



NAeS Consulting SRL

CASCADE VIRTUAL SHARK

Versione V1

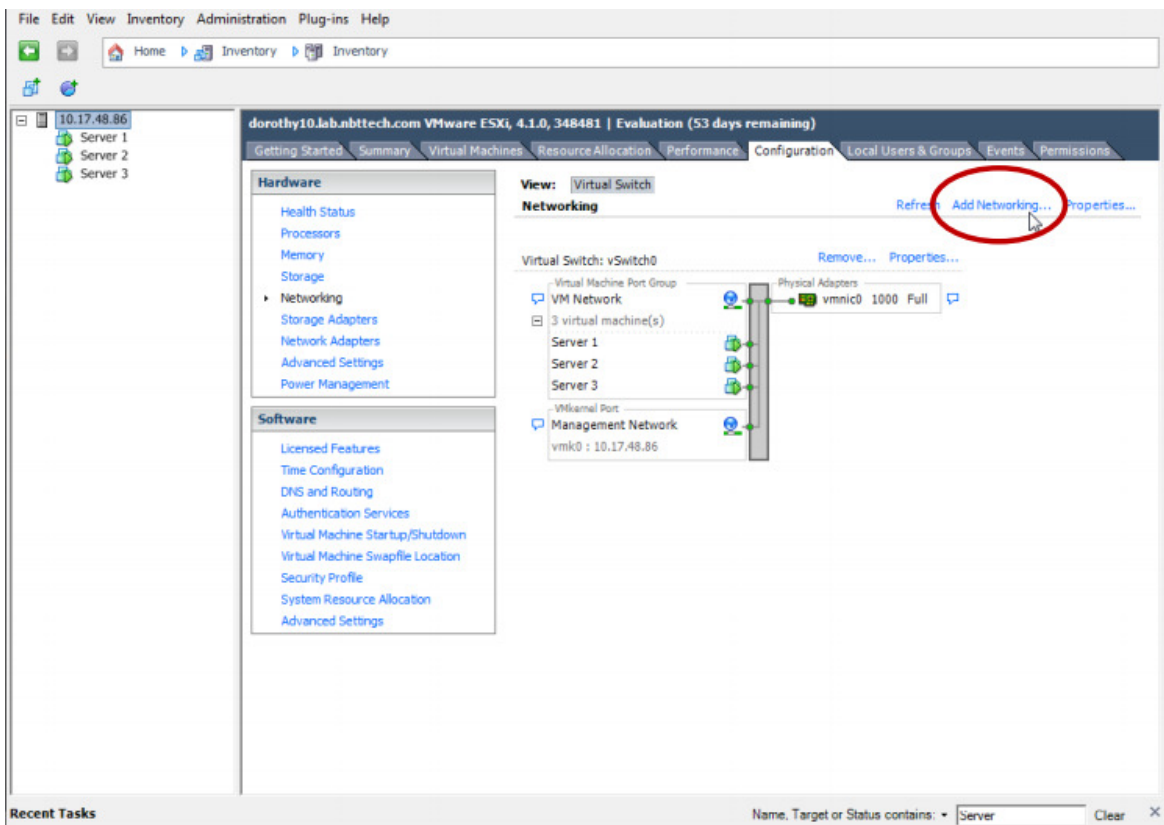
Ing. Jacopo Saladini
18/04/2012

Scopo di questo documento è mostrare la facilità d'installazione di CASCADE VIRTUAL SHARK in ambiente ESX e il suo utilizzo tramite CASCADE PILOT.

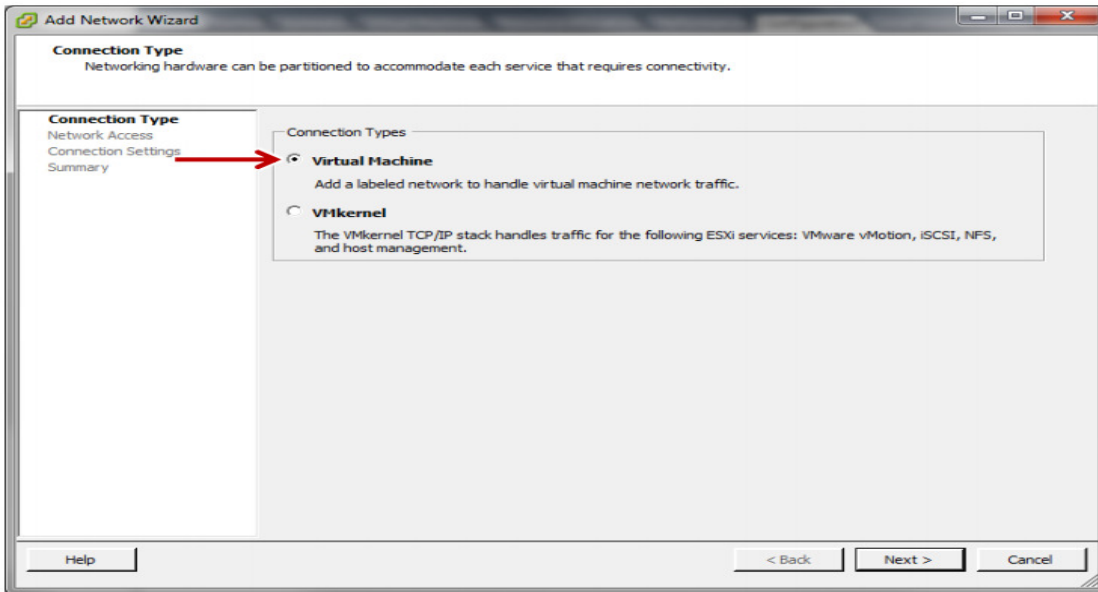
CASCADE VIRTUAL SHARK

Prima di tutto bisogna creare un interfaccia di monitoring per ogni virtual switch presente nell'infrastruttura ESX di cui si voglia monitorare il traffico.

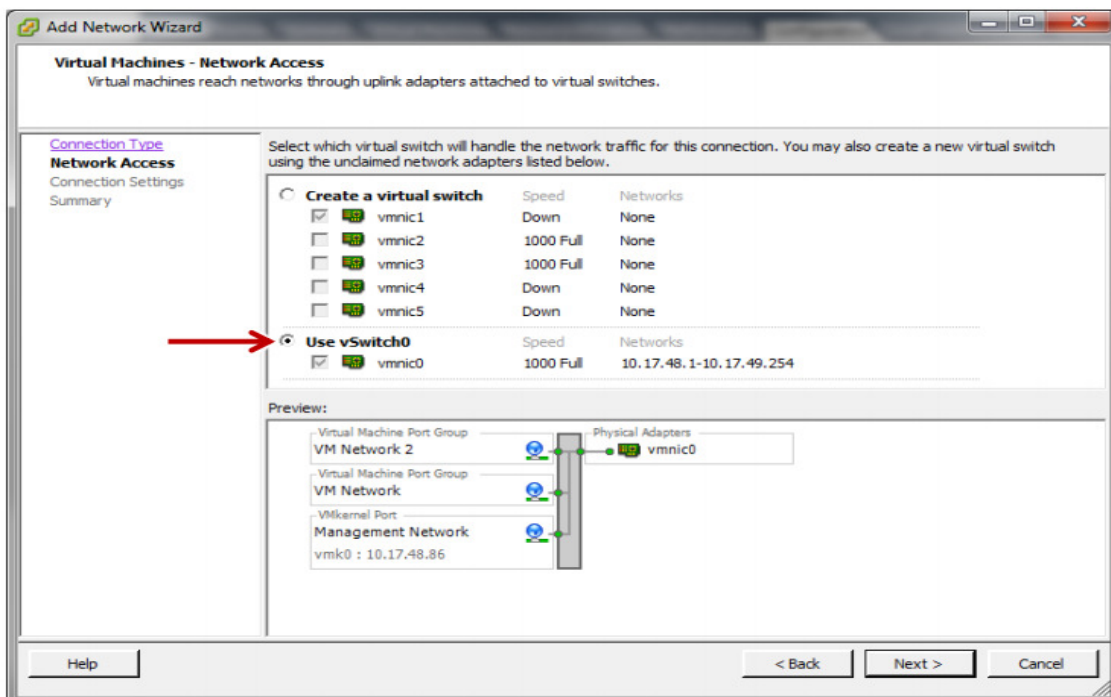
Andare su Configuration → Add Networking:



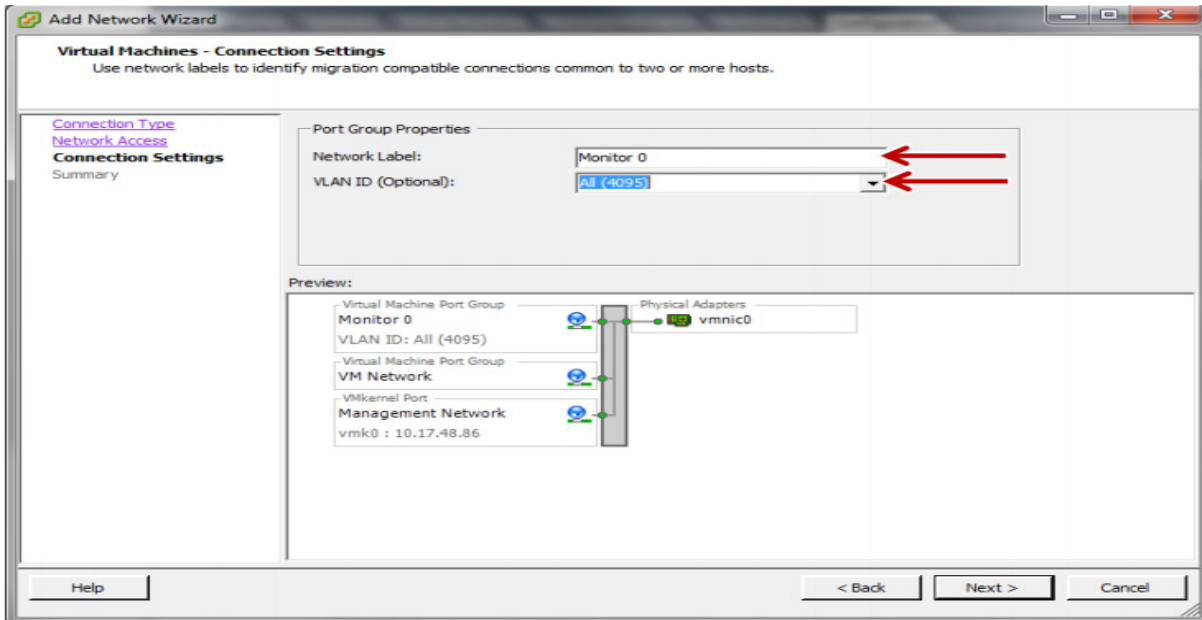
Selezionare virtual machine come tipo di connessione:



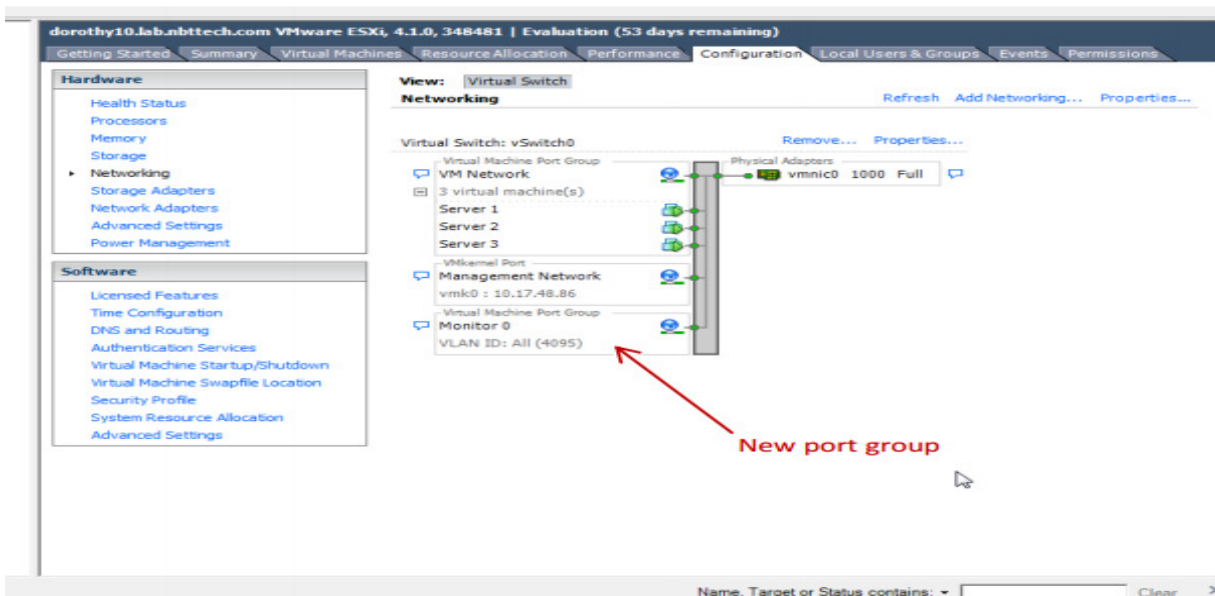
Al passo successivo selezionare il virtual switch dove sono connesse le macchine che si vogliono monitorare, in questo esempio c'è un solo virtual switch con 3 macchine connesse :



Creato il gruppo di porte bisogna assegnargli un nome ed una vlan, per monitorare sia il traffico tagged e untagged la vlan da assegnare è la 4095 (all):

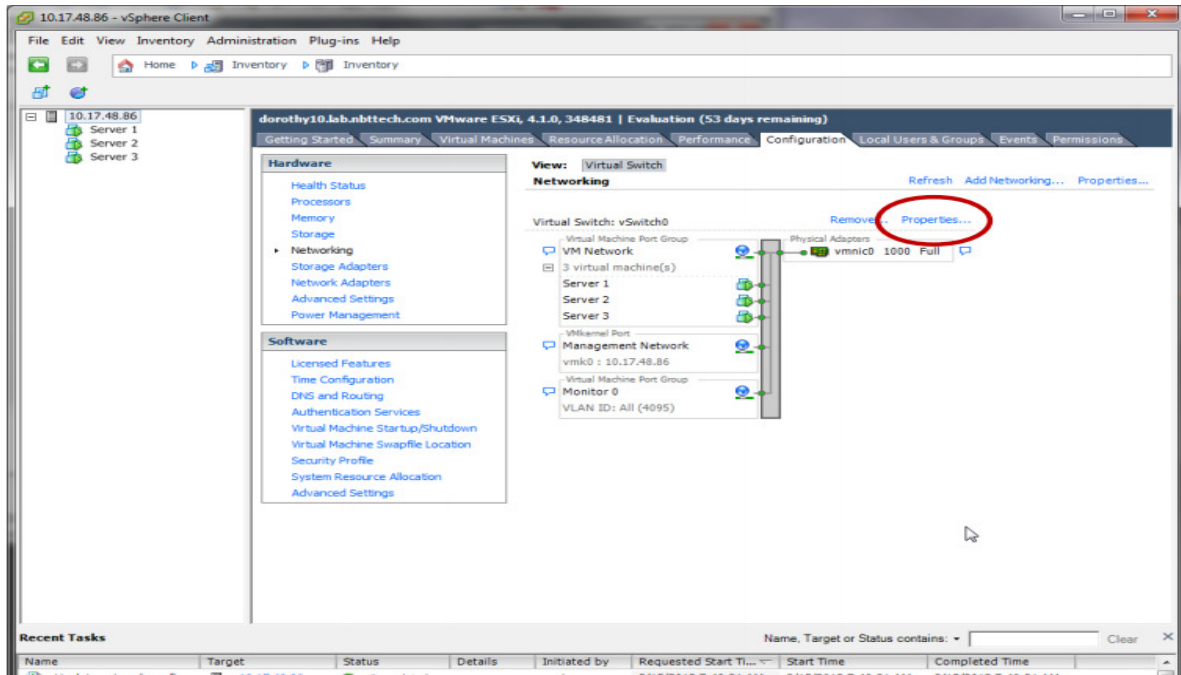


Il risultato finale è :

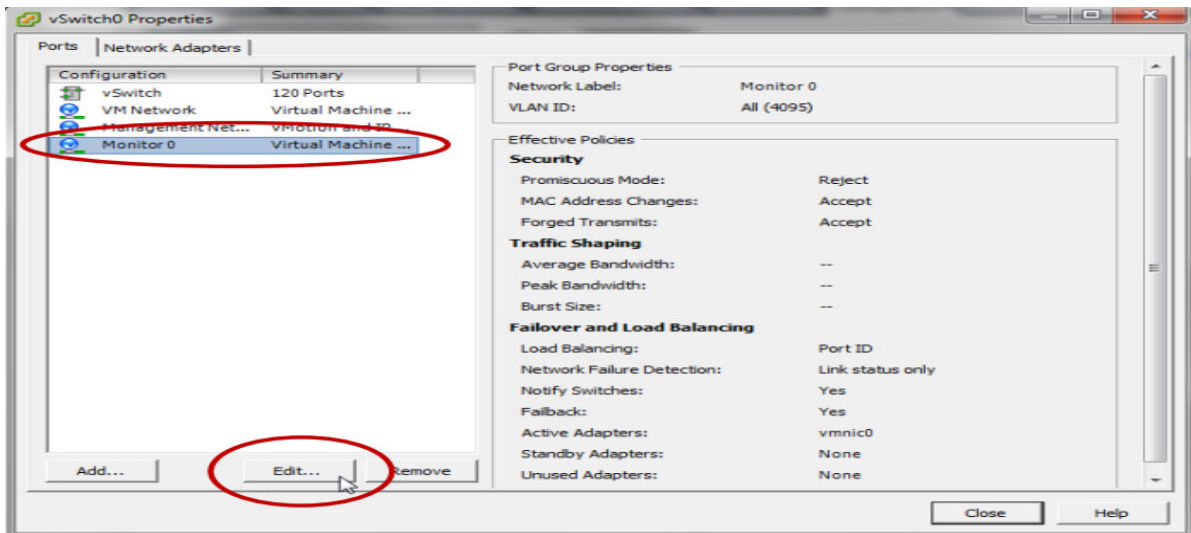


Per effettivamente monitorare il traffico di tutto il virtual switch bisogna impostare la porta di monitoring in promiscuous mode.

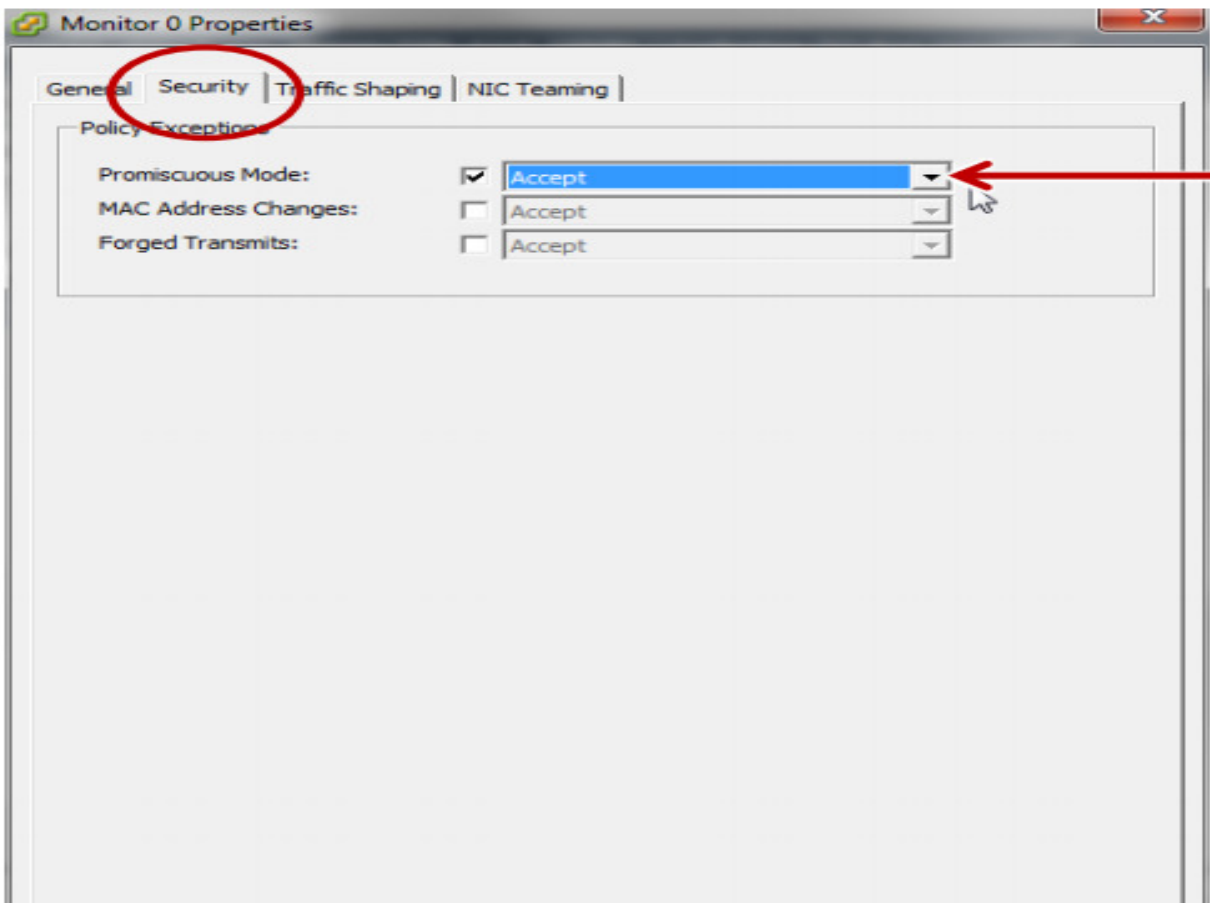
Selezionare le properties del vswitch :



Selezionare la porta di interesse e cliccare su edit:



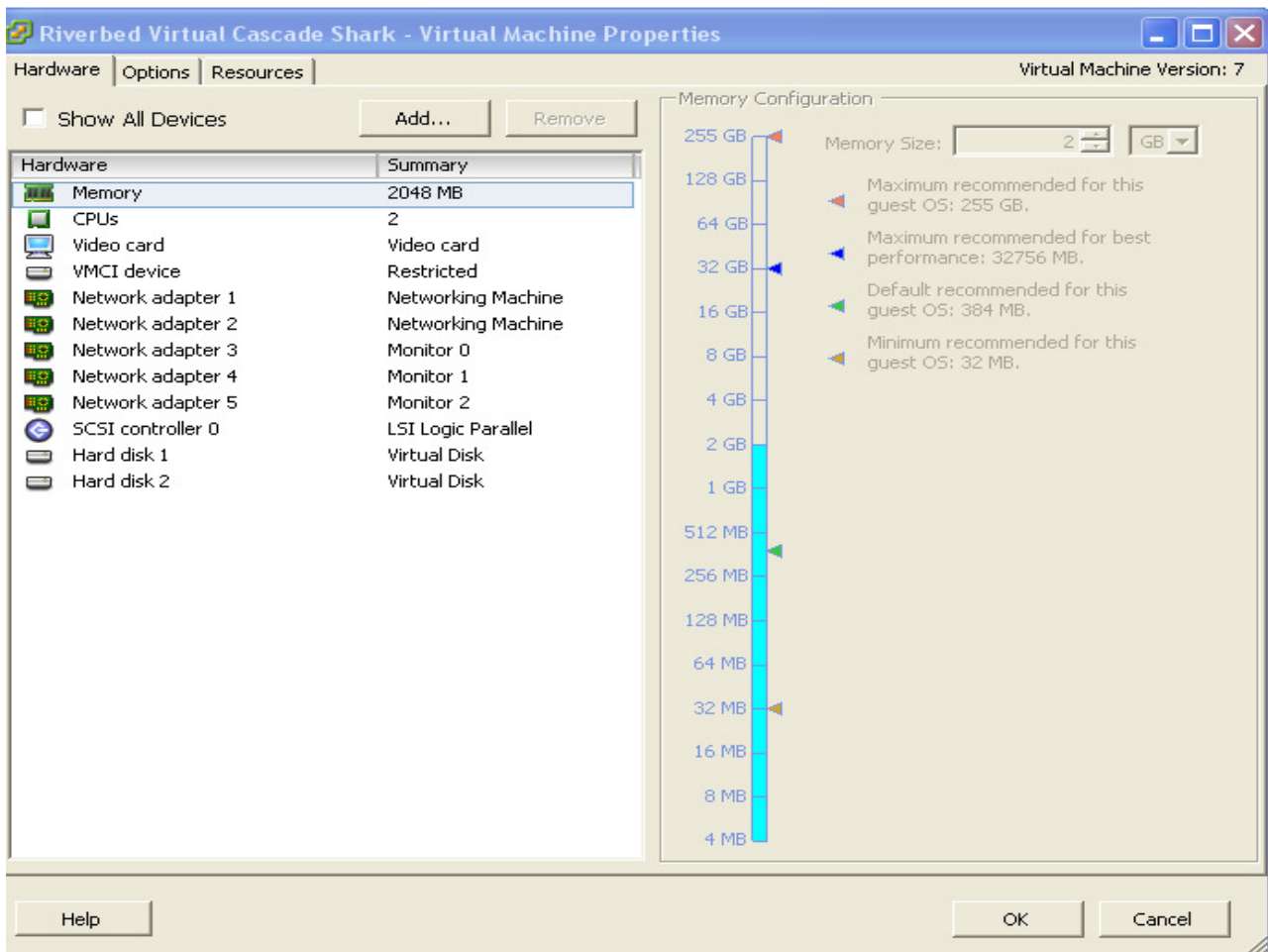
Infine dal tab security impostare accept nel promiscuous mode :



Ora il server ESX è pronto per l'installazione del pacchetto OVA della VIRTUAL SHARK APPLIANCE.

La VIRTUAL SHARK APPLIANCE, di default, ha due interfacce di management (di cui una obbligatoria) un hard disk per il sistema operativo e una porta di monitoraggio . Si può aggiungere un hard disk aggiuntivo per il salvataggio dei file catturati e fino a 3 porte di monitoraggio quindi in totale si possono monitorare fino a 4 vswitch ed i relativi server ad esso collegati.

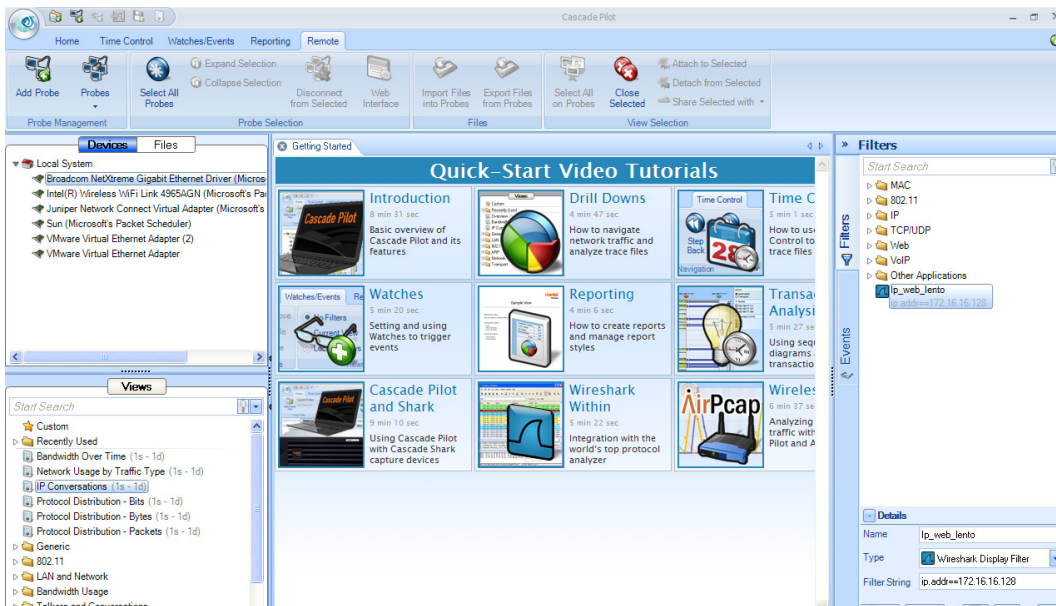
Nel esempio qui sotto si è aggiunto un secondo hard disk e 2 schede aggiuntive di monitoring :



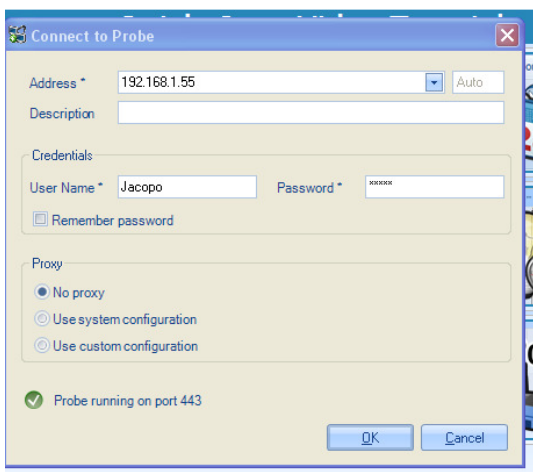
Collegati in console è possibile inizializzare la macchina tramite un wizard e sostanzialmente assegnargli un ip address per poter raggiungere l'appliance tramite l'interfaccia web o tramite il CASCADE PILOT.

CASCADE PILOT

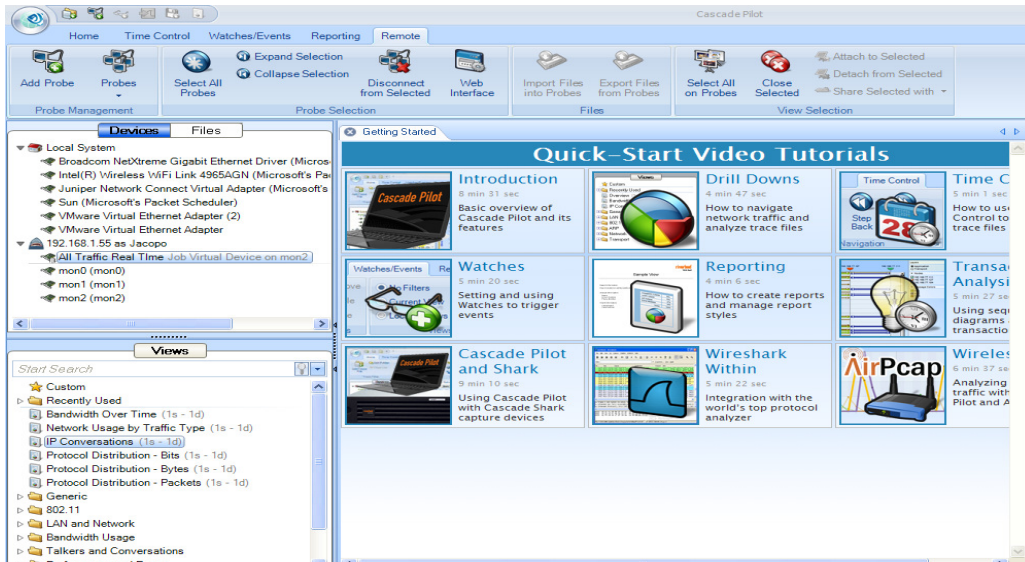
Per collegarsi dal Cascade Pilot alla Virtual Cascade Shark cliccare su remote e poi su Add Probe:



Dopo aver inserito le credenziali impostate, la sonda remota viene mappata come device aggiuntivo:

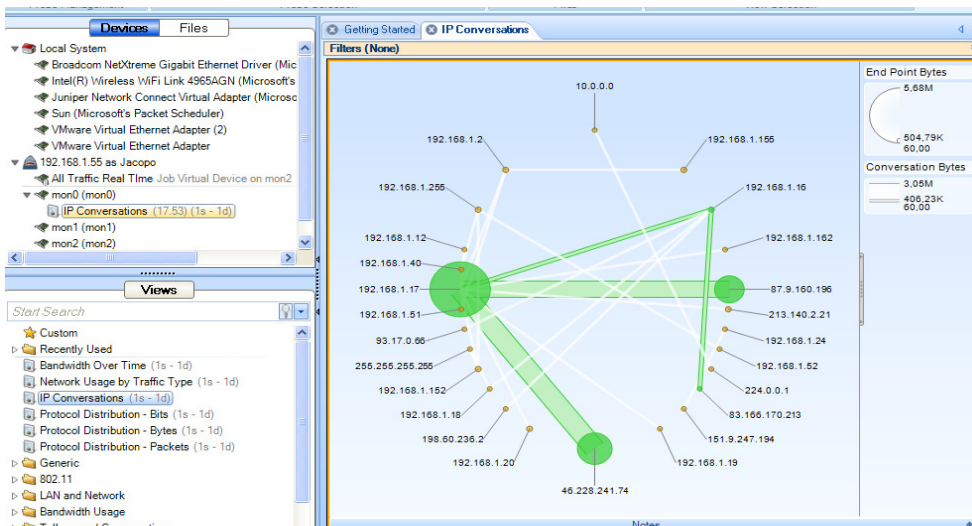


A questo punto Cascade Pilot potrà utilizzare tutta la capacità di analisi sulle tre interfacce di monitoring installate nel ESX server, come se fosse traffico catturato su una delle interfacce locali:

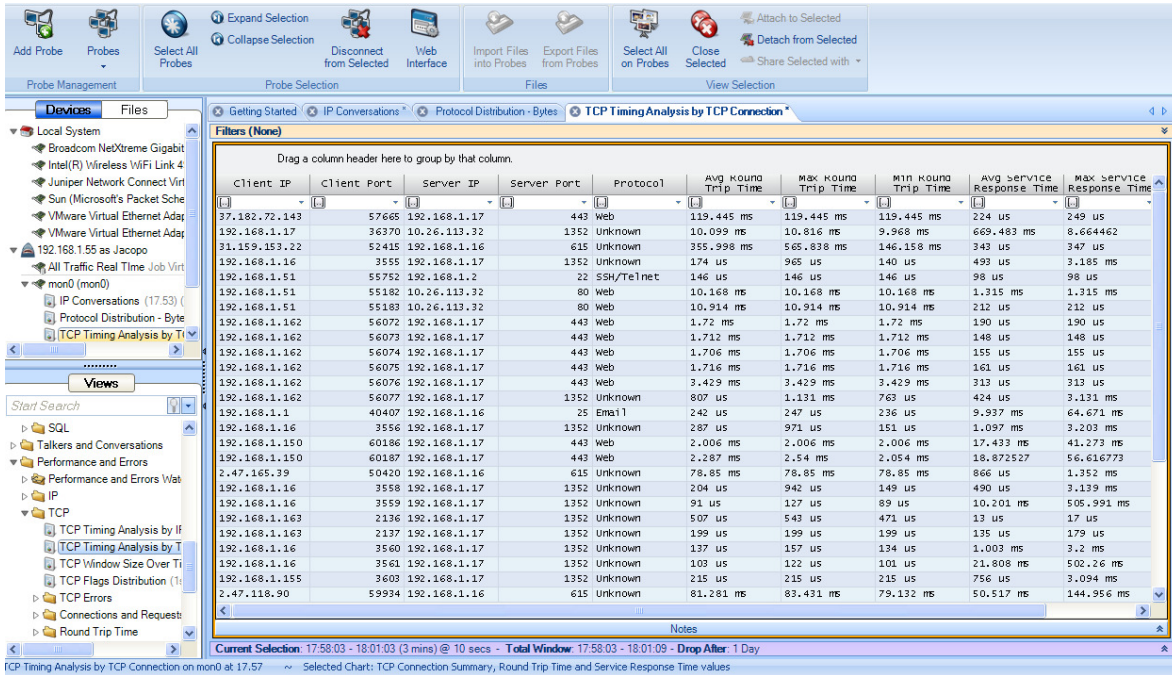


In questo esempio la mon0 è collegata ad un virtual switch dove risiedono tutti i server dell'azienda.

Trascinando per esempio la Views ip conservation si hanno tutti gli ip che dialogano con i server aziendali:



Un'altra vista interessante è la tcp timing analysis dove vengono visualizzate tutte le connessioni esistenti e i tempi di risposta:



Client IP	Client Port	Server IP	Server Port	Protocol	Avg Round Trip Time	Max Round Trip Time	Min Round Trip Time	Avg Service Response Time	Max Service Response Time
37.182.72.143	57665	192.168.1.17	443	Web	119.445 ms	119.445 ms	119.445 ms	224 us	249 us
192.168.1.17	36370	10.26.113.32	1352	Unknown	10.099 ms	10.816 ms	9.968 ms	669.483 ms	8.664462
31.159.153.22	52415	192.168.1.16	615	Unknown	355.998 ms	565.838 ms	146.158 ms	343 us	347 us
192.168.1.16	3555	192.168.1.17	1352	Unknown	174 us	965 us	140 us	493 us	3.185 ms
192.168.1.51	55752	192.168.1.2	22	SSH/Telnet	146 us	146 us	146 us	98 us	98 us
192.168.1.51	55182	10.26.113.32	80	Web	10.168 ms	10.168 ms	10.168 ms	1.315 ms	1.315 ms
192.168.1.51	55183	10.26.113.32	80	Web	10.914 ms	10.914 ms	10.914 ms	212 us	212 us
192.168.1.162	56072	192.168.1.17	443	Web	1.772 ms	1.772 ms	1.772 ms	190 us	190 us
192.168.1.162	56073	192.168.1.17	443	Web	1.712 ms	1.712 ms	1.712 ms	148 us	148 us
192.168.1.162	56074	192.168.1.17	443	Web	1.706 ms	1.706 ms	1.706 ms	155 us	155 us
192.168.1.162	56075	192.168.1.17	443	Web	1.716 ms	1.716 ms	1.716 ms	161 us	161 us
192.168.1.162	56076	192.168.1.17	443	Web	3.429 ms	3.429 ms	3.429 ms	313 us	313 us
192.168.1.162	56077	192.168.1.17	1352	Unknown	807 us	1.131 ms	763 us	424 us	3.131 ms
192.168.1.1	40407	192.168.1.16	25	Email	242 us	247 us	236 us	9.937 ms	64.671 ms
192.168.1.16	3556	192.168.1.17	1352	Unknown	287 us	971 us	151 us	1.097 ms	3.203 ms
192.168.1.150	60186	192.168.1.17	443	Web	2.006 ms	2.006 ms	2.006 ms	17.433 ms	41.273 ms
192.168.1.150	60187	192.168.1.17	443	Web	2.287 ms	2.54 ms	2.054 ms	18.872527	56.616773
2.47.165.39	50420	192.168.1.16	615	Unknown	78.85 ms	78.85 ms	78.85 ms	866 us	1.352 ms
192.168.1.16	3558	192.168.1.17	1352	Unknown	204 us	942 us	149 us	490 us	3.139 ms
192.168.1.16	3559	192.168.1.17	1352	Unknown	91 us	127 us	89 us	10.201 ms	505.991 ms
192.168.1.163	2136	192.168.1.17	1352	Unknown	507 us	543 us	471 us	13 us	17 us
192.168.1.163	2137	192.168.1.17	1352	Unknown	199 us	199 us	199 us	135 us	179 us
192.168.1.16	3560	192.168.1.17	1352	Unknown	137 us	157 us	134 us	1.003 ms	3.2 ms
192.168.1.16	3561	192.168.1.17	1352	Unknown	103 us	122 us	101 us	21.808 ms	502.26 ms
192.168.1.155	3603	192.168.1.17	1352	Unknown	215 us	215 us	215 us	756 us	3.094 ms
2.47.118.90	59934	192.168.1.16	615	Unknown	81.281 ms	83.431 ms	79.132 ms	50.517 ms	144.956 ms

Per una scoprire le potenzialità di analisi di Cascade Pilot consultare gli articoli specifici .