how to install game of active directory on esxi

z-sec.co/guide-to-install-game-of-active-directory-goad-on-vmwareesxi

Zeeshan Mustafa

Good day Mates!
For quite some time, I have been intending to address this matter, albeit various commitments have continuously impeded its realization.

Requirements

For GOAD installation on ESXI you need to download the following tools

1. create an ubuntu machine on ESXI server
2. ovftool —> install it on the ubuntu machine
3. pywinrm and ansible —> install it on the ubuntu machine
4. winrm —> install it on the ubuntu machine
5. winrm-fs —> install it on the ubuntu machine
6. winrm-elevated —> install it on the ubuntu machine
7. GOAD repository

STEP 1

Vagrant installation on Ubuntu Machine

1. `mkdir tools`

2. `cd tools`

3. `wget`https://releases.hashicorp.com/vagrant/2.3.7/vagrant_2.3.7-1_amd64.deb

4. `dpkg -i vagrant_2.3.7-1_amd64.deb`

STEP 2

install vagrant vmware esxi plugins

1. `vagrant plugin install vagrant-vmware-esxi`

2. `vagrant plugin install vagrant-reload`

3. `vagrant plugin install vagrant-vmware-desktop`

4. `vagrant plugin install winrm`

5. `vagrant plugin install winrm-fs`

6. `vagrant plugin install winrm-elevated`

install Ansible and pywinrm

1. `pip3 install --include-deps ansible`

2. `pip3 install ansible-core`

3. `pip3 install ansible-core==2.12.3`

4. `pip3 install pywinrm`

STEP 3

Download the Goad repository from the Github and configure some initial files for vmware_esxi compatibility

`git clone`https://github.com/Orange-Cyberdefense/GOAD

`in this directory GOAD/ansible install the “requirements.yml” file using the following command –> ansible-galaxy install -r ansible/requirements.yml`

STEP 4

In the main directory of the “GOAD” remove the previous goad.sh file and use the provided goad.sh file and replace the old file with this new one provided file.

```
management@management-virtual-machine:~/deploy/GOAD$ ls
ad  ansible  Dockerfile  docs  goad.sh  LICENSE  packer  README.md  scripts  vagrant
management@management-virtual-machine:~/deploy/GOAD$ rm -r goad.sh
```

Create a directory called “vmware_esxi” in this directory → “/GOAD/ad/GOAD-Light/providers”

```
management@management-virtual-machine:~/deploy/GOAD/ad/GOAD-Light/providers$ ls
azure  virtualbox  vmware  vmware_esxi
management@management-virtual-machine:~/deploy/GOAD/ad/GOAD-Light/providers$ mkdir vmware_esxi
```

Now we have the directory called “/GOAD/ad/GOAD-Light/providers/vmware_esxi”

```
/deploy/GOAD/ad/GOAD-Light/providers/vmware_esxi$
```

STEP 5

Now go back to the main GOAD directory and run the goad.sh

Now run the goad.sh using the follwing command:

```
bashgoad.sh-t check -l GOAD-LIGHT -p vmware_esxi -m local
```

```
management@management-virtual-machine:~/tools/GOAD$ bash goad2.sh -t check -l GOAD-Light -p vmware_esxi -m local
[√] Task: check
[√] Lab: GOAD-Light
[√] Provider: vmware_esxi
[√] Method: local
[√] folder ad/GOAD-Light/providers/vmware_esxi found
[√] Launch check : ./scripts/check.sh vmware_esxi local
Usage: ./check.sh <provider> <ansible_host>
provider must be one of the following:
 - virtualbox
 - vmware
 - azure
 - proxmox
Ansible host must be one of the following:
 - docker
 - local
[√] Check is ok, you can start the installation
```

→ 2 file will be generated they will be Vagrantfile and inventory

→ Replace these two files with these Vagrantfile & inventory in the "/GOAD/ad/GOAD-Light/providers/vmware_esxi" directory.

```
management@management-virtual-machine:~/deploy/GOAD/ad/GOAD-Light/providers/vmware_esxi$ ls
inventory  Vagrantfile
management@management-virtual-machine:~/deploy/GOAD/ad/GOAD-Light/providers/vmware_esxi$
```

Note: if you want to change the ips of DC01, DC02, SRV02 you have to change the ips inside the inventory file too. This will be used with ansible-playbook while installing the vulnerable AD-set.

STEP 6

Install the OVFTOOL in the ubuntu machine

Since our ESXI version is 8.0.2 we will download the latest version of ovftool which is “v4.6.2” from “developer.vmware.com/web/tool/4.6.2/ovf-tool”

download-Link with the wget command :

```
wgethttps://vdc-download.vmware.com/vmwb-repository/dcr-public/8a93ce23-4f88-4ae8-b067-ae174291e98f/c609234d-59f2-4758-a113-0ec5bbe4b120/VMware-ovftool-4.6.2-22220919-lin.x86_64.zip
```

```
Unzip the ovftool file by the follwing command

unzip VMware-ovftool-4.6.2-22220919-lin.x86_64.zip

echo $PATH

cd ovftool

pwd

export PATH=/home/management/tools/ovftool:/home/management/.local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
```

STEP 7

Configuring the IP addresses automatically assigned by the vagrant in the provisioning files

Go to the following directory and configure the IP addresses → “/GOAD/ad/GOAD-Light/providers/vmware_esxi”

edit the files as in the screenshots

```
Open  inventory  ~/deploy/GOAD/ad/GOAD-Light/providers/vmware_esxi  Sav
1 [default]
2 ; Note: ansible_host *MUST* be an IPv4 address or setting things like DNS
3 ; servers will break.
4 ; ----------------------------------------------
5 ; sevenkingdoms.local
6 ; ----------------------------------------------
7 dc01 ansible_host=172.70.0.70 dns_domain=dc01 dict_key=dc01
8 ; ----------------------------------------------
9 ; north.sevenkingdoms.local
10 ; ----------------------------------------------
11 dc02 ansible_host=172.70.0.74 dns_domain=dc01 dict_key=dc02
12 srv02 ansible_host=172.70.0.68 dns_domain=dc02 dict_key=srv02
13
14 [all:vars]
15 ; domain_name : folder inside ad/
16 domain_name=GOAD-Light
17
18 force_dns_server=no
19 dns_server=x.x.x.x
20 two_adapters=yes
21
22 ; adapter created by vagrant and vmware (uncomment if you use vmware)
23 nat_adapter=Ethernet1
24 domain_adapter=Ethernet0
25
26 ; winrm connection (windows)
27 ansible_user=vagrant
28 ansible_password=vagrant
```

Set the Ethernet0 IPv4 address of the each machine here

Domain adapter is considered Ethernet0 of windows

```
Open  Vagrantfile  ~/deploy/GOAD/ad/GOAD-Light/providers/vmware_esxi  Save
1 Vagrant.configure("2") do |config|
2   # Set the default provider
3   config.vm.provider :vmware_esxi do |esxi|
4     # ESXi server details
5     esxi.esxi_hostname = "[redacted]"
6     esxi.esxi_username = "[redacted]"
7     esxi.esxi_password = "[redacted]"
8   end
9
10  # Define the configuration for each Windows Server 2019 machine
11  [
12    { name: "GOAD-DC01", ip: "172.70.0.70" },
13    { name: "GOAD-DC02", ip: "172.70.0.74" },
14    { name: "GOAD-SRV02", ip: "172.70.0.68" }
15  ].each do |machine|
16    config.vm.define machine[:name] do |windows|
17      # Box settings
18      windows.vm.box = "StefanScherer/windows_2019"
19      windows.vm.box_version = ">= 2021.05.15"
20
21      # Network settings
```

Set the ip address to communicaate with the esxi machine and Credentials

Set the Ethernet0 IPv4 address of the each machine as done in the previous inventory file

STEP 8

DEPLOYING WINDOWS ACTIVE DIRECTORY MACHINES ON ESXI sever

Go to the following directory “ad/GOAD-Light/providers/vmware_esxi/” Then run the follwing command: vagrant up

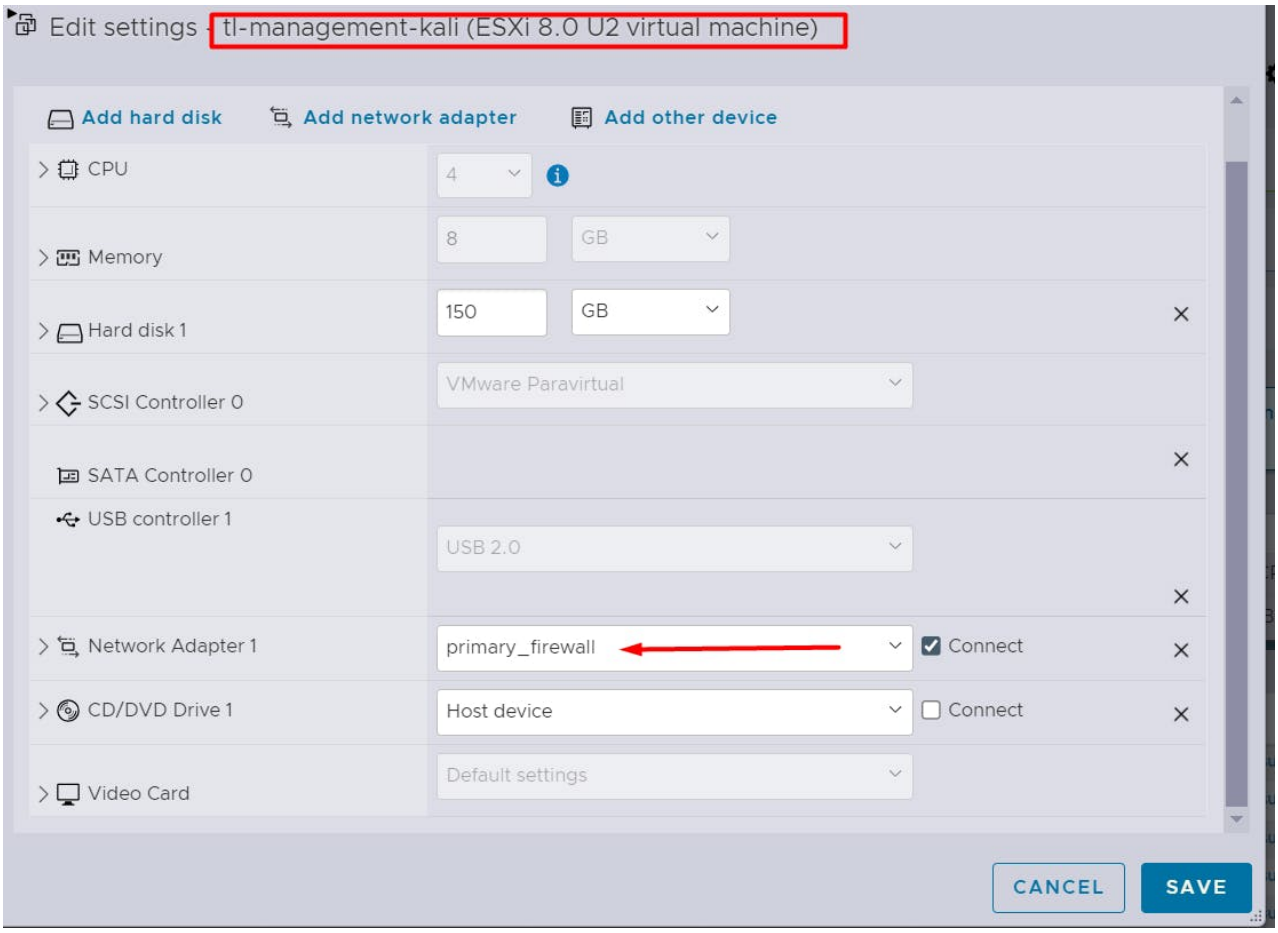
```
management@management-virtual-machine:~/tools/GOAD/ad/GOAD-Light/providers/vmware_esxi$ vagrant up

Bringing machine 'GOAD-DC01' up with 'vmware_esxi' provider...
Bringing machine 'GOAD-DC02' up with 'vmware_esxi' provider...
Bringing machine 'GOAD-SRV02' up with 'vmware_esxi' provider...
==> GOAD-DC01: Virtual Machine will be built.
==> GOAD-DC02: Virtual Machine will be built.
==> GOAD-SRV02: Virtual Machine will be built.
VMware ovftool 4.6.2 (build-22220919)
VMware ovftool 4.6.2 (build-22220919)
VMware ovftool 4.6.2 (build-22220919)
==> GOAD-SRV02: --- WARNING         : esxi_disk_store not set, using "--- Least Used ---"
==> GOAD-DC01: --- WARNING         : esxi_disk_store not set, using "--- Least Used ---"
==> GOAD-DC02: --- WARNING         : esxi_disk_store not set, using "--- Least Used ---"
==> GOAD-SRV02: --- WARNING         : esxi_virtual_network[0] not set, using primary_firewall
==> GOAD-SRV02: --- WARNING         : esxi_virtual_network[1] not found, using primary_firewall
==> GOAD-SRV02: ---   --- ESXi Summary ---
==> GOAD-SRV02: --- ESXi host       : 192.168.18.90
==> GOAD-SRV02: --- Virtual Network : ["primary_firewall", "primary_firewall"]
==> GOAD-SRV02: --- Disk Store      : Hard 2
==> GOAD-SRV02: --- Resource Pool   : /
==> GOAD-SRV02: ---  --- Guest Summary ---
==> GOAD-SRV02: --- VM Name         : GOAD-SRV02.GOAD
==> GOAD-SRV02: --- Box             : StefanScherer/windows_2019
==> GOAD-SRV02: --- Box Ver         : 2021.05.15
==> GOAD-SRV02: --- Memsize (MB)    : 2048
==> GOAD-SRV02: --- CPUS            : 2
==> GOAD-SRV02: --- Guest OS type   : windows9srv-64
==> GOAD-SRV02: ---   --- Guest Build ---
==> GOAD-DC02: --- WARNING         : esxi_virtual_network[0] not set, using primary_firewall
==> GOAD-DC02: --- WARNING         : esxi_virtual_network[1] not found, using primary_firewall
==> GOAD-DC02: ---   --- ESXi Summary ---
==> GOAD-DC02: --- ESXi host       : 192.168.18.90
==> GOAD-DC02: --- Virtual Network : ["primary_firewall", "primary_firewall"]
==> GOAD-DC02: --- Disk Store      : Hard 2
==> GOAD-DC02: --- Resource Pool   : /
==> GOAD-DC02: ---  --- Guest Summary ---
==> GOAD-DC02: --- VM Name         : GOAD-DC02.GOAD
==> GOAD-DC02: --- Box             : StefanScherer/windows_2019
==> GOAD-DC02: --- Box Ver         : 2021.05.15
==> GOAD-DC02: --- Memsize (MB)    : 2048
==> GOAD-DC02: --- CPUS            : 2
==> GOAD-DC02: --- Guest OS type   : windows9srv-64
==> GOAD-DC02: ---   --- Guest Build ---
==> GOAD-DC01: --- WARNING         : esxi_virtual_network[0] not set, using primary_firewall
==> GOAD-DC01: --- WARNING         : esxi_virtual_network[1] not found, using primary_firewall
==> GOAD-DC01: ---   --- ESXi Summary ---
==> GOAD-DC01: --- ESXi host       : 192.168.18.90
==> GOAD-DC01: --- Virtual Network : ["primary_firewall", "primary_firewall"]
==> GOAD-DC01: --- Disk Store      : Hard 2
==> GOAD-DC01: --- Resource Pool   : /
==> GOAD-DC01: ---  --- Guest Summary ---
==> GOAD-DC01: --- VM Name         : GOAD-DC01.GOAD
==> GOAD-DC01: --- Box             : StefanScherer/windows_2019
```

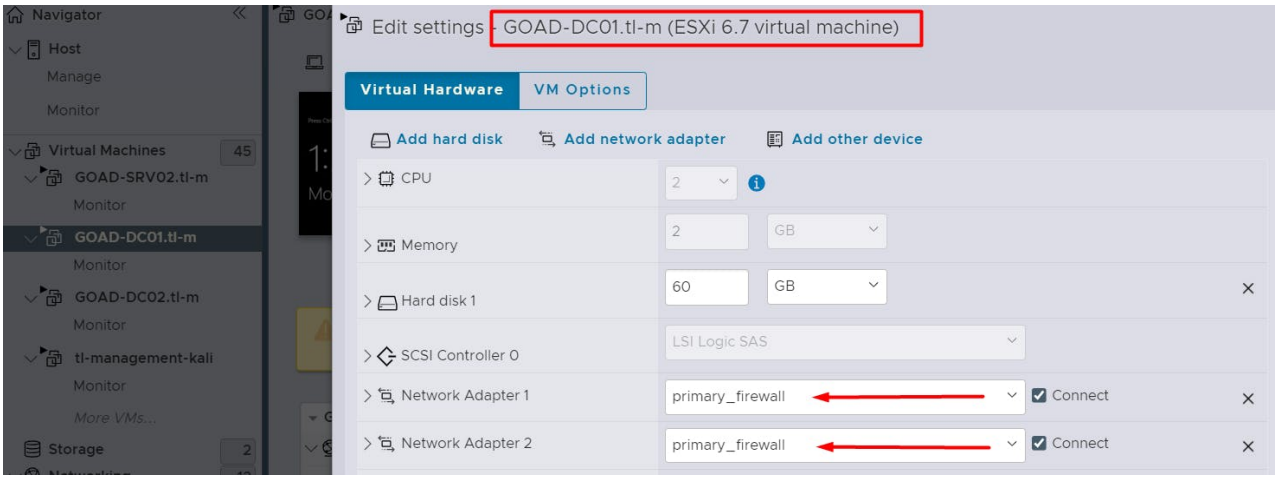
check the adapters of the machines deployed using the vagrant up command

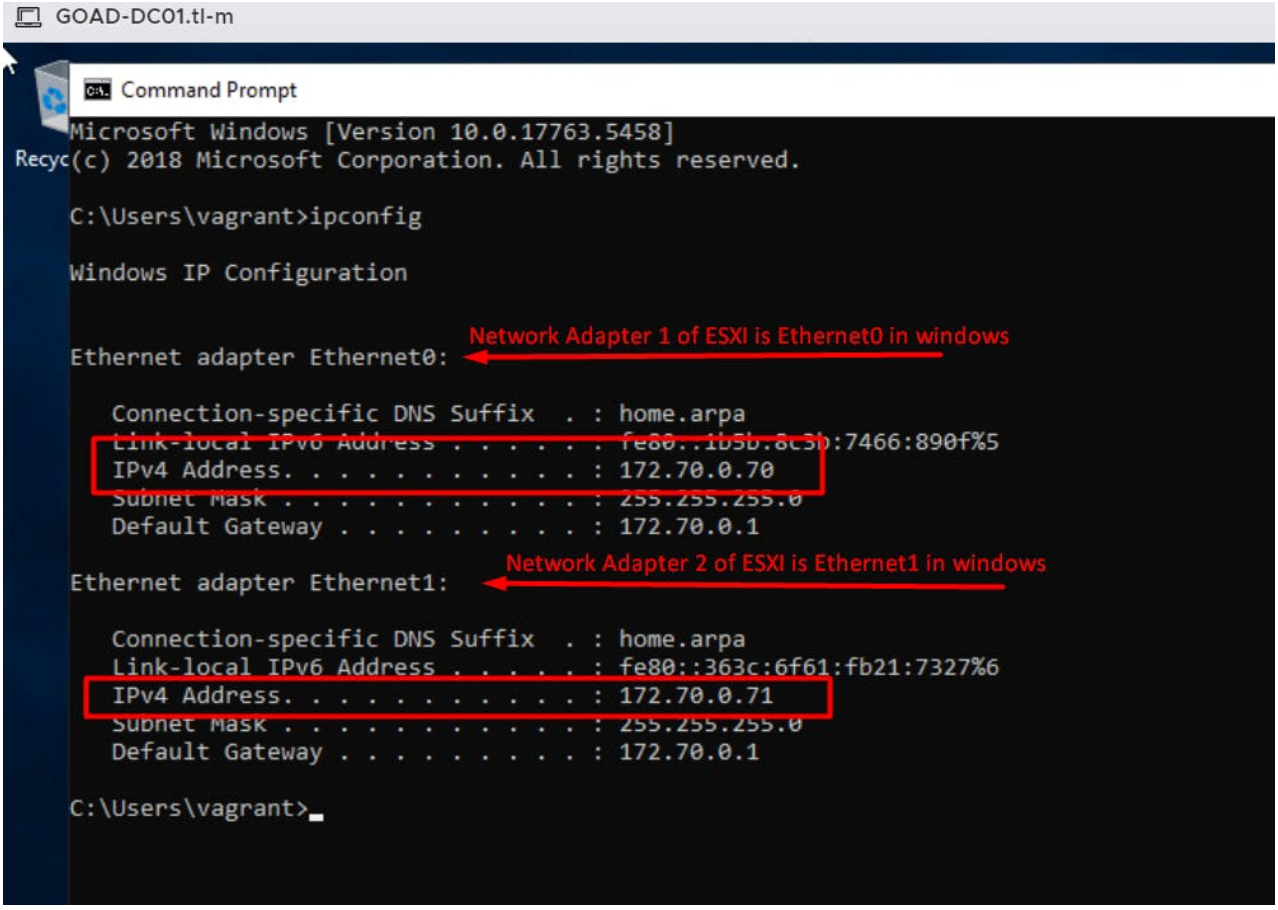
POC of the network adapter of the ubuntu machine

Ubuntu Machine is on the same network as the DCO1 Adapters



POC: we don't need to change the adapters in order for the provisioning to work properly both of the adapters should be on the same network like in the following screenshots





This is the network scheme of all the machines

Important Note: Goad provisioning file considering Ethernet0 as the domain adapter and Ethernet1 as the NAT adapter. We will configure the domain adapter IP addresses in the inventory and the Vagrant file before provisioning.

```
DCO1

Ethernet adapter Ethernet0: IPv4 Address. . . . . : 172.70.0.70

Ethernet adapter Ethernet1: IPv4 Address. . . . . : 172.70.0.71

DC02

Ethernet adapter Ethernet0: IPv4 Address. . . . . : 172.70.0.74

Ethernet adapter Ethernet1: IPv4 Address. . . . . : 172.70.0.75

SRV02

Ethernet adapter Ethernet0: IPv4 Address. . . . . : 172.70.0.68

Ethernet adapter Ethernet1: IPv4 Address. . . . . : 172.70.0.69
```

STEP 9

Start the provisioning using the ansible

Go to the following directory “/GOAD/ansible”

Run the following command before provisioning:

```
export ANSIBLE_COMMAND="ansible-playbook -i ../ad/GOAD-Light/data/inventory
-i ../ad/GOAD-Light/ providers/vmware_esxi/inventory"
```

Run the following command to run the provisioning: `../scripts/provisionning.sh`

Special Thanks to my friend Syed Asadullah for the help especially in networking part he has done a great job.