**Installing Baseline Active Directory with File Share, on Two Windows 10 Hosts with ESXi & PfSense-V1.0**

Change Control - **Version**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Rationale** |
| 1.0 | 12/23/2023 | Josh Lampman | Guide on how to setup basic lab in AD with File Share on ESXI with PfSense. |

**Introduction**

This guide will demonstrate how to set up a baseline Active Directory lab in ESXI for learning purposes, and we will expand on cybersecurity topics in a future guide which is why we will need to have a segmented network to protect our home network from malicious activity.

What you will need,

1. ESXI is already installed.
2. Download VMRC to have better remote console to ESXI VM’s.
3. PfSense ([pfSense® - World's Most Trusted Open Source Firewall](https://www.pfsense.org/)).
4. Windows Server ([Microsoft Evaluation Center](https://www.microsoft.com/en-us/evalcenter)).
5. Windows 10([Microsoft Evaluation Center](https://www.microsoft.com/en-us/evalcenter)).
6. 16GB to 32GB of RAM, anything over 32GB would be perfect.
7. 500GB of free disk space is more than enough to set the lab up.

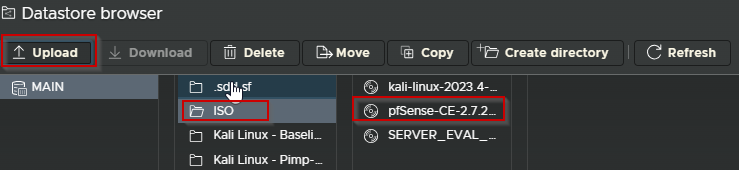
\*If you have any issues during this guide hitting function keys, f11, etc., please make sure to hold the function(fn) key at the same time.

**PfSense Installation (DHCP Server)**

Once you have downloaded the PfSense ISO to your desktop from the PfSense website, you’re now ready to upload the ISO the ESXI Datastore. I store my ISOs under a directory I created called ISO’s.

A screenshot of a computer

Description automatically generated



\*Please make sure you download the AMD64/ISO installer. Please unzip once downloaded. I use 7ZIP (free). At this point you should have .ISO PfSense file, we will proceed with installation.

Before we create the PfSense VM we will need two physical adapters to set the WAN/LAN interfaces. We will create a port group in ESXI with VLAN 30 to segment our traffic.

1. Under the networking tab, please click on the ‘VM Network’, and click ‘settings’, and change the name of the Port Group to ‘WAN’, see picture.A screenshot of a computer

   Description automatically generated
2. Click to expand on ‘Security’ and accept promiscious mode, MAC Address Changes, and Forged Transmits then click ‘Save’A screenshot of a computer

   Description automatically generated
3. Next, under Networking, click + Add Port Group, and add the following settings then click save. We’re now ready to create the VM A screenshot of a computer

   Description automatically generated

1. Please click on Create/Register VM

A screenshot of a computer

Description automatically generated

2. Select ‘Create New Virtual Machine. Click next.

A screenshot of a computer

Description automatically generated

3. Here are the current settings (subject to change). Click next.

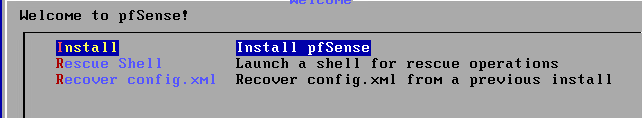
A screenshot of a computer program

Description automatically generated

4. Select storage drive. I have a 1TB drive I will use. Click next.

5. On the next screen you will be able to customize the VM settings, please use these settings

* CPU – **2**
* Memory- **2 GB**
* Hard Disk 1(expand with down arrow) – **32GB** - **Thin Provisioning**
* SCSI Controller 0 – **LSI Logic SAS**
* Network Adapter 1: **WAN**
* Adapter Type: **VMXNET 3**
* Network Adapter 2**: HackLAB-30 \*Click add Network Adapter at the top** ****
* Adapter Type: **VMXNET 3**
* CD/DVD Media: **DataStore ISO File – Browse: Selected PfSense ISO**
* Click Next, and then ‘Finish’

1. Once your PfSense VM is booting up, you should be greeted with a ‘Copyright and Distribution Notice’, please click accept.
2. The next screen is where we will hit enter on ‘Install’ and hit enter on ok to proceed
3. For a single disk, I’m using ‘Auto UFS’A screen shot of a computer

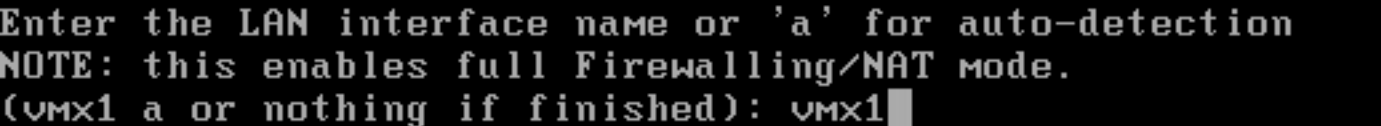
   Description automatically generated
4. Hit enter on ‘Entire Disk’, Select da0 as MBR, Finsh, and Commit to proceed. The installer will verify checksums, and continue to install
5. Once done please click ‘Reboot.’

**Summary**

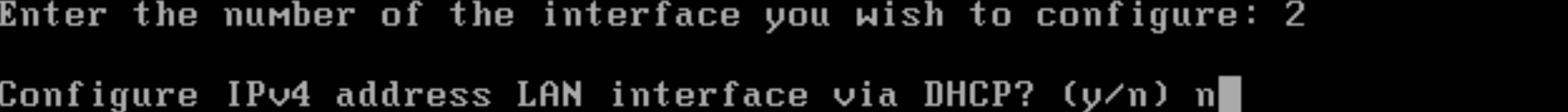
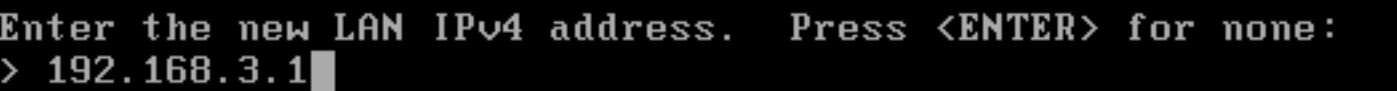
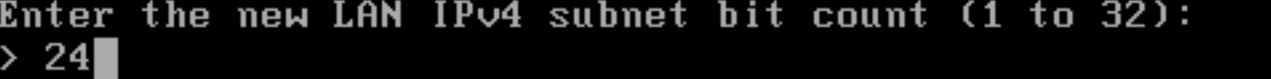
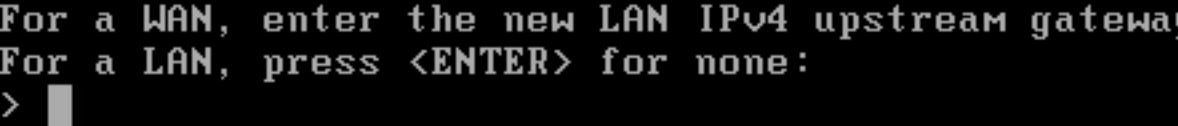
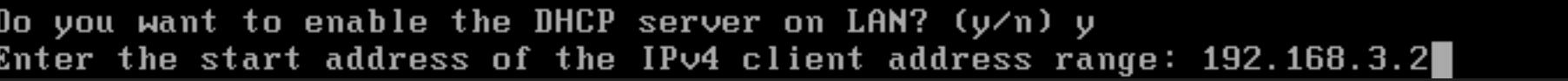
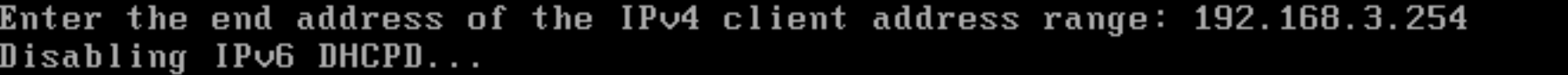
At this point our ESXI host will be utilizing 2GB of RAM, 32GB of HD space for the PfSense VM. We have also added an extra virtual network adapter attached to HackLab-30

In this section, we will be setting PfSense up, so that we will have a DHCP server for our hosts.

**PfSense Configuration**

1. Please start up your PfSense VM, and let it boot up.
2. Once the PfSense VM has booted up, you will see a message regarding VLANS****
3. Please click ‘No’.
4. Please type in vmx0 for the WAN interface, then enter.
5. Please type in vmx1 for the LAN interface, then enter. 
6. Please type ‘y’ for the next prompt A black screen with white text

   Description automatically generated
7. At the next screen you will see IP information with a bunch of numbered options. Please enter option #2 – ‘Set Interface(s) IP Address’.
8. Click 2 for LAN(VMX1).A black screen with white text

   Description automatically generated
9. Enter ‘n’ for configuring via DHCP.
10. Type in 192.168.3.1, then click ‘enter’.
11. Then type in 24 since we’re using a class C 255.255.255.0 private network.
12. Hit enter on this prompt 
13. Hit Enter ‘none’ for configuring IPv6 Address to proceed.
14. Hit Enter ‘none’ for new LAN IPv6 address to proceed
15. Enter ‘y’ for DHCP server on LAN ****
16. Type the start address of 192.168.3.2 
17. Type the end address of 192.168.3.254 
18. Enter ‘n’ on reverting to HTTP, and then hit ‘Enter’ to continue after web configuration message displays.
19. PfSense Configuration Complete

**Installing Windows Server 2022**

At this point, we’re configured with Pfsense, and we now have a DHCP Server, and some flexibility with our lab going forward. Next, we will install the Windows server, and set up our Active Directory Domain.

Microsoft allows the ability to download evaluation/trials of Windows, and that’s where we will get our ISO from. Navigate to the Microsoft Evaluations page, find Windows server, and download the 64Bit ISO. Microsoft will make you enter in some info, but this information can be false.

A screenshot of a computer

Description automatically generated

A close up of a white background

Description automatically generated

Now that you know how to upload an ISO, and how to create a VM, here are the settings we will use for Windows Server 2022:

\*You can use more memory/RAM during installation, and then bring it back down to 4GB after so that things can go a little quicker

* Name: **Hydra-DC \*I’ll be using Marvel theme for AD Domain**
* Compatibility: **ESXI 8.0**
* Guest OS Family: **Windows**
* Guest OS Version**: Windows Server 2022(64 Bit)**
* CPU – **4**
* Memory- **8 GB**
* Hard Disk 1(expand with down arrow) – **32GB** - **Thin Provisioned**
* SCSI Controller 0 – **VMware Paravirtual**
* Network Adapter 1: **HackLab-30**
* Adapter Type: **VMXNET 3**
* CD/DVD Media: **DataStore ISO File – Browse: Selected Windows Server**
* Under VM Options, uncheck ‘Enable UEFI Secure Boot’ A screenshot of a computer program

  Description automatically generated
* Click Next, and then ‘Finish.’

**Windows Server 2022-Installation**

1. If VM doesn’t start, please double check settings.
2. Press any key to boot to CD/ROM ISO, click ‘Install.’
3. Please Select ‘Windows Server 2022 Standard Evaluation (Desktop Experience), and click ‘Next’ A blue and white text

   Description automatically generated
4. Select Custom, and then you can select ‘Drive 0 unallocated Space’ as your storage drive. If the drive is not visible, please shutdown VM, and doublecheck settings, click next.
5. Windows will continue to install. Sit back & relax. (approx., 10-15 minutes)
6. When prompted please enter a password, I will use P@$$w0rd!
7. We’re done installing Windows Server 2022. Please login and click ‘Yes’ on the network sidebar. A screenshot of a blue screen

   Description automatically generated
8. Please open your ‘Command Prompt’ in Windows, and type ‘ipconfig’ you should have the following information
   1. IPv4 Address: 192.168.3.X, mine is 192.168.3.11
   2. Subnet Mask: 255.255.255.0
   3. Default Gateway: 192.168.3.1
9. Take note of your IPv4 address, and navigate to control panel > Network and Sharing Center, and click on ‘Change Adapter settings’ on the left side A screenshot of a computer

   Description automatically generated
10. Find Internet Protocol Version 4(TCP/IPv4), and then click ‘properties’ A screen shot of a computer

    Description automatically generated
11. We will configure the adapter without a gateway, so we can protect our AD Domain from the internet in future guides. We want to create a sandbox environment. Click ‘OK’ to proceed. A screenshot of a computer

    Description automatically generated

**Finish setting up PfSense**

**Windows Server 2022 – Initial configuration**

1. Please install VMware Tools, so that it’ll provide the drivers for full screen. A screenshot of a computer

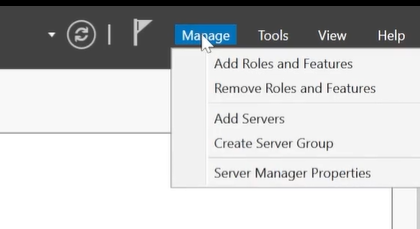
   Description automatically generated
2. Click on the notification A screenshot of a computer

   Description automatically generated, then click ‘setup 64’. Then click on ‘Complete’, ‘Next to install.
3. VMware Tools will need to restart to take effect, deny a restart for now
4. In the search bar please type ‘view your pc name’ and click on it.
5. Next, click on ‘rename this pc’ A screenshot of a computer

   Description automatically generated
6. Since I will be using MARVEL theme, I’ll type in ‘HYDRA-DC’, and hit next A blue box with white text

   Description automatically generated
7. Please restart your machine by clicking ‘Restart Now’

**Windows Server 2022 – Configuring Domain Controller (DC)**

1. You should now be able to full screen your view in VMRC.
2. Please open ‘Server Manager’, and click on Manage > Add Roles and Features 
3. On the ‘Before you begin page’ click next A screenshot of a computer

   Description automatically generated
4. Select ‘Role-Based or Feature Based installation’, and then click next. A black text on a white background

   Description automatically generated
5. Highlight HYDRA-DC, and then click ‘next’ A screenshot of a computer

   Description automatically generated
6. Under ‘Select Server Roles’ you will see Active Directory Domain Services, check the box, and hit next, then ‘Add Features’, and hit next A screenshot of a computer

   Description automatically generated
7. Nothing to check on ‘Features’ just hit next to proceed
8. Nothing to check on ‘AD DS’ just hit next to proceed
9. Check the box ‘Restart the destination server automatically if required A white background with black text

   Description automatically generated
10. Now click ‘Install’. This will take some time.(approx 2 minutes)
11. Once completed click on ‘Promote this server to a domain controller’ A screenshot of a computer

    Description automatically generated
12. Select ‘Add a new Forest’ A white background with black text

    Description automatically generated
13. Type in MARVEL.local in field, hit next, type in password, I will use P@$$w0rd! and then hit next all the way through until you see install. (approx., 2 minutes), and then Server 2022 will reboot.A screenshot of a computer

    Description automatically generated A screenshot of a computer

    Description automatically generated
14. Log in to your Server VM with the password of P@$$w0rd! for MARVEL\Administrator
15. Launch Server Manager
16. Navigate to Manage > Add Roles and Features > Role Based or Feature-Based installation, and click next until ‘Server Roles’
17. Check the box for ‘Active Directory Certificate Services’, and click ‘Add Features’, click next A screenshot of a computer

    Description automatically generated
18. Once you reach the confirmation screen, check ‘Restart the destination server automatically if required’, and then click install(approx 1 minute)A screenshot of a computer

    Description automatically generated
19. Click on ‘Configure Active Directory Certificate Services on the destination server’ , and click next A screenshot of a computer

    Description automatically generated
20. Check the box ‘Certificate Authority.’ And click next.
21. Click next for the defaults all the way to ‘Confirmation’ then click ‘Configure’ to complete (approx. 1 minute)

**Windows Server 2022 – Setting up Windows 10 - ESXI**

Please find the Windows 10 – 64 Bit ISO on Microsoft’s Evaluation page and download it to your machine and upload it to the ESXI Datastore.

Please set up the Windows 10 ESXI VM’s with the following settings. If you need to conserve RAM, please install one at a time. For this example, I’m using 8GB of RAM per machine.

* Name: **PUNISHER**
* Compatibility: **ESXI 8.0**
* Guest OS Family: **Windows**
* Guest OS Version**: Windows 10(64BIT)**
* CPU – **4**
* Memory- **8 GB**
* Hard Disk 1(expand with down arrow) – **32GB** - **Thin Provisioned**
  + Controller Location: **SATA Controller 0**
* SCSI Controller 0 – **VMware Paravirtual**
* Network Adapter 1: **HackLab-30**
* Adapter Type: **VMXNET 3**
* CD/DVD Media: **DataStore ISO File – Browse: Select Windows 10**
* Under VM Options: **Uncheck ‘UEFI Secure Boot’**
* **Install VMware Tools once Windows 10 is installed.**
* Name: **SPIDERMAN**
* Compatibility: **ESXI 8.0**
* Guest OS Family: **Windows**
* Guest OS Version**: Windows 10(64BIT)**
* CPU – **4**
* Memory- **8 GB**
* Hard Disk 1(expand with down arrow) – **32GB** - **Thin Provisioned**
  + Controller Location: **SATA Controller 0**
* SCSI Controller 0 – **VMware Paravirtual**
* Network Adapter 1: **HackLab-30**
* Adapter Type: **VMXNET 3**
* CD/DVD Media: **Datastore ISO File – Browse: Select Windows 10**
* Under VM Options: **Uncheck ‘UEFI Secure Boot’**

**Windows 10 – Configuring OS**

**Punisher – Windows 10 VM - Steps**

1. Once the OS is done installing, and you’re going through setup click ‘Next.’
2. Click ‘I don’t have internet’ & ‘Continue with limited setup’ or ‘Domain Join Instead.’
3. Under ‘Who’s going to use this PC’ put **frankcastle** A screenshot of a computer

   Description automatically generated
4. For password we’re going to use **Password1**
5. Put in false values for all of the security questions, and hit next
6. On the Privacty Settings page slide everything to ‘NO’ and click ‘Accept’
7. Hit ‘Not now’ on Cortana
8. Once able to login **Install VMware Tools**
9. Click ‘Yes’ to allow New Network on right side of screen.
10. Rename PC to **PUNISHER**

**SPIDERMAN – Windows 10 VM - Steps**

1. Once the OS is done installing, and you’re going through setup click ‘Next.’
2. Click ‘I don’t have internet’ & ‘Continue with limited setup’ or ‘Domain Join Instead.’
3. Under ‘Who’s going to use this PC’ put **peterparker**
4. For password we’re going to use **Password1**
5. Put in false values for all of the security questions, and hit next
6. On the Privacty Settings page slide everything to ‘NO’ and click ‘Accept’
7. Hit ‘Not now’ on Cortana
8. Once able to login **Install VMware Tools**
9. Click ‘Yes’ to allow New Network on right side of screen.
10. Rename PC to **SPIDERMAN**

\*Be sure to manually configure the IPv4 adapter settings in Windows, so that the IP’s will not change.

**Windows Server 2022 – Hydra DC – Configuring users.**

1. Please login to your DC
2. Launch Server Manager if it doesn’t AutoStart by itself.
3. Click on Tools, and navigate to Active Directory Users & Computers A screenshot of a computer

   Description automatically generated
4. In order to cleanup the Users group, right click on Marvel.local, and click on ‘New’, and select Organizational Unit(OU) and name the OU **Groups**A screenshot of a computer

   Description automatically generated
5. Highlight all of the accounts listed under users, and move to the new OU called Groups, except for Guest & Administrator A screenshot of a computer

   Description automatically generated
6. Right click the white space within users and select New > User A screenshot of a computer

   Description automatically generated
7. Create a user account called [fcastle@MARVEL.local](mailto:fcastle@MARVEL.local) with a password of Password1 A screenshot of a computer

   Description automatically generated
8. Uncheck ‘User Must change Password at next logon, and check ‘Password Never Expires’ and then click next A screenshot of a login box

   Description automatically generated
9. Create another user account called [pparker@MARVEL.local](mailto:pparker@MARVEL.local) with a password of Password2

**Windows Server 2022 – Creating a file share – Domain Controller**

1. Open Server Manager, and on the left click ‘File & Storage Services’ A screenshot of a computer dashboard

   Description automatically generated
2. Then click on ‘New Share’ under tasks A screenshot of a computer

   Description automatically generated
3. Call the share ‘hacklab’ and click next A screenshot of a computer

   Description automatically generated
4. Click through next until you see ‘create’, and then click it A screenshot of a computer

   Description automatically generated

**Setting IPv4 manually, and DNS Server Address– MARVEL.local**

1. Login to the PUNISHER machine with Password1
2. Navigate to Control Panel > Network and Sharing Center > Change Adapter Settings > TCP/IPv4 you will need statically assign your IP (yours may be different). Under Preferred DNS Server you will need to put in the IP of your Domain Controller. In my case my HYDRA-DC IP is 192.168.3.11 A screenshot of a computer

   Description automatically generated
3. Click ‘OK’ to save
4. Repeat on SPIDERMAN machine

**Joining Users Hosts to Active Directory Domain – MARVEL.local**

1. In the Windows Search bar, type ‘Domain A screenshot of a black screen

   Description automatically generated
2. Click on ‘Access Work Or School’, then click on ‘connect’ A screenshot of a computer

   Description automatically generated
3. Click on ‘Join Locally’ A close-up of a logo

   Description automatically generated
4. Type MARVEL.local in the box, and then click next. A blue rectangle with white text

   Description automatically generated
5. Type in ‘administrator’, and ‘P@$$w0rd1’ A screenshot of a computer screen

   Description automatically generatedA screenshot of a computer

   Description automatically generated
6. Make sure both User Account & Account Type say ‘administrator, and click ‘next, then click ‘Restart now’ A blue box with white text

   Description automatically generated
7. Replicate process on SPIDERMAN machine
8. After rebooting both machines should be on the domain

**Confirming Users are now logged onto the domain – MARVEL.local**

1. Open Active Directory Users & Computers, and then click on Computers A screenshot of a computer

   Description automatically generated

**Confirming File Share is accessible -** [**\\HYDRA-DC\hacklab - MARVEL.local**](file:///\\HYDRA-DC\hacklab%20-%20MARVEL.local)

1. Click on ‘File Explorer’, and navigate to the Network Tab and click on itA screenshot of a computer

   Description automatically generatedA screenshot of a computer

   Description automatically generated
2. Once you click on ‘Network’ you will get a ‘Network Discovery & File Sharing are turned off’ A screenshot of a computer

   Description automatically generated
3. Click on the banner, and select ‘Turn on Network Discovery and File Sharing A screenshot of a computer error

   Description automatically generated
4. Please click on ‘Turn on Network Discovery and file sharing.’
5. Once Network Discovery is enabled, you should be able to see the HYDRA-DC machine, and now the File Share is availableA computer screen shot

   Description automatically generatedA computer screen shot of a person holding a box

   Description automatically generated

\*If unable to get access to file share please try and reinstall VMware tools and reboot the DC. It took me a few tries to get it working.

**End of Guide**