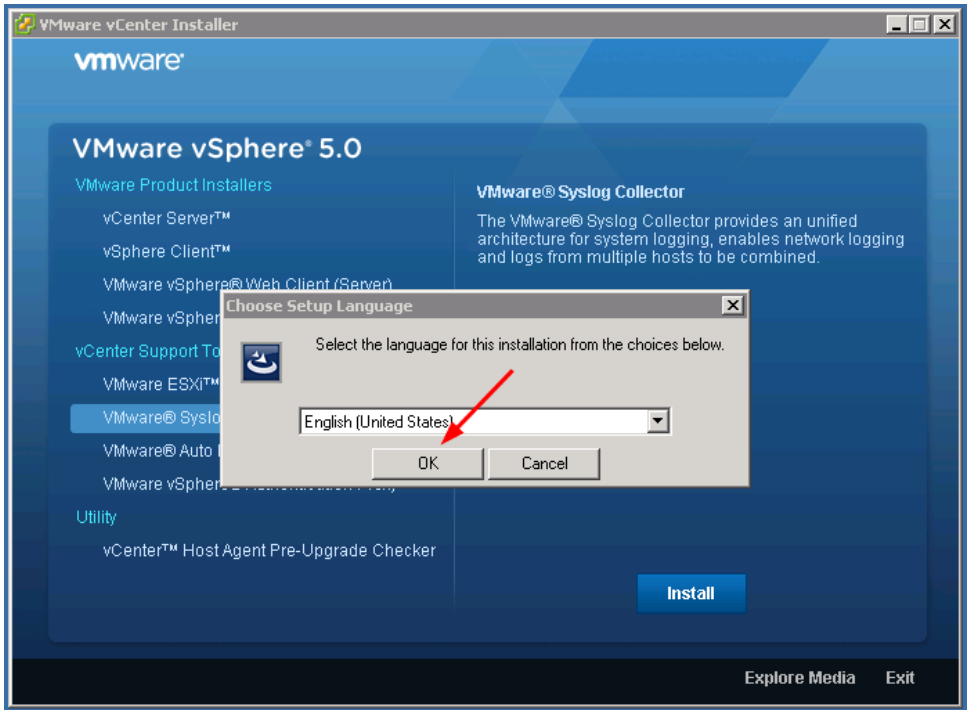
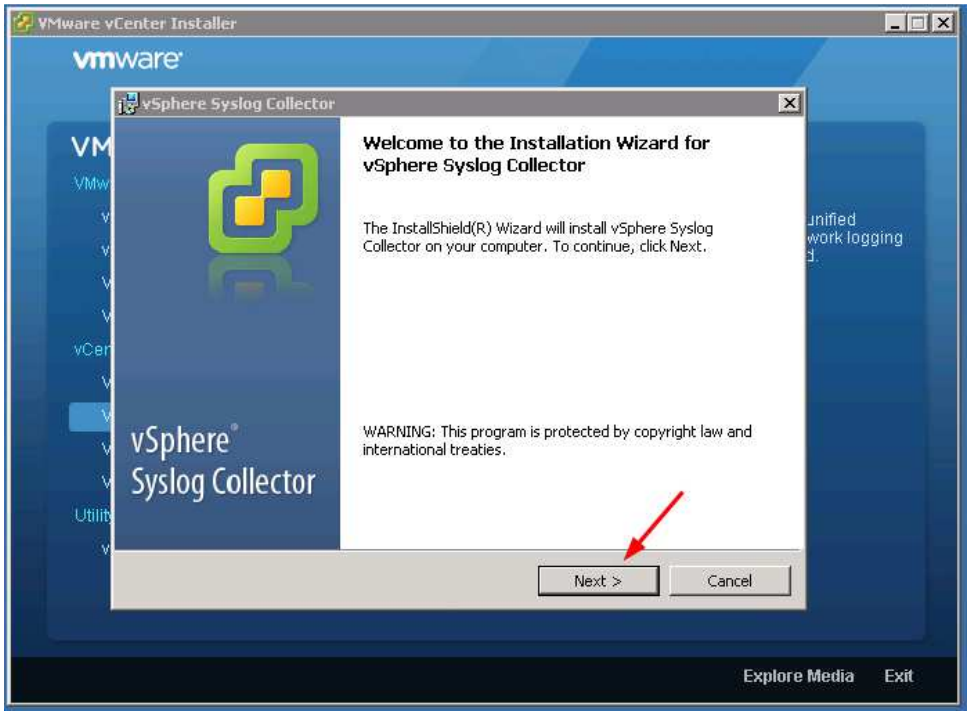
Step by Step: vCenter Syslog Collector installation

I have put together these screenshots detailing the step by step installation of vCenter Syslog Collector for VMware vSphere 5.x. I am assuming the following:

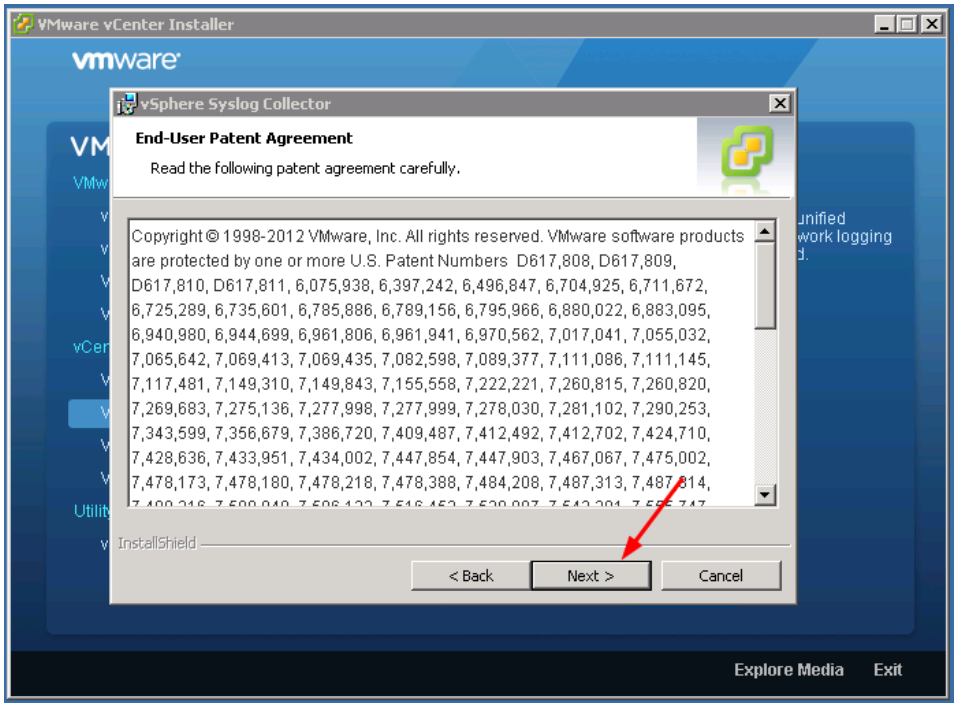
- You have already installed a SQL Server on Windows 2008 Server VM (Refer to my VM build document)
- You have already prepared the databases for vCenter and for vCenter Update Manager (Refer to my SQL Database installation document)
- You have already installed a vCenter Server VM to connect to(Refer to my vCenter Installation document)
- I am also assuming you have installed the above VM's on an ESXi 5.x Server you have already setup with shared storage (or local storage)(Refer to my ESXi 5.x Installation Document)
- I am also assuming you have met the pre-requisites for the installation such as .NET Framework etc.

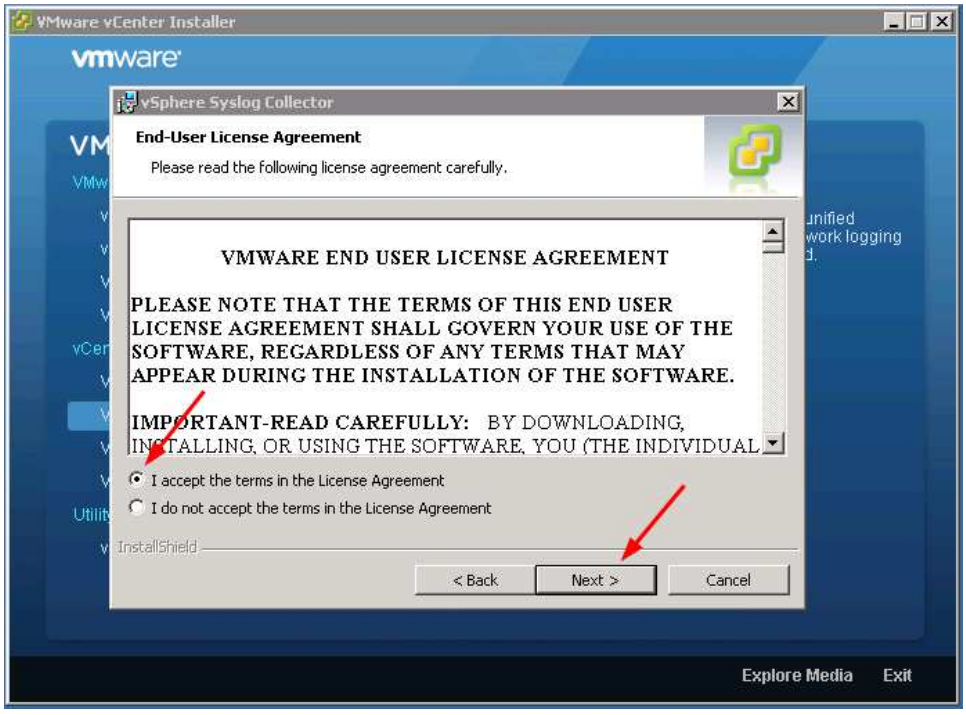
We are going to use the vSphere Installation DVD to install vCenter Syslog Collector

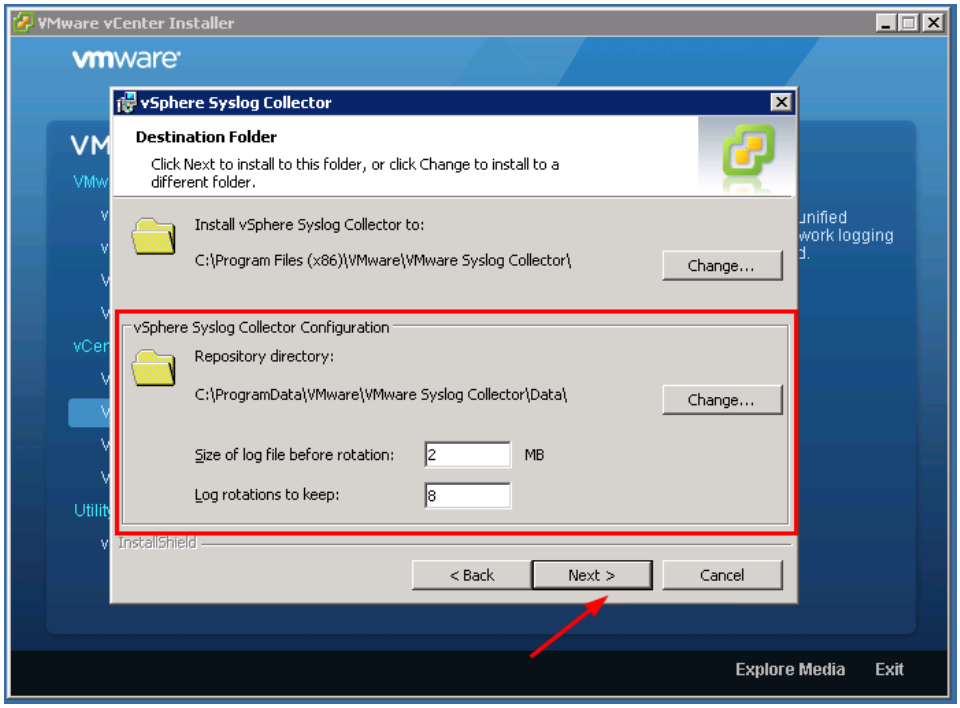




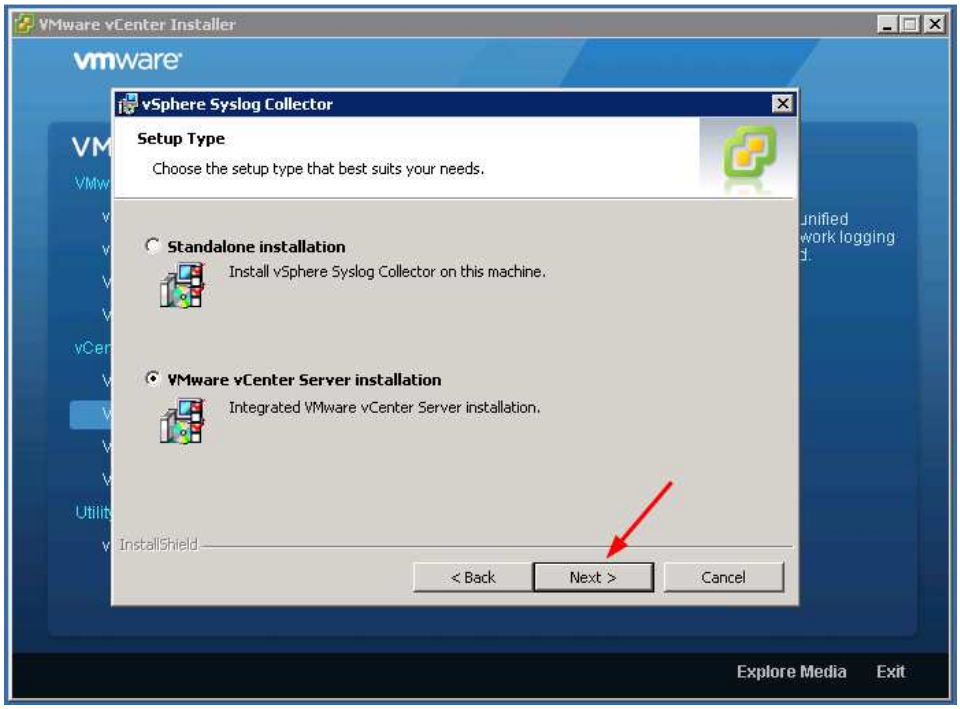
Author: Morne Smith
Doc Version: 1.0


VMware vCenter Installer
vmware
vSphere Syslog Collector
End-User Patent Agreement
Read the following patent agreement carefully.
Copyright © 1998-2012 VMware, Inc. All rights reserved. VMware software products are protected by one or more U.S. Patent Numbers D617,808, D617,809, D617,810, D617,811, 6,075,938, 6,397,242, 6,496,847, 6,704,925, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156, 6,795,966, 6,880,022, 6,883,095, 6,940,980, 6,944,699, 6,961,806, 6,961,941, 6,970,562, 7,017,041, 7,055,032, 7,065,642, 7,069,413, 7,069,435, 7,082,598, 7,089,377, 7,111,086, 7,111,145, 7,117,481, 7,149,310, 7,149,843, 7,155,558, 7,222,221, 7,260,815, 7,260,820, 7,269,683, 7,275,136, 7,277,998, 7,277,999, 7,278,030, 7,281,102, 7,290,253, 7,343,599, 7,356,679, 7,386,720, 7,409,487, 7,412,492, 7,412,702, 7,424,710, 7,428,636, 7,433,951, 7,434,002, 7,447,854, 7,447,903, 7,467,067, 7,475,002, 7,478,173, 7,478,180, 7,478,218, 7,478,388, 7,484,208, 7,487,313, 7,487,314,
InstallShield
< Back
Next >
Cancel
Explore Media
Exit


VMware vCenter Installer
vmware
vSphere Syslog Collector
End-User License Agreement
Please read the following license agreement carefully.
VMWARE END USER LICENSE AGREEMENT
PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.
IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL
I accept the terms in the License Agreement
I do not accept the terms in the License Agreement
InstallShield
< Back
Next >
Cancel
Explore Media
Exit



Here you need to make the decision on how you want your logs to be created. The more important option here is the number of Log Rotations to keep. Depending on your environment you may need to increase this number to ensure you have enough log data to reference back if you ever need to.



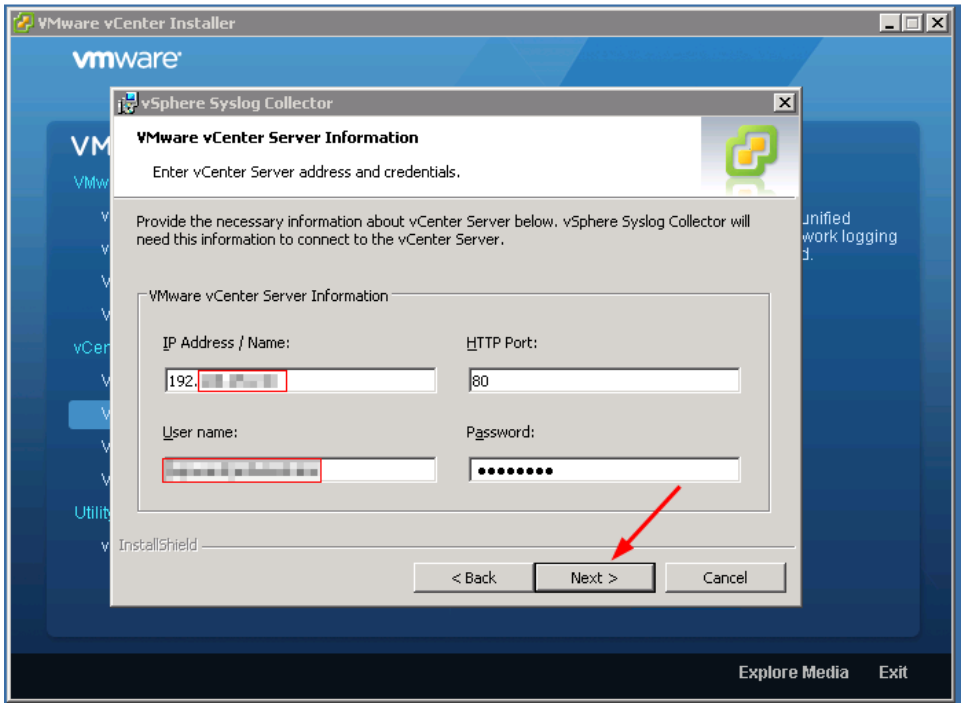
Selecting which setup you want to do is based on the size of the environment and the load on the vCenter server.

If you expect the vCenter server to carry a significant load in administration and management it might be a better option to have a separate Syslog server, thus option one for a Standalone

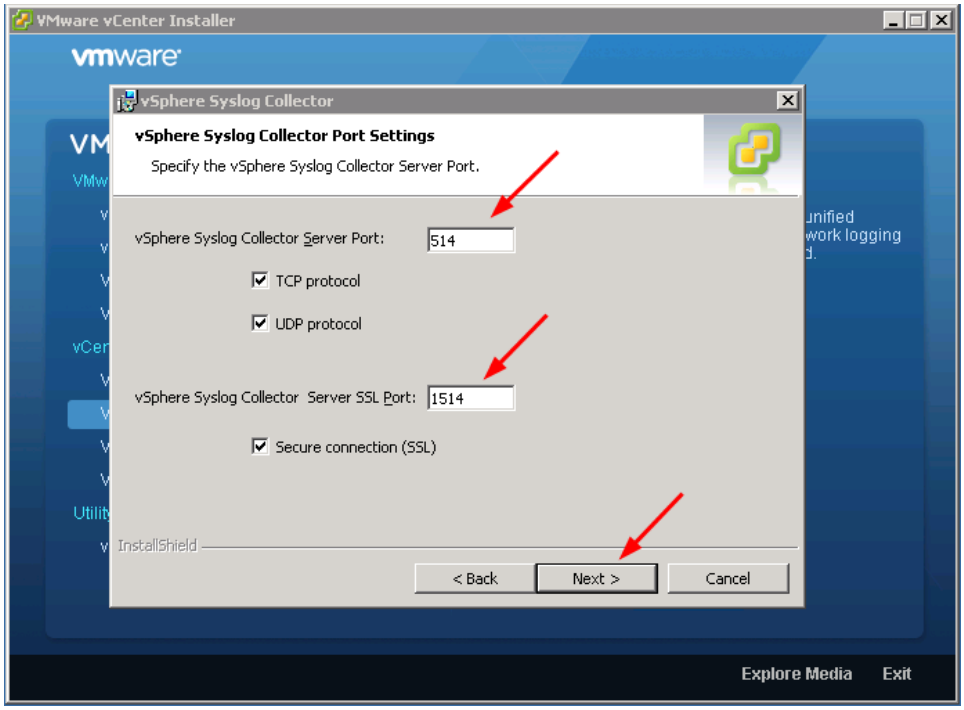
installation.

If however the environment is not that big…or the administration load on the vCenter server is not expected to be significant, you can do option two the vCenter Server installation.

NOTE: Please note that I am not taking your company policies into account with regard to Security requirements, Management requirements etc. These policies may dictate that you have separate systems for the above services; to ensure you can obtain the log files even if the vCenter Server is offline due to an outage.



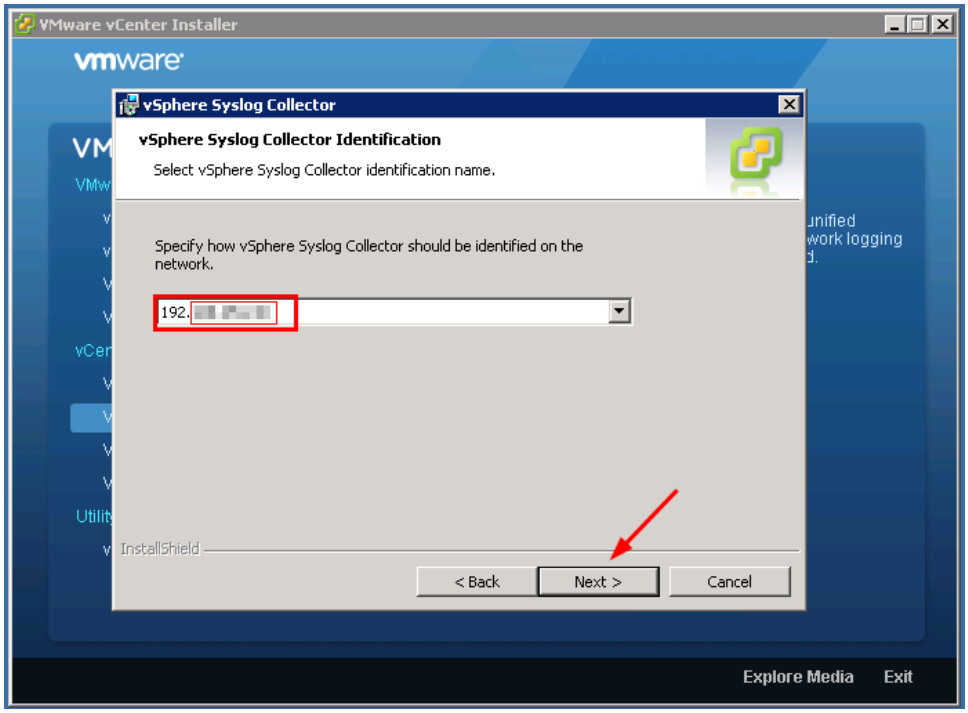
Complete the IP address of the vCenter server and user credentials that will have access to the vCenter server. The user is usually a common VMware account with administrator rights to the vCenter server.

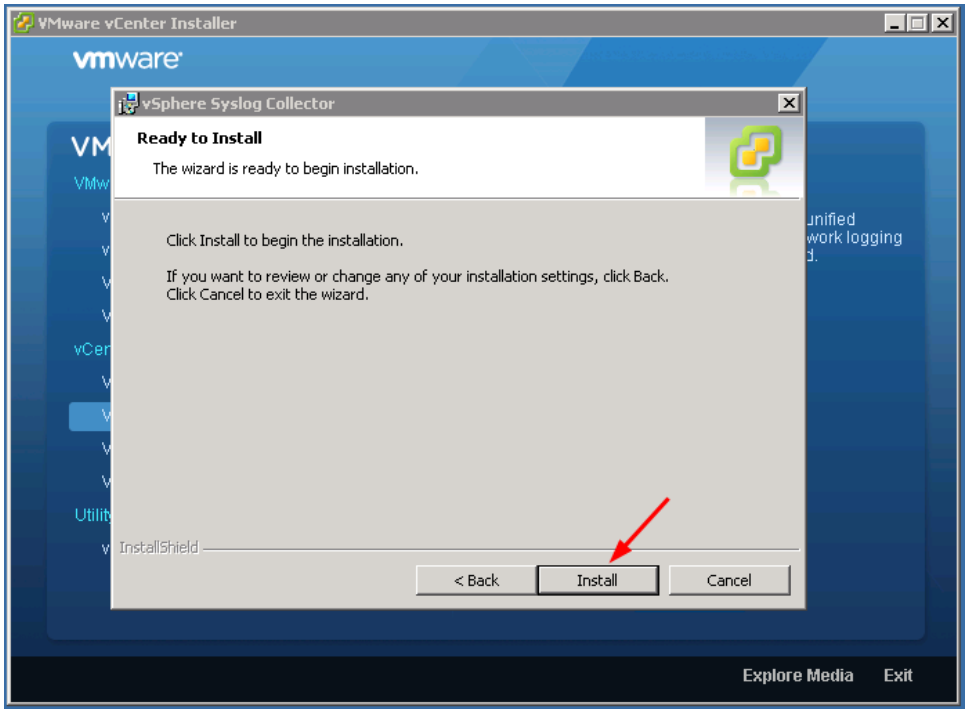


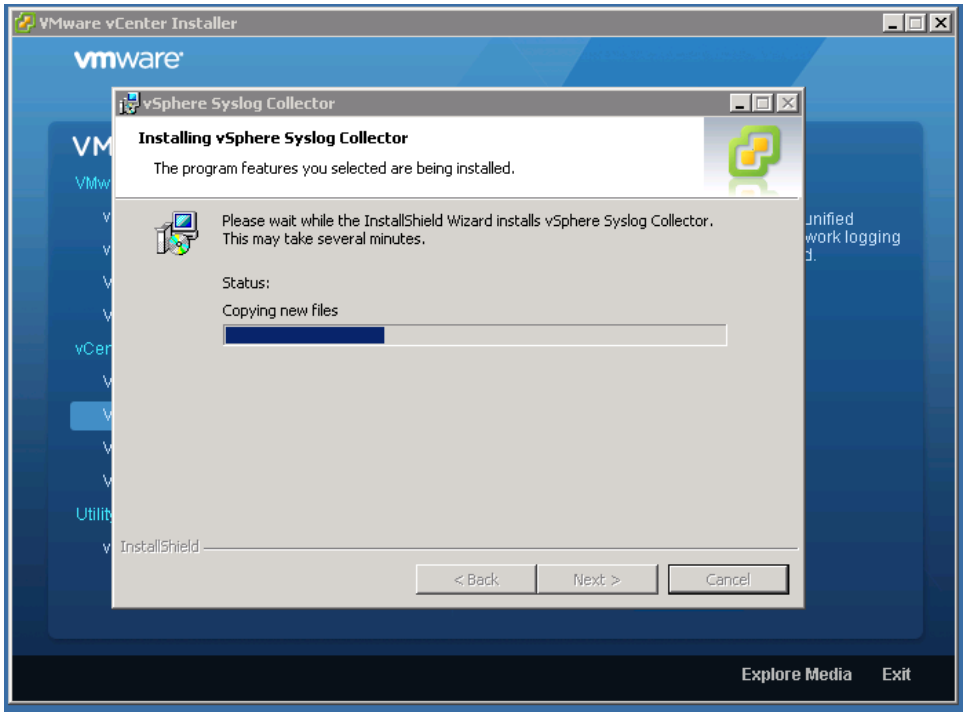
Take note of the port specified here as you will need these either to open firewall ports or to configure your ESXi servers to point to the Syslog server.

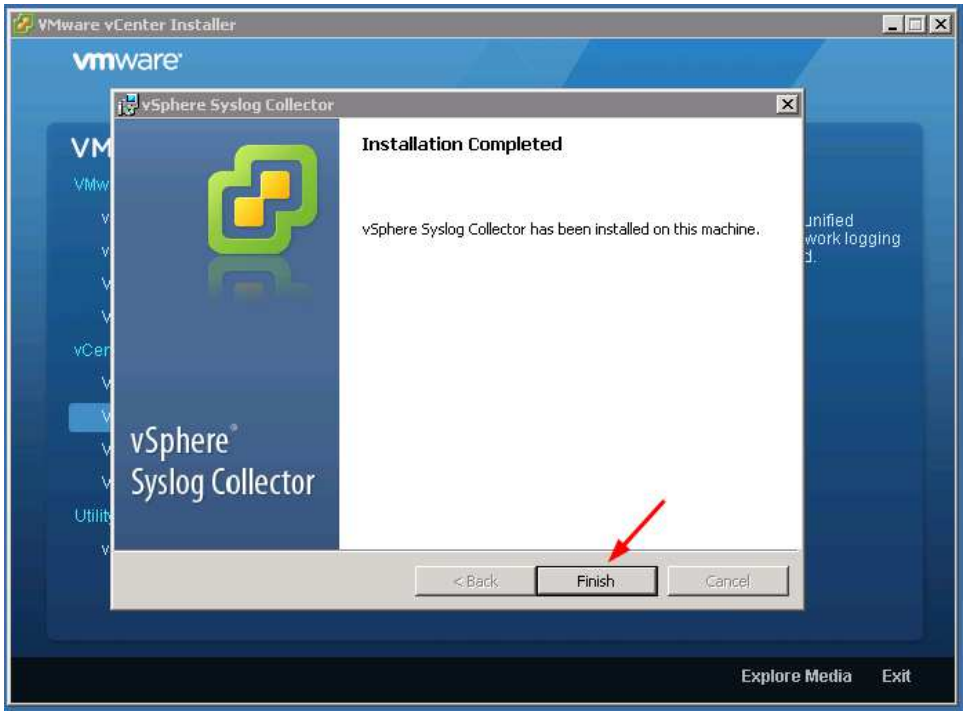
You may also deselect the protocols you do not want to enable for better security.

If you decide to change these ports please ensure you document all changes for future reference.

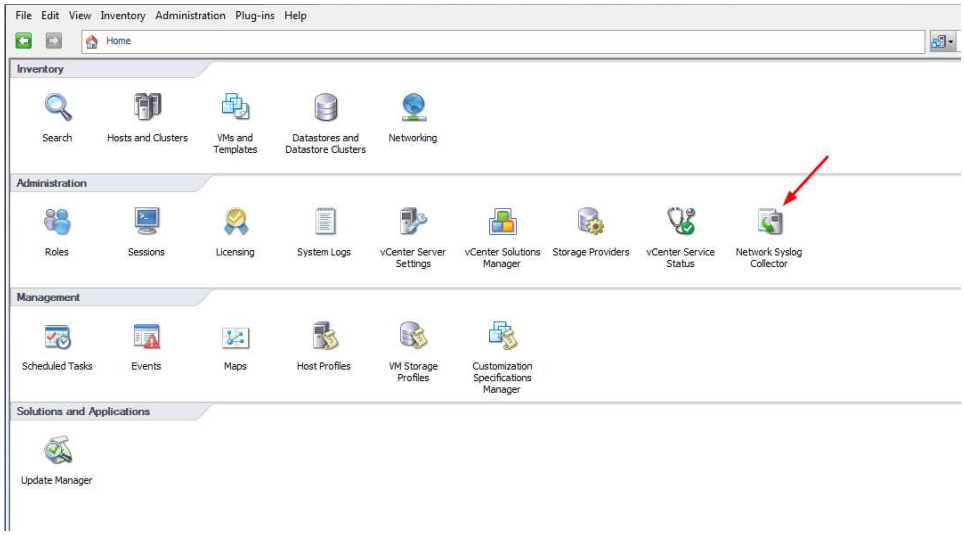


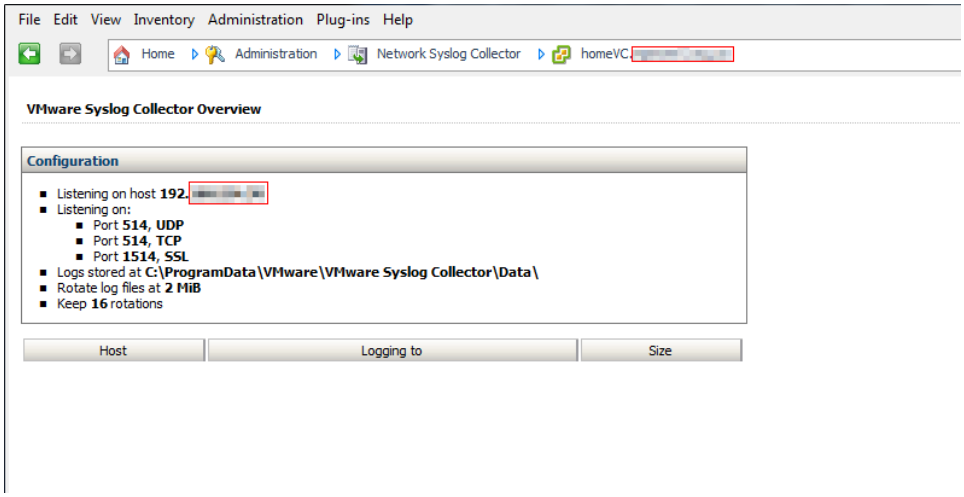

VMware vCenter Installer
vmware
vSphere Syslog Collector
Ready to Install
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back.
Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel
Explore Media
Exit

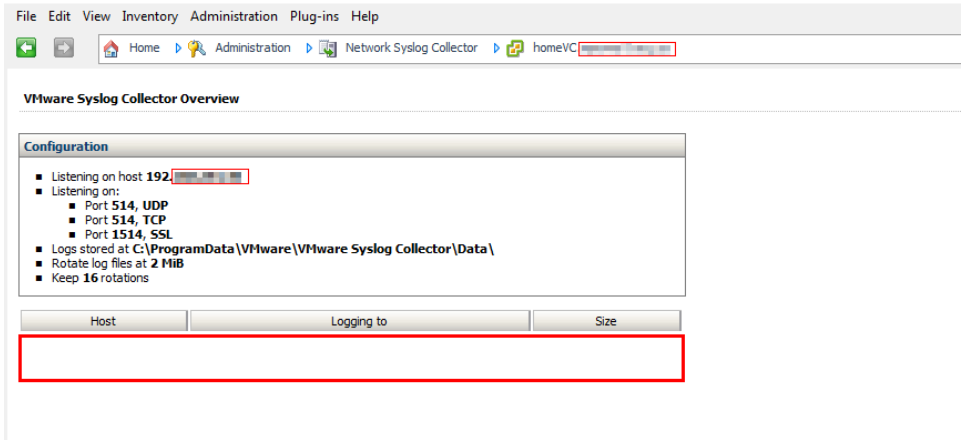

VMware vCenter Installer
vmware
vSphere Syslog Collector
Installing vSphere Syslog Collector
The program features you selected are being installed.
Please wait while the InstallShield Wizard installs vSphere Syslog Collector.
This may take several minutes.
Status:
Copying new files
InstallShield
< Back
Next >
Cancel
Explore Media
Exit



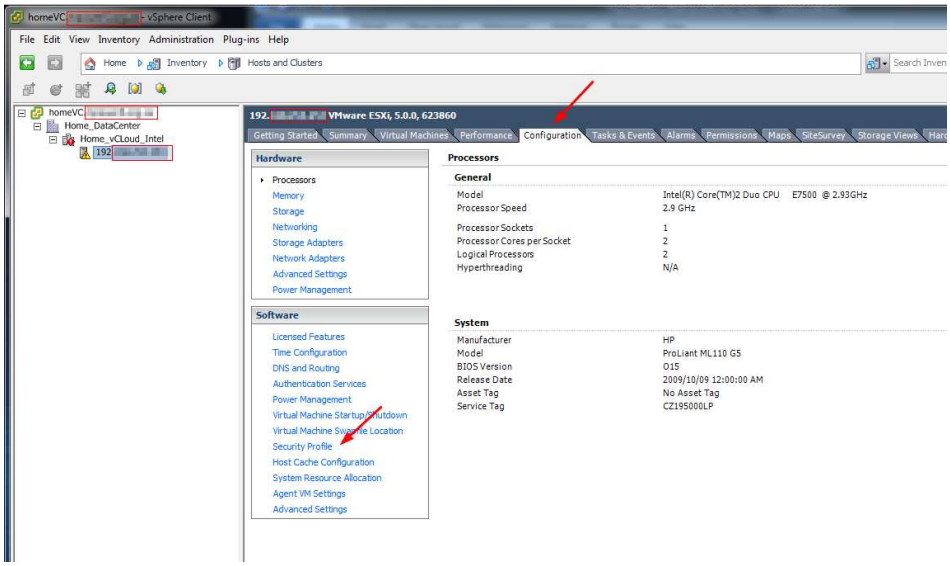
To complete the Sys Log collector setup we shall need to logon to our vCenter server management console (via VI Client) and continue the configuration.

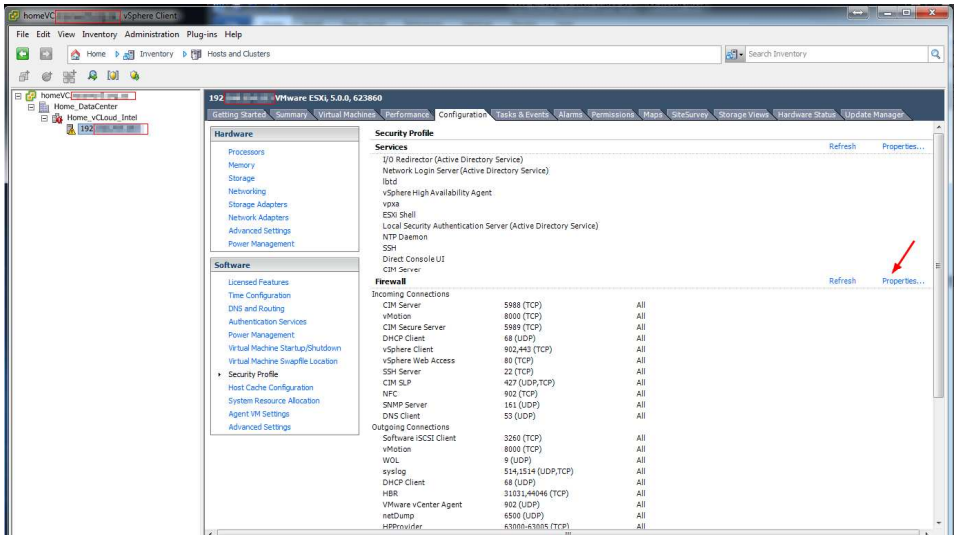


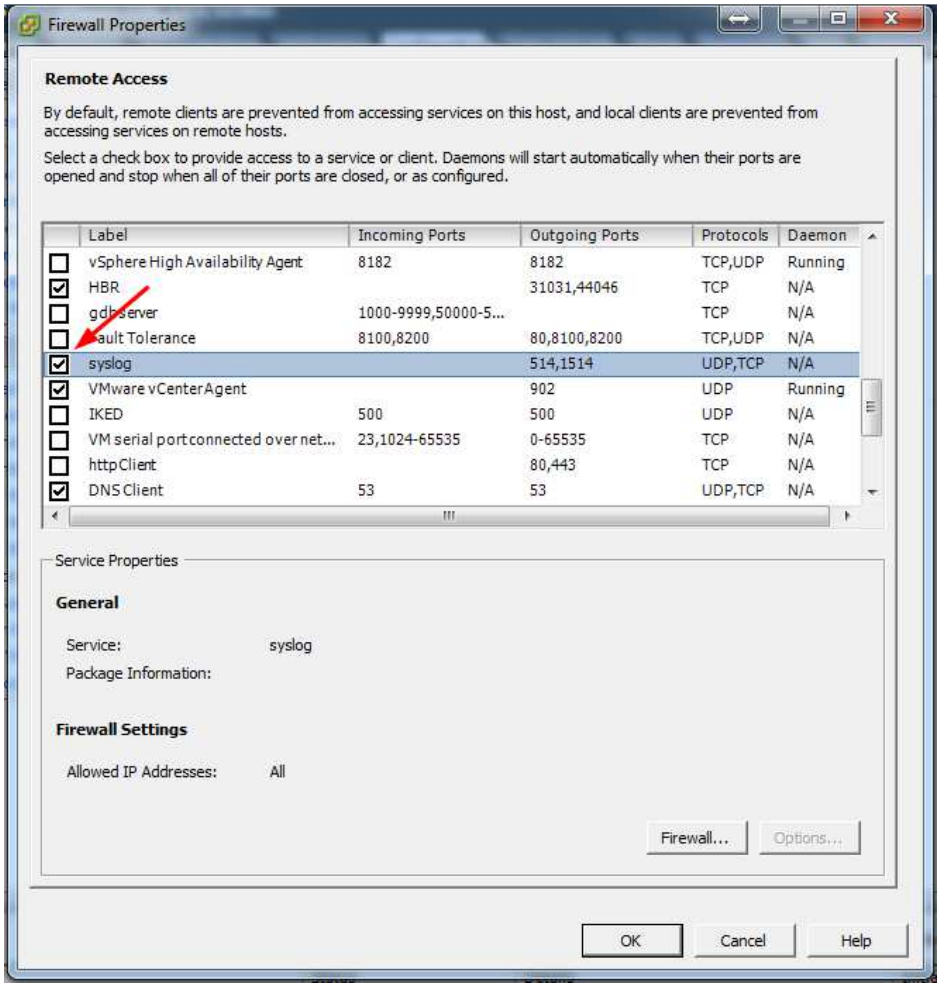




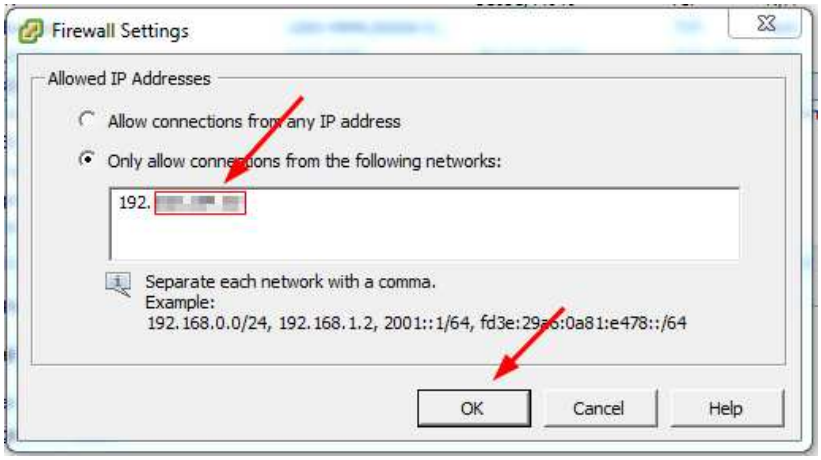
Note that no hosts are showing. We need to point each hosts to the SysLog server.

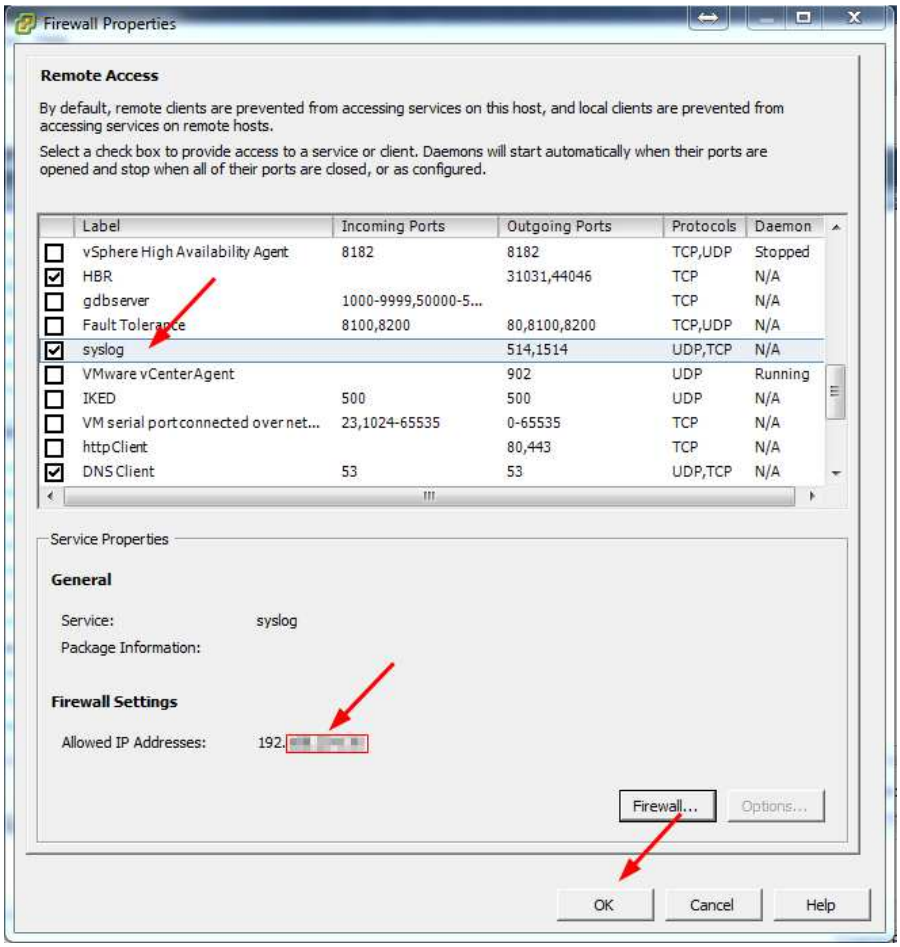


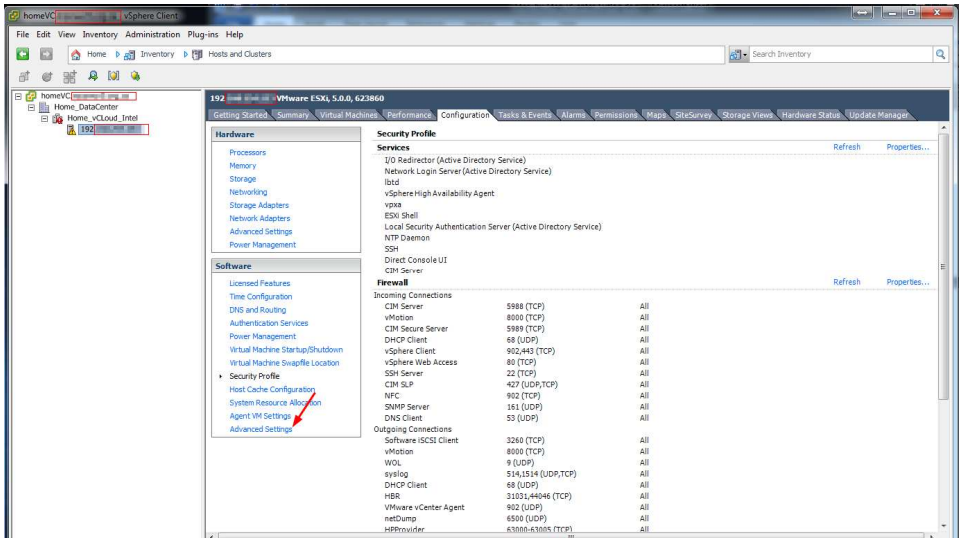


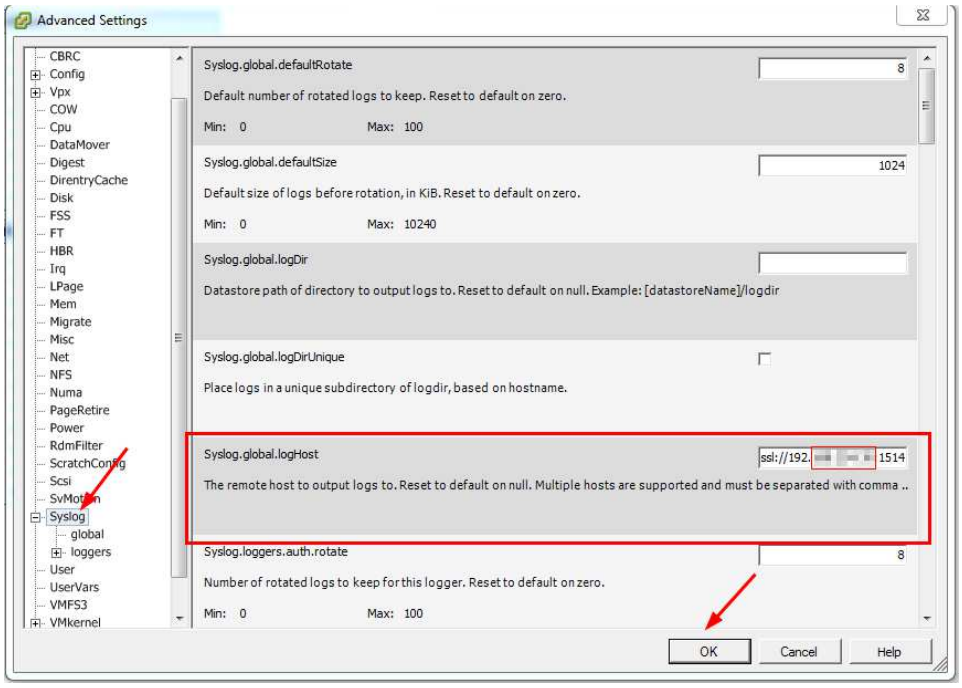


Ensure to check that syslog traffic is allowed on each hosts firewall. If you want to be specific in the traffic that you allow to servers you can click on the Firewall button and add the specific IP addresses or network ranges.

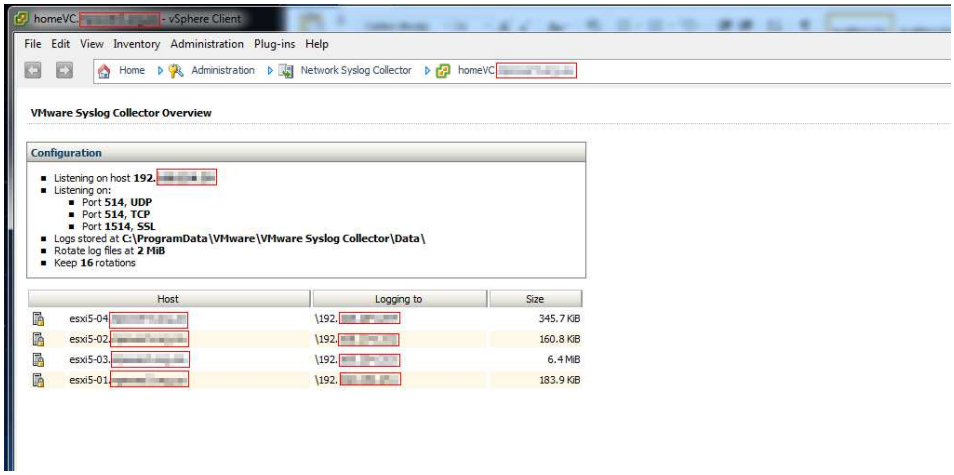

Firewall Settings
Allowed IP Addresses
Allow connections from any IP address
Only allow connections from the following networks:
192.
Separate each network with a comma.
Example:
192.168.0.0/24, 192.168.1.2, 2001::1/64, fd3e:29a6:0a81:e478::/64
OK
Cancel
Help


Firewall Properties
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.
Select a check box to provide access to a service or client. Daemons will start automatically when their ports are opened and stop when all of their ports are closed, or as configured.
Label
Incoming Ports
Outgoing Ports
Protocols
Daemon
vSphere High Availability Agent 8182 8182 TCP,UDP Stopped
HBR 31031,44046 TCP N/A
gdbserver 1000-9999,50000-5... TCP N/A
Fault Tolerance 8100,8200 80,8100,8200 TCP,UDP N/A
syslog 514,1514 UDP,TCP N/A
VMware vCenter Agent 902 UDP Running
IKED 500 500 UDP N/A
VM serial port connected over net... 23,1024-65535 0-65535 TCP N/A
http Client 80,443 TCP N/A
DNS Client 53 53 UDP,TCP N/A
Service Properties
General
Service: syslog
Package Information:
Firewall Settings
Allowed IP Addresses: 192.
Firewall...
Options...
OK
Cancel
Help



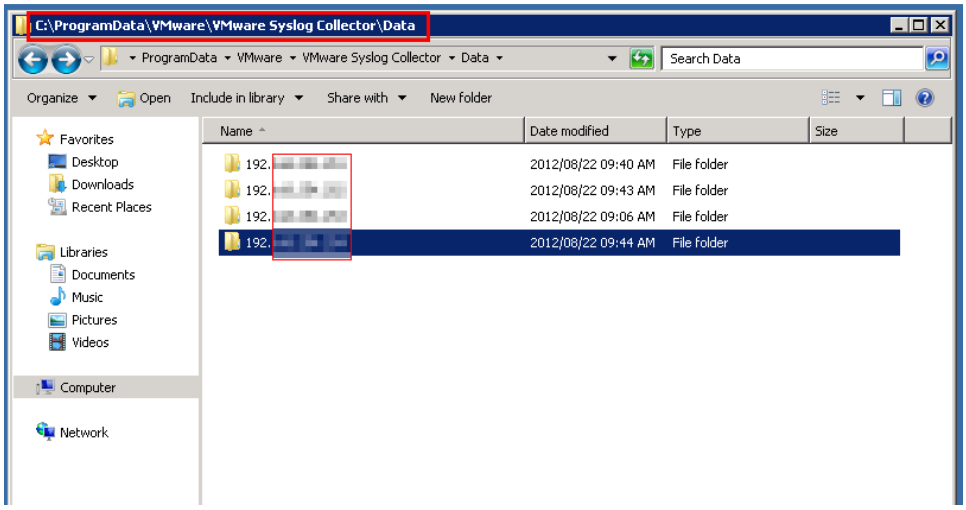


You can either use the secure SSL option IE: ssl://<ip address>:1514 or use the UDP option IE: udp://<ip address>:514.

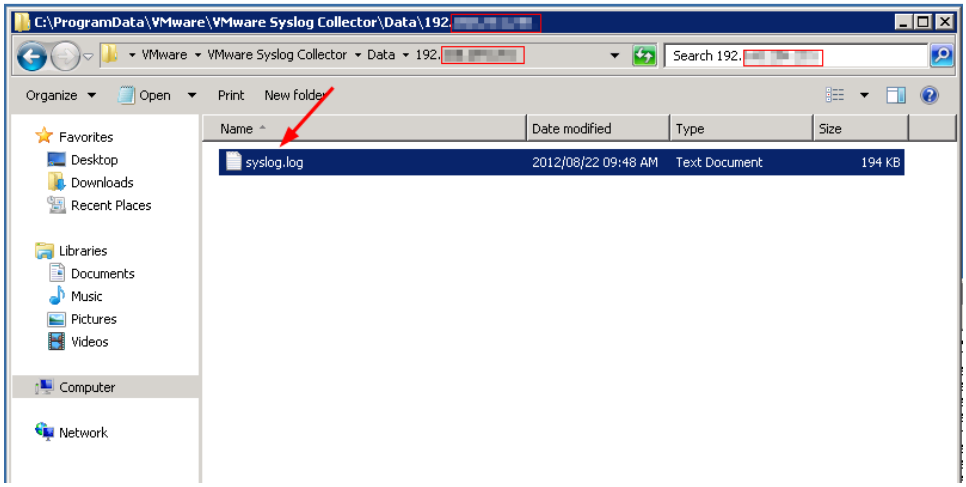


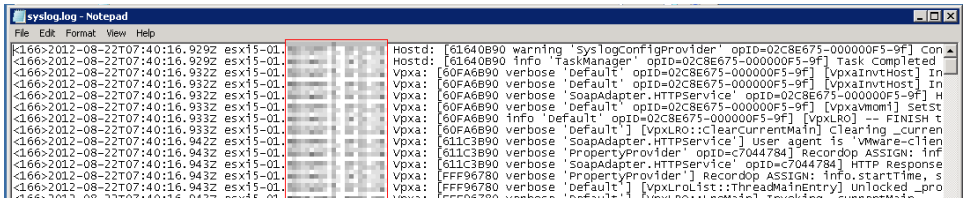
Once you have pointed all the hosts, you will see them listed in the SysLog overview.

NOTE: You most likely will have to close VI Client and re-connect to the vCenter Server to see these.



Logon to the vCenter server and browse to the directory chosen during installation for storing the log files. Here you should see a directory for each ESXi hosts. Within the directory you will find the syslog files.





To follow:

- Configuration of vCenter Server
- Configuration of vCenter Update Manager Server