# VDS交换机介绍

vSphere Distributed Switch 不同与ESXi标准交换机，一个VDS可以包含多个ESXi主机从而不同主机上的虚拟机可以通过VDS进行通信，迁移也不用改网络配置。VDS是一个与vSphere操作系统评级的东西。配置上VDS跟物理交换机相似，一个接口被虚拟机用了，就不能在被其他虚拟机使用。

# 创建VDS交换机

“网络”视图里面找到自己的文件夹，然后右键，选择“新建”，如图 2‑1。

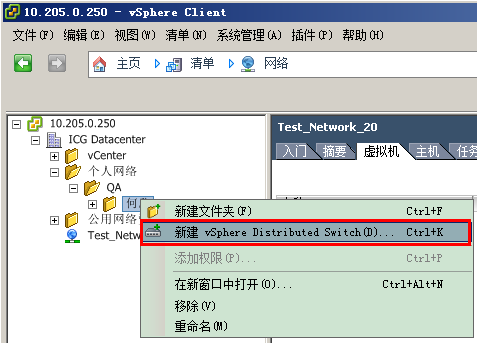


图 2‑1

图 2‑2是选择VDS版本，如果选择了6.0版本的虚拟机，则VDS不能被ESXi5.5的主机使用，下面我用6.0版本做实验。

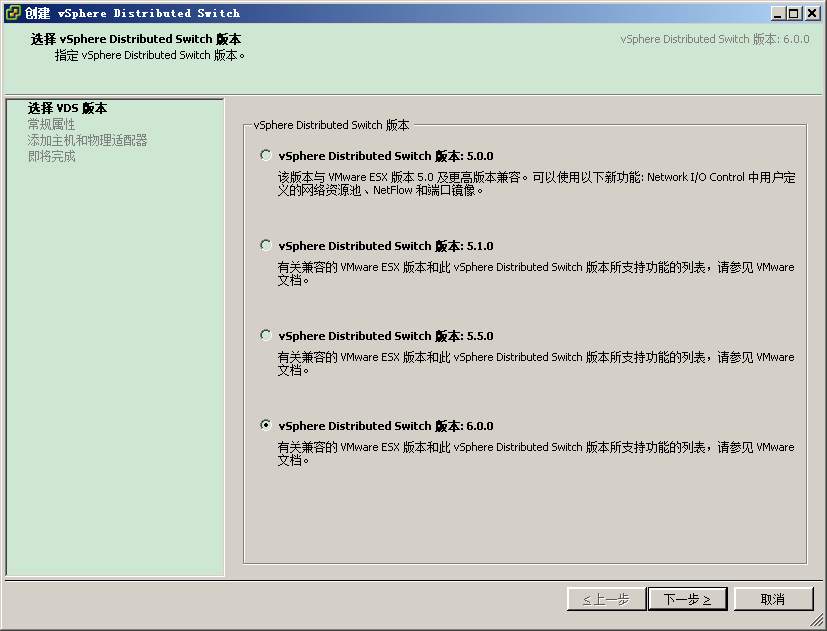


图 2‑2

图 2‑3中建议修改一下交换机名称，上行链路数是VDS可关联的物理网卡数量，我们服务器上所有的物理网卡都有其他用处，而且整个服务器只有4个网卡，不能做到每人一个物理网卡，所以这里建议选择1个，而且下一步不关联网卡。

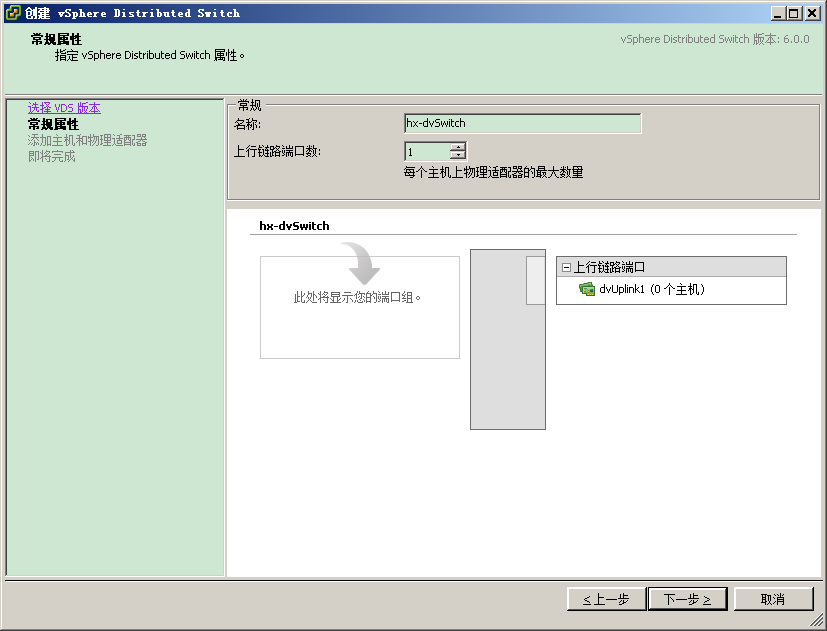


图 2‑3

图 2‑4选择VDS所关联的主机，如果不选物理网卡，不建议同时选中多个主机。而且我们服务器网卡数量紧张，不要勾选vmnicx前面的复选框。虽然不关联网卡，但是，主机前面的复选框必须选，如果不选，主机上的虚拟机会看不见这个VDS，创建这个VDS就没有意义。

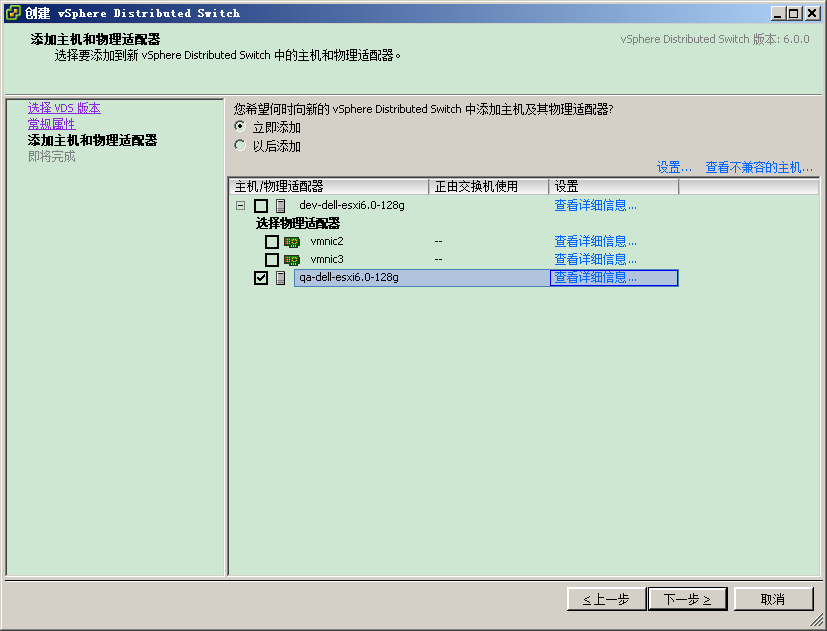


图 2‑4

由于没有选择物理网卡，会有图 2‑5提示，直接点击“是”。

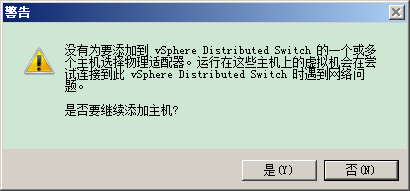


图 2‑5

图 2‑6，就创建成功了，默认端口组一般包括128个端口，可以勾选上（默认），也可以钩掉后自己创建，自己创建时候可以少选点端口，免得看着烦。这里我是不勾选的。

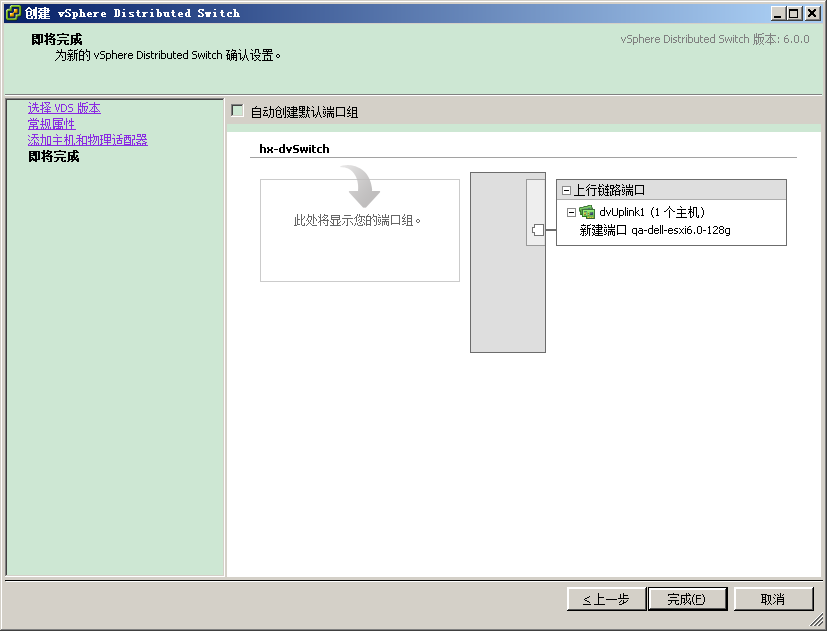


图 2‑6

# 创建端口组

由于我建立VDS时候没有创建端口组，相当与物理交换机上一个端口没有，所以我要手动创建。图 3‑1上选择“新建端口组”。

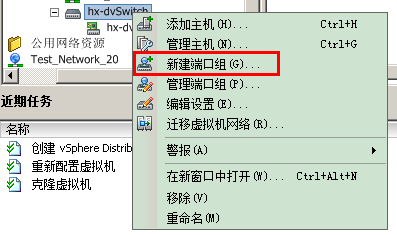


图 3‑1

端口组要自己取名，否则大家名称都一样对于ESXi管理员来说很烦。端口数量输入自己想要的。

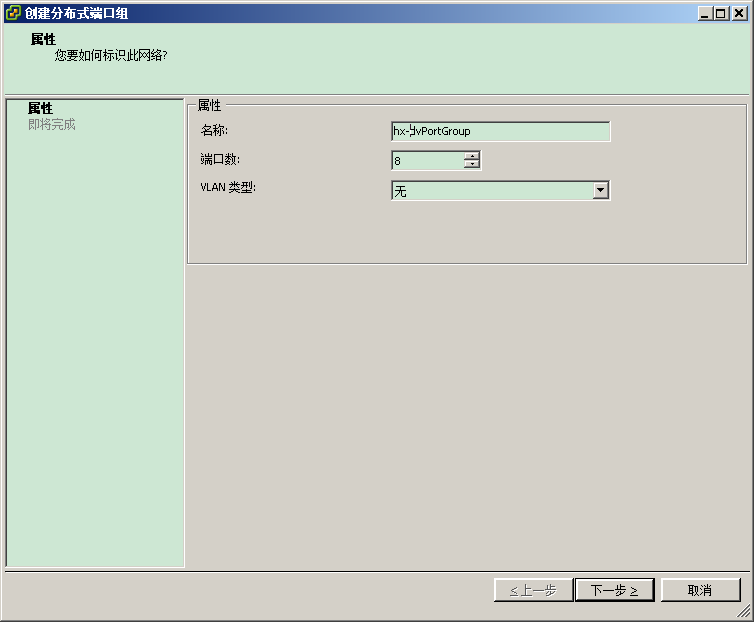


图 3‑2

建立端口组后，需要编辑替代策略，这样就可以使每个端口的策略（所属VLAN、打开关闭、流控、是否混杂）不同，用起来更方便。

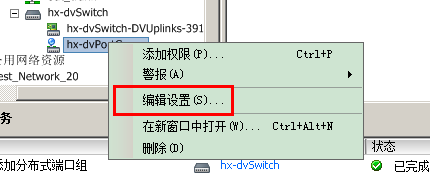


图 3‑3

图 3‑4中我把“安全策略”设置成可替代，后面就可以看到这样做的效果。

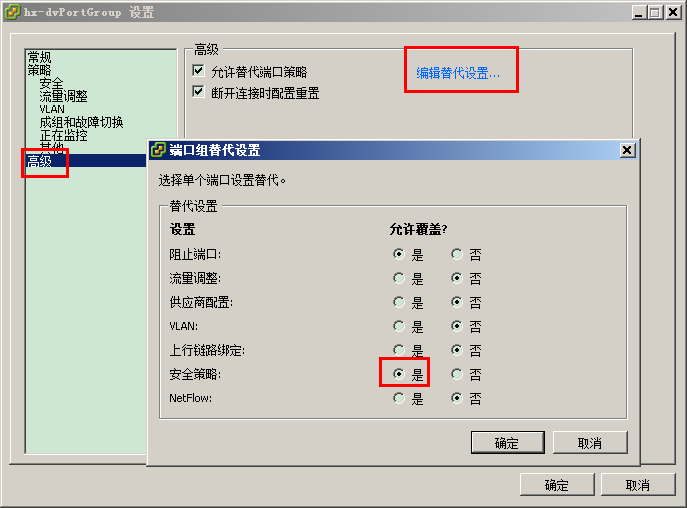


图 3‑4

# 配置镜像口

镜像口是在VDS交换机上配置的。

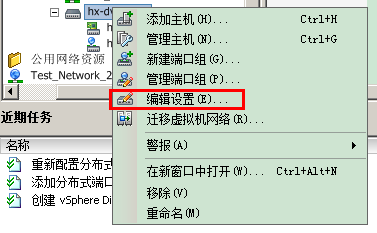


图 4‑1

中文版的Client端要下拉，才能看到添加按钮，英文版不需要下拉。

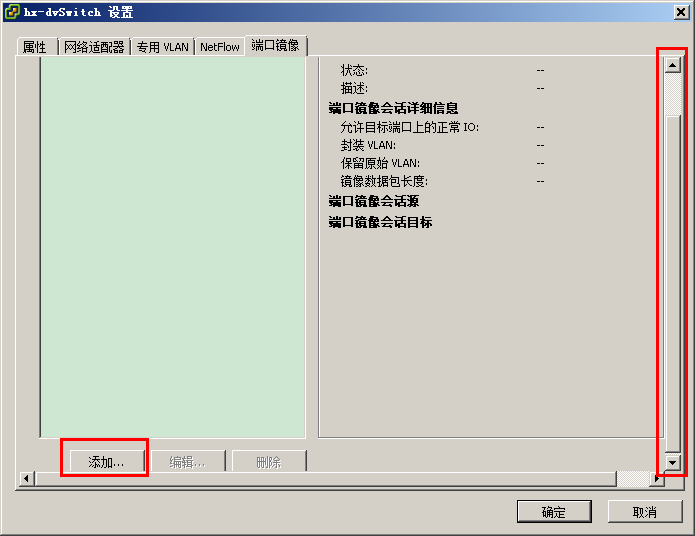


图 4‑2

图 4‑3中，自己写名称，我是把端口1的流量镜像到端口2，所以名称起的让自己明白一点没坏处。会话相信信息中，还可以设置镜像过去的流量打VLAN标签。

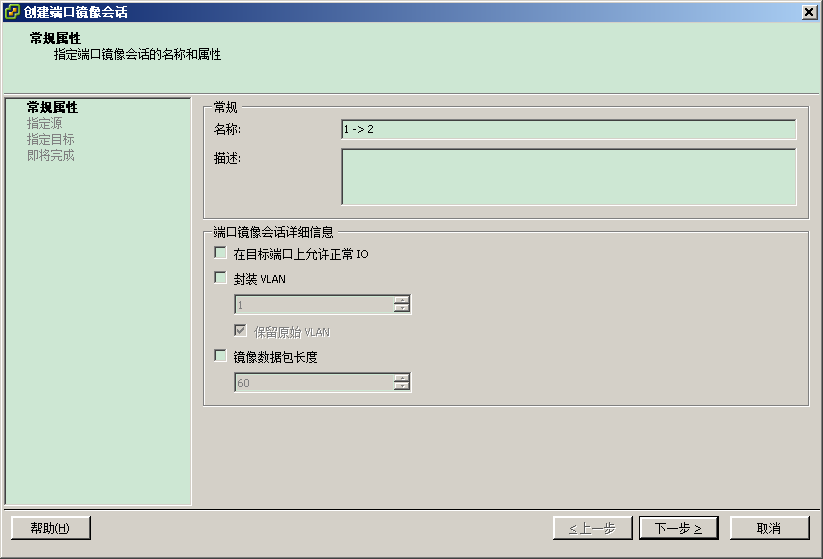


图 4‑3

第二步是选择镜像的源，源配置中可以选择输入\输出流量都镜像还是有选择的。

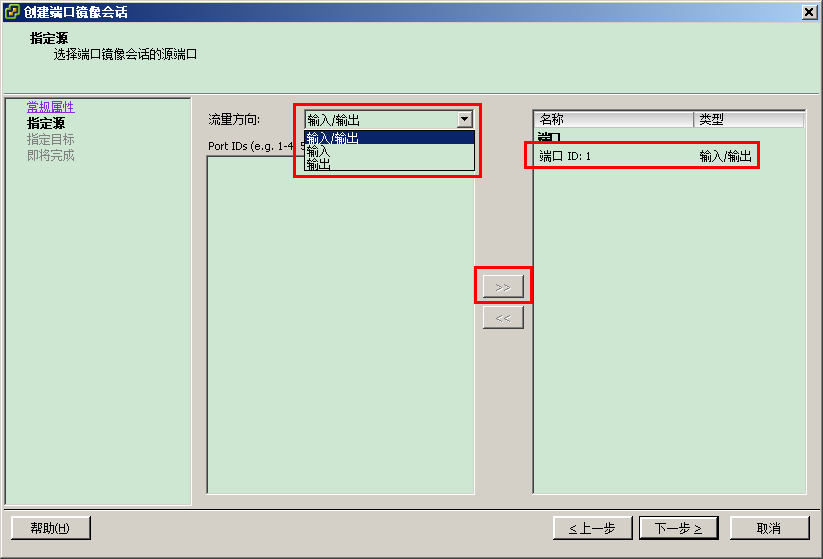


图 4‑4

配置目的端口。

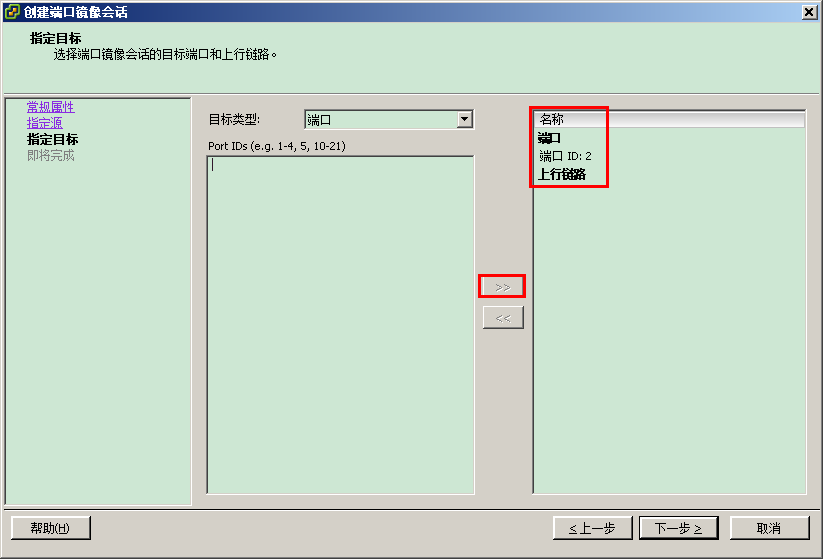


图 4‑5

图 4‑6是我们的配置摘要，选择完成后就可以了。默认镜像是不启用的，可以勾选“启用该端口镜像会话”配置后就自动开启，下面信息也说明了镜像其他参数。

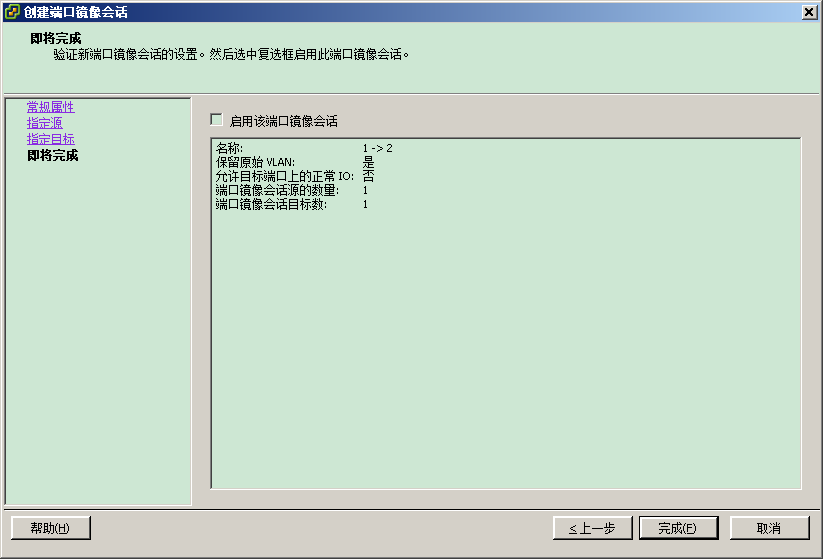


图 4‑6

如果想启用或禁止镜像，图 4‑2中选择“编辑”，默认镜像过去的是保留原始VLAN，如果选择不保留，可以先使能“封装VLAN”，吧“保留原始VLAN”的钩去掉。

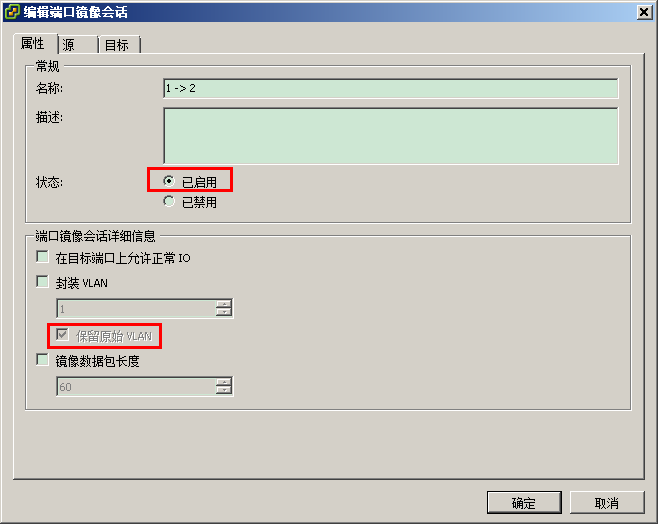


图 4‑7

这是我们创建的镜像信息。

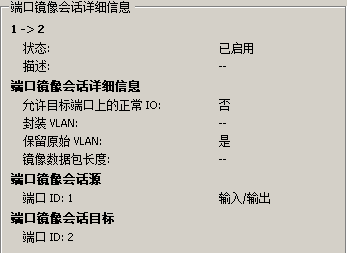


图 4‑8

最后，如果源端口要接ICG的内网口（一边测试镜像一边测试串接部署），就要把源端口设置成接受混杂，但是镜像的目的端口不能接受混杂，否则，镜像口会看到双份流量。因为混杂流量相当与广播，如果正常流量是3 -> 1的，我想把1口流量再镜像到2口，那么如果2口是混杂模式，2口不用镜像就可以收到3 -> 1的流量，再加上1镜像给2的流量，2一共能看到的就是双份。所以，一般情况，只把伪传输与MAC地址更改选成“接受”就可以了。

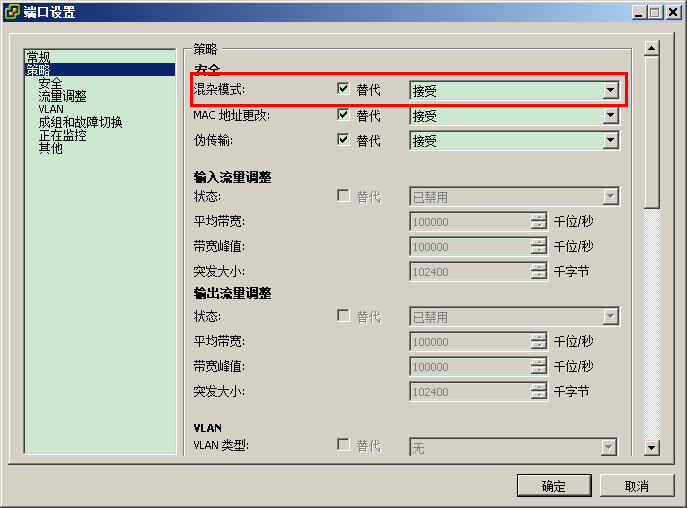


图 4‑9

# 虚拟机网卡配置

使用VDS时候，在虚拟机的配置里面，网卡又下角将多出一个选择项“切换到高级设置”（如果看不到，说明对于这个ESXi，你没有VDS权限或没有建立VDS），点击后出现图 5‑1，这样就可以选择VDS交换机和端口了。

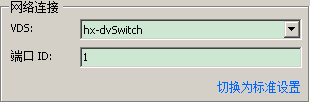


图 5‑1

# 关于安全策略的说明（重要）

**混杂**是指一台机器能够接收所有经过它的数据流，而不论其目的地址是否是他。是相对于通常模式而言的（默认情况下网卡只把发给本机的包与广播包传递给上层程序，其它的包一律丢弃），这被网络管理员使用来诊断网络问题，但是也被无认证的想偷听网络通信的人利用。

**伪传输**将影响出站通信量。此选项设置为“接受”，则意味着 ESXi 主机不会将源 MAC 地址与有效 MAC 地址进行比较。如果将此选项设置为“拒绝”，ESXi 主机会将操作系统正在传输的源 MAC 地址与其适配器的有效 MAC 地址进行比较，查看它们是否匹配。如果地址不匹配，ESXi 会丢弃此数据包。

**MAC 地址更改**会影响入站通信量。默认情况下，MAC 地址更改已设置为“接受”，这意味着 ESX 主机允许将有效 MAC 更改为除初始 MAC 地址以外的其他地址。如果将此选项设置为“拒绝”，则 ESXi 不允许将有效 MAC 地址更改为除初始 MAC 地址以外的其他地址。相反，它将禁用虚拟适配器用来发送请求的端口。因此，如果客户操作系统将有效 MAC 地址更改为与初始 MAC 地址不匹配的地址，虚拟适配器不会接收任何帧。客户操作系统无法检测到 MAC 地址的更改尚未经过授权。