder virtuellen Maschinen können Sie unter „Edit Settings“ für jeden virtuellen Netzwerkadapter festlegen, an welche Portgruppe eines bestimmten vSwitches er angeschlossen ist. Dadurch kommuniziert der Gast in diesem virtuellen Netzwerk. Hat der vSwitch mindestens einen Uplink-Adapter, erreicht der Gast auch das LAN.



- ***Einstellungen im Gast*** – Protokollspezifische Einstellungen wie IP-Adressen, Gateway und DNS-Konfiguration erfolgen im Gastsystem. VMware emuliert standardmäßig einen AMD PCNet Adapter, für den fast alle Betriebssysteme eigene Treiber mitbringen. Die VMware Tools ersetzen diesen Standardtreiber mit einem optimierten Treiber. Für die grundsätzlichen Konfiguration im Gast ist der Treibertyp nicht relevant.



Erstellen virtueller Switches für Testumgebung und Produktion

Mit dem Grundwissen aus diesem Schnelleinstieg können Sie auf dem Host bereits sehr flexible Netzwerke für Testumgebungen oder für die LAN-Anbindung produktiver Maschinen erstellen.

Vorhandene Grundkonfiguration nach der Installation von ESX Server

Die Installation des ESX Servers hat bereits automatisch einen virtuellen Switch vSwitch0 erstellt. Diesem ist der Netzwerkadapter zugeordnet, der während der Installation konfiguriert wurde. Es ist die erste verfügbare physische Netzwerkkarte vmnic0. Mindestens zwei Ports, bzw. Portgruppen existieren bereits an vSwitch0:

- ***VM Network*** - Über diese Portgruppe kommunizieren vorläufig alle Gäste mit dem LAN. Die angeschlossenen Gäste sind in der Übersicht zur Portgruppe dargestellt.

- ***Service Console*** - Über diesen Port kommuniziert die Service Console mit ihrem Anschluss vswif0 mit dem LAN. Darüber läuft unter anderem die Verbindung mit dem VI Client.

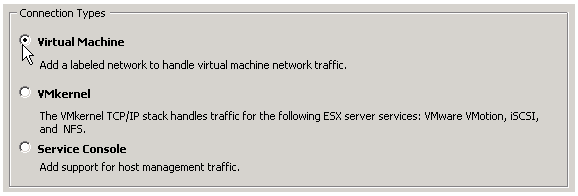
Erweiterte Konfiguration für bessere Sicherheit und Redundanz

In der Grundkonfiguration teilen sich alle Gäste und die Service Console eine einzigen LAN-Verbindung. Bei Ausfall der Netzwerkkarte oder des physischen Switchports kann keinerlei Kommunikation mehr erfolgen. Weiterhin haben alle Gäste direkten Zugang zum Verwaltungsnetzwerk der Infrastruktur am gleichen vSwitch, was aus Sicherheitsgründen nicht ideal ist.

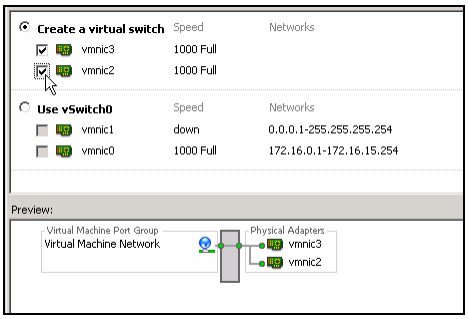
Wenige Handgriffe sorgen für Ausfallsicherheit und Redundanz und trennen gleichzeitig den Verkehr der Gäste von dem Verkehr der Service Console. Erstellen Sie dazu einen neuen vSwitch und weisen Sie ihm zwei physische Netzwerkadapter als Uplink zu.

Hinweis: In diesem Beispiel wird davon ausgegangen, dass der Host über vier Netzwerkports verfügt. Sollte der Host nur über zwei Ports verfügen, können Sie für bessere Redundanz dem vorhandenen vSwitch0 einen zusätzlichen Adapter hinzufügen oder die Adapter auf zwei Switches aufteilen. Letzteres bietet keine Ausfallsicherheit.

1) Klicken Sie auf „Add Networking“ und wählen Sie „Virtual Machine“, um eine neue Portgruppe für die Gäste zu erstellen.



2) Wählen Sie „Create a virtual Switch“ und markieren Sie zwei Netzwerkadapter, die noch nicht von einem anderen vSwitch belegt sind. Diese Adapter werden dem neuen vSwitch zugeordnet.



3) Vergeben Sie unter „Network Label“ einen Namen für die neu erstellte Portgruppe an diesem vSwitch, beispielsweise „Produktion01“. Lassen Sie das Feld „VLAN ID“ frei.

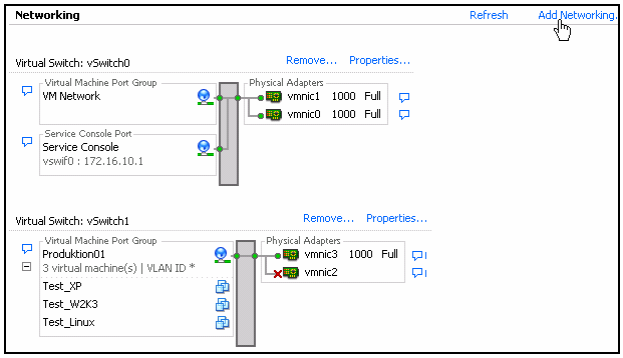
4) Über „Next“ und „Finish“ legen Sie den neuen vSwitch1 mit der Portgruppe Produktion01 an.

   Hinweis: Sie können über „Properties“ weitere Portgruppen oder weitere physische Netzwerkarten hinzufügen, bzw. Einstellungen ändern und Teaming Regeln anpassen. Ausführliche Informationen enthält der der *ESX Server 3 Configuration Guide* auf den VMware Webseiten:

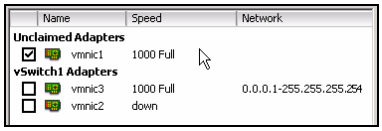
http://www.vmware.com/support/pubs/vi_pages/vi_pubs_35.html

5) Sie können jetzt die Netzwerkadapter der Gäste über die Einstellungen der VM mittels „Edit Settings > Hardware > Network Adapter“ im Feld „Network label“ mit der Portgruppe „Produktion01“ verbinden.

Der neue virtuelle Switch vSwitch1 verfügt über zwei Netzwerkadapter. Fällt ein Adapter aus, läuft die Kommunikation über den anderen weiter. Für optimale Redundanz ist es sinnvoll, die physischen Adapter mit unterschiedlichen physischen Switches zu verbinden, soweit vorhanden.



Weiterhin können Sie für vSwitch0, über den jetzt nur noch die Service Console kommuniziert, ebenfalls eine weitere physische Netzwerkkarte hinzufügen, um für Ausfallsicherheit der Host-Kommunikation zu sorgen. Wählen Sie dazu an vSwitch0 „Properties“ und dort im Reiter „Network Adapter“ mit der Schaltfläche „Add“ eine vmnic aus dem Bereich „Unclaimed Adapters“.



Hinweis: Die Portgruppe „VM Network“ an vSwitch0 kann jetzt über „Properties > Remove“ entfernt werden, da die virtuellen Maschinen nun ihren eigenen vSwitch haben. Später können zusätzliche Funktionen, etwa der Verkehr von VMotion, über vSwitch0 laufen, um die beiden physischen Adapter optimal zu nutzen. Mit Teaming Regeln lässt sich steuern, dass im Normalfall Service Console und VMotion getrennte Adapter verwenden und dass nur bei einem Ausfall beide Funktionen über den gleichen Adapter laufen.

Testnetzwerke und Routing einrichten

Für Testumgebungen sind oftmals abgeschottete Netzwerke sinnvoll, um isoliert vom produktiven LAN zu bleiben. Beispielsweise können virtuelle Abbilder der produktiven Server mit ihren originalen Namen und IP-Einstellungen im internen Netzwerk laufen, ohne das produktive LAN zu stören.

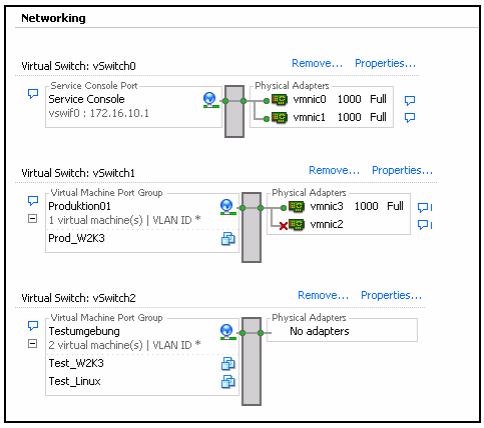
In diesem Beispiel erstellen Sie ein isoliertes virtuelles Test-Netzwerk:

1) Klicken Sie auf „Add Networking“ und wählen Sie „Virtual Machine“, um einen neuen vSwitch mit einer Portgruppe für die Testumgebung zu erstellen.

2) Wählen Sie „Create a virtual Switch“, ohne einen Netzwerkadapter auszuwählen.

3) Vergeben Sie unter „Network Label“ den Namen „Testumgebung“ für die neu erstellte Portgruppe an diesem vSwitch.

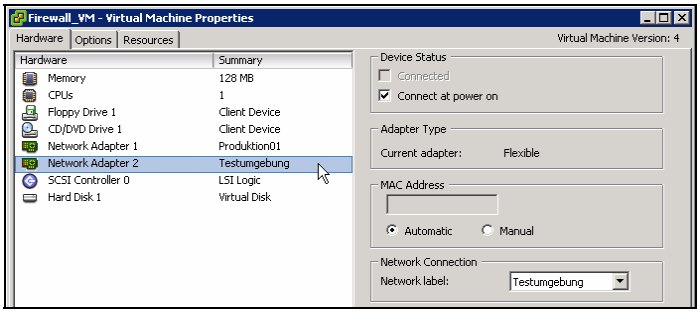
4) Über „Next“ und „Finish“ legen Sie den neuen vSwitch2 mit der Portgruppe „Testumgebung“ an.



Virtuelle Adapter von Test-VMs lassen sich jetzt an die Portgruppe „Testumgebung“ anschließen. Da der zugehörige vSwitch02 über keinen physischen Adapter verfügt, bleiben alle Gäste an vSwitch02 isoliert.

In manchen Fällen ist eine kontrollierte Verbindung der Testumgebung zum physischen LAN wünschenswert, etwa um den Internetzugang mitzunutzen. Dazu kann eine Router-VM mit Firewallfunktion dienen, die einen virtuellen Adapter an Portgruppe „Testumgebung“ und einen zweiten virtuellen Adapter an Portgruppe „Produktion01“ angeschlossen hat. Über Routing- und Firewallregeln kann die Router-VM ausgewählten Verkehr aus der Testumgebung ins LAN passieren lassen und umgekehrt.

Auf diese Weise kann auch eine virtuelle DMZ aufgebaut werden, die über eine Firewall-VM und eine dedizierte Netzwerkkarte ans Internet angebunden ist, genauso lassen sich Abteilungen sicher voneinander trennen.



Hinweis: Als virtuelle Firewall können eigene Gäste mit Lösungen wie Microsoft ISA Server oder speziellen Linux-Distributionen wie IPCop dienen. Auf den VMware Webseiten existieren im *VMware Virtual Appliance Marketplace* bereits fertig installierte VMs mit Linux-Firewalls bereit. Im VI Client könne diese VMs mittels „File > Virtual Appliance > Import“ direkt vom Internet auf den ESX Server importiert und sofort gestartet werden.
http://www.vmware.com/appliances/marketplace.html