

Master Thesis - Security Aspects in Virtual Networks

SITREP 16

Laurent De Wilde

Master of Science in the Applied Computer Science
Vrije Universiteit Brussel

April 16, 2015

While I was experimenting with Hyper-V, the resources on the 1U pizzaserver became sparse and I installed a second Hyper-V server.

This is actually the tower server with the Intel Core i7. I made a **triple boot** installation on this tower server: it now consists of the two original Windows 7 OS's and a Windows Server 2012 R2 OS on a third partition. Therefore, I had to shrink one of the two (dual boot) partitions to make space for WS2012. So the original OS's remained untouched, only a third one was added.

However, I found it rather cumbersome to work with two separate 'Hyper-V Managers' and that's why I decided to make a small private cloud containing these two Hyper-V servers and one common interface to interact with and to manage the VM's. This interface is System Center Virtual Machine Manager 2012 R2.

To be able to install SCVMM, I created a domain controller (VM) and also a dedicated VM that runs SQL Server 2012 and SCVMM. (FOTO NODIG)

I will not cover all the installation and configuration details, but with all the caveats and trial and errors, it took me nearly two days to install SCVMM, to configure the domain, the storage and to get the cloud online. On the next page are some screenshots.

While diving deeper into Hyper-V, I also discovered the "Microsoft Security Compliance Manager" and did some testing with it. For example, I hardened the security of one of the Windows 7 VM's using group policy objects.

Of course, this was not the original intention of my Master Thesis, but I really like Hyper-V and WS2012, which led to the discovering of enhanced utilities such as the Security Compliance Manager and creating a private cloud using System Center 2012 R2 Virtual Machine Manager. System Center 2012 houses other powerful tools, but I did not yet install them.

Maybe I could do some research and testing about private cloud security? Is there something I could test? For example, intrusion detection on private clouds, traffic capture, virtual firewalls, network access control, security of virtual disks that reside on shared storage, system hardening using SCM,

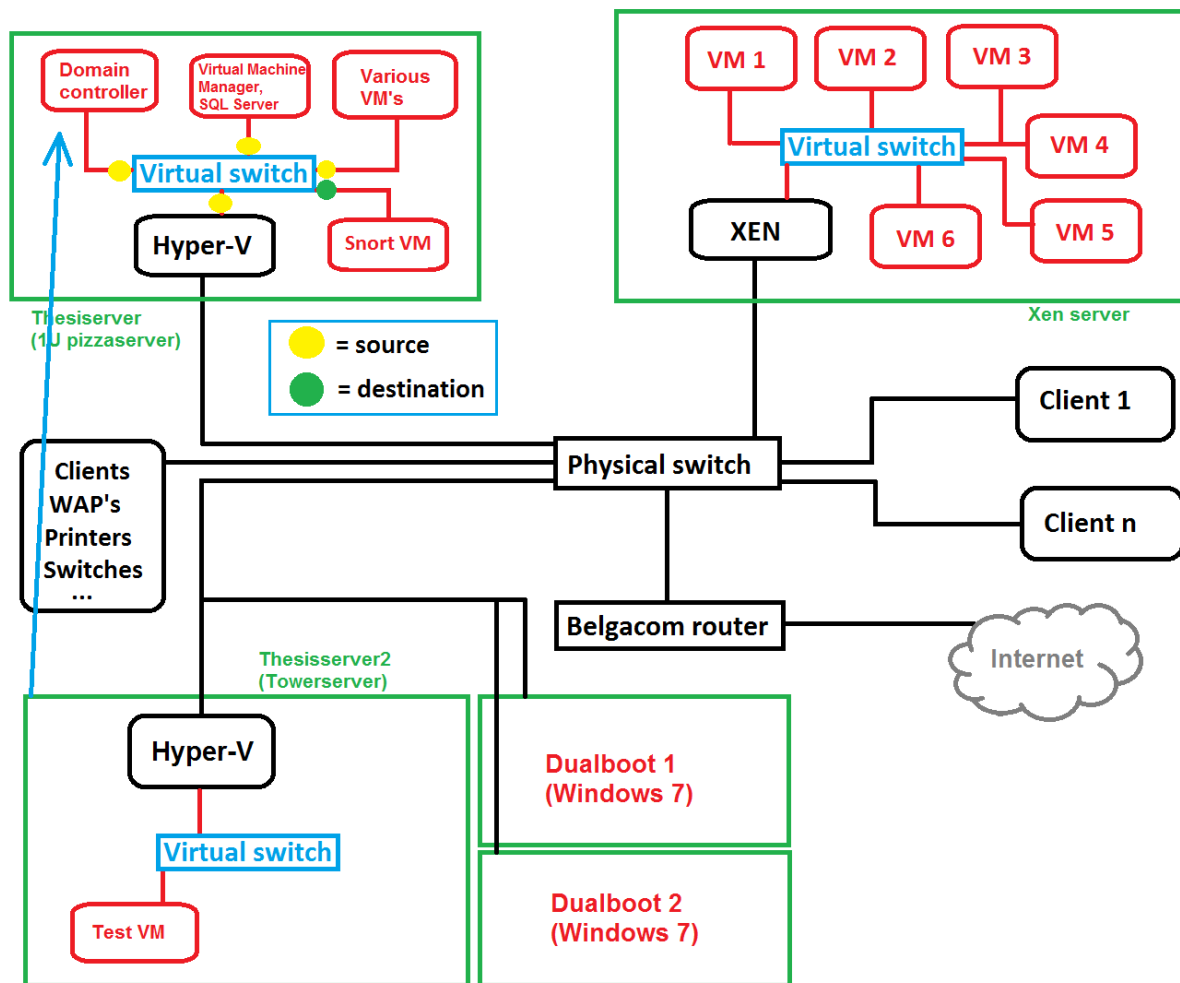


Figure 1: Current infrastructure.

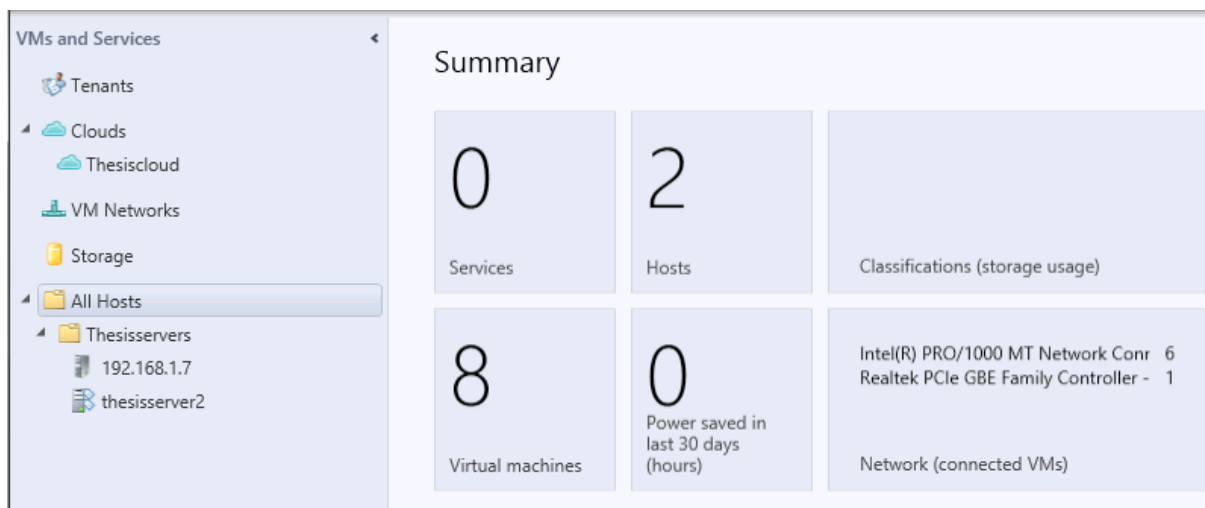


Figure 2: The two Hyper-V hosts with 8 VM's in total.

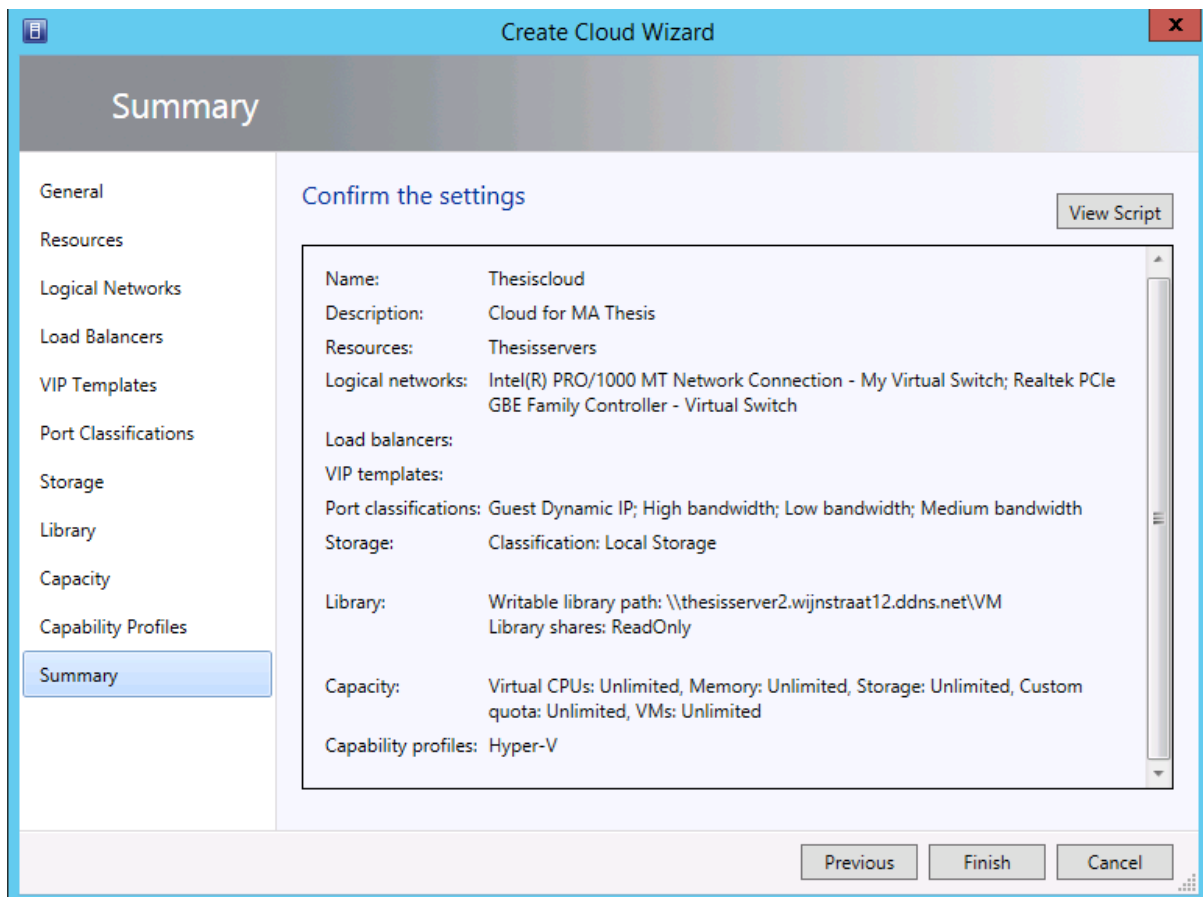


Figure 3: The summary of the private cloud. A library share has also been created to store the .ISO files to install the operating system on the VM's.

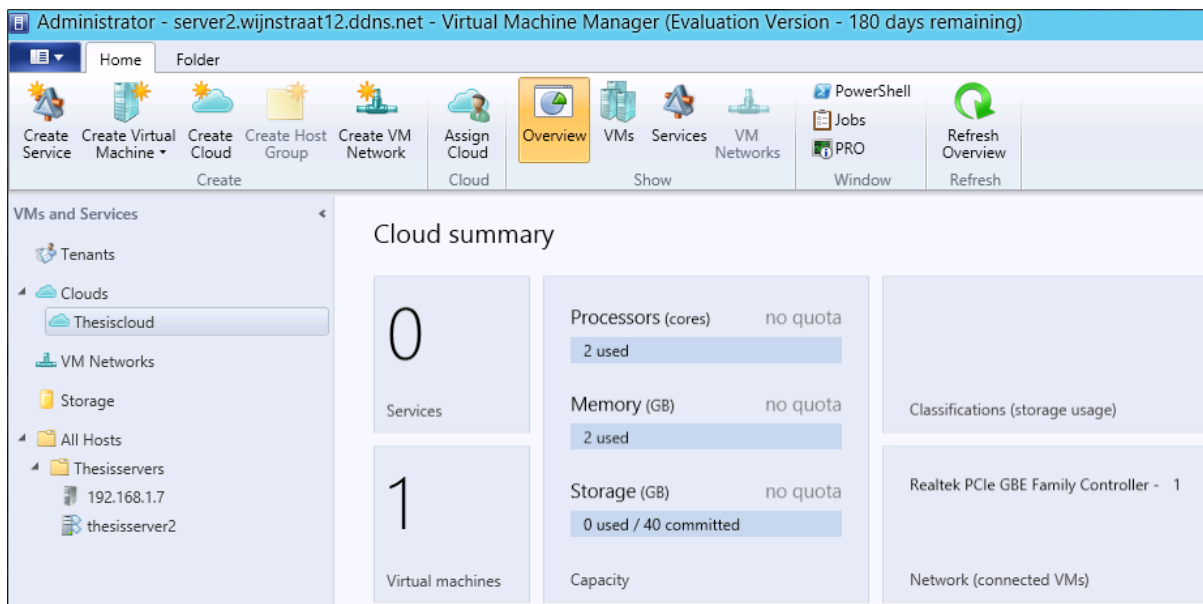
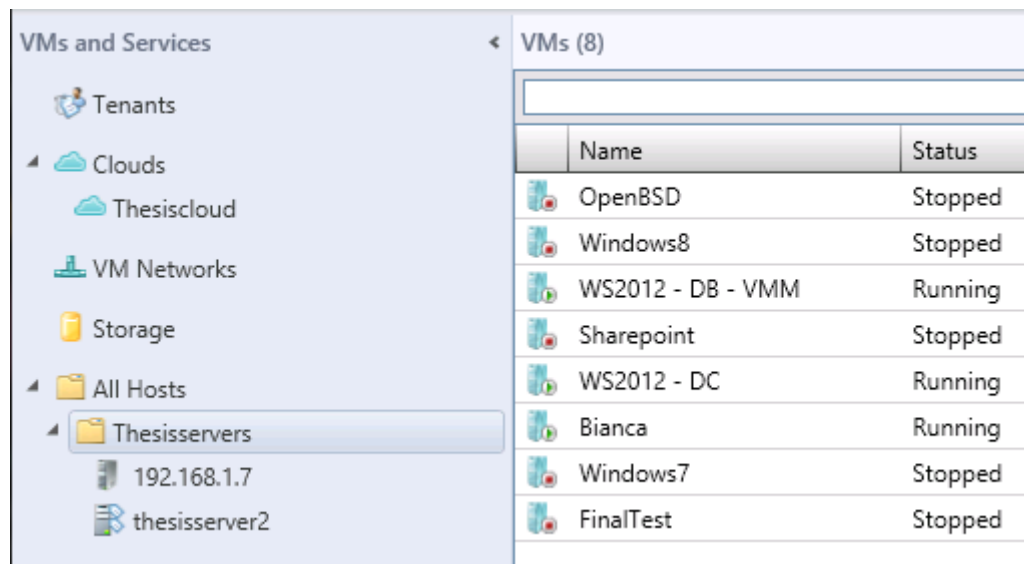


Figure 4: The overview of the private cloud. I created one VM in the new cloud that physically resides on "thesisserver2", the tower server.



VMs (8)	
Name	Status
OpenBSD	Stopped
Windows8	Stopped
WS2012 - DB - VMM	Running
Sharepoint	Stopped
WS2012 - DC	Running
Bianca	Running
Windows7	Stopped
FinalTest	Stopped

Figure 5: List of all the VM's on all the hosts and their current status.

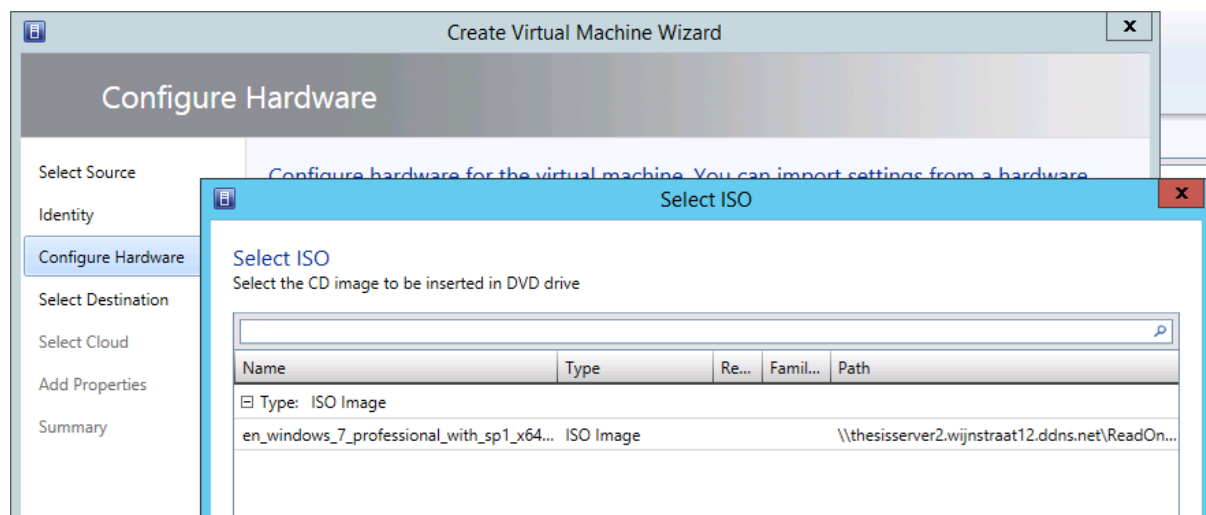


Figure 6: When adding a new VM to the cloud, an ISO image can be selected from a shared library as previously mentioned.

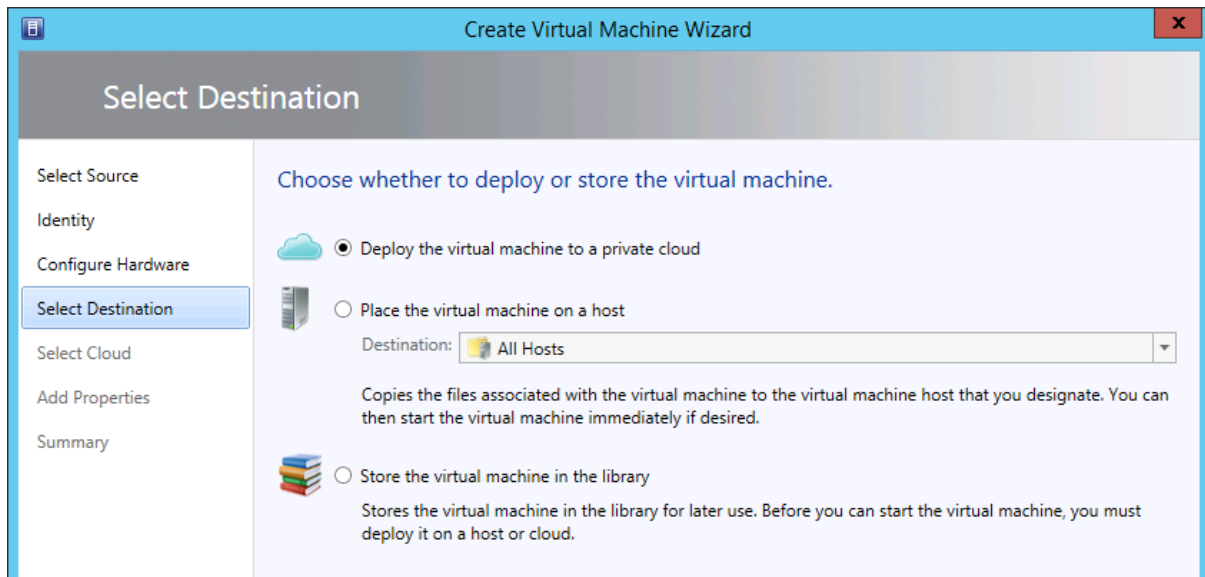


Figure 7: Deployment of the VM in the private cloud.

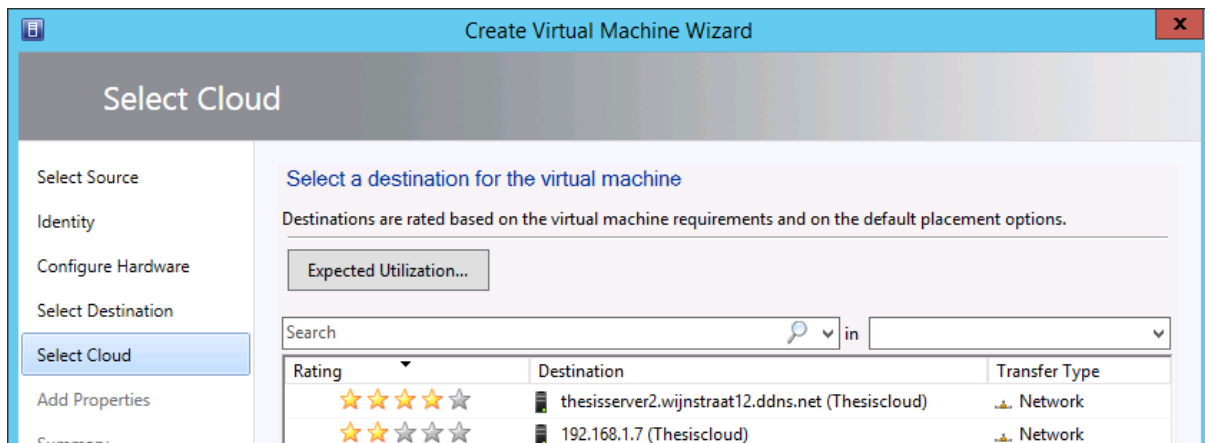


Figure 8: The most suitable place to store (run) the VM is indicated on this screen. The higher the rating, the more suitable. We opt for “thesisserver2”.

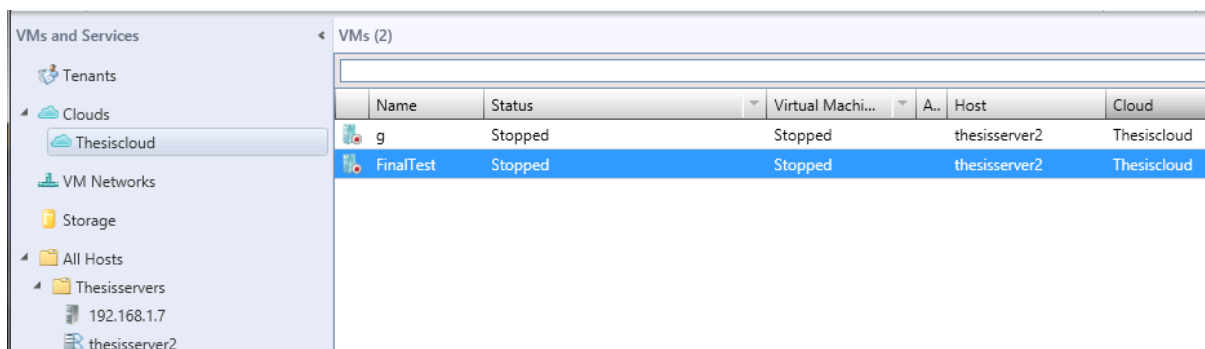
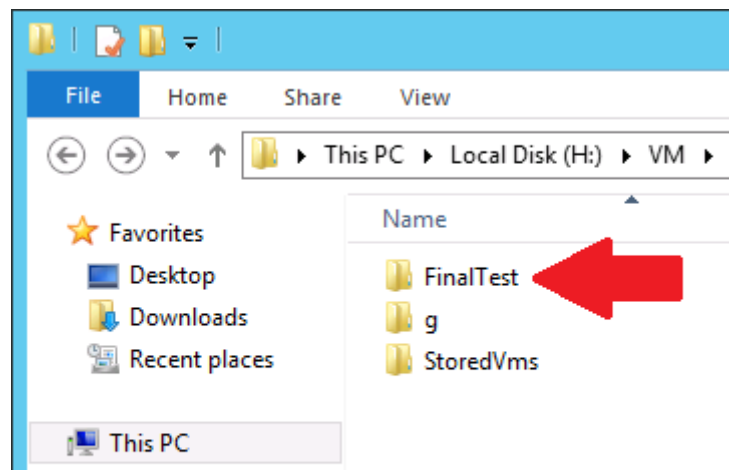


Figure 9: The VM is deployed in the cloud...



Thesisserver2

Figure 10: ... and stored physically on the tower server on the default location that has been specified when I configured the private cloud.

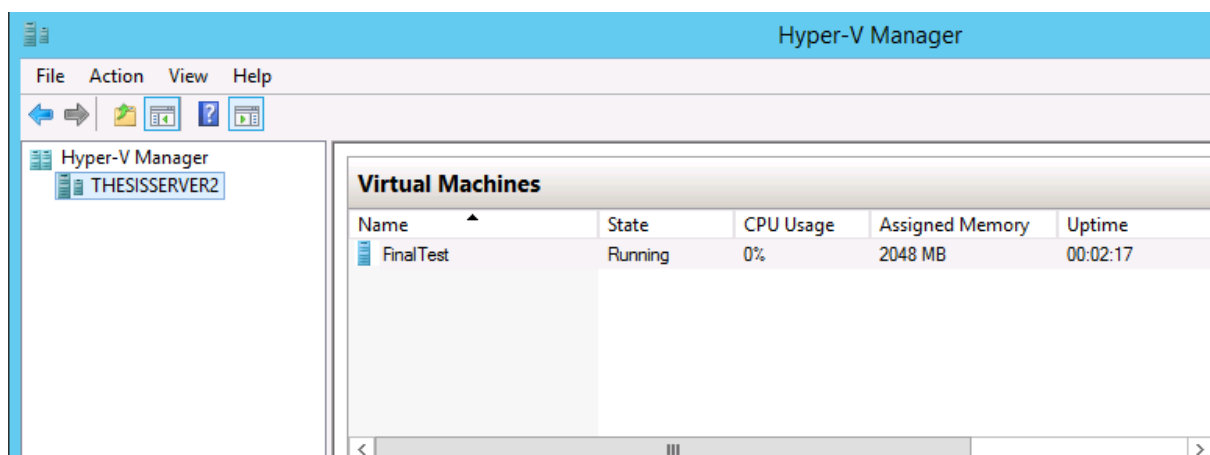


Figure 11: And indeed, the VM is listed in Hyper-V Manager of the target server ...

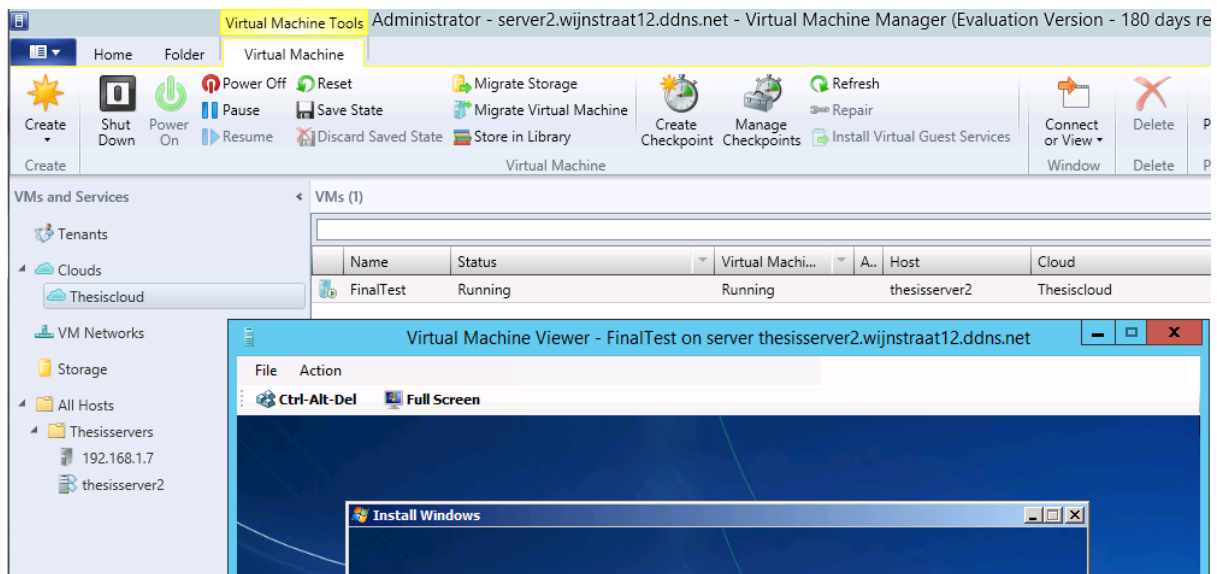


Figure 12: ...but now I can control all the VM's from a single management console, which makes it more efficient. I must say, SCVMM is a very handy and powerful tool. I have never used it before, but will certainly continue using it.

Hosts (2)							
Name	Host Status	Role	Job Status	CPU Average	Available Memory	Operating System	
192.168.1.7	OK	Host	Completed	15%	1,30 GB	Microsoft Windows Server 2012 R2 Datacenter	
thesisserver2...	OK	Library; Host	Completed	0%	6,87 GB	Microsoft Windows Server 2012 R2 Datacenter	

Figure 13: A short overview of the hosts.

Physical Library Objects (3)			
Name	Type	Library Server	
en_windows_7_professional_with_sp1_x64_dvd_u_676939.iso	ISO Image	thesisserver2.wijnstraat12.ddns.net	
en_windows_7_professional_with_sp1_x64_dvd_u_676939.iso	ISO Image	thesisserver2.wijnstraat12.ddns.net	
FinalTest_disk_1.vhdx	VHDX	thesisserver2.wijnstraat12.ddns.net	

Figure 14: The physical objects stored on the library servers.

Planning

Problems

Issues

Assistance

Of course, this was not the original intention of my Master Thesis, but I really like Hyper-V and WS2012, which led to the discovering of enhanced utilities such as the Security Compliance Manager and creating a private cloud using System Center 2012 R2 Virtual Machine Manager. System Center 2012 houses other powerful tools, but I did not yet install them.

Maybe I could do some research and testing about private cloud security? Is there something I could test? For example, intrusion detection on private clouds, traffic capture, virtual firewalls, network access control, security of virtual disks that reside on shared storage, system hardening using SCM,