

traffic monitor between VM guests ...



[dwchan](#) 595 posts since

Mar 25, 2006

If I have 2 VM guests that are reside on the same esx hosts, can you still use a sniffer to monitor the network traffic between them?

dwc



[Craig Baltzer](#) 401 posts since

Oct 3, 2005 1. **Re: traffic monitor between VM guests within the same ESX host** Nov 14, 2008 11:19 PM

Sure. Sniffer-type apps (i.e. Windows Network Monitor, tcpdump, wireshark, etc.) can be installed in a VM, and then enable promiscuous mode on the vSwitch and VM Network port group that connects the VMs. You can also use tcpdump from the service console (http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1000880 has some info on how to set it up)...



[twoodland](#) 38 posts since

Sep 15, 2008 2. **Re: traffic monitor between VM guests within the same ESX host** Nov 14, 2008 11:31 PM

👤 in response to: [Craig Baltzer](#) I don't think you will need to enable promiscuous mode (unless you care about dropped packets as well). If you use a network monitor one of on the hosts you want to monitor, that should be all that is required. You need to be careful when you enable promiscuous mode, it can be hard on cpu resources if you have a ton of traffic.



[Craig Baltzer](#) 401 posts since

Oct 3, 2005 3. **Re: traffic monitor between VM guests within the same ESX host** Nov 14, 2008 11:39 PM

👤 in response to: [twoodland](#) Yup, may not need promiscuous if you're doing the "sniffing" from one of the VMs you want to monitor. Generally I don't like installing sniffer software in one of the VMs I want to monitor to avoid a configuration change to the VM and a configuration change typically requires a change request in most organizations. Agreed that this should only be an "on when you need it, then turn it back off" kind of thing...



[twoodland](#) 38 posts since

Sep 15, 2008 4. **Re: traffic monitor between VM guests within the same ESX host** Nov 14, 2008 11:46 PM

👤 in response to: [Craig Baltzer](#) Depending upon the organization, even enabling promiscuous mode might require change management.

Another idea, assuming your switch is capable, you can bind that machine to it's own vSwitch and physical Nic, mirror the port it's plugged into (at the physical switch level) and put a sniffer on whatever is plugged into the mirrored port. If change management is a big issue in your organization, this one might be harder as it requires changes to the virtual side and the physical switch.